Intelligent Video Surveillance Server

Quick Start Guide

V3.0.0

Foreword

General

This manual describes the structure, function and operation of intelligent video surveillance server (IVSS).

Models

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

Revision History

Version	Revision Content	Release Time
V3.0.0	● Added search by image, cluster, and fisheye dewarp. ● Updated chapters including intelligent operation and device management according to the new device version.	December 2019
V2.1.0	Add video metadata, vehicle recognition, and vehicle comparison functions.	June 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

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 guide, CD-ROM, QR code or our official website. If there is inconsistency between paper guide 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, see our final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the Device.

Important Safeguards and Warnings

The following description is the correct application method of the Device. Read the Guide carefully before use to prevent danger and property loss. Strictly conform to the Guide during application and keep it properly after reading.

Operating Requirement

- Do not place and install the Device in an area exposed to direct sunlight or near heat generating devices.
- Do not install the Device in a humid, dusty or fuliginous area.
- Install the Device at stable places horizontally.
- Make the Device stay away from liquid.
- Install the Device at well-ventilated places; do not block its ventilation opening.
- Use the Device only within rated input and output range.
- Do not dismantle the Device arbitrarily.
- Transport, use and store the Device within allowed humidity and temperature range.

Power Requirement

- Be sure to use the designated battery type. Otherwise there might be explosion risk.
- Be sure to use batteries according to requirements; otherwise, it might 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 this 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, see 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, keep an angle that facilitates operation.

Attention

- Do not insert or take out the expansion drawer without powering off first.
- AI module does not support hot plugging. If you need to replace the AI module, power off the Device first. Otherwise, it will lead to file damage on the AI module.

Table of Contents

1 Overview

1.1 Introduction

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

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

1.2 Login Mode

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

Operations and system configurations in the Guide are mainly based on IVSS client. There might be differences from local or web operation, and the actual interface shall prevail.

Table 1-1 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.
Web login	Connect the Device and PC to the same network, and remotely access the Device through browser (Google Chrome and Firefox) on PC.	Support majority functions of the Device, except live preview, record playback and video-related function.
IVSS client login	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 chapter introduces front panel, rear panel, port function and button function, indicator light status, and so on.

This chapter takes 16-HDD for example. For other models, see user’s manual.

2.1 Front Panel

Figure 2-1 Font panel with LCD

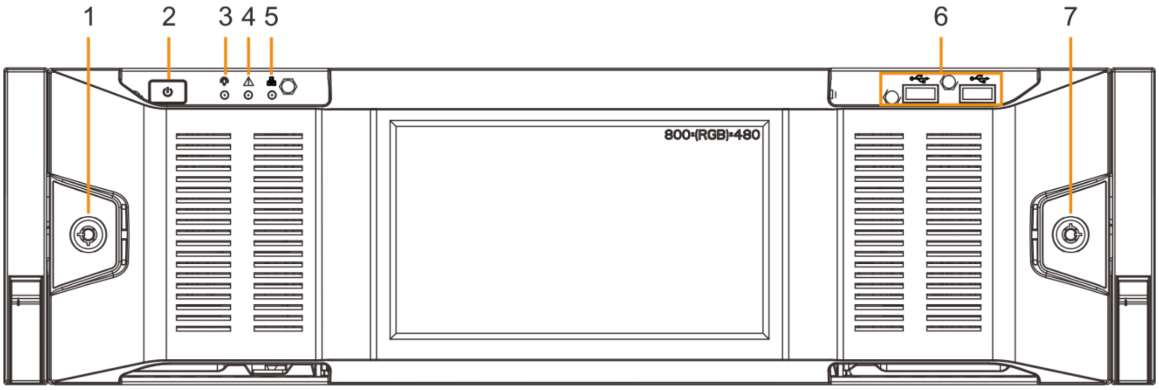


Figure 2-2 Front panel without LCD

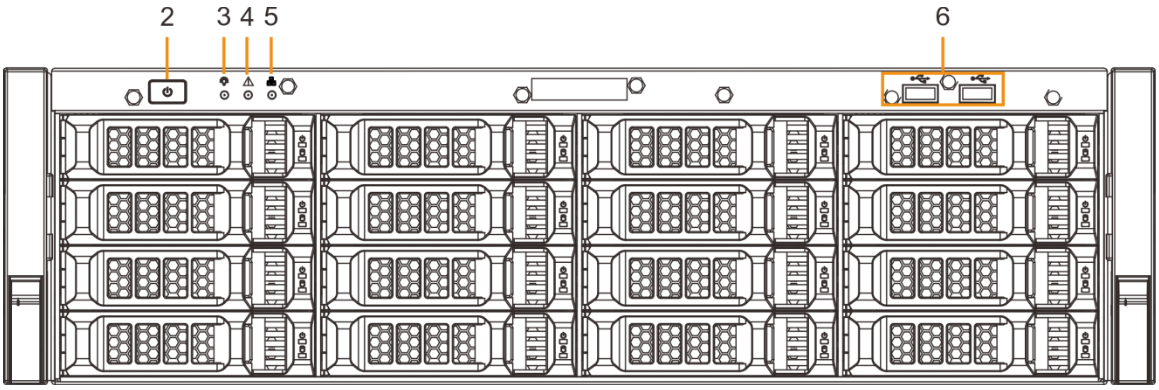


Table 2-1 Front panel description

No.	Name	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 2-2.
2	Power on/off button	Boot up or shut down device. The power on/off button has the indicator light. It can display device running status. ● When device is off (indicator light is off), press the button for a short period to boot up device. ● When device is running, (blue indicator light is on), press the button for at least 4 seconds to shut down the Device.

No.	Name	Description
3	System status indicator	Displays the system running status. ● The blue light is on: Device is running properly. ● The indicator light is off: The device is not running.
4	Alarm indicator light	Displays local input alarm status. ● Red indicator light is on: There is local alarm input event. ● The indicator light is off: There is no local alarm input event.
5	Network indicator light	Displays current network status. ● The indicator light is blue: It means at least one Ethernet port has connected to the network. ● The indicator light is off: No Ethernet ports are connected to the network.
6	USB port	Connects to external devices such as USB storage device, keyboard and mouse.
7	16-HDD slot	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. There are two indicator lights on the HDD slot: HDD indicator light and HDD read/write indicator light. ● ⏻: HDD indicator light. The light is yellow after you install the HDD. ● 🛢: Read/write indicator light. The blue light flashes when it is reading and writing data.

2.2 Rear Panel

Figure 2-3 Rear panel

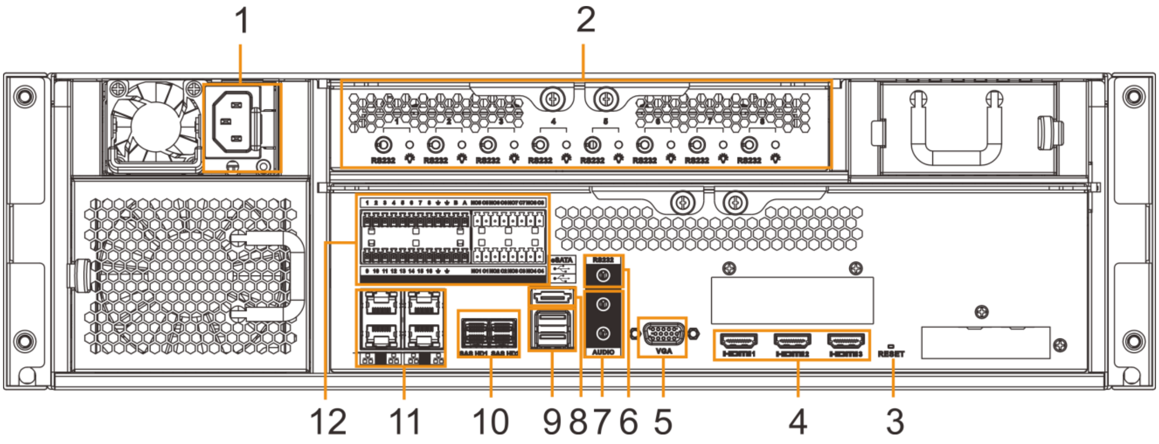


Table 2-2 Rear panel description

No.	Name	Description
1	Power input port	Inputs AC 100V-AC 240V power.

No.	Name	Description
2	AI module indicator light	Displays AI module status. ● The yellow light flashes: AI module is running properly. ● The yellow light is on: AI module is malfunctioning. 📖 This function is valid if there is AI module.
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
	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	16 groups (1–16) of alarm input ports. They are corresponding to ALARM 1–ALARM 16. The alarm becomes valid in low level. ● A and B: Control the A/B cable of the RS-485 device. It is to connect to the PTZ camera. Connect in parallel 120Ω between A/B cables if there are too many PTZ decoders. ● ⏚: GND end.
	Alarm output	8 groups of alarm output ports (NO1 C1–NO8 C8). Output alarm signal to the alarm device. Make sure that there is power to the external alarm device. ● NO: Alarm output port of Normally Open type. ● C: Common alarm output port. ● ⏚: GND end.

2.3 Dimensions

Figure 2-4 Dimensions with LCD (mm[inch])

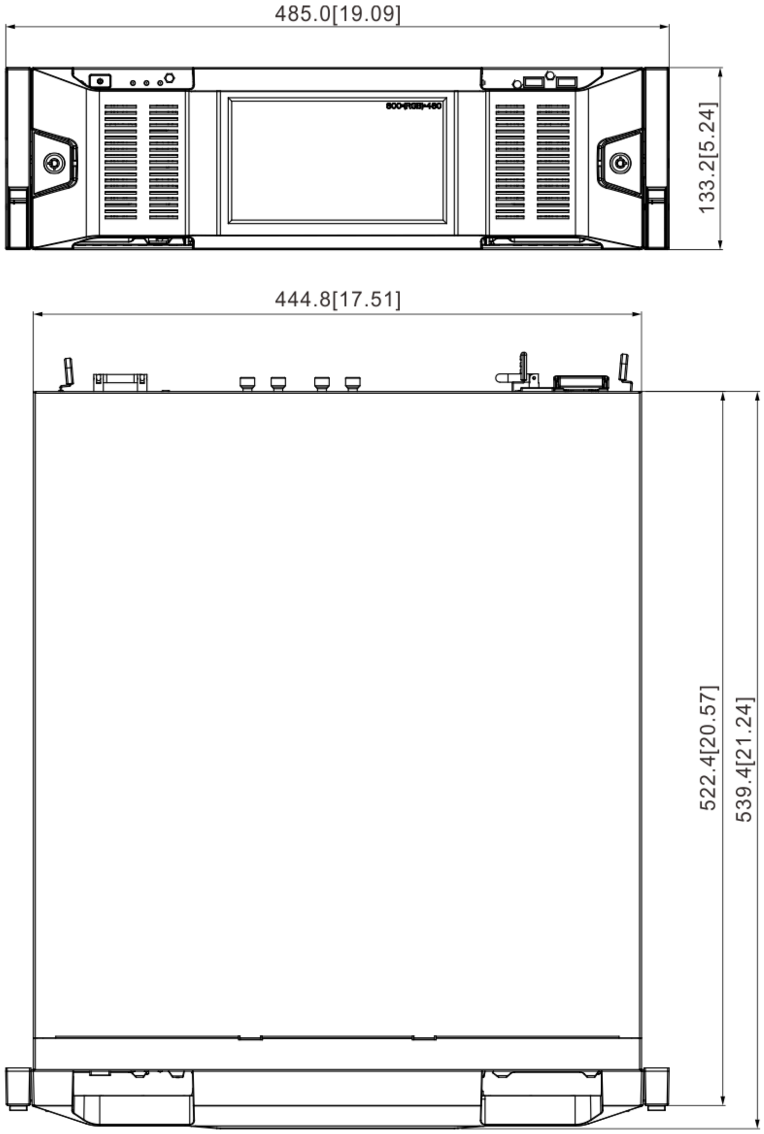
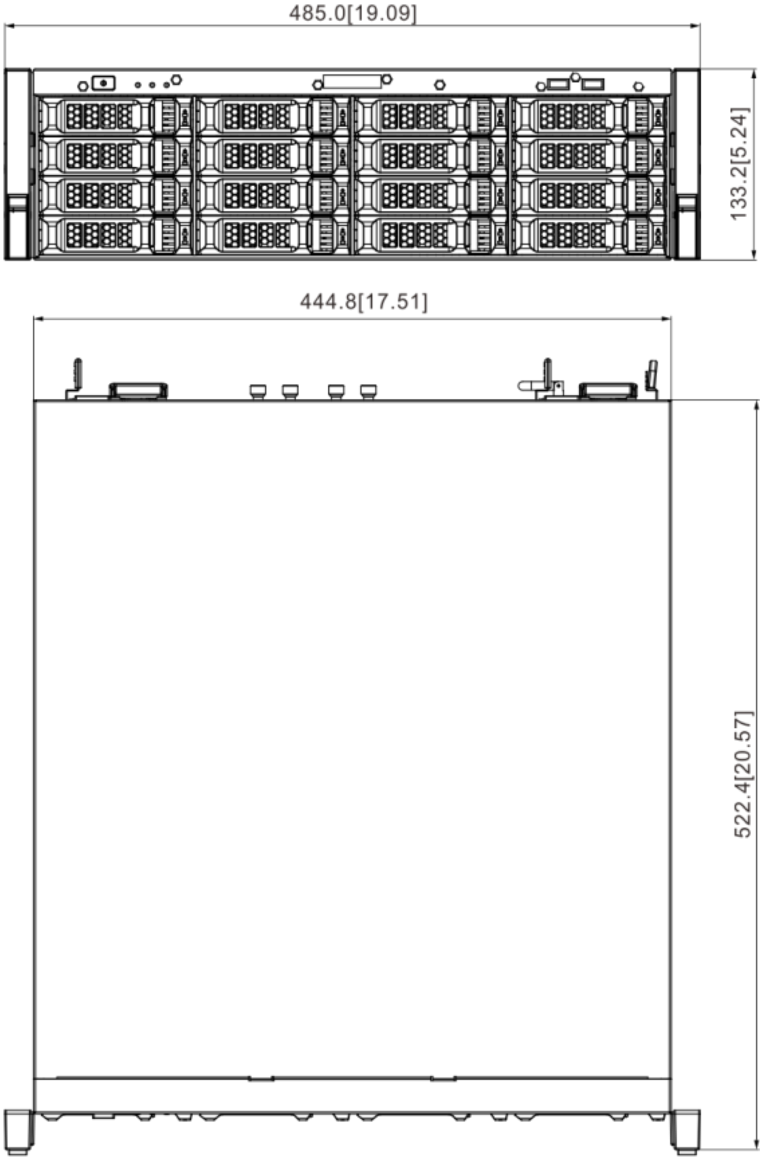


Figure 2-5 Dimensions without LCD (mm[inch])



3 Hardware Installation

This chapter introduces HDD installation, cable connection, and so on.

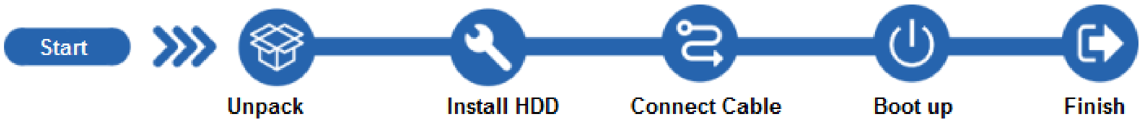
WARNING

Some series product is heavy. It needs several people to carry or move jointly to prevent person injury.

3.1 Installation Flow

See Figure 3-1 for installation flows. Please follow the steps to install.

Figure 3-1 Installation flows



3.2 Unpacking the Box

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

No.	Name		Contents
1	Whole package	Appearance	Whether there is any visible damage or not.
		Package	Whether there is any accidental clash during transportation or not.
		Accessories (list of accessories on the warranty card)	They are complete or not.
2	Device	Appearance	There is any visible damage or not.
		Device model	The model is the same as ordering contract or not.
		The label on the Device	Whether it is torn or not. Do not tear off, or discard the label. Usually you need to show the serial number when requiring after-sales service.

3.3 HDD Installation

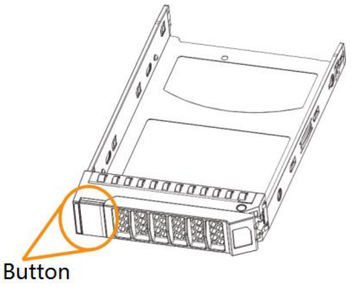
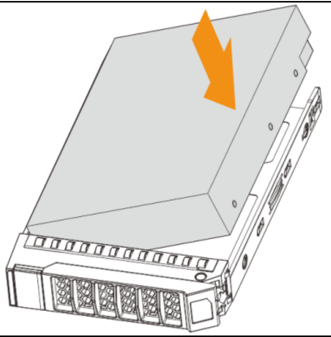
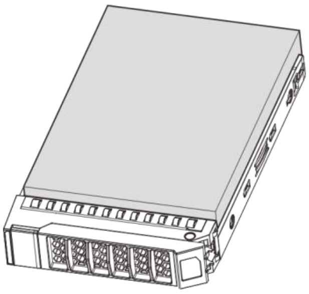
The section introduces HDD installation.

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

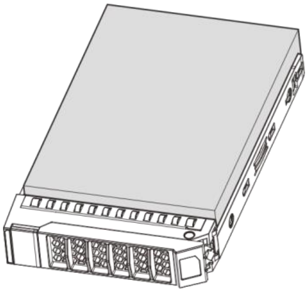
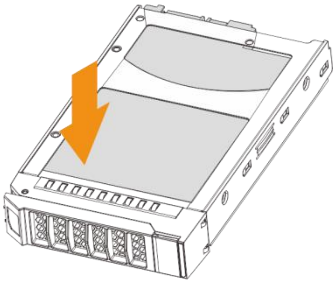
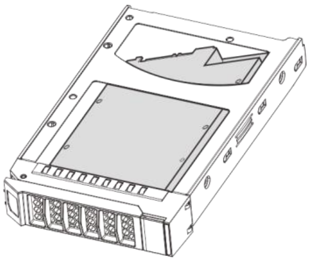
- Different models support different HDD numbers. See the actual situation.

3.3.1 12-HDD Series

Installing HDD

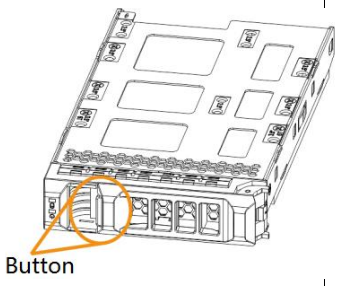
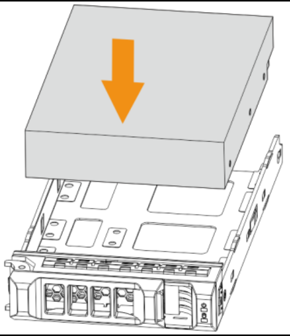
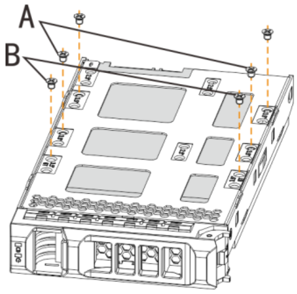
		
①Press the button on the front panel of IVSS device, open the handle, and then pull out the HDD box.	② Place one side of the HDD closely along the upper side of the box and press down to push the HDD down to the lower side of the mounting surface.	③Insert the HDD box into the HDD slot, press it to the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

Removing HDD

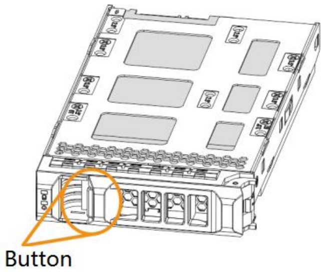
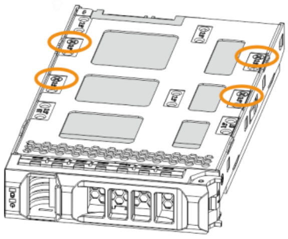
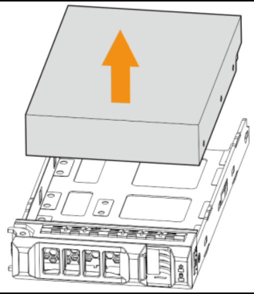
		
①Press the button on the front panel of IVSS device, open the handle, and then pull out the HDD box.	②On the back of the HDD box, press hard on the position indicated by the arrow.	③ Take out the HDD and reinsert the box to the slot. Push it to the bottom and close the box handle.

3.3.2 16/24-HDD Series

Installing HDD

 		
①Press the button on the front panel of IVSS device, open the handle, and then pull out the HDD box.	②Put the HDD into the box along the direction shown in the figure.	③Lock 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. 🕮 In the figure, you only need to lock one set of the screws (Group A or Group B). See the actual situation.

Removing HDD

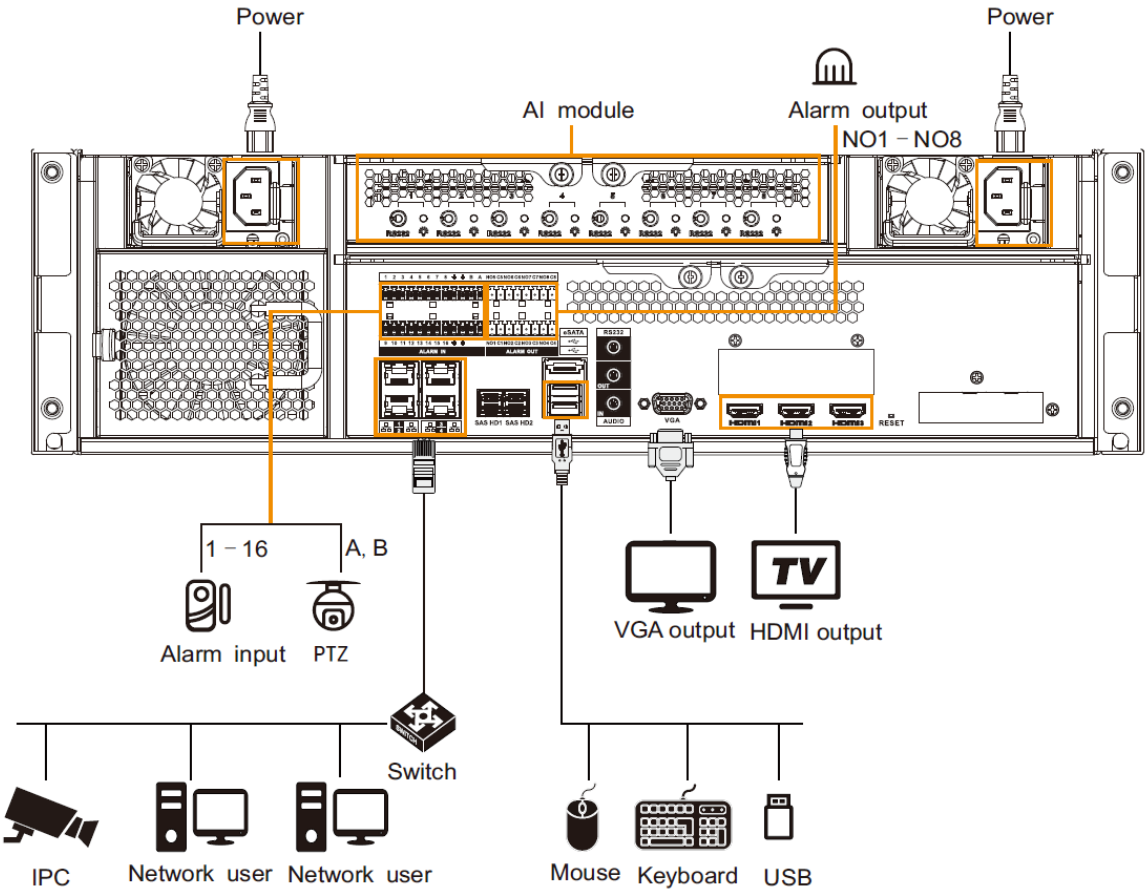
 		
①Press the button on the front panel of IVSS device, open the handle, and then pull out the HDD box.	②Unlock the screws on the back of the HDD box. 🕮 The screws are at different positions for different HDDs. See the actual situation.	③ Take out the HDD and reinsert the box to the slot. Push it to the bottom and close the box handle.

3.4 Connection Diagram

This section takes connecting 16-HDD series device for example. See Figure 3-2. The connection steps might vary depending on the Device, and the actual device shall prevail.

- 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



4 Turning on the Device

⚠CAUTION

- Before the boot-up, make sure that the input voltage matches 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.

Boot-up might vary depending on the model you purchased.

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

5 Initial Settings

For first-time use, you need to initialize the Device, set basic information and functions, and so on.

5.1 Initializing Device

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

Take web remote initialization for example.

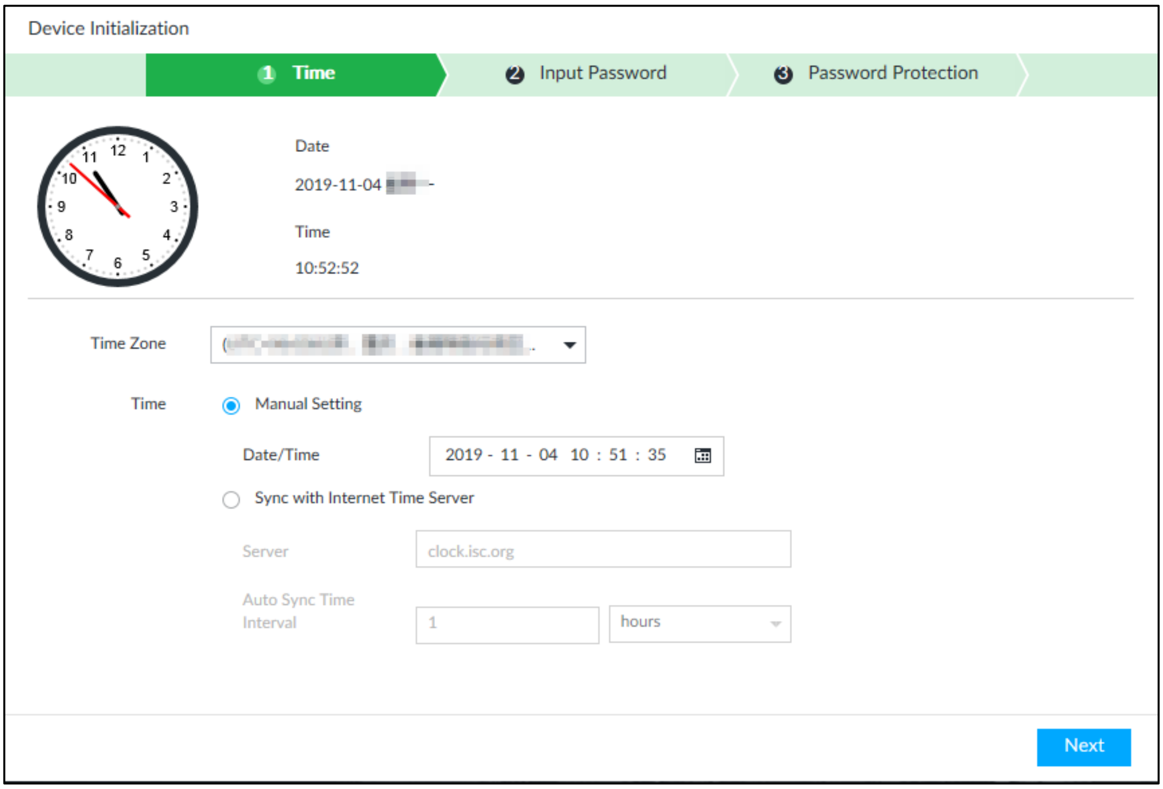
Step 1 Open the browser, enter IP address, and then press **Enter**.

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

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

The **Time** interface is displayed. See Figure 5-1.

Figure 5-1 Time setting



Device Initialization

1 Time | 2 Input Password | 3 Password Protection

Date

2019-11-04 [redacted]

Time

10:52:52

Time Zone ([redacted]

Time ● Manual Setting

Date/Time 2019 - 11 - 04 10 : 51 : 35

○ Sync with Internet Time Server

Server clock.isc.org

Auto Sync Time Interval 1 hours

Next

Step 3 On the **Time** interface, set time parameters. For details, see Table 5-1.

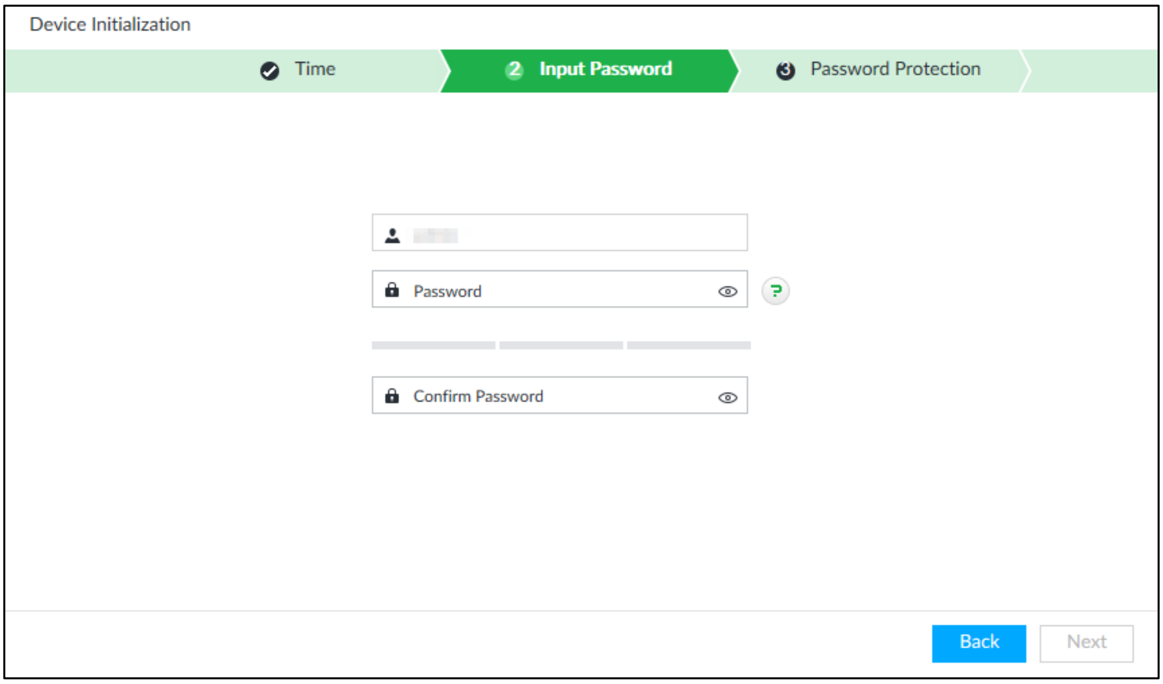
Table 5-1 Time parameters description

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

Step 4 Click **Next**.

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

Figure 5-2 Set password



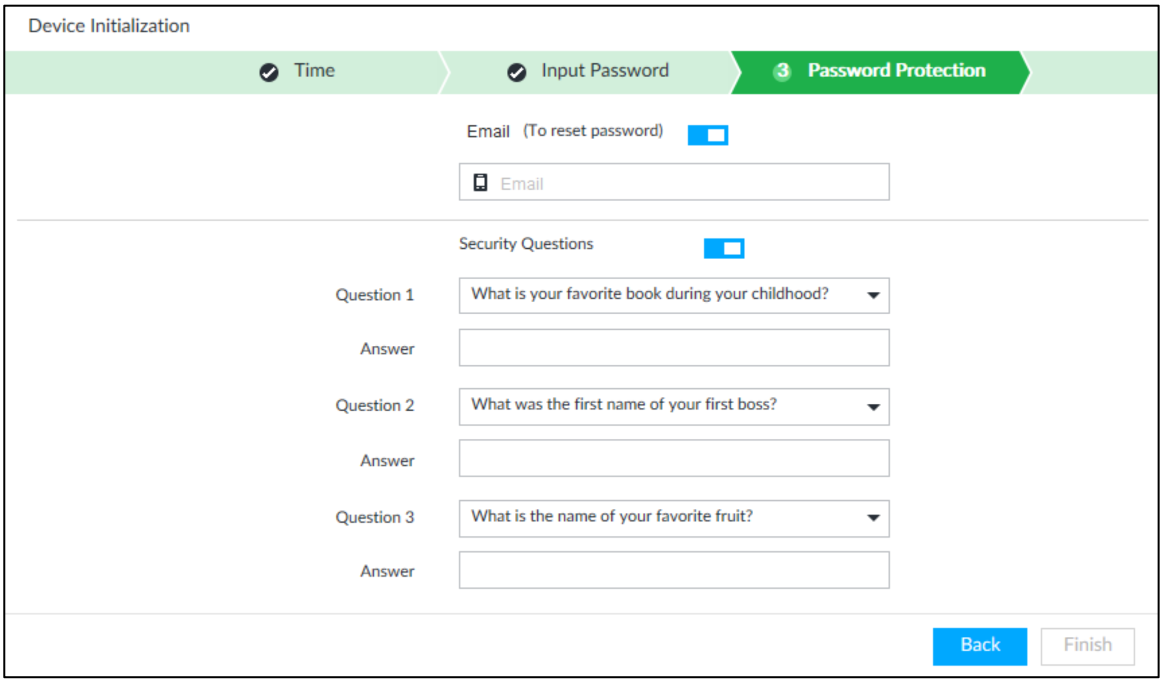
Step 5 Set admin login password.

The new password can be 8 characters to 32 characters in length and contains at least two types from number, letter and special characters (excluding "'", """", ";", ":" "&" and space).

Step 6 Click **Next**.

The **Password Protection** interface is displayed. See Figure 5-3.

Figure 5-3 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:

Step 7 Set password protection information.

You can use the email you input here or answer the security questions to reset admin password.

- Click ▣ to enable email or security questions. Click it again to disable the function.
- If the email or security questions are not set, the password can be reset on the local interface only.

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

The device initialization success interface is displayed. Click **Enter quick setting** button to go to the quick setting interface, and then set device basic information.

5.2 Quick Settings

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

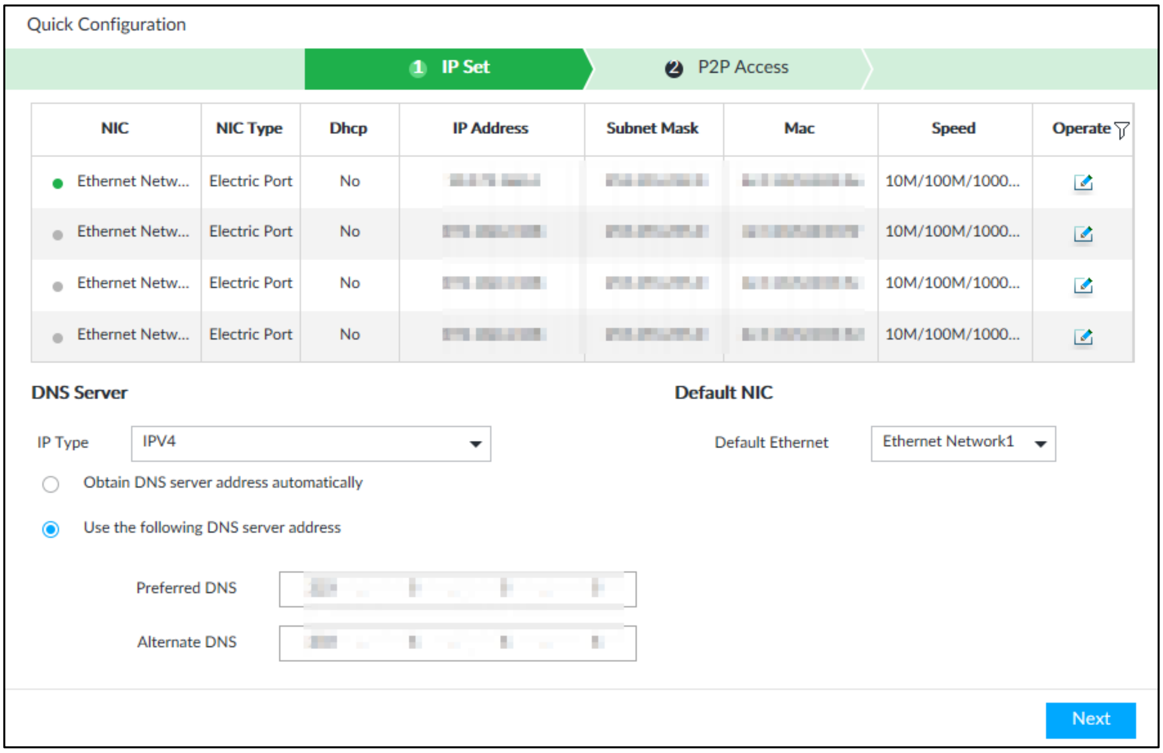
Step 1 Configure IP address.

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

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

The **IP Set** interface is displayed. See Figure 5-4.

Figure 5-4 IP setting



Quick Configuration

1 IP Set | 2 P2P Access

NIC	NIC Type	Dhcp	IP Address	Subnet Mask	Mac	Speed	Operate
● Ethernet Netw...	Electric Port	No	[redacted]	[redacted]	[redacted]	10M/100M/1000...	✎
● Ethernet Netw...	Electric Port	No	[redacted]	[redacted]	[redacted]	10M/100M/1000...	✎
● Ethernet Netw...	Electric Port	No	[redacted]	[redacted]	[redacted]	10M/100M/1000...	✎
● Ethernet Netw...	Electric Port	No	[redacted]	[redacted]	[redacted]	10M/100M/1000...	✎

DNS Server

IP Type: IPV4

○ Obtain DNS server address automatically

● Use the following DNS server address

Preferred DNS: [redacted]

Alternate DNS: [redacted]

Default NIC

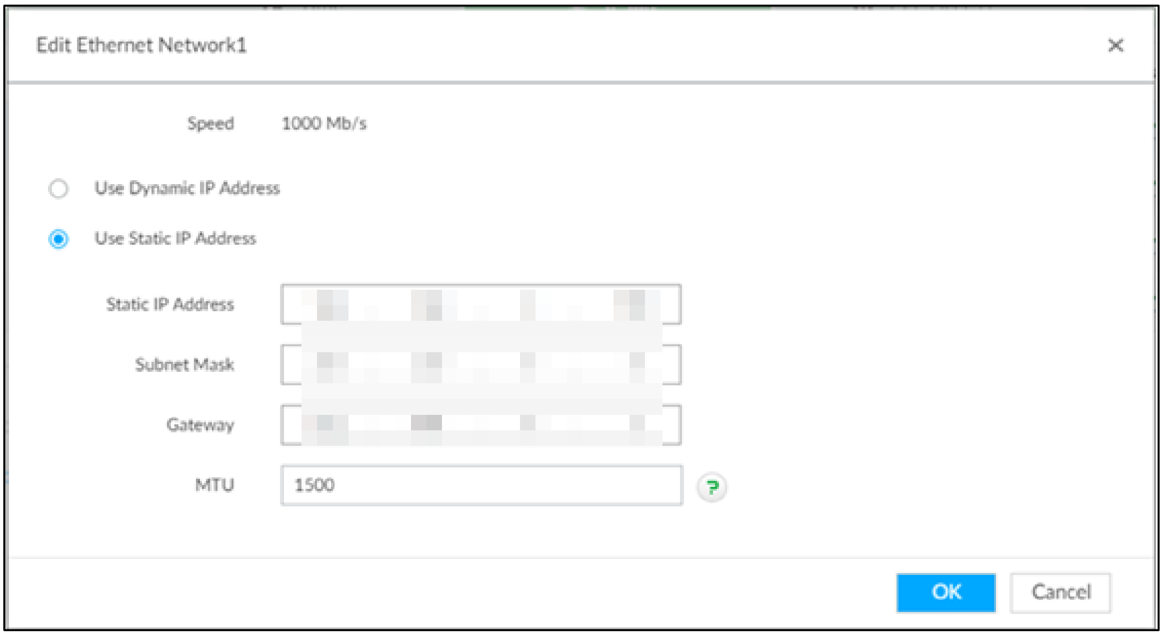
Default Ethernet: Ethernet Network1

Next

2) Click ✎ of the corresponding NIC to configure IP address. See Figure 5-5.

- When there is a DHCP server on the network, check **Use Dynamic IP Address**, system can allocate a dynamic IP address to the Device. There is no need to set IP address manually.
- Check **Use Static IP Address**, and then set static IP address, subnet mask and gateway to set a static IP address for the Device.

Figure 5-5 Edit Ethernet network



Edit Ethernet Network1 ×

Speed: 1000 Mb/s

○ Use Dynamic IP Address

● Use Static IP Address

Static IP Address: [redacted]

Subnet Mask: [redacted]

Gateway: [redacted]

MTU: 1500 ?

OK Cancel

3) Click **OK**.

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

4) Set DNS server information and default NIC.

An NIC that is connected to the network can be set as the default NIC.

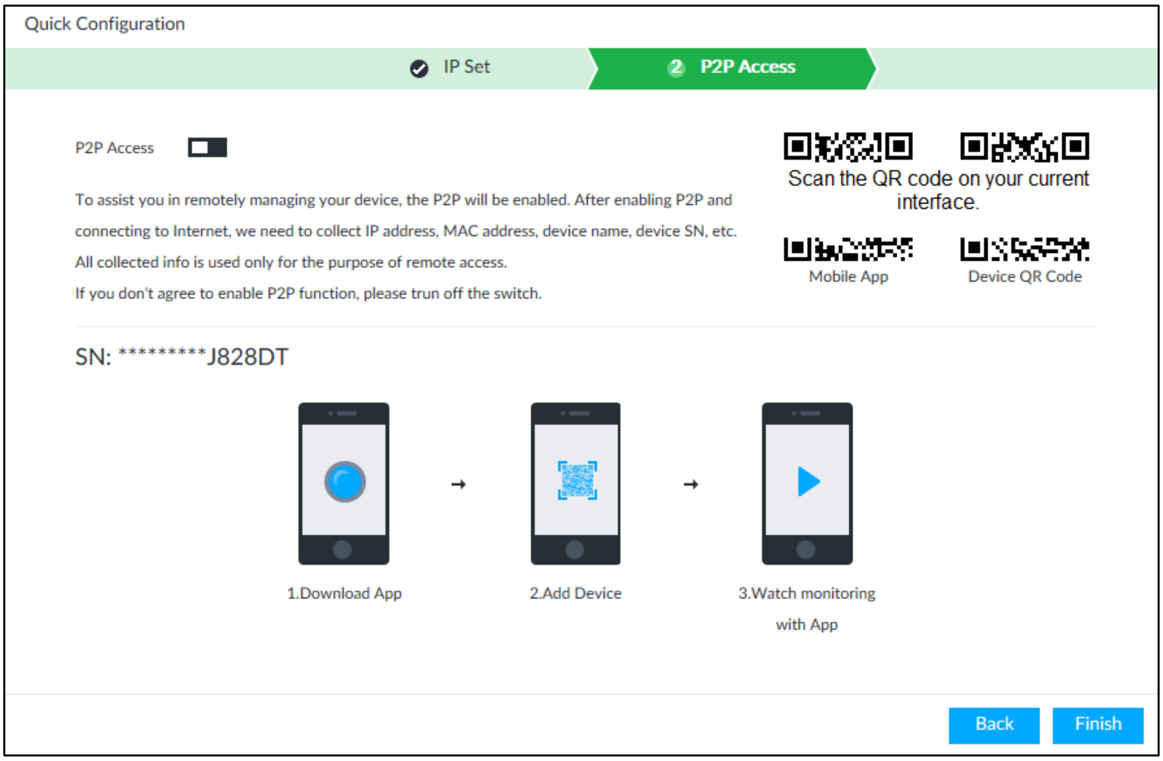
Step 2 Configure P2P settings

Make sure that the system has connected to the network. Otherwise, the P2P function is null.

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

The **P2P Access** interface is displayed. See Figure 5-6.

Figure 5-6 P2P access



To assist you in remotely managing your device, the P2P will be enabled. After enabling P2P and connecting to Internet, we need to collect IP address, MAC address, device name, device SN, etc. All collected info is used only for the purpose of remote access.

If you don't agree to enable P2P function, please trun off the switch.

SN: *********J828DT

2) Click ▭ to enable P2P function.

Step 3 Click **Finish**.

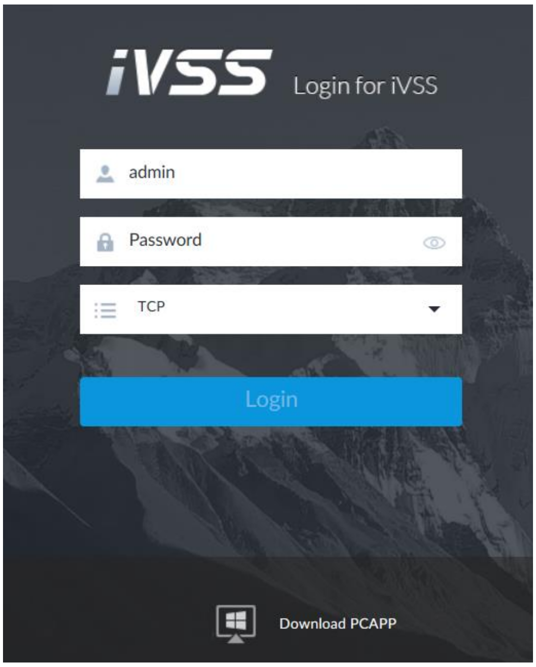
5.3 Login

- The system is logged in by default after you initialize the Device.
- This section takes logging in to the PCAPP client for example.

Step 1 Download PCAPP.

Open the browser, enter IP address, and then press Enter. Click **Download PCAPP** to download PCAPP installation package. See Figure 5-7.

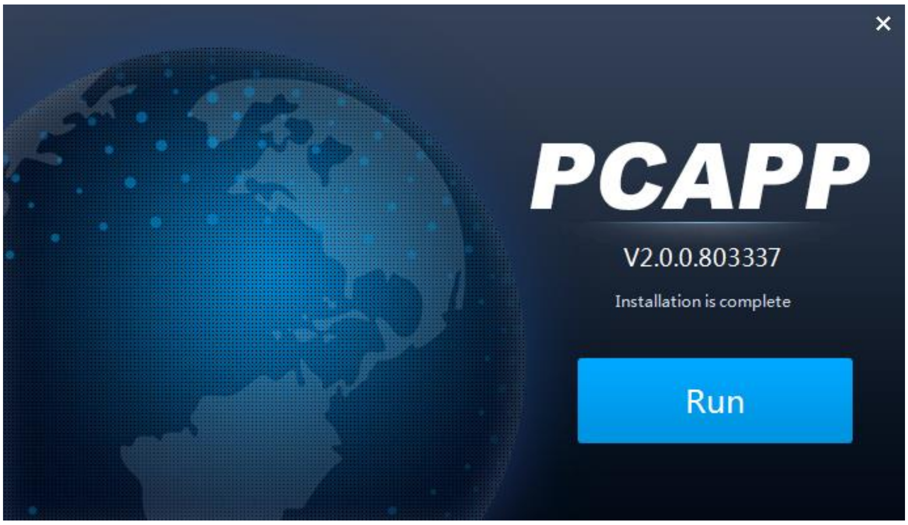
Figure 5-7 Web login interface



Step 2 Double-click the installation package, and then follow the onscreen instructions to complete the installation.

After the installation finishes, the following interface is displayed. See Figure 5-8.

Figure 5-8 Installation finishes

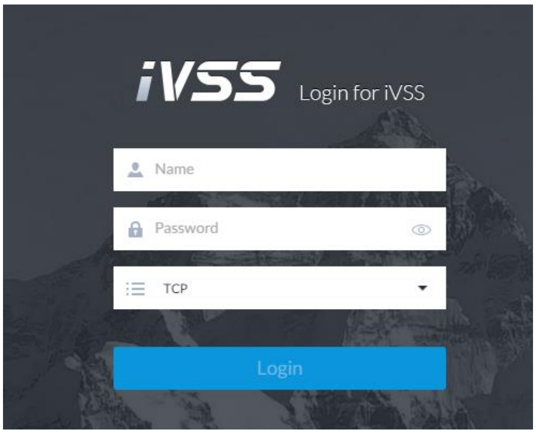


Step 3 On the installation completion interface, click **Run**.

The login interface is displayed. See Figure 5-9.

Click to display the task column. Enter IP address of the Device, and then press Enter to log in.

Figure 5-9 Login



Step 4 Enter device user name and password.

Step 5 Click **Login**.

5.4 Adding Remote Devices

After you initialize remote device, you can view the live video from the remote device, change remote device settings, and so on.

- Uninitialized device cannot be added. For details, see *User's Manual*.
- This section takes **Smart Add** for example.

Step 1 Click ⚙, or click + on **Setting** interface, and then select **DEVICE**.

The **DEVICE** interface is displayed.

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

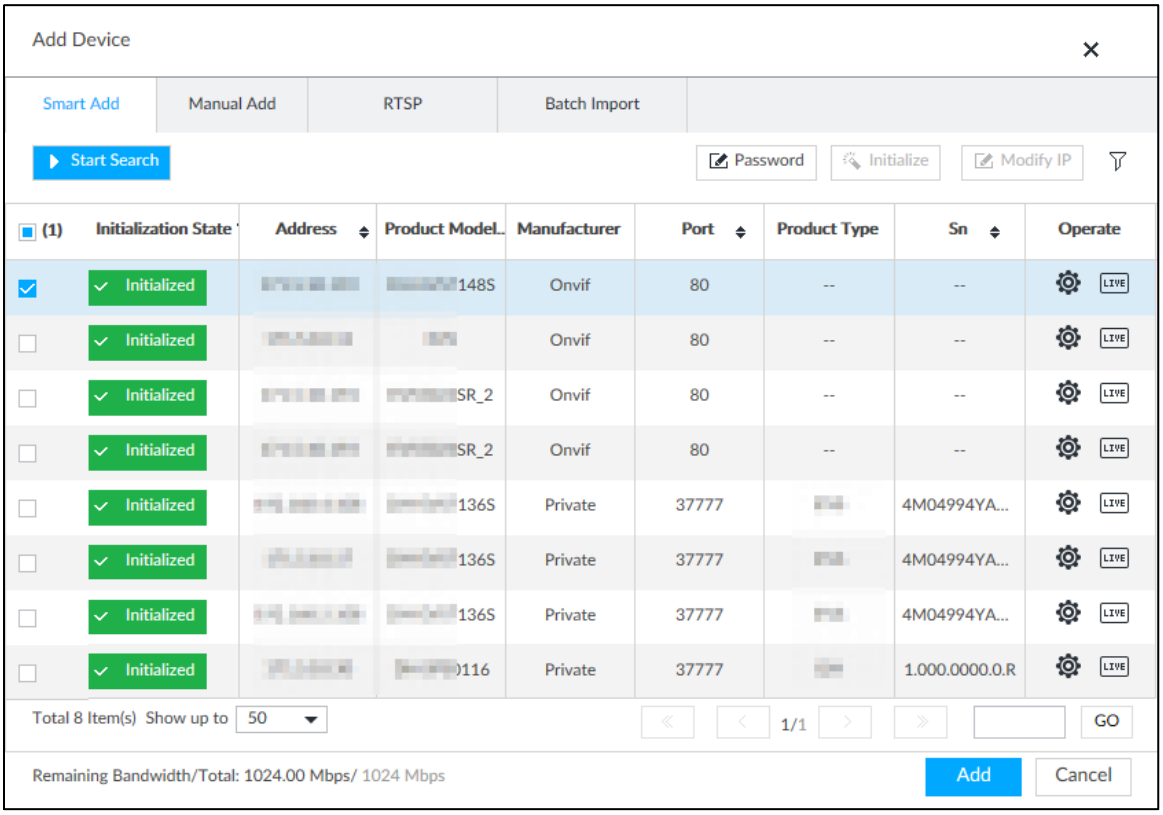
The **Smart Add** interface is displayed.

Step 3 Click **Start Search**.

System starts to search and displays result. See Figure 5-10.

Click ⚙ to set search criteria.

Figure 5-10 Remote device



Add Device ✕

Smart Add | Manual Add | RTSP | Batch Import

▶ Start Search   Password   Initialize   Modify IP

☑ (1)	Initialization State	Address	Product Model	Manufacturer	Port	Product Type	Sn	Operate
☑	✓ Initialized	[redacted]	[redacted]148S	Onvif	80	--	--	⚙ LIVE
□	✓ Initialized	[redacted]	[redacted]	Onvif	80	--	--	⚙ LIVE
□	✓ Initialized	[redacted]	[redacted]SR_2	Onvif	80	--	--	⚙ LIVE
□	✓ Initialized	[redacted]	[redacted]SR_2	Onvif	80	--	--	⚙ LIVE
□	✓ Initialized	[redacted]	[redacted]136S	Private	37777	[redacted]	4M04994YA...	⚙ LIVE
□	✓ Initialized	[redacted]	[redacted]136S	Private	37777	[redacted]	4M04994YA...	⚙ LIVE
□	✓ Initialized	[redacted]	[redacted]136S	Private	37777	[redacted]	4M04994YA...	⚙ LIVE
□	✓ Initialized	[redacted]	[redacted])116	Private	37777	[redacted]	1.000.0000.0.R	⚙ LIVE

Total 8 Item(s) Show up to 50   1/1   GO

Remaining Bandwidth/Total: 1024.00 Mbps/ 1024 Mbps   Add   Cancel

Step 4 Set device username and password.

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

📖

If you do not enter device username and password, the system will try to add the device by using the username and password of the current IVSS.

Step 5 Click **Add**.

To add a multiple-channel remote device, select the channels that you want to add.

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

6 Intelligent Operation

In addition to the basic video monitoring functions, the Device can also provide a number of AI functions including face recognition, people counting, video metadata, ANPR, and IVS (behavior detections such as fence-crossing, intrusion, loitering, crowd gathering, parking and more. See "6.6 IVS").

This chapter introduces how to configure the AI functions respectively.

The AI detections can be done by camera (AI by camera) or by IVSS (AI by device).

- AI by camera: When configuring an intelligent detection, if you select AI by camera, the intelligent analysis job is completed on the camera, and IVSS just receives and processes the results.
- AI by device: When configuring an intelligent detection, if you select AI by device, the camera uploads video and snapshots, and then IVSS is responsible for the video analysis job.

🕮

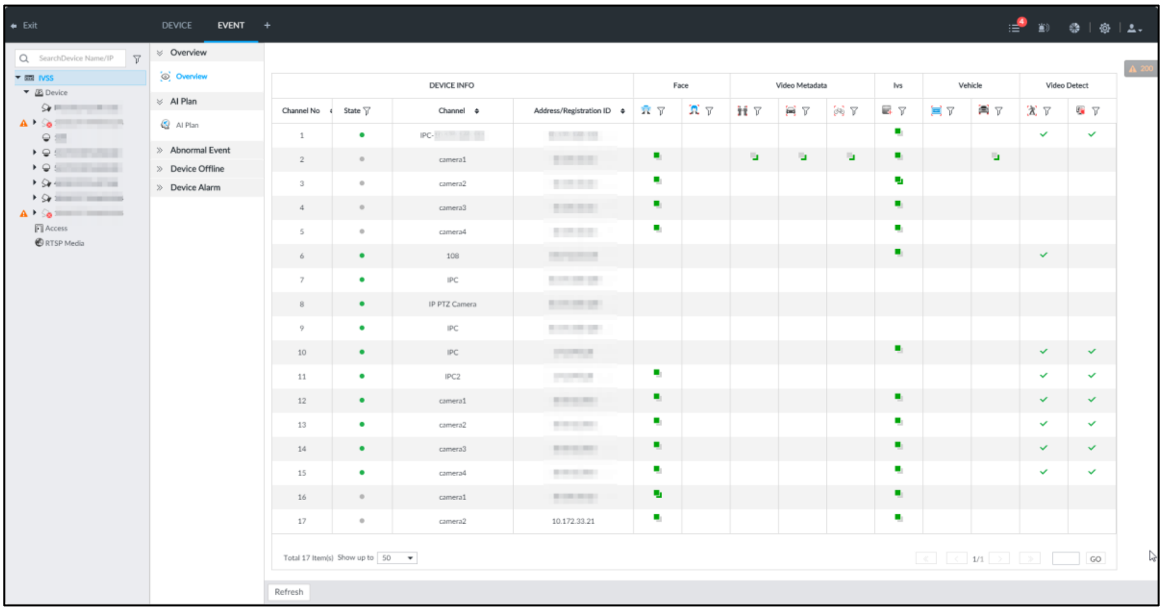
- The AI functions might vary depending on the Device function capability. The actual interface shall prevail.
- When AI by camera is enabled, complete AI detection configuration at remote device. See remote device user’s manual.
- The **AI by Camera** tab does not appear if the current camera does not support this function. The actual interface shall prevail.
- Some AI features are conflicting. Do not enable conflicting AI features at the same time.

6.1 Overview

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

Click ⚙ at the upper-right corner of the homepage to open the **Event** interface. The **Overview** interface is displayed by default, which shows the usage status of the AI functions of all remote devices. See Figure 6-1.

Figure 6-1 Overview



DEVICE INFO				Face		Video Metadata			Ivs	Vehicle		Video Detect	
Channel No	State	Channel	Address/Registration ID										
1	●	IPC-[redacted]	[redacted]						🟩			✓	✓
2	●	camera1	[redacted]	🟩		◪	◪	◪	🟩		◪		
3	●	camera2	[redacted]	🟩					🟩				
4	●	camera3	[redacted]	🟩					🟩				
5	●	camera4	[redacted]	🟩					🟩				
6	●	108	[redacted]						🟩			✓	
7	●	IPC	[redacted]										
8	●	IP PTZ Camera	[redacted]										
9	●	IPC	[redacted]										
10	●	IPC	[redacted]						🟩			✓	✓
11	●	IPC2	[redacted]	🟩								✓	✓
12	●	camera1	[redacted]	🟩					🟩			✓	✓
13	●	camera2	[redacted]	🟩					🟩			✓	✓
14	●	camera3	[redacted]	🟩					🟩			✓	✓
15	●	camera4	[redacted]	🟩					🟩			✓	✓
16	●	camera1	[redacted]	🟩					🟩				
17	●	camera2	10.172.33.21	🟩					🟩				

Total 17 Item(s) Show up to 50 1/1 GO

🟩 indicates that the AI function is enabled. ◪ indicates that AI by device is enabled.

6.2 Face Detection

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

6.2.1 Enabling AI Plan

To use AI by camera, you need to enable AI plan first.

- AI plan is available on select models.
- To use AI by camera, you need first enable the corresponding AI plan; otherwise the AI function does not work.
- The Device automatically shows the AI functions available on the connected cameras.

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

The **EVENT** interface is displayed.

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

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

The **AI Plan** interface is displayed. See Figure 6-2.

- The interface might vary depending on the function capabilities of cameras. The actual interface shall prevail.
- When the camera is a PTZ camera, configure presets on the camera system first, and then you can set AI features for each preset of the PTZ camera. See Figure 6-3.

Figure 6-2 AI plan(1)

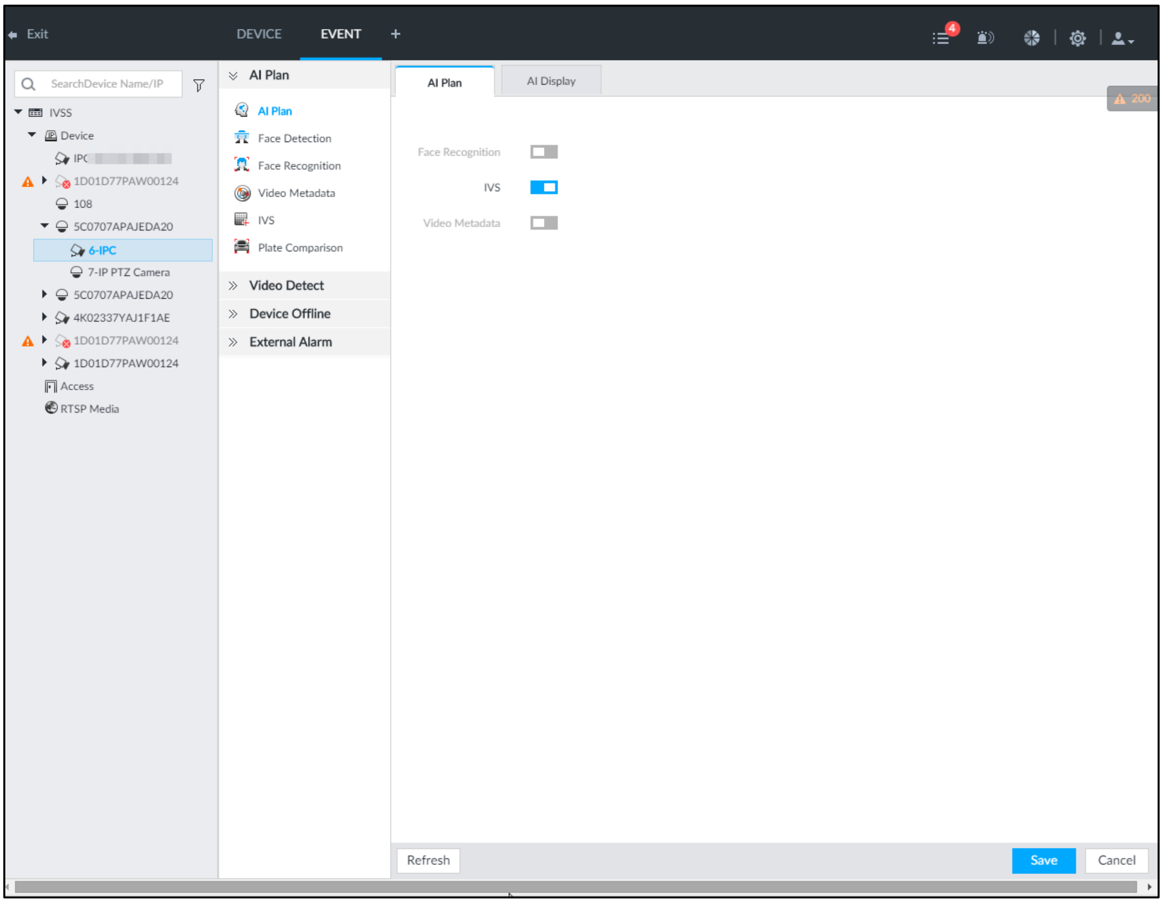
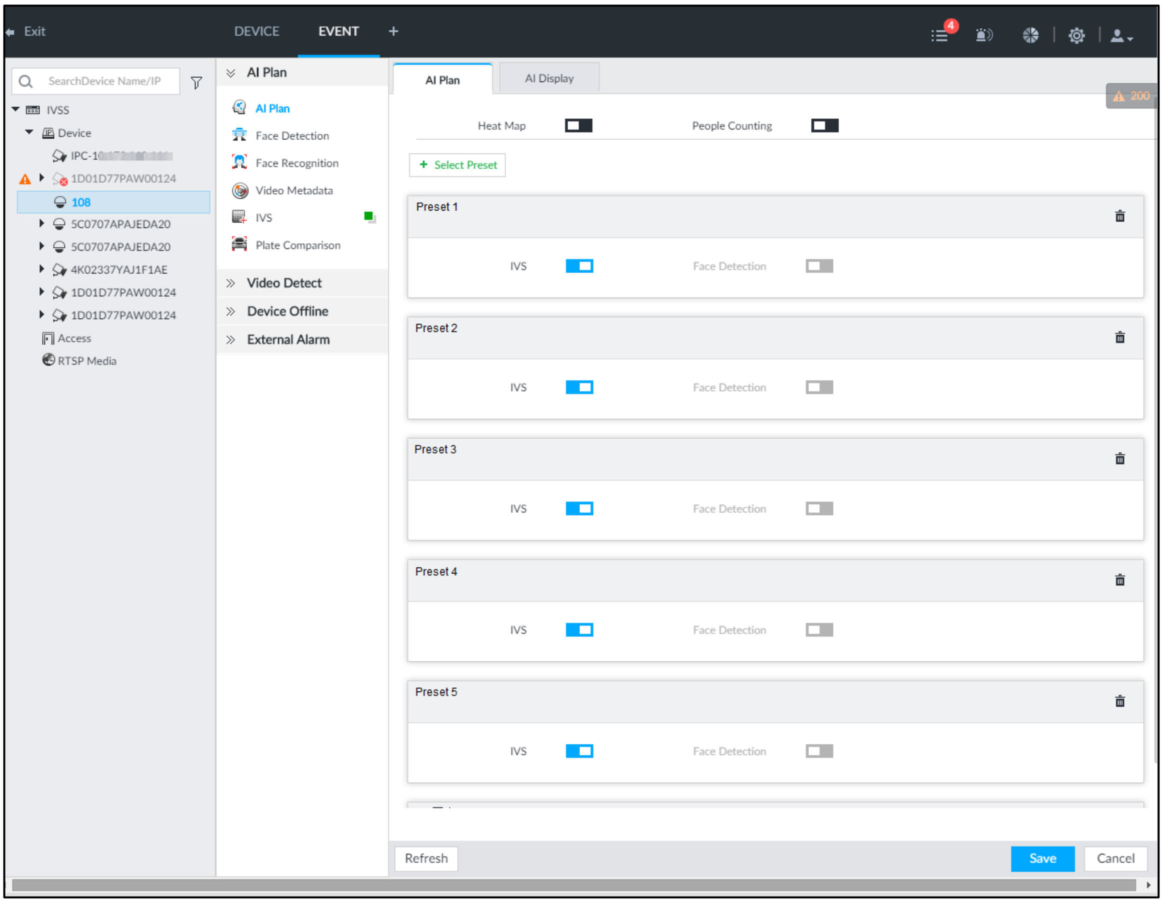


Figure 6-3 AI plan(2)



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

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

Step 5 Click **Save**.

6.2.2 Configuring Face Detection

Configure alarm rule of face detection.

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

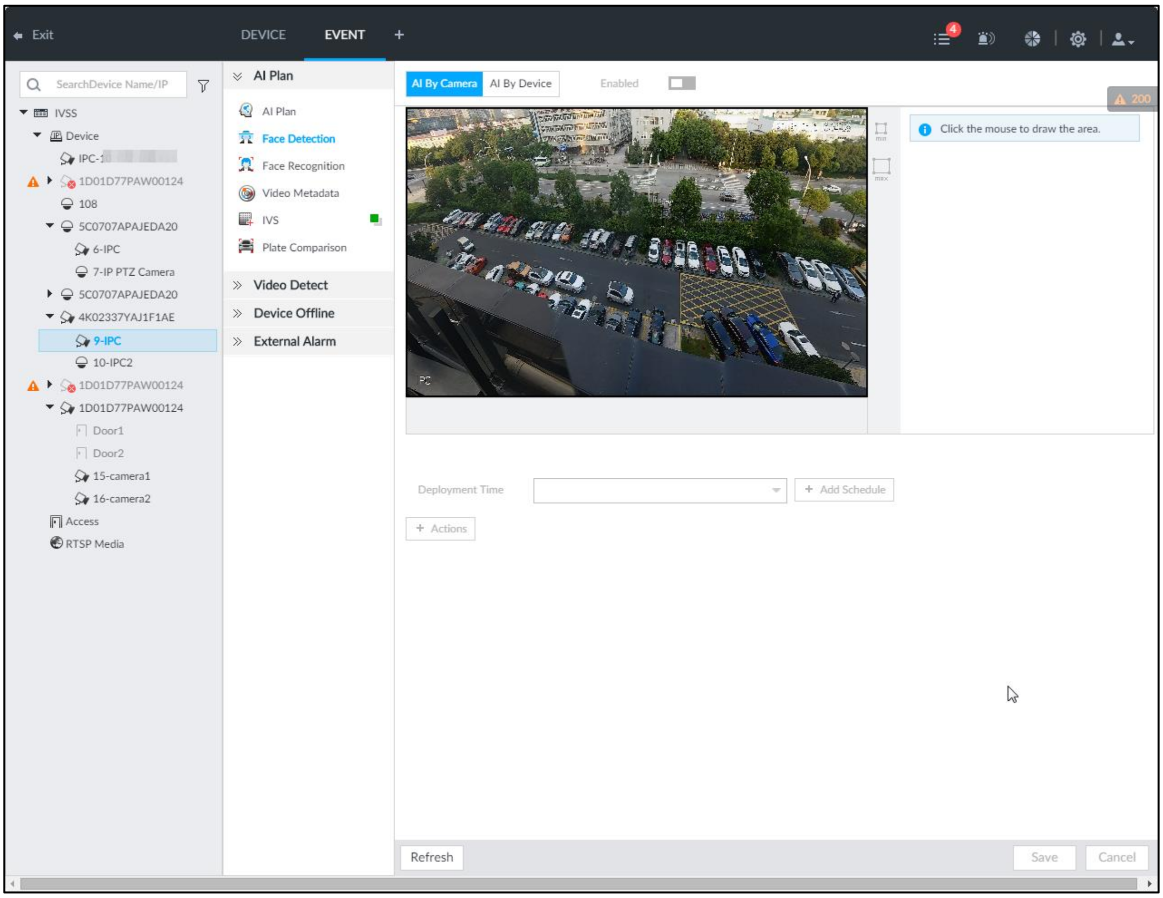
The **EVENT** interface is displayed.

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

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

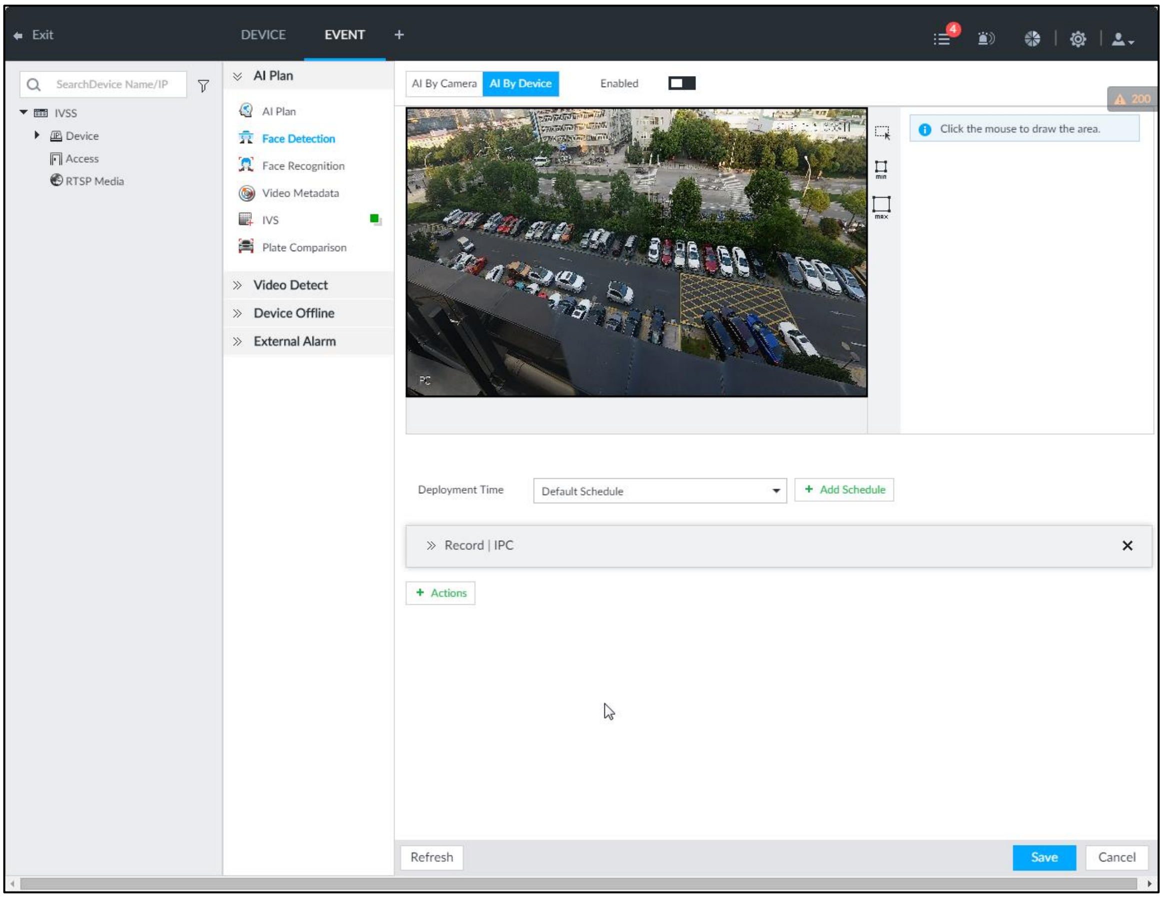
The **Face Detection** interface is displayed. See Figure 6-4 or Figure 6-5.

Figure 6-4 AI by camera



Click the mouse to draw the area.

Figure 6-5 AI by device



Enabled

Click the mouse to draw the area.

Deployment Time: Default Schedule

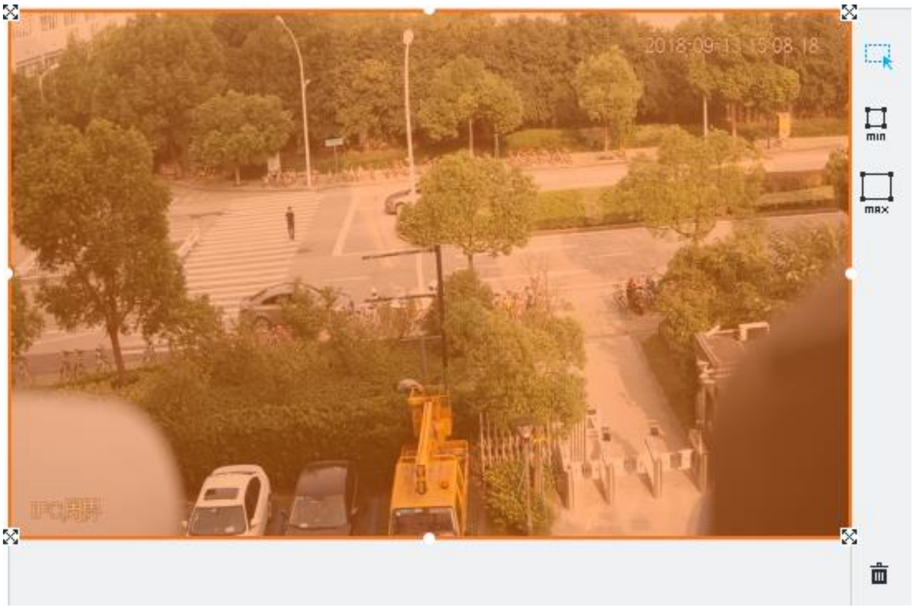
Record | IPC

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

AI by camera supports **Face RoI** function. After enabling **Face RoI** function, system displays enhanced human face zone on the surveillance window.

Step 5 Set detection region on the video (yellow area). See Figure 6-6.

Figure 6-6 Area



- Click or white dot on detect region frame, and drag to adjust its range.

- Click or to set the minimum size or maximum size of the face detection area. System triggers an alarm once the size of detected target is between the maximum size and the minimum size.

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

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

Step 7 Click **Action** to set alarm action. For details, see *User's Manual*.

Step 8 Click **Save**.

6.2.3 Live View of Face Detection

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

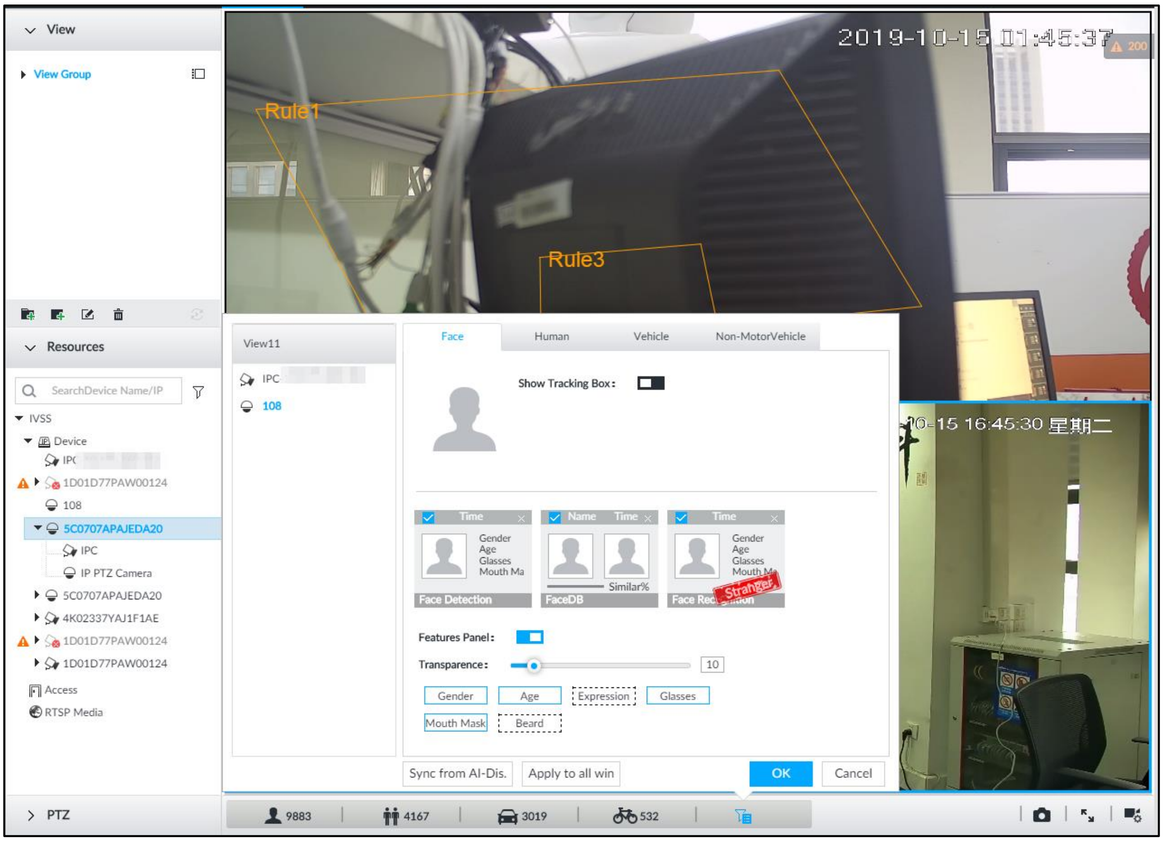
6.2.3.1 Setting AI Display

You can configure display rule of face detection results.

Step 1 On the **LIVE** interface, open a view, click , and then select the **Face** tab.

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

Figure 6-7 Face



Step 2 Enable **Show Tracking Box** and **Features Panel**, and then select feature(s) you want to display. For details, see *User's Manual*.

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

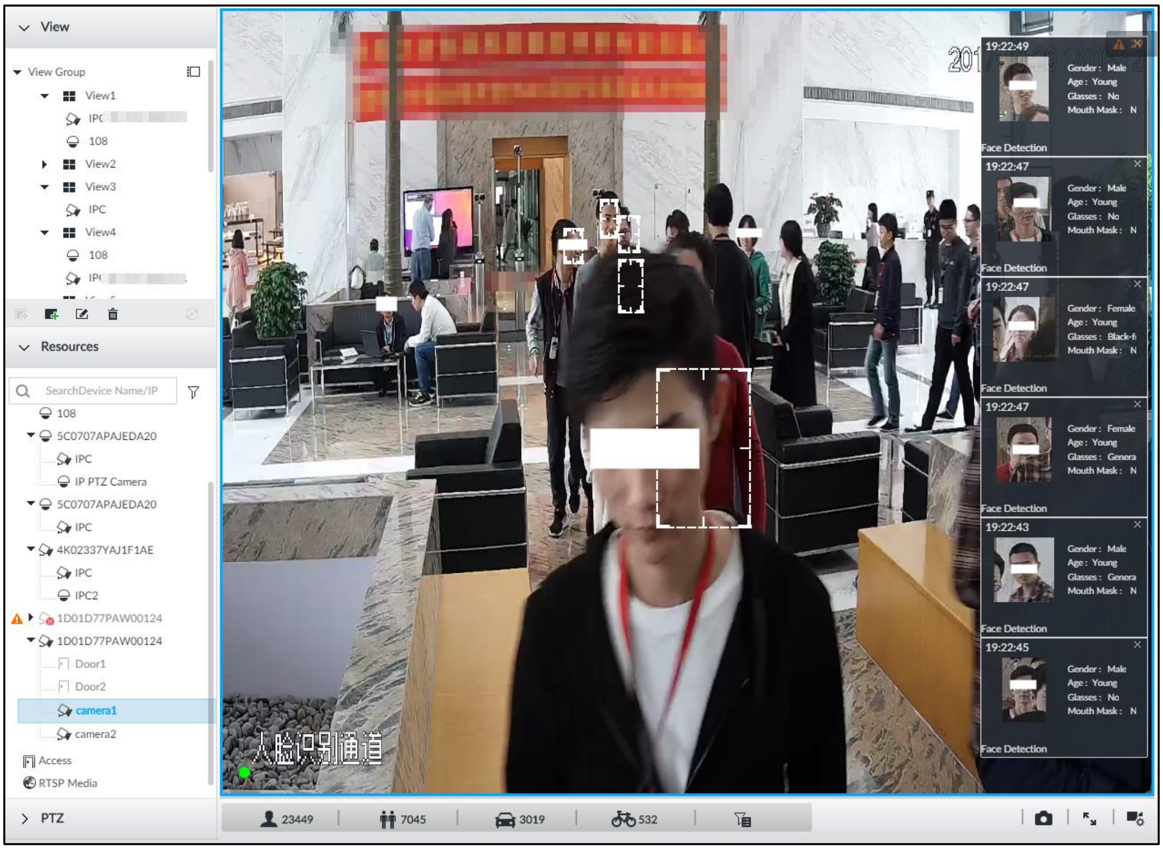
6.2.3.2 Live View

Go to the **LIVE** interface, enable view, and then view videos are displayed. See Figure 6-8.

- The view window displays currently detected face rule boxes.
- Features panels are displayed on the right side in real time.

  The features panel displays detection time, face snapshot and face features details.

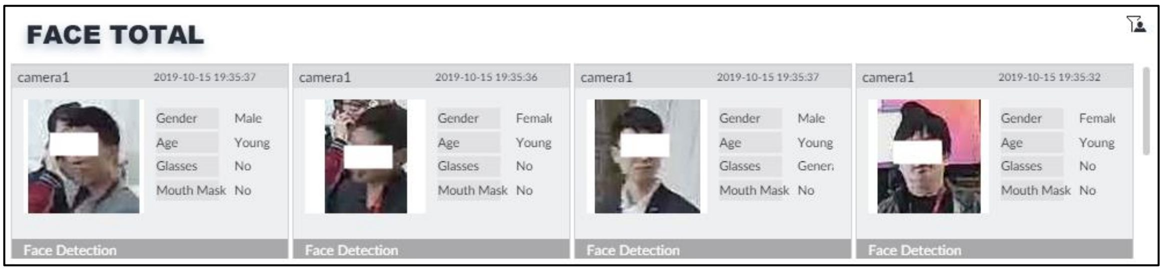
Figure 6-8 Live



6.2.3.3 Face Records

On the **LIVE** interface, click . The **FACE TOTAL** interface is displayed. Click , and then select **Face Detection**. The latest face detection records are displayed. See Figure 6-9.

Figure 6-9 Detection image



FACE TOTAL

camera1 2019-10-15 19:35:37

Gender	Male
Age	Young
Glasses	No
Mouth Mask	No

Face Detection

camera1 2019-10-15 19:35:36

Gender	Femal
Age	Young
Glasses	No
Mouth Mask	No

Face Detection

camera1 2019-10-15 19:35:37

Gender	Male
Age	Young
Glasses	Gener
Mouth Mask	No

Face Detection

camera1 2019-10-15 19:35:32

Gender	Femal
Age	Young
Glasses	No
Mouth Mask	No

Face Detection

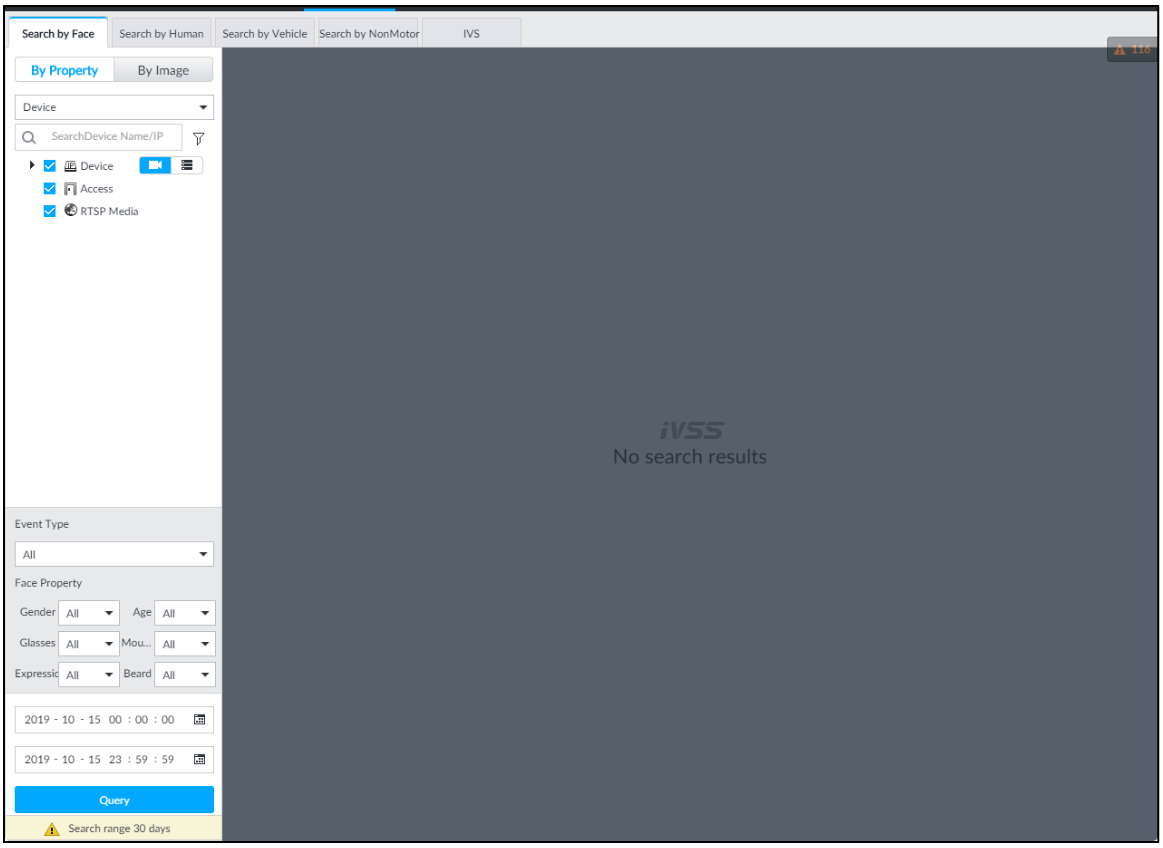
6.2.4 Face Search

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

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

The **By Property** interface is displayed. See Figure 6-10.

Figure 6-10 Search by property



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

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

Step 3 Set face property and time.

Step 4 Click **Query**.

The search results are displayed.

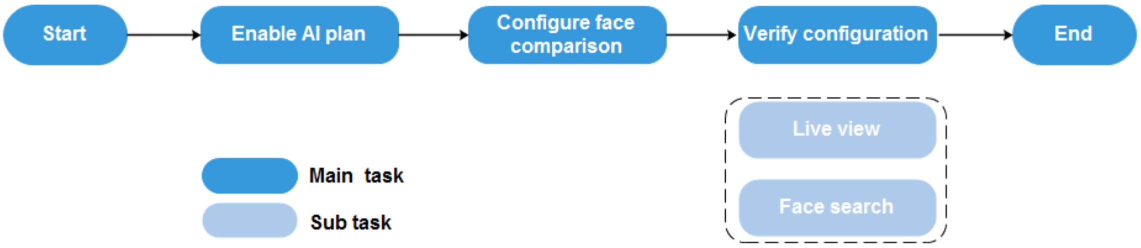
You can also search for face records by uploading a face image. For details, see *User's Manual*.

6.3 Face Recognition

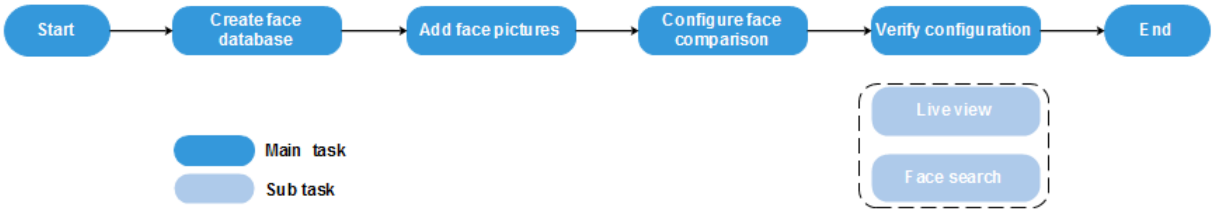
The system compares captured face with the face database and works out the similarity. When the similarity reaches the threshold as you have defined, an alarm will be triggered.

6.3.1 Configuration Procedure

Figure 6-11 Face recognition procedure (AI by camera)



Face recognition procedure (AI by device)



6.3.2 Enabling AI Plan

To use AI by camera, you need to enable the corresponding AI plan first. For details, see "6.2.1 Enabling AI Plan."

6.3.3 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 recognition, human face search, and so on.

6.3.3.1 Creating Face Database

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

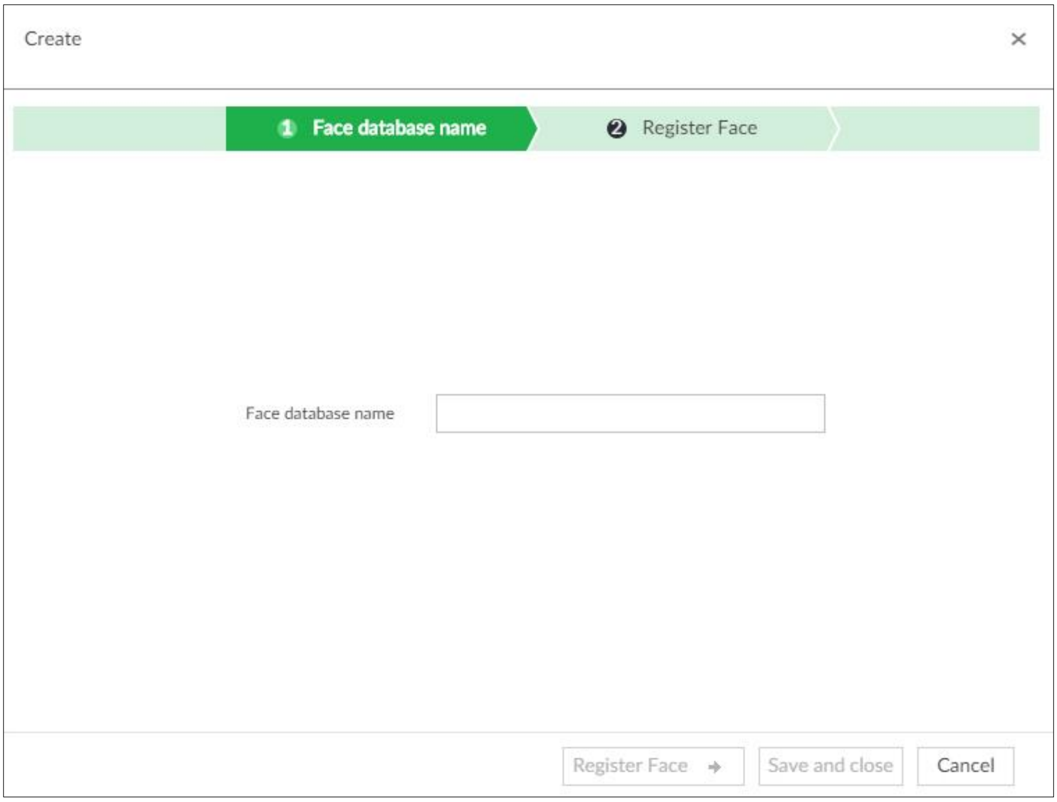
Step 1 On the **LIVE** interface, click +, select **FILE** > **Face Management** > **Face Database**.

The **Face Database** interface is displayed.

Step 2 Click **Create**.

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

Figure 6-12 Create face database


Create

Face database name

Step 3 Set face database name.

Step 4 Click **Save and close**.

6.3.3.2 Adding Face Image

Add face images to the created face database in the way of manual add, batch import or detection. This section takes batch import as an example. For details about manual add or adding from detection results, see *User's Manual*.

📖

- Make sure that 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 PCAPP is located.
- 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 *User's Manual*.

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

Face Database interface is displayed.

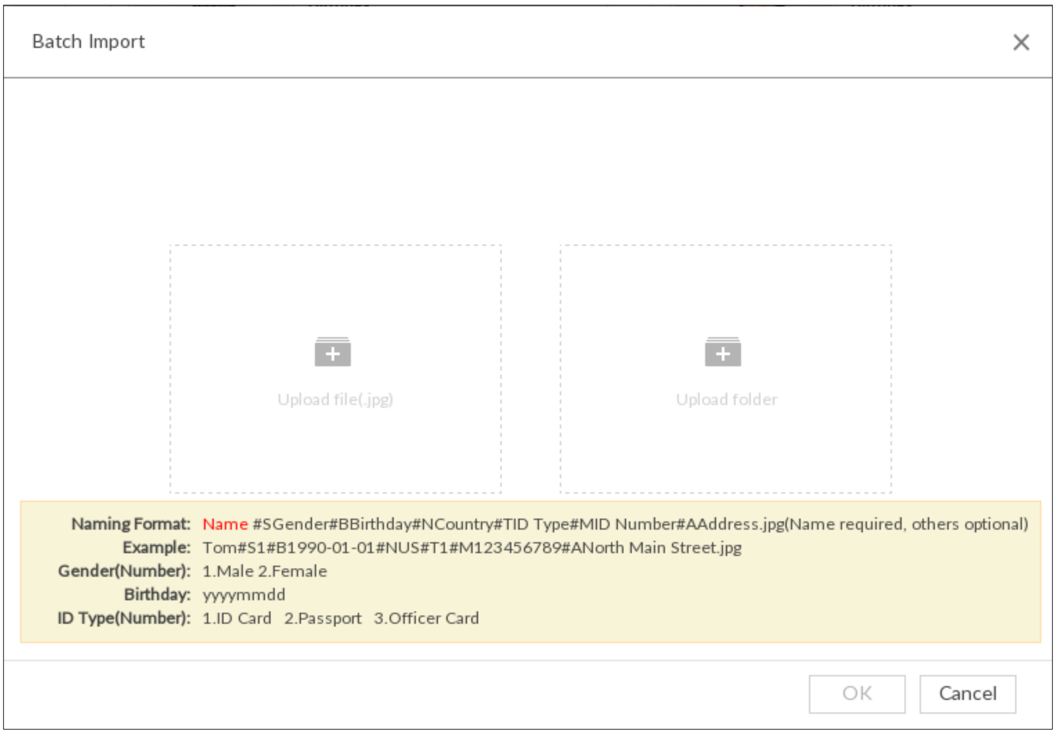
Step 2 Double-click face database.

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



Naming Format: Name #SGender#BBirthday#NCountry#TID Type#MID Number#AAddress.jpg(Name required, others optional)
Example: Tom#S1#B1990-01-01#NUS#T1#M123456789#ANorth Main Street.jpg
Gender(Number): 1.Male 2.Female
Birthday: yyyymmdd
ID Type(Number): 1.ID Card 2.Passport 3.Officer Card

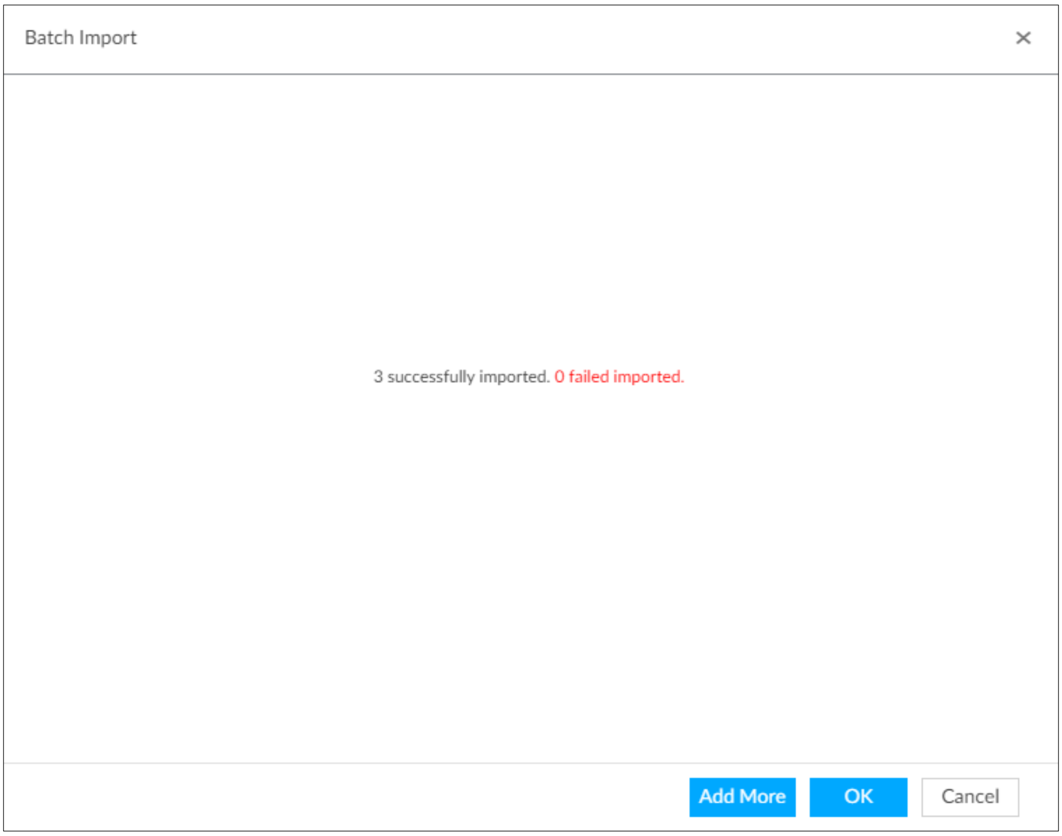
Step 4 Import face image.

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

Step 5 Click **OK**.

The batch import result interface is displayed. See Figure 6-14.

Figure 6-14 Batch import



3 successfully imported. 0 failed imported.

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

After adding the image, at the lower-left corner of the face image, the icon ⟳ appears, which indicates that face information is being processed. For details, see *User's Manual*.

6.3.4 Configuring Face Recognition

Configure face recognition rules.

To use AI by device, enable face detection first. For details, see "6.2.2 Configuring Face Detection."

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

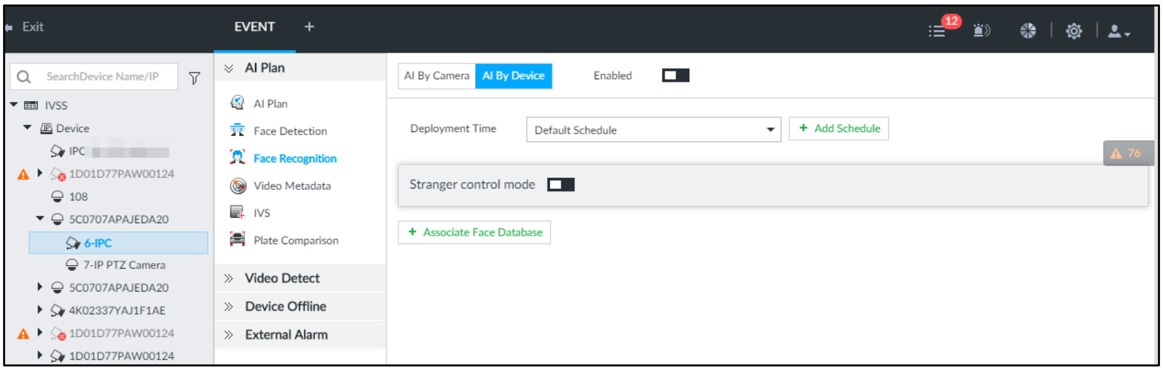
The **EVENT** interface is displayed.

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

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

The **Face Recognition** interface is displayed. See Figure 6-15.

Figure 6-15 Face recognition (AI by Device)



Enabled ▭

Deployment Time: Default Schedule

Stranger control mode ▭

Step 4 Click ▭ to enable face recognition.

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

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

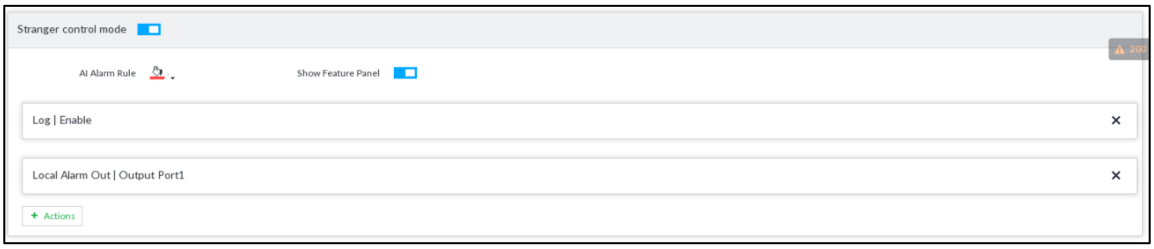
Step 6 Set stranger mode.

Enable stranger mode. Once the face recognition 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 6-16.

Figure 6-16 Stranger control mode



Stranger control mode ▣

Show Feature Panel ▣

Log | Enable ×

Local Alarm Out | Output Port1 ×

2) Set AI alarm rule, and then enable **Show feature panel**.

When **Show feature panel** is enabled, system displays stranger panel once there is an alarm.

3) Click **Actions** to set alarm actions. For details, see *User's Manual*.

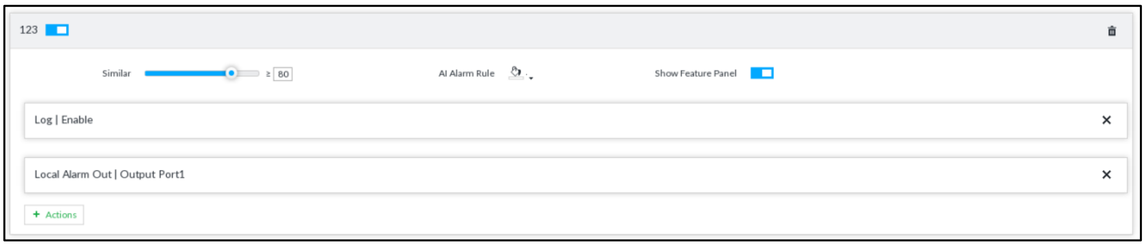
Step 7 Set linked face database.

- Before you use AI by camera function, go to the remote device to set face database. On 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 6-17.

Figure 6-17 Face database configuration



123

Similar ≥ 80

AI Alarm Rule

Show Feature Panel

Log | Enable

Local Alarm Out | Output Port1

+ Actions

2) Set similarity.

   System compares the human face with the image on the face database. System triggers an alarm once the similarity reaches the threshold you set here.

3) Set AI alarm rule, and then enable **Show feature panel**.

4) Click **Actions** to set alarm actions. For details, see *User's Manual*.

Step 8 Click **Save**.

6.3.5 Live View of Face Recognition

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

6.3.5.1 Setting AI Display

You can configure display rule of AI detection results.

Before using this function, ensure that view has been created. For details, see *User's Manual*.

On the **LIVE** interface, open a view window, click , and then select the **Face** tab. Enable **Show Tracking Box** and **Features Panel**, and then select the feature(s) you want to display. For details, see "6.2.3.1 Setting AI Display."

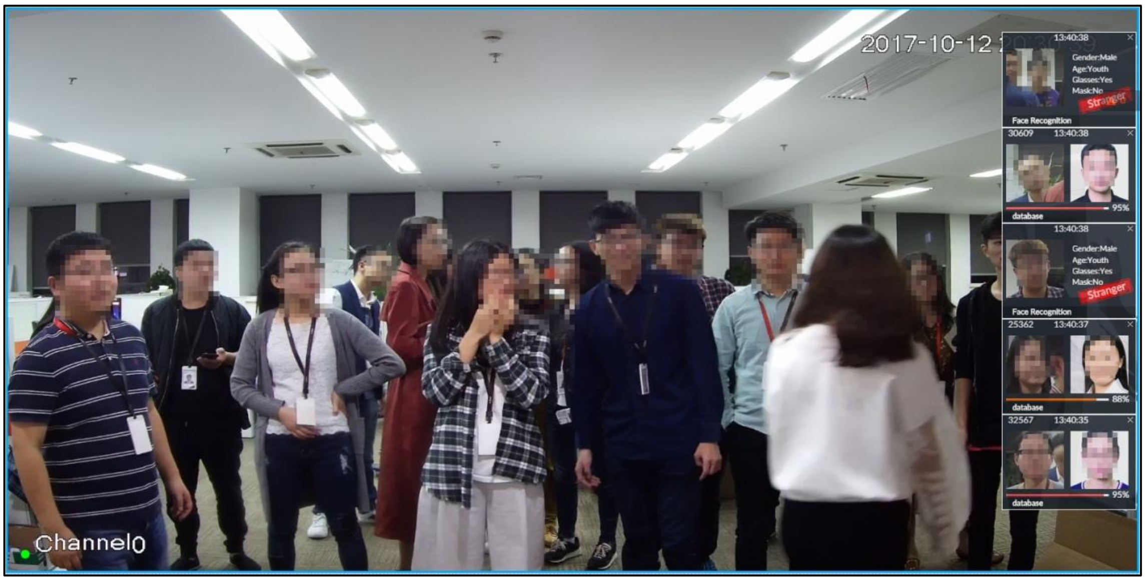
6.3.5.2 Live View

Go to the **LIVE** interface, enable view, and then device displays view video. See Figure 6-8.

- 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 recognition, 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 6-18 Live



13:40:38
Gender:Male
Age:Youth
Glasses:Yes
Mask:No
Stranger
Face Recognition

30609 13:40:38
95%
database

13:40:38
Gender:Male
Age:Youth
Glasses:Yes
Mask:No
Stranger
Face Recognition

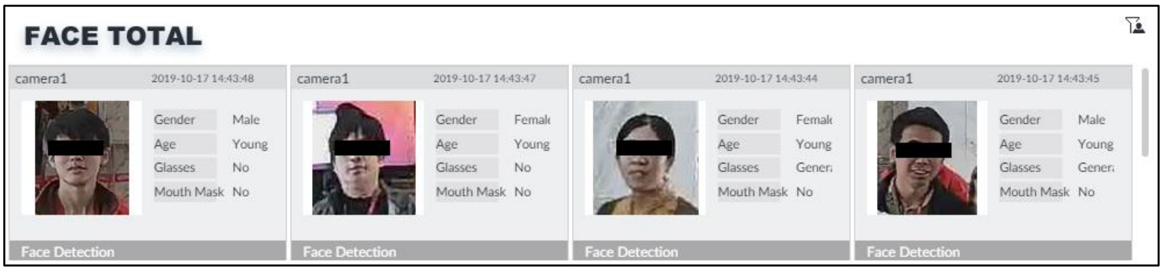
25362 13:40:37
88%
database

32567 13:40:35
95%
database

6.3.5.3 Face Total

On the **LIVE** interface, click . Face detection panel is displayed. See Figure 6-19.

Figure 6-19 Detection image



FACE TOTAL

camera1 2019-10-17 14:43:48
Gender Male
Age Young
Glasses No
Mouth Mask No
Face Detection

camera1 2019-10-17 14:43:47
Gender Femal
Age Young
Glasses No
Mouth Mask No
Face Detection

camera1 2019-10-17 14:43:44
Gender Femal
Age Young
Glasses Gener
Mouth Mask No
Face Detection

camera1 2019-10-17 14:43:45
Gender Male
Age Young
Glasses Gener
Mouth Mask No
Face Detection

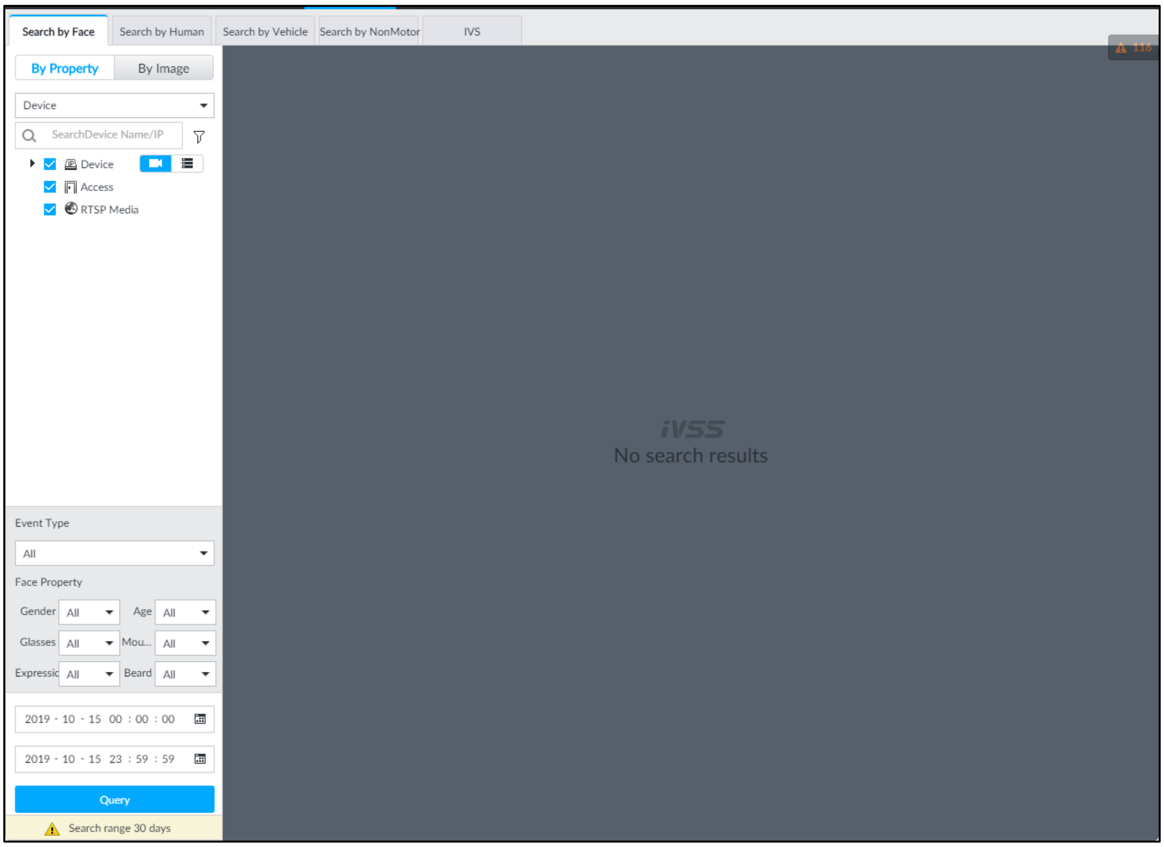
6.3.6 Face Search

Search for face detection information, including face detection image, record and features. You can search by face property, or by uploading a face image. This section takes search by property as an example. For search by image, see *User's Manual*.

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

The **By Property** interface is displayed. See Figure 6-20.

Figure 6-20 Search by property



No search results

Search range 30 days

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

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

Step 3 Set face property and time.

Step 4 Click **Query**.

The search results are displayed.

6.4 People Counting

This section introduces the statistics of in-area people number, and queuing number.

The people counting function is only available with AI by camera. Make sure that the camera has been configured with people counting rules.

6.4.1 Enabling AI Plan

To use AI by camera, you need first enable the corresponding AI plan; otherwise the AI function does not work. For details, see "6.2.1 Enabling AI Plan."

6.4.2 People Counting

The system counts the number of people in and out of the detection area. When the statistical number exceeds the threshold, or the average dwell time is longer than the threshold time, an alarm is triggered.

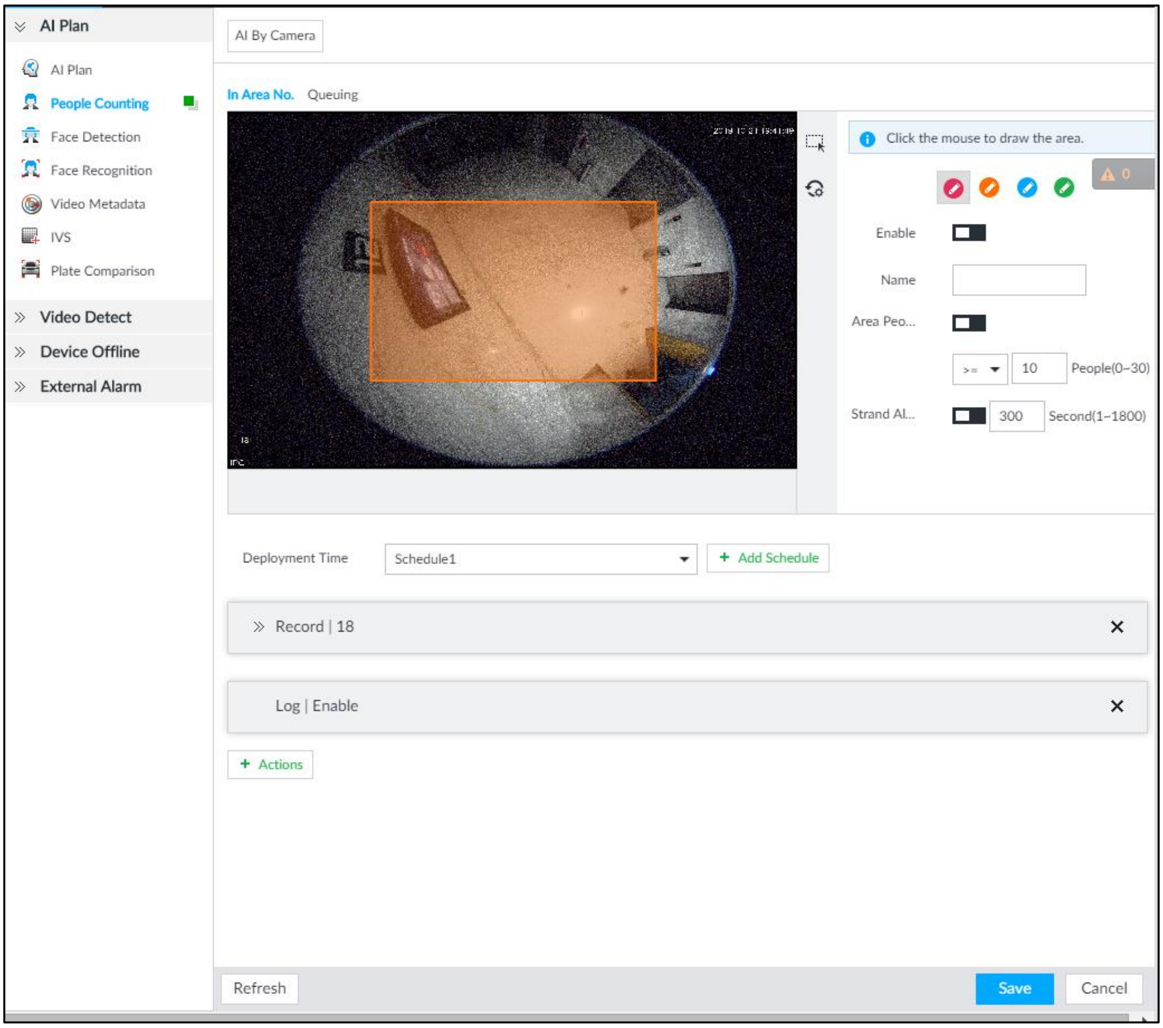
Step 1 Click ⚙, click +, and then select **EVENT**.

The **EVENT** interface is displayed.

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

The **In Area No.** interface is displayed. See Figure 6-21.

Figure 6-21 In Area No.



Enable

Name

Area Peo...

>= 10 People(0~30)

Strand Al... 300 Second(1~1800)

Deployment Time Schedule1

Record | 18

Log | Enable

Step 3 Draw a people counting area.

1) Click ✎ to draw the first detection area.

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

2) Click ⬚ to edit the area.

◇ Click and drag ⤧ to adjust the position and length.

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

◇ Click to restore to the default area.

Step 4 Set parameters. See Table 6-1.

Table 6-1 Parameters description of people counting

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

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

Alarms are triggered only within the scheduled time.

Step 6 Click **Actions** to set alarm linkage actions. For details, see *User's Manual*.

Step 7 Click **Save**.

6.4.3 Queuing Detection

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

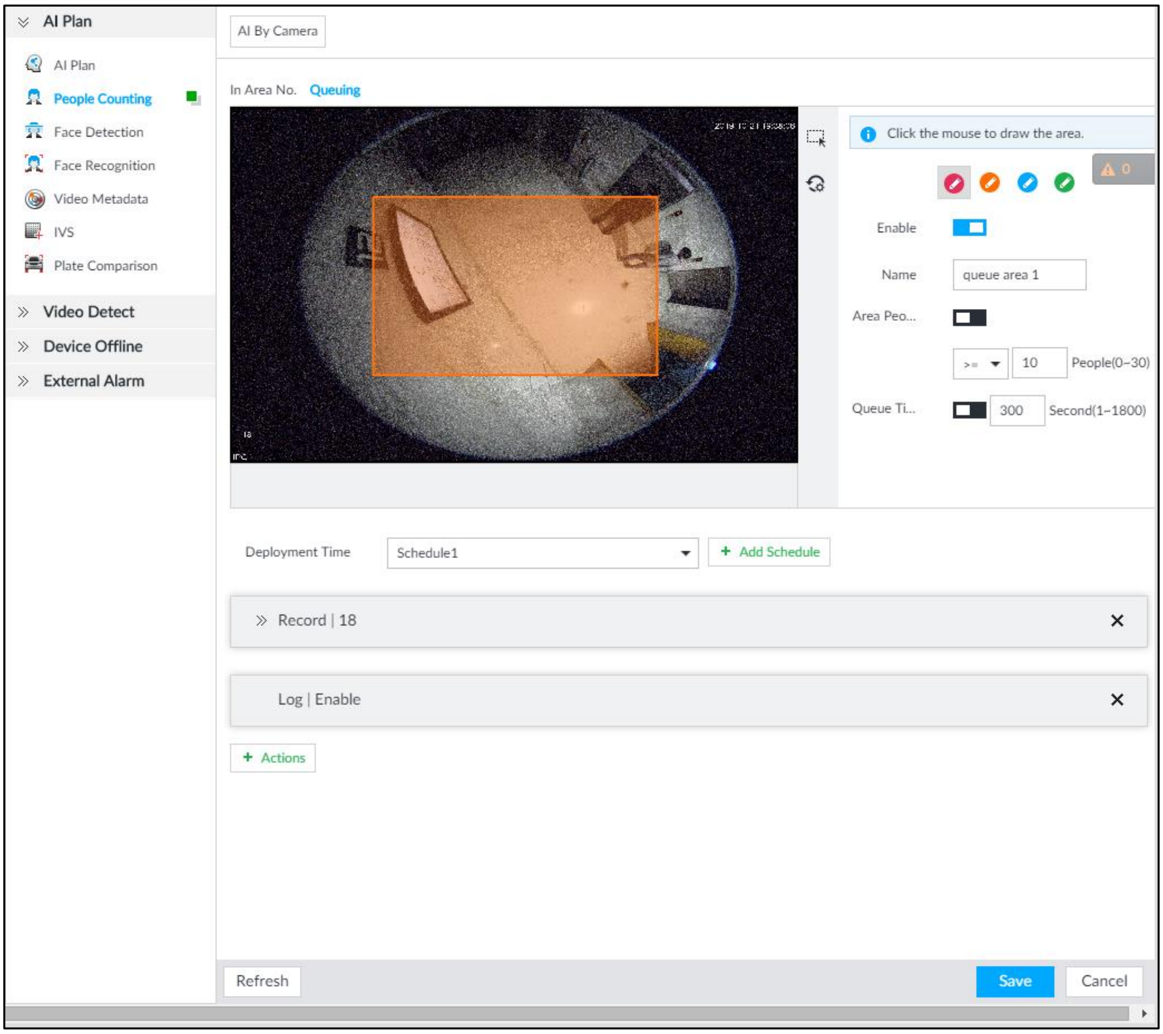
Step 1 Click ⚙, click +, and then select **EVENT**.

The **EVENT** interface is displayed.

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

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

Figure 6-22 Queuing



In Area No. Queuing

Click the mouse to draw the area.

Enable	■	
Name	queue area 1	
Area Peo...	□	
	>= 10	People(0~30)
Queue Ti...	□ 300	Second(1~1800)

Deployment Time: Schedule1

Record | 18

Log | Enable

Step 3 Draw a queuing detection area.

1) Click ✎ to draw the first detection area.

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

2) Click ⬚ to edit the area.

◇ Click and drag ⤧ to adjust the position and length.

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

◇ Click ⟳ to restore to the default area.

Step 4 Set parameters. See Table 6-2.

Table 6-2 Parameters description of queuing detection

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

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

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

Alarms are triggered only within the scheduled time.

Step 6 Click **Actions** to set alarm linkage actions. For details, see *User's Manual*.

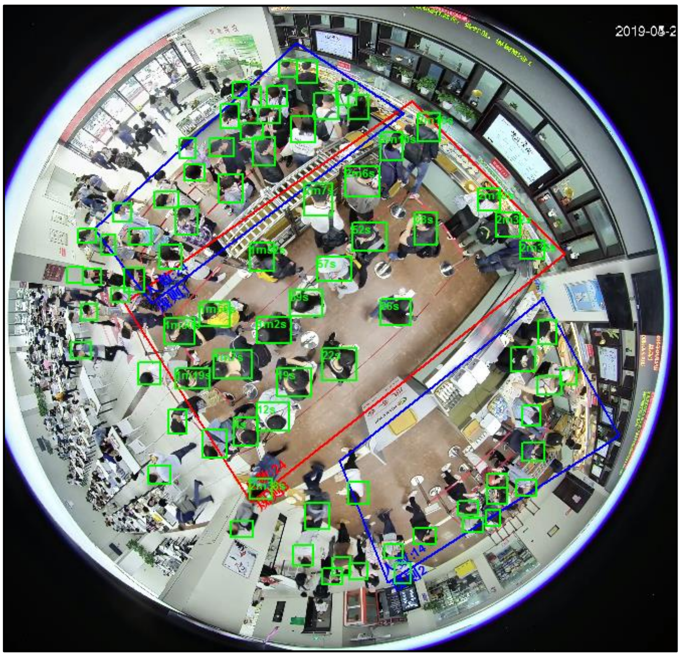
Step 7 Click **Save**.

6.4.4 Live View

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

The live video which shows real-time people number and queuing time is displayed. See Figure 6-23.

Figure 6-23 Live view



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

6.5 Video Metadata

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

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

6.5.1 Enabling AI Plan

You need to enable AI plan when AI by camera is used. For details, see "6.2.1 Enabling AI Plan."

6.5.2 Configuring Video Metadata

After enabling and then configuring video metadata, 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.

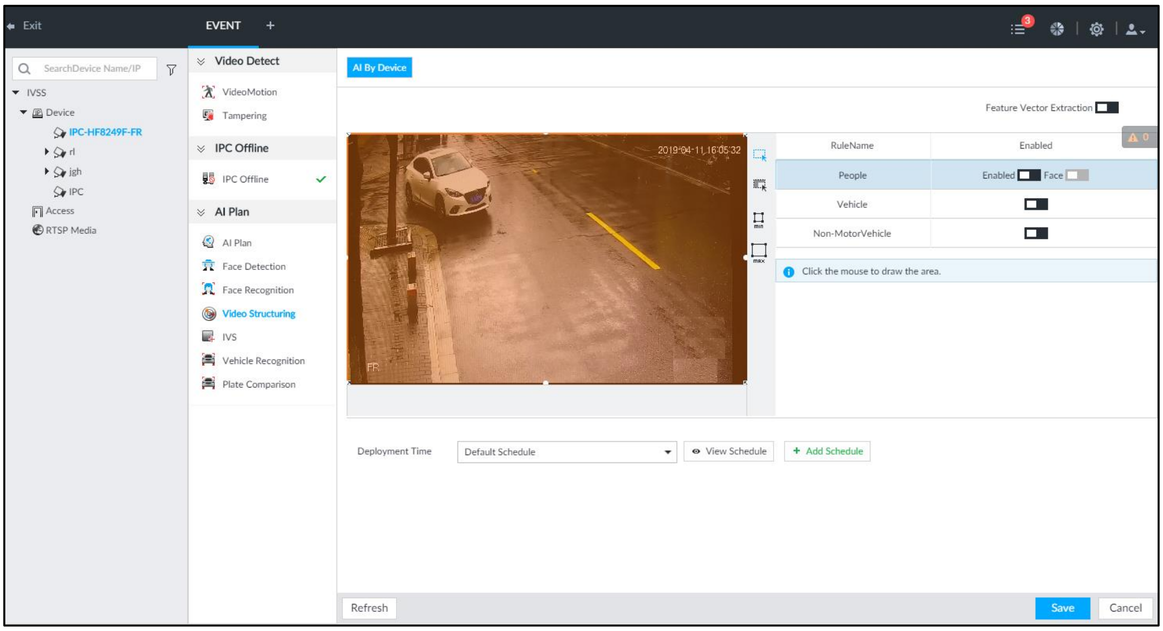
Step 1 Click ⚙ or ＋, and then select **EVENT**.

The **EVENT** interface is displayed.

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

Step 3 Select **AI Plan > Video Metadata > AI By Device**.
The **AI By Device** interface is displayed. See Figure 6-24.

Figure 6-24 AI by device



Feature Vector Extraction

RuleName	Enabled
People	Enabled Face
Vehicle	
Non-MotorVehicle	

Click the mouse to draw the area.

Deployment Time: Default Schedule ▾ | View Schedule | + Add Schedule

Step 4 Click ▭ next to **Feature Vector Extraction** to enable feature extraction, and then IVSS can extract features of human, vehicles and non-motor vehicles and display them on the live view. The search by image function is available only when feature vector extraction 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.

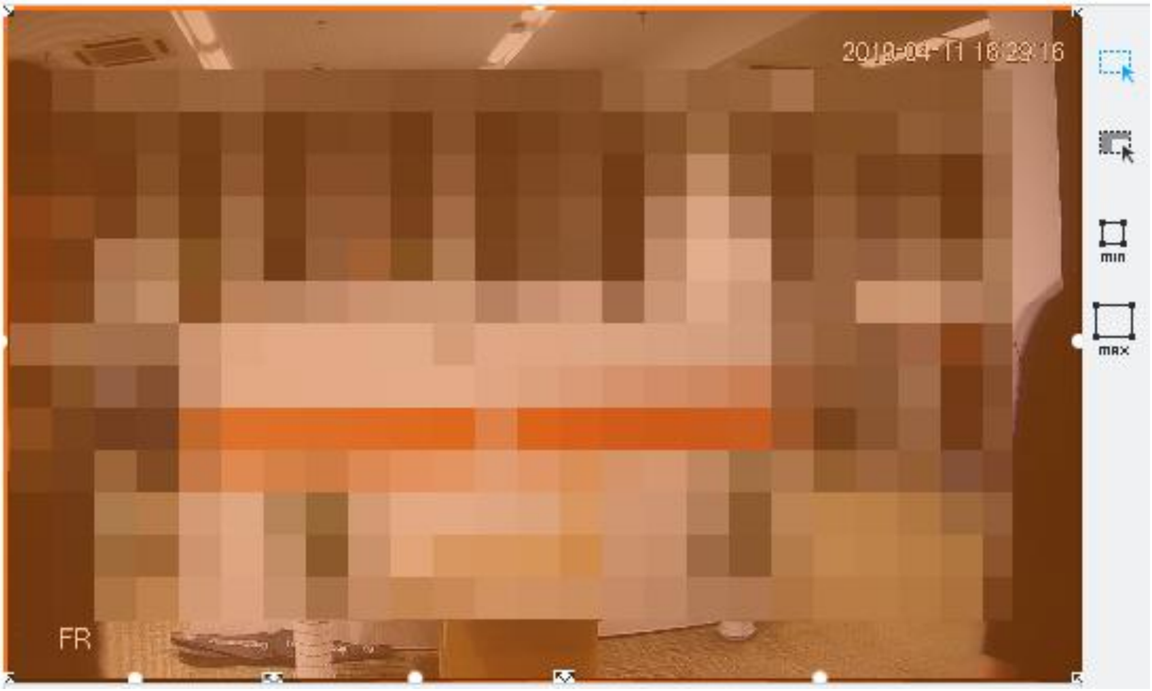
- Vehicle: Click corresponding to enable vehicle detection.
- Non-Motor Vehicle: Click corresponding to enable non-motor vehicle detection.

Step 6 Click (the icon changes to), and then you can configure detection area (orange) in the video image. See Figure 6-25.

The detection region can be set only when AI by device is enabled.

- 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 the face detection area. System triggers an alarm once the size of detected target is between the maximum size and the minimum size.

Figure 6-25 Detection area



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

Step 8 Click **Save**.

6.5.3 Live View of Video Metadata

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

6.5.3.1 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.

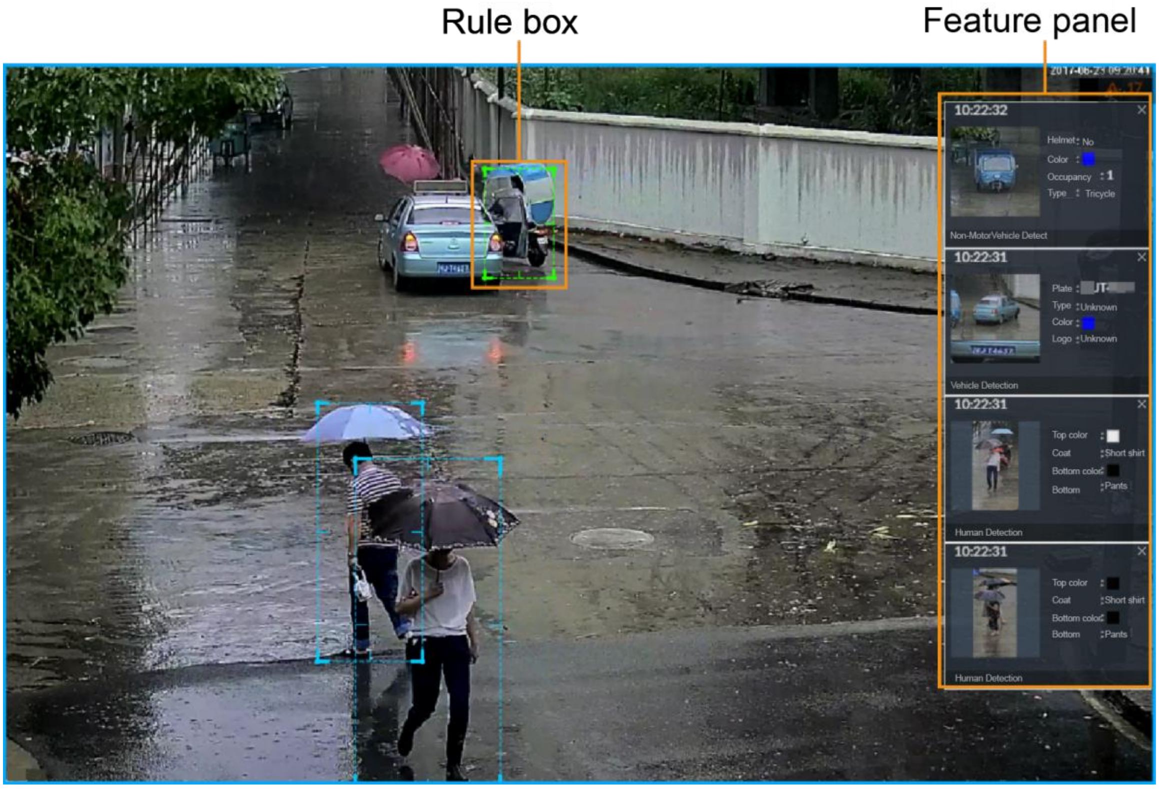
On the **Live** interface, after opening a view, click at the bottom of the **LIVE** interface, and then select **Human**, **Face**, **Vehicle** or **Non-Motor Vehicle**. Enable **Show Tracking Box** and **Features Panel**, and then select the features you need to display on the live view. For details, see "6.2.3.1 Setting AI Display."

6.5.3.2 Live View

On the **LIVE** interface, select a view from **View Group**, and the video image of the view will be displayed. See Figure 6-26.

- 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 6-26 Live



10:22:32
Helmet : No
Color :
Occupancy : 1
Type : Tricycle
Non-MotorVehicle Detect

10:22:31
Plate : [redacted]
Type : Unknown
Color :
Logo : Unknown
Vehicle Detection

10:22:31
Top color :
Coat : Short shirt
Bottom color :
Bottom : Pants
Human Detection

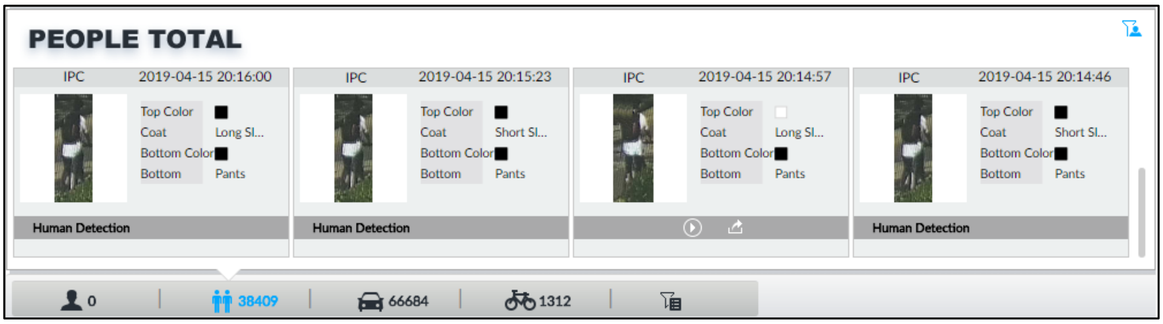
10:22:31
Top color :
Coat : Short shirt
Bottom color :
Bottom : Pants
Human Detection

6.5.3.3 Detection statistics

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

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 6-27.

Figure 6-27 Human detection



PEOPLE TOTAL

IPC 2019-04-15 20:16:00
Top Color ■
Coat Long Sl...
Bottom Color ■
Bottom Pants
Human Detection

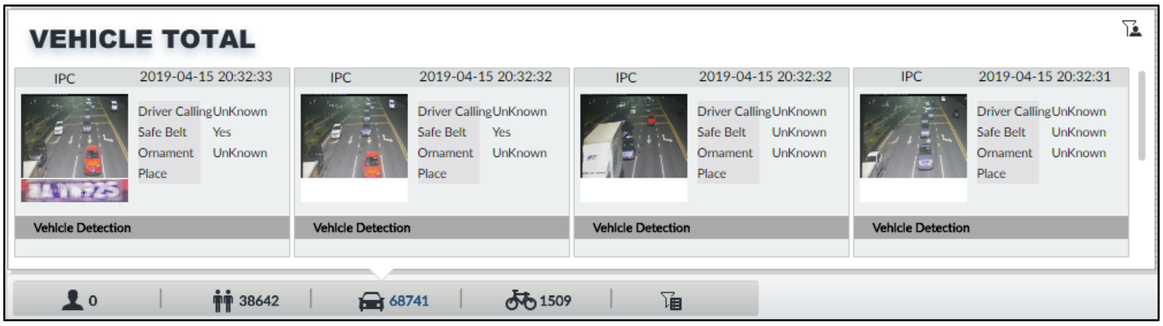
IPC 2019-04-15 20:15:23
Top Color ■
Coat Short Sl...
Bottom Color ■
Bottom Pants
Human Detection

IPC 2019-04-15 20:14:57
Top Color □
Coat Long Sl...
Bottom Color ■
Bottom Pants

IPC 2019-04-15 20:14:46
Top Color ■
Coat Short Sl...
Bottom Color ■
Bottom Pants
Human Detection

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 6-28.

Figure 6-28 Motor vehicle detection



VEHICLE TOTAL

IPC 2019-04-15 20:32:33
Driver Calling UnKnown
Safe Belt Yes
Ornament UnKnown
Place
Vehicle Detection

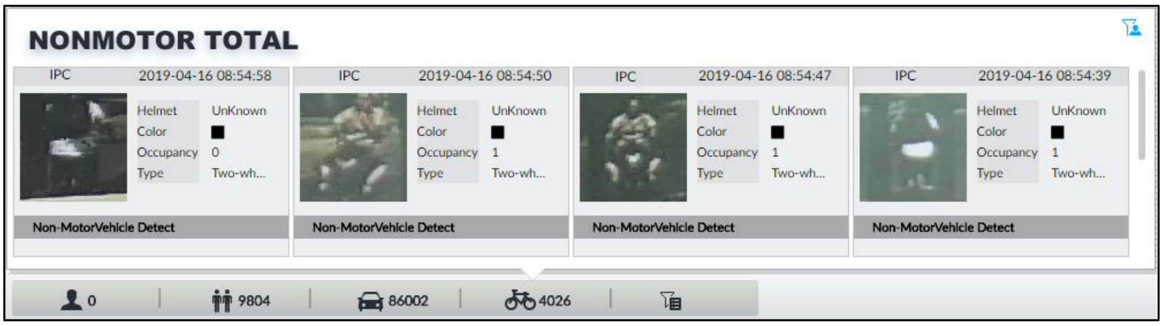
IPC 2019-04-15 20:32:32
Driver Calling UnKnown
Safe Belt Yes
Ornament UnKnown
Place
Vehicle Detection

IPC 2019-04-15 20:32:32
Driver Calling UnKnown
Safe Belt UnKnown
Ornament UnKnown
Place
Vehicle Detection

IPC 2019-04-15 20:32:31
Driver Calling UnKnown
Safe Belt UnKnown
Ornament UnKnown
Place
Vehicle Detection

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 6-29.

Figure 6-29 Non-motor vehicle detection



NONMOTOR TOTAL

IPC 2019-04-16 08:54:58
Helmet UnKnown
Color ■
Occupancy 0
Type Two-wh...
Non-MotorVehicle Detect

IPC 2019-04-16 08:54:50
Helmet UnKnown
Color ■
Occupancy 1
Type Two-wh...
Non-MotorVehicle Detect

IPC 2019-04-16 08:54:47
Helmet UnKnown
Color ■
Occupancy 1
Type Two-wh...
Non-MotorVehicle Detect

IPC 2019-04-16 08:54:39
Helmet UnKnown
Color ■
Occupancy 1
Type Two-wh...
Non-MotorVehicle Detect

6.5.4 AI Search

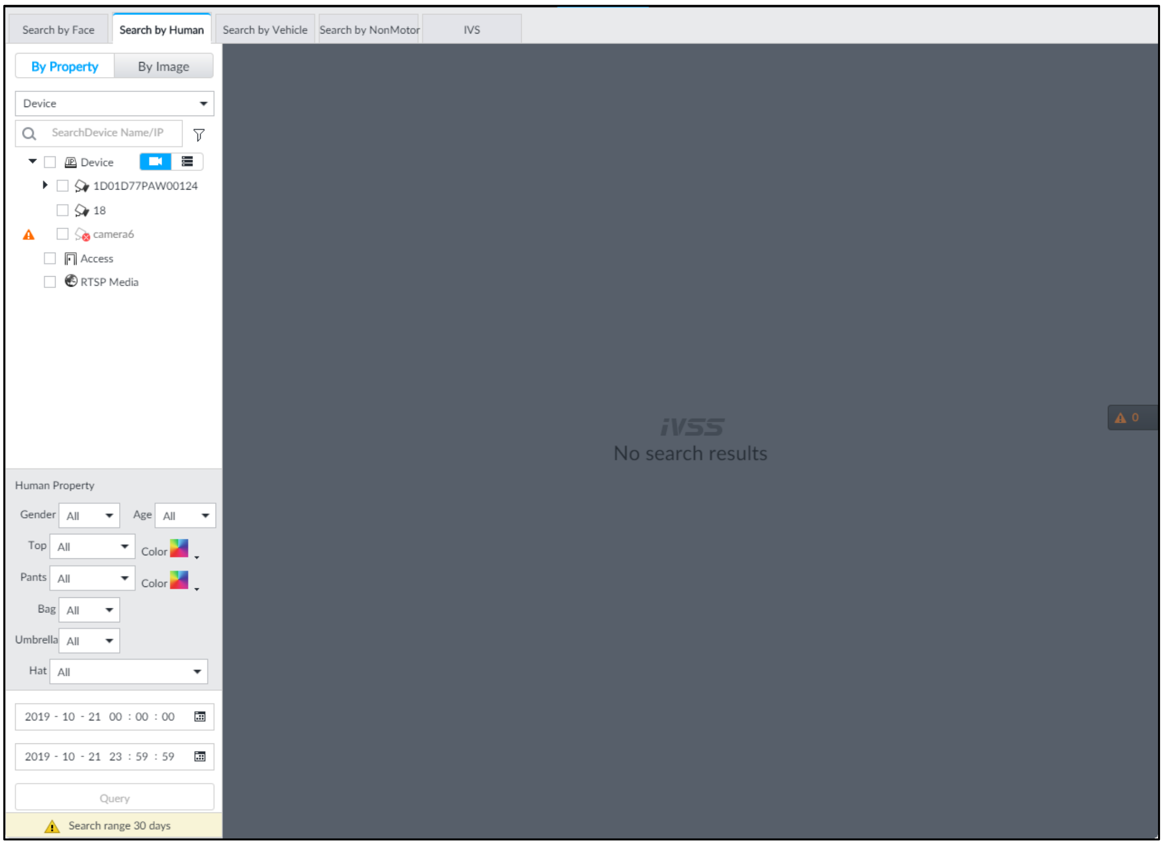
6.5.4.1 Human Search

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

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

The **Search by Human** interface is displayed. See Figure 6-30.

Figure 6-30 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.

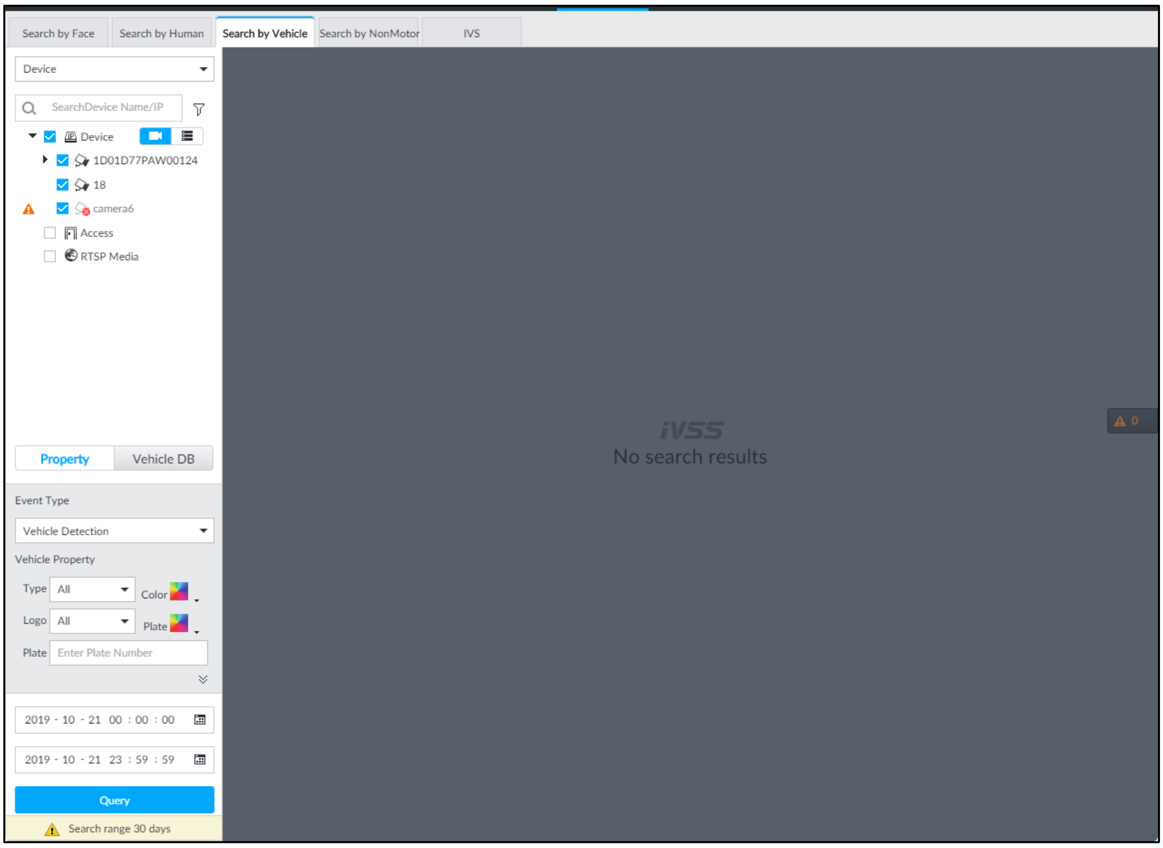
6.5.4.2 Vehicle Search

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 6-31.

Figure 6-31 Property



Event Type: Vehicle Detection

Vehicle Property

Type: All Color

Logo: All Plate

Plate: Enter Plate Number

2019 - 10 - 21 00 : 00 : 00

2019 - 10 - 21 23 : 59 : 59

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**.

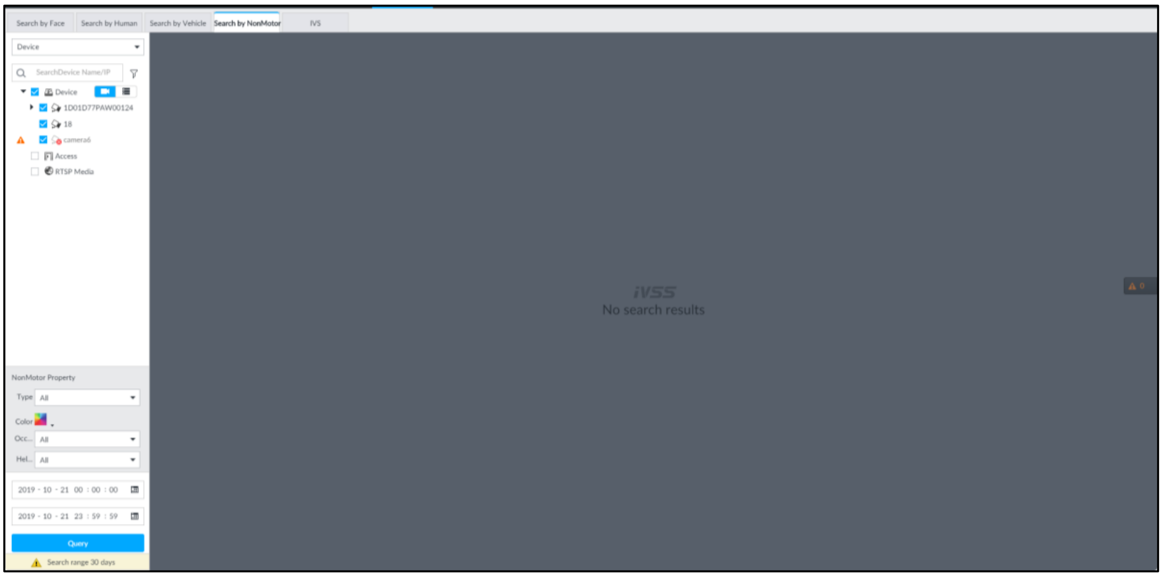
The search result is displayed..

6.5.4.3 Non-motor Vehicle Search

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

The **Search by NonMotor** interface is displayed. See Figure 6-32.

Figure 6-32 Search by non-motor vehicle



Type: All

Occ...: All

Hel...: All

2019 - 10 - 21 00 : 00 : 00

2019 - 10 - 21 23 : 59 : 59

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.

6.6 IVS

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

This section introduces how to configure the intelligent detections.

- For the same camera, IVS and face detection cannot be enabled at the same time.
- Some device models only support IVS by camera. The actual interface shall prevail.

6.6.1 Enabling AI Plan

Enable AI plan when AI by camera is used. For details, see "6.2.1 Enabling AI Plan."

6.6.2 Configuring IVS Rules

Configure IVS rules. IVS functions are different between AI by camera and AI by device. For details, see Table 6-3.

- IVS functions with AI by camera: Fence-crossing, tripwire, intrusion, abandoned object, fast moving, parking detection, people gathering, object removed, and loitering. Different cameras support different functions, and the actual interface shall prevail.
- IVS functions with AI by device: Tripwire, intrusion.

Table 6-3 IVS functions description

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

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

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

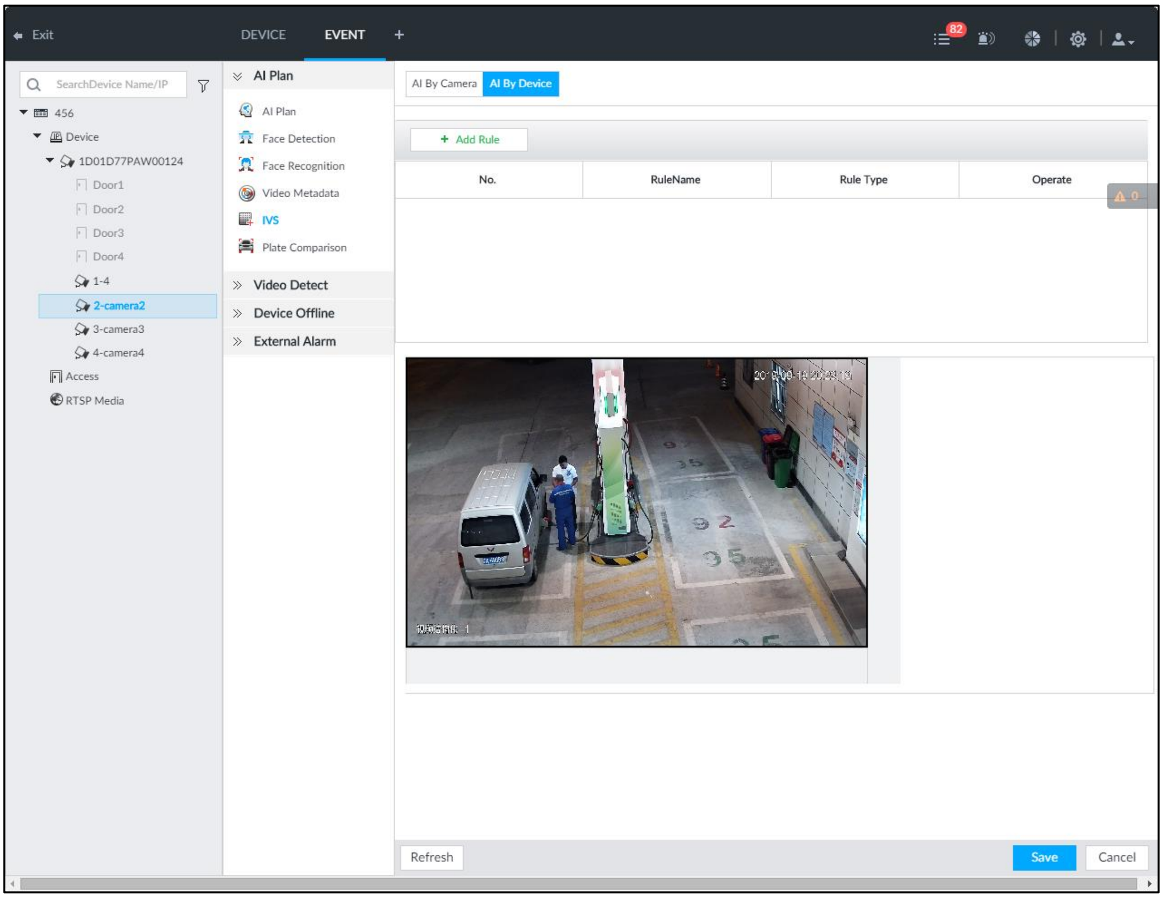
The **EVENT** interface is displayed.

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

Step 3 Select **AI Plan > IVS Rule**. Click **AI by Camera** or **AI by Device**.

The **Add Rule** interface is displayed. See Figure 6-33.

Figure 6-33 Add rules

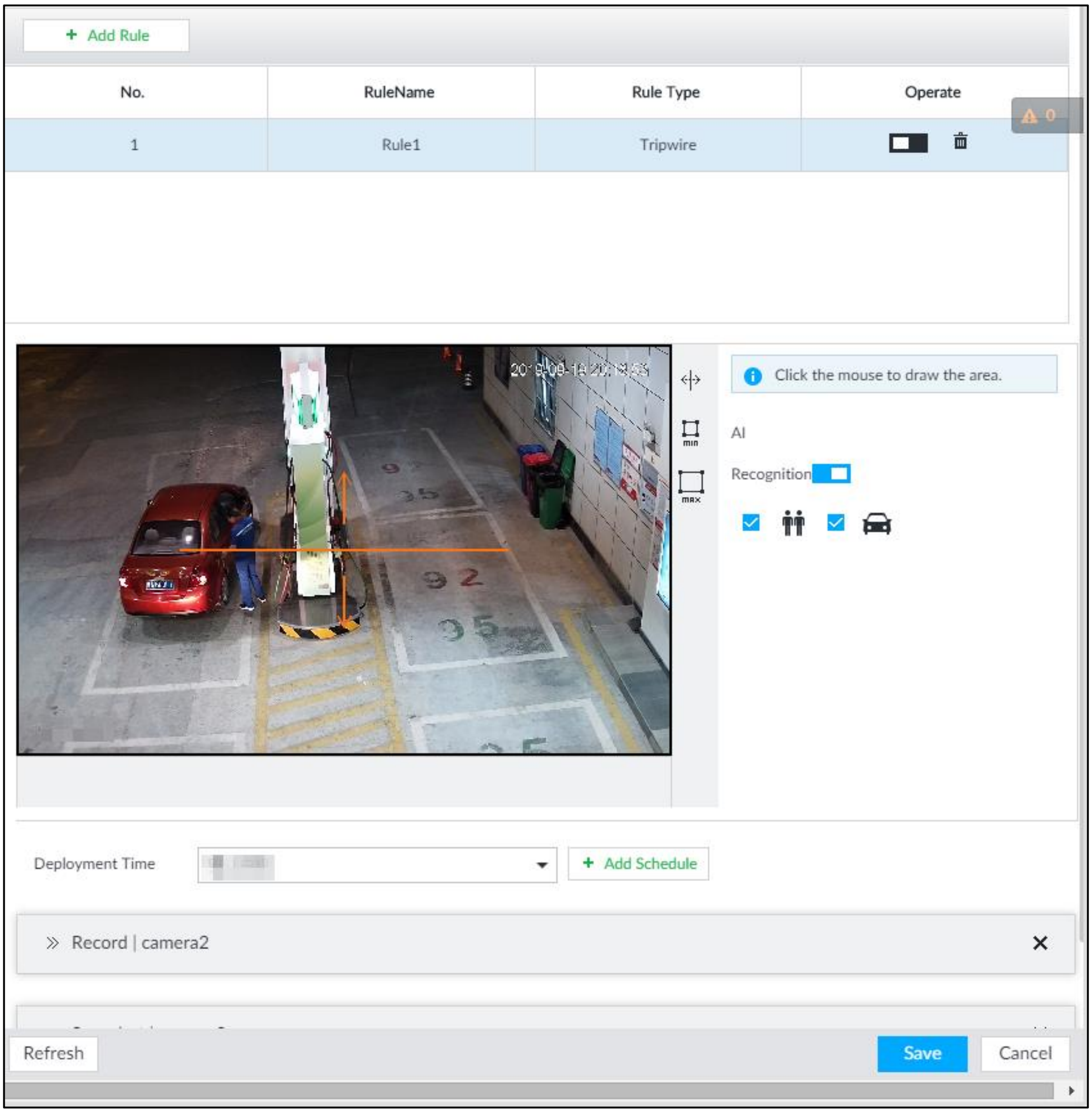


Step 4 Set tripwire rules.

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

The rule information is displayed. See Figure 6-34.

Figure 6-34 Configuring cross line detection rules



No.	RuleName	Rule Type	Operate
1	Rule1	Tripwire	

Click the mouse to draw the area.

2) Click ▭ to enable detection rule.

Click 🗑 to delete detection rule.

3) Click ⟨|⟩ to edit the tripwire line.

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

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

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

Step 5 (Optional) For other requirements, see Table 6-4.

Table 6-4 IVS rules configuration requirements

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

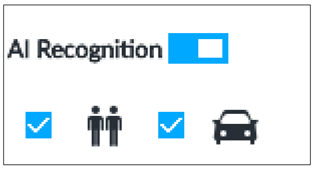
Step 6 Set AI Recognition

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

1) Click ▭ to enable AI recognition function.

The recognition type option is displayed. See Figure 6-35.

Figure 6-35 Type



AI Recognition

☑ 👥 ☑ 🚗

2) Select a recognition type.

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

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

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

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

Step 8 Click **Actions** to set alarm action. For details, see *User's Manual*.

📖

Repeat Step 4-Step 8 to add multiple detection rules. The Device supports adding max. 10 detection rules at the same time.

Step 9 Click **Save**.

6.6.3 Live View of IVS

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

6.6.3.1 Setting AI Display

Set the display rules of detection results.

Make sure that view is created before setting AI display. For details, see *User's Manual*.

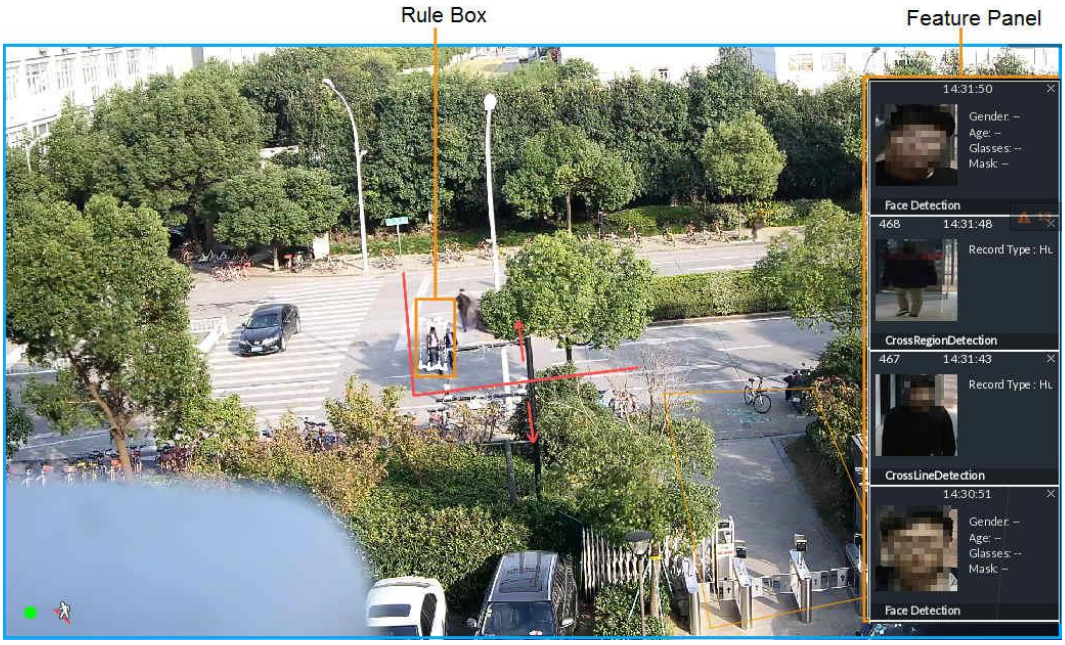
Select a view from **LIVE > View > View Group**. Click , and then select the **Face**, **Human**, **Vehicle** or **Non-Motor Vehicle** tab. Enable **Show Tracking Box** and **Features Panel**. For details, see "6.2.3.1 Setting AI Display."

6.6.3.2 Live View

Go to the **LIVE** interface, enable view, and then the Device displays view video. See Figure 6-36.

- 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 6-36 Live



14:31:50
Gender: --
Age: --
Glasses: --
Mask: --
Face Detection

468 14:31:48
Record Type : Hu
CrossRegionDetection

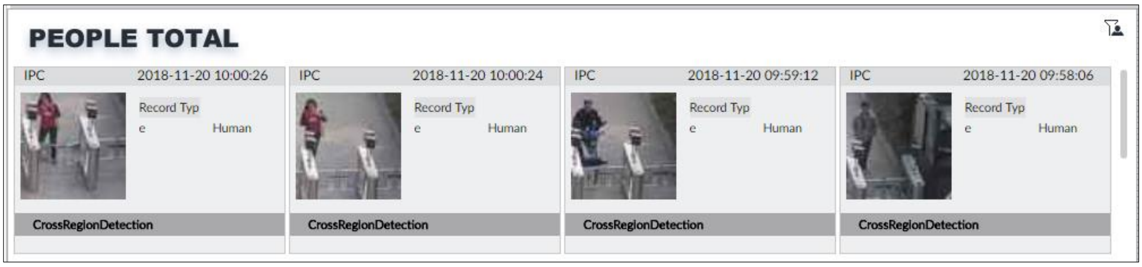
467 14:31:43
Record Type : Hu
CrossLineDetection

14:30:51
Gender: --
Age: --
Glasses: --
Mask: --
Face Detection

6.6.3.3 Detection Statistics

On the **LIVE** interface, click . The **PEOPLE TOTAL** interface is displayed. Click , and then select **IVS**. The people detection records are displayed. See Figure 6-37.

Figure 6-37 People total



PEOPLE TOTAL

IPC 2018-11-20 10:00:26
Record Typ
e Human
CrossRegionDetection

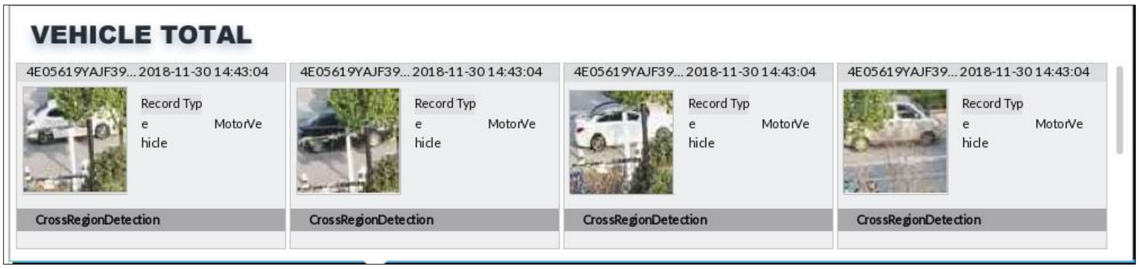
IPC 2018-11-20 10:00:24
Record Typ
e Human
CrossRegionDetection

IPC 2018-11-20 09:59:12
Record Typ
e Human
CrossRegionDetection

IPC 2018-11-20 09:58:06
Record Typ
e Human
CrossRegionDetection

Click 🚗. The **VEHICLE TOTAL** interface is displayed. Click ▽, and then select **IVS**. The detected vehicles are displayed. See Figure 6-38.

Figure 6-38 Vehicle total



VEHICLE TOTAL

4E05619YAJF39... 2018-11-30 14:43:04
Record Typ
e MotorVe
hicle
CrossRegionDetection

4E05619YAJF39... 2018-11-30 14:43:04
Record Typ
e MotorVe
hicle
CrossRegionDetection

4E05619YAJF39... 2018-11-30 14:43:04
Record Typ
e MotorVe
hicle
CrossRegionDetection

4E05619YAJF39... 2018-11-30 14:43:04
Record Typ
e MotorVe
hicle
CrossRegionDetection

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

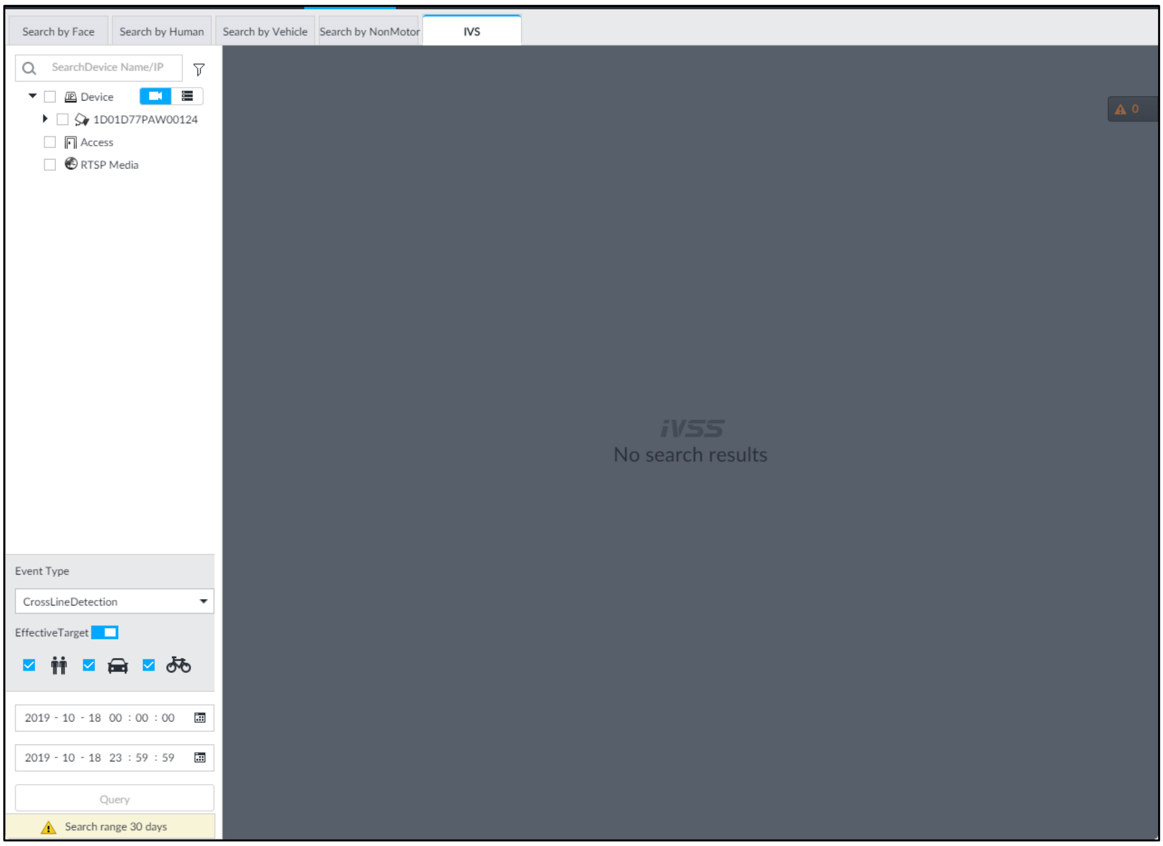
6.6.4 IVS Search

Search for IVS records.

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

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

Figure 6-39 IVS



Event Type: CrossLineDetection

EffectiveTarget

☑ ☑ ☑

2019 - 10 - 18 00 : 00 : 00

2019 - 10 - 18 23 : 59 : 59

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.

6.7 ANPR

You need the ANPR (Automatic Number Plate Recognition) feature to monitor and control vehicle entry & exit. The system detects vehicle number plates in real time, and compares the detected number plates with the ones in the database. For trusted vehicles, the system lets them in by automatically opening the barrier gate; for unwelcome vehicles, you can keep your barrier gate closed to prevent them from coming in.

This section introduces how to configure the ANPR business from creating vehicle database to setting ANPR live view.

6.7.1 Procedure

Figure 6-40 Configuring ANPR (AI by camera)

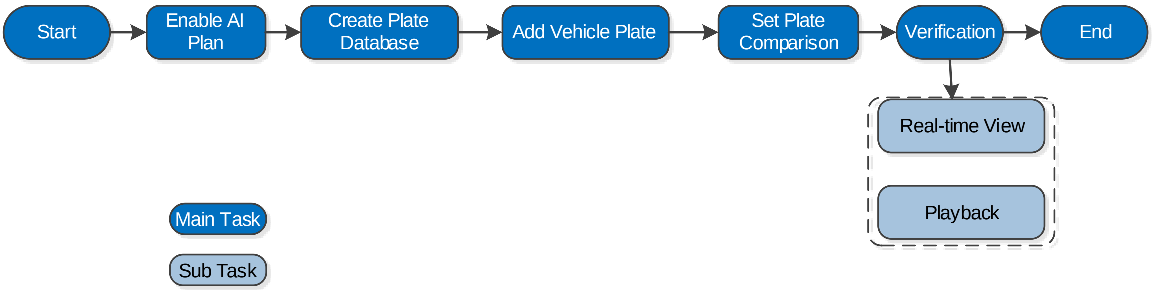
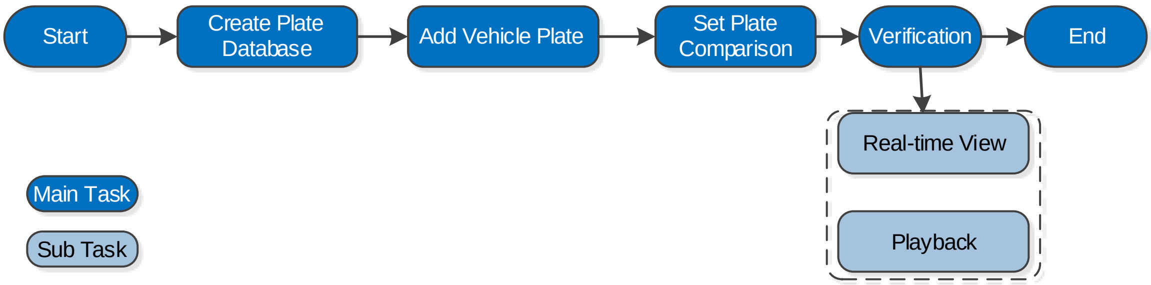


Figure 6-41 Configuring ANPR (AI by IVSS)



6.7.2 Enabling AI Plan

Before using AI by camera, AI plan needs to be enabled first. For details, see "6.2.1 Enabling AI Plan."

6.7.3 Configuring Vehicle Database

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

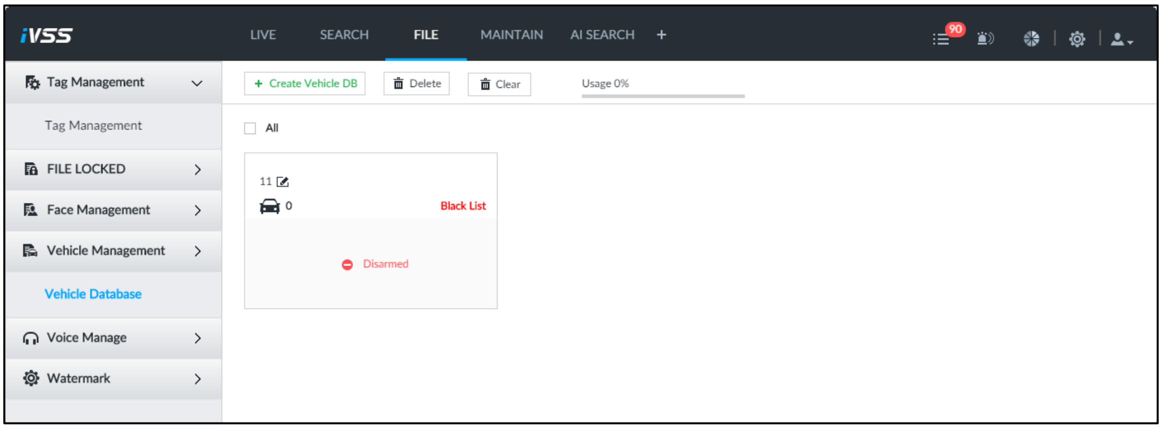
6.7.3.1 Creating Vehicle Database

Create vehicle database, and then classify and manage the database. Database of safe trusted vehicle list and blocked vehicle list can be created.

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

The **Vehicle Database** interface is displayed. See Figure 6-42.

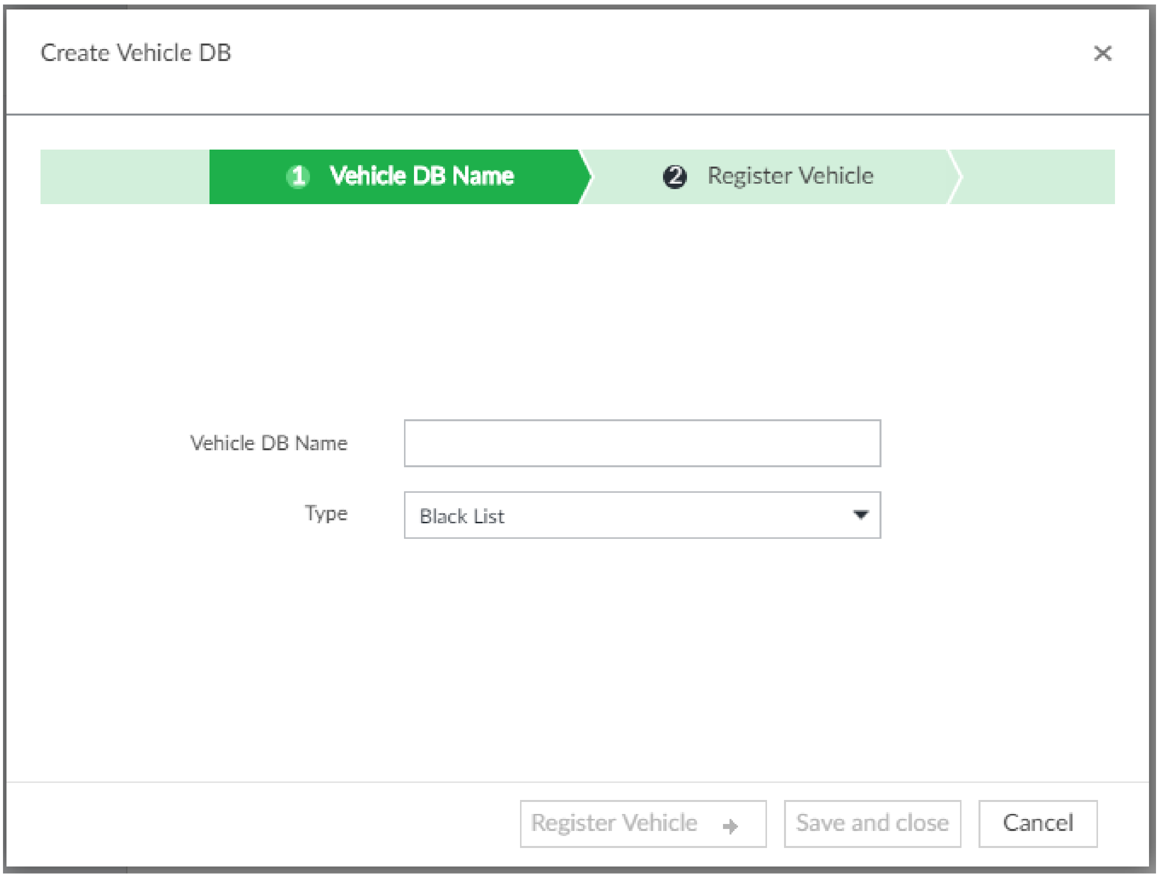
Figure 6-42 Vehicle database



Step 2 Click **Create Vehicle DB**.

The **Create Vehicle DB** interface is displayed. See Figure 6-43.

Figure 6-43 Create vehicle database



Vehicle DB Name

Type: Black List

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

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

6.7.3.2 Registering Vehicle Information

Add vehicle information to the created database. You can add vehicles one by one, in batches or directly add from the detection results. This section takes batch import as an example. For details of the other methods, see *User's Manual*.

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

The **Vehicle Database** interface is displayed.

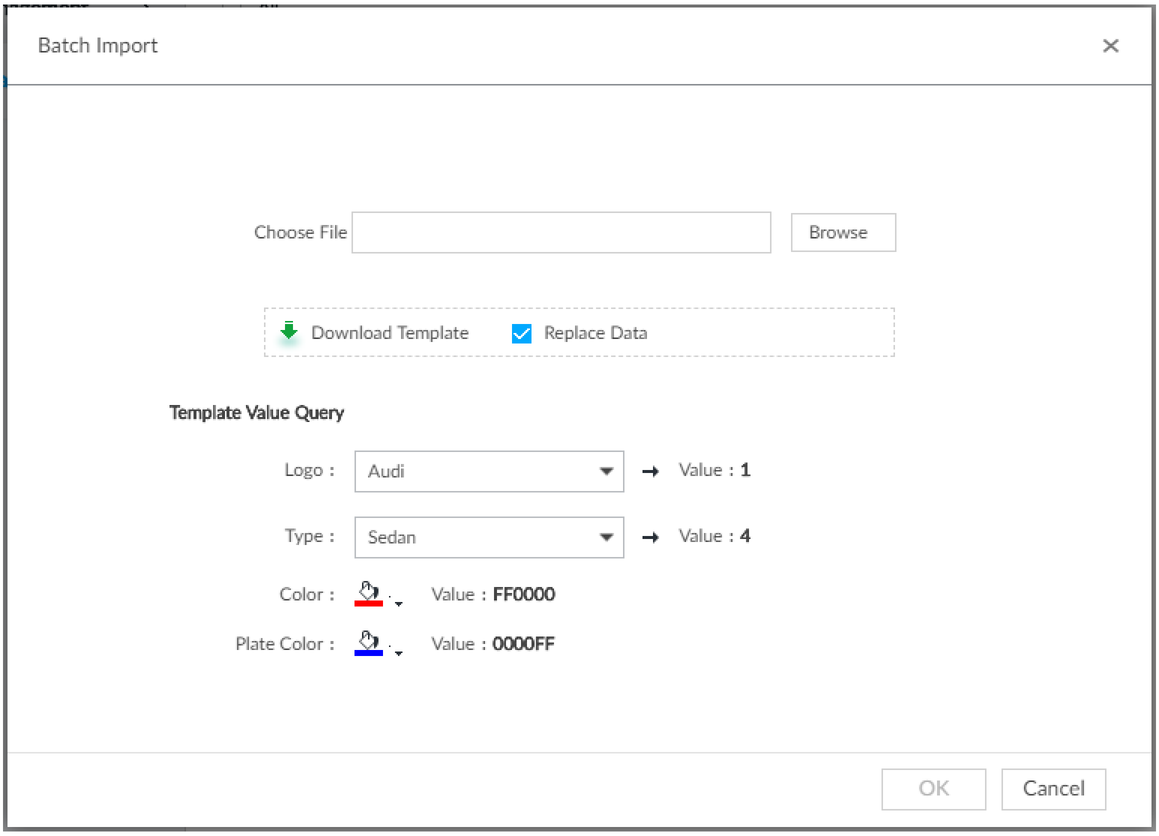
Step 2 Double-click the database.

The database interface is displayed.

Step 3 Click **Batch Import**.

The **Batch Import** interface is displayed. See Figure 6-44.

Figure 6-44 Batch import



Batch Import

Choose File

Browse

Download Template ☑ Replace Data

Template Value Query

Logo : Audi → Value : 1

Type : Sedan → Value : 4

Color : Value : FF0000

Plate Color : Value : 0000FF

OK Cancel

Step 4 Acquire and fill in the template file.

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

   The save path might vary when operating on client or local interface, and the actual interface shall prevail.
2) Fill in the template fill according to your actual needs. For details, see *User's Manual*.

   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 6-44).
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.

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

6.7.4 Configuring Number Plate Comparison

Set the alarm triggering rules after plate comparison.

📖

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

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

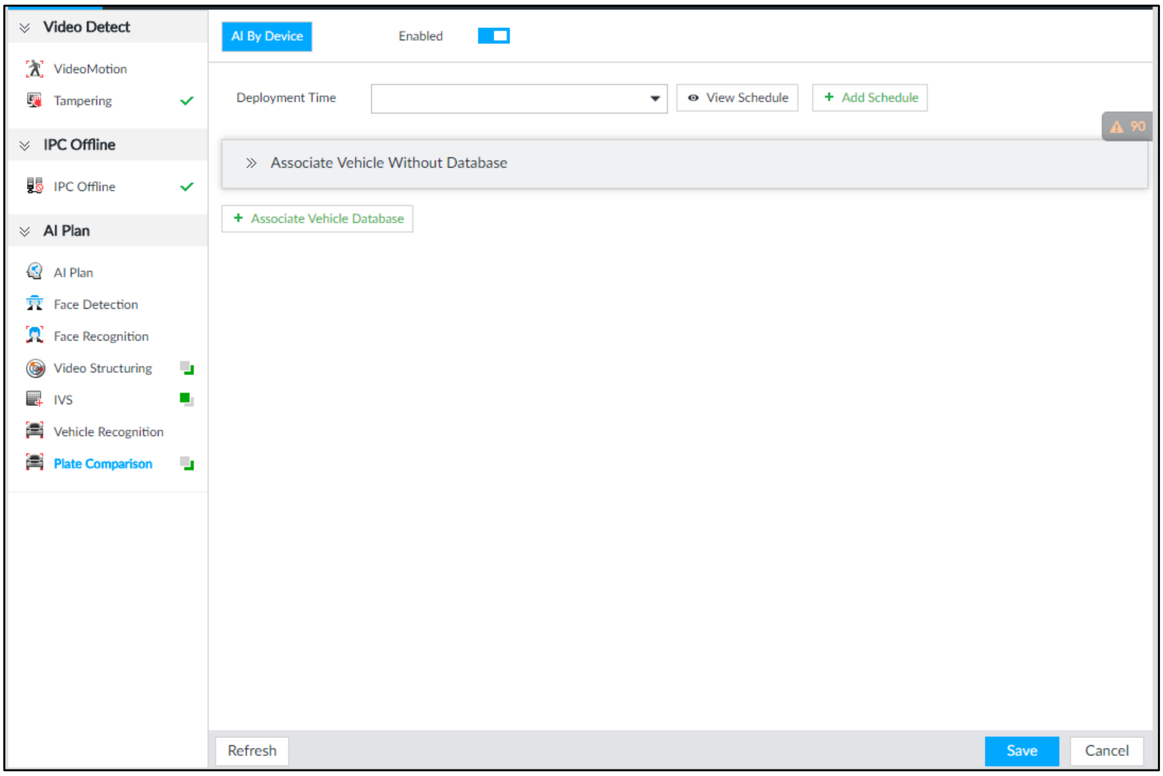
The **EVENT** interface is displayed.

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 6-45.

Figure 6-45 Plate comparison



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

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

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

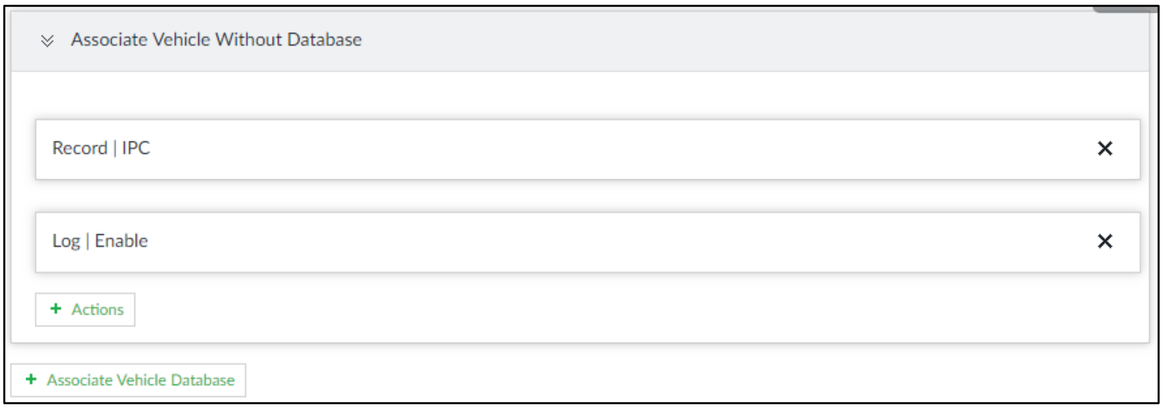
Step 6 Link vehicle without database.

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 6-46.

Figure 6-46 Associate vehicle without database


Associate Vehicle Without Database
Actions
Associate Vehicle Database

Record | IPC

Log | Enable

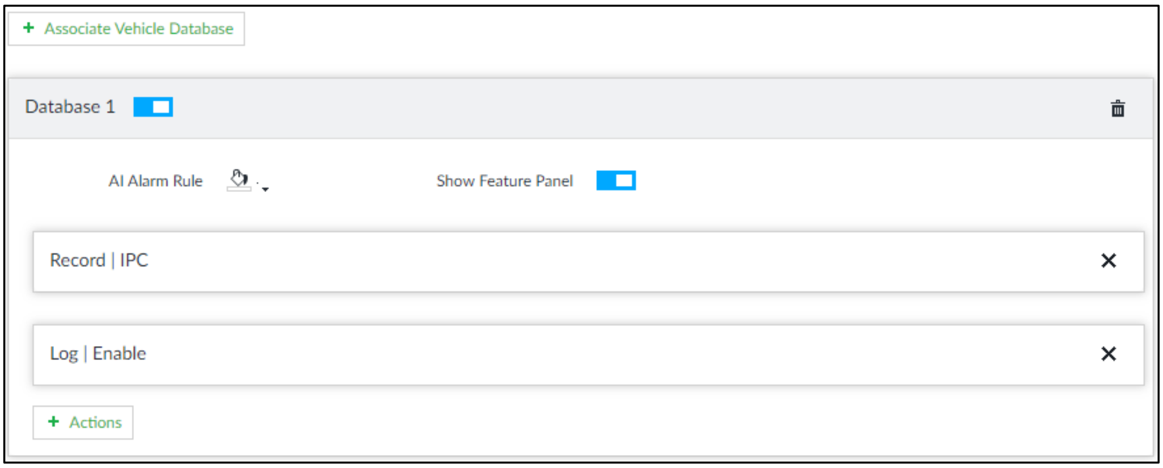
2) Click **Actions** to set alarm linkage event. For details, see *User's Manual*.

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 6-47.

Figure 6-47 Database linkage



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

Table 6-5 Database linkage parameters

Parameters	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 *User's Manual.*

Step 8 Click **Save**.

6.7.5 Live View of ANPR

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

6.7.5.1 Setting AI Display

Set the display rules of detection results.

Make sure that view is created before setting AI display. To create view, see *User's Manual.*

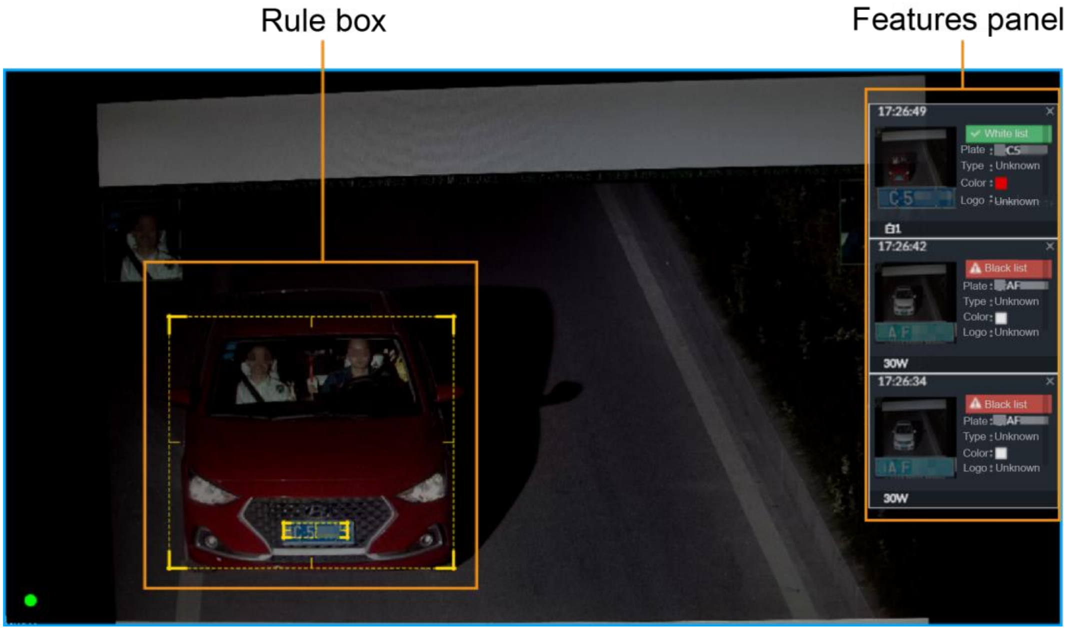
On the **Live** interface, select a view from **LIVE > View > View Group**. Click , and then select **Vehicle** tab. Enable **Show Tracking Box** and **Features Panel**, and then select the features you need to display on the live view. For details, see "6.2.3.1 Setting AI Display."

6.7.5.2 Live View

On the **LIVE** interface, select a view, and the video image of the view is displayed. See Figure 6-48.

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

Figure 6-48 Live



17:26:49
✓ White list
Plate : C5
Type : Unknown
Color : 🟥
Logo : Unknown

17:26:42
Black list
Plate : AF
Type : Unknown
Color : □
Logo : Unknown

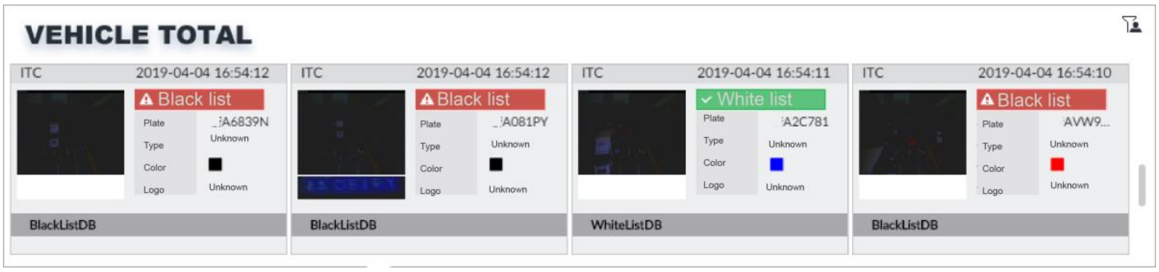
17:26:34
Black list
Plate : AF
Type : Unknown
Color : □
Logo : Unknown

6.7.5.3 Detection Statistics

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 6-49.

Figure 6-49 Vehicle comparison



VEHICLE TOTAL

ITC 2019-04-04 16:54:12	ITC 2019-04-04 16:54:12	ITC 2019-04-04 16:54:11	ITC 2019-04-04 16:54:10
Black list	Black list	✓ White list	Black list
Plate A6839N	Plate A081PY	Plate A2C781	Plate AVW9...
Type Unknown	Type Unknown	Type Unknown	Type Unknown
Color ■	Color ■	Color 🟦	Color 🟥
Logo Unknown	Logo Unknown	Logo Unknown	Logo Unknown
BlackListDB	BlackListDB	WhiteListDB	BlackListDB

6.7.6 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.

6.7.6.1 Searching by Property

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

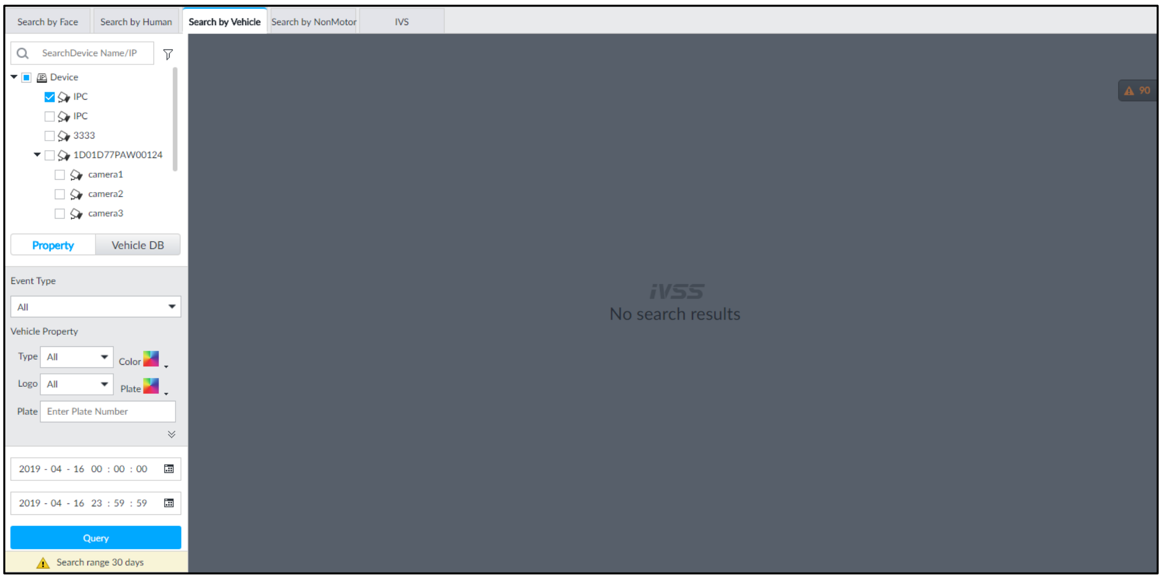
Step 1 On the **LIVE** interface, click +, and then select **AI SEARCH > Search by Vehicle**.

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 6-50.

Figure 6-50 Search by property



☑ IPC

Event Type: All

Vehicle Property

Type: All ▾ Color ▦

Logo: All ▾ Plate ▦

Plate: Enter Plate Number

2019 - 04 - 16 00 : 00 : 00

2019 - 04 - 16 23 : 59 : 59

⚠ Search range 30 days

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.

6.7.6.2 Searching by Database

Search vehicle recognition information according to database.

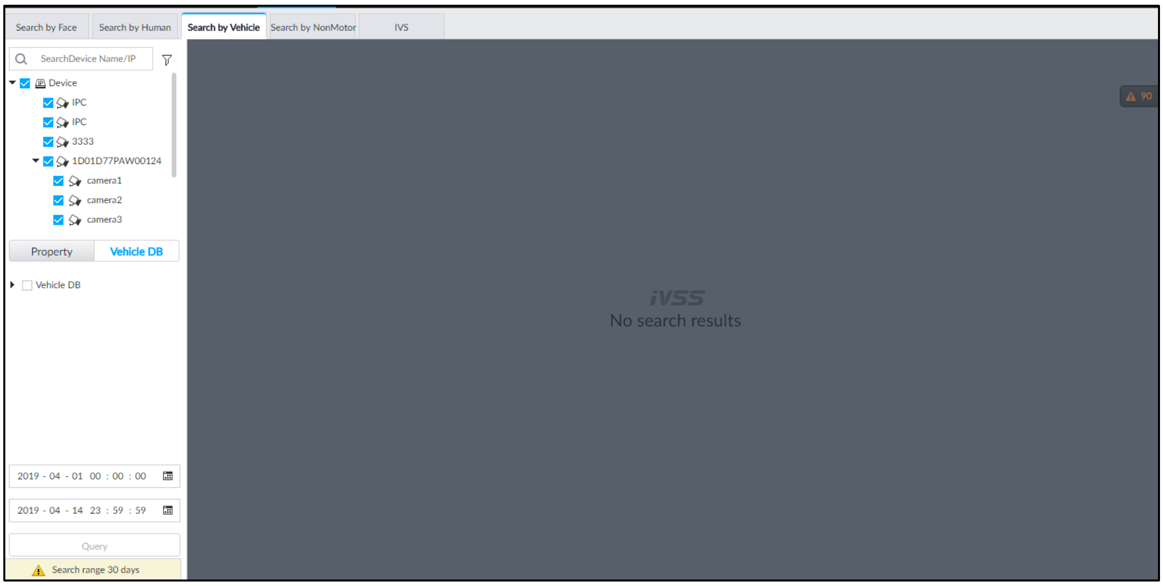
Step 1 On the **LIVE** interface, click +, and then select **AI SEARCH > Search by Vehicle**.

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 6-51.

Figure 6-51 Search by vehicle database



Step 3 Select the database to be searched.

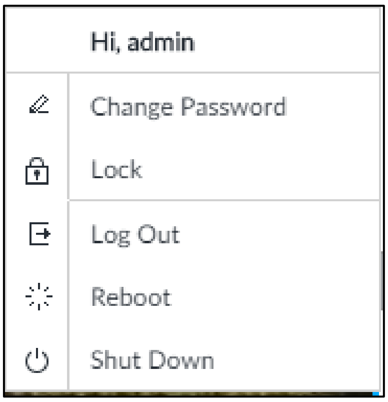
Step 4 Click **Query**.

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

7 Logout, Reboot, Shut Down, Lock

You can log out, reboot and lock out the Device. See Figure 7-1.

Figure 7-1 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

⚠**CAUTION**

To unplug the power cable might result in data (record, image) loss. We recommend Mode 1.

- Mode 1 (recommended): Click , and then select **Shut Down**. System pops up confirm dialogue box, and then click **OK** to shut down.
- Mode 2: Use power on/off button on the Device.
  - ◇ 8-HDD series product: Press power on/off button on rear panel.
  - ◇ Other series products: Press the power on/off button on the Device for at least 4 seconds.
- Mode 3: Unplug the power cable.

Lock

Click 👤▾, and then select **Lock** to lock the client. The locked client cannot be operated.

To unlock the client, click anywhere on the client, and then the **Unlock** dialogue box is displayed. Enter the username and password, and then click **OK**.

Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it’s something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

Mandatory actions to be taken for basic equipment network security:

1. **Use Strong Passwords**

   Please See the following suggestions to set passwords:

   - The length should not be less than 8 characters;
   - Include at least two types of characters; character types include upper and lower case letters, numbers and symbols;
   - Do not contain the account name or the account name in reverse order;
   - Do not use continuous characters, such as 123, abc, etc.;
   - Do not use overlapped characters, such as 111, aaa, etc.;

2. **Update Firmware and Client Software in Time**

   - According to the standard procedure in Tech-industry, we recommend to keep your equipment (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the “auto-check for updates” function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your equipment network security:

1. **Physical Protection**

   We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable equipment (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Set and Update Passwords Reset Information Timely**

   The equipment supports password reset function. Please set up related information for password reset in time, including the end user’s mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. **Enable Account Lock**

The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. **Change Default HTTP and Other Service Ports**

   We suggest you to change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **Enable 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.