Embedded Video Storage (EVS71 Dual-Controller Series)

User’s Manual

V1.0.0

Foreword

General

This User's Manual (hereinafter referred to as "the manual") introduces the functions and operations of the EVS (hereinafter referred to as "the Device").

Model

EVS7124D, EVS7148D

In the name EVS71XXD, XX refers to HDD number (24 or 48); D indicates that the device is has two controllers.

Safety Instructions

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

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

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	September 2020

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.

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

Important Safeguards and Warnings

Operation Requirement

- Do not place or install the Device in a place exposed to sunlight or near the heat source.
- Keep the Device away from dampness, dust or soot.
- Keep the Device installed horizontally on the stable place to prevent it from falling.
- Do not drop or splash liquid onto the Device, and Make sure that there is no object filled with liquid on the Device to prevent liquid from flowing into the Device.
- Install the Device in a well-ventilated place, and do not block the ventilation of the Device.
- Operate the device within the rated range of power input and output.
- Do not dissemble the Device.
- Transport, use and store the Device under the allowed humidity and temperature conditions.

Electrical Safety

- Improper battery use might result in fire, explosion, or inflammation.
- When replacing battery, make sure that the same model is used.
- Use the recommended power cables in the region and conform to the rated power specification.
- Use the power adapter provided with the Device; otherwise, it might result in people injury and device damage.
- The power source shall conform to the requirement of the Safety Extra Low Voltage (SELV) standard, and supply power with rated voltage which conforms to Limited power Source requirement according to IEC60950-1. Please note that the power supply requirement is subject to the device label.
- Connect the device (I-type structure) to the power socket with protective earthing.
- The appliance coupler is a disconnection device. When using the coupler, keep the angle for easy operation.

Attention

Do not insert or take out the expansion drawer without power off first.

Table of Contents

1 Overview

1.1 Introduction

The Device is designed for the management, storage and application of high-definition video data. It uses Linux operation system and professional customized hardware platform, and it is configured with multiple Hard Disk Drive (HDD) management system, front-end HD device management system, HD video analysis system and large capacity video storage system.

It adopts high-traffic data network transmission & forward technology and multi-channel video decoding & display technology, and realizes intelligent management, secure storage, fast forwarding and HD decoding of large capacity and multi-channel HD video data.

The Device provides standard network file sharing service and offers integrated IPSAN solution. It provides centralized storage solutions with large capacity, high scalability and high security for all kinds of video monitoring systems.

1.2 Front Panel

Figure 1-1 EVS7124D

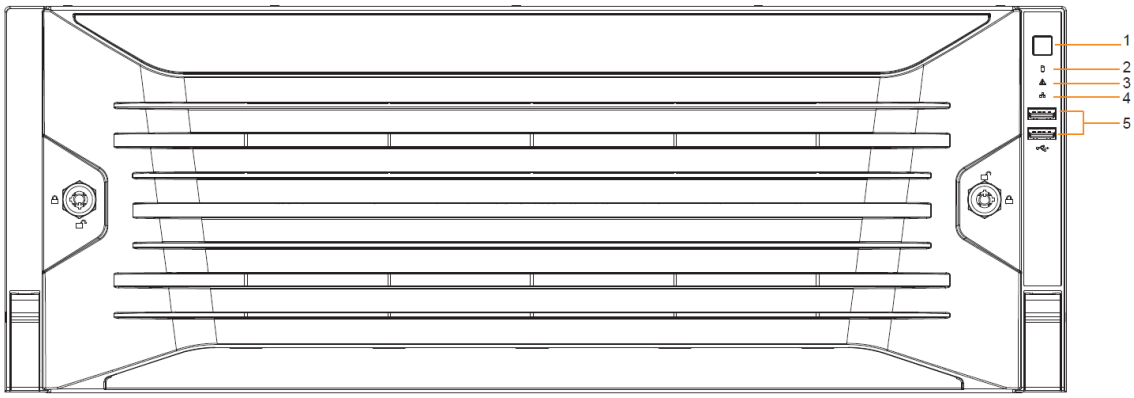


Figure 1-2 EVS7148D

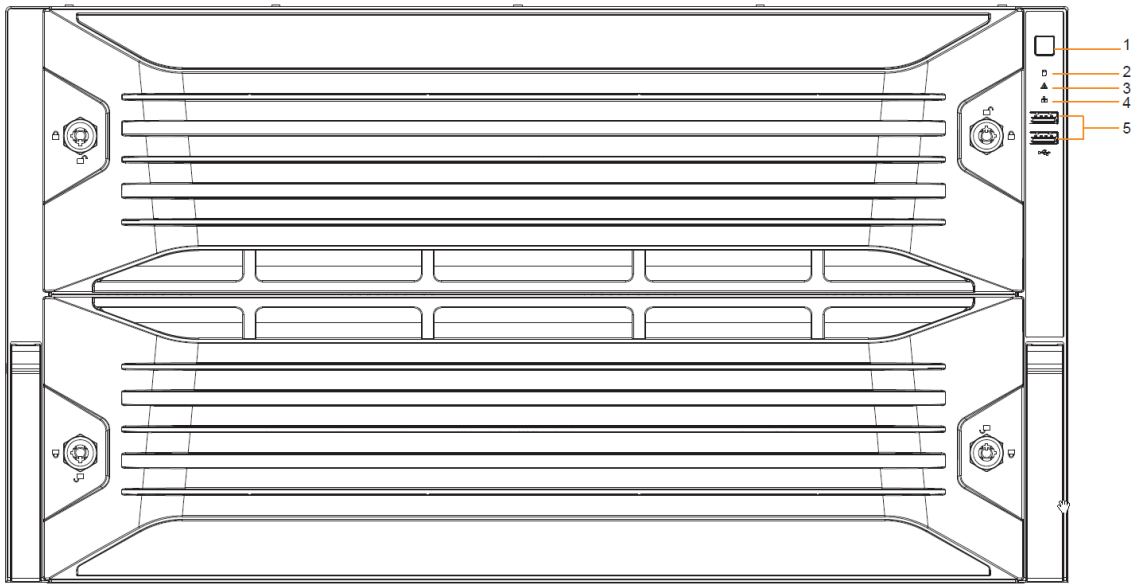


Table 1-1 Front panel interfaces

No.	Indicator/Button	Description
1	Power button	Turns on or off the Device. If the Device is off, press this button to turn the Device on. To turn off the Device, press and hold this button for five seconds.
2	HDD status indicator	The light is out when the HDD is in normal operation. The red light keeps on if no HDD, HDD error or insufficient HDD space.
3	Alarm status indicator	The light is out when the Device is running properly. The red light keeps on when the power, temperature or fan is abnormal.
4	Network status indicator	The red light keeps on if there is a network failure, IP conflict or MAC conflict.
5	USB Ports	Connects to external USB devices, such as flash drive.

1.3 Rear Panel

Figure 1-3 EVS7124D

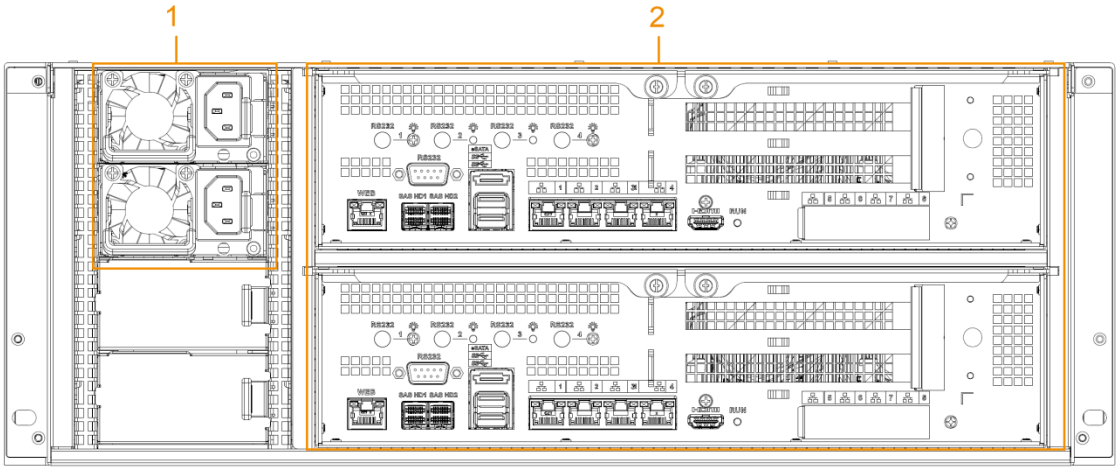


Figure 1-4 EVS7148D

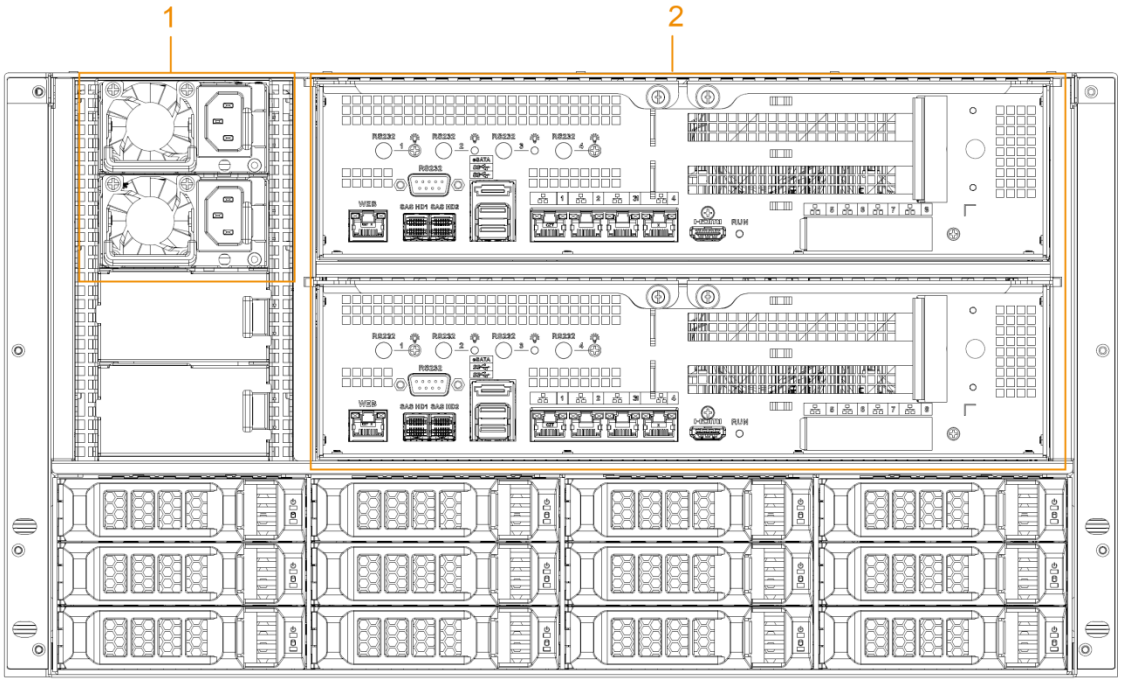


Table 1-2 Rear panel interfaces

No.	Interface	Description
1	Power module	AC power; with fan.
2	Main control module	For description of the interfaces and indicators, see Table 1-3.

Table 1-3 EVS71XXD master control module interfaces

Port/Indicator	Description
RS-232	Connects to RS-232 port for debugging.
WEB	Gigabit management port. Can be used as data port.
SAS HD	Connects the IN interface of the expansion cabinet.
eSATA	Connects to external storage devices.
USB 3.0	Connects the mouse or other USB storage devices.
EX-1–EX-4/1–4	Gigabit Ethernet ports, can be used to transfer data.
HDMI	Outputs high definition video data and multi-channel audio data to external displays.
PCI-E X8	High-speed expansion port, connects to components with X8 plug.
PCI-E X4	High-speed expansion port, connects to components with X4 plug.

1.4 Menu Items

This section introduces the icons and buttons you will frequently use when using the Device.

Table 1-4 Icons and buttons

Icon/Button	Description
Copy	After setting a channel, click this icon and you can copy the configuration of the current channel to other channels.

Icon/Button	Description
Default	Click this icon to restore default configuration. Click **OK** to save the default configuration.
Refresh	Click this icon to get the latest configuration information.
OK	Click this icon to save the modified configuration item.
Cancel	Click this icon to cancel the modified configuration item and close the window.
	Check box. You can select multiple configuration items at the same time. : Selected.
	Radio button. You can select a configuration item. : Selected.
	Drop-down list. Click this icon to display the drop-down menu.

2 Installation and Powering Up

2.1 Installing HDD

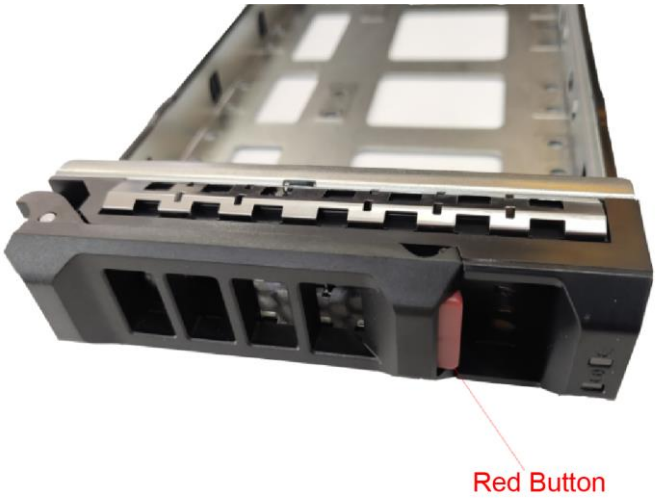
The HDD is not installed by default on factory delivery. You need to install it by yourself.

WARNING

Some devices are heavy and should be carried jointly by several persons to avoid injury.

Step 1 Press the red button on the disk tray to unlock the handle. See Figure 2-1.

Figure 2-1 Opening the handle

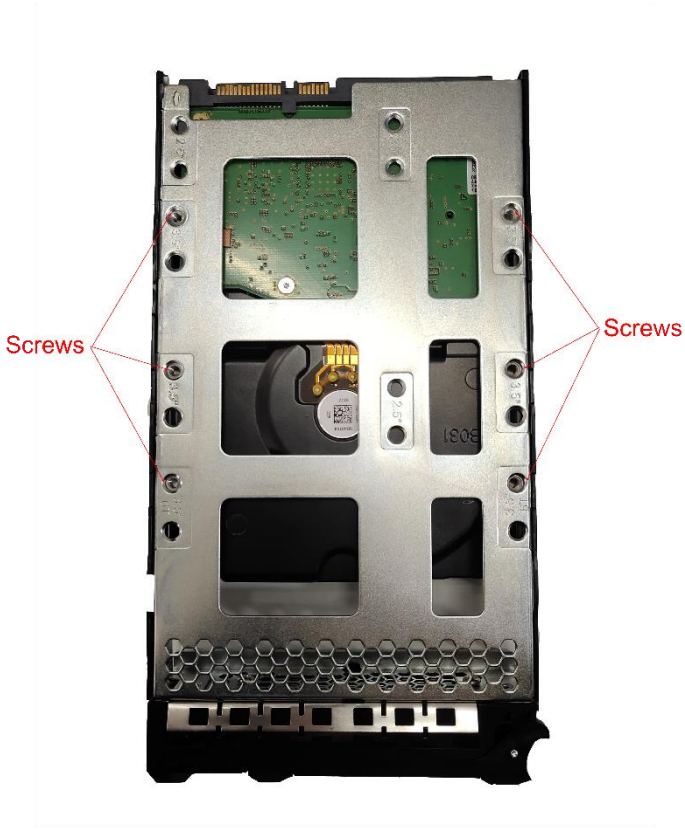


Step 2 Pull out the empty disk tray. See Figure 2-2.

Figure 2-2 Disk tray

Step 3 Put the disk into the disk tray and fasten the screws at the bottom of the tray. See Figure 2-3.

Figure 2-3 Fastening the screws



To avoid any damage to the slot, do not lock the handle until the disk tray has been pushed to the bottom.

Step 4 Insert the disk tray into the HDD slot, push it to the bottom and lock the handle.

2.2 Powering Up

2.2.1 Preparation

Properly connect the cables before powering up the Device and check against the following items:

- Make sure that all power lines are connected correctly.
- Check whether the supplied power voltage complies with device requirements.
- Check whether the network cables and SAS cables are connected correctly.

2.2.2 Powering Up the Device

Press the power button on the front panel, and then check whether the indicators are normally displayed.

- When the indicators are normal, the Device is powered up successfully.
- If the indicators are abnormal, remove the abnormalities according to the corresponding notes and power up the Device again.

3 Initial Settings

When using EVS for the first time, initialize the device, and set basic information and functions first.

3.1 Initializing Device

If it is your first time to use the Device after purchasing or after restoring factory defaults, set a login password of admin (system default user). At the same time, you can set proper password protection method.

Take web remote initialization for example.

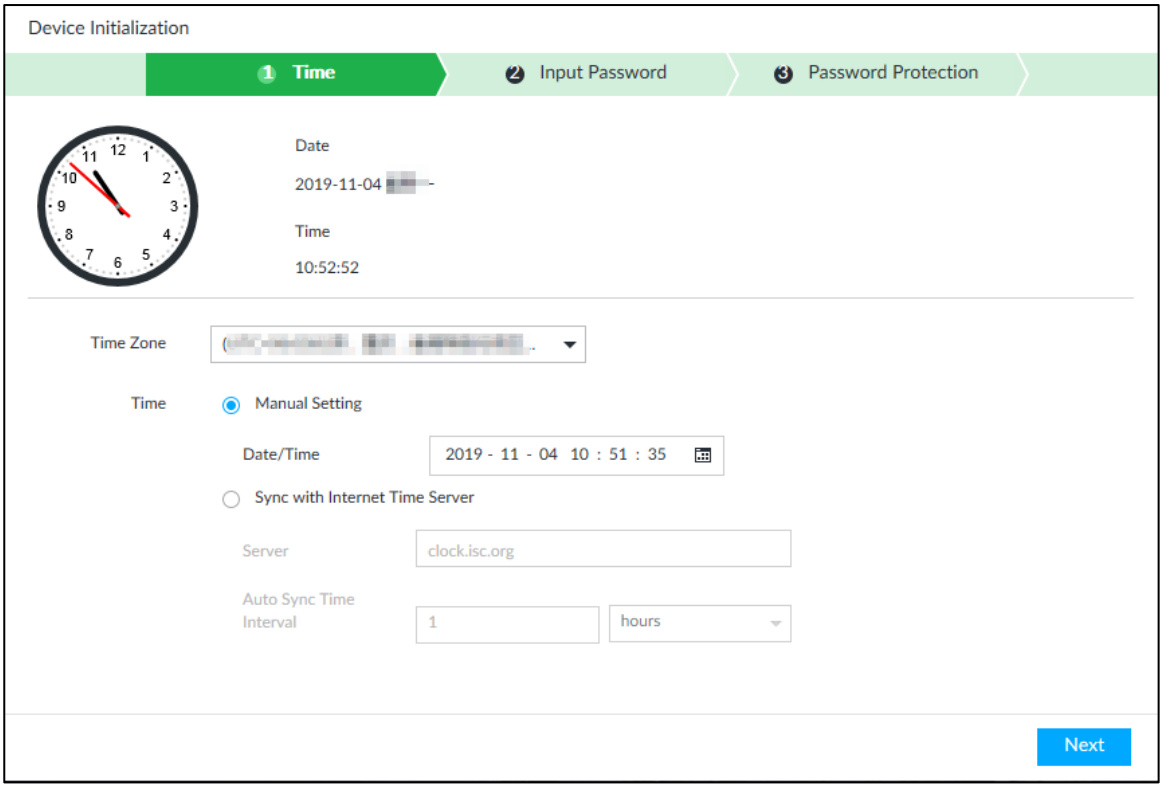
Step 1 Open the browser, enter IP address, and then press Enter.

Default IP address of network port 1 to network port 4 are 192.168.1.108 to 192.168.4.108. Enter the corresponding IP address of the actually connected network port.

Step 2 On the **Language Set** interface, select a country or region, a language, and a language standard. Click **Next**. The language setting step is only available on the local interface of the Device.

The **Time** interface is displayed. See Figure 3-1.

Figure 3-1 Time setting



Step 3 On the **Time** interface, set time parameters. For details, see Table 3-1.

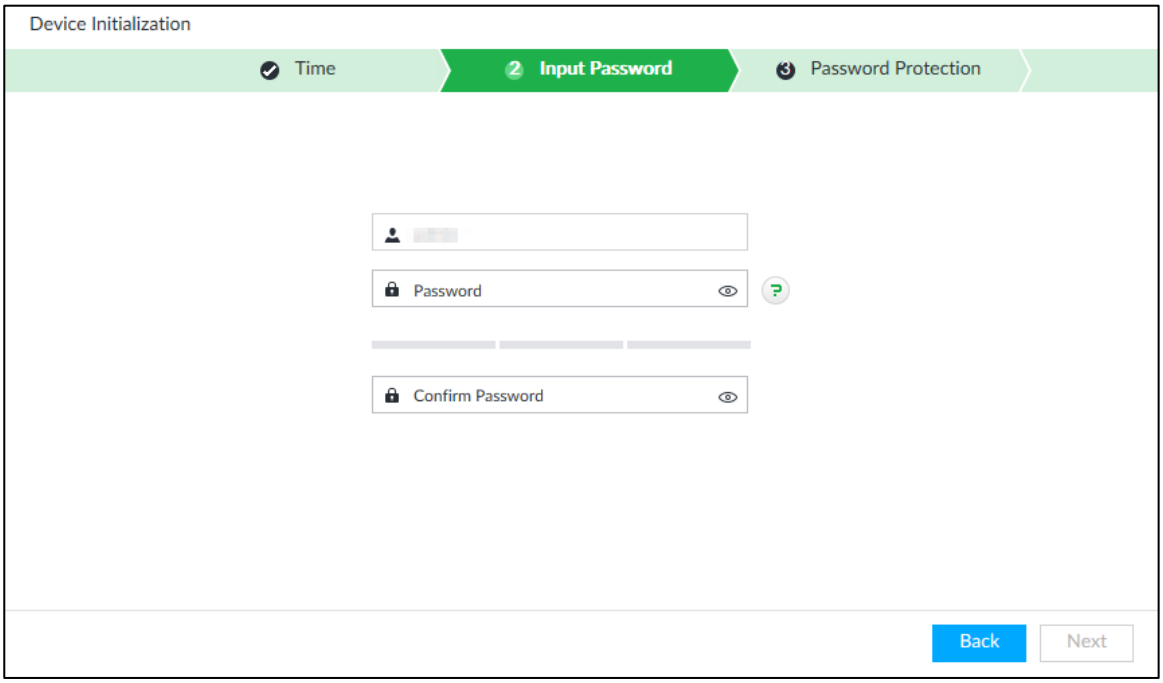
Table 3-1 Time parameters description

Parameters	Description
Time Zone	The time zone of the Device.
Time	Set system date and time manually or by synchronizing with NTP server time. ● Manual setting: Select date and time from the calendar. ● Sync with Internet Time Server: Select **Sync with Internet Time Server**, enter NTP server IP address or domain, and then set the automatic synchronization interval. Device time will synchronize with the server time after **Sync with Internet Time Server** is set.

Step 4 Click **Next**.

The **Input Password** interface is displayed. See Figure 3-2.

Figure 3-2 Set password



Step 5 Set admin login password. See Table 3-2.

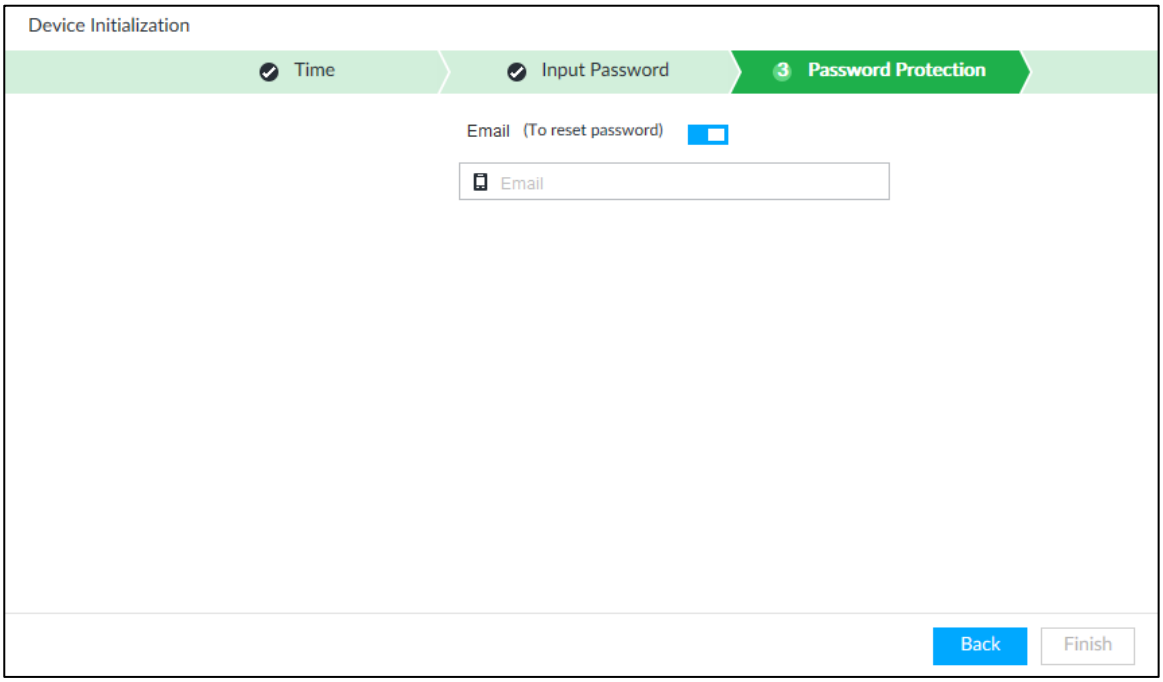
Table 3-2 Description of password parameters

Parameters	Description
Username	The default user name is admin.
Password	Set admin login password, and confirm the password. The password should consist of 8 to 32 non-blank characters and contain at least two types of characters among uppercase, lowercase, number, and special character (excluding ' " ; : &). Enter a strong password according to the password strength indication.
Confirm Password	

Step 6 Click **Next**.

The **Password Protection** interface is displayed. See Figure 3-3.

Figure 3-3 Password protection



Step 7 Set password protection information.

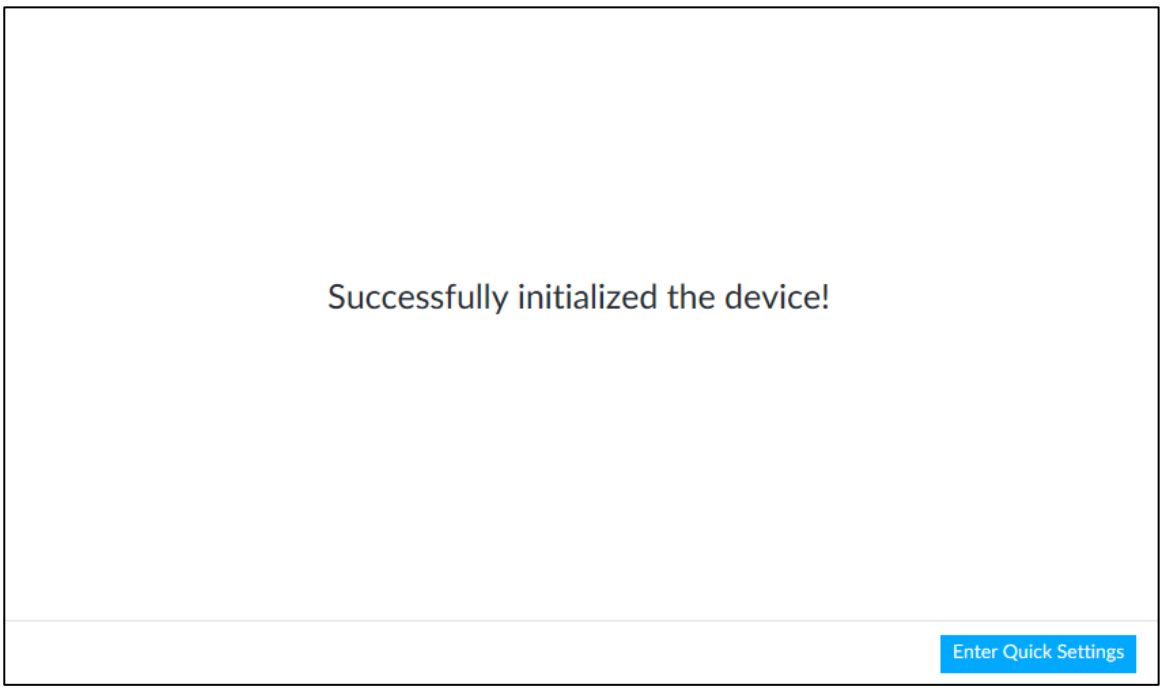
You can use the email you set here to reset admin password. See "6.7.3.2 Resetting Password" for detailed information.

1) Click  to enable email.
2) Enter an email address in the **Email** box.

Step 8 Click **Finish** to complete device initialization.

The device initialization success interface is displayed. See Figure 3-4. Click **Enter quick settings** button to go to the quick setting interface, and then set device basic information. See "3.2 Quick Settings" for details.

Figure 3-4 Initialization completed



3.2 Quick Settings

After initializing the device, the system goes to quick settings interface. You can quickly configure system time, and network settings.

Device has 5 Ethernet ports by default. Make sure that at least one Ethernet port has connected to the network before you set IP address.

Step 1 On the completion interface of initialization, click **Enter Quick Setting**.

Step 2 Enable virtual IP.

1) Click  to enable virtual IP.

2) Configure virtual IP address, subnet mask and gateway.

Virtual IP: Provides a static device IP address for user to access the device however the main controller and the standby controller switch.

- Make sure that the virtual IP is in the same network segment with the default NIC IP.
- Virtual IP is bound to the NIC that corresponds to the default route.

Step 3 Configure IP address.

1) Click  of the corresponding NIC.

2) Set parameters.

Table 3-3 TCP/IP parameters description

Parameters	Description
Speed	Current NIC max network transmission speed.
IP Type	Select IPv4 or IPv6.
Use dynamic IP address	When there is a DHCP server on the network, check **Use Dynamic IP Address**, system can allocate a dynamic IP address to the device. There is no need to set IP address manually.
Use static IP address	Check **Use Static IP Address**, and then set static IP address, subnet mask and gateway to set a static IP address for the device.
MTU	Set NIC MTU value. The default setup is 1500 Byte. We recommend you to check the MTU value of the gateway first and then set the device MTU value equal to or smaller than the gateway value. Reduce the packets slightly and enhance network transmission efficiency. Changing MTU value might result in NIC reboot, network offline and affect current running operation. Please be careful!

3) Click **OK**.

Device goes back to **IP Set** interface.

Step 4 Set DNS server information.

You can select to get DNS server manually or enter DNS server information.

This step is compulsive if you want to use domain service.

1) Select an IP type for DNS server. You can select IPv4 or IPv6.
2) Select the way of setting DNS IP address.
   ◇ Select **Obtain DNS server address automatically**, and then the Device can automatically get the DNS server IP address on the network.
   ◇ Select **Use the following DNS server address**, and then enter the preferred DNS IP address and the alternate DNS IP address.

Step 5 Set default NIC.

Select default NIC from the drop-down list.

Make sure that the default NIC is online.

Step 6 Click **Next** to save settings.

3.3 Login

You can access and manage the device remotely by using the PCAPP (PC client), or the web interface.

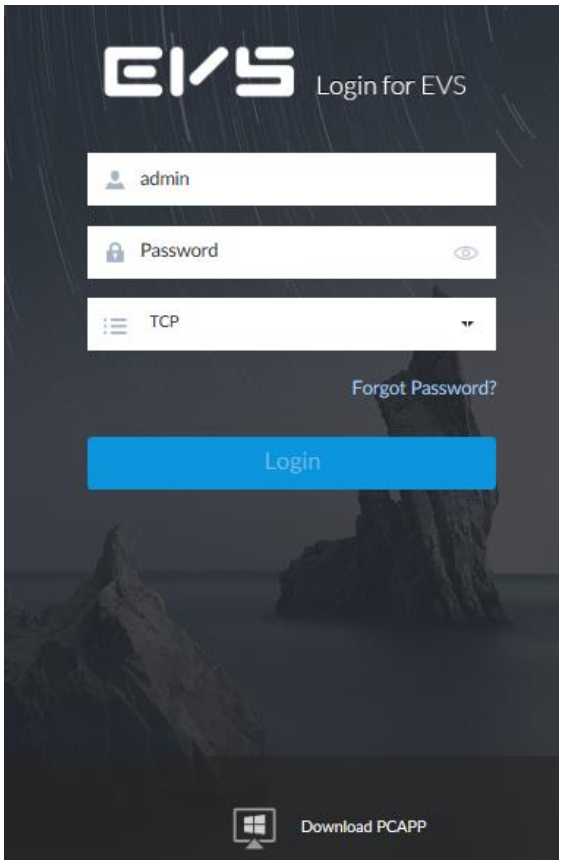
3.3.1 Logging in to PCAPP Client

Log in to the PCAPP for system configuration and operation.

Step 1 Download PCAPP.

1) Open the browser, enter IP address, and press Enter.
   The web login interface is displayed. See Figure 3-5.

Figure 3-5 Web login interface

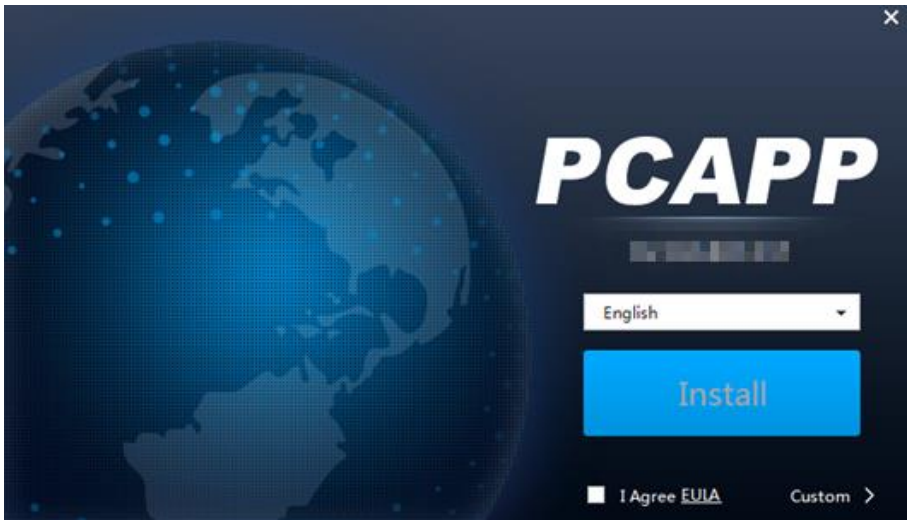


2) Click **Download PCAPP** to download PCAPP installation package.

Step 2 Install PCAPP.

1) Double-click the PCAPP installation package.
   The installation interface is displayed. See Figure 3-6.

Figure 3-6 Installation interface



2) Select a language of the PCAPP.
3) Click **EULA**, read through the content, and then select the check box of **I Agree EULA**.
4) (Optional) Select installation path and create shortcut or not.
   Click **Custom**. The installation path is displayed. See Figure 3-7. Select a path.

Figure 3-7 Custom installation

5) Click **Install**.
   On completion, the completion interface is displayed. See Figure 3-8.

Figure 3-8 The installation is completed

Step 3 Log in to PCAPP.

1) There are two ways to enter PCAPP.

- On the installation completion interface, click **Run**.
- Double-click the shortcut icon on the PC desktop.

The initial interface is displayed. See Figure 3-10.

- When PC theme is not Aero, the system will remind you to switch the theme. See Figure 3-9. To ensure video smoothness, switch your PC to Areo theme. For details, see "9.4 Configuring PCAPP."
- System display PCAPP at full-screen by default. Click to display the task column. See Figure 3-10.

Figure 3-9 Prompt

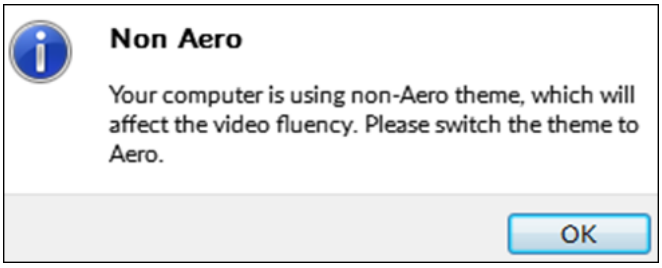
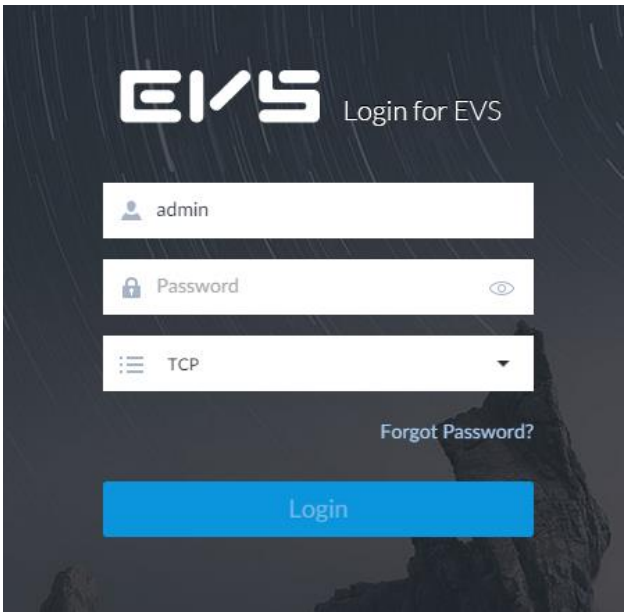


Figure 3-10 Initial interface

2) Enter device IP address, and then press **Enter** or click .

The login interface is displayed. See Figure 3-11.

Figure 3-11 Login



3) Enter device user name and password.

- Click **Login**. For your device safety, change the admin password regularly and keep it well.
- In case you forgot password, click **Forgot password** to reset. See "6.7.3.2 Resetting Password" for detailed information.

4) Select the login type among TCP, UDP and Multicast. Keep it TCP if you have no special requirement for TCP or UDP.

5) Click **Login**.

Figure 3-12 Maintenance interface

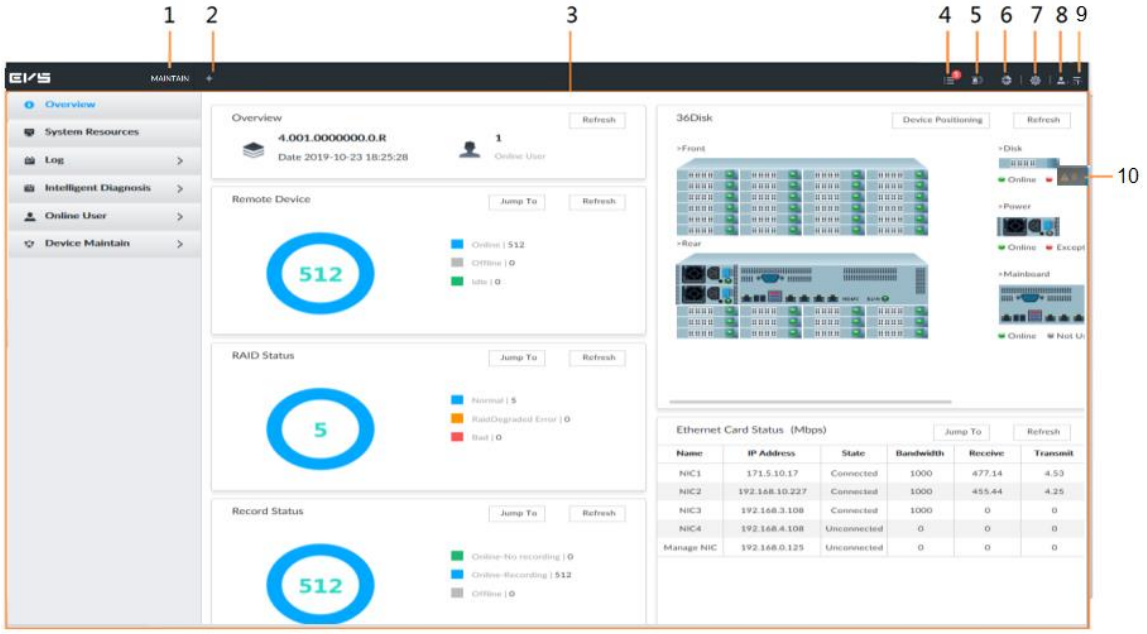


Table 3-4 Main interface description

No.	Name	Description
1	Task column	Displays enabled application icon. Move the mouse to the app and then click  to close the app. The live function is enabled by default and cannot be closed.
2	Add icon	Click to display or hide the app interface. Open the app interface to view or enable app.
3	Operation interface	Displays currently enabled app operation interface.
4	System Info	Click to view system information. See "5.4 System Info" for detailed information.
5	Buzzer	Click the icon to view buzzer messages. For details, see "5.6 Buzzer."
6	Background Task	Click to view the background running task information. See "5.5 Background Task" for detailed information.
7	System config	Click to enter system configuration mode. See "6 System Configuration" for detailed information.
8	Login user	Click it to change user password, lock user, logout user, reboot device or close device.
9	Quick settings	Click this icon and select **Video** or **IP SAN** to go to the **STORAGE** or **IP SAN** interface.
10	Alarm list	Click to view the unprocessed alarm event quantity. See "5.3 Alarm List" for detailed information. Drag this icon to move its position.

3.3.2 Logging in to Web Interface

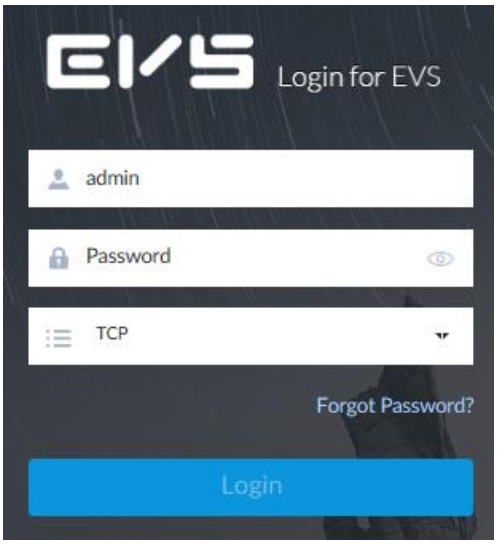
System supports general browser such as Google Chrome, Firefox to access the web to manage the device remotely, operate and maintain the system.

When you are using general browser to access the web, system supports setting function only. It cannot display the view. It is suggested that PCAPP should be used.

Step 1 Open the browser, enter IP address, and then press Enter.

The web login interface is displayed. See Figure 3-13.

Figure 3-13 Web login interface



Step 2 Enter user name and password.

- Click Login. For your device safety, change the admin password regularly and keep it well.
- In case you forgot password, click Forgot password to reset. See "6.7.3.2 Resetting Password" for detailed information.

Step 3 Select the login type among TCP, UDP and Multicast. Keep it TCP if you have no special requirement for TCP or UDP.

Step 4 Click **Login**.

System displays **LIVE** interface.

3.4 Configuring Remote Device

Register remote device to the system. Here you can view the live video from the remote device, change remote device settings, and so on.

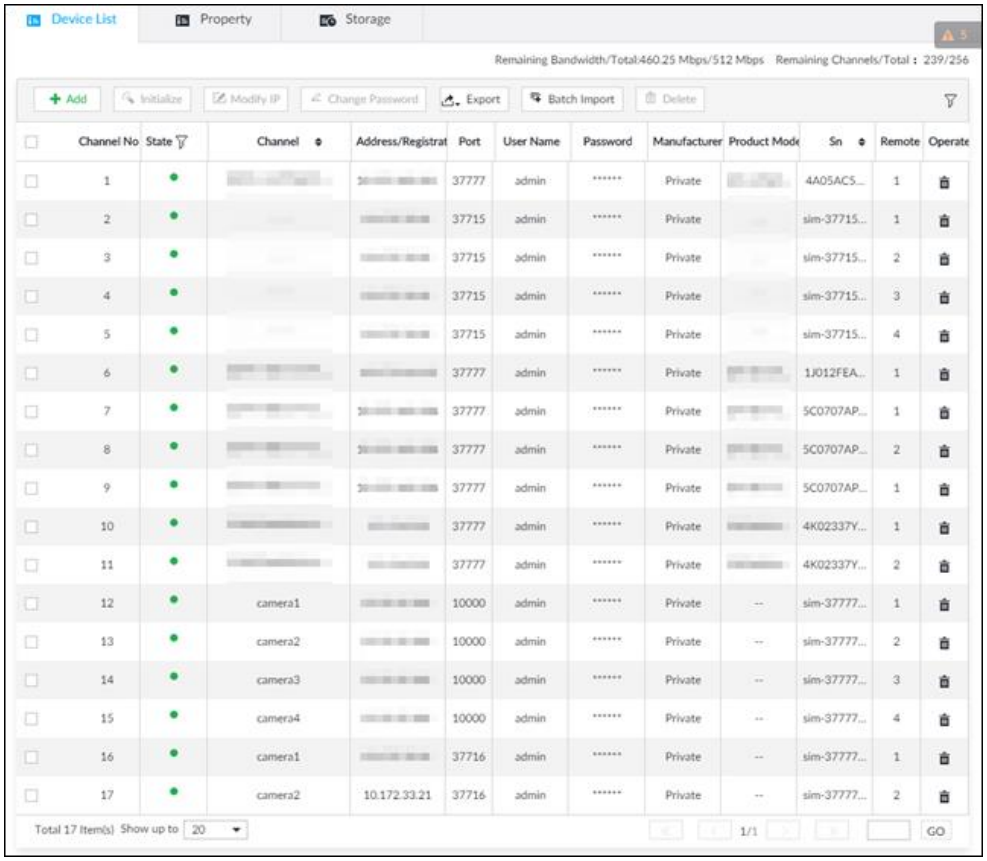
3.4.1 Initializing Remote Device

After you initialize the remote device, you can change remote device login password and IP address. Remote devices can be connected to the Device only after being initialized.

Step 1 Click , or click on the configuration interface, and then select **DEVICE**.

The **DEVICE** interface is displayed. See Figure 3-14.

Figure 3-14 Device management



Step 2 On the **Device List** interface, click **Add**.

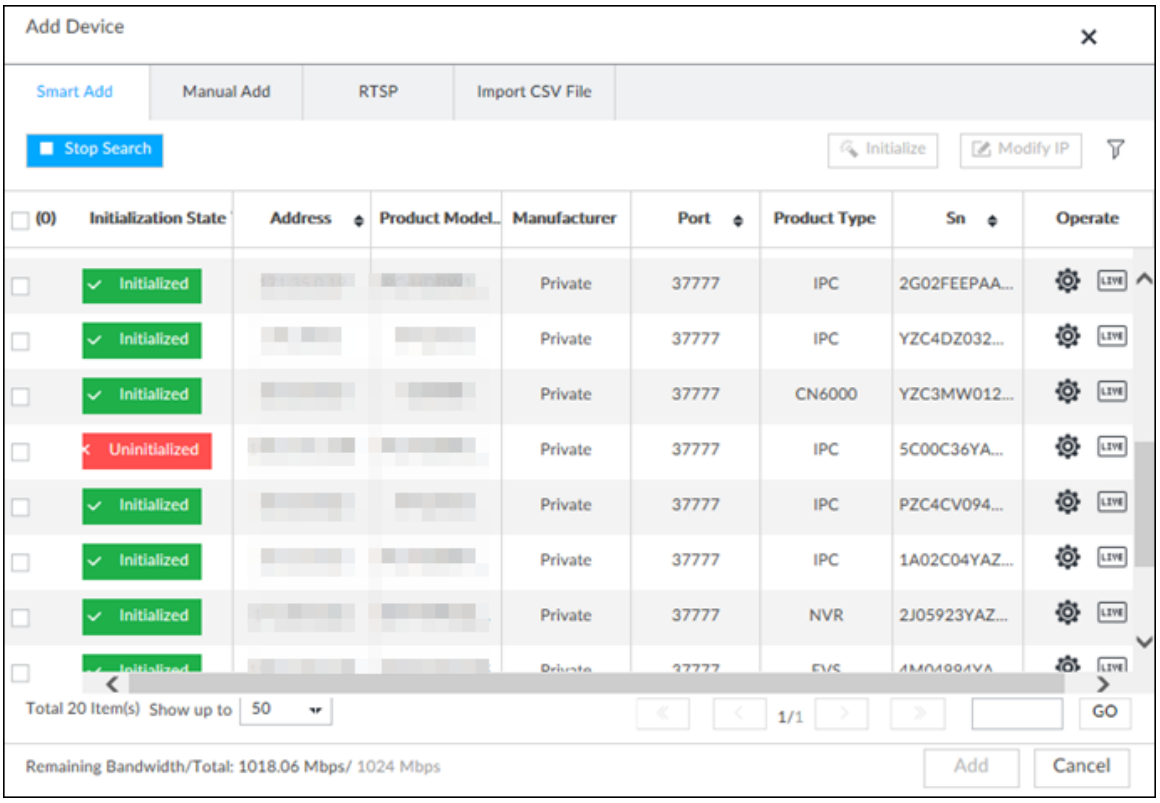
The **Add Device** interface is displayed.

Step 3 On the **Smart Add** interface, click **Smart Search**.

The search results are displayed. See Figure 3-15.

To set search conditions, you can click .

Figure 3-15 Remote device



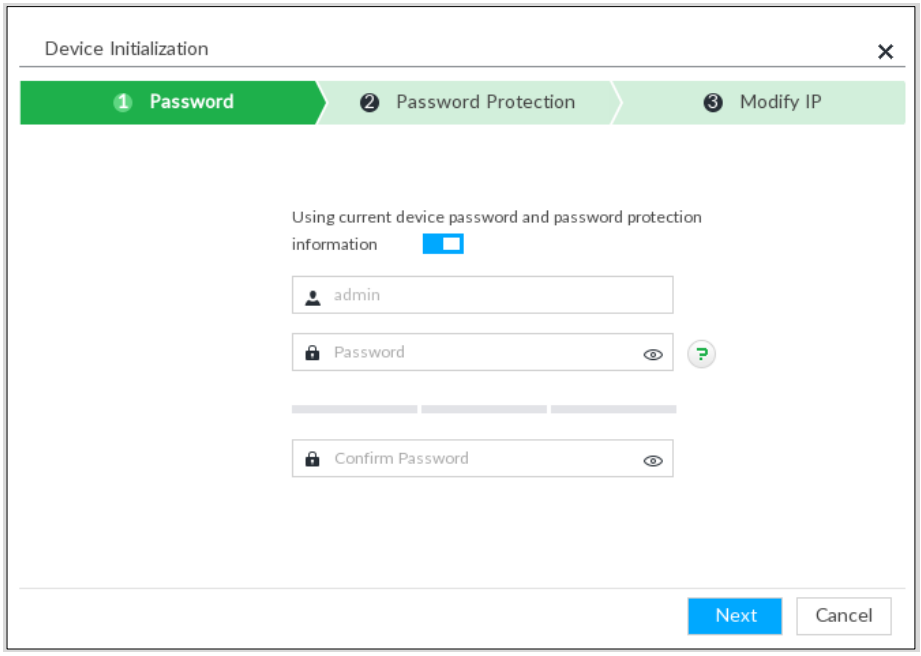
Step 4 Select the uninitialized remote device and then click **Initialize** button.

The **Device Initialization** interface is displayed. See Figure 3-16.

TIPS

Click **Initialization status** and then select **Uninitialized**, you can quickly filter the uninitialized remote device.

Figure 3-16 Initializing the device



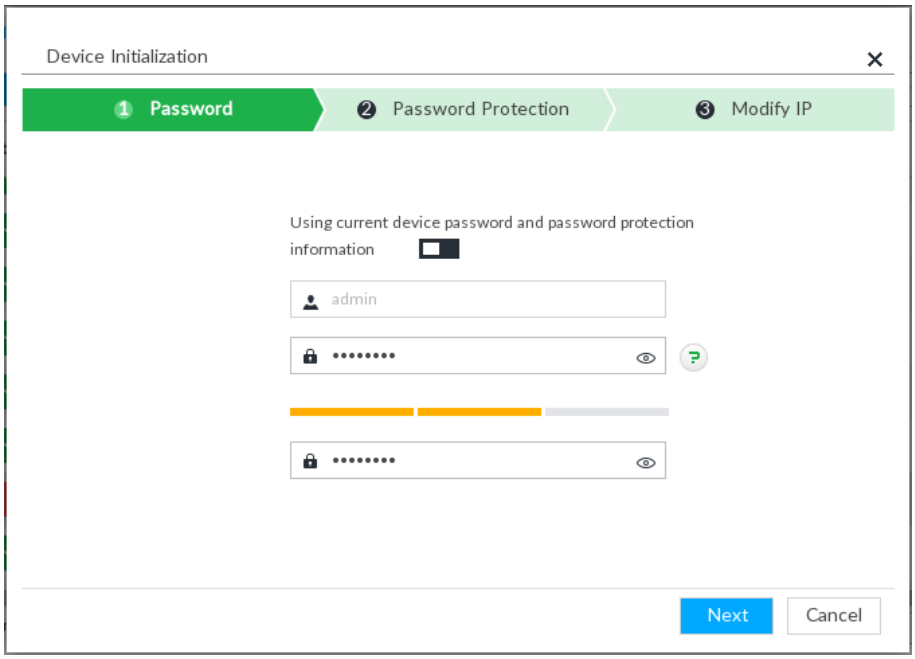
Step 5 Set remote device password and password protection.

Using current device password and password protection information is enabled by default. Keep it enabled so as to automatically use current device admin password

and email information without manual configuration. Go to Step 6 if you keep it enabled.

1) To manually configure password, click  to disable Using current device password and password protection information.
The password setting interface is displayed. See Figure 3-17.

Figure 3-17 Password setting



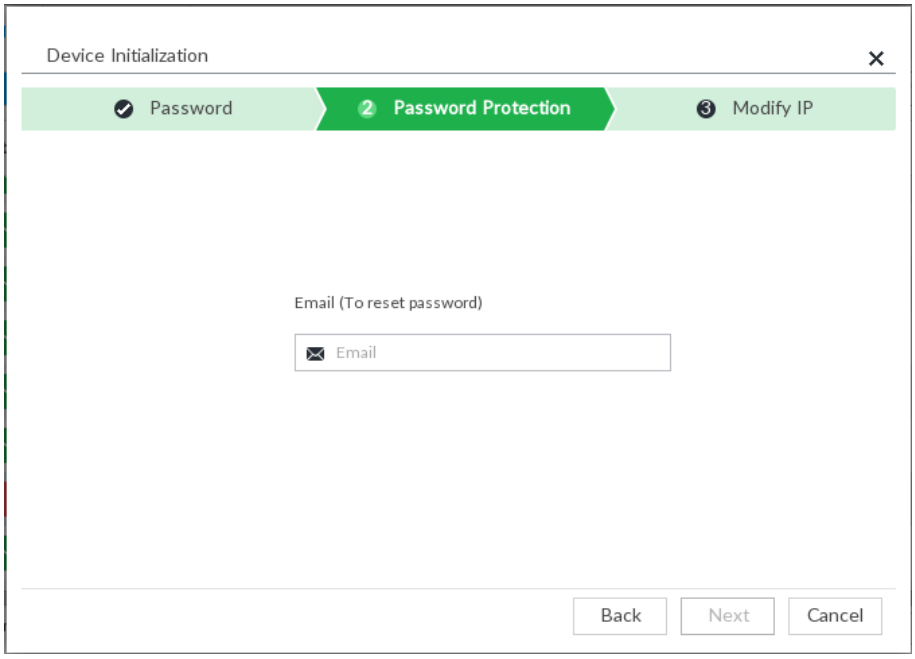
2) Set parameters. For details, see Table 3-5.

Table 3-5 Description of password parameters

Parameters	Description
Username	The default user name is admin.
Password	In the **New Password** box, enter the new password and enter it again in the Confirm Password box. The password should consist of 8 to 32 non-blank characters and contain at least two types of characters among uppercase, lowercase, number, and special character (excluding ' " ; : &). Enter a strong password according to the password strength indication.
Confirm Password	

3) Click **Next**.
The password setting interface is displayed. See Figure 3-18.

Figure 3-18 Password protection



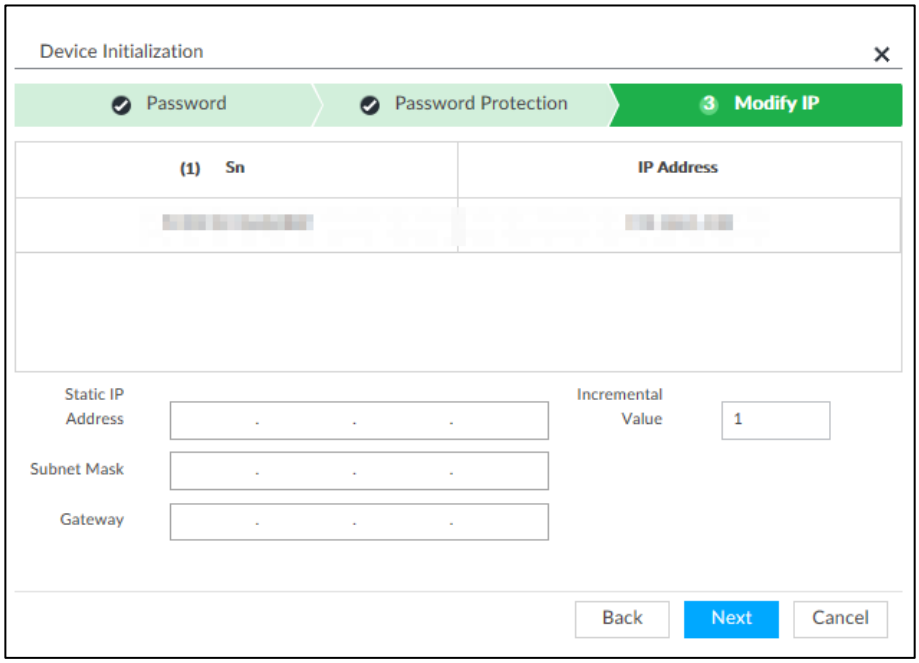
4) Set an email address.

Enter an email address. You can use the email address here to reset password in case you forgot password in the future.

Step 6 Click **Next**.

The **Modify IP** interface is displayed. See Figure 3-19.

Figure 3-19 Modify IP



Step 7 Set camera IP address.

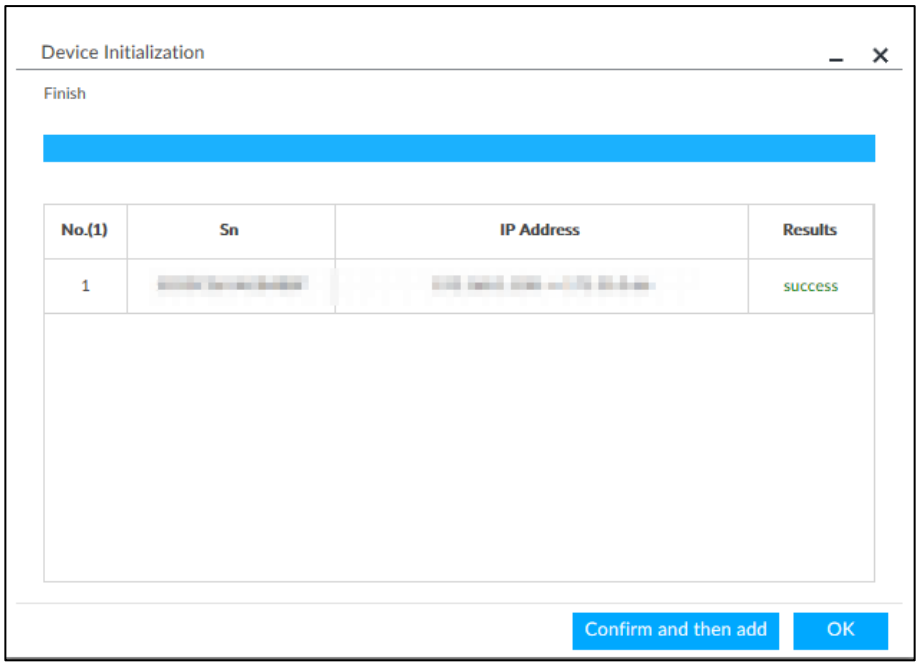
- When there is DHCP server in the network, select DHCP, and the remote device gets dynamic IP address automatically. It is unnecessary to enter IP address, subnet mask and gateway.
- Select **Static**, and then enter static IP address, subnet mask, default gateway and incremental value.

- After you enter incremental value, system can add the fourth address of the IP address one by one to automatically allocate the IP addresses.
- If you want to change several devices IP addresses at the same time, system allocates IP address of the same network segment.
- If there is IP conflict when changing static IP address, device pops up IP conflict dialogue box. If batch change IP address, device automatically skips the conflicted IP and begins the allocation according to the incremental value.

Step 8 Click **Next**.

System begins initializing remote device. See Figure 3-20.

Figure 3-20 Initialize



Step 9 Click **Confirm and Add**, or click **OK**.

- Click **Confirm and Add**: System completes initializing the remote device and then adds the remote device to the list. System goes back to **Add device** interface.
- Click **OK**: System completes initializing remote device. System goes back to **Add device** interface.

3.4.2 Adding Remote Device

Device supports smart add, manual add and template add. For details, see Table 3-6.

Table 3-6 Add mode

Add Mode	Description
Smart Add	Search the remote devices on the same network and then filter to register. For details, see "3.4.2.1 Smart Add." It is useful if you do not know the exact IP address.
Manual Add	Enter the IP address, user name and password of remote device. For details, see "3.4.2.2 Manual Add." For some remote devices, you can enter IP address, user name, and password to register. It is called manual add.

Add Mode	Description
RTSP	Add remote devices through RTSP. For details, see "3.4.2.3 RTSP." To add stream media devices, you are recommended to choose RTSP.
Batch add (by CSV template)	Fill in information about remote device in the template, import the template to add the device. For details, see "3.4.2.4 Batch Add." For batch adding, when IP address, user name and other information of remote device is inconsistent, it is suggested to use this mode.

3.4.2.1 Smart Add

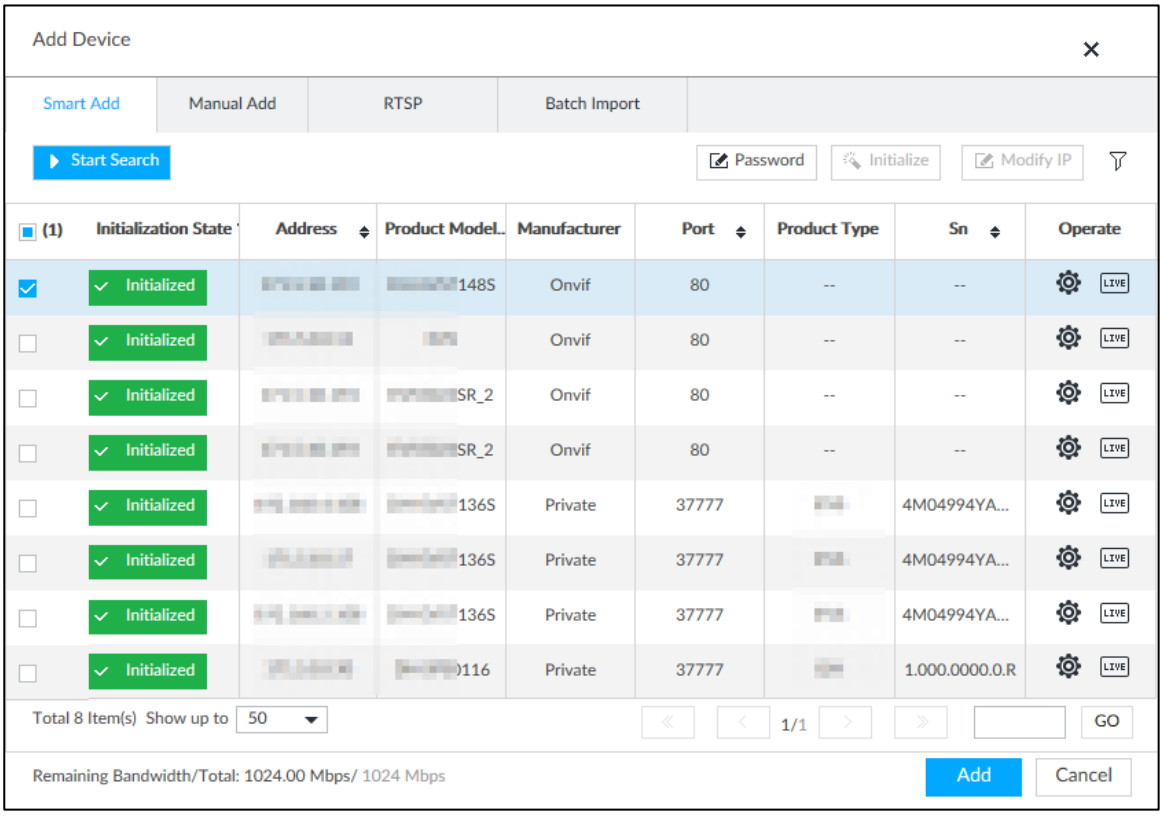
Step 1 Click , and then select **DEVICE**.

The **DEVICE** interface is displayed.

Step 2 Click or **Add**, and then select **Smart Add**.

The **Smart Add** interface is displayed. See Figure 3-21.

Figure 3-21 Smart add



Step 3 Click Start Search.

The search results of online devices are displayed. See Figure 3-22. For details, see Table 3-7.

To set search conditions, you can click .

Figure 3-22 Search results

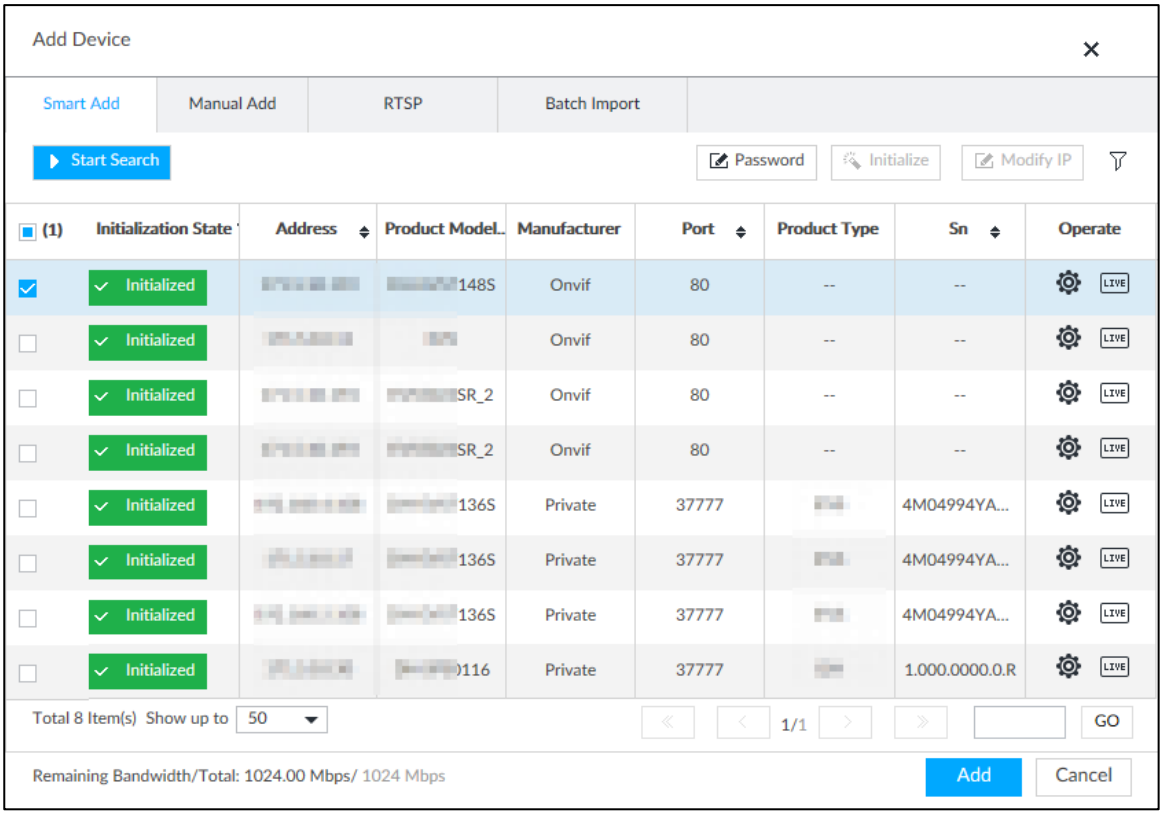
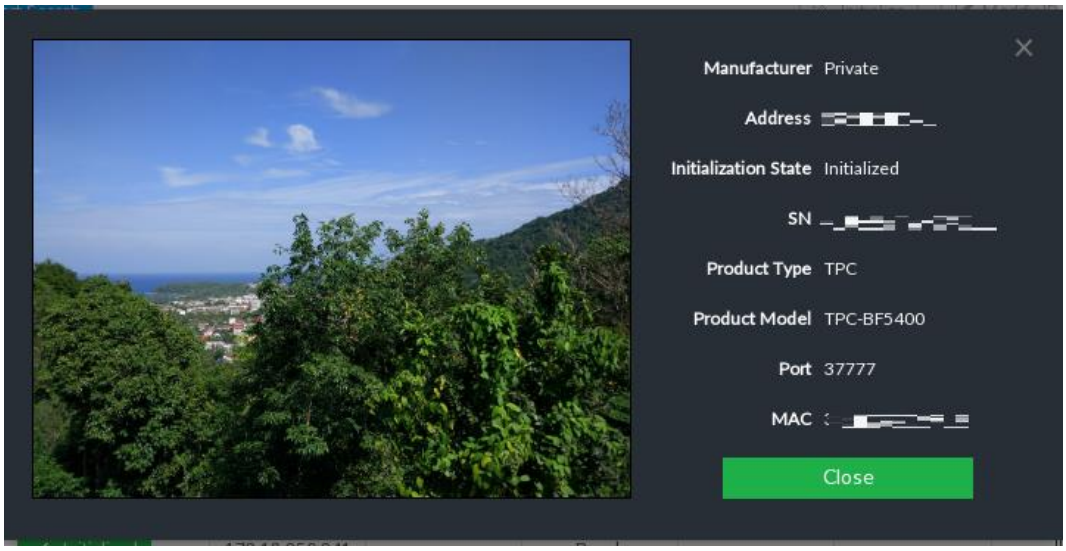


Table 3-7 Result description

Parameters	Description
Start Search	Click **Start Search** to **Start Search**ing remote device. Now it becomes **Stop Search** button. Click **Stop Search** button to stop searching remote device.
Password	Enter the username and password of the selected device for adding it.
Initialize	Select uninitialized remote device and then click **Initialize** button to initialize remote device. See "3.4.1 Initializing Remote Device" for detailed information.
Modify IP	See "6.2.2.2 Changing IP Address" to change the registered device IP address.
Initialization State	Displays remote device initialization status. Click ▼ to filter initialized or uninitialized remote device.
Operation	Click LIVE to display real-time video from the remote device. See Figure 3-22. Click ✕ or **Close** to close the real-time preview window. You can view the live video if admin password of the remote device is admin, or remote device admin password is the same as the system.
Bandwidth	Displays bandwidth remaining and the total bandwodth.

Figure 3-23 Live view



Step 4 Add a remote device.

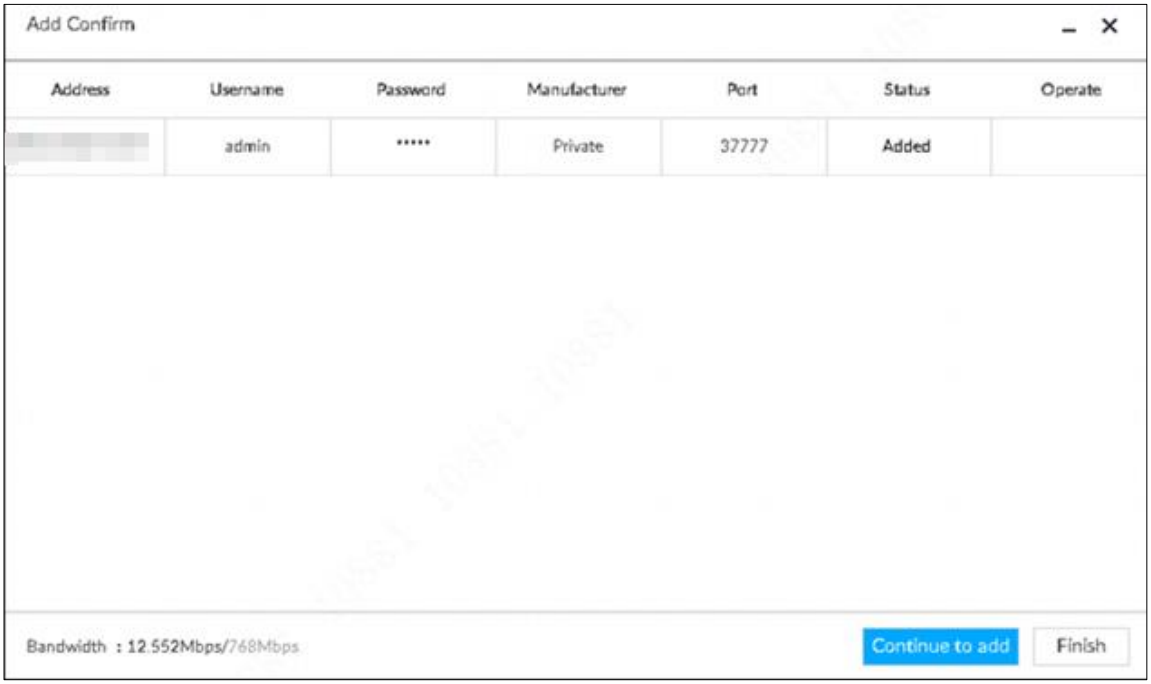
Select a remote device, click **Password**, and then enter the username and password of the selected device. Click **OK**.

- If you do not enter device username and password, the system will try to add the device by using the username and password of the current EVS.
- During the adding process, click **Cancel** button, you can cancel adding process. Click **Stop** button of the corresponding remote device to cancel add.

Step 5 Click **Add**. The confirmation interface is displayed. See Figure 3-24.

- Double-click remote device IP address, user name, password, manufacturer, port to change corresponding information.
- If system fails to add the remote device, see the reason on the **Status** column to change the remote device information and then click **Retry** to try to add again.
- If a remote device is exception due to network disconnection other reasons, it can also be added. It comes online after the exception is resolved.

Figure 3-24 Confirm



Step 6 Click Continue to add or Finish.

- Click **Continue to add**, device goes back to **Smart add** interface to add more remote device.
- Click **Finish** to complete adding remote device process. Device displays **Device** interface to view the newly added remote device information.

3.4.2.2 Manual Add

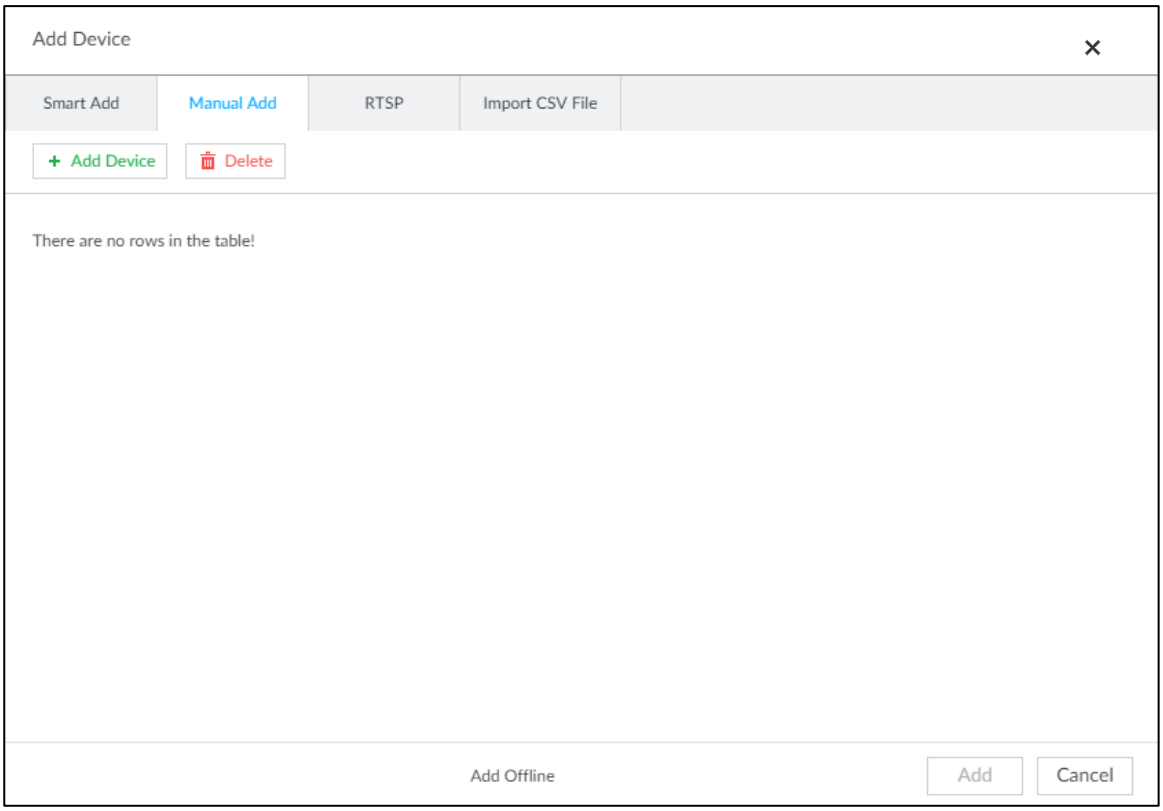
Step 1 Click , and then select **DEVICE**.

The **DEVICE** interface is displayed.

Step 2 Click and then select **Manual add**.

The **Manual Add** interface is displayed. See Figure 3-25.

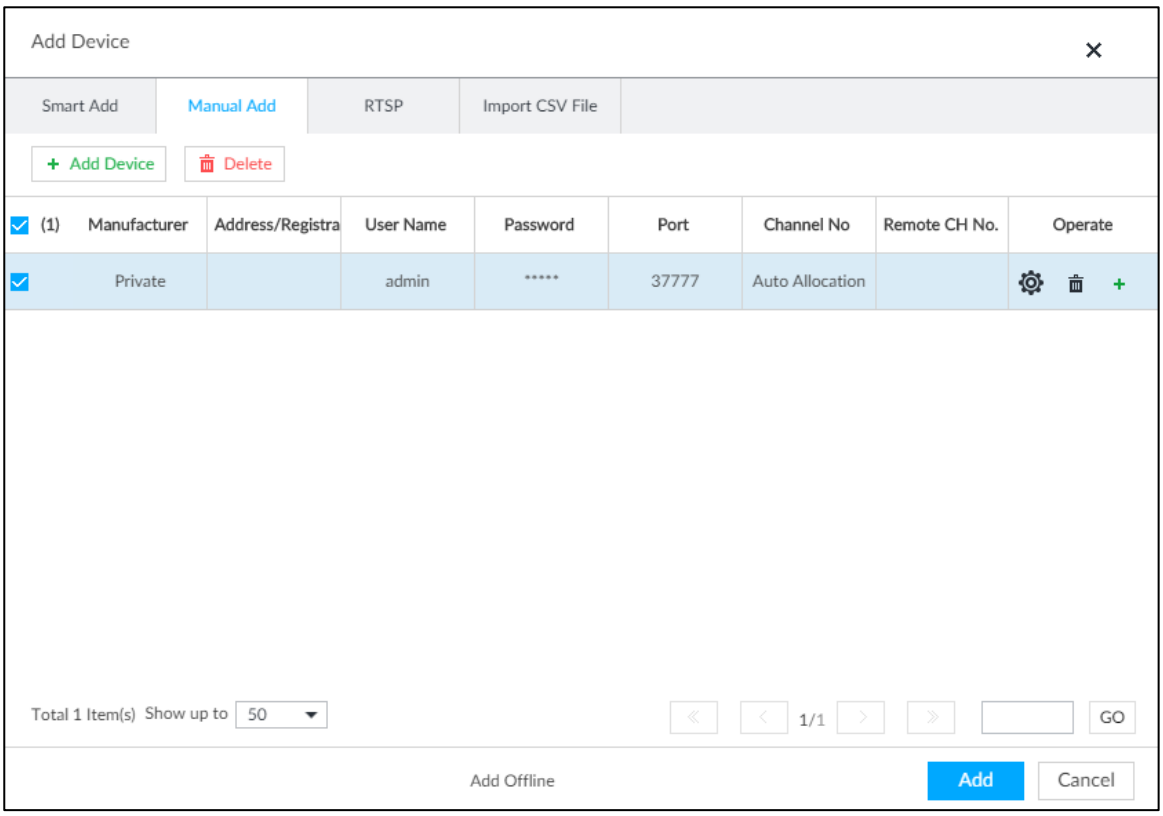
Figure 3-25 Manual add



Step 3 Click Add Device.

The **Add Device** interface is displayed. See Figure 3-26.

Figure 3-26 Add device

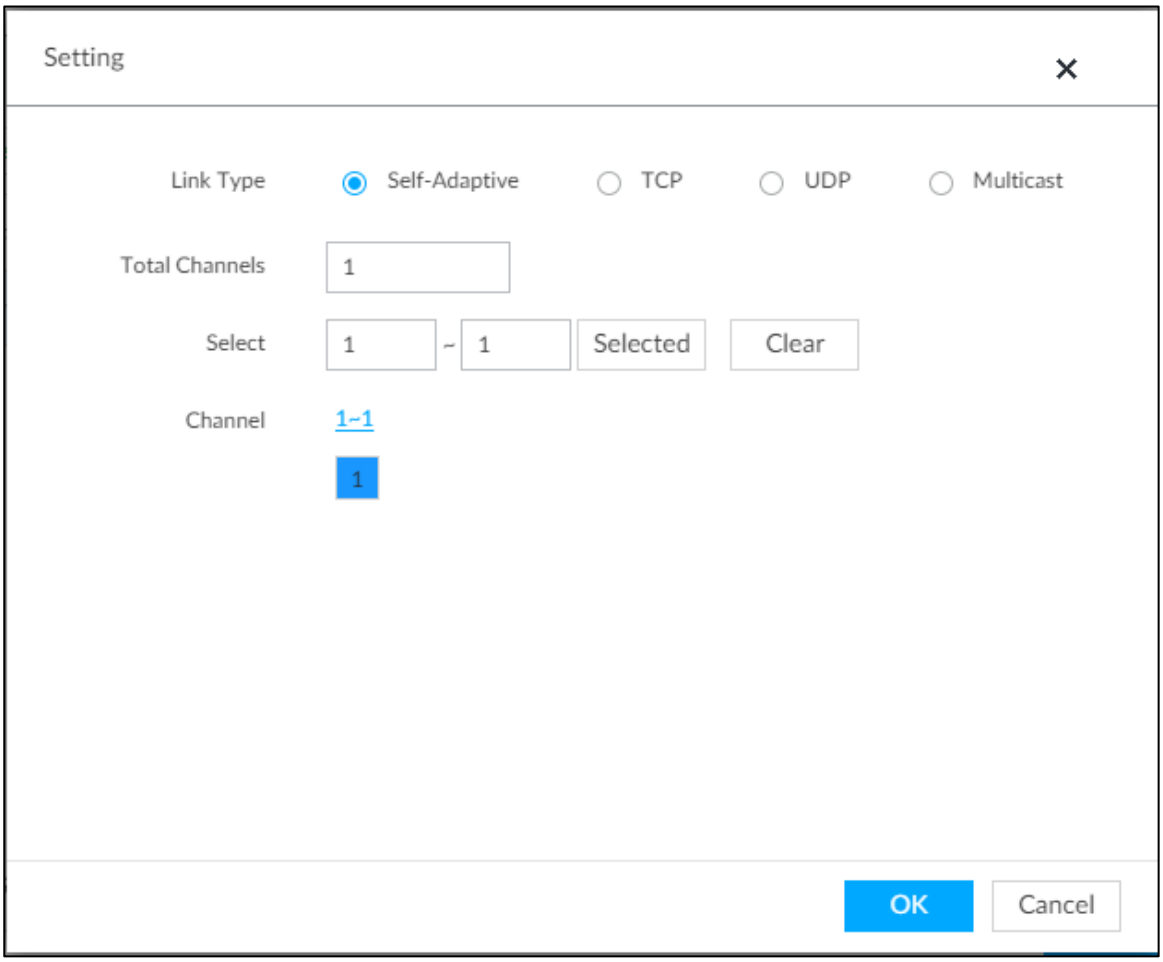


Step 4 Set parameters. For details, see Table 3-8.

Table 3-8 Parameters

Parameters	Description
Manufacturer	Displays the connection protocol of the remote device. Default protocol of the system is **Private**. Double-click **Private** to select other protocols. To add stream media device, select Rtsp protocol, and enter RTSP address of stream media device in Address column. See Figure 3-27. Rtsp://<user name>:<password>@<IP address>:<port>/cam/realmonitor?channel=1&subtype=0U. ● Port: Enter port number. The default setting is 554. ● Channel: Enter channel number of the stream media device to be added. ● Subtype: Set record bit stream type. It includes main stream 0 and sub stream 1. For example rtsp://admin:admin@192.168.20.25:554/cam/realmonitor?channel=1&subtype=0. To add a stream media device, it is unnecessary to set user name, password, and port.
Address/Registration ID	Double-click the empty cell in the **Address/Registration** IP column to enter the IP address or RTSP address of remote device.
Username Password	Double-click the empty cells in the **User Name** and **Password** columns to enter the username and password of remote device.
Port	Displays the default port number of remote device. If the port number has been modified, double-click the port cell to enter the current port number of the remote device.
Channel No.	Double-click this column to select the channel number of the device in EVS. If you select **Auto Allocation**, EVS will provide a channel number automatically.
Remote CH No.	Select the channel number of a remote device. 1. Click in the **Operate** column, the **Setting** interface is displayed. See Figure 3-27. 2. Select a link type. 3. Enter the total number of channels. Click **Selected**, and then the corresponding channel is displayed. 4. Click **OK**.
Others	Delete current line or add a new line. ● Click to delete current line information. Select multiple lines of remote device information, and then click **Delete** to batch delete the selected information. ● Click to add a new line. Enter remote device information to add several devices at the same time.

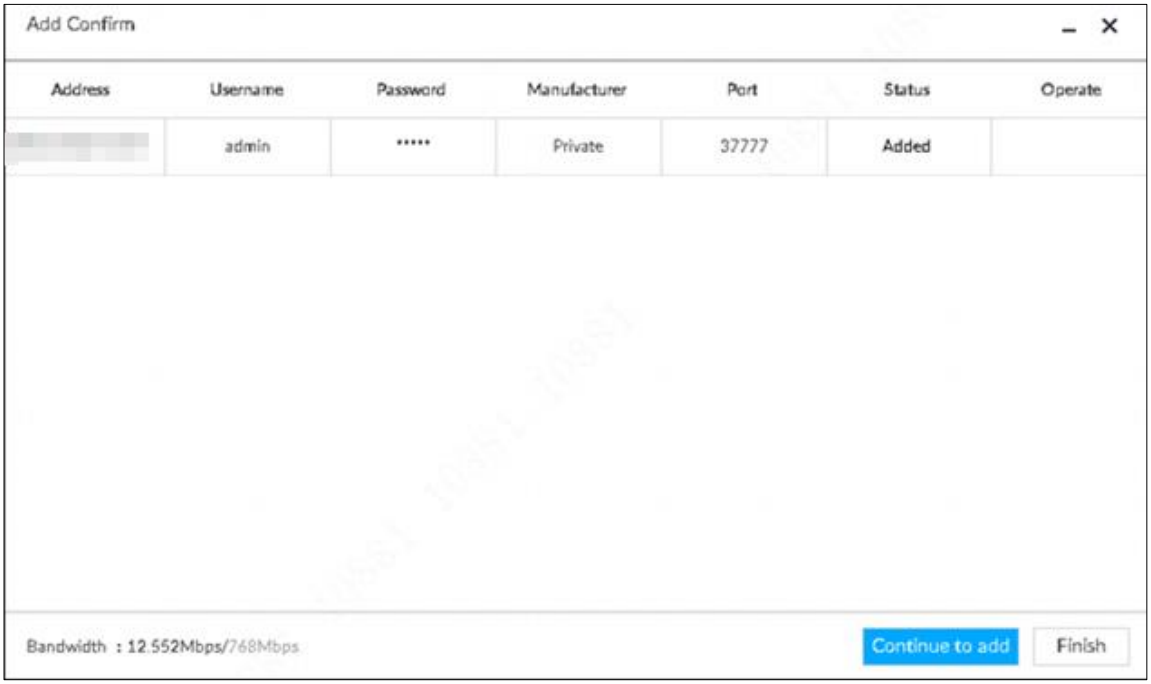
Figure 3-27 Setting



Step 5 Select the remote device and then click **Add**. Device begins adding remote device and pops up the confirmation interface. See Figure 3-28.

- During the adding process, click **Cancel** button, you can cancel adding process. Click **Stop** button of the corresponding remote device to cancel.
- Double-click remote device IP address, user name, password, manufacturer, port to change corresponding information.
- If system fails to add the remote device, see the reason on the **Status** column to change the remote device information and then click **Retry** to try to add again. See Figure 3-28.
- If a remote device is exception due to network disconnection other reasons, it can also be added. It comes online after the exception is resolved.

Figure 3-28 Confirm



Step 6 Click Continue to add or Finish.

- Click **Continue to add**, device goes back to **Smart add** interface to add more remote device.
- Click **Finish** to complete adding remote device process. Device displays **Device** interface to view the newly added remote device information.

3.4.2.3 RTSP

Step 1 Click , and then select **DEVICE**.

The **DEVICE** interface is displayed.

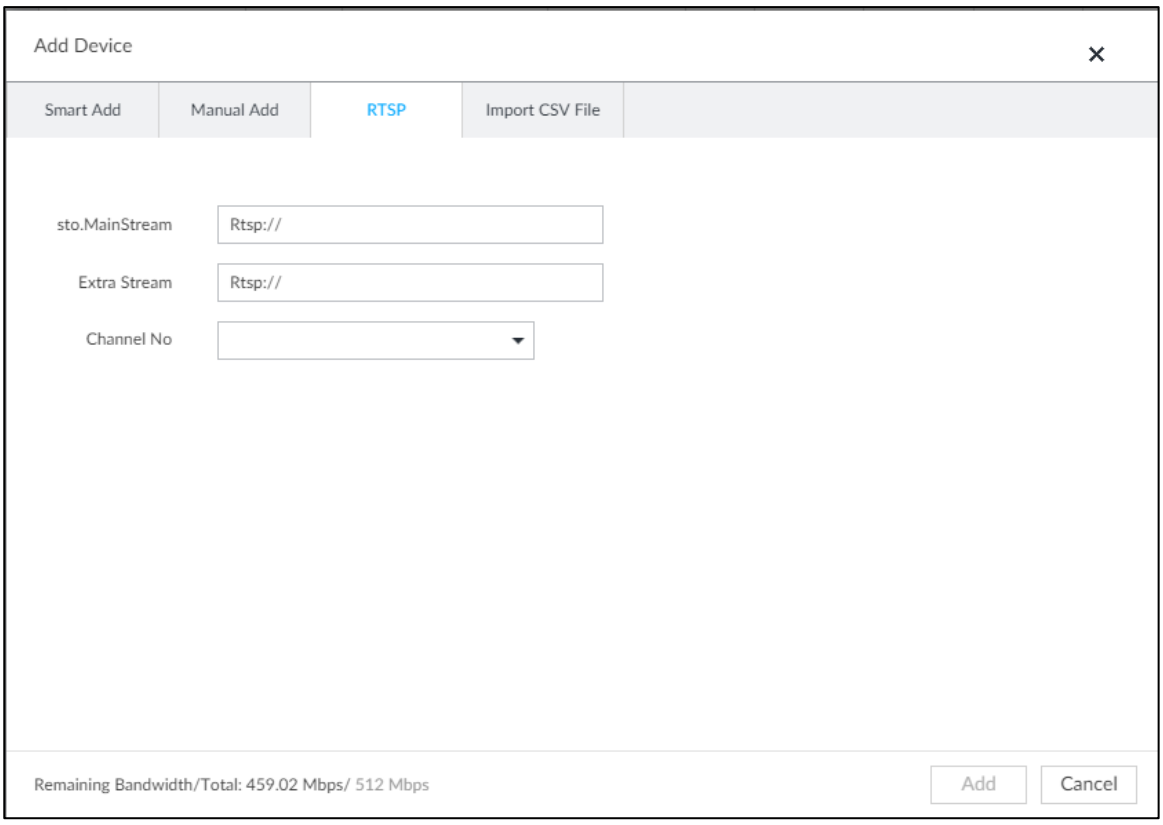
Step 2 In the **Device List** interface, click **Add**.

The **Add Device** interface is displayed.

Step 3 Click **RTSP**.

The **RTSP** interface is displayed. See Figure 3-29.

Figure 3-29 RTSP



Step 4 Enter RTSP address as required.

RTSP address format is rtsp://<*username*>:<*password*>@<*IP address* >:<*port*>/cam/realmonitor?channel=1&subtype=0.

- Port: 554 by default.
- Channel: The channel number of the stream media device to be added.
- Subtype: Stream type. 0 for main stream, and 1 for sub stream.

Step 5 Select a channel No.

Step 6 Click **Add**.

3.4.2.4 Batch Add

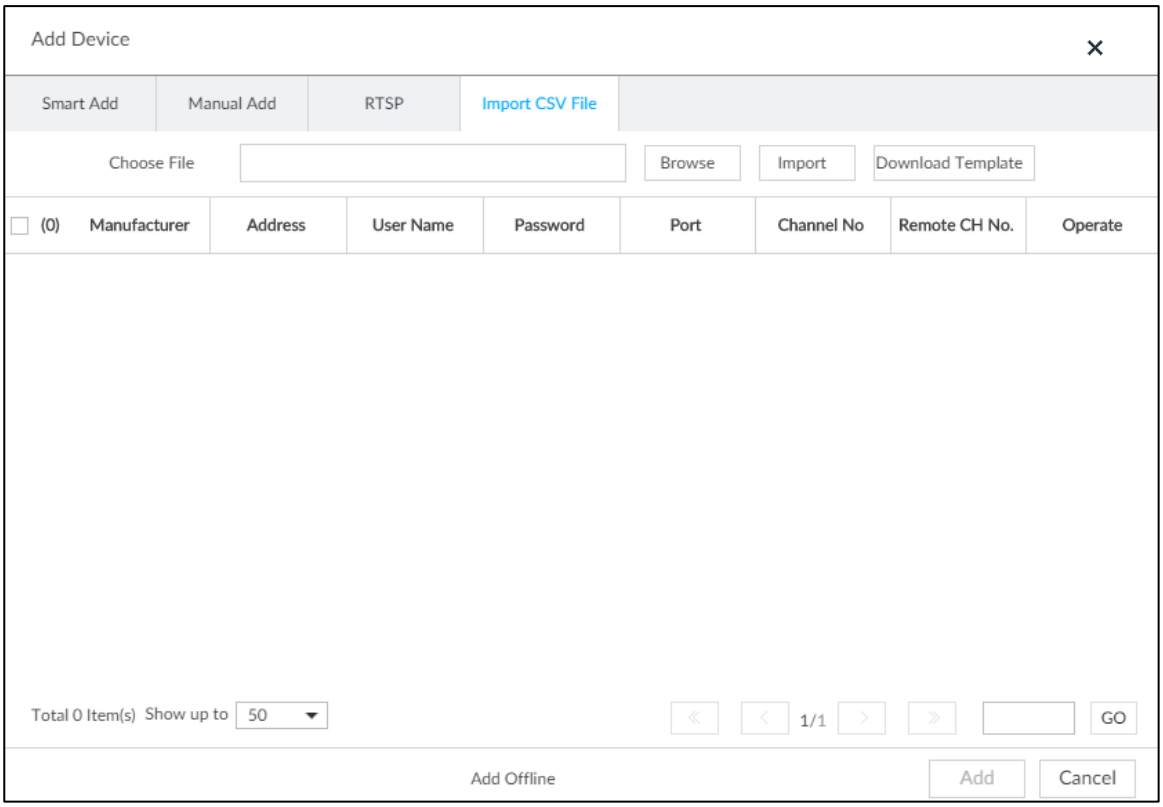
Step 1 Click , and then select **DEVICE**.

The **DEVICE** interface is displayed.

Step 2 Click , and then select **Import CSV file** tab.

The **Import CSV file** interface is displayed. See Figure 3-30.

Figure 3-30 Import CSV file



Step 3 Fill in template file.

1) Click **Download Template** to download template file.

File path might vary depending on interface operations, and the actual interface shall prevail.

- At PCAPP, click , select Download content to view file saving path. For details, see "9.3 Viewing Downloads."
- Select file saving path during local operation.

Connect USB device to the system if you are on the local menu to operate.

- During web operations, files are saved under default downloading path of the browser.

2) Fill in template file and save according to your actual situation.

The following information of template file shall be filled in. See Figure 3-31.

If information about remote device is not filled in completely, improve it after importing template.

Figure 3-31 File

	A	B	C	D	E	F	G
1	IP Address	Port	Channel No.	Channel Name	Manufacturer	User Name	Password
2							
3							

Step 4 Import template file.

1) Click **Browse** to select the upgrade file.
2) Click **Import**.

The imported information about remote device is displayed.

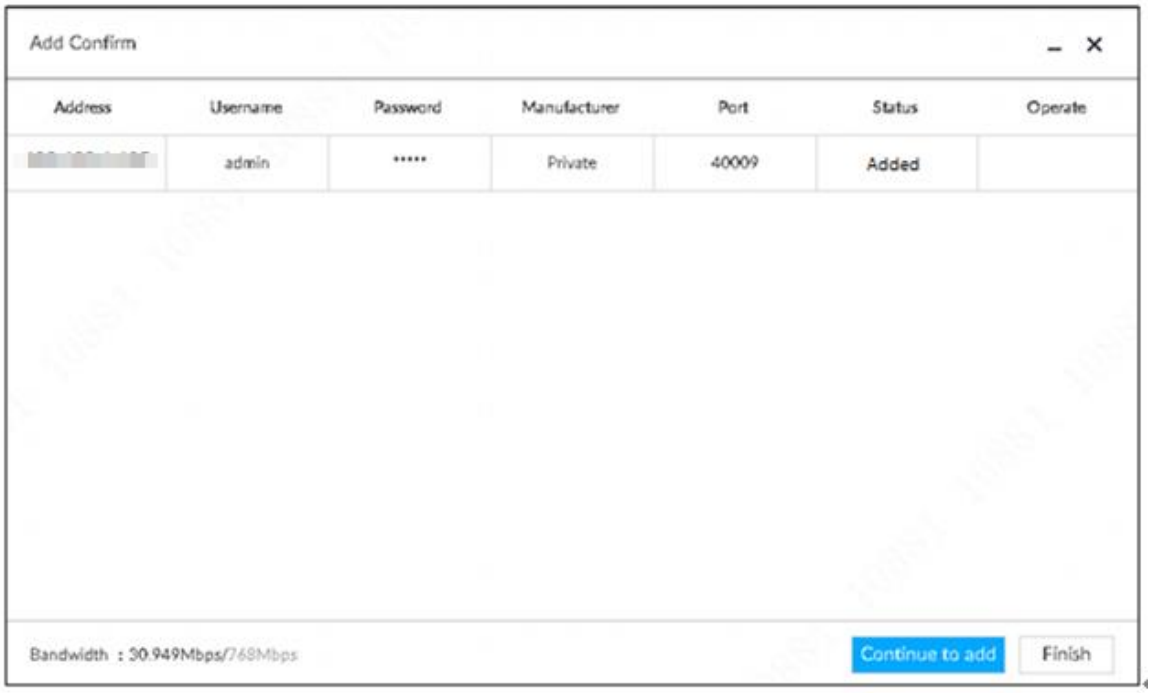
- When information about remote device is incomplete, complement it according to your actual situation.
- Click to delete current line information.

Step 5 Add remote devices.

Select the remote device and then click **Add**. Device begins adding remote device and pops up confirmation interface. See Figure 3-32.

- During the adding process, click **Cancel** button, you can cancel adding process. Click **Stop** button of the corresponding remote device to cancel add.
- Double-click remote device IP address, user name, password, manufacturer, port to change corresponding information.
- If system fails to add the remote device, see the reason on the **Status** column to change the remote device information and then click **Retry** to try to add again.

Figure 3-32 Confirm



Step 6 Click Continue to add or Finish.

- Click **Continue to add**, device goes back to **Smart add** interface to add more remote device.
- Click **Finish** to complete adding remote device process. Device displays **Device manager** interface to view the newly added remote device information.

Step 7 (Optional) You can add offline devices when the network is exception. When the network recovers, the added offline device will automatically come online.

Click next to offline device to add an offline device.

Step 8 (Optional) click next to **Overwrite** to enable the function. This function is used when the IP address of a new device is the same as that of a previously added device, the configuration of the new device will overwrite the old one.

4 AI Operations

In addition to the basic video monitoring functions, the Device can also provide a number of AI functions including face recognition, people counting, video metadata, vehicle recognition, and IVS (behavior detections such as fence-crossing, intrusion, loitering, crowd gathering, parking and more.).

This chapter introduces how to configure the AI functions respectively.

- The AI functions might vary depending on the device function capability. The actual interface shall prevail.
- Some AI features are conflicting. Do not enable conflicting AI features at the same time.

4.1 Overview

View the usage status of the AI functions of all remote devices.

Click  at the upper-right corner of the homepage to open the **Event** interface. The **Overview** interface is displayed by default, which shows the usage status of the AI functions of all remote devices.

indicates that the AI function is enabled.

4.2 Face Detection

System triggers alarms when human faces are detected within the detection zone.

4.2.1 Enabling AI Plan

You need to enable AI plan first.

- AI plan is available on select models.
- You need first enable the corresponding AI plan; otherwise the AI function does not work.
- The Device automatically shows the AI functions available on the connected cameras.

Step 1 Click  , or click  on the configuration interface, and then select **EVENT**.

The **EVENT** interface is displayed.

Step 2 Select a camera in the device tree on the left.

Step 3 Select **AI Plan > AI Plan > AI Plan**.

The **AI Plan** interface is displayed. See Figure 4-1.

- The interface might vary depending on the function capabilities of cameras. The actual interface shall prevail.

- If the camera is a PTZ camera, configure presets on the camera system first, and then you can set AI features for each preset of the PTZ camera. See Figure 4-2.

Figure 4-1 AI plan(1)

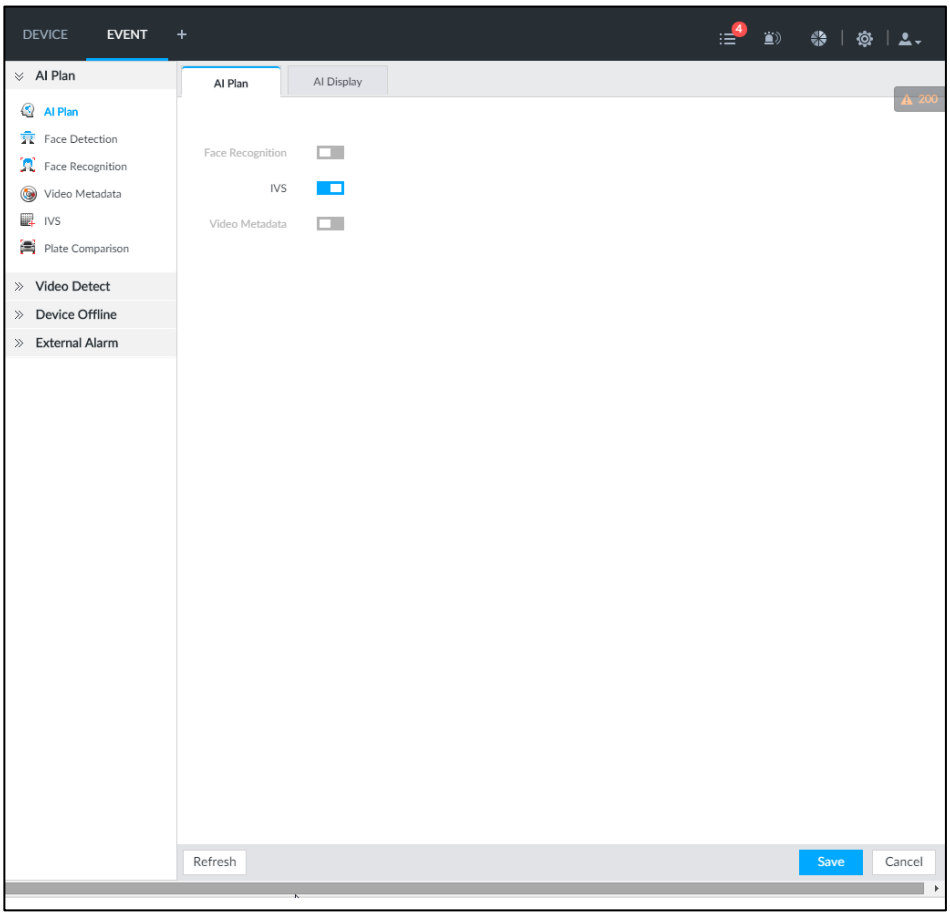
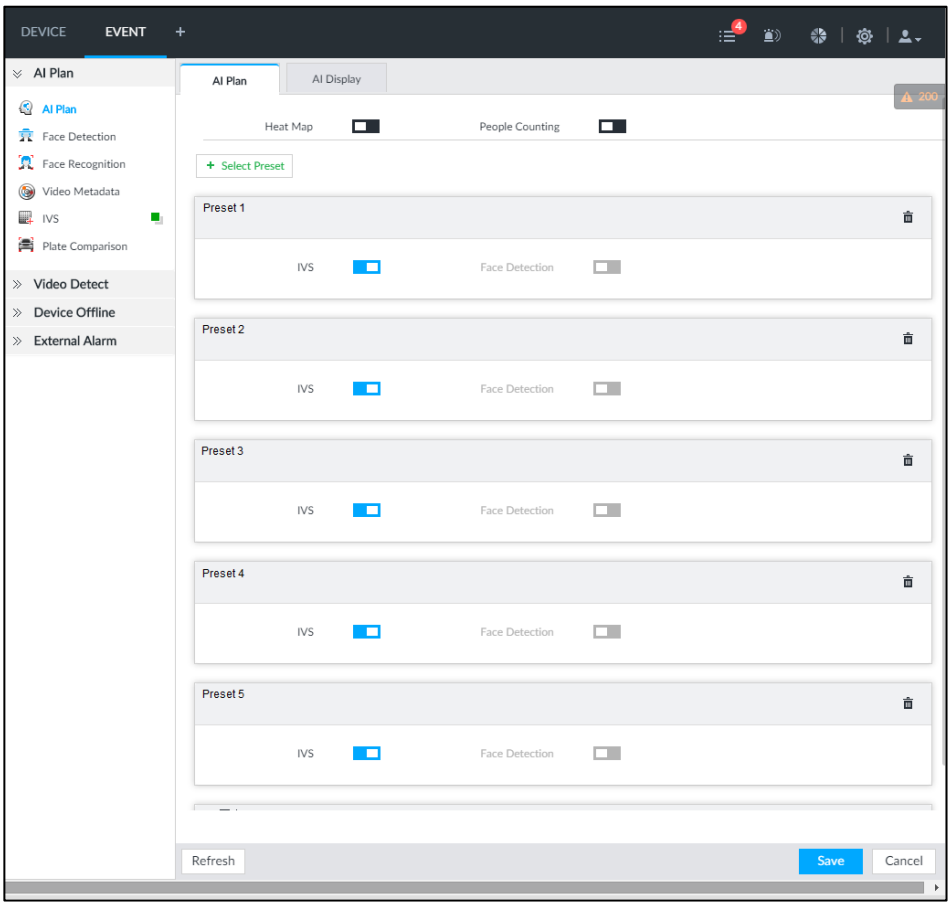


Figure 4-2 AI plan(2)



Step 4 Click  to enable AI detection plan. The icon becomes  .

When there is a conflict between the to-be-enabled AI plan and an enabled plan, disable the enabled plan first.

Step 5 Click **Save**.

4.2.2 Configuring Face Detection

Configure alarm rule of face detection.

Step 1 Click  or click  on the configuration interface, and then select **EVENT**.

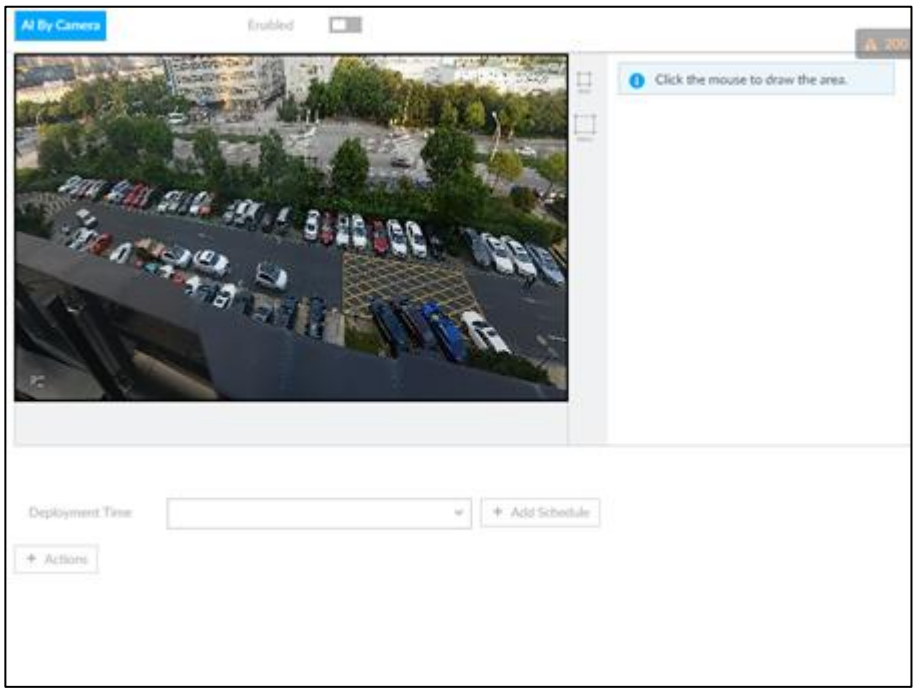
The **EVENT** interface is displayed.

Step 2 Select a remote device in the device tree on the left.

Step 3 Select **AI Plan > Face Detection**.

The **Face Detection** interface is displayed. See Figure 4-3.

Figure 4-3 Face detection

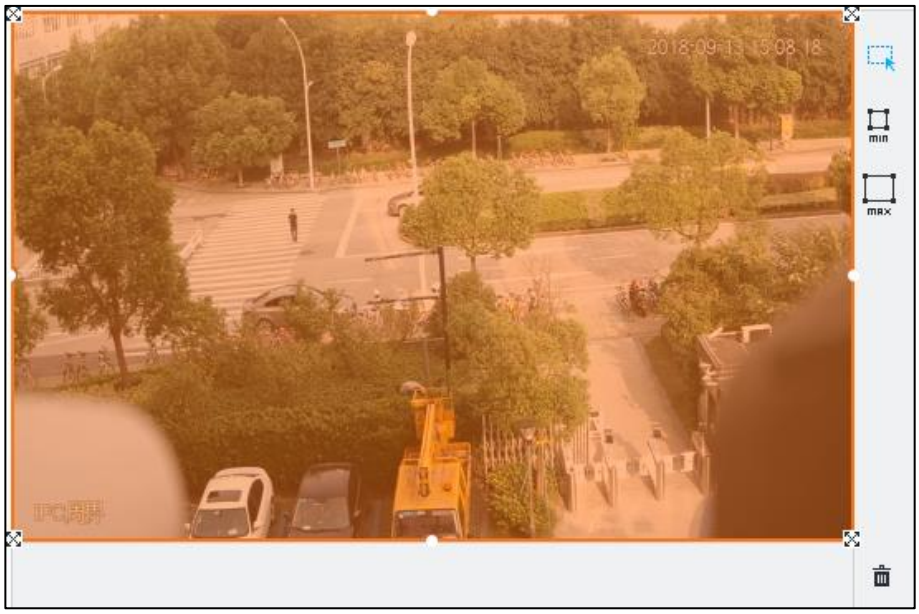


Step 4 Click  to enable face detection.

Support the **Face RoI** function. After enabling **Face RoI** function, system displays enhanced human face zone on the surveillance window.

Step 5 Set detection region on the video (yellow area). See Figure 4-4.

Figure 4-4 Area



- Click or white dot on detect region frame, and drag to adjust its size.
- Click min or max to set the minimum size or maximum size of the face detection area. System triggers an alarm once the size of detected target is between the maximum size and the minimum size.

Step 6 Click **Deployment Time** to select schedule from the drop-down list.

After setting arm period, system triggers corresponding operations when there is a motion detection alarm in the specified period.

You can select an existing schedule from the **Deployment Time** drop-down list. You can also add a new schedule. For details, see "6.8.3 Schedule."

Step 7 Click **Action** to set alarm action. See "6.4.1 Alarm Actions" for detailed information.

Step 8 Click **Save**.

4.2.3 Live View of Face Detection

You can view real-time face detection images and video.

4.2.3.1 Setting AI Display

You can configure display rule of face detection results.

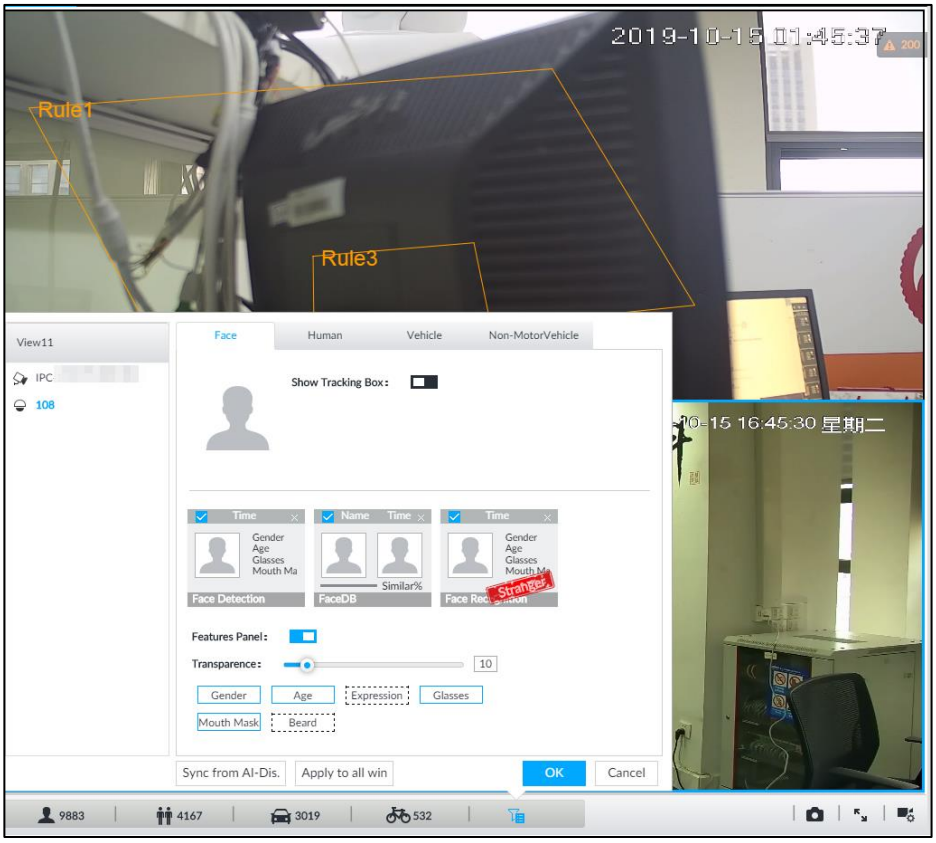
Before using this function, ensure that view has been created. See "5.1.1 View Management" for detailed information.

Step 1 On the **LIVE** interface, click  and select the **Face** tab.

The **Face** interface is displayed. See Figure 4-5.

- Click **Sync from AI-Dis.**, obtain global smart detection display rule of EVS. See "6.4.2.3.2 Setting AI Display" for detailed information.
- Click **Apply to all windows** to copy current configuration to other window(s).

Figure 4-5 Face



Step 2 Enable **Show Tracking Box** by clicking .

After it is enabled, when the system detects face or human, the window will display corresponding rule box.

Step 3 Enable **Features Panel**, and select feature(s) you want to display.

1) Click next to **Features Panel**, to enable the function. When the panel is enabled, the snapshots of detected faces are displayed on the live view.
2) Click to select **Face Detection** tab. indicates that the panel is selected.
3) (Optional) Drag to adjust features panel transparency. The higher the value, the more transparent the features panel.
4) (Optional) Select the features you need to display.
   - System supports displaying 4 feature types.
   - System has checked four features by default. To select other features, cancel the selected features, and then select the ones you need.

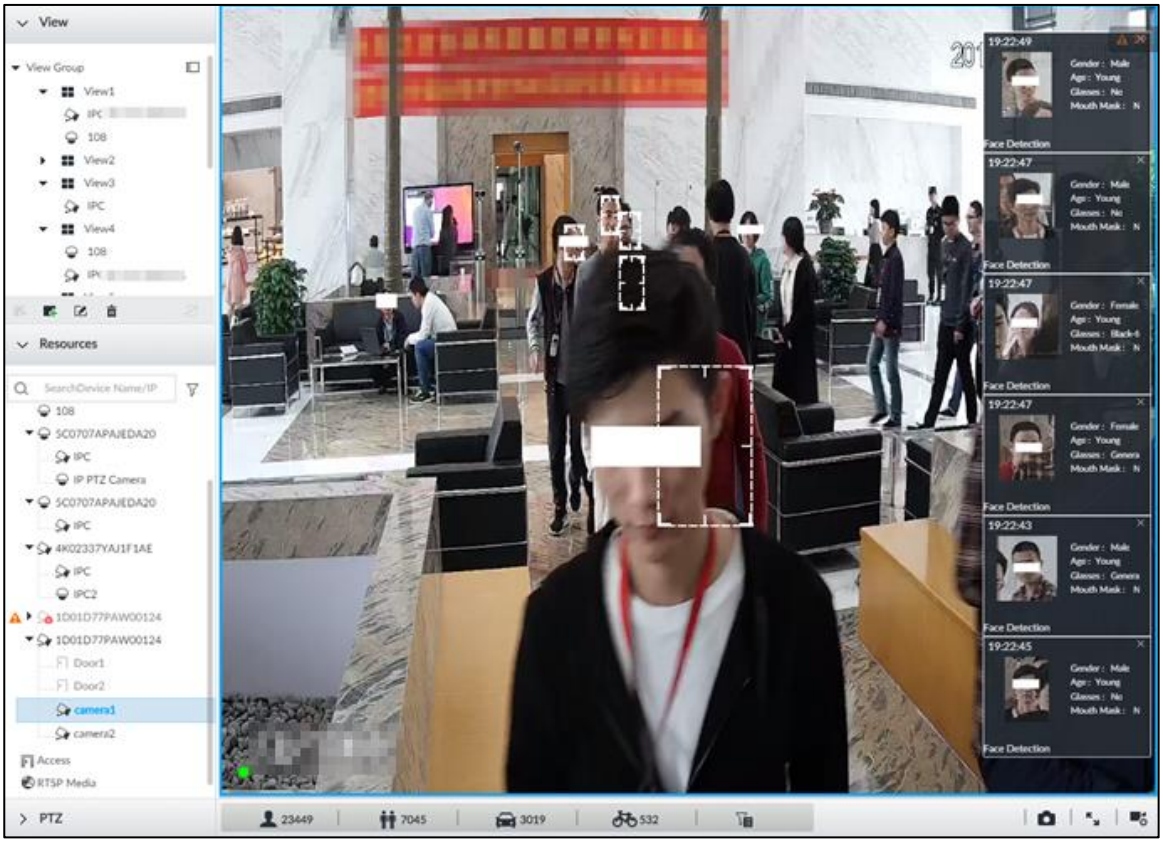
Step 4 Click **OK** to save the configuration.

4.2.3.2 Live View

Go to the **LIVE** interface, enable view, and then view videos are displayed. See Figure 4-6.

- The view window displays currently detected face rule boxes.
- Features panels are displayed on the right side in real time.
  The features panel displays detection time, face snapshot and face features details.

Figure 4-6 Live

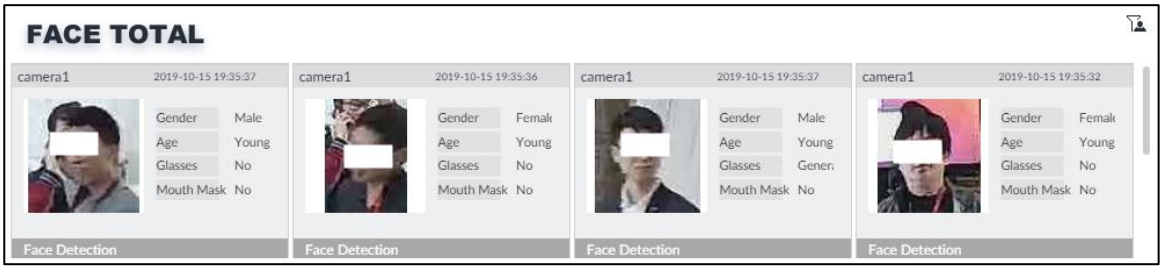


Point to a features panel, and click  or double-click the detected image, so the system starts to play back the recorded videos (about 10 s) at the time of snapshot.

4.2.3.3 Face Records

On the **LIVE** interface, click  . The **FACE TOTAL** interface is displayed. Click  . And then select **Face Detection**. The latest face detection records are displayed. See Figure 4-7.

Figure 4-7 Detection image



On the **FACE TOTAL** interface, the following operations are available.

- Point to a piece of face record, click  or double-click the detected image, and then the system starts to play back the recorded videos (about 10 s) at the time of snapshot.
- Point to a piece of face record, click  , and then you can save that record locally including the video and pictures.

4.2.4 Face Search

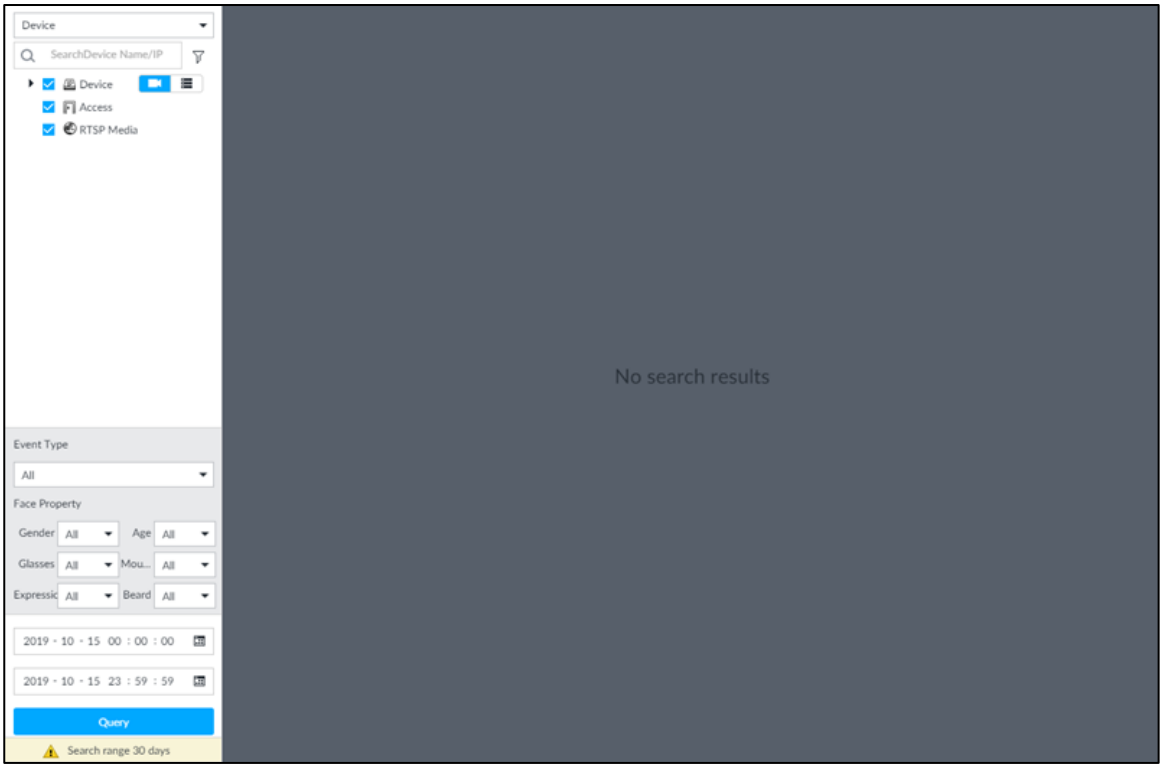
Search for face detection information, including face detection image, record and features.

4.2.4.1 Searching by Property

Step 1 Click , select **AI SEARCH > Search by Face**.

The **Search by Face** interface is displayed. See Figure 4-8.

Figure 4-8 Search by face



Step 2 Select a remote device, and then set **Event Type** to be **Face Detection**.

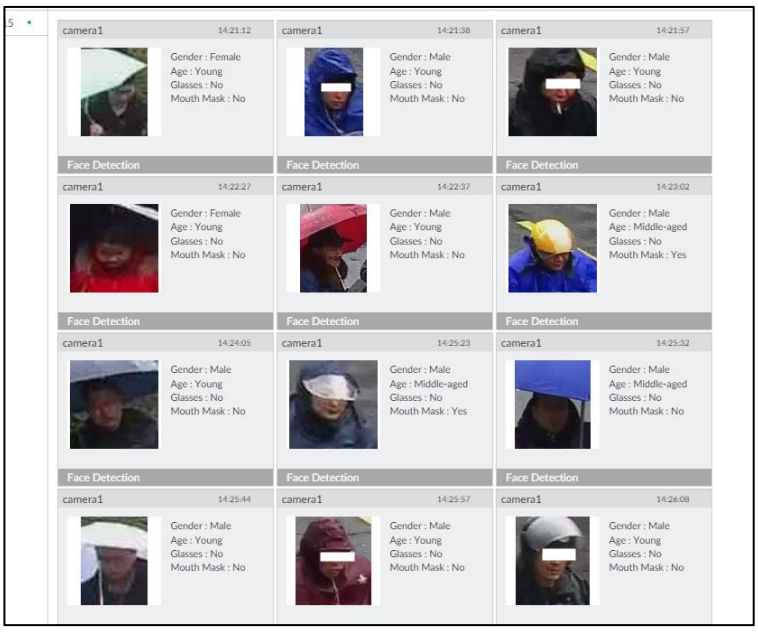
In the **Event Type** drop-down list, if you select **All**, the search results will include both face detection records and face recognition records.

Step 3 Set face property and time.

Step 4 Click **Query**.

The search results are displayed. See Figure 4-9.

Figure 4-9 Search results



Point to a piece of record, and then the following icons are displayed. For details, see Table 4-1.

Table 4-1 Description

Icon	Operation
	● Select one by one: Click the panel or move the mouse pointer onto the panel, and then click to select the panel. means it is selected. ● Batch select: Check **All** to select all panels on the interface.
	Click or double-click the panel, the system starts to play back the recorded videos (about 10 s).
	Click or select the panel and click to export images, videos and Excel to designated storage path. After setting alarm linkage snapshot, during exporting images, the system exports detected images and panoramic images at the time of snapshot.

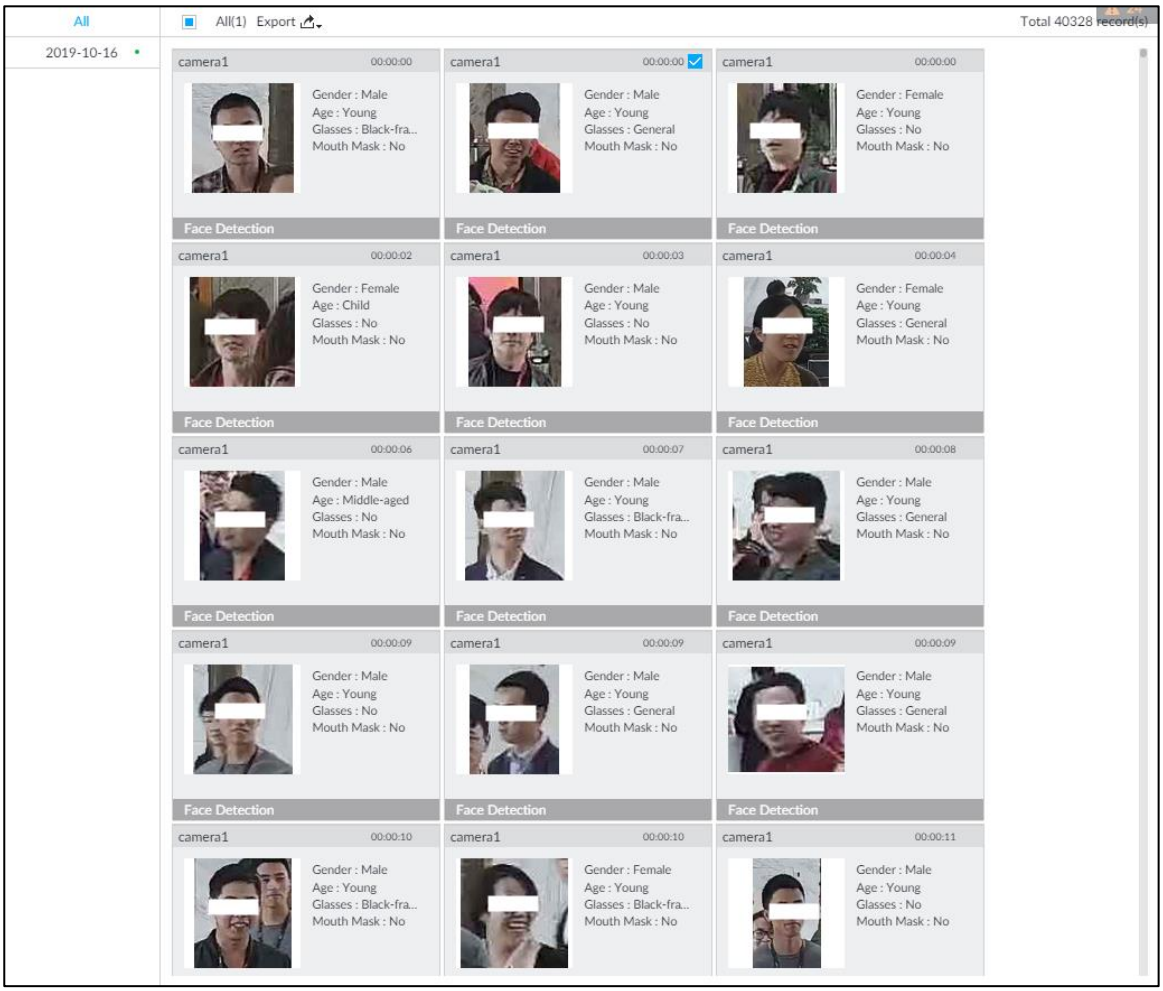
4.2.4.2 Exporting Face Records

The search results of face records can be exported. You can select to export video, picture and excel.

- The exported alarm-linked snapshot contains the face snapshot and the background picture.
- To save the background picture, make sure that you have configured alarm-linked snapshot storage.

The search results are displayed as follows. See Figure 4-10.

Figure 4-10 Search results of face records



- Export in batches

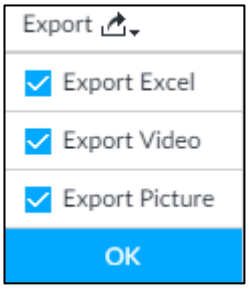
Export more than one record. Support specifying file formats.

Step 1 Select more than one record.

To export all records, select the check box of **All**.

Step 2 Click , and then select file formats. See Figure 4-11.

Figure 4-11 File format



Step 3 Click **OK**, and then follow the onscreen instructions to finish exporting.

- Export one by one

Export one piece of record. The exported file contains excel, snapshot and video by default.

Step 1 Point to a piece of record, and then click .

The **Save** interface is displayed.

Step 2 Select a file type between DAV and MP4, set the saving path, and then click **OK**.

4.3 Face Recognition

The system compares captured face with the face database and works out the similarity. When the similarity reaches the threshold as you have defined, an alarm will be triggered.

Make sure that the face database has been configured on the camera. For details, see user's manual of camera.

4.3.1 Enabling AI Plan

Enable the corresponding AI plan first. For details, see "4.2.1 Enabling AI Plan."

4.3.2 Configuring Face Recognition

Configure face recognition rules.

Step 1 Click , or click on the configuration interface, and then select **EVENT**.

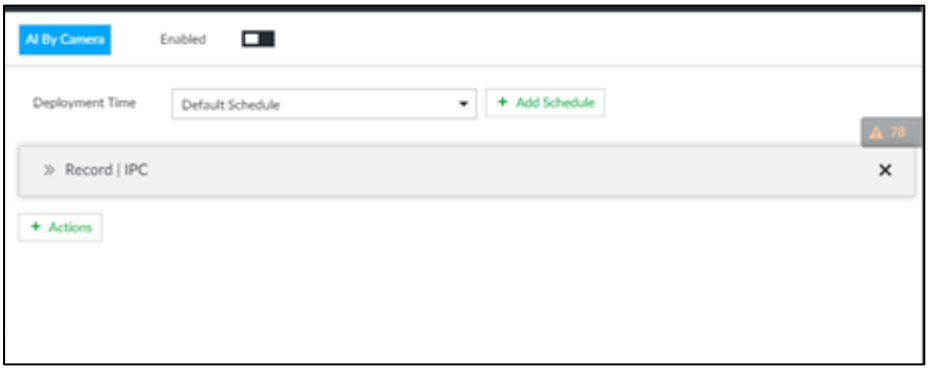
The **EVENT** interface is displayed.

Step 2 Select remote device in the device tree on the left.

Step 3 Select **AI Plan > Face Recognition**.

The **Face Recognition** interface is displayed. See Figure 4-12.

Figure 4-12 Face recognition



Step 4 Click to enable face recognition.

Step 5 Click **Deployment Time** to select schedule from the drop-down list.

After setting arm period, system triggers actions when there is a motion detection alarm in the specified period.

- Click **View Schedule** to view detailed schedule settings.
- If the schedule is not added or the added schedule does not meet actual needs, click **Add Schedule**. See "6.8.3 Schedule" for detailed information.

Step 6 Click **Actions** to set alarm actions. For details, see "6.4.1 Alarm Actions."

Step 7 Click **Save**.

4.3.3 Live View of Face Recognition

Smart panel display. You can view real-time face detection and human face recognition images.

4.3.3.1 Setting AI Display

You can configure display rule of AI detection results.

Before using this function, ensure that view has been created. See "5.1.1 View Management" for detailed information.

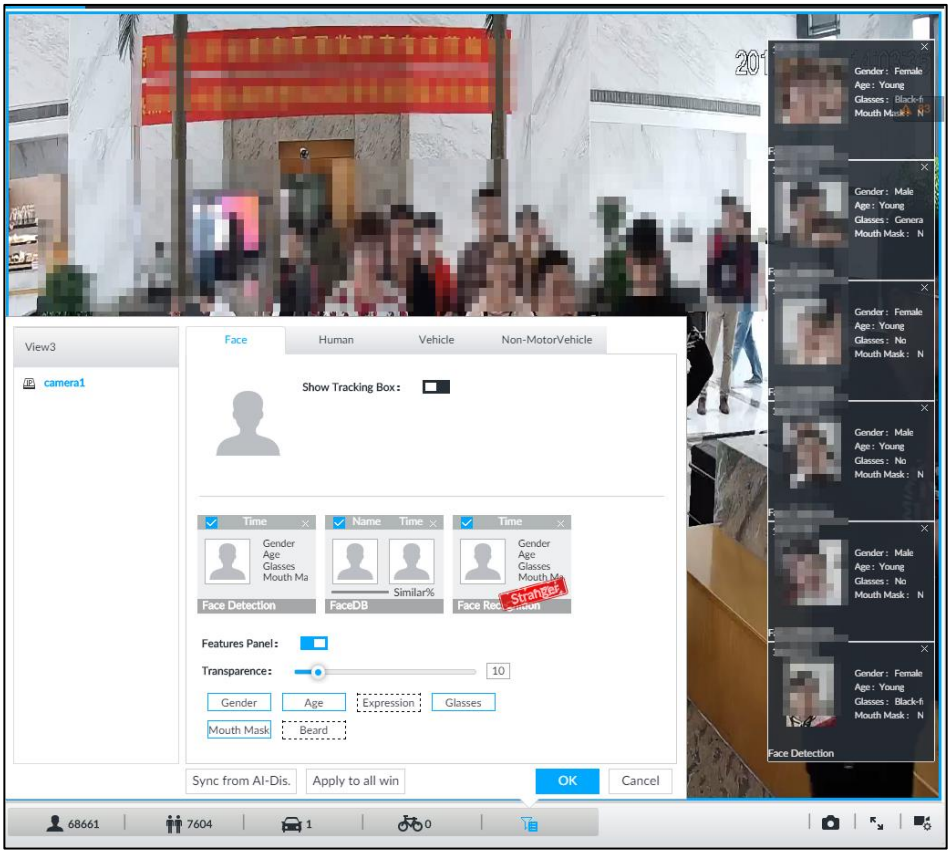
Step 1 On the **LIVE** interface, open a view window.

Step 2 Click and select the **Face** tab.

The **Face** interface is displayed. See Figure 4-5.

- Click **Sync from AI-Dis.**, obtain global smart detection display rule of EVS. See "6.4.2.3.2 Setting AI Display" for detailed information.
- Click **Apply to all windows** to copy current configuration to other window(s).

Figure 4-13 Face



Step 3 Click next to **Show Tracking Box**, to enable the function.

After it is enabled, when the system detects face or human, the window will display corresponding rule box.

Step 4 Enable features panel.

1) Click next to **Features Panel**, to enable the function. When the panel is enabled, the snapshots of detected faces are displayed on the live view.
2) Click to select **Face DB** tab and **Face Recognition** tab. indicates that the panel is selected.

- If the **Face DB** panel is selected, it is displayed on the live video when the similarity between a detected face and one in the face database reaches the threshold.
- If the **Face Recognition** panel is selected, it is displayed on the live video when the similarity between a detected face and one in the face database does not reach the threshold.

3) (Optional) Drag to adjust features panel transparency. The higher the value, the more transparent the features panel.
4) (Optional) Select the features you need to display.
   - System supports displaying 4 feature types.
   - System has checked four features by default. To select other features, cancel the selected features, and then select the ones you need.

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

4.3.3.2 Live View

Go to the **LIVE** interface, enable view, and then device displays view video. See Figure 4-6.

- The view window displays currently detected face rule box.
- The right side displays features panel.
  The features panel displays detection time, face snapshot and face features.

Figure 4-14 Live

Point to a features panel, and then click or double-click the detected image, so the system starts to play back the recorded videos (about 10 s) at the time of snapshot.

4.3.3.3 Face Total

On the **LIVE** interface, click . Face detection panel is displayed. See Figure 4-7. Point to a panel, and the operation icons are displayed.

Figure 4-15 Detection image

- Point to a panel, and click or double-click the detected image, so the system starts to play back the recorded videos (about 10 s) at the time of snapshot.
- Point to a panel, click , and then you can save that record locally.

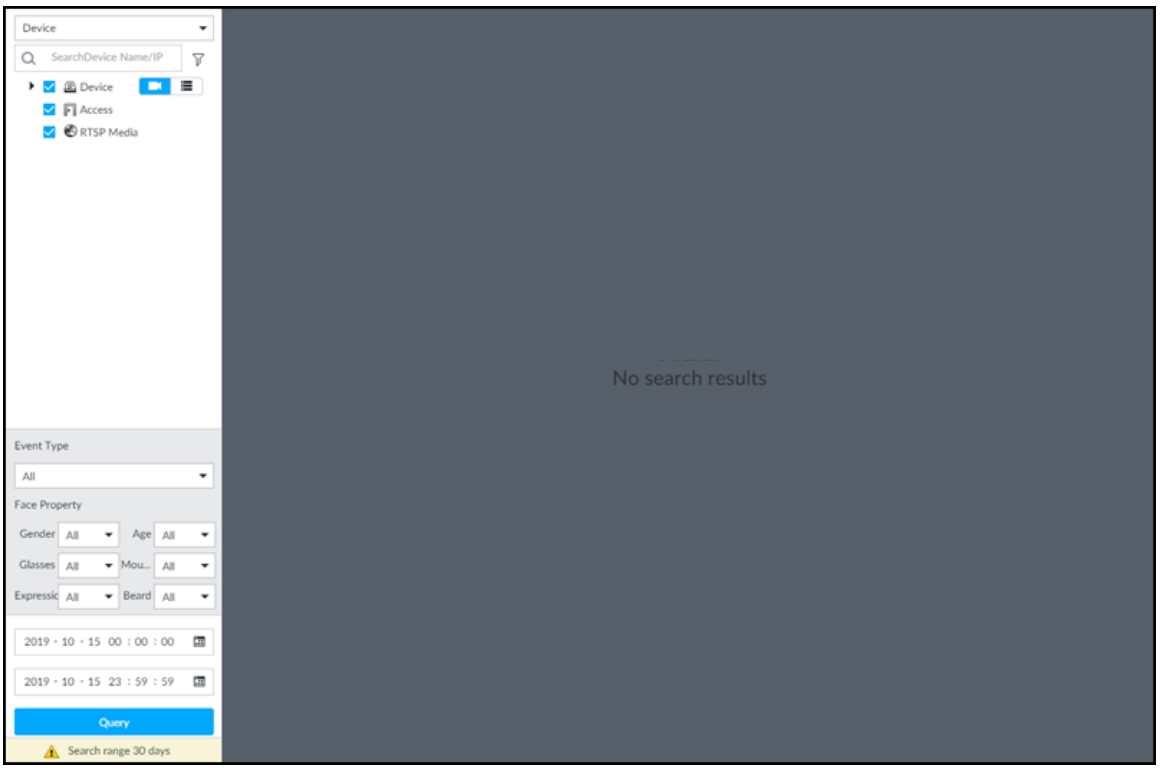
4.3.4 Face Search

Search for face detection information, including face detection image, record and features. Search according to record and image.

Step 1 Click , select **AI SEARCH > Search by Face**.

The **Search by Face** interface is displayed. See Figure 4-8.

Figure 4-16 Search by face



Step 2 Select a remote device, and then set **Event Type** to be **Face Detection**.

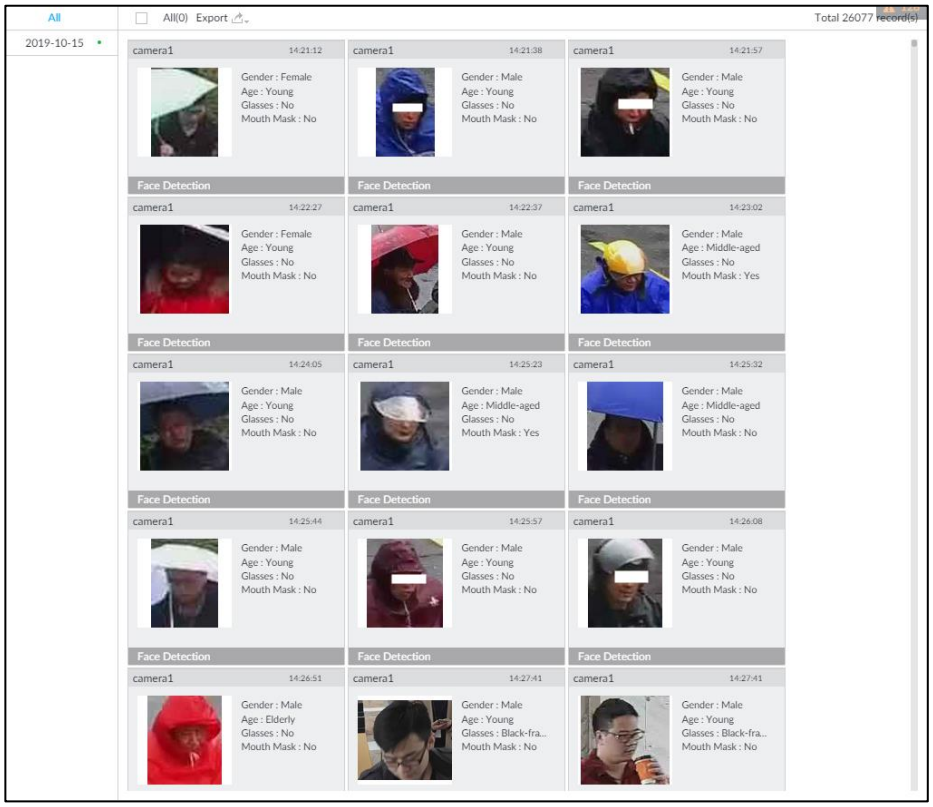
In the **Event Type** drop-down list, if you select **All**, the search results will include both face detection records and face recognition records.

Step 3 Set face property and time.

Step 4 Click **Query**.

The search results are displayed. See Figure 4-17.

Figure 4-17 Search results



Point to a piece of record, the following icons are displayed. For details, see Table 4-2.

Table 4-2 Description

Icon	Operation
	● Select one by one: Click the panel or move the mouse pointer onto the panel, and then click to select the panel. means it is selected. ● Batch select: Check **All** to select all panels on the interface.
	Click or double-click the panel, the system starts to play back the recorded videos (about 10 s).
	Click or select the panel and click to export images, videos and Excel to designated storage path. After setting alarm linkage snapshot, during exporting images, the system exports detected images and panoramic images at the time of snapshot.

4.4 People Counting

Statistics of in-area people number, and queuing number.

The old people counting data will be overwritten when the storage space is runs out. You are recommended to back up the data in time.

4.4.1 Enabling AI Plan

You need first enable the corresponding AI plan; otherwise the AI function does not work. For details, see "4.2.1 Enabling AI Plan."

4.4.2 People Counting

Configure this function to count the number of people in and out of the detection area. When the statistical number is larger or smaller than the threshold, an alarm is triggered.

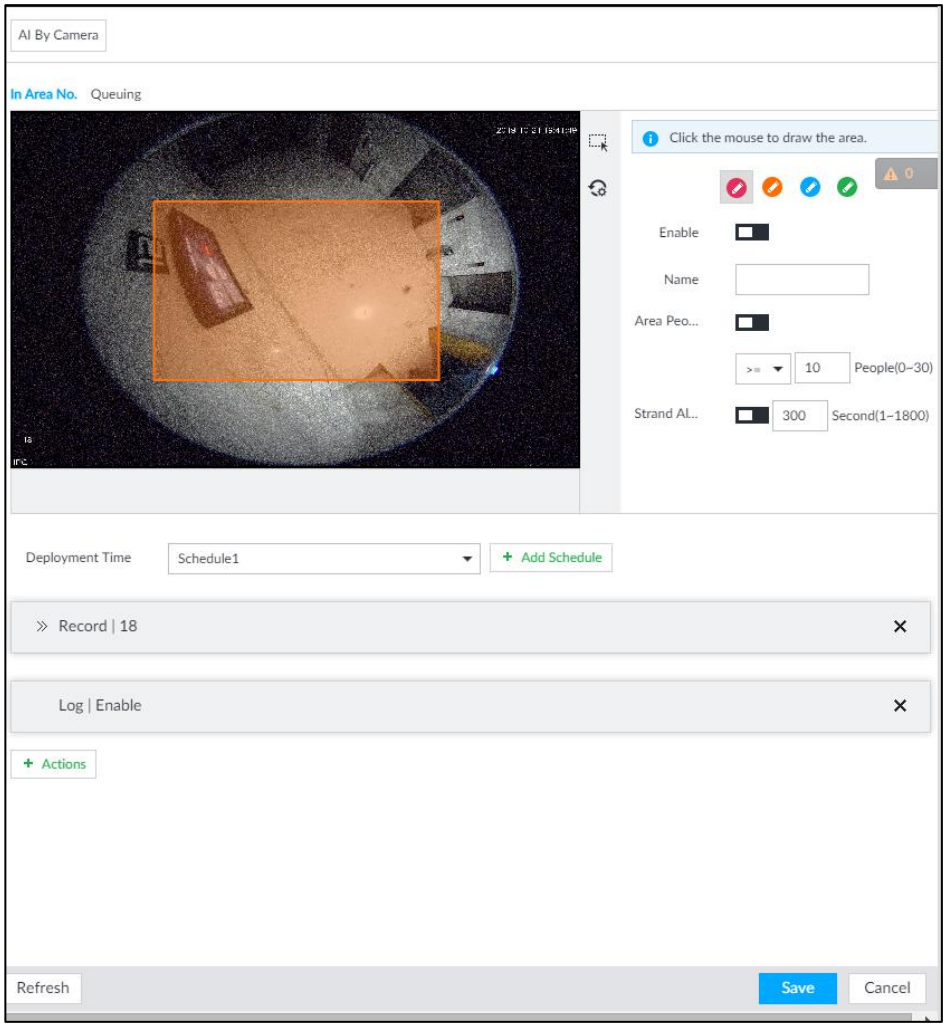
Step 1 Click , click , and then select **EVENT**.

The **EVENT** interface is displayed.

Step 2 Select a camera in the device tree, and then select **AI Plan > People Counting > In Area No.**.

The **In Area No.** interface is displayed. See Figure 4-18.

Figure 4-18 In Area No.



Step 3 Draw a people counting area.

1) Click to draw the first detection area.

Click to draw more areas. You can draw 4 areas at most.

2) Click to edit the area.

◇ Click and drag to adjust the position and length.

◇ Click the white dot on the frame of the area to add turning corners.

◇ Click to restore to the default area.

Step 4 Set parameters. See Table 4-3.

Table 4-3 Parameters description of people counting

Parameters	Description
Enable	Click to enable the selected area.
Name	Enter area name
Area People Counting Alarm	1. Click to enable the alarm. 2. Set people number threshold. ● Select >=, and enter a threshold value. When the people number in the area is greater than the threshold, an alarm will be triggered. ● Select <=, and enter a threshold value. When the people number in the area is smaller than the threshold, an alarm will be triggered.
Strand Alarm	1. Click to enable the alarm. 2. Set time threshold for the alarm. When the dwell time of any person in the area is greater than the threshold, an alarm will be triggered.

Step 5 Select a schedule in the **Deployment Time** drop-down list.

Alarms are triggered only within the scheduled time.

Step 6 Click **Actions** to set alarm linkage actions. For details, see "6.4.1 Alarm Actions."

Step 7 Click **Save**.

4.4.3 Queuing Detection

The system counts the number of people queuing in the detection area. When the number of people exceeds the threshold or the queue time is longer than the pre-defined time, an alarm is triggered.

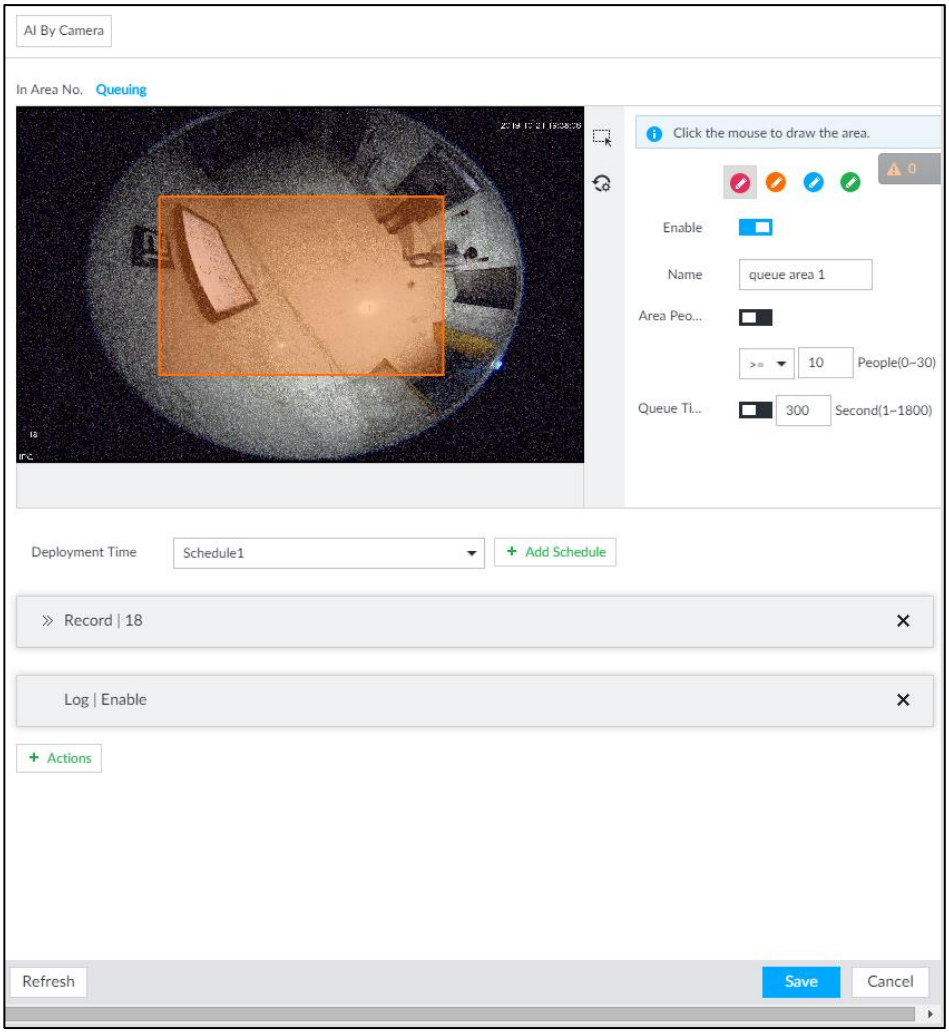
Step 1 Click , click , and then select **EVENT**.

The **EVENT** interface is displayed.

Step 2 Select a camera in the device tree, and then select **AI Plan > People Counting > Queuing**.

The **Queuing** interface is displayed. See Figure 4-19.

Figure 4-19 Queuing



Step 3 Draw a queuing detection area.

1) Click to draw the first detection area.

Click to draw more areas. You can draw 4 areas at most.

2) Click to edit the area.

◇ Click and drag to adjust the position and length.

◇ Click the white dot on the frame of the area to add turning corners.

◇ Click to restore to the default area.

Step 4 Set parameters. See Table 4-4.

Table 4-4 Parameters description of queuing detection

Parameters	Description
Enable	Click to enable the selected area.
Name	Enter the area name
Area People Counting Alarm	1. Click to enable the alarm. 2. Set people number threshold. ● Select >=, and enter a threshold value. When the people number in the area is greater than the

Parameters	Description
	threshold, an alarm will be triggered. ● Select <= , and enter a threshold value. When the people number in the area is smaller than the threshold, an alarm will be triggered.
Queuing Time Alarm	1. Click to enable the alarm. 2. Set time threshold for the alarm. When the queuing time of any person in the area is longer than the threshold, an alarm will be triggered.

Step 5 Select a schedule in the **Deployment Time** drop-down list.
Alarms are triggered only within the scheduled time.

Step 6 Click **Actions** to set alarm linkage actions. For details, see "6.4.1 Alarm Actions."

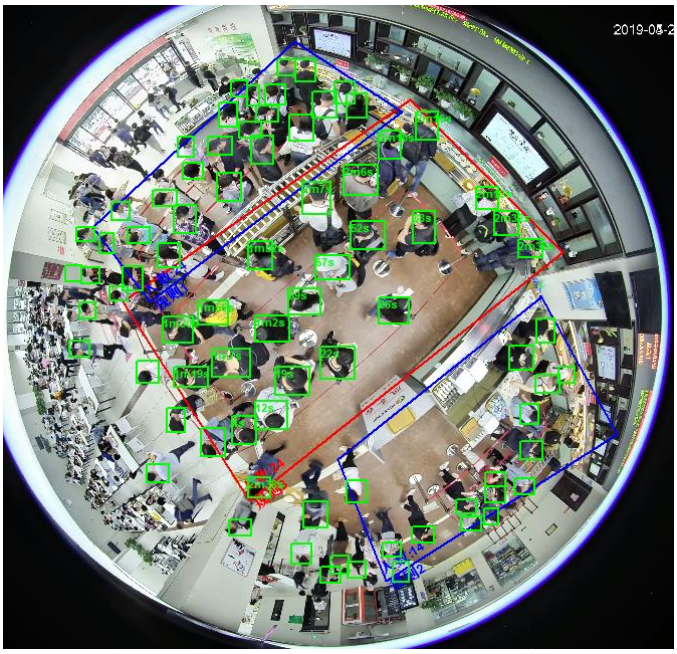
Step 7 Click **Save**.

4.4.4 Live View

On the **LIVE** interface, enable a view window that contains people counting video.

The live video which shows real-time people number and queuing time is displayed. See Figure 4-20.

Figure 4-20 Live view



The live video displays real-time people number in the region, and the region frame flashes red once there is an alarm. The queue-detection live view also shows head frames and the dwell time of each person.

4.5 Video Metadata

The system analyzes real-time video stream to detect the existence of 4 target types: human, human face, motor vehicle, non-motor vehicle. Once a target is detected, the system can record video, take snapshots and trigger alarms.

This section introduces how to configure the video metadata feature from enabling it and selecting target types to setting the live view of video metadata.

4.5.1 Enabling AI Plan

Enable AI plan. See "4.2.1 Enabling AI Plan" to enable AI detect function.

4.5.2 Configuring Video Metadata

After enabling video metadata, EVS links the current remote device for taking snapshots when alarm is triggered.

Video metadata cannot be enabled at the same time with face detection and IVS, because it conflicts with the two functions.

Step 1 Click  or  , and then select **EVENT**.

The **EVENT** interface is displayed.

Step 2 Select a device from the device tree at the left side.

Step 3 Select **AI Plan > Video Metadata**.

Step 4 Select the detection target.

- People: Click the corresponding  to enable people detection. Face detection can also be enabled at the same time.
- Vehicle: Click the corresponding  to enable vehicle detection.
- Non-Motor Vehicle: Click the corresponding  to enable non-motor vehicle detection.

Step 5 Click **Deployment Time** drop-down list to select schedule.

EVS links alarm event when an alarm is triggered within the schedule configured.

- Click **Add Schedule** to add new schedule if no schedule is added or the existing schedule does not meet requirements. For details, see "6.8.3 Schedule."
- Click **View Schedule** to view details of schedule.

Step 6 Click **Save**.

4.5.3 Live View of Video Metadata

View the detection results of face, people, motor vehicle and non-motor vehicle on the **LIVE** interface.

4.5.3.1 Setting AI Display

Set the filtering conditions to display AI detection results.

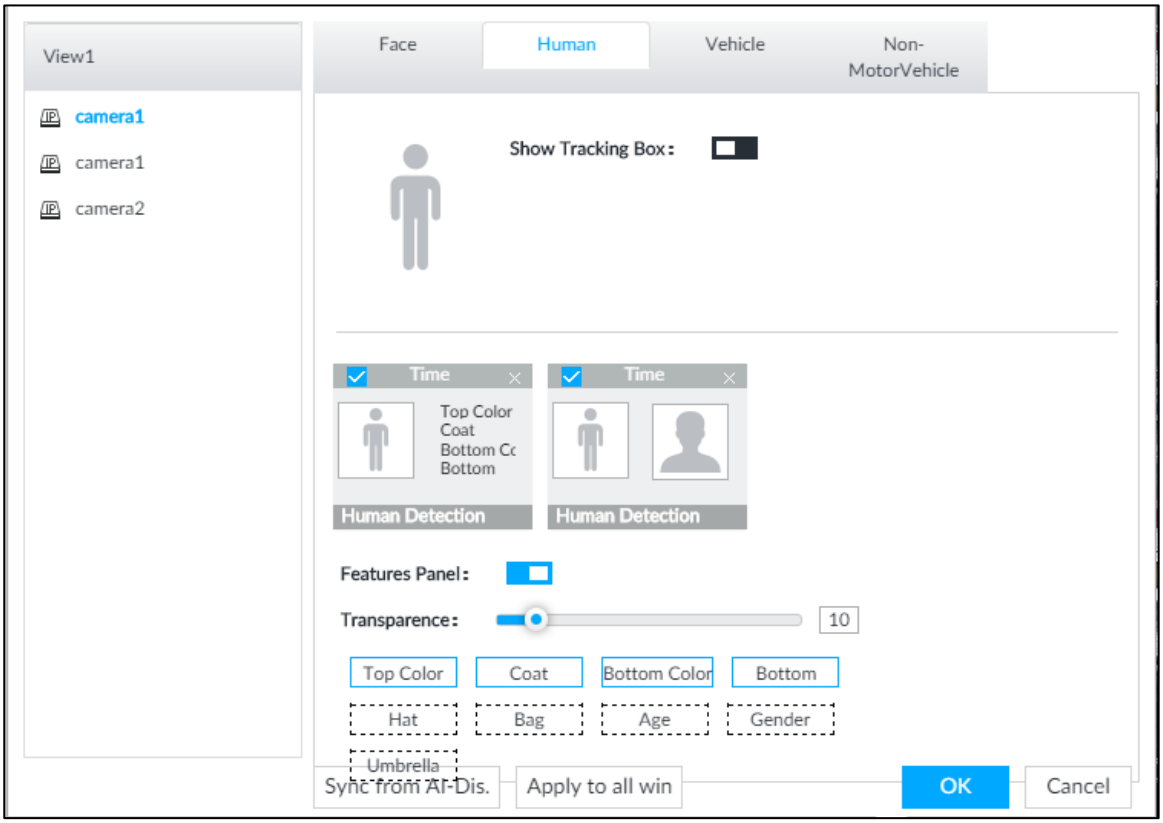
Create view(s) before setting filtering conditions. To create a view, see "5.1.1 View Management."

Step 1 Select a view from **LIVE > View > View Group**.

Step 2 Click at the lower side of the **LIVE** interface, and then select **Face, Human**, **Vehicle** or **Non-Motor Vehicle**. See Figure 4-21.

The figure takes **Human** for example. The interface is for reference only, and the actual interface shall prevail.

Figure 4-21 Human



Step 3 Click next to **Show Tracking Box**, and then a tracking box is displayed in the video when target that meets the filtering conditions is detected.

Step 4 Configure feature panel.

1) Click next to **Features Panel** to enable feature panel.

   A features panel is displayed on the right side of the video when target that meets the conditions is detected.

2) Click to select the panel type, for example, the **Human Detection** tab.

3) (Optional) Drag to adjust the transparency of panel. The higher the value, the more transparent the panel.

4) (Optional) Select the features to be displayed in the panel.

   - Up to 4 features can be displayed.
   - 4 features are selected by default. To select another feature, click the selected feature to cancel it, and then click the feature to be displayed.

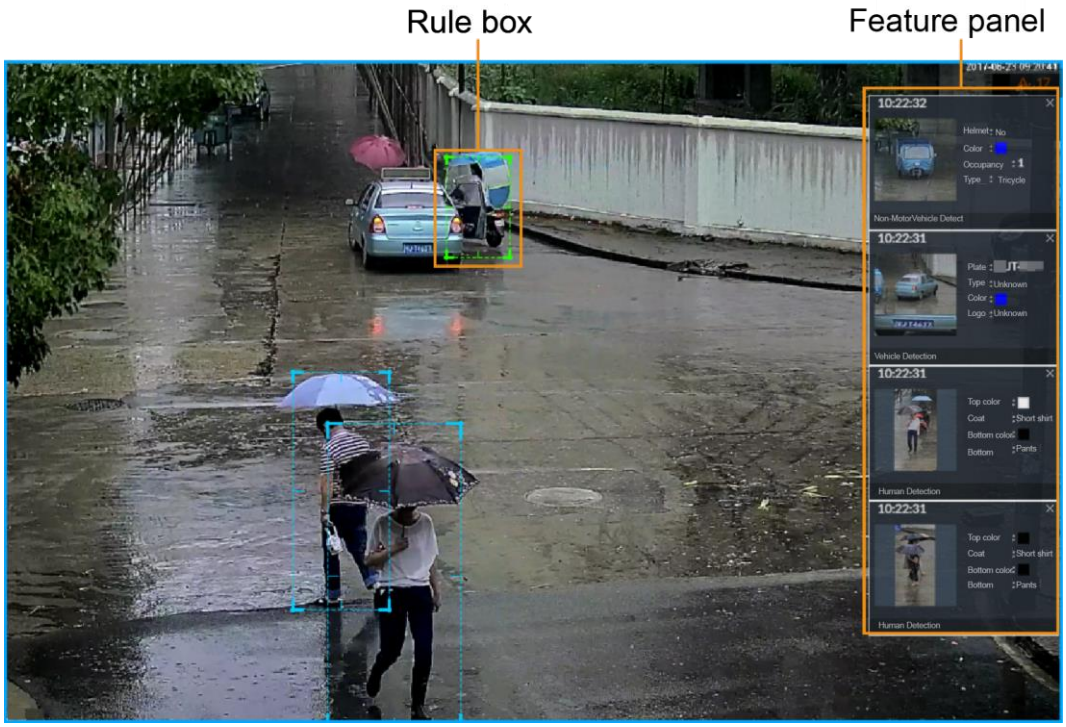
Step 5 Click **OK**.

4.5.3.2 Live View

On the **LIVE** interface, select a view from **View Group**, and the video image of the view will be displayed. See Figure 4-22.

- Rule box is displayed in real-time in the video image. Different detection targets correspond to different colors of rule box, and the actual interface shall prevail.
- Features panels are displayed on the right side of the video image.

Figure 4-22 Live



Point to the features panel, and then click , or double-click the detected image to play back the video record (10 s before and after the snapshot).

4.5.3.3 Detection Statistics

View the detection statistics of human, motor vehicle and non-motor vehicle.

4.5.3.3.1 Human

On the **LIVE** interface, click , the **PEOPLE TOTAL** interface is displayed.

Click , and then select **Snap With Face** and **Snap Without Face**. The information of detected human and face is displayed.

- Point to the snapshot, and then click or double-click a pted picture to play back the video record (10 s before and after the snapshot).
- Point to the snapshot, and then click to export the video record to specified saving

path.

4.5.3.3.2 Motor Vehicle

On the **LIVE** interface, click , the **VEHICLE TOTAL** interface is displayed.

Click , and then select **Vehicle Recognition**, the information of detected vehicles is displayed. See Figure 4-23.

Figure 4-23 Motor vehicle detection

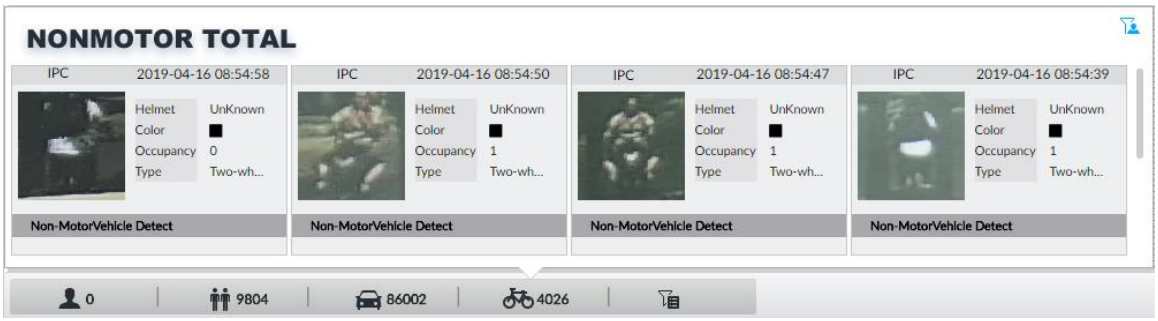
- Move the mouse pointer to the panel, and then click , or double-click detected picture to play back the video record (10 s before and after the snapshot).
- Move the mouse pointer to the panel, and then click to export the video record to specified saving path.

4.5.3.3.3 Non-motor Vehicle

On the **LIVE** interface, click , the **NONMOTOR TOTAL** interface is displayed.

Click , and then select **Snap With Face** and **Snap Without Face**. The information of detected non-motor vehicles is displayed. See Figure 4-24.

Figure 4-24 Non-motor vehicle detection



- Move the mouse pointer to the detected information, and then click , or double-click detected picture to play back the video record (10 s before and after the snapshot).
- Move the mouse pointer to the detected information, and then click to export the video record to specified saving path.

4.5.4 AI Search

Select device and set properties to search for detection results.

4.5.4.1 Human Search

Select device and set human properties to search human detection results.

Step 1 Click , and then select **AI SEARCH > Search by Human**.

The **Search by Human** interface is displayed. See Figure 4-25.

Figure 4-25 Search by human

Step 2 Select a device, and then set human properties and time period.

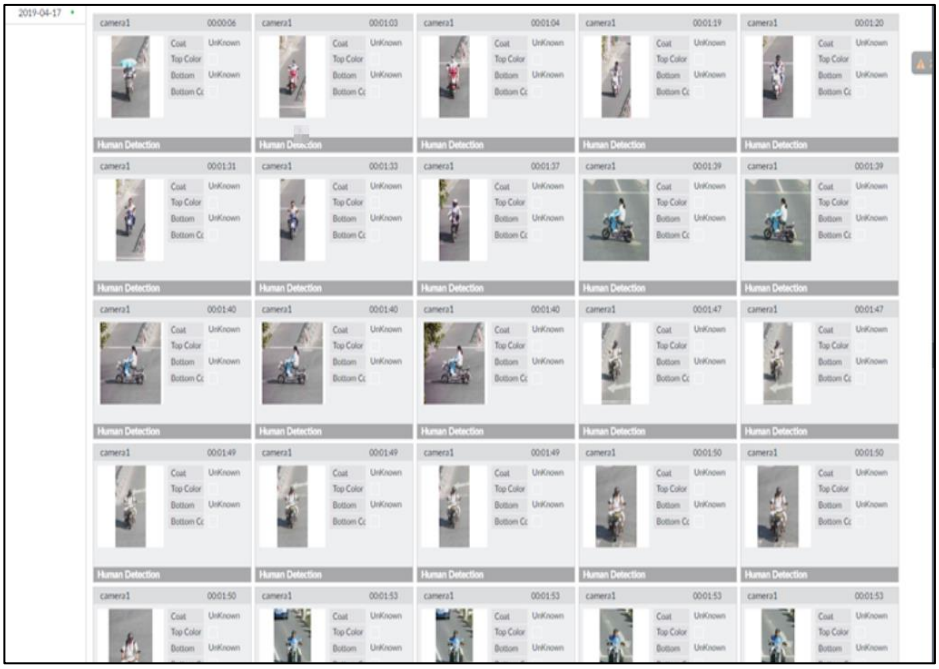
Click or to set the color. means more than one color.

Step 3 Click **Query**.

The search result is displayed. See Figure 4-26.

- If face is captured, the human and face snapshots are displayed.
- If no face is captured, the human snapshot and human properties are displayed.

Figure 4-26 Search result



Other Operations

Click on one displayed panel, and the icons are displayed. For details, see Table 4-5.

Table 4-5 Operation

Icon	Operation
	• Select one by one: Click  to select the panel.  means the panel is selected. • Select in batches: Select **All** to select all the panels on the interface.
	Click  or double-click the panel to play back the video record (10 s before and after the snapshot).
	Click  , or select the panel and then click  to export picture, video, and Excel file to specified saving path.

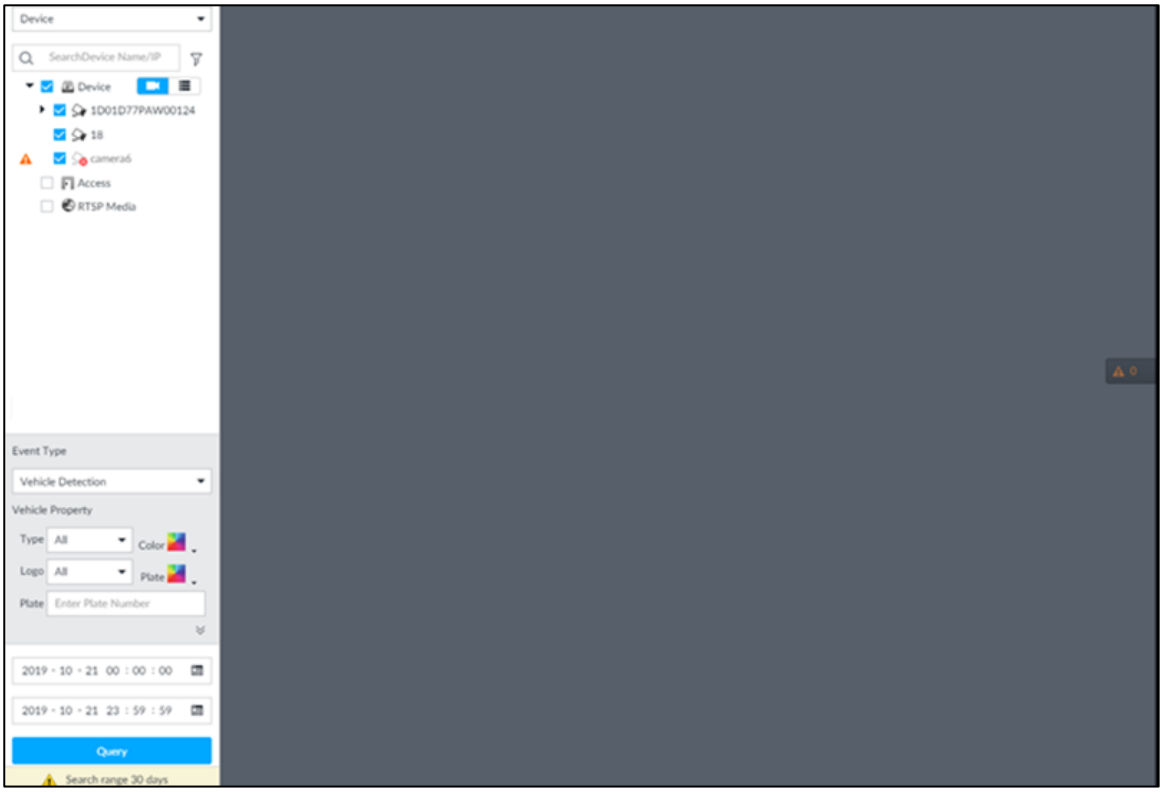
4.5.4.2 Vehicle Search

Set event type and vehicle properties to search vehicle detection results.

Step 1 Click  , and then select **AI SEARCH > Search by Vehicle**.

The **Search by Vehicle** interface is displayed. See Figure 4-27.

Figure 4-27 Vehicle search



Step 2 Select Vehicle Detection as Event Type.

Step 3 Set vehicle properties and time period.

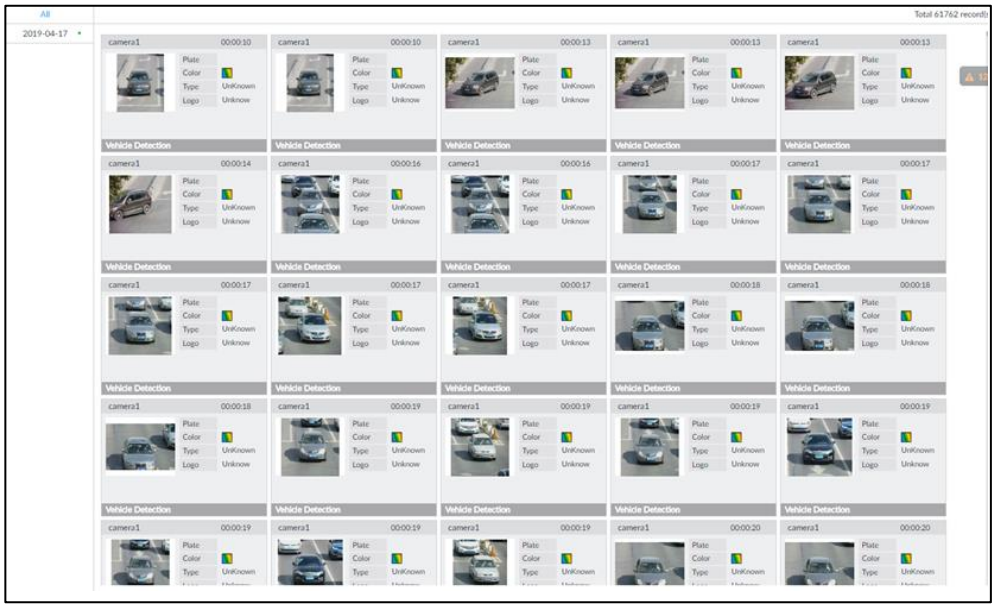
Click  or to set the color.  means more than one color.

Step 4 Click **Query**.

The search results are displayed. See Figure 4-28.

If license plate is detected, both the scenario and the license plate will be displayed.

Figure 4-28 Search result



Click on one displayed panel, and the icons are displayed. See Figure 4-29 and Table 4-6.

Figure 4-29 Icons

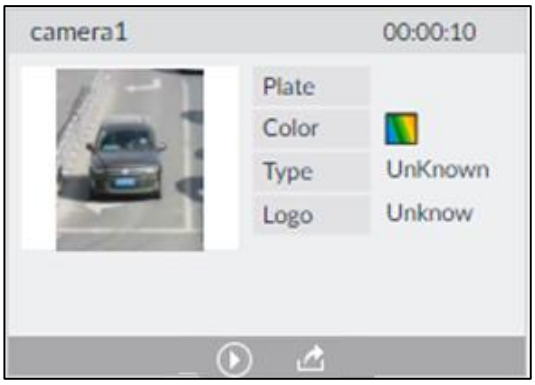


Table 4-6 Operation

Icon	Operation
	• Select one by one: Click to select the panel. means the panel is selected. • Select in batches: Select **All** to select all the panels on the interface.
	Click or double-click the panel to play back the video record (10 s before and after the snapshot).
	Click , or select the panel and then click to export picture, video, and Excel file to specified saving path.

4.5.4.3 Non-motor Vehicle Search

Set event type and non-motor vehicle properties to search non-motor vehicle detection results.

Step 1 Click , and then select **AI SEARCH > Search by NonMotor**.

The **Search by NonMotor** interface is displayed. See Figure 4-30.

Figure 4-30 Search by non-motor vehicle

Step 2 Select the device you want to search.

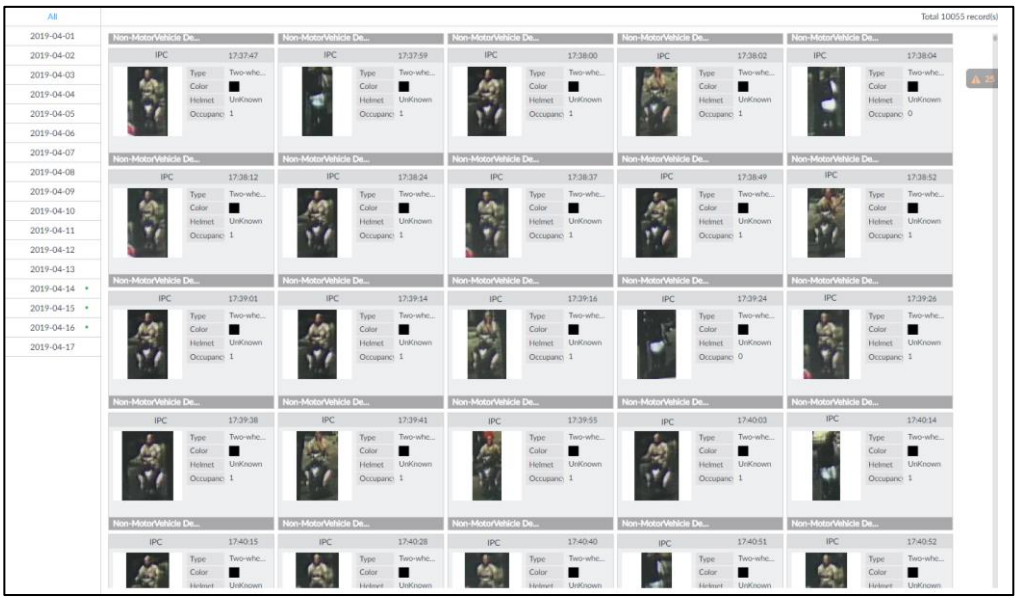
Step 3 Set non-motor vehicle properties and time period.

Click  or to set the color.  means more than one color.

Step 4 Click **Query**.

The search results are displayed. See Figure 4-31.

Figure 4-31 Search results



Click on one displayed panel, and the icons are displayed. See Figure 4-32 and Table 4-7.

Figure 4-32 Icons

Table 4-7 Operation

Icon	Operation
	• Select one by one: Click  to select the panel.  means the panel is selected. • Select in batches: Select **All** to select all the panels on the interface.
	Click  or double-click the panel to play back the video record (10 s before and after the snapshot).
	Click  , or select the panel and then click  to export picture, video, and excel file to specified saving path.

4.6 IVS

The IVS feature includes a number of behavior detections such as fence-crossing, intrusion, tripwire, parking, crowd gathering, missing object, abandoned object, and loitering. You can configure alarm notifications of those intelligent detections.

This section introduces how to configure the intelligent detections.

For the same camera, IVS and face detection cannot be enabled at the same time.

4.6.1 Enabling AI Plan

Enable AI plan. See "4.2.1 Enabling AI Plan" to enable AI detect function.

4.6.2 Configuring IVS

Configure rules of IVS functions such as fence-crossing, tripwire, intrusion, abandoned object, parking detection, people gathering, object removed, and loitering. Different cameras support different functions, and the actual interface shall prevail. For details, see Table 4-8.

Table 4-8 IVS functions description

Functions	Description
Fence-crossing	Alarm is triggered when a target is crossing the pre-defined fence.
Tripwire	Alarm is triggered when a target is crossing the pre-defined tripwire.
Intrusion	Alarm is triggered when a target is entering, leaving, or appears in the detection area.
Abandoned Object	Alarm is triggered when an object is left in the detection area and the existence time is longer than the threshold.
Missing Object	Alarm is triggered when an object is removed from the detection area and not put back after the pre-defined time period.
Parking Detection	Alarm is triggered when a target remains still within a time period longer than the pre-defined time duration.
People Gathering	Alarm is triggered when people gathering is detected or people density is larger than the threshold.
Loitering	Alarm is triggered when a target keeps loitering in a time period longer than the threshold. Alarm will be triggered again if the target stays in the detection area after the first alarm.

Take tripwire as the example. The configuration procedure is as follows.

Step 1 Click , or click on the configuration interface, and then select **EVENT**.

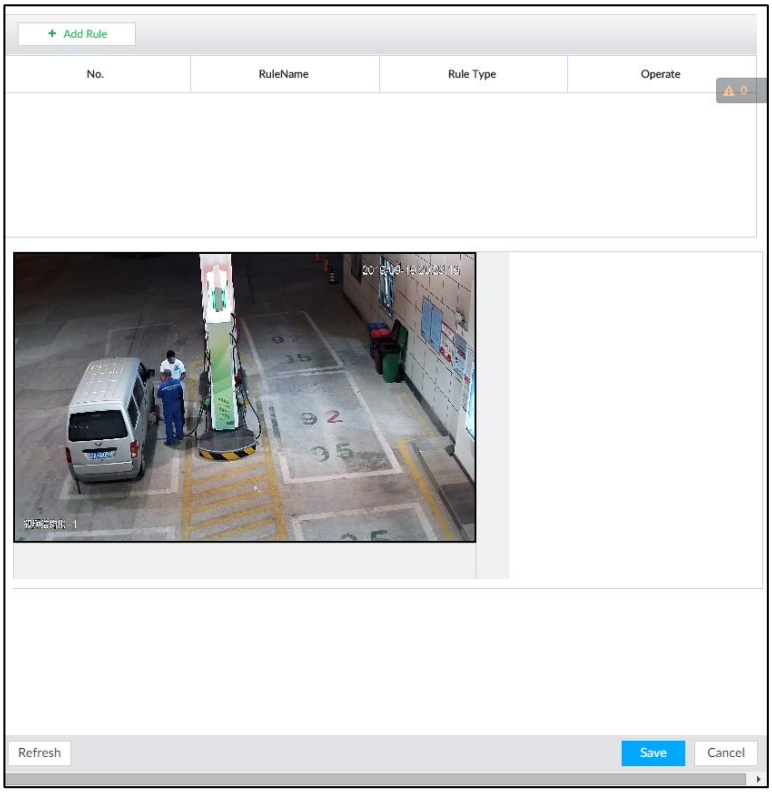
The **EVENT** interface is displayed.

Step 2 Select remote device in the device tree on the left.

Step 3 Select **AI Plan > IVS Rule**.

The **Add Rule** interface is displayed. See Figure 4-33.

Figure 4-33 Add rules

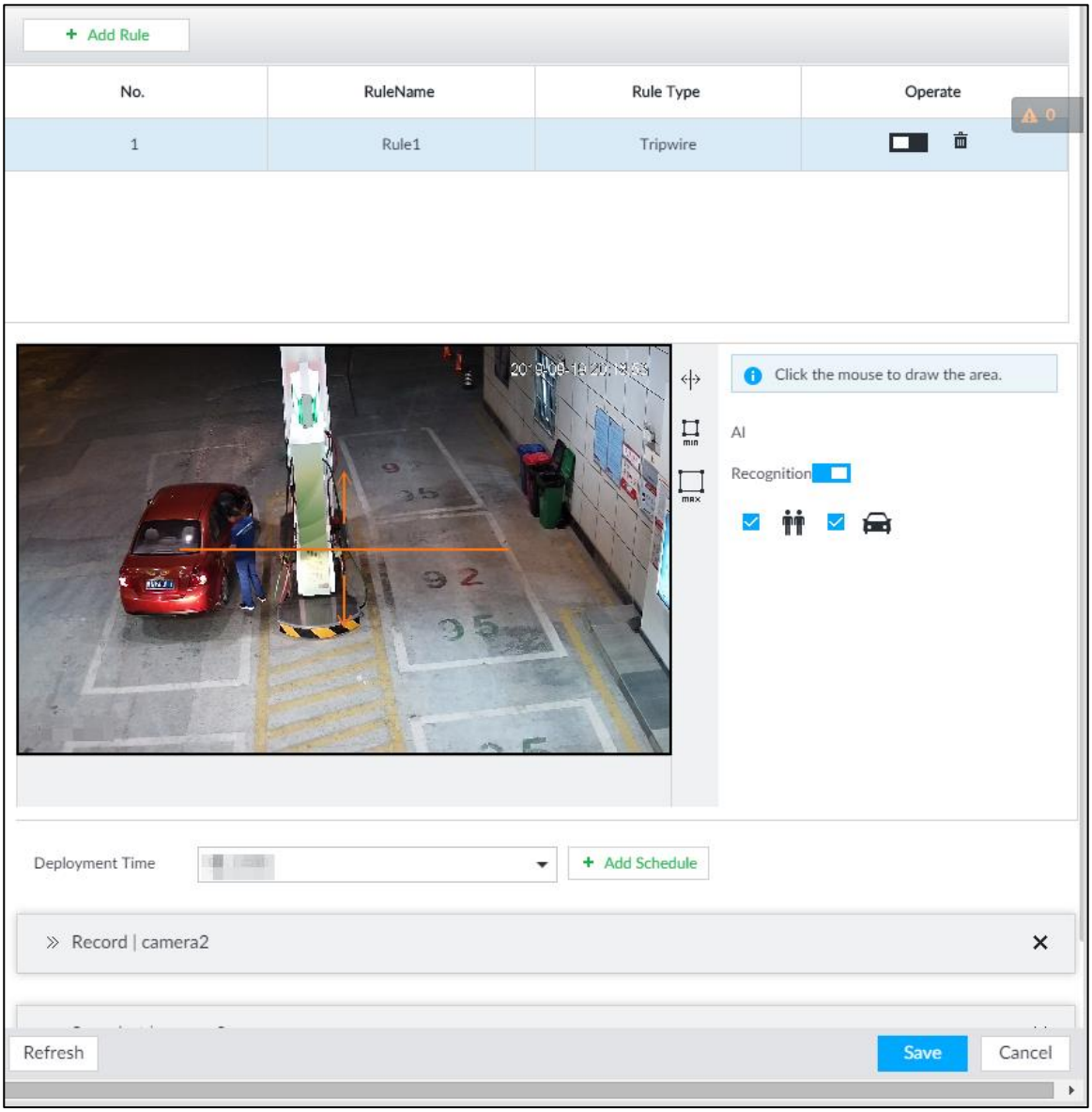


Step 4 Set tripwire rules.

1) Click **Add Rule**, and select **Tripwire**.

The rule information is displayed. See Figure 4-34.

Figure 4-34 Configuring tripwire detection rules



2) Click  to enable detection rule.

   Click  to delete detection rule.

3) Click  to edit the tripwire line.

   - Drag  to adjust position or length of the line.
   - Click or  to set the directions. An alarm will be triggered only when the target crosses the line in the designated direction.
   - Click the white dot on the line to add a turning point. Drag  at the turning point to adjust position or length.

4) Click  or  to set minimum size or maximum size of detection target.

   System triggers an alarm once the detected target size is between the maximum size and the minimum size.

Step 5 (Optional) For other requirements, see Table 4-9.

Table 4-9 IVS rules configuration requirements

Functions	Description
Fence-crossing	Draw 2 detection lines. ● Transparent fences such as iron fence are not supported. ● Extremely short walls (height lower than normal height) are not supported.
Tripwire	Draw 1 detection line.
Intrusion	Draw 1 detection line. With the abandoned object detection, a person or vehicle that stays still for a long time will also trigger an alarm; if the object is smaller than human or vehicle, you can set the target size to filter out people and cars, or extend the minimum lasting duration to avoid false alarms caused by short dwell of people. For the crowd gathering detection, if the installation height is too low, human body size will take a large proportion in the image, or the camera view might be blocked. That might result in false alarms caused by continuous shaking of the camera, shaking leaves, frequent door opening and closing, and dense traffic of vehicles and people.
Abandoned Object	
Missing Object	
Parking Detection	
Crowd Gathering	
Loitering	

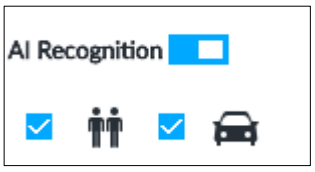
Step 6 Set AI Recognition.

After setting AI recognition, when the system detects a person, vehicle or non-motor vehicle, a rule box will appear beside the target on the video.

1) Click to enable AI recognition function.

The recognition type option is displayed. See Figure 4-35.

Figure 4-35 Type



2) Select a recognition type.

- is to recognize human, and is to recognize vehicle.
- After enabling AI recognition function, at least one recognition type shall be selected.

Step 7 Click **Deployment Time** to select schedule from the drop-down list.

After setting deployment period, system triggers corresponding operations when there is a motion detection alarm in the specified period.

- Click **View Schedule** to view detailed schedule settings.
- If the schedule is not added or the added schedule does not meet actual needs, click **Add Schedule**.

Step 8 Click **Actions** to set alarm action. See "6.4.1 Alarm Actions" for detailed information.

Repeat Step 4-Step 8 to add multiple detection rules. You can add max. 10 detection rules at the same time.

Step 9 Click **Save**.

4.6.3 Live View of IVS

On the **LIVE** interface, view real-time IVS results.

4.6.3.1 Setting AI Display

Set the display rules of detection results.

Make sure that view is created before setting AI display. To create view, see "5.1.1 View Management."

Step 1 Select a view from **LIVE > View > View Group**.

Step 2 Click , and then select the **Human** or **Vehicle** tab.

Figure 4-36 Human

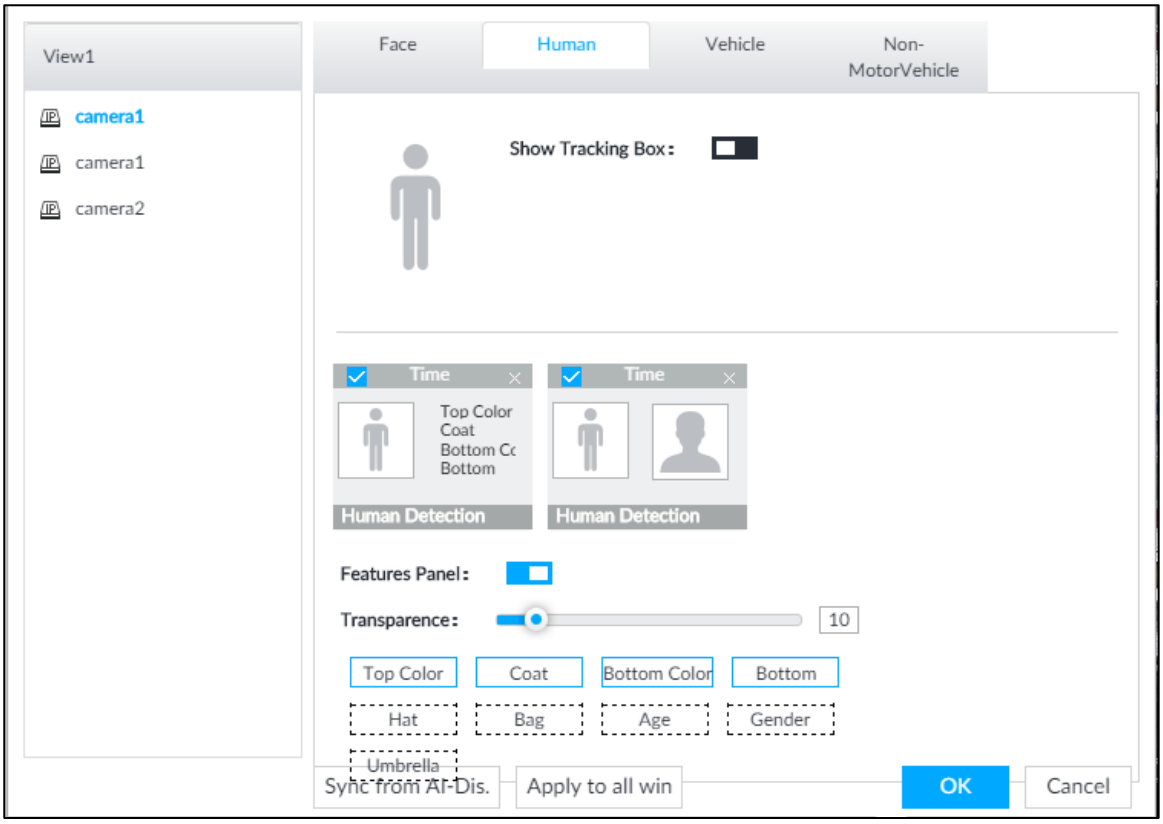
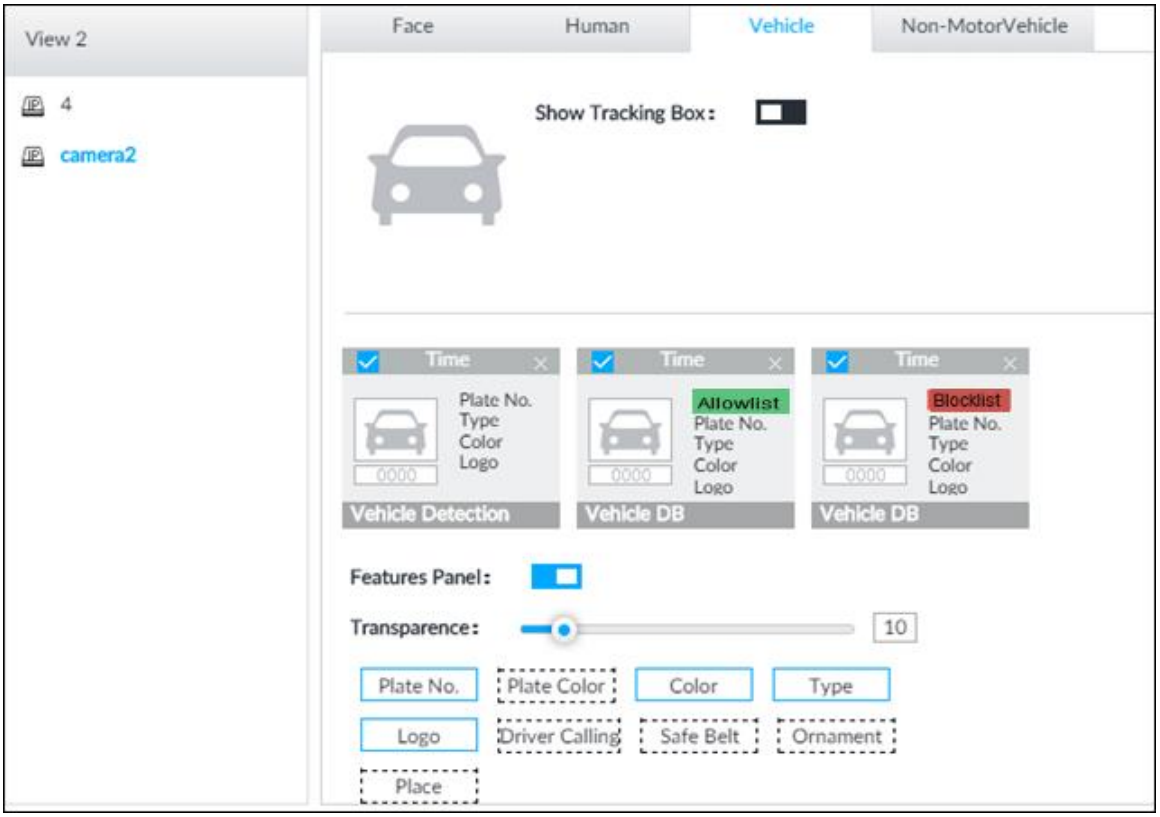


Figure 4-37 Vehicle



Step 3 Click next to **Show Tracking Box**.

Step 4 Configure feature panel.

1) Click next to **Features Panel** to enable feature panel.

   A features panel is displayed on the right side of the video when a target that meets the conditions is detected.

2) Click to select the panel type, for example, the **Human Detection** tab.

3) (Optional) Drag to adjust the transparency of panel. The higher the value, the more transparent the panel.

4) (Optional) Select the features to be displayed in the panel.

   - Up to 4 features can be displayed.
   - 4 features are selected by default. To select another feature, click the selected feature to cancel it, and then click the feature to be displayed.

Step 5 Click **OK**.

4.6.3.2 Live View

Go to the **LIVE** interface, enable view, and then Device displays view video. See Figure 4-38.

- When a target triggers cross line or cross region rule, the line or region frame in the view flickers in red.
- After setting AI recognition, when the system detects a person or vehicle, a rule frame will appear beside the person and vehicle in the view.
- There is a feature panel on the right side of the video window.

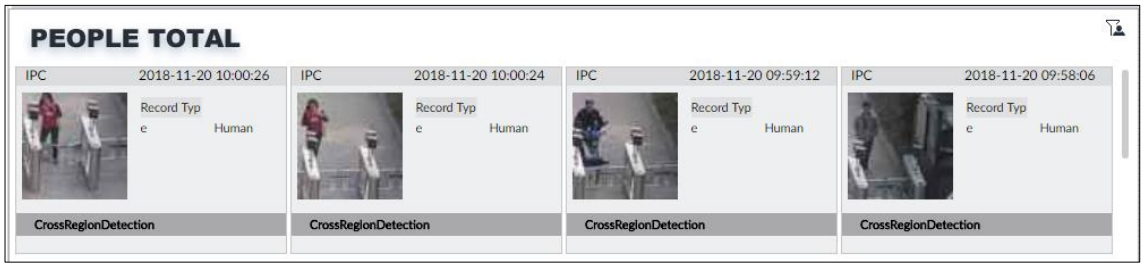
Figure 4-38 Live

Move the mouse to features panel, and the operation icons are displayed. Click or double-click the detected image, so the system starts to play back the recorded videos (10 s before and after the snapshot).

4.6.3.3 Detection Statistics

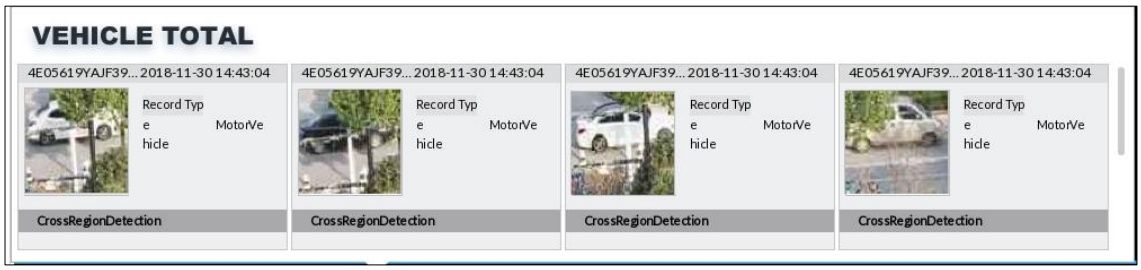
On the **LIVE** interface, click . The **PEOPLE TOTAL** interface is displayed. Click , and then select **IVS**. The people detection records are displayed. See Figure 4-39.

Figure 4-39 People total



Click . The **VEHICLE TOTAL** interface is displayed. Click , and then select **IVS**. The detected vehicles are displayed. See Figure 4-40.

Figure 4-40 Vehicle total



- Point to a picture and click , or double-click the picture, so the system starts playing back video (10 s before and after the snapshot moment).
- Point to a picture and click to export video.

On the **LIVE** interface, click . The **NONMOTOR TOTAL** interface is displayed. Click , and then select **IVS**. The detected non-motor vehicles are displayed.

- Point to a picture and click , or double-click the picture, so the system starts playing back video (10 s before and after the snapshot moment).
- Point to a picture and click to export video.

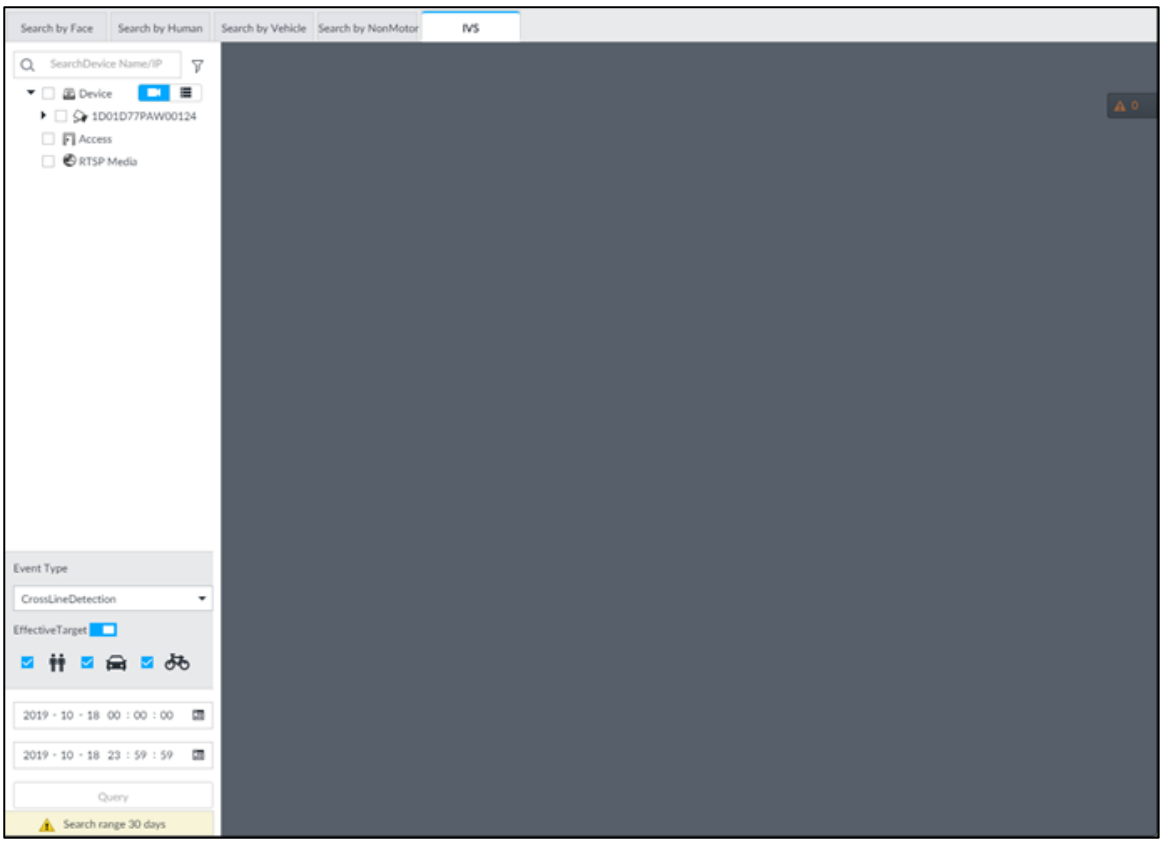
4.6.4 IVS Search

Search for IVS records.

Step 1 Click and then select **AI SEARCH > IVS**.

The **IVS** interface is displayed. See Figure 4-41.

Figure 4-41 IVS

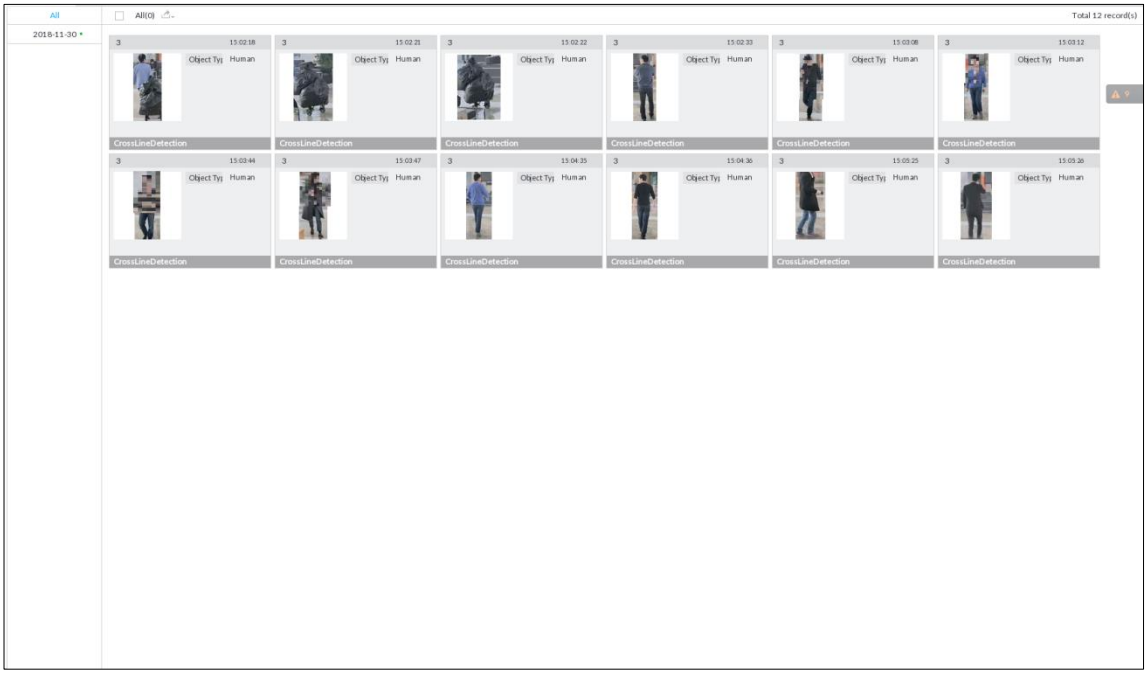


Step 2 Select the remote device, and set event type, effective target and time.

Step 3 Click **Query**.

The search results are displayed in the panel. See Figure 4-42.

Figure 4-42 Search result



Click the panel. The following operation icons are displayed. See Table 4-10.

Table 4-10 More operations

Name	Operation
Select a panel	● Select one by one: Move the mouse onto the panel. Click to select the panel. means it is selected. ● Click **ALL** to select all the panels.
Playback	Click the panel, and click or double-click the panel. The system starts to play back the recorded videos (10 s before and after the snapshot).
Export file	Click the panel and click , or click the panel and click to export images, videos and Excel to designated storage path. After setting alarm linkage snapshot, during exporting images, the system exports detected images and panoramic images at the time of snapshot.

4.7 Vehicle Recognition

Alarm is triggered when vehicle property that meets detection rule is detected.

Make sure that the vehicle recognition parameters of camera are configured. For details, see the user's manual of the camera.

4.7.1 Enabling AI Plan

AI plan needs to be enabled first. For details, see "4.2.1 Enabling AI Plan."

4.7.2 Setting Vehicle Recognition

Set the deployment time of vehicle recognition and alarm linkage event.

Step 1 Click  or  , and then select **EVENT**.

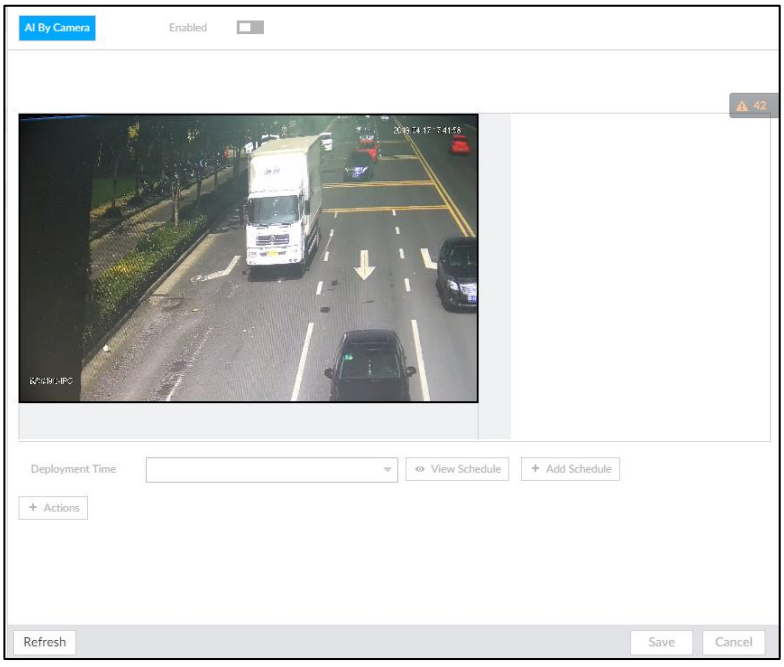
The **EVENT** interface is displayed.

Step 2 Select device from the device tree at the left side.

Step 3 Select **AI Plan > Vehicle Recognition**.

The **Vehicle Recognition** interface is displayed. See Figure 4-43.

Figure 4-43 Vehicle recognition



Step 4 Click the **Deployment Time** drop-down list to select schedule.

EVS links alarm event when alarm is triggered within the defined schedule.

- Click **View Schedule** to view detailed schedule settings.
- If the schedule is not added or the added schedule does not meet actual needs, click **Add Schedule**. For details, see "6.8.3 Schedule."

Step 5 Click **Actions** to set alarm action. For details, see "6.4.1 Alarm Actions."

Step 6 Click **Save**.

4.7.3 Live View of Vehicle Recognition

View vehicle recognition results on the **LIVE** interface.

4.7.3.1 Setting AI Display

Set the display rules of detection results.

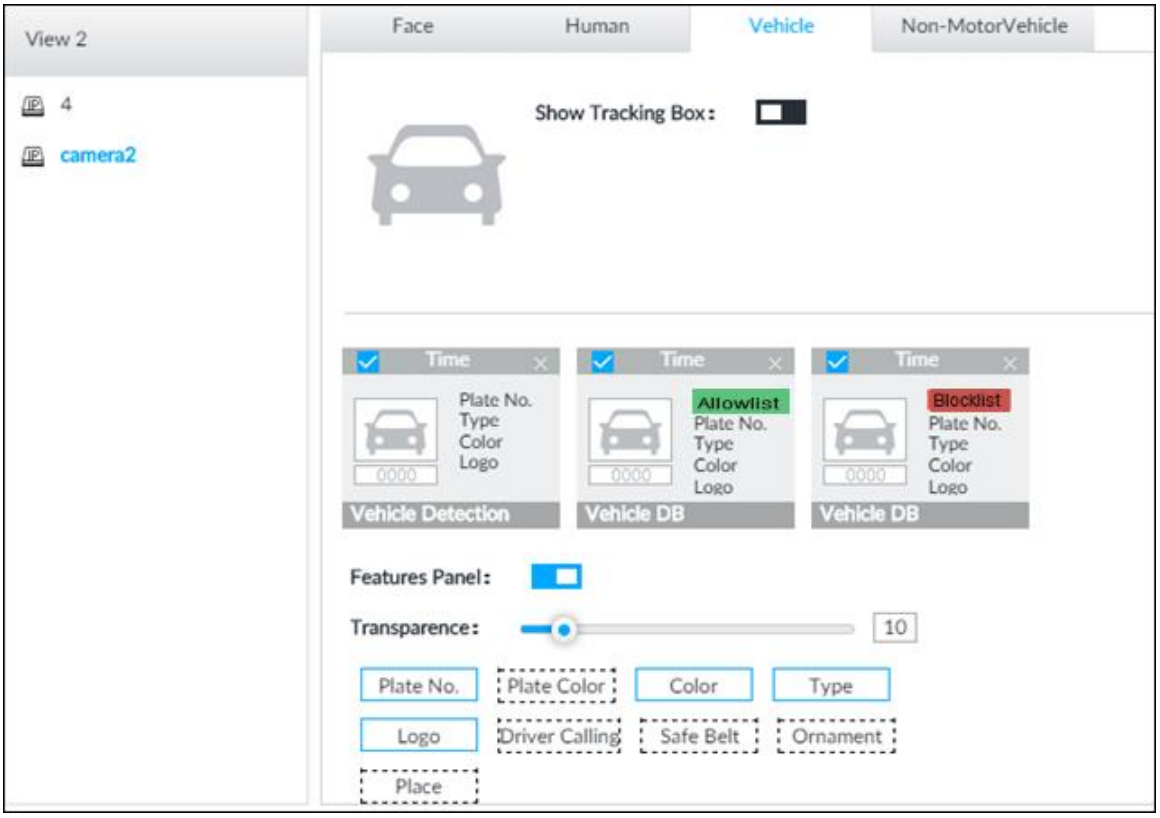
Make sure that view is created before setting AI display. To create view, see "5.1.1 View Management."

Step 1 Select a view from **LIVE > View > View Group**.

Step 2 Click , and then select **Vehicle** tab

The **Vehicle** interface is displayed. See Figure 4-44.

Figure 4-44 Motor vehicle



Step 3 Click next to **Show Tracking Box** to enable tracking box function.

A tracking box is displayed in the video image when target meeting detection rule is detected.

Step 4 Set features panel.

1) Click next to **Features Panel** to enable features panel function.

   Features panel will be displayed at the right side of video image when target with selected features is detected.

2) Select the **Vehicle Detection** panel type by clicking . means the panel is selected.

3) (Optional) Drag to adjust the transparency of panel. The higher the value, the more transparent the panel.

4) (Optional) Select the features to be displayed in the panel.

   - Up to 4 features can be displayed.
   - 4 features are selected by default. To select another feature, click the selected feature to cancel it, and then click the feature to be displayed.

Step 5 Click **OK**.

4.7.3.2 Live View

On the **LIVE** interface, select a view, and the video image of the view is displayed. See Figure 4-45.

- Tracking box is displayed in the video image.
- Features panel is displayed at the right side of the video image.

Figure 4-45 Live

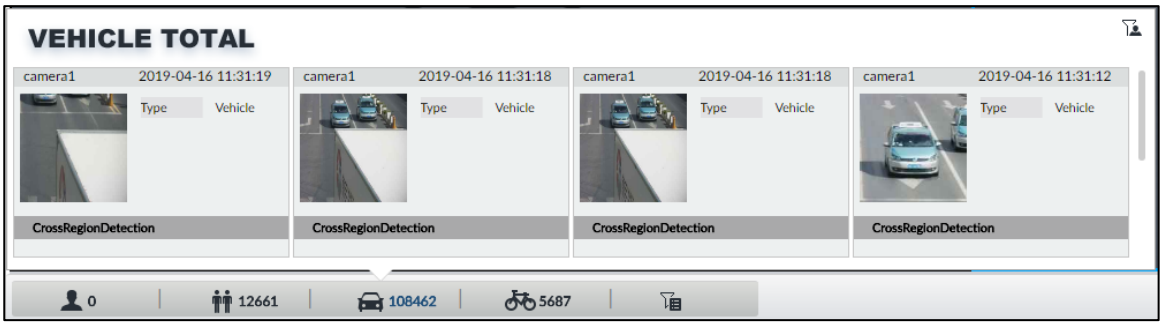
Move the mouse pointer to the features panel, and then you can click  or double-click the vehicle image to play back the video image (10 s before and after the snapshot).

4.7.3.3 Detection Statistics

On the **LIVE** interface, select a view and then click  . The **VEHICLE TOTAL** interface is displayed.

Click  , and then select **Vehicle Detection**. The information of detected vehicles is displayed. See Figure 4-46.

Figure 4-46 Vehicle detection



- Move the mouse pointer to the information panel, and then click  or double-click the picture to play back the video image (10 s before and after the snapshot).

- Move the mouse pointer to the information panel, and then click  to export the video to specified saving path.

4.7.4 Searching for Detection Information

Set event type and vehicle properties, and then search vehicle detection information. For details, see "4.5.4.2 Vehicle Search."

4.8 Crowd Distribution Map

View and monitor people crowd to avoid crowd incidents, for example, stampede.

4.8.1 Enabling AI Plan

Enable the corresponding AI plan. For details, see "4.2.1 Enabling AI Plan."

4.8.2 Configuring Crowd Distribution Map

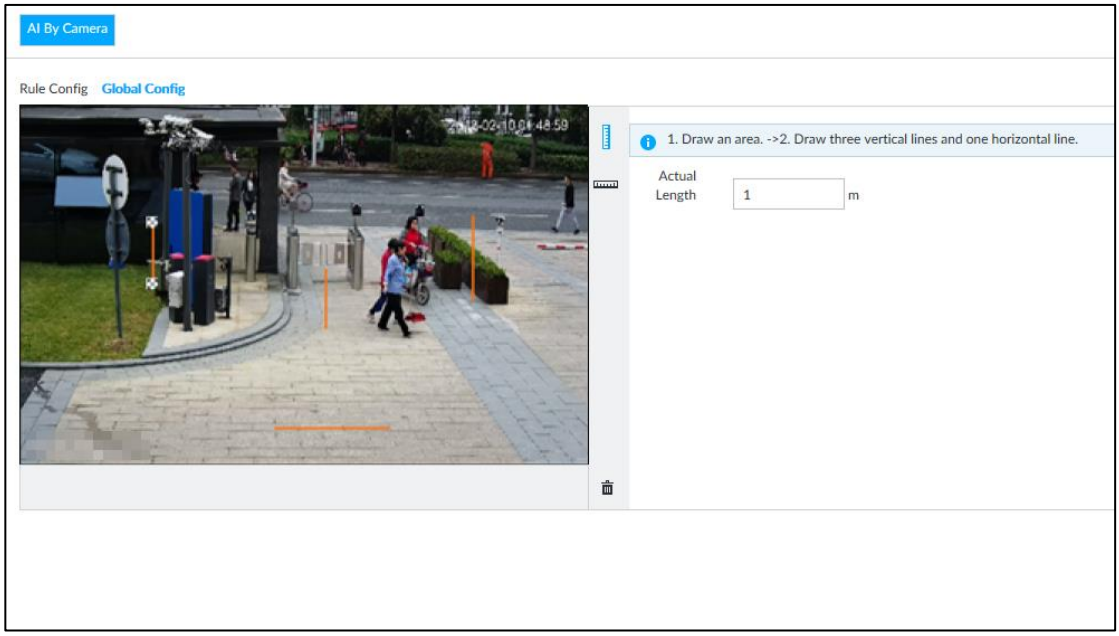
Set crowd distribution alarm rules.

4.8.2.1 Global Configuration

Draw lines on the image to determine the geographical scale of the image.

Step 1 Click  or click  on the configuration interface, and then select **EVENT**.
The **EVENT** interface is displayed.
Step 2 In the device tree, select a camera.
Step 3 Select **AI Plan > Crowd Distribution Map > Global Config**.
The **Global Config** interface is displayed.

Figure 4-47 Global config



Step 4 Draw lines. Draw one horizontal line and three vertical lines.

- Click , draw vertical lines, and then enter their geographical distance values.
- Click , draw a horizontal line, and then enter the geographical distance value.

Step 5 Click **Save**.

4.8.2.2 Rule Configuration

Configure the alarm threshold for crowd monitoring. For example, when the crowd density reaches 8, an alarm is triggered.

Step 1 Click or click on the configuration interface, and then select **EVENT**.

The **EVENT** interface is displayed.

Step 2 In the device tree, select a camera.

Step 3 Select **AI Plan > Crowd Distribution Map > Rule Config**.

The **Rule Config** interface is displayed.

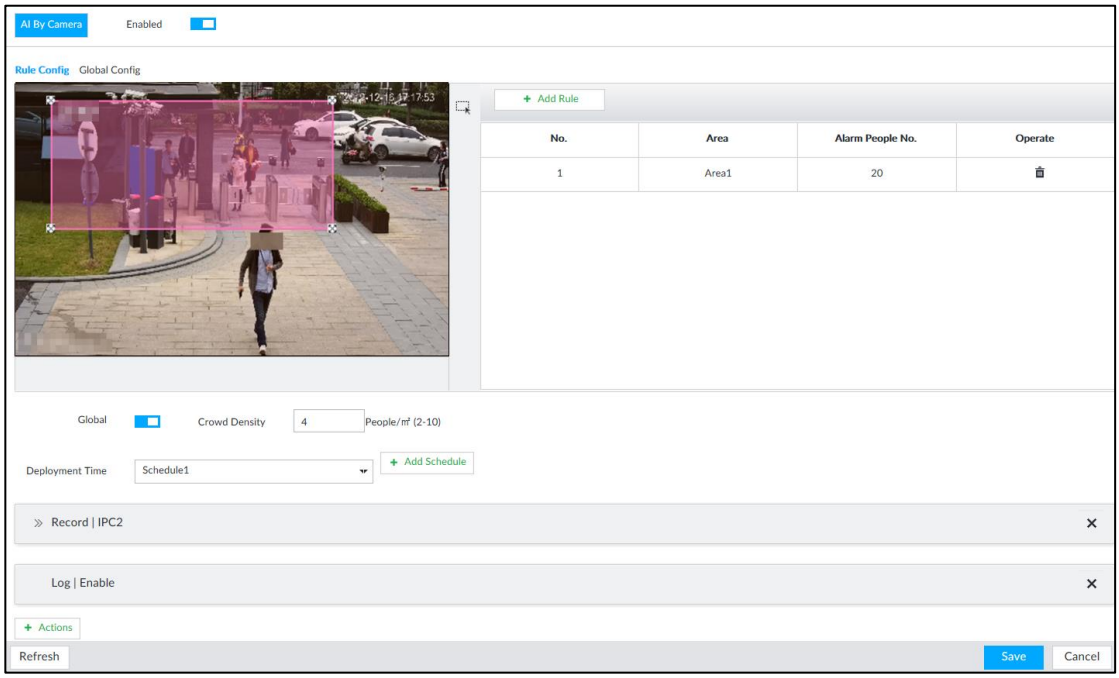
Step 4 Click next to **Enabled** to enable rule configuration.

Step 5 Set detection rules.

- Set regional detection rules.

1) Click **Add Rule**. The following interface is displayed.

Figure 4-48 Add Rules



2) Drag to adjust the size.
3) Configure alarm threshold. Alarm is triggered when the detected people number reaches the threshold.

- Set global alarm.

4) Click , and then drag to adjust the size of the yellow area.
5) Click to enable global detection.
6) Set crowd density. Alarm is triggered when the detected crowd density reaches the threshold.

Step 6 Select a schedule from the **Deployment Time** drop-down list.

The alarm linkage action is triggered only during the scheduled period.

To modify the schedule, click **Add Schedule**.

Step 7 Click **Actions**, and then select an action to be associated to the alarm.

Step 8 Click **Save**.

4.8.3 Live View of Crowd Distribution

On the **LIVE** interface, open a view that contains the crowd distribution detection camera.

The video shows people numbers in the detection areas in real time. The area frame flashes red when there is an alarm in the area.

Figure 4-49 Live view of crowd distribution

- Right-click on the live video, and then select **Crowd Distribution Map > PIP**. A blue section is displayed, and it shows the crowd distribution status inside the current view.
- Right-click on the live video, and then select **Crowd Distribution Map > Global** to switch to the distribution view. The view indicates crowd density and people heads in different colors.

5 General Operations

This chapter introduces general operations such as live view, playback, alarm, AI functions, and IVS.

5.1 Live and Monitor

Click , and then select **LIVE**. The **LIVE** interface is displayed. See Figure 5-1 and Table 5-1.

Move the mouse pointer to the middle of video window and left column. is displayed. Click the icon to hide the left column. See Figure 5-2.

Figure 5-1 Live (1)

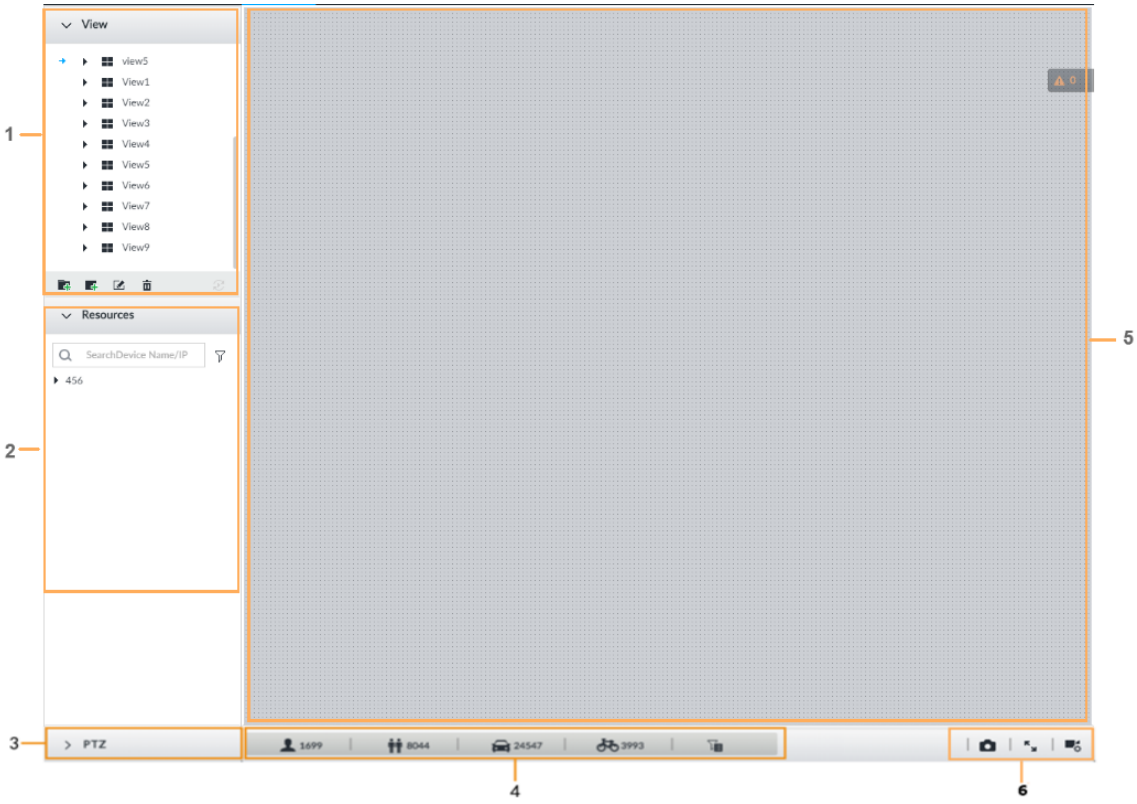


Figure 5-2 Live (2)

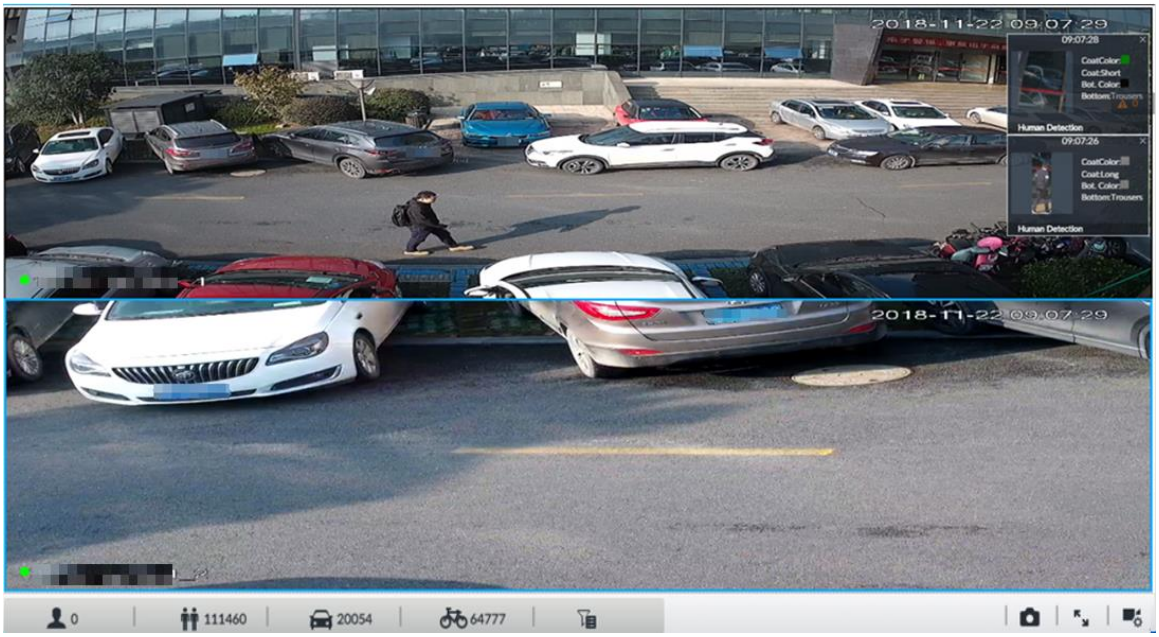


Table 5-1 Live interface description

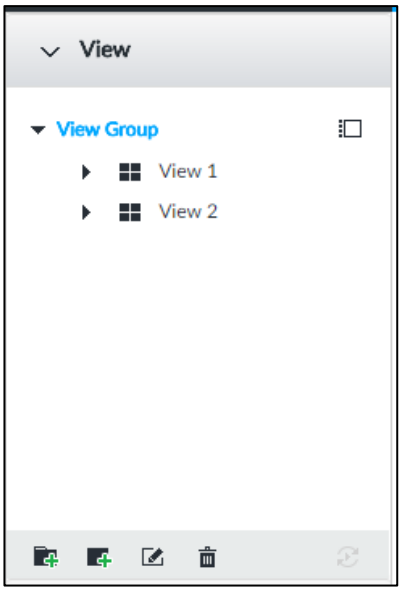
No.	Description
1	View zone. Displays the created view and view group. See "5.1.1 View Management" for detailed information.
2	Resource pool. Displays the added remote device list.
3	PTZ zone. See "5.1.3 PTZ" for detailed information.
4	Smart preview icons. View face statistics, person statistics, IVS statistics and AI display.
5	Video play window. See "5.1.1.3 View Window."
6	● Click to take snapshot. ● Click for full-screen view. ● Click to go to the **VIDEO RECORDING** interface for recording configuration. For details, see "6.9 Storage Management."

5.1.1 View Management

View is composed of video images of several remote devices. Go to the view panel at the top left corner of the **LIVE** interface to view or call the view. See Figure 5-3.

- System has created views by default. Create view or view group under the **View**.
- Double-click a view or drag the view to the play panel on the right side. Device begins playing the real-time video from the remote device.
- Click to select views and its sub-node.

Figure 5-3 View



5.1.1.1 View Group

View group is a group of views. The view group allows you to categorize and manage view. It is easy for you to search and find the view. Create view or view group under the View.

- Device supports maximum 100 view groups.
- The views hierarchy shall not be more than 2. For example, after you create View Group 1 under View, you can create a sub-level View Group 2 under View Group 1. However, you cannot create sub-level group under View Group 2.

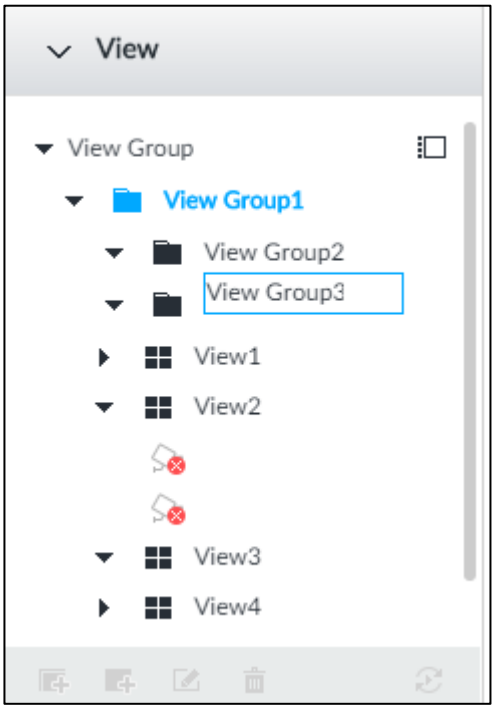
Create view group

Step 1 Follow the steps listed below to create a view group.

- Click **View Group** or a created view group, and then click .
- Right-click **View Group** or a created view group, and then select **Add View Group**.

System creates one view group. See Figure 5-4.

Figure 5-4 Create view group



Step 2 Set view group name.

- The view group name ranges from 1 to 64 characters. It can contain English letters, numbers and special characters.
- View group is to classify different view groups. We recommend the view group name shall be easy to recognize.

Step 3 Click any blank space on the interface.

Device pops up a prompt of success.

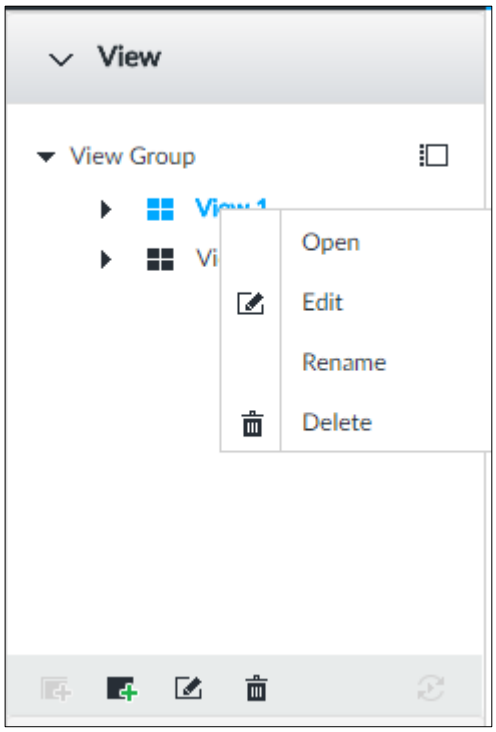
Operation

After creating view group, view group can be renamed or deleted. See Table 5-2 for detailed information.

Table 5-2 View group

Name	Operation
Rename view group	● Select a view group and then click . Set view group name and click any spare panel. ● Right-click view group and select **Rename**. See Figure 5-5. Set view group name and click any spare panel.
Delete View group	Once you delete view group, all views under current view group will be deleted at the same time. Please be careful! ● Select view group and click . ● Right-click view group and then select **Delete**.

Figure 5-5 Rename



5.1.1.2 View

View is a video component of several remote devices. You can drag several remote devices to the same view and when view function is enabled, you can view the real-time video from several remote devices at the same time.

5.1.1.2.1 Creating View

Creating view is to add several associated remote devices to the same View. It is easy to view the real-time video from several remote devices at the same time.

Preparation

Remote device has been added. See "3.4.2 Adding Remote Device" for detailed information.

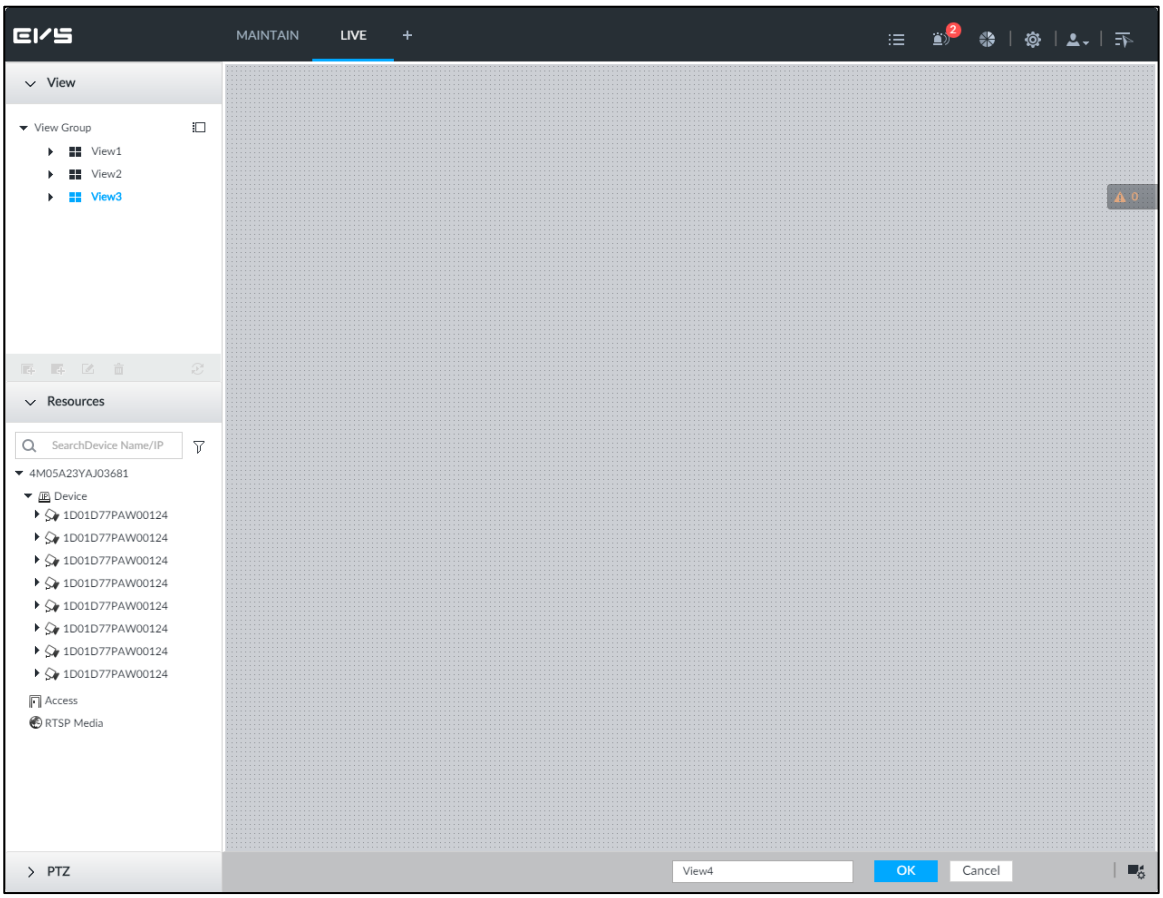
Create View

Step 1 Follow the steps listed below to create view.

- Select a view group, click , and then select **Add view**.
- Right-click a view group, and then select **Add view**.

The **Edit** interface is displayed. See Figure 5-6.

Figure 5-6 Edit view (1)



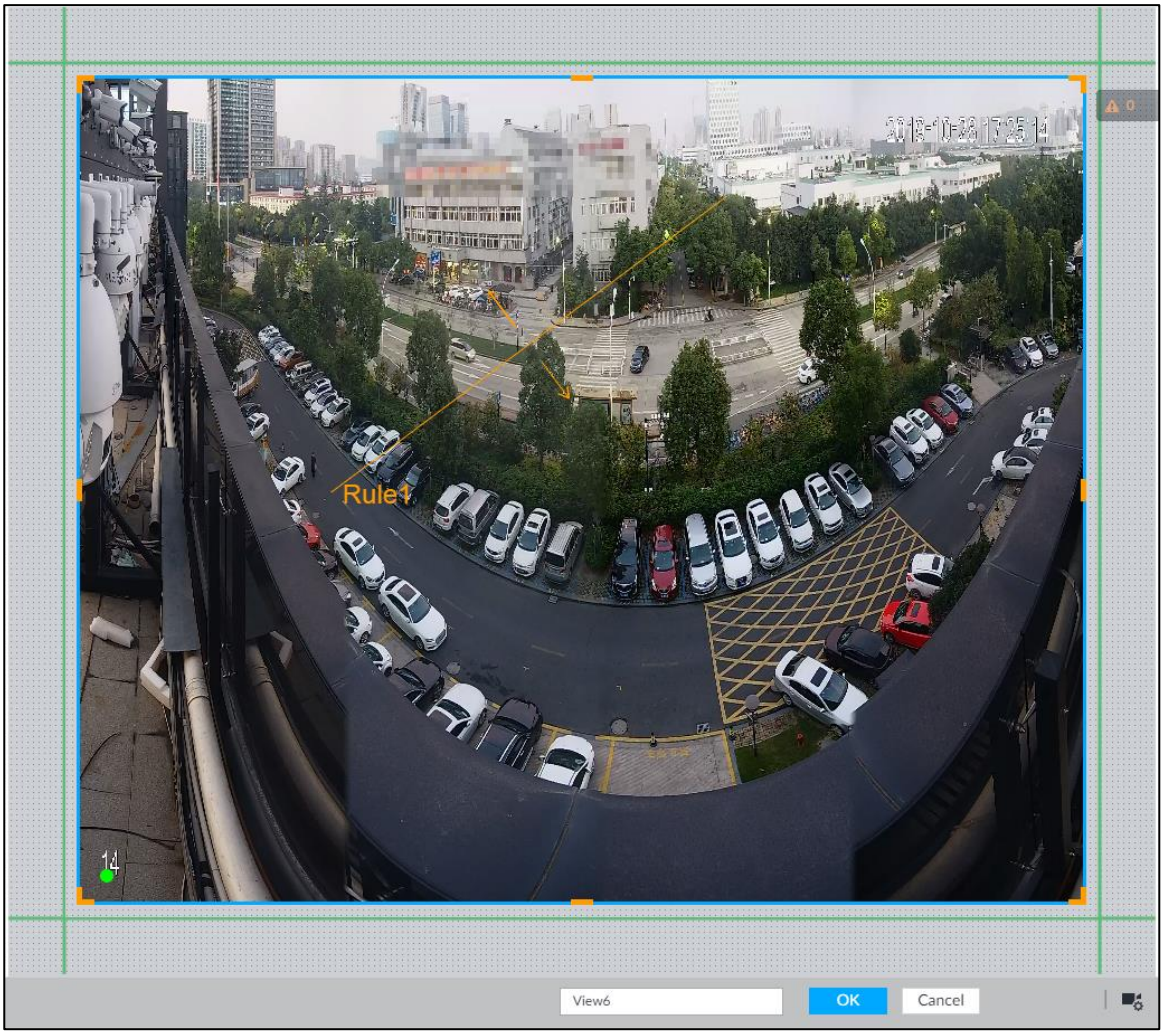
Step 2 Double-click a remote device in resource pool, or drag the remote device to the right panel.

After one remote device is added, layout grid is displayed. See Figure 5-7.

- Each layout grid supports one remote device. If you want to add several remote devices, drag the rest remote device to other idle layout grid.
- If the layout grid has added the remote device, drag another remote device to current grid to replace the original one.
- Move the mouse pointer to the orange panel (such as) of the view window, click the view window, and then drag after you see the arrow icon to adjust view window size.

- Device automatically creates the view grids amount according to the selected remote device amount. Device supports maximum 36 view windows.
- The view window fills in the whole layout grid by default. Right-click to select **Original Scale > ON**, and turn on the **Original Scale**. The device automatically adjusts view window size according to resolution of remote device.
- When adjusting view window position, drag the view window to the layout grid of the green background color. You cannot drag the view window to the grid of red background color.

Figure 5-7 Edit view (2)



Step 3 Set view name.

The view name ranges from 1 to 64 characters. It can contain English letters, number and special character.

Step 4 Click **OK** to save the configuration.

Device pops up a prompt of **Successfully operated**.

Operation

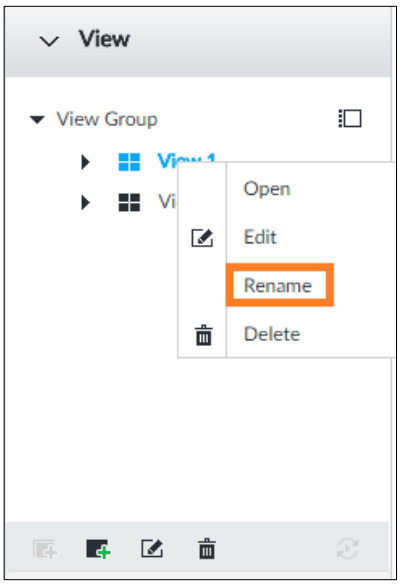
After creating view, view can be edited, enabled, renamed or deleted. See Table 5-3 for detailed information.

Table 5-3 View

Name	Operation
Edit View	Edit remote device in the view, window layout and view name. See "5.1.1.2.2 Editing View" for detailed information.
Enable view	After enabling view, view real-time image of remote device in the view. See "5.1.1.2.3 Enabling view" for detailed information.

Name	Operation
Rename view	• Select a view group and then click . Set view group name and click any spare panel. • Right-click view and select **Rename**. See Figure 5-8. Set view name and click any spare panel.
Delete view	• Delete: Select a view and then click , or right-click view and then select **Delete**. • Batch delete: Click , select views you want to delete and then click .

Figure 5-8 Menu



5.1.1.2.2 Editing View

In edit view mode, you can perform the following functions:

- Add, or delete the remote device on the view.
- Adjust the view grid display.
- Modify view name.

Step 1 Right-click a view and then select **Edit**.

The **Edit** interface is displayed. See Figure 5-9.

Figure 5-9 Edit view

Step 2 Edit view as you require.

- Add remote device: Double-click remote device in the resource pool, or drag the remote device to the free layout grid on the right panel.
- Delete remote device: Move the mouse to window on the right, and click at the top right corner.
- Move window position: Select and hold on a view window, move it to the proper position and release mouse.
- Change window position: Select and hold on one view window and then drag to another view window.
- Change window size: Move your mouse to the orange panel on the window (such as). Hold and drag the view window after you see the arrow icon.
- Modify view name: Set view name on View1.

When adjusting view window position, drag the view window to the layout grid of the green background color. You cannot drag the view window to the grid of red background color.

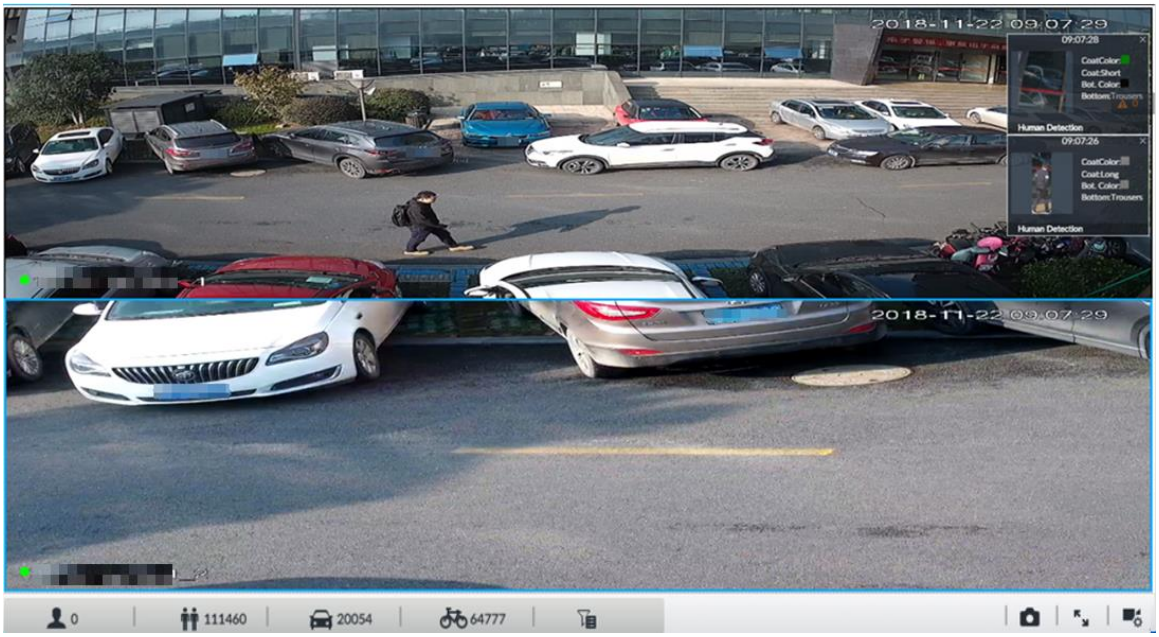
Step 3 Click **OK** to save the configuration.

Device pops up successfully operated.

5.1.1.2.3 Enabling view

Right-click the view and select **Open**, or double-click view. The view window is displayed. See Figure 5-10.

Figure 5-10 View window



When enabling the view, you can change video position, zoom video window. See Table 5-4 for detailed information.

- When adjusting view window position, drag the view window to the layout grid of the green background color. You cannot drag the view window to the grid of red background color.
- Move the mouse to view window. Window task column is displayed to snapshot, enable record and turn off view window. See "5.1.1.3.1 Window Task Column" for detailed information.
- Right-click view window, you can switch bit streams, set digital zoom. See "5.1.1.3.2 Shortcut Menu" for detailed information.

Table 5-4 View function

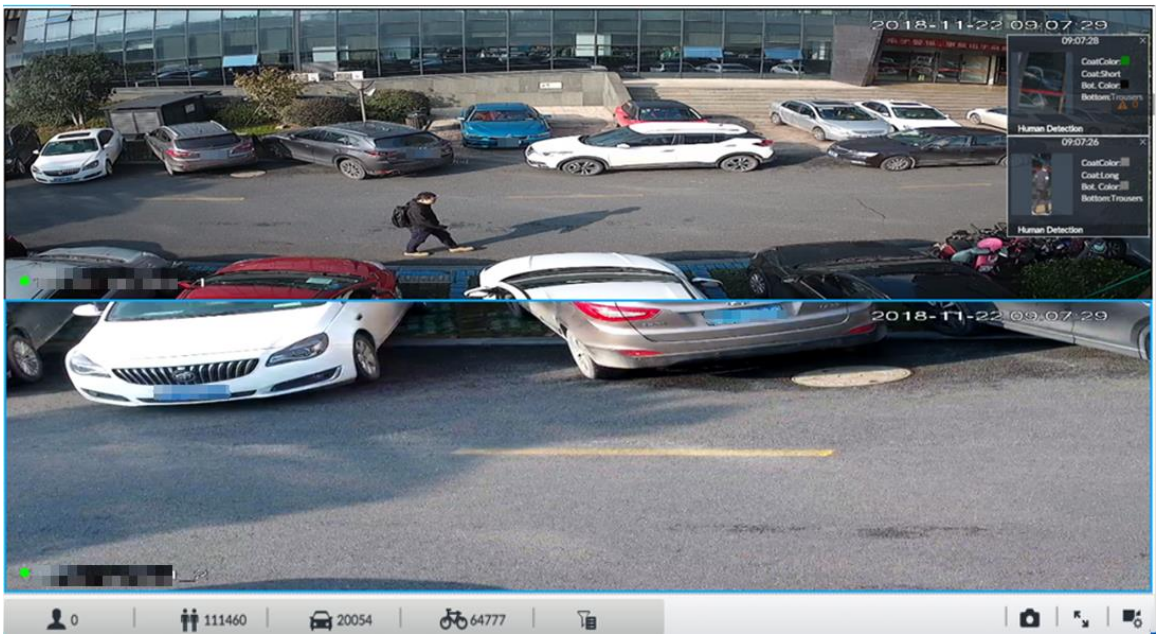
Name	Description
Exchange window position	Press one view window and drag it to another view window to exchange these view window position. The exchanging window position operation is valid only once. Disable and then enable view again, the view window restores original position. If you want to change view window position permanently, go to the view edit mode to set. See "5.1.1.2.2 Editing View" for detailed information.
Zoom in video window	● Once current view window amount is too much (more than 9), click one view window, device displays current view window at the center of the window in the zoom in mode. Click any other blank position, you can view window restores original size. ● Double-click a view window, device displays view window at one window. Double-click view window again or click any blank position, the view window restores original size.

Name	Description
Add view window	In the resource pool, double-click the remote device or drag the remote device to the right panel, you can add remote device to current view. Drag the remote device to the view window to replace the original remote device. The modified view layout is valid only for once if you do not click **OK** button. Close and enable view again, the view layout restores original layout.
Close view window	Move the mouse to one view window, click to close the view window. Close view window, device automatically adjusts view layout according to the rest remote device amount and play panel free space.

5.1.1.3 View Window

Right-click the view, select **Open**, or double-click view. The view window is displayed. See Figure 5-11.

Figure 5-11 View window



5.1.1.3.1 Window Task Column

Move the mouse to view window. The icons are displayed. See Figure 5-12. For details, see Table 5-5.

Figure 5-12 View window

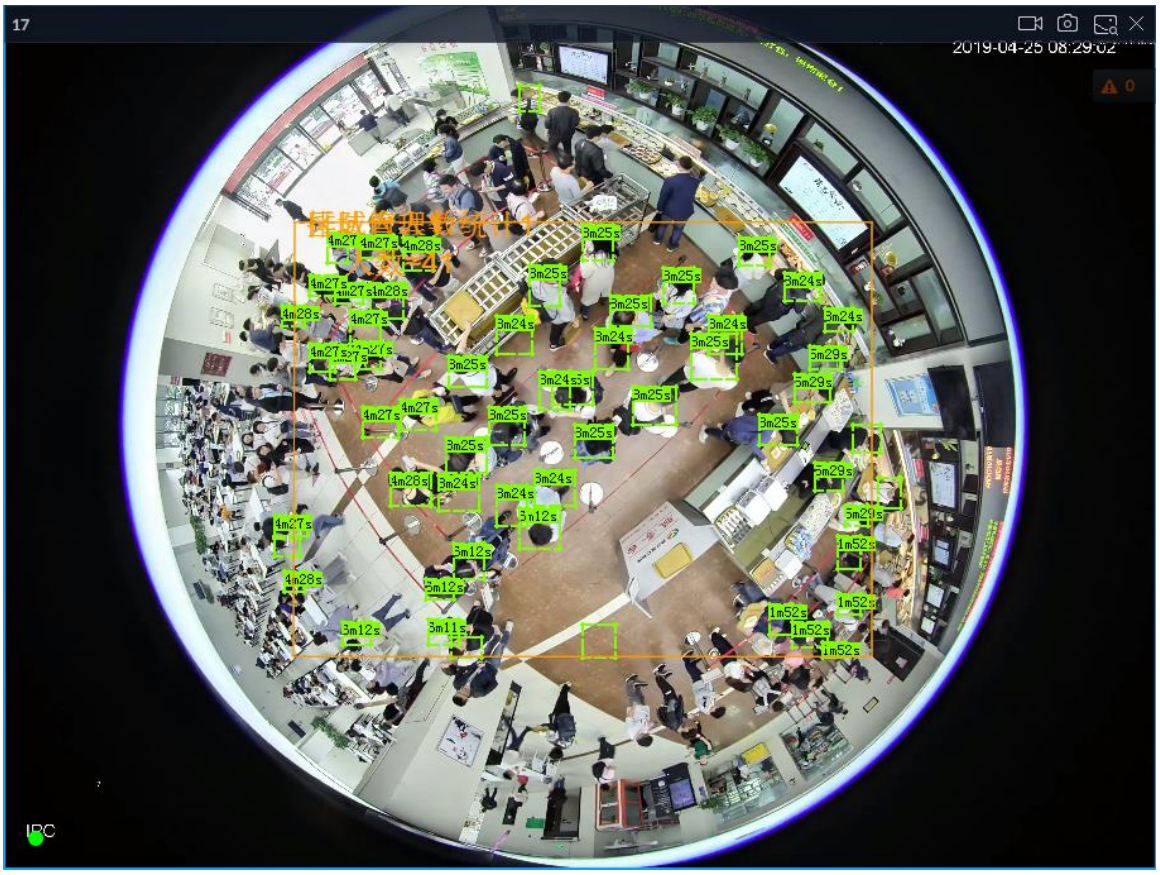


Table 5-5 Window task column

Name	Description
Open Manual Video Recording	Click to start recording manually. Now the icon becomes . Click to stop recording. System stops recording according to the manual record length settings if you do not click again to stop. See "6.2.2.3.5 Storage" for detailed information. At different interfaces, recording storage path varies. ● Local Configurations ◇ When USB storage device is connected, recordings are saved in USB storage device. ◇ Otherwise, the recordings are saved in the device. Query or export manual recording by playback control. See "5.2.1 Playing Back Recorded Video" for detailed information. ● Operate PCAPP. Default storage path of recording is C:/Program Files (x86)/EVS/video. Set storage path. See "6.2.2.3.5 Storage" for detailed information.

Name	Description
Snapshot	Click  to snapshot. At different interfaces, snapshot storage path varies. ● Local Configurations ◇ When USB storage device is connected, snapshots are saved in USB storage device. ◇ Otherwise, the snapshots are saved in the device. Query or export the snapshots by playback control. See "5.2.3 Playing Back Snapshots" for detailed information. ● Operate PCAPP. Default storage path of snapshot is C:/Program Files (x86)/EVS/pictures. Set storage path. See "6.2.2.3.5 Storage" for detailed information.
Close view window	Click  to close view window.

5.1.1.3.2 Shortcut Menu

Right-click the view window. The shortcut menu is displayed. See Figure 5-13. For details, see Table 5-6.

Figure 5-13 Shortcut menu

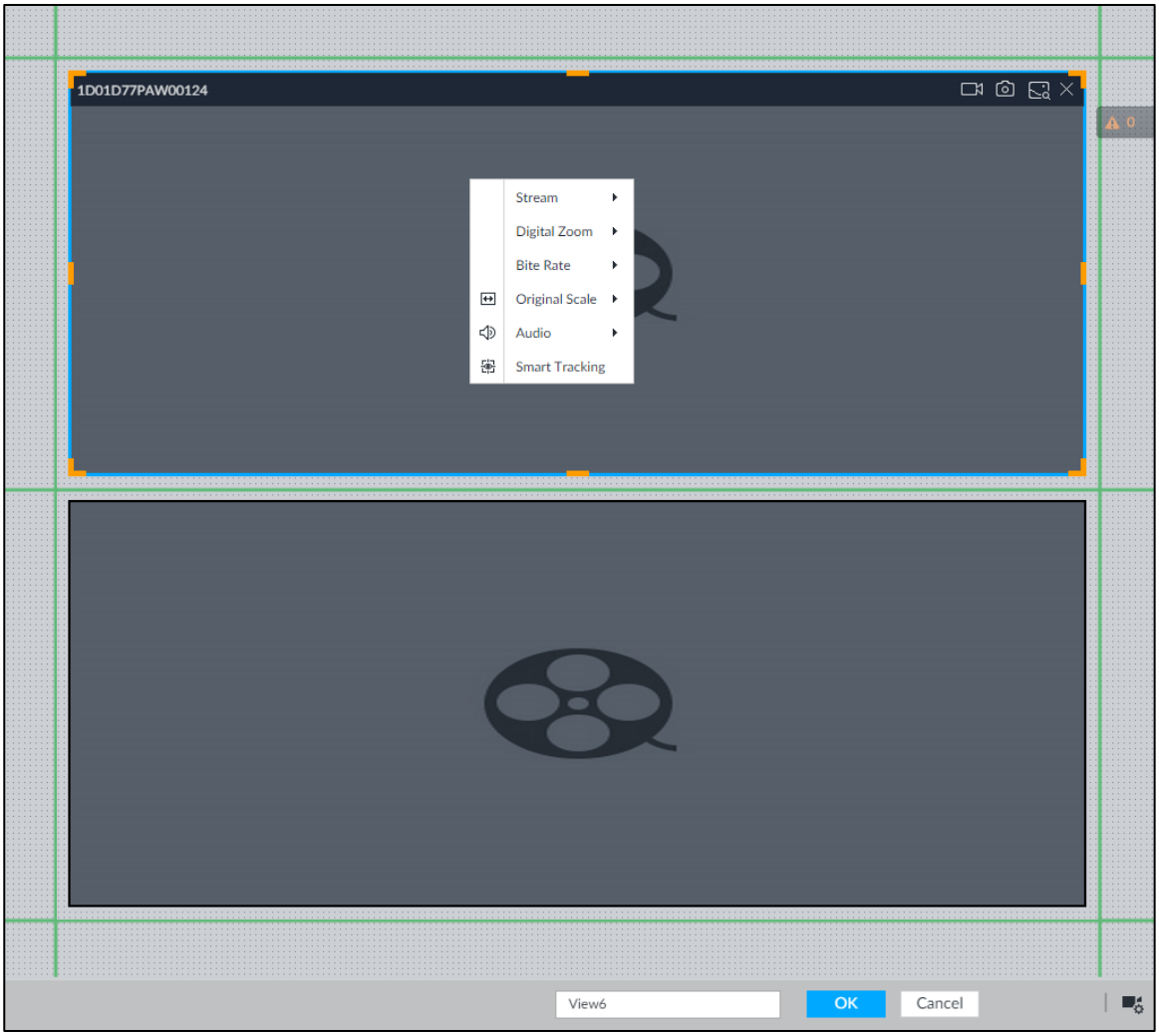
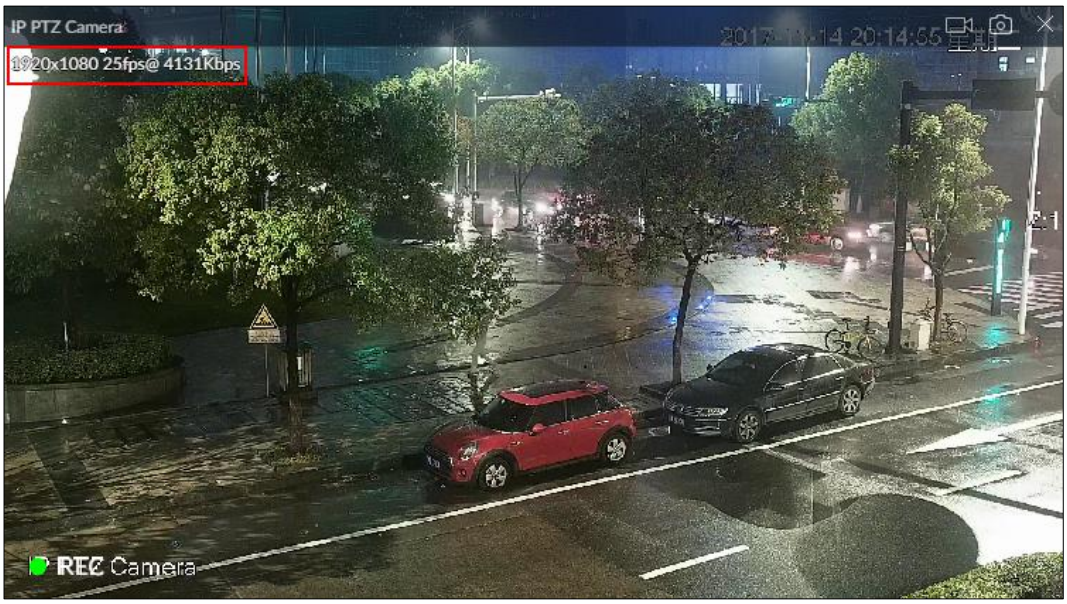


Table 5-6 Shortcut menu

Parameters	Description
Stream	Set current window stream. It includes main stream/sub stream 1/sub stream 2.
Digital zoom	Set digital zoom. Zoom in one part of live image to view details. See "5.1.1.3.3 Digital Zoom" for detailed information.
Bit rate	Displays real-time bit rate on the window or not. See Figure 5-14.
Original Scale	Set video window scale. ● ON: System automatically adjusts video window scale according to the resolution. ● OFF: System automatically adjusts video window scale according to the remote device amount and the free space on the playback panel.
Audio	Set audio output. It includes audio 1, audio 2, mixing and off.
Fisheye Dewarp	Set instalaltion methods and display modes of fisheye cameras. For details, see "5.1.1.3.4 Fisheye Dewarp." This function is only available on fisheye camera.
Smart tracking	Intelligently track targets. For details, see "5.1.1.3.5 Smart Tracking." This function is only available on the multi-sensor panoramic camera + PTZ camera.

Figure 5-14 View window



5.1.1.3.3 Digital Zoom

The digital zoom function allows you to zoom in a specified zone to view the video details.

After enabling view, right-click **Digital Zoom > ON**. Select a zone in view window, and the selected zone will be zoomed in. See Figure 5-15.

- In zoom in status, press any position on the video window and then drag, you can view the zoom in effect of other zones.
- Select a zone you want to zoom in on the video window again, system zooms in the zone at the larger rate.

- Right-click mouse and then select **Digital Zoom > OFF** to cancel zoom in effect. The video restores original effect.

Figure 5-15 Digital zoom:

5.1.1.3.4 Fisheye Dewarp

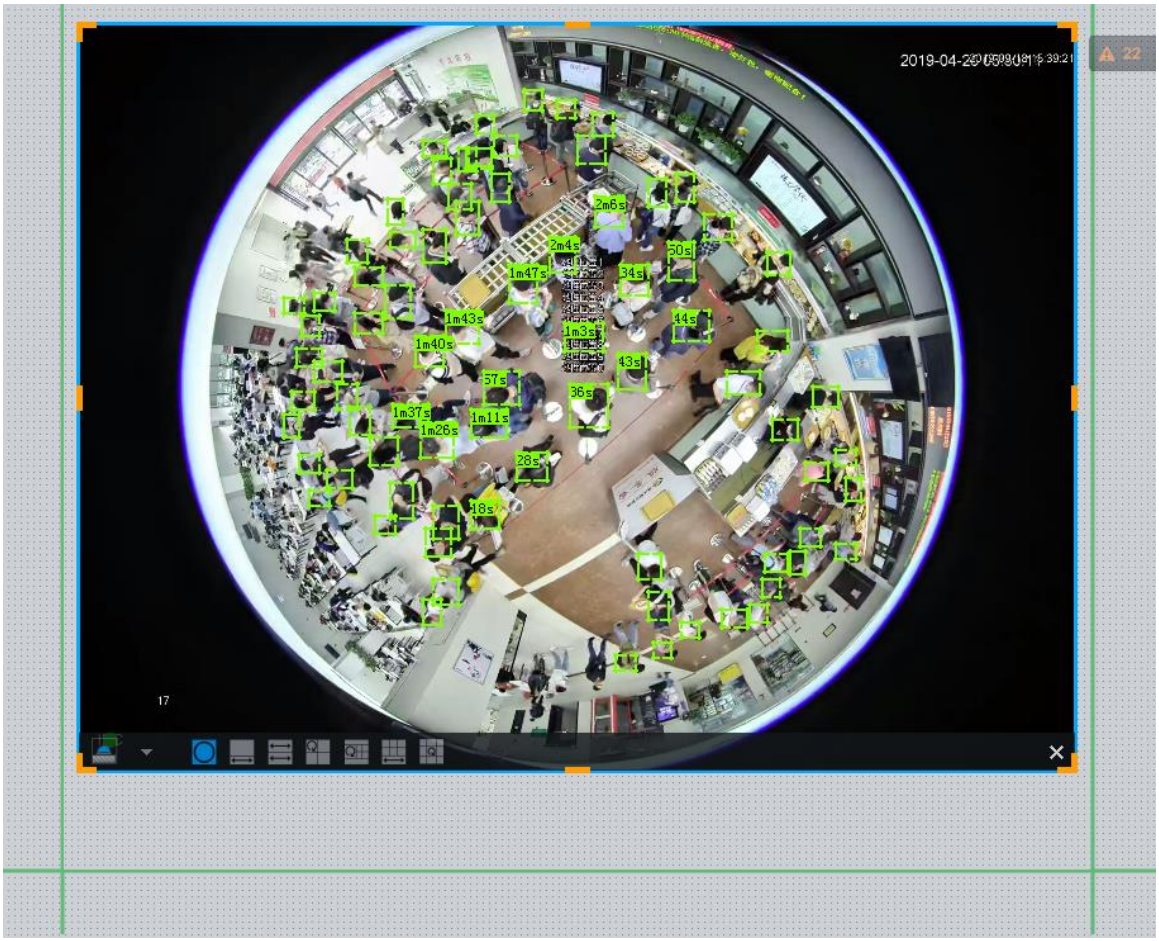
Set the installation method and display mode of fisheye cameras.

- Installation method: Select the installation method according to the actual situation.
- Display mode: Select the display mode of live view.

Step 1 Right-click on the live video, and then select **Fisheye Dewarp**.

The fisheye dewarp interface is displayed. See Figure 5-16.

Figure 5-16 Fisheye dewarp



Step 2 Select an installation method.

- Click  to select ceiling mount.
- Click  to select wall mount.
- Click  to select ground mount.

Step 3 Select a display mode. See Table 5-7.

Table 5-7 Display mode

Installation Method	Display Mode	Description
Ceiling/wall/ground mount		The original fisheye image.
Ceiling/ ground mount	 1P+1	Corrected 360°panoramic image + section images.
	 2P	2 corrected 180°images, which consist the 360° panoramic image.
	 1+3	Original image + 3 section images.
	 1+4	Original image + 4 section images.

Installation Method	Display Mode	Description
	1P+6	Corrected 360°panoramic image + section images.
	1+8	Original image + 8 section images.
Wall mount	1P	Corrected 180° image from left to right.
	1P+3	Corrected 180° image + 3 section images.
	1P+4	Corrected 180° image + 4 section images.
	1P+8	Corrected 180° image + 8 section images.

Step 4 Click **OK**.

5.1.1.3.5 Smart Tracking

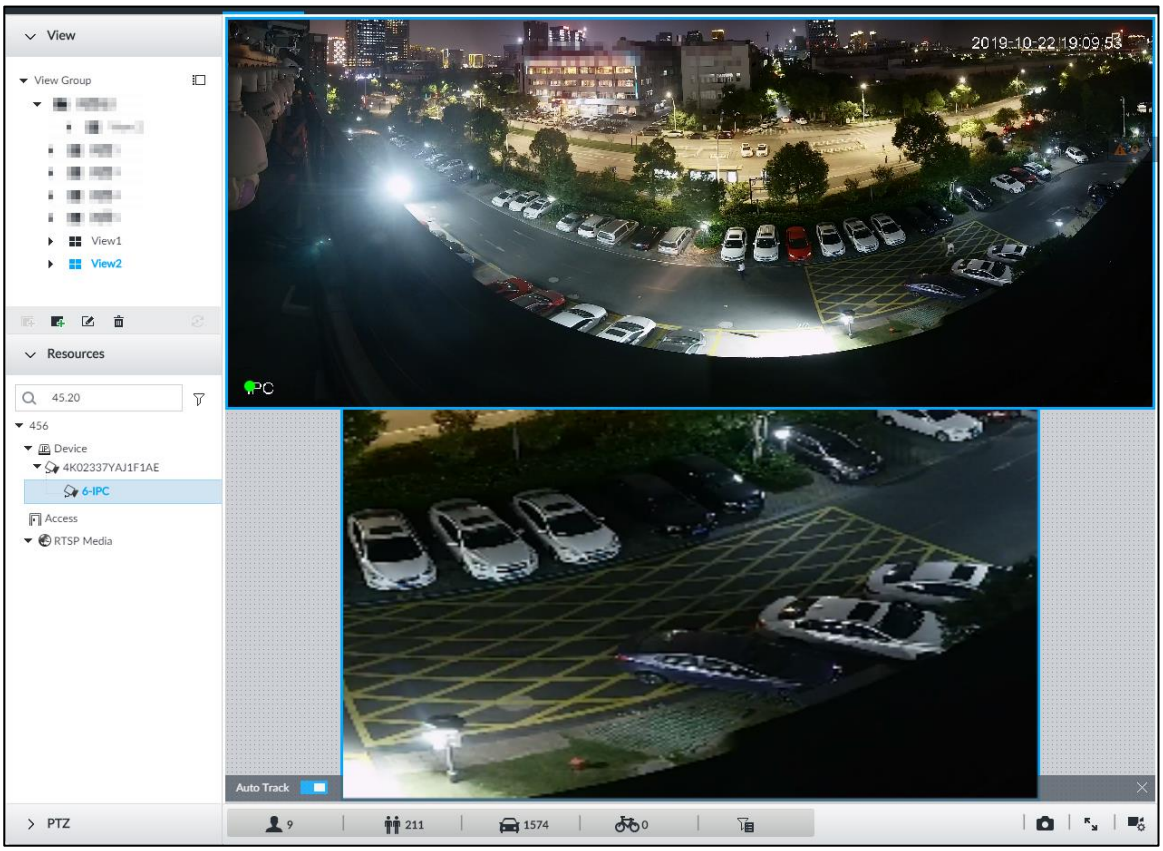
Track targets manually or automatically. This function is only available on the multi-sensor panoramic camera + PTZ camera.

Make sure that the linked tracking function has been enabled.

Step 1 Right-click on the live video, and then select **Smart Tracking > ON**.

The **Smart Tracking** interface is displayed. See Figure 5-17.

Figure 5-17 Smart tracking



Step 2 Select the tracking method.

- Manual positioning: Click a spot or select a zone on the bullet camera video, and then the PTZ camera will automatically rotates there and zoom in.
- Manual tracking: Click or select a target on the bullet camera video, and then the PTZ camera automatically rotates and tracks it.
- Automatic tracking: The tracking action is automatically triggered by alarms in according to the pre-defined rules.

  For automatic tracking, make sure that you have set intrusion detection or tripwire rules for the camera. For details, see "4.6.2 Configuring IVS."

5.1.1.3.6 Thermal

On the **LIVE** interface, a thermal camera has 2 channels: Visible light channel and thermal channel.

Select the thermal channel, point to any position on the live video, and then you can view the real-time temperature of the position. See Figure 5-18.

Figure 5-18 Thermal

5.1.2 Resources Pool

The resource pool displays the added remote device list. The system automatically divides into groups according to device type. See Figure 5-19. See Table 5-8 for detailed information.

Figure 5-19 Resources pool

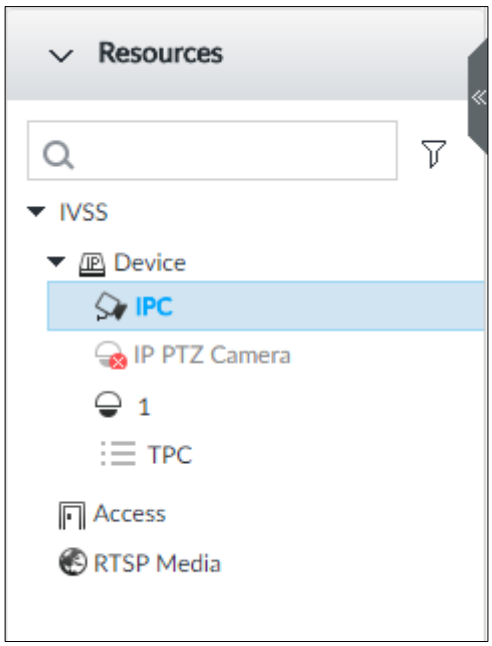


Table 5-8 Resources pool description

Operation	Description
Search device	Input key words at , device displays the corresponding remote devices. Support fuzzy search.
Filter device	Click and then select all, online, offline to filter the disqualified remote device.
View device status	Display remote device status on the resources pool. ● If the remote device name and icon is black, it means the remote device is online. For example, IP PTZ Camera. ● If the remote device name and icon is gray, it means the remote device is offline. For example, IPC. ● If there is an icon before the remote device, it means remote device is abnormal, alarming, and so on. Move the mouse to , to view the detailed information.

Operation	Description
Mouse Operations	• Move the mouse to the remote device name, you can view remote device IP address and port number. • On the device list, click one remote device and then press Ctrl, click other remote device, you can select several remote devices at the same time. • On the device list, select one remote device and then press Shift, click other remote device, select current two remote devices and all remote devices listed between them. • Right-click a remote device to connect to disconnect it. • Double-click remote device or drag the remote device to the view window on the right panel, you can enter edit view interface. Edit the view. See "5.1.1.2.2 Editing View" for detailed information.

5.1.3 PTZ

Control the PTZ, you can move the PTZ at all directions, lens zoom in/zoom out, focus control, and so on. In this way, it can display PTZ at all angles from different positions.

On the **LIVE** interface, PTZ is displayed at the lower-left corner. See Figure 5-20. For details, see Table 5-9.

The following figure for reference only. The grey button means current function is null.

Figure 5-20 PTZ

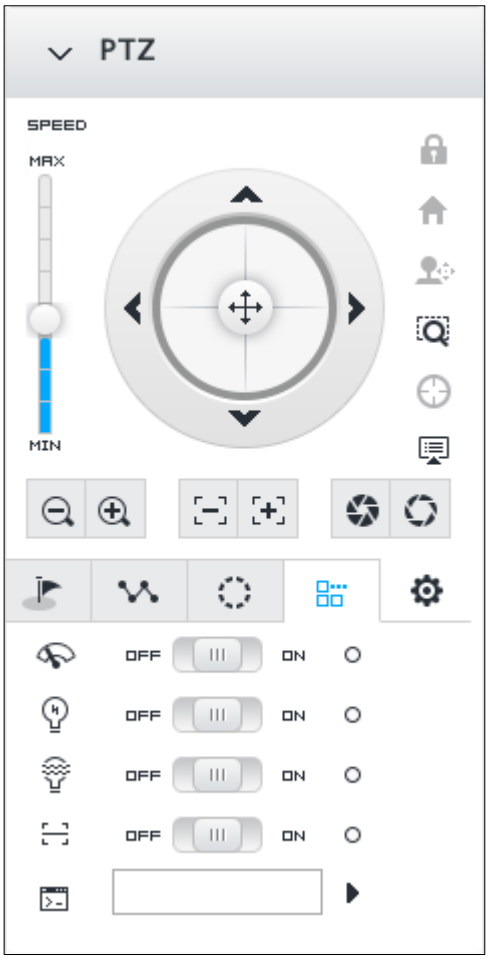


Table 5-9 PTZ Icons description

Signal Words	Description
	Press and hold on , and drag it up and down. Set PTZ speed. The higher the value is, the faster the PTZ speed is.
	Control PTZ movement in the following ways. ● Press and hold on to control PTZ top/bottom/left/right/top left/top right/lower-left/lower-right direction. ● Click , , or to control PTZ top/bottom/left/right direction.
	Click to enable 3D positioning function.
	Click to enter PTZ menu mode. See "5.1.3.2 PTZ Menu Settings" for detailed information.
	Zoom. Click to adjust lens zoom rate of the remote device.
	Focus. Click to adjust lens focus of the remote device.
	Iris. Click it to adjust iris size of the remote device.
	Click to enter PTZ call interface. Go to the remote device to set corresponding PTZ function before you call it. ● Click to enter preset call interface. See "5.1.3.3.1 Calling Preset" for detailed information. ● Click to enter call cruise interface. See "5.1.3.3.2 Calling Cruise" for detailed information. ● Click to enter call pattern interface. See "5.1.3.3.3 Calling Pattern" for detailed information.

5.1.3.2 PTZ Menu Settings

Enable PTZ menu function, device displays PTZ main menu on the view window. The PTZ main menu includes camera settings, PTZ settings, system management, and so on. Use direction button and confirm button to set the remote device.

PTZ menu function is for remote device that supports PTZ function only.

Step 1 Enable view and then select a remote device on the view.

Step 2 On PTZ panel, click .

The OSD menu is displayed on the screen. See Figure 5-21. For details, see Table 5-10.

Figure 5-21 PTZ menu interface

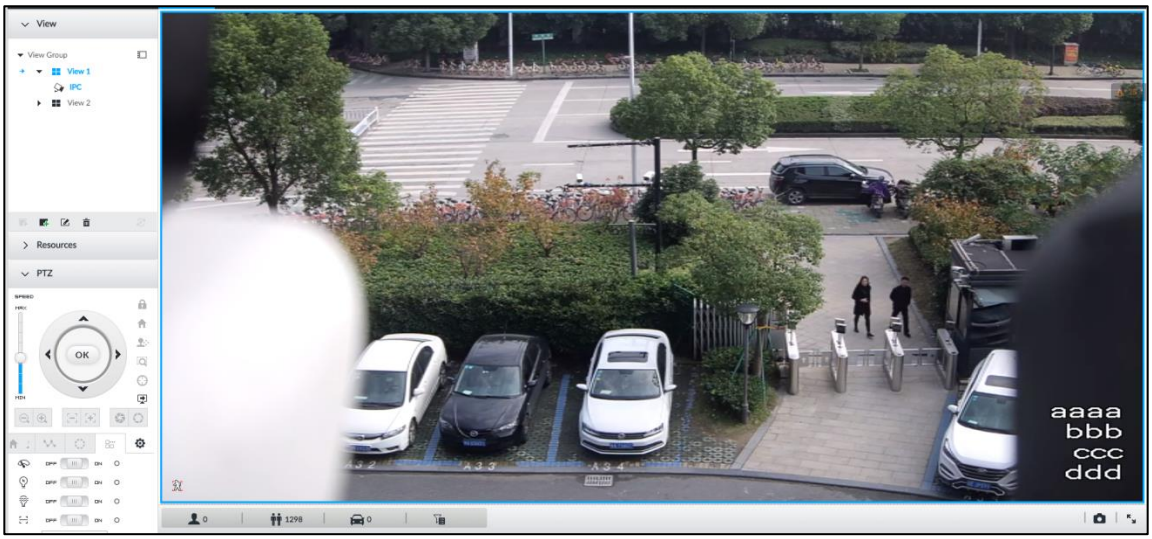


Table 5-10 PTZ menu description

Parameters	Description
Camera	Enter camera interface, you can set remote device image parameters. It includes picture, exposure, backlight, WB, day and night, focus and zoom, defog, default, and so on. (Different series products have different menu items.)
PTZ	Enter PTZ interface, you can set remote device PTZ function. It includes preset, cruise, scan, pattern, rotation, PTZ restart and so on.
System	Enter system interface, you can set remote device PTZ simulator, restore default, manage remote device peripheral device, view remote device software version, PTZ version and so on.
Exit	Exit PTZ menu interface.

Step 3 Set PTZ menu parameters.

Enter PTZ menu interface with PTZ operation icons, and set configuration items.

- Click or to select items.
- Click or to set parameters.
- Click OK to confirm current items.

◇ When there is sub-menu of the item on the main menu, move the mouse to the current item and then click OK, enter sub-menu interface.

◇ Select **Back** and then click OK, return to upper-level menu.

◇ Select Exit and then click OK to exit PTZ menu mode.

Step 4 Click to exit PTZ menu mode.

5.1.3.3 Calling PTZ Functions

Call PTZ function, control PTZ device to implement corresponding operations.

Different PTZ devices support different PTZ functions. See the actual interface for detailed information.

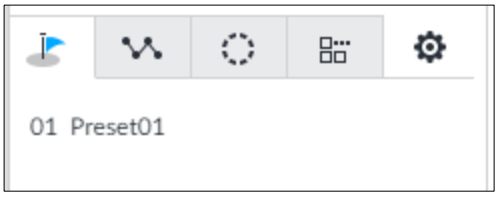
5.1.3.3.1 Calling Presets

Preset function is to save the position information (such as PTZ pan/tilt, focus) to the memory, so that you can quickly call these parameters and adjust the PTZ to the correct position.

Step 1 Click .

The **Preset** interface is displayed. See Figure 5-22.

Figure 5-22 Call preset



Step 2 Move the mouse to the preset name.

The displays at the right side of the preset name.

Step 3 Click .

PTZ device goes to the corresponding position.

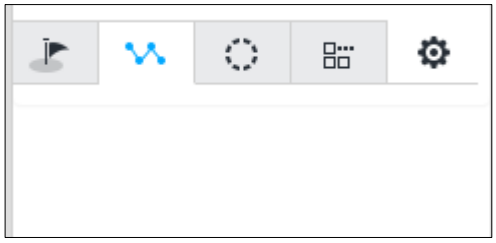
5.1.3.3.2 Calling Cruise

Cruise is to add presets into a routine in a desired order and then set time and stop duration for each position. The dome will begin an auto cruise between these presets.

Step 1 Click .

The call cruise interface is displayed. See Figure 5-23.

Figure 5-23 Call cruise



Step 2 Move the mouse to the cruise name.

The displays at the right side of the cruise name.

Step 3 Click .

PTZ device calls cruise path and goes to the presets at the specified order and interval.

Step 4 Click to stop calling cruise.

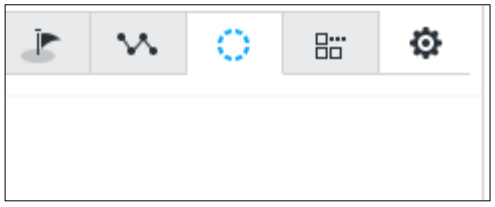
5.1.3.3.3 Calling Patterns

Pattern is to memorize dome operation such as pan, tilt, and zoom to repeat. Start position of record is starting point. You can call it to repeat the previous operation.

Step 1 Click .

The call pattern interface is displayed. See Figure 5-24.

Figure 5-24 Call pattern



Step 2 Move the mouse to the pattern name.

The displays at the right side of the pattern name.

Step 3 Click .

PTZ device calls pattern and move back and forth according to the settings.

Step 4 Click to stop calling pattern.

5.2 Recorded Files

Search or play back the record file or image on the device. At the same time, you can export record file or image to designated storage path.

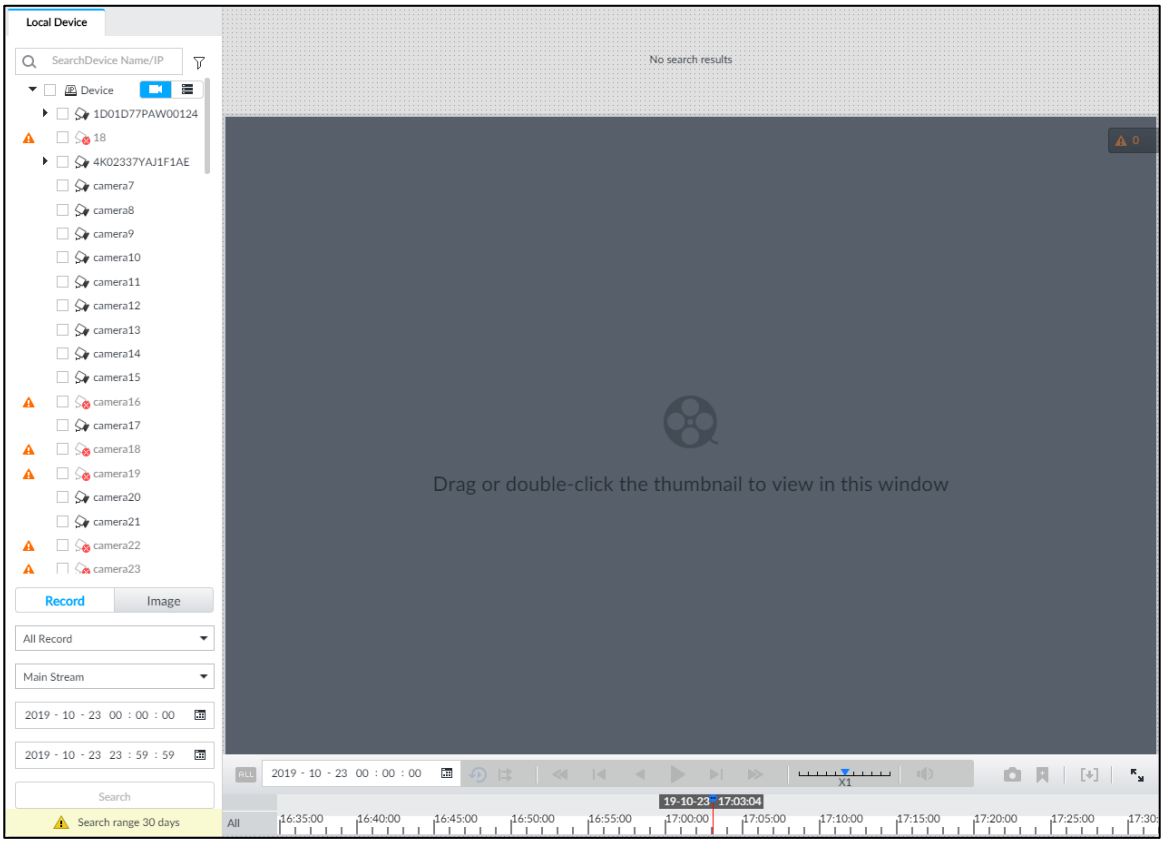
5.2.1 Playing Back Recorded Video

Search and playback record file according to remote device, record type, and record time.

Step 1 Click + and then select **SEARCH**.

The **SEARCH** interface is displayed. See Figure 5-25.

Figure 5-25 Search



Step 2 Select a remote device, and then click **Record** tab.

Click ☰ to display only channels. Click 📹 to display channels and devices.

Step 3 Select a record type from among All Record, Manual Record, Video Detect, and IO Alarm and Thermal.

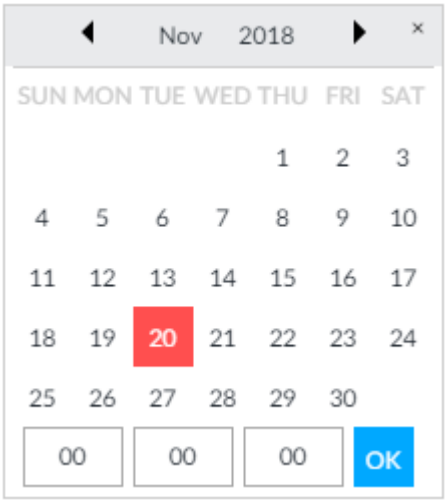
- All record: Search all records.
- Manual record: Search the records that are manually enabled by the user. For manual record, see "5.1.1.3.1 Window Task Column" for detailed information.
- Video detect: Search the records of video detection. For setting of video detection record, see "6.4.3.1 Video Detect."
- IO alarm: Search local alarm linkage records. For setting of local alarm linkage record, see "6.4.3.3 IPC External Alarm."
- Thermal: Search for videos of thermal alarms. For setting of thermal alarm linkage, see "6.4.3.4 Thermal Alarm."

Step 4 Set search time.

- Method 1: Click the date or time on the time column, change time or date value.
- Method 2: Click the date or time on the time column, use the mouse middle button to adjust time or date value.
- Method 3: Click 📅, set date or time on the schedule, click **OK** button. See Figure 5-26.

In the schedule interface, if there is a dot under one date (such as 24), the date has records.

Figure 5-26 Schedule interface

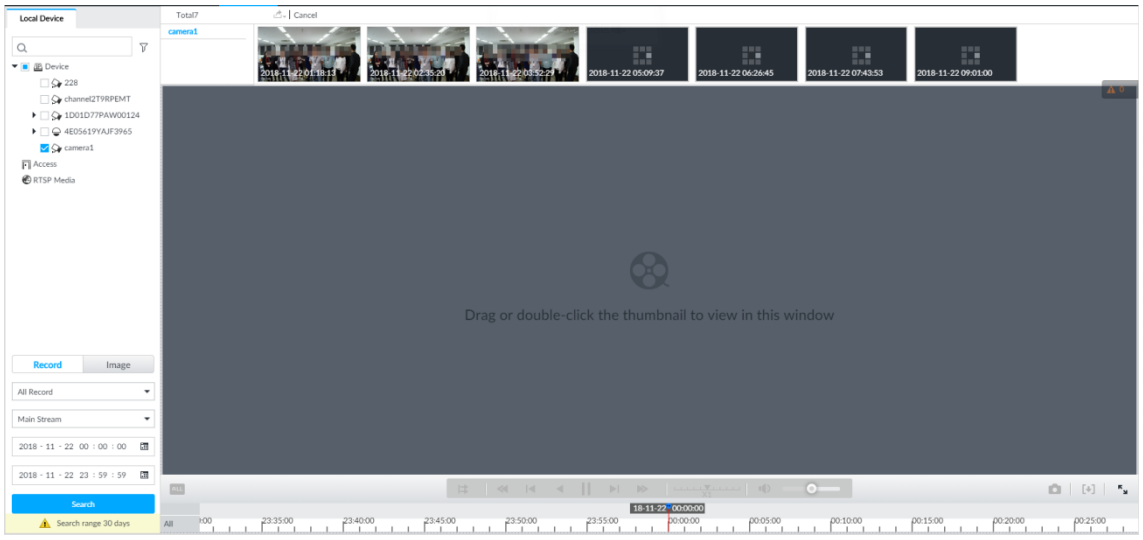


Step 5 Click **Search**.

The record thumbnail is at the top of the remote device, and the time bar displays the record period (green color means there is a record). See Figure 5-27.

- The selected remote device is on the left panel. Click a remote device, and the record file thumbnail is on the right panel.
- Click or to move thumbnail list or hide/display the thumbnail.
- Move the mouse pointer to the thumbnail, you can view remote device name, record start time, and end time of the corresponding record.
- Move the mouse pointer to the thumbnail list. The interface displays . Click the icon to hide the thumbnail list. If the thumbnail list is hidden, click to display the thumbnail list.

Figure 5-27 Search result



Step 6 Drag the thumbnail to the playback window or double-click the thumbnail.

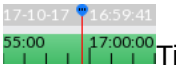
Device begins playing the record. See Figure 5-28. See Table 5-11 for detailed information.

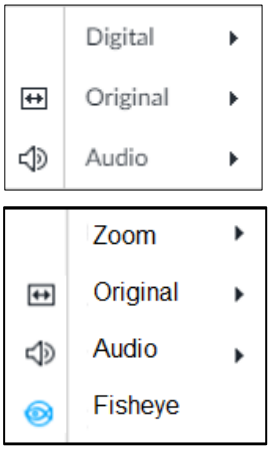
- The playback window amount depends on the thumbnail amount you can drag or select. System supports maximum 16 windows. System automatically adjusts each window size according to the original scale of playback file.
- The thumbnail with ▶ means system is playing record file of current thumbnail.

Figure 5-28 Search

Table 5-11 Search icons description

Signal Words	Description
ALL	Click to synchronize playback mode. You can use the playback control icon to control several windows, such as fast forward/backward at the same time. Click ALL to cancel synchronization operation.
2019 - 09 - 20 00 : 00 : 00	Set a time period. Click to start playing the videos in the set time period.
	Play back several record files at the same time. Click the icon to switch to time synchronization mode. All other windows play the video file of the same time of current window. Click to cancel time synchronization. Click , system enables synchronization operation function. If you want to cancel synchronization, click .
	Click to play back video file at slow speed. The slow speed includes×1/2,×1/4,×1/8, and×1/16. Click the icon once, the playback speed degrades one level.
	Click to switch to frame by frame backward playback. It is only valid in pause mode.

Signal Words	Description
	Click to play backward. Now the icon becomes  . Click  to stop backward play.
	Click to start playback. Now the icon becomes  . Click  to pause playback video.
	Click to switch to frame by frame playback.  It is only valid in pause mode.
	Click to play back at fast speed. The fast speed includes×1,×2,×4,×8, and×16. Click the icon once, the playback speed upgrades one level.
	Displays playback speed. Drag  to the left or right to playback at fast forward or fast backward.
	Click to capture an image.
	Click this icon to tag the current video.
	Click to obtain one part of record, and save it in designated storage path. See "5.2.2 Clipping Recorded Video" for detailed information.
	Click  to mute. The icon becomes  . Click  to unmute.
	Click to play back at full screen.
–	Time bar. Displays record type and record file period. ● There are two record file bars on the time bar. The top bar is to display record time of selected window. The bottom bar is to display record time of all selected remote devices. ● The time bar adopts color to categorize record type. Green=Regular record. Red=Alarm record. Blank=No record. ●  Time scale is to display record file date and time. System automatically adjusts time scale according to the record playback process. ● On the time bar, you can: ◇ Click the time bar and rotate the mouse wheel button to adjust the time accuracy. ◇ Press the time bar and then drag to the left or right to move the time bar to view the hidden record time. ◇ Drag time scale to adjust start time of record playback. ◇ Click or drag the time scale to position where there is a record, system starts playing from the selected time. ◇ Click or drag the time scale to position where there is no record, system stops playing record.

Signal Words	Description
	Shortcut menu: Right-click mouse on the playback window, you can view the shortcut menu. ● Zoom: It is to zoom in a specified zone and view the details. See "5.1.1.3.3 Digital Zoom" for detailed information. ● Original scale: Set view window scale. ◇ ON: System automatically adjusts video window scale according to the video resolution. ◇ OFF: System automatically adjusts video window scale according to the remote device amount and the free space on the playback panel. ● Audio: Set audio output. ● Fisheye: Set the installation method and display mode of fisheye camera. For details, see "5.1.1.3.4 Fisheye Dewarp."
	Move mouse pointer to the playback window, system pops up task column. Click the icon to close the playback window.

5.2.2 Clipping Recorded Video

Clip one part of the recorded video, and save it in designated storage path.

Connect USB device to the system if you are on the local menu to operate.

Step 1 Click  and then select **SEARCH**.

The **SEARCH** interface is displayed.

Step 2 Play video file. See "5.2.1 Playing Back Recorded Video."

The video playback interface is displayed. See Figure 5-29.

Figure 5-29 Playback

Step 3 Click  .

Video clipping frame appears on the time bar. See Figure 5-30.

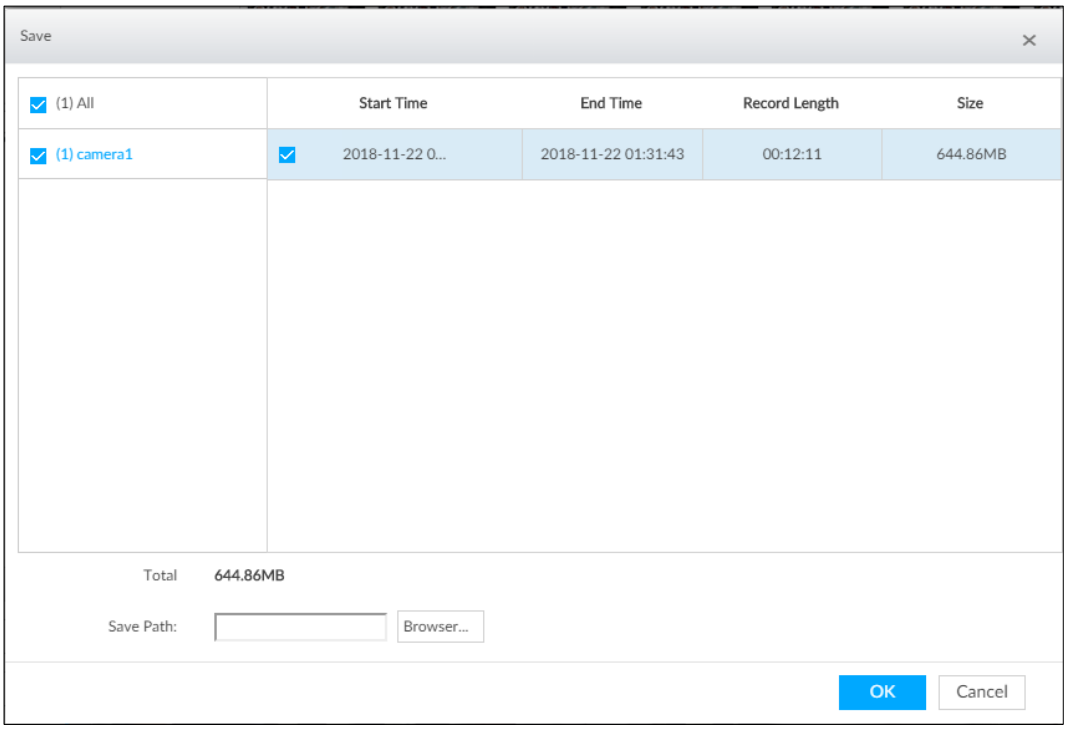
Figure 5-30 Video clipping frame

Step 4 Click the record edit column (the blue column on Figure 5-30) and drag to the left or right, to select start time and end time of clipping.

Step 5 Click Save Immediately.

The **Save** interface is displayed. See Figure 5-31.

Figure 5-31 Save



Step 6 Click **Browser** to select saving path.

Step 7 Click **OK**.

Save the clipping to designated storage path.

5.2.3 Playing Back Snapshots

Search and play back image according to remote device, image type, and snapshot time.

Step 1 Click  and then select **SEARCH**.

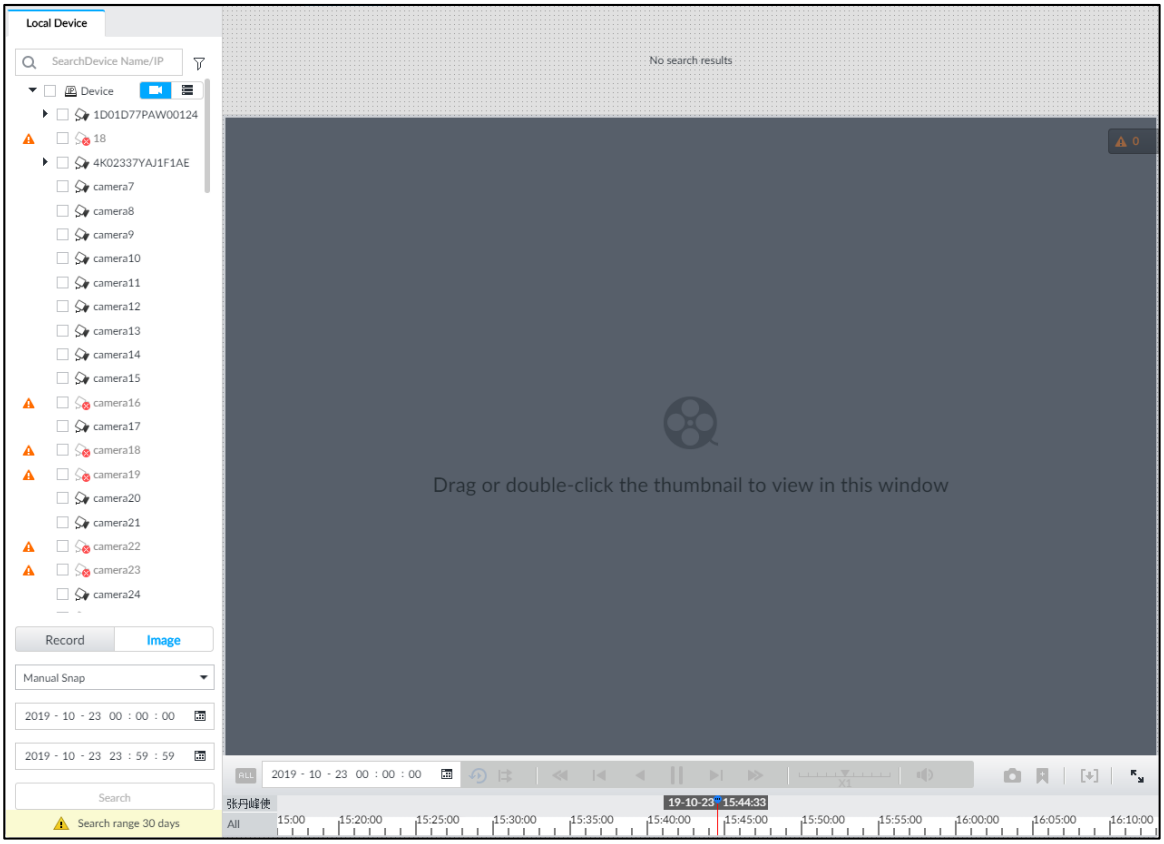
The **SEARCH** interface is displayed.

Step 2 Select a remote device, and then click **Image**.

The **SEARCH** interface is displayed. See Figure 5-32.

System supports maximum 1 remote device.

Figure 5-32 Image playback (1)



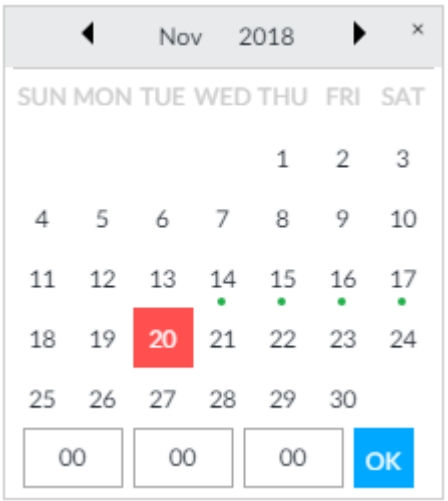
Step 3 Select image type, including manual snap and video detect.

Step 4 Set search time.

- Method 1: Click the date or time on the time column, change time or date value.
- Method 2: Click the date or time on the time column, use the mouse wheel to adjust time or date value.
- Method 3: Click , set date or time on the schedule, click **OK** button. See Figure 5-33.

  In the schedule interface, if there is a dot under one date (such as 24), the date has records.

Figure 5-33 Schedule interface



Step 5 Click **Search**.

System displays searched image thumbnail. See Figure 5-34.

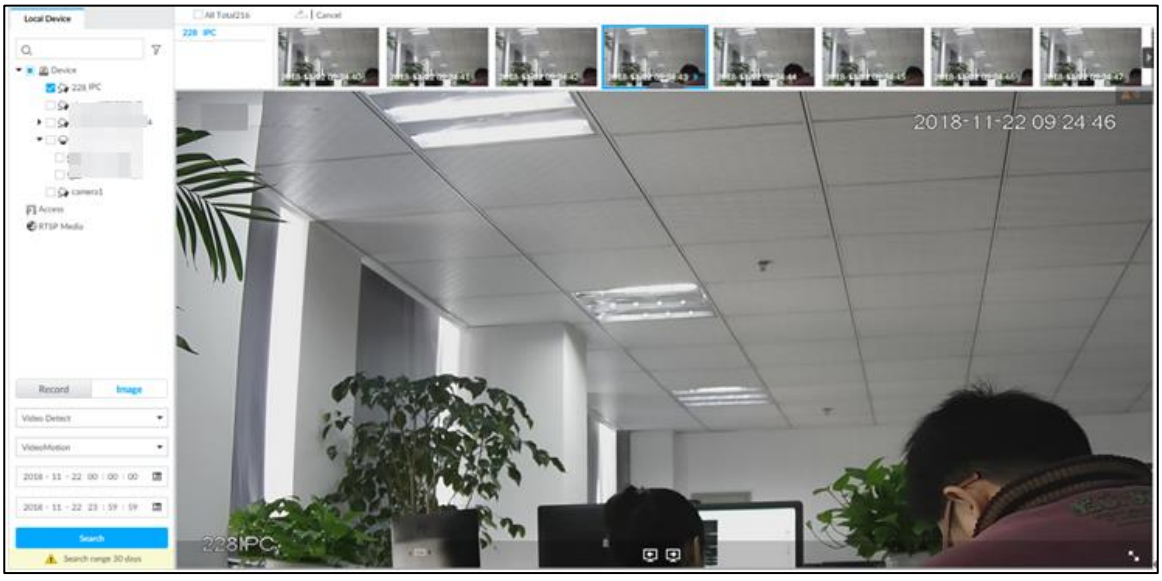
Figure 5-34 Image thumbnail

- The selected remote device is on the left panel. Click a remote device, and the image thumbnail is on the right panel.
- Click or to move thumbnail list, and display the hidden thumbnail.
- Move the mouse pointer to the thumbnail, you can view remote device name, and snapshot time of the corresponding thumbnail.
- Move the mouse pointer to the thumbnail list. The interface displays . Click the icon to hide the thumbnail list. If the thumbnail list is hidden, click to display the thumbnail list.

Step 6 Drag the thumbnail to the playback window or double-click the thumbnail.

Device begins playing the image. See Figure 5-35. See Table 5-12 for detailed information.

Figure 5-35 Image playback (2)



Move the mouse pointer to the playback window, you can see the following icons.

Table 5-12 Icons

Icon	Description
	Click to switch to the previous image or the next image.
	Switch to the previous or next image or image group. ● When playing one image, click the icon to go to the previous image or the next image. ● When playing several images at the same time, click the icon to go to the previous group or the next group.

Icon	Description
	Click to display at full screen. Click again to cancel full screen.

5.2.4 Exporting File

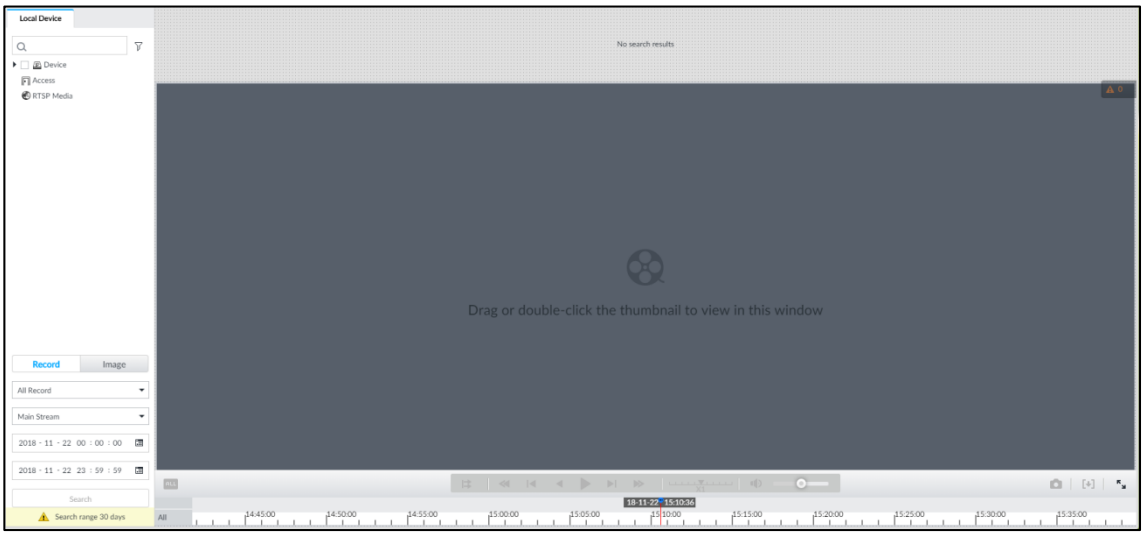
Export record file or image to the designated storage path.

- The default record file mode is .dav and the image file mode is .jpg.
- Connect USB device to the system if you are on the local menu to operate.

Step 1 Click  and then select **SEARCH**.

The **SEARCH** interface is displayed. See Figure 5-36.

Figure 5-36 Search (1)

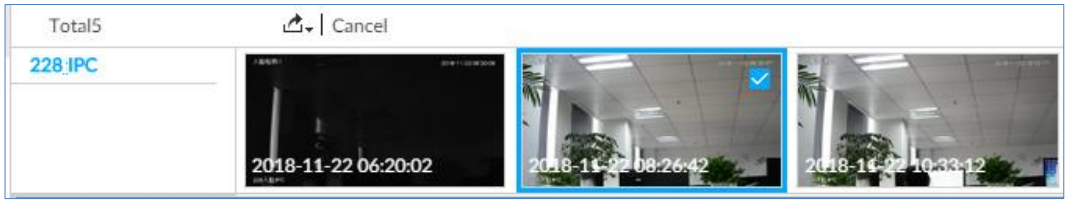


Step 2 Search record file or image.

1) Click **Record** or **Image** tab.
2) Select a remote device and then set search criteria.
3) Click **Query**.

System displays searched record or image thumbnail. See Figure 5-37.

Figure 5-37 Thumbnail



Step 3 Select the record file or image you want to export.

- Move the mouse pointer to the thumbnail and then click  to select the thumbnail.  means checked.
- Click **Cancel** to cancel all record files or images.

Step 4 Select file storage path.

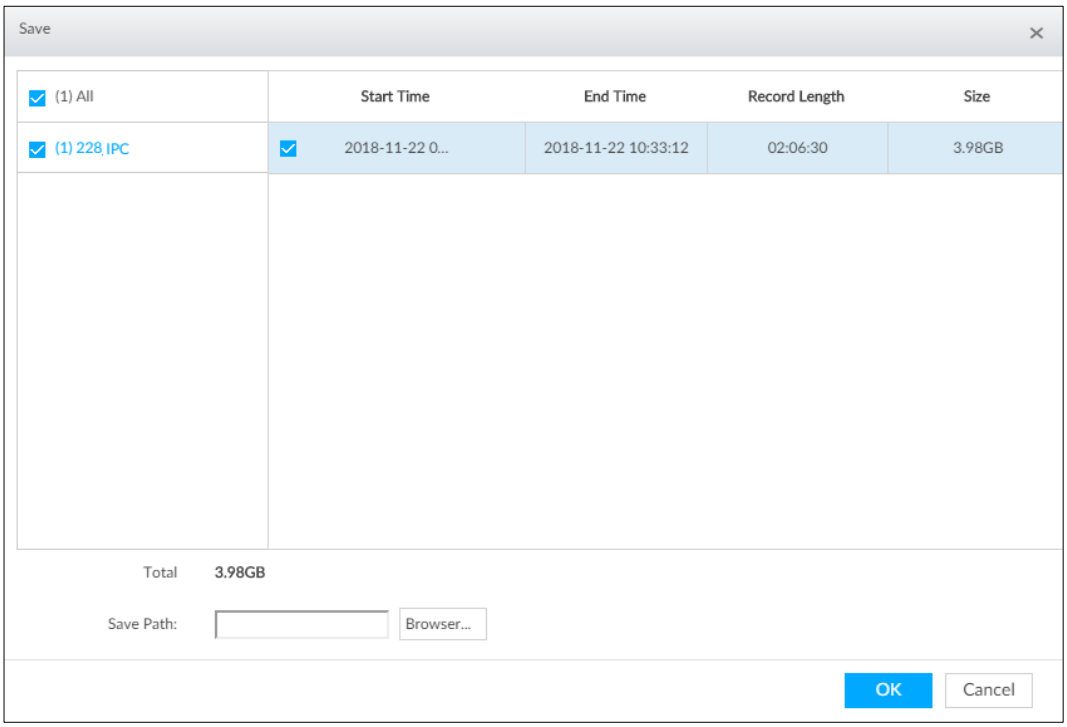
1) Click  and then select **Export record** or **Export image**.

The following steps are to export video file. See the actual interface for detailed information.

2) Click **OK**.

The **Save** interface is displayed. See Figure 5-38.

Figure 5-38 Save



3) Click **Browser** to select saving path.

For local menu operation, after you set storage path, the **Save** interface displays **Format** button. Click **Format** button to clear all data on the USB storage device. The formatting operation will clear all data. Be cautious.

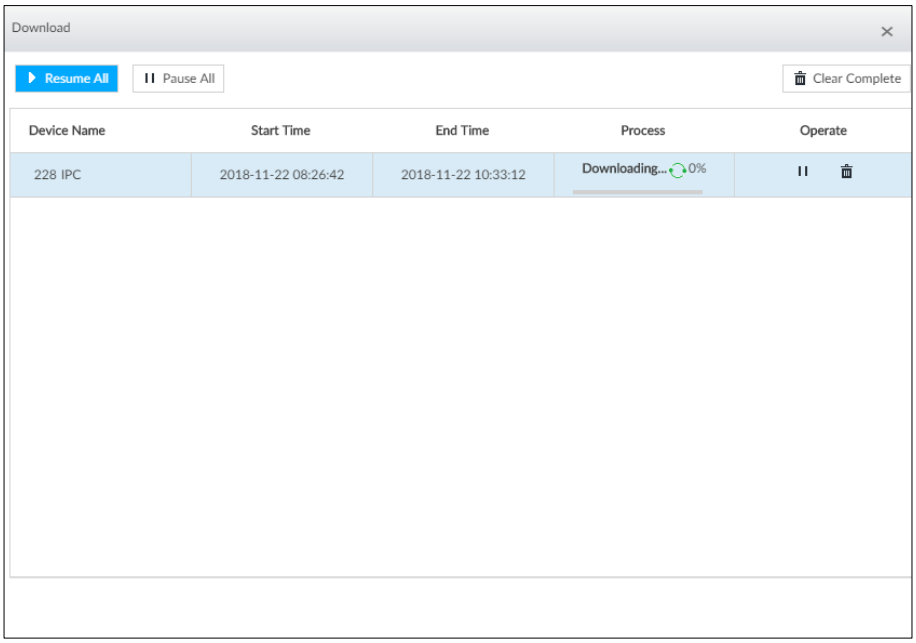
4) Click **OK**.

Device goes back to **Save** interface.

Step 5 Click **OK**.

The system starts to export files. The file downloading interface is displayed. See Figure 5-39.

Figure 5-39 Download



- Click **Pause all** to pause all download tasks. Click **Start all** to resume download tasks.
- Click **Clear completed columns** to delete all downloaded tasks.
- Click of the corresponding task to pause download task. Click to resume download.
- Click of the corresponding task to delete download task.

5.2.5 Video Tag

Tag specific video segments or pictures for the ease of search. For details about viewing tagged files, see "7.1.1Video Tag Management."

Step 1 Click , and then select **SEARCH**.

The **SEARCH** interface is displayed. See Figure 5-36.

Step 2 Search for pictures or videos.

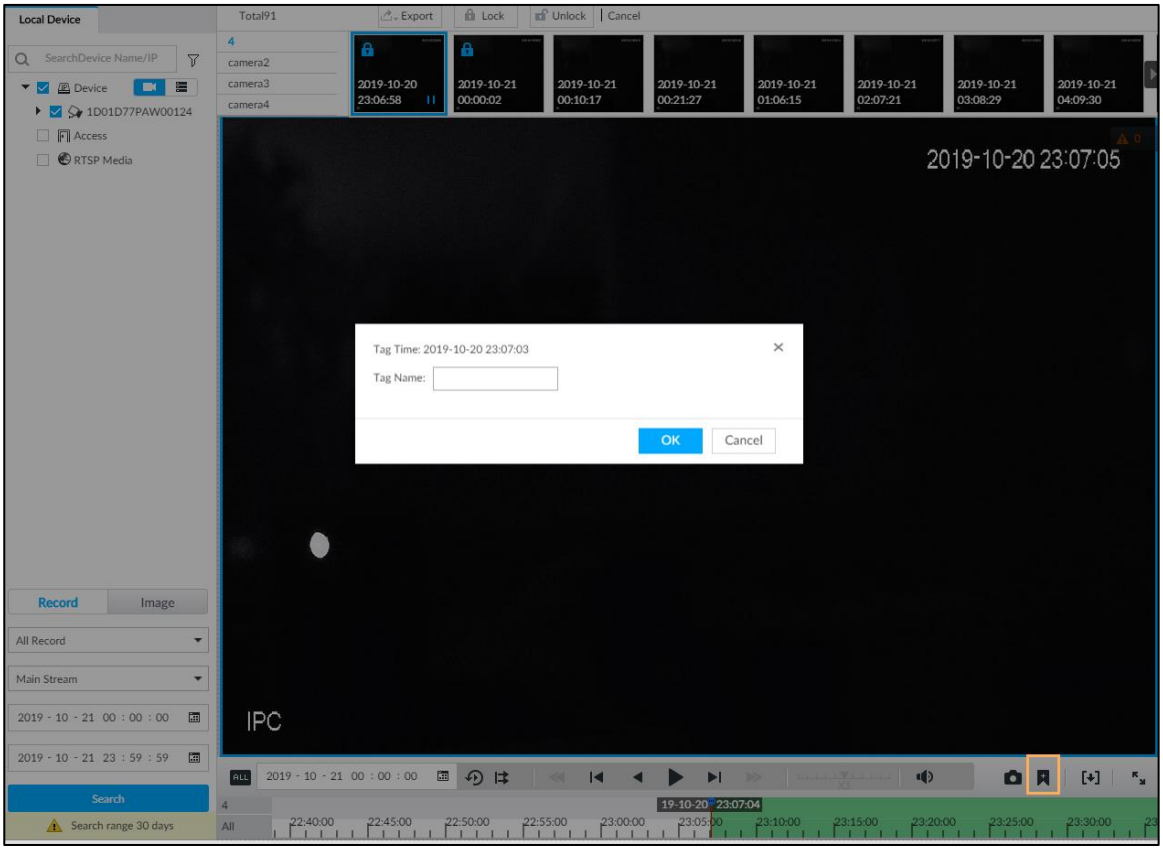
1) Click the **Record** or **Image** tab.
2) Select a camera, and then set search conditions.
3) Click **Search**.

The search results are displayed. See Figure 5-37.

Step 3 Click at the lower-right corner of the playback window.

The following dialogue box is displayed. See Figure 5-40.

Figure 5-40 Tag



Step 4 Enter tag name, and then click **OK**.

5.2.6 Locking Files

Lock specific videos or pictures so they cannot be viewed. An locked file can only be viewed after being unlocked.

Step 1 Click , and then select **SEARCH**.

The **SEARCH** interface is displayed. See Figure 5-36.

Step 2 Search for pictures or videos.

1) Click the **Record** or **Image** tab.
2) Select a camera, and then set search conditions.
3) Click **Search**.

The search results are displayed. See Figure 5-37.

Step 3 Select the video files to be locked.

- Point to the thumbnail, and then click to select the video.
- You can click **Cancel** to cancel the selected videos.

Step 4 Click **Lock**.

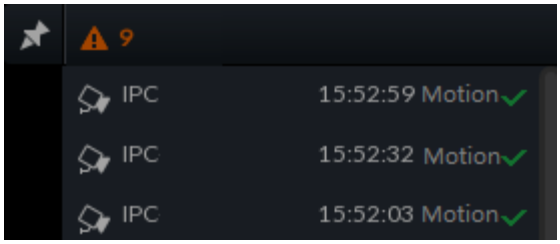
Step 5 (Optional) Click **Unlock** to unlock the locked videos.

You can also unlock videos in **FILE > FILE LOCKED**. See "7.1.2 FILE LOCKED."

5.3 Alarm List

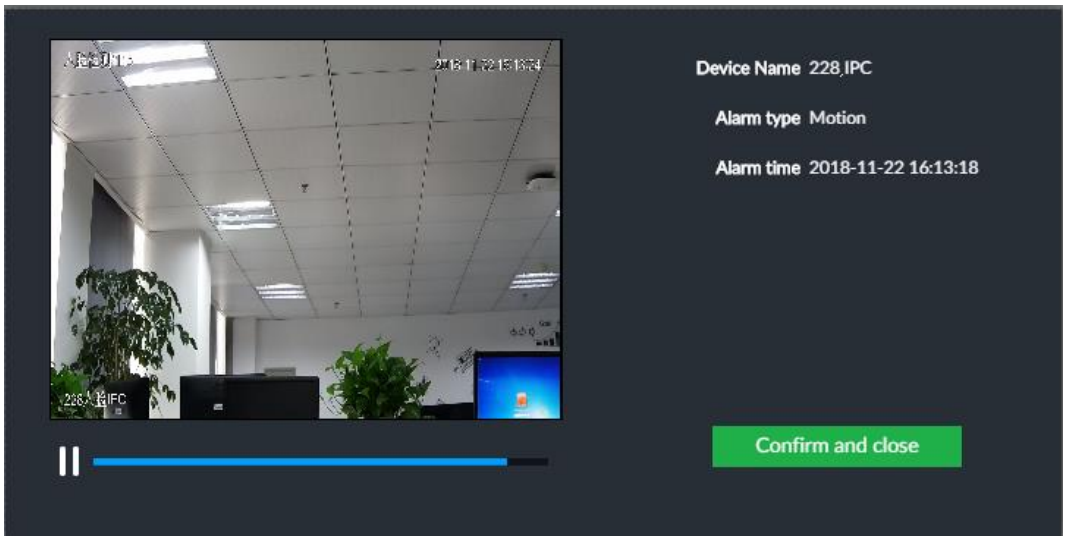
Click  to display alarm list. See Figure 5-41. View alarm device name, alarm time and alarm type.

Figure 5-41 Alarm list



- Number 9 is the number of alarm event to be processed. The value changes according to alarm amount. It displays maximum 200 unprocessed alarm events.
- Click  to lock alarm list. The alarm list is open and cannot hide. Click the icon again to cancel lock function. Move the mouse pointer to other position, and the alarm list displays for a period of time and then automatically hides.
- Click  to confirm alarm event. The confirmed event will be removed from the alarm list.
- Click the alarm event on the alarm list. The device displays the 20 seconds video before and after the alarm event occurred. See Figure 5-42.
  - ◇ Click  to pause play. Now the icon becomes  . Click  again to continue to play.
  - ◇ Click **OK and close**, confirm the alarm event and then exit the interface.

Figure 5-42 Alarm video

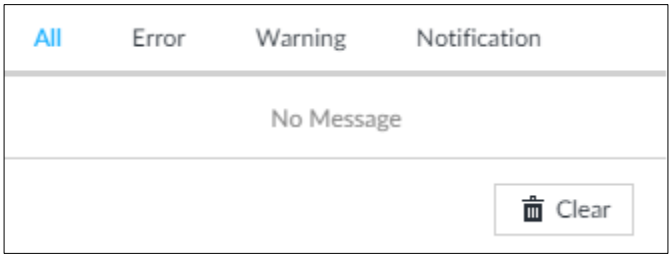


5.4 System Info

View system information including system error, system alarm and system notification.

Click  to display background task list. See Figure 5-43.

Figure 5-43 System info



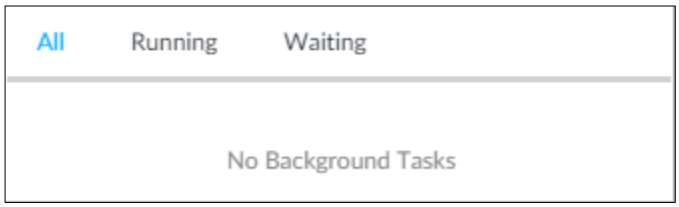
- Click **All**, **Error**, **Warning**, or **Notification** tab to view the corresponding system information list.
- Click  to clear the corresponding system information.
- Click **Clear** to clear system information under current tab.
  For example, click **All** tab and then click **Clear** button to clear all system information. Click **Error** tab and then click **Clear** button to clear all system error information.

5.5 Background Task

View background task running status.

Click  , device displays background task list. See Figure 5-44. Click **All**, **Running**, or **Waiting** to view the corresponding background task list.

Figure 5-44 Background task

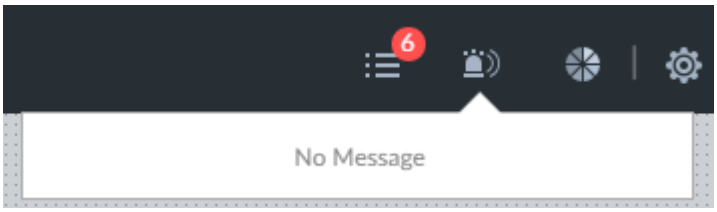


5.6 Buzzer

View buzzer alarm messages.

Click  . The alarm messages are displayed. See Figure 5-45.

Figure 5-45 Buzzer



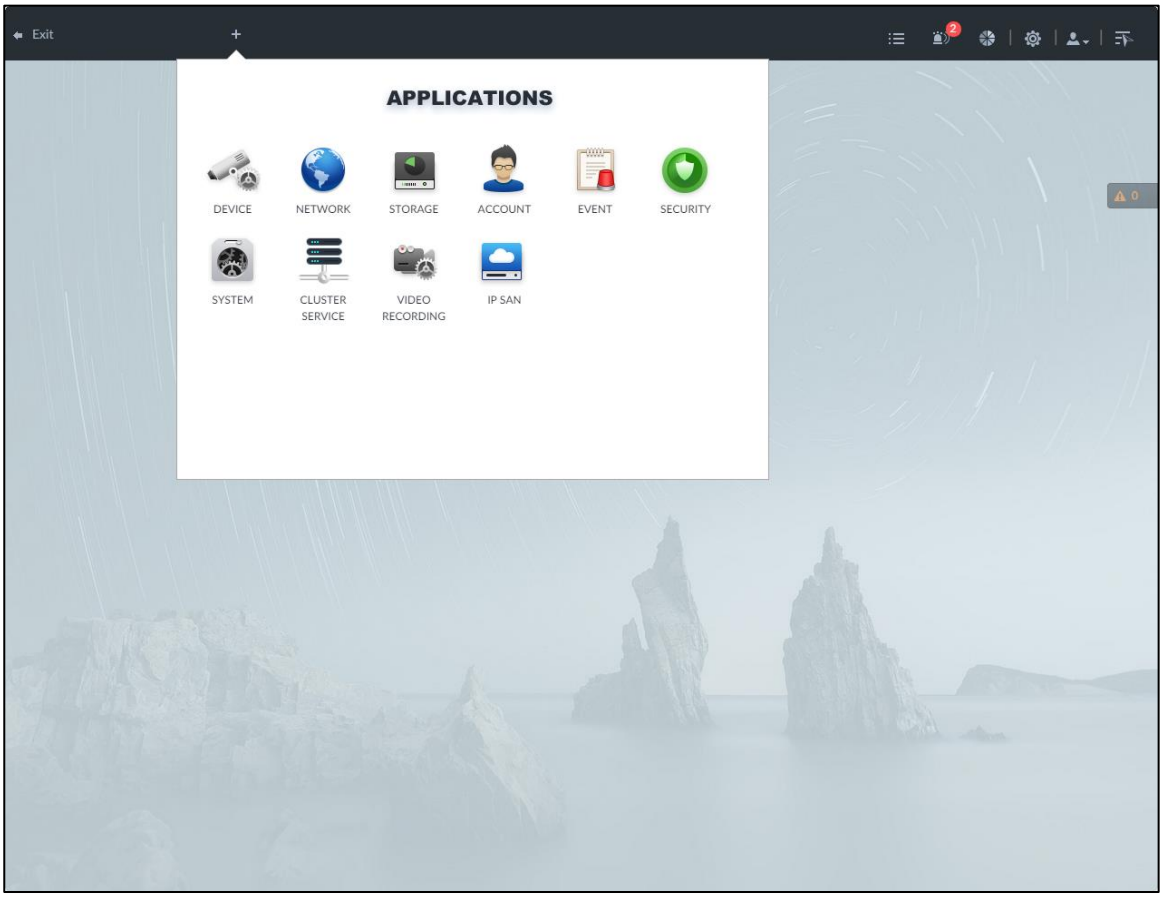
6 System Configuration

This chapter introduces system configuration functions such as managing remote device, setting network, setting alarm event, setting HDD storage, managing user information, setting device security strategy, and setting system parameters.

6.1 Configuration Interface

Click  . The following interface is displayed. See Figure 6-1.

Figure 6-1 Configuration interface



On this interface, you can:

- Click the corresponding app icon to go to the corresponding interface. The task column displays current running app name. Move the mouse pointer to the app name and then click  to close the app.
- Click **Exit** to exit the interface.

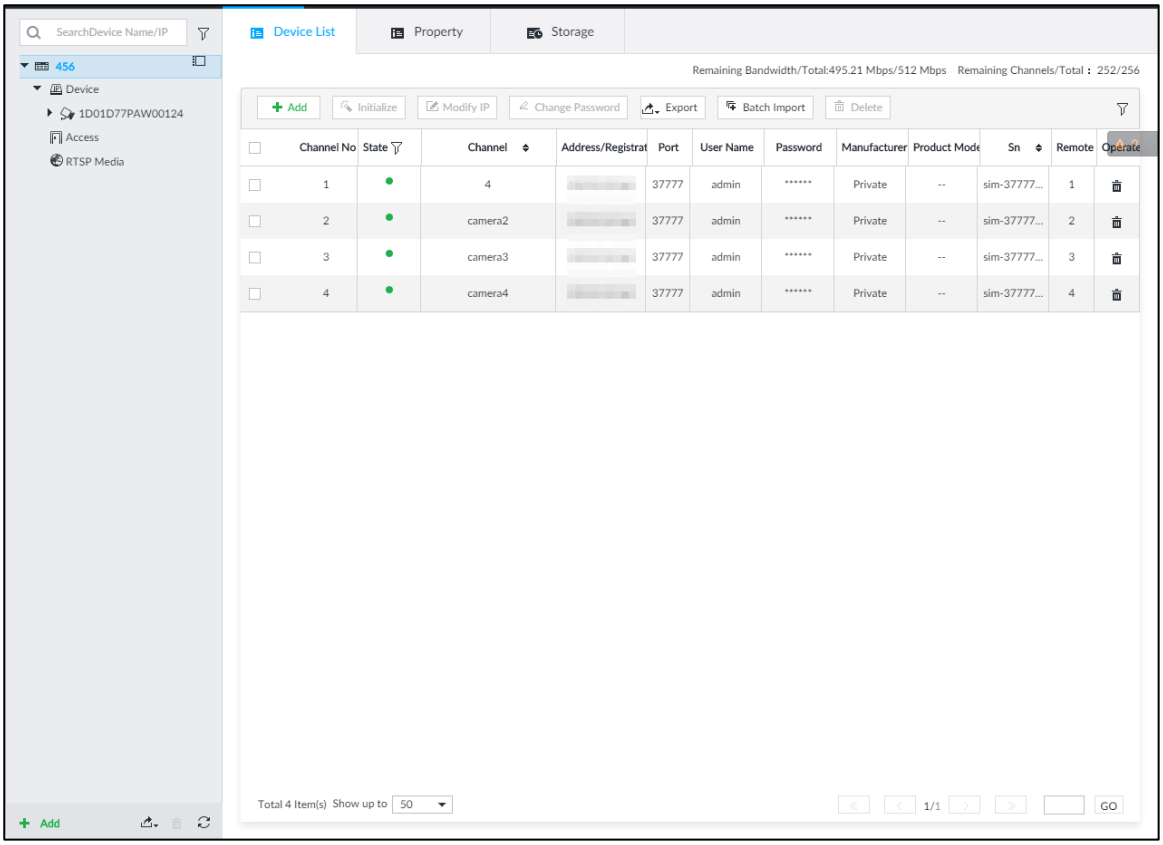
6.2 Device Management

Click or click on the configuration interface, and then select **DEVICE**. The **DEVICE** interface is displayed. See Figure 6-2. You can set EVS or remote devices.

- Select the root node 456 in the resource tree to set EVS name and storage plan.
- Select a remote device in the device list. Set its property, connection, video, OSD, and storage plan.

Click or click **Add** to add remote device to the system. See "3.4.2 Adding Remote Device" for detailed information.

Figure 6-2 Device management



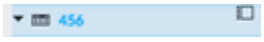
6.2.1 Local Device

Set device property and record storage plan.

6.2.1.1 Configuring Property Parameters

Set device name, view device information.

Step 1 Click , and then select **DEVICE**.

Step 2 Select the root node  in the resource tree, and then click the **Property** tab.

Step 3 Set parameters. For details, see Table 6-1.

Table 6-1 Property parameters description

Parameters	Description
Name	Set device name.
Description	Enter device description.
Device info	Displays info of the main board and the standby board, including type, SN, MAC, video in/out, audio in/out, alarm in/out and system version.

Step 4 Click **Save**.

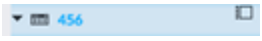
6.2.1.2 Configuring Storage Plans

Set device global record and image storage plan according to the actual situation.

On this interface, the record and image storage plan is for all registered remote devices. You can select one remote device to set specified storage plan. See "6.2.2.3.5 Storage" for detailed information.

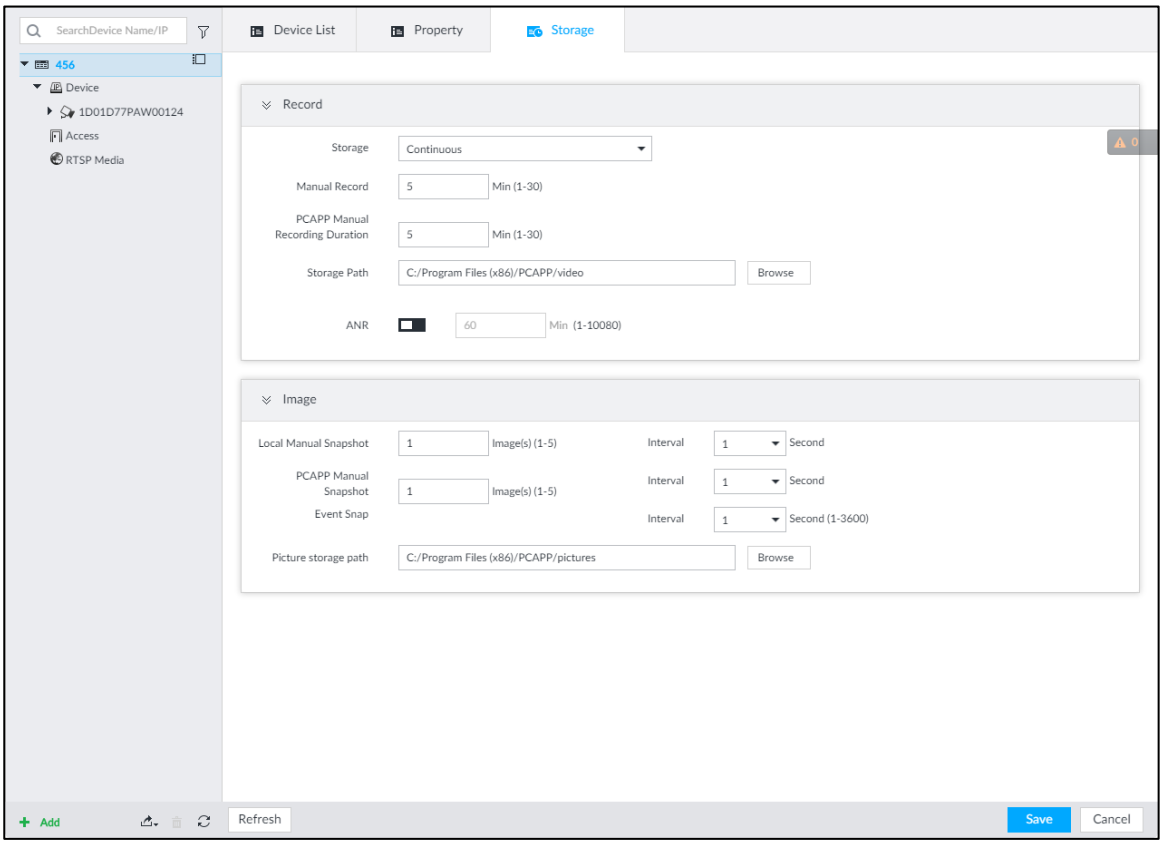
Step 1 Click  , or click  on the configuration interface, and then select **DEVICE**.

The **DEVICE** interface is displayed.

Step 2 Select the root node  in the resource tree, and then click **Storage** tab.

The storage interface is displayed. See Figure 6-3.

Figure 6-3 Storage



Step 3 Set parameters. See Table 6-2.

Table 6-2 Storage parameters description

Parameters		Description
Record	Storage	Set record strategy. ● Continuous Recording: 24-hour continuous recording. ● Not Recording: Device is not recording. ● Event Recording: Device only records when there is corresponding alarm event. ● Scheduled: Record in the scheduled time. ● Scheduled & Event: Record in the scheduled time and also on the basis of event-triggering.
	ANR	● When a camera gets disconnected with EVS, it stores the recorded videos in its local SD card. When the camera is connected again, it will upload the video during the disconnection to EVS. ● Set the maximum length of the to-be-uploaded video so that after getting reconnected, the camera will only upload video of the pre-defined length to EVS. Make sure that the camera has an SD card.
	Manual Record (duration)	Set manual record file length. On the **LIVE** interface, click to start record. If you do not click the icon to stop record, system stops recording automatically according to the record length here.
	PCAPP Manual Recording Duration	Set the time length of manual recording performed on the PCAPP client. Click to start manual recording on the PCAPP client. The manual recording automatically finishes at the end of the pre-defined time period.
	Storage Path	Click **Browser** to set manual record storage path. Only PCAPP supports this function.
Image	Local Manual Snapshot	Set manual snapshot amount and snapshot speed.
	PCAPP Manual Snapshot	Set the number and speed of manual snapshot on the PCAPP.
	Event Snap	Set event snapshot interval. Select **Customize** to set customized interval. The maximum internal is 3600 seconds.
	Picture storage path	Click **Browser** to set snapshot image storage path. Only PCAPP supports this function.

Step 4 Click **Save**.

6.2.2 Remote Device

The Device supports to add remote device, modify its IP address and configurations, and export its information.

See "3.4.2 Adding Remote Device" for detailed information.

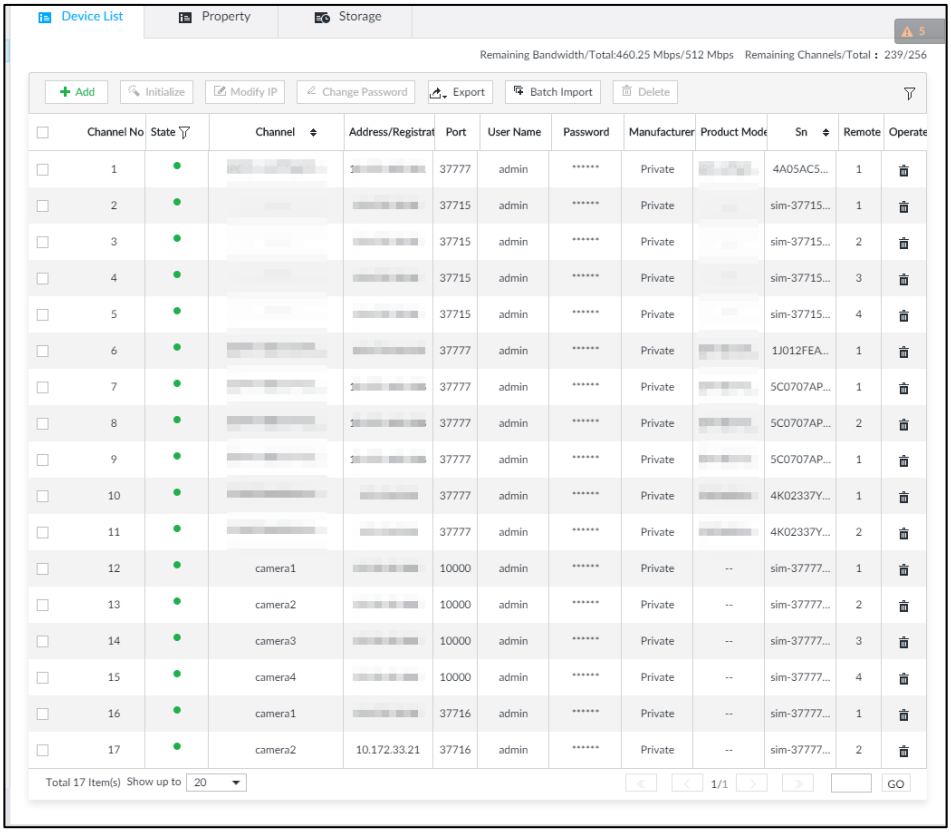
6.2.2.1 Viewing Remote Devices

View connected remote devices. For details about adding devices, see "3.4 Configuring Remote Device."

Step 1 Click , or click on the configuration interface, and then select **DEVICE**.

The **DEVICE** interface is displayed. See Figure 6-4.

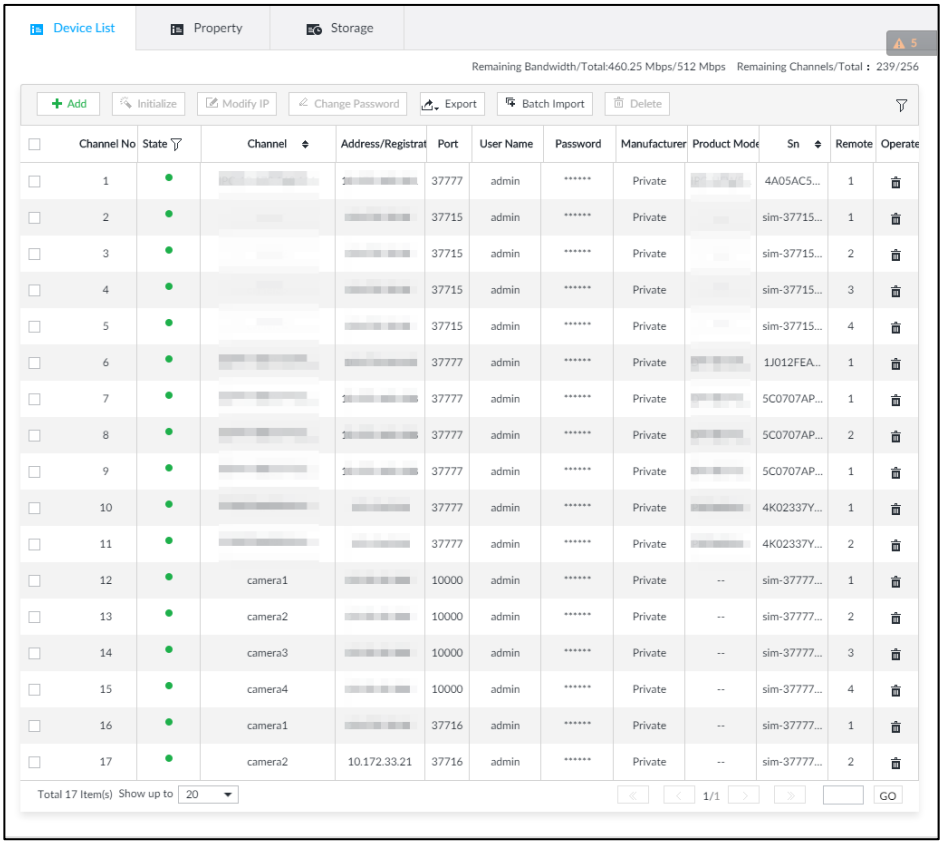
Figure 6-4 Device management



Step 2 Select the root node IVSS in the resource tree, and then click the **Device List** tab.

The **Device List** interface is displayed. See Figure 6-5.

Figure 6-5 Device list



Step 3 View details of connected devices, including IP address and serial number.

- In the **Status** column, indicates that the device is offline.
- In the **Status** column, indicates that the device is online.
- In the **Status** column, indicates that the device is exception. Point to , and then you are prompted about the details of the exception, such as being uninitialized, device mismatch, and wrong password.

Step 4 (Optional) Click to set searching conditions.

Step 5 (Optional) You can select the uninitialized devices to initialize them. For details, see "3.4.1 Initializing Remote Device."

6.2.2.2 Changing IP Address

Modify IP address of the remote device connected or not connected to the Device.

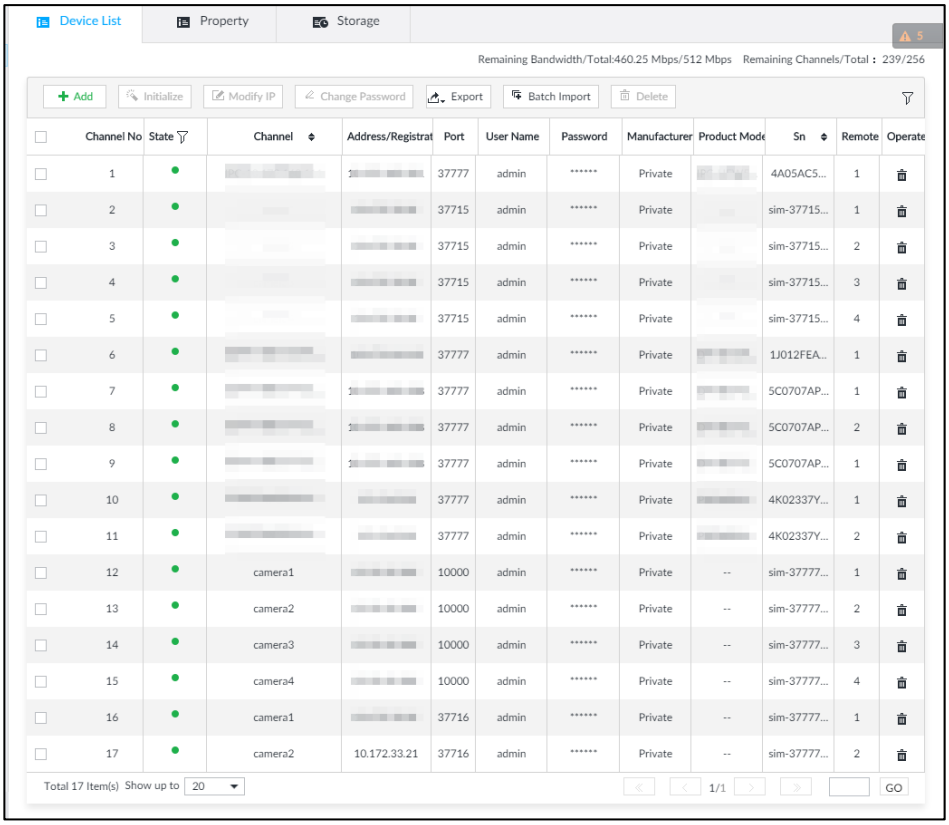
6.2.2.2.1 Modifying IP of Unconnected Devices

- You can only modify the IP address of initialized devices. For remote device initialization, see "3.4.1 Initializing Remote Device" for detailed information.
- You can only modify the IP address of remote devices connected with private protocol.

Step 1 Click , or click on the configuration interface, and then select **DEVICE**.

The **DEVICE** interface is displayed. See Figure 6-6.

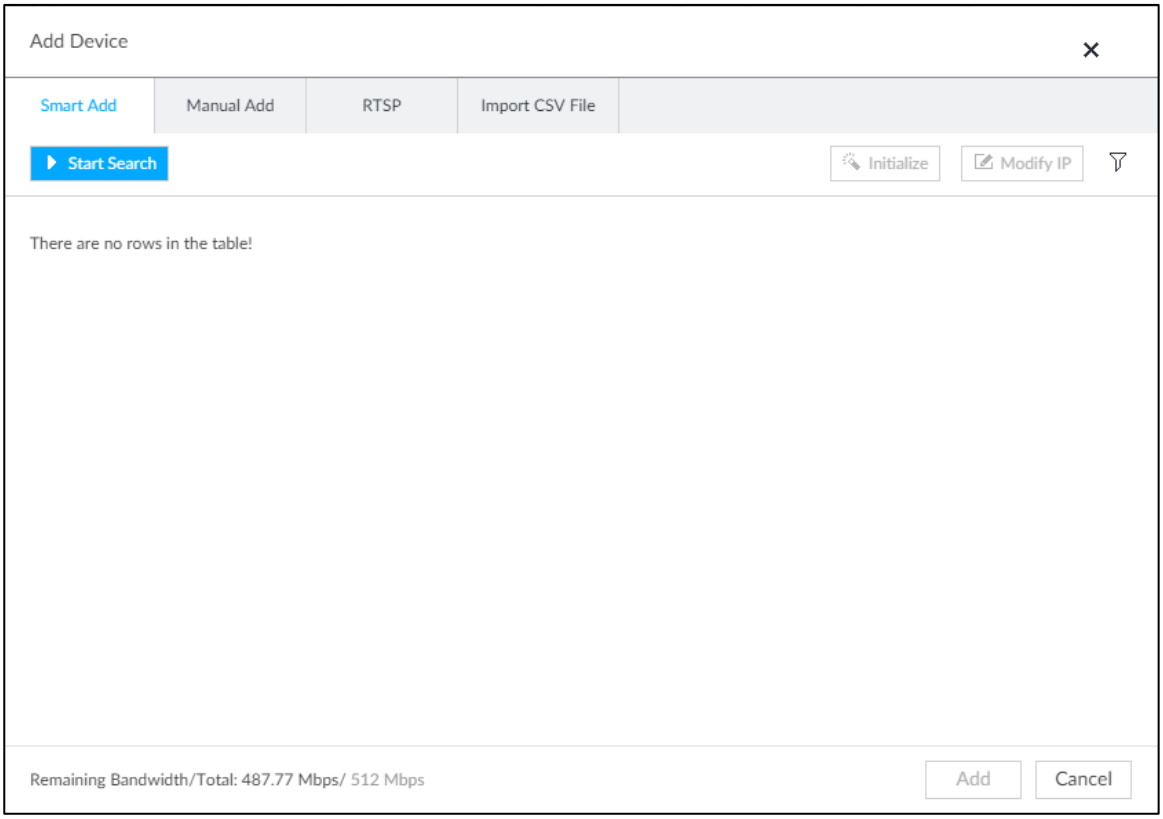
Figure 6-6 Device management



Step 2 Click  or click **Add**, and then select **Smart Add**.

The **Smart Add** interface is displayed.

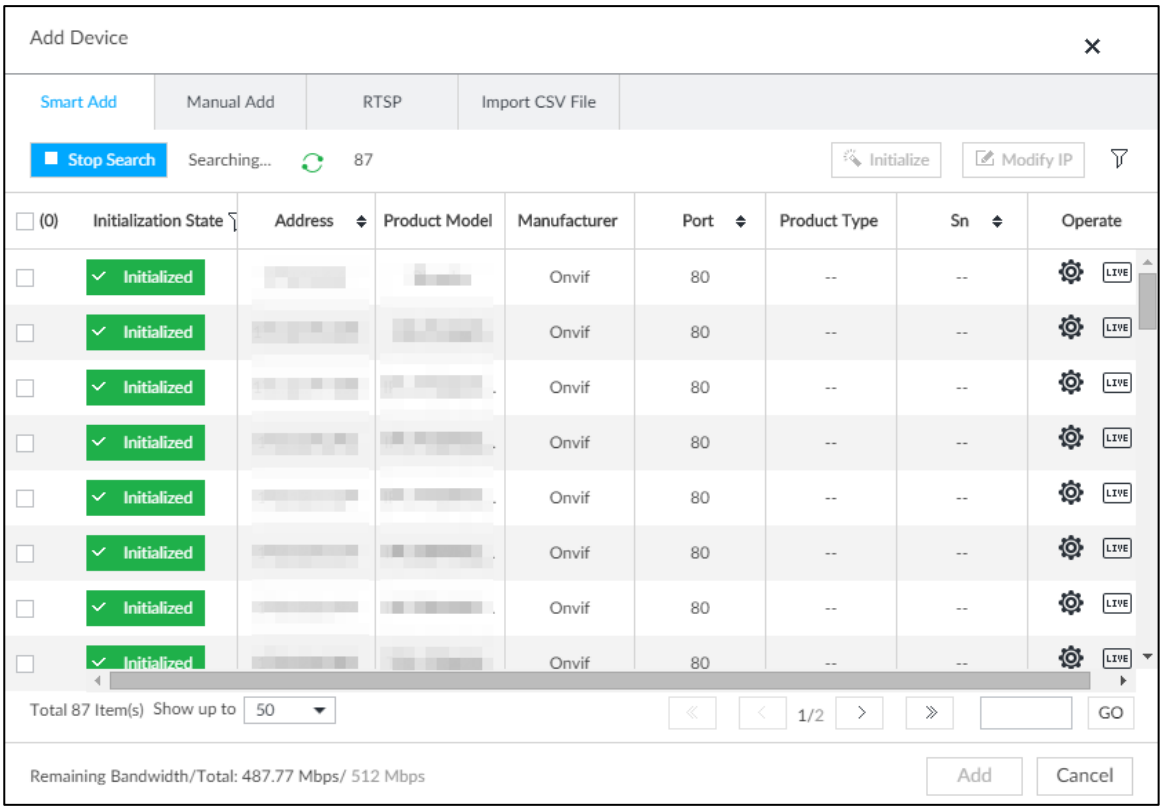
Figure 6-7 Smart add



Step 3 Click Start Search.

System starts to search and displays result. See Figure 6-8.

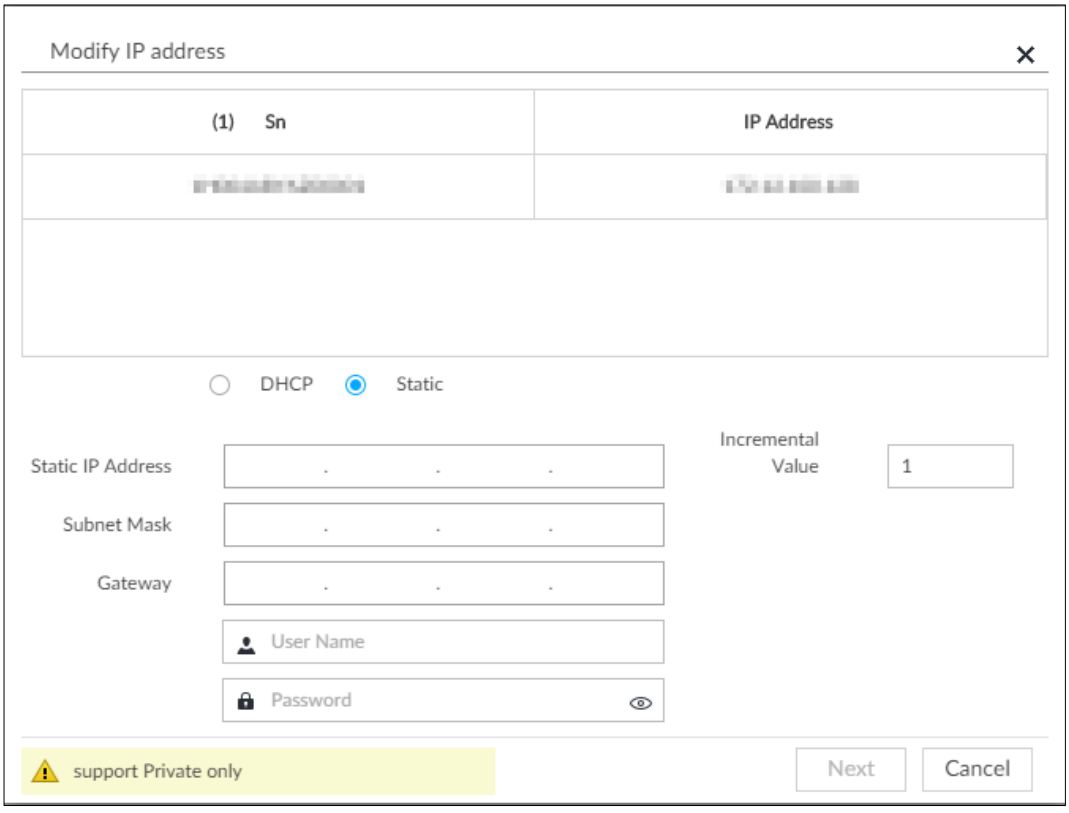
Figure 6-8 Remote device



Step 4 Select a remote device and then click **Modify IP**.

The **Modify IP** interface is displayed. See Figure 6-9.

Figure 6-9 Modify IP



Step 5 Enter the static IP address, subnet mask, gateway, and incremental value.

- Enter incremental value only when multiple remote devices are modified. If you want to change IP addresses of several devices at the same time, system allocates IP address one by one according to your setting at the fourth bit of the IP address.
- If there is IP conflict when changing static IP address, device pops up IP conflict dialogue box. To change IP addresses in batches, system automatically skips the conflicted IP and begins the allocation according to the incremental value.

Step 6 Enter the user name and password of remote device.

When you are changing several device IP addresses, make sure that the user name and password of these remote devices are the same.

Step 7 Click **Next**.

The modification result is displayed.

Step 8 Click **OK** to complete the modification.

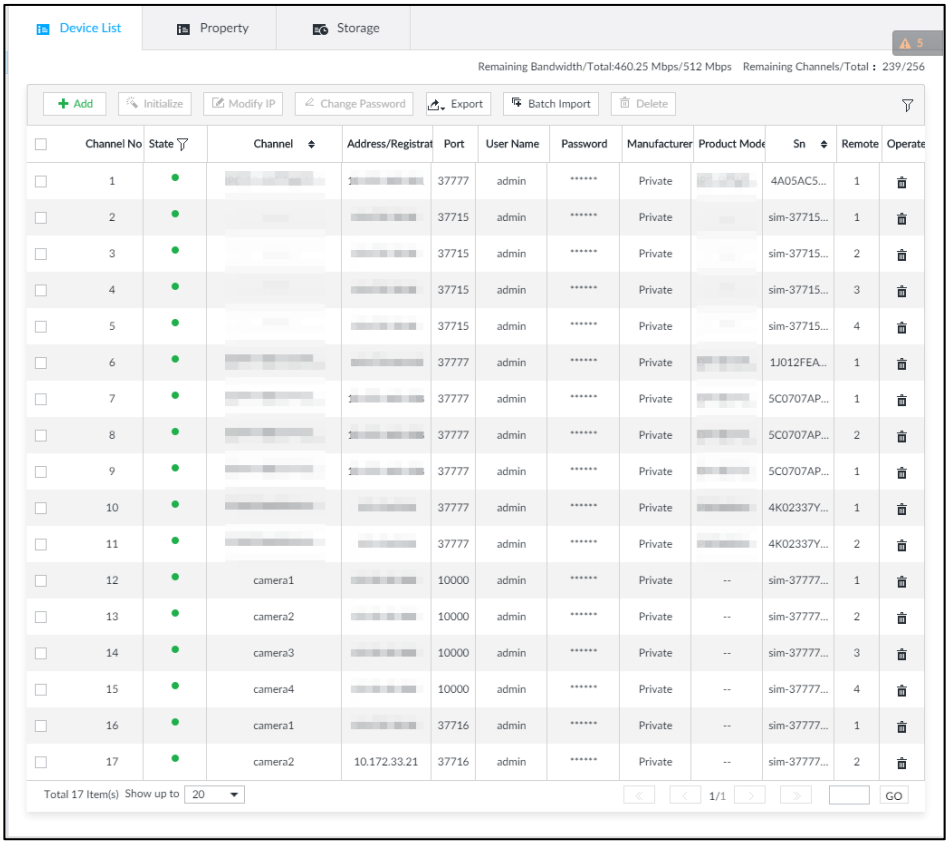
6.2.2.2.2 Modifying IP of Connected Devices

- You can only modify the IP address of initialized devices. For remote device initialization, see "3.4.1 Initializing Remote Device" for detailed information.
- You can only modify the IP address of remote devices connected through private protocol.
- To modify the IP address of connected devices one by one, see "6.2.2.3.2 Configuring Connection Information."

Step 1 Click  , or click  on the configuration interface, and then select **DEVICE**.

The **DEVICE** interface is displayed. See Figure 6-10.

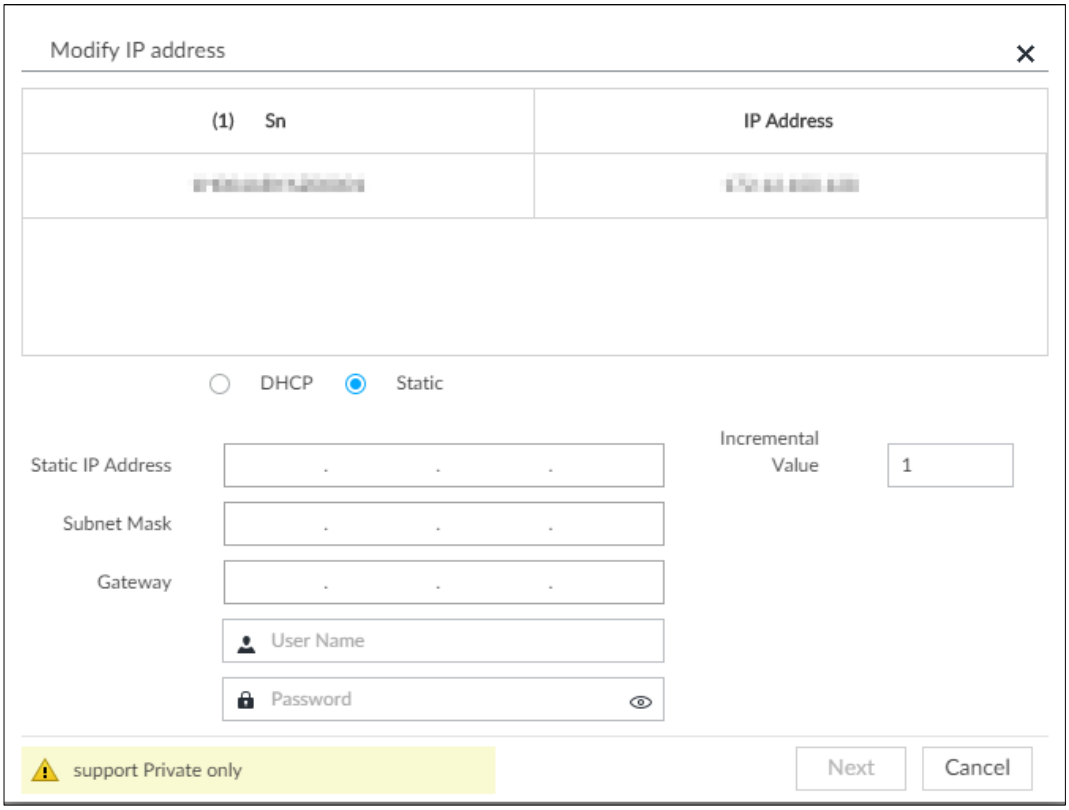
Figure 6-10 Device management



Step 2 Select a remote device and then click **Modify IP**.

The **Modify IP** interface is displayed. See Figure 6-11.

Figure 6-11 Modify IP



Step 3 Enter the IP address, subnet mask, gateway, and incremental value.

- Enter incremental value only when multiple remote devices are modified. If you want to change IP addresses of several devices at the same time, system allocates IP address one by one according to your setting at the fourth bit of the IP address.
- If there is IP conflict when changing static IP address, device pops up IP conflict dialogue box. To change IP addresses in batches, system automatically skips the conflicted IP and begins the allocation according to the incremental value.

Step 4 Enter the user name and password of remote device.

When you are changing several device IP addresses, make sure that the user name and password of these remote devices are the same.

Step 5 Click **Next**.

The result of IP modification is displayed.

Step 6 Click **OK**.

6.2.2.3 Configuring Remote Devices

Set remote device property, connection information, and video parameters.

Different remote devices have different interfaces. See the actual interface for detailed information.

6.2.2.3.1 Configuring Device Property

Set remote device name, and view device information.

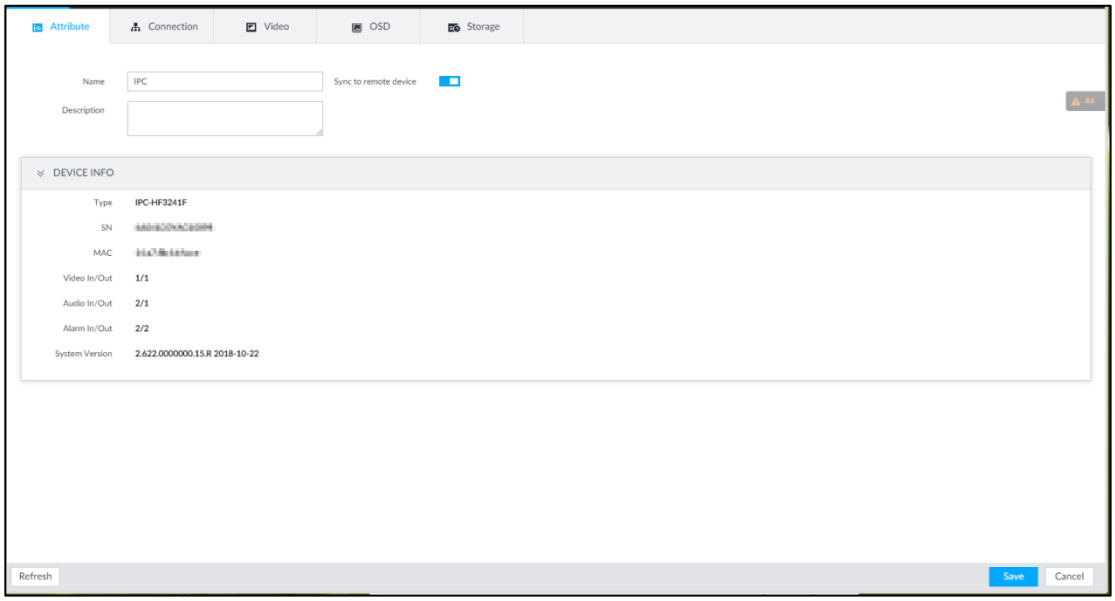
Step 1 Click , or click on the configuration interface, and then select **DEVICE**.

The **DEVICE** interface is displayed.

Step 2 Select a remote device on the left panel and then click **Property** tab.

The **Property** interface is displayed. See Figure 6-12.

Figure 6-12 Property



Step 3 Set parameters. For details, see Table 6-3.

Table 6-3 Property parameters description

Parameters	Description
Name	Set remote device name. Enable **Sync to remote device** and save the settings to synchronize new name to the remote device.
Description	Input remote device description.
Device info	Displays remote device information. It includes remote device type, SN, MAC address, video in/out, audio in/out, alarm in/out, and system version.

Step 4 Click **Save**.

6.2.2.3.2 Configuring Connection Information

Set connection information of remote device, such as IP address and port number.

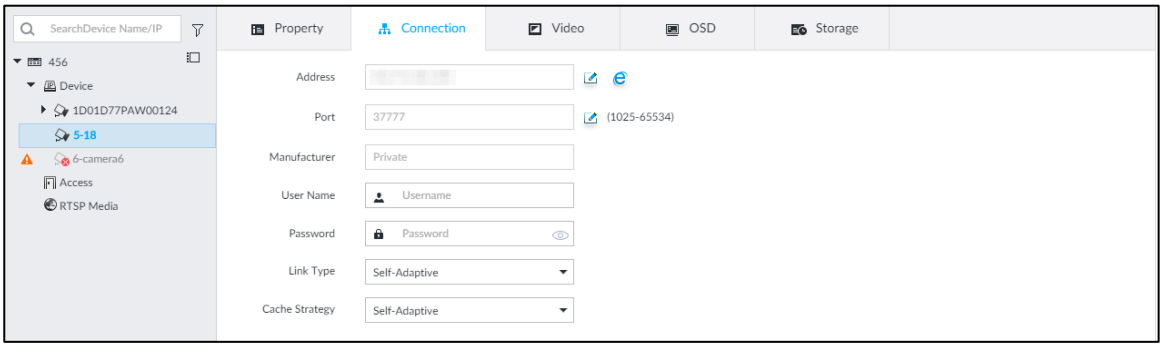
Step 1 Click , or click on the configuration interface, and then select **DEVICE**.

The **DEVICE** interface is displayed.

Step 2 Select a remote device on the left panel and then click the **Connection** tab.

The **Connection** interface is displayed. See Figure 6-13.

Figure 6-13 Connection information

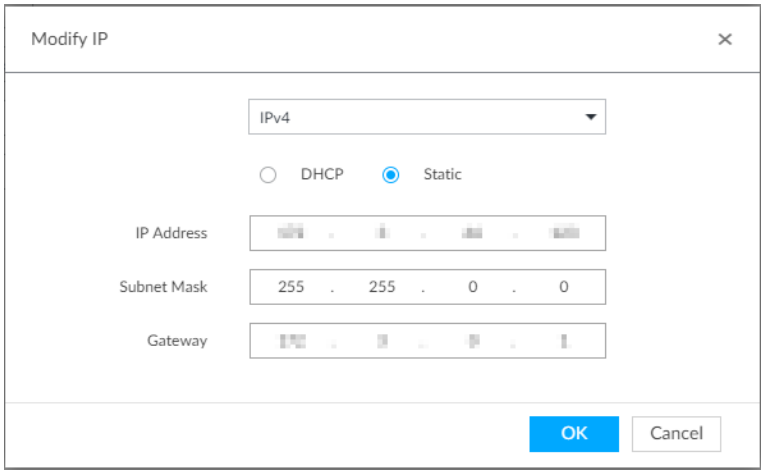


Step 3 Change IP address.

1) Click of the corresponding address.

The **Modify IP** interface is displayed. See Figure 6-14.

Figure 6-14 Modify IP



2) Select IP mode.

- Check DHCP, there is no need to enter IP address, subnet mask, and default gateway. Device automatically allocates dynamic IP address to the remote device.
- Check Static, and then enter IP address, subnet mask, default gateway and incremental value.

- Enter incremental value only when multiple remote devices are modified. If you want to change IP addresses of several devices at the same time, system allocates IP address one by one according to your configuration at the fourth bit of the IP address.
- If there is IP conflict when changing static IP address, device pops up IP conflict dialogue box. To change IP addresses in batches, device automatically skips the conflicted IP and begins the allocation according to the incremental value.

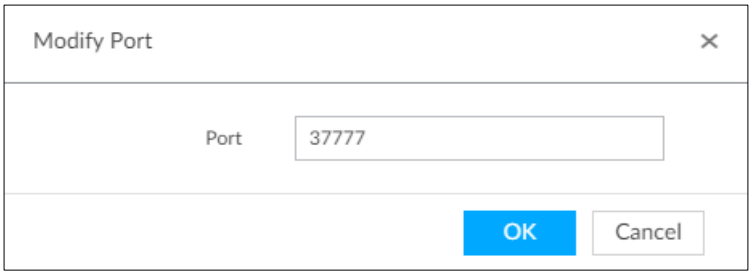
3) Click **OK** to save setting.

Step 4 Change port number.

1) Click  of the corresponding port.

The **Modify Port** interface is displayed. See Figure 6-15.

Figure 6-15 Port



2) Change port number.
3) Click **OK** to save setting.

Step 5 Set other parameters. See Table 6-4 for detailed information.

Table 6-4 Connection parameters description

Parameters	Description
Manufacturer	Displays the connection protocol of the remote device.
Username	Enter user name and password of remote device. The password should consist of 8 to 32 non-blank characters and contain at least two types of characters among uppercase, lowercase, number, and special character (excluding ' " ; : &). Enter a strong password according to the password strength indication.
Password	
Link type	Displays link type of the system and remote device. It is self-adaptive.
Cache strategy	Set cache strategy of remote device video stream. ● Self-adaptive: System automatically adjusts video stream cache status according to the network bandwidth. ● Realtime: Guarantee video realtimeness. When the network bandwidth is not sufficient, the video might not be fluent. ● Fluency: Guarantee video fluency. When the network bandwidth is not sufficient, the video might not be clear.

Step 6 Click **Save**.

Step 7 (Optional) Click , and then you can go to the web interface of the remote device.

On the local interface of the Device, you cannot click to go to the web interface of the remote device.

6.2.2.3.3 Configuring Video Parameters

Set different video parameters according to different bit stream types based on the bandwidth.

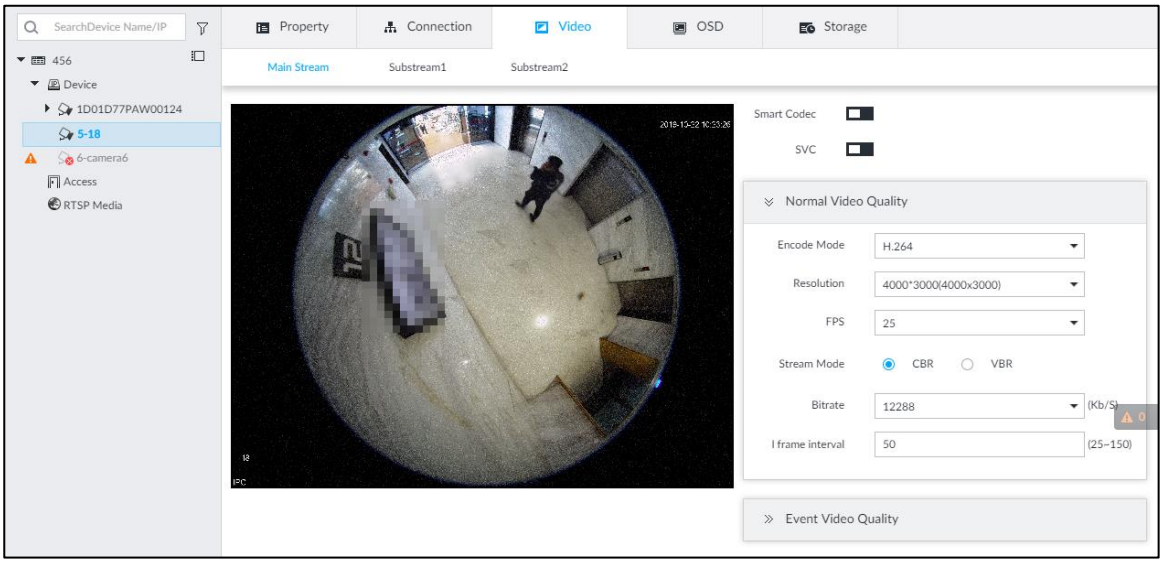
Step 1 Click , or click on the configuration interface, and then select **DEVICE**.

The **DEVICE** interface is displayed.

Step 2 Select a remote device on the left panel and then click **Video** tab.

The **Video** interface is displayed. See Figure 6-16.

Figure 6-16 Video



Step 3 Set main stream, sub stream 1, or sub stream 2.

Step 4 Set general video quality parameters. See Table 6-5 for detailed information.

Table 6-5 Video parameters description

Parameters	Description
Smart Codec	Enable this function to enhance performance of video compression and thus reduce storage space requirement. This function is only available for main stream.
SVC	Select the check box to enable SVC function. Select 1 or 2 from the drop-down list on the right. The default setup is 1, there is no scaled encoding. SVC refers to the scaled video coding. It can split the video stream to basic stream and enhanced scale.

Parameters	Description
Encode mode	Set video encode mode. ● H.264: It is a highly compressed video encoding or encoding standard. At the same video quality, it has increased the compression rate by 2X compared with the MPEG-2. ● H.265: It is a new video encode standard coming after H.264. It has improved the complicated relationship among bit stream, encode quality, latch and algorithm on the previous standard. It can get the best encoding.
Resolution	Set video resolution. The higher the resolution is, the better the video quality is. Different series products support different resolutions. See the actual interface for detailed information.
FPS	Set the frame amount displayed at each second. The higher the frame rate is, the more vivid and fluent the video is.
Stream mode	Set video bit stream control mode. ● CBR: The bit stream changes slightly. The bit stream is near the value you set here. ● VBR: The bit stream might change according to the environment.
Quality	Set video quality. It includes low, middle, high. It is null when the stream mode is CBR.
Bitrate	Set video bitrate. ● Main stream: In the **Bit Rate** list, select a value or enter a customized value to change the image quality. The larger the value is, the better the image will become. ● Sub stream: In CBR mode, the bit stream changes around the value you set. In VBR mode, it changes according to the bit stream value, but its max value is near the specified value.
I frame interval	Set the P frame amount between two I frames. Usually we recommend it is the 2X of the frame rate.

Step 5 Enable **Event Video Quality** and set FPS and stream mode.

Event video quality is for main stream only.

Step 6 Click **Save**.

6.2.2.3.4 OSD

Configure overlay time information, and channel information on the video.

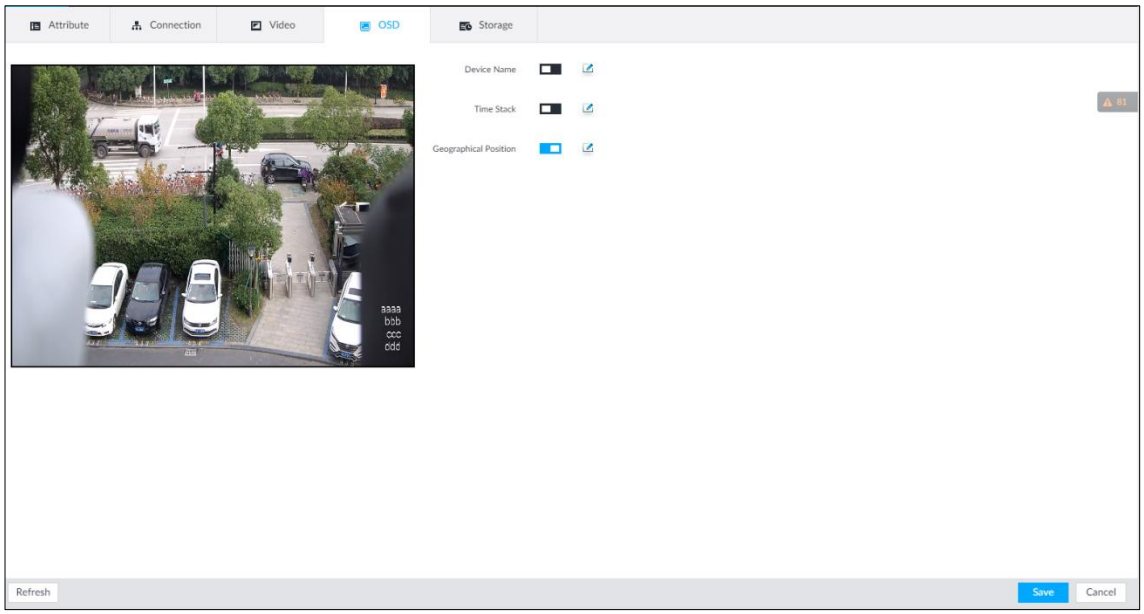
Step 1 Click , or click on the configuration interface, and then select **DEVICE**.

The **DEVICE** interface is displayed.

Step 2 Select a remote device on the left panel and then click **OSD** tab.

The **OSD** interface is displayed. See Figure 6-17.

Figure 6-17 OSD



Step 3 Enable OSD information according to actual requirements.

1) Click  to enable OSD function.

2) Click  .

The video displays the text boxes. See Figure 6-18, Figure 6-19 or Figure 6-20.

Figure 6-18 Device name

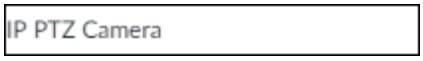


Figure 6-19 Time

Figure 6-20 Geographical position

3) Set device name.

Skip this step if you do not want to use device name function.

4) Set geographical position information.

Skip this step if you do not want to use geographical position function.

Click  or  to create a text box. Enter the geographical position information.

◇ Click  to adjust font alignment mode.

◇ Click  or  again, add one text box at the top or the bottom of the text box.

◇ Click  to delete the text box.

5) Drag the text box to the proper position.

6) Click  to save.

Step 4 Click **Save**.

6.2.2.3.5 Storage

Set video file and image storage plan of remote device according to the actual situation.

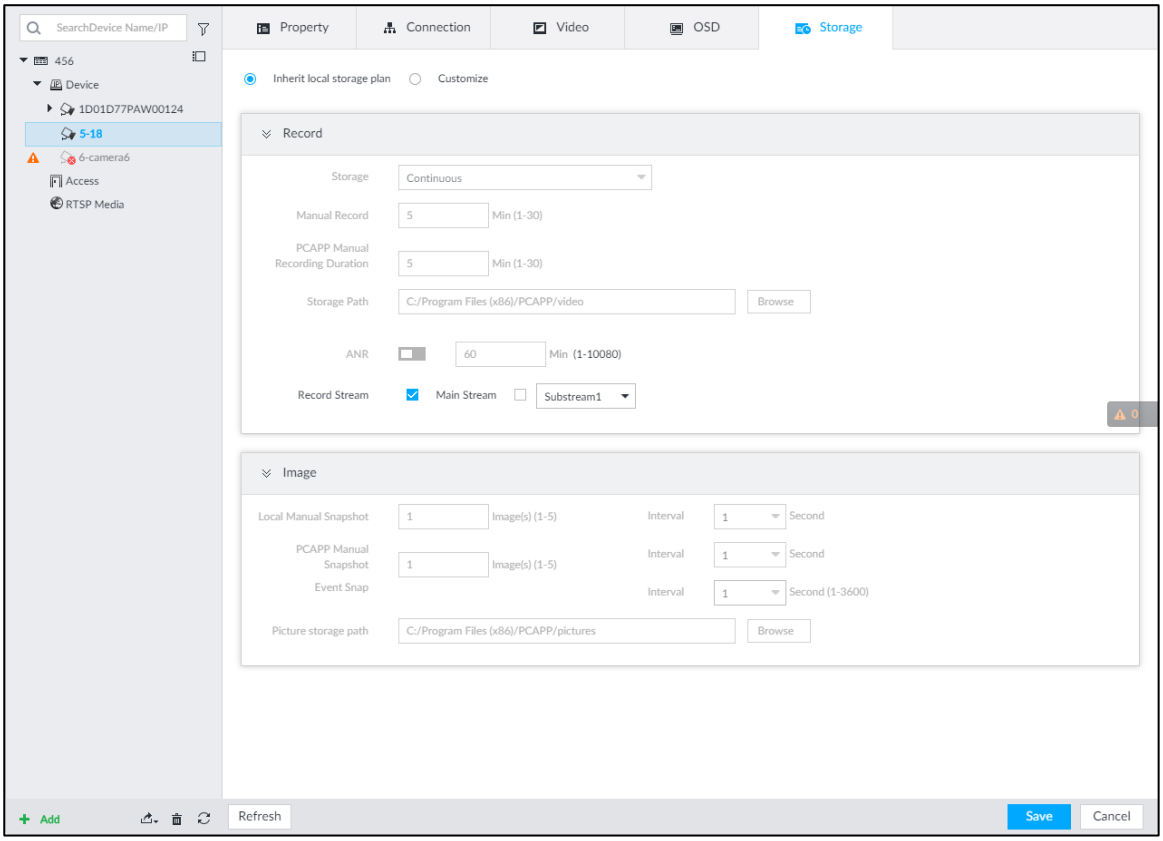
Step 1 Click  , or click  on the configuration interface, and then select **DEVICE**.

The **DEVICE** interface is displayed.

Step 2 Select a remote device on the left panel and then click **Storage** tab.

The **Storage** interface is displayed. See Figure 6-21.

Figure 6-21 Storage



Step 3 Select Inherit local storage plan or Customize.

- **Inherit local storage plan**: The remote device adopts global storage plan of the Device. For details, see "6.2.1.2 Configuring Storage Plans."
- **Customize**: Set customized storage plan.

Step 4 Set parameters. For details, see Table 6-6.

Set record streams only if you select **Inherit local storage plan**.

Table 6-6 Storage parameters description

Parameters		Description
Record	Storage	Set record strategy. ● Continuous Recording: 24-hour continuous recording. ● Not Recording: Device is not recording. ● Event Recording: Device only records when there is corresponding alarm event. ● Scheduled: Record in the scheduled time. ● Scheduled & Event: Record in the scheduled time and also on the basis of event-triggering.
	ANR	● When a camera gets disconnected with EVS, it stores the recorded videos in its local SD card. When the camera is connected again, it will upload the video during the disconnection to EVS. ● Set the maximum length of the to-be-uploaded video so that after getting reconnected, the camera will only upload video of the pre-defined length to EVS. Make sure that the camera has an SD card.
	Manual Record (length)	Set manual record file length. On the **LIVE** interface, click to start record. If you do not click the icon to stop record, system stops recording automatically according to the record length here.
	PCAPP Manual Recording Duration	Set the time length of manual recording performed on the PCAPP client. Click to start manual recording on the PCAPP client. The manual recording automatically finishes at the end of the pre-defined time period.
	Storage Path	Click **Browser** to set manual record storage path. Only PCAPP supports this function.
Image	Local Manual Snapshot	Set manual snapshot amount and snapshot speed.
	Event Snap	Set event snapshot interval. Select **Customize** to set customized interval. The maximum internal is 3600 seconds.
	Picture storage path	Click **Browser** to set snapshot image storage path. Only PCAPP supports this function.

Step 5 Click **Save**.

6.2.2.4 Exporting Remote Devices in Batches

Export the added remote device. When the device restores factory default settings or information of remote device is lost, export information of remote device to recover quickly.

See "3.4.2 Adding Remote Device" for detailed information.

Step 1 Click , or click on the configuration interface, and then select **DEVICE**.

The **DEVICE** interface is displayed.

Step 2 Click at the lower-left corner.

The **Export** interface is displayed. See Figure 6-22.

Click **Download Template** to download template file of the remote device, and add remote device through the template.

Figure 6-22 Export

Step 3 Select encryption or not.

- If you select **Yes**, the system exports encrypted .backup file.
- If you select No, the system exports .csv file, which can be opened with Excel. The exported .csv file contains IP address, port number, channel number, channel name, manufacturer and user name (excluding password) of the remote device.

When unencrypted file is exported, keep the file properly to avoid data leakage.

Step 4 Click **OK**.

The following prompt interface is displayed.

Step 5 Click **Save**.

File path might be different depending on interface operations. See actual interfaces.

- On PCAPP, click , select **Downloads** to view file saving path. For details, see "9.3 Viewing Downloads."
- Select file saving path during local operation.

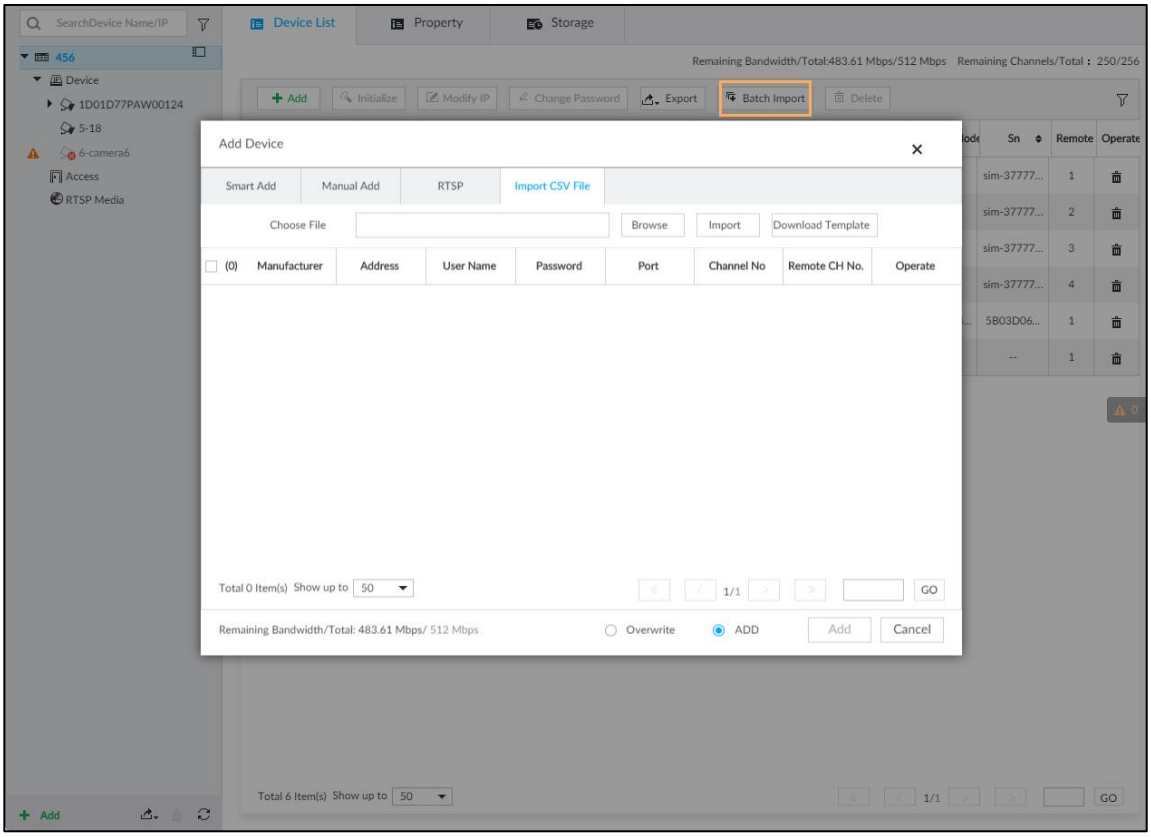
  Connect USB device to the system if you are on the local menu to operate.
- During web operations, files are saved under default downloading path of the browser.

6.2.2.5 Importing Remote Devices in Batches

Import devices in batches by using the template.

On the **Device List** interface, click **Batch Import** to go to the **Add Device** interface. On the **Add Device** interface, click the **Import CSV File** tab. For further operation instruction about how to use the CSV file to import devices in batches, see "3.4.2.4 Batch Add."

Figure 6-23 Import in batches



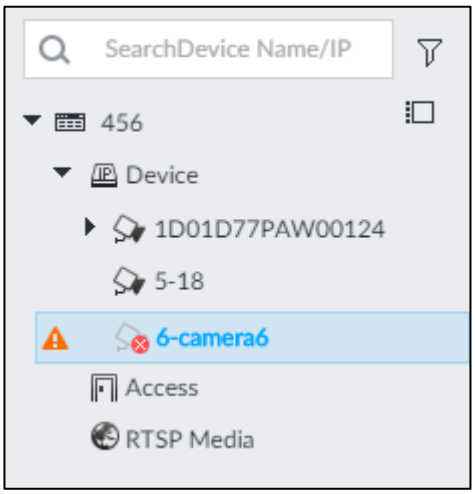
6.2.2.6 Connecting Remote Devices

On the **Device** interface, view connection status of remote device in the device list. See Figure 6-24.

When the remote device name and icon is black, SDT5A403 for example, it means the remote device is online. When they are gray, C2 8249 for example, it means the remote device is offline.

- Right-click the offline device, and then select **Connect** to connect the device.
- Right-click the online device, and then select **Disconnect** to disconnect the device.
- Right-click the online device, and then select **Open WEB** to go to the web interface of the device.

Figure 6-24 Device list



6.2.2.7 Deleting Remote Devices

On the **Device** interface, delete the registered remote device.

- Delete one by one:
  - ◇ Select a remote device and then click to delete.
  - ◇ On the **Device List** interface, right-click a remote device and then click **Delete**.
  - ◇ On the **Device List** interface, select a remote device, and then click .
  - ◇ On the **Device List** interface, select a remote device, and then click **Delete**.
- Batch delete:
  - ◇ Click , device list displays check box for you to select multiple remote devices. Click to delete the selected devices.
  - ◇ On the device list, click one remote device, press Ctrl to select other remote devices and then click to delete them.
  - ◇ On the device list, click one remote device, press Shift and then click another remote device to select all remote devices between these two, and then click to delete them.
  - ◇ On the **Device List** interface, select multiple remote devices, and then click **Delete.**

6.2.2.8 Modifying Device Password

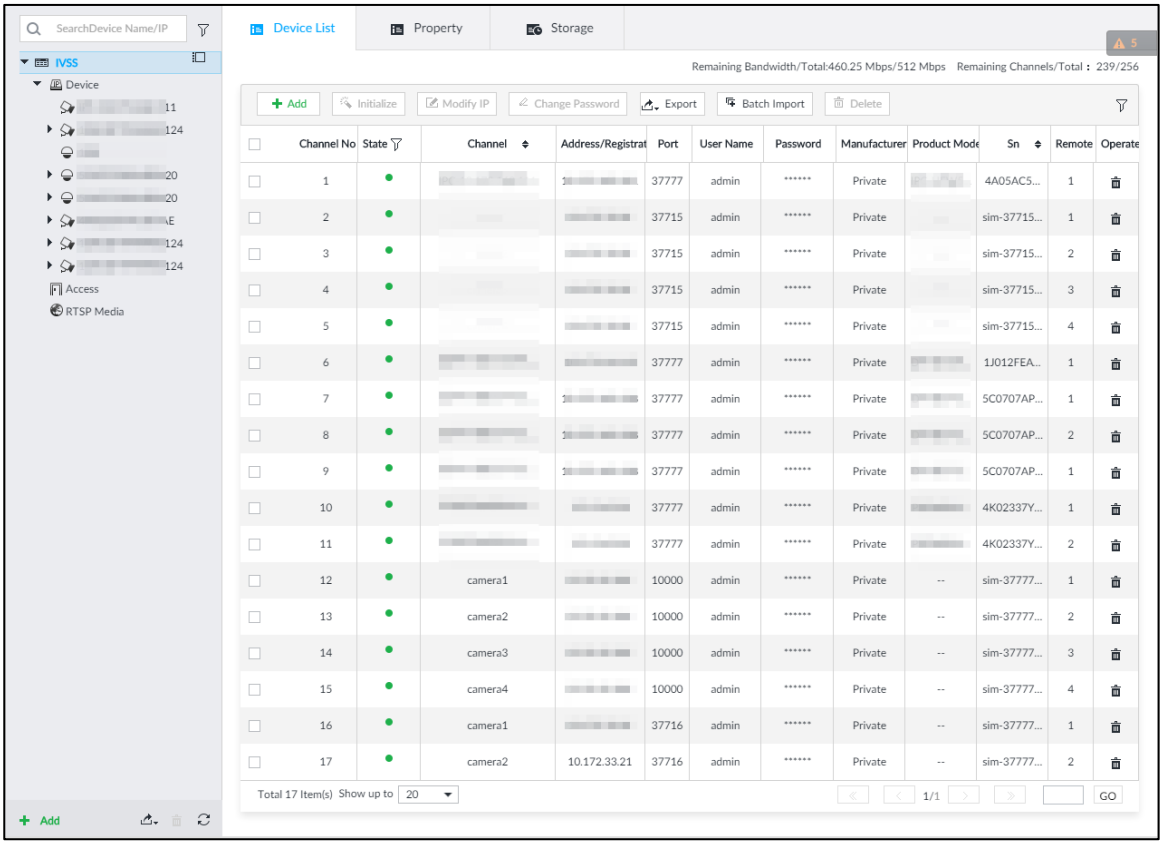
Modify passwords of connected devices.

You can only modify devices successfully connected to EVS via private protocol.

Step 1 Click , or click on the configuration interface, and then select **DEVICE**.

The **DEVICE** interface is displayed. See Figure 6-25.

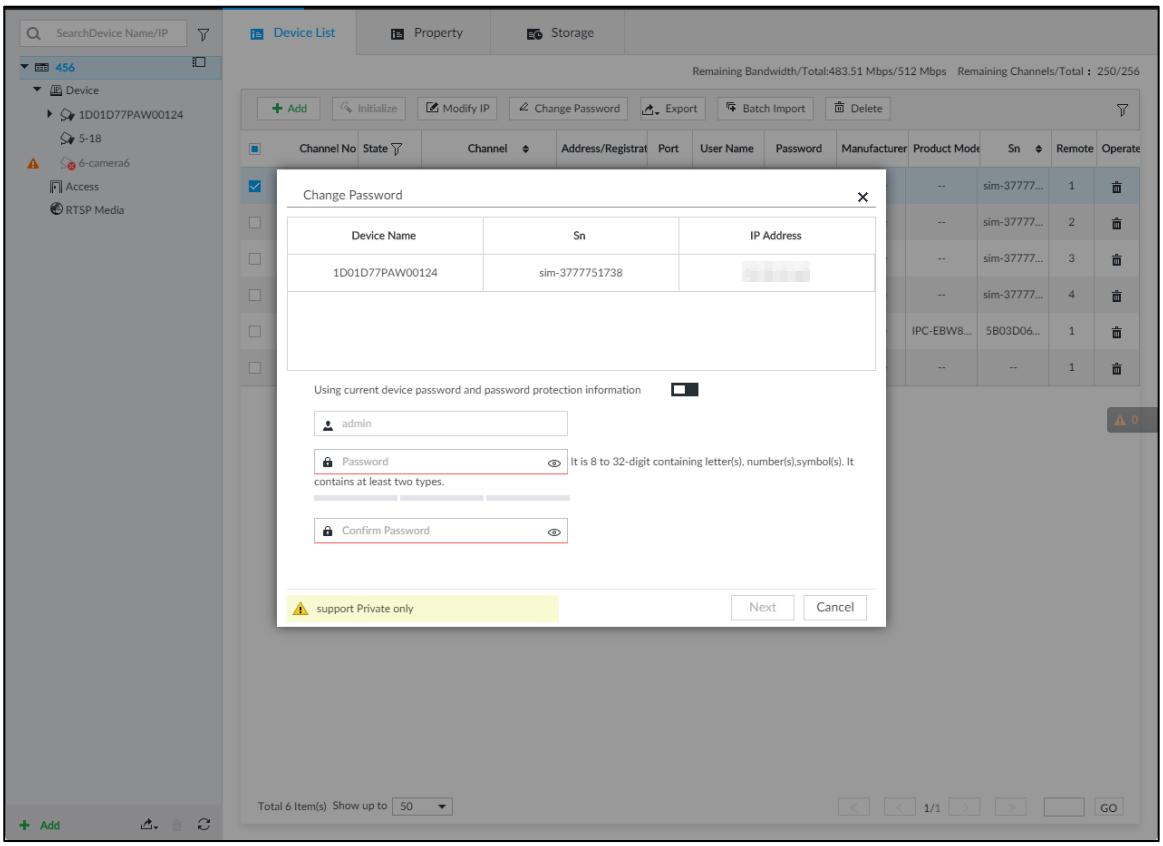
Figure 6-25 Device management



Step 2 Select a remote device and then click **Change Password**.

The **Change Password** interface is displayed. See Figure 6-26.

Figure 6-26 Modify password



Step 3 Keep Using current device password and password protection information disabled.

 means that the function is disabled.

Step 4 Enter the new password, and then confirm it as required.

Step 5 Click **Next** button.

The result of password modification is displayed.

Step 6 Click **OK**.

Step 7 (Optional) On the **Device List** interface, double-click the device name, and then you can modify device name.

6.3 Network Management

Click  or click  on the configuration interface, select **NETWORK**. The **NETWORK** interface is displayed. You can set basic network parameters and application.

6.3.1 Basic Network

Set basic network parameters of the device, such as IP address, port aggregation and port number, to connect with other devices in the network.

6.3.1.1 Configuring IP Address

Set device IP address, DNS server information and other information according to network planning.

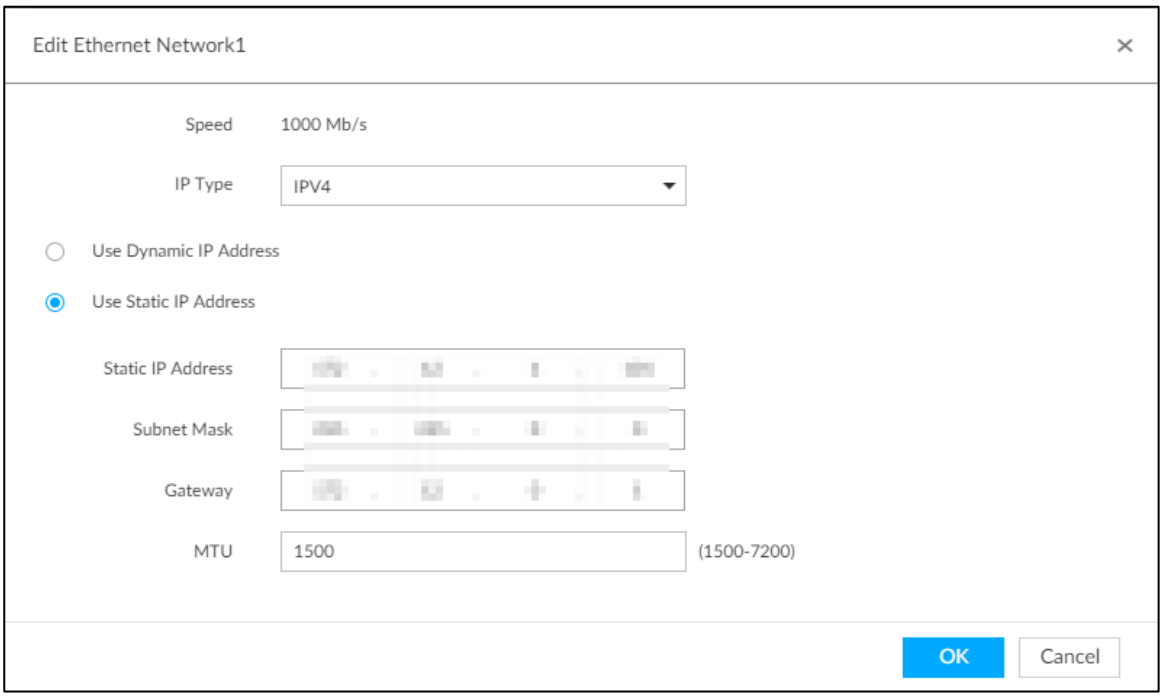
Device has 4 Ethernet ports by default. Make sure that at least one Ethernet port has connected to the network before you set IP address.

Step 1 Click  or click  on the configuration interface, and then select **NETWORK > Basic Network > TCP/IP**.

Step 2 Click  of the corresponding NIC.

The **Edit Ethernet Network** interface is displayed. See Figure 6-27.

Figure 6-27 Edit Ethernet network



Step 3 Set parameters. For details, see Table 6-7.

Table 6-7 TCP/IP parameters description

Parameters	Description
Speed	Current NIC max network transmission speed.
IP Type	Select IPv4or IPv6.
Use Dynamic IP Address	When there is a DHCP server on the network, check the box to use dynamic IP address, system can allocate an dynamic IP address to the device. There is no need to set IP address manually.
Use Static IP Address	Check the box to use static IP address. Set static IP address, subnet mask and gateway. Set a static IP address for the device.
MTU	Set NIC MTU value. The default setup is 1500 Byte. We recommend you to check the MTU value of the gateway first and then set the device MTU value equal to or smaller than the gateway value. Reduce the packets slightly and enhance network transmission efficiency. Changing MTU value might result in NIC reboot, network offline and affect current running operation. Please be careful!

Step 4 Click **OK.**

Go back to **TCP/IP** interface.

Step 5 Set DNS server information.

You can select to get DNS server manually or input DNS server information.

This step is compulsive if you want to use domain service.

- Check the box to auto get DNS server address, device can automatically get the DNS server IP address on the network.
- Check the box to use the following DNS server addresses, and then enter primary DNS and alternate DNS IP address.

Step 6 Set default NIC.

Select default NIC from the drop-down list.

Make sure that the default NIC is online.

Step 7 Click **Save**.

6.3.1.2 Port Aggregation

Bind multiple NIC to create one logic NIC and use one IP address for peripheral device. The bonded NIC can work as the specified aggregation mode to work. It enhances network bandwidth and network reliability.

System supports configuring load balance, fault tolerance, and link aggregation. See Table 6-8.

Table 6-8 Aggregation mode description

Aggregation mode	Description
Load balance	Device has bonded several NICs at the same time and use one IP address to communicate with the external device. The bonded NICs are working together to bear the network load. The load balance mode adds the network throughput data amount and enhances network flexibility and availability. In this mode, the network is offline once all NICs break down.
Fault-tolerance	In this mode, device has bonded several NICs and set one NIC as the master card and the rest NICs are the alternative NICs. Usually, only the master NIC card is working. System can automatically enable other alternate cards to work when the master card breaks down. Fault-tolerance is a network mode to enhance NIC reliability. In this mode, the network is offline once all NICs break down.
Link aggregation	Device has bonded several NICs and all NICs are working together to share the network load. System allocates data to each NIC according to your allocated strategy. Once the system detects that one NIC breaks down, it stops sending data with this NIC, and then system transmits the data among the rest NICs. System calculates transmission data again after malfunctioning NIC resumes work. In this mode, the network is offline once all bonded NICs are malfunctioning. Make sure that the switch supports link aggregation and you have set the link aggregation mode.

6.3.1.2.2 Binding NIC

System supports load balance, fault-tolerance, and link aggregation. Select bind mode according to your actual requirements.

Step 1 Click  or click  on the configuration interface, and then select **NETWORK > Basic Network > TCP/IP**.

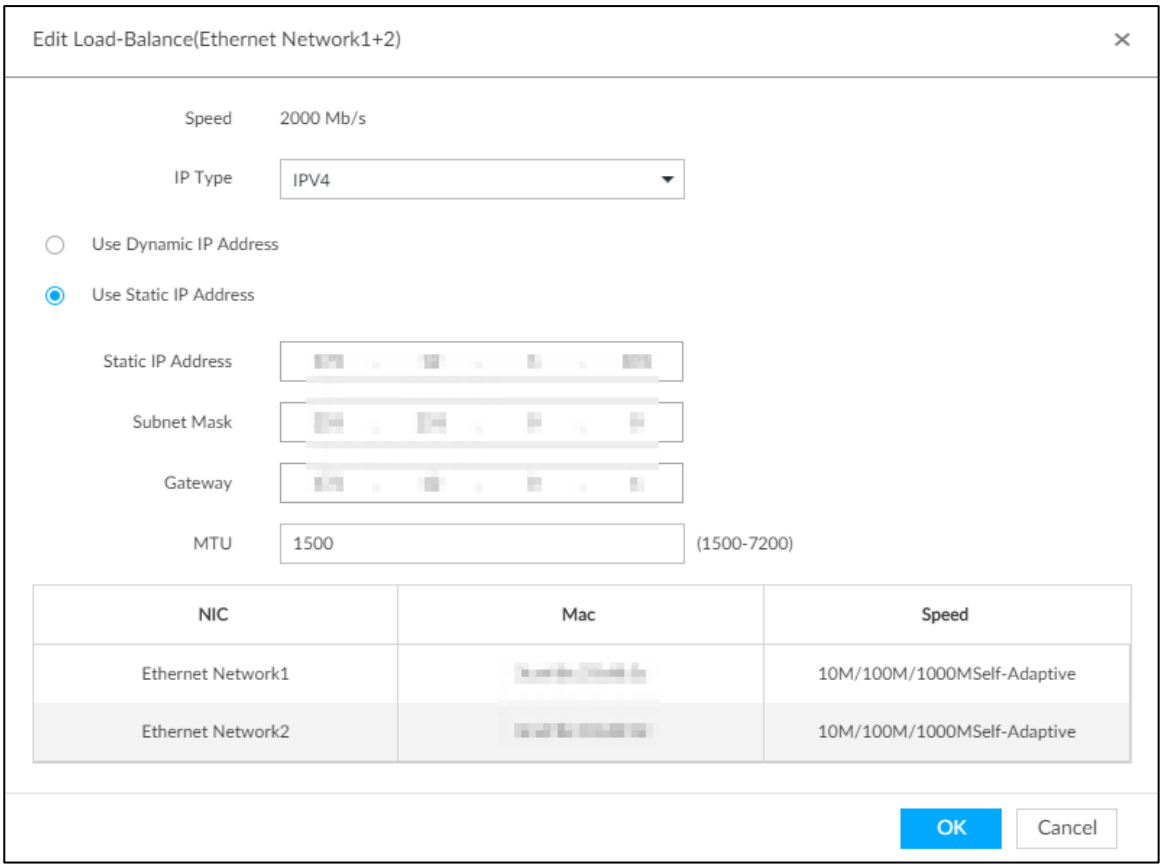
Step 2 Bind NICs.

1) Click Port Aggregation.
2) Select the NICs you want to bind.
3) Select an aggregation mode.
4) Click Port Aggregation.

The corresponding setting interface is displayed. See Figure 6-28.

The setting interface varies depending on the aggregation mode you have selected. Figure 6-28 is the load balance setting interface. For the other two modes, the actual interface shall prevail.

Figure 6-28 Edit load balance



5) Set parameters. For details, see Table 6-9.

Table 6-9 TCP/IP parameters description

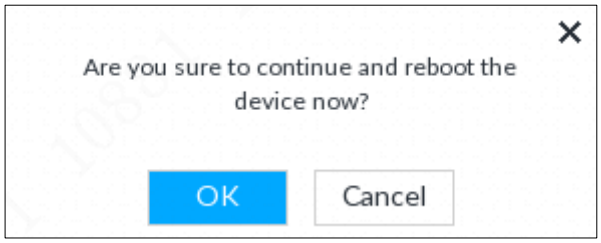
Parameters	Description
Speed	Maximum network transmission speed of current NIC.
IP Type	Select IPv4 or IPv6.
Use Dynamic IP Address	When there is a DHCP server on the network, check the box to use dynamic IP address. System can allocate a dynamic IP address to the device. There is no need to set IP address manually.
Use Static IP Address	Check the box to use static IP address. Set static IP address, subnet mask and gateway. Set a static IP address for the device.

Parameters	Description
MTU	Set NIC MTU value. The default setup is 1500 Byte. We recommend you to check the MTU value of the gateway first and then set the device MTU value equal to or smaller than the gateway value. Reduce the packets slightly and enhance network transmission efficiency. Changing MTU value might result in NIC reboot, network offline and affect current running operation. Please be careful!

6) Click **OK**.
Go back to **TCP/IP** interface.

Step 3 Click **Save**.
System pops up a confirmation box. See Figure 6-29.

Figure 6-29 Confirmation



Step 4 Click **OK** to save the configuration.
The binding card information becomes activated after reboot operation.

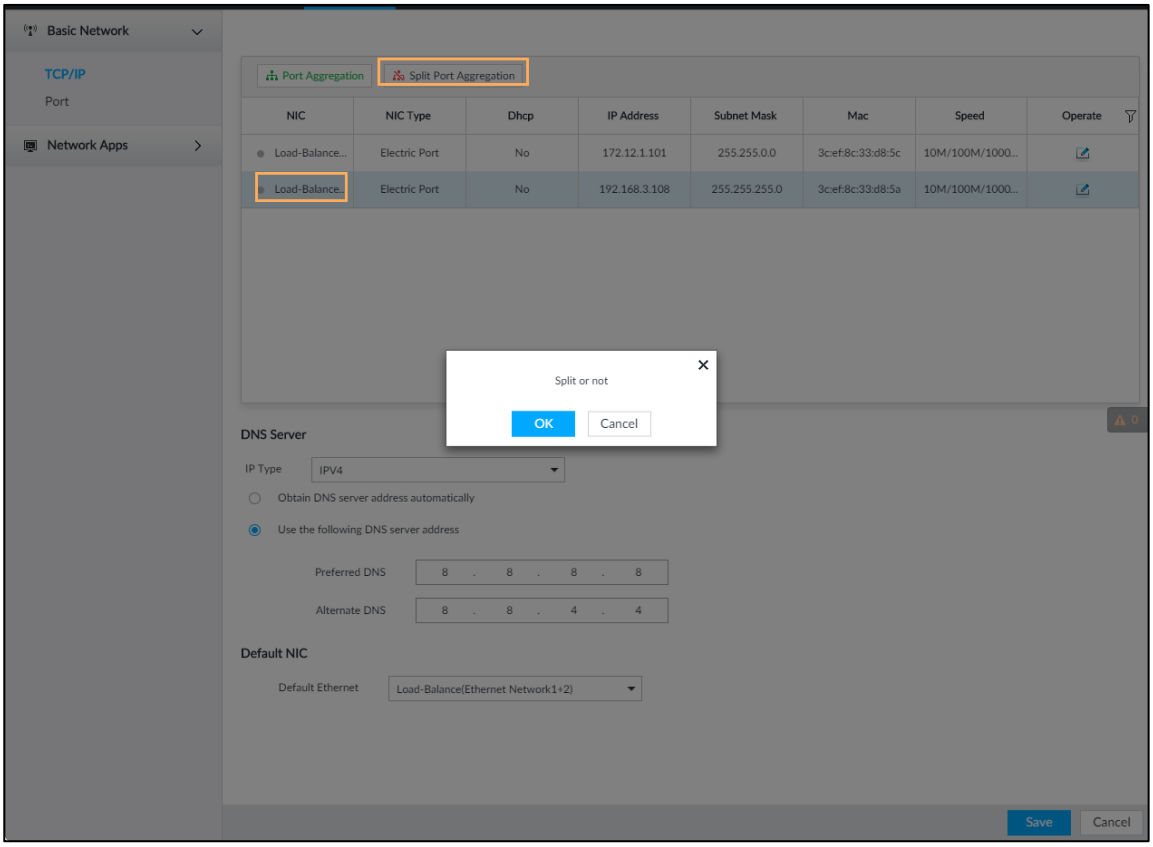
6.3.1.2.3 Cancelling Binding NIC

Cancel port aggregation and allow the bonded NICs to work as independent card.

Step 1 Click or click on the configuration interface, and then select **NETWORK > Basic Network > TCP/IP**.
The **TCP/IP** interface is displayed.

Step 2 Select a bonded NIC.
The confirm dialogue box is displayed. See Figure 6-30.

Figure 6-30 Confirm



Step 3 Click **OK**.

System splits the bonded NIC.

After splitting NIC binding, the first NIC reserves the IP address configured during binding, while the rest NICs restore default IP addresses.

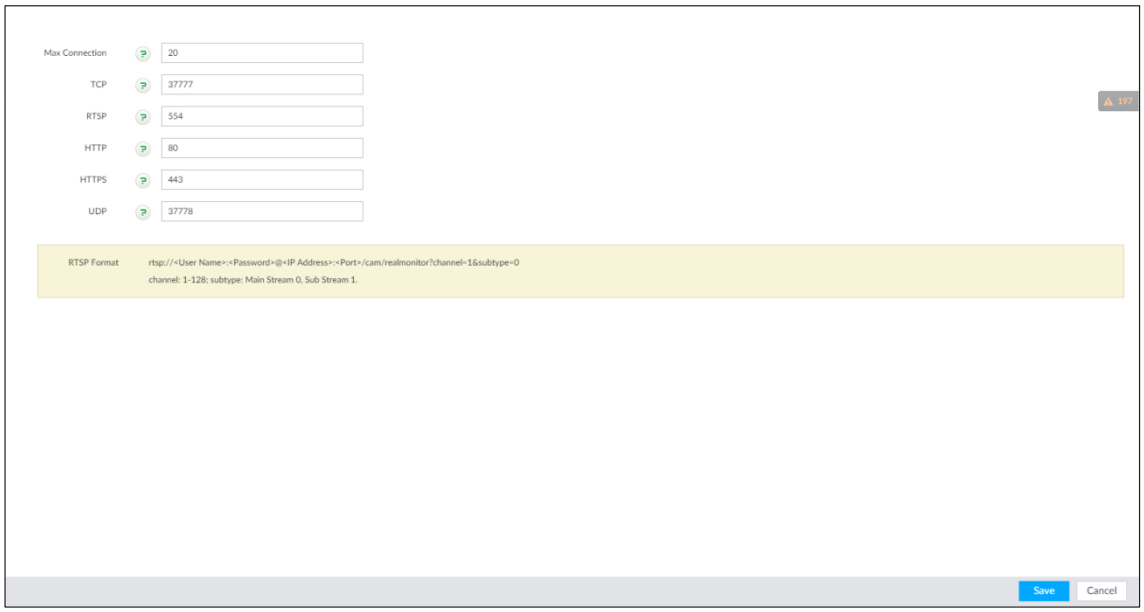
6.3.1.3 Setting Port Number

Set device port number.

Step 1 Click , or click on the configuration interface, and then select **NETWORK > Basic Network > Port**.

The **Port** interface is displayed. See Figure 6-31.

Figure 6-31 Port



Step 2 Set parameters. For details, see Table 6-10.

Log in again after modifying parameters except **Max Connection**.

Table 6-10 Connection setting parameters description

Parameters	Description
Max Connection	The allowable maximum clients accessing the Device at the same time, such as web, PCAPP, and Platform. Select a value between 1 and 128. The default value setting is 20.
TCP Port	Set according to the actual requirements. The default value is 37777. The value ranges from 1025 to 65535.
RTSP Port	Set according to the actual requirements. The default value is 554. The value ranges from 1 to 65535.
HTTP Port	Set according to the actual requirements. The default value is 80. The value ranges from 1 to 65535. If the value you set is not 80, please add the port number after the IP address when you are using browser to login the device.
HTTPS Port	Set according to the actual requirements. The default value is 443. The value ranges from 1 to 65535.
UDP Port	Set according to the actual requirements. The default value is 37778. The value ranges from 1025 to 65535.

Step 3 Click **Save**.

System reboots corresponding service of the port.

6.3.2 Network Apps

Set device network parameters, so that system can connect to other devices.

6.3.2.1 P2P

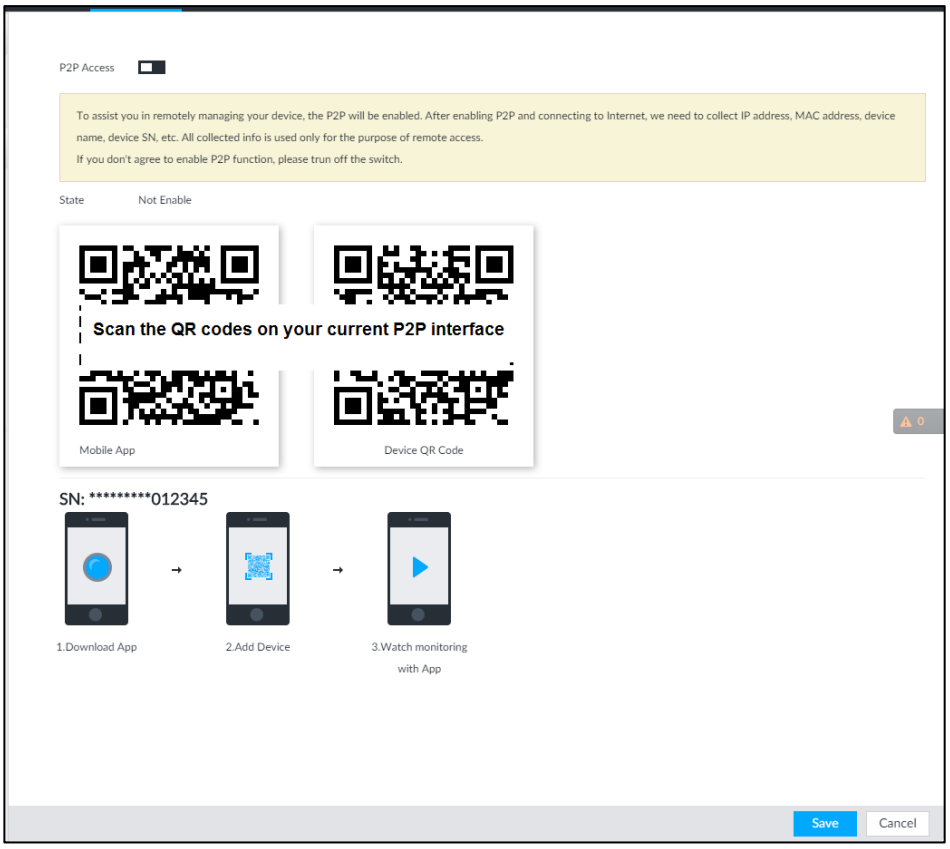
P2P is a peer to peer technology. You can scan the QR code to download cellphone APP without DDNS service or the port mapping or installing the transmission server. After register the device to the APP, you can view the remote video, playback record file and so on.

- Make sure that the system has connected to the network. Otherwise, the P2P function is null.
- When using the P2P function, we will collect device information such as IP address, MAC address, name and serial number. The collected information is only used for remote access.

Step 1 Click , or click on the configuration interface, and then select **NETWORK > Network Apps> P2P**.

The **P2P** interface is displayed. See Figure 6-32. Scan the QR code on the actual interface.

Figure 6-32 P2P



Step 2 Click to enable P2P function.

Step 3 Click **Save**.

After the configuration, you can register a device to the APP to view remote video, playback record file, and so on. See corresponding cellphone APP for detailed information.

After successfully connected to the P2P, the status displayed as Success.

6.3.2.2 DDNS

After setting DDNS parameters, when IP address of EVS changes frequently, the system dynamically updates the relation between domain name and IP address on DNS server. You can use domain name to remotely access EVS, without need to note down IP address.

Preparation

Confirm whether EVS supports the DDNS Type and log in the website provided by the DDNS service provider to register the information such as domain from PC located in the WAN.

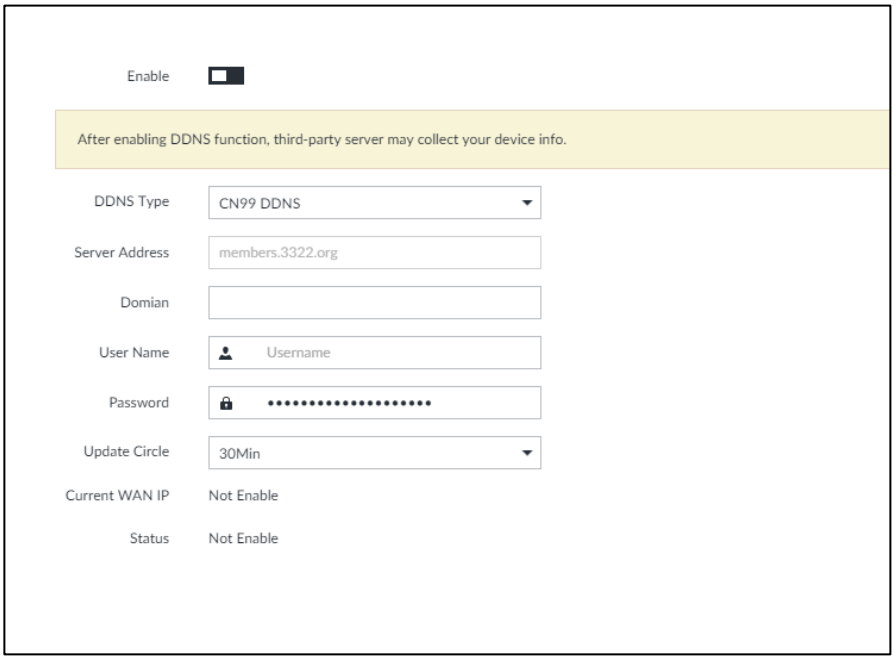
After you have registered and logged in the DDNS website successfully, you can view the information of all the connected devices under this user name.

Procedure

Step 1 Click , or click on the configuration interface, and then select **NETWORK > Basic Network > DDNS**.

The **DDNS** interface is displayed. See Figure 6-33.

Figure 6-33 DDNS



Step 2 Click to enable DDNS function.

After enabling DDNS function, the third-party server might collect your device information. Pay attention to privacy security.

Step 3 Set the corresponding parameters. For details, see Table 6-11.

Table 6-11 DDNS setting parameters description

Parameters	Description
DDNS Type	Name and address of DDNS service provider. ● Dyndns DDNS: members.dyndns.org ● NO-IP DDNS: dynupdate.no-ip.com ● CN99 DDNS: members.3322.org
Server Address	
Domain	The domain name for registering on the website of DDNS service provider.
Username	Enter the user name and password obtained from DDNS service provider. You need to register (including user name and password) on the website of DDNS service provider.
Password	
Update Circle	Enter the amount of time that you want to update the DDNS.
Current WAN IP	Displays the WAN IP address of EVS.
Status	Displays DDNS registration result or update status.

Step 4 Click **Save**.

After successful configuration, enter domain name in address bar of the browser or PCAPP, and press Enter key to access the EVS.

6.3.2.3 Email

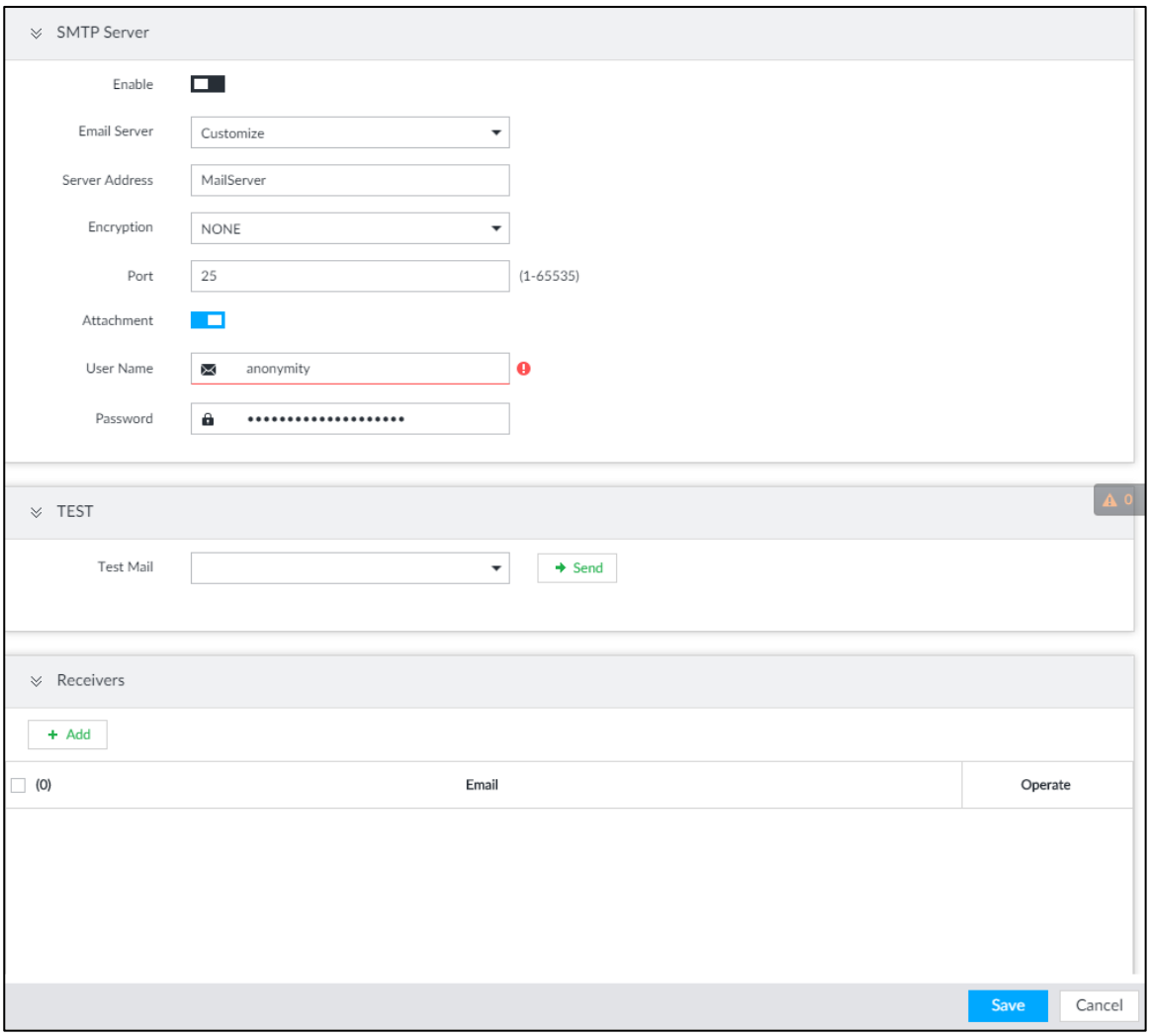
Configure email information, and enable alarm linkage email. When NVR has alarm events, the system automatically sends emails to the user.

Device data will be sent to specific servers after the email function is enabled. Be cautious.

Step 1 Click  , or click  on the configuration interface, and then select **NETWORK > Network Apps > Email**.

The **Email** interface is displayed. See Figure 6-34.

Figure 6-34 Configuring Email



Step 2 Click  to enable the email function.

Step 3 Set parameters.

Table 6-12 EMAIL parameter description

Parameters	Description
Email Server	Select email server type, including Customize, Gmail, Hotmail, and Yahoo.
Server Address	Enter email server address.
Encryption	Select encryption type of email server, including NONE, SSL, and TLS. You are recommended to select TLS. The other encryption methods might not be safe..
Port	Enter the port number of email server. For details, see.
User name and password	Enter the configured user name and password of email server. For details, see.

Step 4 Add the information of email receiver.

1) Click **Add**.

The **Add** interface is displayed.

2) Enter a receiver email address. See Figure 6-35.

Figure 6-35 Email address

3) Click **Add** or  to add other receiver email address.

- Click  to delete the added receiver.
- Select a receiver. The **Delete** button is displayed. Click **Delete** button to delete the selected receiver.

Step 5 Click **Save**.

Step 6 (Optional) Test the email sending function.

1) In **Test Mail,** select or enter a receiver email address.
2) Click **Send**.
   - When the configuration is correct, the system pops up a message of success, and the receiver will receive the test mail.
   - Otherwise, the system pops up a message of failure, and the receiver will not receive the test mail.

6.3.2.4 SNMP

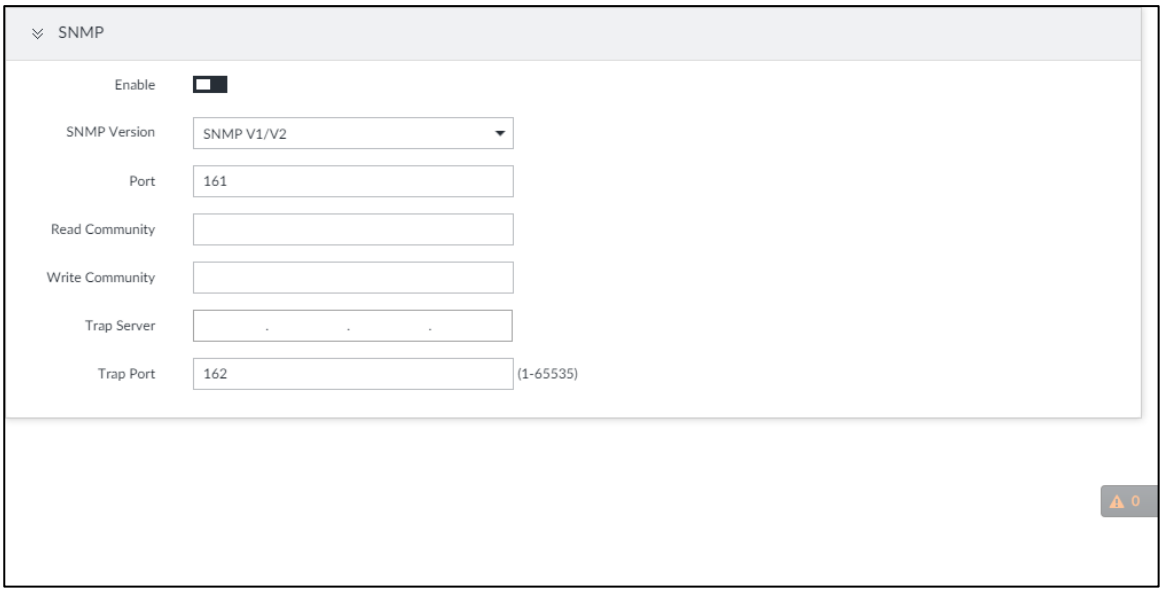
After setting SNMP (Simple Network Management Protocol) and successfully connecting devices through relevant software tools such as MIB Builder, and MG-SOFT MIB Browser, you can directly manage and monitor devices on software tools.

- Install SNMP device monitoring and management tools, such as MIB Builder and MG-SOFT MIB Browser.
- Obtain the MIB file corresponding to the current version from technical support.

Step 1 Click  , or click  on the configuration interface, and then select **NETWORK >Network Apps > SNMP**.

The **SNMP** interface is displayed. See Figure 6-36.

Figure 6-36 SNMP (1)



Step 2 Click  to enable the function.

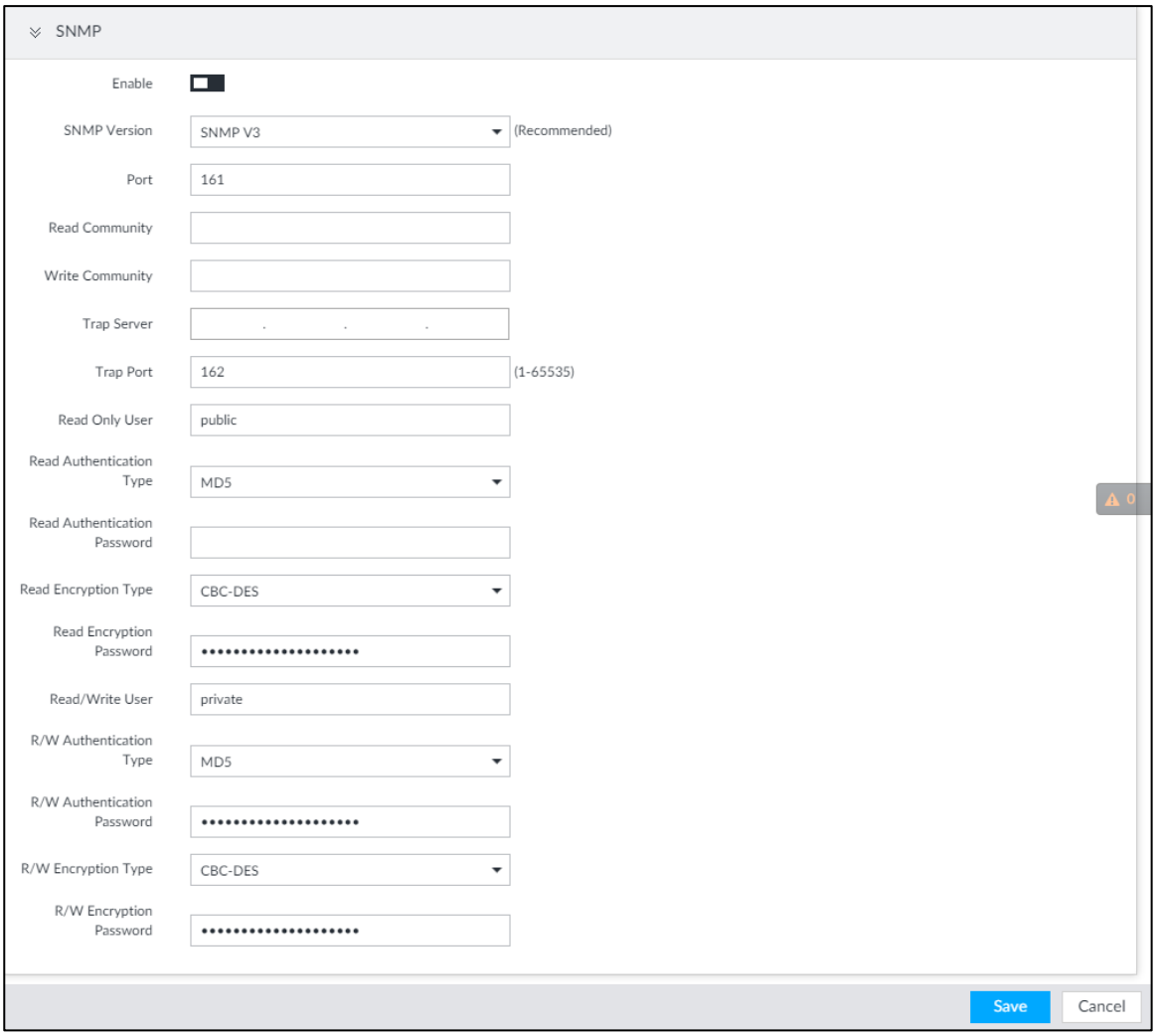
Step 3 Select SNMP version.

- If you have selected SNMP V1/V2, see Figure 6-36.

  SNMP V1/V2 has security risks. You are recommended to use SNMP V3.

- If you have selected SNMP V3, see Figure 6-37.

Figure 6-37 SNMP(2)



Step 4 Set parameters. For Trap server address, enter the IP address of the PC that has MG-SOFT MIB Browser. Keep the other parameters as default. For detailed description, see Table 6-13.

Table 6-13 SNMP parameters

Parameters	Description
Port	Listening port of agent programs on the device.
Read Community, Write Community	Read or Write Community supported by the agent programs. The name can only contain numbers, letters, underscores, and middle lines.
Trap Server	The destination address of Trap information sent by the agent program.
Trap Port	The destination port of Trap information sent by the agent program.
Read Only User	Set the username the read-only user. The read-only user can only have the read-only permission. The name can only contain numbers, letters, and underscores.

Parameters	Description
Read Authentication Type	You can select MD5 or SHA. It is MD5 by default.
Read Authentication Passwrod	The password must contain at least 8 digits.
Read Encryption Type	CFB-AES by default.
Read Encryption Password	The password must contain at least 8 digits.
Read/Write User	The username is *private* by default. If you log in using this username, you have the read-and-write permission. The name can only contain numbers, letters, and underscores.
R/W Authentication Type	You can select MD5 or SHA. It is MD5 by default.
R/W Authentication Passwrod	The password must contain at least 8 digits.
R/W Encryption Type	CFB-AES by default.
R/W Encryption Password	The password must contain at least 8 digits.

Step 5 Click **Save**.

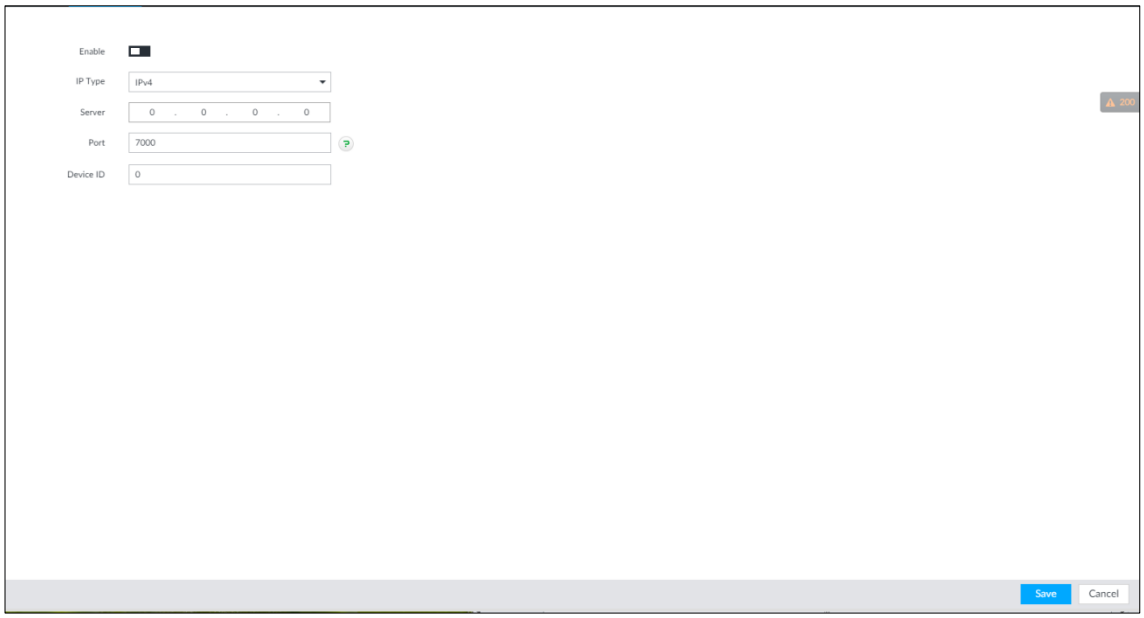
6.3.2.5 Register

Register the device on designated proxy server, and client software visits the device through the proxy server.

Step 1 Click  , or click  on the configuration interface, and then select **NETWORK > Network Apps > Register**.

The **REGISTER** interface is displayed. See Figure 6-38.

Figure 6-38 Register



Step 2 Click  to enable the function.

Step 3 Set parameters. For details, see Table 6-14.

Table 6-14 Register

Parameters	Description
IP Type	Select IP address of server for registration.
Server	In the Server box, enter the IP address of server for registration.
Port	Enter the port number of the server for registration.
Device ID	Enter Device ID to identify EVS uniquely. Device ID shall be consistent with server configuration.

Step 4 Click **Save**.

6.3.2.6 UPnP

Through the UPnP (Universal Plug and Play) protocol, you can establish a mapping relationship between the LAN and the WAN, the WAN user can use the WAN IP address to directly access the device in the LAN.

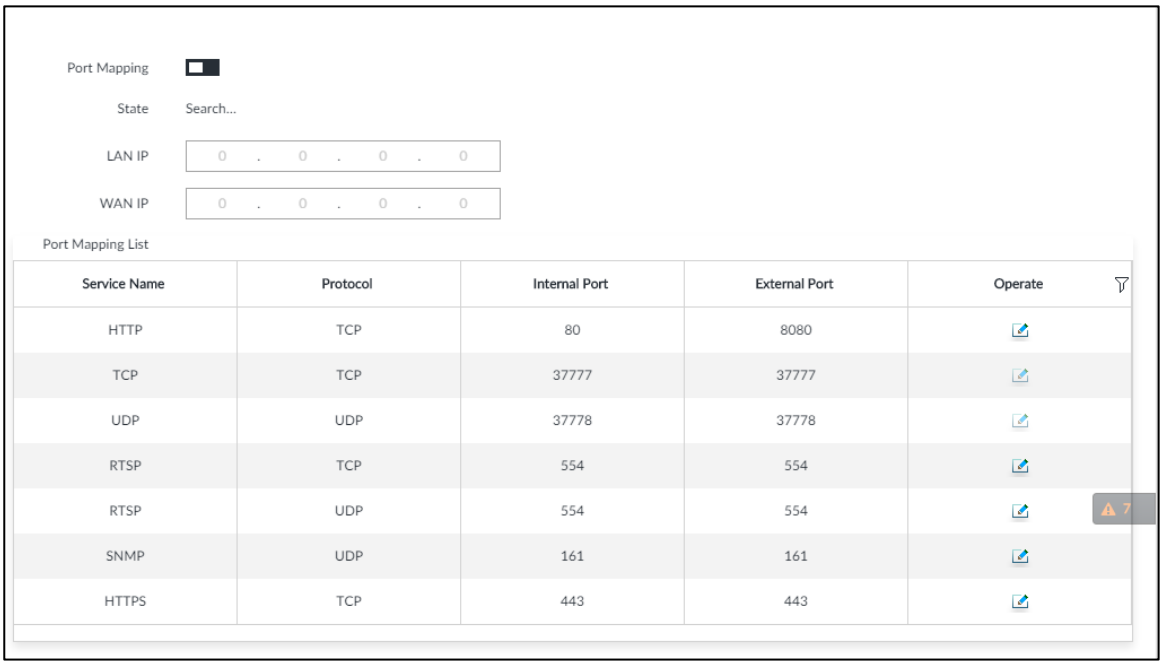
Device services and ports will be mapped to the public network after UPnP is enabled. Be cautious

- Make sure that your PC has UPnP network services installed.
- Log in to the router and set the WAN port IP address of router.
- Enables the UPnP function on the router.
- Connect the device to the router LAN (Local Area Network, LAN) port.
- Select **NETWORK >Basic Network >TCP/IP**, and then set the IP address to be the private-network IP of the router, or select DHCP to automatically obtain the IP address.

Step 1 Click , or click on the configuration interface, and then select **NETWORK > Network Apps > UPnP**.

The **UPnP** interface is displayed. See Figure 6-39.

Figure 6-39 UPnP



Step 2 Set parameters. For details, see Table 6-15.

Table 6-15 UPnP parameters

Parameters	Description
Port Mapping	Click to enable UPnP.
State	The status of port mapping.
LAN IP	The LAN IP address of router. The IP address is automatically obtained after the mapping succeeds.
WAN IP	The WAN IP address of router. The IP address is automatically obtained after the mapping succeeds.
Port Mapping List	The list is consistent with the UPnP port mapping list on the router. ● Internal Port: The EVS port to be mapped on the router. ● External Port: The WAN port of the internal port. ● When setting the external port, use the ports between 1024 and 5000, and do not use the well-known ports 1 to 255 and the system ports 256 to 1023, so as to avoid conflicts. ● When there are multiple devices within the LAN, properly plan the port mapping to avoid conflicts of WAN ports.. ● When making a port mapping, make sure that the port you are mapping is not occupied or restricted. ● The TCP/UDP WAN and LAN ports must be consistent and cannot be modified.

Parameters	Description
Modification	Click  , and then you can modify the external port.

Step 3 Click **Save**.

Enter *http://WAN IP: WAN port number* in the browser to access the device with the corresponding port number in the router network.

6.3.2.7 Multicast

When multiple users are viewing live video of the same device at the same time, it might cause failure due to limited bandwidth. To solve this problem, you can set a multicast IP address (224.0.0.0–239.255.255.255) for the Device.

Step 1 Click  , or click  on the configuration interface, and then select **NETWORK > Network Apps > Multicast**.

The **Multicast** interface is displayed. See Figure 6-40.

Figure 6-40 Multicast

Step 2 Click  to enable multicast.

Step 3 Set parameters. See Table 6-16.

Table 6-16 Parameters

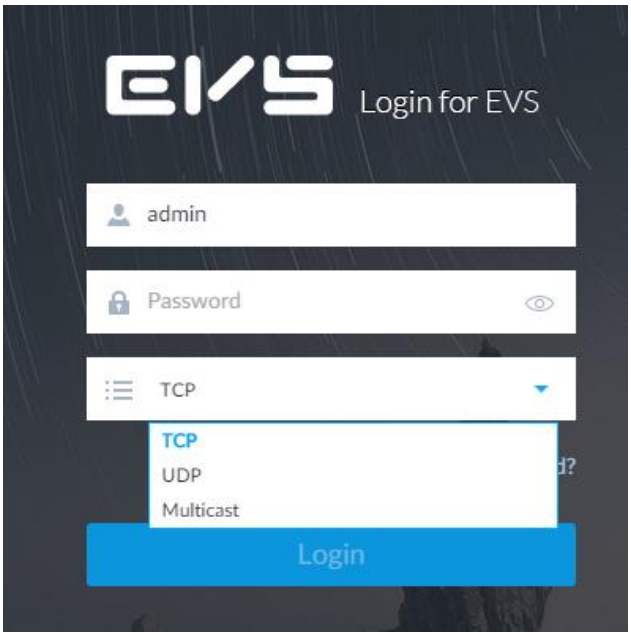
Parameters	Description
IP Address	Set the multicast IP address of the device(224.0.1.0–239.255.255.255).
Port	Set the multicast port (1025–65000).

Step 4 Click **Save**.

After configuring the multicast address and port, you can log in to the web interface or PCAPP client through the multicast protocol.

Take PCAPP for example. On the login interface of PCAPP, select **Multicast** as the login type. See Figure 6-41. The PCAPP client will automatically obtain the multicast address and join the multicast group. After login, you can view live videos through multicast protocol.

Figure 6-41 Log in through multicast



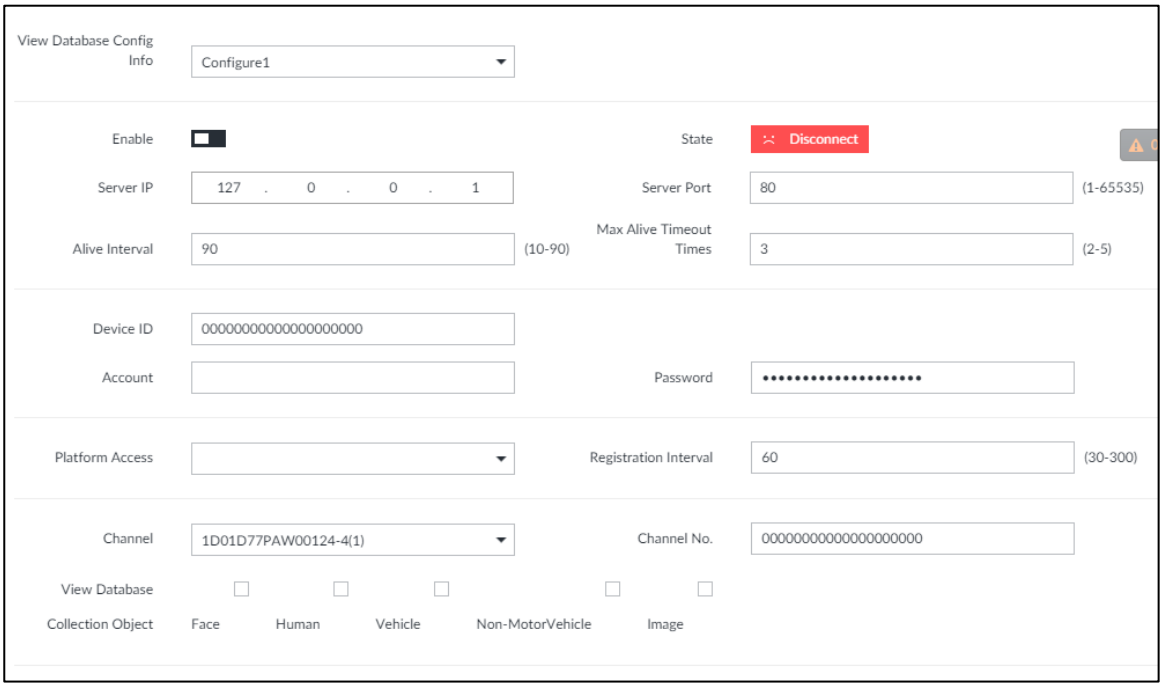
6.3.2.8 GAVI

The device is connected to the server supporting view database, and after the connection, the server can collect information from the device, which is divided into human, face, motor vehicle, non-motor vehicle and image.

Step 1 Click , or click on the configuration interface, and then select **NETWORK > Network Apps > GAVI**.

The **GAVI** interface is displayed. See Figure 6-42.

Figure 6-42 GAVI



Step 2 Select vide database config info, and enable it.

Configure 1 and Configure 2 refers to two platforms. The device can connect 2 servers at the same time.

-  indicates that the device is not connected to the platform server.
-  indicates that the device is connected to the platform server.

Step 3 Set parameters. See Table 6-17.

Table 6-17 Parameters

Parameters	Description
Server IP	Video database server IP.
Server Port	Video database server port. It is 80 by default. This port must be consistent with the server port.
Alive Interval	The interval of heartbeat between vide database and server. It is 90 seconds by default.
Max Alive TimeoutTimes	Set the number of heartbeat timeout times between the device and view database. After the defined the times of timeout, the device disconnects with the server. It is 3 times by default.
Device ID	The ID given by the server. IDs or devices are unique.
Account	Username and password of the view database server.
Password	
Platform Access	The access protocol between the device and platform server.
Registration Interval	The device keeps sending registration requests to the platform at the pre-defined interval if it failed to register for the first time. The registration interval is 30 seconds to 300 seconds.
Channel	Select a channel and set channel number for it. Channel: For a multi-channel device, you can select the specific channels to collect information; for a single-channel device, the channel number is 0 bydefault. Channel No.: Set the number of channel, so as to differentiate the channels.
Channel No.	
View Database Collection Object	Set the information types that the server needs to collect from the device through view database.

Step 4 Click **Save**.

6.4 Event Management

Click  or click  on the configuration interface, select **EVENT**. The **EVENT** interface is displayed.

On the interface, configure alarm event, including alarm event of EVS and remote device.

- Select the root node  in the resource tree on the left to set alarm event of the Device. See "6.4.2 Local Device" for detailed information.
- Select remote device in the device tree on the left, to set alarm event of this remote device. See "6.4.3 Remote Device" for detailed information.

- The alarm event might be different depending on the model you purchased. The actual interface shall prevail.
- means that the corresponding alarm event has been enabled.

6.4.1 Alarm Actions

System can trigger the corresponding actions when an alarm occurs.

The supported actions might be different depending on the model you purchased. The actual interface shall prevail.

On the alarm configuration interface, click **Actions** to display actions. See Table 6-18 for detailed information. Configure actions according to your actual need.

- After setting actions, click **Save** on the interface.
- After enabling actions, click to disable the corresponding actions.

Table 6-18 Actions description

Actions	Description	Preparation
Record	The system links the selected remote device to record when there is a corresponding alarm event.	Remote device, such as IPC, has been added. See "3.4.2 Adding Remote Device" for detailed information.
Buzzer	The system activates a buzzer alarm when there is a corresponding alarm event.	–
Log	The system notes down the alarm information in the log when there is a corresponding alarm event.	–
Email	The system sends alarm email to all added receivers when there is corresponding an alarm event.	Email configuration has been completed. See "6.3.2.3 Email" for detailed information.
Snapshot	The system takes snapshots of the linked channel hen there is corresponding an alarm event.	–
Preset	The system links the selected remote device to rotate to the designated preset point when there is a corresponding alarm event.	PTZ device has been added, and preset point has been added. See "3.4.2 Adding Remote Device" for detailed information.
IPC Alarm Output Settings	When there is an alarm, system can trigger the corresponding device to generate alarm.	IPC has been added, and IPC is connected with alarm output device. See "3.4.2 Adding Remote Device" for detailed information.

Actions	Description	Preparation
Access	When there is an alarm, system can trigger the corresponding access control device to open door and close door.	See "3.4.2 Adding Remote Device" for detailed information.
Smart tracking	Alarm is triggered when a tripwire or intrusion behavior is detected. If smart tracking action is configured, the PTZ camera automatically rotates to the target view to track it.	See "6.4.1.9 Smart Tracking."

6.4.1.1 Record

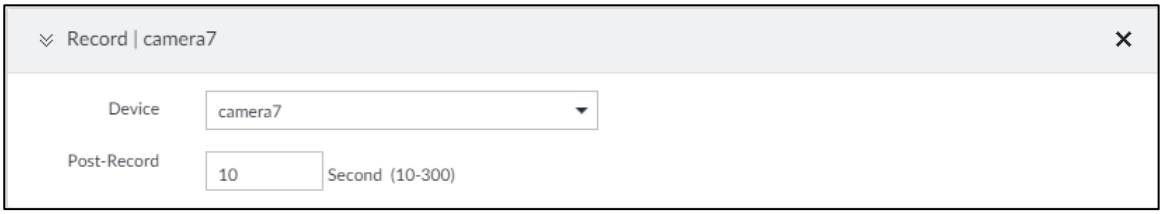
Enable record control function. The system links the selected remote device to record when there is corresponding alarm event.

Make sure that the remote device, such as IPC, has been added. See "3.4.2 Adding Remote Device" for detailed information.

Step 1 Click **Actions**, and then select **Record.**

The record setting interface is displayed. See Figure 6-43.

Figure 6-43 Record



Step 2 Set the time length of recording after the event moment.

Step 3 (Optional) Repeat Step 1–Step 2 to link multiple remote devices to record.

6.4.1.2 Buzzer

The system activates a buzzer alarm when there is corresponding alarm event.

Click **Actions** and select **Buzzer** to enable this function. See Figure 6-44.

Figure 6-44 Buzzer

6.4.1.3 Log

Enable the log function. The system notes down the alarm information in the log when there is corresponding alarm event.

Click **Actions** and select **Log** to enable this function. See Figure 6-45.

Figure 6-45 Log

When log function is enabled, after an alarm is triggered, click + on **LIVE** interface, select **MAINTAIN > Log > Event**.

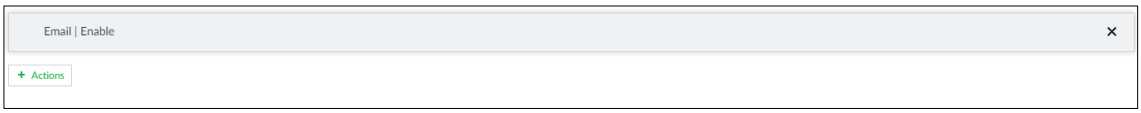
6.4.1.4 Email

Enable email function. The system sends alarm email to all added receivers when there is corresponding alarm event.

Make sure that the Email configuration has been completed. See 6.3.2.3 Email for detailed information.

Click **Actions** and select **Email** to enable this function. See Figure 6-46.

Figure 6-46 Email



6.4.1.5 Preset

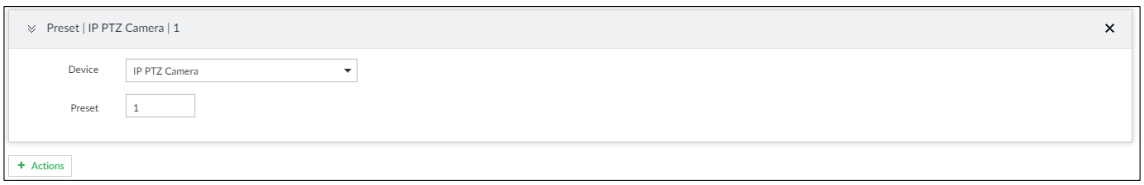
Set preset function. The system links the selected remote device to rotate to the designated preset point when there is corresponding alarm event.

Make sure that the PTZ device has been added, and preset has been added. See "3.4.2 Adding Remote Device" for detailed information.

Step 1 Click **Actions** and select **Preset.**

The **Preset** interface is displayed. See Figure 6-47.

Figure 6-47 Preset



Step 2 Select PTZ device, and enter preset number.

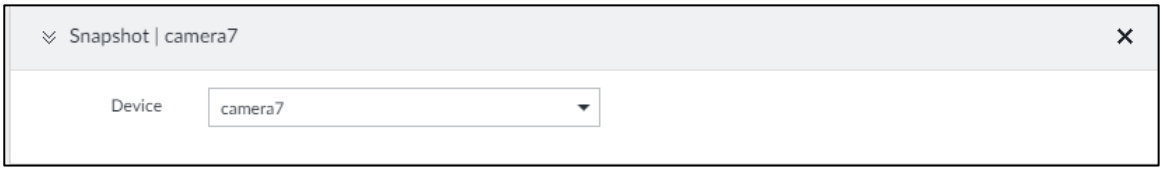
Step 3 (Optional) Repeat Step 1–Step 2, and link multiple PTZ devices to turn to designated presets.

6.4.1.6 Snapshot

Set the snapshot linkage action for alarms, so that once an alarm happens, it will triggered a snapshot of the alarm.

Click **Actions**, and then select **Snapshot**. The **Snapshot** interface is displayed. See Figure 6-48.

Figure 6-48 Snapshot action



6.4.1.7 IPC Alarm Out

Set IPC alarm output. System can trigger the corresponding alarm output device when an alarm occurs.

Make sure that the IPC has been added, and IPC is connected with alarm output device. See "3.4.2 Adding Remote Device" for detailed information.

Step 1 Click Actions and select IPC Alarm Out.

The **IPC Alarm Out** interface is displayed. See Figure 6-49.

Figure 6-49 IPC alarm output settings

Step 2 Select IPC and alarm output port.

You can select multiple alarm output ports.

Step 3 (Optional) Repeat Step 1–Step 2, and link multiple IPC alarm output devices.

6.4.1.8 Access

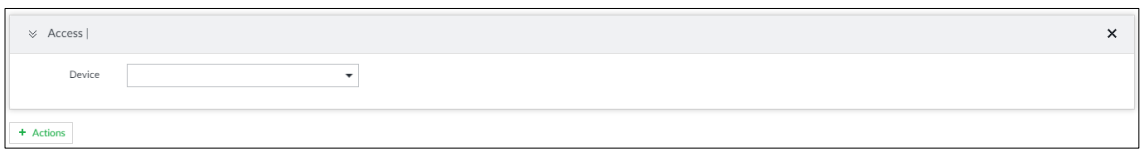
Set access control function. When there is an alarm, system can trigger the corresponding access control device to open door and close door.

Make sure that access control device has been added. See "3.4.2 Adding Remote Device" for detailed information.

Step 1 Click **Actions** and select **Access.**

The **Access** setting interface is displayed. See Figure 6-50.

Figure 6-50 Access



Step 2 Select access control device.

Not all models support this function. The actual interface shall prevail.

Step 3 (Optional) Repeat Step 1–Step 2, and link multiple access control devices.

6.4.1.9 Smart Tracking

Alarm is triggered when a tripwire or intrusion behavior is detected. If smart tracking action is configured, the PTZ camera automatically rotates to the target view to track it.

On the event configuration interface, select **Actions > Smart Tracking** to enable the action.

6.4.2 Local Device

Set EVS alarm event, including abnormal event, device offline alarm, AI plan, and local device alarm.

6.4.2.1 Abnormal Event

Set the alarm mode when an abnormal event occurs.

The Device supports HDD, storage error, network, AI module, fan and power fault alarm. For details, see Table 6-19.

Table 6-19 Abnormal event description

Name	Description
No HDD	System triggers an alarm when there is no HDD. It is enabled by default.
Storage error	System triggers an alarm in case of HDD error, RAID degrade, RAID broken, and storage pool error. It is enabled by default.
Storage space full	System triggers an alarm when the used storage space reaches the pre-defined threshold. It is disabled by default. The alarm is valid only when the storage mode is set as **Stop** on the **Local Hard Disk** interface. For details, see "6.5.1.4 Setting Storage Strategy."
IP conflict	System triggers an alarm when its IP address conflicts with IP address of other device in the same LAN. It is enabled by default.
MAC conflict	System triggers an alarm when its MAC address conflicts with MAC address of other device in the same LAN. It is enabled by default.
Lock in	System triggers an alarm when an account login error has reached the threshold. At the same time, system locks current account. It is disabled by default. Go to the **Security** interface to set account error threshold. See "6.6.3 Safety Protection" for detailed information.
AI module temp	When AI module temperature is higher than the specified value, system triggers an alarm. It is enabled by default.
AI module offline	When AI module and system is disconnected, system triggers an alarm. It is enabled by default.
Fan speed alarm	When EVS fan speed is abnormal, system triggers an alarm. It is enabled by default.
Power fault	When EVS power supply is abnormal, system triggers an alarm. It is disabled by default.

Here we take AI module temp for example. For other events, the setting steps are similar. See the actual interface for detailed information.

Step 1 Click , or click on the configuration interface, and then select **EVENT**.

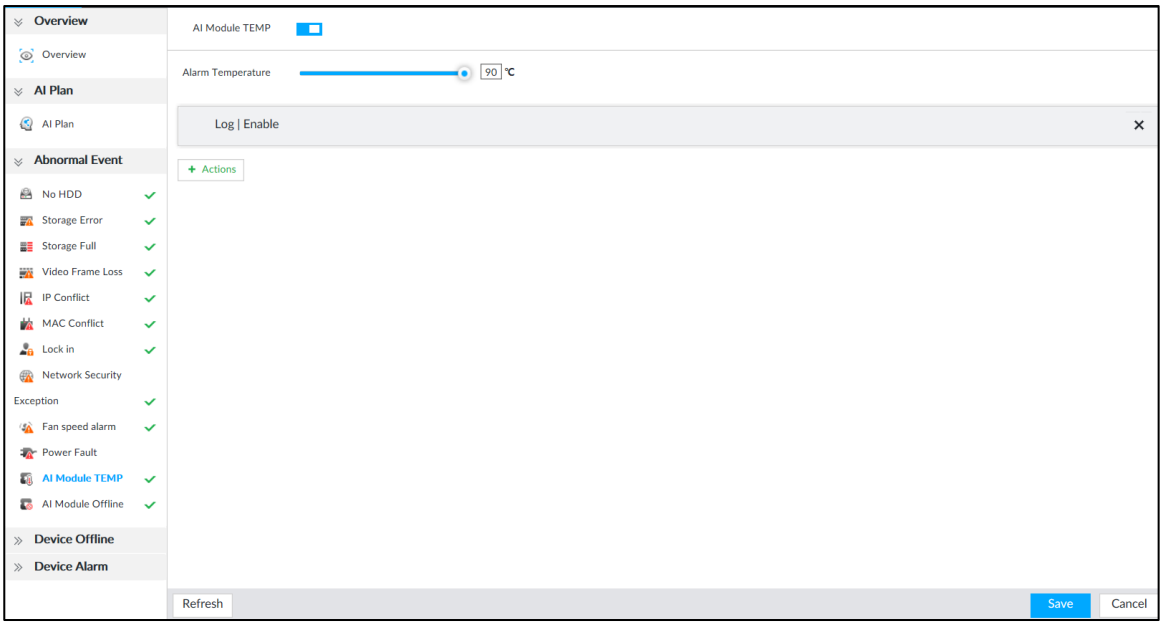
The **EVENT** interface is displayed.

Step 2 Select the root node in the device tree.

Step 3 Select **Abnormal Event > AI Module TEMP**.

The **AI Module TEMP** interface is displayed. See Figure 6-51.

Figure 6-51 AI module temp



Step 4 Click to enable AI module temperature alarm function.

Step 5 Drag to set alarm temperature threshold.

The above step is for AI module temperature alarm only.

Step 6 Click **Actions** to set alarm actions. See "6.4.1 Alarm Actions" for detailed information.

Step 7 Click **Save**.

6.4.2.2 Offline Alarm

Set EVS network offline alarm. If you have not set offline alarm for a specified remote device, once the remote device is disconnect from the system, system adopts EVS alarm strategy to trigger an alarm.

Step 1 Click , or click on the configuration interface, and then select **EVENT**.

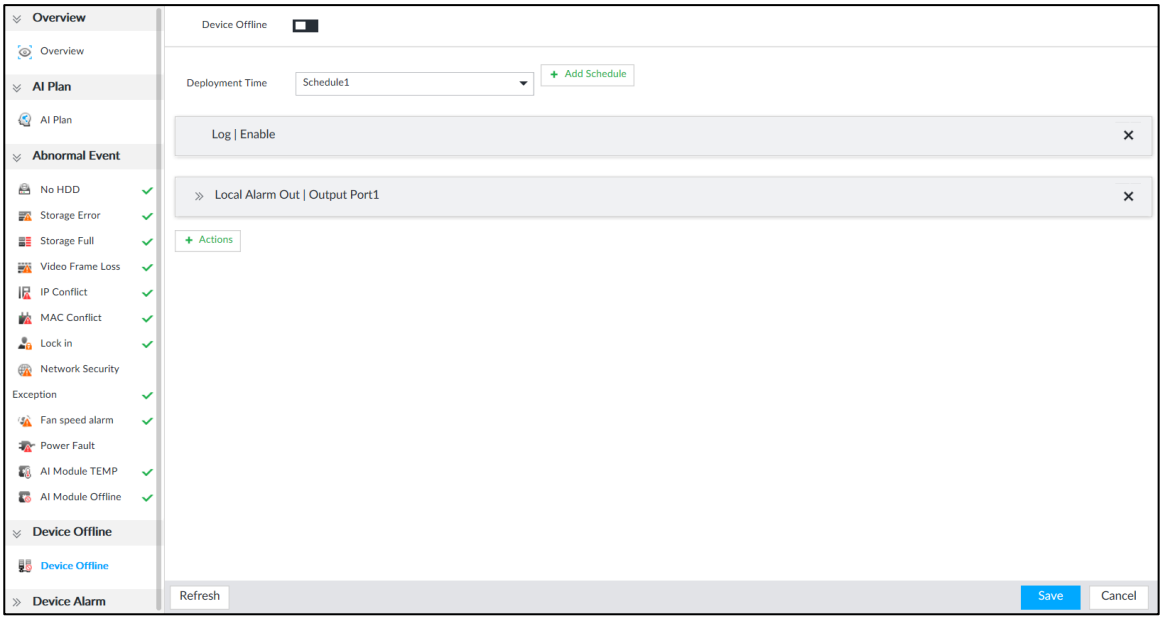
The **EVENT** interface is displayed.

Step 2 Select the root node in the device tree on the left.

Step 3 Select **Device Offline > Device Offline**.

The **Device Offline** interface is displayed. See Figure 6-52.

Figure 6-52 Offline alarm



Step 4 Click  to enable device offline alarm.

Step 5 Click **Deployment Time** to select schedule from the drop-down list.

After setting deployment period, system triggers corresponding operations when there is a motion detection alarm in the specified period.

- Click **View Schedule** to view detailed schedule settings.
- If the schedule is not added or the added schedule does not meet actual needs, click **Add Schedule**. See "6.8.3 Schedule" for detailed information.

Step 6 Click **Actions** to set alarm actions. See "6.4.1 Alarm Actions" for detailed information.

Step 7 Click **Save**.

6.4.2.3 Configuring AI Plan

Configure AI detection result display strategy of EVS. If you have not set AI display settings for current remote device, the remote device inherits AI display mode of EVS.

6.4.2.3.1 Viewing AI Plan

After adding remote device, on EVS, obtain AI detection type and status of the remote device.

On the **EVENT** interface, select the root node in the device tree on the left. Select **AI Plan > AI Plan > AI Plan**. The **AI Plan** interface is displayed.

After installing the AI module, and the remote device supports AI detection, and you have enabled the AI detection function, you can view channel name of the remote device on the corresponding AI detection panel.

6.4.2.3.2 Setting AI Display

Set the property that shall be displayed in rule box and feature property panel. View AI detection result through smart preview, and support to display face, human and vehicle.

Take the procedure of configuring face detection AI display as an example. For other AI detection functions, the procedures are similar.

Step 1 Click , or click on the configuration interface, and then select **EVENT**.

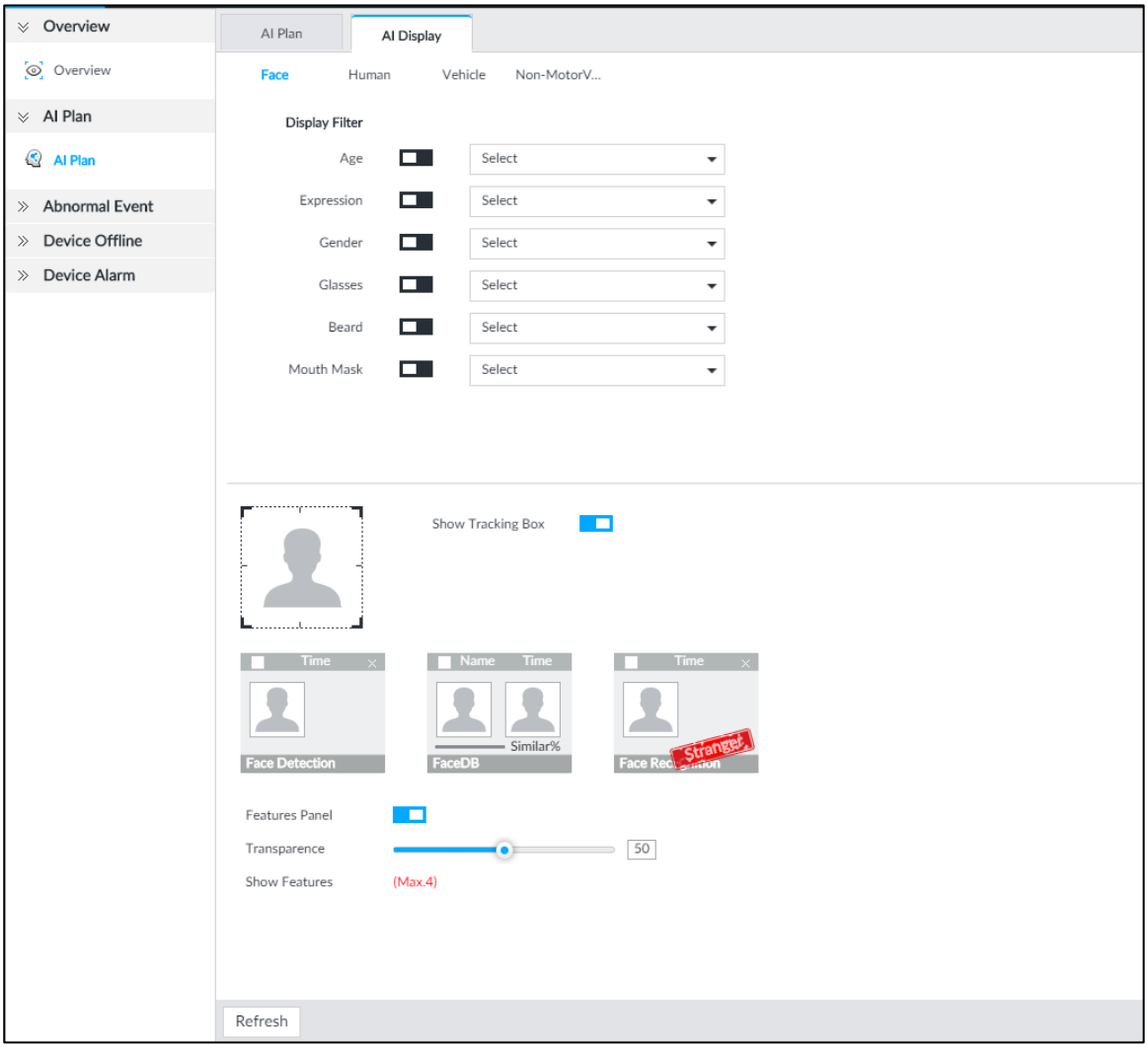
The **EVENT** interface is displayed.

Step 2 Select the root node in the device tree on the left.

Step 3 Select **AI Plan > AI Plan > AI Display > Face**.

The **Face** interface is displayed. See Figure 6-53.

Figure 6-53 Face



Step 4 Configure display filter information.

After setting filter criteria, only the qualified detection result will be displayed. For example, enable Age, and then select youth from the drop-down list. The tracking box and the features panel only display the human face of the youth age.

1) Click to enable corresponding filter type.

2) Set display filter criteria.

Click to set the filter color.

Step 5 Click in the right of **Show Tracking Box** to enable.

After enabled, when the system detects face or human, tracking box will be shown beside the face or human in the view window. See Figure 6-54.

Figure 6-54 Tracking box

Step 6 Click in the right of **Features Panel** to enable, and select the features that shall be displayed on the **LIVE** interface.

After enabled, there is a features panel on the right side of the view window. See Figure 6-55.

- Drag to adjust features panel transparency. The higher the value, the more transparent the features panel.
- System supports maximum 4 features. System has checked four features by default. To select other features, cancel the selected features, and then select the ones you need.
- Click to display the features panel on the **LIVE** interface, including face detection panel, stranger panel and face DB panel.

Figure 6-55 Features panel

Step 7 Click **Save**.

6.4.3 Remote Device

Set alarm actions of remote device, including video detection alarm, offline alarm and AI plan of remote device.

The parameters might be different depending on the model you purchased. The actual interface shall prevail.

6.4.3.1 Video Detect

Video detection function adopts the PC visual, image and graphical processing technology to analyze the video image and check there is considerable changes on the video. Once there are considerable video changes (such as there is any moving object, or the video is blurred), system triggers corresponding alarm event.

6.4.3.1.1 Configuring Video Motion

After analyzing video, system can generate a video motion alarm when the detected moving target reaches the sensitivity you set here.

Step 1 Click , or click on the configuration interface, and then select **EVENT**.

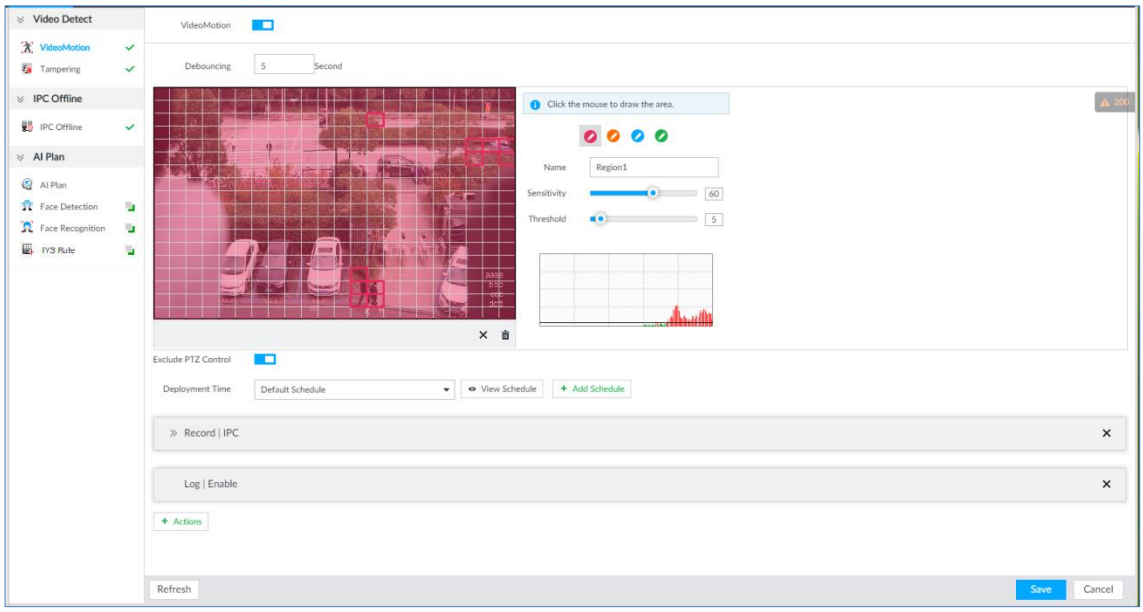
The **EVENT** interface is displayed.

Step 2 Select remote device in the device tree on the left.

Step 3 Select **Video Detect > Video Motion**.

The **Video Motion** interface is displayed. See Figure 6-56.

Figure 6-56 Video motion



Step 4 Click  to enable video motion detection.

Step 5 Set parameters. For details, see Table 6-20.

Table 6-20 Motion detect parameters description

Parameters	Description
Debouncing	System only records one alarm event during the debouncing period.
Exclude PTZ control	After enabling exclude PTZ control, system does not trigger an alarm when you are manually control the PTZ. It is for PTZ camera only.

Step 6 Set motion detection region.

System supports maximum four detection zones. After setting, once there is an alarm from any of these four zones, the remote device trigger an alarm.

1) Click motion detection zone icon  .
2) On the surveillance video, press and hold on the left button of mouse to select detection zone.
   - Select the motion detect zone you have drawn. Click  to delete the zone.
   - Click  to clear the zone you have drawn.
3) Set parameters. For details, see Table 6-21.

Table 6-21 Description of zone parameters

Parameters	Description
Name	Set detection zone name to distinguish different zones.

Parameters	Description
Sensitivity	Drag to set sensitivity. The higher the sensitivity is, the easier it is to trigger an alarm. At the same time, the false alarm rate increases as well. Usually we recommend the default value.
Threshold	Drag to adjust threshold. Once the detected percentage (the percentage of target to detection zone) is equivalent to or larger than the specified threshold, system triggers alarm. For example, the threshold is 10. Once the detected target occupies the 10% of the detection zone, system triggers an alarm.

Step 7 Click **Deployment Time** to select schedule from the drop-down list.

After setting deployment period, system triggers corresponding operations when there is a motion detection alarm in the specified period.

- Click **View Schedule** to view detailed schedule settings.
- If the schedule is not added or the added schedule does not meet actual needs, click **Add Schedule**. See "6.8.3 Schedule" for detailed information.

Step 8 Click **Actions** to set alarm actions. See "6.4.1 Alarm Actions" for detailed information.

Step 9 Click **Save**.

6.4.3.1.2 Tampering

Once something tampers the surveillance video, and the output video is in one color, the system can generate an alarm.

Step 1 Click , or click on the configuration interface, and then select **EVENT**.

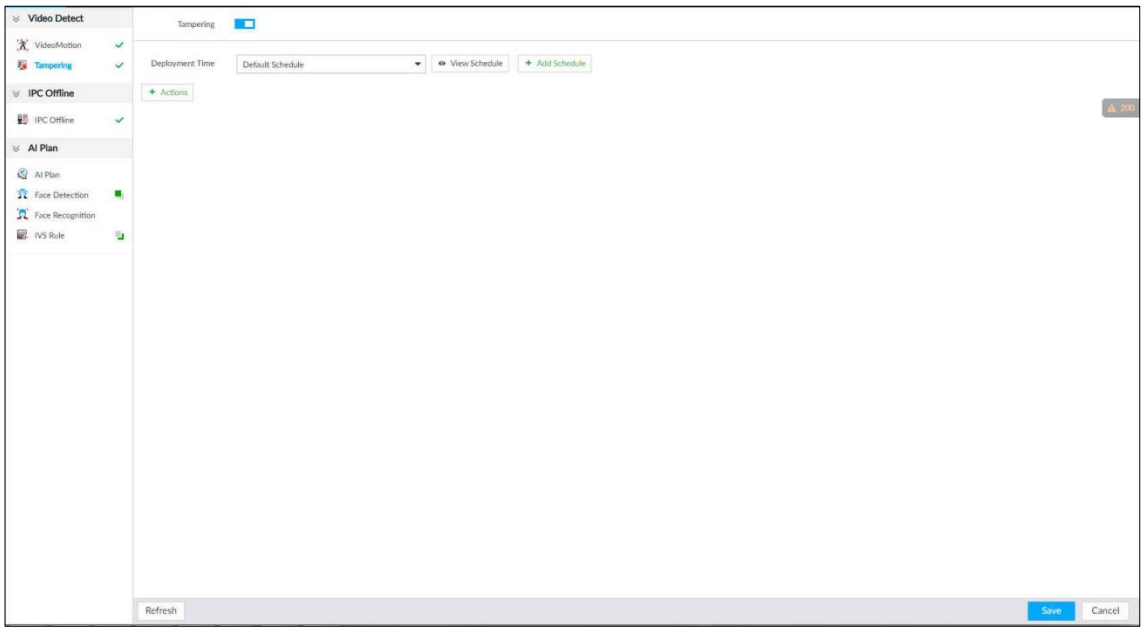
The **EVENT** interface is displayed.

Step 2 Select remote device in the device tree on the left.

Step 3 Select **Video Detect > Tampering**.

The **Tampering** interface is displayed. See Figure 6-57.

Figure 6-57 Tampering



Step 4 Click  to enable tampering alarm.

Step 5 Click **Deployment Time** to select schedule from the drop-down list.

After setting deployment period, system triggers corresponding operations when there is a motion detection alarm in the specified period.

- Click **View Schedule** to view detailed schedule settings.
- If the schedule is not added or the added schedule does not meet actual needs, click **Add Schedule**. See "6.8.3 Schedule" for detailed information.

Step 6 Click **Actions** to set alarm actions. See "6.4.1 Alarm Actions" for detailed information.

Step 7 Click **Save**.

6.4.3.2 Offline Alarm

When the remote device and the EVS are disconnected, system can trigger an alarm.

Step 1 Click  , or click  on the configuration interface, and then select **EVENT**.

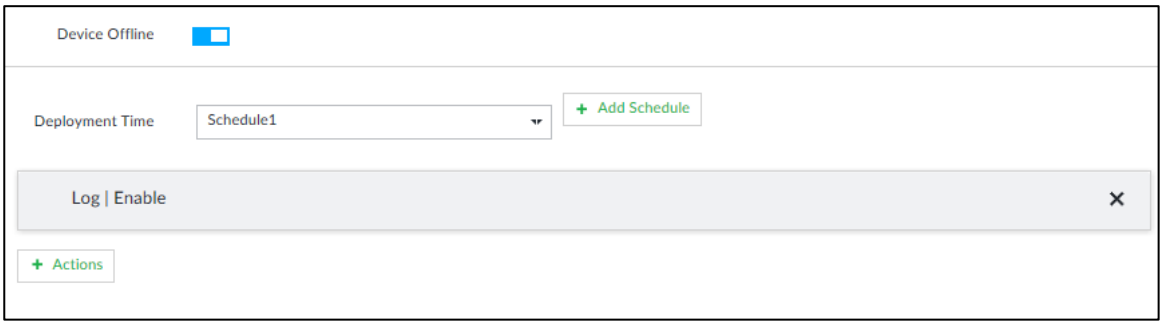
The **EVENT** interface is displayed.

Step 2 Select a remote device in the device tree on the left.

Step 3 Select **Device Offline > Device Offline**.

The **Device Offline** interface is displayed. See Figure 6-58.

Figure 6-58 IPC offline



Step 4 Click  to enable offline alarm.

The device offline alarm is enabled by default. You can skip this step.

Step 5 Click **Deployment Time** to select schedule from the drop-down list.

After setting deployment period, system triggers corresponding operations when there is a device offline alarm in the specified period.

- Click **View Schedule** to view detailed schedule settings.
- If the schedule is not added or the added schedule does not meet actual needs, click **Add Schedule**. See "6.8.3 Schedule" for detailed information.

Step 6 Click **Actions** to set alarm actions. See "6.4.1 Alarm Actions" for detailed information.

Step 7 Click **Save**.

6.4.3.3 IPC External Alarm

Set IPC alarm input event, so that when there is an alarm input to the IPC, IPC uploads the alarm to the Device. If the camera has multiple IO channels, you can set the alarm input event for each of them as you might need.

Step 1 Click , or click on the configuration interface, and then select **EVENT**.

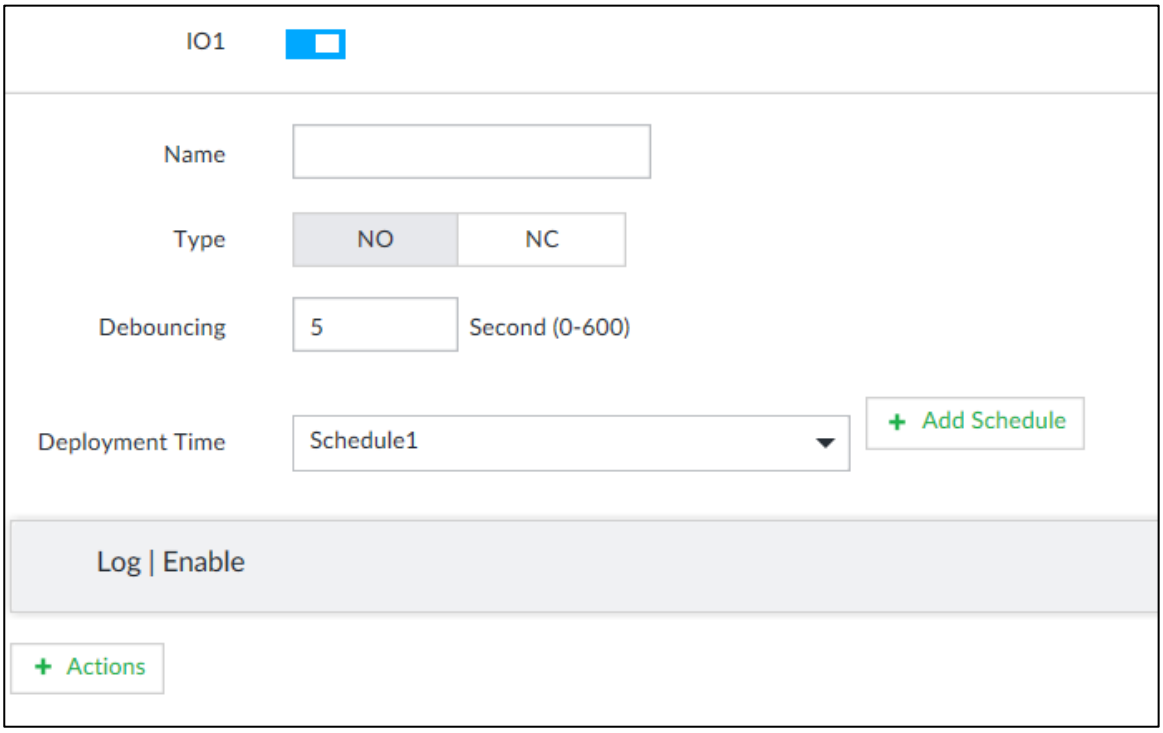
The **EVENT** interface is displayed.

Step 2 Select a remote device in the device tree on the left.

Step 3 Select **External Alarm > IO1**.

The **IO1** interface is displayed. See Figure 6-59.

Figure 6-59 IO1



Step 4 Click to enable the alarm.

Step 5 Set parameters. For details, see Table 6-22.

Table 6-22 Local alarm parameters description

Parameters	Description
Name	In the Alarm name box, enter a name for the alarm.
Type	Select alarm input device type. Both NO and NC are supported.
Debouncing	The system records only one event during this period.

Step 6 Click **Deployment Time** to select schedule from the drop-down list.

After setting deployment period, system triggers corresponding operations when there is a motion detection alarm in the specified period.

- Click **View Schedule** to view detailed schedule settings.
- If the schedule is not added or the added schedule does not meet actual needs, click **Add Schedule**. See "6.8.3 Schedule" for detailed information.

Step 7 Click **Actions** to set alarm actions. See "6.4.1 Alarm Actions" for detailed information.

Step 8 Click **Save**.

6.4.3.4 Thermal Alarm

- Alarm types vary depending on the models of thermal cameras. The actual interface shall prevail.
- Make sure that configurations of thermal detections such as fire detection and temperature detection have been done on the thermal camera.

Support the following thermal camera alarms. See Table 6-23.

Table 6-23 Thermal alarms

Function	Description
Fire alarm	When the thermal camera detects a fire, the alarm signal is transmitted to the EVS device, which performs an alarm linkage action.
Temperature alarm	When the thermal camera detects that the temperature is above or below the threshold value, the alarm signal is transmitted to the EVS device, which performs an alarm linkage action.
Temperature difference alarm	When the thermal camera detects a temperature difference greater than the set value, the alarm signal is transmitted to the EVS device, and the EVS device will perform an alarm linkage action.
Hot spot alarm	When the maximum temperature detected by the thermal camera is higher than the set value, the alarm signal is transmitted to the EVS device, and the EVS device will perform an alarm linkage action.
Cold spot alarm	When the lowest temperature detected by the thermal camera is below the set value, the alarm signal is transmitted to the EVS device, and the EVS device will perform an alarm linkage action.

Take the procedure of configuring fire alarm as an example. The procedures are similar, and the actual interface shall prevail.

Step 1 Click , or click on the configuration interface, and then select **EVENT**.

The **EVENT** interface is displayed.

Step 2 Select the root node in the device tree on the left.

Step 3 Select **Thermal Alarm > Fire Alarm**.

The **Fire Alarm** interface is displayed.

Step 4 Click **Deployment Time** to select schedule from the drop-down list.

After setting deployment period, system triggers corresponding operations when there is a motion detection alarm in the specified period.

- Click **View Schedule** to view detailed schedule settings.
- If the schedule is not added or the added schedule does not meet actual needs, click **Add Schedule**. See "6.8.3 Schedule" for detailed information.

Step 5 Click **Actions** to set alarm actions. See "6.4.1 Alarm Actions" for detailed information.

Step 6 Click **Save**.

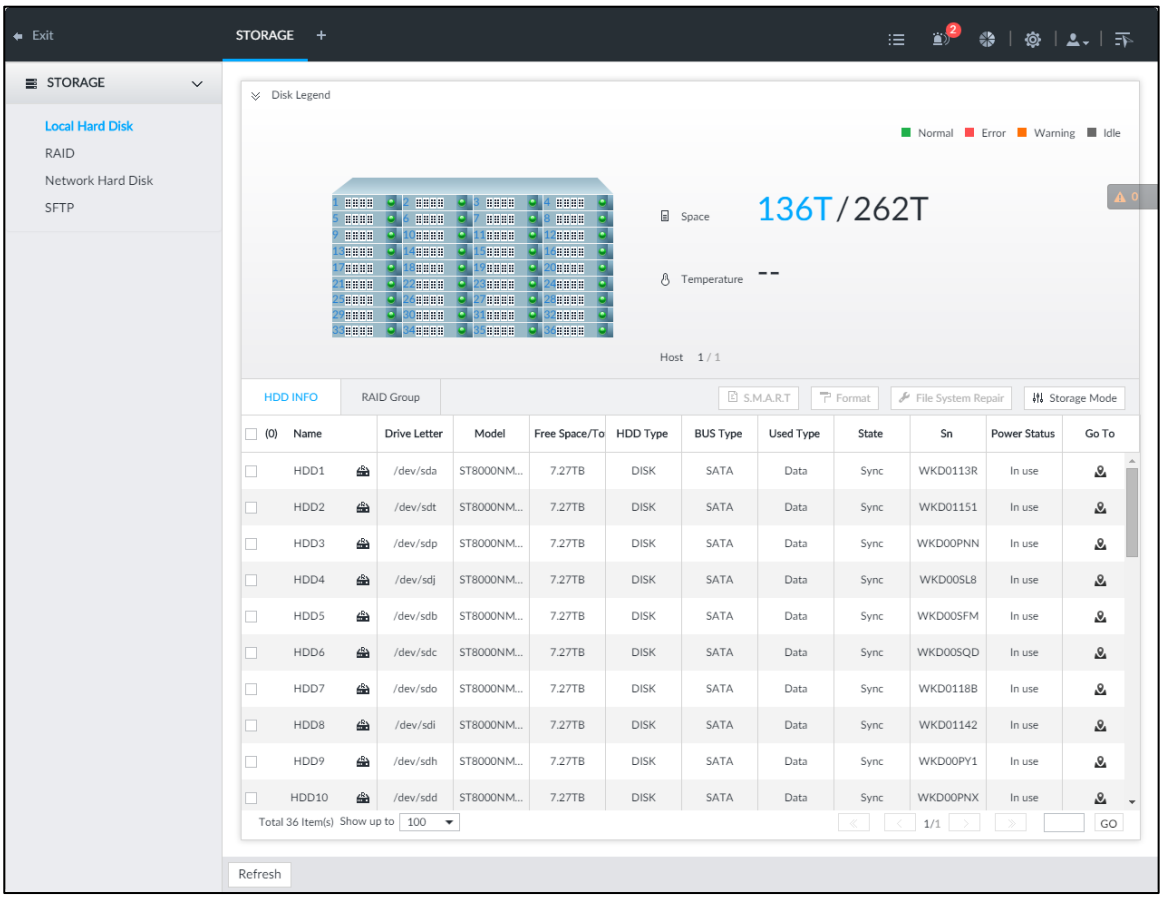
6.5 Storage Management

Click or click on the configuration interface, select **STORAGE**. The **STORAGE** interface is displayed. See Figure 6-60. Manage storage resources (such as recording file) and space, so you can use and improve utilization ratio of storage space.

The system supports pre-check and routine inspection function, displays health status on the Storage interface, so you obtain real-time status of device and avoid data loss.

- Pre-check: During device operation, the system automatically detects disc status in case of change (reboot, insert and pull the disc).
- Routine inspection: the system carries out routine inspection of the disc continuously. During device operation, the disc might go wrong due to service life, environment and other factors. Find out any problems during routine inspection.

Figure 6-60 Storage management



6.5.1 Local Hard Disk

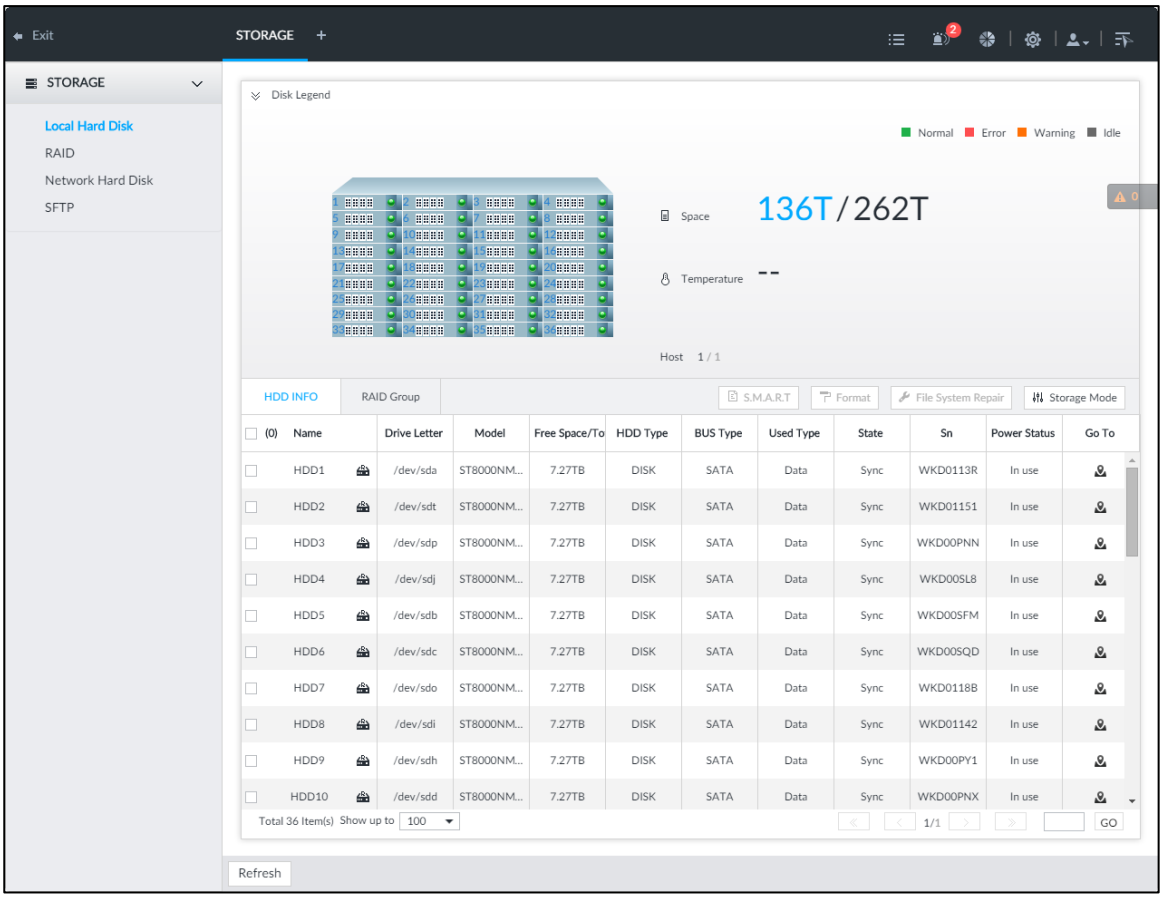
The local hard disk refers to the HDD installed on the system. On this interface, you can view HDD space (free space/total space), temperature (centigrade/Fahrenheit), HDD information and so on.

Click , or click on the configuration interface, and then select **STORAGE > Local Hard Disk**. The **Local Hard Disk** interface is displayed. See Figure 6-61. There is a corresponding icon near the HDD name after you create the RAID and hot spare HDD.

- : RAID HDD.
- : Global hot spare HDD.
- : Invalid HDD of RAID group.

Slight difference might be found on the user interface. The actual interface shall prevail.

Figure 6-61 HDD



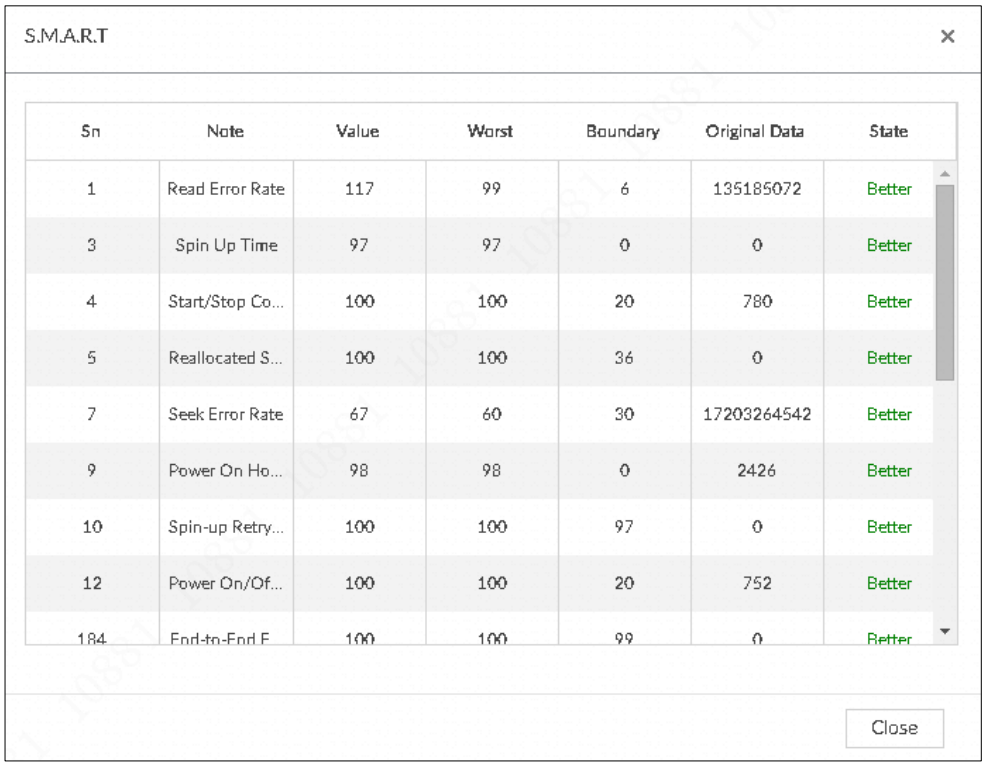
6.5.1.1 Viewing S.M.A.R.T

S.M.A.R.T is so called Self-Monitoring Analysis and Reporting Technology. It is a technical standard to check HDD drive status and report potential problems. System monitors the HDD running status and compares with the specified safety value. Once the monitor status is higher than the specified value, system displays alarm information to guarantee HDD data security.

Check one HDD to view S.M.A.R.T information at one time.

On the **Local Hard Disk** interface, select a HDD, and then click **S.M.A.R.T**. The **S.M.A.R.T** interface is displayed. See Figure 6-62. Check whether the HDD status is **OK** or not. If there is any problem, fix it in time.

Figure 6-62 S.M.A.R.T



6.5.1.2 Formatting HDD

- Formatting HDD will clear all data on the HDD. Be careful!
- Hot spare HDD cannot be formatted.

Enter the **Local Hard Disk** interface, select one or more HDD(s), and click **Format** to format the selected HDD.

6.5.1.3 File System Repair

Once you cannot mount the HDD or you cannot properly use the HDD, you can try to use the **File System Repair** function to fix the problem.

Enter the **Local Hard Disk** interface, select one or more HDD(s) you cannot mount, and click **File System Repair**, you can repair the selected file system of the corresponding HDD(s). The repaired HDD can work properly or to be mounted.

6.5.1.4 Setting Storage Strategy

Set storage strategy when HDD space is full.

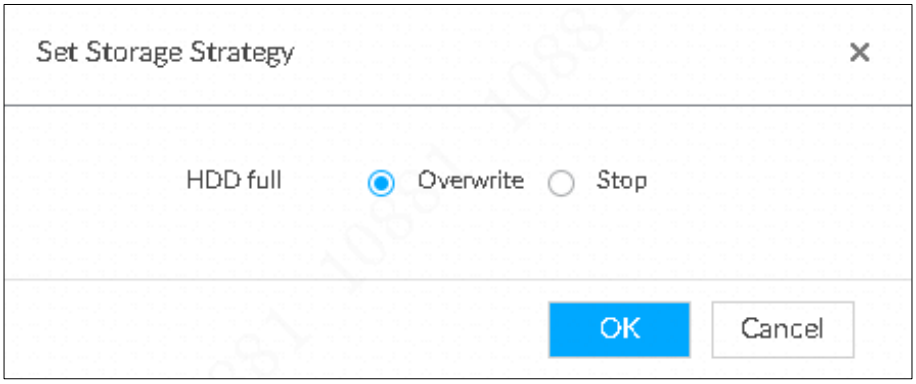
Step 1 Click , or click on the configuration interface, and then select **STORAGE > Local Hard Disk**.

The **Local Hard Disk** interface is displayed.

Step 2 Click Storage Strategy.

The **Set Storage Strategy** interface is displayed. See Figure 6-63.

Figure 6-63 Set storage strategy



Step 3 Set storage strategy.

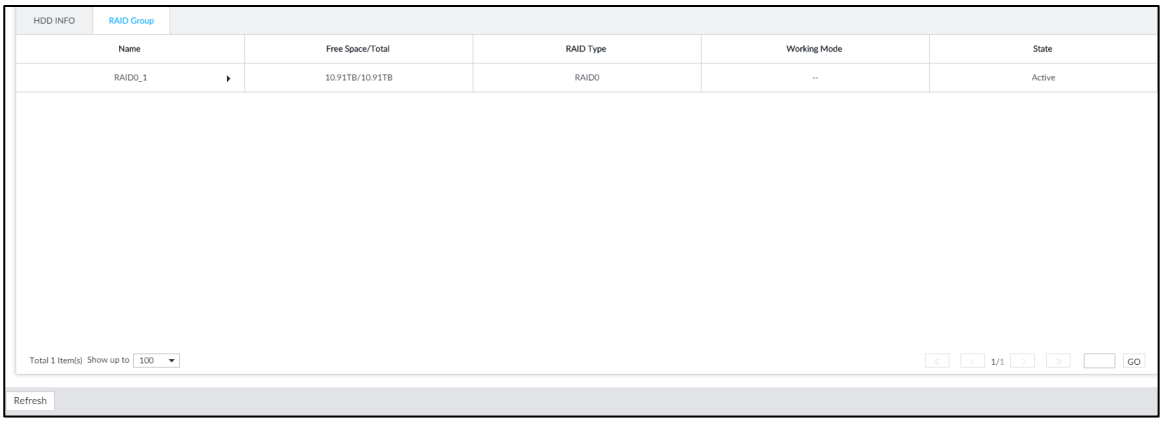
- Overwrite: When HDD free space is less than 150G or 4% of the total space (the larger of the two values prevails), system continues to record and begins overwriting the oldest record file.
- Stop: When HDD free space is less than 150G or 4% of the total space (the larger of the two values prevails), system stops recording. Stop recording will trigger an alarm. For details, see "6.4.2.1 Abnormal Event."

Step 4 Click **OK** to save the configuration.

6.5.1.5 Viewing RAID Group

Click , or click on the configuration interface, and then select **STORAGE > Local Hard Disk >RAID Group**. The **RAID Group** interface is displayed. You can view free space, RAID type, working mode and status of RAID group.

Figure 6-64 RAID group



- Click next to the RAID name to display the RAID member list, and then you can view RAID member details.

- Point to the **Status** column, and then click to display the **Details** interface to view RAID group details.

6.5.2 RAID

RAID (Redundant Array of Independent Disks) is a data storage virtualization technology that combines multiple physical HDD components into a single logical unit for the purposes of data redundancy, performance improvement, or both.

- The Device supports RAID 0, RAID 1, RAID5, RAID6, RAID10, RAID50 and RAID60. See "Appendix 1 RAID" for detailed information.
- You are recommended to use enterprise HDD when you are creating RAID.

6.5.2.1 Creating RAID

RAID has different levels such as RAID5, RAID6 and so on. Different RAID levels have different data protection, data availability and performance levels. Create RAID according to your actual requirements.

Creating RAID operation is going to clear all data on these HDD. Be careful!

Strategy of automatic creation

With the auto creation strategy, system creates RAID 5 by the following principle. See Table 6-24.

In the following table, among the numbers in the creation strategy, the number without () represents the disk number of the RAID group. The number with () represents the number of hot spare disks. For example, for 24 HDDs, the creation strategy is 7+7+9+(1). It means three RAID5 and one hot spare, and each RAID5 respectively contains 7 disks, 7 disks and 9 disks.

Table 6-24 Automatic creation strategy

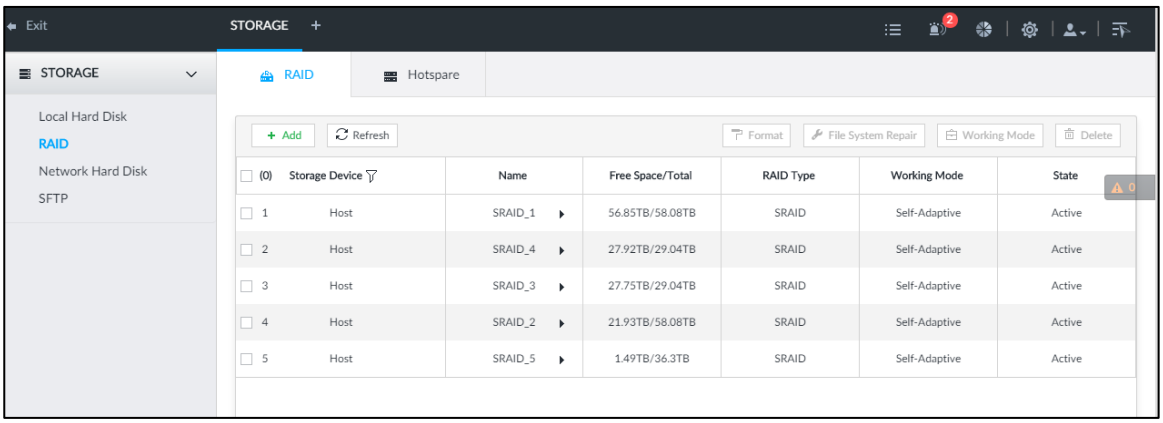
HDD No.	Creation Strategy
24	7+7+9+(1)
36	9+9+5+6+6+(1)
48	9+9+9+6+7+7+(1)

Create RAID

Step 1 Click , or click on the configuration interface, and then select **STORAGE > RAID > RAID**.

The **RAID** interface is displayed. See Figure 6-65.

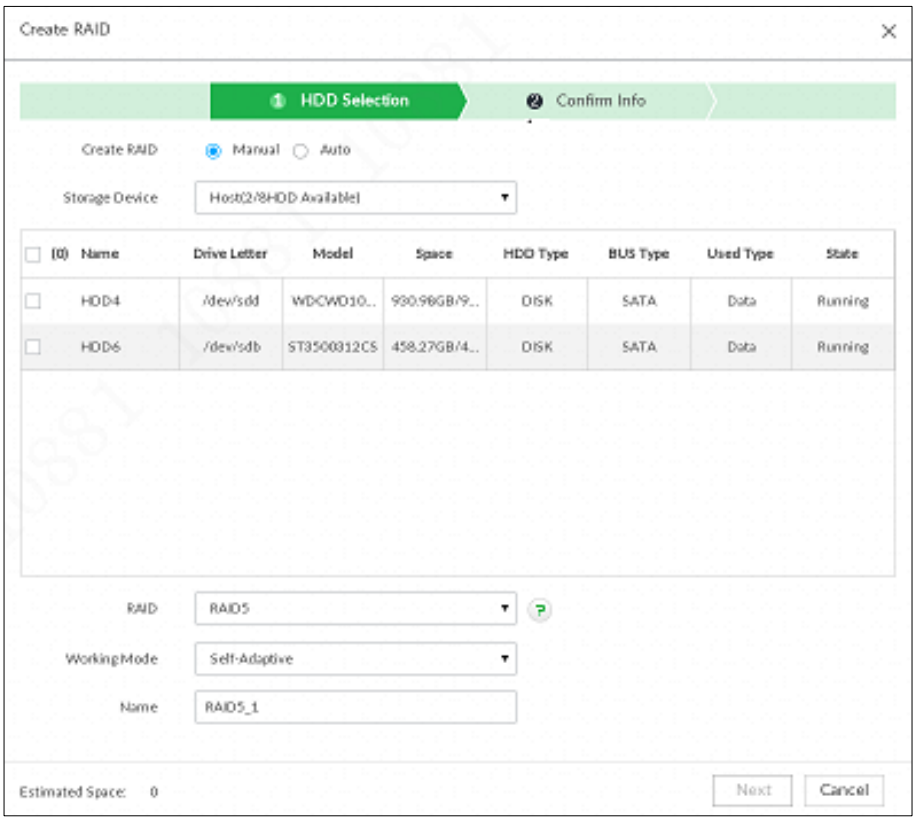
Figure 6-65 RAID



Step 2 Click **Add**.

The **Create RAID** interface is displayed. See Figure 6-66.

Figure 6-66 Create RAID (1)



Step 3 Set RAID parameters.

Select RAID creation type according to actual situation. It includes **Manual RAID** and **Auto RAID**.

- Manual RAID: System creates a specified RAID type according to the selected HDD amount.

1) Select Manual RAID.
2) Select HDD you want to use.
3) Set parameters. For details, see Table 6-25.

Table 6-25 Manual creation parameters description

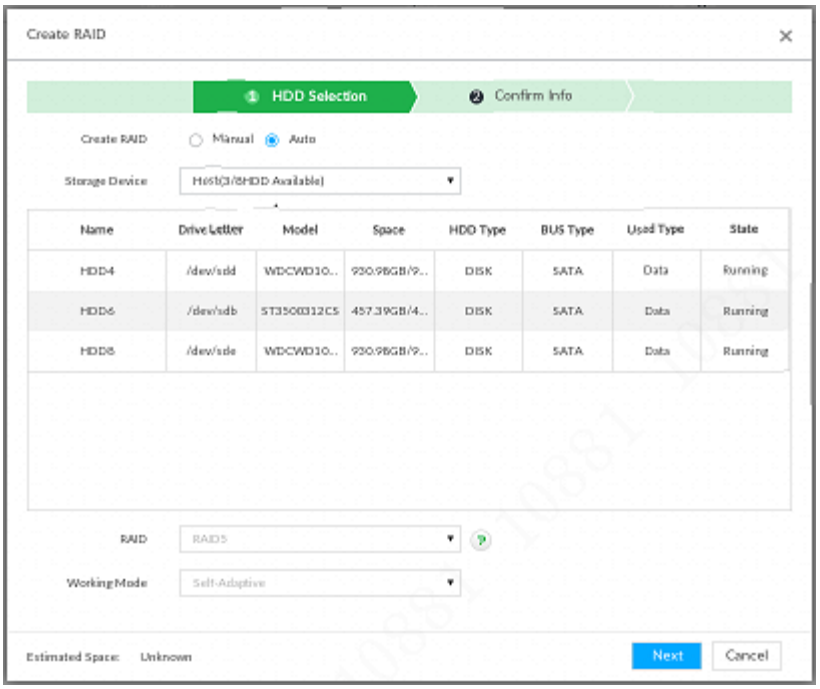
Parameters	Description
Storage Device	Select the HDD you want to add to the RAID. Different RAID types need different HDD amounts, and the actual situation shall prevail.
RAID	Select a RAID type you want to create.
Working mode	Set RAID resources allocation mode. The default setup is self-adaptive. ● Self-adaptive means the system can automatically adjust RAID synchronization speed according to current business load. When there is no external business, the synchronization speed is at high speed. When there is external business, the synchronization speed is at low speed. ● Sync first: Allocate resources to RAID synchronization first. ● Business first: Allocate resources to business first. ● Load-Balance: Allocate resources to business and RAID synchronization equally.
Name	Set RAID name.

- Auto: System creates RAID5 according to the HDD amount.

1) Select **Auto**.

The **Auto** interface is displayed. See Figure 6-67.

Figure 6-67 Create RAID (2)



2) Set parameters. For details, see Table 6-26.

Table 6-26 Auto parameters description

Parameters	Description
Storage Device	Select the storage device of the HDD.

Parameters	Description
Working mode	Set RAID resources allocation mode. The default setup is self-adaptive. ● Self-adaptive means the system can automatically adjust RAID synchronization speed according to current business load. When there is no external business, the synchronization speed is at high speed. When there is external business, the synchronization speed is at low speed. ● Sync first: Allocate resources to RAID synchronization first. ● Business first: Allocate resources to business first. ● Load-Balance: Allocate resources to business and RAID synchronization equally.

Step 4 Click **Next**.

The **Confirm Info** interface is displayed. See Figure 6-68 or Figure 6-69.

Figure 6-68 Confirm info (manual)

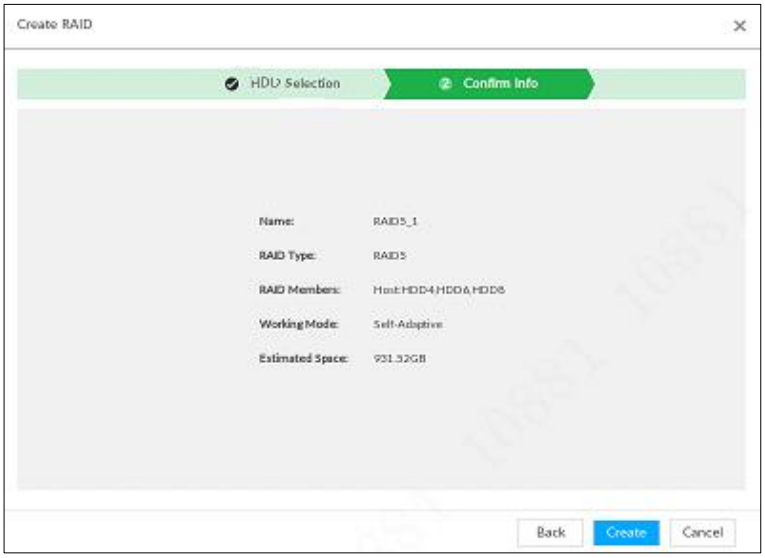
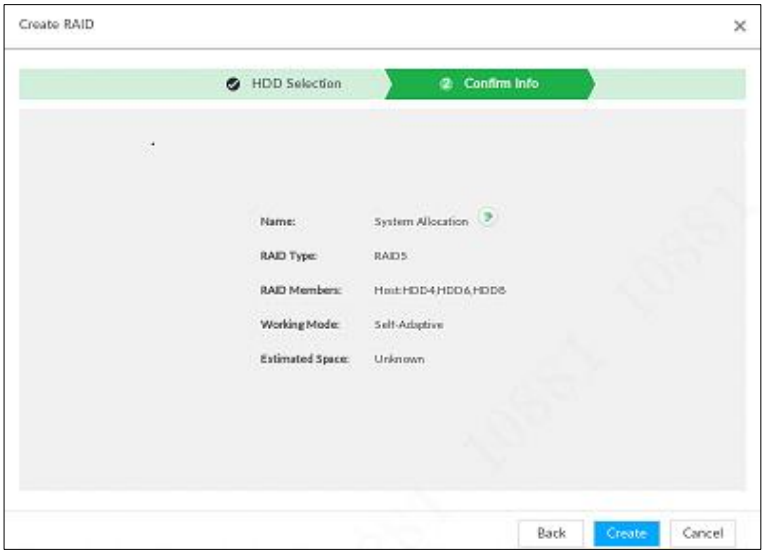


Figure 6-69 Confirm info (Auto)



Step 5 Confirm info.

If the entered information is wrong, click **Back** to set RAID parameters again.

Step 6 Click **Create**.

System begins to create RAID. It displays RAID information after creation. See Figure 6-70.

Figure 6-70 RAID (2)

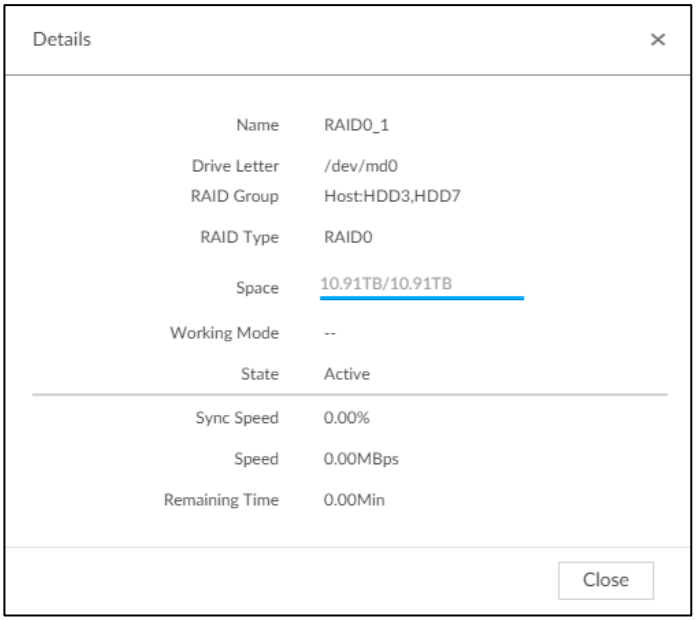
Operation

After creating RAID, view RAID disk status and details, clear up RAID, and repair file system. For details, see Table 6-27.

Table 6-27 RAID operation

Name	Operation
View RAID HDD status	Click  at the right side of the RAID name to open the RAID HDD list. View RAID HDD space, status and so on.
View RAID details	Click  . It displays detailed information. See Figure 6-71. View RAID detailed information.
File System Repair	Once you cannot mount the RAID or you cannot properly use the RAID, you can try to use repair file system function to fix. Enter RAID interface, select one or more RAID(s) you cannot mount, click **File System Repair**, you can repair the selected file system of the corresponding RAID(s). The repaired RAID can work properly or to be mounted.
Modify Working Mode	Select one or more RAIDs, and then click **Working Mode** to modify the working mode.
Format RAID	 Formatting RAID is to clear all data on the RAID and cancel the RAID group. Please be careful. Enter RAID interface, select one and more RAID groups. Click **Format** to format the selected RAID.
Delete RAID	 Deleting RAID is to clear all data on the RAID and cancel the RAID group. Please be careful. Enter RAID interface, select one and more RAID groups. Click **Delete** to delete the selected RAID.

Figure 6-71 RAID details



6.5.2.2 Creating Hot Spare HDD

When a HDD of the RAID group is malfunctioning or has a problem, the hot spare HDD can replace the malfunctioning HDD. There is no risk of data loss and it can guarantee storage system reliability.

Step 1 Click , or click on the configuration interface, and then select **STORAGE > RAID > Hot spare**.

The **Hot spare** interface is displayed. See Figure 6-72.

Figure 6-72 Hot spare (1)

Step 2 Click **Add**.

The **Add** interface is displayed. See Figure 6-73 or Figure 6-74.

Figure 6-73 Global hot spare

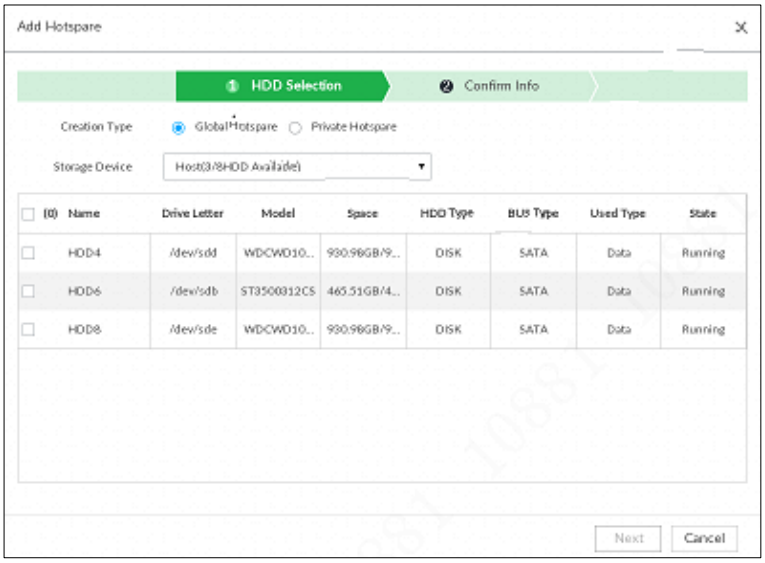
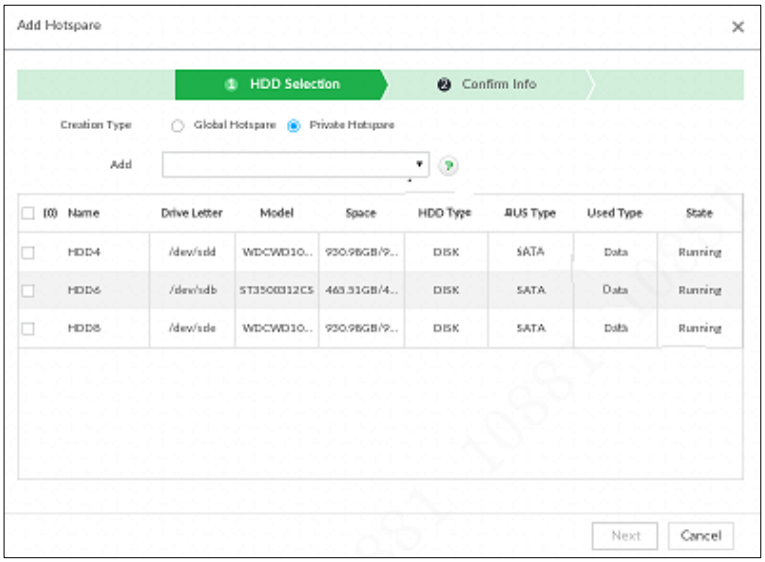


Figure 6-74 Private hot spare



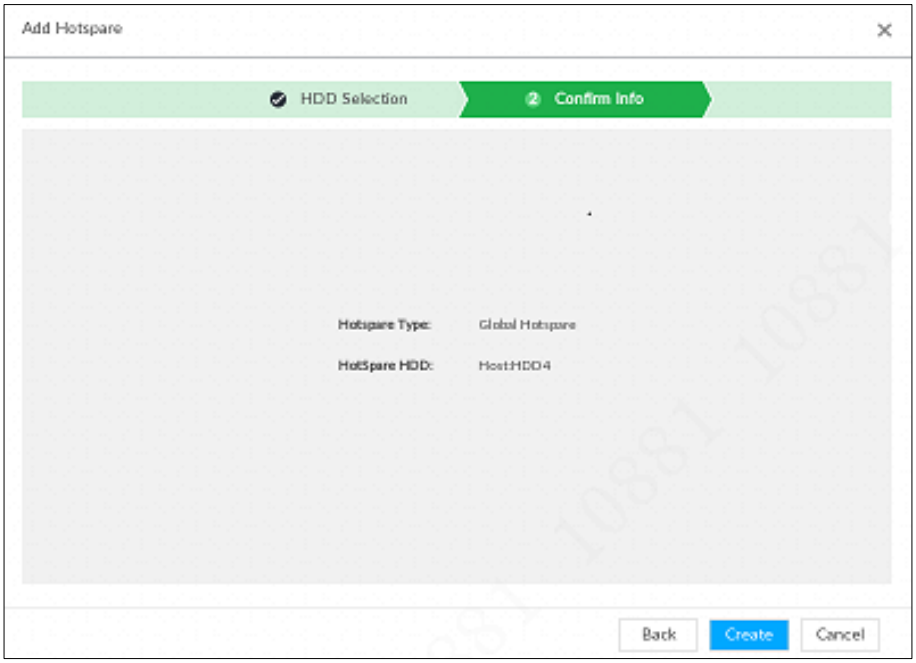
Step 3 Select hot spare creation type.

- Global hot spare: Create hot spare for all RAID. It is not a hot spare HDD for a specified RAID group.
- Private hot spare: Select **Private Hot spare** and **Add** it to a RAID group. The private hot spare HDD is for a specified RAID group.

Step 4 Select one or more HDD(s) and then click **Next**.

The **Confirm Info** interface is displayed. See Figure 6-75.

Figure 6-75 Confirm info



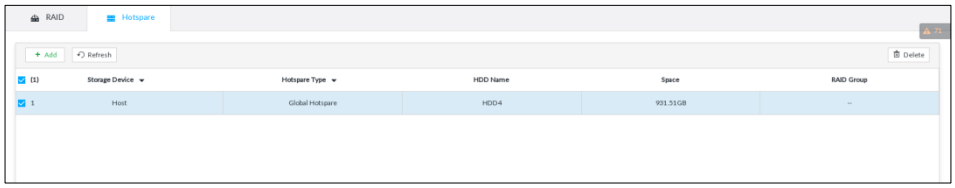
Step 5 Confirm info.

Click **Back** to select hot spare HDD(s) again if you want to change settings.

Step 6 Click **Create** to save settings.

System displays the added hot spare HDD information. See Figure 6-76.

Figure 6-76 Hot spare (2)



Select a hot spare HDD and then click **Delete** to delete hot spare HDD.

6.5.3 Network Hard Disk

Network hard disk is a network-based online storage service that stores device information in the network hard disk through the iSCSI protocol.

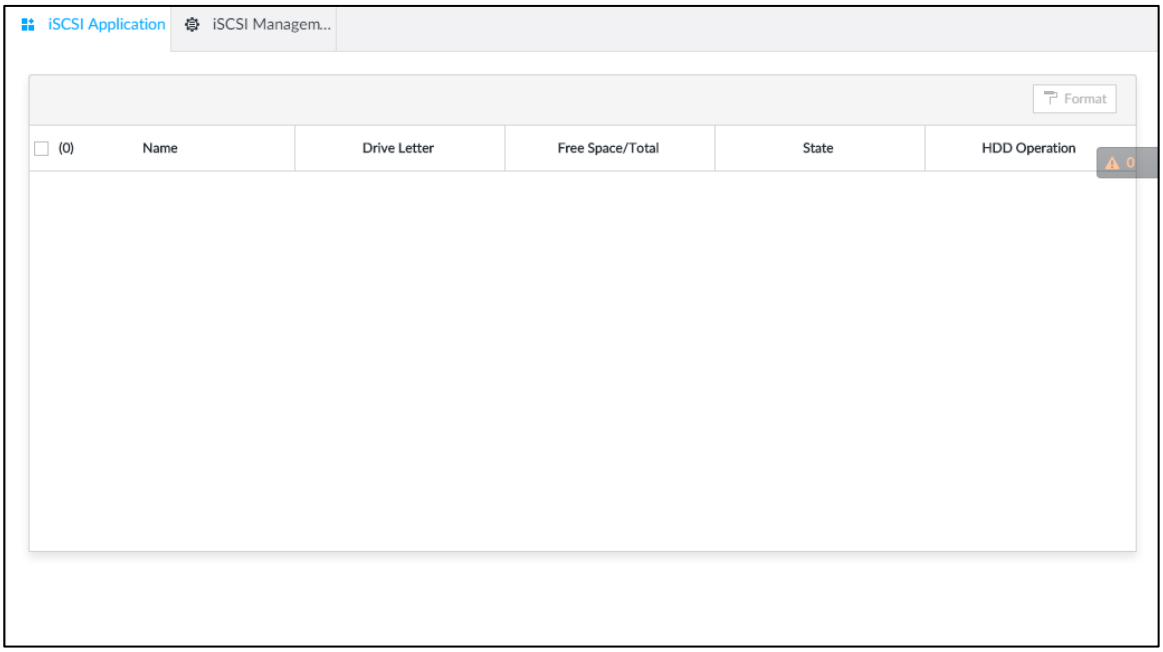
6.5.3.1 iSCSI Application

View network hard disk usage, including remaining capacity, and hard disk status.

Click , or click on the configuration interface, and then select **STORAGE > Network Hard Disk > iSCSI Application**.

The **iSCSI Application** interface is displayed. See Figure 6-77.

Figure 6-77 ISCSI application



- Select a network hard disk, and then click **Format** to format the disk. Formatting your hard disk will erase all data from your hard disk, so do it carefully.
- Click the **HDD Operation** column, and then you can select an HDD operation permission type.
  - ◇ Read/Write: One can read, edit, add, and delete data of this disk.
  - ◇ Read Only: One can only read data of this disk.

6.5.3.2 iSCSI Management

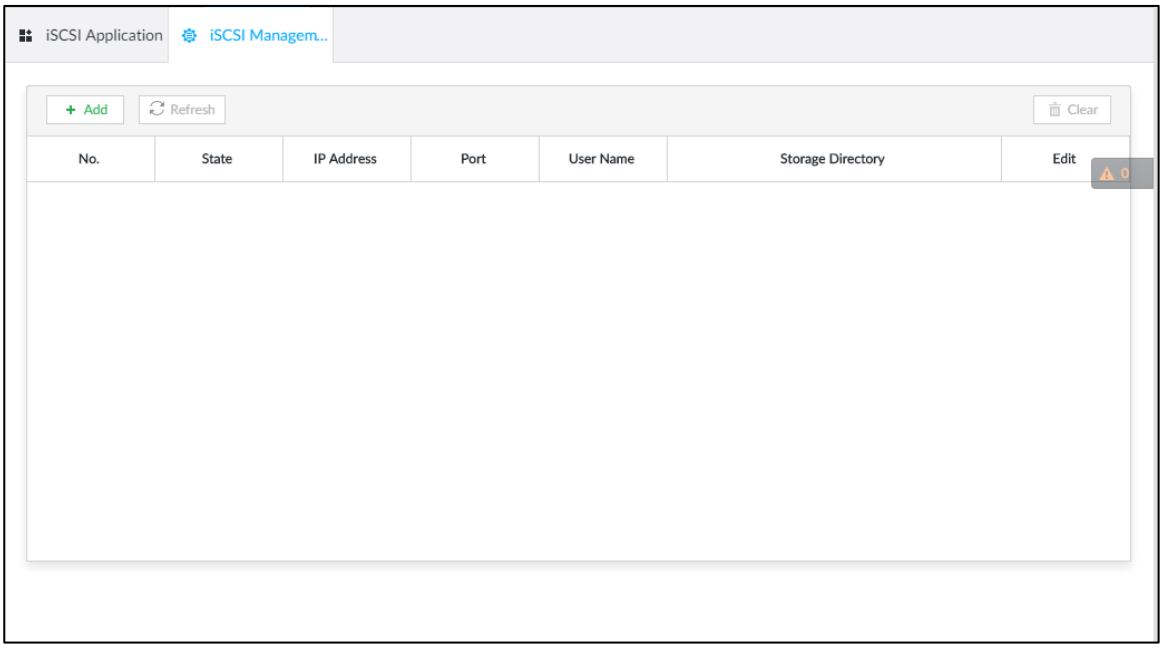
Set up the network disk through iSCSI and map the network disk to the device so that the device can use the network disk for storage.

- iSCSI is a networked storage technology that runs SCSI protocols on the IP network.
- The network disk mapped to the device cannot be used to create a RAID.
- Make sure that service has been enabled on the iSCSI server and the server has provided the shared file directory.

Step 1 Click , or click on the configuration interface, and then select **STORAGE > Network Hard Disk > iSCSI Management**.

The **iSCSI Management** interface is displayed. See Figure 6-78.

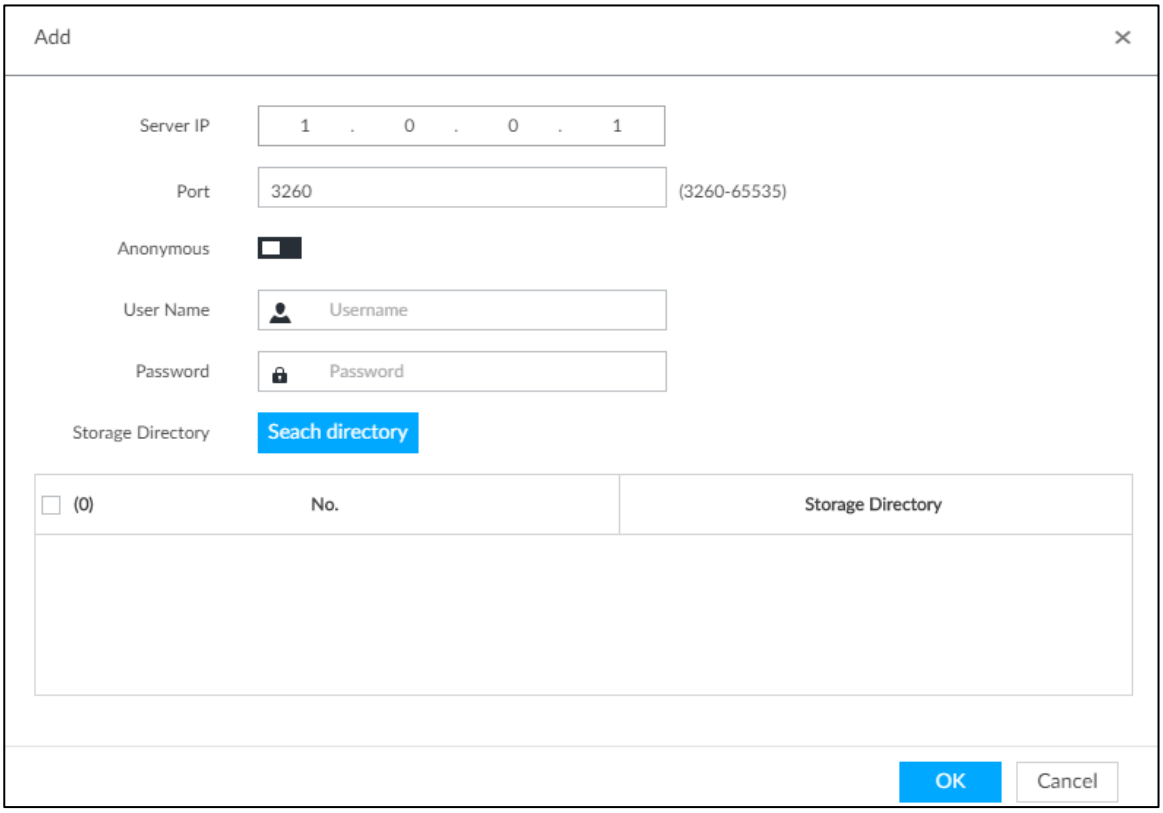
Figure 6-78 Network hard disk



Step 2 Click + .

The **Add** interface is displayed. See Figure 6-79.

Figure 6-79 Add iSCSI



Step 3 Set parameters. See Table 6-28.

Table 6-28 Network hard disk parameters

Parameters	Description
Server IP	Enter iSCSI server IP address.
Port	Enter iSCSI server port number. It is 3260 by default.

Parameters	Description
Anonymous	If iSCSI server has no permission limitation, you can select anonymous login. ● indicates that anonymous login is enabled and there is no need to set username and password. ● indicates that anonymous login is disabled.
Username Password	If access permission has been limited when creating the shared file directory on the iSCSI server, you need to enter username and password.
Storage Directory	Click **Search Directory** to select the storage directory. The storage directory is generated when the shared file directory is being created on the iSCSI server. Each directory is an iSCSI disk.

Step 4 Click **OK**.

The added network disk is displayed.

- Click to delete a disk; click **Refresh** to refresh the disk list.
- On the Disk Group interface, you can configure network disk groups. For details, see "6.9.1.1Setting Disk Group."

6.5.4 FTP/SFTP

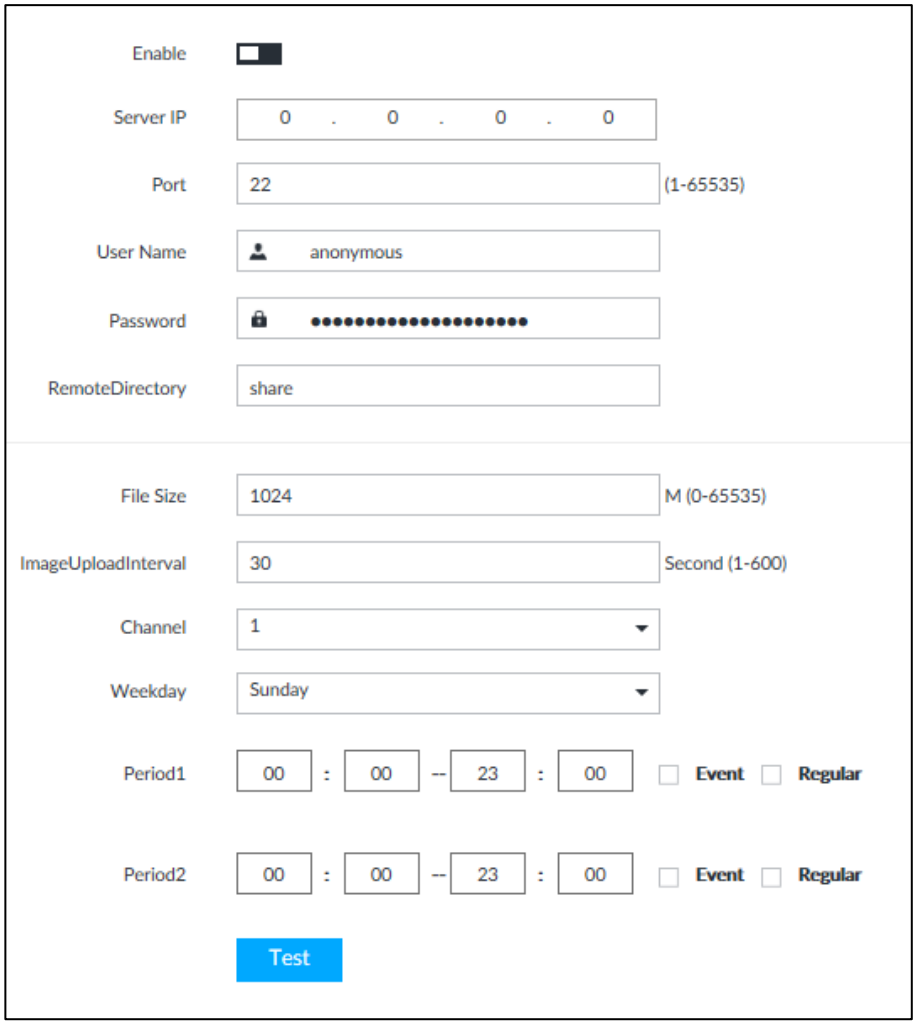
Configure FTP/SFTP server for video and picture storage. This section takes configuring SFTP as an example.

- FTP is unencrypted transmission, while SFTP is encrypted transmission. You are recommended to use SFTP.
- When creating SFTP user, you need to configure write permission of SFTP folder. Otherwise, you cannot upload files.
- You need to purchase or download SFTP tool and install it on your PC.

Step 1 Click , or click on the configuration interface, and then select **STORAGE > SFTP**.

The **SFTP** interface is displayed. See Figure 6-80.

Figure 6-80 SFTP



Step 2 Click to enable SFTP.

Step 3 Set parameters. See Table 6-29.

Table 6-29 SFTP parameters

Parameters	Description
Server IP	SFTP server IP address.
Port	It is 22 by default.
User Name	The username and password of the SFTP server. You can keep the username as **anonymous**, so as to log in in an anonymous way.
Password	
Remote Directory	Enter the SFTP directory. ● The system automatically establishes folders according to the IP, time, and channel information if you leave the directory empty. ● Enter the directory name, and then the system creates a folder accordingly under the root directory of SFTP and generates different folders according to the IP, time, and channel information.

File Size	Set the size of the file to be uploaded. ● If the to-be-uploaded file is larger than the threshold, the system uploads only part of it (the same size with the threshold). ● If the to-be-uploaded file is smaller than the threshold, the system uploads the whole of it. ● If the threshold you have set is 0, the system uploads the whole of the file.
Image Upload Interval	Set the upload intervalof images.
Channel	Set the channel number of the video file.
Weekday	Select the day, the time period, and file type (event file or regular file).
Period	The system uploads files in the time periods as you have set.
Test	Click Test to test the SFTP connection.

Step 4 Click **Save**.

6.6 Security Strategy

Click or click on the configuration interface, select **SECURITY**. The **SECURITY** interface is displayed. See Figure 6-81.

Set security strategy to guarantee device network and data safety. It includes HTTPS, set host IP access rights, enable network security protection.

HTTPS function is for web interface and PCAPP only. See the actual interface for detailed information.

Figure 6-81 Security center

6.6.1 HTTPS

HTTPS can use the reliable and stable technological means to guarantee user information and device security and communication data security. After installing the certificate, you can use the HTTPS on the PC to access the device.

You are recommended to enable HTTPS service. Otherwise, you might risk data leakage.

6.6.1.1 Installing Certificate

There are two ways to install the certificate.

- Manually create a certificate and then install.
- Upload a signature certificate and then install.

6.6.1.1.1 Installing the Created Certificate

Install the created certificate manually. It includes creating the certificate on the device, downloading and installing the certificate on the PC.

- Create and install root certificate if it is your first time to use HTTPS or you have changed device IP address.
- After creating server certificate and installing root certificate, download and install root certificate on the new PC, or download the certificate and then copy to the new PC.

Step 1 Click , or click on the configuration interface, and then select **SECURITY > Credential**.

The **Credential** interface is displayed. See Figure 6-82.

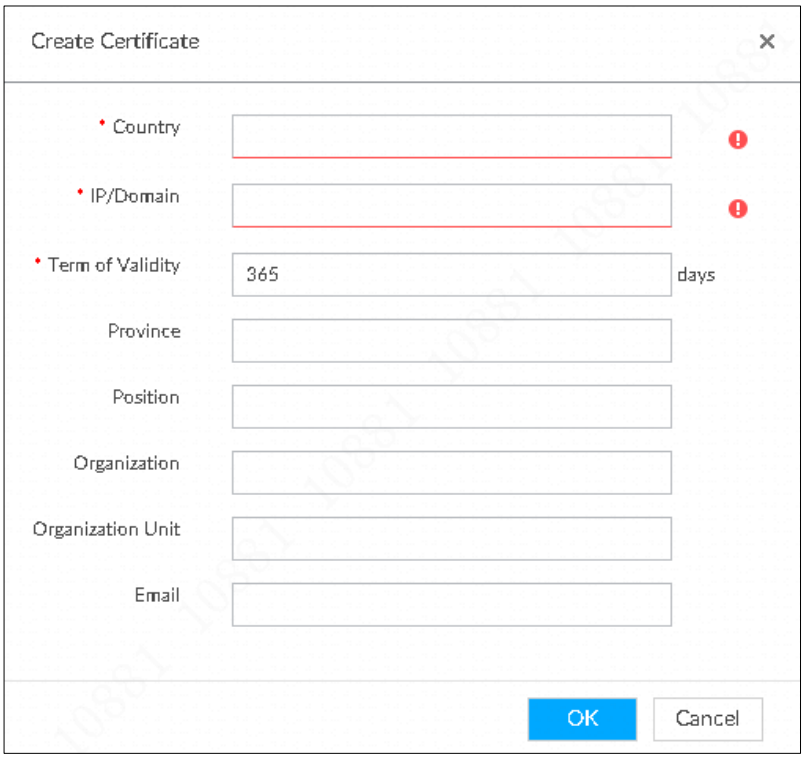
Figure 6-82 Credential (1)

Step 2 Create certificate on the device.

1) Click Create certificate.

The **Create certificate** interface is displayed. See Figure 6-83.

Figure 6-83 Create certificate



2) Set country, IP/domain, valid date and so on.

- Country, IP/domain, and valid date are required items. Other items are optional.
- IP/domain shall be the device IP or the domain.

3) Click **OK**.

System begins to install certificate, and then displays certificate information after the installation. See Figure 6-84.

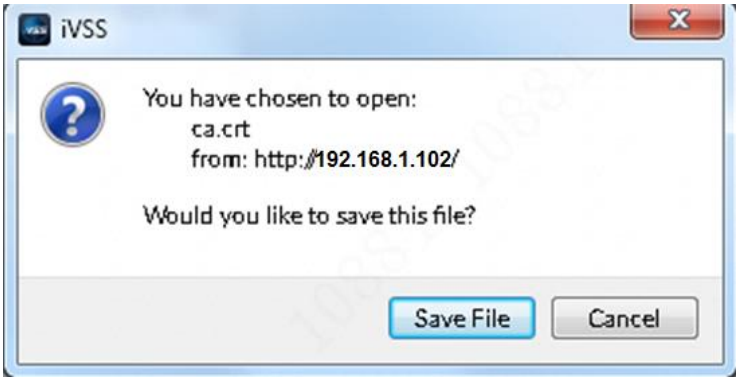
Figure 6-84 Credential (2)

Step 3 Download certificate.

1) Click Download.

The **Opening ca.crt** interface is displayed. See Figure 6-85.

Figure 6-85 Opening ca.crt



2) Click **Save File** to select file saved path.
3) Click **Save**.
   System begins downloading certificate file.

Step 4 Install root certificate on the PC.

1) Double-click the certificate.
   System displays **Open file-security warning** interface.
2) Click **Open**.
   System displays **Certificate** interface. See Figure 6-86.

Figure 6-86 Certificate

3) Click Install Certificate.
   The **Certificate Import Wizard** interface is displayed. See Figure 6-87.

Figure 6-87 Certificate import wizard

4) Follow the prompts to import the certificate.
System goes back to **Certificate** interface.

Step 5 Click **OK** to complete certificate installation.

6.6.1.1.2 Installing Signature Certificate

Upload signature certificate to install.

Preparation

Before installation, make sure that you have obtained safe and valid signature certificate.

Operation Steps

Step 1 Click , or click on the configuration interface, and then select **SECURITY > Credential**.

The **Credential** interface is displayed. See Figure 6-88.

Figure 6-88 Credential(1)

Step 2 Click Install Signature Certificate.

The **Install Signature Certificate** interface is displayed. See Figure 6-89.

Figure 6-89 Install signature certificate

Step 3 Click **Browse** and then select certificate and credential file.

Step 4 Click **Install**.

System begins to install certificate, and then displays certificate information after the installation.

Step 5 Install the root certificate on the PC.

This root certificate is the one obtained with signed certificate.

6.6.1.2 Enabling HTTPS

After you install the certificate and enable HTTPS function, you can use the HTTPS on the PC to access the device.

Step 1 Click , or click on the configuration interface, and then select **SECURITY > Credential**.

The **Credential** interface is displayed.

Step 2 Click to enable HTTPS function. See Figure 6-90.

Figure 6-90 Credential

Step 3 Click **Save**.

After you successfully save the settings, you can use HTTPS to access the web interface.

Open the browser and then enter https://IP address:port, press Enter, and the login interface is displayed.

- IP address is device IP or the domain name.
- Port refers to device HTTPS port number. If the HTTPS port is the default value 443, just use https://IP address to access.

6.6.1.3 Uninstalling the Certificate

Uninstall the certificate.

- You cannot use the HTTPS function after you uninstall the certificate.
- The certificate cannot be restored after being uninstalled. Be cautious.

Step 1 Click , or click on the configuration interface, and then select **SECURITY > Credential**.

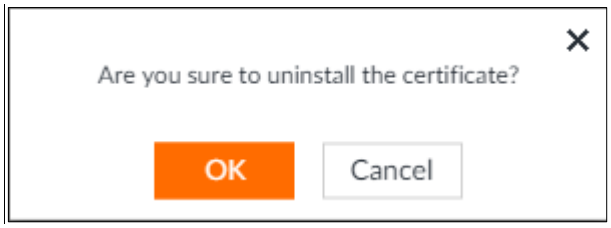
The **Credential** interface is displayed. See Figure 6-91.

Figure 6-91 Credential

Step 2 Click Uninstall.

System pops up a confirmation box. See Figure 6-92.

Figure 6-92 Confirmation



Step 3 Click **OK** to uninstall the certificate.

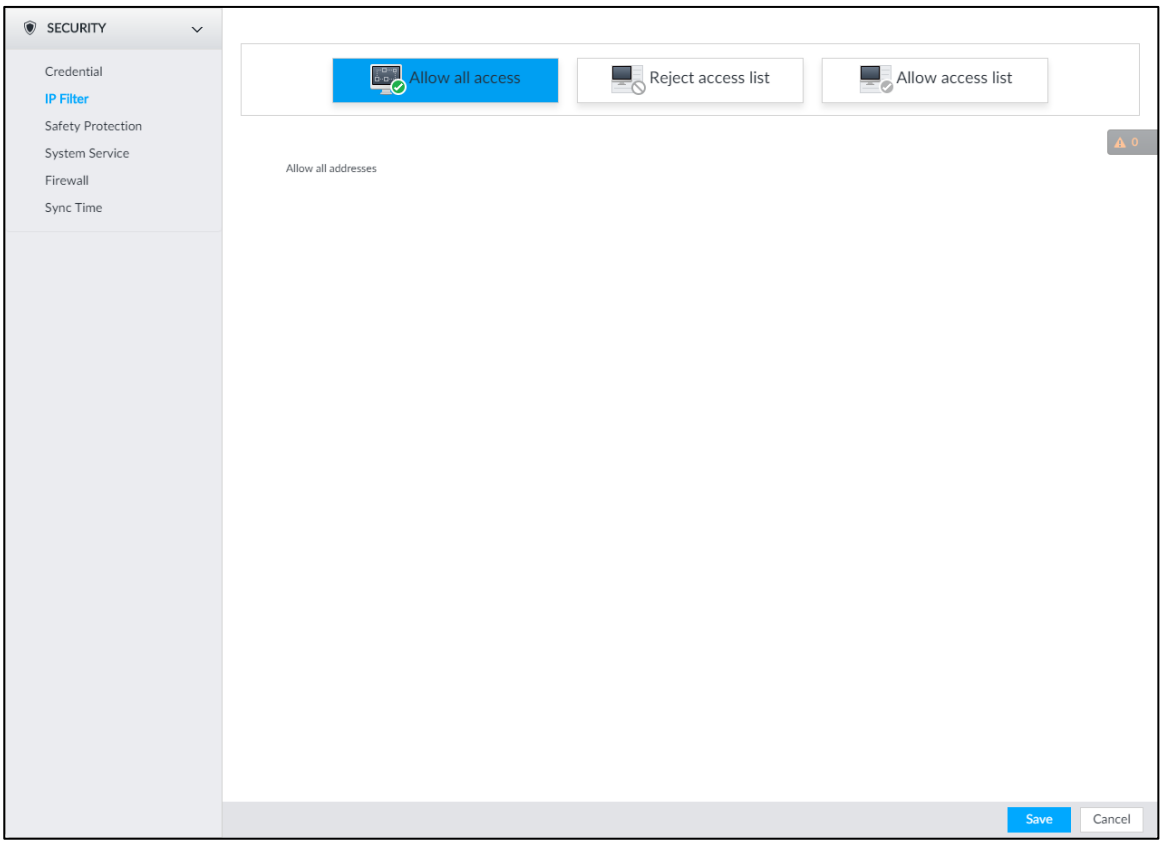
6.6.2 Configuring Access Permission

Set the specified IP addresses to access the device, to enhance device network and data security.

Step 1 Click , or click on the configuration interface, and then select **SECURITY > IP Filter**.

The **IP Filter** interface is displayed. See Figure 6-93.

Figure 6-93 IP Filter



Step 2 Select IP access rights.

- Allow all access: It is to allow all IP addresses in the same IP segment to access the device.
- Reject access list: It means the IP address in the list cannot access the device.
- Allow access list: It means the IP address in the list can access the device.

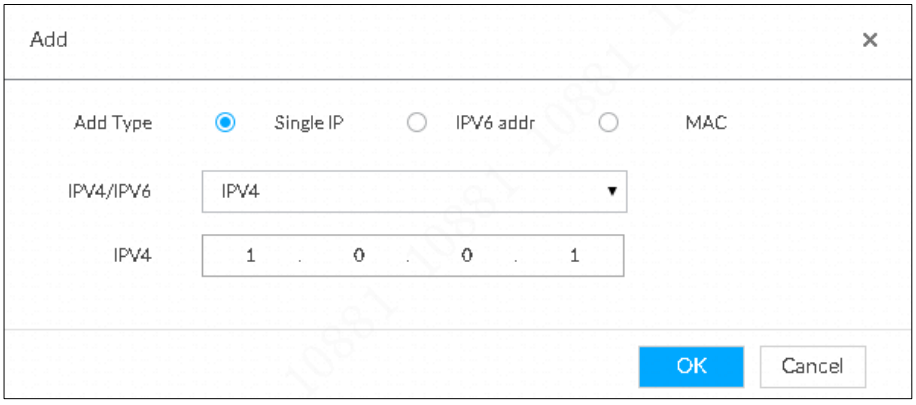
Step 3 Add IP host.

The following steps are to set reject access list or allow access list.

1) Click **Add**.

The **Add** interface is displayed. See Figure 6-94.

Figure 6-94 Add



2) Select **Add Type**, and set IP address or MAC address of IP host.

- Single IP: Enter host IP address.
- IP segment: Enter IP segment. It can add multiple IP addresses in current IP segment.

- MAC: Enter MAC address of IP host.

3) Click **OK** to add the IP host.
System displays added IP host list.

- Click **Add** to add more IP hosts.
- Click to edit the IP host.
- Select an IP host and then click **Delete** to delete.

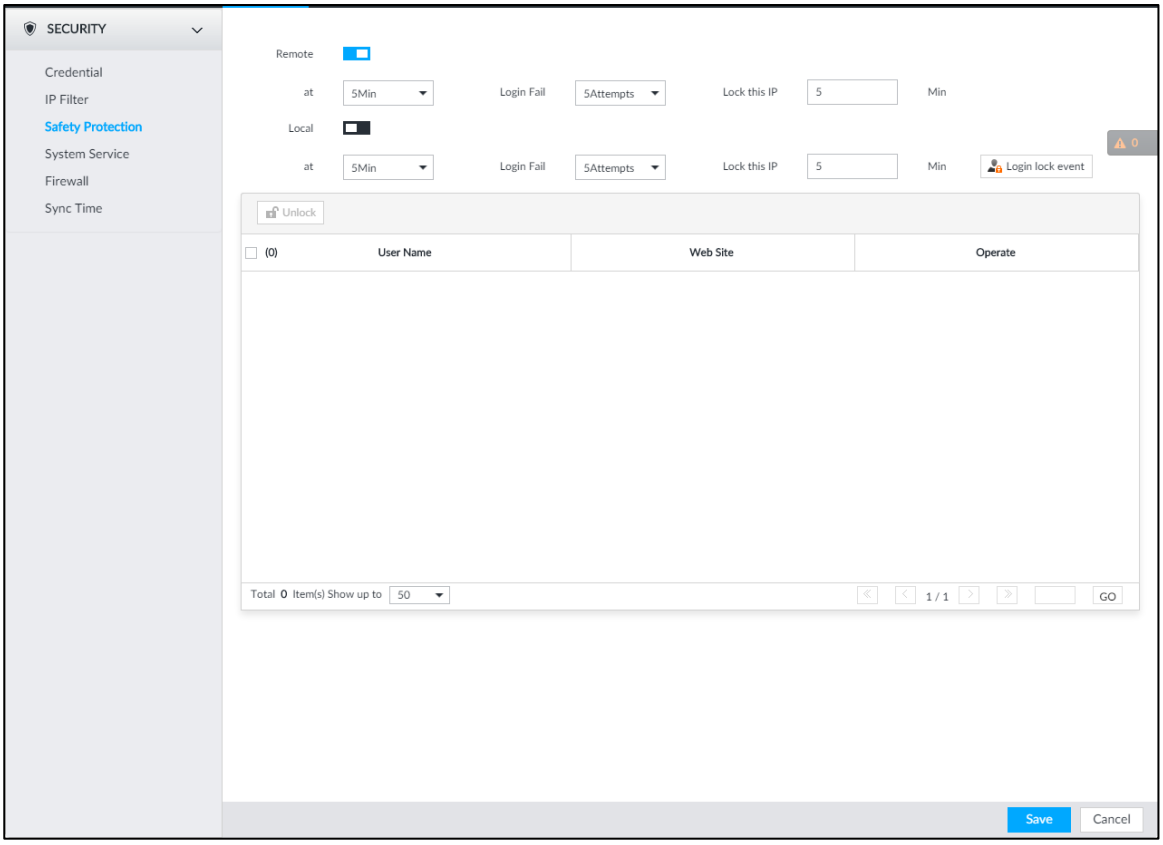
Step 4 Click **Save**.

6.6.3 Safety Protection

Set the login password lock strategy once the login password error has exceeded the specified threshold. System can lock current IP host for a period of time.

Step 1 Click , or click on the configuration interface, and then select **SECURITY > Safety Protection**.
The **Safety Protection** interface is displayed. See Figure 6-95.

Figure 6-95 Safety protection (1)



Step 2 Click to enable security protection function.

- Remote: When you are using web interface, PCAPP to access the device remotely, once the login password error has exceeded the threshold, system locks the IP host for a period of time.

- Local: When you are accessing local menu of the device, once the login password error has exceeded the threshold, system locks the account for a period of time.

Step 3 Set lock strategy according to the actual situation.

Step 4 Click **Save**.

Once the IP host has been locked, you can view the locked IP host on the list. Select an IP host and then click **Unlock**, or click the of the corresponding IP host to unlock.

Step 5 (Optional) Click **Login lock event** to go to the **Event** interface where you can select **Abnormal Event > Lock** in to configure a **Lock in** event.

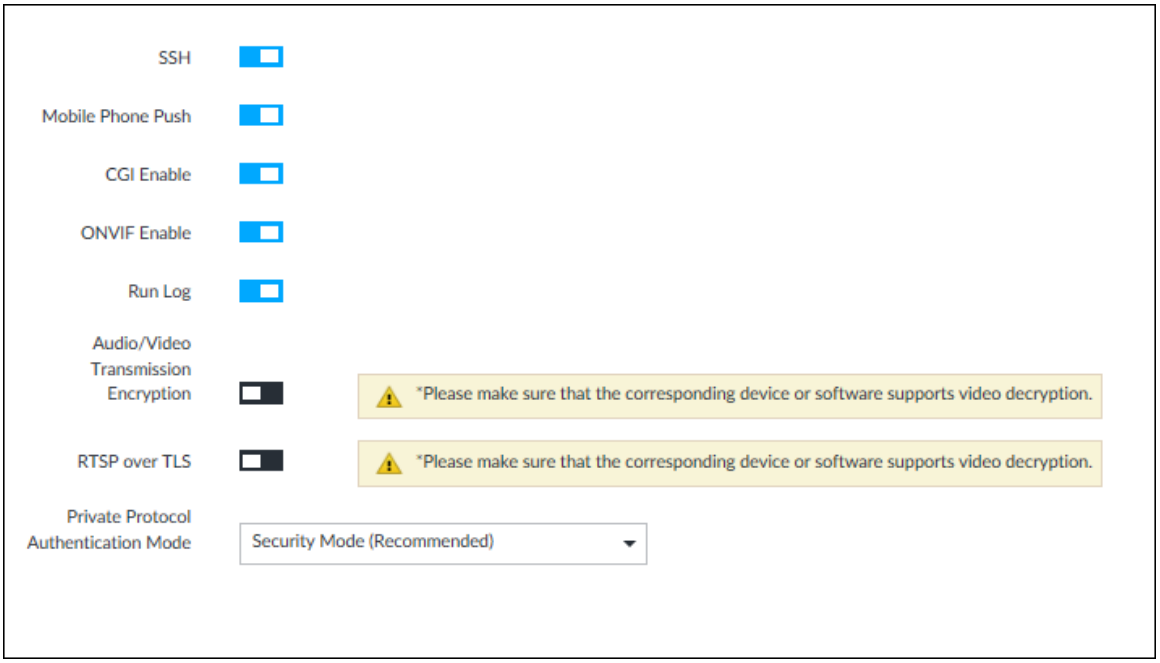
6.6.4 Enabling System Service Manually

Enable system services for third-party access.

Step 1 Click , or click on the configuration interface, and then select **SECURITY > System Service**.

The **System Service** interface is displayed. See Figure 6-96.

Figure 6-96 System service



Step 2 Enable or disable system service according to your actual situation.

See Table 6-30 for detailed information.

Table 6-30 System service

System service	Description
SSH	After enabling this function, you can access EVS through SSH protocol to carry out system debugging and IP configuration. This function is disabled by default. You are recommended to disable this function. Otherwise there might be security risks.

System service	Description
Mobile Phone Push	After enabling this function, you can access EVS with mobile phone client, to receive information from EVS. You are recommended to disable this function. Otherwise there might be security risks.
CGI Enable	After this function is enabled, third-party platform can connect EVS through CGI protocol. You are recommended to disable this function. Otherwise there might be security risks.
ONVIF Enable	After this function is enabled, other devices can connect EVS through ONVIF protocol. You are recommended to disable this function. Otherwise there might be security risks.
Run Log	After enabling it, you can view system running logs in **Intelligent Diagnosis > Run Log**.
Audio/Video Transmission Encryption	When this function is enabled, stream trasmission will be encrypted. You are recommended to enable this function. Otherwise you might risk data leakage.
RTSP over TLS	Enable this function to encrypt stream transmission. You are recommended to enable this function. Otherwise you might risk data leakage.
Private Protocol Authentication Mode	Select a private protocol authentication mode between secruity mode and compatible mode. Compatible mode is recommended.

Step 3 Click **Save**.

6.6.5 Configuring Firewall

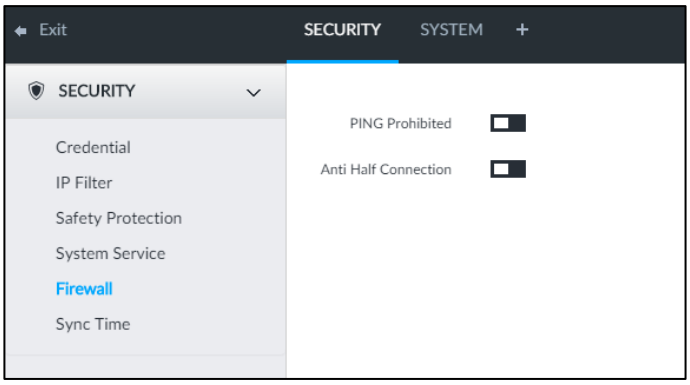
Enhance network and data security by prohibiting Ping and half-connection.

- PING Prohibited: When **PING Prohibited** is enabled, the device does not respond to Ping requests.
- Anti Half Connection: When **Anti Half Connection** is enabled, and the device can provide service normally under half-connection attack.

Step 1 Click , or click on the configuration interface, and then select **SECURITY > Firewall**.

The **Firewall** interface is displayed. See Figure 6-97.

Figure 6-97 Firewall



Step 2 Click to enable PING Prohibited or Anti Hal Connection.

Step 3 Click **Save**.

6.6.6 Configuring Time Synchronization Permission

Configure permissions of time synchronization actions from other devices or servers.

Step 1 Click , or click on the configuration interface, and then select **SECURITY > Synch Time**.

Step 2 Click to enable time synchronization restriction.

Step 3 Select **Allowlist** or **Blocklist**.

- Hosts in the allowlist have the permission to synchronize time of the Device.
- Hosts in the allowlist cannot synchronize time of the Device.

Step 4 On the **Allowlist** interface or the **Blocklist** interface, add hosts.

1) Click **Add**. The following interface is displayed.
2) Select an IP version, and then enter an IP address.
3) Click **OK**.

Step 5 Click **Save**.

You can also perform the following functions after configuring the allowlist or blocklist. See Table 6-31.

Table 6-31 Other functions

Function	Description
Edit IP address	Click to edit IP address.
Delete IP address	Click to delete a host from the list.
Configure IP address permission	Click the corresponding of each host, so as to enable the allowlist or balcklist configuration for the host. Click to disable the allowlist or balcklist configuration for the host.

6.7 Account Management

Device account adopts two-level management mode: user and user group. You can manage their basic information. To conveniently manage the user, we recommend the general user authorities shall be lower than high-level user authorities.

- To ensure device safety, enter correct login password to operate Account interface (for example, add or delete user).
- After a correct login password is entered on Account interface, if you do not close Account interface, you can do other operations directly. If you close the interface and enter it again, you shall enter the correct login password again. The actual interface shall prevail.

6.7.1 User Group

Different users might have different authorities to access the device. You can divide the users to different groups. It is easy for you to maintain and manage the user information.

- System supports maximum 64 user groups. User group name supports maximum 64 characters.
- System has two default user groups (read-only): admin and ONVIF.
- Create new user group under the root.

Adding User Group

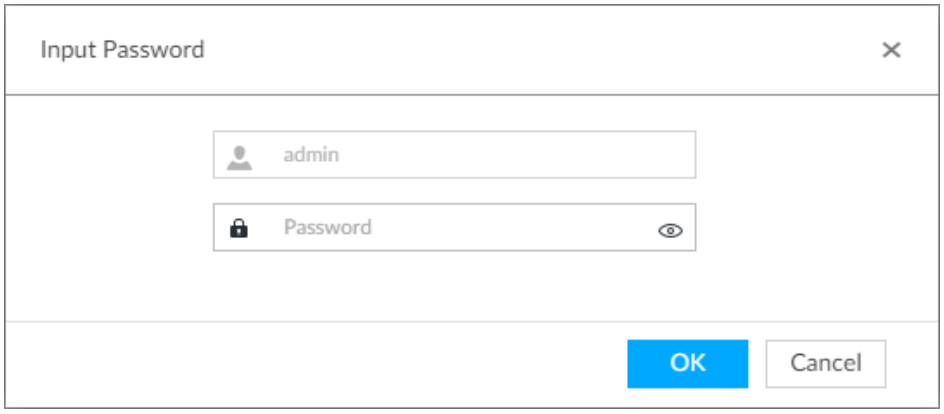
Step 1 Click , or click on the configuration interface, and then select **ACCOUNT**.

The **ACCOUNT** interface is displayed.

Step 2 Select the root node in the device tree on the left and then click at the lower-left corner.

The **Input Password** is displayed. See Figure 6-98.

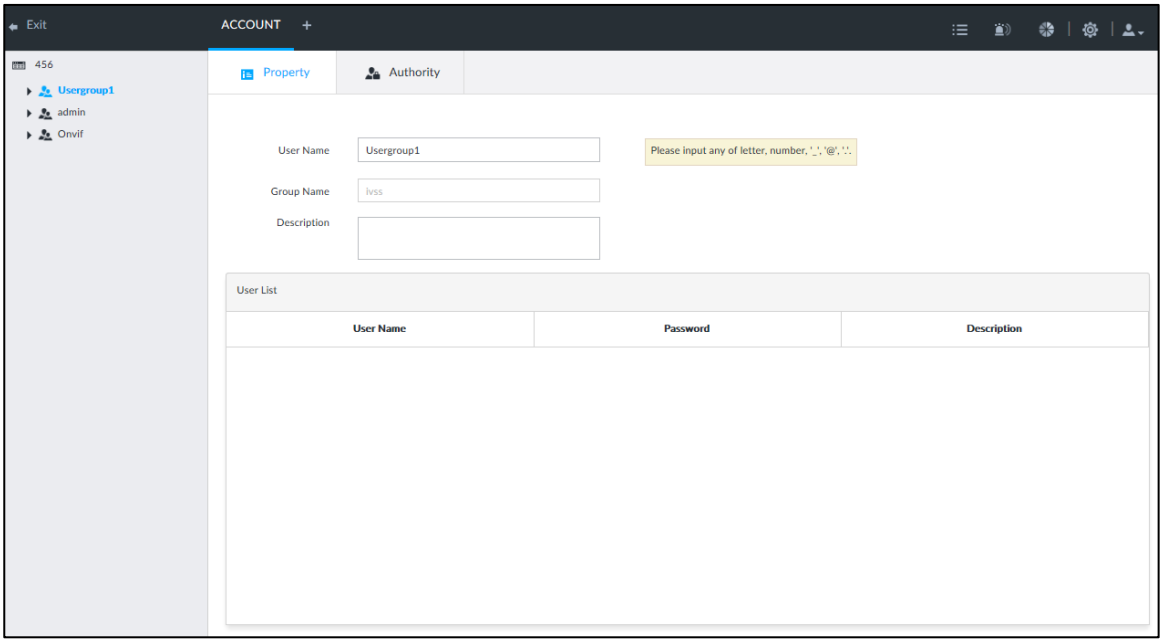
Figure 6-98 Input password



Step 3 Enter current user's login password, and then click **OK**.

System creates one user group and displays **Property** interface. See Figure 6-99.

Figure 6-99 User group property



Step 4 Set parameters. For details, see Table 6-32.

Table 6-32 User group

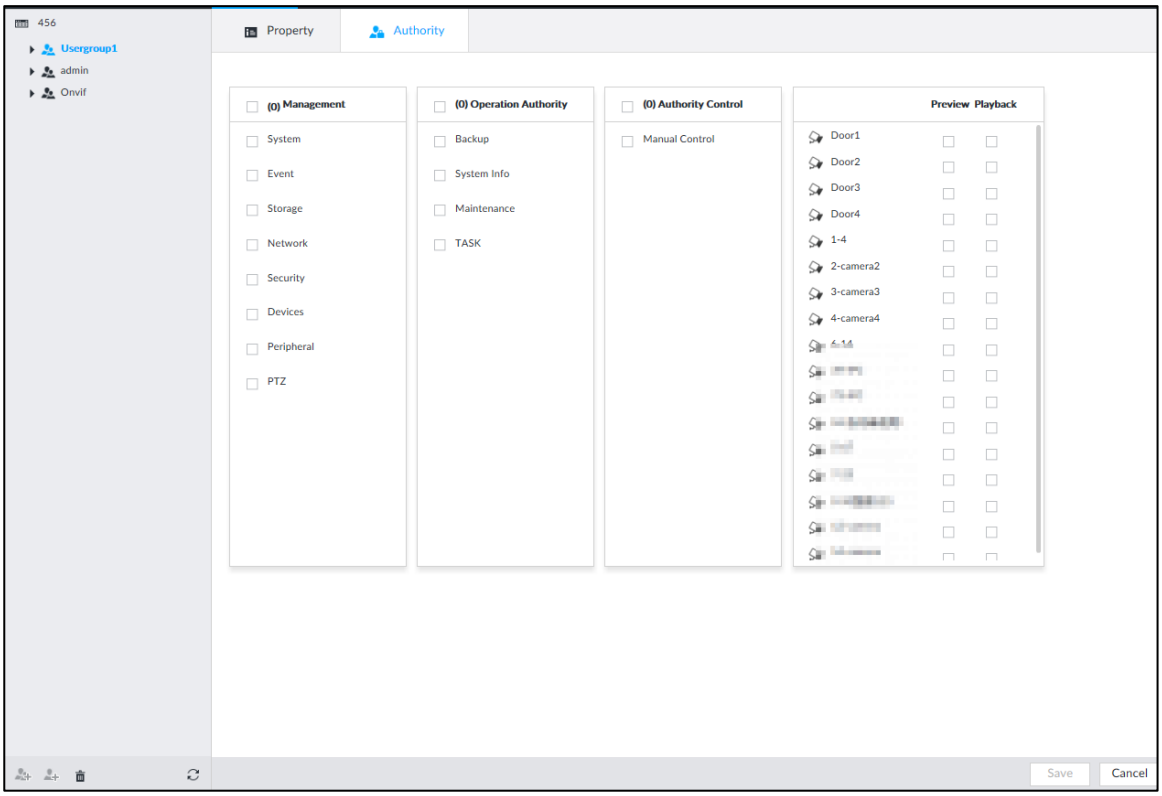
Parameters	Description
Name	Set user group name. The name should consist of 1 to 64 characters and contain English letters, number and special characters.
Group name	Displays user group organization node. System automatically recognizes the group name.
Description	Enter user group description information.
User list	Displays user information of current group.

Step 5 Select user authority.

1) Click **Authority** tab.

The **Authority** interface is displayed. See Figure 6-100.

Figure 6-100 Authority



2) Set user group authorities according to actual situation.

- : means it has the corresponding authority.
- Check the box at the top of the authority list (such as (0) Authority Control) to select all authorities of current category.

Step 6 Click **Save**.

Deleting user group

- Before you delete a user group, delete all users of current group first. User group cannot be restored after being deleted. Be cautious.
- Admin and ONVIF user cannot be deleted.

Step 1 Click , or click on the configuration interface, and then select **ACCOUNT**.

The **Account** interface is displayed.

Step 2 Select user group and click .

The **Input Password** interface is displayed. See Figure 6-101.

Figure 6-101 Enter password

Step 3 Enter current user's login password, and then click **OK**.
The following prompt interface is displayed.

Step 4 Click **OK**.

6.7.2 Device User

The device user is to access and manage the device. System default administrator is admin. It is to add a user and then set corresponding authorities, so that the user can access the resources within its own rights range only.

User authorities adopt the user group authorities settings. It is read-only.

Adding a User

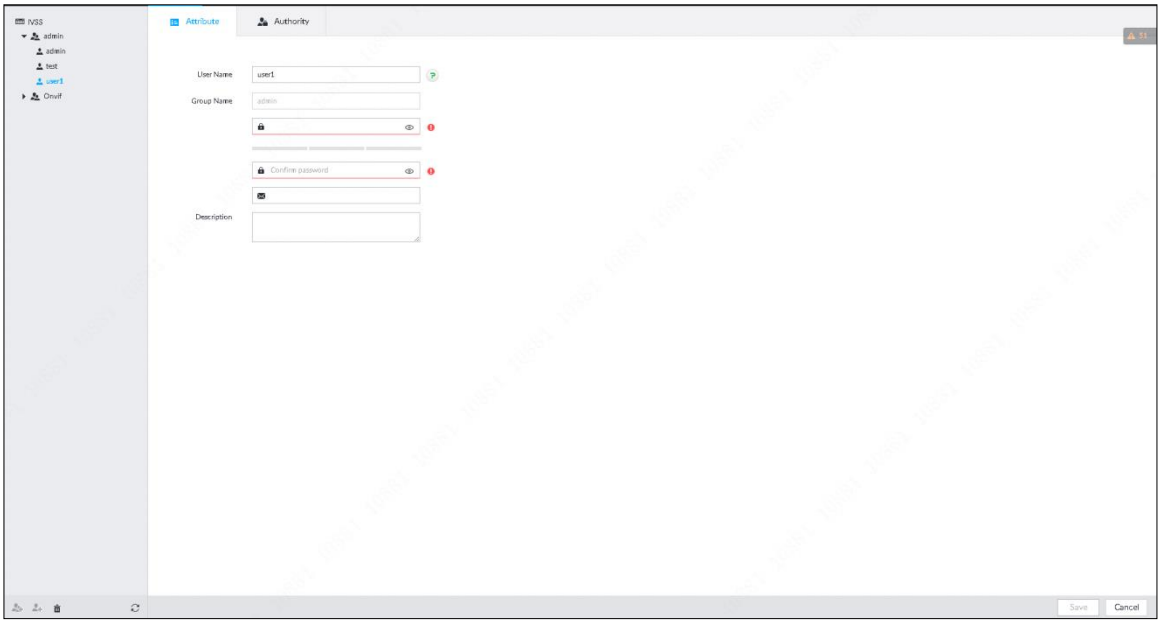
Step 1 Click , or click on the configuration interface, and then select **ACCOUNT**.
The **Account** interface is displayed.

Step 2 Select admin user group or other newly added user group, and then click at the lower-left corner.
The **Input Password** is displayed. See Figure 6-102.

Figure 6-102 Enter password

Step 3 Enter current user's login password, and then click **OK**.
The **Property** interface is displayed. See Figure 6-103.

Figure 6-103 Property



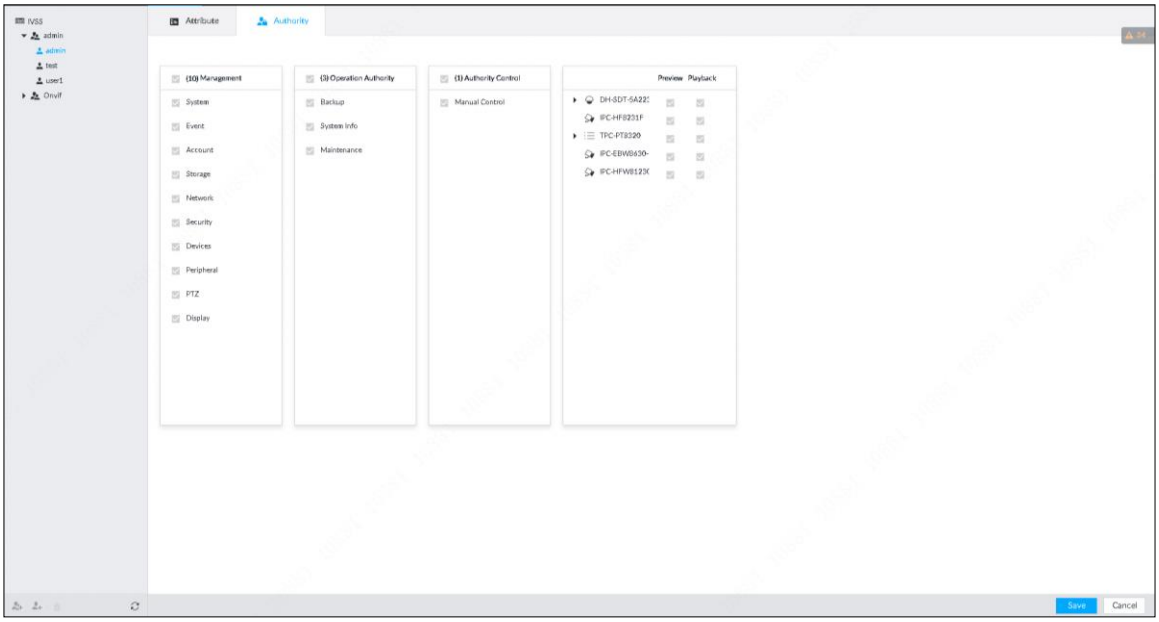
Step 4 Set parameters. For details, see Table 6-33.

Table 6-33 User management

Parameters	Description
Name	Set user name. The name ranges from 1 to 31 characters. It can contain English letters, numbers and special characters (_ @ .).
Group name	Displays user organization node. System automatically identifies it.
Password	In the new password box, enter the new password and enter it again in the Confirm Password box. The password should consist of 8 to 32 non-blank characters and contain at least two types of characters among uppercase, lowercase, number, and special character (excluding ' " ; : &). Usually we recommend the strong password.
Confirm Password	
Description	Describe the user.

Step 5 (Optional) Click the **Authority** tab to view user authority.

Figure 6-104 Authority



Step 6 Click **Save**.

Operation

After adding a user, you can modify user information or delete the user. For details, see Table 6-34.

The user with account management authority can change its own and other users' information.

Table 6-34 User operation

Name	Operation
Edit user information	Select a user from user list. The **Property** interface of the user is displayed, and the user's login password and description information can be modified.
Delete User	Select a user from user list, and then click to delete. ● Before deleting online user, shield the user first. For details, see "8.5 Online User". ● User information cannot be restored after being deleted. Be cautious.

6.7.3 Password Maintenance

Maintain and manage user's login password.

6.7.3.1 Modifying Password

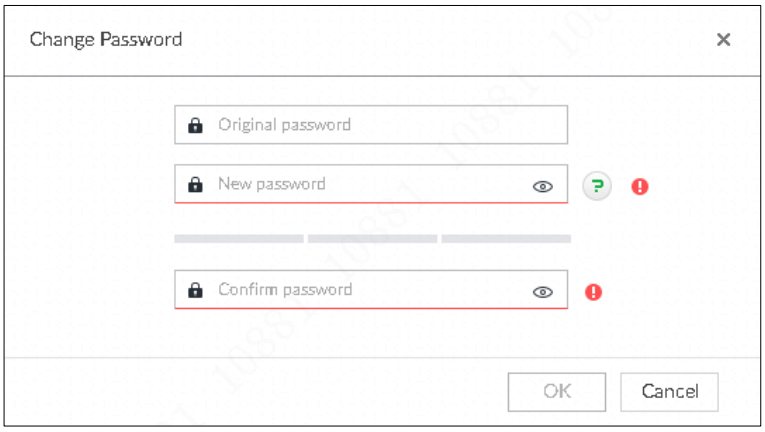
Modify user's login password.

Modifying Password of the Current User

Step 1 Click  at the top right corner, and then select **Modify Password**.

The **Change Password** interface is displayed. See Figure 6-105.

Figure 6-105 Modify password



Step 2 Input old password and then enter new password and then confirm.

Step 3 Click **OK**.

Modifying Password of Other User

Only **Admin** account supports this function.

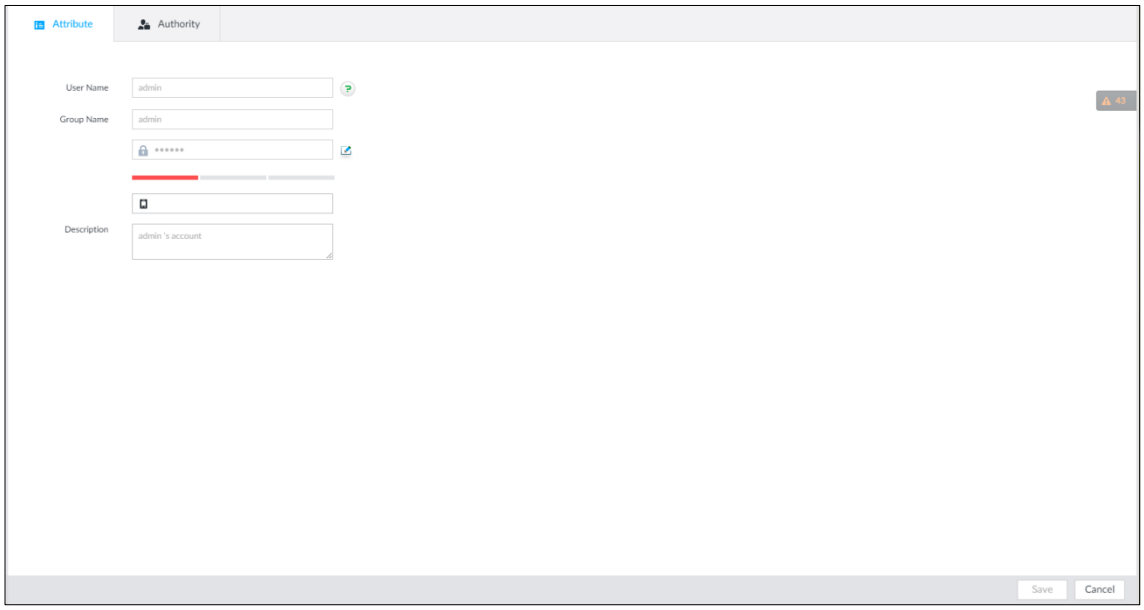
Step 1 Click  , or click  on the configuration interface, and then select **ACCOUNT**.

The **Account** interface is displayed.

Step 2 Select a user.

The **Property** interface is displayed. See Figure 6-106.

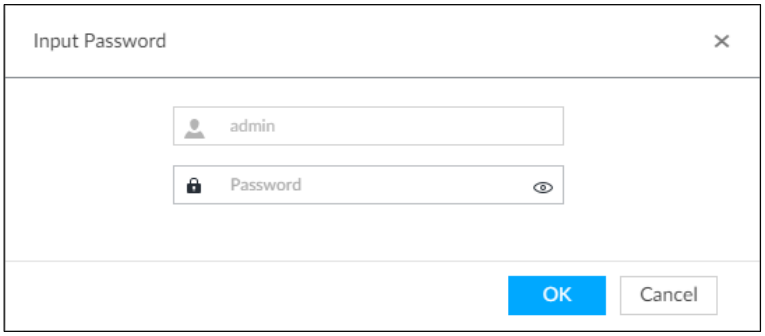
Figure 6-106 Property



Step 3 Click  .

The **Input Password** interface is displayed. See Figure 6-107.

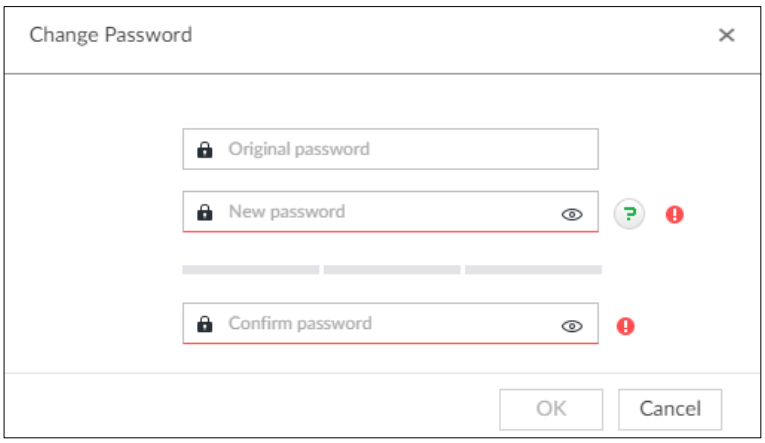
Figure 6-107 Input password



Step 4 Enter current user's login password, and then click **OK**.

The **Change Password** interface is displayed. See Figure 6-108.

Figure 6-108 Modify password



Step 5 In the **New Password** box, enter the new password and enter it again in the **Confirm Password** box.

Step 6 Click **OK**.

6.7.3.2 Resetting Password

You can use email address to reset password once you forgot it.

Enable password reset

Enable the password reset function, and then leave an email address for password reset.

Step 1 Click  , or click  on the configuration interface, and then select **ACCOUNT**.

The **Account** interface is displayed.

Step 2 Select the root node in the device tree on the left.

The **Password Reset** interface is displayed.

Step 3 Click  to enable the password reset function.

Step 4 Enter an email address for resetting password.

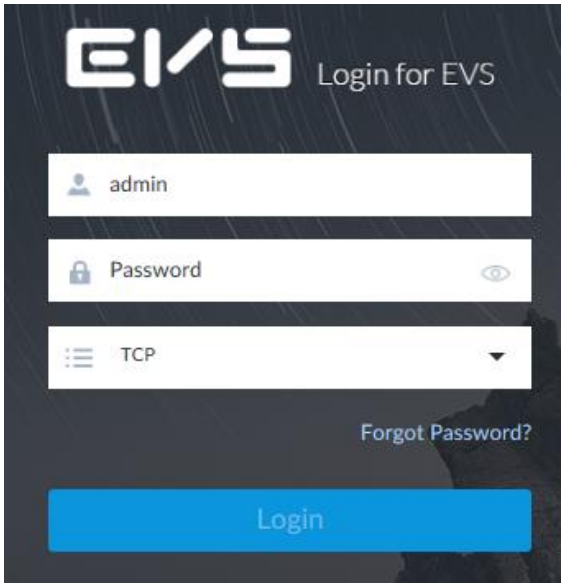
Step 5 Click **Save**.

Reset password

- You can only reset password through the web interface or the PCAPP.
- Make sure that the password reset function is enabled.
- Make sure that the email address for password reset is set.

Step 1 Go to the login interface of the Device. See Figure 6-109.

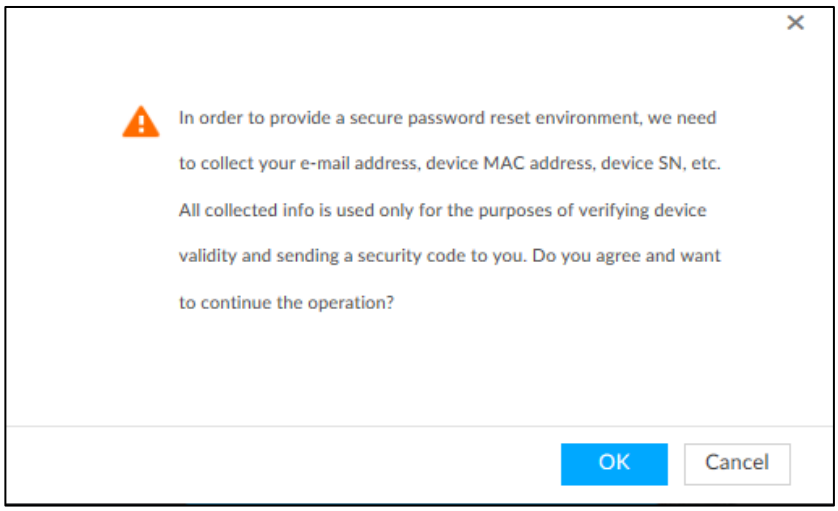
Figure 6-109 Login



Step 2 Click Forgot Password.

- If you have not set the email address information, you cannot reset password. Contact your technical support for help.
- If you have set the email address information, the following prompt is displayed. See Figure 6-110.

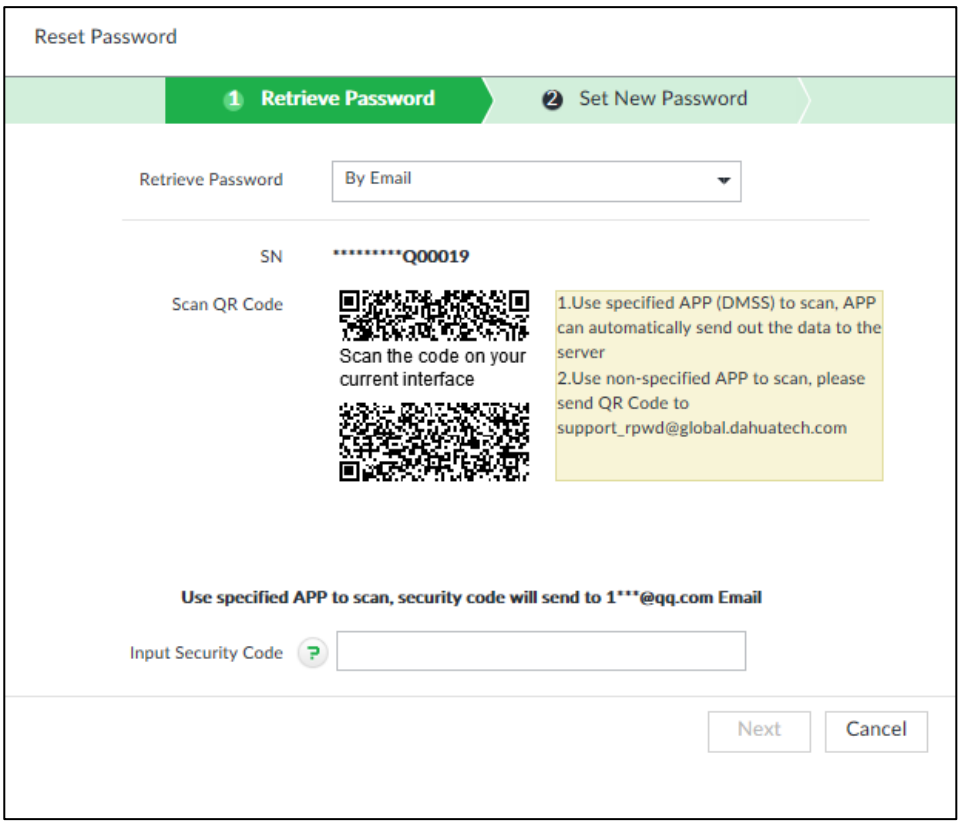
Figure 6-110 Prompt



Step 3 Click **OK**.

The QR code interface is displayed. See Figure 6-111.

Figure 6-111 Scan QR code



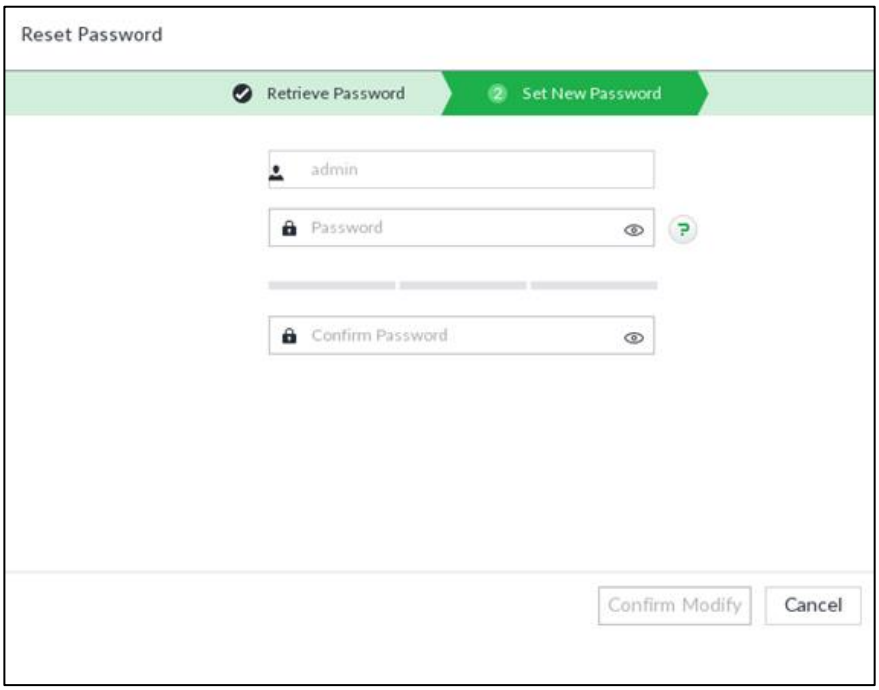
Step 4 Scan the QR code to obtain the security code. Enter the security code that you received in the security code box.

- You can get security codes twice by scanning the same QR code. If you need to get the security code once again, refresh the interface.
- Use the security code to reset the password within 24 hours; otherwise the security code becomes invalid.

Step 5 Click **Next**.

The new password setting interface is displayed. See Figure 6-112.

Figure 6-112 New password setting



Step 6 Set parameters. For details, see Table 6-35.

Table 6-35 Description of password parameters

Parameters	Description
User	The default user name is admin.
Password	In the **New Password** box, enter the new password and enter it again in the **Confirm Password** box. The password should consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special characters (excluding ' " ; : & and space). Enter a strong password according to the password strength indication.
Confirm Password	

Step 7 Click Confirm Modify.

You can log in with the new password.

6.7.4 ONVIF

When the remote device is connecting with the device through ONVIF protocol, use the verified ONVIF account.

- System adopts three ONVIF user groups (admin, user and operator). You cannot add ONVIF user group manually.
- You cannot add user under ONVIF group directly.

Adding ONVIF User

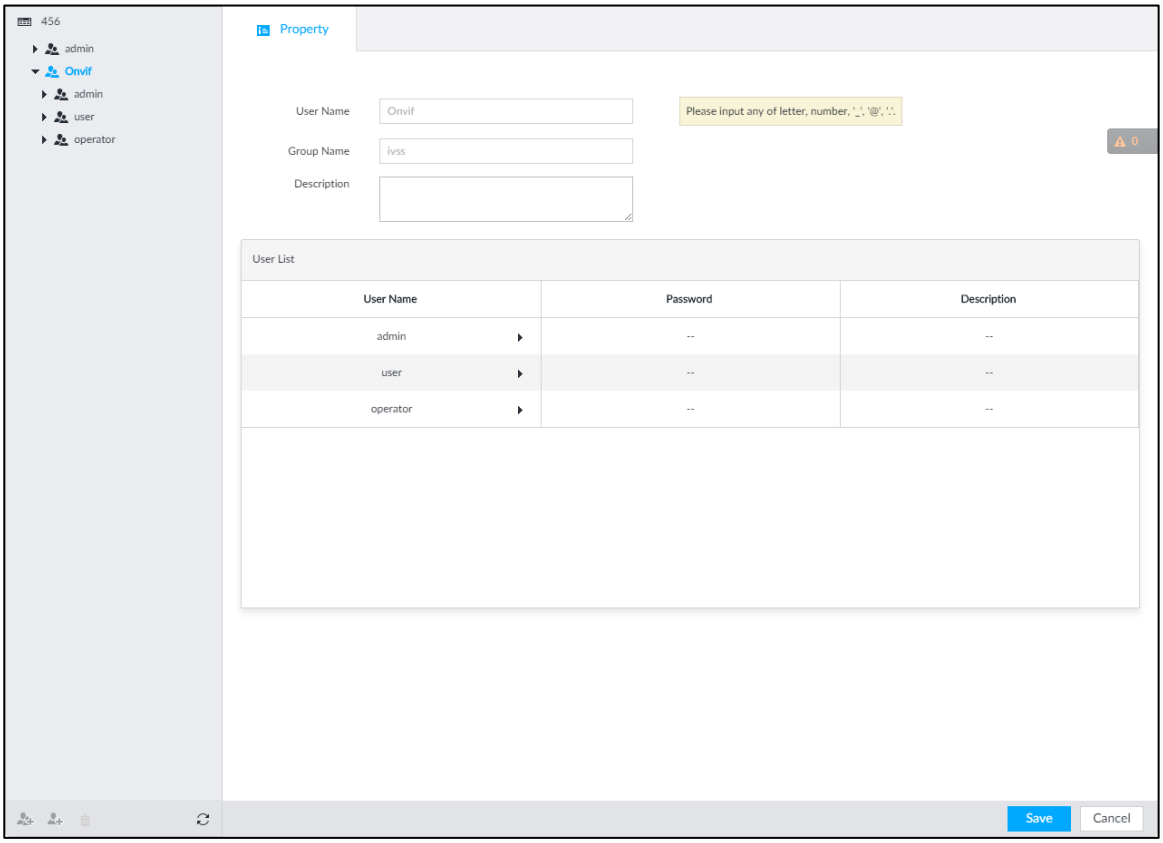
Step 1 Click , or click on the configuration interface, and then select **ACCOUNT**.

The **Account** interface is displayed.

Step 2 Select user group under ONVIF.

The **Property** interface of ONVIF group is displayed. See Figure 6-113.

Figure 6-113 ONVIF



Step 3 Click  at the lower-left corner of the **Property** interface.

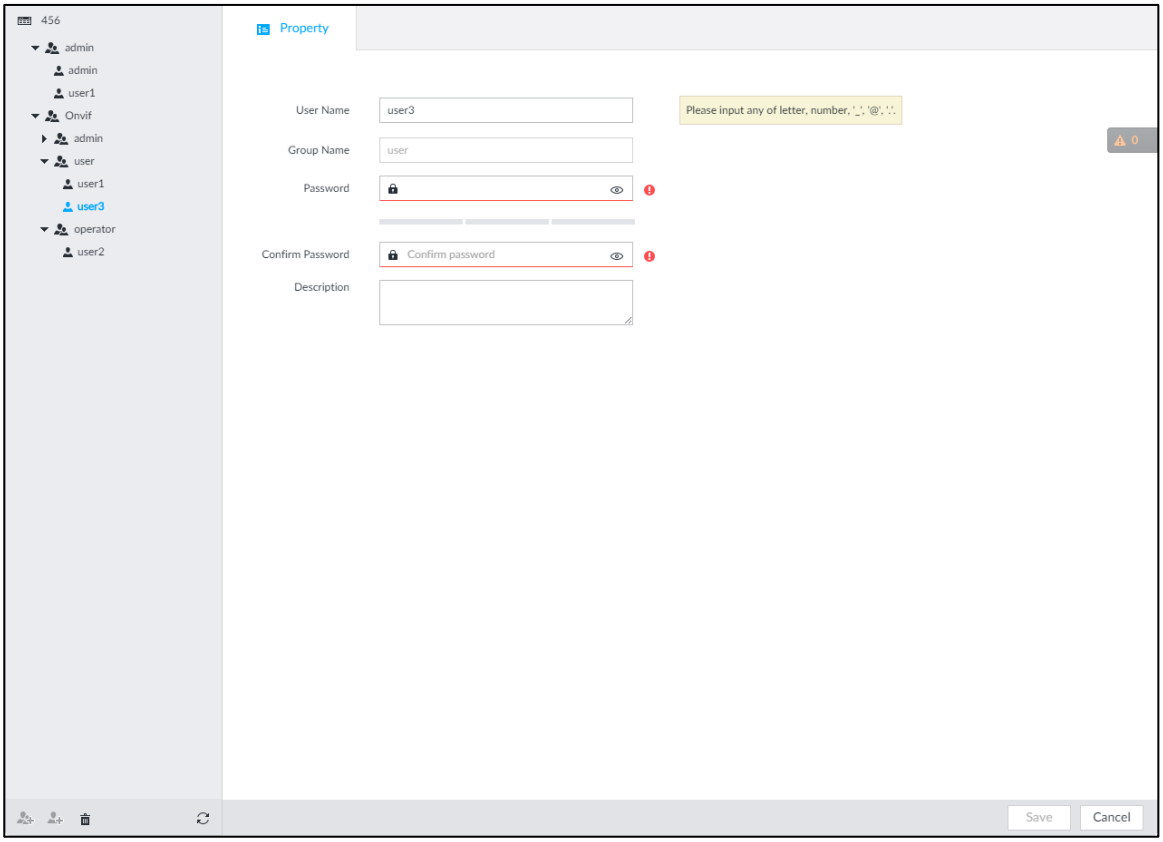
The **Input Password** interface is displayed. See Figure 6-114.

Figure 6-114 Input password

Step 4 Enter the login password of current user, and then click **OK**.

The **Property** interface is displayed. See Figure 6-115.

Figure 6-115 ONVIF property



Step 5 Set parameters. For details, see Table 6-36.

Table 6-36 ONVIF parameters description

Parameters	Description
User Name	Set ONVIF user name. The name ranges from 1 to 31 characters. It can contain English letters, number and special character (_ @ .).
Group name	Displays user organization node. System automatically identifies it.
Password	Set ONVIF user password. The password should consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special characters (excluding ' " ; : & and space).
Confirm Password	
Description	Enter ONVIF user description information.

Step 6 Click **Save**.

Delete ONVIF User

Deleting the admin account is not supported.

Step 1 Click , or click on the configuration interface, and then select **ACCOUNT**.

The **Account** interface is displayed.

Step 2 Select an ONVIF user and click .

The **Input Password** interface is displayed. See Figure 6-116.

Figure 6-116 Input password

Step 3 Enter current user's login password, and then click **OK**.
The following prompt interface is displayed.

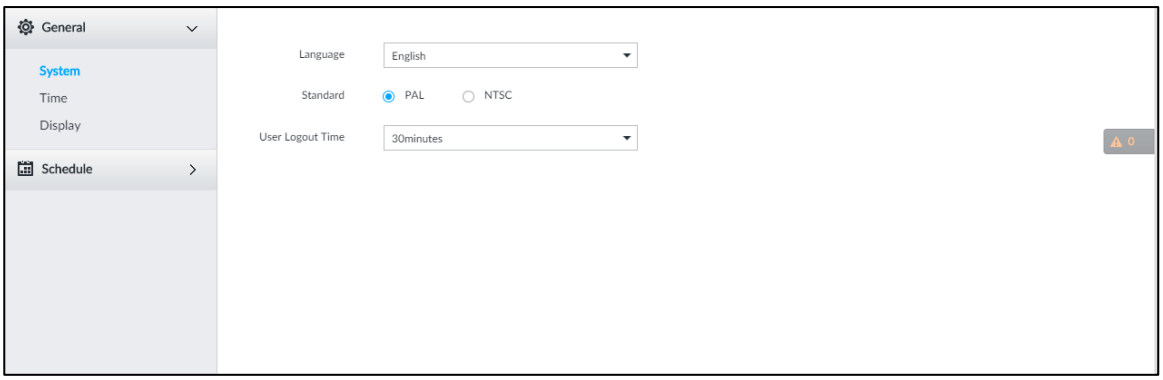
Step 4 Click **OK**.

6.8 System Configuration

Click or click on the configuration interface, select **SYSTEM**. The **SYSTEM** interface is displayed. See Figure 6-117.

Set system basic settings, such as general parameters, time, display parameter, schedule, and voice.

Figure 6-117 System management

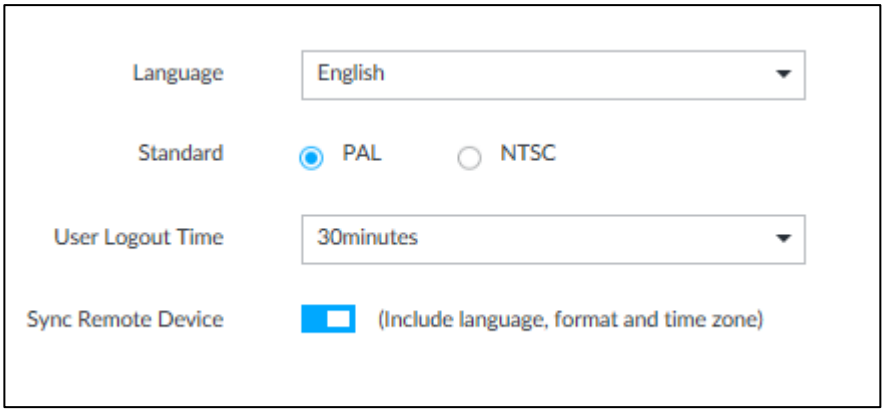


6.8.1 Setting System Parameters

Set system language, standard, user logout time, virtual keyboard, and mouse moving speed.

Step 1 Click , or click on the configuration interface, and then select **SYSTEM > General > System**.
The **SYSTEM** interface is displayed. See Figure 6-118.

Figure 6-118 Configuring system settings



Step 2 Set parameters. For details, see Table 6-37.

Table 6-37 System parameters description

Parameters	Description
Language	Set system language.
Standard	Select video standard. ● PAL is mainly used in China, Middle East and Europe. ● NTSC is mainly used in Japan, United States of America, Canada and Mexico. As a technical standard of processing video and audio signals, PAL and NTSC mainly differ in encoding, decoding mode and field scanning frequency.
User Logout Time	Set automatic logout interval for log-time inactivity. After auto logout, the user needs to log in again to operate. If you set as No Logout, system does not automatically log out.
Sync Remote Device	Click to enable the function. If enabled, the language, standard and time settings configured here will be synchronized to all the connected remote devices.

Step 3 Click **Save**.

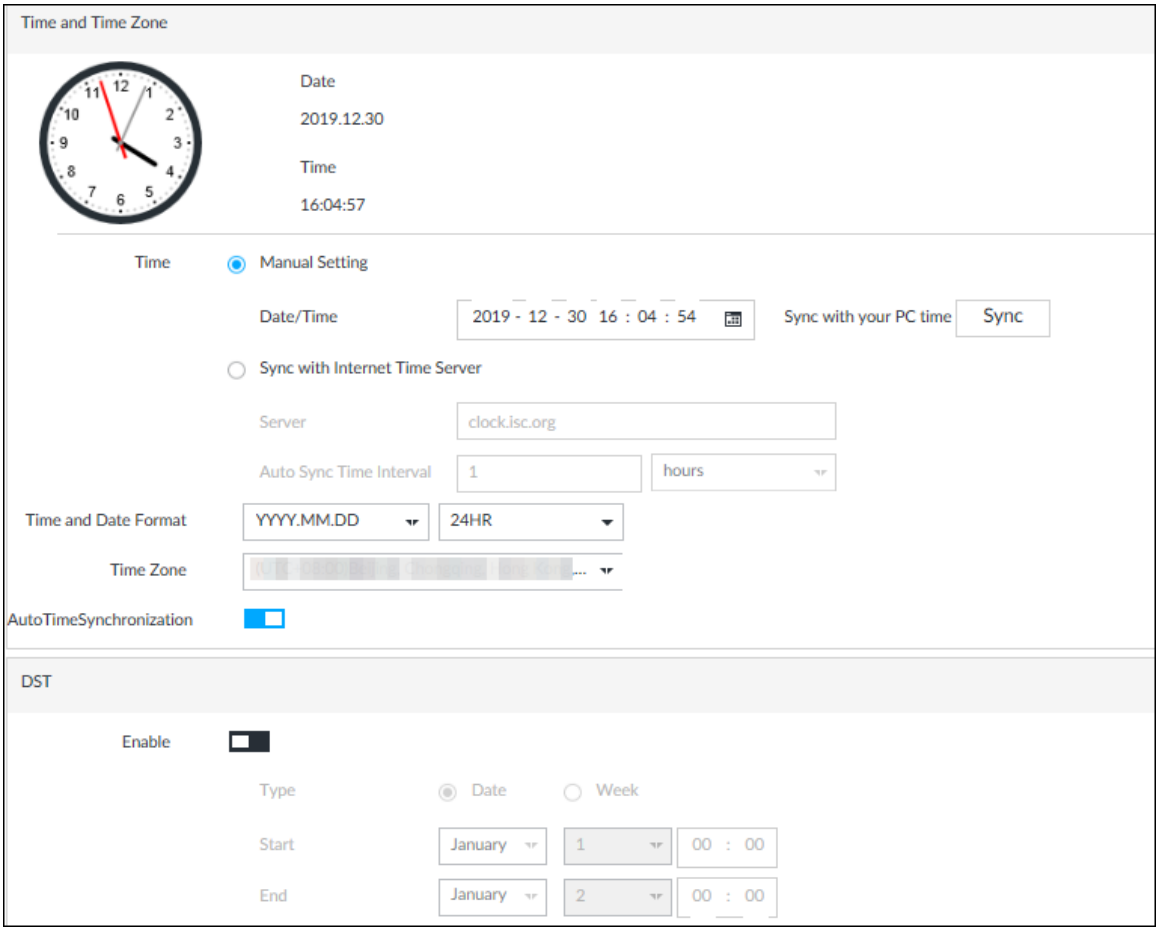
6.8.2 System Time

Set system time, and enable NTP function according to your need. After enabling NTP function, device can automatically synchronize time with the NTP server.

Step 1 Click , or click on the configuration interface, and then select **SYSTEM > General > Time**.

The **Time** interface is displayed. See Figure 6-119.

Figure 6-119 Time



Step 2 Set parameters. For details, see Table 6-38.

Table 6-38 System parameters description

Parameters	Description
Time	Set system date and time. You can set manually or set device to synchronize time with the NTP server. ● **Manual Setting**: Select **Manual Setting** and then set the actual date and time in the following two ways. ◇ Click , and then set the time and date in the calendar. ◇ Click **Sync** to synchronize device time with your PC. ● When using IE11, Google Chrome75 or Firefox61 and later versions, on the web interface of the Device, click **Sync** to synchronize both device time and time zone with the PC. ● When using earlier versions of browser, on the web interface of the Device, click **Sync** to synchronize only device time with PC. ● **Sync with the Internet Time Server**: Check the box and then enter NTP server IP address or domain, and then set **Auto Sync Time Interval**.
Time and date format	Set time and date display format.
Time Zone	Set device time zone.

Parameters	Description
Auto Time Synchronization	After enabling this function, EVS detects system time of remote device once in every interval. When time of remote device is inconsistent with EVS time, EVS will calibrate the time of remote device automatically.

Step 3 (Optional) Set DST.

DST is a system to stipulate local time, in order to save energy. If the country or region where the device is located follows DST, you can enable DST to ensure that system time is correct.

1) Click to enable DST.
2) Select DST mode. It includes **Date** and **Week**.
3) Set DST start time and end time.

Step 4 Click **Save**.

6.8.3 Schedule

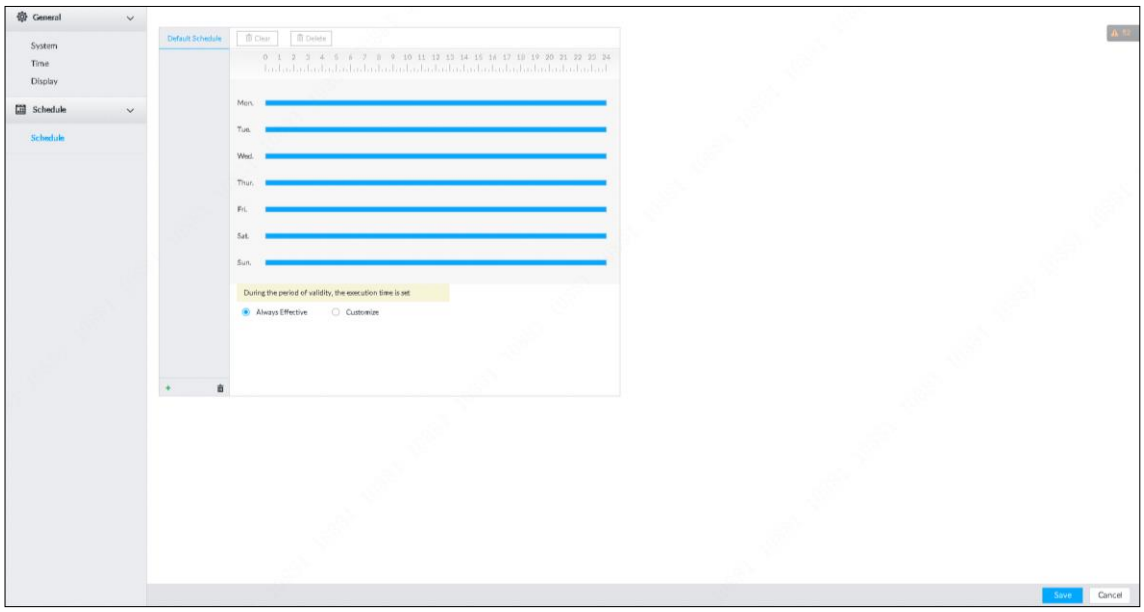
Set schedule. When you are configuring alarm, record arm/disarm period, system can call the schedule directly. System only triggers the corresponding operations during the specified schedule.

Default schedule has been created by default. Default schedule is **Always Effective**, and cannot be modified or deleted.

Step 1 Click , or click on the configuration interface, and then select **SYSTEM > Schedule > Schedule**.

The **Schedule** interface is displayed. See Figure 6-120.

Figure 6-120 Schedule

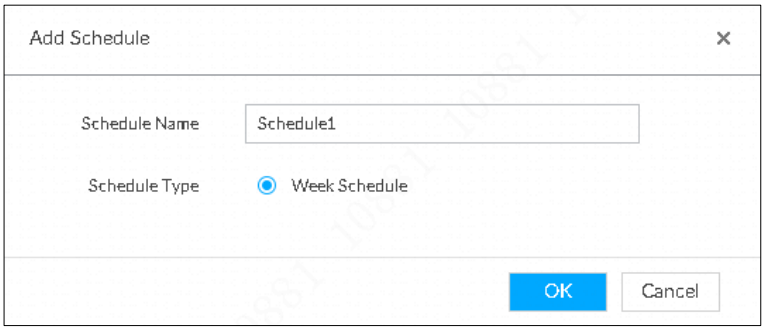


Step 2 Add schedule.

1) Click .

The **Add Schedule** interface is displayed. See Figure 6-121.

Figure 6-121 Adding schedule



2) Set schedule name.
3) Click **OK** to save the configuration.

Step 3 Set valid time period. It includes **Always Effective** and **Customize**.

Step 4 Set validity period of schedule.

- The step is for customized mode only.
- Each calendar supports maximum 50 validity periods.
- The blue area on the time bar means the validity period.

On the time bar, you can:

- Click the blue area, and is displayed. Drag to adjust the start time and end time of validity period.
- Press the any blank space on the time bar, and drag to the right to add a validity period.
- Click **Clear** to clear all validity periods of current schedule.
- Select a validity period, and then click **Delete** to delete the period.

Step 5 Click **Save**.

Select an added schedule, and then click to delete.

6.9 Storage Management

6.9.1 Storage Mode

Allocate disks or RAID groups to different disk groups, and store video and image to specified disk group.

6.9.1.1 Setting Disk Group

Disk and created RAID group are allocated to group 1 by default. You can allocate disk and RAID group to other groups according to your actual needs.

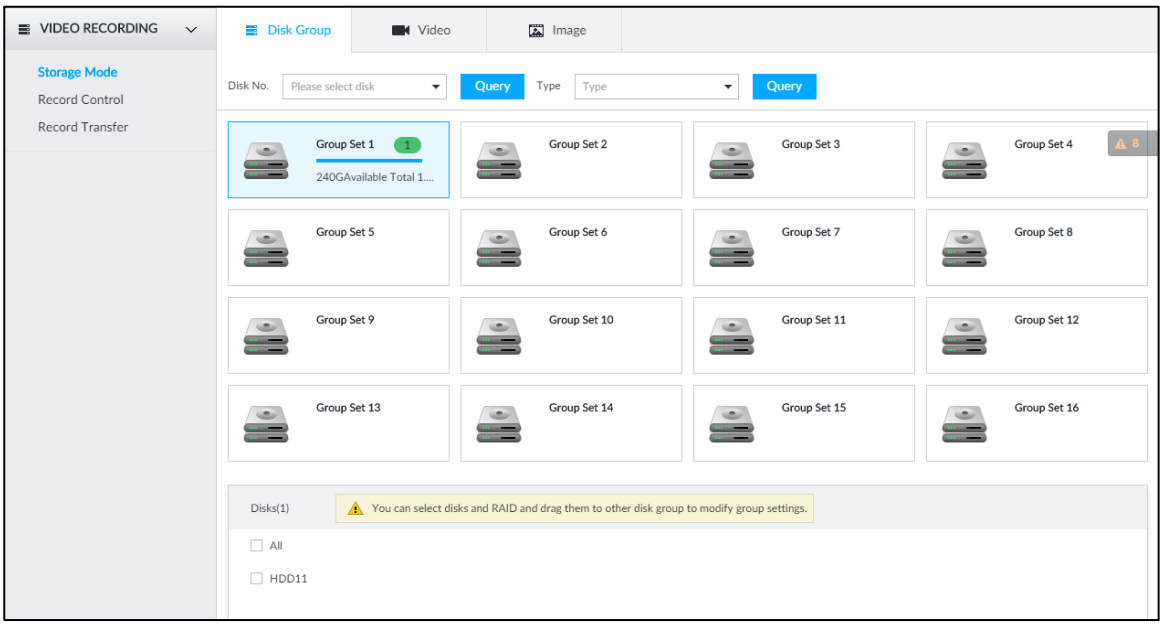
The default number of disk group is the same as the maximum number of HDD that EVS supports. Fox example, the Device supports a maximum number of 16 HDDs, and then the default number of disk group is 16.

Step 1 Click , or click on the configuration interface, and then select **VIDEO RECORDING > Storage Mode > Disk Group**.

The **Disk Group** interface is displayed. See Figure 6-122.

- Select HDD or RAID group from Please select disk, and then click **Query** to search the disk group of HDD or RAID group.
- The value (such as 1) next to the group name refers to the number of HDD and RAID group in the disk group. If instead, is displayed, it means no available HDD or RAID group in the disk group, but there is video or image stored in the disk group.

Figure 6-122 Disk group



Step 2 Click a disk group.

The disk information of the group is displayed.

Step 3 Select HDD or RAID group from **Disks**, and then drag the HDD or the RAID group to another disk group.

Disk grouping takes effect immediately.

Select **All** to select all the HDDs and RAID groups of the disk group.

After configuring disk groups, you can also view which disk group the selected disk, video or picture belongs to. For details, see Table 6-39.

Table 6-39 Disk group functions

Function	Description
View the disk group of a disk, video or picture	Click Disk No. Please select disk, select a disk or RAID group, and then click Query to search for the disk group that the selected disk or RAID group belongs to.

View disk groups of video or image	Select **Video** or **Image** from Type Type , and then click **Query** to search for disk groups of the selected type.

6.9.1.2 Setting Video/Image Storage

Videos/images of all channels are stored in disk group 1 by default. You can store the videos/images in different disk groups according to actual needs. Two methods are available to set video/image storage.

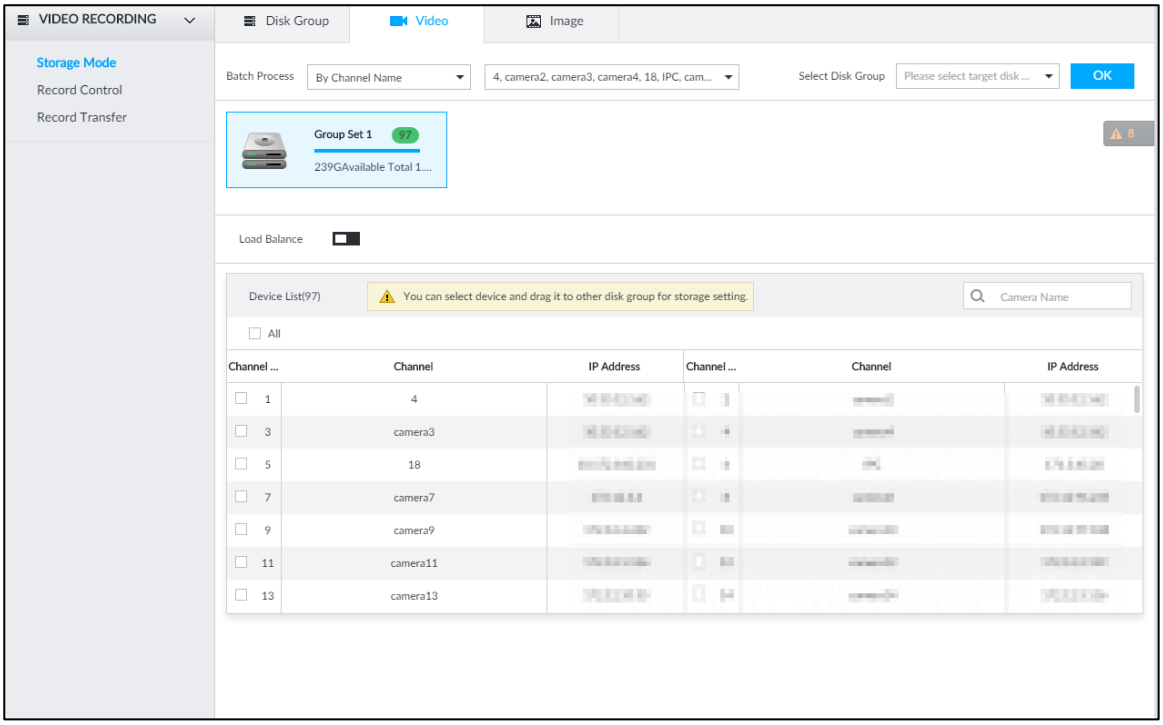
This section takes storing video for example. To store images, the procedure is similar.

Method 1

Step 1 Click , or click on the configuration interface, and then select **VIDEO RECORDING > Storage Mode >Video**.

The **Video** interface is displayed. See Figure 6-123.

Figure 6-123 Video



Step 2 Select filtering way from the **Batch Process** drop-down list.

- By Channel Name: Select channel according to the channel name.
- By Logical Channel No.: Select channel that is connected to EVS. In this case, **Start Channel No.** and **End Channel No.** need to be configured.

Step 3 In the **Select Disk Group** drop-down list, select target disk group.

In the drop-down list, only disk group with available HDD or RAID group is displayed.

Step 4 Click **OK**.

Disk grouping takes effect immediately.

Method 2

Step 1 Click , or click on the configuration interface, and then select **VIDEO RECORDING > Storage Mode >Video**.

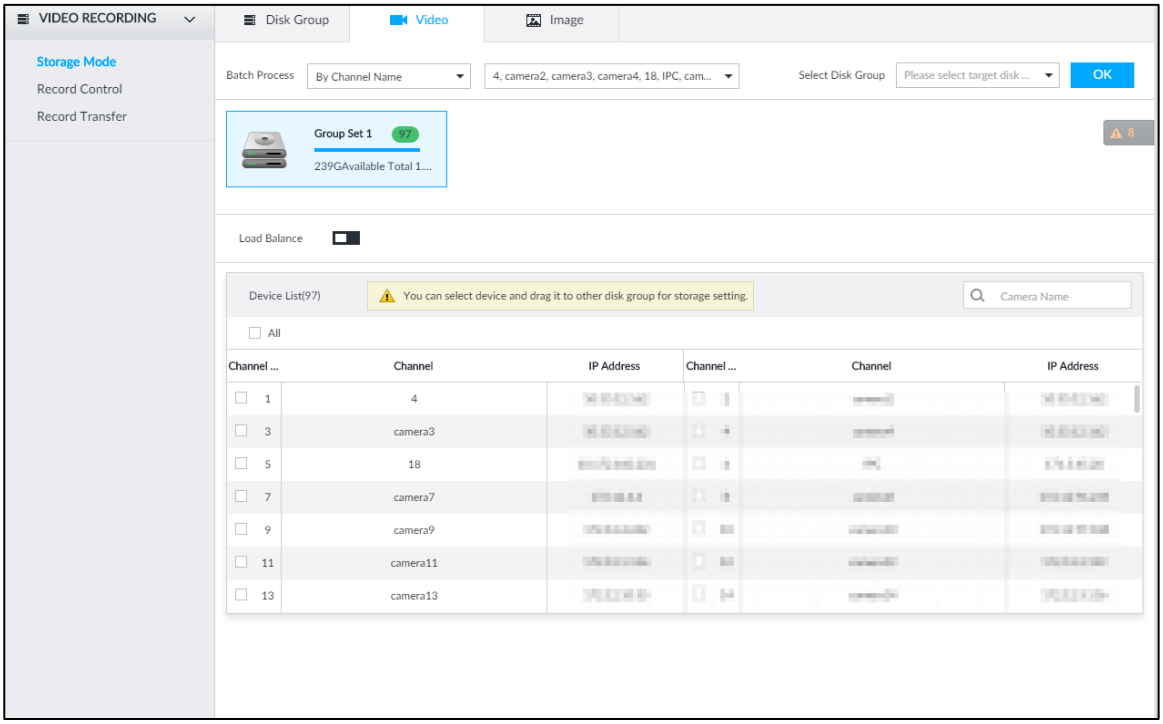
The **Video** interface is displayed. See Figure 6-123.

Step 2 Click a disk group.

The linked channels of the disk group are displayed in **Device List**. See Figure 6-124.

- Only disk group with available HDD or RAID group or linked channel is displayed.
- The value (such as 1) next to the group name refers to the number of HDD and RAID group in the disk group. If instead, is displayed, it means no available HDD or RAID group in the disk group, but there is video or image stored in the disk group.

Figure 6-124 Device list



Step 3 (Optional) Click to enable load balance, and then the icon turns into blue. To disable it, click it again, and then the icon turns into gray.

- After load balance is enabled, if one disk group has no usable disk, the video of all channels that belong to this disk group will be stored into all the usable disk groups.
- When load balance is not enabled, if one disk group has no usable disk, the video of all channels that belong to this disk group will be stored in another usable disk group.

Step 4 Select a channel from the device list, and drag the channel to the target disk group. Disk grouping takes effect immediately.

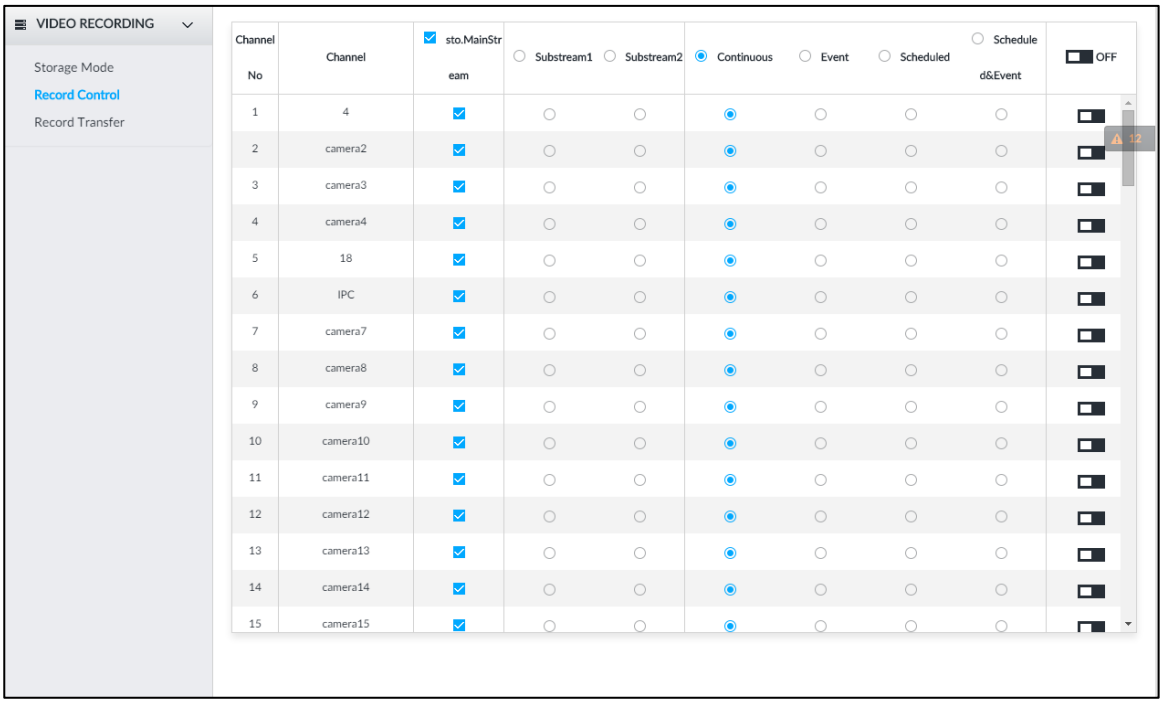
6.9.2 Record Control

Configure recording schedules for channels.

Step 1 Click , or click on the configuration interface, and then select **VIDEO RECORDING > Record Control**.

The **Record Control** interface is displayed. See Figure 6-125.

Figure 6-125 Record control



Step 2 Select one stream type.

- means that the type is selected.
- means that the type is not selected.

Step 3 Select a recording method.

Step 4 (Optional) click to disabled the recording schedule configuration of the selected channel

Step 5 Click **Save**.

6.9.3 Record Transfer

When the device and an IPC are disconnected, the IPC continues to record and stores the recording in the SD card. After the network is recovered, the device will download the recording during the disconnection from the IPC.

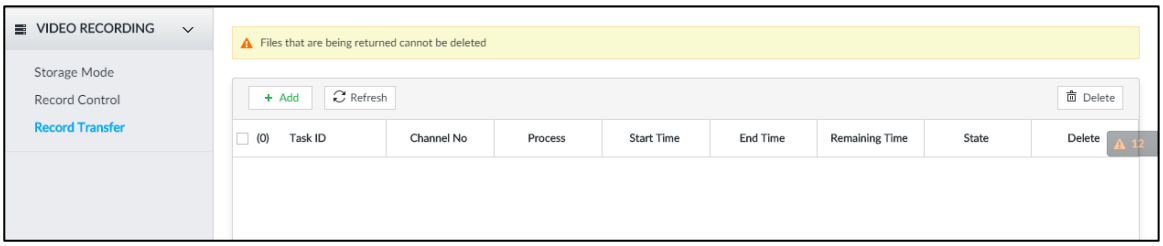
Two ways for record transfer after the network recovers.

- Automatic download: After the network recovers, the device automatically downloads the recording in the set time period, see "6.2.1.2 Configuring Storage Plans."
- Manual download: If ANR is not enabled when you set the storage plan, after the network recovers, the device can not automatically download the recording during the disconnection, the user can manually create the download task.

Step 1 Click , or click on the configuration interface, and then select **VIDEO RECORDING > Record Transfer**.

The **Record Transfer** interface is displayed. See Figure 6-126.

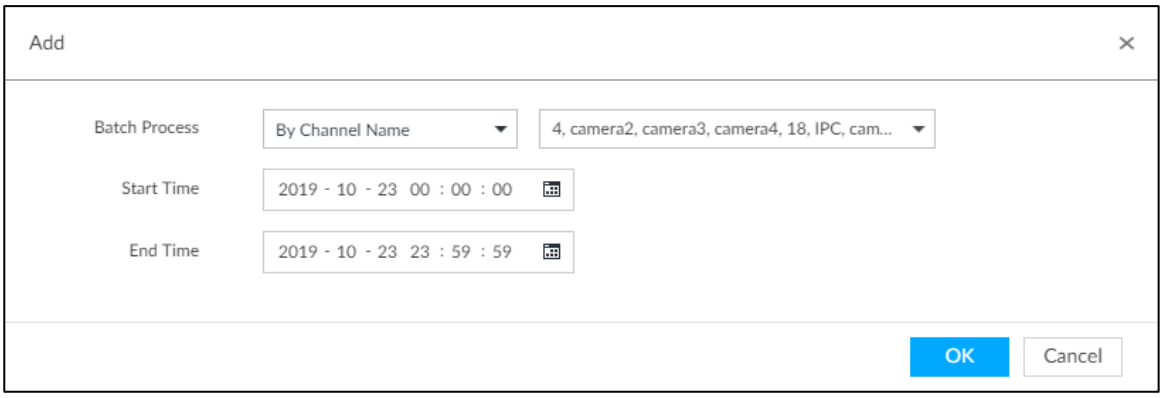
Figure 6-126 Record transfer



Step 2 Click **Add**.

The **Add** interface is displayed. See Figure 6-127.

Figure 6-127 Add



Step 3 Select By Channel Name or By Channel No. in the Batch Process drop-down list.

Step 4 Set time period of the video to be searched.

Step 5 Click **OK**.

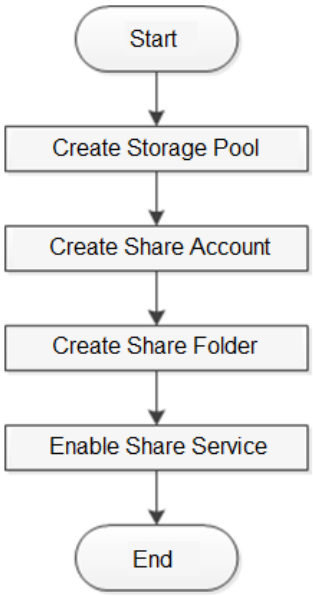
The transfer progress is displayed.

Select a transfer task, click Delete to delete it. A task in progress cannot be deleted.

6.10 IPSAN

IPSAN is a storage technology based on IP network. After you create a storage pool, you can share your storage directory with other devices through iSCSI.

Figure 6-128 Configuring IPSAN



6.10.1 Creating Storage Pool

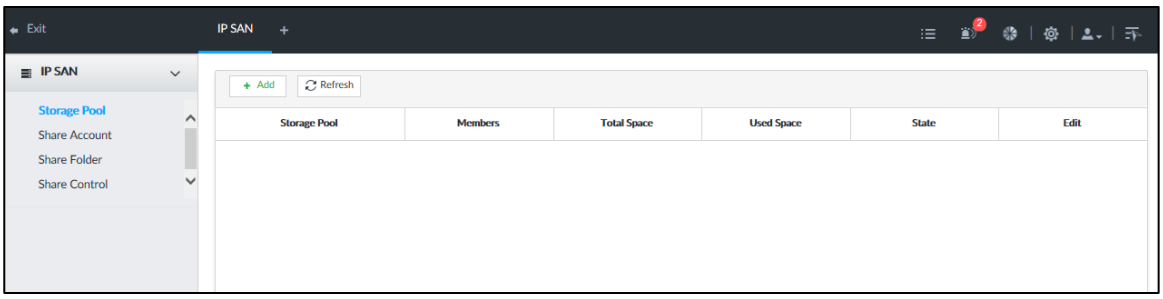
Storage pool is a logical storage space after the storage device is virtualized. It is managed by the system, and can be composed of multiple actual disks or RAID. IPSAN is one of the major means to realize storage virtualization.

Creating storage pool will format the disk. Be careful!

Step 1 Click , or click on the configuration interface, and then select **IPSAN > Storage Pool**.

The **Storage Pool** interface is displayed. See Figure 6-129.

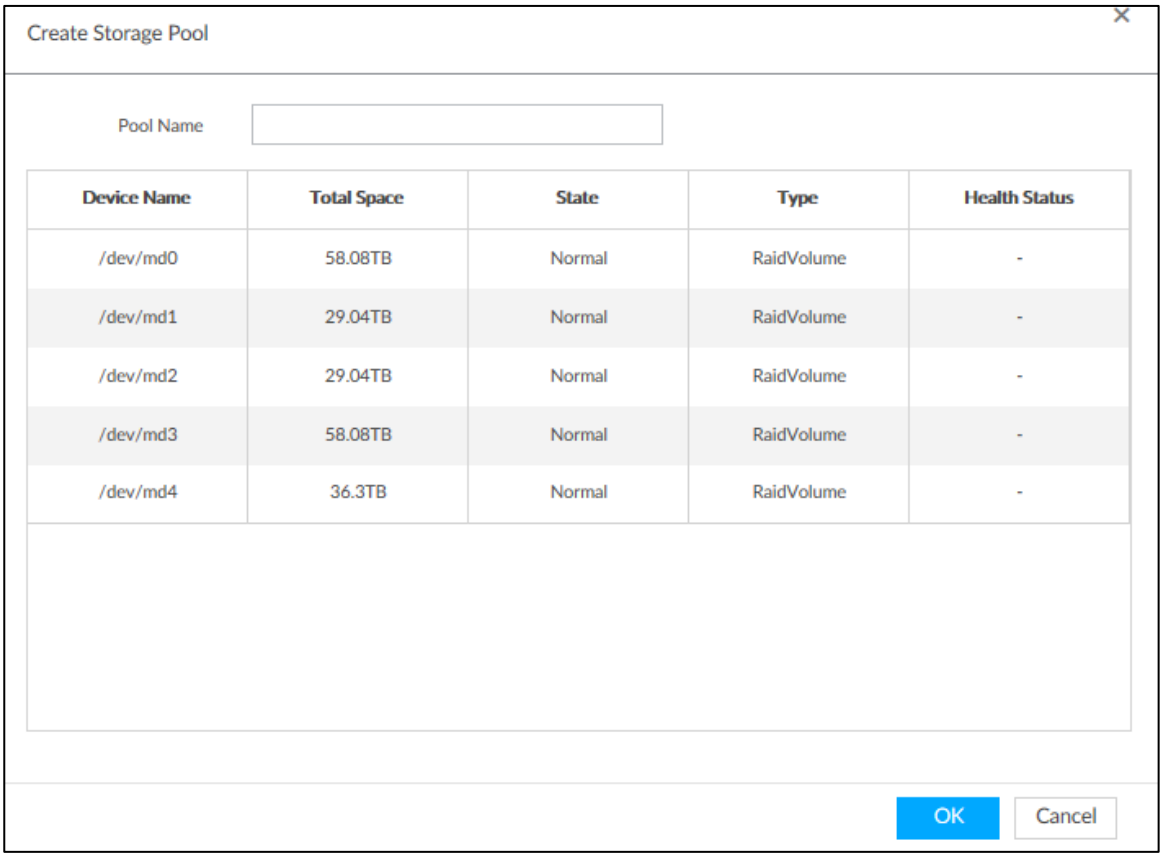
Figure 6-129 Storage pool



Step 2 Click **Add**.

The **Create Storage Pool** interface is displayed. See Figure 6-130

Figure 6-130 Create storage pool



Step 3 Name the pool, and then select a disk or RAID group.

By default, in the **Device Name** column, "sdx" (x ranges from a to z) is a disk, such as /dev/sda, and "mdx" (x is number) is a RAID group, such as /dev/md0.

Step 4 Click **OK**.

The confirmation dialogue box is displayed.

Step 5 Click **OK**.

The system starts to create storage pool.

To delete a pool, click . To refresh the storage pool list, click **Refresh**.

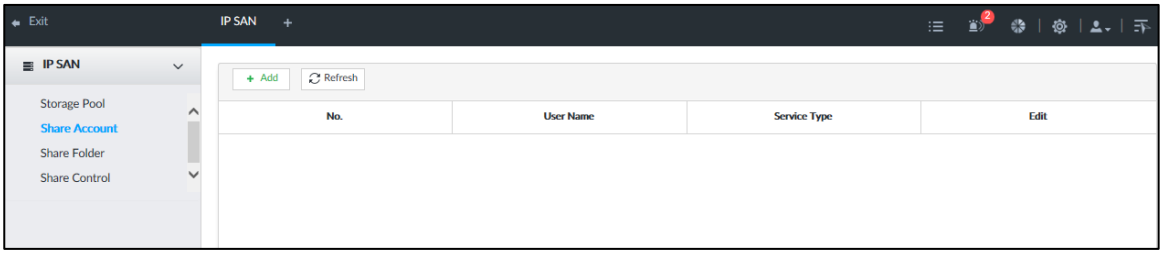
6.10.2 Managing Share Account

Use share account to access the shared folder.

Step 1 Click , or click on the configuration interface, and then select **IPSAN > Share Account**.

The **Share Account** interface is displayed. See Figure 6-131.

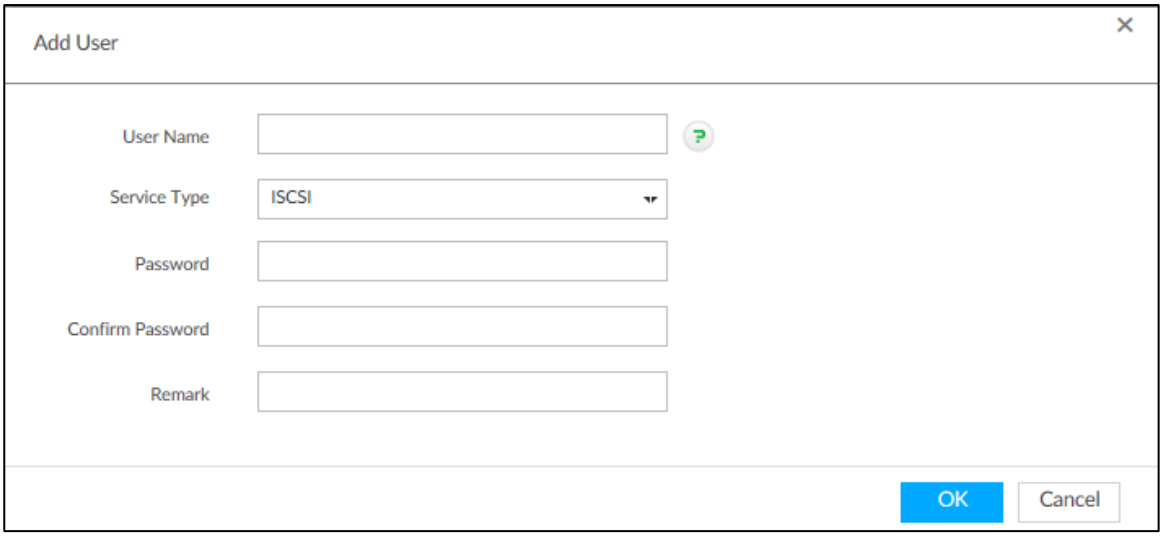
Figure 6-131 Share account



Step 2 Click **Add**.

The **Add User** interface is displayed. See Figure 6-132.

Figure 6-132 Add user



Step 3 Set parameters. For details, see Table 6-40.

Table 6-40 Parameters description

Parameters	Description
User Name	Name the user.
Service Type	You can add an iSCSI share user.
Password	Set a password for the user. The password shall be 12-digit if the service type is iSCSI.
Confirm password	
Remark	Set the remark information for identifying the user.

Step 4 Click **OK**.

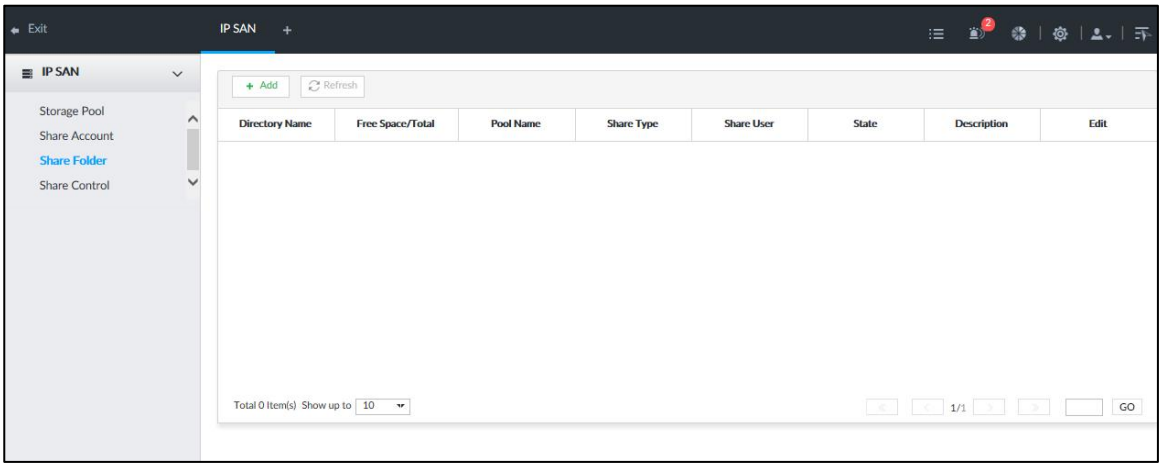
6.10.3 Configuring Share Folder

Configure the share folders that other users can access remotely.

Step 1 Click , or click on the configuration interface, and then select **IPSAN > Share Folder**.

The **Share Folder** interface is displayed. See Figure 6-133.

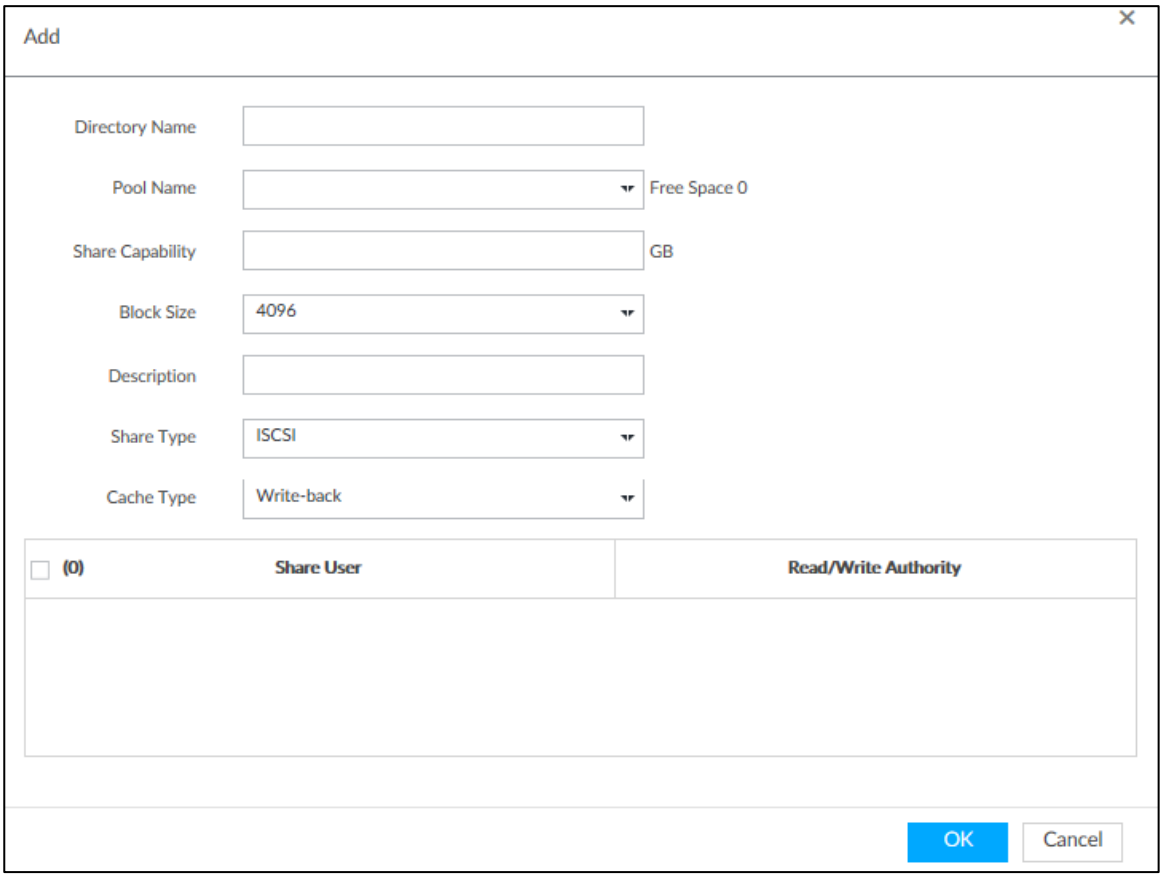
Figure 6-133 Share folder



Step 2 Click **Add**.

The **Add** interface is displayed. See Figure 6-134.

Figure 6-134 Add (iSCSI)



Step 3 Set parameters. For details, see Table 6-41.

Table 6-41 Parameters description

Parameters	Description
Directory Name	Name the folder.
Pool Name	Select a pool. The available free space of the selected pool is displayed beside the pool name.

Parameters	Description
Share Capacity	Set the space of the folder.
Block Size	Set the block size of the folder, such as 512 Byte, 1024 Byte, 2048 Byte and 4096 Byte. You need to set block size when the service type is iSCSI.
Descriptipon	(Optional) Describe the folder for the ease of identifying it.
Share Type	You can only select iSCSI.
Cache Type	Set the cache strategy of the share folder, including **Write-back** and **Direct-write**. ● Direct-write: Write data directly into be disk and refresh the cache data. You are recommended to select direct-write when you have less data to store and have a high requirement for data integrity. ● Write-back: Write data into the cache, and then store it into the disk when the cache is full or system is available. You are recommended to select write-back when you have much more data to store and have a low requirement for data integrity. You need to select the cache type when the service type is iSCSI.

Step 4 Click **OK**.

- The system forces to disable automatic maintenance the first time you create a share folder, or when you create a folder when automatic maintenance is enabled automatically. Once you have configured IPSAN, you can manually enable automatic maintenance. For details, see "8.6.3 Automatic Maintenance."
- Click to delete a share folder; click to edit a share folder; click **Refresh** to refresh the current configuration.
- Modifying cache type takes effect after the Device restarts.

6.10.4 Share Control

Users can access the share folders only when the share service is enabled.

Step 1 Click , or click on the configuration interface, and then select **IPSAN > Share Control**.

The **Share Control** interface is displayed. See Figure 6-135.

Figure 6-135 Share control

Step 2 Click  to enable share service; click  to disable share service.

Step 3 Click **OK**.

7 System Management

This chapter introduces system management operations including file management, maintenance, and task management.

7.1 File Management

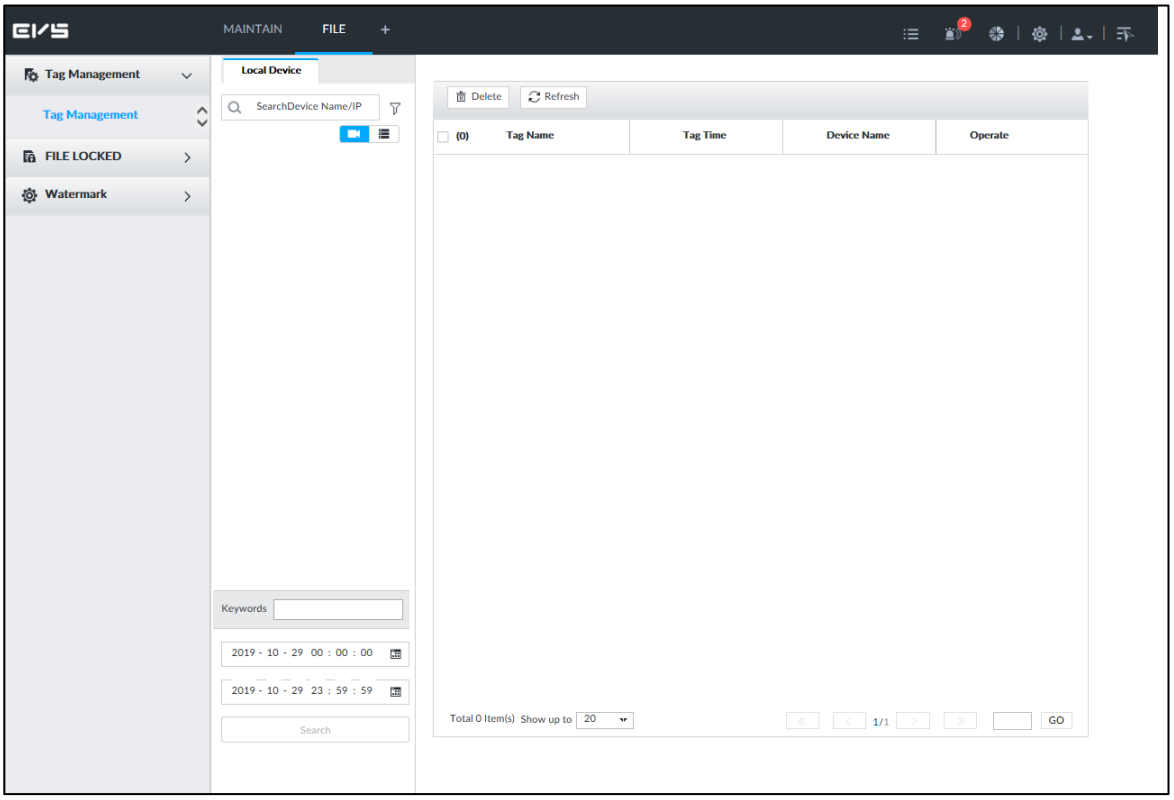
This section introduces the management of tags, lock filed and watermark.

7.1.1 Video Tag Management

Step 1 Click , and then select **FILE > Tag Management > Tag Management**.

The **Tag Management** interface is displayed. See Figure 7-1.

Figure 7-1 Tag management



Step 2 Select a channel, set start time and end time, and then click **Search**.

The tags during the set time period are displayed.

- Click to view the corresponding video.
- Click to edit the tag.
- Click to delete the tag.
- Select multiple tags and click **Delete** to delete the tags in batches.
- Click **Refresh** to video the latest tags.

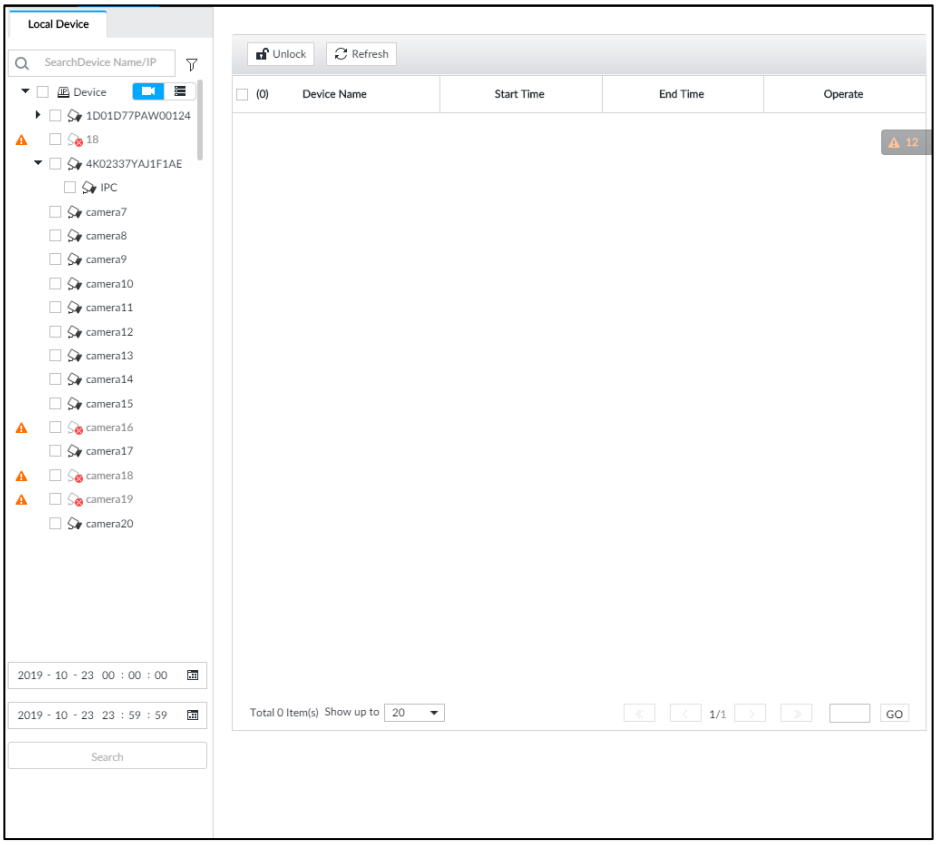
7.1.2 FILE LOCKED

View the locked video files, and you can unlock them.

Step 1 Click , and then select **FILE > FILE LOCKED > FILE LOCKED**.

The **FILE LOCKED** interface is displayed. See Figure 7-2.

Figure 7-2 FILE LOCKED interface



Step 2 Select a channel, set start time and end time, and then click **Search**.

The locked files are displayed.

- Click to view the video of the locked file.
- Click **Refresh** to view the latest locked files.
- Click to unlock a file.
- Select multiple files and click **Unlock** to unlock the files in batches.

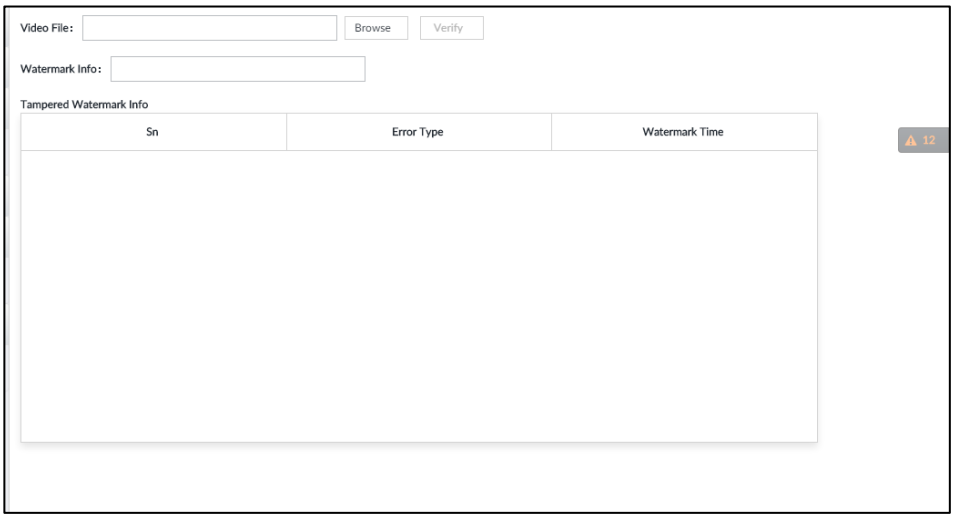
7.1.3 Watermark Verification

Verify whether a video filed is tempered.

Step 1 Click , and then select **FILE > Watermark > Watermark**.

The **Watermark** interface is displayed. See Figure 7-3.

Figure 7-3 Watermark



Step 2 Click **Browse** to select a video file.

Step 3 Click **Verify**.

- Normal
  If the verification result is normal, the correct watermark is displayed.
- Exception
  If the verification result is abnormal, the abnormal watermark and its type are displayed.

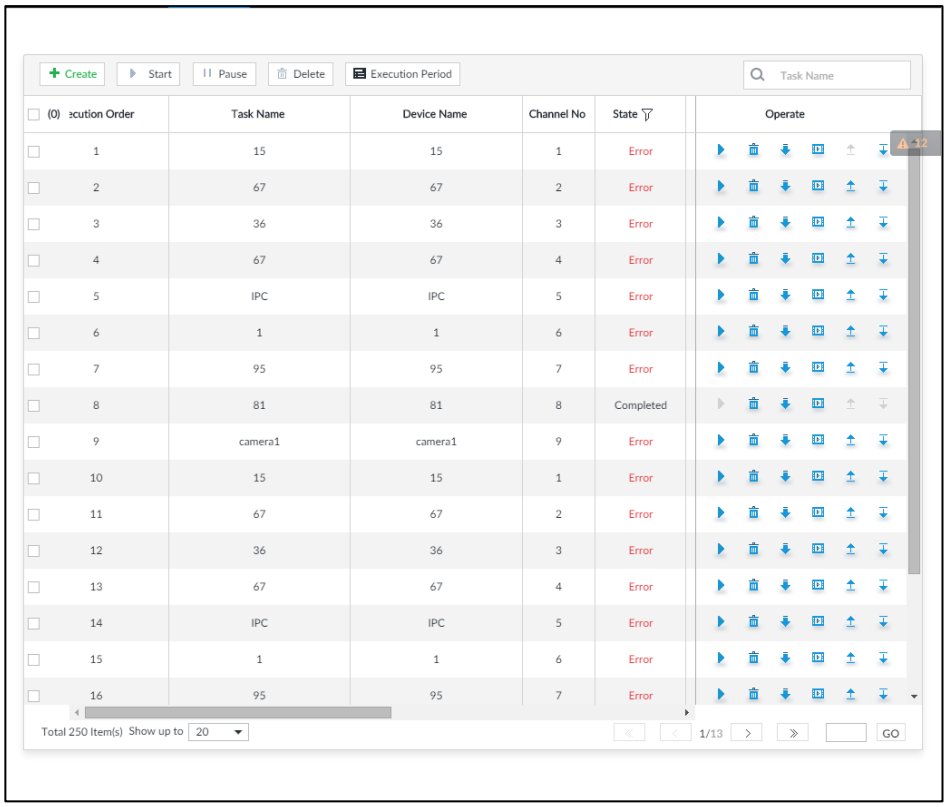
7.2 Task Management

Configure intelligent analysis tasks for metadata of recorded videos. After the intelligent analysis task is completed, you can view the metadata video on the playback interface.

Step 1 Click  , and then select **TASK**.

The **TASK** interface is displayed. See Figure 7-4.

Figure 7-4 Task management

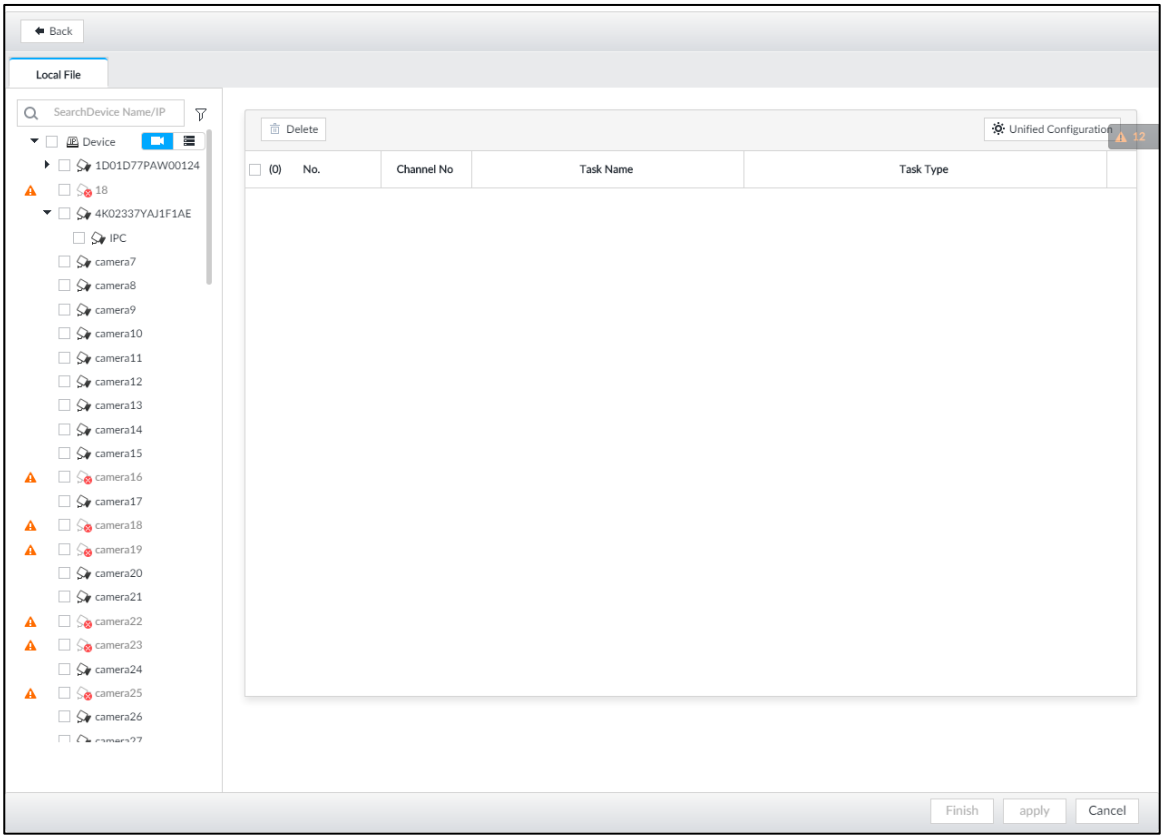


Step 2 Click **Create**.

The **Create** interface is displayed. See Figure 7-5.

In the device tree, indicates that the camera has been configured with intelligent analysis task.

Figure 7-5 Create a task

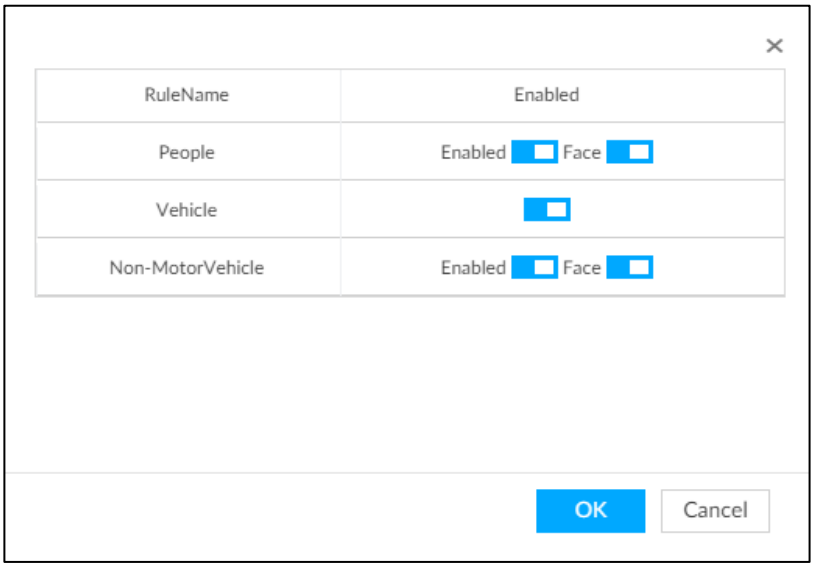


Step 3 Select a channel from the resource tree.

Step 4 Select a task type in the **Task Type** drop-down list.

1) Click the task type cell. The following dialogue box is displayed. See Figure 7-6.

Figure 7-6 Task type



2) Select a task type. For details, see Table 7-1.

Table 7-1 Task type description

Rule Name	Operations
People	● Click next to **Enabled** to enable human detection as well as face detection. ● Click next to **Face** to disable face detection. You can only enable face detection after human detection has been enabled.
Vehicle	Click to enable vehicle detection.
Non-Motor Vehicle	● Click next to **Enabled** to enable non-motor vehicle detection as well as face detection. ● Click next to **Face** to disable face detection. You can only enable face detection after non-motor vehicle detection has been enabled.

3) Click **OK**.

Select multiple channels, click **Unified Configuration**, and then you can configure tasks in batches.

Step 5 Select start time and end time.

Step 6 Click **Apply**.

After creating the tasks, you can perform the following operations. See Table 7-2.

Table 7-2 Task operations

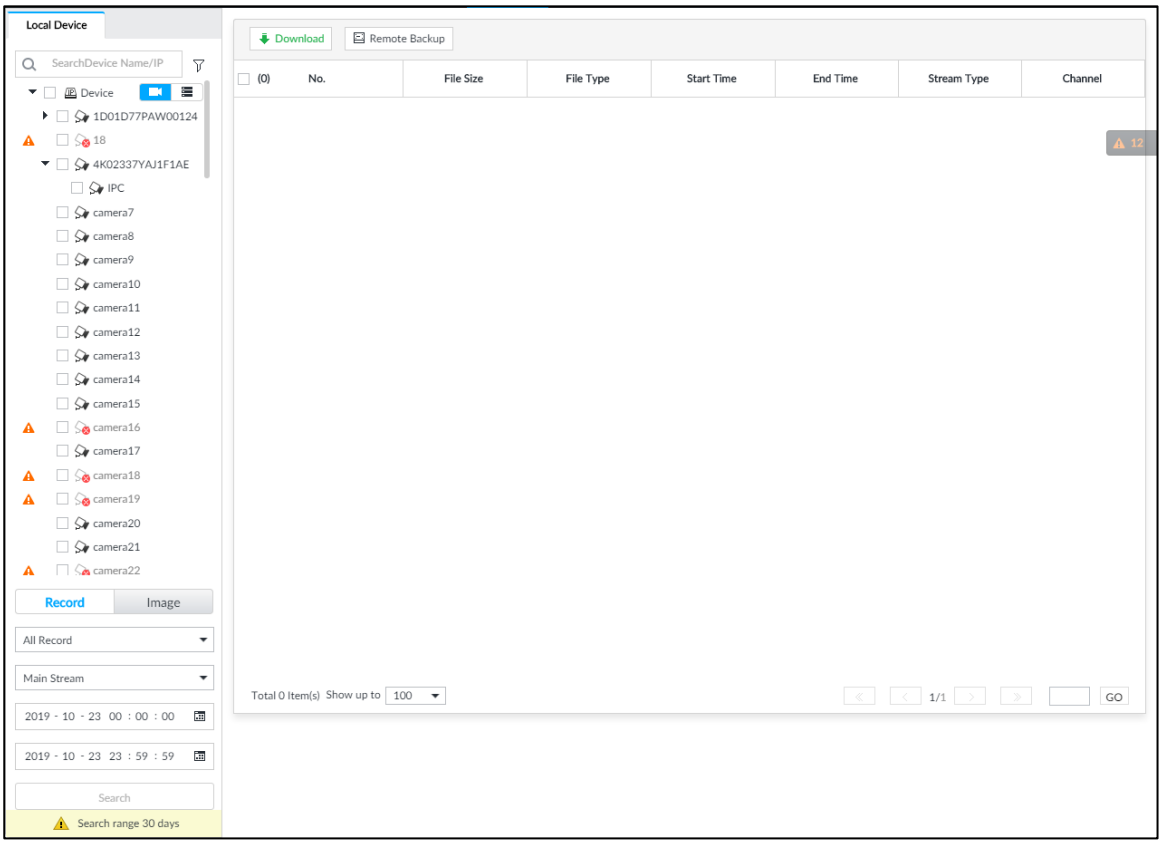
Function	Operation
	Click to start a task.
	Click to delete a task.
	Click to download the task video.
	Click to play back video of the task.
	Click to increase the priority of the task.
	Click to lower the priority of the task.
Start	Select tasks, and then click **Start** to start the tasks in batches.
Pause	Select tasks, and then click Pause to pause the tasks in batches.
Delete	Select tasks, and then click **Delete** to delete the tasks in batches.
Execution Period	Select one or more tasks, click **Execution Period**, and then select a time period. Tasks automatically run during this time period.

7.3 Backup

Step 1 Click , and then select **BACKUP**.

The **BACKUP** interface is displayed. See Figure 7-7.

Figure 7-7 Backup



Step 2 Select a channel from the resource tree on the left.

Step 3 Select a file type.

- Record
  - ◇ You can select record types including **All**, **Manual Record**, **Video Detect**, and **IO Alarm**.
  - ◇ You can select a stream type including **Main Stream** and **Sub Stream**.
  - ◇ Set the time period.
- Image

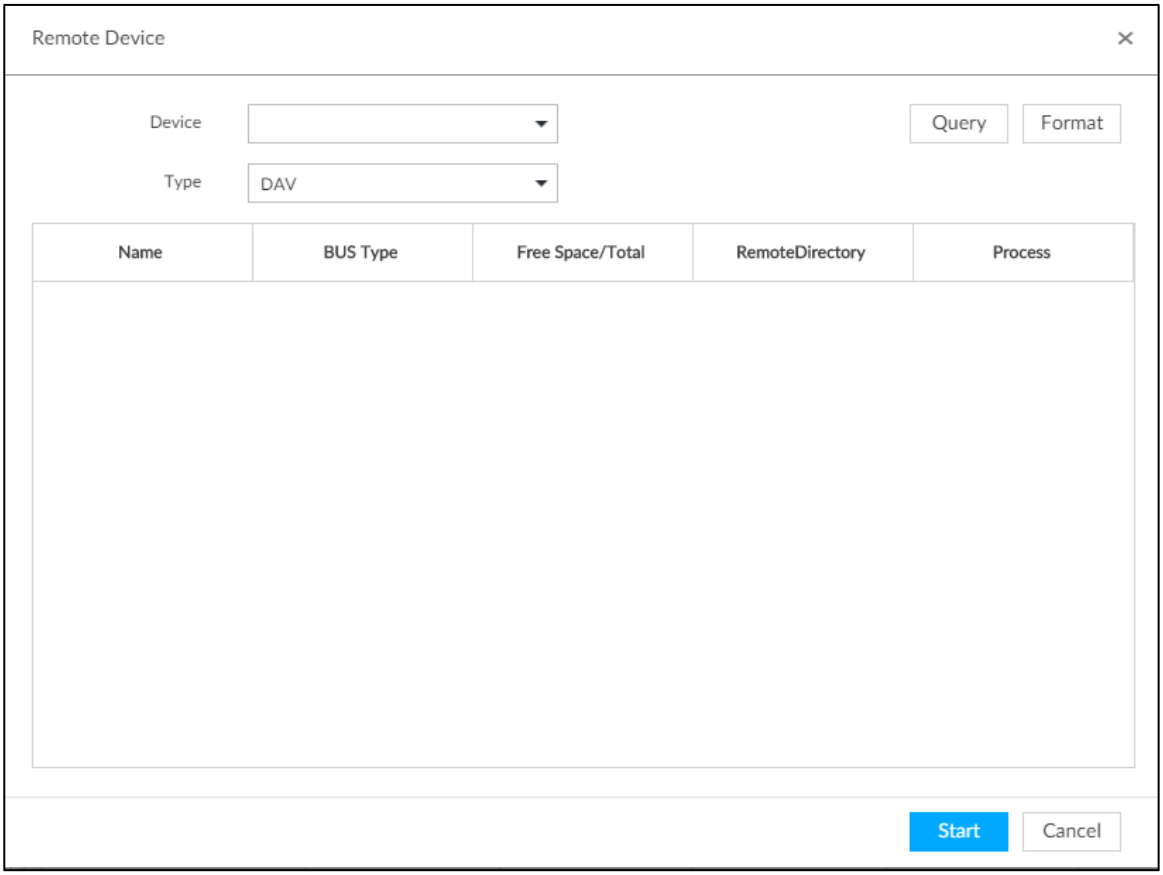
  Select a snapshot type from **Manual Snap** and **Video Detect**.

Step 4 Click **Search**.

Step 5 Select a searched file, and then click **Remote Backup**.

The **Remote Backup** interface is displayed. See Figure 7-8.

Figure 7-8 Remote backup



Step 6 Click **Query** to search for connected third-party storage devices.

Step 7 Select a storage device, and then in the **Type** box, select a target format for the file.

Step 8 (Optional) Click **Format** to format the selected storage device. The formatting operation will clear all data of the storage device. Be cautious.

Step 9 Click **Start** to start backing up the file.

Step 10 (Optional) You can select a searched file, and then click **Download** to download it.

7.4 AI Report

Click , select **AI REPORT** and then you can view in-area people counting report and queue people counting report.

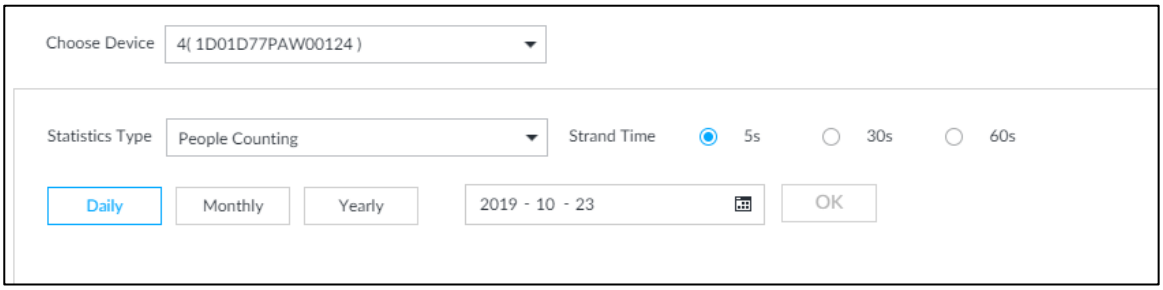
When viewing the report of a camera, make sure that people counting rules hva been configured on it. For details, see "4.4 People Counting."

7.4.1 In-area People Counting Report

Step 1 Click , select **AI REPORT > AI REPORT> In Area** People Counting Report.

The **In Area People Counting Report** interface is displayed. See Figure 7-9.

Figure 7-9 In-area people counting report



Step 2 Select a device to be searched. You can only select AI fisheye camera.

Step 3 Select a statistics type.

- People counting: Select **People Counting**, and then select the strand time (5 s, 30 s, 60 s).
- Average strand time: The report shows the average strand time during different time periods.

Step 4 Select a time period type from **Daily**, **Monthly**, and **Yearly**, and then set the corresponding date, month or year.

Step 5 Click **OK**.

The report is displayed. See Figure 7-10 and Figure 7-11.

Figure 7-10 People counting report

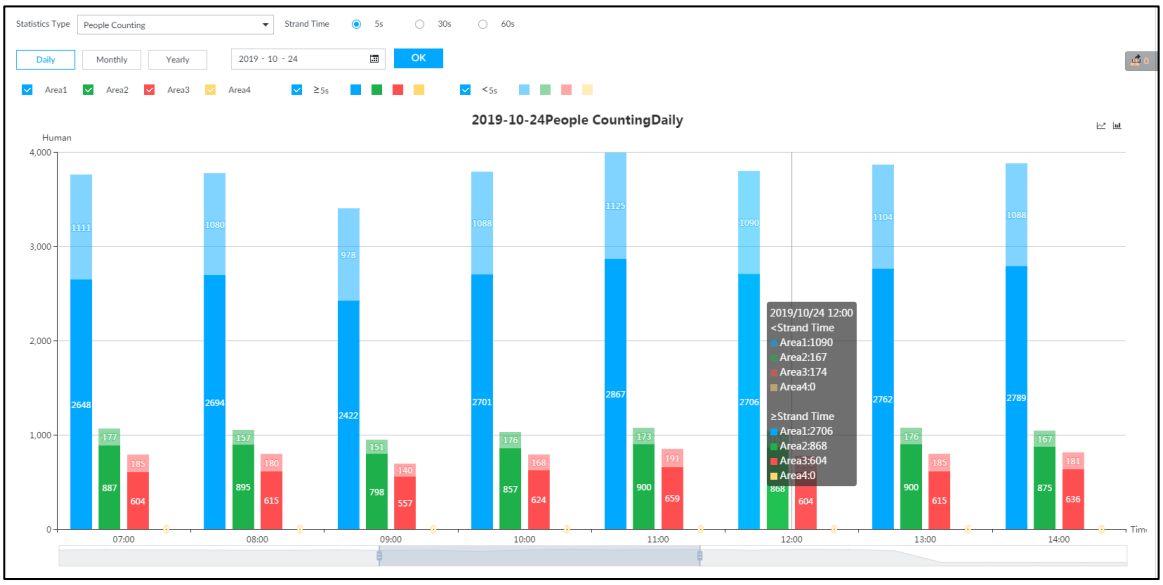


Figure 7-11 Average strand time report

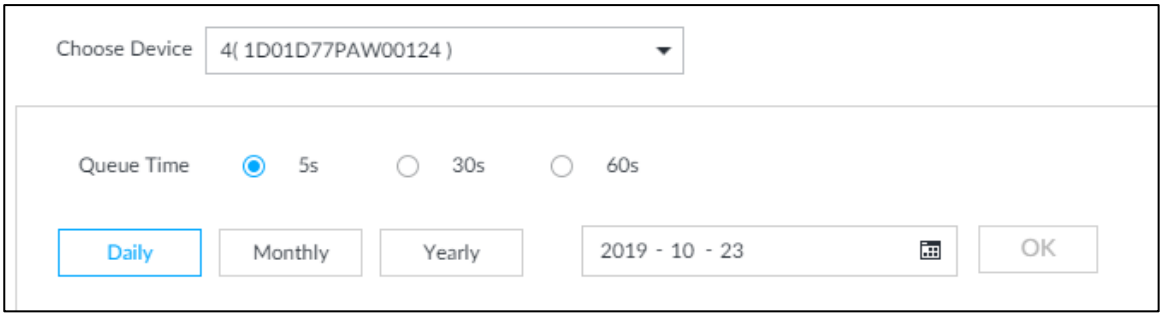
- Click Area1 Area2 Area3 Area4 to select the areas of which you need to view the reports. The ordinate of the report displays different areas in different colors, showing the number of people in different areas or the average strand time.
- For people counting report, click Strand Time 5s 30s 60s to select a strand time. The report shows the people numbers of which the strand time is greater or less than the selected strand time.
- Point to the report, and then the report shows the details at that time point.
- Drag the gray scroll bar under the ordinate to view the statistics for different time periods.
- Click to view the line chart.
- Click to view the bar chart.
- Click to export the report.

7.4.2 Queue People Counting Report

Step 1 Click , and then select **AI REPORT > AI REPORT> Queue People Counting**.

The **Queue People Counting** interface is displayed. See Figure 7-12.

Figure 7-12 Queue people counting



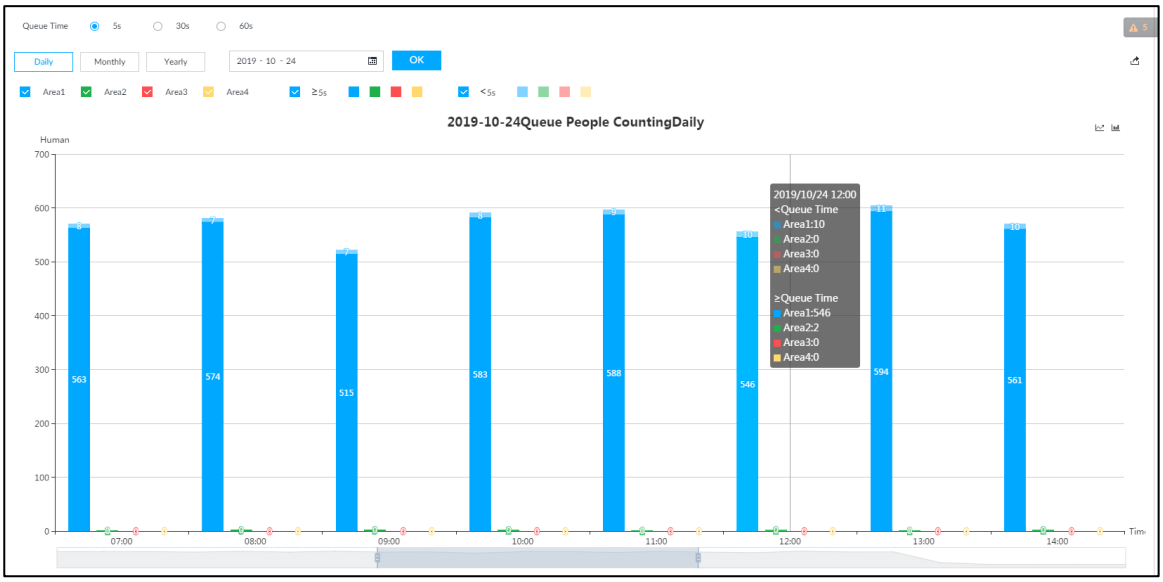
Step 2 Select a device to be searched. You can only select AI fisheye camera.

Step 3 Select a queue time.

Step 4 Select a time period type from **Daily**, **Monthly**, and **Yearly**, and then set the corresponding date, month or year.

Step 5 Click **OK**. The report is displayed. See Figure 7-13.

Figure 7-13 Queuing people counting report



- The ordinate of the report displays different areas in different colors, showing the number of people in different areas or the average dwell time.
- Point to the report, and then the report shows the details at that time point.
- Drag the gray scroll bar under the ordinate to view the statistics for different time periods.
- Click to view the line chart.
- Click to view the bar chart.

8 System Maintenance

On the **MAINTAIN** interface, you can operate and maintain the device working environment to guarantee proper operation.

8.1 Overview

Select **MAINTAIN > Overview**.

Figure 8-1 Overview

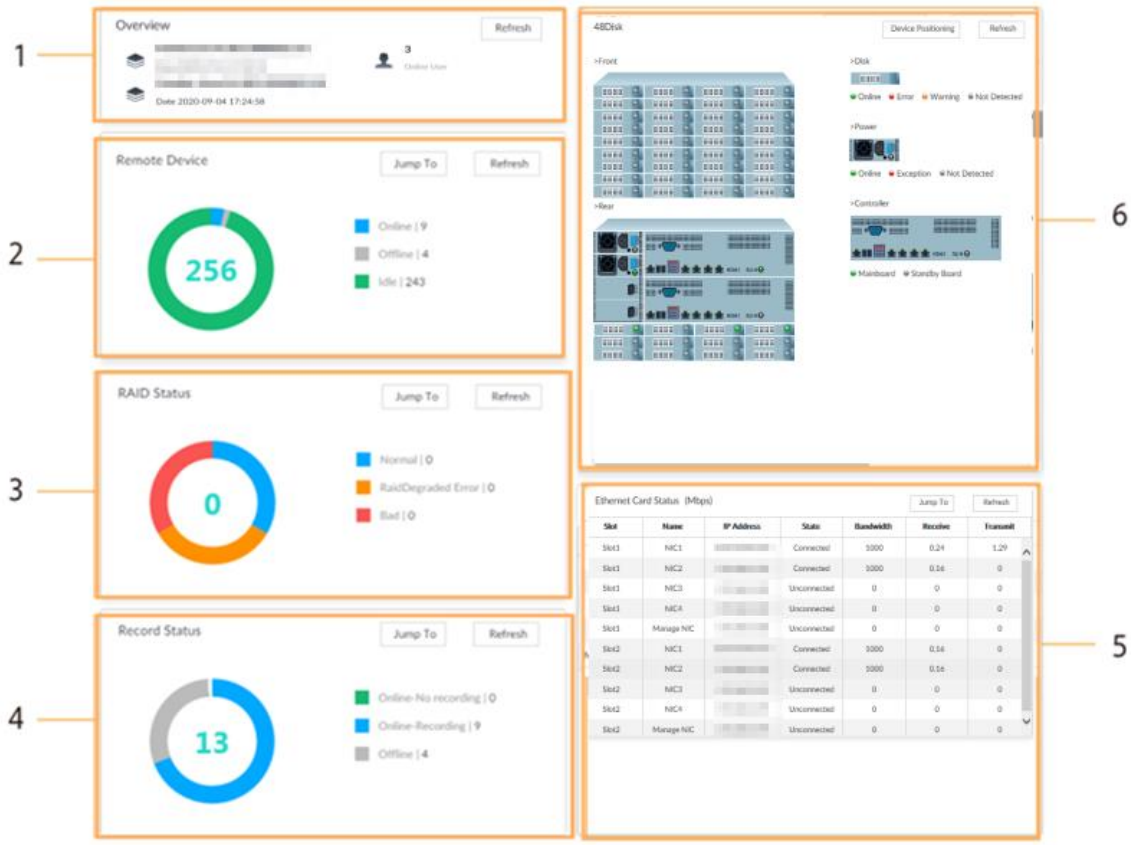


Table 8-1 Overview

No.	Function	Description
1	Overview	View device version details and online users. Click **Refresh** to refresh the data. ● Inactive: If a board is not new, click Activate to clear old data. ● Online User: Due to the login protocol, when the user use one PC to log in to the Device through PCAPP, 2 online users will be occupied. For how to configure the maximum number of online users, see "6.3.1.3 Setting Port Number."
2	Remote Device	View the connection and idle status of remote

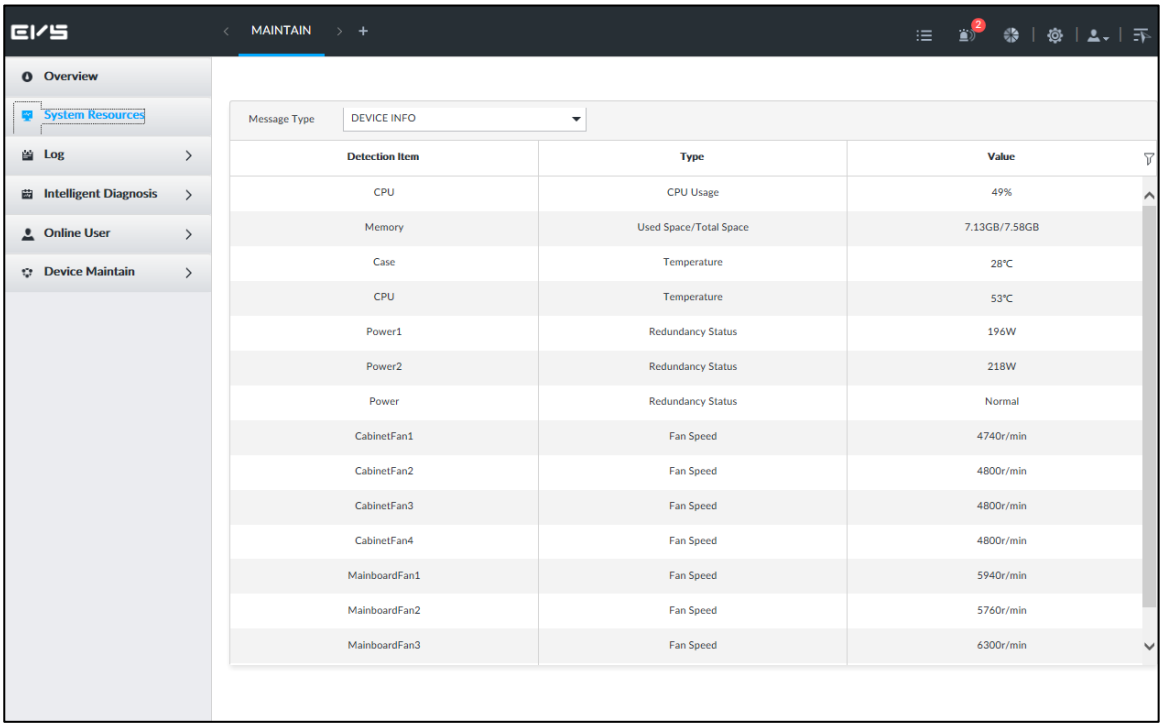
No.	Function	Description
		devices ● Click **Jump To** to go to the **DEVICE** interface for detailed information. ● Click **Refresh** to refresh the data.
3	RAID Status	View RAID status. ● Click **Jump To** to go to the **STORAGE** interface for detailed information. ● Click **Refresh** to refresh the data.
4	Record Status	View recording status of remote devices. ● Click **Jump To** to go to the **VIDEO RECORDING** interface for detailed information. ● Click **Refresh** to refresh the data.
5	Ethernet Card Status (Mbps)	View NIC status. ● Click **Jump To** to go to the **TCP/IP** interface for detailed information. ● Click **Refresh** to refresh the data.
6	Disk	● Display the status of the front panel and rear panel. View status of disk, mainboard, and power. ◇ Disk status indicates that the disk is normal. indicates that the disk is exception. indicates that disk is not connected. ◇ Power status indicates that power is normal. indicates that power is exception. indicates that power is not connected. ◇ Mainboard status indicates that mainboard is normal. indicates that mainboard is exception. indicates that mainboard is not connected. ● Click **Device Positioning**, and then the device positioning indicator flashes. In this way, you can quickly find the device. ● Click **Refresh** to refresh the data.

8.2 System Resources

Select **MAINTAIN > System Resources**.

The **System Resources** interface is displayed. See Figure 8-2. You can view resource status including CPU and memory usage, power status, cabinet temperature and fan speed.

Figure 8-2 System resources



- Click to filter the search conditions.
- Click **Refresh** to refresh the data.

8.3 Logs

The logs record all kinds of system running information. Check the log periodically and fix the problems in time to guarantee system proper operation.

Log Classification

Search system log, user log, event log, and link log. For details, see Table 8-2.

Table 8-2 Log description

Log	Type
System log	Search system log. It includes logs of system running status, file management, hot spare, hardware detect and scheduled task.
User operation log	Search user operation log. It includes user operation and user configuration log.
Event log	Search alarm event log. It includes logs of cross line detection, storage error, storage full, lock in, power fault, video motion, fan speed alarm, face detection, face recognition, human detect, device offline, tampering, no HDD, IPC offline, AI module offline, AI module temp, IO alarm, IP conflict, MAC conflict, and cross region detection.

Log	Type
Link log	Search device link log. You can search or export link log including user login/logout, session hijack, session blast and remote device.

Log Search

The following steps are to search system log. See the actual interface for detailed information.

Step 1 Select **MAINTAIN > Log > System**.

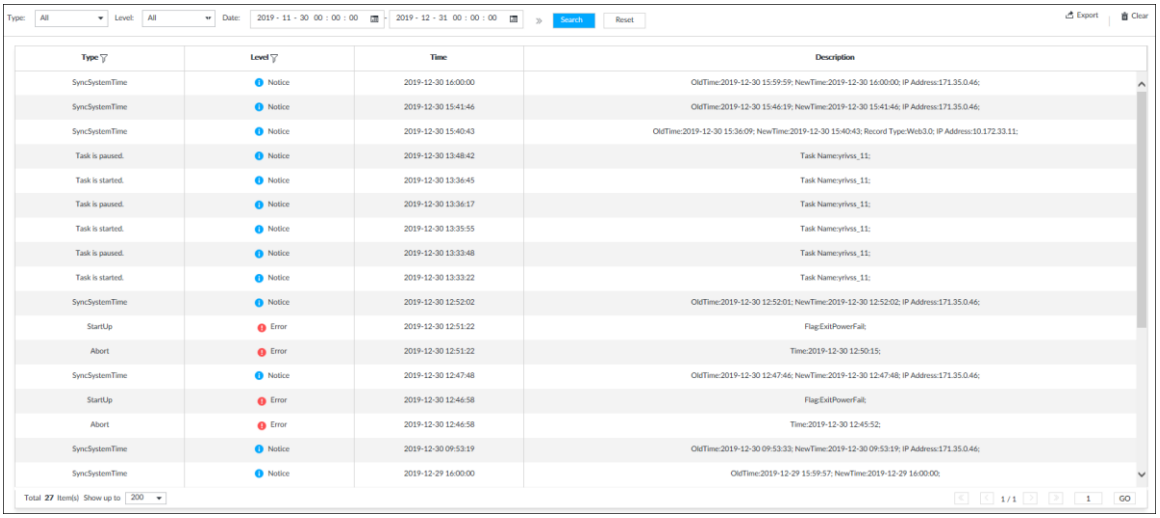
The **system** interface is displayed.

Step 2 Set search criteria such as system log level, type and date.

Step 3 Click **Search**.

The search results are displayed. See Figure 8-3.

Figure 8-3 System log



Operation

Search, export and clear log. For details, see Table 8-3.

Table 8-3 Log operation

Name	Operation
Export log	Click to export log information to local PC or USB storage device.
Clear log	You will be unable to track the system error reason if you clear log. Click **Clear all** to clear all system logs.

8.4 Intelligent Diagnosis

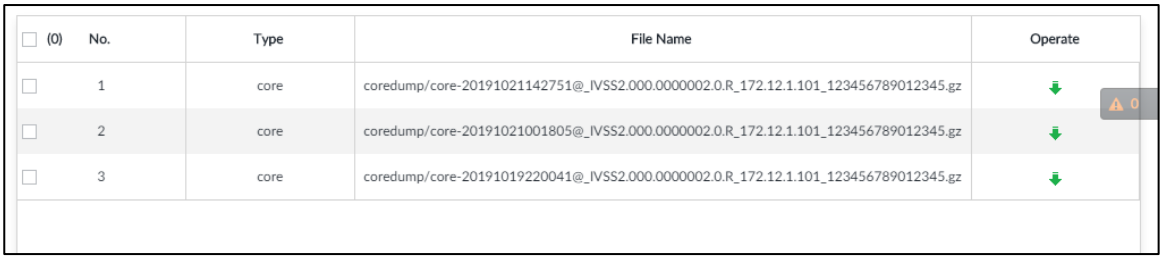
8.4.1 Run Log

View system running logs for troubleshooting.

Make sure that you have enabled **Run Log** in **SECURITY > System Service**. Otherwise there is no log data.

Select **MAINTAIN > Intelligent Diagnosis > Run Log**. The **SYSTEM** interface is displayed. See Figure 8-4.

Figure 8-4 Logs



- Click to export a log.
- After selecting multiple logs, click **Export** to export them in batches.

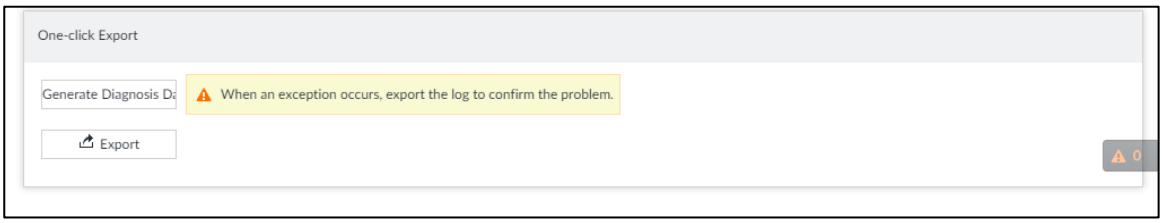
8.4.2 One-click Export

Export the diagnosis data for troubleshooting when the device is exception.

Step 1 Select **MAINTAIN > Intelligent Diagnosis > One-click Export**.

The **One-click Export** interface is displayed. See Figure 8-5.

Figure 8-5 One-click export



Step 2 Click **Generate Diagnosis Data** to generate diagnosis data.

Step 3 Click **Export** to export the diagnosis result.

8.5 Online User

Search remote access network user information or you can block a user from access for a period of time. During the block period, the selected user cannot access the Device.

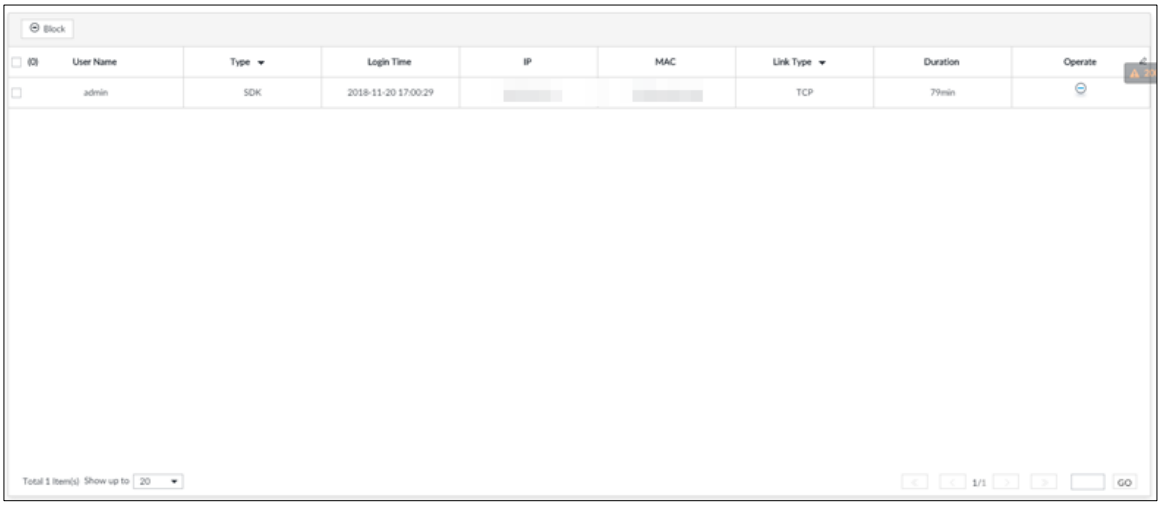
Cannot block yourself or block admin.

Step 1 Select **MAINTAIN > Online User > Online User**.

The **Online User** interface is displayed. See Figure 8-6.

The list displays the connected user information.

Figure 8-6 Online user

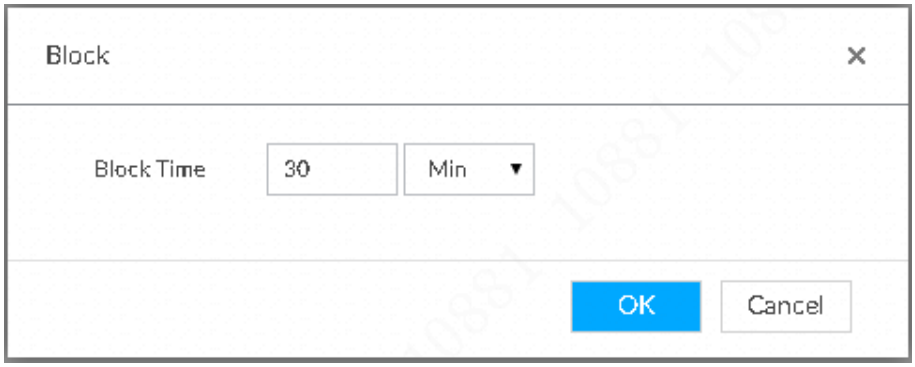


Step 2 Block user.

- Block: Click corresponding to the user.
- Batch block: Select multiple users you want to block and then click **Block**.

The **Block** interface is displayed. See Figure 8-7.

Figure 8-7 Block



Step 3 Set block period. The default period is 30 minutes.

Step 4 Click **OK** to save the configuration.

8.6 Device Maintenance

Device maintenance is to reboot device, restore factory default setup, or upgrade system and so on. Clear the malfunction or error during the system operation and enhance device running performance.

8.6.1 Upgrading Device

Upgrade device or the AI module version.

8.6.1.1 Upgrading the Device

Import the upgrade file to upgrade device version. The upgrade file extension name shall be .bin.

- During upgrading, do not disconnect from power and network, and reboot or shut down the Device.
- Make sure that the upgrade file is correct. Improper upgrade file might result in device error!

Step 1 Select **MAINTAIN > Device Maintain > Upgrade > Host**.

Step 2 Click **Browse** to select an upgrade file.

Step 3 Click **Upgrade Now**.

Step 4 Click **OK**.

The system starts upgrading. Device automatically reboots after successfully upgraded.

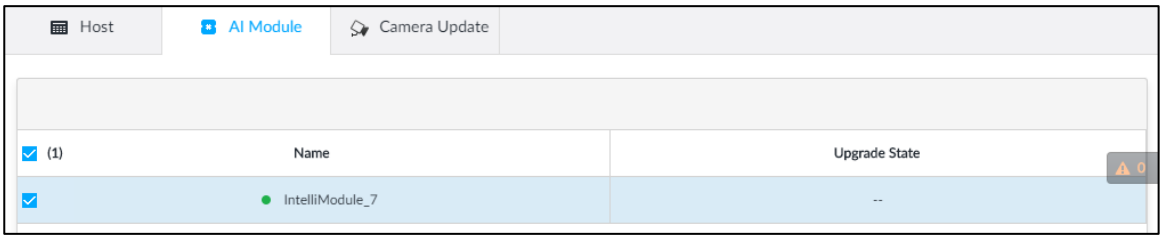
8.6.1.2 Viewing AI module

View the system version of the AI module installed on the device.

Step 1 Select **MAINTAIN > Device Maintain > Upgrade > AI Module**.

The **AI Module** interface is displayed. See Figure 8-8.

Figure 8-8 Upgrade AI module



Step 2 View AI module status.

- indicates that the AI module is online.
- indicates that the AI module is not started.
- Blank row indicates that the AI module is disconnected.

8.6.1.3 Upgrading Cameras

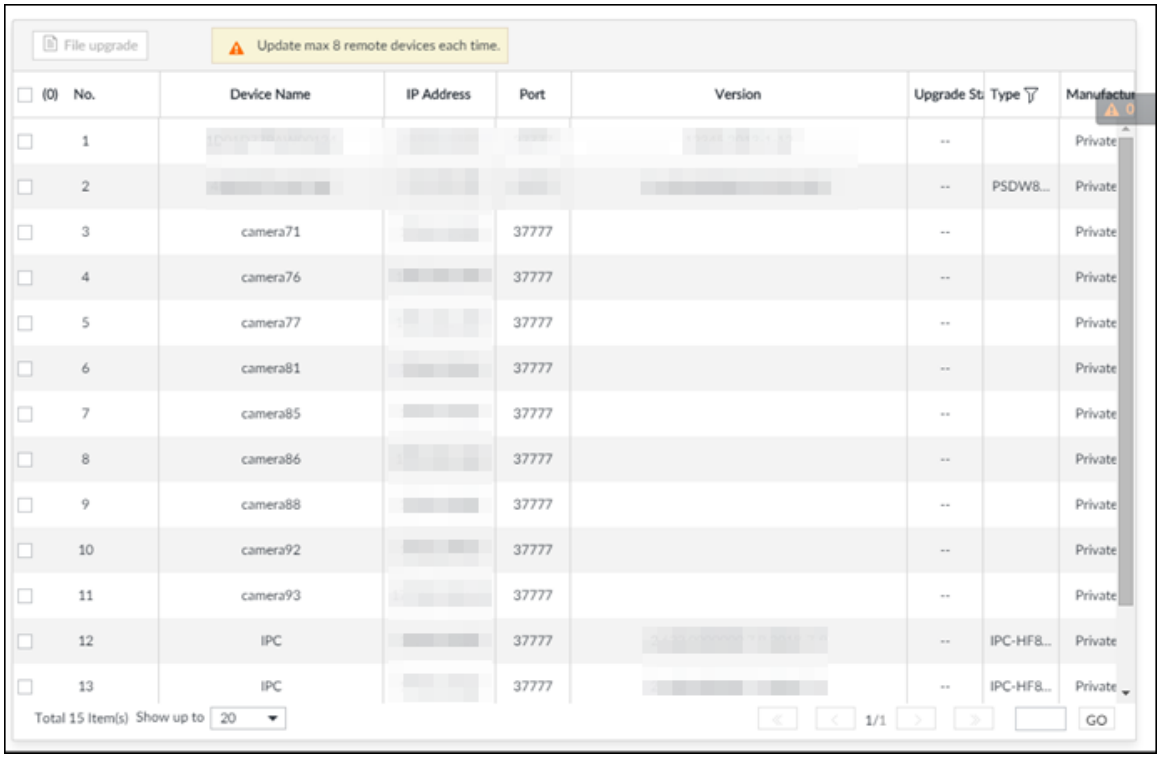
Import the upgrade file to upgrade a camera.

Make sure that you have got the upgrade file and placed it in the correct directory.

Step 1 Select **MAINTAIN > Device Maintain > Upgrade > Camera Upgrade**.

The **Camera Upgrade** interface is displayed. See Figure 8-9.

Figure 8-9 Upgrade camera



Step 2 Select a camera, and then click **File upgrade**.

The **File upgrade** interface is displayed. See Figure 8-10.

Stop recording on the camera first; otherwise the upgrade might fail. If recording is not disabled, you will be prompted as follows. See Figure 8-11.

Figure 8-10 Upgrade

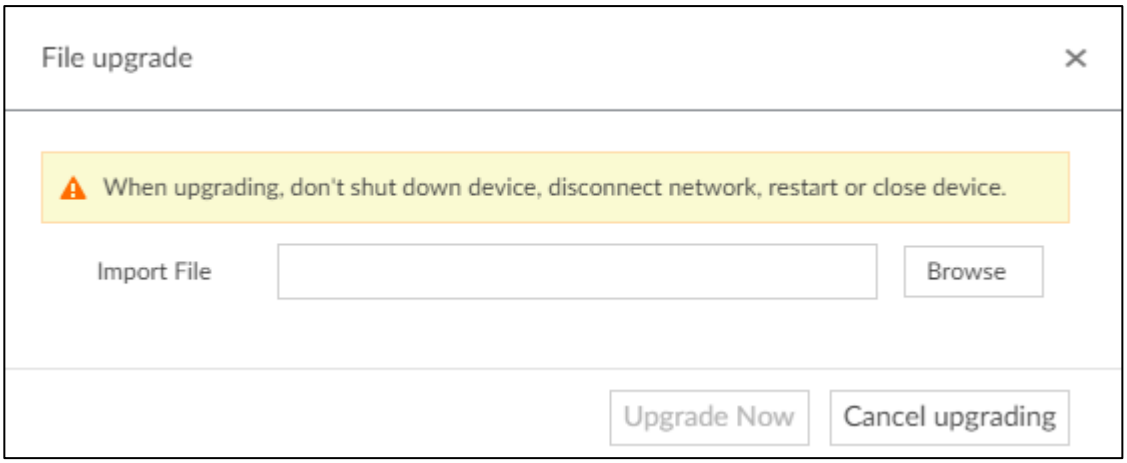
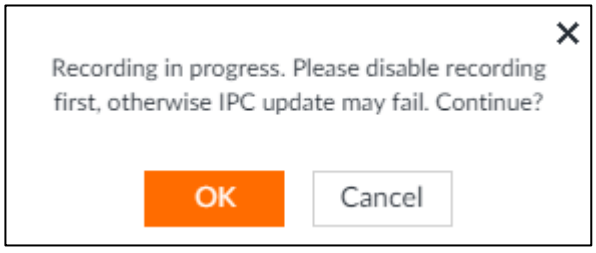


Figure 8-11 Prompt



Step 3 Click **Browse** to select an upgrade file.

Step 4 Click Upgrade Now.

8.6.2 Default

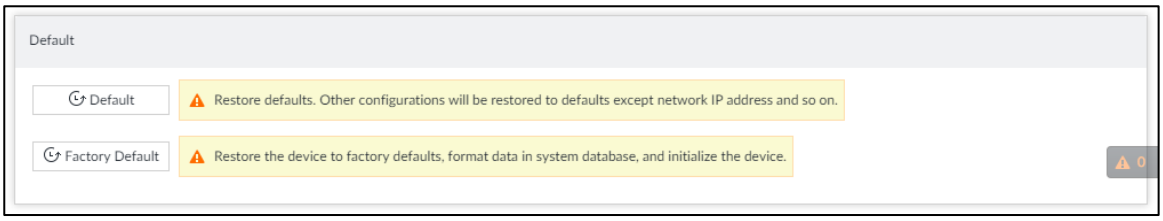
When the system runs slowly and has configuration errors, try to solve the problems by restoring the default settings.

All configurations are lost after factory default operation.

Step 1 Select **MAINTAIN > Device Maintain > Default**.

The **Default** interface is displayed. See Figure 8-12.

Figure 8-12 Default

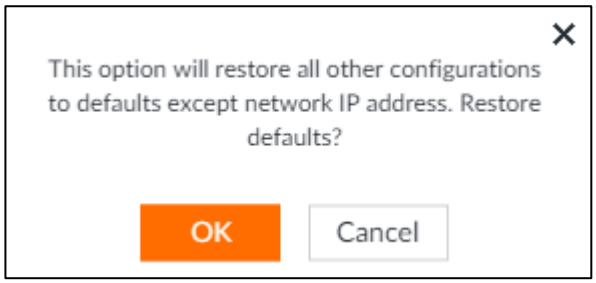


Step 2 Select a method.

- Click **Default**.

  The following prompt is displayed. See Figure 8-13.

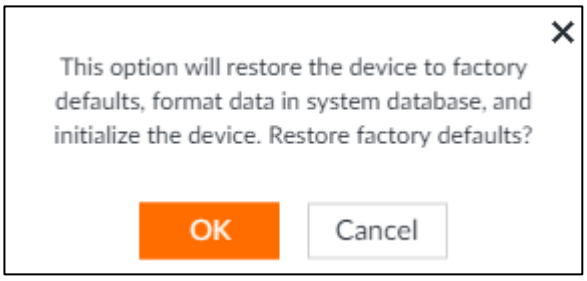
  Figure 8-13 Prompt (1)



- Click **Factory Default**.

  The following prompt is displayed. See Figure 8-14.

  Figure 8-14 Prompt (2)



Step 3 Click **OK**.

System begins to restore default settings. After successfully restored default settings, system prompts to restart the device.

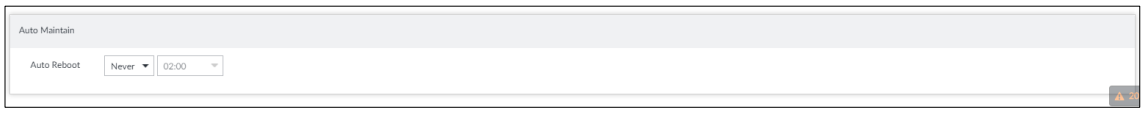
8.6.3 Automatic Maintenance

If the device has run for a long time, you can set to automatically reboot the device at idle time.

Step 1 Select **MAINTAIN > Device Maintain > Auto Maintain**.

The **Auto Maintain** interface is displayed. See Figure 8-15.

Figure 8-15 Auto Maintain



Step 2 Set auto reboot time.

Step 3 Click **Save**.

8.6.4 IMP/EXP

Export device configuration file to local PC or USB storage device, to backup it. When the configuration is lost due to abnormal operation, import the backup configuration file to restore system configurations quickly.

Select **MAINTAIN > Device Maintain > IMP/EXP**. The **IMP/EXP** interface is displayed. See Figure 8-16.

Figure 8-16 IMP/EXP

Export Configuration File

Click **Export** to export configuration file to local PC or USB storage device. File path might vary depending on interface operations, and the actual interface shall prevail.

- On PCAPP, click , and then select **Download content** to view file saving path. For details, see "9.3 Viewing Downloads."
- During web operations, files are saved under default downloading path of the browser.

Import Configuration File

Step 1 Click **Browse** to select the configuration file.

Step 2 Click **Import**.

After the configuration file is imported successfully, the device will reboot automatically.

9 PCAPP Introduction

After installing PCAPP, system supports to access the Device remotely to carry out system configuration, function operations and system maintenance.

For details about installing PCAPP, see "3.3.1 Logging in to PCAPP Client."

9.1 Interface Description

Double-click on the PC desktop. System displays PCAPP at full screen by default. Click to display the task column. See Figure 9-1. See Table 9-1 for detailed information.

Figure 9-1 EVS task column

Table 9-1 Icons

Icons	Description
PCAPP | Please Enter URL	Address bar: Enter the IP address of remote device.
	Enter device IP address and then click the button to go to the login interface. Now the icon turns into . Click to refresh the interface.
	Click to view history login record, view downloads, set compatibility mode and view EVS version information.
	Click to minimize PCAPP.
	Click to maximize PCAPP.
	Click to display PCAPP at full screen.
	Click to close PCAPP.

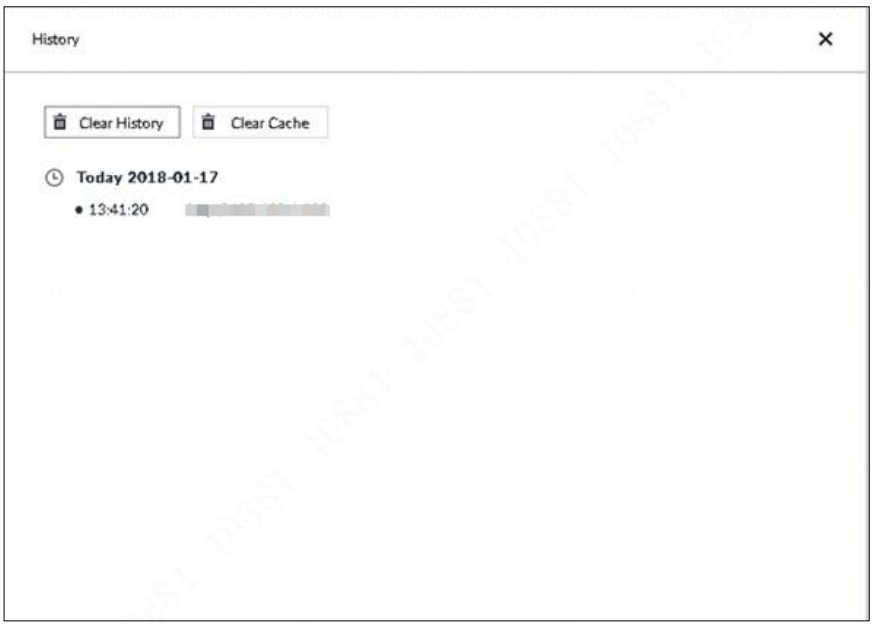
9.2 History Record

Click , and then select **History**.

The **History** interface is displayed. See Figure 9-2. You can view history access record and clear buffer.

- Click **Clear History** to clear all history records.
- Click **Clear Buffer** to clear buffer data, and reboot PCAPP.

Figure 9-2 History record

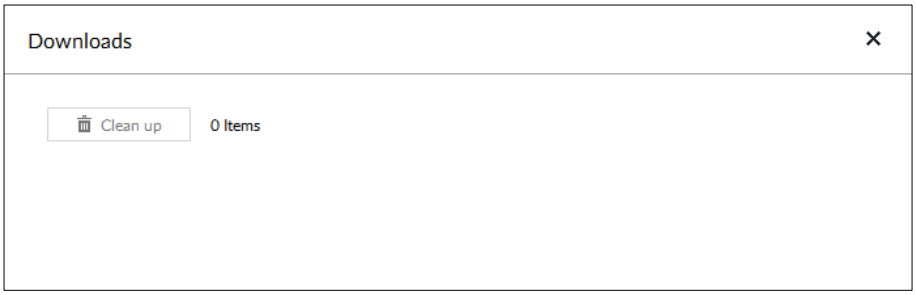


9.3 Viewing Downloads

To view and clear history downloads, click , and then select **Downloads**. The **Downloads** interface is displayed. See Figure 9-3.

- Double-click file name to open it.
- Click **Displayed in Folder** to open the folder where the file is located.
- Click **Clear Downloads** to clear history download records.

Figure 9-3 Downloads



9.4 Configuring PCAPP

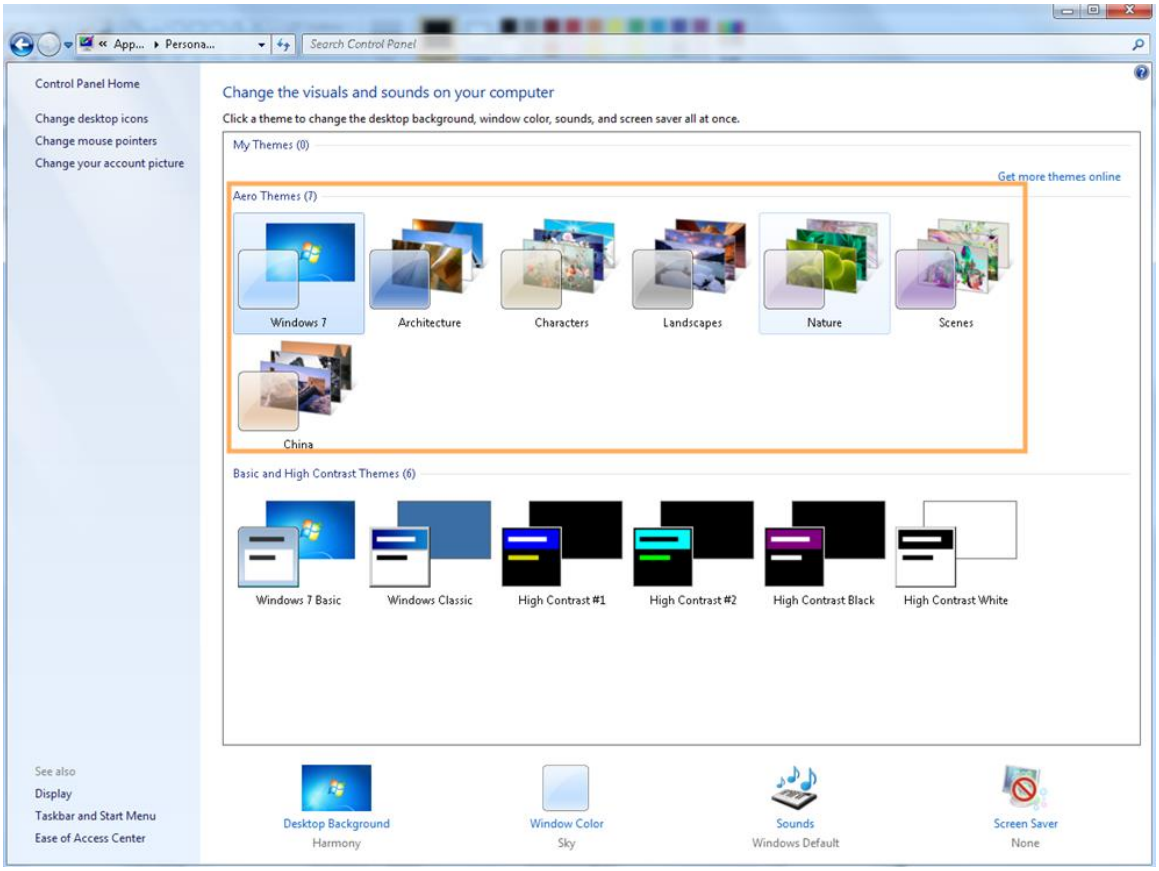
When PC theme is not Areo, video of PCAPP might not be displayed normally. It is suggested that PC theme should be switched to Areo, or compatibility mode of PCAPP should be enabled.

Switching PC Theme

This section takes Windows 7 as an example.

Right-click any blank position on PC desktop, select **Personalize**, and then switch to Aero theme. See Figure 9-4. Restart the PCAPP before the Aero theme takes effect.

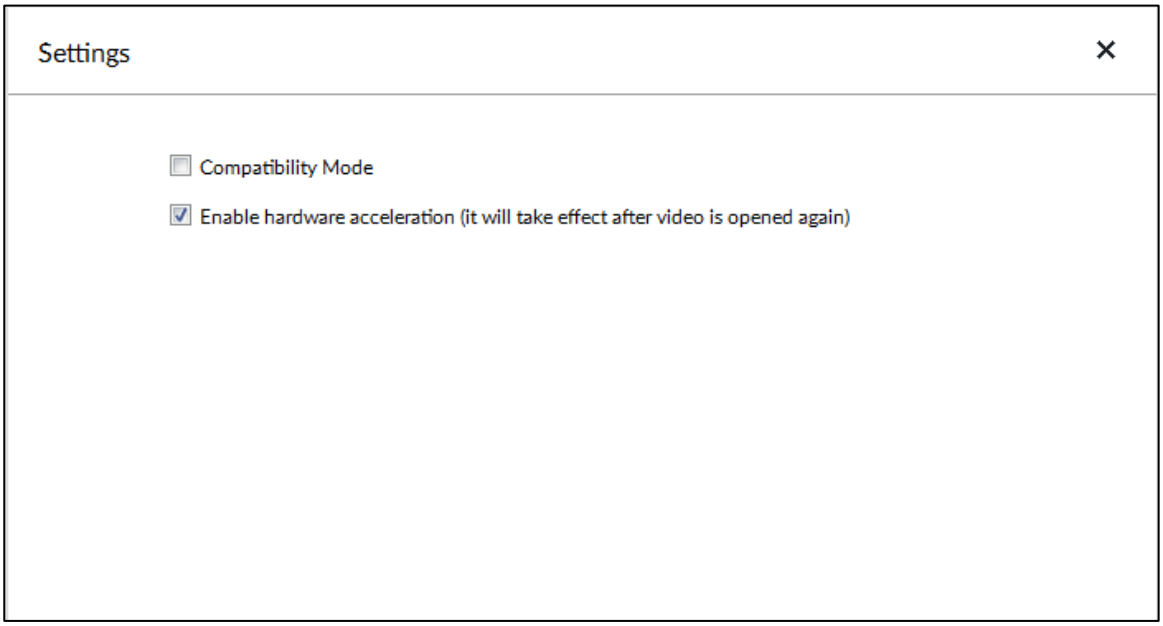
Figure 9-4 PC theme



Enable Compatibility Mode

Click ☰, and select **Settings**. The **Settings** interface is displayed. See Figure 9-5. Select **compatibility mode**. Restart PCAPP before the compatibility mode takes effect.

Figure 9-5 Setting



Enable Hardware Acceleration

Click , and select **Settings**. The **Settings** interface is displayed. See Figure 9-5. Select **Enable hardware acceleration (it will take effect after video is opened again)**.

The live view becomes much more fluent when this function is enabled.

9.5 Viewing Version Details

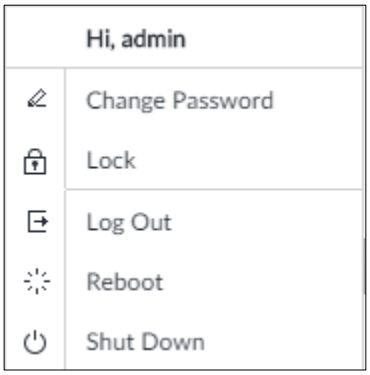
Click and then select **About**. The **About** interface is displayed. See Figure 9-6. View PCAPP version information.

Figure 9-6 About

10 Log Out, Reboot, Shut Down, Lock

Log out, reboot, shut down and lock out the Device. See Figure 10-1.

Figure 10-1 User operation



Log Out

Click , and then select **Log Out**.

Reboot

Click , and then select **Reboot**. System pops up confirm dialogue box. Click **OK** to reboot.

Shut Down

To unplug the power cable might result in data (record and image) loss.

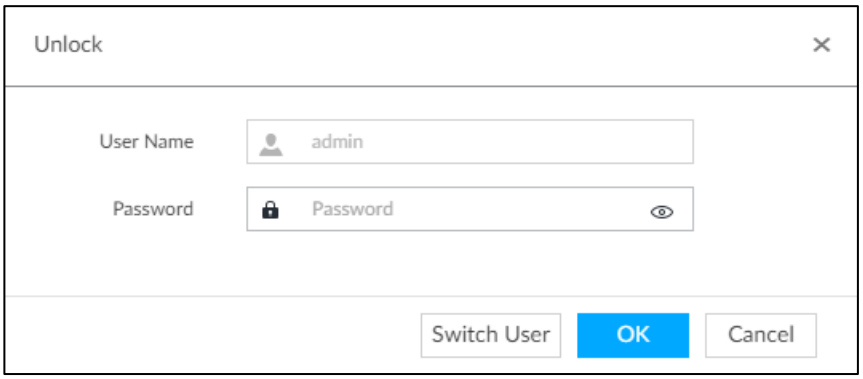
- Mode 1 (recommended): Click , and then select **Shutdown**. System pops up confirm dialogue box and then click **OK** to shut down.
- Mode 2: Use power on-off button on the device.
  - ◇ 8-HDD series product: Press power on-off button on rear panel.
  - ◇ Other series products: Press the power on-off button on the device for at least 4 seconds.
- Mode 3: Unplug the power cable.

Lock

Click , and then select **Lock** to lock the client. The locked client cannot be operated.

To unlock the client, click anywhere on the client, and then the **Unlock** dialogue box is displayed. See Figure 10-2. Enter the username and password, and then click **OK**. You can also click **Switch User** to switch to another user account.

Figure 10-2 Unlock the client



Appendix 1 **RAID**

RAID is an abbreviation of Redundant Array of Independent Disks. It combines several independent HDDs (physical HDD) to form a HDD group (logic HDD) to provide more storage capacity and data redundancy.

RAID Level

RAID level refers to the way that the disk array is organized. Different RAID levels have different data protection, availability and performance.

RAID Level	**Description**	**Min. HDD Needed**
RAID 0	RAID 0 is called striping. RAID 0 is to save the continued data fragmentation on several HDDs. It can process the read and write at the same time, so its read/write speed is N (N refers to the HDD amount of the RAID 0) times as many as one HDD. RAID 0 does not have data redundant, so one HDD damage might result in data loss that cannot be restored.	2
RAID 1	It is also called mirror or mirroring. RAID 1 data is written to two HDDs equally, which guarantee the system reliability and can be repaired. RAID 1 read speed is almost close to the total volume of all HDDs. The write speed is limited by the slowest HDD. At the same time, the RAID 1 has the lowest HDD usage rate. It is only 50%.	2
RAID5	RAID5 is to save the data and the corresponding odd/even verification information to each HDD of the RAID5 group and save the verification information and corresponding data to different HDDs. When one HDD of the RAID5 is damaged, system can use the rest data and corresponding verification information to restore the damaged data. It does not affect data integrity.	3
RAID6	Based on the RAID5, RAID6 adds one odd/even verification HDD. The two independent odd/even systems adopt different algorithm, the data reliability is very high. Even two HDDs are br**OK**en at the same time, there is no data loss risk. Comparing to RAID5, the RAID6 needs to allocate larger HDD space for odd/even verification information, so its read/write is even worse.	4
RAID 10	RAID 10 is a combination of the RAID 1 and RAID 0. It uses the extra high speed efficient of the RAID 0 and high data protection and restores capability of the RAID 1. It has high read/write performance and security. However, the RAID 10 HDD usage efficiency is as low as RAID 1.	4

RAID Capacity

See the sheet for RAID space information.

Capacity N refers to the mini HDD amount to create the corresponding RAID.

RAID Level	Total Space of the N HDD
RAID0	The total amount of current RAID group
RAID1	Min (capacityN)
RAID5	(N-1) ×min (capacityN)
RAID6	(N-2) ×min (capacityN)
RAID10	(N/2)×min (capacityN)
RAID50	(N-2) ×min (capacityN)
RAID60	(N-4) ×min (capacityN)

Appendix 2 **Glossary**

FTP	File Transfer Protocol (FTP) is a protocol of the TCP/IP protocol group. It transfers file from one PC to another, without consideration of the location, connection type, and operation system of the PC.
IP SAN	Internet Protocol Storage Area Network (IP SAN) is an IP-based network storage technology.
iSCSI	Internet Small Computer System Interface (iSCSI) is an internet protocol standard in Ethernet, and an SCSI instruction set for hardware to be used in IP protocol layer. Briefly, iSCSI can realize SCSI protocol in the IP network, so router option is available in high-speed 1000M Ethernet.
LAN	Local Area Network (LAN) is a computer network that interconnects computers within a limited area (such as an office building or a school).
NFS	Network File System (NFS) is a distributed file system protocol. It allows a client computer to access files or peripheral devices of another PC. It is mainly used in UNIX-like platforms.
MTU	Maximum Transmission Unit (MTU) is the size of the largest protocol data unit that can be communicated in a single network layer transaction.
SAMBA	It is a free software that can realize Server Messages Block (SMB) on Linux and Unix systems. It consists of server and client.
SATA	Serial Advanced Technology Attachment (SATA) is a serial HDD interface that can realize serial data transmission. The current released Serial ATA 2.0 enjoys maximum theoretical transfer speed of 300MB/s.
SATA HDD	HDD that adopts SATA standard. Some leading manufacturers such as Seagate, Western Digital, and Hitachi are offering SATA HDDs.
SMART	Self-Monitoring Analysis and Reporting Technology (SMART) is an automatic monitoring and alarming system of HDD status. It monitors and records the HDD through monitoring instructions in the HDD, and compares the monitoring results with the pre-defined security value of the manufacturer. If the monitoring situation is about to exceed or already exceeded the pre-defined value, an alarm will be triggered, and small-scale repair will be initiated. This helps ensure the security of HDD data.
TCP	Transmission Control Protocol (TCP) is a transmission-layer communication protocol that provides reliable and ordered delivery of a stream of bytes.
UDP	User Datagram Protocol (UDP) is a connectionless communication protocol used for processing data packets.
WAN	Wide Area Network (WAN) is a computer network that extends over a large geographical distance. It connects physically disparate LANs and computer systems for the purpose of resource sharing.
Storage Pool	It is a virtual logic device. It can consist of several HDDs and RAID groups. It is a main way to realize virtual storage.

Synchronization	After creating RAID1 or RAID5, and before using it, the system needs to read and write the HDD at a fixed speed and adopts an algorithm to calculate. This process is called synchronization. During synchronization, the system performance speed is very low.
Shared Directory	Local PC access the top path of the shared storage space. You can create, remove, authenticate and set valid user at the storage device. User is only allowed to operate folder and file performance in the under-layer. According to different share protocols, it can be divided into SAMBA share folder, NFS share folder and FTP share folder.
Working Status	It is for RAID6/RAID5/RAID1. It is the RAID status after it completes synchronization operation. When the RAID group is in working status, on the **Storage > RAID** interface, the RAID device status is "clean."
Degraded Status	It is a status after you remove one disk from RAID1/RAID5 (working status) or remove two disks from RAID6. The status shows "degraded."
Manageable Status	It is a device status when controller configure device by web. Actually, when there is no error or damage, the device shall always be in manageable status.
Ready Status	It is a device status when controller access HDD by network. The system is ready to use after you configure correctly in accordance with the Manual. Some non-device error (such as configuration error, hot swap error) might result in device failure. You can configure again to boot up the Device. But data loss might occur during this process.

Appendix 3 **Cybersecurity Recommendations**

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

Mandatory actions to be taken for basic equipment network security:

1. **Use Strong Passwords**

   Please See the following suggestions to set passwords:

   - The length should not be less than 8 characters;
   - Include at least two types of characters; character types include upper and lower case letters, numbers and symbols;
   - Do not contain the account name or the account name in reverse order;
   - Do not use continuous characters, such as 123, abc, etc.;
   - Do not use overlapped characters, such as 111, aaa, etc.;

2. **Update Firmware and Client Software in Time**

   - According to the standard procedure in Tech-industry, we recommend to keep your equipment (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your equipment network security:

1. **Physical Protection**

   We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable equipment (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Set and Update Passwords Reset Information Timely**

   The equipment supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. **Enable Account Lock**

   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. **Change Default HTTP and Other Service Ports**

We suggest you to change default HTTP and other service ports into any set of numbers between 1024–65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **Enable Allowlist**

   We suggest you to enable allowlist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the allowlist.

8. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.

9. **Assign Accounts and Privileges Reasonably**

   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

10. **Disable Unnecessary Services and Choose Secure Modes**

    If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

    If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

    - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
    - SMTP: Choose TLS to access mailbox server.
    - FTP: Choose SFTP, and set up strong passwords.
    - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

11. **Audio and Video Encrypted Transmission**

    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

    Reminder: encrypted transmission will cause some loss in transmission efficiency.

12. **Secure Auditing**

    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

13. **Network Log**

    Due to the limited storage capacity of the equipment, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

14. **Construct a Safe Network Environment**

    In order to better ensure the safety of equipment and reduce potential cyber risks, we recommend:

    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.

- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
- It is recommended that you enable your device's firewall or blocklist and allowlist feature to reduce the risk that your device might be attacked.