Intelligent Video Surveillance Server

Quick Start Guide

V1.1.0

Cybersecurity Recommendations

Mandatory actions to be taken towards cybersecurity

1. Change Passwords and Use Strong Passwords:

The number one reason systems get “hacked” is due to having weak or default passwords. It is recommended to change default passwords immediately and choose a strong password whenever possible. A strong password should be made up of at least 8 characters and a combination of special characters, numbers, and upper and lower case letters.

2. Update Firmware

As is standard procedure in the tech-industry, we recommend keeping NVR, DVR, and IP camera firmware up-to-date to ensure the system is current with the latest security patches and fixes.

“Nice to have” recommendations to improve your network security

1. Change Passwords Regularly

Regularly change the credentials to your devices to help ensure that only authorized users are able to access the system.

2. Change Default HTTP and TCP Ports:

● Change default HTTP and TCP ports for systems. These are the two ports used to communicate and to view video feeds remotely.

● These ports can be changed to any set of numbers between 1025-65535. Avoiding the default ports reduces the risk of outsiders being able to guess which ports you are using.

3. Enable HTTPS/SSL:

Set up an SSL Certificate to enable HTTPS. This will encrypt all communication between your devices and recorder.

4. Enable IP Filter:

Enabling your IP filter will prevent everyone, except those with specified IP addresses, from accessing the system.

5. Change ONVIF Password:

On older IP Camera firmware, the ONVIF password does not change when you change the system’s credentials. You will need to either update the camera’s firmware to the latest revision or manually change the ONVIF password.

6. Forward Only Ports You Need:

● Only forward the HTTP and TCP ports that you need to use. Do not forward a huge range of numbers to the device. Do not DMZ the device's IP address.

● You do not need to forward any ports for individual cameras if they are all connected to a recorder on site; just the NVR is needed.

7. Disable Auto-Login on SmartPSS:

Those using SmartPSS to view their system and on a computer that is used by multiple people should disable auto-login. This adds a layer of security to prevent users without the appropriate credentials from accessing the system.

8. Use a Different Username and Password for SmartPSS:

In the event that your social media, bank, email, etc. account is compromised, you would not want someone collecting those passwords and trying them out on your video surveillance system. Using a different username and password for your security system will make it more difficult for someone to guess their way into your system.

9. Limit Features of Guest Accounts:

If your system is set up for multiple users, ensure that each user only has rights to features and functions they need to use to perform their job.

10. UPnP:

● UPnP will automatically try to forward ports in your router or modem. Normally this would be a good thing. However, if your system automatically forwards the ports and you leave the credentials defaulted, you may end up with unwanted visitors.

● If you manually forwarded the HTTP and TCP ports in your router/modem, this feature should be turned off regardless. Disabling UPnP is recommended when the function is not used in real applications.

11. SNMP:

Disable SNMP if you are not using it. If you are using SNMP, you should do so only temporarily, for tracing and testing purposes only.

12. Multicast:

Multicast is used to share video streams between two recorders. Currently there are no known issues involving Multicast, but if you are not using this feature, deactivation can enhance your network security.

13. Check the Log:

If you suspect that someone has gained unauthorized access to your system, you can check the system log. The system log will show you which IP addresses were used to login to your system and what was accessed.

14. Physically Lock Down the Device:

Ideally, you want to prevent any unauthorized physical access to your system. The best way to achieve this is to install the recorder in a lockbox, locking server rack, or in a room that is behind a lock and key.

15. Connect IP Cameras to the PoE Ports on the Back of an NVR:

Cameras connected to the PoE ports on the back of an NVR are isolated from the outside world and cannot be accessed directly.

16. Isolate NVR and IP Camera Network

The network your NVR and IP camera resides on should not be the same network as your public computer network. This will prevent any visitors or unwanted guests from getting access to the same network the security system needs in order to function properly.

Foreword

General

This quick start guide (hereinafter referred to be "the Guide") introduces the functions and operations of the Intelligent Video Surveillance Server (IVSS) device (hereinafter referred to be "the Device").

Safety Instructions

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

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.

Privacy Protection Notice

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

About the Guide

- The Guide is for reference only. If there is inconsistency between the Guide 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 Guide.
- The Guide would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official

website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.

- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the Guide. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our final explanation.
- Upgrade the reader software or try other mainstream reader software if the Guide (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the Guide are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the Device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Writing Conventions

In order to simplify the description, the commonly used functional names in the Guide are made as follows.

- The remote device in the Guide refers to the front-end device such as IPC and speed dome connected to the IVSS device via the network.
- The AI Module in the Guide refers to the AI card installed in the IVSS device.
- The Device supports local, WEB and IVSS client operation and the Guide is based on the local interface and operation. There might be differences when using Web or IVSS client operation. The actual interface shall prevail.
- To guarantee the security of personal privacy, the private information such as human face and car plate number has been dealt with.

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

- Don’t place and install the Device in an area exposed to direct sunlight or near heat generating device.
- Don’t install the Device in a humid, dusty or fuliginous area.
- Keep its horizontal installation, or install it at stable places, and prevent it from falling.
- Don’t drip or splash liquids onto the Device; don’t put on the device anything filled with liquids, in order to prevent liquids from flowing into the Device.
- Install the Device at well-ventilated places; don’t block its ventilation opening.
- Use the Device only within rated input and output range.
- Don’t dismantle the Device arbitrarily.
- Transport, use and store the Device within allowed humidity and temperature range.

Power Requirement

- Make sure to use the designated battery type. Otherwise there may be explosion risk.
- Make sure to use batteries according to requirements; otherwise, it may result in fire, explosion or burning risks of batteries!
- To replace batteries, only the same type of batteries can be used.
- Make 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.
- Make 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, please refer to device labels.
- Products with category I structure shall be connected to grid power output socket, which is equipped with protective grounding.
- Appliance coupler is a disconnecting device. During normal use, please keep an angle that facilitates operation.

Points for Attention:

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

Table of Contents

1 General Introduction

1.1 Overview

Intelligent video surveillance server is a product of new form. Compatible with the general functions of video surveillance of security industry, it has added AI functions such as human face recognition and features extraction based on the deep learning technology.

This series product includes general system settings, video surveillance, video storage, alarm settings, log management, record search and playback, intelligent analysis (such as human face real-time recognition, search human face by specified image and then play back videos). This series product has user-friendly interface which is suitable for users to operate. At the same time, it supports real-time alarm and search record file or image by human face features, which greatly enhance record file search speed.

This series product supports 4K and H.265 decoding. It meets the main development trend of current market.

This series product can be widely used in areas such as intelligent building, large parking lot, safe city project and financial planning.

1.2 Structure

It is to introduce front panel, rear panel, ports, buttons and indicator lights. The following contents are based on the 16-HDD series product. For detailed information of other series, see *User’s Manual*.

1.2.1 Front Panel

Figure 1-1 Front panel (with LCD panel)

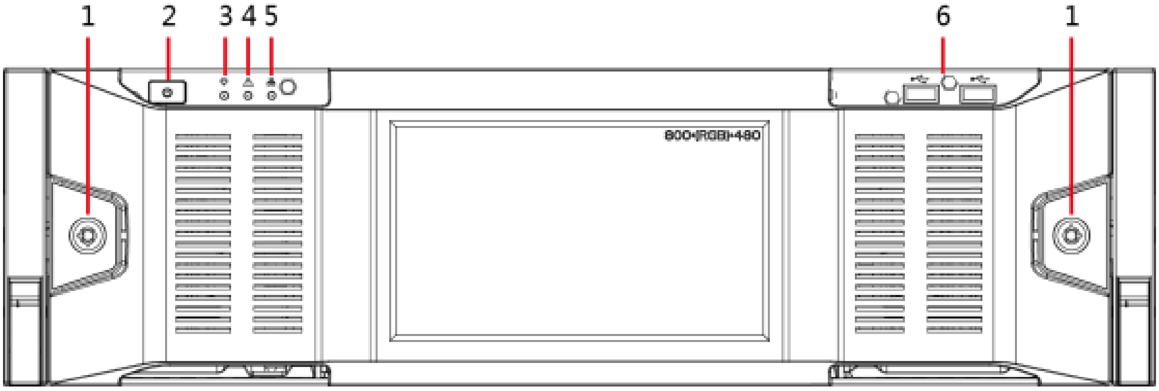


Figure 1-2 Front panel (without LCD panel)

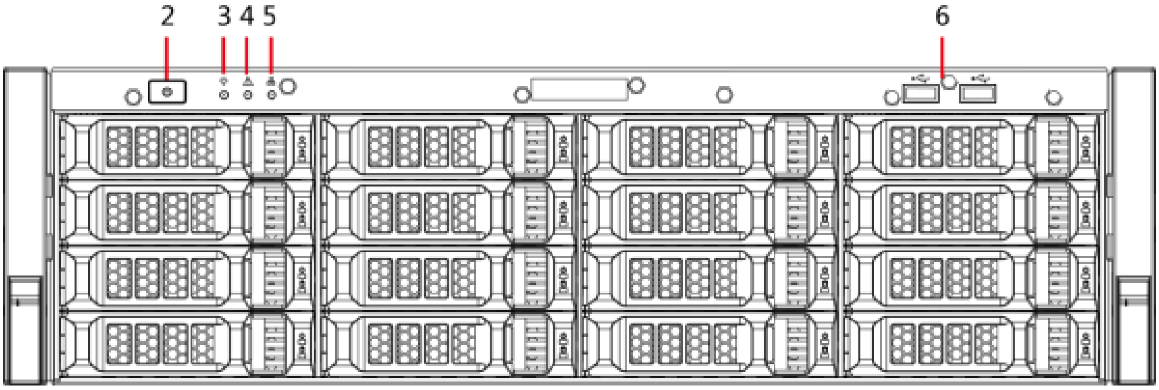


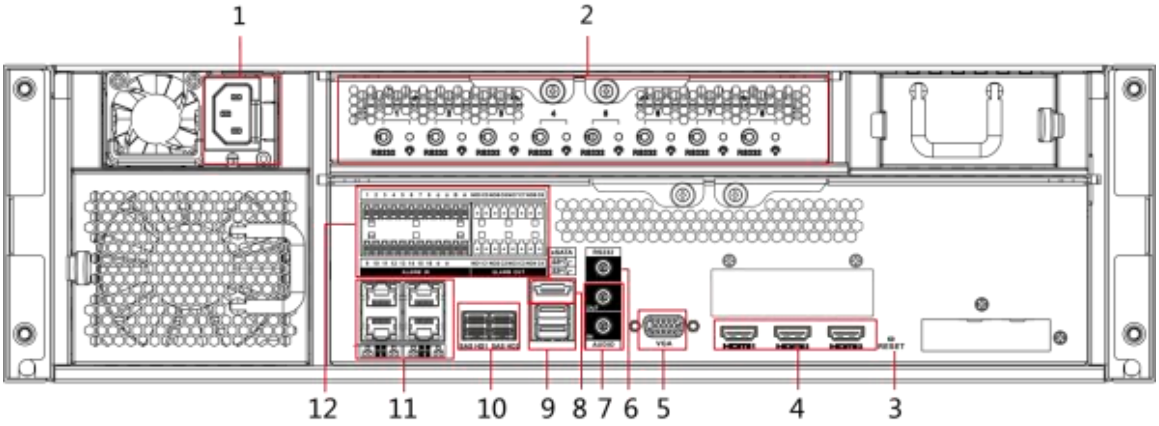
Table 1-1 Front panel description

No.	Name	Description
1	Front panel lock	Once the front panel lock is locked, it can prevent HDD from being stolen or removed by mistake. Unlock the front panel lock, remove the front panel, and you can view 16 HDD slots.
2	Power on-off button	Boot up or shut down the Device. The power on-off button has the indicator light. It can display device-running status. ● When the Device is off (indicator light is off), press the button for a short period to boot up the Device. ● When the Device is running, (blue indicator light is on), press the button for at least 4 seconds to shut down the Device.
3	System status indicator light	It is to display system-running status. ● The blue light is on: Device is running properly. ● The indicator light is off: Device is not running.
4	Alarm indicator light	It is to display local input alarm status. ● The indicator light is off: There is no local alarm input event. ● The blue indicator light is on: There is one or more local alarm input event.
5	Network indicator light	It is to display current network status. ● The blue indicator light is on: At least one Ethernet port has connected to the network. ● The indicator light is off: No Ethernet port is connected to the network.
6	USB port	Connect to mouse, keyboard, USB storage device ,etc.
7	16-HDD slot	After you remove the front panel, you can see 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 bracket: HDD indicator light and HDD read/write indicator light. ● HDD indicator light: The light is yellow after you install the HDD. ● HDD read/write indicator light: The blue light flashes when system is reading or writing the data.

1.2.2 Rear Panel

For the single-power series, the interface is shown as in Figure 1-3.

Figure 1-3 Rear panel (single power)



For the redundant series, the interface is shown as in Figure 1-4.

Figure 1-4 Rear panel (dual power)

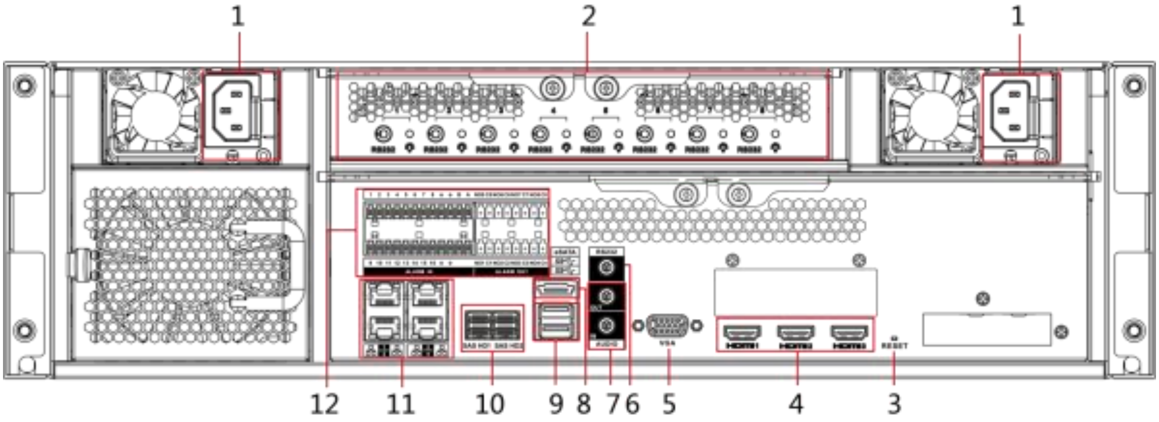


Table 1-2 Rear panel description

No.	Name	Description
1	Power port	Input AC 100V-240V power
2	AI module indicator light	It is to display AI module status. ● When the yellow light flashes, AI module is running properly. ● When the yellow light is on, AI module is in malfunction. **NOTE** This function is null if there is no AI module.
3	RESET button	Use a needle or something like that to press the button, device restores factory default settings.
4	High Definition Media Interface	High definition audio and video signal output port. It transmits uncompressed high definition video and multiple-channel data to the HDMI port of the display device.

No.	Name	Description
5	VGA video output port	VGA video output port. Output analog video signal. It can connect to the monitor to view analog video.
6	AUDIO IN	Audio input port
	AUDIO OUT	Audio output port
7	RS232 port	RS232 COM debug. It is to debug general COM, set IP address and transmit transparent COM data.
8	eSATA port	SATA peripheral port. Connect to device of SATA port.
9	USB port	USB port. Connect to mouse, USB storage device ,etc.
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） alarm input ports, corresponding to ALARM 1～ALARM 16. The alarm becomes valid in low level. ● A/B cable: Control the A/B cable of the RS485 device. It is to connect to the PTZ camera. Please parallel connect 120Ω between A/B cables if there are too many PTZ decoders. ● ⏚: Alarm input ground end.
	Alarm output	8 groups of alarm output ports (NO1 C1～NO8 C8). Output alarm signal to the alarm device. Please make sure there is power to the external alarm device. ● NO: Normal open alarm output port. ● C: Alarm output public end. ● ⏚: Alarm output GND end.

2 Installation and Connection

This chapter is to introduce HDD installation, cable connection, etc.

⚠ **WARNING**

Products of some series are heavy. It needs several persons to carry or move in case there is person injury.

2.1 Checking the Components

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

Sequence	Checking items		Requirement
1	Package	Appearance	No obvious damage.
		Packing materials	No broken or distorted positions that could be caused by hit.
		Accessories	Complete.
2	Labels	Labels on the Device	Not torn up. NOTE Do not tear up or throw away the labels; otherwise the warranty services are not ensured. You need to provide the serial number of the product when you call the after-sales service.
3	Device	Appearance	No obvious damage.
		Data cables, power cables, fan cables, mainboard	No connection loose.

2.2 Installing HDD

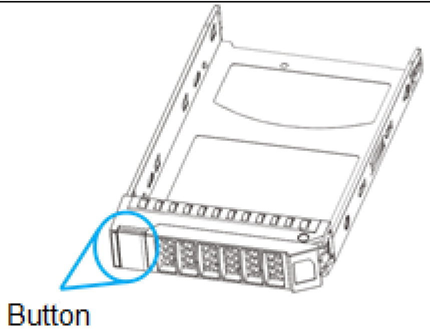
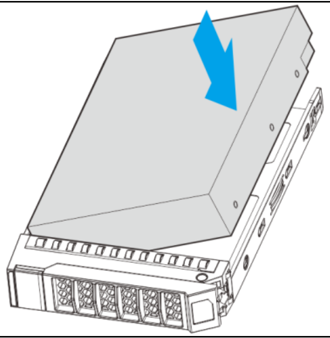
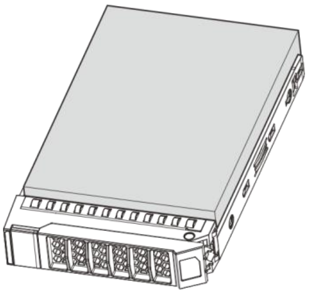
The section introduces the detailed operations to install the HDD.

CAUTION

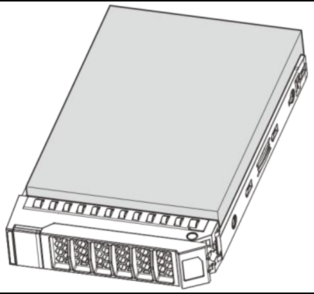
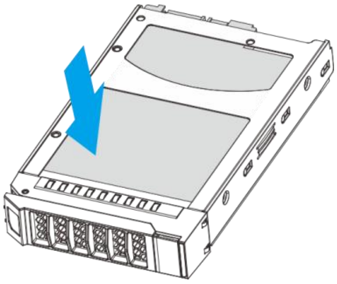
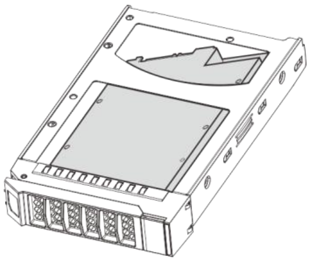
- Different models support different HDD numbers. See the actual situation.
- If you have not pushed the HDD box to the bottom, do not close the handle to avoid any damage to the HDD slot.

2.2.1 12-HDD

Installing HDD

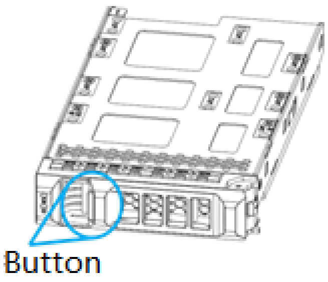
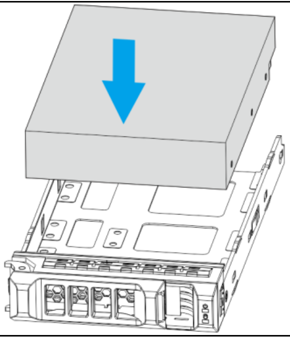
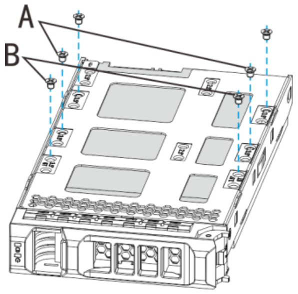
		
① Press the button on the front panel of IVSS device, open the handle, and then pull out the empty HDD box.	② Place one side of the HDD closely along the upper side of the box and press down to push the HDD down to the lower side of the mounting surface.	③ Insert the HDD box into the HDD slot, press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

Removing HDD

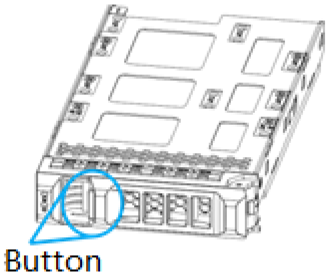
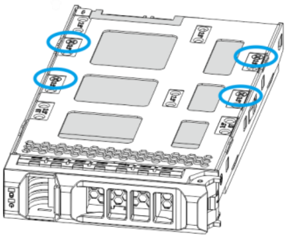
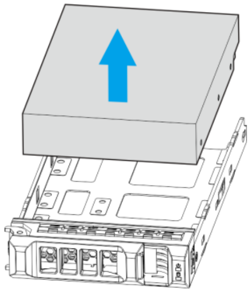
		
① Press the button on the front panel of IVSS device, open the handle, and then pull out the HDD box.	② On the back of the HDD box, press hard on the position indicated by the arrow.	③ Take out the HDD and reinsert the box to the slot. Push it to the bottom and close the box handle.

2.2.2 16/24-HDD

Installing HDD

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

Removing HDD

		
① Press 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. **NOTE** 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.

2.3 Installing AI Module

The Device supports to install AI module to realize smart detective functions such as face detection and face recognition. You can view the running status of the AI module from the corresponding indicator on the rear panel.

AI module is not the standard accessory. You can select it according to actual needs.

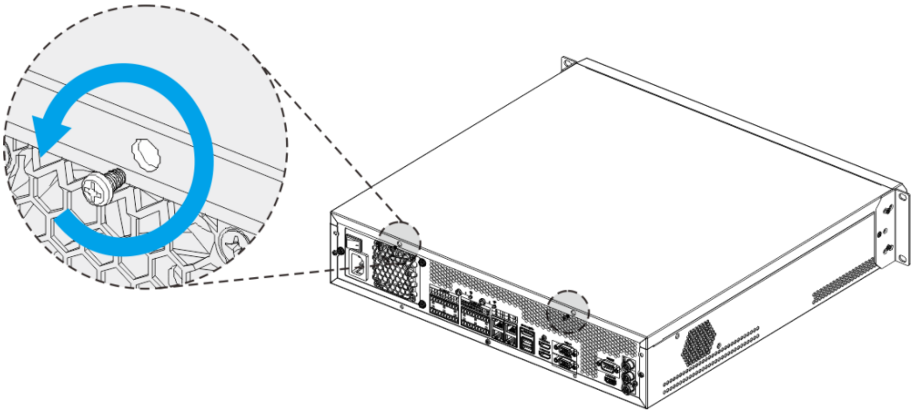
CAUTION

- The following contents apply to devices of 8-HDD and 12-HDD only.

- The following figures are for reference only. The actual product shall prevail.
- Devices of different models support different numbers of AI modules. See the actual situation.
- AI module does not support hot plug. If you need to replace the AI module, unplug the device power cable first. Otherwise, it will lead to file damage on the AI module.

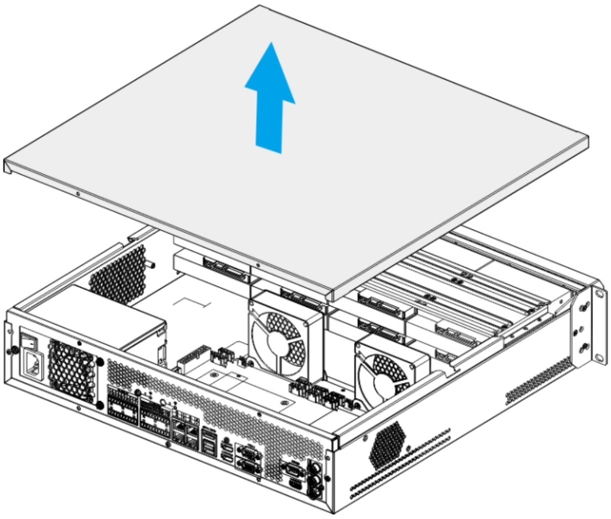
Step 1 Remove the screws on the rear panel of the Device. See Figure 2-1.

Figure 2-1 Install AI module (1)



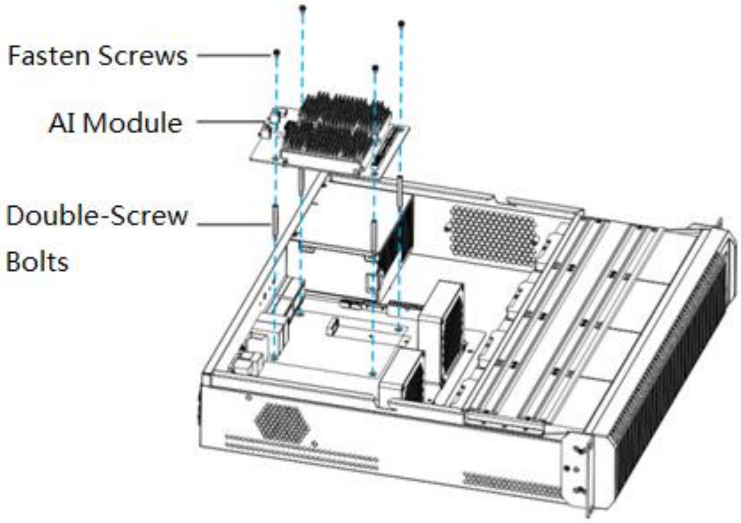
Step 2 Remove the case cover. See Figure 2-2.

Figure 2-2 Install AI module (2)



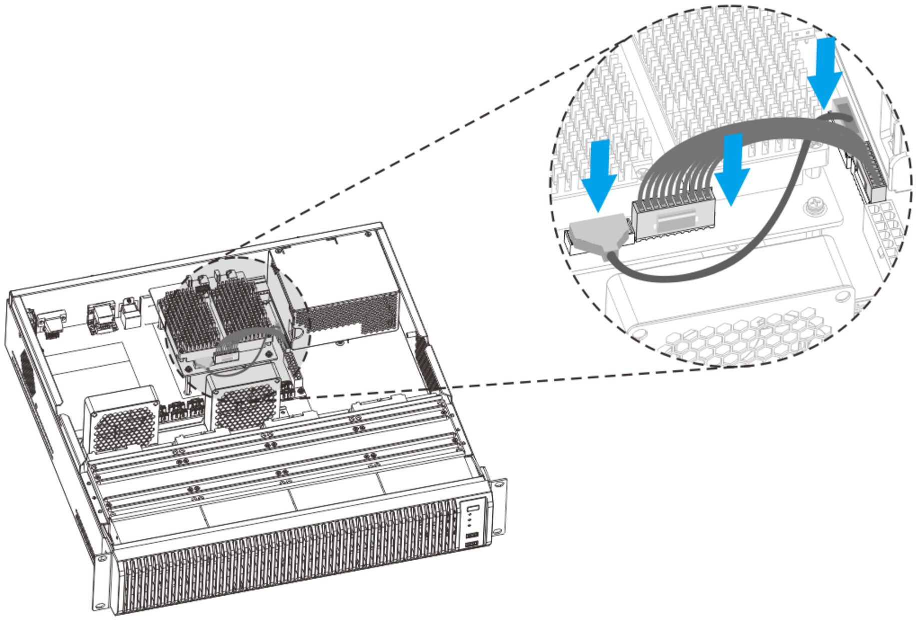
Step 3 Install the double-screw bolts and AI module and then fasten the screws. See Figure 2-3.

Figure 2-3 Install AI module (3)



Step 4 Connect the power cable and data cable of the AI module. See Figure 2-4.

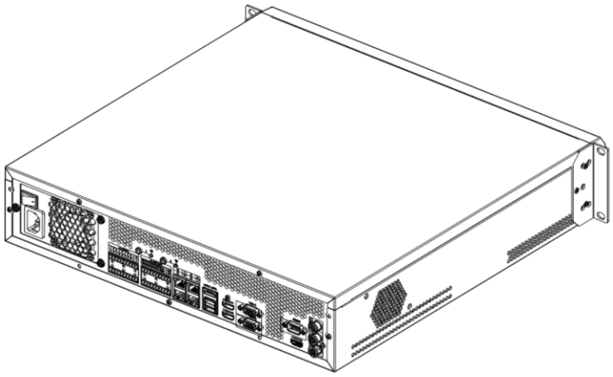
Figure 2-4 Install AI module (4)



Step 5 (Optional) Install the rest AI modules according to Step 3 to Step 4.

Step 6 Put back the cover and fasten the screws on the rear panel. See Figure 2-5.

Figure 2-5 Install AI module (5)



Step 7 Check AI module version.

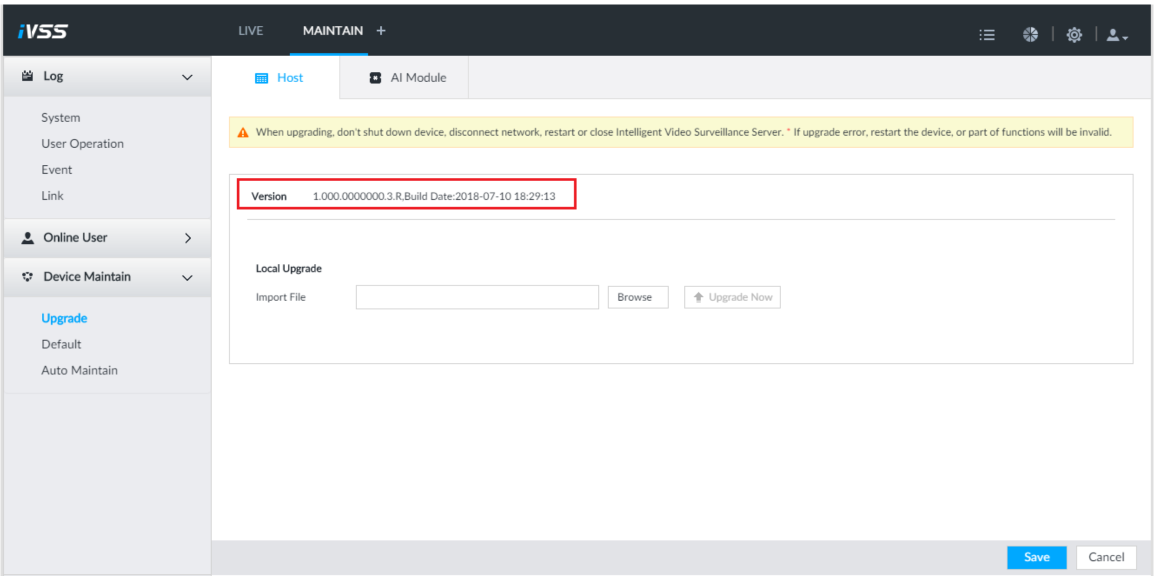
1) Turn on the Device.

2) Click ＋ on the LIVE interface and select MAINTAIN > Device Maintain > Upgrade”.

3) Click the Host tab and AI Module tab respectively to check if the host version matches with the AI module version. See Figure 2-6 and Figure 2-7.

   If the version is not matched, you need to upgrade the host. For details, see *IVSS User’s Manual*.

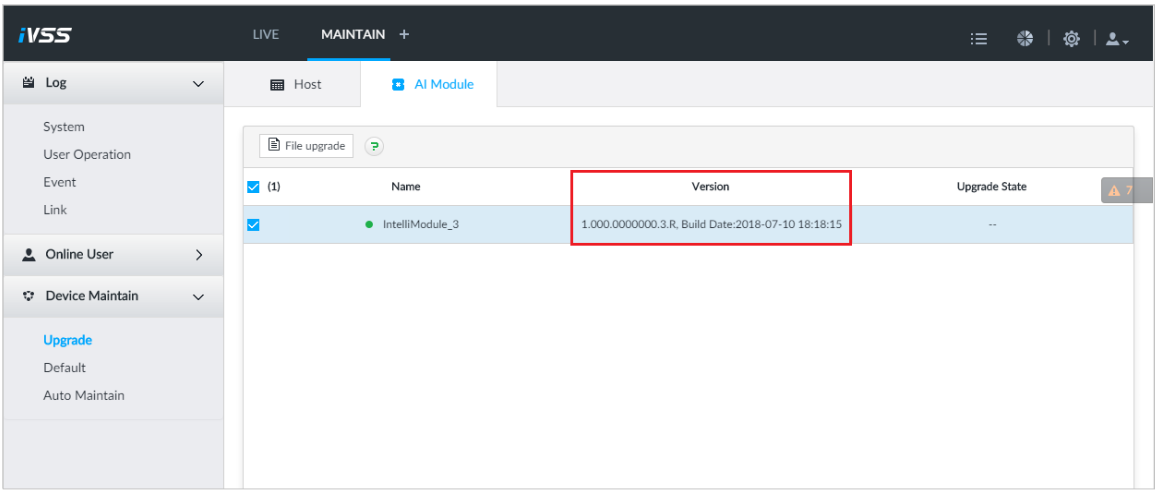
Figure 2-6 Host upgrade



When upgrading, don't shut down device, disconnect network, restart or close Intelligent Video Surveillance Server. * If upgrade error, restart the device, or part of functions will be invalid.

Version 1.000.0000000.3.R,Build Date:2018-07-10 18:29:13

Figure 2-7 AI module upgrade



☑ (1)	Name	Version	Upgrade State
☑	● IntelliModule_3	1.000.0000000.3.R, Build Date:2018-07-10 18:18:15	--

2.4 Connecting Cables

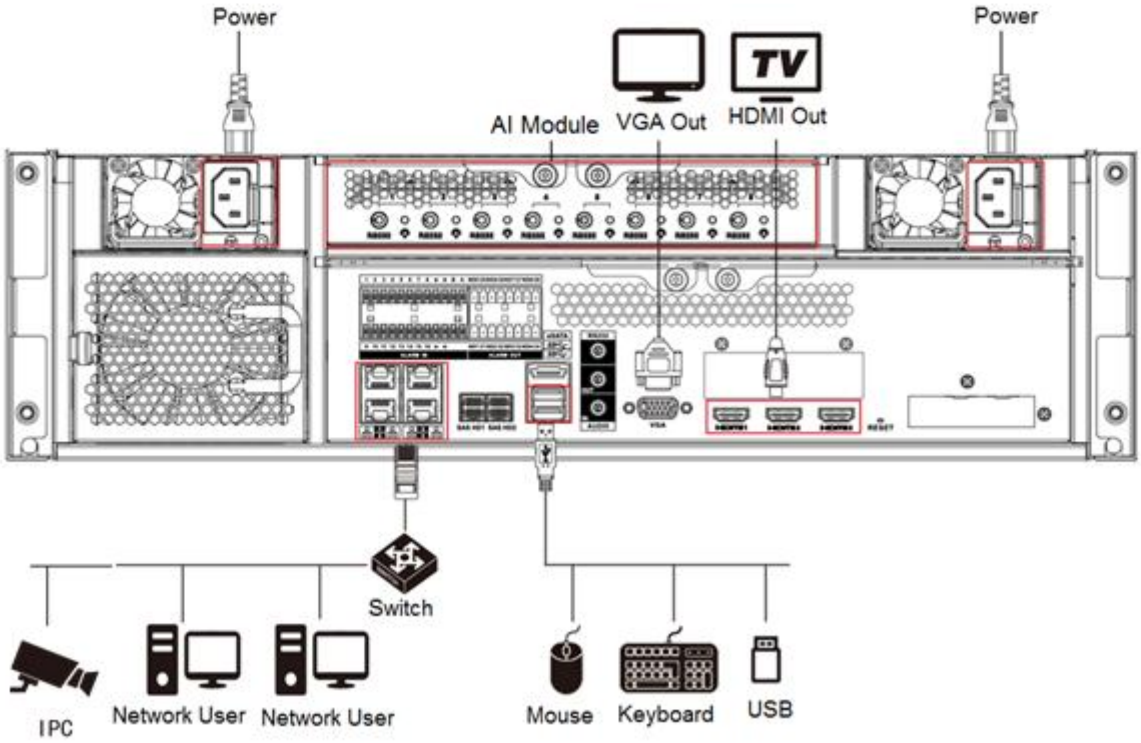
For the device connection, see Figure 2-8. The following figure is for reference only. The actual product shall prevail.

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

⚠CAUTION

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

Figure 2-8 Connection



3 Initial Configuration

If it is your first time to boot up the Device, please initialize the Device and set the basic information and functions.

3.1 Boot up

⚠**CAUTION**

Before the boot up, please make sure:

- The rated input voltage shall match the device power on-off button. Please make sure the power wire connection is OK.
- For device security, please connect all the other device cables first and then connect the Device to the power.
- Always use the stable current with little ripple interference, if necessary UPS is a best alternative measure.
- Some series products do not have power on-off button, connect the Device to the power socket to boot up directly.

Before you boot up the Device, see "2.4 Connecting Cables" to connect the cables.

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

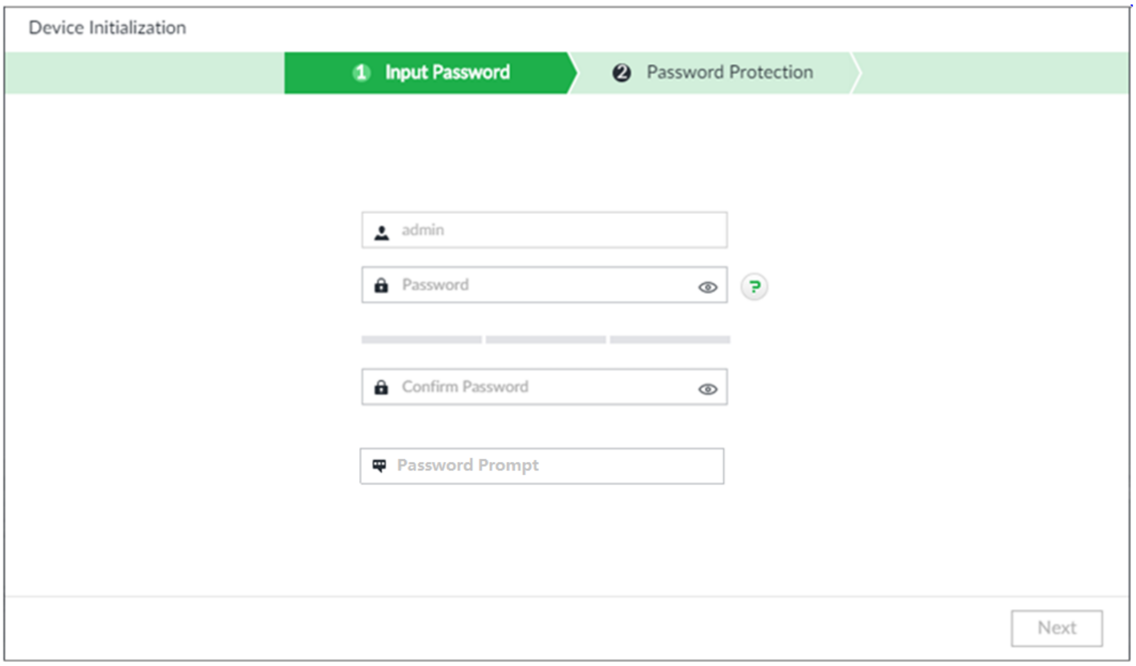
3.2 Initializing the Device

If it is your first time to use the Device, please set a login password of **admin** (system default user). At the same time, you can set proper password protection method.

Step 1 Turn on the Device.

Enter device initialization interface. See Figure 3-1.

Figure 3-1 Device initialization



Step 2 Set **admin** login password.

The password can be set from 8 characters through 32 characters and contain at least two types from number, letter and special character (excluding"'", """, ";", ":" and "&"). It is recommended to set password of high security according to the prompts.

Step 3 Click Next.

Enter password protection interface. See Figure 3-2.

Figure 3-2 Password protection

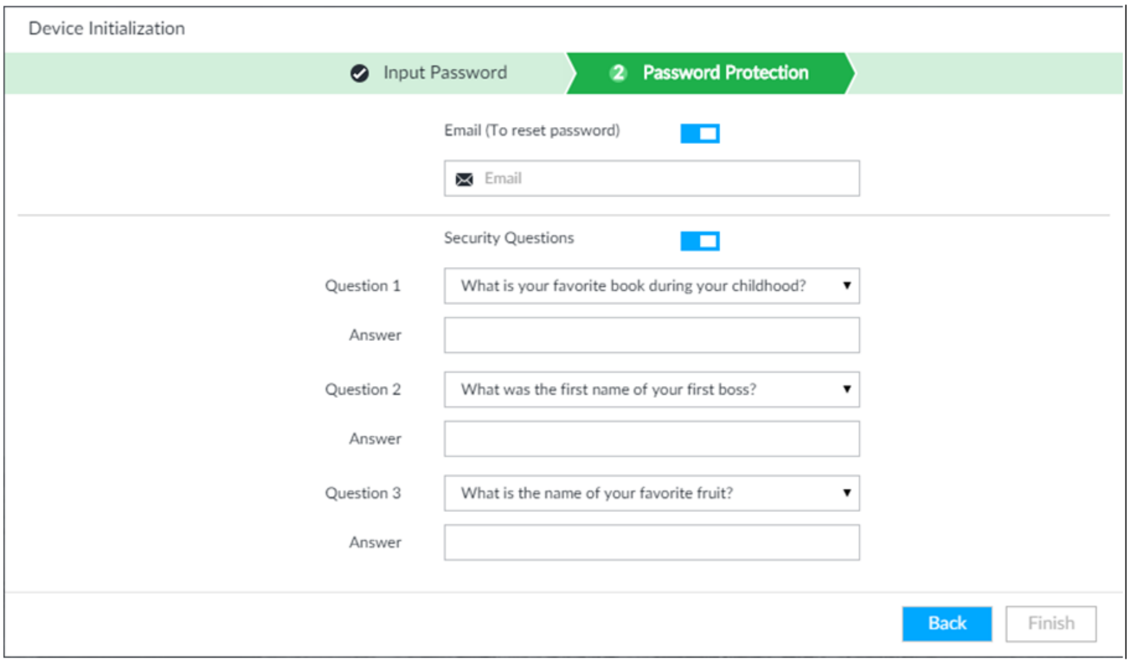

Device Initialization
Input Password
2 Password Protection
Email (To reset password)
Email
Security Questions
Question 1
What is your favorite book during your childhood?
Answer
Question 2
What was the first name of your first boss?
Answer
Question 3
What is the name of your favorite fruit?
Answer
Back
Finish

Figure 3-1

Step 4 Set password protection information. For details, see Figure 3-1.

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

NOTE

Click ▣ to cancel the email or security questions box.

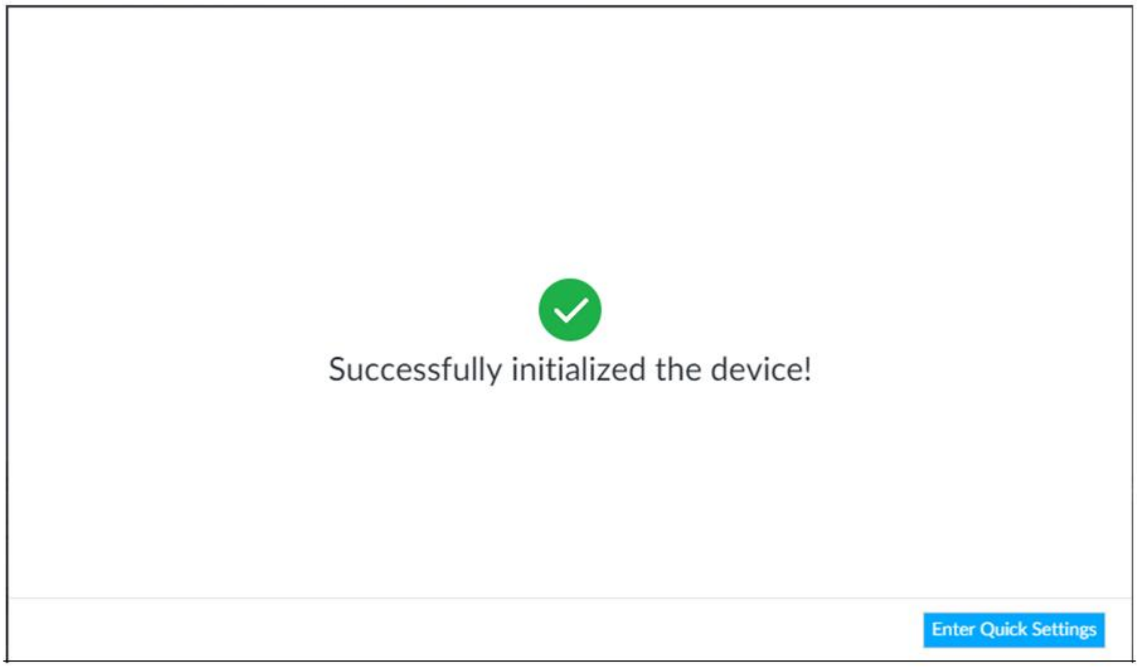
Table 3-1 Password protection description

Password protection	Note
Email	Input an email address for password reset. In case you forgot password in the future, input the security code you got on the assigned email to reset the password of **admin**. Select Main Menu > Setting > System > Account to set it. For details, see *User's Manual*.
Security question	Set security questions and corresponding answers. Properly answer the questions to reset **admin** password.

Step 5 Click Finish to complete device initialization.

System displays device initialization successful interface. See Figure 3-3. Click Enter Quick Settings to go to the quick setting interface. It is to set device basic information. For details, see "3.3 Quick Settings."

Figure 3-3 Successful



Successfully initialized the device!

3.3 Quick Settings

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

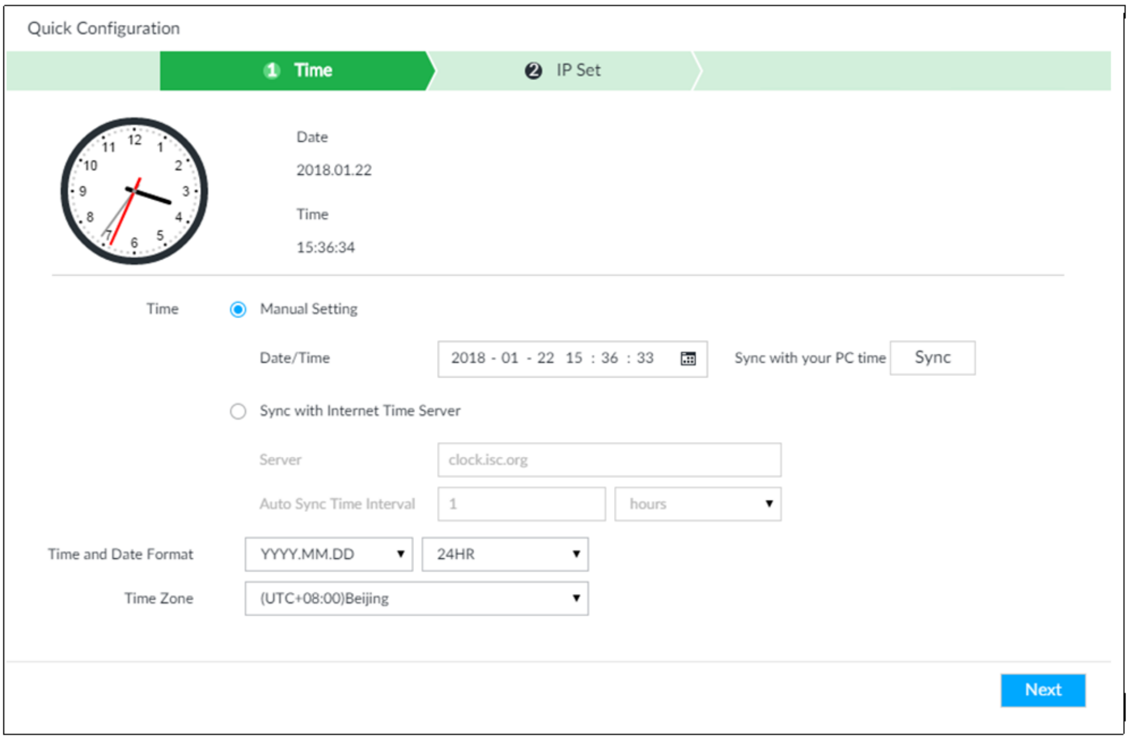
3.3.1 System Time

Set the device system time. You can select to enable NTP or not according to practical needs. If NTP is enabled, the system automatically syncs time with the NTP server.

Step 1 Click Enter Quick Settings on the successful initialization interface.

The Time interface is displayed. See Figure 3-4.

Figure 3-4 Time Setting



Quick Configuration

1 Time

2 IP Set

Date

2018.01.22

Time

15:36:34

Time ● Manual Setting

Date/Time 2018 - 01 - 22 15 : 36 : 33

Sync with your PC time Sync

○ Sync with Internet Time Server

Server clock.isc.org

Auto Sync Time Interval 1 hours

Time and Date Format YYYY.MM.DD 24HR

Time Zone (UTC+08:00)Beijing

Step 2 Configure the parameters. For details, see Table 3-2.

Table 3-2 Description of system time parameters

Parameter	Description
Time	Configure the system date and time. You can choose manual setting or auto sync to NTP server. ● Manual Setting: Select the Manual Setting check box and configure the date and time according to practical situation. ● Sync with Internet Time Server: Select the Sync with Internet Time Server check box, enter the IP address or domain name of the NTP server, and then enter the time interval.
Time and Date Format	Select the display format of system date and time.
Time Zone	Select the time zone that the Device locates.

Step 3 Click Next to save the configuration.

3.3.2 IP Address Settings

Modify device information such as IP address and DNS server according to the network plan.

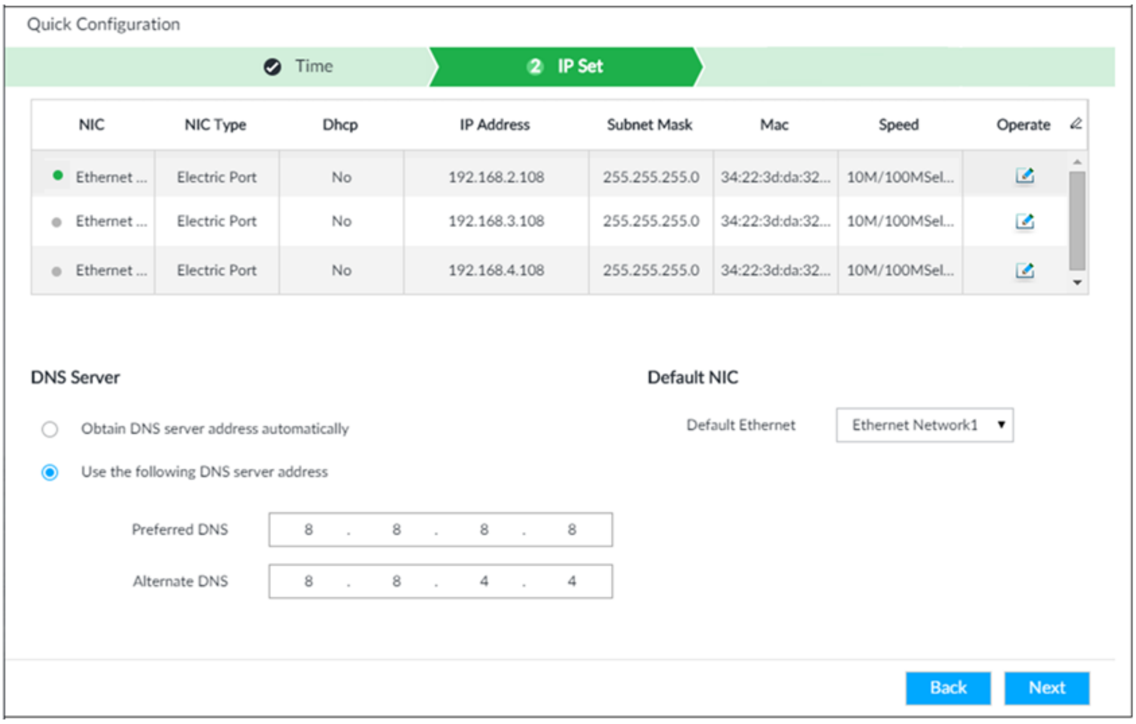
NOTE

There are four Ethernet ports available. Make sure that at least one port is connected to the network before setting the IP address.

Step 1 Click Next on the Time interface.

The IP Set interface is displayed. See Figure 3-5.

Figure 3-5 IP Setting



Quick Configuration

✓ Time | ② IP Set

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

DNS Server

○ Obtain DNS server address automatically

● Use the following DNS server address

Preferred DNS 8 . 8 . 8 . 8

Alternate DNS 8 . 8 . 4 . 4

Default NIC

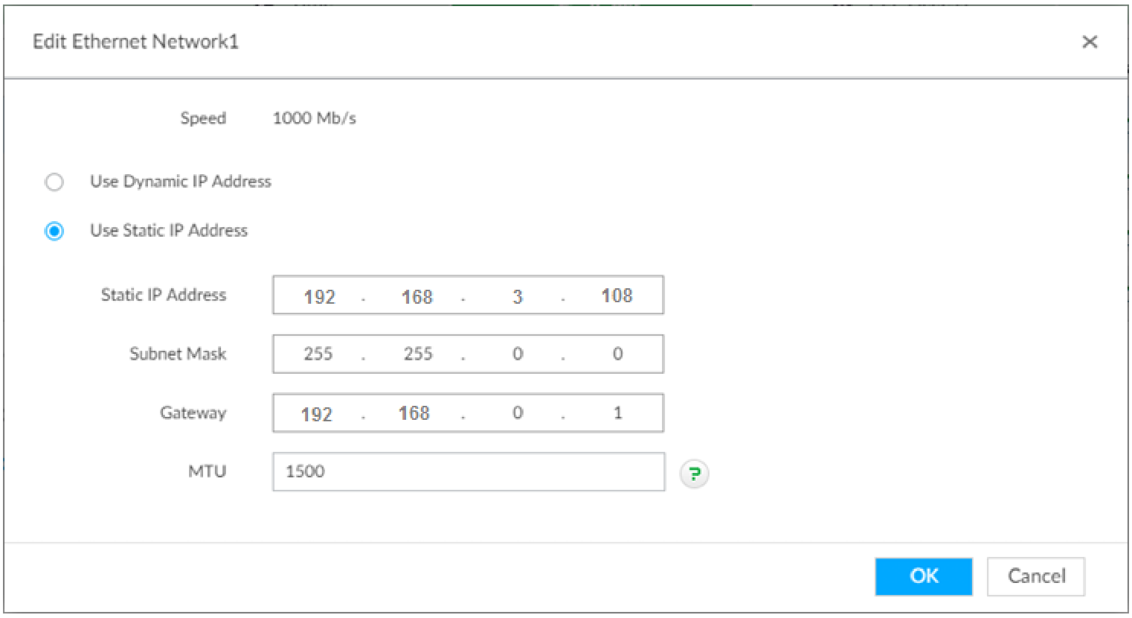
Default Ethernet: Ethernet Network1 ▾

Step 2 Configure the IP address.

1) Click ✎ corresponding to the Ethernet port.

The Edit Ethernet Network 1 interface is displayed. See Figure 3-6.

Figure 3-6 Editing Ethernet network



Edit Ethernet Network1

Speed 1000 Mb/s

○ Use Dynamic IP Address

● Use Static IP Address

Static IP Address 192 . 168 . 3 . 108

Subnet Mask 255 . 255 . 0 . 0

Gateway 192 . 168 . 0 . 1

MTU 1500

2) Configure the parameters.

- ◇ When there is a DHCP server in the network, select this check box and the system can allocate a dynamic IP address to the Device. There is no need to set IP address manually.
- ◇ When selecting using static IP address, you can enter the static IP address, subnet mask and gateway to set a fixed IP address for the Device.

CAUTION

Changing MTU value will result in NIC reboot and network offline. It will affect the running operations. Be careful!

3) Click OK.

The system returns to the IP Set interface.

Step 3 Configure the DNS server.

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

Step 4 Set the default NIC.

Click the Default Ethernet drop-down list to select the default NIC according to practical needs.

NOTE

Only the NIC connected to the network can be set as default NIC.

Step 5 Click Next to save the configuration.

3.3.3 P2P Settings

P2P is a peer to peer technology. You can scan the QR code to download cellphone APP without DDNS service or the port mapping or installing the transmission server. After registering the device to the APP, you can view the remote video and play back records.

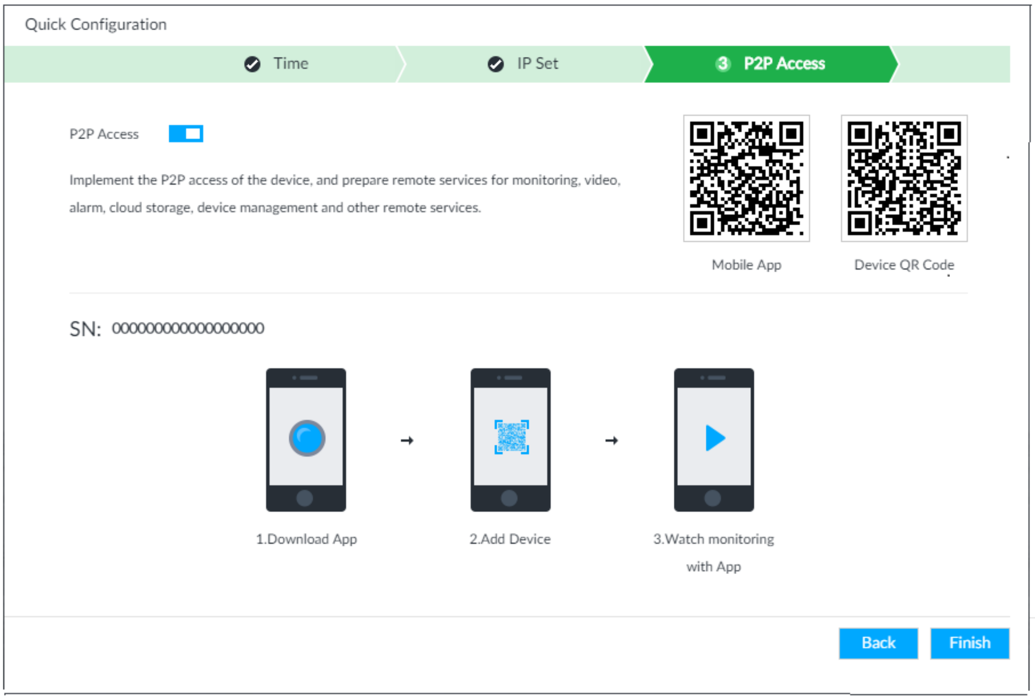
NOTE

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

Step 1 On IP setting interface, click Next.

Enter P2P interface. See Figure 3-7.

Figure 3-7 P2P



Quick Configuration

P2P Access

Implement the P2P access of the device, and prepare remote services for monitoring, video, alarm, cloud storage, device management and other remote services.

SN: 000000000000000000

Step 2 Click ▭ to enable P2P function.

Step 3 Click Finish to save the settings.

After the configuration, you can register a device to the APP to view remote video and play back records.

3.4 Registering Remote Device

After you register the remote device to the system, you can view the real-time video from the remote device and change remote device settings.

The Device supports two adding modes: Smart add and manual add.

- Smart add: It is to search the remote devices on the same network and then filter to register. It is useful if you do not know the exact IP address.
- Manual add: For some remote devices, you can input IP address, user name, and password to register.

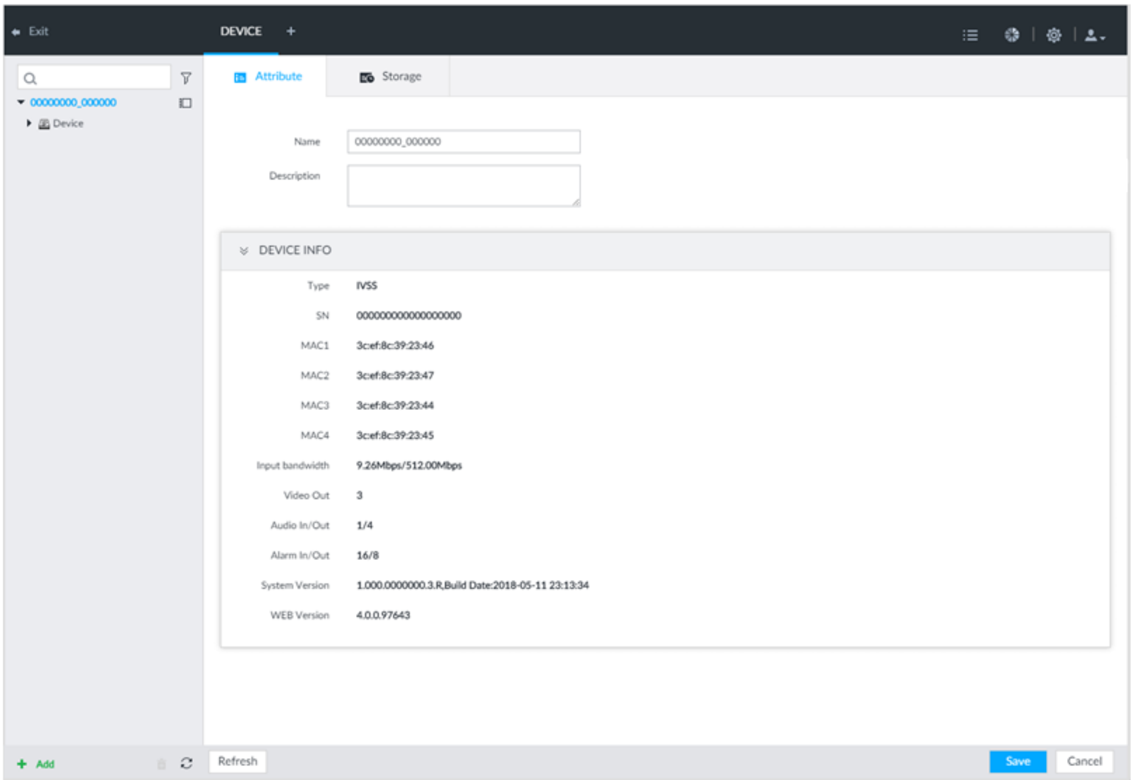
NOTE

- Uninitialized remote device cannot register to the system. For detailed information, see *User's Manual.*
- The following contents are introduced in the example of smart add. For the operations of manual add, see *User's Manual*.

Step 1 Click ⚙ on the top right corner of the window and select DEVICE.

The DEVICE interface is displayed. See Figure 3-8.

Figure 3-8 Device manager



Name: 00000000_000000

Description:

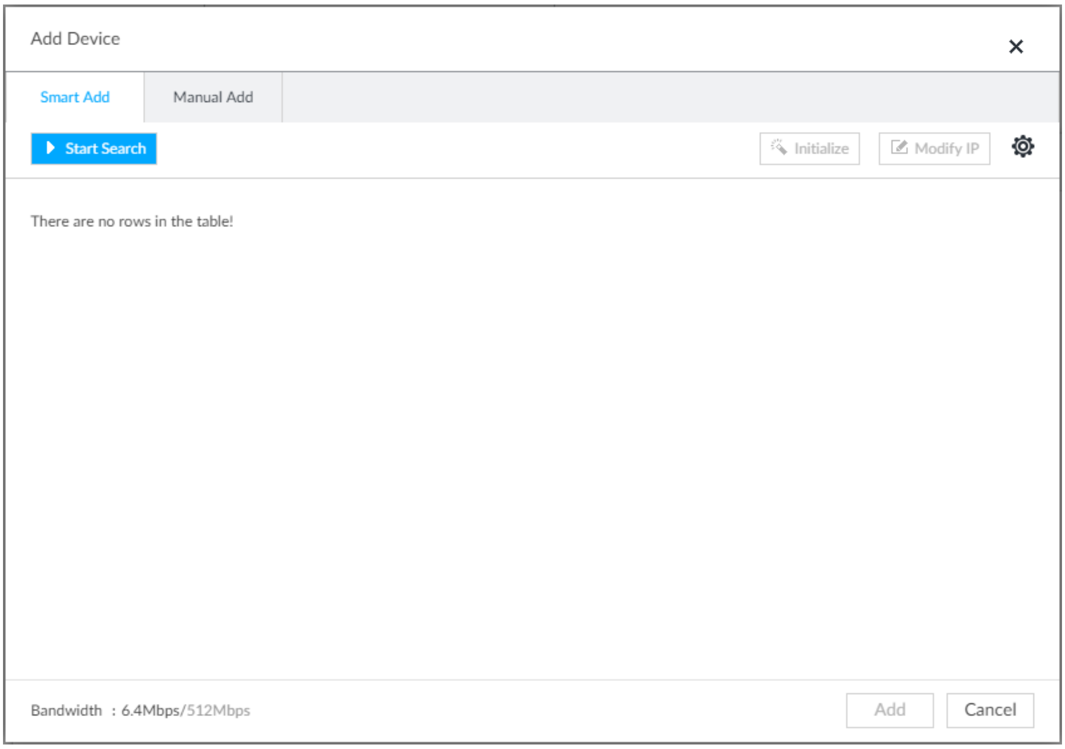
DEVICE INFO

Type	IVSS
SN	000000000000000000
MAC1	3c:ef:8c:39:23:46
MAC2	3c:ef:8c:39:23:47
MAC3	3c:ef:8c:39:23:44
MAC4	3c:ef:8c:39:23:45
Input bandwidth	9.26Mbps/512.00Mbps
Video Out	3
Audio In/Out	1/4
Alarm In/Out	16/8
System Version	1.000.0000000.3.R,Build Date:2018-05-11 23:13:34
WEB Version	4.0.0.97643

Step 2 Click ✚ or click Add and select the Smart Add tab.

The Smart Add interface is displayed. See Figure 3-9.

Figure 3-9 Smart add



Add Device ✕

Smart Add | Manual Add

▶ Start Search | Initialize | Modify IP | ⚙

There are no rows in the table!

Bandwidth : 6.4Mbps/512Mbps

Add | Cancel

Step 3 Search remote device.

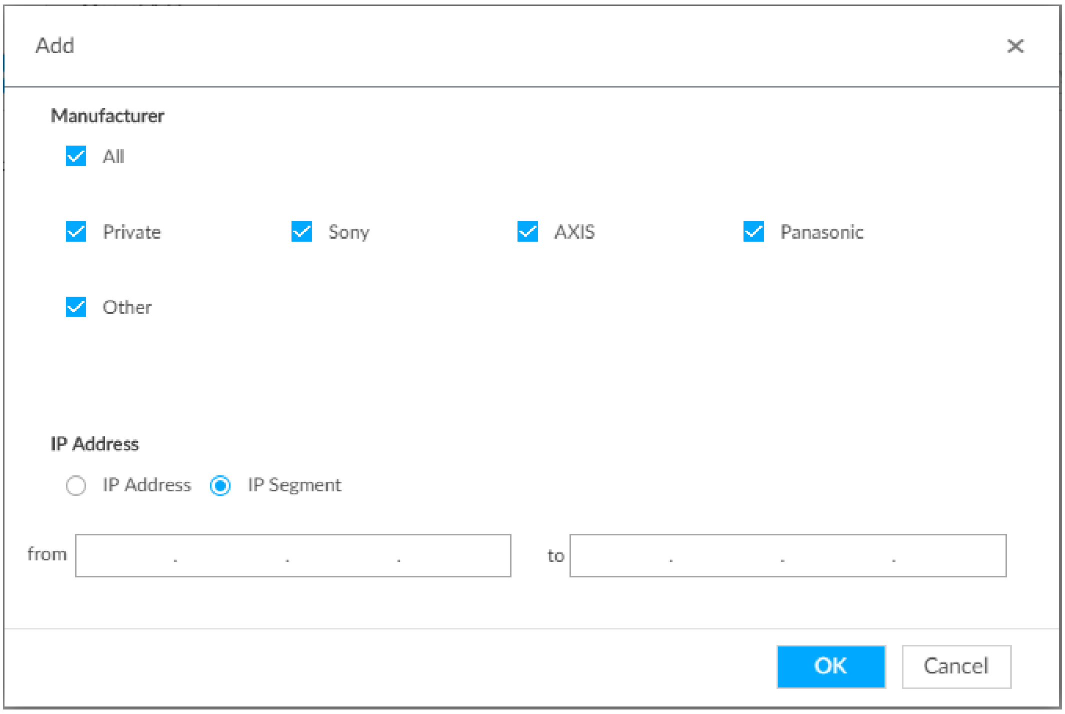
NOTE

If there is no specified search condition, the system searches for the remote devices in the same IP segment by default.

1) Click ⚙.

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

Figure 3-10 Remote device register



Add ✕

Manufacturer

☑ All

☑ Private ☑ Sony ☑ AXIS ☑ Panasonic

☑ Other

IP Address

○ IP Address ● IP Segment

from . . . to . . .

OK | Cancel

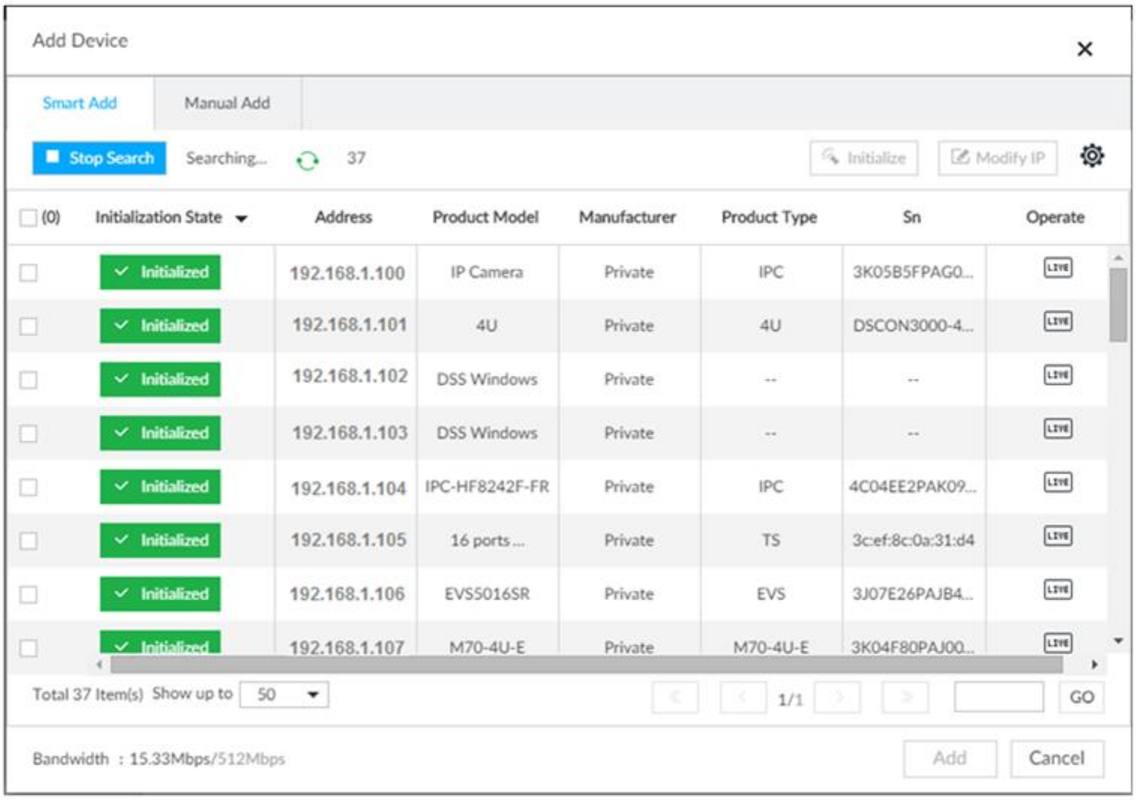
2) Select the manufacturer and enter the IP address to search for.

- IP address: Enter the IP address of the remote device. The system only searches for the corresponding remote device.

- IP segment: Enter the IP segment range of the remote device. The system searches for the remote devices within the segment range.

3) Click OK to save the configuration.
   The system returns to the Add Device interface.
4) Click Start Search.
   The system starts to search the remote devices and displays the results. See Figure 3-11.

Figure 3-11 Search results



□ (0)	Initialization State	Address	Product Model	Manufacturer	Product Type	Sn	Operate
□	✓ Initialized	192.168.1.100	IP Camera	Private	IPC	3K05B5FPAG0...	LIVE
□	✓ Initialized	192.168.1.101	4U	Private	4U	DSCON3000-4...	LIVE
□	✓ Initialized	192.168.1.102	DSS Windows	Private	--	--	LIVE
□	✓ Initialized	192.168.1.103	DSS Windows	Private	--	--	LIVE
□	✓ Initialized	192.168.1.104	IPC-HF8242F-FR	Private	IPC	4C04EE2PAK09...	LIVE
□	✓ Initialized	192.168.1.105	16 ports ...	Private	TS	3c:ef:8c:0a:31:d4	LIVE
□	✓ Initialized	192.168.1.106	EVS5016SR	Private	EVS	3J07E26PAJB4...	LIVE
□	✓ Initialized	192.168.1.107	M70-4U-E	Private	M70-4U-E	3K04F80PAJ00...	LIVE

Total 37 Item(s) Show up to 50

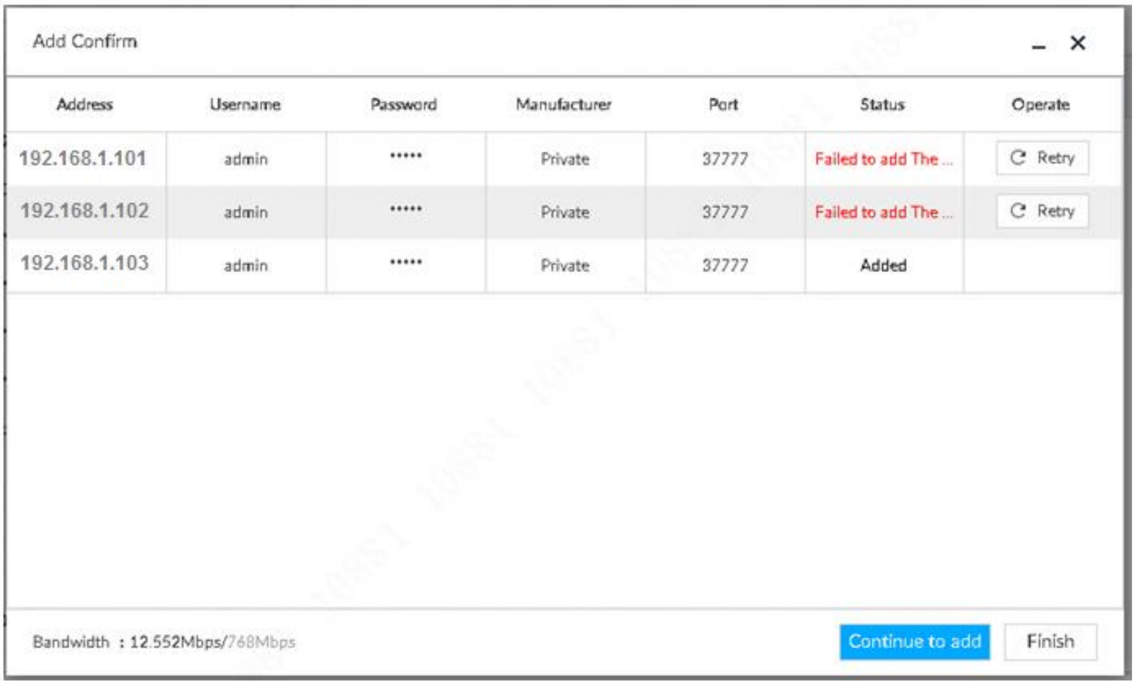
1/1 GO

Bandwidth : 15.33Mbps/512Mbps

Step 4 Register remote device.

- Add 1-channel remote device.
  Select a remote device and then click Add. The Device begins adding remote device and pops up confirmation interface. See Figure 3-12.

Figure 3-12 Add confirmation (1)



Add Confirm

Address	Username	Password	Manufacturer	Port	Status	Operate
192.168.1.101	admin	•••••	Private	37777	Failed to add The ...	Retry
192.168.1.102	admin	•••••	Private	37777	Failed to add The ...	Retry
192.168.1.103	admin	•••••	Private	37777	Added	

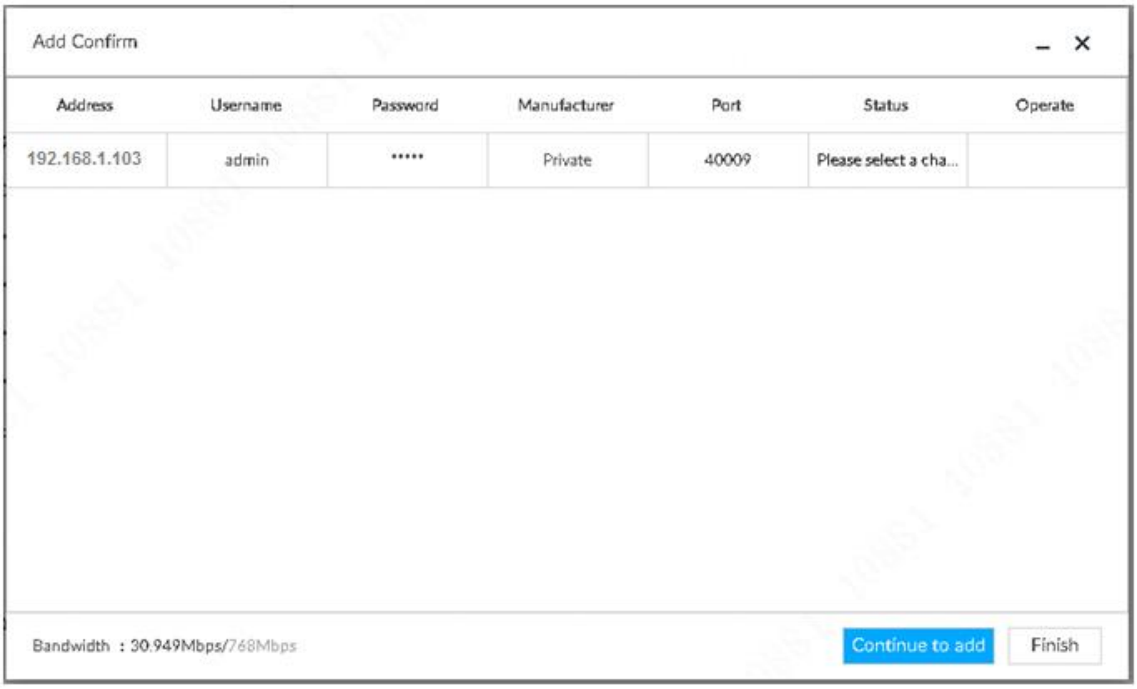
Bandwidth : 12.552Mbps/768Mbps

- Add multiple-channel remote device

1) Select the remote devices and click Add.

The Add Confirm interface is displayed. See Figure 3-13.

Figure 3-13 Add confirmation (2)



Add Confirm

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

Bandwidth : 30.949Mbps/768Mbps

2) Double-click Please select a channel and select the channel you need to add.

Click ▼ , enter the key words in the search box, and then you can search the channel quickly.

3) Click OK to add the selected channel.

Step 5 Click Continue to add or Finish.

- Continue to add: System goes back to Smart Add interface to add more remote devices.

- Finish: Complete adding remote device. System displays Device Manager interface to view the newly added remote device information.

4 Business Operations

4.1 Logging In

After booting up the Device, input the corresponding user name and password to log in.

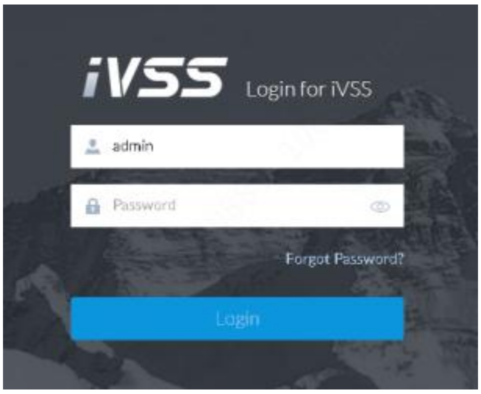
NOTE

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

Step 1 Turn on the Device.

Enter login interface. See Figure 4-1.

Figure 4-1 Login



Step 2 Enter the username and password.

NOTE

- Default user name is admin. The password is that you set during initialization process. For your device safety, change the admin password regularly and keep it well.
- In case you forgot password, click Forgot password to reset it. For details, see *User's Manual*.

Step 3 Click Login

Enter the main interface. See Figure 4-2. For details, see Table 4-1.

Figure 4-2 IVSS main interface

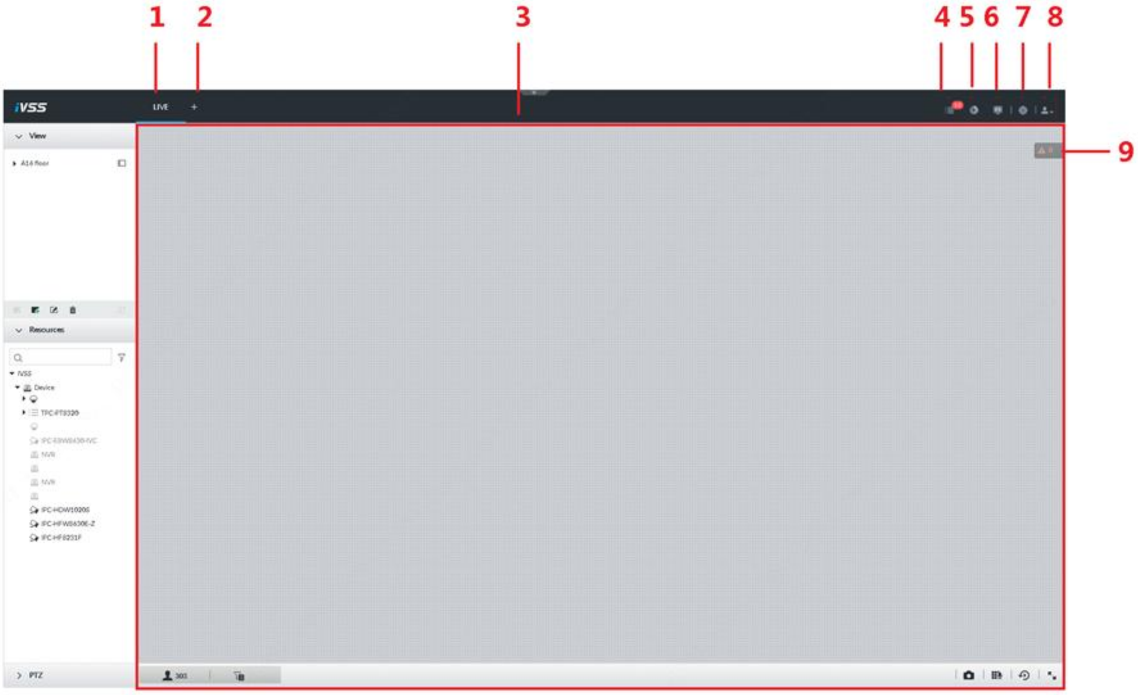


Table 4-1 Main interface description

SN	Name	Description
1	Task column	It is to display enabled application icon. Move the mouse to the app and then click × to close the app. **NOTE** The preview function is enabled by default and cannot be closed.
2	Add icon	Click to display or hide app interfaces. On App interface to view or enable the applications.
3	Operation interface	It is to display currently enabled app operation interface.
4	System info	Click to view system information.
5	Background task	Click to view the background running task information.
6	Multiple-screen control	Click to control the local screen. **NOTE** This function is for local menu only.
7	System settings	Click to enter system setting interface.
8	Login user	Click it to change user password, lock user, log out user, reboot device or close device. **NOTE** Reboot and shutdown function is for local menu only.

SN	Name	Description
9	Alarm list	It is to display currently unprocessed alarm event amount. Click the icon to view detailed alarm information. **NOTE** Press and hold down the icon and move up and down to adjust the icon position.

4.2 Preview and Monitor

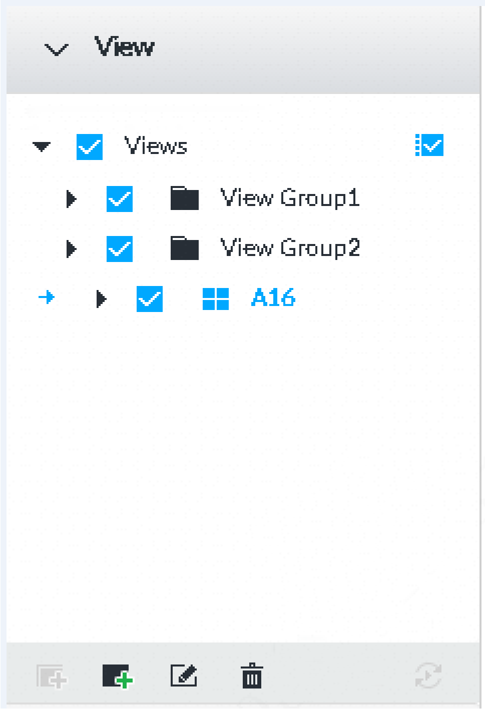
After logging in the Device, system displays Live interface by default.

4.2.1 View Management

View is a video component of several remote devices. Go to the view pane at the top left corner of the Live interface to view or call the view. See Figure 4-3.

- System has created View Group by default. Please create more views or view groups under the View Group.
- Double click the view or drag the view to the play pane on the right side and the system begins to play the real-time video from the remote device.
- Click ☐ to select Views and its sub-node.

Figure 4-3 View



4.2.1.1 Create View

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

NOTE

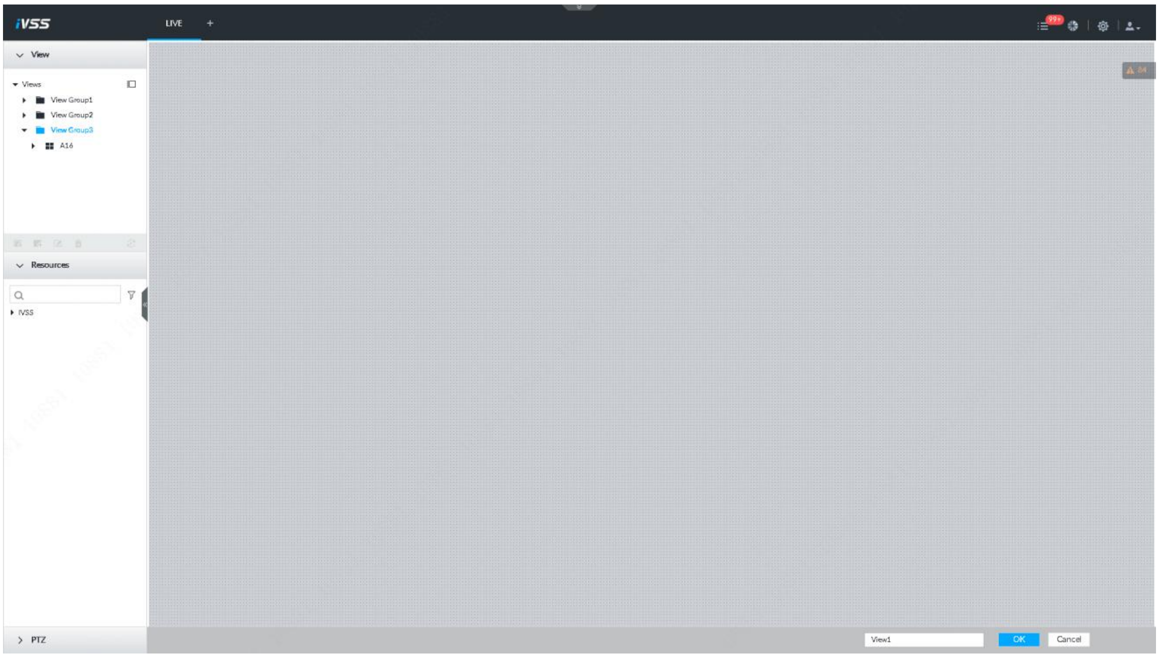
Before you create view, make sure you have added the remote device. For details, see "3.4 Registering Remote Device."

Step 1 Follow the steps listed below to create view.

- Select View group, click , and then select Add view.
- Right-click the view group and select Add view.

Enter edit view interface. See Figure 4-4.

Figure 4-4 Edit view (1)



Step 2 Double click a remote device on the device tree, or drag the remote device to the right pane.

After adding one remote device, the view edit pane displays layout split line. See Figure 4-5.

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

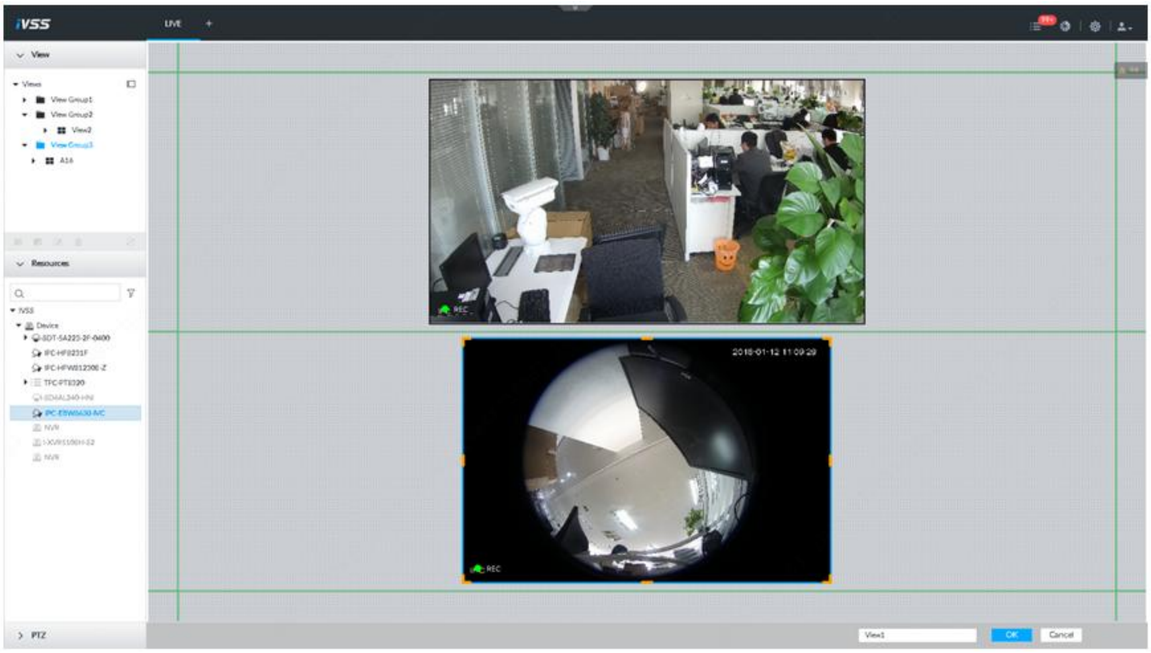
NOTE

- Device automatically creates the view grids amount accoridng to the selected remote device amount. Device max supports 36 view windows.
- Device automaticlaly allocates the view window size according to the remote device resolution by default. If the Device cannot get the remote device resolution

or the remote device has no resolution, device automatically adjusts view windiow size according to remote device amount and playback pane.

- When adjusting view window position, drag the view window to the layout grid of the green background color. Cannot drag the view window to the layout grid if its background color is orange.

Figure 4-5 Edit view (2)



Step 3 Set view name.

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

Step 4 Click OK to save the settings.

System pops up the successful interface.

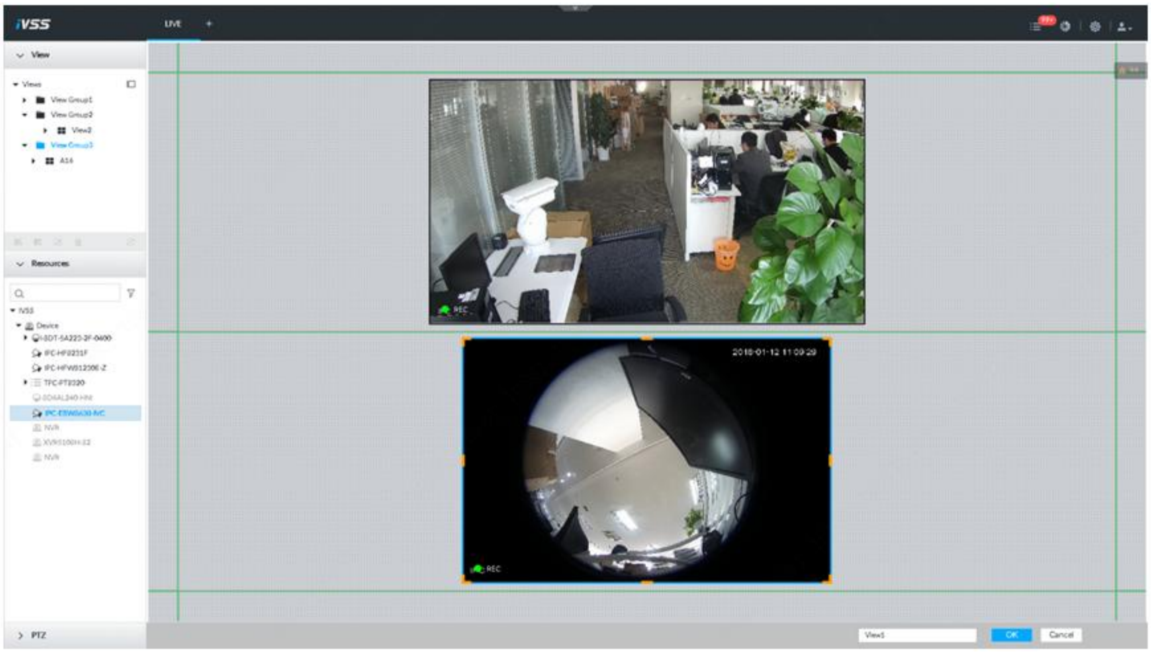
4.2.1.2 Enable view

Follow the steps listed below to enable view.

- Right click view and then select Open.
- Double click view.

Enter view window. See Figure 4-6.

Figure 4-6 View window



When the view is enabled, you can do operations such as changing video position and zooming in the video window.

NOTE

- Move your mouse to the view window and the system displays window task column. You can snapshot view or close video window.
- Right click view window and you can switch bit streams, set digital zoom, etc.

Table 4-2 Description of view functions

Name	Function
Exchange window position	Press and hold down one view window and drag it to another view window, it is to exchange the view window position. **NOTE** The exchanging window position operation is valid only once. Disable and then enable view again, the view window restore original position. If you want to change view window position permanently, go to the view edit mode to set. For details, see *User's Manual*.
Zoom in video window	● Once the current view window number is too many (more than 9),click one view window and the system displays current view window at the center of the window in the zoom in mode. Click any other blank position and you can view window restores original size. ● Double click a view window and the system displays view window at one window. Double click view window again or click any blank position, and then the view window restores original size.
Add view window	On the device tree, double click the remote device or drag the remote device to the right pane, and then you can add remote device to the current view. Drag the remote device to the view window to replace the original remote device. **NOTE** The modified view layout is valid only for once if you do not click OK. Close and enable view again, the view layout restores original layout.

Name	Function
Close view window	Move the mouse to one view window, click ✕ to close the view window. **NOTE** Close view window and the system automatically adjusts view layout according to the rest remote device number and play pane free space.

4.2.2 Preview

After enabling AI detection function, go to the preview interface to view AI detection results.

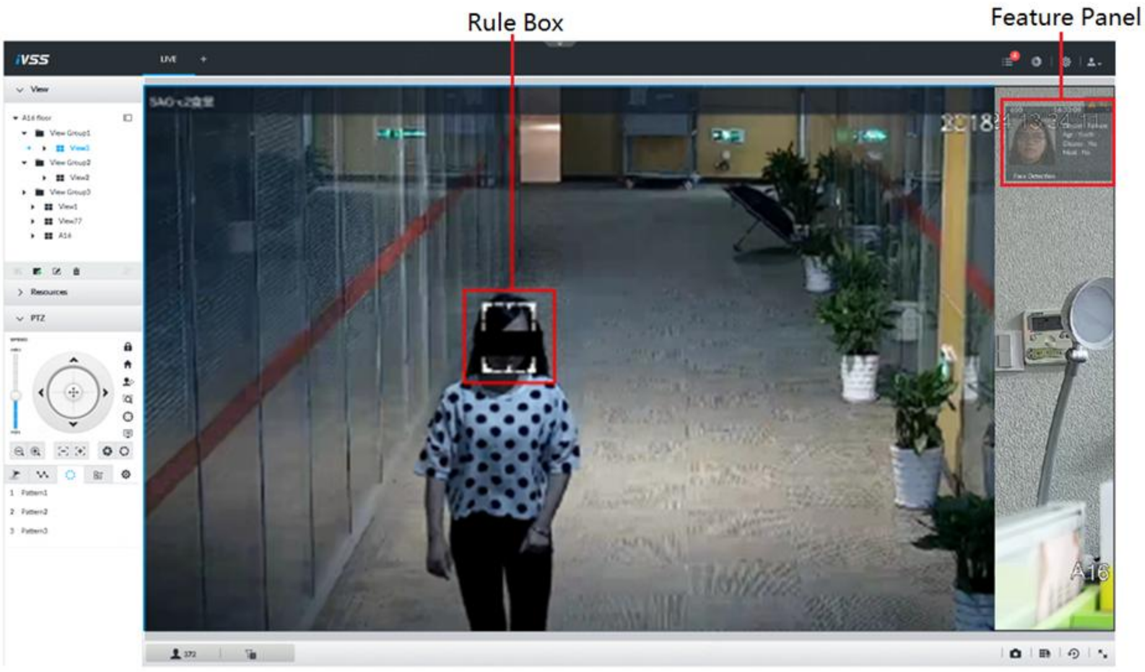
NOTE

To enable AI detect function, see *User's Manual*.

Go to the Live interface, enable view and the system displays view video. See Figure 4-7.

- The view window displays currently detected human face rule rectangle.
- The view window displays properties pane such as human face detected image and human face comparison results on the right pane.

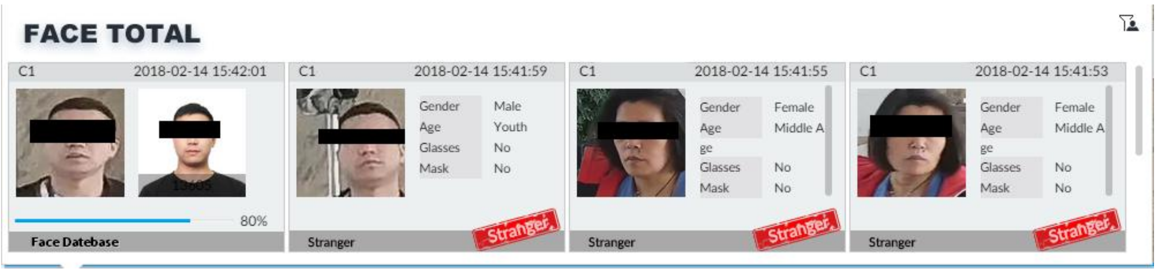
Figure 4-7 Preview



4.2.2.1 View image

Click 👤 on the LIVE interface to view detected images. See Figure 4-8.

Figure 4-8 AI detection images



FACE TOTAL

C1 2018-02-14 15:42:01
80%
Face Datebase

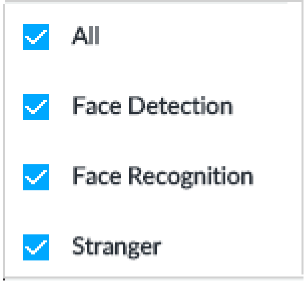
C1 2018-02-14 15:41:59
Gender Male
Age Youth
Glasses No
Mask No
Stranger

C1 2018-02-14 15:41:55
Gender Female
Age Middle Age
Glasses No
Mask No
Stranger

C1 2018-02-14 15:41:53
Gender Female
Age Middle Age
Glasses No
Mask No
Stranger

- Click ⏷ to screen the images. See Figure 4-9.

Figure 4-9 Filter



☑ All

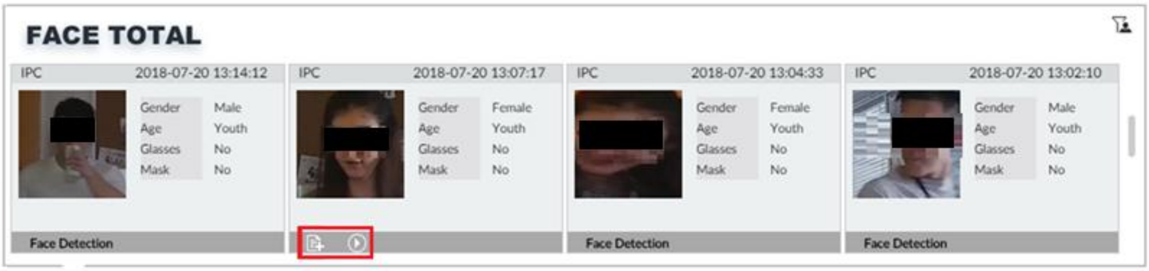
☑ Face Detection

☑ Face Recognition

☑ Stranger

- Move the cursor to the face image and system displays the icon ⊞ on the bottom left corner. See Figure 4-10. Click ⊞ to add this image to the face database.

Figure 4-10 AI detection images (2)



FACE TOTAL

IPC 2018-07-20 13:14:12
Gender Male
Age Youth
Glasses No
Mask No
Face Detection

IPC 2018-07-20 13:07:17
Gender Female
Age Youth
Glasses No
Mask No

IPC 2018-07-20 13:04:33
Gender Female
Age Youth
Glasses No
Mask No
Face Detection

IPC 2018-07-20 13:02:10
Gender Male
Age Youth
Glasses No
Mask No
Face Detection

- Move the cursor to the detected face image and click ⊙ or double-click the image and the system plays the record 20 seconds before and after the image. See Figure 4-11.

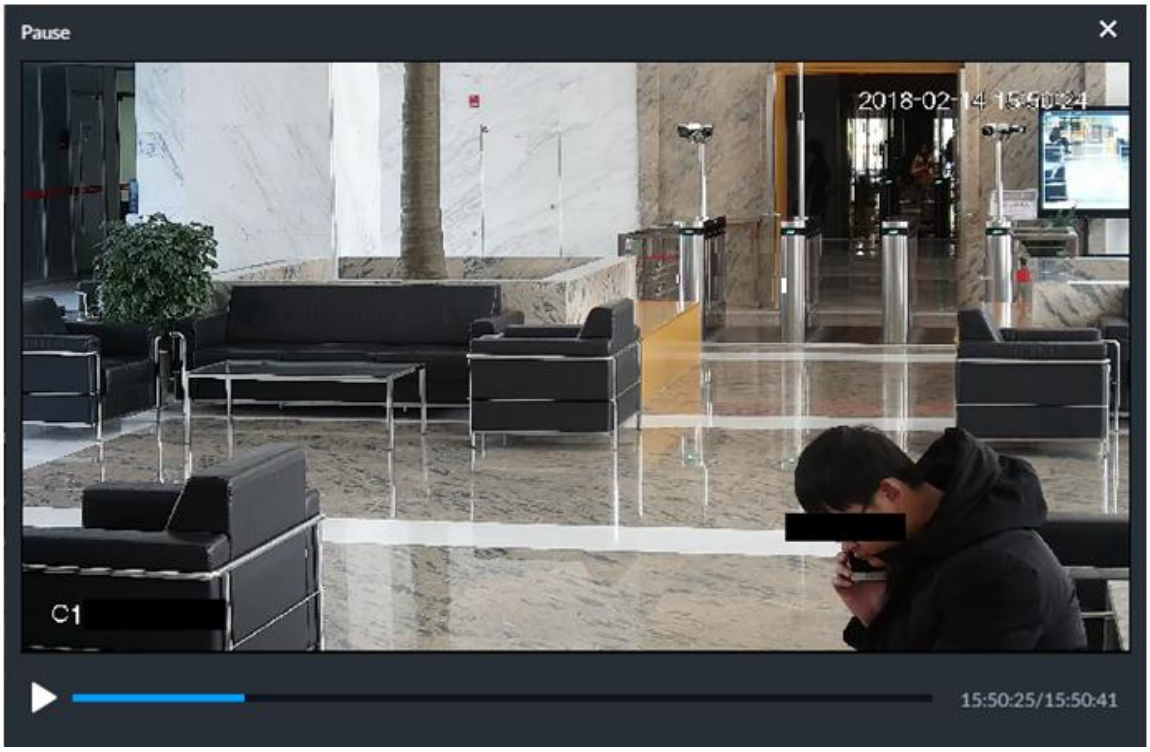
NOTE

The system supports this function only when a record is available.

◇ Click ‖ to pause and the icon becomes ▶. Click ▶ to continue.

◇ Click ✕ to exit the record.

Figure 4-11 Record



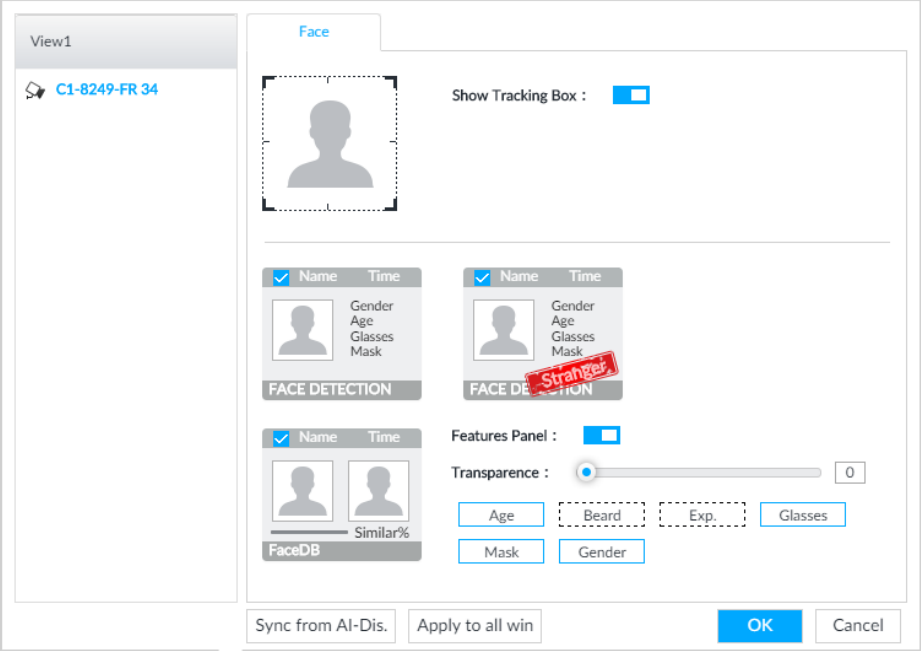
4.2.2.2 AI display settings

On the preview interface, click . Enter human face interface. See Figure 4-12. It is to set AI detection results displayed rule and features pane transparency.

NOTE

- Click Sync from AI-Dis and you can get global intelligent detection display rule from the device directly. For details, see *User's Manual.*
- Click Apply to all windows to copy current configuration to other window(s).

Figure 4-12 Human face



Show Tracking Box :

Features Panel :

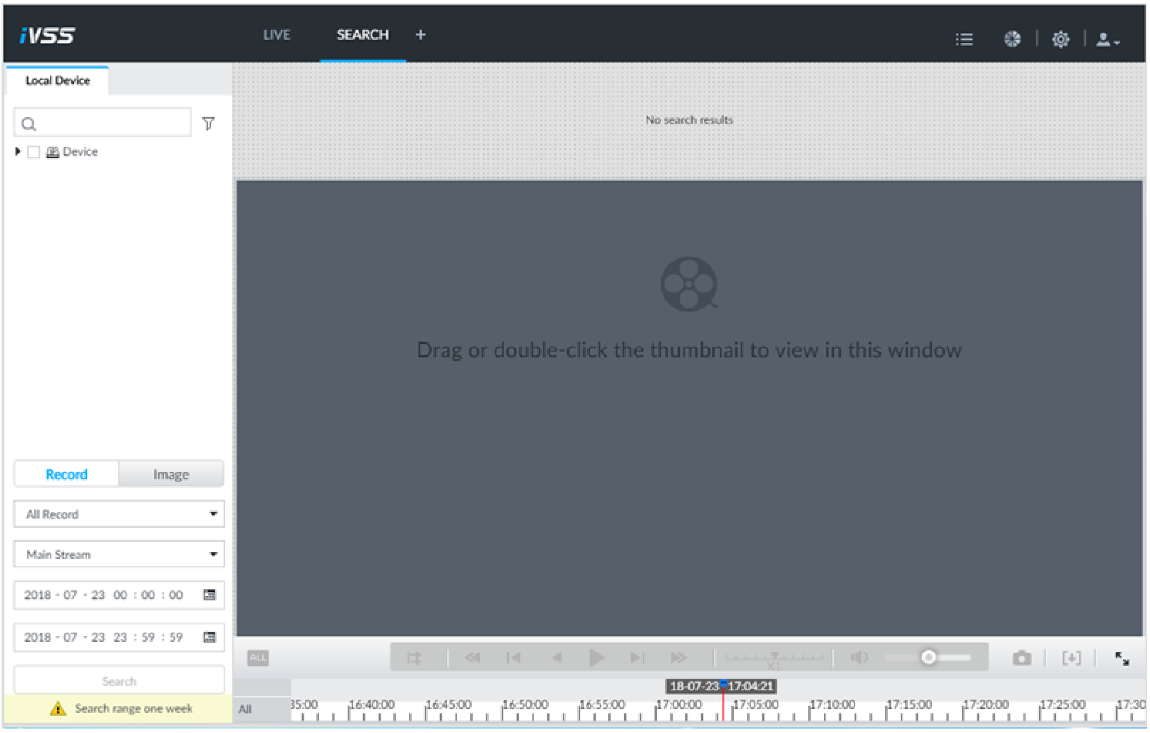
Transparence : 0

4.3 Record Playback

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

Step 1 On the Live interface, click + and then select Search.

Enter Search interface. See Figure 4-13.



No search results

Drag or double-click the thumbnail to view in this window

All Record

Main Stream

2018 - 07 - 23 00 : 00 : 00

2018 - 07 - 23 23 : 59 : 59

Search range one week

Figure 4-13 Playback (1)

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

Step 3 Set record type and record search time.

Device displays search results. The record thumbnail is at the top of the remote device. The time bar displays the record period (green color means there is a record).

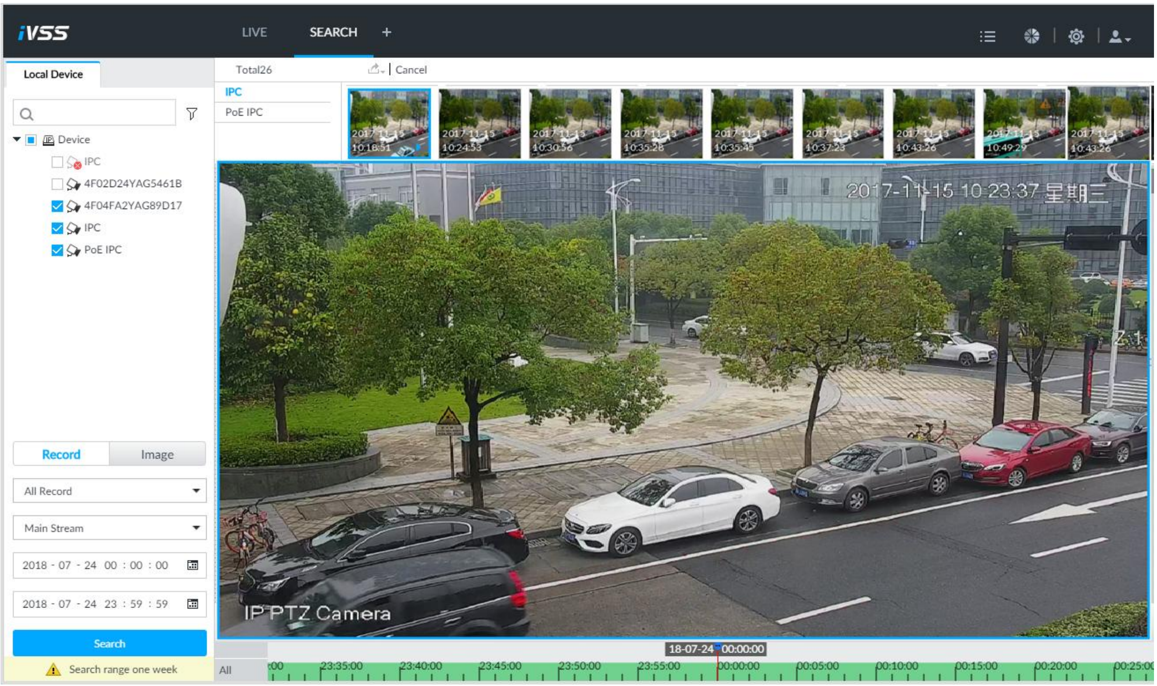
Step 4 Drag the thumbnail to the playback window or double click the thumbnail.

Device begins to play the record. See Figure 4-14.

NOTE

- The playback window amount depends on the thumbnail amount or you can drag to set. System max supports 16 windows. System automatically adjusts each window size according to the playback file original rate.
- Thumbnail with ▶: It means system is playing record file of current thumbnail.
- Use the playback control bar for synchronization playback, slow playback, fast playback, backward playback, frame by frame playback and etc. For details, see *User's Manual.*

Figure 4-14 Playback (2)



All Record

Main Stream

2018 - 07 - 24 00 : 00 : 00

2018 - 07 - 24 23 : 59 : 59

4.4 AI Detection Settings

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

4.4.1 Enabling AI Plan

The AI detection function becomes valid once you enabled AI plan.

NOTE

- Some remote devices do not support AI plan. See the actual interface.
- The interface might vary since the remote device supports different AI functions. See the actual interface.

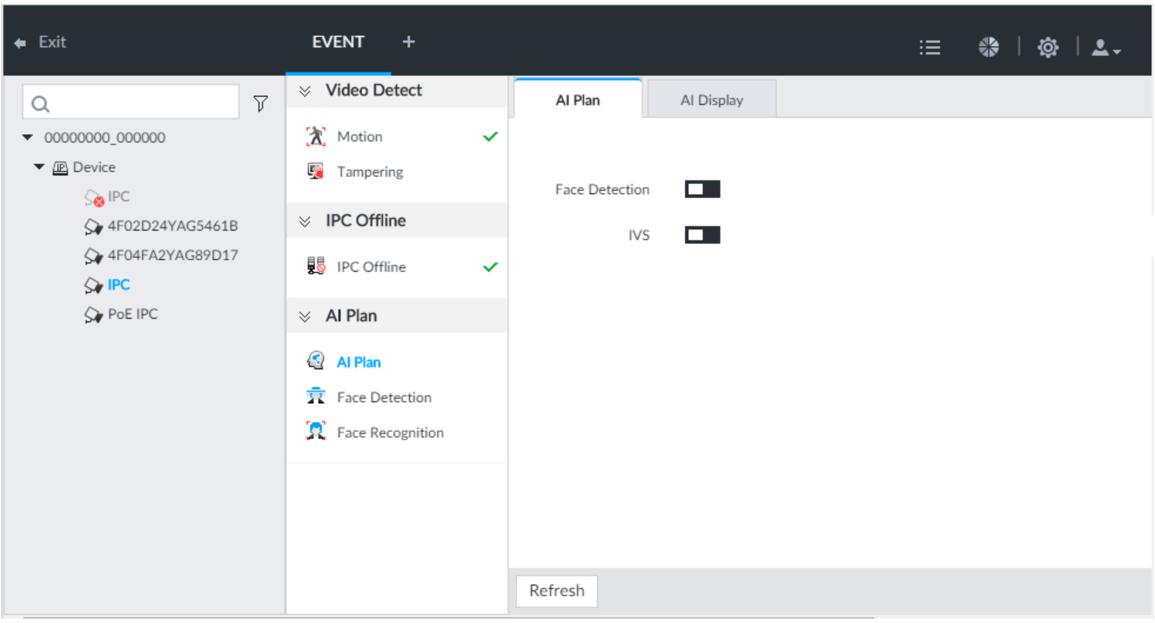
Step 1 Click ⚙ and select EVENT.

The EVENT interface is displayed.

Step 2 After selecting the remote device, select AI Plan > AI Plan > AI Plan.

The AI Plan interface is displayed. See Figure 4-15.

Figure 4-15 AI plan



Step 3 Click ◧ to enable the corresponding AI plan.

Step 4 Click Save to save the configuration.

4.4.2 Human Face Detection

It is to analyze the videos collected by the IPC and the system triggers alarm once any human face information is detected.

NOTE

Enable human face detection plan. For details, see "4.4.1 Enabling AI Plan."

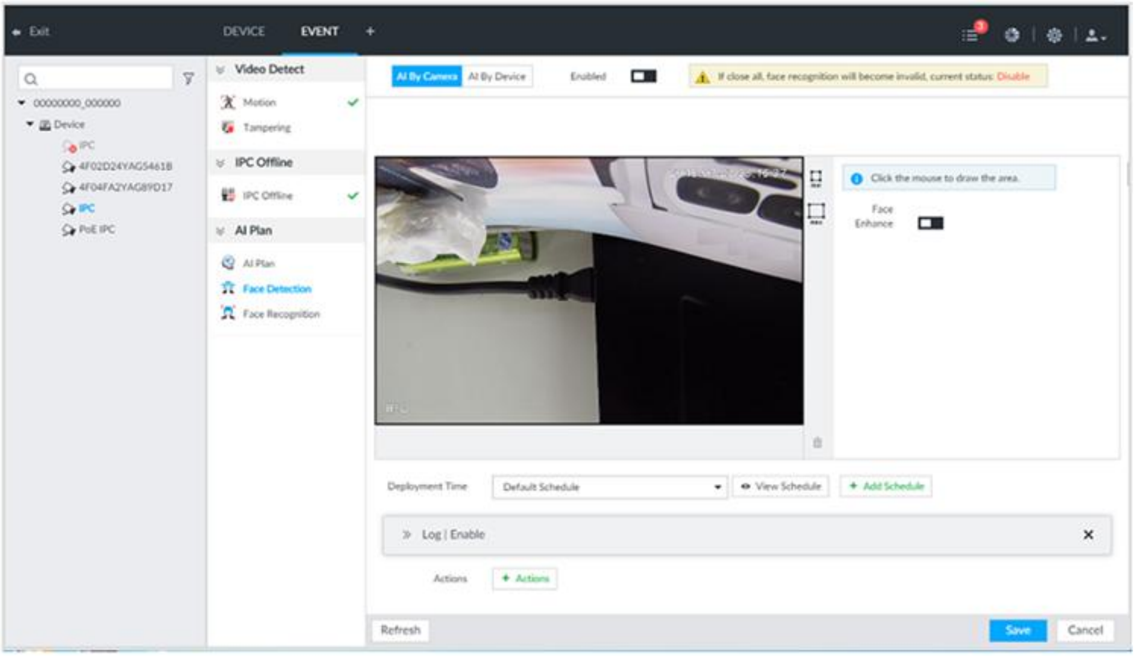
Step 1 Click ⚙ and select EVENT.

The EVENT interface is displayed.

Step 2 Select the remote device in the Device list and then select AI Plan > Face Detection.

The Face Detection interface is displayed. See Figure 4-16.

Figure 4-16 Face detection (AI by camera)



Step 3 Click the AI By Camera tab or AI By Device tab and click ▣ on the right of Enabled to enable the corresponding function.

- AI by camera: The remote device such as smart IPC supports smart detection. The Device only needs to support to detect and display the smart alarm information from the remote device, and perform smart detection configuration and record playback for the remote device.
- AI by device: The remote device does not support AI analysis and the IVSS device performs intelligent detection for the remote device.

Step 4 Click ▣ to enable face enhance.

After face enhance is enabled, the system displays enhanced human faces on the monitor screen.

NOTE

Only AI by camera supports this function.

Step 5 Press and hold down the left mouse button and draw the face detection zone on the screen.

- Click min or max to set the minimum size and maximum size of face detection. Only when the target size is between the min size and max size, the system triggers alarm.
- Select the face detection zone you have drawn and click 🗑 to delete it.

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

After setting the period, the system triggers the corresponding alarm within the set time period.

- Click View Schedule to view the detailed schedule information.
- If the schedule is not available or the existing schedule does not meet actual

needs, click **+ Add Schedule** to add schedule.

Step 7 Click **+ Actions** to set the alarm activation action.

NOTE

- When selecting Snap, the system only supports to activate the current channel to do snapshot.
- Click **+ Actions** again, select Record and set to trigger several channels to record at the same time.

Step 8 Click Save to save the configuration.

4.4.3 Human Face Recognition

It is to compare the detected human faces with the images in the face database. Once similarity is equal to or higher than the specified value, system can trigger an alarm.

NOTE

- The following contents are based on AI by device.
- Face database is already created. For details, see *User’s Manual.*
- You need to enable the face detection function. For details, see "4.4.2 Human Face Detection."

Step 1 Click ⚙ and select EVENT.

The EVENT interface is displayed.

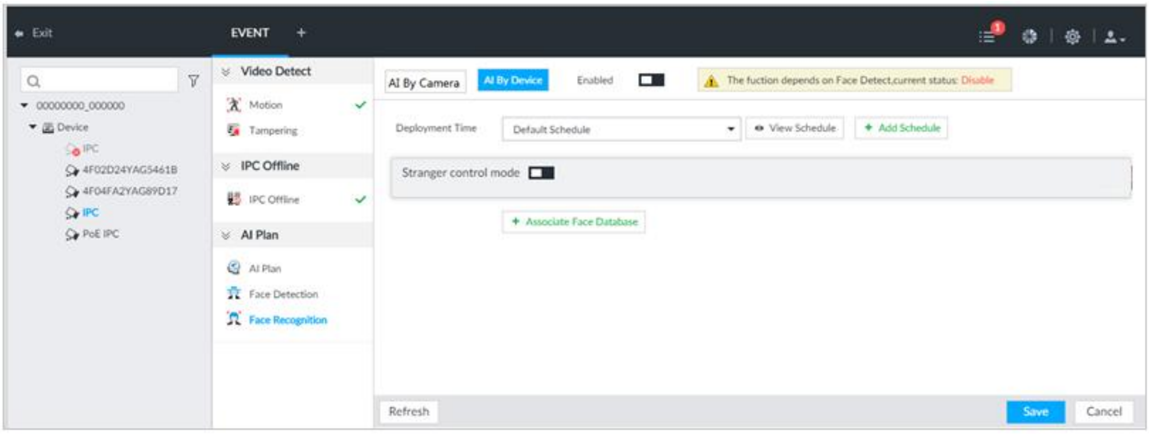
Step 2 After selecting the remote device, select AI Plan > Face Recognition.

The Face Recognition interface is displayed.

Step 3 Click AI by Device Tab.

The AI by device interface is displayed. See Figure 4-17.

Figure 4-17 Face recognition (AI by device)



Enabled ◧

The fuction depends on Face Detect,current status: Disable

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

Stranger control mode ◧

+ Associate Face Database

Step 4 Click ◧ to enable AI by device.

Step 5 Click the Deployment Time drop-down list and select the schedule.

After setting the period, the system triggers the corresponding alarm within the set time period.

- Click **View Schedule** to view the detailed schedule information.
- If the schedule is not available or the existing schedule does not meet actual needs, click **+ Add Schedule** to add schedule.

Step 6 Set stranger control mode.

Enable stranger control mode. When the face similarity is lower than the set value, the system triggers an alarm.

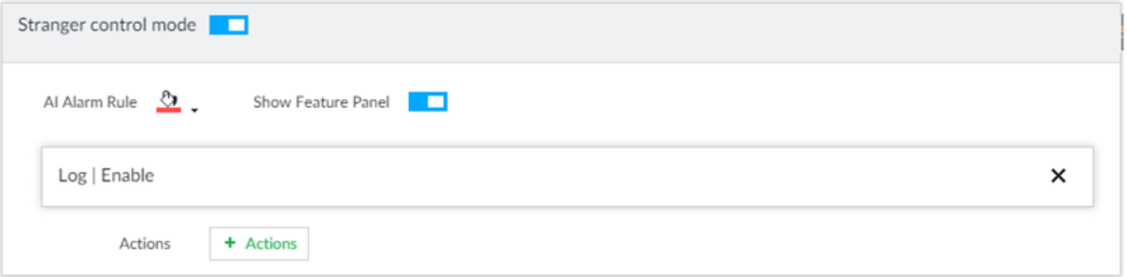
NOTE

If the stranger control mode is disabled, the system displays the face detection panel on the LIVE interface when the face similarity is lower than the set value.

1) Click to enable the stranger control mode.

The stranger control mode setting interface is displayed. See Figure 4-18.

Figure 4-18 Stranger control mode



Stranger control mode

AI Alarm Rule

Show Feature Panel

Log | Enable ✕

Actions + Actions

2) Configure the parameters. For details, see Table 4-3.

Table 4-3 Description of stranger control mode parameters

Parameter	Description
AI Alarm Rule	Click it to select the color for the alarm rule box.
Show Feature Panel	When it is enabled, the system displays the stranger panel on the LIVE interface when an alarm is triggered.

3) Configure alarm linked events.

Step 7 Configure the linked face database.

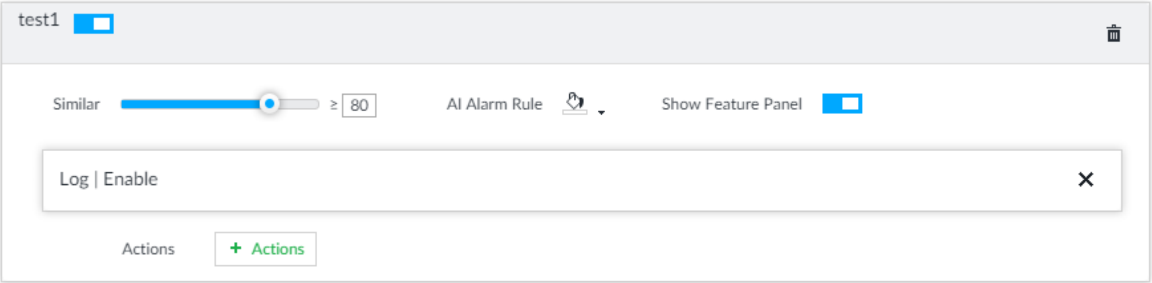
NOTE

- When AI by camera is enabled, you shall configure the face database information on the remote device. Only alarm linked events shall be configured here.
- Repeat this step to activate several face databases at the same time.

1) Click **+ Associate Face Database** to select the associated database.

The face database configuration interface is displayed. See Figure 4-19.

Figure 4-19 Face database configuration



test1

Similar ≥ 80

AI Alarm Rule

Show Feature Panel

Log | Enable ✕

Actions + Actions

2) Configure the parameters. For details, see Table 4-4.

Table 4-4 Description of face recognition parameters

Parameter	Description
Similar	The system compares the detected faces with the images in the face database. When the similarity is equal to or higher than the set value, the system triggers an alarm.
AI Alarm Rule	Click the color zone to set color for alarm rule box.
Show Feature Panel	Enable Show Feature Panel and the system displays the face recognition panel on the LIVE interface.

3) Click **+ Actions** to configure the alarm linked events.

📖 **NOTE**

- When selecting snapshot, the system only supports to activate the current channel for snapshot.
- The system supports to activate multiple channels for video recording.

Step 8 Click **Save** to save the configuration.

4.5 Logout/Reboot/Shutdown

- Logout : Click 👤▾ and then select logout.
- Reboot: Click 👤▾ and then select reboot. Click OK on the pop-up window.
- Shut down: Click 👤▾ and then seelct shut down. Click OK on the pop-up window.

5 Web Operations

System supports general browser such as Google Chrome, Firefox to access the Web to manage the Device remotely.

CAUTION

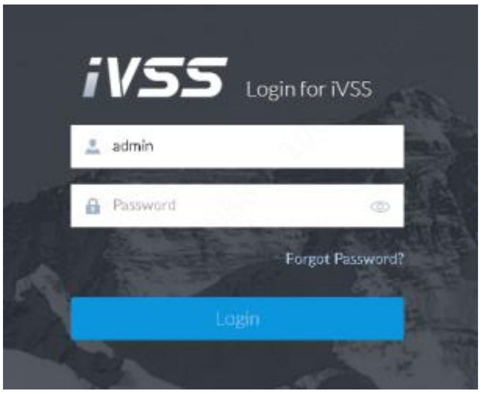
- When you are using general browser to access the Web, system supports setting function only. It cannot display the view. We strongly recommend you to use IVSS browser. For details, see "6 IVSS Client."
- Before you use Web function, make sure the network between the Device and PC is proper.
- System supports general browser such as Google Chrome and Firefox to access Web. Please use the latest browser version.

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

Enter Web login interface. See Figure 5-1.

Step 2 Enter the username and password, and then click Login to enter the Web interface.

Figure 5-1 Login



6 IVSS Client

System supports to work with the corresponding general applications (IVSS) to access the Device remotely. It is to realize system configuration and operations.

If you are using general browser to login the Device, Web login interface displays IVSS browser information. You can get IVSS installation package.

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

Enter Web login interface.

Step 2 Click Download to download IVSS browser installation package.

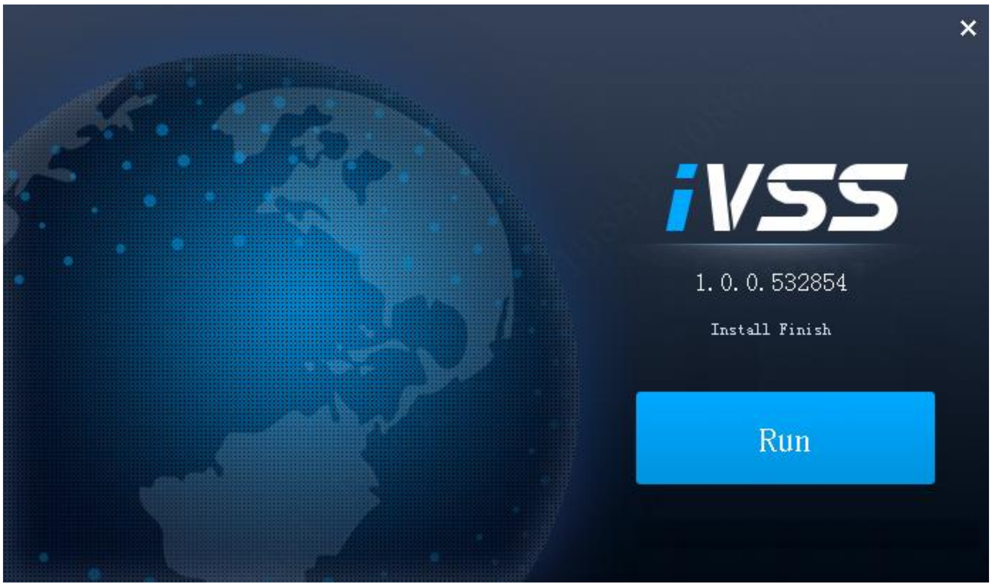
NOTE

If you have downloaded IVSS browser packages, click Run to enable IVSS browser.

Step 3 Double click the IVSS installation package and install the IVSS client according to the prompts.

After the installation is completed, the interface is shown as in Figure 6-1.

Figure 6-1 Successful installation



Step 4 Click Run to enter the IVSS client.

7 FAQ

Problem	Possible Reason & Solution
After enabling AI by device, there is no human face recognition event.	● The AI module is offline Click + on the LIVE interface. Select MAINTAIN > Device Maintain > Upgrade > AI Module to check if the AI module is online or not. ● There are too many filter criteria on the AI display interface. ● The registered remote device does not support human face detection. Enable AI by device. For details, see "4.4.2 Human Face Detection." ● It is not within the deployment period, ● There is no activation human face database or the human face database has no data. ● The human face similarity setting is too high.
After enabling AI by camera, there is no human face recognition event.	● Human face recognition is not enabled on the AI plan. ● Human face database is not configured on the Web interface of the remote device. ● It is not within the deployment period.
There is no human face search result.	● The human face similarity setting is too high. ● The selected remote device does not trigger human face recognition. ● There is no human face recognition within the search period ● The specified human face image is not in the human face database.