

# Intelligent Video Surveillance Server

User's Manual

V2.1.0

# Foreword

## General






The user's manual (hereinafter referred to as "the Manual") describes the structure, function and operation of intelligent video surveillance server (hereinafter referred to as "IVSS").

## Model

8-HDD, 12-HDD, 16-HDD, and 24-HDD.

## Safety Instructions

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

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

## Revision History

Version	Revision Content	Release Time
V2.1.0	Add video structuring, vehicle recognition, and vehicle comparison functions.	April 2019
V2.0.1	Add attention in important safeguards and warnings.	January 2019
V2.0.0	Update figures of 16-HDD series IVSS.	December 2018
V1.0.0	First release.	November 2018

## Privacy Protection Notice

As the device user or data controller, you might collect personal data of other such as face, fingerprints, car plate number, Email address, phone number, GPS and so on. You need to be in compliance with the local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures include but not limited to: providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact.

## About the Manual

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

# Important Safeguards and Warnings

This section introduces the correct application method of IVSS. Read the Manual carefully before use to prevent danger and property loss. Strictly conform to the Manual during application and keep it properly after reading.

## Operating Requirement

- The IVSS needs to be installed in restricted access areas, and anyone who operates the device needs to be aware of the safety requirements of the device.
- Do not place and install the IVSS in an area exposed to direct sunlight or near heat generating devices.
- Do not install the IVSS in a humid, dusty or fuliginous area.
- Install the IVSS at stable places horizontally.
- Make the IVSS stay away from liquid.
- Install the IVSS at well-ventilated places; do not block its ventilation opening.
- Use the IVSS only within rated input and output range.
- Do not dismantle the IVSS arbitrarily.
- Transport, use and store the IVSS within allowed humidity and temperature range.













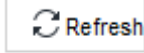
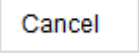





## Power Requirement







- Be sure to use the designated battery type. Otherwise there may be explosion risk.
- Be sure to use batteries according to requirements; otherwise, it may result in fire, explosion or burning risks of batteries!
- To replace batteries, only the same type of batteries can be used.
- Be sure to dispose the exhausted batteries according to the instructions.
- The product shall use electric wires (power wires) recommended by this area, which shall be used within its rated specification.
- Be sure to use standard power adapter matched with the device. Otherwise, the user shall undertake resulting personnel injuries or device damages.
- Use power supply that meets SELV (safety extra low voltage) requirements, and supply power with rated voltage that conforms to Limited Power Source in IEC60950-1. For specific power supply requirements, please refer to device labels.
- Products with category I structure shall be connected to grid power output socket, which is equipped with protective grounding.
- Appliance coupler is a disconnecting device. During normal use, please keep an angle that facilitates operation.

## Attention

AI module does not support hot plugging. If you need to replace the AI module, unplug the device power cable first. Otherwise, it will lead to file damage on the AI module.

## Signal Words

Icon/Button	Description
	After you have input password, press the icon with your pointer, you can see the password is displayed in letters and number; Release mouse or move pointer to other places, the password is displayed in the form of black dots.
	Add icon. Click the icon, system can display the hidden applications interface. You can view or open the applications.
	Help information. Move the cursor to the icon, device can display help information.
	Display or hide icon. Click the icon to display the hidden menu.  Now the icon is shown as  . Click  again to hide the menu items.
<input data-bbox="284 813 316 846" type="checkbox"/>	Check the box, you can select multiple menu items at the same time. <input checked="" data-bbox="756 835 788 869" type="checkbox"/> means selected.
<input data-bbox="284 920 316 954" type="radio"/>	Check box, select one menu item, <input checked="" data-bbox="1098 920 1129 954" type="radio"/> means selected.
	Dropdown box, click the box to view the dropdown menu.
	Enable icon. <ul style="list-style-type: none"> <li>• : Disabled function.</li> <li>• : Enabled function.</li> <li>• : The function cannot be enabled.</li> <li>• : The function cannot be disabled.</li> </ul>
	Refresh button, click it to view the latest configuration information.
	Cancel button, click it to cancel the configuration items and then return to the upper-level menu.
	Click Reset to clear all search criteria settings.
	Page switch. <ul style="list-style-type: none"> <li>• : Page up/page down.</li> <li>• , go to the first page or the last page.</li> </ul>
	Play window. Input page number in the box. Click <b>Jump</b> to go to the specified page.

Icon/Button	Description
	Filter icon. Click it to set filter criteria.
	Select icon. Click the icon, the system displays a check box, so you can select multiple objects.
	Search column. Input key words, click  to search the corresponding information.
	Text column. Input number, letter, symbol and so on.
	Close button. Click the icon to close the window.

# Table of Contents

<b>Foreword</b> .....	<b>I</b>
<b>Important Safeguards and Warnings</b> .....	<b>III</b>
<b>1 Overview</b> .....	<b>1</b>
1.1 Introduction .....	1
1.2 Main Functions .....	1
1.3 Login Mode .....	3
<b>2 The Grand Tour</b> .....	<b>1</b>
2.1 8-HDD Series .....	1
2.1.1 Front Panel .....	1
2.1.2 Rear Panel .....	2
2.1.3 Dimensions .....	3
2.2 12-HDD Series .....	4
2.2.1 Front Panel .....	4
2.2.2 Rear Panel .....	5
2.2.3 Dimensions .....	7
2.3 16-HDD Series .....	7
2.3.1 Front Panel .....	7
2.3.2 Rear Panel .....	9
2.3.3 Dimensions .....	11
2.4 24-HDD Series .....	12
2.4.1 Front Panel .....	12
2.4.2 Rear Panel .....	14
2.4.3 Dimensions .....	16
<b>3 Hardware Installation</b> .....	<b>18</b>
3.1 Installation Flow .....	18
3.2 Unpacking the Box .....	18
3.3 HDD Installation .....	18
3.3.1 12-HDD Series .....	19
3.3.2 16/24-HDD Series .....	19
3.4 Device Connection .....	20
3.4.1 Alarm Connection .....	22
3.4.2 PTZ Decoder Connection .....	24
3.4.3 Notes to Grounding .....	24
<b>4 Booting Up IVSS</b> .....	<b>25</b>
<b>5 Initial Settings</b> .....	<b>26</b>
5.1 Initializing Device .....	26
5.2 Quick Settings .....	28
5.2.1 System Time .....	28
5.2.2 IP Address .....	29
5.2.3 P2P Settings .....	31
5.3 Login .....	31

5.3.1 Logging in Client.....	32
5.3.2 Logging in Local Interface .....	35
5.3.3 Logging in Web.....	37
5.4 Configuring Remote Device.....	38
5.4.1 Initializing Remote Device .....	38
5.4.2 Adding Remote Device .....	43
<b>6 AI Operations .....</b>	<b>57</b>
6.1 Enabling AI Plan.....	57
6.2 Face Detection .....	58
6.2.1 Setting.....	58
6.2.2 Configuring Face Database.....	58
6.2.3 Configuring Face Detection .....	71
6.2.4 Configuring Face Recognition .....	73
6.2.5 Real-time View.....	76
6.2.6 Face Search .....	79
6.3 Video Structuring.....	87
6.3.1 Enabling AI Plan .....	88
6.3.2 Configuring Video Structuring.....	88
6.3.3 Live .....	89
6.3.4 AI Search .....	94
6.4 IVS.....	102
6.4.1 Setting.....	102
6.4.2 IVS .....	102
6.4.3 Real-time View.....	105
6.4.4 Search Interface .....	108
6.5 Vehicle Recognition .....	110
6.5.1 Enabling AI Plan .....	110
6.5.2 Setting Vehicle Recognition.....	110
6.5.3 Real-time View.....	111
6.5.4 Searching Detection Information .....	114
6.6 Vehicle Comparison .....	114
6.6.1 Procedure .....	114
6.6.2 Enabling AI Plan .....	115
6.6.3 Setting Vehicle Database .....	115
6.6.4 Setting Plate Comparison.....	127
6.6.5 Real-time View.....	129
6.6.6 AI Search .....	132
<b>7 General Operations .....</b>	<b>136</b>
7.1 Live and Monitor.....	136
7.1.1 View Management.....	137
7.1.2 Resources Pool .....	148
7.1.3 PTZ .....	149
7.2 Search.....	153
7.2.1 Playing Back Recorded Video.....	153
7.2.2 Clipping Recorded Video.....	158
7.2.3 Playing Back Snapshots.....	160
7.2.4 Exporting File.....	162



7.3 File Management .....	165
7.3.2 Editing Face Image.....	165
7.3.3 Copying Face Image .....	166
7.3.4 Deleting Face Image .....	167
7.4 Alarm List .....	167
7.5 Display Management .....	168
7.5.1 Multiple-screen Control.....	168
7.5.2 Locking Screen .....	169
7.6 System Info .....	170
7.7 Background Task.....	170
<b>8 System Configuration .....</b>	<b>171</b>
8.1 Configuring Interface.....	171
8.2 Device Management .....	171
8.2.1 Local Device .....	172
8.2.2 Remote Device .....	174
8.3 Network Management.....	187
8.3.1 Basic Network.....	187
8.3.2 Network Apps.....	195
8.4 Event Management.....	200
8.4.1 Alarm Actions .....	201
8.4.2 Local Device .....	207
8.4.3 Remote Device .....	213
8.5 Storage Management .....	217
8.5.1 HDD .....	218
8.5.2 RAID .....	222
8.5.3 Storage Strategy.....	230
8.6 Security Strategy.....	233
8.6.1 HTTPS .....	234
8.6.2 Configuring Access Right .....	240
8.6.3 Safety Protection .....	242
8.6.4 Enabling System Service Manually .....	243
8.7 Account Management .....	244
8.7.1 User Group .....	245
8.7.2 Device User .....	247
8.7.3 Password Maintenance .....	249
8.7.4 ONVIF .....	258
8.8 System Management .....	261
8.8.1 Setting System Parameter.....	261
8.8.2 System Time .....	262
8.8.3 Display .....	264
8.8.4 Schedule.....	265
8.8.5 Enabling Voice Manage Function.....	266
<b>9 System Maintenance.....</b>	<b>269</b>
9.1 Searching Log.....	269
9.2 Online User .....	271
9.3 Device Maintenance .....	272
9.3.1 Upgrading Device .....	272

9.3.2 Default.....	274
9.3.3 Auto Maintain .....	275
9.3.4 IMP/EXP .....	275
<b>10 IVSS Client Introduction .....</b>	<b>277</b>
10.1 Interface Description .....	277
10.2 History Record .....	277
10.3 View Downloads.....	278
10.4 Configuring IVSS Client .....	278
10.5 Viewing Version Details .....	279
<b>11 Log Out/Reboot/Shut Down .....</b>	<b>281</b>
<b>12 FAQ .....</b>	<b>282</b>
<b>Appendix 1 Operation Description.....</b>	<b>283</b>
Appendix 1.1 Mouse Operations .....	283
Appendix 1.2 Virtual Keyboard .....	283
<b>Appendix 2 RAID .....</b>	<b>286</b>
<b>Appendix 3 HDD Capacity Calculation .....</b>	<b>288</b>
<b>Appendix 4 Glossary.....</b>	<b>289</b>
<b>Appendix 5 Cybersecurity Recommendations .....</b>	<b>291</b>

# 1 Overview

## 1.1 Introduction

Intelligent video surveillance server (IVSS) is compatible with most video surveillance products. Based on deep learning technology, IVSS has AI functions including human face recognition, and features extraction.

- General system settings, video surveillance, video storage, alarm settings, log management, record search and playback, intelligent analysis (such as human face real-time recognition, search human face by specified image and then play back video).
- User-friendly interface, suitable for user to operate.
- Supports 4K and H.265 decode.
- Widely used in intelligent building, large parking lot, safe city project, financial planning area, and so on.

## 1.2 Main Functions

Table 1-1 Main functions introduction

Name	Description
Intelligent analytics	<p>Configuring smart detection alarm.</p> <ul style="list-style-type: none"><li>• Human face detection and human face comparison alarm (available with AI by camera or AI by device).</li><li>• Upload human face image to search images, and supports searching and comparing 10 face images simultaneously.</li><li>• Quickly search smart detection record of face property.</li><li>• Set properties parameters to filter the comparison results twice and quickly filter the information needed.</li><li>• Double-click the search results to play the associated record files.</li></ul>
Live view and monitor	<p>View live pictures, smart detection pictures and record of remote device.</p> <ul style="list-style-type: none"><li>• Supports creating maximum 100 views. Each view supports maximum 36-channel remote devices.</li><li>• Supports creating view group, and view management.</li><li>• Local zoom-in of view window, and control zoom-in magnification with mouse wheel; display real-time bit stream, enable original scale, switch main stream/sub stream on the view window.</li><li>• Display smart feature property panel, view the real-time snapshots of smart detection, play the record taken during snapshots, and export pictures.</li><li>• View statistics of smart detection pictures, and set smart detection prompt quickly.</li></ul>

Name	Description
Search	<p>View and play back records/snapshots.</p> <ul style="list-style-type: none"> <li>● Through smart detection type, search smart detection record/pictures quickly.</li> <li>● Search and play back record/pictures according to type, remote device and time.</li> <li>● Adopt image to display search results. At the same time, it can export recorded video file/image to peripheral device or the PC.</li> <li>● Playback dual-bar control. Display selected channel and the record process of all searched channels.</li> <li>● Use cursor, time bar, mouse click to fast positioning recorded video playback time.</li> <li>● Use mouse wheel to zoom in the time bar, max unit is 24 hours, min unit is 1 second. It can quickly view channel record status.</li> <li>● Multiple-record playback mode. It includes slow play, fast play, backward play, and frame by frame playback.</li> <li>● When playback record, it can display event occurred time and select any video panel to zoom in/zoom out.</li> </ul>
Device management	<p>Manage devices information, add and configure remote devices.</p> <ul style="list-style-type: none"> <li>● Modify device name and set device storage plan.</li> <li>● Add remote devices through ONVIF, AXIS, SONY protocol and so on.</li> <li>● Search remote device with broadcast. Use manufacturer, IP filter to narrow search range.</li> <li>● Initialize remote device, modify remote device name, IP address, and so on.</li> <li>● Set remote device encode parameters, connection information, OSD, and storage plan, and so on.</li> </ul>
File management	<p>Manage face database and face image information.</p> <ul style="list-style-type: none"> <li>● Human face database creation.</li> <li>● Manual upload, batch import human face images. Maximum support 300,000 images.</li> </ul>
Network management	<p>Configure basic network and network applications.</p> <ul style="list-style-type: none"> <li>● With 4 self-adaptive Ethernet ports, set device IP address, visit and manage the device through web and client.</li> <li>● Set port number. Bind the port with load balance, fault-tolerance, link aggregation working mode.</li> <li>● Support P2P, DDNS, Email, and auto register.</li> </ul>
Event management	<p>It is to set alarm event. When there is an alarm, system can trigger the corresponding device to generate alarm operation.</p> <ul style="list-style-type: none"> <li>● Set device error alarm, including no HDD, storage error, full storage space, IP conflict, MAC conflict, login lock, AI module temperature, AI module offline, fan speed, power error, device offline, AI plan, and local alarm.</li> <li>● Set video detection alarm, offline alarm and AI plan of remote device.</li> <li>● Set alarm linkage, including alarm linkage record, snapshot, buzzer, log, Email, preset point, local alarm output, IPC alarm output, access control, and audio prompt.</li> <li>● Customize alarm arm time.</li> </ul>

Name	Description
User management	<p>Manage local user and ONVIF user.</p> <ul style="list-style-type: none"> <li>Local user adopts two levels of management, including user and user group. Each user group is a set of the authorities, which is a sub-set of total authority set and can be edited.</li> <li>Reset system default user (admin) password.</li> <li>Support to add, modify and delete ONVIF user.</li> </ul>
Storage management	<p>Manage physical HDD and network mapping HDD.</p> <ul style="list-style-type: none"> <li>Get HDD slot status, HDD model, and space of physical HDD.</li> <li>Support RAID 0, RAID 1, RAID 5, RAID 6 and RAID 10. Support one-click creation of RAID, global hot spare and local hot spare.</li> <li>Support FTP storage configuration and iSCSI network mapping.</li> </ul>
Security center	<p>It is to set security access strategy of the device.</p> <ul style="list-style-type: none"> <li>Set HTTPS login; remotely access the device through HTTPS protocol.</li> <li>Set IP authority. Forbid other devices logging in with IP address, MAC address.</li> <li>Set account locking strategy. Lock the specified IP address for a period of time, once the login attempts has reached the threshold.</li> <li>Enable system service manually.</li> </ul>
System config	<p>Set basic configuration items of the system.</p> <ul style="list-style-type: none"> <li>System language settings, user logout period settings.</li> <li>Manually set device time, or sync time with the NTP.</li> <li>Set displayer resolution and refresh frequency.</li> <li>Create weekly schedule, to be used as alarm arm time.</li> <li>Audio management manages audio files.</li> </ul>
System Notice	<ul style="list-style-type: none"> <li>View system information, background running tasks.</li> <li>View and deal with alarm information.</li> </ul>
Operation and maintenance management	<p>It is to operate and maintain the device working environment to guarantee proper operation.</p> <ul style="list-style-type: none"> <li>Search system log, user operation log, event log, and linkage log.</li> <li>Display online user, and block online user.</li> <li>Device maintenance function such as device upgrade, restore factory default settings, auto maintain, and configuration backup.</li> </ul>

## 1.3 Login Mode

The device supports local, web and IVSS client operation. For details, see Table 1-2.



Operation and system configuration in this manual is mainly based on IVSS client. There might be differences from local or web operation. The actual interface shall prevail.

Table 1-2 Login mode

Login Mode	Operation	Description
Local login	Connect the display, mouse and keyboard to the device. View and operate the local menu on the display.	Support all functions of the device.

Login Mode	Operation	Description
Web login interface	Connect the device and PC into the same network, and remotely access the device through browser (Google Chrome and Firefox) on PC.	Support majority functions of the device, except live, record playback and video-related function.
Log in IVSS client	Connect the device and PC into the same network, download and install IVSS Client on PC, and then remotely access the device with IVSS Client.	Support all functions of the device.

# 2 The Grand Tour

This section introduces front panel, rear panel, port function and button function, indicator light status, and so on.

## 2.1 8-HDD Series

### 2.1.1 Front Panel

Figure 2-1 Front panel

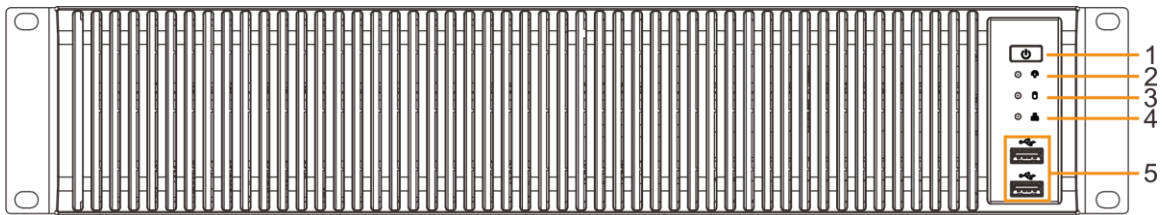


Table 2-1 Front panel description

No.	Button/Port	Description
1	Power	Boot up or shut down device. Power indicator light status is as follows: <ul style="list-style-type: none"><li>• When device is off (indicator light is off), press the button for a short period to boot up device.</li><li>• When device is running, (blue indicator light is on), press the button for at least 4 seconds to shut down the device.</li></ul>
2	Alarm indicator light	Displays local input alarm status. <ul style="list-style-type: none"><li>• The indicator light is off: There is no local alarm input event.</li><li>• Red indicator light is on: There is local alarm input event.</li></ul>
3	System status indicator light	Displays the system running status. <ul style="list-style-type: none"><li>• The blue light is on: Device is running properly.</li><li>• The indicator light is off: The device is not running.</li></ul>
4	Network indicator light	Displays current network status. <ul style="list-style-type: none"><li>• The indicator light is blue: It means at least one Ethernet port has connected to the network.</li><li>• The indicator light is off: No Ethernet ports are connected to the network.</li></ul>
5	USB	Connects to external devices such as USB storage device, keyboard and mouse.

## 2.1.2 Rear Panel

Figure 2-2 Rear panel

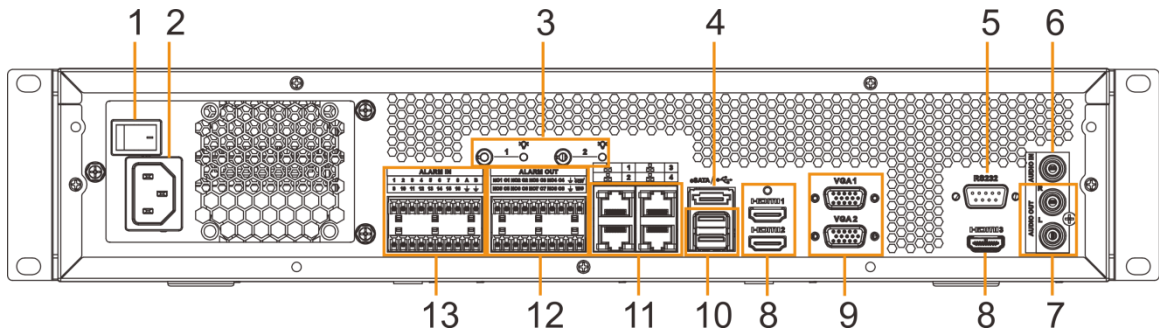





Table 2-2 Rear panel description

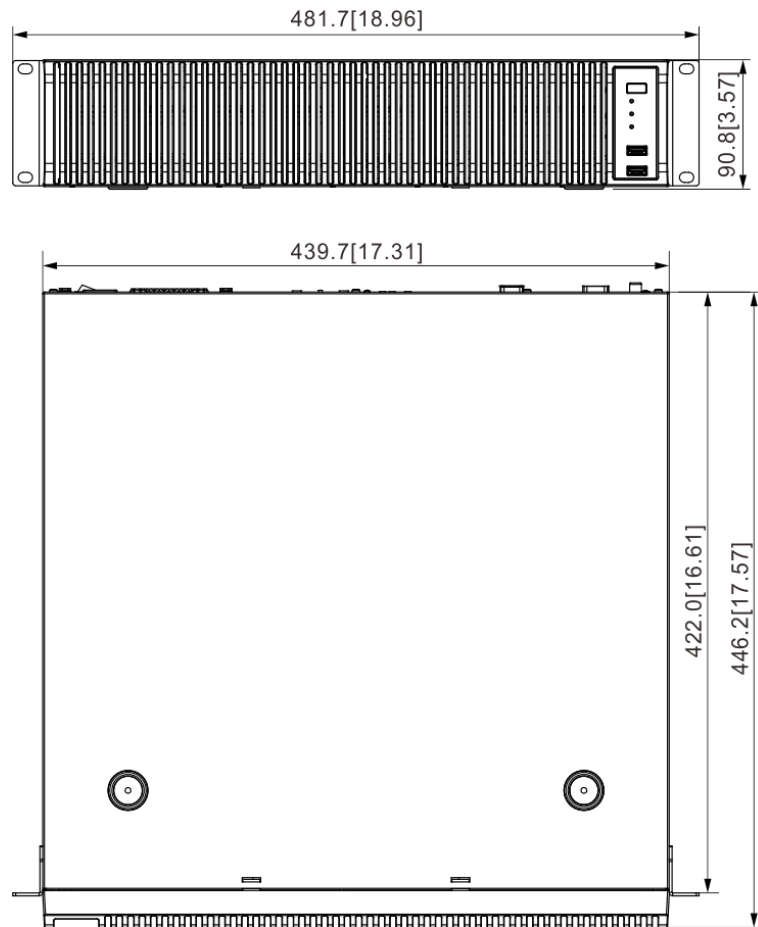
No.	Button/Port	Description
1	Power	Power on/off button.
2	Power input	Inputs AC 100V-240V power.
3	AI module indicator light	Displays AI module status. <ul style="list-style-type: none"> <li>Yellow light flashes: AI module is running properly.</li> <li>Yellow light is on: AI module is malfunctioning.</li> </ul>  <p>This function is not available without AI module.</p>
4	eSATA	SATA peripheral port. Connect to SATA port or eSATA device.
5	RS-232	RS-232 COM debug. It is for general COM debug, set IP address, transmit transparent COM data.
6	AUDIO IN	Audio input port.
7	AUDIO OUT	Audio output port.
8	HDMI	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. The three HDMI ports are different source output.
9	VGA	VGA video output port. Output analog video signal. It can connect to the monitor to view analog video. The two VGA ports are different source output. <ul style="list-style-type: none"> <li>VGA1 and HDMI 1 are same source output.</li> <li>VGA2 and HDMI 2 are same source output.</li> </ul>
10	USB	Connects to external devices such as USB storage device, keyboard and mouse.
11	Network	10M/100/1000Mbps self-adaptive Ethernet port. Connect to the network cable.
12	Alarm output	8 groups of alarm output ports (NO1 C1–NO8 C8). Output alarm signal to the alarm device. Please make sure there is power to the external alarm device. <ul style="list-style-type: none"> <li>NO: Alarm output port of Normally Open type.</li> <li>C: Common alarm output port.</li> <li>: GND end.</li> </ul>



No.	Button/Port	Description
13	Alarm input	<p>16 groups (1–16) alarm input ports, they are corresponding to ALARM 1–ALARM 16. The alarm becomes valid in low level.</p> <ul style="list-style-type: none"> <li>A and B: Control the A/B cable of the RS-485 device. It is to connect to the PTZ camera. Please parallel connect 120Ω between A/B cables if there are too many PTZ decoders.</li> <li>: GND end.</li> </ul>

### 2.1.3 Dimensions

Figure 2-3 Dimension (mm [inch])



## 2.2 12-HDD Series

### 2.2.1 Front Panel

Figure 2-4 Front panel

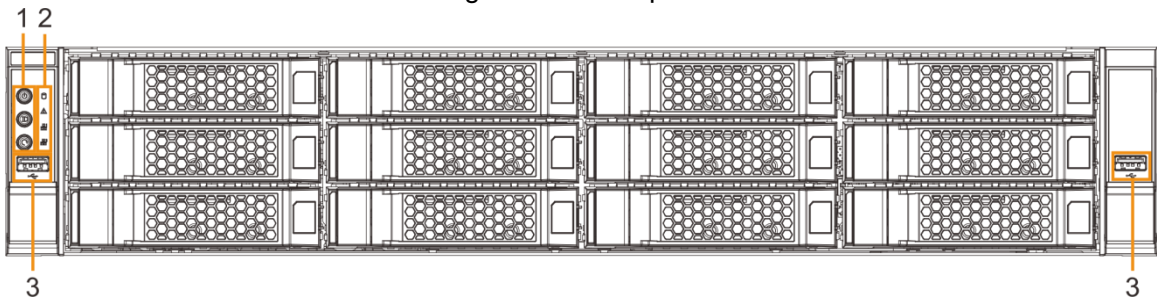



Table 2-3 Front panel description

No.	Button/Port	Description
1	Power	<p>Boot up or shut down device. Power indicator light status is as follows:</p> <ul style="list-style-type: none"> <li>When device is off (indicator light is off), press the button for a short period to boot up device.</li> <li>When device is running, (blue indicator light is on), press the button for at least 4 seconds to shut down the device.</li> </ul>
	ID button	<p>Position button. It is to control the ID indicator light on the rear panel. It is to positioning the device.</p>  <p>ID button has the indicator light function. Its display status is the same with the ID indicator light on the rear panel.</p>
	RESET button	Click to reboot the device.
2	Power indicator light	<p>Displays power status.</p> <ul style="list-style-type: none"> <li>Blue light is on: The device has properly connected to the power source.</li> <li>The indicator light is off: The device has not connected to the power source.</li> </ul>
	Alarm indicator light	<p>Displays local input alarm status.</p> <ul style="list-style-type: none"> <li>Green light on: There is no local alarm input alarm.</li> <li>Red indicator light is on: There is local alarm input event.</li> </ul>
	Network indicator light 1	<p>Displays network statuses of Ethernet port 1 and Ethernet port 2.</p> <ul style="list-style-type: none"> <li>The indicator light flashes green: At least one Ethernet port has connected to the network.</li> <li>The indicator light is off: All Ethernet ports are not connected to the network.</li> </ul>
	Network indicator light 2	<p>Displays network statuses of Ethernet port 3 and Ethernet port 4.</p> <ul style="list-style-type: none"> <li>The indicator light flashes green: At least one Ethernet port has connected to the network.</li> <li>The indicator light is off: All Ethernet ports are not connected to the network.</li> </ul>
3	USB 3.0 port	Connects to external devices such as USB storage device, keyboard and mouse.

## 2.2.2 Rear Panel

Figure 2-5 Rear panel (the single-power series)

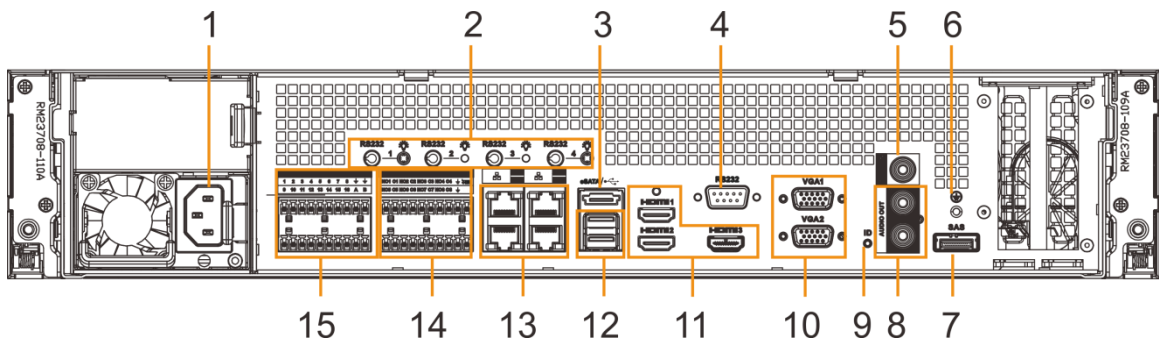


Figure 2-6 Rear panel (the redundant series)

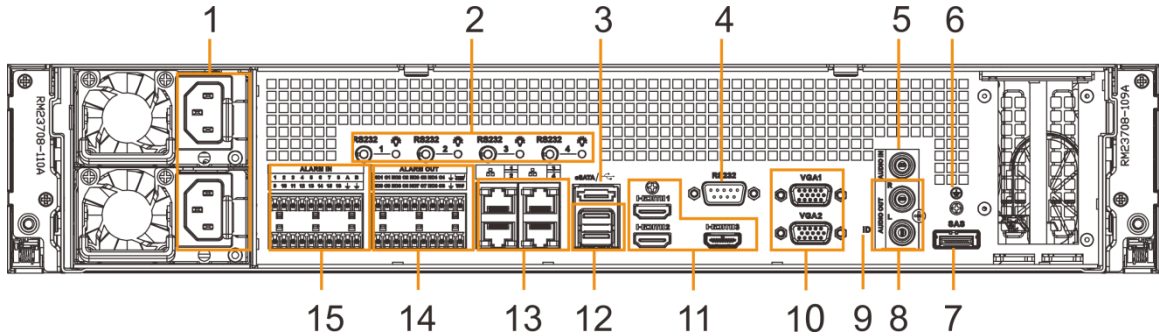





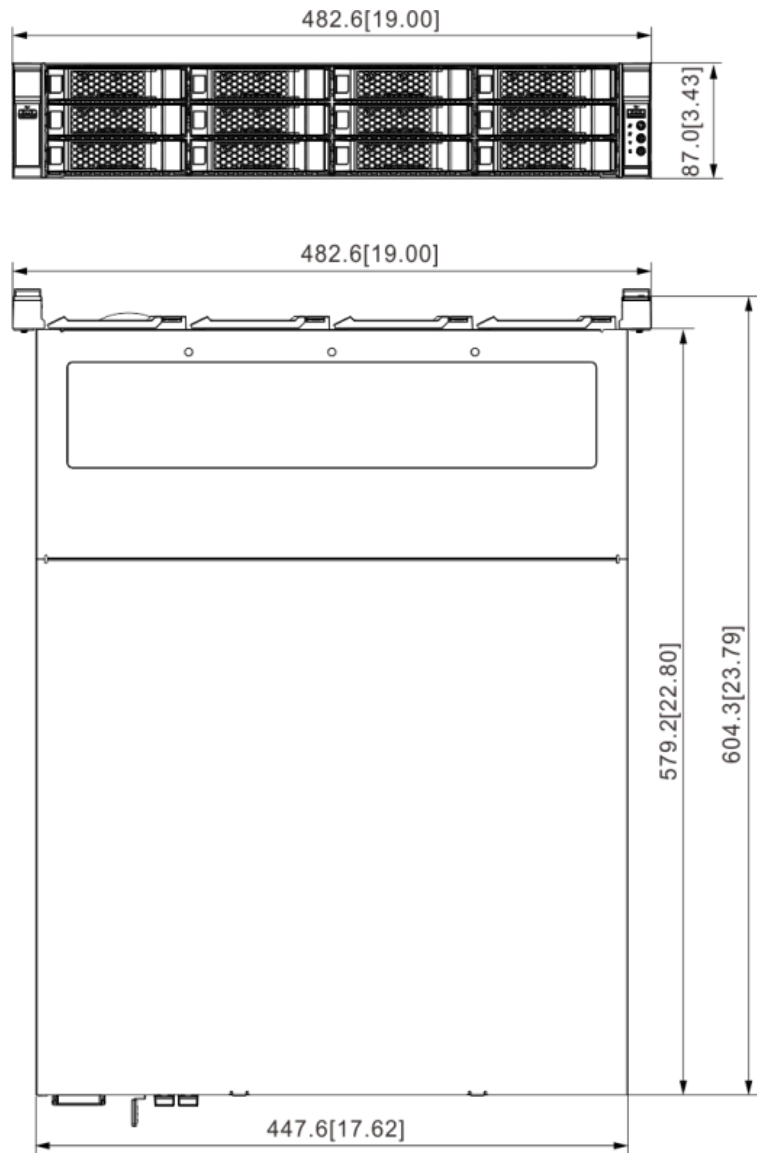
Table 2-4 Rear panel description

No.	Name	Description
1	Power input port	Inputs AC 100V-240V power.
2	AI module indicator light	Displays AI module status. <ul style="list-style-type: none"> <li>The yellow light flashes: AI module is running properly.</li> <li>The yellow light is on: AI module is malfunctioning.</li> </ul>  This function is not available without AI module.
3	eSATA port	SATA peripheral port. Connect to SATA port or eSATA device.
4	RS-232 port	RS-232 COM debug. It is for general COM debug, set IP address, transmit transparent COM data.
5	AUDIO IN	Audio input port
6	Ground port.	Ground port.
7	SAS port	SAS extension port. It can connect to the SAS extension controller.
8	AUDIO OUT	Audio output port
9	ID indicator light	Positioning indicator light. It is controlled by the ID button on the front panel. <ul style="list-style-type: none"> <li>The blue light is on, device is positioning now.</li> <li>The indicator light is off: The device is not positioning.</li> </ul>
10	VGA port	VGA video output port. Output analog video signal. It can connect to the monitor to view analog video. The two VGA ports are different source output. <ul style="list-style-type: none"> <li>VGA1 and HDMI 1 are same source output.</li> <li>VGA2 and HDMI 2 are same source output.</li> </ul>

No.	Name	Description
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. The three HDMI ports are different source output.
12	USB port	Connects to external devices such as USB storage device, keyboard and mouse.
13	Network port	10M/100/1000Mbps self-adaptive Ethernet port. Connect to the network cable.
14	Alarm output	8 groups of alarm output ports (NO1 C1–NO8 C8). Output alarm signal to the alarm device. Please make sure there is power to the external alarm device. <ul style="list-style-type: none"> <li>• NO: Alarm output port of Normally Open type.</li> <li>• C: Common alarm output port.</li> <li>• : GND end.</li> </ul>
15	Alarm input	16 groups (1–16) alarm input ports, they are corresponding to ALARM 1–ALARM 16. The alarm becomes valid in low level. <ul style="list-style-type: none"> <li>• A and B: Control the A/B cable of the RS–485 device. It is to connect to the PTZ camera. Please parallel connect 120Ω between A/B cables if there are too many PTZ decoders.</li> <li>• : GND end.</li> </ul>

## 2.2.3 Dimensions

Figure 2-7 Dimensions (mm [inch])



## 2.3 16-HDD Series

### 2.3.1 Front Panel

Figure 2-8 Front panel with LCD

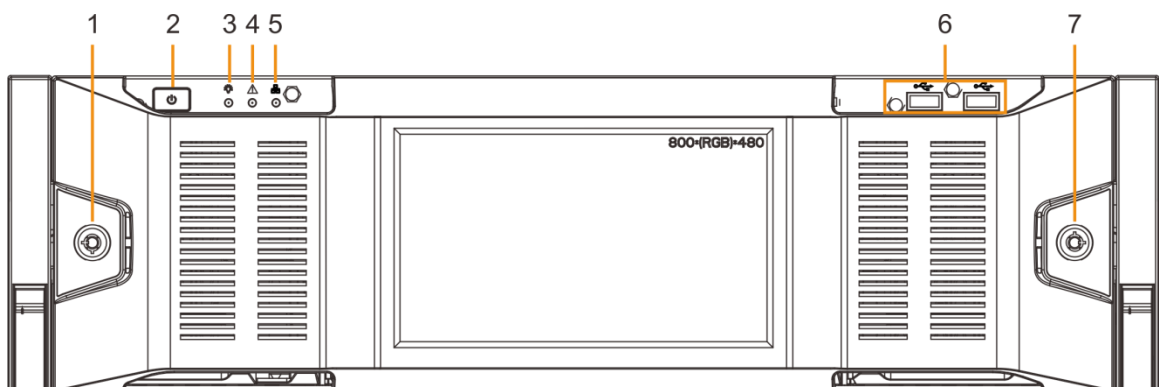


Figure 2-9 Front panel without LCD

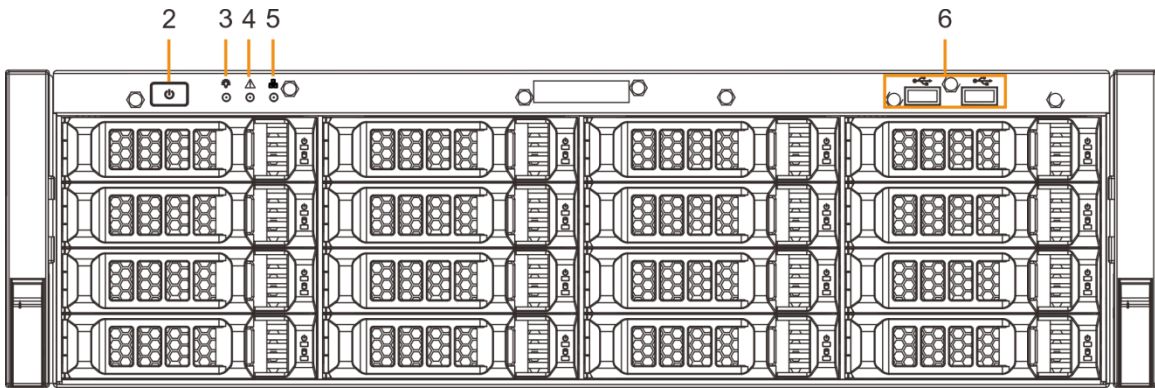




Table 2-5 Front panel description

No.	Button/Port	Description
1	Front panel lock	Once the front panel lock is secure, it can prevent HDD from being stolen or removed by mistake. Unlock the front panel lock and remove the front panel, you can view 16 HDD slots. See Figure 2-9.
2	Power	<p>Boot up or shut down device. The power on/off button has the indicator light. It can display device-running status.</p> <ul style="list-style-type: none"> <li>When device is off (indicator light is off), press the button for a short period to boot up device.</li> <li>When device is running, (blue indicator light is on), press the button for at least 4 seconds to shut down the device.</li> </ul>
3	System status indicator light	<p>Displays the system running status.</p> <ul style="list-style-type: none"> <li>The blue light is on: Device is running properly.</li> <li>The indicator light is off: The device is not running.</li> </ul>
4	Alarm indicator light	<p>Displays local input alarm status.</p> <ul style="list-style-type: none"> <li>Red indicator light is on: There is local alarm input event.</li> <li>The indicator light is off: There is no local alarm input event.</li> </ul>
5	Network indicator light	<p>Displays current network status.</p> <ul style="list-style-type: none"> <li>The indicator light is blue: It means at least one Ethernet port has connected to the network.</li> <li>The indicator light is off: No Ethernet ports are connected to the network.</li> </ul>
6	USB port	Connects to external devices such as USB storage device, keyboard and mouse.
7	16-HDD slot	<p>After you remove the front panel, you can see there are 16 HDDs. From the left to the right and from the top to the bottom, it ranges from 1–4, 5–8, 9–12, and 13–16.</p> <p>There are two indicator lights on the HDD slot: HDD indicator light and HDD read/write indicator light.</p> <ul style="list-style-type: none"> <li>: HDD indicator light. The light is yellow after you install the HDD.</li> <li>: Read/write indicator light. The blue light flashes when it is reading and writing data.</li> </ul>

## 2.3.2 Rear Panel

Figure 2-10 Rear panel (the single-power series)

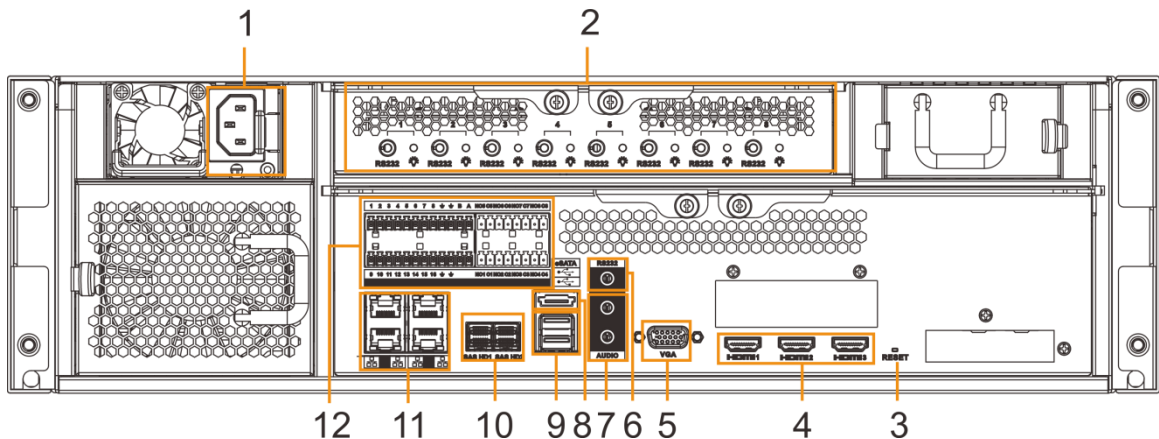


Figure 2-11 Rear panel (the redundant series)

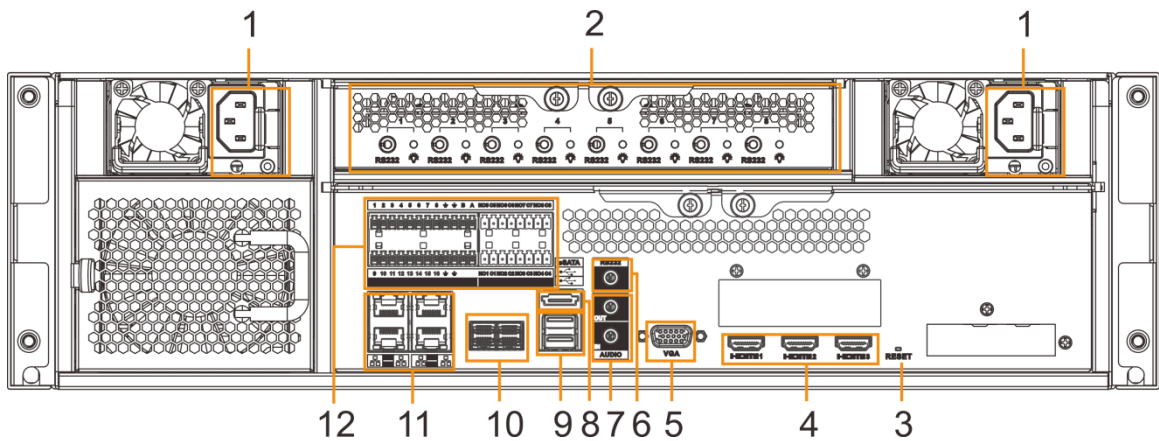





Table 2-6 Rear panel description

No.	Name	Description
1	Power input port	Inputs AC 100V-240V power.
2	AI module indicator light	Displays AI module status. <ul style="list-style-type: none"> <li>The yellow light flashes: AI module is running properly.</li> <li>The yellow light is on: AI module is malfunctioning.</li> </ul>  <p>This function is valid if there is AI module.</p>
3	RESET button	Reserved.
4	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. The three HDMI ports are different source output.
5	VGA port	VGA video output port. Output analog video signal. It can connect to the monitor to view analog video. The VGA port and HDMI 1 port are same source output.
6	RS-232 port	RS-232 COM debug. It is for general COM debug, set IP address, transmit transparent COM data.
7	AUDIO IN	Audio input port

No.	Name	Description
	AUDIO OUT	Audio output port
8	eSATA port	SATA peripheral port. Connect to SATA port or eSATA device.
9	USB port	Connects to external devices such as USB storage device, keyboard and mouse.
10	SAS port	SAS extension port. It can connect to the SAS extension controller.
11	Network port	10M/100/1000Mbps self-adaptive Ethernet port. Connect to the network cable.
12	Alarm Input	<p>16 groups (1–16) alarm input ports, they are corresponding to ALARM 1–ALARM 16. The alarm becomes valid in low level.</p> <ul style="list-style-type: none"> <li>• A and B: Control the A/B cable of the RS–485 device. It is to connect to the PTZ camera. Please parallel connect 120Ω between A/B cables if there are too many PTZ decoders.</li> <li>• : GND end.</li> </ul>
	Alarm Output	<p>8 groups of alarm output ports (NO1 C1–NO8 C8). Output alarm signal to the alarm device. Please make sure there is power to the external alarm device.</p> <ul style="list-style-type: none"> <li>• NO: Alarm output port of Normally Open type.</li> <li>• C: Common alarm output port.</li> <li>• : GND end.</li> </ul>



### 2.3.3 Dimensions

Figure 2-12 Dimensions with LCD (mm [inch])

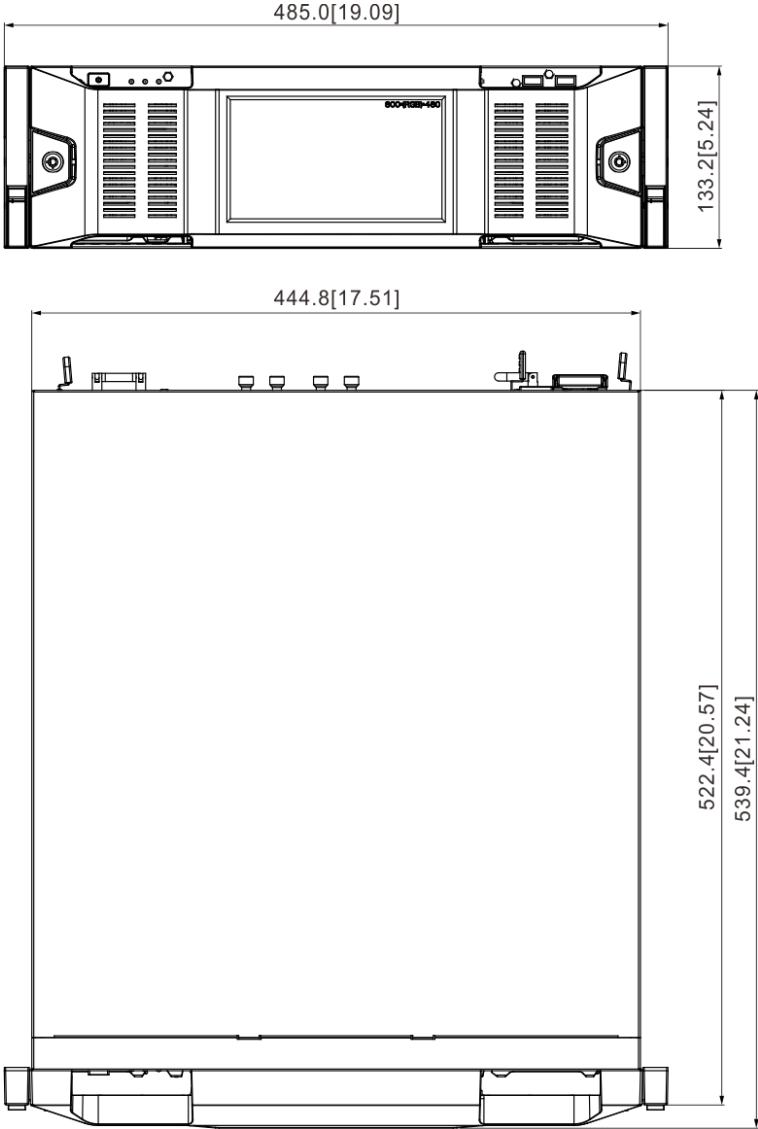
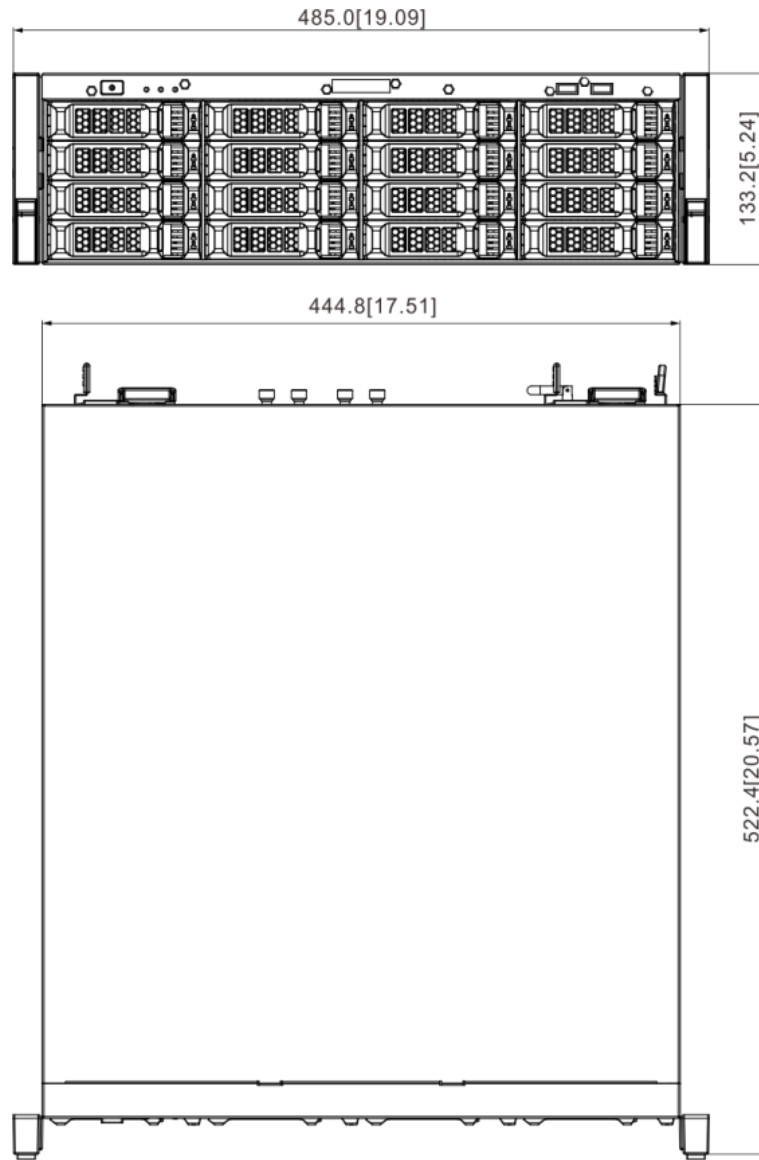


Figure 2-13 Dimensions without LCD (mm [inch])



## 2.4 24-HDD Series

### 2.4.1 Front Panel

Figure 2-14 Front panel with LCD

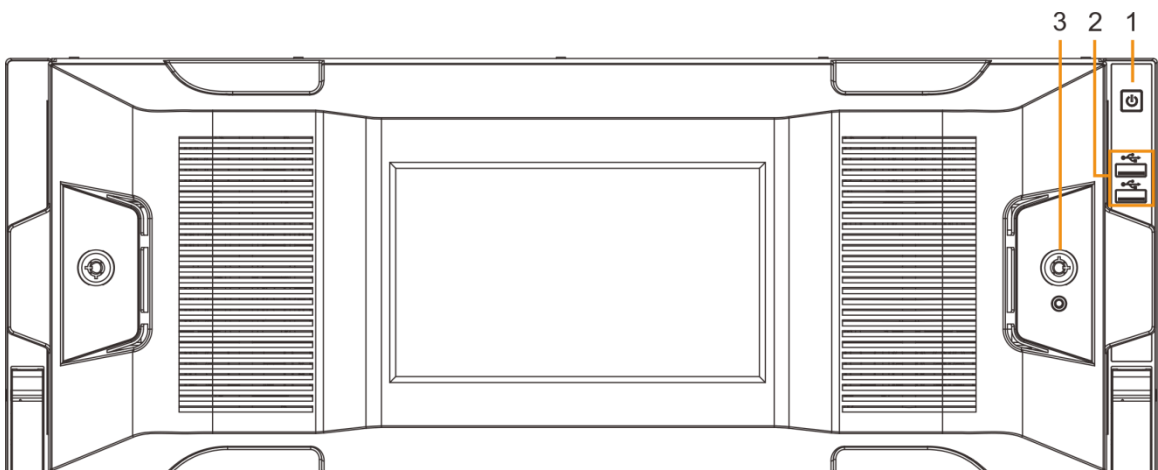


Figure 2-15 Front panel without LCD

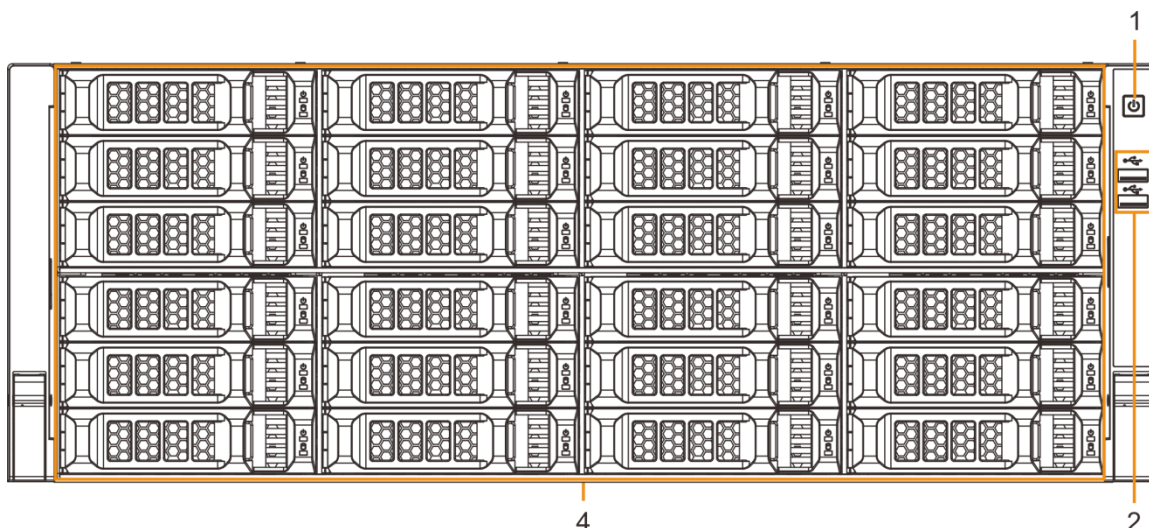




Table 2-7 Front panel description

No.	Button/Port	Description
1	Power on/off button	<p>Boot up or shut down device. The power on/off button has the indicator light. It can display device-running status.</p> <ul style="list-style-type: none"> <li>When device is off (indicator light is off), press the button for a short period to boot up device.</li> <li>When device is running, (blue indicator light is on), press the button for at least 4 seconds to shut down the device.</li> </ul>
2	USB port	Connects to external devices such as USB storage device, keyboard and mouse.
3	Front panel lock	Once the front panel lock is secure, it can prevent HDD from being stolen or removed by mistake. Unlock the front panel lock and remove the front panel, you can view 16 HDD slots. See Figure 2-15.
4	24-HDD slot	<p>After you remove the front panel, you can see there are 24 HDDs. From the left to the right and from the top to the bottom, it ranges from 1–4, 5–8, 9–12, 13–16, 17–20, and 21–24.</p> <p>There are two indicator lights on the HDD slot: HDD indicator light and HDD read/write indicator light.</p> <ul style="list-style-type: none"> <li>: HDD indicator light. The light is yellow after you install the HDD.</li> <li>: Read/write indicator light. The blue light flashes when it is reading and writing data.</li> </ul>

## 2.4.2 Rear Panel

Figure 2-16 Rear panel (the single-power series)

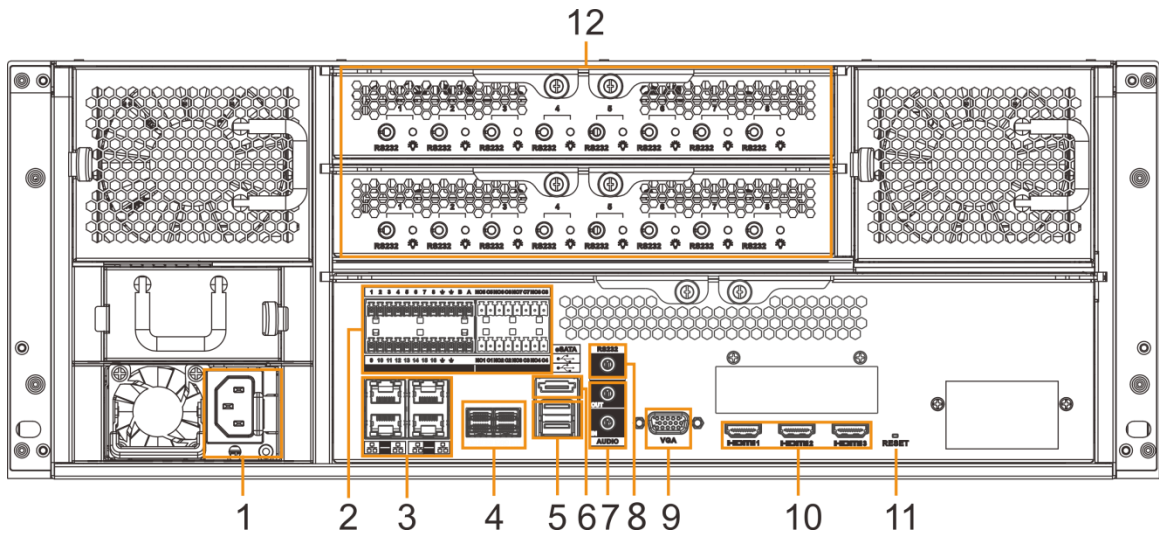


Figure 2-17 Rear panel (the redundant series)

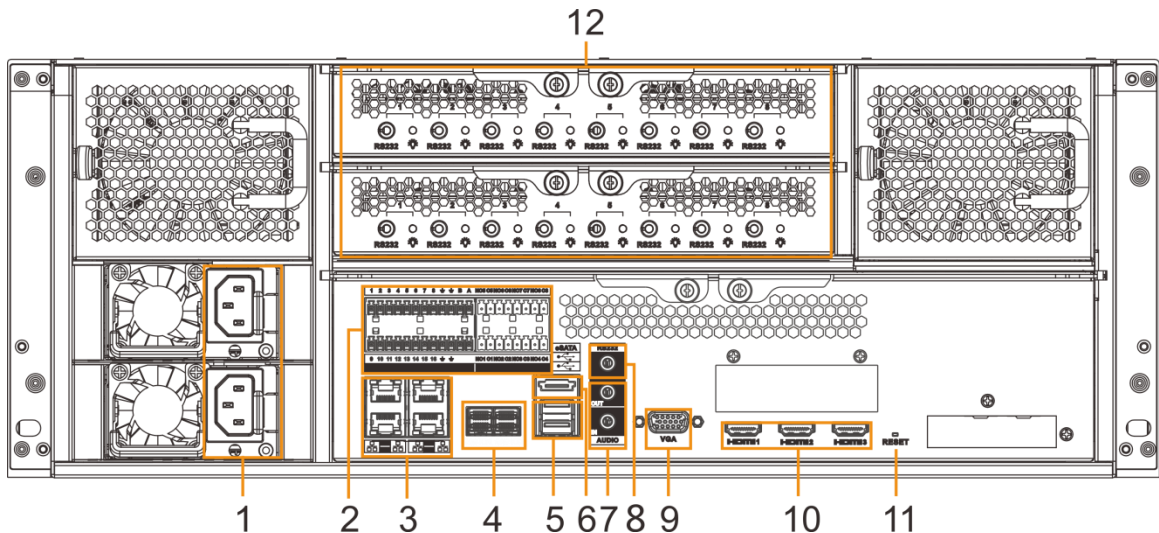




Table 2-8 Rear panel description

No.	Button/Port	Description
1	Power input port	Inputs AC 100V-240V power.
2	Alarm Input	<p>16 groups (1–16) alarm input ports, they are corresponding to ALARM 1–ALARM 16. The alarm becomes valid in low level.</p> <ul style="list-style-type: none"> <li>• A and B: Control the A/B cable of the RS–485 device. It is to connect to the PTZ camera. Please parallel connect 120Ω between A/B cables if there are too many PTZ decoders.</li> <li>• <math>\perp</math>: GND end.</li> </ul>

No.	Button/Port	Description
	Alarm Output	<p>8 groups of alarm output ports (NO1 C1–NO8 C8). Output alarm signal to the alarm device. Please make sure there is power to the external alarm device.</p> <ul style="list-style-type: none"> <li>• NO: Alarm output port of Normally Open type.</li> <li>• C: Common alarm output port.</li> <li>• : GND end.</li> </ul>
3	Network port	10M/100/1000Mbps self-adaptive Ethernet port. Connect to the network cable.
4	SAS port	SAS extension port. It can connect to the SAS extension controller.
5	USB port	Connects to external devices such as USB storage device, keyboard and mouse.
6	eSATA port	SATA peripheral port. Connect to SATA port or eSATA device.
7	AUDIO IN	Audio input port
	AUDIO OUT	Audio output port
8	RS-232 port	RS-232 COM debug. It is for general COM debug, set IP address, transmit transparent COM data.
9	VGA port	VGA video output port. Output analog video signal. It can connect to the monitor to view analog video. The VGA port and HDMI 1 port are same source output.
10	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. The three HDMI ports are different source output.
11	RESET button	Reserved.
12	AI module indicator light	<p>Displays AI module status.</p> <ul style="list-style-type: none"> <li>• The yellow light flashes: AI module is running properly.</li> <li>• The yellow light is on: AI module is malfunctioning.</li> </ul>  <p>This function is not available without AI module.</p>

# 2.4.3 Dimensions

Figure 2-18 Dimensions with LCD (mm [inch])

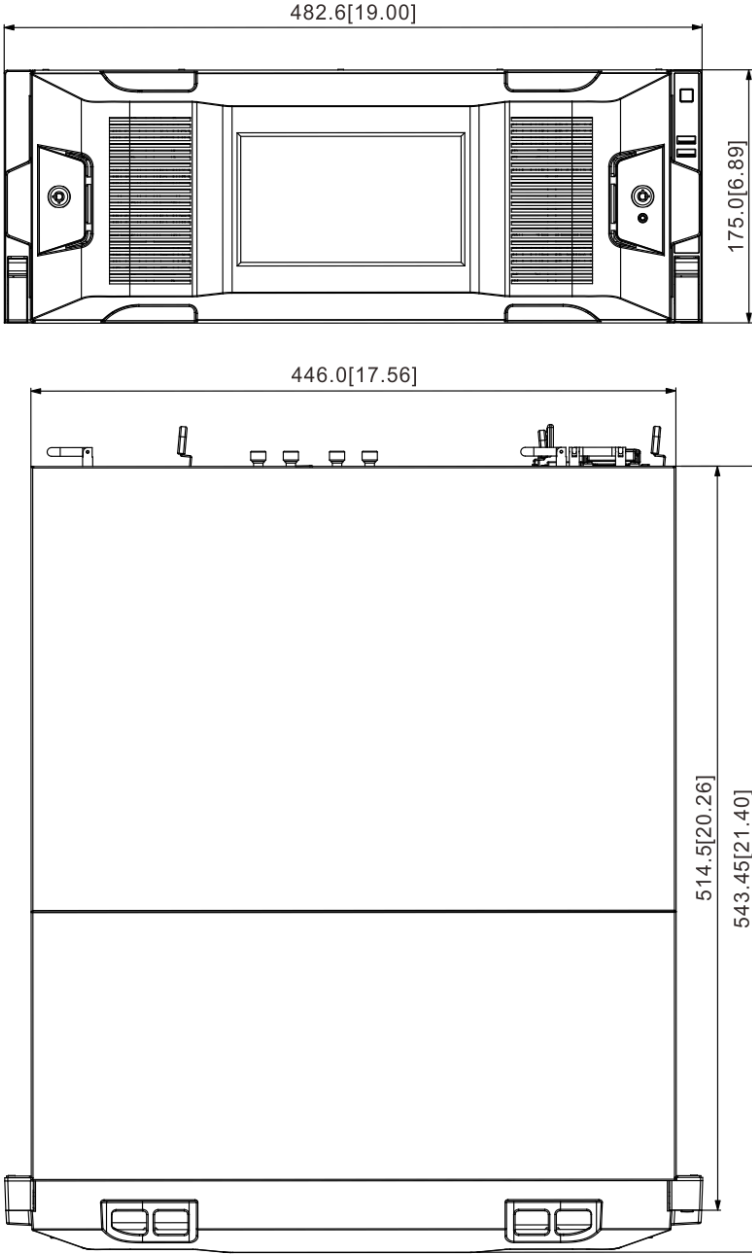
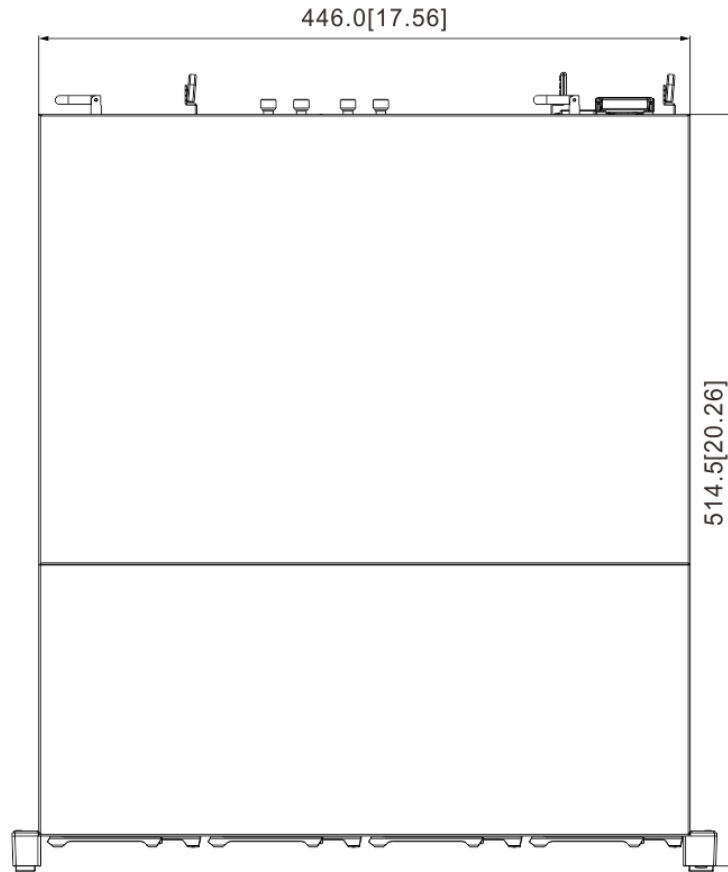
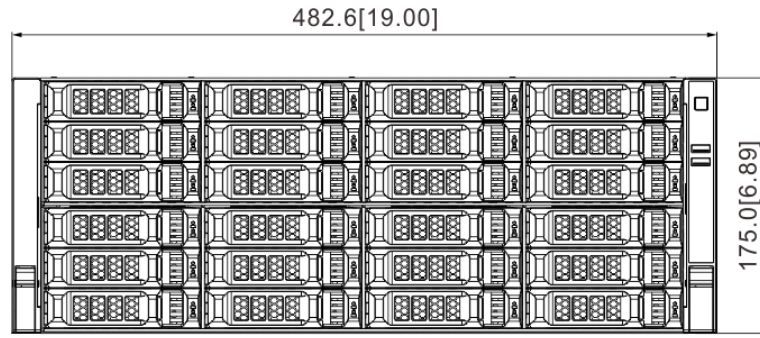


Figure 2-19 Dimensions without LCD (mm [inch])



# 3 Hardware Installation

You need to install HDD, connect cable, and so on, so IVSS can store videos and images for features and properties analysis and comparison.

## WARNING

Some products are heavy. Several people may be required to carry the product jointly to prevent personal injury.


## 3.1 Installation Flow

Follow Figure 3-1 to install the hardware.



## 3.2 Unpacking the Box

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

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

Install the number of HDD you require as per the following guidance.



Different models support different HDD numbers, and the actual product shall prevail.

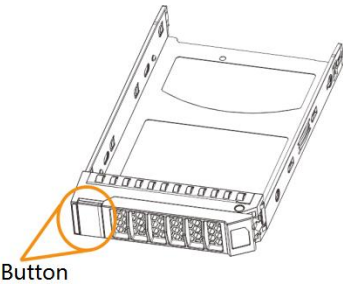
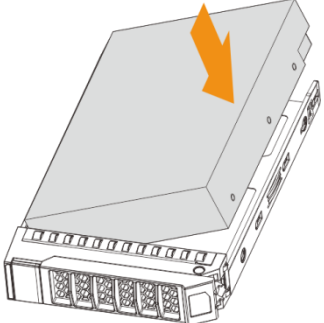
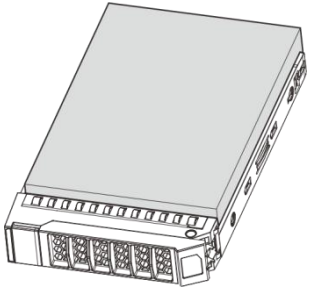


### 3.3.1 12-HDD Series

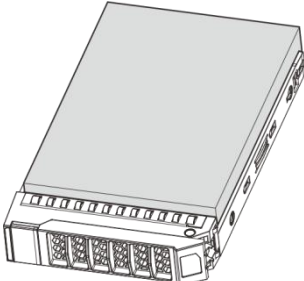
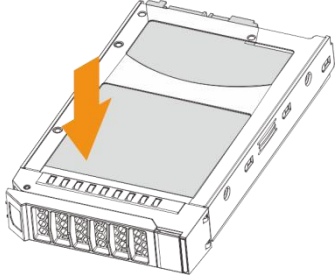
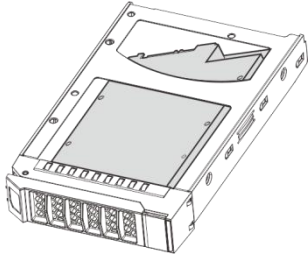


If you have not pushed the HDD box to the bottom, do not close the handle to avoid any damage to the HDD slot.

#### Installing HDD

 <p>Button</p>		
<p>① Press the button on the front panel of IVSS, open the handle, and then pull out the HDD box.</p>	<p>② Place one side of the HDD closely along the upper side of the box and press down to push the HDD down to the lower side of the mounting surface.</p>	<p>③ Insert the HDD box into the HDD slot, press it to the bottom, and then close the box handle.</p>

#### Removing HDD

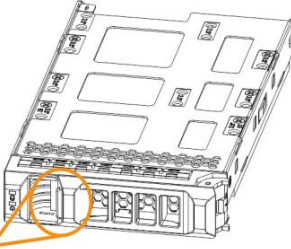
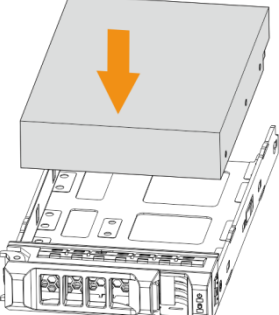
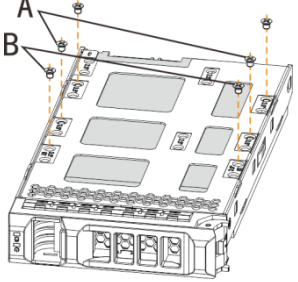

		
<p>① Press the button on the front panel of IVSS, open the handle, and then pull out the HDD box.</p>	<p>② On the back of the HDD box, press hard on the position indicated by the arrow.</p>	<p>③ Take out the HDD and reinsert the box to the slot. Push it to the bottom and close the box handle.</p>

### 3.3.2 16/24-HDD Series

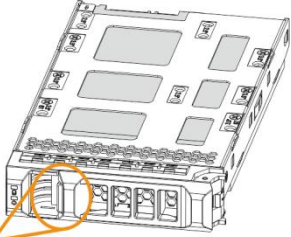
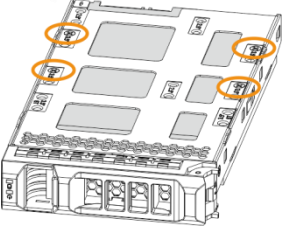
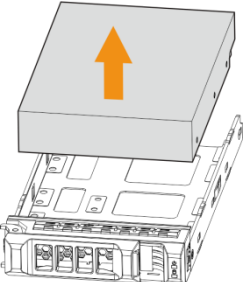



If you have not pushed the HDD box to the bottom, do not close the handle to avoid any damage to the HDD slot.

#### Installing HDD

 <p>Button</p>		
<p>① Press the button on the front panel of IVSS, open the handle, and then pull out the HDD box.</p>	<p>② Put the HDD into the box along the direction shown in the figure.</p>	<p>③ Lock the screws on the back of the HDD box. Insert the box into the HDD slot, push it to the bottom, and then close the handle.</p> <p></p> <p>In the figure, you only need to lock one set of the screws (Group A or Group B). See the actual situation.</p>

## Removing HDD

 <p>Button</p>		
<p>① Press the button on the front panel of IVSS, open the handle, and then pull out the HDD box.</p>	<p>② Unlock the screws on the back of the HDD box.</p> <p></p> <p>The screws are at different positions for different HDDs, and the actual product shall prevail.</p>	<p>③ Take out the HDD and reinsert the box to the slot. Push it to the bottom and close the box handle.</p>

## 3.4 Device Connection

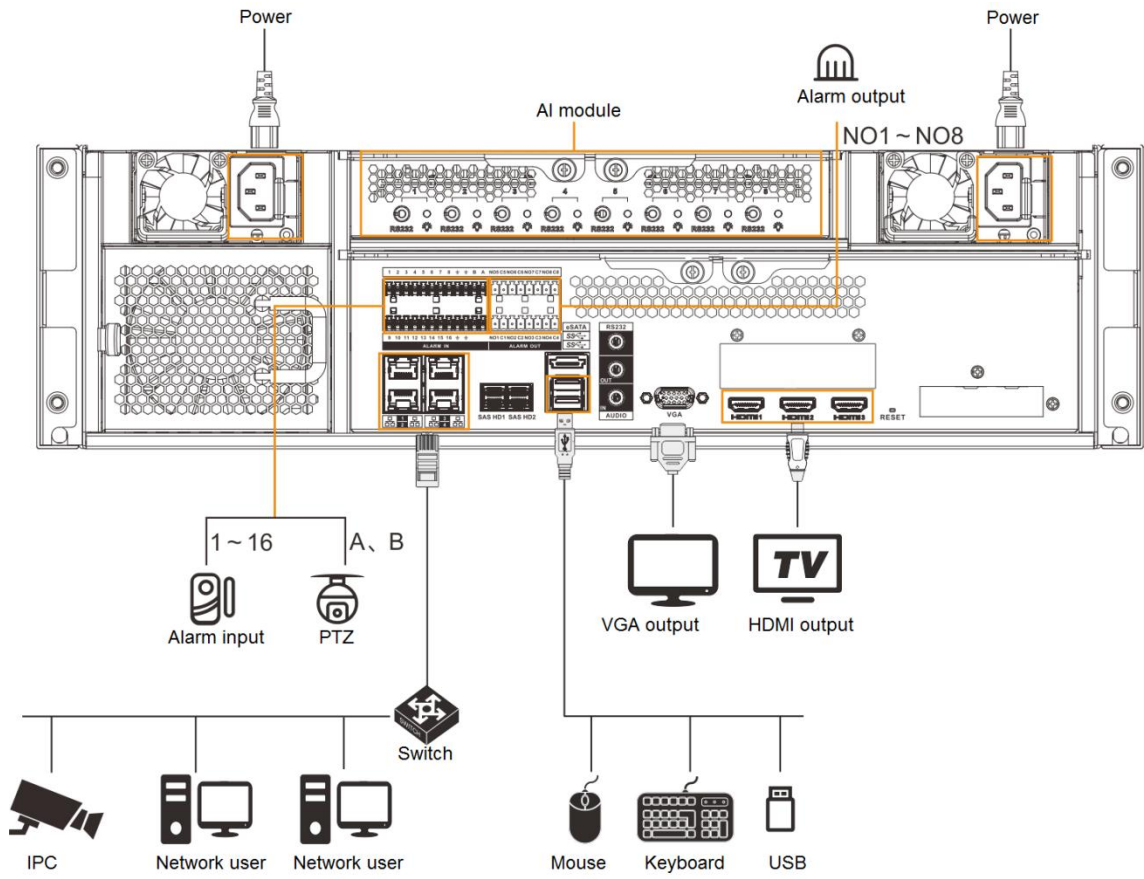
You need to connect the ports of IVSS to different devices, so the IVSS can realize various functions such as trigger alarm, stores videos/images to USB storage devices. See Figure 3-2.



The following steps are to connect 16-HDD series device. Please refer to the actual product for detailed information.

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

Figure 3-2 Connection diagram



### 3.4.1 Alarm Connection

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

#### 3.4.1.1 Alarm Port

For alarm port, see Figure 3-3 or Figure 3-4. For details, see Table 3-1.

Figure 3-3 Alarm port (8 and 12-HDD)

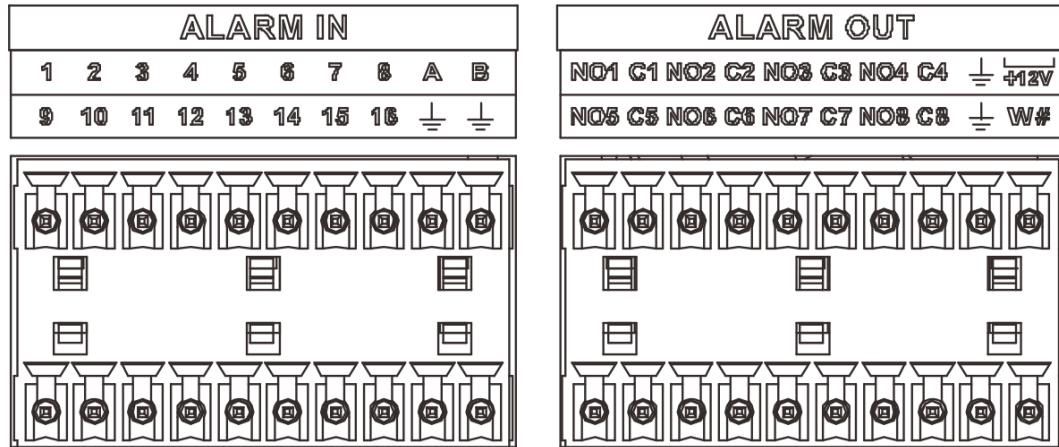


Figure 3-4 Alarm port (16 and 24-HDD)

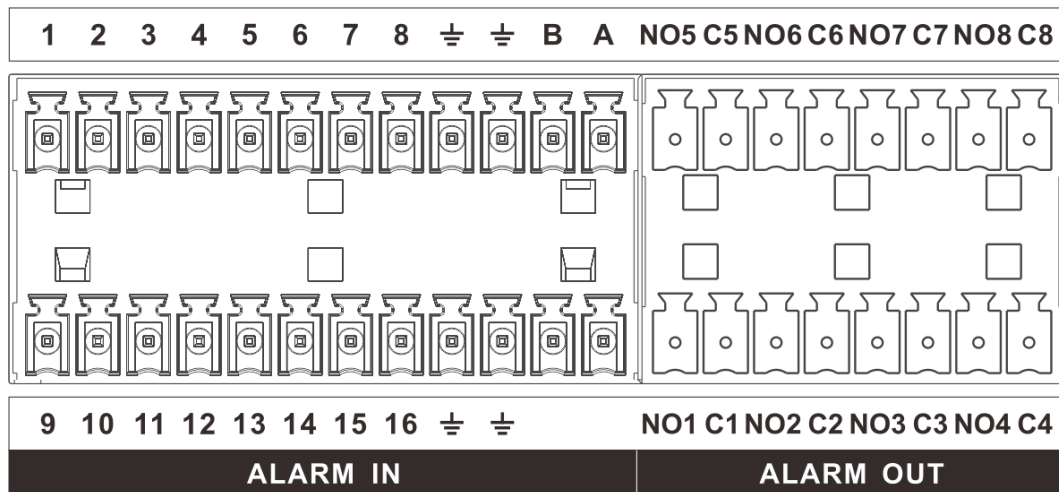


Table 3-1 Alarm port

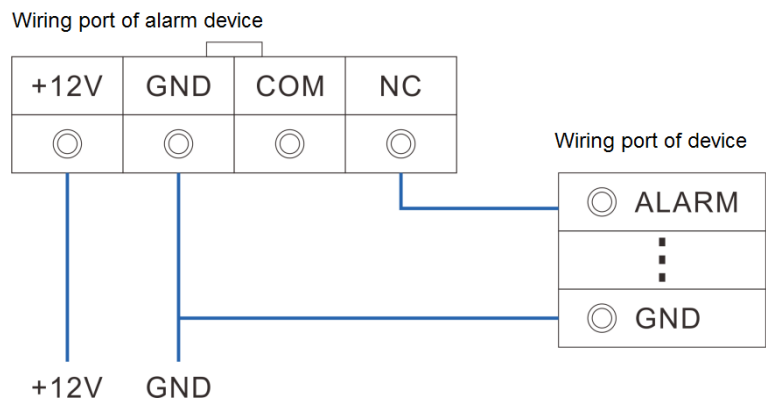
Icon	Description
1–16	They are corresponding to ALARM 1–ALARM 16. The alarm becomes valid in low level.
NO1 C1–NO8 C8	Eight groups of normally open linkage output (on/off value)
+12V	Constant power output, 500mA current.
⏏	Grounding wire.
A, B	A and B: Control the A/B cable of the RS–485 device. It is to connect to the PTZ camera. Please parallel connect 120Ω between A/B cables if there are too many PTZ decoders.

### 3.4.1.2 Alarm Input

Both NO and NC are supported. The alarm input port supports alarm signal from ground and device of 12V-24V voltage. If the alarm device is connected to the Device and other devices, use relay for isolation. See Figure 3-5.

- GND and COM of alarm device shall be connected in parallel. Alarm device shall be powered with 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 (1–16).

Figure 3-5 NC alarm input connection



### 3.4.1.3 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.

- 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, please refer to the parameters about relay. For details, see Table 3-2.

Table 3-2 Relay parameters of alarm output port

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

### 3.4.2 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 lightning protection.
- Remotely import  $120\Omega$  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 5V.

### 3.4.3 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 IVSS.

# 4 Booting Up IVSS



- Before booting up IVSS, make sure the input voltage shall 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.

Startup may vary depending on the model you purchased.

- 8-HDD series IVSS: Press the power button on the rear panel to boot up IVSS.
- For other series IVSS:
  - ◇ Connect to the power socket to boot up IVSS.
  - ◇ After clicking shutdown button on the GUI to shut down the device, press the power button for a short period of time to boot up the device.

# 5 Initial Settings

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

## 5.1 Initializing Device

For first-time use after purchasing IVSS or restoring factory settings, set the login password of admin (system default user). You can also set password protection.



This section takes initialization on web for example.

**Step 1** Open the browser, input IP address of IVSS, and press Enter key.

The **Device Initialization** interface is displayed. See Figure 5-1.



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



Figure 5-1 Initializing the device

**Step 2** Set admin login password. See Table 5-1 for details.

Table 5-1 Description of password parameters

Parameter	Description
User	The default user name is admin.
Password	Set admin login password, and confirm the password. The new password can be set from 8 characters through 32 characters and contains at least two types from number, letter and special characters (excluding "", "", ";", ":" and "&"). Enter a strong password according to the password strength prompt.
Confirm Password	

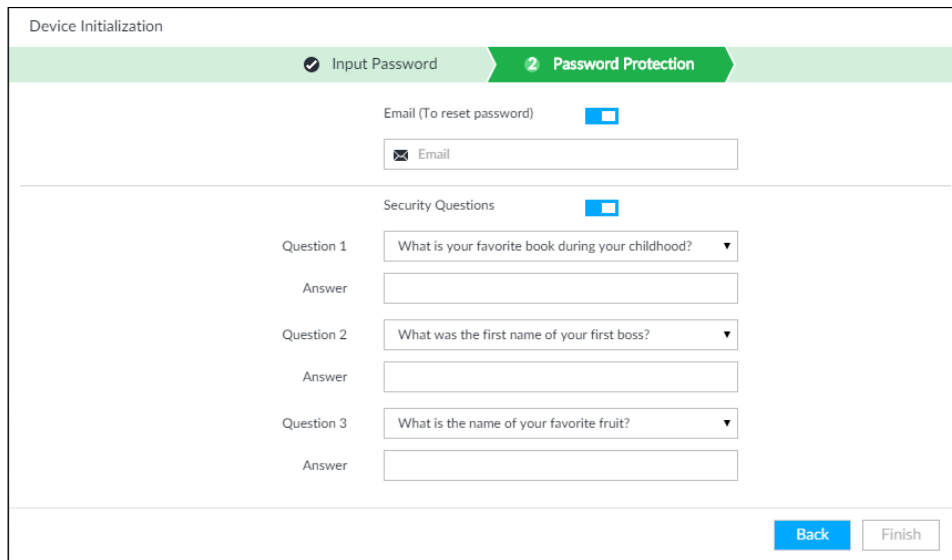


Parameter	Description
Prompt question 	After setting the prompt, when you move the mouse to  on the login interface, the system pops up a prompt to help you remember the password.  The prompt question function is for local login interface only. Refer to the actual interface for detailed information.

**Step 3** Click **Next**.

The **Password Protection** interface is displayed. See Figure 5-2.

Figure 5-2 Password protection



Device Initialization

1 Input Password 2 Password Protection

Email (To reset password)

Email

Security Questions

Question 1 What is your favorite book during your childhood?

Answer

Question 2 What was the first name of your first boss?

Answer

Question 3 What is the name of your favorite fruit?

Answer

Back Finish

**Step 4** Set password protection information. For details, see Table 5-2.

Setting the security questions here, you can use the email you input here or answer the security questions to reset admin password. To reset password, see "8.7.3.2 Reset Password."



- Click  to cancel Email or Security Questions box.
- If the email or security questions box is not set, the password can be reset on local interface only.

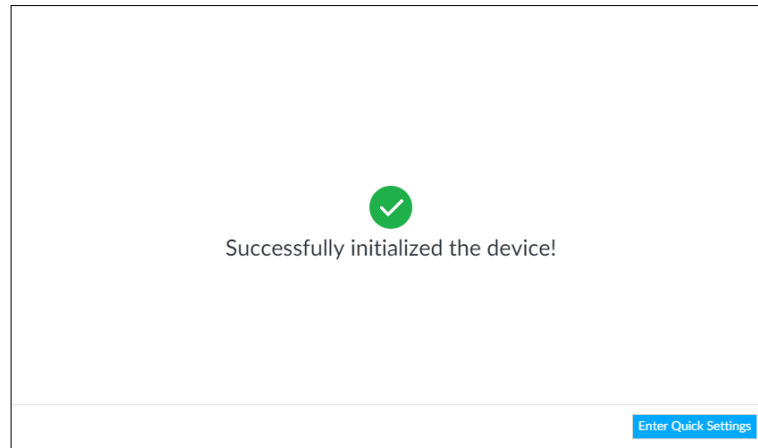
Table 5-2 Password protection

Password protection mode	Description
Email	Set email address. Reset the password through the reserved email address.
Security question	Set security questions and corresponding answers. Reset the password through the security question.

**Step 5** Click **Finish** to complete device initialization.

The device initialization success interface is displayed. See Figure 5-3. Click **Enter Quick Settings** to go to the quick setting interface, where you can quickly set system time, IP address, and P2P. Refer to "5.2 Quick Settings" for more details.

Figure 5-3 Initialization completed



## 5.2 Quick Settings

After initializing the device, it goes to quick settings interface. You can quickly set system time, IP address, and P2P.

### 5.2.1 System Time

You can set system time and enable NTP function. After NTP is enabled, IVSS automatically synchronizes time with the NTP server.


**Step 1** On the initialization interface, click **Enter Quick Settings**.

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

Figure 5-4 Time

Quick Configuration

1 Time 2 IP Set 3 P2P Access

 Date  
2018.01.22

Time  
15:36:34

Time  Manual Setting

Date/Time    Sync with your PC time

Sync with Internet Time Server

Server


Auto Sync Time Interval

Time and Date Format

Time Zone

**Step 2** Set parameters. See 0.

Table 5-3 System Time

Parameter	Description
Time	<p>You can set system date and time by selecting <b>Manual Setting</b> or <b>Sync with Internet Time Server</b>.</p> <ul style="list-style-type: none"> <li>• Select <b>Manual Setting</b> and then input actual date and time. Click <b>Sync</b>, to synchronize system time with PC time.</li> <li>• <b>Sync with the Internet Time Server</b>: Check the box and then input NTP server IP address or domain, and then set <b>Auto Sync Time Interval</b>.</li> </ul> <p> Only IVSS client or web interface supports time synchronization function.</p>
Time and date format	Set system date and time display format.
Time Zone	Set device time zone.

**Step 3** Click **Next** to save settings.

## 5.2.2 IP Address

It is to set device IP address, DNS server information and other information according to network planning.

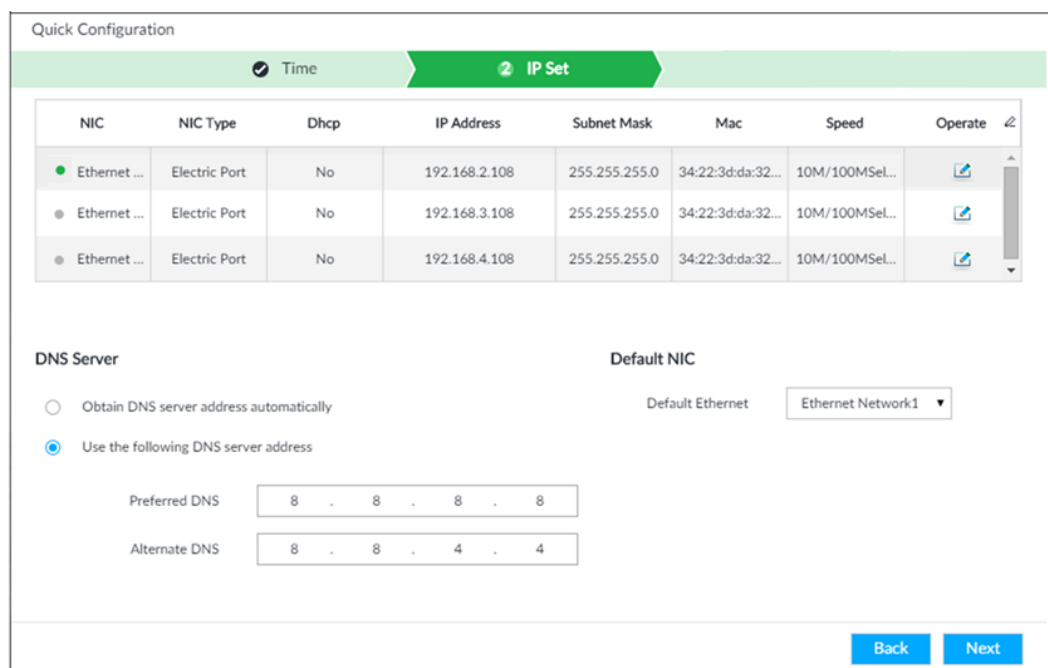


IVSS has 4 Ethernet ports by default. Make sure at least one Ethernet port is connected to network before setting IP address.

**Step 1** On **Time** setting interface, click **Next**.

The **IP Set** interface is displayed. See Figure 5-5.

Figure 5-5 Set IP



Quick Configuration

Time **2 IP Set**

NIC	NIC Type	Dhcp	IP Address	Subnet Mask	Mac	Speed	Operate
Ethernet ...	Electric Port	No	192.168.2.108	255.255.255.0	34:22:3d:da:32...	10M/100MSe...	
Ethernet ...	Electric Port	No	192.168.3.108	255.255.255.0	34:22:3d:da:32...	10M/100MSe...	
Ethernet ...	Electric Port	No	192.168.4.108	255.255.255.0	34:22:3d:da:32...	10M/100MSe...	

**DNS Server**

Obtain DNS server address automatically

Use the following DNS server address

Preferred DNS:


Alternate DNS:

**Default NIC**

Default Ethernet:

**Back** **Next**

**Step 2** Configure IP address.


- 1) Click  of the corresponding NIC.

The **Edit Ethernet Network 1** interface is displayed. See Figure 5-6.

Figure 5-6 Edit Ethernet network 1

1) Set parameters. See Table 5-4.

Table 5-4 TCP/IP parameters description

Parameter	Description
Speed	Current NIC max network transmission speed.
Use dynamic IP address	When there is a DHCP server on the network, check <b>Use Dynamic IP Address</b> , a dynamic IP address will be allocated to IVSS, and you don't need to set IP address manually.
Use static IP address	Set a static IP address for IVSS. Check <b>Use Static IP Address</b> , and then set static IP address, subnet mask and gateway.
MTU	<p>Set NIC MTU value. The default value is 1500 byte.</p> <p>We recommend you to check the MTU value of the gateway first and then set the device MTU value equal to or smaller than the gateway value. This helps reduce the packets slightly and enhance network transmission efficiency.</p>  <p>Changing MTU value may result in NIC reboot, network offline and affect current running operation. Please be careful!</p>

2) Click **OK**.

The **IP Set** interface is displayed.

**Step 3** Set DNS server information.

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



DNS server information must be configured if you want to use domain service.

- Select **Obtain DNS server address automatically**, then IVSS automatically gets the DNS server IP address on the network.
- Select **Use the following DNS server address**, and then you need to manually input preferred DNS and alternate DNS.

**Step 4** Set default NIC.

Select default NIC from the dropdown list.



Make sure the default NIC is online.

**Step 5** Click **Next** to save settings.

## 5.2.3 P2P Settings

P2P (peer-to-peer) allows resources directly available to network participants, with no need of central coordination by hosts or servers.

For IVSS, you can scan the QR code to download cellphone APP without DDNS service or port mapping or installing the transmission server. After registering a device account on the APP, you can view the remote video, play back record file, and so on.

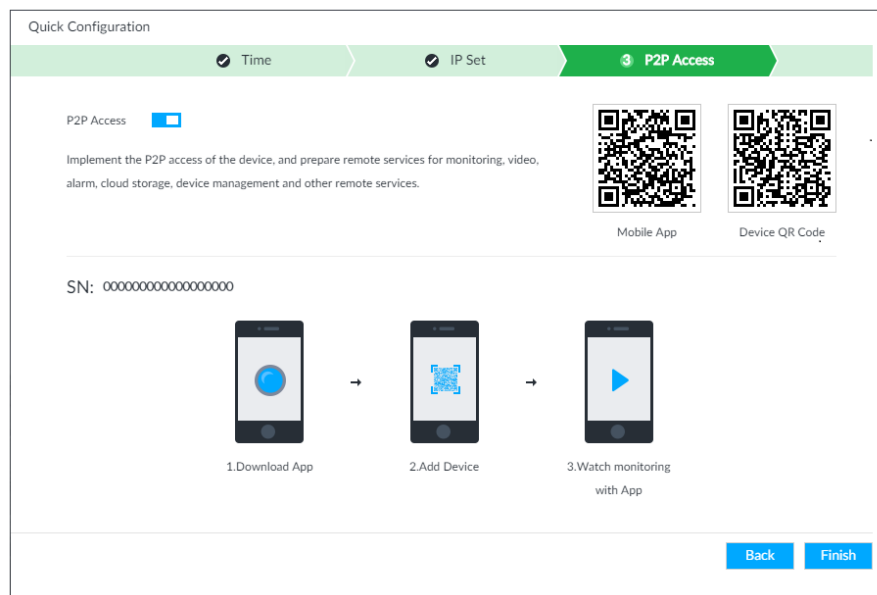


Make sure the system is connected to the network. Otherwise, the P2P function is not available.

**Step 1** On **IP Set** interface, click **Next**.

The **P2P Access** interface is displayed. See Figure 5-7. Scan the QR code on the actual interface.

Figure 5-7 P2P access



**Step 2** Click  to enable P2P function. The function is disabled by default.

**Step 3** Click **Finish** to save settings.

After the configuration, you can register a device account on the APP to view video, play back record file, and so on. Refer to corresponding cellphone APP for detailed information.

## 5.3 Login

The device supports local, web and IVSS client operation.

- Display and mouse are needed for local operation.
- Remotely access with web and IVSS client. IVSS client is recommended.



After initializing IVSS, you have logged in by default. Now you can set system settings and do operations.

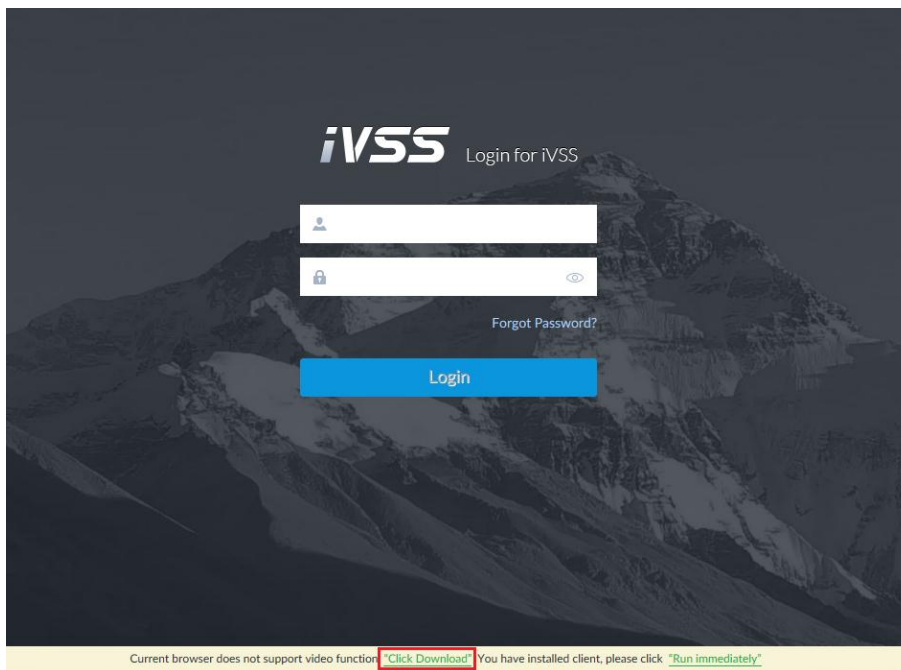
## 5.3.1 Logging in Client

System supports working with the corresponding general applications (IVSS) to access the device remotely. It is to realize system configuration, operations and system maintenance.

**Step 1** Double-click the IVSS installation package.

- 1) Open the browser, enter IP address, and press Enter key.  
Web login interface is displayed. See Figure 5-8.

Figure 5-8 Web login interface



- 2) Click **Download** to download IVSS Client installation package.



If you have downloaded IVSS Client packages, click **Run Immediately** to start IVSS Client.

**Step 2** Install IVSS Client.

- 1) Double-click the IVSS installation package.  
The **Install** interface is displayed. See Figure 5-9.

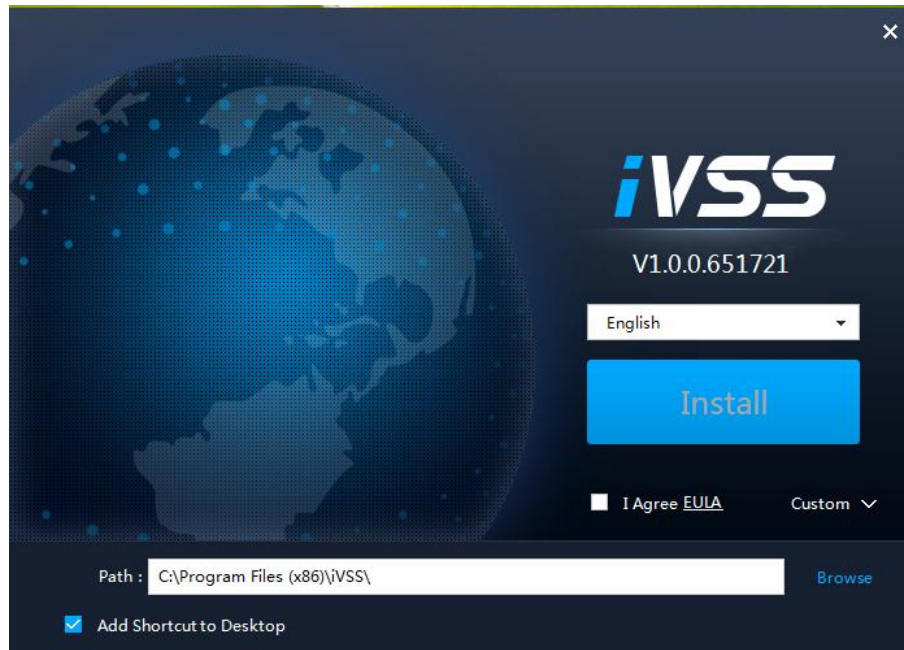
Figure 5-9 Installation interface



- 2) Select language.

- 3) Read **EULA** and then select **I Agree EULA**.
- 4) (Optional) Click **Custom** to select installation path and create shortcut. See Figure 5-10.

Figure 5-10 Custom installation.



- 5) Tick **I Agree**, and click **Install** to install IVSS client. Upon completion, the completion interface is displayed. See Figure 5-11.

Figure 5-11 The installation is completed



**Step 3** Click **Run** or double-click shortcut icon  on PC desktop to log in IVSS Client.




- When PC theme is not Aero, the system will remind you to switch the theme. See Figure 5-12. To ensure video smoothness, switch your PC to Aero theme. For details, see "10.4 Configuring IVSS Client."
- System display IVSS Client at full-screen by default. Click  to display the task column. See Figure 5-13.

Figure 5-12 Prompt

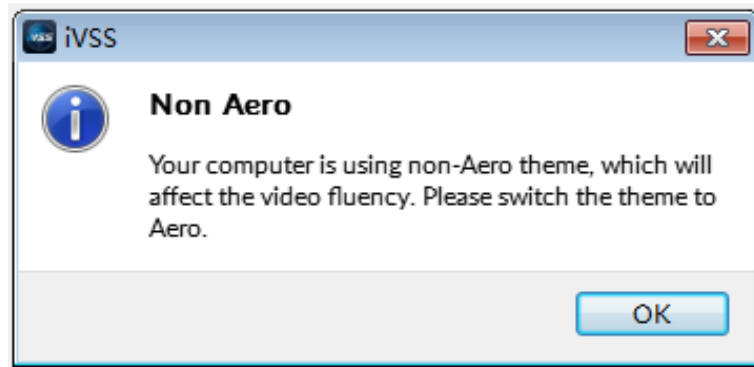
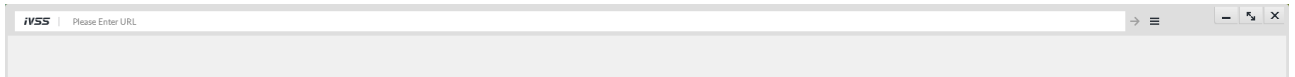


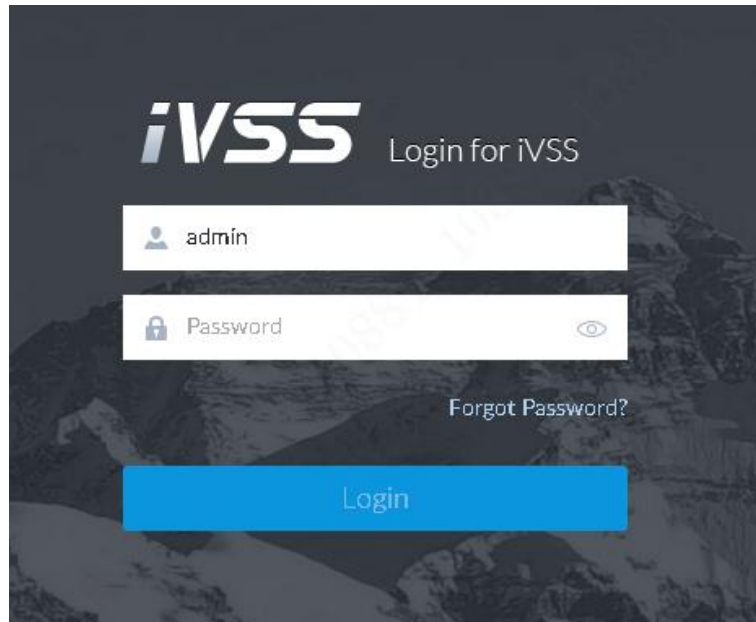
Figure 5-13 Main interface



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

The **Login** interface is displayed. See Figure 5-14.

Figure 5-14 Login



- 2) Enter device user name and password.



- Click **Login**. For your device safety, change the admin password regularly and keep it well.
- In case you forgot password, click **Forgot password?** and then follow the prompts to reset the password.

- 3) Click **Login**.

The **LIVE** interface is displayed. See Figure 5-15 and Table 5-5.



Figure 5-15 Preview

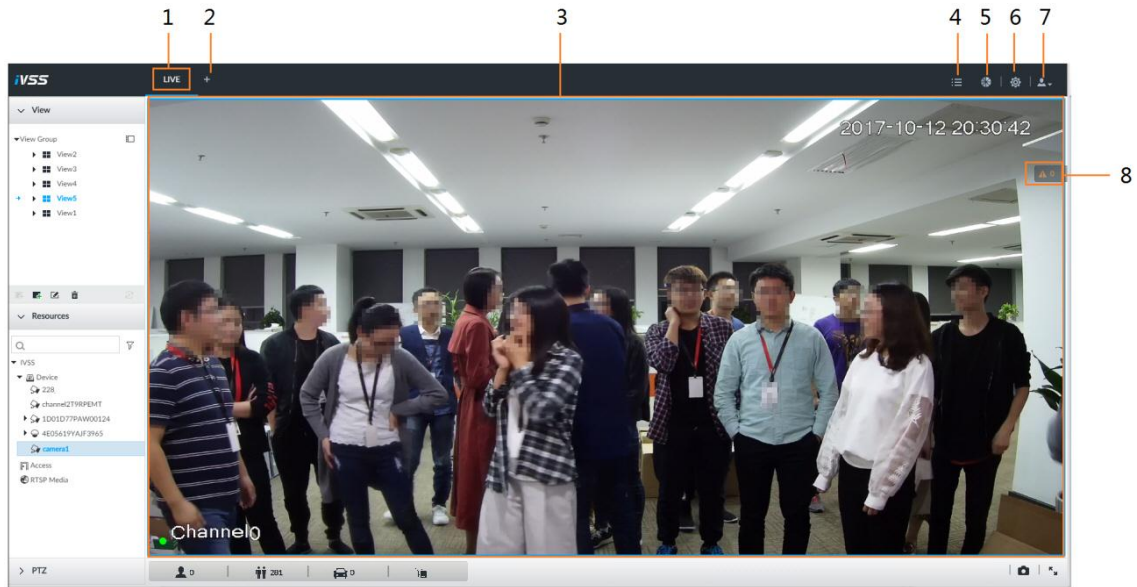





Table 5-5 Main interface description

No.	Name	Description
1	Task column	<p>Displays enabled application icon.</p> <p>Move the mouse to the app and then click  to close the app.</p> <p></p> <p>The live function is enabled by default and cannot be closed.</p>
2	Add icon	Click to display or hide app interface. On app interface to view or enable app.
3	Operation interface	Displays currently enabled app operation interface.
4	System info	Click to view system information, which includes system error, system alarm and system notification.
5	Background task	Click to view the background running task information. You can view the all tasks, running tasks or waiting tasks.
6	System config	Click to enter system configuration mode. You can configure system settings such as network, event, and storage. See "8 System Configuration" for detailed information.
7	Login user	Click it to change user password, lock user, logout user, reboot device or shut down device.
8	Alarm list	<p>Click to view alarm device name, alarm time and alarm type. For details, see "7.4 Alarm List."</p> <p></p> <p>Click Press this icon to drag up and down to adjust its position.</p>

### 5.3.2 Logging in Local Interface

IVSS can be directly connected with VGA display or HDMI display, and can carry out local operation on the display.

#### Preparation

Ensure that IVSS is connected with display, mouse and keyboard.

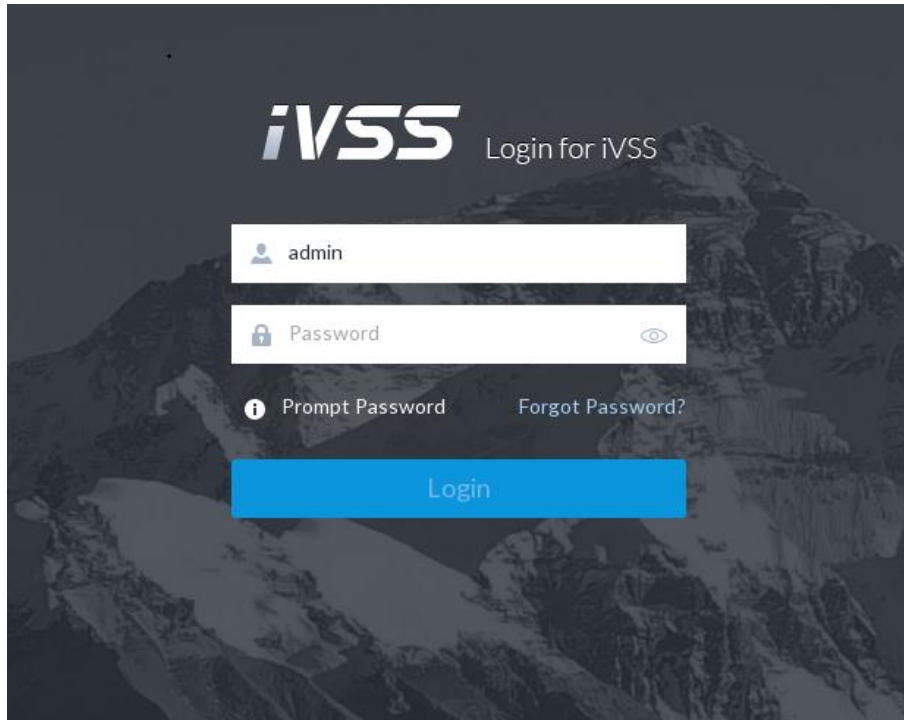
Properly wire all the required devices. For cable connection, see "3.4 Device Connection".

## Operation Steps

Step 1 Turn on IVSS.


The **Login** interface is displayed. See Figure 5-16.

Figure 5-16 Login



Step 2 Enter user name and password.



- Click **Login**. For your device safety, change the admin password regularly and keep it well.
- Move the mouse to  to view the password prompt information. It is to help you remember password.
- In case you forgot password, click **Forgot password?** and then follow the prompts to reset password.

Step 3 Click **Login**.

The **LIVE** interface is displayed. See Figure 5-17.




Click  to control the local screen. Device can connect to multiple displays at the same time. You can select a display you want to use.

Figure 5-17 Live



### 5.3.3 Logging in Web

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

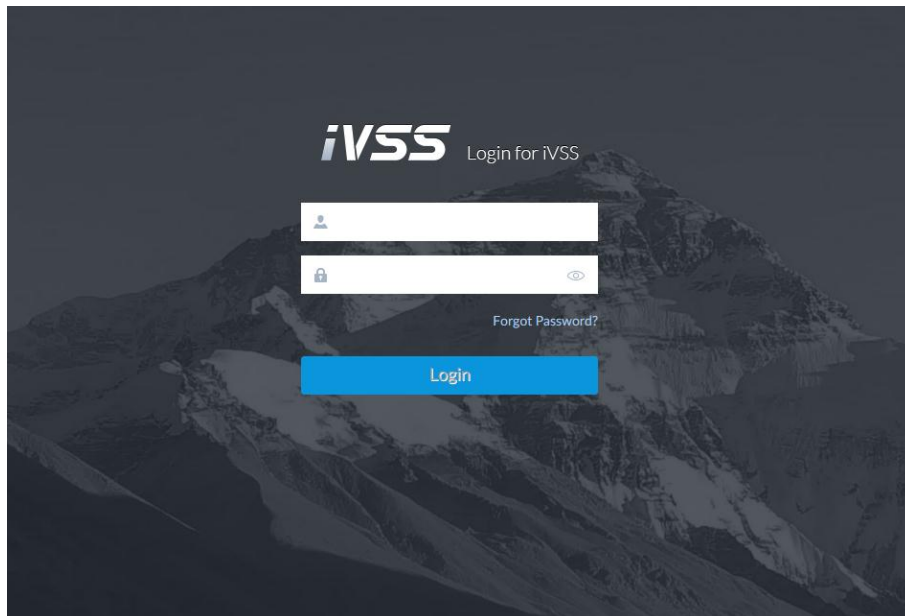


When you are using general browser to access the web, system supports setting function only. It cannot display the view. It is suggested that IVSS client should be used.

**Step 1** Open the browser, input IP address, and click **Enter**.

The **Login** interface is displayed. See Figure 5-18.

Figure 5-18 Web login interface



**Step 2** Enter user name and password.



- Click **Login**. For your device safety, change the admin password regularly and keep it well.
- In case you forgot password, click **Forgot password?** and then follow the prompts to reset password.

**Step 3** Click **Login**.

The **LIVE** interface is displayed.

## 5.4 Configuring Remote Device

Initialize remote device and then add it to IVSS, then you can manage remote device and set its parameters through IVSS.

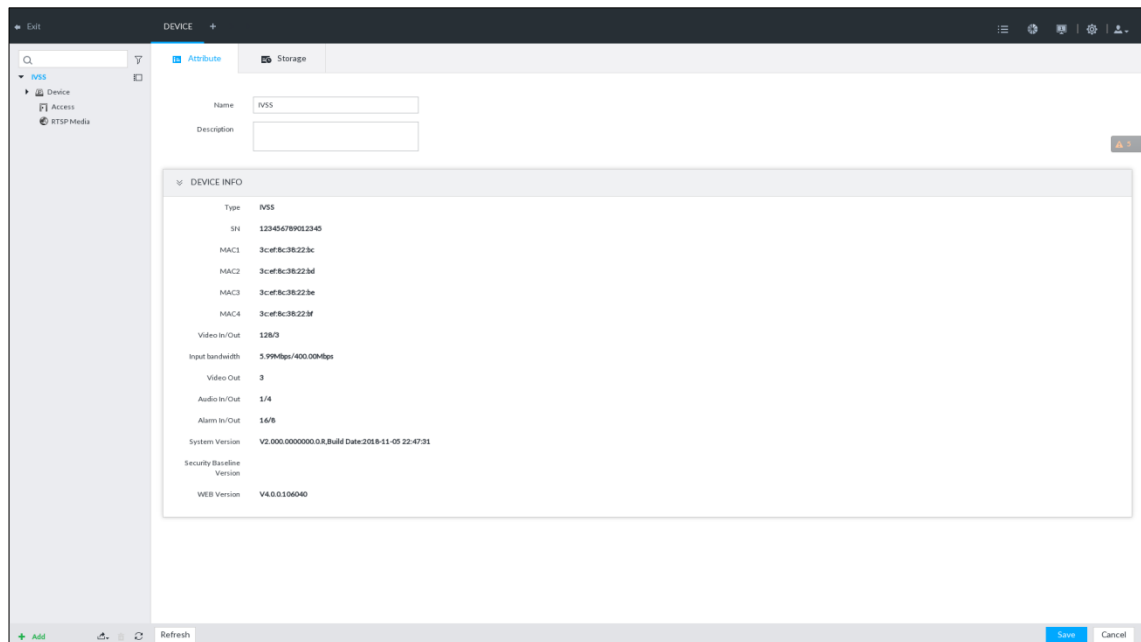
### 5.4.1 Initializing Remote Device


After you initialize remote device, you can change remote device login password and IP address. After initialization of remote device, IVSS can be connected.

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

The **DEVICE** interface is displayed. See Figure 5-19.

Figure 5-19 Device management



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

The **Smart add** interface is displayed.

**Step 3** Search remote device.



System searches the remote devices of current IP segment by default.

1) Click .

The **Add** interface is displayed. See Figure 5-20.

Figure 5-20 Add

- 2) Select manufacturer and set IP address you want to search.
  - It is to set remote device IP address. System can search the corresponding remote device.
  - It is to set remote device IP segment. System can search the remote devices of current IP segment.
- 3) Click **OK** to save the configuration.  
System goes back to Device interface.
- 4) Click **Start Search**.  
System starts to search and then displays search results. See Figure 5-21.

Figure 5-21 Remote device

<input type="checkbox"/>	Initialization State	Address	Product Model	Manufacturer	Product Type	Sn	Operate
<input type="checkbox"/>	✓ Initialized	[Redacted]	EVS	Private	EVS	--	[LIVE]
<input type="checkbox"/>	✓ Initialized	[Redacted]	PC-NVR	Private	--	--	[LIVE]
<input type="checkbox"/>	✓ Initialized	[Redacted]	IPC-HFW8281E	Private	IPC	YZC4DZ029W0...	[LIVE]
<input type="checkbox"/>	✓ Initialized	[Redacted]	DH-TPC-PT862...	Private	TPC	4K052E2YAK7...	[LIVE]
<input type="checkbox"/>	✓ Initialized	[Redacted]	JF-NC301RP-K...	Private	IPC	2A01E8AYA20...	[LIVE]
<input type="checkbox"/>	✓ Initialized	[Redacted]	NVR	WatchNet	NVR	.	[LIVE]
<input type="checkbox"/>	✓ Initialized	[Redacted]	RVi-1NR08120-P	Private	RVi	--	[LIVE]
<input type="checkbox"/>	✓ Initialized	[Redacted]	IPC-HF8249F-FR	Private	IPC	3L05538PAK00...	[LIVE]

Total 75 Item(s) Show up to 50

Bandwidth : 13.5Mbps/512Mbps

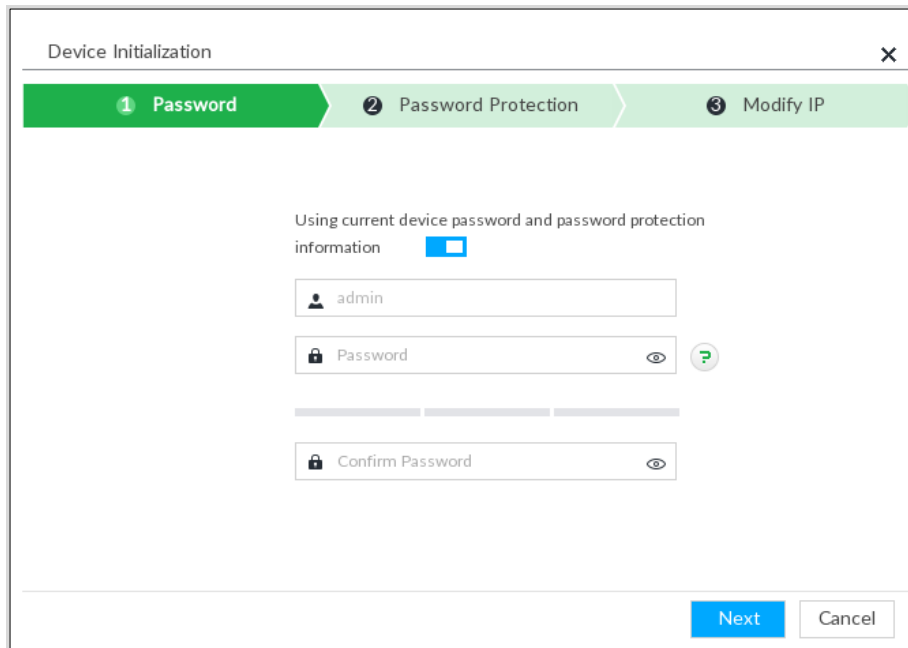
**Step 4** Select uninitialized remote device and then click **Initialize** button.

The **Device Initialization** interface is displayed. See Figure 5-22.

 **TIPS**

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

Figure 5-22 Initializing the device




The screenshot shows the 'Device Initialization' window with three steps: 1. Password (active), 2. Password Protection, and 3. Modify IP. Under the 'Using current device password and password protection information' checkbox, which is checked, there are three input fields: 'admin' for the username, 'Password' for the password, and 'Confirm Password' for the confirmation. Each password field has an eye icon for visibility and a help icon. At the bottom right, there are 'Next' and 'Cancel' buttons.

**Step 5** Set remote device password and password protection.

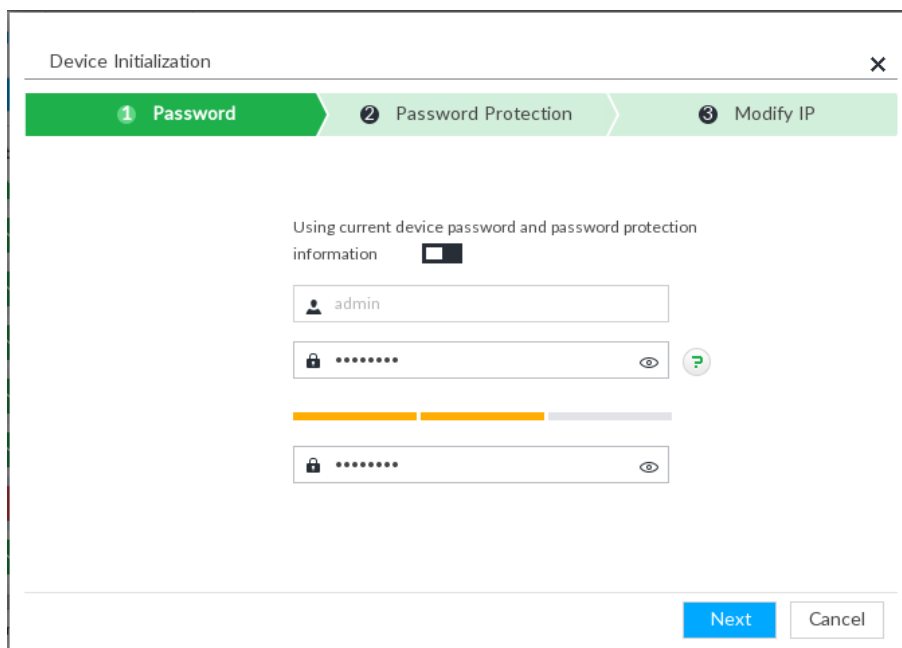


Using current device password and password protection information: Check the box to use current device admin account and email information. There is no need to set password and email. Go to Step 6.

1) Click  to select the **Using current device password and password protection information** check box.

The password setting interface is displayed. See Figure 5-23.

Figure 5-23 Password setting



The screenshot shows the 'Device Initialization' window with three steps: 1. Password, 2. Password Protection (active), and 3. Modify IP. Under the 'Using current device password and password protection information' checkbox, which is unchecked, there are three input fields: 'admin' for the username, a masked password field (represented by dots), and another masked password field for confirmation. Each password field has an eye icon for visibility and a help icon. At the bottom right, there are 'Next' and 'Cancel' buttons.

- 2) Set parameters. See Table 5-6.

Table 5-6 Description of password parameters

Parameter	Description
Username	The default user name is admin.
Password	In the New Password box, enter the new password and enter it again in the Confirm Password box.
Confirm Password	The new password can be set from 8 characters through 32 characters and contains at least two types from number, letter and special characters (excluding "'", '"', ";", ":" and "&"). Enter a strong password according to the password strength indication.

- 3) Click **Next**.

The **Password Protection** interface is displayed. See Figure 5-24.

Figure 5-24 Password protection

The screenshot shows a 'Device Initialization' window with a progress bar at the top. The progress bar has three steps: '1 Password' (completed), '2 Password Protection' (current step, highlighted in green), and '3 Modify IP'. Below the progress bar, the text 'Email (To reset password)' is displayed above an input field with an envelope icon and the placeholder text 'Email'. At the bottom right of the window, there are three buttons: 'Back', 'Next', and 'Cancel'.

- 4) Set an Email address.

Input an email address for resetting password purpose. You can use the email address here to reset password in case you forgot password in the future.

**Step 6** Click **Next**.

The **Modify IP** interface is displayed. See Figure 5-25.

Figure 5-25 Modify IP

(1) Sn	IP Address
32:c5:f8:1d:f1:b1	192.168.1.103

DHCP  Static

Static IP Address: [ . . . ] Incremental Value: [ 1 ]

Subnet Mask: [ . . . ]

Gateway: [ . . . ]

Back Next Cancel

**Step 7** Set camera IP address.

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



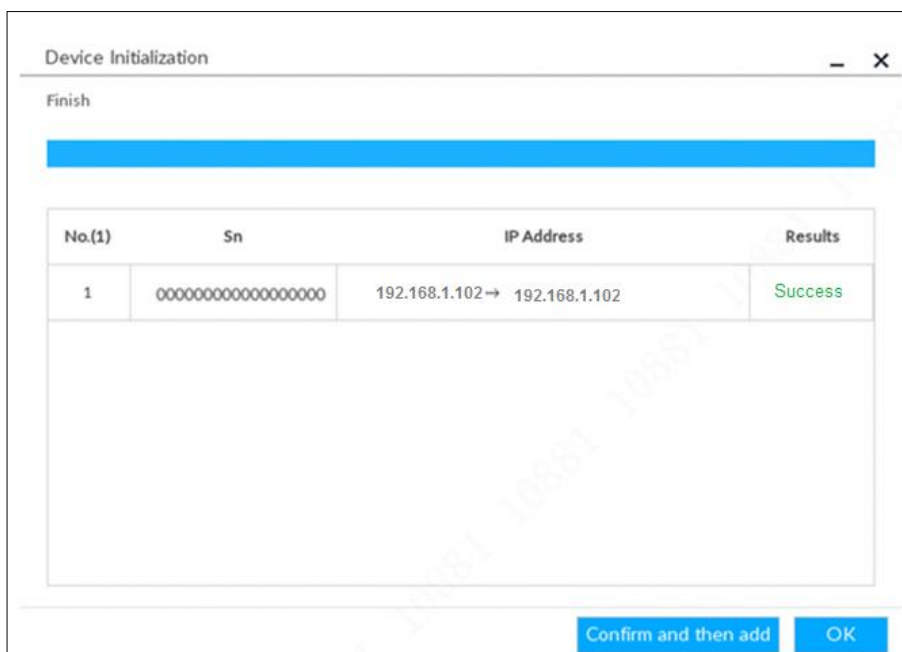
- After you input incremental value, system can add the fourth address of the IP address one by one to automatically allocate the IP addresses.
- If you want to change several devices IP addresses at the same time, system allocates IP address of the same network segment.
- If there is IP conflict when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

**Step 8** Click **Next**.

Device initialization starts. See Figure 5-26.



Figure 5-26 Initialize




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

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


## 5.4.2 Adding Remote Device

### 5.4.2.1 Smart Add

Search the remote devices on the same network and then filter to register. It is applicable when you don't know the exact IP address.

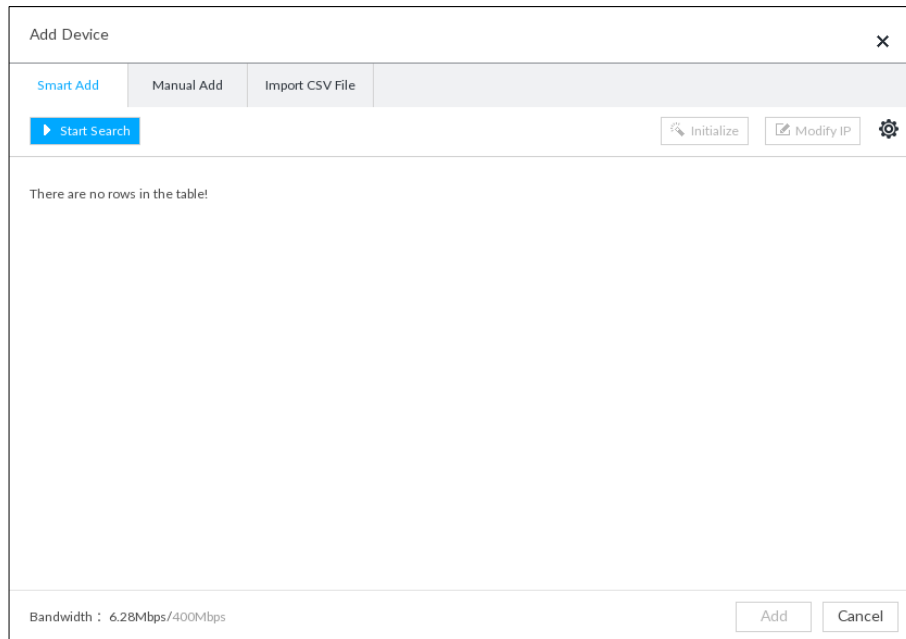
**Step 1** Click , and then select **Device**.

The **Device** interface is displayed.

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

The **Smart Add** interface is displayed. See Figure 5-27.

Figure 5-27 Short-cut menu



**Step 3** Search remote device.



IVSS searches the remote devices of current IP segment by default.

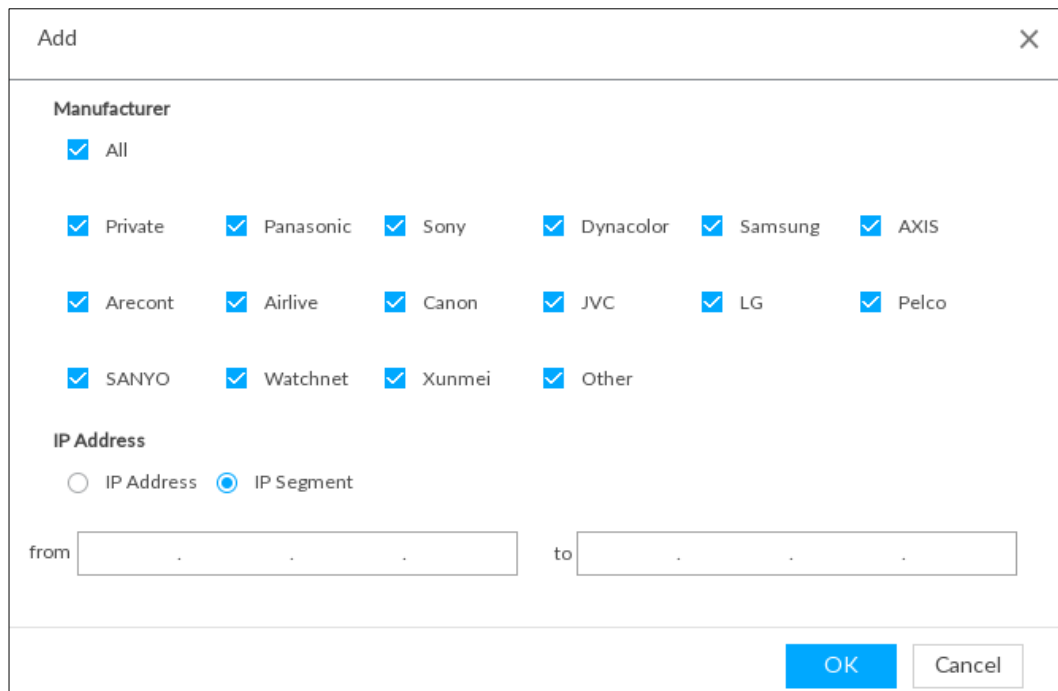
- 1) Click .

The **Add** interface is displayed. See Figure 5-28.



The actual interface shall prevail.

Figure 5-28 Add



- 2) Select manufacturer and set IP address you want to search.
  - It is to set remote device IP address. System can search the corresponding remote device.

- It is to set remote device IP segment. System can search the remote devices of current IP segment.
- 3) Click **OK** to save the configuration.  
The **Add** interface is displayed.
  - 4) Click **Start Search**.  
Search result is displayed. See Figure 5-29. Select remote device and then click Add. Device begins add remote device and pops up confirmation interface. For details, see Table 5-7.

Figure 5-29 Search result

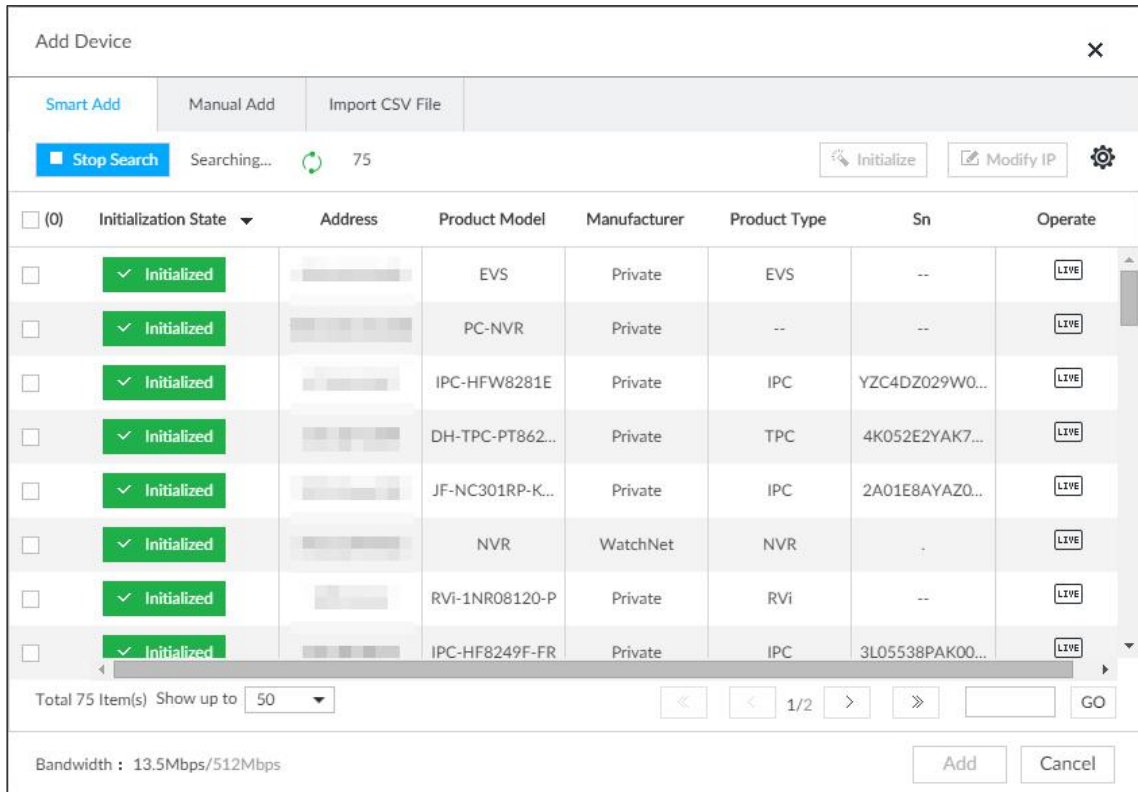



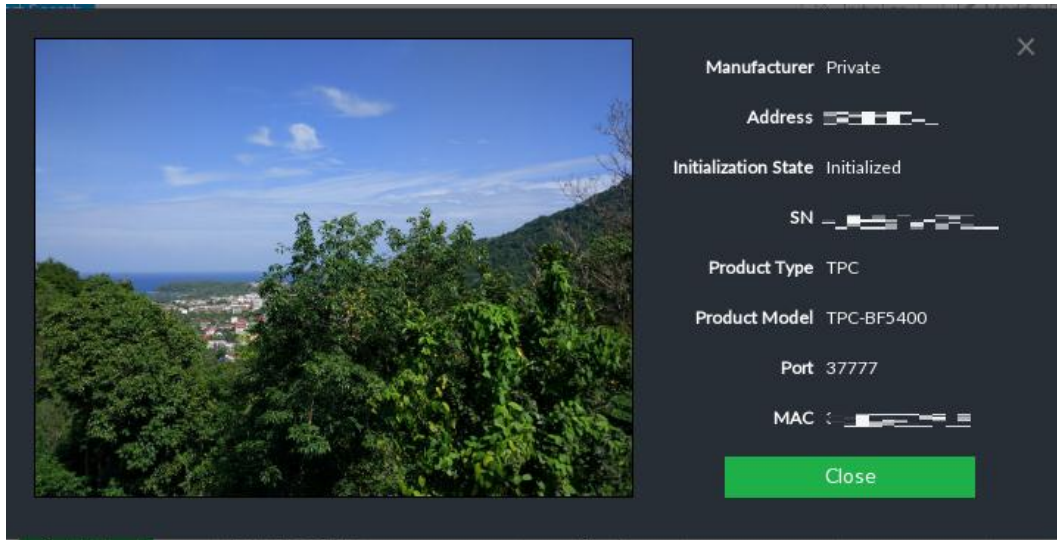


Table 5-7 Result description

Parameter	Description
Start search	Click <b>Start Search</b> to start searching remote device. Now it becomes <b>Stop Search</b> button. Click <b>Stop Search</b> button to stop searching remote device.
Initialize	Select uninitialized remote device and then click <b>Initialize</b> button to initialize remote device. Refer to "5.4.1 Initializing Remote Device" for detailed information.
Initialization State	Displays remote device initialization status. Click ▼ to filter initialized or uninitialized remote device.
Operation	Click  to display real-time preview video from the remote device. See Figure 5-30. Click  or <b>Close</b> to close the real-time preview window.  You can view the live video if admin password of the remote device is admin, or remote device admin's password is the same as the system.

Parameter	Description
Bandwidth	Displays registered remote device bandwidth and supported remote device bandwidth.

Figure 5-30 Real-time view



**Step 4** Adding a remote device.

- Add 1-channel remote device.  
Select a remote device and then click **Add**. Device begins adding remote device and pops up confirmation interface. See Figure 5-31.



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

Figure 5-31 Add confirm (1-channel)



- Add multiple-channel remote device
  - 1) Select a remote device and then click **Add** button.  
The **Add** interface is displayed. See Figure 5-32.

Figure 5-32 Add confirm (multiple-channel)

Address	Username	Password	Manufacturer	Port	Status	Operate
192.168.1.103	admin	****	Private	40009	Please select a cha...	

Bandwidth : 30.949Mbps/768Mbps

[Continue to add](#) [Finish](#)

- 2) Double click **Please select a channel**.  
The **Video Device** interface is displayed. See Figure 5-33.

Figure 5-33 Video device

(0) Video Device ▼

IP PTZ Camera

CAM 2

[OK](#) [Cancel](#)

- 3) Select a channel you want to add.

Click ▼ and then input the key words, it can quickly search the channel you want to add.

- 4) Click **OK** to add the select channels.

**Step 5** Click **Continue to add** or **Finish**.


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

## 5.4.2.2 Manual Add

Enter the IP address, user name and password of remote device, and then add it to IVSS. It is applicable when you want to add a specific device to IVSS.

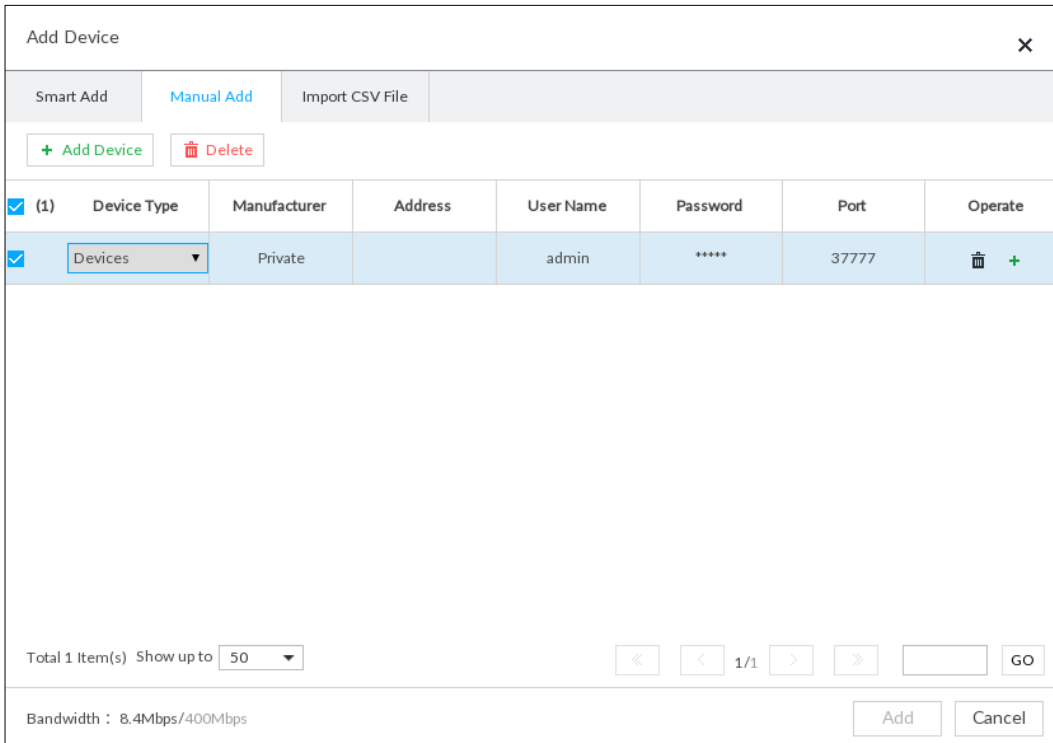
**Step 1** Click , and then select **Device**.

The **Device** interface is displayed.

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

The **Manual Add** interface is displayed. See Figure 5-34.

Figure 5-34 Manual add



Add Device								
Smart Add		Manual Add		Import CSV File				
<input type="button" value="+ Add Device"/>		<input type="button" value="Delete"/>						
<input checked="" type="checkbox"/>	(1)	Device Type	Manufacturer	Address	User Name	Password	Port	Operate
<input checked="" type="checkbox"/>		Devices	Private		admin	*****	37777	<input type="button" value="Delete"/> <input type="button" value="+"/>

Total 1 Item(s) Show up to 50

Bandwidth : 8.4Mbps/400Mbps


**Step 3** Click **Add Device** button.

The **Add Device** interface is displayed. See Figure 5-35.

Figure 5-35 Add device

**Step 4** Set parameters. For details, refer to Table 5-8.

Table 5-8 Remote Devices Configurations Description

Parameter	Description
Type	It is to select remote device type. The default type is Devices.
Manufacturer	<p>Displays the connection protocol of the remote device. Default protocol of the system is <b>Private</b>. Double click <b>Private</b> to select other protocols.</p> <p>To add stream media device, select Rtsp protocol, and enter RTSP address of stream media device in Address column. See Figure 5-36.</p> <p>Rtsp://&lt;user name&gt;:&lt;password&gt;@&lt;IP address&gt;:&lt;port&gt;/cam/realmonitor?channel=1&amp;subtype=0U.</p> <ul style="list-style-type: none"> <li>● Port: Enter port number. The default setting is 554.</li> <li>● Channel: Enter channel number of the stream media device to be added.</li> <li>● Subtype: It is to set record bit stream type. It includes main stream 0 and sub stream 1.</li> </ul> <p>For example rtsp://admin:admin@192.168.20.25:554/cam/realmonitor?channel=1&amp;subtype=0.</p> <p> To add a stream media device, it is unnecessary to set user name, password, and port.</p>
Address	Enter the IP address or RTSP address of remote device.
Username	It is to input user name and password of remote device.
Password	
Port	Displays port number of remote device.



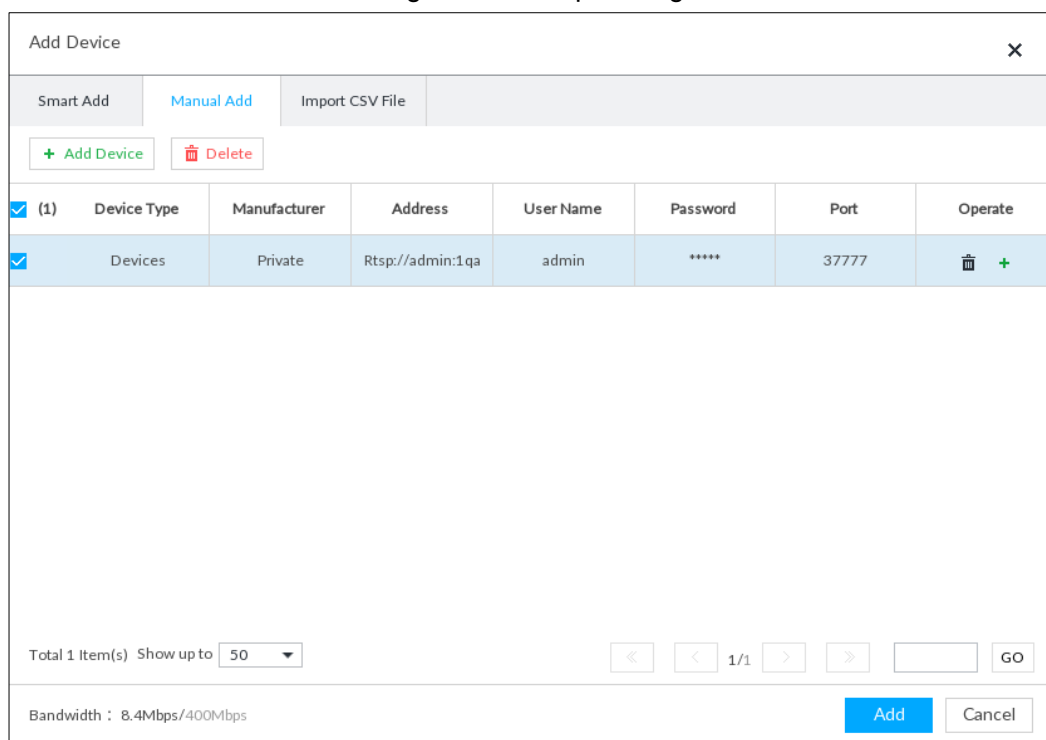
Parameter	Description
Operation	<p>Delete current line or add a new line.</p> <ul style="list-style-type: none"> <li>Click  to delete current line information. Select multiple lines of remote device information, and then click <b>Delete</b> to batch delete the selected information.</li> <li>Click  to add a new line. Enter remote device information to add several devices at the same time.</li> </ul>

Figure 5-36 Rtsp Adding



The screenshot shows a web interface titled "Add Device" with a close button (X) in the top right. Below the title bar are three tabs: "Smart Add", "Manual Add" (which is active), and "Import CSV File". There are two buttons: "+ Add Device" and "Delete". Below these is a table with the following columns: checkboxes, (1), Device Type, Manufacturer, Address, User Name, Password, Port, and Operate. One row is visible with the following data: checked checkbox, (1), Devices, Private, Rtsp://admin:1qa, admin, \*\*\*\*\*, 37777, and icons for delete and add. At the bottom, there is a status bar showing "Total 1 Item(s) Show up to 50", navigation arrows, "1/1", a search box, and a "GO" button. A bandwidth indicator shows "Bandwidth : 8.4Mbps/400Mbps". At the bottom right are "Add" and "Cancel" buttons.

**Step 5** Adding a Remote Device.

- Add 1-channel remote device.  
Select remote device and then click **Add** button. Device begins add remote device and pops up confirmation interface. See Figure 5-37.



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



Figure 5-37 Add confirm

Address	Username	Password	Manufacturer	Port	Status	Operate
192.168.1.105	admin	*****	Private	40009	Added	

Bandwidth : 30.949Mbps/768Mbps

[Continue to add](#) [Finish](#)

- Add multiple-channel remote device
  - 1) Click **Add**.  
The **Add Device** interface is displayed. See Figure 5-38.

Figure 5-38 Add confirm

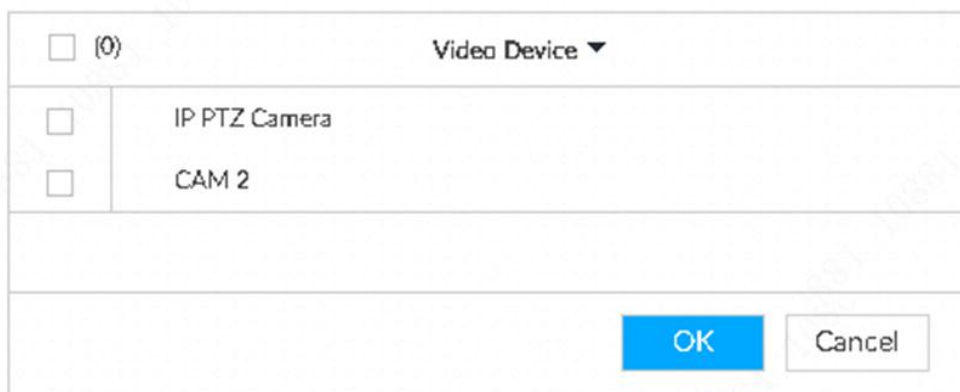
Address	Username	Password	Manufacturer	Port	Status	Operate
192.168.1.106	admin	*****	Private	40009	Please select a cha...	

Bandwidth : 30.949Mbps/768Mbps

[Continue to add](#) [Finish](#)

- 2) Double click **Please select a channel**.  
The **Video Device** interface is displayed. See Figure 5-39.

Figure 5-39 Video device



3) Select a channel you want to add.

Click ▼ and then input the key words, it can quickly search the channel you want to add.


4) Click **OK** to add the select channels.

**Step 6** Click **Continue to add** or **Finish**.


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

### 5.4.2.3 Template Add

Fill in information about remote device in the template, import the template to add the device. It is applicable when user name and other information of remote devices are not the same.

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

The **Device** interface is displayed.

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



The **Import CSV file** interface is displayed. See Figure 5-40.

Figure 5-40 Import CSV file

**Step 3** Fill in template file.

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

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

- At IVSS client, click , select Download content to view file saving path.  
For details, see 10.3 View Downloads
- Select file saving path during local operation.  
  
Connect USB device to IVSS if you are on the local menu to operate.
- During web operations, files are saved under default downloading path of the browser.

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

The following information of template file shall be filled in. See Figure 5-41.



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

Figure 5-41 File

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

**Step 4** Import template file

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

The imported information about remote device is displayed. See Figure 5-42.



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


- Click  to delete current line information.

Figure 5-42 Device information

Add Device
×

Smart Add | Manual Add | Import CSV File

Choose File

<input type="checkbox"/>	(0)	Device Type	Manufacturer	Address	User Name	Password	Port	Operate

Total 0 Item(s) Show up to 



1/1

Bandwidth : 13.44Mbps/400Mbps

**Step 5** Add remote device.

- Add 1-channel remote device.  
Select a remote device and then click **Add** button. Device begins adding remote device and pops up confirmation interface. See Figure 5-37.



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

Figure 5-43 Add confirm

Address	Username	Password	Manufacturer	Port	Status	Operate
192.168.1.105	admin	*****	Private	40009	Added	

Bandwidth : 30.949Mbps/768Mbps

[Continue to add](#) [Finish](#)

- Add multiple-channel remote device
  - 1) Select a remote device and then click **Add** button.  
Enter **Add** interface. See Figure 5-44.

Figure 5-44 Confirm

Address	Username	Password	Manufacturer	Port	Status	Operate
192.168.1.106	admin	*****	Private	40009	Please select a cha...	

Bandwidth : 30.949Mbps/768Mbps

[Continue to add](#) [Finish](#)

- 2) Double-click **Select a channel**.  
Enter **Video channel** interface. See Figure 5-45.

Figure 5-45 Video device

<input type="checkbox"/> (0)	Video Device ▼
<input type="checkbox"/>	IP PTZ Camera
<input type="checkbox"/>	CAM 2
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

3) Select a channel you want to add.

Click ▼ and then input the key words, it can quickly search the channel you want to add.

4) Click **OK** to add the select channels.

**Step 6** Click **Continue to add** or **Finish**.

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

# 6 AI Operations

AI detection is to process and analyze the video and take the key information, compare the key information with the preset detection rule and trigger an alarm once the detected behavior matches the detection rule.

The device supports AI by camera and AI by device.

- AI by camera: The camera supports smart detection. The IVSS needs to detect and display the intelligent alarm information from the remote device.
- AI by device: The camera only provides videos and snapshots, but IVSS supports smart detection.



When AI by camera is enabled, smart detection configuration has to be set on remote device. See remote device user's manual.

## 6.1 Enabling AI Plan

AI functions, such as AI detection and analysis, will not work before AI plan is enabled.



- AI plan is available on select models.
- The interface may vary with different AI functions.

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

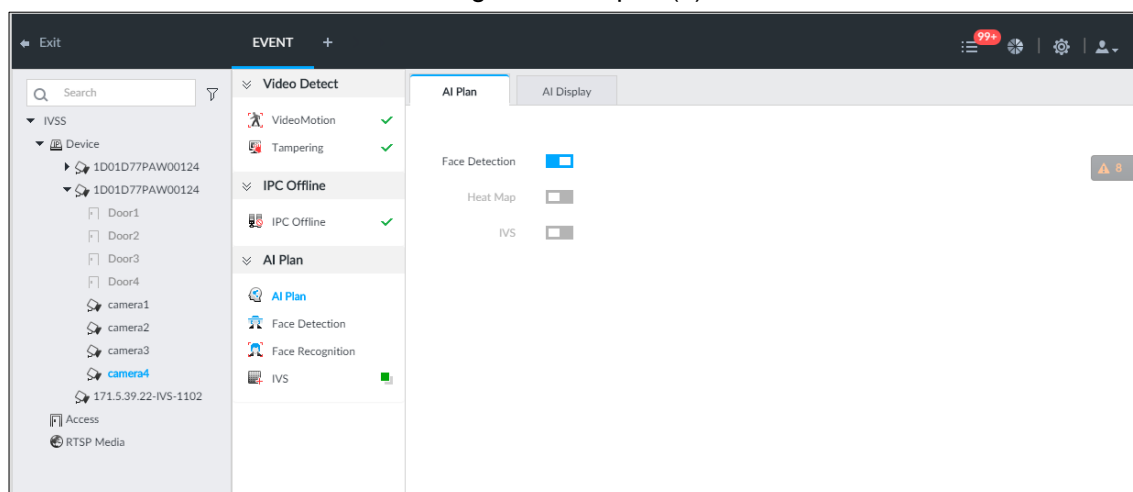
The **EVENT** interface is displayed.

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

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

The **AI Plan** interface is displayed. See Figure 6-1.

Figure 6-1 AI plan(1)



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

**Step 5** Click **Save**.

## 6.2 Face Detection

- After you configure face detection and face comparison function, the device processes and analyzes video image, extract face information from the video, and compare it with face images in the face database.
- Alarm is triggered when similarity reaches or exceeds the designated similarity.
- IVSS supports real-time view of face detection and face comparison information; searches and plays back video according to face features.



IVS and face detection function cannot be enabled at the same time.

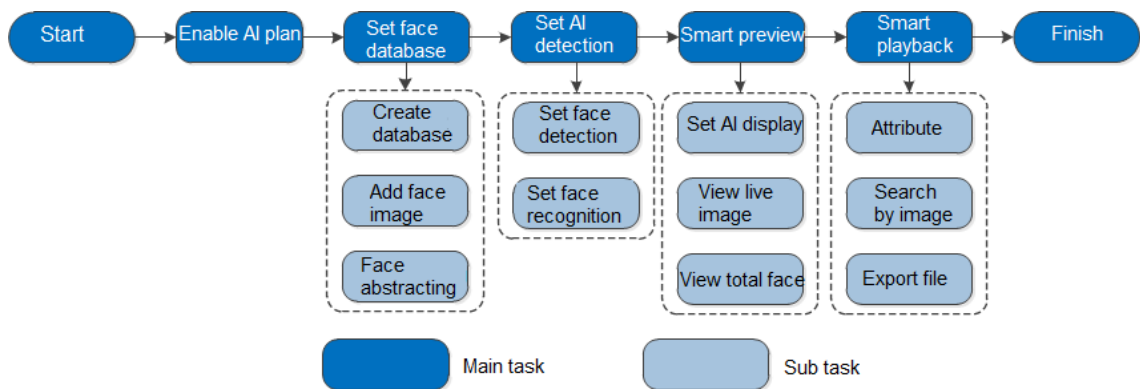
### 6.2.1 Setting

Set face comparison flow. See Figure 6-2.



- You need to enable AI plan before using AI by camera. Refer to "6.1 Enabling AI Plan" to enable AI detect function.
- You cannot search by image when you are using AI by camera and face comparison.

Figure 6-2 Face comparison flow



### 6.2.2 Configuring Face Database

You can create the face database to save face image, and the intelligent detection function can trigger the face database to carry out human face comparison, human face search, and so on. For face database configuration flow, see Figure 6-3.

Figure 6-3 Deleting face database



#### 6.2.2.1 Creating Face Database

Create human face database to sort out and manage the face images uploaded to IVSS.

#### Creating human face database



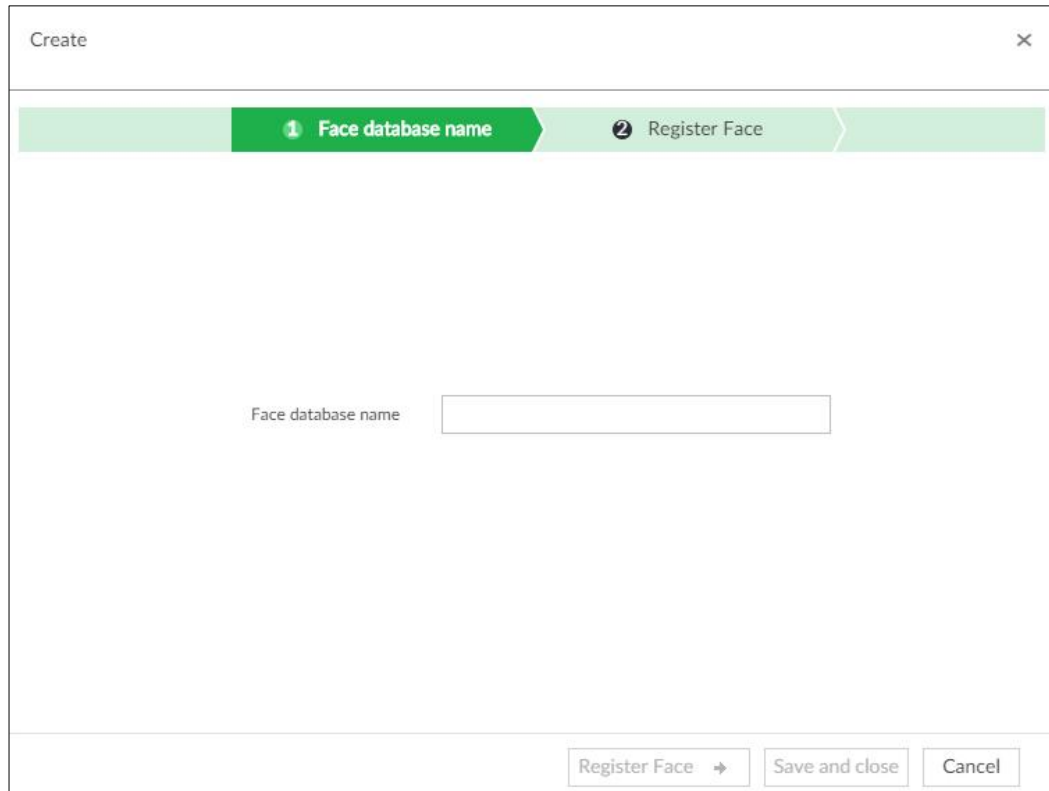
Step 1 On the **LIVE** interface, click **+**, select **File > Face database**.

**Face database** interface is displayed.

Step 2 Click **Create**.

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

Figure 6-4 Create face database



The screenshot shows a 'Create' dialog box. At the top, there is a title bar with the word 'Create' and a close button (X). Below the title bar is a progress bar with two steps: '1 Face database name' (highlighted in green) and '2 Register Face'. The main area of the dialog contains a text input field labeled 'Face database name'. At the bottom right, there are three buttons: 'Register Face' with a right arrow, 'Save and close', and 'Cancel'.

Step 3 Set **Face database name**.

Step 4 Click **Register face** or **Save and close**.

- Click **Register face**, and then add human face on the newly created human database. See Figure 6-5.

Figure 6-5 Register face

Create Usage 0%

Face database name 2 Register Face

Add mode  Manual Add  Batch Import

Name

Gender  Male  Female

Birthday

Country or Region

Address

ID Type

ID No.

Back Save and continue to add OK Cancel

- Click **Save and close** to create a human face database with no data. After creating face database, you can go to the **Face Database** interface to view the newly created face database information. See Figure 6-6. For details, see 0.

Figure 6-6 Face database

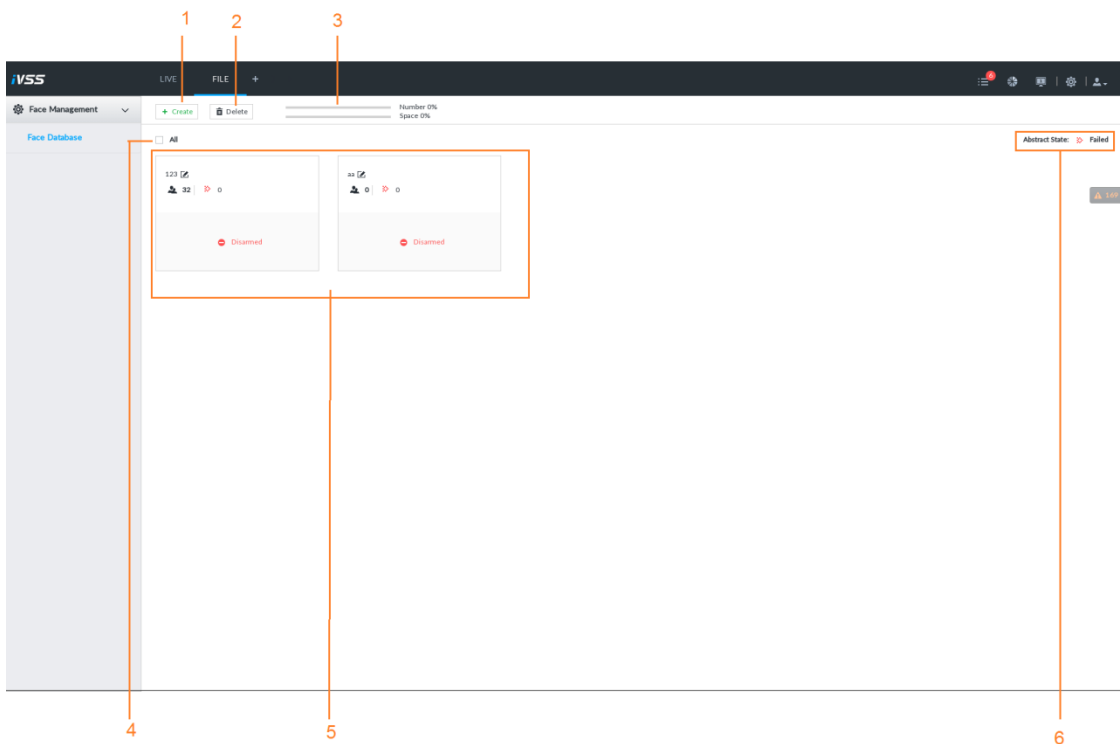










Table 6-1 Description


No.	Description
1	Click <b>Create</b> to create a face database. For details, refer to "6.2.2.1 Creating Face Database".
2	Select a face database, and then click <b>Delete</b> to delete the database.
3	<p>Display number and space information of face database.</p> <ul style="list-style-type: none"> <li>Number: The percentage ratio of the added face image quantity to the allowable total quantity of face image. Device supports maximum 300,000 face images.</li> <li>Space: The percentage ratio of the created face database quantity to the allowable total quantity of face database. Human face database creation. Maximum 50 databases.</li> </ul>
4	Check <b>All</b> to select all face databases.
5	Display the list of created databases.
6	<p>Display abstract state.</p> <p>  displays face image of current database that failed to abstract.</p>

## Operation

You can modify database name, upload face images to database, arm or delete the database, after the database is created. Refer to Table 6-2 for detailed information.

Table 6-2 Operation of face database

Name	Operation
View face database information and state.	<p>View face database information and state in face database zone.</p> <ul style="list-style-type: none"> <li> Set Human face database name.</li> <li> 3945 is to display face image of current database.</li> <li>  is to display human face that failed abstracting. Refer to "6.2.2.3 Human Face for detailed information.</li> <li> means current face database has not connected to the corresponding channel to compare human face. After arm, the interface can display the remote device that is connected with the face database.</li> </ul>
Change face database name	Click  to change face database name.
Managing face image	Double click face database to enter face database interface and manage face images. For details, refer to "7.3 File Management".
Arming face database	Link the face database to compare faces, and arm the face database. For details, refer to "6.2.4 Configuring Face ".

Name	Operation
Deleting face database	<ul style="list-style-type: none"> <li>● Delete: Move the cursor to the face database and click  at the top right corner of the face database to delete.</li> <li>● Batch delete: Move the cursor to the face database and then click <input type="checkbox"/> at the top left corner of the face database. Select several face databases at the same time and then click <b>Delete</b> to delete them.</li> <li>● Check <b>All</b> box and then click <b>Delete</b> to delete all face database.</li> </ul>

## 6.2.2.2 Adding Face Image

Add face images to the created face database in the way of manual add, batch import and detection.

### Preparation

- A face image has been obtained, and it meets the following requirements:
  - ◇ The image format is .jpg.
  - ◇ The image size shall be less than or equal to 4MB.
  - ◇ The resolution ranges from 100×100 to 6000×5000.
- You have obtained the face image and saved it in the proper path.
  - ◇ When operating on the local interface, save the image in the USB storage device and then connect the USB storage device to the IVSS.
  - ◇ When operating on the Web or IVSS interface, save the image on the PC in which the Web or IVSS client is located.

#### 6.2.2.2.1 Manual Add

You can add human face image one by one. If the registered human face image quantity is small, you can use manual add mode.

**Step 1** On **LIVE** interface, click , select **File > Face Database**.

**Face Database** interface is displayed.

**Step 2** Double click face database.

Face database interface is displayed. See Figure 6-7.

Figure 6-7 Manual add



**Step 3** Click **Manual Add**.

The **Face Register** interface is displayed. See Figure 6-8.

Figure 6-8 Face register

Face Register

Name

Gender  Male  Female

Birthday

Country or Region

Address

ID Type

ID No.

Save and continue to add OK Cancel

**Step 4** Click  and select face image.

The **Open** interface is displayed. See Figure 6-9.



- When the uploaded image is half-length photo or full-body photo, the system automatically selects the frame of the uploaded image and only the face area will be retained.
- When there are multiple faces in the uploaded images, the system automatically identifies the faces in the images and uploads multiple face images according to the number of faces recognized. See Figure 6-10. Select face image you want to upload. Blue frame means that it is selected.
- Click Cancel to cancel all checked face images.

Figure 6-9 Confirm choice

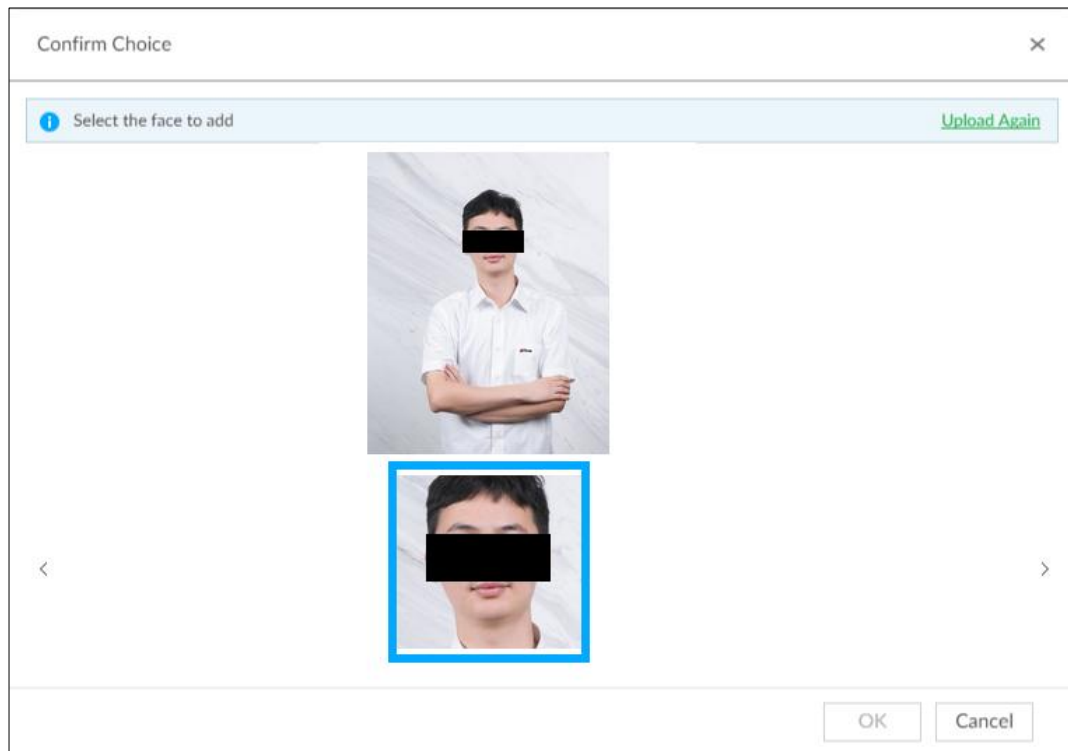
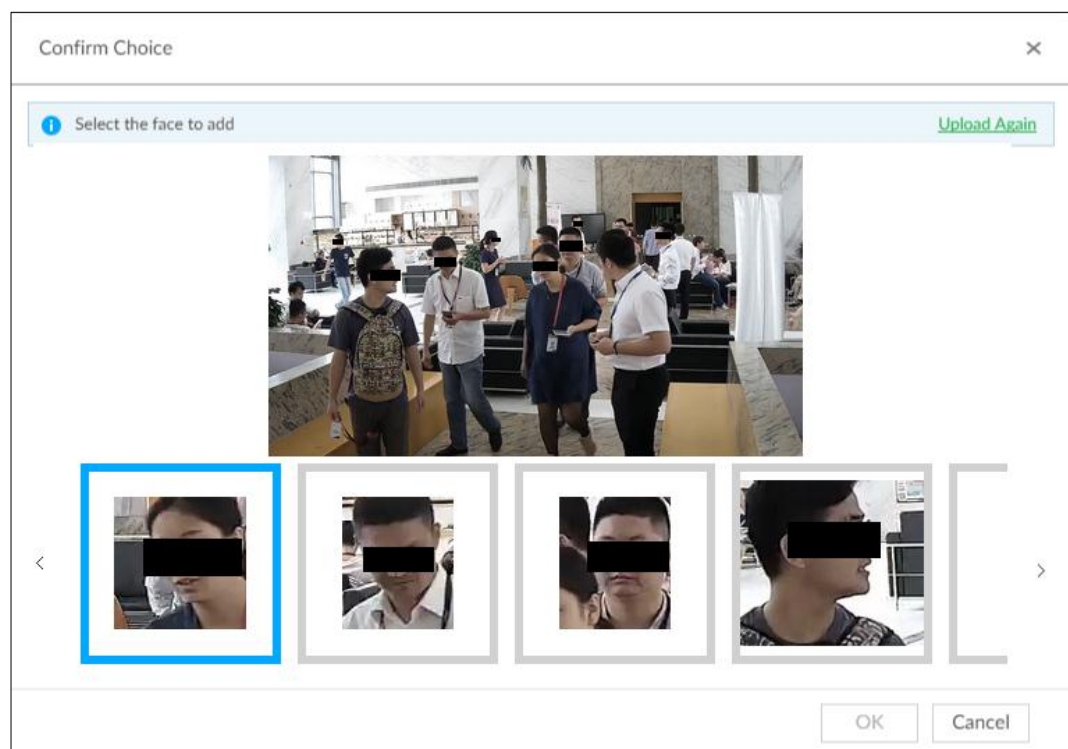


Figure 6-10 Confirm choice



**Step 5** Click **OK**, import face image.

The **Face Register** interface is displayed. See Figure 6-11.



Move the cursor to the face image and click **Change Image** to change it.

Figure 6-11 Face register

Face Register

Name: [Redacted]

Gender:  Male  Female

Birthday: [Redacted]

Country or Region: [Redacted]

Address: [Redacted]

ID Type: [Redacted]

ID No.: [Redacted]

Change Image

Save and continue to add OK Cancel

**Step 6** Fill in face image information.

**Step 7** Click **Save and continue to add** or **OK**.

- Click **Save and continue to add**, it is to save current face image information and add another human face image.
- Click **OK** to save current face image information and complete registration.


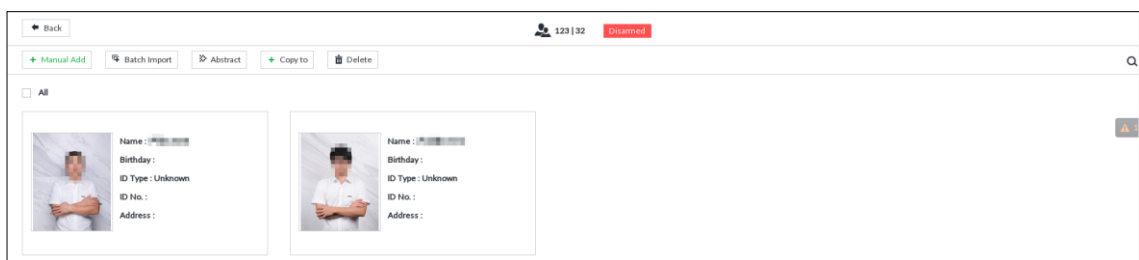
After adding the image, at the bottom left corner of the human face image, there is an icon . It means device is creating module. See Figure 6-12. Refer to "6.2.2.3 Human Face" for detailed information.

Figure 6-12 Manual add



### 6.2.2.2.2 Batch Import

Batch import is to import multiple face images at the same time by uploading file or uploading folder. If you want to register a large number of face images, batch import is recommended.

### Preparation

Before the batch import, name the face image according to the following rule: "Name#SGender#BBirthday#NNation#PProvince#TIDtype#MIDnumber#AAddress.jpg" (such as "Tim#S1#B20000101#NCN#PZheJiang#T1#M0000#AAddress").

Name the face image according to the rule. After successful import, the system will identify the face image automatically. For details about naming rule, see Table 6-3.



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

Table 6-3 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 yyyyymmdd or yyyy-mm-dd. For example, 20181123.
Abbreviation of countries/regions	Enter the corresponding abbreviation of the nation/region.
Province	Enter the corresponding spelling or English name of the province.
ID type	Enter the corresponding number. 1. ID card, 2. Passport, 3. Officer Card.
ID number	Fill in the corresponding ID number.
Address	Enter the detailed address.

## Operation Steps

**Step 1** On the **LIVE** interface, click , select **File > Face Database**.

**Face Database** interface is displayed.

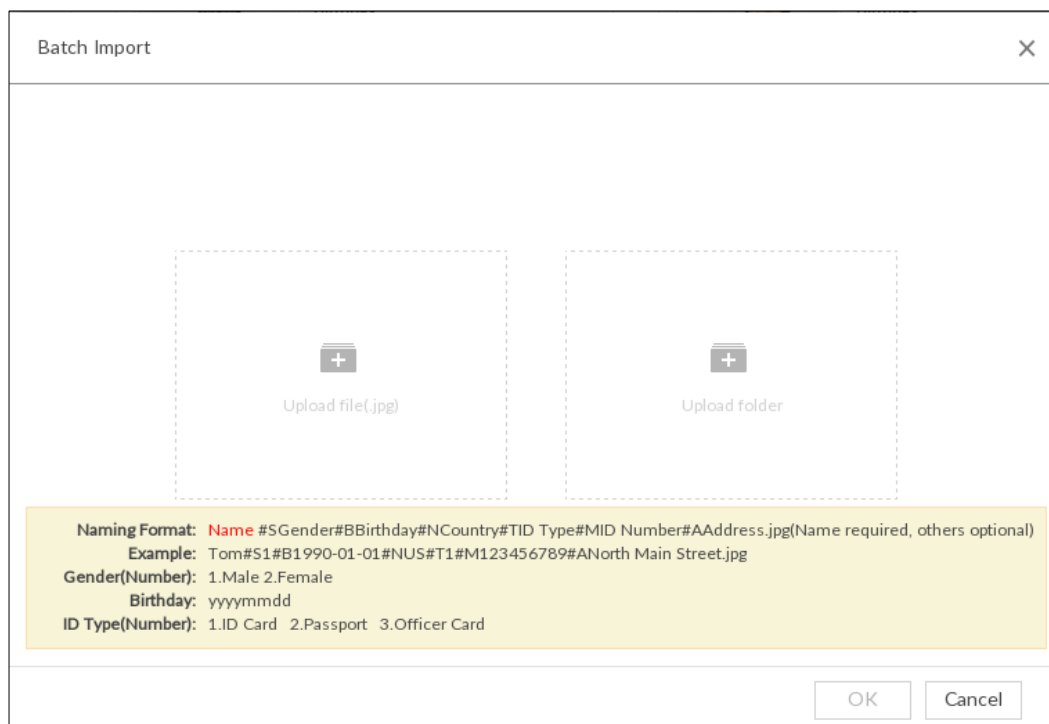
**Step 2** Double-click face database.

The face database interface is displayed.

**Step 3** Click **Batch Import**.

The **Batch Import** interface is displayed. See Figure 6-13.

Figure 6-13 Batch import







**Step 4** Import face image.

The system supports to upload file and folder. Select according to your actual need.

- Upload File

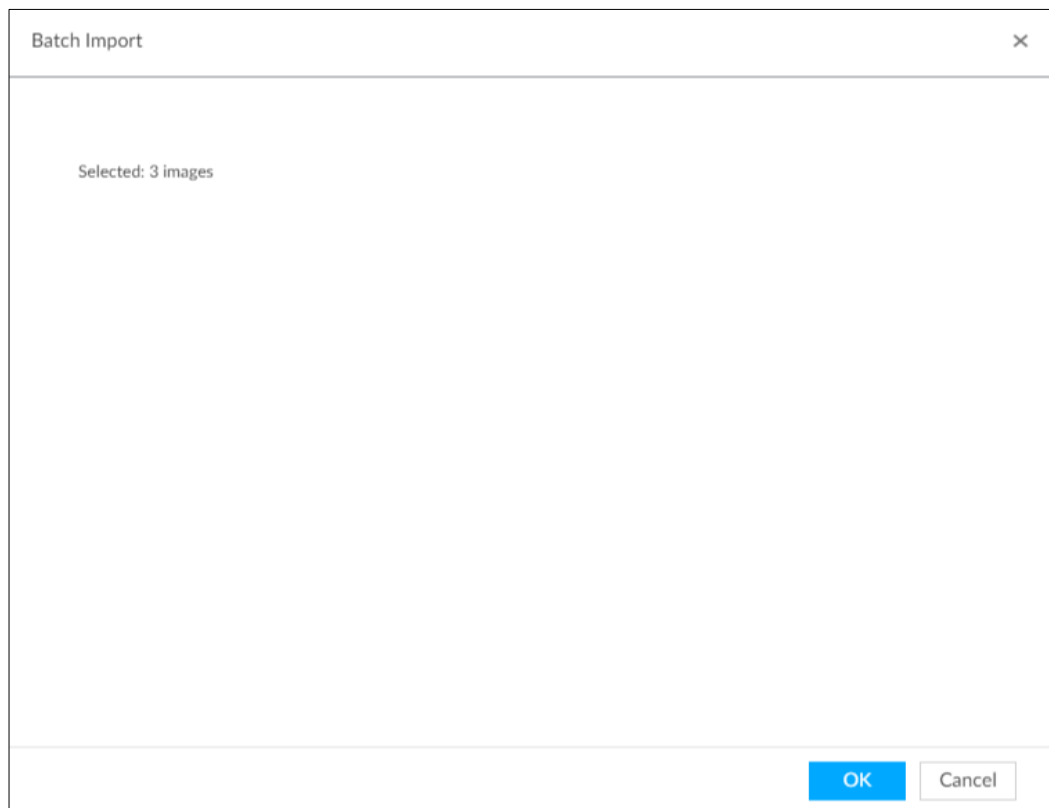
- 1) Click  to select multiple face images.
  - ◇ Press and hold Shift, click any two images, so both images and all images between them can be selected.
  - ◇ Press and hold Ctrl, click multiple face images to select them.
- 2) Click **Open**.

- Upload Folder

- 1) Click  and select the folder where there are face images.
- 2) Click **OK**.

The number of face images is displayed. See Figure 6-14.

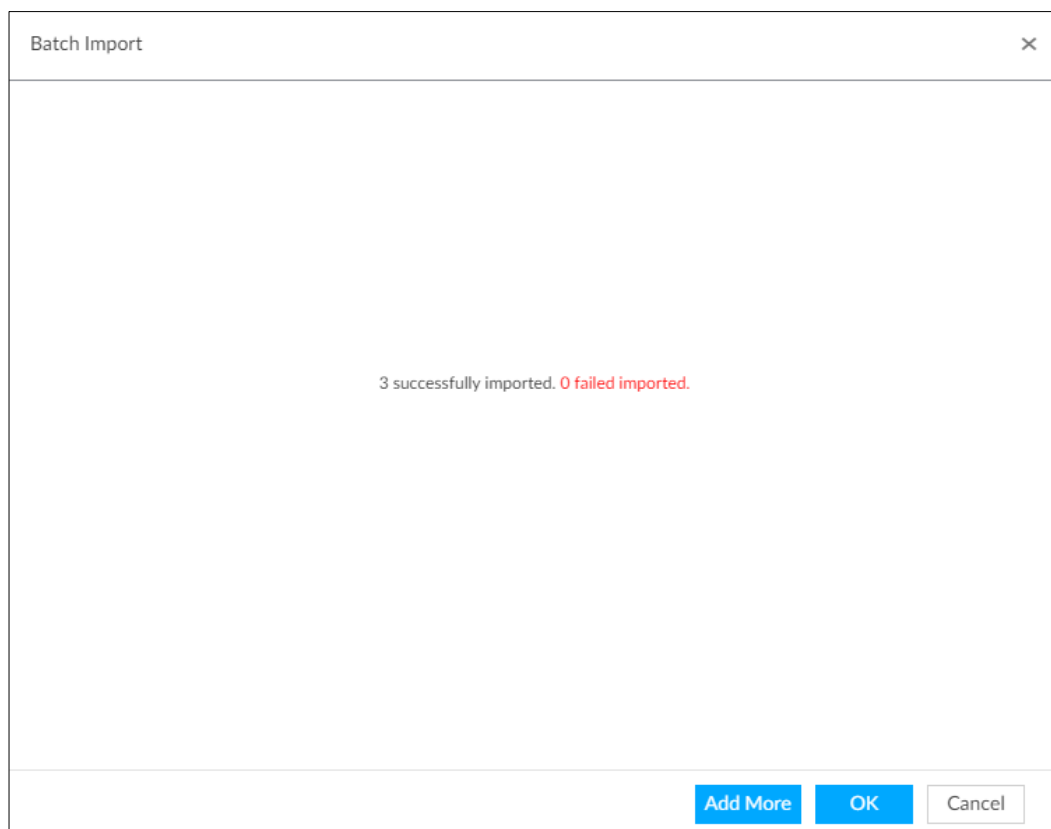
Figure 6-14 Batch import



**Step 5** Click **OK**.

The batch import result interface is displayed. See Figure 6-15.

Figure 6-15 Batch import

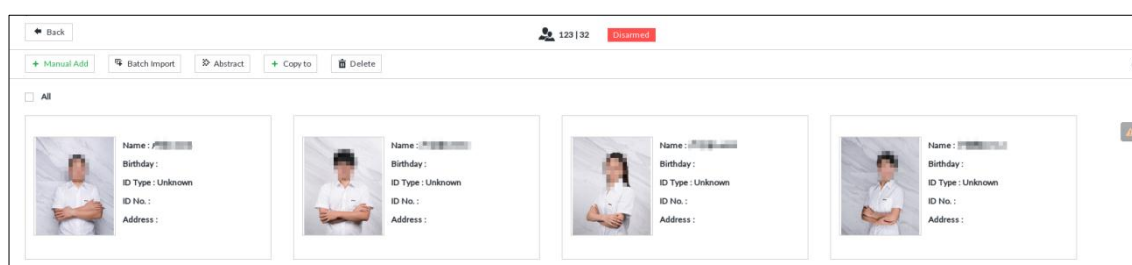


**Step 6** Click **Continue to add** or **OK**.

- Click **Continue to add** to add more images.
- Click **OK** to complete adding images. Face database interface is displayed, and you can see the added images. See Figure 6-16.

After adding the image, at the bottom left corner of the face image, there is an icon. It means device is creating module. Refer to "6.2.2.3 Human Face for detailed information.



Figure 6-16 Face database



### 6.2.2.2.3 Detection Add

You can add snapshots from AI detection to the created face database.

**Step 1** Select face images on the **LIVE** interface.

- Click  or , and move the mouse to the image.
- After opening face detection window, move the mouse to face image in the feature panel.



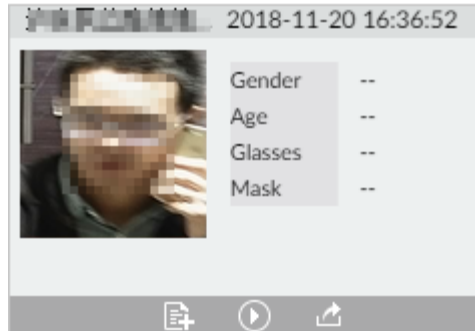
Take adding face detection image for example.

The operation icons are displayed. See Figure 6-17 and Figure 6-18.

Figure 6-17 Face total



Figure 6-18 Operation icon



**Step 2** Click  or .

The Face Register interface is displayed. See Figure 6-19.

Figure 6-19 Face register

The screenshot shows a "Face Register" dialog box with a close button (X) in the top right corner. On the left side, there is a face image of a person wearing glasses. To the right of the image are several form fields: "FaceDB" (a dropdown menu with "Select" selected), "Name" (a text input field), "Gender" (radio buttons for "Male" and "Female", with "Male" selected), "Birthday" (a date picker), "Country or Region" (a dropdown menu), "Address" (a text input field), "ID Type" (a dropdown menu), and "ID No." (a text input field). At the bottom right of the dialog box, there are two buttons: "OK" and "Cancel".

**Step 3** Select the face database, and fill in person information according to your actual situation.

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

## 6.2.2.3 Human Face Abstract

The human face abstracting is to abstract the corresponding information of the face image and import to the database, and then create the human face features module. In this way, device can compare human face, and search human face.



- The greater the face image quantity is, the longer the face abstracting time it takes.
- During the abstracting creation process, some intelligent functions (such as human face comparison, search human face and so on.) are null. These functions become normal after the abstracting process is completed.
- When the uploaded image is half-length photo or full-body photo, the system automatically selects the frame of the uploaded image and only the face area will be retained.

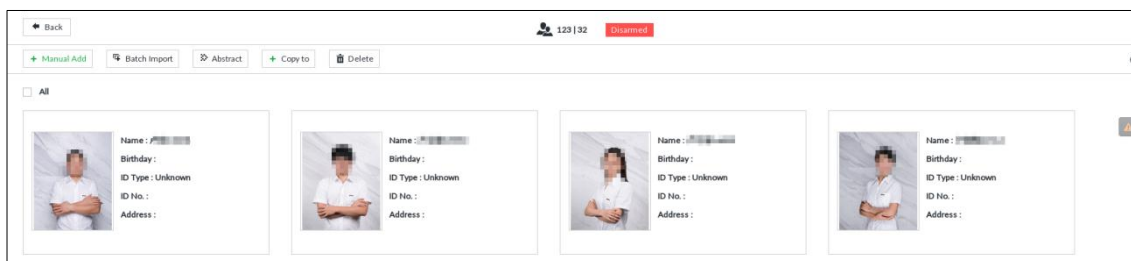
**Step 1** On the **LIVE** interface, click , select **File > Face Database**.

**Face Database** interface is displayed.

**Step 2** Double click face database.

Face database interface is displayed. See Figure 6-20.

Figure 6-20 Face database interface(1)



**Step 3** Select face images and then click **Abstract**.

System pops up a confirmation box. See Figure 6-21.




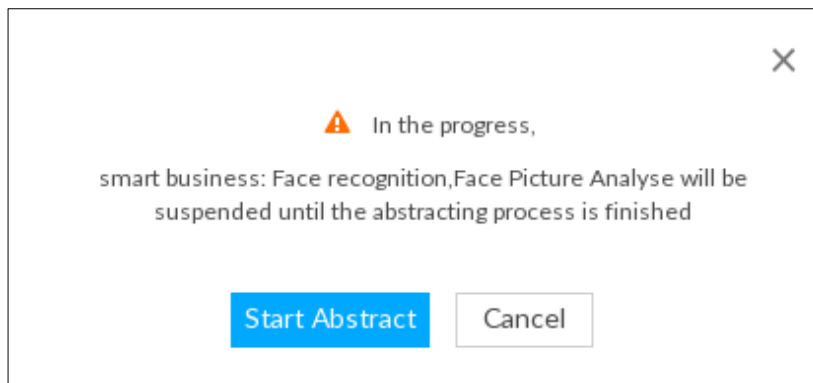
- Select **All** to select all face images in current human face database.
- If there are too many human face images in the human face database, click  to set search conditions (such as name, gender, birthday, country, province, ID type, ID number or abstracting status) to quickly find the human face images.

Figure 6-21 Prompt



**Step 4** Click **Start Abstract**.

Device begins creating module. See Figure 6-22.



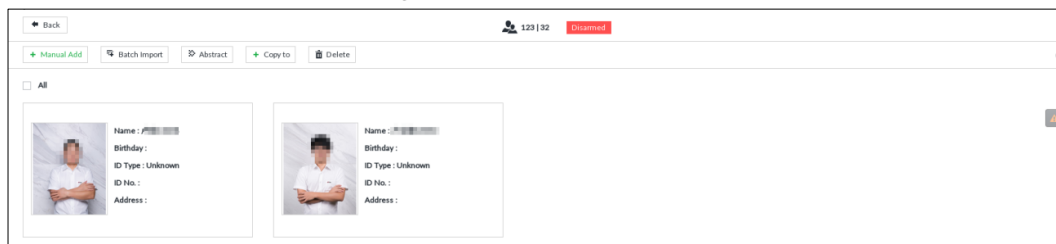


- The abstracting is successful if  is no longer at the bottom left corner of the face image. The abstracting may fail if the face image is not clear or does not contain complete information, and  appears at the bottom left corner of the face image.
- When the uploaded image is half-length photo or full-body photo, the system automatically selects the frame of the uploaded image and only the face area will be retained.

Figure 6-22 Abstract result



## 6.2.3 Configuring Face Detection

You can configure alarm rule of face detection.

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

The **EVENT** interface is displayed.

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

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

The **Face Detection** interface is displayed. See Figure 6-23 or Figure 6-24.

Figure 6-23 AI by camera

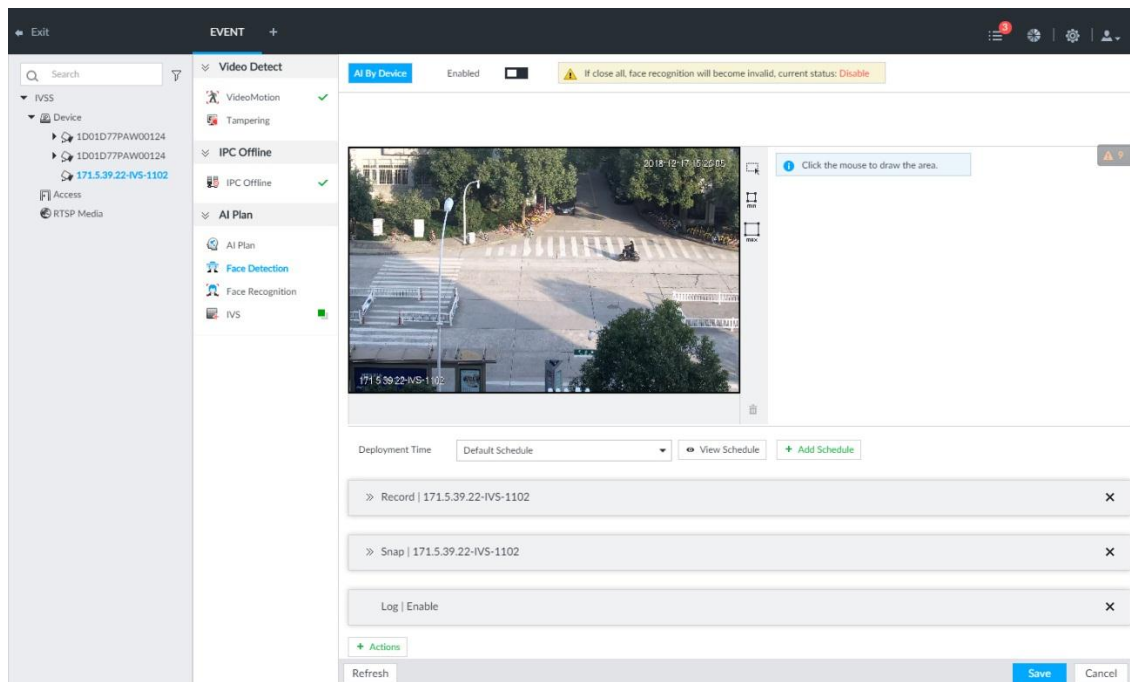
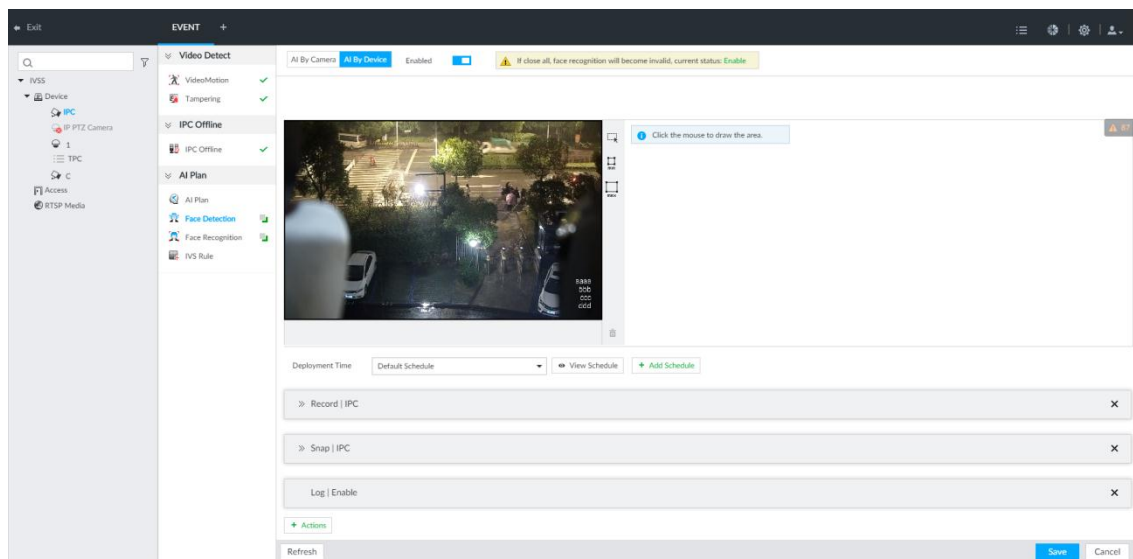



Figure 6-24 Face detection (AI by device)



**Step 4** Click AI by camera or AI by device, and then click  to enable AI function.



AI by camera supports face recognition (FR) function. After enabling FR function, IVSS displays enhanced human face zone on the surveillance window.

**Step 5** Set detection region.



It only supports setting minimum size and maximum size.






1) Click , and set detection region in surveillance window. See Figure 6-25.

Figure 6-25 Area



- Click  or white dot on detect region frame, and drag to adjust its range.
- Click  or  to set human face detection minimum size or maximum size. System triggers an alarm once the detected human size is not larger than the maximum size or smaller than the minimum size.

- Select the motion detect zone you drew. Click  to delete the zone.

2) Click  to complete the settings.

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

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

- Click **View Schedule** to view detailed schedule settings.
- If the schedule is not added or the added schedule does not meet actual needs, click **Add Schedule**. For details, see "8.8.4 Schedule."

Step 7 Click **Action** to set alarm action. For details, see "8.4.1 Alarm Actions."

Step 8 Click **Save**.

## 6.2.4 Configuring Face Recognition

You can configure face recognition alarm rule.

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

The **EVENT** interface is displayed.

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

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

**Face Recognition** interface is displayed. See Figure 6-26 or Figure 6-27.

Figure 6-26 Face recognition

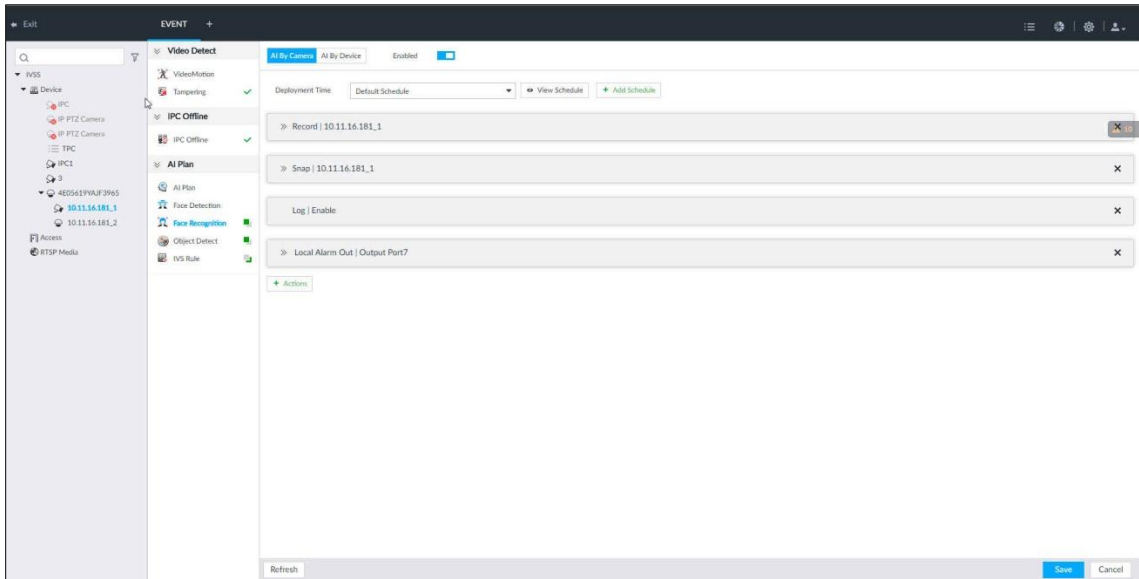
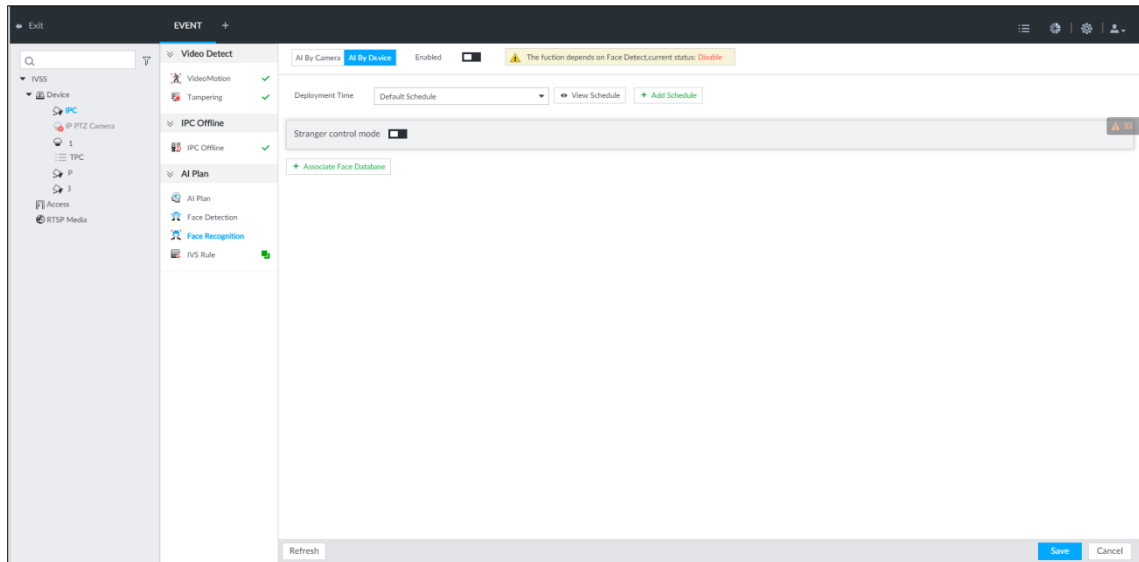


Figure 6-27 Face recognition



**Step 4** Click **AI by Camera** or **AI by Device**, and then click  to enable intelligent function.

**Step 5** Click **Deployment Time** to select schedule from the drop-down list. After setting arm period, system triggers actions when there is a motion detection alarm in the specified period.

- Click **View Schedule** to view detailed schedule settings.
- If the schedule is not added or the added schedule does not meet actual needs, click **Add Schedule**. Refer to "8.8.4 Schedule" for detailed information.

**Step 6** Set stranger mode.

It is to enable stranger mode. Once the face comparison similarity is lower than the specified value, system triggers an alarm.

- 1) Click  to enable stranger mode.

The **Stranger control mode** interface is displayed. See Figure 6-28.




Figure 6-28 Stranger control mode



2) Set parameters. For details, refer to Table 6-4.

Table 6-4 Stranger control mode description

Parameter	Description
AI alarm rule	Click  to set alarm rule box color.
Show feature panel	Check <input checked="" type="checkbox"/> to enable features panel function. System displays stranger panel once there is an alarm.

3) Click **Actions** to set alarm actions. Refer to "8.4.1 Alarm Actions" for detailed information.

Step 7 Set triggered face database.

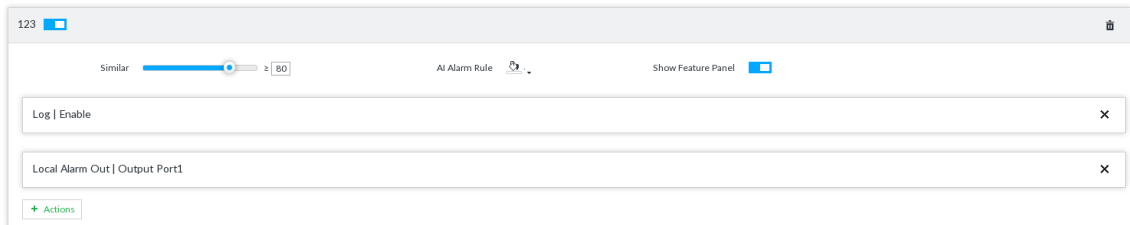


- Before you use AI by camera function, go to the remote device to set face database. At IVSS interface, set alarm activation event.
- Repeat the step to trigger several human databases at the same time.

1) Click **Associate Face Database**, and then select the triggered human face database.


Face database configuration interface is displayed. See Figure 6-29.

Figure 6-29 Face database configuration



2) Set parameters. For details, refer to Table 6-5.

Table 6-5 Configuration description

Parameter	Description
Similar	It is to set human face similarity. System compares the human face with the image on the face database, system triggers an alarm once the similarity reaches threshold you set here.
AI alarm rule	Click  to set alarm rule box color.
Show feature panel	Click <input checked="" type="checkbox"/> to enable features panel function. System displays features panel once there is an alarm.

3) Click **Actions** to set alarm actions. Refer to "8.4.1 Alarm Actions" for detailed information.

Step 8 Click **Save**.

## 6.2.5 Real-time View


You can view real-time face detection and human face comparison images.

### 6.2.5.1 Setting AI Display

You can configure display rule of AI detection results.



Before using this function, ensure that view has been created. Refer to "7.1.1 View Management" for detailed information.

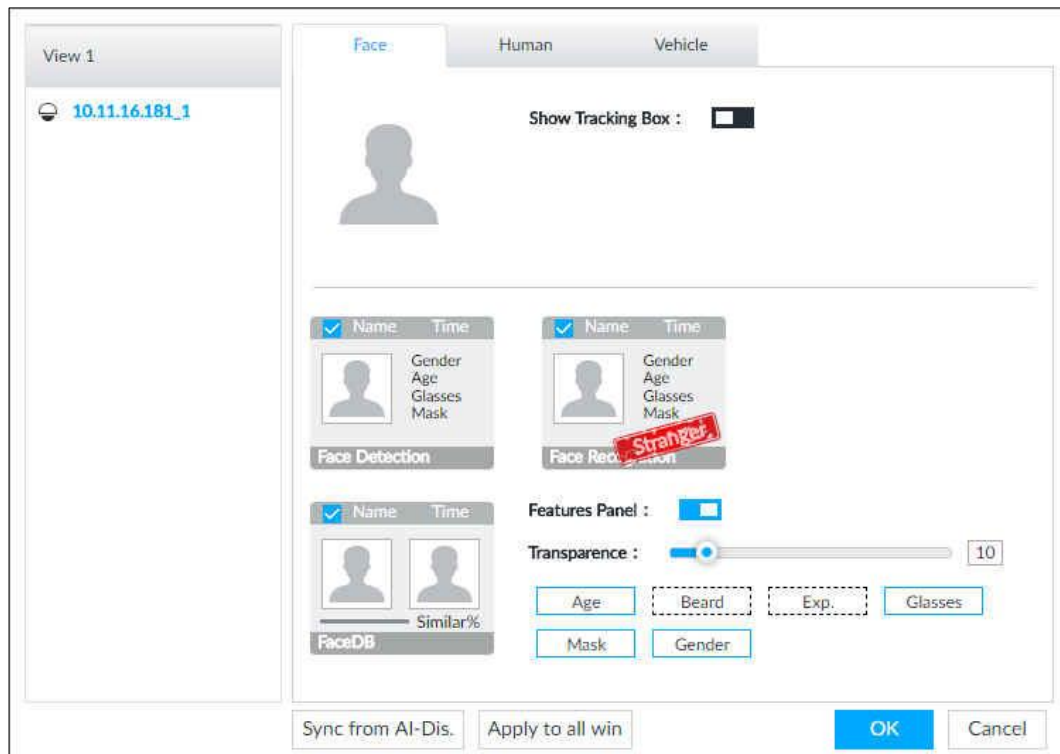
**Step 1** On the **LIVE** interface, click  and select **Face** tab.

The **Face** interface is displayed. See Figure 6-30.



- Click **Sync from AI-Dis.**, obtain global smart detection display rule of IVSS. Refer to "8.4.2.3.2 Setting AI Display" for detailed information.
- Click **Apply to all windows**, it is to copy current configuration to other window(s).

Figure 6-30 Face





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

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

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

After enabling the features panel function, there is a features panel on the right side of the video window.

- Drag  to adjust features panel transparency. The higher the value, the more transparent the features panel.
- System supports maximum 4 features.
- System has checked four features by default. To select other features, cancel the selected features, and then select the ones you need.
- Click  to display the corresponding features panel on the **LIVE** interface, including face detection panel, face recognition panel and face DB panel.

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

## 6.2.5.2 Live

Go to the **LIVE** interface, enable view, device displays view video. See Figure 6-31.

- The view window displays currently detected face rule box.
- The right side displays features panel.
  - ◇ During face detection, features panel displays detection time, the detected face image and feature.
  - ◇ During face comparison, features panel displays detection time, the detected face image, face image in the database, comparison result and database name. After setting stranger mode, when the detected face image mismatches face image in the database, features panel will have Stranger tag.


Figure 6-31 Live




Move the mouse to features panel, and the operation icons are displayed. See Figure 6-32

Figure 6-32 Face database



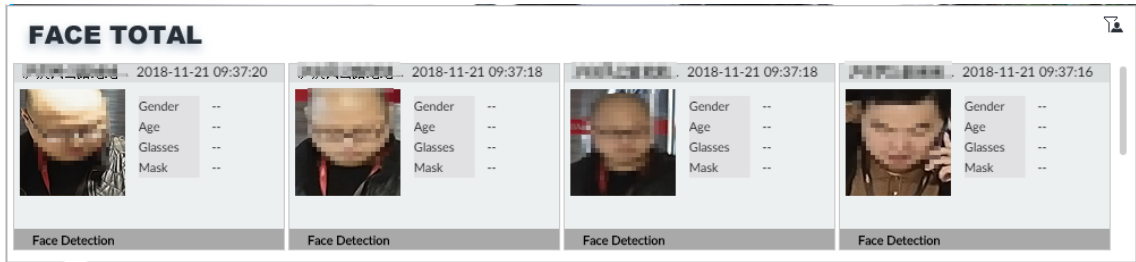
- Click  to add this image to the face database. Refer to "6.2.2.2.3 Detection Add" for detailed information.

- Click  or double click the detected image, so the system starts to play back the recorded videos (about 20s) at the time of snapshot.

### 6.2.5.3 Face Total

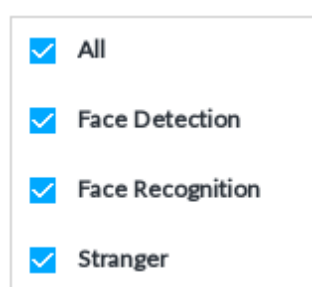
On the **Live** interface, click . Face detection panel is displayed. See Figure 6-33.

Figure 6-33 Detection image (1)



Click  to filter the images. See Figure 6-34.

Figure 6-34 Filter



Move the cursor to features panel, and the operation icons are displayed. See Figure 6-35.

Figure 6-35 Detection image (2)









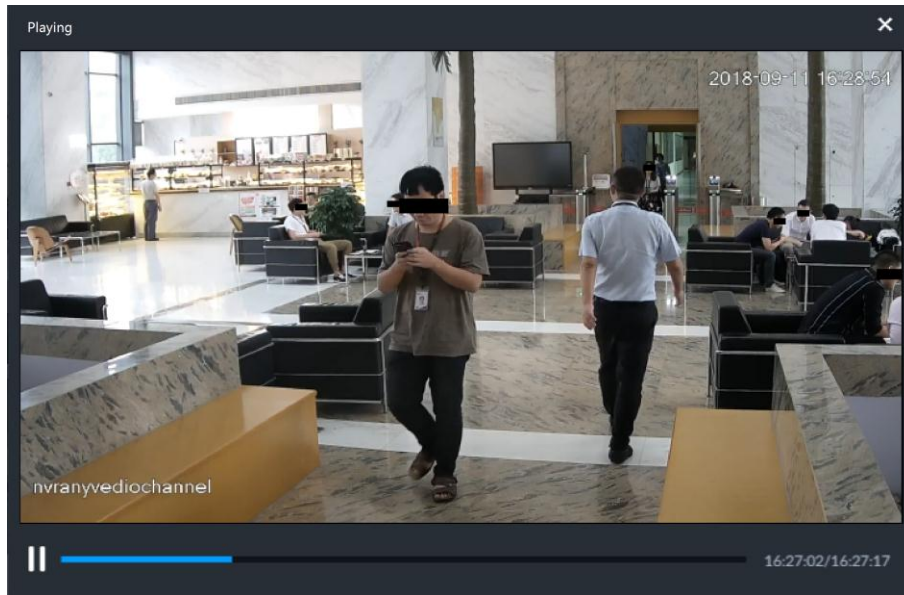

- : Click it to add this image to the face database. Refer to "6.2.2.2.3 Detection Add" for detailed information.
- : click it, or double-click the detected image, IVSS starts to play back the recorded video (10 s before and after the time of snapshot). See Figure 6-36.
  - ◇ Click  to pause play. Now the icon becomes . Click  to play back video again.
  - ◇ Click  to close view window.

Figure 6-36 Record

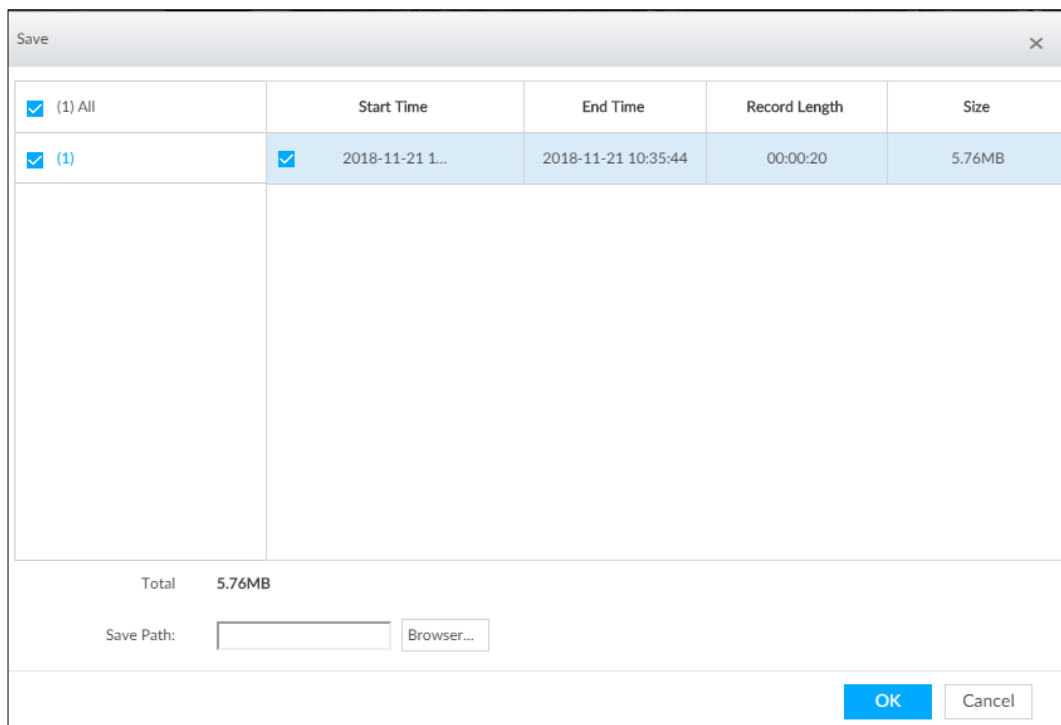


- : Click it, and the **Save** interface is displayed. See Figure 6-37. Click **Browse** to select the storage path, and then click **OK** to export records to the selected path.



Connect USB device to IVSS if you are on the local menu to operate and store the file to USB storage device.

Figure 6-37 Save



## 6.2.6 Face Search

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

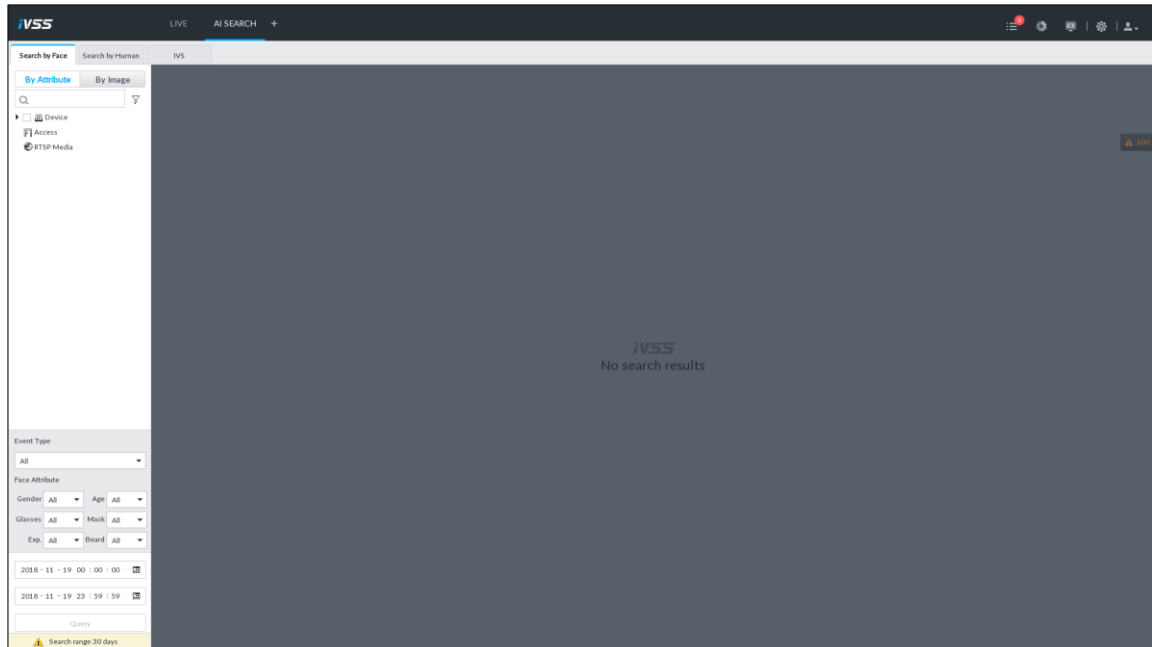
## 6.2.6.1 Search by Attribute

Set event type and attribute, to search qualified face information.

**Step 1** On the **LIVE** interface, click **+**, select **AI Search > Search by Face > By Attribute**.

**By Attribute** interface is displayed. See Figure 6-38.

Figure 6-38 Search by attribute

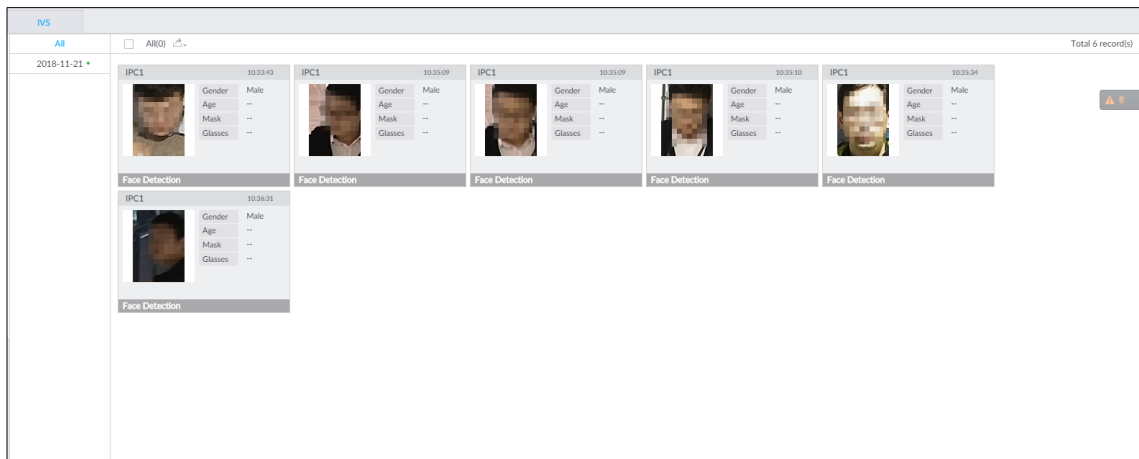


**Step 2** Select the remote device, and set event type, face attribute and time.

**Step 3** Click **Query**.

The search results are displayed in the panel. See Figure 6-39. Click the panel. The operation icons are displayed. See Figure 6-40.

Figure 6-39 Search result



After search, you can play back record, add image to the face database, and export the file. See Figure 6-40 and 0.

Figure 6-40 Icon

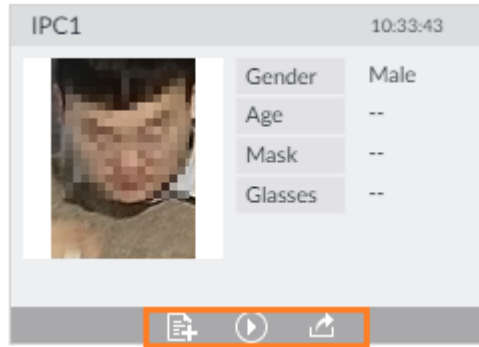













Table 6-6 Search by image

Icon	Operation
	<ul style="list-style-type: none"> <li>Select one by one: Click the panel or move the cursor onto the panel, and then click  to select the panel.  means it is selected.</li> <li>Batch select: Check <b>All</b> to select all panels on the interface.</li> </ul>
	Click  or double-click the panel, the system starts to play back the recorded videos (about 20s).
	Click  to add the image to the face database. Refer to "6.2.2.2.3 Detection Add" for detailed information.
	<p>Click  or select the panel and click  to export images, videos and Excel to designated storage path.</p> <p></p> <p>After setting alarm linkage snapshot, during exporting images, the system exports detected images and panoramic images at the time of snapshot.</p>

## 6.2.6.2 Search by Image

It is to upload face image and then compare with the human face in the record file. Device can filter the record file in which the human face similarity has reached the threshold.

Device supports to use the face image on the face database or the local face.

- When you use face database images to search, ensure face database has been configured. Refer to "6.2.2 Configuring Face Database" for detailed information.
- If you want to use the local images, you need to obtain the face image and saved it in the corresponding path.
  - ◇ When operating on the local interface, save the image in the USB storage device and then connect the USB storage device to the IVSS.
  - ◇ When operating on the Web or IVSS interface, save the image on the PC in which the Web or IVSS client is located.

### 6.2.6.2.1 Device Search

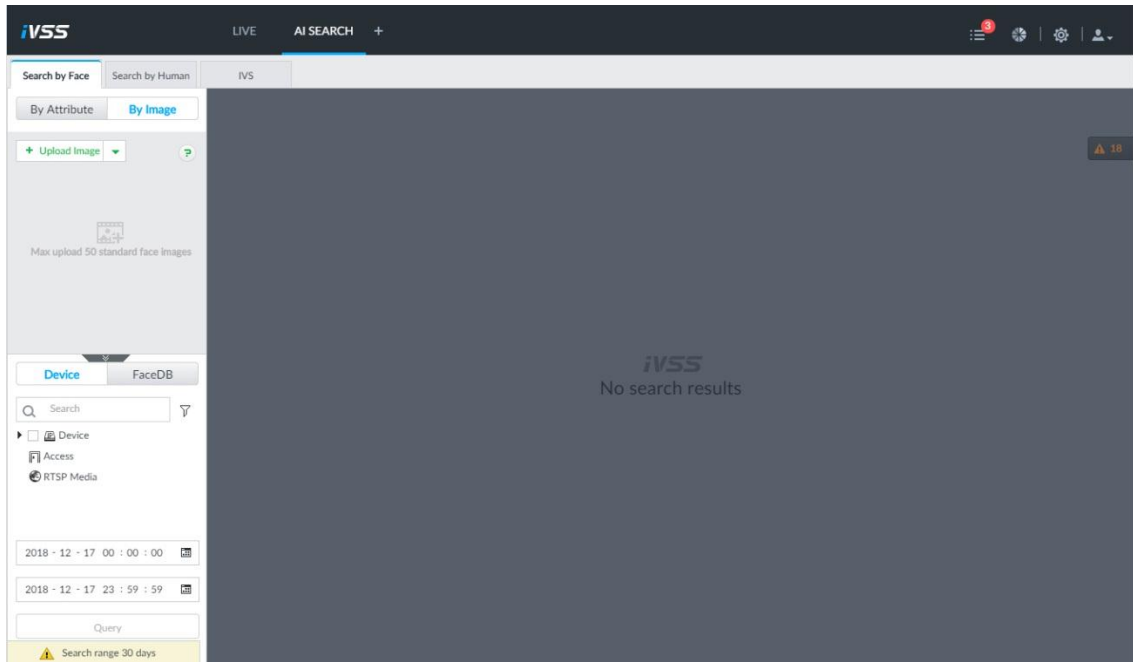
Upload face image, compare it with face detection result of remote device, and find face detection information that meets the set similarity.

Step 1 On **LIVE** interface, click , select **AI Search > Search by Face > By Image**.

The **By Image** interface is displayed. See Figure 6-41.



Figure 6-41 Search by image



**Step 2** Click **Device** tab.

**Step 3** Upload face image.



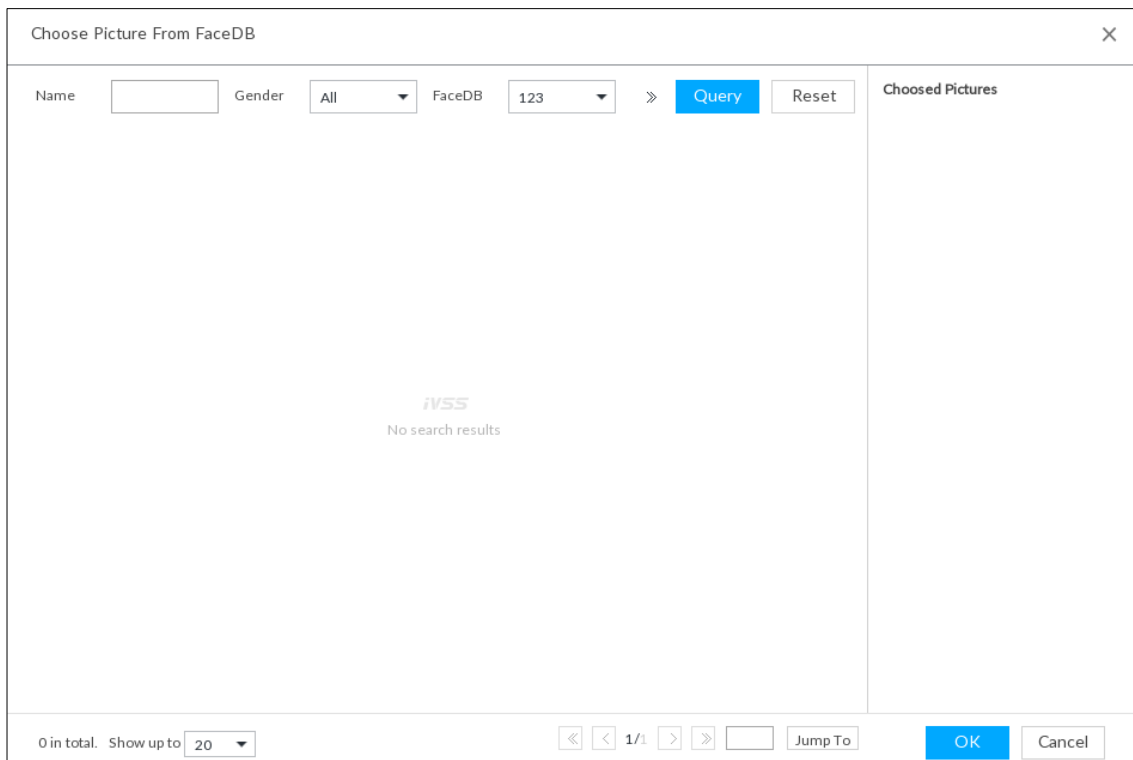
Device supports to upload maximum 50 face images. Device supports to select maximum 10 face images at one time.

- Upload the image from the face image database to search corresponding face.



1) Move the mouse to  and select **Face DB**.

The **Choose Picture From Face DB** interface is displayed. See Figure 6-42.

Figure 6-42 Choose picture from face DB

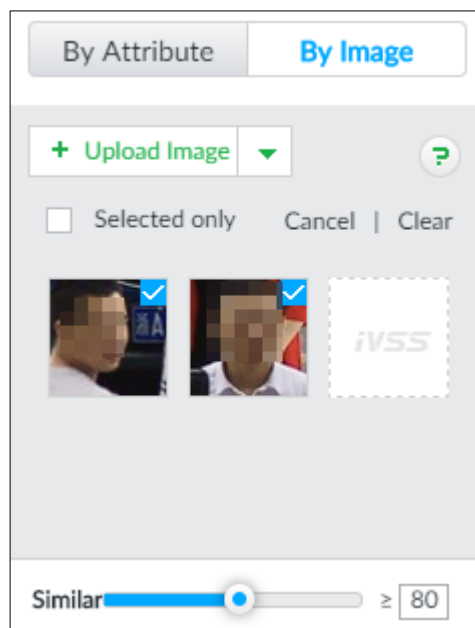


- 2) Select face database and then set search criteria.
    - ◇ If there are too many face images on the database, set name, gender to filter.
    - ◇ Click » to set the search ID number.
  - 3) Click **Query**.  
Device displays the searched face images.
  - 4) Select face image.  
The selected face image is displayed on the **Chosen Pictures** on the right side.
  - 5) Click **OK** to upload face image.
- Local image: Upload images from local PC or USB storage device.

- 1) Move the mouse to  and select **Local**.
- 2) Select face image you want to upload.  
  
You can select several face images at the same time.
- 3) Click **OK** to upload face image.

After uploading the images, device displays the face images on the top left corner. The latest 10 images are selected. See Figure 6-43.

Figure 6-43 By image



- When the uploaded image is half-length photo or full-body photo, the system automatically selects the frame of the uploaded image and only the face area will be retained.
- When there are multiple faces in the uploaded images, the system automatically identifies the faces in the images and uploads multiple face images according to the number of faces recognized.
- Device supports to select maximum 10 face images.
- Click **Cancel** to cancel all checked face images.
- Select **Selected only**, device displays checked human face images only.

- Click **Clear** to clear all uploaded face images.

**Step 4** Hold on and drag  to set human face similarity. It is 80% by default.

**Step 5** Select remote device on the device list and then set record file time period.

**Step 6** Click **Query**.

The Result is displayed. See Figure 6-44 and Table 6-7.

Figure 6-44 Query

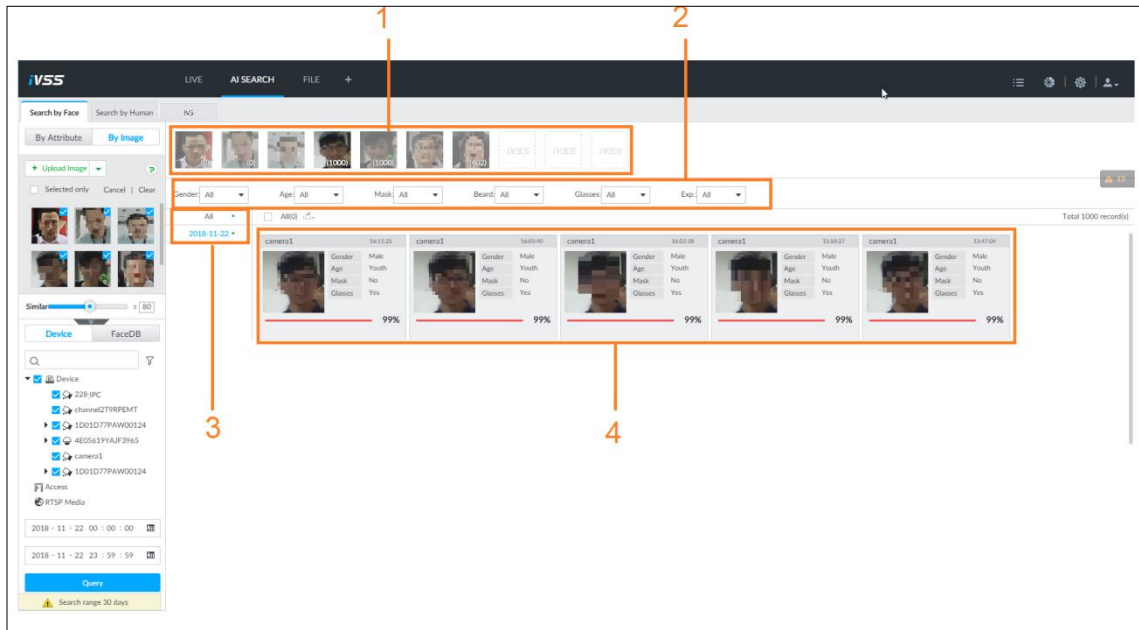


Table 6-7 Device search description




No.	Description
1	Displays selected face images. The number at the bottom right of the face image is to display the searched image amount. Click one image to view its query result.
2	It is to set filter criteria. It can quickly search the required image according to the face features.
3	Displays searched schedule list. Click a date, you can view the image list on current date on the right panel.
4	Displays the searched face panel, including face image, feature attribute and similarity.

## Operation

After query, you can play back video file and export. Refer to Table 6-8 for detailed information.

Table 6-8 Device search operation

Icon	Operation
Select panel	<ul style="list-style-type: none"> <li>• Select one by one: Click the panel or move the mouse onto the panel. Click <input type="checkbox"/> to select the panel. <input checked="" type="checkbox"/> means it is selected.</li> <li>• Batch select: Click <b>All</b> to select all panels on this page.</li> </ul>

Icon	Operation
Playing back recorded video	Double-click the panel to play back recorded video (about 20s).
Export file	<p>Move the mouse to panel and click , or click the panel and click  to export images, videos and Excel to designated storage path. Refer to "6.4 IVS" for detailed information.</p> <p></p> <p>After setting alarm linkage snapshot, during exporting images, the system exports detected images and panoramic images at the time of snapshot.</p>

### 6.2.6.2.2 Searching Face Database

Upload face image, compare it with face image in face database, and find face image that meets the set similarity.

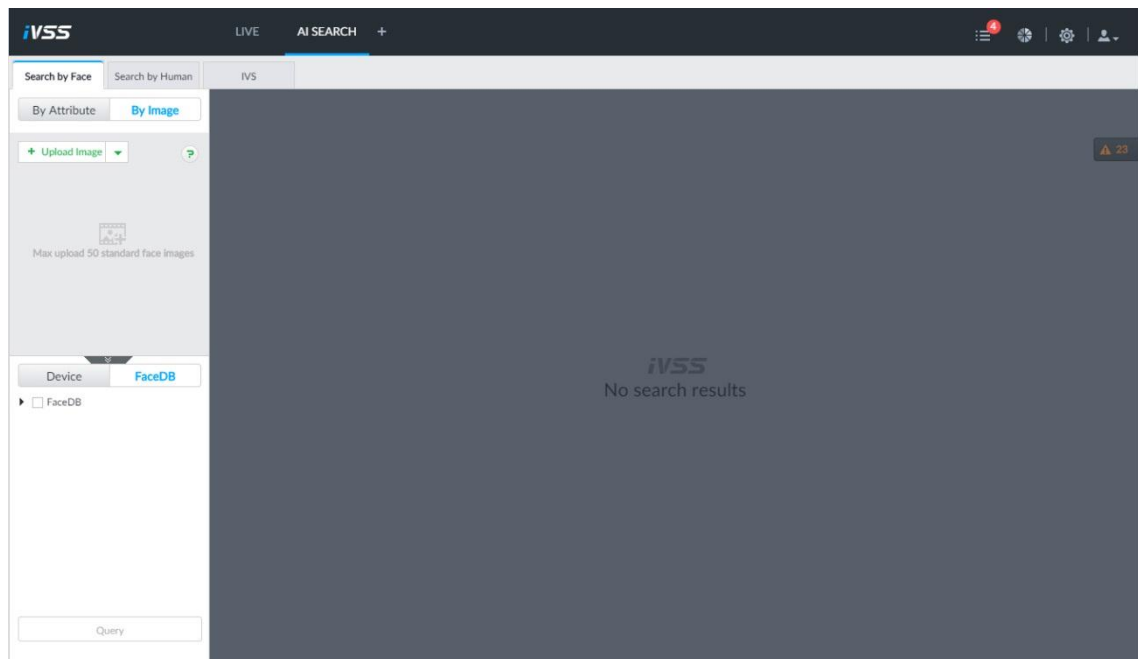
**Step 1** On **Live** interface, click , select **AI Search > Search by Face > By Image**.

The **By Image** interface is displayed.

**Step 2** Click the **FaceDB** tab.

**FaceDB** interface is displayed. See Figure 6-45.

Figure 6-45 Face database



**Step 3** Upload face image. Refer to "6.2.6.2.1 Device Search Step 3" for detailed information.

**Step 4** Hold on and drag  to set human face similarity. It is 80% by default.

**Step 5** Select the face database.

**Step 6** Click **Query**.

The Result is displayed. See Figure 6-46. For details, see Table 6-9.

Figure 6-46 Result

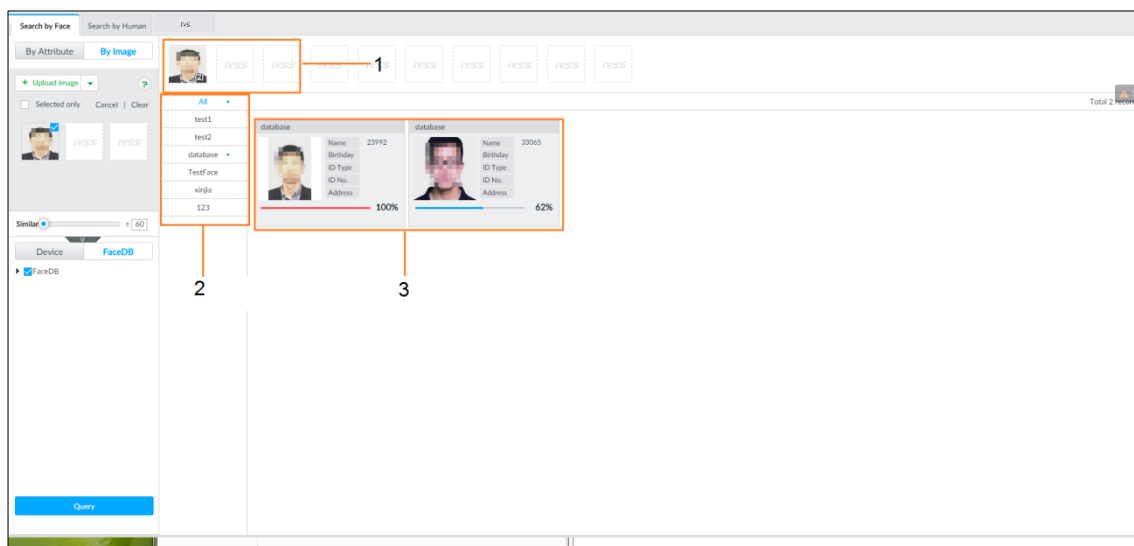



Table 6-9 Description

No.	Description
1	Displays selected face images. The number at the bottom right of the face image is to display the searched image amount. Click one image to view its query result.
2	Displays searched schedule list. Click a date, you can view the image list on current date on the right panel.
3	Displays the searched face panel, including face image, information and similarity.

## Operation

After query, you can play back video file and export. Refer to Table 6-10 for detailed information.

Table 6-10 Face database operation

Name	Operation
Select a panel.	<ul style="list-style-type: none"> <li>Select one by one: Click the panel or move the mouse onto the panel. Click <input type="checkbox"/> to select the panel. <input checked="" type="checkbox"/> means it is selected.</li> <li>Batch select: Check All to select all panels on this page.</li> </ul>
Export File	Click the panel and click  to export images to designated storage path. Refer to "6.4 IVS" for detailed information.

## 6.3 Video Structuring

With video structuring, IVSS can detect, recognize, and extract features from human body, face, motor vehicle, and non-motor vehicle. For example, features such as gender, age, and top color can be extracted from human, and you can then search a certain human face or configure alarm with these features.

## 6.3.1 Enabling AI Plan

You need to enable AI plan when AI by camera is used. Refer to "6.1 Enabling AI Plan" to enable AI detect function.

## 6.3.2 Configuring Video Structuring

After enabling and then configuring video structuring, IVSS can only link the current remote device for taking snapshots when alarm is triggered.



This section takes AI by device for example. AI by camera only supports enabling detection function and setting deployment time.

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

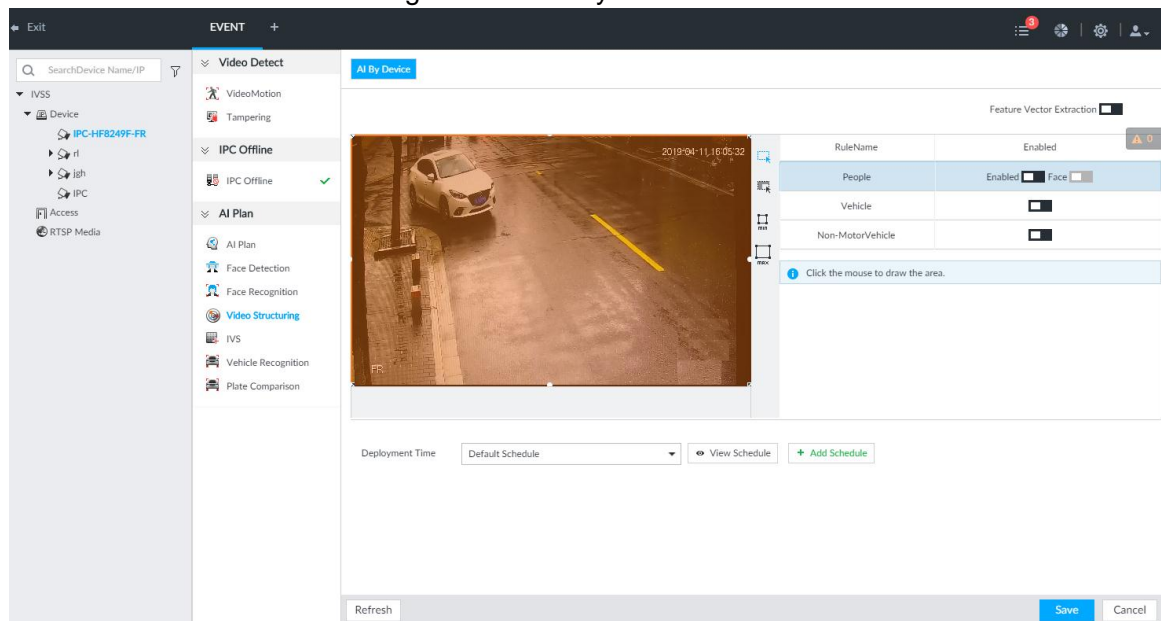
The **EVENT** interface is displayed.

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

**Step 3** Select **AI Plan > Video Structuring > AI By Device**.

The **AI By Device** interface is displayed. See Figure 6-47.

Figure 6-47 AI by device



**Step 4** Click  next to **Feature Vector Extraction** to enable feature extraction, then IVSS can extract features of face and human, such as gender, age, and top color.







Feature vector extraction is available only after **Human** detection is enabled.


**Step 5** Select the detection target.

- People: Click  next to **Enabled** to enable people detection. Face detection can also be enabled at the same time.
- Vehicle: Click corresponding  to enable vehicle detection.


- Non-Motor Vehicle: Click corresponding  to enable non-motor vehicle detection.



Step 6 Click  (the icon changes to ) , then you can configure detection area (orange) in the video image. See Figure 6-48.

- Click any white dot on the frame, and the dot changes to . Drag  to adjust the detection area.

Click  to draw an excluded area which will not be detected. IVSS does not detect target within the excluded area.

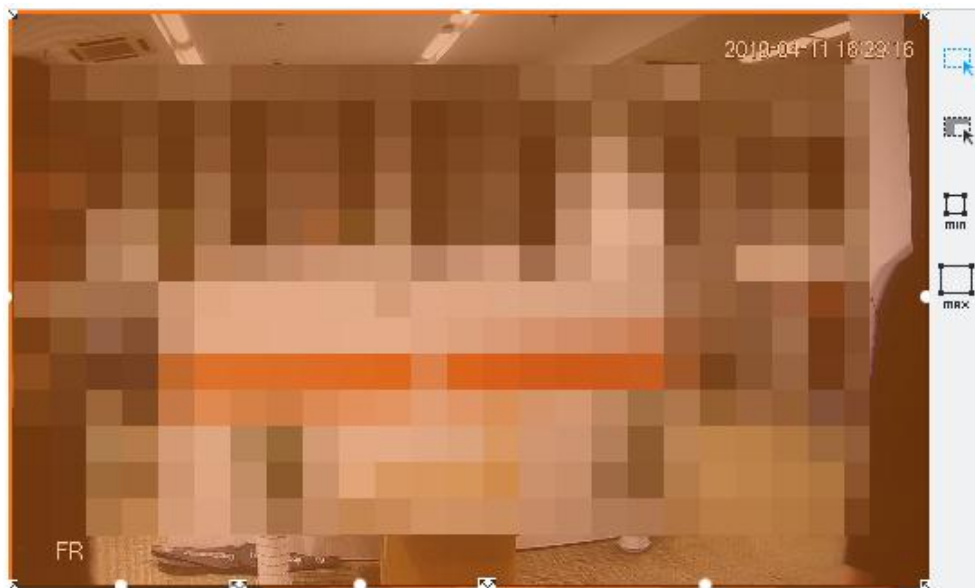
◇ Up to 4 excluded areas can be drawn.

◇ To delete an excluded area, select the area, and then click .

- Click  or  to set the minimum size or maximum size of detection target.

Alarm will be triggered when the size of detection target is within the minimum and maximum sizes.

Figure 6-48 Detection area



Step 7 Click **Deployment Time** dropdown list to select schedule. IVSS links alarm event when an alarm is triggered within the schedule configured.

- Click **Add Schedule** to add new schedule if no schedule is added or the existing schedule does not meet requirements. For details, see "8.8.4 Schedule."
- Click **View Schedule** to view details of schedule.

Step 8 Click **Save**.

### 6.3.3 Live

You can view the detected features and properties of face, people, motor vehicle and non-motor vehicle on the **LIVE** interface.


### 6.3.3.1 Setting AI Display

You can set the features and properties that you want to display in the real-time video image of the **LIVE** interface.



Before setting the features and properties, you need to create a view by adding cameras to the view so you can check video and pictures captured by the cameras. For details of creating a view, see "7.1.1 View Management."

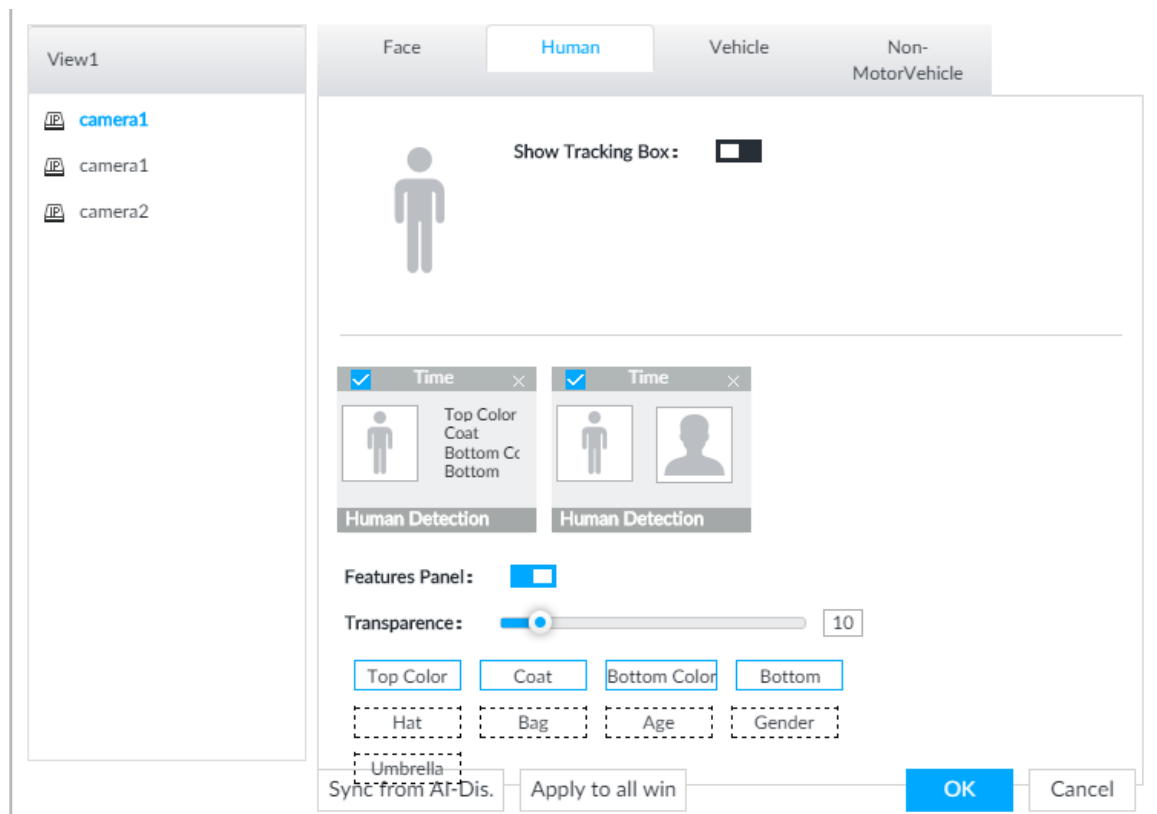
**Step 1** Select a view from **Live > View > View Group**.

**Step 2** Click  at the lower side of the **LIVE** interface, and then select **Human**, **Vehicle** or **Non-Motor Vehicle**. See Figure 6-49.



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

Figure 6-49 Human



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


**Step 4** Configure feature panel.

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

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

2) Select the target you want to detect. You can select from Face, Human, Vehicle, and Non-Vehicle Motor.



- 3) (Optional) Drag  to adjust the transparency of panel. The higher the value, the more transparent the panel.
- 4) (Optional) Select the features to be displayed in the panel.
  - Up to 4 features can be displayed.
  - 4 features are selected by default. To select another feature, click the selected feature to cancel it, and then click the feature to be displayed.

Step 5 Click **OK**.

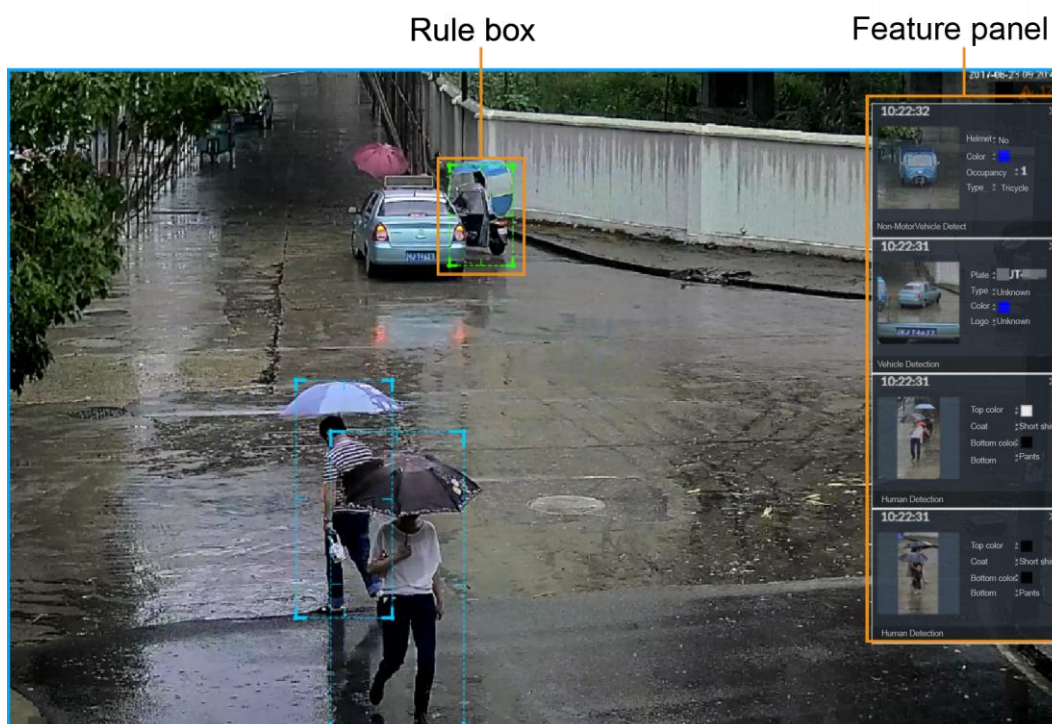
### 6.3.3.2 Real-time View

You can view the detected features and properties of face, people, motor vehicle and non-motor vehicle in the real-time video image.

On the **LIVE** interface, select a view from View Group, and the video image of the view will be displayed. See Figure 6-50.

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

Figure 6-50 Live



Move the cursor to the features panel, and the icons are displayed. See Figure 6-51 or Figure 6-52.

Figure 6-51 Icons (vehicle detection)

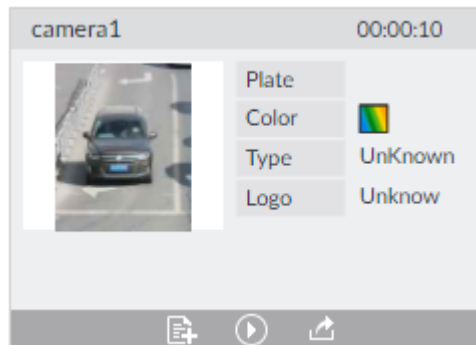
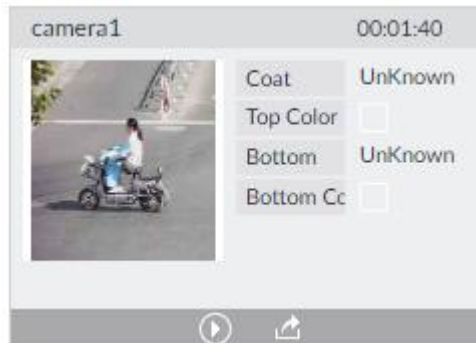




Figure 6-52 Icons (other detection)



- Click  to add plate information to plate database.
- Click , or double-click the detected image to play back the video record (10 s before and after the time of snapshot).

### 6.3.3.3 Detection statistics

You can view the features and properties of detected human body, face, motor vehicle and non-motor vehicle.

#### 6.3.3.3.1 Human

You can view the features and properties of detected human body and face.

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


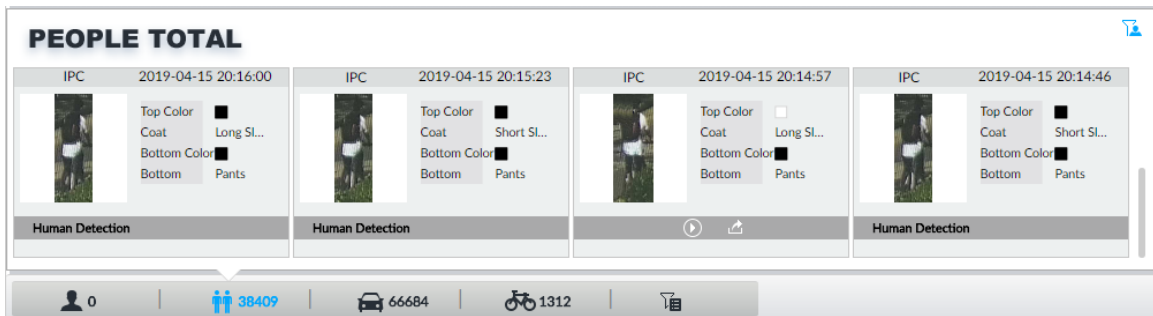


Click , and then select **Snap With Face** and **Snap Without Face**. The information of detected human and face is displayed. See Figure 6-53.



Figure 6-53 Human detection




Move the cursor to a panel, and the following icons are displayed:

- : Click it to add the face image to face database. For details, see "6.2.2.2.3 Detection Add."
 



This function is available when face image is captured.
- : Click it, or double-click detected picture to play back the video record (10 s before and after the time of snapshot).
- : Click it to export the video record to specified save path (PC or USB storage device).
 



If store the video record to USB storage device, make sure the device is connected.

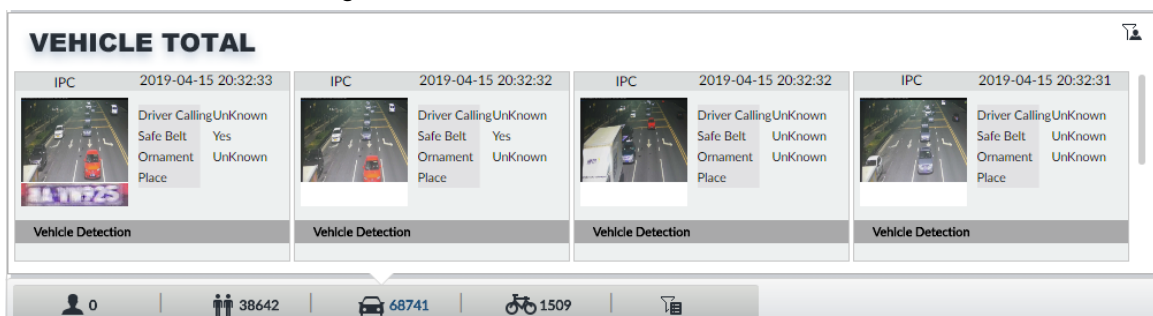
### 6.3.3.3.2 Motor Vehicle

You can view the features and properties of detected motor vehicles.



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

Click , and then select **Vehicle Recognition**, the information of detected vehicles is displayed. See Figure 6-54.


Figure 6-54 Motor vehicle detection



Move the cursor to a panel, and the following icons are displayed:

- : Click it to add the license plate image to plate database. For details, see "6.6.3.2.3 Add by Searching."
- : Click it, or double-click detected picture to play back the video record (10 s before and

after the time of taking the snapshot).

- : Click it to export the video record to specified save path (PC or USB storage device).



If store the video record to USB storage device, make sure the device is connected.

### 6.3.3.3 Non-motor Vehicle

You can view the features and properties of detected non-motor vehicles.

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


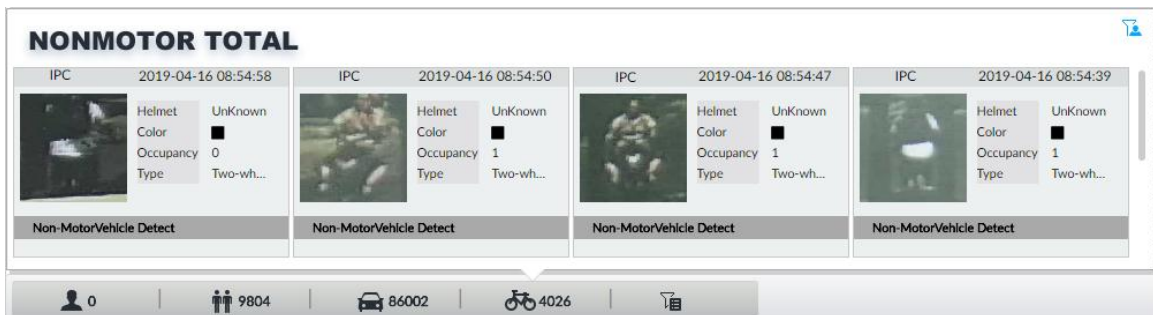


Click , and then select **Snap With Face** and **Snap Without Face**. The detected non-motor vehicle features and properties are displayed. See Figure 6-55.

Figure 6-55 Non-motor vehicle detection



Move the cursor to the panel, and the following icons are displayed:

- : Click it, or double-click the detected image to play back the video record (10 s before and after the time of taking the snapshot).
- : Click it to export the video record to specified save path.




Make sure USB storage device is inserted during local operation.

## 6.3.4 AI Search

Select device and set properties to search detection results. For example, you can set human properties such as gender, age, top, pants, and search human with these properties.

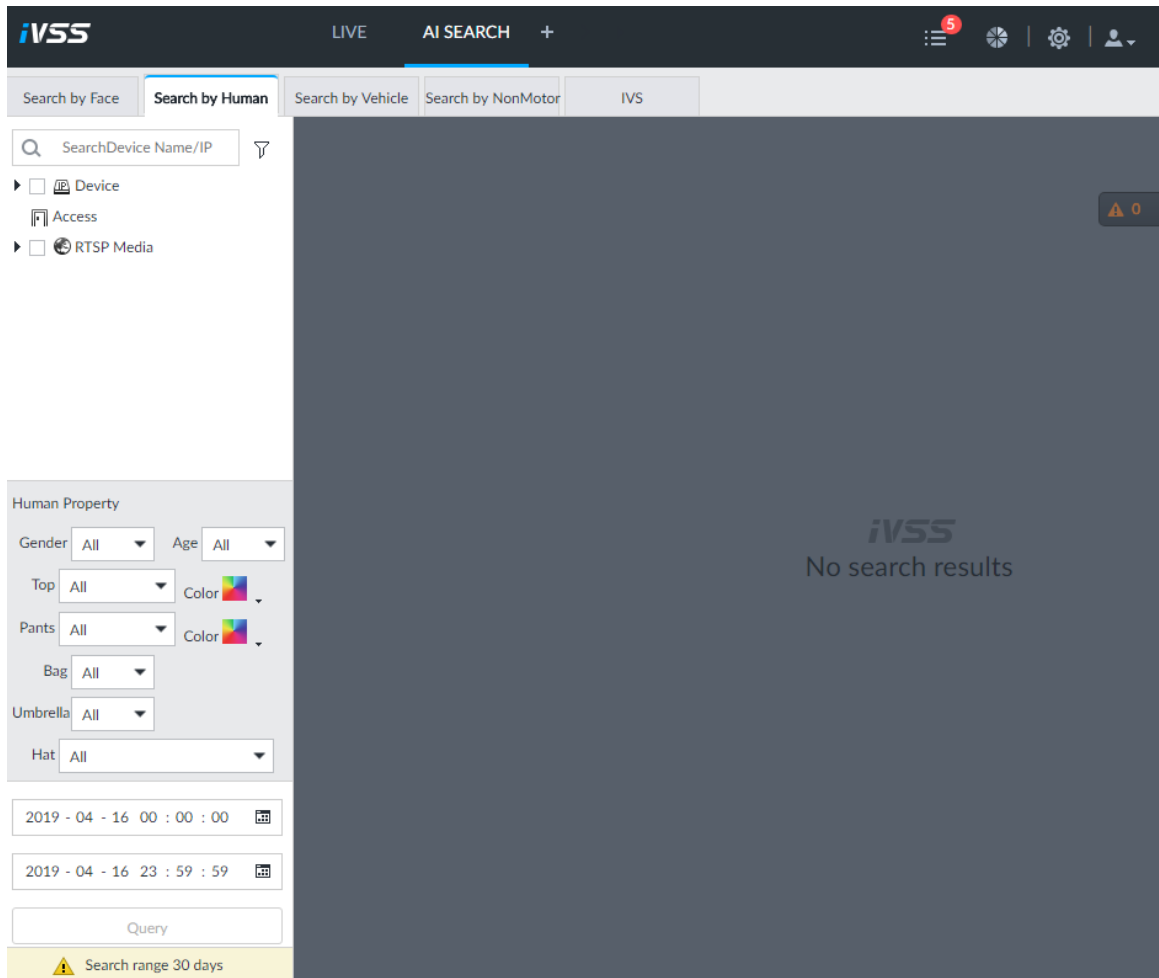
### 6.3.4.1 Search by Human

Select device, and set human properties and features, so you can search human with the defined properties and features.

Step 1 On the **LIVE** interface, click , and then select **AI SEARCH > Search by Human**.

The **Search by Human** interface is displayed. See Figure 6-56.

Figure 6-56 Search by human



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

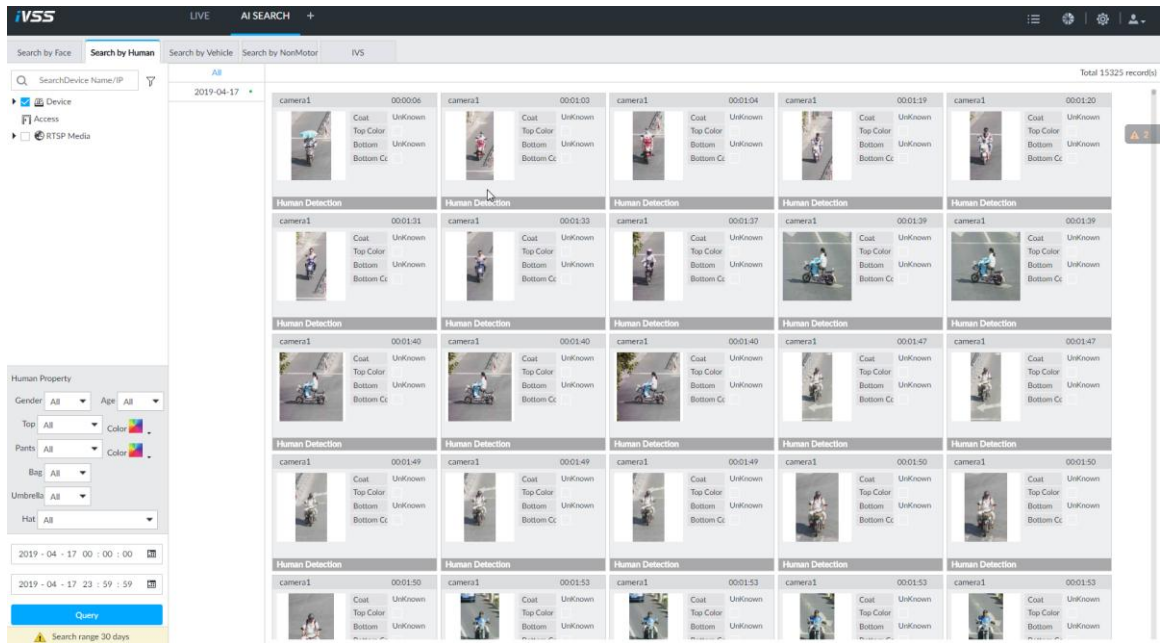
Click  or  to set the color.  means more than one color.

**Step 3** Click **Query**.

The search result is displayed. See Figure 6-57.

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

Figure 6-57 Search result



## Other Operations

Click on one displayed panel, and the icons are displayed. See Figure 6-58 or Figure 6-59. For details, see Table 6-11.

Figure 6-58 Icons (1)

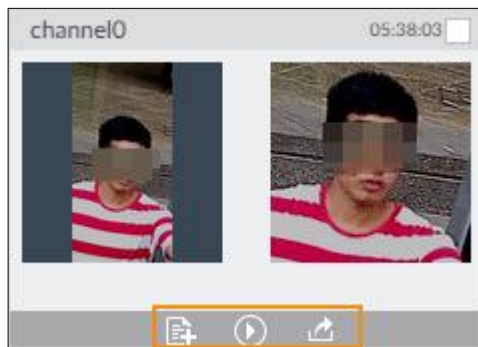


Figure 6-59 Icons (2)

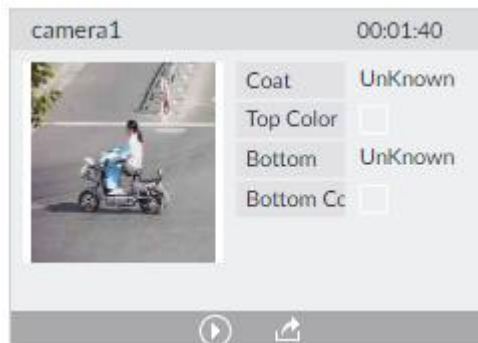













Table 6-11 Operation

Icon	Operation
------	-----------

Icon	Operation
	<ul style="list-style-type: none"> <li>Select one by one: Click  to select the panel.  means the panel is selected.</li> <li>Select in batches: Select <b>All</b> to select all the panels on the interface.</li> </ul>
	Click  or double-click the panel to play back the video record (10 s before and after the time of taking the snapshot).
	Click  to add picture to database. See "6.2.2.2.3 Detection Add."
	Click  , or select the panel and then click  to export picture, video, and Excel file to specified save path.

### 6.3.4.2 Search by Vehicle

Set event type and vehicle properties to search vehicle detection results. For example, you can set vehicle properties such as type, logo, plate, and search vehicles with these properties.

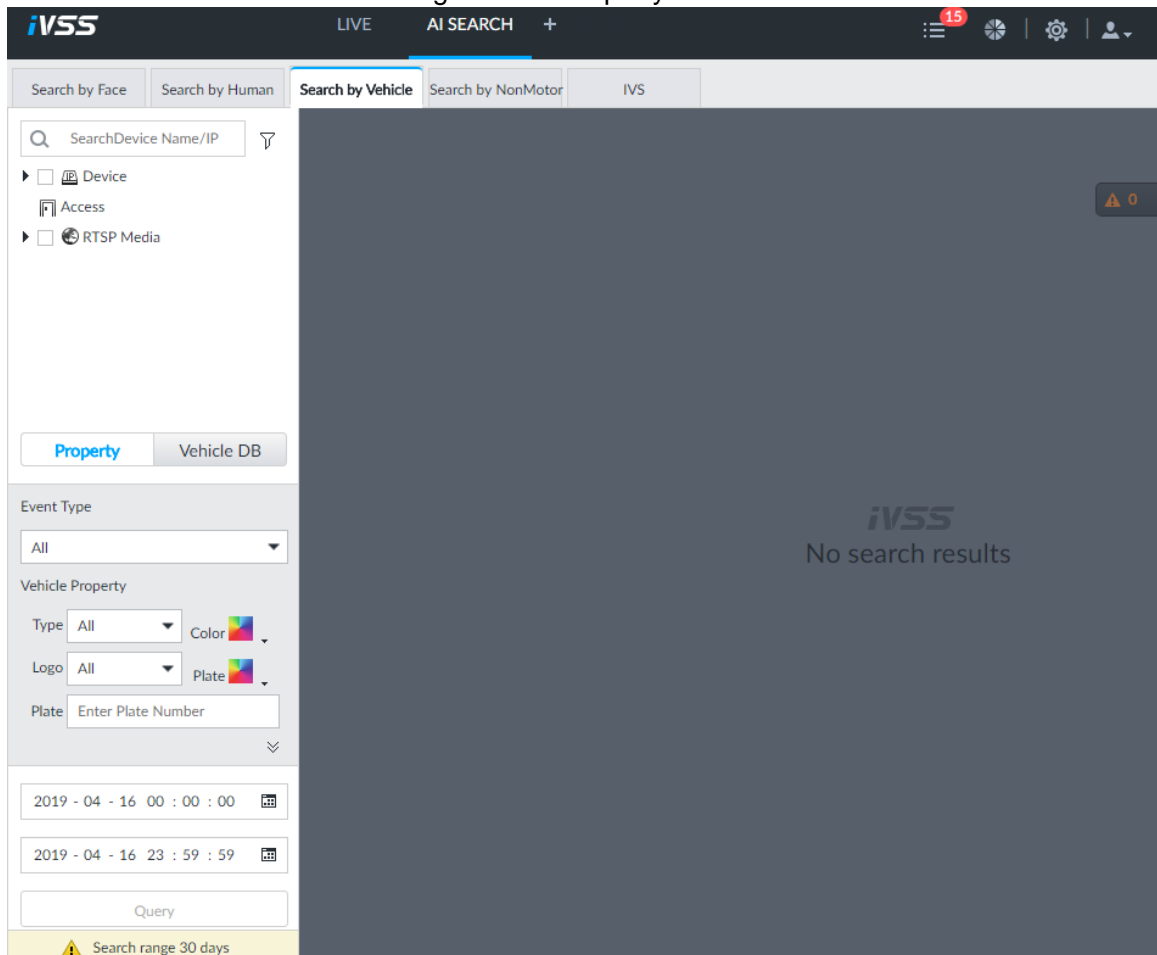
Step 1 On the **LIVE** interface, click , and then select **AI SEARCH > Search by Vehicle**.

The **Search by Vehicle** interface is displayed.

Step 2 Select device, and then click **Property** tab.

The **Property** interface is displayed. See Figure 6-60.

Figure 6-60 Property



**Step 3** Select **Vehicle Detection** as **Event Type**.

**Step 4** Set vehicle properties and time period.

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

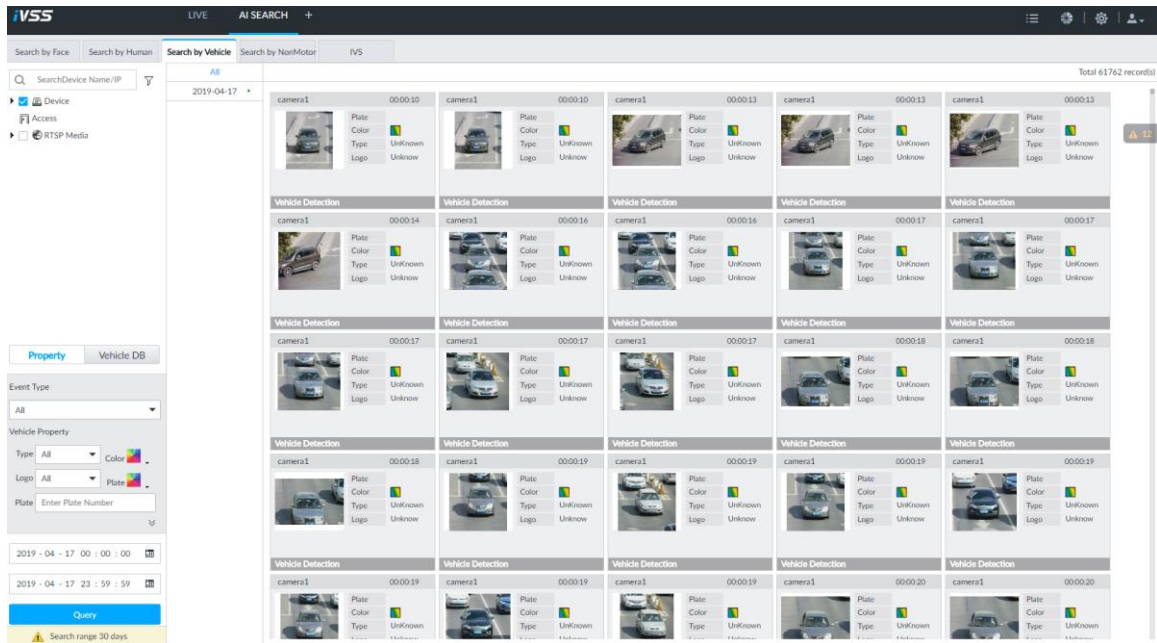
**Step 5** Click **Query**.

The search result is displayed. See Figure 6-61.

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



Figure 6-61 Search result



## Other Operations

Click on one displayed panel, and the icons are displayed. See Figure 6-62 and Table 6-12.

Figure 6-62 Icons

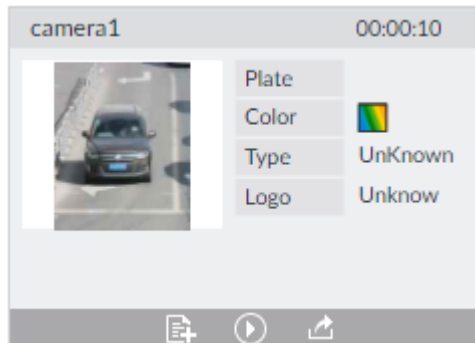



Table 6-12 Operation

Icon	Operation
	<ul style="list-style-type: none"> <li>Select one by one: Click  to select the panel. <input checked="" type="checkbox"/> means the panel is selected.</li> <li>Select in batches: Select <b>All</b> to select all the panels on the interface.</li> </ul>
	Click  or double-click the panel to play back the video record (10 s before and after the time of taking the snapshot).
	Click  to add picture to database. See "6.2.2.2.3 Detection Add."
	Click , or select the panel and then click  to export picture, video, and Excel file to specified save path.

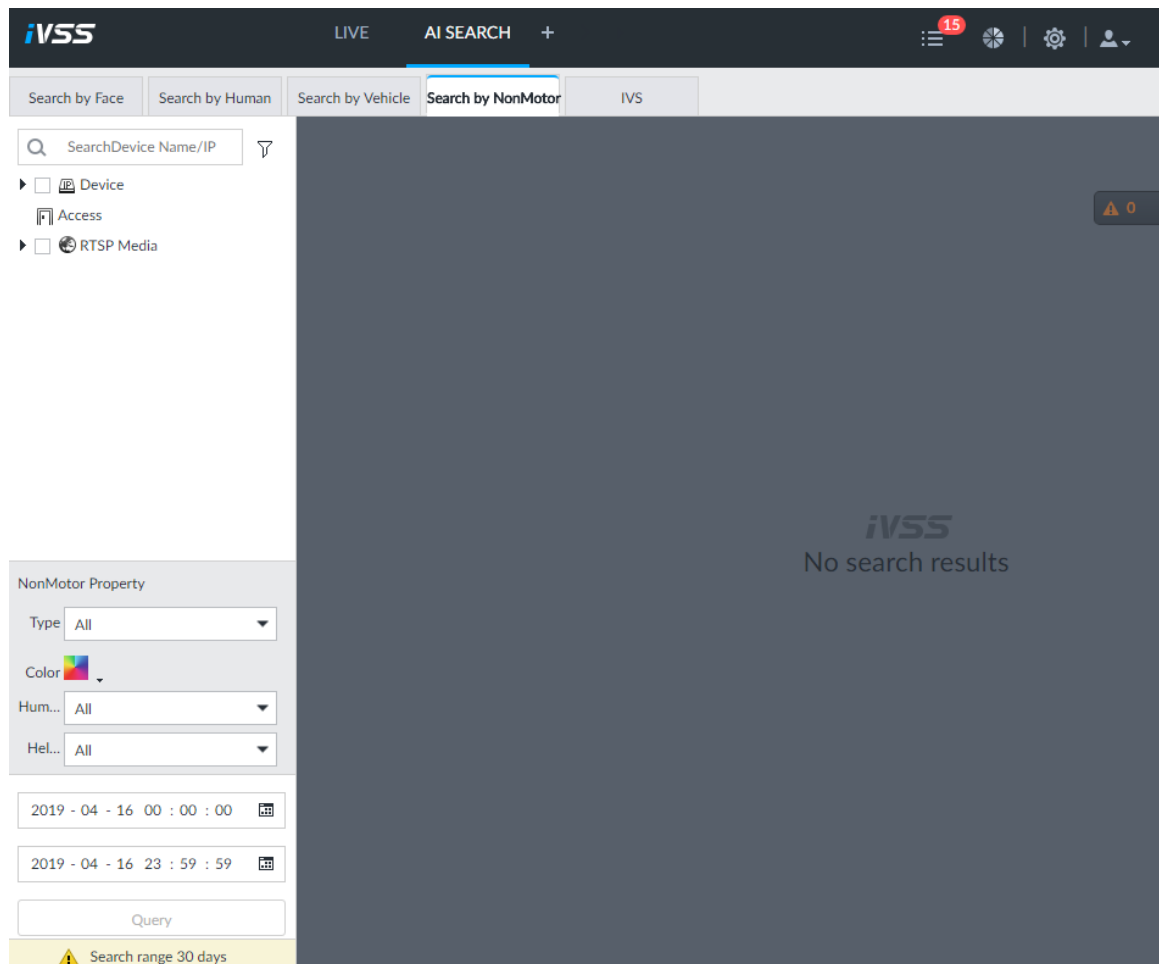
### 6.3.4.3 Search by Non-motor Vehicle

Set event type and non-motor vehicle properties to search non-motor vehicle detection results. For example, you can set non-motor vehicle properties such as type, color, helmet, and search non-motor vehicles with these properties.

**Step 1** On the **LIVE** interface, click , and then select **AI SEARCH > Search by NonMotor**.

The **Search by NonMotor** interface is displayed. See Figure 6-63.

Figure 6-63 Search by non-motor vehicle



**Step 2** Select the device you want to search.

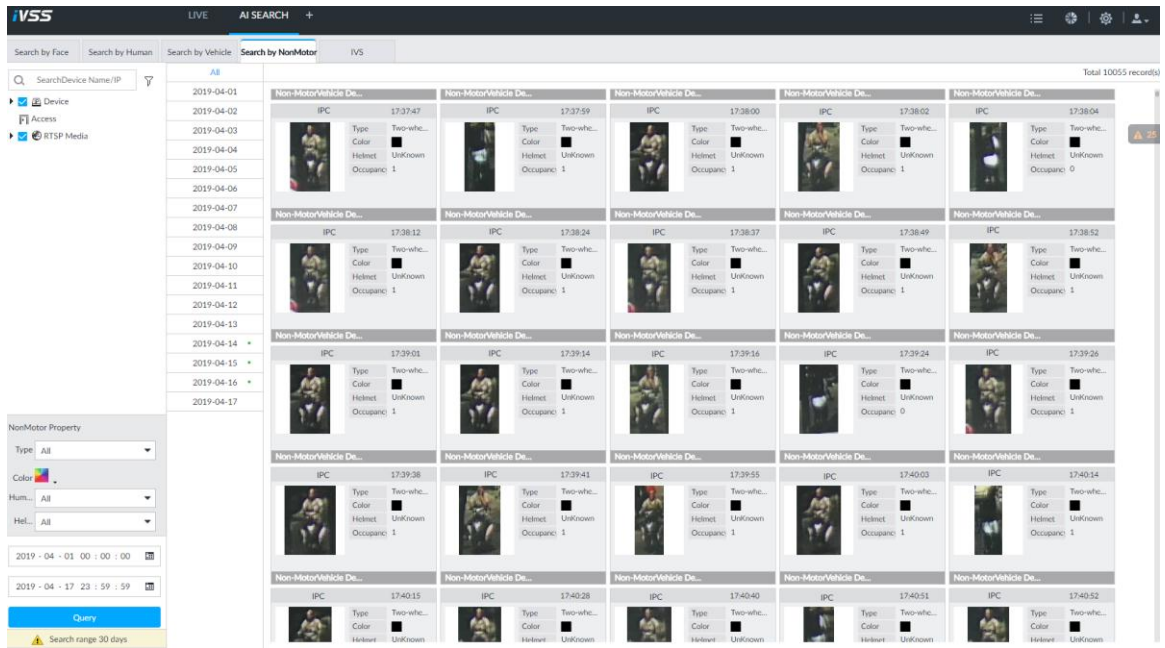
**Step 3** Set non-motor vehicle properties and time period.

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

**Step 4** Click **Query**.

The search result is displayed. See Figure 6-64.

Figure 6-64 Search result



## Other Operations

Click on one displayed panel, and the icons are displayed. See Figure 6-65 and Table 6-13.

Figure 6-65 Icons

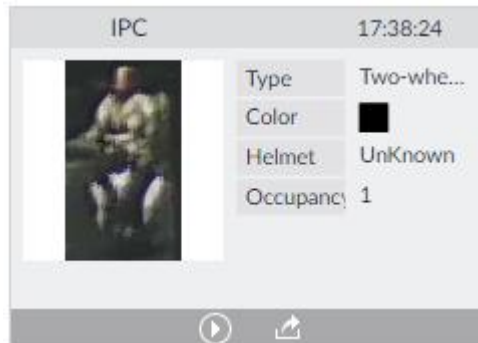


Table 6-13 Operation

Icon	Operation
	<ul style="list-style-type: none"> <li>Select one by one: Click  to select the panel. <input checked="" type="checkbox"/> means the panel is selected.</li> <li>Select in batches: Select <b>All</b> to select all the panels on the interface.</li> </ul>
	Click  or double-click the panel to play back the video record (10 s before and after the time of taking the snapshot).
	Click  to add picture to database. See "6.2.2.2.3 Detection Add."
	Click , or select the panel and then click  to export picture, video, and Excel file to specified save path.

## 6.4 IVS

With IVS function, IVSS processes and analyzes images, extracts key information from video records, compares the key information with the predefined detection rule, and triggers alarm once the detected behavior matches the detection rule.

IVS type includes cross line detection and cross region detection.



IVS and face detection function of the same camera cannot be used at the same time.

IVS scene requirement is as follows:

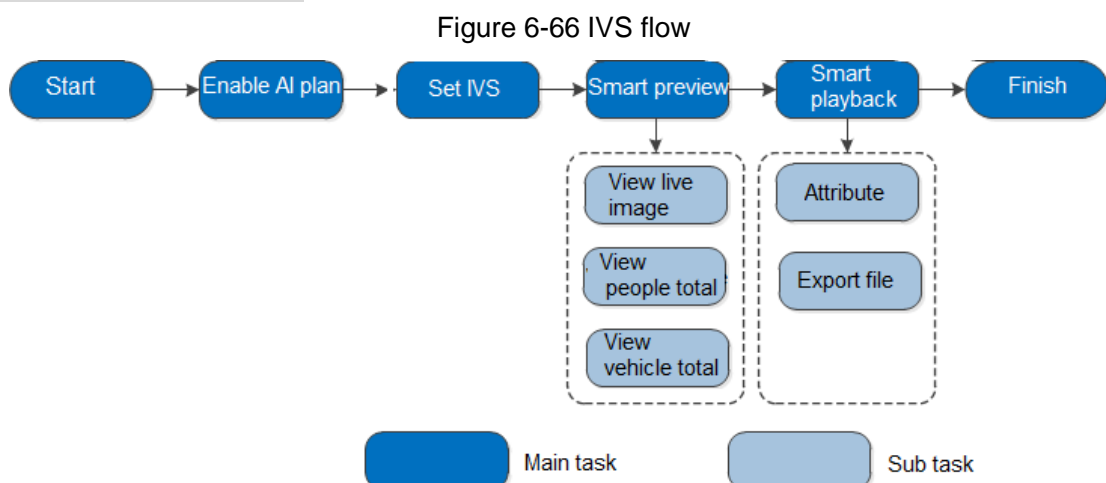
- Total area of the target does not exceed 10% of the image.
- Target size in the image shall not be less than 10 pixels × 10 pixels, and leftover target size shall not be less than 15 pixels × 15 pixels (CIF image). Target height and width shall not exceed 1/3 height and width of the image. It is suggested that target height should be 10% of image height.
- Brightness difference of target and background shall not be less than 10 gray levels.
- Ensure that the target appears in the field of view for over 2s, movement distance exceeds target width and shall not be less than 15 pixels (CIF image).
- When conditions allow, try to reduce complexity of surveillance analysis scene. It is not recommended to use IVS in the scene with gathered targets and frequent changes of light.
- Try to avoid glass, reflection of light on the ground and water; try to avoid tree branches, shadows and areas with mosquito; try to avoid backlight and direct light.

### 6.4.1 Setting

The flow of setting IVS is shown in Figure 6-66.



You need to enable AI plan when AI by camera is used. Refer to "6.1 Enabling AI Plan" to enable AI detect function.



### 6.4.2 IVS

Set alarm rule of IVS. Alarm is triggered when IVSS detects target that goes against the IVS rule.



- IVSS supports AI by camera and AI by device. When both are enabled, AI by device is prior.
- This section takes setting AI by device for example.

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

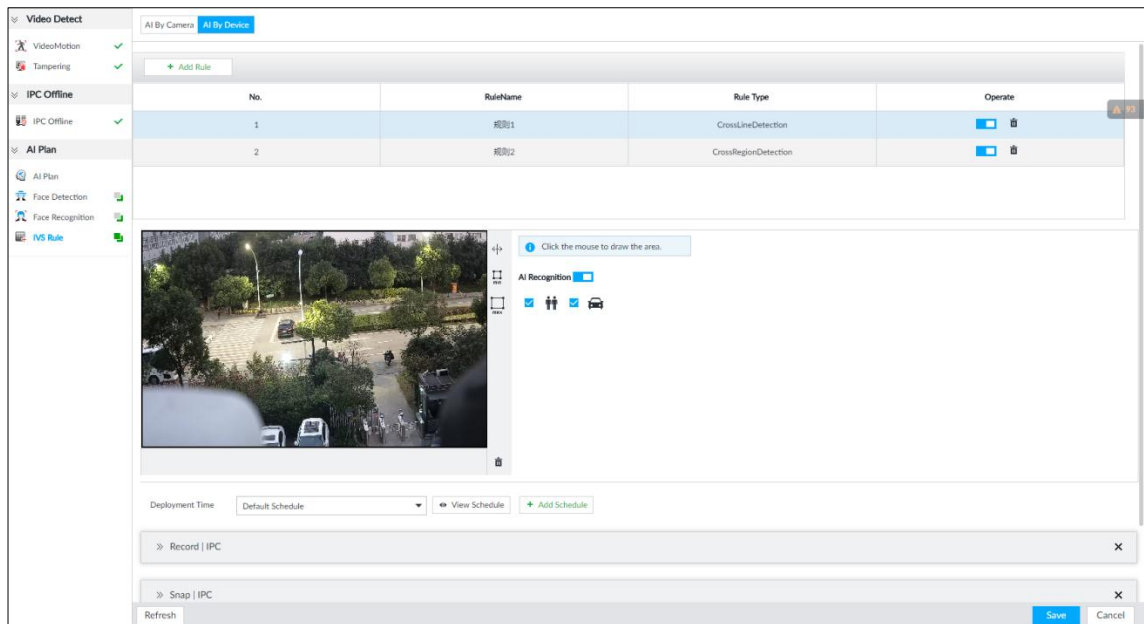
The **EVENT** interface is displayed.

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

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

The **AI by device** interface is displayed. See Figure 6-67.

Figure 6-67 AI by device



**Step 4** Set cross line detection and cross region detection rule.

- 1) Click **Add Rule**, and select **Cross Line Detection** or **Cross Region Detection**. The rule information is displayed. See Figure 6-68 or Figure 6-69.

Figure 6-68 Configuring cross line detection rules








No.	RuleName	Rule Type	Operate
1	Rule1	CrossLineDetection	 

Figure 6-69 Configuring cross region detection rules

No.	RuleName	Rule Type	Operate
1	Rule1	CrossRegionDetection	 

- 2) Click  to enable detection rule.

Click  to delete detection rule.

- 3) Click  to edit cross line. See Figure 6-70. Click  to edit cross region. See Figure 6-71.

- Hold on  and drag it to adjust position or length of the line and region.





- Click  or  on cross line direction to set the direction. An alarm will be triggered only when the target crosses the line in the designated direction.
- Click white dot on the line or region frame to add a turning point. Hold on  at the turning point and drag it to adjust position or length of the line and region.
- Select a line and then click  to delete.

Figure 6-70 Configuring cross line

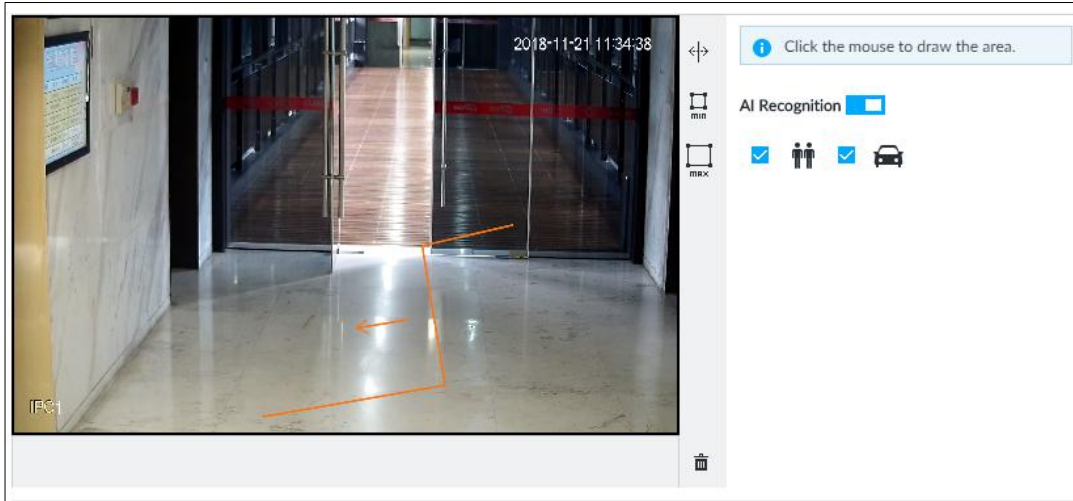
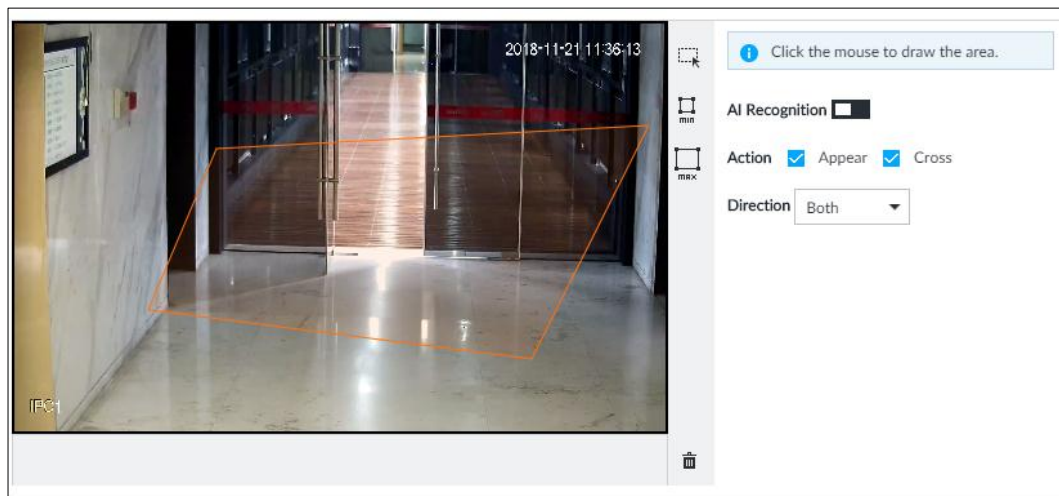




Figure 6-71 Configuring cross region



- 4) Set cross region action and direction.




Go to this step only when you set cross region.

- 5) Click  or  to set minimum size or maximum size of detection target. System triggers an alarm once the detected target size is not larger than the maximum size or smaller than the minimum size.

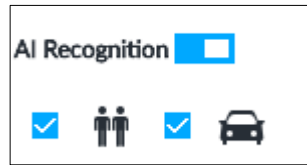
#### Step 5 AI recognition

After setting AI recognition, when the system detects a person or vehicle, a rule box will appear beside the person and vehicle in the surveillance image.



- 1) Click  to enable AI recognition function.

The recognition type option displayed. See Figure 6-72.

Figure 6-72 Type



2) Select a recognition type.

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

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

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

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

**Step 7** Click **Actions** to set alarm action. Refer to "8.4.1 Alarm Actions" for detailed information.



Repeat Step 4-Step 7 to add multiple detection rules. Support to add max. 10 detection rules at the same time.

**Step 8** Click **Save**.

## 6.4.3 Real-time View

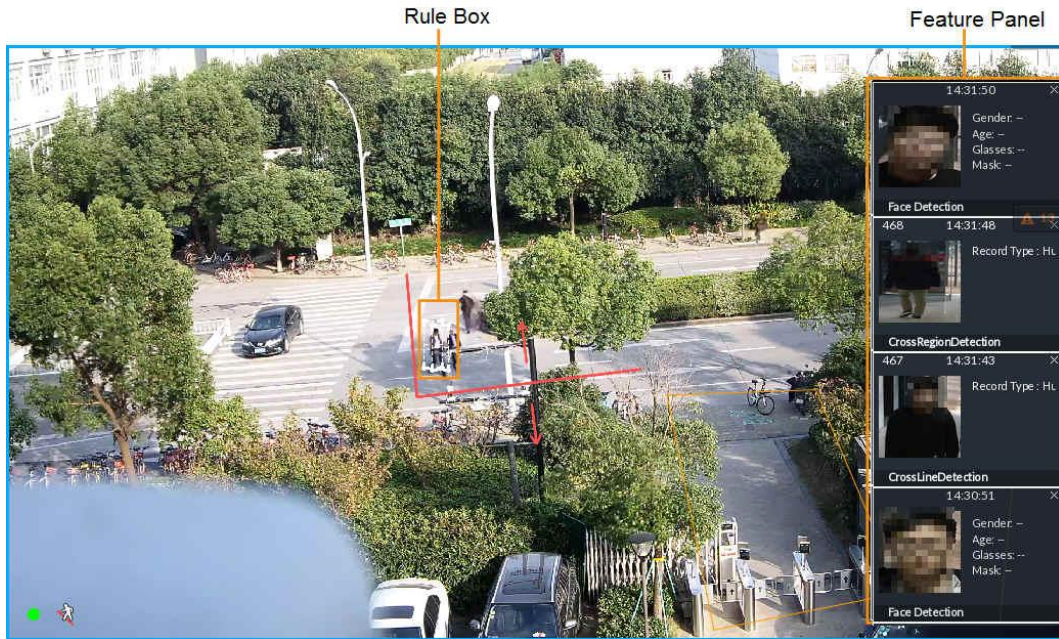
You can view real-time IVS results on the **LIVE** interface. Results such as detected face features and cross line detection are displayed on the right side of the real-time video image.

### 6.4.3.1 Live

Go to the **LIVE** interface, enable view, device displays view video. See Figure 6-73.

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

Figure 6-73 Live



Move the mouse to features panel, and the operation icons are displayed. See Figure 6-74.


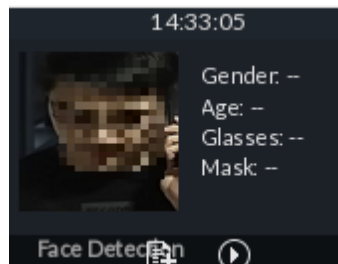
Click  or double-click the detected image, so the system starts to play back the recorded videos (10 s before and after the time of taking the snapshot).

Figure 6-74 Cross line



### 6.4.3.2 Detection Statistics

You can view the IVS results of detected human body, face, vehicle, and non-motor vehicle. For example, you can view whether people cross a region or cross a line.

On the **LIVE** interface, click . The **PEOPLE TOTAL** interface is displayed. See Figure 6-75.

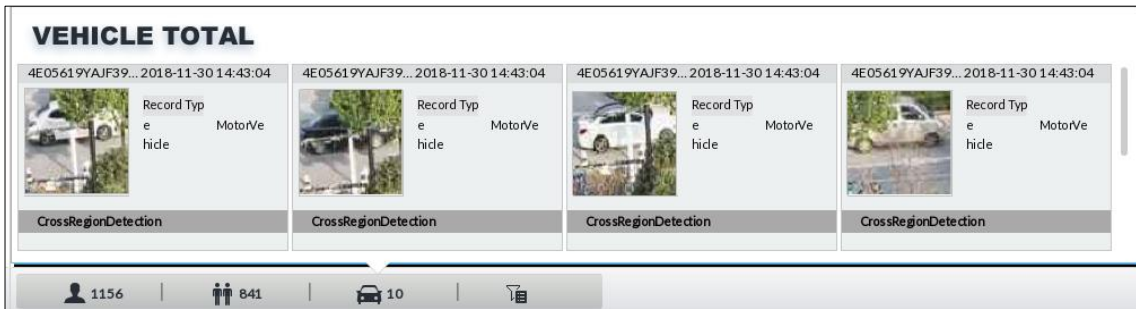
Figure 6-75 People total



Click . The **VEHICLE TOTAL** interface is displayed. See Figure 6-76.



Figure 6-76 Vehicle total



Move the cursor to detection panel, and the operation icons are displayed. See Figure 6-77.

Figure 6-77 Operation icon








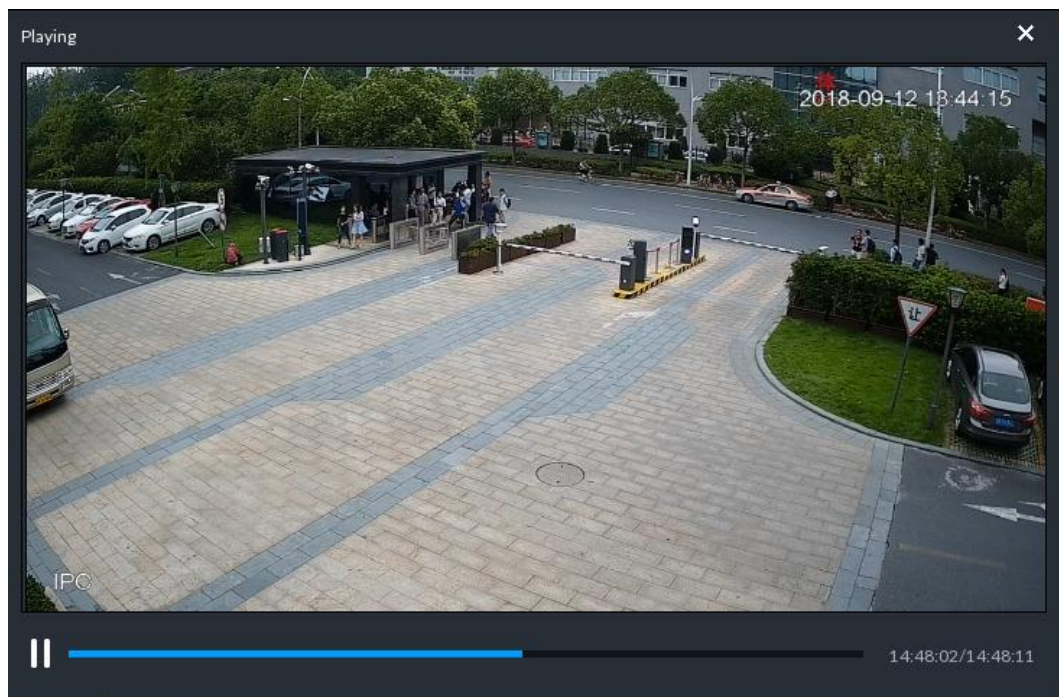

- : Click it, or double-click the detected image, IVSS starts to play back the recorded videos (10 s before and after the time of taking the snapshot). See Figure 6-78.
- ◇ Click  to pause play. Now the icon turns into . Click  again to continue to play.
- ◇ Click  to close view window.

Figure 6-78 Record

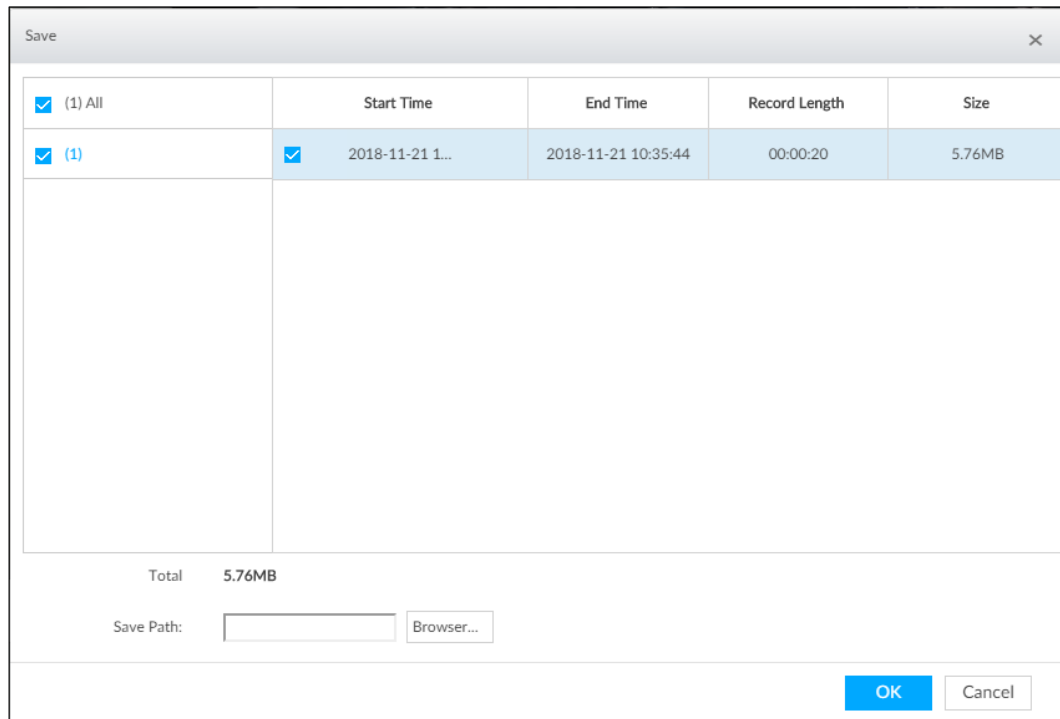


- : Click it, and the **Save** interface is displayed. See Figure 6-79. Click **Browser** to select storage path, and then click **OK** to export records to the selected storage path.



Connect USB storage device to IVSS if you want to store the records to such storage device.

Figure 6-79 Save



## 6.4.4 Search Interface

Select remote device and set event type to search IVS information. For example, you can set event type as cross line detection, and detected targets that cross line will all be displayed.

### Search image

Step 1 On the **LIVE** interface, click  and then select **AI Search > IVS**.

The **IVS** interface is displayed. See Figure 6-80.

Figure 6-80 IVS

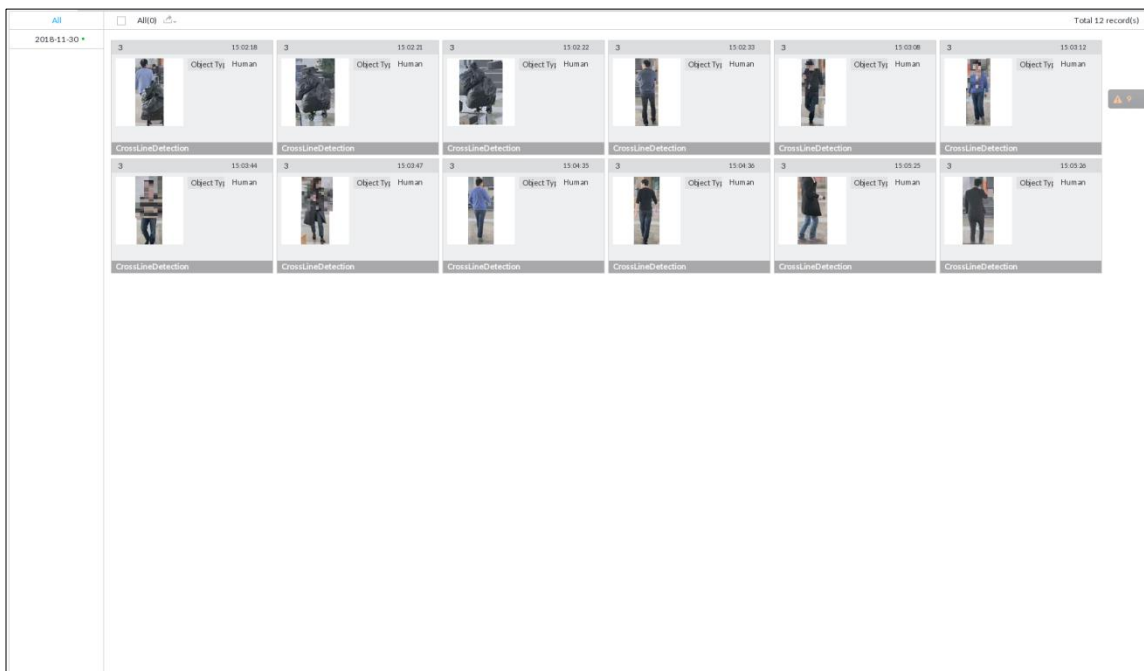


**Step 2** Select the remote device, and set event type, effective target and time.

**Step 3** Click **Query**.

The search results are displayed in the panel. See Figure 6-81.

Figure 6-81 Search result



Click the panel, and the operation icons are displayed. See Figure 6-82.

Figure 6-82 Operation icon

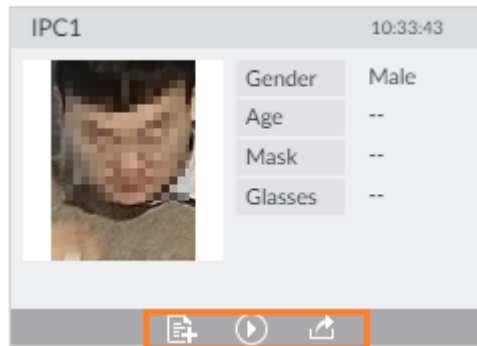


Table 6-14 Search by image

Icon	Operation
	Move the mouse onto the panel. Click  to select the panel.  means it is selected.
	Click  to add picture to database. See "6.2.2.2.3 Detection Add."
	Click the panel, and click  or double click the panel. The system starts to play back the recorded videos (10 s before and after the time of taking the snapshot).
	Click the panel and click , or click the panel and click  to export images, videos and Excel to designated storage path.  After setting alarm linkage snapshot, during exporting images, the system exports detected images and panoramic images at the time of snapshot.

## 6.5 Vehicle Recognition

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



IVSS supports only vehicle recognition through AI by camera. Make sure the vehicle recognition parameters of camera are configured. For details, see the user's manual of the camera.

### 6.5.1 Enabling AI Plan

Before using AI by camera, AI plan needs to be enabled first. For details, see "6.1 Enabling AI Plan."

### 6.5.2 Setting Vehicle Recognition

Set the deployment time of vehicle recognition and alarm linkage event, and IVSS links alarm event when alarm is triggered within the defined time.

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

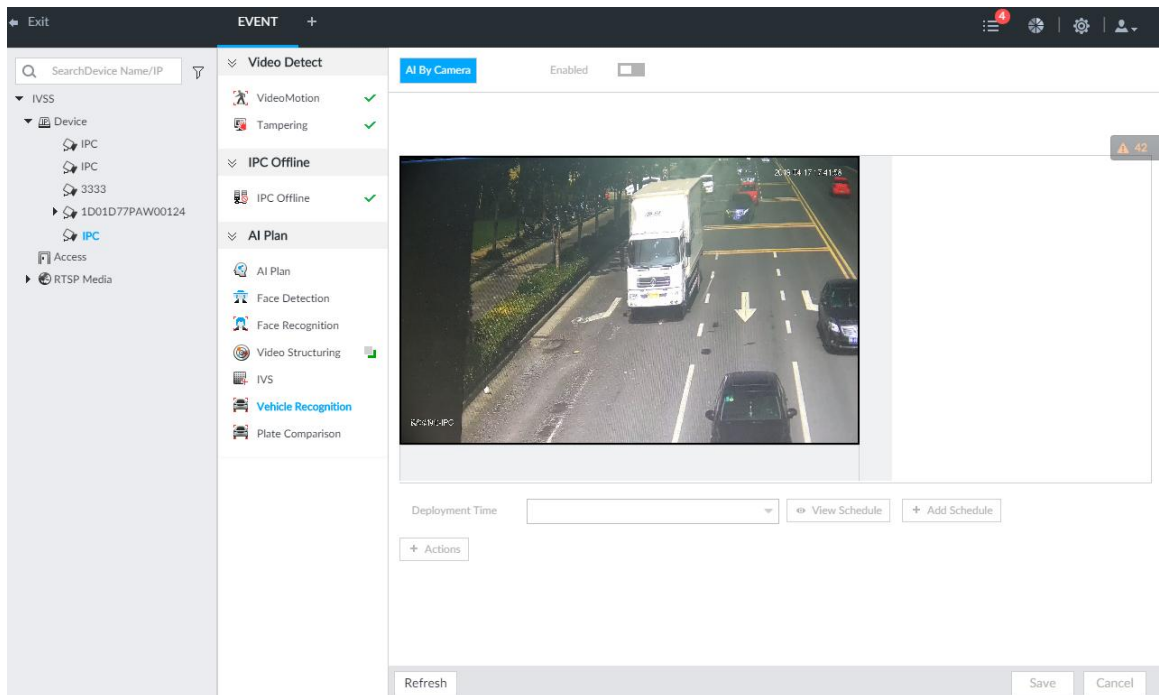
The **EVENT** interface is displayed.

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

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

The Vehicle Recognition interface is displayed. See Figure 6-83.

Figure 6-83 Vehicle recognition



**Step 4** Click the **Deployment Time** dropdown list to select schedule.

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

- Click **View Schedule** to view detailed schedule settings.
- If the schedule is not added or the added schedule does not meet actual needs, click **Add Schedule**. For details, see "8.8.4 Schedule."

**Step 5** Click **Actions** to set alarm action. For details, see "8.4.1 Alarm Actions."

**Step 6** Click **Save**.

## 6.5.3 Real-time View

On the **LIVE** interface, you can set the vehicle properties that you want to display on the real-time video image, and view such properties.


### 6.5.3.1 Setting AI Display

You can set the vehicle properties that you want to display on the real-time video image.



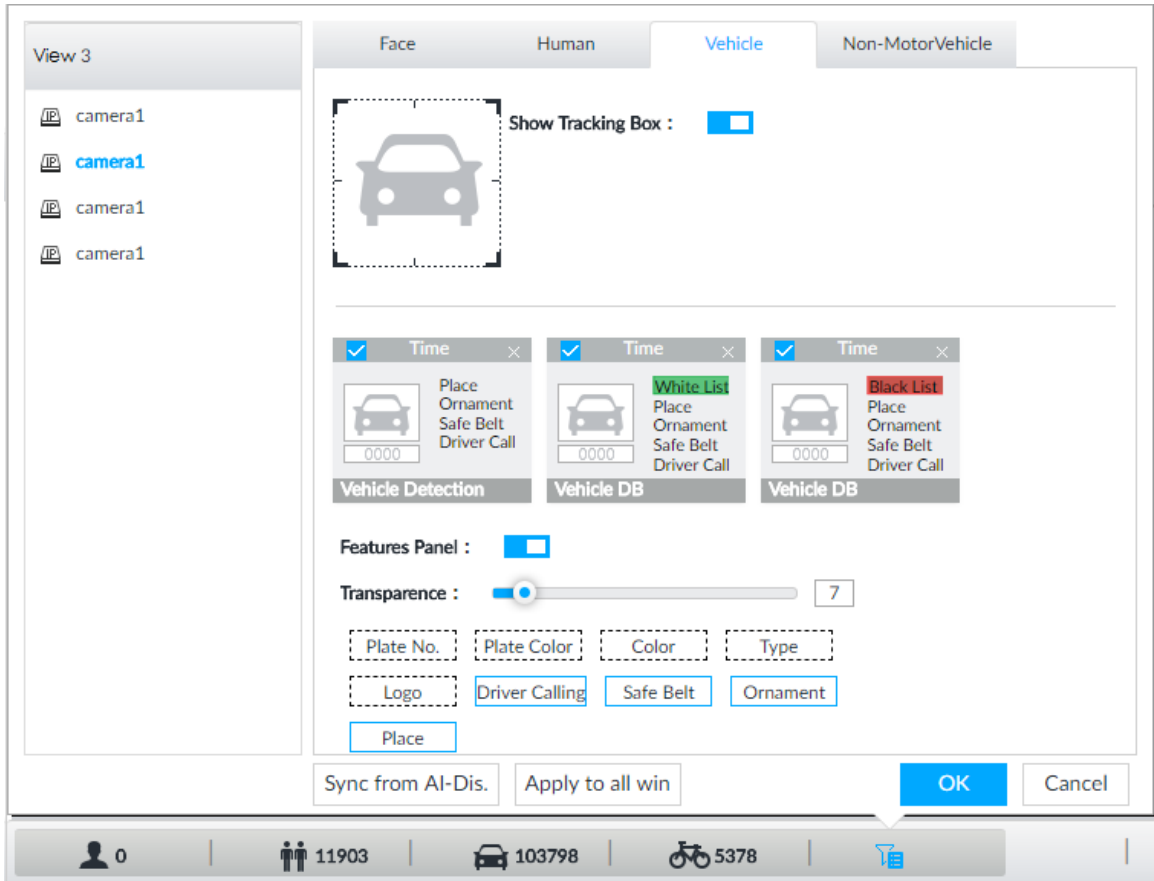
Before setting the features and properties, you need to create a view by adding cameras to the view so you can check video and pictures captured by the cameras. To create view, see "7.1.1 View Management."

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

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

The **Vehicle** interface is displayed. See Figure 6-84.

Figure 6-84 Motor vehicle



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

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

**Step 4** Set features panel.

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

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

2) Select a vehicle information panel.  means the panel is selected.

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

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

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

**Step 5** Click **OK**.

### 6.5.3.2 Live

On the **LIVE** interface, select a view, and the video image of the view is displayed. See Figure 6-85.

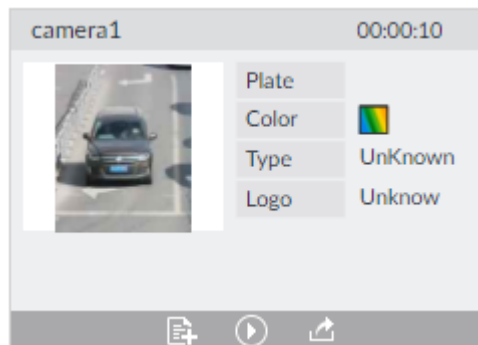
- Tracking box is displayed in the video image.
- Features panel is displayed at the right side of the video image.



Figure 6-85 Live



Move the cursor to the features panel, and the operation icons are displayed. See Figure 6-86.


Figure 6-86 Icons



- Click  to add license plate information to the plate database. For details, see "6.6.3.2.3 Add by Searching."
- Click  or double-click the vehicle image to play back the video image (10 s before and after the time of taking the snapshot).

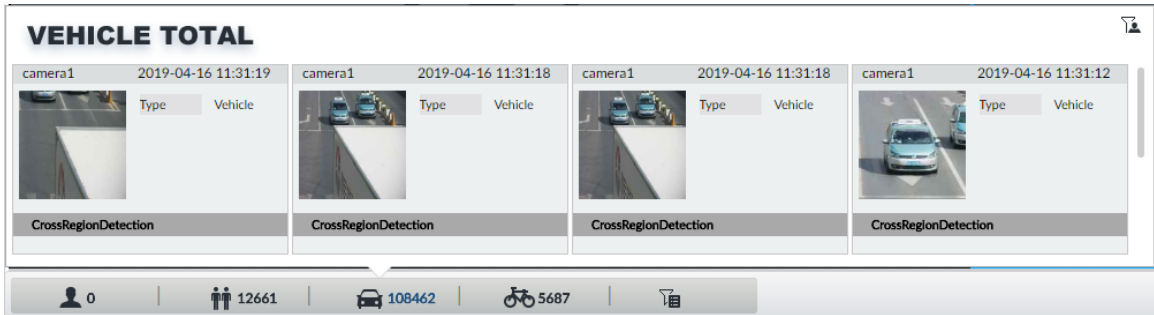
### 6.5.3.3 Detection Statistics

You can view the features and properties of detected motor vehicles.

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

Click , and then select **Vehicle Comparison**, the information of detected vehicles is displayed. See Figure 6-87.

Figure 6-87 Vehicle detection



Move the cursor to the features panel, and the following operation icons are displayed:

- : Click it to add license plate information to plate database. For details, see "6.6.3.2.3 Add by Searching."
- : Click it or double-click the picture to play back the video image (10 s before and after the time of taking the snapshot).
- : Click it to export the video to specified save path.



Make sure USB storage device is connected during local operation.

## 6.5.4 Searching Detection Information

Set event type and vehicle properties, such as plate, vehicle color, plate color, logo, and then search vehicles with these properties. For details, see "6.3.4.2 Search by Vehicle."

## 6.6 Vehicle Comparison

IVSS compares the detected vehicle properties with plate pictures of linked plate database, and then triggers alarm when the matched similarity reaches or exceeds the defined similarity.

### 6.6.1 Procedure

The procedures of setting vehicle comparison are shown in Figure 6-88 and Figure 6-89.

Figure 6-88 Vehicle comparison procedure (AI by camera)

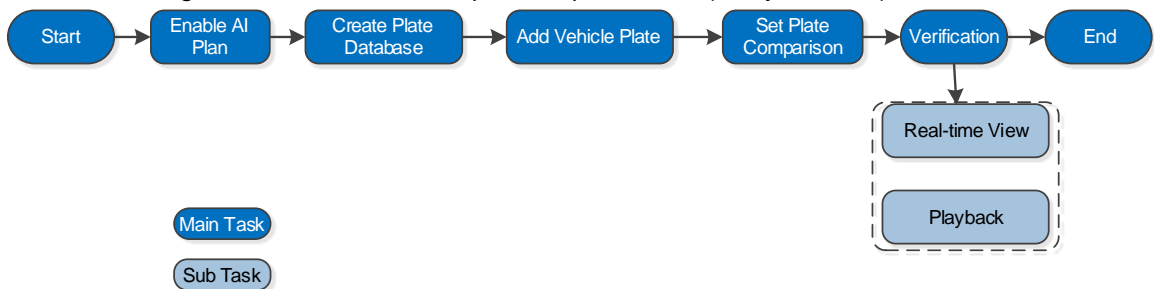
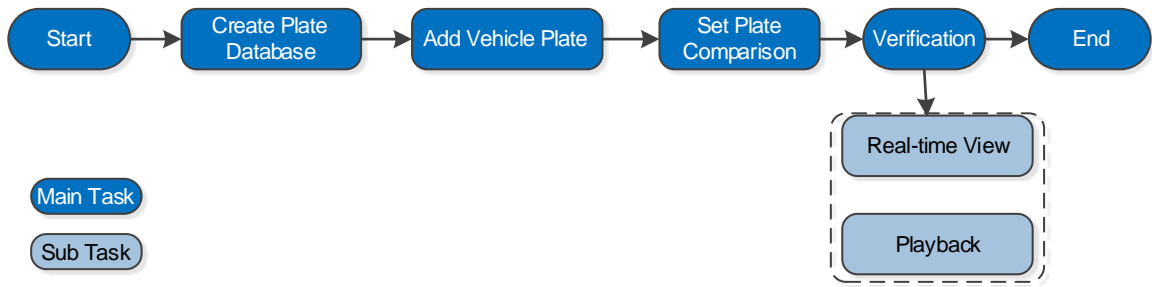




Figure 6-89 Vehicle comparison procedure (AI by IVSS)



## 6.6.2 Enabling AI Plan

Before using AI by camera, AI plan needs to be enabled first. For details, see "6.1 Enabling AI Plan."

## 6.6.3 Setting Vehicle Database

Set vehicle database, and then IVSS can analyze and compare vehicle plates with information in the database.

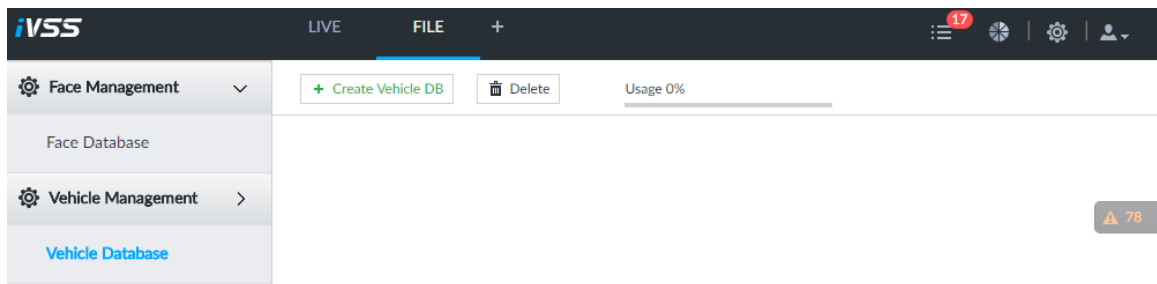
### 6.6.3.1 Creating Vehicle Database

You can create vehicle database, and then classify and manage the database. Database of trusted vehicle list and blocked vehicle list can be created. Alarm will be triggered when vehicle in the blocked list is detected.

**Step 1** On the **LIVE** interface, click **+**, and then select **FILE > Vehicle Management > Vehicle Database**.

The **Vehicle Database** interface is displayed. See Figure 6-90.

Figure 6-90 Vehicle database



**Step 2** Click **Create Vehicle DB**.

The **Create Vehicle DB** interface is displayed. See Figure 6-91.

Figure 6-91 Create vehicle database

Create Vehicle DB

1 Vehicle DB Name

2 Register Vehicle

Vehicle DB Name

Type

Black List

Register Vehicle → Save and close Cancel

Step 3 Set **Vehicle DB Name**, and select **Type** of vehicle database.

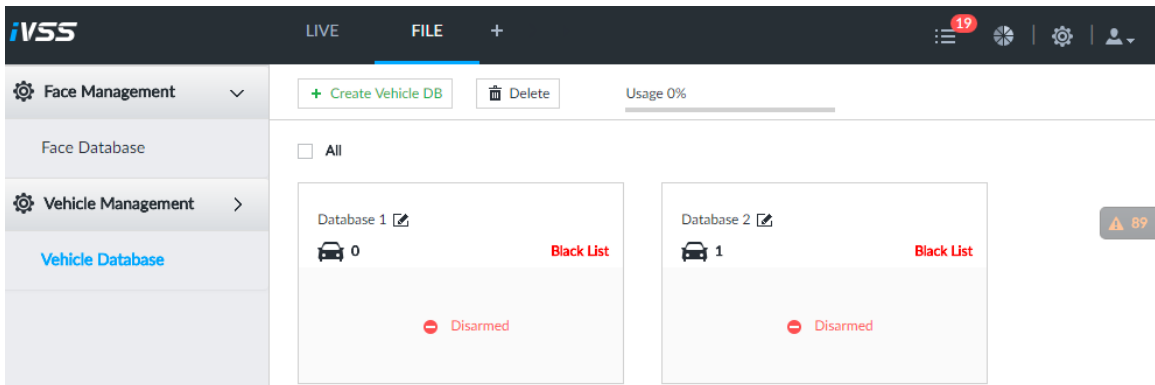
Step 4 Click **Register Vehicle** or **Save and close**.

- Click **Register Vehicle**, and add the vehicle information to the database. See Figure 6-92. For details, see "6.6.3.2 Registering Vehicle Information."

Figure 6-92 Register vehicle plate

- Click **Save and close** to create a database without editing its information. The newly-created database can be viewed on the **Vehicle Database** interface. See Figure 6-93.

Figure 6-93 Vehicle database









## Other Operations

Operations after a database is created include modifying the database name, registering plate information, arming the database, and deleting the database. See Table 6-15.

Table 6-15 Other operations

Operation	Description
-----------	-------------


Operation	Description
View database information and status	<ul style="list-style-type: none"> <li>● <b>Database 2</b> : Database name.</li> <li>●  <b>1</b>: Number of vehicle plate in the database.</li> <li>● <b>Black List</b> / <b>White List</b> : The database is in the blocked/trusted list.</li> <li>●  <b>Disarmed</b> : The database is not linked to channel for vehicle plate comparison. If armed, the linked device channel will be displayed.</li> </ul>
Modify database name	Click  next the database name to modify its name.
Manage database	Double-click the database, and you can manage the vehicle plate information in the database. For details, see "6.6.3.3 Managing Vehicle Information."
Arm database	Link the database to camera channel for vehicle plate comparison. For details, see "6.6.4 Setting Plate Comparison."
Delete database	<ul style="list-style-type: none"> <li>● Delete one by one: Move the cursor to the database, and click  at the upper right corner to delete it.</li> <li>● Delete in batch: Move the cursor to a database, and check <input type="checkbox"/> to select the database. Select multiple databases in this way, and then click  <b>Delete</b> to delete the selected databases.</li> <li>● Delete all: Select <b>All</b>, and then click  <b>Delete</b> to delete all databases.</li> </ul>

### 6.6.3.2 Registering Vehicle Information

Add vehicle information in the created databases. Supports manual add and batch import.

#### 6.6.3.2.1 Manual Add

Add information of one vehicle at a time.

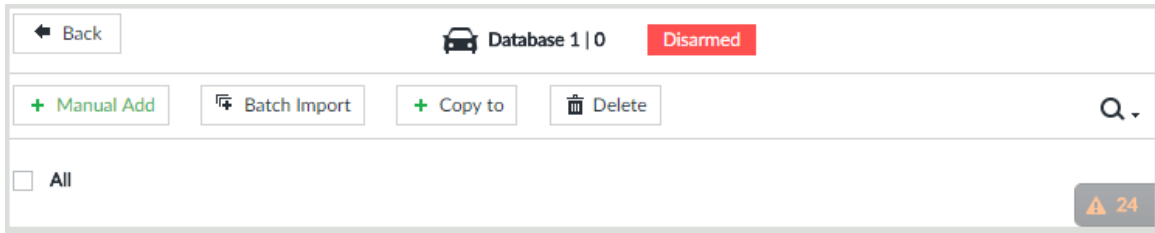
Step 1 On the **LIVE** interface, click , and then select **FILE > Vehicle Management > Vehicle Database**.

The **Vehicle Database** interface is displayed.

Step 2 Double-click the database.

The database interface is displayed. See Figure 6-94.

Figure 6-94 Database



**Step 3** Click **Manual Add**.

The **Vehicle Register** interface is displayed. See Figure 6-95.

Figure 6-95 Vehicle register


The 'Vehicle Register' form is displayed in a window with a close button (X) in the top right corner. It contains the following fields and controls:

- Country or Region:** A dropdown menu.
- Name:** A text input field.
- Driver ID:** A text input field.
- Cell Phone:** A text input field.
- Email:** A text input field.
- Address:** A text input field.
- Plate:** A text input field with a red asterisk indicating it is required.
- Logo:** A dropdown menu.
- Color:** A color selection icon with a dropdown arrow.
- Plate Color:** A color selection icon with a dropdown arrow.
- Type:** A selection area containing a dashed outline of a car and a 'Select' button with an upward-pointing arrow.

At the bottom of the form, there are three buttons: 'Save and continue to add', 'OK', and 'Cancel'.

**Step 4** Set the parameters. See Table 6-16.

Table 6-16 Vehicle register parameters

Parameter	Description
Country or Region	The country or region that the vehicle belongs to.
Name	Driver's name.
Driver ID	Driver's license number.
Cell Phone	Driver's cell phone.
Email	Driver's Email.
Address	Driver's address.
Plate	Vehicle plate number.
Logo	Vehicle logo.
Color	Click  to select the color of vehicle.



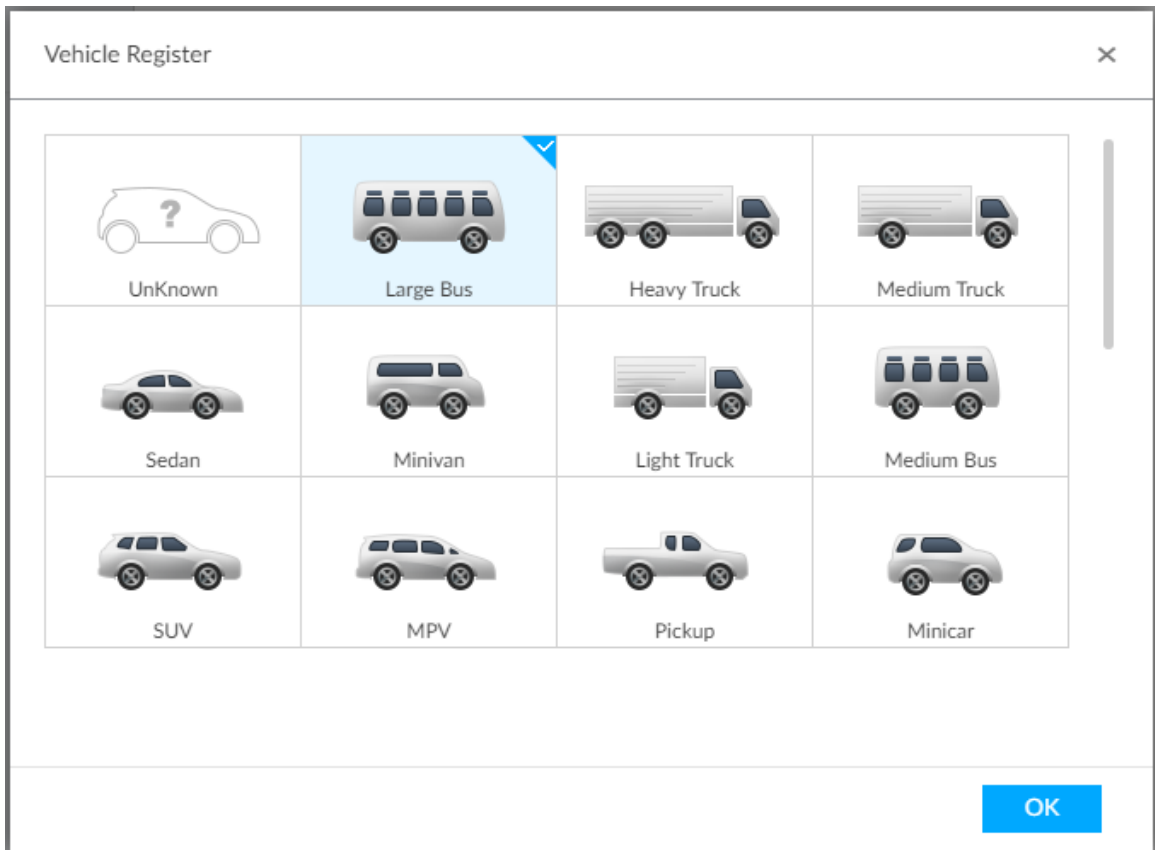
Parameter	Description
Plate Color	Click  to select the color of vehicle plate.
Type	Click  , and you can select the vehicle type. See Figure 6-96. Blue means already selected.

Figure 6-96 Vehicle type

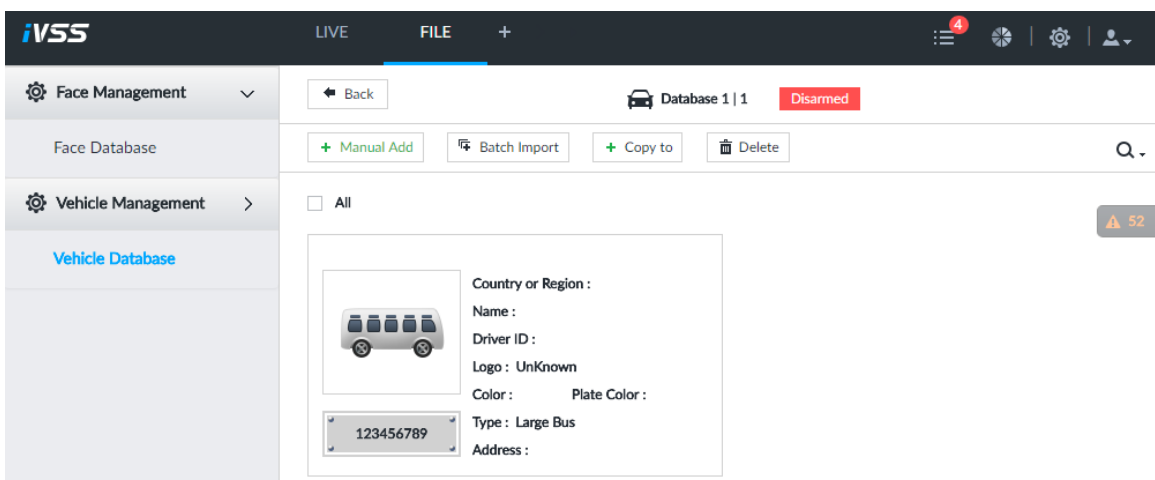


**Step 5** Click **Save and continue to add** or **OK**.

- Click **Save and continue to add**: Save the current vehicle information, and then continue to add next vehicle.
- Click **OK**: Save the current vehicle information.


The added vehicle information is displayed. See Figure 6-97.

Figure 6-97 Vehicle information



### 6.6.3.2.2 Batch Import

Import vehicle information to the database in batches.

**Step 1** On the **LIVE** interface, click , and then select **FILE > Vehicle Management > Vehicle Database**.

The **Vehicle Database** interface is displayed.

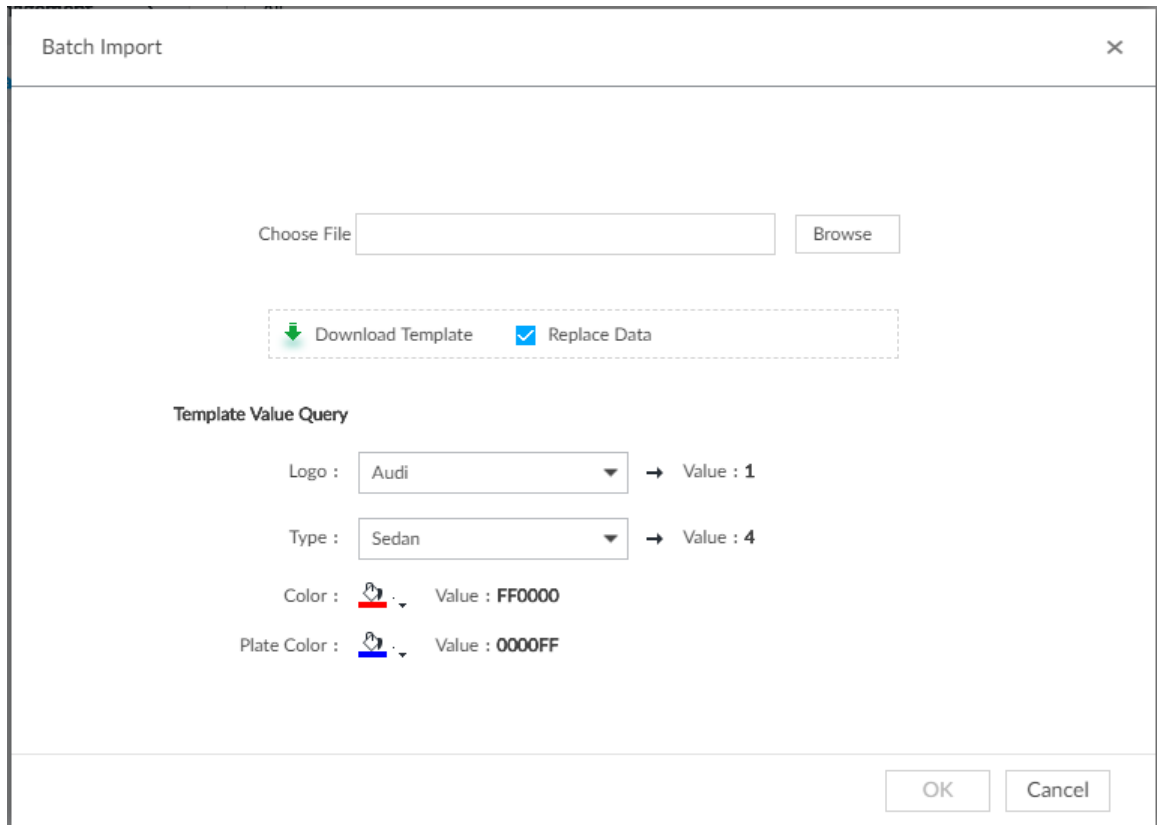
**Step 2** Double-click the database.

The database interface is displayed.

**Step 3** Click **Batch Import**.

The **Batch Import** interface is displayed. See Figure 6-98.




Figure 6-98 Batch import



**Step 4** Acquire and fill in the template file.

- 1) Click **Download Template** to download the template to PC or USB storage device.

The save path may vary when operating on client or local interface, and the actual interface shall prevail.

- On client: Click  on the upper right side, and then select  | **Download** to view the save path of template file.
- On local interface: Select the save path of template file.  
  
Make sure USB storage device is connected during local operation.
- On web interface: Template file is saved in the default download path of browser.

- 2) Fill in the template fill according to your actual needs. See Figure 6-99.

Fill in the vehicle information according to the instructions. For logo, type, color, and plate color, fill in the corresponding code or value. Search the code or value on the **Batch Import** interface (See Figure 6-98).

Figure 6-99 Template file

Serial No	*Plate No	Country	Logo	Type	Color	Plate Col	Owner	License	Tel	Email	Address
1	BD51SMR	GB		1	2 FFFFFFF	FFFFFF	Peter	L-PETER12	T-0712345	123@gmail	Birmingham
<b>&amp;&amp;Explain:</b> 1. With * is required 2. Country: Conform to ISO3166 specification. 2 bytes uppercase format. Example Great Britain GB Chinese CN. 3. Logo: Please input code number of vehicle logo. Example Bentley 54. The code number can be querying on the page of downloaded this. 4. Type: Please input code number of vehicle type. Example SaloonCar 4. The code number can be querying on the page of downloaded this. 5. Vehicle Color: Please input RGB color. Example Red FF0000. The code number can be querying on the page of downloaded this. 6. Plate Color: Please input RGB color. Example Red FF0000. The code number can be querying on the page of downloaded this. 7. License: Please add prefix 'L-'. 8. Tel: Please add prefix 'T-'.											

3) Save template file.

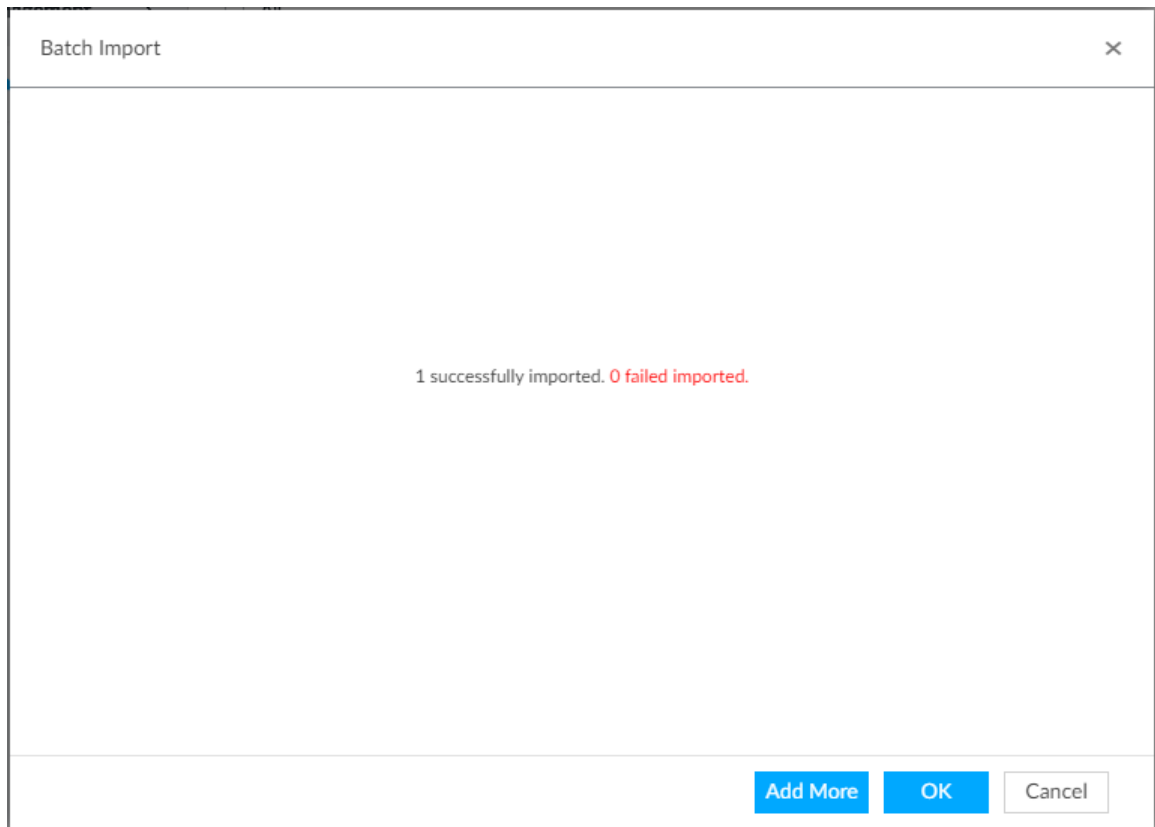
**Step 5** On the **Batch Import** interface, click **Browse** to import template file.

If the plate number in the template is the same as the number in the database, select **Replace Data** to overlap the information in the database.

**Step 6** Click **OK**.

The batch import result is displayed. See Figure 6-100.

Figure 6-100 Batch import result



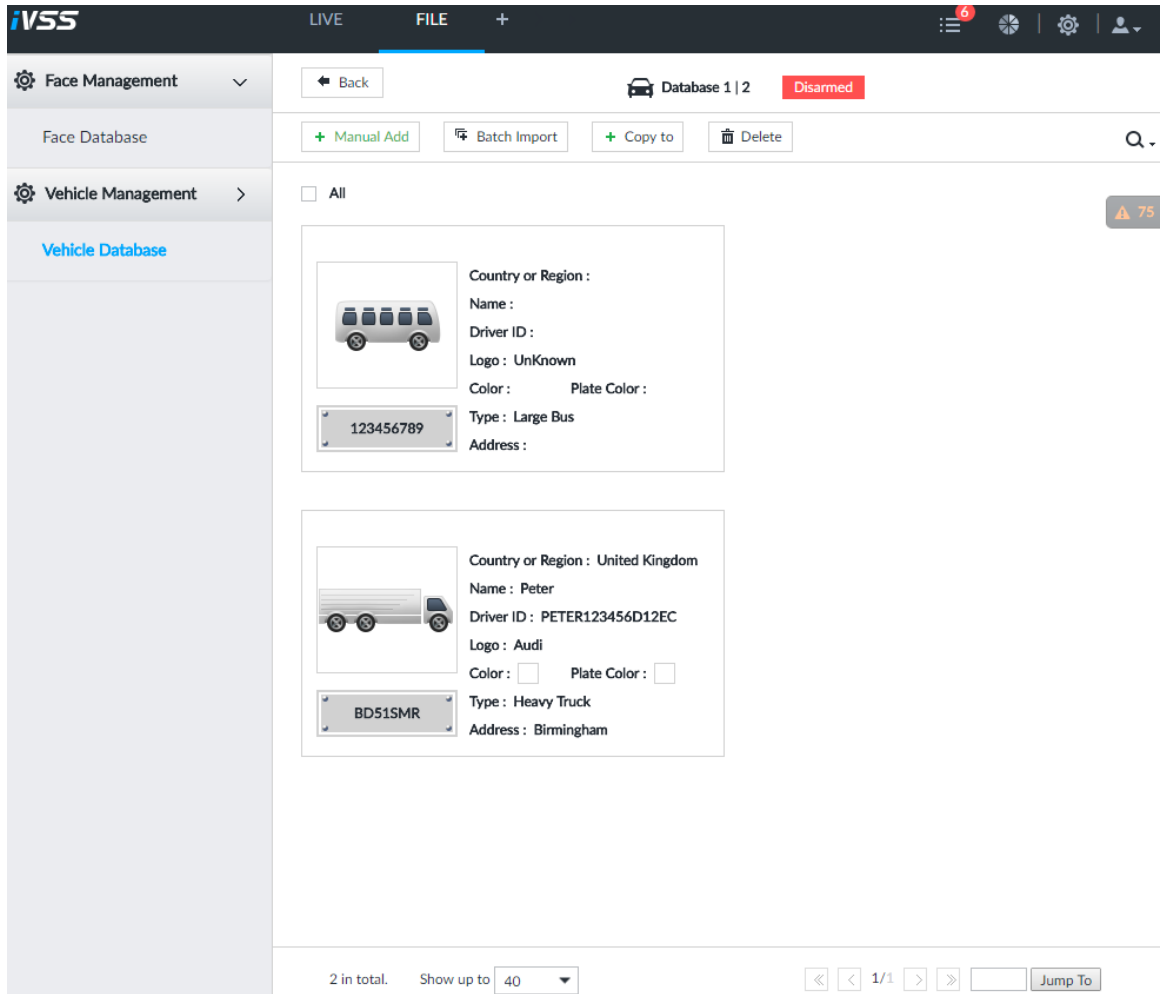
**Step 7** Click **Add More** or **OK**.

- Click **Add More**: Import vehicle information, and continue to add vehicle information.
- Click **OK**: Import vehicle information.

The added vehicle information can be viewed on the **Vehicle Database** interface. See Figure 6-101.






Figure 6-101 Vehicle information



### 6.6.3.2.3 Add by Searching

Add plate information from vehicle recognition or detection to the database.

**Step 1** On the **LIVE** interface, select the vehicle information to be added.

- Click , move the cursor to the information panel, then click .
- On the **Vehicle Recognition** or **Video Structuring** interface, move the cursor to the vehicle recognition or vehicle detection panel, and then click .

The **Vehicle Register** interface is displayed. See Figure 6-102.

Figure 6-102 Vehicle register

**Step 2** Select **Vehicle DB**, and enter **Plate**. Other information can be filled in according to actual conditions.

**Step 3** Click **OK**.

### 6.6.3.3 Managing Vehicle Information

After adding the vehicle information, such as plate, vehicle type, vehicle color, plate color, logo, to the database, the information needs to be properly managed and maintained to keep it accurate and complete.


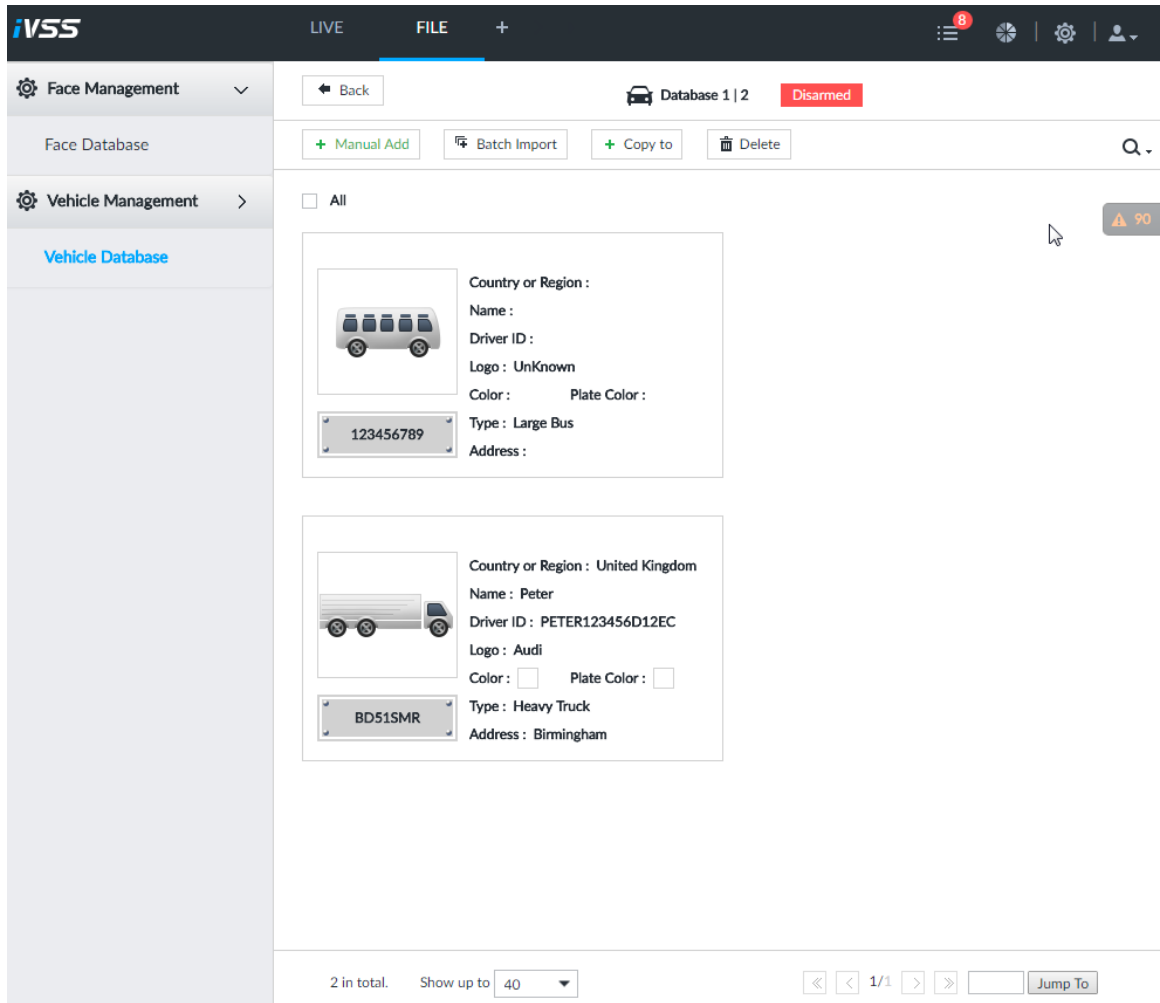
On the **LIVE** interface, click , and then select **FILE > Vehicle Management > Vehicle Database**. The database interface is displayed. See Figure 6-103. You can edit or delete the vehicle information, or copy or cut the information to another database.

Figure 6-103 Database



### 6.6.3.3.2 Editing Vehicle Information


Step 1 Move the cursor to the database, and then click  .  
The **Edit** interface is displayed. See Figure 6-104.

Figure 6-104 Edit

The 'Edit' dialog box contains the following fields and options:

- Country or Region: A dropdown menu.
- Name: A text input field.
- Driver ID: A text input field.
- Cell Phone: A text input field.
- Email: A text input field.
- Address: A text input field.
- Plate: A text input field containing '123456789'.
- Logo: A dropdown menu with 'UnKnown' selected.
- Color: A color selection icon.
- Plate Color: A color selection icon.
- Type: A dropdown menu showing a 'Large Bus' icon and the text 'Large Bus'.

At the bottom right, there are 'OK' and 'Cancel' buttons.

Step 2 Modify vehicle information according to actual needs.

Step 3 Click **OK**.

### 6.6.3.3.3 Copying Vehicle Information

Copy the vehicle information in a database to another database. IVSS Supports only copy and apply the vehicle information to database of the same type. For example, vehicle information in a black list database can only be copied to another black list database.

Step 1 Move the cursor to the database, and then click .

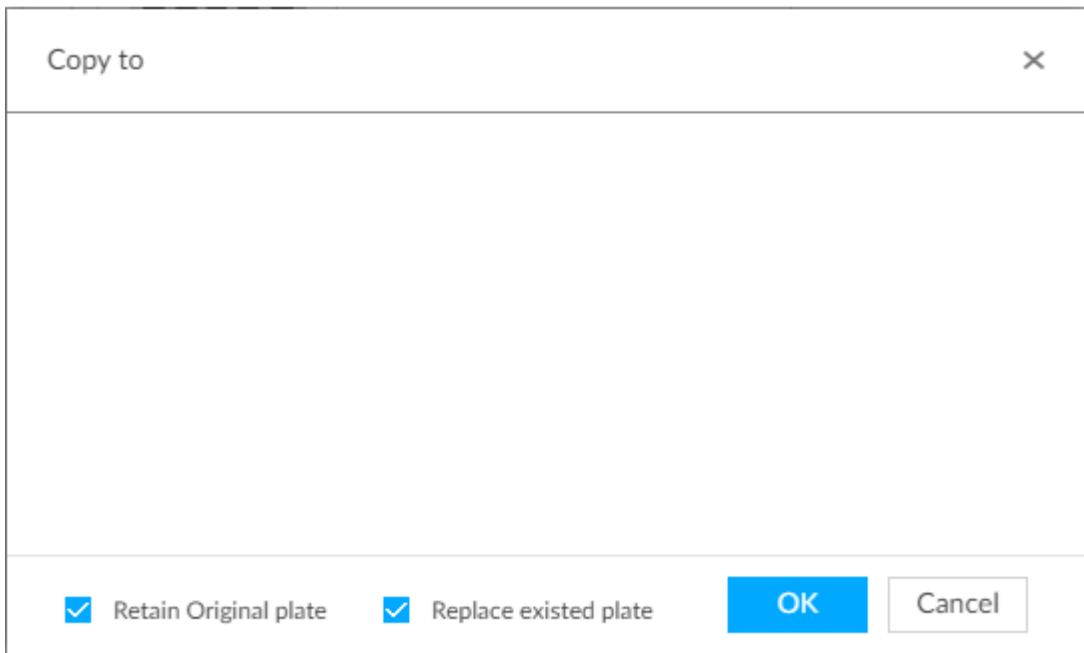


- Multiple vehicle information can be selected at a time.
- Select **All** to select information of all vehicles on the interface.

Step 2 Click .


The **Copy to** interface is displayed. See Figure 6-105.

Figure 6-105 Copy to






**Step 3** Select the target database.



- Multiple databases can be selected at a time. Blue means already selected, for example .
- Select **Retain Original plate**: When the same plate is detected, the vehicle information in the target database will not be replaced.
- Select **Replace existed plate**: When the same plate is detected, the vehicle information in the target database will be replaced.

**Step 4** Click **OK**.

#### 6.6.3.3.4 Deleting Vehicle Information



- Delete one by one: Move the cursor to the database, and then click  at the upper right corner to delete the database.
- Delete in batch
  - ◇ Move the cursor to the database, and then click  at the upper left corner to select the database. Select multiple databases in this way, and then click  to delete selected databases.
  - ◇ Select **All**, and then click  to delete all the databases on the interface.

### 6.6.4 Setting Plate Comparison

IVSS compares detected plate with plate information in the database, and trigger alarms when plate in the black vehicle list is detected.



The section takes AI by device for example, and the actual interface shall prevail.

**Step 1** Click  or  on the setting interface, then select **EVENT**.

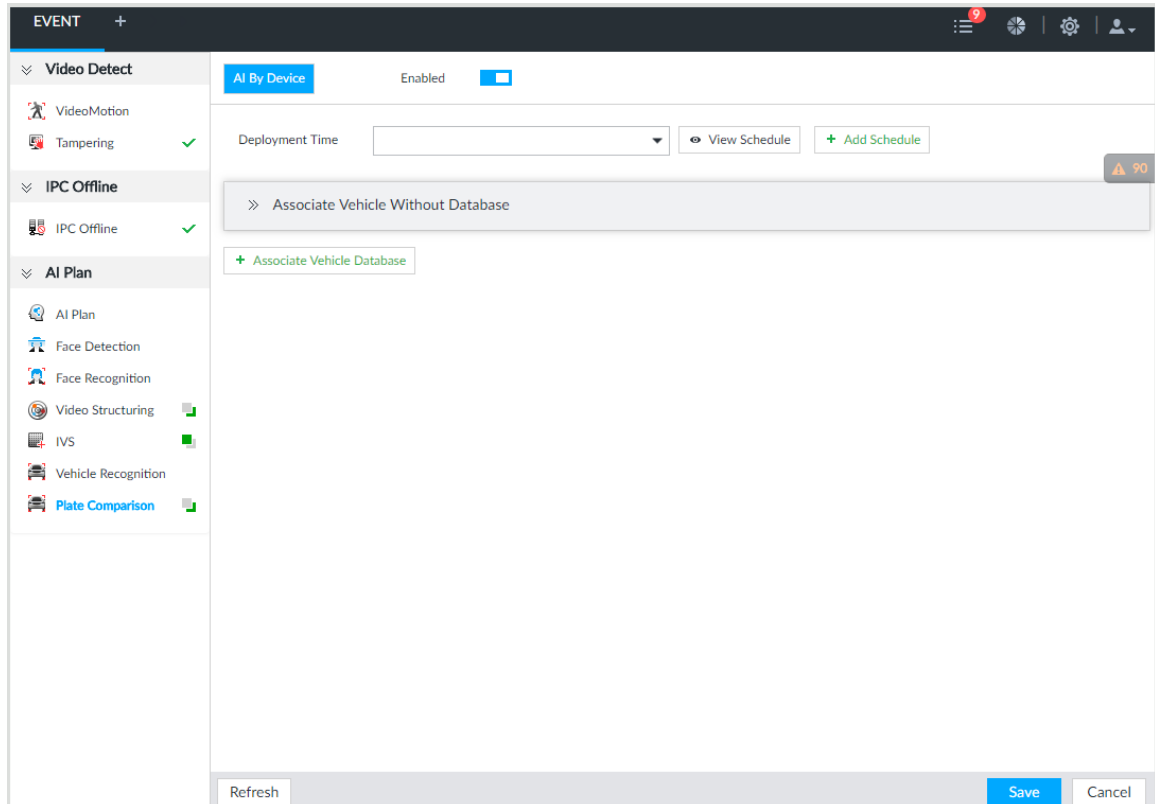
The **EVENT** interface is displayed.

**Step 2** Select device from the device tree on the left side.

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

The **Plate Comparison** interface is displayed. See Figure 6-106.

Figure 6-106 Plate comparison



**Step 4** Click  to enable plate comparison. The icon changes to .

**Step 5** Click **Deployment Time** dropdown list to select schedule.

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

- Click **Add Schedule** to add new schedule if no schedule is added or the existing schedule does not meet requirements. For details, see "8.8.4 Schedule."
- Click **View Schedule** to view details of schedule.

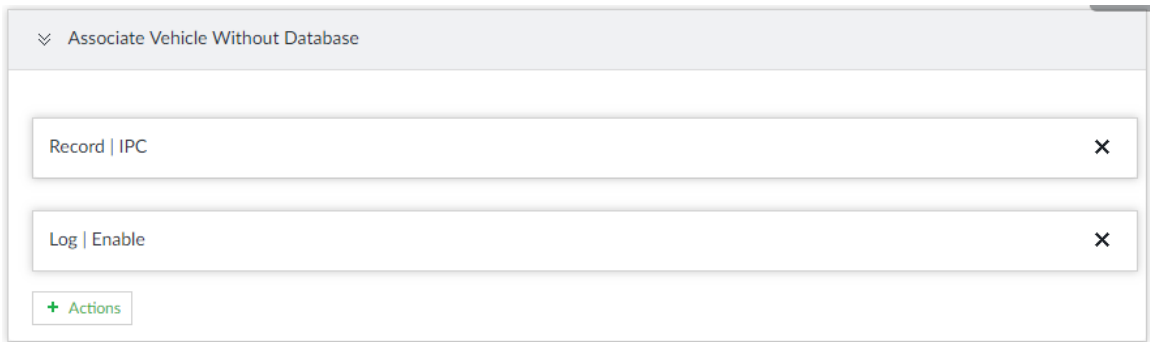
**Step 6** Link vehicle without database.

Enable linkage of vehicle without database. Alarm is triggered when vehicle not in the database is detected.

1) Click .

The **Associate Vehicle Without Database** interface is displayed. See Figure 6-107.

Figure 6-107 Associate vehicle without database



+ Associate Vehicle Database

2) Click **Actions** to set alarm linkage event. For details, see "8.4.1 Alarm ."

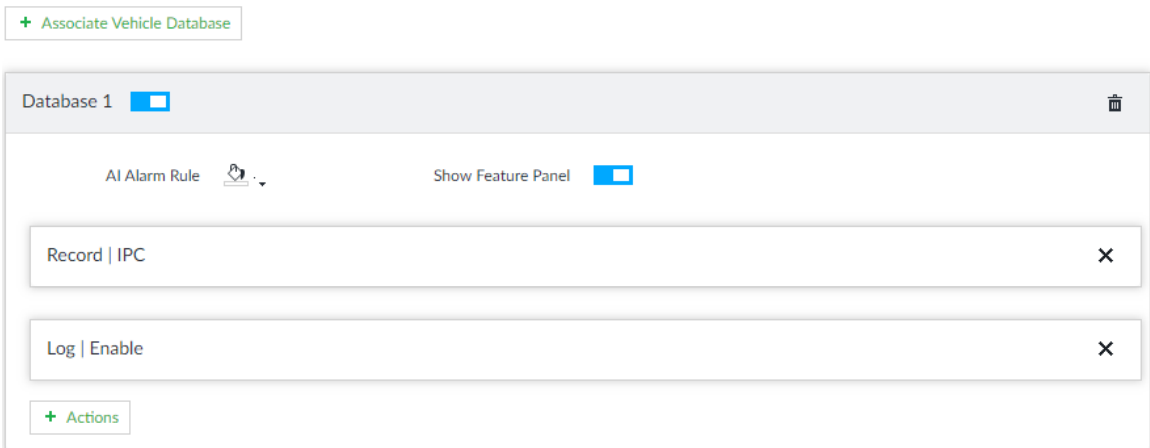
**Step 7** Link database.



Repeat the following steps to link multiple databases.



1) Click **Associate Vehicle Database**, and select the database to be linked. The database linkage interface is displayed. See Figure 6-108.

Figure 6-108 Database linkage



2) Set the parameters. See Table 6-17.

Table 6-17 Database linkage parameters

Parameter	Description
AI Alarm Rule	Click  to set the color of alarm rule box.
Show Feature Panel	Click  , and when alarm is triggered, the plate comparison information is displayed in the feature panel of video image.

3) Click **Actions** to set alarm linkage event. For details, see "8.4.1 Alarm ."

**Step 8** Click **Save**.

## 6.6.5 Real-time View

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

You can view real-time vehicle comparison results on the **LIVE** interface. If vehicle in the database is detected, properties of the vehicle, such as plate, type, color, and logo, are displayed on the right side of the real-time video image.


## 6.6.5.1 Setting AI Display

You can set the vehicle properties that you want to display on the real-time video image.



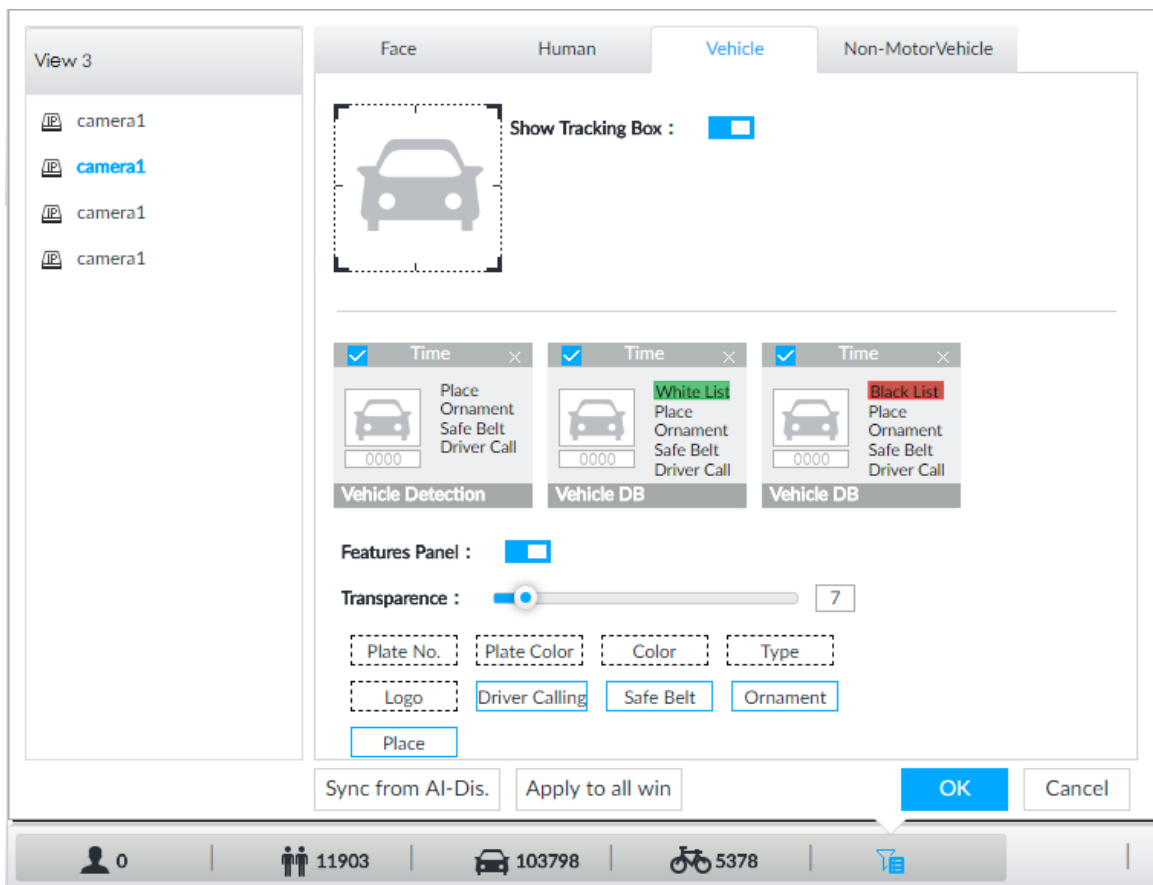
Before setting the features and properties, you need to create a view by adding cameras to the view so you can check video and pictures captured by the cameras. To create view, see "7.1.1 View Management."

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

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

The **Vehicle** interface is displayed. See Figure 6-109.



Figure 6-109 Vehicle



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

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

**Step 4** Set features panel.

- 1) Click  next to Features Panel to enable features panel function.  
Features panel will be displayed at the right side of video image when target with selected features is detected.
- 2) Select a vehicle information panel.  means the panel is selected.
- 3) (Optional) Drag  to adjust the transparency of panel. The higher the value, the



more transparent the panel.

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

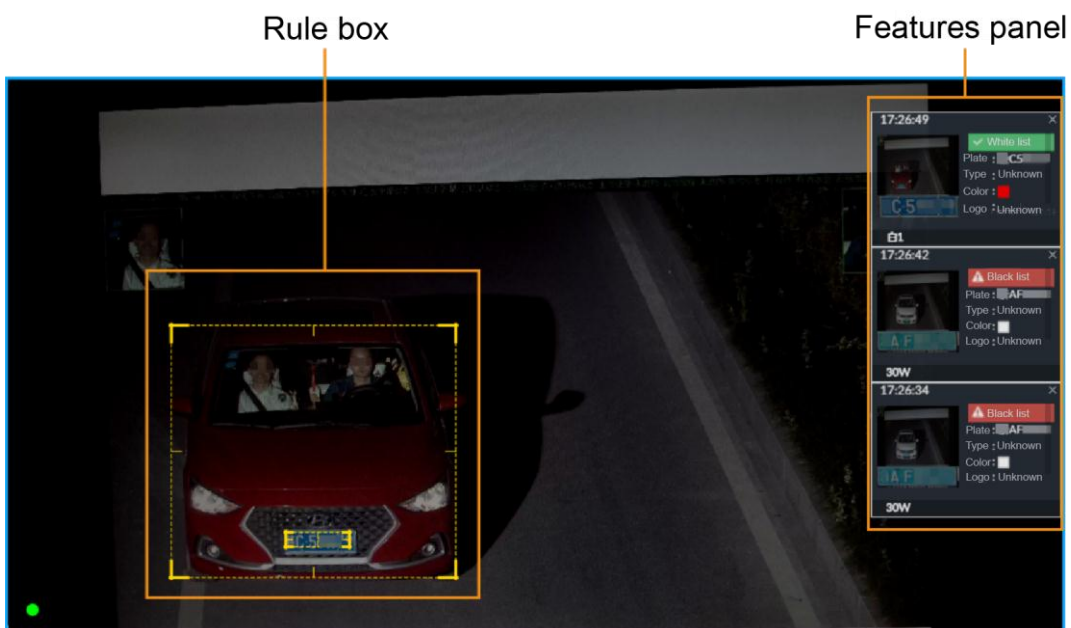
Step 5 Click **OK**.

## 6.6.5.2 Live

On the **LIVE** interface, select a view, and the video image of the view is displayed. See Figure 6-110.

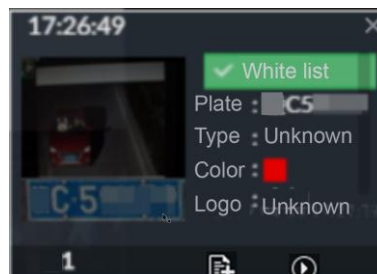
- Tracking box is displayed in the video image.
- Features panel is displayed at the right side of the video image.



Figure 6-110 Live



Move the cursor to the features panel, and the operation icons are displayed. See Figure 6-111.


Figure 6-111 Icons



- Click  to add license plate information to the plate database. For details, see "6.6.3.2.3 Add by Searching."
- Click  or double-click the vehicle image to play back the video image (10 s before and after the time of taking the snapshot).

### 6.6.5.3 Detection Statistics

You can view the vehicle comparison results. For example, you can view whether a vehicle is in the blacklist database or whitelist database.

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


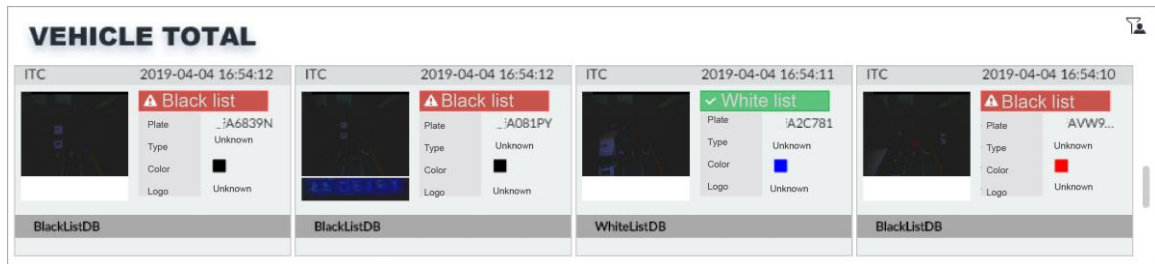



Click , and then select **Vehicle Comparison (Black List)** and **Vehicle Comparison (White List)**. The vehicle comparison result is displayed. See Figure 6-112.

Figure 6-112 Vehicle comparison



Move the cursor to the information panel, and the following icons are displayed:

- : Click it to add license plate information to plate database. For details, see "6.6.3.2.3 Add by Searching."
- : Click it or double-click the picture to play back the video image (10 s before and after the time of taking the snapshot).
- : Click it to export the video to specified save path (PC or USB storage device).




Make sure USB storage device is connected if you want to store the file to such storage device.

## 6.6.6 AI Search

Set search conditions such as device and properties, and then search information that meets the conditions. IVSS supports search by property and search by database.

### 6.6.6.1 Search by Property

Set search conditions such as device and properties, and then search vehicle recognition information that meets the conditions.

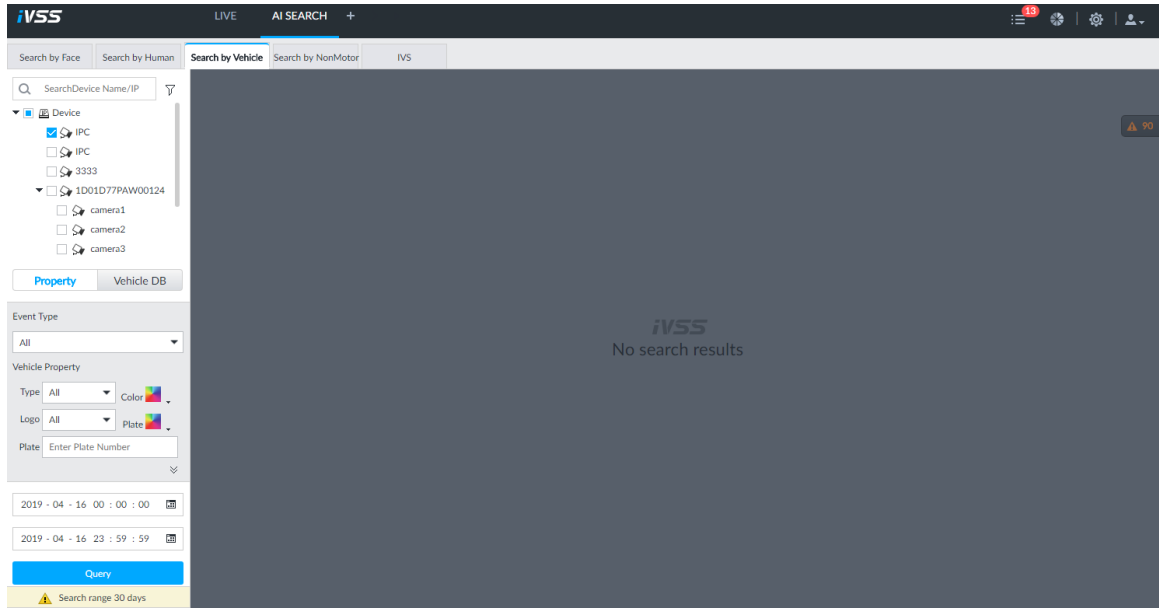
Step 1 On the **LIVE** interface, click , and then select **AI Search > Search by Vehicle**.

The **Search by Vehicle** interface is displayed.

Step 2 Select device, and then click **Property** tab.

The search by property interface is displayed. See Figure 6-113.

Figure 6-113 Search by property



**Step 3** Select **Plate Comparison** as the **Event Type**.

**Step 4** Set vehicle properties and time period.

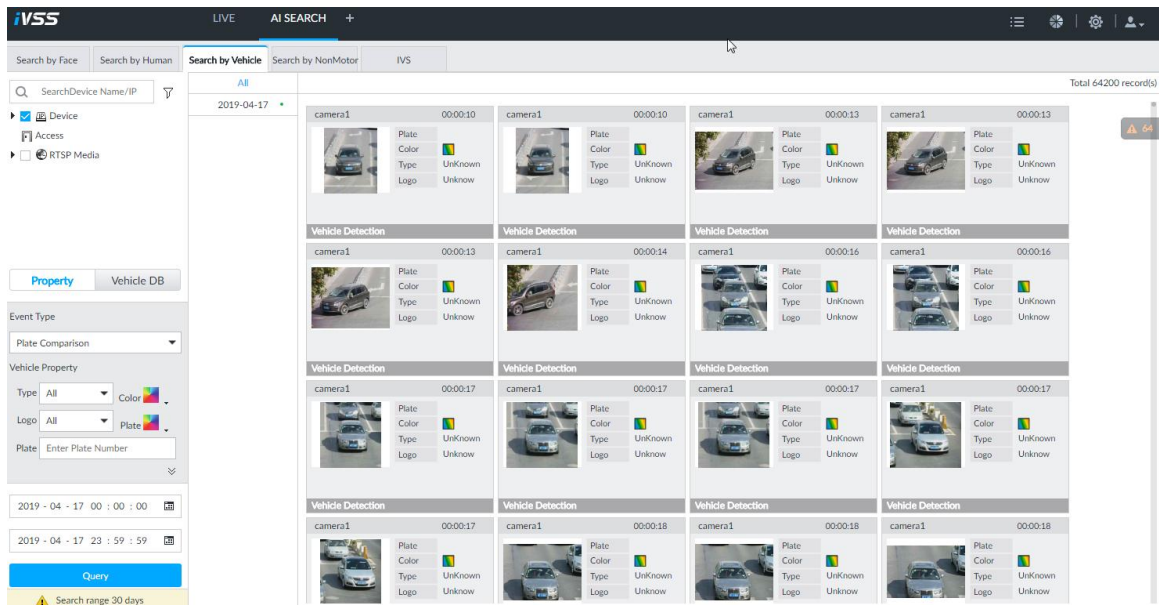
Click  or  to set the color.  means more than one color.

**Step 5** Click **Query**.

The search result is displayed. See Figure 6-114.

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

Figure 6-114 Search result



## Other Operations

Click on one displayed panel, and the icons are displayed. See Figure 6-115 and Table 6-18.

Figure 6-115 Icons

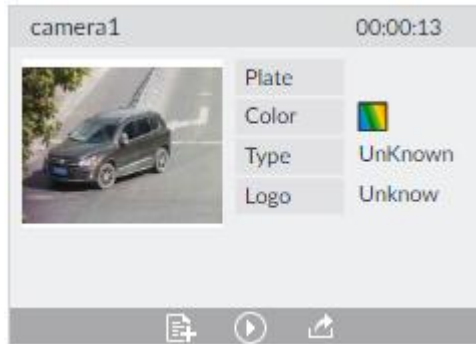


Table 6-18 Operation

Icon	Operation
	<ul style="list-style-type: none"> <li>• Select one by one: Move the cursor to the panel, and then click  at the upper right side to select the panel.  means the panel is selected.</li> <li>• Select in batches: Select <b>All</b> to select all the panels on the interface.</li> </ul>
	Move the cursor to the panel, and then click  or double-click the panel to play back the video record (10 s before and after the time of taking the snapshot).
	Move the cursor to the panel, and then click  to add picture to database. See "6.2.2.2.3 Detection Add."
	Move the cursor to the panel, and then click , or select the panel and then click  to export picture, video, and Excel file to specified save path.

### 6.6.6.2 Search by Database

Search vehicle recognition information according to database.

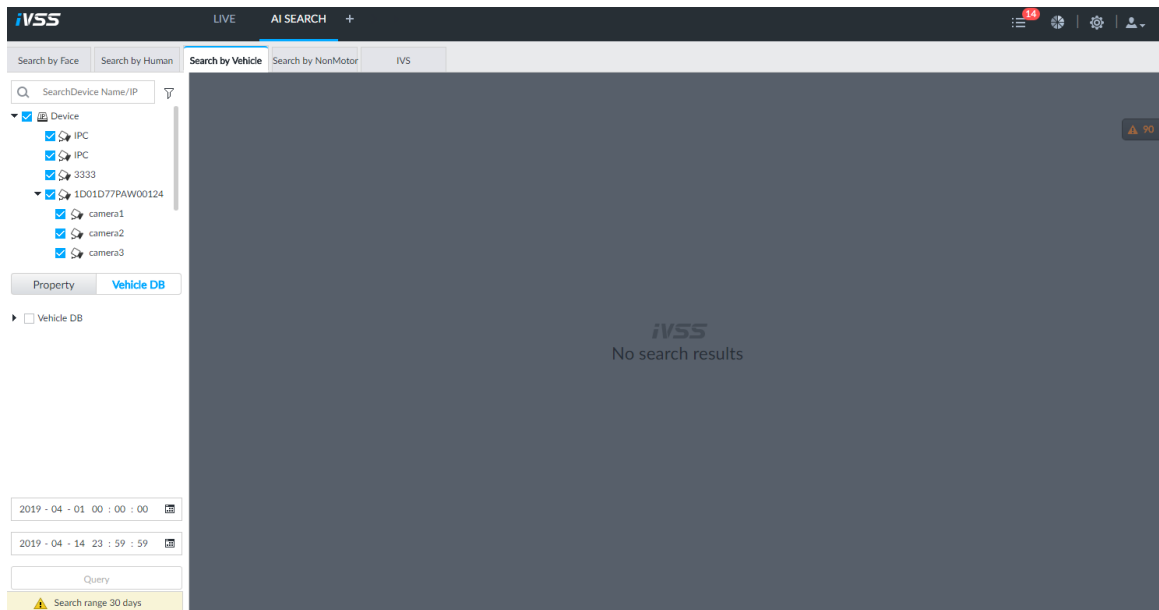
**Step 1** On the **LIVE** interface, click , and then select **AI Search > Search by Vehicle**.

The **Search by Vehicle** interface is displayed.

**Step 2** Select device from the device tree, and then click **Vehicle DB** tab.

The search by database interface is displayed. See Figure 6-116.

Figure 6-116 Search by vehicle database



**Step 3** Select the database to be searched.

**Step 4** Click **Query**.

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

## Other Operations

Click on one displayed panel, and the icons are displayed. For operations of icons, see "6.6.6.1 Search by Property."

# 7 General Operations

It is to introduce general operations such as preview and monitor, playback, alarm, AI function, and IVS.

## 7.1 Live and Monitor

After logging in device, the **Live** interface is displayed. See Figure 7-1 and Table 7-1.




Move the mouse to the middle of video window and left column.  is displayed. Click the icon to hide the left column. See Figure 7-2.

Figure 7-1 Live (1)



Figure 7-2 Live (2)

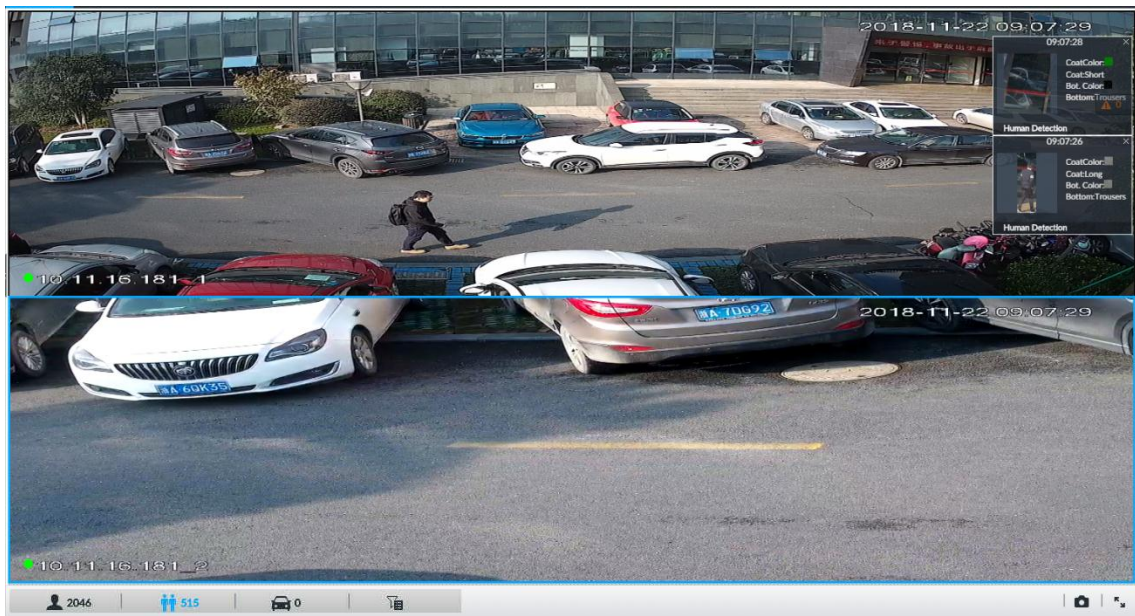


Table 7-1 Live interface description

No.	Description
1	View zone. Displays the created view and view group. Refer to "7.1.1 View Management for detailed information."
2	Resource pool. Displays the added remote device list. Refer to "7.1.2 Resources Pool for detailed information."
3	PTZ zone. It is to control the PTZ. Refer to "7.1.3 PTZ for detailed information."
4	Smart preview icons. View face statistics, person statistics, IVS statistics and AI display.
5	Video play window. Refer to "7.1.1.3 View Window for detailed information."

## 7.1.1 View Management

View refers to video images of several remote devices. Go to the view panel at the upper left corner on the **LIVE** interface to check the view. See Figure 7-3.


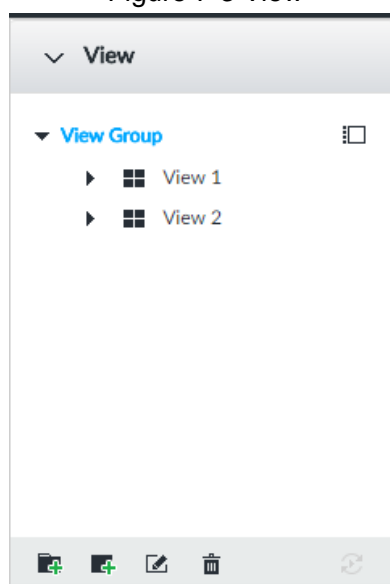
- A view group is created by default. You can add view(s) to this view group, or create new view group before adding view(s).
- Double-click the view or drag the view to the play panel on the right side. IVSS begins playing the real-time video of corresponding remote device.
- Click  to select views and its sub-node.

Figure 7-3 View



### 7.1.1.1 View Group

View group is a group of views. The view group allows you to categorize and manage view, so you can easily search and find the view.



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

## Create view group

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


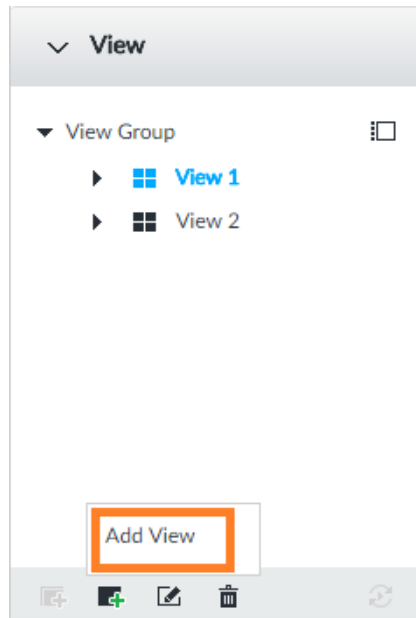
- Select Views or created view group and then click .
- Select **Add View** to add new view group. Set the group name, and click **OK**. System creates one view group. See Figure 7-4.

Figure 7-4 Create view group



**Step 2** Set view group name.

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


**Step 3** Click any spare panel on the interface.

Device pops up successfully operated.

## Operation

After creating view group, view group can be renamed or deleted. Refer to Table 7-2 for detailed information.

Table 7-2 View group

Operation	Description
Rename view group	<ul style="list-style-type: none"> <li>• Select a view group and then click . Set view group name and click any spare panel.</li> <li>• Right-click view group and select <b>Rename</b>. See Figure 7-5. Set view group name and click any spare panel.</li> </ul>





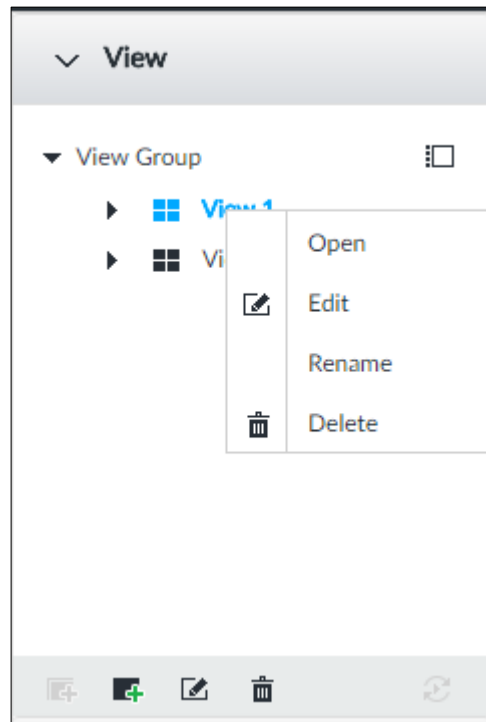
Operation	Description
Delete View group	 <p>Once you delete view group, all views under current view group will be deleted at the same time. Please be careful!</p> <ul style="list-style-type: none"> <li>• Select view group and click .</li> <li>• Right-click view group and then select <b>Delete</b>.</li> </ul>

Figure 7-5 Rename



## 7.1.1.2 View

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

### 7.1.1.2.1 Create View


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

## Preparation

Remote device has been added. Refer to "5.4.2 Adding Remote Device" for detailed information.

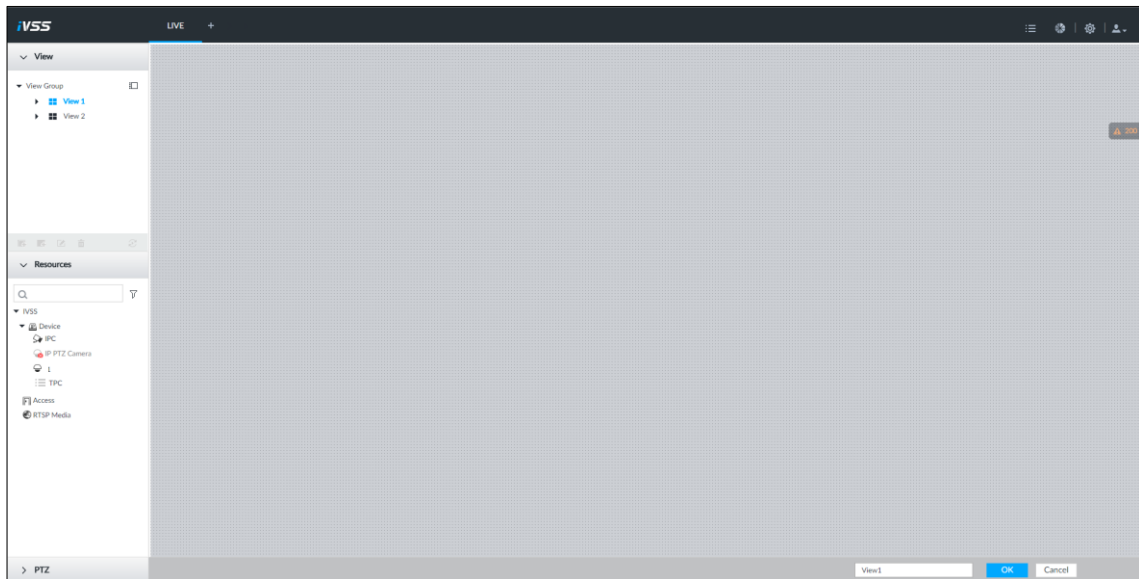
## Create View

Step 1 Follow the steps listed below to create view.

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


The **Edit** interface is displayed. See Figure 7-6.

Figure 7-6 Edit



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

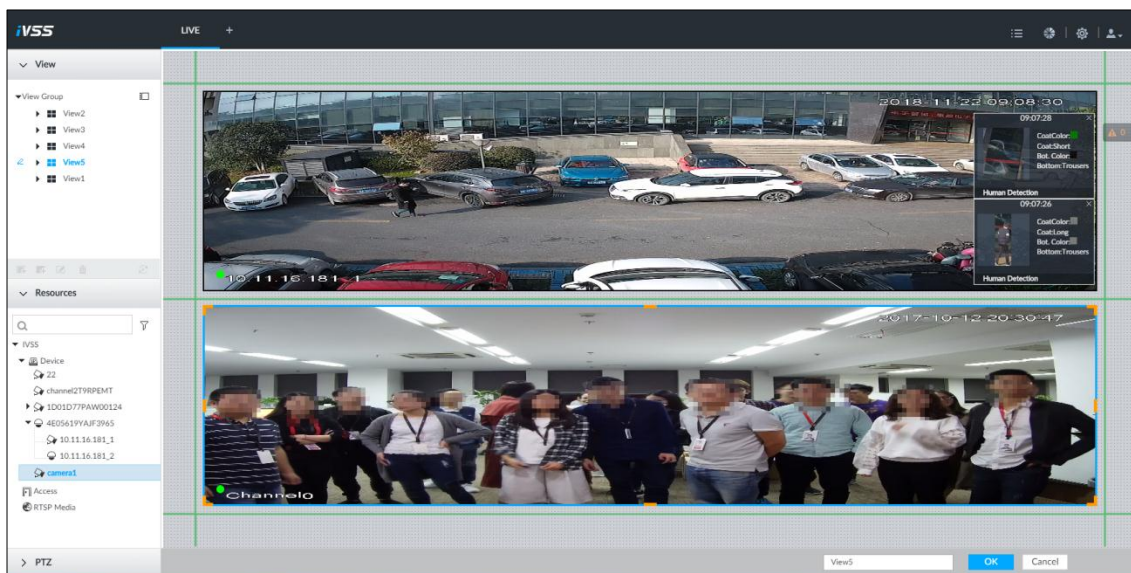
After one remote device is added, layout grid is displayed. See Figure 7-7.

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



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

Figure 7-7 Edit view



**Step 3** Set view name.

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

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

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

## Operation

After creating view, view be edited, enabled, renamed or deleted. Refer to Table 7-3 for detailed information.

Table 7-3 View





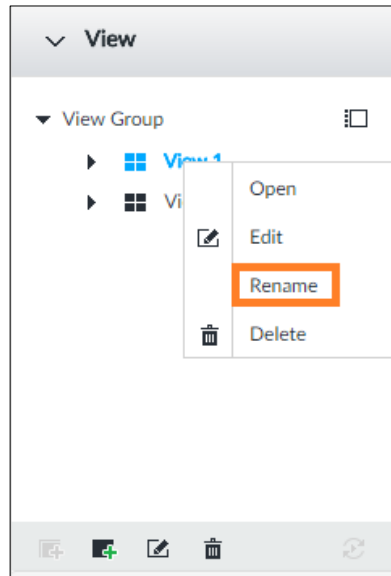
Operation	Description
Edit view	Edit remote device in the view, window layout and view name. Refer to "7.1.1.2.2 Edit View" for detailed information.
Enable view	After enabling view, view real-time image of remote device in the view. Refer to "7.1.1.2.3 Enable View" for detailed information.
Rename view	<ul style="list-style-type: none"> <li>Select a view group and then click . Set view group name and click any spare panel.</li> <li>Right-click view and select Rename. See Figure 7-8. Set view name and click any spare panel.</li> </ul>
Delete view	<ul style="list-style-type: none"> <li>Delete: Select a view and then click , or right-click view and then select <b>Delete</b>.</li> <li>Batch delete: Click , select views you want to delete and then click .</li> </ul>

Figure 7-8 Menu



### 7.1.1.2.2 Edit View

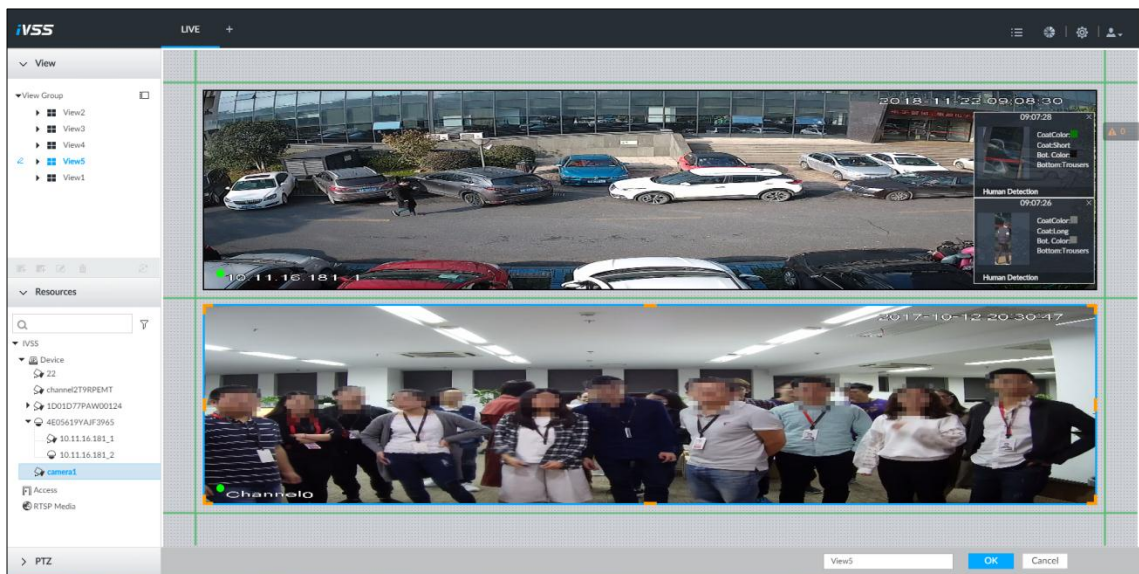
In edit view mode, it supports following functions:

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


**Step 1** Right-click View and then select **Edit**.


The **Edit** interface is displayed. See Figure 7-9.

Figure 7-9 Edit view



**Step 2** Edit view as your requirement.

- Add remote device: Double click remote device in the resource pool, or drag the remote device to the free layout grid on the right panel.
- Delete remote device: Move the mouse to window on the right, and click  at the top right corner.
- Move window position: Select and hold on a view window, move it to the proper position and release mouse.

- Change window position: Select and hold on one view window and then drag to another view window.
- Change window size: Move your mouse to the orange panel on the window (such as ). Press and drag the view window after you see the arrow icon.
- Modify view name: Set view name on .



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

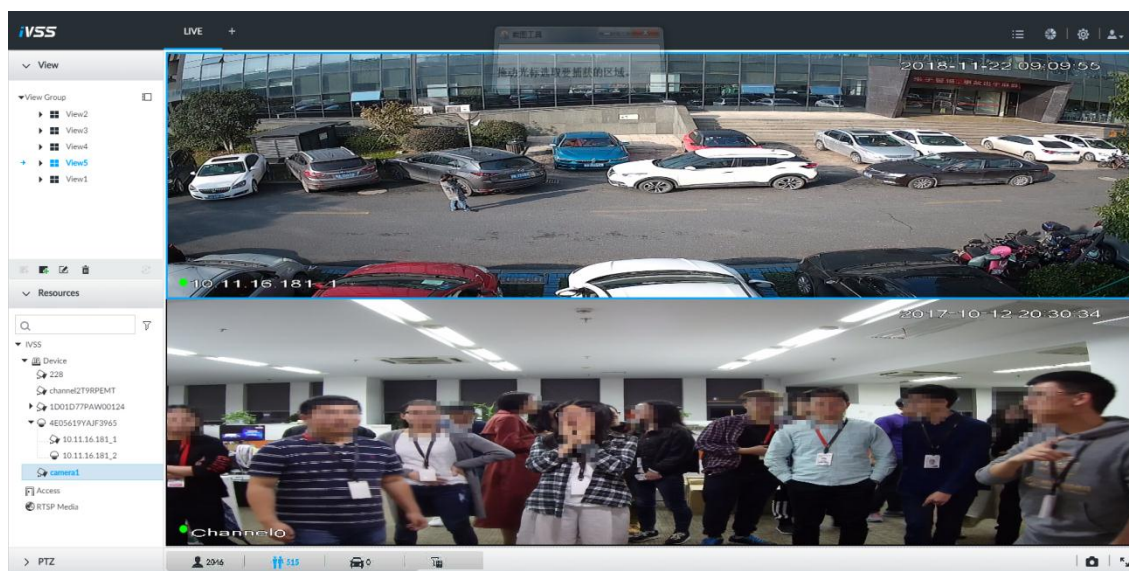
**Step 3** Click **OK** to save the configuration.

Device pops up successfully operated.

### 7.1.1.2.3 Enable View

Right-click the view and select **Open**, or double-click view. The view window is displayed. See Figure 7-10.

Figure 7-10 View window






When enabling the view, you can change video position, zoom video window. Refer to 0 for detailed information.



- When adjusting view window position, drag the view window to the layout grid of the green background color. You cannot drag the view window to the grid of red background color.
- Move the mouse to view window. Window task column is displayed to snapshot, enable record and turn off view window. Refer to "7.1.1.3.2 Window task column" for detailed information.
- Right-click view window, you can switch bit streams, set digital zoom. Refer to "7.1.1.3.3 Shortcut menu" for detailed information.

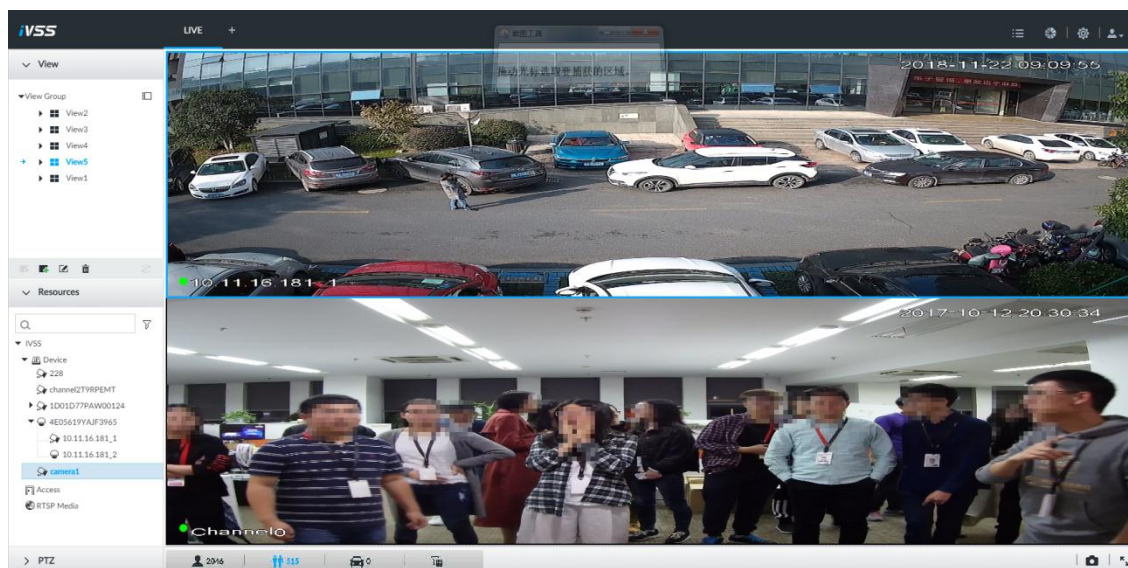
Table 7-4 View function

Operation	Description
Exchange window position	<p>Press one view window and drag it to another view window, it is to exchange these view window position.</p>  <p>The exchanging window position operation is valid only once. Disable and then enable view again, the view window restores original position. If you want to change view window position permanently, go to the view edit mode to set. Refer to "7.1.1.2.2 Edit View" for detailed information.</p>
Zoom in video window	<ul style="list-style-type: none"> <li>Once current view window amount is too much (more than 9), click one view window, device displays current view window at the center of the window in the zoom in mode. Click any other blank position, you can view window restores original size.</li> <li>Double click a view window, device displays view window at one window. Double click view window again or click any blank position, the view window restores original size.</li> </ul>
Add view window	<p>In the resource pool, double click the remote device or drag the remote device to the right panel, you can add remote device to current view.</p> <p>Drag the remote device to the view window to replace the original remote device.</p>  <p>The modified view layout is valid only for once if you do not click <b>OK</b> button. Close and enable view again, the view layout restores original layout.</p>
Close view window	<p>Move the mouse to one view window, click  to close the view window.</p> <p>Close view window, device automatically adjusts view layout according to the rest remote device amount and play panel free space.</p>

### 7.1.1.3 View Window

Right-click the view, select **Open**, or double click view. The view window is displayed. See Figure 7-11.

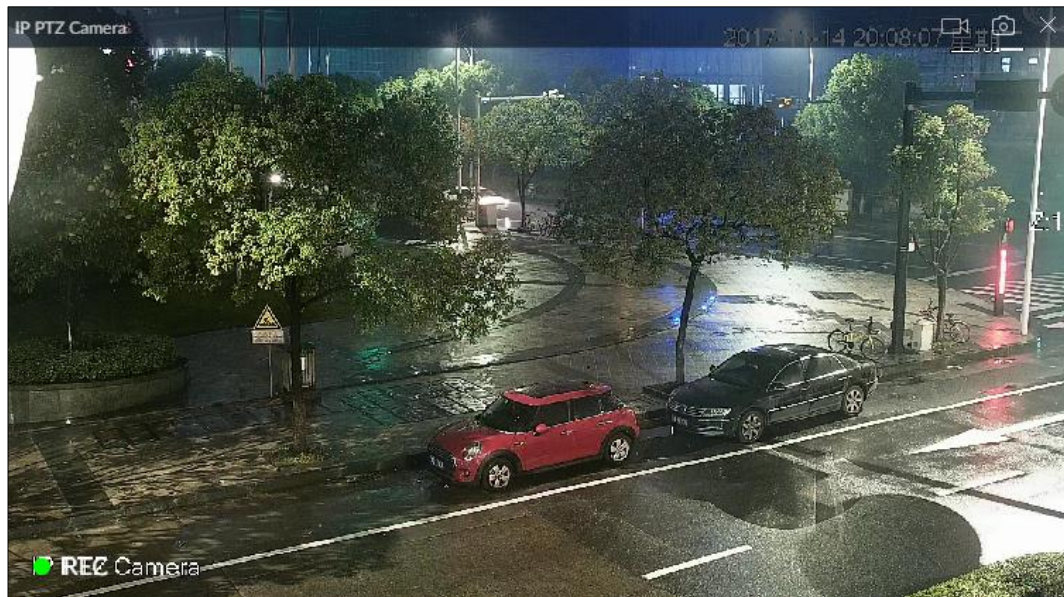
Figure 7-11 View window



### 7.1.1.3.2 Window task column





Move the mouse to view window. The window task column is displayed. See Figure 7-12.



Figure 7-12 View window



In the view window task column, enable manual recording, snapshot or close view window. Refer to Table 7-5 for detailed information.

Table 7-5 Window task column

Operation	Description
Open Manual Video Recording	<p>Click  to start recording manually. Now the icon becomes . Click  to stop recording.</p> <p>System stops recording according to the manual record length settings if you do not click  again to stop. Refer to "8.2.2.2.5 Storage" for detailed information.</p> <p>At different interfaces, recording storage path varies.</p> <ul style="list-style-type: none"> <li>● Local Configurations               <ul style="list-style-type: none"> <li>◇ When USB storage device is connected, recordings are saved in USB storage device.</li> <li>◇ Otherwise, the recordings are saved in the device. Query or export manual recording by playback control. Refer to "7.2.1 Playing Back Recorded Video" for detailed information.</li> </ul> </li> <li>● Operate IVSS Client.                Default storage path of recording is C:/Program Files (x86)/iVSS/video. Set storage path. Refer to "8.2.2.2.5 Storage" for detailed information.</li> </ul>

Operation	Description
Snapshot	<p>Click  to snapshot.</p> <p>At different interfaces, snapshot storage path varies.</p> <ul style="list-style-type: none"> <li>• Local Configurations <ul style="list-style-type: none"> <li>◇ When USB storage device is connected, snapshots are saved in USB storage device.</li> <li>◇ Otherwise, the snapshots are saved in the device. Query or export the snapshots by playback control. Refer to "7.2.3 Playing Back Snapshots" for detailed information.</li> </ul> </li> <li>• Operate IVSS Client. Default storage path of snapshot is C:/Program Files (x86)/iVSS/pictures. Set storage path. Refer to "8.2.2.2.5 Storage" for detailed information.</li> </ul>
Close view window	Click  to close view window.

### 7.1.1.3.3 Shortcut menu

Right-click video window. The shortcut menu is displayed. See Figure 7-13. For details, see Table 7-6.

Figure 7-13 Shortcut menu

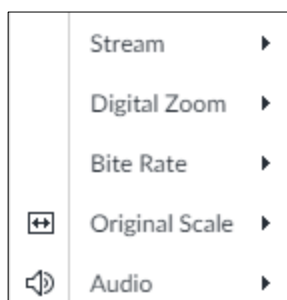
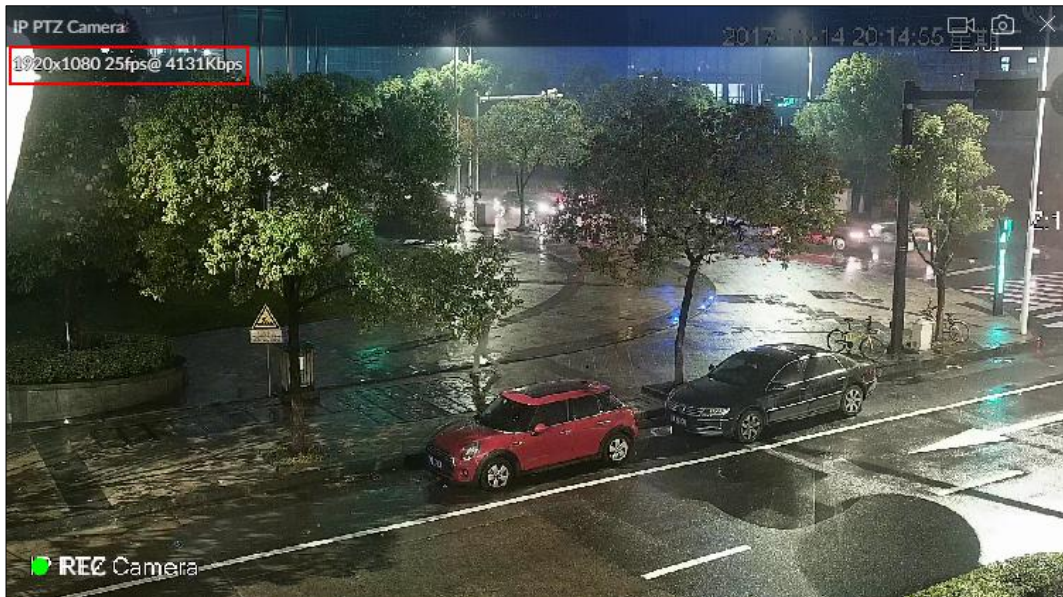


Table 7-6 Shortcut menu

Parameter	Description
Stream	It is to set current window stream. It includes main stream/sub stream 1/sub stream 2.
Digital zoom	It is to set digital zoom. Zoom in one part of live image to view details. Refer to "7.1.1.3.4 Digital zoom" for detailed information.
Bit rate	Displays real-time bit rate on the window or not. See Figure 7-14.
Original Scale	<p>It is to set video window scale.</p> <ul style="list-style-type: none"> <li>• ON: System automatically adjusts video window scale according to the resolution.</li> <li>• OFF: System automatically adjusts video window scale according to the remote device amount and the free space on the playback panel.</li> </ul>
Audio	It is to set audio output. It includes audio 1, audio 2, mixing and off.



Figure 7-14 View window



#### 7.1.1.3.4 Digital zoom

The digital zoom function allows you to zoom in a specified zone to view the video details. After enabling view, right-click **Digital Zoom** > **ON**. Select a zone in view window, and the selected zone will be zoomed in. See Figure 7-15.

- In zoom in status, press any position on the video window and then drag, you can view the zoom in effect of other zones.
- Select a zone you want to zoom in on the video window again, system zooms in the zone at the larger rate.
- Right-click mouse and then select **Digital Zoom** > **OFF**, it is to cancel zoom in effect. The video restores original effect.

Figure 7-15 Digital zoom:



## 7.1.2 Resources Pool

Displays the added remote device list. The system automatically divides into groups according to device type. See Figure 7-16. Refer to Table 7-7 for detailed information.

Figure 7-16 Resources pool

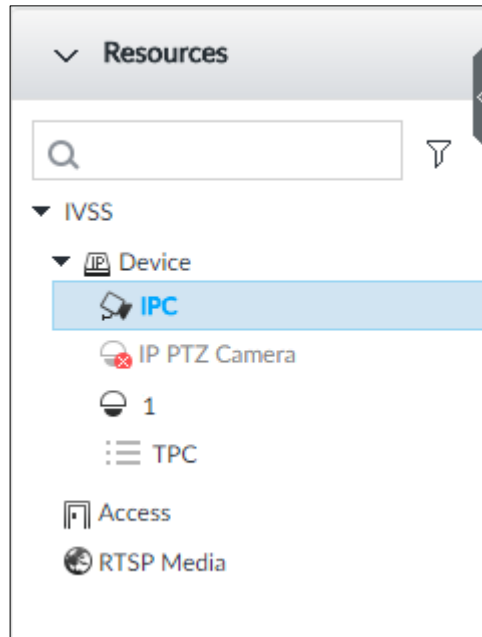









Table 7-7 Resources pool description

Operation	Description
Search device	Input key words at  <input type="text"/> , device displays the corresponding remote devices.  Support fuzzy search.
Filter device	Click  and then select all, online, offline. It is to filter the disqualified remote device.
View device status	Display remote device status on the resources pool. <ul style="list-style-type: none"> <li>If the remote device name and icon is black, it means the remote device is online. For example,  IP PTZ Camera.</li> <li>If the remote device name and icon is gray, it means the remote device is offline. For example,  IPC .</li> <li>If there is an icon  before the remote device, it means remote device is abnormal, alarming, and so on. Move the mouse to , to view the detailed information.</li> </ul>

Operation	Description
Mouse Operations	<ul style="list-style-type: none"> <li>• Move the mouse to the remote device name, you can view remote device IP address and port number.</li> <li>• On the device list, click one remote device and then press Ctrl, click other remote device, you can select several remote devices at the same time.</li> <li>• On the device list, select one remote device and then press Shift, click other remote device, select current two remote devices and all remote devices listed between them.</li> <li>• Right-click a remote device to connect to disconnect it.</li> <li>• Double click remote device or drag the remote device to the view window on the right panel, you can enter edit view interface. Edit the view. Refer to "7.1.1.2.2 Edit View" for detailed information.</li> </ul>

### 7.1.3 PTZ

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

On the Live interface, PTZ is displayed at the bottom left corner. See Figure 7-17. For details, see Table 7-8.



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

Figure 7-17 PTZ

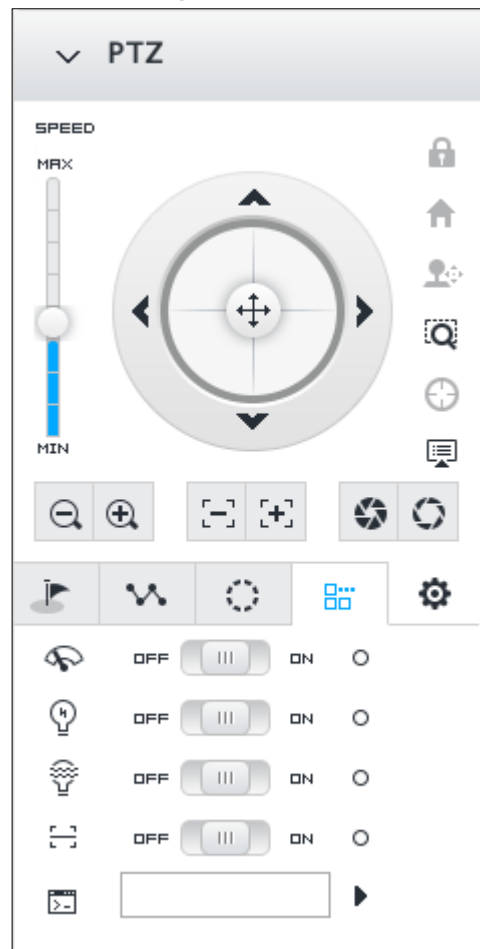




















Table 7-8 PTZ Icons description

Signal Words	Description
 <p>A vertical slider control labeled 'SPEED' at the top. The slider has a blue bar at the bottom and a white bar at the top. The top is labeled 'MAX' and the bottom is labeled 'MIN'. A white circular knob is positioned on the slider.</p>	<p>Press and hold on , and drag it up and down. It is to set PTZ speed. The higher the value is, the faster the PTZ speed is.</p>
 <p>A circular control pad with a central crosshair icon. The pad has four concentric rings and four directional arrows (up, down, left, right) pointing outwards from the center.</p>	<p>Control PTZ movement in the following ways.</p> <ul style="list-style-type: none"> <li>• Press and hold on  to control PTZ top/bottom/left/right/top left/top right/bottom left/bottom right direction.</li> <li>• Click , ,  or , it is to control PTZ top/bottom/left/right direction.</li> </ul>
 <p>A square icon with a dashed border and a small 'Q' in the center, representing 3D positioning.</p>	<p>Click to enable 3D positioning function.</p>
 <p>A square icon with a speech bubble and a list of three items, representing the PTZ menu.</p>	<p>Click to enter PTZ menu mode. Refer to "7.1.3.2 PTZ Menu Settings" for detailed information.</p>
 <p>Two square icons side-by-side: a magnifying glass with a minus sign (zoom out) and a magnifying glass with a plus sign (zoom in).</p>	<p>Zoom. Click to adjust lens zoom rate of the remote device.</p>
 <p>Two square icons side-by-side: a square with a minus sign and a square with a plus sign, representing focus adjustment.</p>	<p>Focus. Click to adjust lens focus of the remote device.</p>
 <p>Two square icons side-by-side: a camera lens icon and a circular iris icon, representing iris adjustment.</p>	<p>Iris. Click it to adjust iris size of the remote device.</p>
 <p>A horizontal row of four square icons: a flag on a pole, a zigzag line, a circular arrow, and a grid of four squares.</p>	<p>Click to enter PTZ call interface.</p> <p></p> <p>Go to the remote device to set corresponding PTZ function before you call it.</p> <ul style="list-style-type: none"> <li>• Click  to enter preset call interface. Refer to "7.1.3.3.1 Call preset" for detailed information.</li> <li>• Click  to enter call cruise interface. Refer to "7.1.3.3.2 Call cruise" for detailed information.</li> <li>• Click  to enter call pattern interface. Refer to "7.1.3.3.3 Call pattern" for detailed information.</li> </ul>


### 7.1.3.2 PTZ Menu Settings

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



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

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

**Step 2** On PTZ panel, click .

The OSD menu is displayed on the screen. See Figure 7-18. For details, see Table 7-9.

Figure 7-18 PTZ menu interface

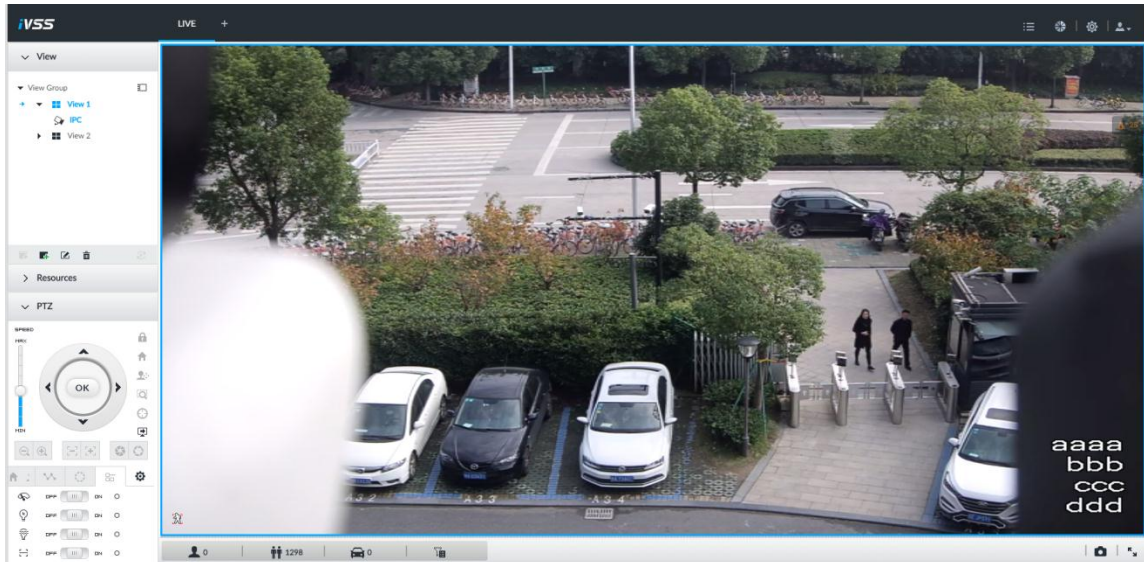









Table 7-9 PTZ menu description


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

**Step 3** Set PTZ menu parameters.

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

- Click  or , it is to select items.
- Click  or , it is to set parameters.
- Click  to confirm current items.
  - ◇ When there is sub-menu of the item on the main menu, move the mouse to the current item and then click , enter sub-menu interface.
  - ◇ Select **Back** and then click , return to upper-level menu.

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

Step 4 Click  to exit PTZ menu mode.

### 7.1.3.3 Calling PTZ Functions

It is to call PTZ function, control PTZ device to implement corresponding operations.



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

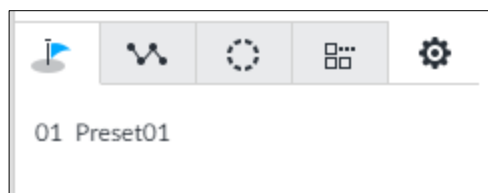
#### 7.1.3.3.1 Call preset

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

Step 1 Click .


The **Preset** interface is displayed. See Figure 7-19.

Figure 7-19 Call preset



Step 2 Move the mouse to the preset name.

The  displays at the right side of the preset name.

Step 3 Click .

PTZ device goes to the corresponding position.

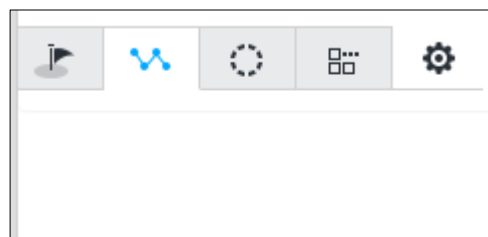
#### 7.1.3.3.2 Call cruise

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

Step 1 Click .


The call cruise interface is displayed. See Figure 7-20.

Figure 7-20 Call cruise




Step 2 Move the mouse to the cruise name.

The  displays at the right side of the cruise name.

Step 3 Click  .

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

Step 4 Click  to stop calling cruise.

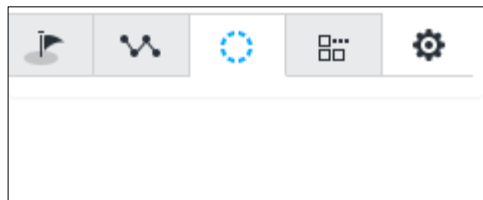
### 7.1.3.3.3 Call pattern

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


Step 1 Click  .


The call pattern interface is displayed. See Figure 7-21.

Figure 7-21 Call pattern




Step 2 Move the mouse to the pattern name.

The  displays at the right side of the pattern name.

Step 3 Click  .

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

Step 4 Click  to stop calling pattern.

## 7.2 Search

It is to search or playback the record file or image on the device. At the same time, you can export record file or image to designated storage path.

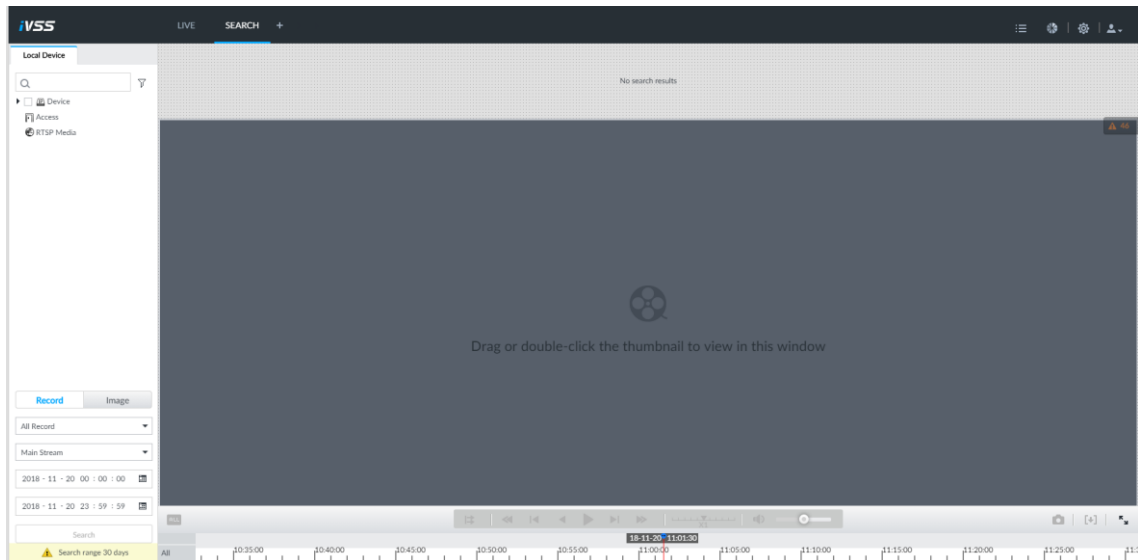
### 7.2.1 Playing Back Recorded Video

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

Step 1 On the **Live** interface, click  and then select **Search**.

Search interface is displayed. See Figure 7-22.

Figure 7-22 Search




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

**Step 3** Select record type.

The record type includes **All Record**, **Manual Record**, **Video Detect**, and **IO Alarm**.

- All record: Search all records.
- Manual record: Search the records that are manually enabled by the user. For manual record, refer to "7.1.1.3.2 Window task column" for detailed information.
- Video detect: Search the records of video detection. For setting of video detection record, refer to "8.4.3.1 Video Detect".
- IO alarm: Search local alarm linkage records. For setting of local alarm linkage record, see "8.4.2.4 Configuring Device Alarm".

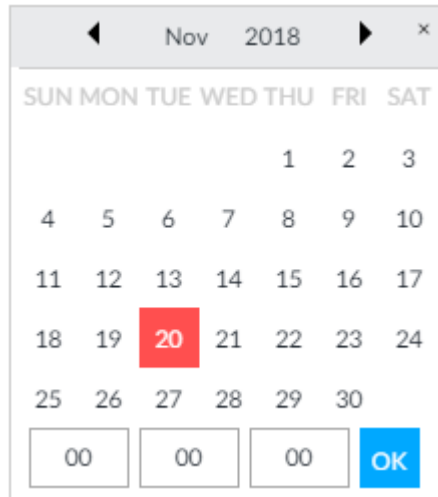
**Step 4** Set search time.

- Method 1: Click the date or time on the time column, change time or date value.
- Method 2: Click the date or time on the time column, use the mouse middle button to adjust time or date value.
- Method 3: Click , set date or time on the schedule, click **OK** button. See Figure 7-23.

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



Figure 7-23 Schedule interface



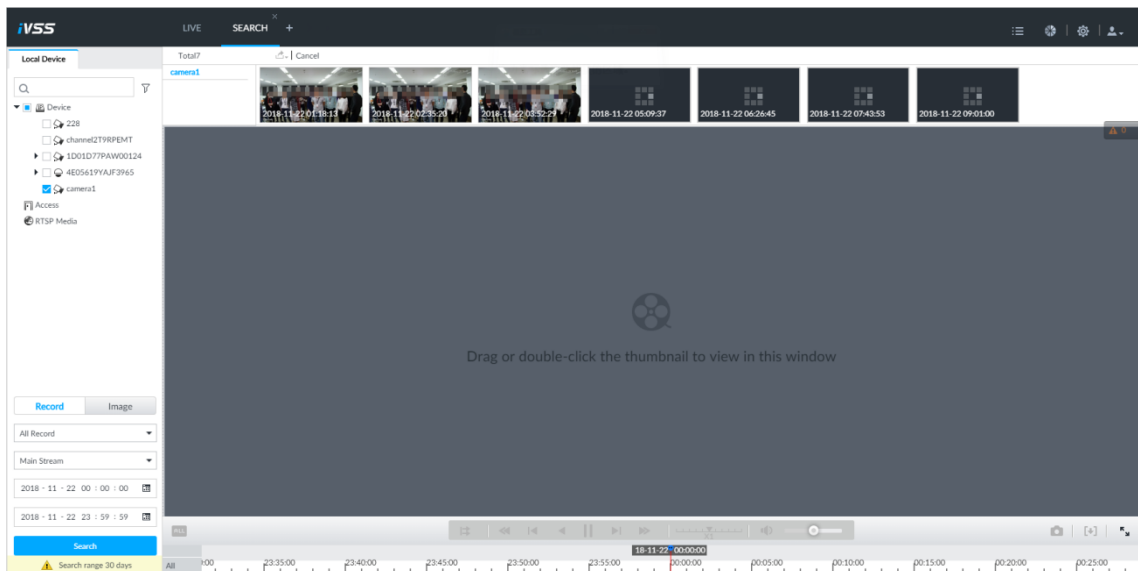
**Step 5** Click **Search**.

The record thumbnail is at the top of the remote device, and the time bar displays the record period (green color means there is a record). See Figure 7-24.



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

Figure 7-24 Search result



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

Device begins playing the record. See Figure 7-25. Refer to Table 7-10 for detailed information.



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

Figure 7-25 Search (2)

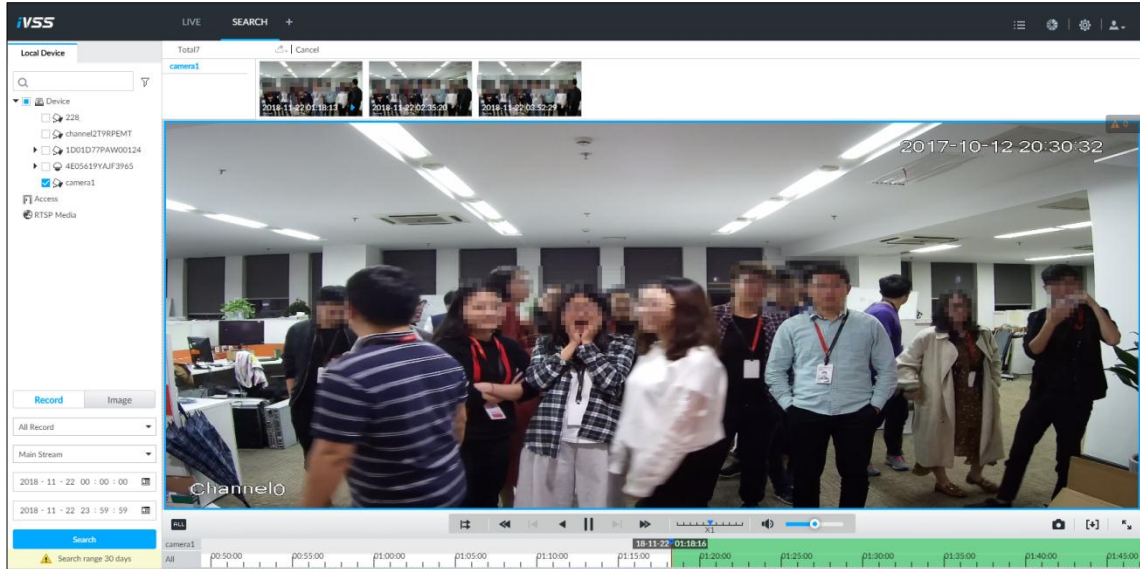













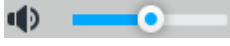





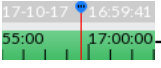
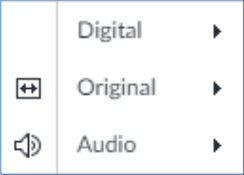



Table 7-10 Search icons description

Icon	Description
	<p>Click to synchronize playback mode. You can use the playback control icon to control several windows, such as fast forward/backward at the same time.</p> <p>Click  to cancel synchronization operation.</p>
	<p>Play back several record files at the same time. Click the icon to switch to time synchronization mode. All other windows play the video file of the same time of current window.</p> <p>Click  to cancel time synchronization.</p> <p></p> <p>Click , system enables synchronization operation function. If you want to cancel synchronization, click .</p>
	<p>Click to play back video file at slow speed.</p> <p>The slow speed includes <math>\times 1/2</math>, <math>\times 1/4</math>, <math>\times 1/8</math>, and <math>\times 1/16</math>. Click the icon once, the playback speed degrades one level.</p>
	<p>Click to switch to frame by frame backward playback.</p> <p></p> <p>It is only valid in pause mode.</p>

Icon	Description
	Click to play backward. Now the icon becomes  . Click  to stop backward play.
	Click to start playback. Now the icon becomes  . Click  to pause playback video.
	Click to switch to frame by frame playback.  It is only valid in pause mode.
	Click to playback at fast speed. The fast speed includes $\times 1$ , $\times 2$ , $\times 4$ , $\times 8$ , and $\times 16$ . Click the icon once, the playback speed upgrades one level.
	Displays playback speed. Drag  to the left or right, it is to playback at fast forward or fast backward.
	Click to snapshot an image.
	Click to obtain one part of record, and save it in designated storage path. Refer to "7.2.2 Clipping Recorded Video" for detailed information.
	Control volume. <ul style="list-style-type: none"> <li>• Drag  to set volume level.</li> <li>• Click  to mute. Now the icon becomes . Click  to cancel mute.</li> </ul>
	Click to playback at full screen.

Icon	Description
-	<p>Time bar. Displays record type and record file period.</p> <ul style="list-style-type: none"> <li>• There are two record file bars on the time bar. The top bar is to display record time of selected window. The bottom bar is to display record time of all selected remote devices.</li> <li>• The time bar adopts color to categorize record type. Green=Regular record. Red=Alarm record. Blank=No record.</li> </ul>  <ul style="list-style-type: none"> <li>• Time scale is to display record file date and time. System automatically adjusts time scale according to the record playback process.</li> <li>• On the time bar, you can: <ul style="list-style-type: none"> <li>◇ Click the time bar and rotate the mouse wheel button to adjust the time accuracy.</li> <li>◇ Press the time bar and then drag to the left or right. It is to move the time bar to view the hidden record time.</li> <li>◇ Drag time scale to adjust start time of record playback.</li> <li>◇ Click or drag the time scale to position where there is a record, system starts playing from the selected time.</li> <li>◇ Click or drag the time scale to position where there is no record, system stops playing record.</li> </ul> </li> </ul>
	<p>Shortcut menu: Right-click mouse on the playback window, you can view the shortcut menu.</p> <ul style="list-style-type: none"> <li>• Zoom: It is to zoom in a specified zone and view the details. Refer to "7.1.1.3.4 Digital zoom" for detailed information.</li> <li>• Original scale: It is to set view window scale. <ul style="list-style-type: none"> <li>◇ ON: System automatically adjusts video window scale according to the video resolution.</li> <li>◇ OFF: System automatically adjusts video window scale according to the remote device amount and the free space on the playback panel.</li> </ul> </li> <li>• Audio: Set audio output.</li> </ul>
	<p>Move cursor to the playback window, system pops up task column. Click the icon to close the playback window.</p>

## 7.2.2 Clipping Recorded Video

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



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

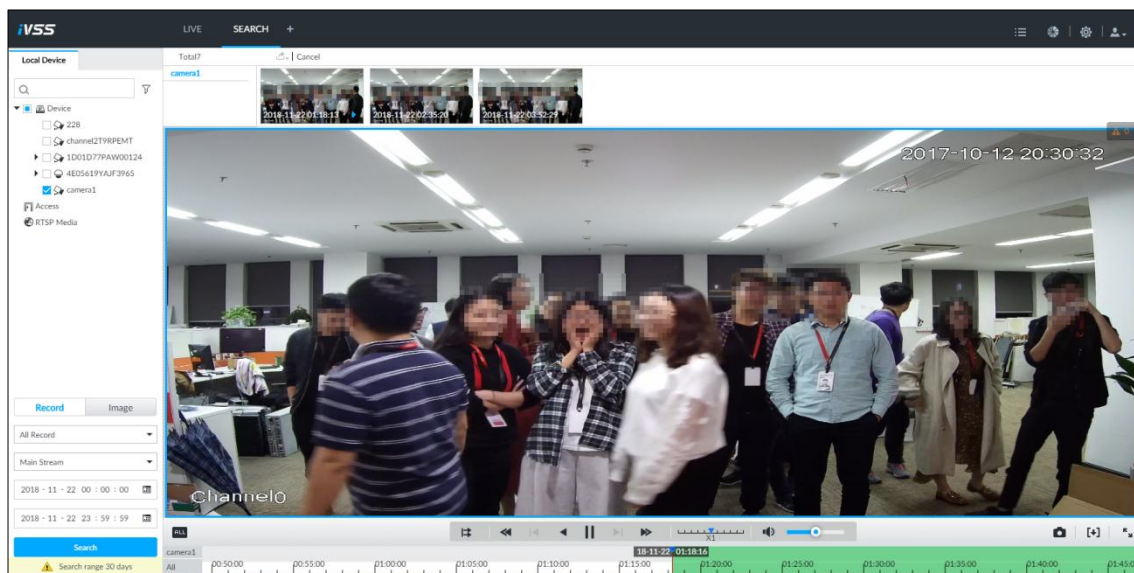
**Step 1** On the **Live** interface, click  and then select **Search**.

The **Search** interface is displayed.

**Step 2** Refer to "7.2.1 Playing Back Recorded Video" to play video file.

The video playback interface is displayed. See Figure 7-26.

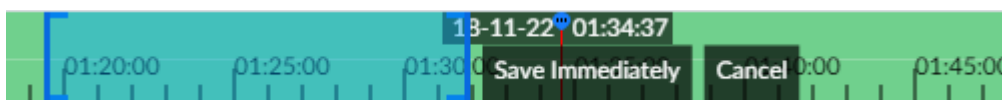
Figure 7-26 Playback



**Step 3** Click .

Video clipping frame appears on the time bar. See Figure 7-27.

Figure 7-27 Video clipping frame

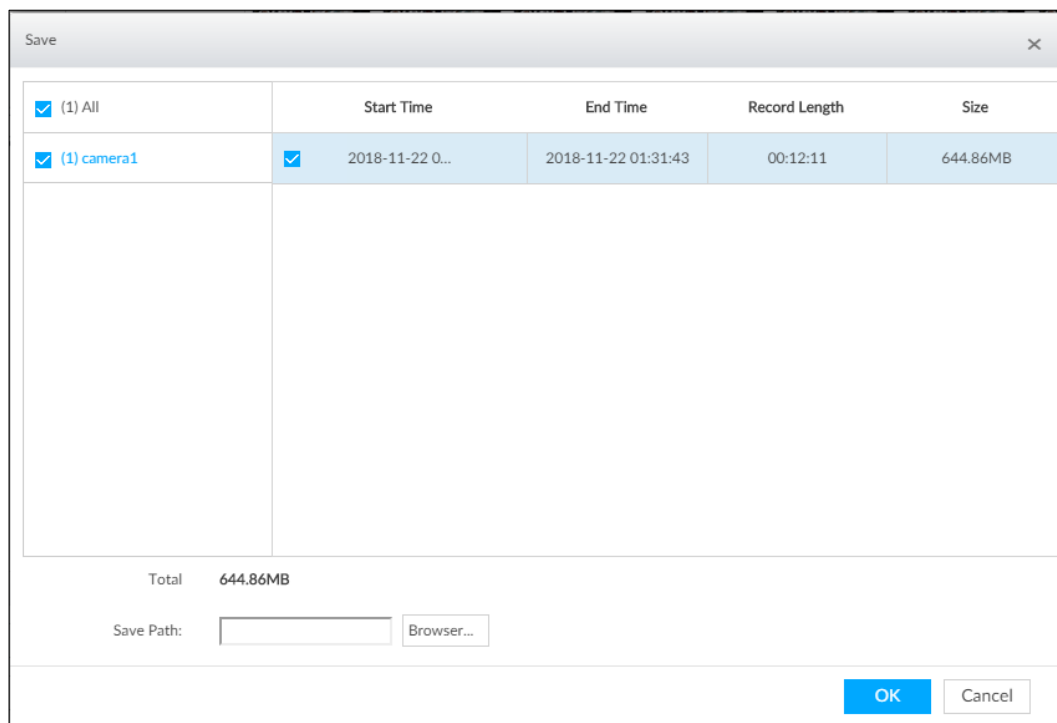


**Step 4** Press the record edit column (the blue column on Figure 7-27) and drag to the left or right, to select start time and end time of clipping.

**Step 5** Click **Save Immediately**.

The **Save** interface is displayed. See Figure 7-28.

Figure 7-28 Save



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

**Step 7** Click **OK**.

Save the clipping to designated storage path.

## 7.2.3 Playing Back Snapshots

It is to search and playback image according to remote device, image type, and snapshot time.

**Step 1** On the **Live** interface, click  and then select **Search**.

The **Search** interface is displayed.

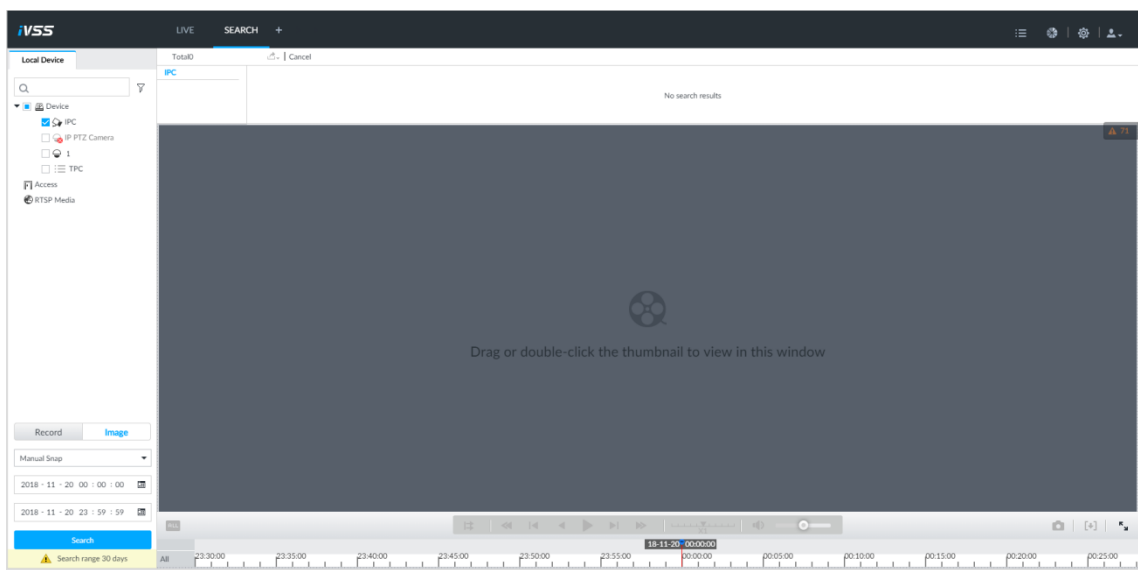
**Step 2** Select a remote device, and then click **Image**.

The **Search** interface is displayed. See Figure 7-29.




System supports maximum 1 remote device.

Figure 7-29 Image playback (1)



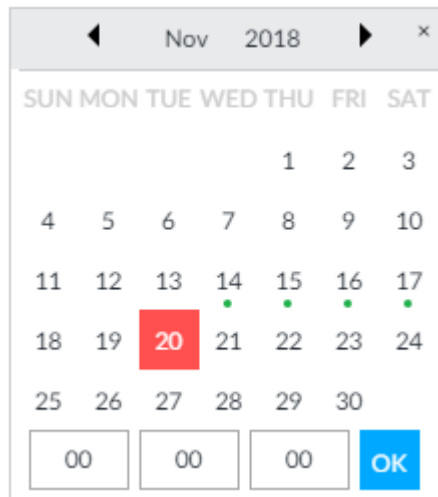
**Step 3** Select image type, including manual snap and video detect.

**Step 4** Set search time.

- Method 1: Click the date or time on the time column, change time or date value.
- Method 2: Click the date or time on the time column, use the mouse middle button to adjust time or date value.
- Method 3: Click , set date or time on the schedule, click **OK** button. See Figure 7-30.

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

Figure 7-30 Schedule interface







**Step 5** Click **Search**.

System displays searched image thumbnail. See Figure 7-31.

Figure 7-31 Image thumbnail

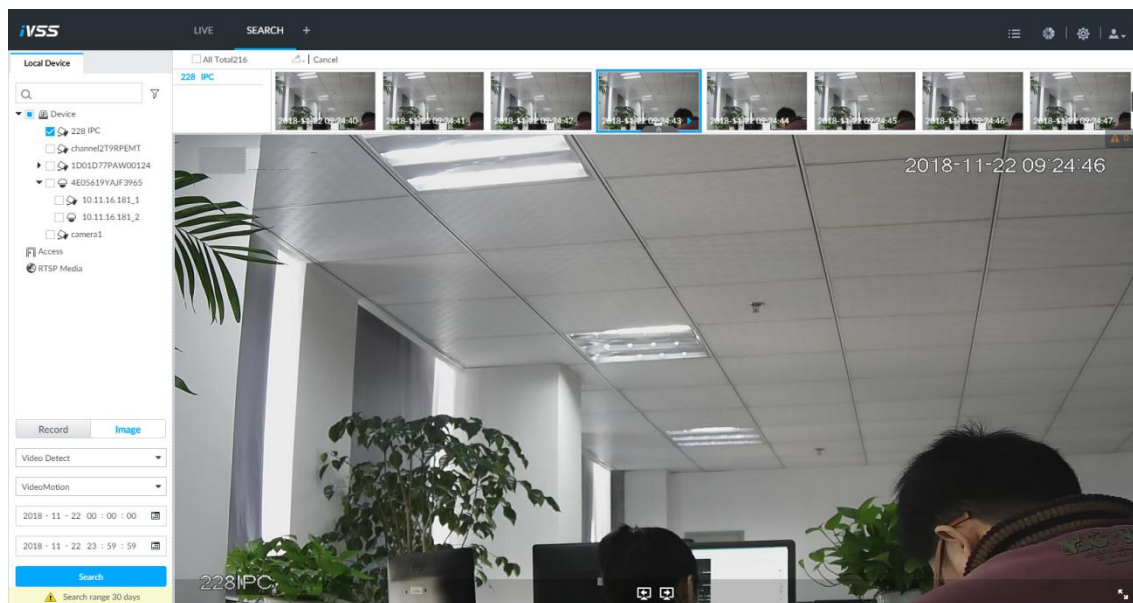


- The selected remote device is on the left panel. Click a remote device, and the image thumbnail is on the right panel.
- Click  or  to move thumbnail list, and display the hidden thumbnail.
- Move the cursor to the thumbnail, you can view remote device name, and snapshot time of the corresponding thumbnail.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

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




Device begins playing the image. See Figure 7-32. Refer to Table 7-11 for detailed information.

Figure 7-32 Image playback (2)



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

Table 7-11 Icons

Icon	Description
	Click to switch to the previous image or the next image.
	Switch image. <ul style="list-style-type: none"> <li>To play one image, click to go to the previous image or the next image.</li> <li>To play several images at the same time, click to go to the previous group or the next group.</li> </ul>
	Click to display at full screen. Click again to cancel full screen.

## 7.2.4 Exporting File

It is to export record file or image to the designated storage path.



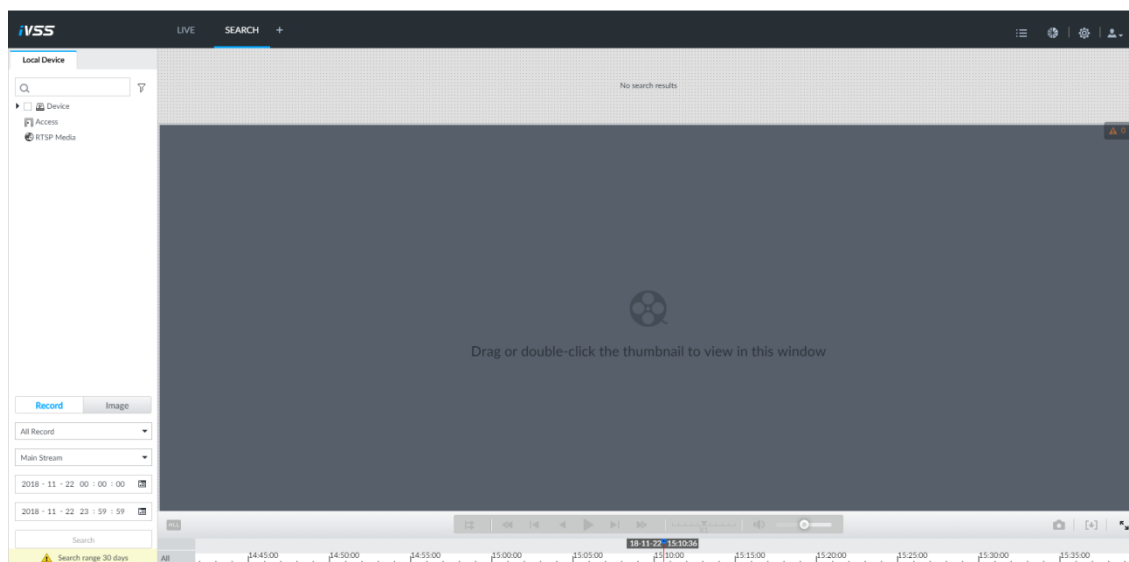
- The default record file mode is .dav and the image file mode is .jpg.
- Connect USB device to IVSS if you are on the local menu to operate.

**Step 1** On the **Live** interface, click  and then select **Search**.

The **Search** interface is displayed. See Figure 7-33.



Figure 7-33 Search (1)

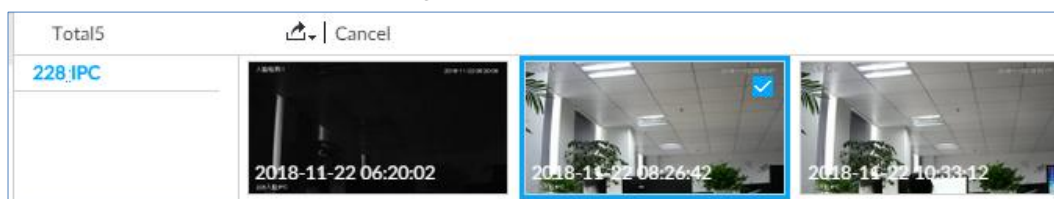


**Step 2** Search record file or image.

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

System displays searched record or image thumbnail. See Figure 7-34.

Figure 7-34 Thumbnail



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

- Move the cursor to the thumbnail and then click  to select the thumbnail.  means checked.
- Click **Cancel**, it is to cancel all record files or images.

**Step 4** Select file storage path.

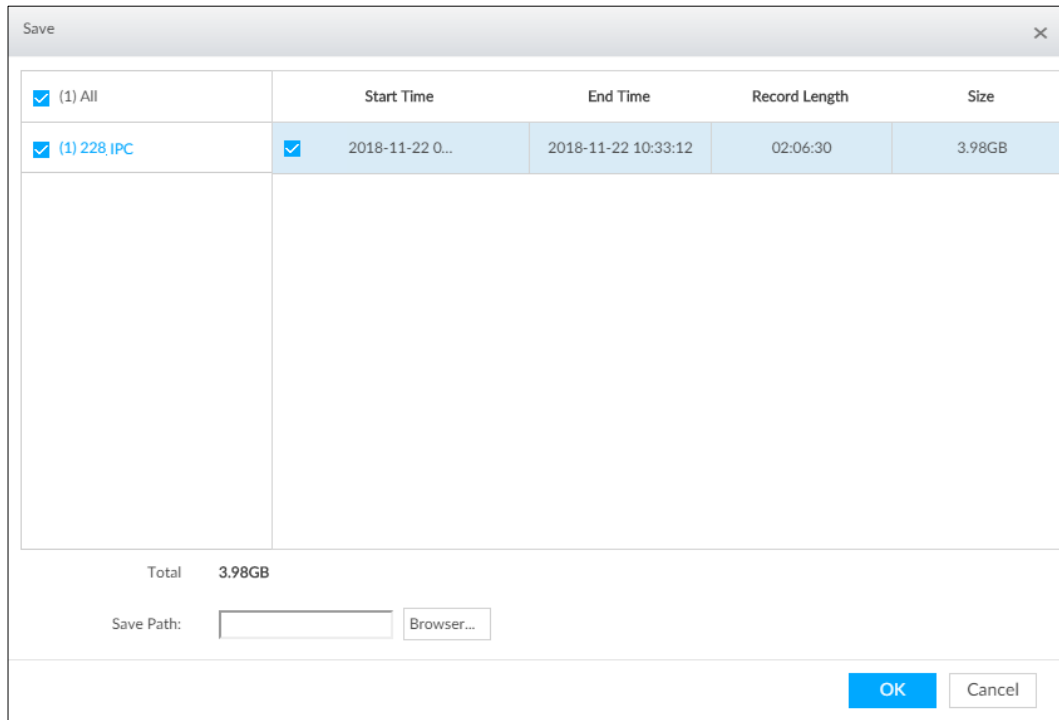
- 1) Click  and then select **Export record** or **Export image**.



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

- 2) Click **OK**.  
The **Save** interface is displayed. See Figure 7-35.

Figure 7-35 Save



- 3) Click **Browser** to select save path.



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

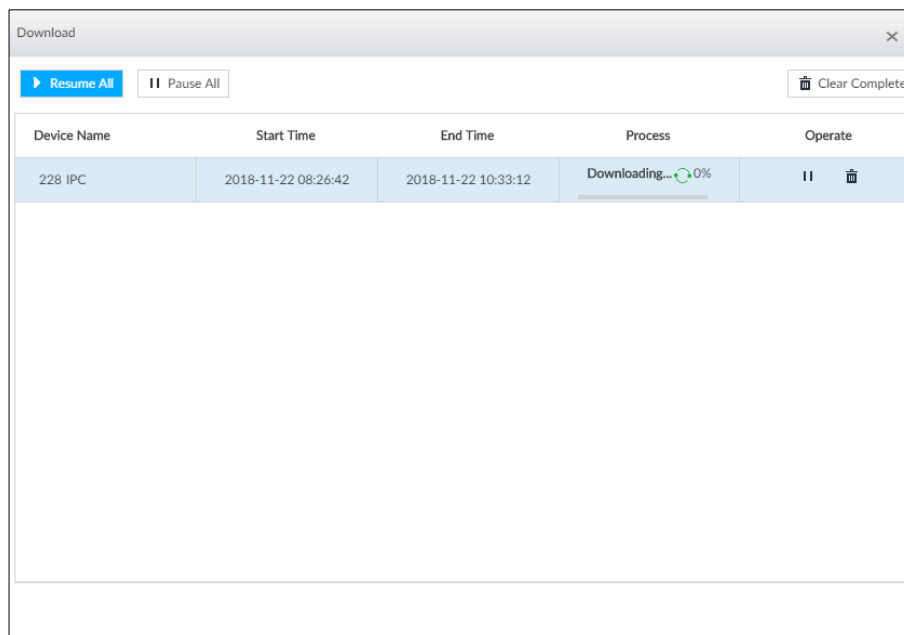
- 4) Click **OK**.

Device goes back to **Save** interface.




**Step 5** Click **OK**.

The system starts to export files. The file downloading interface is displayed. See Figure 7-36.

Figure 7-36 Download




- Click **Pause all** to pause all download tasks. Click **Start all** to resume download tasks.

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

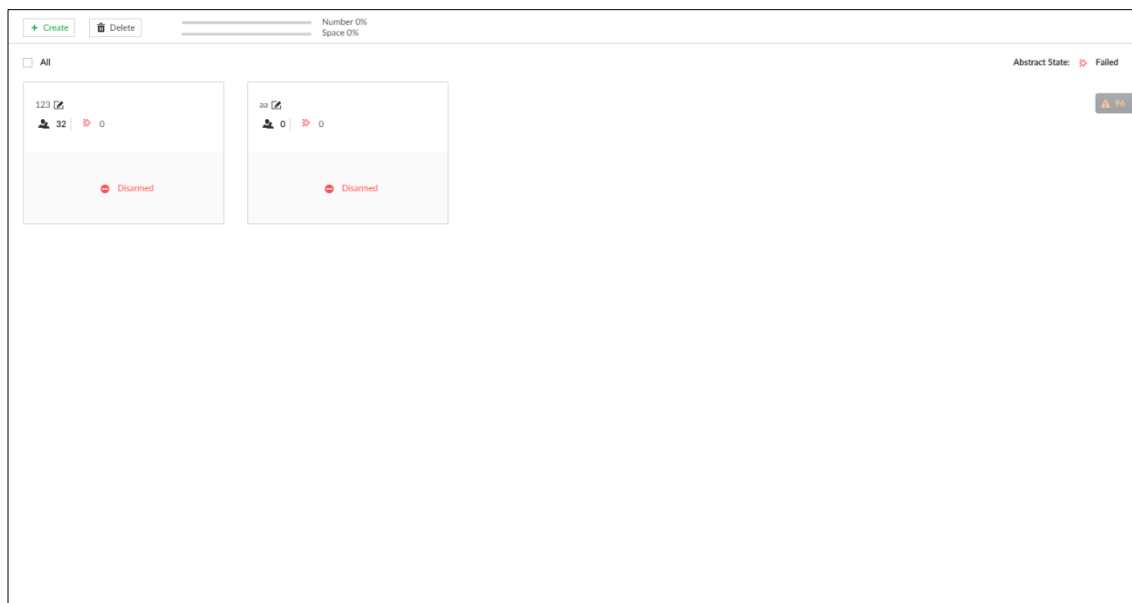
## 7.3 File Management

It is to add face image to the face database. It is to manage and maintain the human face images to guarantee information is correct.


On the **Live** interface, click , select **File > Face Database**. The **Face Database** interface is displayed. Double click a face database to show it. See Figure 7-37.

At **Face Database** interface, edit face image information, copy face image to other databases or delete face image.

Figure 7-37 Face database

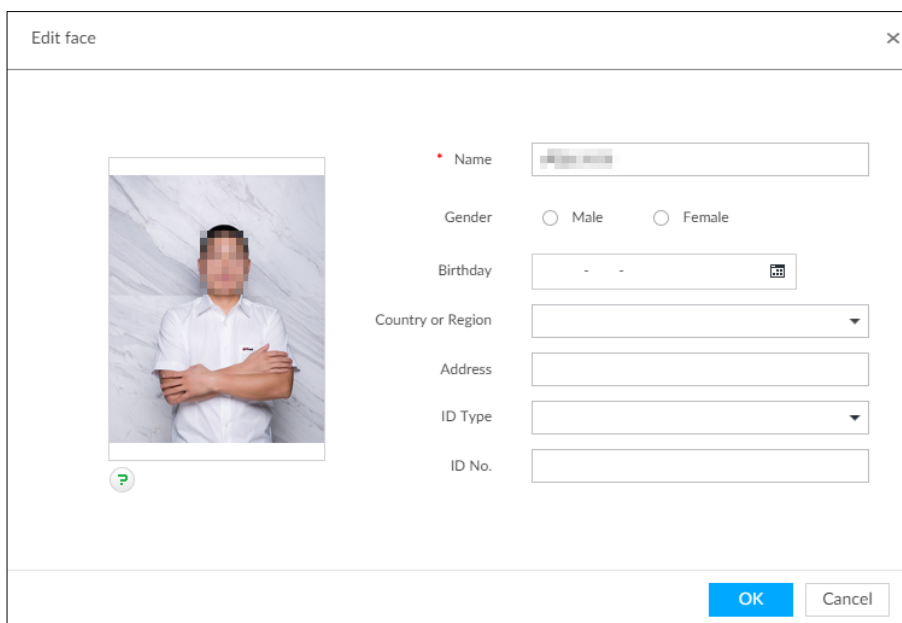


### 7.3.2 Editing Face Image

Step 1 Enter face database, move the cursor to the face image and then click .

The **Edit face** interface is displayed. See Figure 7-38.

Figure 7-38 Edit face



The 'Edit face' dialog box contains the following fields and controls:

- Name:
- Gender:  Male  Female
- Birthday:
- Country or Region:
- Address:
- ID Type:
- ID No.:
- Buttons:

Step 2 Change face information according to your actual situation.

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

### 7.3.3 Copying Face Image

Step 1 Enter face database, move the cursor to the face image and then click .

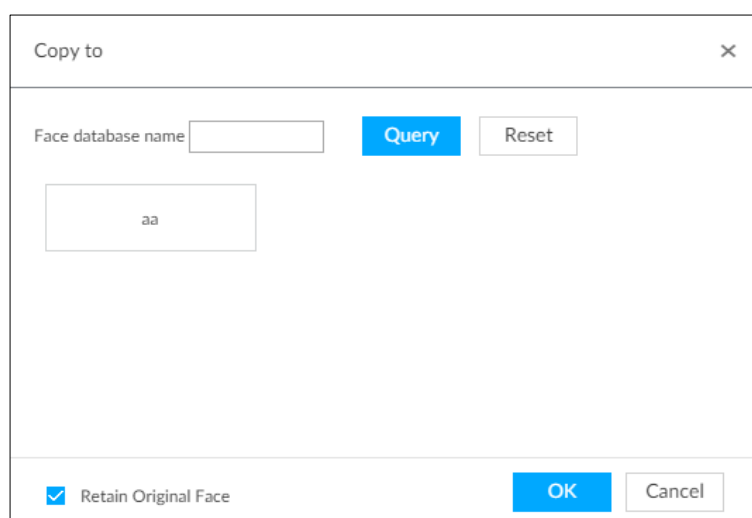


- You can select several face images at the same time.
- Check **All** button to select all face images on current page.

Step 2 Click **Copy to**.

The **Copy to** interface is displayed. See Figure 7-39.

Figure 7-39 Copy to




The 'Copy to' dialog box contains the following elements:

- Face database name:
- Buttons:
- List box: aa
- Checkbox:  Retain Original Face
- Buttons:

Step 3 Select the face database to receive the image.





- You can select several face images at the same time. Blue means it is selected.  
For example, .
- Enter face database name in Face database name text box, and click **Query** to search it. After face database name is entered, click **Reset** to clear the entered content.
- Select **Retain Original Face** to retain face images in the current face database. It is selected by default.

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

### 7.3.4 Deleting Face Image

Enter face database, and delete the created human face image.

- Delete: Move the cursor to the face image and click  at the top right corner of the face image to delete it.
- Batch delete:
  - ◇ Move the cursor to the face image and then click  at the top left corner of the several human face images. Click **Delete** to delete the selected human face images.
  - ◇ Check **All** box and then click **Delete** to delete all human face images on the current page.

## 7.4 Alarm List


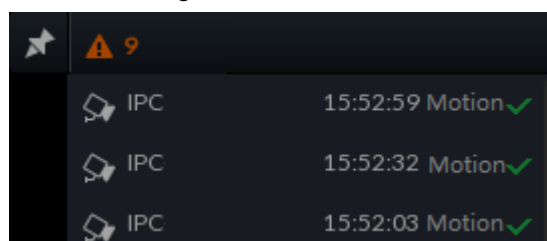


Click  to display alarm list. See Figure 7-40. It is to view alarm device name, alarm time and alarm type.

Figure 7-40 Alarm list



Alarm Device	Alarm Time	Alarm Type
IPC	15:52:59	Motion ✓
IPC	15:52:32	Motion ✓
IPC	15:52:03	Motion ✓

- Number 9 is the number of alarm event to be processed. The value changes according to alarm amount. It displays maximum 200 unprocessed alarm events.
- Click  to lock alarm list. The alarm list is open and cannot hide. Click the icon again to cancel lock function. Move the cursor to other position, and the alarm list displays for a period of time and then automatically hides.
- Click  to confirm alarm event. The confirmed event will be removed from the alarm list.
- Click the alarm event on the alarm list. The device displays the 20 seconds video before and after the alarm event occurred. See Figure 7-41.




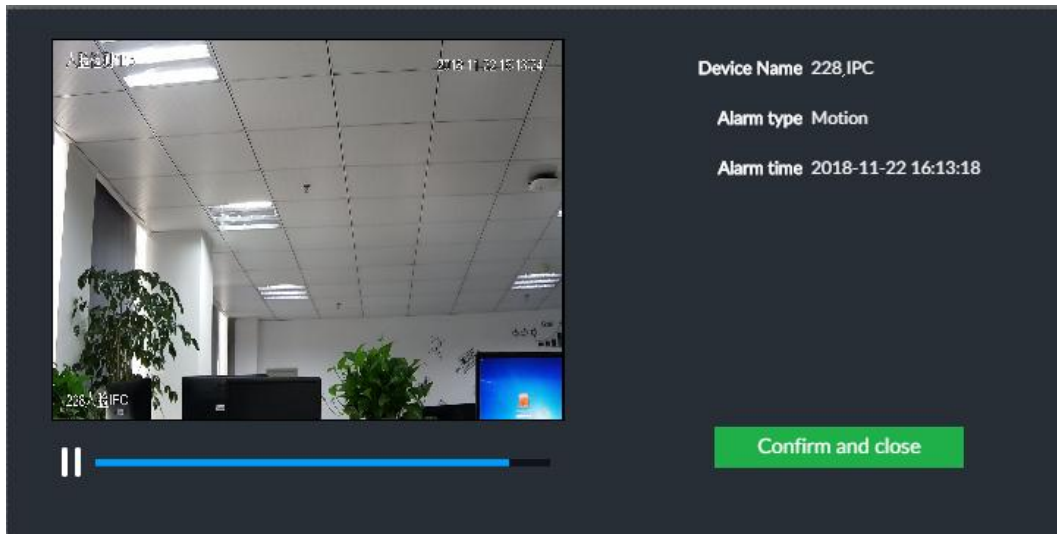
- ◇ Click  to pause play. Now the icon becomes . Click  again to continue to play.
- ◇ Click **OK and close**, confirm the alarm event and then exit the interface.

Figure 7-41 Alarm video



## 7.5 Display Management


It is to enable connected display or lock the screen.

### 7.5.1 Multiple-screen Control

Device can connect to multiple displays at the same time. You can select a display you want to use.





- The multiple-screen control function is for local menu only.
- Enter **Display Output** interface, you can enable a display or set its resolution. Refer to "8.8.3 Display" for detailed information.
- The interface may vary since the connected display amount is not the same.

Click . The **Display** interface is displayed. See Figure 7-42.

- SN 1–3 represent displays connected to HDMI 1–HDMI 3. The main screen refers to the device connected to VGA and HDMI 1 port (The HDMI/VGA port on Figure 7-42.). The displays connected to the HDMI 2 and HDMI 3 are the sub screens. The output interfaces of main screen and the sub screen are not the same and the supported functions are different. Refer to Table 7-12 for detailed information.
- VGA and HDMI 1 are outputting the same video source. Three HDMI ports can output different video sources.



-  means connected and enabled display.  means connected but not enabled display.



- Click  or  to disable or enable display. Device adopts main screen by default and the main screen cannot be disabled.

Figure 7-42 Display

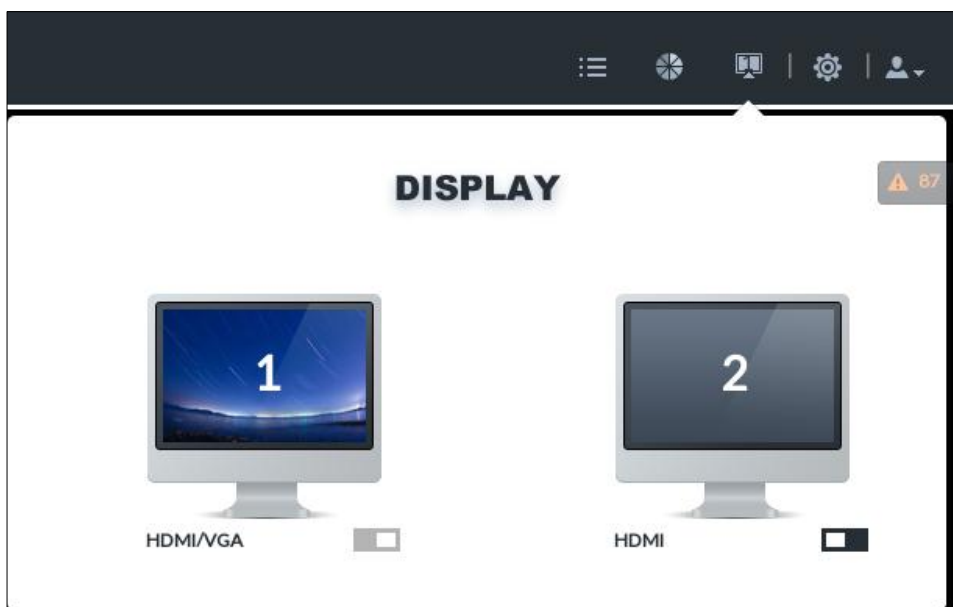



Table 7-12 Difference between main screen and sub screen

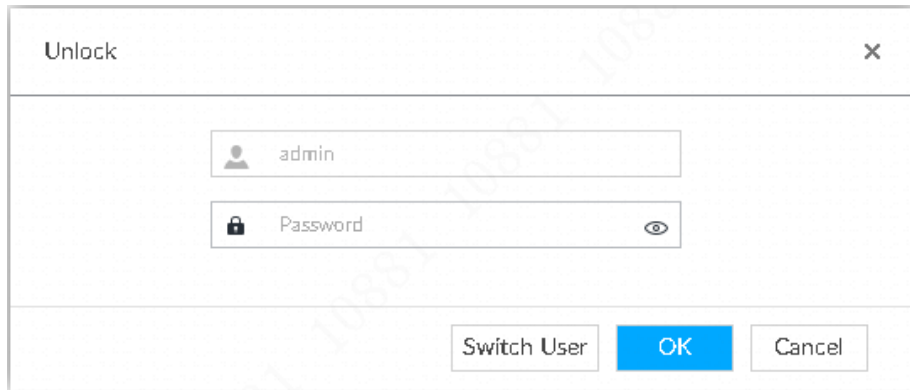
Name		Main screen	Sub screen
Function Operations	User operation (Login, log out, modify password, lock)	Supported	Supported
	Preview and Monitor	Supported	Supported
	Search	Supported	Supported
	Confirm alarm	Supported	N/A
	File Management	Supported	Supported
	Intelligent Analytics	Supported	Supported
	Multiple-screen control	Supported	N/A
	System Info	Supported	Supported
	Background Task	Supported	Supported
	Operation and Maintenance Management	Supported	Supported
	Device Operation (Reboot, shut down)	Supported	N/A
System Configuration	Device, network, event, storage, Account, security strategy, and system management.	Supported	N/A

## 7.5.2 Locking Screen

Click  and then select Lock to lock the screen. The screen stops at current interface and cannot operate other functions.

If you want to unlock the screen, click any position on the screen, enter password or user other account to login. See Figure 7-43.

Figure 7-43 Unlock screen

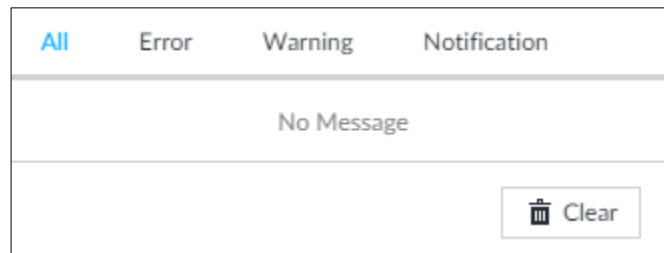



## 7.6 System Info

It is to view system information including system error, system alarm and system notification.

Click  to display background task list. See Figure 7-44.

Figure 7-44 System info



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

## 7.7 Background Task

It is to view background task running status.


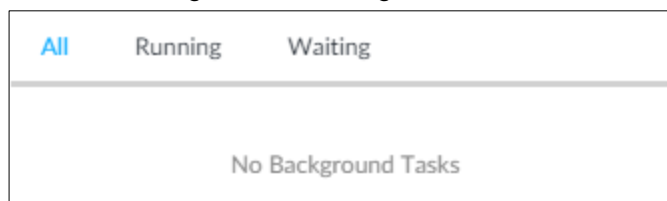
Click , device displays background task list. See Figure 7-45. Click **All**, **Running**, or **Waiting** to view the corresponding background task list.

Figure 7-45 Background task





# 8 System Configuration

This chapter is to introduce system configuration such as manage remote device, set network, set alarm event, set HDD storage, manage user information, set device security strategy, set system parameters.

## 8.1 Configuring Interface


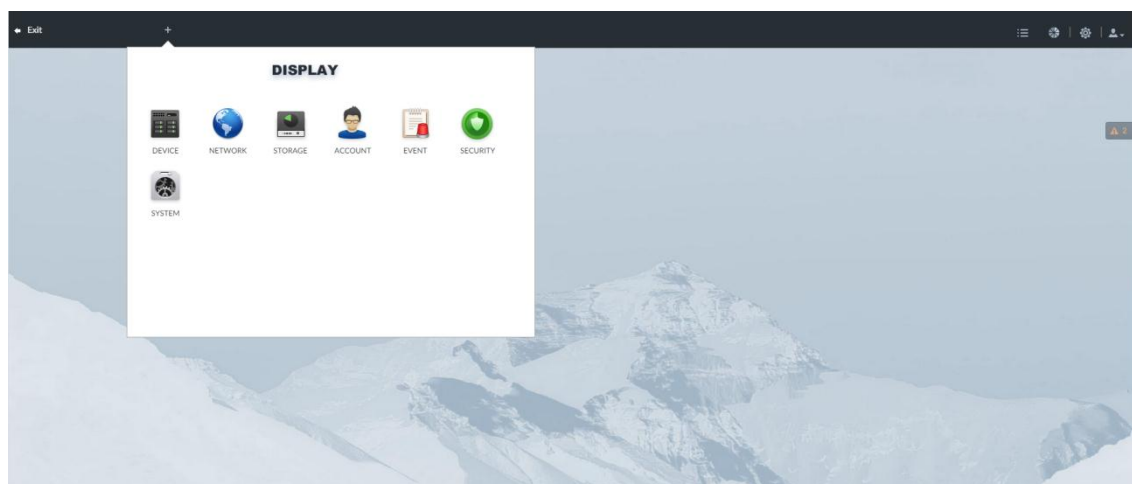


Click . The setting interface is displayed. See Figure 8-1.



Figure 8-1 Setting interface



On the setting interface, you can:

- Click  to display or hide applications interface. When all applications are open, device does not display this icon any more.
- Click the corresponding app icon to go to the corresponding interface. The task column displays current running app name. Move the cursor to the app name and then click  to close the app.
- Click **Exit** to exit the interface.

## 8.2 Device Management

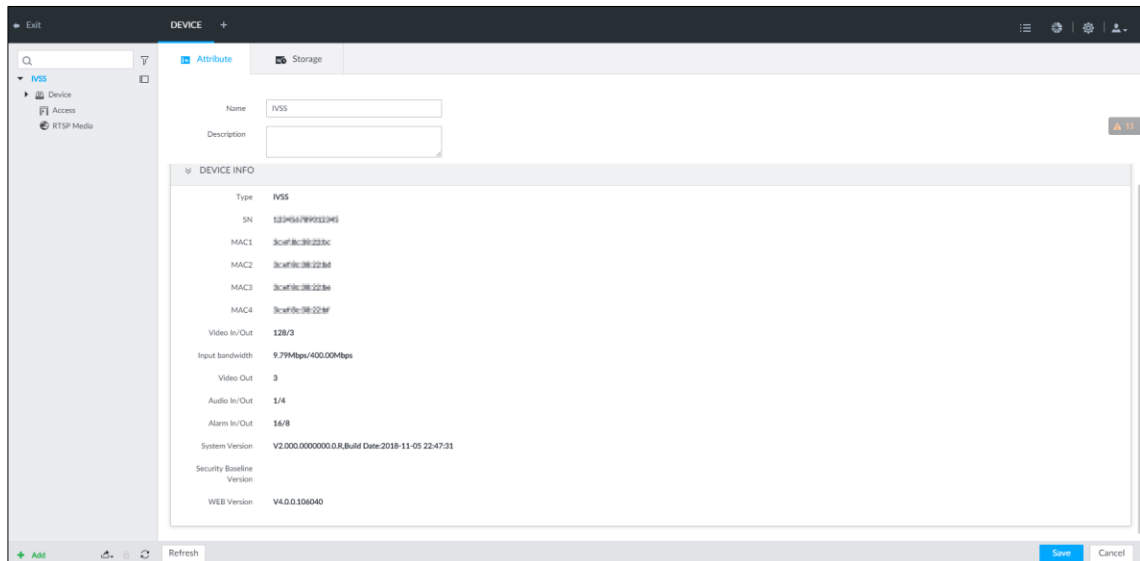
Click  or click  on the setting interface, select DEVICE. The DEVICE interface is displayed. See Figure 8-2. You can set IVSS or remote device.

- Select root node in the device list to set IVSS name and storage plan.
- Select a remote device in the device list. Set its attribute, connection, video, OSD, and storage plan.



Click **+** or click **Add** to add remote device to the system. Refer to "5.4.2 Adding Remote Device" for detailed information.

Figure 8-2 Device management



## 8.2.1 Local Device

It is to set device attribute and record storage plan.

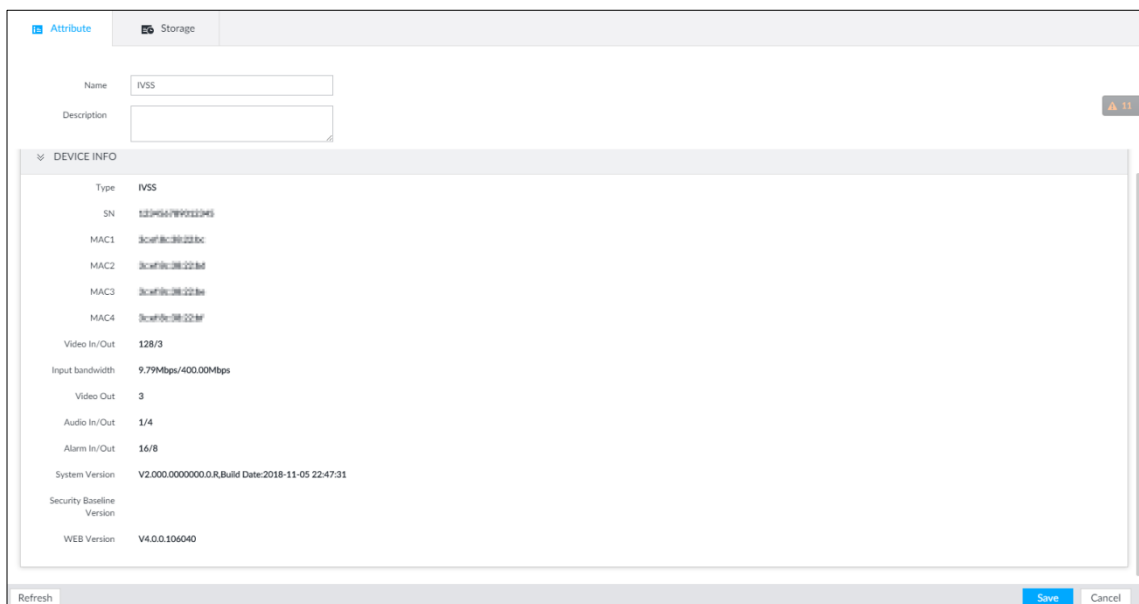
### 8.2.1.1 Set attribute parameters.

It is to set device name, view device information.

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

The **Device** interface is displayed. See Figure 8-3.

Figure 8-3 Device



**Step 2** Select the root node in the device list, and then click **Attribute** tab.

The **Attribute** interface is displayed.

**Step 3** Set parameters. For details, refer to Table 8-1.

Table 8-1 Attribute parameters description

Parameter	Description
Name	It is to set device name.
Description	It is to input device description.
Device info	Displays device info, including type, SN, MAC, video in/out, audio in/out, Alarm in/out and system version.

**Step 4** Click **Save**.

## 8.2.1.2 Storage

It is to set device global record and image storage plan according to the actual scene.



In this interface, the record and image storage plan is for all registered remote device. You can select one remote device to set specified storage plan. Refer to "8.2.2.2.5 Storage" for detailed information.

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

The Device interface is displayed.

**Step 2** Select root node in the device list and click **Storage** tab.




The storage interface is displayed. See Figure 8-4.

Figure 8-4 Storage

**Step 3** Set parameters. For details, refer to Table 8-2.

Table 8-2 Storage parameters description

Parameter	Description
-----------	-------------

Parameter		Description
Record	Record plan	It is to set record strategy. <ul style="list-style-type: none"> <li>Continuous recording: 24-hour continuous recording.</li> <li>Not recording: Device is not recording.</li> <li>Event recording: Device only records when there is corresponding alarm event.</li> </ul>
	Manual record length	It is to set manual record file length. On the <b>Live</b> interface, click  to start record. If you do not click the icon to stop record, system stops recording automatically according to the record length here.
	Storage path	Click <b>Browser</b> to set manual record storage path.  Only IVSS client supports this function.
Image	Manual snap	It is to set manual snapshot amount and snapshot speed.
	Event snap	It is to set event snapshot interval. Select <b>Customize</b> to set customized interval. The maximum internal is 3600 seconds.
	Image storage path	Click <b>Browser</b> to set snapshot image storage path.  Only IVSS client supports this function.

Step 4 Click **Save**.

## 8.2.2 Remote Device

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



Refer to "5.4.2 Adding Remote Device" for detailed information.

### 8.2.2.1 Changing IP Address

It is to change IP address of the remote device. Pay attention that the device shall have not registered to the system.

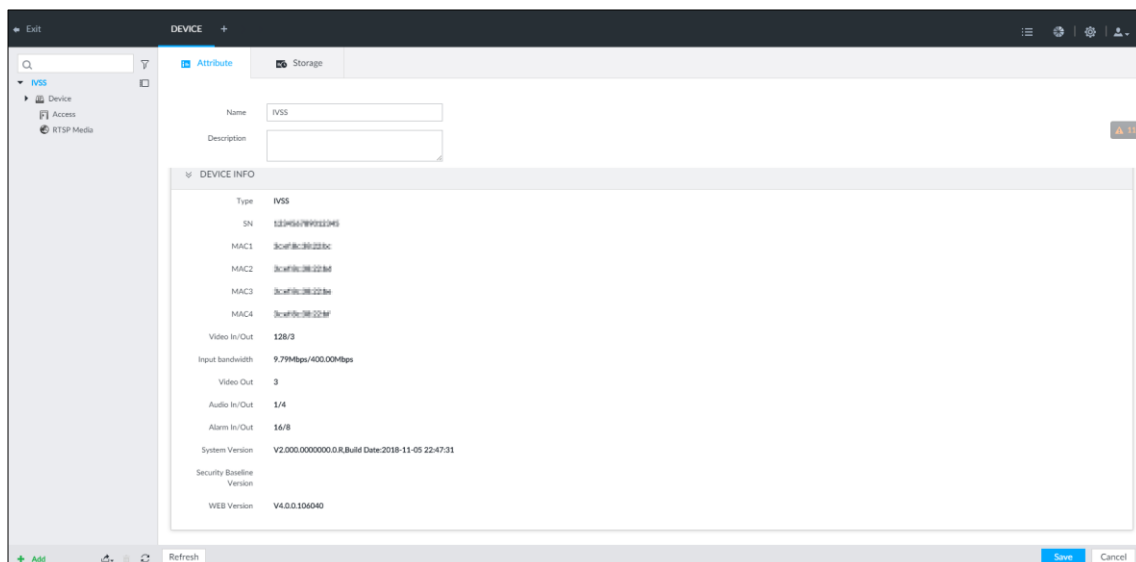


- It only supports to modify the IP address of initialized device. For remote device initialization, refer to "5.4.1 Initializing Remote Device" for detailed information.
- It only supports to modify the IP address of remote device connected with private protocol.
- Refer to "8.2.2.2.2 Setting Connection Information" to change the IP address of registered device.

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

The **Device** interface is displayed. See Figure 8-5.

Figure 8-5 Device management



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

The **Smart Add** interface is displayed.

**Step 3** Search remote device.

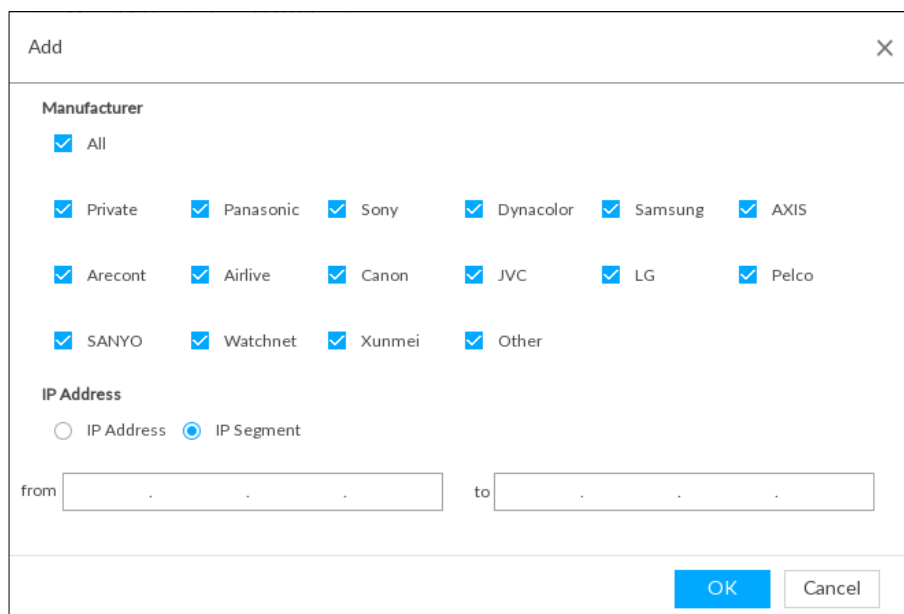


System searches the remote devices of current IP segment by default.

1) Click .

The **Add** interface is displayed. See Figure 8-6.

Figure 8-6 Add



- 2) Select manufacturer and set IP address you want to search.
  - It is to set remote device IP address. System can search the corresponding remote device.
  - It is to set remote device IP segment. System can search the remote devices of current IP segment.
- 3) Click **OK** to save the configuration. System goes back to **Device** interface.

4) Click **Start Search**.

System starts to search and displays result. See Figure 8-7.

Figure 8-7 Remote device

<input type="checkbox"/> (0)	Initialization State	Address	Product Model	Manufacturer	Product Type	Sn	Operate
<input type="checkbox"/>	✓ Initialized	172.12.4.67	IPC-HFS7229...	Private	IPC	00111ab0d2534	LIVE
<input type="checkbox"/>	✓ Initialized	172.12.108.128	H4D3PRV2	Neutral	H4D3PRV2	34084467A20...	LIVE
<input type="checkbox"/>	✓ Initialized	172.12.4.65	IP Camera	Private	IP Camera	Y3CAGL397W6...	LIVE
<input type="checkbox"/>	✓ Initialized	192.168.153.208	PC-NVR	Private	--	--	LIVE
<input type="checkbox"/>	✓ Initialized	172.12.16.128	HFD5PR1	Neutral	HFD5PR1	A178102526	LIVE
<input type="checkbox"/>	✓ Initialized	172.12.12.112	MCS7024R	Private	MCS	3102041F400...	LIVE
<input type="checkbox"/>	✓ Initialized	172.12.3.555	PI-HDW1120S...	Private	IPC	2F86C8E7A80...	LIVE
<input type="checkbox"/>	✓ Initialized	172.12.4.89	NVR	Private	NVR	5021877A200...	LIVE

Total 116 Item(s) Show up to 50

Bandwidth : 11.93Mbps/400Mbps

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

The **Modify IP** interface is displayed. See Figure 8-8.

Figure 8-8 Modify IP (1)

(1) Sn	IP Address
172.12.108.128	172.12.108.128

DHCP  Static

Static IP Address: . . .

Subnet Mask: . . .

Gateway: . . .

Incremental Value: 1

User Name: \_\_\_\_\_

Password: \_\_\_\_\_

! support Private only

Next Cancel

**Step 5** Select IP mode.

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



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

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



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

**Step 7** Click **Next** button.

System displays IP address modification interface.

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

## 8.2.2.2 Configuring Remote Devices

It is to set remote device attributes, connection information, and video parameters.



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

### 8.2.2.2.1 Setting Device Attribute

It is to set remote device name, and view device information.

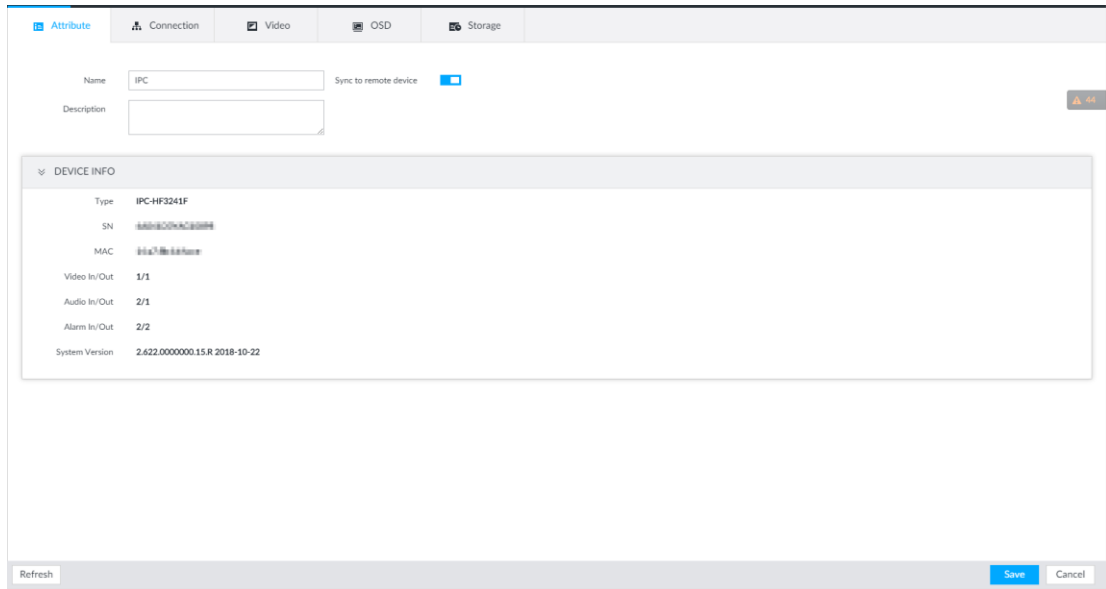
**Step 1** Click , or click  on setting interface, and then select **DEVICE**.

The **Device** interface is displayed.

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

The **Attribute** interface is displayed. See Figure 8-9.

Figure 8-9 Attribute



**Step 3** Set parameters. For details, refer to Table 8-3.

Table 8-3 Attribute parameters description

Parameter	Description
Name	It is to set remote device name. After enabling <b>Sync to remote device</b> and save the settings. It is to synchronize new name to the remote device.
Description	Input remote device description.
Device info	Displays remote device information. It includes remote device type, SN, MAC address, video in/out, audio in/out, alarm in/out, and system version.

**Step 4** Click **Save**.

#### 8.2.2.2.2 Setting Connection Information

It is to set connection information of remote device, such as IP address, and port number.

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

The **Device** interface is displayed.

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

The **Connection** interface is displayed. See Figure 8-10.



Figure 8-10 Connection information

The screenshot shows a configuration window with the following fields and values:

- Address: 172.3.66.123
- Port: 37777
- Manufacturer: Private
- Username: admin
- Password: [Redacted]
- Link Type: Self-Adaptive
- Cache Strategy: Self-Adaptive

Buttons: Refresh, Save, Cancel

**Step 3** Change IP address.

- 1) Click  of the corresponding address.

The **Modify IP** interface is displayed. See Figure 8-11.

Figure 8-11 Modify IP

The dialog box contains the following elements:

- Protocol: IPv4
- Mode:  DHCP,  Static
- IP Address: [Input field]
- Subnet Mask: 255 . 255 . 0 . 0
- Gateway: [Input field]
- Buttons: OK, Cancel

- 2) Select IP mode.

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




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

skips the conflicted IP and begins the allocation according to the incremental value.

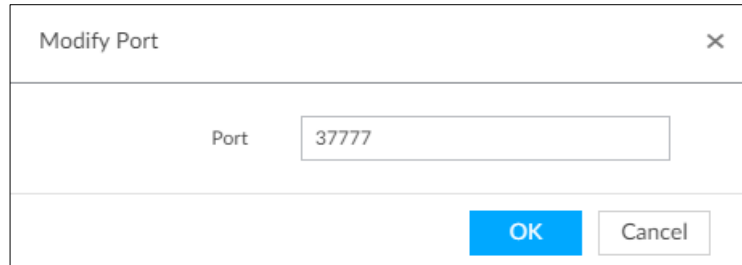
- 3) Click OK to save setting.

**Step 4** Change port number.

- 1) Click  of the corresponding port.

The **Modify Port** interface is displayed. See Figure 8-12.

Figure 8-12 Port



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

**Step 5** Set other parameters. Refer to Table 8-4 for detailed information.

Table 8-4 Connection parameters description

Parameter	Description
Manufacturer	Displays the connection protocol of the remote device.
Username	It is to input user name and password of remote device.
Password	The new password can be set from 8 characters through 32 characters and contains at least two types from number, letter and special characters (excluding "", "", ";", ":" and "&"). Enter a strong password according to the password strength indication.
Link type	Displays link type of the system and remote device. It is self-adaptive.
Cache strategy	It is to set cache strategy of remote device video stream. <ul style="list-style-type: none"> <li>• Self-adaptive: System automatically adjusts video stream cache status according to the network bandwidth.</li> <li>• Realtime: It is to guarantee video realtimeness. When the network bandwidth is not sufficient, the video may not be fluent.</li> <li>• Fluency: It is to guarantee video fluency. When the network bandwidth is not sufficient, the video may not be clear.</li> </ul>

**Step 6** Click **Save**.

### 8.2.2.2.3 Setting Video Parameters

It is to set different video parameters according to different bit stream types based on the bandwidth.

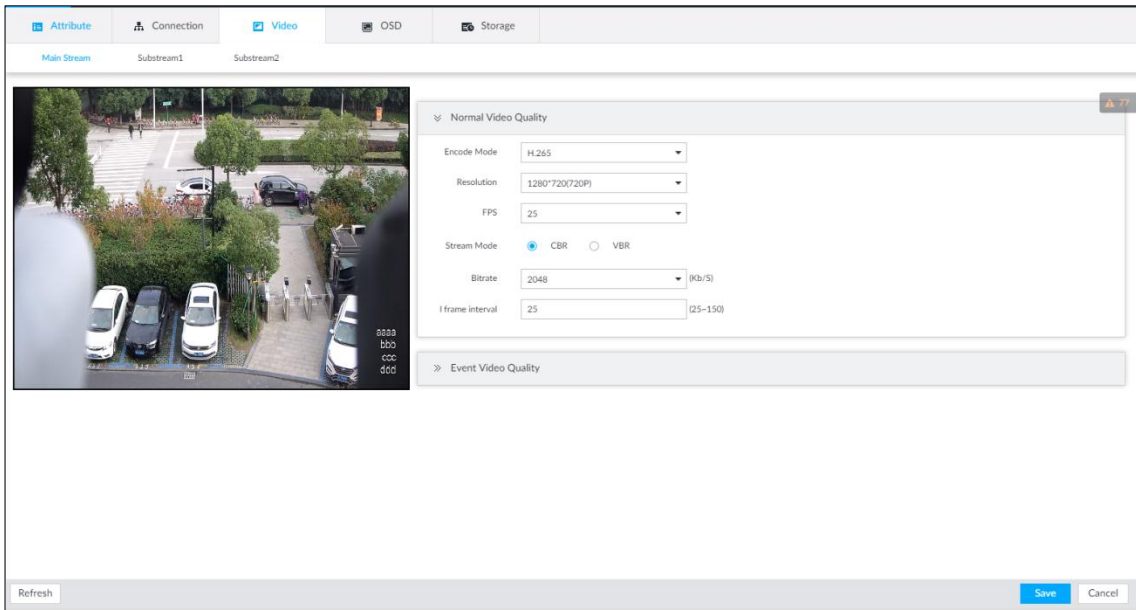
**Step 1** Click , or click  on setting interface, and then select **DEVICE**.

The **Device** interface is displayed.

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

The **Video** interface is displayed. See Figure 8-13.




Figure 8-13 Video



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

**Step 4** Set general video quality parameters. Refer to Table 8-5 for detailed information.

Table 8-5 Video parameters description

Parameter	Description
SVC	<p>Check the box to enable SVC function. Select 1 or 2 from the drop-down list on the right. The default setup is 1, there is no scaled encoding.</p> <p> SVC refers to the scaled video coding. It can split the video stream to basic stream and enhanced scale.</p>
Encode mode	<p>It is to set video encode mode.</p> <ul style="list-style-type: none"> <li>H.264: It is a highly compressed video encode/decode standard. At the same video quality, it has increased the compression rate by 2X compared with the MPEG-2.</li> <li>H.265: It is a new video encode standard coming after H.264. It has improved the complicated relationship among bit stream, encode quality, latch and algorithm on the previous standard. It can get the best encoding.</li> </ul>
Resolution	<p>It is to set video resolution. The higher the resolution is, the better the video quality is.</p> <p> Different series products support different resolutions. Refer to the actual interface for detailed information.</p>
FPS	<p>It is to set the frame amount displayed at each second. The higher the frame rate is, the more vivid and fluent the video is.</p>
Stream mode	<p>It is to set video bit stream control mode.</p> <ul style="list-style-type: none"> <li>CBR: The bit stream changes slightly. The bit stream is near the value you set here.</li> <li>VBR: The bit stream may change according to the environment.</li> </ul>
Quality	<p>It is to set video quality. It includes low, middle, high.</p> <p> It is null when the stream mode is CBR.</p>

Parameter	Description
Bitrate	<p>It is to set video bitrate.</p> <ul style="list-style-type: none"> <li>● Main Stream: In the <b>Bit Rate</b> list, select a value or enter a customized value to change the image quality. The bigger the value is, the better the image will become.</li> <li>● Sub Stream: In CBR mode, the bit stream changes around the value you set. In VBR mode, it changes according to the bit stream value, but its max value is near the specified value.</li> </ul>
I frame interval	It is to set the P frame amount between two I frames. Usually we recommend it is the 2X of the frame rate.

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



Event video quality is for main stream only.

**Step 6** Click **Save**.

#### 8.2.2.2.4 OSD

It is to overlay time information, and channel information on the video.

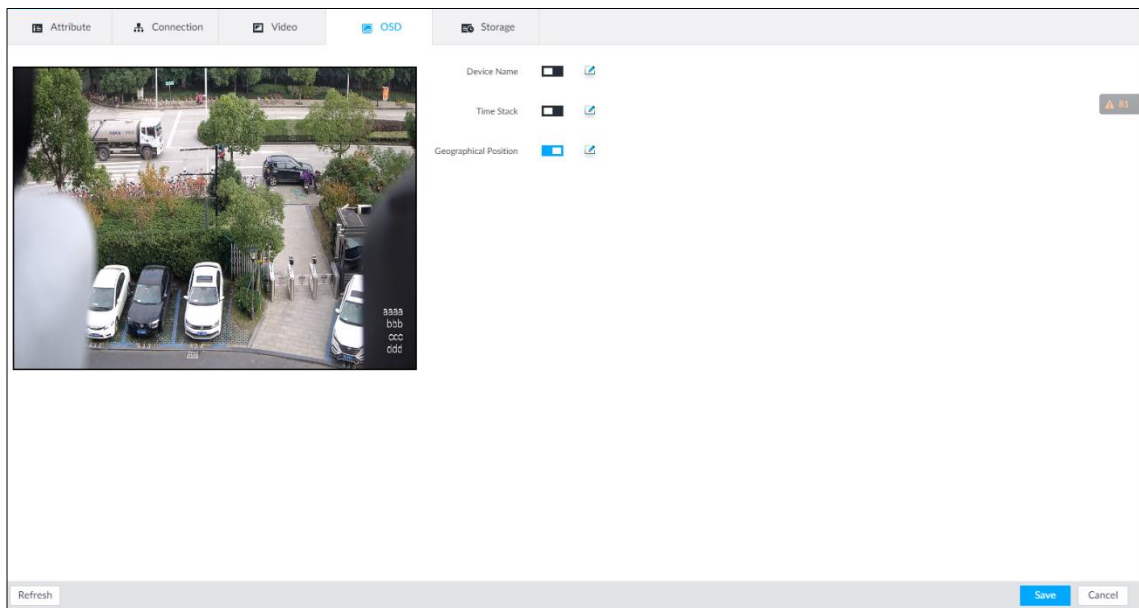
**Step 1** Click , or click  on setting interface, and then select **DEVICE**.

The **Device** interface is displayed.

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

The **OSD** interface is displayed. See Figure 8-14.

Figure 8-14 OSD



**Step 3** Enable OSD information according to actual requirements.

1) Click  to enable OSD function.

2) Click .

The video displays the text boxes. See Figure 8-15, Figure 8-16 or Figure 8-17.

Figure 8-15 Device name

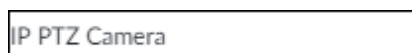


Figure 8-16 Time

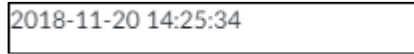


Figure 8-17 Geographical position



- 3) Set device name.






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



- 4) Set geographical position information.



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

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

◇ Click  to adjust font alignment mode.

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

◇ Click  to delete the text box.

- 5) Drag the text box to the proper position.

- 6) Click  to save.

Step 4 Click **Save**.

### 8.2.2.2.5 Storage

It is to set video file and image storage plan of remote device according to the actual situation.

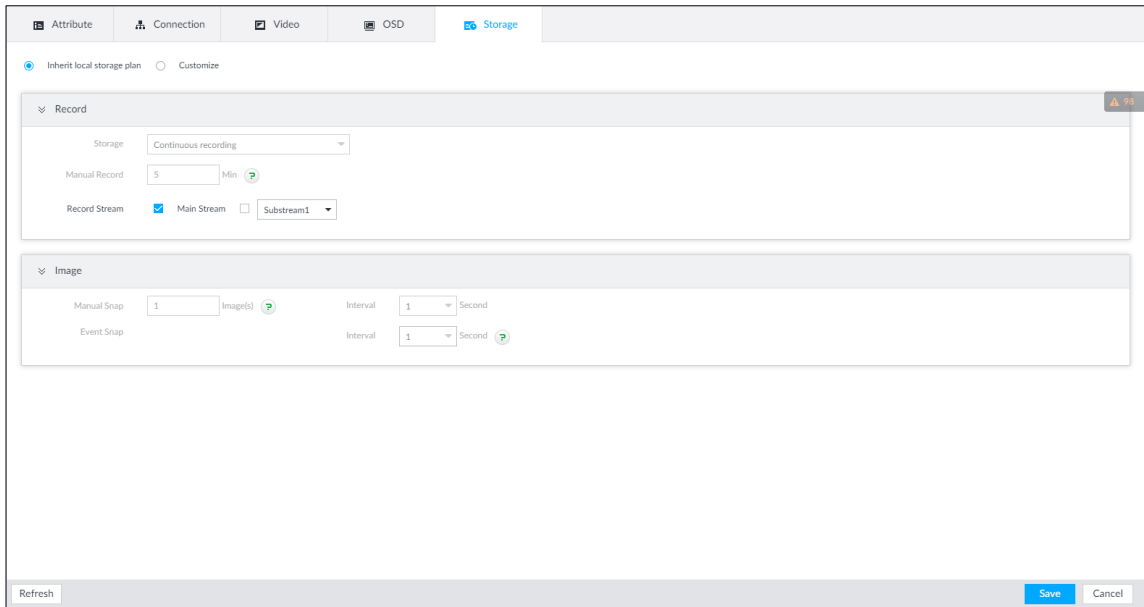
Step 1 Click , or click  on setting interface, and then select **DEVICE**.

The **Device** interface is displayed.

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

The **Storage** interface is displayed. See Figure 8-18.

Figure 8-18 Storage



**Step 3** Select **Inherit local storage plan** or **Customize**.


- **Inherit local storage plan:** The remote device adopts global storage plan of the device.
- **Customize:** Set customized storage plan.

**Step 4** Set parameters. For details, refer to Table 8-6.



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

Table 8-6 Storage parameters description

Parameter		Description
Record	Record plan	It is to set record strategy. <ul style="list-style-type: none"> <li>● Continuous recording: Device records for all day.</li> <li>● Not recording: Device does not record.</li> <li>● Event recording: Device only records when there is corresponding alarm event.</li> </ul>
	Manual record length	It is to set manual record file length. On the <b>Live</b> interface, click  to start record. If you do not click the icon to stop record, system stops recording automatically according to the record length here.
	Record stream	It is to set record stream type. It includes main stream, sub stream 1, and sub stream 2.
Image	Manual snap	It is to set manual snapshot amount and snapshot speed.
	Event snap	It is to set event snapshot interval. Select <b>Customize</b> to set customized interval. The maximum internal is 3600 seconds.

**Step 5** Click **Save**.

## 8.2.2.3 Exporting Remote Device


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



Refer to "5.4.2 Adding Remote Device" for detailed information.

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

The **Device** interface is displayed.

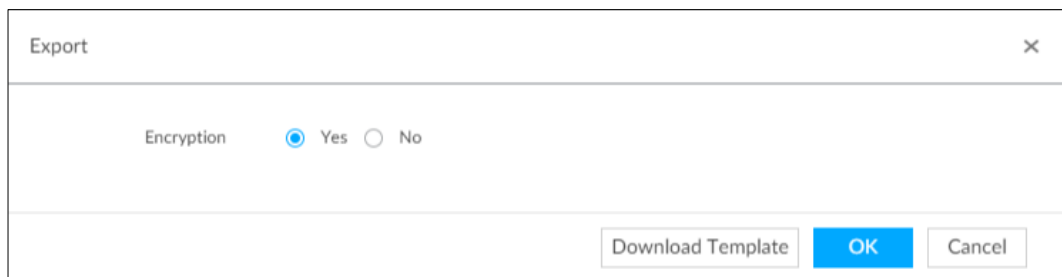
**Step 2** Click  at the bottom left corner.

The **Export** interface is displayed. See Figure 8-19.



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

Figure 8-19 Export



**Step 3** Select encryption or not.

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




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

**Step 4** Click **OK**.

The following prompt interface is displayed.

**Step 5** Click **Save**.

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

- At IVSS client, click , select Download content to view file saving path. For details, see 10.3 View Downloads
- Select file saving path during local operation.




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

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

## 8.2.2.4 Connecting Remote Device

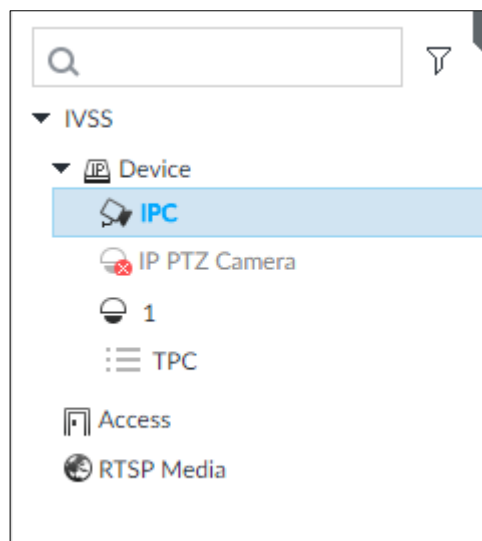
On the **Device** interface, view connection status of remote device in the device list. See Figure 8-20.

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

example,  C2 8249.






- Right-click the offline device, select **Connect** to connect the device.
- Right-click the online device, select **Disconnect** to disconnect the device.

Figure 8-20 Device list



## 8.2.2.5 Deleting Remote Device

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

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



## 8.3 Network Management



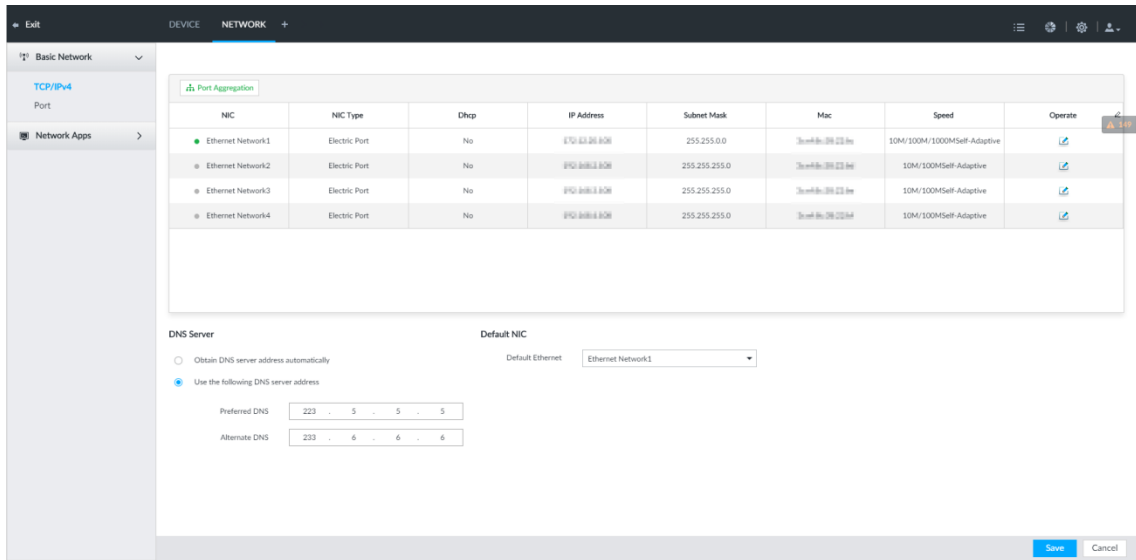
Click  or click  on setting interface, select **NETWORK**. The **NETWORK** interface is displayed. See Figure 8-21. You can set basic network parameters and application.

Figure 8-21 Network management



### 8.3.1 Basic Network



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

#### 8.3.1.1 Configuring IP Address

It is to set device IP address, DNS server information and other information according to network planning.



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

**Step 1** Click  or click  on setting interface, and then select **Network > Basic Network > TCP/IPv4**.

The **TCP/IPv4** interface is displayed. See Figure 8-22.




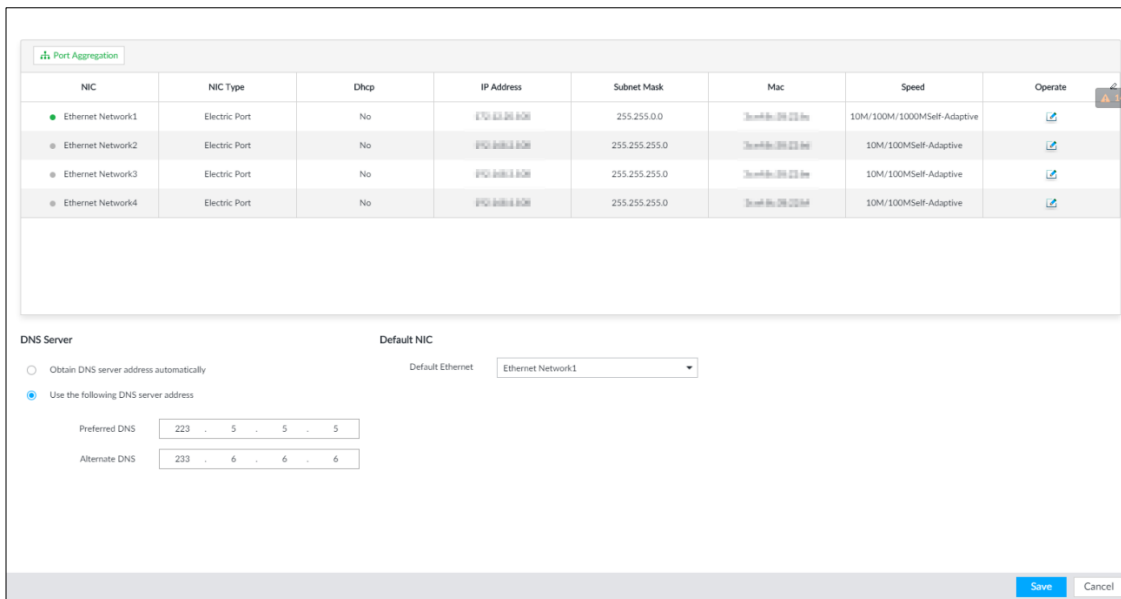
Click  to view the NIC parameter information.

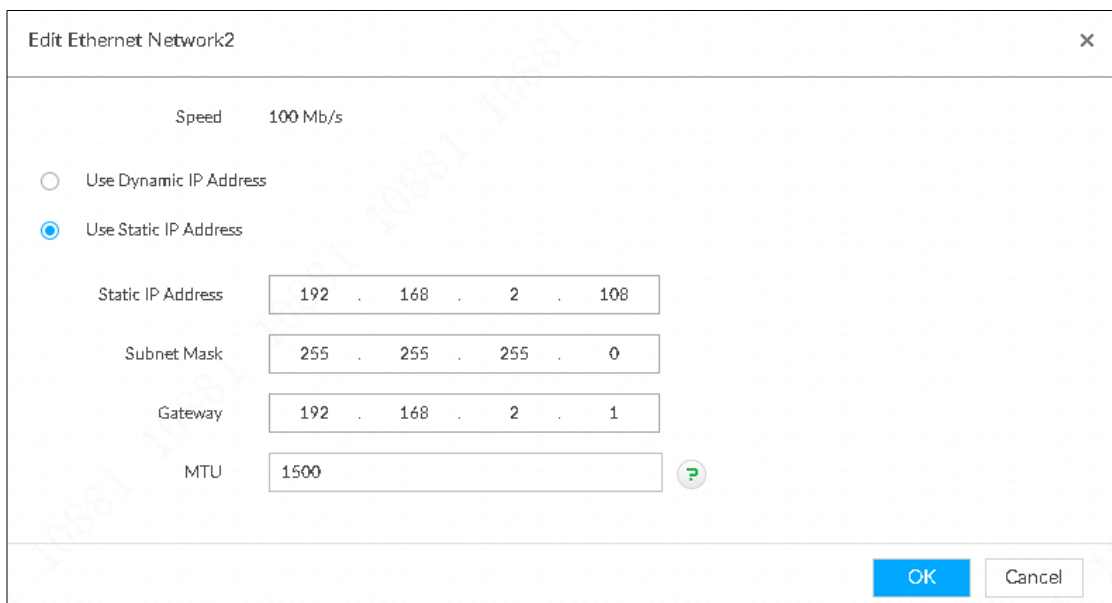
Figure 8-22 TCP/IPv4



**Step 2** Click of the corresponding NIC.

The **Edit Ethernet Network** interface is displayed. See Figure 8-23.


Figure 8-23 Edit Ethernet network



**Step 3** Set parameters. For details, refer to Table 8-7.

Table 8-7 TCP/IP parameters description

Parameter	Description
Speed	Current NIC max network transmission speed.
Use dynamic IP address	When there is a DHCP server on the network, check the box to use dynamic IP address, system can allocate an dynamic IP address to the device. There is no need to set IP address manually.
Use static IP address	Check the box to use static IP address. Set static IP address, subnet mask and gateway. It is to set a static IP address for the device.

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

**Step 4** Click **OK**.

Go back to **TCP/IPv4** interface.

**Step 5** Set DNS server information.

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



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

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

**Step 6** Set default NIC.

Select default NIC from the dropdown list.



Make sure the default NIC is online.



**Step 7** Click **Save**.

### 8.3.1.2 Port Aggregation

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

#### 8.3.1.2.1 Binding NIC

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

**Step 1** Click  or click  on setting interface, and then select **Network > Basic**

**Network > TCP/IPv4.**

The **TCP/IPv4** interface is displayed. See Figure 8-24.

Figure 8-24 TCP/IPv4

The screenshot shows the 'Port Aggregation' configuration window. At the top, there is a table with the following data:

NIC	NIC Type	Dhcp	IP Address	Subnet Mask	Mac	Speed	Operate
Ethernet Network1	Electric Port	No	192.168.1.108	255.255.0.0	3c:ef:8c:39:23:46	10M/100M/1000MSelf-Adaptive	
Ethernet Network2	Electric Port	No	192.168.2.108	255.255.255.0	3c:ef:8c:39:23:47	10M/100MSelf-Adaptive	
Ethernet Network3	Electric Port	No	192.168.3.108	255.255.255.0	3c:ef:8c:39:23:44	10M/100MSelf-Adaptive	
Ethernet Network4	Electric Port	No	192.168.4.108	255.255.255.0	3c:ef:8c:39:23:45	10M/100MSelf-Adaptive	

Below the table, there are sections for 'DNS Server' and 'Default NIC'. The 'DNS Server' section has two radio buttons: 'Obtain DNS server address automatically' (unselected) and 'Use the following DNS server address' (selected). Under the selected option, there are input fields for 'Preferred DNS' (223.5.5.5) and 'Alternate DNS' (233.6.6.6). The 'Default NIC' section has a dropdown menu set to 'Ethernet Network1'. At the bottom right, there are 'Save' and 'Cancel' buttons.

**Step 2** Bind NIC card.

1) Click **Port Aggregation**.

The **Port Aggregation** interface is displayed. See Figure 8-25.

Figure 8-25 Port aggregation

The screenshot shows the 'Port Aggregation' configuration window. At the top, there is a table with the following data:

<input type="checkbox"/> (0)	Nic	Dhcp	IP Address	Subnet Mask	Gateway	Mac	Speed
<input type="checkbox"/>	Ethernet Network1	No	192.168.1.108	255.255.0.0	192.168.1.1	3c:ef:8c:39:23:46	10M/100MSelf-A...
<input type="checkbox"/>	Ethernet Network2	No	192.168.2.108	255.255.255.0	192.168.2.1	3c:ef:8c:39:23:47	10M/100MSelf-A...
<input type="checkbox"/>	Ethernet Network3	No	192.168.3.108	255.255.255.0	192.168.3.1	3c:ef:8c:39:23:44	10M/100MSelf-A...
<input type="checkbox"/>	Ethernet Network4	No	192.168.4.108	255.255.255.0	192.168.4.1	3c:ef:8c:39:23:45	10M/100MSelf-A...


Below the table, there is an 'Aggregation Mode' section with three radio buttons: 'Load Balance' (selected), 'Fault-Tolerance' (unselected), and 'Link Aggregation' (unselected). At the bottom right, there are 'Port Aggregation' and 'Cancel' buttons.

2) Select the NIC you want to bind.

3) Select NIC aggregation mode. For details, see Table 8-8.

Table 8-8 Aggregation mode description

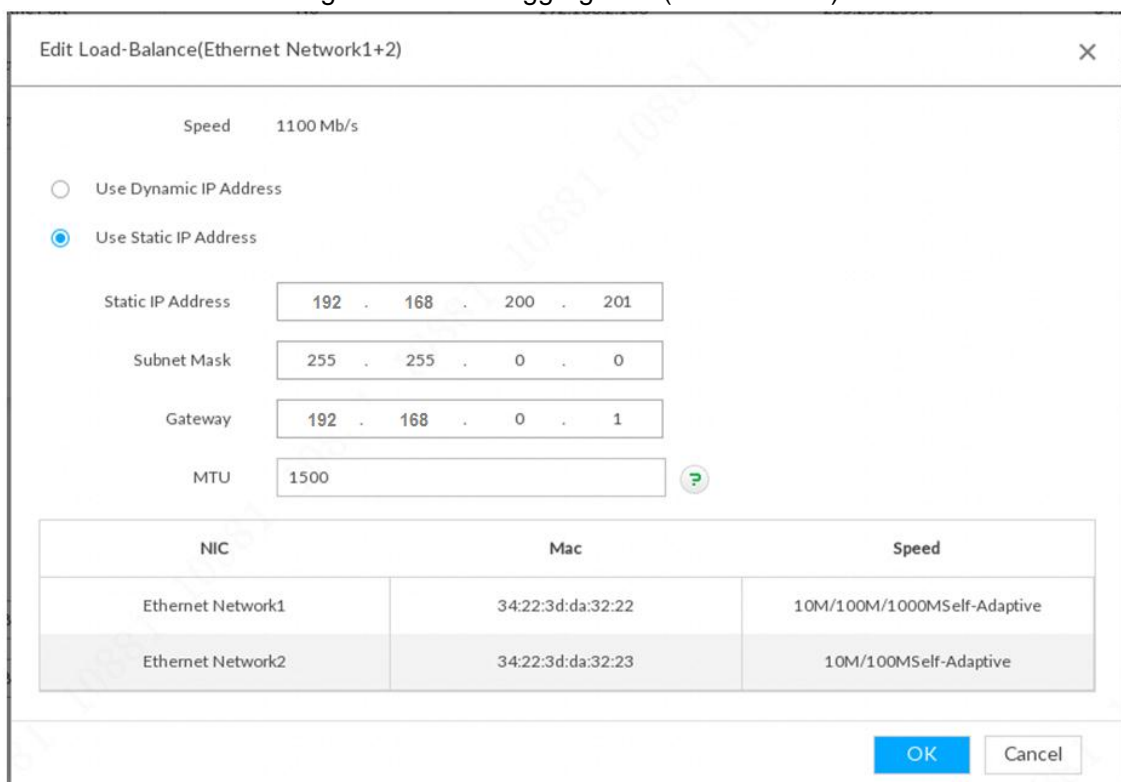
Aggregation mode	Description
------------------	-------------

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

4) Click **Port Aggregation**.

The **Port Aggregation** interface is displayed. See Figure 8-26, Figure 8-27 or Figure 8-28.

Figure 8-26 Port aggregation (load balance)



Edit Load-Balance(Ethernet Network1+2)

Speed 1100 Mb/s

Use Dynamic IP Address  
 Use Static IP Address

Static IP Address 192 . 168 . 200 . 201

Subnet Mask 255 . 255 . 0 . 0

Gateway 192 . 168 . 0 . 1

MTU 1500

NIC	Mac	Speed
Ethernet Network1	34:22:3d:da:32:22	10M/100M/1000M Self-Adaptive
Ethernet Network2	34:22:3d:da:32:23	10M/100M Self-Adaptive

OK Cancel

Figure 8-27 Port aggregation (fault-tolerance)

Speed 1100 Mb/s

Use Dynamic IP Address

Use Static IP Address

Static IP Address 192 . 168 . 200 . 201

Subnet Mask 255 . 255 . 0 . 0

Gateway 192 . 168 . 0 . 1

MTU 1500

NIC	Mac	Speed
Ethernet Network1	34:22:3d:da:32:22	10M/100M/1000M Self-Adaptive
Ethernet Network2	34:22:3d:da:32:23	10M/100M Self-Adaptive

OK Cancel

Figure 8-28 Port aggregation (link aggregation)

Speed 1100 Mb/s

Use Dynamic IP Address

Use Static IP Address

Static IP Address 192 . 168 . 200 . 201

Subnet Mask 255 . 255 . 0 . 0

Gateway 192 . 168 . 0 . 1

MTU 1500


NIC	Mac	Speed
Ethernet Network1	34:22:3d:da:32:22	10M/100M/1000M Self-Adaptive
Ethernet Network2	34:22:3d:da:32:23	10M/100M Self-Adaptive

OK Cancel

5) Set parameters. For details, refer to Table 8-9.

Table 8-9 TCP/IP parameters description

Parameter	Description
Speed	Maximum network transmission speed of current NIC.

Parameter	Description
Use dynamic IP address	When there is a DHCP server on the network, check the box to use dynamic IP address. System can allocate a dynamic IP address to the device. There is no need to set IP address manually.
Use static IP address	Check the box to use static IP address. Set static IP address, subnet mask and gateway. It is to set a static IP address for the device.
MTU	<p>Set NIC MTU value. The default setup is 1500 Byte.</p> <p>We recommend you to check the MTU value of the gateway first and then set the device MTU value equal to or smaller than the gateway value. It is to reduce the packets slightly and enhance network transmission efficiency.</p>  <p>Changing MTU value may result in NIC reboot, network offline and affect current running operation. Please be careful!</p>

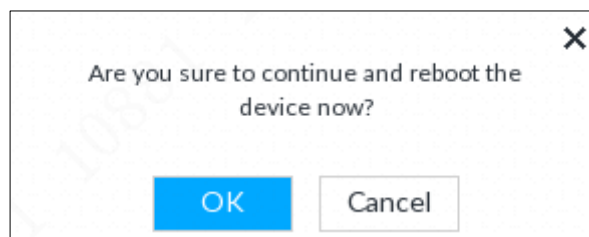
6) Click OK.

Go back to **TCP/IPv4** interface.

**Step 3** Click **Save**.

System pops up a confirmation box. See Figure 8-29.

Figure 8-29 Confirmation





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

Auto Reboot The binding card information becomes activated after reboot operation.

### 8.3.1.2.2 Cancelling Binding NIC

It is to cancel port aggregation and allow the bonded NICs to work as independent card.

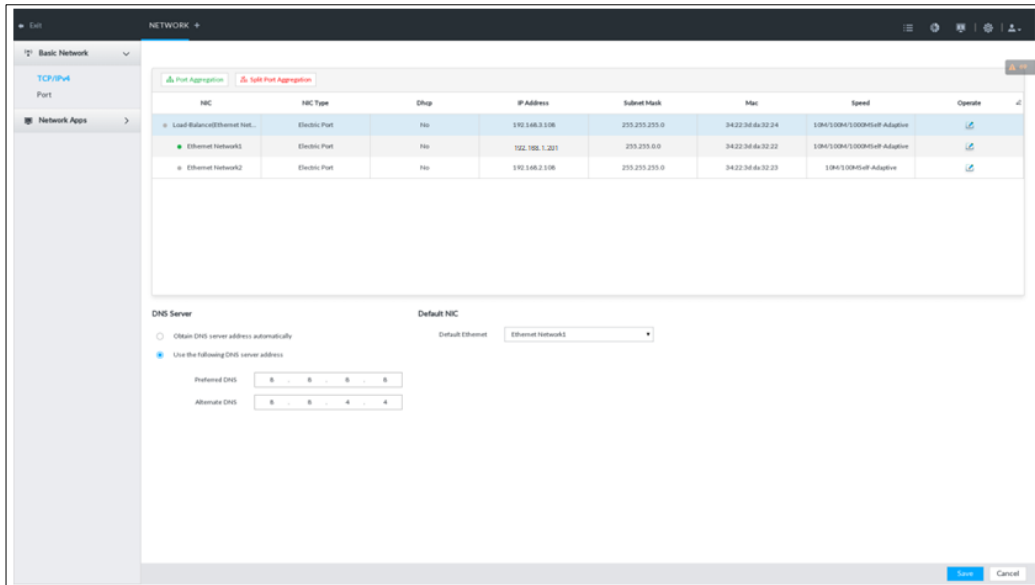
**Step 1** Click  or click  on setting interface, and then select **Network > Basic Network > TCP/IPv4**.

The **TCP/IPv4** interface is displayed.

**Step 2** Select bonded NIC.

System displays **Split Port Aggregation** interface. See Figure 8-30.

Figure 8-30 TCP/IPv4



**Step 3** Click **Split Port Aggregation**.

System pops up confirmation interface.

**Step 4** Click **OK**.

System splits the bonded NIC.



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

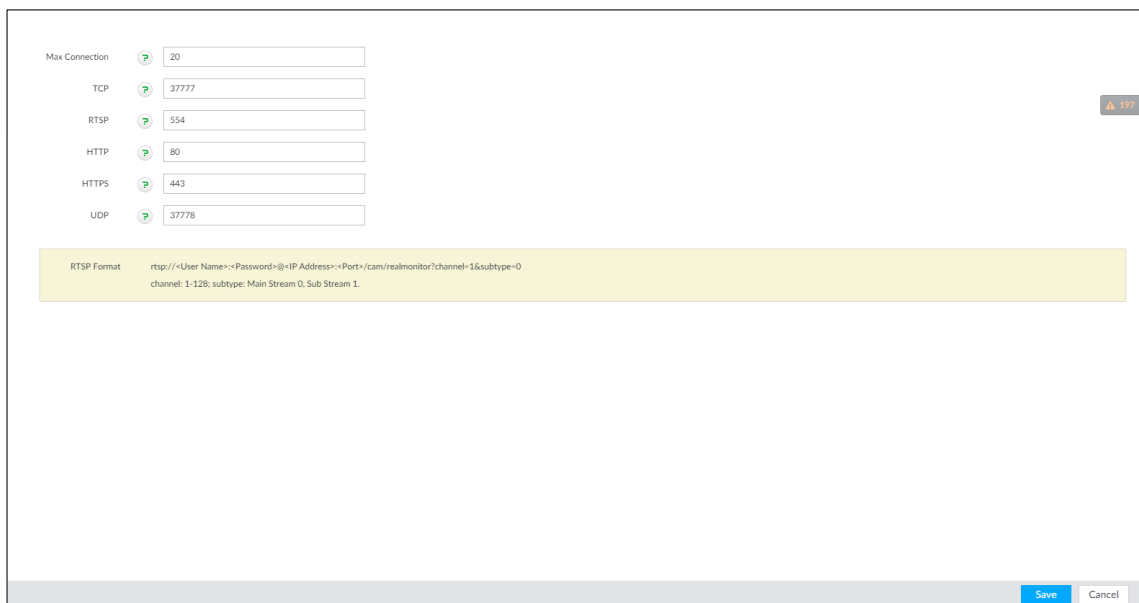
### 8.3.1.3 Setting Port Number

It is to set device port number.

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

The Port interface is displayed. See Figure 8-31.

Figure 8-31 Port





**Step 2** Set parameters. For details, refer to Table 8-10.



Login again after modifying parameters, except Max Connection.

Table 8-10 Connection setting parameters description

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

**Step 3** Click **Save**.

System reboots corresponding service of the port.

## 8.3.2 Network Apps



It is to set device network parameters, so that system can connect to other devices.

### 8.3.2.1 P2P

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

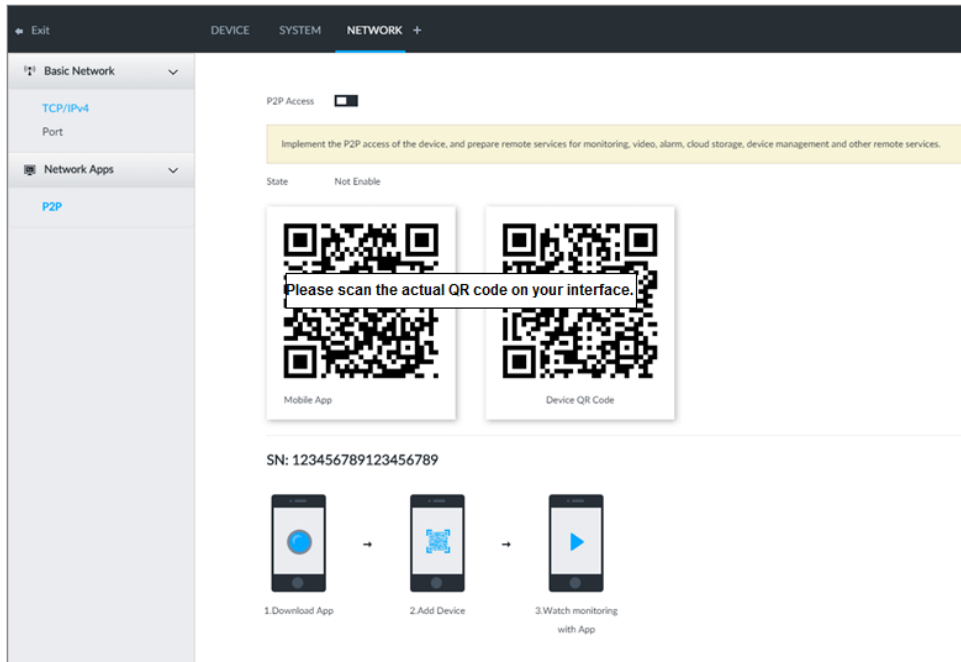



- Make sure the system has connected to the network. Otherwise, the P2P function is null.
- When using the P2P function, we will collect device information such as IP address, MAC address, name and serial number. The collected information is only used for remote access.

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

The **P2P** interface is displayed. See Figure 8-32. Scan the QR code on the actual interface.

Figure 8-32 P2P



**Step 2** Click  to enable P2P function.

**Step 3** Click **Save**.

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



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

### 8.3.2.2 DDNS

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



#### Preparation

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




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

#### Procedure

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

The **DDNS** interface is displayed. See Figure 8-33.

Figure 8-33 DDNS

**Step 2** Click  to enable DDNS function.



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

**Step 3** Set the corresponding parameters. For details, see Table 8-11.

Table 8-11 DDNS setting parameters description


Parameter	Description
DDNS Type	Name and address of DDNS service provider.
Server IP	<ul style="list-style-type: none"> <li>• Dyndns DDNS: members.dyndns.org</li> <li>• NO-IP DDNS: dynupdate.no-ip.com</li> <li>• CN99 DDNS: members.3322.org</li> </ul>
Domain Name	The domain name for registering on the website of DDNS service provider.
Username	Enter the user name and password obtained from DDNS service provider. You need to register (including user name and password) on the website of DDNS service provider.
Password	
Update circle	Enter the amount of time that you want to update the DDNS.
Current WAN IP	Displays the WAN IP address of IVSS.
Status	Displays DDNS registration result or update status.

**Step 4** Click **Save**.

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

### 8.3.2.3 Configuring Email Settings

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

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

The **Email** interface is displayed. See Figure 8-34.

Figure 8-34 Configuring Email


**Step 2** Click  to enable Email function.


**Step 3** Set parameters. For details, refer to Table 8-12.

Table 8-12 EMAIL parameter description

Parameter	Description
Email Server	Select Email server type, including Customize, Gmail, Hotmail, and Yahoo.
Server Address	Enter Email server address. For details, see Table 8-13.
Encryption	Select encryption type of Email server, including NONE, SSL, and TLS. For details, see Table 8-13.
Port	Enter the port number of Email server. For details, see Table 8-13.
User name and password	Enter the configured user name and password of Email server. For details, see Table 8-13.

Table 8-13 Common Email parameters

Email type	Email Server	Encryption	Port	Description
QQ	smtp.qq.com	SSL	465	<ul style="list-style-type: none"> <li>Do not select <b>NONE</b> for encryption.</li> <li>The mailbox must have applied SMTP service.</li> <li>The password must be an "authorized password". Both the QQ login password and email login password are invalid.</li> </ul>  <p>Obtain the authorized password when your mailbox is applying for SMTP service.</p>
163	smtp.163.com	SSL	465/994	<ul style="list-style-type: none"> <li>The mailbox must have applied</li> </ul>



Email type	Email Server	Encryption	Port	Description
		TLS	25	SMTP service. <ul style="list-style-type: none"> <li>The password must be an "authorized password". The email login password is invalid.</li> </ul>  Obtain the authorized password when your mailbox is applying for SMTP service.
		NONE	25	
126	smtp.126.com	NONE	25	The mailbox must have applied SMTP service.

**Step 4** Add the information of mail receiver.

- 1) Click **Add**.  
The Add interface is displayed.
- 2) Enter a receiver' Email address. See Figure 8-35.

Figure 8-35 Email address



- 3) Click Add or  to add other receivers' Email address.
  - Click  to delete the added receiver.
  - Select a receiver. The **Delete** button is displayed. Click **Delete** button to delete the selected receiver.



**Step 5** Click **Save**.

**Step 6** (Optional) Test the email sending function.

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

### 8.3.2.4 Register

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

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

The **REGISTER** interface is displayed. See Figure 8-36.

Figure 8-36 Register

**Step 2** Click  to enable register function.

**Step 3** Set parameters. For details, refer to Table 8-14.

Table 8-14 Register

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

**Step 4** Click **Save**.

## 8.4 Event Management

Click or click on setting interface, select **EVENT**. The **EVENT** interface is displayed.

See Figure 8-37.

On the interface, configure alarm event, including alarm event of IVSS and remote device.

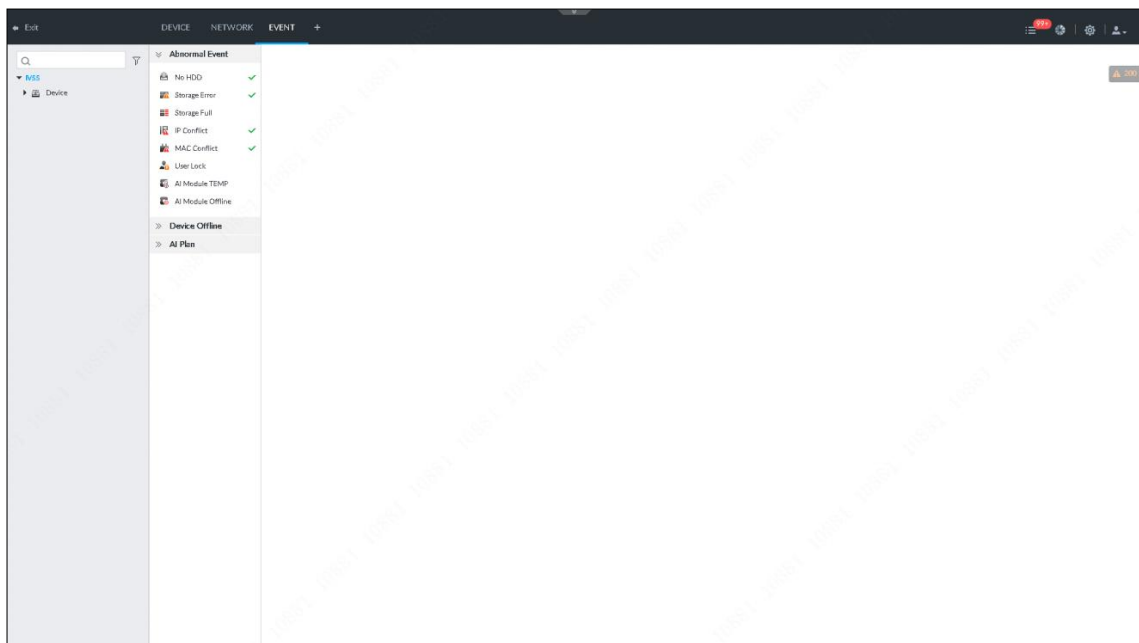
- Select root node in the device tree on the left to set IVSS alarm event. Refer to "8.4.2 Local Device" for detailed information.
- Select remote device in the device tree on the left, to set alarm event of this remote device. Refer to "8.4.3 Remote Device" for detailed information.



- The alarm event might be different depending on the model you purchased. The actual interface shall prevail.
- in the right of alarm event means that this alarm event has been enabled.

- in the right of AI detection means that AI by camera has been enabled; ■ means that AI by device has been enabled; ■ means that both have been enabled.

Figure 8-37 Event management



## 8.4.1 Alarm Actions

System can trigger the corresponding actions when an alarm occurs.



The supported actions might be different depending on the model you purchased. The actual interface shall prevail.

On the alarm configuration interface, click **Actions** to display actions. See Figure 8-38. Refer to Table 8-15 for detailed information. Configure actions according to your actual need.

- After setting actions, click **Save** on the interface.
- After enabling actions, click × to disable the corresponding actions.

Figure 8-38 Actions

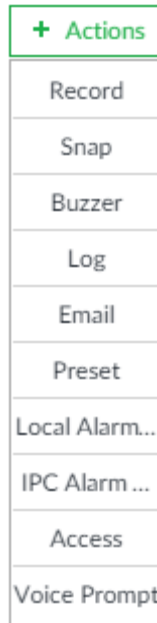


Table 8-15 Actions description

Actions	Description	Preparation
Record	The system links the selected remote device to record when there is corresponding alarm event.	Remote device, such as IPC, has been added. Refer to "5.4.2 Adding Remote Device" for detailed information.
Snapshot	The system links the selected remote device to snapshot when there is corresponding alarm event.	-
Buzzer	The system activates a buzzer alarm when there is corresponding alarm event.	-
Log	The system notes down the alarm information in the log when there is corresponding alarm event.	
Email	The system sends alarm Email to all added receivers when there is corresponding alarm event.	Email configuration has been completed. Refer to "8.3.2.3 Configuring Email Settings" for detailed information.
Preset	The system links the selected remote device to rotate to the designated preset point when there is corresponding alarm event.	PTZ device has been added, and preset point has been added. Refer to "5.4.2 Adding Remote Device" for detailed information.
Local Alarm Output	When there is an alarm, system can trigger the corresponding device to generate alarm.	IVSS is connected with alarm output device.



Actions	Description	Preparation
IPC Alarm Output Settings	When there is an alarm, system can trigger the corresponding device to generate alarm.	IPC has been added, and IPC is connected with alarm output device. Refer to "5.4.2 Adding Remote Device" for detailed information.
Access	When there is an alarm, system can trigger the corresponding access control device to open door and close door.	Refer to "5.4.2 Adding Remote Device" for detailed information.
Voice Prompt	When there is an alarm, system can play the selected audio file.	Audio function has been configured. Refer to "8.8.5 Enabling Voice Manage Function" for detailed information.

### 8.4.1.1 Record

Enable record control function. The system links the selected remote device to record when there is corresponding alarm event.

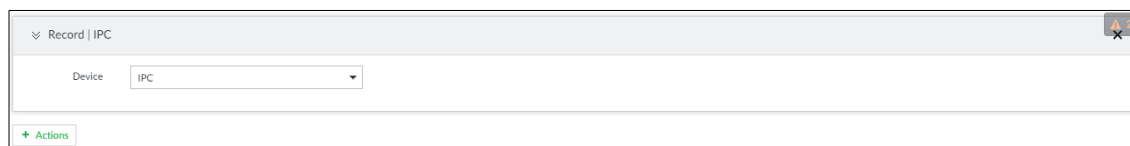


Make sure the remote device, such as IPC, has been added. Refer to "5.4.2 Adding Remote Device" for detailed information.

**Step 1** Click **Actions** and select **Record**.

The record setting interface is displayed. See Figure 8-39.

Figure 8-39 Record



**Step 2** Select a remote device.

**Step 3** (Optional) Repeat Step 1–Step 2, and link multiple remote devices to record.

### 8.4.1.2 IPC Alarm Out

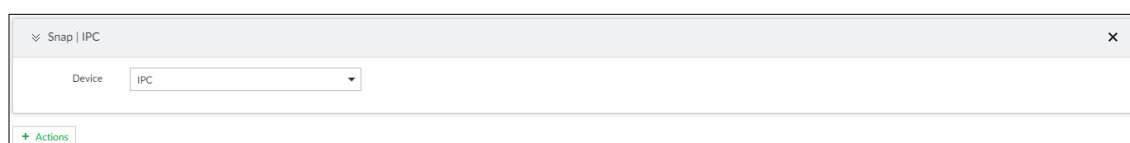
The system links the selected remote device to snapshot when there is corresponding alarm event.

Click **Actions** and select **IPC Alarm Out** to enable this function. See Figure 8-40.



Only remote device supports this function, and only the current remote device can be linked to snapshot.

Figure 8-40 IPC alarm out



### 8.4.1.3 Buzzer

The system activates a buzzer alarm when there is corresponding alarm event.

Click **Actions** and select **Buzzer** to enable this function. See Figure 8-41.

Figure 8-41 Buzzer

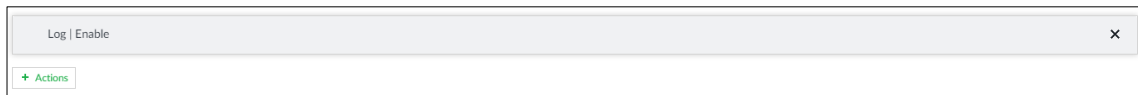



### 8.4.1.4 Log

Enable the log function. The system notes down the alarm information in the log when there is corresponding alarm event.

Click **Actions** and select **Log** to enable this function. See Figure 8-42.

Figure 8-42 Log



When log function is enabled, after an alarm is triggered, click  on **LIVE** interface, select **Maintain > Log > Event**.

### 8.4.1.5 Email

Enable Email function. The system sends alarm email to all added receivers when there is corresponding alarm event.



Make sure the Email configuration has been completed. Refer to 8.3.2.3 Configuring Email Settings for detailed information.

Click **Actions** and select **Email** to enable this function. See Figure 8-43.

Figure 8-43 Email



### 8.4.1.6 Preset

Set preset point function. The system links the selected remote device to rotate to the designated preset point when there is corresponding alarm event.

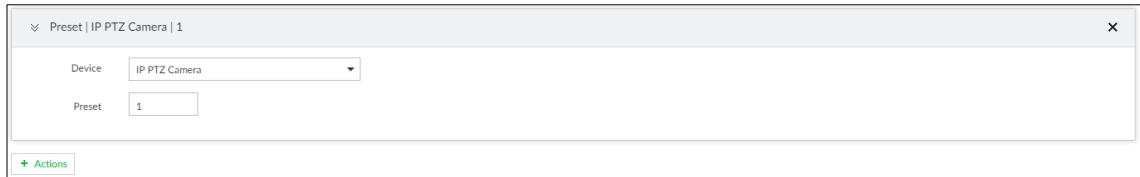


Make sure the PTZ device has been added, and preset point has been added. Refer to "5.4.2 Adding Remote Device" for detailed information.

Step 1 Click **Actions** and select **Preset**.

The **Preset** interface is displayed. See Figure 8-44.

Figure 8-44 Preset



**Step 2** Select PTZ device, and enter preset point number.

**Step 3** (Optional) Repeat Step 1–Step 2, and link multiple PTZ devices to turn to designated preset points.

### 8.4.1.7 Local Alarm Out

Set local alarm output. System can trigger the corresponding alarm event when an alarm occurs.

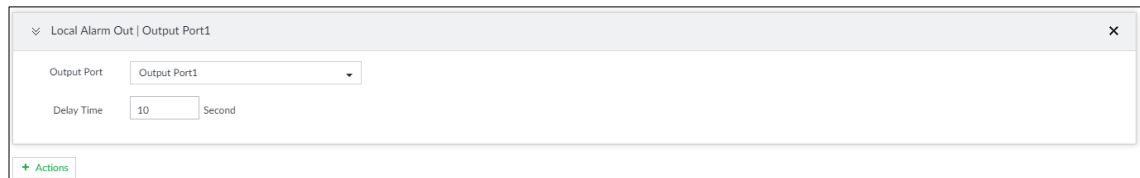


Make sure IVSS is connected with alarm output device.

**Step 1** Click **Actions** and select **Local Alarm Out**.

The **Local Alarm Out** interface is displayed. See Figure 8-45.

Figure 8-45 Local alarm out



**Step 2** Select alarm output port.

Support to select multiple alarm output ports.

**Step 3** Set delay time.

Set a delay time. After alarm event is ended, alarm will end after the delay time. You can configure from 0 seconds through 300 seconds, and the default value is 10 seconds.

### 8.4.1.8 IPC Alarm Out

Set IPC alarm output. System can trigger the corresponding alarm output device when an alarm occurs.

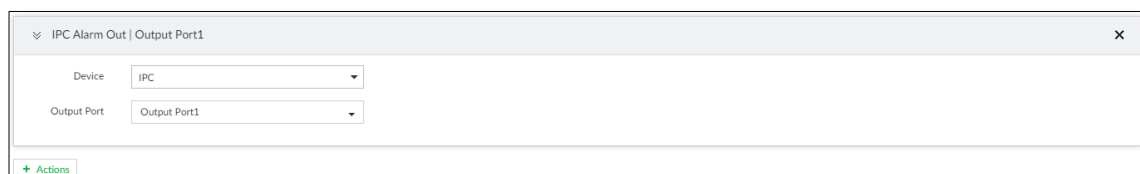


Make sure the IPC has been added, and IPC is connected with alarm output device. Refer to "5.4.2 Adding Remote Device" for detailed information.

**Step 1** Click **Actions** and select **IPC Alarm Out**.

The **IPC Alarm Out** interface is displayed. See Figure 8-46.

Figure 8-46 IPC alarm output settings



**Step 2** Select IPC and alarm output port.

Support to select multiple alarm output ports.

**Step 3** (Optional) Repeat Step 1–Step 2, and link multiple IPC alarm output devices.

### 8.4.1.9 Access

Set access control function. When there is an alarm, system can trigger the corresponding access control device to open door and close door.

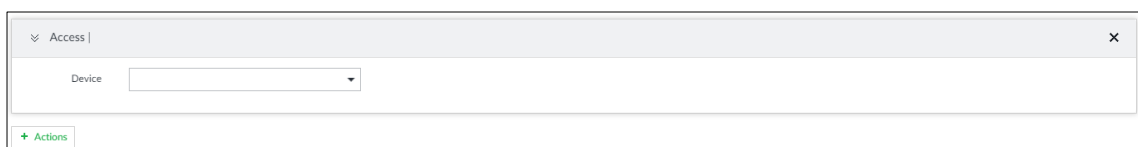


Make sure that access control device has been added. Refer to "5.4.2 Adding Remote Device" for detailed information.

**Step 1** Click **Actions** and select **Access**.

The **Access** setting interface is displayed. See Figure 8-47.

Figure 8-47 Access



**Step 2** Select access control device.



Not all models support this function. The actual interface shall prevail.

**Step 3** (Optional) Repeat Step 1–Step 2, and link multiple access control devices.

### 8.4.1.10 Voice Prompt

Set voice prompt function. When there is an alarm, system can play the selected audio file.

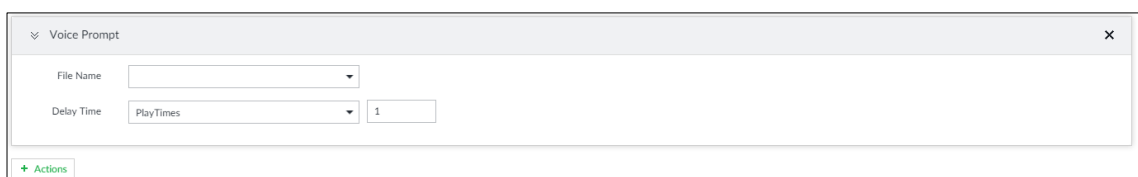


Make sure the voice function has been configured. Refer to "8.8.5 Enabling Voice Manage Function" for detailed information.

**Step 1** Click **Actions** and select **Voice Prompt**.

The **Voice Prompt** interface is displayed. See Figure 8-48.

Figure 8-48 Voice prompt



**Step 2** In the **File Name** list, select the audio file that you want to play for this configured period.

**Step 3** Set delay time.

- Play times: Select **Play Times** and enter the times to play the file. After the alarm event is ended, system will continue to play the voice file according to the play times.
- Duration: Select **Duration** and enter the delayed play duration. After the alarm event is ended, system will continue to play the voice file according to the duration.

## 8.4.2 Local Device

Set IVSS alarm event, including abnormal event, device offline alarm, AI plan, and local device alarm.


### 8.4.2.1 Abnormal Event

It is to set alarm mode when an abnormal event occurs.

#### Name

IVSS supports HDD, storage error, network, AI module, fan and power fault alarm. For details, see Table 8-16.

Table 8-16 Abnormal event description

Name	Description
No HDD	System triggers an alarm when there is no HDD. It is enabled by default.
Storage error	System triggers an alarm when the HDD or the RAID has error. It is enabled by default.
Storage full	System triggers an alarm when HDD space is full. It is disabled by default.
IP conflict	System triggers an alarm when its IP address conflicts with IP address of other device in the same LAN. It is enabled by default.
MAC conflict	System triggers an alarm when its MAC address conflicts with MAC address of other device in the same LAN. It is enabled by default.
Lock in	System triggers an alarm when an account login error has reached the threshold. At the same time, system locks current account. It is disabled by default.  Go to the <b>Security</b> interface to set account error threshold. Refer to "8.6.3 Safety Protection" for detailed information.
AI module temp	When AI module temperature is higher than the specified value, system triggers an alarm. It is enabled by default.
AI module offline	When AI module and system is disconnected, system triggers an alarm. It is enabled by default.
Fan speed alarm	When IVSS fan speed is abnormal, system triggers an alarm. It is enabled by default.
Power fault	When IVSS power supply is abnormal, system triggers an alarm. It is disabled by default.

#### Operation Steps



Here we use AI module temp for example. For other events, the setting steps are similar. Refer to the actual interface for detailed information.

Step 1 Click , or click  on setting interface, and then select **Event**.

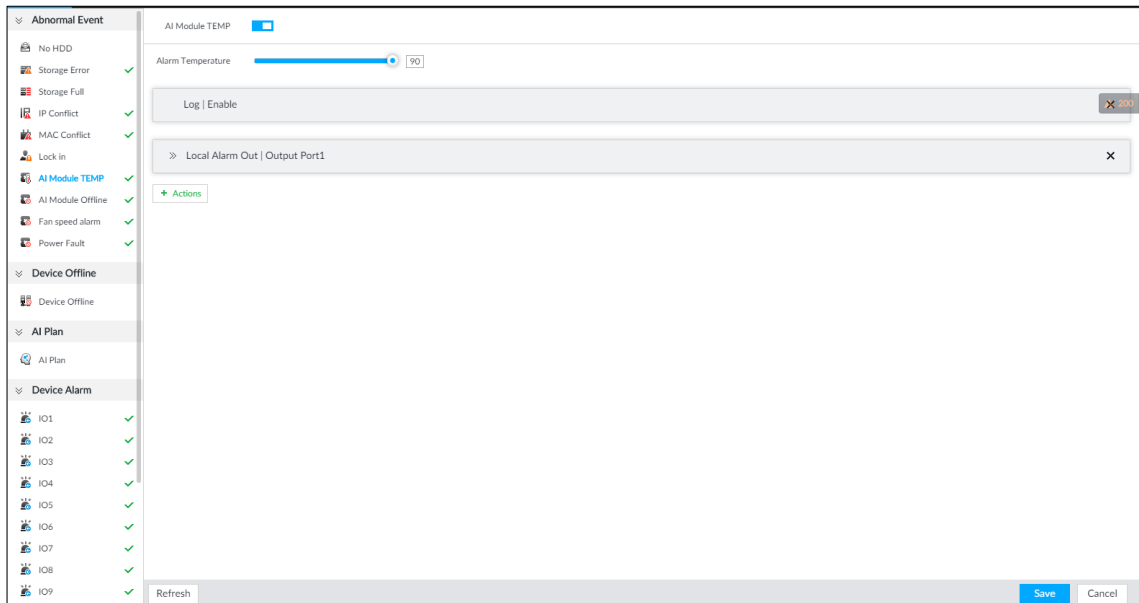
The **Event** interface is displayed.


**Step 2** Select root node on the left list.

**Step 3** Select **Abnormal Event > AI Module TEMP**.

The **AI Module TEMP** interface is displayed. See Figure 8-49.

Figure 8-49 AI module temp



**Step 4** Click  to enable AI module temperature alarm function.

**Step 5** Drag  to set alarm temperature threshold.



The above step is for AI module temperature alarm only.

**Step 6** Click **Actions** to set alarm actions. Refer to "8.4.1 Alarm Actions" for detailed information.

**Step 7** Click **Save**.

## 8.4.2.2 Offline Alarm

Set IVSS network offline alarm. If you have not set offline alarm for a specified remote device, once the remote device is disconnect from the system, system adopts alarm strategy of IVSS to trigger an alarm.

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

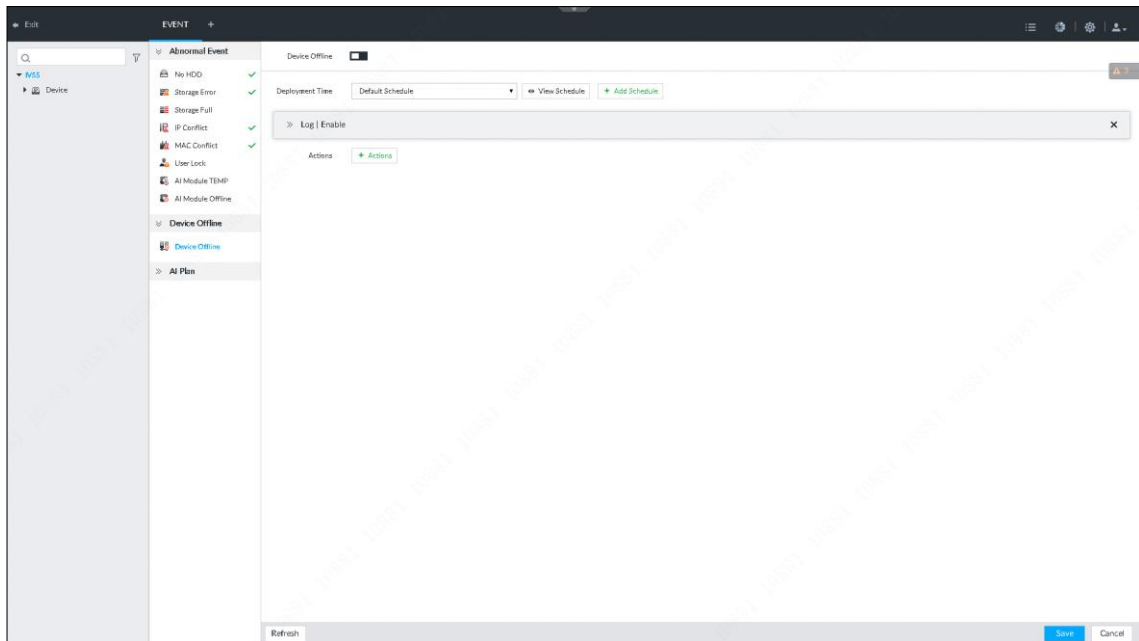
The **EVENT** interface is displayed.

**Step 2** Select root node on the left list.

**Step 3** Select **Device Offline > Device Offline**.

The **Device Offline** interface is displayed. See Figure 8-50.

Figure 8-50 Network offline



**Step 4** Click  to enable device offline alarm.

**Step 5** Click **Deployment Time** to select schedule from the drop-down list. After setting deployment period, system triggers corresponding operations when there is a motion detection alarm in the specified period.

- Click **View Schedule** to view detailed schedule settings.
- If the schedule is not added or the added schedule does not meet actual needs, click **Add Schedule**. Refer to "8.8.4 Schedule" for detailed information.

**Step 6** Click **Actions** to set alarm actions. Refer to "8.4.1 Alarm Actions" for detailed information.

**Step 7** Click **Save**.

### 8.4.2.3 Configuring AI Plan

Configure AI detection result display strategy of IVSS. If you have not set AI display settings for current remote device, the remote device inherits AI display mode of IVSS.

#### 8.4.2.3.1 Viewing AI Plan

After adding remote device, on IVSS, obtain AI detection type and status of the remote device.

On the **EVENT** interface, select root node on the left device tree. Select **AI Plan > AI Plan > AI Plan**. The **AI Plan** interface is displayed. See Figure 8-51.

After installing the AI module, and the remote device supports AI detection, and you have enabled the AI detection function, you can view channel name of the remote device on the corresponding AI detection panel.

Figure 8-51 AI plan



### 8.4.2.3.2 Setting AI Display

Set the attribute that shall be displayed in rule box and feature attribute panel. View AI detection result through smart preview, and support to display face, human and vehicle.

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

The **EVENT** interface is displayed.

**Step 2** Select root node on the left device tree.

**Step 3** Select **AI Plan > AI Plan > AI Display > Face**, or select **AI Plan > AI Plan > AI Display > Human**.

The **Face** or **Human** interface is displayed. See Figure 8-52 or Figure 8-53.

Figure 8-52 Face

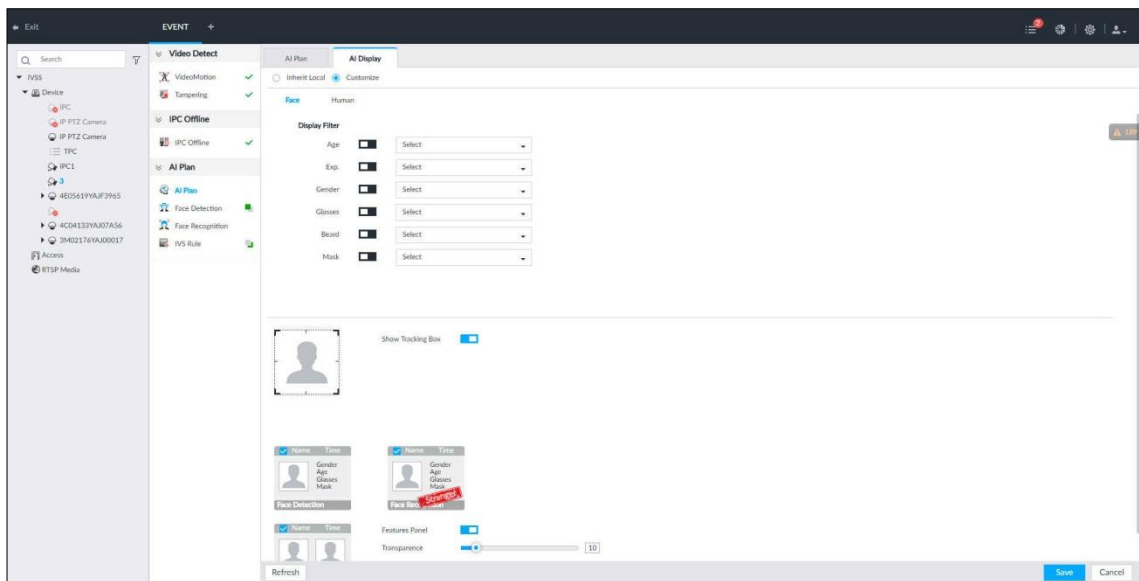
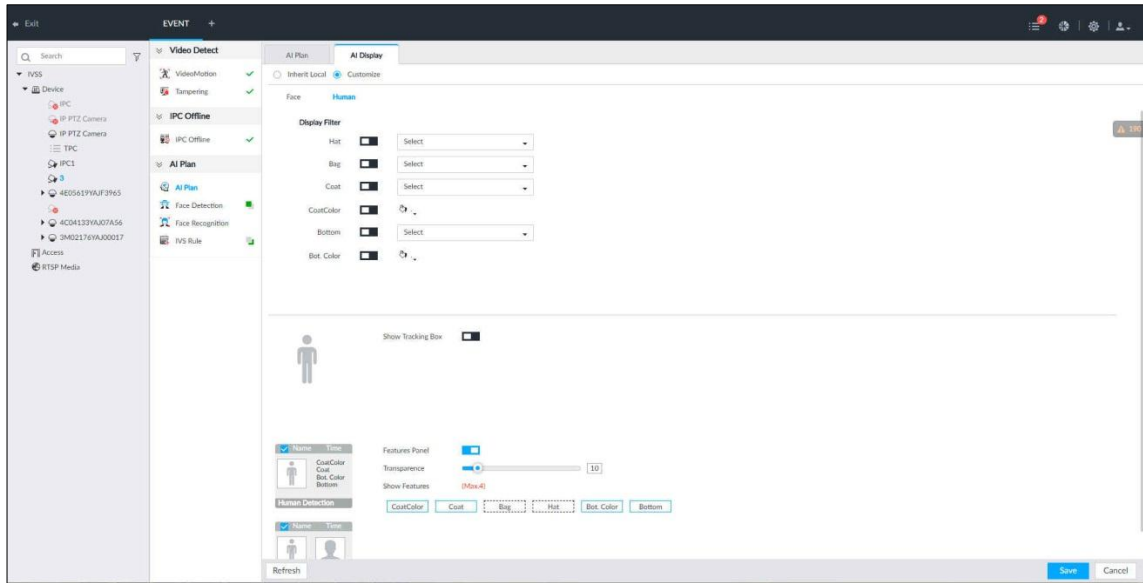





Figure 8-53 Human



**Step 4** Configure display filter information.

After setting filter criteria, only the qualified detection result will be displayed. For example, enable Age, and then select youth from the drop-down list. The tracking box and the features panel only display the human face of the youth age.

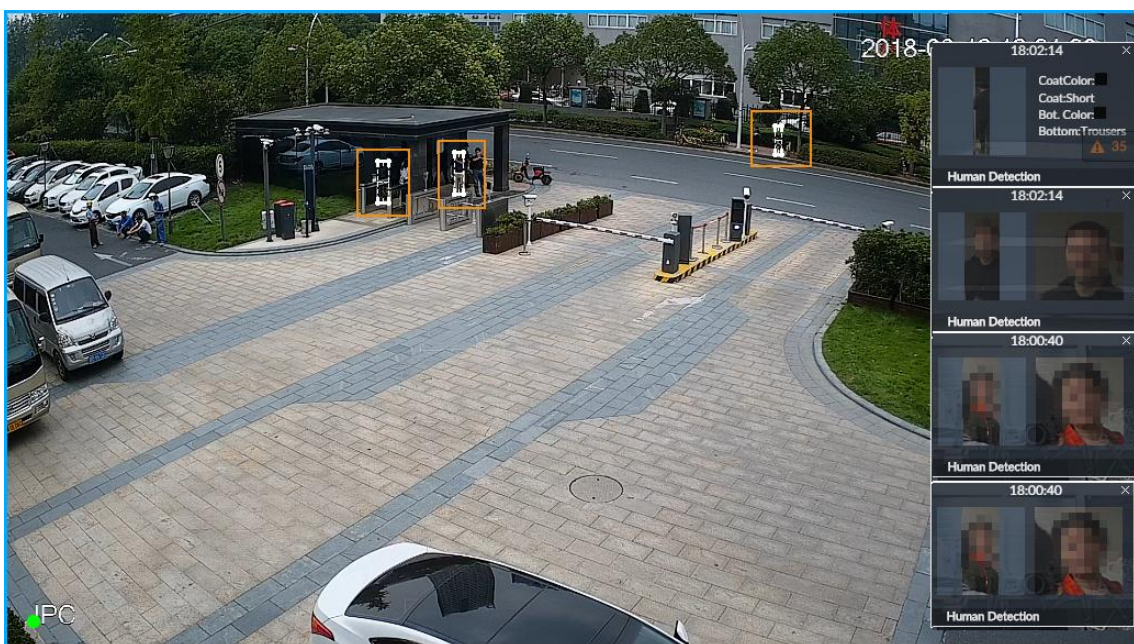
- 1) Click  to enable corresponding filter type.
- 2) It is to set display filter criteria.


Click  to set the filter color.

**Step 5** Click  in the right of **Show Tracking Box** to enable.

After enabled, when the system detects face or human, tracking box will be shown beside the face or human in the view window. See Figure 8-54.

Figure 8-54 Tracking box



**Step 6** Click  in the right of **Features Panel** to enable, and select the features that shall be displayed on the Live interface.  
After enabled, there is a features panel on the right side of the view window. See Figure 8-55.



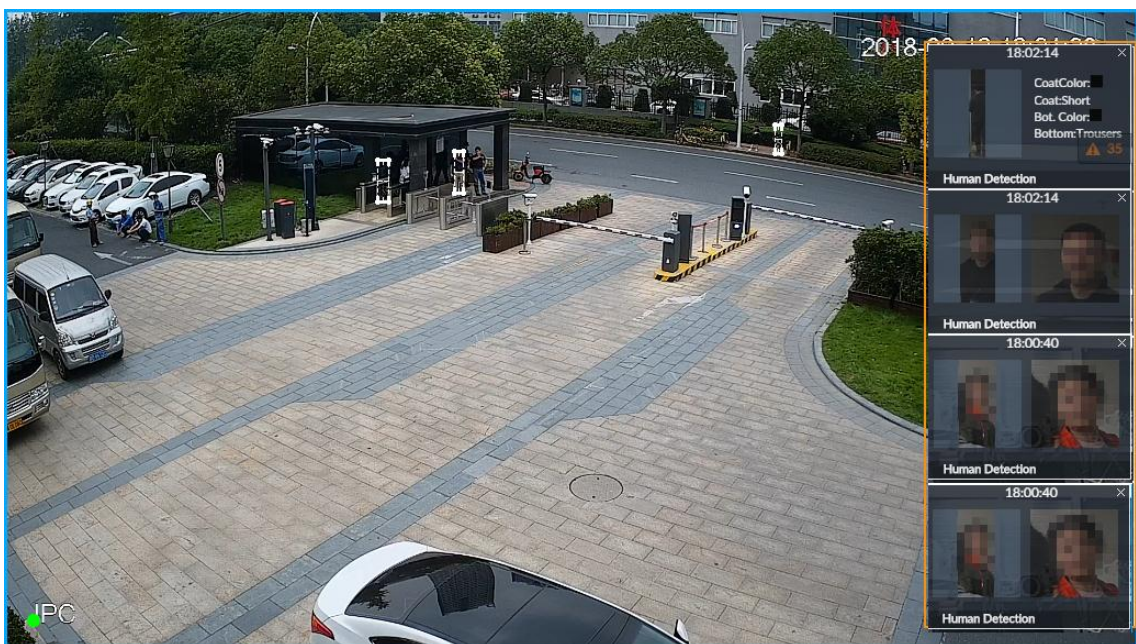
- Drag  to adjust features panel transparency. The higher the value, the more transparent the features panel.
- System supports maximum 4 features. System has checked four features by default. To select other features, cancel the selected features, and then select the ones you need.
- Click  to display the features panel on the **LIVE** interface, including face detection panel, stranger panel and face DB panel.

Figure 8-55 Features panel



**Step 7** Click **Save**.

#### 8.4.2.4 Configuring Device Alarm

Set device alarm. When alarm input device sends an alarm signal to IVSS, an alarm is triggered.

##### Preparation

IVSS is connected with alarm input device.

##### Operation Steps



IVSS supports 16-channel alarm input. Configure according to actual port of alarm input device. Take ALARM1 port connection for example.

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

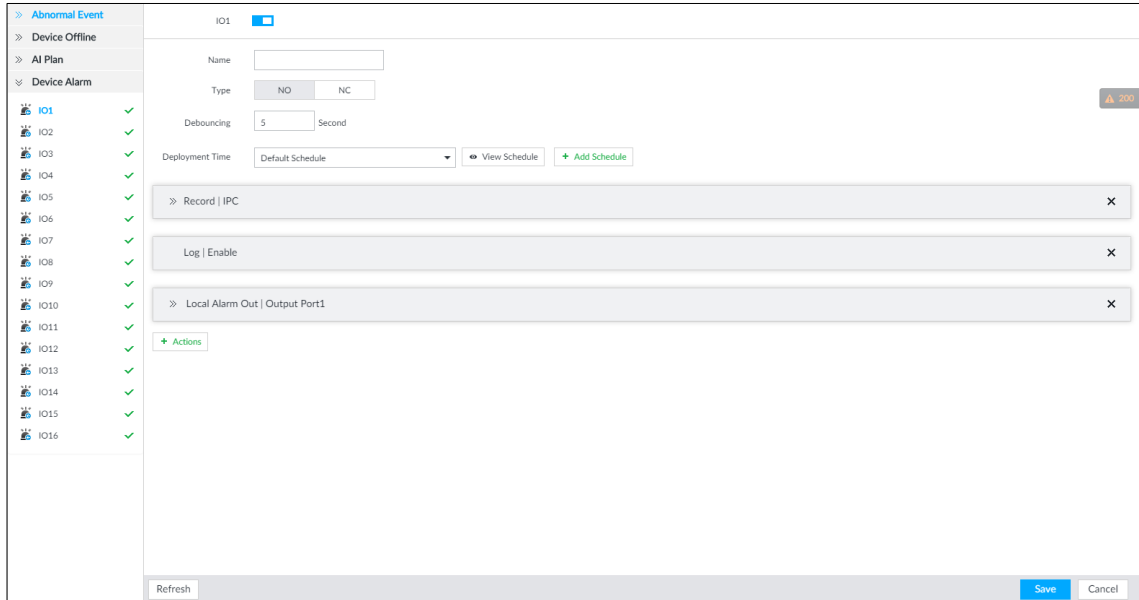
The **EVENT** interface is displayed.

**Step 2** Select root node on the left device tree.

**Step 3** Select **Device Alarm > IO1**.

The **IO1** interface is displayed. See Figure 8-56.

Figure 8-56 IO1



**Step 4** Click  to enable local alarm.

**Step 5** Set parameters. For details, refer to Table 8-17.

Table 8-17 Local alarm parameters description

Parameter	Description
Name	In the Alarm name box, enter a name for the alarm.
Type	Select alarm input device type. Both NO and NC are supported.
Debouncing	The system records only one event during this period.

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

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

- Click **View Schedule** to view detailed schedule settings.
- If the schedule is not added or the added schedule does not meet actual needs, click **Add Schedule**. Refer to "8.8.4 Schedule" for detailed information.

**Step 7** Click **Actions** to set alarm actions. Refer to "8.4.1 Alarm Actions" for detailed information.

**Step 8** Click **Save**.

### 8.4.3 Remote Device

Set alarm actions of remote device, including video detection alarm, offline alarm and AI plan of remote device.



The parameters might be different depending on the model you purchased. The actual interface shall prevail.

### 8.4.3.1 Video Detect

Video detection function adopts the PC visual, image and graphical processing technology to analyze the video image and check there is considerable changes on the video. Once there is considerable video changes (such as there is any moving object, or the video is blurred), system triggers corresponding alarm event.

#### 8.4.3.1.1 Configuring Video Motion

After analyzing video, system can generate a video motion alarm when the detected moving target reaches the sensitivity you set here.

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

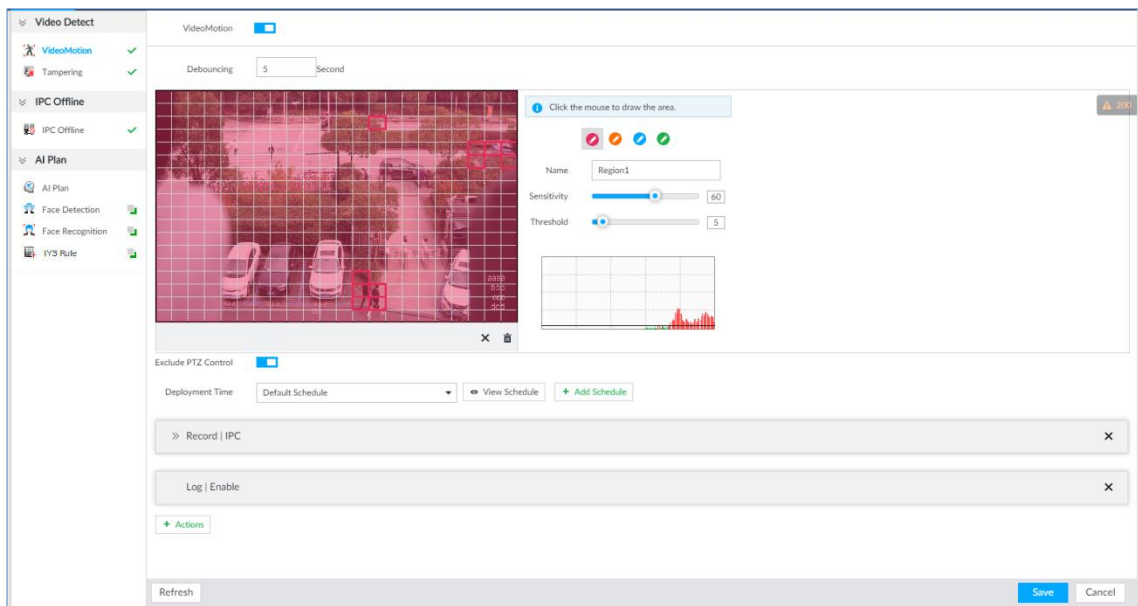
The **EVENT** interface is displayed.


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

**Step 3** Select **Video Detect > Video Motion**.

The **Video Motion** interface is displayed. See Figure 8-57.

Figure 8-57 Video motion




**Step 4** Click  to enable video motion detection.

**Step 5** Set parameters. For details, refer to Table 8-18.

Table 8-18 Motion detect parameters description

Parameter	Description
Debouncing	System only records one alarm event during the debouncing period.

Parameter	Description
Exclude PTZ control	After enabling exclude PTZ control, system does not trigger an alarm when you are manually control the PTZ.  It is for PTZ camera only.

**Step 6** Set motion detection region.

System supports maximum four detection zones. After setting, once there is an alarm from any of these four zones, the remote device trigger an alarm.






- 1) Click motion detection zone icon .
- 2) On the surveillance video, press and hold on the left button of mouse to select detection zone.
  - Select the motion detect zone you have drawn. Click  to delete the zone.
  - Click  to clear the zone you have drawn.
- 3) Set parameters. For details, refer to Table 8-19.

Table 8-19 Description of zone parameters

Parameter	Description
Name	It is to set detection zone name to distinguish different zones.
Sensitivity	Drag  to set sensitivity. The higher the sensitivity is, the easier it is to trigger an alarm. At the same time, the false alarm rate increases as well. Usually we recommend the default value.
Threshold	Drag  to adjust threshold. Once the detected percentage (the percentage of target to detection zone) is equivalent to or larger than the specified threshold, system triggers alarm. For example, the threshold is 10. Once the detected target occupies the 10% of the detection zone, system triggers an alarm.

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

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

- Click **View Schedule** to view detailed schedule settings.
- If the schedule is not added or the added schedule does not meet actual needs, click **Add Schedule**. Refer to "8.8.4 Schedule" for detailed information.

**Step 8** Click **Actions** to set alarm actions. Refer to "8.4.1 Alarm Actions" for detailed information.

**Step 9** Click **Save**.

### 8.4.3.1.2 Tampering

Once something tampers the surveillance video, and the output video is in one color, the system can generate an alarm.

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

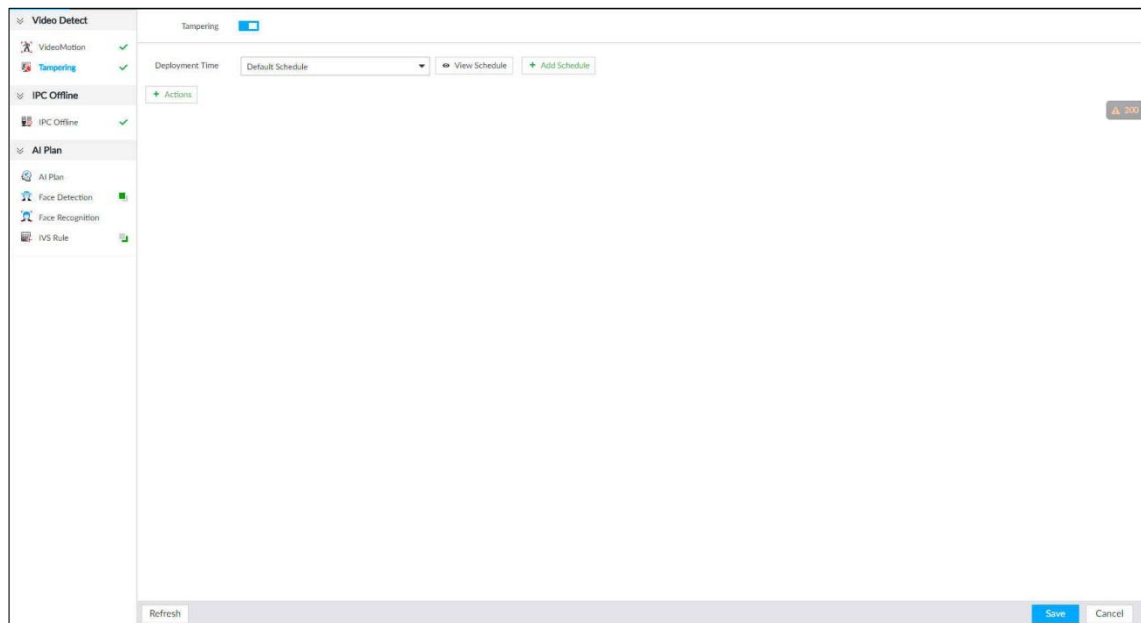
The **EVENT** interface is displayed.


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

**Step 3** Select **Video Detect > Tampering**.

The **Tampering** interface is displayed. See Figure 8-58.

Figure 8-58 Tampering



**Step 4** Click  to enable tampering alarm.

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

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

- Click **View Schedule** to view detailed schedule settings.
- If the schedule is not added or the added schedule does not meet actual needs, click **Add Schedule**. Refer to "8.8.4 Schedule" for detailed information.

**Step 6** Click **Actions** to set alarm actions. Refer to "8.4.1 Alarm Actions" for detailed information.

**Step 7** Click **Save**.

### 8.4.3.2 Offline Alarm

When the remote device and the IVSS is disconnected, system can trigger an alarm.

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

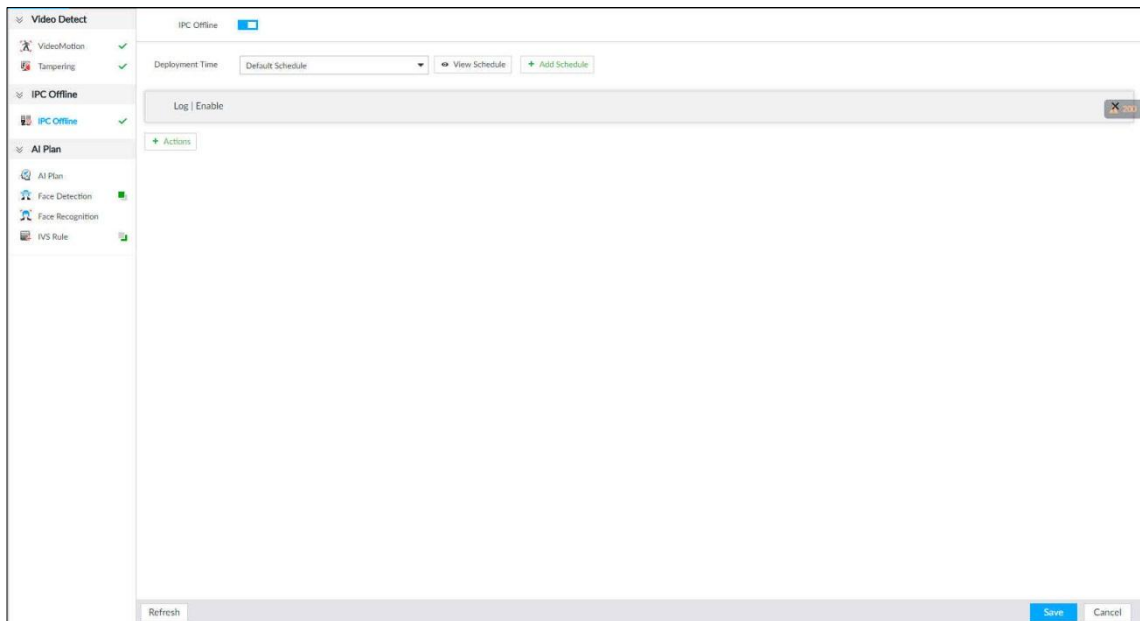
The **EVENT** interface is displayed.


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

**Step 3** Select **IPC Offline > IPC Offline**.

The **IPC Offline** interface is displayed. See Figure 8-59.

Figure 8-59 IPC offline



**Step 4** Click  to enable IPC offline alarm.



The IPC offline alarm is enabled by default. You can skip this step.

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



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

- Click **View Schedule** to view detailed schedule settings.
- If the schedule is not added or the added schedule does not meet actual needs, click **Add Schedule**. Refer to "8.8.4 Schedule" for detailed information.

**Step 6** Click **Actions** to set alarm actions. Refer to "8.4.1 Alarm Actions" for detailed information.

**Step 7** Click **Save**.

## 8.5 Storage Management

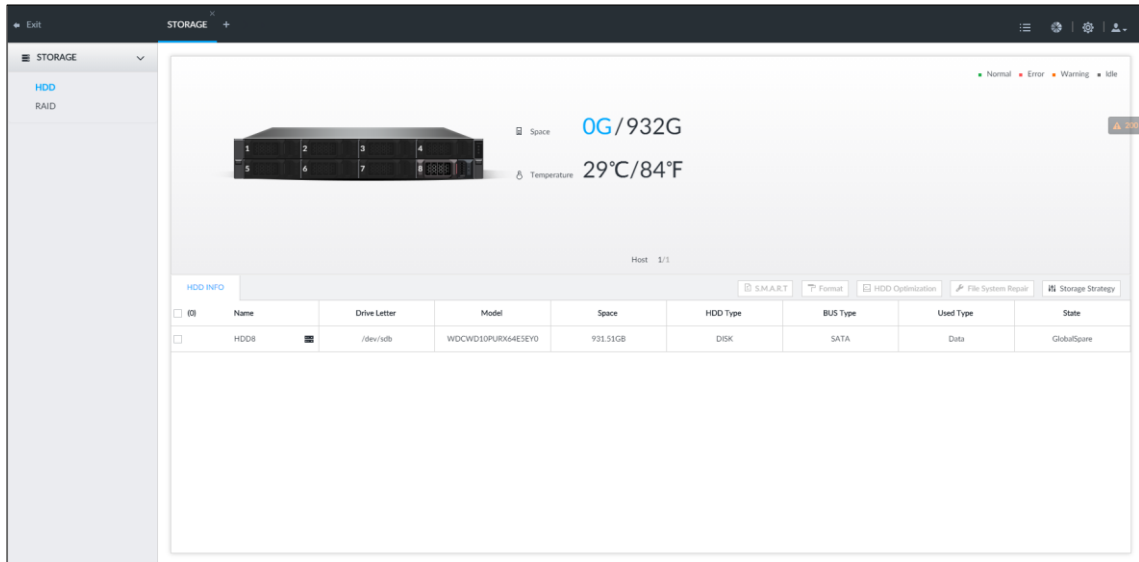
Click  or click  on setting interface, select **Storage**. The **Storage** interface is displayed. See Figure 8-60. Manage storage resources (such as recording file) and space, so you can use and improve utilization ratio of storage space.



The system supports pre-check and routine inspection function, displays health status on the Storage interface, so you obtain real-time status of device and avoid data loss.



- **Pre-check:** during device operation, the system automatically detects disc status in case of change (reboot, insert and pull the disc).
- **Routine inspection:** the system carries out routine inspection of the disc continuously. During device operation, the disc may go wrong due to service life, environment and other factors. Find out any problems during routine inspection.




Figure 8-60 Storage management



## 8.5.1 HDD

The physical HDD refers to the HDD installed on the system. On this interface, you can view HDD space (free space/total space), temperature (centigrade/Fahrenheit), HDD information and so on.

Click , or click  on setting interface, and then select **Storage > HDD**. The **HDD** interface is displayed. See Figure 8-61. There is a corresponding icon near the HDD name after you create the RAID and hot spare HDD.

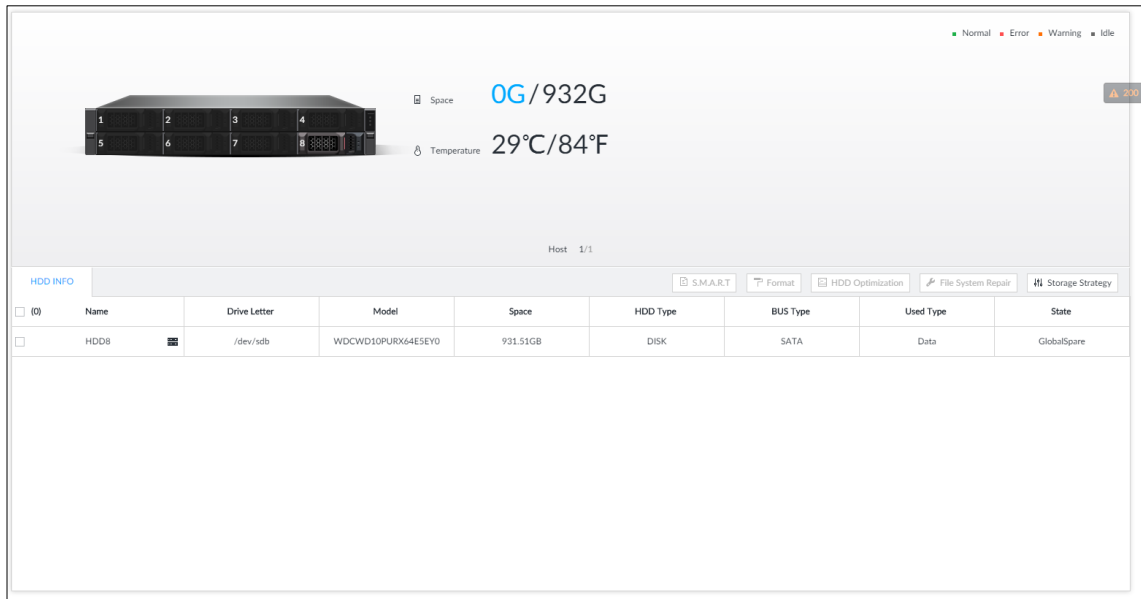
-  : RAID HDD.
-  : Global hot spare HDD.
-  : Invalid private hot spare HDD.



Slight difference may be found on the user interface. The actual interface shall prevail.



Figure 8-61 HDD



### 8.5.1.1 View S.M.A.R.T

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



Check one HDD to view S.M.A.R.T information at one time.



On the HDD interface, select a HDD, and then click **S.M.A.R.T**. The **S.M.A.R.T** interface is displayed. See Figure 8-62. Check whether the HDD status is OK or not. If there is any problem, fix it in time.

Figure 8-62 S.M.A.R.T

Sn	Note	Value	Worst	Boundary	Original Data	State
1	Read Error Rate	117	99	6	135185072	Better
3	Spin Up Time	97	97	0	0	Better
4	Start/Stop Co...	100	100	20	780	Better
5	Reallocated S...	100	100	36	0	Better
7	Seek Error Rate	67	60	30	17203264542	Better
9	Power On Ho...	98	98	0	2426	Better
10	Spin-up Retry...	100	100	97	0	Better
12	Power On/Of...	100	100	20	752	Better
184	End-to-End F	100	100	99	0	Better

### 8.5.1.2 Set storage strategy

It is to set storage strategy when HDD space is full.

**Step 1** Click , or click  on setting interface, and then select **Storage > HDD**.

The **HDD** interface is displayed.

**Step 2** Click **Storage Strategy**.

The **Storage Strategy** interface is displayed. See Figure 8-63.

Figure 8-63 Set storage strategy

Set Storage Strategy ✕

---

HDD full     Overwrite     Stop

---

**Step 3** Set storage strategy.

- **Overwrite:** When HDD free space is less than 50G or it is less than 1% of the total space, which one it is larger, system continues to record and begins overwriting the oldest record file.
- **Stop:** When HDD free space is less than 50G or it is less than 1% of the total space, which one it is larger, system stops recording.



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

### 8.5.1.3 HDD Cleanup

After the HDD is working for a period time, since it is repeatedly written or files are deleted, the files are saved on the discontinued physical position on the HDD. It may result in too much HDD fragmentation and slow down the HDD access speed. The HDD cleanup is to organize the fragmentation files on the HDD and make the fragmentation files become the continuous files. It can enhance HDD whole performance and running speed.



HDD cleanup may result in some record file loss.

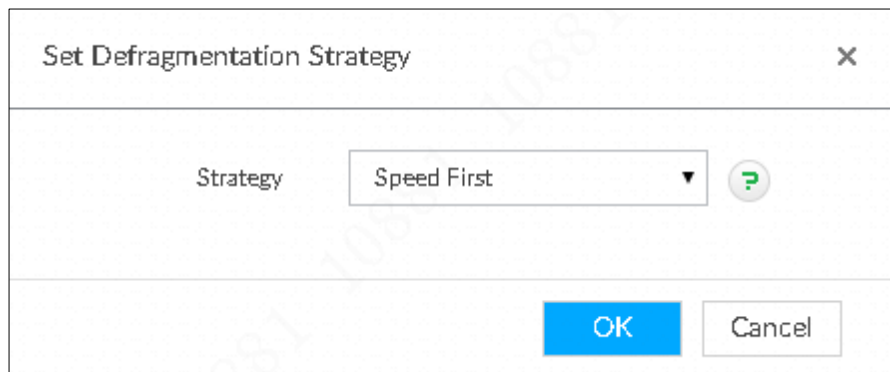
**Step 1** Click , or click  on setting interface, and then select **Storage > HDD**.

The **HDD** interface is displayed.

**Step 2** Select one and more HDD(s) and then click **HDD Optimization**.

The **Set Defragmentation Strategy** is displayed. See Figure 8-64.

Figure 8-64 Set defragmentation strategy



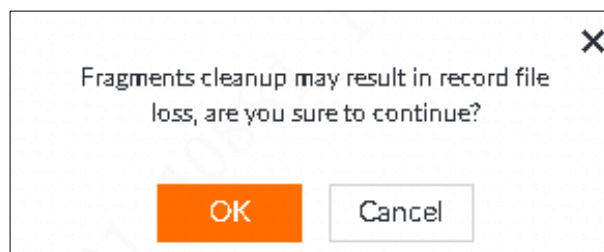
**Step 3** Select HDD defragmentation strategy.

- Speed first: Cleanup HDD at fast speed. The max speed is 100M/s.
- Business first: System automatically adjusts HDD Cleanup speed according to current business load status.

**Step 4** Click **OK**.

The following prompt interface is displayed.

Figure 8-65 Prompt interface



**Step 5** Click **OK**.

System begins clearing up HDD. Now the HDD status displays as "**Cleanup**". After the HDD Cleanup, status becomes "**Running**".

## 8.5.1.4 Format



The format HDD operation is going to clear all data on the HDD. Be careful!

Enter HDD interface, select one or more HDD(s), and click **Format**. It is to format the selected HDD.

## 8.5.1.5 File system repair

Once you cannot mount the HDD or you cannot properly use the HDD, you can try to use repair file system function to fix.

Enter HDD interface, select one or more HDD(s) you cannot mount, and click **File System Repair**, you can repair the selected file system of the corresponding HDD(s). The repaired HDD can work properly or to be mounted.

## 8.5.2 RAID

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



- Right now, device supports RAID 0, RAID 1, RAID 5, RAID 6, and RAID 10. Refer to "Appendix 2 RAID" for detailed information.
- It is recommended to use enterprise HDD when you are creating RAID. It is recommended to use surveillance HDD in case of one HDD.

### 8.5.2.1 Create RAID

RAID has different levels such as RAID 5, RAID 6 and so on. Different RAID levels have different data protection, data availability and performance levels. Create RAID according to your actual requirements.



Creating RAID operation is going to clear all data on these HDD. Be careful!

### Shortcut menu to create RAID

Shortcut menu to create RAID 5. To create RAID 5 with shortcut menu, the system adopts different creation strategies according to disc quantity. For details, see Table 8-20.



In the following table, among the numbers in the creation strategy, the number without () represents the disk number of the RAID group. The number with () represents the number of hot spare disks. For example, for 24 HDD, the creation strategy is 7+7+9+(1). It means three

RAID 5 and one hot spare, and each RAID 5 respectively contains 7 disks, 7 disks and 9 disks.

Table 8-20 Shortcut menu to create RAID

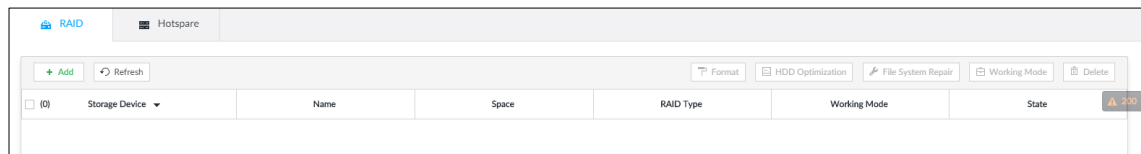
HDD No.	Creation Strategy	HDD No.	Creation Strategy
3	Not recommended	14	6+7+(1)
4	Not recommended	15	7+7+(1)
5	5	16	5+5+5+(1)
6	5+(1)	17	5+5+6+(1)
7	6+(1)	18	5+6+6+(1)
8	7+(1)	19	6+6+6+(1)
9	8+(1)	20	6+6+7+(1)
10	9+(1)	21	6+7+7+(1)
11	5+5+(1)	22	7+7+7+(1)
12	5+6+(1)	23	7+7+8+(1)
13	6+6+(1)	24	7+7+9+(1)

## Create RAID

**Step 1** Click , or click  on setting interface, and then select **Storage > RAID > RAID**.

The **RAID** interface is displayed. See Figure 8-66.

Figure 8-66 RAID (1)



**Step 2** Click **Add**.

The **Create RAID** interface is displayed. See Figure 8-67.

Figure 8-67 Create RAID (1)

Create RAID

1 HDD Selection 2 Confirm Info

Create RAID  Manual  Auto

Storage Device: Host02/8HDD Available

<input type="checkbox"/>	(0) Name	Drive Letter	Model	Space	HDD Type	BUS Type	Used Type	State
<input type="checkbox"/>	HDD4	/dev/sdd	WDCWD10..	930.96GB/9..	DISK	SATA	Data	Running
<input type="checkbox"/>	HDD6	/dev/sdb	ST3500312C5	458.27GB/4..	DISK	SATA	Data	Running

RAID: RAID5

WorkingMode: Self-Adaptive

Name: RAID5\_1

Estimated Space: 0


Next Cancel

**Step 3** Set RAID parameters.

Select RAID creation type according to actual situation. It includes Manual RAID and Auto RAID.

- Manual RAID: System creates a specified RAID type according to the selected HDD amount.
  1. Select **Manual RAID**.
  2. Select HDD you want to use.
  3. Set parameters. For details, refer to Table 8-21.

Table 8-21 Manual creation parameters description

Parameter	Description
Storage Device	It is to select storage device of the HDD and select the HDD you want to add to the RAID.  Different RAID types need different HDD amounts, and the actual situation shall prevail.
RAID	Select a RAID type you want to create.
Working mode	It is to set RAID resources allocation mode. The default setup is self-adaptive. <ul style="list-style-type: none"> <li>• Self-adaptive means the system can automatically adjust RAID synchronization speed according to current business load. When there is no external business, the synchronization speed is at high speed. When there is external business, the synchronization speed is at low speed.</li> <li>• Sync first: Allocate resources to RAID synchronization first.</li> <li>• Business first: Allocate resources to business first.</li> <li>• Load-Balance: Allocate resources to business and RAID synchronization equally.</li> </ul>

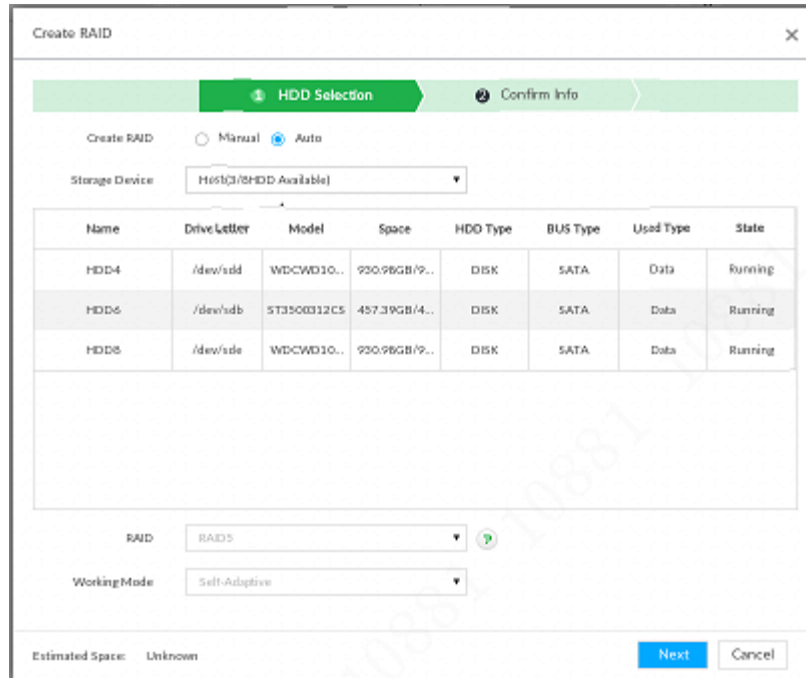
Parameter	Description
Name	It is to set RAID name.

- Auto: System creates RAID 5 according to the HDD amount.

1. Select **Auto**.

The **Auto** interface is displayed. See Figure 8-68.

Figure 8-68 Create RAID (2)



2. Set parameters. For details, refer to Table 8-21.

Table 8-22 Auto parameters description

Parameter	Description
Storage Device	It is to select storage device of the HDD.
Working mode	<p>It is to set RAID resources allocation mode. The default setup is self-adaptive.</p> <ul style="list-style-type: none"> <li>• Self-adaptive means the system can automatically adjust RAID synchronization speed according to current business load. When there is no external business, the synchronization speed is at high speed. When there is external business, the synchronization speed is at low speed.</li> <li>• Sync first: Allocate resources to RAID synchronization first.</li> <li>• Business first: Allocate resources to business first.</li> <li>• Load-Balance: Allocate resources to business and RAID synchronization equally.</li> </ul>

**Step 4** Click **Next** button.

The **Confirm Info** interface is displayed. See Figure 8-69 or Figure 8-70.

Figure 8-69 Confirm info (manual)

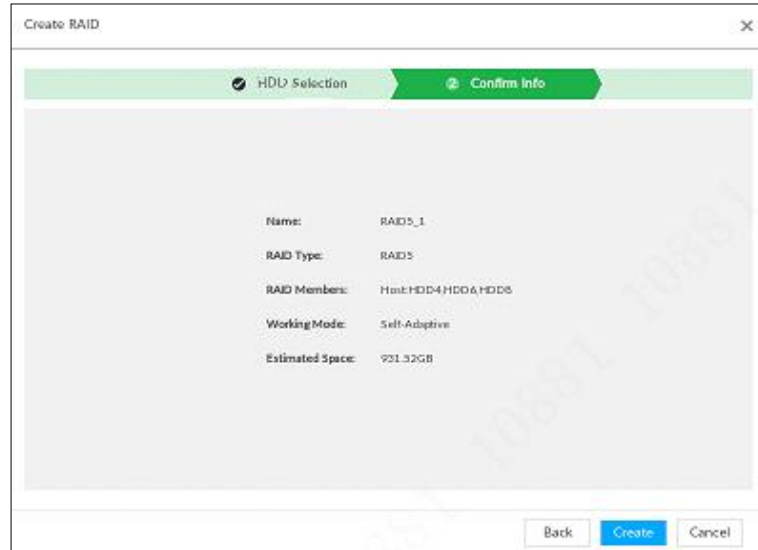
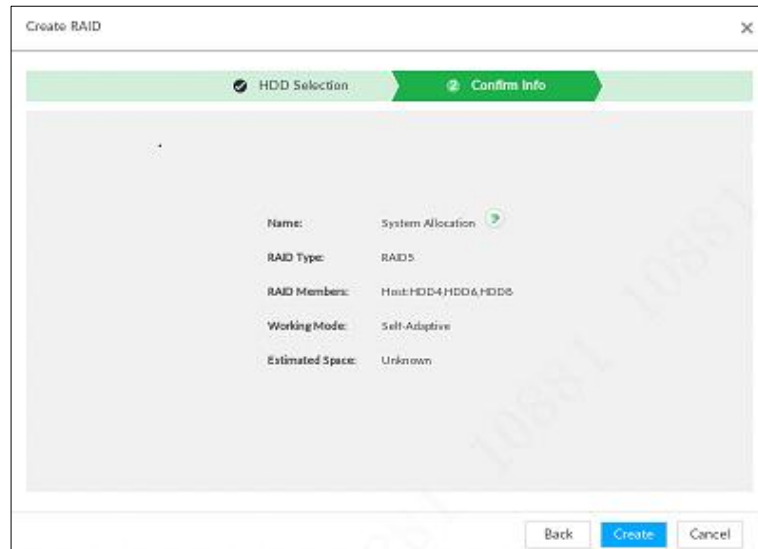


Figure 8-70 Confirm info (Auto)



**Step 5** Confirm info.



If the input information is wrong, click **Back** to set RAID parameters again.

**Step 6** Click **Create**.

System begins to create RAID. It displays RAID information after creation. See Figure 8-71.

Figure 8-71 RAID (2)

	Storage Device	Name	Space	RAID Type	Working Mode	State
1	Host	RAID5_1	~931.32GB	RAID5	Self-Adaptive	Active, Degraded, Recovering

## Operation

After creating RAID, view RAID disk status and details, clear up RAID, and repair file system. For details, see Table 8-23.

Table 8-23 RAID operation







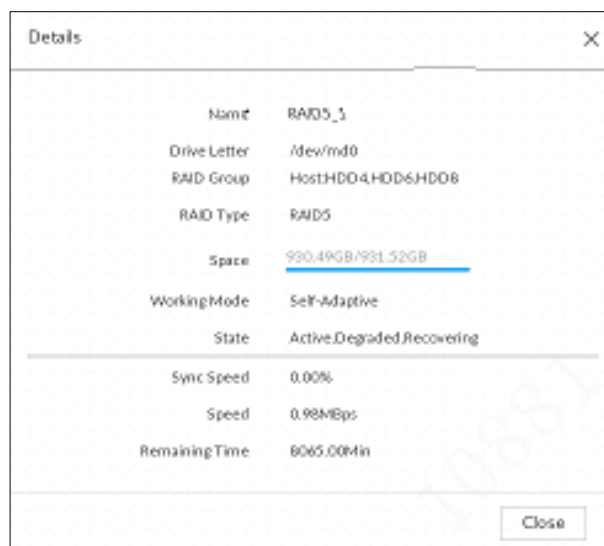


Name	Operation
View RAID HDD status	Click  at the right side of the RAID name to open the RAID HDD list. It is to view RAID HDD space, status and so on.
View RAID detail	Click  . It displays detailed information. See Figure 8-72. It is to view RAID detailed information.
RAID Cleanup	Enter RAID interface and then select one or more RAID, click <b>HDD Cleanup</b> . It is to Cleanup HDD and files. Refer to "8.5.1.3 HDD for detailed information.
File system repair	Once you cannot mount the RAID or you cannot properly use the RAID, you can try to use repair file system function to fix. Enter RAID interface, select one or more RAID(s) you cannot mount, click <b>File System Repair</b> , you can repair the selected file system of the corresponding RAID(s). The repaired RAID can work properly or to be mounted.
Format RAID	 Formatting RAID is to clear all data on the RAID and cancel the RAID group. Please be careful. Enter RAID interface, select one and more RAID groups. Click <b>Format</b> to format the selected RAID.
Delete RAID	 Deleting RAID is to clear all data on the RAID and cancel the RAID group. Please be careful. Enter RAID interface, select one and more RAID groups. Click <b>Delete</b> to delete the selected RAID.

Figure 8-72 RAID detail



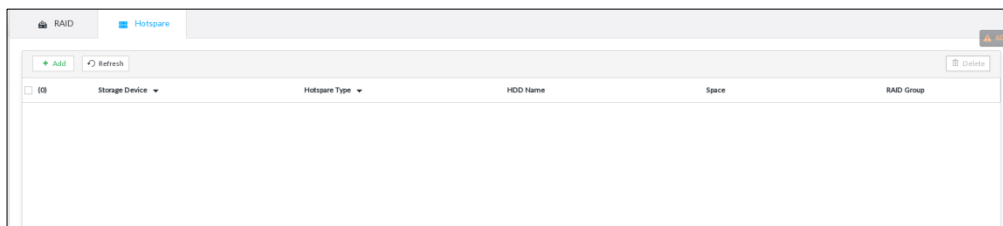
## 8.5.2.2 Create Hot spare HDD

When a HDD of the RAID group is malfunctioning or has a problem, the hot spare HDD can replace the malfunctioning HDD. There is no risk of data loss and it can guarantee storage system reliability.

**Step 1** Click , or click  on setting interface, and then select **Storage > RAID > Hot spare**.

The **Hot spare** interface is displayed. See Figure 8-73.

Figure 8-73 Hot spare (1)



**Step 2** Click **Add**.

The **Add** interface is displayed. See Figure 8-74 or Figure 8-75.

Figure 8-74 Global hot spare

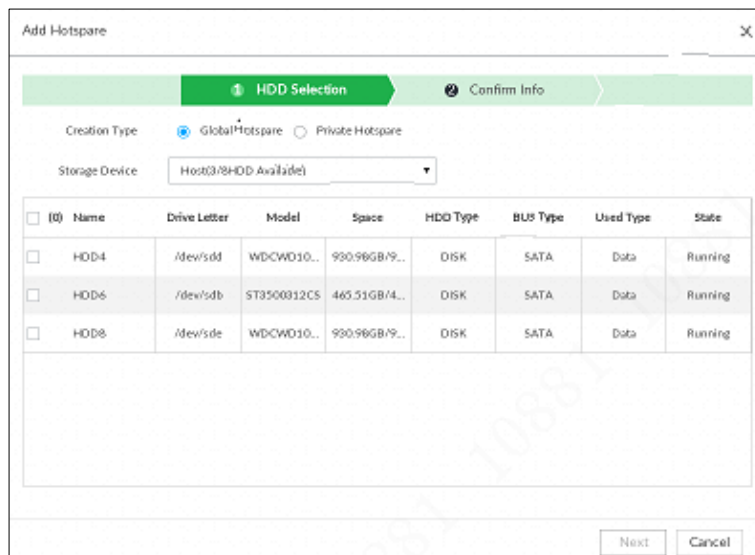
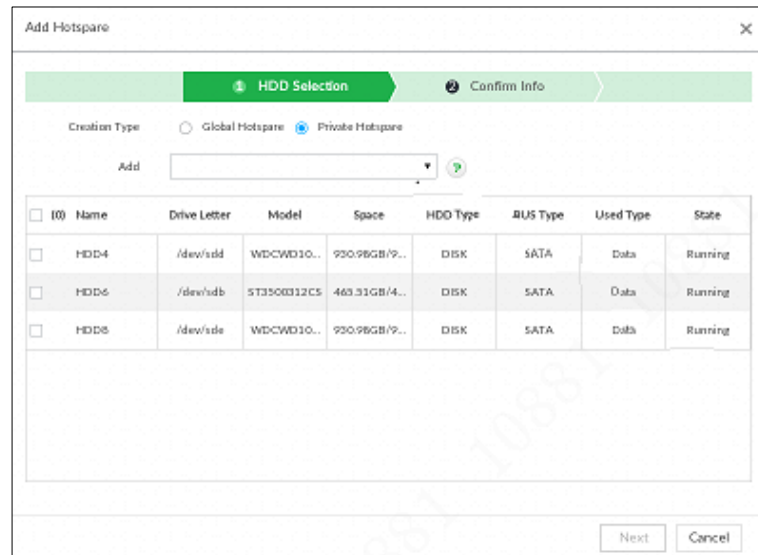


Figure 8-75 Private hot spare



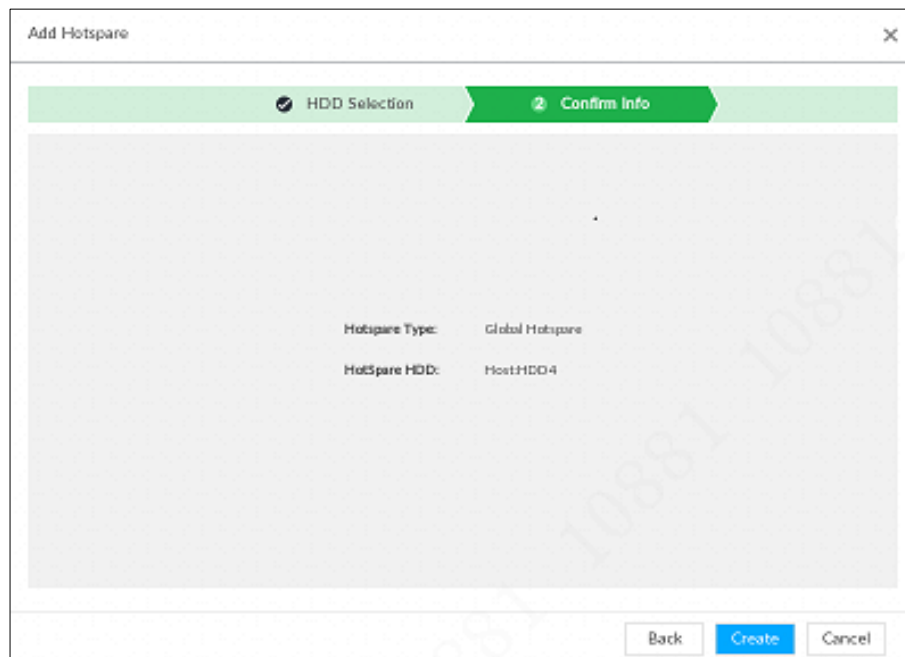
**Step 3** Select hot spare creation type.

- Global hot spare: It is to create hot spare for all RAID. It is not a hot spare HDD for a specified RAID group.
- Private hot spare: Select **Private Hot spare** and **Add** it to a RAID group. The private hot spare HDD is for a specified RAID group.

**Step 4** Select one or more HDD(s) and then click **Next**.

The **Confirm Info** interface is displayed. See Figure 8-76.

Figure 8-76 Confirm info



**Step 5** Confirm info.



Click **Back** to select hot spare HDD(s) again if you want to change settings.

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

System displays the added hot spare HDD information. See Figure 8-77.

Figure 8-77 Hot spare (2)



	Storage Device	Hotspare Type	HDD Name	Space	RAID Group
1	Host	Global Hotspare	HDD4	901.53GB	-



Select a hot spare HDD and then click **Delete**, it is to delete hot spare HDD.



## 8.5.3 Storage Strategy

Allocate disks or RAID groups to different disk groups, and store video and image to specified disk group.

### 8.5.3.1 Setting Disk Group

Disk and created RAID group are allocated to group 1 by default. You can allocate disk and RAID group to other groups according to your actual needs.

The default number of disk group is the same as the maximum number of HDD that IVSS supports. For example, IVSS supports a maximum number of 16 HDDs, then the default number of disk group is 16.

**Step 1** Click , or click  on the setting interface, and then select **STORAGE > Storage Strategy > Disk Group**.

The **Disk Group** interface is displayed. See Figure 8-78.





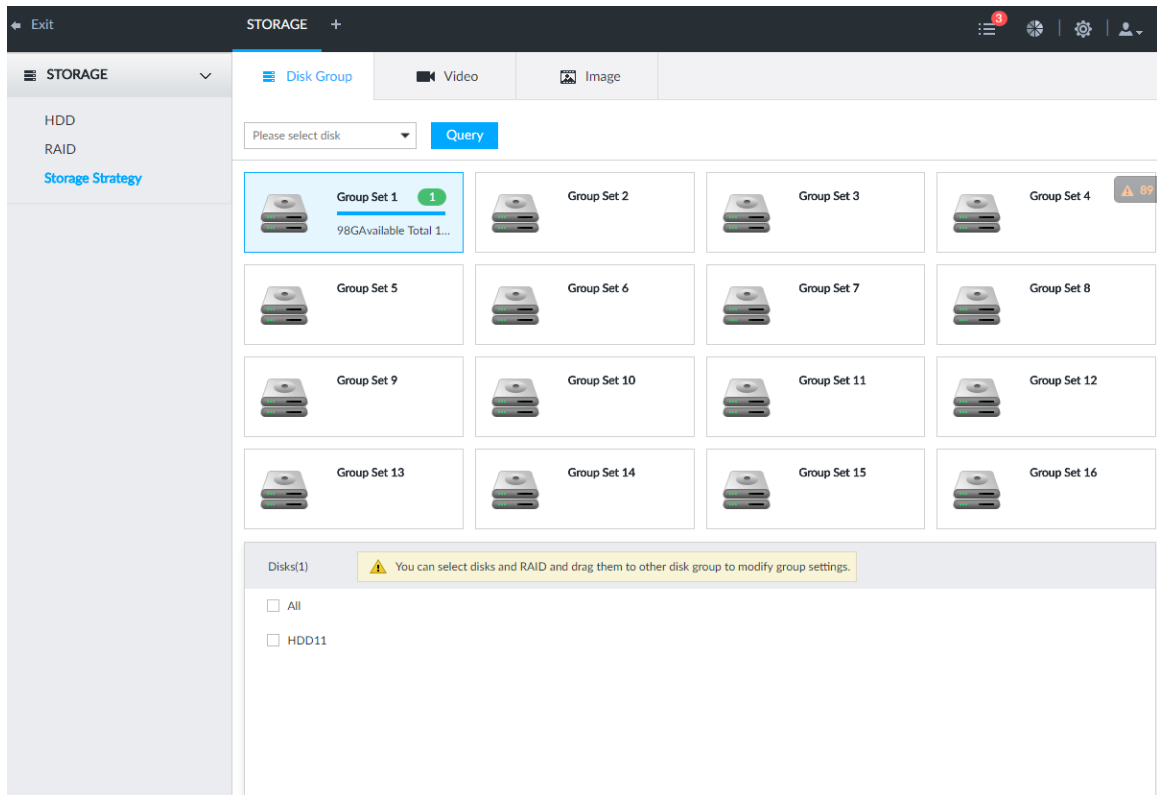
- Select HDD or RAID group from  , and then click **Query** to search the disk group of HDD or RAID group.
- The value (such as ) next to the group name refers to the number of HDD and RAID group in the disk group. If instead,  is displayed, it means no available HDD or RAID group in the disk group, but there is video or image stored in the disk group.

Figure 8-78 Disk group



**Step 2** Click a disk group.

The disk information of the group is displayed.

**Step 3** Select HDD or RAID group from **Disks**, and then drag the HDD or the RAID group to another disk group.

Disk grouping takes effect immediately.



Select **All** to select all the HDDs and RAID groups of the disk group.



### 8.5.3.2 Setting Video/Image Storage

Videos/images of all channels are stored in disk group 1 by default. You can store the videos/images in different disk groups according to actual needs. Two methods are available to set video/image storage.



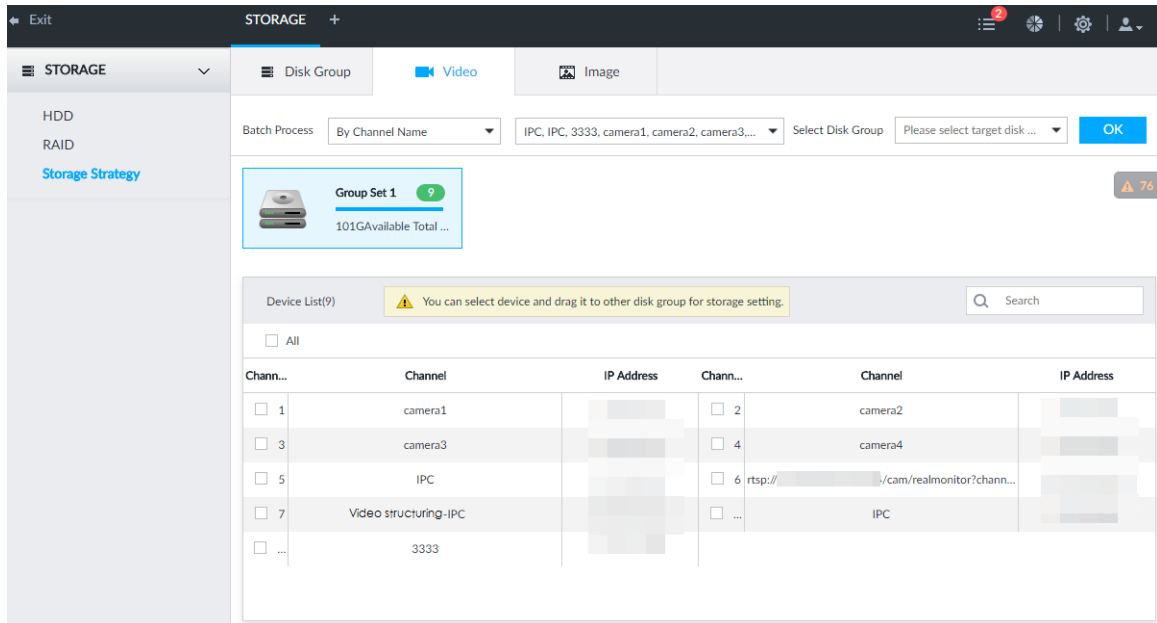
This section takes storing video for example. To store images, refer to this section.

#### Method 1

**Step 1** Click , or click  on the setting interface, then select **STORAGE > Storage Strategy > Video**.

The **Video** interface is displayed. See Figure 8-79.

Figure 8-79 Video



**Step 2** Select filtering way from the **Batch Process** dropdown list.

- By Channel Name: Select channel according to the channel name.
- By Logical Channel No.: Select channel that is connected to IVSS. In this case, **Start Channel No.** and **End Channel No.** need to be configured.

**Step 3** In the **Select Disk Group** dropdown list, select target disk group.





In the dropdown list, only disk group with available HDD or RAID group is displayed.

**Step 4** Click **OK**.

Disk grouping takes effect immediately.

## Method 2

**Step 1** Click , or click  on the setting interface, then select **STORAGE > Storage Strategy > Video**.

The **Video** interface is displayed. See Figure 8-79.

**Step 2** Click a disk group.

The linked channels of the disk group are displayed in **Device List**. See Figure 8-80.





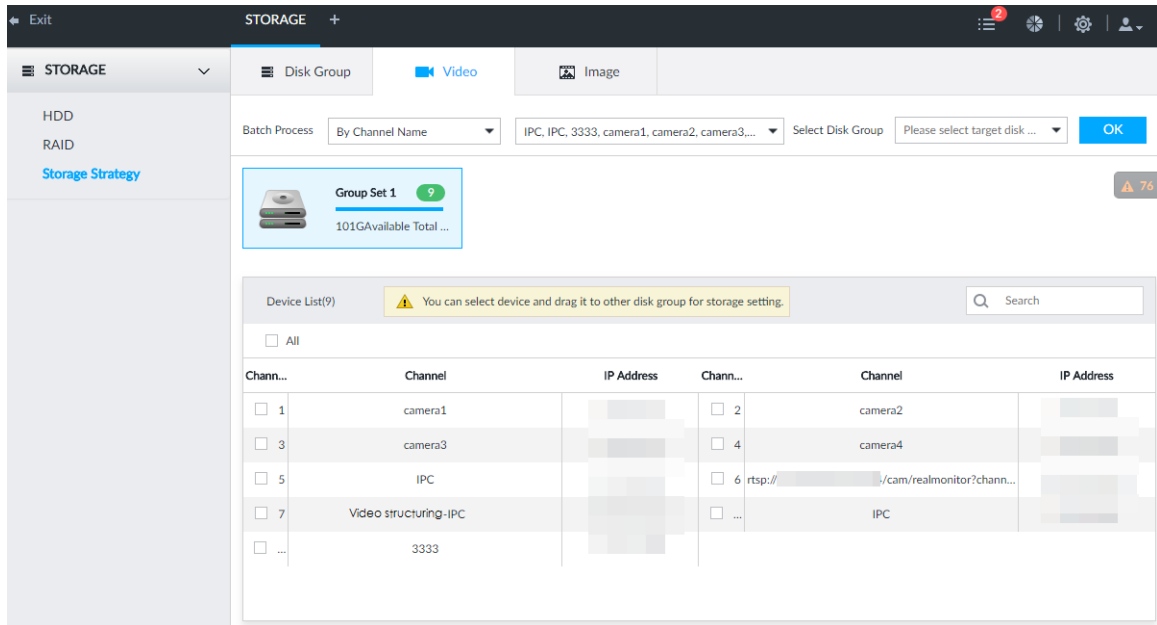


- Only disk group with available HDD or RAID group or linked channel is displayed.
- The value (such as ) next to the group name refers to the number of HDD and RAID group in the disk group. If instead,  is displayed, it means no available HDD or RAID group in the disk group, but there is video or image stored in the disk group.
-

Figure 8-80 Device list



**Step 3** Select channel from the device list, and drag the channel to the target disk group. Disk grouping takes effect immediately.

## 8.6 Security Strategy

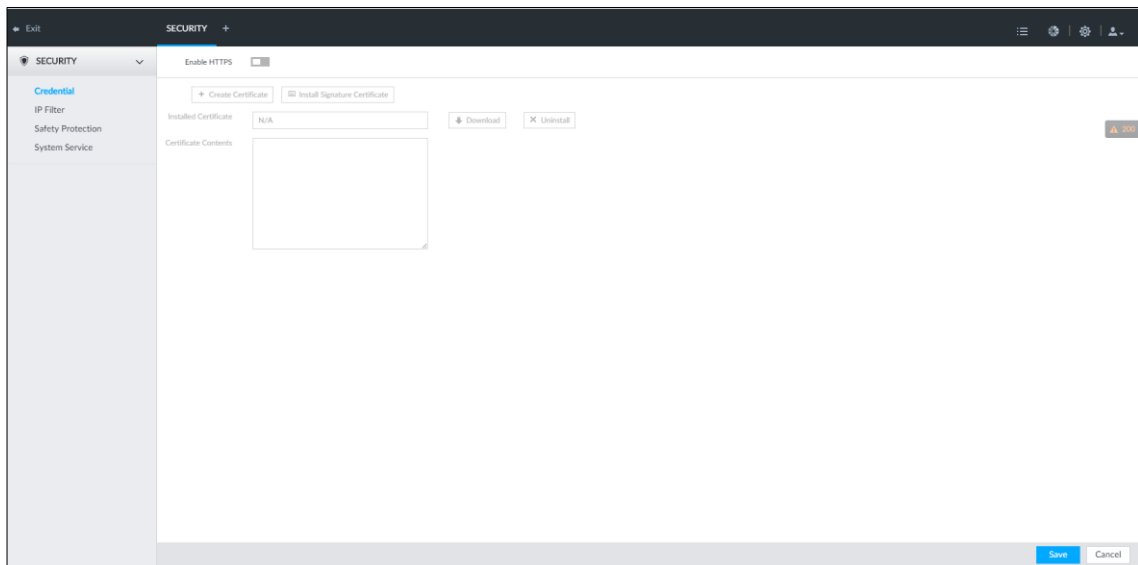
Click  or click  on setting interface, select **Security**. The **Security** interface is displayed. See Figure 8-81.

It is to set security strategy to guarantee device network and data safety. It includes HTTPS, set host IP access rights, enable network security protection.



HTTPS function is for WEB and IVSS Client only. Refer to the actual interface for detailed information.

Figure 8-81 Security center



## 8.6.1 HTTPS

HTTPS can use the reliable and stable technological means to guarantee user information and device security and communication data security. After installing the certificate, you can use the HTTPS on the PC to access the device.

### 8.6.1.1 Install Certificate

System supports these two certificates. Install according to your actual requirements.

- Manually create the certificate.
- Install the signed certificate.

#### 8.6.1.1.1 Install the Created Certificate

It is to install the created certificate manually. It includes creating the certificate on the device, downloading and installing the certificate on the PC.

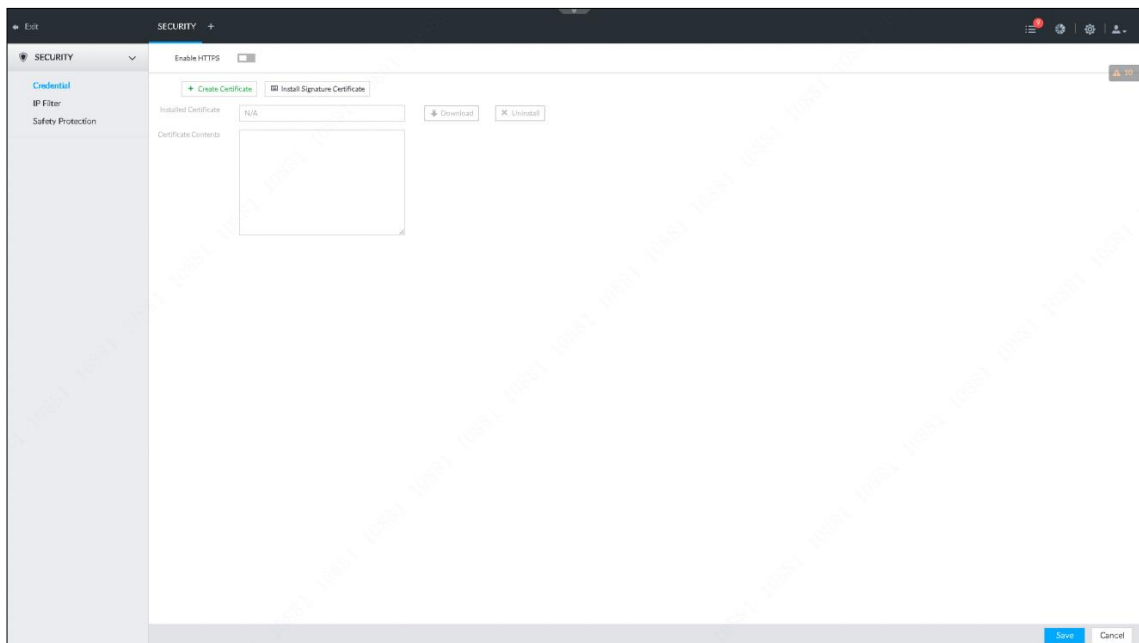


- Create and install root certificate if it is your first time to use HTTPS or you have changed device IP address.
- After creating server certificate and installing root certificate, download and install root certificate on the new PC, or download the certificate and then copy to the new PC.

Step 1 Click , or click  on setting interface, and then select **Security > Credential**.

The **Credential** interface is displayed. See Figure 8-82.

Figure 8-82 Credential (1)



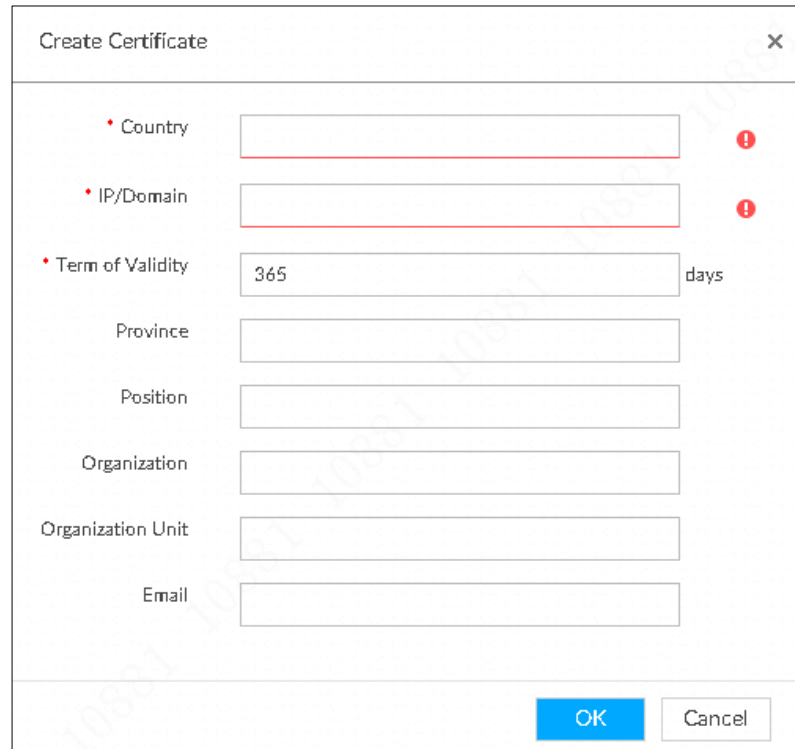
Step 2 Create certificate on the device.

- 1) Click **Create certificate**.

The **Create certificate** interface is displayed. See Figure 8-83.



Figure 8-83 Create certificate



The 'Create Certificate' dialog box contains the following fields:

- Country: [Empty] (Required, indicated by a red dot and exclamation mark)
- IP/Domain: [Empty] (Required, indicated by a red dot and exclamation mark)
- Term of Validity: 365 days
- Province: [Empty]
- Position: [Empty]
- Organization: [Empty]
- Organization Unit: [Empty]
- Email: [Empty]

Buttons: OK, Cancel

2) Set country, IP/domain, valid date and so on.

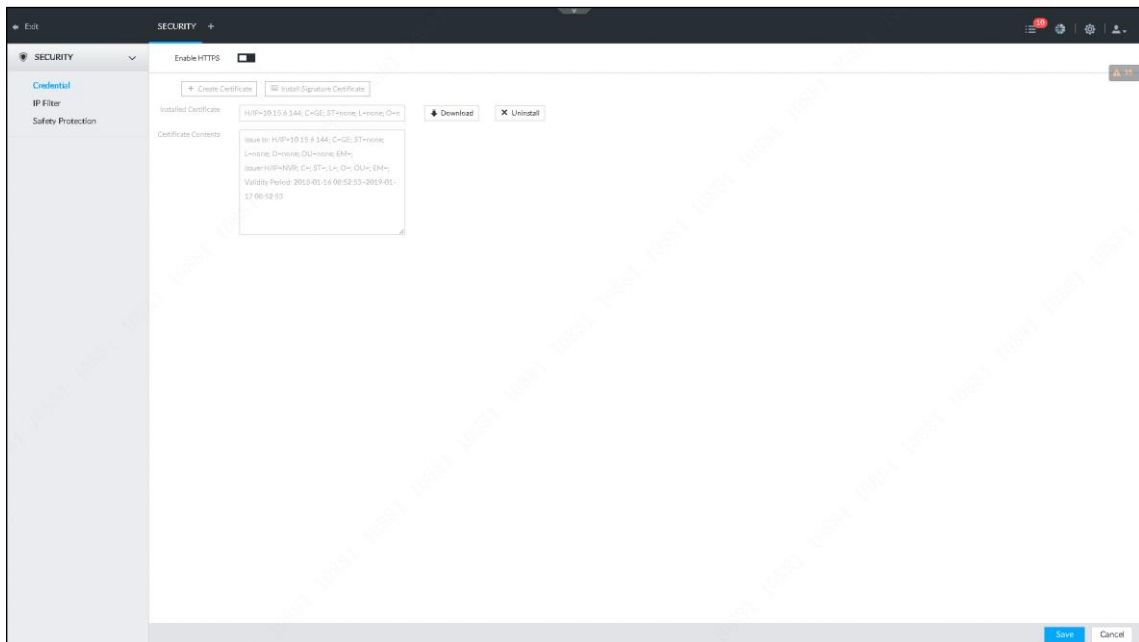


- Country, IP/domain, and valid date are required items. Other items are optional.
- IP/domain shall be the device IP or the domain.

3) Click **OK**.

System begins to install certificate, and then displays certificate information after the installation. See Figure 8-84.

Figure 8-84 Credential (2)

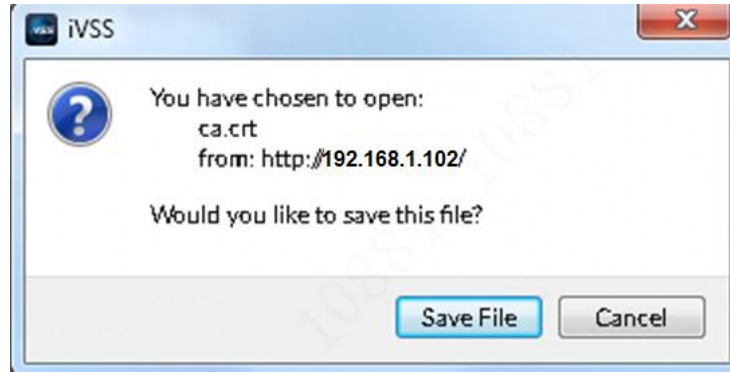


Step 3 Download certificate.

- 1) Click .

The **Opening ca.crt** interface is displayed. See Figure 8-85.

Figure 8-85 Opening ca.crt



- 2) Click **Save File** to select file saved path.
- 3) Click **Save**.  
System begins downloading certificate file.

**Step 4** Install root certificate on the PC.

- 1) Double click the certificate.  
System displays **Open file-security warning** interface.
- 2) Click **Open**.  
System displays **Certificate** interface. See Figure 8-86.

Figure 8-86 Certificate



- 3) Click **Install Certificate**.  
The **Certificate Import Wizard** interface is displayed. See Figure 8-87.

Figure 8-87 Certificate import wizard



- 4) Follow the prompts to import the certificate.  
System goes back to **Certificate** interface.

Step 5 Click **OK** to complete certificate installation.

#### 8.6.1.1.2 Install Signature Certificate

It is to upload signature certificate to install.

#### Preparation

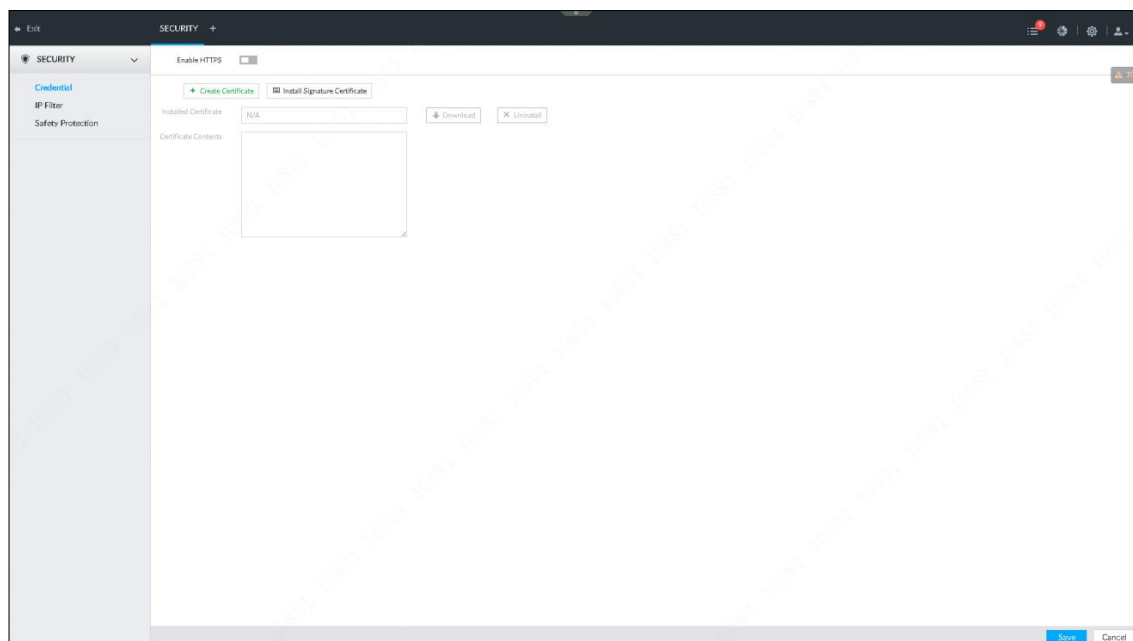
Before installation, make sure you have obtained safe and valid signature certificate.

#### Operation Steps

Step 1 Click , or click  on setting interface, and then select **Security > Credential**.

The **Credential** interface is displayed. See Figure 8-88.

Figure 8-88 Credential(1)



**Step 2** Click **Install Signature Certificate**.

The **Install Signature Certificate** interface is displayed. See Figure 8-89.

Figure 8-89 Install signature certificate



**Step 3** Click **Browse** and then select certificate and credential file.

**Step 4** Click **Install**.

System begins to install certificate, and then displays certificate information after the installation.

**Step 5** Install the root certificate on the PC. Refer to "8.6.1.1.1 Install the Created Certificate Step 4" for detailed information.



This root certificate is the one obtained with signed certificate.

## 8.6.1.2 Enable HTTPS

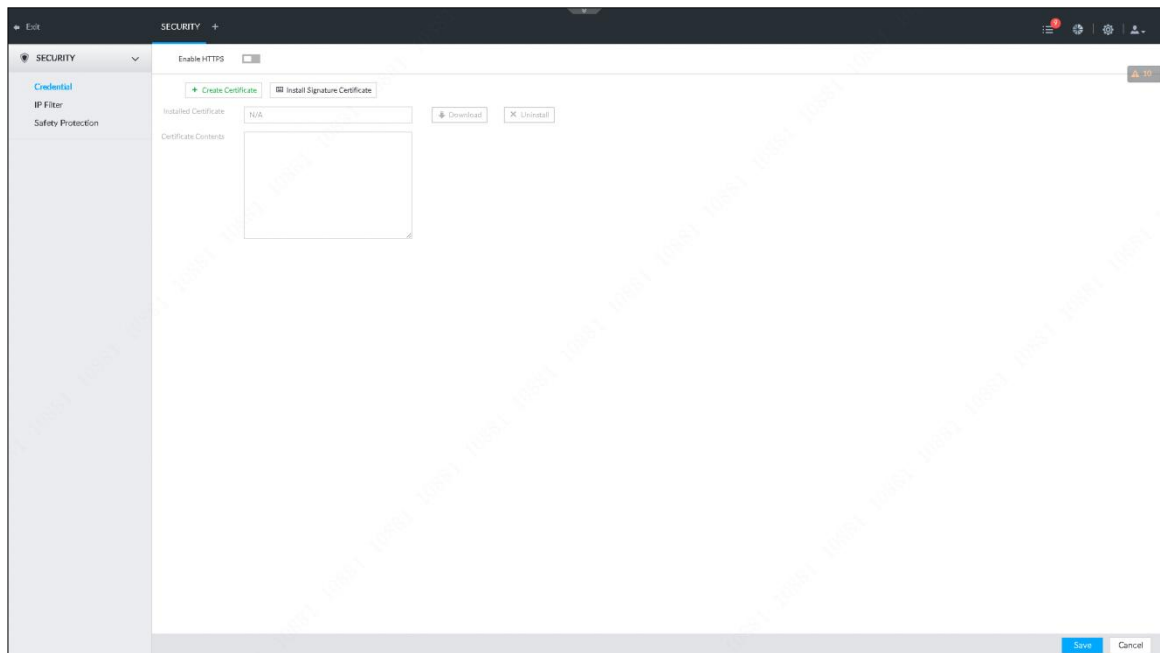
After you install the certificate and enable HTTPS function, you can use the HTTPS on the PC to access the device.

**Step 1** Click , or click  on setting interface, and then select **Security > Credential**.

The **Credential** interface is displayed.

**Step 2** Click  to enable HTTPS function. See Figure 8-90.

Figure 8-90 Credential



**Step 3** Click **Save**.

After you successfully save the settings, you can use HTTPS to access the WEB interface.

Open the browser and then input https://IP address:port, click **Enter**, and the login interface is displayed.



- IP address is device IP or the domain name.
- Port refers to device HTTPS port number. If the HTTPS port is the default value 443, just use https://IP address to access.

### 8.6.1.3 Uninstall the Certificate

It is to uninstall the certificate.

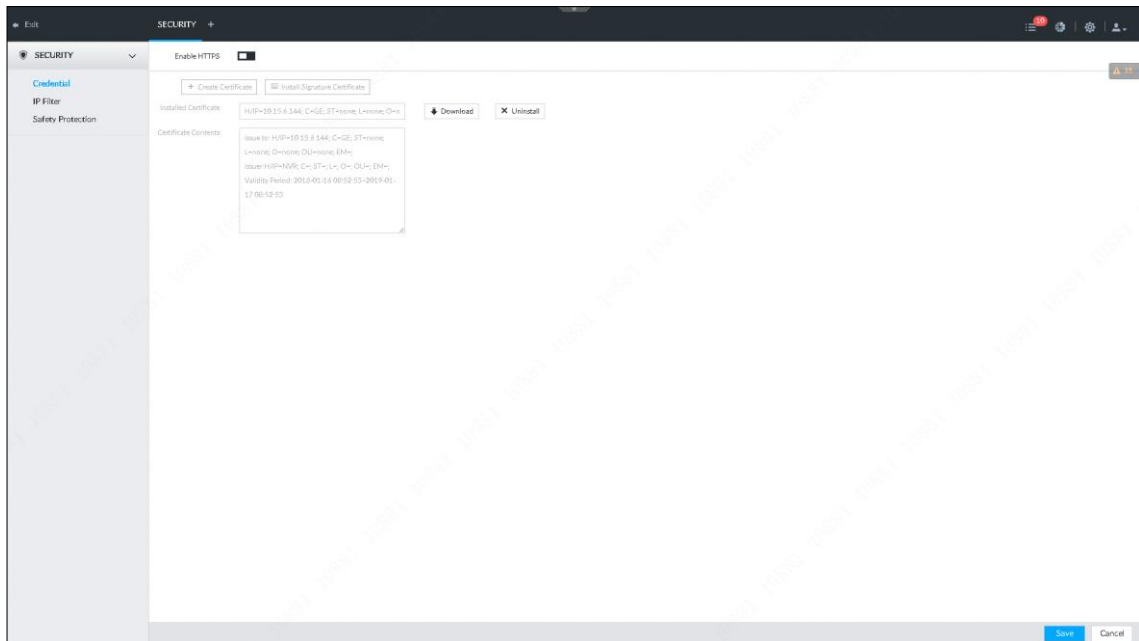


You cannot use the HTTPS function after you uninstall the certificate.

**Step 1** Click , or click  on setting interface, and then select **Security > Credential**.

The **Credential** interface is displayed. See Figure 8-91.

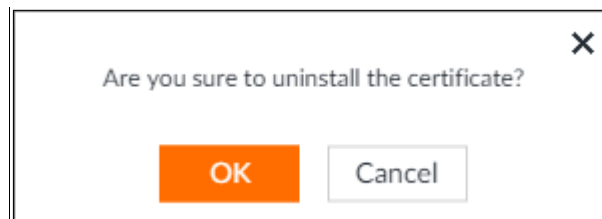
Figure 8-91 Credential



**Step 2** Click **Uninstall**.

System pops up a confirmation box. See Figure 8-92.

Figure 8-92 Confirmation



**Step 3** Click **OK** to uninstall the certificate.

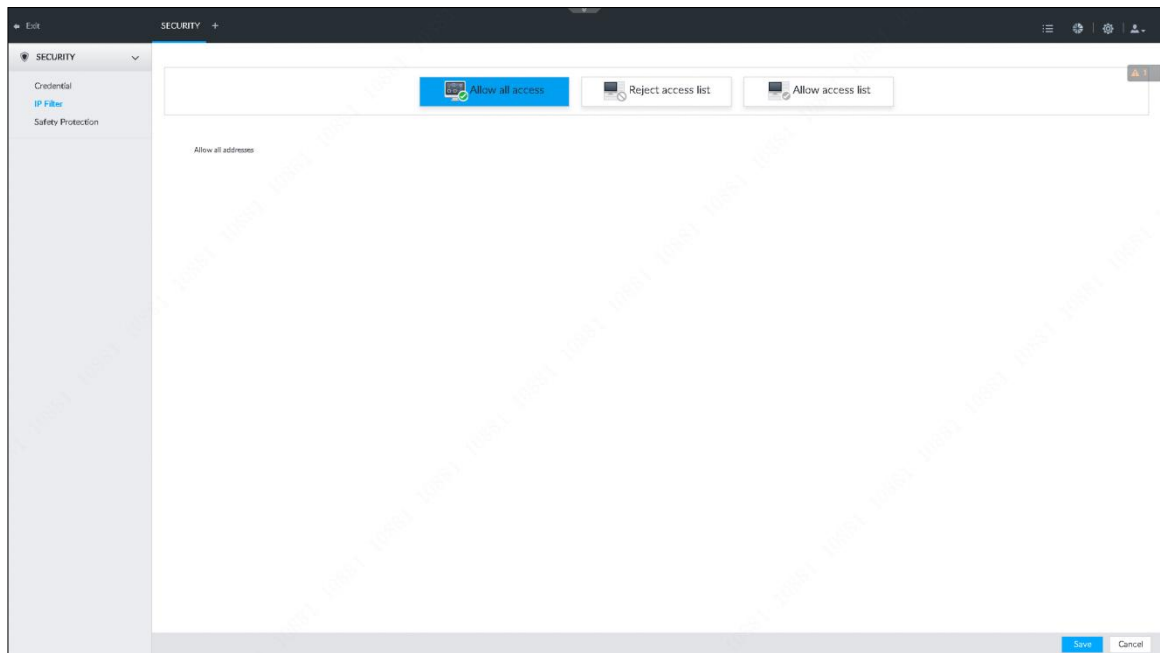
## 8.6.2 Configuring Access Right

It is to set the specified IP addresses to access the device, to enhance device network and data security.

**Step 1** Click , or click  on setting interface, and then select **Security > IP Filter**.

The **IP Filter** interface is displayed. See Figure 8-93.

Figure 8-93 IP Filter



**Step 2** It is to select IP access rights.

- Allow all access: It is to allow all IP addresses in the same IP segment to access the device.
- Reject access list: It means the IP address in the list cannot access the device.
- Allow access list: It means the IP address in the list can access the device.

**Step 3** Add IP host.



The following steps are to set reject access list or allow access list.

1) Click **Add**.

The **Add** interface is displayed. See Figure 8-94.

Figure 8-94 Add

2) Select **Add Type**, and set IP address or MAC address of IP host.

- Single IP: Enter host IP address.
- IP segment: Enter IP segment. It can add multiple IP addresses in current IP segment.
- MAC: Enter MAC address of IP host.

3) Click **OK** to add the IP host.

System displays added IP host list. See Figure 8-95.



- Click **Add** to add more IP hosts.


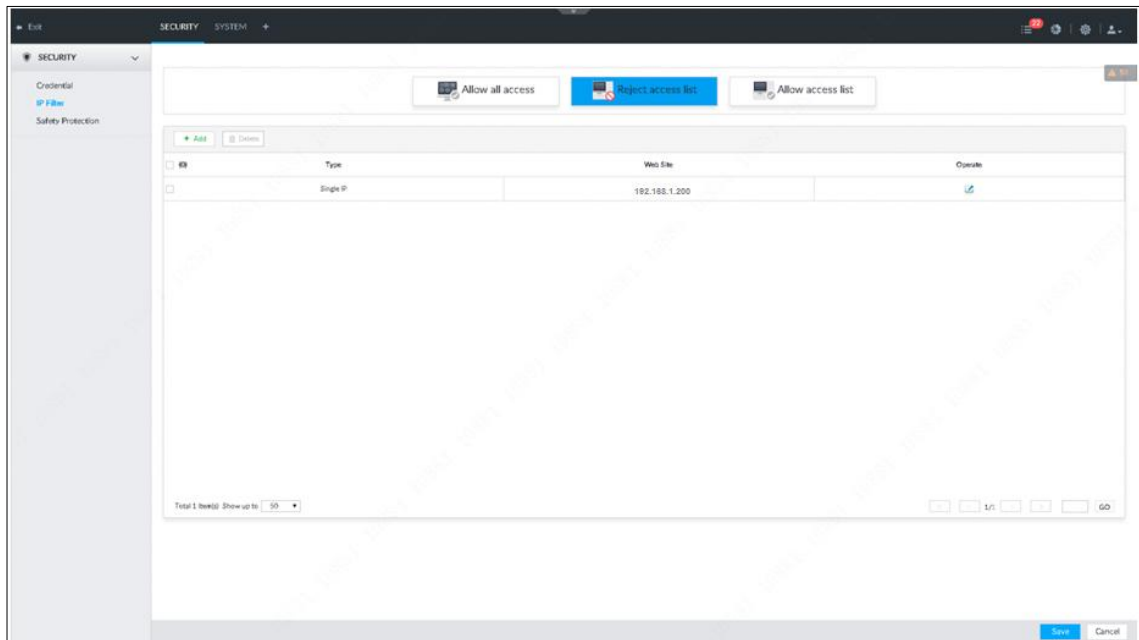
- Click  to edit the IP host.
- Select an IP host and then click **Delete** to delete.



Figure 8-95 IP host list



Step 4 Click **Save**.

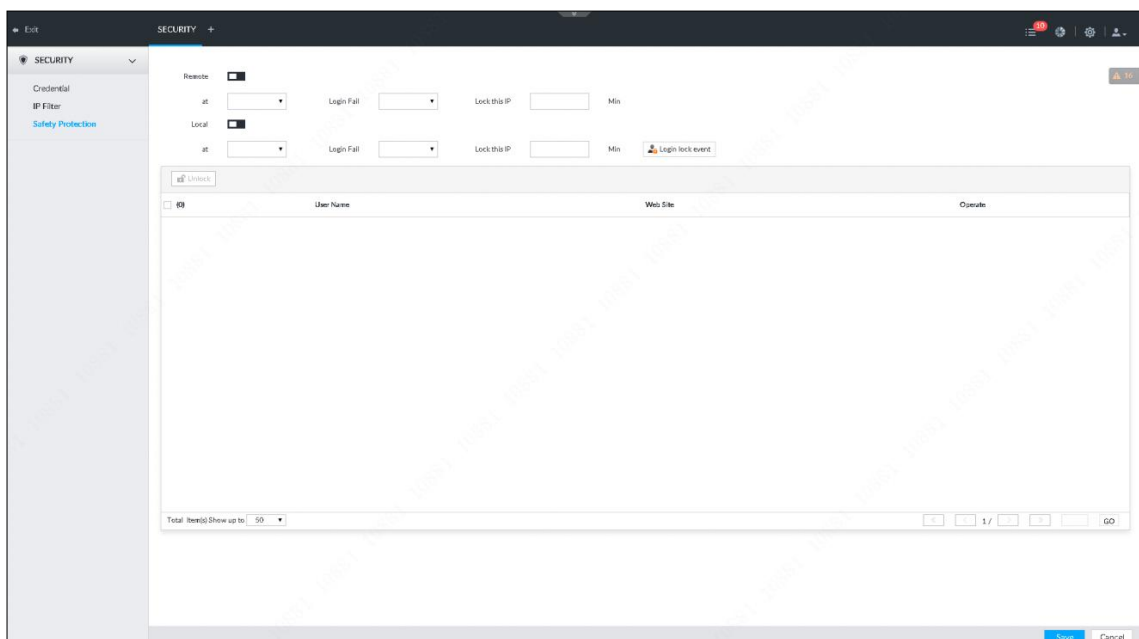
### 8.6.3 Safety Protection

It is to set the login password lock strategy once the login password error has exceeded the specified threshold. System can lock current IP host for a period of time.


Step 1 Click , or click  on setting interface, and then select **Security > Safety Protection**.

The **Safety Protection** interface is displayed. See Figure 8-96.

Figure 8-96 Safety protection (1)





**Step 2** Click  to enable security protection function.

- Remote: When you are using WEB, IVSS Client to access the device remotely, once the login password error has exceeded the threshold, system locks the IP host for a period of time.
- Local: When you are accessing local menu of the device, once the login password error has exceeded the threshold, system locks the account for a period of time.

**Step 3** Set lock strategy according to the actual situation.

**Step 4** Click **Save**.


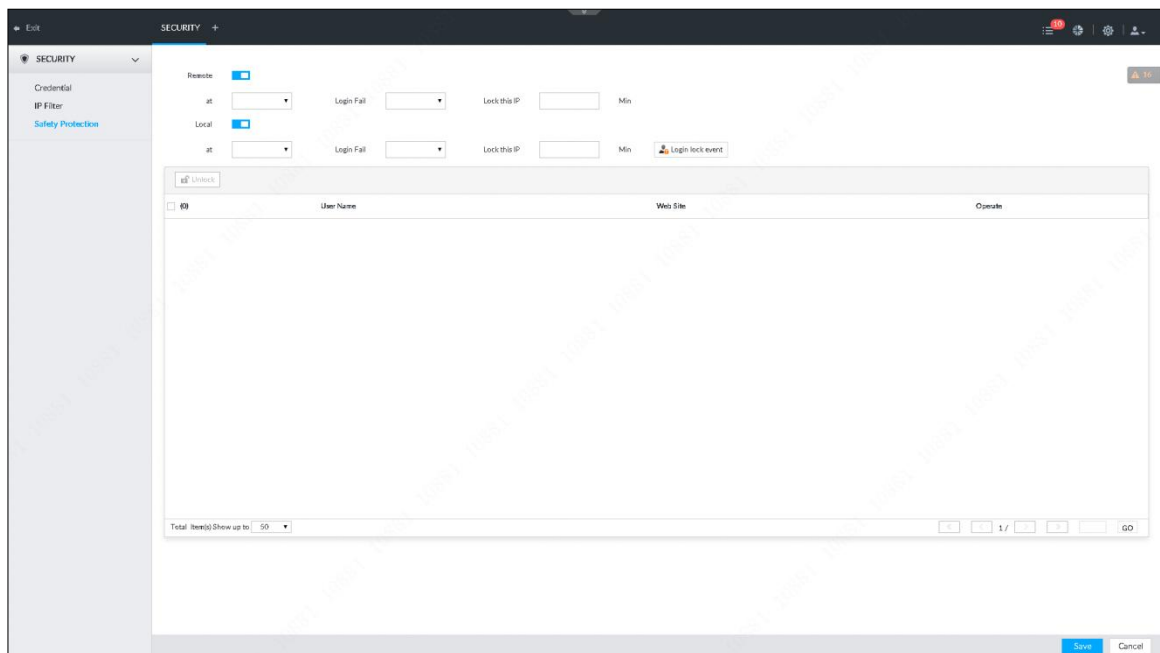


Once the IP host has been locked, you can view the locked IP host on the list. See Figure 8-97. Select an IP host and then click **Unlock**, or click the  of the corresponding IP host to unlock.

Figure 8-97 Safety protection (2)

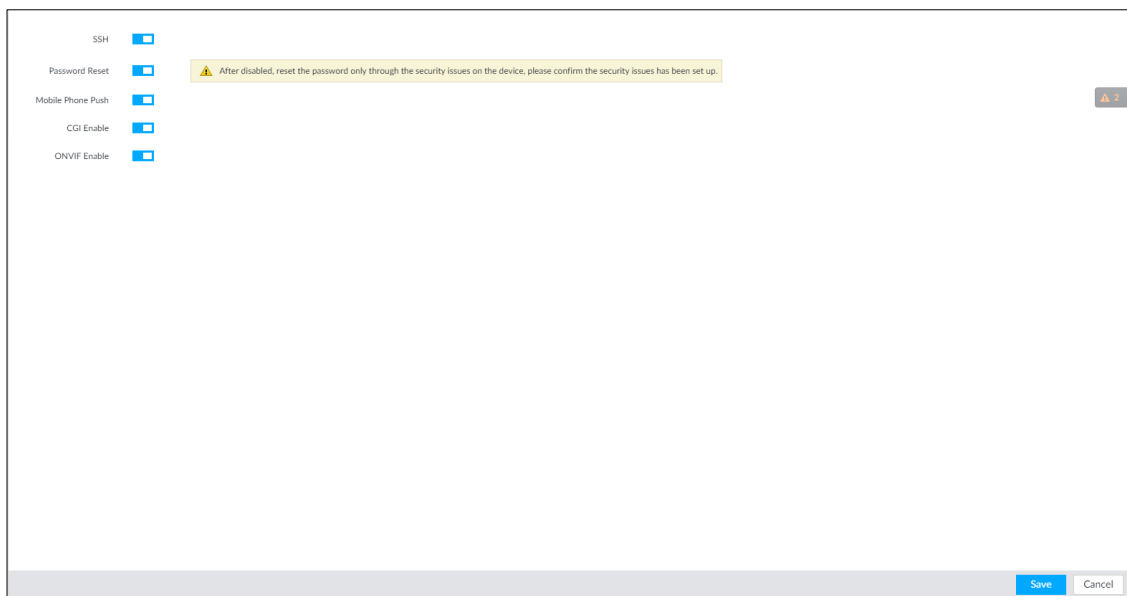


## 8.6.4 Enabling System Service Manually

**Step 1** Click , or click  on setting interface, and then select **Security > System Service**.

The **System Service** interface is displayed. See Figure 8-98.

Figure 8-98 System service



**Step 2** Enable or disable system service according to your actual situation.  
Refer to Table 8-24 for detailed information.

Table 8-24 System service

System service	Description
SSH	After enabling this function, you can access IVSS with SSH protocol, to carry out system debugging and IP configuration. It is disabled by default.
Password Reset	After enabling this function, you can use Email or answer the security questions to reset password once you forgot. It is enabled by default. If it is not enabled, you can only reset password at local device. Refer to "8.7.3.2 Reset Password" for detailed information.
Mobile phone push	After enabling this function, you can access IVSS with mobile phone client, to receive information from IVSS.
CGI Enable	After enabling this function, third-party platform can connect IVSS with CGI protocol.
ONVIF Enable	After enabling this function, other devices can connect IVSS with ONVIF protocol.

**Step 3** Click **Save**.

## 8.7 Account Management

Device account adopts two-level management mode: user and user group. You can manage their basic information. To conveniently manage the user, we recommend the general user authorities shall be lower than high-level user authorities.



- To ensure device safety, enter correct login password to operate Account interface (for example, add or delete user).
- After a correct login password is entered on Account interface, if you do not close Account interface, you can do other operations directly. If you close the interface and enter it again, you shall enter the correct login password again. The actual interface shall prevail.

## 8.7.1 User Group


Different users may have different authorities to access the device. You can divide the users to different groups. It is easy for you to maintain and manage the user information.

- System supports maximum 64 user groups. User group name supports maximum 64 characters.
- System has two default user groups (read-only): admin and ONVIF.
- Create new user group under the root.

### Add User Group

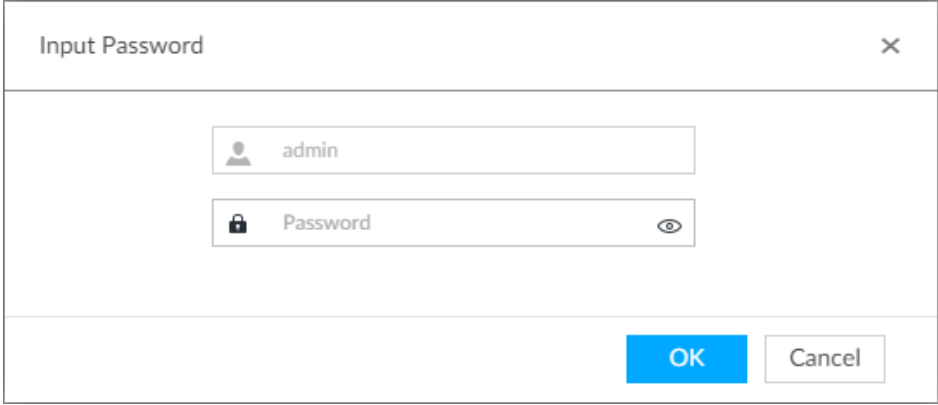
**Step 1** Click , or click  on setting interface, and then select **Account**.

The **Account** interface is displayed.

**Step 2** Select root node at the left list and then click  at the bottom left corner.

The **Input Password** is displayed. See Figure 8-99.

Figure 8-99 Input password

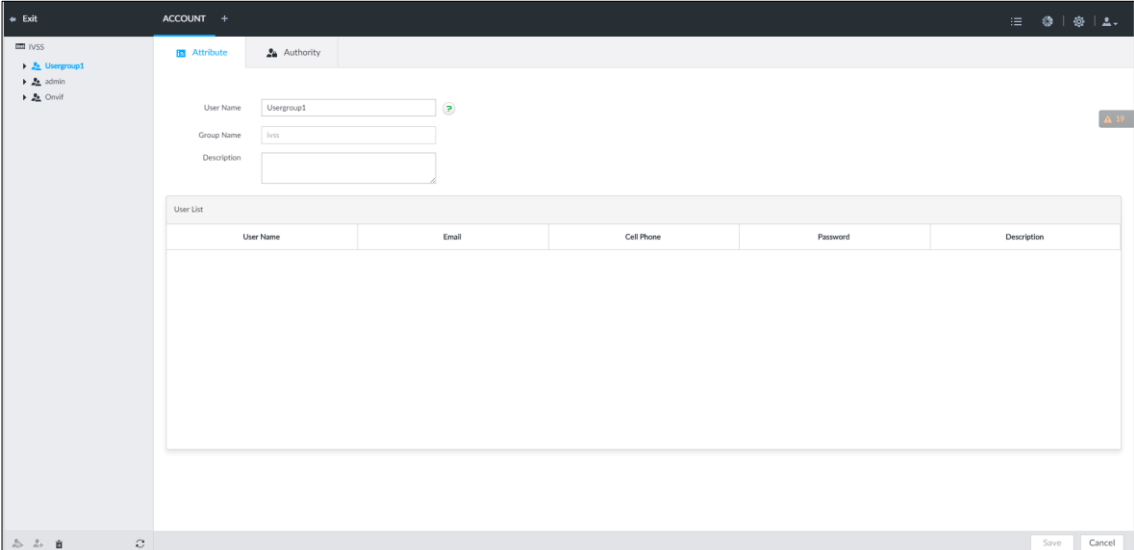


The dialog box titled "Input Password" contains two input fields. The first field is labeled "admin" and has a user icon on the left. The second field is labeled "Password" and has a lock icon on the left and an eye icon on the right. At the bottom right, there are two buttons: "OK" (blue) and "Cancel" (white).

**Step 3** Enter current user's login password, and then click **OK**.

System creates one user group and displays **Attribute** interface. See Figure 8-100.

Figure 8-100 User group attribute



The "Attribute" interface shows a sidebar with a tree view containing "Usergroup1", "admin", and "Onvif". The main area has tabs for "Attribute" and "Authority". Under "Attribute", there are input fields for "User Name" (containing "Usergroup1"), "Group Name" (containing "test"), and "Description". Below these is a "User List" table with columns for "User Name", "Email", "Cell Phone", "Password", and "Description". The table is currently empty. At the bottom right, there are "Save" and "Cancel" buttons.

**Step 4** Set parameters. For details, refer to Table 8-25.

Table 8-25 User group

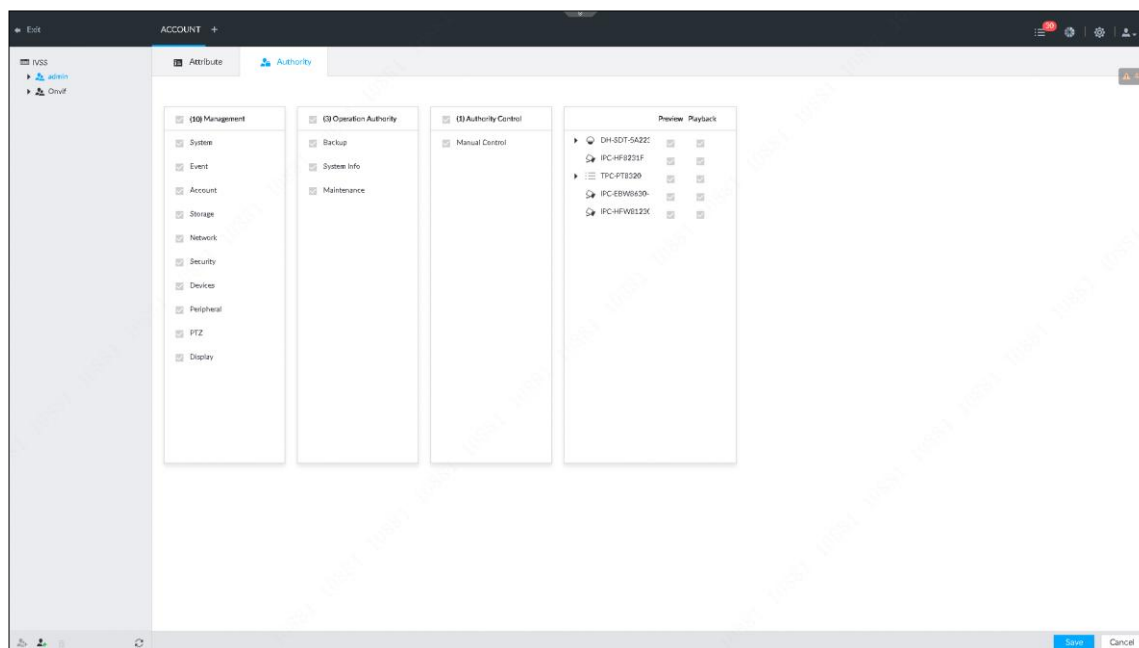
Parameter	Description
Name	Set user group name. The name ranges from 1 to 64 characters. It can contain English letters, number and special character ("_", "@", ".").
Group name	Displays user group organization node. System automatically recognizes the group name.
Description	It is to input user group description information.
User list	Displays user information of current group.

**Step 5** Select user authority.

1) Click **Authority** tab.

The **Authority** interface is displayed. See Figure 8-101.

Figure 8-101 Authority



2) Set user group authorities according to actual situation.

- : means it has the corresponding authority.
- Check the box at the top of the authority list (such as (0) Authority Control) to select all authorities of current category.

**Step 6** Click **Save**.


## Delete user group



- Before you delete a user group, delete all users of current group first.
- Admin and ONVIF user cannot be deleted.

**Step 1** Click , or click  on setting interface, and then select **Account**.

The **Account** interface is displayed.

**Step 2** Select user group and click .

The **Input Password** is displayed. See Figure 8-102.

Figure 8-102 Input password



**Step 3** Enter current user's login password, and then click **OK**.

The following prompt interface is displayed.

**Step 4** Click **OK**.

## 8.7.2 Device User

The device user is to access and manage the device. System default administrator is admin. It is to add a user and then set corresponding authorities, so that the user can access the resources within its own rights range only.




User authorities adopt the user group authorities settings. It is read-only.

### Adding a user

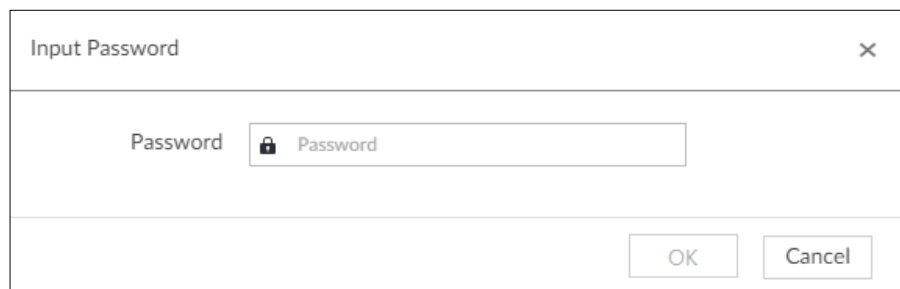
**Step 1** Click , or click  on setting interface, and then select **Account**.

The **Account** interface is displayed.

**Step 2** Select admin user group or other newly added user group, and then click  at the bottom left corner.

The **Input Password** is displayed. See Figure 8-103.

Figure 8-103 Input password

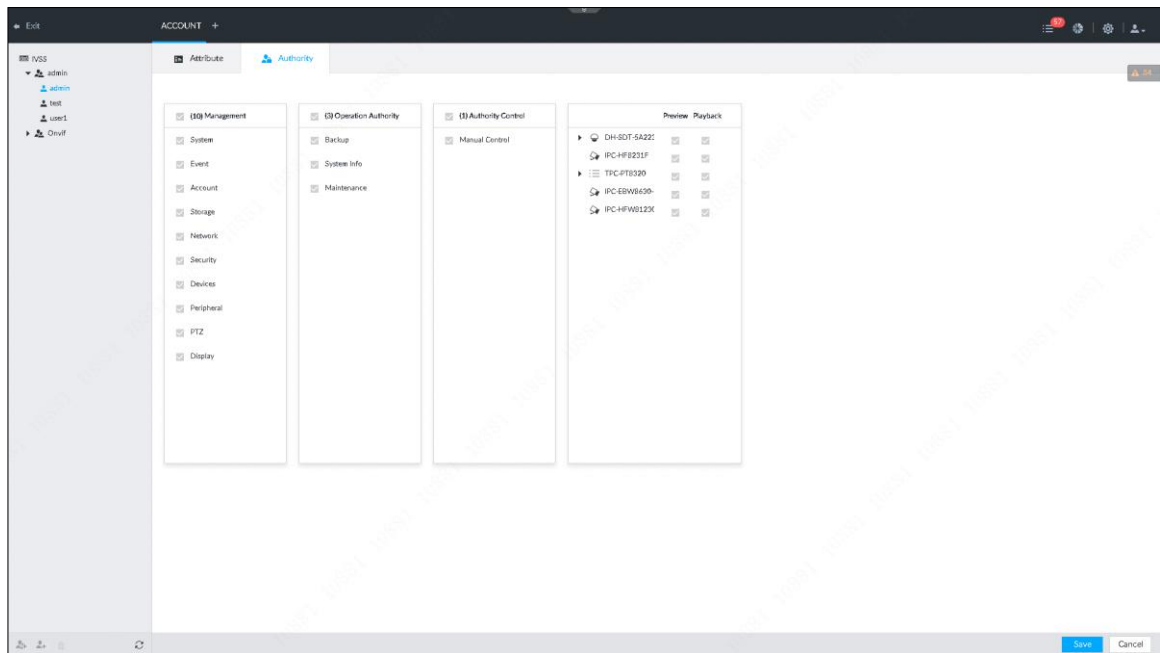


**Step 3** Enter current user's login password, and then click **OK**.

The **Attribute** interface is displayed. See Figure 8-104.



Figure 8-105 Authority



**Step 6** Click **Save**.



## Operation

After adding a user, you can modify user information or delete the user. For details, see Table 8-27.



The user with account management authority can change its own and other users' information.

Table 8-27 User operation

Name	Operation
Edit user information	Select a user from user list. The <b>Attribute</b> interface of the user is displayed, and the user's login password and description information can be modified.
Delete User	Select a user from user list, and then click  to delete.  Before deleting online user, shield the user first. For details, see "9.2 Online User".

## 8.7.3 Password Maintenance

Maintain and manage user's login password.

### 8.7.3.1 Modify Password

Modify user's login password.

Modify the user's own password


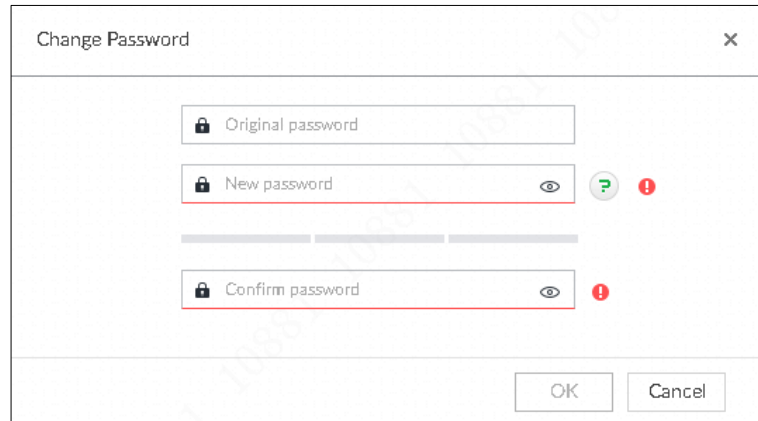
- Step 1** Click  at the top right corner, and then select **Modify Password**.  
The **Change Password** is displayed. See Figure 8-106.

Figure 8-106 Modify password





The dialog box titled "Change Password" contains three password input fields: "Original password", "New password", and "Confirm password". Each field has a lock icon on the left and an eye icon on the right. The "New password" and "Confirm password" fields are highlighted with a red border. To the right of the "New password" field are a green question mark icon and a red exclamation mark icon. To the right of the "Confirm password" field is a red exclamation mark icon. At the bottom right, there are "OK" and "Cancel" buttons.

- Step 2** Input old password and then input new password and then confirm.  
**Step 3** Click **OK**.

## Modify another user's password.

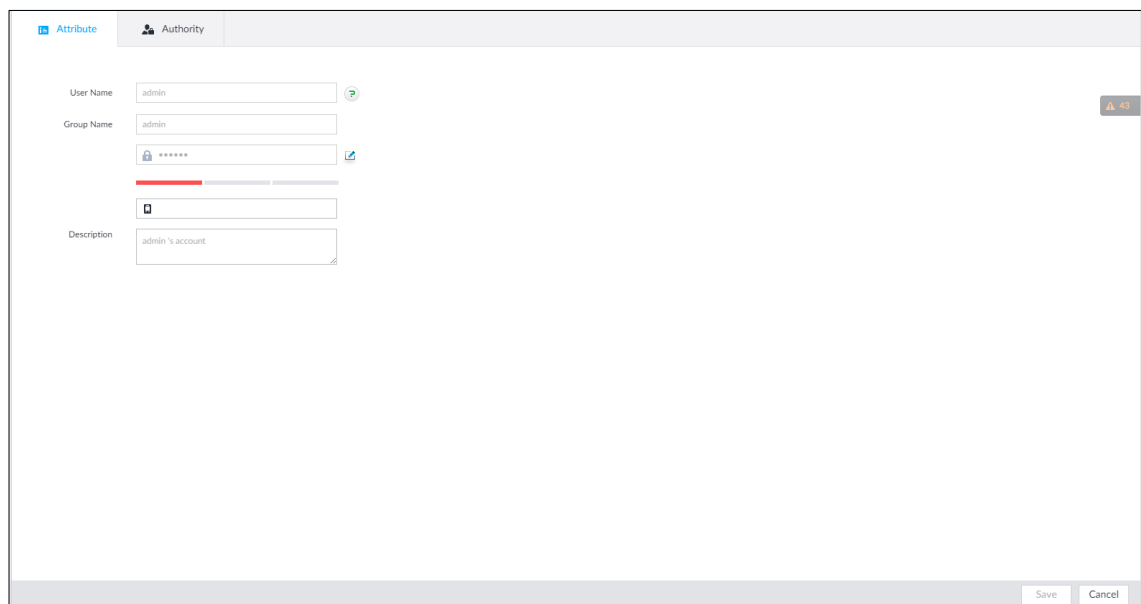


Only **Admin** account supports this function.


- Step 1** Click , or click  on setting interface, and then select **Account**.  
The **Account** interface is displayed.

- Step 2** Select a user.  
The **Attribute** interface is displayed. See Figure 8-107.

Figure 8-107 Attribute



The "Attribute" interface shows fields for "User Name" (admin), "Group Name" (admin), and "Description" (admin's account). The password field is masked with asterisks and has a strength indicator bar below it. There are "Save" and "Cancel" buttons at the bottom right.

- Step 3** Click .

The **Input Password** interface is displayed. See Figure 8-108.



Figure 8-108 Input password

**Step 4** Enter current user's login password, and then click **OK**.  
The **Change Password** is displayed. See Figure 8-109.

Figure 8-109 Modify password

**Step 5** In the New Password box, enter the new password and enter it again in the Confirm Password box.

**Step 6** Click **Save**.

### 8.7.3.2 Reset Password

You can use Email or answer the security questions to reset password once you forgot. The system supports to reset password in a local and remote way (web and IVSS client). For details, see Table 8-28.



- When password resetting function is not enabled, the password cannot be reset if the security questions are not set.
- Web and IVSS client only reset password with Email.
- Refer to "8.6.4 Enabling System Service Manually" for detailed information.

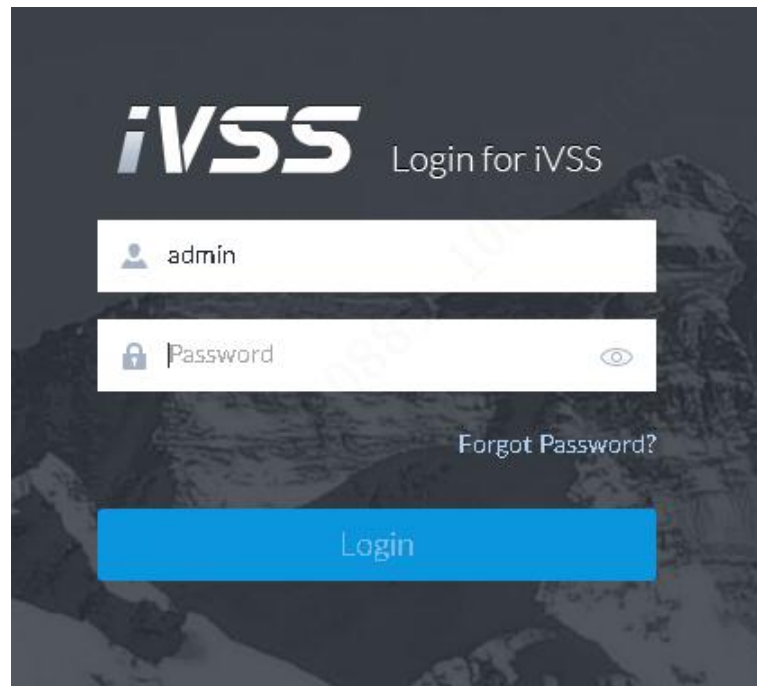
Table 8-28 Reset password

Reset	Operation	Applicable scene
Remote reset	The system supports to reset password in a local and remote way (web and IVSS client).	Password resetting function is enabled, and Email is set.
Local reset	Reset password at local interface.	It applies to all scenes.

#### Remote reset

Step 1 The **Login** interface of device is displayed. See Figure 8-110.

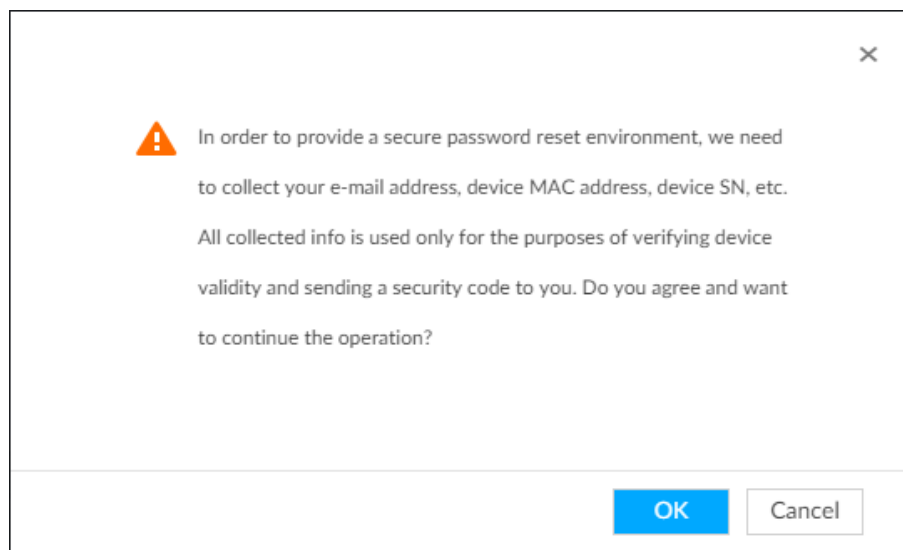
Figure 8-110 Login



Step 2 Click **Forgot Password**.

System pops up a confirmation box. See Figure 8-111.

Figure 8-111 Prompt interface



Step 3 Click **OK**.

The **Reset the password** interface is displayed. See Figure 8-112.

Figure 8-112 Reset password

Reset Password

1 Retrieve Password 2 Set New Password

Retrieve Password By Email

SN \*\*\*\*\*J56F1F

Scan QR Code

1. Use specified APP (DMSS) to scan, APP can automatically send out the data to the server  
2. Use non-specified APP to scan, please send QR Code to support\_rpwd@global.dahuatech.com

Scan the QR code on the actual interface.

Security code will be sent to \*\*\*@dahuatech.com.

Input Security Code ?

Next Cancel

**Step 4** Rest the login password.

Scan the QR code to obtain the security code according to system prompts. Enter the security code in your Email into the box of Input Security Code.



- You can get security codes twice by scanning the same QR code. If you need to get the security code once again, refresh the interface.
- Use the security code received in your email box to reset the password within 24 hours; otherwise the security code becomes invalid.



**Step 5** Click **Next** button.

The **Reset Password** interface is displayed. See Figure 8-113.

Figure 8-113 Reset password

**Step 6** Set parameters. For details, refer to Table 8-29.

Table 8-29 Description of password parameters

Parameter	Description
User	The default user name is admin.
Password	In the New Password box, enter the new password and enter it again in the Confirm Password box.
Confirm Password	The new password can be set from 8 through 32 non-empty characters and contains at least two types from number, letter and special characters (excluding "", "", ";", ":" and "&"). Enter a strong password according to the password strength indication.
Prompt question	After setting the prompt, when you move the mouse to  on the login interface, the system pops up a prompt to help you remember the password.  The prompt question function is for local login interface only. Refer to the actual interface for detailed information.

**Step 7** Click OK to complete the password reset.  
You can log in with the new password.

## Local reset

**Step 1** Through local connection, the **Login** interface of device is displayed. See Figure 8-114.

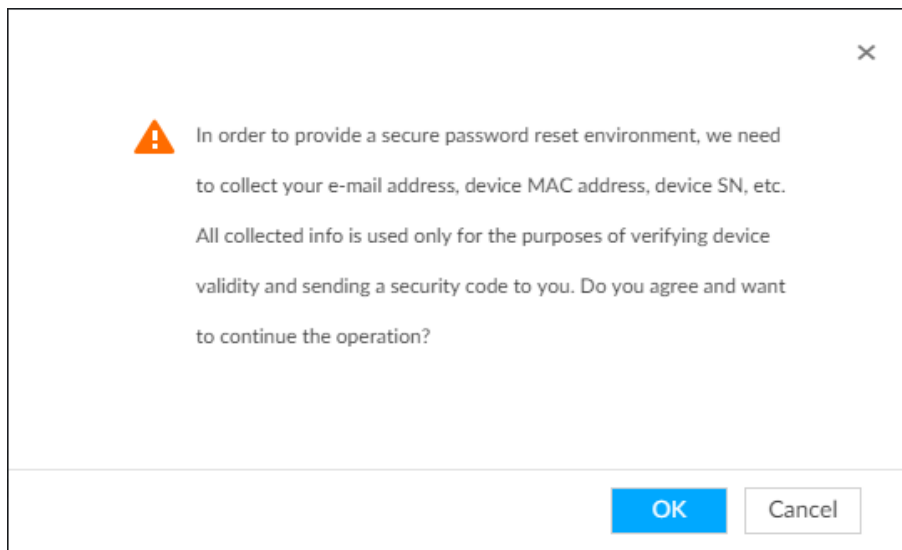
Figure 8-114 Login



Step 2 Click **Forgot Password**.

System pops up a confirmation box. See Figure 8-115.

Figure 8-115 Prompt interface



Step 3 Click **OK**.

- If you have set the reserved Email, the interface is displayed as Figure 8-116
- If you have not set the reserved Email, the interface is displayed as Figure 8-117. After you set the reserved Email and click **Next**, the interface is displayed as Figure 8-116.

Figure 8-116 Reset password (1)

Reset Password

1 Retrieve Password 2 Set New Password

Retrieve Password By Email

SN \*\*\*\*\*J56F1F

Scan QR Code

Scan the QR code on the actual interface.

1. Use specified APP (DMSS) to scan, APP can automatically send out the data to the server  
2. Use non-specified APP to scan, please send QR Code to support\_rpwd@global.dahuatech.com

Security code will be sent to \*\*\*@dahuatech.com.

Input Security Code ?

Next Cancel

Figure 8-117 Reset password (2)

Reset Password

1 Password Protection 2 Retrieve Password 3 Set New Password

Email (To reset password)

Email Address

Next Cancel

**Step 4** Reset the password.

- Email

Scan the QR code to obtain the security code according to system prompts. Enter the security code in your Email into the box of Input Security Code.



- ◇ You can get security codes twice by scanning the same QR code. If you need to get the security code once again, refresh the interface.

- ◇ Use the security code received in your email box to reset the password within 24 hours; otherwise the security code becomes invalid.
- Security Questions  
In the **Retrieve Password** drop-down list in Figure 8-116, select **Security Questions**, and the security questions interface is displayed, see Figure 8-118. In the **Answer** boxes, enter the correct answers.

Figure 8-118 Reset password (3)

Reset Password

1 Retrieve Password 2 Set New Password

Retrieve Password Retrieve Password ▼

Question 1 What is your favorite book during your childhood

\* Answer

Question 2 What was the first name of your first boss?

\* Answer

Question 3 What is the name of your favorite fruit?

\* Answer

Next Cancel



Step 5 Click **Next** button.

The new password setting interface is displayed. See Figure 8-119.

Figure 8-119 New password setting

**Step 6** Set parameters. For details, refer to Table 8-30.

Table 8-30 Description of password parameters

Parameter	Description
User	The default user name is admin.
Password	In the New Password box, enter the new password and enter it again in the Confirm Password box.
Confirm Password	The new password can be set from 8 through 32 non-empty characters and contains at least two types from number, letter and special characters (excluding "", "", ";", ":" and "&"). Enter a strong password according to the password strength indication.
Prompt question	After setting the prompt, when you move the mouse to  on the login interface, the system pops up a prompt to help you remember the password.  The prompt question function is for local login interface only. Refer to the actual interface for detailed information.

**Step 7** Click **OK** to complete the password reset.

You can log in with the new password.

## 8.7.4 ONVIF

When the remote device is connecting with the device through ONVIF protocol, use the verified ONVIF account.



- System adopts three ONVIF user groups (admin, user and operator). You cannot add ONVIF user group manually.



- You cannot add user under ONVIF group directly.

## Add ONVIF User

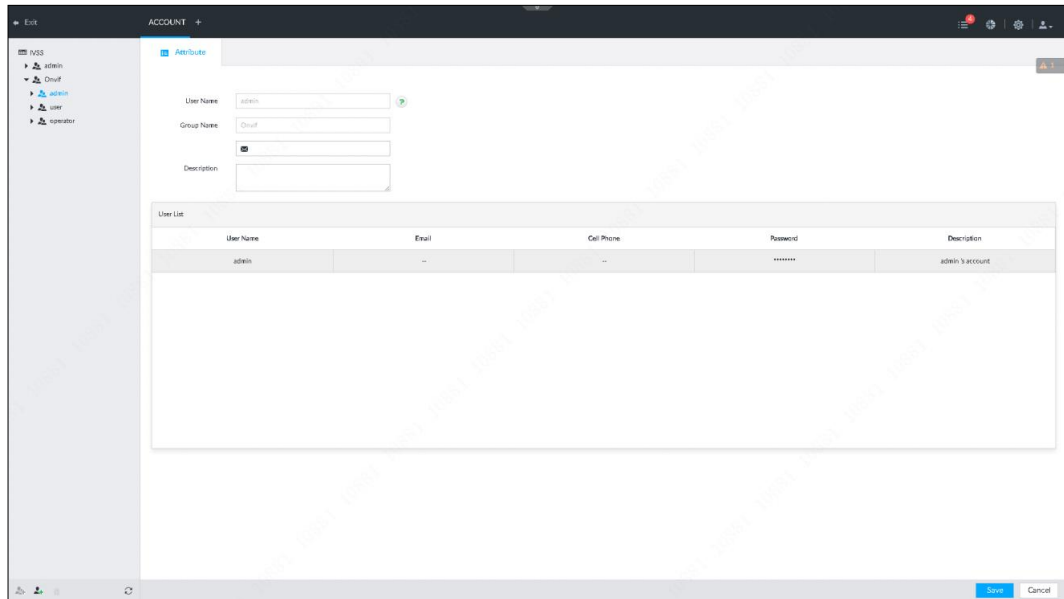
**Step 1** Click , or click  on setting interface, and then select **Account**.


The **Account** interface is displayed.

**Step 2** Select user group under ONVIF.

The **Attribute** interface of ONVIF group is displayed. See Figure 8-120.

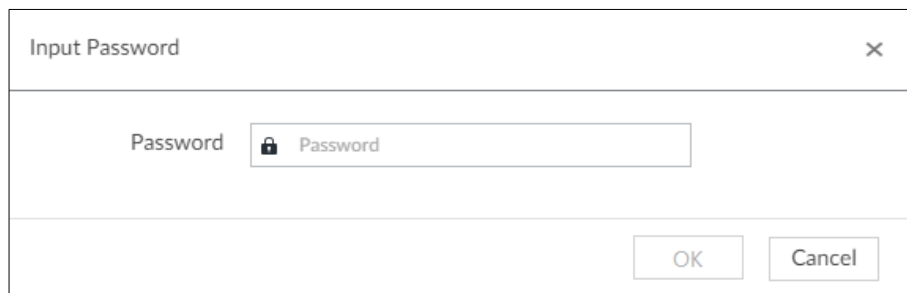
Figure 8-120 ONVIF



**Step 3** Click .

The **Input Password** interface is displayed. See Figure 8-121.

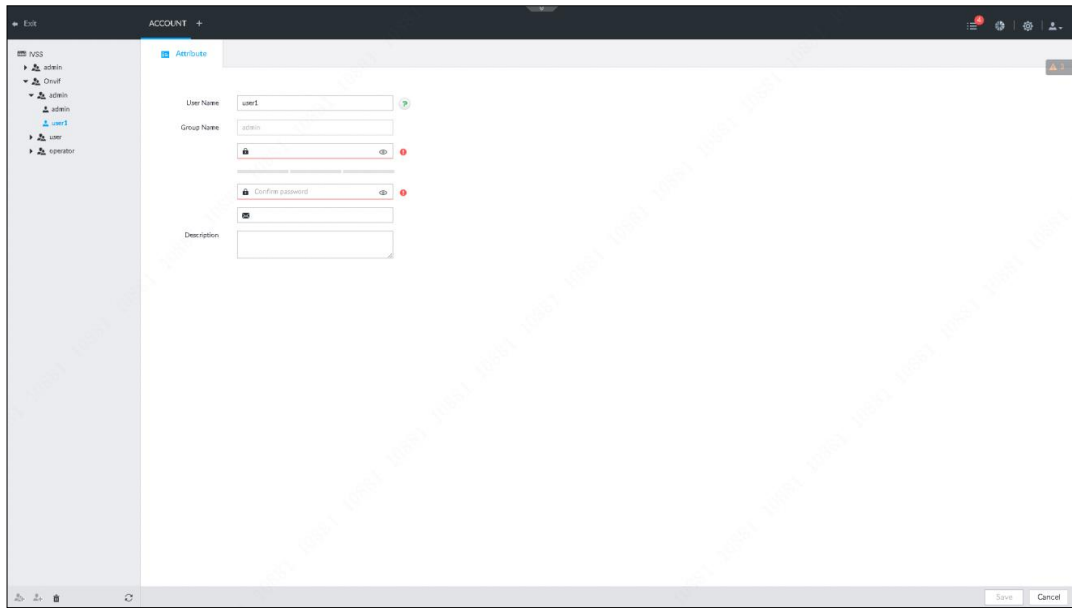
Figure 8-121 Input password



**Step 4** Enter current user's login password, and then click **OK**.

The **Attribute** interface is displayed. See Figure 8-122.

Figure 8-122 ONVIF attribute



**Step 5** Set parameters. For details, refer to Table 8-31.

Table 8-31 ONVIF parameters description

Parameter	Description
Name	It is to set ONVIF user name. The name ranges from 1 to 31 characters. It can contain English letters, number and special character ("_", "@", ".").
Group name	Displays user organization node. System automatically identifies it.
Password	It is to set ONVIF user password. The password ranges from 8 to 32 non-empty characters. It can contain letters, numbers and special characters (excluding "'", "\"", ";", ":", "&"). The password shall contain at least two categories. Usually we recommend the strong password.
Confirm Password	
Description	Input ONVIF user description information.

**Step 6** Click **Save**.

## Delete ONVIF User



Deleting the admin account is not supported.

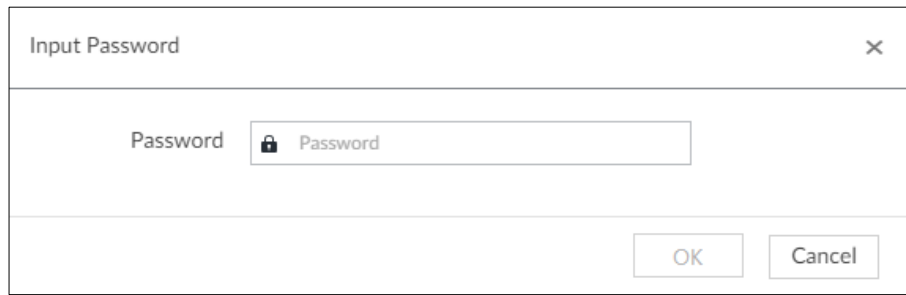
**Step 1** Click , or click  on setting interface, and then select **Account**.

The **Account** interface is displayed.

**Step 2** Select ONVIF and click .

The **Input Password** interface is displayed. See Figure 8-123.



Figure 8-123 Input password



**Step 3** Enter current user's login password, and then click **OK**.  
The following prompt interface is displayed.

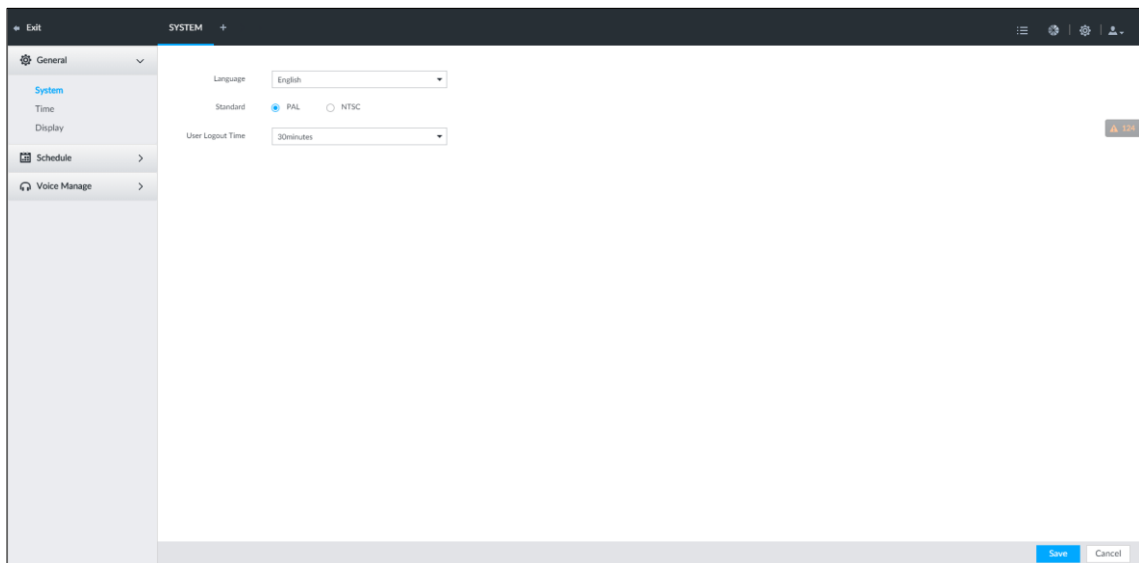
**Step 4** Click **OK**.

## 8.8 System Management

Click  or click  on setting interface, select **System**. The **System** interface is displayed. See Figure 8-124.



It is to set system basic settings, such as general parameters, time, display parameter, schedule, and voice.

Figure 8-124 System management



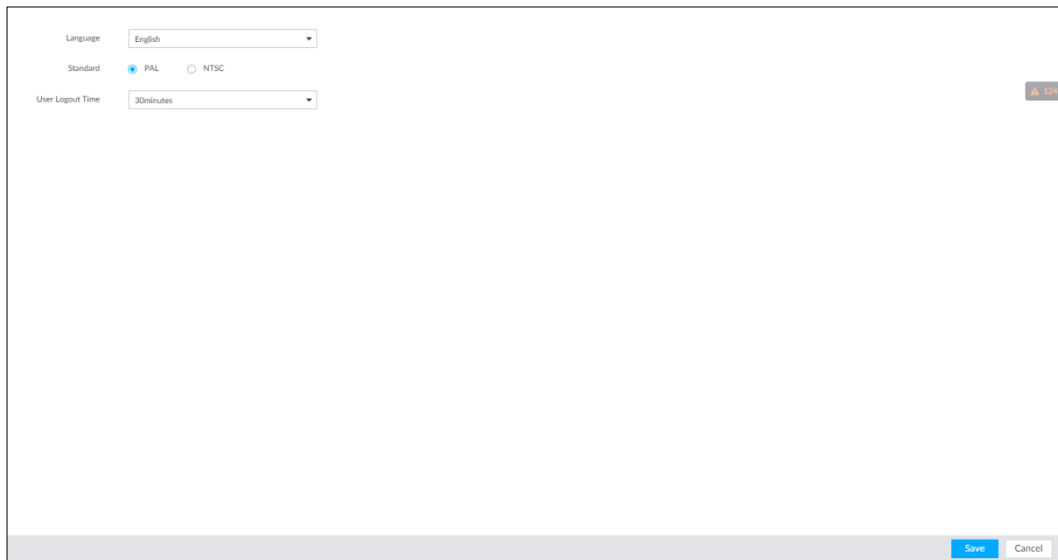
### 8.8.1 Setting System Parameter

It is to set system language, standard, user logout time, virtual keyboard, and mouse moving speed.

**Step 1** Click , or click  on setting interface, and then select **System > General > System**.




The **System** interface is displayed. See Figure 8-125.

Figure 8-125 Configuring system settings



**Step 2** Set parameters. For details, refer to Table 8-32.



Table 8-32 System parameters description

Parameter	Description
Language	It is to set system language.
Standard	<p>Select video standard.</p> <ul style="list-style-type: none"> <li>• PAL is mainly used in China, Hong Kong, Middle East and Europe.</li> <li>• NTSC is mainly used in Japan, United States of America, Canada and Mexico.</li> </ul> <p> As a technical standard of processing video and audio signals, PAL and NTSC mainly differ in encoding, decoding mode and field scanning frequency.</p>
User logout time	<p>It is to set auto logout interval once you remains inactive for a specified period or the device exceeds the set value. After auto logout, the user needs to login again to operate.</p> <p>If you set as No Logout, system does not automatically log out.</p>
Virtual keyboard	<p>It is to enable virtual keyboard function on the local menu. Refer to "Appendix 1.2 Virtual Keyboard" for detailed information.</p> <p> This function is for local menu only.</p>
Mouse moving speed	<p>It is to set mouse moving speed on the local interface.</p> <p> This function is for local menu only.</p>

**Step 3** Click **Save**.

## 8.8.2 System Time

It is to set system time, and enable NTP function according to your need. After enabling NTP function, device can automatically synchronize time with the NTP server.

**Step 1** Click , or click  on setting interface, and then select **System > General > Time**.

The **Time** interface is displayed. See Figure 8-126.

Figure 8-126 Time

**Step 2** Set parameters. For details, refer to Table 8-33.

Table 8-33 System parameters description

Parameter	Description
Time	It is to set system date and time. You can set manually or set device to synchronize time with the NTP server. <ul style="list-style-type: none"> <li>Select <b>Manual Setting</b> and then input actual date and time.</li> <li><b>Sync with the Internet Time Server:</b> Check the box and then input NTP server IP address or domain, and then set <b>Auto Sync Time Interval</b>.</li> </ul>
Time and date format	Set time and date display format.
Time Zone	Set device time zone.
Auto Time Synchronization	After enabling this function, IVSS detects system time of remote device once in every interval. When time of remote device is inconsistent with IVSS time, IVSS will calibrate the time of remote device automatically.

**Step 3** (Optional) Set DST.





DST is a system to stipulate local time, in order to save energy. If the country or region where the device is located follows DST, you can enable DST to ensure that system time is correct.

- 1) Click  to enable DST.
- 2) Select DST mode. It includes **Date** and **Week**.
- 3) Set DST start time and end time.

**Step 4** Click **Save**.

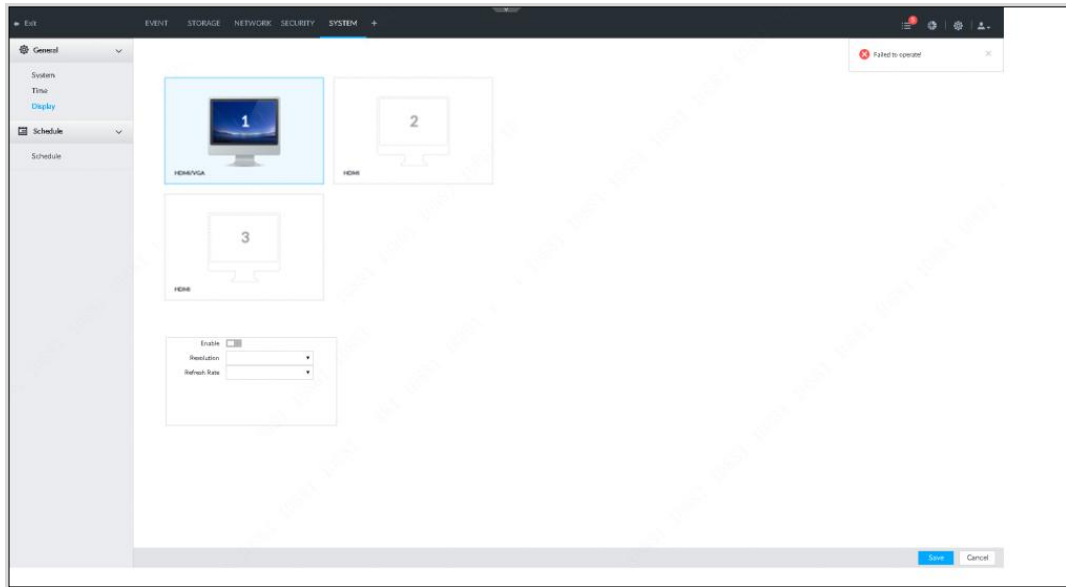
## 8.8.3 Display

It is to set connected display resolution and refresh rate.

**Step 1** Click , or click  on setting interface, and then select **System > General > Display**.


The **Display** interface is displayed. See Figure 8-127.

Figure 8-127 Display




- SN 1–3 refers HDMI 1–HDMI 3. Among which, HDMI/VGA is the main display, while the VGA and HDMI 1 outputs the same video.
- VGA and HDMI 1 are outputting the same video source. Three HDMI ports can output different video sources.



-  means display is connected and enabled.  means display is




 means display is disconnected.

**Step 2** Select display.

**Step 3** Set parameters. For details, refer to Table 8-34.

Table 8-34 Display parameters description

Parameter	Description
Enable	Start or stop display.  System adopts main screen by default. The main screen cannot be disabled.
Resolution	It is to set display resolution. Different displays support different resolutions. Refer to your actual interface for detailed information.
Refresh rate	It is to set refresh rate of the display.



**Step 4** Click **Save**.

## 8.8.4 Schedule

It is to set schedule. When you are configuring alarm, record arm/disarm period, system can call the schedule directly. System only triggers the corresponding operations during the specified schedule.

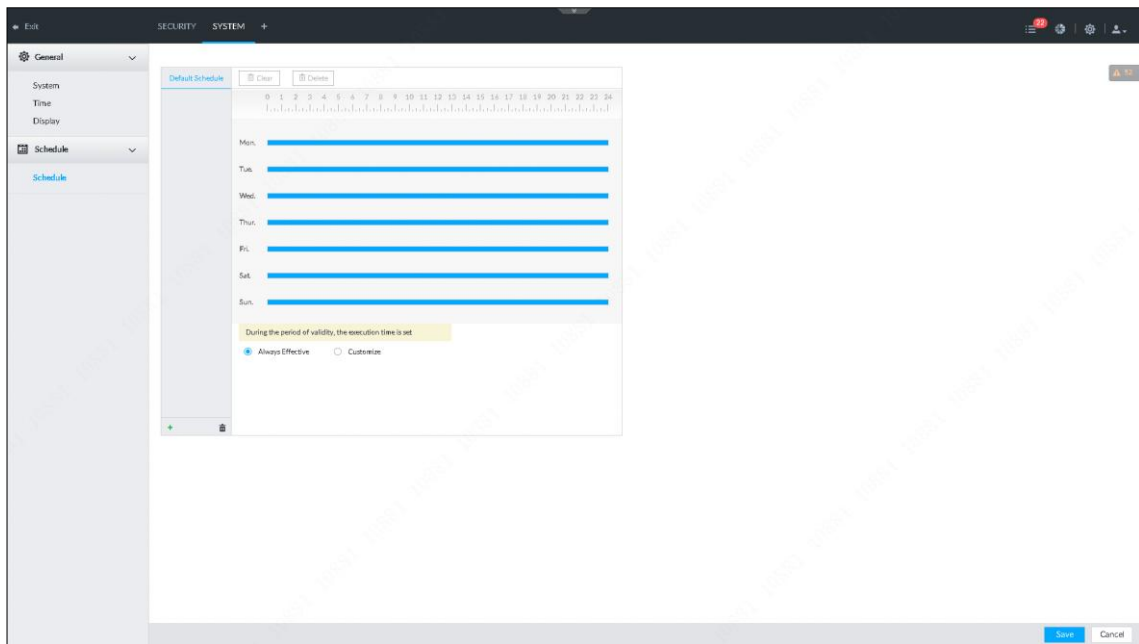


Default schedule has been created by default. Default schedule is **Always Effective**, and cannot be modified or deleted.

**Step 1** Click , or click  on setting interface, and then select **System > Schedule > Schedule**.

The **Schedule** interface is displayed. See Figure 8-128.

Figure 8-128 Schedule



**Step 2** Add schedule.

1) Click .

The **Add Schedule** interface is displayed. See Figure 8-129.

Figure 8-129 Adding schedule

- 2) Set schedule name.
- 3) Click **OK** to save the configuration.



**Step 3** Set valid time period. It includes **Always Effective** and **Customize**.

**Step 4** Set validity period of schedule.




- The step is for customized mode only.
- Each calendar supports maximum 50 validity periods.
- The blue area on the time bar means the validity period.

On the time bar, you can:

- Click the blue area, and  is displayed. Drag  to adjust the start time and end time of validity period.
- Press the any blank space on the time bar, and drag to the right to add a validity period.
- Click **Clear** to clear all validity periods of current schedule.
- Select a validity period, and then click **Delete** to delete the period.

Step 5 Click **Save**.



Select an added schedule, and then click  to delete.



## 8.8.5 Enabling Voice Manage Function

This function is used to upload and manage audio files, so the device plays audios in case of events.



- Only support to import .pcm files.
- A single audio file shall not be less than 2KB and shall not exceed 10MB.
- Total size of imported audio files shall not exceed 200MB.

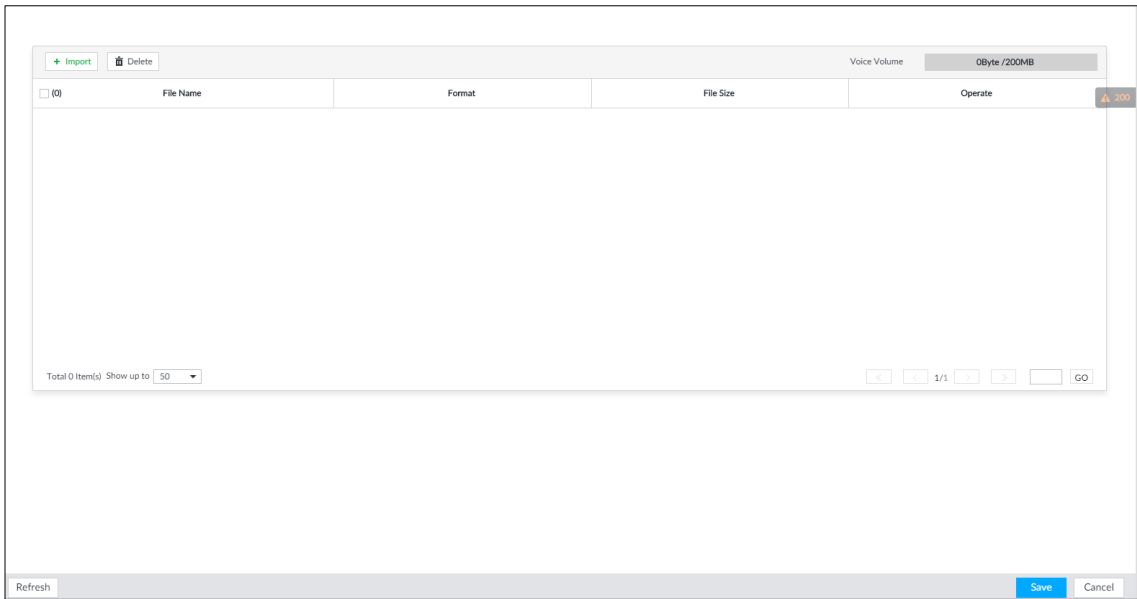
### Import audio file

Step 1 Click , or click  on setting interface, and then select **System > Voice Manage > Voice Manage**.

The **Audio Manage** interface is displayed. See Figure 8-130.



Figure 8-130 Audio manage

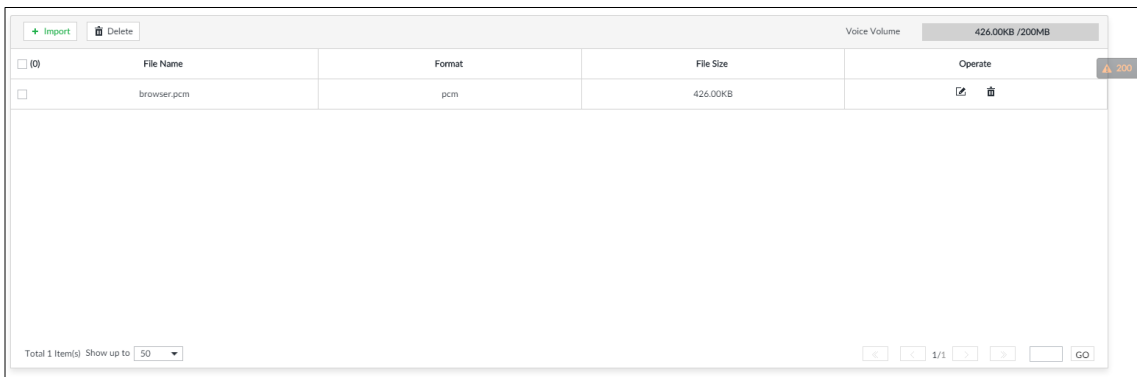


**Step 2** Click **Import** to select the audio files that you want to import.

**Step 3** Click **OK**.

The uploaded audio file is displayed. See Figure 8-131.

Figure 8-131 Audio file



## Operation

After audio file is uploaded, audio file can be renamed or deleted. For details, see Table 8-35.

Table 8-35 Audio file operation



Name	Operation
Rename audio file	Click  beside the audio file. The <b>Rename</b> interface is displayed. See Figure 8-132. You can rename the audio file.
Delete audio file	<ul style="list-style-type: none"> <li>Delete: Click  beside the audio file to delete it.</li> <li>Batch delete: Select multiple audio files, and click <b>Delete</b> to delete all of the selected audio files.</li> </ul>

Figure 8-132 Rename



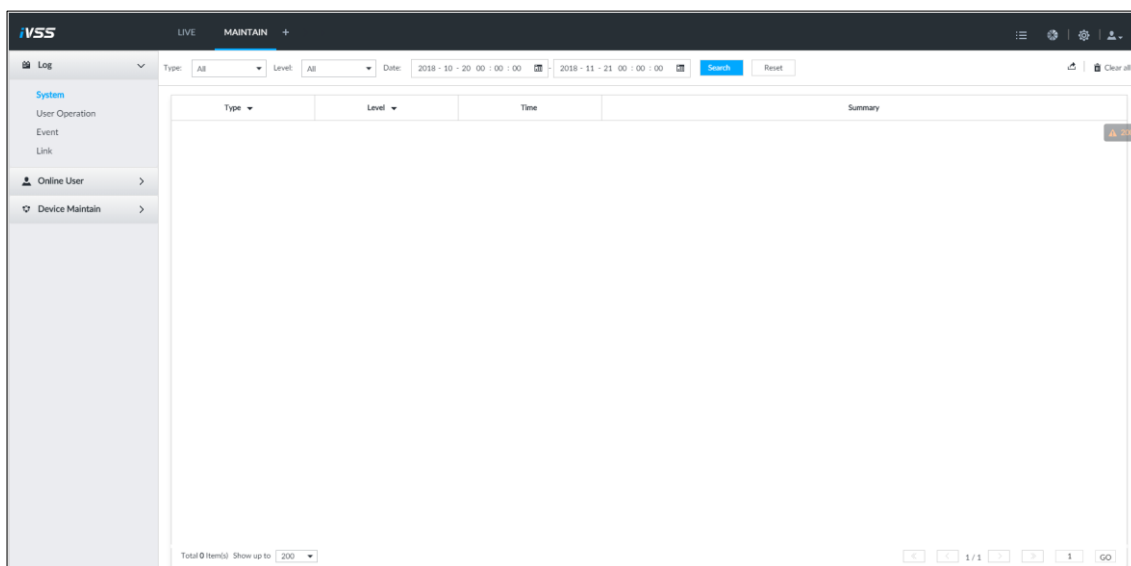
A dialog box titled "Rename" with a close button (X) in the top right corner. The dialog contains a label "File name:" followed by a text input field containing the text "browser". At the bottom right of the dialog are two buttons: "OK" (highlighted in blue) and "Cancel".

# 9 System Maintenance

Click  on the **LIVE** interface, and select **Maintain**. The **Maintain** interface is displayed. See Figure 9-1.

On the **LIVE** interface, you can operate and maintain the device working environment to guarantee proper operation.

Figure 9-1 Maintain



## 9.1 Searching Log

The logs record all kinds of system running information. Check the log periodically and fix the problems in time to guarantee system proper operation.

### Log classification

Search system log, user log, event log, and link log. For details, see Table 9-1.

Table 9-1 Log description

Log	Type
System log	Search system log. It includes logs of system running status, file management, hot spare, hardware detect and scheduled task.
User operation log	Search user operation log. It includes user operation and user configuration log.
Event log	Search alarm event log. It includes logs of cross line detection, storage error, storage full, lock in, power fault, video motion, fan speed alarm, face detection, face recognition, human detect, device offline, tampering, no HDD, IPC offline, AI module offline, AI module temp, IO alarm, IP conflict, MAC conflict, and cross region detection.

Log	Type
Link log	Search device link log. You can search or export link log including user login/logout, session hijack, session blast and remote device.

## Search log

The following steps are to search system log. Refer to the actual interface for detailed information.

**Step 1** On the **LIVE** interface, click , and select **Maintain > Log > System**.

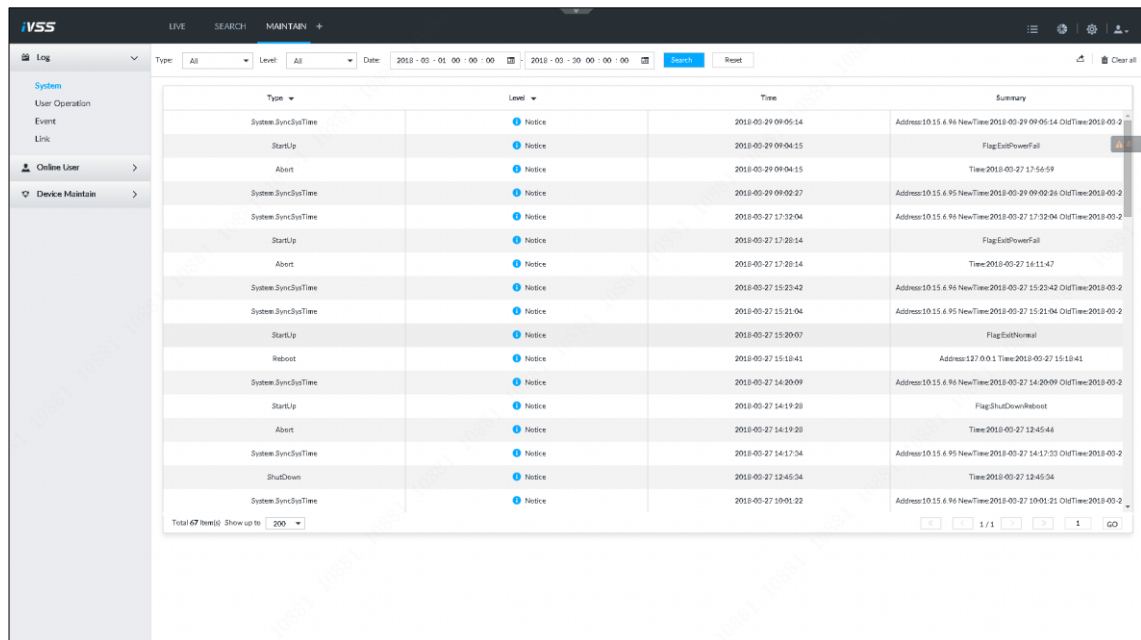
The **System** interface is displayed.

**Step 2** Set search criteria such as system log level, type and date.

**Step 3** Click **Search**.

The search results are displayed. See Figure 9-2.

Figure 9-2 System log





Type	Level	Time	Summary
System.SyncSysTime	Notice	2018-03-29 09:05:14	Address:10.15.4.96 NewTime:2018-03-29 09:05:14 OldTime:2018-03-29 09:05:14
StartUp	Notice	2018-03-29 09:04:15	Flag:ExitPowerFall
Alert	Notice	2018-03-29 09:04:15	Time:2018-03-27 17:56:59
System.SyncSysTime	Notice	2018-03-29 09:02:27	Address:10.15.4.95 NewTime:2018-03-29 09:02:26 OldTime:2018-03-29 09:02:26
System.SyncSysTime	Notice	2018-03-27 17:32:04	Address:10.15.4.96 NewTime:2018-03-27 17:32:04 OldTime:2018-03-27 17:32:04
StartUp	Notice	2018-03-27 17:28:54	Flag:ExitPowerFall
Alert	Notice	2018-03-27 17:28:54	Time:2018-03-27 16:11:47
System.SyncSysTime	Notice	2018-03-27 15:23:42	Address:10.15.4.95 NewTime:2018-03-27 15:23:42 OldTime:2018-03-27 15:23:42
System.SyncSysTime	Notice	2018-03-27 15:21:04	Address:10.15.4.95 NewTime:2018-03-27 15:21:04 OldTime:2018-03-27 15:21:04
StartUp	Notice	2018-03-27 15:20:07	Flag:ExitNormal
Reboot	Notice	2018-03-27 15:18:41	Address:127.0.0.1 Time:2018-03-27 15:18:41
System.SyncSysTime	Notice	2018-03-27 14:20:09	Address:10.15.4.96 NewTime:2018-03-27 14:20:09 OldTime:2018-03-27 14:20:09
StartUp	Notice	2018-03-27 14:19:28	Flag:ShutdownReboot
Alert	Notice	2018-03-27 14:19:28	Time:2018-03-27 12:45:44
System.SyncSysTime	Notice	2018-03-27 14:17:54	Address:10.15.4.95 NewTime:2018-03-27 14:17:53 OldTime:2018-03-27 14:17:53
ShutDown	Notice	2018-03-27 12:45:54	Time:2018-03-27 12:45:54
System.SyncSysTime	Notice	2018-03-27 10:01:22	Address:10.15.4.96 NewTime:2018-03-27 10:01:21 OldTime:2018-03-27 10:01:21

## Operation

Search, export and clear log. For details, see Table 9-2.

Table 9-2 Log operation

Name	Operation
Export log	Click  to export log information to local PC or USB storage device.
Clear log	 <p>You will be unable to track the system error reason if you clear log.</p> <p>Click <b>Clear all</b> to clear all system logs.</p>

## 9.2 Online User

It is to search remote access network user information or you can block a user from access for a period of time. During the block period, the selected user cannot access the Device.



Cannot block yourself or block admin.

**Step 1** On the **LIVE** interface, click **+**, and select **Maintain > Online User > Online User**.

The **Online User** interface is displayed. See Figure 9-3.



The list displays the connected user information.

Figure 9-3 Online user

<input type="checkbox"/>	User Name	Type	Login Time	IP	MAC	Link Type	Duration	Operate
<input type="checkbox"/>	admin	SDK	2018-11-20 17:00:29	10.33.12.154	74:85:c4:b1:9c:0a	TCP	79min	⊖

**Step 2** Block user.

- Block: Click corresponding to the user.
- Batch block: Select multiple users you want to block and then click **Block**.

The **Block** interface is displayed. See Figure 9-4.

Figure 9-4 Block

Block Time:  Min

**Step 3** Set block period. The default period is 30 minutes.

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

## 9.3 Device Maintenance

Device maintenance is to reboot device, restore factory default setup, or upgrade system and so on. It is to clear the malfunction or error during the system operation and enhance device running performance.

### 9.3.1 Upgrading Device

It is to upgrade device or the AI module version.

#### 9.3.1.1 Upgrading Host

It is to import the upgrade file to upgrade device version. The upgrade file extension name shall be .bin.




- During upgrading, do not disconnect from power and network, and reboot or shut down the Device.
- Make sure the upgrade file is right. Improper upgrade file may result in device error!

#### Preparation

You need to obtain the correct upgrade file and save it in the corresponding path.

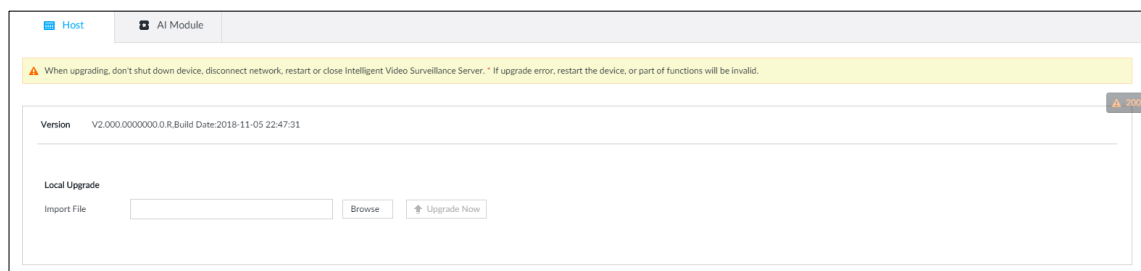
- When operating on the local interface, save the upgrade file in the USB storage device and then connect the USB storage device to the IVSS.
- When operating on the web or IVSS interface, save the upgrade file on the PC in which the Web or IVSS client is located.

#### Operation Steps

**Step 1** On the **LIVE** interface, click , and select **Maintain > Device Maintain > Upgrade > Host**.

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

Figure 9-5 Upgrade host

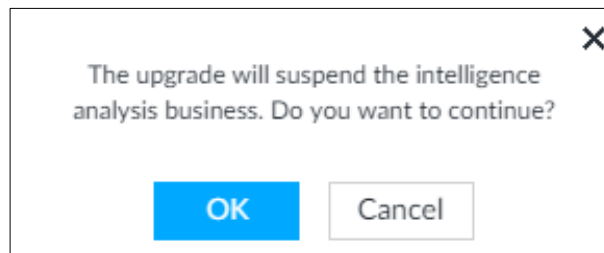


**Step 2** Click **Browse** to select an upgrade file.

**Step 3** Click **Upgrade Now**.

System pops up a confirmation box. See Figure 9-6.

Figure 9-6 Note



Step 4 Click **OK**.

The system starts upgrading. Device automatically reboots after successfully upgraded.

### 9.3.1.2 Upgrade AI module

It is to upgrade the system version of the AI module installed on the device.



- During upgrading, do not disconnect from power and network, and reboot or shut down the Device.
- Make sure the upgrade file is right. Improper upgrade file may result in device error!
- System cannot upgrade different AI modules at the same time.

#### Preparation

- You need to obtain the correct upgrade file and save it in the corresponding path.
  - ◇ When operating on the local interface, save the upgrade file in the USB storage device and then connect the USB storage device to the IVSS.
  - ◇ When operating on the web or IVSS interface, save the upgrade file on the PC in which the Web or IVSS client is located.
- The AI module you want to upgrade is online.

#### Operation Steps

Step 1 On the **LIVE** interface, click , from **Maintain > Device Maintain > Upgrade > AI Module**.

The **AI Module** interface is displayed. See Figure 9-7.




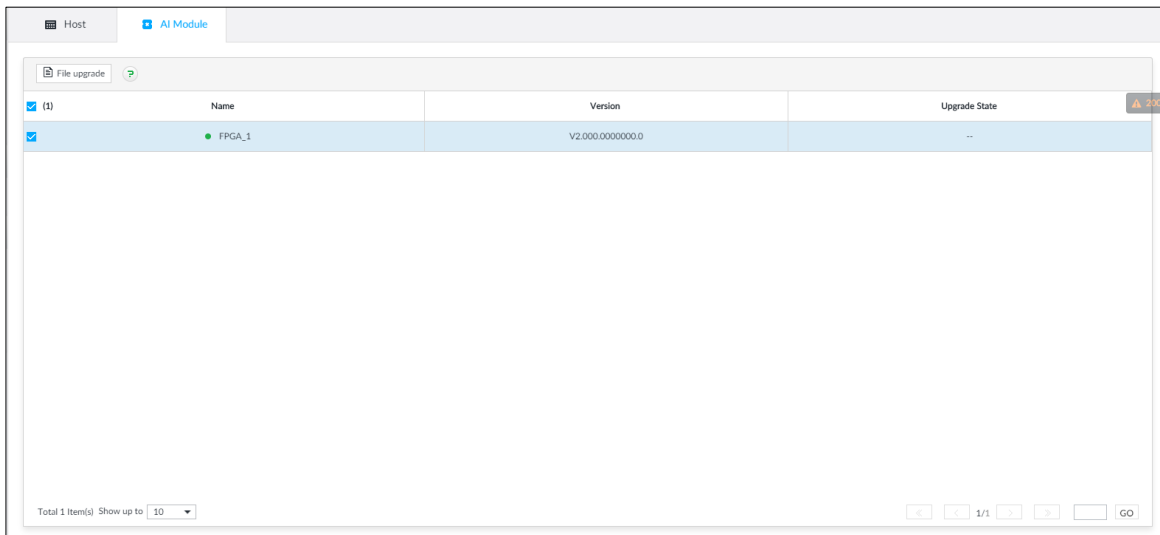
 means AI module is online.

Figure 9-7 Upgrade AI module



**Step 2** Select the AI module.

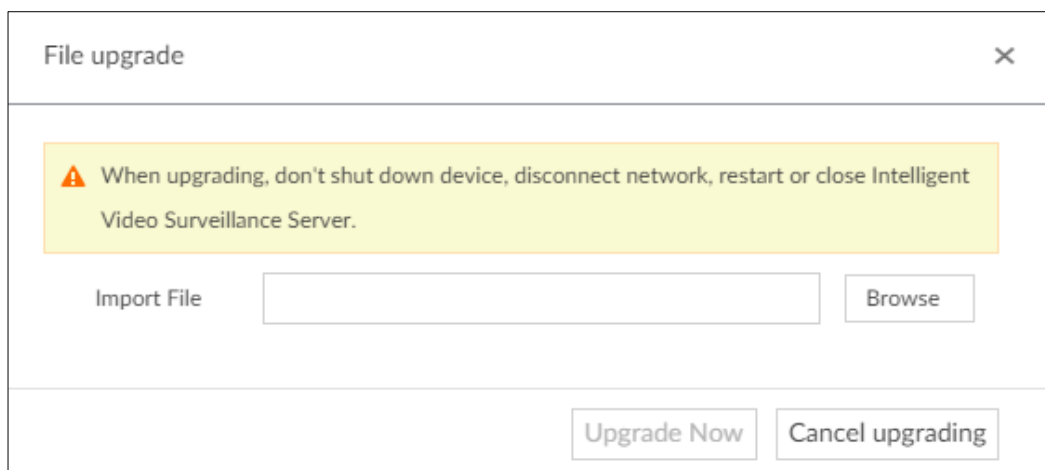


- You can select multiple AI modules at the same time.
- System cannot upgrade different types of AI modules at the same time.

**Step 3** Click **File Upgrade**.

The **File Upgrade** interface is displayed. See Figure 9-8.

Figure 9-8 File upgrade



**Step 4** Click **Browse** to select an upgrade file.

**Step 5** Click **Upgrade Now**.


The system starts upgrading. After the upgrade is completed, AI module automatically reboots.

## 9.3.2 Default

When the system runs slowly and has configuration errors, try to solve the problems by restoring the default settings.



All configurations are lost after factory default operation.

**Step 1** On the **LIVE** interface, click , from **Maintain > Device Maintain > Default**.



The **Default** interface is displayed. See Figure 9-9.

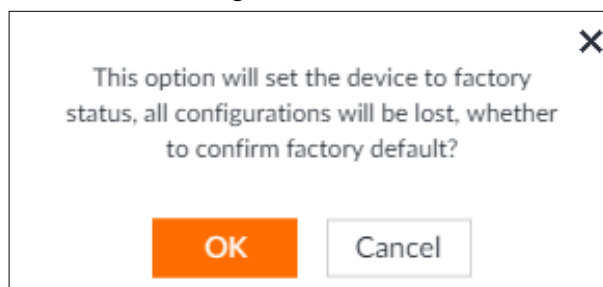
Figure 9-9 Default



**Step 2** Click **Factory Default**.

System pops up a confirmation box. See Figure 9-10.

Figure 9-10 Note




**Step 3** Click **OK**.

System begins to restore default settings. After successfully restored default settings, system prompts to reboot the device.

### 9.3.3 Auto Maintain

If the device has run for a long time, you can set to automatically reboot the device at idle time.

**Step 1** On the **LIVE** interface, click , from **Maintain > Device Maintain > Auto Maintain**.

The **Auto Maintain** interface is displayed. See Figure 9-11.

Figure 9-11 Auto Maintain



**Step 2** Set auto reboot time.

**Step 3** Click **Save**.

### 9.3.4 IMP/EXP

Export device configuration file to local PC or USB storage device, to backup it. When the configuration is lost due to abnormal operation, import the backup configuration file to restore system configurations quickly.


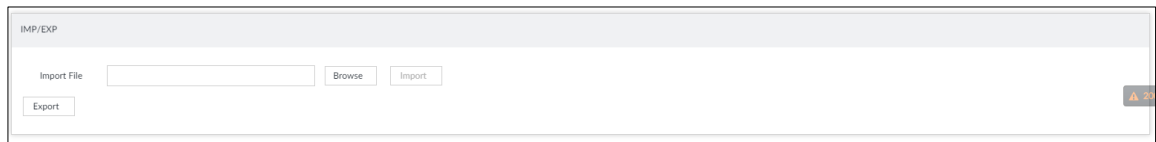


On the **LIVE** interface, click , and select **Maintain > Device Maintain > IMP/EXP**. The **IMP/EXP** interface is displayed. See Figure 9-12.

Figure 9-12 IMP/EXP



## Export Config

Click **Export** to export configuration file to local PC or USB storage device. File path may vary depending on interface operations, and the actual interface shall prevail.

- On IVSS client, click , select Download content to view file saving path. For details, see 10.3 View Downloads
- Select file saving path during local operation.  
  
Connect USB device to IVSS if you are on the local menu to operate.
- During web operations, files are saved under default downloading path of the browser.

## Import Config

Step 1 Click **Browse** to select the configuration file.

Step 2 Click **Import**.

After the configuration file is imported successfully, the device will reboot automatically.

# 10 IVSS Client Introduction

After installing IVSS client, system supports to access the device remotely. It is to realize system configuration, function operations and system maintenance.



Refer to "5.3.1 Logging in Client" for detailed information.

## 10.1 Interface Description










Double-click  on the PC desktop. System displays IVSS Client at full screen by default. Click  to display the task column. See Figure 10-1. Refer to Table 10-1 for detailed information.


Figure 10-1 IVSS task column



Table 10-1 Icons

Icons	Description
	Address bar: Enter the IP address of remote device.
	Input device IP address and then click the button to go to the login interface. Now the icon turns into  . Click to refresh the interface.
	Click to view history login record, view downloads, set compatibility mode and view IVSS version information.
	Click to minimize IVSS Client.
	Click to display IVSS Client at full screen.
	Click to close IVSS Client.

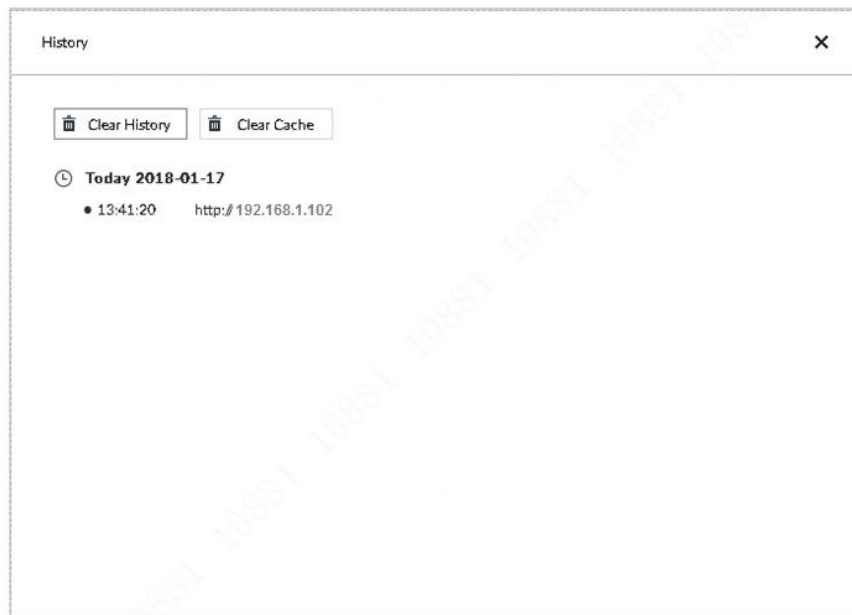
## 10.2 History Record

Click , and then select **History Record**.


The **History Record** interface is displayed. See Figure 10-2. It is to view history access record and clear buffer.

- Click **Clear History** to clear all history records.
- Click **Clear Buffer** to clear buffer data, and reboot IVSS client.

Figure 10-2 History record



## 10.3 View Downloads

Click , and then select **Downloads**. The **Downloads** interface is displayed. See Figure 10-3. It is to view and clear history downloads.

- Double click file name to open it.
- Click **Displayed in Folder** to open the folder where the file is located.
- Click **Clear Downloads** to clear history download records.

Figure 10-3 Downloads



## 10.4 Configuring IVSS Client

When PC theme is not Areo, video of IVSS client might not be displayed normally. It is suggested that PC theme should be switched to Areo, or compatibility mode of IVSS client should be enabled.

### Switching PC Theme



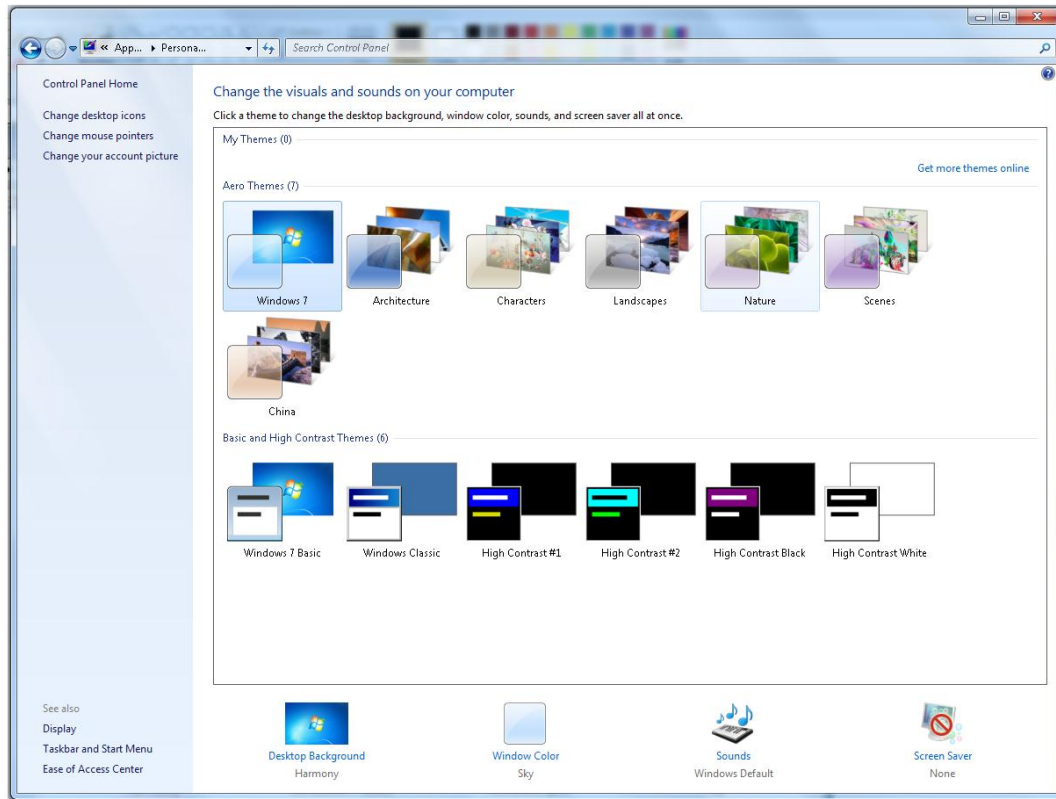
The following steps are to take Windows 7 for example. Refer to the actual interface for detailed information.

Right-click any blank position on PC desktop, select **Personalize**, and switch to Aero theme. See Figure 10-4.




After switching PC Theme, it will take effect after rebooting IVSS client.

Figure 10-4 PC theme



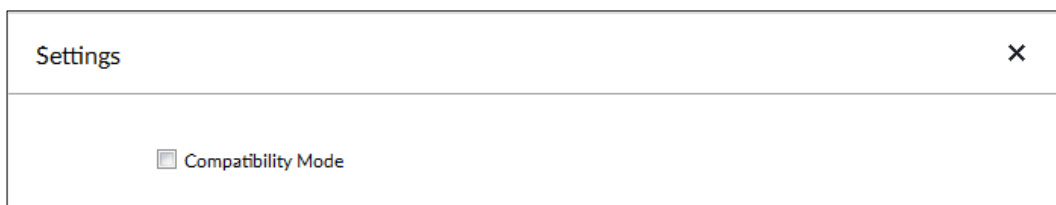
## Enable compatibility mode

Click , and select **Settings**. The **Settings** interface is displayed. See Figure 10-5. Select **compatibility mode**.



After enabling the mode, it will take effect after rebooting IVSS client.

Figure 10-5 Setting



## 10.5 Viewing Version Details


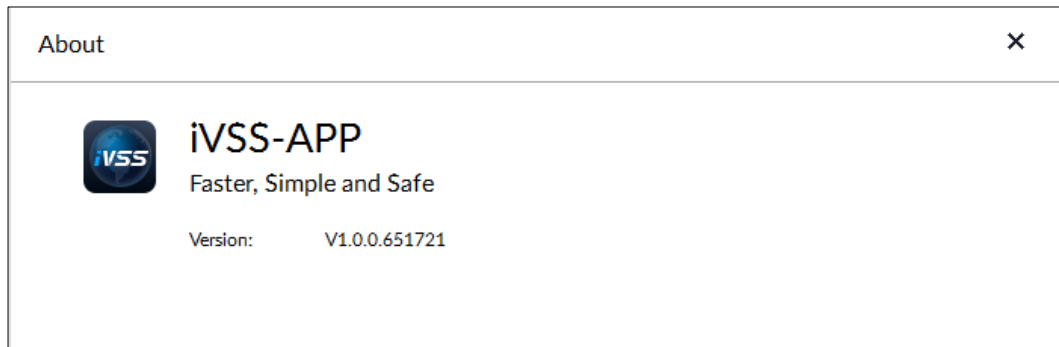
Click  and then select **About**. The **About** interface is displayed. See Figure 10-6. It is to view IVSS Client version information.

Figure 10-6 About

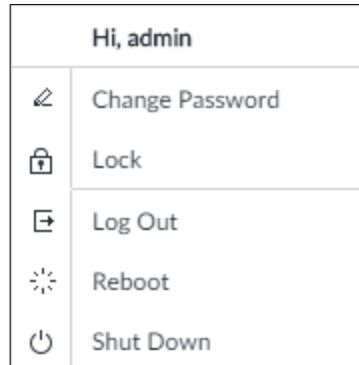


# 11


## Log Out/Reboot/Shut Down

It is to log out, reboot and shutdown the device. See Figure 11-1.


Figure 11-1 User operation



### Log Out

Click , and then select **Log Out**.


### Reboot

Click , and then select **Reboot**. System pops up confirm dialogue box. Click **OK** to reboot.


### Shut Down



To unplug the power cable may result in data (record, image) loss. We recommend Mode 1.

- Mode 1 (recommended): Click , and then select **Shutdown**. System pops up confirm dialogue box and then click **OK** to shut down.
- Mode 2: Use power on/off button on the device.
  - ◇ 8-HDD series product: Press power on/off button on rear panel.
  - ◇ Other series products: Press the power on/off button on the device for at least 4 seconds.
- Mode 3: Unplug the power cable.

# 12 FAQ

Problem	Possibilities and Solutions
<p>After enabling AI by device function, there is no human face comparison event.</p>	<ul style="list-style-type: none"> <li>● The AI module is offline.</li> </ul> <p>On the <b>LIVE</b> interface, click . Select <b>System &gt; Maintain &gt; Upgrade &gt; AI Module</b>, check the AI module is online or not.</p> <ul style="list-style-type: none"> <li>● There are too many filter criteria on the AI display interface.</li> <li>● The registered remote device does not support face detection function.</li> </ul> <p>Enable AI by device function. Refer to "6.2.3 Configuring Face Detection" for detailed information.</p> <ul style="list-style-type: none"> <li>● It is not in the deployment period.</li> <li>● There is no linked face database or the face database has no data.</li> <li>● The human face similarity setting is too high.</li> </ul>
<p>After enabling AI by camera function, there is no human face comparison event.</p>	<ul style="list-style-type: none"> <li>● The human face comparison function has not been enabled on the AI plan.</li> <li>● There is no human face database on the WEB interface of the remote device.</li> <li>● It is not in the deployment period.</li> </ul>
<p>There are no human face search results.</p>	<ul style="list-style-type: none"> <li>● The human face similarity setting is too high.</li> <li>● The selected remote device does not trigger the human face comparison.</li> <li>● There is no human face comparison on the search period</li> <li>● The specified human face image is not on the human face database.</li> </ul>



# Appendix 1 Operation Description

## Appendix 1.1 Mouse Operations

Connect mouse to the USB port, you can use the mouse to control the local menu. Refer to Appendix table 1-1 for detailed information.

Appendix table 1-1 Mouse operation description

Operation	Description
Click (click the left mouse button)	<ul style="list-style-type: none"><li>• Left-click mouse to select a function menu, to enter the corresponding menu interface.</li><li>• Implement the operation indicated on the control.</li><li>• Change check box and option button status.</li><li>• Left-click check box to display dropdown list.</li><li>• On virtual keyboard, select letter, symbol, English upper letter and lower letter, and Chinese characters.</li></ul>
Double-click (click the left mouse button twice)	<ul style="list-style-type: none"><li>• On the <b>LIVE</b> interface, double-click one video window to zoom in the window. Click any position out of the window, so the video window restores original size.</li><li>• On the <b>LIVE</b> interface, double-click the remote device in the device tree. Switch to video edit status, and add remote device.</li><li>• Double-click the image or record file thumbnail, to playback record file or view the image.</li></ul>
Right-click (click the right mouse button)	<ul style="list-style-type: none"><li>• On the <b>LIVE</b> or <b>SEARCH</b> interface, right-click one video window to display right-click menu.</li><li>• On the <b>LIVE</b> interface, right-click the view in the list or the remote device in the device tree, to display right-click menu.</li></ul>
Wheel button	<ul style="list-style-type: none"><li>• On <b>SEARCH</b> interface, move the cursor to the time bar, and then click the mouse middle button, to adjust the accurate time on the time bar.</li><li>• Click the control that needs to input number (such as input date or time). Roll the middle button to adjust the number value.</li></ul>
Drag the mouse	<ul style="list-style-type: none"><li>• Drag the mouse to select the motion detect zone.</li><li>• On the <b>LIVE</b> interface, drag the remote device in the device tree to the play window, switch to the view status. It is to add the remote device.</li><li>• On <b>SEARCH</b> interface, drag the record file or the image thumbnail to the playback window. It is to play back the corresponding record file or image.</li></ul>

## Appendix 1.2 Virtual Keyboard

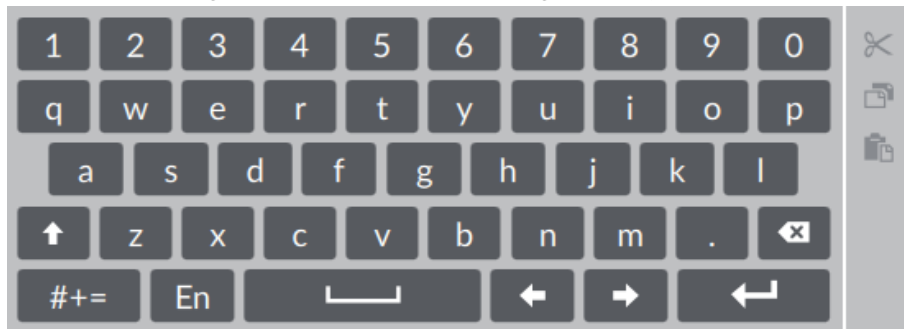
On local menu, it supports virtual keyboard function.

Click the text box to display virtual keyboard interface. See Appendix figure 1-1 or Appendix figure 1-2. Refer to Appendix table 1-2 for detailed information.



If the device has connected to the peripheral keyboard, click the text column. Virtual keyboard will disappear.





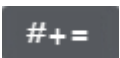








Appendix figure 1-1 Virtual keyboard (global keyboard)



Appendix figure 1-2 Virtual keyboard (digital keyboard)



Appendix table 1-2 Virtual keyboard icon

Signal Words	Description
	Click the icon to switch to upper case. The icon becomes  . Click  to switch to lower case.
	Click to delete letter.
	Click to input letter. See Appendix figure 1-3. Now the icon turns into  . Click  to restore previous input mode.
	Click to input space.
	Click to control cursor position.
	Click to switch to the next line.
	Select text and click the icon to cut the selected contents.
	Select text and click the icon to copy the selected contents.
	Cut or copy the contents, click the text box and click the icon to paste the contents.

Appendix figure 1-3 Virtual keyboard (input letter)



# Appendix 2 RAID

RAID is an abbreviation for Redundant Array of Independent Disks. It is to combine several independent HDDs (physical HDD) to form a HDD group (logic HDD).

Comparing with one HDD, RAID provides more storage capacity and data redundancy. The different redundant arrays have different RAID level. Each RAID level has its own data protection, data availability and performance degree.

## RAID Level

RAID Level	Description	Min. HDD Needed
RAID 0	RAID 0 is so called striping. RAID 0 is to save the continued data fragmentation on several HDDs. It can process the read and write at the same time, so its read/write speed is N (N refers to the HDD amount of the RAID 0) times as many as one HDD. RAID 0 does not have data redundant, so one HDD damage may result in data loss that cannot be restored.	2
RAID 1	It is also called mirror or mirroring. RAID 1 data is written to two HDDs equally, which guarantee the system reliability and can be repaired. RAID 1 read speed is almost close to the total volume of all HDDs. The write speed is limited by the slowest HDD. At the same time, the RAID 1 has the lowest HDD usage rate. It is only 50%.	2
RAID 5	RAID 5 is to save the data and the corresponding odd/even verification information to each HDD of the RAID 5 group and save the verification information and corresponding data to different HDDs. When one HDD of the RAID 5 is damaged, system can use the rest data and corresponding verification information to restore the damaged data. It does not affect data integrity.	3
RAID 6	Based on the RAID 5, RAID 6 adds one odd/even verification HDD. The two independent odd/even systems adopt different algorithm, the data reliability is very high. Even two HDDs are broken at the same time, there is no data loss risk. Comparing to RAID 5, the RAID 6 needs to allocate larger HDD space for odd/even verification information, so its read/write is even worse.	4
RAID 10	RAID 10 is a combination of the RAID 1 and RAID 0. It uses the extra high speed efficient of the RAID 0 and high data protection and restores capability of the RAID 1. It has high read/write performance and security. However, the RAID 10 HDD usage efficiency is as low as RAID 1.	4

## RAID Capacity

Refer to the sheet for RAID space information.

capacityN refers to the mini HDD amount to create the corresponding RAID.

<b>RAID Level</b>	<b>Total Space of the N HDD</b>
RAID 0	The total amount of current RAID group
RAID 1	Min (capacityN)
RAID 5	$(N-1) \times \text{min (capacityN)}$
RAID 6	$(N-2) \times \text{min (capacityN)}$
RAID 10	$(N/2) \times \text{min (capacityN)}$
RAID 50	$(N-2) \times \text{min (capacityN)}$
RAID 60	$(N-4) \times \text{min (capacityN)}$

# 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.

$$\text{Recording time (hour)} = \frac{\text{Total capacity (M)}}{\text{HDD capacity occupied per hour (M/hour)} \times \text{Channel number}}$$

For example, for single-channel recording, HDD capacity occupied per hour is 200M/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 × 200M/hour = 576G. Therefore, five 120G HDD or four 160G HDD shall 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):

Bit stream size (max.)	File size	Bit stream size (max.)	File size
≤ 96K	42M	128K	56M
160K	70M	192K	84M
224K	98M	256K	112M
320K	140M	384K	168M
448K	196M	512K	225M
640K	281M	768K	337M
896K	393M	1024K	450M
1280K	562M	1536K	675M
1792K	787M	2048K	900M

## Appendix 4 Glossary

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 defines 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.
RAID	RAID is an abbreviation for Redundant Array of Independent Disks. It is to combine several independent HDDs (physical HDD) to form a HDD group (logic HDD), to provide higher storage performance and data redundancy.
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 5 Cybersecurity

## Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

### **Mandatory actions to be taken for basic equipment network security:**

#### **1. Use Strong Passwords**

Please refer to the following suggestions to set passwords:

- The length should not be less than 8 characters;
- Include at least two types of characters; character types include upper and lower case letters, numbers and symbols;
- Do not contain the account name or the account name in reverse order;
- Do not use continuous characters, such as 123, abc, etc.;
- Do not use overlapped characters, such as 111, aaa, etc.;

#### **2. Update Firmware and Client Software in Time**

- According to the standard procedure in Tech-industry, we recommend to keep your equipment (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
- We suggest that you download and use the latest version of client software.

### **"Nice to have" recommendations to improve your equipment network security:**

#### **1. Physical Protection**

We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable equipment (such as USB flash disk, serial port), etc.

#### **2. Change Passwords Regularly**

We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

#### **3. Set and Update Passwords Reset Information Timely**

The equipment supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

#### **4. Enable Account Lock**

The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

#### **5. Change Default HTTP and Other Service Ports**

We suggest you to change default HTTP and other service ports into any set of numbers between 1024–65535, reducing the risk of outsiders being able to guess which ports you are using.

#### **6. Enable HTTPS**

We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

#### **7. Enable Whitelist**

We suggest you to enable whitelist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the whitelist.

#### **8. MAC Address Binding**

We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.

#### **9. Assign Accounts and Privileges Reasonably**

According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

#### **10. Disable Unnecessary Services and Choose Secure Modes**

If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

- SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up strong passwords.
- AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

#### **11. Audio and Video Encrypted Transmission**

If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

Reminder: encrypted transmission will cause some loss in transmission efficiency.

#### **12. Secure Auditing**

- Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
- Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

#### **13. Network Log**

Due to the limited storage capacity of the equipment, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

#### **14. Construct a Safe Network Environment**

In order to better ensure the safety of equipment and reduce potential cyber risks, we recommend:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.