

Intelligent Video Surveillance Server

Quick Start Guide

V1.0.2

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.

Table of Contents

1	General Introduction	9
1.1	Overview	9
1.2	Structure.....	9
2	Installation and Connection	13
2.1	Unpacking.....	13
2.2	HDD Installation	13
2.3	Cable Connection	15
3	Start-Up.....	16
3.1	Boot up	16
3.2	Device Initialization.....	16
3.3	Quick Settings	18
3.4	Register Remote Device.....	25
4	Operations.....	30
4.1	Login IVSS	30
4.2	Preview and Monitor.....	31
4.3	Playback Record File	37
4.4	AI Detection	39
4.5	Logout/Reboot/Shut down.....	44

General

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

Models

HDD No.	Model
8-HDD	IVSS708、IVSS708-FG、IVSS608
12-HDD	IVSS712
16-HDD	IVSS716、IVSS716D、IVSS716DR、IVSS716-FG、IVSS716DR-FG
24-HDD	IVSS724、IVSS724D、IVSS724DR

 NOTE

- Model name with R: Device with redundant power.
- Model name with D: Device with display screen.

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.
 ELECTRICITY	Indicates dangerous high voltage. Take care to avoid coming into contact with electricity.
 LASER BEAM	Indicates a laser radiation hazard. Take care to avoid exposure to a laser beam.
 ESD	Electrostatic Sensitive Devices. Indicates a device that is sensitive to electrostatic discharge.
 TIPS	Provides methods to help you solve a problem or save you time.



Provides additional information as the emphasis and supplement to the text.

Writing Conventions

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

- Without otherwise specified, the Device in this guide refers to the IVSS device.
- The Remote Device in this 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 this guide refers to the AI card installed in the IVSS device.
- The Device supports operations on the local PC, in the Web and IVSS browser. The operation steps and interface images in the Guide are only for reference. The actual interfaces shall prevail.
- To guarantee the security of personal privacy, the private information such as human face and car plate number has been dealt with.

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 include but not limited to: providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact.

About the Guide

- The Guide is for reference only. If there is inconsistency between the Guide and the actual product, the actual product shall govern.
- We are not liable for any loss caused by the operations that do not comply with the Guide.
- 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.

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 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.
- 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.

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, 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 playback video). This series product has user-friendly interface, suitable for user 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 decode, it meets the main development trend of current market.

This series product can be widely used in the intelligent building, large parking lot, safe city project, financial planning area, etc.

1.2 Structure

It is to introduce front panel, rear panel, port function and button function, indicator light status, etc.



Note

- The following contents are based on the 16-HDD series product. Refer to the user's manual for detailed information of other series product,
- Device supports AI module to realize human face detection, human face recognition, etc. For some series products, AI module is optional. Please purchase separately if necessary.

1.2.1 Front Panel

The front panel with LCD is shown as below. See Figure 1-1.

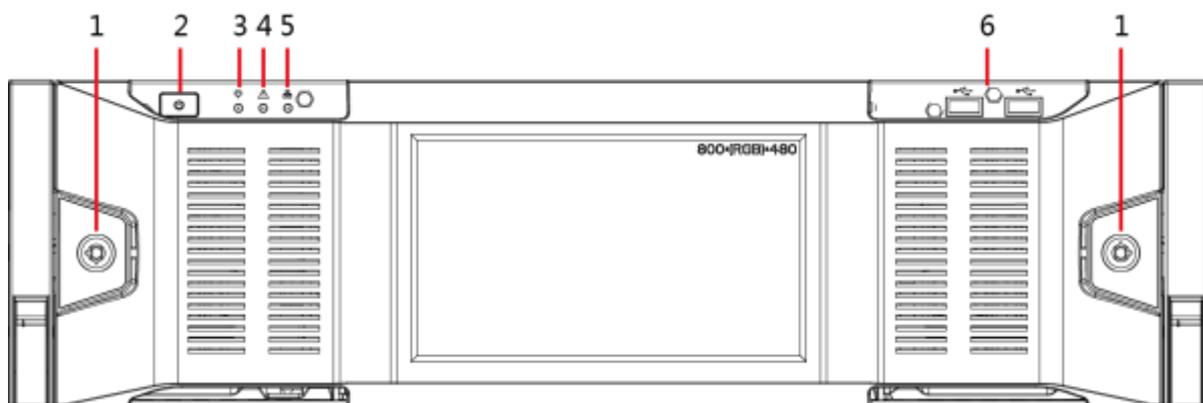


Figure 1-1

The front panel without LCD is shown as below. See Figure 1-2.

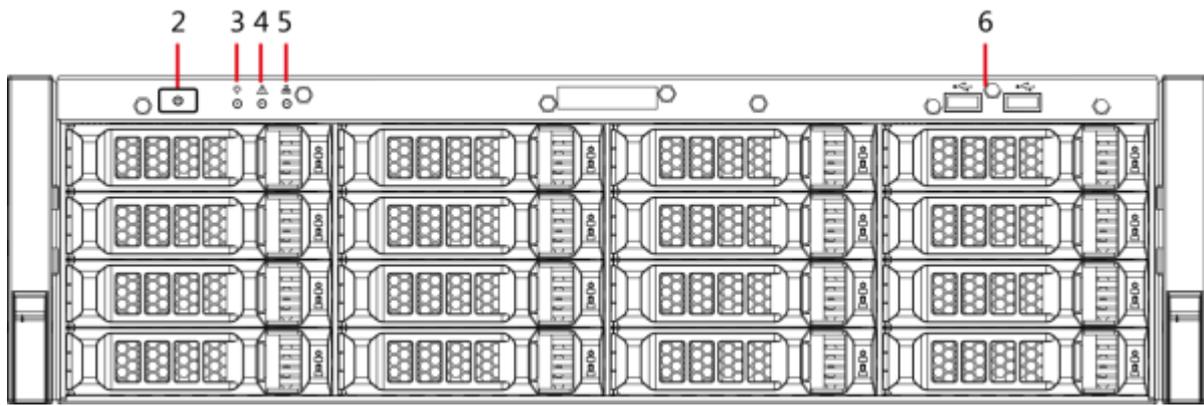


Figure 1-2

Please refer to the following sheet for detailed information.

SN	Name	Function
1	Front panel lock	Once the front panel lock is secure, it can prevent HDD stealing or remove by mistake. Unlock the front panel lock and remove the front panel, you can view 16 HDD slots. See Figure 1-2.
2	Power on-off button	<p>Boot up or shut down device. The power on-off button has the indicator light. It can display device-running status.</p> <ul style="list-style-type: none"> ● 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.
3	System status indicator light	<p>It is to display system-running status.</p> <ul style="list-style-type: none"> ● The blue light is on: Device is running properly. ● The indicator light is off: The device is not running.
4	Alarm indicator light	<p>It is to display local input alarm status.</p> <ul style="list-style-type: none"> ● 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	<p>It is to display current network status.</p> <ul style="list-style-type: none"> ● The blue indicator light becomes on: 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	Connect to mouse, keyboard, USB storage device ,etc.
7	16-HDD slot	<p>After you remove the front panel, you can see there are 16 HDDs. From the left to the right and from the top to the bottom, it ranges from 1~4, 5~8, 9~12, 13~16.</p> <p>There are two indicator lights on the HDD bracket: HDD indicator light and HDD read/write indicator light.</p> <ul style="list-style-type: none"> ● : 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.

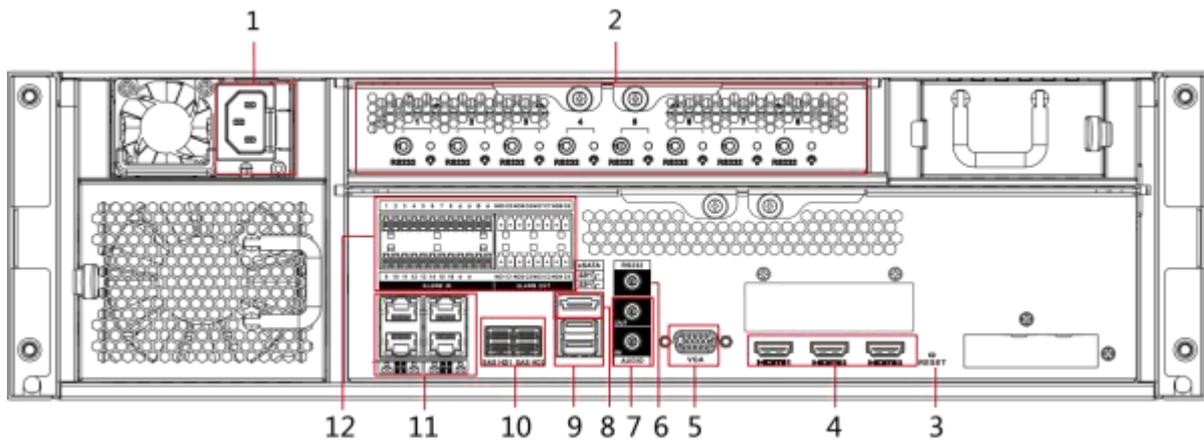


Figure 1-3

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

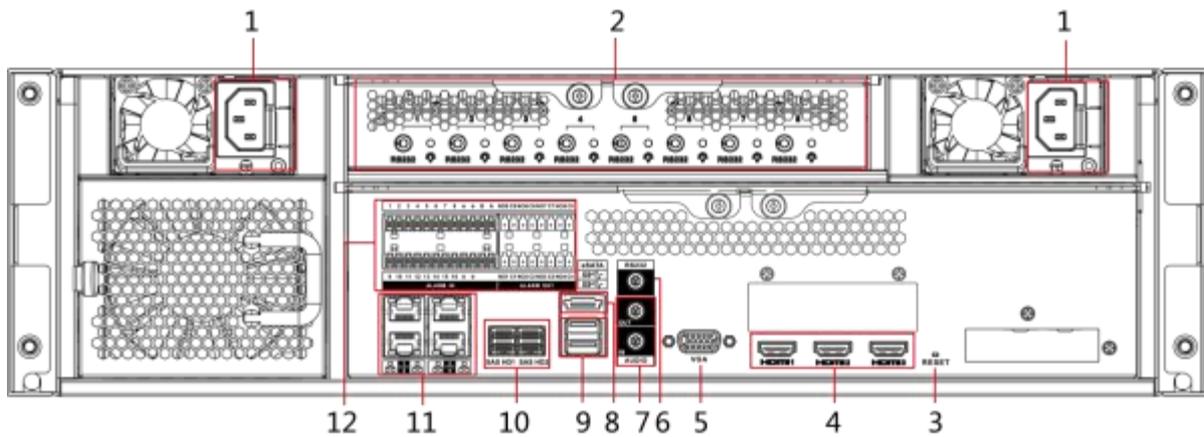


Figure 1-4

Please refer to the following sheet for rear panel button information.

SN	Name	Note
1	Power port	Input AC 100V-240V power
2	AI module indicator light	It is to display AI module status. <ul style="list-style-type: none"> ● The yellow light flashes, AI module is running properly. ● The yellow light is on, AI module is malfunction. Note This function is null if there is no AI module.
3	RESET button	User 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.
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 OUT	Audio input port Audio output port
7	RS232 port	RS232 COM debug. It is for general COM debug, set IP address, 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.

SN	Name	Note
10	SAS port	SAS extension port. It can connect to the SAS extension controller.
11	Network port	10M/100/1000Mbps self-adaptive Ethernet port. Connect to the network cable.
12	Alarm input	<p>16 groups (1~16) alarm output ports, they are corresponding to ALARM 1~ALARM 16. The alarm becomes valid in low level.</p> <ul style="list-style-type: none"> ● 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	<p>8 groups of alarm input ports (NO1 C1~NO8 C8) . Output alarm signal to the alarm device. Please make sure there is power to the external alarm device.</p> <ul style="list-style-type: none"> ● 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

Some series product is heavy. It needs several persons to carry or move in case there is person injury.

2.1 Unpacking

After you received the device from the forwarder, please open the box and then check with the following sheet. If there is any problem, contact your local retailer or service engineer for help.

SN	Name		Contents
1	Whole package	Appearance	There is any visible damage or not.
		Package	There is any accidental clash during transportation or not.
2	Front panel and rear panel	Appearance	There is any visible damage or not.
		Device model	The model is right or not.
		The label on the device	It is neat and clean or not.  Note Do not tear off, or discard the label. Usually we need you to represent the serial number when we provide the service after sales.

2.2 HDD Installation

This chapter is to introduce HDD installation information.

Note

Different series products support different HDD amount. Refer to the actual product for detailed information.

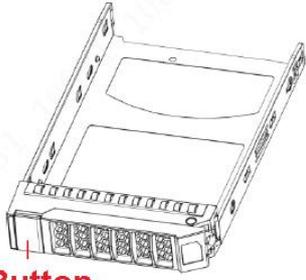
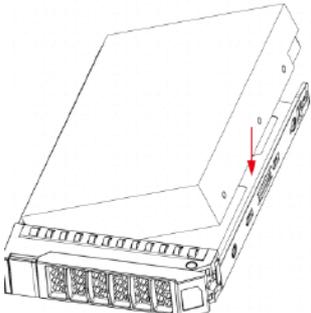
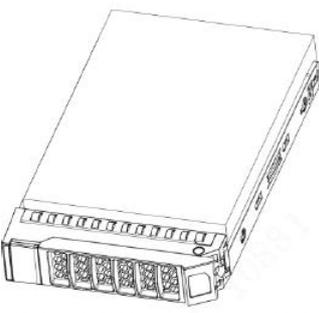
2.2.1 12-HDD Series



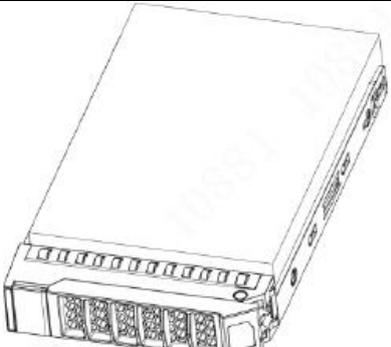
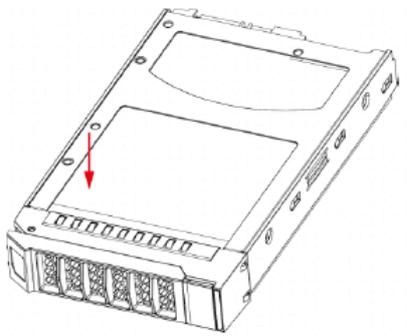
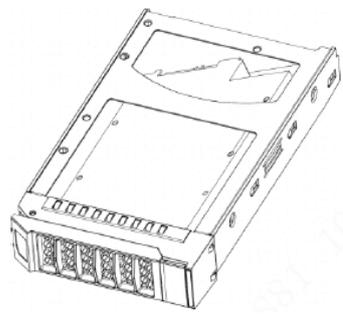
CAUTION

Do not close the handle if you have not pushed the HDD box to the end. Otherwise, it may result in HDD slot damage.

Install HDD

 <p>Button</p>		
<p>① Press the button on the HDD box at the front panel, open the handle and pull out to take the empty HDD box.</p>	<p>② Follow the higher side of the installation surface to install the HDD and then push down. It is to install the HDD to the other side of the installation surface.</p>	<p>③ Insert the HDD box to the HDD slot of the device, and then push to the end to close then HDD box handle.</p>

Remove HDD

		
<p>① Press the button on the HDD box at the front panel, open the handle and pull out to take the empty HDD box.</p>	<p>② On the back side of the HDD box, refer to icon marked on the above figure to push hard.</p>	<p>③ Take the HDD out. Insert the HDD box back to the HDD slot, push to the end and then close the HDD box handle</p>

2.2.2 16/24-HDD Series



CAUTION

Do not close the handle if you have not pushed the HDD box to the end. Otherwise, it may result in HDD slot damage.

Install HDD



① Press the red button on the HDD box at the front panel, open the handle.	② Pull out to take the empty HDD box and then Install the HDD to the HDD box	③ Secure the screws at the bottom of the box, insert the HDD box to the HDD box slot and then push to the end, and then close the HDD box handle.
--	--	---

Remove HDD

- Step 1 Press the red button on the HDD box at the front panel, open the handle.
- Step 2 Pull out to take the HDD box.
- Step 3 Unfasten the screws on the rear panel of the HDD box, and then take out the HDD.
- Step 4 Insert the HDD box back to the HDD slot, push to the end and then close the HDD box handle.

2.3 Cable Connection

Refer to Figure 2-1 for device cable connection information.

- Connect displayer, mouse, and keyboard and so on for local menu operation.
- Install AI module if you want to use intelligent functions such as human face detection, human face recognition function.



CAUTION

DO NOT CHANGE OR REPLACE THE AI MODULE WHEN DEVICE IS RUNNING. Shut down the device first and then remove the AI module, otherwise, the data on the AI module may result in damage.

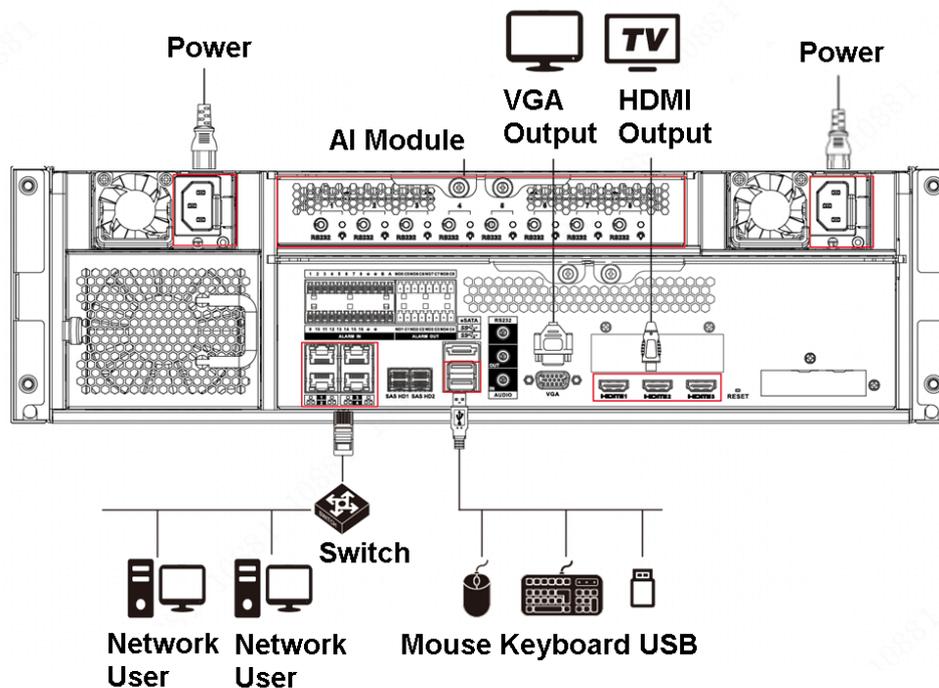


Figure 2-1

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

3.1 Boot up



Warning

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 the device to the power adapter first and then connect the device to the power socket.
- The rated input voltage matches the device power on-off button. Please make sure the power wire connection is OK. Then click the power on-off button.
- Always use the stable current, 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 device, please refer to chapter 2.3 Cable connection to connect cable.

- For 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 click shutdown button on the GUI to turn off the device, press the power button for a short period of time to boot up device.

3.2 Device Initialization

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.

Steps

- Step 1 Boot up device.
Enter device initialization interface. See Figure 3-1.

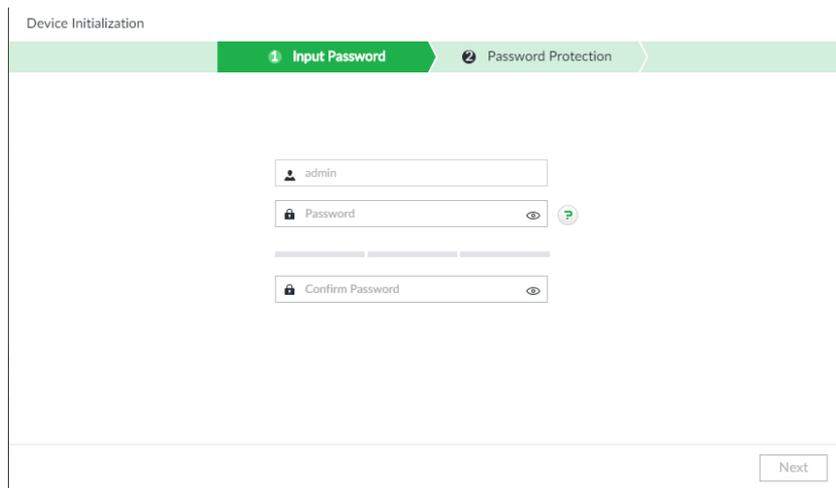


Figure 3-1

Step 2 Set **admin** login password.

Name	Function
User	The default user name is admin .
Password	The password ranges from 8 to 32 digitals. It can contain letters, numbers and special characters (excluding “”, “”, “”, “”, “&”). The password shall contain at least two categories. Usually we recommend the strong password. Note
Confirm password	After input password, use mouse to press to display password. Release the mouse or move mouse to other position, the password is displayed at hidden mode again.
Prompt question	After you set proper question, move the mouse to the on the login interface, system displays corresponding password prompt question. It is to help you remember password. Note The prompt question function is for local login interface only. Refer to the actual interface for detailed informaiton.

Step 3 Click Next.

Enter password protection interface. See Figure 3-2.

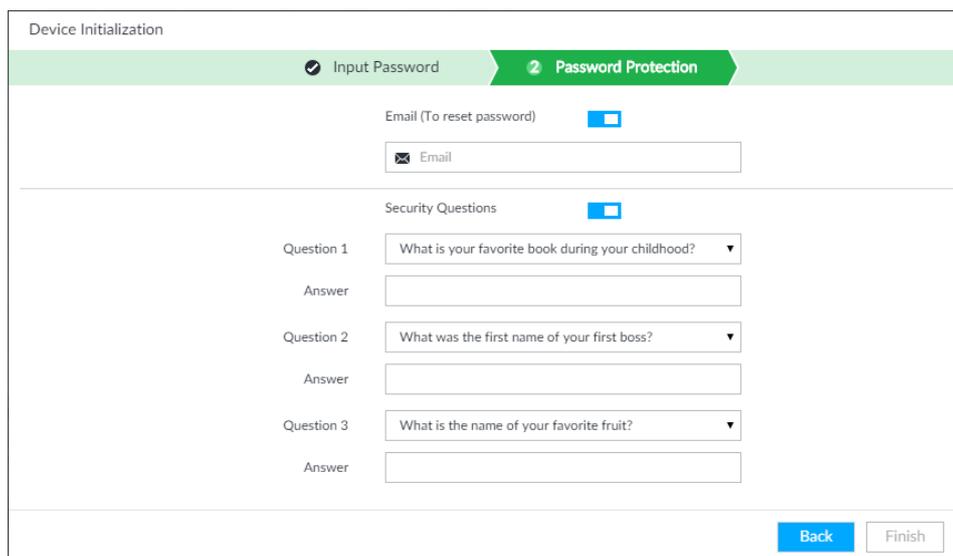


Figure 3-2

Step 4 Set password protection information.

Setting the security questions here, you can use the email you input here or answer the security questions to reset **admin** password. Refer to user's manual for detailed information.

 **Note**

Click  to cancel the email or security questions box.

Password protection	Note
Email	Input an email address for reset password purpose. In case you forgot password in the future, input the security code you got on the assigned email to reset the password of admin . Go to the main menu->Setting->System->Account to set. Refer to user's manual for detailed information.
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 button to go to the quick setting interface. It is to set device basic information. Refer to chapter 3.3 Quick settings for detailed information.

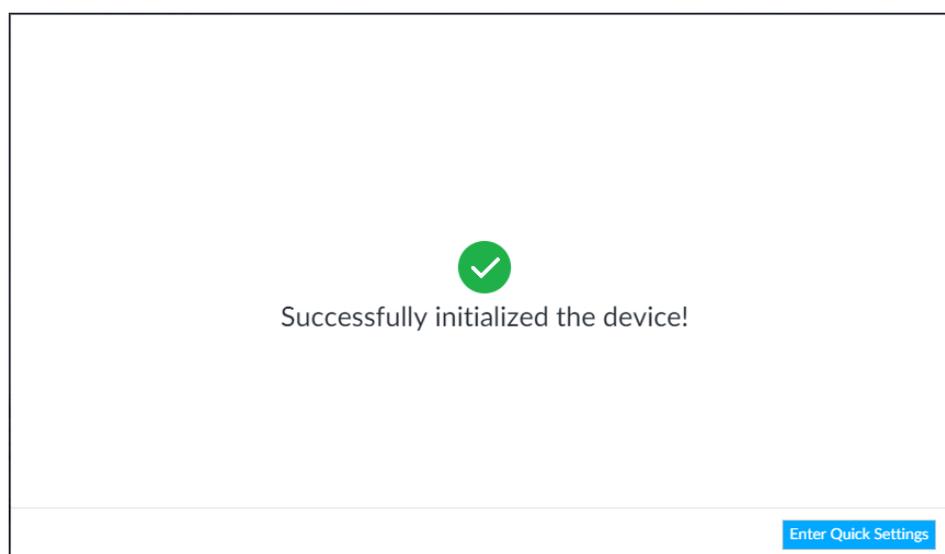


Figure 3-3

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

It is to set system time. Please enable/disable NTP function according to your actual requirements. After enable NTP function, device can automatically synchronize time with the NTP server.

Steps

Step 1 On initialization interface, click Enter quick settings button. Enter time setting interface. See Figure 3-4.

Quick Configuration

1 Time 2 IP Set 3 P2P Access



Date
2018.01.22

Time
15:36:34

Time Manual Setting

Date/Time Sync with your PC time

Sync with Internet Time Server

Server

Auto Sync Time Interval hours

Time and Date Format

Time Zone

Figure 3-4

Step 2 Set parameters.

Name	Function
Time	It is to set system date and time. You can set manually or set device to synchronize time with the NTP server. <ul style="list-style-type: none"> Manual setting: Select manual setting and then input actual date and time. Sync with the Internet Time Server: Check the box and then input NTP server IP address or domain, and then set the synchronization interval.
Time and date format	Set system date and time display format.
Time zone	Set device time zone.

Step 3 Click Next to save settings.

3.3.2 IP Address

It is to change device IP address, DNS server information and so on according to the actual situation.

Note

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

Steps

Step 1 On Time setting interface, click Next button. Enter IP setting interface. See Figure 3-5.

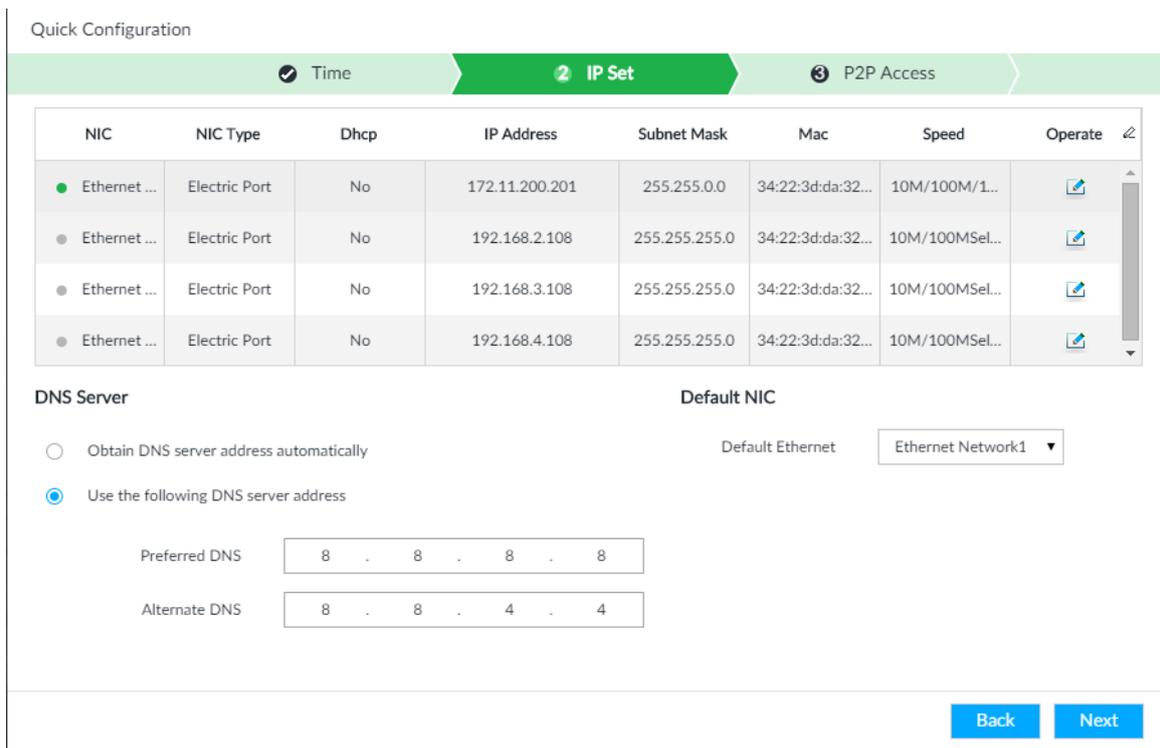


Figure 3-5

Step 2 Set IP address.

1. Click the  of the corresponding Ethernet port.

Enter Edit Ethernet setting interface. See Figure 3-6.

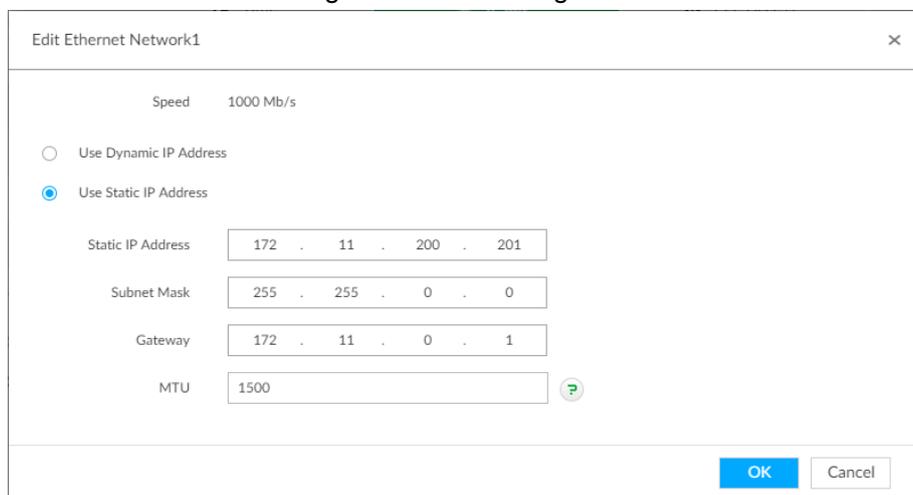


Figure 3-6

2. Set parameters.

Name	Function
Speed	Current NIC max network transmission speed.
Use dynamic IP address	When there is a DHCP server on the network, check the box to use dynamic IP address, system can allocate an dynamic IP address to the device. There is no need to set IP address manually.
Use static IP address	Check the box to use static IP address. Please set static IP address, subnet mask and gateway. It is to set a static IP address for the device.

Name	Function
MTU	<p>Set NIC MTU value. The default setup is 1500 Byte. We recommend you to check the MTU value of the gateway first and then set the device MTU value equal to or smaller than the gateway value. It is to reduce the packets slightly and enhance network transmission efficiency.</p> <p> Caution Changing MTU value may result in NIC reboot, network offline and it may affect current running operation. Please be careful!</p>

3. Click OK.

Device goes back to IP setting interface.

Step 3 Set DNS server information.

You can select to automatically to get DNS address or input DNS server address manually.

 **Note**

Follow the steps listed below if you want to use domain service.

- Auto get DNS server address: Check the box to auto get DNS server address, device can automatically get the DNS server IP address on the network.
- Use the following DNS server address: Check the box to use the following DNS server addresses, and then input primary DNS and alternate DNS IP address.

Step 4 Set default NIC.

Select default Ethernet card from the dropdown list.

 **Note**

Make sure the network card has connected to the network.

Step 5 Click OK.

3.3.3 P2P

P2P is a peer to peer technology. You can scan the QR code to download cellphone APP without DDNS service or the port mapping or installing the transmission server. After register the device to the APP, you can view the remote video, playback record file etc.

 **Note**

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

Steps

Step 1 On IP setting interface, click Next.
Enter P2P interface. See Figure 3-7.

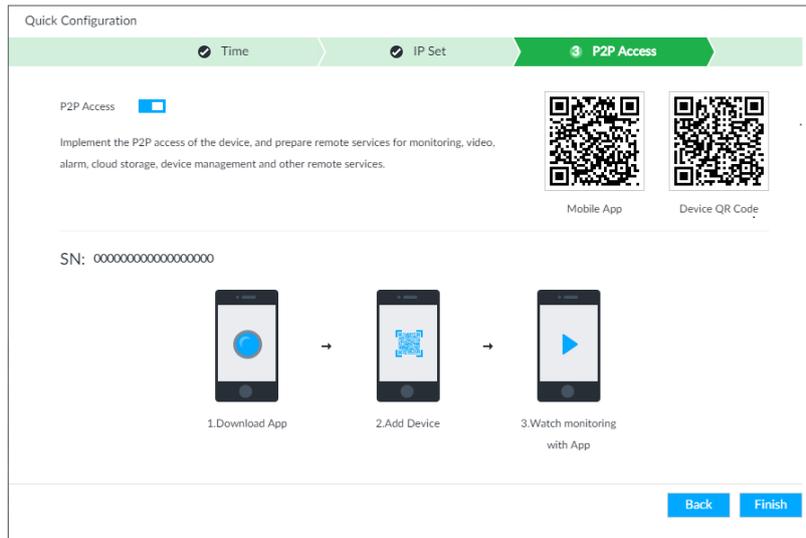


Figure 3-7

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

Step 3 Click Finish to save settings.

After the configuration, you can register a device to the APP to view remote video, playback record file, etc. Refer to corresponding cellphone APP for detailed information.

Cellphone APP

Step 1 Download and then install the cellphone APP.

1. Use an APP of scan function to scan the download cellphone APP QR code.
2. Download and install the cellphone APP according to the cellphone OS type.

Step 2 Run the cellphone APP and select Camera.

System enters real-time surveillance interface. See Figure 3-8.

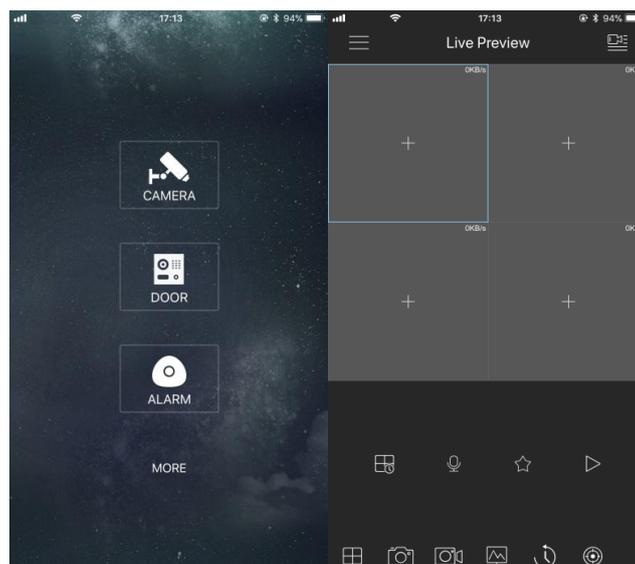


Figure 3-8

Step 3 Register a device to the cellphone APP.

 **Note**

Before register the device to the APP, make sure the device you want to register has been initialized. Otherwise, you cannot properly use the device.

1. Tap  and then select Device manager.

Enter Device manager interface. See Figure 3-9.

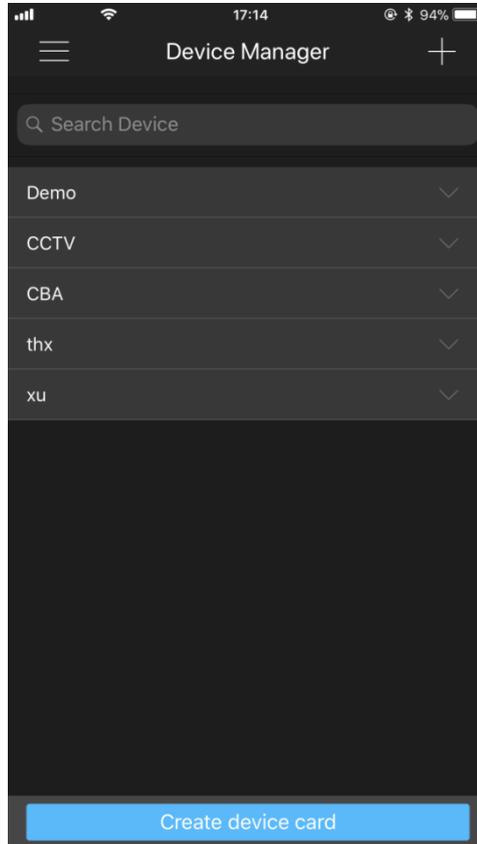


Figure 3-9

2. Tap .

Enter Add device interface. See Figure 3-10.

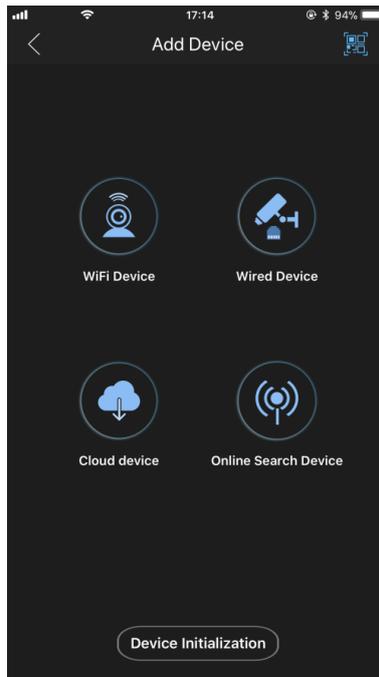


Figure 3-10

3. Select device connection type, and then follow the prompts to connect to the device. System displays device SN. See Figure 3-11.

Note

You can scan the QR code to connect to the device. Follow the steps listed below:

Tap , enter the QR code of current device. Scan the QR code on  Figure 3-7 (scan the QR code on the actual interface) .

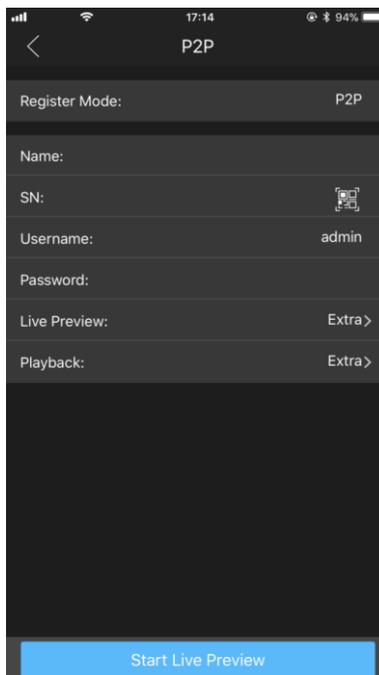


Figure 3-11

4. Set device name, user name and password according to the actual situation.

- Step 4 Click Start live preview.
System begins connecting to the device. After device successfully registered to the system, you can view the real-time surveillance video.

3.4 Register Remote Device

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

Device supports two add modes: short-cut add, and manual add.

- Short-cut 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. It is so called manual add.



Caution

Uninitialized remote device cannot register to the system. Refer to user's manual for detailed information.



Note

Here we use short-cut add to continue. Refer user's manual for manual add information.

Steps

- Step 1 Click .

Enter Setting interface. See Figure 3-12.

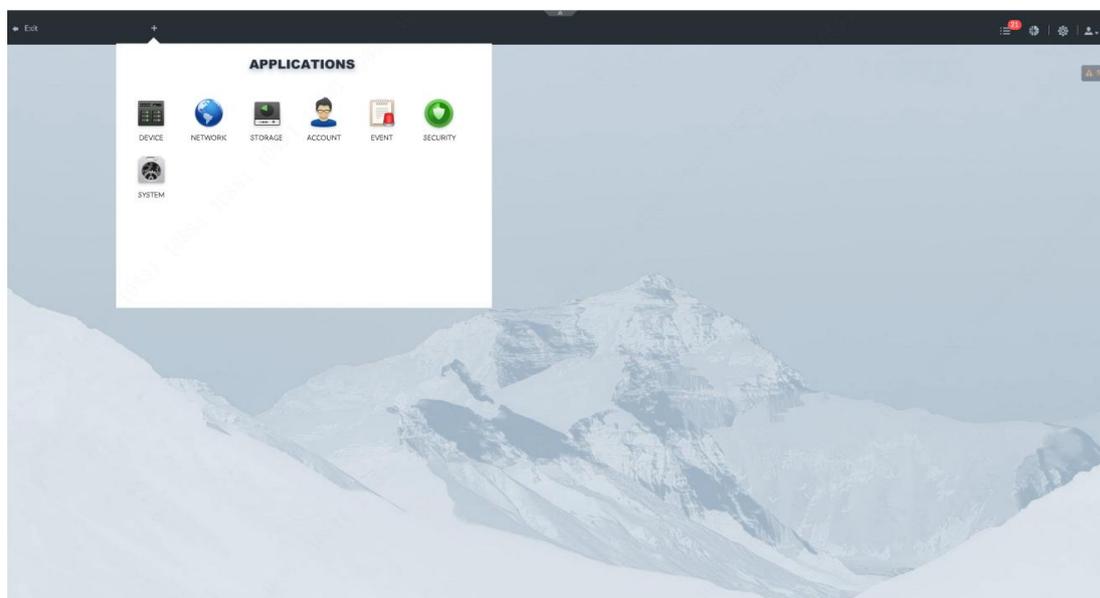


Figure 3-12

- Step 2 Select Device.
Enter device manager interface. See Figure 3-13.

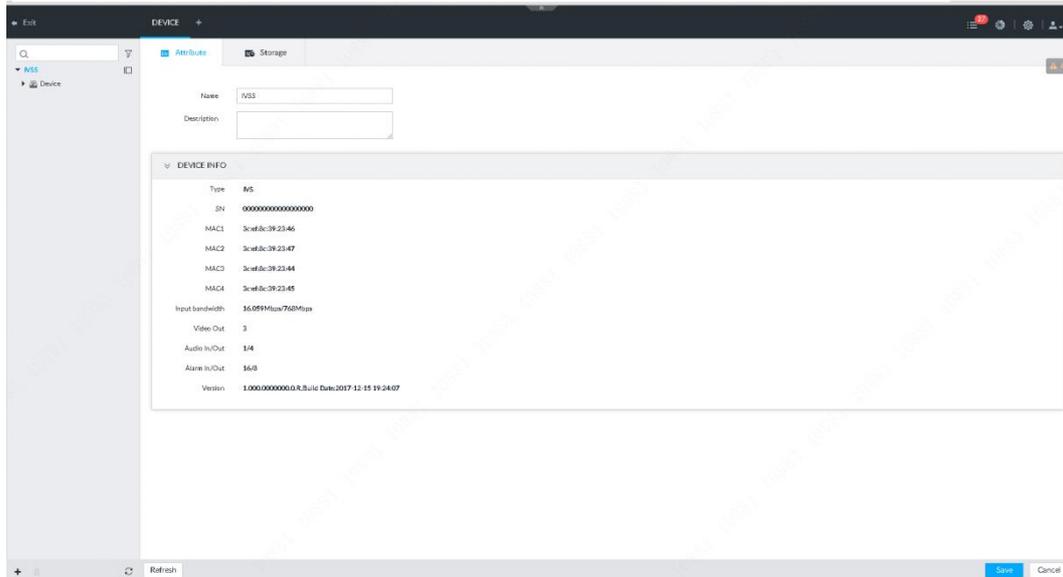


Figure 3-13

Step 3 Click **+** at the bottom left corner and then select Smart add.
Enter add device interface. See Figure 3-14.

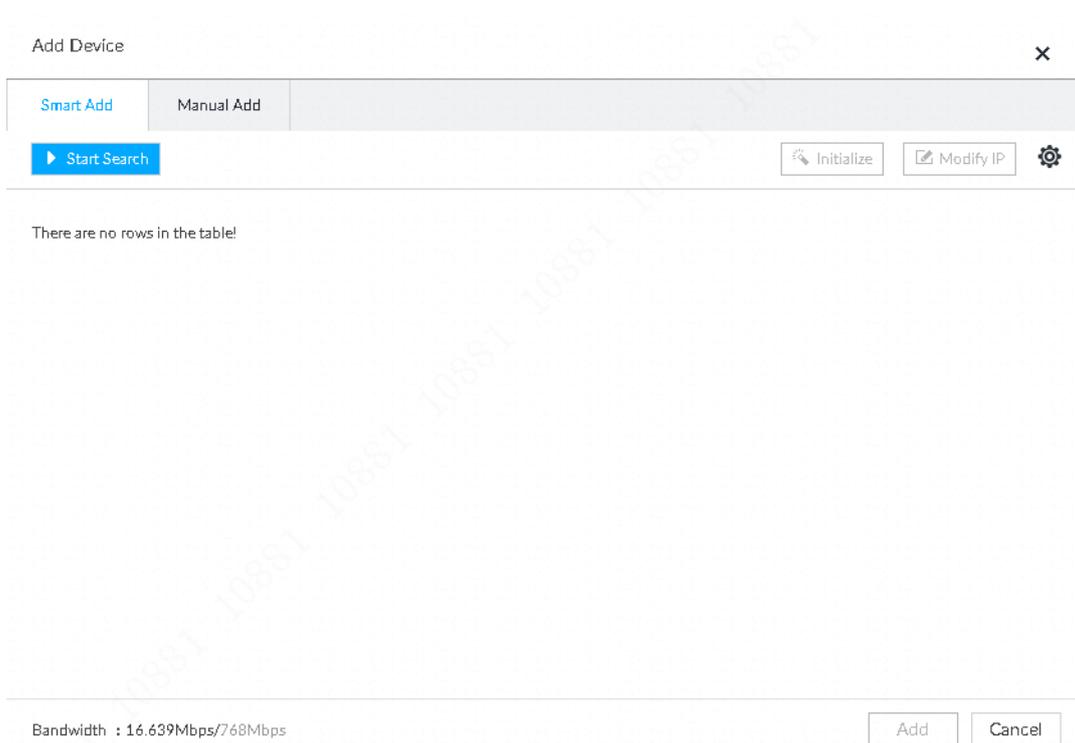


Figure 3-14

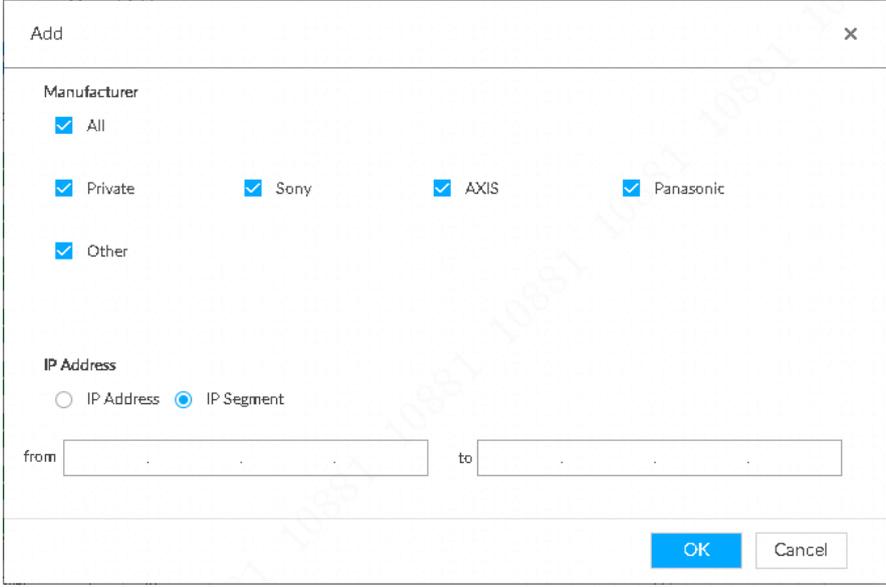
Step 4 Search remote device.

Note

Device searches the remote devices on the device same IP segment by default if there is no search criteria.

1. Click .

Enter Add interface. See Figure 3-15.



The 'Add' dialog box contains the following elements:

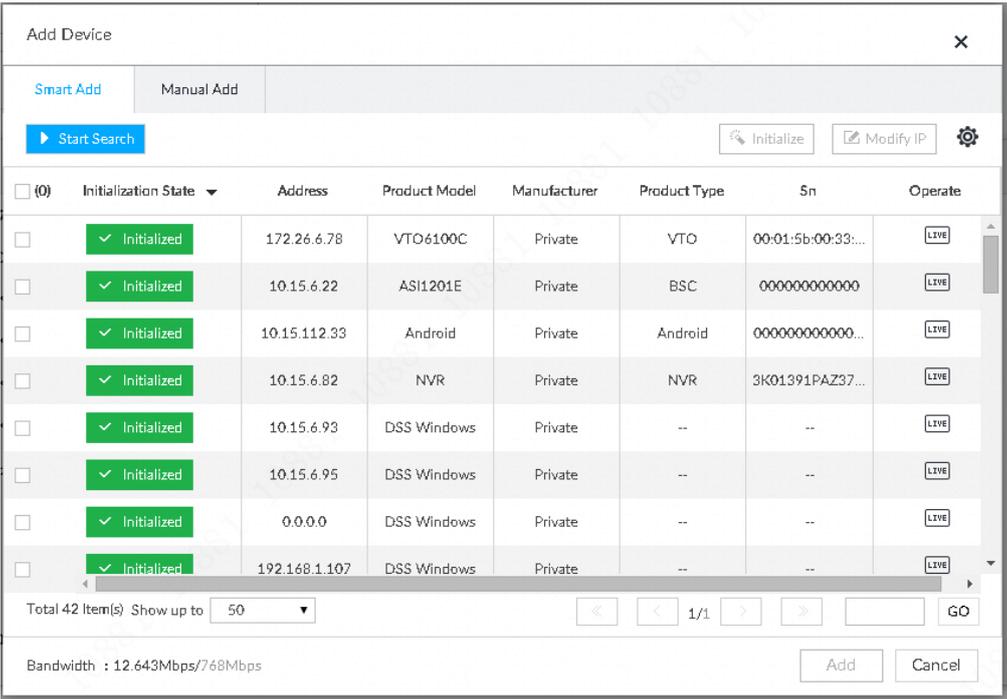
- Manufacturer:** A group of checkboxes including 'All', 'Private', 'Other', 'Sony', 'AXIS', and 'Panasonic', all of which are checked.
- IP Address:** Two radio buttons: 'IP Address' (unchecked) and 'IP Segment' (checked).
- IP Range:** Two text input fields labeled 'from' and 'to' for specifying an IP range.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

Figure 3-15

2. Select manufacturer name, and then set IP address you want to search.
 - IP address: Set remote device IP address. Device only searches the remote device of the specified IP address.
 - IP segment: Set remote device IP segment. Device searches the remote devices of the specified IP segment.
3. Click OK to save settings.

Device goes back to device manager interface.
4. Click Start search.

Device begins search remote devices and display search result. See Figure 3-16.



The 'Add Device' interface shows a table of search results with the following columns: Selection, Initialization State, Address, Product Model, Manufacturer, Product Type, Sn, and Operate. The table contains 8 rows of data, all with 'Initialized' status. Below the table, there is a summary of 42 items, a 'Show up to' dropdown set to 50, and navigation buttons. At the bottom, there is a bandwidth indicator and 'Add' and 'Cancel' buttons.

<input type="checkbox"/>	Initialization State	Address	Product Model	Manufacturer	Product Type	Sn	Operate
<input type="checkbox"/>	✓ Initialized	172.26.6.78	VTO6100C	Private	VTO	00-01-5b-00-33...	
<input type="checkbox"/>	✓ Initialized	10.15.6.22	ASI1201E	Private	BSC	000000000000	
<input type="checkbox"/>	✓ Initialized	10.15.112.33	Android	Private	Android	000000000000...	
<input type="checkbox"/>	✓ Initialized	10.15.6.82	NVR	Private	NVR	3K01391PAZ37...	
<input type="checkbox"/>	✓ Initialized	10.15.6.93	DSS Windows	Private	--	--	
<input type="checkbox"/>	✓ Initialized	10.15.6.95	DSS Windows	Private	--	--	
<input type="checkbox"/>	✓ Initialized	0.0.0.0	DSS Windows	Private	--	--	
<input type="checkbox"/>	✓ Initialized	192.168.1.107	DSS Windows	Private	--	--	

Figure 3-16

Step 5 Add remote device.

- Add 1-channel remote device.

Select a remote device and then click Add bottom. Device begins adding remote device and pops up confirmation interface. See Figure 3-17.

 **Note**

During the adding process, click Cancel button, you can cancel adding process.
Click the stop button of the corresponding remote device to cancel add.

Add Confirm							—	×
Address	Username	Password	Manufacturer	Port	Status	Operate		
10.15.112.15	admin	*****	Private	37777	Failed to add The ...	<input type="button" value="Retry"/>		
10.15.5.221	admin	*****	Private	37777	Failed to add The ...	<input type="button" value="Retry"/>		
10.15.6.108	admin	*****	Private	37777	Added			

Bandwidth : 12.552Mbps/768Mbps

Figure 3-17

- Add multiple-channel remote device
 1. Select a remote device and then click Add button.
Enter add confirmation interface. See Figure 3-18.

Add Confirm							—	×
Address	Username	Password	Manufacturer	Port	Status	Operate		
10.15.6.85	admin	*****	Private	40009	Please select a cha...			

Bandwidth : 30.949Mbps/768Mbps

Figure 3-18

2. Double click select a channel.
Enter video device interface. See Figure 3-19.

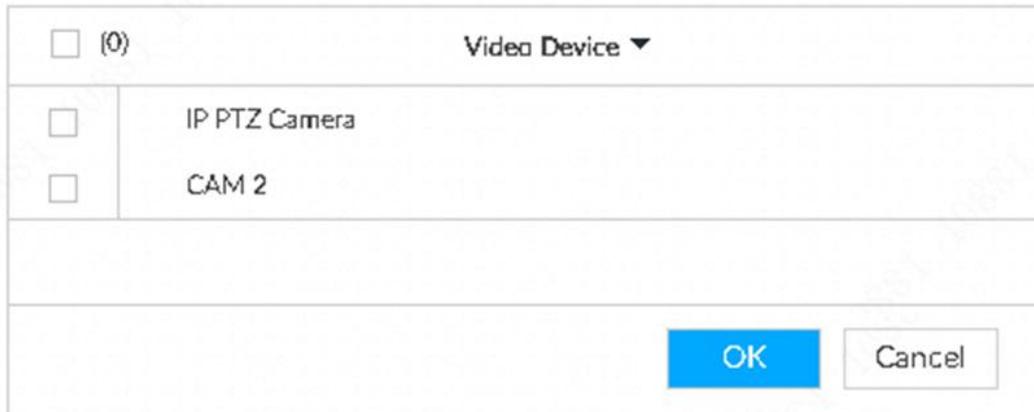


Figure 3-19

3. Select a channel you want to add.

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

4. Click OK to add the select channels.

Step 6 Click Continue to add or Finish.

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

4 Operations

4.1 Login IVSS

After boot up device, please input the corresponding user name and password to login.

Note

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

Steps

- Step 1 Boot up device.
Enter login interface. See Figure 4-1.



Figure 4-1

- Step 2 Input user name and password.

Note

- Default user name is **admin**. The password is that you set during initialization process. For your device safety, please change the **admin** password regularly and keep it well.
- After input password, use mouse to press  to display password. Release mouse or move mouse to  other position, the password is displayed at hidden mode again.
- Move the mouse to the  to view the password prompt information. It is to help you remember password.
- In case you forgot password, click Forgot password to reset. Refer to user's manual for detailed information.

- Step 3 Click Login
Enter main interface. See Figure 4-2.

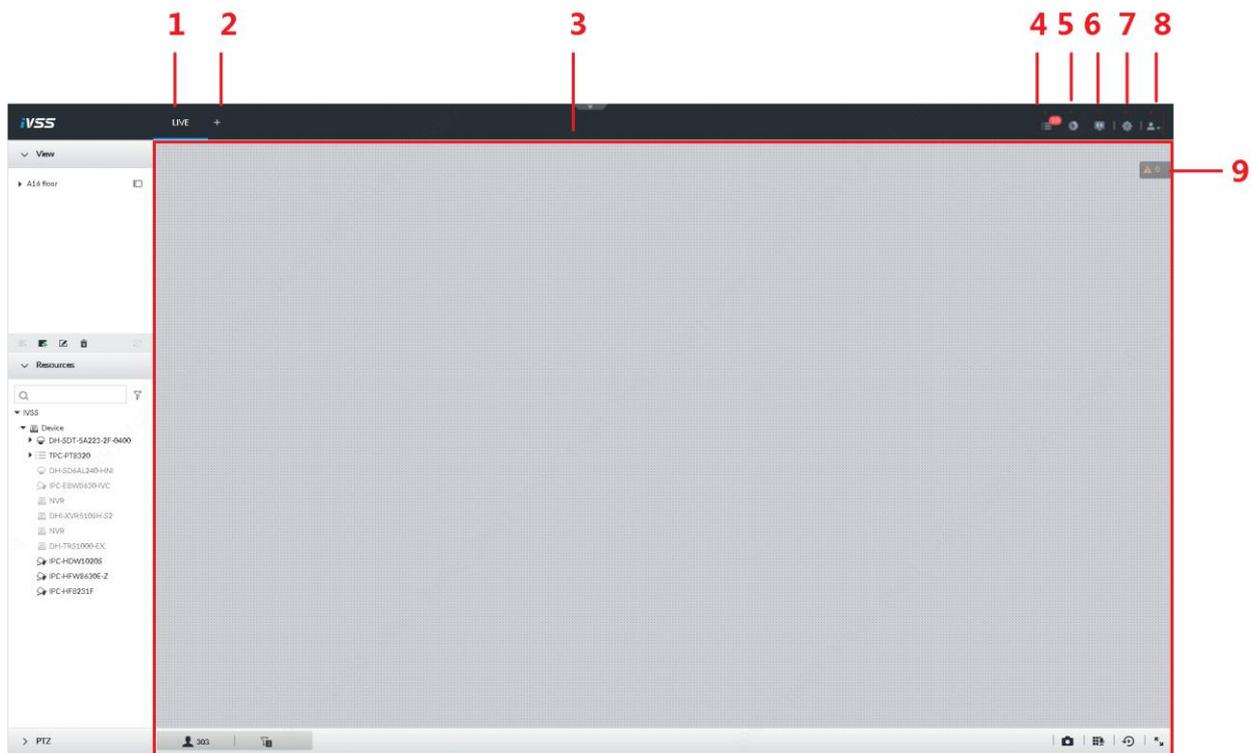


Figure 4-2

SN	Name	Function
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 interface. On app interface to view or enable appl.
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, logout user, reboot device or close device.  Note Reboot and shut down function is for local menu only.
9	Alarm list	It is to display currently unprocessed alarm event amount. Click the icon to view detailed alarm information.

4.2 Preview and Monitor

After logged 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 Views group by default. Please create view or view group under the View.
- Double click the view or drag the view to the play pane on the right side, device begins play the real-time video from the remote device.
- Click  to select Views and its sub-node.

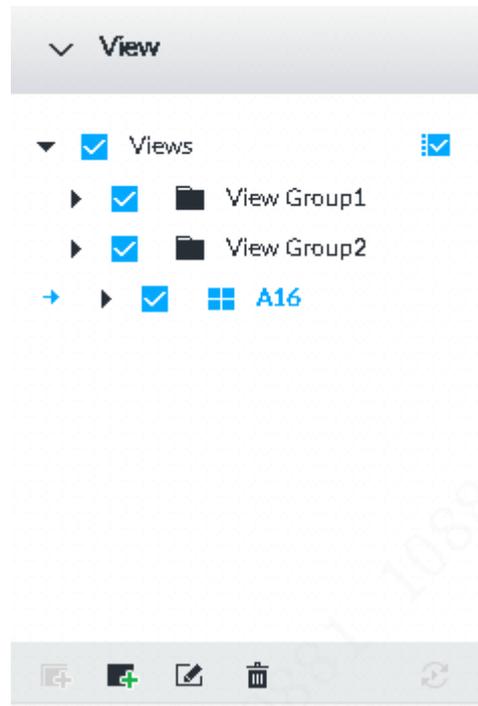


Figure 4-3

4.2.1.1 Create View

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

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

Preparation

Before you create view, please make sure you have added the remote device. Refer to chapter 3.4 Register remote device for detailed information.

Steps

Step 1 Follow the steps listed below to create view.

- Select Views or the created view group and then click , select Add view.
- Right click View or the create view group, select new views. Enter edit view interface. See Figure 4-4.

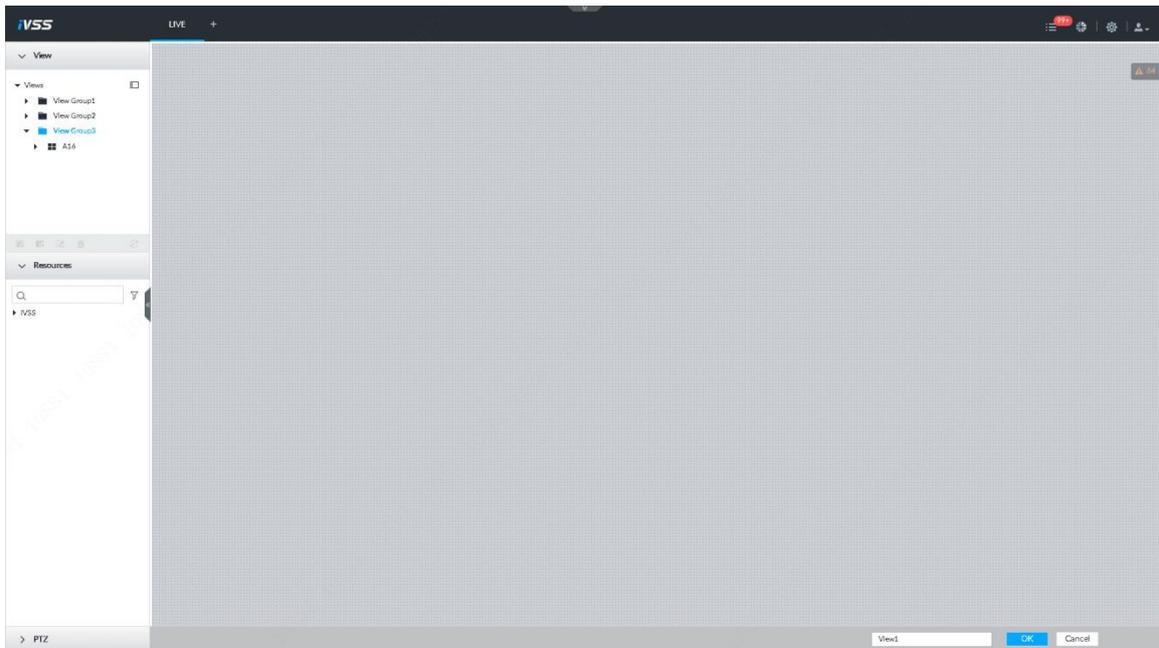


Figure 4-4

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

After added 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, drag another remote device to 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 according to the select remote device amount. Device max supports 36 view windows.
- Device automatically 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 adjust view window size according to remote device amount and playback pane.
- When adjusting view window position, please 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.

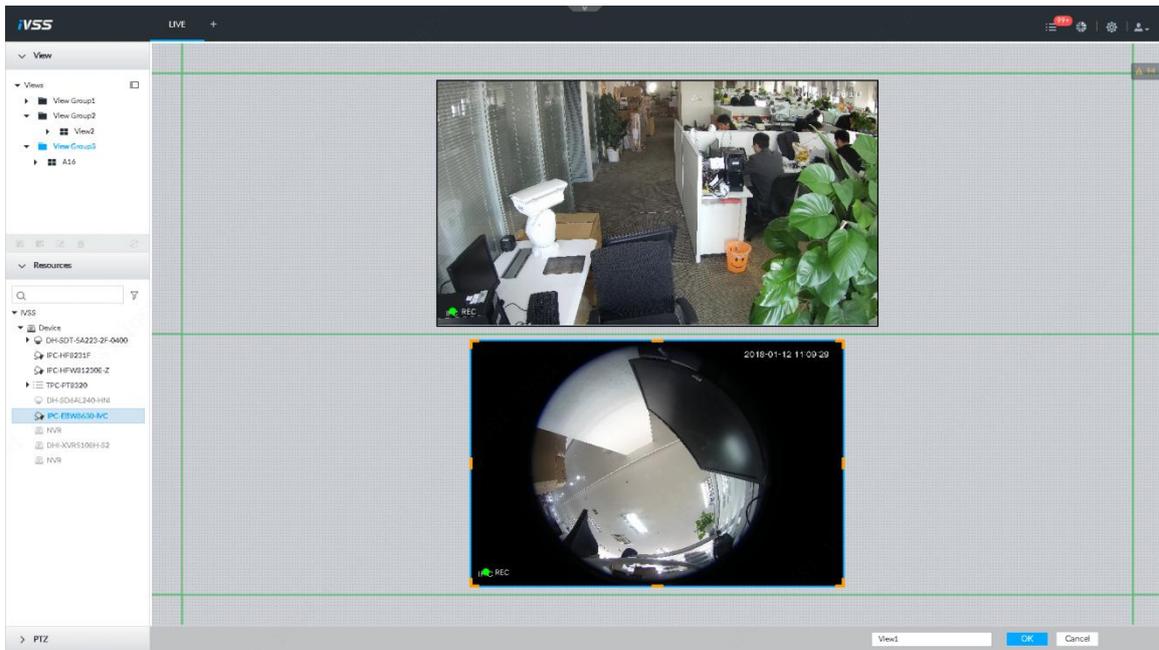


Figure 4-5

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 settings.

System pops 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.

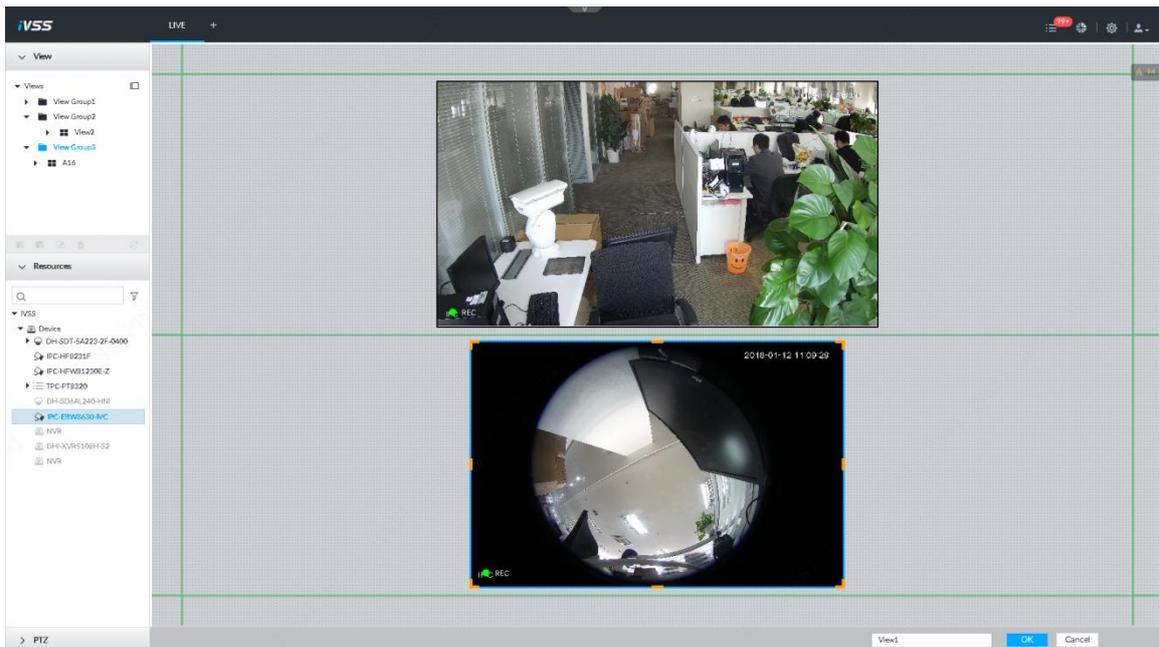


Figure 4-6

When enable the view, you can change video position, zoom video window ,etc.

 **Note**

- When you are adjusting view window position, you can only drag the view window to the grid of green background color. You cannot drag the view window to the grid of red background color.
- Move your mouse to the view window, device displays window task column. You can snapshot view or close video window.
- Right click view window, you can switch bit streams, set digital zoom, etc.

Name	Function
Exchange window position	Press one view window and drag it to the another view window, it is to exchange these 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. Please go to the view edit mode to set. Refer to user's manual for detailed information.
Zoom in video window	<ul style="list-style-type: none"> ● Once current view window amount is too much(more than 9),click one view window, device displays current view window at the center of the window in the zoom in mode. Click any other blank position, you can view window restores original size. ● Double click a view window, device displays view window at one window. Double click view window again or click any blank position, the view window restores original size.
Zoom in Window	When there are too much video windows (more than 9),click one video window, system display selected window at the center. Click any other position, the selected window restore original size. Double click a video window, system displays selected window at one-screen mode. Double click the selected window again or click any other position to restore original window display mode.
Add view window	On the device tree, double click the remote device or drag the remote device to the right pane, you can add remote device to 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 button. Close and enable view again, the view layout restores original layout.
Close view window	Move the mouse to one view window, click  to close the view window.  Note Close view window, device automatically adjusts view layout according to the rest remote device amount and play pane free space.

4.2.2 Preview

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

 **Note**

Refer to user's manual to enable AI detect function.

Go to the Live interface, enable view, device 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.

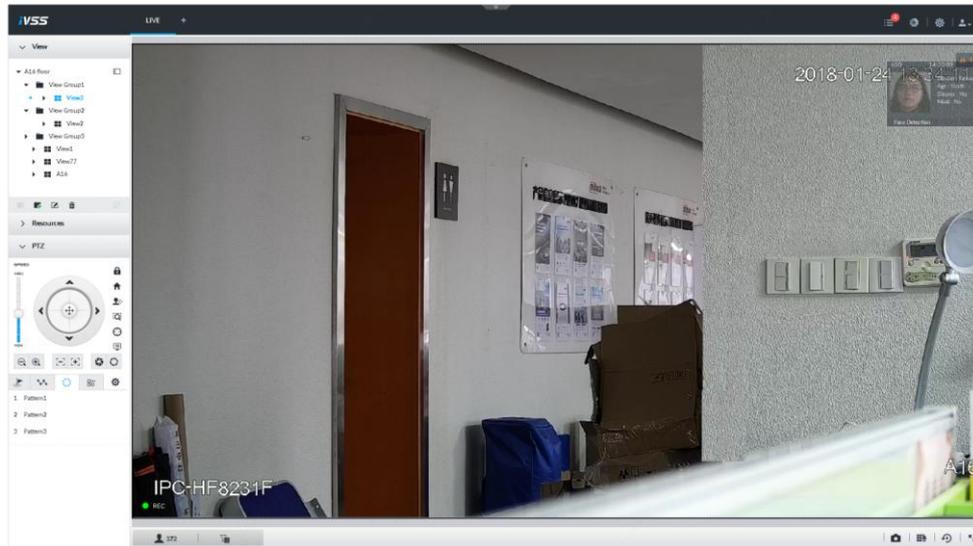


Figure 4-7

4.2.2.1 View image

On preview interface, click  to view AI detection image. See Figure 4-8.



Figure 4-8

- Click  to filter the Ai detection mode. See Figure 4-9

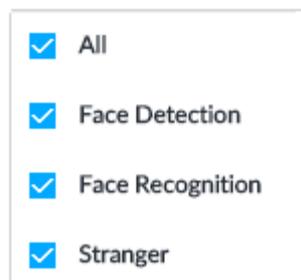


Figure 4-9

- Double click AI detection image, system displays the the 20 seconds video before and after the image.

✧ Click  to pause play. Now the icon becomes , click  to continue play.

✧ Click  to exit record interface. See Figure 4-10.

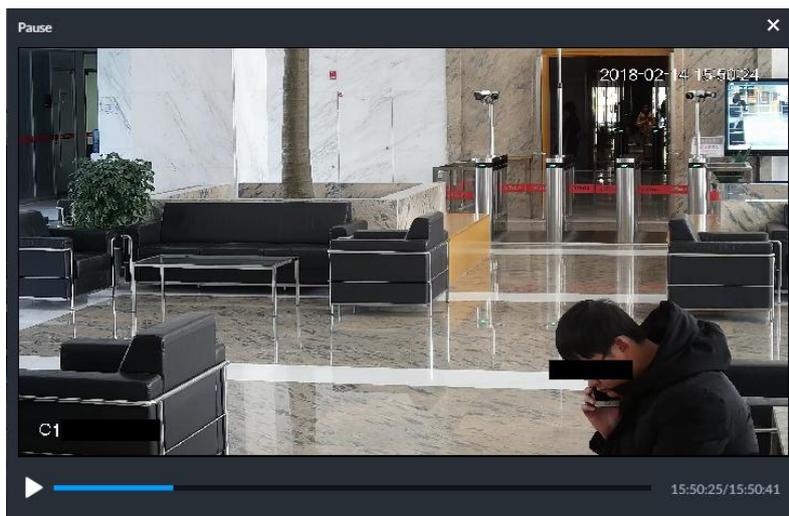


Figure 4-10

4.2.2.2 AI display settings

On the preview interface, click . Enter human face interface. See Figure 4-11. It is to set AI detection results displayed rule and features pane transparency.

Note

- Click Sync from AI-DIs, you can get global intelligent detection display rule from the device directly. Refer to user's manual for detailed information.
- Click Apply to all windows, it is to copy current configuration to other window(s).

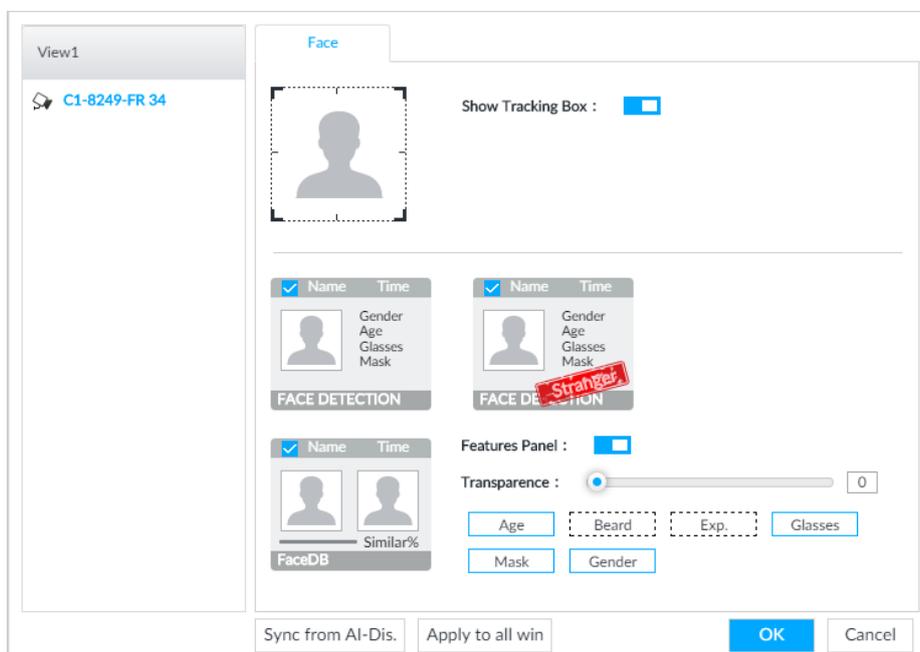


Figure 4-11

4.3 Playback Record File

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

Steps

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

Enter Search interface. See Figure 4-12.

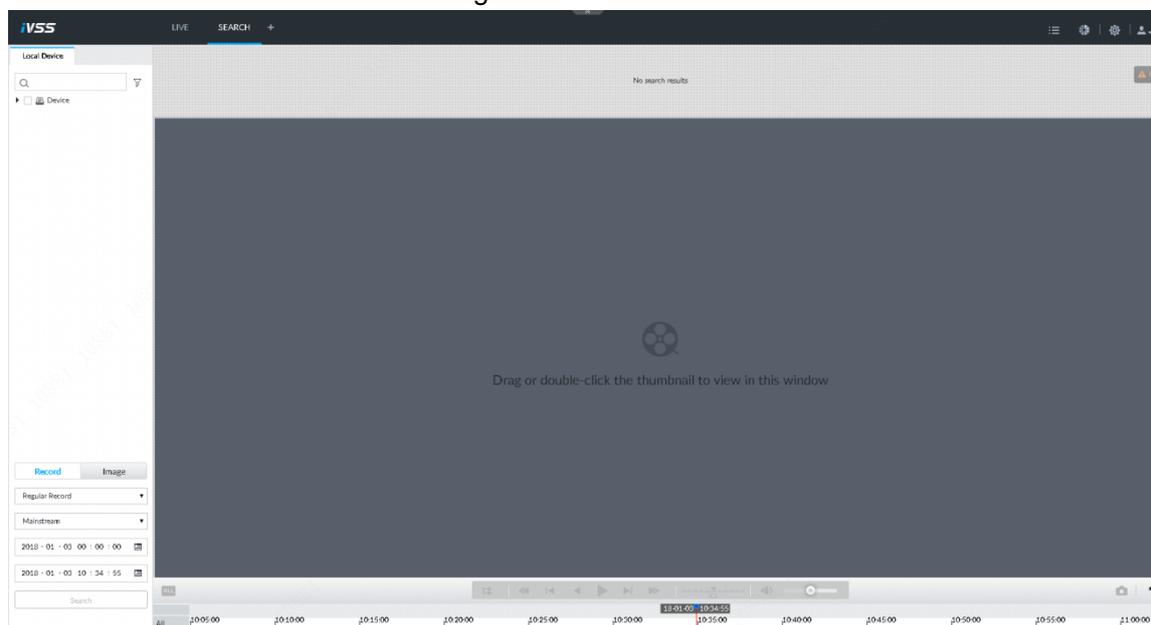


Figure 4-12

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 playing the record. See Figure 4-13.

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.
- The thumbnail with , it means system is playing record file of current thumbnail.
- Use the playback control bar to synchronization playback, slow playback, fast playback, backward playback, frame by frame playback and etc. Refer to user's manual for detailed information.

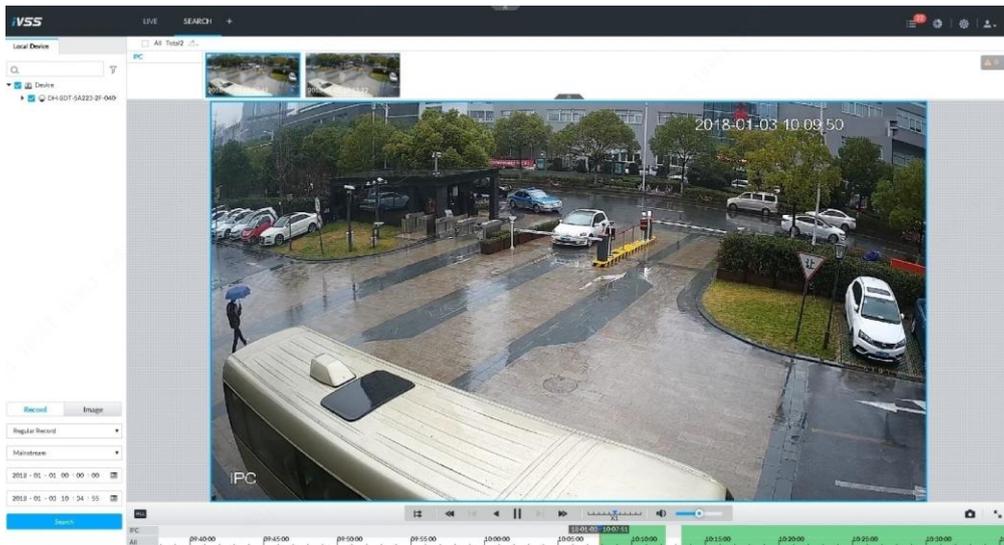


Figure 4-13

4.4 AI Detection

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



Note

Make sure the remote device supports AI detection function.

4.4.1 Enable AI plan

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



Note

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

Steps

- Step 1 On Setting interface click , or click  and then select Event.
Enter Event interface.
- Step 2 Select a remote device, from AI plan->AI plan->AI plan.
Enter AI plan interface. See Figure 4-14.

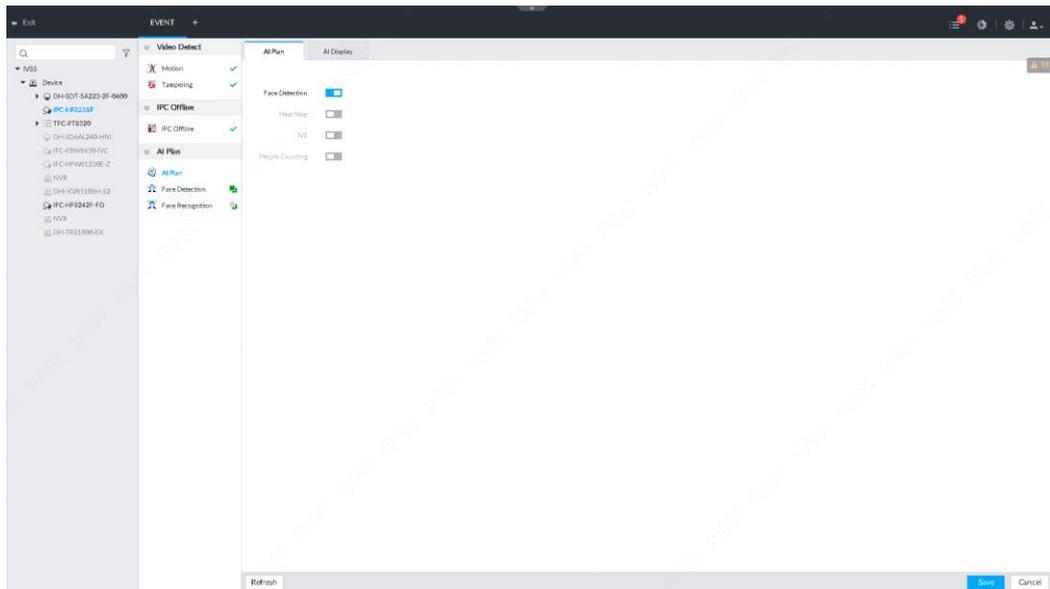


Figure 4-14

Step 3 Click to enable AI detection plan.

Step 4 Click Save.

4.4.2 Human face detection

It is to analyze the video from the remote device, and system can trigger an alarm once there is any detected human face information.

Preparation

Please make sure you have enabled human face detection plan. Refer to user's manual for detailed information.

Steps

Step 1 On Setting interface click , or click and then select Event.

Enter Event interface.

Step 2 Select a remote device, from AI plan->Face detection.

Enter AI plan interface. See Figure 4-15. The following figure is based on AI by camera.

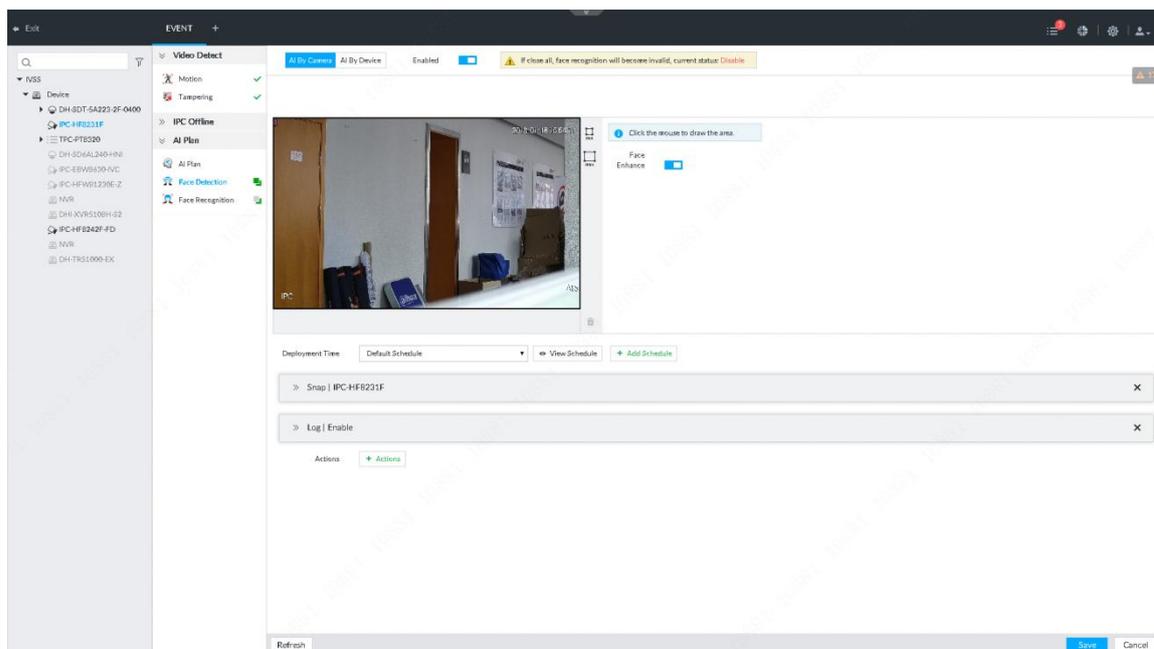


Figure 4-15

Step 3 Click AI by camera or AI by device, and then click  to enable intelligent function.

- AI by camera: The remote device supports intelligent detection such as smart network camera. The system needs to support detect and display the intelligent alarm information from the remote device and use the remote device to set intelligent detect and record playback.
- AI by device: The connected remote device does not support intelligent analysis function, system supports intelligent detection.

Step 4 Click  to enable Face Rol.

After enable Face Rol function, system displays enhanced human face zone on the surveillance window.

 **Note**

This function is for AI by camera mode only.

Step 5 Left click mouse and draw the human face detection pane on the video window.

- Click  or  to set human face detection minimum size and maximum size. System triggers an alarm once the detected human size is not larger than then maximum size or smaller than the minimum size.
- Select a human face detection zone you have drawn and then click  to delete.

Step 6 Click arm time and then select calendar from the dropdown list.

After set arm period, system triggers corresponding operations when there is an alarm in the specified period.

- Click  to view detailed schedule settings.
- If there is no plan or the added plan does not fit the actual requirements, click

 to add a schedule. Refer to user's manual for detailed

information.

Step 7 Set corresponding linkage event.

- Set alarm to trigger Record or Snap:

Click  **Actions** and then select Record or Snap, and then select the corresponding device to record or snap when an alarm occurs.



Note

- ◇ Select Snap, system can only current channel to snap.

- ◇ Click  **Actions** again, and then select Record, you can set to trigger several channels to record at the same time.

- Set alarm to trigger buzzer or log.

Click  **Actions** and then select buzzer and log. It is to enable buzzer or record log file when an alarm occurs.

Step 8 Click Save.

4.4.3 Human face comparison

It is to compare the human face detected image with the image on the human face database. Once similarity is equal to or more than the specified value, system can trigger an alarm.

Preparation

- Make sure you have added the human face database. Refer to chapter 4.4.2 Configuring face database for detailed information.
- If you want to use system to implement human face comparison, please enable human face detection function. Refer to chapter 4.4.2 Human face detection for detailed information.

Steps

Step 1 On Setting interface click , or click  and then select Event.

Enter Event interface.

Step 2 Select a remote device, from AI plan->Face recognition.

Enter face recognition interface. See Figure 4-16.

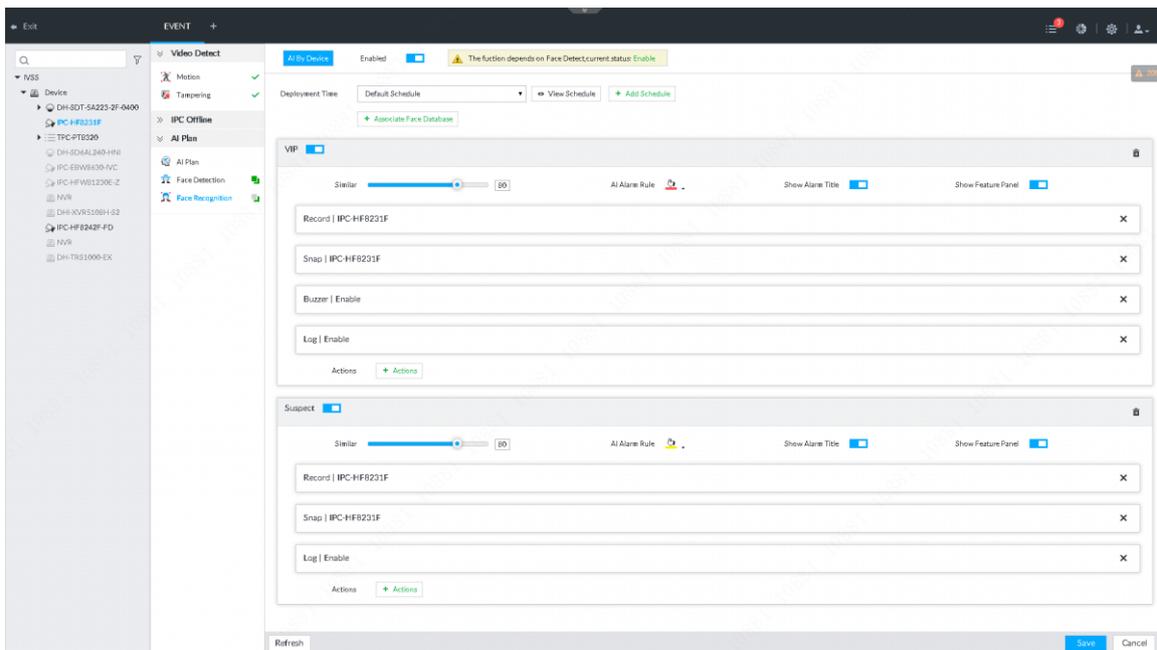


Figure 4-16

Step 3 Click AI by camera or AI by device, and then click to enable intelligent function.

- AI by camera: The remote device supports intelligent detection such as smart network camera. The system needs to support detect and display the intelligent alarm information from the remote device and use the remote device to set intelligent detect and record playback.
- AI by device: The remote device does not support intelligent analysis function, system supports intelligent detection.

Step 4 Click arm time and then select calendar from the dropdown list. After set arm period, system triggers corresponding operations when there is an motion detect alarm in the specified period.

- Click to view detailed schedule settings.
- If there is no plan or the added plan does not fit the actual requirements, click

to add a schedule. Refer to user's manual for detailed information.

Step 5 Set stranger mode.

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

Note

If the stranger mode is disabled, the preview interface displays human face detection pane once the human face comparison similarity is lower than the specified value.

1. Click to enable stranger mode.

System displays stranger mode interface. See Figure 4-17.

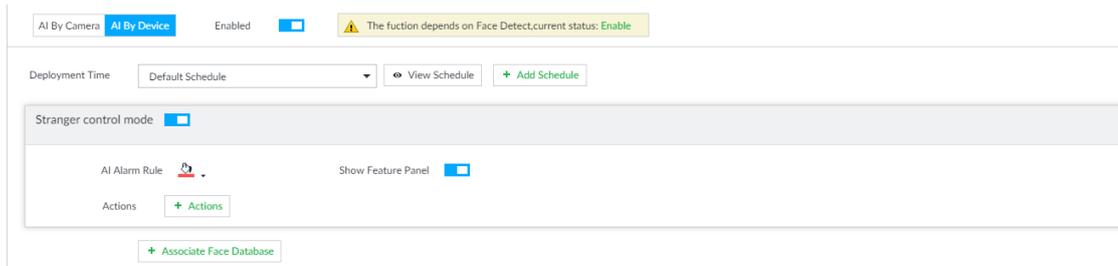


Figure 4-17

2. Set parameters.

Name	Function
AI alarm rule	Click the color zone to set alarm rule box color.
Features pane	Check the box to enable features pane function. System displays stranger pane once there is an alarm.

3. Click  to set alarm activation events.

Step 6 Set triggered human face database.

 **Note**

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

1. Click trigger face database, and then select the triggered human face database. Enable trigger human face database function.

2. Set parameters.

Name	Function
Similarity	It is to set human face similarity. System compares the human face with the image on the human face database, system triggers an alarm once the similarity reaches threshold you set here.
AI alarm rule	Click the color zone to set alarm rule box color.
Features pane	Check the box to enable features pane function. System displays features pane once there is an alarm.

3. Click  to set alarm activation events.

 **Note**

- Snapshot function is for current channel only.
- System can trigger several remote devices to record at the same time.

Step 7 Click Save.

4.5 Logout/Reboot/Shut down

It is to logout, reboot, and shutdown the device.

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

 **Note**

- Slight difference may be found in user interface. All the designs and software here are subject to change without prior written notice. Refer to the user's manual for detailed operation information.
- All trademarks and registered trademarks mentioned are the properties of their respective owners.
- If there is any uncertainty or controversy, please refer to the final explanation of us.
- Please visit our website for more information.