IVD

User Manual



ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V2.1.0

Foreword

General

This manual introduces the installation, functions and operations of the IVD (hereinafter referred to as the "the Device" or "IVD"). Read carefully before using the device, and keep the manual safe for future reference.

Models

DHI-IVD7132-1M; DHI-IVD7132-2M; DHI-IVD3116-1M; DHI-IVD3116-2M; DHI-IVD3116-1I; DHI-IVD5148 series; DHI-IVD5148WT-1I; DHI-IVD5148WT-1I-4G; DHI-IVD5148-1I-4G; DHI-IVD5348.

Symbols

The following symbols might appear in the manual.

Symbol	Description
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.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V2.1.0	• Updated the important safeguards and warnings, homepage, AI operations, general operations and system operations. • Added the contents of auto registration, viewing tracks, attendance records and PTRZ. • Added DHI-IVD5348 series installation method. • Updated the contents of smart application orchestration.	August 2026
V2.0.1	• Updated the rear panel. • Deleted the contents of the people counting.	April 2026
V2.0.0	• A fresh new interface. • Added the new model.	September 2025
V1.0.3	Updated the sample database.	January 2025

Version	Revision Content	Release Time
V1.0.2	• Updated AcuPick. • Updated search by image. • Updated storage mode. • Added AI open platform. • Added intelligent compression.	September 2024
V1.0.1	Added the model.	August 2024
V1.0.0	First release.	January 2024

Privacy Protection Notice

As the device user, you might collect the personal data of individuals such as their names, email addresses, face images, audio and fingerprints. You shall be fully responsible for any activities associated with processing personal data. You commit to comply with your local privacy protection laws and regulations to protect the legitimate rights and interests of individuals, and shall implement measures which are required by applicable law, including but not limited to, providing clear and comprehensive information to individuals before processing their personal data, obtaining consent from individuals when necessary, informing individuals of the existence of the surveillance area, and providing required contact information.

Intelligent Product Usage Statement

Intelligent products utilize AI technology to effectively enhance security. The intelligent recognition and alarm functions of the product might be affected by factors such as environmental lighting, camera angles, object obstructions, and network delays, potentially leading to false alarms, missed alerts, or response delays. This intelligent product is solely intended to be used as a security assistance tool. The results from performing identification are for reference only and do not constitute absolute guarantee of personal or property safety. Users need to combine these products with necessary physical security measures to enhance overall protection. Except as otherwise provided by laws or in the event of intentional or gross negligence on the part of the company, the company shall not be liable for any losses caused by the aforementioned factors not attributable to the company.

About the Manual

- This manual is provided for general reference only. Discrepancies might exist between the product and this manual, including but not limited to printed, electronic, or any other editions.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. Specifications and documentation are subject to change without prior notice. For the latest versions, as well as legal notices, consult the printed manual, the product webpage, our official website, or scan the QR code to access the electronic edition.
- The manual will be updated as necessary to reflect product changes and applicable legal requirements. These updates will not diminish your statutory rights, nor will they remove or weaken the safety information or essential instructions provided at the time of purchase.
- Although we make every effort to ensure accuracy, errors or deviations in descriptions of functions, operations, or technical data might occur. If there is any uncertainty or controversy, we reserve the right of final explanation.
- All trademarks, registered trademarks and company names referenced in this manual are the property of their respective owners.

Icons and Buttons

Icon/Button	Description
	After you have entered the password, click the icon to display the password in letters and numbers. Release the mouse or point to other places, the password is displayed in the form of black dots.
	Click the icon to access the management of remote devices, network, storage, account, and more.
	Point to the icon to display help information.
	Click the icon to display the hidden menu. Now the icon becomes / / . Click / / again to hide the menu items.
	Select the checkboxes to select multiple menu items at the same time. means selected.
	Check the box to select one menu item, means selected.
	Click the icon to view the drop-down list.
	● : Disabled. ● : Enabled
	Refresh the data.
	Cancel the unsaved configuration.
	Page switch. ● / : page up/page down. ● / : Go to the first page or the last page.
	Filter icon. Click it to set filter criteria.
	Click the icon, the system displays checkboxes, so you can select multiple objects.
	Enter keywords, and then click to search for the corresponding information.
	Enter numbers, letters, symbols and more.
	Click the icon to close the window.

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 Device under allowed humidity and temperature conditions.

Storage Requirements



Store the Device under allowed humidity and temperature conditions.

Installation Requirements

 **DANGER**

-  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.

 **WARNING**

- Do not connect the power adapter to the Device while the adapter is powered on.
- Strictly comply with the local electric safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the Device.
- Use the standard power adapter or cabinet power supply. We will assume no responsibility for any injuries or damages caused by the use of a nonstandard power adapter.
- Please follow the electrical requirements to power the Device.
  - ◇ Following are the requirements for selecting a power adapter.
    - ○ The power supply must conform to the requirements of IEC 60950-1 and IEC 62368-1 standards.
    - ○ The voltage must meet the SELV (Safety Extra Low Voltage) requirements and not exceed ES-1 standards.
    - ○ When the power of the device does not exceed 100 W, the power supply must meet LPS requirements and be no higher than PS2.

- We recommend using the power adapter provided with the Device.
- When selecting the power adapter, the power supply requirements (such as rated voltage) are subject to the Device label.

- 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 server on a stable surface to prevent it from falling.
- Use power cords that conform to your local requirements, and are rated specifications.
- 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 are 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.
- Install the server in an area that only professionals can access.
- Extra protection is necessary for the Device casing to reduce the transient voltage to the defined range.
- If you did not push the HDD box to the bottom, then do not close the handle to avoid damage to the HDD slot.
- Install the Device near a power socket for emergency disconnect.
- It is prohibited for non-professionals and unauthorized personnel to open the Device casing.
- Affix the Device securely to the building before use.

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

- 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.

- Check whether the power supply is correct before use.
- Do not unplug the power cord on the side of the Device while the adapter is powered on.
- Operate the Device within the rated range of power input and output.
- Use the Device under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the Device, and make sure that there is no object filled with liquid on the Device to prevent liquid from flowing into 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: 0 °C to 45 °C (32 °F to 113 °F).
- Salt pray in the operating environment of the device might corrode its electronic components and cables. To ensure the normal operation of the device and prolong its service life, use the device in an indoor environment that is 3 kilometers away from the sea.

Maintenance Requirements

DANGER

- 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.

- 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.
- 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

Foreword I
Important Safeguards and Warnings IV
1 Overview 1
1.1 Introduction 1
1.2 Login Mode 1
2 The Grand Tour 2
2.1 DHI-IVD7132-1M and DHI-IVD7132-2M 2
2.1.1 Front Panel 2
2.1.2 Rear Panel 3
2.2 DHI-IVD3116-1M/DHI-IVD3116-2M/DHI-IVD3116-1I/DHI-IVD5148 series/DHI-IVD5148WT-1I/DHI-IVD5148WT-1I-4G/DHI-IVD5148-1I-4G/DHI-IVD5348 4
2.2.1 Front Panel 4
2.2.2 Rear Panel 7
3 Hardware Installation 12
3.1 Installation Flow 12
3.2 Unpacking the Box 12
3.3 HDD Installation 13
3.3.1 DHI-IVD7132-1M and DHI-IVD7132-2M 13
3.3.2 DHI-IVD3116-1M and DHI-IVD3116-2M 15
3.3.3 DHI-IVD3116-1I and DHI-IVD5148 series 18
3.3.4 DHI-IVD5148WT-1I 19
3.3.5 DHI-IVD5348 Series 22
3.4 Cable Connection 23
3.4.1 Alarm Connection 23
3.4.2 Connection Diagram 27
4 Starting the Device 28
5 Initial Settings 29
5.1 Initializing the Device 29
5.2 Quick Settings 31
5.3 Login 34
5.3.1 Logging in to the PC Client 34
5.3.2 Logging in to Local Interface 35
5.3.3 Logging in to Webpage 35
5.4 Home Page 36
5.5 Configuring Remote Devices 40
5.5.1 Initializing Remote Devices 40
5.5.2 Adding Remote Devices 42
6 AI Operations 51

6.1 Overview....51
6.2 Scheduled Tour....52
6.2.1 Configuring Tasks by Time Intervals....54
6.2.2 Configuring Tasks by Tours....55
6.3 AcuPick....57
6.3.1 Enabling AcuPick....57
6.3.2 Applying AcuPick....58
6.4 Advanced Search....66
6.4.1 Enabling Advanced Search....66
6.4.2 Applying Advanced Search....68
6.5 Face Detection....71
6.5.1 Enabling the Smart Plan....71
6.5.2 Configuring Face Detection....72
6.5.3 Live View of Face Detection....73
6.5.4 Face Search....75
6.6 Face Recognition....86
6.6.1 Configuration Modes....87
6.6.2 Face Comparison by Camera....87
6.6.3 Face Detection by Camera + Face Comparison by Recorder....95
6.6.4 Face Comparison by Camera + Face Comparison by Recorder....108
6.6.5 Face Detection by Recorder + Face Recognition by Recorder....109
6.6.6 Video Metadata + Face Comparison by Recorder....111
6.7 Video Metadata....112
6.7.1 Enabling the Smart Plan....112
6.7.2 Configuring Video Metadata....112
6.7.3 Live View of Video Metadata....115
6.7.4 AI Search....117
6.7.5 Viewing AI Report....120
6.8 IVS....121
6.8.1 Enabling the Smart Plan....121
6.8.2 Configuring IVS....121
6.8.3 Live View of IVS....125
6.8.4 IVS Search....127
6.9 Call Alarm....128
6.9.1 Enabling the Smart Plan....128
6.9.2 Configuring Call Alarm....128
6.9.3 Live View of Call Alarm....129
6.9.4 Call Alarm Search....129
6.10 High-Rise Littering....129
6.10.1 Live View....129

6.10.2 High-Rise Littering Search....130
6.11 Smart Application Orchestration....130
6.12 Text-Defined Alarms....139
7 General Operations....141
7.1 Live and Monitor....141
7.1.1 View Management....142
7.1.2 Device Tree....153
7.1.3 (Optional) PTZ....155
7.1.4 (Optional) PTRZ....161
7.2 Recorded Files....163
7.2.1 Playing back Recorded Videos....163
7.2.2 Clipping a Video....167
7.2.3 Video Tag....168
7.2.4 Locking Files....169
7.2.5 Playing Back Snapshots....169
7.2.6 Backing up Files....169
7.2.7 Watermark Verification....170
7.3 Display Management....170
7.3.1 Multiple-Screen Control....171
7.3.2 Sub Screen Operations....171
7.3.3 Locking the Screen....172
7.4 Audio Management....172
7.5 Event Center....173
7.5.1 Real-Time Events....173
7.5.2 Event History....175
8 System Configuration....177
8.1 Device Management....177
8.1.1 Viewing Remote Devices....177
8.1.2 Configuring Intelligent Compression....178
8.1.3 Changing IP Address....182
8.1.4 Configuring Remote Devices....185
8.1.5 Exporting Remote Devices....192
8.1.6 Importing Remote Devices....193
8.1.7 Connecting Remote Devices....193
8.1.8 Deleting Remote Devices....193
8.2 Network Management....194
8.2.1 Basic Network....194
8.2.2 Network Application....201
8.3 Event Management....221
8.3.1 Overview....222

8.3.2 Batch Configuring Events 223
8.3.3 Alarm Actions 224
8.3.4 Local Device 231
8.3.5 Remote Device 240
8.4 Storage Management 245
8.4.1 Storage Resource 246
8.4.2 Storage Settings 256
8.5 Algorithm 263
8.5.1 Configuring the AI Module 263
8.5.2 Updating the Algorithm 264
8.5.3 Generating Algorithm Based on Texts 265
8.6 System Management 267
8.6.1 General Configurations 267
8.6.2 Configuring Time Plan 273
8.6.3 Account Management 275
8.6.4 Security 282
8.7 AI Application 294
8.7.1 Resource Management 294
8.7.2 AI Analysis Task 295
8.7.3 Extracting Eigenvector Again 295
8.7.4 1:1 Face Recognition 296
9 System Maintenance 298
9.1 Overview 298
9.2 System Information 299
9.2.1 Viewing Device Information 299
9.2.2 Viewing Legal Information 299
9.2.3 Viewing Algorithm Version 299
9.2.4 Viewing Storage Information 300
9.2.5 Online User 300
9.3 System Resources 301
9.3.1 Viewing Device Resources 301
9.3.2 Viewing AI Module Information 301
9.4 Network Detection 301
9.5 Disk Maintenance 302
9.5.1 S.M.A.R.T Detection 302
9.5.2 System Disk Health Detection 303
9.5.3 Firmware Update 303
9.6 Log Info 303
9.6.1 Log Classification 304
9.6.2 Log Search 304

9.7 One-click Diagnosis 305
9.8 Advanced Maintenance 305
9.8.1 Export 305
9.8.2 Running Logs 305
9.8.3 Operator Maintenance 306
9.9 Updating 306
9.9.1 Host Update 306
9.9.2 Algorithm Update 307
9.9.3 Camera Update 307
9.10 Maintenance Management 307
9.10.1 Default 308
9.10.2 Maintenance 308
9.10.3 Configuration Backup 309
10 PC Client 310
10.1 Page Description 310
10.2 History Record 310
10.3 Viewing Downloads 310
10.4 Configuring the Client Settings 311
10.5 Viewing the Client Version 311
11 Log Out, Restart, Shut Down, Lock 312
12 FAQ 314
Appendix 1 Glossary 315
Appendix 2 Mouse and Keyboard Operations 317
Appendix 2.1 Mouse Operations 317
Appendix 2.2 Virtual Keyboard 317
Appendix 3 HDD Capacity Calculation 319
Appendix 4 Particulate and Gaseous Contamination Specifications 320
Appendix 4.1 Particulate Contamination Specifications 320
Appendix 4.2 Gaseous Contamination Specifications 320
Appendix 5 Security Commitment and Recommendation 322

1 Overview

1.1 Introduction

As an intelligent video device (hereinafter referred to as IVD or the Device), IVD delivers not only the basic video surveillance functions, but also a bunch of advanced AI features including face comparison, perimeter protection, video metadata and ANPR, providing an AI-based all-in-one surveillance solution for customers.

- General functions: Video surveillance, video storage, alarm, record search and playback, and intelligent analysis.
- User-friendly interface.
- 4K and H.265 decoding.
- Applicable to scenarios such as intelligent building, large parking lot, financial planning area and more.

1.2 Login Mode

You can operate the Device by using the local interface, web interface and computer client.

- The local interface is available on select models.
- Operation and system configuration in this manual is mainly based on the computer client. There might be differences from local or web operation.

Table 1-1 Login mode

Login Mode	Operation	Description
Local interface	Connects a monitor, mouse and keyboard to the Device, and then you can view and operate the local menu on the monitor.	Supports all functions of the Device.
Web interface	Connects the Device and your computer into the same network, and remotely access the device through browser (Google Chrome and Firefox) on your computer.	Supports majority functions of the Device, except live, record playback, video download and other video-related functions.
PC client	Connects the Device and your computer into the same network, download and install the computer client on your computer, and then remotely access the Device with the computer client.	Supports all functions of the Device.

2 The Grand Tour

2.1 DHI-IVD7132-1M and DHI-IVD7132-2M

2.1.1 Front Panel

Figure 2-1 Front panel

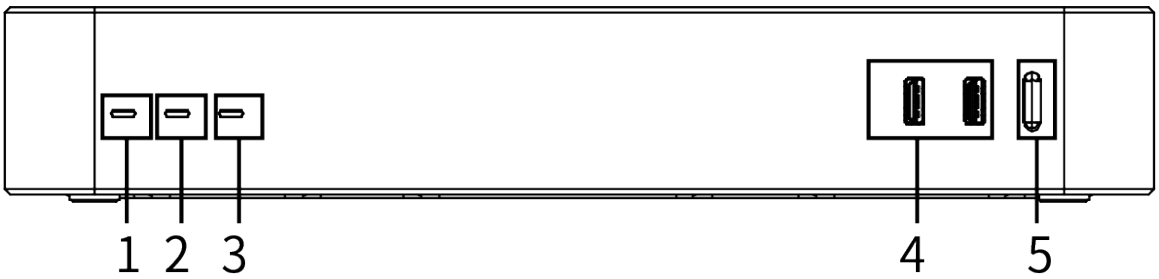


Table 2-1 Front panel description

No.	Button/Port	Description
1	System status indicator light	Displays the system running status. ● The blue light is on: The Device is running properly. ● The indicator light is off: The Device is not running.
2	Alarm indicator light	Displays local alarm input status. ● The red light is on: There is local alarm input. ● The indicator light is off: There is no local alarm input.
3	Network indicator light	Displays current network status. ● The light glows blue: At least one Ethernet port is connected to the network. ● The light is off: No Ethernet ports are connected to the network.
4	USB port	Connects to external devices such as USB storage device, keyboard and mouse.
5	Power button	Start or shut down the Device.

2.1.2 Rear Panel

Figure 2-2 Rear panel

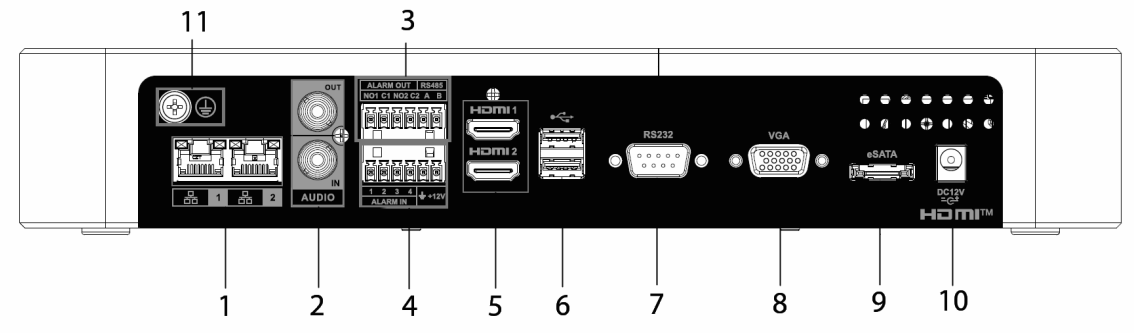


Table 2-2 Rear panel description

No.	Name	Description
1	Network port	10/100/1000 Mbps self-adaptive Ethernet port.
2	Audio port	Audio input and output ports.
3	Alarm output	2 groups of alarm output ports (NO1 C1–NO8 C8). Outputs alarm signal to the alarm device. Make sure that there is power to the external alarm device. ● NO: Alarm output port of Normally Open type. ● C: Common alarm output port. ● A and B: Control the A/B cable of the RS-485 device. It is used to connect to the PTZ camera. Please parallel connect 120 Ω between A/B cables if there are too many PTZ decoders.
4	Alarm input	● 4 groups of alarm input ports: ALARM1–ALARM4. The alarm becomes valid in low level. ● ⏚: GND end.
5	HDMI port	High definition audio and video signal output port. The port outputs the uncompressed high definition video and multi-channel audio data to the connected display with HDMI port.
6	USB port	Connects to external devices such as USB storage device, keyboard and mouse.
7	RS-232 port	RS-232 COM debug. It is for general COM debug, setting IP address and transmitting transparent COM data.
8	VGA port	VGA video output port. Outputs analog video signal. It can connect to the monitor to view analog video. The VGA port and HDMI port support simultaneous video sources output.
9	eSATA port	SATA peripheral port. Connects to SATA port.

No.	Name	Description
10	Power input port	Inputs 12 VDC power.
11	GND	Ground end.

2.2 DHI-IVD3116-1M/DHI-IVD3116-2M/DHI-IVD3116-1I/DHI-IVD5148 series/DHI-IVD5148WT-1I/DHI-IVD5148WT-1I-4G/DHI-IVD5148-1I-4G/DHI-IVD5348

2.2.1 Front Panel

The images below are for reference only. Please refer to the actual device for detailed information.

Figure 2-3 DHI-IVD3116-1M/DHI-IVD3116-2M front panel

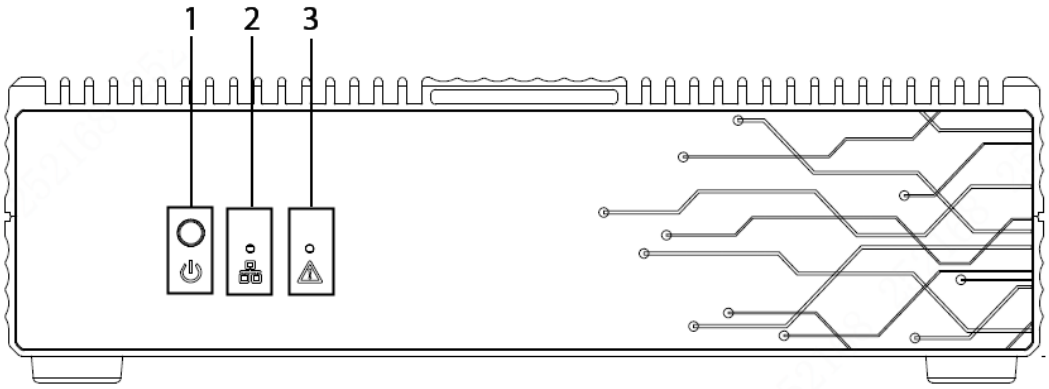


Figure 2-4 DHI-IVD3116-1I/DHI-IVD5148 series/DHI-IVD5148WT-1I front panel

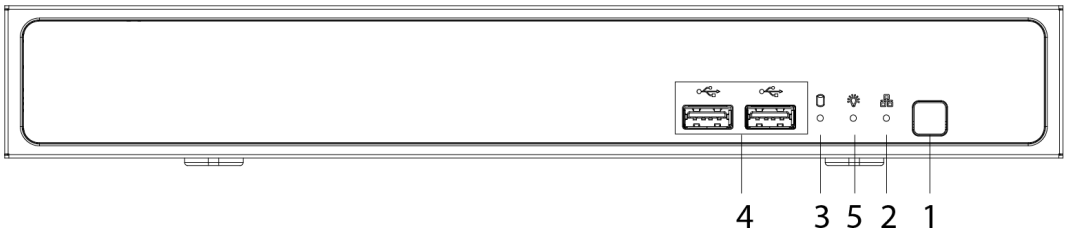


Figure 2-5 DHI-IVD5148-1I-4G front panel

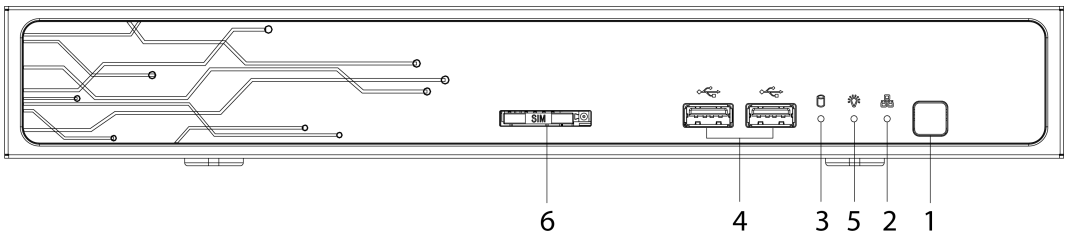


Table 2-3 Front panel description

No.	Button/Port	Description
1	Power button	Start or shut down the Device.
2	Network indicator light	Displays current network status. ● The light glows blue: At least one Ethernet port has connected to the network. ● The light is off: No Ethernet ports are connected to the network.
3	System status indicator light	Displays the system running status. ● The blue light is on: The Device is running properly. ● The indicator light is off: The device is not running.
4	USB port	Connects to external devices such as USB storage device, keyboard and mouse.
5	Alarm indicator light	Displays local alarm input status. ● The red light is on: There is local alarm input. ● The indicator light is off: There is no local alarm input.
6	SIM card slot	Install a standard SIM card to connect the Device to the network.

Figure 2-6 DHI-IVD5148WT-1I-4G front panel

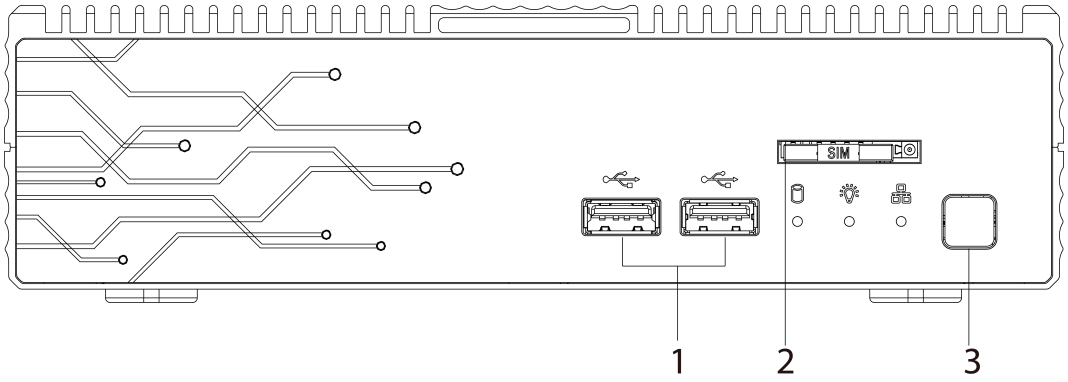


Table 2-4 Front panel description

No.	Button/Port	Description
1	USB port	Connects to external devices such as USB storage device, keyboard and mouse.
2	SIM card slot	Install a standard SIM card to connect the Device to the network.
3	Power button	Start or shut down the Device.

Figure 2-7 DHI-IVD5348 front panel

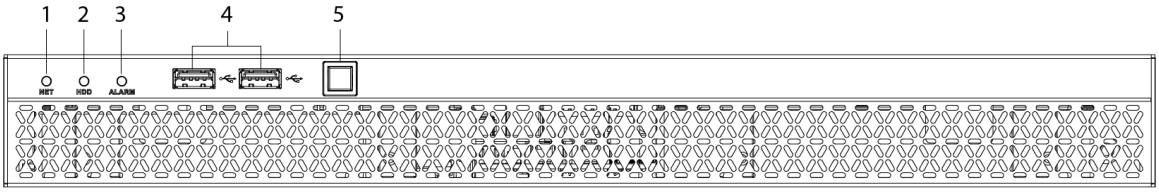


Table 2-5 Front panel description

No.	Button/Port	Description
1	Network indicator light	Displays current network status. ● The light glows blue: At least one Ethernet port has connected to the network. ● The light is off: No Ethernet ports are connected to the network.
2	Storage status indicator light	Displays storage status. ● Solid red: There is a storage failure, such as no available disks, storage error or insufficient storage capacity. ● The indicator light is off: Indicates normal storage status.
3	Alarm indicator light	Displays local alarm input status. ● The red light is on: There is local alarm input. ● The indicator light is off: There is no local alarm input.
4	USB port	Connects to external devices such as USB storage device, keyboard and mouse.
5	Power (Integrated light switch)	Boot up or shut down the device. Power indicator light status is as follows: ● When device is off (indicator light is off), press the button for a short period to boot up device. ● When device is running, (blue indicator light is on), press the button for at least 4 seconds to shut down the device.

2.2.2 Rear Panel

Figure 2-8 DHI-IVD3116-1M/DHI-IVD3116-2M rear panel

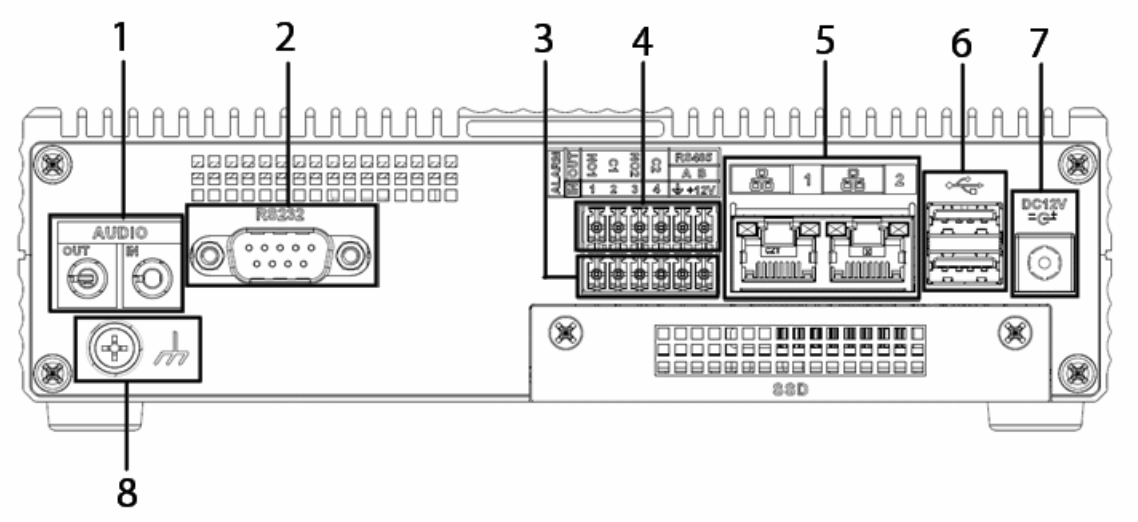


Figure 2-9 DHI-IVD3116-1I rear panel

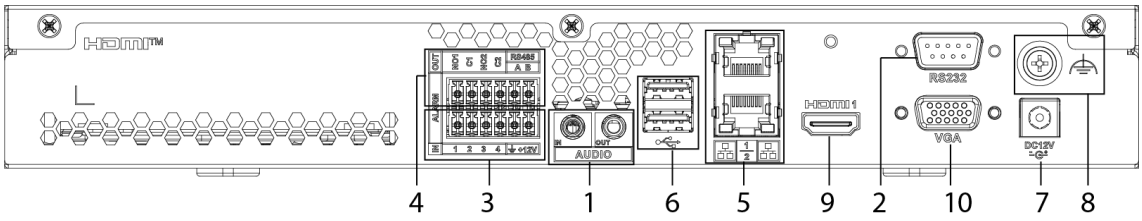


Figure 2-10 DHI-IVD5148 rear panel

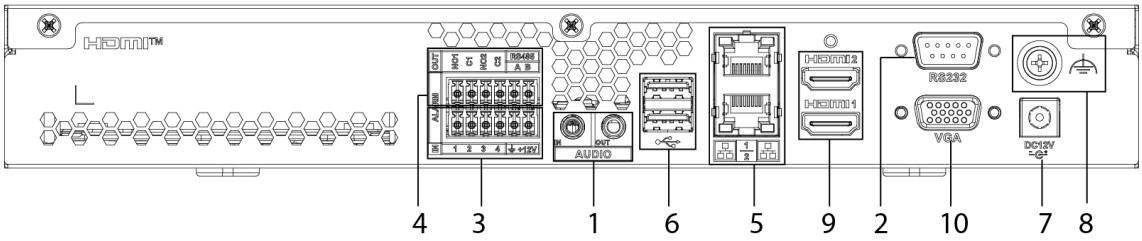


Figure 2-11 DHI-IVD5148WT-1I rear panel

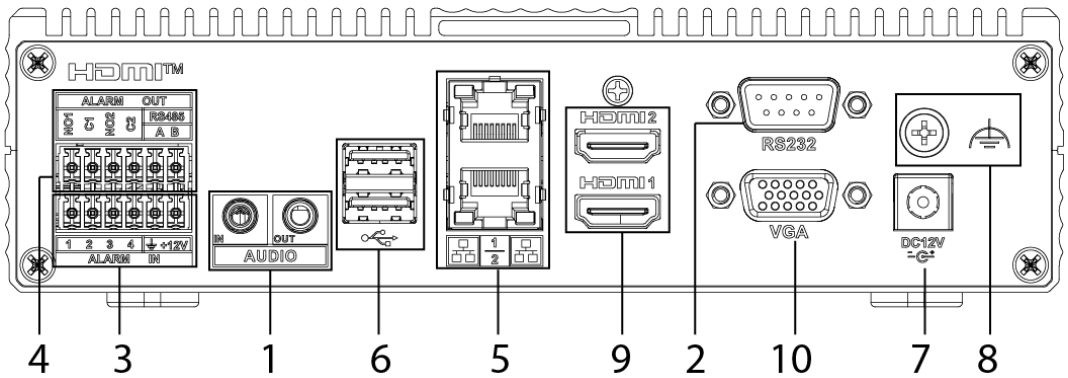


Figure 2-12 DHI-IVD5148WT-1I-4G

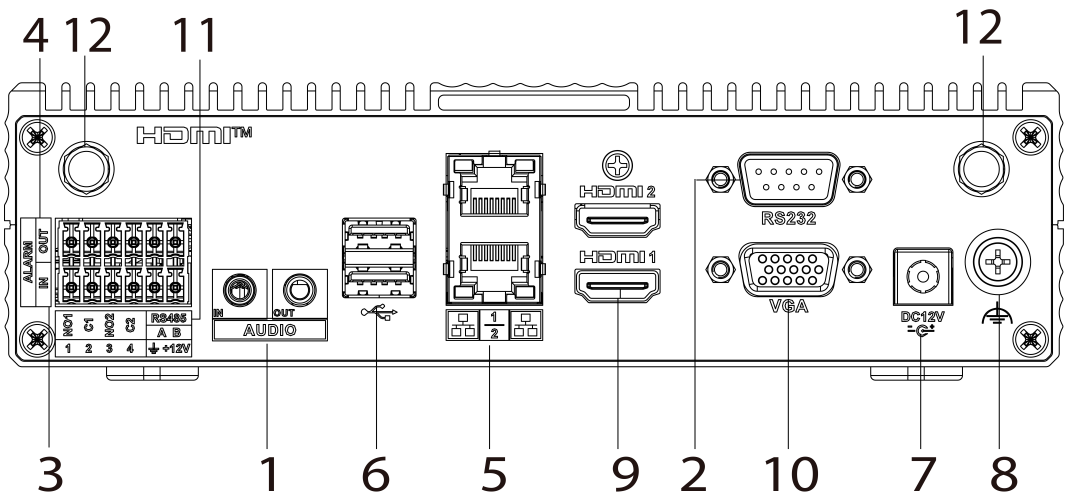


Table 2-6 Rear panel description

No.	Name	Description
1	Audio port	Audio input and output ports.
2	RS-232 port	RS-232 COM debug. It is for general COM debug port, setting IP address, and transmitting transparent COM data.
3	Alarm input	• 4 groups of alarm input ports: ALARM1–ALARM4. The alarm becomes valid in low level. • ⏚: GND end.
4	Alarm output	2 groups of alarm output ports (NO1 C1–NO8 C8). Output alarm signal to the alarm device. Please make sure that there is power to the external alarm device. • NO: Alarm output port of Normally Open type. • C: Common alarm output port. • A and B: Control the A/B cable of the RS-485 device. It is used to connect to the PTZ camera. Please parallel connect 120 Ω between A/B cables if there are too many PTZ decoders.
5	Network port	10/100/1000 Mbps self-adaptive Ethernet port.
6	USB port	Connects to external devices such as USB storage device, keyboard and mouse.
7	Power input port	Inputs 12 VDC power.
8	GND	Ground end.

No.	Name	Description
9	HDMI port	High definition audio and video signal output port. The port outputs the uncompressed high definition video and multi-channel audio data to the connected display with HDMI port.
10	VGA port	VGA video output port. Outputs analog video signal. It can connect to the monitor to view analog video. The VGA port and HDMI port support simultaneous video sources output.
11	RS-485 port	Connects to the external devices such as PTZ and so on.
12	Antenna	The external antenna needs to be used with the antenna glue stick in the installation attachment.

Figure 2-13 DHI-IVD5148-1I-4G rear panel

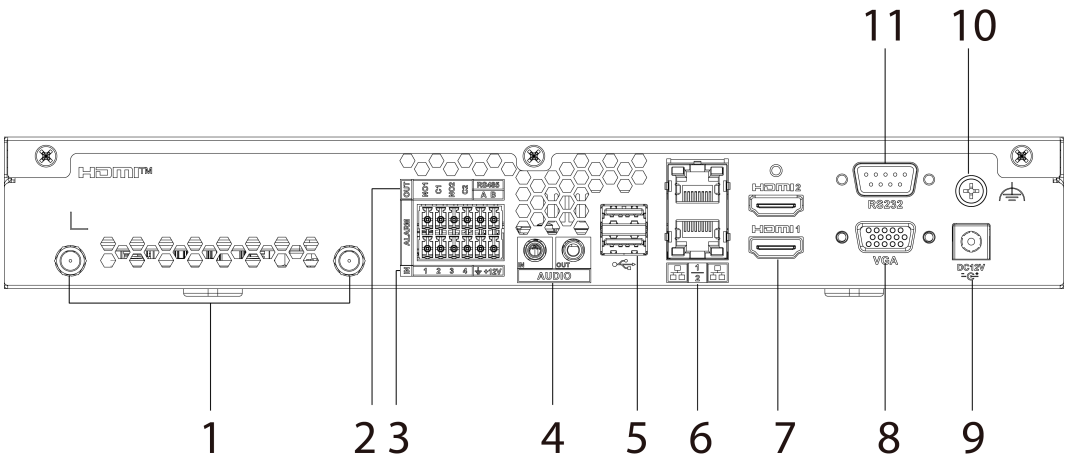


Table 2-7 Rear panel description

No.	Name	Description
1	Cellular network antenna port	Used to connect external signal line to receive 4G signal.
2	Alarm output	2 groups of alarm output ports (NO1 C1–NO8 C8). Output alarm signal to the alarm device. Please make sure that there is power to the external alarm device. ● NO: Alarm output port of Normally Open type. ● C: Common alarm output port. ● A and B: Controls the A/B cable of the RS-485 device. It is used to connect to the PTZ camera. Please parallel connect 120 Ω between A/B cables if there are too many PTZ decoders.
3	Alarm input	● 4 groups of alarm input ports: ALARM1–ALARM4. The alarm becomes valid in low level. ● ⏚: GND end.

No.	Name	Description
4	Audio port	Audio input and output ports.
5	USB port	Connects to external devices such as USB storage device, keyboard and mouse.
6	Network port	10/100/1000 Mbps self-adaptive Ethernet port.
7	HDMI port	High definition audio and video signal output port. The port outputs the uncompressed high definition video and multi-channel audio data to the connected display with HDMI port.
8	VGA port	VGA video output port. Outputs analog video signal. It can connect to the monitor to view analog video. The VGA port and HDMI port support simultaneous video sources output.
9	Power input port	Inputs 12 VDC power.
10	GND	Ground end.
11	RS-232 port	RS-232 COM debug. It is for general COM debug port, setting IP address, and transmitting transparent COM data.

Figure 2-14 DHI-IVD5348 rear panel

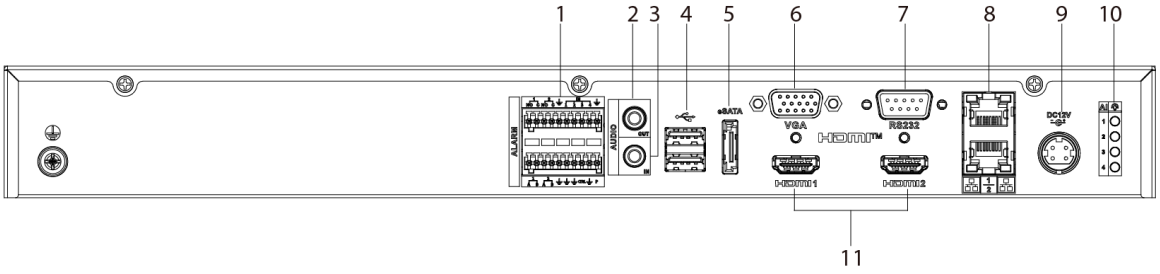


Table 2-8 Rear panel description

No.	Name	Description
1	Alarm input/output	• 4 groups of alarm input ports: ALARM1–ALARM4. The alarm becomes valid in low level. • 2 groups of alarm output ports (NO1 C1–NO2 C2). Output alarm signal to the alarm device. Please make sure that there is power to the external alarm device. ◇ NO: Alarm output port of Normally Open type. ◇ C: Common alarm output port. • A and B: Controls the A/B cable of the RS-485 device. It is used to connect to the PTZ camera. • ⏚: GND end. • ctrl: Variable power output (+12 V). • P: Constant power output (+12 V).
2	AUDIO OUT	Audio input and output ports.
3	AUDIO IN	

No.	Name	Description
4	USB port	Connects to external devices such as USB storage device, keyboard and mouse.
5	eSATA port	It is an external SATA interface that can connect to SATA devices.
6	VGA port	VGA video output port. Outputs analog video signal. It can connect to the monitor to view analog video. The VGA port and HDMI port support simultaneous video sources output.
7	RS-232 port	RS-232 COM debug. It is for general COM debug port, setting IP address, and transmitting transparent COM data.
8	Network port	10/100/1000 Mbps self-adaptive Ethernet port.
9	Power port	Inputs 100–240 VAC power supply.
10	Intelligent module indicator light	Displays intelligent module status. • Light flashes green: The intelligent module is operating normally. • Solid green: There is abnormal operation of the intelligent module. This function is only available when the intelligent module is installed.
11	HDMI port	High definition audio and video signal output port. The port outputs the uncompressed high definition video and multi-channel audio data to the connected display with HDMI port.

3 Hardware Installation

This section introduces HDD installation, cable connection, and more.

- Some series products are heavy. They need several persons to carry or move, in order to prevent personal injury.
- The recommended maximum weight for manual handling is below 25 kg. When there is an increase in lifting frequency/duration, bending, lifting overhead, or working in confined spaces, the limit should be further reduced. When lifted by multiple people, the weight borne by each person should not exceed the individual limit.

3.1 Installation Flow

Figure 3-1 Installation flow



3.2 Unpacking the Box

When you receive the Device, please check against the following checking list. If any of the items are missing or damaged, contact the local retailer or after-sales engineer immediately.

Table 3-1 Checking list

No.	Item		Content
1	Whole package	Appearance	Check whether there is any visible damage.
		Package	Check whether there is any accidental clash during transportation.
		Accessories (list of accessories on the warranty card)	Check whether they are complete.
2	Device	Appearance	Check whether there is any visible damage.
		Device model	Check whether the model is the same as order contract.
		The label on the device	Check whether it is torn or not. Do not tear off, or discard the label. Usually you need to show the serial number when we provide after-sales service.

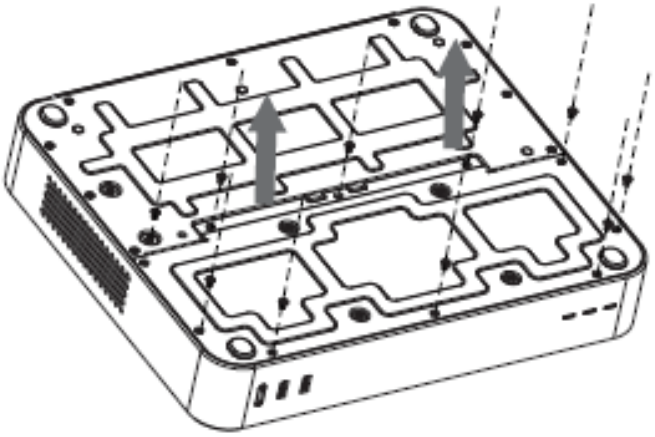
3.3 HDD Installation

3.3.1 DHI-IVD7132-1M and DHI-IVD7132-2M

Procedure

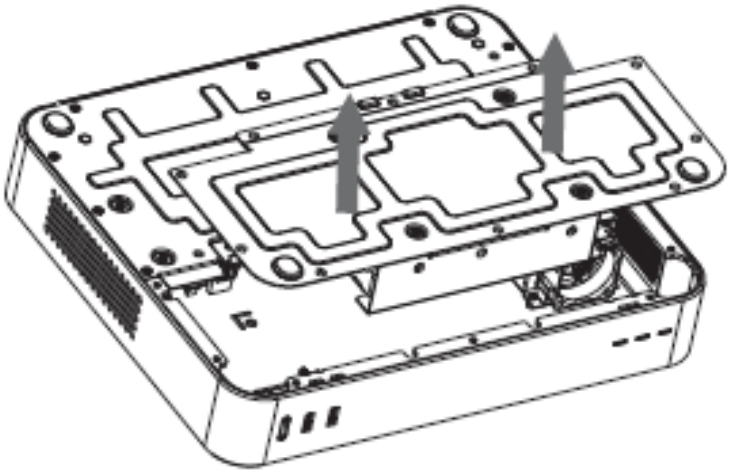
Step 1 Remove the screws on the cover.

Figure 3-2 Remove screws



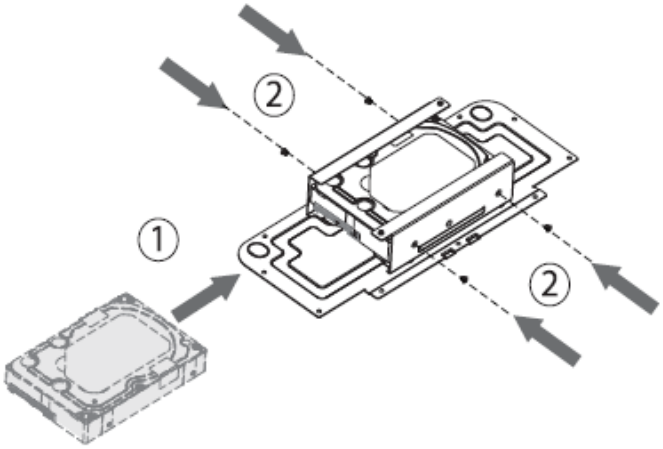
Step 2 Remove the HDD tray attached to the cover.

Figure 3-3 Remove HDD tray



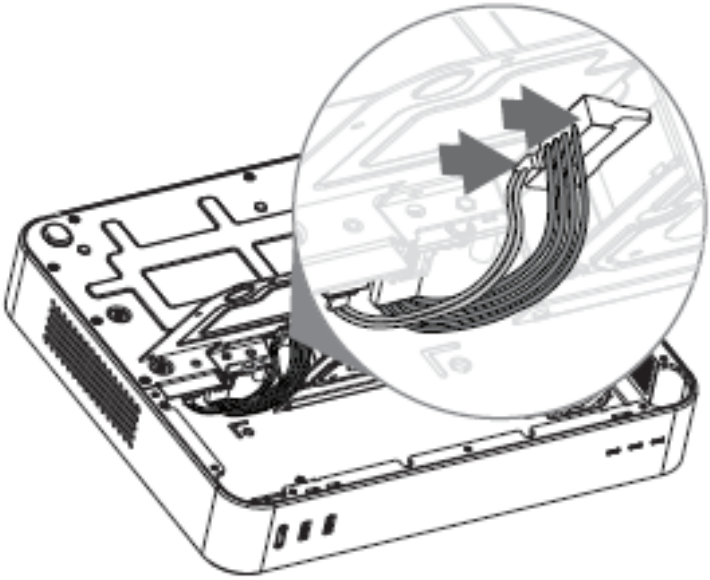
Step 3 Push the HDD into the tray, and then tighten the screws.

Figure 3-4 Install HDD



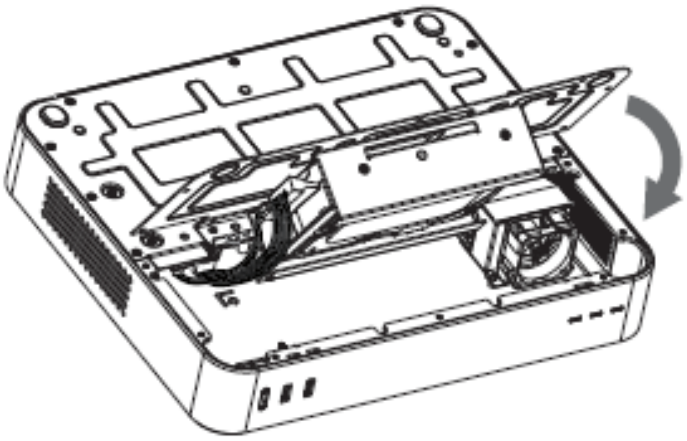
Step 4 Connect HDD data cable and power cord.

Figure 3-5 Connect cables



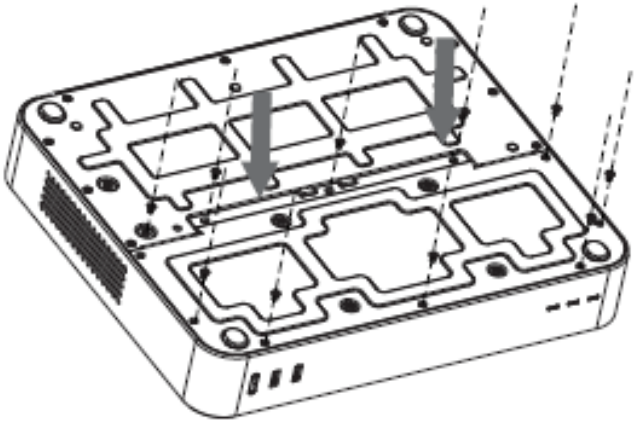
Step 5 Close the cover.

Figure 3-6 Close cover



Step 6 Tighten the screws onto the cover.

Figure 3-7 Tighten screws

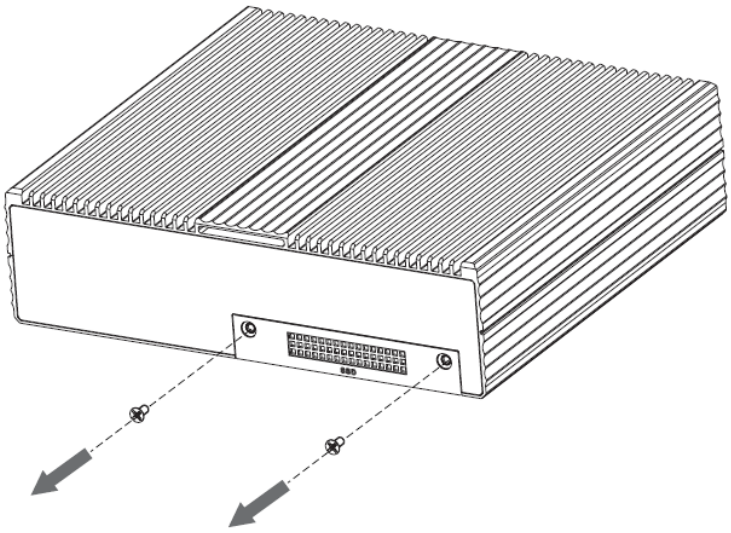


3.3.2 DHI-IVD3116-1M and DHI-IVD3116-2M

Procedure

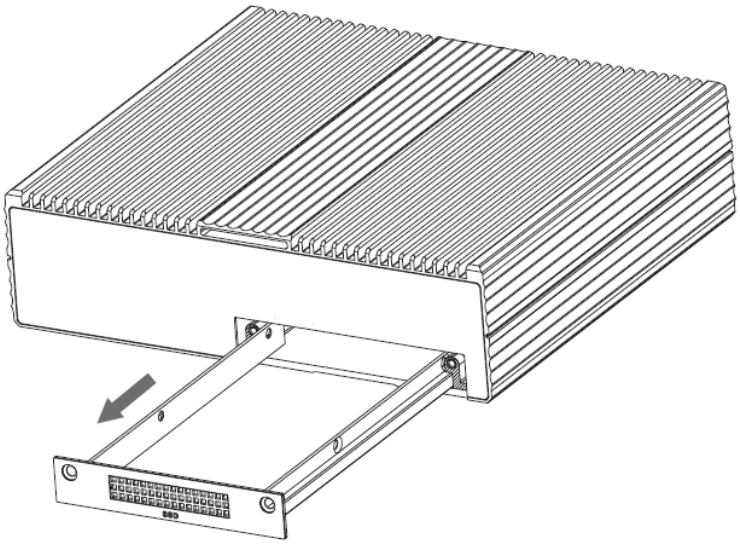
Step 1 Remove the screws on the HDD slot.

Figure 3-8 Remove screws



Step 2 Pull out the HDD tray.

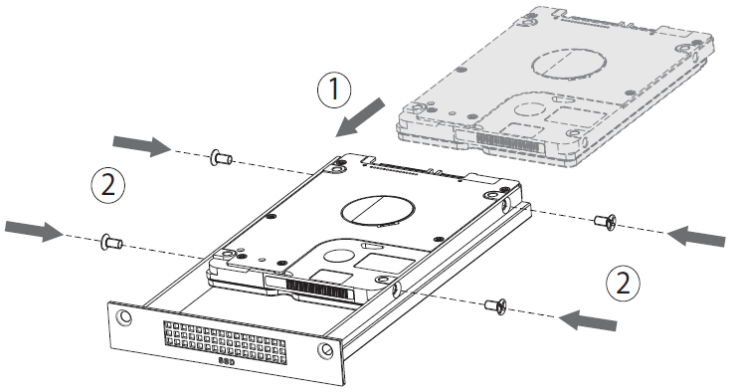
Figure 3-9 Pull out the HDD tray



Step 3 Push the HDD into the tray, and then tighten the screws.

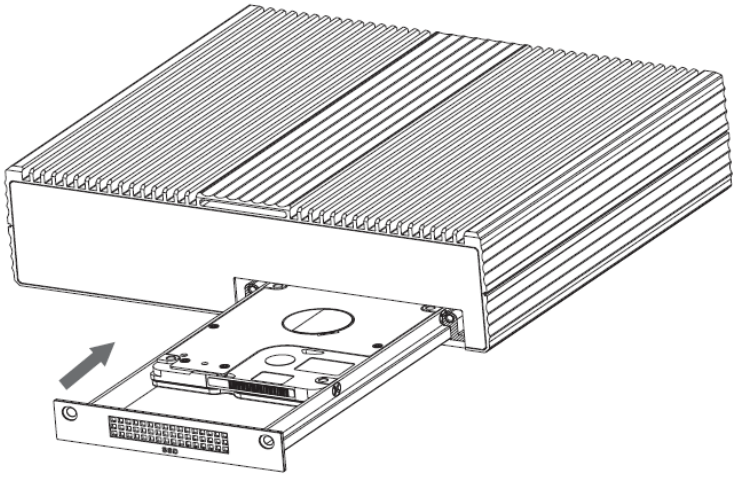
Make sure to use a 2.5-inch SATA HDD with height no more than 9 mm.

Figure 3-10 Remove the screws



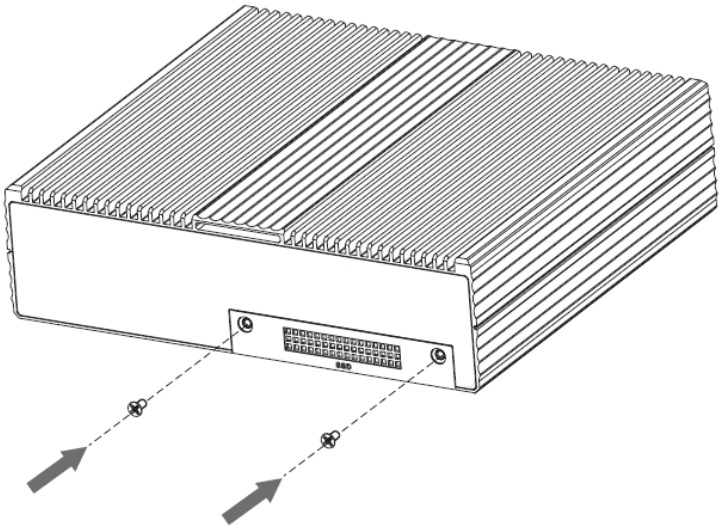
Step 4 Push the HDD tray back into the HDD slot.

Figure 3-11 Push back the HDD tray



Step 5 Tighten the screws on the HDD slot.

Figure 3-12 Tighten screws

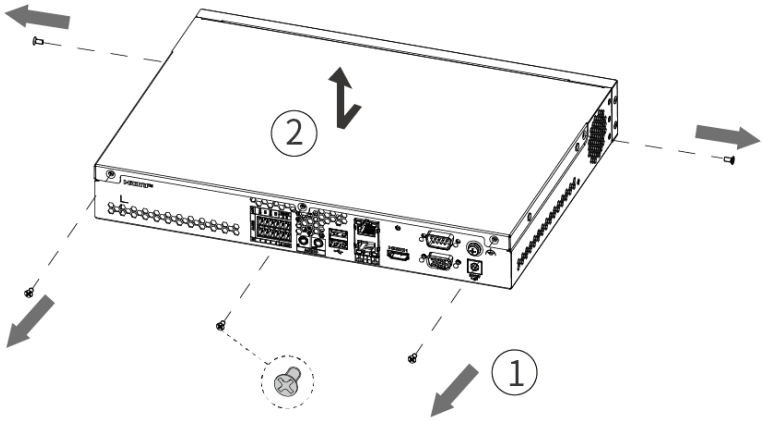


3.3.3 DHI-IVD3116-1I and DHI-IVD5148 series

Procedure

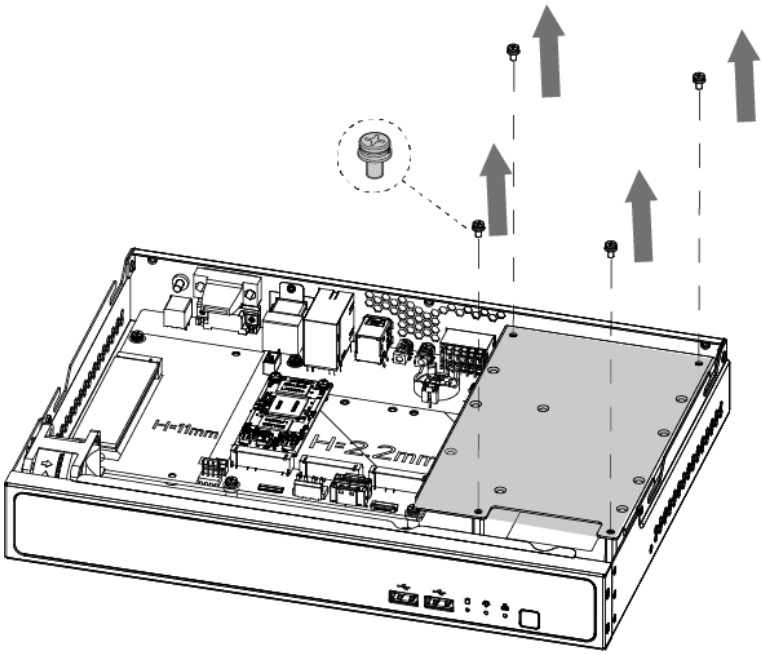
Step 1 Remove the screws, and then take out the cover.

Figure 3-13 Remove screws



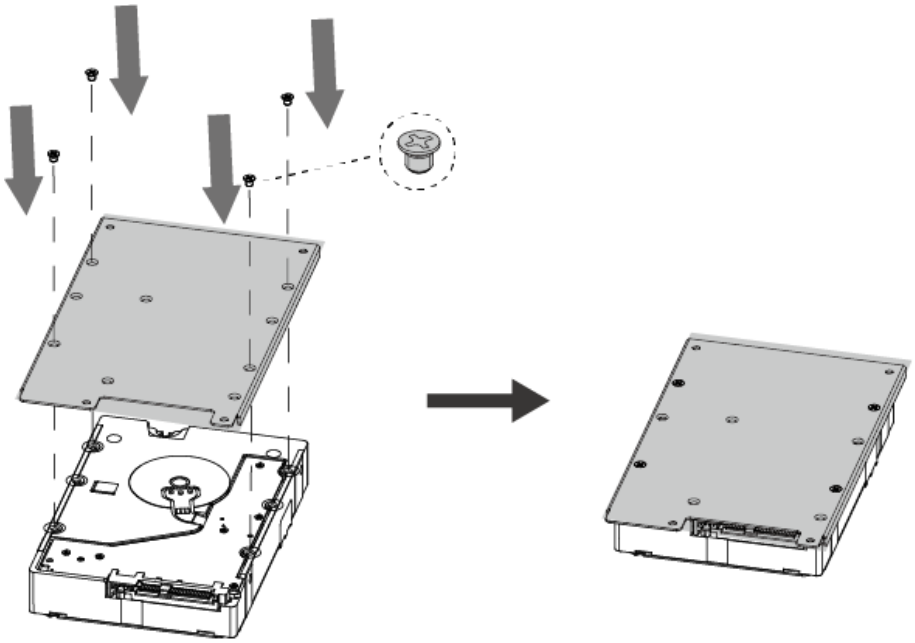
Step 2 Remove the screws on the HDD tray, and then take out the HDD tray.

Figure 3-14 Take out the HDD tray



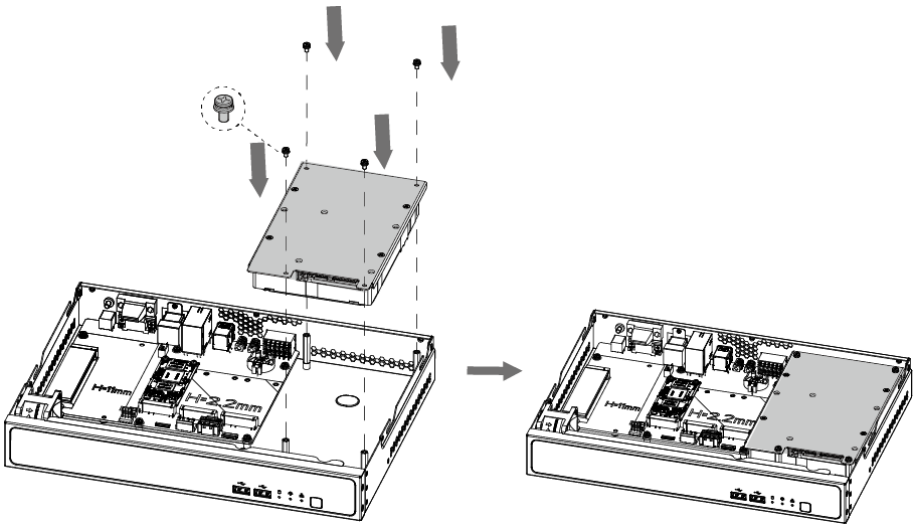
Step 3 Align the 4 screw holes on the HDD with the screw holes on the HDD tray, and then tighten the screws.

Figure 3-15 Install HDD



Step 4 Fix the HDD tray on the Device.

Figure 3-16 Fix the HDD tray



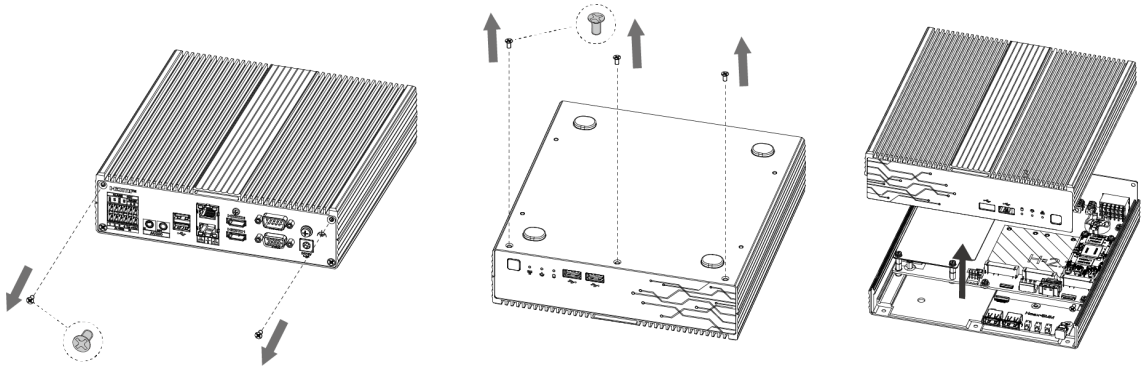
Step 5 Close the cover, and then tighten the screws onto the cover.

3.3.4 DHI-IVD5148WT-1I

Procedure

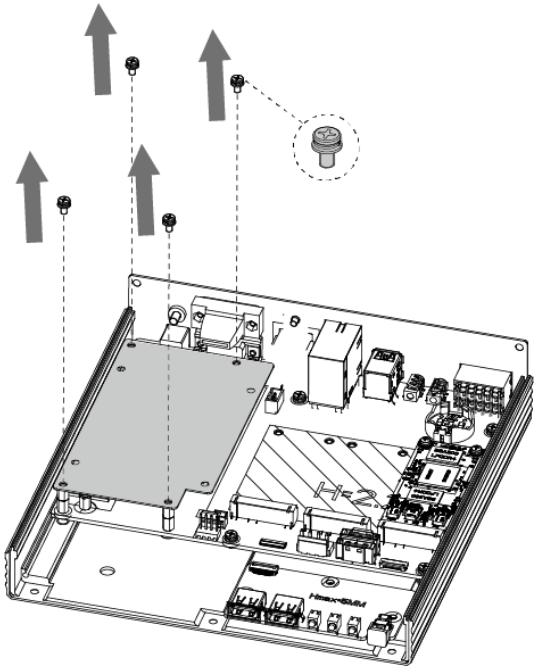
Step 1 Remove the 2 screws on the rear panel, and then remove the 3 screws on the bottom to detach the cover.

Figure 3-17 Detach the cover



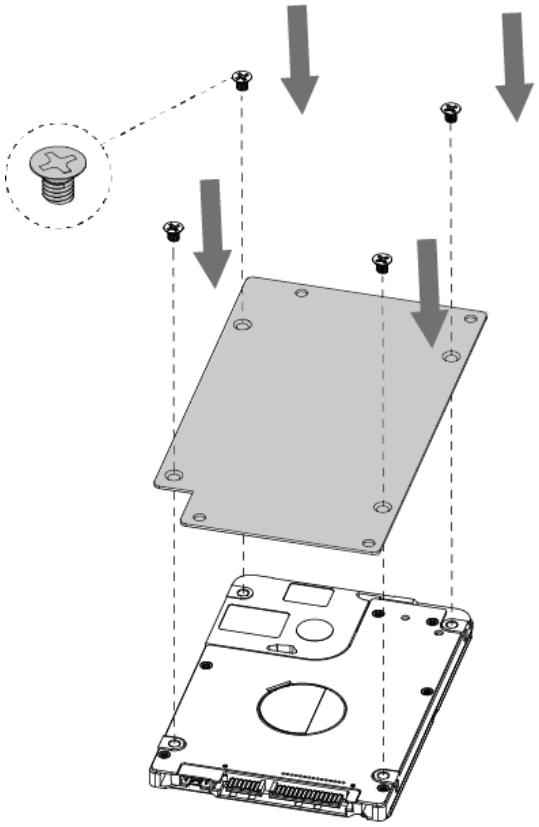
Step 2 Remove the screws from the HDD tray, and then take out the HDD tray.

Figure 3-18 Take out the HDD tray



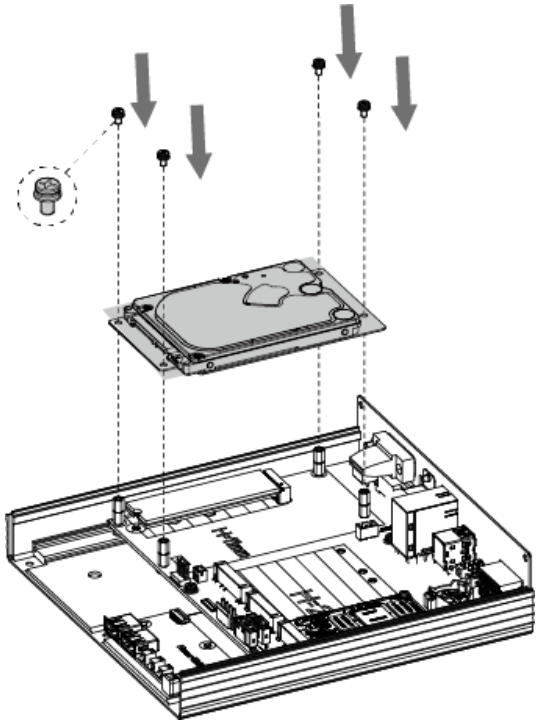
Step 3 Align the 4 screw holes on the HDD with the screw holes on the HDD tray, and then tighten the screws.

Figure 3-19 Install HDD



Step 4 Fix the HDD tray on the Device.

Figure 3-20 Fix the HDD tray



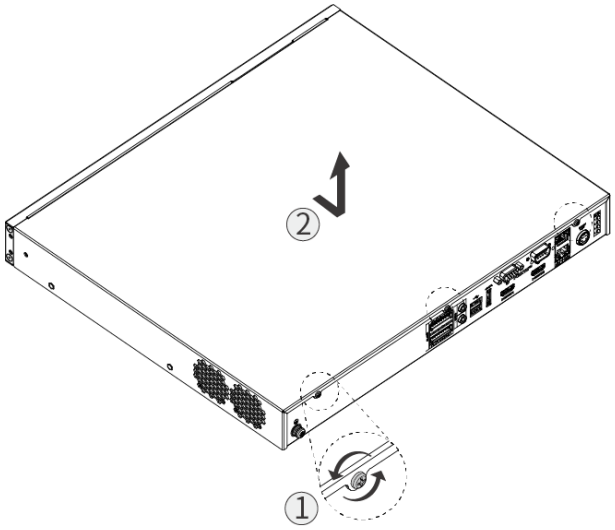
Step 5 Close the cover, and then tighten the screws onto the cover.

3.3.5 DHI-IVD5348 Series

Procedure

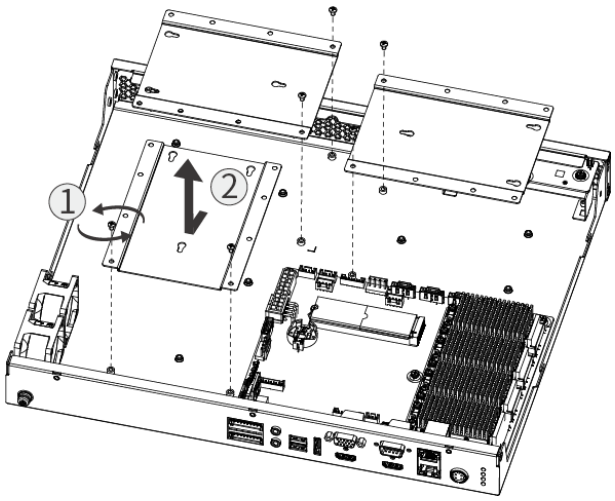
Step 1 Remove the 3 screws on the rear panel, and then remove the chassis cover in the direction indicated by the arrow.

Figure 3-21 Remove screws



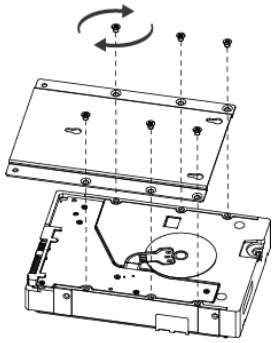
Step 2 Loosen the screws on the HDD holder (each bracket has 2 screws), and then remove the holder from the chassis.

Figure 3-22 Remove HDD holder



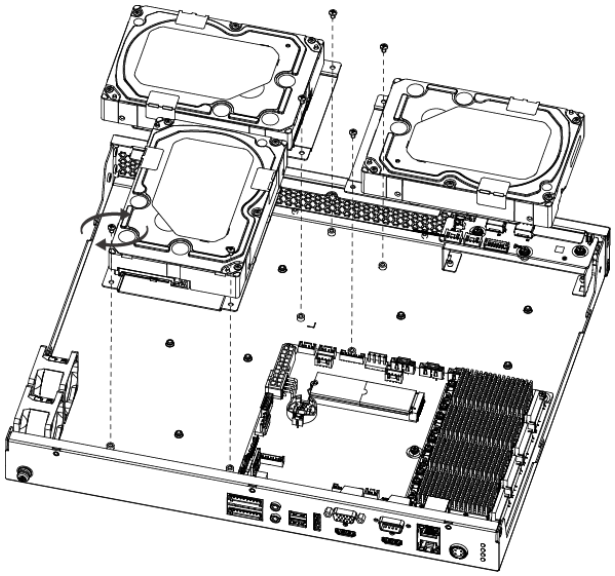
Step 3 Align the 6 screw holes on the HDD to the 6 screw holes on the HDD holder, and then tighten the screws in place.

Figure 3-23 Install HDD



Step 4 Place the HDDs back into the chassis, and then tighten the screws on the edge of the holders.

Figure 3-24 Install HDD holders



Step 5 Connect HDD signal wire and power cord.

Step 6 Put back the cover, and then tighten the 3 screws on the rear panel.

3.4 Cable Connection

The section introduces cable connection of the Device.

3.4.1 Alarm Connection

Before using the alarm, connect alarm input or alarm output device.

3.4.1.1 Connection

The section introduces alarm connection of the Device.

Alarm Input

- Both NO and NC are supported.
- The alarm input port supports alarm signal from ground and device of 12-24 V voltage.
- If the alarm device is connected to the Device and other devices, use relay for isolation.

Alarm Output

The alarm output port cannot be connected to high-power load (less than 1A). When forming output circuit, the excessive current should be prevented from causing damage to the relay. Use the contactor for isolation when applying high-power loads.

PTZ Decoder Connection

- The common-ground must be prepared for PTZ decoder and the Device; otherwise the common-mode voltage might not be able to control the PTZ. It is recommended to use shielded twisted pair, and the shielding layer can be used for common ground.
- Prevent interference from high-voltage power, make reasonable wiring, and take measures for lighting protection.
- Remotely import 120 Ω to reduce resistance reflection and protect the signal quality.
- The Device A line and B line cannot connect to other RS-485 output device in parallel.
- The voltage between the A line and B line of PTZ decoder must be less than 5 V.

Notes to Grounding

- Poor grounding of camera might damage the chip.
- When supplying external power source to the alarm device, the alarm device should be common-grounded with the Device.

3.4.1.2 Alarm Port

Figure 3-25 Alarm port

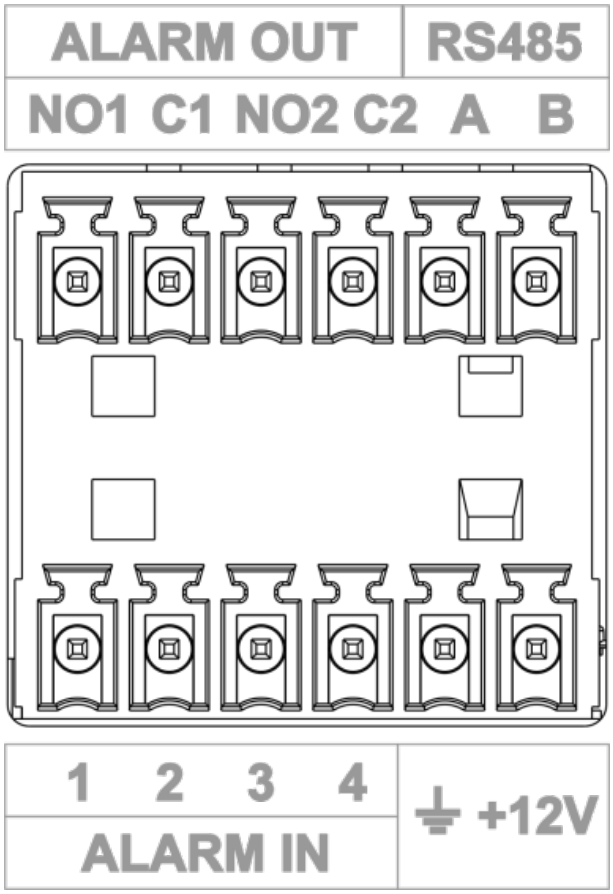


Table 3-2 Alarm port

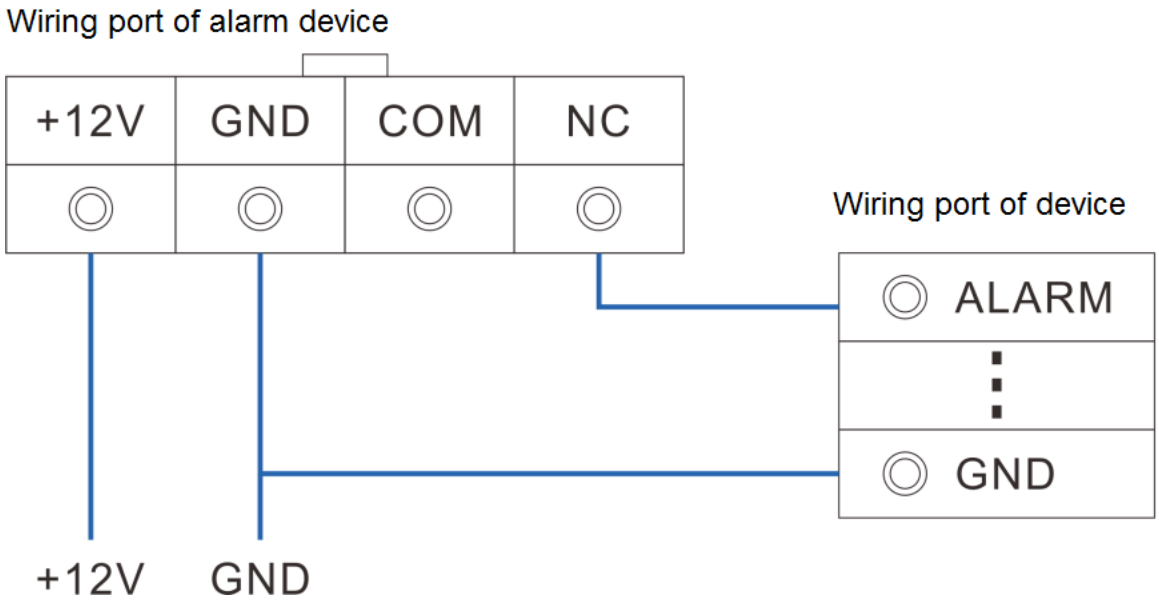
Icon	Description
1–4	They are corresponding to ALARM 1–ALARM 4. The alarm becomes valid in low level.
NO1 C1–NO2 C2	Two groups of normally open linkage output (on-off value).
+12V	Constant power output, 500 mA current.
⏚	Grounding wire.
A, B	A and B: Control the A/B cable of the RS–485 device. It is used to connect to the PTZ camera. Please parallel connect 120 Ω between A/B cables if there are too many PTZ decoders.

3.4.1.3 Alarm Input

Both NO and NC are supported. For connection of NC alarm input port, see the following figures.

- GND and COM of alarm device shall be connected in parallel. The alarm device must be powered with an external power source.
- Connect GND of alarm device with GND of Device in parallel.
- Connect the NC port of alarm device to the alarm input port (1–4).

Figure 3-26 NC alarm input connection



3.4.1.4 Alarm Output

- The alarm output is on-off output (Normally Open Contact), and there should be external power supply to alarm output device.
- RS-485 A line and B line: connecting the A line and B line on the PTZ decoder.
- To avoid overload from damaging the Device, see the parameters about relay.

Table 3-3 Relay parameters of alarm output port

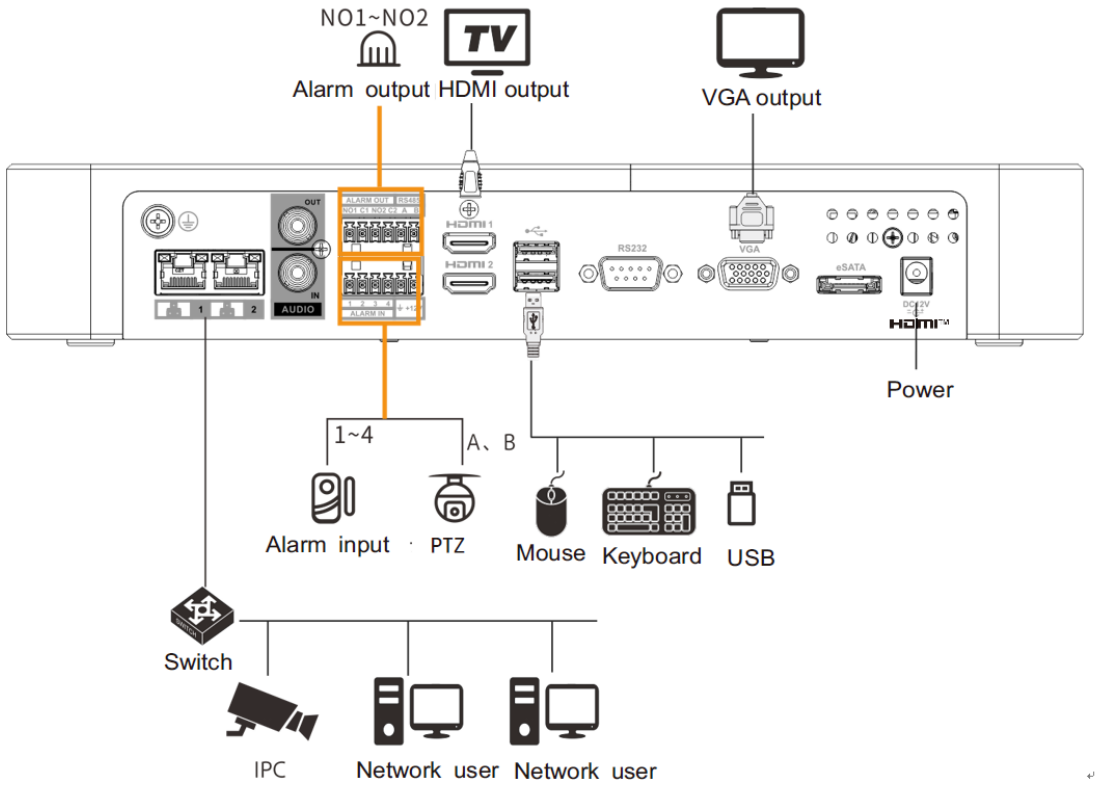
Model		HRB1-S-DC5V
Contact material		Silver
Rated value (resistance load)	Rated power capacity	24 VDC 2 A, 125 VAC 2 A
	Maximum power	62.5 VAC/30 W
	Maximum power voltage	125 VAC, 60 VDC
	Maximum power current	2 A
Insulation	Between contacts	1000 VAC 1 minute
	Between contact and loop	400 VAC 1 minute
Insulation voltage		1,000 MΩ (500 VDC)
Turn-on Time		< 5 ms
Turn-off Time		< 5 ms
Life	Mechanical	300 times per minute
	Electrical	30 times per minute
Operating ambient temperature		-30 ℃ to +70 ℃

3.4.2 Connection Diagram

The following figure is for reference only and might differ from the actual product.

- Display, mouse and keyboard are needed for local operation.
- Before using the smart detection functions such as face detection and face comparison, you must install the AI module first.

Figure 3-27 Connection diagram



4 Starting the Device

- Before starting the device, make sure that the input voltage must match the device power requirement.
- To ensure stable operation of the device and prolong service life of HDD, provide stable voltage with less ripple interference by reference to international standard.
- For device security, connect other cables of the device first, and then connect the device to the power socket.

Press the power button on the rear panel to start the Device.

5 Initial Settings

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

5.1 Initializing the Device

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

Prerequisites

The IP address of the computer must be set to the same subnet as the device's default IP address.

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 **I have read and agree to the terms of Software License Agreement and Privacy Policy.** , and then click **Device Initialization**.

Step 3 Set admin account information and time parameters.

Figure 5-1 Initialization settings

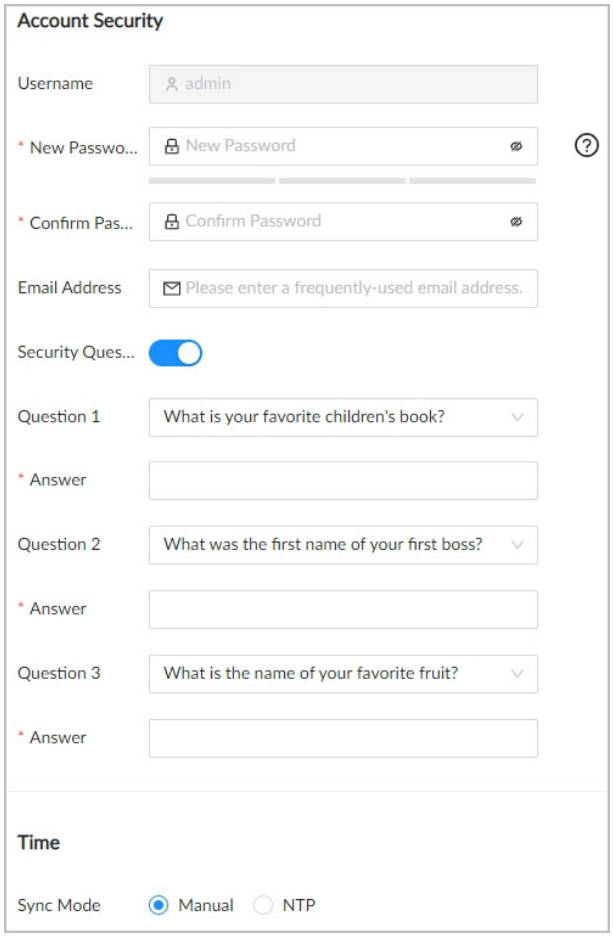


Table 5-1 Description of initialization parameters

Parameter	Description
New Password	Set the login password for the admin user and confirm the password. The password must consist of 8–32 non-blank characters and contain at least two types of the following characters: Uppercase, lowercase, numbers, and special characters (excluding ' " ; : &). Set a high-security password based on the password strength guidelines. Click to view the password requirement.
Confirm Password	
Email Address	You can reset your password using the linked email address or by answering the security questions. If you do not set a backup email address, you can only reset your password locally.
Security Question	

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

Step 4 Click **OK**.

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

5.2 Quick Settings

After the device initialization is complete, enter the **Quick Config** to quickly complete direct storage configuration, AI configuration and network configuration.

Prerequisites

Make sure that at least one Ethernet port has been connected to the network.

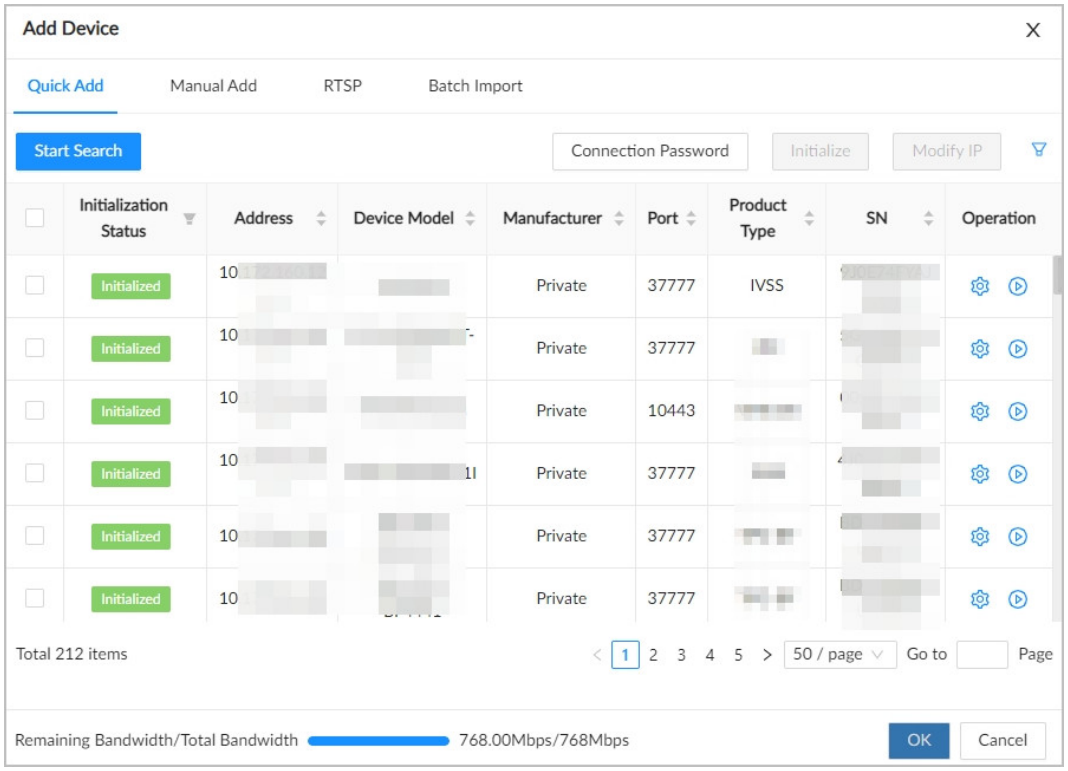
Procedure

Step 1 On the initialization completion page, click **Quick Config**.

Step 2 Add cameras by using quick add, manual add, RTSP, or batch import, and then click **OK** > **Complete** > **Next**.

For more information about adding cameras, see "5.5 Configuring Remote Devices".

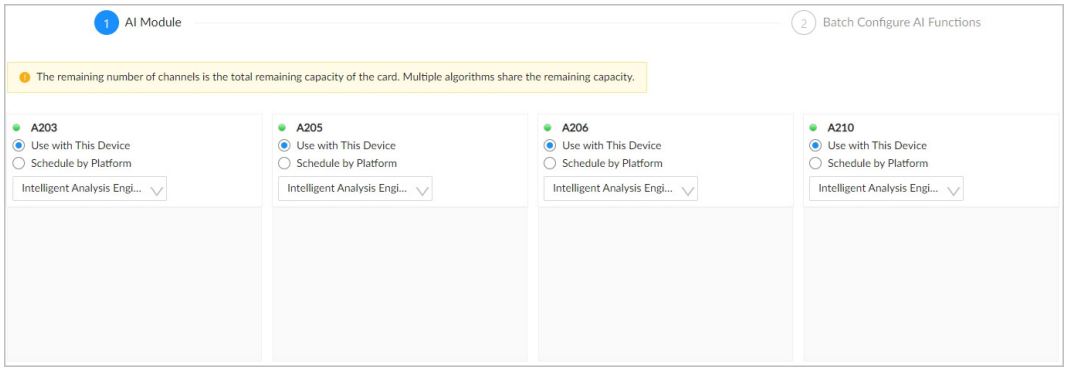
Figure 5-2 Add the camera



Step 3 Configure the AI module and AI functions.

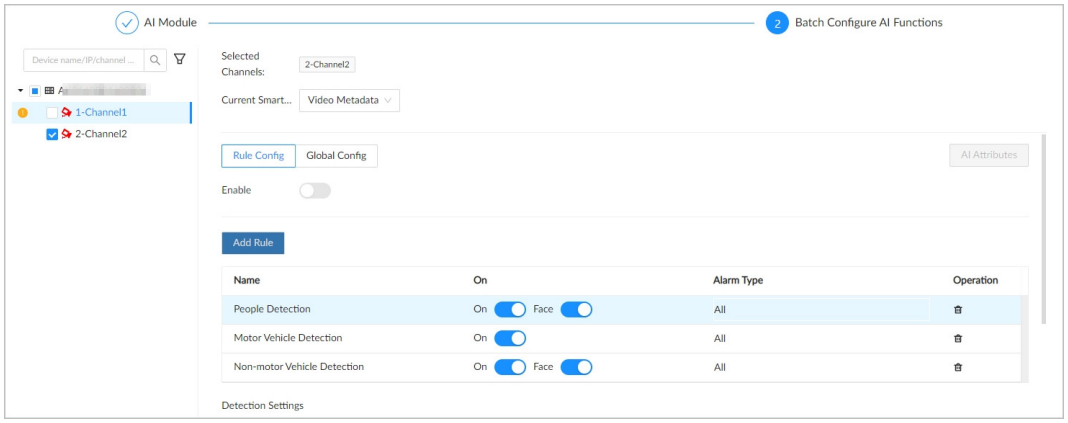
1. Select the AI module type, and then click **Next**.

Figure 5-3 Configure the AI module



2. Select the channel, set the smart features in batches, and then click **Save** > **OK** > **Next**.

Figure 5-4 Configure the AI functions



3. Complete the smart configuration, and then click **Network Config**.

Step 4 Configure the network parameters.

1. Click of the corresponding NIC, set the IP address, and then click **OK**.
2. Select the default network card from the drop-down list of **Default Card** according to your actual needs.

   Only network cards that are connected to the network can be set as the default network card.
3. Choose the DNS server IP type (IPv4 or IPv6) and the method for obtaining the DNS server address.

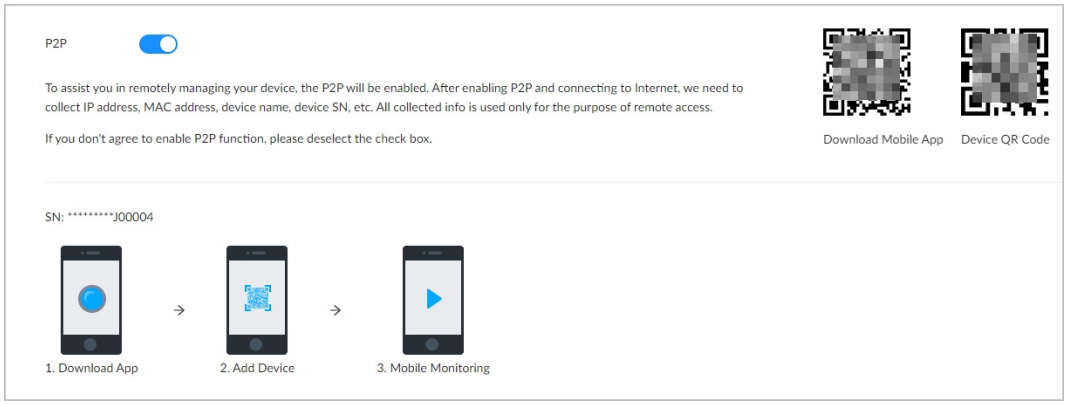
   The methods for obtaining the DNS server address include DHCP and static.

   - 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: Enter the IP addresses of the preferred and alternate DNS servers.

   This step is compulsory if you want to use domain service.
4. You can register the Device to the app for remote monitoring and management. For details, see the corresponding user manual of the app.

   - P2P function is enabled by default. If you do not agree to enable P2P function, deselect the check box.
   - To use the P2P function, we will collect information such as IP address, MAC address, device name and serial number. The collected information is only used for remote access.
   - Some models support this function. Refer to the actual page for details.

Figure 5-5 P2P access



Step 5 Click **Save and Go Home**.

5.3 Login

You can operate the device by using the local interface, web interface and PC client.

- Monitor and mouse are needed for local operation.
- You can remotely access the Device through the web interface and PC client. We recommend you use the PC client.

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

5.3.1 Logging in to the PC Client

Log in to the PC client for system configuration and operation.

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.

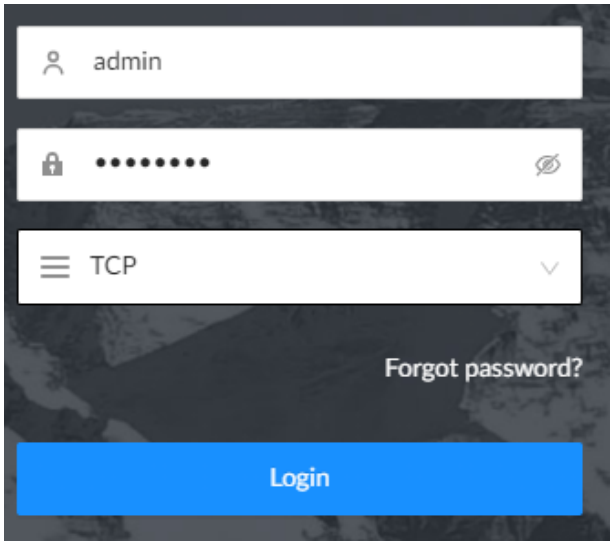
Step 3 Open the PC client, enter the IP address of the Device, and then press Enter.

When the theme of your computer is not Aero, the system will prompt you to switch the theme. To ensure video smoothness, switch your computer to Aero theme.

Step 4 Enter the username and password, select a login type, and then click **Login**.

- The default administrator user name 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.

Figure 5-6 Login (PC client)



5.3.2 Logging in to Local Interface

Prerequisites

Ensure that the Device is connected with display, mouse and keyboard.

Procedure

Step 1 Turn on the Device.

Step 2 Enter user name and password.

- The default administrator user name 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.
- Click to view the password prompt information. It is to help you remember password.
- If you forget the password of the admin account, click **Forgot password?** to reset.

Step 3 Click **Login**.

5.3.3 Logging in to Webpage

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

When you are using a general browser to access the webpage, some functions might be not available. We recommend you use the PC client.

Procedure

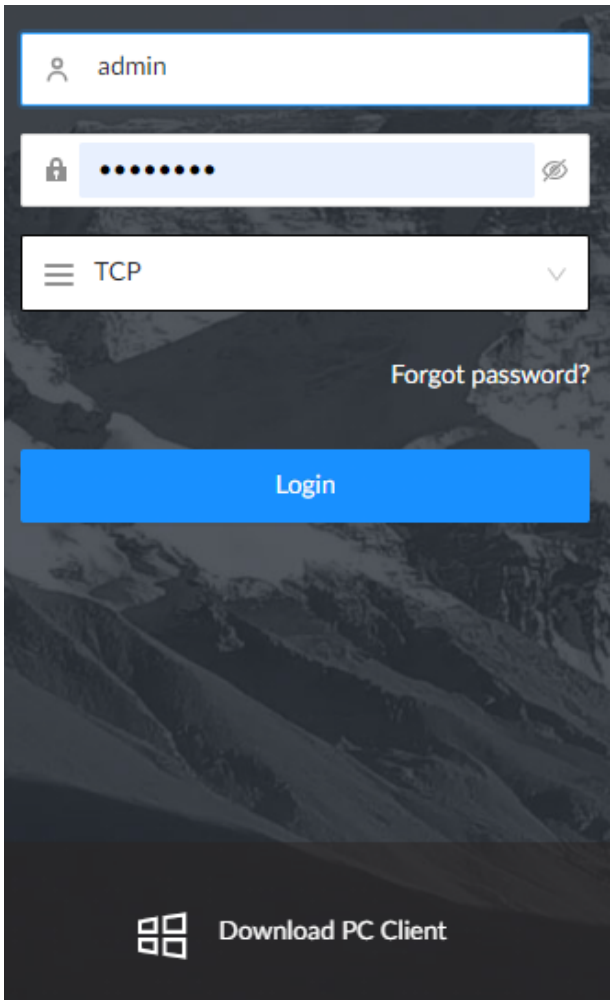
Step 1 Open the browser, enter IP address, and then press Enter.

Step 2 Enter user name and password.

- The default administrator user name 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 Select the login type, and then click **Login**.

Figure 5-7 Login (web)

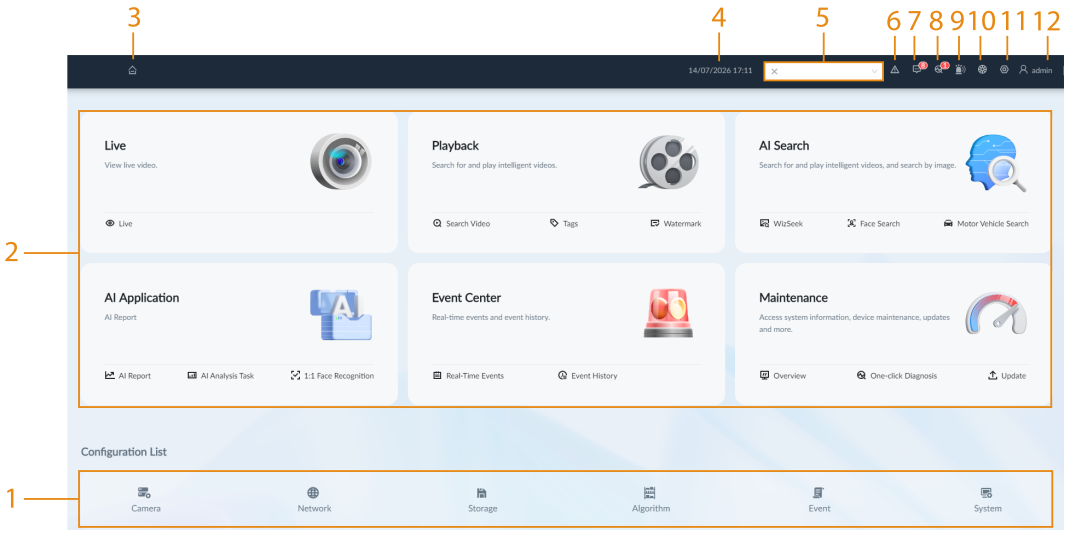


5.4 Home Page

Different device models support various features. Refer to the actual page for details.

Click on the upper-right corner of the page to scan and obtain more user information.

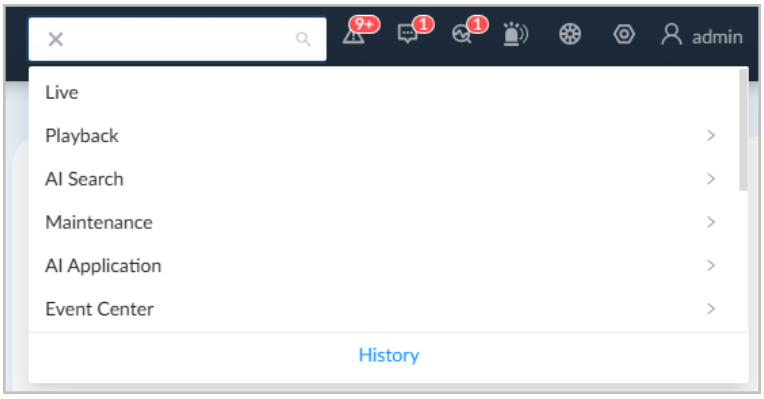
Figure 5-8 Home page

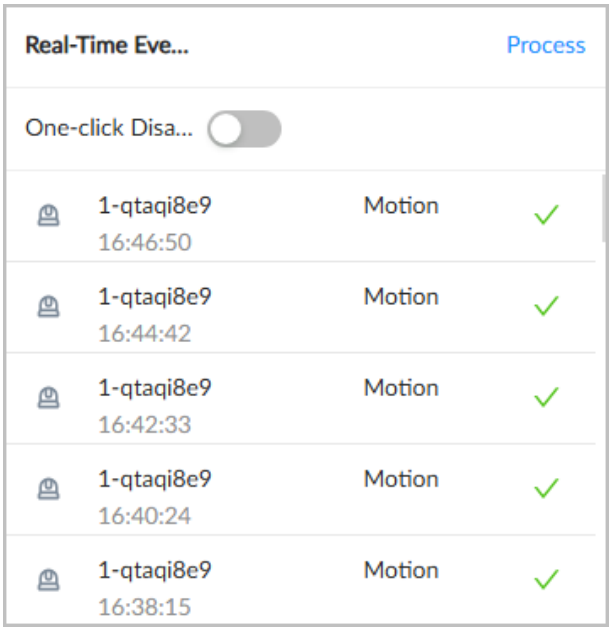


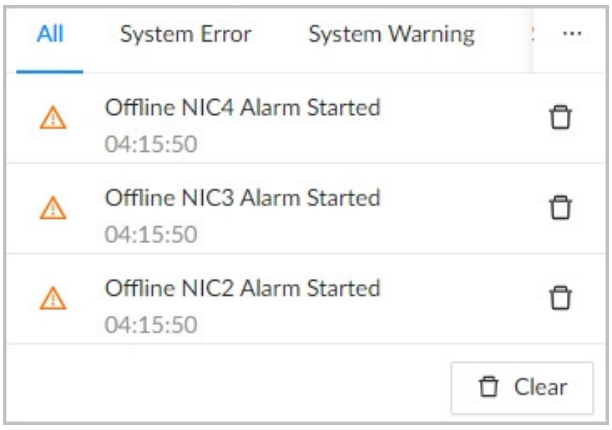
When you log in to the local page, you can click to control the screens.

Table 5-2 Home page description

No.	Name	Description
1	Configuration list	Click the corresponding feature to configure the relevant parameters.
2	Function tiles	Click each tile to access the corresponding function. The application sections include up to three shortcut links for their respective features, which can be clicked to quickly navigate to the corresponding feature configuration page.
3	Home page	Go back to the home page.
4	Time	Displays the current date and time.

No.	Name	Description
5	Search	Supports 3 types: ● Enter the keyword of the feature name to search for and quickly redirect to the corresponding feature configuration page. ● Navigate through the function menu for step-by-step searching, and quickly jump to the corresponding feature configuration page. ● Click **History** , the button will switch to **View menu**, and then historical search records will be displayed. Click any record to quickly jump to the corresponding function configuration page. Click **View menu** again to switch back to the menu search page. 

No.	Name	Description
6	Event information	View system event information, including the name of the alarm device, the alarm time and the alarm type. ● The number on the icon  is the number of unprocessed alarm events. When the number exceeds 9, only **9+** is displayed. ● Click **Process** to jump to **Event Center** > **Real-Time Events** > **Alarm Event**. Supports viewing the alarm events and performing batch processing. ● Click  to confirm the alarm event. The confirmed event will be removed from the alarm list. ● Enable one-click disarm to cancel linked alarm items. 

No.	Name	Description
7	System notifications	View system error messages, warnings, and notifications. ● Click **All** , **System Error**, **System Warning** or **System Notifications** to view the corresponding system message list. ● Click to delete the corresponding system message. ● Click **Clear** to clear the system messages under the current tab. For example, after selecting the **All** tab, click **Clear** to delete all system messages. After selecting the **System Error** tab, click **Clear** to delete all system error messages. 
8	One-click diagnosis	One-click diagnosis of device configuration and status to help users use the device better.
9	Buzzer	View buzzer messages.
10	Background task	View the tasks running in the background. Click **All** , **In progress**, or **Waiting** to view the background tasks of different statuses.
11	Setting	You can access the configuration of accounts, network, events, and more by clicking the icon or from the configuration list on the home page.
12	Login user	Change the password, lock the user, log out, restart or shut down the Device.

5.5 Configuring Remote Devices

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

5.5.1 Initializing Remote Devices

After you initialize the remote devices, you can change their login passwords and IP addresses. Remote devices can be connected to the Device only after being initialized.

Procedure

Step 1 Log in to the PC client.

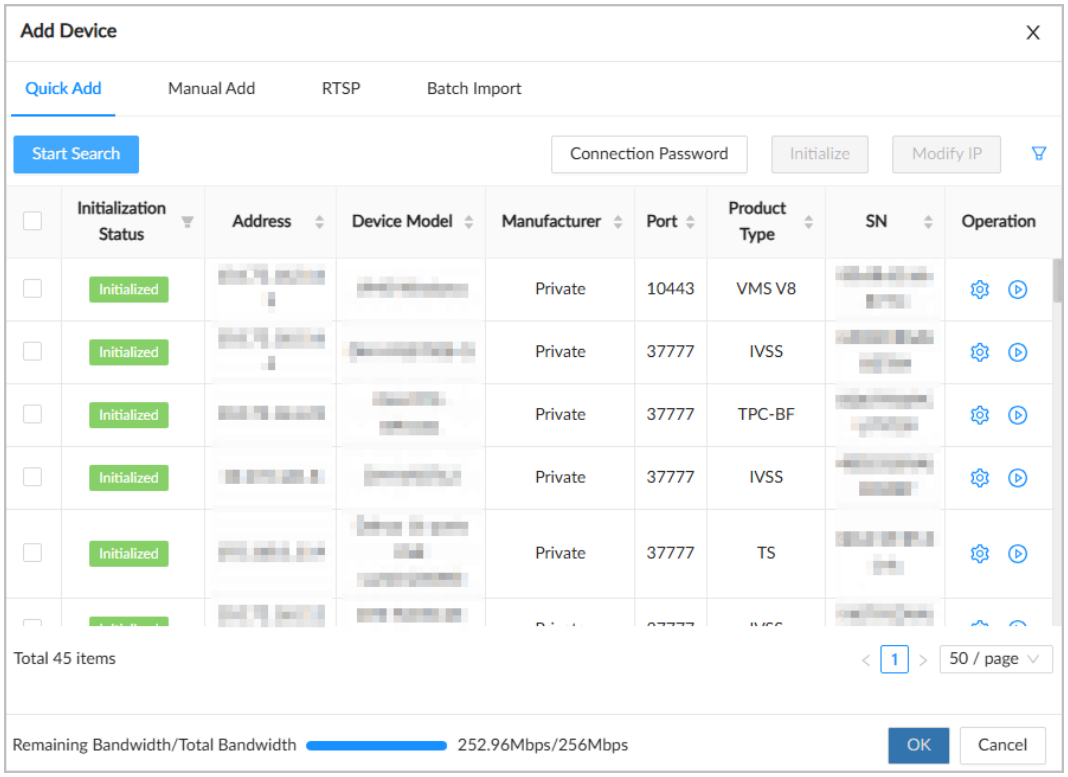
Step 2 Click on the upper-right corner of the page, and then click **Camera**.

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.

Figure 5-9 Add the device



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

The search results are displayed.

To filter the search results, you can click .

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 Choose whether to continue using the device password, and then click **Next**.

You can skip this step if you keep **Use Local Password and Password Protection** enabled by default. The remote device automatically uses the current admin password of the Device.

1. To manually configure the password, disable **Use Local Password and Password Protection**.
2. Enter and confirm the password, and then click **Next**.

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

Enter the static IP, subnet mask and default gateway.

- 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 **Next** > **OK**.

5.5.2 Adding Remote Devices

You can add remote devices to the Device in any of the following ways.

Table 5-3 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, user name 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, user names, 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, user names and password vary with each other.

5.5.2.1 Quick Adding

Procedure

Step 1 Under the **Quick Add** tab, click **Start Search**.

You can click to filter the search results.

Figure 5-10 Search results

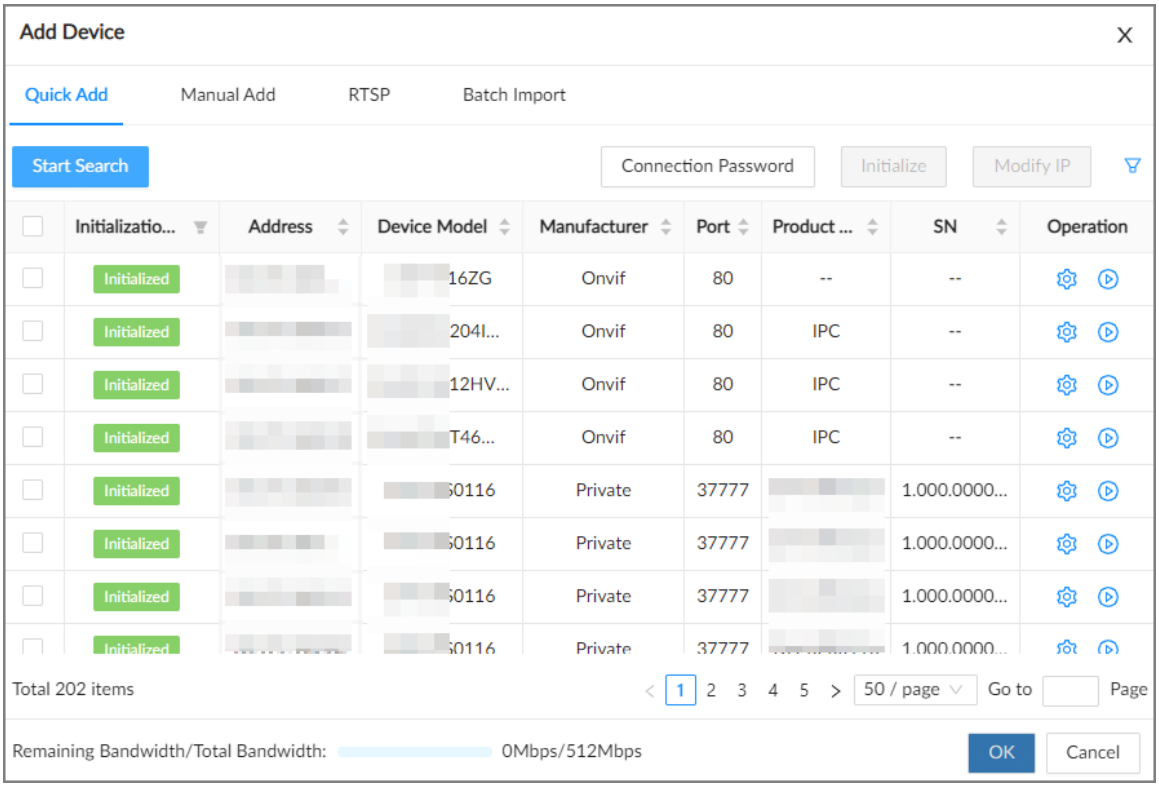


Table 5-4 Description of search results

Parameter	Description
Start Search	Click **Start Search** to search for remote devices again. Click **Stop Search** to stop search.
Connection Password	Click **Connection Password** to set the user name 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 user name 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.

Parameter	Description
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.
Bandwidth	Displays the remaining and total bandwidth. You cannot add more remote devices when the bandwidth runs out.

Step 2 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 3 Click **Add more** or **Complete**.

- Click **Add more** , and then 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.

5.5.2.2 Manual Adding

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 5-11 Remote device settings

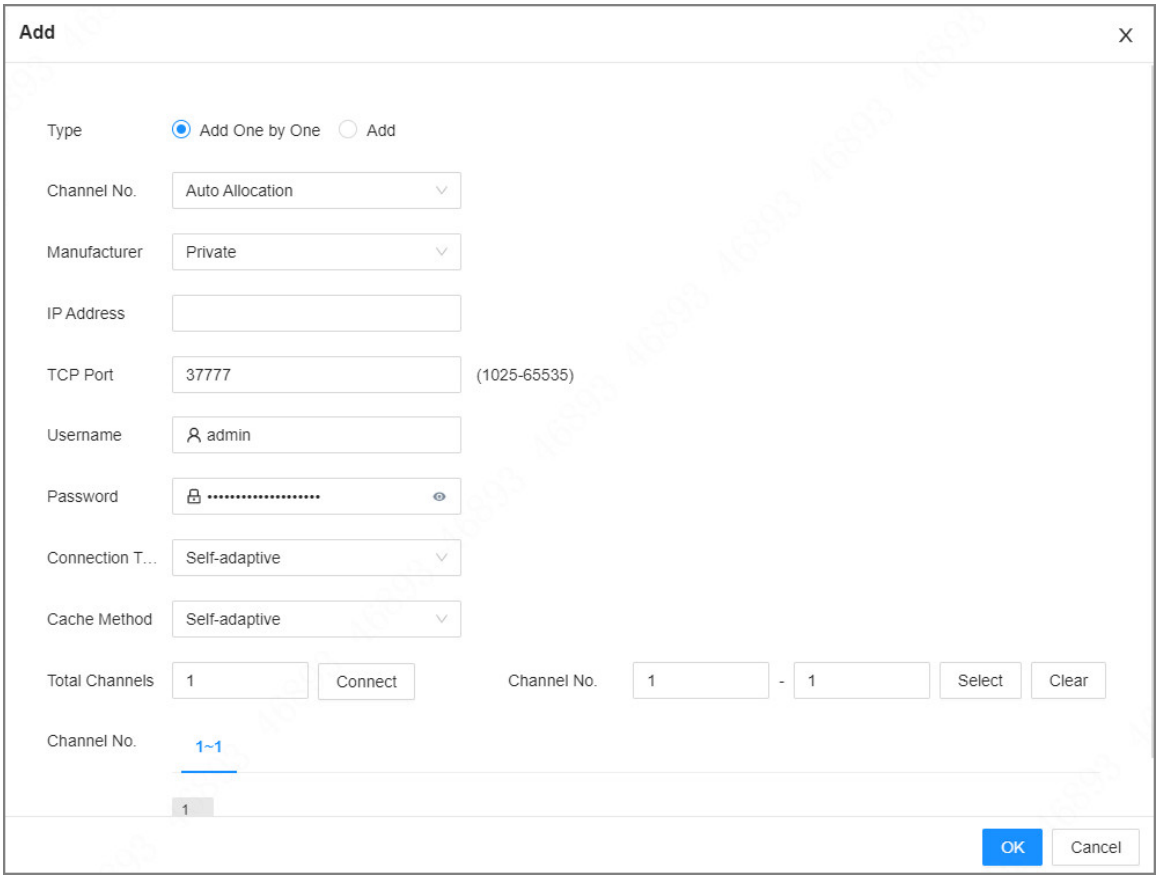


Table 5-5 Parameters of adding remote device

Parameters	Description
Type	You can add one by one or add in batches.
Channel No.	Select a channel number for the remote device on IVD. If you select **Auto Allocation**, IVD 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.
Device No.	Enter the unique device No. allocated by the server for the remote device. When **Manufacturer** is **Register**, you need to configure this parameter.
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.

Parameters	Description
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.
Username	Enter the user name and password of the remote device.
Password	
TCP Port	Enter the TCP port number of the remote device. When **Manufacturer** is **Private**, you need to configure this parameter.
Connection Type	Select a connection type from **Self-adaptive** , **TCP**, **UDP** and **Multicast**. The connection types available might differ depending on the manufacturer.
Cache Method	Select a cache method from **Self-adaptive** , **Realtime** and **Fluent**.
Remote CH No.	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. You can click 1 2 to select or cancel the selection of specific channels. 3. Click **OK**.
Channel No.	

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

Step 7 Click **Add more** or **Complete**.

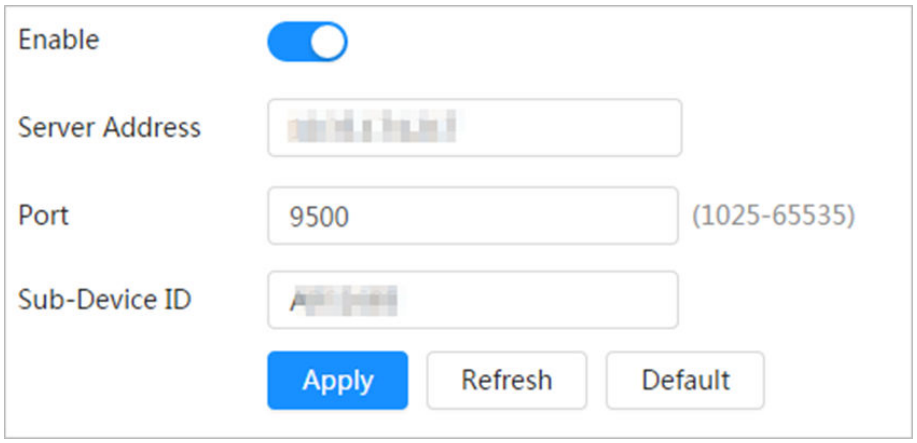
- Click **Add more** , the Device goes back to the **Quick Add** window and you can add more remote devices.
- Click **Complete** if you do not want to add more remote devices at the moment. The Device goes back to the **Camera** tab where you can view the added remote devices.

5.5.2.3 Auto Registration

Prerequisites

Make sure that front-end device has configured with the auto registration function.

Figure 5-12 Auto Registration (1)



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**.

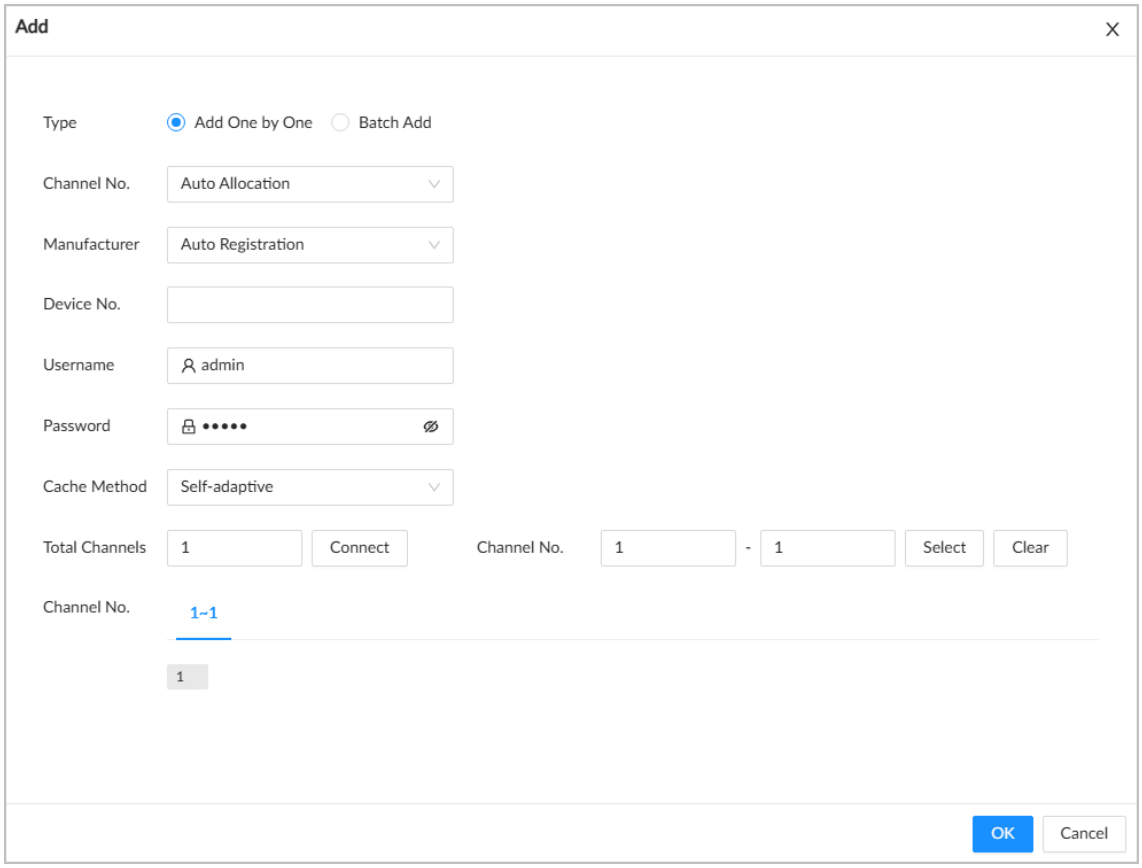
You can also click **Add** under the device tree.

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

Step 5 Select **Add One by One** checkbox, select **Auto Registration** in the **Manufacturer** list, and then set the other parameters.

Device No. must be consistent with the sub-device ID configured on the front-end device. For information about other parameters, see Table 5-5 .

Figure 5-13 Setting



Step 6 Click **OK**.

5.5.2.4 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**.

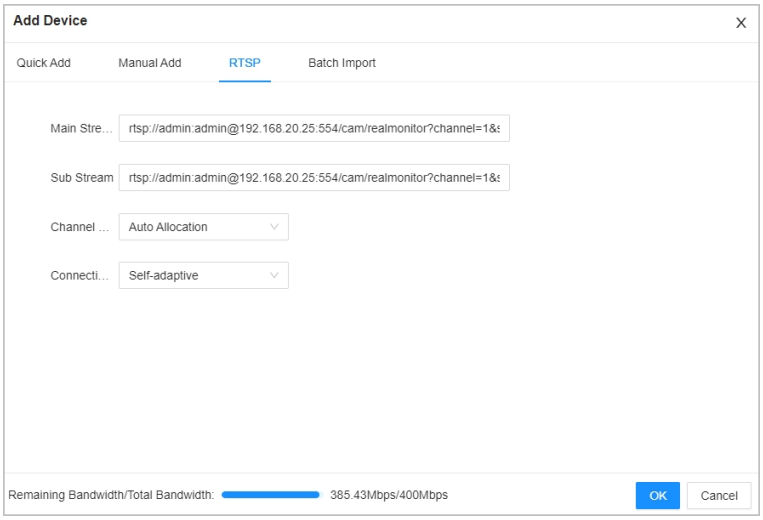
You can also click **Add** under the device tree.

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: User name 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 5-14 RTSP



Step 5 Select a channel No. and connection type.

Step 6 Click **OK**.

5.5.2.5 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.

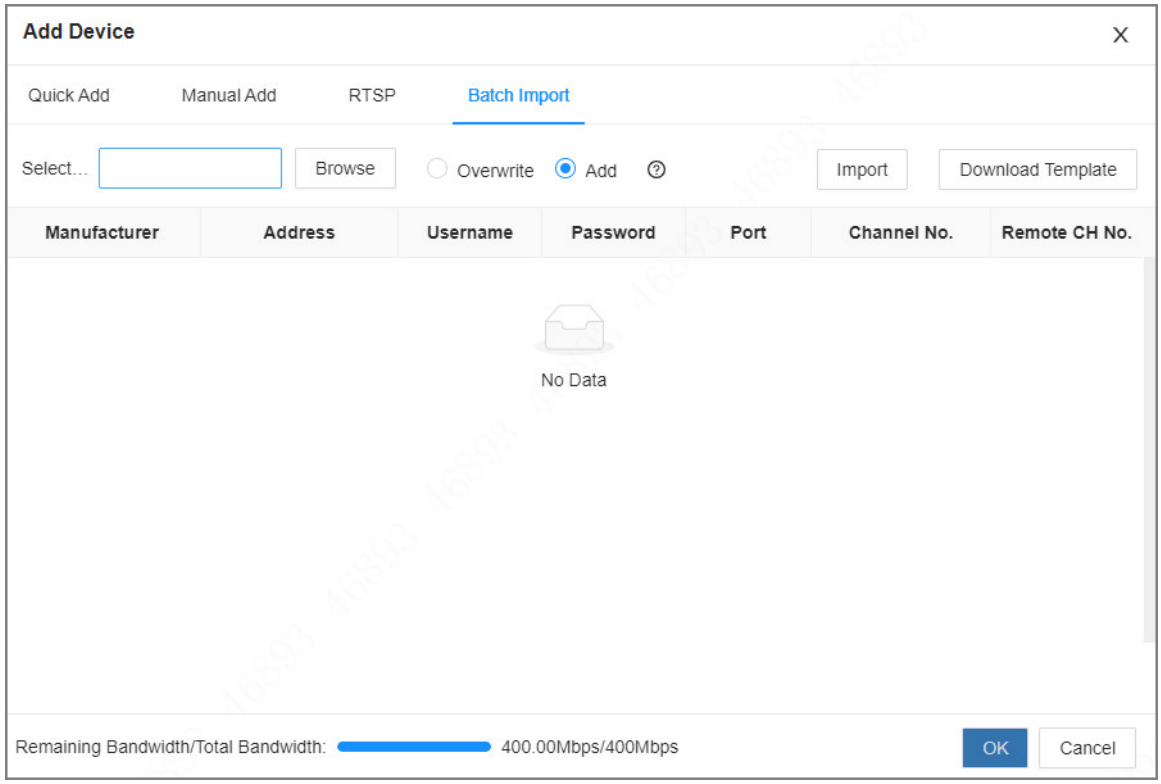
Step 3 Under the **Camera** tab, click **Add**.

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 local interface, you can select the file storage path.
- On the web interface, files are saved to the default downloading path of the browser.

Figure 5-15 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 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 8 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.

6 AI Operations

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

The AI detections can be performed by the camera (AI by Camera) or by IVD (AI by Recorder).

- AI by Camera: If you use AI by Camera for intelligent detection, the intelligent analysis job is completed on the camera, and the Device just receives and displays the results.
- AI by Recorder: If you use AI by Recorder for intelligent detection, the camera uploads videos and snapshots, and then the Device is responsible for the video analysis job.

- The AI functions might vary depending on the model you are using.
- When AI by Camera is enabled, you can configure AI detection on the remote device. For details, see the user's manual of the remote device.
- The **AI by Camera** tab does not appear if the current camera does not support this function.

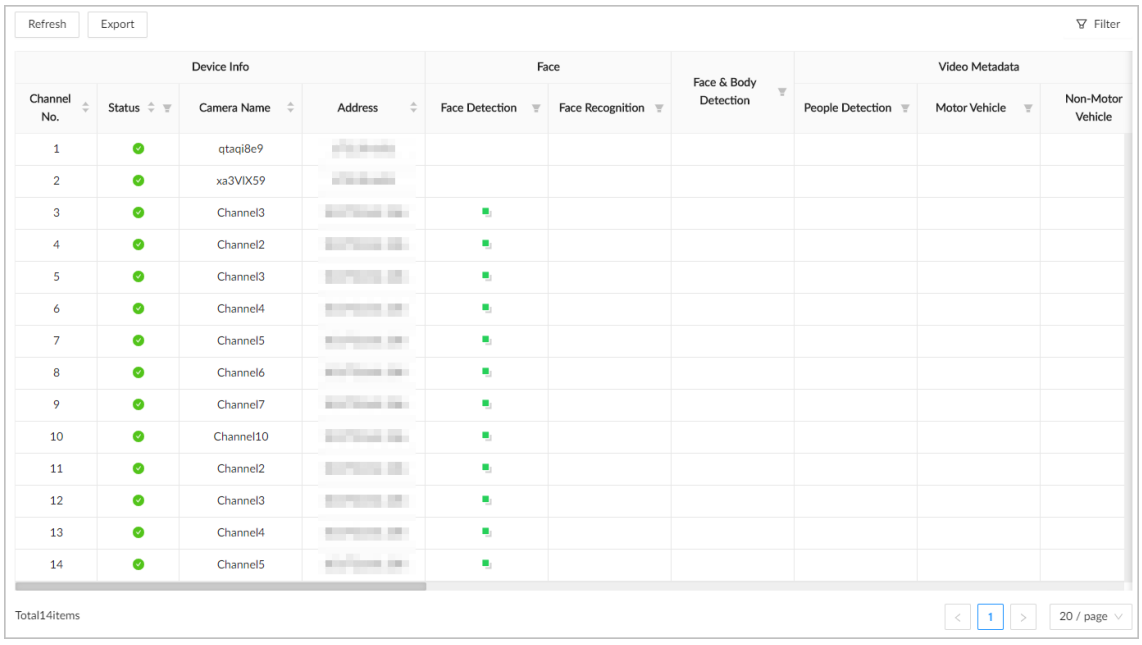
6.1 Overview

Viewing Event Enabling Status

Log in to the PC client, select **Event** from the configuration list on the home page, select the root node on the device tree, and then click **Overview**. You can view the events enabled on the Device.

Click **Export** to export the list of event enabling status in .csv format.

Figure 6-1 Overview



- indicates that AI by Camera is enabled.
- indicates that AI by Recorder is enabled.

- indicates that AI by Camera and AI by Recorder are both enabled.
- indicates that smart motion detection is enabled.

AI Events by Recorder or Camera

Table 6-1 AI events by Recorder or Camera

AI Event	AI by Camera	AI by Recorder
Face Detection	Yes	Yes
Face Comparison	Yes	Yes
People Counting	Yes	Yes
Video Metadata	Yes	Yes
IVS	Yes	Yes
Crowd Distribution	Yes	No
Call Alarm	Yes	Yes
Smoking Alarm	Yes	Yes
ANPR	Yes	No
Plate Comparison	No	Yes

To use people counting, call alarm and smoking alarm, you must configure the corresponding algorithms.

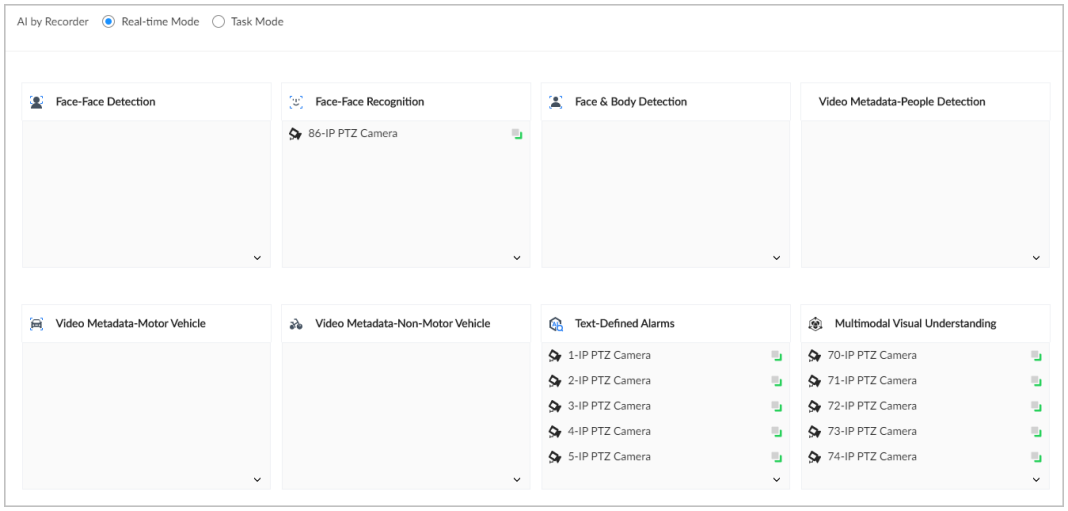
Click to go to the webpage of the corresponding device quickly.

6.2 Scheduled Tour

The smart plans of the AI by Recorder support both real-time mode and task mode. The following describes how to configure task mode.

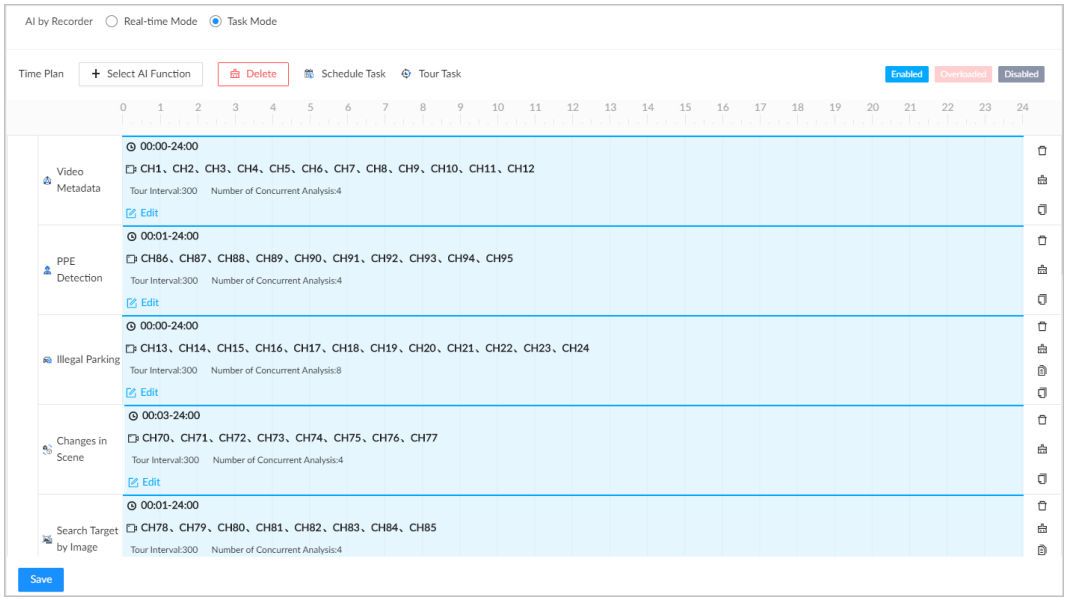
- **Real-time Mode** : Enable or disable smart plans for each channel to conduct real-time analysis.

Figure 6-2 Real-time mode



- **Task Mode** : Set schedule tasks and tour tasks for specified channels based on the type of smart plans.

Figure 6-3 Task mode



- ◇ **Schedule Task** : Set a specific type of smart plans for designated channels to be executed within a certain time period to achieve single-channel multiple intelligence and tidal intelligence.
- ◇ **Tour Task** : Set up tour inspections for designated channels within a specific time period to achieve effective resource detection across multiple scenarios.

Schedule Task and **Tour Task** cannot be configured simultaneously for the same channel during the same time period.

6.2.1 Configuring Tasks by Time Intervals

Procedure

Step 1 Log in to the PC client.

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

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

Step 3 Select a remote device in the device tree on the left, and then select **Smart Plan** > **Smart Plan**.

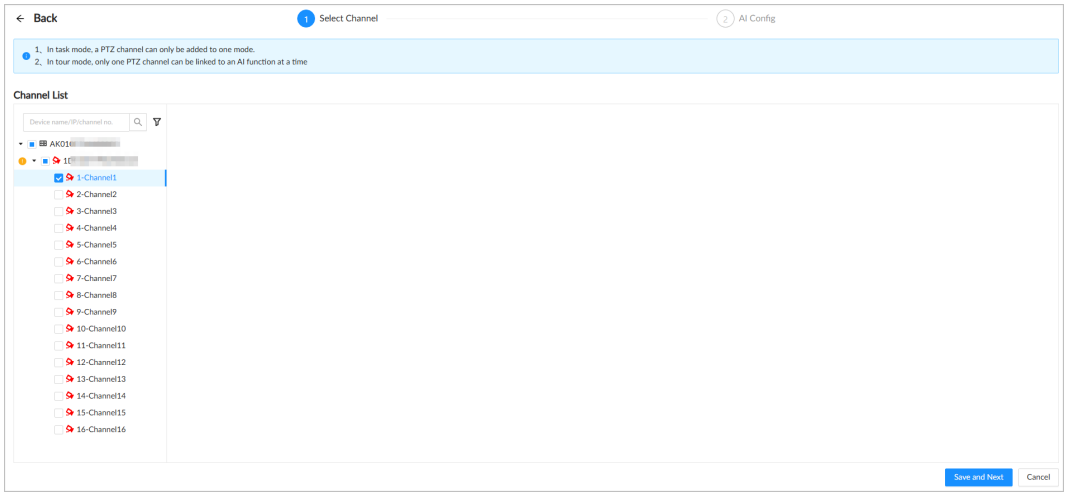
Step 4 Select **Task Mode** , and then click **OK** in the pop-up page.

Step 5 Click **Select AI Function** , select the **Schedule Task** in the pop-up page, click , select the specific smart plan, and then click **OK**.

Step 6 On the displayed smart plans, drag to select the time period, and then click **Configure Now**. Select the channel for executing the scheduled tasks and configure the smart plan.

1. Select the channel, and then click **Save and Next**.

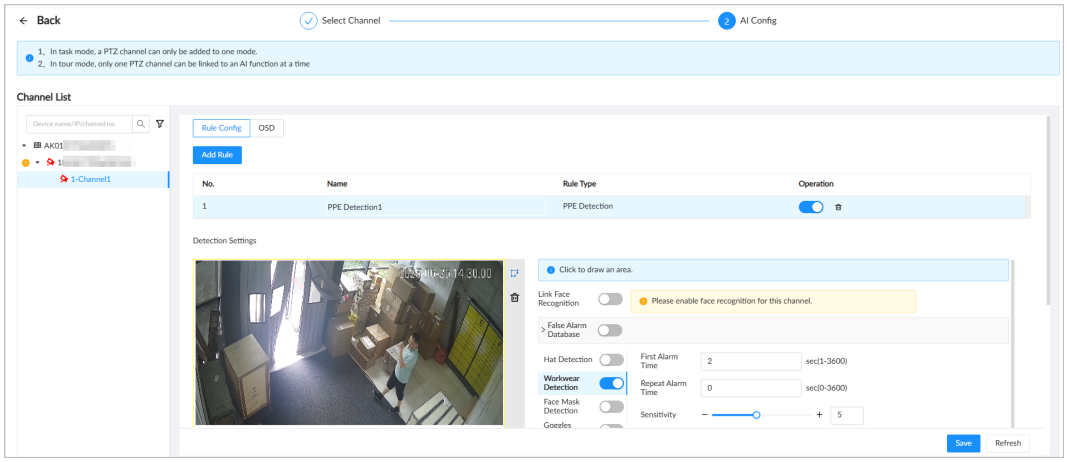
Figure 6-4 Configure the task



2. Select a channel in the device tree on the left, configure the smart plan, and then click **Save**.

After configuring the smart plan for each channel, click **Save**. If not saved, the configuration will be lost.

Figure 6-5 Rule configuration



Repeat this step to complete the configuration of the smart plans for all channels. For more information about the smart plans, refer to the subsequent chapters.

3. Click **Close**.

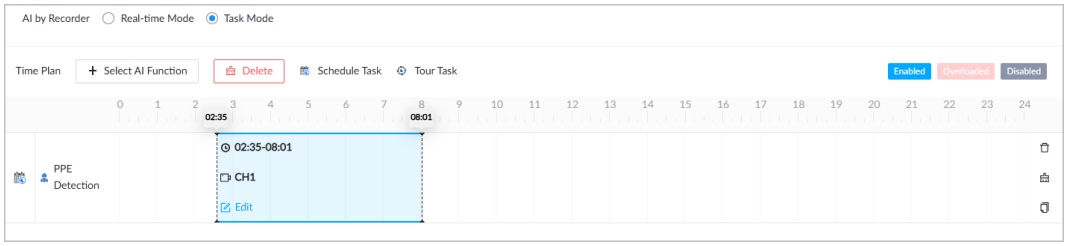
Repeat the above operation to set up time-specific tasks for all smart plans during different time periods.

Step 7 Click **Save**.

The status of the smart plan can be determined by the background color of the task.

- The smart plan displays in blue indicating that it is enabled.
- The smart plan displays in red indicating that it is overloaded.
- The smart plan displays in gray indicating that it is disabled.

Figure 6-6 Tasks



6.2.2 Configuring Tasks by Tours

Procedure

Step 1 Log in to the PC client.

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

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

Step 3 Select a remote device in the device tree on the left, and then select **Smart Plan** > **Smart Plan**.

Step 4 Select **Task Mode** , and then click **OK** in the pop-up page.

Step 5 Click **Select AI Function** , select the **Tour Task** in the pop-up page, click , select the specific smart plan, and then click **OK**.

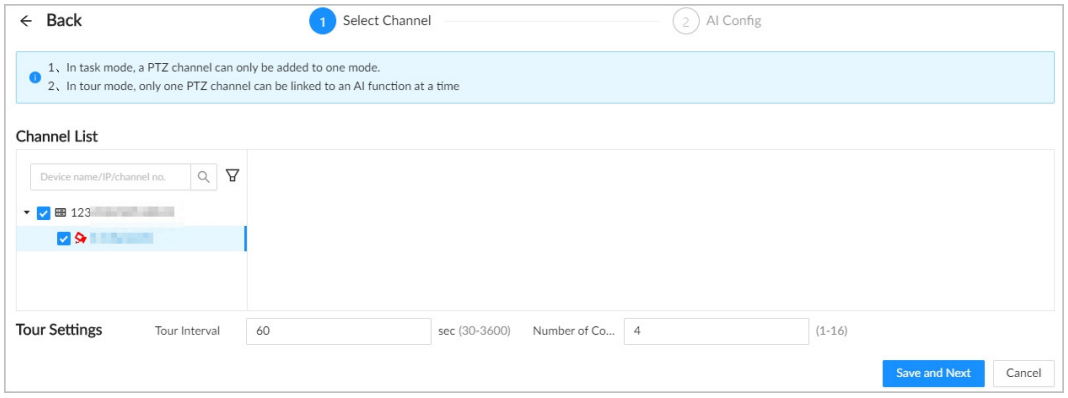
Step 6 On the displayed smart plans, drag to select the time period, and then click **Configure Now**. Select the channel for executing the tour tasks and configure the smart plan.

1. Select the channel, set the tour interval and the number of concurrent analysis, and then click **Save and Next**.

   When selecting a PTZ channel, it supports selecting a preset point for configuration. At the same time, a single PTZ channel can only be added to one intelligent system.

   - **Tour Interval** : Indicates how long to wait before transitioning to the next scene analysis, applicable to all selected devices.
   - **Number of Concurrent Analysis** : The number of channels that can be analyzed simultaneously, with a maximum value that corresponds to the maximum channels supported by the device for this intelligence.

   Figure 6-7 Configure the task



2. Select a channel in the device tree on the left, configure the smart plan, and then click **Save**.

   After configuring the smart plan for each channel, click **Save**. If not saved, the configuration will be lost.

   Repeat this step to complete the configuration of the smart plans for all channels. For a detailed introduction to the smart plans, refer to the subsequent chapters.

3. Click **Close**.

   The system will automatically exit to the smart plan page.

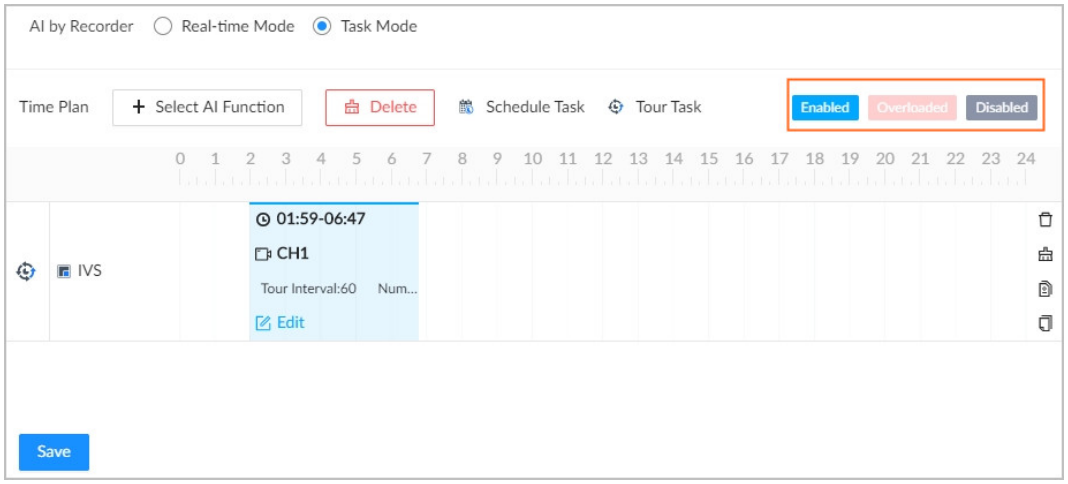
Repeat the above operations to set up tour tasks for all smart plans at different time intervals.

Step 7 Click **Save**.

The status of the smart plan can be determined by the background color of the task.

- The smart plan displays in blue indicating that it is enabled.
- The smart plan displays in red indicating that it is overloaded.
- The smart plan displays in grey indicating that it is disabled.

Figure 6-8 Tasks



- : Delete the task.
- : Clear the parameters of corresponding task.
- : Batch configure the multiple channel's parameters.
- : Copy the time plan to other tasks.

6.3 AcuPick

Enable AcuPick and you can click the box to select the human faces, human bodies, motor vehicles and animals in the **Live** , **Playback** or **AI Search** page. Also supports the selection of a target for full-channel detection capture record.

6.3.1 Enabling AcuPick

Prerequisites

The intelligent analysis function has been assigned to the intelligent analysis card through **Algorithm** > **Algorithm Management** > **AI Module**.

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 a remote device in the device tree on the left.

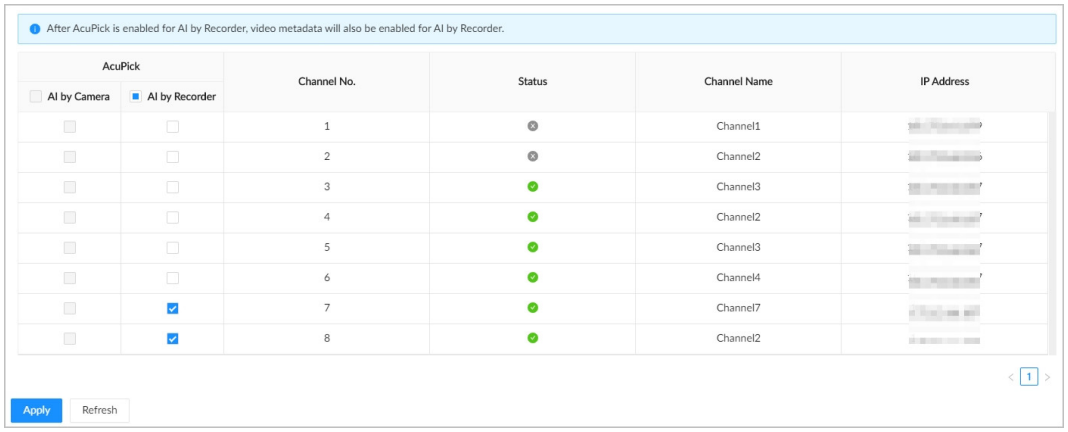
Step 4 Select **Smart Plan** > **AcuPick**.

Step 5 Select the AI by recorder check box corresponding to the channel.

After AcuPick is enabled for AI by Recorder, video metadata will also be enabled for AI by Recorder.

If the channel supports AI by Camera, AI by Recorder can be turned off or turned on through the Device.

Figure 6-9 Enable AI by Recorder



Step 6 Click **Apply**.

6.3.2 Applying AcuPick

6.3.2.1 AcuPick through the Live Video Page

Procedure

Step 1 Log in to the PC client.

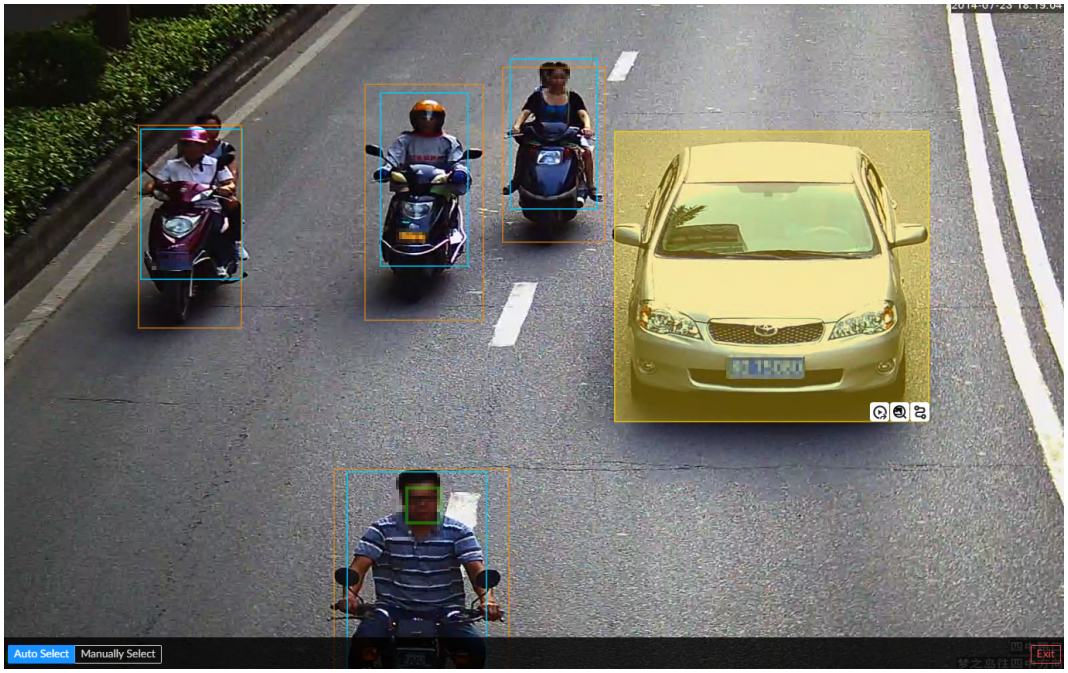
Step 2 Click **Live** and turn on the channel.

Step 3 Click on the upper-right corner of the video window or the lower-right corner of the menu bar, and then freeze the current screen.

Step 4 Select the targets to be retrieved through automatic or manual frame selection.

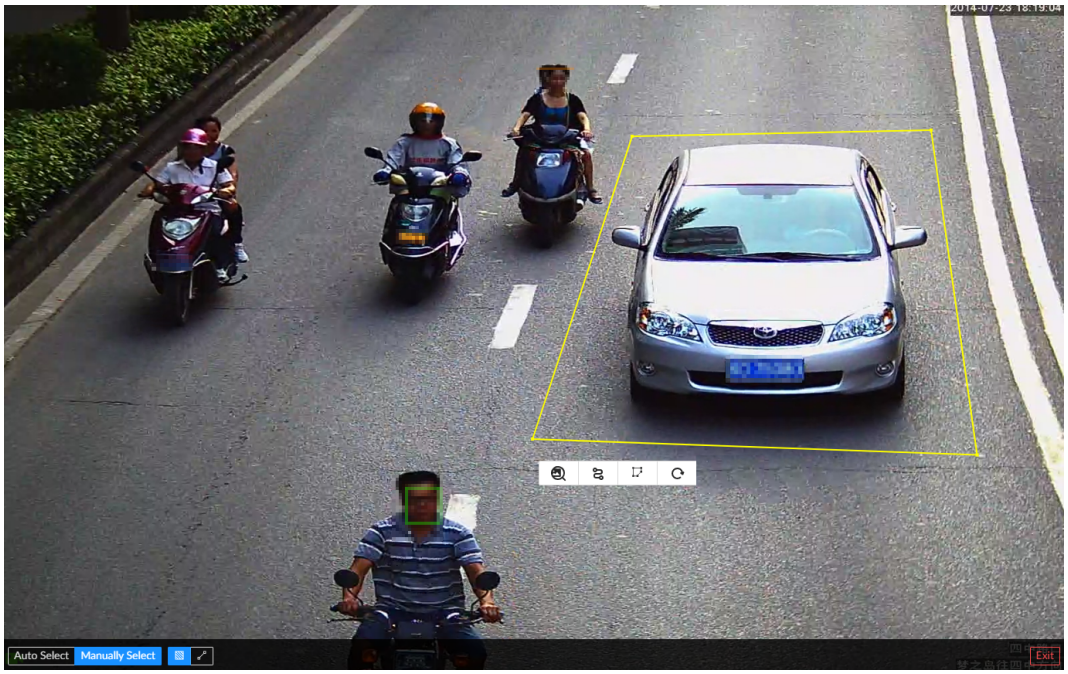
- Auto select: When the frame is frozen, the system automatically selects targets such as human faces, human bodies, motor vehicles and animals with target area. Click on any target area at this moment, and then will be displayed.

Figure 6-10 Auto select



- Manually select: Click **Manually select** at the lower left of the page, and then the target area and will be displayed. Drag the four corners of the target area to manually adjust the size of the area.

Figure 6-11 Manually select



Step 5 Click each AcuPick icon as needed to perform target retrieval.

- Playback: Click , the system will go to the playback page and search for the object in all channels.
- Search by image: Click , the system will go to the **Search by Image** page of the corresponding target in the **AI Search**. For example, when you select a motor vehicle,

the system will go to the **Motor Vehicle Search**. Automatically select all cameras and search this picture.

- Track: Click , the system will go to the **Search by Image** page of the corresponding target in the **AI Search**. For example, when you select a face, the system will go to the **Face Search**. Automatically select all cameras and track this face. For details, see "6.5.4.3 Viewing tracks".
- Search by area: When manually selecting targets by framing, you can perform retrieval by the search area or tripwire. The operations are as follows.

  1. Click or next to **Manually select**.
     - Click : Search for targets that pass through the specified area.
     - Click : Search for targets that cross the tripwire.
  2. Adjust the search area or tripwire, and then click .
  3. Select the target type in the pop-up page, and then click **OK**.

     Go to the playback page, where the corresponding channel will be automatically selected, and the recordings under that channel will be retrieved.

- Search by image is not supported for animals.
- Click to reset the search area or tripwire.

6.3.2.2 AcuPick through the Playback Page

Procedure

Step 1 Log in to the PC client.

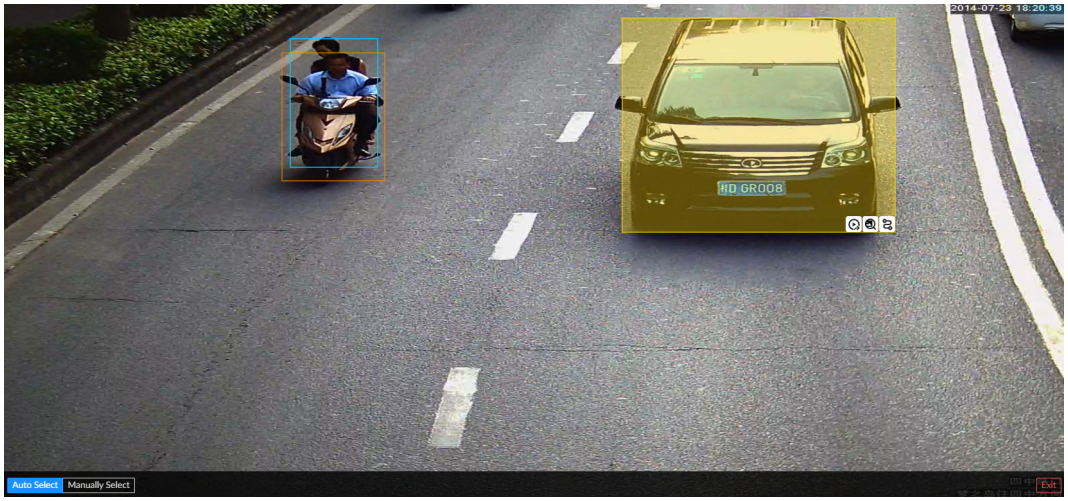
Step 2 Click **Playback** , select the playback channel on the **Search Video** tab, set the search conditions, and then click **Search**.

Step 3 Select a channel screen, and then click on the playback record video screen to freeze the current screen.

Step 4 Select the targets to be retrieved through automatic or manual frame selection.

- Auto select: When the frame is frozen, the system automatically selects targets such as human faces, human bodies, motor vehicles and animals with target area. Click on any target area at this moment, and then will be displayed.

Figure 6-12 Auto select



- Manually select: Click **Manually select** at the lower left of the page, and then the target area and will be displayed. Drag the four corners of the target area to manually adjust the size of the area.

Figure 6-13 Manually select



Step 5 Click each AcuPick icon as needed to perform target retrieval.

- Playback: Click , the system will search for the object in all channels.
- Search by image: Click , the system will go to the **Search by Image** page of the corresponding target in the **AI Search**. For example, when you select a motor vehicle, the system will go to the **Motor Vehicle Search**. Automatically select all cameras and search this picture.
- Track: Click , the system will go to the **Search by Image** page of the corresponding target in the **AI Search**. For example, when you select a face, the system will go to the **Face Search**. Automatically select all cameras and track this face. For details, see "6.5.4.3 Viewing tracks".
- Search by area: When manually selecting targets by framing, you can perform retrieval by the search area or tripwire. The operations are as follows.

  1. Click or next to **Manually select**.

- Click : Search for targets that pass through the specified area.
- Click : Search for targets that cross the tripwire.

2. Adjust the search area or tripwire, and then click .
3. Select the target type in the pop-up page, and then click **OK**.

   The corresponding channel will be automatically selected, and then the recordings under that channel will be retrieved.

- Search by image is not supported for animals.
- Click  to reset the search area or tripwire.

6.3.2.3 AcuPick through the AI Search page

Attribute search or image search for AI search supports AcuPick. The following uses the detailed page of **Search by Attribute** in **Human Search** as an example.

Procedure

Step 1 Log in to the PC client.

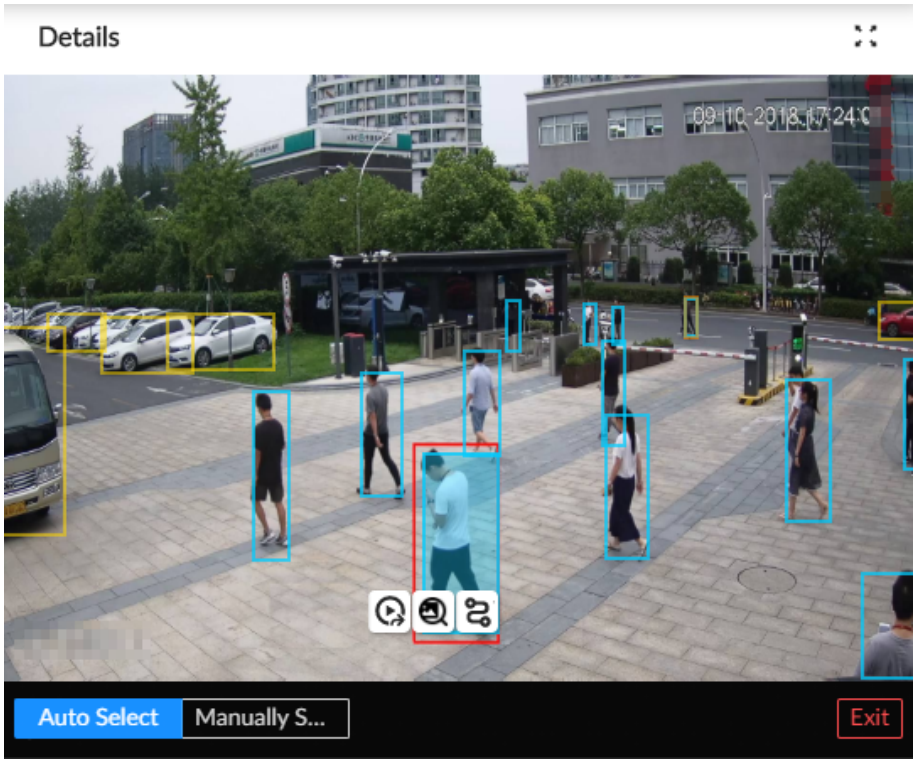
Step 2 Select **AI Search** > **Human Search** > **Search by Attribute**, select the corresponding channel, set the search conditions, and then click **Search**.

Step 3 Select a channel screen, and then click  in the details screen on the right.

Step 4 Select the targets to be retrieved through automatic or manual frame selection.

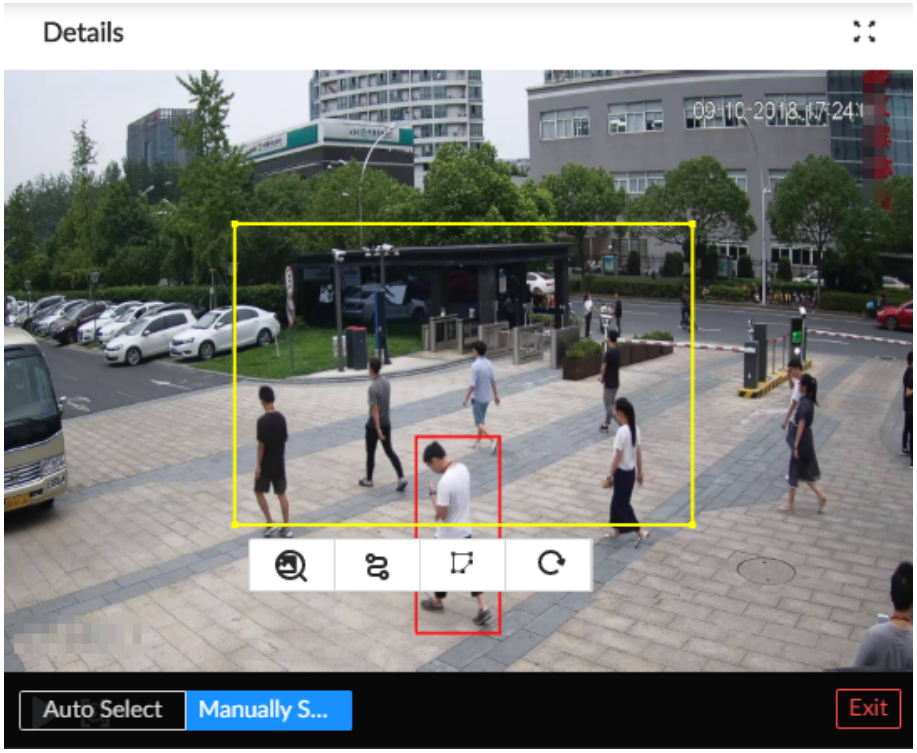
- Auto select: When the frame is frozen, the system automatically selects targets such as human faces, human bodies, motor vehicles and animals with target area. Click on any target area at this moment, and then  will be displayed.

Figure 6-14 Auto select



- Manually select: Click **Manually select** at the lower left of the page, and then the target area and will be displayed. Drag the four corners of the target area to manually adjust the size of the area.

Figure 6-15 Manually select



Step 5 Click each AcuPick icon as needed to perform target retrieval.

- Playback: Click , the system will go to the playback page and search for the object in all channels.
- Search by image: Click , the system will go to the **Search by Image** page of the corresponding target in the **AI Search**. For example, when you select a motor vehicle, the system will go to the **Motor Vehicle Search**. Automatically select all cameras and search this picture.
- Track: Click , the system will go to the **Search by Image** page of the corresponding target in the **AI Search**. For example, when you select a face, the system will go to the **Face Search**. Automatically select all cameras and track this face. For details, see "6.5.4.3 Viewing tracks".
- Search by area: When manually selecting targets by framing, you can perform retrieval by the search area or tripwire. The operations are as follows.

  1. Click or next to **Manually select**.
     - Click : Search for targets that pass through the specified area.
     - Click : Search for targets that cross the tripwire.
  2. Adjust the search area or tripwire, and then click .
  3. Select the target type in the pop-up page, and then click **OK**.

     Go to the playback page, where the corresponding channel will be automatically selected, and the recordings under that channel will be retrieved.

- Search by image is not supported for animals.
- Click to reset the search area or tripwire.

6.3.2.4 AcuPick through the Advanced Search Page

Procedure

Step 1 Log in to the PC client.

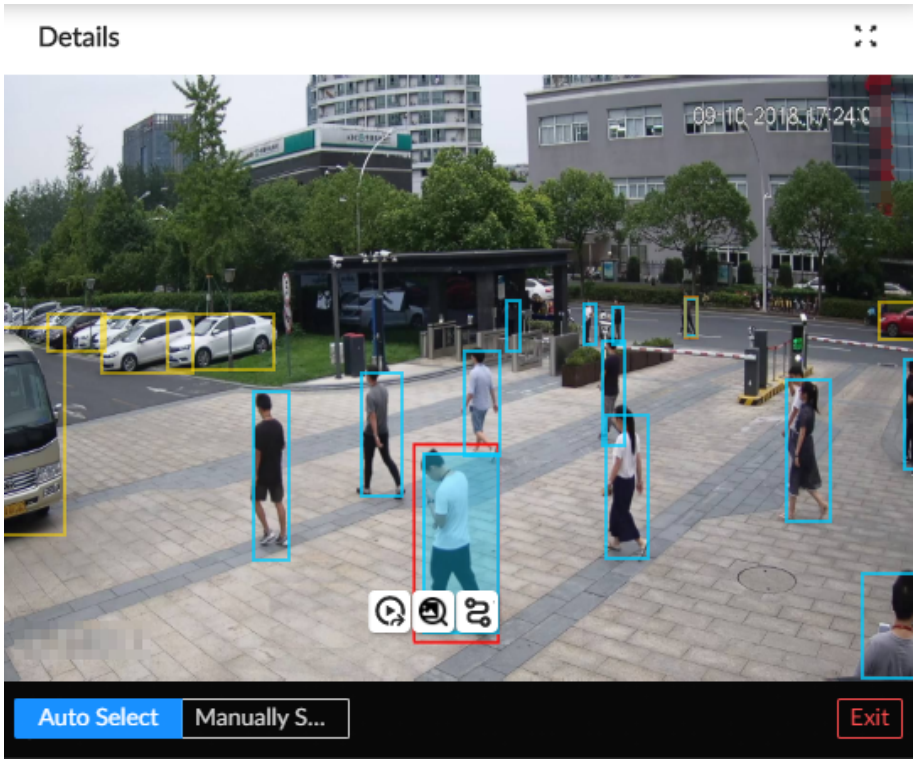
Step 2 Select **AI Search** > **Wizseek**, set the search conditions, and then click **Search**.

Step 3 Select a channel screen, and then click in the details page on the right.

Step 4 Select the targets to be retrieved through automatic or manual frame selection.

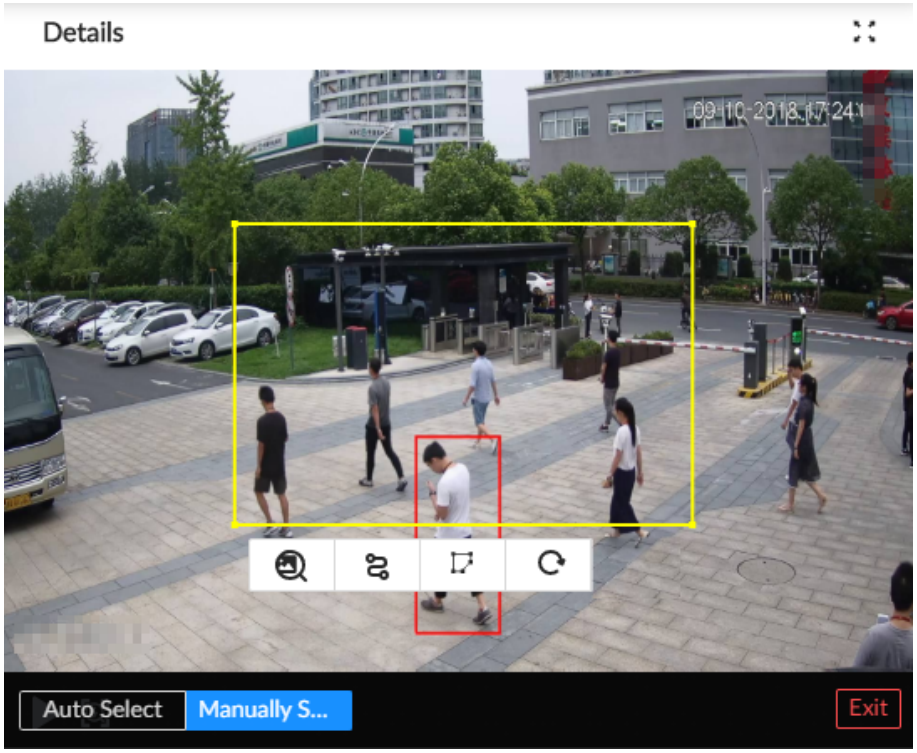
- Auto select: When the frame is frozen, the system automatically selects targets such as human faces, human bodies, motor vehicles and animals with target area. Click on any target area at this moment, and then will be displayed.

Figure 6-16 Auto select



- Manually select: Click **Manually select** at the lower left of the page, and then the target area and will be displayed. Drag the four corners of the target area to manually adjust the size of the area.

Figure 6-17 Manually select



Step 5 Click each AcuPick icon as needed to perform target retrieval.

- Playback: Click , the system will go to the playback page and search for the object in all channels.
- Search by image: Click , the system will go to the **Search by Image** page of the corresponding target in the **AI Search**. For example, when you select a motor vehicle, the system will go to the **Motor Vehicle Search**. Automatically select all cameras and search this picture.
- Track: Click , the system will go to the **Search by Image** page of the corresponding target in the **AI Search**. For example, when you select a face, the system will go to the **Face Search**. Automatically select all cameras and track this face. For details, see "6.5.4.3 Viewing tracks".
- Search by area: When manually selecting targets by framing, you can perform retrieval by the search area or tripwire. The operations are as follows.

  1. Click or next to **Manually select**.
     - Click : Search for targets that pass through the specified area.
     - Click : Search for targets that cross the tripwire.
  2. Adjust the search area or tripwire, and then click .
  3. Select the target type in the pop-up page, and then click **OK**.

     Go to the playback page, where the corresponding channel will be automatically selected, and the recordings under that channel will be retrieved.

- Search by image is not supported for animals.
- Click to reset the search area or tripwire.

6.4 Advanced Search

6.4.1 Enabling Advanced Search

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 left device tree, and then select **Smart Plan** > **Advanced Search**.

Step 4 Select the **Wizseek** checkbox of each channel.

Step 5 Enable image sources for search across each channels.

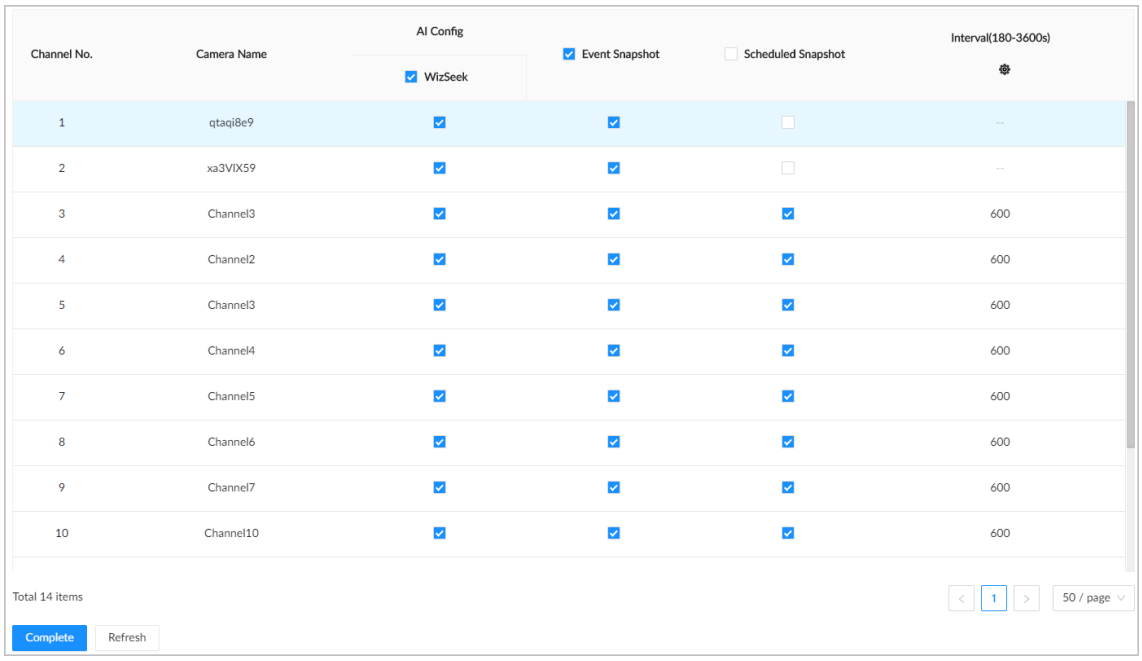
The image source includes event snapshots or scheduled snapshots.

- Event snapshot: Capture images at set time intervals as image sources for advance retrieval.

- Scheduled snapshot: Uses snapshots generated when an event alarm is triggered as image sources for advance retrieval.

If no image source is selected, **Wizseek** will not be able to search images from that channel.

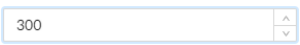
Figure 6-18 Set the image source



When the data source is set to **Scheduled Snapshot**, it is necessary to set the capture interval, which supports the following two methods of configuration.

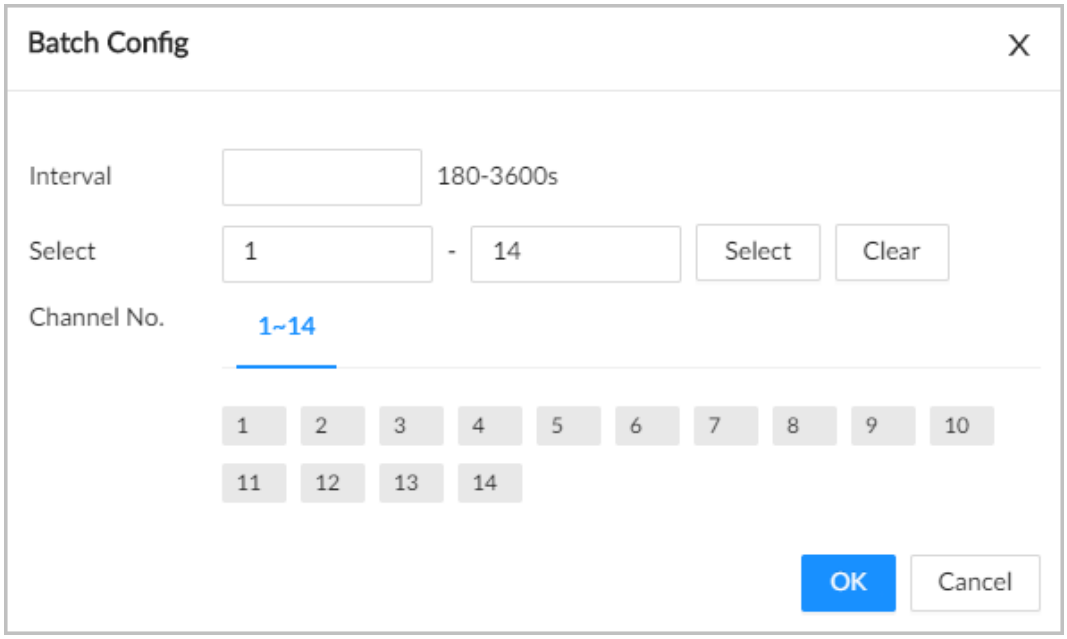
- Single configuration for capture interval: In the **Interval** column of the channel, click the value (for example, 300 as shown in the figure below), which supports inputting or clicking or to adjust the value.

Figure 6-19 Single configuration



- Batch configuration for capture interval: Click below the **Interval**, set the duration of the capture interval in the pop-up page, select the channels, and then click **OK**.

Figure 6-20 Batch configuration



Step 6 Click **Complete**.

6.4.2 Applying Advanced Search

Procedure

Step 1 Log in to the PC client.

Step 2 Select **AI Search** > **Advanced Search** on the home page, set the search conditions (including time, channel, and event type), and then click **Search**.

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

Step 3 Enter the search content, and then click **Search**.

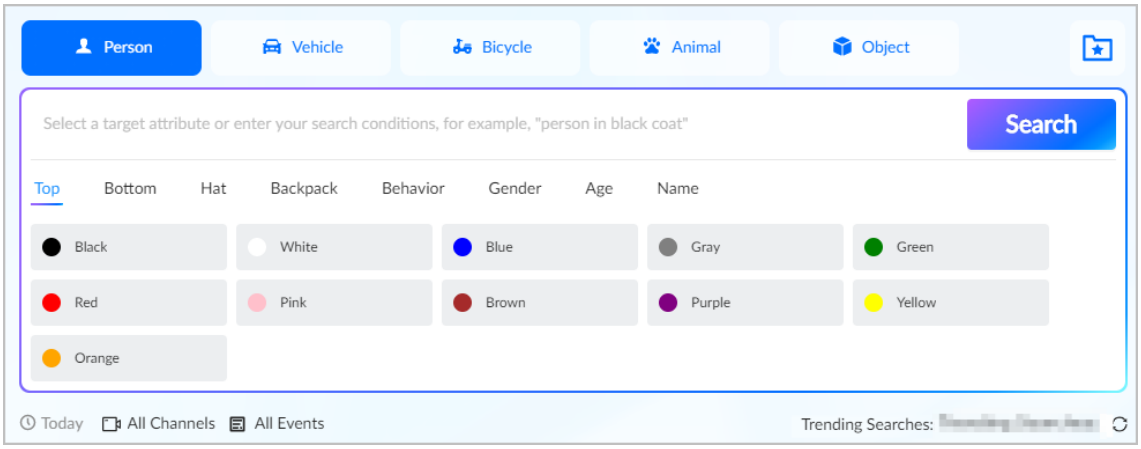
Supports the following 4 ways to input search content.

- Directly enter the content in the search box.
- Select the search objects through the various preset target attributes above the search box.

  For example, select the **Person** tab, set the attributes **Bottom** to **White**, and then the search box will automatically fill in the information (**A person is wearing white trousers**).
- Select the desired search terms from the **Trending Searches**.

  Click to refresh the search terms.

Figure 6-21 Advanced search



Step 4 View the search results.

Hover over the search results to display more options.

Figure 6-22 Search results

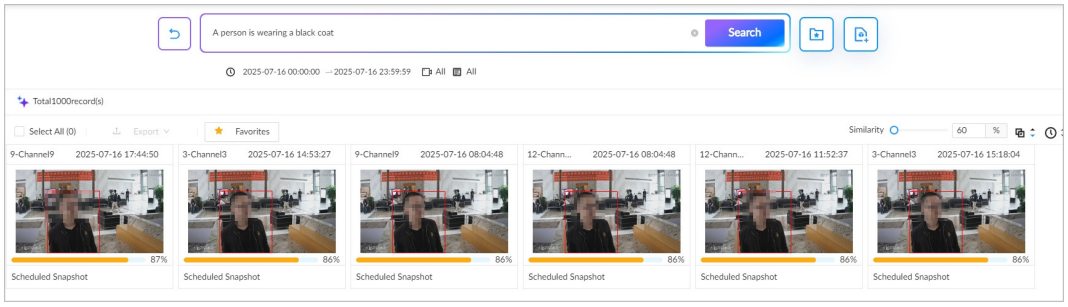
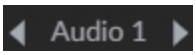
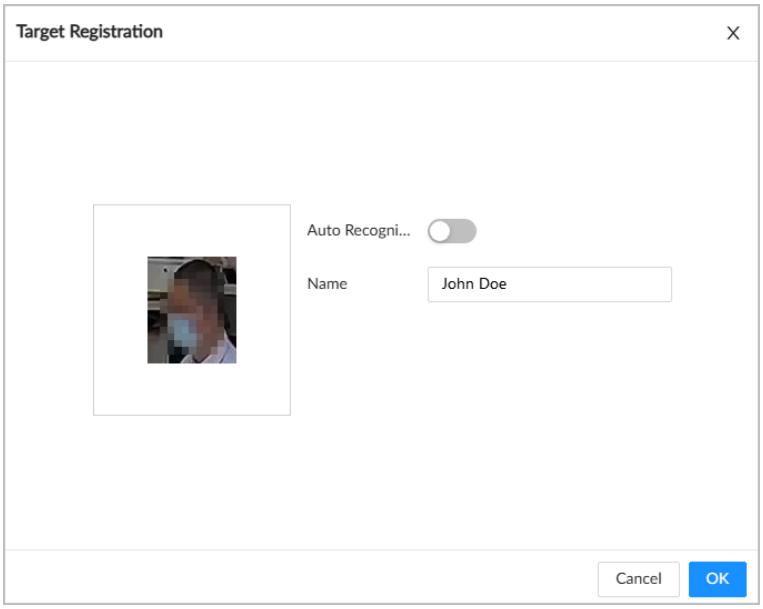


Table 6-2 Operations related to search results

Function	Description
Favorite query results	Click ☆ on the query results panel, or select multiple query results panels, and click **Favorites** to add the query results to your favorites. Click on the right of the search box will take you to the **Favorites** page. The operations supported in the **Favorites** page are similar to the other operations below. You can follow the same steps to configure settings.
Go to the **Text-Defined Alarms** page	Click on the right of the search box will quickly go to the **Text-Defined Alarms** page and initiate the algorithm creation process with the current search content.
Result sorting	On the upper-right corner area Similarity 60 %, you can sort the search results by similarity from high to low, or by time in earliest first or latest first.

Function	Description
Play video	Click the panel of the query results, and then the system will start playing back the recording (10 seconds before and after the snapshot). ● Click , switch to the playback page, and the icon changes to . The supported operations in the playback page are as follows: ● Click  to stop playing videos. ● Click  to pause playing videos. ● Click  or  to play the previous or next video. ● Click the left or right button of the  to switch between Audio 1, Audio 2, or the mixed audio. ● Click  to adjust the volume. ● Click  to display the detection area or exclusion area. ● Click  to display the rule line or target box. ● Click , and then select human faces, human bodies, motor vehicles and animals. ◇ Playback: Click , the system will go to the playback page and search for the object in all channels. ◇ Search by image: Click , the system will go to the **Search by Image** page of the corresponding target in the **AI Search**. For example, when you select a motor vehicle, the system will go to the **Motor Vehicle Search**. Automatically select all cameras and search this picture. ◇ Track: Click , the system will go to the **Search by Image** page of the corresponding target in the **AI Search**. For example, when you select a face, the system will go to the **Face Search**. Automatically select all cameras and track this face. ● Click  to switch the playback duration of the recorded video. ● Click  to download the videos.
Export file	● Single export: Click  on the export option in the query results panel to export images, videos, and video players to the specified save path. ● Batch export: Select multiple items in the query results panel, click **Export**, and then export images, videos, and Excel files to the specified save path.  After setting up the alarm linkage for snapshots, when you export images, the system will simultaneously export the detected image along with the panoramic image captured at the time of the detection.

Function	Description
Search by image	Click , the system will go to the **Search by Image** page of the corresponding target in the **AI Search**. For example, when you select a motor vehicle, the system will go to the **Motor Vehicle Search**. Automatically select all cameras and search this picture.
View the track	Click , the system will go to the **Search by Image** page of the corresponding target in the **AI Search**. For example, when you select a face, the system will go to the **Face Search**. Automatically select all cameras and track this face.
Target registration	On the panel of query results, click to open the **Target Registration** dialog will appear. You can manually register a name for each detected face, or enable automatic recognition to match faces against your face database. 

6.5 Face Detection

An alarm is triggered when human faces are detected within the detection zone.

6.5.1 Enabling the Smart Plan

To use AI by Camera, you need to enable the smart plan first.

- The Device automatically shows the smart functions available on the connected remote devices.
- Smart plan is available on select remote devices.

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 a remote device in the device tree on the left.

Step 4 Select **Smart Plan** > **Smart Plan**.

- The smart functions available might differ depending on the remote devices.
- When the remote device is a PTZ camera, configure presets on the camera system first, and then you can set AI functions for each preset of the PTZ camera.

Step 5 Click to enable the smart plan.

Step 6 Click **Apply**.

6.5.2 Configuring Face Detection

Configure the alarm rule of face 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 a remote device on the device tree, and then select **Smart Plan** > **Face Detection**.

Step 4 Configure face detection.

- AI by Camera.
  1. Click **AI by Camera**, and then click to enable face detection.
  2. Click to enable face enhancement, which enables the system to preferably guarantee clear faces with low stream.
  3. Click or to set the minimum size or maximum size of the face detection zone. The system triggers an alarm only when the size of detected target is between the maximum size and the minimum size.

     AI by Camera supports **Face Enhancement** function. When you enable **Face Enhancement**, it prioritizes ensuring face clarity when the bitrate settings are relatively low.
- AI by Recorder.
  1. Click **AI by Recorder**, and then click to enable face detection.
  2. Click to draw a detection zone on the video.
     - Click , and then you can zoom in to full screen and draw again.
     - Click the dots on the frame of the detection zone, and then drag to adjust its range.
     - Click or to set the minimum size or maximum size of the face detection zone. The system triggers an alarm only when the size of detected target is between the maximum size and the minimum size.
  3. Select the snapshot mode and then set the parameters.

Table 6-3 Parameters of snapshot mode

Parameter		Description
Snapshot Mode		◇ **Optimized** : Capture the clearest face image within the configured period after the camera detects a face. ◇ **Quality Priority** : Capture face images only when the quality of the detected face exceeds the threshold.
Advanced	Elevation Angle	Set snapshot angle to be filtered during face detection.
	Left or Right Turn Angle	
	Head Tilt Angle	
	Snapshot Sensitivity	Set snapshot sensitivity during the face detection. The higher the sensitivity, the easier for the system to detect a face.
	Quality Threshold	When you select **Quality Priority**, we can detect face attributes only when the quality of the captured face image exceeds this threshold.
	Optimized Duration	Set the period during which the system captures the clearest face image after the camera detects a face.

Step 5 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 6 Click **Select** next to **Event Linkage** to set alarm actions.

Step 7 Click **Save**.

6.5.3 Live View of Face Detection

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

6.5.3.1 Setting Attribute Display

You can configure the display rule of face detection results.

Prerequisites

Before using this function, make sure that view has been created.

Procedure

Step 1 Log in to the PC client.

Step 2 Under the **Live** tab, open a view window.

Step 3 Click and then select the **Face** tab.

Step 4 Enable **Target Box Overlay**.

After it is enabled, when the system detects a face, a box will appear on the target.

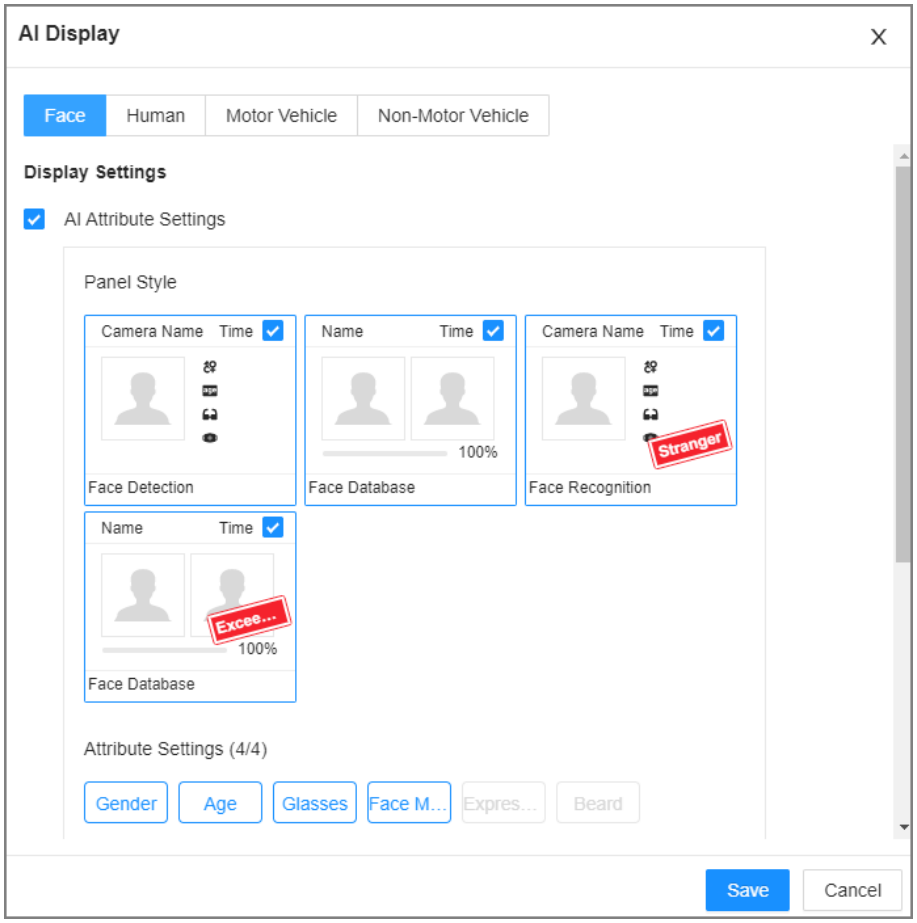
Step 5 Configure AI attributes settings.

With **AI Attributes Settings** enabled by default, when the system detects a face, a features panel appears on the live video. You can configure the style of the features panel and the attributes that you want to display.

1. Select the **Face Detection** panel.
2. Select the attributes that you want to display.
   - You can select up to 4 attributes.
   - 4 attributes have been selected by default. To select other attributes, cancel the selected attributes, and then select the ones you need.
3. On the **AI Attributes** section, select the attribute groups for face detection.

   Each face attribute is broken down into more specific groups. For example, you can select **Male** , **Female** or **Unknown** for **Gender**.

Figure 6-23 Attribute display



Step 6 Click **Save**.

6.5.3.2 Live View

Log in to the PC client, and then under the **Live** tab, open a view window.

- The video window displays the target boxes of currently detected faces.
- The number next to at the upper-right corner of the **Live** page represents the number of detected faces.

Figure 6-24 Face record



- You can view the detection time, face snapshot, and face attributes on the features panel on the right side of the **Live** page.
- Features panels are displayed on the right side of the **Live** page.

  Point to a features panel, and then the icons are displayed.

  - : Click the icon to add the detected images to face database.
  - : Click the icon or double-click the record to play back the 10 seconds of video before and after the snapshot.
  - : Click the icon to search for similar faces in historical face images across all channels.
  - : Click the icon to download the face snapshot and related video.

6.5.4 Face Search

6.5.4.1 Searching by Attributes

Procedure

Step 1 Log in to the PC client.

Step 2 Click on the upper-right corner of the **Live** page, or select **AI Search** on the home page.

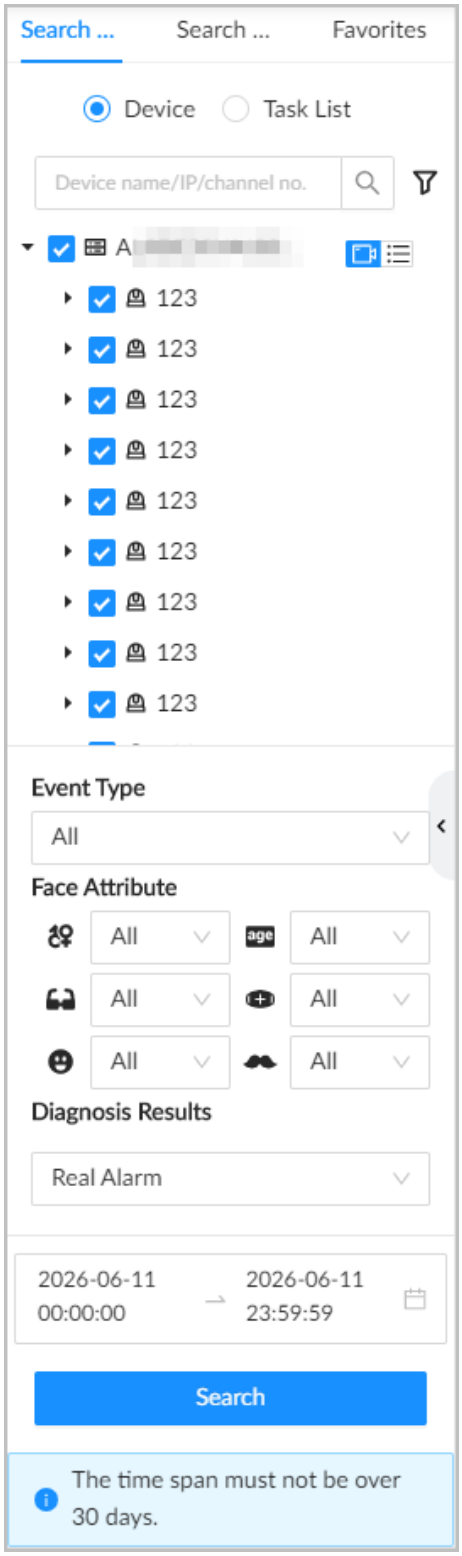
Step 3 Select **Face Search** .

Step 4 Select one or more remote devices, and then set **Event Type** to **Face Detection**.

Step 5 Set face attributes and search period.

The search results of face detection include two types: Face comparison with the face database and face results from human body comparison.

Figure 6-25 Set the search conditions



Step 6 Click **Search**.

Related Operations

Hover over a record, and then the following icons are displayed.

Table 6-4 Management of search results

Function	Operation
View Playback/ View Large Image	Click ▷ or double-click the record to play back the video and view large image, with attribute information displayed on the panel simultaneously. On the **View Playback** page, play the record automatically (10 seconds before and after the snapshot), and the following operations are supported. ● : Starts to play the video. ● : Stops playing the video. ● : Play the last/next video. ● : Auto play the following videos continuously. ● : Displays the detection area or exclusion area. ● : Displays the rule line or target box. ● : Switch from audio 1, auduo2 and mix. ● : Adjust the volume. ● : Displays the video in full screen. ● : Search by image. ● : Download the video. ● : Add the detected face to the face database. ● : Search for the tracks. On the **View Large Image** page, the following operations are supported. ● : Displays the last/next large image. ● : Displays the image in full screen. ● : Search by image. ● : Download the video. ● : Add the detected face to the face database. ● : Search for the tracks.

Function	Operation
View Details and Operations	Displays details on the right side. ● : Starts to play the video. ● : Pausing the video. ● : Stops playing the video. ● / : Play the last/next video. ● / : Switch from audio 1, audio2 and mix. ● : Adjust the volume. ● : Displays the detection area or exclusion area. ● : Displays the rule line or target box. ● : Rectangles the face, body, motor vehicle and animal objects. ◇ Playback: Click , the system will go to the playback page and search for the object in all channels. ◇ Search by image: Click , the system will go to the **Search by Image** page of the corresponding target in the **AI Search**. For example, when you select a motor vehicle, the system will go to the **Motor Vehicle Search**. Automatically select all cameras and search this picture. ◇ Track: Click , the system will go to the **Search by Image** page of the corresponding target in the **AI Search**. For example, when you select a face, the system will go to the **Face Search**. Automatically select all cameras and track this face. ● : Switch the playback duration of the video. ● : Download the video.
Add to Plate Database	In the results panel, click to add detected plate information to the plate database or add the detected face to the face database.
Search by Image	In the results panel, click to go to the **Search by image** page and search for similar records.
Search Track	In the results panel, click to go to the **Search by image** page and search for the person's tracks.

Function	Operation
Export	• Single export: Click on the query results panel to export images, videos, and video files to the specified save path. • Batch export: Select multiple items in the query results panel, click **Export**, and then export images, videos, and Excel files to the specified save path. After setting up the alarm linkage for snapshots, when you export images, the system will simultaneously export the detected image along with the panoramic image captured at the time of the detection.

6.5.4.2 Searching by Image

Background Information

Filter out the images whose similarity reaches the set value according to the given images.

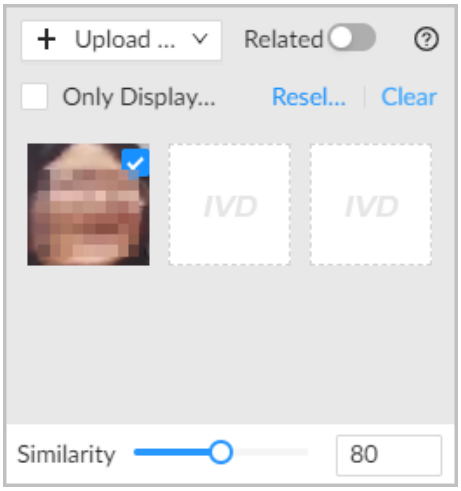
Search by image through the preview page

You can upload up to 50 face images. After uploading face images, you can select up to 10 images for search at one time.

1. Log in to the PC client.
2. Click **AI Search** , and then select **Face Search**, **Human Search** or **Motor Vehicle Search**.
3. Click **Search by Image** tag, move the mouse to **Upload Picture**, and then select **Sample Database Image**, **Passerby Database Image** or **Local Image**.
   - **Sample Database Image** : Set the search conditions for face pictures, and then click **Search**. Select the pictures of the sample database and click **OK**.
   - **Passerby Database Image** : Set the search conditions for face pictures, and then click **Search**. Select the pictures of the passerby database image and click **OK**.
   - **Local Image** : Select the pictures on the computer or USB storage devices, and then upload pictures.

   - Only face search supports selecting **Sample Database Image** and **Passerby Database Image**. When you use images in the face database to search, make sure that the face database has been configured.
   - If you want to use the local images, you need to make sure the images have been saved in the correct path.
     - When operating on the local interface, save the images in a USB storage device and then connect the USB storage device to the Device.
     - When operating on the webpage or PC client, save the images on your computer.
   - When the uploaded face picture is a half-length of full-body photo, the system will automatically process the uploaded picture, leaving only the face.
   - When existing multiple faces, the system automatically recognizes the faces in the picture and uploads multiple face pictures according to the number of faces recognized.
   - Click **Reselect**, and you can cancel selected face pictures.
   - Click **Only Display Selected Images**, the page only shows the selected face pictures.
   - Click **Clear**, and you can clear all uploaded face pictures.

Figure 6-26 Search by image



4. Tap to slide back, and then set the comparison similarity.
5. Select **Device** , **Face Database** or **Task List**, set the search conditions, and then click **Search**.
   - **Device** : Compare with the test results of the specified remote device to filter out the information that meets the setting conditions.
   - **Face Database** : Compare with the pictures of the face database and filter out the information that meets the setting conditions.

     Only face search supports **Face Database** search.
   - **Task List** : Compare with the intelligent task analysis results of task management and filter out the information that meets the setting conditions.

Search by image in the intelligence playback search results

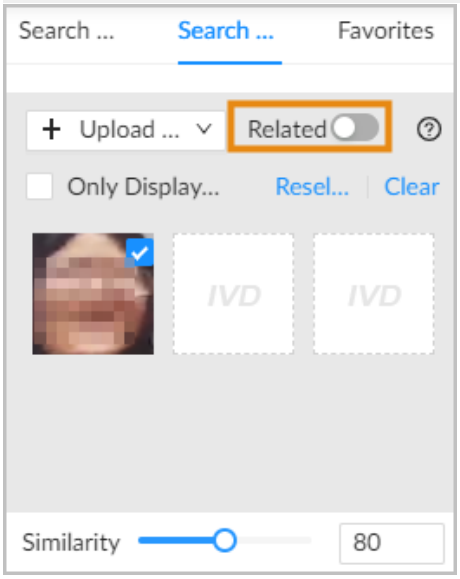
1. Log in to the PC client.
2. Click **AI Search** , and then select **Face Search**, **Human Search** or **Motor Vehicle Search**.
3. Select the channel, set search conditions, and then click **Search**.
4. Click on the search result panel.

   The system jumps to the **Search by Image** page and uses this image for retrieval.

Related operations

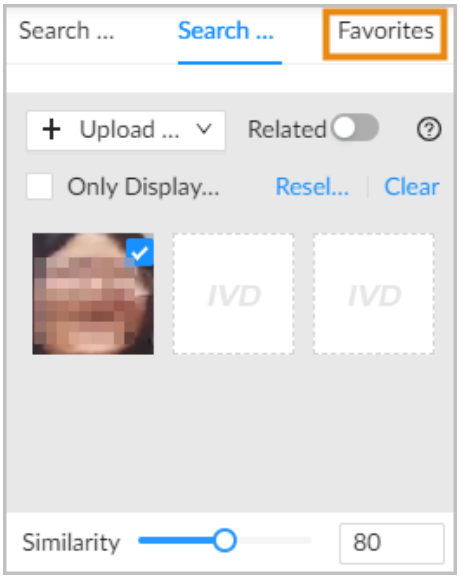
Search by Image page supports the following operations.

Table 6-5 Description of the intelligent playback page

Function Bar	Description
Related Search	Click **Face Search** or **Human Search**, and then click **Search by Image**. You can enable related search and the search results include face comparison and human body detection comparison. When searching only in **Device** or **Task List**, it is supported to enable related search. 
Thumbnail	Displays the selected image in thumbnail format above the search result. Click the picture to view picture results. 
Menu Bar	Set filter conditions, quickly filter out the required pictures according to feature attributes, and then sort them by time or similarity.
Time List	Displays the date list of the search.
Search Results	Displays the searched panel.
Sorting Method	Displays the pictures searched by time or similarity.

Function Bar	Description
View Playback/View Large Image	Click or double-click the record to play back the video and view large image, with attribute information displayed on the panel simultaneously. On the **View Playback** page, play the record automatically (10 seconds before and after the snapshot), and the following operations are supported. ● : Starts to play the video. ● : Stops playing the video. ● / : Play the last/next video. ● : Auto play the following videos continuously. ● : Displays the detection area or exclusion area. ● : Displays the rule line or target box. ● / : Switch from audio 1, auduo2 and mix. ● : Adjust the volume. ● : Displays the video in full screen. ● : Search by image. ● : Download the video. ● : Add the detected face to the face database. ● : Search for the tracks. ● : Add this result to your favorites, and then you can click the Favorites tab to quickly find the information later. ● : Hide the result. On the **View Large Image** page, the following operations are supported. ● / : Displays the last/next large image. ● : Displays the image in full screen. ● : Search by image. ● : Download the video. ● : Add the detected face to the face database. ● : Search for the tracks. ● : Add this result to your favorites, and then you can click the Favorites tab to quickly find the information later. ● : Hide the result.

Function Bar	Description
View Details and operations	Displays details on the right side. ● : Starts to play the video. ● : Pausing the video. ● : Stops playing the video. ● / : Play the last/next video. ● / : Switch from audio 1, auduo2 and mix. ● : Adjust the volume. ● : Displays the detection area or exclusion area. ● : Displays the rule line or target box. ● : Rectangles the face, body, motor vehicle and animal objects. ◇ Playback: Click , the system will go to the playback page and search for the object in all channels. ◇ Search by image: Click , the system will go to the **Search by Image** page of the corresponding target in the **AI Search**. For example, when you select a motor vehicle, the system will go to the **Motor Vehicle Search**. Automatically select all cameras and search this picture. ◇ Track: Click , the system will go to the **Search by Image** page of the corresponding target in the **AI Search**. For example, when you select a face, the system will go to the **Face Search**. Automatically select all cameras and track this face. ● : Switch the playback duration of the video.
Add to Plate Database	In the results panel, click to add detected plate information to the plate database or add the detected face to the face database.
Search by Image	In the results panel, click to go to the **Search by image** page and search for similar records.
Search Track	In the results panel, click to go to the **Search by image** page and search for the person's tracks.

Function Bar	Description
Export	• Single export: Click on the query results panel to export images, videos, and video players to the specified save path. • Batch export: Select multiple items in the query results panel, click **Export**, and then export images, videos, and Excel files to the specified save path. After setting up the alarm linkage for snapshots, when you export images, the system will simultaneously export the detected image along with the panoramic image captured at the time of the detection.
Favorites	In the search results panel of searching by picture, click ☆ to add this result to your favorites. 
Hide	In the search results panel of searching by picture, click to hide the result.

6.5.4.3 Viewing tracks

Add a digital map, and then bind the channels to actual locations on the map. If the same person is detected by multiple channels, the system can automatically draw connecting lines on the map to generate the movement path for route analysis.

Prerequisites

The map has been uploaded and channels points have been bound. For details, see "8.6.1.4 Configuring E-map".

Background Information

Multiple page such as **Live** and **Playback** support jumping to the **AI Search** page for tracks query.

Procedure

Step 1 Log in to the PC client.

Step 2 Click **AI Search** , select **Face Search** or **Human Search**, and then click **Search by Image** tab.

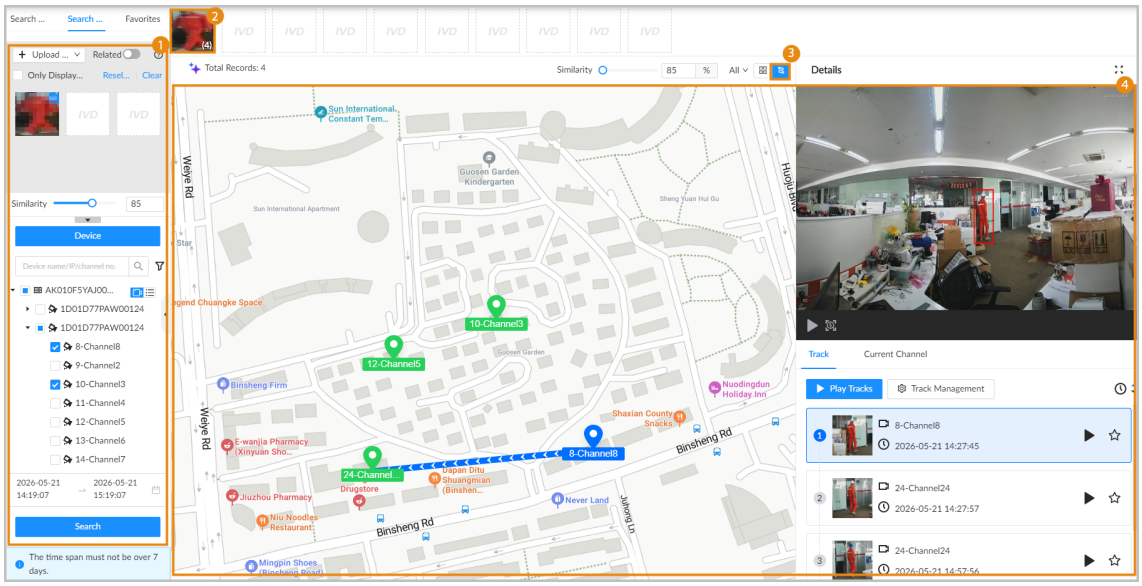
Step 3 Upload images, set query conditions, and then click **Search**.

Step 4 Select the target form the search results, and then click to switch to track mode.

Step 5 View location information on the left map and watch videos in the **Details** area on the right.

Details area supports various operations such as play, pause and precise retrieval. For details, see Table 6-5 .

Figure 6-27 View tracks



Track and **Current Channel** tabs supports the following operations.

- **Track** : Play video from each location in the order of people's movements. Supports exporting videos to local devices and adding videos to favorites.

  Click **Track Management** to perform the following operations.

Figure 6-28 Track management

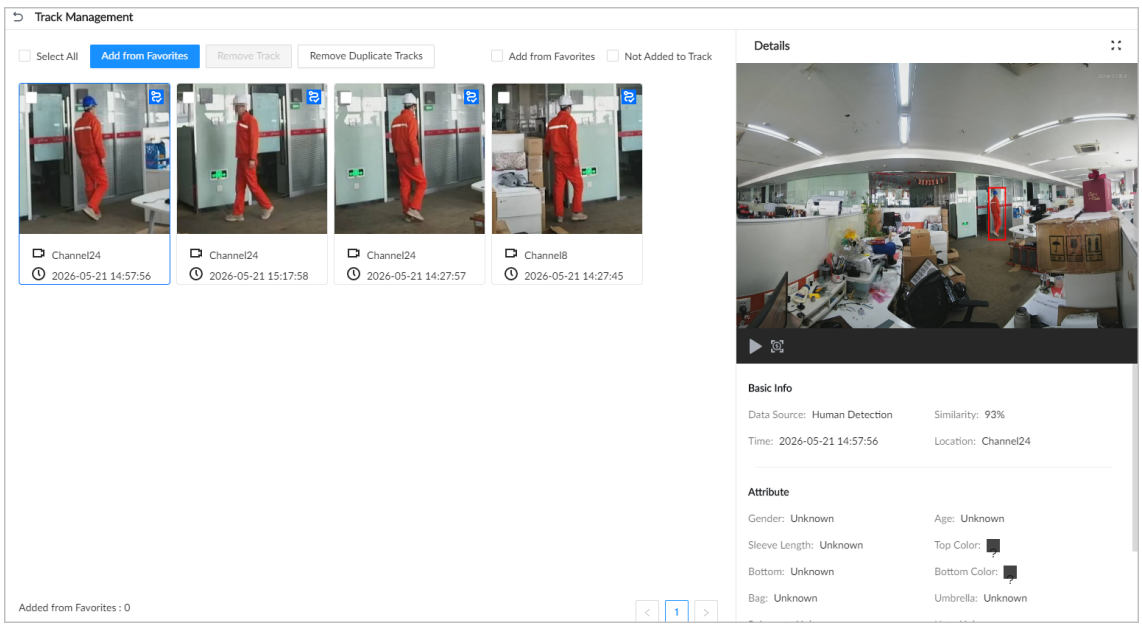


Table 6-6 Description of the track management

Function	Description
Add from Favorites	Click **Add from Favorites** , select the track in the favorites, and then click **Add to Track** to add it to the current track.
Remove Track	Select multiple tracks, click or tap the upper-right corner of a single track to remove it.
Remove Duplicate Tracks	Click **Remove Duplicate Tracks** to delete duplicate tracks.
Filter Tracks from Favorites or Not Added	◇ Click **Add from Favorites** checkbox to only display tracks added from favorites. ◇ Click **Not Added to Track** checkbox to only display removed tracks.
Details Operations	Supports various operations such as play, pause and precise retrieval. For details, see Table 6-5 .

- **Current Channel** : Click the channel points or click **Current Channel** on the right to view videos of targets at the points. Supports play videos, export videos locally and add videos to favorites.

6.5.4.4 Exporting Face Records

After you search for face images under the **AI Search** tab, you can export the search results.

- When operating on the local interface, you need to insert a USB storage device into your IVD.
- If you have configured alarm-linked picture storage, the exported alarm-linked snapshot contains the face snapshot and the background picture.

- Export in batches.

  Export more than one record. Support specifying file formats.

  1. Select one or more face records.

     To export all records, select the checkbox next to **Select All**.
  2. Click **Export**, and then select the format of the information that you want to export. You can export the images, videos and an excel that contains attributes information.
  3. Click **Browse** to select a storage path.
  4. Click **OK**.
- Export one by one.

  The exported file contains the image, video and video player by default.

  1. Point to the panel of a record, and then click .
  2. Select a file type for the video, set the storage path.
  3. Click **OK**.

6.6 Face Recognition

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

6.6.1 Configuration Modes

Face comparison can be configured in the following modes:

- Face recognition by Camera.
- Face detection by Camera+ face recognition by Recorder.
- Face recognition by Camera + face recognition by Recorder.
- Face detection by Recorder + face recognition by Recorder.
- Video metadata by Camera or by Recorder + face recognition by Recorder.

6.6.2 Face Comparison by Camera

6.6.2.1 Configuration Procedure

Figure 6-29 Configure face recognition (AI by camera)



6.6.2.2 Enabling the Smart Plan

To use AI by Camera, you need to enable the corresponding smart plan first. For details, see "6.5.1 Enabling the Smart Plan".

6.6.2.3 Configuring Remote Face Database

The Device can get face databases from the remote devices, and also allows creating face databases for remote devices. The remote device face database is used for face comparison (AI by Camera).

You cannot view the image information in the remote face database from the Device.

6.6.2.3.1 Creating a Remote Face Database

On this device, you can access the face database created on a remote device, and it also supports creating a face database on the device to manage face images on the remote device categorically. The face database created can be synchronized to the remote device. The face database on the remote device is applicable for AI by Camera face comparison.

Background Information

On this device, you cannot view the image information in the face database on the remote device.

Procedure

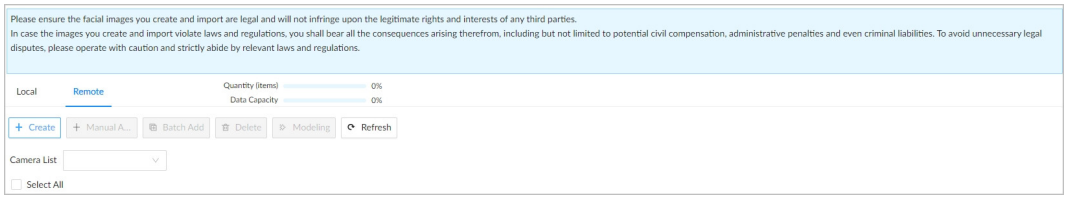
Step 1 Log in to the PC client.

Step 2 On the home page, select **Algorithm** > **Database Management** > **Sample Database** > **Remote**.

Step 3 Select a remote device from **Camera List**.

Step 4 Click **Create**.

Figure 6-30 Remote face databases



Step 5 Enter a name for the face database.

Step 6 Click **Register** or **Save and Close**.

- Click **Register** to add face images to the database.
- Click **Save and Close** if you want to add face images later.

Related Operations

- View face database details and status.

Figure 6-31 Face database

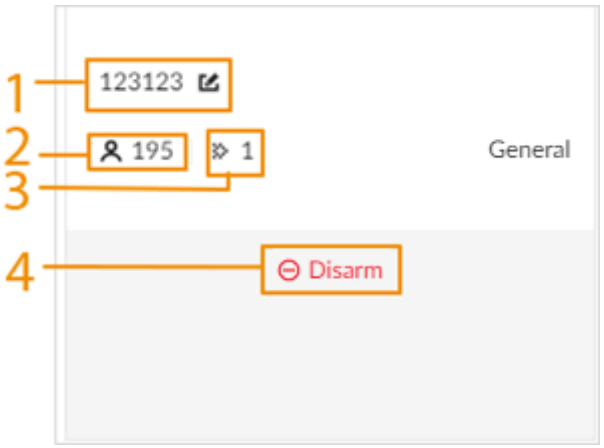


Table 6-7 Parameters of face database

No.	Description
1	Face database name. Click to change the name.
2	Number of face images in the face database.
3	Number of face images that failed to be modeled.
4	Remote devices associated to this face database for face comparison. Disarm indicates that no remote devices are associated to the database.

- Search for face images.

  Click to search for images in the database by name, gender, birthday, credential type and No., and modeling status.
- Arm the face database.
- Delete face databases:

  ◇ One by one: Click .

- In batches: Hover over the face database, and then select the database by clicking . After selecting multiple databases, click .
- Delete all: Click **Select All** , and then click **Delete**.

- Clear a face database.

  To clear a face database, select the face database, and then click **Clear**.

6.6.2.3.2 Adding Face Images for Remote Devices

Add face images to the created face database.

Make sure that you have obtained the face images and saved them in the proper path.

- When operating on the local interface, save the images in a USB storage device and then connect the USB storage device to the Device.
- When operating on the web interface or PC client, save the images on your computer.

Manual Add

You can add face images one by one. We recommend this method if you register only a few face images.

1. Log in to the PC client.
2. Select **Algorithm** > **Database Management** > **Sample Database** > **Remote**.
3. Select a face database, and then click **Manual Add**.
4. Click and select a face image.

   - When the uploaded image is half-length photo or full-body photo, the system automatically processes the image to retain only the face area.
   - When there are multiple faces in an image, the system automatically identifies the faces in the image. You can select the face images that you want to upload.
   - Click **Reselect** to cancel the selection of face images.
5. Click **Save** and import face images.

   Point to the face image and then click **Upload Again** to change it.
6. Fill in face image information.
7. Click **Add More** or **Save**.

   - Click **Add More** to save current face image information and add another more face images.
   - Click **Save** to save current face image information and complete registration.

Batch Import

Before the batch import, name the face image in the format of "Name#SGender#BBirthday#NCountry/Region#TCredential Type#MCredential No.#AAddress.jpg". After successful import, the system will identify the face image automatically.

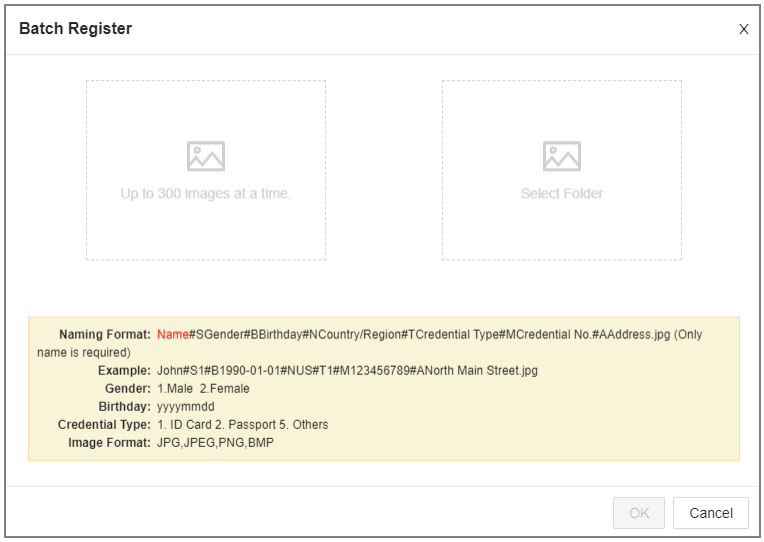
Name is required and the rest are optional. For example, if you want to enter the name and ID number only, the name can be Tim#S#B#N#R#T#M0000#A.jpg or Tim#M0000.jpg.

Table 6-8 Naming rules for batch import

Item	Description
Name	Enter the corresponding name.
Gender	Enter number. 1: Male; 2: Female.
Birthday	Enter number in the format of yyyymmdd or yyyy-mm-dd. For example, 20181123.
Country/Region	Enter the corresponding abbreviation of the country or region.
Credential type	Enter the corresponding number. 1. ID card, 2. Passport, 5. Others.
Credential No.	Fill in the corresponding credential No.
Address	Enter the detailed address.

1. Log in to the PC client.
2. Select **Algorithm** > **Database Management** > **Sample Database** > **Remote**.
3. Select a face database, and then click **Add**.
4. Import face images.
   - Upload a file: Click on the left, select multiple face images, and then click **Open**.
   - Upload a folder: Click on the right, and then select the folder with face images.

Figure 6-32 Batch import



5. Click **OK**.
6. Click **Add More** or **Complete**.
   - Click **Add More** to save current face image information and add more face images.
   - Click **Complete** to save current face image information and complete registration.

Database Import

To import face images from another device into the current device, you can import a bin file of face images exported from that device.

1. Log in to the PC client.
2. Select **Algorithm** > **Database Management** > **Sample Database** > **Local**.

3. Select a face database, and then click **Import Database**.
4. Click **Browse** to select a bin file, enter the password that you set when exporting the database, and then click **OK**.

   A bin file is divided into multiple parts when being exported if it is larger than 4 GB. When importing the file parts, you just need to select any one part of the file, and then all parts are imported.
5. Click **Add More** or **Save**.
   - Click **Add More** to save current face image information and add another more face images.
   - Click **Save** to save current face image information and complete registration.

6.6.2.4 Configuring Face Comparison (by Camera)

Background Information

Configure the alarm rule of face comparison.

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 a remote device on the device tree, and then select **Smart Plan** > **Face Comparison**.

Step 4 Click **AI by Camera** , and then click  to enable face comparison.

Step 5 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 6 Click **Select** next to **Event Linkage** to set alarm actions.

Step 7 Click **Save**.

6.6.2.5 Live View of Face Comparison

You can view real-time face comparison images under the **Live** tab.

6.6.2.5.1 Setting Attribute Display

You can configure display rule of AI detection results.

Before using this function, make sure that view has been created.

Procedure

Step 1 Log in to the PC client.

Step 2 Under the **Live** tab, open a view window.

Step 3 Click , and then select the **Face** tab.

Step 4 Enable **Target Box Overlay**.

After it is enabled, when the system detects a face, a box will appear on the target.

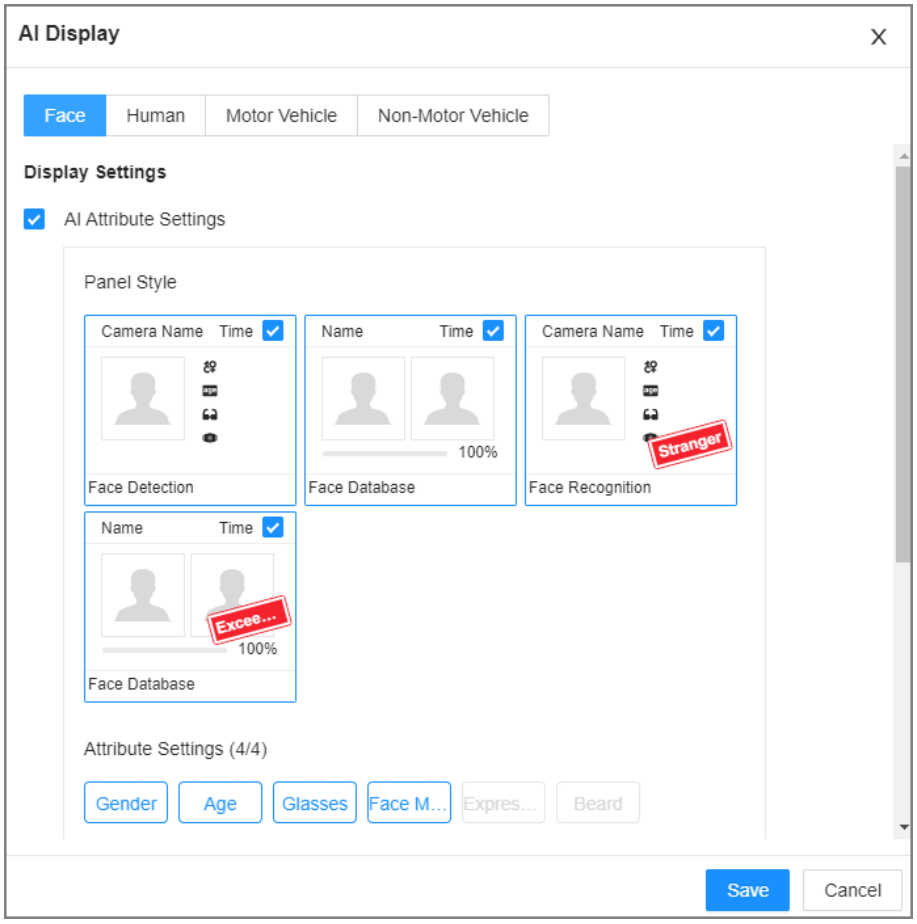
Step 5 Configure AI attributes settings.

With **AI Attributes Settings** enabled by default, when the system detects a face, a features panel appears on the live video. You can configure the style of the features panel and the attributes that you want to display.

1. Select the panels of **Face Database** , **Stranger** and **Exceed10**.
   - If the **Face Database** panel is selected, it is displayed on the live video when the similarity between a detected face and one in the face database reaches the threshold.
   - If the **Stranger** panel is selected, it is displayed on the live video when the similarity between a detected face and one in the face database does not reach the threshold.
   - If the **Exceed10** panel is selected, it is displayed on the live video when the similarity between a detected face and one in the face database reaches the threshold and the detected entries reach the defined number.
2. Select the attributes that you want to display.
   - You can select up to 4 attributes.
   - 4 attributes have been selected by default. To select other attributes, cancel the selected attributes, and then select the ones you need.
3. On the **AI Attributes** section, select the attribute groups for face detection.

   Each face attribute is broken down into more specific groups. For example, you can select **Male** , **Female** or **Unknown** for **Gender**.

Figure 6-33 Attribute display



Step 6 Click **Save**.

6.6.2.5.2 Live View

Log in to the PC client, and then under the **Live** tab, open a view window.

- The video window displays the target boxes of currently detected faces.
- The number next to at the upper-right corner of the **Live** page represents the number of detected faces.
- You can view the detection time, the detected face image, face image in the database, comparison result and database name on the features panel on the right side of the **Live** page. After enabling the stranger mode, when the detected face image has no match in the database, a **Stranger** tag appears on the features panel.
- Point to a features panel and then the operations icons are displayed.
  - : Click the icon to add the detected images to face database.
  - : Click the icon or double-click the record to play back the 10 seconds of video before and after the snapshot.
  - : Click the icon to search for similar faces in historical face images across all channels.
  - : Click the icon to download the face snapshot and related video.

6.6.2.6 Face Search

You can search face records by attributes or by image, and then export the search results.

6.6.2.6.1 Searching by Attributes

Procedure

Step 1 Log in to the PC client.

Step 2 Click on the upper-right corner of the **Live** page, or select **AI Search** on the home page.

Step 3 Select **Search by Face** > **Search by Attributes**.

Step 4 Select one or more remote devices, and then set **Event Type** to **Face Recognition**.

Step 5 Select a face mode.

- **General** : Search for faces without the stranger or high frequency tag.
- **Stranger** : Search for faces with the stranger tag.

  Make sure that stranger mode has been enabled for face comparison.
- **Exceeding Max Entries** : Search for faces with the high frequency tag.

  Make sure that entries frequency has been configured.

Step 6 Set face attributes and search period.

Step 7 Click **Search**.

Related Operations

After the query, the system displays the query results in the form of a panel. For details, see Table 6-4 .

6.6.2.6.2 Searching by Image

Upload face pictures to search the records for similar faces. For details, see "6.5.4.2 Searching by Image".

6.6.2.6.3 Viewing Tracks

Add a digital map, and then bind the channels to actual locations on the map. If the same person is detected by multiple channels, the system can automatically draw connecting lines on the map to generate the movement path for route analysis. For details, see "6.5.4.3 Viewing tracks".

6.6.2.6.4 Exporting Face Records

Export the face records, including pictures, videos and detailed information. For details, see "6.5.4.4 Exporting Face Records".

6.6.3 Face Detection by Camera + Face Comparison by Recorder

6.6.3.1 Configuration Procedure

Figure 6-34 Configure face detection (AI by camera)

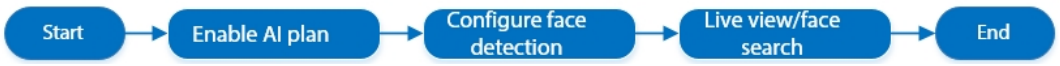
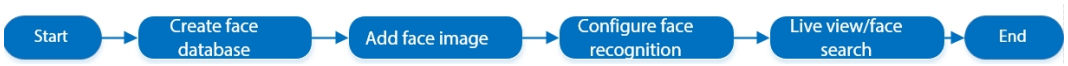


Figure 6-35 Configure face recognition (AI by recorder)



6.6.3.2 Enabling the Smart Plan

To use AI by Camera, you need to enable the corresponding smart plan first. For details, see "6.5.1 Enabling the Smart Plan".

6.6.3.3 Configuring Face Detection (by Camera)

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 a remote device on the device tree, and then select **Smart Plan** > **Face Detection**.

Step 4 Click **AI by Camera**, and then click to enable face detection.

AI by Camera supports face enhancement, which enables the system to preferably guarantee clear faces with low stream.

Step 5 Draw a detection zone on the video.

- Click the dots on the frame of the detection zone, and drag to adjust its range.
- Click or to set the minimum size or maximum size of the face detection zone. The system triggers an alarm only when the size of detected target is between the maximum size and the minimum size.

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. You can also add a new schedule.

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

Step 8 Click **Save**.

6.6.3.4 Configuring Local Face Database

You can create local face databases on the Device to manage face images for face comparison (AI by Recorder).

6.6.3.4.1 Creating a Local Face Database

Create a local face database to sort out and manage the face images uploaded to the Device.

Procedure

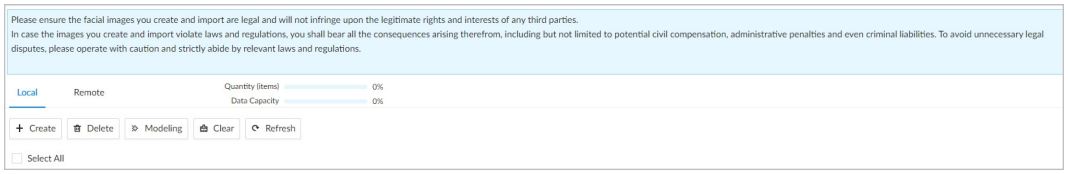
Step 1 Log in to the PC client.

Step 2 On the home page, select **Algorithm** > **Database Management** > **Sample Database** > **Local**.

Step 3 Click **Create**.

- **Quantity** : The proportion of the number of added face images in the sample databases and passerby databases to the allowed face images in total.
- **Data Capacity** : The proportion of the space occupied by the sample databases and passerby databases to the allowed space in total.

Figure 6-36 Local face database



Step 4 Enter the information for the face database.

Figure 6-37 Add local face database

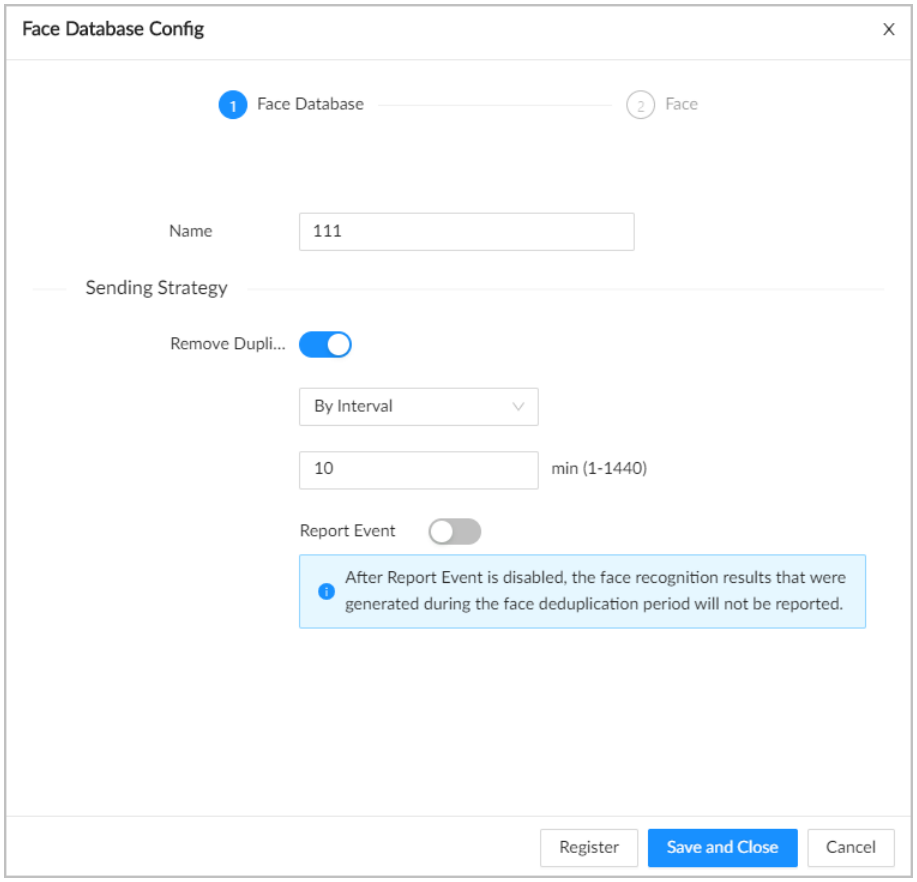


Table 6-9 Description of local face database

Parameter	Description
Name	Enter the name of the database.
Remove Duplicate Faces	When the captured face snapshot has a match in the local database, and its quality is higher than that of the one in the database, the system replaces the face image in the database with the snapshot. In this case, the duplicate face will not trigger the event. • **Always**: Always remove duplicate face images. • **By Interval**: Remove duplicate face images by interval to control comparison pressure. • **By Duration**: Remove duplicate face images within the defined period.
Report Event	• If remove duplicate faces is disabled, report event is disabled by default. In this case, the system will not report the event in live, AI search or AI report. • If remove duplicate faces and report event are enabled, a duplicate face panel is displayed on the live page.

Step 5 Click **Register** or **Save and Close**.

- Click **Register** to add face images to the database.
- Click **Save and Close** to finish now. You can add face images later.

Related Operations

- View face database details and status.

Figure 6-38 Face database

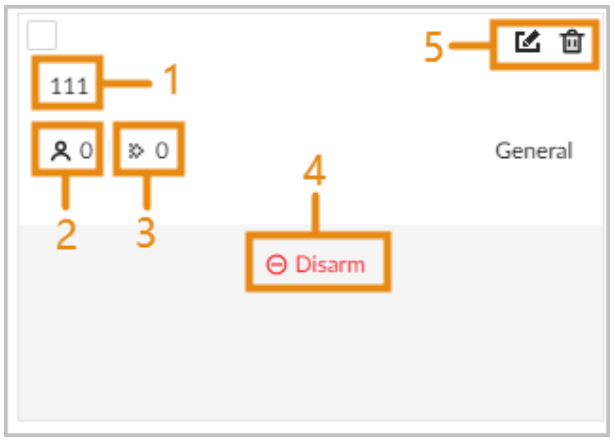


Table 6-10 Parameters of face database

No.	Description
1	Face database name. Click to change the name.
2	Number of face images in the face database.
3	Number of face images that failed to be modeled.
4	Remote devices associated to this face database for face comparison. Disarm indicates that no remote devices are associated to the database.
5	Hover the mouse over the face database card to display the edit and delete icons, which support modifying configurations or deleting the face database.

- Search for face images.

  Click to search for images in the database by name, gender, birthday, credential type and No., and modeling status.
- Arm the face database.

  For details, see "6.6.3.5 Configuring Face Recognition (by Recorder)".
- Delete face databases.
  - One by one: Click .
  - In batches: Hover over the face database, and then select the database by clicking . After selecting multiple databases, click .
  - Delete all: Select the **Select All** checkbox, and then click **Delete**.
- Clear a face database.

  To clear a face database, select the face database, and then click **Clear**.

6.6.3.4.2 Exporting a Face Database

You can export a bin file of face images from the current device into another device so that the face database can be shared among devices. The exported file is encrypted for better security.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **Algorithm** > **Database Management** > **Sample Database** > **Local**.

Step 3 Select one or more face databases, and then click **Export Database**.

Step 4 Click **Browse** to select the storage path.

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

The password is required when you import the exported database.

Step 6 When the export process is complete, click **Complete**.

If the bin file being exported is larger than 4 GB, the file is divided into multiple parts, with the first named as device name_database name_exporting time_part1.zip.

6.6.3.4.3 Adding Face Images

Add face images to the created face database.

Make sure that you have obtained the face images and saved them in the proper path.

- When operating on the local interface, save the images in a USB storage device and then connect the USB storage device to the Device.
- When operating on the web interface or PC client, save the images on your computer.

Manual Add

You can add face images one by one. We recommend this method if you register only a few face images.

1. Log in to the PC client.
2. Select **Algorithm** > **Database Management** > **Sample Database** > **Remote**.
3. Select a face database, and then click **Manual Add**.
4. Click , and then select a face image.

   - When the uploaded image is half-length photo or full-body photo, the system automatically processes the image to retain only the face area.
   - When there are multiple faces in an image, the system automatically identifies the faces in the image. You can select the face images that you want to upload.
   - Click **Reselect** to cancel the selection of face images.
5. Click **OK**, and then import face images.

   Point to the face image and then click **Upload Again** to change it.
6. Fill in face image information.

7. Click **Add More** or **Save**.
   - Click **Add More** to save current face image information and add another more face images.
   - Click **Save** to save current face image information and complete registration.

You can add face images one by one. We recommend this method if you register only a few face images.

1. Log in to the PC client.
2. Select **Algorithm** > **Database Management** > **Sample Database** > **Local**.
3. Select a face database, and then click **Manual Add**.
4. Click and select a face image.

   - When the uploaded image is half-length photo or full-body photo, the system automatically processes the image to retain only the face area.
   - When there are multiple faces in an image, the system automatically identifies the faces in the image. You can select the face images that you want to upload.
   - Click **Reselect** to cancel the selection of face images.
5. Click **Save** and import face images.

   Point to the face image and then click **Upload Again** to change it.
6. Fill in face image information.
7. Click **Add More** or **Save**.
   - Click **Add More** to save current face image information and add another more face images.
   - Click **Save** to save current face image information and complete registration.

After adding the image, at the lower-left corner of the face image, there is an icon . It means the Device is modeling the face.

Bin Import

To import face images from another device into the current device, you can import a bin file of face images exported from that device.

1. Log in to the PC client.
2. Select **Algorithm** > **Database Management** > **Sample Database** > **Local**.
3. Double-click a face database.
4. Click **Import Database**.
5. Click **Browse** to select a bin file, enter the password that you set when exporting the database, and then click **OK**.

   A bin file is divided into multiple parts when being exported if it is larger than 4 GB. When importing the file parts, you just need to select any one part of the file, and then all parts are imported.
6. Click **Add More** or **Save**.
   - Click **Add More** to save current face image information and add another more face images.
   - Click **Save** to save current face image information and complete registration.

Adding from Detection Snapshots

Add the snapshot of face detection or face comparison to the face database.

1. Log in to the PC client.
2. Select face images under the **Live** tab.

   The following two ways are available.

   - Point to a face snapshot in the refreshing snapshot list on the right side of the live video, and then click .
   - Click , point to a face snapshot, and then click .
3. Select a face database, and fill in person information.
4. Click **OK**.

6.6.3.4.4 Creating a Passerby Database

If you configure an alarm to link a passerby database, when the detected face is not in the linked sample database, the system automatically captures the face image, and then save it to the linked passerby database.

Procedure

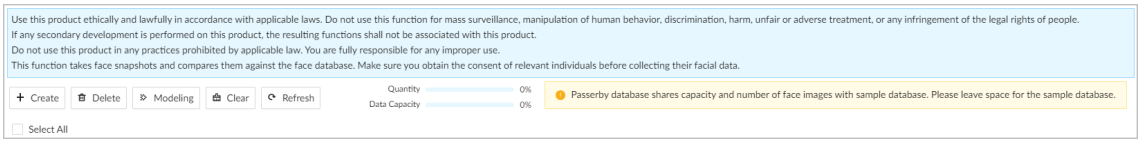
Step 1 Log in to the PC client.

Step 2 On the home page, select **Algorithm** > **Database Management** > **Passerby Database**.

Step 3 Click **Create**.

- **Quantity** : The proportion of the number of added face images in the sample databases and passerby databases to the allowed face images in total.
- **Data Capacity** : The proportion of the space occupied by the sample databases and passerby databases to the allowed space in total.

Figure 6-39 Local passerby database



Step 4 Enter the information, and then click **Save**.

Figure 6-40 Passerby database

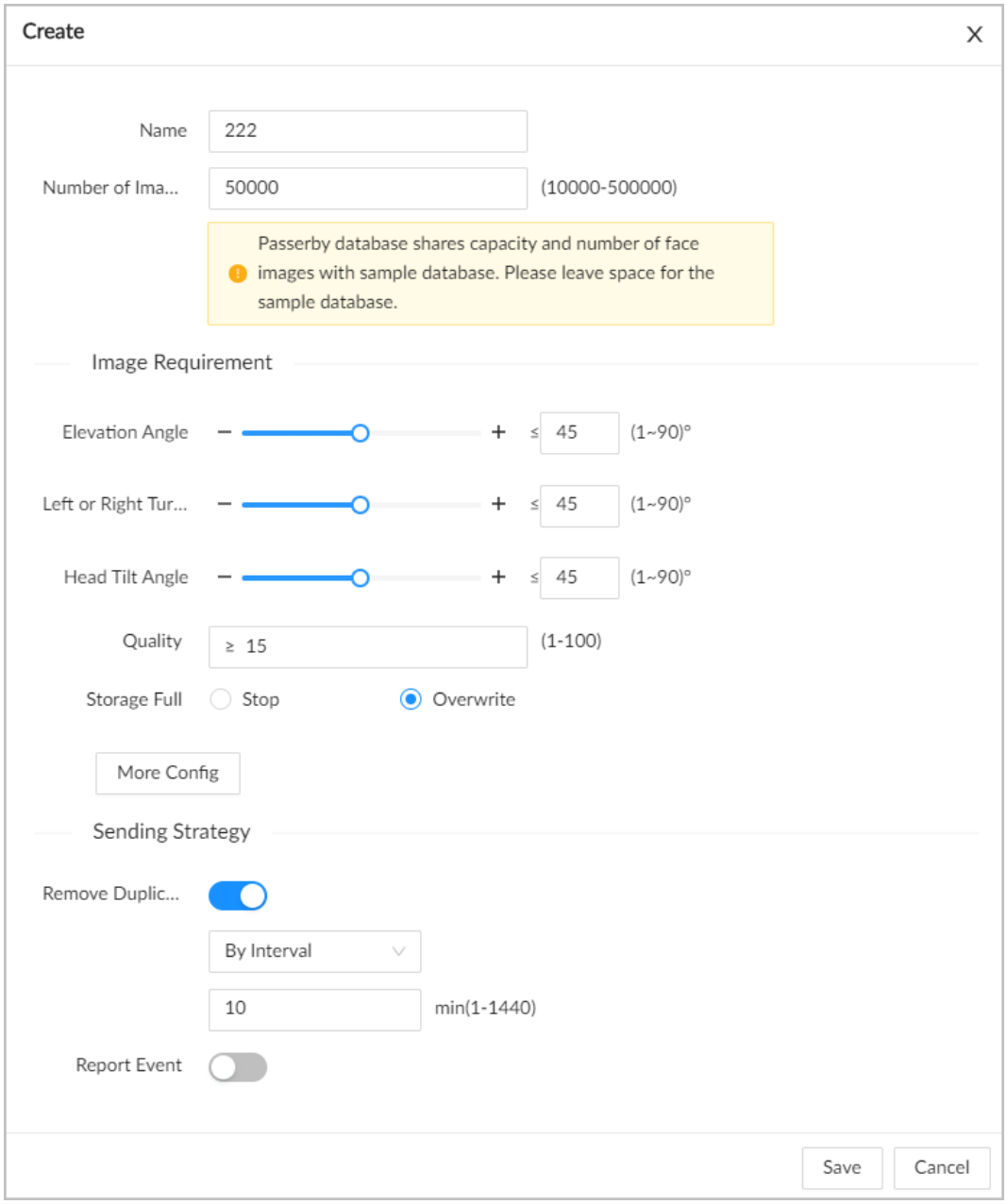


Table 6-11 Parameters of creating passerby database

Parameter	Description
Name	Enter the name of the database.

Parameter		Description
Number of Images		Configure how many face images the database can store. ● Maximum = Total number of face images of the Device – the face image number of the current sample databases – the face image number of the current passerby databases. ● Minimum: 10,000. Share capacity and entry numbers with the sample database, you must reserve sufficient space for this number.
Image Requirement	Elevation Angle	Set the allowed angle for the face image. The value ranges from 0 through 90 degrees.
	Left or Right Turn Angle	
	Heat Tilt Angle	
	Quality	Set a quality threshold. Only face images at or above the threshold can be added. The value range from 1 to 100.
	Storage Full	The storage strategy when storage space is used up. ● **Stop** : No more images can be added. ● **Overwrite** : The newest images overwrite the oldest images. Remember to back up the old images as necessary.
	More Configuration	Click **More Config**, set parameters on the pop-up dialog, such as pupillary distance, alignment level, clarity, and enable functions including mask wearing permission, sunglasses detection and detection of blocked eyes, mouth and forehead.
Sending Strategy	Remove Duplicate Faces	When the captured face snapshot has a match in the passerby database, and its quality is higher than that of the one in the database, the system replaces the face image in the database with the snapshot. In this case, the duplicate face will not trigger an event. ● **Always** : Always remove duplicate face images. ● **By Interval** : Remove duplicate face images by interval to control comparison pressure. ● **By Duration** : Remove duplicate face images within the defined period.
	Report Event	● If remove duplicate faces is disabled, report event is disabled by default. In this case, the system will not report the event in **Live** , **AI search** or **AI report**. ● If remove duplicate faces and report event are enabled, a duplicate face panel is displayed on the live page.

Related Operations

- View face database details and status.

Figure 6-41 Face database

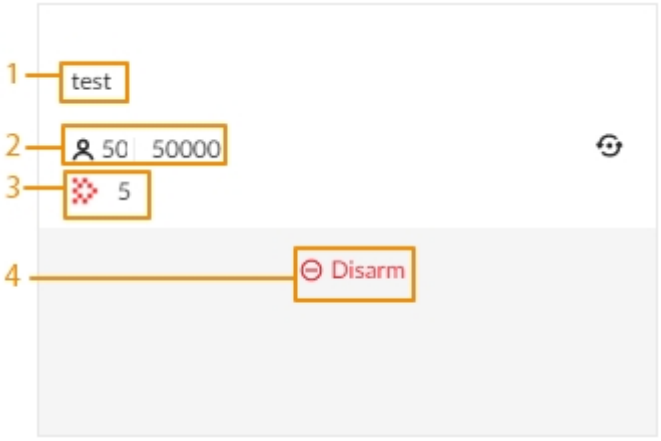


Table 6-12 Parameters of face database

No.	Description
1	Face database name. Click to change the name.
2	The number of added face images in the face database and the total number of images that can be added to the database.
3	Number of face images that failed to be modeled.
4	Remote devices associated to this face database for face comparison. Disarm indicates that no remote devices are associated to the database.

- Manage face images.

  Double-click the face database, and then you can model and delete face images in the database.
- Arm the face database.
- Delete face databases.
  - One by one: Click .
  - In batches: Hover over the face database, and then select the database by clicking . After selecting multiple databases, click .
  - Delete all: Click **Select All** , and then click **Delete**.
- Clear a face database.

  To clear a face database, select the face database, and then click **Clear**.

6.6.3.4.5 Modeling Faces

Model faces to abstract the information of the face image and then import the information to the database. After that, the Device can compare human faces, and search for human faces.

- After you add face images to the databases, the images will be modeled automatically. This section is for reference when modeling fails or you want to model the images again.
- The more the face images, the longer the modeling process takes.
- During the modeling process, some functions such as face comparison, face search by image become unavailable. These functions become available after the modeling process is complete.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **Algorithm** > **Database Management** > **Sample Database**.

Step 3 Double-click a face database.

Step 4 Select face images and then click **Modeling**.

- Select the **Select All** checkbox to select all face images in the database.
- If there are too many face images in the face database, click to filter the face images.

Step 5 Click **Start**.

The modeling is successful if disappears from the lower-left corner of the face image. The modeling might fail if the face image is not clear or does not contain complete information, and appears at the lower-left corner of the face image.

6.6.3.4.6 Managing Face Images

Log in to the PC client, and then on the home page, select **Algorithm** > **Database Management**. You can maintain and manage face images in the face databases to ensure that people information is always correct. The system supports editing face picture information, copying face pictures to other face databases and deleting face pictures.

Editing Face Images

1. Double-click a local sample database, point to a face picture, and then click .

   You cannot edit the face images in the remote sample databases or passerby databases.
2. Edit the information.
3. Click **OK**.

Copying Face Images

1. Double-click a face database, select one or more face images, and then click **Copy**.
2. Select the database to which you are copying the face images.

   - If there are many databases, you can enter all or part of the database, and then click **Search** to search for the database.
   - Cancel the selection of **Reserve data in original database** if you want to delete the copied face images in the original database.
3. Click **Save**.

Deleting Face Images

Double-click a face database, and then you can delete face images one by one or in batches.

- One by one: Point to the face image, and then click .

- In batches:
  - Select multiple images, and then click **Delete** to delete the selected images.
  - Select the **Select All** checkbox, and then click **Delete** to delete all the images.

Exporting Face Images

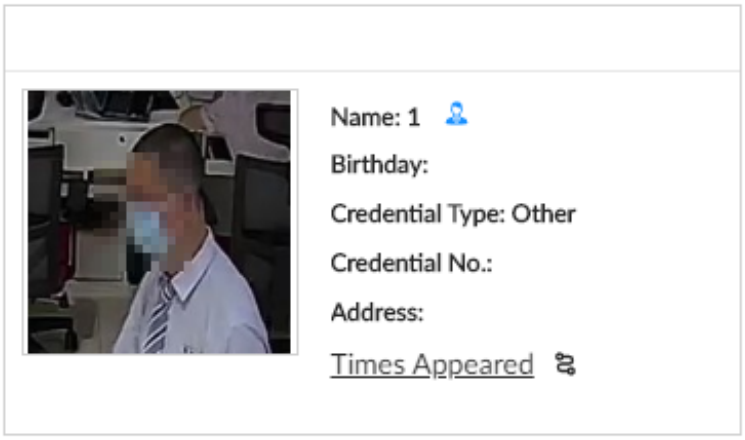
Export the face image from the sample database to the local device.

1. Double-click a face database.
2. Select the face image, and then click **Export**.
3. Click **OK** in the pop-up dialog.
4. Select a local save path, and then click **OK** to export the face image to the local device.

6.6.3.4.7 Viewing Comparison Records and Tracks

Log in to the PC client, on the home page, select **Algorithm** > **Database Management**, and then double-click a local sample database.

Figure 6-42 Time appeared



- Click **Time Appeared** on the face card to check the historical comparison records of the person.
- Click on the face card to view the track details. For details, see "6.5.4.3 Viewing tracks".

  The favorites function is not supported when viewing tracks in the sample database and passerby database.

6.6.3.5 Configuring Face Recognition (by Recorder)

Prerequisites

To use face comparison (AI by Recorder), you need to enable face detection first.

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 a remote device on the device tree, and then select **Smart Plan** > **Face Comparison**.

Step 4 Click **AI by Recorder** , and then click to enable face comparison.

Step 5 Click **Schedule** to select a schedule from the drop-down list.

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

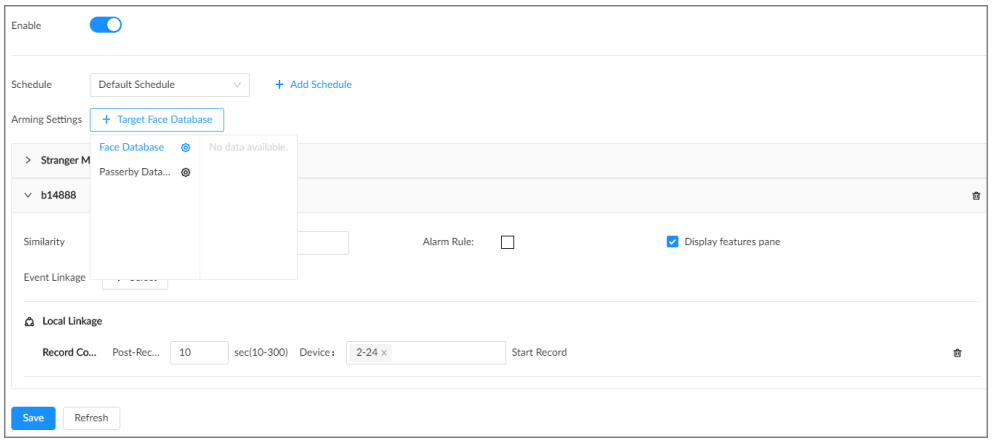
You can select an existing schedule from the **Schedule** drop-down list or add a new schedule.

Step 6 Set the linked face database.

1. Click **Target Face database**, and then select a face database.

Click , and then you can go to the **Face Database Config** page where you can configure the face databases.

Figure 6-43 Configure face comparison (by recorder)



2. Configure the parameters.

Table 6-13 Configuration of target face database

Icon/Parameter	Description
	The selected database is enabled by default. Click the icon to disable it.
	Delete the database.
Similarity	Set the similarity threshold for comparison. The system compares the detected result with the images in the database. An alarm is triggered when the similarity reaches the threshold.
Alarm Rule	Click to select a color for the alarm rule box.
Display Feature Pane	Select the checkbox to enable the features pane. The features pane appears on the live video once there is an alarm.

3. Click **Select** next to **Event Linkage** to set alarm actions.

Step 7 (Optional) Enable the stranger mode.

With the stranger mode enabled, an alarm is triggered when the face comparison similarity is lower than the configured threshold.

1. Click to enable the stranger mode.
2. Set the parameters.

Table 6-14 Stranger control mode description

Parameter	Description
Alarm Rule	Click to select a color for the alarm rule box.
Display Feature Pane	Click to enable the features pane. The features pane appears on the live video once there is an alarm.

3. Click **Select** next to **Event Linkage** to set alarm actions.

Step 8 Click **Save**.

6.6.3.6 Live View

You can view real-time face comparison images.

6.6.3.7 Face Search

You can search face records by attributes or by image, and then export the search results. For details, see "6.5.4 Face Search".

6.6.4 Face Comparison by Camera + Face Comparison by Recorder

6.6.4.1 Configuration Procedure

Figure 6-44 Configure face recognition (AI by camera)



Figure 6-45 Configure face recognition (AI by recorder)



6.6.4.2 Enabling the Smart Plan

To use AI by Camera, you need to enable the corresponding smart plan first. For details, see "6.5.1 Enabling the Smart Plan".

6.6.4.3 Configuring Face Recognition (by Camera)

Configure face comparison rules. For details, see "6.6.2.4 Configuring Face Comparison (by Camera)".

6.6.4.4 Configuring Local Face Databases

You can create local face databases on the Device to manage face images for face comparison (by Recorder). For details, see "6.6.3.4 Configuring Local Face Database".

6.6.4.5 Configuring Face Recognition (by Recorder)

Configure face recognition rules. For details, see "6.6.3.5 Configuring Face Recognition (by Recorder)".

6.6.4.6 Live View

You can view real-time face comparison images. For details, see "6.6.2.5 Live View of Face Comparison".

6.6.4.7 Face Search

You can search face records by attributes or by image, and then export the search results.

6.6.5 Face Detection by Recorder + Face Recognition by Recorder

6.6.5.1 Configuration Procedure

Figure 6-46 Configure face detection (AI by recorder)



Figure 6-47 Configure face recognition (AI by recorder)



6.6.5.2 Configuring Face Detection (by Recorder)

Background Information

Configure the alarm rule of face 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 a remote device on the device tree, and then select **Smart Plan** > **Face Detection**.

Step 4 Click **AI by Recorder** , and then click to enable face detection.

Step 5 Click to draw a detection zone on the video.

- Click the dots on the frame of the detection zone, and then drag to adjust its range.
- Click min or max to set the minimum size or maximum size of the face detection zone. The system triggers an alarm only when the size of detected target is between the maximum size and the minimum size.

Step 6 Select the snapshot mode and then set the parameters.

- **Optimized** : Capture the clearest face image within the configured period after the camera detects a face.
- **Quality Priority** : Capture face images only when the quality of the detected face exceeds the threshold.

Figure 6-48 Snapshot mode

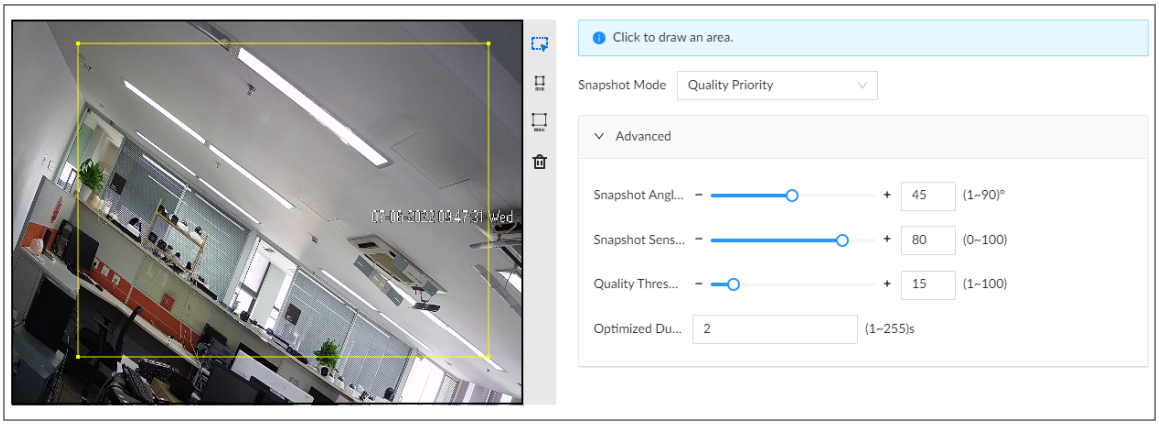


Table 6-15 Parameters of snapshot mode

Parameter	Description
Snapshot Angle Filter	Set snapshot angle to be filtered during face detection.
Snapshot Sensitivity	Set snapshot sensitivity during the face detection. The higher the sensitivity, the easier for the system to detect a face.
Quality Threshold	When the snapshot mode is **Quality Priority**, the system detects face attributes only when the quality of captured face image exceeds the configured threshold.
Optimized Duration	Set the period during which the system captures the clearest face image after the camera detects a face.

Step 7 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. You can also add a new schedule.

Step 8 Click **Select** next to **Event Linkage** to set alarm actions.

Step 9 Click **Save**.

6.6.5.3 Configuring Local Face Database

You can create local face databases on the Device to manage face images for face comparison (by Recorder). For details, see "6.6.3.4 Configuring Local Face Database".

6.6.5.4 Configuring Face Recognition (by Recorder)

Configure face recognition rules. For details, see "6.6.3.5 Configuring Face Recognition (by Recorder)".

6.6.5.5 Live View

You can view real-time face comparison images. For details, see "6.6.2.5 Live View of Face Comparison".

6.6.5.6 Face Search

You can search face records by attributes or by image, and then export the search results. For details, see "6.5.4 Face Search".

6.6.6 Video Metadata + Face Comparison by Recorder

For scenes that prioritize the accuracy of face comparison, we recommend the combination of face detection and face comparison. Video metadata is not an ideal option for face comparison in such scenes.

6.6.6.1 Configuration Procedure

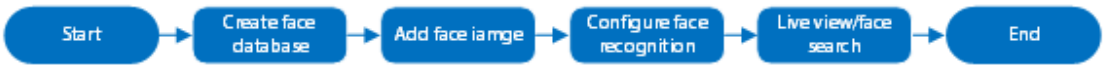
Figure 6-49 Configure video metadata (AI by camera)



Figure 6-50 Configure video metadata (AI by recorder)



Figure 6-51 Configure face recognition (AI by recorder)



6.6.6.2 Enabling the Smart Plan

To use AI by Camera, you need to enable the corresponding smart plan first. For details, see "6.5.1 Enabling the Smart Plan".

6.6.6.3 Configuring Video Metadata

The Device supports metadata (AI by Camera or by Recorder). For details, see "6.7.2 Configuring Video Metadata".

6.6.6.4 Configuring Face Recognition (by Recorder)

Configure face recognition rules. For details, see "6.6.3.5 Configuring Face Recognition (by Recorder)".

6.6.6.5 Live View

You can view real-time face comparison images. For details, see "6.6.2.5 Live View of Face Comparison".

6.6.6.6 Face Search

You can search face records by attributes or by image, and then export the search results. For details, see "6.5.4 Face Search".

6.7 Video Metadata

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

6.7.1 Enabling the Smart Plan

To use AI by Camera, you need to enable the corresponding smart plan first. For details, see "6.5.1 Enabling the Smart Plan".

6.7.2 Configuring Video Metadata

After enabling video metadata, the Device links the current remote device to record video when an alarm is triggered. You cannot set other linkage actions for video metadata when AI by Camera is used. This section uses video metadata (AI by Recorder) as an example.

6.7.2.1 Rule 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 a remote device on the device tree, and then select **Smart Plan** > **Video Metadata**.

Step 4 Configure video metadata.

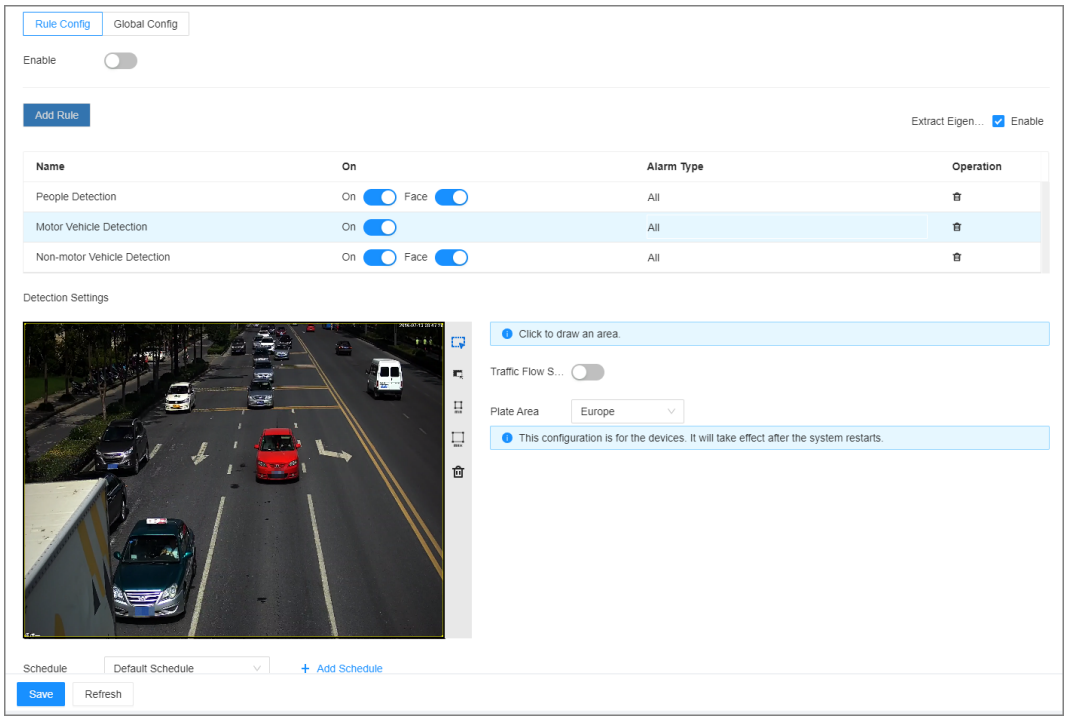
- AI by Camera.

  1. Click **AI by Camera**, and then click to enable the function.
  2. Click next to **On** to enable people detection, motor vehicle detection and non-motor vehicle detection.

- AI by Recorder.

  1. Select **Rule Config** tab, and then click to enable this function.
  2. Select **Enable** next to **Extract Eigenvector** to enable eigenvector extraction, and then the Device can extract features of human, vehicles and non-motor vehicles and display them on the live view. The search by image function for video metadata is available only when feature vector extraction is enabled.
  3. Click next to **On** to enable people detection, motor vehicle detection and non-motor vehicle detection.
     - ◇ People detection: Support face detection and people flow statistics.
     - ◇ Motor vehicle detection: Support traffic flow statistics and plate area selection. After you configured the plate area, the system could recognize the plate in the selected region and display the information in live page.
     - ◇ Non-motor vehicle detection: Support traffic flow statistics.

Figure 6-52 Rule configuration



  4. Click **AI Attributes** on the upper-right corner to configure the attributes, and then select the alarm type.
     - ◇ **All** : An alarm is triggered when a target is detected.

- **Match Attributes Alarm** : An alarm is triggered when the detected target matches the defined attributes.
- **Mismatch Attributes Alarm** : An alarm is triggered when the detected target does not match the defined attributes.

5. Click to draw a detection zone on the video.
   - Click the dots on the frame of the detection zone, and then drag to adjust its range.
   - Click to draw an exclusion area. The Device does not detect targets within the excluded area.
   - Click or to set the minimum size or maximum size of the detection zone. The system triggers an alarm only when the size of the detected target is between the maximum size and the minimum size.

Step 5 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 6 Click **Select** next to **Event Linkage** to set alarm actions.

Step 7 Click **Save**.

6.7.2.2 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 a remote device on the device tree, and then select **Smart Plan** > **Video Metadata**.

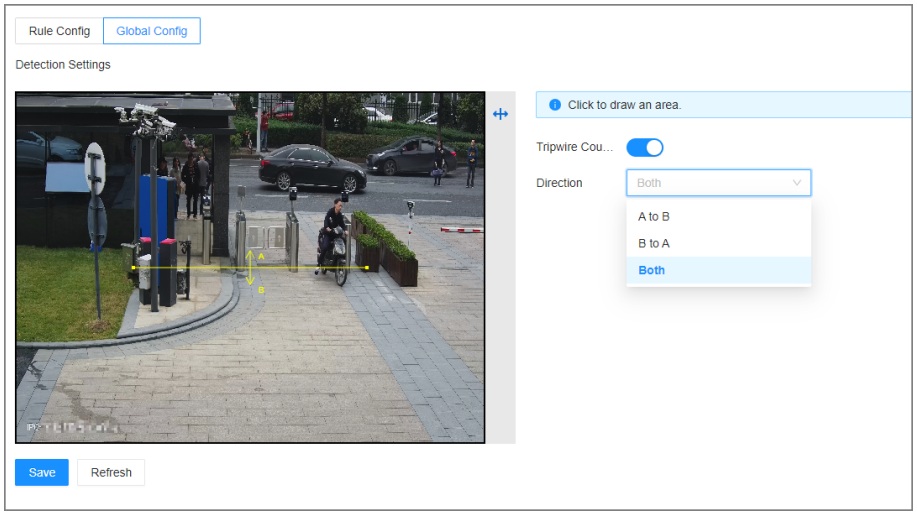
Step 4 Select **AI by Recorder** tab, and then select **Global Config**.

Step 5 Click next to **Tripwire counting** to enable this function.

Step 6 Select the detection from the drop-down list.

Step 7 Click **Save**.

Figure 6-53 Global config



6.7.3 Live View of Video Metadata

View the detection results of face, people, motor vehicle and non-motor vehicle under the **Live** tab.

6.7.3.1 Setting Attribute Display

Configure the display rule of video metadata detection results.

Prerequisites

Before using this function, make sure that view has been created.

Procedure

Step 1 Log in to the PC client.

Step 2 Under the **Live** tab, open a view window.

Step 3 Click , and then select the **Human** tab.

Step 4 Enable **Target Box Overlay**.

After it is enabled, when the system detects a target, a box will appear on the target.

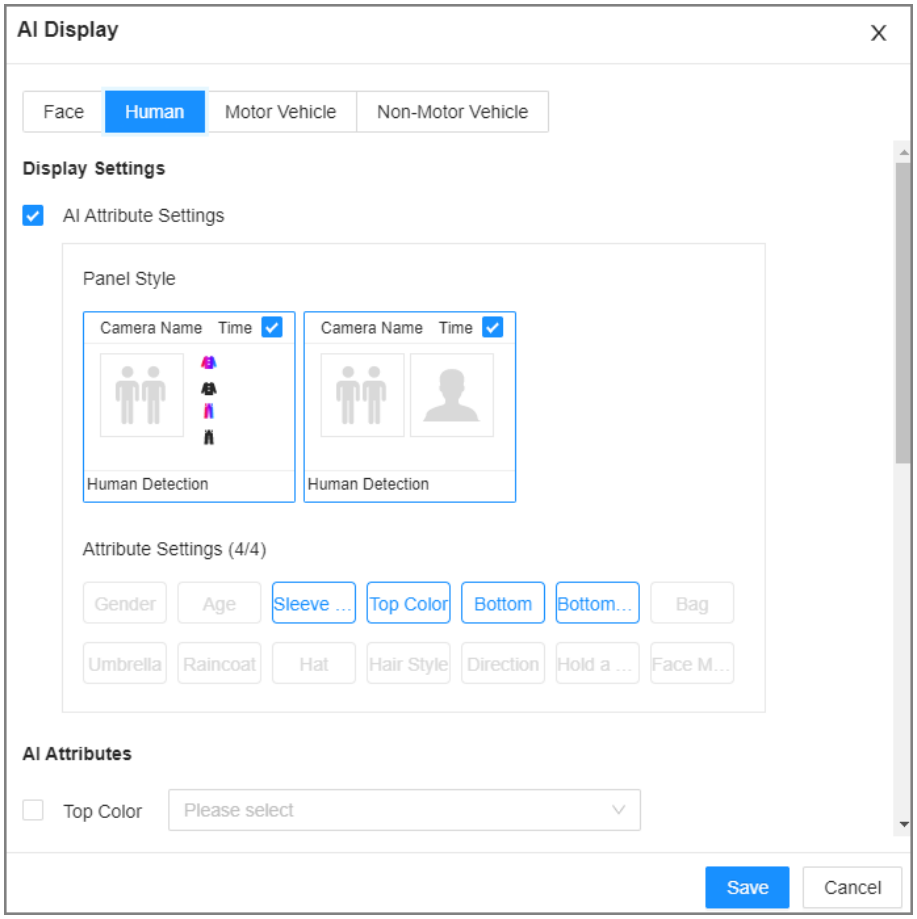
Step 5 Configure AI attributes settings.

With **AI Attributes Settings** enabled by default, when the system detects a target, a features panel appears on the live video. You can configure the style of the features panel and the attributes that you want to display.

1. Select the panel styles.
2. Select the attributes that you want to display.
   - You can select up to 4 attributes.
   - 4 attributes have been selected by default. To select other attributes, cancel the selected attributes, and then select the ones you need.
3. On the **AI Attributes** section, select the attribute groups for video metadata.

   Each attribute is broken down into more specific groups. For example, you can select **Male** , **Female** or **Unknown** for **Gender**.

Figure 6-54 Attribute display



Step 6 Click **Save**.

6.7.3.2 Live View

Log in to the PC client, and then under the **Live** tab, open a view window. The video image of the view is displayed.

- The target box is displayed in real-time in the video image. Different detection targets correspond to different colors of target boxes.
- You can view the statistics on the detected targets at the upper-right corner of the **Live** page.
  - : face.
  - : human.
  - : motor vehicle.
  - : non-motor vehicle.
- Features panels are displayed on the right side of the **Live** page.

  Point to a features panel, and then the icons are displayed.

Table 6-16 Management of detection results

Icon	Operation
	Use this image to search all channels for similar records.
	Download the snapshot and related video. When operating on the local interface, you need to insert a USB storage device into the Device.
	Click the icon or double-click the record to play back the 10 seconds of video before and after the snapshot.
	Add the detected plate information to the plate database, or add the detected face to the face database.

6.7.4 AI Search

You can search for video metadata detection records.

6.7.4.1 Human Search

Search for human detection results.

6.7.4.1.1 Searching by Attributes

Procedure

Step 1 Log in to the PC client.

Step 2 Click on the upper-right corner of the **Live** page, or select **AI Search** on the home page.

Step 3 Select **Human Search** > **Search by Attributes**.

Step 4 Select one or more remote devices, and then set **Event Type** to **Human Detection**.

Step 5 Set human attributes and search period.

Click to select a color. indicates all colors.

Step 6 Select an alarm type.

- **Match Attributes Alarm** : Search for alarms triggered when the detected target matches the defined attributes.
- **Mismatch Attributes Alarm** : Search for alarms triggered when the detected target does not match the defined attributes.

Step 7 Click **Search**.

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

Related Operations

After the query, the system displays the query results in the form of panels. Click a panel, and then the system will show operation icons. For details, see Table 6-4 .

- When a face image is captured, the panel displays the human body detection image and the captured face image.
- When no face image is captured, the panel displays the human body detection image and human body detection attributes.

6.7.4.1.2 Searching by Image

Filter out information whose similarity with the given picture reaches the set value. For details, see "6.5.4.2 Searching by Image".

6.7.4.1.3 Viewing Tracks

Add a digital map, and then bind the channels to actual locations on the map. If the same person is detected by multiple channels, the system can automatically draw connecting lines on the map to generate the movement path for route analysis. For details, see "6.5.4.3 Viewing tracks".

6.7.4.2 Vehicle Search

6.7.4.2.1 Searching by Attributes

Search for vehicle detection results.

Procedure

Step 1 Log in to the PC client.

Step 2 Click on the upper-right corner of the **Live** page, or select **AI Search** on the home page.

Step 3 Select **Motor Vehicle Search**, and then select one or more remote devices.

Step 4 Under the **Attribute** tab, set **Event Type** to **Motor Vehicle Detection**.

Step 5 Select an alarm type.

- **Match Attributes Alarm** : Search for alarms triggered when the detected target matches the defined attributes.
- **Mismatch Attributes Alarm** : Search for alarms triggered when the detected target does not match the defined attributes.

Step 6 Set vehicle attributes and search period.

Click to select a color. indicates all colors.

Step 7 Click **Search**.

If license plate is detected, both the scene of the vehicle and the license plate will be displayed.

Related Operations

Point to a record, and then the following icons are displayed.

Table 6-17 Management of search results

Icon	Operation
	Click the icon to select the record. To select all the records at a time, select the checkbox next to **Select All**.

Icon	Operation
	Export the snapshot, video and video player. To export in batches, select multiple records, and then click **Export** to export snapshots, videos or Excel files. After you set alarm linkage snapshot, the system exports detected images and panoramic images at the time of snapshot.
	Click the icon or double-click the record to play back the 10 seconds of video before and after the snapshot.
	Add this image to the plate database.

6.7.4.2.2 Search by Image

Filter out information whose similarity with the given picture reaches the set value. For details, see "6.5.4.2 Searching by Image".

6.7.4.2.3 Viewing Tracks

Add a digital map, and then bind the channels to actual locations on the map. If the same person is detected by multiple channels, the system can automatically draw connecting lines on the map to generate the movement path for route analysis. For details, see "6.5.4.3 Viewing tracks".

6.7.4.3 Non-motor Vehicle Search

Search for non-motor vehicle detection results.

Procedure

Step 1 Log in to the PC client.

Step 2 Click on the upper-right corner of the **Live** page, or select **AI Search** on the home page.

Step 3 Select **Search by Non-Motor Vehicle**, and then select one or more remote devices.

Step 4 Set **Event Type** to **Non-motor Vehicle Detection**.

Step 5 Set vehicle attributes and search period.

Click to select a color. indicates all colors.

Step 6 Click **Search**.

Related Operations

Point to a record, and then the following icons are displayed.

Table 6-18 Management of search results

Icon	Operation
	Click the icon to select the record. To select all the records at a time, select the checkbox next to **Select All**.

Icon	Operation
	Use this image to search all channels for similar records.
	Export the snapshot, video and video player. To export in batches, select multiple records, and then click **Export** to export snapshots, videos or excel. After you set alarm linkage snapshot, the system exports detected images and panoramic images at the time of snapshot.
	Click the icon or double-click the record to play back the 10 seconds of video before and after the snapshot.
	Add this image to the face database.

6.7.5 Viewing AI Report

Procedure

Step 1 Log in to the PC client.

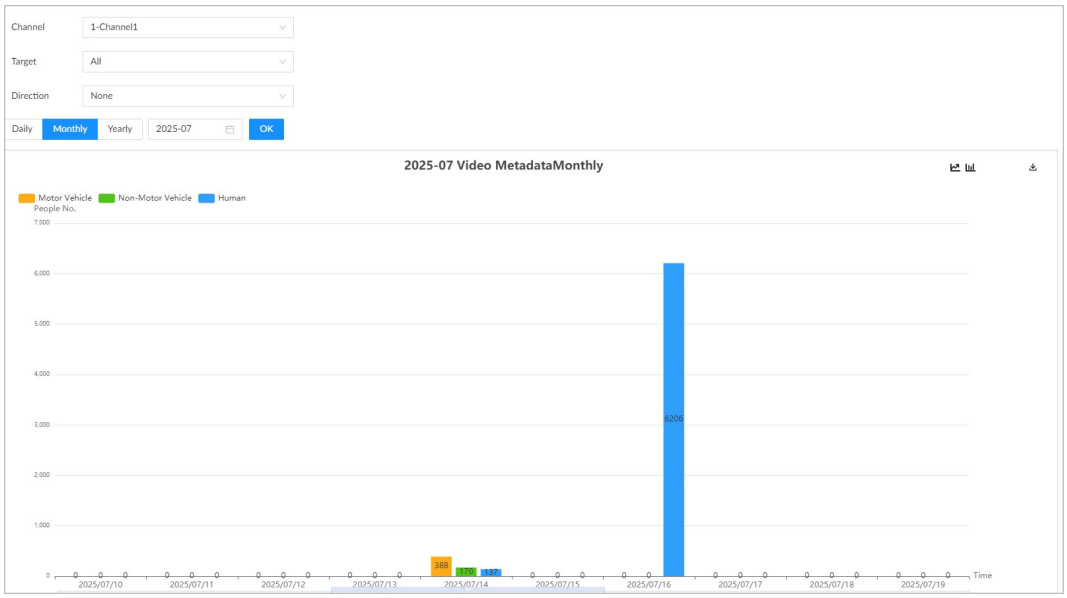
Step 2 On the home page, select **AI Application** > **AI Report** > **Video Metadata**.

Step 3 Select the channel and direction.

Step 4 Select a period type from **Daily** , **Monthly**, and **Yearly**, and then set the corresponding date, month or year.

Step 5 Click **OK**. The report is displayed.

Figure 6-55 AI report



Related Operations

- Point to the report, and then the report shows the details at that time point.
- Drag the gray scroll bar under the ordinate to view the statistics for different time periods.
- Click to view the line chart.

- Click to view the bar chart.
- Click to export the report.

6.8 IVS

The IVS feature includes a number of behavior detections such as fence-crossing, intrusion, tripwire, parking, crowd gathering, missing object, abandoned object, and loitering.

Some models only support some IVS functions by Recorder.

6.8.1 Enabling the Smart Plan

To use AI by Camera, you need to enable the corresponding smart plan first. For details, see "6.5.1 Enabling the Smart Plan".

6.8.2 Configuring IVS

6.8.2.1 Global Configuration

Configure global rules of IVS.

Global configuration is needed only when AI by Camera is used.

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 a remote device on the device tree, and then select **Smart Plan** > **IVS**.

Step 4 Select **AI By Camera** > **Global Config**.

Step 5 Drag to adjust sensitivity.

Step 6 Calibrate horizontal and vertical scales.

1. Click to draw an area.
2. Click to draw three vertical lines, enter the actual length, and then click **Calibration Verification**.
3. Click to draw a horizontal line, enter the actual length, and then click **Calibration Verification**.

Step 7 Click **Save**.

6.8.2.2 Rule Configuration

Configure IVS rules. IVS functions are different between AI by Camera and AI by Recorder. IVS functions with AI by Camera include crossing fence, tripwire, intrusion, abandoned object, parking

detection, people gathering, object removed, loitering, stay and climbing. Different cameras support different functions.

Table 6-19 IVS functions description

Functions	Description	Scene
Tripwire	When the target crosses tripwire from the defined motion direction, an alarm is triggered, and then the system performs configured alarm linkages.	Scenes with sparse targets and no occlusion among targets, such as the perimeter protection of unattended area.
Intrusion	When the target enters, leaves, or appears in the detection area, an alarm is triggered, and the system performs configured alarm linkages.	
Abandoned Object	When an object is abandoned in the detection area over the configured time, an alarm is triggered, and then the system performs configured alarm linkages.	Scenes with sparse targets and without obvious and frequent light change. Simple scene in the detection area is recommended. ● Missed alarm might increase in the scenes with dense targets, frequent occlusion, and people staying. ● In scenes with complex foreground and background, false alarm might be triggered for abandoned or missing object.
Missing Object	When an object is taken out of the detection area for more than the defined period, an alarm is triggered, and then the system performs configured alarm linkages.	
Fast Moving	When the target moves fast in the detection area, an alarm is triggered, and then the system performs configured alarm linkages.	Scene with sparse targets and less occlusion. The camera should be installed right above the monitoring area. The light direction should be vertical to the motion direction.
Parking Detection	When the vehicle stays in the detection area longer than the configured duration, an alarm is triggered, and then the system performs configured alarm linkages.	Road monitoring and traffic management.
Crowd Gathering	When the crowd gathers or the crowd density is large, an alarm is triggered, and then the system performs configured alarm linkages.	Scenes with medium or long distance, such as outdoor plaza, government entrance, station entrance and exit. It is not suitable for short-distance view analysis.
Crossing Fence	When the target crosses the warning line toward the defined direction, an alarm is triggered, and then the system performs configured alarm linkages.	Scenes with median strips such as roads, and airports.

Functions	Description	Scene
Loitering	When the target loiters over the shortest alarm period, an alarm is triggered, and then the system performs configured alarm linkages. Set the **Repeat Alarm Time**, when the alarm is triggered and this state lasts for repetitive alarm time, the alarm will be triggered again.	Scenes such as park and hall.
Stay	When the target stays in the detection area longer than the defined duration, an alarm is triggered, and then the system performs configured alarm linkages. Set the **Repeat Alarm Time**, when the alarm is triggered and this state lasts for repetitive alarm time, the alarm will be triggered again.	
Climbing	When the target climbs and reaches the configured line, an alarm is triggered, and then the system performs configured alarm linkages.	Scenes such as wall and fence of the park.

This section uses the configuration of tripwire as the example.

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 a remote device on the device tree, and then select **Smart Plan** > **IVS**.

Step 4 Set tripwire rules.

- AI by Camera.
  1. Select **AI By Camera** > **Rule Config**.
  2. Click **Add Rule** , and then select **Tripwire**.
  3. Click  to enable the detection rule.
  4. Click  to edit the tripwire line.
     - Click the dots on the 2 ends of the line to adjust its length.
     - Drag the line to adjust its position.
     - Select a direction from **A to B** , **B to A**, and **Both**. An alarm will be triggered only when the target crosses the line in the designated direction.
  5. Click  or  to set minimum size or maximum size of the detection target.

     The system triggers an alarm only when the detected target size is between the maximum size and the minimum size.

- AI by Recorder.

  1. Click **AI by Recorder**.
  2. Click  to enable IVS.
  3. Click **Add Rule** , and then select **Tripwire**.
  4. Click  to enable the detection rule.
  5. Click  to edit the tripwire line.
     - Click the dots on the 2 ends of the line to adjust its length.
     - Drag the line to adjust its position.
     - Select a direction from **A to B** , **B to A**, and **Both**. An alarm will be triggered only when the target crosses the line in the designated direction.
  6. Click  or  to set minimum size or maximum size of the detection target.

     The system triggers an alarm only when the detected target size is between the maximum size and the minimum size.

Step 5 Configure target filter and sensitivity.

After setting target filter and the target type, when the system detects a target, a rule box will appear beside the target on the video.

1. Click  to enable the function.
2. Select a recognition type.
   - : Human.
   - : Vehicle.
   - : Animal.
3. Configure sensitivity.

   The higher the sensitivity, the easier to trigger tripwire alarm, but meanwhile the higher probability of false alarm.

   Sensitivity is available when AI by Recorder is used, or when AI by Camera is used and the camera supports this function.

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**.

- Repeat Step 4 through Step 7 to add multiple detection rules.
- You can add up to 10 detection rules for a remote device.

6.8.3 Live View of IVS

Under the **Live** tab, view the real-time IVS results.

6.8.3.1 Setting Attribute Display

Configure the display rule of IVS detection results.

Prerequisites

Before using this function, make sure that view has been created.

Procedure

Step 1 Log in to the PC client.

Step 2 Under the **Live** tab, open a view window.

Step 3 Click and then select the **Human** , and **Motor Vehicle** tab.

Figure 6-56 Human

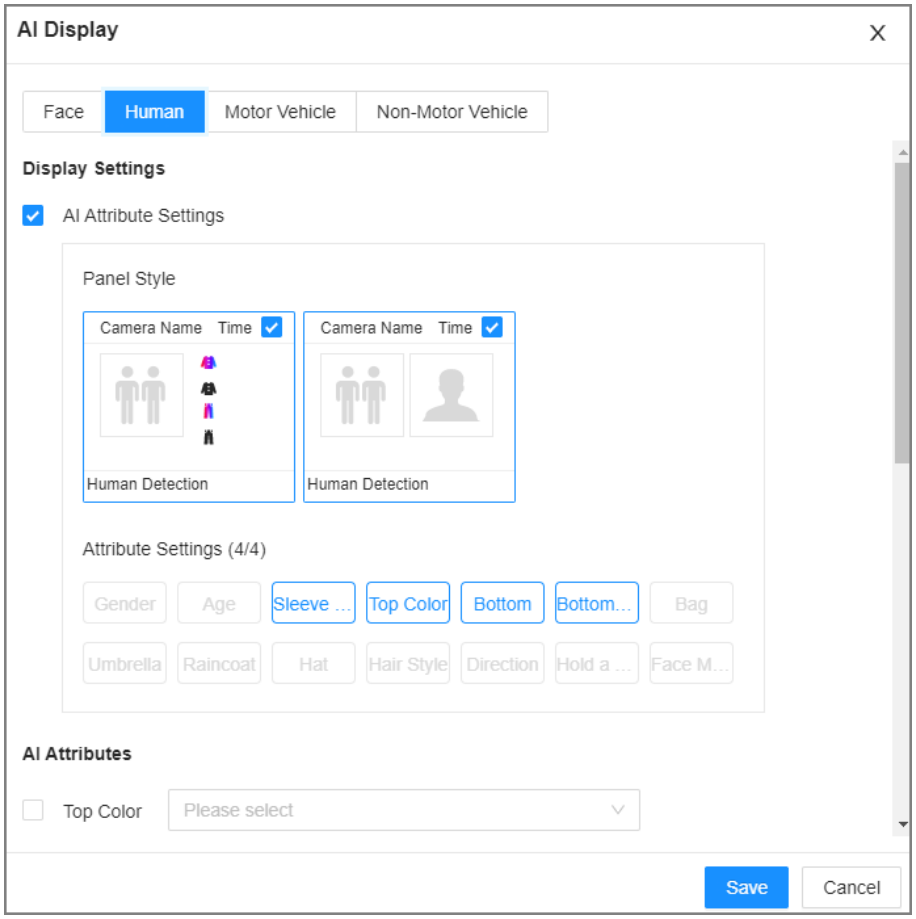
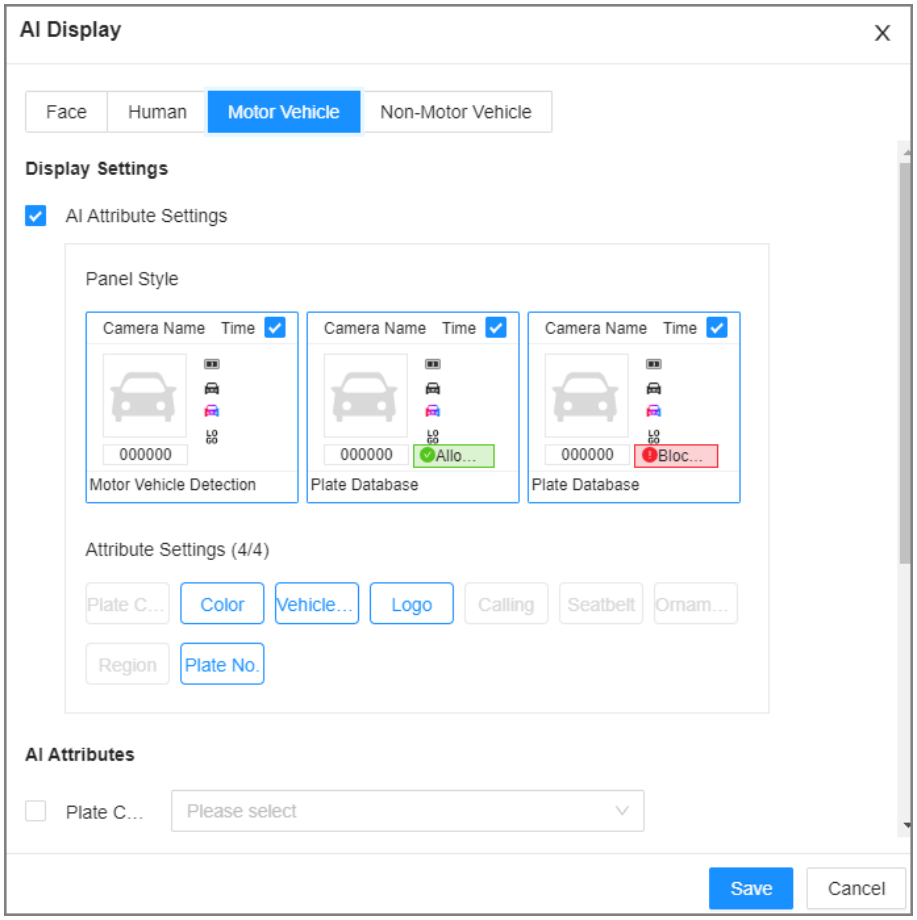


Figure 6-57 Motor vehicle



Step 4 Configure AI attributes settings.

With **AI Attributes Settings** enabled by default, when the system detects a target, a features panel appears on the live video. You can configure the style of the features panel and the attributes that you want to display.

1. Select the panel styles.
2. Select the attributes that you want to display.
   - You can select up to 4 attributes.
   - 4 attributes have been selected by default. To select other attributes, cancel the selected attributes, and then select the ones you need.
3. On the **AI Attributes** section, select the attribute groups for video metadata.

   Each attribute is broken down into more specific groups. For example, you can select **Male** , **Female** or **Unknown** for **Gender**.

Step 5 Click **Save**.

6.8.3.2 Live View

Log in to the PC client, and then under the **Live** tab, open a view window. The video image of the view is displayed.

- When a target triggers tripwire or intrusion rule, the line or region frame in the view flickers in red.
- After setting target filter, when the system detects a person or vehicle, a rule box will appear beside the person and vehicle in the view.

- You can view the detection statistics on the upper-righter corner of the **Live** page.

Figure 6-58 Detection statistics



- Features panels are displayed on the right side of the video image.

  Point to the features panel, and the icons are displayed.

  - : Click the icon or double-click the record to play back the 10 seconds of video before and after the snapshot.
  - : Use this image to search all channels for similar records.
  - Point to a record, and then click to export the snapshot and video to the specified storage path.

    Make sure that USB storage device is connected during local operation.

6.8.4 IVS Search

Search for IVS records.

Procedure

Step 1 Log in to the PC client.

Step 2 Click on the upper-right corner of the **Live** page, or select **AI Search** on the home page.

Step 3 Select **IVS**, and then select one or more remote devices.

Step 4 Set the event type, effective target and search period.

Step 5 Click **Search**.

Related Operations

Point to a record, and then the following icons are displayed.

Table 6-20 Management of search results

Icon	Operation
/	Click the icon to configure the sorting method.
	Click the icon to select the record. To select all the records at a time, select the checkbox next to **Select All**.
	Export the snapshot, video and video player. To export in batches, select multiple records, and then click **Export** to export snapshots, videos or excel. After you set alarm linkage snapshot, the system exports detected images and panoramic images at the time of snapshot.

Icon	Operation
	Click the icon or double-click the record to play back the 10 seconds of video before and after the snapshot.

6.9 Call Alarm

An alarm is triggered when the system detects a person calling. To configure call alarm, set call detection rules for the visible light channel of a thermal camera.

Call alarm is only available with AI by Camera.

6.9.1 Enabling the Smart Plan

To use AI by Camera, you need to enable the corresponding smart plan first.

6.9.2 Configuring Call Alarm

Configure call alarm rules. The call alarm is only available with thermal cameras.

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 On the device tree, select the visible light channel of a thermal camera.

Step 4 Select **Smart Plan** > **Call Detection**.

Step 5 Click  to enable the function.

Step 6 Click  and then drag the corners to adjust the detection zone.

Step 7 Set the sensitivity and the first alarm time.

- Sensitivity: The higher the sensitivity, the easier the call action is detected but meanwhile the higher probability of false alarms.
- First alarm time: When the system detects that the target is calling for a certain duration, it identifies the action as a phone call.

Step 8 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 9 Click **Select** next to **Event Linkage** to set alarm actions.

Step 10 Click **Save**.

6.9.3 Live View of Call Alarm

Log in to the PC client, and then under the **Live** tab, open a view window. The video image of the view is displayed. When an alarm is triggered, the detection zone flashes red.

6.9.4 Call Alarm Search

Search for videos or images of call alarm.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, click **Search**.

Step 3 Select one or more devices.

Step 4 You can search for the videos or images of call detection.

- Videos
  1. Under the **Record** tab, select **Thermal** as video type.
  2. Select **Call Detection** as detection type.
  3. Select a stream type.
  4. Set the search period.
  5. Click **Search**.
- Images
  1. Under the **Picture** tab, select **Thermal** as snapshot type.
  2. Select **Call Detection** as detection type.
  3. Set the search period.
  4. Click **Search**.

6.10 High-Rise Littering

6.10.1 Live View

Log in to the PC client, and then under the **Live** tab, open a view window that contains high toss video. When an alarm is triggered, the live view displays the motion track, and the feature panel is displayed on the right side of the video image.

Figure 6-59 Live view



6.10.2 High-Rise Littering Search

Procedure

Step 1 Log in to the PC client.

Step 2 Click on the upper-right corner of the **Live** page, or select **AI Search** on the home page.

Step 3 Select **High-rise Littering** tab.

Step 4 Select one or more remote devices, configure the time, and then click **Search**.

Step 5 Double click the select image or click to check the playback (10 seconds of video before and after the alarm triggered).

6.11 Smart Application Orchestration

You can flexibly combine multiple algorithms in serial or parallel order through the smart combination feature to adapt to the detection needs of different complex scenarios. For example, to detect whether there is smoke or fire in an area when no one is present, the smart combination feature orchestrates the person detection and smoke/fire detection algorithms to achieve the monitoring purpose.

Prerequisites

Select **Algorithm** > **Algorithm Management** > **AI Module**, and then select **Intelligent Analysis Engine** as the smart module type.

Procedure

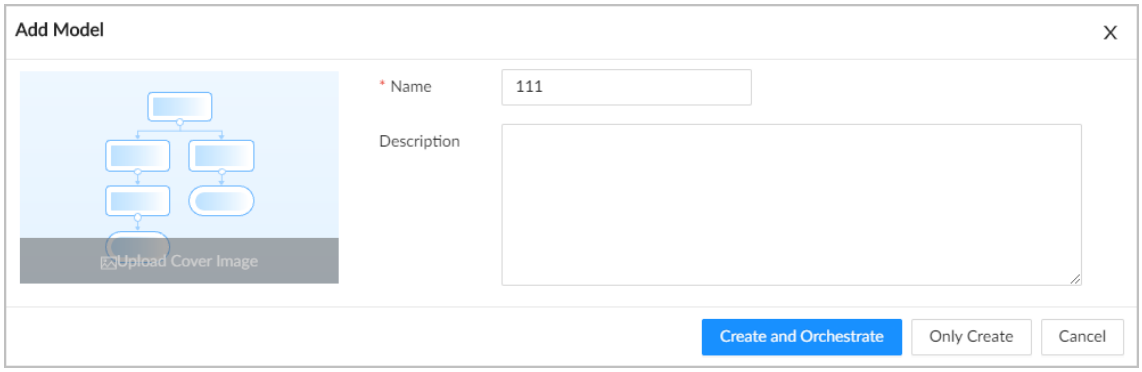
Step 1 Log in to the PC client.

Step 2 Select **Algorithm** > **AI Application Orchestration** from the configuration list, or click to select **Algorithm** > **AI Application Orchestration**.

Step 3 Click **Create** to create the smart combination.

1. Enter the name and description of the combination.
2. Click **Upload Cover Image** , select an image locally and click **Open** to open it.
3. Click **Create and Orchestrate** or **Only Create**.
   - Select **Create and Orchestrate**, and then you can go directly to the orchestration page.
   - Select **Only Create**, the page displays the orchestration list, and then click of the lower-right corner of the smart combination to enter the orchestration page.

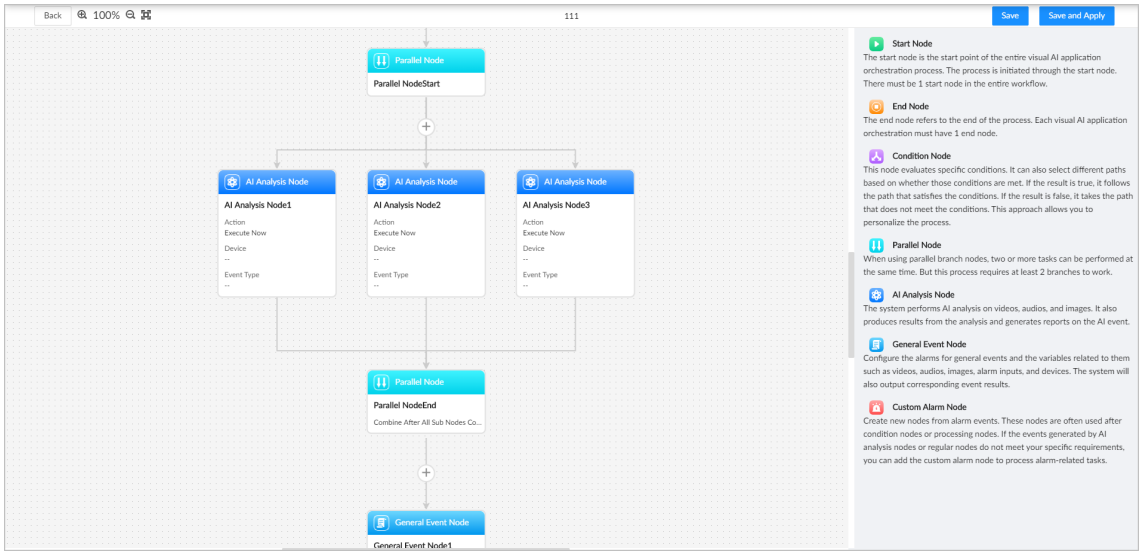
Figure 6-60 Create the combination



Step 4 Start orchestrating the algorithm combination.

You can learn about the functions of various nodes on the right side of the orchestration page. Among them, the **Start Node** and **End Node** are added to the combination by default.

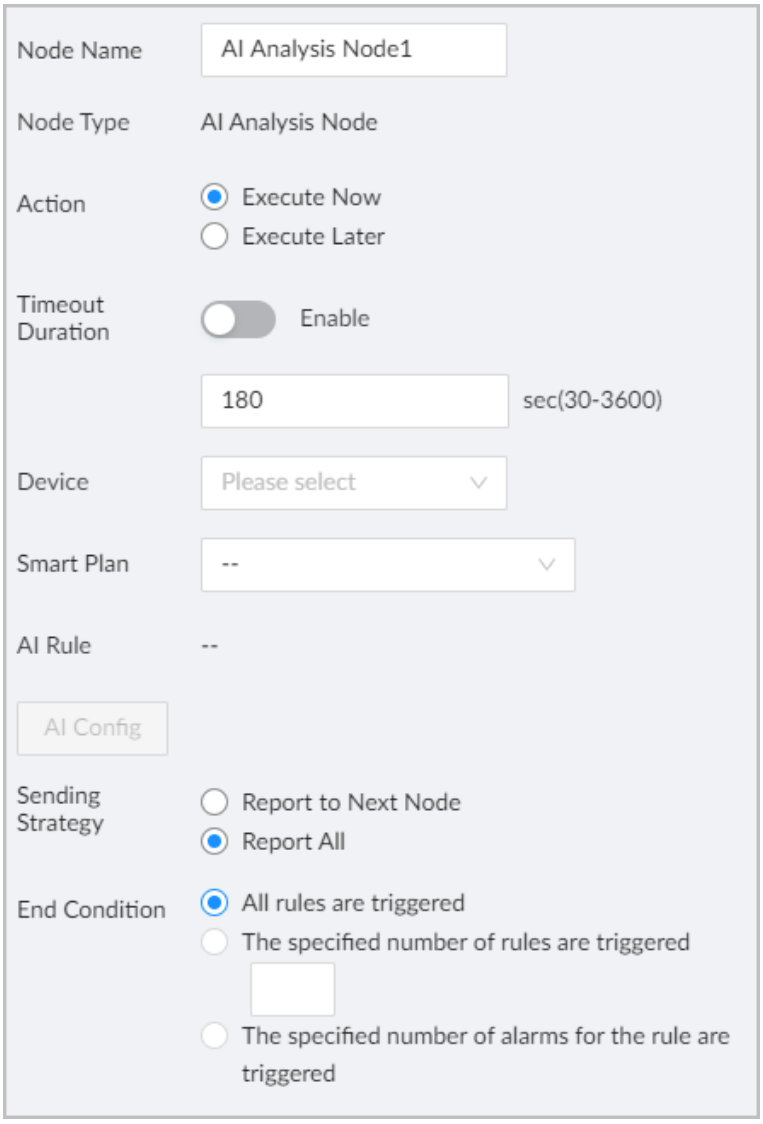
Figure 6-61 Orchestrate a combination



The operation methods of 7 nodes are as follows. Refer to the table below for parameter description.

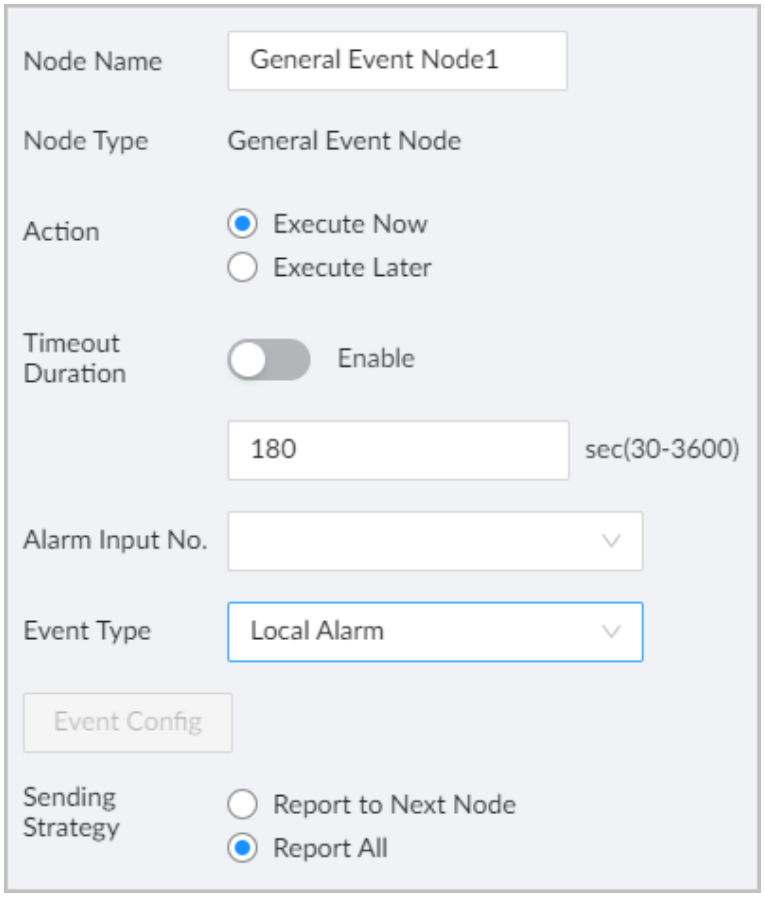
- **AI Analysis Node** : Select and click **AI Analysis Node**, and then set the parameters on the right side of the page.

Figure 6-62 AI analysis node



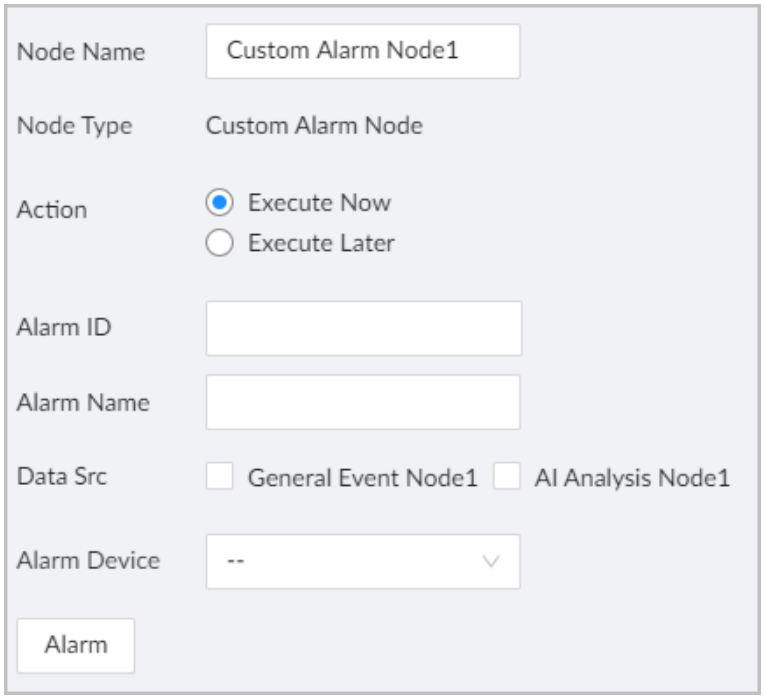
- **General Event Node** : Select and click **General Event Node**, and then set the parameters on the right side of the page.

Figure 6-63 General event node



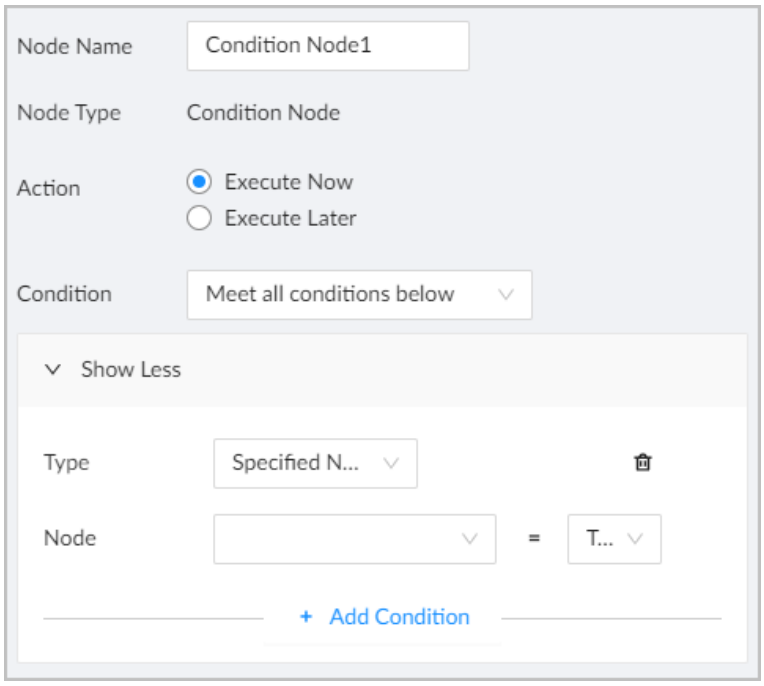
- **Custom Alarm Node** : Select and click **Custom Alarm Node**, and then set the parameters on the right side of the page.

Figure 6-64 Custom alarm node



- **Condition Node** : Select and click **Condition Node**, and then set the parameters on the right side of the page. Click on **Y** or **N** path as needed to add the new nodes.

Figure 6-65 Condition node



- **Parallel Node**.
  1. Select and click **Parallel Node**, and then set the node name on the right side of the page.

     A maximum of 2 groups of parallel nodes can be added.
  2. Click between **Paralled NodeStart** and **Paralled NodeEnd**, and then select **AI Analysis Node** or **General Event Node**.

     Repeat this operation to add multiple **Parallel Node** or **General Event Node**. The system will pop up a prompt when the number exceeds the upper limit.
  3. Click a node, and then set the parameters on the right side of the page.

The upper-left corner of the page supports the following operations:

- Click 100% to zoom in or zoom out the orchestration canvas.
- Click to reset the orchestration canvas to 100%.

Table 6-21 Key parameter description for serial combination

Parameter	Description
Node Name	Customize node names.

Parameter	Description
Action	Choose to execute immediately or with a delay. When selecting delayed execution, a delay time needs to be set. When the task reaches this node, perform the analysis immediately or with a delay based on the configuration.
Timeout Duration	Enable the timeout and set the timeout duration. If the execution time of this node exceeds the timeout duration, stop the node and proceed to the next node.
Device Smart Plan AI Configuration Pre-algorithm Node	1. Select the channel and the desired plan type. 2. Click **AI Config**, and then proceed to the intelligent rule configuration page. 3. Click **Add Rule**, and then select the corresponding rule.  • Configuration is only supported for **AI Analysis Node**. For detailed information on intelligent rule configuration, refer to the chapters on various intelligent events. • Only partial smart plans can be configured, subject to the actual page.
Alarm Input No. Event Type Event Configuration	Select the **Alarm Input No.** and **Event Type** (local alarm), click **Event Config**, and then proceed to the event configuration page.  Configuration is only supported for **General Event Node**. For more information about the event configuration, see "8.3.4.5 Configuring Local Alarm".
Sending Strategy	Choose to report only to the next node or report to all nodes. • **Report to Next Node** : Alarm events triggered by this node will only be reported to the next node and will not be forwarded to connected devices or platforms. • **Report All** : Alarm events triggered by this node will be reported to the next node as well as connected devices and platforms.  Regardless of whether you choose to report only to the next node or report to all nodes, alarm events will be stored locally.

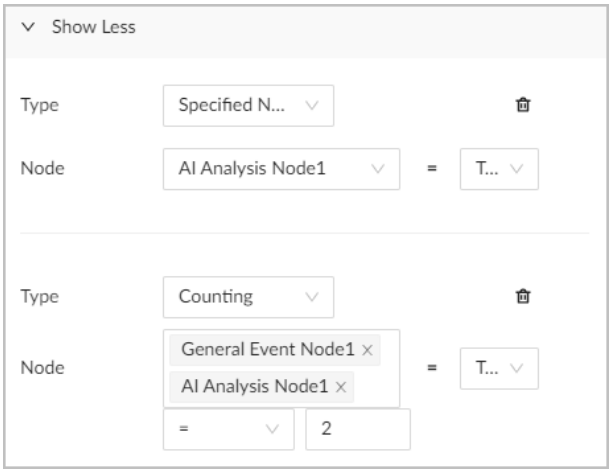
Parameter	Description
Add Condition	Select items that meet all or any of the following conditions. Click **Add Condition** to set the type and node. Support adding multiple conditions. • **Type** : Select **Specified Node** or **Counting**. When **Counting** is selected, the judgment condition is based on the triggered times of nodes. • **Node** : Select the specific node and set the result to **True** or **False**. Example 1: Select **Specified Node** as the type, choose **AI Analysis Node1** as the node, and then set this parameter to **True**. When **AI Analysis Node1** triggers an event, determine that this condition has been met. Example 2: Select **Counting** as the type, choose **AI Analysis Node1** and **General Event Node1** as the node, set this parameter to **True**, and then set the judgment condition and quantity to **=2** (indicating that 2 nodes trigger the event). When **AI Analysis Node1** and **General Event Node1** trigger events, determine that this condition has been met. 
Condition Settings	
Alarm Name	Custom alarm ID and alarm name.
Alarm ID	
Data Source	Select the node of data sources as needed. Captured images from channels of selected notes will be displayed on the live screen and AI search screen. If no data source is selected, no captured images will be shown on the live screen and AI search screen.
Alarm Device	Select the channel. Alarm capture results will pop up only when viewing the channel in the live screen.
Alarm Linkage	Click **Alarm** to set specific linkage actions, such as buzzer, log, and more.

Table 6-22 Description of specific algorithm scenarios

Dimension	Face Recognition	Text-Define Alarms
Analysis Mode	The image stream.	The image stream.

Dimension	Face Recognition	Text-Define Alarms
Analysis source	The image stream comes from the designated **Pre-algorithm Node**.	The image stream comes from the designated **Pre-algorithm Node**.
Pre-algorithm Node Requirements	The pre-algorithm node must produce a face image stream as its output.	The algorithm type of the pre-algorithm node must be consistent with the pre-algorithm type selected when creating the text-define alarms. For example, when creating a text-defined alarm, if the pre-algorithm is set to **IVS** , only intelligent nodes with the intelligent scheme of **IVS** can be selected as the **Pre-algorithm Node** for the text-define alarms' node during orchestration.

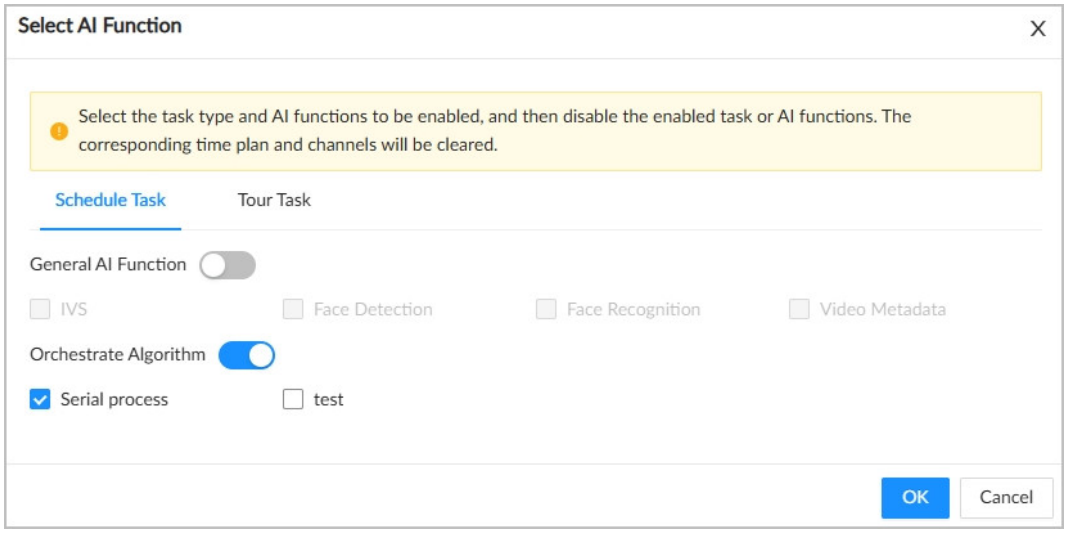
Step 5 Click **Save** or **Save and Apply**.

- Click **Save** , and then the page displays the orchestration list. Enter the smart solution page by clicking in the lower-right corner of the smart combination or clicking **Go** to go to **Smart Plan** page.
- Click **Save and Apply** to directly go to **Smart Plan** page.

Step 6 Set up task plans in the **Smart Plan** page.

1. Select the root node on the left device tree, and then select **Smart Plan** > **Smart Plan**.
2. Set the AI by Recorder mode to **Task Mode**.
3. Click **Select AI Function** , enable the **Orchestrate Algorithm** in the pop-up page, select the pre-configured algorithm combination, and then click **OK**.

Figure 6-66 Select the AI function

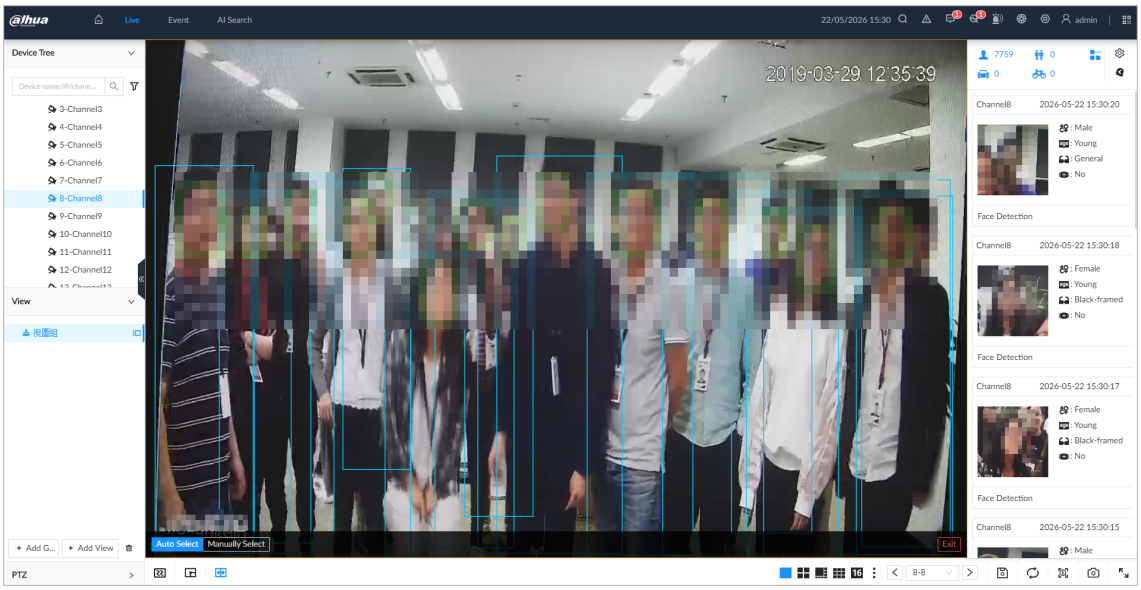


4. On the displayed smart solution, drag to select the time period for task execution.
   - Click **Edit**, set the number of runs in the pop-up page, which supports single run and unlimited options.
   - Click **Orchestrate** to go to the orchestration page and modify the orchestration configuration.
5. Click **Save**.

Results

- Enter the live page, select the orchestrated channel in the device tree, and then view the event detection results in the right panel.

Figure 6-67 Live screen



- Enter the AI search page, select **AI Application Orchestration** on the left, select the smart combination, set the query conditions, and then click **Search**.

Results can also be searched in the AI search page of the orchestrated smart events.

Related Operations

On the **Orchestration List** page, you can view the status of smart combinations. **Orchestrated** means orchestration is completed but no task plan is configured. **Applied** means the task plan is configured. **Unorchestrated** means no algorithmic orchestration has been performed.

Figure 6-68 Smart combination



6.12 Text-Defined Alarms

Deploy the algorithm for generating customized text content to the required channels to achieve intelligent detection.

Prerequisites

The text generation algorithm has been configured, and the corresponding pre-processing algorithm has been enabled.

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 a remote device on the left device tree.

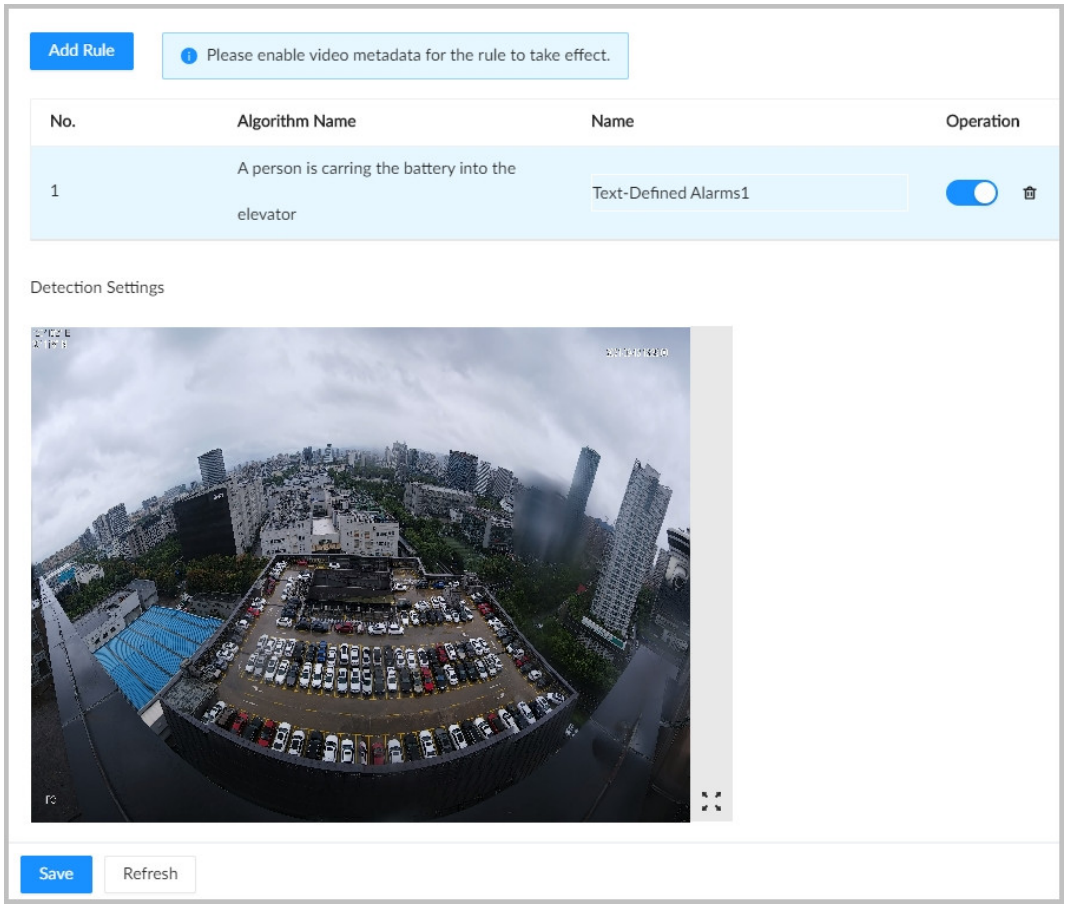
Step 4 Select **Smart Plan** > **Text-Defined Alarms** > **AI by Recorder**.

Step 5 Click **Add Rule** to select the configured text-defined algorithm.

Click **Create** , the system goes to the **Text-Defined Alarms** page quickly, and then you can add the new algorithm.

Step 6 Click of **Operation** to enable algorithm detection.

Figure 6-69 Text-defined alarms



Step 7 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 8 Click **Select** next to **Event Linkage** to set alarm actions.

Step 9 Click **Save**.

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 under the **Live** tab, you can view the live videos.

Point to the left and right edges of the video windows, and then click or to hide or display the left and right columns.

- When operating through the local page, the screen number is displayed on the screen.
- The functions of the local page and the webpage might differ. Refer to the actual page for accurate information.

Figure 7-1 Live view

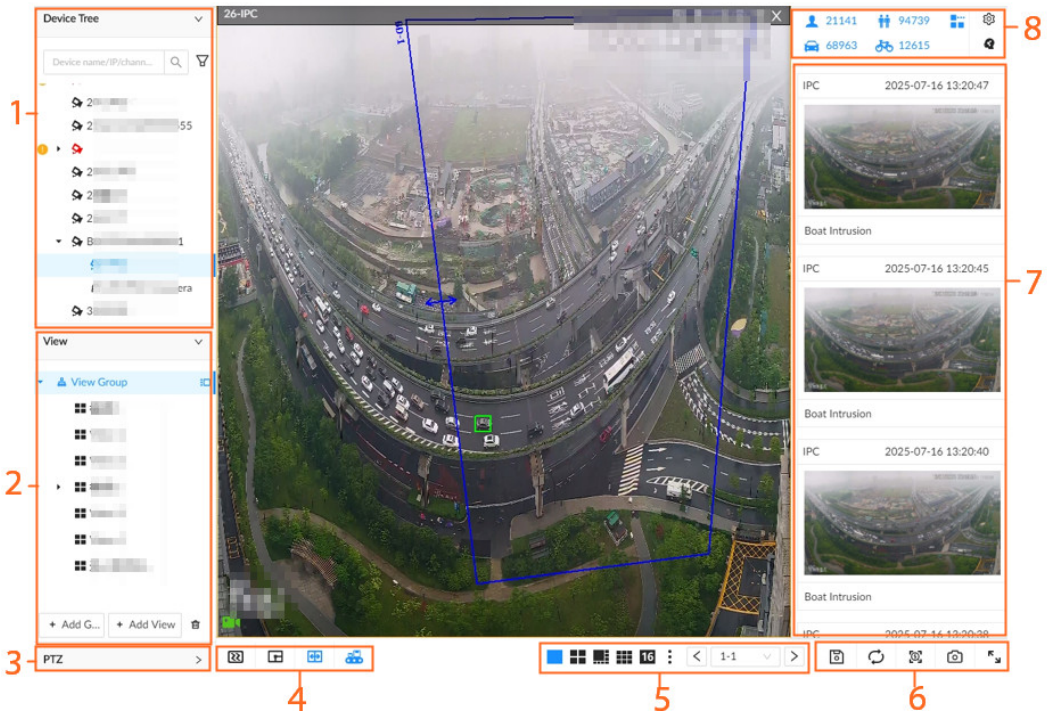


Table 7-1 Live page description

No.	Description
1	Device tree. Displays added remote devices.
2	View zone. Displays the created views and view groups.
3	PTZ control zone.

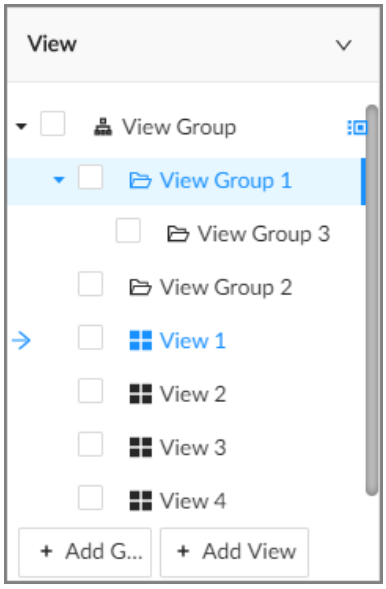
No.	Description
4	• Click : You can select **Default** , **Realtime** or **Fluent**. • Click : You can adjust the detection area and excluded area. • Click : Turn rule box display on or off. • Click : When you configure intelligent events for the conveyor belt, you can turn the visualization panel on or off to view the status of the conveyor belt.
5	Layout adjustment. • Click to set the layout. • Click or to switch the channel.
6	• : Saves the current layout as a view. • : Displays the live view in full screen. • : Starts AcuPick. • : Starts tour. • : Captures the current screen and save it locally.
7	Features panels. A features panel appears when the system detected a target according to the configured rule.
8	Detection statistics. Displays the number of detected targets. • : Face. • : Human. • : Motor vehicle. • : Non-motor vehicle. • : Set attribute display. • : Go to **AI Search**.

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.

- 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.

7.1.1.1.1 Creating a View Group

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.

7.1.1.1.2 Managing View Groups

After creating a view group, you can rename or delete the view group.

Figure 7-3 Manage view groups

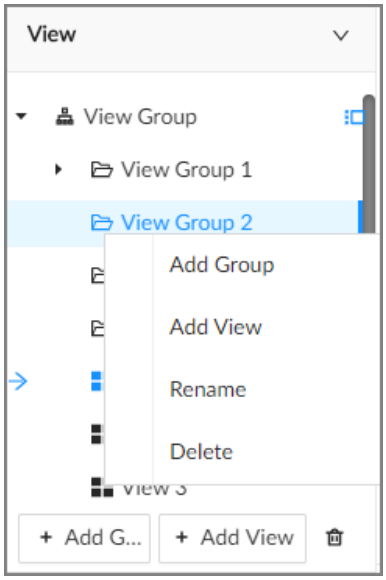


Table 7-2 View group management

Operation	Description
Rename	Right-click a view group and select **Rename**. Set view group name and click any blank space.
Delete View group	⚠ Please be advised that once you delete a view group, all views under the view group will be deleted at the same time. • Select one or more view groups, and then click 🗑. • Right-click a view group, and then click **Delete**.

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 a 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 characters.

Step 5 Click **OK**.

Related Operations

Table 7-3 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: Select a view, 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 a View

Procedure

Step 1 Log in to the PC client.

Step 2 Under the **Live** tab, right-click a view, and then click **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, click at the upper-right corner, and then click **OK**.

- Move the video windows: Drag a video window to a proper position, release the mouse, and then click **OK**.
- Change window positions: Drag a video window to another video window, and then click **OK**.

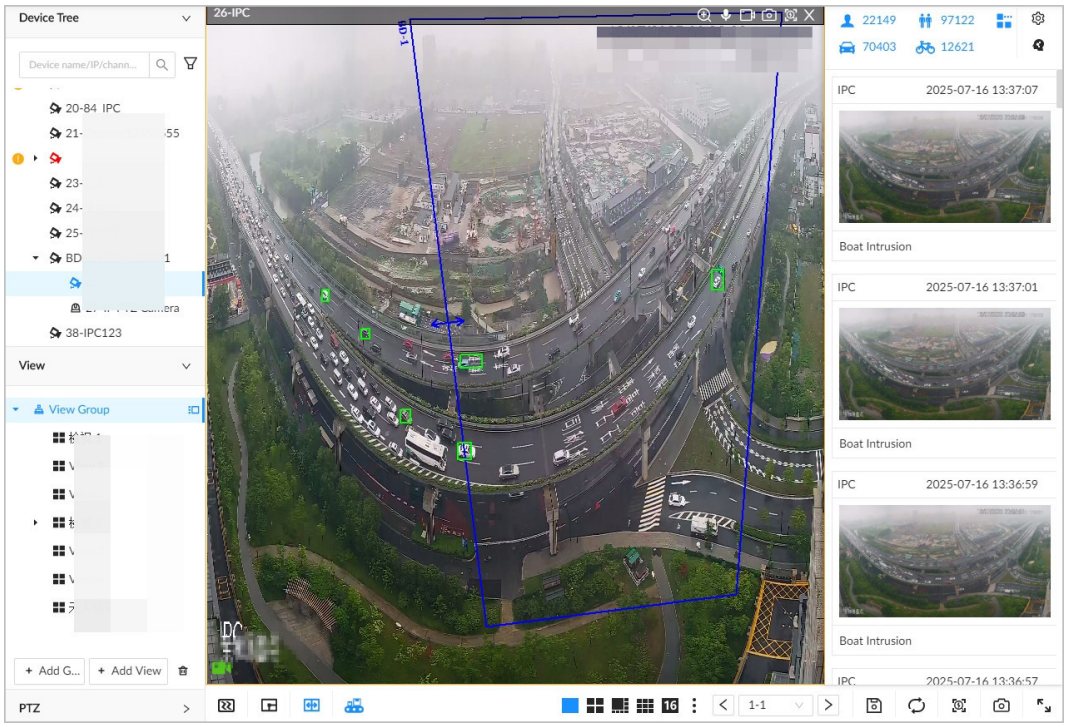
When adjusting the positions of video windows, drag the video window to the layout grid whose background color is green. You cannot drag the video window to the grid of red background color.

- 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 Opening a 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.

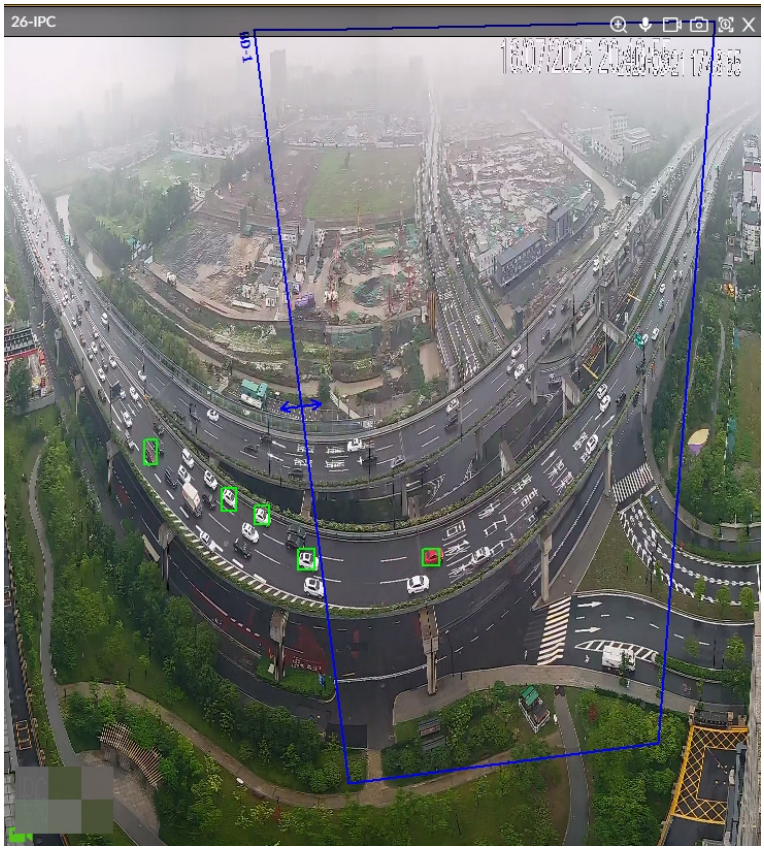
Table 7-4 View function

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.
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.

7.1.1.3 View Window

Log in to the PC client, under the **Live** tab, right-click a view and then select **Open**, or double-click view to open the view window.

Figure 7-5 View window



7.1.1.3.1 Taskbar

Log in to the PC client, under the **Live** tab, open a view and then point to a video window. The taskbar is displayed.

Figure 7-6 View window

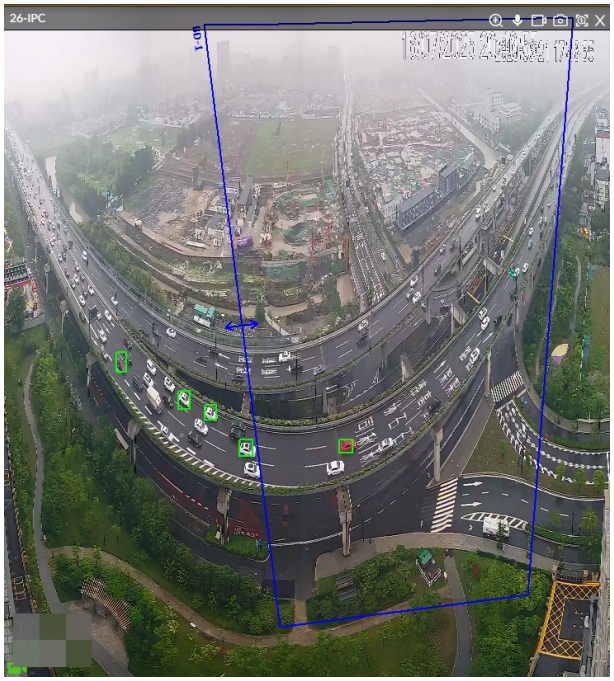


Table 7-5 Window taskbar

Icon	Description
	Zoom. Click the icon, and then select a zone on the video window to zoom in.
	Talk. The Talk function enables voice interaction between the Device and remote devices.
	Instant record. Click  to start recording manually. Then the icon becomes . Click  to stop recording. The system stops recording according to the configured instant recording length if you do not click  to stop. The video storage path varies on different interfaces. ● Local interface. ◇ When a USB storage device is connected, the videos are saved to the USB storage device. ◇ Otherwise, the videos are saved on the Device. You can search for and export videos under the **Search** tab. ● PC client. The default storage path of videos is C:/Program Files (x86)/PCAPP/video.
	Manual snapshot. The snapshot storage path varies on different interfaces. ● Local interface. ◇ When a USB storage device is connected, snapshots are saved to the USB storage device. ◇ Otherwise, the snapshots are saved on the Device. You can search for and export videos under the **Search** tab. ● PC client. The default storage path of snapshots is C:/Program Files (x86)/PCAPP/pictures.
	Search by image. Take a snapshot of face or human during live view, and then use the snapshot to search for similar targets.
	Close the window.

7.1.1.3.2 Shortcut Menu

Log in to the PC client, under the **Live** tab, open a view and then right-click a video window. The shortcut menu is displayed.

The shortcut menu might vary depending on the remote devices.

Figure 7-7 Shortcut menu

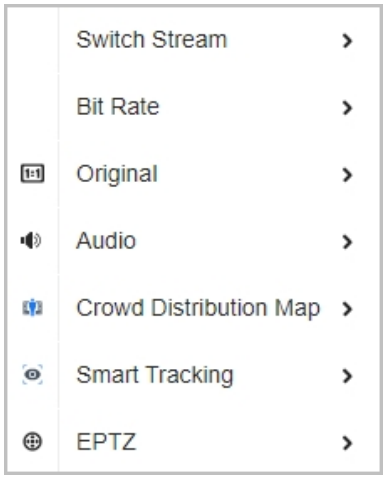


Table 7-6 Shortcut menu description

Parameter	Description
Switch Stream	Select a stream type from **Main Stream** , **Sub Stream 1** and **Sub Stream 2**.
Bit Rate	Select whether to display the real-time bit rate on the upper-left corner of the video window.
Original	Set video window scale. • **ON** : The system automatically adjusts video window scale according to the resolution. • **OFF** : The system automatically adjusts video window scale according to the number of remote devices and the available display space.
Audio	Set an audio output mode from **Audio 1** , **Audio 2**, **Mixing** and **Close**.
Crowd Distribution Map	Set the crowd distribution map to view and monitor crowd density.
Smart Tracking	Intelligently track targets. This function is only available on the multi-sensor panoramic camera + PTZ camera.

Parameter	Description
EPTZ	Click **EPTZ** and select **On**. ● Display mode: Select the number of channels tracked. ◇ : Full screen ◇ : 1Full screen+1Detail ◇ or : 1Full screen+3Detail ◇ : 1Full screen+5Detail ● Linkage track and tracking duration: After turning on linkage track and setting the tracking duration, track the intelligent events. ◇ Customize: Set the tracking duration range. For example, the time is set to 30 to 60 seconds and after tracking target A lasts for 30 seconds, if a new target B appears, and then start tracking target B. If there is no new target appears in the process of tracking A, continue to track A until A disappears or the tracking time reaches 60 seconds. ◇ Continue until the object disappears: Keep track of the target until the target disappears.

7.1.1.3.3 Digital Zoom

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

Log in to the PC client, open a view under the **Live** tab, and then you can zoom in the video window in either of the following ways.

- Point to the center of the zone that you want to zoom in or zoom out, and then scroll the mouse to zoom in or zoom out.
- Click , select a zone on the video window. The zone is enlarged. Release the mouse to restore the original effect.

7.1.1.3.4 Searching by Image

Draw a frame on the video to select an image that contains targets, and then use the image to search for similar faces or human bodies. For details, see "6.3.2 Applying AcuPick".

7.1.1.3.5 Fisheye Dewarp

Set the installation method and display mode of fisheye cameras.

This function is available on select models.

Procedure

Step 1 Log in to the PC client.

Step 2 Under the **Live** tab, open a view.

Step 3 Right-click on the live video, and then select **Fisheye Dewarp**.

Step 4 Select an installation method.

- Click to select ceiling mount.

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

Step 5 Select a display mode.

Table 7-7 Display mode

Installation Method	Display Mode	Description
Ceiling/wall/ground mount		The original fisheye image.
Ceiling/ ground mount	1P+1	Corrected 360° panoramic image + section images.
	2P	2 corrected 180° images that together constitute a 360° panoramic image.
	1+3	Original image + 3 section images.
	1+4	Original image + 4 section images.
	1P+6	Corrected 360° panoramic image + 6 section images.
	1+8	Original image + 8 section images.
Wall mount	1P	Corrected 180° image from left to right.
	1P+3	Corrected 180° image + 3 section images.
	1P+4	Corrected 180° image + 4 section images.
	1P+8	Corrected 180° image + 8 section images.

Step 6 Click **OK**.

7.1.1.3.6 Smart Tracking

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

Make sure that the linked tracking function has been enabled.

Procedure

Step 1 Log in to the PC client.

Step 2 Under the **Live** tab, open a view.

Step 3 Right-click the live video, and then select **Smart Tracking** > **ON**.

Step 4 Select the tracking method.

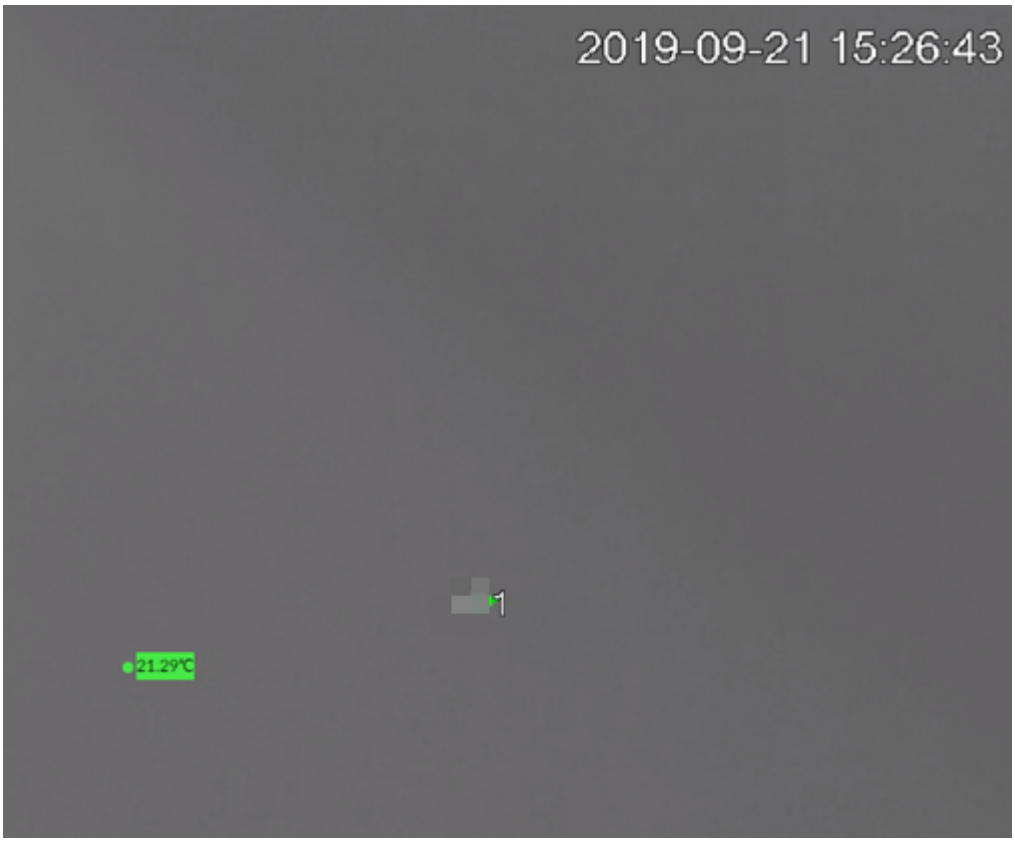
- Manual positioning: Click a spot or select a zone on the bullet camera video, and then the PTZ camera will automatically rotates there and zoom in.
- Manual tracking: Click or select a target on the bullet camera video, and then the PTZ camera automatically rotates and tracks it.
- Automatic tracking: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

7.1.1.3.7 Thermal

Log in to the PC client. Under the **Live** tab, a thermal camera has 2 channels by default: visible light channel and thermal channel.

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

Figure 7-8 Thermal



7.1.1.3.8 Talk

The Talk function enables voice interaction between the Device and remote devices, improving the efficiency in handling emergency events.

Procedure

Step 1 Log in to the PC client.

Step 2 Open a view under the **Live** client.

Step 3 Click  at the upper-right corner of the view window to enable the Talk function. Click again to disable the function.

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 7-9 Device tree

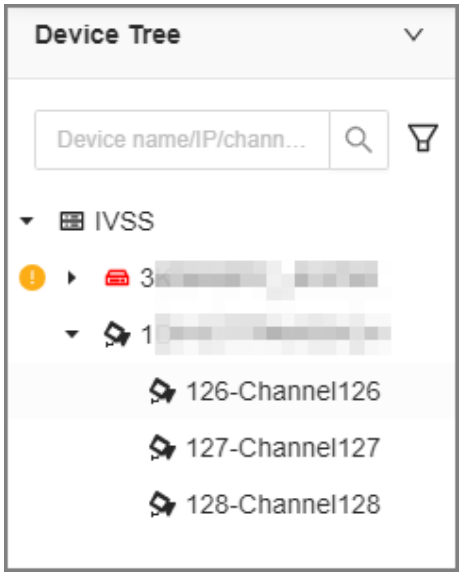


Table 7-8 Device tree description

Operation	Description
Search for devices	Enter keywords in Device name/IP/chann... . Supports fuzzy search.
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 IVSS 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 (Optional) PTZ

7.1.3.1 Configuring 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.

- Some front-end models support PTZ. Refer to the actual page for details.
- The PTZ functions might vary depending on the device models.

Figure 7-10 PTZ

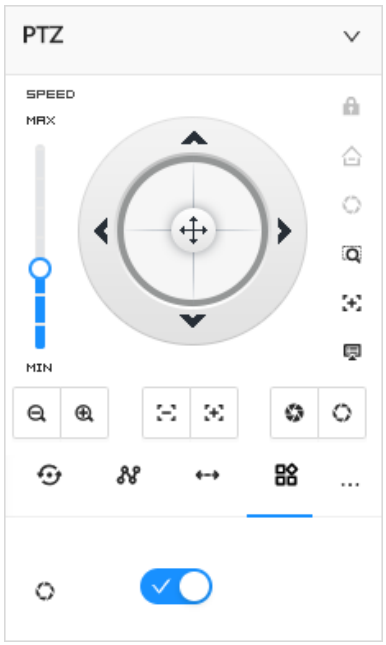


Table 7-9 PTZ control panel

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.

Icons	Description
	Click to enable auto focus, and then the camera image becomes focused automatically.
	Click to enter the PTZ menu mode. For details, see "7.1.3.2 PTZ Menu Settings".
	Zoom. Click to adjust lens zoom rate of the remote device.
	Focus. Click to adjust lens focus of the remote device.
	Iris. Click it to adjust iris size of the remote device.
	Click to use windshield wiper. : Click to enable windshield wiper.
	Click to use PTZ functions. Before using PTZ functions, you need to configure the PTZ functions. For details, see "7.1.3.3 Configuring PTZ Functions". • : preset. • : tour group. • : pattern. • : scan.

7.1.3.2 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.

Figure 7-11 PTZ menu

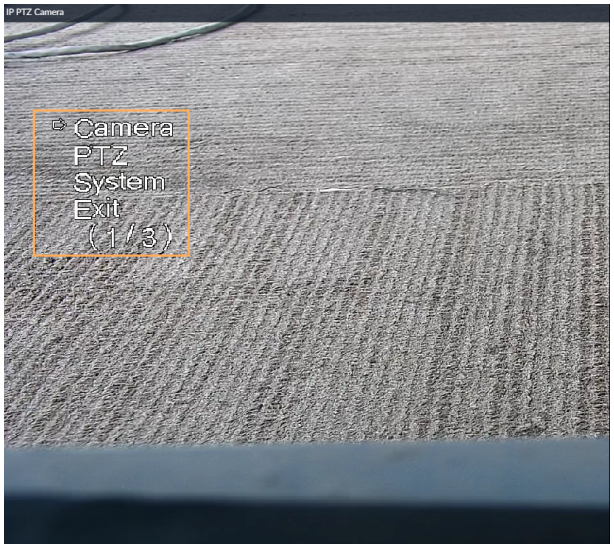


Table 7-10 PTZ menu description

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.

7.1.3.3 Configuring PTZ Functions

Control PTZ device to implement corresponding operations.

The PTZ functions might vary depending on the device models.

7.1.3.3.1 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

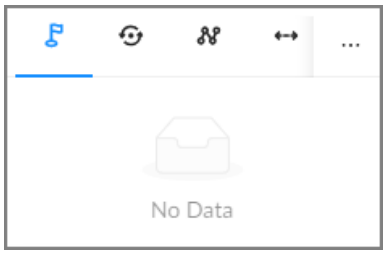
Step 1 Log in to the PC client.

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 7-12 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.

7.1.3.3.2 Setting a Tour Group

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.

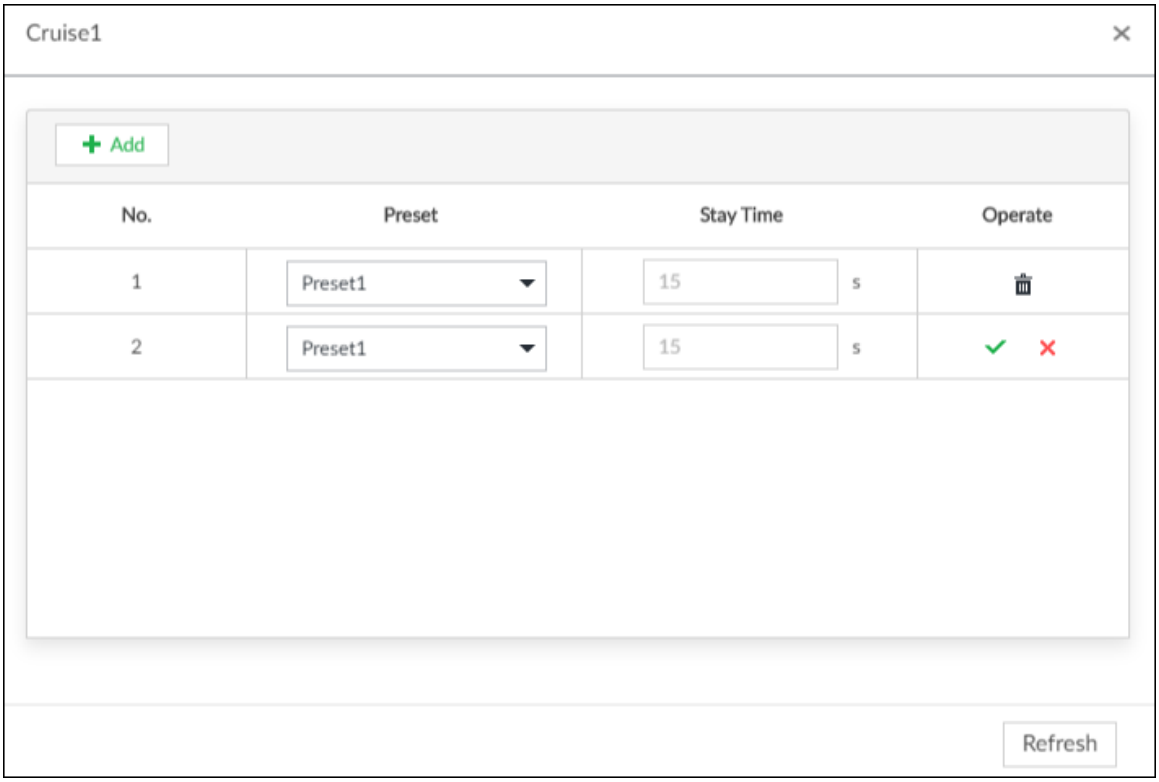
Step 4 On the PTZ panel, click .

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.

Figure 7-13 Add a 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.

7.1.3.3.3 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 pattern. 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.

7.1.3.3.4 Setting a Scan

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 limit 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 .

7.1.3.3.5 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.

7.1.4 (Optional) PTRZ

7.1.4.1 Configuring PTRZ

Log in to the PC client. Use the PTRZ panel at the lower-left corner of the **Live** tab to perform PTRZ control so that the PTRZ camera can rotate accordingly to monitor all directions.

- Some front-end models support PTRZ. Refer to the actual page for details.
- The PTRZ functions might vary depending on the device models.

Figure 7-14 PTRZ

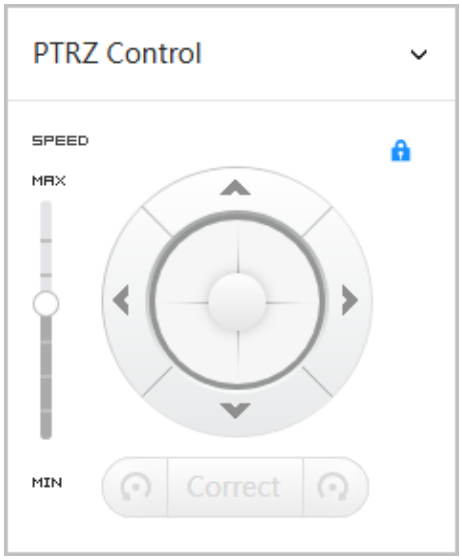
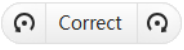


Table 7-11 PTRZ control panel

Icons	Description
	Slide to set PTRZ speed. The higher the value, the faster the PTRZ speed.
	Click the arrows to control PTRZ movement.
	Control scene correction in the following ways. • Click or to adjust the angle of the scene. • Click **Correct** to adjust the scene and keep the image horizontal.
/	Click the icon to toggle between locked and unlocked PTRZ status. For details, see "7.1.4.2 Setting PTRZ State". • : The PTRZ is locked. • : The PTRZ is unlocked.

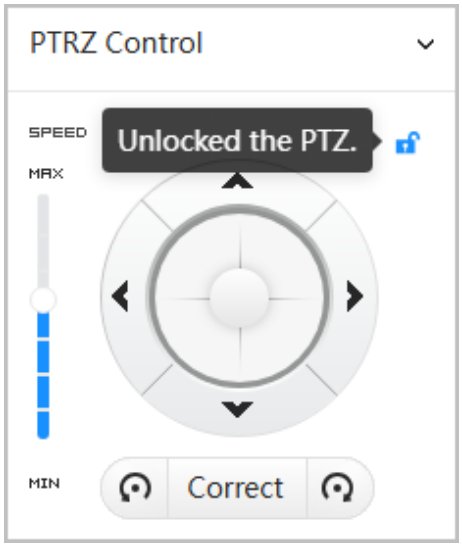
7.1.4.2 Setting PTRZ State

At the lower-left corner of the **Live** page, you can switch the PTRZ state.

- Click to unlock the PTRZ.

  In the unlocked state, you can operate the PTRZ through the panel, including controlling the PTRZ movement, setting the PTRZ speed and using scene correction function.

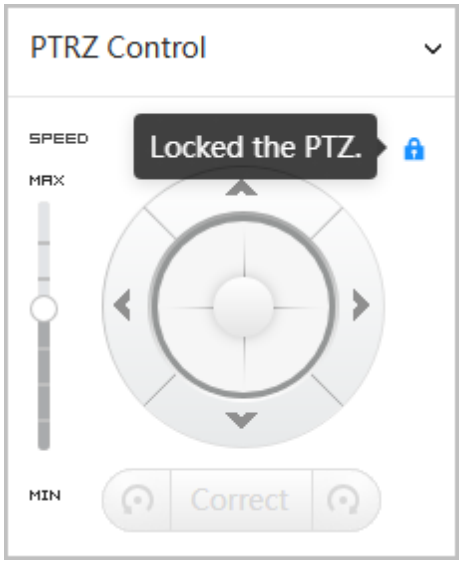
Figure 7-15 The unlocked state of PTRZ



- Click to lock the PTRZ.

  In the locked state, the functions on the PTRZ panel are disabled.

Figure 7-16 The locked state of PTRZ



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.

Enable **Effective Target**, select a target type, such as . Then search the selected channel for the target record video of this type for playback.

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

Table 7-12 Recording search conditions

Search conditions	Description
Stream types	Select a stream type from **Main Stream** and **Sub Stream**.
Search time	Set the search period in the following way. ● Click the date or time in the time box to modify the date or time value. ● Click the date or time in the time box and slide the mouse wheel to adjust the date or time value. ● Click the date or time in the time box, set the date and time in the displayed calendar page, and then click **OK**.

Step 4 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.

  ◇ When the record video length is ≤ 1 hour, the record video file is expanded into 5-minute segments.
  ◇ When 1 hour < the record video length ≤ 2 hours, the record video file is expanded into segments of 10 minutes.
  ◇ When 2 hours < the recorded video length ≤ 3 hours, the recorded video file is expanded into segments of 15 minutes.
  ◇ When the record video length is greater than 3 hours, the record video file is expanded into segments of 20 minutes.

  ◇ 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 7-17 Timeline playback

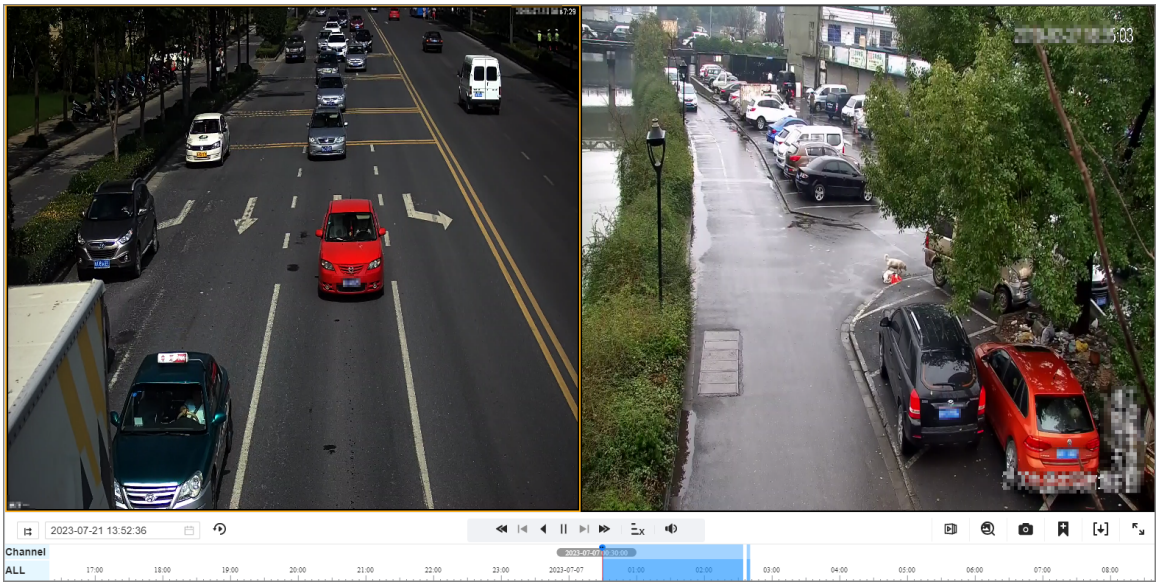


Figure 7-18 File playback

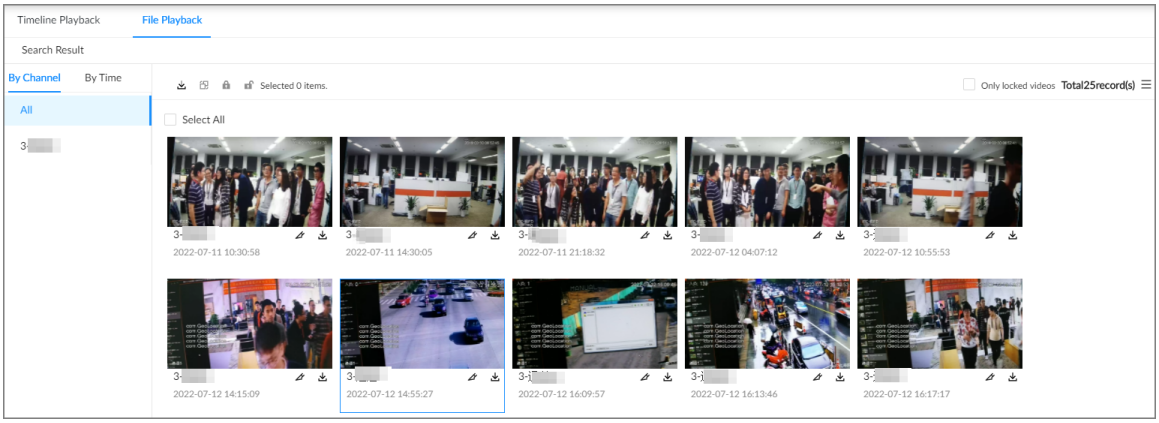
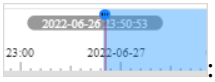


Table 7-13 Search icons description

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 .
	Displays or hides the detection area/exclusion area.

Signal Words	Description
	Displays or hides the rule line/target box.
	Play back video files 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.
	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.
	Click to shut down the recorded video screen being played back and search again for playback.
	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.
	Close the playback window.

7.2.2 Clipping a 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 **Playback**.

Step 3 Search for recorded videos and then play back a video.

Step 4 Click .

Figure 7-19 Clip a video



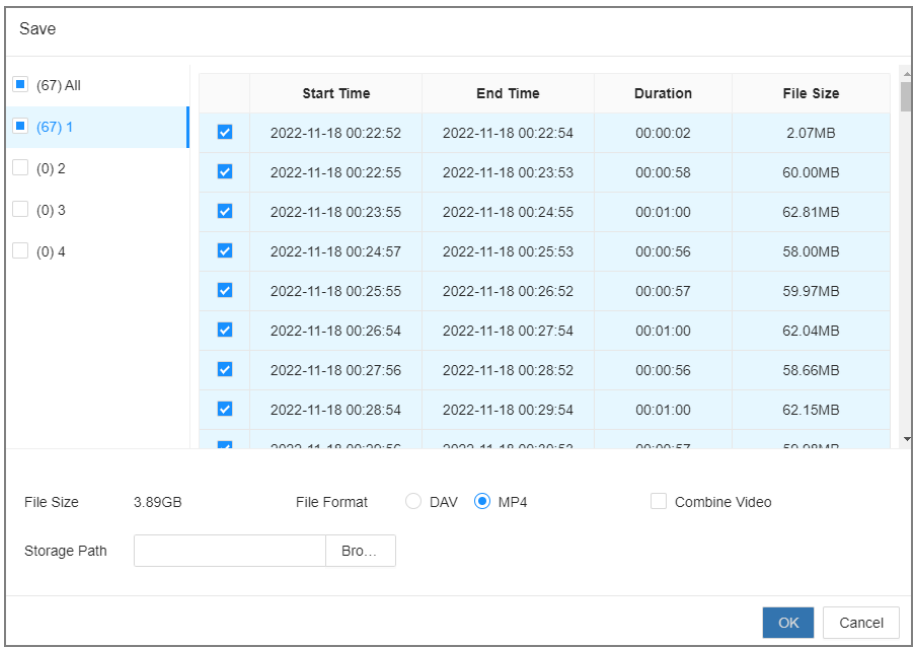
Step 5 Drag the left and right edges of the blue frame to select the start time and end time of clipping.

Step 6 Click .

Step 7 Select a file format, and then click **Browse** to select the storage path.

Select **Combine Video** to combine and download multiple segments of recorded videos.

Figure 7-20 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 **Playback**.

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 **Playback** > **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 **Playback**.

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 Playing Back Snapshots

Search for and view snapshots according to remote device, image type, and snapshot time.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **Playback**.

Step 3 Select a remote device, click **Picture** tab, and then set the conditions.



A maximum of one remote device can be selected.

Step 4 Select an image type.

- **Manual Snapshot** : Manual snapshots.
- **Video Detection** : Snapshots linked with video detection.
- **External Alarm** : Snapshots linked with internal and external alarms.
- **Thermal** : Snapshots linked with thermal alarms.
- **Smart Motion Detection** : Snapshots linked with smart motion detection.
- **AI Event** : Snapshots linked with AI events.

Step 5 Set the search period.

Step 6 Click **Search**.

7.2.6 Backing up Files

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 **Playback**.

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.

7.2.7 Watermark Verification

Verify whether a video file is tempered.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **Playback** > **Watermark**.

Step 3 Click **Browse** to select a video file.

Step 4 After the file is uploaded, click **Parity**.

- Normal: If the verification result is normal, the correct watermark is displayed.
- Error: If the verification result is abnormal, the abnormal watermark and its type are displayed.

7.3 Display Management

Enable connected monitors or lock the screen.

7.3.1 Multiple-Screen Control

The Device can connect to multiple monitors at the same time. You can select a monitor you want to use.

- The multiple-screen control function only available on the local interface.
- Go to **System** > **General** > **Display** to enable a monitor or set its resolution.
- The page might vary depending on the number of the connected monitors.

Click on the local interface.

- The 1–3 monitors represent monitors connected to HDMI 1–HDMI 3. The main screen refers to the monitor connected to VGA or HDMI 1 port. The monitors connected to the HDMI 2 and HDMI 3 are the sub screens. The main screen and sub screen display different content and support different resolutions and refresh intervals.
- VGA and HDMI 1 output the same video source. The 3 HDMI ports can output different video sources.
-  means connecting and enabling a monitor.  means monitors that are connected but not enabled.
- Click  to enable the monitor. The main screen is enabled by default and cannot be disabled.

7.3.2 Sub Screen Operations

The local page supports sub screen operations.

Procedure

1. Connect multiple screens to the HDMI ports of the device.

   Connect the main screen to the HDMI1 port, and connect the sub screens to the remaining HDMI ports, such as HDMI2 to HDMI4, corresponding to sub screen 2 to 4 respectively.
2. View the live videos on the screen, with the screen number shown in the upper-right corner of the image.

   - The main screen supports preview-related operations (such as screen splitting, video patrol, view inspection and channel switching), as well as configuration functions.
   - The sub screen 2 only supports preview-related operations (such as screen splitting, video patrol, view inspection, and channel switching) and does not support the configuration of other functions.
   - The sub screens 3 and 4 only support single-screen splitting, while other operations are the same as those of the sub screen 2.
   - If you want to view the layout on the sub screen, please first configure the layout on the main screen.

7.3.3 Locking the Screen

Log in to the PC client. Click admin and then select **Lock**. The screen is locked at the current page.

If you want to unlock the screen for more operations, click any position on the screen, enter the password of the current account or use another account to log in.

7.4 Audio Management

Upload and manage audio files that the Device plays when an alarm event occurs.

- You can upload .pcm, .mp3, .wav, and .aac files.
- A single audio file must not be less than 2 KB and must not exceed 10 MB.
- The total size of imported audio files must not exceed 200 MB.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **System** > **Audio File**.

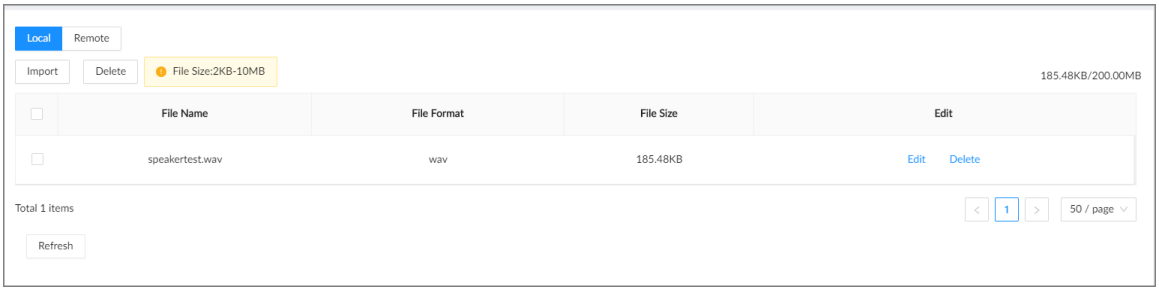
Step 3 Import audio files to the Device or remote devices.

- Import audio to the Device.
  1. Under the **Local** tab, click **Import**.
  2. Select an audio file and then click **Open**.
- Import audio to a remote device.
  1. Under the **Remote** tab, select a remote device from the camera list.
  2. Click **Import**.
  3. Select an audio file and then click **Open**.

Step 4 Click **Import** to select the audio files that you want to import.

Step 5 Click **OK**.

Figure 7-21 Audio file



Related Operations

- Rename the audio file.

  Click **Edit** in the **Edit** column, enter the new name, and then click **OK**.
- Delete the audio file.
  - ◇ Delete one by one: Click **Delete** next to **Edit**.
  - ◇ Delete in batches: Select one or more files, and then click **Delete** next to **Import**.

7.5 Event Center

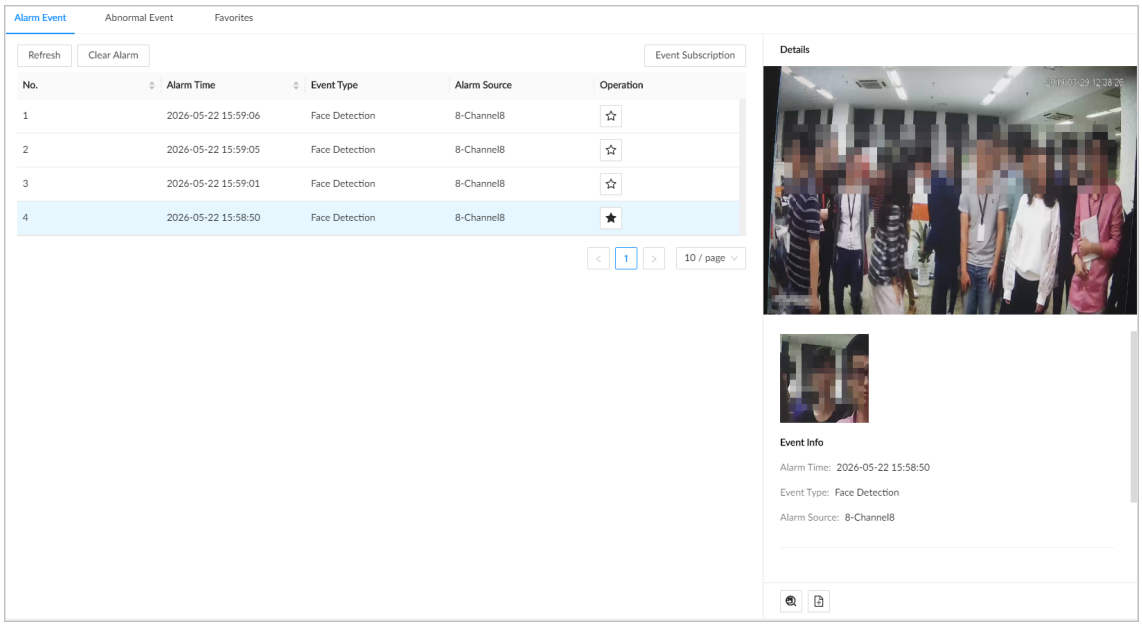
7.5.1 Real-Time Events

7.5.1.1 Alarm Event

Log in to the PC client. Select **Event Center** > **Real-Time Events** > **Alarm Event**, and then the system displays alarm events in real time.

- Click **Pause Refresh** to stop refreshing real-time alarm events.
- Click **Event Subscription**. In the pop-up window, select the event type to show only the selected real-time alarm events.
- Click an alarm event to display details on the right side of the page, and then click the page to start replaying the video (10 seconds before and after the snapshot).
- Click ☆ of the **Operation** column to add this event to favorites.
- Click **Clear Alarm** to clear the currently displayed real-time alarm events.

Figure 7-22 Alarm events



The following operations are supported on the event details page.

The detection results of some alarm events support the following operations.

- Click to enter the search by image of **AI Search** page.
- Click to add detection results to the comparison database, such as false alarm experience database, plate database, and more. The specific databases that can be added are determined by event types.

Table 7-14 Operations related to event details

Function	Operation
	Click  to pause the playback recording, and the icon changes to .
	Click  to stop the playback recording. You can drag the right progress bar to quickly go to a specific time.
	Displays the detection area or exclusion area.
	Displays the rule line or recording box.
	Switch among audio 1, audio 2, or mix.
	Adjust volume.
	Select playback duration: 20 seconds, 5 minutes, 15 minutes, or 1 hour.
	Full-screen display.

7.5.1.2 Abnormal Event

Log in to the PC client. Select **Event Center** > **Real-Time Events** > **Abnormal Event**, and then the system displays abnormal events in real time.

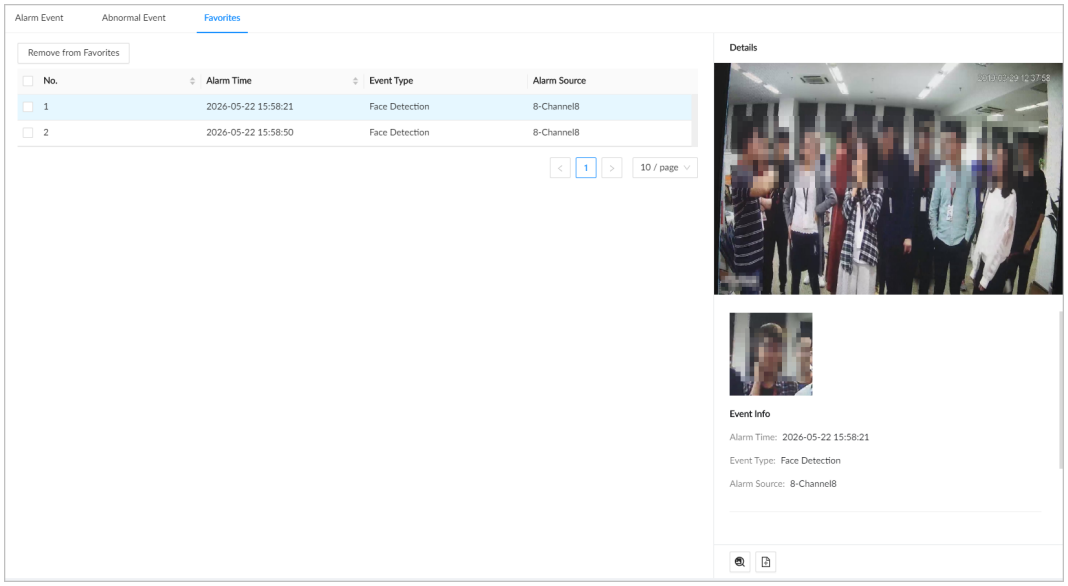
- Click **Pause Refresh** to stop refreshing real-time abnormal events.
- Click **Event Subscription**. In the pop-up window, select the event type to show only the selected real-time abnormal events.
- Click  of the **Operation** column to add this event to favorites.
- Click **Clear Alarm** to clear the currently displayed real-time abnormal events.

7.5.1.3 Favorites

Log in to the PC client. Select **Event Center** > **Real-Time Events** > **Favorites**, and then the system displays collected alarm events and abnormal events.

- Click an alarm event to display details on the right side of the page. Click the screen to start playback of the recording (10 seconds before and after the capture). The playback operations are similar to those on the alarm event page, and you can refer to the alarm event operations. Some intelligent event detection results support the following operations.
  - Click  to enter the search by image of the **AI Search** page.
  - Click  to add detection results to the comparison database, such as false alarm experience database, license plate database. The specific databases that can be added are determined by the event type.
- Select the event and click **Remove from Favorites** to remove the event information from your favorites.

Figure 7-23 Favorites



7.5.2 Event History

Procedure

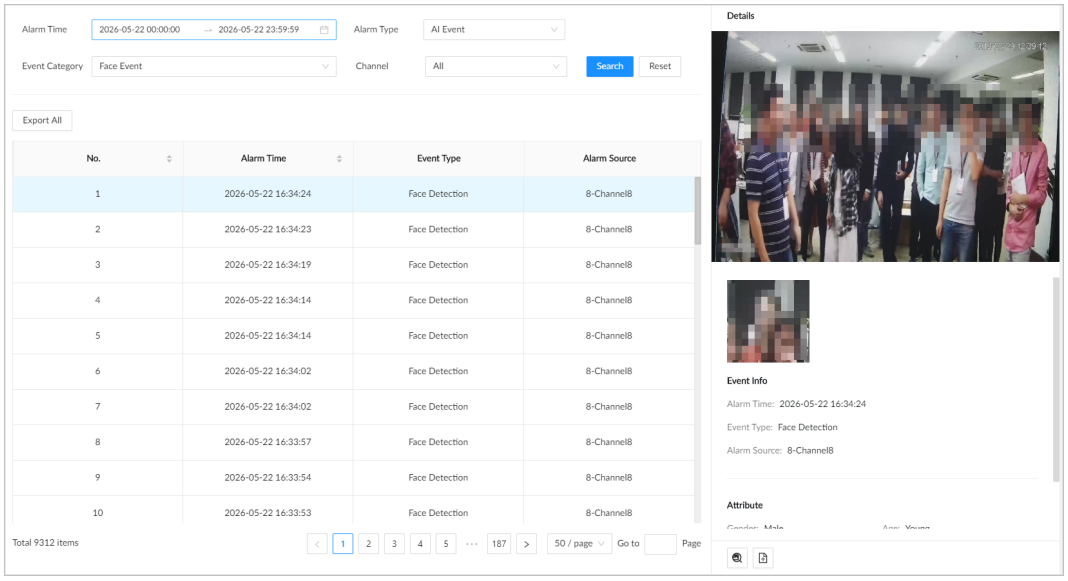
Step 1 Log in to the PC client.

Step 2 Select **Event Center** > **Event History**.

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

Click **Export All** . In the pop-up window, set the save path, and then click **OK** to export the event information to the local device.

Figure 7-24 History events



Step 4 Click an alarm event to display details on the right side of the page. Click the page to start playback of the recording.

The operations supported for playback recording are similar to those in the **Alarm Event** page, you can refer to the operations of alarm events. The detection results of some alarm events support the following operations.

- Click to enter the search by image of **AI Search** page.
- Click to add detection results to the comparison database, such as false alarm experience database, plate database, and more. The specific databases that can be added are determined by event type.

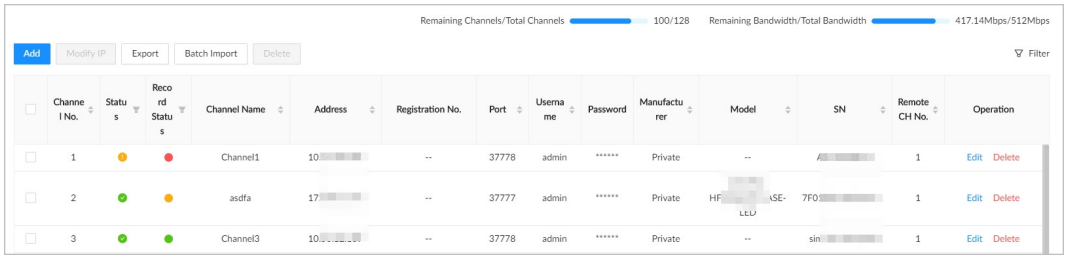
8 System Configuration

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.

8.1 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 8-1 Device management



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

8.1.1 Viewing Remote Devices

View connected remote devices.

Procedure

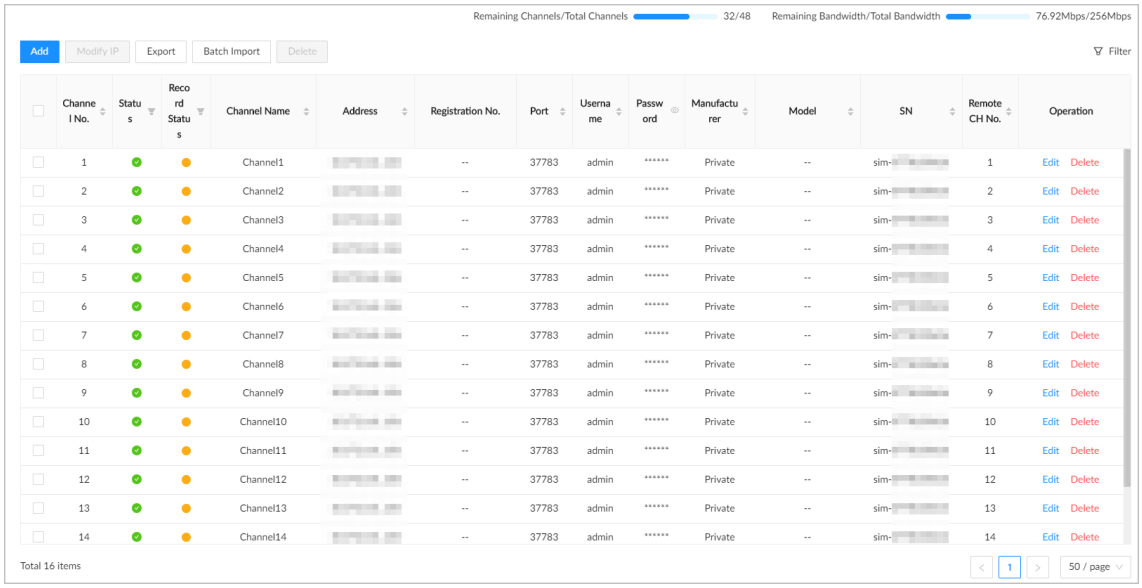
Step 1 Log in to the PC client.

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 in the device tree, and then under the **Camera** tab, you can view the remote devices added to IVD.

Figure 8-2 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.

8.1.2 Configuring Intelligent Compression

Using the video compression function, the front-end video data can be effectively compressed, reducing video storage space and solving problems such as video lag.

The compression mode includes the scheduling mode and the access mode.

- Scheduling mode: Without accessing the front-end device, cooperate with the platform to remotely schedule any front-end video streaming for compression preview, playback, etc. For example, when a remote device is accessed through the platform, this device can use the scheduling mode to compress the number of channels data of the remote device.
- Access mode: Access to the front-end device. Supports compression preview, playback, download, and support storage after compression of the main stream connected to the front-end.

8.1.2.1 Configuring Compression Plans

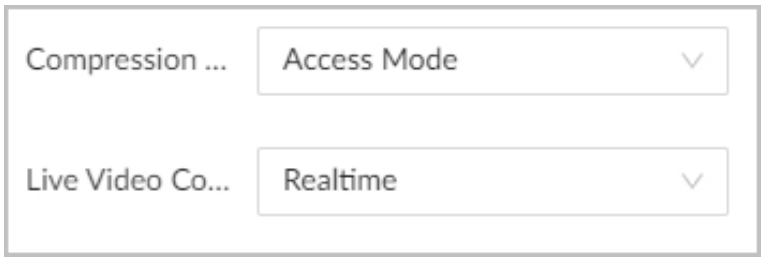
Procedure

Step 1 Log in to the PC client.

Step 2 Click **Camera** of the **Configuration List**, or click , and then select **Camera**.

Step 3 Select the root node in the device tree on the left, select **Compression Status** tab, and select a compression plan and compression preview mode.

Figure 8-3 Compression plans



Step 4 Click **Apply**.

8.1.2.2 Configuring Compression Parameters

Prerequisites

Select **Algorithm** > **Algorithm Management** > **AI Module**, and then set the AI module to **Compression Engine**.

Procedure

Step 1 Log in to the PC client.

Step 2 Click **Camera** of the **Configuration List**, or click , and then select **Camera**.

Step 3 Select the root node in the device tree on the left, and then select **Intelligent Compression** tab.

Step 4 Configure **Intelligent Compression** parameters.

- The parameters supported by the scheduling mode and access mode are different. Refer to the actual page.
- When selecting remote devices, **Intelligent Compression** parameters support either **Use Configuration of Local Device** or **Custom**.

Figure 8-4 Scheduling mode

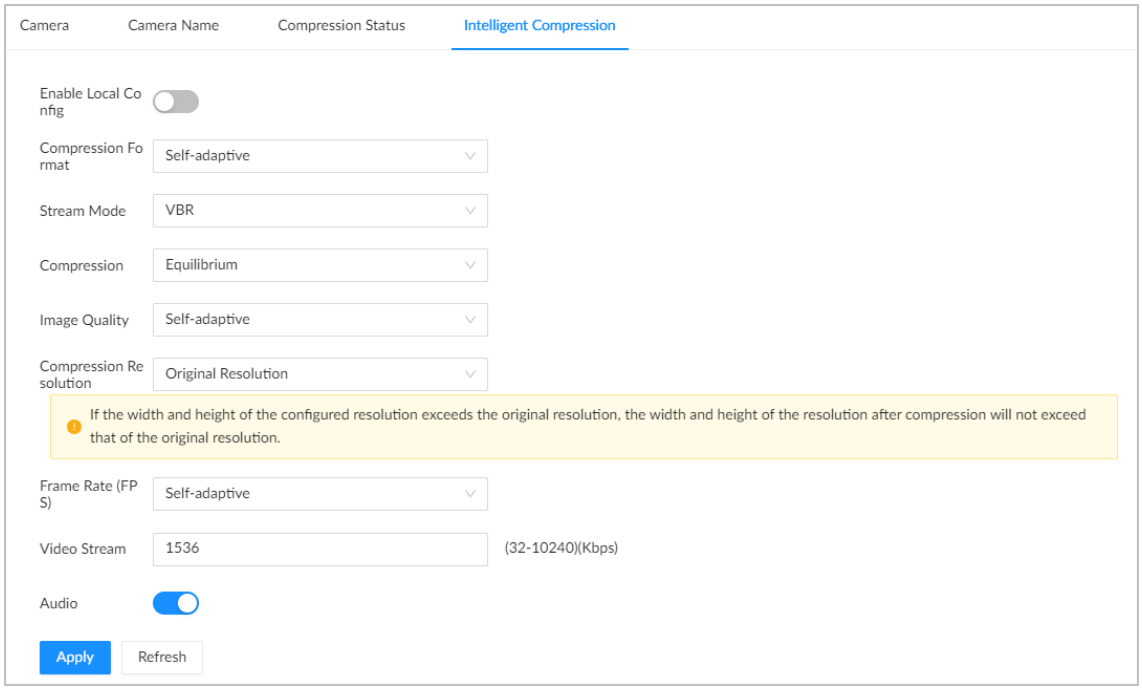


Figure 8-5 Access mode

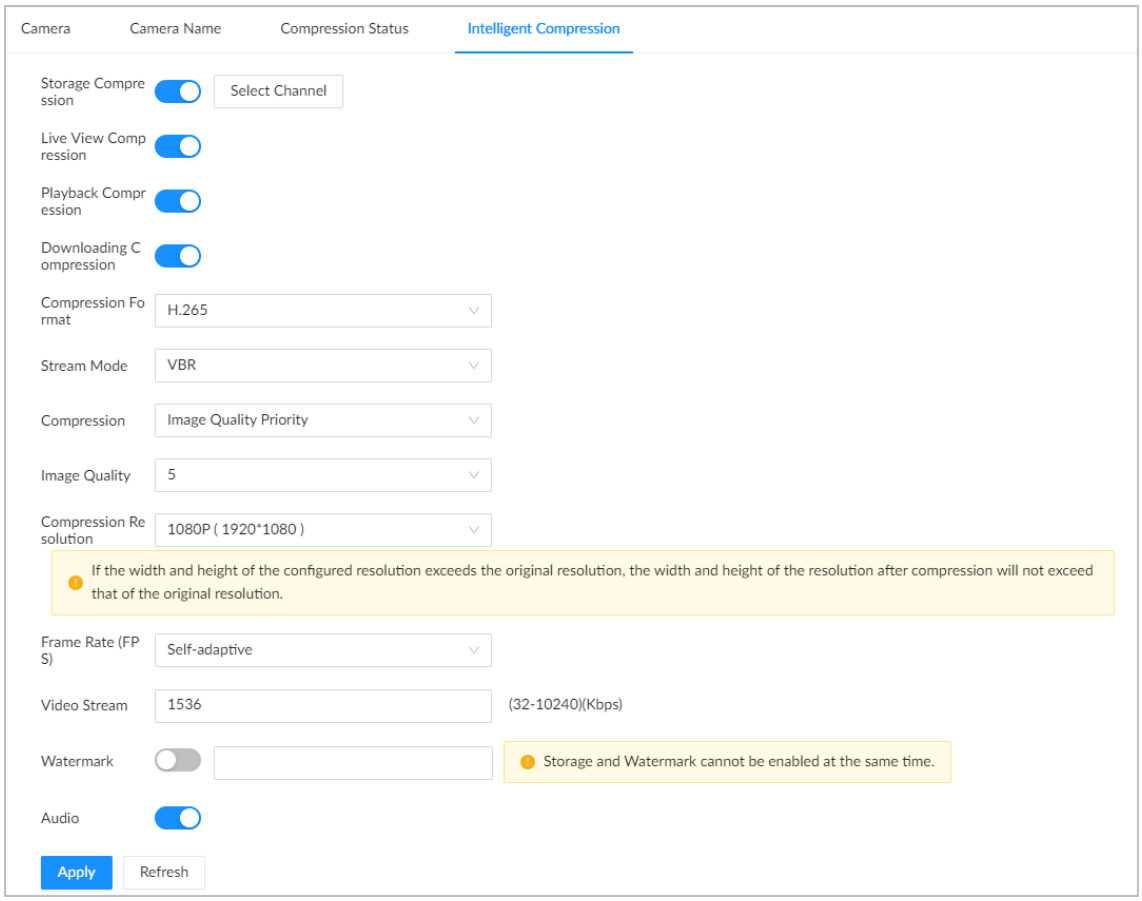


Table 8-1 Intelligent compression parameter description

Parameter	Description
Storage Compression	Enable compression storage, click **Select Channel**, and then select the remote device channel to which the compression configuration should be applied in the pop-up page.
Live View Compression	Enable compression preview to compress the video stream when previewing the channel.
Playback Compression	Turn on compression playback to compress the video stream when playing back record video.
Downloading Compression	Turn on compression download and compress the video stream when downloading record video.
Enable Local Configuration	Click next to **Enable Local Config**, and then enable on-premises settings to compress video according to the settings of this device.
Compression Format	Select the encoding format after stream compression, including **Self-adaptive** , **H.264** and **H.265**.
Stream Mode	Includes **VBR** and **CBR**.
Compression	Including **Compression Priority** , **Image Quality Priority** and **Equilibrium**.
Image Quality	Including self-adaptive and 1 to 6, the higher the level, the better the image quality, but the lower the compression rate.
Compression Resolution	Select the resolution after stream compression according to actual needs.
Frame Rate (FPS)	Set the number of frames per second displayed by the video. The higher the frame rate, the more realistic and smooth the image.
Video Stream	Enter range from 32 Kbps through 10,240 Kbps.
Watermark	Enable the watermark function and add the watermark information to the compressed video.
Audio	If turned on, the audio is included after stream compression. If turned off, there is no audio after stream compression.

Step 5 Click **Apply**.

8.1.2.3 Viewing Compression Status

Procedure

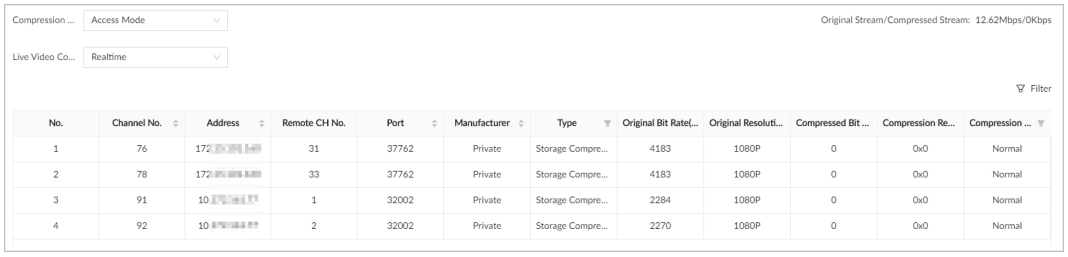
Step 1 Log in to the PC client.

Step 2 Click **Camera** of the **Configuration List**, or click , and then select **Camera**.

Step 3 Select the root node in the device tree on the left, select **Compression Status** tab, and then view the compression status of each remote channel.

The upper-right corner of the page displays the data of the original stream and compressed stream.

Figure 8-6 Compression status



8.1.3 Changing IP Address

Modify IP address of the remote devices that are connected or not connected to the Device.

8.1.3.1 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 Under the **Camera** tab, click **Add**.

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

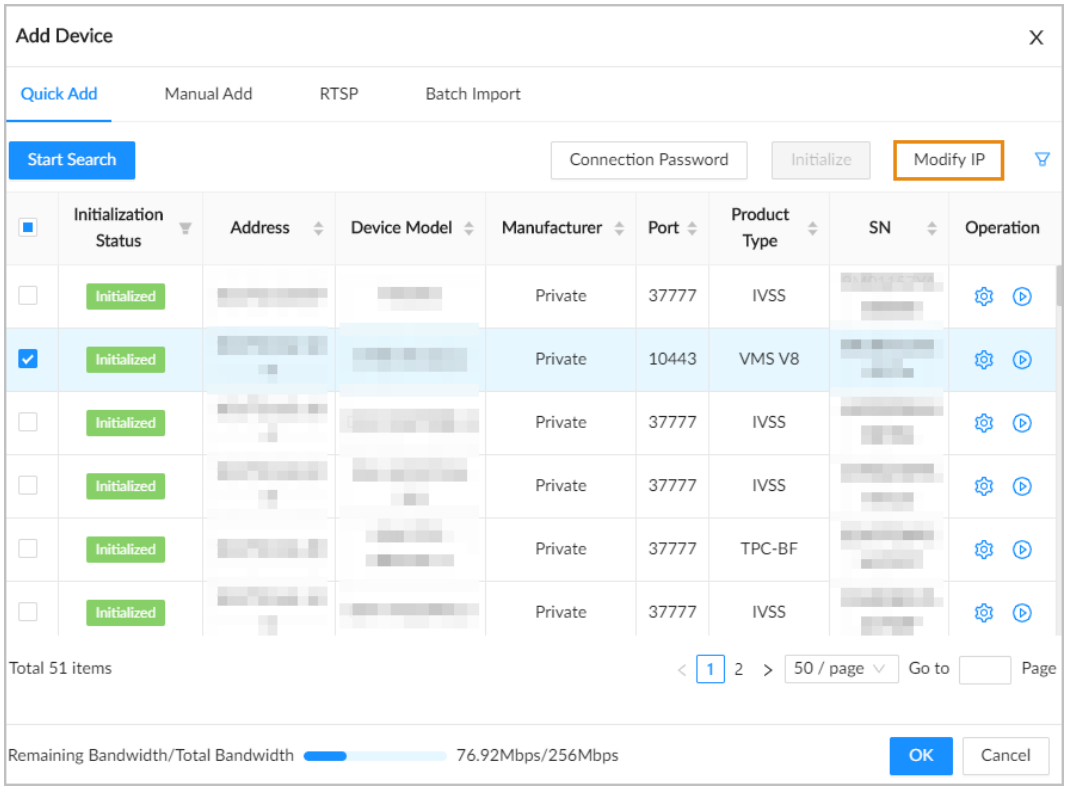
Step 4 Under the **Quick Add** tab, click **Start Search**.

You can click to filter the search results.

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

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

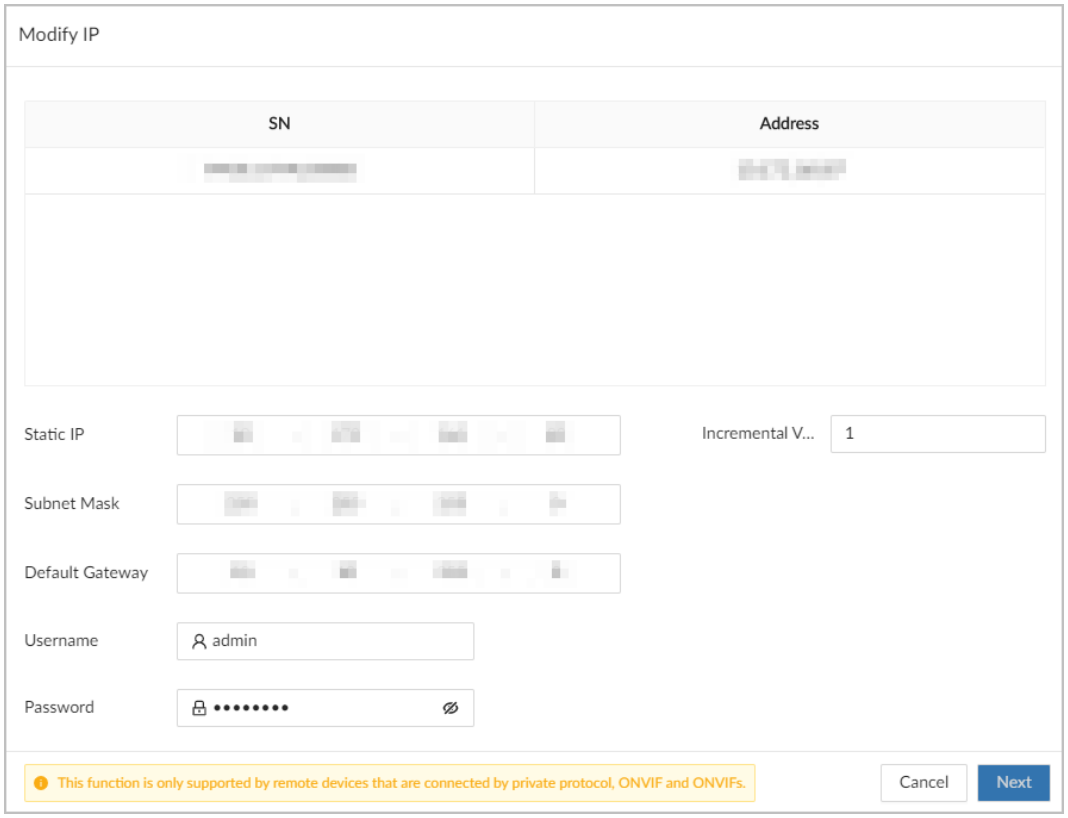
Figure 8-7 Remote device



Step 6 Enter the static IP address, subnet mask, gateway, user name 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 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 occurs 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 user name and password.

Figure 8-8 Modify IP



Step 7 Click **OK**.

8.1.3.2 Modifying IP of Connected Devices

- You can only modify the IP address of initialized devices.
- You can only modify the IP address of remote devices connected through **Private** , **Onvif** or **Onvifs** protocol.

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.

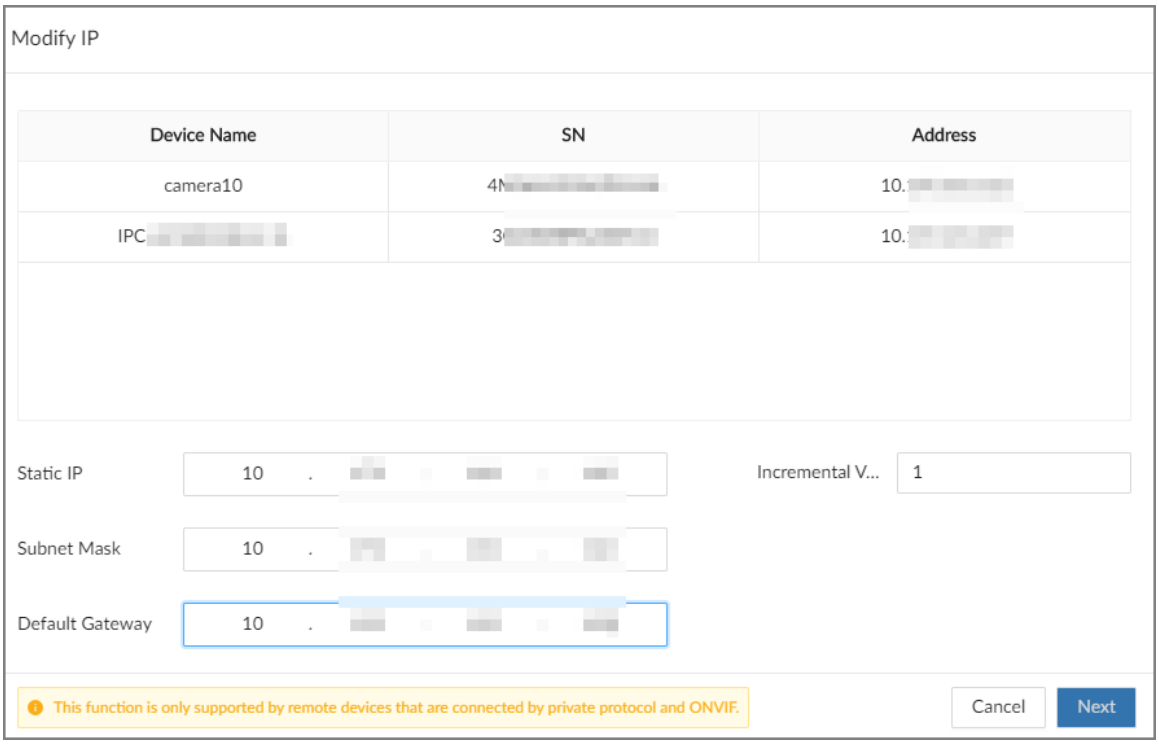
Step 3 Under the **Camera** tab, select one or remote devices, and then click **Modify IP**.

- 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, user name 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 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 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 user name and password.

Figure 8-9 Modify IP (2)



Step 5 Click **OK**.

8.1.4 Configuring Remote Devices

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

The pages might vary with remote devices.

8.1.4.1 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 its model, MAC address, system version, and more.

Figure 8-10 Attributes



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

8.1.4.2 Configuring Connection Information

Set connection information of remote devices, such as the connection type and cache method.

Procedure

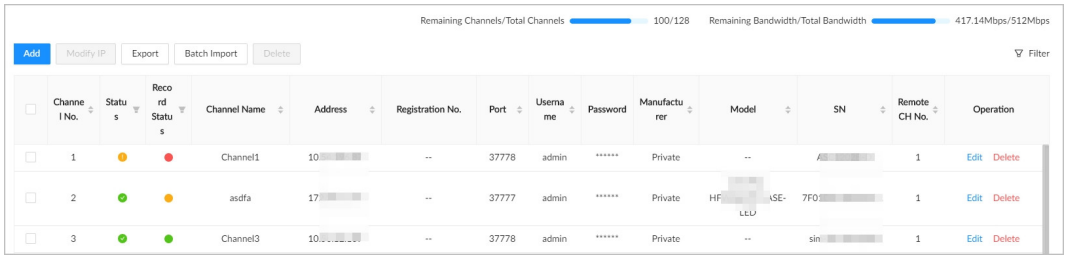
Step 1 Log in to the PC client.

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 in the device tree, and then click the **Camera** tab.

Figure 8-11 Device list



Step 4 Click **Edit**. You can view the connection information of the remote device such as manufacturer, IP address and TCP port, and configure its connection type and cache method.

Table 8-2 Connection parameters description

Parameter	Description
Password	Enter the password of the remote device.
Connection Type	Select a connection type for the system and remote device. It is self-adaptive by default.
Cache Method	Set cache strategy of remote device video stream. ● **Self-adaptive** : The system automatically adjusts video stream cache status according to the network bandwidth. ● **Realtime** : Guarantee the real-timeness of the video. When the network bandwidth is not sufficient, the video might not be fluent. ● **Fluent** : Guarantee video fluency. When the network bandwidth is not sufficient, the video might not be clear.

Step 5 Click **Save**.

8.1.4.3 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** 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 more video channels, and then click **Delete Video Channel**.

8.1.4.4 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**.

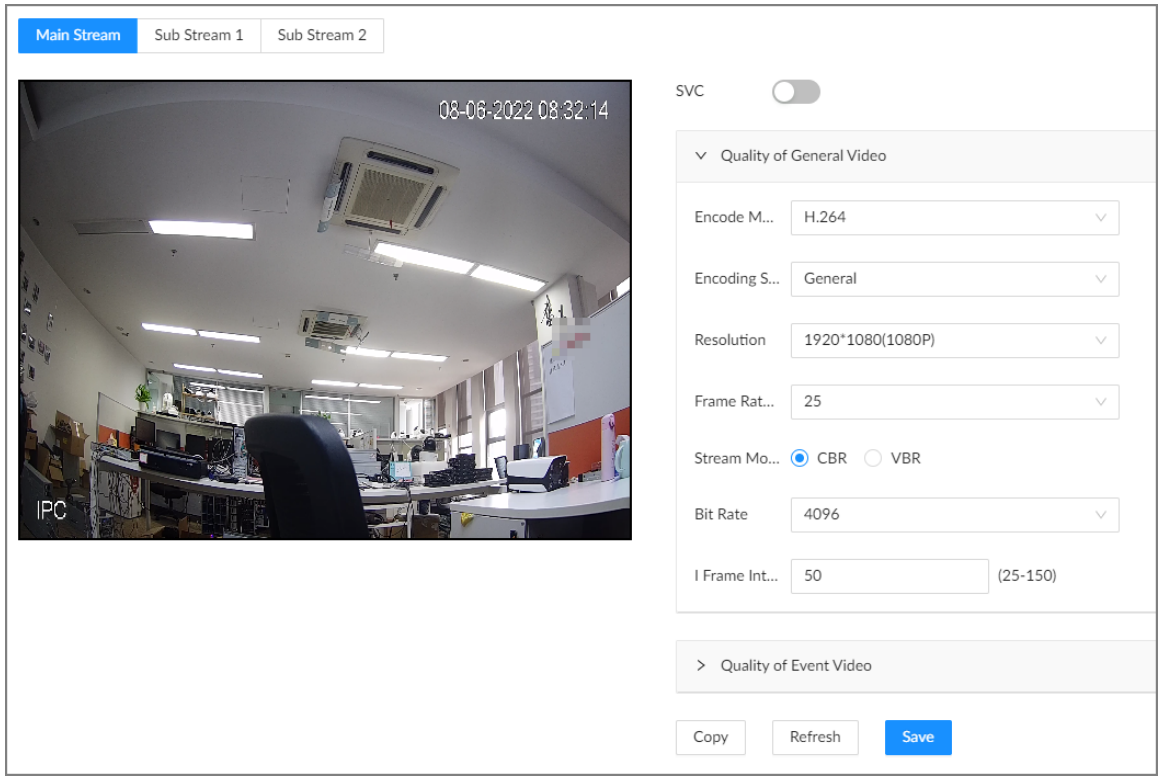
You can also click **Camera** from the configuration list on the home page.

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 8-12 Video



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

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

1. Click to enable SVC, and then select 1 or 2 from the drop-down list on the right.

   SVC refers to the scaled video coding, which can split the video stream to basic stream and enhanced scale. If you select 1, there is no scaled encoding.

   This function is available when the encoding mode is H.264, H.264B or H.264H.

2. Configure the quality parameters of general videos.

Table 8-3 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.
Encoding Strategy	● **General** : Use general coding strategy. ● **Smart Codec** : Enable this function to enhance performance of video compression and reduce required storage space.
Resolution	Set video resolution. The higher the resolution, the better the video quality. Different models of remote devices support different resolutions. See 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 recommended 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.

3. 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 available only for main stream.

Step 6 Click **Save**.

8.1.4.5 Configuring OSD

Set OSD information on the video.

Procedure

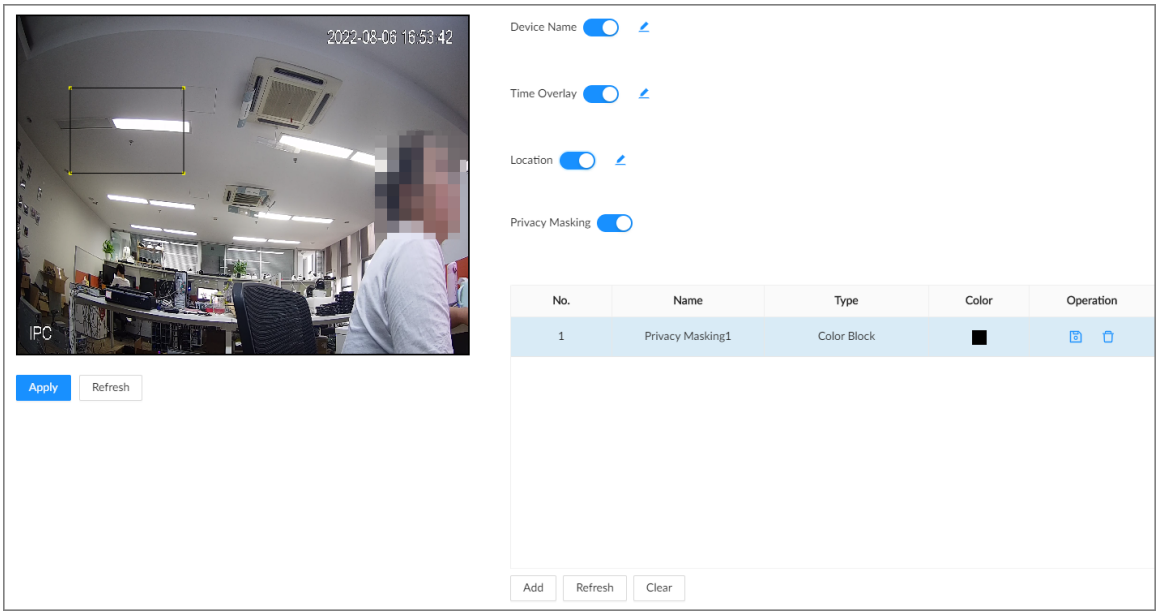
Step 1 Log in to the PC client.

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 8-13 OSD



Step 4 Configure OSD information.

- Device name.
  1. Click to enable OSD of device name.
  2. Click .
  3. Enter the device name.
  4. Drag the text box to the proper position.
- Time.
  1. Click to enable OSD of time.
  2. Click .
  3. Drag the text box to the proper position.
- Geographical position
  1. Click to enable OSD of geographical position.
  2. Click .
  3. Enter the geographical position information.

- Click  to adjust the alignment of text boxes.
- Click  to create a text box.
- Click  to delete a text box.

4. Drag the text box to the proper position.

- Set privacy masking

This function is available only when the camera supports privacy masking.

1. Click  to enable privacy masking.
2. Click **Add**, select the masking type and color, and then draw mosaic or color blocks in the image as needed.
3. Drag blocks to the proper position.
4. Click .

Step 5 Click **Apply**.

8.1.4.6 Configuring Audio Parameters

Procedure

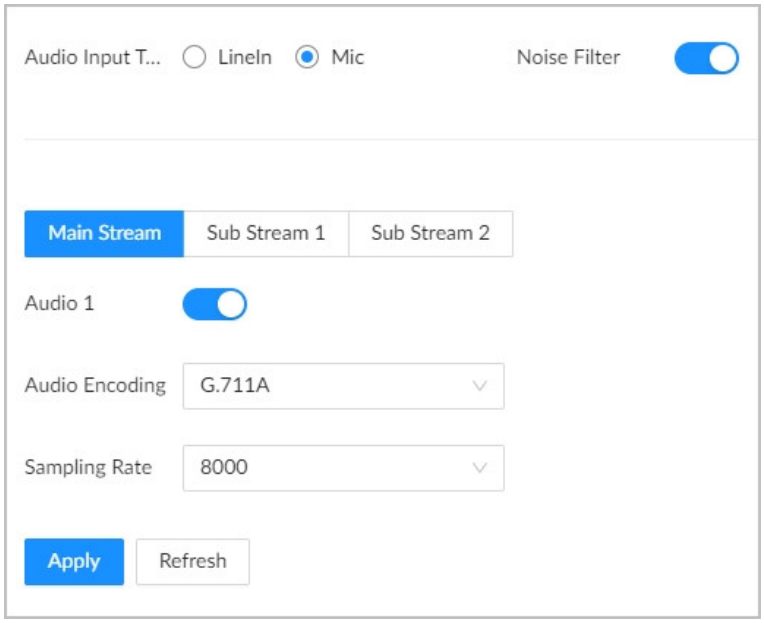
Step 1 Log in to the PC client.

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 **Audio** tab.

Figure 8-14 Audio



Step 4 Select an audio output type.

- LineIn: The Device acquires audio signals through the external audio device.

- Mic: The Device acquires audio signals through internal microphone.

Step 5 Click to enable Noise Filter.

This function is available with select models of remote devices.

Step 6 Click the **Main Stream** , **Sub Stream 1** or **Sub Stream 2** tab, and then configure the parameters.

Table 8-4 Audio parameters

Parameter	Description
Audio Encoding	The audio encoding mode applies to both audio streams and voice talks. We recommend leaving it as default.
Sampling Frequency	The number of samples of a sound that are taken per second. The higher the value, the more accurate the digital representation of the sound can be.

Step 7 Click **Apply**.

8.1.5 Exporting Remote Devices

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

Procedure

Step 1 Log in to the PC client.

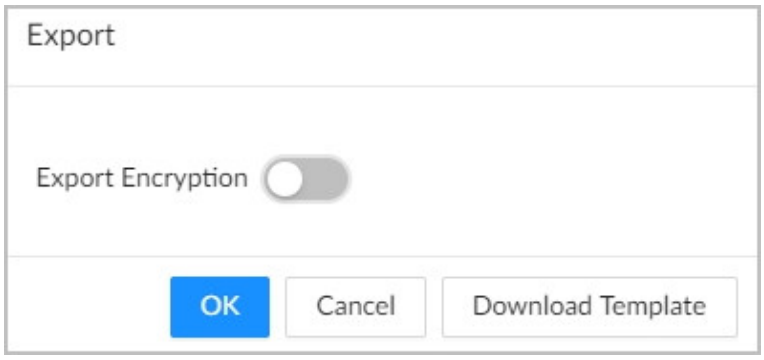
Step 2 Click on the upper-right corner of the page and then click **Camera**.

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 8-15 Export



Step 4 (Optional) Click to enable export encryption.

The exported backup file is encrypted and cannot be edited. If 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 user name (excluding password) of the remote device.

When 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.

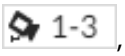
- On the PC client, click ≡, select **Download** to view the file storage path.
- On the local interface, you can select a file storage path.
- On the web interface, files are saved to the default downloading path of the browser.

8.1.6 Importing Remote Devices

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.

8.1.7 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 device, and then select **Open Device Webpage** to go to the web page of the remote device.

8.1.8 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 **Edit** 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**.

8.2 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.

8.2.1 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.

8.2.1.1 Configuring IP Address

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

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

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 8-16 Edit Ethernet network

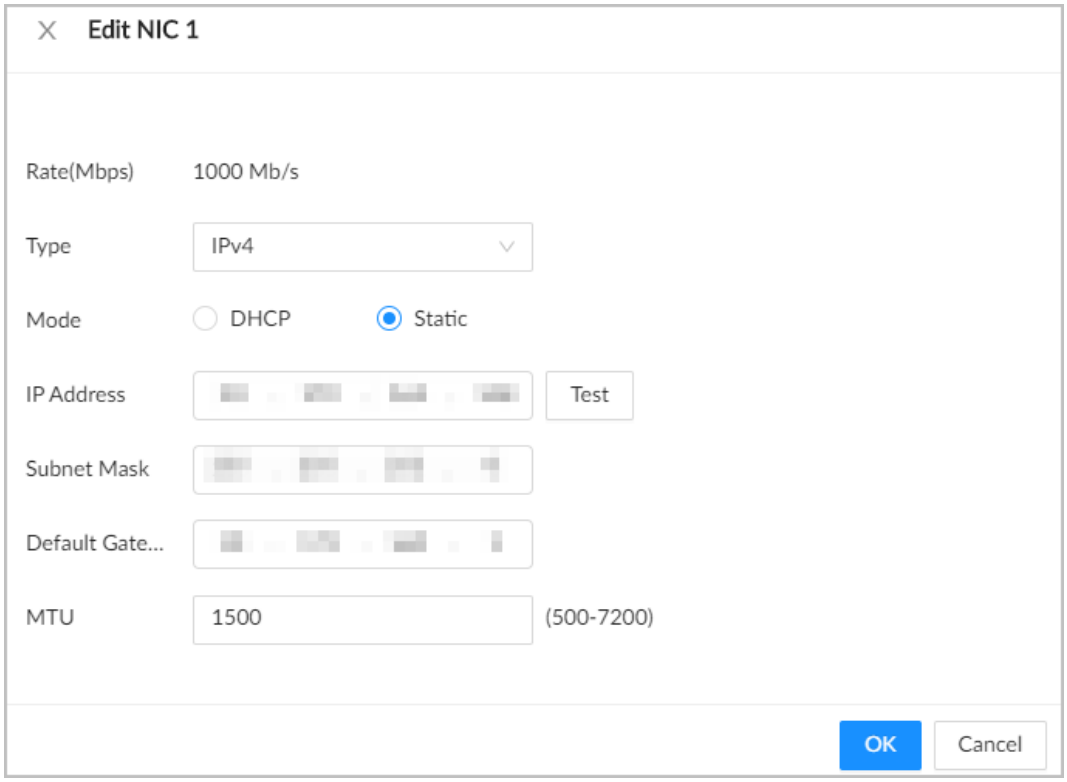


Table 8-5 NIC parameters description

Parameter	Description
Rate (Mbps)	The maximum network transmission speed that the current NIC supports.
Type	Select IPv4 or IPv6.
Mode IP Address Subnet Mask Default Gateway	• **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** : Enter the **IP Address**, **Subnet Mask** and **Default Gateway** to set a static IP address for the Device.
Test	Test whether the IP address is valid.
MTU	Set NIC MTU value. The default setup is 1500 bytes. We recommend you to 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**.

8.2.1.2 Port Aggregation

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

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

Table 8-6 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 adds the network throughput data amount and enhances network flexibility and availability. 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 breaks down. This mode enhances NIC reliability. In this mode, the network is offline when all NICs break down.
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 breaks down, 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 break down. Make sure that the switch supports link aggregation and you have configured the link aggregation mode.

8.2.1.2.1 Binding NICs

Procedure

Step 1 Log in to the PC client.

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

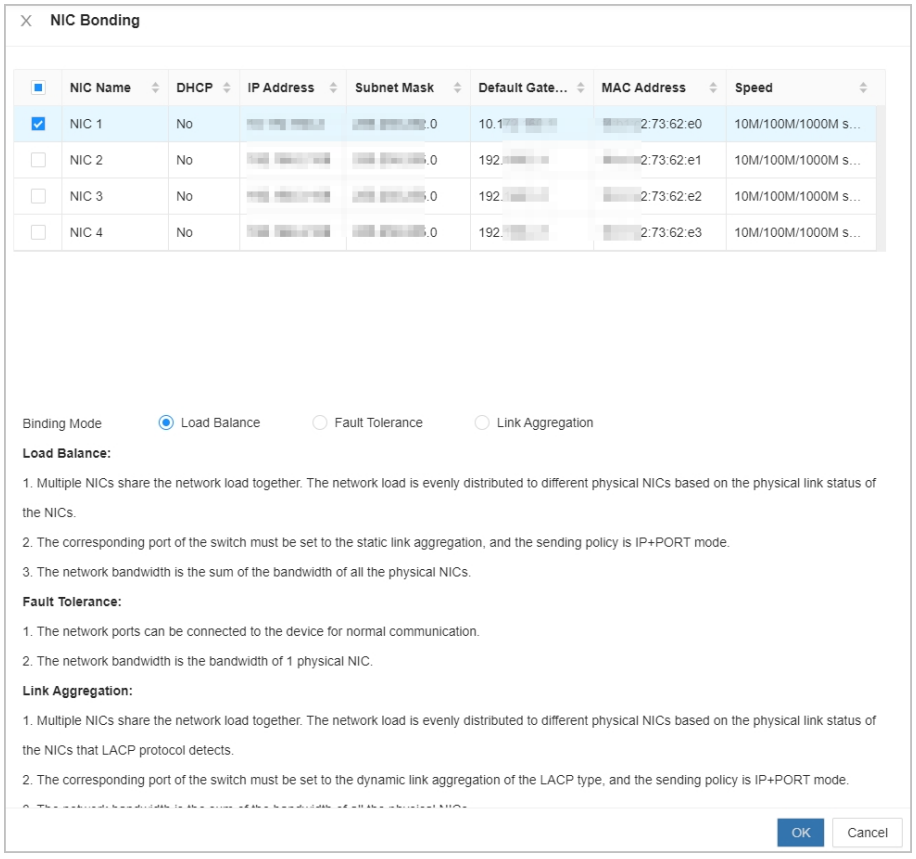
You can also click **Network** from the configuration list on the home page.

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

Step 4 Bind NICs.

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

Figure 8-17 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.

5. Set parameters.

Figure 8-18 Edit load balance

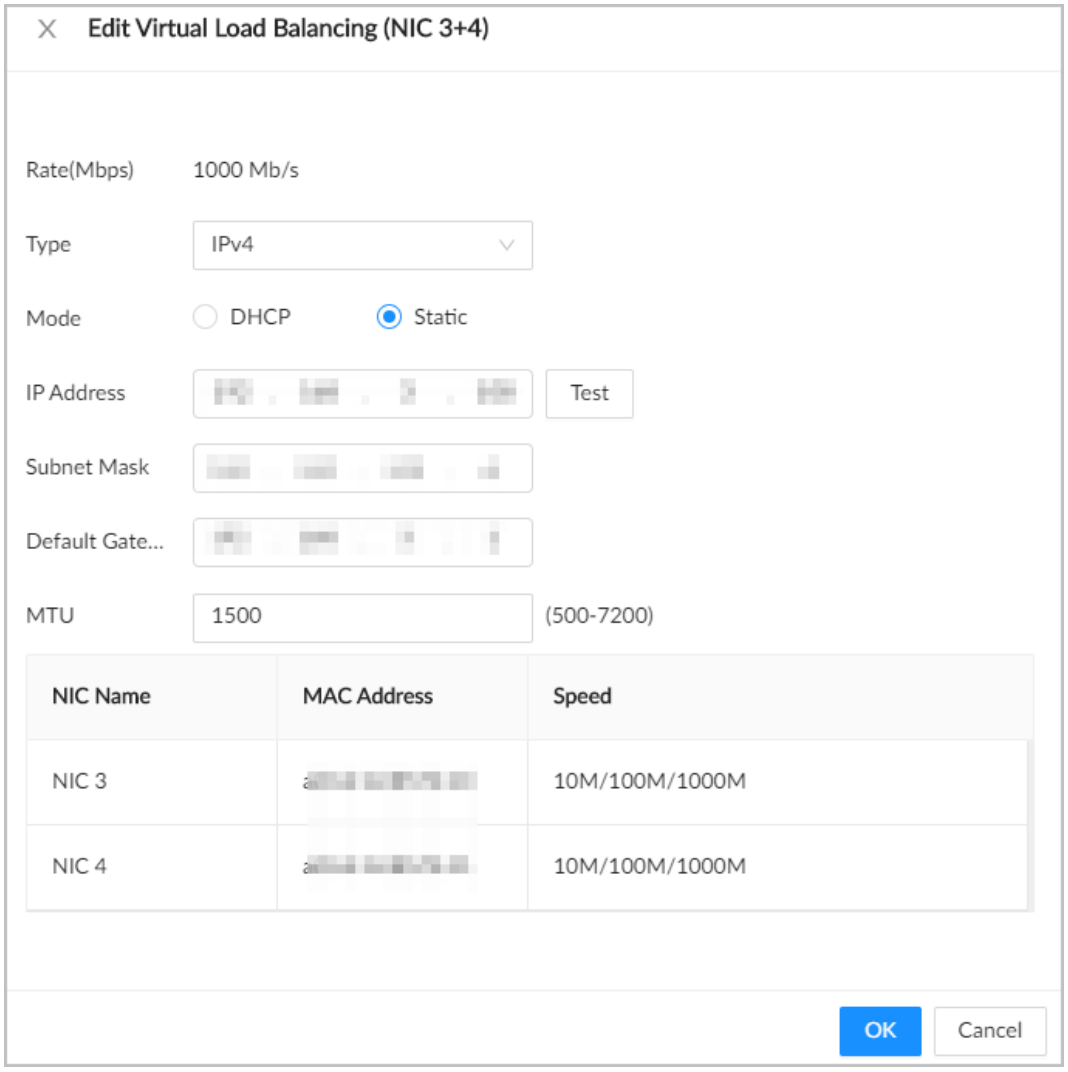


Table 8-7 NIC parameters description

Parameters	Description
Rate (Mbps)	The maximum network transmission speed that the bonded NICs support.
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** : Enter the **IP Address**, **Subnet Mask** and **Default Gateway** to set a static IP address for the Device.
IP Address	
Subnet Mask	
Default 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 to 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 5 Click **Apply**.

The system pops up a confirmation box.

Step 6 Click **OK**.

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

8.2.1.2.2 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.

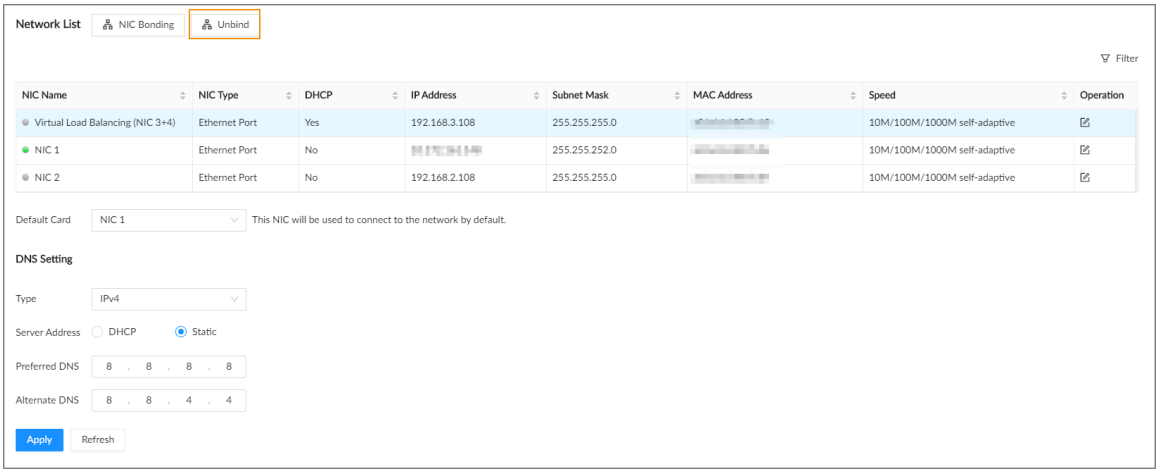
Step 2 Click on the upper-right corner and then click **Network**.

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

Step 3 Select a bonded NIC.

Step 4 Click **Unbind**.

Figure 8-19 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.

8.2.1.3 Setting Port Number

Set device 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 8-20 Port



Step 4 Configure the parameters.

- When you log in via TCP, you do not need to log in again to make you changes in max connection, RTSP port, and UDP port become effective.
- When you log in by 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 8-8 Port parameters 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 according to the actual requirements. The default value is 37777. The value ranges from 1025 to 65535.
RTSP	Set according to the actual requirements. The default value is 554. The value ranges from 1 to 65535.

Parameter	Description
HTTP	Set according to the actual requirements. The default value is 80. The value ranges from 1 to 65535. If the value you set is not 80, remember to add the port number after the IP address when you are using a browser to log in to the device.
HTTPS	Set according to the actual requirements. The default value is 443. The value ranges from 1 to 65535.
UDP	Set 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.

8.2.2 Network Application

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

8.2.2.1 Access Service

8.2.2.1.1 P2P

P2P is a peer to peer technology. You can scan the QR code to download mobile app without DDNS service or the port mapping or installing the transmission server. After you register the Device to the app, you can view the remote videos, play back recorded videos and more.

- Make sure that the Device has connected to the network.
- To use the P2P function, we will collect information such as IP address, MAC address, and serial number. The collected information is only used for remote access.

Procedure

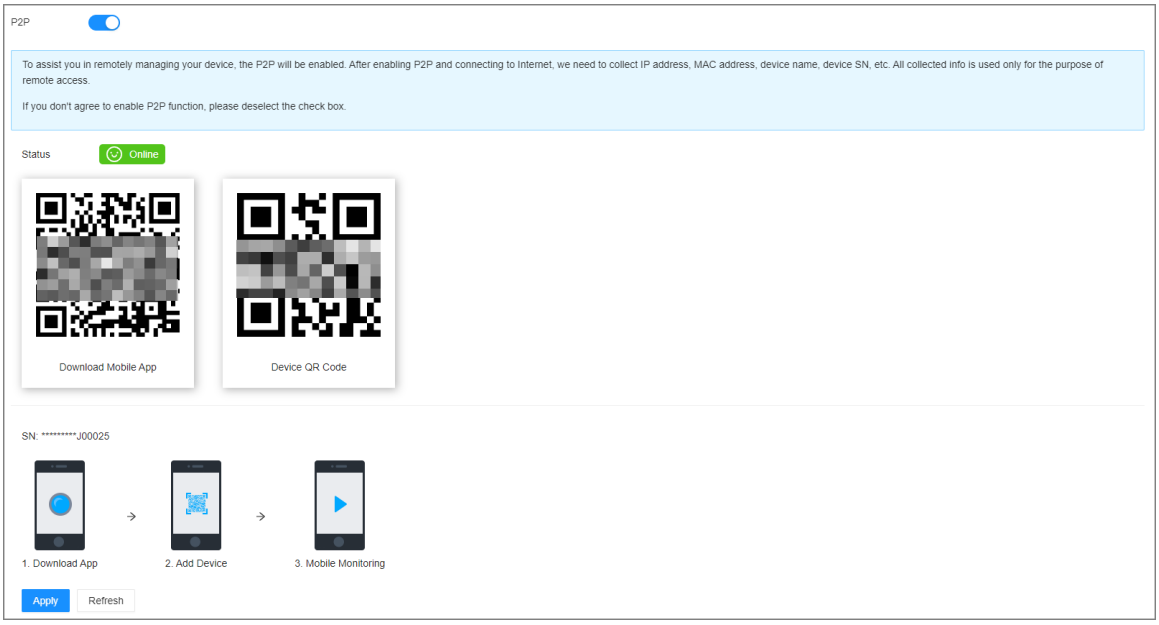
Step 1 Log in to the PC client.

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** > **Access Service**.

Figure 8-21 P2P



Step 4 Click to enable the P2P function.

Step 5 Click **Apply**.

You can register the Device to the app for remote monitoring and management. For details, see the corresponding user's manual of the app.

8.2.2.1.2 GB28181 Server

After enabling the GB28181 service, the device can be connect to the server through the GB28181 protocol. The device also supports connecting the remote device to itself through the GB28181 protocol.

Procedure

Step 1 Log in to the PC client.

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

Step 3 Select **Network Application** > **Access Service** > **GB28181 Server**.

Step 4 Click to enable the function.

The parameter items of the interface must be consistent with the information provided by the server, otherwise it might lead to device registration failure or function failure.

Figure 8-22 GB28181 server

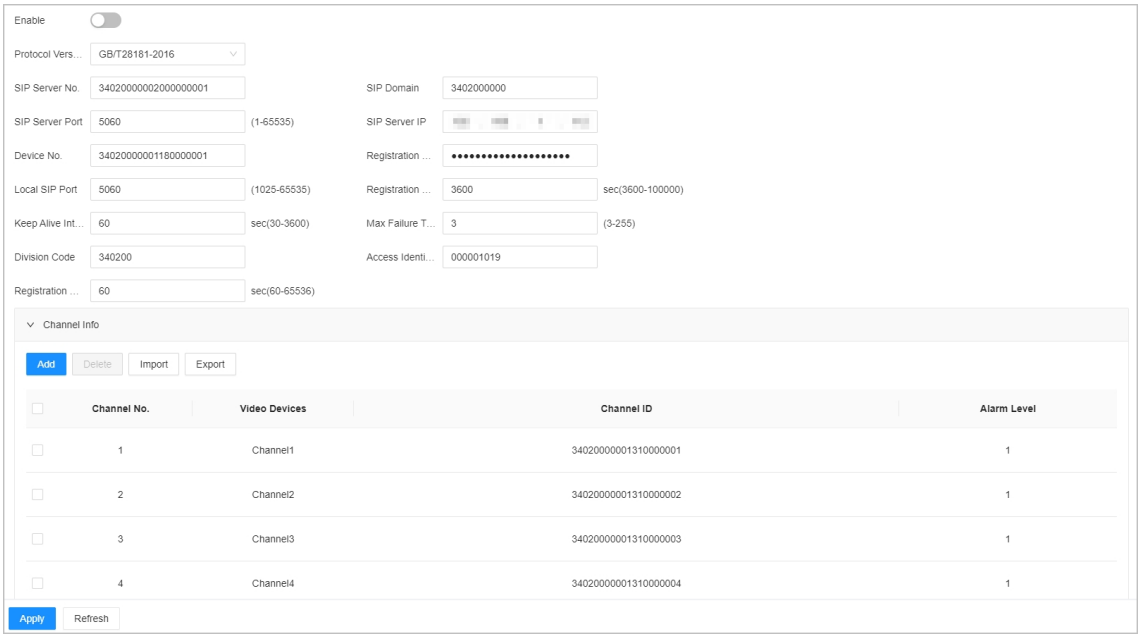


Table 8-9 The description of parameter

Parameter	Description
Protocol Version	Set the protocol version of access.
SIP Server No.	Set the number of the server, the default is 34020000002000000001.
SIP Domain	Set the domain name number of the server, the default is 3402000000.
SIP Server Port	Set the port of the server, the default is 5060.
SIP Server IP	Set the IP address of the server.
Device No.	Enter the device number.
Registration Password	Set the password for the device to register to the server.
Local SIP Port	Set the port for the device to register to the server, the default is 5060.
Registration Validity Period	Set the effective time for each time the device sends a registration message to the server, the default is 3,600 seconds.
Keep Alive Interval	Set the interval between the device to send registration messages to the server, the default is 60 seconds.
Max Failure Times	Set the maximum number of times to allow a heartbeat connection to timeout. When the number of heartbeat connections between the device and the server exceeds this value, the device actively disconnects from the server.
Division Code	Set the administrative division code of the area where the device is located. Fill in according to the actual situation.

Parameter	Description
Access Identification Code	Set the access identification code. The default is 000001019.
Registration Failure Interval	The interval time allowed for re-registration (after a registration failure).

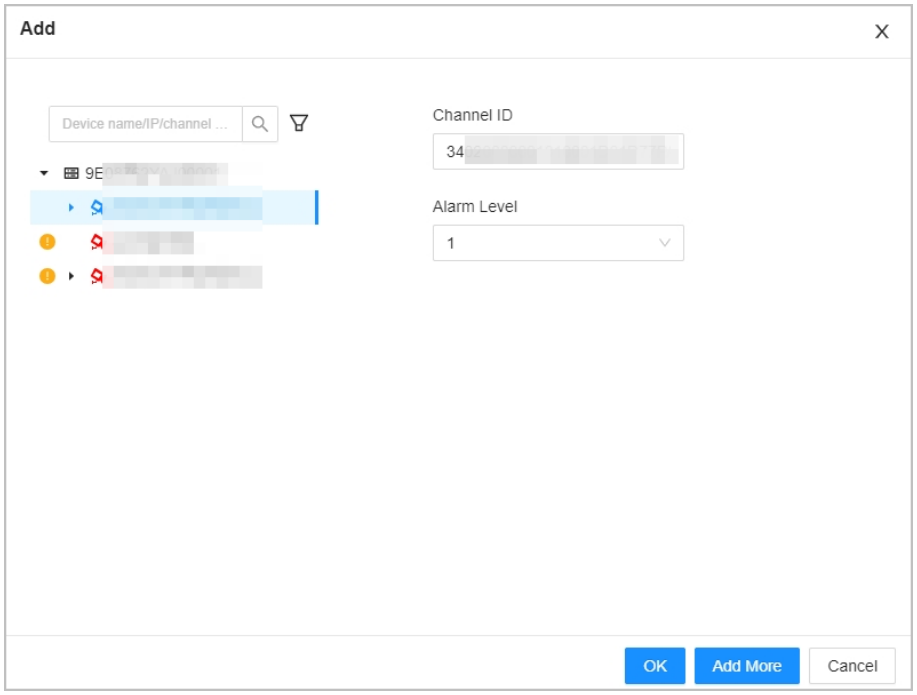
Step 5 Set up channel information.

When the alarm event is triggered, the system automatically uploads the video to the server after adding video information.

1. Click **Add**.
2. Select the device from the list on the left.

   The system automatically generates the channel ID.

Figure 8-23 Add



3. Select **Alarm Level**.

   The alarm level can be set from 1 to 6. The smaller the value, the higher the alarm level.
4. Click **OK**.

Click **Add More** to continue to add video information of multiple remote devices.

After the addition is completed, you can perform the following operations on the added video information.

- Double click **Channel No.** , **Video Devices**, **Channel ID**, **Alarm Level**, and then modify the video information.

  appears after the channel ID indicates that the channel ID is duplicated. Modify the duplicated channel ID.
- Select video information and click **Delete**.

Step 6 Refer to the step 5 to set the alarm information.

Step 7 Click **Apply**.

8.2.2.1.3 GB28181 Client

After opening the GB access, the remote device can be registered to the device through a certain protocol.

Procedure

Step 1 Log in to the PC client.

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

Step 3 Select **Network Application** > **Access Service** > **GB28181 Client**.

Step 4 Click to enable the function.

Step 5 Set the parameters.

The parameters of the interface must be consistent with the information provided by the server, otherwise it might lead to device registration failure or function failure.

Figure 8-24 GB28181 client

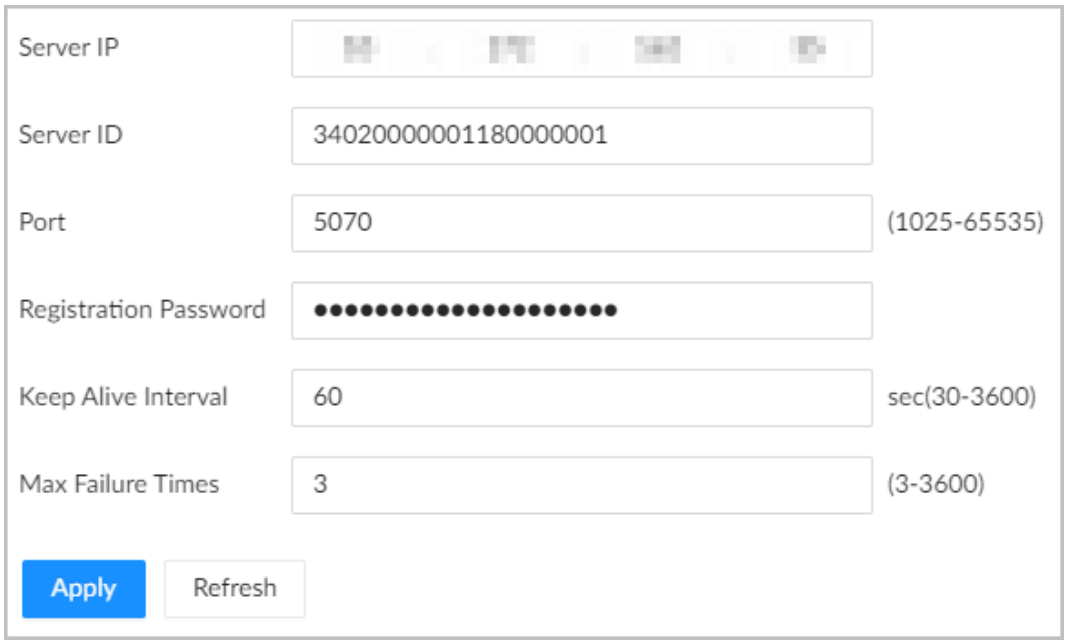


Table 8-10 The description of parameter

Parameter	Description
Server IP	After selecting the network card, the Device will automatically fill in the IP address corresponding to the network card. When the device IP address changes, the GB server needs to be reconfigured.
Server ID	Set the ID of the server.

Parameter	Description
Port	Set the port of the server. The default is 5070.
Registration Password	Set the password for the device to register to the server.
Keep Alive Interval	Set the interval for the device to send registration messages to the server. The default is 60 seconds.
Max Failure Times	Set the maximum number of times to allow a heartbeat connection to timeout. When the number of heartbeat connections between the device and the server exceeds this value, the device actively disconnects from the server.

Step 6 Click **Apply**.

8.2.2.1.4 RTMP

The Device connects with a third-party platform through the RTMP protocol to achieve video live broadcast.

Background Information

- Only admin user supports configuring **RTMP**.
- **RTMP** only supports H.264, H.264B and H.264H video formats, as well as AAC audio formats.

Procedure

Step 1 Log in to the PC client.

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

Step 3 Select **Network Application** > **Access Service** > **RTMP**.

Step 4 Select channel, and then click  to enable RTMP.



When the function is enabled, make sure the address filled in is trustworthy.

Step 5 Set the parameters.

Figure 8-25 RTMP

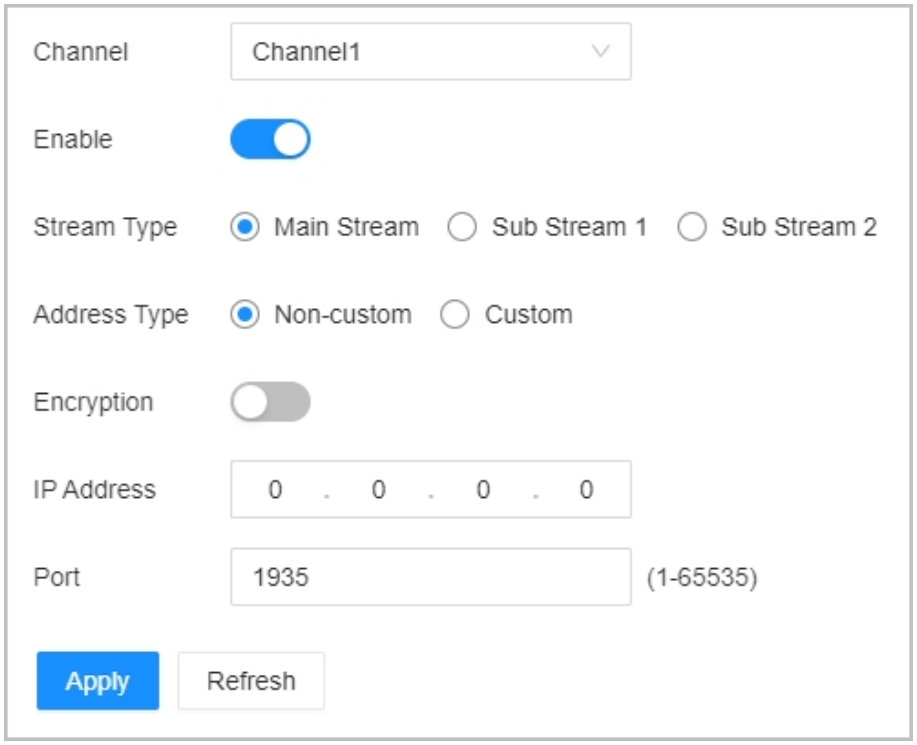


Table 8-11 The description of parameter

Parameter	Description
Stream Type	Select the type of stream of the live broadcast. Make sure that video format is H.264, H.264B or H.264H and audio format is AAC of the stream. When the device IP address changes, the GB server needs to be reconfigured.
Address Type	Including non-custom and custom. • Non-custom: Fill in the server IP. • Custom: Fill in the path assigned by the server.
Encryption	Select **Non-custom** and it supports enablement of data encryption.
IP Address	Select **Non-custom** and it needed to be filled in the IP address and port of the server.
Port	

Step 6 Click **Apply**.

8.2.2.1.5 ONVIF

The Device integrate with third-party platforms through the ONVIF protocol.

Procedure

Step 1 Log in to the PC client.

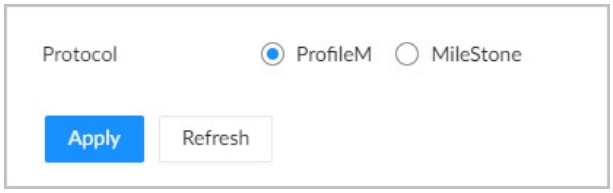
Step 2 Click on the upper-right corner, and then click **Network**.

Step 3 Select **Network Application** > **Access Service** > **ONVIF**.

Step 4 Select the type of the protocol.

- ProfileM: When the other party uses ONVIF protocol for authentication, select this protocol.
- MileStone: When the other party is the Milestone platform, select this protocol.

Figure 8-26 ONVIF



Step 5 Click **Apply**.

8.2.2.2 Auto Registration

Register the Device on a designated proxy server so that client software can access the Device through the proxy server.

Procedure

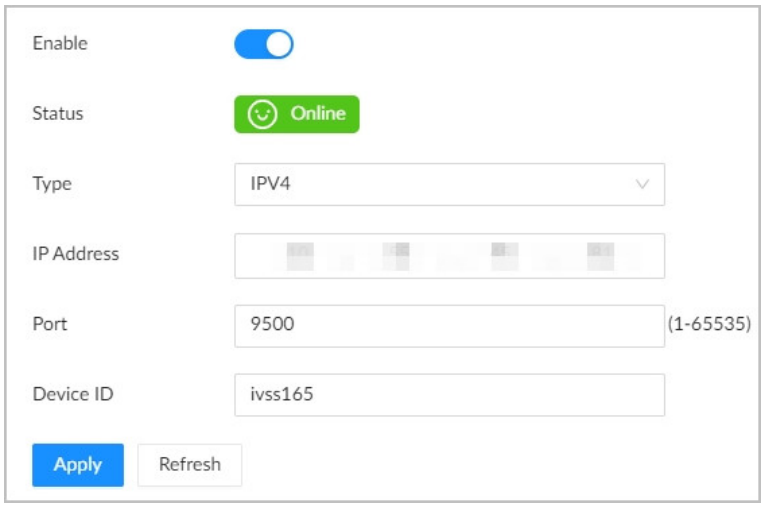
Step 1 Log in to the PC client.

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** > **Auto Registration**.

Figure 8-27 Register



Step 4 Click to enable the function.

Step 5 Set parameters.

Table 8-12 Register

Parameter	Description
Type	Select an IP type from **IPv4** and **IPv6**.
IP Address	Enter the IP address of the server that you are registering the Device to.
Port	Enter the port number of the server for registration.
Device ID	Customize the ID for the Device.

Step 6 Click **Apply**.

8.2.2.3 Email

Configure email information. When an alarm event linked with email occurs, the system automatically sends emails to the user.

Please be advised that device data will be sent to specific servers after the email function is enabled.

Procedure

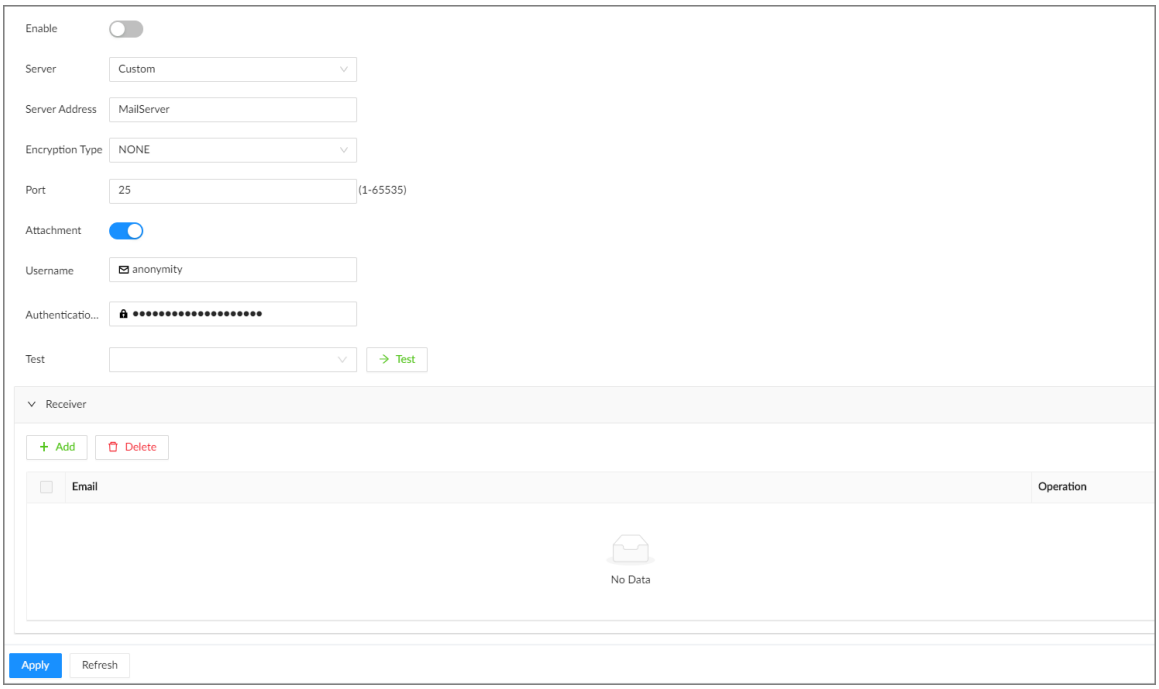
Step 1 Log in to PC client.

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** > **Email**.

Figure 8-28 Email



Step 4 Click to enable the email function.

Step 5 Set parameters.

Table 8-13 Emails parameter description

Parameter	Description
Server	Select a server type from **Custom** , **Gmail**, **Hotmail**, and **Yahoo Mail**.
Server Address	Enter the address of the email server.
Encryption	Select an encryption type from **NONE** , **SSL**, and **TLS**. We recommend you select TLS. Other encryption methods might not be safe.
Port	Enter the port number of the email server.
Attachment	Click to allow the system to send emails with attachments.
Username	Enter the configured user name and password of the email server.
Authentication Password	

Step 6 Add the information of mail receiver.

1. Click **Add**.
2. Enter the email address of the receiver.
3. Click **Add** to add more receiver email addresses.
   - Click to delete the added receiver.
   - Select a receiver and then click **Delete** to delete the selected receiver.

Step 7 Click **Apply**.

Step 8 (Optional) Test the email sending function.

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

8.2.2.4 Alarm Center

Configure the alarm center server. After events linked with alarm upload occur, the system uploads alarm information to the alarm center.

Make sure that alarm center server is deployed.

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** > **Alarm Center**.

Step 4 Select **Upload Mode** , click next to **Enable** to enable alarm center.

- **Private Protocol** : Access the alarm center through SDK.
- **HTTP/HTTPS** : Access the alarm center through HTTP or HTTPS, and then upload the alarm information, images and reports to the alarm center.

Step 5 Configure the parameters.

Figure 8-29 Alarm center (Private protocol)

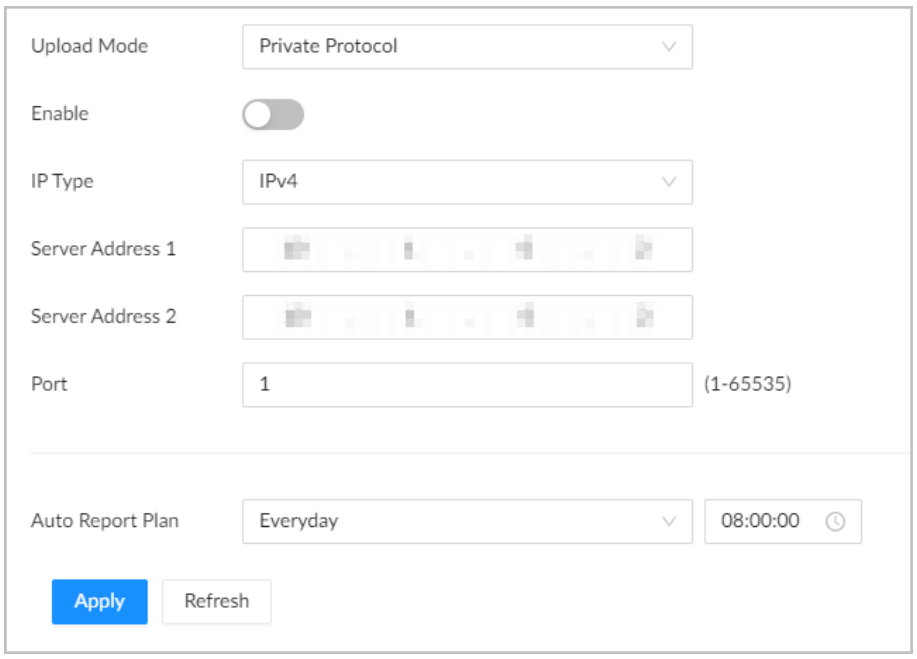


Table 8-14 Alarm center (Private protocol) parameters

Parameter	Description
IP Type	Select the IP type of the server address (IPv4 or IPv6). The default IP type is **IPv4**.
Server Address 1	Enter the server IP address to register.
Server Address 2	
Port	Enter the port number for active server registration.
Auto Report Plan	Select the alarm reporting cycle from the drop-down list, and then set the specific time.

Figure 8-30 Alarm center (HTTP/HTTPS)



Table 8-15 Alarm center (HTTP/HTTPS) parameters

Parameter	Description
Device ID	Set the identifier of the current device, used by the alarm center to identify the alarm source.
Type	Select the IP type of the server address (IPv4 or IPv6). The default IP type is **IPv4**.
Server Address 1	Enter the IP address or domain name of the connected alarm center server.
Server Address 2	
Port	Enter the port number for active server registration.

Parameter	Description
HTTPS	Once HTTPS (Hypertext Transfer Protocol Secure) is enabled on the device, all communication data will be encrypted to ensure the security of data during transmission.
Authentication	When enabled, the device will include authentication credentials in upload requests, allowing the server to verify request authenticity. Authentication is disabled by default. You must enable with a user name and password set when HTTPS is activated.
Keep-alive Interval	Set the heartbeat packet transmission interval between device and alarm center, used to keep persistent connection from timing out. **0** means no heartbeat packets will be sent.
Image Upload Path	Relative path prefix for image uploads, used to organize file storage structure and must start with **/**.

Step 6 Click **Apply**.

After completing the configuration, click **Test** to verify the network reachability of the server.

8.2.2.5 UPnP

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

Prerequisites

- Make sure that your computer has been installed with UPnP network services.
- Log in to the router and set the WAN port IP address of router.
- Enable the UPnP function on the router.
- Connect the Device to the LAN port of the router.
- Select **Network** > **Basic Network** > **TCP/IP**, and then set the IP address to the LAN IP of the router, or select DHCP to automatically obtain the IP address.

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

Procedure

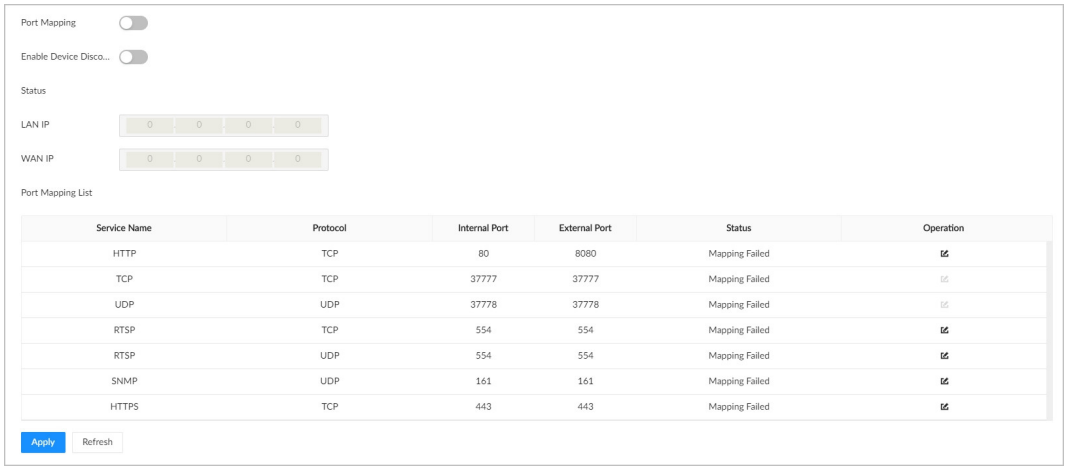
Step 1 Log in to the PC client.

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** > **UPnP**.

Figure 8-31 UPnP



Step 4 Set parameters.

Table 8-16 UPnP parameters

Parameter	Description
Port Mapping	Click to enable port mapping.
Enable Device Discovery	After enabling, it supports searching for devices through the network neighborhood on the PC. The serial number is the device name.
Status	The status of port mapping.
LAN IP	The LAN IP address of the router. The IP address is automatically obtained after the mapping succeeds.
WAN IP	The WAN IP address of router. The IP address is automatically obtained after the mapping succeeds.
Port Mapping List	The list is consistent with the UPnP port mapping list on the router. • **Internal Port** : The ports of the IVD to be mapped on the router. • **External Port** : The ports mapped on the router. Click , and then you can modify the external ports. • When setting the external port, use the ports between 1024 and 5000, and do not use the well-known ports 1 to 255 and the system ports 256 to 1023, otherwise conflicts might occur. • When there are multiple devices on the LAN, properly plan the port mapping to avoid conflicts in WAN ports. • When making a port mapping, make sure that the port you are mapping is not occupied or restricted. • The TCP/UDP WAN and LAN ports must be consistent and cannot be modified.

Step 5 Click **Apply**.

Enter http://*WAN IP: WAN port number* in the browser to access the Device with the corresponding port number on the router network.

8.2.2.6 SNMP

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

Prerequisites

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

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** > **SNMP**.

Step 4 Click  to enable the function.

Step 5 Select SNMP version.

SNMP V1/V2 has security risks. For data security, we recommend you to use **SNMP V3**.

Step 6 Set parameters. For **Trap Address**, enter the IP address of the computer installed with the MG-SOFT MIB Browser, and then keep the other parameters as default.

Figure 8-32 SNMP

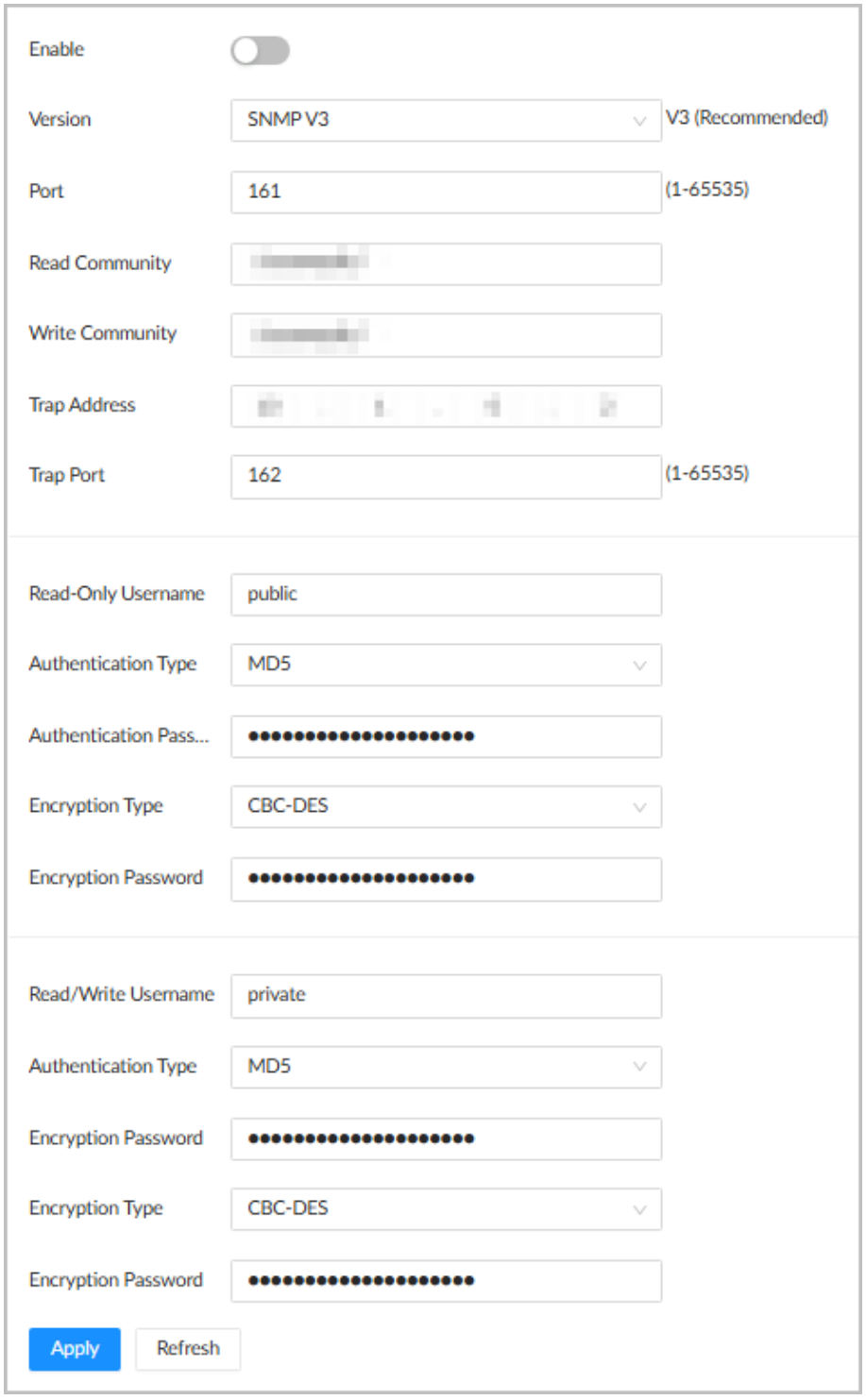


Table 8-17 SNMP parameters

Parameter	Description
Port	The listening port of agent programs on the device.

Parameter	Description
Read Community	The read or write community supported by the agent programs. The name can only contain numbers, letters, underscores, and middle lines.
Write Community	
Trap Address	The destination address of trap information sent by the agent program.
Trap Port	The destination port of trap information sent by the agent program.
Read-Only User Name	Set the read-only user name for device access. It is **Read-Only Username** by default. The read-only user only has the read-only permission. The name can only contain numbers, letters, and underscores.
Authentication Type	You can select the read authentication type between MD5 and SHA. It is MD5 by default.
Authentication Password	Enter the read authentication password. The password must contain at least 8 digits.
Encryption Type	Set the read encryption type. It is CFB-AES by default.
Encryption Password	Set the read encryption password. The password must contain at least 8 digits.
Read/Write User Name	The user name is private by default. If you log in using this user name, you have the read-and-write permission. The name can only contain numbers, letters, and underscores.
Authentication Type	You can select the read-and-write authentication type from **MD5** or **SHA**. It is **MD5** by default.
Authentication Password	Enter the read-and-write authentication password. The password must contain at least 8 digits.
Encryption Type	Select a read-and-write encryption type. It is **CFB-AES** by default.
Encryption Password	Enter a read-and-write encryption type. The password must contain at least 8 digits.

Step 7 Click **Apply**.

8.2.2.7 Multicast

When multiple users are viewing live video of the same device at the same time, it might cause failure due to limited bandwidth. To solve this problem, you can set a multicast IP address (224.100.0.0–239.200.255.255) for the Device.

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** > **Multicast**.

Step 4 Click to enable multicast.

Step 5 Set parameters.

Table 8-18 Multicast parameter

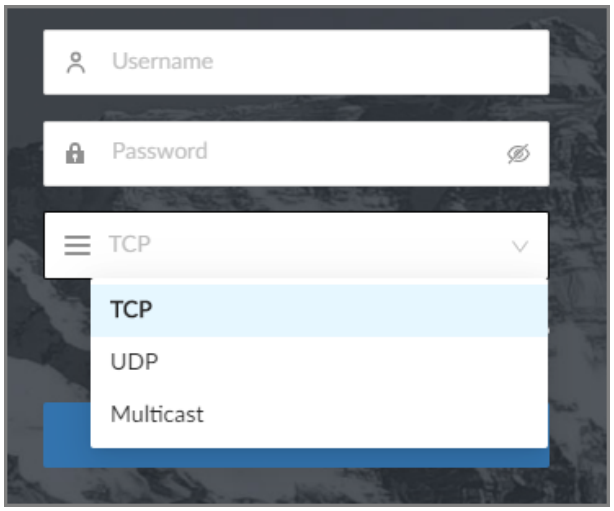
Parameter	Description
IPV4/IPV6	Select an IP type and then enter the IP address Enter the IP address that you want to use as the multicast IP.
IP Address	
Port	Set the multicast port.

Step 6 Click **Apply**.

After configuring the multicast address and port, you can log in to the web interface or the PC client via multicast.

For example, on the login page of the PC client, select **Multicast** as the login type. The PC client will automatically obtain the multicast address and join the multicast group. After login, you can view live videos through multicast protocol.

Figure 8-33 Log in through multicast



8.2.2.8 DDNS

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

Prerequisites

Check the type of DDNS that the Device supports and then log in to the website provided by the DDNS service provider to register domain and other information.

After registration, you can log in to the DDNS website to view the information of all the connected devices under the registered account.

Procedure

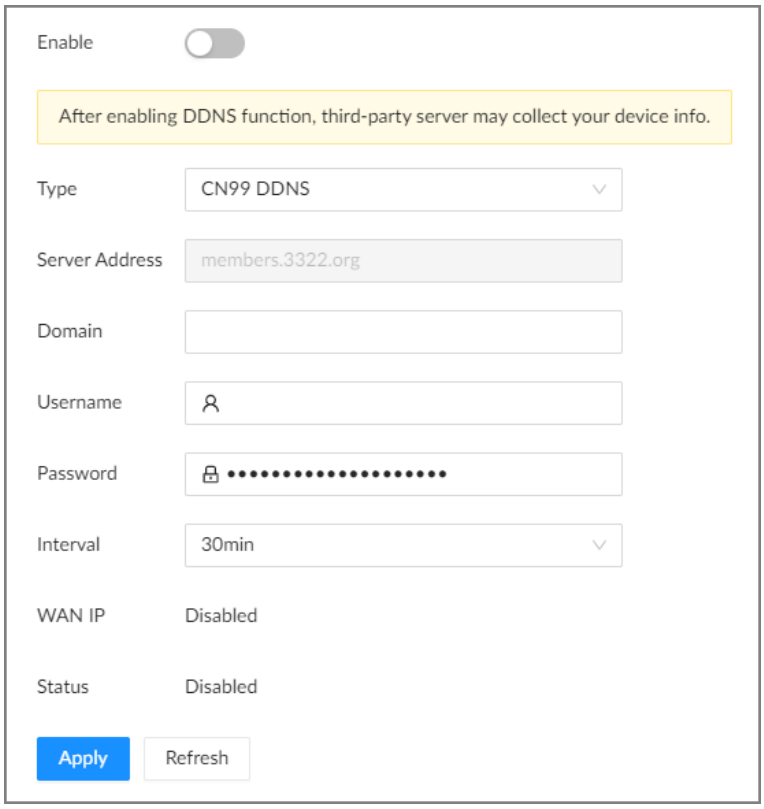
Step 1 Log in to the PC client.

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** > **DDNS**.

Figure 8-34 DDNS



Step 4 Click to enable the DDNS function.

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

Step 5 Set the parameters.

Table 8-19 DDNS parameters

Parameters	Description
Type	Select the type of the DDNS service provider and then corresponding address displays. • Dyndns DDNS: members.dyndns.org • NO-IP DDNS: dynupdate.no-ip.com • CN99 DDNS: members.3322.org
Server Address	
Domain	Enter the domain name that you have registered on the DDNS website.

Parameters	Description
Username	Enter the user name and password obtained from DDNS service provider. You need to register (including user name and password) on the website of DDNS service provider in advance.
Password	
Interval	Enter the interval at which you want to update the DDNS.
WAN IP	Displays the WAN IP address of IVD.
Status	Displays DDNS registration result or update status.

Step 6 Click **Apply**.

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

8.2.2.9 Routing Table

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.

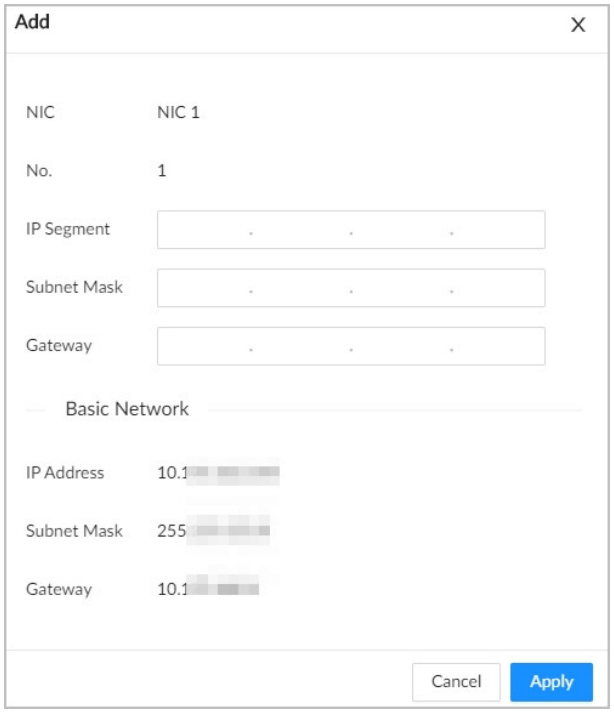
Step 2 Click  on the upper-right corner and then click **Network**.

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 8-35 Add route table



Step 5 Configure the parameters.

Step 6 Click **Apply**.

8.2.2.10 VPN

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** > **VPN**.

Step 4 Configure the parameters.

Figure 8-36 VPN

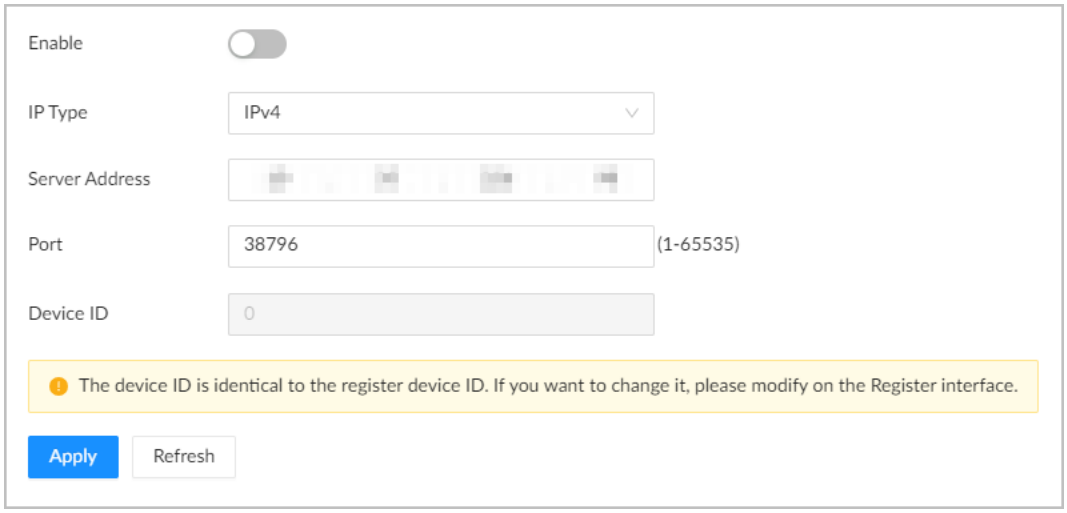


Table 8-20 VPN parameters

Parameters	Description
IP Type	Select the IP type (IPv4 or IPv6). The default IP type is **IPv4**.
Server Address	Enter the IP address or domain name of the connected VPN server.
Port	Enter the port number used when communicating with the VPN server.
Device ID	Set the identifier of the current device, used by the VPN server to identify the Device.

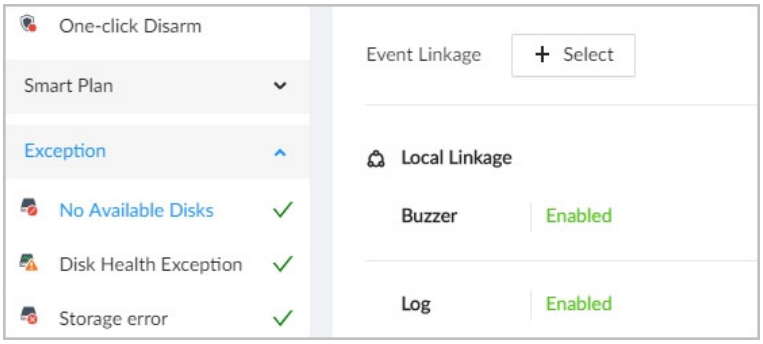
Step 5 Click **Apply**.

8.3 Event Management

Log in to the PC client. Click on the upper-right corner, and then click **Event**. On this page, you can configure alarm events for the Device and remote devices.

Different devices support different alarm event settings; refer to the actual page for confirmation.

Figure 8-37 Event management

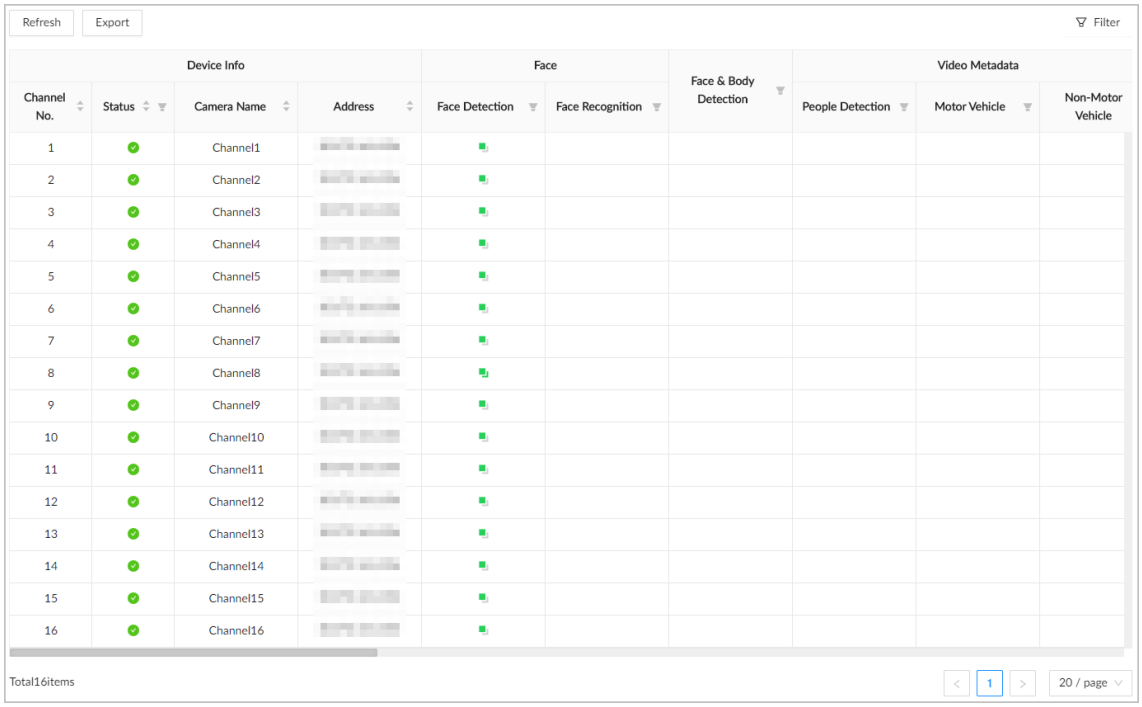


8.3.1 Overview

Log in to the PC client. Click on the upper-right corner, and then click **Event** . Select the root node on the left device tree, and then select **Overview**.

- The alarm event 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.
- Click **Export** to export the overview information locally.

Figure 8-38 Overview



8.3.2 Batch Configuring Events

Supports batch configuring events.

Procedure

Step 1 Log in to the PC client.

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

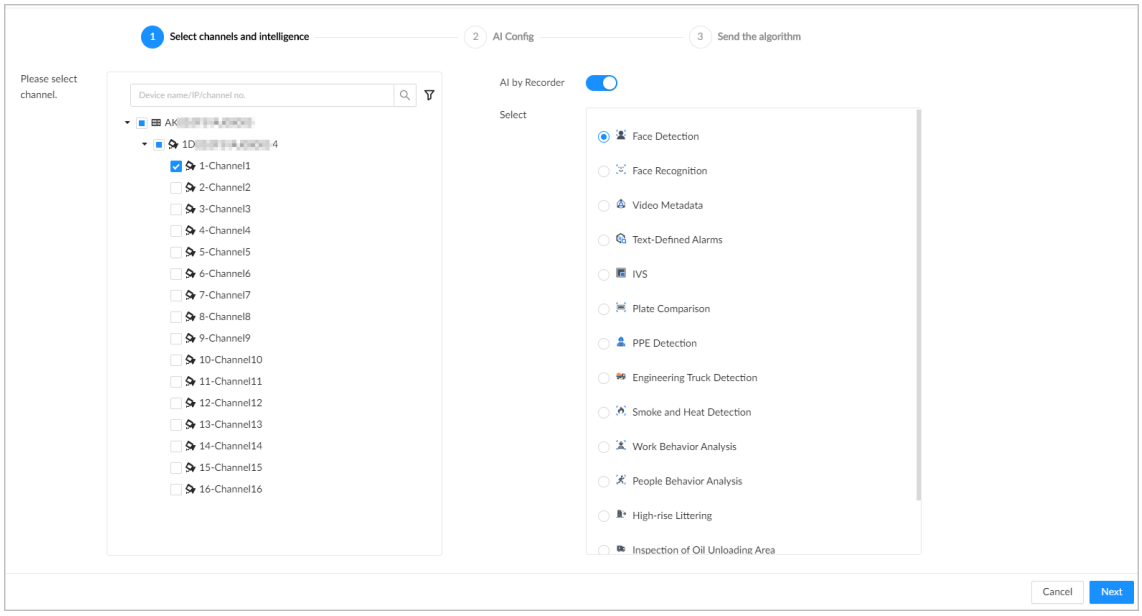
You can also click **Event** from the configuration list on the home page.

Step 3 Click **Overview** > **Batch Config**.

Step 4 Select the channels, enable or disable **AI by Recorder** , select the AI operation, and then click **Next**.

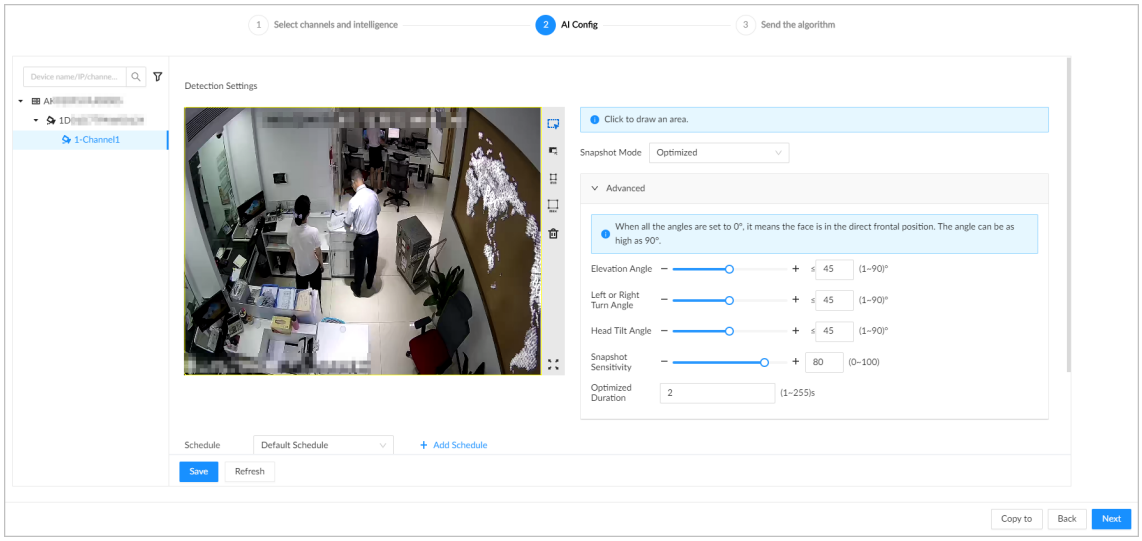
- Channels: Select the root node on the left device tree to set the alarm events for the Device.
- Operation: Click next to **AI by Recorder** to manually enable or disable the alarm events in batches.

Figure 8-39 Select channels and intelligence



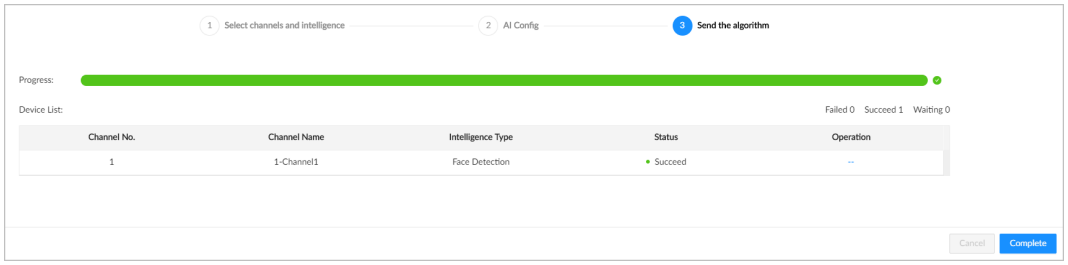
Step 5 Configure the intelligent rules for each channel. For more information about parameters, see the configuration chapter of AI application.

Figure 8-40 AI configuration



Step 6 Click **Complete** after the distribution is completed.

Figure 8-41 Send the algorithm



8.3.3 Alarm Actions

The system triggers the corresponding actions when an alarm occurs.

The supported actions might be different depending on the AI function.

On the alarm configuration page, click **Select** next to **Event Linkage** to select linkage actions. Configure actions according to your actual need.

Table 8-21 Actions description

Action	Description	Preparation
Record	The system links the selected remote device to record videos when a linkage event occurs.	A remote device, such as an IPC, has been added.
Buzzer	The system activates a buzzer alarm when a linkage event occurs.	—
Log	The system logs the alarm information in the log when a linkage event occurs.	

Action	Description	Preparation
Send Email	The system sends alarm email to all added recipients when a linkage event occurs.	Email configuration has been completed.
Report Alarm	When a linkage event occurs, the system reports the alarm to the alarm center.	The alarm center has been enabled.
Local Alarm Output	When a linkage event occurs, the alarm output device connected with the Device generates the corresponding alarm when a linkage event occurs.	The Device is connected with an alarm output device.
Remote Device Alarm Output	When a linkage event occurs, the system links the corresponding remote alarm output device to generate an alarm when a linkage event occurs.	The remote device has been added, and the remote device is connected with an alarm output device.
Audio Linkage	When a linkage event occurs, the system plays the selected audio file.	The audio function has been configured.
Alarm Window Pop Up	When a linkage event occurs, the system pops up the live view window.	The alarm window pop up function is enabled in the **Display** page.
Send Command	When a linkage event occurs, the system sends customized commands to the connected platform.	Connected to a third-party platform.
Preset	When a linkage event occurs, the system links the selected remote device to rotate to the designated preset point.	The PTZ device has been added, and a preset point has been added.
Camera Audio	When a linkage event occurs, the system triggers linked audio playback on the camera.	IPC devices supporting audio playback function have been added.
Picture Storage	• AI by Camera: When a linkage event occurs, the front-end device captures images, and then saves them on the Device. • AI by Recorder: When a linkage event occurs, the system links corresponding channels to snap images, and then stores the images on the Device.	—

Action	Description	Preparation
Remote Warning Light	When a linkage event occurs, the system links remote devices, and then triggers the remote warning lights alarm.	IPC devices supporting remote warning light alarms have been added.
Access Control	When a linkage event occurs, the system links the corresponding access control device to open and close doors.	The access control device has been added.
Smart Tracking	When a linkage event occurs, the linked camera automatically rotates to track the target.	—

8.3.3.1 Record

Enable the record control function. The system links the selected remote device to record when a linkage event occurs.

Make sure that a remote device, such as IPC, has been added.

Procedure

Step 1 On the alarm configuration page, click **Select** next to **Event Linkage**, and then select **Record**.

Figure 8-42 Record



Step 2 Set the time length of recording after the event moment.

Step 3 In the **Device** box, select one or more remote devices for linkage recording.

Step 4 Click **Save**.

8.3.3.2 Buzzer

Enable the buzzer function. The system activates a buzzer alarm when a linkage event occurs.

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

Figure 8-43 Buzzer



8.3.3.3 Log

Enable the log function. The system logs 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 **Save**.

After the log function is enabled, you can select **Maintain** > **Log Info** > **Event Logs** on the home page to search for logs.

8.3.3.4 Email

Enable the email function. The system sends alarm email to all added recipients when a linkage event occurs.

Make sure that the email configuration has been completed. For details, see "8.2.2.3 Email".

On the alarm configuration page, click **Select** next to **Event Linkage**, select **Send Email**, and then click **Save**.

8.3.3.5 Report Alarms

Enable the alarm upload function. When a linkage event occurs, the system reports the alarm to the alarm center.

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

Make sure that alarm center has been enabled. For details, see "8.2.2.4 Alarm Center".

8.3.3.6 Local Alarm Output

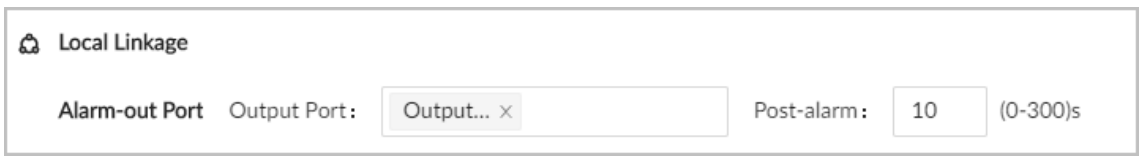
Enable the local alarm output function. The alarm output device connected with the Device generates the corresponding alarm when a linkage event occurs.

Make sure that the Device is connected with an alarm output device.

Procedure

Step 1 On the alarm configuration page, click **Select** next to **Event Linkage**, and then select **Alarm-out Port**.

Figure 8-44 Local alarm output



Step 2 Select one or more alarm output ports.

Step 3 In the **Post-alarm** box, configure the length of time for the alarm to continue after the event ends.

Step 4 Click **Save**.

8.3.3.7 Remote Device Alarm Output

Enable the remote device alarm output function. The system links the corresponding remote alarm output device to generate an alarm when a linkage event occurs.

Make sure that the remote device has been added, and the remote device is connected with an alarm output device.

Procedure

Step 1 On the alarm configuration page, click **Select** next to **Event Linkage**, and then select **Remote Device Alarm Output**.

Figure 8-45 Remote device alarm output



Step 2 Select a remote device and then select one or more alarm output ports.

Step 3 Click to link multiple remote alarm output devices.

8.3.3.8 Audio Linkage

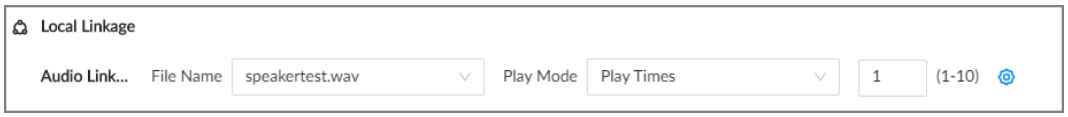
Enable the audio linkage function. The system plays the selected audio file when a linkage event occurs.

Make sure that the audio function has been configured. For details, see "7.4 Audio Management".

Procedure

Step 1 On the alarm configuration page, click **Select** next to **Event Linkage**, and then select **Audio Linkage**.

Figure 8-46 Audio linkage



Step 2 Select the audio file and then set the play mode.

- **Play Times** : After the event ends, the system continues to play the audio file according to the play times.
- **Duration** : After the event ends, the system continues to play the audio file according to the duration.

You can click to go to the **Audio** page where you can configure the audio files.

Step 3 Click **Save**.

8.3.3.9 Alarm Window Pop Up

Enable the alarm window pop up function. The system pops up the live view window when a linkage event occurs.

Procedure

Step 1 On the alarm configuration page, click **Select** next to **Event Linkage**, and then select **Alarm Window Pop Up**.

Step 2 Select the linked channel from the drop-down list.

Make sure the alarm window pop up function is enabled in **Display** page. For details, see Table 8-36 . You can also click to configure.

Step 3 Click **Save**.

8.3.3.10 Send Command

Enabled the send command function. The system sends customized commands to the connected platform when a linkage event occurs.

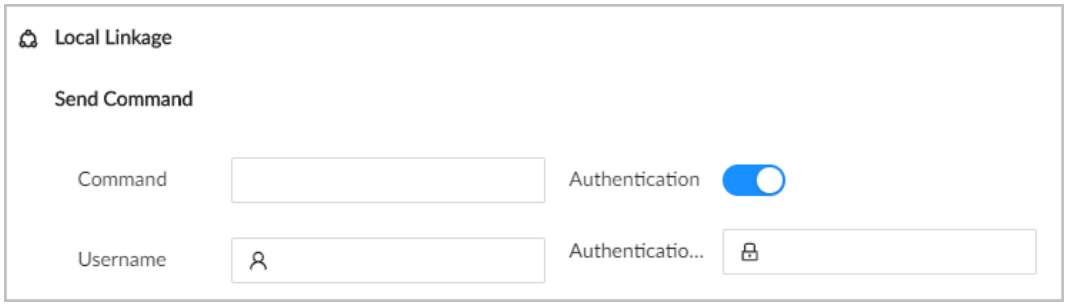
Procedure

Step 1 On the alarm configuration page, click **Select** next to **Event Linkage**, and then select **Send Command**.

Step 2 Configure the parameters.

- Customize the command content.
- (Optional) Click next to **Authentication**, and then enter the user name and authentication password of the third-party platform.

Figure 8-47 Send command



- Make sure that the third-party platform has been connected.
- The command format is determined by the connected third-party platform.
- When authentication is enabled, you must enter the user name and authentication password of the third-party platform.

Step 3 Click **Save**.

8.3.3.11 Preset

Enabled the preset function. The system links the selected remote device to rotate to the designated preset point when a linkage event occurs.

Make sure that the PTZ device has been added, and preset has been added.

Procedure

Step 1 On the alarm configuration page, click **Select** next to **Event Linkage**, and then select **Preset**.

Figure 8-48 Preset



Step 2 Select a PTZ device, and then enter the preset number.

Step 3 (Optional) Click to link multiple PTZ devices to turn to designated presets.

Step 4 Click **Save**.

8.3.3.12 Camera Audio

Enable the camera audio function. The system triggers linked playback of audio on the camera when a linkage event occurs.

Procedure

Step 1 Click **Select** next to **Event Linkage**, select **Camera Audio**, and then click **Save**.

Figure 8-49 Camera audio



Step 2 Select the camera and the file, and then set the play mode.

Step 3 Click **Save**.

8.3.3.13 Picture Storage

Enable the picture storage linkage function. A snapshot is taken and saved on the Device when a linkage event occurs.

When AI by Camera is used, make sure that the remote device has been configured with snapshot linkage.

On the alarm configuration page, click **Select** next to **Event Linkage**, select **Picture Storage**, and then click **Save**.

8.3.3.14 Remote Warning Light

Background Information

Enable the linkage remote warning light function. The system associates with the remote device to turn on the warning light when a linkage event occurs.

Remote warning light is available when AI by camera is used for IVS detection and the camera supports this function.

Procedure

Step 1 On the alarm configuration page, click **Select** next to **Event Linkage**, and then select **Remote Warning Light**.

Step 2 Select the remote device and then set the duration.

Step 3 Click **Save**.

8.3.3.15 Access Control

Enable the access control function. The system links the corresponding access control device to open door and close door when a linkage event occurs.

Make sure that the access control device has been added.

Procedure

Step 1 On the alarm configuration page, click **Select** next to **Event Linkage**, and then select **Access Control**.

Step 2 Select an access control device.

For some access controls devices, you can select channels.

Step 3 (Optional) Click to link multiple access control devices.

Step 4 Click **Save**.

8.3.3.16 Smart Tracking

Enable the smart tracking function. The linked PTZ camera automatically rotates to the target to track it when a tripwire or intrusion event occurs.

- Smart tracking is only available for AI by Camera.
- Smart tracking is only available on the multi-sensor panoramic camera + PTZ camera.

On the alarm configuration page, click **Select** next to **Event Linkage**, select **Smart Tracking**, and then click **Save**.

8.3.4 Local Device

You can set alarms for system errors, system offline, configure smart plans, and more.

8.3.4.1 One-click Disarming

Disarm alarm linkage actions as needed to avoid interference caused by alarms.

Procedure

Step 1 Log in to the PC client.

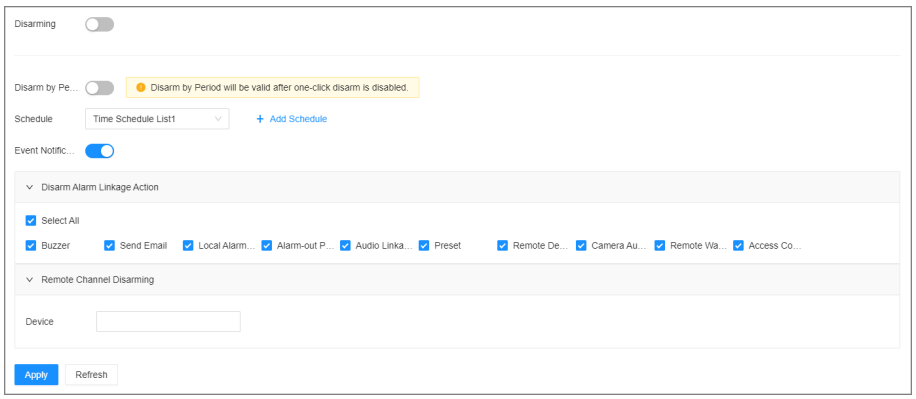
Step 2 Click on the upper-right corner, and then click **Event**.

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 **Overview** > **One-click Disarm**.

Figure 8-50 Disarming



Step 5 Click to enable disarming.

Step 6 Cancel the selection of alarm linkage actions as needed.

Step 7 (Optional) Configure disarming by period.

1. Click to enable disarming by period.
2. Click **Add Schedule** to add a disarming schedule. The alarm linkage actions remain armed during periods beyond the disarming schedule.
3. Click **Apply**.

After disarming by period is enabled, one-click disarming is disabled automatically.

Step 8 Configure remote channel disarming.

1. Click the **Device Name** list in the **Remote Channel Disarming** section. The remote devices that support one-click disarming are displayed.
2. Select the device that you want to synchronize the disarming configuration with.

Step 9 Click **Apply**.

8.3.4.2 Abnormal Events

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

Table 8-22 Abnormal events

Name	Description
No Available Disk	The system triggers an alarm when there is no available disk. It is enabled by default.
SSD health exception	The system triggers an alarm when SSD health exception occurs.
Storage error	The system triggers an alarm when disk error occurs. It is enabled by default.
Low disk space warning	The system triggers an alarm when the used storage space reaches the predefined threshold. It is disabled by default.
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 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 **System** > **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.
Fan speed exception	When the fan speed is abnormal, the system triggers an alarm. It is enabled by default.
Power alarm	When the power supply is abnormal, the system triggers an alarm. It is disabled 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 offline	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.

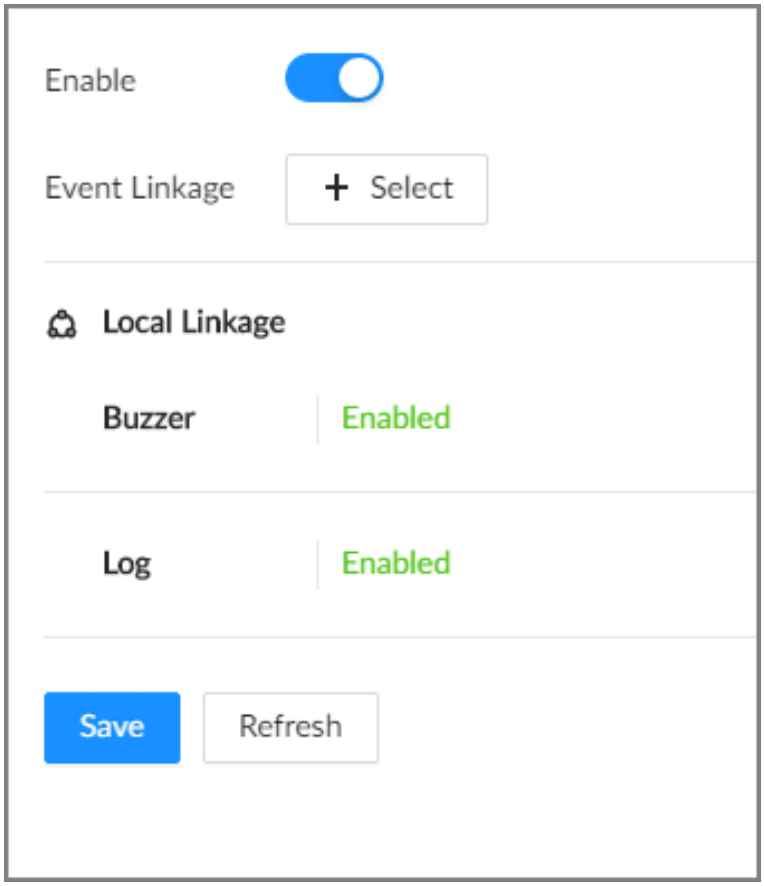
Step 2 Click on the upper-right corner, and then click **Event**.

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 8-51 No disk



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**.

8.3.4.3 Offline Alarm

Set the offline alarm for IVD. 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 IVD to trigger an alarm.

Procedure

Step 1 Log in to the PC client.

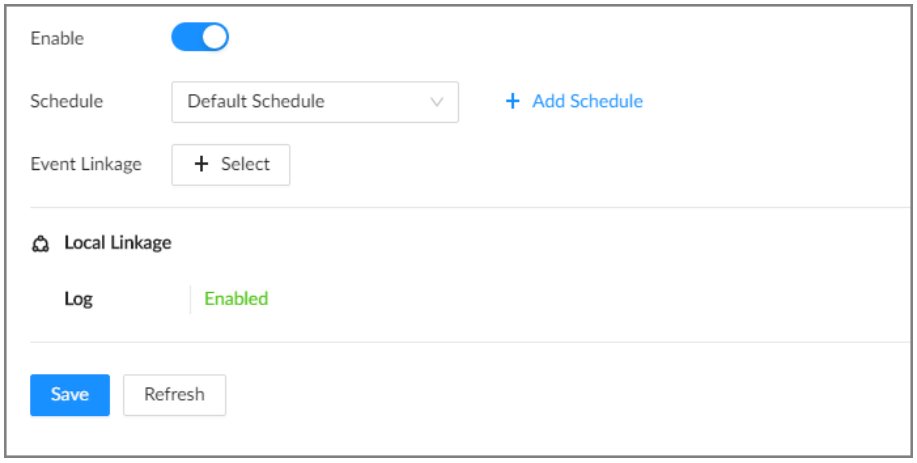
Step 2 Click on the upper-right corner, and then click **Event**.

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 8-52 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**.

8.3.4.4 Configuring Smart Plan

You can view smart plans, and configure entries frequency, and video quality analytics.

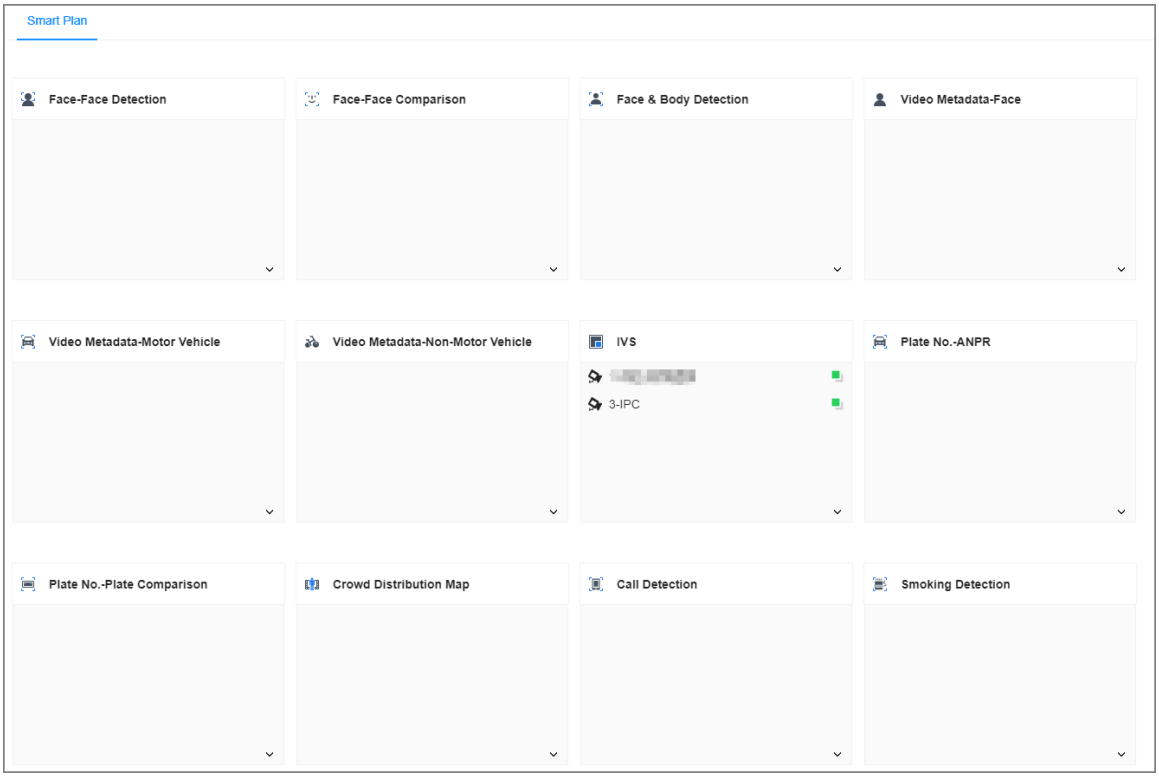
8.3.4.4.1 Viewing Smart Plans

After you add the remote devices to the IVD, the system obtains the smart detection functions of the remote devices.

Log in to the PC client. Click on the upper-right corner of the page and then click **Event**. Select the root node on the device tree on the left, and then select **Smart Plan** > **Smart Plan**. You can view the smart detection functions that IVD supports and the channels on which each smart function is enabled.

indicates that AI by Camera is enabled; indicates that AI by Recorder is enabled.

Figure 8-53 Smart plan



8.3.4.4.2 Setting Entries Frequency

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 **Smart Plan** > **Entries Frequency**.

Figure 8-54 Entries frequency



Step 5 Click **Target Face Database**, and then select the database to be linked.

Step 6 Configure the parameters.

Table 8-23 Entries frequency parameters

Parameter	Description
Entries Counter	Click to enable entries counter. Entries will be counted.
Statistical Cycle	Set the statistical cycle. The statistical cycle is 7 days by default.
Entries Detected	Set the threshold of entries frequency. When the entries detected reaches or exceeds the threshold, an alarm is triggered.
Reset	Clear all entry counts.

Step 7 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 8 Click **Select** next to **Event Linkage** to set alarm actions.

Step 9 Click **Save**.

When the entries detected of a person reach or exceed the threshold, the features panel on the right side of the video window displays a high frequency tag. You can find the tagged faces using live view or AI search.

- For details about live view, see "6.5.3 Live View of Face Detection".
- For details about face search, see "6.6.2.6.1 Searching by Attributes".

8.3.4.4.3 Video Quality Analytics

The Device can analyze and trigger alarm against blurry image, tampering, color cast and more, and then generate statistics reports.

Configuring Video Quality Analytics

After you enable video quality analytics, the Device triggers an alarm when the video quality is affected by blurry image, tampering, color cast and more.

Procedure

Step 1 Log in to the PC client.

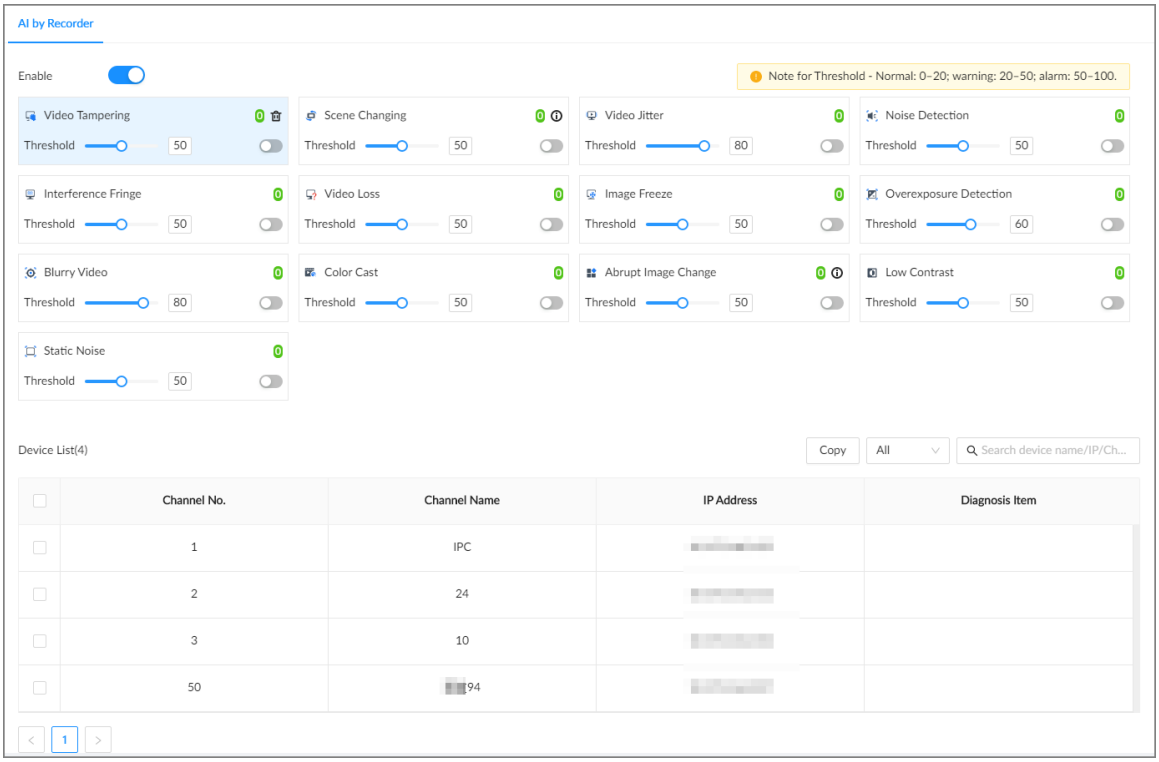
Step 2 Click on the upper-right corner, and then click **Event**.

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 **Smart Plan** > **Video Quality Analytics**.

Figure 8-55 Video quality analytics



Step 5 Click to enable video quality analytics.

Step 6 Configure the parameters.

1. Click to enable the corresponding diagnosis item, for example, video tampering.
2. Set the threshold.
3. On the device list, select one or more devices.
4. Set the detection interval.

Step 7 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 8 Click **Select** next to **Event Linkage** to set alarm actions.

Step 9 Click **Save**.

Viewing AI Report

You can view the daily, monthly, or yearly video diagnosis statistics report of specific devices.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **AI Application** > **AI Report** > **Video Quality Analytics**

Step 3 Select one or more remote devices and then select one or more diagnosis items.

Step 4 Select **Daily** , **Monthly**, **Yearly** and then set a specific date, month or year.

Step 5 Click **OK**.

The diagnosis statistics are displayed in a statistical chart. You can view the channel name and diagnosis time on the list below the chart.

- Click to display the statistics in a bar chart.
- Click to display the statistics in a pie chart.
- Click to export the report to local storage.

8.3.4.5 Configuring Local Alarm

Set local alarm. When the alarm input device sends an alarm signal to the Device, an alarm is triggered.

- Make sure that the Device is connected with an alarm input device.
- The Device supports 16-channel alarm input. Configure according to actual port of alarm input device. This section uses alarm-in port 1 as an example.

Procedure

Step 1 Log in to the PC client.

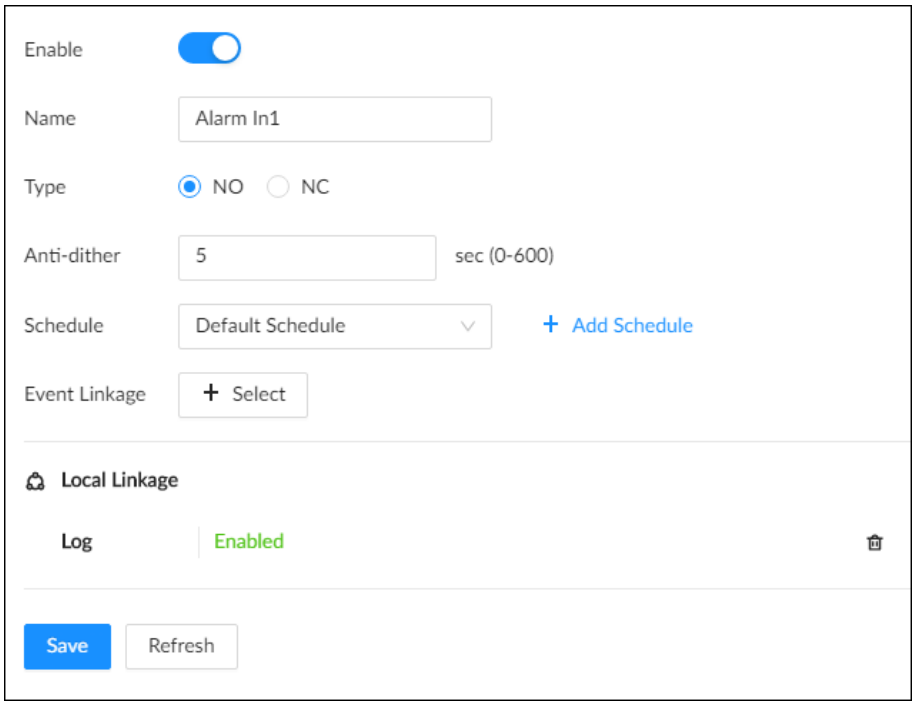
Step 2 Click on the upper-right corner, and then click **Event**.

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 **Local Alarm** > **Alarm-in Port1**.

Figure 8-56 Alarm-in port 1



Step 5 Click to enable local alarm.

Step 6 Set parameters.

Table 8-24 Local alarm parameters description

Parameter	Description
Name	Enter a name for the alarm.
Type	Select a type of the alarm input device. Both NO and NC are supported.
Anti-dither	The system records only one alarm event during this period.

Step 7 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 8 Click **Select** next to **Event Linkage** to set alarm actions.

Step 9 Click **Save**.

8.3.5 Remote Device

Set alarm actions for remote devices, including video detection alarm, offline alarm and smart detection alarm.

The parameters might be different depending on the model you purchased.

8.3.5.1 Video Detection

The system monitors and analyzes the video image. When there are considerable changes on the video, for example, the image becomes blurry, the system triggers an alarm.

8.3.5.1.1 Configuring Video Motion Detection

The system generates a video motion alarm when the detected moving target reaches the configured sensitivity.

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 a remote device from the device tree.

Step 4 Select **Video Detection** > **Motion Detection**.

Step 5 Click  to enable video motion detection.

Step 6 Configure the parameters.

- Configure the anti-dither period. The system only records one alarm event during the anti-dither period.
- Configure motion detection regions.

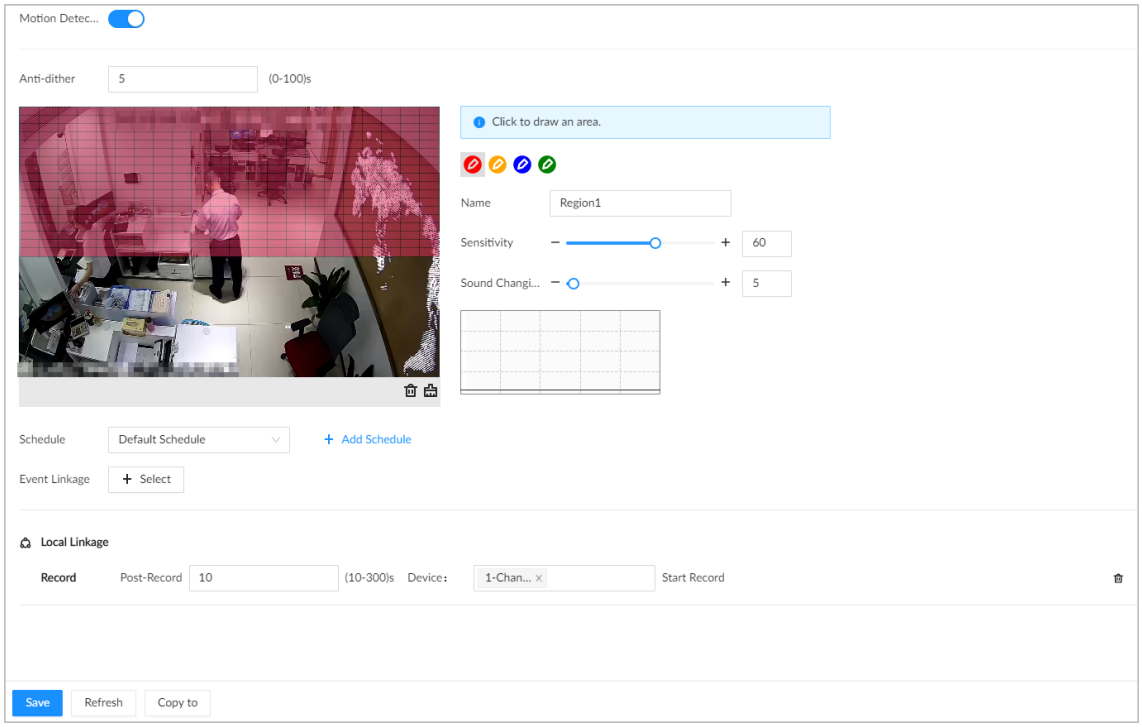
You can draw up to 4 detection zones. When motion is detected in any of the 4 regions, an alarm is triggered.

1. Click the motion detection zone icon .
2. On the video image, drag the mouse to draw a detection zone.
   - ◇ Click an icon in and then click to delete the corresponding detection zone.
   - ◇ Click to clear all the detection zones.
3. Set the parameters.

Table 8-25 Motion detection zone parameters

Parameter	Description
Name	Set detection zone name to distinguish different zones.
Sensitivity	Drag to set sensitivity. The higher the sensitivity, the easier it is to trigger an alarm. At the same time, the false alarm rate increases as well. We recommend the default value.
Threshold	Drag to adjust the threshold. Once the detected percentage (the percentage of the moving target to the detection zone) is equal to or larger than the specified threshold, the system triggers an alarm. For example, the threshold is 10. Once the detected target occupies 10% or more of the detection zone, the system triggers an alarm.

Figure 8-57 Motion detection



Step 7 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 8 Click **Select** next to **Event Linkage** to set alarm actions.

Step 9 Click **Save**.

8.3.5.1.2 Tampering

When something tampers the surveillance video, and the output video is in one color, the system triggers an alarm.

Procedure

Step 1 Log in to the PC client.

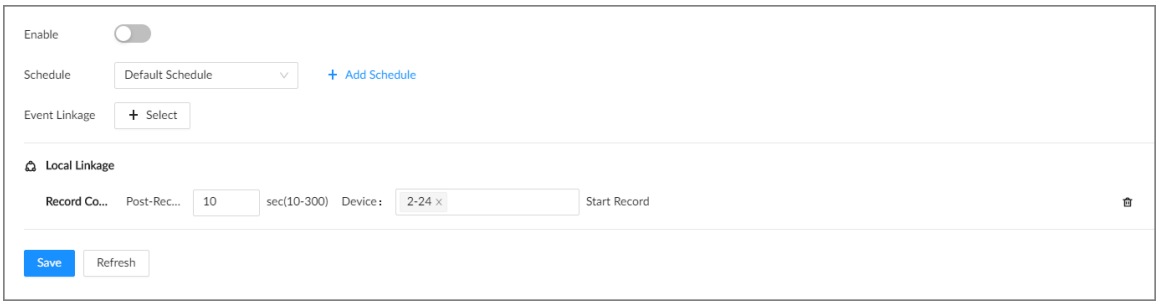
Step 2 Click on the upper-right corner, and then click **Event**.

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

Step 3 Select a remote device from the device tree.

Step 4 Select **Video Detection** > **Video Tampering**.

Figure 8-58 Tampering



Step 5 Click to enable tampering 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**.

8.3.5.2 Offline Alarm

When the remote device is disconnected from the IVD, the system triggers an alarm.

Procedure

Step 1 Log in to the PC client.

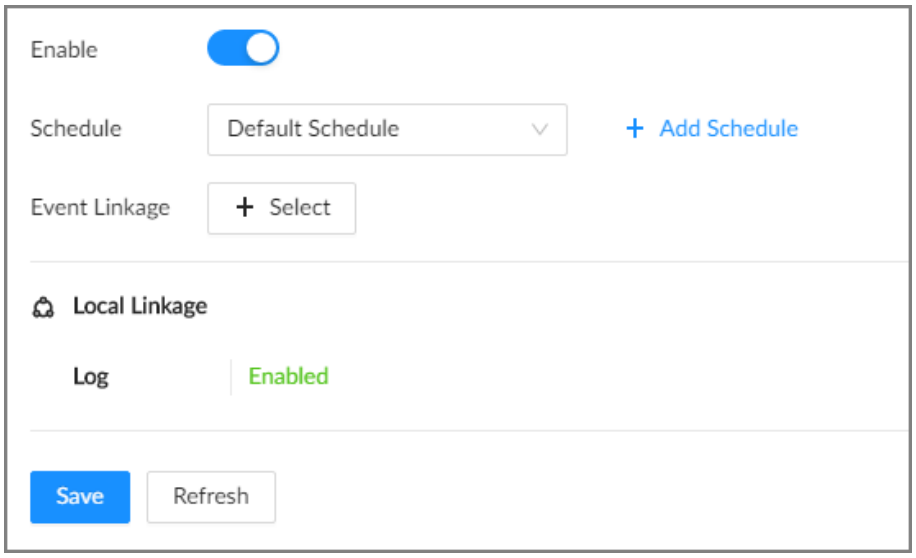
Step 2 Click on the upper-right corner, and then click **Event**.

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

Step 3 Select a remote device from the device tree.

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

Figure 8-59 Offline alarm



Step 5 Click to enable offline alarm.

The offline alarm is enabled by default. You can skip this step.

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**.

8.3.5.3 IPC External Alarm

Set the external alarm input event, so that when there is an alarm input to the remote device, the remote device uploads the alarm to the Device. If the remote device has multiple IO ports, you can set the alarm input event for each port.

Procedure

Step 1 Log in to the PC client.

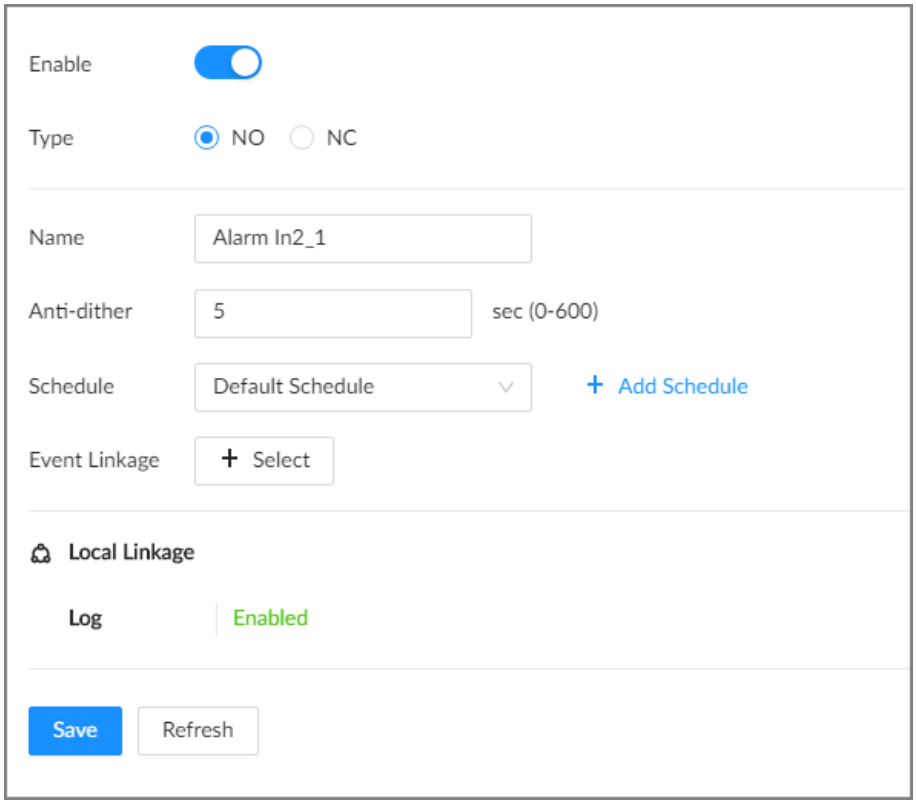
Step 2 Click on the upper-right corner, and then click **Event**.

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

Step 3 Select a remote device from the device tree.

Step 4 Select **External Alarm** > **Alarm-in Port1**.

Figure 8-60 Alarm-in port 1



Step 5 Click to enable the alarm.

Step 6 Set parameters.

Table 8-26 External alarm parameters description

Parameter	Description
Name	Enter a name for the alarm.
Type	Select the type of the alarm input device. Both NO and NC are supported.
Anti-dither	The system records only one event during this period.

Step 7 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 8 Click **Select** next to **Event Linkage** to set alarm actions.

Step 9 Click **Save**.

8.3.5.4 Thermal Alarm

- Alarm types might vary depending on the models of thermal cameras.

- Make sure that thermal detections such as heat detection and temperature detection have been configured on the thermal camera.

Table 8-27 Thermal alarms

Function	Description
Heat alarm	When the thermal camera detects a heat source, the alarm signal is transmitted to the Device, and the Device will perform an alarm linkage action.
Temperature alarm	When the thermal camera detects that the temperature is above or below the threshold value, the alarm signal is transmitted to the Device, and the Device will perform an alarm linkage action.
Temperature difference alarm	When the thermal camera detects a temperature difference greater than the set value, the alarm signal is transmitted to the Device, and the Device will perform an alarm linkage action.
Hot spot alarm	When the maximum temperature detected by the thermal camera is higher than the set value, the alarm signal is transmitted to the Device, and the Device will perform an alarm linkage action.
Cold spot alarm	When the lowest temperature detected by the thermal camera is below the set value, the alarm signal is transmitted to the Device, and the Device will perform an alarm linkage action.

This section uses the configuration of temperature alarm as an example.

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 a thermal channel from the device tree.

Step 4 Select **Thermal Alarm** > **Temperature Alarm**.

Step 5 Click  to enable the 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**.

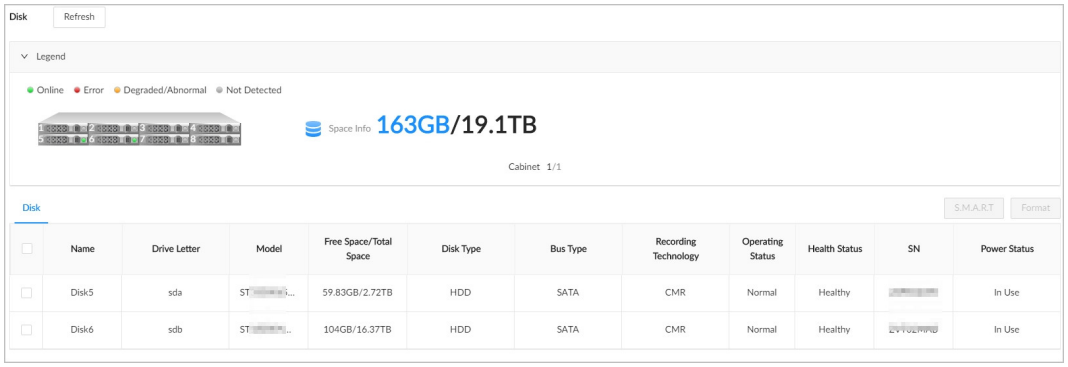
8.4 Storage Management

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 (restart, insert and pull the disk).
- Routine inspection: The system executes 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.

Figure 8-61 Storage management



8.4.1 Storage Resource

8.4.1.1 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 more.

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

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

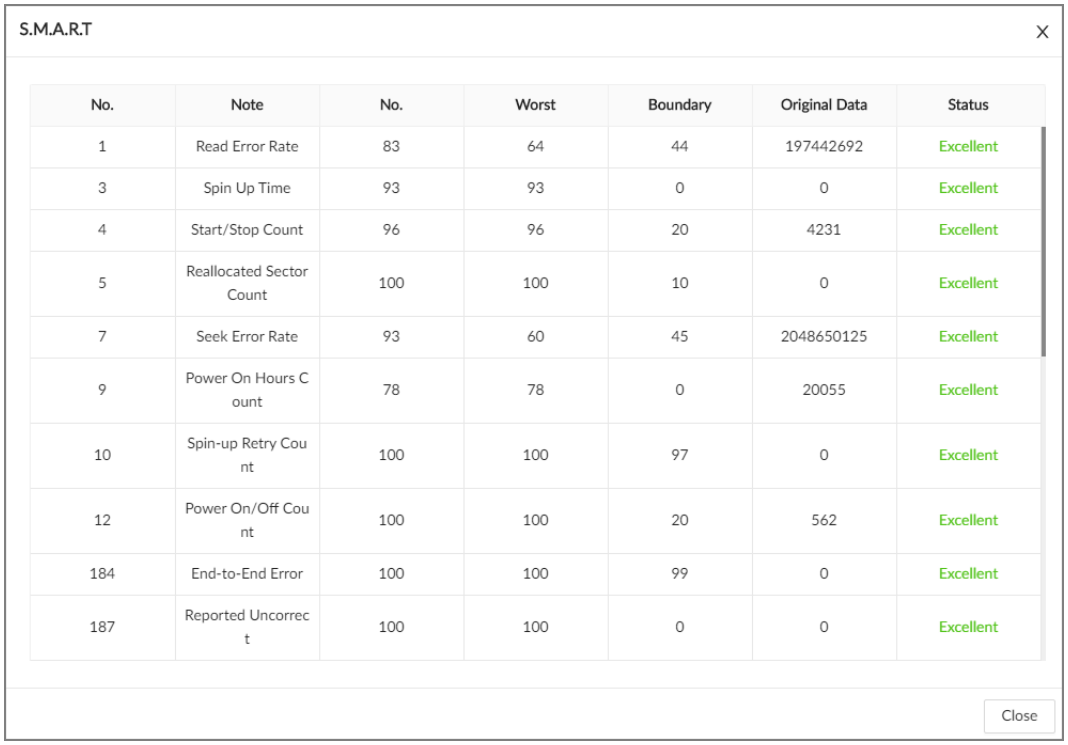
Slight difference might be found on the user page.

8.4.1.1.1 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.

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 8-62 S.M.A.R.T



8.4.1.1.2 Formatting

Please be advised that formatting will clear all data on the disk.

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

8.4.1.1.3 Fixing the File System

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 the disk, 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.

8.4.1.2 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.

- The Device supports RAID0, RAID1, RAID5, RAID6, RAID10, RAID50 and RAID60.
- We recommend you use enterprise HDD when you are creating RAID, and use surveillance HDD for single-HDD mode.

8.4.1.2.1 Creating RAID

Background Information

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** > **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 8-63 Manual create

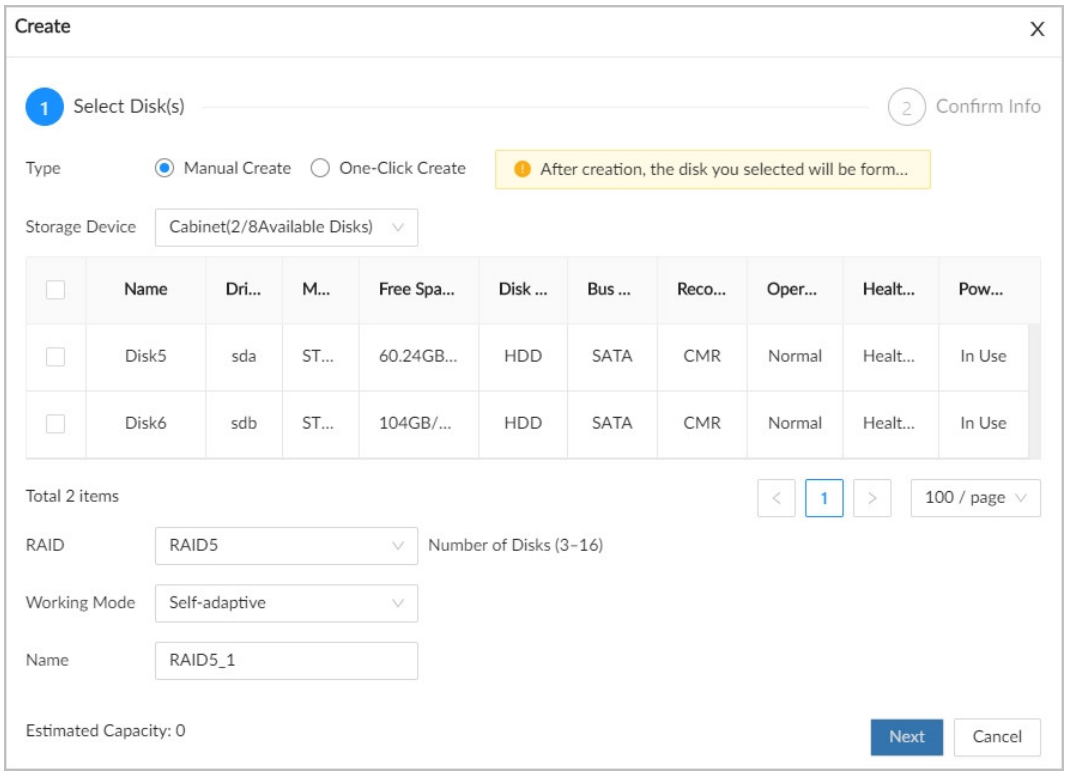


Table 8-28 Manual creation parameters description

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 8-64 One-click create

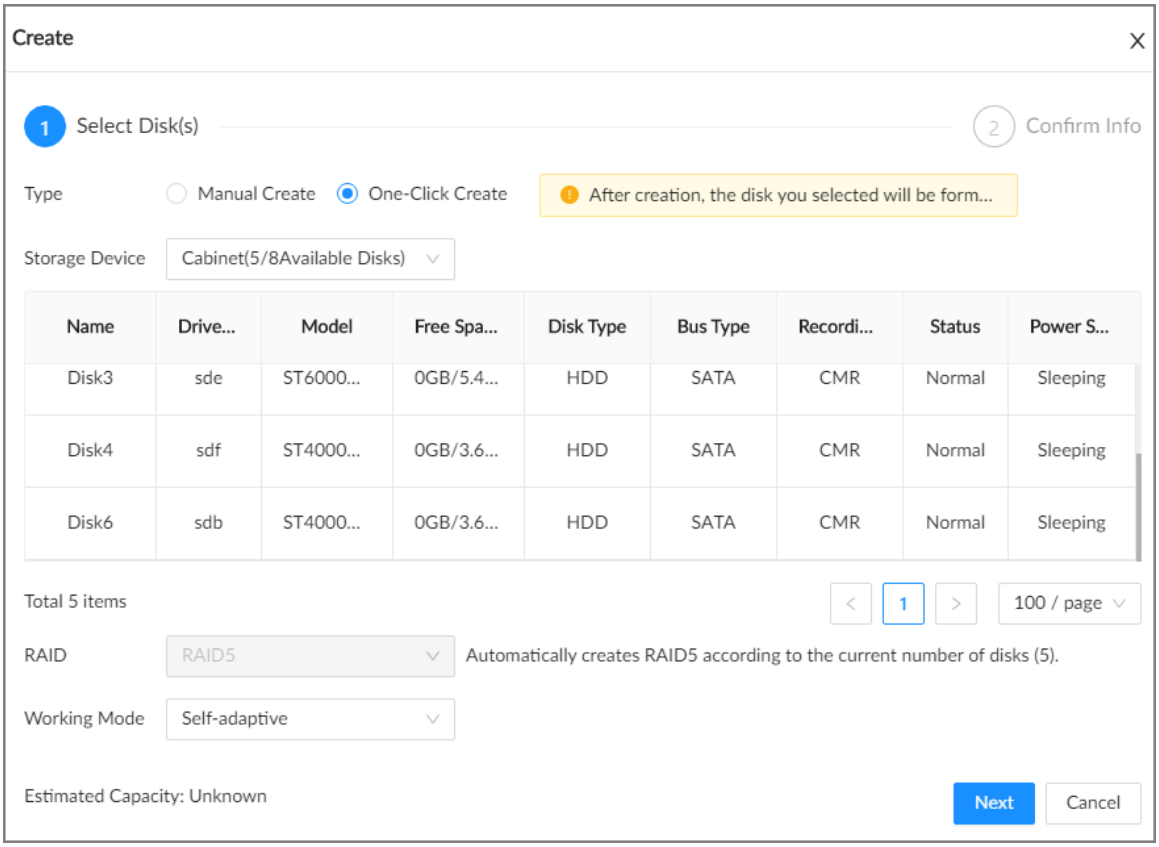


Table 8-29 One-click creation parameters description

Parameter	Description
Storage Device	Select the storage device where the disks are located.
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 8-30 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 more 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.

8.4.1.2.2 Creating a Hot Standby Disk

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 8-65 Global hot standby

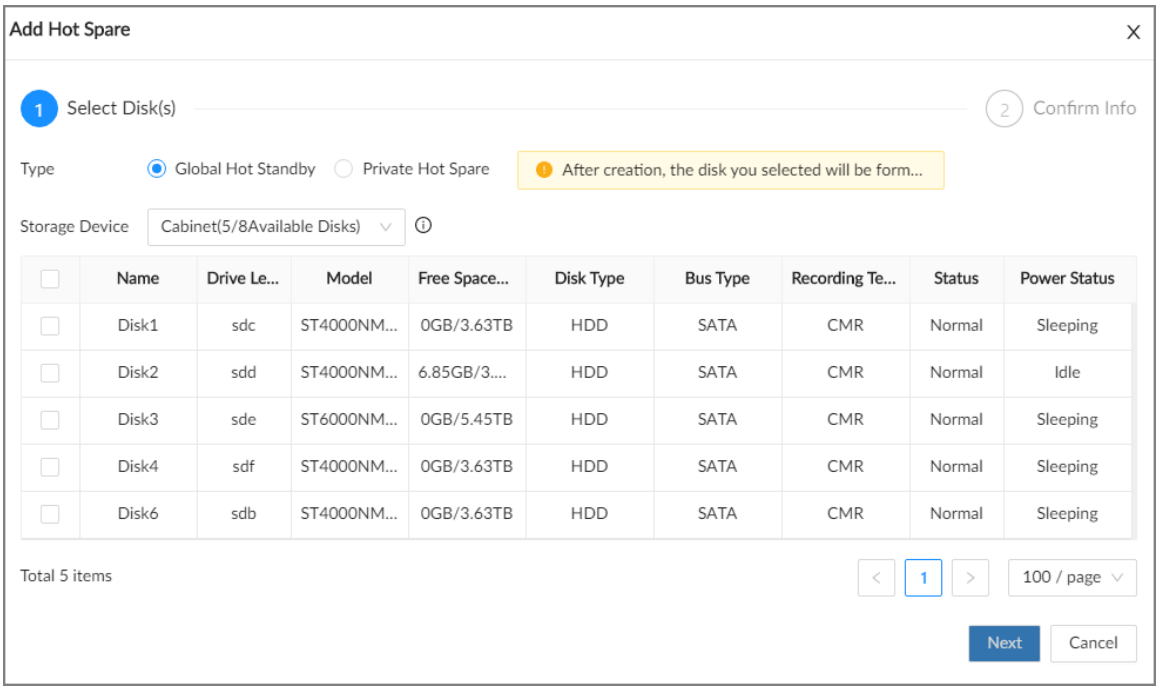
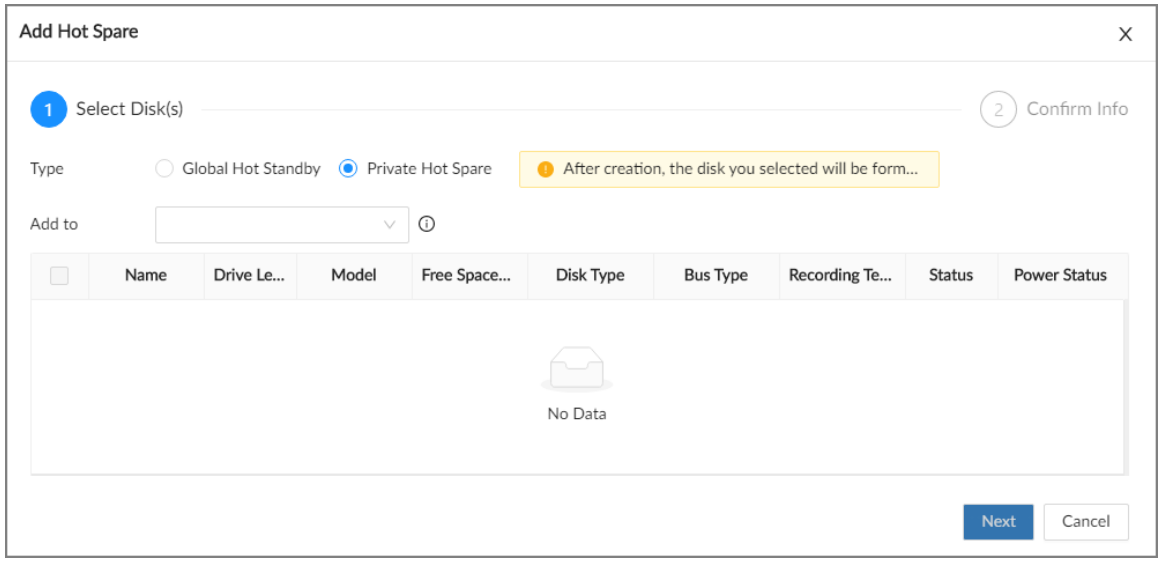


Figure 8-66 Private hot standby



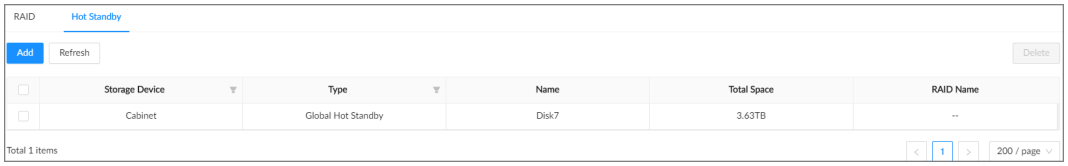
Step 6 Click **Next**.

Step 7 Confirm information.

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

Step 8 Click **Create**.

Figure 8-67 Hot standby



8.4.1.3 Network Disk

Network disk is a network-based online storage service that stores device information on the network hard disk through the iSCSI protocol.

8.4.1.3.1 iSCSI Application

Log in to the PC client. Click on the upper-right corner and then select **Storage** > **Storage Resource** > **Network Disk** > **iSCSI Application**. You can view usage of the network disk, including its remaining capacity and status.

- Select a network disk, and then click **Format** to format the disk.

  Please be advised that formatting will erase all data on the disk.
- Click the box in the **Disk Operation** column, and then you can select an operation permission type.
  - ◇ Read/Write: One can read, edit, add, and delete data on this disk.
  - ◇ Read Only: One can only read data on this disk.

8.4.1.3.2 iSCSI Management

Set up the network disk through iSCSI and map the network disk to the Device so that the Device can use the network disk for storage.

Make sure that service has been enabled on the iSCSI server and the server has provided the shared file directory.

Procedure

Step 1 Log in to the PC client.

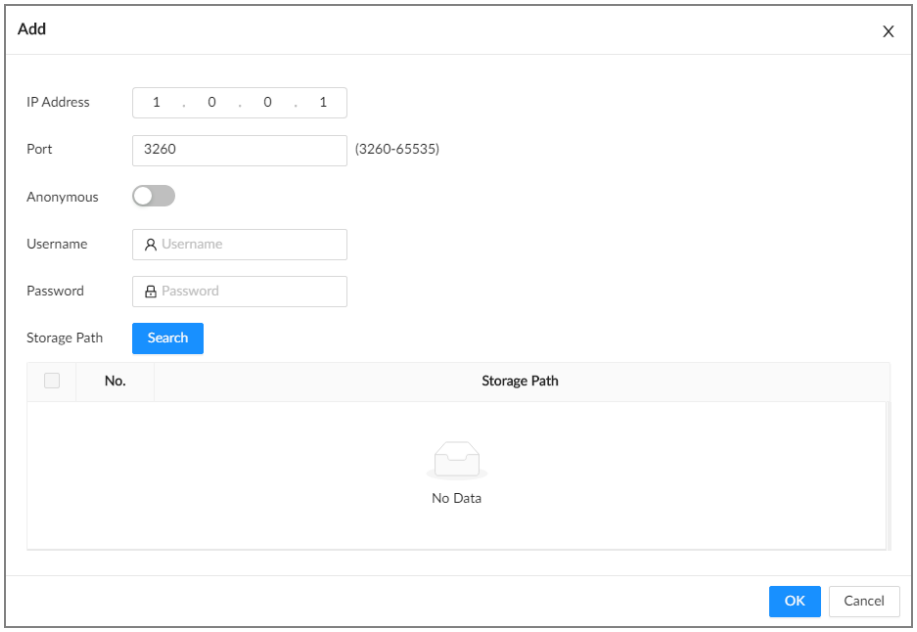
Step 2 Click on the upper-right corner and then click **Storage**.

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

Step 3 Select **Storage Resource** > **Network Disk** > **iSCSI Management**.

Step 4 Click **Add**.

Figure 8-68 Add iSCSI



Step 5 Set parameters.

Table 8-31 Network disk parameters

Parameter	Description
IP Address	Enter the IP address of the iSCSI server.
Port	Enter the port number of the iSCSI server. It is 3260 by default.
Anonymous	Click to enable anonymous login. If iSCSI server has no permission limitation, you can log in to the server without entering the password and user name.
User Name	If permission is required to access the shared file directory on the iSCSI server, you need to enter user name and password.
Password	

Parameter	Description
Storage Path	Click **Search** to select the storage directory. The storage directory is generated when the shared file directory is being created on the iSCSI server. Each directory represents an iSCSI disk.

Step 6 Click **OK**.

- Click to delete a disk; click **Refresh** to refresh the disk list.
- On the **Disk Group Settings** page, you can configure network disk groups.

8.4.1.4 SFTP

After setting up the SFTP server, you can store recordings and images from the configured channels and time range on the SFTP server.

Prerequisites

You have purchased or downloaded the SFTP service tool and installed it on the computer.

When creating an SFTP user, you must set write permissions for the SFTP folder. Otherwise, files cannot be uploaded.

Procedure

Step 1 Log in to the PC client.

Step 2 Click on the upper-right corner and then select **Storage** > **Storage Resource** > **SFTP**.

Step 3 Click to enable SFTP.

Step 4 Configure the parameters.

Figure 8-69 SFTP

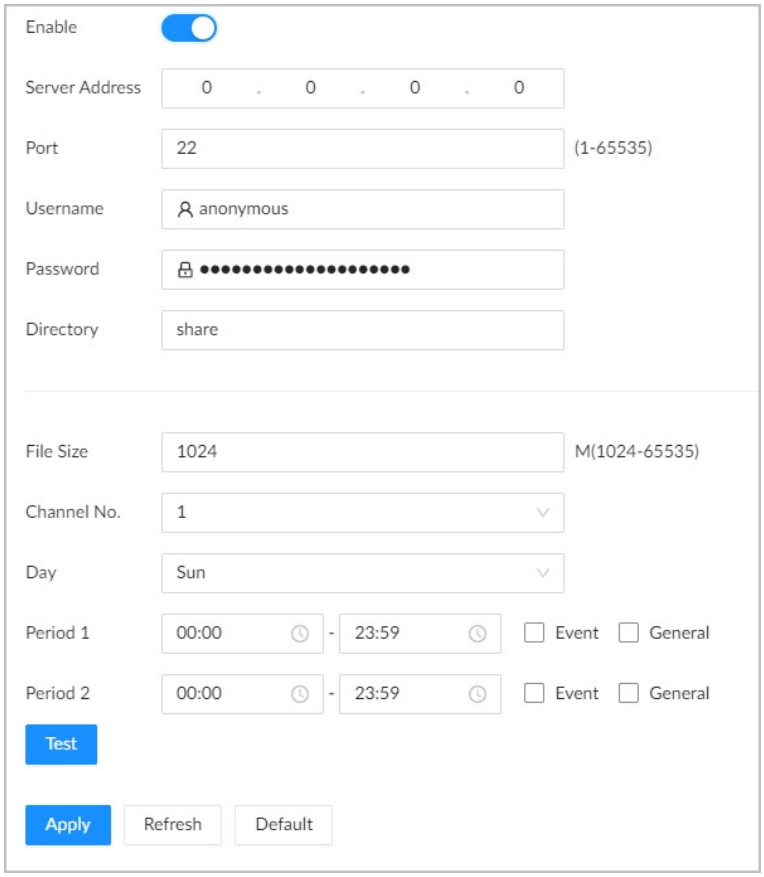


Table 8-32 SFTP parameter description

Parameter	Description
Server Address	Enter the IP of the SFTP server.
Port	The default port is 22.
User Name	User name and password for accessing the SFTP server.
Password	
Directory	Create folders according to the rules in the root directory of the SFTP account. ● When the remote directory is empty, the system will automatically create different folders based on IP, time, and channel. ● Enter the remote directory name, and the system will create a corresponding folder in the root directory of the SFTP account. Then, it will create different folders based on IP, time, and channel.
File Size	Set the size for uploading video files. ● If the specified duration is shorter than the total length of the video recording, only the segment within the specified duration will be uploaded. ● If the specified length is greater than the size of the video file, upload the entire video file. ● When the set value is **0**, upload the entire video file.

Parameter	Description
Channel No.	Select the channel number for uploading the video file.
Day	Select the day of the week, time period, and alarm type. The system will upload the videos or images at scheduled times according to the settings. Two time periods can be set for each week.
Period	
Test	Click **Test** to test if the SFTP connection is successful. If successful, the system will indicate that the SFTP test is successful. If it fails, the system will show an error message for the SFTP test. You need check if the network or configuration is correct.

Step 5 Click **Apply**.

8.4.2 Storage Settings

8.4.2.1 Configuring Disk Groups

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.

Procedure

Step 1 Log in to the PC client.

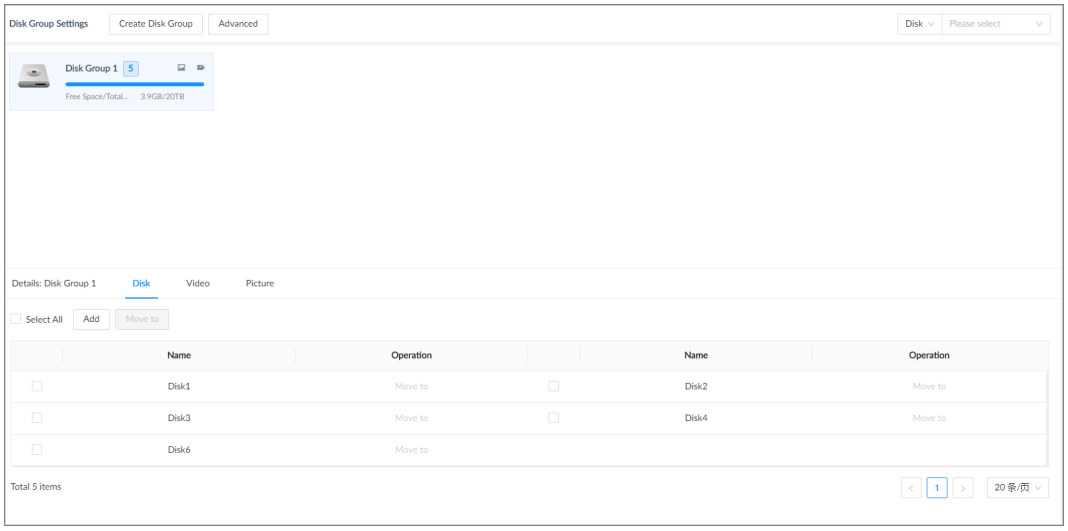
Step 2 Click  on the upper-right corner and then click **Storage**.

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

Step 3 Select **Storage** > **Disk Group Settings**.

- The value (such as ) next to the group name refers to the number of disks and RAID groups in the disk group. If  is displayed, it means there were videos or images stored in the disk group but now there is no available disk or RAID group in the disk group.
-  indicates picture storage.  indicates video storage.

Figure 8-70 Disk group



Step 4 Click **Add** , enter the group name, and then click **OK**.

A new disk group is created.

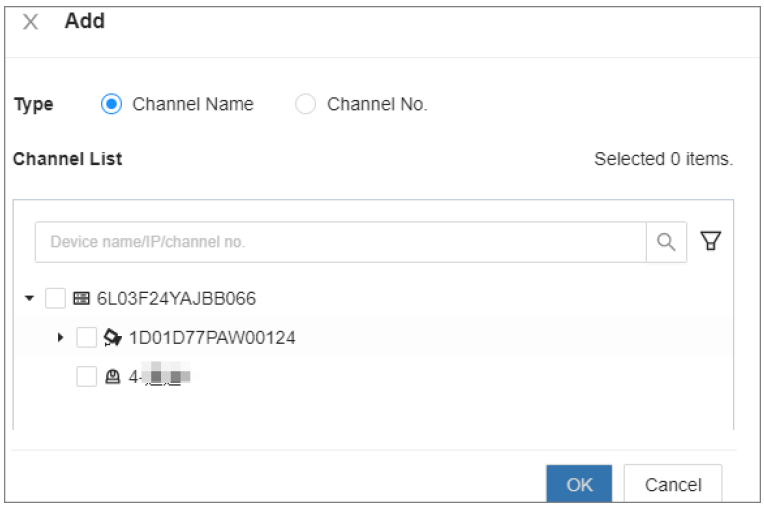
Step 5 Click a disk group and then under the **Disk** tab, you can allocate the disks or RAID groups for the disk group.

- Add disks or RAID groups to the current disk group: Click **Add** , select one or more disks or RAID groups, and then click **OK**.
- Move disks or RAID groups to another disk group.
  - ◇ One by one: Click **Move to** under **Operation**, select a disk group, and then click **OK**.
  - ◇ In batches: Select one or more disks or RAID groups, click **Move to** next to **Add**, select a disk group, and then click **OK**.

Step 6 Click a disk group and then under the **Video** or **Picture** tab, you can allocate the video or image storage of different channels to disk groups.

- Add channels to the current disk group for video or image storage: Click **Add** , click **Channel Name** or **Channel No.** to search for channels, select one or more channels, and then click **OK**.

Figure 8-71 Add channels



- Move channels to another disk group for video or image storage.

- One by one: Click **Move to** under **Operation**, select a disk group, and then click **OK**.
- In batches: Select one or more channels, click **Move to** next to **Add**, select a disk group, and then click **OK**.

Step 7 (Optional) Click **Advanced**, and then select the checkbox to enable load balancing.

After you enable load balance, the system automatically moves videos from ineffective disk groups and evenly allocates them to functional groups.

8.4.2.2 Recording Control

Configure recording modes and schedules for channels.

8.4.2.2.1 Configuring Recording Mode

Configure recording modes for channels.

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.

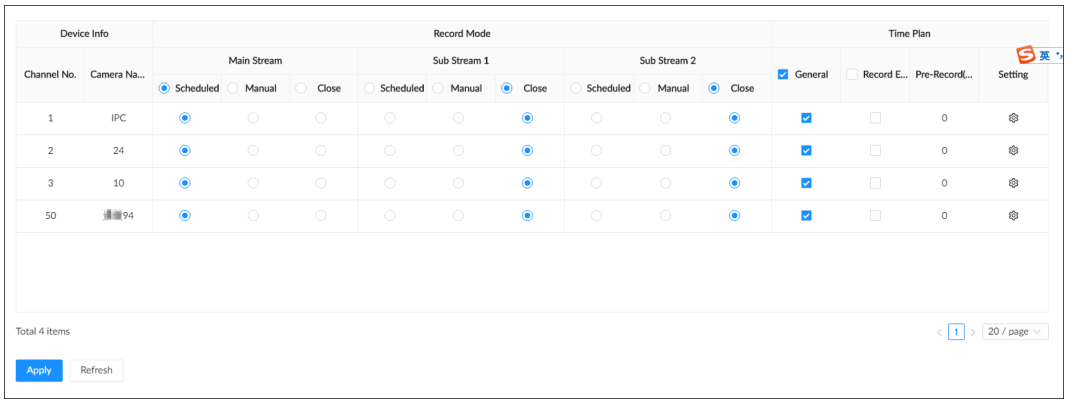
Step 3 Select **Storage** > **Record Control**.

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 8-72 Recording Mode



Step 5 Click **Apply**.

8.4.2.2.2 Configuring Recording Schedule

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

Procedure

Step 1 Log in to the PC client.

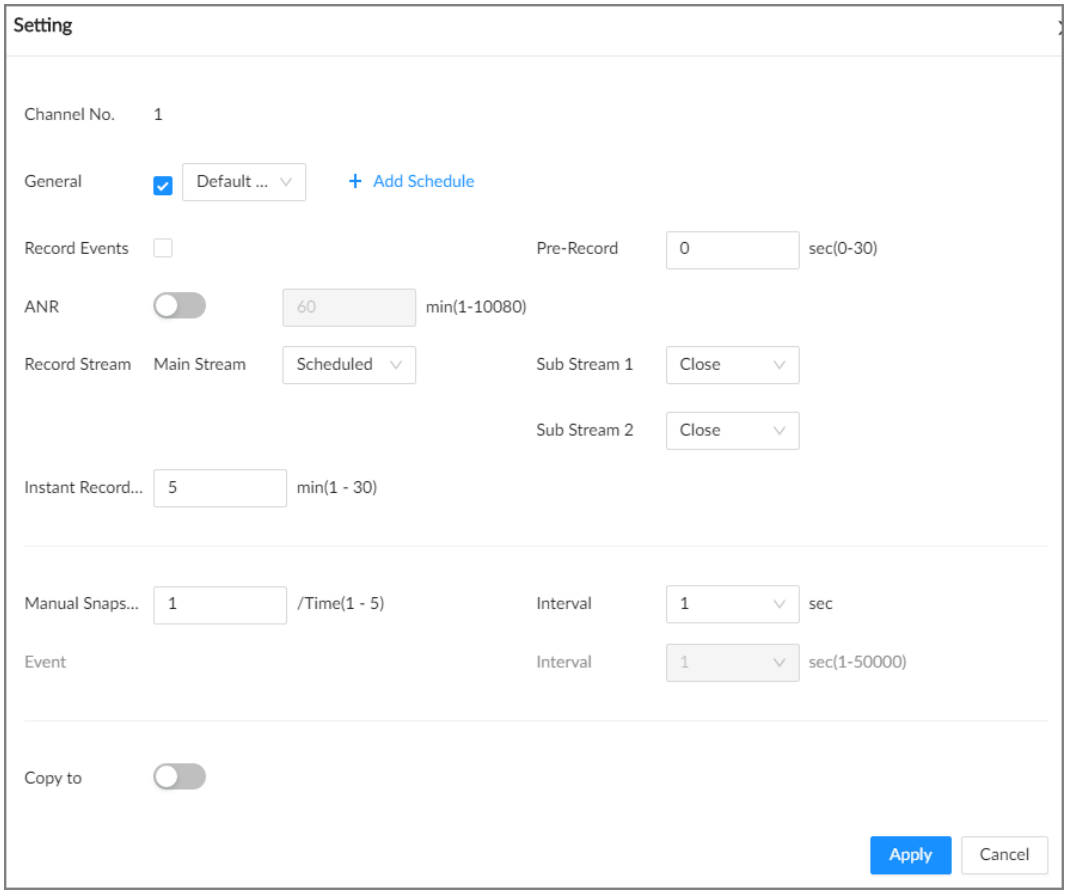
Step 2 Click on the upper-right corner and then click **Storage**.

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 8-73 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. For details, see IVSS user's manual.
- **Record Events** : Set the pre-record time. The Device records before an event occurs.

Step 6 Configure other parameters.

Table 8-33 Time plan parameters

Parameter	Description
ANR	Click to enable ANR (Automatic Network Replenishment). When the network connection between the Device and IPC fails, the IPC continues to record videos and store videos on the SD card on the camera. When network recovers, the Device downloads those videos from IPC. Set the maximum recording upload period. If the offline period is longer than the defined period, IPC will only upload the recording file during the specified period. Make sure that the IPC has an SD card and is recording.
Record Stream	Select stream types and recording modes.
Instant Record Duration	The duration of instant recording. After starting instant recording under the **Live** tab, if you do not stop recording, the system will automatically stop after the defined duration.
Manual Snapshot	The number of images for each manual capture action. You can also configure the interval between manual snapshots.
Event Snap	Configure the interval between event snapshots.
Copy to	Copy the current settings to other channels.

Step 7 Click **Apply**.

8.4.2.3 Basic Storage Settings

Configure the storage mode when the disk space is used up, automatic deletion of expired files, and image storage strategy.

8.4.2.3.1 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**.

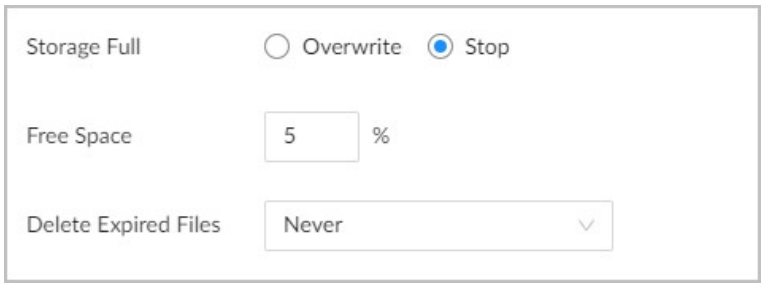
Step 4 Select **Storage Full**.

- **Overwrite** : When 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 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 8-74 Storage mode



Step 5 Set image storage strategy.

- **Linkage Configuration** : The default option configures the storage image according to various event linkages.
- **Always Use** : When enabled, the event image is always stored on the device which can be used with the platform.

Step 6 Click **Apply**.

8.4.2.3.2 Setting Automatic File Deletion

You can enable the Device to automatically delete files older than a certain number of days.

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.

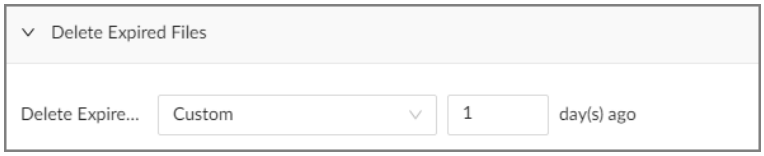
Step 3 Select **Storage** > **Basic**.

Step 4 Set automatic file deletion.

- **Never** : The Device does not delete files automatically.
- **Custom** : The Device automatically deletes files older than the configured number of days.

The deleted files cannot be recovered.

Figure 8-75 Delete expired files



Step 5 Click **Apply**.

8.4.2.3.3 Setting Image Storage Strategy

Procedure

Step 1 Log in to the PC client.

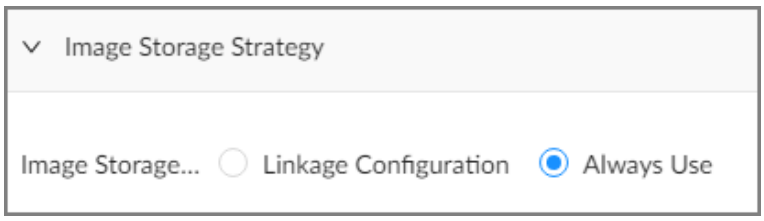
Step 2 Click on the upper-right corner and then click **Storage**.

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

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

Step 4 Select an image storage strategy from **Linkage Configuration** and **Always Use**.

Figure 8-76 Image storage strategy



Step 5 Click **Apply**.

8.4.2.4 Record Transfer

When the Device and an IPC are disconnected, the IPC continues to record and stores the recording in the SD card. After the network recovers, the Device will download the recording during the disconnection from the IPC.

There are 2 ways for record transfer after the network recovers.

- Automatic download: After the network recovers, the Device automatically downloads the recording in the defined time period.
- Manual download: If ANR is not enabled when you set the recording schedule, after the network recovers, the Device cannot automatically download the recording during the disconnection, but you can manually create a download task.

Procedure

Step 1 Log in to the PC client.

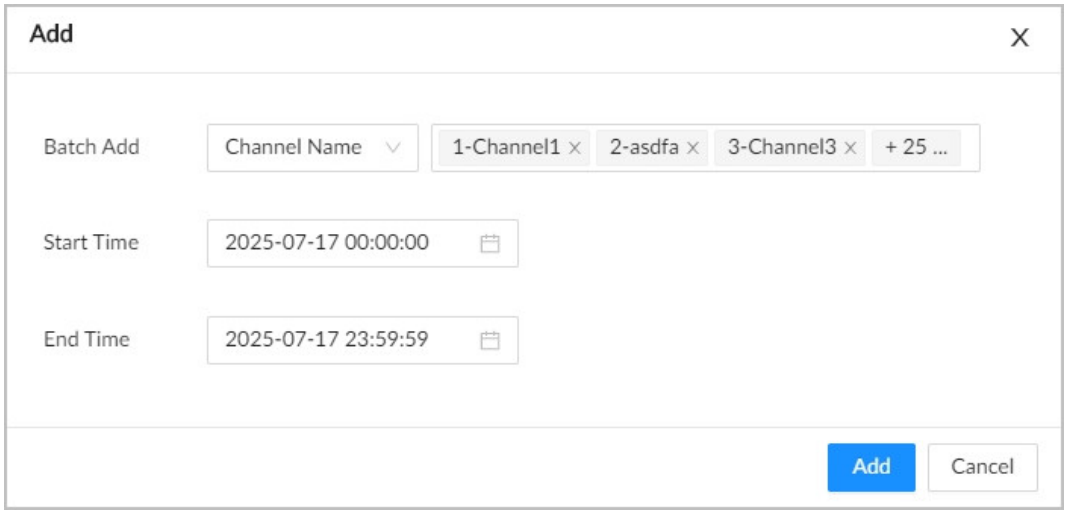
Step 2 Click on the upper-right corner and then click **Storage**.

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

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

Step 4 Click **Add**.

Figure 8-77 Add a task



Step 5 Select **Channel Name** or **Channel No.** to search for channels.

Step 6 Select channels and then set the time period.

Step 7 Click **Add**.

The system downloads files recorded on the selected channels during the defined period.

Select a transfer task, click **Delete** to delete it. A task in progress cannot be deleted.

8.5 Algorithm

8.5.1 Configuring the AI Module

Procedure

Step 1 Log in to the PC client.

Step 2 Select **Algorithm** > **Algorithm Management** > **AI Module** from the configuration list, or click to select **Algorithm** > **Algorithm Management** > **AI Module**.

Step 3 (Optional) Switch between **AI** and **General** at the upper-right corner of area **A0**, click **Apply** and restart the device for the settings to take effect.

A0 refers to the device's own CPU. This function switches between intelligent and normal modes by leveraging CPU computing power.

- **General** : In this mode, the system will free up CPU computing power and resume the operation of video quality diagnosis and heterogeneous output functions.
- **AI** : In this mode, the system will invoke CPU resources to run intelligent analysis, compression, text search and other functions, while reducing decoding and display capabilities, and video quality diagnosis is not supported.

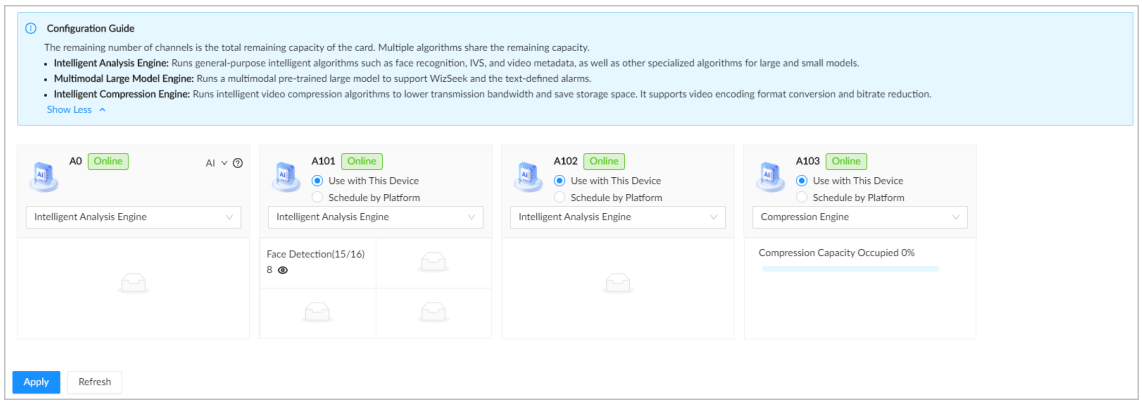
Only available on select models.

Step 4 Click **Use with This Device** , and then select **Intelligent Analysis Engine** in the drop-down list.

When you select **Schedule by Platform**, the platform uses the intelligent module.

The supported engine types of the Device are subject to the actual page.

Figure 8-78 Configure the AI Module



Step 5 Click **Apply**.

8.5.2 Updating the Algorithm

Upgrade the algorithm by importing the upgrade file. The upgrade file is a .bin type file.

Prerequisites

The correct version of the upgrade file has been obtained and placed in the appropriate path.

- When operating locally, store the upgrade file on a USB storage device and connect the USB storage device to the Device.
- When operating via WEB or PC client, place the upgrade file on the computer where the WEB or PC client is located.

Procedure

Step 1 Log in to the PC client.

Step 2 Click on the upper-right corner and then select **Algorithm** > **Algorithm Management** > **Algorithm Update**.

Step 3 Click **File Update**.

Step 4 Click **Browse** , select the update file, and then click **Update Now**.

The system starts the upgrade. After the upgrade is complete, the device will automatically restart.

- Supports upgrading algorithms in batches by selecting multiple upgrade files.
- If the algorithm version is mismatched or the algorithm version is upgradeable, the algorithm status will display the corresponding state.

8.5.3 Generating Algorithm Based on Texts

Generate an intelligent detection algorithm by inputting text contents.

Procedure

Step 1 Log in to the PC client.

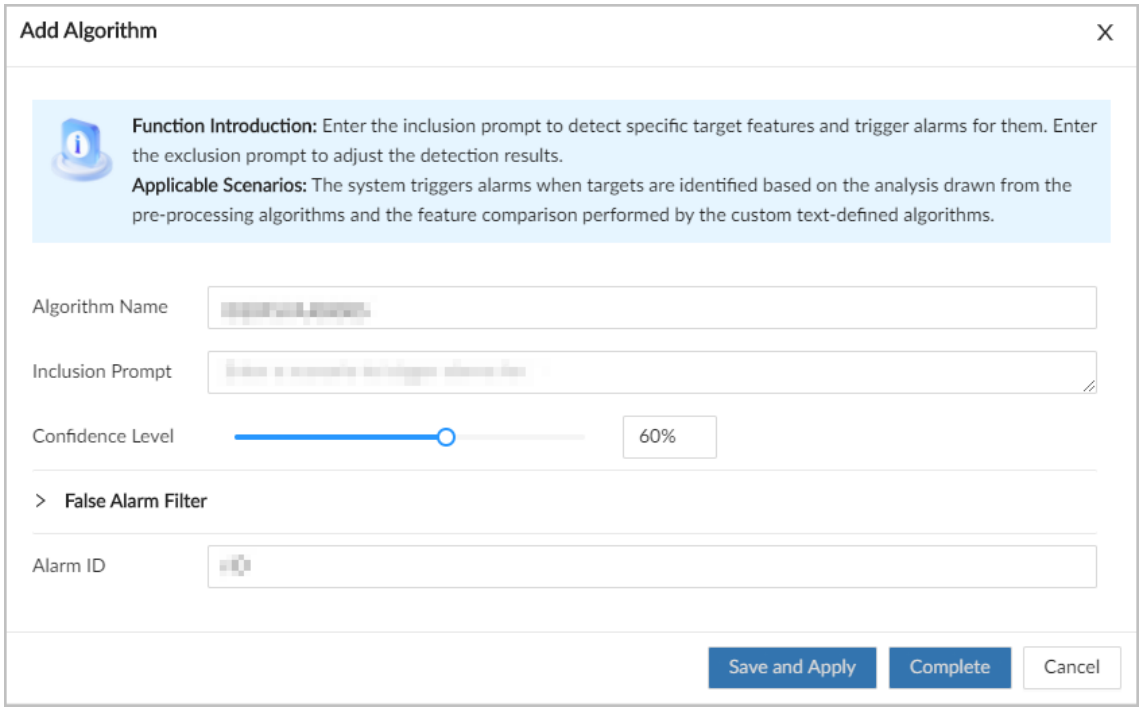
Step 2 Click on the upper-right corner and then select **Algorithm** > **Zero-Sample Algorithm** > **Text-Defined Alarms**.

Step 3 Click **Add Algorithm** to create a text generation algorithm following the guide.

1. Enter the algorithm name and the inclusion prompt, set the confidence level.

   Confidence level represents the similarity between the event image and the feature of the prompt.

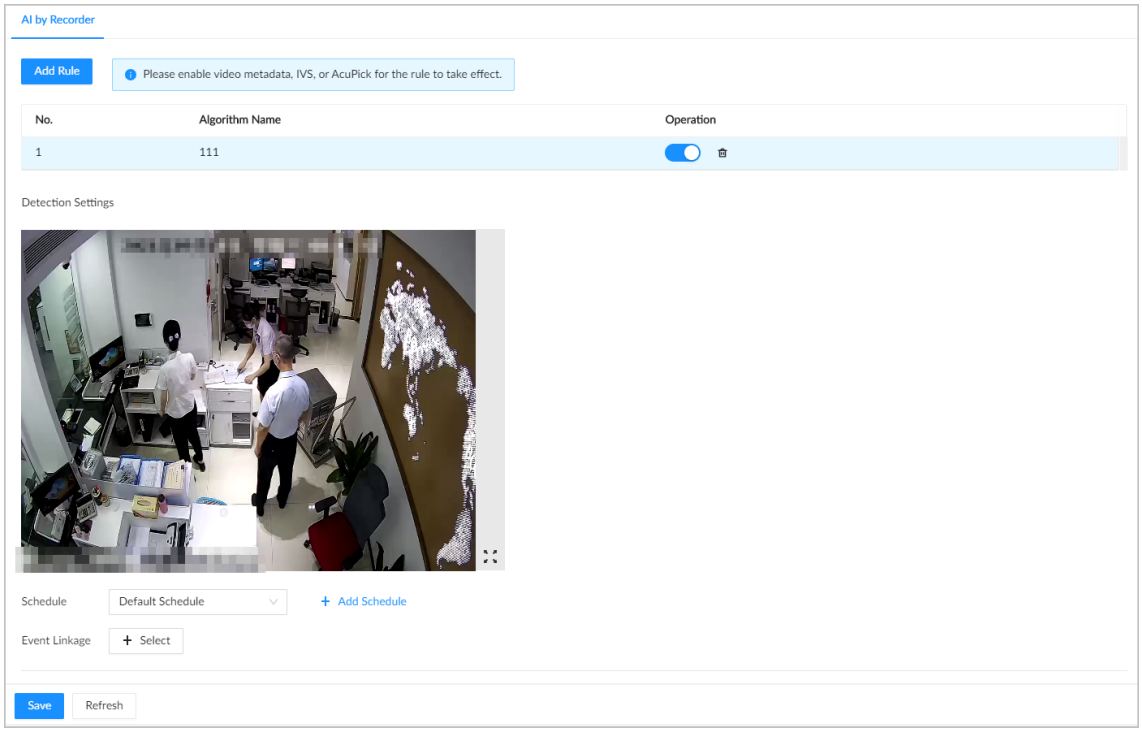
Figure 8-79 Create the algorithm



2. Open **False Alarm Filter**, click + to add the exclusion prompt, and then set the confidence level.

   Supports adding multiple exclusion prompts.
3. Set the **Alarm ID**.
4. Click **Save and Apply** , the system goes to **Text-Defined Alarms** of the **Event** page.
5. Click **Add Rule** , select the algorithm type, and then click **Save**. For details, see "6.12 Text-Defined Alarms".

Figure 8-80 Algorithm application



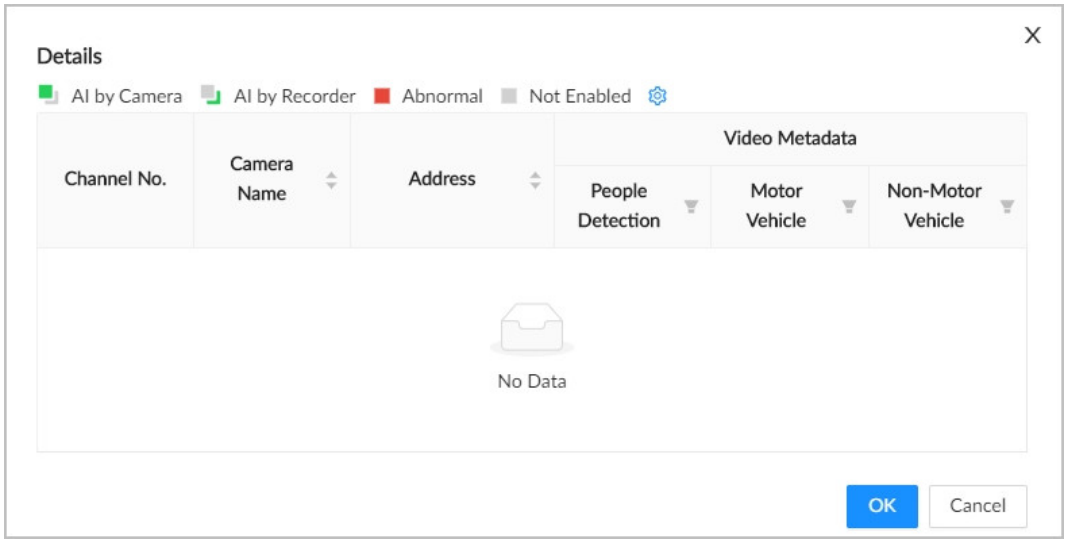
Related Operations

Text-Defined Alarms supports the following operations.

- View algorithm details: Click or operation column to see the pre-processing algorithm details. Click to configure the pre-processing algorithm.

  means that the pre-processing algorithm is not running properly.

Figure 8-81 Details



- Edit the algorithm: Click of the operation column to edit the algorithm.

8.6 System Management

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.

8.6.1 General Configurations

8.6.1.1 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** > **General** > **System Settings**.

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

Step 3 Configure the parameters.

Figure 8-82 Basic system settings

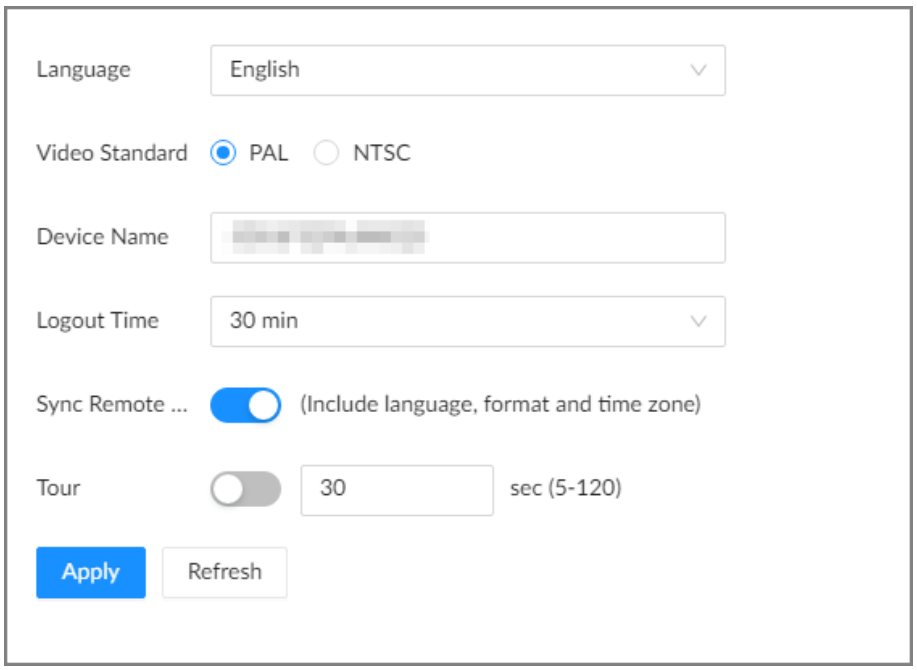


Table 8-34 System parameters description

Parameter	Description
Language	Set system language.

Parameter	Description
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 a 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.
Tour	Click to enable tour and then enter the tour time.
Virtual Keyboard	Enable virtual keyboard on the local interface. This function is available only on the local interface.
Mouse Moving Speed	Set mouse moving speed on the local interface. This function is only available on the local interface.

Step 4 Click **Apply**.

8.6.1.2 Configuring 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.

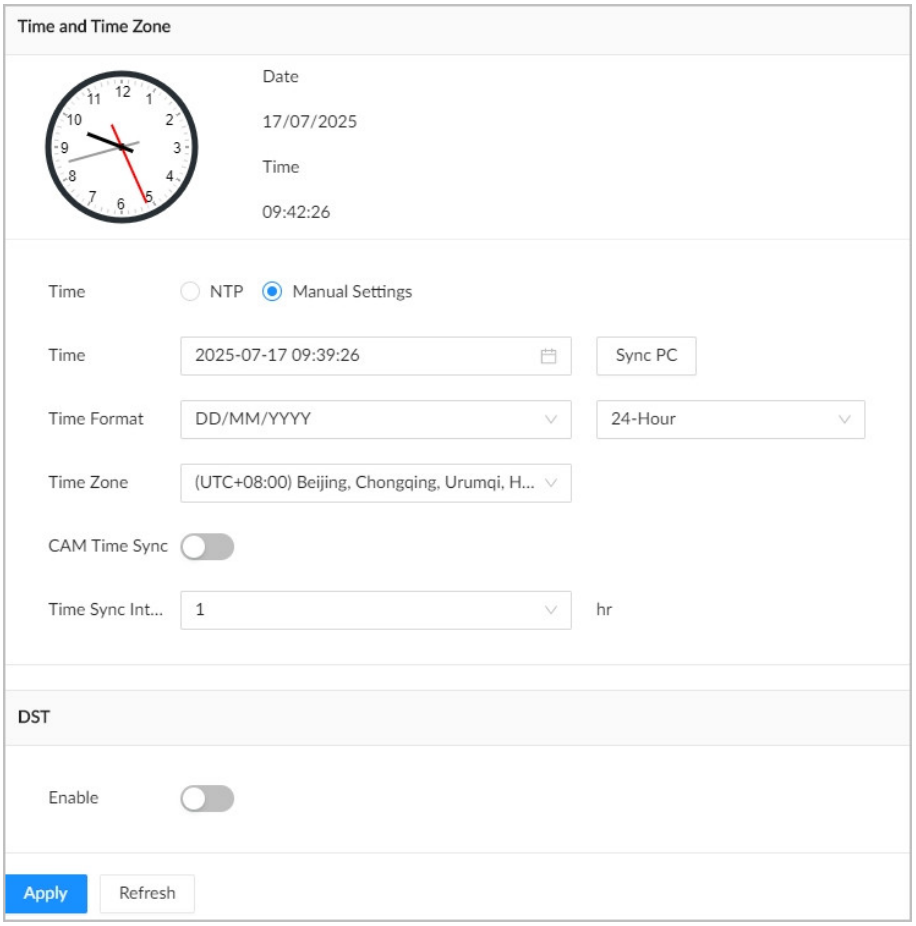
Procedure

Step 1 Log in to the PC client.

Step 2 Click on the upper-right corner, and then click **System** > **General** > **Time**.

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

Figure 8-83 Time



Step 3 Configure the parameters.

Table 8-35 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.
CAM Time Sync	After you enable this function, IVD detects the system time of remote devices once in every interval. When the time of a remote device is inconsistent with IVD time, IVD will calibrate the time of the remote device automatically.

Step 4 (Optional) Set DST.

DST is a system to stipulate local time, in order to save energy. If the country or region where the Device is located follows DST, you can enable DST to ensure that system time is correct.

1. Click to enable DST.
2. Select a DST mode from **Date** and **Week**.
3. Set DST start time and end time.

Step 5 Click **Apply**.

8.6.1.3 Configuring Display

Set the resolution and refresh rate of connected monitors.

Procedure

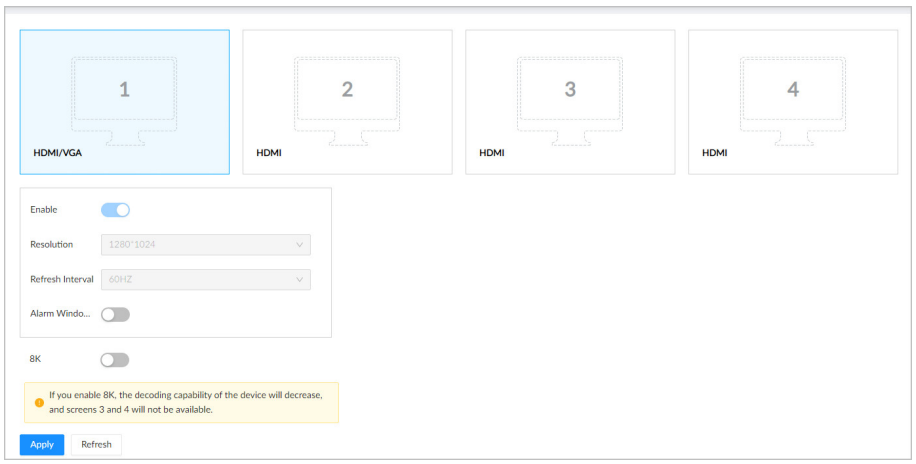
Step 1 Log in to the PC client.

Step 2 Click on the upper-right corner, and then click **System** > **General** > **Display**.

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

- 8K mode configuration is available on select models.
- SN 1–4 refers HDMI 1–HDMI 4. Among which, HDMI/VGA is the main screen, while the VGA and HDMI 1 outputs the same video. The main screen refers to the monitor connected to VGA or HDMI 1 port.
- VGA and HDMI 1 output the same video source. The 3 HDMI ports can output different video sources.
- means the monitor is connected and enabled. means the monitor is connected but has not enabled. means no monitor is connected.

Figure 8-84 Display



Step 3 Select a monitor, and then click to enable the selected monitor.

Step 4 Set parameters.

Table 8-36 Display parameters description

Parameter	Description
Resolution	Set the resolution of the monitors. Different monitors support different resolutions.
Refresh Interval	Set refresh rate of the display.
Alarm Window Pop Up	When the alarm is triggered, enable this function to pop up the live view window. Configure the **Delay Switching Alarm Window** as needed. This function is available only when the device is connected to a monitor.
8K	Click to enable 8K mode. Once enabled, the **Resolution** dropdown list will support the selection of 8K. • To display content in 8K resolution, an HDMI 2.1 cable must be used to connect the display to the HDMI 1 port. • After enabling 8K mode on the main screen, the decoding capability of the sub screen might decrease, potentially leading to no video output or reduced function. Please refer to the actual page for details

Step 5 Click **Apply**.

8.6.1.4 Configuring E-map

Add a digital map, and then bind the channels to actual locations on the map. If the same person is detected by multiple channels, the system can automatically draw connecting lines on the map to generate the movement path for route analysis.

Procedure

Step 1 Log in to the PC client.

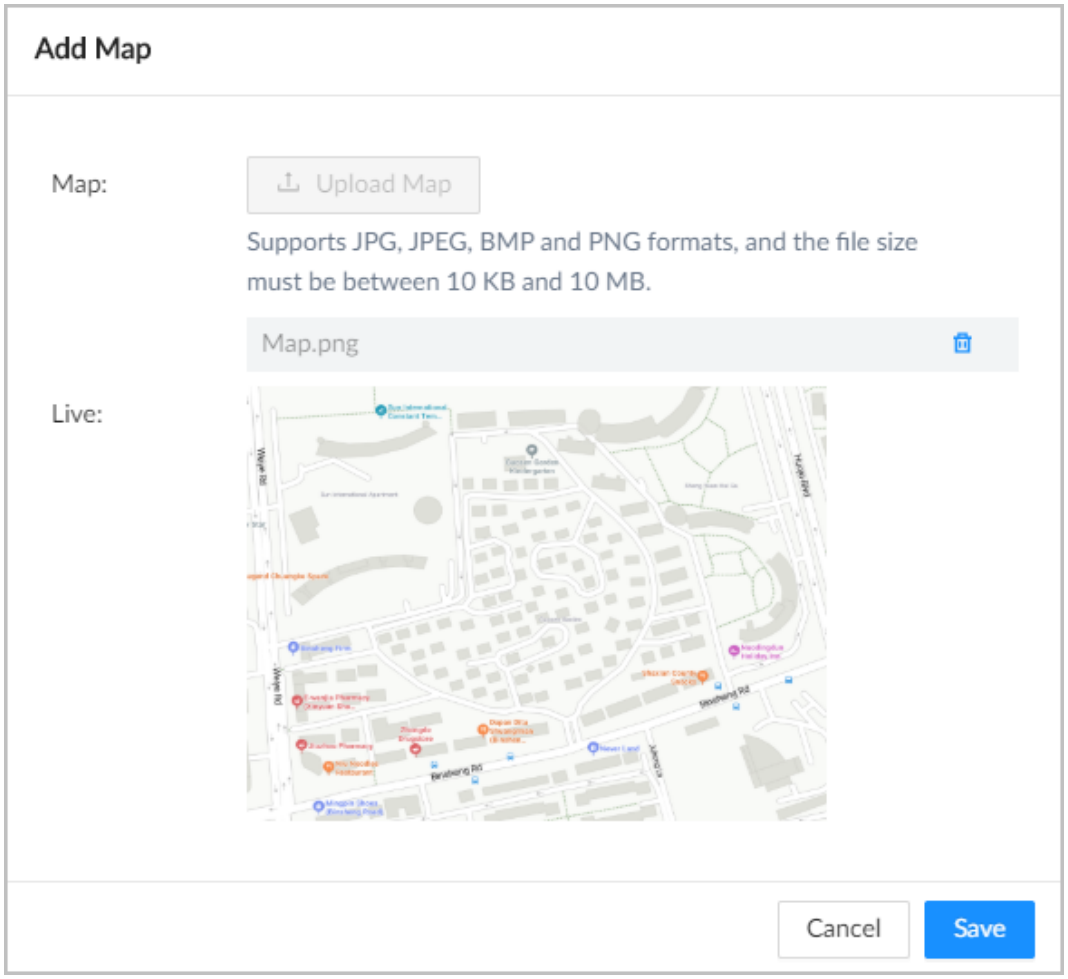
Step 2 Click on the upper-right corner, and then click **System** > **General** > **E-map**.

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

Step 3 Upload map.

1. Click **Add map** , and then click **Upload Map** in the pop up dialogs.
2. Select a map image locally, and then click **Open**.
3. Click **Save**.

Figure 8-85 Upload the map

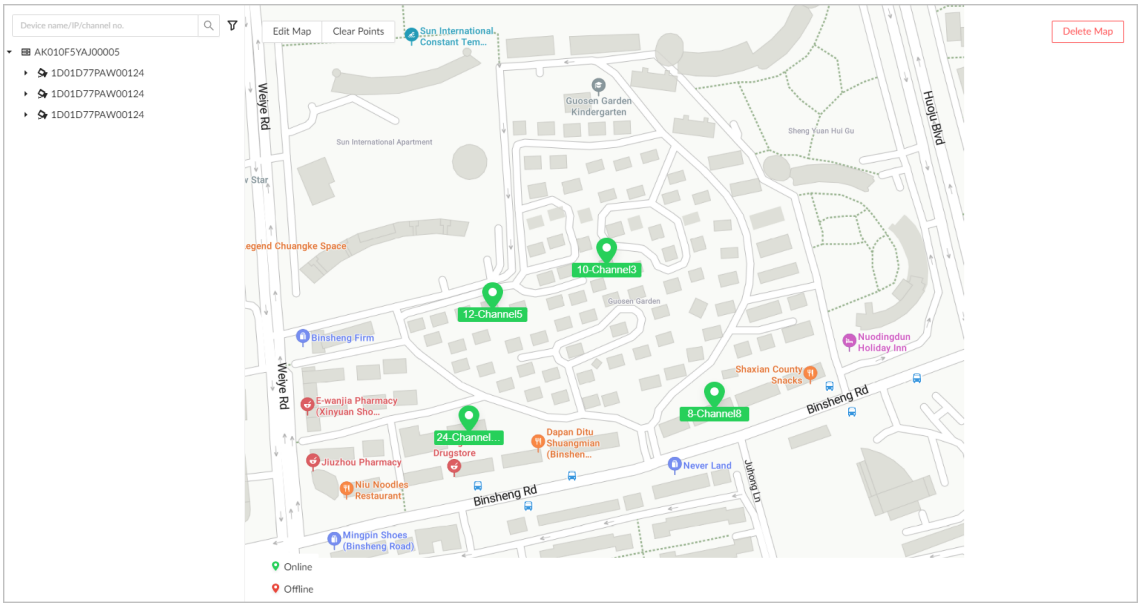


Step 4 Bind the channel to the map.

1. Expand the left channel list.
2. Drag the channel to designated the positions on the map according to the actual installation locations.

   Repeat this operation to complete the binding of multiple channels.

Figure 8-86 Bind the channel



Related Operations

E-map page supports the following operations.

- Clean points: Click **Clean Points**, and then delete all bound channel points on the map.
- Map replacement: Click **Edit Map** , click **Upload Map** in the pop-up dialog, and then select the new map. After uploading, the original map will be replaced and all points on it will be cleared.
- Delete map: Click **Delete Map** , click **OK** in the pop-up dialog.

8.6.2 Configuring Time Plan

8.6.2.1 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.

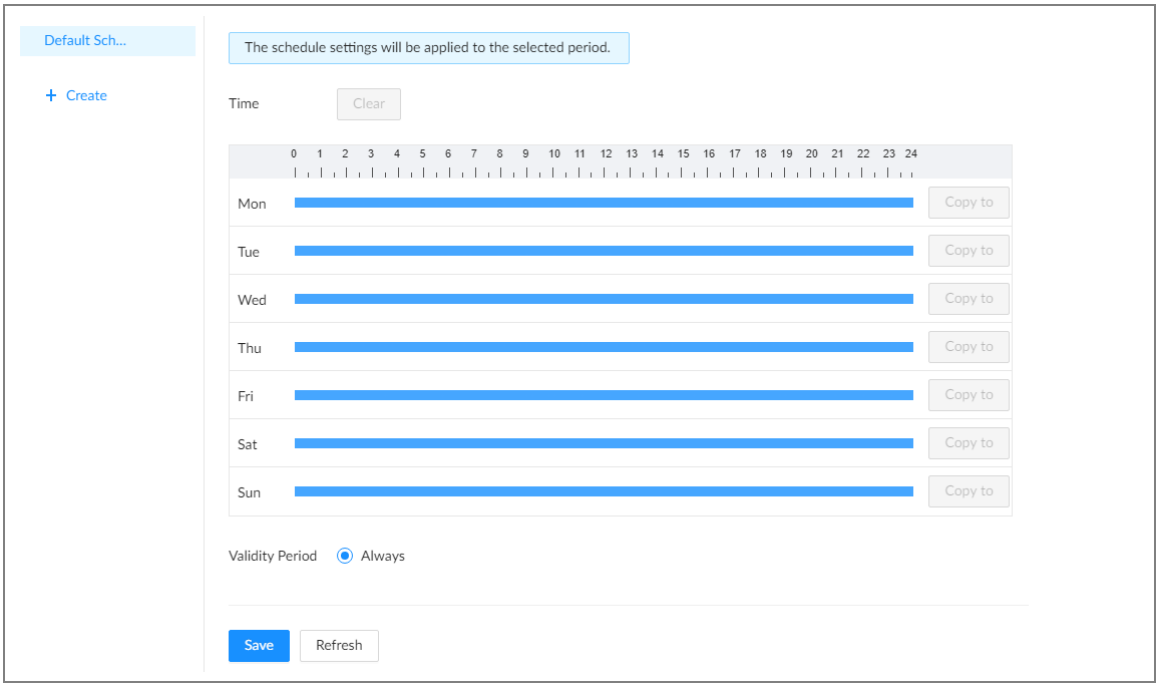
Default Schedule has been created by default, which is always effective and cannot be modified or deleted.

Procedure

Step 1 Log in to the PC client.

Step 2 On the configuration page, select **System** > **Time Plan** > **Time Plan**. Or click , and then select **System** > **Time Plan** > **Time Plan**.

Figure 8-87 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**, copy the current settings to other dates.

Step 5 Click **Save**.

Related Operations

Select a schedule and then click to delete it.

8.6.2.2 Configuring Holiday

Procedure

Step 1 Log in to the PC client.

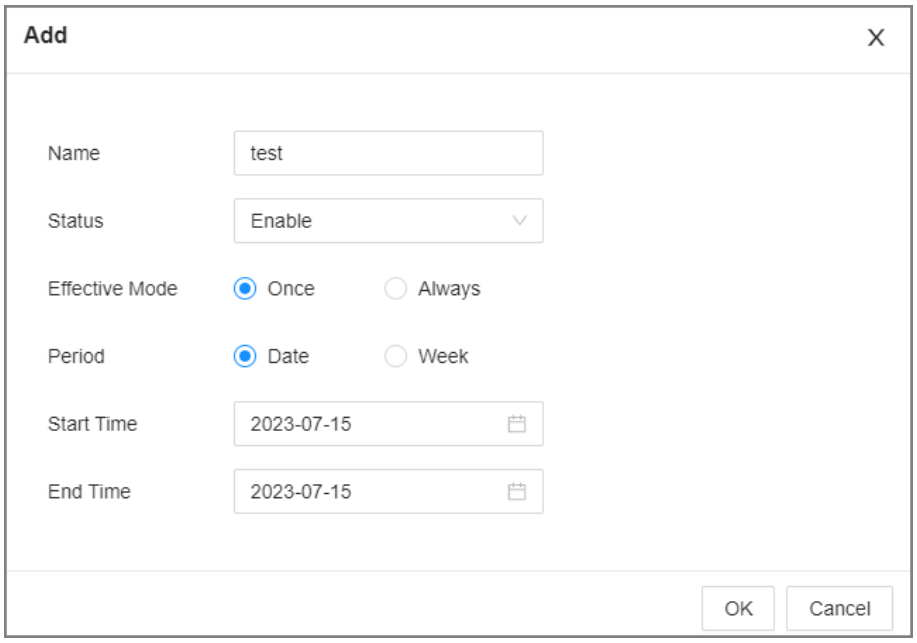
Step 2 On the configuration page, select **System** > **Time Plan** > **Holiday**. Or click , and then select **System** > **Time Plan** > **Holiday**.

Step 3 Add holidays.

1. Click **Add**.
2. Set the name and status.

3. Set the effective mode and period.
4. Set the time, and then click **OK**.

Figure 8-88 Add holiday



Step 4 Click **Apply**.

8.6.3 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).

8.6.3.1 Adding User Groups

The **admin** and **Onvif** groups are 2 default 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.

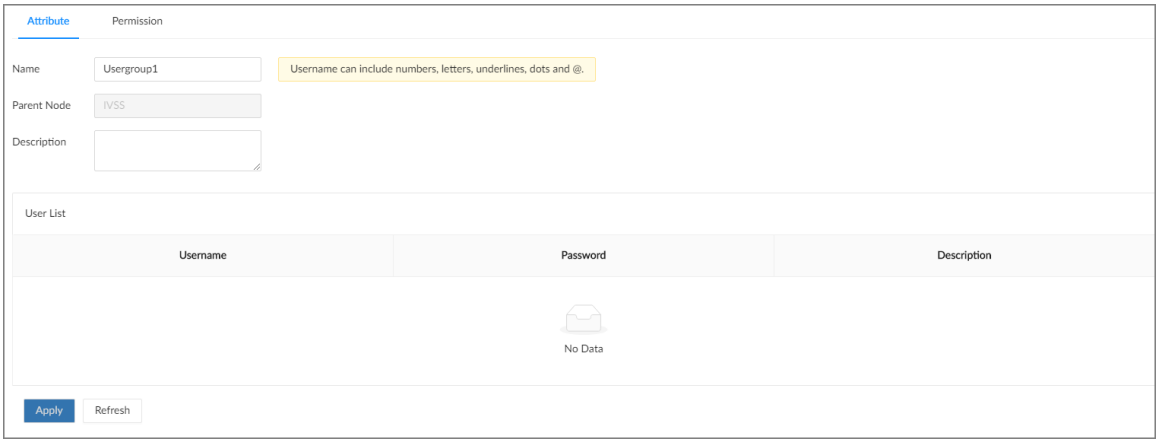
Step 2 Click on the upper-right corner and then click **Account**.

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 8-89 User group property



Step 5 Configure the parameters.

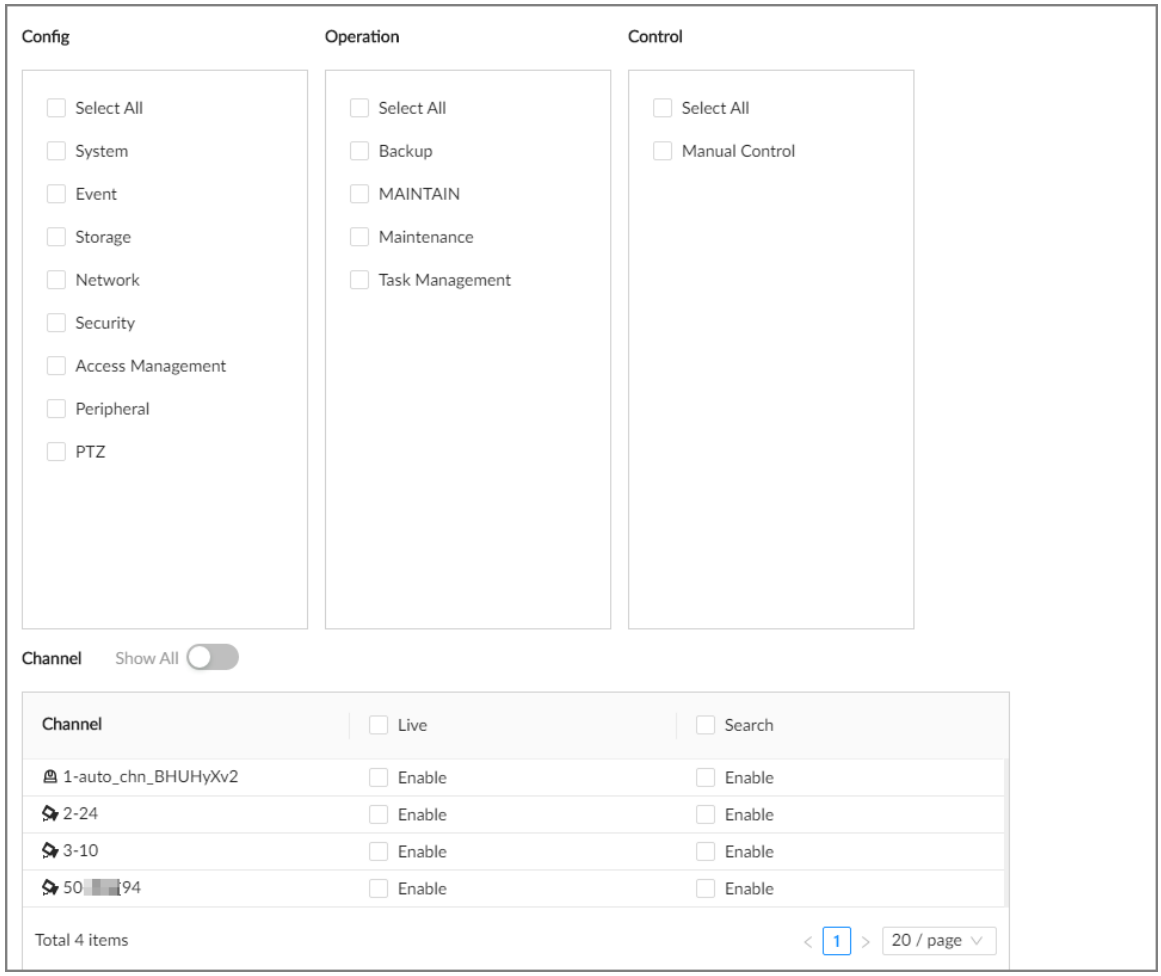
Table 8-37 User group attribute parameters

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 descriptions for the user group.
User List	Displays users in the group.

Step 6 Select user permissions.

1. Click the **Permission** tab.

Figure 8-90 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** and **Onvif** user groups cannot be deleted.

8.6.3.2 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.

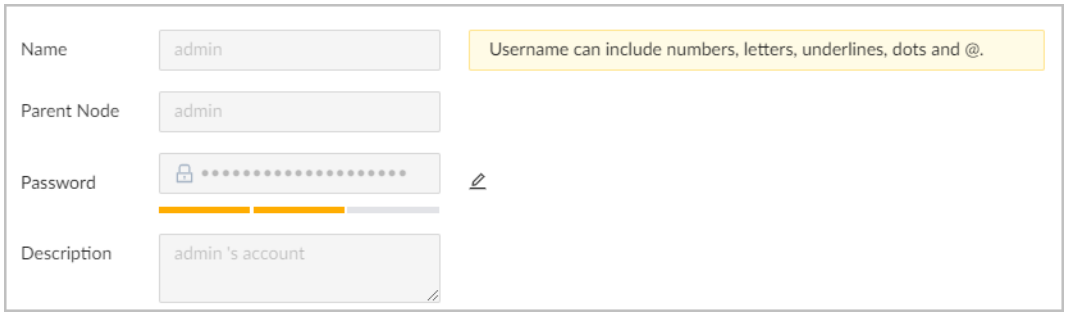
Step 2 Click on the upper-right corner and then click **Account**.

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 8-91 User attributes



Step 5 Configure the parameters.

Table 8-38 User attributes parameters

Parameter	Description
Name	Set the user name. The name ranges from 1 to 31 characters. It can contain English letters, numbers and special characters ("_", "@", ".").
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 descriptions for the user.

Step 6 Click the **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.

8.6.3.3 Password Maintenance

Maintain and manage the login passwords of users.

8.6.3.3.1 Changing Password of the Current User

Procedure

Step 1 Log in to the PC client.

Step 2 Select the root node.

Step 3 Click 

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**.

8.6.3.3.2 Changing Password of Other Users

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**.

8.6.3.3.3 Resetting the Password

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

Leaving Email Address and Security Questions

Enable the password reset function, leave an email address and set security questions. You can only use the local interface to set security questions.

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

   You can also click **Account** from the configuration list on the home page.
3. Select the root node at the upper-left corner.
4. Click  to enable the password reset function.
5. Enter an email address for resetting password.
6. Set security questions. You can only set security questions on the local interface of the Device.
7. Click **Apply**.

Resetting Password on Local Interface

1. Connect a monitor to the Device, and then go to the **Login** page of the Device.

2. Click **Forgot password?**.
3. Click **OK**.
4. (Optional) If you have not configured the linked email address, enter the email address and then click **Next**.
5. Select the reset mode and then reset the password.
   - Email.

     Follow the on-screen instructions to get the security code in your linked email address. After that, enter the security code and then click **Next**.
   - Security questions.

     Answer the security questions and then click **Next**.
6. Set parameters.

Table 8-39 Description of password parameters

Parameter	Description
User Name	The default user name is admin.
Password	Enter the new password and confirm the password.
Confirm Password	
Prompt question	After setting the prompt, when you point to on the login page, the system pops up a prompt to remind you of the password. The password prompt is available only on the login page of the local interface.

7. Click **Confirm Modify**.

   You can log in with the new password.

Resetting Password on the Web Interface or PC Client

Make sure that you have configured the linked email address.

1. Enter the IP address of the Device in the address bar of the browser or PC client, and then press Enter.
2. Click **Forgot password?**.
3. Click **OK**.
4. Follow on-screen instructions to get security code and then enter the security code.
5. Click **Next**.
6. Set a new password.

Table 8-40 Description of password parameters

Parameter	Description
User Name	The default user name is admin.
Password	Enter the new password and confirm the password.
Confirm Password	

7. Click **Confirm Modify**.

   You can log in with the new password.

8.6.3.4 Adding ONVIF User

The remote devices can connect with the Device through ONVIF protocol by using a verified ONVIF account.

There are 3 ONVIF user groups by default: **admin** , **user**, and **operator**. You can only add users in the 3 groups. You cannot create other ONVIF user groups.

Procedure

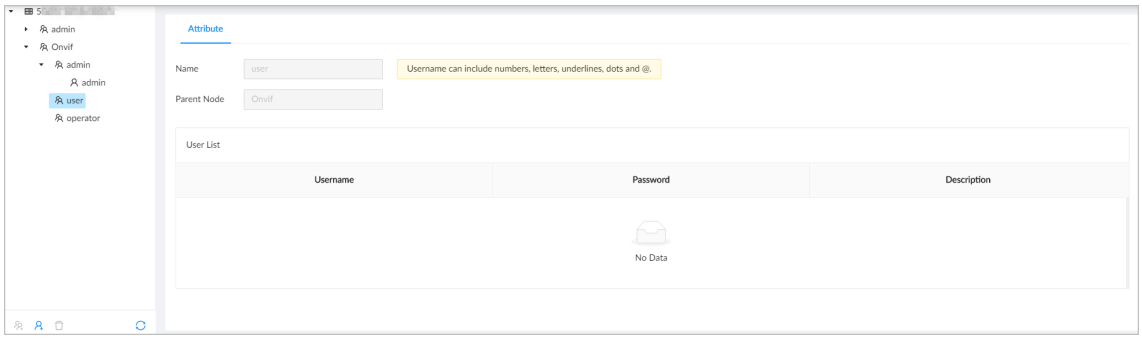
Step 1 Log in to the PC client.

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 an ONVIF user group, and then click .

Figure 8-92 ONVIF user group



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

Step 5 Set parameters.

Table 8-41 User attributes parameters

Parameter	Description
Name	Set the user name. 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 descriptions for the user.

Step 6 Click **Apply**.

Related Operations

Select an ONVIF user, and then click to delete it.

The admin ONVIF user cannot be deleted.

8.6.4 Security

8.6.4.1 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.

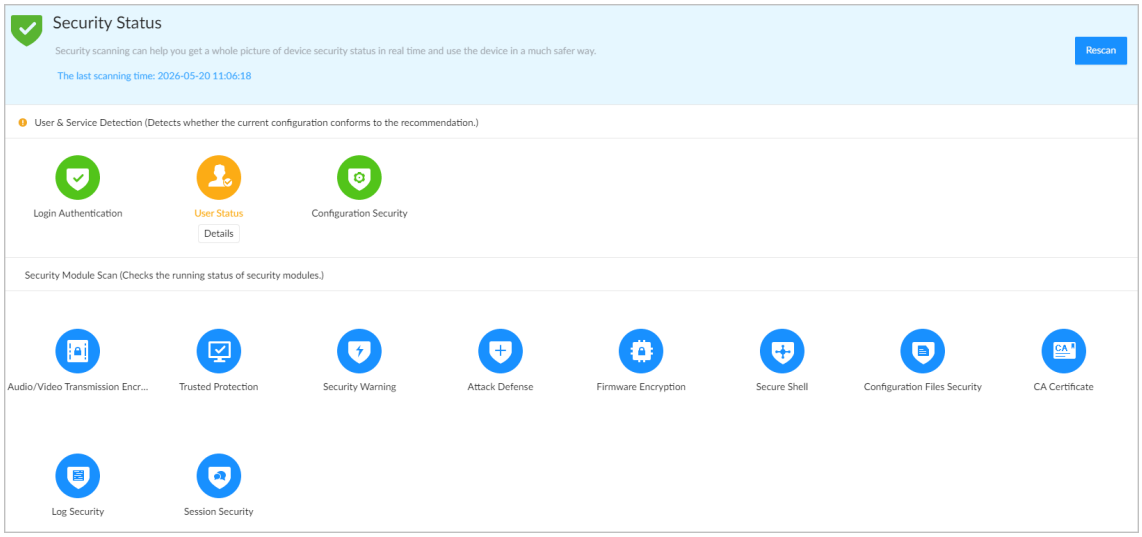
Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **System** > **Security** > **Security Status**.

Step 3 Click **Rescan**.

Figure 8-93 Security status



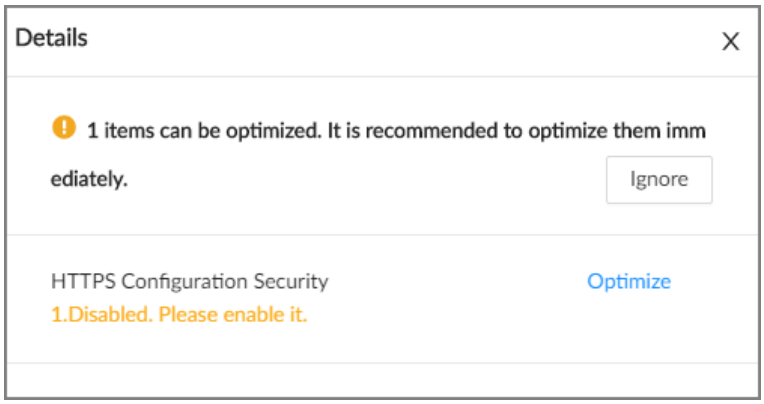
Related Operations

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.

Figure 8-94 Details



8.6.4.2 System Service

8.6.4.2.1 Basic Services

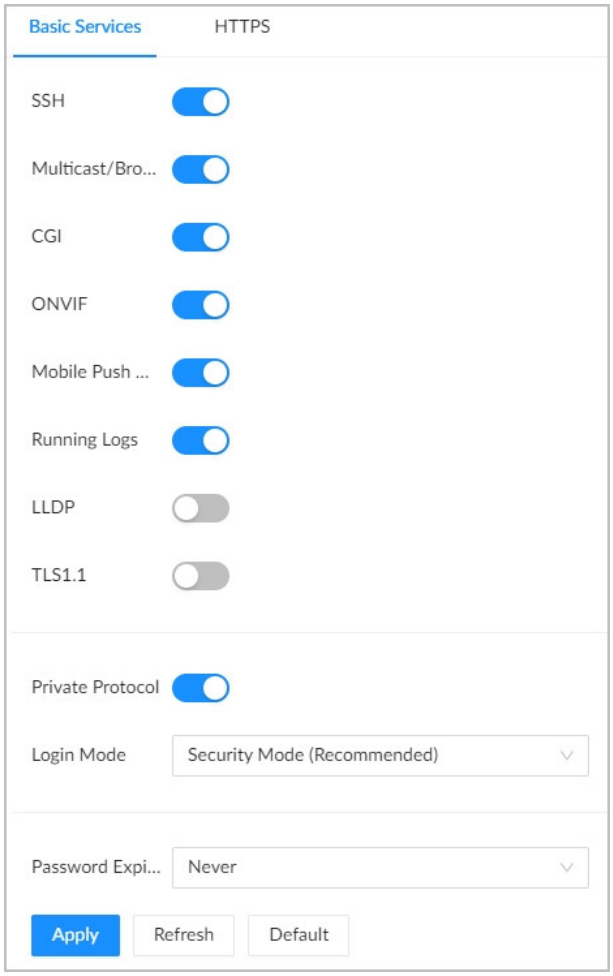
Enable basic system services for third-party access.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **System** > **Security** > **System Service** > **Basic Services**.

Figure 8-95 Basic services



Step 3 Enable or disable system services.

Table 8-42 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.
Multicast/ Broadcast Search	After enabled, you can multicast or search for broadcast devices.
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.

Name	Description
ONVIF	After this function is enabled, other devices can connect the Device through ONVIF protocol. For data security, we recommend you disable this function when it is not needed.
Mobile Push Notifications	After enabling this function, you can use your mobile phone to receive notifications from the Device. For data security, we recommend you disable this function when it is not needed.
Running Logs	After enabling it, you can view system running logs in **Maintain** > **Intelligent Diagnosis** > **Run Log**.
LLDP	Enable this function to help the network administrator identify the device.
TLS1.1	Enable the protocol compatibility.
Private Protocol	After enabled, the device can be accessed through this protocol.
Login Mode	Select an authentication mode between security mode and compatibility mode. Security mode is recommended.
Password Expires in	Configure the password expiration interval. The Device prompts you to change the password when the password expires.

Step 4 Click **Apply**.

8.6.4.2.2 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.

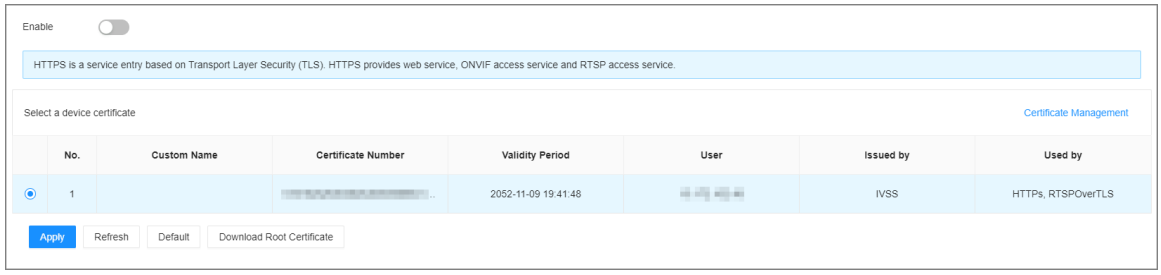
Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **System** > **Security** > **System Service** > **HTTPS**.

Step 3 Click  to enable HTTPS function.

Figure 8-96 HTTPS



Step 4 (Optional) Click to enable **Auto Redirect to HTTPS**.

Step 5 Click **Apply**.

You can use HTTPS to access the web interface.

Open the browser, enter https://*IP address:port* in the address bar, and then 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.

8.6.4.3 Attack Defense

8.6.4.3.1 Firewall

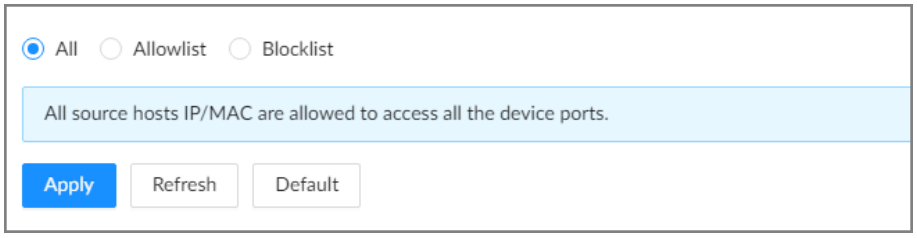
You can configure the hosts that are allowed or prohibited to access the Device.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **System** > **Security** > **Attack Defense** > **Firewall**.

Figure 8-97 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**.

8.6.4.3.2 Account Lockout

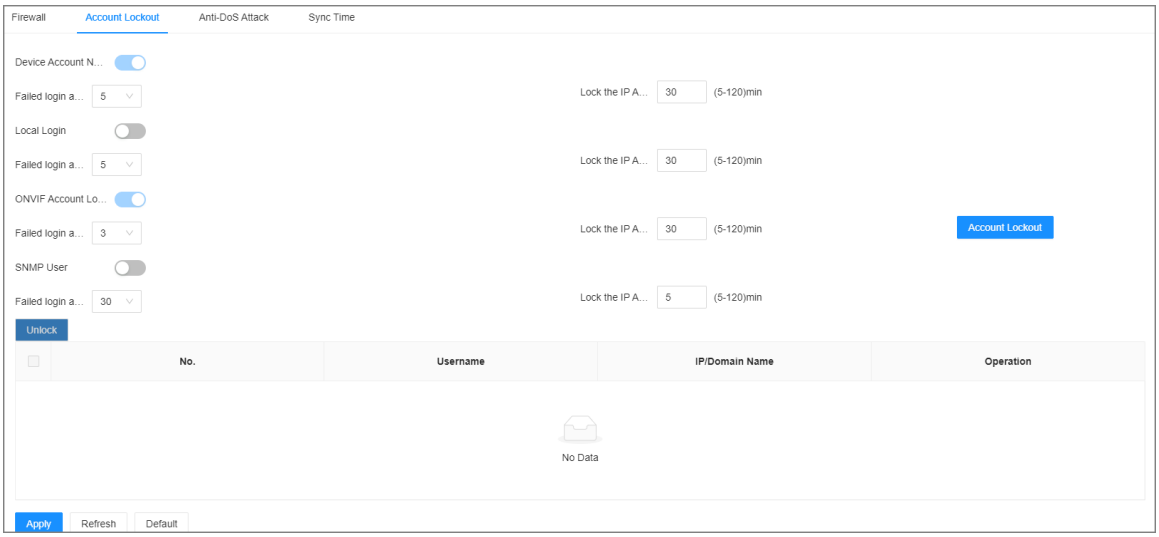
You can configure the number of allowed failed login attempts. When the number of failed login attempts reaches the defined threshold, the account will be locked for the defined duration.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **System** > **Security** > **Attack Defense** > **Account Lockout**.

Figure 8-98 Account lockout



Step 3 Click  to enable the lockout limitation for different types of login accounts, and then configure the number of allowed login attempts and lock duration.

The lockout limitation for network login of the device account and login of the ONVIF account is enabled by default and cannot be disabled.

Step 4 Click **Apply**.

Step 5 (Optional) Click Account Lockout to go to the **Event** page where you can configure the lockout alarm event.

8.6.4.3.3 Anti-Dos Attack

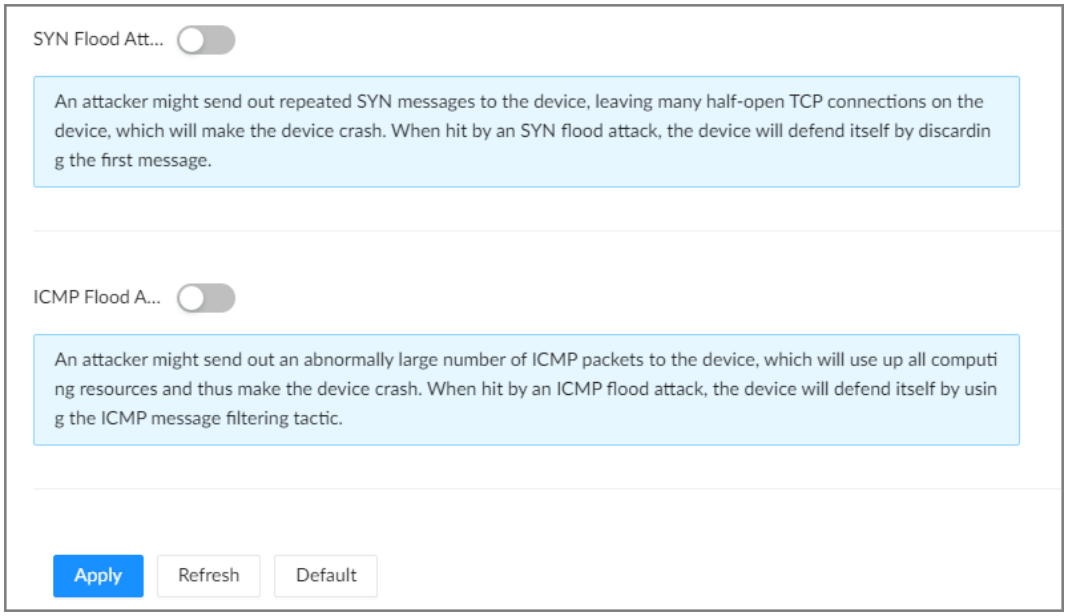
You can enable **SYN Flood Attack Defense** and **ICMP Flood Attack Defense** to defend the Device against Dos attacks.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **System** > **Security** > **Attack Defense** > **Anti-Dos Attack**.

Figure 8-99 Account lockout



Step 3 Click to enable **SYN Flood Attack Defense** or **ICMP Flood Attack Defense**.

Step 4 Click **Apply**.

8.6.4.3.4 Time Synchronization Permission

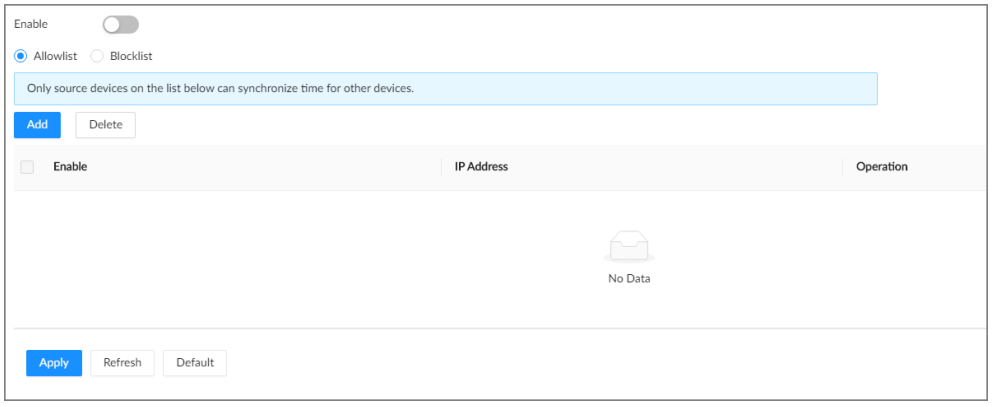
Configure permissions of time synchronization actions from other devices or servers.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **System** > **Security** > **Attack Defense** > **Sync Time**.

Figure 8-100 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. Support IPv4, IPv6 and domain.
2. Enter an IP address.
3. Click **OK**.

Step 6 Click **Apply**.

8.6.4.4 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.

8.6.4.4.1 Installing the Device Certificate

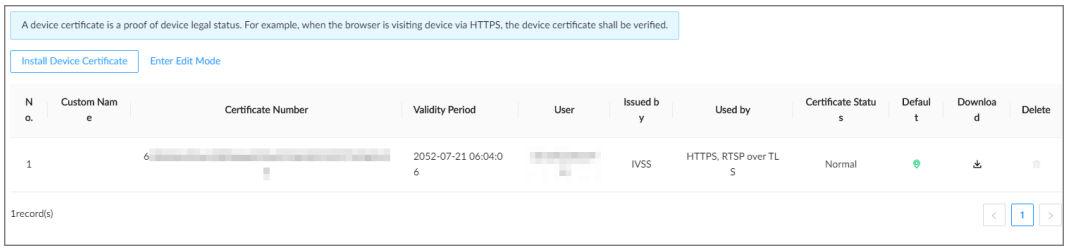
A device certificate is a proof of device legal status. For example, if you want to access IVD through a browser, you need to install the root certificate on your computer in advance.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **System** > **Security** > **CA Certificate** > **Device Certificate**.

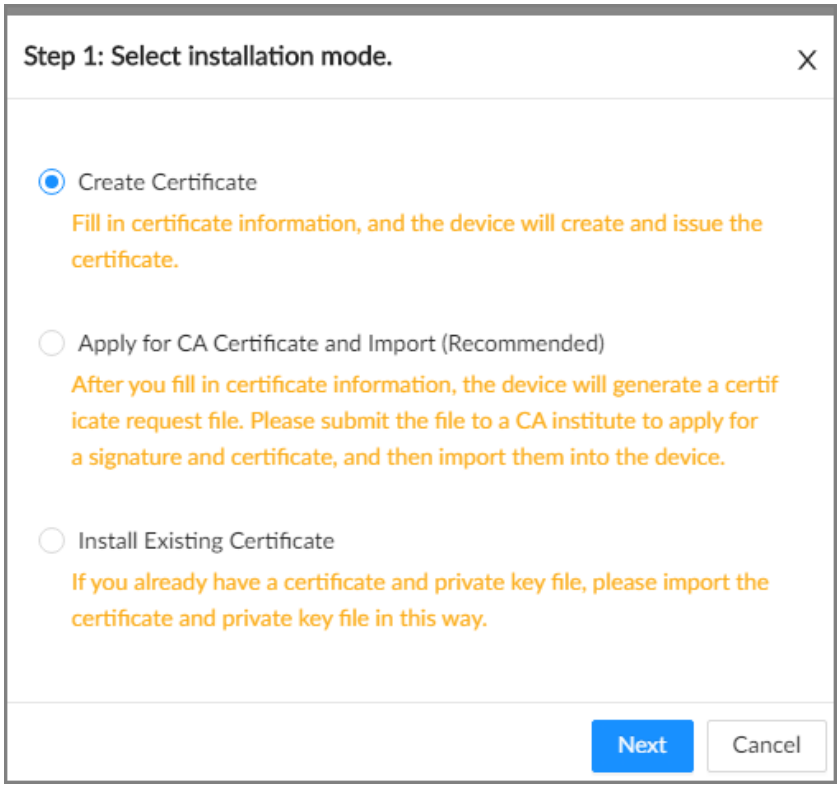
Figure 8-101 Device certificate



Step 3 Click **Install Device Certificate** to install a certificate in any of the following ways.

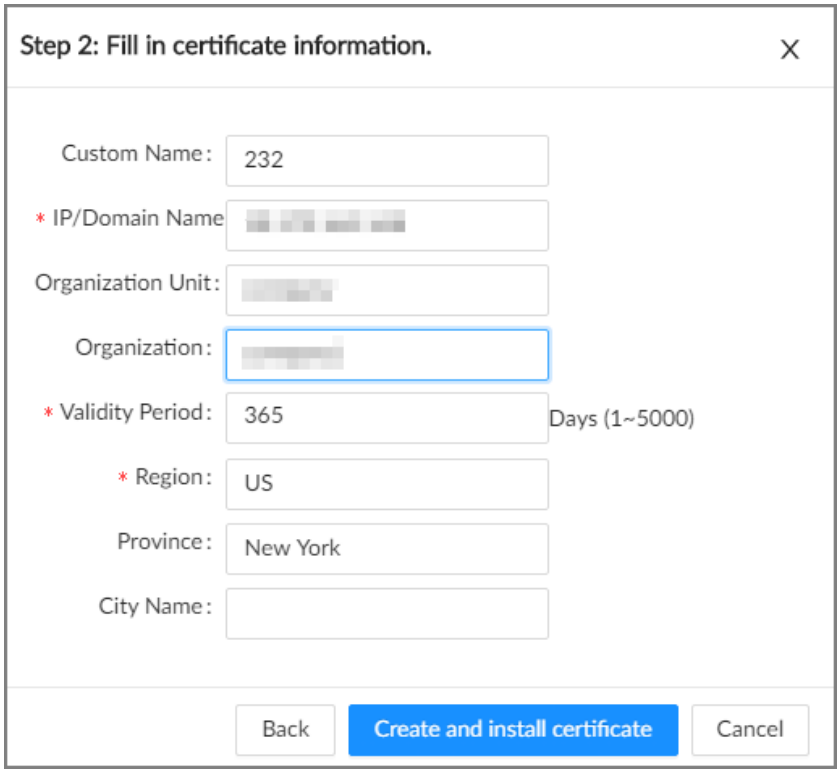
- Create a certificate.
  1. Select **Create Certificate** and then click **Next**.

Figure 8-102 Create certificate



2. Enter the information.

Figure 8-103 Certificate information



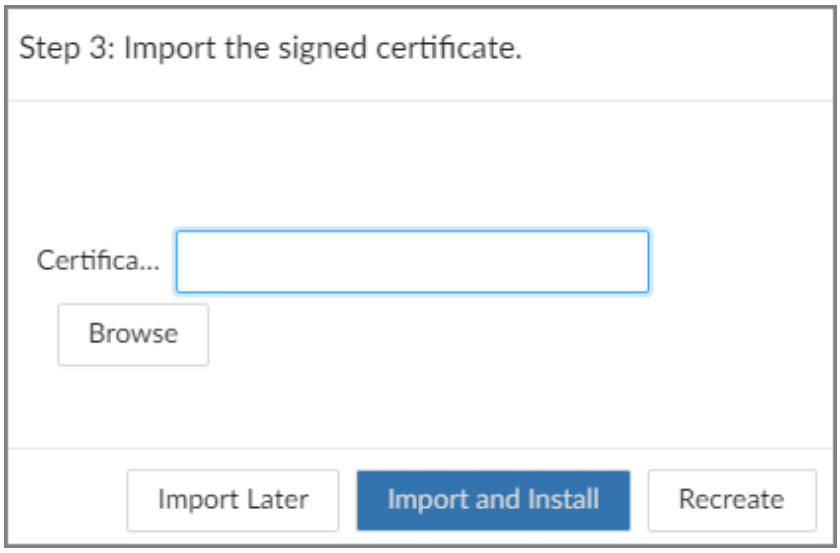
3. Click **Create and install certificate**.

- 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 8-104 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.

8.6.4.4.2 Installing the Trusted CA Certificate

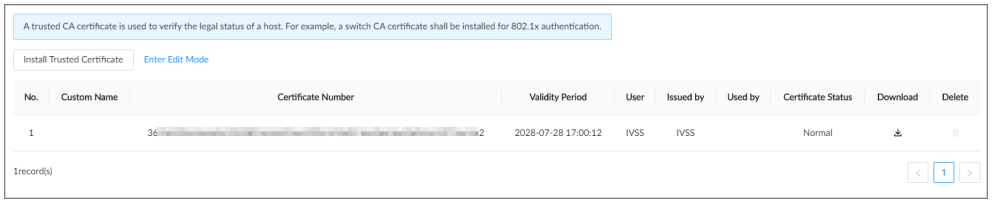
A trusted CA certificate is used to verify the legal status of a host. For example, a switch CA certificate must be installed for 802.1x authentication.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **System** > **Security** > **CA Certificate** > **Trusted CA Certificate**.

Figure 8-105 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.

8.6.4.5 A/V Encryption

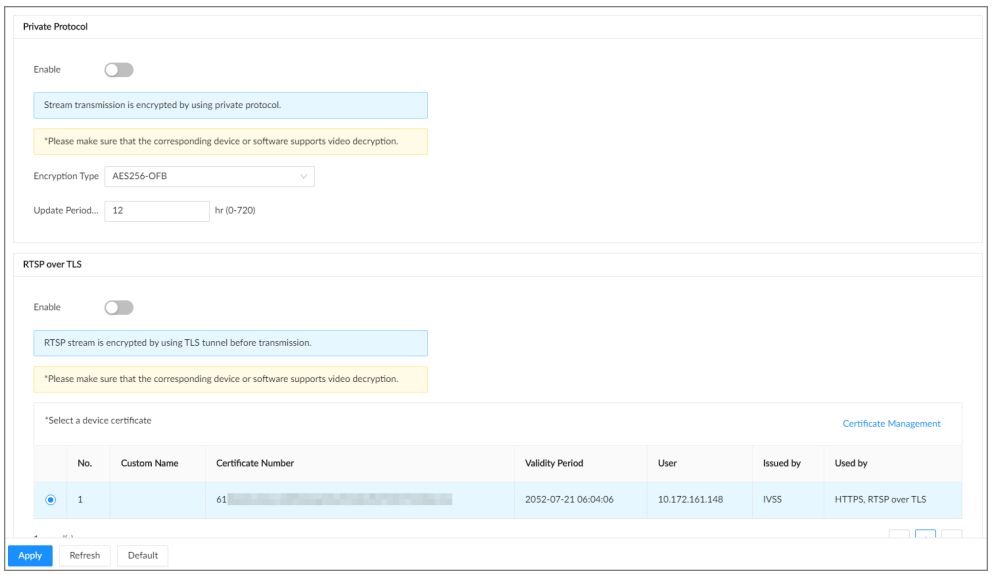
The Device supports audio and video encryption during data transmission.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **System** > **Security** > **A/V Encryption**.

Figure 8-106 Video encryption



Step 3 Configure the parameters.

Table 8-43 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**.

8.6.4.6 Security Warning

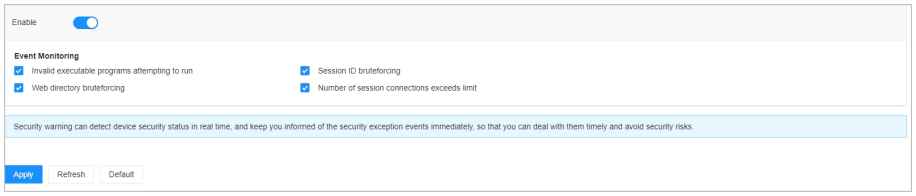
The Device gives warnings to the user when a security error occurs.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **System** > **Security** > **Security Warning**.

Figure 8-107 Security warning



Step 3 Click to enable the function.

Step 4 Select the events to be monitored.

Step 5 Click **Select** next to **Event Linkage** to set alarm actions.

Step 6 Click **Apply**.

8.6.4.7 Security Authentication

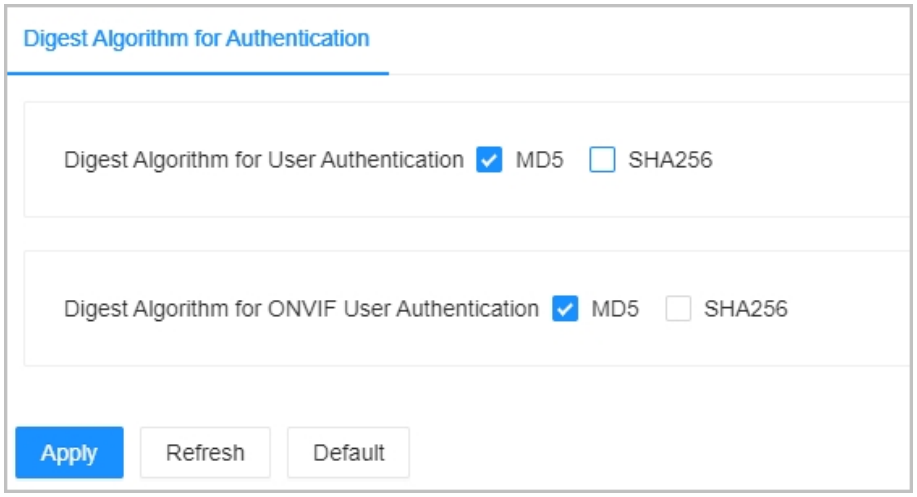
Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **System** > **Security** > **Security Authentication**.

Step 3 Select digest algorithm for authentication.

Figure 8-108 Security Authentication



Step 4 Click **Apply**.

8.7 AI Application

8.7.1 Resource Management

You can import and manage the video resource.

Procedure

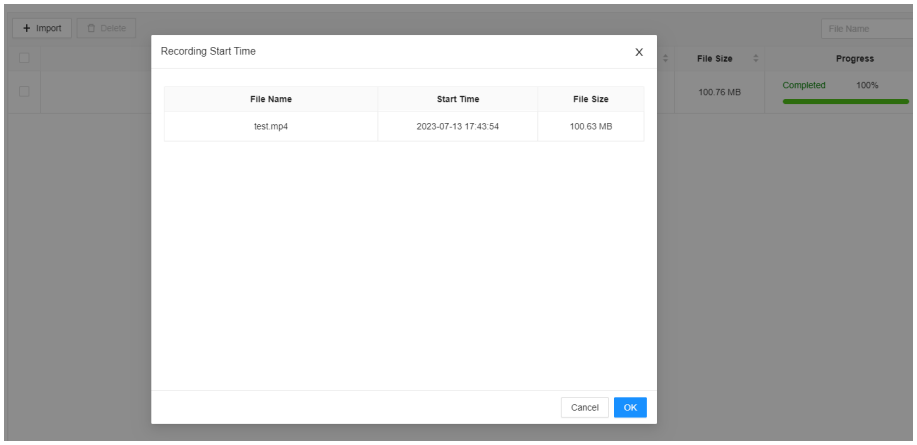
Step 1 Log in to the PC client.

Step 2 On the home page, select **AI Application** > **AI Analysis for File** > **Resources**.

Step 3 Click **Import** to import files in .dav or .mp4 formats from local or external storage devices.

When importing files in .mp4 format, you need to configure the **Start Time** for the video.

Figure 8-109 Import files



8.7.2 AI Analysis Task

Create AI analysis tasks and metadata analysis historical recordings of channels. After the AI analysis is completed, the structured analysis results can be searched on the AI search page.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **AI Application** > **AI Analysis for File** > **AI Analysis Task**.

Step 3 Click **Manual Create**.

- Video file: Select **Video File**, and then select video file on the device tree.
- Local file: Select **Local File**, and then select channel on the device tree.

Step 4 Select the analysis type of the channel, click to enable the corresponding task, and then click **OK**.

- Click **Unified configuration** to configure the analysis type in batch.
- To enable the face analysis function, you must first enable the human body analysis function. It is not supported to enable the face analysis function separately.
- Non-motor vehicle analysis function must be enabled first. It is not supported to enable the non-motor vehicle analysis function separately.

Step 5 Select the start time and end time.

Step 6 Click **Add**.

Related Operations

Check the analysis result.

- When the type is **Human**, see "6.7.4.1 Human Search".
- When the type is **Motor Vehicle**, see "6.7.4.2.1 Searching by Attributes".
- When the type is **Non-Motor Vehicle**, see "6.7.4.3 Non-motor Vehicle Search".
- When the type is **Face**, see "6.5.4 Face Search".

8.7.3 Extracting Eigenvector Again

Re-extract Eigenvector of images with unmatched versions, to improve AI analysis accuracy.

The Extract Eigenvector Again function is triggered automatically after Eigenvector model is updated. After the model version update, the system re-extracts face sample databases and passerby databases first and then hot data. The hot data includes history capture data.

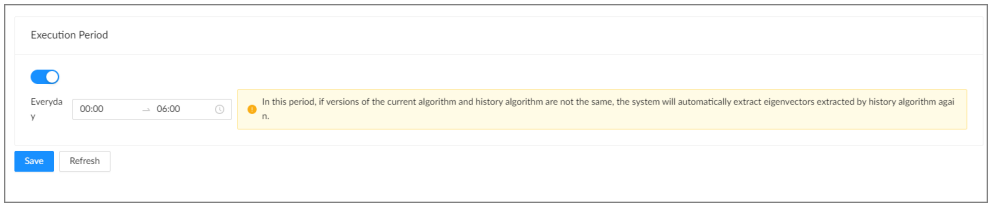
Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **AI Application** > **Extract Eigenvector Again**.

Step 3 Click to enable the function.

Figure 8-110 Extract Eigenvector again



Step 4 Set the start time and end time of the day.

- The system automatically creates tasks to re-extract Eigenvector of historical images with unmatched model versions during the period.
- During the re-extraction period, AI by Recorder is not available.

Step 5 Click **Save**.

8.7.4 1:1 Face Recognition

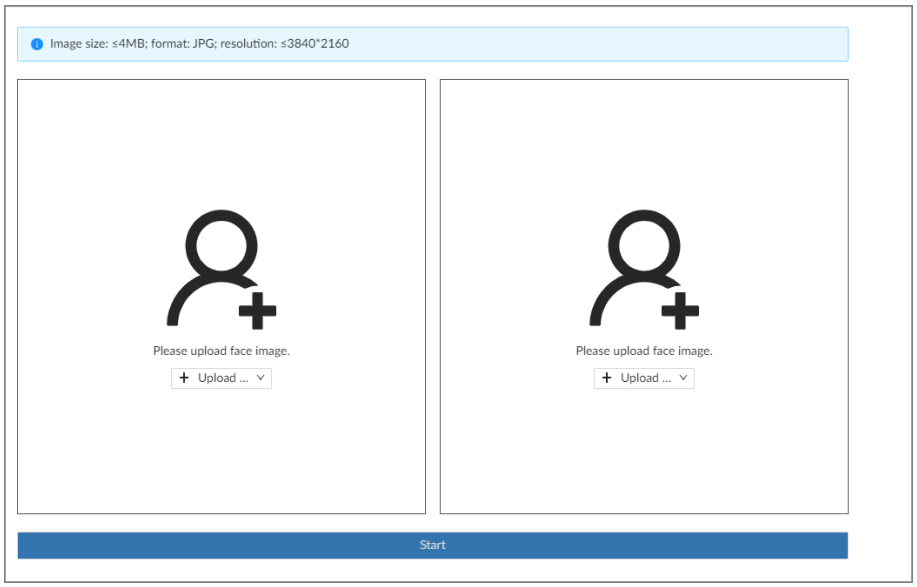
Through 1:1 face comparison, the system analyzes the similarity between two images.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **AI Application** > **1:1 Face Recognition**.

Figure 8-111 1:1 face comparison



Step 3 Click **Upload** and then upload 2 images to be compared.

Image sources include the sample database, the passerby database and the local image.

- Sample Database Image: Set the search conditions, click **Search** , and then the page will display the images retrieved from the sample database. Select the face images and click **OK**.
- Passerby Database Image: Set the search conditions, click **Search** , and then the page will display the images retrieved from the passerby database. Select the face images and click **OK**.
- Local Image: Select the face images from the local storage.

Step 4 Click **Start**.

The comparison result is displayed.

9 System Maintenance

9.1 Overview

Log in to the PC client. On the home page, select **Maintenance** > **Overview**.

Figure 9-1 Overview

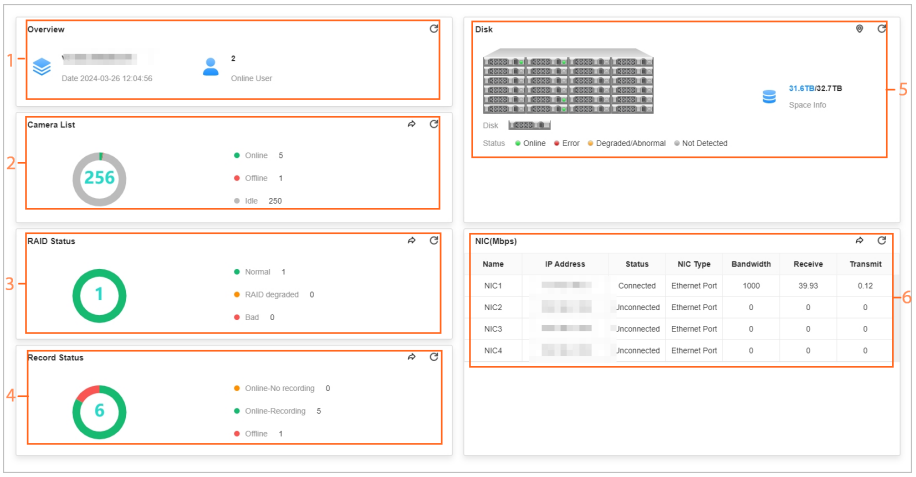


Table 9-1 Overview

No.	Function	Description
1	Overview	View device version details and 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	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
4	Disk	• View disk status and storage usage. ◇ : disk online. ◇ : disk error. ◇ : disk warning. ◇ : 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.
5	NIC (Mbps)	View NIC status. • Click to go to the **TCP/IP** page for detailed information. • Click to refresh the data.

9.2 System Information

9.2.1 Viewing Device Information

Log in to the PC client. On the home page, select **Maintenance** > **System Info** > **Device Info**. You can view device information such as input bandwidth, system version, and web version.

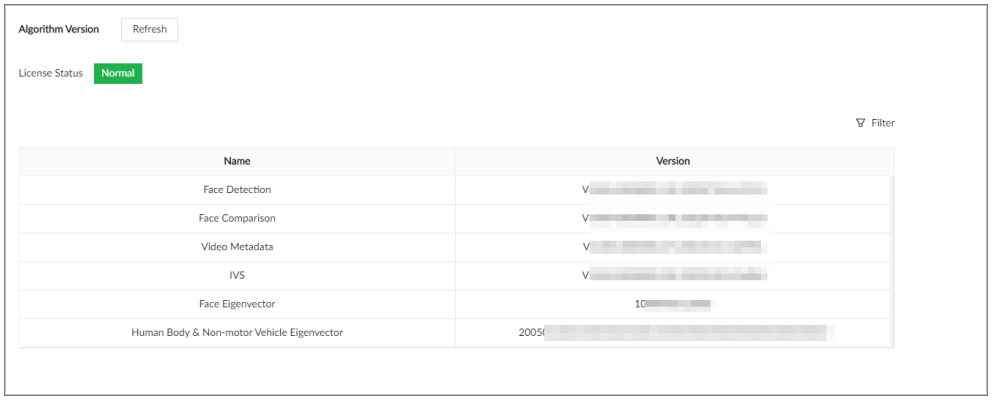
9.2.2 Viewing Legal Information

Log in to the PC client. On the home page, select **Maintenance** > **System Info** > **Legal Info**. You can view the software license agreement, privacy policy, and open-source software note.

9.2.3 Viewing Algorithm Version

Log in to the PC client. On the home page, select **Maintenance** > **System Info** > **Algorithm Version**. You can view the algorithm license status and versions of smart functions.

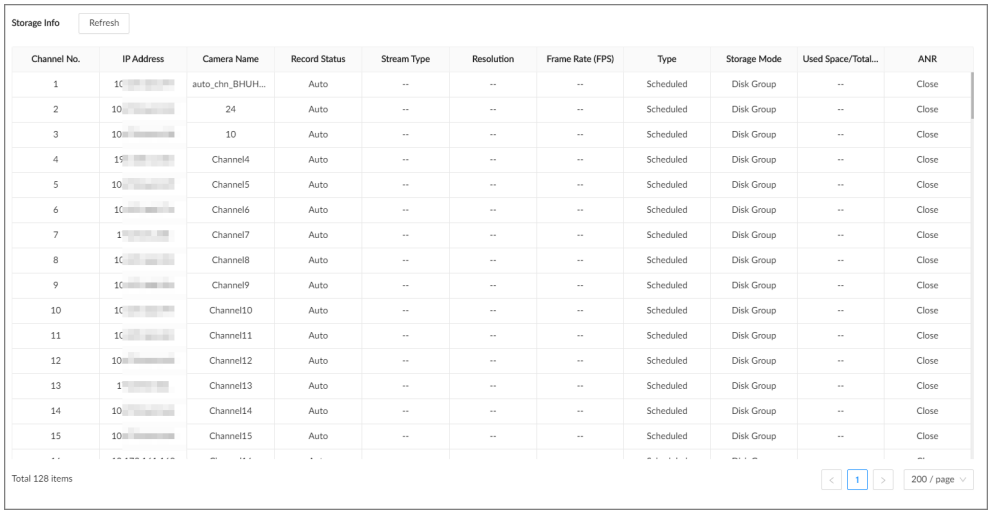
Figure 9-2 Algorithm version



9.2.4 Viewing Storage Information

Log in to the PC client. On the home page, select **Maintenance** > **System Info** > **Storage Info**. You can view the storage information of each channel.

Figure 9-3 Storage information



9.2.5 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** > **System Info** > **Online User**.

The list displays currently connected users.

Figure 9-4 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.

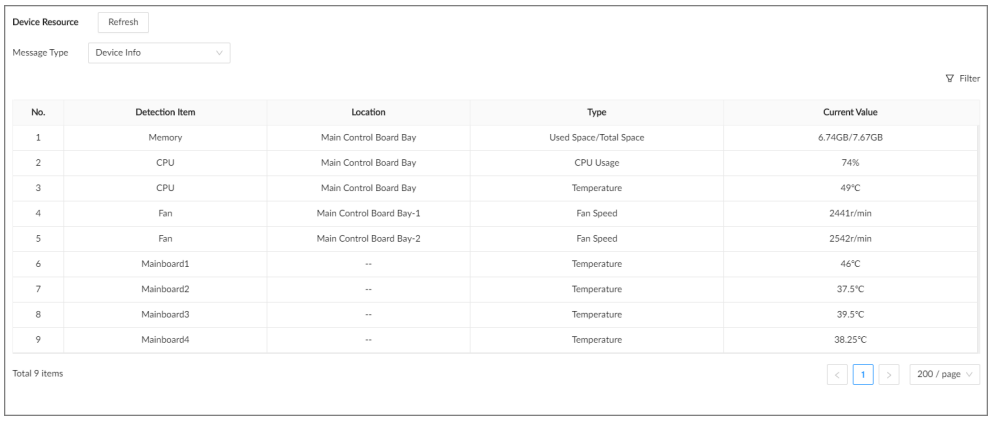
Step 5 Click **OK**.

9.3 System Resources

9.3.1 Viewing Device Resources

Log in to the PC client. On the home page, select **Maintenance** > **System Resources** > **Device Resource**. You can view resource status including CPU and memory usage, mainboard temperature and fan speed.

Figure 9-5 System resources



- Click to select the items that you want to view.
- Click **Refresh** to refresh the data.

9.3.2 Viewing AI Module Information

Log in to the PC client. On the home page, select **Maintenance** > **System Resources** > **AI Module Resource**. You can view the status of AI modules.

9.4 Network Detection

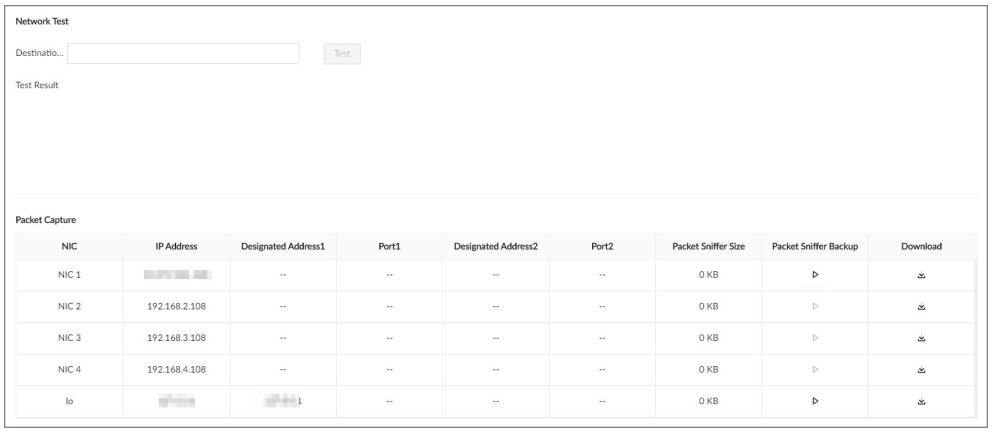
You can test network connection and capture packets. Packet capture is the practice of intercepting a data packet that is crossing or moving over a specific computer network. The captured packet is stored temporarily for analysis. The packet is inspected to help diagnose and solve network problems and 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** > **Network Detection** > **Network Test**.

Figure 9-6 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.

9.5 Disk Maintenance

Check the disk status to handle disk errors in time.

9.5.1 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** > **Disk Maintenance** > **S.M.A.R.T Detection**.

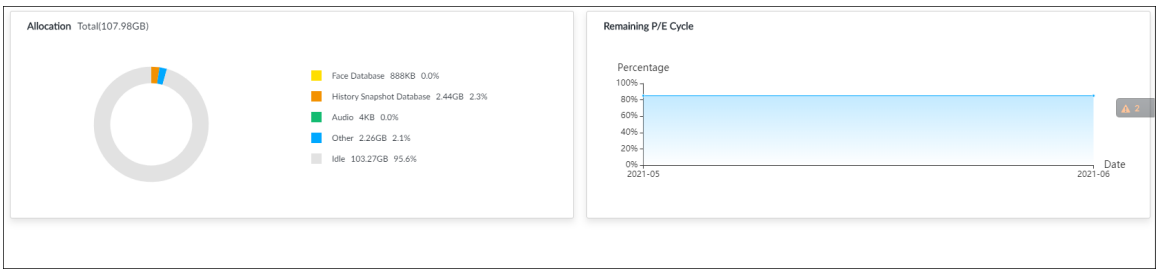
Step 3 Set the detection period.

Step 4 Click **OK**.

9.5.2 System Disk Health Detection

On the home page, select **Maintenance** > **Disk Maintenance** > **System Disk Health Detection**, and then you can view the storage allocation and remaining P/E cycle of system disk.

Figure 9-7 System Disk health detection



9.5.3 Firmware Update

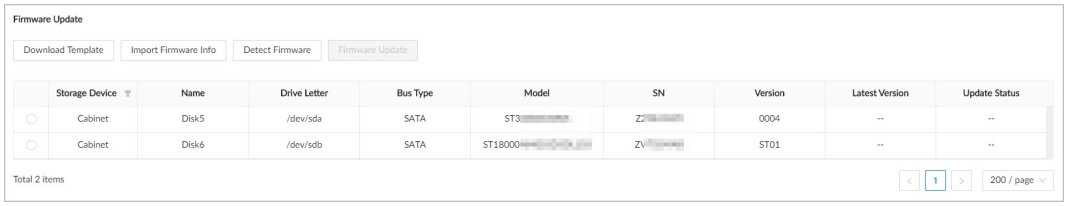
Import update file to update HDD information.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **Maintenance** > **Disk Maintenance** > **Firmware Update**.

Figure 9-8 Firmware update



Step 3 Click **Download Template** to download the update template.

Step 4 Click , select **Download**, and then open and fill in the downloaded template.

Step 5 Select a disk, click **Import Firmware Info** , click **Browse** to choose the template to be imported, and then click **OK**.

Step 6 Click **Firmware Update** to update the firmware information.

Step 7 Click **Detect Firmware** to refresh the firmware information on the page.

9.6 Log Info

The logs record all kinds of system running information. We recommend you check the logs periodically and fix the problems in time.

9.6.1 Log Classification

Table 9-2 Log categories

Log	Type
System log	Logs of system running status, file management, hardware detection and scheduled task.
User operation log	User operation and user configuration logs.
Event log	Logs of different events, such as IP conflict, MAC conflict, login lock, and stay detection.
Connection log	Logs of user login and logout, session hijack, session blast and camera list.

9.6.2 Log Search

You search for different categories of logs. This section uses system logs as an example.

Procedure

Step 1 Log in to the PC client.

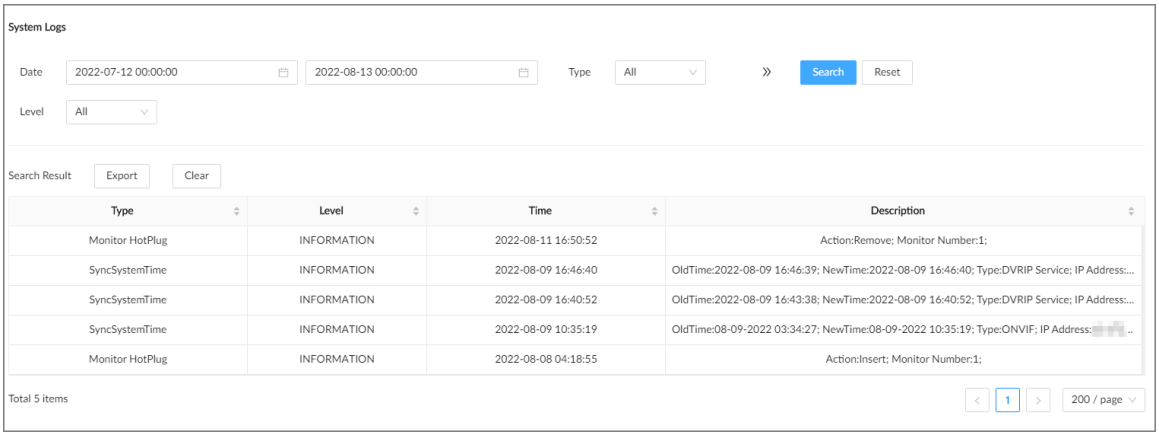
Step 2 On the home page, select **Maintenance** > **Log Info** > **System Logs**.

Step 3 Set the search period, and then select the log type.

Step 4 (Optional) Click », and then select a log level.

Step 5 Click **Search**.

Figure 9-9 System logs



Related Operations

- Export logs.

  Click **Export** to export the logs. You can select whether to encrypt the exported logs.

  - Select **Yes** , set a password, and then click **OK**. The exported logs will be encrypted. The password is required to unzip the exported file.
  - If you select **No**, the logs will be exported to your computer or USB storage device without encryption.

    Keep the unencrypted logs safe to prevent data leakage.

- Clear logs.

  Click **Clear all** to clear all the logs.

  You might be unable to track the reasons of system errors if you clear logs.

9.7 One-click Diagnosis

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **Maintenance** > **One-click Diagnosis**.

Step 3 Click **Diagnose** , and then click **View Details** to view the corresponding diagnosis information.

9.8 Advanced Maintenance

9.8.1 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.

9.8.2 Running Logs

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** > **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**.

9.8.3 Operator Maintenance

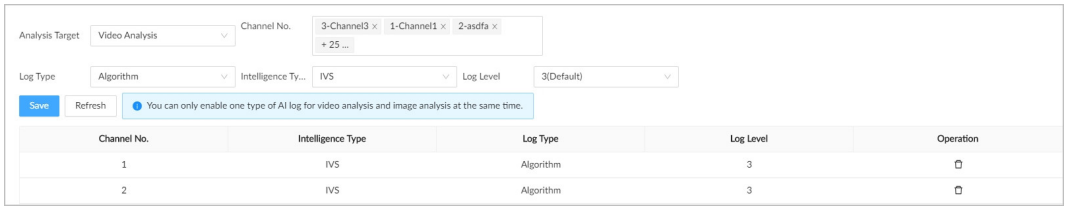
Procedure

Step 1 Log in to the PC client. On the home page, select **Maintenance** > **Advanced Maintenance** > **Operator Maintenance**.

Step 2 Select the analysis type, channel number, log type, intelligence type and log level.

The higher the log level, the more information is printed, which helps in troubleshooting and identifying the cause of issues.

Figure 9-10 Operator maintenance



Step 3 Click **Save** to change the log level.

9.9 Updating

9.9.1 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.

- When operating on the local interface, save the update file in the USB storage device and then connect the USB storage device to the IVD.
- When operating on the web interface or PC client, save the update file on your computer.



- During update, do not disconnect the Device from power and network, or restart or shut down the Device.
- Make sure that the update file is correct. Improper update file might result in device error.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **Maintenance** > **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.

9.9.2 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.

- When operating on the local interface, save the update file in the USB storage device and then connect the USB storage device to the IVD.
- When operating on the web interface or PC client, save the update file on your computer.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **Maintenance** > **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.

9.9.3 Camera Update

You can import the update file to update the cameras.

Prerequisites

You need to obtain the correct update file and save it in the corresponding path.

- When operating on the local interface, save the update file in the USB storage device and then connect the USB storage device to the IVD.
- When operating on the web interface or PC client, save the update file on your computer.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **Maintenance** > **Update** > **Camera Update**.

Step 3 Select one or more cameras and then click **File upgrade**.

Stop recording before update. If you are updating a camera that is recording, the system will prompt you to disable recording first.

Step 4 Click **Browse** to select an update file.

Step 5 Click **Update Now**.

Step 6 Click **OK**.

9.10 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.

9.10.1 Default

When the system runs slowly and has configuration errors, try to solve the problems by restoring the default settings.

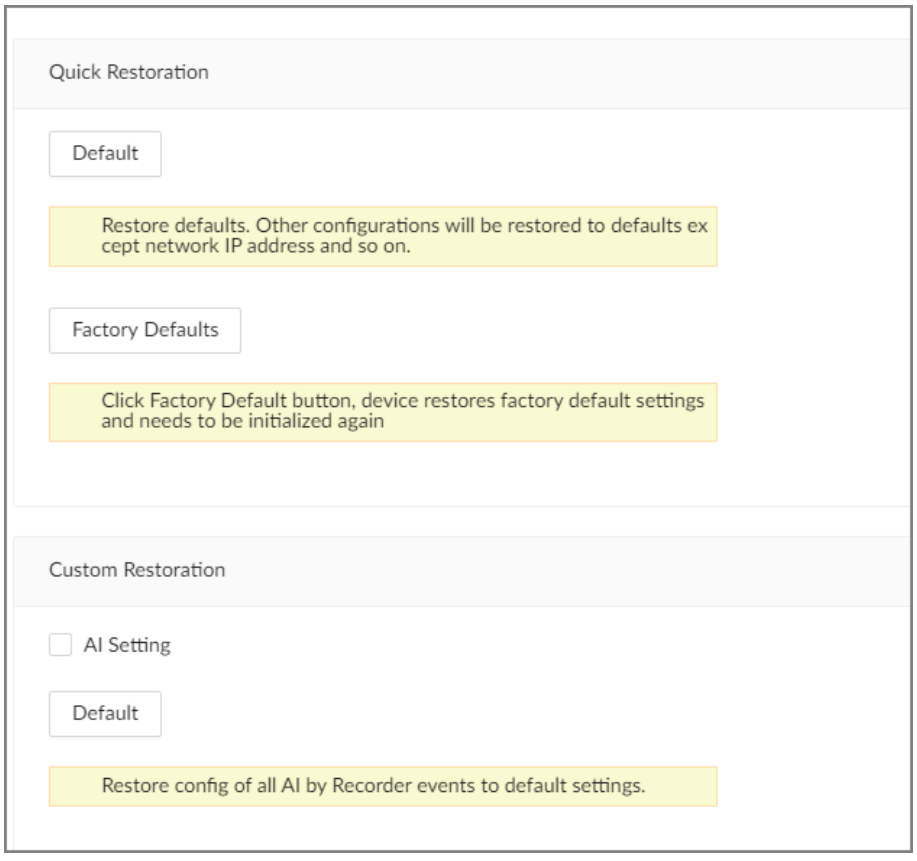
All configurations are lost after factory default operation.

Procedure

Step 1 Log in to the PC client.

Step 2 On the home page, select **Maintenance** > **Maintenance Management** > **Default**.

Figure 9-11 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.

9.10.2 Maintenance

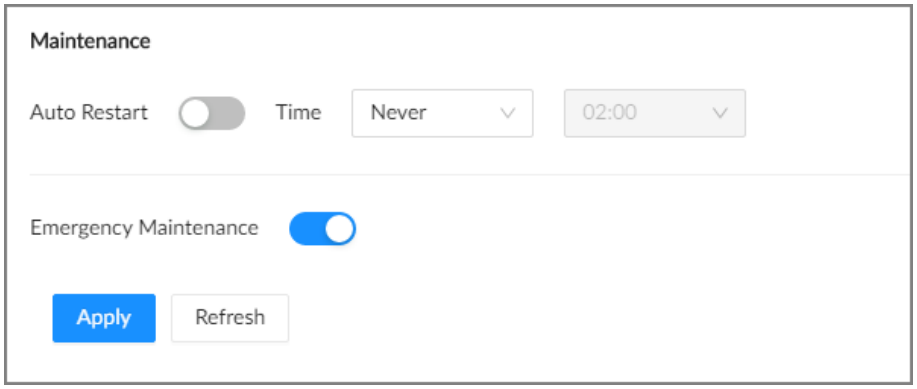
If the device has run for a long time, you can set the Device to automatically restart at idle time.

Procedure

Step 1 Log in to thee PC client.

Step 2 On the home page, select **Maintenance** > **Maintenance Management** > **Maintenance**.

Figure 9-12 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**.

9.10.3 Configuration 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** > **Maintenance Management** > **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.

10 PC Client

After installing the PC client, you can access the Device remotely through the PC client to carry out system configuration, function operations and system maintenance.

10.1 Page Description

Double-click the shortcut icon of the PC client on the desktop of your computer.

Figure 10-1 Taskbar



Table 10-1 Icons

Icon	Description
PCAPP Please Enter URL	Address bar: Enter the IP address of the Device.
	Enter IP address and then click the button to go to the login page. The icon turns into . Click to refresh the page.
	View history login records, downloads, client settings and client version.
	Minimize the client.
	Maximize the client.
	Display the client at full screen.
	Close the client.

10.2 History Record

Click , and then select **History**.

You can view history access records and clear cache.

- Click **Clear History** to clear all history records.
- Click **Clear Cache** to clear cache data, and restart the PC client.

10.3 Viewing Downloads

To view and clear history downloads, click , and then select **Download** . The **Downloads** window is displayed.

- Double-click a file name to open it.
- Click **Displayed in Folder** to open the folder where the file is located.
- Click **Clear** to clear history download records.

10.4 Configuring the Client Settings

When the theme of your computer is not Aero, videos might not be displayed normally on the PC client. We recommend you switch the computer theme to Aero, or enable the compatibility mode of the client.

Switching Computer Theme

This section uses Windows 7 as an example.

Right-click any blank position on the computer desktop, select **Personalize**, and then switch to Aero theme. Restart the PC client to make the Aero theme take effect.

Setting Video and Picture Storage Path

Click **Browse** to specify the paths for saving videos and pictures. This function is available only on the PC client.

Enabling Compatibility Mode

Click ≡, and select **Settings** . Select the checkbox to enable **Compatibility Mode**. Restart the PC client to make the compatibility mode take effect.

Enabling Hardware Acceleration

Click ≡, and select **Settings** . Select the checkbox to enable **Enable hardware acceleration (it will take effect after video is opened again)**.

The live videos become more fluent when this function is enabled.

Enabling Audio Linkage

Click ≡, and select **Settings** . Select the checkbox to enable **Enable audio linkage** and the event linkage configuration sets the linkage audio.

When the event alarm is triggered, the linkage PCAPP broadcasts the voice.

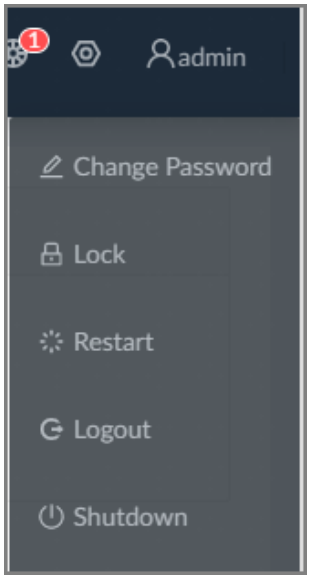
10.5 Viewing the Client Version

Click ≡ and then select **About** to view the client version.

11 Log Out, Restart, Shut Down, Lock

Log out of, restart, shut down and lock out the Device.

Figure 11-1 User operation



Logging Out

Click admin, and then select **Logout**.

Restarting

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 user name and password, and then click **OK**. You can also click **Switch User** to switch to another user account.

12 FAQ

Table 12-1 FAQ

Problem	Possibilities and Solutions
After you enable face comparison (AI by Recorder), there is no human face comparison event.	• The AI module is offline. Click **Maintain** > **System Resources** > **AI Module Resource**. You can view status of the AI modules. • There are too many filter criteria on the AI display page. • The registered remote device does not support face detection function. In this case, you need to enable face detection (AI by Recorder). • It is not in the deployment period. • There is no linked face database or the face database has no data. • The human face similarity threshold is too high.
After you enable face comparison (AI by Camera), there is no human face comparison event.	• The face comparison function has not been enabled on the smart plan. • No human face database has been configured on the web interface of the remote device. • It is not in the deployment period.
Failed to search for face comparison results.	• The human face similarity threshold is too high. • The selected remote device has not triggered face comparison in the search period. • The specified face image is not in the face database.

Appendix 1 Glossary

Appendix Table 1-1Glossary

Name	Description
CGI	Common Gateway Interface (CGI) is an important Internet technology. With CGI, client can ask data from program running on network server. CGI describes data transmission standard between server and asking processing program.
DDNS	Dynamic Domain Name System (DDNS) is to map the user dynamic IP address to a specified domain analysis service. Each time, when the user connects to the network, the client can transmit the host dynamic address to the server application on the host of the service provider. The server applications are to provide the DNS service and realize dynamic domain analysis. That is to say, the user does not need to remember the changeable IP address, just uses the domain name to login the device or the address.
DHCP	Dynamic Host Configuration Protocol (DHCP) is a network protocol in the LAN. It is to automatically allocate IP address for the internal network or the ISP (Internet service provider).It is to manage the computer IP address by the unified means of management.
DNS	Domain Name System (DNS) is to save the all host domain name and corresponding IP address in the network. It has the ability to change the domain to the IP address.
DVR	Digital Video Recorder.
FTP	File Transfer Protocol (FTP) is used to control bilateral transmission of file on the Internet.
HDMI	High Definition Multimedia Interface (HDMI) is a special digital interface suitable for audio/video transmission. It can transmit audio signal and video signal at the same time.
HTTPS	Hyper Text Transfer Protocol over Secure Socket Layer (HTTPS) is a HTTP channel for security purpose. The HTTPS has defined the browser the world wide web service safety communication rule. It adopts encryption technology to guaranty safety access to the webpage.
IP	Internet Protocol.
IPC	IP Camera.
NTP	Network Time Protocol (NTP) is a protocol to synchronize computer time. It adopts wireless network protocol UDP, so that the computer time synchronizes with the server or the time source. It is to provide time correction of high accuracy.
NTSC	National Television Standards Committee, American national standard television and broadcast transmission and receiving protocol. This is a television standard that television scanning beam is 525 beams, 30 frames per second, interlaced scanning, odd field first and then it is followed by even field. NTSC is used in the United States of America, Japan, and so on.
NVR	Network Video Recorder
MTU	Maximum Transmission Unit (MTU) refers to the maximum data packet amount (byte) on one layer of the communication protocol.

Name	Description
ONVIF	Open Network Video Interface Forum (ONVIF) is the defined general protocol for information exchange among the network video devices. It includes search device, real-time audio/video, metadata, information control, and so on.
PAL	Phase Alteration Line, this is a television standard that television scanning beam is 625 beams, 25 frames per second, phase alteration, odd field first and then it is followed by even field. PAL color encoding is used. PAL is used in China, Europe, and so on.
PTZ	Pan Tilt Zoom (PTZ) refers to the PTZ all-direction movement, lens zoom, and focus control.
S.M.A.R.T	Self-Monitoring Analysis and Reporting Technology (S.M.A.R.T) is a technical standard to detect HDD drive status and report potential problems.
SSH	Secure Shell (SSH) is a security protocol formulated by IETF network group on the basis of application layer. SSH protocol can effectively prevent information leakage problem during remote management.
SVC	Scalable Video Coding (SVC) is a video encoding technology. It can split the video streams to one basic layer and several enhanced layers according to the requirements. The basic layer provides the general video quality, frame rate and resolution, and the enhanced layer is to perfect the video quality.
VGA	Video Graphics Array (VGA) is a video transmission standard. It has high resolution, high display speed and abundant colors.
WLAN	Wireless Local Area Networks (WLAN) adopts radio frequency to realize data transmission.

Appendix 2 Mouse and Keyboard Operations

This section introduces mouse and keyboard operations.

Appendix 2.1 Mouse Operations

Connect mouse (wireless mouse is supported) to the USB port, and then you can use the mouse to control the local menu.

Appendix Table 2-1Mouse operations

Operation	Description
Click (click the left mouse button)	Click to select a function menu, to enter the corresponding menu page. ● Implement the operation indicated on the control. ● Change checkbox and option button status. ● Click the checkbox to display drop-down list. ● On virtual keyboard, select letter, symbol, English upper letter and lower letter, and Chinese characters.
Double-click (click the left mouse button twice)	● On the **Live** page, double-click a view window to display it in one-split mode. Double-click the view window again to restore the original layout. ● On the **Live** page, double-click a remote device in the device tree to enable video edit mode, and then add remote devices to the view.
Right-click (click the right mouse button)	● On the **Live** or **Search** page, right-click one video window to display the shortcut menu. ● On the **Live** page, right-click the view in the list or the remote device in the device tree, to display the shortcut menu.
Wheel button	On the **Search** page, point to the time bar, and then scroll the mouse wheel to adjust the accurate time on the time bar.
Drag the mouse	● Drag the mouse pointer to select the motion detection zone. ● On the **Live** page, drag the remote device in the device tree to the play window to switch to the view status. You can add the remote device to the view.

Appendix 2.2 Virtual Keyboard

The local menu supports virtual keyboard.

Click the text box to display virtual keyboard. For details, see the following pictures and table.

If the device has connected to the peripheral keyboard, click the text column. Virtual keyboard will disappear.

Appendix Figure 2-1 Virtual keyboard (global keyboard)



Appendix Figure 2-2 Virtual keyboard (input letter)



Appendix 3 HDD Capacity Calculation

HDD capacity calculation formula:

Total capacity (M) = Channel number × Demand time length (hour) × HDD capacity occupied per hour (M/hour)

According to the above formula, get recording time calculation formula.

Recording time (hour) =

$$\frac{\text{Total capacity (M)}}{\text{HDD capacity occupied per hour (M/hour)} \times \text{Channel number}}$$

For example, for single-channel recording, HDD capacity occupied per hour is 200 M/hour. Use 4-channel device to make 24-hour continuous recording in every day of one month (30 days), the required HDD space is: 4 channels × 30 days × 24 hours × 200 M/hour = 576 G. Therefore, five 120 G HDD or four 160 G HDD must be installed.

According to the above formula, at different stream values, recording file size of 1 channel in 1 hour is shown as follows (for your reference):

Appendix Table 3-1HDD capacity calculation

Bit stream Size (max.)	File Size	Bit Stream Size (max.)	File Size
≤ 96 K	42 M	128 K	56 M
160 K	70 M	192 K	84 M
224 K	98 M	256 K	112 M
320 K	140 M	384 K	168 M
448 K	196 M	512 K	225 M
640 K	281 M	768 K	337 M
896 K	393 M	1024 K	450 M
1280 K	562 M	1536 K	675 M
1792 K	787 M	2048 K	900 M

Appendix 4 Particulate and Gaseous Contamination Specifications

Appendix 4.1 Particulate Contamination Specifications

The following table defines the limitations of the particulate contamination in the operating environment of the device. If the level of particulate contamination exceeds the specified limitations and result in device damage or failure, you need to rectify the environmental conditions.

Appendix Table 4-1Particulate contamination specifications

Particulate contamination	Specifications
Air filtration	Class 8 as defined by ISO 14644-1.
Conductive dust	Air must be free of conductive dust, zinc whiskers, or other conductive particles.
Corrosive dust	Air must be free of corrosive dust. Residual dust present in the air must have a deliquescent point less than 60% relative humidity.

Appendix Table 4-2ISO 14644-1 cleanroom classification

Class	Maximum particles/m^3					
—	≥ 0.1 μm	≥ 0.2 μm	≥ 0.3 μm	≥ 0.5 μm	≥ 1 μm	≥ 5 μm
Class 1	10	2	—	—	—	—
Class 2	100	24	10	4	—	—
Class 3	1000	237	102	35	8	–7
Class 4	10000	2370	1020	352	83	—
Class 5	100000	23700	10200	3520	832	29
Class 6	1000000	237000	102000	35200	8320	293
Class 7	—	—	—	352000	83200	2930
Class 8	—	—	—	3520000	832000	29300
Class 9	—	—	—	—	8320000	293000

Appendix 4.2 Gaseous Contamination Specifications

Usually indoor and outdoor atmospheric environments contain a small amount of common corrosive gas pollutants. When these mixed or single corrosive gas pollutants react with other environmental factors such as temperature or relative humidity in the long term, the device might suffer from a risk of corrosion and failure. The following table defines the limitations of the gaseous contamination in the operating environment of the device.

Appendix Table 4-3Gaseous contamination specifications

Gaseous contamination	Specifications
Copper coupon corrosion rate	< 300 Å/month per Class G1 as defined by ANSI/ISA71.04-2013
Silver coupon corrosion rate	< 200 Å/month per Class G1 as defined by ANSI/ISA71.04-2013

Appendix Table 4-4ANSI/ISA-71.04-2013 classification of reactive environments

Class	Copper Reactivity	Silver Reactivity	Description
G1 (mild)	< 300 Å/month	< 200 Å/month	Corrosion is not a factor in determining equipment reliability.
G2 (moderate)	< 1000 Å/month	< 1000 Å/month	Corrosion effects are measurable and corrosion might be a factor.
G3 (harsh)	< 2000 Å/month	< 2000 Å/month	High probability that corrosive attack will occur.
GX (severe)	≥ 2000 Å/month	≥ 2000 Å/month	Only specially designed and packaged devices are expected to survive.

Appendix 5 Security Commitment and Recommendation

Zhejiang 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;
   - Establish 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