Intelligent Video Analysis Server for Traffic Event Detection (TB9000)

User Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.2.0

Foreword

General

This manual introduces the installation, configuration and operations of the intelligent video analysis server for traffic event detection (hereinafter referred to as "the Device"). Read carefully before using the device, and keep the manual safe for future reference.

Models

IVS-TB9000-2EA-RM1

IVS-TB9000-*x*EA-GU2

IVS-TB9000-*x*EA-DC2

IVS-TB9000-*x*EA-TS2

The *x* in models represents the numbers 2 to 6, and the specific number varies depending on the Model. Please refer to the actual situation for the specific number.

Safety Instructions

The following signal words might appear in the manual.

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

Icons

Icon	Description
	Delete icon. Click it to delete configuration item.
	Edit icon. Click it to modify configuration item.
/	Switch icon. Click it to enable/disable function.

Icon	Description
⚙	Set icon. Configure the related parameters.
*	Required Parameter.

Revision History

Version	Revision Content	Release Time
V1.2.0	• Updated smart configuration settings, batch events and traffic event detection. • Added new model configurations, secondary analysis, operator maintenance and intelligent module.	April 2025
V1.1.1	Updated the panel.	November 2024
V1.1.0	Updated the models.	October 2024
V1.0.0	First release.	June 2024

Privacy Protection Notice

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

About the Manual

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

- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

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

Transportation Requirements

Transport the server under allowed humidity and temperature conditions.

Storage Requirements

Store the server under allowed humidity and temperature conditions.

Installation Requirements

-  Electrical Hazard

  Preventive measures: Make sure the power is off when you put your hand into the device.
- Stability Hazard

  Possible result: The rack might fall down and cause serious personal injury.

  Preventive measures (including but not limited to):

  - Before extending the rack to the installation position, read the installation instructions.
  - When the device is installed on the slide rail, do not place any load on it.
  - Do not retract the slide rail while the device is installed on it.

- Do not connect the power adapter to the device while the adapter is powered on.
- Strictly comply with the local electrical safety code and standards. Make sure that the ambient voltage is stable and meets the power supply requirements of the device.
- Use the standard power adapter or cabinet power supple. We will assume no responsibility for any injuries or damages caused by the use of a nonstandard power adapter.
-  Rotating Fan Blades Hazard

  Avoid touching the fan blades, especially when they are moving.
-  Before installation, disconnect all the power cords.

- Do not place the device in a place exposed to sunlight or near heat sources.

- Keep the device away from dampness, dust, and soot.
- Put the device in a well-ventilated place, and do not block its ventilation.
- Install the switch horizontally on a stable surface to prevent it from falling.
- The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.
- Use power cords that conform to your local requirements and rated specifications.
- Before connecting the power supply, make sure the input voltage matches the server power requirement.
- When installing the device, make sure that the power plug and appliance coupler can be easily reached to cut off power.
- Extra protection is necessary for the device casing to reduce the transient voltage to the defined range.
- The device must be installed in a location that only professionals can access. Non-professionals are not allowed to enter the installation area.
- It is prohibited for non-professionals and unauthorized personnel to open the device casing.
- Install the device near a power socket for emergency disconnect.

Operation Requirements

DANGER

- The device or remote control contains button batteries. Do not swallow the batteries due to the risk of chemical burns.

  Possible result: The swallowed button battery can cause serious internal burns and death within 2 hours.

  Preventive measures (including but not limited to):

  - Keep new and used batteries out of reach of children.
  - If the battery compartment is not securely closed, stop using the product immediately and keep out of reach of children.
  - Seek immediate medical attention if a battery is believed to be swallowed or inserted inside any part of the body.
- Battery Pack Precautions

  Preventive measures (including but not limited to):

  - Do not transport, store or use the batteries in high altitudes with low pressure and environments with extremely high and low temperatures.
  - Do not dispose the batteries in fire or a hot oven, or mechanically crush or cut the batteries to avoid an explosion.
  - Do not leave the batteries in environments with extremely high temperatures to avoid explosions and leakage of flammable liquid or gas.
  - Do not subject the batteries to extremely low air pressure to avoid explosions and the leakage of flammable liquid or gas.

WARNING

- In a domestic environment this may cause radio interference in which case you may be required to take adequate measures.
- The device is heavy and needs to be carried by several persons together to avoid personal injuries.
- Place the device in a location that children cannot easily access.

- Make sure that the power supply is correct before use.
- Operate the device within the rated range of power input and output.
- Use the device under allowed humidity and temperature conditions.
- Do not drip or splash liquid onto the device, make sure that there is no object filled with liquid on the device to prevent liquid from flowing into it.
- Do not disassemble the device without professional instruction.
- Your configurations will be lost after performing a factory reset. Please be advised.
- Do not restart, shut down or disconnect the power to the device during an update.
- Make sure the update file is correct because an incorrect file can result in a device error occurring.
- The system cannot upgrade different types of AI modules at the same time.
- Do not frequently turn on/off the device. Otherwise, the product life might be shortened.
- Back up important data on a regular basis when using the device.
- Operating temperature: 10 °C to 35 °C (50 °F to 95 °F).

Maintenance Requirements

- Replacing unwanted batteries with the wrong type of new batteries might result in explosion.

  Preventive measures (including but not limited to):

  - Replace unwanted batteries with new batteries of the same type and model to avoid the risk of fire and explosion.
  - Dispose of the old batteries as instructed.
- Power off the device before maintenance to make sure that the device is disconnected from the power supply.

- Make sure you use the same model when replacing the battery to avoid fire or explosion. Dispose the battery strictly following the instructions.
- Power off the device before maintenance.

- AI module does not support hot plug. If you need to install or replace the AI module, unplug the device power cord first. Otherwise, it will lead to file damage on the AI module.
- The device casing provides protection for internal components. Use a screwdriver to loosen the screws before detaching the casing. Make sure to put the casing back on and secure it in its original place before powering on and using the device.
- Clean the ventilation pipe regularly to avoid obstructions.
- It is prohibited for non-professionals and unauthorized personnel to open the device casing.
- The appliance coupler is a disconnection device. Keep it at a convenient angle when using it. Before repairing or performing maintenance on the device, first disconnect the appliance coupler.

Table of Contents

1 Product Introduction

Based on intelligent platform, video analysis server integrates server resources and intelligent analysis algorithms to analyze streams of network devices. It is widely used in traffic management and road operation and maintenance scenarios such as expressways, overpasses, tunnels, and cross-sea bridges.

1.1 Functions

Table 1-1 Function description

Function	Description
Parking Detection	Detects an event when a vehicle moves and then stops, and the stop time exceeds the defined value.
Pedestrian Detection	Detects an event when a pedestrian walks onto the vehicle lane or into a pedestrian-prohibited area and the duration exceeds the defined value.
Non-motor Vehicle Detection	Detects two-wheelers and tricycles.
Traffic jam detection	Detects an event when a lane is congested and the duration exceeds the defined value.
Traffic Flow Statistics	Statistics on the number of vehicles passing through a road section within a specified time.
Road Debris Detection	Detects an event when an object littered by a person in a vehicle or a pedestrian disturbs traffic and the duration exceeds the defined value.
Driving in Emergency Lane	Detects an event when a vehicle enters the emergency lane.
Lane Change	Detects an event when a vehicle crosses the lane line (yellow or white solid line) and the duration exceeds the defined value.
Wrong-way Driving Detection	Detects an event when a vehicle is moving opposite to the specified direction and the duration exceeds the defined value.
Illegal Backing Detection	Detects an event when a vehicle is backing, for instance when missing the correct expressway intersection, and the duration exceeds the defined value.
Construction Detection	Detects construction signs in the area for longer than the defined value.
Roadblock Detection	Detects barriers, such as boxes, that are in the area for longer than the defined value.
Traffic Accident Detection	Detects an event when vehicles clash and the duration exceeds the defined value.
Dense Fog Detection	Detects an event when radiation fog exists in the area and the duration exceeds the defined value.
Smoke Detection	Detects an event when smog exists in the area and the duration exceeds the defined value.

Function	Description
Heat Detection	Detects an event when fire exists in the area and the duration exceeds the defined value.
Crossing Solid Line Detection	Detects an event when a vehicle crosses the lane line (yellow or white solid line) and the duration exceeds the defined value. Do not consider lane changing scenarios.
Speeding Detection	Detects an event when the driving speed of a vehicle and the duration exceed the defined value.
Driving Too Slow Detection	Detects an event when the driving speed of a vehicle is lower than the defined value and the duration exceeds the defined value.
Intrusion	Detects an event when an object exists in an area and the duration exceeds the defined value.
Truck Entered Prohibited Area	Detects an event when a truck enters the detection zone.
Hazardous Material Transport Vehicle Detection	Detects whether a vehicle with hazardous material crosses the detection line.

1.2 Structure

1.2.1 RM1 Front Panel

Figure 1-1 Front panel

Table 1-2 Panel description

No.	Name	Description
1	UID switch and indicator	After pressing the UID button, the UID indicator next to the button and the UID indicator on the back panel are flashing blue.
2	USB3.0 port	Connects to external devices, such as a mouse and a keyboard.
3	BMC management network port indicator	• Solid green: Network connected. • Green light off: Network disconnected.

No.	Name	Description
4	Network status indicator	From left to right, Ethernet port 1 corresponds to Ethernet port 4. ● Solid green: Network connected. ● Green light off: Network disconnected.
5	System status indicator	Indicates the running status of the server. ● Solid green: System runs normally. ● Solid red: System runs in redundancy or with decreased performance. It is a warning of system failure, such as on the redundant power supply or the cooling fan. ● Light off: System is not running.
6	Power switch and indicator	Press the power switch to turn the server on or off. ● Solid blue: The server is turned on. ● Light off: The server is not turned on.

1.2.2 RM1 Rear Panel

Figure 1-2 Rear panel

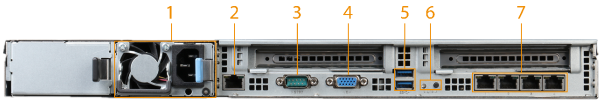


Table 1-3 Panel description

No.	Name	Description
1	Power port	Input 100-240 VAC power supply.
2	BMC management network port	100Mbps management network port, only for access to BMC. It cannot be used as a data network port.
3	RS-232 port	RS-232 transparent debugging serial port, used for ordinary serial port debugging and transmission of transparent serial port
4	VGA port	VGA video output interface, output analog video signal, can be connected to the display to watch the server local interface.
5	USB3.0 port	Connects to external devices, such as a mouse and a keyboard.

No.	Name	Description
6	UID switch and indicator	After pressing the UID button, the UID indicator next to the button and the UID indicator on the back panel are flashing blue. The UID function can remotely control the light on or off.
7	Ethernet port	4 1000 Mbps/100 Mbps Ethernet port. Connects to the network. Each Ethernet port has two indicators, ACTIVE indicator (left) and LINK indicator (right). ● ACTIVE indicator ◇ Orange light flashes: The data is being transmitted. ◇ Light off: No data transmission. ● LINK indicator ◇ Solid green: Network connected. ◇ Light off: Network disconnected.

1.2.3 GU2 Front Panel

Figure 1-3 Front panel

Table 1-4 Panel description

No.	Name	Description
1	Power switch	Press the button for more than 4 seconds to shut down the server in the power-on state.
	UID switch	The UID button can be used as an indicator to conveniently locate the server. Press the button to control whether the indicator is on or off. ● Solid blue: The server is being located. ● Light off: The server is not located. Through the virtual front panel function of BMC, you can remotely control whether the indicator is on or off.
	Reset button	Press the button and restart the server.

No.	Name	Description
2	Power indicator 	Indicates the power supply status. ● Solid blue: The server has been powered on normally. ● Light off: The server is not powered on.
	System status indicator 	Indicates the running status of the server. ● Green light flashes: System runs normally. ● Red light flashes: System runs in redundancy or with decreased performance. It is a warning of system failure, such as on the redundant power supply or the cooling fan. ● Light off: System is not running.
	Network status indicator1/2 	● Green light flashes: Network connected. ● Light off: Network disconnected.
3	HDD status indicator	Indicates the running status of the HDD. ● Solid blue: HDD is active. ● Light off: HDD is inactive.
	HDD read and write indicator	Indicates the read and write status of the HDD. ● When the RAID card is not installed. ◇ Green light flashes: The HDD is in read and write state. ◇ Light off: The HDD is not in place or malfunctioning. ● When installing the RAID card. ◇ Green light flashes: The HDD is in read and write state. ◇ Light off: The HDD is not in place or malfunctioning.
	HDD failure and location indicator	Indicates the failure of the HDD or locates the HDD. ● When the RAID card is not installed, the indicator is invalid. ● When installing the RAID card. ◇ Solid red: The system detects failures of the HDD. ◇ Red light flash quickly (frequency is 4 times per second): The HDD is being located. ◇ Red light flash slowly (frequency is 1 times per second): The RAID is reconstructing. ◇ Light off: The HDD runs normally or is not in place.
4	VGA port	VGA video output interface, output analog video signal, can be connected to the display to watch the server local interface.

No.	Name	Description
5	USB3.0 port	Connects to external devices, such as a mouse and a keyboard.

1.2.4 GU2 Rear Panel

Figure 1-4 Rear panel

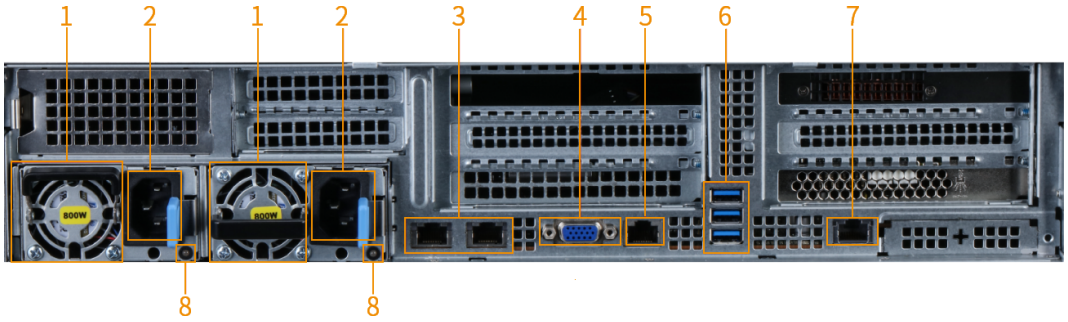


Table 1-5 Panel description

No.	Name	Description
1	Fan	The fan turns on automatically after the power is turned on.
2	Power port	Connects to the power supply.
3	Ethernet port	2 10 Gbps Ethernet ports, connected to the network cable. Ethernet ports can be used to access BMC.
4	VGA port	VGA video output port. Outputs analog video signal, and it can be connected to the display to watch the server local interface.
5	Serial port	Used for ordinary serial port debugging and transmission of transparent serial port
6	USB3.0 port	Connects to external devices, such as a mouse and a keyboard.
7	BMC management network port indicator	100 Mbps management network port, only for access BMC. It cannot be used as a data network port.

No.	Name	Description
8	Power indicator	• Solid green: Connects to the power supply and runs normally. • Amber flashing: PSU abnormality. • Light off: Power supply disconnected. • Green light flashes: When the firmware of PSU is updated, the PSU handle flashes green. • Green light flashes and turns off: When hot-swappable PSU, the PSU handle flashes the green light at a frequency of 4 times per second, and then turns off, indicating that the PSU does not match the efficiency, function group, operating condition and the supported voltage.

1.2.5 DC2 Front Panel

Figure 1-5 Front panel

Table 1-6 Panel description

No.	Name	Description
1	UID switch and indicator	UID switch/indicator are used to locate the device to be operated. • UID indicator ◇ Light off: The device is not located. ◇ Flashing blue (flashing for 255 seconds): The device is focused. ◇ Solid blue: The device is located. • UID switch ◇ The lights can be turned off, on, or blinking by manually pressing the Web UIremote control of the UID switch, iBMC command, or iBMC. ◇ Press the UID switch to turn on or shut down locator light. ◇ Press and hold UID switch for 5 seconds, and then you can reset the iBMC management system of the server.
2	Health status indicator	• Solid green: The device runs normally. • Red light flashes slowly: The system has a serious alarm. • Red light flashes quickly: The system has an emergency alarm.

No.	Name	Description
3	Power switch/ indicator	• Power indicator ◇ Solid yellow: The device is in standby state. ◇ Solid green: The device is powered on. ◇ Yellow light flashes: The iBMC management system is starting. ◇ Light off: The device is not powered up. • Power switch ◇ In the power-on state, press the switch to shut down operating system. ◇ In the power-on state, press and hold the switch for 6 seconds to power down the server. ◇ In the standby state, press the switch to power on the server.
4	Error diagnostics nixie tube	• Displays --- : Server is normal. • Displays error code: Server has a part error.
5	Network adapter bit indicator (1, 2)	• 1, 2: 1 represents network adapter 1 and 2 represents network adapter 2. • Solid green: The network adapter is in place and can be recognized normally. • Light off: The network adapter is not in place or network adapter error.
6	HDD slot	Used to install the HDD.
7	VGA port	VGA video output interface, outputs analog video signal, can be connected to the display to watch the server local interface.
8	USB 3.0 port	Connects to external devices, such as a mouse and a keyboard.

1.2.6 DC2 Rear Panel

Figure 1-6 Rear panel

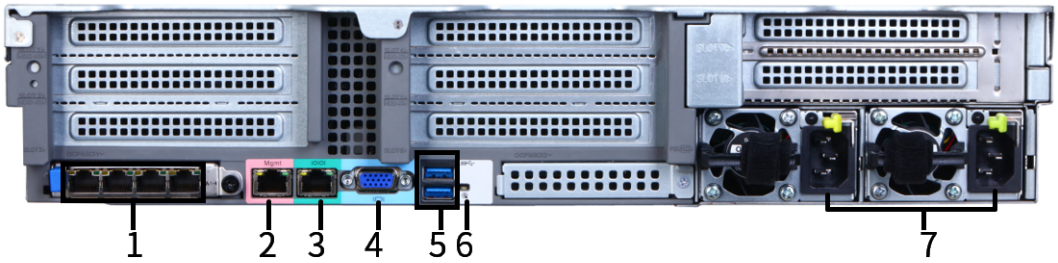


Table 1-7 Panel description

No.	Name	Description
1	Ethernet port	Four 1000 Mbps/100 Mbps Ethernet port. Connects to the network. Each Ethernet port has 2 indicators, data transfer status indicator (left) and connection status indicator (right). ● Data transfer status indicator ◇ Yellow light flashes: The data is being transmitted. ◇ Light off: No data transmission. ● Connection status indicator ◇ Solid green: Network connected. ◇ Light off: Network disconnected.
2	Ethernet management port	One 1000 Mbps/100 Mbps/10 Mbps adaptive Ethernet management port is used to access the iBMC and manage the server.
3	Commissioning serial port	The default is the system serial port which can be set to the iBMC serial port through the command line. It is mainly used for commissioning.
4	VGA port	VGA video output interface, outputs analog video signal, can be connected to the display to watch the server local interface.
5	USB 3.0 port	Connects to external devices, such as a mouse and a keyboard.
6	UID indicator	The UID indicator can be used to locate the server. ● Light off: The device is not located. ● Solid blue: The device is being located. ● Flashing blue (flashing for 255 seconds): The device is focused.
7	The power module interface	Inputs 100-240 VAC power supply.

1.2.7 TS2 Front Panel

Figure 1-7 Front panel

Table 1-8 Panel description

No.	Name	Description
1	USB 2.0 port	Connects to external devices, such as a mouse and a keyboard.
2	Power switch	In the power-on state, press and hold the switch for 4 seconds to shut down the server.
3	UID switch and indicator	UID switch and indicator are used to locate the device to be operated. Press the UID switch to turn on or shut down the locator light. Press and hold UID switch for 4 seconds, and then you can reset the iBMC management system of the server.
4	Network indicator	Indicates the current network status. ● Solid green: Network connected. ● Green light flashes: Network data is being transmitted. ● Light off: Network disconnected.
5	System status indicator	Indicates the running status of the server. ● Solid green: System runs normally. ● Red light flashes: Indicates a serious error occurred on the server. ● Solid red: Indicates an urgent error occurred on the server.

1.2.8 TS2 Rear Panel

Figure 1-8 Rear panel

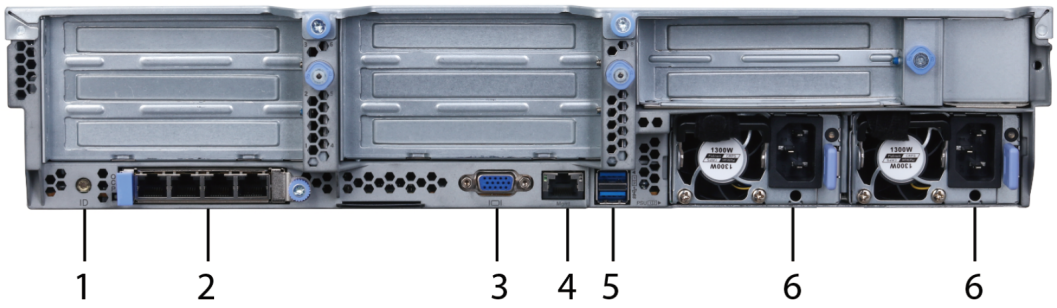


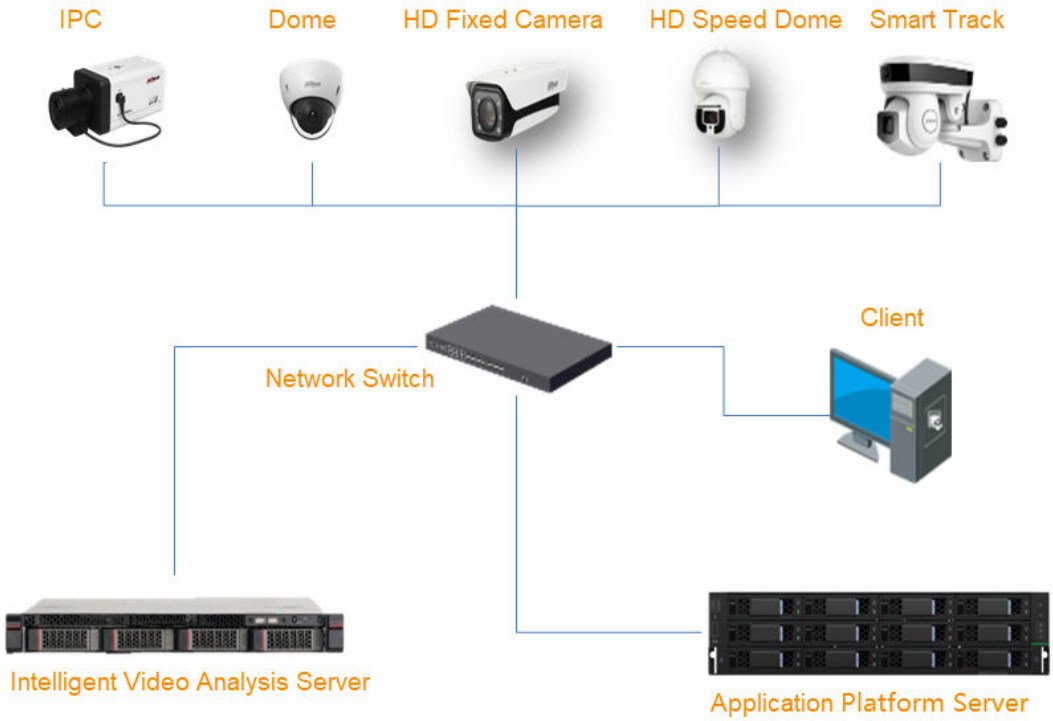
Table 1-9 Panel description

No.	Name	Description
1	ID indicator	Used to locate the device to be operated.
2	Ethernet port	Four 1000 Mbps adaptive Ethernet ports. Connects to the network cable.
3	VGA port	Connects to a VGA monitor or a physical KVM.

No.	Name	Description
4	Management network port	Management network port, only for access to BMC. It cannot be used as a data network port.
5	USB 3.0 port	Connects to external devices, such as a mouse and a keyboard.
6	Power port	Connects to the power supply. To ensure the stability and reliability of the server, we recommend connecting 2 power ports at the same time to achieve redundancy power supply. When one power supply fails, the other power supply can still supply power to the server, reducing the impact of device error or downtime.

1.3 Typical Networking

Figure 1-9 Typical networking



Networking description:

- Confirm that the devices in the network are connected.
- Log in to the Client to operate the server. Set intelligent rules and record alarm events.
- One analysis card supports up to 32 channels of 1080P camera video data at the same time.

If a large model is configured on an analysis card, it only supports analyzing video data from two 1080P cameras.

- By default, the server is delivered with software installed completely. The default IP address is 192.168.1.108. Switch to the local IP once started. The default username and password are admin and admin123 respectively. Change your password in time on your first successful login.

  During the initialization process, you can change the IP address.

- Initialization password is required for the first-time login to the server. We recommended you change the password promptly after the first successful login.

2 Cable Connection

Prerequisites

Make sure all cables are properly connected before powering on the Device. Make sure that there is no obvious damage to the Device and the cables.

Procedure

Step 1 Connect the display through VGA port and connect the mouse and the keyboard through USB ports.

Step 2 Insert one end of the network cable into the Ethernet port on the rear panel of the Device, and the other end to the network.

Step 3 Connect the power, and then the Device will be started in about 1 minute.

The Device can be accessed through the network after it is powered on.

3 Initial Settings

When using the Device for the first time, initialize the Device, and configure basic information and functions first.

3.1 Initializing the Device

If it is your first time to use the Device after purchasing or restoring the Device to factory settings, set a login password of admin (system default user). At the same time, you can set a proper password protection method. This section uses remote initialization on the web interface as an example.

Prerequisites

The IP address of the PC needs to be set to the same network segment as the default IP address of the Device.

Procedure

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

The default IP addresses 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 Set the language and region, select the video standard that is used in your region, and then click **Next**.

Step 3 Configure the time parameters, and then click **Next**.

Figure 3-1 Time

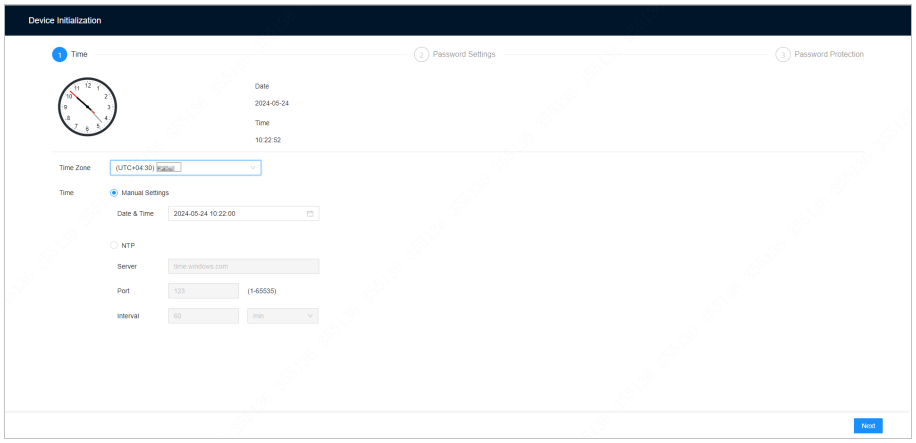


Table 3-1 Time parameters description

Parameter	Description
Time Zone	Select the time zone of the Device.

Parameter	Description
Time	Set system date and time manually or by synchronizing with NTP server time. • **Manual Settings** : Select date and time from the calendar. • **NTP** : Select **NTP**, enter the IP address or domain of the NTP server, and then set the automatic synchronization interval. Enable **NTP**. The time of the Device will be automatically synchronized with the server time.

Step 4 Set admin login password, and then click **Next**.

Figure 3-2 Password

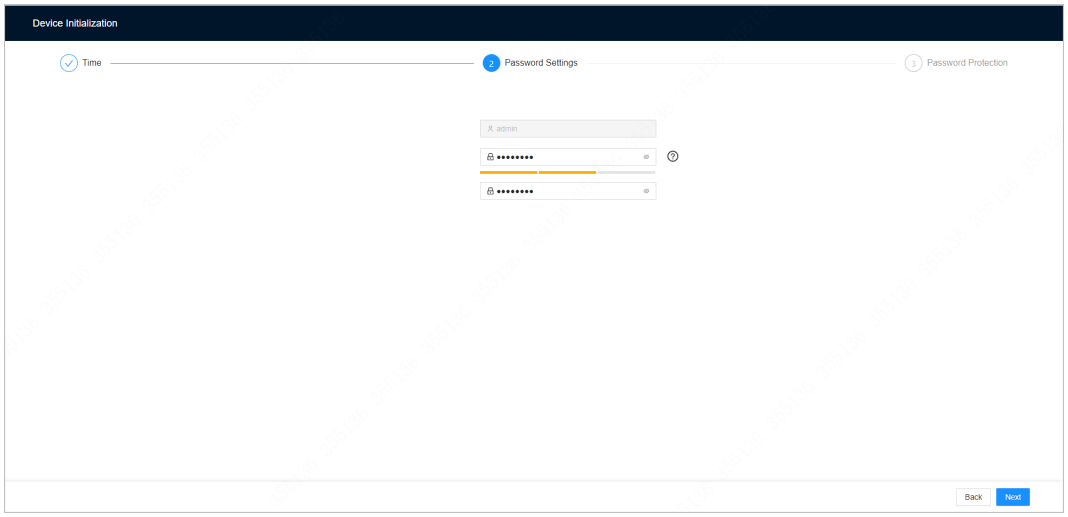


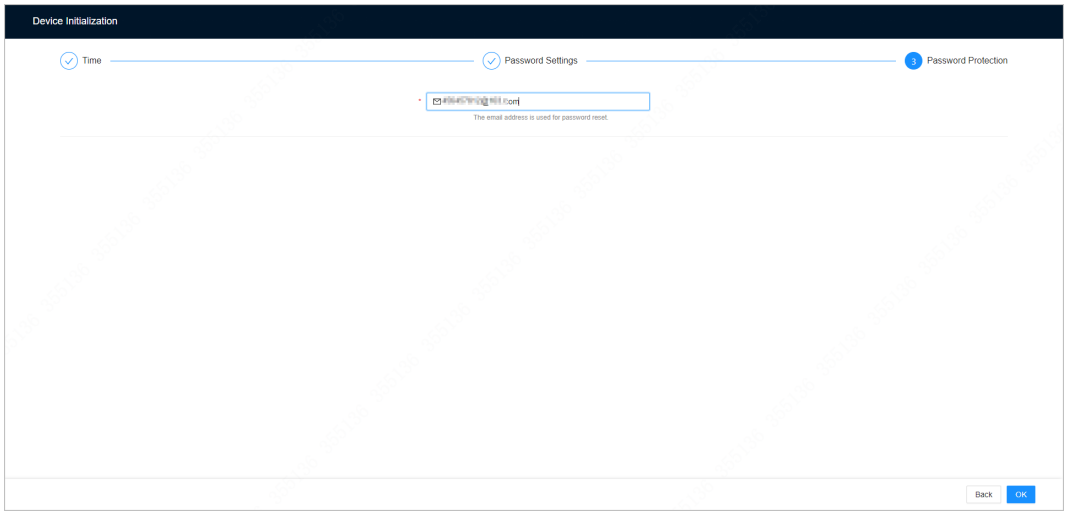
Table 3-2 Description of password parameters

Parameter	Description
Username	The default username is admin.
Password	Set admin login password, and then confirm the password. Click to view the password requirements.
Confirm Password	

Step 5 Enter the reserved email address.

You can use the reserved email address to reset admin password.

Figure 3-3 Password protection



Step 6 Click **OK**.

The Device is initialized. You can click **Quick Config** to configure quick settings.

3.2 Quick Settings

Configure the IP address and DNS server information of the Device according to network planning.

Prerequisites

Make sure that at least one Ethernet port has been connected to the network before you set IP address.

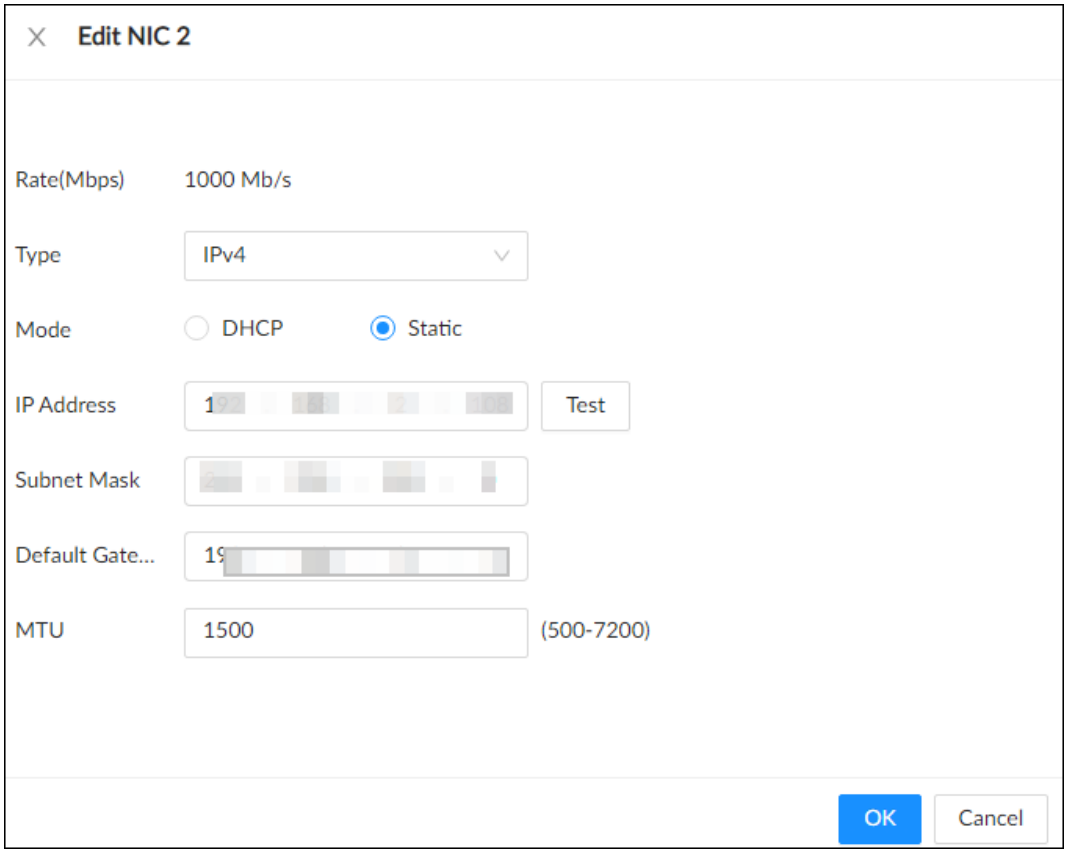
Procedure

Step 1 On the page that prompts you initialization succeeded, click **Quick Config**.

Step 2 Configure the IP address.

1. Click of the corresponding NIC.

Figure 3-4 Edit Ethernet network



2. Set parameters.

Table 3-3 NIC parameters description

Parameter	Description
Rate (Mbps)	The maximum network transmission speed that the current NIC supports.
Type	Select IPv4 or IPv6.
Mode	• **DHCP** : When there is a DHCP server on the network, you can enable DHCP. The system allocates a dynamic IP address to the Device. There is no need to set IP address manually. • **Static** : You need to enter the IP address, subnet mask and gateway.
IP Address	Select **Static**. Need to provide the IP address, subnet mask, and default gateway for the network planning and input device. Click **Test** and check if the IP address is valid.
Subnet Mask	
Default Gateway	

Parameter	Description
MTU	Set NIC MTU value. The default setup is 1500 bytes. We recommend you check the MTU value of the gateway first and then set the MTU value of the Device equal to or smaller than the gateway value, which helps to reduce the packets slightly and enhance network transmission efficiency. Please be advised that changing MTU value might result in NIC restart, network offline and affect current running operation.

3. Click **OK**.

Step 3 Set the default NIC.

Select the default NIC from the dropdown menu in the **Default NIC** according to your specific needs.

Make sure that the default NIC is online.

Step 4 Set the DNS server information.

You can choose to automatically obtain the DNS server address or manually enter the DNS server address.

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

1. Select the type of DNS server IP address, either optional IPv4 or IPv6 address format.
2. Select the method to obtain the DNS server address.
   - Select **DHCP** so that the Device can automatically get the IP address of the DNS server on the network.
   - Select **Static** and then enter the preferred and alternate DNS addresses.

Step 5 Click **OK**.

3.3 Login

You can operate the Device by using the web interface and PC client.

After initializing the Device, you have logged in by default. Now you can configure system settings and operate it.

3.3.1 Logging in to PC Client

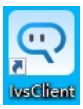
The system supports remote access to the Device through the PC client, and then you can configure functions and maintenance the system on the PC client.

Procedure

Step 1 Download the PC client.

1. Open the browser, enter IP address, and then press the Enter key.
2. Click **Download PC Client** to download the installation package.

Step 2 Double-click the installation package, and then follow the on-screen instructions to install the PC client.

Step 3 After installation, a desktop icon 

will be generated.

Step 4 Select **I have read and agreed to the privacy policy and user agreement** and then click **OK**.

3.3.2 Logging in to Webpage

You can use the general browser such as Google Chrome, and Firefox to access the webpage to manage the Device remotely, operate and maintain the system.

Procedure

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

Step 2 Enter username and password.

- The default administrator username is admin. The password of the admin account is what you set during initialization. For your device safety, change the password of the admin account regularly and keep it safe.
- If you forget the password of the admin account, click **Forgot password?** to reset.

Step 3 Click **Login**.

3.4 Initializing Remote Device

After you initialize the remote devices, you can change their login passwords and IP addresses. You can connect remote devices to the Device only after the remote devices have been initialized.

Procedure

Step 1 Log in to the PC client.

Step 2 Click  on the upper-right corner of the page and then click **Camera**.

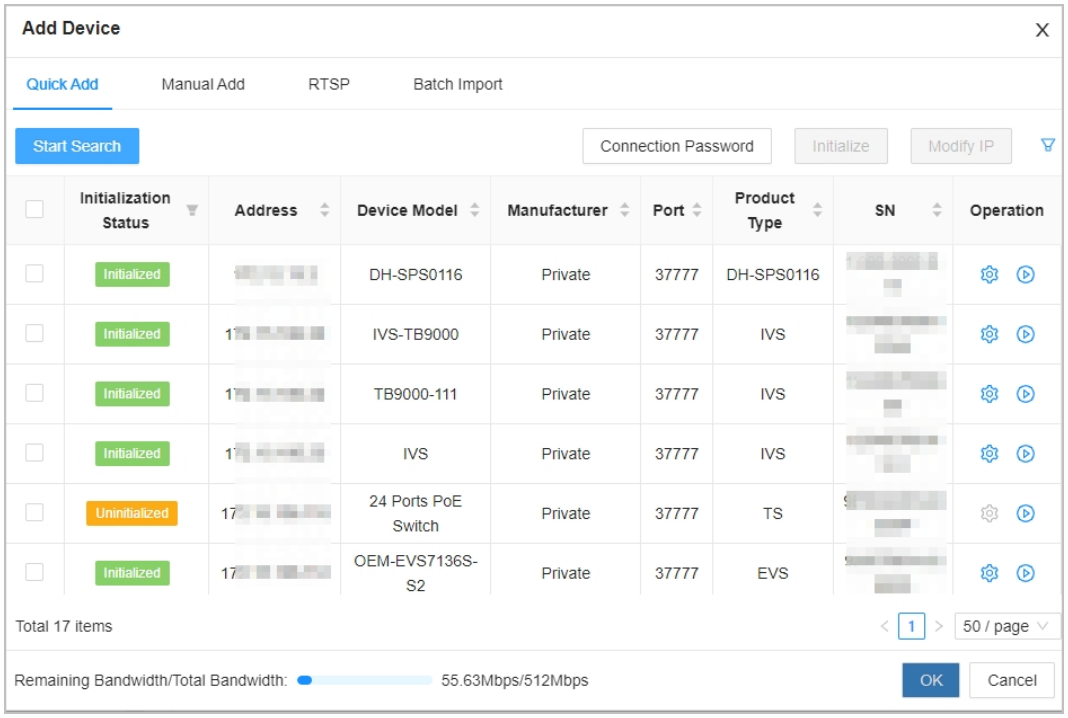
You can also click **Camera** from the configuration list on the home page.

Step 3 Under the **Camera** tab, click **Add**.

You can also click **Add** under the device tree.

Step 4 Under the **Quick Add** tab, click **Start Search**.

Figure 3-5 Search for remote device



Step 5 Select an uninitialized remote device and then click **Initialize**.

Click next to **Initialization Status** and then select **Uninitialized** to show uninitialized remote devices only.

Step 6 Set the password and linked email address for the remote device.

You can skip this step if you keep **Using current device password and password protection information** enabled as default. The remote device automatically uses the current admin password and email address of the Device.

1. To manually configure the password, disable **Using current device password and password protection information**.
2. Enter and confirm the password, and then click **Next**.
3. Set an email address, and then click **Next**.

   You can use the email address to reset the password of the remote device if you forget the password.

Step 7 Set the IP address of the remote device and then click **Next**.

- When there is a DHCP server on the network, select **DHCP**, and the remote device gets dynamic IP address automatically. You do not need to enter IP address, subnet mask and gateway.
- If you select **Static**, enter static IP address, subnet mask, default gateway and incremental value.

- Enter incremental value only when you want to change IP addresses of several devices at the same time. The system will allocate IP address one by one with the fourth part of the IP address increasing by the incremental value.

- If an IP conflict occurs when you change the static IP address, the system will notify you of the issue. When an IP conflict happens when you are changing IP addresses in batches, the system automatically skips the conflicted IP and begins the allocation according to the incremental value.

Step 8 Click **Add** or **OK**.

- Click **Add** : The system completes initializing the remote device and then adds the remote device to the Device.
- Click **OK** : The system completes initializing remote device without adding the remote device to the Device.

3.5 Adding Remote Devices

After adding a remote device, you can view the real-time screen of the remote device and modify its configuration. You can add remote devices to the Device in any of the following ways.

Table 3-4 Methods of adding remote devices

Method	Description
Quick Add	Search for the remote devices on the same network and then filter the search results to register the remote devices that you need. We recommend this method if you do not know the exact IP address of the remote device.
Manual Add	Enter the IP address, username and password of the remote device. We recommend this method when you want to add only a few remote devices and you know their IP addresses, usernames, and passwords.
RTSP	Add remote devices through RTSP. We recommend this method when you add stream media devices.
Batch Import	Fill in information on remote devices in the template, and then import the template to add the remote devices. We recommend this method when you want to add a lot of remote devices whose IP addresses, usernames and password vary with each other.

3.5.1 Quick Add

Procedure

Step 1 Log in to the PC client.

Step 2 Click  on the upper-right corner of the page and then click **Camera**.

You can also click **Camera** from the configuration list on the home page.

Step 3 Under the **Camera** tab, click **Add**.

You can also click **Add** under the device tree.

Step 4 Under the **Quick Add** tab, click **Start Search**.

Click **Stop Search** to stop searching for remote devices.

To filter the search results, you can click .

Table 3-5 Description of search results

Parameter	Description
Connection Password	Click **Connection Password** to set the username and password for the remote devices. If you do not set the username and password for the remote device, the system will try to add the remote device by using the username and password of the Device.
Initialize	Select uninitialized remote devices, and then click **Initialize** to start initialization.
Modify IP	Select one or more remote devices, and then click **Modify IP** to change their IP addresses.
Initialization Status	Click and then select **Initialized** or **Uninitialized** to show initialized or uninitialized remote devices only.
Operation	• Click to configure parameters of the remote device. • Click to view the real-time video from the remote device. You can view the live video only when the admin password of the remote device is admin, or the same as the admin password of the Device.
Remaining Bandwidth/Total Bandwidt	Displays the remaining and total bandwidth. You cannot add more remote devices when the bandwidth runs out.

Step 5 Select one or more remote devices, and then click **OK**.

- During the adding process, click **Cancel** to cancel adding the remote device.
- If a remote device is in exception due to network disconnection or other reasons, it can still be added. It comes online after the exception is resolved.

Step 6 Click **Add more** or **Complete**.

- Click **Add more** , the Device goes back to the **Quick Add** window and you can add more remote devices.
- Click **Complete** if you do not want to add more remote devices at the moment. The Device goes back to the **Camera** tab where you can view the added remote devices.

3.5.2 Manual Add

Procedure

Step 1 Log in to the PC client.

Step 2 Click on the upper-right corner of the page and then click **Camera**.

You can also click **Camera** from the configuration list on the home page.

Step 3 Under the **Camera** tab, click **Add**.

You can also click **Add** under the device tree.

Step 4 Under the **Manual Add** tab, click **Add Device**.

Step 5 Set parameters and then click **OK**.

Figure 3-6 Remote device settings

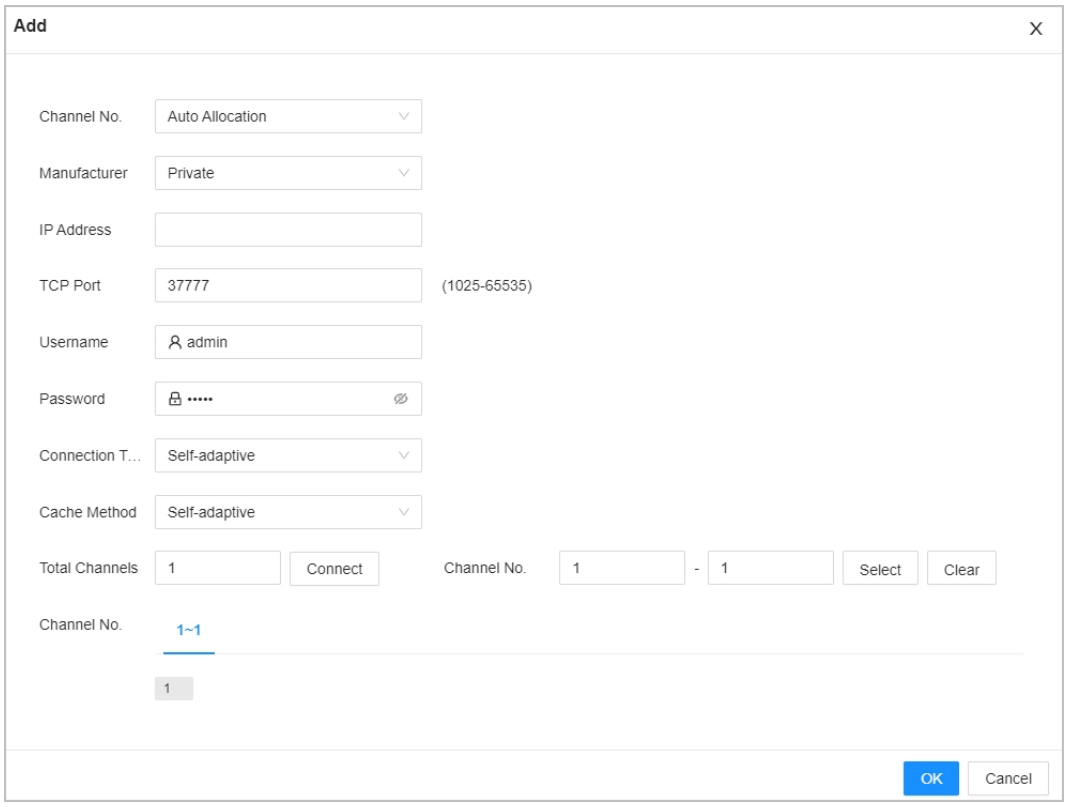


Table 3-6 Parameters of adding remote device

Parameters	Description
Channel No.	Select a channel number for the remote device on the Device. If you select **Auto Allocation**, system will provide a channel number automatically.
Manufacturer	Select the connection protocol of the remote device. **Private** is selected by default.
IP Address	Enter the IP address of the remote device.
TCP Port	Enter the TCP port number of the remote device. Default is 37777.
Username	Enter the username and password of the remote device.
Password	

Parameters	Description
Connection Type	Select a connection type from **Self-adaptive** , **TCP**, **UDP** and **Multicast**. The connection types available might differ depending on the manufacturer.
RTSP Mode	Select **Self-adaptive** or **Custom**. When **Manufacturer** is ONVIF or ONVIFS, you need to configure this parameter.
RTSP Port	When you select **Custom** for **RTSP Mode**, enter the RTSP port number. The default port number is 554. The value ranges from 1 through 65535.
HTTP Port	Enter the HTTP port number. The default port number is 80. The value ranges from 1 through 65535. After changing the HTTP port number, you need to add the HTTP port number to the IP address in the address bar of the browser so that you can log in to the web interface of the remote device.
HTTPS Port	Enter the HTTP port number. The default port number is 80. The value ranges from 1 through 65535. When **Manufacturer** is **Onvifs**, you need to configure this parameter.
Cache Method	Select a cache method from **Self-adaptive** , **Realtime** and **Fluent**.
Total Channels	When the remote device has multiple channels, you can select one or more channels of the remote device that you want to add to the Device. 1. Click **Connect** to get the total number of channels of the remote channel. 2. Enter the range of channels that you need, and then click **Select** to select all the channels in the range. 3. Click **OK**.

Step 6 Select the remote device and then click **OK**.

3.5.3 RTSP

Procedure

Step 1 Log in to the PC client.

Step 2 Click on the upper-right corner of the page and then click **Camera**.

You can also click **Camera** from the configuration list on the home page.

Step 3 Under the **Camera** tab, click **Add**.

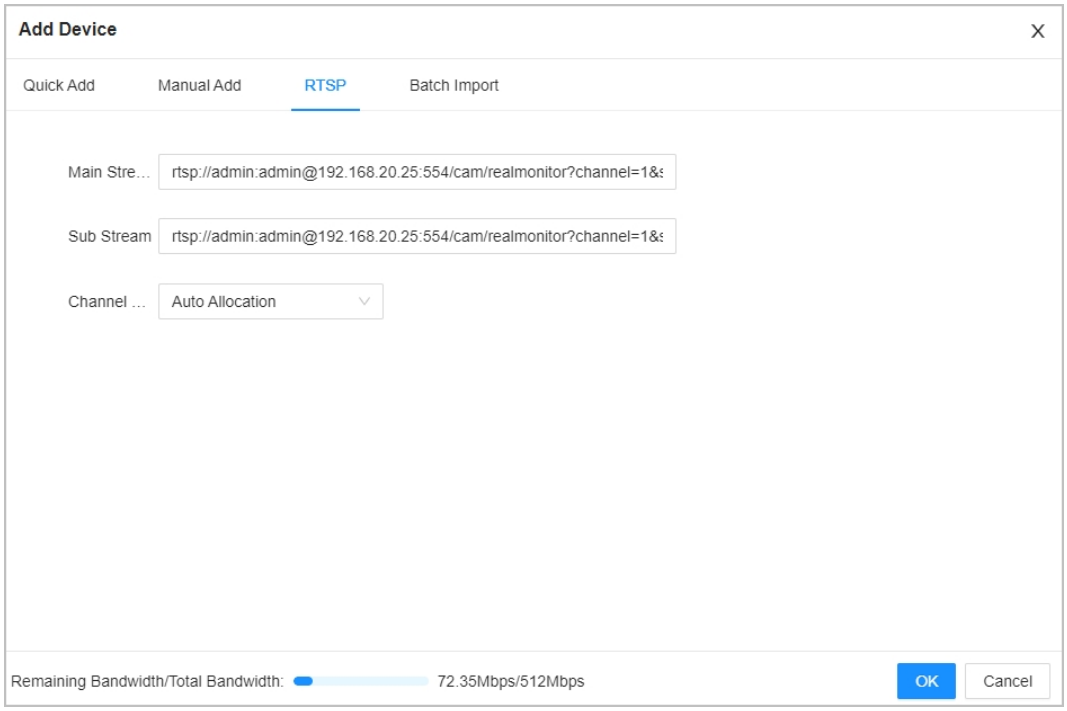
You can also click **Add** under the device tree.

Step 4 Under the **RTSP** tab, enter the RTSP address.

The RTSP address format is rtsp://<username>:<password>@<IP address >:<port>/cam/realmonitor?channel=1&subtype=0. For example, rtsp://admin:admin@192.168.20.25:554/cam/realmonitor?channel=1&subtype=0.

- Username: Username of the remote device.
- Password: Password of the remote device.
- IP address: IP address of the remote device.
- 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.

Figure 3-7 RTSP



Step 5 Click **OK**.

3.5.4 Batch Add

Procedure

Step 1 Log in to the PC client.

Step 2 Click on the upper-right corner of the page and then click **Camera**.

You can also click **Camera** from the configuration list on the home page.

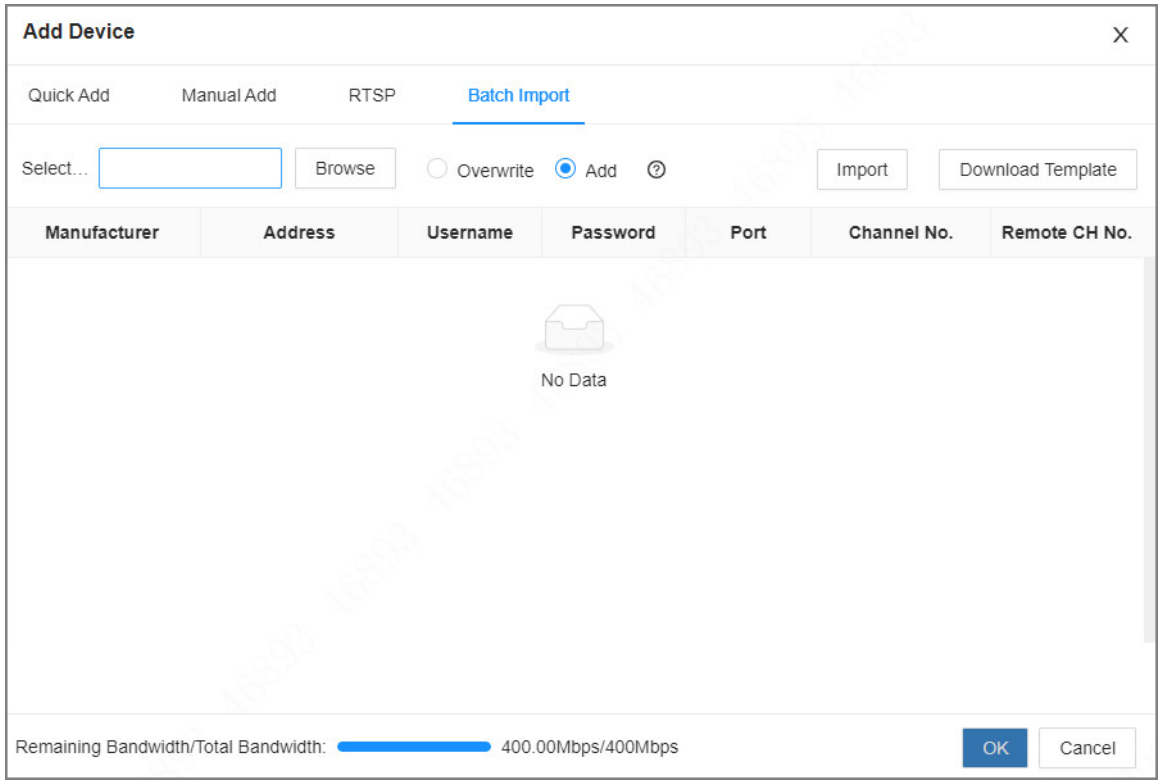
Step 3 Under the **Camera** tab, click **Add**.

You can also click **Add** under the device tree.

Step 4 Under the **Batch Import** tab, click **Download Template** to download the template.

- On the PC client, click at the top of the client, select **Download** to view the storage path.
- On the web interface, files are saved to the default downloading path of the browser.

Figure 3-8 Import CSV file



Step 5 Fill in and save the template file.

Step 6 Import the template.

1. Under the **Batch Import** tab, click **Browse** to select the file that you have filled in.
2. Select an import mode.
   - **Overwrite** : The system removes the added remote devices before importing new devices.

     If you select **Overwrite**, all the existing devices will be deleted.
   - **Add** : The system imports remote devices without deleting the existing ones.
3. Click **Import**. You can view the imported information on the remote devices.

   If the information on remote devices is not filled in completely, you can improve it after importing the template.

Step 7 Click **OK**.

4 Client Configuration

You can log in to the Device client to configure detection solutions and rules.

4.1 Preparation

Before configuration, make sure that:

- The server is enabled.
- Once the server is powered on, the light on the front panel will be on. It indicates that the server started and is running normally.
- The Client is installed.
- The network for the PC where the Client is to be installed has already been set up, and that the network cameras, and server are already on the network segment.

4.2 Client Homepage

Figure 4-1 Client homepage

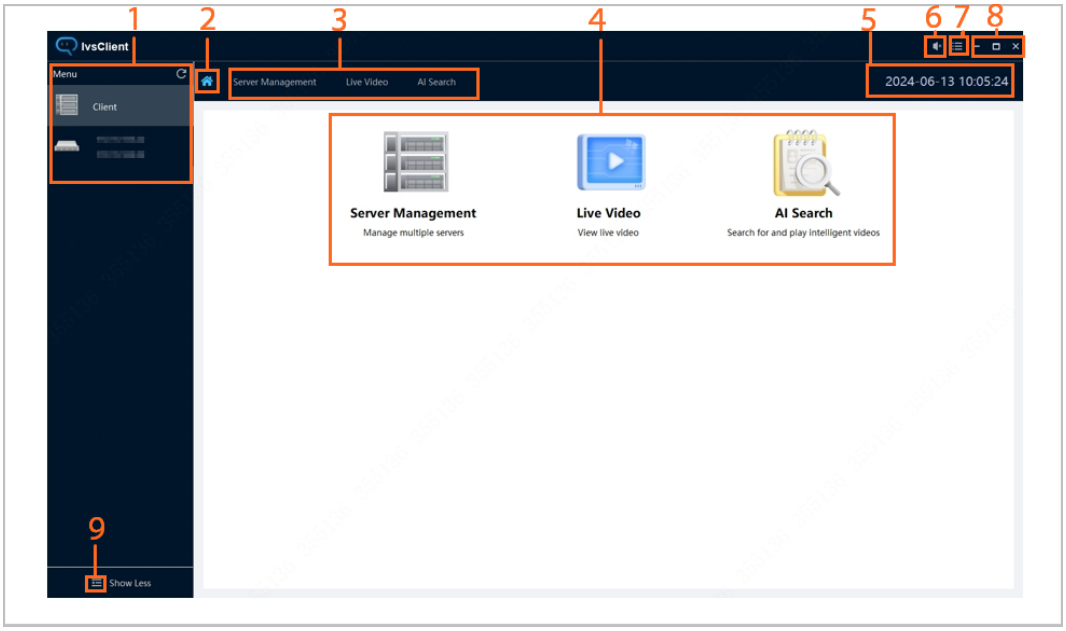


Table 4-1 Client homepage description

NO.	Description
1	Menu Choose to enter the client on-premises or the server homepage that has been added based on actual needs.
2	Click and return to the client homepage.
3	Function list Click on the corresponding function to configure the corresponding parameters.

NO.	Description
4	Function configuration Click on the corresponding functional module to enter the corresponding function configuration page.
5	Display the date and time.
6	Alarm sound on/off.
7	Click and view the system information, open source declaration, license agreement, and privacy policy.
8	Minimize, maximize, and shut down the Client.
9	• Click . Expand the menu, the interface on the left displays the list of servers that have been added, and you can switch servers. • Click . Show less the menu.

4.3 Server Homepage

On the client homepage you can switch to the corresponding server homepage by using the device tree in the left menu bar.

Figure 4-2 Server homepage

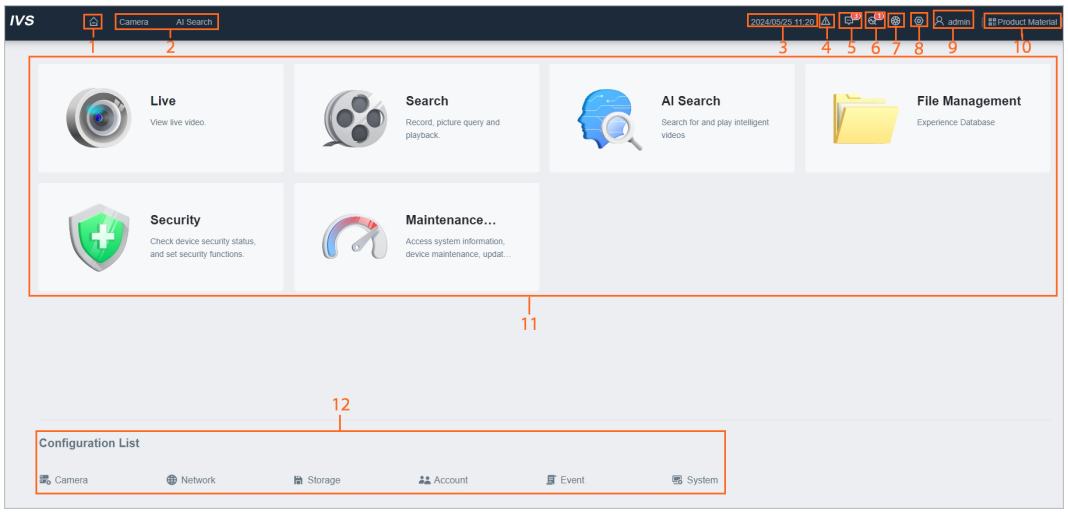


Table 4-2 Server homepage description

NO.	Description
1	Click and return to the server homepage.
2	Function list Click on the corresponding function to configure the corresponding parameters.
3	Display the date and time.
4	View the system event information.

NO.	Description
5	View the system information.
6	One-click diagnosis Assists you in better using the Device by diagnosing the configuration and status of the Device.
7	View information about running tasks in the background.
8	System configuration Click it to select the menu that needs to be configured.
9	Modify the user password, lockout user, log out logged-in user, restart device or shut down device.
10	QR Code Scan the code to obtain product-related information.
11	Function configuration Click on the corresponding functional module to enter the corresponding function configuration page.
12	System configuration list Click on the corresponding function to configure the corresponding parameters.

4.4 Managing Server

You can add and delete the information of the server.

4.4.1 Adding Servers

Procedure

Step 1 Double-click 

to open the Client, and then click **Server Management**.

Step 2 Click **Add** to add servers.

Figure 4-3 Add server

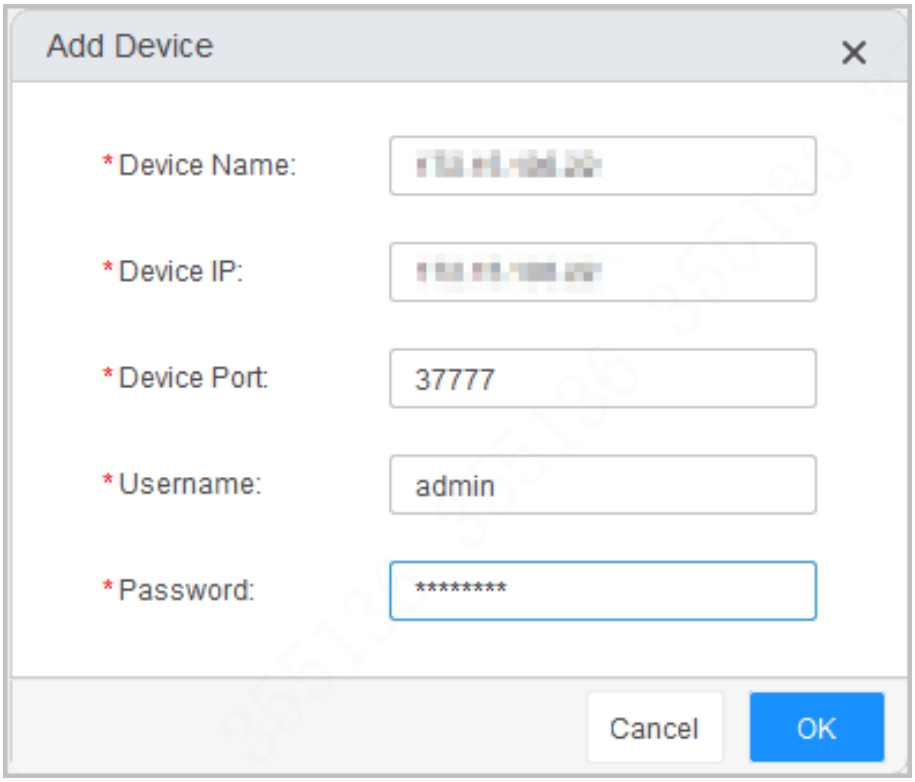


Table 4-3 Description of adding device parameters

Parameter	Description
Device Name	Name the server on the Client to differentiate it from others.
Device IP	The IP address of the server.
Device Port	The protocol port number corresponding to the server, which is 37777 by default.
Username	Server login username and password. The default username is admin. The password is the password that you set when initializing the web client.
Password	

Step 3 Click **Ok**.

After the server is added, it will be online automatically. The channel information is also displayed automatically.

Related Operations

- To delete a server, click corresponding to the server.
- To log out of a server, click corresponding to the server.
- To enter the server homepage, click corresponding to the server.

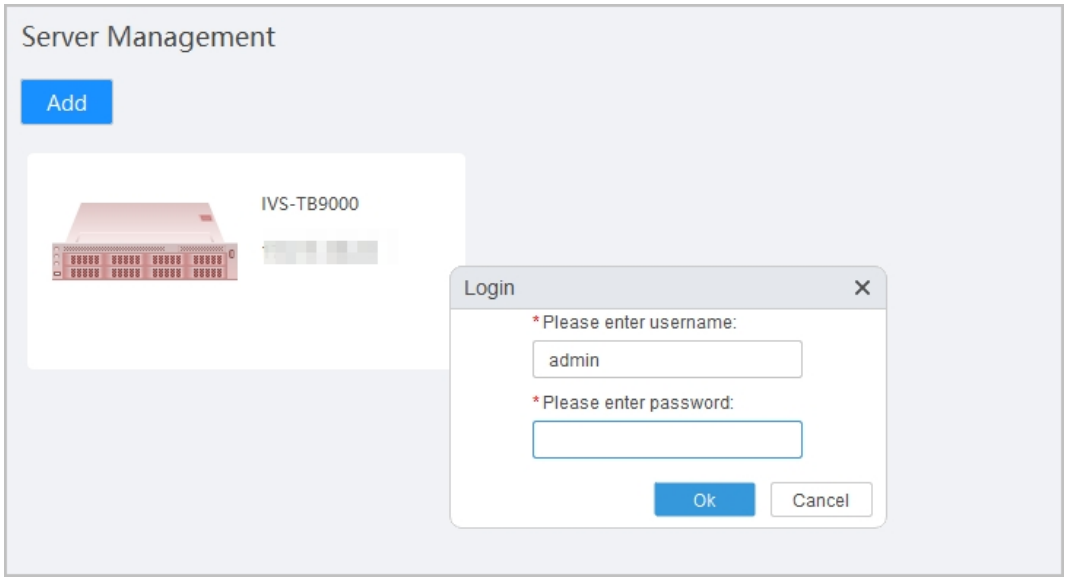
4.4.2 Logging in to and out of Server

Logging in to the Server

Log in to the server to do live view, send out alarm search and other related operations. There are two ways to log in.

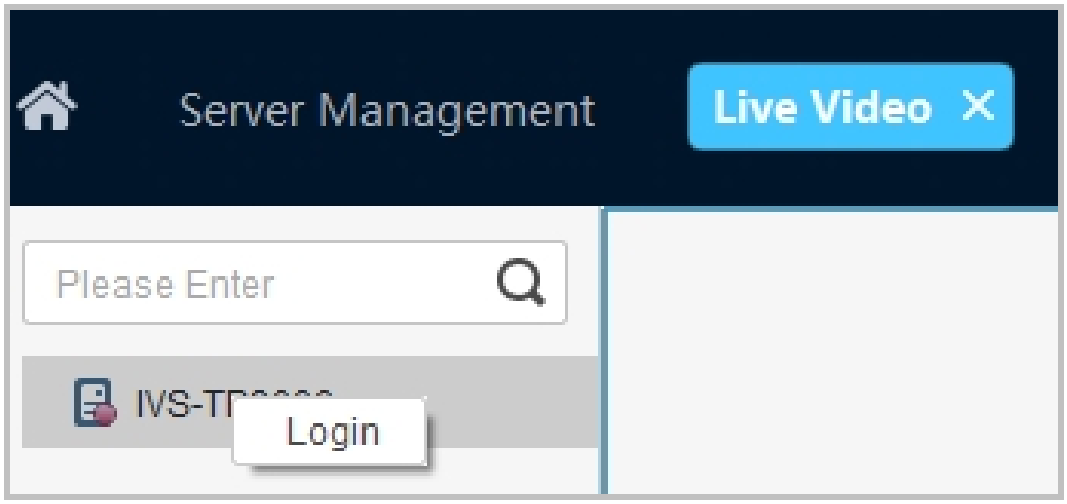
- Open the Client. On the **Server Management** page, select a server, click , and then enter the password.

Figure 4-4 Log in to the server (1)



- Open the Client. On the **Live Video** page, right-click a server, and then click **Login**.

Figure 4-5 Log in to the server (2)

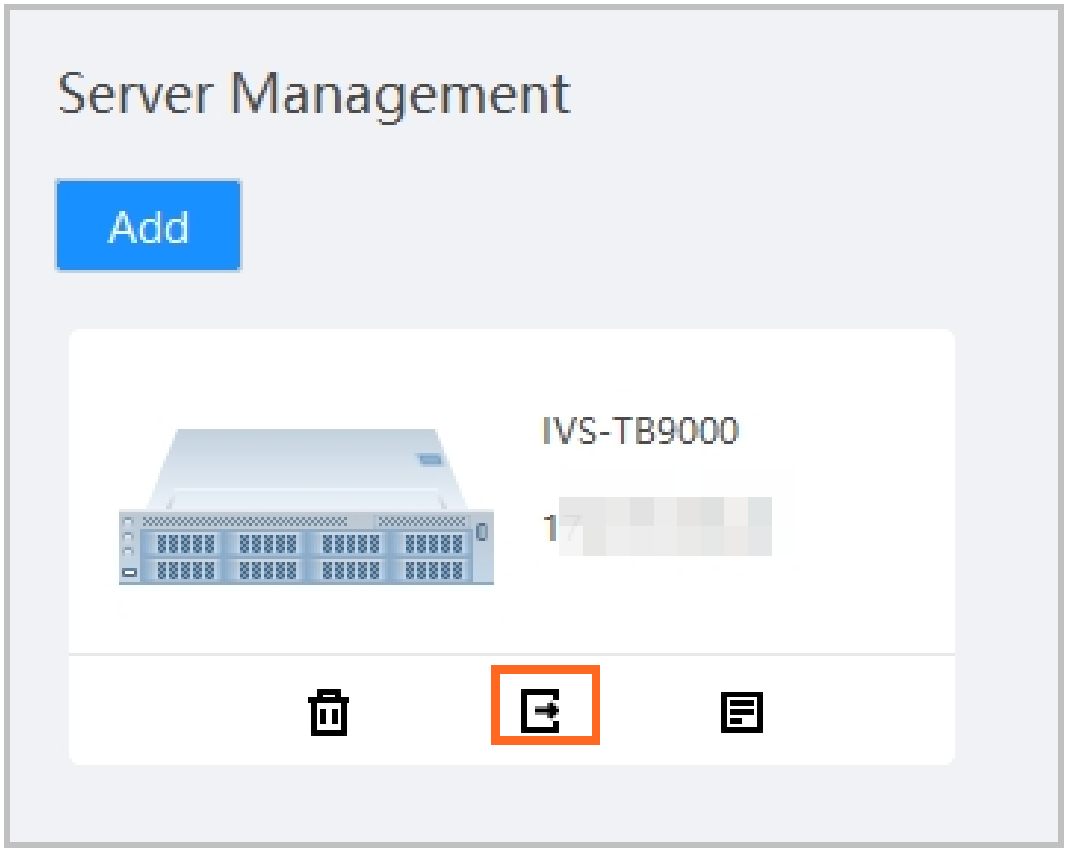


Logging out of the Server

There are two ways to log out:

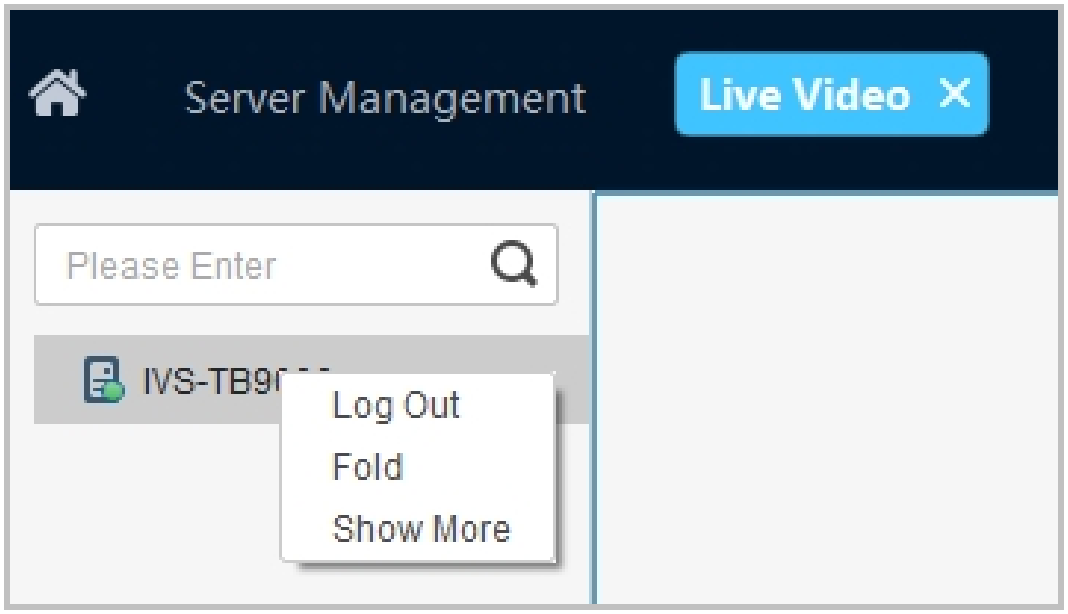
- Open the Client. On the **Server Management** page, select a server, and then click .

Figure 4-6 Log out of the server (1)

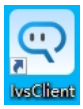


- Open the Client. On the **Live Video** page, right-click a server, and then click **Log Out**.

Figure 4-7 Log out of the server (2)



4.5 Live Video

Double-click 

to open the client, and then click **Live Video** tab.

- If the server is not added, the interface will remind you. You can add a server through the **Server Management**.
- If the server has been added, the interface will display a list of servers. You can preview videos, subscribe to events, and view event information.

Figure 4-8 Live video

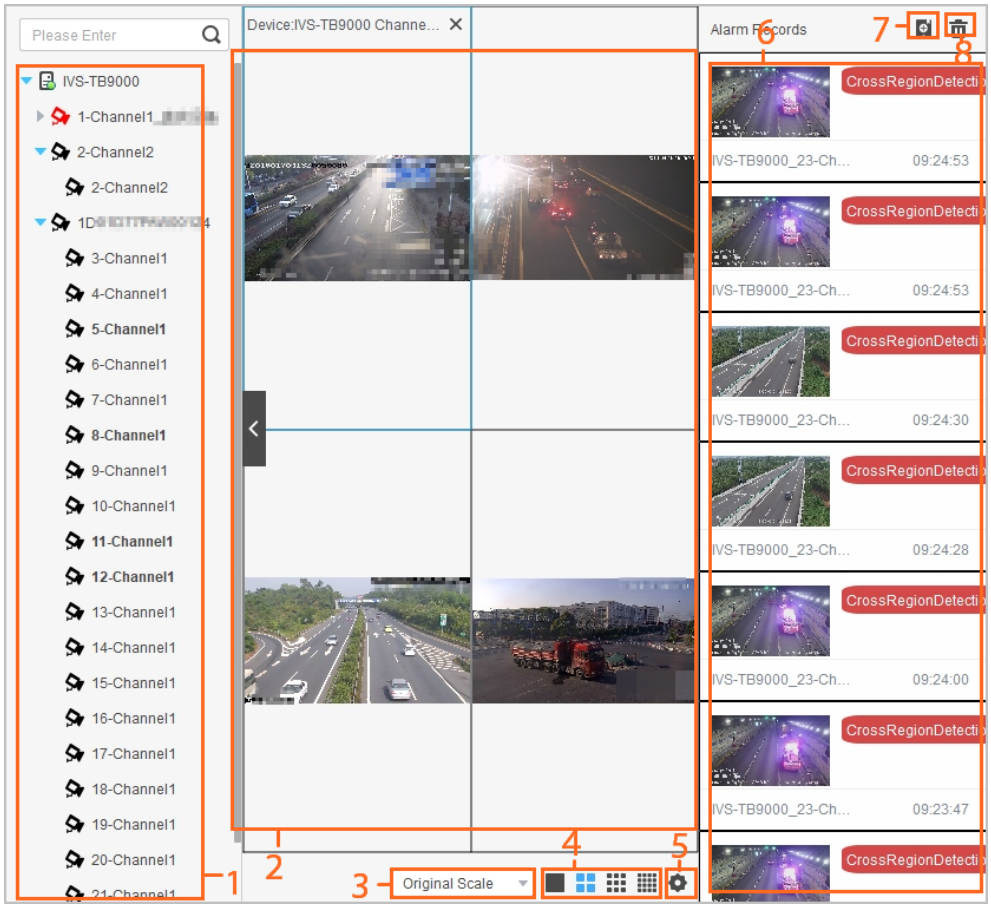


Table 4-4 Live video

No.	Description
1	Channel list. Displays the online and offline status of the server and channels. ● indicates the server is offline. Right-click **Login** on the server to log in to the server. ● indicates the server is online. Right-click **Logout** on the server to log out of the server.

No.	Description
2	Enable live view ● Select a live view window, and then double-click a channel to enable real-time view. ● Drag a channel to a live view window to enable real-time view. ● Select a live view window, right-click a channel, and then select **Start Preview** to enable real-time view. ● 5-Channel1 The channel number is highlighted in bold indicates the channel with live view enabled. ● 4-Channel1 The channel number is not bolded indicates the channel with live view disabled. Right-click the channel to select **Start Preview** to open the monitoring screen. ● indicates channels offline.
3	● In the Original drop-down list at the bottom of the **Live View** page, select the display scale of the video image. ◇ **Full Screen** : The image is expanded to cover the whole screen. ◇ **Original** : The image is displayed with its original size.
4	Select a window layout from . Select single screen, 4-split, 9-split, or 16-split as needed.
5	Intelligent display settings.
6	Alarm information. When intelligent rules are configured, if there is an alarm event, a pop-up window will appear in the bottom right corner of the computer screen, and the traffic event detection alarm will also be displayed on the right side of the client's video preview interface. Supports for viewing large images and playing videos. Alarm information can be found in the intelligent playback interface search, including alarm review results.
7	Alarm subscription. Click to subscribe to alarm information. ● Only alarm information on subscribed channels can be displayed. ● Supports subscribing to multiple server channels at the same time.
8	Click the icon and delete alarm information.

4.6 AI Search

Procedure

Step 1 Double-click IvsClient to open the client, and then click **AI Search** tab.

Please add the server first.

Step 2 Select the server from the server list above the interface. Click **Traffic Event Detection** , **Smoke and Heat Detection** or **Road Debris Detection** tab according to your actual needs. Set the relevant search criteria and click **Search**.

5 Intelligent Operations

Intelligent detection is achieved by performing image processing and analysis to extract key information from videos or images, and then matching it with pre-defined detection rules. When the detected behavior matches the detection rules, an alarm is triggered.

5.1 Setting the Smart Plan

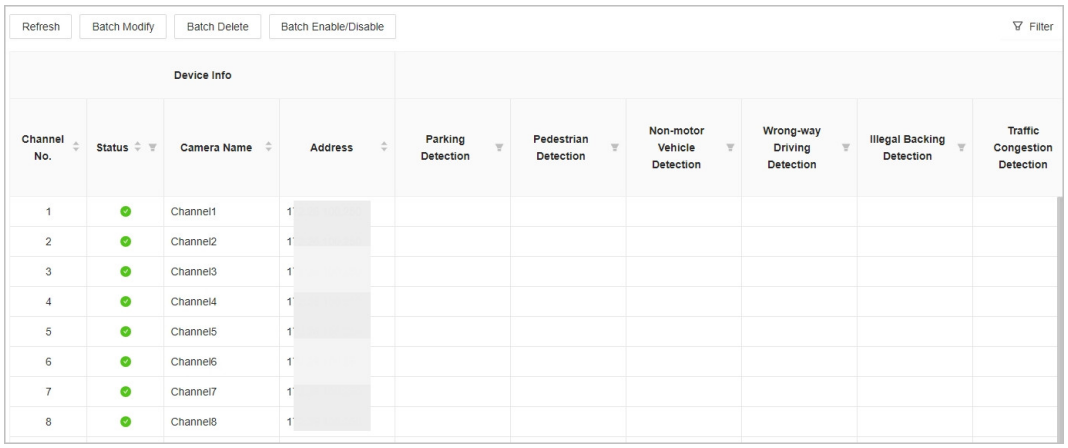
View the status of remote device event functionality and the supported intelligence type for intelligent functions.

View the Event Opening Status

View the status of all remote device event functions in the Device.

Log in to the PC client. Click on the upper-right corner, and then click **Event** . You can also click **Event** from the configuration list on the home page.

Figure 5-1 Overview



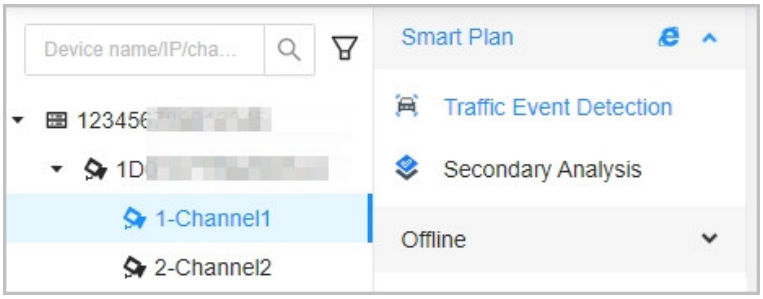
Click on the right side of the **Smart Plan** in the frontend device, it supports directly going to the corresponding frontend login configuration interface.

View the Smart Plan

After adding a remote device, you can obtain the supported AI detection types and the status of AI detection on the remote device.

Log in to the PC client. Click on the upper-right corner, and then click **Event** . You can also click **Event** from the configuration list on the home page. After selecting the channel under the root node in the device tree on the left, select **Smart Plan**.

Figure 5-2 Smart plan



5.2 Scene Selection

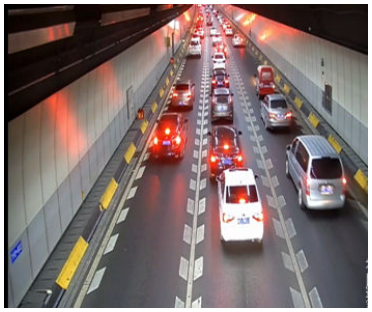
Traffic Event Detection, Smoke and Heat Detection, and Road Debris Detection are suitable for highways, elevated roads, bridges, tunnels, and urban expressways.

Applicable Scenarios

- The resolution for Video input ranges from 2 million to 12 MP.
- The target types include motor vehicles, non-motor vehicles, and pedestrians. The target information includes the target rectangle coordinates and the target type.
- Camera recommendation: Front Mount or Side Mount cameras are recommended when the included angle between the camera and the ground lane is less than 30°, and they cover unidirectional lanes. These cameras are suitable for scenes with up to 8 lanes.
- Suggested installation height for the camera is 6 m to 8 m, with a coverage range of 20 m to 200 m.
- In the case of a 2 MP resolution when accessing video, the pixel requirements for various targets are as follows:
  - The size of the motor vehicle is ≥100 pixels × 100 pixels.
  - Pedestrian, non-motorized vehicle size ≥ 50 pixels × 100 pixels.
  - Litter size ≥ 60 pixels × 60 pixels.
  - Firework size ≥ 60 pixels × 60 pixels.
  - Construction sign size ≥ 80 pixels × 80 pixels.
  - Roadblock size ≥ 40 pixels × 80 pixels.

Table 5-1 Example of applicable scenarios

Scenarios	Example
Highway	

Scenarios	Example
Elevated road	
Bridge	
Tunnel	

Not applicable scenario

- Checkpoint capture scenario: Event capture detection requires a long process, and in this scenario, the camera coverage area is small. When vehicles pass by quickly, it is difficult for the algorithm to detect and track the target, and the effective duration of the event cannot be guaranteed.

Figure 5-3 Depth of Field (DOF) covers a smaller range of close-up scenes.

- Traffic police scene: In this scenario, the front-end E-police is usually responsible for traffic violation punishment and does not perform event analysis.

Figure 5-4 Traffic police scene

- Scene of a dark night: There is no valid illumination, making it difficult to detect targets, especially events caused by scattered objects. Interference from light can result in a large number of false alarms.

Figure 5-5 Scene of a dark night

- Public security point: In this scenario, pedestrians, motor vehicles, and non-motor vehicles are mixed. The event analysis scenario is not applicable.

Figure 5-6 Public security point

- High altitude location: In this scenario, the camera's installation height is too high, which is not suitable for the detection and tracking algorithm as well as the event analysis algorithm.

Figure 5-7 High altitude location

5.3 Batch Modifying Events

Supports setting detection rules for multiple channels simultaneously.

Background Information

Only channels with configured rules support batch modification.

Procedure

Step 1 Log in to the PC client.

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

You can also click **Event** from the configuration list on the home page.

Step 3 Select **Overview** after selecting the root node in the device tree on the left.

Step 4 Click **Batch Modify**.

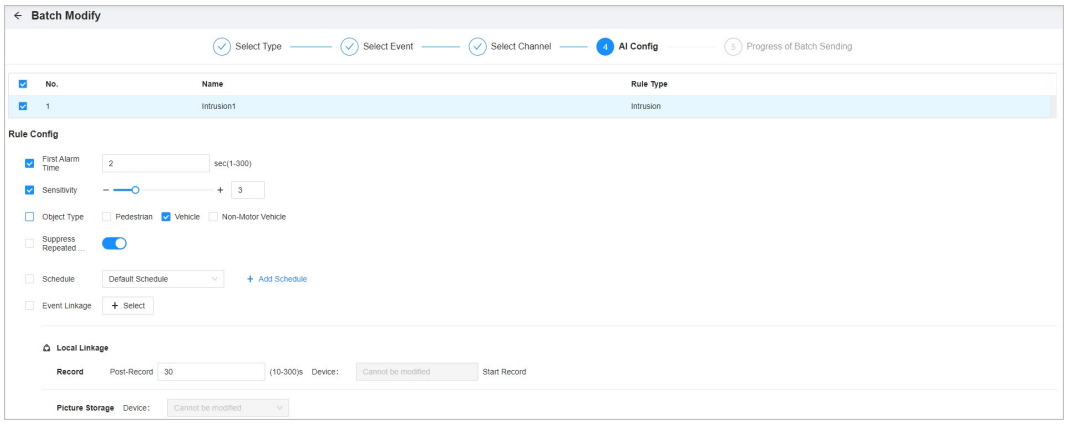
Step 5 According to the page wizard, complete the event configuration.

1. Select the model type, including the small model the and large model, and then click **Next**.
2. Select one event type, and then click **Next**.
3. Select one or more video channels where this event is enabled, then click **Next**.
4. Select the configuration items you need to modify and set the parameters.

   Please refer to the configuration section of each rule below for a detailed introduction to the parameter rule.
5. Click **Save**.

   Page displays batch modify progress. When status indication is successful, it means the setup has been completed.

Figure 5-8 Batch modify



Step 6 Click **OK**.

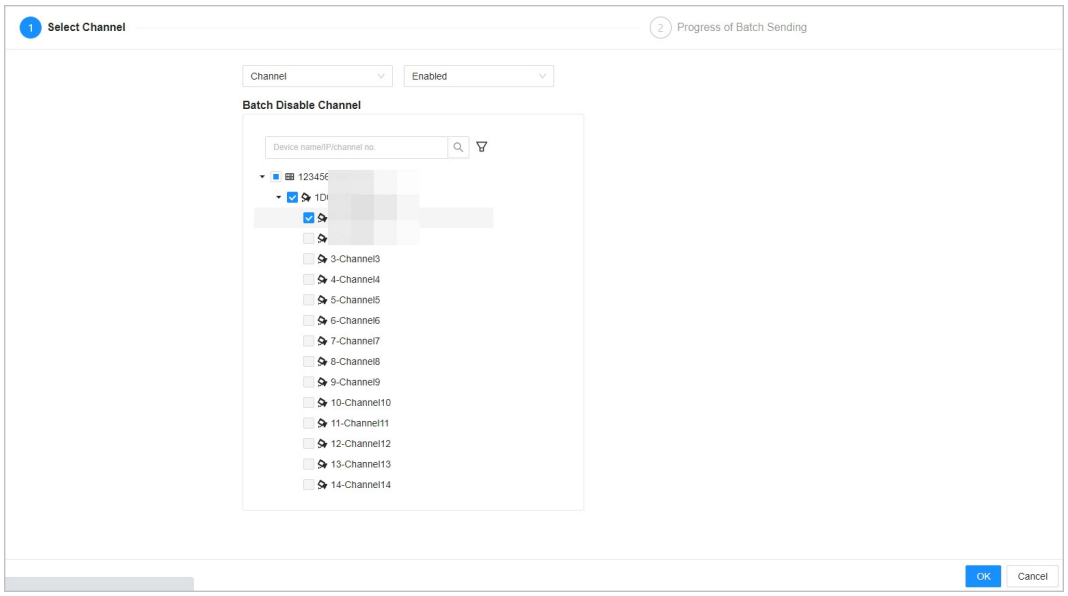
Related Operations

Supports batch modify and delete.

- Batch Enable/Disable: Batch enable or disable smart events for certain channels or presets. Take batch disable smart events for channels as an example.

  1. Click **Batch Enable/Disable**.
  2. Select the object type (**Channel** or **Preset**) and status (**Enabled** or **Not Enabled**). In this example, select **Channel** and **Enabled**, which indicates the need to batch disable smart events.
  3. Select the channels you need to disable, then click **OK**.

Figure 5-9 Batch enable/disable



4. Once the processing is successful, click **Complete**.

- Batch Delete: Supports deleting smart events based on event type or the channel/preset.

1. Click **Batch Delete** , select one event type, and then click **Next**.

   Types include **Event** , **Channel**, **Preset** and **Channel and Preset**.
2. (Optional) Select one event type, then click **Next**.

   When the type is selected as **Channel** , **Preset** or **Channel and Preset**, there is no need to select an event type.
3. Select the video channel, and then click **Next**.
4. (Optional) Select the rule, and then click **Delete**.

   When the type is selected as **Channel** , **Preset** or **Channel and Preset**, there is no need to select a rule.
5. After the deletion is successful, click **OK**.

- When selecting a video channel, you can only choose a channel that has been configured for that event type.
- Traffic flow statistics does not support batch modify.

5.4 Model Configuration

Procedure

Step 1 Log in to the PC client.

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

You can also click **Event** from the configuration list on the home page.

Step 3 Select **Overview** > **Model Config** after selecting the root node in the device tree on the left.

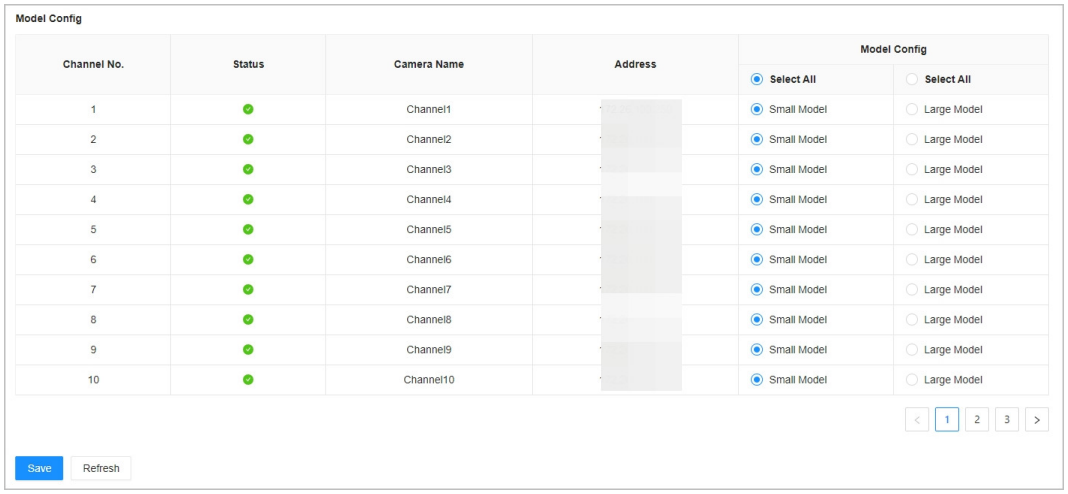
Step 4 Set the model type for each channel.

- Large Model: Select **System** > **AI Config** > **AI Module**, and then set the intelligent analysis card to **Traffic Large Model**.

- Using a large model for event detection can improve detection effectiveness, but the performance will be reduced.
- Smoke detection and heat detection do not support large models.

- Small Model: Select **System** > **AI Config** > **AI Module**, and then set the intelligent analysis card to **Intelligent Analysis Engine**.

Figure 5-10 Model configuration



Step 5 Click **Save**.

5.5 Traffic Event Detection

5.5.1 Global Configuration (Required Operations)

Configure lane, size filtering, detection region, exclusion area and calibrate.

Background Information

Before you start configuring specific rules, it is necessary to complete the global configuration.

Procedure

Step 1 Log in to the PC client.

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

You can also click **Event** from the configuration list on the home page.

Step 3 Select the remote device in the left-hand side device tree.

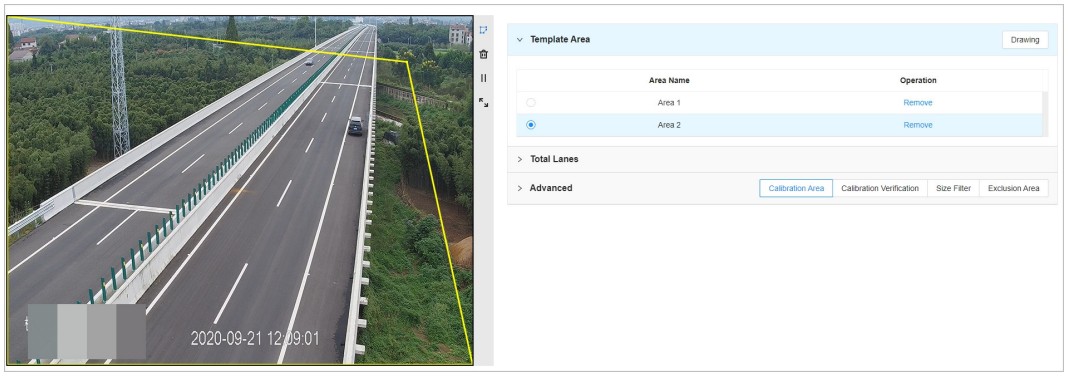
Step 4 Select **Smart Plan** > **Traffic Event Detection** > **Global Config**.

Figure 5-11 Global configuration

Step 5 Click **Drawing** in the **Template Area**, add a new area, and then drag the area box in the video image to adjust its range. Multiple areas are supported for addition.

- Click to delete the area.
- Click to pause screen. Click to play it.
- Click to enter the full screen mode.

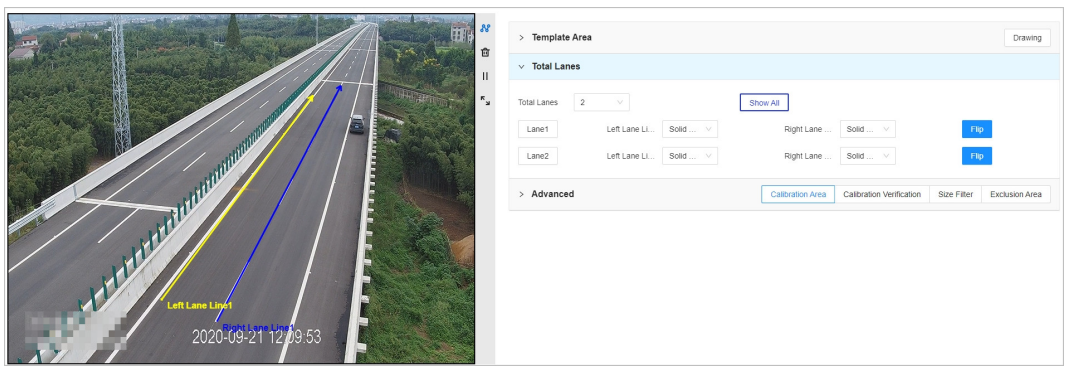
Figure 5-12 Add the area



Step 6 Configure the lane.

Lanes serve as the basis for determining violations such as changing lanes illegally, wrong-way driving, and traffic congestion events.

Figure 5-13 Configure the lane



1. Set the total number of lanes.

   The number of lanes changes with the total number of lanes.

2. Select the lane where lane lines need to be drawn, and then click .
   a. Move the mouse to the starting position of the lane line on the left side of the screen, and click the left button to start drawing.
   b. Move the mouse to the end position of the lane line, click the left button and then click the right button to complete the drawing of this lane line.
   c. Hover over the starting position of the other lane line in the lane, repeat the above steps, and complete the drawing of the remaining lane lines.

   - Supports mouse drag to edit the lane line. Click to edit.
   - Lane line should ideally include the maximum number of vehicles traveling in that lane.
   - The narrowing of the road in the distant view affects judgment. To avoid errors, the lane line can be widened on both sides as needed.
   - A lane consists of two lane lines. When drawing lane lines, make sure to keep the direction of the arrows consistent with the direction of vehicle travel.
   - If you need to draw multiple lanes, please repeat the above steps to draw each lane. You can draw up to 8 lanes.
3. Select the left and right lane line types for the lane.

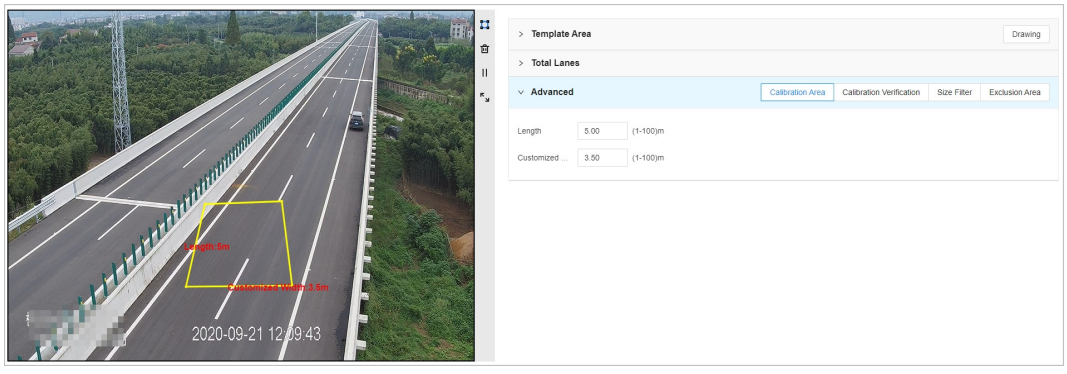
   Supports selecting **Solid White Line** , **Broken White Line** and **Solid Yellow Line**.

   - Click **Show All** to display all lane lines.
   - Click on a lane, such as **Lane 1**, to display the corresponding lane lines.
   - Click **Flip** to flip the direction of the lane lines.

Step 7 Click **Calibration Area** in the **Advanced**, and then configure the calibration.

Calibration is used to measure speed in speed detection events. In the live video of the channel, draw a quadrilateral that corresponds to a rectangular area in the actual scene. Set the length of the rectangle, detect the time it takes for a vehicle to pass through, and then calculate the vehicle's speed.

Figure 5-14 Configure the calibration area



1. Click to draw the calibration area as needed in the video image.

   Move the mouse to the starting position of the calibration area on the left side of the screen and click to begin drawing. During the drawing process, left click again, and then the system will automatically close the area to complete the drawing.

Supports mouse drag to edit calibration areas. Click to delete the corresponding calibration areas.

2. Enter the actual length and width of the corresponding area in the real-world environment for the quadrilateral.

The length and width entered must match the actual dimensions in the real-world environment. Otherwise, it will affect the accuracy of the speed measurement.

3. Click **Calibration Verification** to draw the verification line.

After the verification line is drawn, the actual ground length value calculated by the algorithm will be displayed next to it. Please verify whether this value matches the actual ground length.

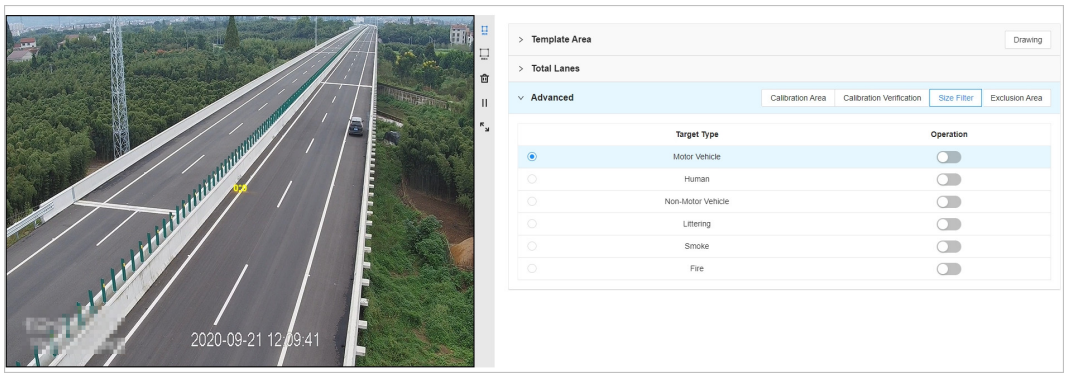
You need to configure the rules before you can perform the calibration verification.

The verification line should be drawn vertically, preferably along the center white line of the road. Compare the length value calculated by the algorithm with the actual length of the white line on the ground to ensure the accuracy of the calibrated area's length.

Step 8 Configure the size filter.

Draw two target boxes, one large and one small. An alarm will only be triggered when the size of the target falls between the two boxes according to the triggering rules.

Figure 5-15 Configure size filter



1. Click **Size Filter**.
2. Select types of targets, including **Motor Vehicle** , **Human**, **Non-Motor Vehicle**, **Littering**, **Smoke** and **Fire**.
3. Click to draw a small box and click to draw a big box.
4. Adjust the size of the filter box at any position on the screen.

When the target is larger than the big box or smaller than the small box, no alarm will be triggered.

Repeat the above steps to draw filtering boxes for multiple types of targets.

Step 9 Click **Exclusion Area**, and then click to draw the exclusion area.

Supports mouse drag to edit the exclusion area. Click  to delete the corresponding exclusion area.

- Only exclusion areas can be drawn within the template area.
- At most, ten exclusion areas can be drawn.
- Expand the detection area as needed to include large vehicle targets.
- To avoid errors, we do not recommend including distant or curved areas in the detection range.

Step 10 Click **OK**.

When you save the configuration, it is necessary to verify that the lane line has been drawn. Otherwise, the page will prompt 'The lane lines for global configuration are not drawn'.

5.5.2 Parking Detection

An alarm will be triggered when the duration of a vehicle parking on the expressway exceeds the defined value. When a traffic jam occurs or vehicles move slowly, parking alarm will not be triggered.

Procedure

Step 1 Log in to the PC client.

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

You can also click **Event** from the configuration list on the home page.

Step 3 Select the remote device in the left-hand side device tree.

Step 4 Select **Smart Plan** > **Traffic Event Detection**, and then click  on the right side of the **Enable**.

Step 5 Click **Add Template Rule** , and then select **Parking Detection**.

You can quickly search for rule types through search. It supports adding multiple rules.

When you add multiple rules, click **Expand All** to open all rule panels and click **Show Less** to close all rule panels.

Step 6 Select the area.

Supports selecting multiple areas.

- Click  to pause screen. Click  to play it.
- Click  to enter the full screen.

Step 7 Configure parameters.

Figure 5-16 Parking detection

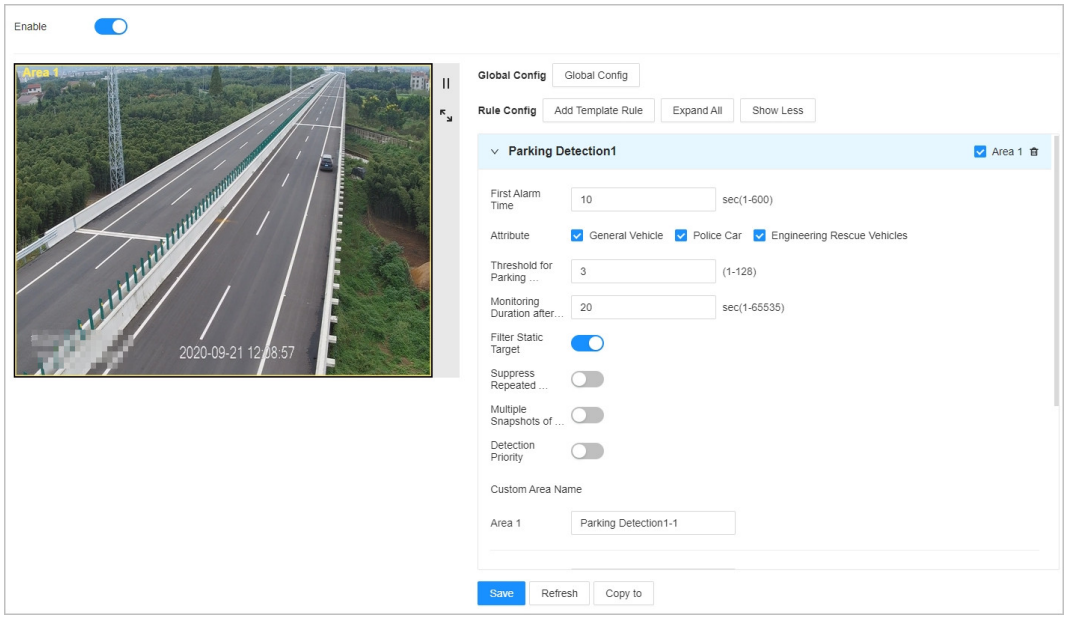


Table 5-2 Description of parking detection parameters

Parameter	Description
First Alarm Time	An alarm will be triggered when a pedestrian appears in the detection zone and stays longer than the defined time.
Attribute	You can select **General Vehicle** , **Police Car** or **Engineering Rescue Vehicles** from the list.
Threshold for Parking Vehicles Detection	Mainly used to control the number of alarm targets for parking in congested situations. If the number exceeds the set value, the parking event will not be reported.
Monitoring Duration after Target Disappears	The event ends when the disappearing duration of the object reaches the defined time.
Filter Static Target	Enable this feature to only capture vehicles with motion; Disable this feature to capture both moving and stationary targets.
Suppress Repeated Alarms	Enable this feature can reduce repetitive alarms for the same target. It is recommended to enable it.
Multiple Snapshots of Parking Vehicles	Enable this function, if the same target parks multiple times in the same vehicle regulation area, it will be captured multiple times; Disable this function, if the same target parks multiple times in the same vehicle regulation area, it will only be captured once.
Detection Priority	When the same vehicle is obscured in the frame and then reappears, 2 IDs will be generated for it. If detection priority is not enabled, the system will not consider the vehicle that reappears after being obscured as a new target, and might not trigger an alarm. If detection priority is enabled, the system will consider the vehicle that reappears after being obscured as a new target and generate an alarm to reduce missed alarms.
Custom Area Name	Set the names of events reported for each area.

Step 8 Click the dropdown menu for **Schedule**, and then select time schedule.

The system will only trigger a linkage alarm event when an alarm is triggered within the set arming time range.

If the added schedule does not meet the actual requirements, you can click **+ Add** to add a new schedule.

Step 9 Click **+ Select** on the right side of **Event Linkage**. Select the alarm linkage type (such as record, picture storage, etc.) and configure the parameters.

Supports linkage for both local and remote alarm linkage items.

Step 10 Click **Save**.

5.5.3 Pedestrian Detection

Set the alarm rules for pedestrian detection.

Procedure

Step 1 Log in to the PC client.

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

You can also click **Event** from the configuration list on the home page.

Step 3 Select the remote device in the left-hand side device tree.

Step 4 Select **Smart Plan** > **Traffic Event Detection**, and then click on the right side of the **Enable**.

Step 5 Click **Add Template Rule** , and then select **Pedestrian Detection**.

You can quickly search for rule types through search. It supports adding multiple rules.

When you add multiple rules, click **Expand All** to open all rule panels and click **Show Less** to close all rule panels.

Step 6 Draw the detection area.

- Click to draw the detection area.

  The detection area should cover the valid vehicle targets, and avoid being too large to be interfered from other objects.

- Click to delete the detection area.
- Click to pause screen.
- Click to enter the full screen.

Step 7 Configure parameters.

Figure 5-17 Pedestrian detection

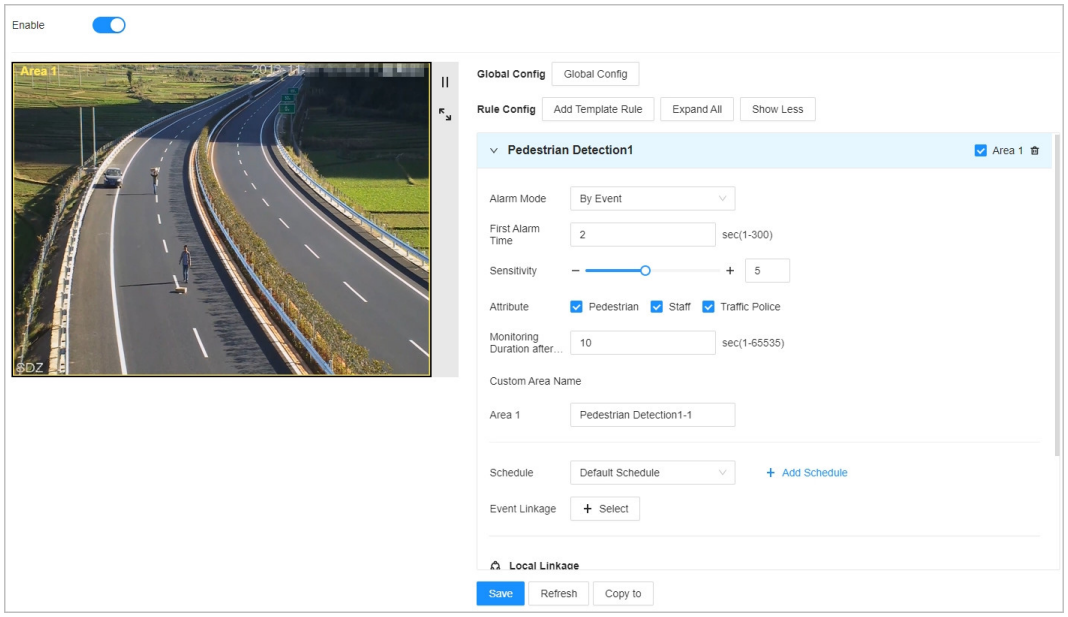


Table 5-3 Description of pedestrian detection parameters

Parameter	Description
Alarm Mode	You can select **By Event** or **By Target** from the drop down list as the alarm type. • **By Event** : There are valid targets in the scene, and if the alarm conditions are met, they will be reported. An alarm contains multiple valid targets that have been detected. The report is sent when the number of valid targets in the detection area increases, and it is not sent when the number decreases. • **By Target** : Report when a single target meets the alarm condition.
First Alarm Time	An alarm will be triggered when a pedestrian appears in the detection zone and stays longer than the defined time.
Sensitivity	Set the range from 1 to 10, where a higher value indicates a more sensitive detection but also a higher false positive rate.
Attribute	You can select **Pedestrian** , **Staff** or **Traffic Police** from the list.
Monitoring Duration after Target Disappears	The event ends when the disappearing duration of the object reaches the defined time.
Custom Area Name	Set the names of events reported for each area.

Step 8 Click the dropdown menu for **Schedule**, and then select time schedule.

The system will only trigger a linkage alarm event when an alarm is triggered within the set arming time range.

If the added schedule does not meet the actual requirements, you can click **+ Add** to add a new schedule.

Step 9 Click **+ Select** on the right side of **Event Linkage**. Select the alarm linkage type (such as record and picture storage) and configure the parameters.

Supports linkage for both local and remote alarm linkage items.

Step 10 Click **Save**.

5.5.4 Non-motor Vehicle Detection

An alarm will be triggered when non-motor vehicles, such as electric mopeds and trishaws, are driving in vehicle lane for longer than the defined value.

Procedure

Step 1 Log in to the PC client.

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

You can also click **Event** from the configuration list on the home page.

Step 3 Select the remote device in the left-hand side device tree.

Step 4 Select **Smart Plan** > **Traffic Event Detection**, and then click on the right side of the **Enable**.

Step 5 Click **Add Template Rule** , and then select **Non-motor Vehicle Detection**.

You can quickly search for rule types through search. It supports adding multiple rules.

When you add multiple rules, click **Expand All** to open all rule panels and click **Show Less** to close all rule panels.

Step 6 Select the area.

Supports selecting multiple areas.

- Click to pause screen. Click to play it.
- Click to enter the full screen.

Step 7 Configure parameters.

Figure 5-18 Non-motor vehicle detection

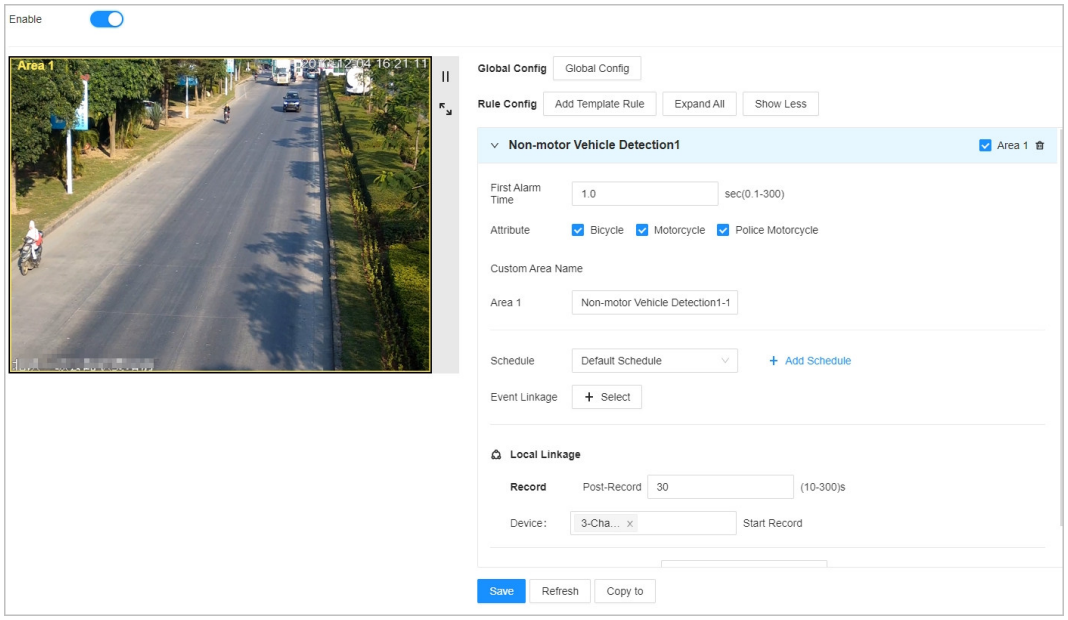


Table 5-4 Description of non-motor vehicle detection parameters

Parameter	Description
First Alarm Time	An alarm will be triggered when the time for non-motor vehicles to appear in the scene exceeds the scheduled interval.
Attribute	Select the type of the non-motor vehicle.
Custom Area Name	Set the names of events reported for each area.

Step 8 Click the dropdown menu for **Schedule**, and then select time schedule.

The system will only trigger a linkage alarm event when an alarm is triggered within the set arming time range.

If the added schedule does not meet the actual requirements, you can click **+ Add** to add a new schedule.

Step 9 Click **+ Select** on the right side of **Event Linkage**. Select the alarm linkage type (such as record, picture storage, etc.) and configure the parameters.

Supports linkage for both local and remote alarm linkage items.

Step 10 Click **Save**.

5.5.5 Wrong-way Driving Detection

When a vehicle is detected to be driving in the wrong direction, an alarm will be triggered.

Procedure

Step 1 Log in to the PC client.

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

You can also click **Event** from the configuration list on the home page.

Step 3 Select the remote device in the left-hand side device tree.

Step 4 Select **Smart Plan** > **Traffic Event Detection**, and then click on the right side of the **Enable**.

Step 5 Click **Add Template Rule** , and then select **Wrong-way Driving Detection**.

You can quickly search for rule types through search. It supports adding multiple rules.

When you add multiple rules, click **Expand All** to open all rule panels and click **Show Less** to close all rule panels.

Step 6 Select the area.

Supports selecting multiple areas.

- Click to pause screen. Click to play it.
- Click to enter the full screen.

Step 7 Configure parameters.

Figure 5-19 Wrong-way driving detection

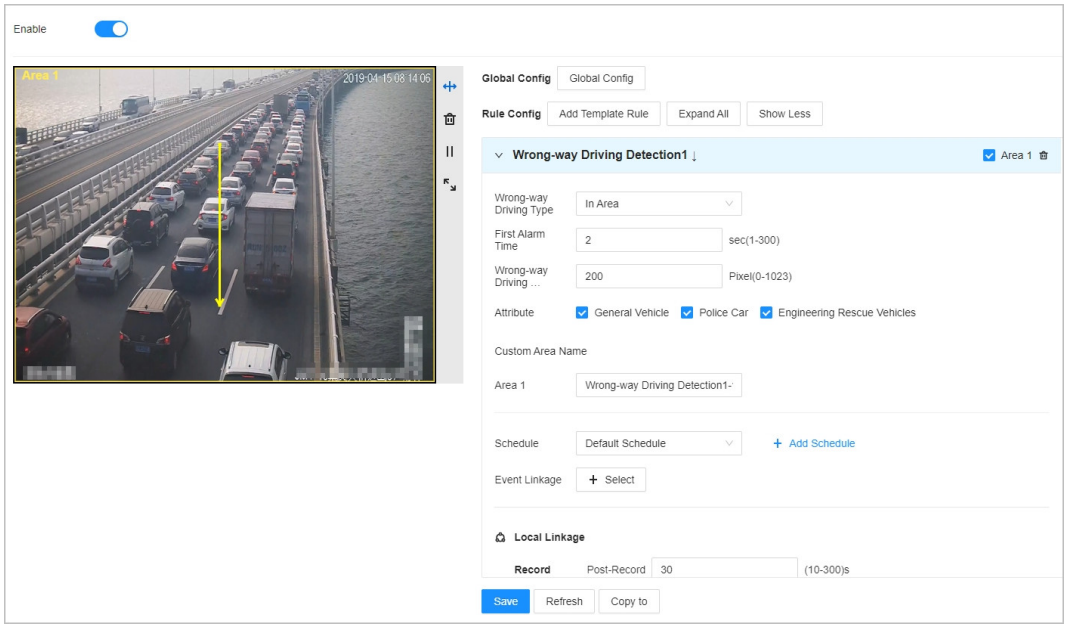


Table 5-5 Description of wrong-way driving detection parameters

Parameter	Description
Wrong-way Driving Type	Select **In Area** or **In Lane**. When detecting wrong-way driving, it is necessary to draw the detection region and direction lines.
First Alarm Time	An alarm will be triggered when the wrong-way driving target time exceeds the defined time.
Wrong-way Driving Distance	An alarm will be triggered when the target in the frame exceeds the set pixel value for wrong-way driving distance.
Attribute	Select the target types, including **General Vehicle** , **Police Car** and **Engineering Rescue Vehicles**. An alarm will be triggered when a specified target type is detected.
Custom Area Name	Set the names of events reported for each area.

Step 8 Click the dropdown menu for **Schedule**, and then select time schedule.

The system will only trigger a linkage alarm event when an alarm is triggered within the set arming time range.

If the added schedule does not meet the actual requirements, you can click **+ Add** to add a new schedule.

Step 9 Click **+ Select** on the right side of **Event Linkage**. Select the alarm linkage type (such as record and picture storage) and configure the parameters.

Supports linkage for both local and remote alarm linkage items.

Step 10 Click **Save**.

5.5.6 Illegal Backing Detection

When a vehicle is backing and the backing time exceeds the defined value, an alarm will be triggered. For example, a vehicle is backing on the highway.

Procedure

Step 1 Log in to the PC client.

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

You can also click **Event** from the configuration list on the home page.

Step 3 Select the remote device in the left-hand side device tree.

Step 4 Select **Smart Plan** > **Traffic Event Detection**, and then click on the right side of the **Enable**.

Step 5 Click **Add Template Rule** , and then select **Illegal Backing Detection**.

You can quickly search for rule types through search. It supports adding multiple rules.

When you add multiple rules, click **Expand All** to open all rule panels and click **Show Less** to close all rule panels.

Step 6 Select the area.

Supports selecting multiple areas.

- Click to pause screen. Click to play it.
- Click to enter the full screen.

Step 7 Configure parameters.

Figure 5-20 Illegal backing detection

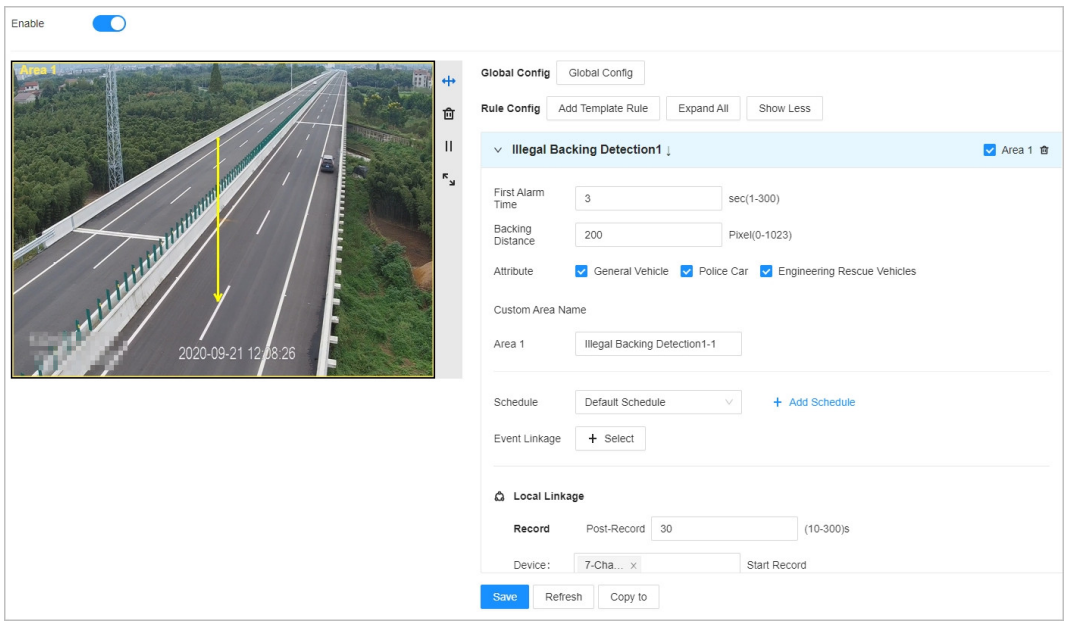


Table 5-6 Description of Illegal backing detection parameters

Parameter	Description
First Alarm Time	An alarm will be triggered when the reverse time longer than the defined time.
Backing Distance	Trigger an alarm when the distance of the reverse movement in the frame exceeds the set pixel value.
Attribute	Select the target types, including **General Vehicle** , **Police Car** and **Engineering Rescue Vehicles**. An alarm will be triggered when a specified target type is detected.
Custom Area Name	Set the names of events reported for each area.

Step 8 Click the dropdown menu for **Schedule**, and then select time schedule.

The system will only trigger a linkage alarm event when an alarm is triggered within the set arming time range.

If the added schedule does not meet the actual requirements, you can click **+ Add** to add a new schedule.

Step 9 Click **+ Select** on the right side of **Event Linkage**. Select the alarm linkage type (such as record, picture storage, etc.) and configure the parameters.

Supports linkage for both local and remote alarm linkage items.

Step 10 Click **Save**.

5.5.7 Traffic Congestion Detection

An alarm will be triggered when the number of parked vehicles on the lane and the lane occupancy ratio exceed the set threshold.

Procedure

Step 1 Log in to the PC client.

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

You can also click **Event** from the configuration list on the home page.

Step 3 Select the remote device in the left-hand side device tree.

Step 4 Select **Smart Plan** > **Traffic Event Detection**, and then click on the right side of the **Enable**.

Step 5 Click **Add Template Rule** , and then select **Traffic Congestion Detection**.

You can quickly search for rule types through search. It supports adding multiple rules.

When you add multiple rules, click **Expand All** to open all rule panels and click **Show Less** to close all rule panels.

Step 6 Select the area.

Supports selecting multiple areas.

- Click to pause screen. Click to play it.

- Click  to enter the full screen.

Step 7 Configure parameters.

Figure 5-21 Traffic congestion detection

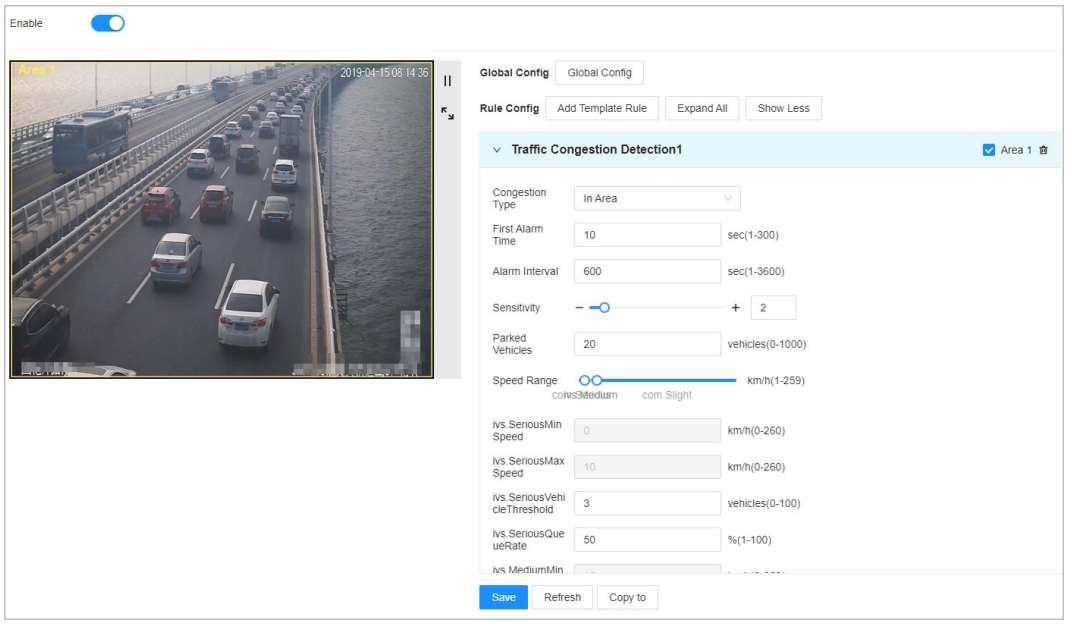


Table 5-7 Description of traffic congestion detection parameters

Parameter	Description
Congestion Type	Select **In Area** or **In Lane** based on the actual situation.
Alarm Interval	Used to prevent multiple reports of the same congestion event within a short period of time, if congestion persists within the alarm interval, only one alarm message will be reported.
First Alarm Time	An alarm will be triggered when roadblock appears in the detection zone and stays longer than the defined time.
Parked Vehicles	One of the conditions for determining congestion is when the number of parked vehicles in the area exceeds the set value, triggering an alarm.
Sensitivity	Set the range from 1 to 10, where a higher value indicates a more sensitive detection but also a higher false positive rate.

Parameter	Description
Congestion Threshold	The ratio of the queue length to the lane length during an alarm is used as a criterion to determine congestion. If the ratio exceeds the set threshold, it indicates congestion. An alarm will be triggered when both congestion condition one and congestion condition two are met. • Congestion Condition One: The ratio of the vehicle queue length to the detected lane length exceeds the occupancy threshold. Specifically, the vehicle queue length divided by the detected lane length is greater than the occupancy threshold. The detected lane length is a fixed value and is independent of the marked length in the video frame. • Congestion Condition Two: The speed of slow-moving vehicles approaches a standstill. Specifically, the number of slow-moving vehicles in the lane is greater than the occupancy threshold divided by 10. Considering the effectiveness of congestion detection and the interference from parking events, we recommend setting the occupancy threshold at 50%.
Discontinuous Time Threshold	The time difference between the last recorded congestion time and the current congestion time is defined as the clear time. If the clear time exceeds the specified time threshold, the situation is not considered congestion, and the alarm count is reset.
Crowd Level	Enable the congestion level classification and configure the thresholds for speed, vehicle count, and queue length corresponding to the three levels: Serious, medium and slight, to determine the congestion level. • Adjust the speed thresholds corresponding to the three levels through the **Speed Range**. • Configuration is supported only when the congestion type is lane congestion.
Speed Range	
ivs.SeriousMin Speed	
ivs.SeriousMax Speed	
ivs.SeriousVehicle Threshold	
ivs.SeriousQueueRate	
ivs.MediumMin Speed	
ivs.MediumMax Speed	
ivs.MediumVehicle Threshold	
ivs.MediumQueueRate	
ivs.SlightMinSpeed	
ivs.SlightMaxSpeed	
ivs.SlightMaxVehicle Threshold	
ivs.SlightMaxQueueRate	
Custom Area Name	Set the names of events reported for each area.

Step 8 Click the dropdown menu for **Schedule**, and then select time schedule.

The system will only trigger a linkage alarm event when an alarm is triggered within the set arming time range.

If the added schedule does not meet the actual requirements, you can click **+ Add** to add a new schedule.

Step 9 Click **+ Select** on the right side of **Event Linkage**. Select the alarm linkage type (such as record, picture storage, etc.) and configure the parameters.

Supports linkage for both local and remote alarm linkage items.

Step 10 Click **Save**.

5.5.8 Traffic Accident Detection

An alarm will be triggered when vehicles crash and the event lasts longer than the defined value.

Procedure

Step 1 Log in to the PC client.

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

You can also click **Event** from the configuration list on the home page.

Step 3 Select the remote device in the left-hand side device tree.

Step 4 Select **Smart Plan** > **Traffic Event Detection**, and then click  on the right side of the **Enable**.

Step 5 Click **Add Template Rule** , and then select **Traffic Accident Detection**.

You can quickly search for rule types through search. It supports adding multiple rules.

When you add multiple rules, click **Expand All** to open all rule panels and click **Show Less** to close all rule panels.

Step 6 Select the area.

Supports selecting multiple areas.

- Click  to pause screen. Click  to play it.
- Click  to enter the full screen.

Step 7 Configure parameters.

Figure 5-22 Traffic accident detection

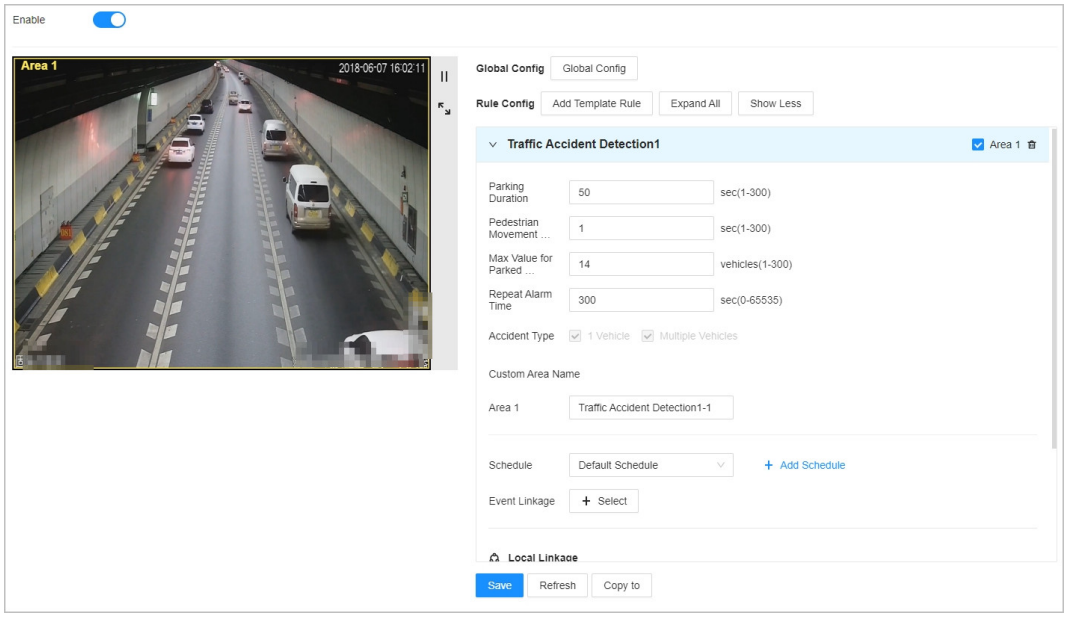


Table 5-8 Description of traffic accident detection parameters

Parameter	Description
Repeat Alarm Time	After the first alarm is triggered, if the same event stays within the detection region for a duration longer than the set interval, an alarm will be triggered.
Parking Duration	When the stationary time of the accident vehicle reaches the set parking time value, and the pedestrian time in the detection area reaches the set pedestrian time value, the accident detection alarm is triggered.
Pedestrian Movement Duration	
Max Value for Parked Vehicles Detection	The number of stationary vehicles in congested state. Threshold is used to prevent false alarms caused by congested parking. When the number of stationary vehicles in the detection area is greater than this value, it is not considered an accident.
Custom Area Name	Set the names of events reported for each area.

Step 8 Click the dropdown menu for **Schedule**, and then select time schedule.

The system will only trigger a linkage alarm event when an alarm is triggered within the set arming time range.

If the added schedule does not meet the actual requirements, you can click **+ Add** to add a new schedule.

Step 9 Click **+ Select** on the right side of **Event Linkage**. Select the alarm linkage type (such as record, picture storage, etc.) and configure the parameters.

Supports linkage for both local and remote alarm linkage items.

Step 10 Click **Save**.

5.5.9 Construction Detection

When a construction sign is detected and it stays longer than the defined value, the road section is identified as a construction zone and an alarm will be triggered.

Procedure

Step 1 Log in to the PC client.

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

You can also click **Event** from the configuration list on the home page.

Step 3 Select the remote device in the left-hand side device tree.

Step 4 Select **Smart Plan** > **Traffic Event Detection**, and then click on the right side of the **Enable**.

Step 5 Click **Add Template Rule** , and then select **Construction Detection**.

You can quickly search for rule types through search. It supports adding multiple rules.

When you add multiple rules, click **Expand All** to open all rule panels and click **Show Less** to close all rule panels.

Step 6 Select the area.

Supports selecting multiple areas.

- Click to pause screen. Click to play it.
- Click to enter the full screen.

Step 7 Configure parameters.

Figure 5-23 Construction detection

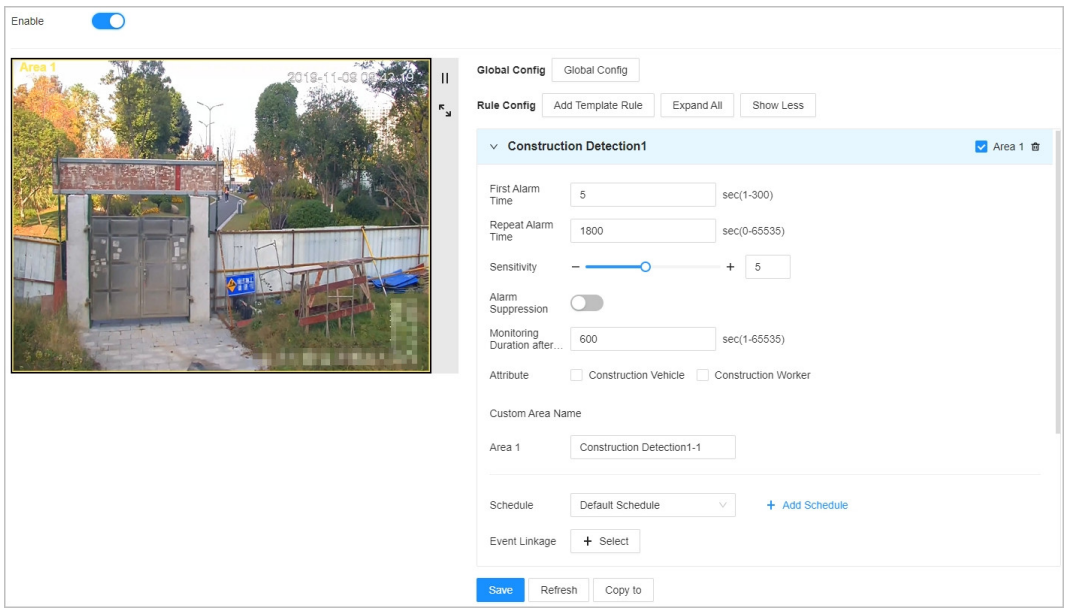


Table 5-9 Description of construction detection parameters

Parameter	Description
First Alarm Time	An alarm will be triggered when construction sign appears in the detection zone and stays longer than the defined time.
Repeat Alarm Time	If construction sign persists within the scheduled interval, only one alarm message will be reported. This is to prevent multiple alarm reports for the same construction sign occurrence within a short period of time. Event removed, there will be 3 alarm images in the alarm details, including the image at the first alarm, the image when the repeat alarm time interval is met, and the image at the time of removal.
Sensitivity	Set the range from 1 to 10, where a higher value indicates a more sensitive detection but also a higher false positive rate.
Monitoring Duration after Target Disappears	The event ends when the disappearing duration of the object reaches the defined time.
Alarm Suppression	Click to enable alarm suppression to avoid duplicate alarms. Only when alarm suppression is shut down, duplicate alarms will be considered valid.
Custom Area Name	Set the names of events reported for each area.

Step 8 Click the dropdown menu for **Schedule**, and then select time schedule.

The system will only trigger a linkage alarm event when an alarm is triggered within the set arming time range.

If the added schedule does not meet the actual requirements, you can click **+ Add** to add a new schedule.

Step 9 Click **+ Select** on the right side of **Event Linkage**. Select the alarm linkage type (such as record, picture storage, etc.) and configure the parameters.

Supports linkage for both local and remote alarm linkage items.

Step 10 Click **Save**.

5.5.10 Road Debris Detection

When the detection region detects objects left behind by vehicles or pedestrians, and the duration exceeds the set value, an alarm will be triggered.

Procedure

Step 1 Log in to the PC client.

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

You can also click **Event** from the configuration list on the home page.

Step 3 Select the remote device in the left-hand side device tree.

Step 4 Select **Smart Plan** > **Road Debris Detection**, and then click on the right side of the **Enable**.

Step 5 Click **Add Template Rule** , and then select **Road Debris Detection**.

You can quickly search for rule types through search. It supports adding multiple rules.

When you add multiple rules, click **Expand All** to open all rule panels and click **Show Less** to close all rule panels.

Step 6 Select the area.

Supports selecting multiple areas.

- Click to pause screen. Click to play it.
- Click to enter the full screen.

Step 7 Configure parameters.

Figure 5-24 Smoke detection

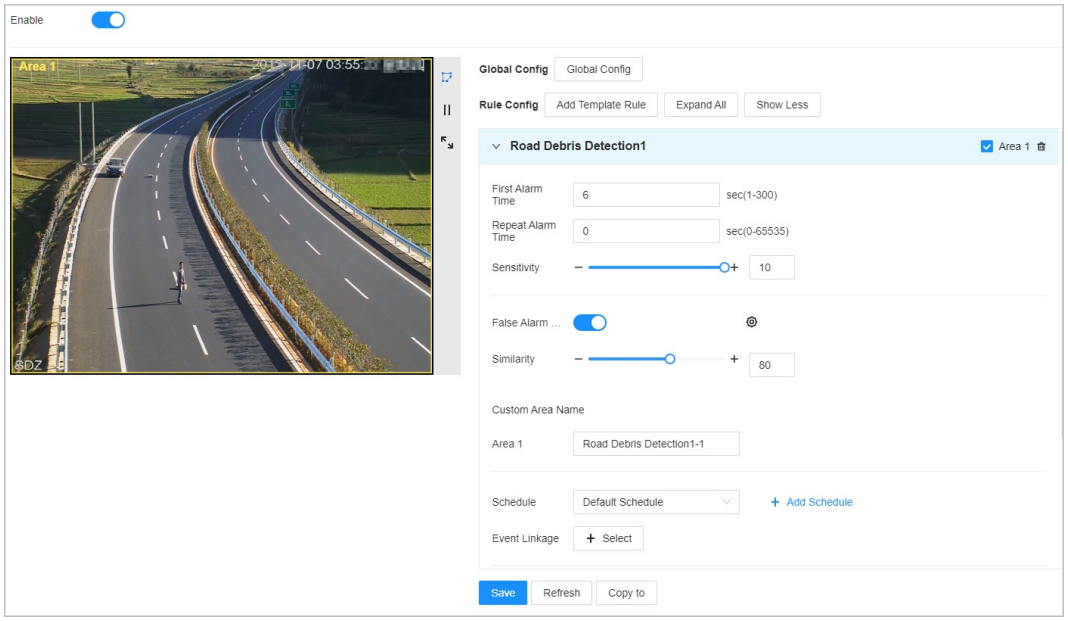


Table 5-10 Description of smoke detection parameters

Parameter	Description
First Alarm Time	An alarm will be triggered when the littering in the detection region exceeds the set value.
Repeat Alarm Time	Enable repetitive alarms and set the repetition time. When the littering continues to appear and exceeds the repetition time, the alarm information will be reported again.
Sensitivity	Set the range from 1 to 10, where a higher value indicates a more sensitive detection but also a higher false positive rate.

Parameter	Description
False Alarm Filter	Click on the right side of the false alarm filter and set the similarity threshold to enable the false alarm filtering function. The system will compare the detected debris with images in the false alarm experience database. If the similarity meets the set threshold, it will be judged as a false alarm and will not be reported as an alert event. • Click or select **File Management** > **Experience Database Config** > **False Alarm Experience Database** to configure the false alarm experience database. • Manual creation of the false alarm experience database is not supported. When no images are added to the database, the false alarm experience database remains empty. • After enabling false alarm filtering, remote devices will be automatically added to the associated channel list of the false alarm experience database.
Similarity	
Custom Area Name	Set the names of events reported for each area.

Step 8 (Optional) Click on the right side of the **False Alarm Filter** and set similarity to enable the false alarm filter function.

The system compares the detected debris with the images in the false alarm experience library. If the similarity meets the set threshold, it is considered a false alarm and will not be reported as an alarm event.

- Click to configure the false alarm experience database.
- It is not possible to manually create a false alarm experience database. When no image is added to the knowledge base, the false alarm experience database is empty.
- When false alarm filter is enabled, the remote device will automatically be added to the linked channel in the false alarm experience database.

Step 9 Click the dropdown menu for **Schedule**, and then select time schedule.

The system will only trigger a linkage alarm event when an alarm is triggered within the set arming time range.

If the added schedule does not meet the actual requirements, you can click **+ Add** to add a new schedule.

Step 10 Click **+ Select** on the right side of **Event Linkage**. Select the alarm linkage type (such as record, picture storage, etc.) and configure the parameters.

Supports linkage for both local and remote alarm linkage items.

Step 11 Click **Save**.

Related Operations

False alarm experience database operations are as follows.

- Modeling: Select one or multiple photos, or click **Select All** to choose all photos. Click **Model** to obtain features again.

When the false alarm filter function is not available, it is necessary to extract the feature again, otherwise the features might become ineffective.

- Clear: Select one or multiple photos, or click **Select All** to choose all photos. Click **Clear** to delete photos.

5.5.11 Driving in Emergency Lane

An alarm will be triggered when a vehicle occupies the emergency lane.

Procedure

Step 1 Log in to the PC client.

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

You can also click **Event** from the configuration list on the home page.

Step 3 Select the remote device in the left-hand side device tree.

Step 4 Select **Smart Plan** > **Traffic Event Detection**, and then click on the right side of the **Enable**.

Step 5 Click **Add Template Rule** , and then select **Driving in Emergency Line**.

You can quickly search for rule types through search. It supports adding multiple rules.

When you add multiple rules, click **Expand All** to open all rule panels and click **Show Less** to close all rule panels.

Step 6 Select the area.

Supports selecting multiple areas.

- Click  to pause screen. Click  to play it.
- Click  to enter the full screen.

Step 7 Configure parameters.

Figure 5-25 Emergency lane occupation detection

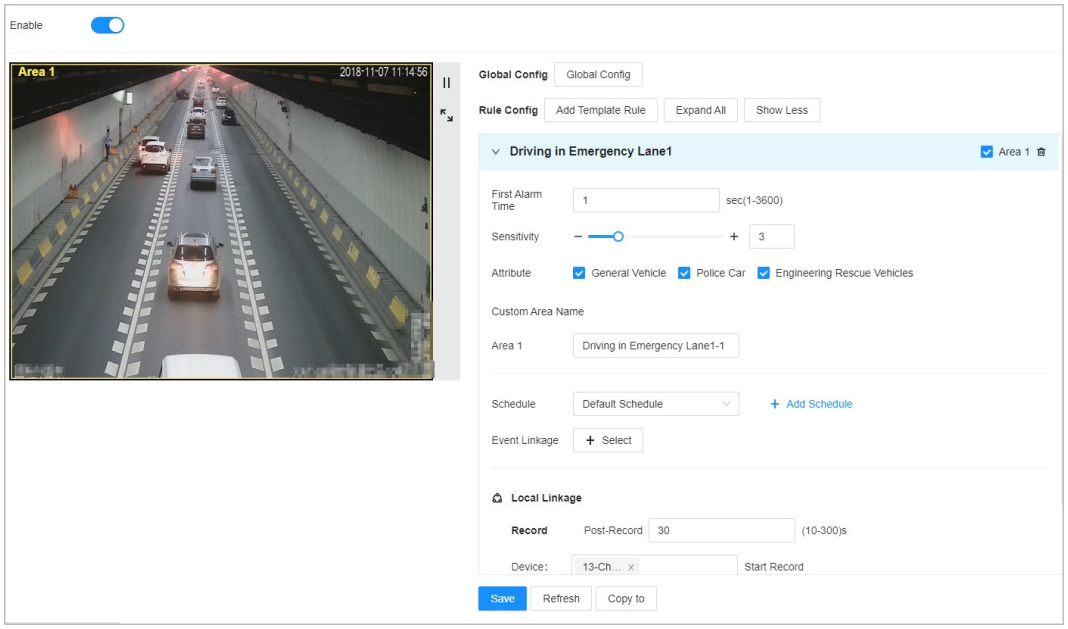


Table 5-11 Description of emergency lane occupation detection parameters

Parameter	Description
First Alarm Time	An alarm will be triggered when a motor vehicle appears in the detection zone and stays longer than the defined time.
Sensitivity	Set the range from 1 to 10, where a higher value indicates a more sensitive detection but also a higher false positive rate.
Attribute	Select the vehicle type, including **General Vehicle** , **Police Car** and **Engineering Rescue Vehicles**. When a target of the specified type is detected, an alarm will be triggered.
Custom Area Name	Set the names of events reported for each area.

Step 8 Click the dropdown menu for **Schedule**, and then select time schedule.

The system will only trigger a linkage alarm event when an alarm is triggered within the set arming time range.

If the added schedule does not meet the actual requirements, you can click **+ Add** to add a new schedule.

Step 9 Click **+ Select** on the right side of **Event Linkage**. Select the alarm linkage type (such as record, picture storage, etc.) and configure the parameters.

Supports linkage for both local and remote alarm linkage items.

Step 10 Click **Save**.

5.5.12 Roadblock Detection

An alarm will be triggered when a barrier, such as a box, stays in the detection area for longer than the defined value.

Procedure

Step 1 Log in to the PC client.

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

You can also click **Event** from the configuration list on the home page.

Step 3 Select the remote device in the left-hand side device tree.

Step 4 Select **Smart Plan** > **Traffic Event Detection**, and then click on the right side of the **Enable**.

Step 5 Click **Add Template Rule** , and then select **Roadblock Detection**.

You can quickly search for rule types through search. It supports adding multiple rules.

When you add multiple rules, click **Expand All** to open all rule panels and click **Show Less** to close all rule panels.

Step 6 Select the area.

Supports selecting multiple areas.

- Click to pause screen. Click to play it.
- Click to enter the full screen.

Step 7 Configure parameters.

Figure 5-26 Roadblock detection

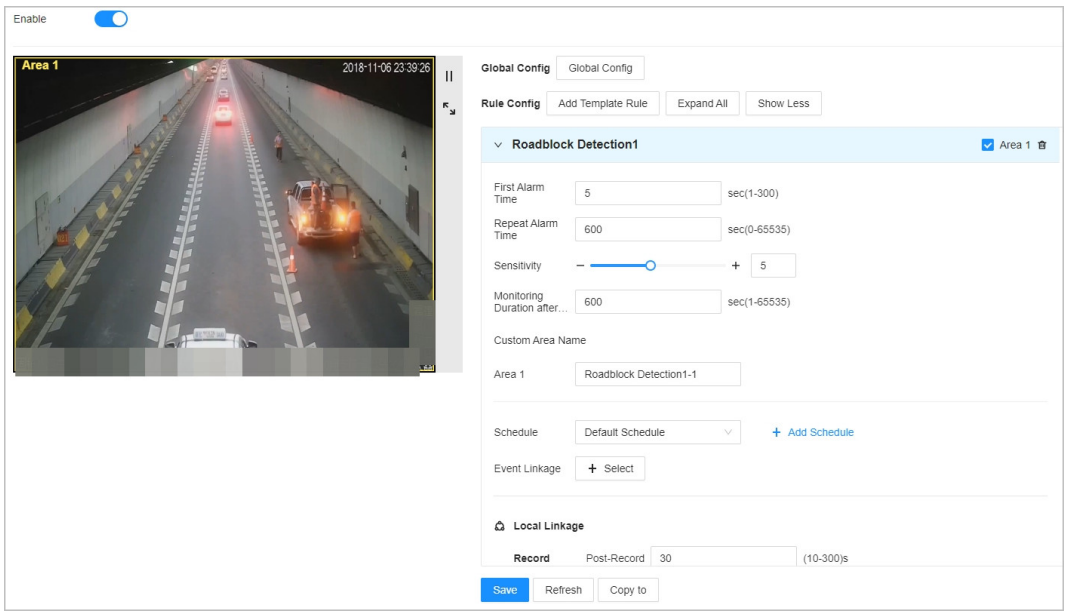


Table 5-12 Description of roadblock detection parameters

Parameter	Description
First Alarm Time	An alarm will be triggered when roadblock appears in the detection zone and stays longer than the defined time.
Repeat Alarm Time	If roadblock persists within the scheduled interval, only one alarm message will be reported. This is to prevent multiple alarm reports for the same roadblock occurrence within a short period of time. Event removed, there will be 3 alarm images in the alarm details, including the image at the first alarm, the image when the repeat alarm time interval is met, and the image at the time of removal.
Sensitivity	Set the range from 1 to 10, where a higher value indicates a more sensitive detection but also a higher false positive rate.
Monitoring Duration after Target Disappears	The event ends when the disappearing duration of the object reaches the defined time.
Custom Area Name	Set the names of events reported for each area.

Step 8 Click the dropdown menu for **Schedule**, and then select time schedule.

The system will only trigger a linkage alarm event when an alarm is triggered within the set arming time range.

If the added schedule does not meet the actual requirements, you can click **+ Add** to add a new schedule.

Step 9 Click **+ Select** on the right side of **Event Linkage**. Select the alarm linkage type (such as record, picture storage, etc.) and configure the parameters.

Supports linkage for both local and remote alarm linkage items.

Step 10 Click **Save**.

5.5.13 Traffic Flow Statistics

Statistics on the number of vehicles passing through a road section within a specified time.

Procedure

Step 1 Log in to the PC client.

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

You can also click **Event** from the configuration list on the home page.

Step 3 Select the remote device in the left-hand side device tree.

Step 4 Select **Smart Plan** > **Traffic Event Detection**, and then click on the right side of the **Enable**.

Step 5 Click **Add Template Rule** , and then select **Traffic Flow Statistics**.

You can quickly search for rule types through search. It supports adding multiple rules.

When you add multiple rules, click **Expand All** to open all rule panels and click **Show Less** to close all rule panels.

Step 6 Select the area.

Supports selecting multiple areas.

- Click  to pause screen. Click  to play it.
- Click  to enter the full screen.

Step 7 Configure parameters.

Figure 5-27 Traffic flow statistics

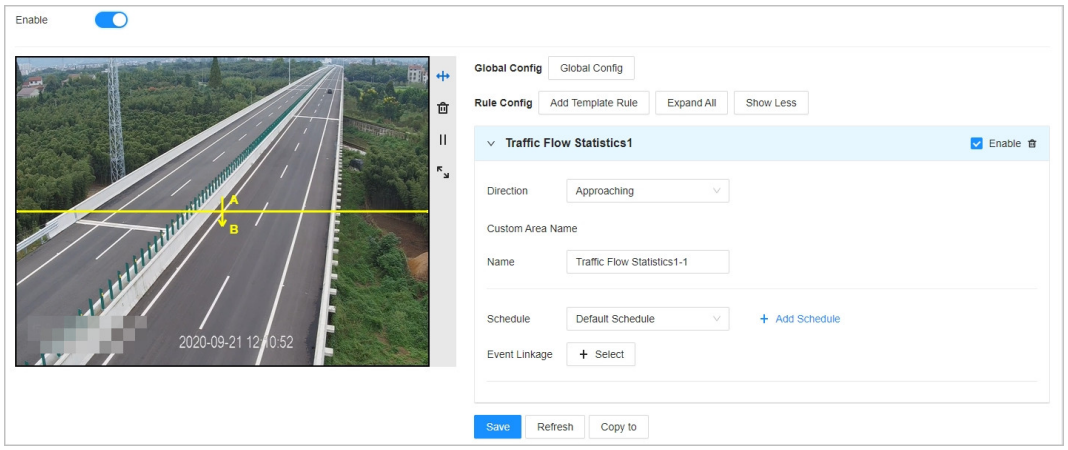


Table 5-13 Description of traffic flow statistics parameters

Parameter	Description
Direction	• Bidirectional: The direction of traffic flow is not specified. Lane numbers need to be configured. • Approaching: The far end of the video is the starting point, and the near end of the video is the ending point. • Departing: The near end of the video is the starting point, and the far end of the video is the ending point.
Custom Area Name	Set the names of events reported for each area.

Step 8 Click the dropdown menu for **Schedule**, and then select time schedule.

The system will only trigger a linkage alarm event when an alarm is triggered within the set arming time range.

If the added schedule does not meet the actual requirements, you can click **+ Add** to add a new schedule.

Step 9 Click **+ Select** on the right side of **Event Linkage**. Select the alarm linkage type (such as record, picture storage, etc.) and configure the parameters.

Supports linkage for both local and remote alarm linkage items.

Step 10 Click **Save**.

5.5.14 Hazardous Material Transport Vehicle Detection

An alarm will be triggered when a hazardous material transport vehicle crosses the inspection line.

Procedure

Step 1 Log in to the PC client.

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

You can also click **Event** from the configuration list on the home page.

Step 3 Select the remote device in the left-hand side device tree.

Step 4 Select **Smart Plan** > **Traffic Event Detection**, and then click on the right side of the **Enable**.

Step 5 Click **Add Template Rule** , and then select **Hazardous Material Transport Vehicle Detection**.

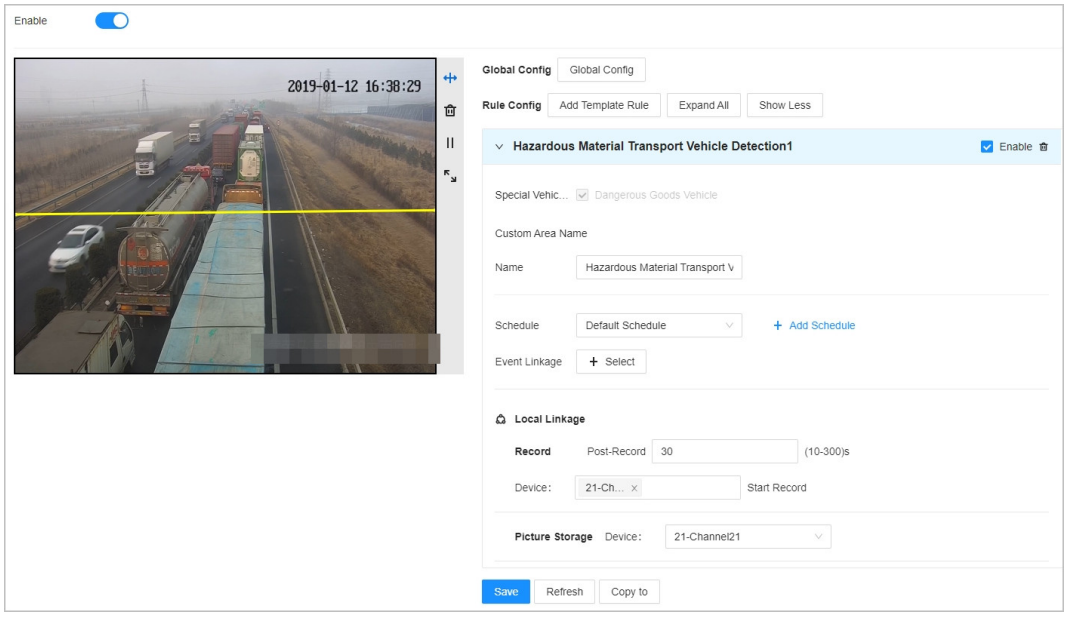
You can quickly search for rule types through search. It supports adding multiple rules.

When you add multiple rules, click **Expand All** to open all rule panels and click **Show Less** to close all rule panels.

Step 6 Click **Enable** on the right side of the detection rule, and then set the reporting name.

- Click to draw the detection line.
- Click to pause screen. Click to play it.
- Click to enter the full screen.

Figure 5-28 Hazardous material transport vehicle detection



Step 7 Click the dropdown menu for **Schedule**, and then select time schedule.

The system will only trigger a linkage alarm event when an alarm is triggered within the set arming time range.

If the added schedule does not meet the actual requirements, you can click **+ Add** to add a new schedule.

Step 8 Click **+ Select** on the right side of **Event Linkage**. Select the alarm linkage type (such as record, picture storage, etc.) and configure the parameters.

Supports linkage for both local and remote alarm linkage items.

Step 9 Click **Save**.

5.5.15 Truck Entered Prohibited Area

An alarm will be triggered when a truck enters the detection area.

Procedure

Step 1 Log in to the PC client.

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

You can also click **Event** from the configuration list on the home page.

Step 3 Select the remote device in the left-hand side device tree.

Step 4 Select **Smart Plan** > **Traffic Event Detection**, and then click on the right side of the **Enable**.

Step 5 Click **Add Template Rule** , and then select **Truck Entered Prohibited Area**.

You can quickly search for rule types through search. It supports adding multiple rules.

When you add multiple rules, click **Expand All** to open all rule panels and click **Show Less** to close all rule panels.

Step 6 Select the area.

Supports selecting multiple areas.

- Click to pause screen. Click to play it.
- Click to enter the full screen.

Step 7 Configure parameters.

Figure 5-29 Truck entered prohibited area

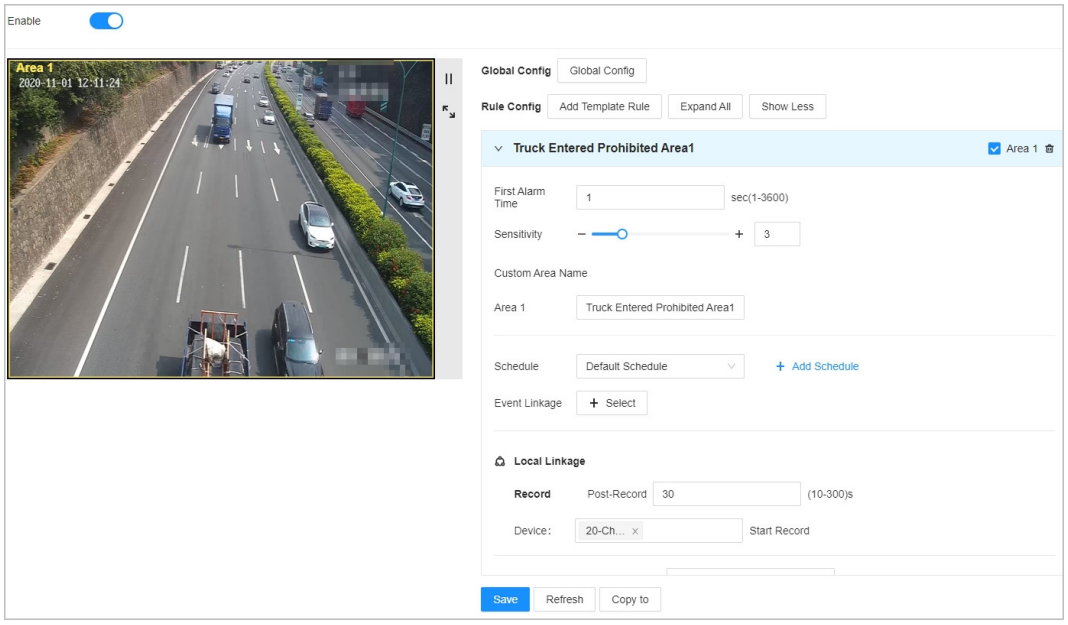


Table 5-14 Description of truck entered prohibited area parameters

Parameter	Description
First Alarm Time	An alarm will be triggered when the truck appears in the detection zone and stays longer than the defined time.
Sensitivity	Set the range from 1 to 10, where a higher value indicates a more sensitive detection but also a higher false positive rate.
Custom Area Name	Set the names of events reported for each area.

Step 8 Click the dropdown menu for **Schedule**, and then select time schedule.

The system will only trigger a linkage alarm event when an alarm is triggered within the set arming time range.

If the added schedule does not meet the actual requirements, you can click **+ Add** to add a new schedule.

Step 9 Click **+ Select** on the right side of **Event Linkage**. Select the alarm linkage type (such as record, picture storage, etc.) and configure the parameters.

Supports linkage for both local and remote alarm linkage items.

Step 10 Click **Save**.

5.5.16 Heat Detection

An alarm will be triggered when fire is detected in the detection zone and the duration exceeds the defined value.

Procedure

Step 1 Log in to the PC client.

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

You can also click **Event** from the configuration list on the home page.

Step 3 Select the remote device in the left-hand side device tree.

Step 4 Select **Smart Plan** > **Smoke and Heat Detection**, and then click on the right side of the **Enable**.

Step 5 Click **Add Template Rule** , and then select **Heat Detection**.

You can quickly search for rule types through search. It supports adding multiple rules.

When you add multiple rules, click **Expand All** to open all rule panels and click **Show Less** to close all rule panels.

Step 6 Select the area.

Supports selecting multiple areas.

- Click to pause screen. Click to play it.
- Click to enter the full screen.

Step 7 Configure parameters.

Figure 5-30 Heat detection

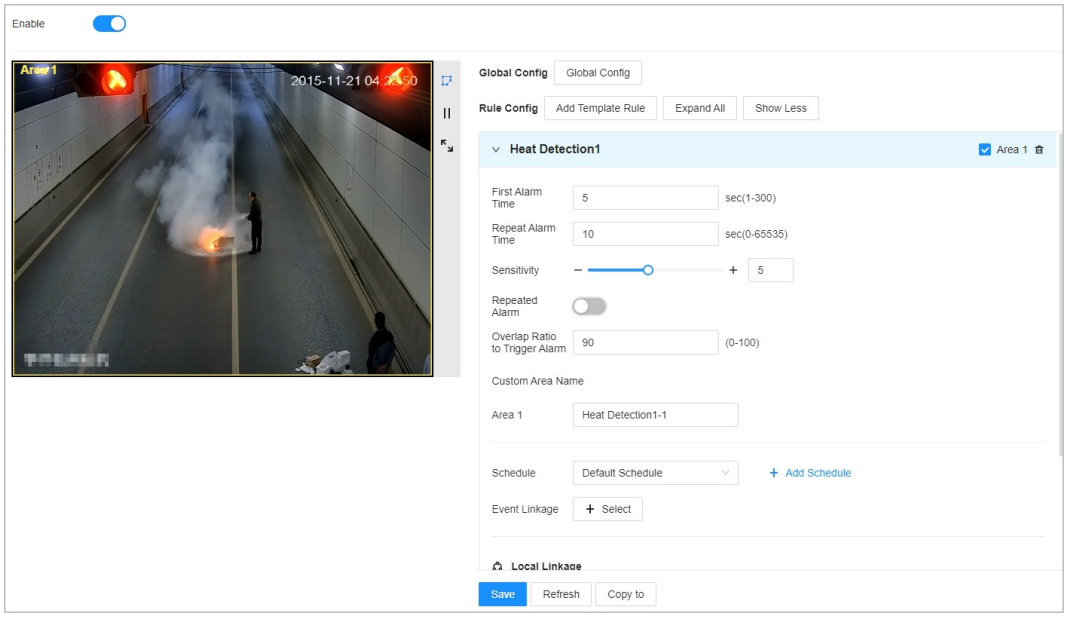


Table 5-15 Description of heat detection parameters

Parameter	Description
First Alarm Time	An alarm will be triggered when the flame duration exceeds the set value.
Repeat Alarm Time	When the flame persists and exceeds the set time, the alarm information will be reported again, with a default of 10 seconds.
Repeated Alarm	It is disabled by default, and enabling it is not recommended.
Sensitivity	Set the range from 1 to 10, where a higher value indicates a more sensitive detection but also a higher false positive rate.

Parameter	Description
Overlap Ratio to Trigger Alarm	Compare the previous frame with the next frame to obtain the overlap area. If the proportion of the overlap area is greater than the set value, an alarm will be triggered.
Custom Area Name	Set the names of events reported for each area.

Step 8 Click the dropdown menu for **Schedule**, and then select time schedule.

The system will only trigger a linkage alarm event when an alarm is triggered within the set arming time range.

If the added schedule does not meet the actual requirements, you can click **+ Add** to add a new schedule.

Step 9 Click **+ Select** on the right side of **Event Linkage**. Select the alarm linkage type (such as record, picture storage, etc.) and configure the parameters.

Supports linkage for both local and remote alarm linkage items.

Step 10 Click **Save**.

5.5.17 Smoke Detection

An alarm will be triggered when smoke is detected in the detection zone and the duration exceeds the defined value.

Procedure

Step 1 Log in to the PC client.

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

You can also click **Event** from the configuration list on the home page.

Step 3 Select the remote device in the left-hand side device tree.

Step 4 Select **Smart Plan** > **Smoke and Heat Detection**, and then click  on the right side of the **Enable**.

Step 5 Click **Add Template Rule** , and then select **Smoke Detection**.

You can quickly search for rule types through search. It supports adding multiple rules.

When you add multiple rules, click **Expand All** to open all rule panels and click **Show Less** to close all rule panels.

Step 6 Select the area.

Supports selecting multiple areas.

- Click  to pause screen. Click  to play it.
- Click  to enter the full screen.

Step 7 Configure parameters.

Figure 5-31 Smoke detection

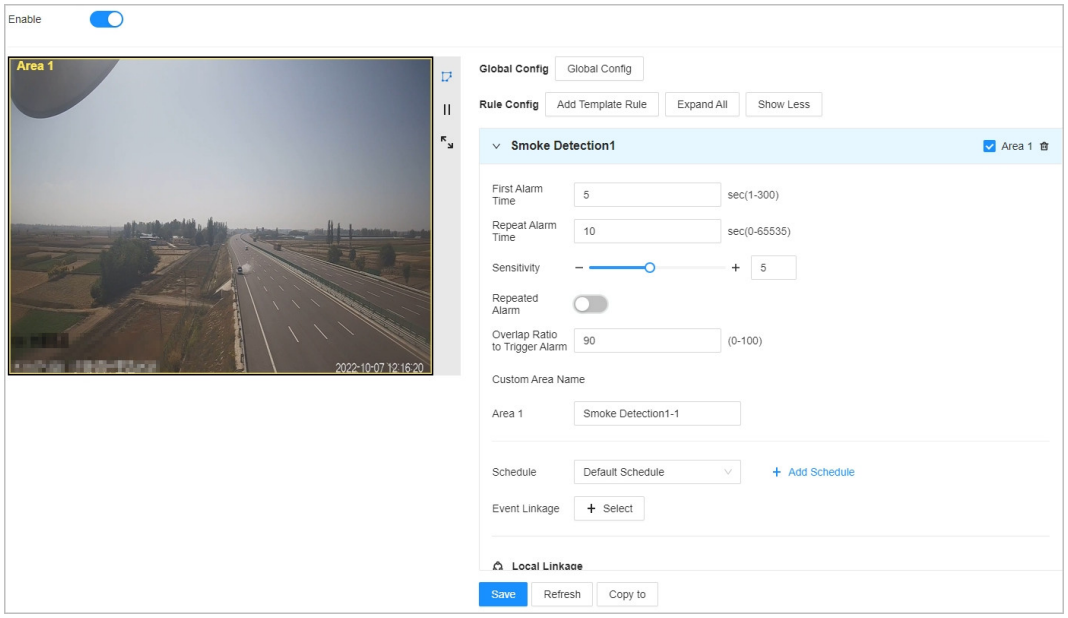


Table 5-16 Description of smoke detection parameters

Parameter	Description
First Alarm Time	An alarm will be triggered when the smoke duration exceeds the set value.
Repeat Alarm Time	When the flame persists and exceeds the set time, the alarm information will be reported again, with a default of 10 seconds.
Repeated Alarm	Disabled by default and enabling is not recommended.
Sensitivity	Set the range from 1 to 10, where a higher value indicates a more sensitive detection but also a higher false positive rate.
Overlap Ratio to Trigger Alarm	Compare the previous frame with the next frame to obtain the overlap area. If the proportion of the overlap area is greater than the set value, an alarm will be triggered.
Custom Area Name	Set the names of events reported for each area.

Step 8 Click the dropdown menu for **Schedule**, and then select time schedule.

The system will only trigger a linkage alarm event when an alarm is triggered within the set arming time range.

If the added schedule does not meet the actual requirements, you can click **+ Add** to add a new schedule.

Step 9 Click **+ Select** on the right side of **Event Linkage**. Select the alarm linkage type (such as record, picture storage, etc.) and configure the parameters.

Supports linkage for both local and remote alarm linkage items.

Step 10 Click **Save**.

5.5.18 Lane Change

An alarm will be triggered when a vehicle crosses the lane line (white solid line or yellow solid line).

Prerequisites

There are at least two lanes in the scene, and two or more lane lines have been drawn.

Procedure

Step 1 Log in to the PC client.

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

You can also click **Event** from the configuration list on the home page.

Step 3 Select the remote device in the left-hand side device tree.

Step 4 Select **Smart Plan** > **Traffic Event Detection**, and then click on the right side of the **Enable**.

Step 5 Click **Add Template Rule** , and then select **Lane Change**.

You can quickly search for rule types through search. It supports adding multiple rules.

When you add multiple rules, click **Expand All** to open all rule panels and click **Show Less** to close all rule panels.

Step 6 Select the area.

Supports selecting multiple areas.

- Click to pause screen. Click to play it.
- Click to enter the full screen.

Step 7 Configure parameters.

Figure 5-32 Lane change

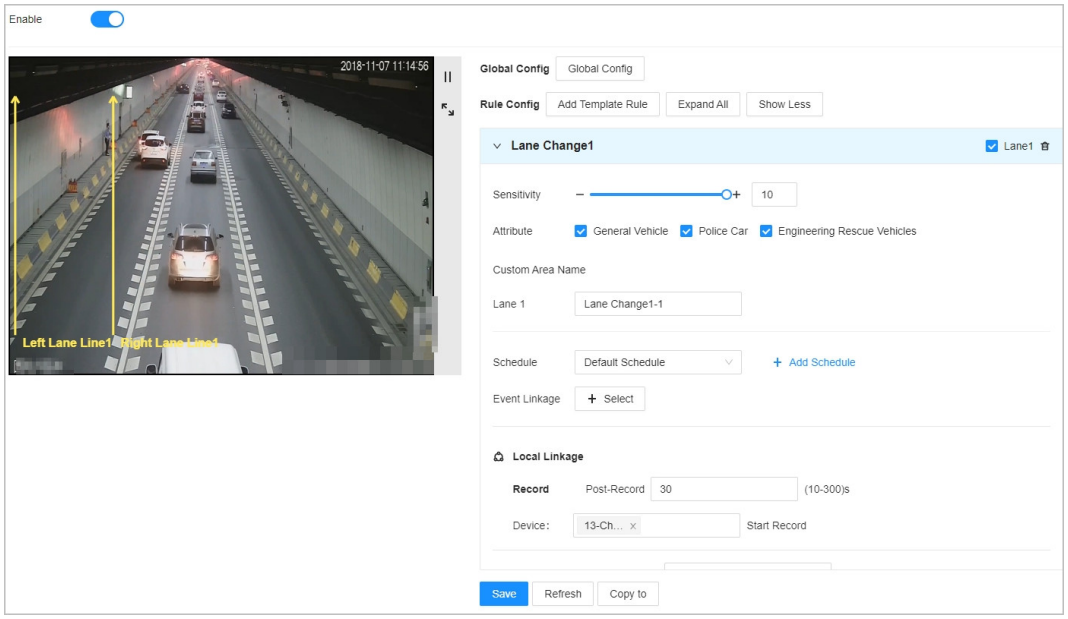


Table 5-17 Description of lane change parameters

Parameter	Description
Lane 1	Select the lane number to be checked.
Sensitivity	Set the range from 1 to 10, where a higher value indicates a more sensitive detection but also a higher false positive rate.
Attribute	Select the vehicle type, including **General Vehicle** , **Police Car** and **Engineering Rescue Vehicles**. When a target of the specified type is detected, an alarm will be triggered.
Custom Area Name	Set the names of events reported for each area.

Step 8 Click the dropdown menu for **Schedule**, and then select time schedule.

The system will only trigger a linkage alarm event when an alarm is triggered within the set arming time range.

If the added schedule does not meet the actual requirements, you can click **+ Add** to add a new schedule.

Step 9 Click **+ Select** on the right side of **Event Linkage**. Select the alarm linkage type (such as record, picture storage, etc.) and configure the parameters.

Supports linkage for both local and remote alarm linkage items.

Step 10 Click **Save**.

5.5.19 Crossing Solid Line Detection

An alarm will be triggered when a vehicle crosses a solid yellow line or solid white line.

Procedure

Step 1 Log in to the PC client.

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

You can also click **Event** from the configuration list on the home page.

Step 3 Select the remote device in the left-hand side device tree.

Step 4 Select **Smart Plan** > **Traffic Event Detection**, and then click  on the right side of the **Enable**.

Step 5 Click **Add Template Rule** , and then select **Crossing Solid Line Detection**.

You can quickly search for rule types through search. It supports adding multiple rules.

When you add multiple rules, click **Expand All** to open all rule panels and click **Show Less** to close all rule panels.

Step 6 Select the area.

Supports selecting multiple areas.

- Click  to pause screen. Click  to play it.
- Click  to enter the full screen.

Step 7 Configure parameters.

Figure 5-33 Crossing solid line detection

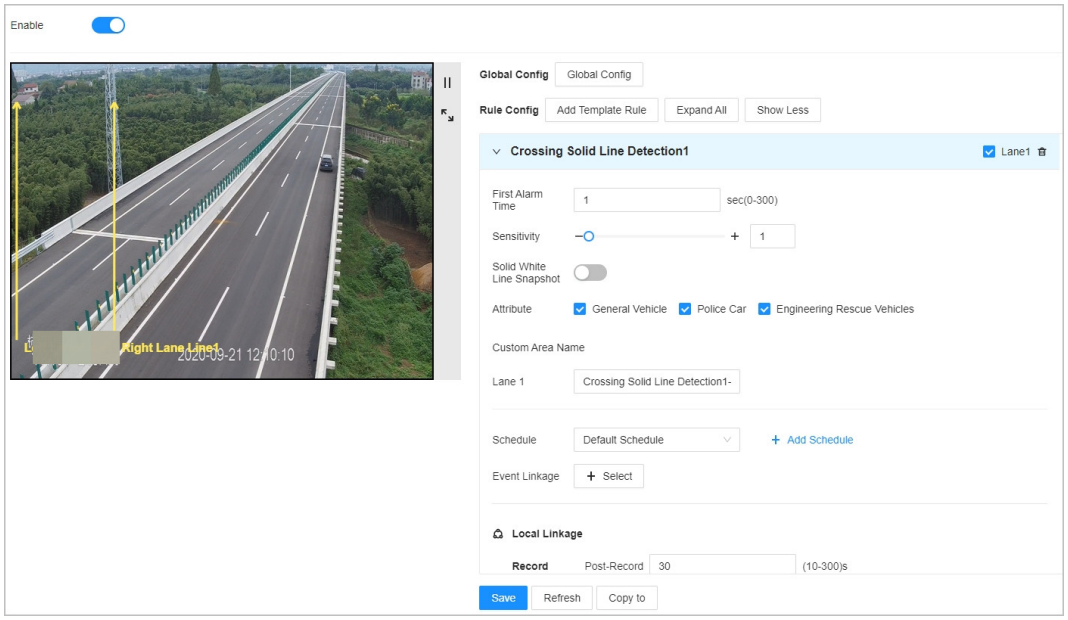


Table 5-18 Description of crossing solid line detection parameters

Parameter	Description
Lane 1	Enter the lane number that needs to be checked for low speed.
First Alarm Time	An alarm will be triggered when a motor vehicle appears in the detection zone and stays longer than the defined time.
Sensitivity	Set the range from 1 to 10, where a higher value indicates a more sensitive detection but also a higher false positive rate.
Solid White Line Snapshot	Click to enable solid white line snapshot. Default detects yellow solid line.
Custom Area Name	Set the names of events reported for each area.

Step 8 Click the dropdown menu for **Schedule**, and then select time schedule.

The system will only trigger a linkage alarm event when an alarm is triggered within the set arming time range.

If the added schedule does not meet the actual requirements, you can click **+ Add** to add a new schedule.

Step 9 Click **+ Select** on the right side of **Event Linkage**. Select the alarm linkage type (such as record, picture storage, etc.) and configure the parameters.

Supports linkage for both local and remote alarm linkage items.

Step 10 Click **Save**.

5.5.20 Dense Fog Detection

An alarm will be triggered when radiation fog is detected in the detection zone and the duration exceeds the defined value.

Procedure

Step 1 Log in to the PC client.

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

You can also click **Event** from the configuration list on the home page.

Step 3 Select the remote device in the left-hand side device tree.

Step 4 Select **Smart Plan** > **Traffic Event Detection**, and then click on the right side of the **Enable**.

Step 5 Click **Add Template Rule** , and then select **Dense Fog Detection**.

You can quickly search for rule types through search. It supports adding multiple rules.

When you add multiple rules, click **Expand All** to open all rule panels and click **Show Less** to close all rule panels.

Step 6 Select the area.

Supports selecting multiple areas.

- Click to pause screen. Click to play it.
- Click to enter the full screen.

Step 7 Configure parameters.

Figure 5-34 Dense fog detection

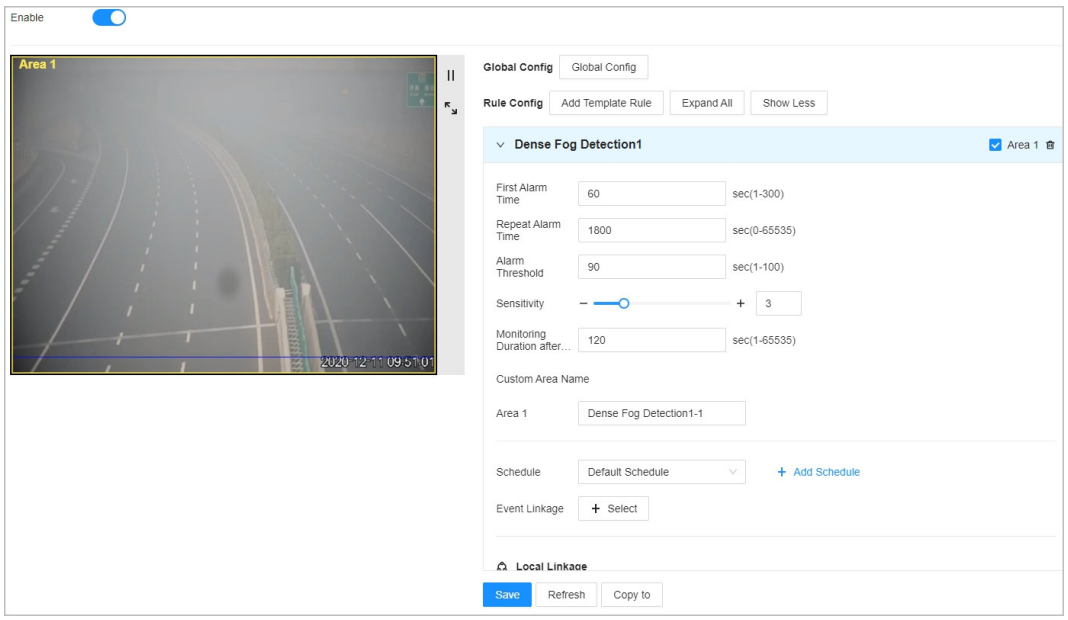


Table 5-19 Description of dense fog detection parameters

Parameter	Description
First Alarm Time	An alarm will be triggered when dense fog appears in the detection zone and stays longer than the defined time.
Repeat Alarm Time	If fog persists within the scheduled interval, only one alarm message will be reported. This is to prevent multiple alarm reports for the same fog occurrence within a short period of time. Event removed, there will be three alarm images in the alarm details, including the image at the first alarm, the image when the repeat alarm time interval is met, and the image at the time of removal.
Alarm Threshold	An alarm will be triggered when the concentration of fog in the group exceeds the set percentage.
Sensitivity	Set the range from 1 to 10, where a higher value indicates a more sensitive detection but also a higher false positive rate.
Monitoring Duration after Target Disappears	The event ends when the disappearing duration of the object reaches the defined time.
Custom Area Name	Set the names of events reported for each area.

Step 8 Click the dropdown menu for **Schedule**, and then select time schedule.

The system will only trigger a linkage alarm event when an alarm is triggered within the set arming time range.

If the added schedule does not meet the actual requirements, you can click **+ Add** to add a new schedule.

Step 9 Click **+ Select** on the right side of **Event Linkage**. Select the alarm linkage type (such as record, picture storage, etc.) and configure the parameters.

Supports linkage for both local and remote alarm linkage items.

Step 10 Click **Save**.

5.5.21 Intrusion

An alarm will be triggered when the target enters the detection area.

Procedure

Step 1 Log in to the PC client.

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

You can also click **Event** from the configuration list on the home page.

Step 3 Select the remote device in the left-hand side device tree.

Step 4 Select **Smart Plan** > **Traffic Event Detection**, and then click on the right side of the **Enable**.

Step 5 Click **Add Template Rule** , and then select **Intrusion**.

You can quickly search for rule types through search. It supports adding multiple rules.

When you add multiple rules, click **Expand All** to open all rule panels and click **Show Less** to close all rule panels.

Step 6 Select the area.

Supports selecting multiple areas.

- Click to pause screen. Click to play it.
- Click to enter the full screen.

Step 7 Configure parameters.

Figure 5-35 Intrusion

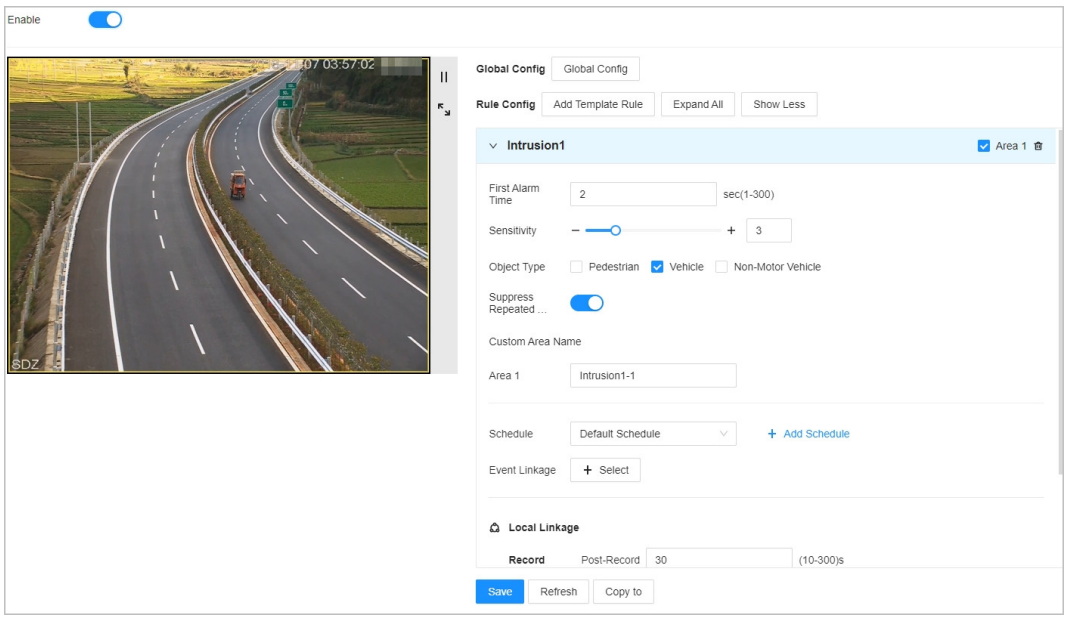


Table 5-20 Description of intrusion parameters

Parameter	Description
First Alarm Time	An alarm will be triggered when the target appears in the frame for longer than the defined time.
Sensitivity	Set the range from 1 to 10, where a higher value indicates a more sensitive detection but also a higher false positive rate.
Object Type	Select the type of object to be detected.
Suppress Repeated Alarms	Enabling this feature can reduce repeated alarms for the same target. It is recommended to enable it.
Custom Area Name	Set the names of events reported for each area.

Step 8 Click the dropdown menu for **Schedule**, and then select time schedule.

The system will only trigger a linkage alarm event when an alarm is triggered within the set arming time range.

If the added schedule does not meet the actual requirements, you can click **+ Add** to add a new schedule.

Step 9 Click **+ Select** on the right side of **Event Linkage**. Select the alarm linkage type (such as record, picture storage, etc.) and configure the parameters.

Supports linkage for both local and remote alarm linkage items.

Step 10 Click **Save**.

5.5.22 Driving Too Slow Detection

An alarm will be triggered when the driving speed is lower than the defined minimum speed and the duration exceeds the defined value.

Procedure

Step 1 Log in to the PC client.

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

You can also click **Event** from the configuration list on the home page.

Step 3 Select the remote device in the left-hand side device tree.

Step 4 Select **Smart Plan** > **Traffic Event Detection**, and then click  on the right side of the **Enable**.

Step 5 Click **Add Template Rule** , and then select **Driving Too Slow Detection**.

You can quickly search for rule types through search. It supports adding multiple rules.

When you add multiple rules, click **Expand All** to open all rule panels and click **Show Less** to close all rule panels.

Step 6 Select the area.

Supports selecting multiple areas.

- Click  to pause screen. Click  to play it.
- Click  to enter the full screen.

Step 7 Configure parameters.

Figure 5-36 Driving too slow detection

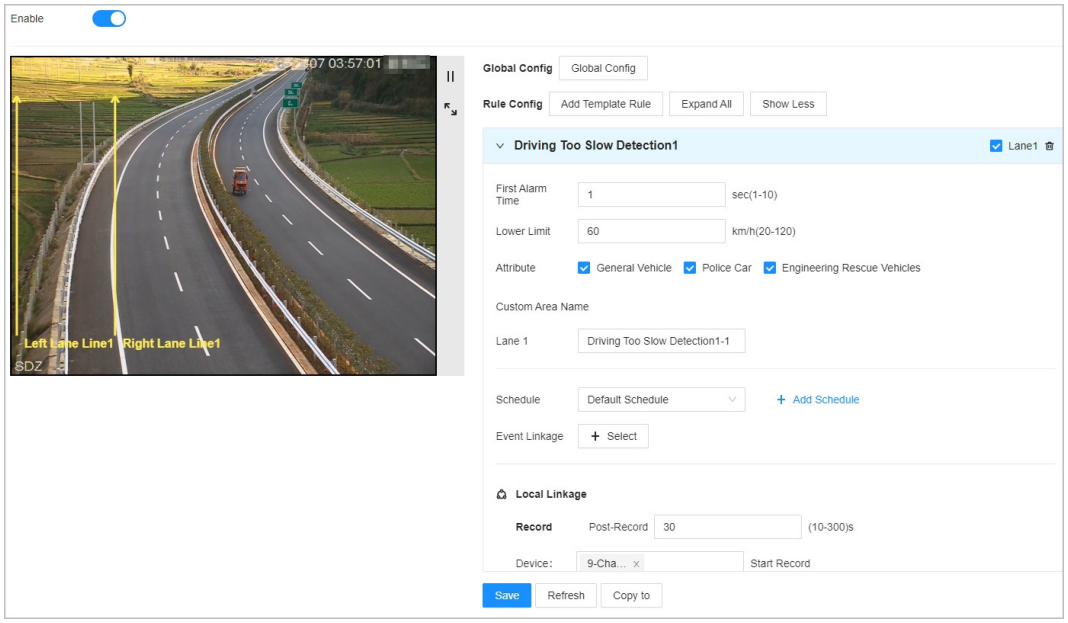


Table 5-21 Description of driving too slow detection parameters

Parameter	Description
First Alarm Time	An alarm will be triggered when the vehicle's speed is lower than the minimum speed and the duration reaches the preset value of the first alarm time
Lower Limit	
Attribute	Select the vehicle type, including **General Vehicle** , **Police Car** and **Engineering Rescue Vehicles**. An alarm will be triggered when a target of the specified type is detected.
Custom Area Name	Set the names of events reported for each area.

Step 8 Click the dropdown menu for **Schedule**, and then select time schedule.

The system will only trigger a linkage alarm event when an alarm is triggered within the set arming time range.

If the added schedule does not meet the actual requirements, you can click **+ Add** to add a new schedule.

Step 9 Click **+ Select** on the right side of **Event Linkage**. Select the alarm linkage type (such as record, picture storage, etc.) and configure the parameters.

Supports linkage for both local and remote alarm linkage items.

Step 10 Click **Save**.

5.5.23 Speeding Detection

When the speed of a vehicle is higher than the defined maximum speed and the duration exceeds the defined value, an alarm will be triggered.

Procedure

Step 1 Log in to the PC client.

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

You can also click **Event** from the configuration list on the home page.

Step 3 Select the remote device in the left-hand side device tree.

Step 4 Select **Smart Plan** > **Traffic Event Detection**, and then click on the right side of the **Enable**.

Step 5 Click **Add Template Rule** , and then select **Speeding Detection**.

You can quickly search for rule types through search. It supports adding multiple rules.

When you add multiple rules, click **Expand All** to open all rule panels and click **Show Less** to close all rule panels.

Step 6 Select the area.

Supports selecting multiple areas.

- Click to pause screen. Click to play it.
- Click to enter the full screen.

Step 7 Configure parameters.

Figure 5-37 Speeding detection

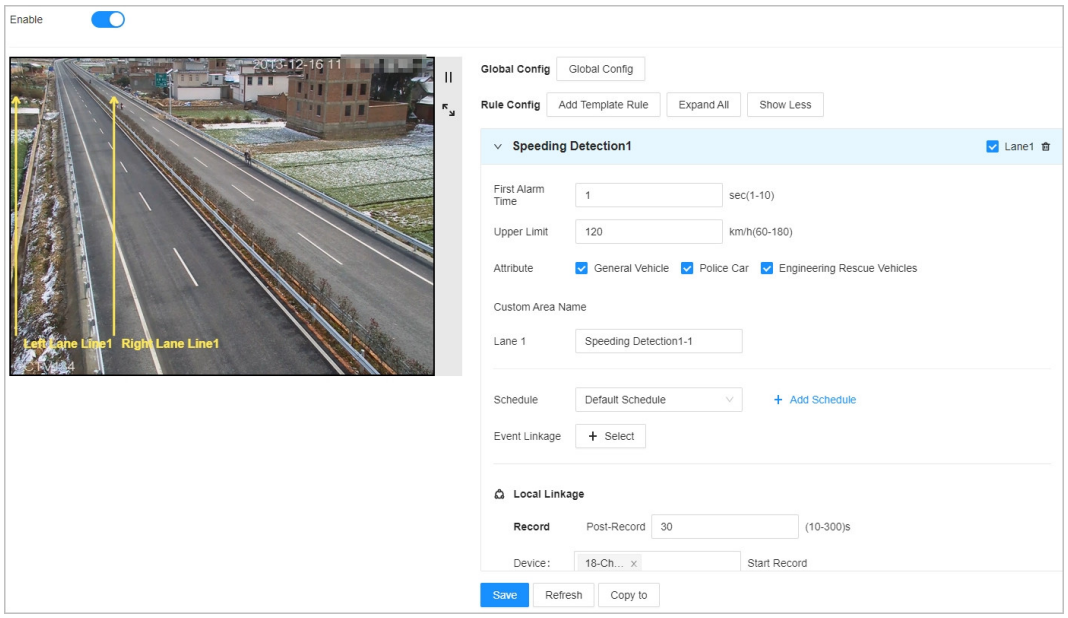


Table 5-22 Description of speeding detection parameters

Parameter	Description
First Alarm Time	An alarm will be triggered when the vehicle's speed is higher than the maximum speed and the duration reaches the preset value of the first alarm time
Upper Limit	
Attribute	Select the vehicle type, including **General Vehicle** , **Police Car** and **Engineering Rescue Vehicles**. An alarm will be triggered when a target of the specified type is detected.
Custom Area Name	Set the names of events reported for each area.

Step 8 Click the dropdown menu for **Schedule**, and then select time schedule.

The system will only trigger a linkage alarm event when an alarm is triggered within the set arming time range.

If the added schedule does not meet the actual requirements, you can click **+ Add** to add a new schedule.

Step 9 Click **+ Select** on the right side of **Event Linkage**. Select the alarm linkage type (such as record, picture storage, etc.) and configure the parameters.

Supports linkage for both local and remote alarm linkage items.

Step 10 Click **Save**.

5.5.24 Copying rules

Supports quickly copying configured global settings and rule parameters to other channels or presets.

Procedure

Step 1 Log in to the PC client.

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

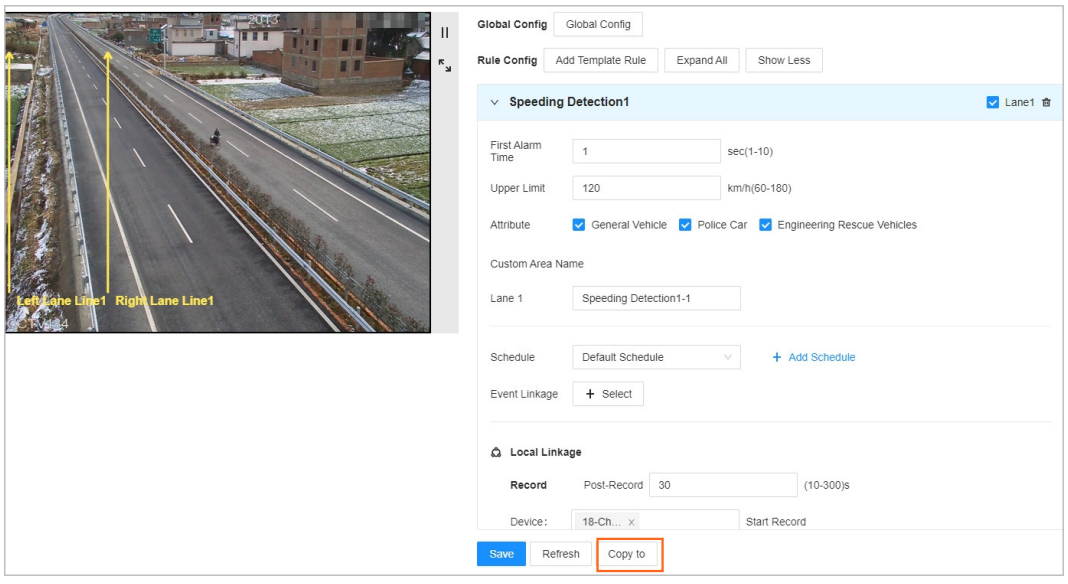
You can also click **Event** from the configuration list on the home page.

Step 3 Select the remote device in the left-hand side device tree.

Step 4 Select **Smart Plan** > **Traffic Event Detection**.

Step 5 Click **Copy to**.

Figure 5-38 Copy to

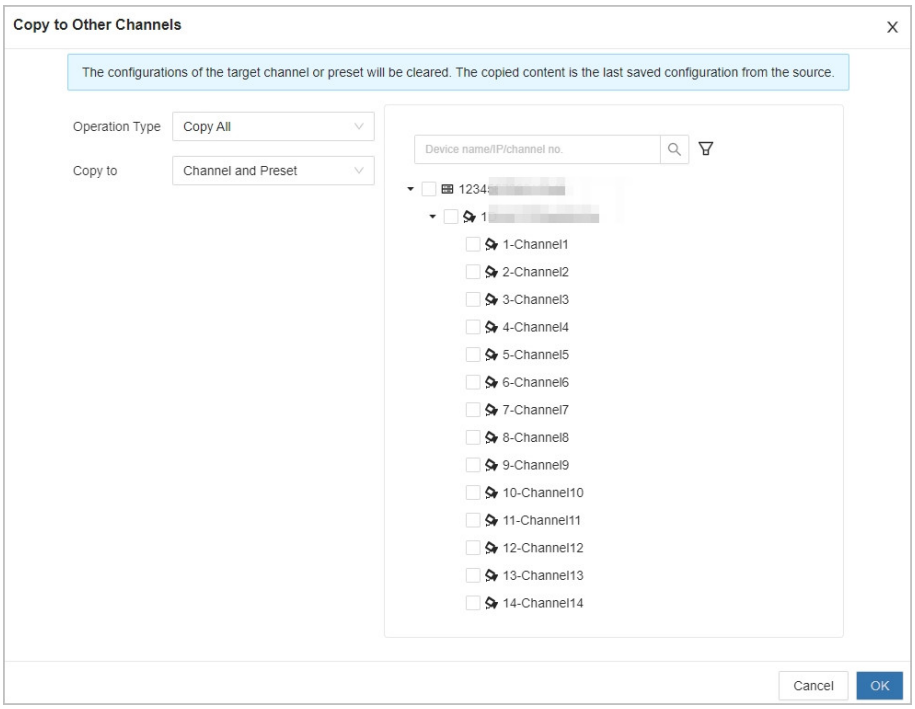


Step 6 Select the operation type and the target type for copying, and then select the channel or preset on the right side.

- Operation Type: **Copy All** and **Copy Template Rule**. When **Copy All** is selected, both global configurations and rule configurations are copied. When **Copy Template Rule** is selected, only rule configurations are copied.

- Copy to: **Channel and Preset** , **Only Channel** and **Only Preset**. The right side will display content based on the selected target type.

Figure 5-39 Copy to other channels



Step 7 Click **OK**.

5.5.25 AI Search

Search for traffic event detection information that meets the conditions by setting the event type and other search conditions.

Procedure

Step 1 Log in to the PC client.

Step 2 Select **AI Search** > **Road Traffic Detection**.

For debris object events, select **Road Debris Detection** ; for smoke and heat events, select **Smoke and Heat Detection**.

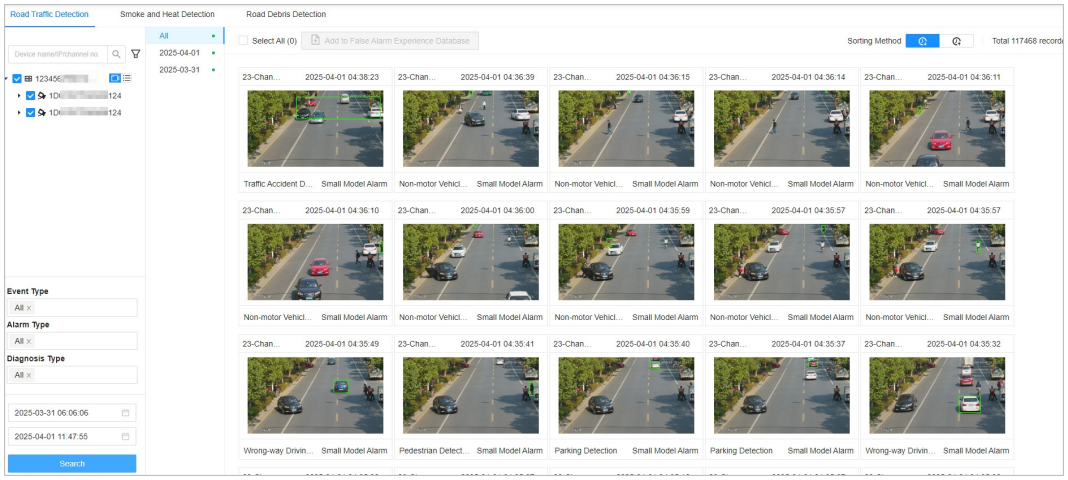
Step 3 Select the remote device you want to search for.

Step 4 Select **Event Type** , **Alarm Type**, **Diagnosis Type** and time.

Step 5 Click **Search**.

Search results support sorting by time.

Figure 5-40 Search results



Related Operations

Click in the search results panel; click to display the details page, which displays images by default. Click the small icon in the upper-right corner to switch to the video view. The right side of the page allows for reviewing alarm results.

Figure 5-41 Details

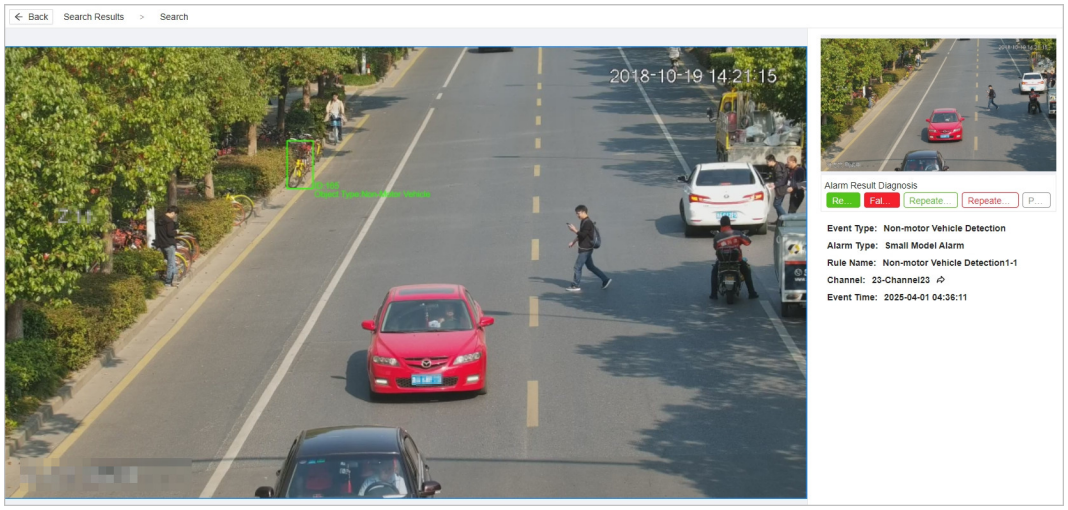
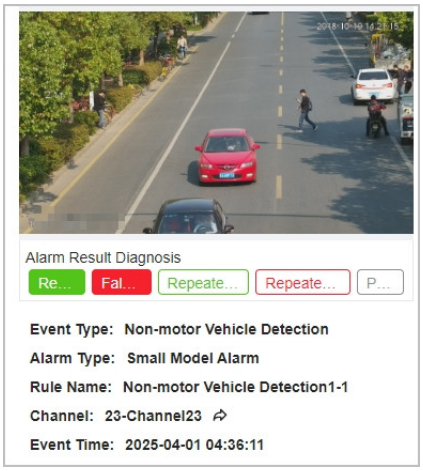


Table 5-23 Related operations

Function	Operation
Audit alarm result	Click **Real Alarm** , **False Alarm**, **Repeated Real Alarm**, **Repeated False Alarm** or **Pending**, and then the corresponding tag will be displayed on the screen. ● Real Alarm: Confirm that this alarm is a valid alarm. ● False Alarm: Confirm that this alarm is a false alarm. ● Repeated Real Alarm: Confirm that this alarm is a duplicate valid alarm for the same event. ● Repeated False Alarm: Confirm that this alarm is a duplicate false alarm for the same event. ● Pending: Do not diagnose this alarm temporarily. 
Playback record video	● and : Pause or play record video. ● : Drag the progress bar to select the time for play. ● : Enter the interface settings and select the information to be overlaid on the screen.
Previous or next	Click **Previous** or **Next** to switch different alarm results.

5.6 Secondary Analysis

First, analyze the video using a small model, and then perform a secondary analysis after reporting the results. This can effectively reduce false alarms.

Prerequisites

- The channel's model is configured as a small model.
- At least one intelligent analysis card is set for secondary analysis. Select **System** > **AI Config** > **AI Module**, and then you can modify it.

Procedure

Step 1 Log in to the PC client.

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

You can also click **Event** from the configuration list on the home page.

Step 3 Select the channel in the left-hand side device tree.

Step 4 Select **Smart plan** > **Secondary Analysis**.

Step 5 Click **Event Type** , select the events that require secondary analysis, and then click **OK**.

Step 6 Configure parameters.

Figure 5-42 Secondary analysis

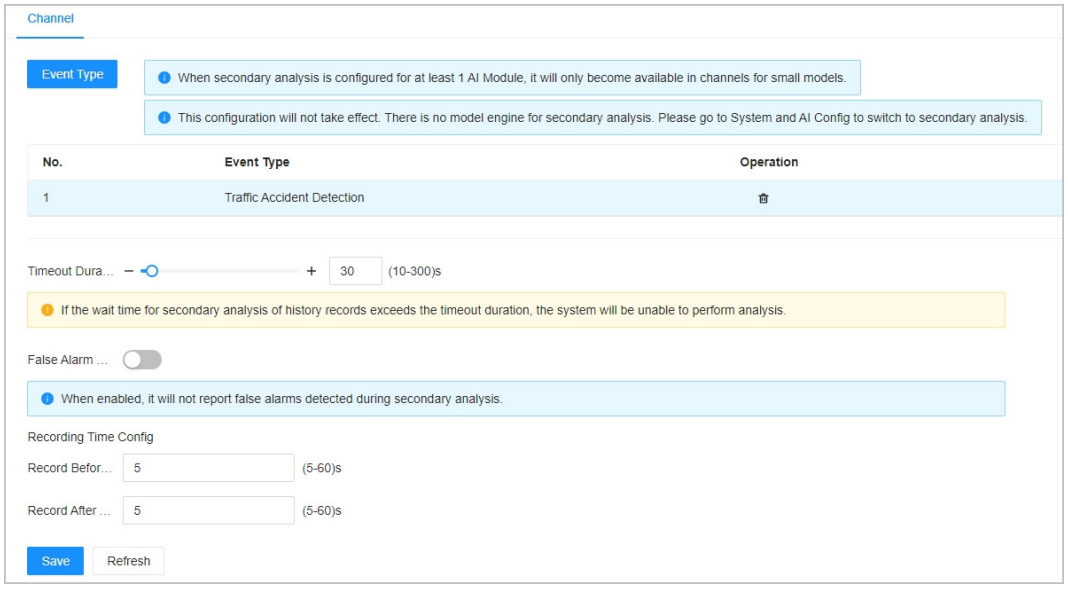


Table 5-24 Description of secondary analysis parameters

Parameter	Description
Timeout Duration	After an event is triggered, it enters the secondary analysis queue for analysis. If the waiting time reaches the timeout limit, the secondary analysis for the event will be canceled.
False Alarm Filter	If false alarm filter is enabled, alarms identified as false alarms by the secondary analysis module will not be pushed to the client pop-up window or be available for query.
Record Before Alarm	Capture video of the scene prior to the event according to the set time duration.
Record After Alarm	Capture video of the scene following the event according to the set time duration.

Step 7 Click **Save**.

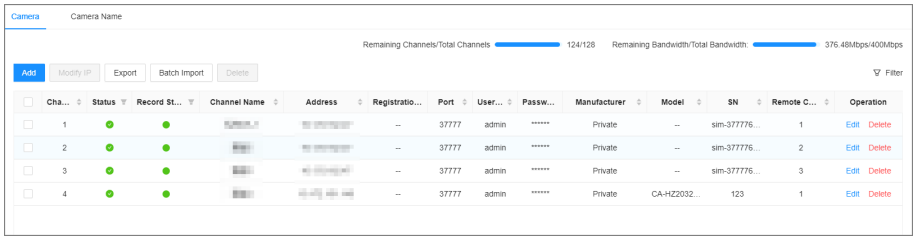
6 System Configuration

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

6.1 Device Management

Log in to the PC client, click on the upper-right corner, and then click **Camera** , or click **Camera** from the configuration list on the home page. You can add remote devices, modify their IP addresses and configurations, and export their information. You can view the online status and recording status of the device.

Figure 6-1 Device management



Click + on the lower-left corner or click **Add** to add remote devices to the Device.

6.1.1 Viewing Remote Devices

View connected remote devices.

Procedure

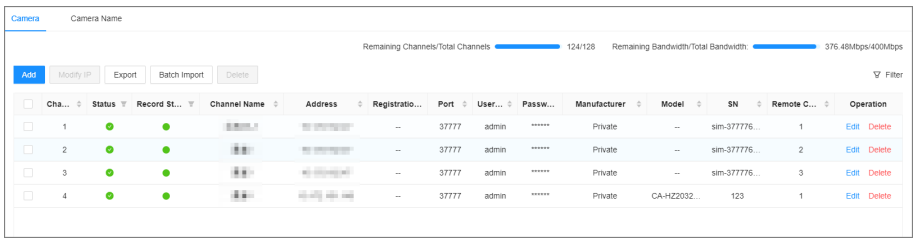
Step 1 Log in to the PC client.

Step 2 Click on the upper-right corner of the page, and then click **Camera**.

You can also click **Camera** from the configuration list on the home page.

Step 3 Select the root node on the device tree, and then under the **Camera** tab, you can view the remote devices.

Figure 6-2 Device list



Step 4 View details on the connected devices, including IP address, serial number, connection status, and more.

- indicates that the remote device is offline.

- indicates that the remote device is online.
- indicates that the connection with the remote device failed.

You can click to filter the remote devices.

6.1.2 Changing IP Address

Modify IP address of the remote devices that only support private protocol and ONVIF protocol.

6.1.2.1 Modifying IP of Unconnected Devices

Procedure

Step 1 Log in to the PC client.

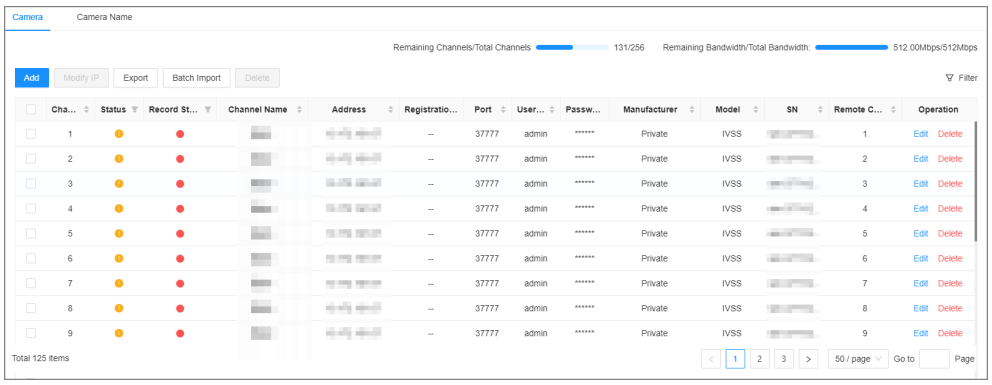
Step 2 Click on the upper-right corner of the page and then click **Camera**.

You can also click **Camera** from the configuration list on the home page.

Step 3 On the **Camera** tab, click **Add**.

You can also click **Add** under the device tree.

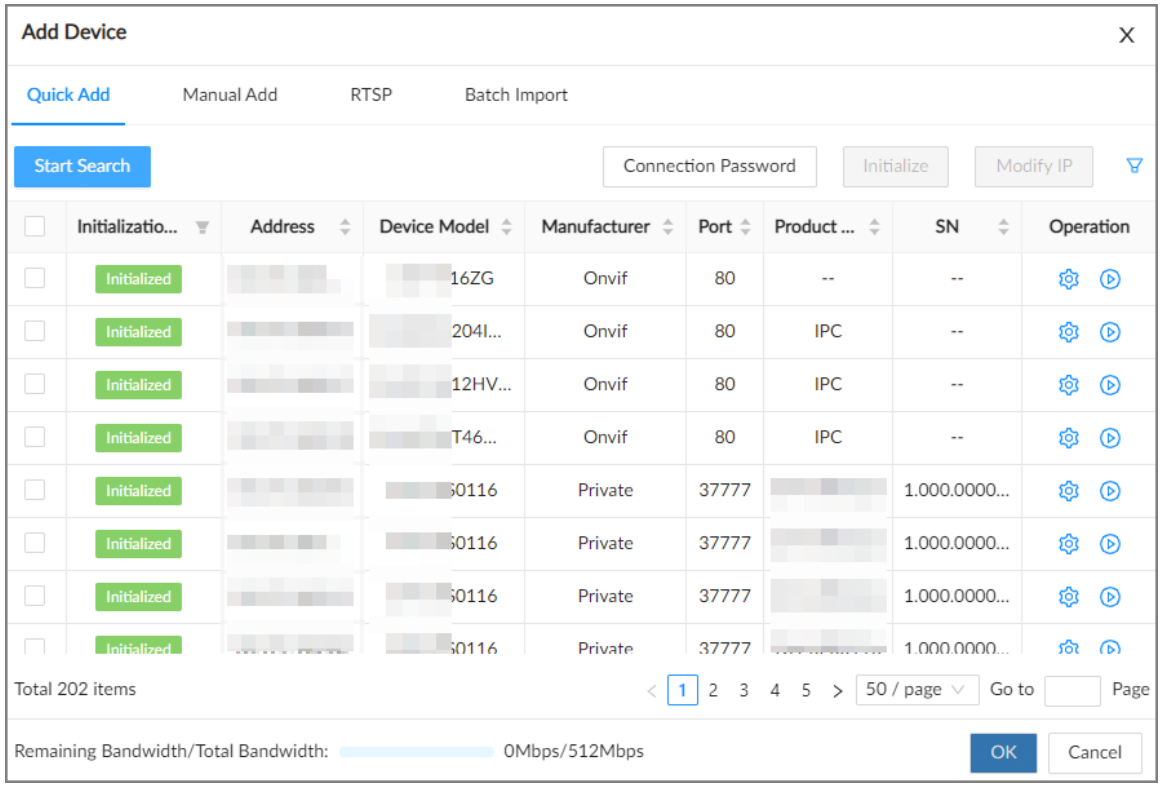
Figure 6-3 Camera



Step 4 On the **Quick Add** tab, click **Start Search**.

You can click to filter the search results.

Figure 6-4 Search results



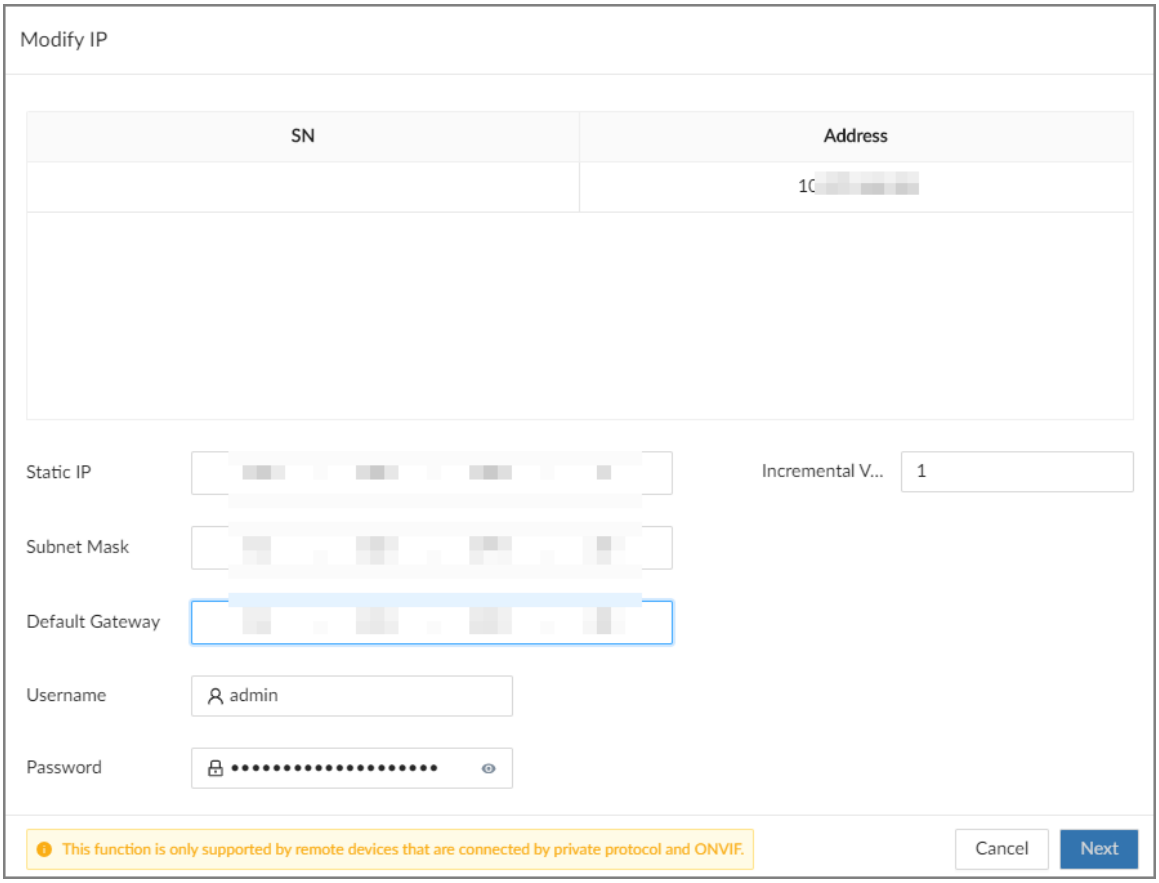
Step 5 Select one or multiple remote devices, and then click **Modify IP**.

- You can only modify the IP address of initialized devices.
- You can only modify the IP address of remote devices that are using the private or ONVIF protocol.

Step 6 Enter the static IP address, subnet mask, gateway, username and password of the remote device, and then click **Next**.

- Enter incremental value only when you want to change IP addresses of several devices at the same time. The system will allocate IP addresses one by one with the fourth part of the IP address increasing by the incremental value.
- If an IP conflict occurs when you change the static IP address, the system will notify you of the issue. When an IP conflicts happens when you are changing IP addresses in batches, the system automatically skips the conflicted IP and begins the allocation according to the incremental value.
- If you want to change IP addresses of multiple remote devices, make sure that they share the same username and password.

Figure 6-5 Modify IP



Step 7 Click **OK**.

6.1.2.2 Modifying IP of Connected Devices

Procedure

Step 1 Log in to the PC client.

Step 2 Click on the upper-right corner of the page and then click **Camera**.

You can also click **Camera** from the configuration list on the home page.

Step 3 Under the **Camera** tab, select one or remote devices, and then click **Modify IP**.

- You can only modify the IP address of initialized devices.
- You can only modify the IP address of remote devices that are using the private or ONVIF protocol.

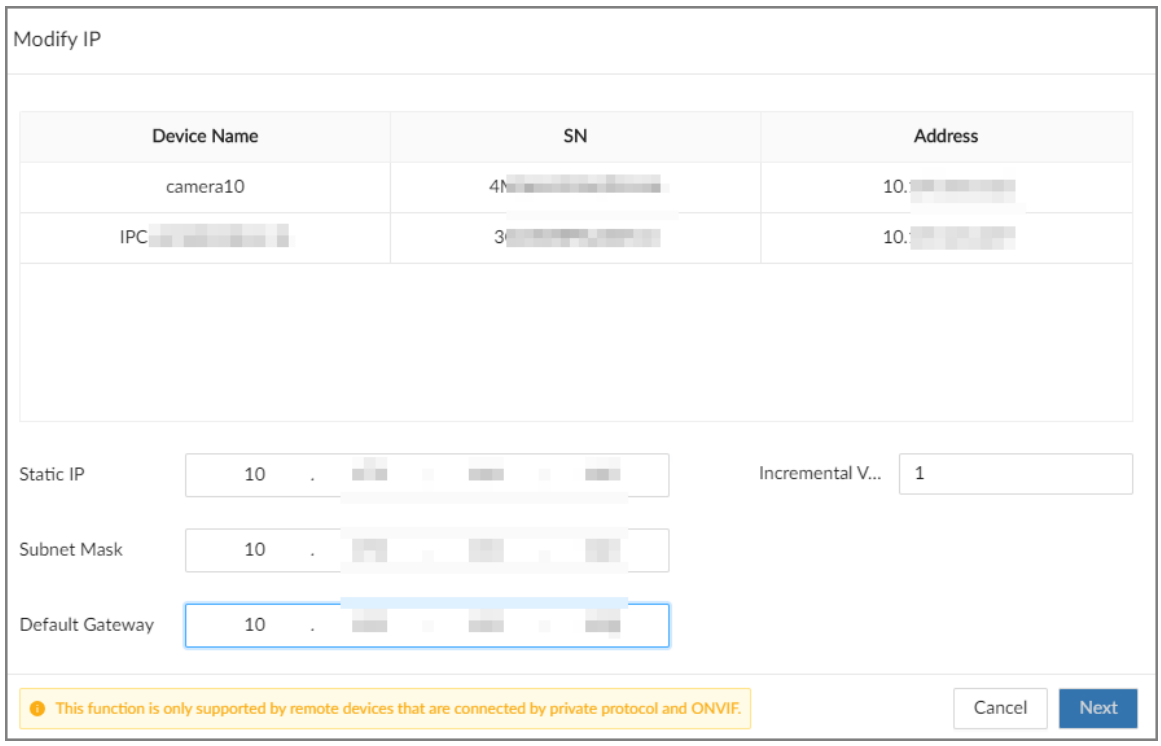
Step 4 Enter the static IP address, subnet mask, gateway, username and password of the remote device, and then click **Next**.

- Enter incremental value only when you want to change IP addresses of several devices at the same time. The system will allocate IP addresses one by one with the fourth part of the IP address increasing by the incremental value.
- If an IP conflict occurs when you change the static IP address, the system will notify you of the issue. When an IP conflicts happens when you are changing IP addresses in

batches, the system automatically skips the conflicted IP and begins the allocation according to the incremental value.

- If you want to change IP addresses of multiple remote devices, make sure that they share the same username and password.

Figure 6-6 Modify IP



Step 5 Click **OK**.

6.1.3 Configuring Remote Devices

Set the attributes, video parameters and other parameters of remote devices connected to the Device.

The pages might vary with remote devices.

6.1.3.1 Configuring Attributes of Remote Devices

View information on the remote devices.

Procedure

Step 1 Log in to the PC client.

Step 2 Click on the upper-right corner of the page and then click **Camera**.

You can also click **Camera** from the configuration list on the home page.

Step 3 Select a remote device from the device tree, and then click the **Attribute** tab.

You can view information on the remote device, such as model, MAC, system version, and more.

Figure 6-7 Attributes

Step 4 (Optional) Enter description for the remote device, and then click **Save**.

6.1.3.2 Managing Video Channels of Multichannel Devices

When the connected remote device has multiple video channels, you can add or delete the video channels connected to the Device.

Procedure

Step 1 Log in to the PC client.

Step 2 Click on the upper-right corner of the page and then click **Camera**.

You can also click **Camera** from the configuration list on the home page.

Step 3 Select a multichannel remote device from the device tree, and then click the **Connection Info** tab.

You can view the video channels under the group.

Step 4 Add or delete the video channels.

- Add video channels.

  Click **Add Video Channel** to add more video channels to the group.
- Delete video channels.

- ◇ Delete one by one: Click **Delete** under **Operation** to delete the corresponding video channel.
- ◇ Delete in batches: Select one or multiple video channels, and then click **Delete Video Channel**.

6.1.3.3 Configuring Video Parameters

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

Procedure

Step 1 Log in to the PC client.

Step 2 Click on the upper-right corner of the page and then click **Camera**.

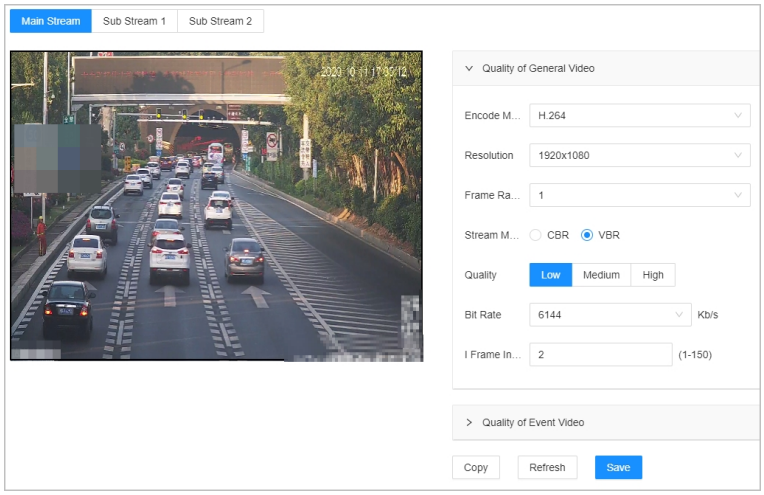
You can also click **Camera** from the configuration list on the home page.

Step 3 Select a remote device from the device tree, and then click the **Video** tab.

You can view information on the remote device, such as its model, MAC address, system version, and more.

Step 4 Select a remote device from the device tree, and then click the **Video** tab.

Figure 6-8 Video



Step 5 Set the parameters under the **Main Stream** , **Sub Stream 1** and **Sub Stream 2** tab.

This section uses the configuration for the main stream as an example.

1. Configure the quality parameters of general videos.

Table 6-1 General video parameters

Parameter	Description
Encode Mode	Select a video encoding mode. ● H.264: A highly compressed video encoding standard. It includes H.264B (baseline profile encode mode), H.264 (main profile encode mode) and H. 264H (high profile encode mode). Under the same image quality, the bandwidth of the three decreases in turn. ● H.265: A new video encoding standard coming after H.264. Under the same image quality, it requires smaller bandwidth than H.264.

Parameter	Description
Resolution	Set video resolution. The higher the resolution, the better the video quality. Different models of remote devices support different resolutions. Refer to the actual page for detailed information.
Frame Rate	Set the number of frames displayed each second. The higher the FPS, the more vivid and fluent the video.
Stream Mode	Select a stream mode. ● CBR: The bit rate changes slightly around the defined value. We recommend you select CBR when there might be only small changes in the monitoring environment. ● VBR: The bit rate changes with monitoring scenes. Select VBR when there might be big changes in the monitoring environment.
Quality	Select a video quality level from **Low** , **Medium**, and **High**. This parameter is available only when the stream mode is VBR.
Bit Rate	Set video bit rate. ● Main stream: Select a value or enter a customized value for bit rate. The bigger the value, the better the image quality. ● Sub stream: In CBR mode, the bit rate changes around the defined value. In VBR mode, the bit rate changes along with the video image, but its maximum value stays near the defined value.
I Frame Interval	Set the number of P frames between 2 I frames. The lower the value, the better the video quality. The recommended value is 2 times of the frame rate.

2. Click **Quality of Event Video**, and then set frame rate, stream mode, and bit rate for event videos.

   The **Quality of Event Video** section is only available for main stream.

Step 6 Click **Save**.

6.1.3.4 Configuring OSD

Set OSD information on the video.

Procedure

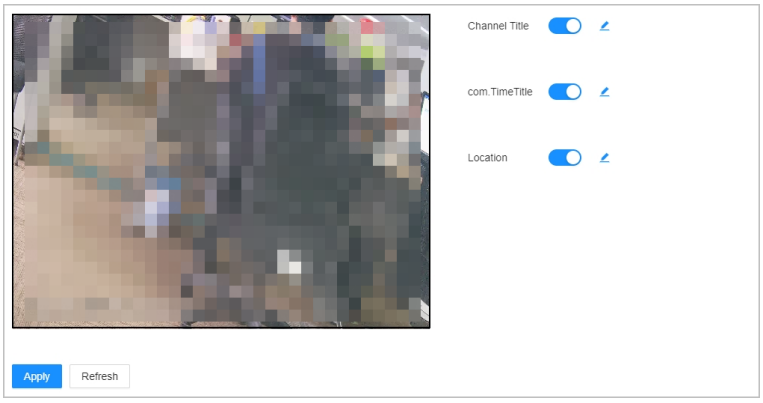
Step 1 Log in to the PC client.

Step 2 Click on the upper-right corner of the page and then click **Camera**.

You can also click **Camera** from the configuration list on the home page.

Step 3 Select a remote device from the device tree, and then click the **OSD** tab.

Figure 6-9 OSD



Step 4 Configure OSD information.

- Channel Title
  1. Click to enable OSD of channel title.
  2. Click .
  3. Enter the channel title.
  4. Drag the text box to the proper position.
- com. TimeTitle
  1. Click to enable OSD of time.
  2. Click .
  3. Drag the text box to the proper position.
- Location
  1. Click to enable OSD of location.
  2. Click .
  3. Enter the location information.

     ◇ Click to adjust the alignment of text boxes.

     ◇ Click or to create a text box.

     ◇ Click to delete a text box.
  4. Drag the text box to the proper position.

Step 5 Click **Apply**.

6.1.4 Exporting Remote Devices in Batches

Export the added remote devices. When the Device restores factory default settings or lost information of remote devices, you can import the exported information of remote devices to recover quickly.

Procedure

Step 1 Log in to the PC client.

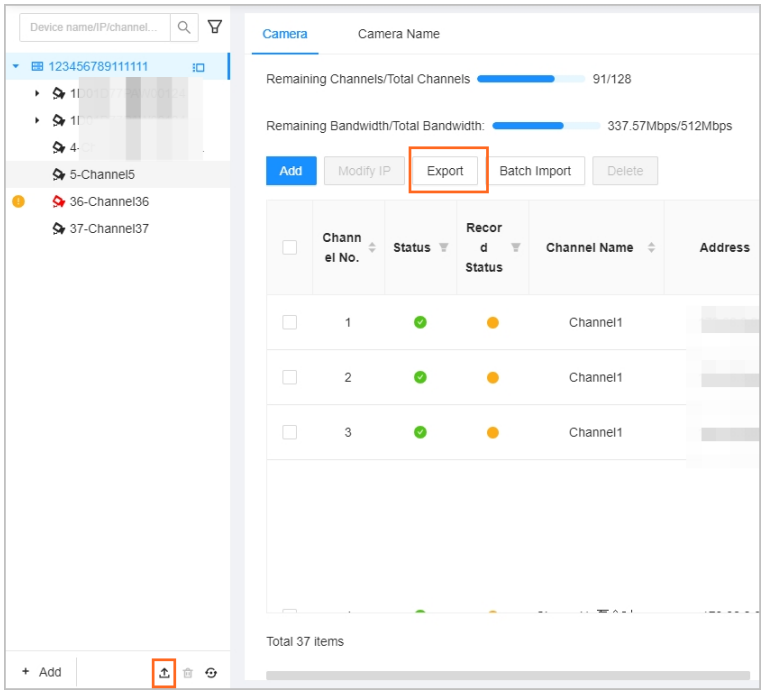
Step 2 Click on the upper-right corner of the page, and then click **Camera**.

You can also click **Camera** from the configuration list on the home page.

Step 3 Click under the device tree or **Export** under the **Camera** tab.

Click **Download Template** to download the template. You can use the template to import remote devices.

Figure 6-10 Export



Step 4 (Optional) Click to enable export encryption.

The exported .backup file is encrypted and cannot be edited. If you do not enable encryption, 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 username (excluding password) of the remote device.

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

Step 5 Click **OK**.

Step 6 Click **Save File**.

File path might be different depending on your operations.

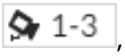
- On the PC client, click , and then select **Download** to view the file storage path.
- On the local interface, you can select a file storage path.
- On the web interface, files are saved to the default downloading path of the browser.

6.1.5 Importing Remote Devices in Batches

Log in to the PC client. Click on the upper-right corner of the page and then click **Camera** . Click **Batch Import** to import remote devices.

6.1.6 Connecting Remote Devices

Log in to the PC client. Click on the upper-right corner of the page and then click **Camera**. You can view connection status of remote devices on the device list.

When the icon of the remote device is black, for example 

, the remote device is online.

When the icon is red, for example 

, the remote device is offline.

- Right-click an offline remote device, and then select **Connect** to connect the remote device.
- Right-click an online remote device, and then select **Disconnect** to disconnect the remote device.
- Right-click an online remote device, and then select **Delete** to delete the remote device.
- Right-click an online device, and then select **Open Device Webpage** to go to the webpage of the remote device.

6.1.7 Deleting Remote Devices

Log in to the PC client. Click on the upper-right corner of the page and then click **Camera**. You can delete the added remote devices one by one or in batches.

- Delete one by one.
  - Select a remote device from the device tree and then click under the device tree.
  - Right-click a remote device on the device tree and then select **Delete**.
  - Under the **Camera** tab, click **Delete** next to **Batch Import** to delete the corresponding remote device.
- Delete in batches.
  - Click next to the root node on the device tree, select multiple remote devices, and then click .
  - On the device list under the **Camera** tab, select a remote device, press Shift and then select another remote device. All remote devices between these two are selected. Click **Delete** next to **Batch Import** to delete them.
  - On the device list under the **Camera** tab, select multiple remote devices, and then click **Delete** next to **Batch Import**.

6.2 Network Management

Log in to the PC client. Click on the upper-right corner of the page and then click **Network**. You can set basic network parameters and applications.

6.2.1 Basic Network

Set basic network parameters of the Device, such as IP address, port aggregation and port number, to make sure the Device can connect with other devices on the network.

6.2.1.1 Configuring IP Address

Set IP address of the Device, DNS server information and other information according to network planning.

Procedure

Step 1 Log in to the PC client.

Step 2 Click on the upper-right corner and then click **Network**.

You can also click **Network** from the configuration list on the home page.

Step 3 Select **Basic Network** > **TCP/IP**.

Step 4 Click to configure the corresponding NIC .

Step 5 Configure the parameters.

Figure 6-11 Edit Ethernet network

Table 6-2 NIC parameters description

Parameter	Description
Rate (Mbps)	The maximum network transmission speed that the current NIC supports.
Type	Select IPv4 or IPv6.
Mode	• **DHCP** : When there is a DHCP server on the network, you can enable DHCP. The system allocates a dynamic IP address to the Device. There is no need to set IP address manually. • **Static** : You need to enter the IP address, subnet mask and gateway.
Test	Test whether the IP address is valid.

Parameter	Description
MTU	Set NIC MTU value. The default setup is 1500 bytes. We recommend you check the MTU value of the gateway first and then set the MTU value of the Device equal to or smaller than the gateway value, which helps to reduce the packets slightly and enhance network transmission efficiency. ⚠ Please be advised that changing MTU value might result in NIC restart, network offline and affect current running operation.

Step 6 Click **OK**.

Step 7 Set DNS server information.

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

- Select **DHCP** so that the Device can automatically get the IP address of the DNS server on the network.
- Select **Static** and then enter the preferred and alternate DNS addresses.

Step 8 Set the default NIC.

Make sure that the default NIC is online.

Step 9 Click **Apply**.

6.2.1.2 Port Aggregation

Bind multiple NICs to create one logic NIC and use one IP address for peripherals. The working mode of bonded NICs work is dependent on the aggregation mode. Port aggregation enhances the network bandwidth and network reliability.

The system supports 3 aggregation modes: load balance, fault tolerance, and link aggregation.

Table 6-3 Aggregation mode description

Aggregation mode	Description
Load balance	The Device bonds several NICs at the same time and use one IP address to communicate with other devices. The bonded NICs are working together to bear the network load. The load balance mode increases the network throughput data amount and enhances the flexibility and availability of the network. In this mode, the network is offline when all NICs break down.
Fault tolerance	The Device bonds several NICs and use one NIC as the main card and the rest as standby. Usually, only the main NIC card is working. The other standby cards automatically take over the job when the main card fails. This mode enhances the reliability of NIC. In this mode, the network is offline when all NICs fail.

Aggregation mode	Description
Link aggregation	The Device bonds several NICs and all NICs are working together to share the network load. The system allocates data to each NIC according to your allocation strategy. Once the system detects that one NIC fails, it stops sending data through this NIC, and transmits the data among the rest NICs. The system calculates transmission data again after the malfunctioning NIC resumes work. In this mode, the network is offline when all bonded NICs fail. Make sure that the switch supports link aggregation and you have configured the link aggregation mode.

6.2.1.2.1 Binding NICs

Procedure

Step 1 Log in to the PC client.

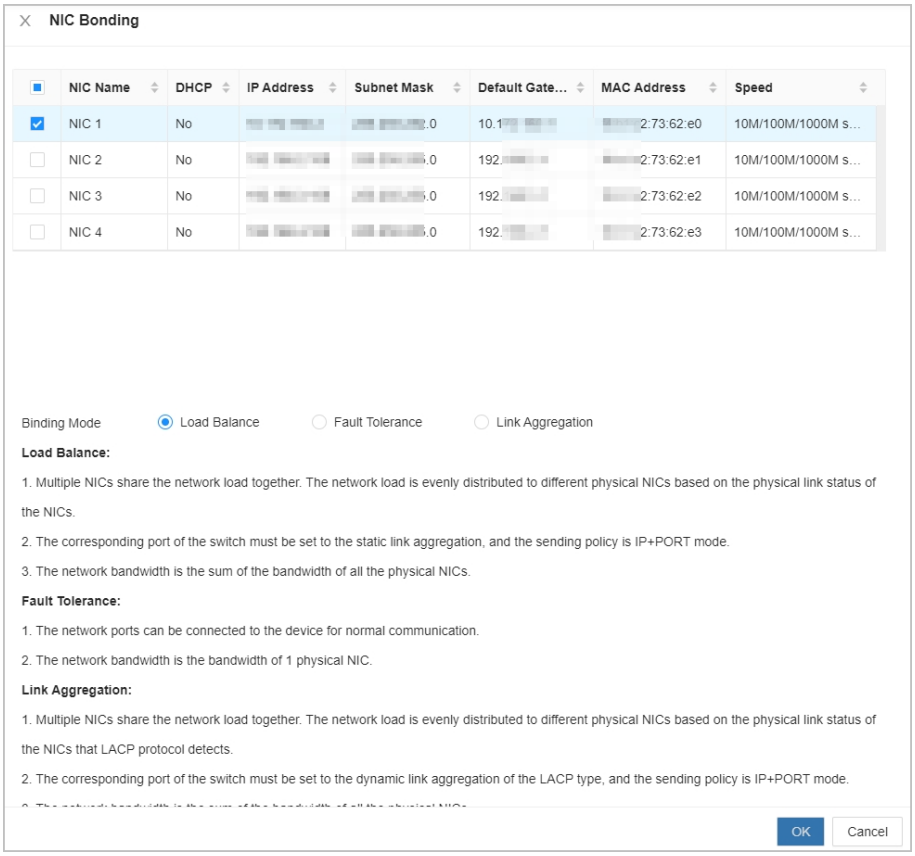
Step 2 Click  on the upper-right corner and then click **Network**.

You can also click **Network** from the configuration list on the home page.

Step 3 Bind NICs.

1. Click **NIC Bonding**.
2. Select the NICs you want to bind.
3. Select an aggregation mode.

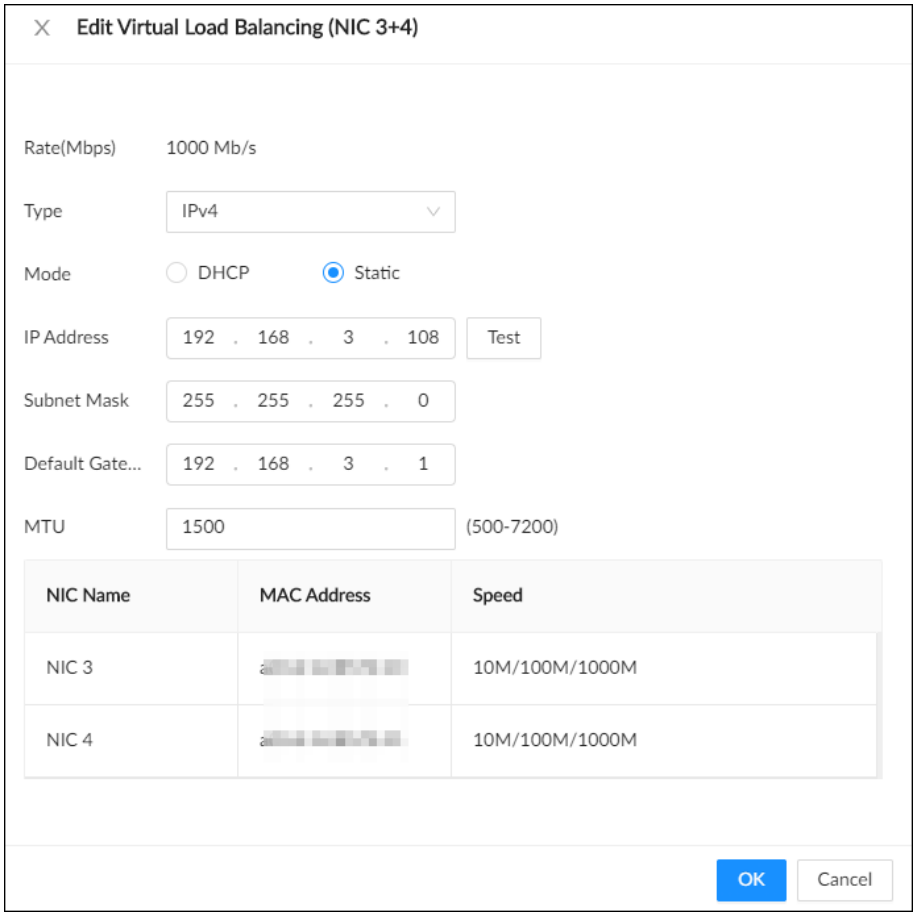
Figure 6-12 NIC bonding



4. Click **OK**.

The setting page varies depending on the aggregation mode you have selected. The following figure is the load balance setting page.

Figure 6-13 Edit load balance



5. Set parameters.

Table 6-4 NIC parameters description

Parameters	Description
Rate (Mbps)	The maximum network transmission speed that the bonded NICs support.
IP Type	Select IPv4 or IPv6.
Use Dynamic IP Address	When there is a DHCP server on the network, you can enable DHCP. The system allocates a dynamic IP address to the Device. There is no need to set IP address manually.
Use Static IP Address	Set a static IP address for the Device. You need to enter a static IP address, subnet mask and gateway.
Test	Test whether the IP address is valid.

Parameters	Description
MTU	Set NIC MTU value. The default setup is 1500 bytes. We recommend you check the MTU value of the gateway first and then set the MTU value of the Device equal to or smaller than the gateway value, which helps to reduce the packets slightly and enhance network transmission efficiency. ⚠ Please be advised that changing MTU value might result in NIC restart, network offline and affect current running operation.

6. Click **OK**.

Step 4 Click **Apply**.

The system pops up a confirmation box.

Step 5 Click **OK**.

The configuration of binding NICs takes effect after the Device restarts.

6.2.1.2.2 Cancelling Binding NIC

Cancel port aggregation so that the NICs are no longer bonded and work as independent NICs.

Procedure

Step 1 Log in to the PC client.

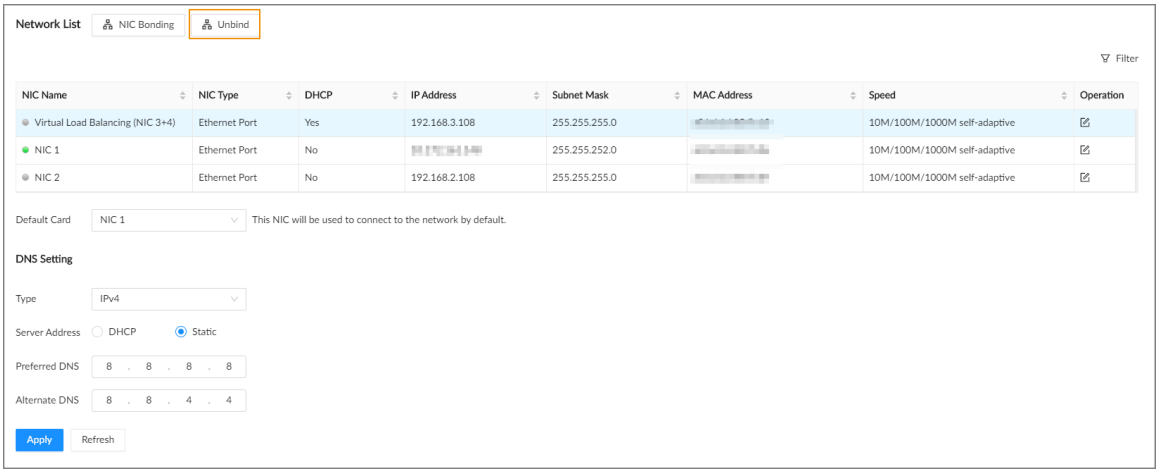
Step 2 Click  on the upper-right corner and then click **Network**.

You can also click **Network** from the configuration list on the home page.

Step 3 Select a bonded NIC.

Step 4 Click **Unbind**.

Figure 6-14 Unbind



Step 5 Click **Apply**.

The system splits the bonded NICs.

Among the split NICs that were bonded together, the first NIC reserves the IP address configured during binding, and the rest NICs restore their default IP addresses.

6.2.1.3 Setting Port Number

Procedure

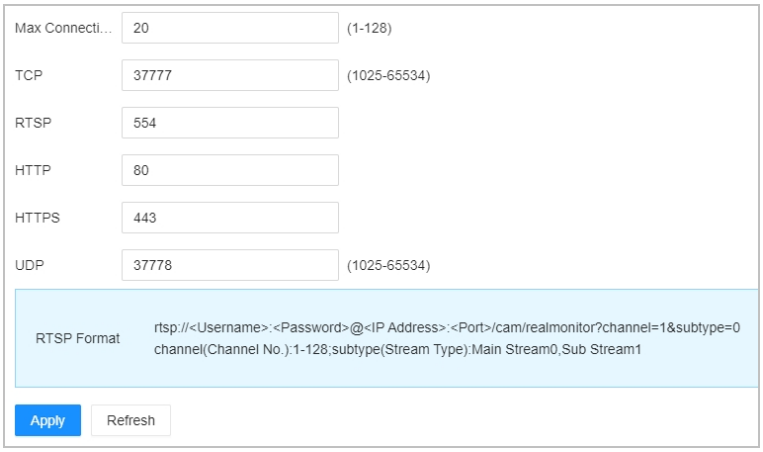
Step 1 Log in to the PC client.

Step 2 Click on the upper-right corner and then click **Network**.

You can also click **Network** from the configuration list on the home page.

Step 3 Select **Basic Network** > **Port**.

Figure 6-15 Port



Step 4 Configure the parameters.

- When you log in via TCP, you do not need to log in again after modifying the max. number of connections, RTSP port, and UDP.
- When you log in with other methods, you need to log in again after you modify the port parameters except max connection.
- Log in again after modifying parameters except **Max Connection**.

Table 6-5 Port parameter description

Parameter	Description
Max Connection	The allowable maximum number of clients accessing the Device at the same time, such as web, PC client, and platform. Select a value between 1 and 128. The default value setting is 20.
TCP	Set the parameter according to the actual requirements. The default value is 37777. The value ranges from 1025 to 65535.
RTSP	Set the parameter according to the actual requirements. The default value is 554. The value ranges from 1 to 65535.
HTTP	Set the parameter 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, remember to add the port number after the IP address when you are using a browser to log in to the device.
HTTPS	Set the parameter according to the actual requirements. The default value is 443. The value ranges from 1 to 65535.

Parameter	Description
UDP	Set the parameter according to the actual requirements. The default value is 37778. The value ranges from 1025 to 65535.

Step 5 Click **Apply**.

The system restarts the corresponding services of the ports.

6.2.2 Network Application

Set the parameters of network applications, so that system can connect to other devices.

Configure the route table so that the system can automatically calculates the best path for data transmission.

Procedure

Step 1 Log in to the PC client.

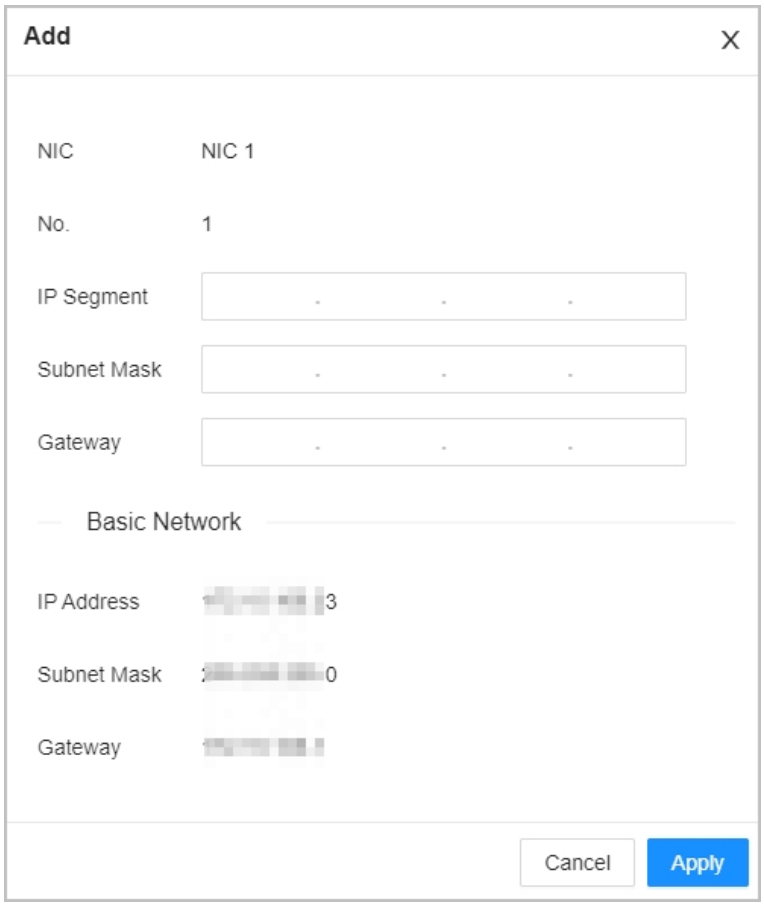
Step 2 Click on the upper-right corner and then click **Network**.

You can also click **Network** from the configuration list on the home page.

Step 3 Select **Network Application** > **Routing Table**.

Step 4 Click **Add**.

Figure 6-16 Add a route table



Step 5 Configure the parameters.

Step 6 Click **Apply**.

6.3 Storage Management

Log in to the PC client. Click on the upper-right corner and then click **Storage**. You can manage storage resources (such as recorded videos) and space to improve the utilization ratio of storage space.

The system supports pre-check and routine inspection, and you can obtain real-time storage status of the Device and avoid data loss.

- Pre-check: During device operation, the system automatically detects disk status in case of change (restarting, inserting and pulling the disk).
- Routine inspection: The system executes t routine inspection on the disks continuously. During device operation, the disk might go wrong due to service life, environment and other factors. You can find out problems during routine inspections.

6.3.1 Storage Resource

6.3.1.1 Local Hard Disk

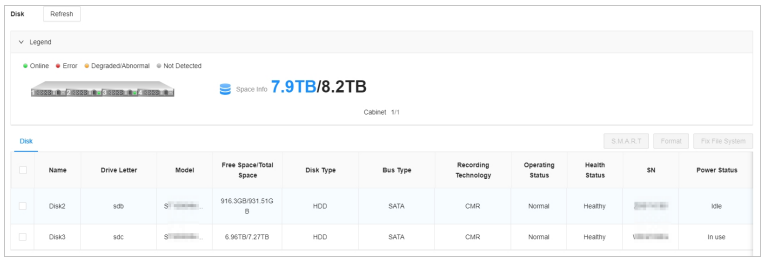
The local hard disk refers to the HDD installed on the system. You can view disk space (free space/ total space), temperature (centigrade/Fahrenheit), disk information and so on.

Click on the upper-right corner, and then select **Storage** > **Storage Resource** > **Disk**. There is a corresponding icon next to the disk name after you create the RAID and hot standby disk.

- : RAID.
- : Global hot spare disk.
- : Invalid disk of RAID group.

Slight difference might be found on the user interface.

Figure 6-17 HDD



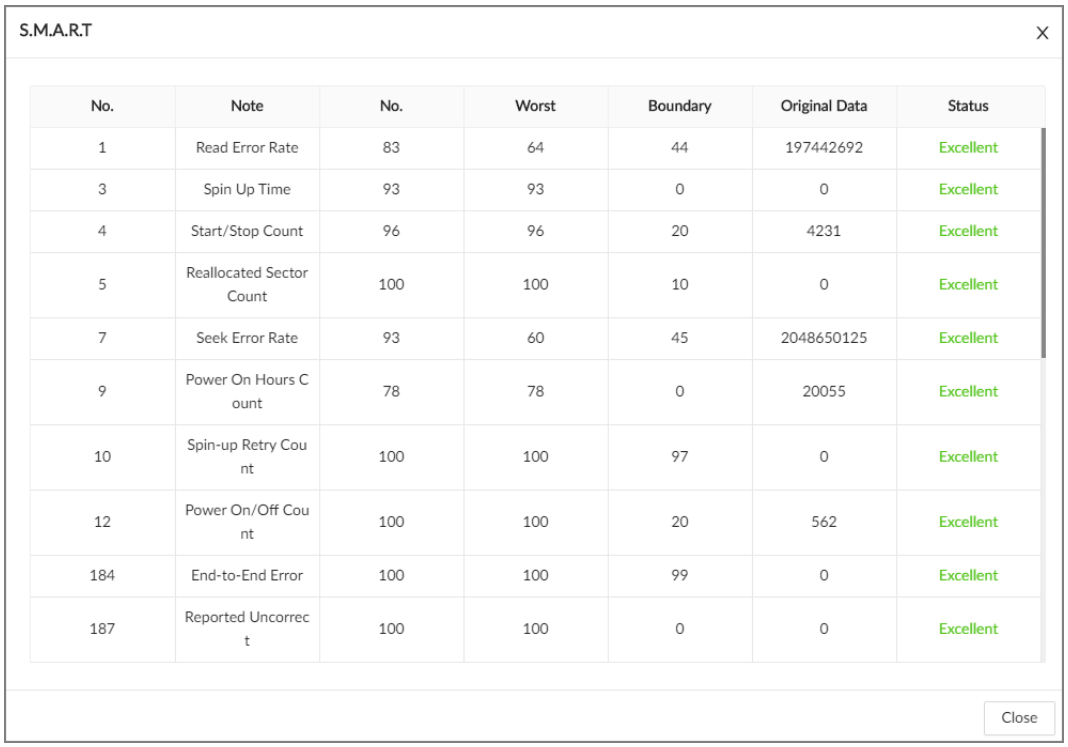
6.3.1.1.1 Viewing S.M.A.R.T

S.M.A.R.T is Self-Monitoring Analysis and Reporting Technology. It is a technical standard to check disk status and report potential problems. The system monitors the disk running status and compares with the specified safety value. Once the status is higher than the specified value, the system displays alarm information to guarantee disk data security.

You can only view S.M.A.R.T information of a disk at one time.

Log in to the PC client. Click on the upper-right corner and then select **Storage** > **Storage Resource** > **Disk**. Select a disk, and then click **S.M.A.R.T**. You can check the disk status. If there is any problem, fix it in time.

Figure 6-18 S.M.A.R.T



6.3.1.1.2 Formatting

- Please be advised that formatting will clear all data on the disk.
- The hot standby disk cannot be formatted.

Log in to the PC client. Click on the upper-right corner and then select **Storage** > **Storage Resource** > **Disk**. Select one or multiple disks, and then click **Format**.

6.3.1.1.3 File System Repair

When you cannot mount the disk or you cannot properly use the disk, you can try to fix the file system.

Log in to the PC client. Click on the upper-right corner and then select **Storage** > **Storage Resource** > **Disk**. Select one or multiple disks, and then click **Fix File System**. You can repair the file system of the corresponding disk. The repaired disk can be mounted and work properly.

6.3.1.2 RAID

RAID (Redundant Array of Independent Disks) is a data storage virtualization technology that combines multiple physical disks into a single logical unit for the purposes of data redundancy, performance improvement, or both.

6.3.1.2.1 Creating RAID

RAID has different levels such as RAID5, RAID6 and more. Different RAID levels are different in data protection, data availability and performance. Create RAID according to your actual requirements.

Please be advised that creating RAID will clear all data on the member disks.

Procedure

Step 1 Log in to the PC client.

Step 2 Click on the upper-right corner and then click **Storage**.

You can also click **Storage** from the configuration list on the home page.

Step 3 Select **Storage Resource** > **RAID**.

Step 4 Click **Add**.

Step 5 Set RAID parameters.

Select a RAID level according to actual situation. You can select **Manual Create** and **One-Click Create**.

- **Manual Create** : The system creates the specified level of RAID using the selected disks.

Figure 6-19 Manual create

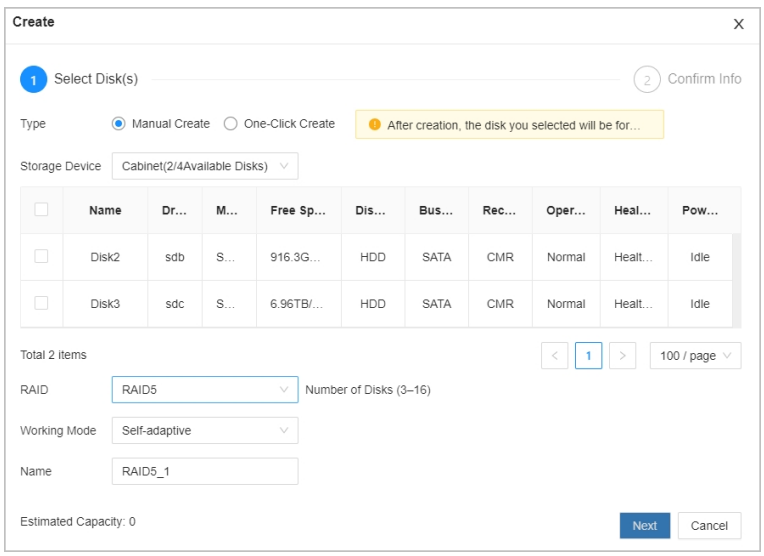


Table 6-6 Manual creation parameters description

Parameter	Description
Storage Device	Select the storage device where the disks are located and select the disks you want to add to the RAID. Different levels of RAID might need different number of disks.
RAID	Select the level of RAID that you want to create.
Working Mode	Set RAID resources allocation mode. The default mode is self-adaptive. ◇ **Self-adaptive** : The system automatically adjusts RAID synchronization speed according to current business load. When there is no external business, the synchronization speed is high. When there is external business, the synchronization speed is low. ◇ **Sync Priority** : The system allocates resources to RAID synchronization first. ◇ **Operation Priority** : The system allocates resources to business first. ◇ **Load Balance** : The system allocates resources to business and RAID synchronization equally.
Name	Set RAID name.

- **One-Click Create** : The system creates RAID5 according to the current number of disks.

Figure 6-20 One-click create

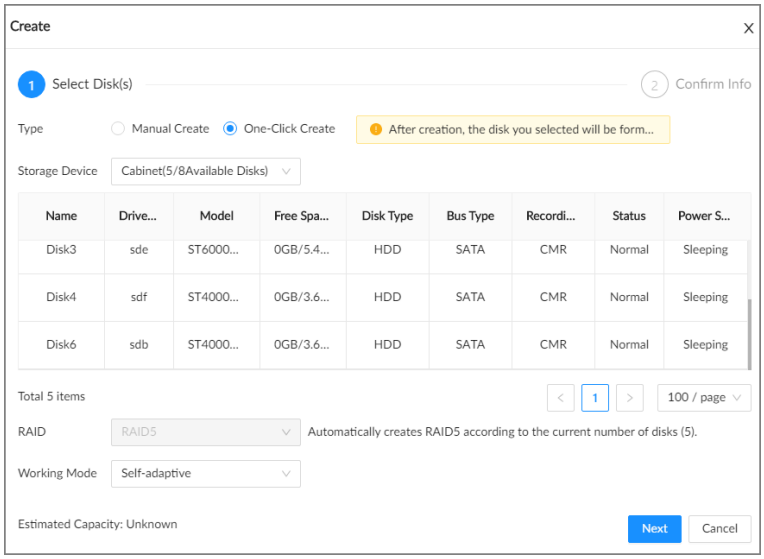


Table 6-7 One-click creation parameters description

Parameter	Description
Storage Device	Select the storage device where the disks are located.

Parameter	Description
Working Mode	Set RAID resources allocation mode. The default mode is self-adaptive. ◇ **Self-adaptive** : The system automatically adjusts RAID synchronization speed according to current business load. When there is no external business, the synchronization speed is high. When there is external business, the synchronization speed is low. ◇ **Sync Priority** : The system allocates resources to RAID synchronization first. ◇ **Operation Priority** : The system allocates resources to business first. ◇ **Load Balance** : The system allocates resources to business and RAID synchronization equally.

Step 6 Click **Next**.

Step 7 Confirm information, and then click **Create**.

If the information is wrong, click **Back** to modify the RAID parameters.

Related Operations

After creating RAID, you can view RAID disk status and details, clear up RAID, and repair file system.

Table 6-8 RAID operations

Name	Operation
View the status of RAID member disks	Click next to the RAID name to open the RAID disk list. You can view the space and status of the member disks.
View RAID details	Click the icon under **Status** to view details on the RAID.
Fix file system	When you cannot mount the RAID or you cannot properly use the RAID, you can try to fix the file system. Select one or multiple RAID groups, and then click **Fix File System**. The repaired RAID can work properly or be mounted.
Modify working mode	Select one or more RAID groups, and then click **Working Mode** to modify the working mode.
Format RAID	Select one and more RAID groups, and then click **Format**. Please be advised that formatting will clear all data on the RAID.
Delete RAID	Select one and more RAID groups, and then click **Delete**. Please be advised that deletion will clear all data on the RAID and destroy the RAID group.

6.3.1.2.2 Creating Hot Spare HDD

When a disk in the RAID group is malfunctioning or has a problem, the hot spare disk can replace the malfunctioning disk to avoid data loss and ensure reliability of the storage system.

Procedure

Step 1 Log in to the PC client.

Step 2 Click on the upper-right corner and then click **Storage**.

You can also click **Storage** from the configuration list on the home page.

Step 3 Select **Storage Resource** > **RAID** > **Hot Standby**.

Step 4 Click **Add**.

Step 5 Select hot standby creation type.

- **Global Hot Standby** : Create a hot standby disk for all RAID groups. Select the storage device and then select one or more disks that you want to add to the global hot standby.

  The system only displays disks with a storage capacity of at least 3 TB.

- **Private Hot Spare** : Create a hot standby disk for a specified RAID group. Click the **Add to** box to select the RAID group that the private hot standby works for and then select one or more disks that you want to add to the private hot standby.

Figure 6-21 Global hot standby

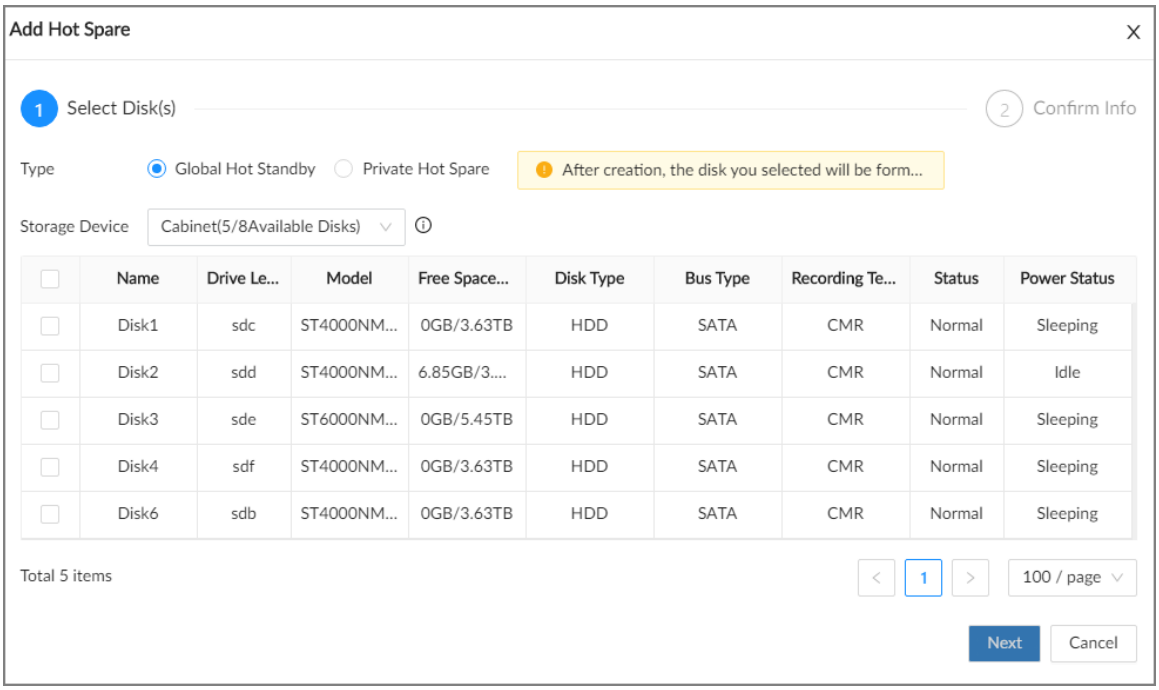
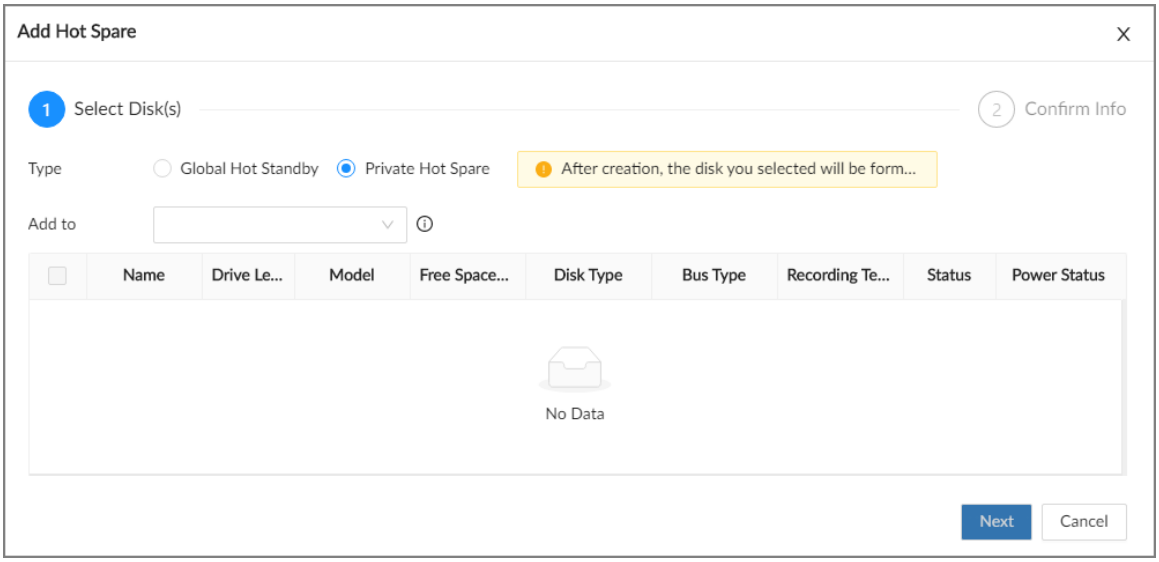


Figure 6-22 Private hot standby



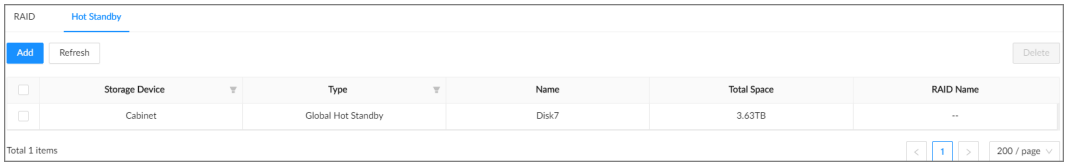
Step 6 Click **Next**.

Step 7 Confirm the information, and then click **Create**.

If the information is wrong, click **Back** to modify the hot standby parameters.

Step 8 Click **Create**.

Figure 6-23 Hot standby



6.3.2 Storage Settings

6.3.2.1 Disk Groups Settings

The installed disks and created RAID groups are allocated to group 1 by default. You can create more disk groups and allocate disks and RAID groups to other groups. The videos and images of all channels are stored in disk group 1 by default. You can allocate the video and image storage of different channels to different disk groups.

6.3.2.2 Recording Schedule

Configure the recording modes and schedules for channels.

6.3.2.2.1 Setting Storage Mode

Configure the storage mode when there is no more disk space available.

Procedure

Step 1 Log in to the PC client.

Step 2 Click on the upper-right corner and then click **Storage**.

You can also click **Storage** from the configuration list on the home page.

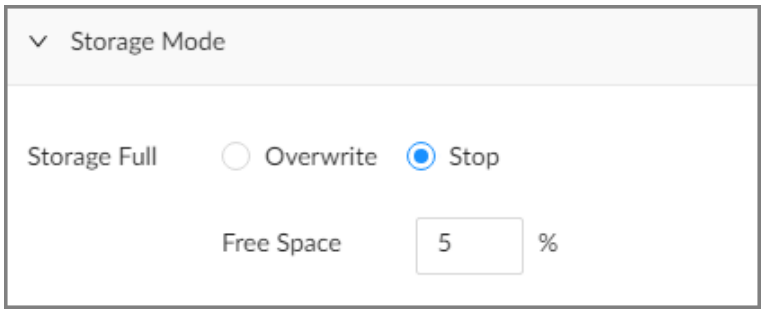
Step 3 Select **Storage** > **Basic**.

Step 4 Set the storage mode.

- **Overwrite** : When the free disk space is less than 100 GB or 2% of the total space (the larger of the two values prevails), the Device deletes 100 GB of the earliest record files and continues to record.

  Data will be overwritten in the **Overwrite** mode. Back up in time.
- **Stop** : When the free disk space is less than the defined free space alarm rate of the total space, an alarm is triggered and the Device continues recording until free disk space is used up.

Figure 6-24 Storage mode



Step 5 Click **Apply**.

6.3.2.2.2 Configuring Recording Mode

Procedure

Step 1 Log in to the PC client.

Step 2 Click on the upper-right corner and then click **Storage**.

You can also click **Storage** from the configuration list on the home page.

Step 3 Select **Storage** > **Record Control**.

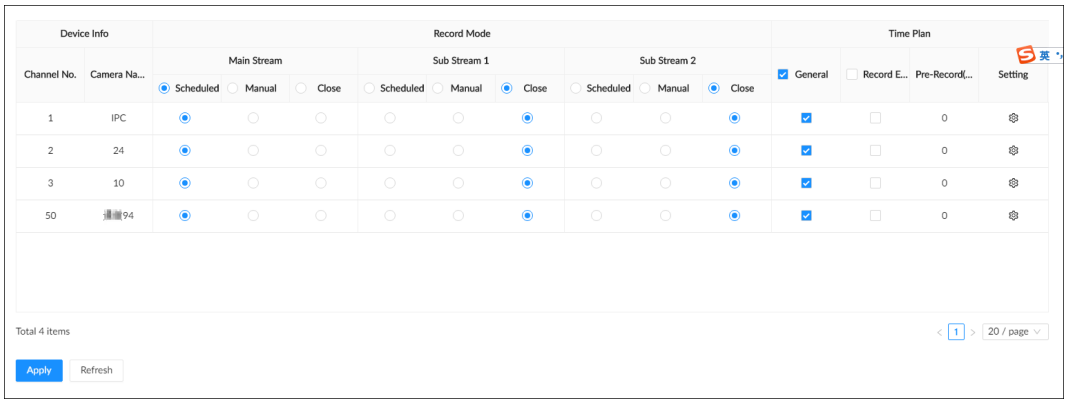
Step 4 Configure the recording mode for each channel.

- **Scheduled** : The Device records automatically according to the schedule.
- **Manual** : The Device records around the clock and does not respond to the recording schedule.
- **Close** : The Device does not record for the channel.

- means that the type is selected.

- **Sub Stream 1** and **Sub Stream 2** cannot be enabled at the same time.

Figure 6-25 Recording Mode



Step 5 Click **Apply**.

6.3.2.2.3 Configuring Recording Schedule

Configure video and picture recording schedules so that the Device records videos and captures pictures as configured in the specified period.

Procedure

Step 1 Log in to the PC client.

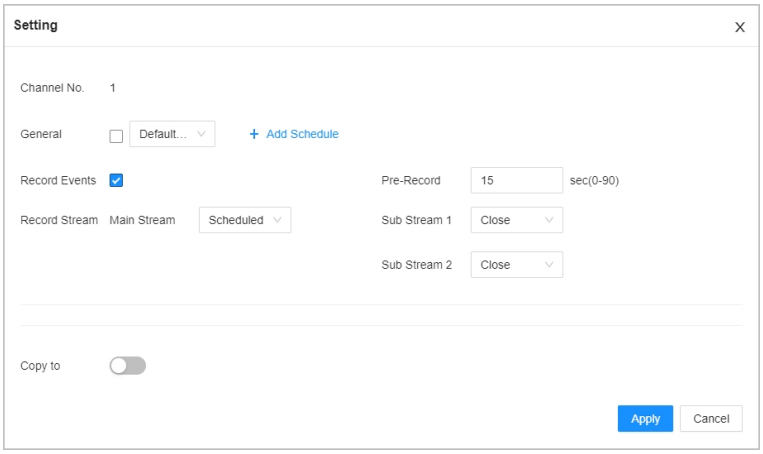
Step 2 Click on the upper-right corner and then click **Storage**.

You can also click **Storage** from the configuration list on the home page.

Step 3 Select **Storage** > **Record Control**.

Step 4 Click , and then set a recording schedule.

Figure 6-26 Set a recording schedule



Step 5 Select **General** , **Record Events**, or both as the recording type.

- **General** : Click the box next to **General** to select a schedule or click **Add Schedule** to add a new schedule. The Device records in the configured schedule.
- **Record Events** : Set the pre-record time. The Device records before an event occurs.

Step 6 Configure other parameters.

Table 6-9 Time plan parameters

Parameter	Description
Genaral	Select the check box, and then click on the drop-down menu. Select schedule, and then enable regular recording during the armed time.
Record Events	Select the check box to enable this feature.
Record Stream	Select stream types and recording modes.
Copy to	Copy the current settings to other channels.

Step 7 Click **Apply**.

6.4 Account Management

The Device adopts two-level account management mode: user and user group. Every user must belong to a group, and one user only belongs to one group. To conveniently manage the users, we recommend the permissions of general users should be lower than those of high-level users.

To ensure device security, you need to enter the correct login password to operate on the **Account** page (for example, add or delete a user).

6.4.1 Adding User Groups

You can create more user groups to manage users with different levels of permissions.

Procedure

Step 1 Log in to the PC client.

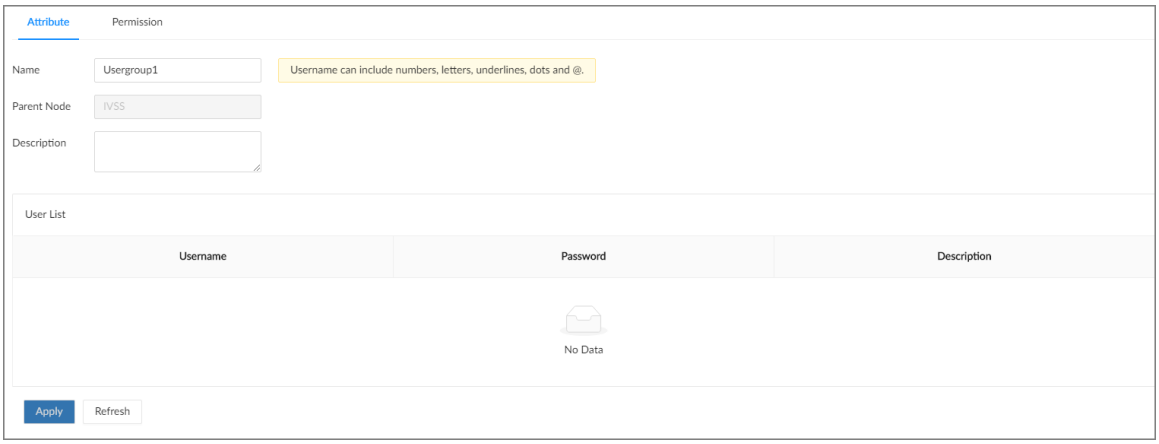
Step 2 Click on the upper-right corner, and then click **Account**.

You can also click **Account** from the configuration list on the home page.

Step 3 Select the root node at the upper-left corner and then click at the lower-left corner.

Step 4 Enter the login password of the current account, and then click **OK**.

Figure 6-27 User group property



Step 5 Configure the parameters.

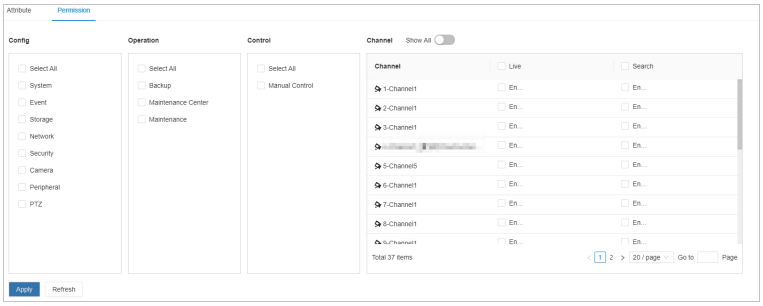
Table 6-10 User group attribute parameters

Parameter	Description
Name	Customize a user group name. The name ranges from 1 to 64 characters. It can contain English letters, numbers and special characters ("_", "@", ".").
Parent Node	Displays the organization node that the user group belongs to. The system automatically recognizes the parent node.
Description	Enter the description for the user group.
User List	Displays users in the group.

Step 6 Select user permissions.

1. Click the **Permission** tab.

Figure 6-28 Permission



2. Select the permissions for the user group.

Step 7 Click **Apply**.

Related Operations

Select a user group, click , enter the login password, and then click **OK** to delete the user group.

- Before you delete a user group, you need to delete all users in the current group first.
- The deleted user group cannot be restored.
- The **admin** user group cannot be deleted.

6.4.2 Adding Device Users

A device user can access and manage the Device. The default administrator is admin. You can add more users with different permissions depending on the user groups that the user belongs to.

Procedure

Step 1 Log in to the PC client.

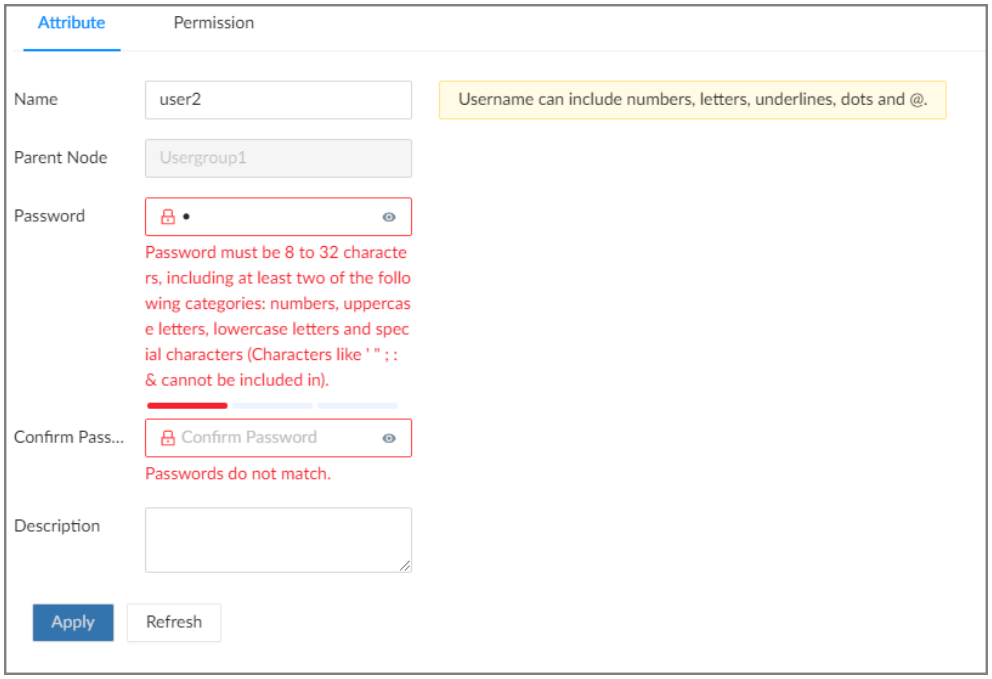
Step 2 Click on the upper-right corner and then click **Account**.

You can also click **Account** from the configuration list on the home page.

Step 3 Select a user group, and then click .

Step 4 Enter the login password of the current account, and then click **OK**.

Figure 6-29 User attributes



Step 5 Configure the parameters.

Table 6-11 User attributes parameters

Parameter	Description
Name	Set the username. The name ranges from 1 to 31 characters. It can contain English letters, number and special character ("_", "@", ".").
Parent Node	Displays the user group that the user belongs to.
Password	Enter the password and then confirm it. Set a strong password according to the on-screen prompt.
Confirm Password	
Description	Enter the description for the user.

Step 6 Click **Permission** to view the permissions of the user.

Step 7 Click **Apply**.

Related Operations

After adding a user, you can modify user information or delete the user.

Only users in the **admin** group have the permission to manage accounts.

- Edit user information.

  Select a user, and then under the **Attribute** tab, you can change the password and description of the user.
- Delete a user.

  Select a user, and then click .

- Before deleting an online user, you need to block the user first.
- The deleted user cannot be restored.

6.4.3 Password Maintenance

Maintain and manage the login passwords of users.

6.4.3.1 Changing Password

Change the login password of the user.

6.4.3.1.1 Changing Password of the Current User

Procedure

Step 1 Log in to the PC client.

Step 2 Select the root node.

Step 3 Click admin at the upper-right corner, and then select **Change Password**.

Step 4 Enter the old password, the new password and then confirm the new password.

Step 5 Click **OK**.

6.4.3.1.2 Changing Password of Other User

Only users in the **admin** group have the permission to change passwords of other users.

Procedure

Step 1 Log in to the PC client.

Step 2 Click on the upper-right corner and then click **Account**.

You can also click **Account** from the configuration list on the home page.

Step 3 Select a user and then click under the **Attribute** tab.

Step 4 Enter the password of the current account, and then click **OK**.

Step 5 Enter the new password and then confirm the password.

Step 6 Click **OK**.

6.4.3.2 Resetting Password

You can use email address or answer the security questions to reset the password if you forgot it.

Procedure

Step 1 Log in to the PC client.

Step 2 Click on the upper-right corner and then click **Account**.

You can also click **Account** from the configuration list on the home page.

Step 3 Select the root node at the upper-left corner.

Step 4 Click to enable the password reset function.

Step 5 Enter an email address for resetting password.

Step 6 Set security questions. You can only set security questions on the local interface of the Device.

Step 7 Click **Apply**.

6.5 Event Management

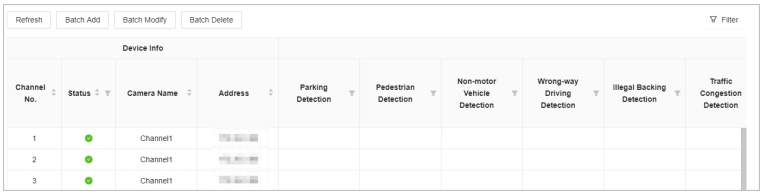
Log in to the PC client. Click on the upper-right corner and then click **Event**.

On the **Event** page, configure alarm events for the Device and remote devices.

- Select the root node on the device tree to set alarm events for the Device.
- Select a remote device on the device tree to set alarm events for the remote device.

- The alarm events might be different depending on the model you purchased.
- means that the corresponding alarm event has been enabled.
- means that AI by camera has been enabled; means that AI by recorder has been enabled; means that both AI by camera and AI by recorder have been enabled.

Figure 6-30 Event management



6.5.1 Local Device

Set the alarm events for the Device and remote device. The alarm events for the device include system anomaly alarm and device disconnection alarm, while the alarm events for remotef device include remote device disconnection alarm.

6.5.1.1 Abnormal Events

Set the alarms for abnormal events such as no available disk, storage errors, and IP conflict.

Table 6-12 Abnormal events

Name	Description
No Available Disks	The system triggers an alarm when there is no available disk. It is enabled by default.
Disk Health Exception	The system triggers an alarm when the SSD health exception occurs.
Storage Error	The system triggers an alarm when a disk error occurs. It is enabled by default.

Name	Description
Low Space	The system triggers an alarm when the used storage space reaches the predefined threshold. It is disabled by default.
RAID Exception	The system triggers an alarm in case of RAID degrade, RAID broken or other RAID exceptions.
Video Frame Loss	The recording video of device has dropped frames, triggering an alarm and it is enabled by default.
IP Conflict	The system triggers an alarm when its IP address conflicts with IP addresses of other devices on the same LAN. It is enabled by default.
MAC Conflict	The system triggers an alarm when its MAC address conflicts with MAC addresses of other devices on the same LAN. It is enabled by default.
Abnormal System Disk	The system triggers an alarm when the system disk is abnormal.
Account Lockout	The system triggers an alarm when the number of failed login attempts has reached the threshold. At the same time, the system locks current account. It is disabled by default. Go to **Security** > **Attack Defense** > **Account Lockout** to set the allowed number of failed login attempts.
Security Exception	The system triggers an alarm when a security issue occurs. It is enabled by default.
AI Module Temp	When the temperature of the AI module is higher than the specified value, the system triggers an alarm. It is enabled by default.
AI Module Disconnected	When the AI module is disconnected from the system, the system triggers an alarm. It is enabled by default.

This section uses no disk as an example. For other events, the setting steps are similar.

Procedure

Step 1 Log in to the PC client.

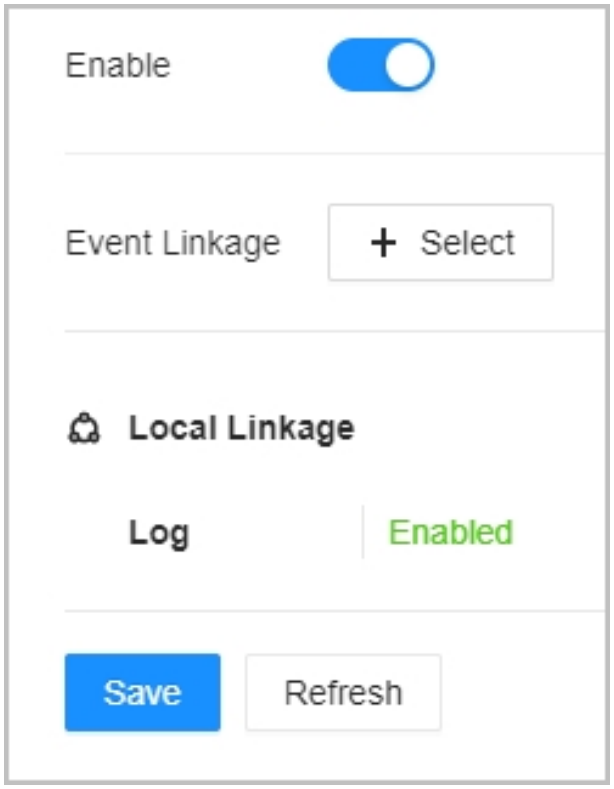
Step 2 Click  on the upper-right corner, and then click **Event**.

You can also click **Event** from the configuration list on the home page.

Step 3 Select the root node on the device tree.

Step 4 Select **Exception** > **No Available Disks**.

Figure 6-31 No svailable disks



Step 5 Click to enable the alarm against no disk.

Step 6 Click **Select** next to **Event Linkage** to set alarm actions.

Step 7 Click **Save**.

6.5.1.2 Offline Alarm

Set the offline alarm for the Device. If you have not set offline alarm for a remote device, once the remote device is disconnected from the system, the system adopts the alarm strategy for the Device to trigger an alarm.

Procedure

Step 1 Log in to the PC client.

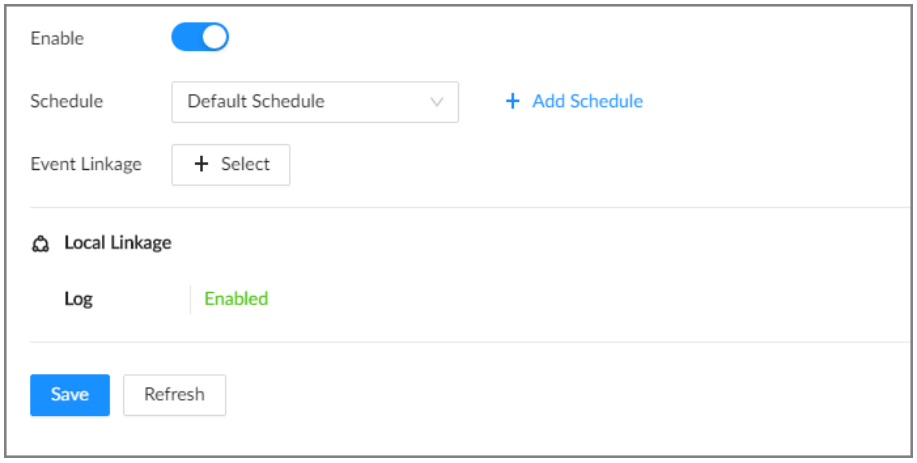
Step 2 Click on the upper-right corner, and then click **Event**.

You can also click **Event** from the configuration list on the home page.

Step 3 Select the root node on the device tree.

Step 4 Select **Offline** > **Offline**.

Figure 6-32 Offline alarm



Step 5 Click to enable the offline alarm.

Step 6 Click **Schedule** to select a schedule from the drop-down list.

The system triggers corresponding alarm actions only during the alarm deployment period.

You can select an existing schedule from the **Schedule** drop-down list or add a new schedule.

Step 7 Click **Select** next to **Event Linkage** to set alarm actions.

Step 8 Click **Save**.

6.5.2 Log

Enable the log function. The system notes down the alarm information in the log when a linkage event occurs.

On the alarm configuration page, click **Select** next to **Event Linkage**, select **Log**, and then click **Apply**.

After the log function is enabled, you can select **Maintenance** > **Log Info** > **Event Logs** on the home page to search for logs.

6.6 System Settings

Log in to the PC client. Click on the upper-right corner and then select **System**. You can configure system settings, such as general parameters, time, and display parameters.

6.6.1 Configuring Basic System Parameters

Set system language, standard, user logout time, virtual keyboard, and mouse moving speed.

Procedure

Step 1 Log in to the PC client.

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

You can also click **System** from the configuration list on the home page.

Step 3 Configure the parameters.

Figure 6-33 Basic system settings

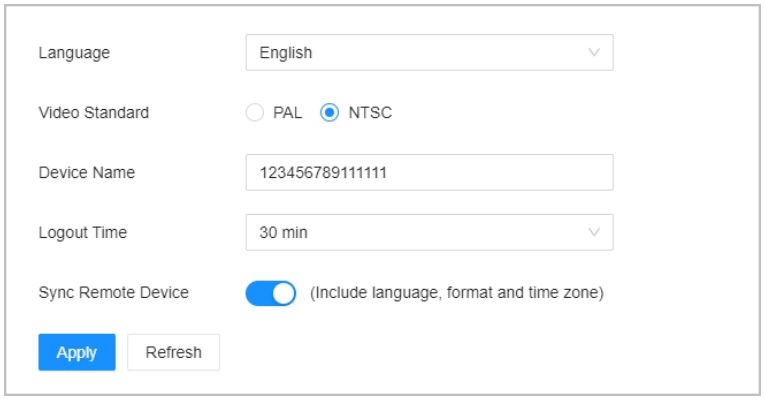


Table 6-13 System parameters description

Parameter	Description
Language	Set the system language.
Video Standard	Select a video standard. • PAL is mainly used in China, Middle East and Europe. • NTSC is mainly used in Japan, United States, Canada and Mexico. As the technical standard of processing video and audio signals, PAL and NTSC mainly differ in the encoding and decoding modes and field scanning frequency.
Device Name	Customize a name for the Device.
Logout Time	Enter the time of inactivity before logout. The Device logs out automatically after the period of inactivity. If you select **None**, the Device does not automatically log out.
Sync Remote Device	Click to synchronize the system settings such as language and time zone with remote devices.

Step 4 Click **Apply**.

6.6.2 System Time

Set system time, and enable the NTP function according to your need. After you enable the NTP function, the Device can automatically synchronize time with the NTP server.

Procedure

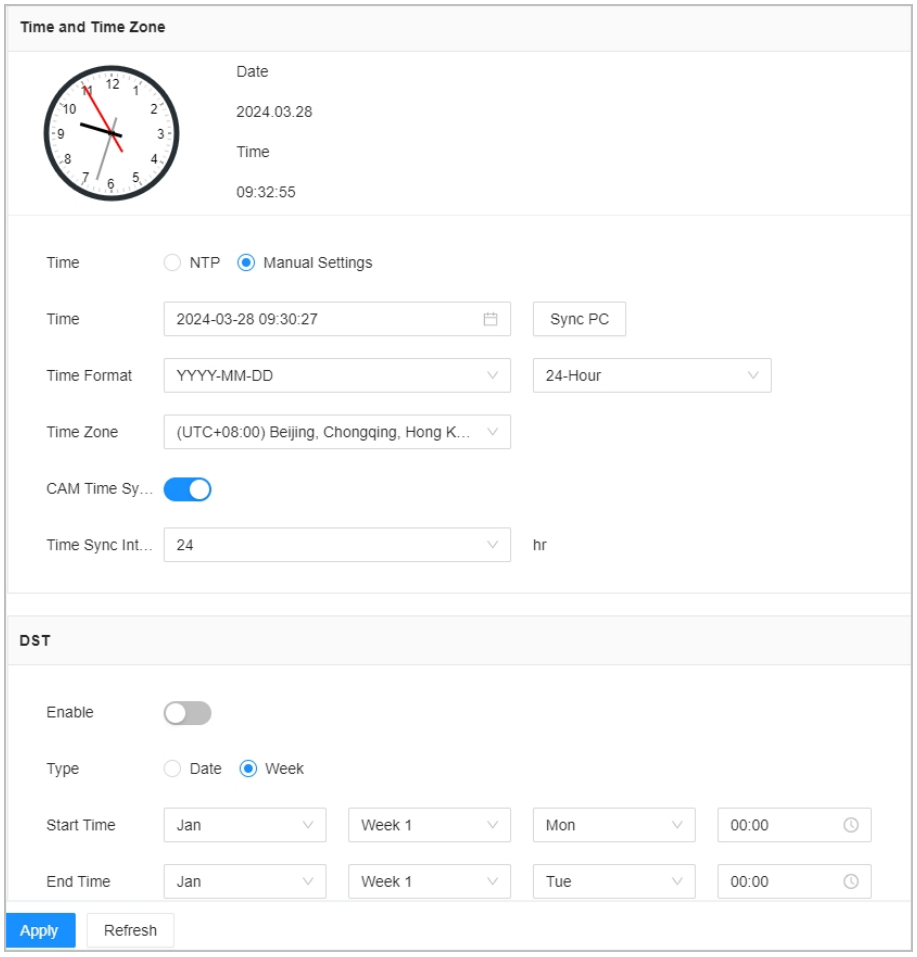
Step 1 Log in to the PC client.

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

You can also click **System** from the configuration list on the home page.

Step 3 Select **General** > **Time**.

Figure 6-34 Time



Step 4 Configure the parameters.

Table 6-14 Time parameters description

Parameters	Description
Time	Set system date and time. You can set the time manually or enable NTP so that the Device can automatically synchronize time with the NTP server. ● **Manual Settings** : Set the actual date and time in either of the following ways. ◇ Click , and then select the time and date in the calendar. ◇ Click **Sync PC** to synchronize system time with your computer. ● **NTP** : Enter the IP address or domain of the NTP server, and then set the time synchronization interval.
Time Format	Set the time and date format.
Time Zone	Select a time zone.

Parameters	Description
CAM Time Sync	After you enable this function, IVSSIVD detects the system time of remote devices once in every interval. When the time of a remote device is inconsistent with IVSSIVD time, IVSSIVD will calibrate the time of the remote device automatically.

Step 5 (Optional) Set DST.

DST is a system to stipulate local time 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 a DST mode from **Date** and **Week**.
3. Set DST start time and end time.

Step 6 Click **Apply**.

6.6.3 Time Plan

When you are configuring alarm, recording and other settings, you can use the schedule to define the validity periods. The system only triggers the corresponding operations during the specified schedule.

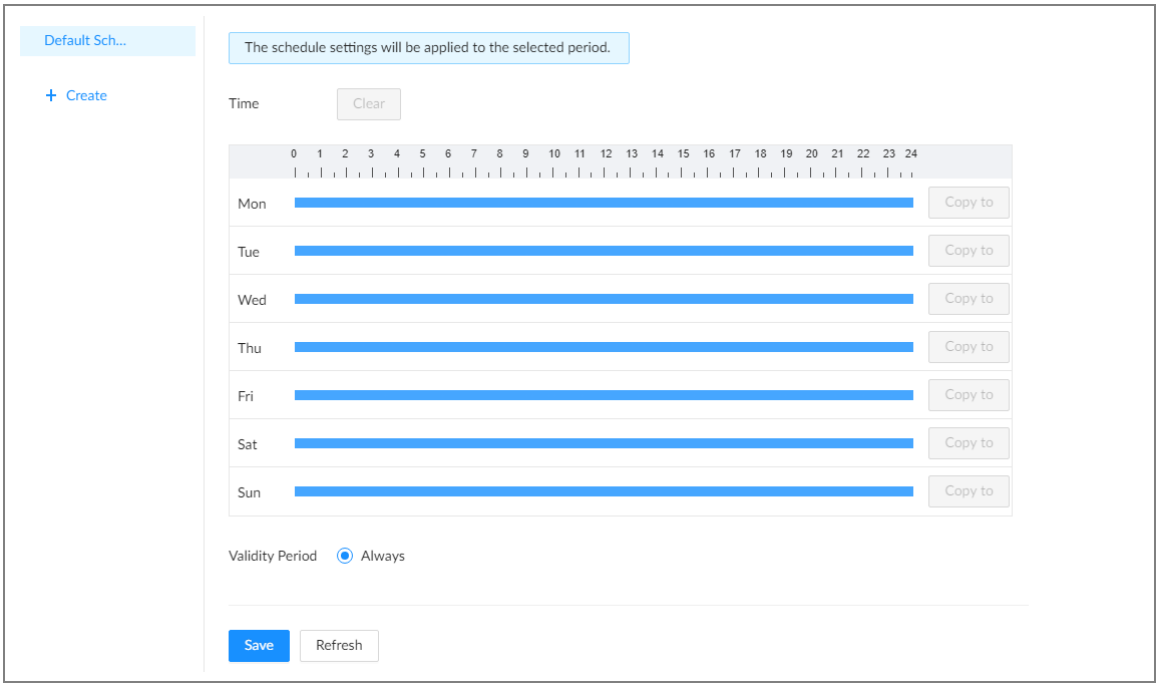
Default Schedule has been created by default, which is always effective and cannot be modified or deleted.

Procedure

Step 1 Log in to the PC client.

Step 2 On the configuration page, select **System** > **Time Plan** > **Time Plan**.

Figure 6-35 Time plan



Step 3 Add a schedule.

1. Click **Create**.
2. Click  to edit the schedule name.

Step 4 Set the validity periods.

- **Always** : The schedule is always effective.
- **Custom** : Customize validity periods for the schedule. Click the time bar, and then drag the blue strip to set a period.

  - ◇ You can add up to 50 validity periods for each schedule.
  - ◇ Click **Clear** to clear all validity periods.
  - ◇ Click a blue strip, and then click **Delete** to delete the corresponding period.
  - ◇ Click **Copy** to copy the current settings to other dates.

Step 5 Click **Save**.

Related Operations

Select a schedule and then click  to delete it.

6.7 Security

6.7.1 Security Status

Background Information

Security scanning helps get a whole picture of the device security status.

- User and service detection: Detects whether the current login authentication, user status, and configuration security conform to recommended settings.
- Security modules scanning: Scans the running status of the security modules such as attach defense, log security and session security.

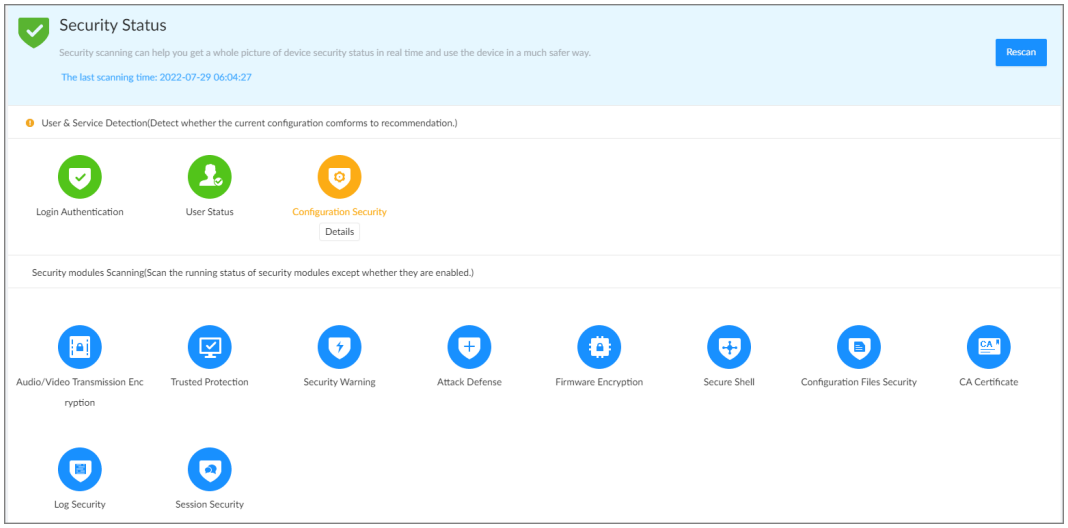
Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **Security** > **Security Status**.

Step 3 Click **Rescan**.

Figure 6-36 Security status



Related Operations

Different colors indicate different security statuses (green: normal; yellow: abnormal). For abnormal items, you can click **Details** to view details.

- Click **Ignore** to ignore the abnormal item. The item will not be checked in subsequent scans.

  Click **Rejoin Detection** to include the ignored item into the security scan.
- Click **Optimize** to go to the corresponding configuration page where you can optimize the security settings.

6.7.2 System Service

6.7.2.1 Basic Services

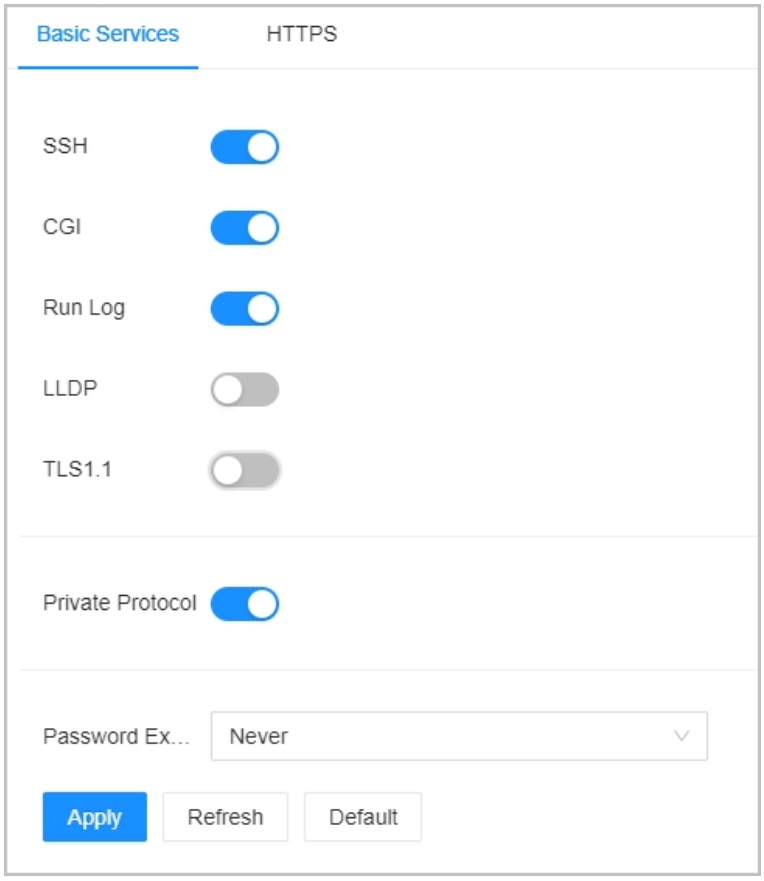
Enable basic system services for third-party access.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **Security** > **System Service** > **Basic Services**.

Figure 6-37 Basic services



Step 3 Enable or disable system services.

Table 6-15 System services

Name	Description
SSH	After enabling this function, you can access the Device through SSH protocol to carry out system debugging and IP configuration. This function is disabled by default. For data security, we recommend you disable this function when it is not needed.
CGI	After this function is enabled, a third-party platform can connect the Device through CGI protocol. For data security, we recommend you disable this function when it is not needed.
Run Log	After enabling it, you can view system running logs in **Maintenance Center** > **Advanced Maintenance** > **Run Log**.
LLDP	Enable this function to help the network administrator identify the device.
TLS1.1	Enable the protocol compatibility.

Name	Description
Private Protocol	After enabled, the device can be accessed through this protocol.
Password Expires in	Configure the password expiration interval. The Device prompts you to change the password when it expires.

Step 4 Click **Apply**.

6.7.2.2 Enabling HTTPS

HTTPS can use the reliable and stable technological means to guarantee user information and device security and communication data security. After you install the certificate and enable HTTPS function, you can use your computer to access the Device through HTTPS. To reduce the risk of data leakage, we recommend you enable the HTTPS service.

Prerequisites

Install the certificate.

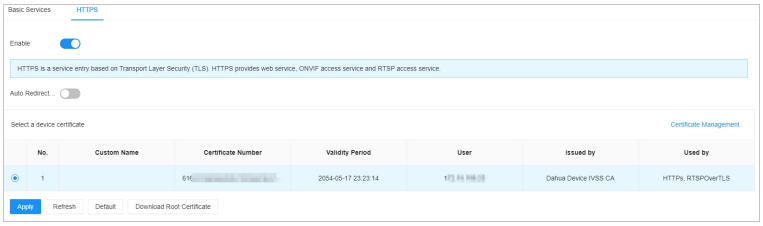
Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **Security** > **System Service** > **HTTPS**.

Step 3 Click  to enable HTTPS function.

Figure 6-38 HTTPS



Step 4 (Optional) Click  to enable **Compatible with TLSv1.1 and earlier versions**.

TLS (Transport Layer Security) provides privacy and data integrity between two communications application programs.

Step 5 Click **Apply**.

You can use HTTPS to access the webpage.

Open the browser, enter https://*IP address:port* in the address bar, press Enter, and then you can log in to the webpage.

- IP address is IP address or the domain name of the Device.
- Port refers to HTTPS port number of the Device. If the HTTPS port is the default value 443, just use https://*IP address* to access the webpage.

6.7.3 Attack Defense

6.7.3.1 Configuring Firewall

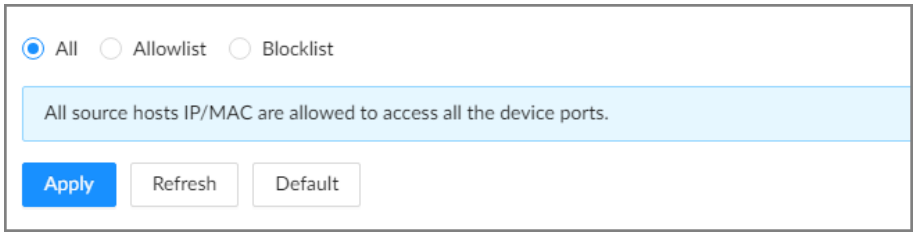
You can configure the hosts that are allowed or prohibited to access the Device.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **Security** > **Attack Defense** > **Firewall**.

Figure 6-39 Firewall



Step 3 Select a firewall mode.

- **All** : All hosts can access the Device.
- **Allowlist** : The hosts on the allowlist can access the Device.
- **Blocklist** : The hosts on the blocklist are prohibited to access the Device.

Allowlist and blocklist cannot be used at the same time.

Step 4 If you select **Allowlist** or **Blocklist**, click **Add** to add an allowlist or blocklist.

You can allow or prohibit a specific IP address, IP addresses on a specific network segment, or a specific MAC address to access the Device.

Step 5 Click **Apply**.

6.7.3.2 Account Lockout

You can configure the number of allowed failed login attempts. When the number of failed login attempts reaches the defined threshold, the account will be locked for the defined duration.

Procedure

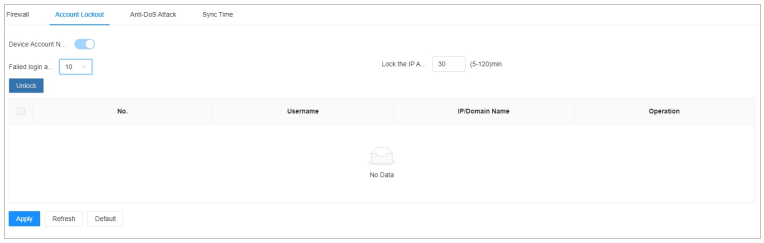
Step 1 Log in to the PC client.

Step 2 On the home page, select **Security** > **Attack Defense** > **Account Lockout**.

Step 3 Set the different account lockout parameters.

- Failed login attempts reached: Set the maximum number of consecutive login errors allowed. When the number of login errors reaches or exceeds the set value, the system will lock out the main server.
- Lock the IP Address: Set the time for each lockout main server.

Figure 6-40 Account lockout



Step 4 Click **Apply**.

6.7.3.3 Anti-Dos Attack

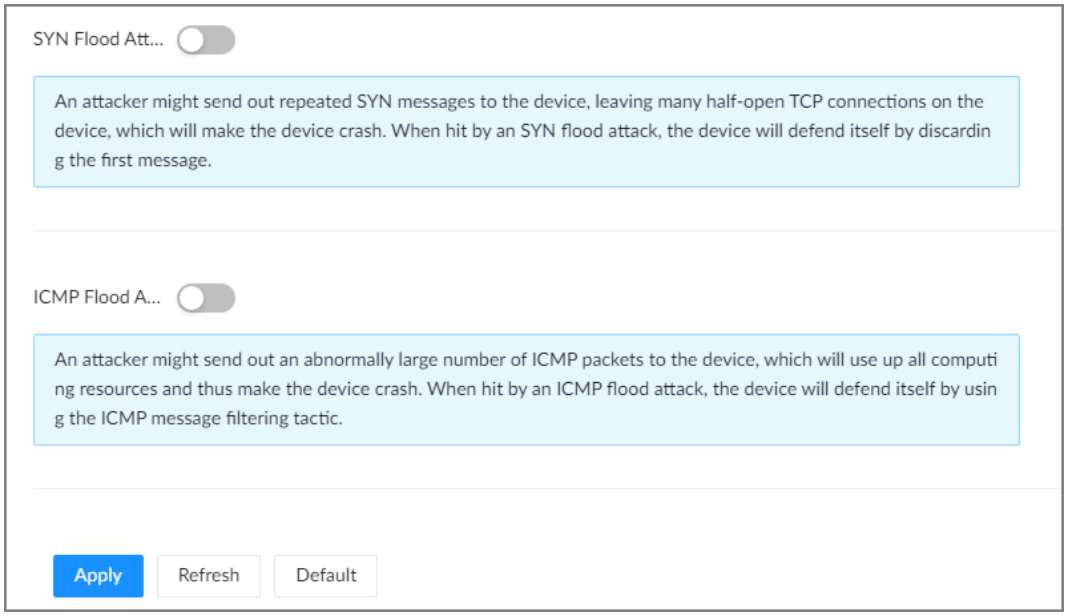
You can enable **SYN Flood Attack Defense** and **ICMP Flood Attack Defense** to defend the Device against Dos attacks.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **Security** > **Attack Defense** > **Anti-Dos Attack**.

Figure 6-41 Account lockout



Step 3 Click to enable **SYN Flood Attack Defense** or **ICMP Flood Attack Defense**.

Step 4 Click **Apply**.

6.7.3.4 Sync Time

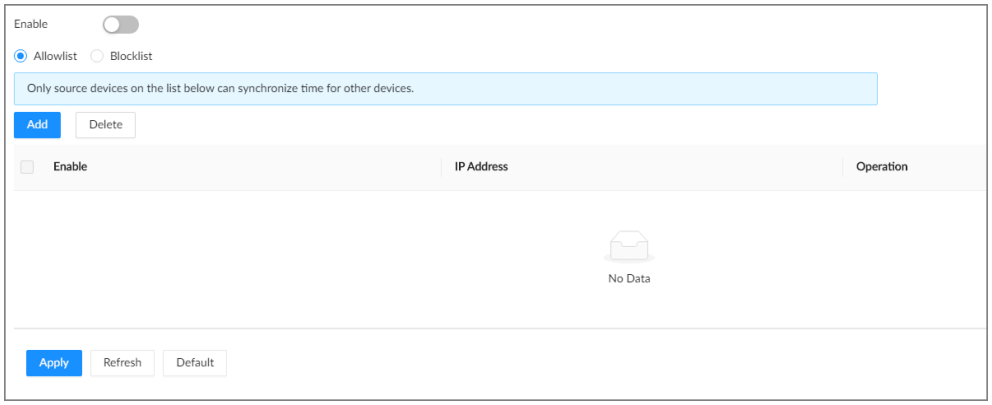
Configure permissions of time synchronization actions from other devices or servers.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **Security** > **Attack Defense** > **Sync Time**.

Figure 6-42 Sync time



Step 3 Click  to enable time synchronization restriction.

Step 4 Select **Allowlist** or **Blocklist**.

- **Allowlist** : Hosts on the allowlist have the permission to synchronize time of the Device.
- **Blocklist** : Hosts on the blocklist cannot synchronize time of the Device.

Step 5 Click **Add** to add an allowlist or blocklist.

1. Select an IP version. Only support IPv4.
2. Enter an IP address.
3. Click **OK**.

Step 6 Click **Apply**.

6.7.4 CA Certificate

A CA certificate is a digital certificate issued by a certificate authority (CA). The CA verifies trusted certificates for trusted roots. Trusted roots are the foundation upon which chains of trust are built in certificates.

6.7.4.1 Installing the Created Certificate

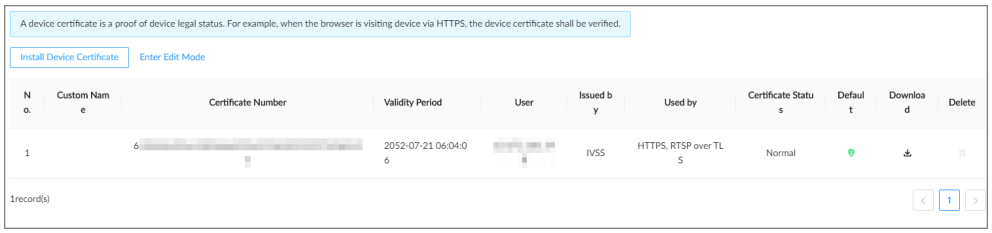
A device certificate is a proof of device legal status. For example, if you want to access the Device through a browser, you need to install the root certificate on your computer in advance.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **Security** > **CA Certificate** > **Device Certificate**.

Figure 6-43 Device certificate

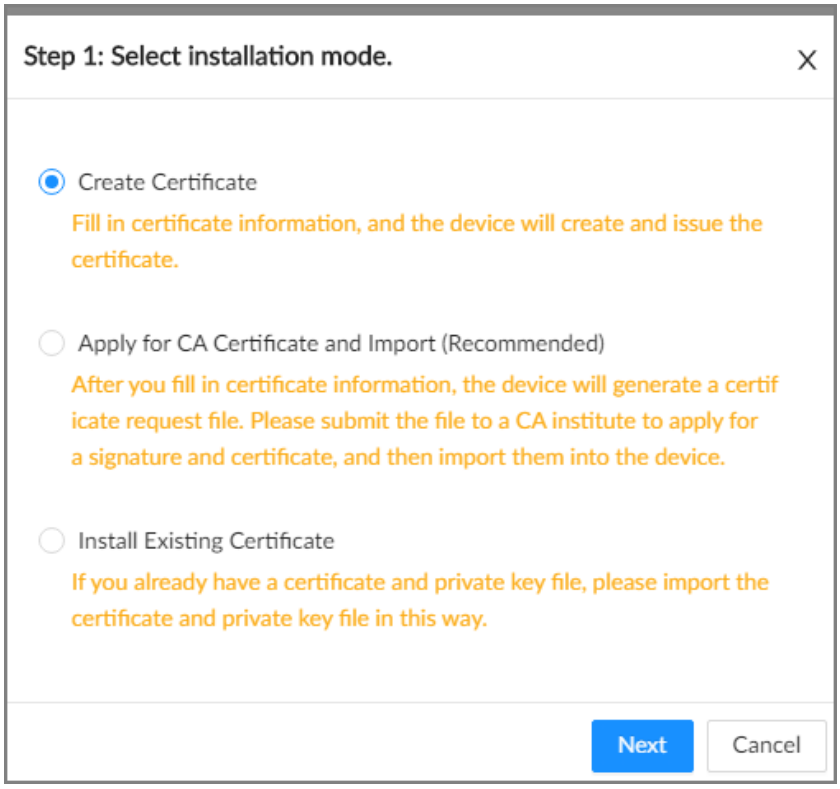


Step 3 Click **Install Device Certificate** to install a certificate in any of the following ways.

- Create a certificate.

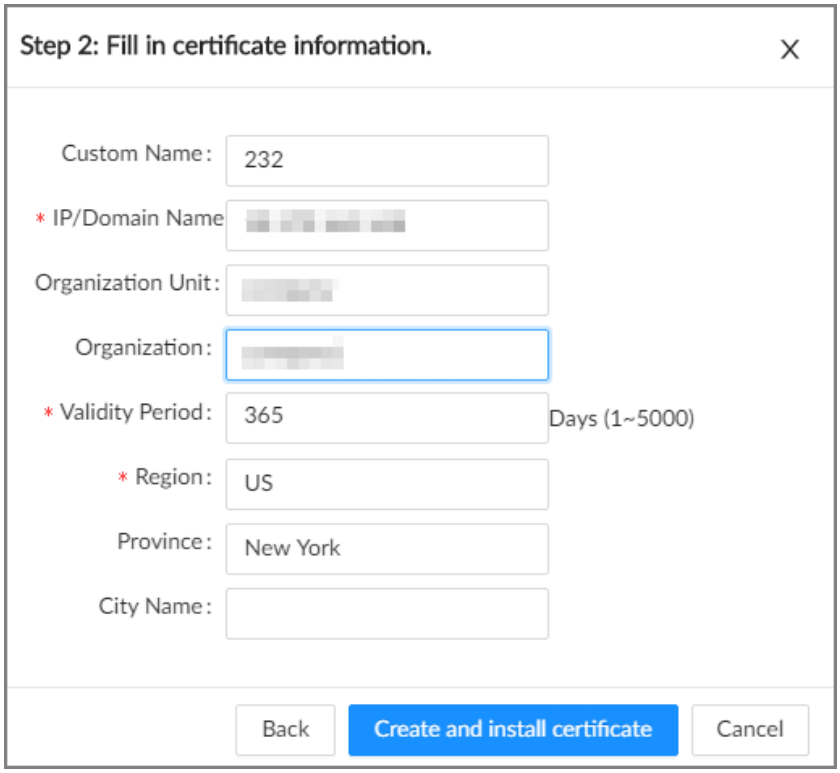
1. Select **Create Certificate** and then click **Next**.

Figure 6-44 Create certificate



2. Enter the information.

Figure 6-45 Certificate information

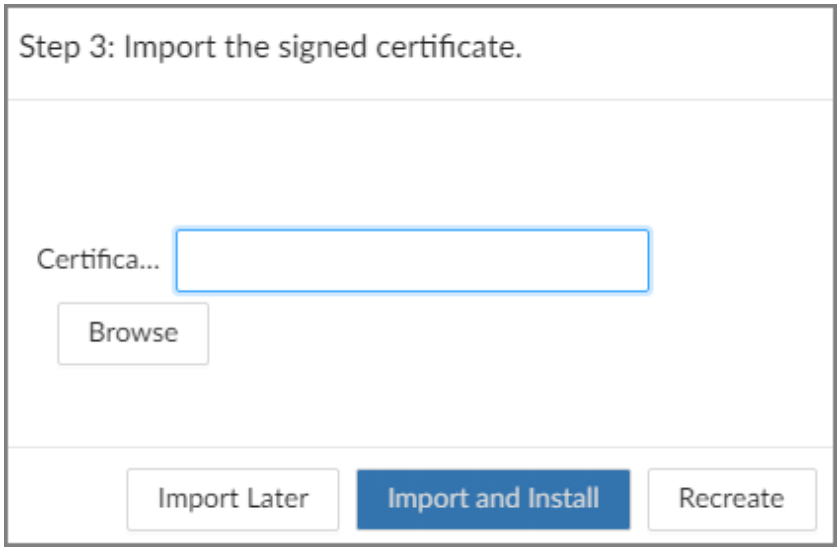


3. Click **Create and install certificate**.

- Apply for and import a certificate.

1. Select **Apply for CA Certificate and Import (Recommended)** and then click **Next**.
2. Enter the information.
3. Click **Create and Download**. The Device creates and downloads a certificate request file. Submit the file to a CA institute to apply for a signed certificate.
4. Click **Browse** to select the certificate.

Figure 6-46 Import the certificate



5. Click **Import and Install**.

- Import an existing certificate.

1. Select **Install Existing Certificate** and then click **Next**.
2. Enter the information.
3. Click **Browse** to select the certificate and private key.
4. Enter the password for the private key.
5. Click **Import and Install**.

Related Operations

You can edit and download the installed certificate.

- Edit

  Click **Enter Edit Mode** , enter a custom name for the certificate, and then click **Save Config**.
- Download

  Click to download the certificate.

6.7.4.2 Installing the Trusted Certificate

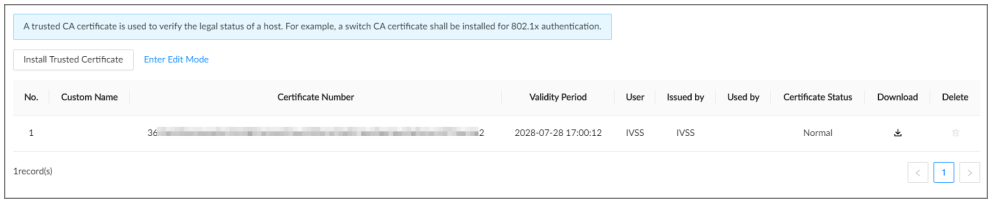
A trusted CA certificate is used to verify the legal status of a host. When a device connect to a local area through 802.1x authentication, it needs to verify the CA certificate.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **Security** > **CA Certificate** > **Trusted CA Certificates**.

Figure 6-47 Trusted CA certificate



Step 3 Click **Install Trusted Certificate**.

Step 4 Click **Browse** to select a trusted certificate.

Step 5 Click **OK**.

Related Operations

You can edit and download the installed certificate.

- Edit

  Click **Enter Edit Mode** , enter a custom name for the certificate, and then click **Save Config**.
- Download

  Click to download the certificate.

6.7.5 A/V Encryption

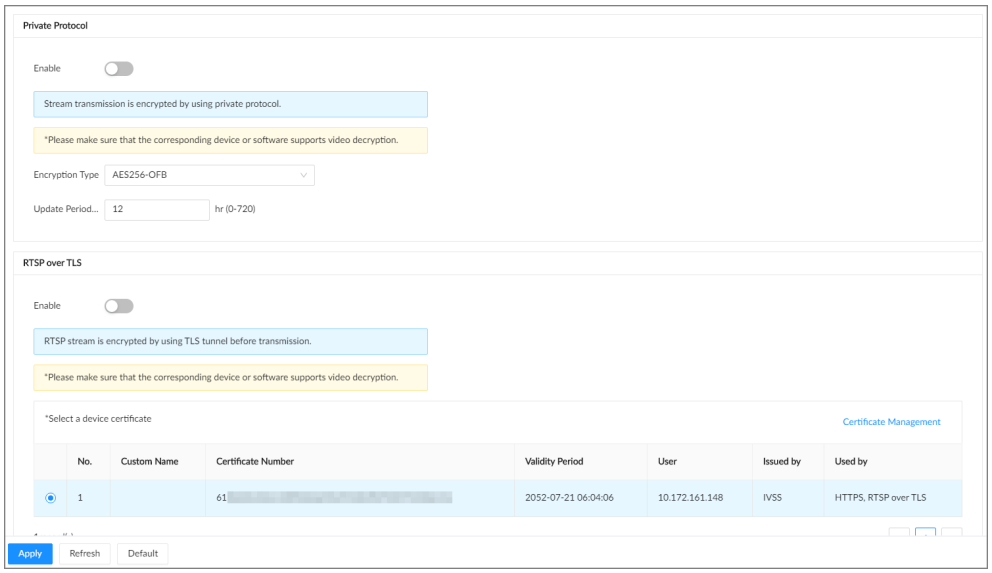
The Device supports audio and video encryption during data transmission.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **Security** > **A/V Encryption** > **Encrypted Transmission**.

Figure 6-48 Video encryption



Step 3 Configure the parameters.

Table 6-16 Encryption parameters

Encryption Method	Description
Private Protocol	Click to enable encryption using the private protocol. • **Encryption Type** : Leave it as default. • **Update Period of Secret Key** : The value range from 0 hours through 720 hours. 0 means never update the secret key.
RTSP over TLS	Click to enable RTSP encryption using the TLS tunnel, and then select a device certificate. We recommend you enable this function to ensure data security. You can click **Certificate Management** to install a device certificate.

Step 4 Click **Apply**.

6.7.6 Security Warning

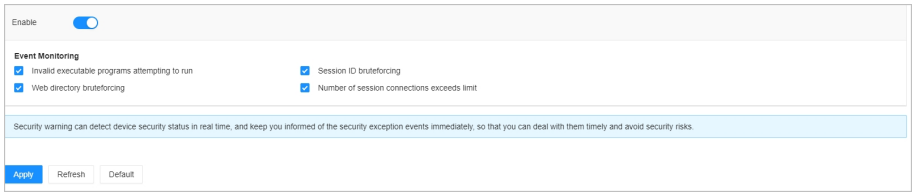
The Device gives warnings to the user when a security error occurs.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **Security** > **Security Warning**.

Figure 6-49 Security warning



Step 3 Click to enable the function.

Step 4 Select the events to be monitored.

Step 5 Click **Apply**.

6.7.7 Security Authentication

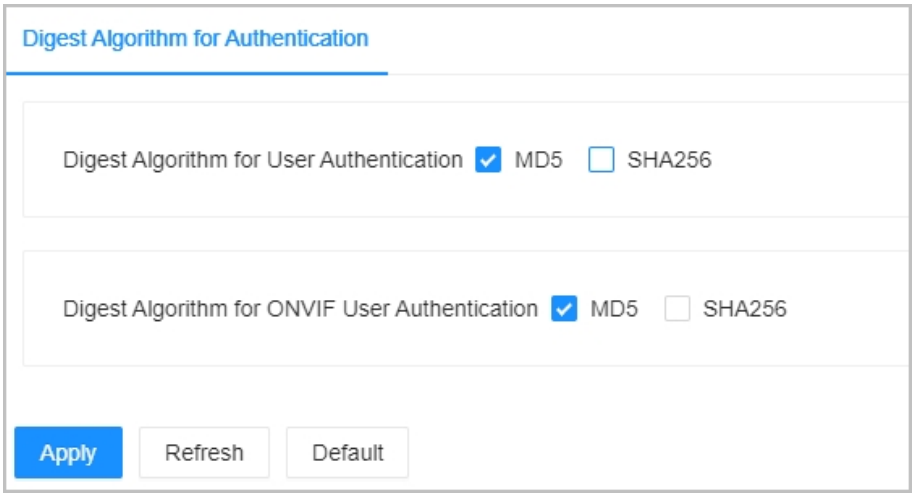
Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **Security** > **Security Authentication**.

Step 3 Select digest algorithm for authentication.

Figure 6-50 Security Authentication



Step 4 Click **Apply**.

7 General Operations

This chapter introduces general operations such as live view, playback, alarm, and more.

7.1 Live and Monitor

Log in to the PC client, and then view the live videos under the **Live** tab.

Point to the left and right edges of the video windows, and then click or to hide or display the left and right columns.

Figure 7-1 Live view

Table 7-1 Live page description

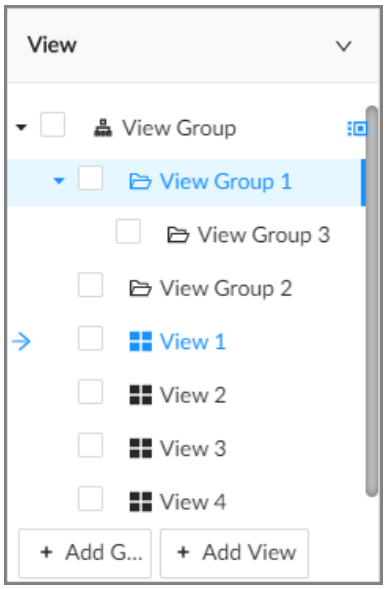
No.	Description
1	Device tree. Displays added remote devices.
2	View zone. Displays the created views and view groups.
3	PTZ control zone.
4	Layout adjustment. • Click to set the layout. • Click or to switch the channel.
5	• Click to edit the view window. • Click to set attribute display.
6	Features panels. A features panel appears when the system detected a target according to the configured rule.

7.1.1 View Management

A view is composed of video images of several remote devices. Go to the view panel at the lower-left corner of the **Live** tab to check and open the view.

- **View Group** is created by default, under which you can create view groups and views.
- Double-click a view or drag the view to the play panel in the middle of the **Live** tab. The Device begins playing the real-time video from the remote device in the view.
- Click to select views, view groups and their sub-nodes.

Figure 7-2 View



7.1.1.1 View Group

A view group is a group of views. The view group helps you to categorize, search for and manage views quickly. Under **View Group** created by default, you can create view groups.

Background Information

- You can create up to 100 view groups.
- The views hierarchy must not be more than 2. For example, after you create View Group 1 under **View Group**, you can create a sub-level View Group 2 under View Group 1. However, you cannot create a sub-level group under View Group 2.

Procedure

Step 1 Log in to the PC client.

Step 2 Under the **Live** tab, click **View Group** or a view group under it, and then click **Add Group**.

You can also right-click an existing view group and then click **Add Group**.

Step 3 Set the view group name.

- The group name consists of 1 to 64 characters. It can contain English letters, numbers and special characters.

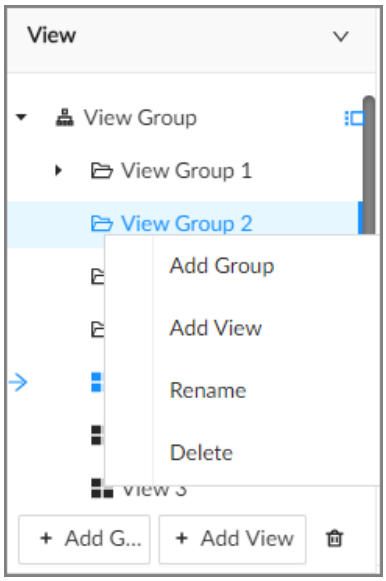
- We recommend you set a name that help to distinguish and classify different view groups.

Step 4 Click any blank space on the page to finish.

Related Operations

After creating a view group, you can rename or delete the view group.

Figure 7-3 Manage view groups



7.1.1.2 View

A view contains video images from one or more remote devices. You can drag several remote devices to the same view and when view is enabled, you can view the real-time video from the remote devices at the same time.

7.1.1.2.1 Creating View

Create a view and then add several remote devices to the view so that you can view the live videos from several channels at the same time.

Prerequisites

Remote devices have been added.

Procedure

Step 1 Log in to the PC client.

Step 2 Under the **Live** tab, click **View Group** or a view group under it, and then click **Add View**.

You can also right-click an existing view group and then click **Add View**.

Step 3 Double-click a remote device in resource pool, or drag the remote device to the view window.

After one remote device is added, the view window is split into several grids.

- Each grid supports one remote device. If you want to add more remote devices, drag them to unoccupied layout grids.
- If the layout grid has been occupied by a remote device, you can drag another remote device to the current grid to replace the original one.
- Drag the edges of the view window to adjust its size.

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

Step 4 Set the view name.

The view name consists of 1 to 64 characters. It can contain English letters, numbers and special character.

Step 5 Click **OK**.

Related Operations

Table 7-2 View management

Operation	Description
Edit	Edit remote devices in the view, window layout and view name.
Open	Open a view to watch real-time video of remote devices in the view.
Rename	Right-click a view, click **Rename**, enter the new name, and then click any blank space.
Delete	• Delete one by one: Click a view and then click , or right-click a view and then select **Delete**. • Delete in batches: Click , select views and then click .

7.1.1.2.2 Editing View

Procedure

Step 1 Log in to the PC client.

Step 2 Under the **Live** tab, right-click a view and then select **Edit**.

Step 3 Edit the view.

- Add a remote device: Double-click a remote device in the resource pool, or drag the remote device to an unoccupied layout grid on the view window, and then click **OK**.
- Delete a remote device: Point to a video window, and then click at the upper-right corner, and then click **OK**.
- Move the video windows: Drag a video window to a proper position and then release the mouse, and then click **OK**.
- Change window positions: Drag a video window to another video window, and then click **OK**.

  When adjusting the positions of video windows, drag the video window to the layout grid whose background color is green. You cannot drag the video window to the grid of red background color.
- Change the window size: Drag the edges of the video window to adjust its size, and then click **OK**.

- Save the view as a new one: Change the view name in View1 and then click **OK**.

7.1.1.2.3 Enabling view

Right-click the view and select **Open**, or double-click a view to open the view window.

Figure 7-4 View window

When opening the view, you can change video position, zoom video window.

- When adjusting the positions of video windows, drag the video window to the layout grid whose background color is green. You cannot drag the video window to the grid of red background color.
- Point to the video window. The taskbar is displayed. You can take a snapshot, enable recording and close the video window.
- Right-click the video window, you can switch bit streams, set digital zoom and more.

Table 7-3 View function

Operation	Description
Change window position	Drag a video window to another video window, and then click **OK**. The change in the window positions is valid only once. After you close and then open the view again, the view restores its original layout. If you want to change view window positions permanently, go to the view edit mode to set.
Zoom in video window	• When there are more than 9 video windows, click one video window to display it at the center of all windows in the zoom in mode. Click any other blank position to restore the original size. • Double-click a view window to display it in one-split mode. Double-click the view window again to restore the original layout.

Operation	Description
Add device to view window	In the resource pool, double-click a remote device or drag a remote device to a video window to add a remote device to the current view. Drag a remote device to an occupied video window to replace the original remote device. The modified view layout is valid only once if you do not click **OK**. After you close and then open the view again, the view restores its original layout.
Close view window	Point to one video window, and then click . After you close a video window, the system automatically adjusts window layout according to the rest number of remote devices and the available display space.

7.1.2 Device Tree

Log in to the PC client. The device tree on the upper-left corner of the **Live** tab displays the added remote devices, which are grouped automatically according to device type.

Figure 7-5 Device tree

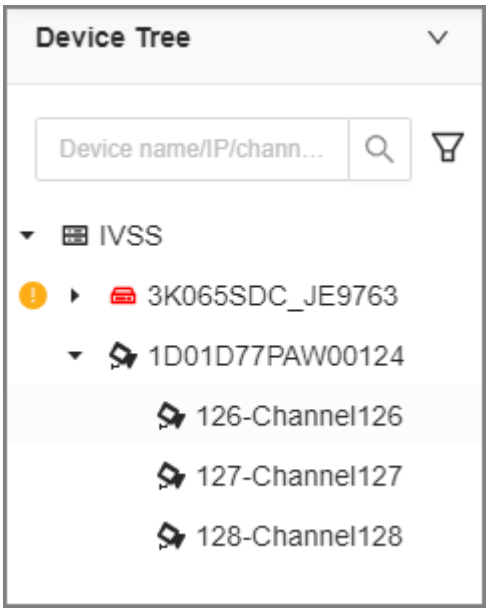


Table 7-4 Device tree description

Operation	Description
Search for devices	Enter keywords in . Support fuzzy search.

Operation	Description
Filter devices	Click and then select **All** , **Online**, **Offline**, **Device mismatch** and **Incorrect Username or Password** to filter the remote devices. **Device mismatch** refers to the situation where the remote device is not compatible with the Device due to inconsistent languages.
View device status	• If the icon of the remote device is black, the remote device is online. For example, IP PTZ Camera. • If the icon of the remote device is red, the remote device is offline. For example, 1-IPC . • If appears, the remote device is abnormal, alarming, and more. Point to to view the detailed information.
Mouse operations	• Point to the name of a remote device and then you can view its IP address and port number. • Right-click a remote device to connect, disconnect, and open the webpage of the remote device. • Double-click a remote device or drag the remote device to a video window, and then you can enter edit the view.

7.1.3 PTZ

Log in to the PC client. Use the PTZ panel at the lower-left corner of the **Live** tab to perform PTZ control so that the PTZ camera can rotate accordingly to monitor all directions.

The PTZ functions might vary depending on the device models.

Figure 7-6 PTZ

Table 7-5 PTZ control panel

Icons	Description
	Drag to set PTZ speed. The higher the value, the faster the PTZ speed.
	Control PTZ movement in the following ways. • Drag in different directions to control the PTZ direction. • Click the arrows to control the PTZ direction.
	Click to enable 3D positioning function.
	Click to enable auto focus, and then the camera image becomes focused automatically.
	Click to enter the PTZ menu mode.
	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.

Icons	Description
	Click to use windshield wiper. : Click to enable windshield wiper.
	Click to use PTZ functions. Before using PTZ functions, you need to configure the PTZ functions. • : preset. • : tour group. • : pattern. • : scan.

7.1.3.1 PTZ Menu Settings

The Device displays PTZ main menu on the view window. The PTZ main menu enables you to perform camera settings, PTZ settings, system management, and more. You can use the direction and confirm buttons to set the remote device.

Procedure

Step 1 Log in to the PC client.

Step 2 Under the **Live** tab, open a view and then select a remote device on the view.

Step 3 On the PTZ panel, click to open the OSD menu.

Table 7-6 PTZ menu description

Parameter	Description
Camera	Set camera parameters of the remote device including picture, exposure, backlight, WB, day and night, focus and zoom, defog, and default.
PTZ	Set PTZ functions of the remote device such as preset, tour group, scan, pattern, rotation, and PTZ restart.
System	Configure system settings of the remote device. You can set PTZ simulator, restore default, manage peripheral devices of the remote device, view the software version and PTZ version of the remote device, and more.
Exit	Exit the PTZ menu.

Step 4 Set PTZ menu parameters.

- Click or to select options .
- Click or to set values.
- Click OK to confirm.

Step 5 Click to exit PTZ menu mode.

7.1.3.2 Configuring PTZ Functions

Control PTZ device to implement corresponding operations.

The PTZ functions might vary depending on the device models.

7.1.3.2.1 Setting a Preset

A preset is the saved information of a specific position, angle, and focal length of the PTZ camera. You can set a preset so that you can quickly adjust the PTZ to the desired position when needed.

Procedure

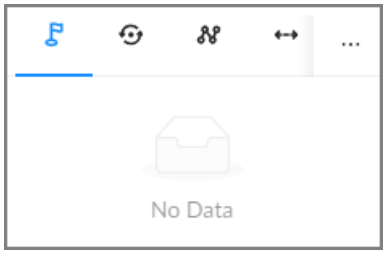
Step 1 Log in to the PC client.

Step 2 Under the **Live** tab, open a view.

Step 3 Select the video window of a PTZ camera.

Step 4 On the PTZ panel, click .

Figure 7-7 Call a preset



Step 5 Click the direction icons to rotate the PTZ camera to a specific position.

Step 6 Click , enter the name of the new preset, and then click to save the preset.

Step 7 Execute the preset.

1. Hover over the preset name.
2. Click next to the preset name. The PTZ camera rotates to the preset point.

Related Operations

- Edit a preset:
  - Double-click the name, and then the camera rotates to the preset after the double-click. You can change the name,
  - Select the preset, click to adjust the position of the preset, and then click .
  - Click to quit.
- Select a preset and then click to delete it.
- Click to refresh the preset list.

7.1.3.2.2 Setting a Cruise

A tour group is a sequential set of presets. When a tour group is used, the PTZ camera automatically rotates to the presets one by one at the predefined interval.

Procedure

Step 1 Log in to the PC client.

Step 2 Under the **Live** tab, open a view.

Step 3 Select the video window of a PTZ camera.

Step 4 On the PTZ panel, click .

Step 5 Click , enter the name of the new tour group, and then click to save.

Step 6 Click **Add**, select a preset, and then click .

Repeat this step to add multiple presets into the tour group.

Step 7 Execute the tour group.

1. Hover over the name of the tour group.
2. Click next to the name of the tour group. The PTZ camera rotates to the preset point in the configured sequence.
3. Click to stop the PTZ tour.

Related Operations

- Edit a tour group:
  - Double-click a tour group to rename it.
  - Select the tour group, click to modify the tour group, and then click .
  - Click to quit.
- Select a tour group and then click to delete it.
- Click to refresh the list of tour groups.

7.1.3.2.3 Setting a Pattern

A pattern is a recorded series of PTZ operations such as pan, tilt, zoom and focusing. You use a pattern to let the camera repeat the corresponding operations.

Procedure

Step 1 Log in to the PC client.

Step 2 Under the **Live** tab, open a view.

Step 3 Select the video window of a PTZ camera.

Step 4 On the PTZ panel, click .

Step 5 Double-click the name of a pattern, click **Start Record** , perform a series of PTZ actions, and then click **Stop Record**.

Step 6 Execute the pattern.

1. Hover over the name of the pattern.
2. Click next to the name of the tour group. The PTZ camera executes the actions in the pattern.

3. Click to stop the PTZ actions.

Related Operations

- Edit a pattern.

  Select the pattern, and then click . Click **Start Record** and record a new pattern, and then click **Stop Record**.

- Select a pattern and then click to delete it.
- Click to refresh the list of patterns.

7.1.3.2.4 Setting Linear Scanning

In the linear scanning mode, the camera scans repeatedly from side to side within the predefined left and then right limit.

Procedure

Step 1 Log in to the PC client.

Step 2 Under the **Live** tab, open a view.

Step 3 Select the video window of a PTZ camera.

Step 4 On the PTZ panel, click .

Step 5 Double-click the name of a scan, rotate the PTZ to the desired left and then click to save; rotate the PTZ to the desired right limit and then click .

The maximum number of scans depends on the camera capability. If the camera permits, you can configure up to 5 scans by default.

Step 6 Execute the scan.

1. Hover over the name of the scan.
2. Click next to the name of the scan. The PTZ camera executes the scan.
3. Click to stop the scan.

Related Operations

Edit the scan.

1. Select a scan, and then click .
2. Rotate the PTZ camera to a new left limit, and then click .
3. Rotate the PTZ camera to a new right limit, and then click .

7.1.3.2.5 Enabling Auxiliary Functions

Enable PTZ windshield wiper, light and IR.

Procedure

Step 1 Log in to the PC client.

Step 2 Under the **Live** tab, open a view.

Step 3 Select the video window of a PTZ camera.

Step 4 On the PTZ panel, click .

Step 5 Click  to enable the function.

7.2 Recorded Files

You can search for, play back, export the recorded videos or images, and more.

7.2.1 Playing back Recorded Videos

Search for and play back recorded videos according to remote device, recording type, and recording time.

Procedure

Step 1 Log in to the PC client.

Step 2 Select **Search** on the home page.

Step 3 Select one or more remote devices, and then click the **Record** tab.

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

Step 4 Select a stream type from **Main Stream** and **Sub Stream**.

Step 5 Set the search period.

Step 6 Click **Search**.

The search results are displayed. You can select **Timeline Playback** or **File Playback** to play back the videos.

- Timeline playback: Play back videos automatically.
- Place the mouse on the time axis of **Timeline Playback** to display the thumbnails of 9 frames before and after the current time node. Click the corresponding thumbnail to play the video of the node.
- File playback: The videos files are displayed by channel or by time. Click a file to play back.

  - You can click  to divide a video into multiple splices. It will divide the video file into 1, 4, 8 or 16 equal durations based on the total recording duration, to reduce the video playback time.
  - Select **Only locked videos** on the upper-right corner of the **File Playback** tab to display locked videos only.
  - Click  or  on the upper-right corner of the **File Playback** tab to switch the display mode of the video files.

Figure 7-8 Timeline playback

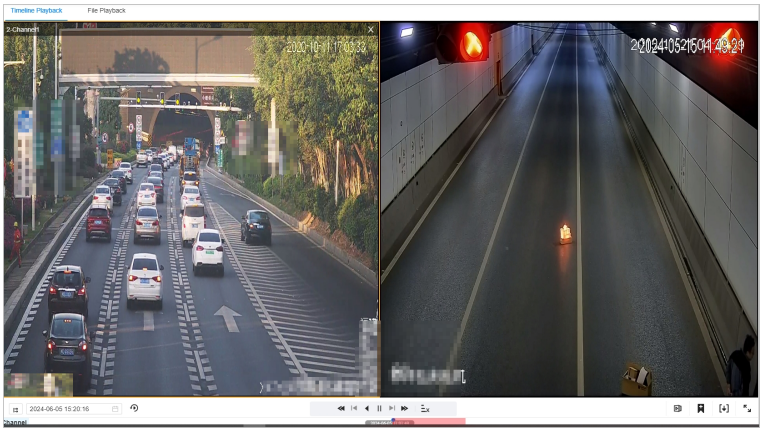


Figure 7-9 File playback

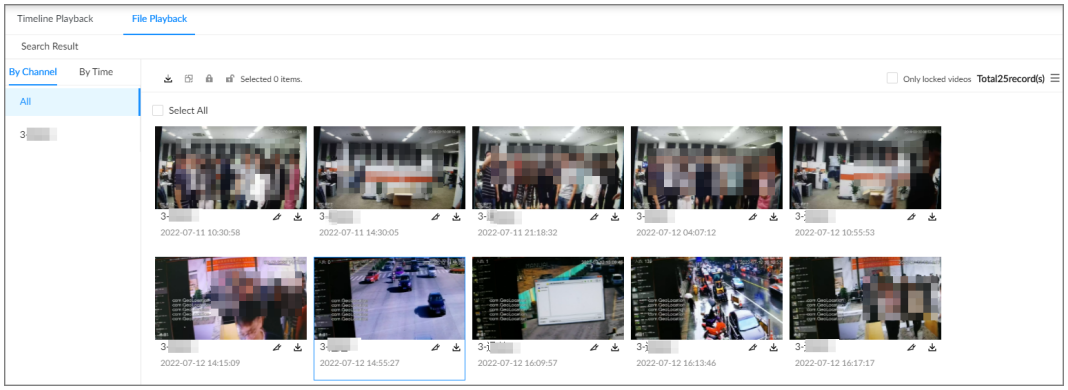
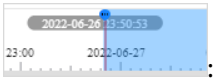


Table 7-7 Search icons description

Signal Words	Description
2022-08-05 10:04:10	Set a time period. Click to start playing the videos in the configured time period.
	When you play back several videos at the same time, click the icon to switch to time synchronization mode. All other windows play the video of the same time of current window. Click to cancel time synchronization. When you click , the system enables operation synchronization as well. If you want to cancel synchronization, click .
	Play back video file at a slow speed. The slow speed includes1/2,1/4,1/8, and1/16. Click the icon once, and then the playback speed becomes one level slower.

Signal Words	Description
	Play the previous frame. The function is only available in pause mode.
	Click to play backward. The icon becomes . Click to stop backward play.
	Click to start playback. The icon becomes . Click to pause playback.
	Play the next frame. The function is only available in pause mode.
	Play back at a fast speed. The fast speed includes 1, 2, 4, 8, and 16. Click the icon once, the playback speed becomes one level faster.
	Select a playback speed.
	Capture an image.
	Add tags to mark important points in time on the video.
	Clip one part of the video, and then save it in designated storage path.
	Click the icon and then drag the slider to adjust the volume.
	Play back at full screen.
	In full-screen playback page, click this icon to fix the toolbar; click it again to cancel it.

Signal Words	Description
—	Time bar. Displays recording type and recording period. ● There are 2 recording file bars on the time bar. The top bar displays recording time of selected window. The bottom bar displays recording time of all selected remote devices. ● The time bar uses different colors to categorize record types. ◇ Green: regular recording. ◇ Red: alarm recording. ◇ Blank: no recording. ●  : The time scale displays recording date and time, which changes automatically during the playback process. ● On the time bar, you can: ◇ Click the time bar and scroll your mouse to adjust the time accuracy. ◇ Drag the time bar to the left or right to view the hidden recording time.
	Right-click the playback window to bring up the shortcut menu. ● Original: Set video window scale. ◇ **On** : The system automatically adjusts video window scale according to the video resolution. ◇ **Close** : The system automatically adjusts video window scale according to the number of remote devices and the available display space. ● Audio: Set audio output. ● Fisheye: Set the installation method and display mode of fisheye camera.
	Extract the frame when the network playback speed is more than 4x.
	Select faces or humans on the video to search for similar targets.
	Close the playback window.

7.2.2 Clipping Recorded Video

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

Connect a USB device to the Device if you are operating on the local interface.

Procedure

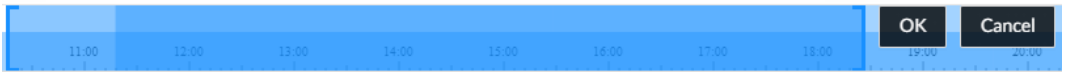
Step 1 Log in to the PC client.

Step 2 On the home page, select **Search**.

Step 3 Search for recorded videos and then play back a video.

Step 4 Click [+].

Figure 7-10 Clip a video

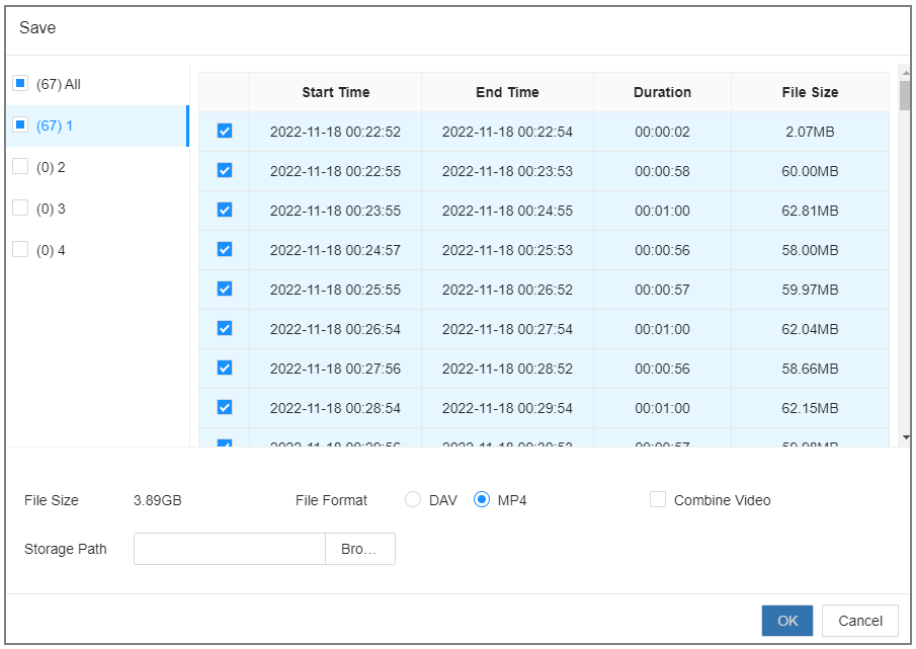


Step 5 Drag the left and right edges of the blue frame to select the start time and end time of clipping.

Step 6 Click ✓.

Step 7 Select a file format, and then click **Browse** to select the storage path.

Figure 7-11 Save the video



Step 8 Click **OK**.

7.2.3 Video Tag

During playback, you can add a tag to mark an important point in time on the video. After playback, you can use time or the tag keywords to search for the corresponding video and then play.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **Search**.

Step 3 Search for videos and play back a video.

Step 4 During playback, click at the lower-right corner of the playback window.

Step 5 Enter tag name, and then click **OK**.

Related Operations

You can search for and manage tagged files.

1. Log in to the PC client.
2. On the home page, select **Search** > **Tags**.
3. Select one or more channels, enter keywords, and then set the search period.
4. Click **Search**.

- 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 refresh the tag list.

7.2.4 Locking Files

Lock specific videos or snapshot so they will not be overwritten.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **Search**.

Step 3 Search for videos or snapshots

Step 4 Under the **File Playback** tab, select one or more search results and then click .

The files are locked. Select the locked files and then click to unlock them.

7.2.5 Exporting File

Back up videos or images by downloading or remote backup.

Connect a USB device to the Device if you are operating on the local interface.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **Search**.

Step 3 Search for videos or images.

Step 4 Under the **File Playback** tab, select one or more files to back up.

- Download.
  1. Click .
  2. Select a file type.
  3. Click **Browse** to select the storage path. You can download files to your computer or a USB storage device.
  4. Click **OK**.

  Select **Combined Video** to merging and download several video clips.
- Remote backup.
  1. Click .
  2. Click **Search** to search for connected third-party storage devices.
  3. Select a storage device, and then select a file format.
  4. Click **Format** to format the selected storage device.

  Please be advised that formatting the storage device will clear all data on it.

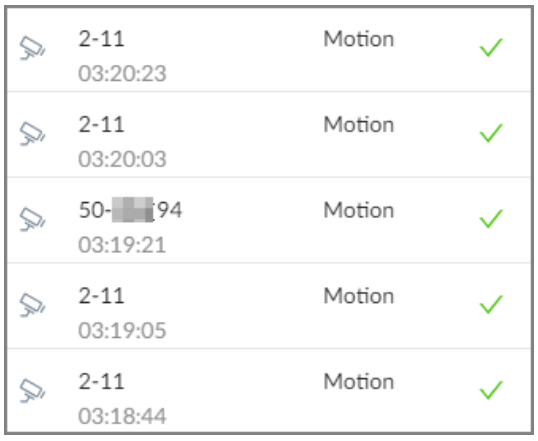
5. Click **Start**.

Make sure that an external HDD or disk array enclosure has been connected to the eSATA port of the Device.

7.3 Alarm List

Log in to the PC client. Click on the upper-right corner to display the alarm list. You can view the name of alarm device, alarm time and alarm type.

Figure 7-12 Alarm list

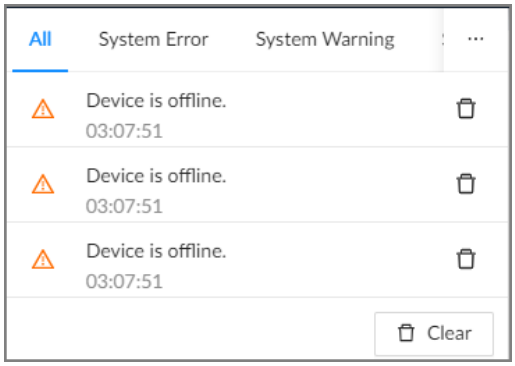


- The number on the icon is the number of unprocessed alarm events. The alarm list displays up to 200 unprocessed alarm events.
- Click to confirm the alarm event. The confirmed event will be removed from the alarm list.

7.4 System Info

Log in to the PC client, and then click on the upper-right corner to view system messages including system errors, system alarms and system notifications.

Figure 7-13 System messages



- Click **All** , **System Error**, **System Warning**, or **System Notifications** to view the corresponding system messages.

- Click to delete the corresponding system message.
- Click **Clear** to clear all system messages under current tab.

  For example, you can click **Clear** under the **All** tab to clear all system messages, or click **Clear** under the **System Error** tab to clear all system error messages.

7.5 Background Task

View the status of the tasks running in the background.

Log in to the PC client, and then click to display the background tasks. Click **All** , **In progress**, or **Waiting** to view the background tasks of different statuses.

8 System Maintenance

8.1 Overview

Log in to the PC client. On the home page, select **Maintenance Center** > **Overview**.

Figure 8-1 Overview

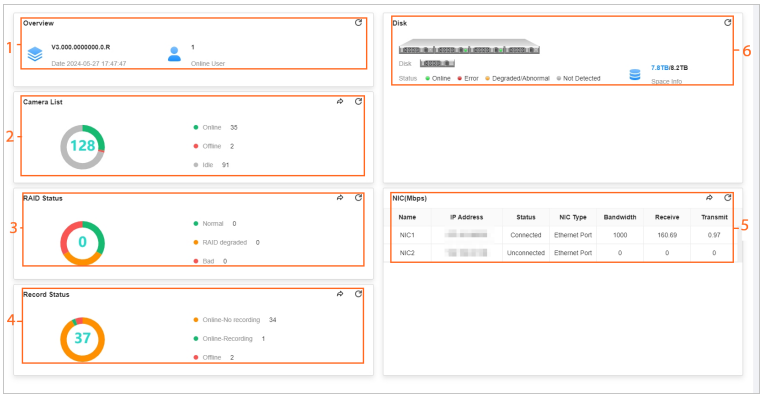


Table 8-1 Overview

No.	Function	Description
1	Overview	View device version and the number of online users. Click to refresh the data.
2	Camera List	View the connection and idle status of remote devices. • Click to go to the **Access Management** page for detailed information. • Click to refresh the data.
3	RAID Status	View RAID status. • Click to go to the **Storage** page for detailed information. • Click to refresh the data.
4	Record Status	View recording status of remote devices. • Click to go to the **Storage** page for detailed information. • Click to refresh the data.

No.	Function	Description
5	NIC (Mbps)	View NIC status. ● Click to go to the **TCP/IP** page for detailed information. ● Click to refresh the data.
6	Disk	● View disk status and storage usage. ◇ : disk online. ◇ : disk error. ◇ : disk degraded or abnormal. ◇ : no disk detected. ● Click , click to enable device positioning and then set the interval at which the positioning indicator light of the Device flashes. The flashing indicator light helps you quickly find the Device. ● Click to refresh the data.

8.2 System Information

8.2.1 Viewing Device Information

Log in to the PC client. On the home page, select **Maintenance Center** > **System Info** > **Device Info**. You can view device information such as input bandwidth, system version, and web version.

8.2.2 Viewing Legal Information

Log in to the PC client. On the home page, select **Maintenance Center** > **System Info** > **Legal Info**. You can view the software license agreement, privacy policy, and open-source software note.

8.2.3 Viewing Algorithm Version

Log in to the PC client. On the home page, select **Maintenance Center** > **System Info** > **Algorithm Version**. You can view the algorithm license status and versions of smart functions.

Figure 8-2 Algorithm version

8.2.4 Online User

Manage the online user that can access the Device. You can block a user from access for a period of time. During the block period, the selected user cannot access the Device.

You cannot block yourself or admin user.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **Maintenance Center** > **System Info** > **Online User**.

The list displays currently connected users.

Figure 8-3 Online user

Step 3 Block one or more users.

- Block one by one: Click ⊘ corresponding to the user.
- Block in batches: Select multiple users and then click **Block**.

Step 4 Set the block period. The default period is 30 minutes.

Step 5 Click **OK**.

8.2.5 Viewing License Info

View the authorization information of the Device, including the authorization status, duration, and expiration time.

Log in to the PC client. On the home page, select **Maintenance Center** > **System Info** > **License Info**. You can view the license information of each channel.

Figure 8-4 License information

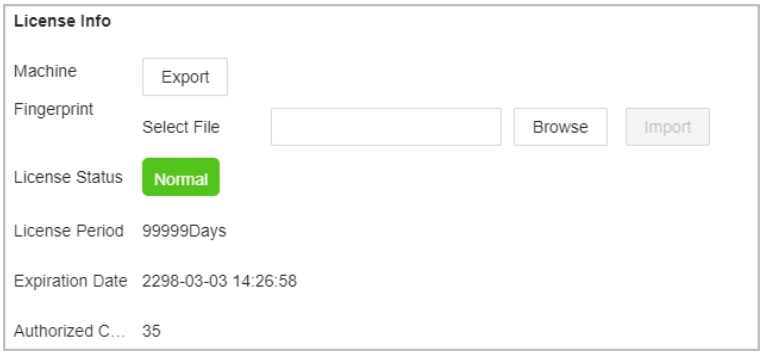


Table 8-2 License information parameter description

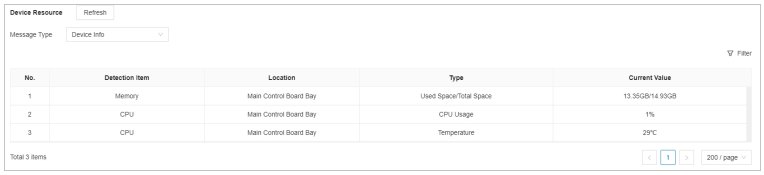
Parameter	Description
Machine Fingerprint	Used for encrypting data tied to the machine. Supports machine fingerprint export.
Select File	Support selecting specific authorization files for import. Successful import will display green text, while failed import will display red text.
License Status	Displays according to the actual situation.
License Period	Duration of application for permissions.
Expiration Date	Expiration date of authorization.

8.3 System Resources

8.3.1 Viewing Device Resources

Log in to the PC client. On the home page, select **Maintenance Center** > **System Resources** > **Device Resource**. You can view resource status including CPU and memory usage, mainboard temperature and fan speed.

Figure 8-5 Device resources



- Click  to select the items that you want to view.
- Click **Refresh** to refresh the data.

8.3.2 Viewing AI Module Information

Log in to the PC client. On the home page, select **Maintenance Center** > **System Resources** > **AI Module Resource**. You can view the status of AI modules.

8.4 Network Detection

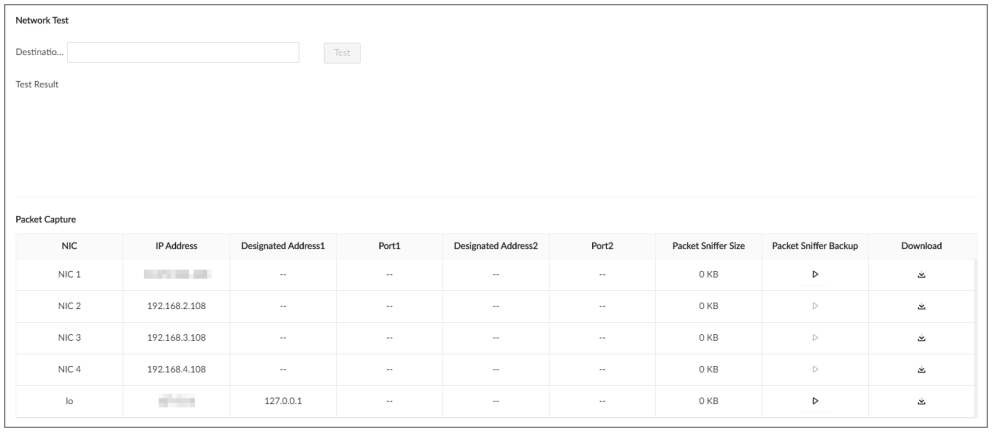
You can test network connection and capture packets. Packet capture is the practice of intercepting a data packet that is crossing or moving over a specific computer network. The captured packet is stored temporarily for analysis. The packet is inspected to help diagnose and solve network problems and determine whether its structure follows network security policies.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **Maintenance Center** > **Network Detection** > **Network Test**.

Figure 8-6 Network test



Step 3 In the **Network Test** section, enter the target address, and then click **Test**.

After testing is completed, the test result is displayed. You can check the evaluation for average delay, packet loss, and network status.

Step 4 In the **Packet Capture** section, click ▷ to start capturing the packets of the corresponding NIC, and then click ⏸ to stop.

- You cannot capture packets of several NICs at the same time.
- During packet capturing, you can go to other pages for operation and go back to the **Network Test** page later to stop packet capturing.

Step 5 Click ⬇ to download the captured packet.

8.5 S.M.A.R.T Detection

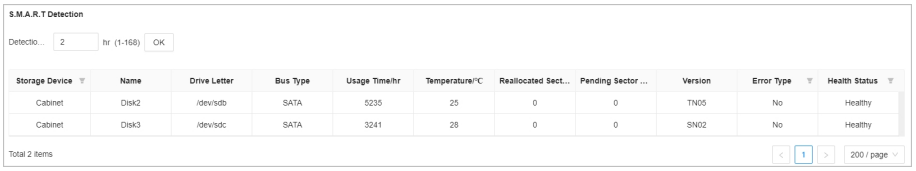
Run S.M.A.R.T detection to check HDD status.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **Maintenance Center** > **Disk Maintenance** > **S.M.A.R.T Detection**.

Figure 8-7 S.M.A.R.T detection



Step 3 Set the detection period.

Step 4 Click **OK**.

8.6 Log Info

The logs record all kinds of system running information. We recommend you check the logs periodically and fix the problems in time.

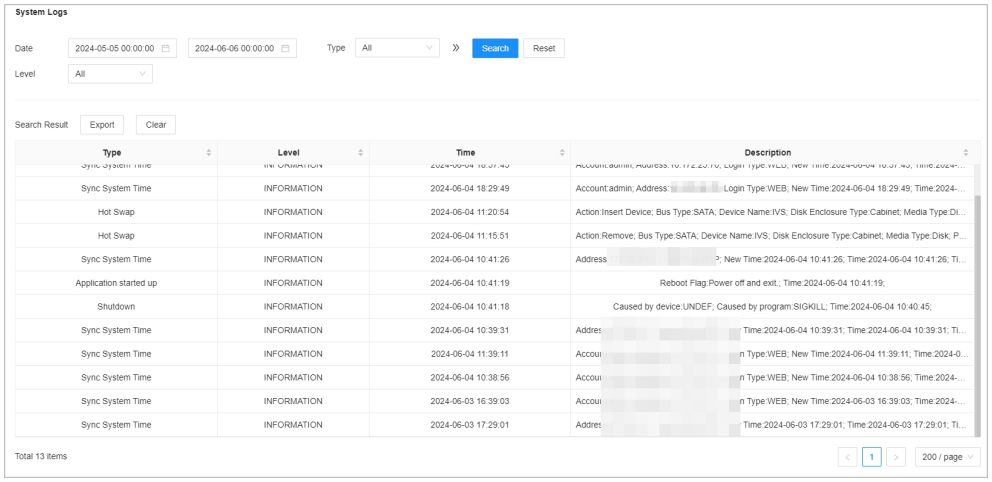
8.6.1 System Logs

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **Maintenance Center** > **Log Info** > **System Logs**.

Figure 8-8 System logs



Step 3 Set the search condition, including system log type, date, description, and level.

Step 4 Click **Search**.

Step 5 (Optional) Click **Export** , and then select whether to **Export Encryption** based on the actual situation.

8.6.2 User Operation Logs

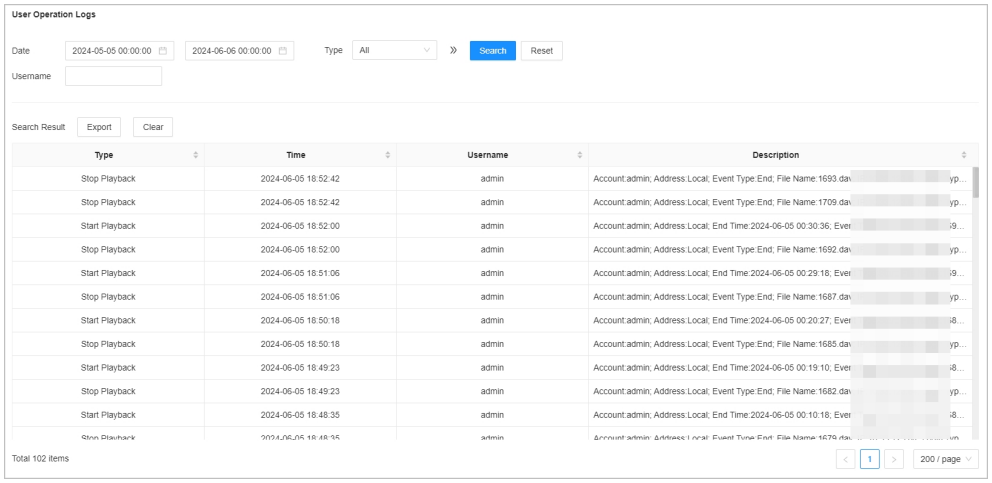
Search user operation logs, including user operations and user configuration logs.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **Maintenance Center** > **Log Info** > **User Operation Logs**.

Figure 8-9 User operation logs



Step 3 Set the search condition, including user operation log type, date, description, and username.

Step 4 Click **Search**.

Step 5 (Optional) Click **Export** , and then select whether to **Export Encryption** based on the actual situation.

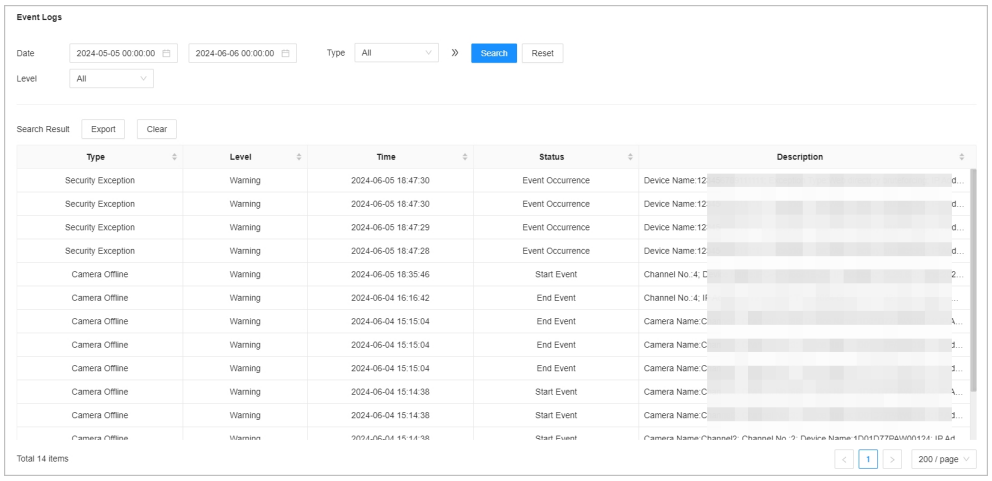
8.6.3 Event Logs

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **Maintenance Center** > **Log Info** > **Event Logs**.

Figure 8-10 Event logs



Step 3 Set the search condition, including event log type, date, description, and level.

Step 4 Click **Search**.

Step 5 (Optional) Click **Export** , and then select whether to **Export Encryption** based on the actual situation.

8.6.4 Connection Logs

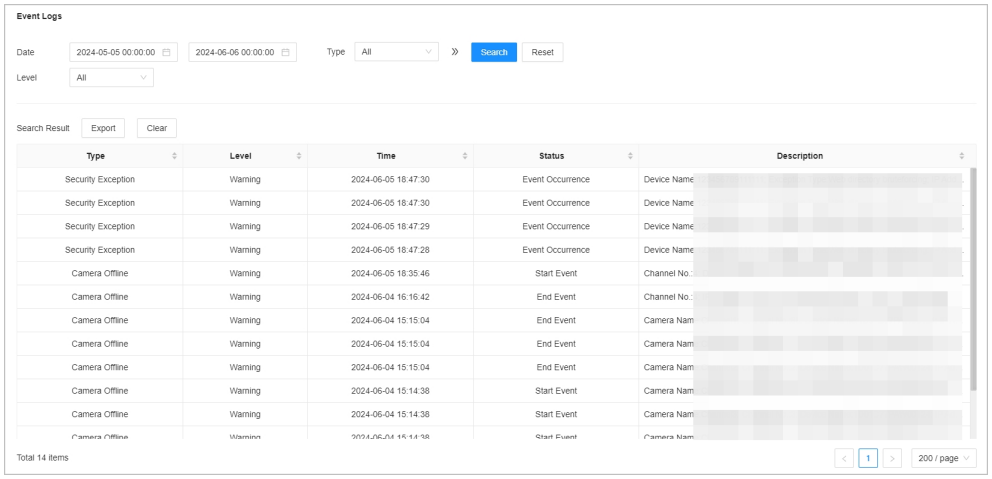
Search for logs related to device connection, including user login/logout, session hijacking, session brute-forcing, and remote device.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **Maintenance Center** > **Log Info** > **Connection Logs**.

Figure 8-11 Connection logs



Step 3 Set the search condition, including connection log type, date, description, and username.

Step 4 Click **Search**.

Step 5 (Optional) Click **Export** , and then select whether to **Export Encryption** based on the actual situation.

8.7 One-click Diagnosis

One-click diagnosis helps users better use the device by diagnosing the configuration and status of the device.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **Maintenance Center** > **One-click Diagnosis**.

Step 3 Click **Diagnose** , and then click **Details** to view the corresponding diagnosis information.

8.8 Advanced Maintenance

8.8.1 Export

Export the diagnosis data for troubleshooting when the Device is in exception.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **Maintenance Center** > **Advanced Maintenance** > **Export**.

Step 3 Click **Generate Diagnosis Data** to generate diagnosis data.

Step 4 Click **Export** to export the diagnosis results.

8.8.2 Run Log

View system run logs for troubleshooting.

Make sure that you have enabled **Run Log** in **Security** > **System Service**. Otherwise there is no log data.

Log in to the PC client. On the home page, select **Maintenance Center** > **Advanced Maintenance** > **Run Log**.

The logs might be overwritten when the storage space runs out. Back up the logs in time.

- Export logs one by one: Click to export a log.
- Export logs in batches: Select multiple logs, and then click **Export**.

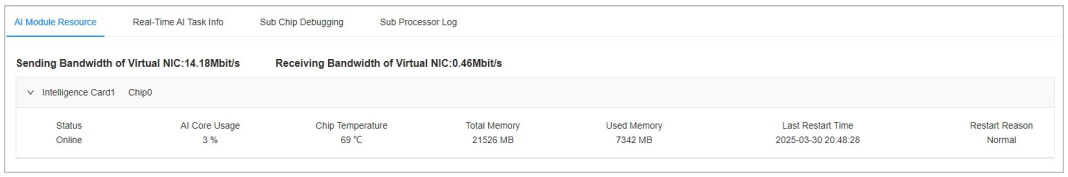
8.8.3 Operator O&M

8.8.3.1 AI Module Resource

View the usage rate of the intelligent analysis card, chip temperature, memory usage and other related metrics.

Log in to the PC client. Select **Maintenance Center** > **Advanced Maintenance** > **Operator O&M** > **AI Module Resource**.

Figure 8-12 AI module resource



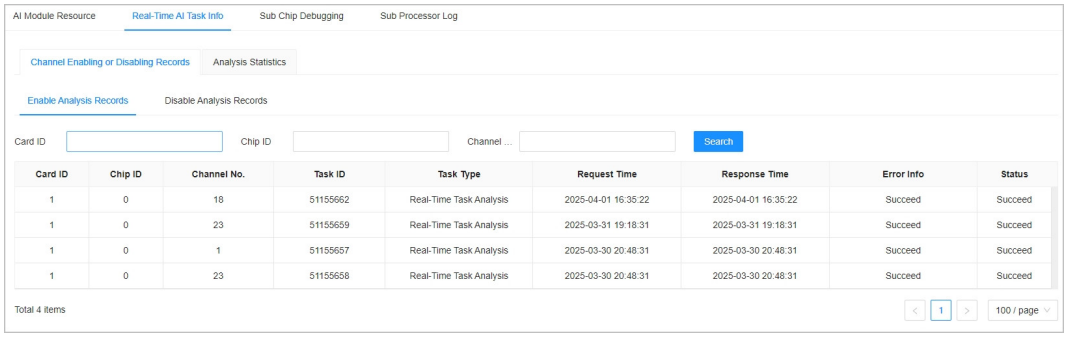
8.8.3.2 Real-Time AI Task Info

View data related to intelligent analysis, such as records of channel analysis being enabled/disabled, the status of analysis stream pulling and so on.

Log in to the PC client. Select **Maintenance Center** > **Advanced Maintenance** > **Operator O&M** > **Real-Time AI Task Info**.

- Channel Enabling or Disabling Records: Select **Enable Analysis Records** or **Disable Analysis Records**, set search conditions, and then click **Search**.
- Analysis Statistics: Set search conditions, and then click **Search**.

Figure 8-13 Real-time AI task information

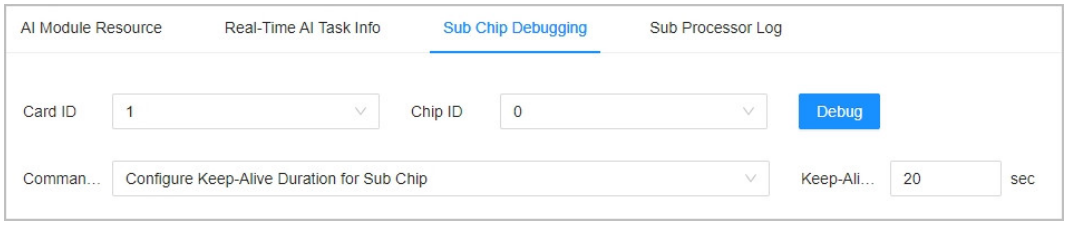


8.8.3.3 Sub Chip Debugging

The sub chip debugging function is exclusively for use by technical support personnel.

Log in to the PC client. Select **Maintenance Center** > **Advanced Maintenance** > **Operator O&M** > **Sub Chip Debugging**, select the card ID and chip ID, and then click **Debug**.

Figure 8-14 Sub chip debugging



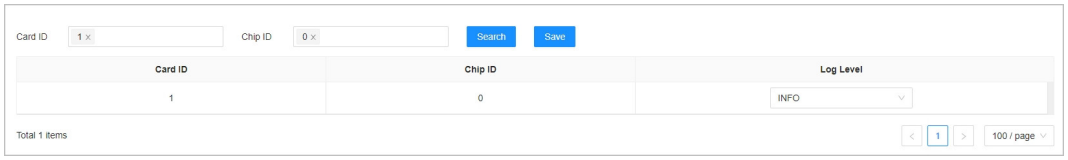
8.8.3.4 Sub Processor Log

The chip log function is exclusively for use by technical support personnel.

Log in to the PC client. Select **Maintenance Center** > **Advanced Maintenance** > **Operator O&M** > **Sub Processor Log**, select the card ID and chip ID, and then click **Search**.

Supports modifying the log level, and then click **Save**.

Figure 8-15 Sub processor logs



8.9 Updating

Perform a system version upgrade for the device.

To perform a full version upgrade, start by updating the host program, and then proceed with the algorithm upgrade.

8.9.1 Host Update

You can import the update file to update the system version of the Device. The extension name of the update file is .bin.

Prerequisites

You need to obtain the correct update file and save it in the corresponding path.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **Maintenance Center** > **Update** > **Host Update**.

Step 3 Click **Import Update File** to select an update file.

Step 4 Click **OK**.

The system starts updating. The Device automatically restarts after successfully updated.

8.9.2 Algorithm Update

You can import the update file to update the AI module. The extension name of the update file is .bin.

Prerequisites

You need to obtain the correct update file and save it in the corresponding path.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **Maintenance Center** > **Update** > **Algorithm Update**.

Step 3 Click **File Update**.

Step 4 Click **Browse** to select an update file.

Step 5 Click **Update Now**.

Step 6 Click **OK**.

The system starts updating the AI module. The Device automatically restarts after the update is complete.

8.10 Maintenance Management

To clear the malfunction or error during the system operation and enhance operation performance, you can restart the Device, restore factory default setup, update the system and more.

8.10.1 Default

When the system runs slowly and has configuration errors, try to solve the problems by restoring the default settings.

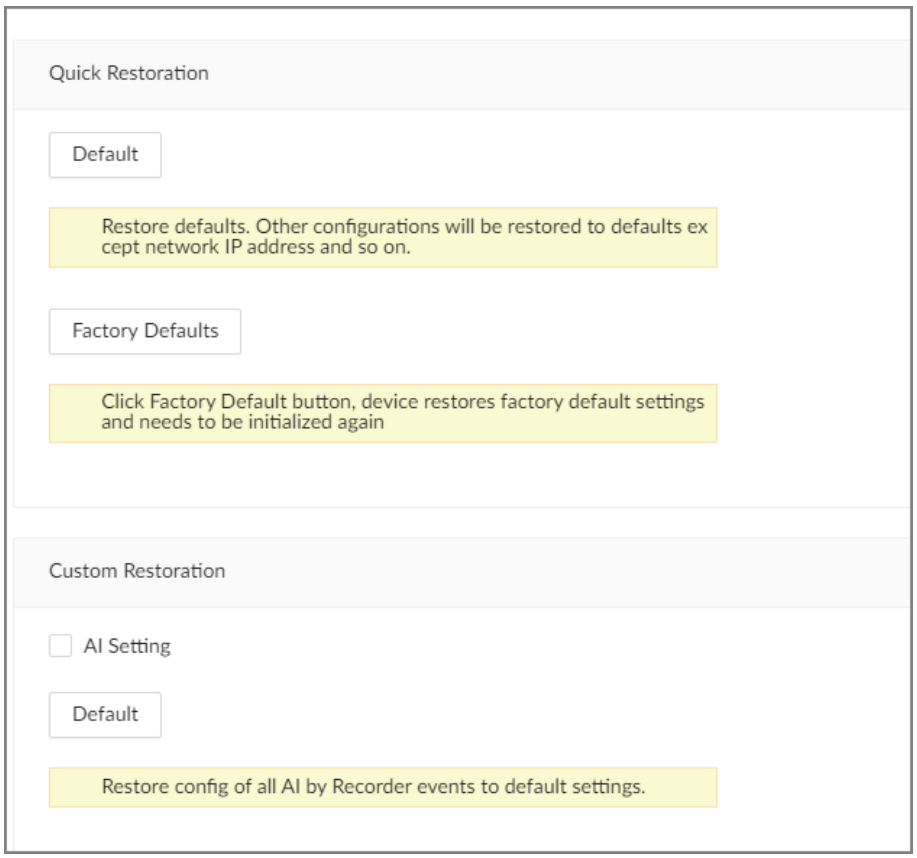
All configurations are lost after factory default operation.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **Maintenance Center** > **Manager** > **Default**.

Figure 8-16 Default



Step 3 Select a method between **Quick Restoration** and **Custom Restoration**.

Step 4 Click **OK**.

The system begins to restore default settings. After that, the system prompts you to restart the Device.

8.10.2 Maintenance

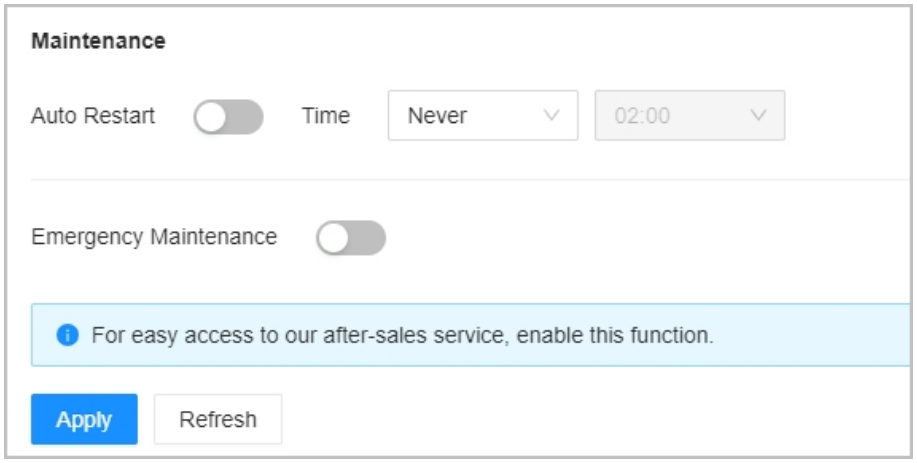
If the device has run for a long time, you can set the Device to automatically restart at idle time.

Procedure

Step 1 Log in to thee PC client.

Step 2 On the home page, select **Maintenance Center** > **Manager** > **Maintenance**.

Figure 8-17 Auto Maintain



Step 3 Set the automatic time.

Step 4 Click to enable emergency maintenance.

When an upgrade power outage, running error and other problems occur, and you cannot log in, you can restart or update the Device, and clear configurations through emergency maintenance.

To use the function, make sure that you have installed Device Diagnostic Tool.

Step 5 Click **Apply**.

8.10.3 Config Backup

You can export the configuration file of the Device to your computer or a USB storage device for backup. When the configurations are lost due to abnormal operation, you can import the backup configuration file to restore system configurations quickly.

Exporting Configuration File

On the home page, select **Maintenance Center** > **Manager** > **Config Backup**. Click **Export** to export the configuration file. The file storage path varies depending on the interface you are operating.

- On the PC client, click , and then select **Download** to view file saving path.
- On the local interface, you can select the file storage path.

  Connect USB device to the Device if you are operating on the local interface.
- On the web interface, files are saved to the default downloading path of the browser.

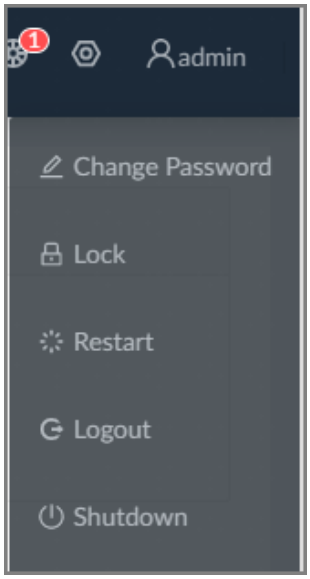
Importing Configuration File

Click **Browse** to select the configuration file, and then click **Import**. After the configuration file is imported successfully, the Device will restart automatically.

9 Log Out, Restart, Shut Down, Lock

Log out of, restart, shut down and lock out the Device.

Figure 9-1 User operation



Logging Out

Click admin, and then select **Logout**.

Restart

Click admin, select **Restart** , and then click **OK**.

Shutting Down

Shutting down the Device by unplug the power cable might cause data loss, and is not recommended.

- Mode 1 (recommended): Click admin, select **Shutdown** , and then click **OK**.
- Mode 2: Press the power button on the Device.
- Mode 3: Unplug the power cord.

Locking

Click admin, and then select **Lock** to lock the screen. The locked client cannot be operated.

To unlock the client, click anywhere on the client, and then the **Unlock** window appears. Enter the username and password, and then click **OK**. You can also click **Switch User** to switch to another user account.

10 Solution Application(CyberCity)

Procedure

Step 1 Open the browser, and then enter http://*Cybercity IP address*, click **Download** to download the Client.

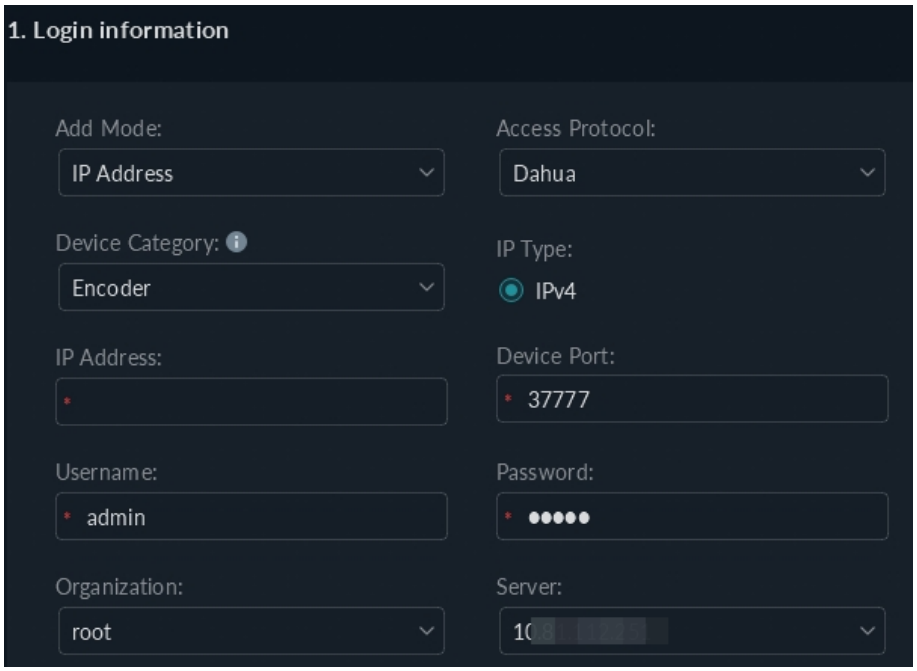
Step 2 Enter the IP address, port, username, password and select **English** as the language of the Client.

Step 3 Click **Logging in**.

Step 4 On home page, select **Configuration** > **Device**, click **+Add** to add TB9000 to the platform.

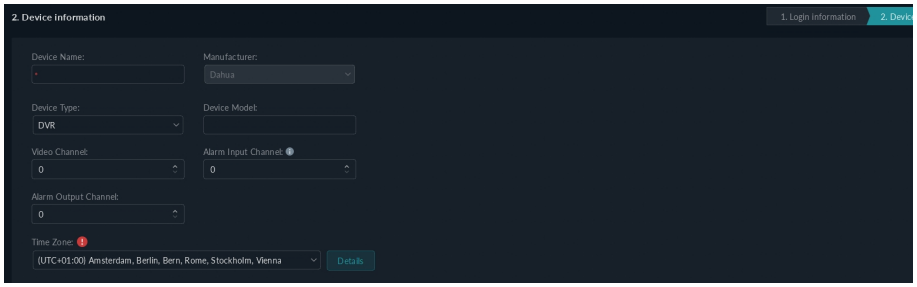
1. Enter the login information, and then click **Add**.
   - **IP Address** : The IP address of TB9000.
   - **Username** and **Password**: The username and password of TB9000.

Figure 10-1 Login information



2. Enter the device inforamtion, and then click **OK**.
   - **Device Name** : Enter the device name to differentiate it from others.
   - Enter the number of video channel.
   - Select the **Time Zone**.

Figure 10-2 Device Information



If the added device displays online, it means that the device is added successfully.

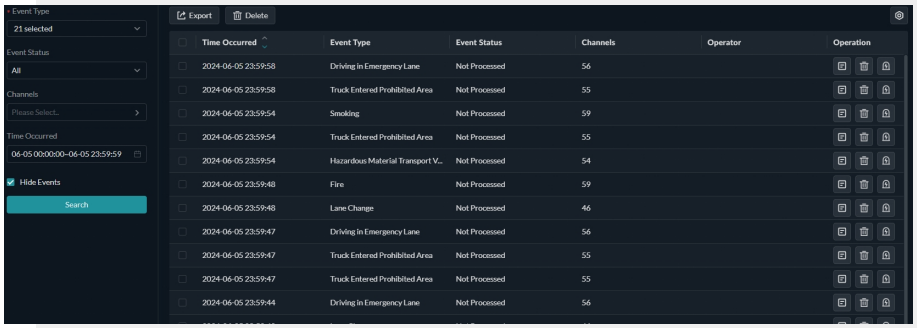
Step 5 View alarm information.

1. On home page, select **Application** > **Road Event**.
2. Set search conditions, and then click **Search**.

Select **Hide Events** to display the hidden events.

The results will be displayed on the left and you can view the detailed information, delete the records or export the alarm records. For details, see the Cyber City user's manual.

Figure 10-3 Search results



Appendix 1 Security Commitment and Recommendation

Dahua Vision Technology Co., Ltd. (hereinafter referred to as "Dahua") attaches great importance to cybersecurity and privacy protection, and continues to invest special funds to comprehensively improve the security awareness and capabilities of Dahua employees and provide adequate security for products. Dahua has established a professional security team to provide full life cycle security empowerment and control for product design, development, testing, production, delivery and maintenance. While adhering to the principle of minimizing data collection, minimizing services, prohibiting backdoor implantation, and removing unnecessary and insecure services (such as Telnet), Dahua products continue to introduce innovative security technologies, and strive to improve the product security assurance capabilities, providing global users with security alarm and 24/7 security incident response services to better protect users' security rights and interests. At the same time, Dahua encourages users, partners, suppliers, government agencies, industry organizations and independent researchers to report any potential risks or vulnerabilities discovered on Dahua devices to Dahua PSIRT, for specific reporting methods, please refer to the cyber security section of Dahua official website.

Product security requires not only the continuous attention and efforts of manufacturers in R&D, production, and delivery, but also the active participation of users that can help improve the environment and methods of product usage, so as to better ensure the security of products after they are put into use. For this reason, we recommend that users safely use the device, including but not limited to:

Account Management

1. **Use complex passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters;
   - Include at least two types of characters: 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 repeating characters, such as 111, aaa, etc.

2. **Change passwords periodically**

   It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.

3. **Allocate accounts and permissions appropriately**

   Appropriately add users based on service and management requirements and assign minimum permission sets to users.

4. **Enable account lockout function**

   The account lockout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.

5. **Set and update password reset information in a timely manner**

   Dahua device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

Service Configuration

1. **Enable HTTPS**

   It is recommended that you enable HTTPS to access Web services through secure channels.
2. **Encrypted transmission of audio and video**

   If your audio and video data contents are very important or sensitive, we recommend you to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped during transmission.
3. **Turn off non-essential services and use safe mode**

   If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.

   If necessary, it is highly recommended to choose safe modes, including but not limited to the following services:

   - SNMP: Choose SNMP v3, and set up strong encryption and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up complex passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up complex passwords.
4. **Change HTTP and other default service ports**

   It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

Network Configuration

1. **Enable Allowlist**

   It is recommended that you turn on the allowlist function, and only allow IP in the allowlist to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allowlist.
2. **MAC address binding**

   It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.
3. **Build a secure network environment**

   In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:

   - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
   - According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;
   - Stablish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

Security Auditing

1. **Check online users**

   It is recommended to check online users regularly to identify illegal users.
2. **Check device log**

By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.

3. **Configure network log**

   Due to the limited storage capacity of devices, the stored log is limited. If you need to save the log for a long time, it is recommended to enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

Software Security

1. **Update firmware in time**

   According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.

2. **Update client software in time**

   We recommend you to download and use the latest client software.

Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).

ENABLING A SMARTER SOCIETY AND BETTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053
Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188