Capture advance

Digital Video Recorder (DVR)
User Manual

Issue	**V4.7.2**
Date	**2025-06-03**

Legal Notice

Trademark Statement：

VGA is a trademark of IBM Corporation.

The Windows logo and Windows are trademarks or registered trademarks of Microsoft Corporation.

Other trademarks or company names that may be mentioned in this document are the property of their respective owners.

Responsibility statement：

To the extent permitted by applicable law, in no event shall the Company compensate for any special, incidental, consequential, or consequential damages resulting from the contents of the documentation and the products described, nor any Compensation for loss of profits, data, goodwill, loss of documentation, or expected savings.

The products described in this document are provided "**as it is at present**", except as required by applicable law, the company does not provide any warranty or implied warranties, including but not limited to, merchantability, quality satisfaction, and fitness for a particular purpose, does not infringe the rights of third parties, and other guarantees.

Privacy Protection Reminder:

If you have installed our products, you may **collect personal information** such as faces, fingerprints, license plates, emails, telephones, and GPS. In the process of using the product, you need to comply with the privacy protection laws and regulations of your region or country to protect the legitimate rights and interests of others. For example, provide clear and visible signs, inform the relevant rights holders of the existence of video surveillance areas, and provide corresponding contact information.

About This Document：

- This document is for several models. The appearance and function of the products are subject to the actual products.
- Any loss caused by failure to follow the instructions in this document is the responsibility of the user.
- This document will be **updated in real time** according to the laws and regulations of the relevant region. For details, please refer to the product's paper, electronic CD, QR code, or official website. If the paper and electronic files are inconsistent, please refer to the electronic file.
- The company reserves the right to **modify any information** in this document at any time.
- The revised content will be **added to the new version** of this document without prior notice.
- This document may contain **technical inaccuracies, inconsistencies with product features** and **operations**, or typographical errors, which are subject to the company's final interpretation.
- If the obtained PDF document cannot be opened, please use the latest version of the most mainstream reading tool.

Network Security Advice

Required measures to ensure basic network security of equipment:

Modify the password regularly and set a strong password.

Devices that do not change the password regularly or use a weak password are the easiest to hack. Users are advised to modify the default password and use strong passwords whenever possible (minimum of 6 characters, including uppercase, lowercase, numbers, and symbols).

Update firmware

According to the standard operating specifications of the technology industry, the firmware of DVR, and cameras should be updated to the latest version to ensure the latest features and security of the device.

The following recommendations can enhance your device's network security:

1. **Change your password regularly**

   Regularly modifying the login credentials ensures that authorized users can log in to the device.

2. **Modify the default HTTP and data ports**

   Modify the device's default HTTP and data ports, which are used for remote communication and video browsing.

   These two ports can be set to any number between 1025 and 65535. Changing the default port reduces the risk of the intruder guessing which port you are using.

3. **Use HTTPS/SSL encryption**

   Set up an SSL certificate to enable HTTPS encrypted transmission. The information transmission between the front-end device and the recording device is fully encrypted.

4. **Enable IP filtering**

   After IP filtering is enabled, only devices with the specified IP address can access the system.

5. **Only forward the ports that must be used**

   Only forward the network ports that must be used. Avoid forwarding a long port area. Do not set the device's IP to DMZ.

   If the camera is connected locally to the DVR, you do not need to forward the port for each camera. Only the ports of the DVR need to be forwarded.

6. **Use a different username and password for the video surveillance system.**

   In the unlikely event that your social media account, bank, email, etc. account information is leaked, the person who obtained the account information will not be able to invade your video surveillance system.

7. **Restrict the permissions of the ordinary account**

   If your system is serving multiple users, make sure that each user has permission to access only its permissions.

8. **Support UPNP**

   When the UPnP protocol is enabled, the router will automatically map the intranet ports. Functionally, this is user-friendly, but it causes the system to automatically forward the data of the corresponding port, causing the data that should be restricted to be stolen by others.

   If you have manually opened HTTP and TCP port mappings on your router, we strongly recommend that you turn this feature off. In actual usage scenarios, we strongly recommend that you do not turn this feature on.

9. **Support SNMP**

   If you do not use the SNMP, we strongly recommend that you turn it off. The SNMP function is limited to temporary use for testing purposes.

10. **Support Multicast**

    Multicast technology is suitable for the technical means of transmitting video data in multiple video storage devices. There have been no known vulnerabilities involving multicast technology so far, but if you are not using this feature, we recommend that you turn off multicast playback on your network.

11. **Check logs**

    If you want to know if your device is secure, you can check the logs to find some unusual access operations. The device log will tell you which IP address you have tried to log in from or what the user has done.

12. **Physically protect your device**

    For the safety of your device, we strongly recommend that you physically protect your device from unauthorized boring operations. We recommend that you place the device in a locked room and place it in a locked cabinet with a locked box.

    It is highly recommended that you use coaxial cable to connect analog cameras to DVR.

13. **Network isolation between DVR and IP cameras**

    We recommend isolating your DVR and IP cameras from your computer network. This will protect unauthorized users on your computer network from having access to these devices.

About This Document

Purpose

This document describes in detail the installation, use, and interface operation of the DVR (Network Video Recorder) device.

Symbol Conventions

The symbols that may be found in this document, are defined as follows:

Symbol	Description
⚠ DANGER	Indicates an immediate and critical hazard. If not avoided, will result in death or life-threatening injuries.
⚠ WARNING	Indicates a potential hazard with moderate risk. If not avoided, could lead to non-life-threatening injuries (e.g., burns, cuts, or temporary disability).
⚠ CAUTION	Indicates a risk-prone scenario. If not avoided, may cause property damage, data loss, impaired performance, or unintended operational outcomes.
🔑 TIP	Provides helpful tips to solve problems or save time.
📖 NOTE	Highlights important additional information that supplements the main content.

Safety instructions

The following are the correct uses of the product. To prevent danger and property damage, please read this manual carefully before using the device and strictly comply when using it. Please save the manual after reading it.

Requirements

- **Put On Desktop:** The DVR device does not support wall mounting.
- **Avoid Sunlight and Heat Sources:** Do not place or install the device in direct sunlight or near heat-generating equipment.
- **Environmental Conditions:** Do not install the device in a place subject to high humidity, dust, or soot.
- **Avoid falling:** Please keep the equipment installed horizontally or install the equipment in a stable place, taking care to prevent the product from falling.
- **Keep Dry:** Do not drop or spill liquid into the device, and ensure that no liquid-filled items are placed on the device to prevent liquid from flowing into the device.
- **Maintain Ventilation:** Install the device in a well-ventilated area, and do not block the ventilation openings of the device.
- **Correct Use:** Use the device only within the rated input and output range.
- **Keep Assembled:** Do not disassemble the device at will.
- **Transportation:** Please transport, use, and store the device within the permissible humidity and temperature range.

Power Requirement

- Be sure to use the specified manufacturer's model battery; otherwise, there is a danger of explosion!
- Be sure to use the battery as required; otherwise, there is a danger of the battery catching fire, exploding, or burning!
- Only use the same model of battery when replacing the battery!
- Be sure to dispose of the used battery as per the instructions of the battery!

- Be sure to use the power adapter that meets the standard of the device; otherwise, the personal injury or equipment damage caused by the user will be borne by the user.
- Use a power supply that meets the SELV (Safety Extra Low Voltage) requirements and supply power according to the rated voltage of IEC60950-1 following the Limited Power Source. The specific power supply requirements are based on the equipment label.
- Connect the Class I product to the power outlet with a protective ground connection.
- The appliance is coupled to the port unit. Keep it at a proper angle for normal use.

Important Statement

Users are required to enable and maintain the lawful interception (LI) interfaces of video surveillance products in strict compliance with relevant laws and regulations. Installation of surveillance devices in an office area by an enterprise or individual to monitor employee behavior and working efficiency outside the permitted scope of the local law and use of video surveillance devices for eavesdropping for illegal purposes constitute behaviors of unlawful interception.

This manual is only for reference and does not ensure that the information is consistent with the actual products. For consistency, see the actual products.

Contents

1 Preface

1.1 Product Description

This product is a **high-performance** DVR device. The product has a local preview, video multi-screen split display, local real-time storage function of video files, and added support for mouse shortcut operation, remote management, and control.

This product supports three **storage methods**: central storage, front-end storage, and client storage. The front-end monitoring point can be located anywhere in the network without geographical restrictions. It is combined with other front-end devices such as **network cameras**, network construction of **network video servers**, and professional video **surveillance systems** to form a powerful security monitoring network.

In the **networked deployment system** of this product, the central point and the monitoring point need only one network cable to connect. There is no need to connect video and audio cables. The operation is simple, and the cost of wiring and maintenance is low.

This product is widely used in public security, transportation, electric power, education, and other industries.

1.2 Product Features

Cloud Upgrade: For devices that have access to the public network, you can update the software of the devices online.

Real-time Monitoring: It has a VGA (Video Graphics Array) port and an HDMI (High Definition Media Interface) port. It can realize monitoring functions through monitors and displays, and support VGA and HDMI output at the same time.

Playback: Each channel has independent real-time recordings and multiple functions, such as retrieval, playback, network monitoring, video query, and download. Please refer to the c*hapter Playback*.

- The exact time when the event occurred can be displayed during playback of the recording.
- You can select any area of the screen for partial magnification.

User Management: Each user group has a rights management set, which can be selected autonomously. The total rights set is a subset, and the user rights in the group cannot exceed the rights management set of the user group.

Storage Function: According to the user's configuration and policies (alarm or time settings), the corresponding audio and video data transmitted by the remote device is stored in the DVR device. For details, please refer to the chapter Storage Management.
Users can record by WEB mode as needed. The video files are stored on the computer where the client is located. Please refer to *chapter Storage*.

Alarm Function: Real-time response to external alarm input, correct processing according to the user's preset linkage settings, and corresponding prompts.
The setting options of the central alarm receiving server are provided so that the alarm information can be actively and remotely notified, and the alarm input can come from various external devices connected.
The alarm information can be notified to the user by mail or APP push information.

Network Monitoring: Through the network, the audio and video data of the IP camera or NVS (Network Video Server) of the DVR device is transmitted to the network terminal for decompression and reproduction.
The device supports **8 simultaneous online users** to perform streaming operations.
The audio and video data is transmitted using protocols such as **HTTP** (Hyper Text Transfer Protocol), **TCP** (Transmission Control Protocol), **UDF** (User Datagram Protocol), **MULTICAST**, **RTP** (Real-time Transport Protocol), and **RTCP** (Real Time Streaming

Protocol).
Use **SNMP** (Simple Network Management Protocol) for some alarm data or information.
Support **WEB** mode to access the system in WAN, and LAN environments.

Split Screen: Image compression and digitization are used to compress several images in the same scale and display them on the display of a monitor. **1/4/8/9/16/32 screen splitting** is supported during preview; **1/4/9/16 screen splitting** is supported during playback.

Recording Function: The device supports **regular recording, motion detection** recording, **alarm** recording, and intelligent recording. The recording file is placed on the **hard disk device**, **USB** (Universal Serial Bus) device, and **client PC** (personal computer). It can be connected to the WEB terminal, USB device, or local device. Query and playback the stored video files.

Backup Function: Support **USB**, **eSATA** video backup, and **NAS** (Network Attached Storage).

External Device Control: The peripheral control function is supported, and the control protocol and connection interface of each peripheral can be set as you need.
Support transparent data transmission of multiple interfaces, such as **RS232** and **RS485**.

Accessibility:

- Supports video **NTSC** (National Television Standards Committee) system and **PAL** (Phase Alteration Line) system.
- Supports **system resource** information and **real-time display** of running status.
- Supports for **logging recording**.
- Supports **local GUI** (graphical user interface) output and quick menu operation via mouse.
- Supports playback of audio and video from **remote IPC** or **NVS devices**.

NOTE

For other functions, please see the following text.

2 Product Structure

2.1 Front Panel

Figure 2-1 Model A

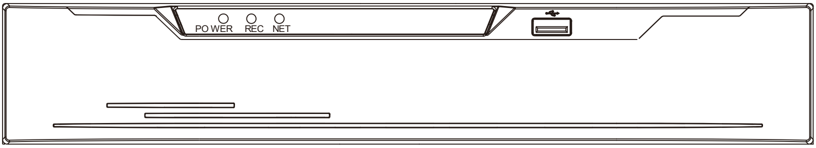


Table 2-1 Front panel function

Port	Description
PWR	When the DVR is operating, the PWR indicator is steady. When the DVR is shut down, the PWR indicator is turned off.
HDD	Hard disk status indicator. This indicator flashes when data is transmitted.
⭠	Only connected to a USB mouse.

Figure 2-2

2.2 Back Panel

Different models have different rear panels. This chapter explains the functions of all interfaces; It cannot represent that the device you purchased has all the functions. Please refer to the actual product, and the pictures are for reference only.

Figure 2-3 Back panel (model 1)

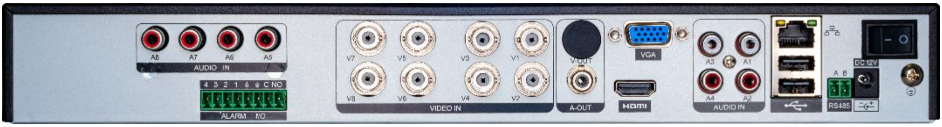


Figure 2-4 Back panel (model 2)

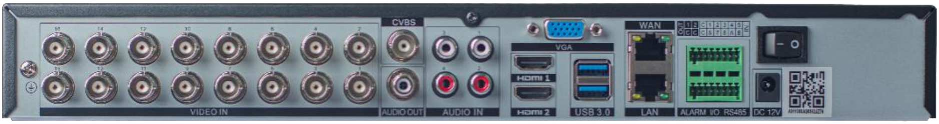
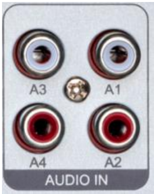
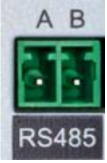
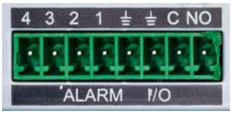


Table 2-2 Rear panel function

Port	Description
 Network interface	RJ45 10/100/1000 Mbps adaptive Ethernet interface, connected to a switch or router; the cameras are connected to the same local area network, and they can be added to the DVR. This port can be connected to an external Wide Area Network.
 LAN	LAN/LAN2, RJ 45 10/100/1000 Mbps adaptive Ethernet interface, connected to switch or router, the cameras are connected to the same local area network, and they can be added to DVR. If there is only a LAN interface, the LAN can be connected to an external Wide Area Network.
 WAN	WAN/LAN1 RJ 45 10/100/1000 Mbps adaptive Ethernet interface, connected to a switch or router, is connected to an external Wide Area Network, which is for multi-users to manage the DVR.
	Video in, plug the analog cameras.
 Audio input	Audio input can be connected to audio input devices such as microphones. These interfaces are required for the intercom.
	Audio output can be connected to audio output devices such as speakers. These interfaces are required for the intercom.

Audio output	
 HDMI	HDMI video output interface; users use an HDMI cable to connect to the monitor.
 VGA	Video output interface; users use a VGA cable to connect to the monitor. If the device has an auxiliary screen function, the VGA will show the content of the auxiliary screen.
 CVBS	CVBS video output interface; users use coaxial cable to connect to the analog monitor.
 USB port	Only connected to 3.0 U disk.
 ESATA port	Connected external hard disk interface. This port is applied in DVR.
	A/B represents the two terminals of RS485
 Alarm output/Alarm input	Alarm output/Alarm input and RS485. C represents the COM terminal, and OUT represents the alarm output terminal and can be connected to alarm output devices such as alarm lights and buzzers. IN represents the alarm input terminal, which can be connected to alarm input devices such as doorbells and switches.
 GND	GND, safety grounding screw.

 Power socket	AC 110V/220V power input interface
 Power switch	Power switch
 Power socket	Connected to an external power adapter DC 12V.

2.3 Important Notes

Thank you for choosing the DVR. Please read the user manual carefully before using this product.

The DVR is a complex system-based device. To avoid misoperations and malfunctions caused by environmental factors and human factors during installation, commission, and application, note the following points when installing and using this product:

Read the user manual carefully before installing and using this product.

- Use **dedicated monitoring hard disks** as the storage devices of the DVR with high stability and competitive price/performance ratios (the quality of hard disks sold on markets varies greatly with different brands and models).
- Do not open the enclosure of this product unless performed by **a professional person** to avoid damage and electric shock.
- We are not liable for any **video data loss** caused by improper installation, configuration, operation, or hard disk errors.
- All images in the document are for **reference only**; please refer to the actual products.

2.4 About This User Manual

Please note the following points before using this user manual.

- This user manual is intended for persons who **operate and use** the DVR.
- The information in this user manual applies to the full series DVR, **HDDVR4C2T**, as an example for description.

- **Read this user manual** carefully before using the DVR, and follow the methods described in this manual when using the DVR.
- If you have any doubts when using the DVR, contact your product seller.
- As our products are subject to continuous improvement, we reserve the right to modify the product manual without notice and without incurring any obligation.

2.5 Installation Environment and Precautions

Installation environment

Table 2-3 defines the installation environment of the DVR.

Table 2-3 Installation environment

Item	Description
Electromagnetism	The DVR conforms to national standards of electromagnetic radiation and does not cause harm to the human body.
Temperature	**–10ºC** to + **50ºC**
Humidity	Less than **90% RH**
Atmospheric pressure	**86 Kpa** to **106 Kpa**
Power supply	DC 12V 4A/ AC 110V/220V 4A
Power consumption	<15W (not including the hard disk)

Installation precautions

Note the following points when installing and operating the DVR:

- The input of the power adapter should be correct; the voltage **can't exceed ±20%**. Do not use the DVR when the voltage is too high or too low.
- Install the DVR **horizontally**.
- Avoid direct sunlight on the DVR and keep it away from any heat sources and hot environments.
- Connect the DVR to other devices correctly during installation.
- The DVR is not configured with any hard disk upon delivery. Install one or more hard disks when using the DVR for the first time.

The DVR identifies hard disk capacity automatically and supports mainstream hard disk models. You'd better use a **high-quality hard disk** so that the DVR can work stably and reliably. Please refer to Chapter 9 Disk Compatibility

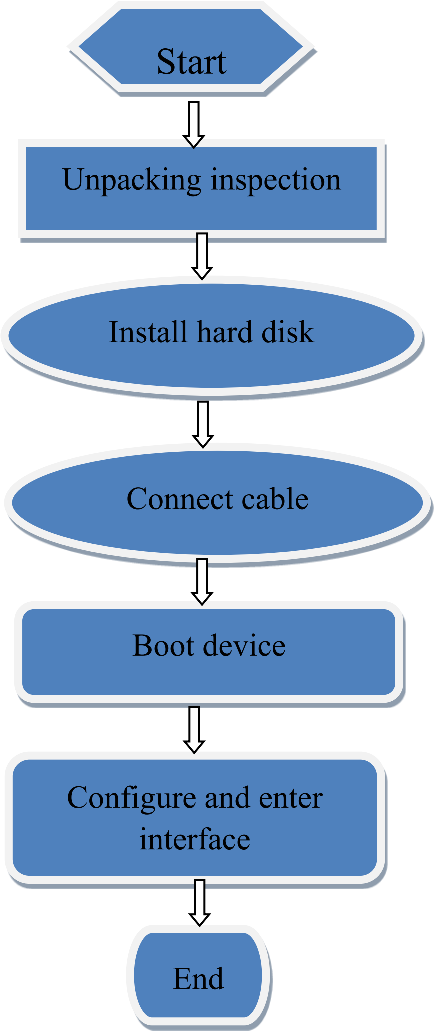
Other Precautions

- Clean the DVR with a piece of soft and dry cloth. Do not use chemical solvents.
- Do not place objects on the DVR.

The DVR meets the national standards of electromagnetic radiation and does not cause electromagnetic radiation to the human body.

3 Install device

3.1 Process



Step 1 Check the appearance, packaging, and label of the device to make sure there is no damage.

Step 2 Install the hard disk and fix it to the device bracket.

Step 3 Connect the device cable.

Step 4 Make sure the device is properly connected. Power up and turn on the device.

Step 5 Configure the initial parameters of the device. The boot wizard contains network configuration, adds cameras, and manages disks. For details, please refer to the *Chapter Wizard*.

3.2 Unpacking Inspection

When you receive the video recorder, please check it against the following table.

Should you have any issues, please don't hesitate to contact our after-sales support.

Table 3-1 Unpacking inspection

No	Item		Check content
1	Overall packaging	Appearance	Is there any obvious damage
		Package	Is there an accidental impact
		Accessories	Is it complete
2	Label	Label of device	Is the equipment model consistent with the order contract? Whether the label is torn NOTE Do not tear or discard, otherwise warranty service is not guaranteed. When you call the company for sales personnel calls, you need to provide the serial number of the product on the label.
3	Cabinet	Package	Is there any obvious damage
		Data cable, power cable, fan power supply, and motherboard	Is the connection loose? NOTE If it is loose, please contact the company's after-sales personnel.

3.3 Install Hard Disk

Check if the hard disk is installed during the first installation. Please use the recommended hard disk model. For more details, see ***Chapter 9 Disk Compatibility.*** It is not recommended to use a PC dedicated hard disk.

CAUTION

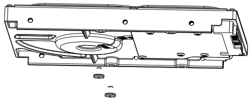
- When replacing the hard disk, please **turn off the power** and then open the device to replace the hard disk.
- Please use the monitoring dedicated SATA hard disk recommended by the hard disk manufacturer.
- Choose the hard disk capacity according to the recording requirements.

3.3.1 Install One Or Two Hard Disks

Step 1 Remove the screws for fixing the upper cover and take down the cover.

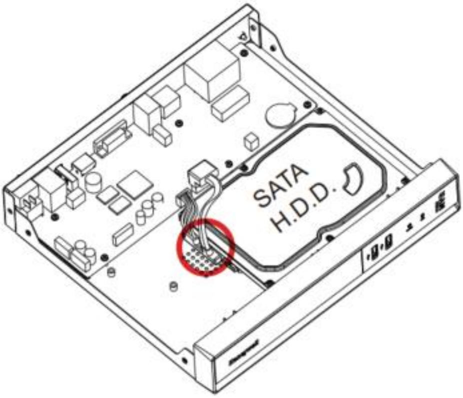
Step 2 Take out the screws and silicone cushion, pass the screws through the silicone cushion, and secure it to the screw holes, as shown in Figure 3-1.

Figure 3-1 Installing the hard disk screws



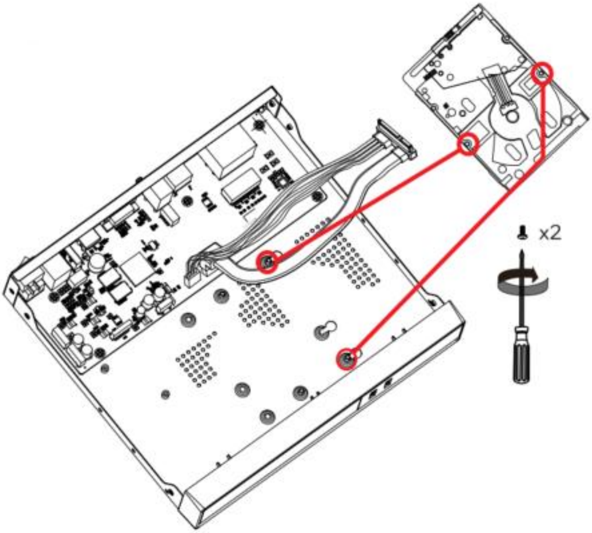
Step 3 Pass the screws through the holes on the base and put the hard disk in place, as shown in Figure 3-2.

Figure 3-2 Install hard disk



Step 4 Turn the device over, and fasten the fixing of the rest 2 screws, as shown in Figure 3-3.

Figure 3-3 Install hard disk



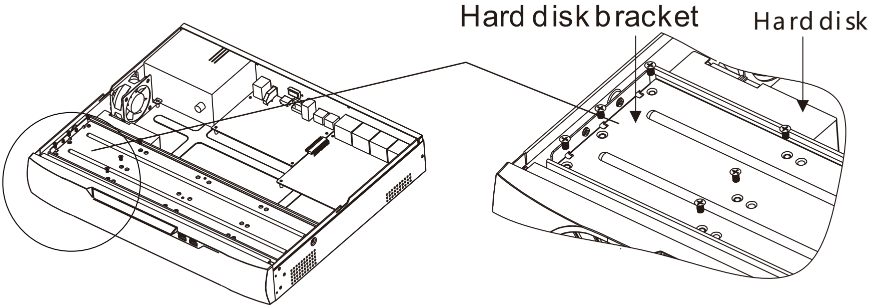
Step 5 Insert the hard disk data cable and power cable, then put back the upper cover and fasten the fixing screws.

3.3.2 Install Four Hard disks

Step 1 Remove the top cover by loosening the screws.

Step 2 Put the hard disk under the hard disk bracket, hold the hard disk with one hand and aim the hard disk hole at the bracket hole, and then tighten the screws to fix it (first install the hard disk near the fan), as shown in Figure 3-4.

Figure 3-4 Installing the hard disks



Step 3 Install other hard disks following step 2.

Step 4 Insert the hard disk data cable and power cable, and then put back the upper cover and tighten the fixing screws.

NOTE

The hard disk is strictly detected during device startup. If the detection result fails, the possible causes are as follows.

- The hard disk is new and is not formatted. Log in to the system and format the hard disk.
- The hard disk is formatted, but the file system is inconsistent with the file system supported by the DVR. Format the hard disk.
- The hard disk is damaged.

4 Basic Operations

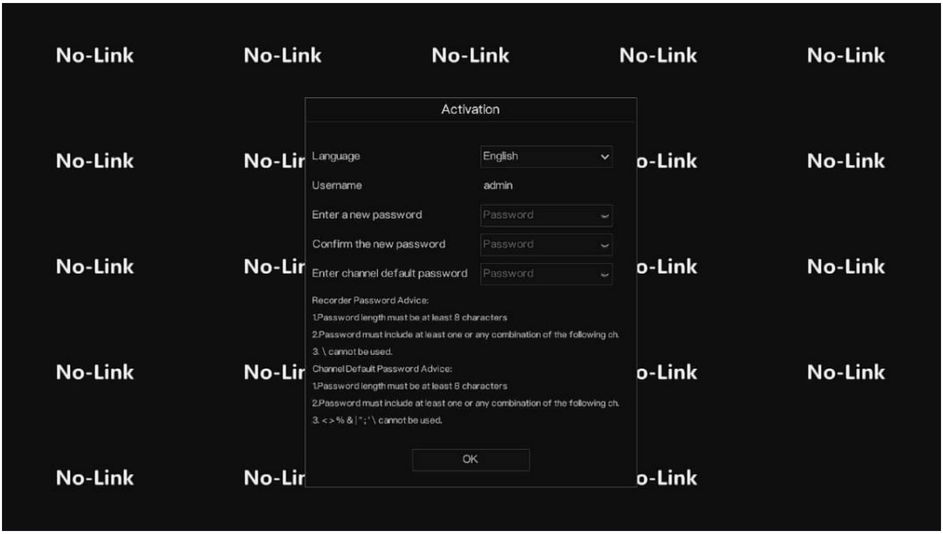
4.1 Power on the Device

⚠ **CAUTION**

- Ensure that the DVR is correctly connected to a power supply; and a display is correctly connected to the high-definition multimedia interface (HDMI) or video graphics array (VGA) port of the DVR before powering on.
- In some environments, an abnormal power supply may cause the failure of the DVR to work properly and even damage the DVR in severe cases. It is recommended to use a **regulated power supply** to power up the DVR in such environments.

After connecting the DVR to a power supply, the power indicator is always on. Start the DVR. The real-time video screen is displayed as shown in Figure 4-1.

Figure 4-1 Real-time video screen



Language English

Username admin

Enter a new password Password

Confirm the new password Password

Enter channel default password Password

Recorder Password Advice:

1.Password length must be at least 8 characters

2.Password must include at least one or any combination of the following ch.

3. \ cannot be used.

Channel Default Password Advice:

1.Password length must be at least 8 characters

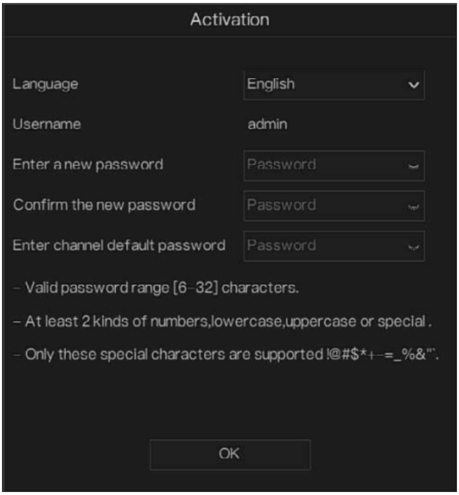
2.Password must include at least one or any combination of the following ch.

3. < > % & | " ; ' \ cannot be used.

4.2 Activation

First-time users: Create a password when prompted, then proceed to the login page, as shown in Figure 4-2. Set the password as per the table.

Figure 4-2 Activation



Activation

Language: English

Username: admin

Enter a new password: Password

Confirm the new password: Password

Enter channel default password: Password

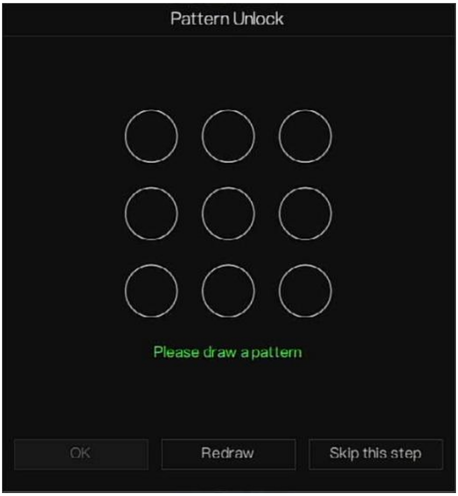
- Valid password range [6–32] characters.
- At least 2 kinds of numbers,lowercase,uppercase or special .
- Only these special characters are supported !@#$*+-=_%&"'.

Table 4-1 Description of activation

Name	Description
Username	The default username is **admin**, and “admin” is super administrator.
Password	Valid password range 6-32 characters. At least 2 kinds of numbers, lower case, upper case, or special characters contained. Only these special characters are supported！ @#&*+=-%&”`(),/’.:;< >?^|~[]{}. The channel default password limit is not empty.
Confirm password	
Channel password	The DVR channel connection password is the camera login password.

Users can set the pattern unlock to log in to the device, as shown in Figure 4-3.

Figure 4-3 Set pattern unlock

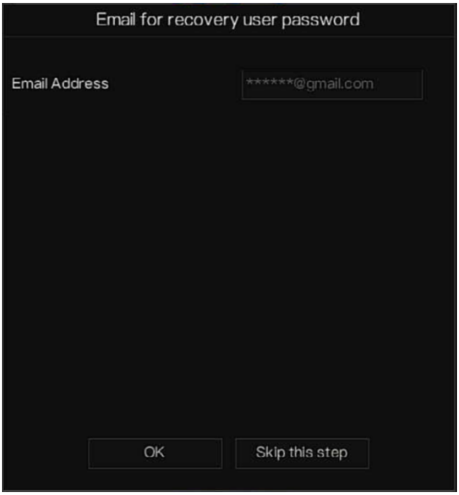


NOTE

- After setting pattern unlock, the system default login will be **pattern unlock login**. If pattern unlock is not set, you need to enter the password to log in.
- If you don't need to set the pattern to unlock, click "Skip this step".

Allow the mailbox to receive a verification code. The password will be reset when you forget it, as shown in Figure 4-4.

Figure 4-4 Set Email



Email for recovery user password

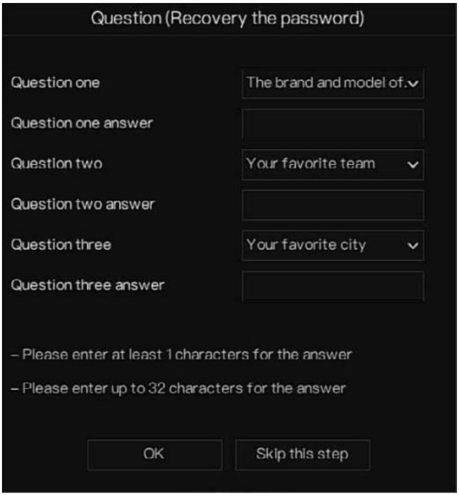
Email Address: ******@gmail.com

NOTE

- Set the email address; if you **forget the password**, you can use the email address to receive the verification and **reset the password**.
- If the email address is not set, you can reply to the secure question or send the **QR code** to the seller to get **the temporary password** to log in to the device.
- If you don't need to set the email, click "Skip this step".

Set the secure questions to create a new password in case the user forgets the password.

Figure 4-5 Set question



Question (Recovery the password)

Question one: The brand and model of

Question one answer:

Question two: Your favorite team

Question two answer:

Question three: Your favorite city

Question three answer:

– Please enter at least 1 characters for the answer

– Please enter up to 32 characters for the answer

NOTE

- The user can set three questions, and if they forget the password, they can answer the question and enter the reset password interface.
- Questions one can be set: Your favorite animal
    - Company name of your first job
    - The name of the first boy/girl you like
    - The worst security question you have ever seen
    - The funniest worst design you have ever seen
    - Your favorite team
    - Your favorite city
- The three question options cannot be set to the same issue.
- The answer requires a minimum of four characters and a maximum of 32 characters.
- If you do not want to set a password question, you can click Skip this step.

4.3 Wizard

Log in to the DVR; the wizard is showing on live video, click **Start Wizard,** and the pop-up window will show as Figure 4-6.

Figure 4-6 Wizard

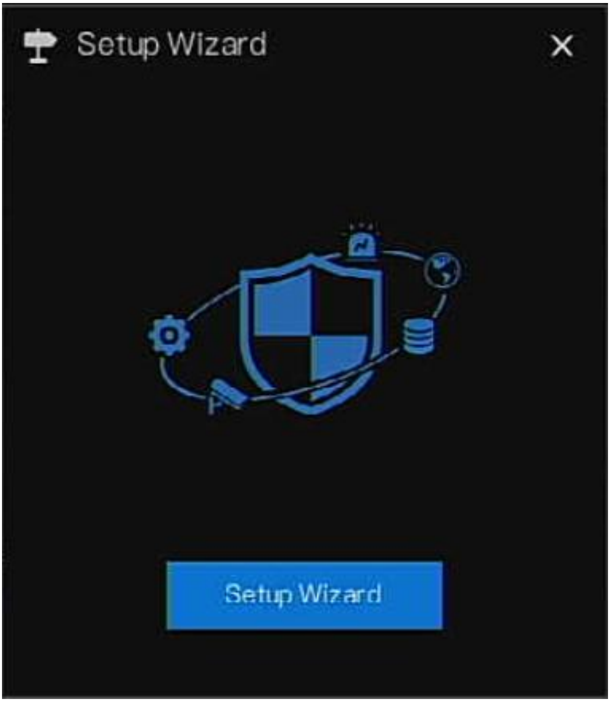
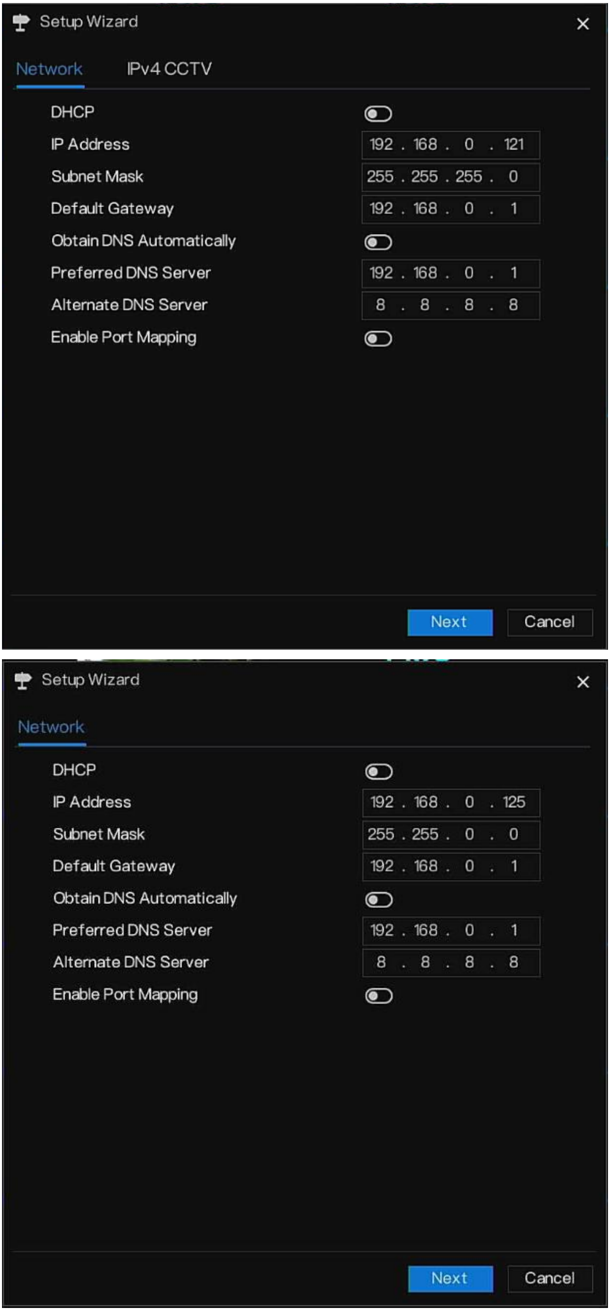


Figure 4-7 Wizard of network



DHCP

IP Address 192 . 168 . 0 . 121

Subnet Mask 255 . 255 . 255 . 0

Default Gateway 192 . 168 . 0 . 1

Obtain DNS Automatically

Preferred DNS Server 192 . 168 . 0 . 1

Alternate DNS Server 8 . 8 . 8 . 8

Enable Port Mapping

DHCP

IP Address 192 . 168 . 0 . 125

Subnet Mask 255 . 255 . 0 . 0

Default Gateway 192 . 168 . 0 . 1

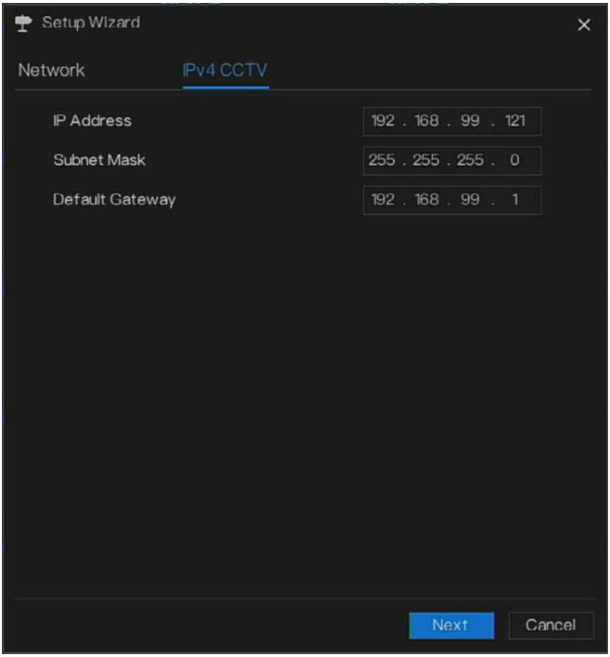
Obtain DNS Automatically

Preferred DNS Server 192 . 168 . 0 . 1

Alternate DNS Server 8 . 8 . 8 . 8

Enable Port Mapping

Figure 4-8 IPv4CCTV



IP Address 192 . 168 . 99 . 121

Subnet Mask 255 . 255 . 255 . 0

Default Gateway 192 . 168 . 99 . 1

Step 1 Contains the parameter, details please refer to Table 4-1.

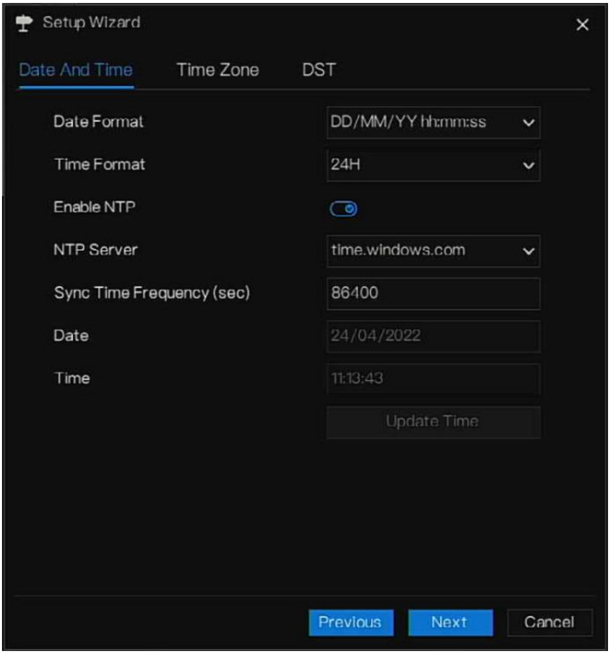
Table 4-1 Network parameter

Parameter	Description	Configuration
DHCP	Enable DHCP, the device will obtain the IP address from the DHCP server.	[Setting method] Enable
IP Address	Set the IP of the device when DHCP is disabled	[Setting method] Manual
Subnet mask	Set the subnet mask of the device	[Setting method] Manual [Default value] 255.255.255.0
Gateway	If the user wants to access the device, he must set that	[Setting method] Manual [Default value] 192.168.0.1

Parameter	Description	Configuration
Obtain DNS automatically	Enable the function to get the DNS address automatically. If you learn about the local DNS server IP, you can input the preferred DNS server and alternate DNS server manually.	[Setting method] Enable
Preferred DNS Server	In the Preferred DNS box, enter the IP address of the DNS.	[Setting method] Manual [Default value] 192.168.0.1
Alternate DNS Server	In the Alternate DNS box, enter the IP address of the alternate DNS.	[Setting method] Manual [Default value] 8.8.8.8
Enable Port Mapping	Enable to set the ports of HTTP, HTTPS, RSTP, and Control. Auto: device to obtain Web port, data port, and client port. Manual: The user sets the port manually.	[Setting method] Choose a type from the drop-down list [Default value] Auto
HTTP Port	The default value setting is 80. You can enter the value according to your actual situation.	[Setting method] When Port Mapping is manual, you need to set these.
HTTPS Port	If you enter another value, for example, 443, you should enter 443 after the IP address when logging in to the Device by browser.	
RTSP Port	Real-Time Streaming Protocol. The default value setting is 554. You can select the value according to your actual situation.	
Control Port	The default value setting is 30001. You can enter the value according to your actual situation.	

Step 2 Click Next to view the basic device information, as shown in Figure 4-9.

Figure 4-9 Wizard of date and time



Setup Wizard

Date And Time | Time Zone | DST

Date Format: DD/MM/YY hh:mm:ss

Time Format: 24H

Enable NTP

NTP Server: time.windows.com

Sync Time Frequency (sec): 86400

Date: 24/04/2022

Time: 11:13:43

Choose the date format and time format from the drop-down list.

Enable NTP:

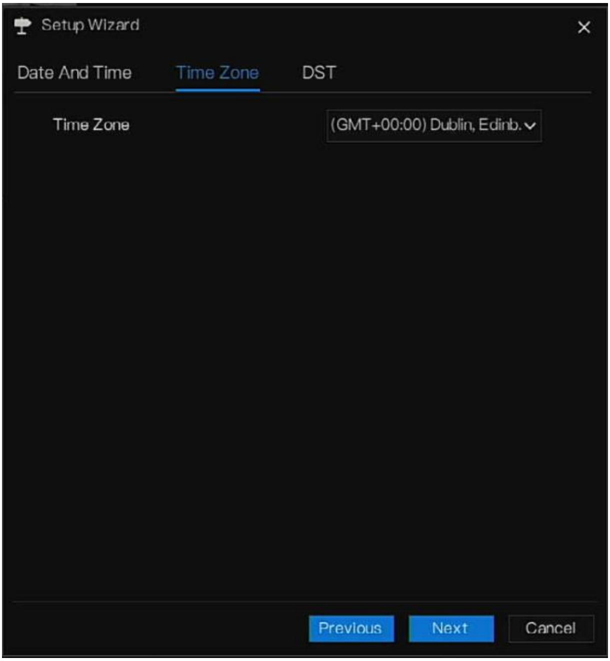
- Click to synchrony time from the network.

Disable the NTP-Sync, and set the time manually.

- Roll the mouse to choose year, month, and day when clicking the date.
- Roll the mouse to choose hour, minute, and second when clicking the date.
- Click **Update Time** to save the time.

Step 3 Click **Time Zone,** and choose the current time zone from the drop-down list as shown in Figure 4-10.

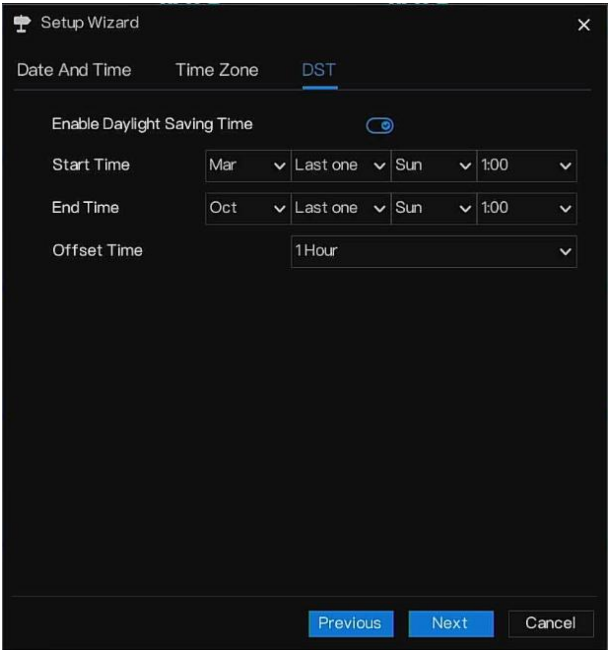
Figure 4-10 Wizard of time zone



Time Zone (GMT+00:00) Dublin, Edinb.

Step 4 Click **DST,** enable the DST, and set the start and the end time. Select offset time from the drop-down list.

Figure 4-11 Wizard of DST



Enable Daylight Saving Time ●

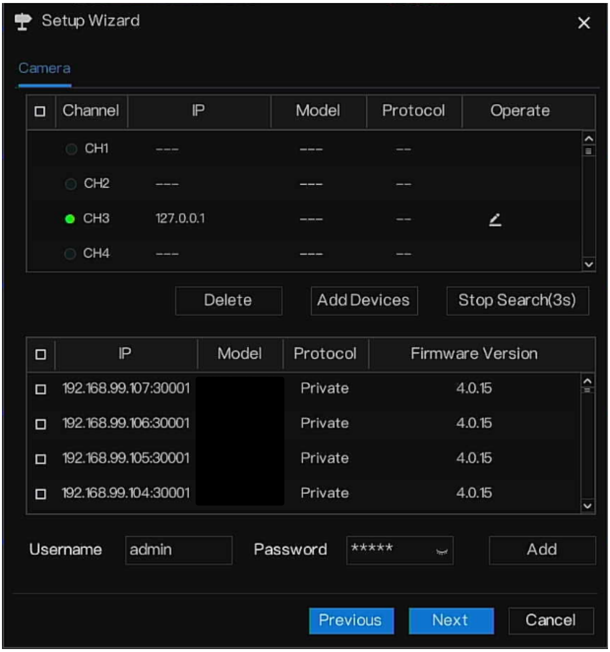
Start Time: Mar, Last one, Sun, 1:00

End Time: Oct, Last one, Sun, 1:00

Offset Time: 1 Hour

Step 5 Click Next to enter the adding camera wizard, as shown in Figure 4-12.

Figure 4-12 Wizard of adding camera



Setup Wizard ✕

Camera

□	Channel	IP	Model	Protocol	Operate
	○ CH1	----	----	--	
	○ CH2	----	----	--	
	● CH3	127.0.0.1	----	--	✎
	○ CH4	----	----	--	

Delete | Add Devices | Stop Search(3s)

□	IP	Model	Protocol	Firmware Version
□	192.168.99.107:30001	[redacted]	Private	4.0.15
□	192.168.99.106:30001	[redacted]	Private	4.0.15
□	192.168.99.105:30001	[redacted]	Private	4.0.15
□	192.168.99.104:30001	[redacted]	Private	4.0.15

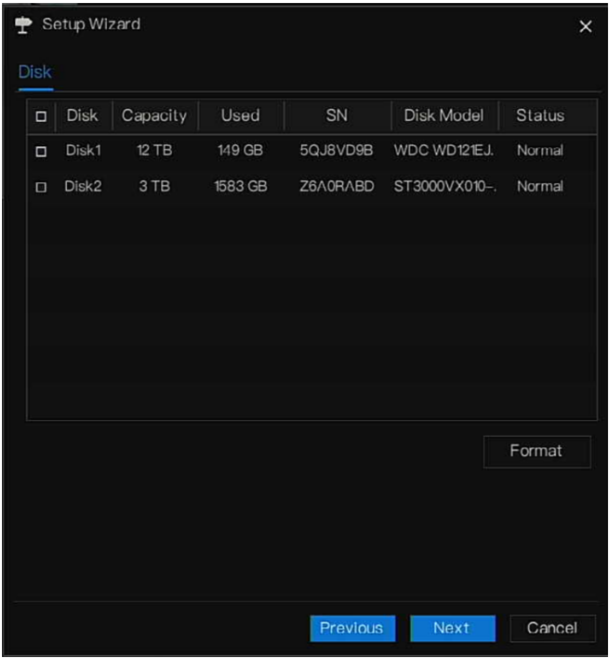
Username: admin Password: ***** Add

Previous | Next | Cancel

For the details of adding cameras please refer to *chapter 6.1*.

Step 6 Click Next to enter the wizard of disk, as shown in Figure 4-13.

Figure 4-13 Wizard of disk

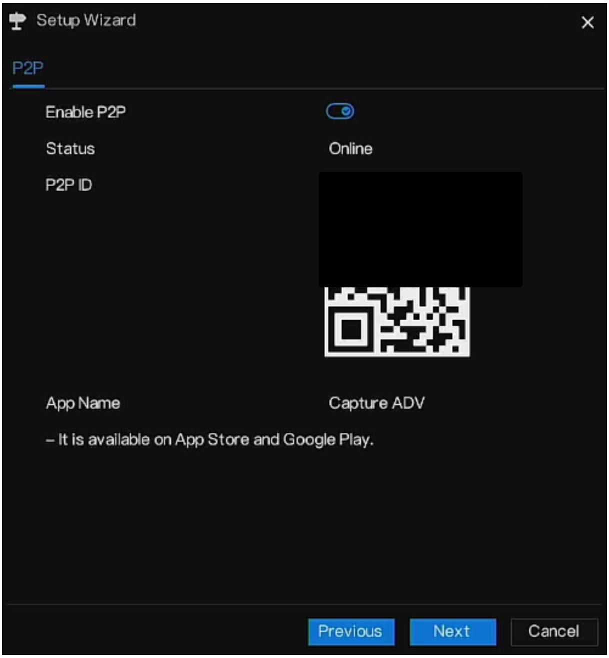


□	Disk	Capacity	Used	SN	Disk Model	Status
□	Disk1	12 TB	149 GB	5QJ8VD9B	WDC WD121EJ.	Normal
□	Disk2	3 TB	1583 GB	Z6A0RABD	ST3000VX010-.	Normal

You can view the general information about the disk. You can also format the disk. If you plug the disk into the device for the first time, you must format the disk.

Step 7 Click Next to enter the wizard of P2P, as shown in Figure 4-14

Figure 4-14 P2P



Enable P2P

Status: Online

P2P ID: [redacted]

App Name: Capture ADV

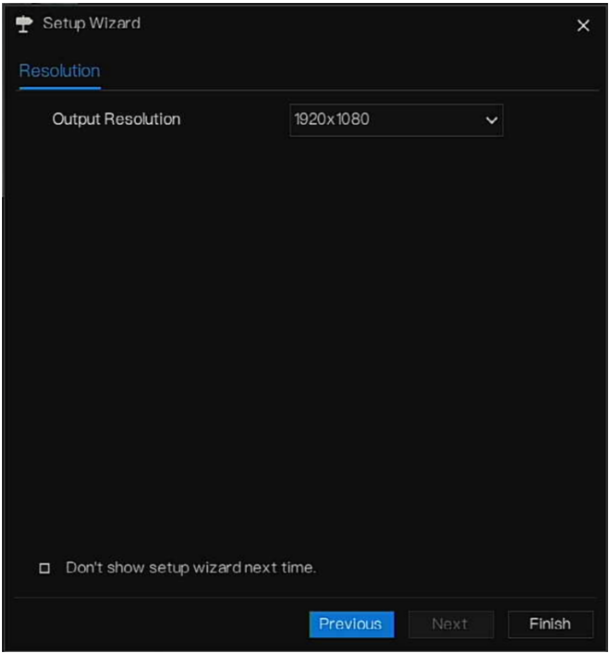
– It is available on App Store and Google Play.

Step 8 Enable the P2P, user can use mobile devices to manage the DVR by scanning the P2P ID if the mobile phone has loaded the (search the APP at the **App Store** or **Google Play**).

Step 9 Click Next to enter the wizard of resolution, as shown in Figure 4-15. Choose a resolution from the drop-down list.

(The highest resolution is **3840*2160**, the resolution should match the resolution of the monitor, if the setting resolution is higher than the monitor, the video can be displayed, and the screen will be blank. You should log in web interface to modify the resolution.)

Figure 4-15 Wizard of resolution



Output Resolution 1920x1080

□ Don't show setup wizard next time.

Step 10 Click Finish to end the wizard, tick the **Don't show setup wizard next time,** it would not show at next time. Reopen the wizard at **System > User > Advance setting**.

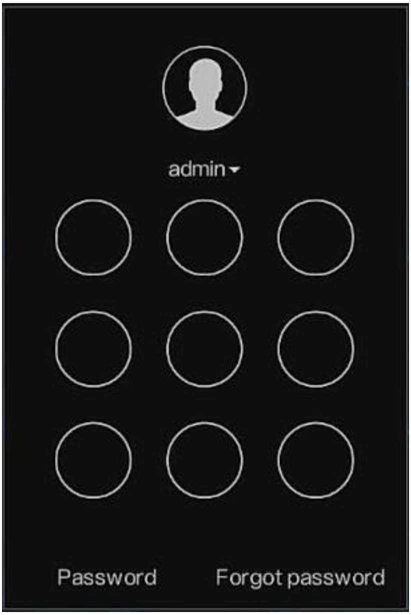
4.4 Power off the Device

Click the main menu and choose **System** > **Maintenance;** the maintenance setting page is displayed, and click **Shutdown** to power off the DVR. If there is a power switch on the rear panel of the DVR, you can power off the power switch to disconnect the DVR from the power supply.

4.5 Login to the System

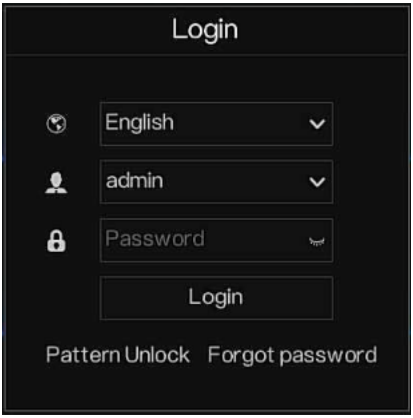
Step 1 Login to the device（two modes to login). The pattern unlock is shown in Figure 4-16.

Figure 4-16 Pattern unlock login page



Step 2 On the DVR login page, click "Password" to enter the pattern unlock interface. If users don't set the pattern to unlock, it will show the password to the login interface directly; select the language as shown in Figure 4-17.

Figure 4-17 Password login page



Step 3 Input the username and password.

NOTE

If the password is incorrect more than 3 times, please log in again after 5 minutes. You can also power off and power on to start the device and input the correct password to avoid waiting five minutes.

If the user forgets the password, click Forgot password. Users can choose a way to create a new password:

1. Scan the QR code and send the QR code to your seller; the seller will send you the verification code to create a new password.
2. Answer the secure question to create a new password.
3. Receive the verification code for recovery of user password by Email.

----End

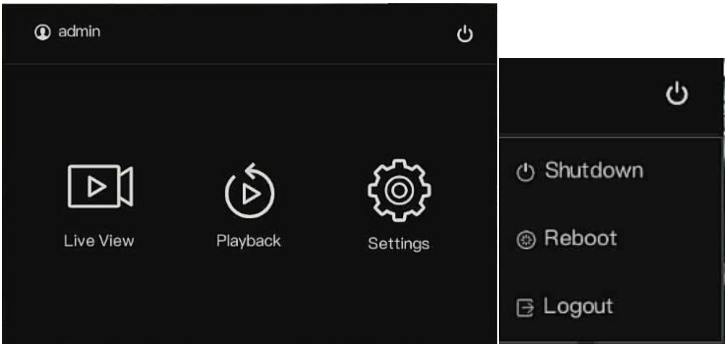
5 Quick Navigation

5.1 Quick Bar

After the DVR operation screen is displayed, move the cursor to the far bottom of the DVR screen. The DVR floating menu bar is displaying.

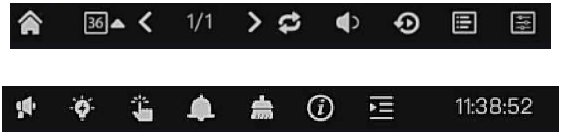
Click 🏠 on the left of the DVR floating menu bar. The quick home menu is showing. The quick home menu contains **Live View**, **Playback**, **System Settings,** and **Power (Shutdown, Reboot, and Logout)** as shown in Figure 5-1.

Figure 5-1 Quick home menu

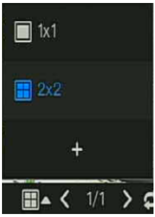


In the middle of the DVR floating menu bar, the video toolbar provides **video window switching**, **auto SEQ, volume, playback,** and **channel information,** as shown in Figure 5-2.

Figure 5-2 Real-time video toolbar

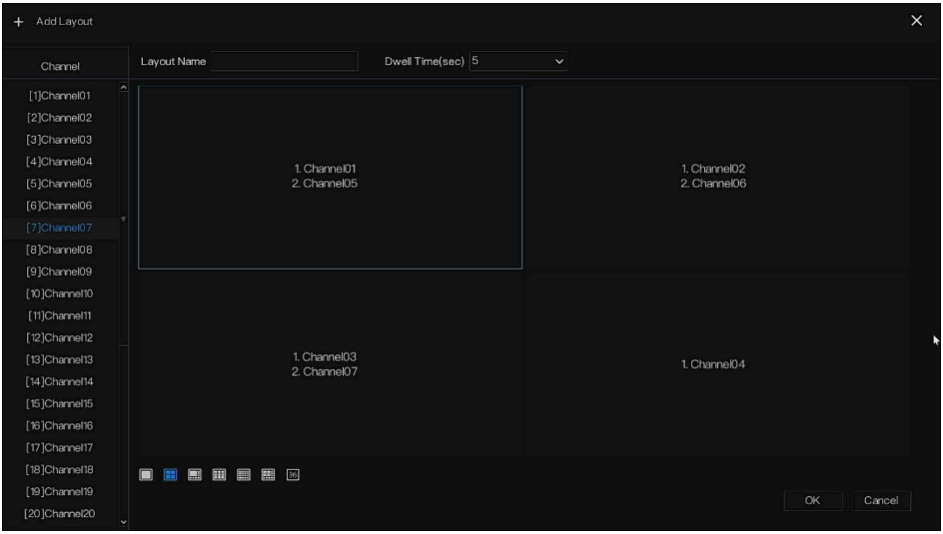


The real-time video toolbar is as follows:



: Layout. Users can choose the layout and add new layout strategies as shown in Figure 5-3. Click on the right of the screen splitting format and choose the channels to view the video. Click + to add a new layout.

Figure 5-3 Add layout



Channel

[1]Channel01
[2]Channel02
[3]Channel03
[4]Channel04
[5]Channel05
[6]Channel06
[7]Channel07
[8]Channel08
[9]Channel09
[10]Channel10
[11]Channel11
[12]Channel12
[13]Channel13
[14]Channel14
[15]Channel15
[16]Channel16
[17]Channel17
[18]Channel18
[19]Channel19
[20]Channel20

Layout Name

Dwell Time(sec) 5

1. Channel01
2. Channel05

1. Channel02
2. Channel06

1. Channel03
2. Channel07

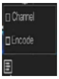
1. Channel04

Input the layout name, choose the dwell time, and choose the splitting format. Choose one channel or several channels to add to the screen.

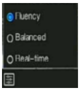
: Auto SEQ. Click the icon, and the layout dwell on screen is enabled, for how to set the dwell on, please see *chapter 6.7.5.*

: Audio. Click on the icon, the audio setting screen will be displayed, where you can choose the channel and adjust the volume.

: Playback. Click the icon to enter the playback interface.



: Channel information, tick the channel or encode, the live video will show the channel information.

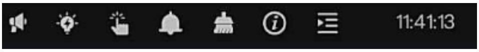


: Preview strategy, users can switch the real-time preview mode according to the network.

There are three modes: fluency, balance, and real-time.

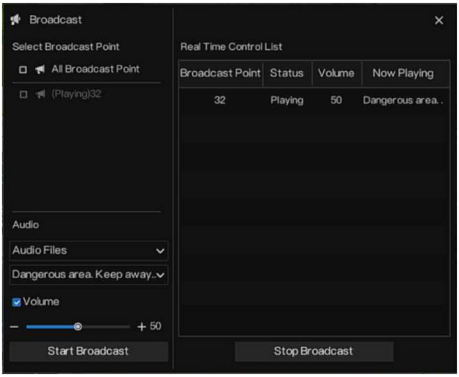
A main menu quick toolbar is on the right of the DVR floating menu bar. The main menu quick toolbar provides **Manual alarm, Alarm information, Clean alarm, Information,** and **time**, as shown in Figure 5-4.

Figure 5-4 Main menu quick toolbar



: Broadcast. The user adds the speaker to DVR and selects the speaker to broadcast. Choose the audio file from the drop-down list. Click the **Start Broadcast** to play the audio files. Click the **Stop Broadcast** to end playing.

Figure 5-5 Broadcast



Broadcast

Select Broadcast Point

□ All Broadcast Point

□ (Playing)32

Audio

Audio Files

Dangerous area. Keep away..

☑ Volume

– + 50

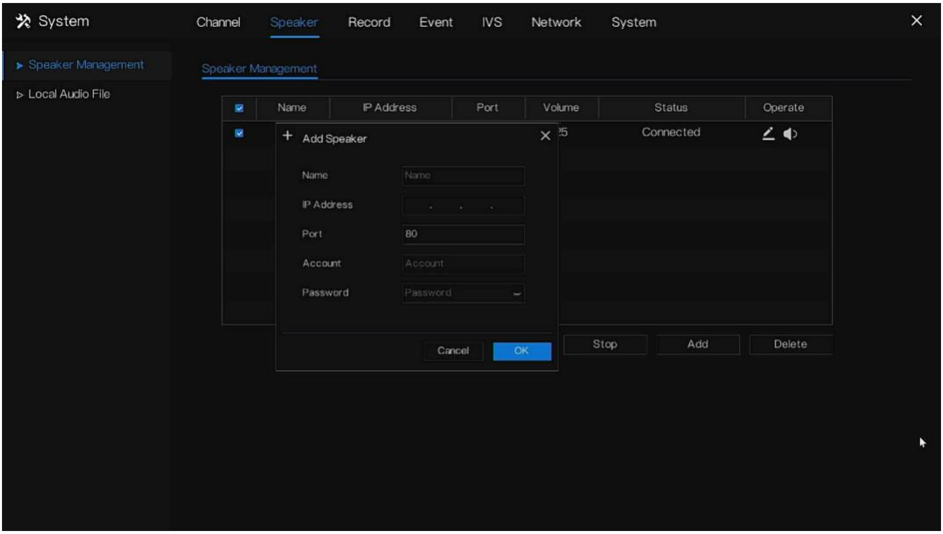
Start Broadcast

Real Time Control List

Broadcast Point	Status	Volume	Now Playing
32	Playing	50	Dangerous area..

Stop Broadcast

Figure 5-6 Add speaker

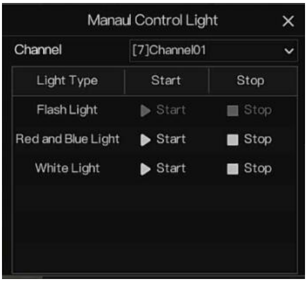


Name	Name
IP Address	. . .
Port	80
Account	Account
Password	Password

The audio files can be set at **Settings > Speaker > Local Audio File** interface.

: Manual control light, for the camera with the light(flash light, red and blue light, or white light), click Start to open the light manually, and click Stop to close the light.

Figure 5-7 Manual control light

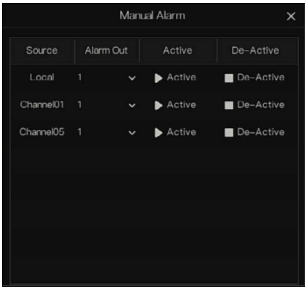


Channel [7]Channel01

Light Type	Start	Stop
Flash Light	▶ Start	■ Stop
Red and Blue Light	▶ Start	■ Stop
White Light	▶ Start	■ Stop

: Manual alarm, click the icon, users can set different channels, choose alarm out, the window shows in Figure 5-8.

Figure 5-8 Manual alarm

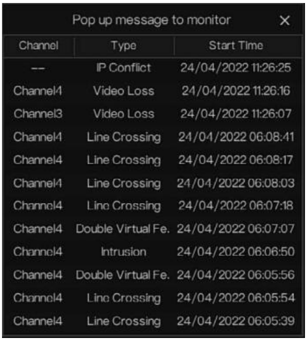


Manual Alarm

Source	Alarm Out	Active	De-Active
Local	1	▶ Active	■ De-Active
Channel01	1	▶ Active	■ De-Active
Channel05	1	▶ Active	■ De-Active

: Event list, click on the icon for more details as shown in Figure 5-9.

Figure 5-9 Event list



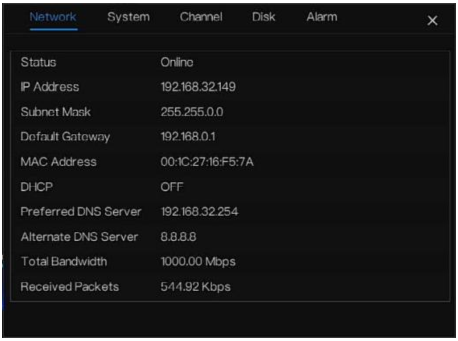
Pop up message to monitor

Channel	Type	Start Time
--	IP Conflict	24/04/2022 11:26:25
Channel4	Video Loss	24/04/2022 11:26:16
Channel3	Video Loss	24/04/2022 11:26:07
Channel4	Line Crossing	24/04/2022 06:08:41
Channel4	Line Crossing	24/04/2022 06:08:17
Channel4	Line Crossing	24/04/2022 06:08:03
Channel4	Line Crossing	24/04/2022 06:07:18
Channel4	Double Virtual Fe.	24/04/2022 06:07:07
Channel4	Intrusion	24/04/2022 06:06:50
Channel4	Double Virtual Fe.	24/04/2022 06:05:56
Channel4	Line Crossing	24/04/2022 06:05:54
Channel4	Line Crossing	24/04/2022 06:05:39

: Clean alarm, click the icon and clean the current alarm actions like voice and external alarm out.

: Information, click the icon and the general information will show, like network, system, channel, disk, and alarm, as shown in Figure 5-10. : The red icon means the disk needs to be formatted.

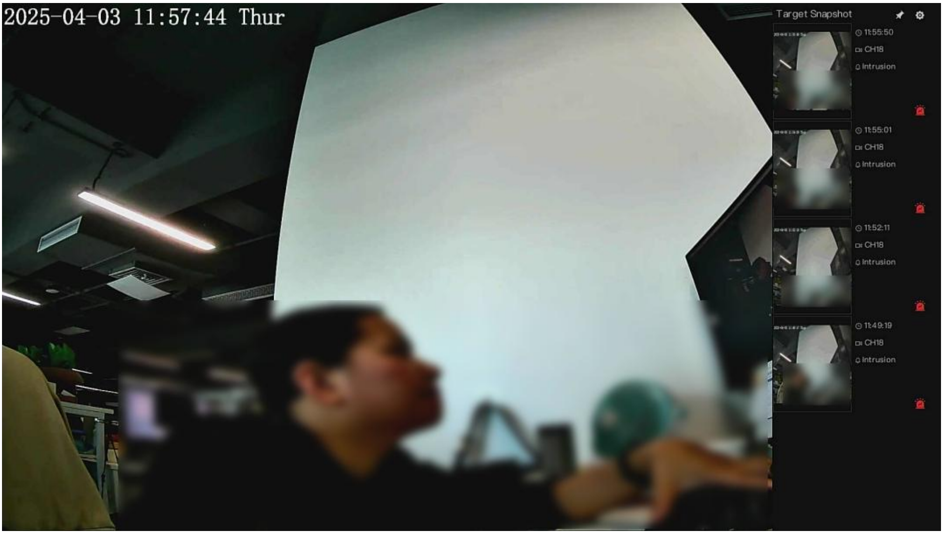
Figure 5-10 Information



Status	Online
IP Address	192.168.32.149
Subnet Mask	255.255.0.0
Default Gateway	192.168.0.1
MAC Address	00:1C:27:16:F5:7A
DHCP	OFF
Preferred DNS Server	192.168.32.254
Alternate DNS Server	8.8.8.8
Total Bandwidth	1000.00 Mbps
Received Packets	544.92 Kbps

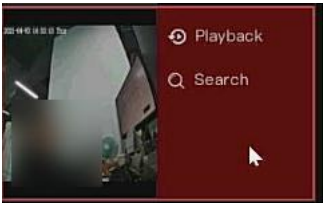
☰: Disable snapshot list, the snapshot list is enabled by default, the alarm snapshots will be shown in this list.

Figure 5-11 Snapshot list



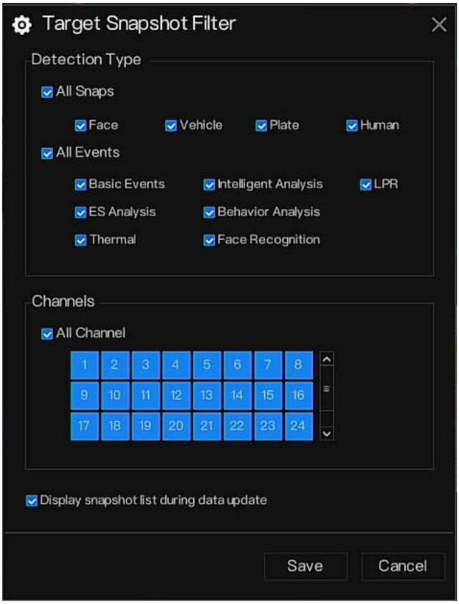
Choose one snapshot to playback, search the result by the picture, and add this one to the list.

Figure 5-12 Snapshot list



You can choose the event types and channels, as shown in Figure 5-13.

Figure 5-13 Target snapshot filter



Target Snapshot Filter

Detection Type

☑ All Snaps

☑ Face ☑ Vehicle ☑ Plate ☑ Human

☑ All Events

☑ Basic Events ☑ Intelligent Analysis ☑ LPR

☑ ES Analysis ☑ Behavior Analysis

☑ Thermal ☑ Face Recognition

Channels

☑ All Channel

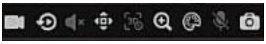
1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24

☑ Display snapshot list during data update

Save Cancel

5.2 Real-Time Video Bar

Right-click on the real-time image and the quick setting will show the figure.



Record: click the icon and start to record the video. Click again to end the record.

Instant playback: click the icon, and the window will record the video five minutes ago.

is the time bar of playback.

Audio: open or close the audio.

PTZ: This function is only applied for speed dome cameras. The monitored camera can focus, zoom, or iris at this pop-up window. You can adjust every parameter as shown in Figure 5-14. For analog camera, click ■ to enter the OSD menu.

Figure 5-14 PTZ adjust screen

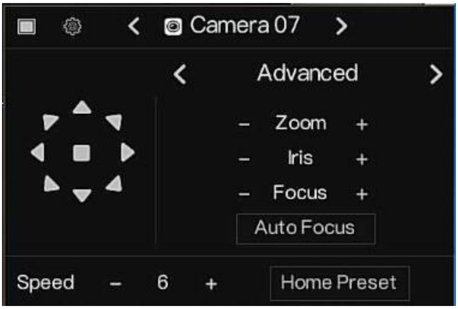
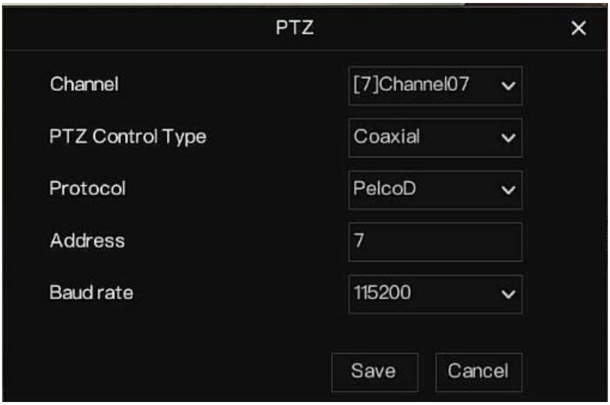


Figure 5-15



Channel [7]Channel07

PTZ Control Type Coaxial

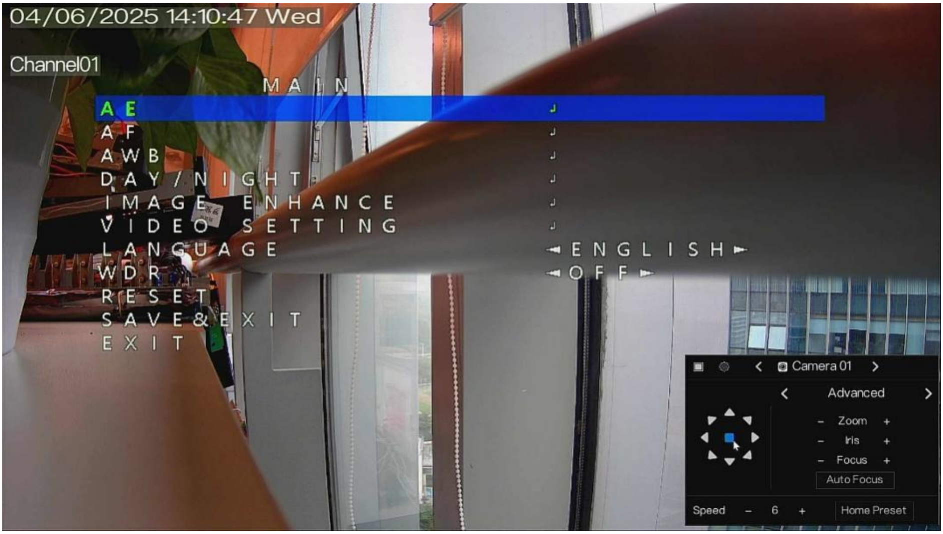
Protocol PelcoD

Address 7

Baud rate 115200

✥: Adjust the direction of the camera. ▣: Click it to multi-screen or single-screen to play the live video. Click the Home Preset to go to the home position. For analog camera, click ■ to enter the OSD menu, as shown in Figure 5-16 .

Figure 5-16 Main menu of analgo camera



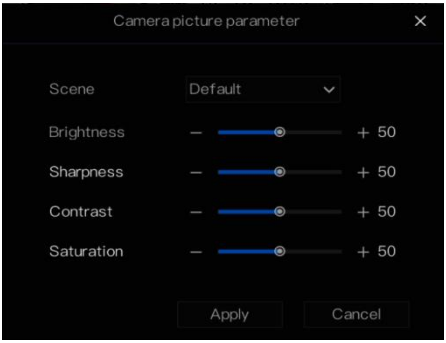
: At this part, perform **Advanced, Scan,** and **Tour** settings.

: 3D, this function can only be used for high-speed dome cameras. Click the icon to enter the camera's live video screen, use the mouse to move the camera, or zoom in or out the lens. Click the point to zoom in. Drag and draw the area, zoom in on the drawing area, and Reverse drag to zoom out.

: Zoom in, click zoom in, and roll the mouse wheel to zoom in and zoom out. Right-click to exit the zooming.

: Image, click the icon, as shown in Figure 5-17. Select the scene, and drag the cursor to adjust the value of brightness, sharpness, contrast, and saturation.

Figure 5-17 Camera picture parameter



Camera picture parameter ✕

Scene: Default

Brightness: 50

Sharpness: 50

Contrast: 50

Saturation: 50

☎: Two-way audio. The DVR and camera can talk to each other.

📷: Snapshot panorama. If a USB storage device is connected to the DVR device, click to save the panorama snapshot directly.

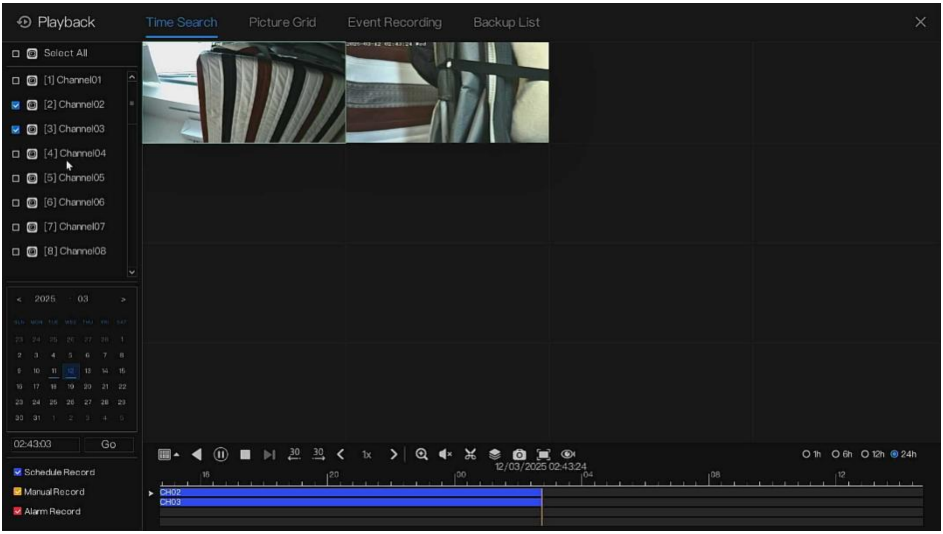
🎥: The current channel is recording.

🏃: Alarm, the current channel has a motion-detection alarm

5.3 Playback

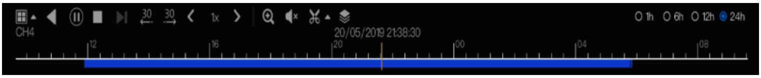
Playback refers to playing back a video, fixed-point playback, or playback of the search type. Click ⟲ in the quick navigation bar to access the playback screen, as shown in Figure 5-18.

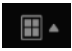
Figure 5-18 Playback screen

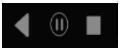


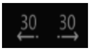
Choose the channels from the channels list, and click one day to play (the date has the blue line, which means there is a recording video on this day, it doesn't mean that all channels have video.) It may have three color bars on the time bar, the blue one is a schedule record, the yellow one is a manual record, and the red one is an alarm record.

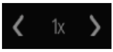
The toolbar at the bottom of the playback screen is described as follows:

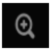


: Layout.

: Reversed, pause/play, stop.

:30s backward, 30s forward.

: Triple speed, it supports up to 32 times playback. Click the Number to switch the speed.

: Zoom. Roll the roller of the mouse to zoom in or out.

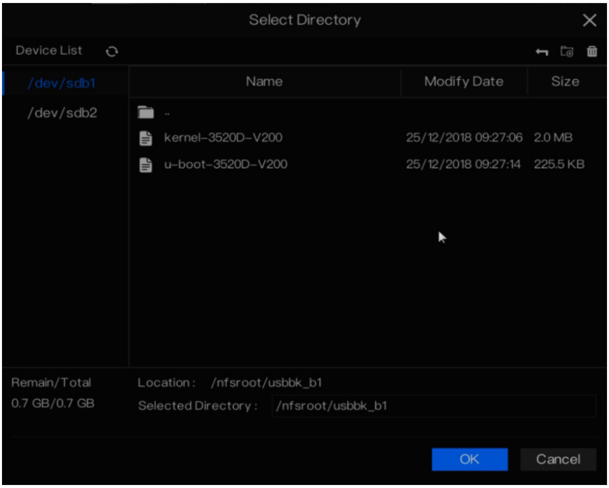
🔇: Audio.

✂: Start and end backup. Click the icon, and the video backup starts, select the video, and click the icon again.

The backup type appears. Click **save**. And **saving the file** pop-ups as Figure 5-19. Click **OK** to save.

This function is available after a USB disk is plugged into the device.

Figure 5-19 Select directory



/dev/sdb1
/dev/sdb2

Name	Modify Date	Size
..		
kernel-3520D-V200	25/12/2018 09:27:06	2.0 MB
u-boot-3520D-V200	25/12/2018 09:27:14	225.5 KB

Remain/Total
0.7 GB/0.7 GB

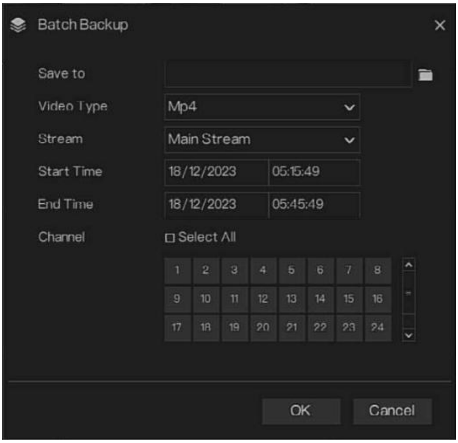
Location : /nfsroot/usbbk_b1

Selected Directory : /nfsroot/usbbk_b1

≋: Batch backup, click the icon to backup multi-channels, as shown in Figure 5-20.

Choose the folder to save, select the stream information from the drop-down list, set the start time and end time, select the channels, and Click **OK** to backup. The backup videos are marked by a watermark, you can view it by our player. If the user adds the NAS account, the backup recording can be saved to the NAS.

Figure 5-20 Batch backup



Batch Backup

Save to

Video Type: Mp4

Stream: Main Stream

Start Time: 18/12/2023 05:15:49

End Time: 18/12/2023 05:45:49

Channel: □ Select All

1 2 3 4 5 6 7 8
9 10 11 12 13 14 15 16
17 18 19 20 21 22 23 24

: Snapshot panorama. Click to save it to a USB storage device on DVR.

: Fisheye. Click to choose the fisheye mode to play the recording video.

○ 1h ○ 6h ○ 12h ● 24h: Type of time bar, recording video can show

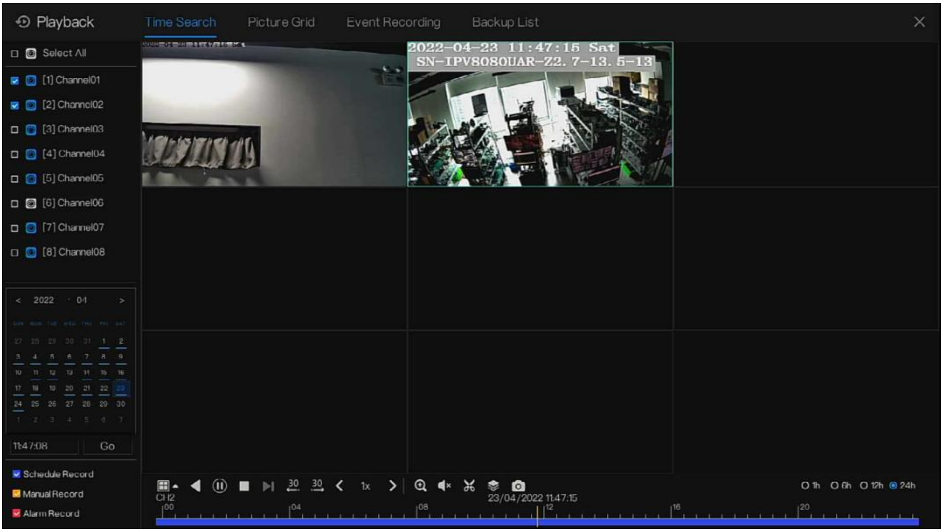
5.3.1 Time Search

Search refers to searching for a video by date and time.

Operation Description

Click in the quick navigation bar to access the search screen, as shown in Figure 5-21.

Figure 5-21 Time Search screen



Operation Steps

Step 1 Select a camera or cameras in the camera list on the left side of the search screen. The video view of the selected camera is displayed in the play window.

Step 2 Select a date in the calendar on the light-down side of the search screen.

Step 3 Choose the record type, and search the video quickly.

Step 4 Choose the proper button to adjust the video.

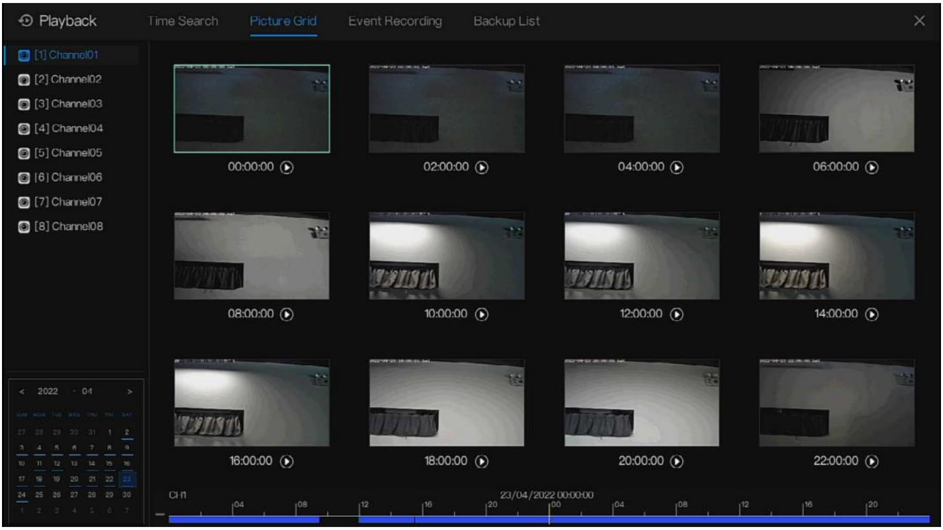
----End

5.3.2 Picture Grid

Picture grid refers to evenly dividing the video of a channel by time range and searching for a video based on thumbnails divided by time range.

Click Picture Grid on the quick navigation bar to access the picture grid screen, as shown in Figure 5-22.

Figure 5-22 Picture grid screen



Operation Steps

Step 1 Select a camera in the camera list on the left side of the picture grid screen. Videos shot by the camera in the earliest time range on the current day are displayed as thumbnails in the window on the right side.

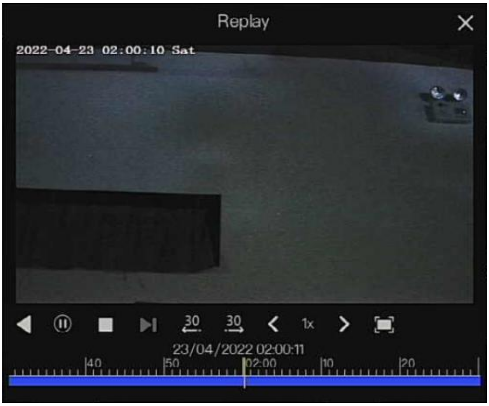
Step 2 Select a date from the calendar.

Step 3 A day is divided into 12 grids, every two hours is a grid. Click the image to change the interval.

Step 4 Select a required thumbnail and double-click it, then the time can also be divided into ten minutes or one minute. Right-click to enlarge the time to interval.

Step 5 Click ▶ to replay the gird individually.

Figure 5-23 Replay

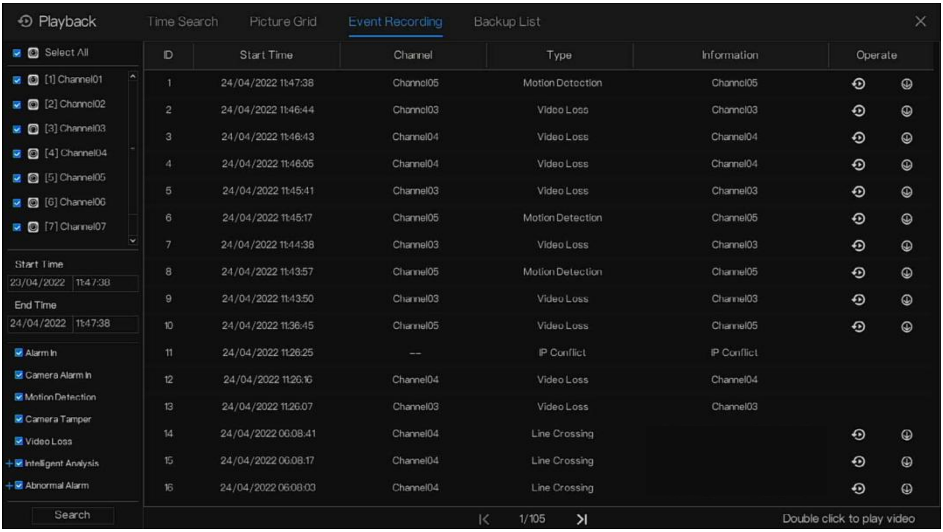


----End

5.3.3 Event Recording

Click on the quick navigation bar; choose **Event** at title to access the alarm event screen, as shown in Figure 5-24

Figure 5-24 Event screen



☑ Select All

☑ [1] Channel01
☑ [2] Channel02
☑ [3] Channel03
☑ [4] Channel04
☑ [5] Channel05
☑ [6] Channel06
☑ [7] Channel07

Start Time: 23/04/2022 11:47:38

End Time: 24/04/2022 11:47:38

☑ Alarm In
☑ Camera Alarm In
☑ Motion Detection
☑ Camera Tamper
☑ Video Loss
+☑ Intelligent Analysis
+☑ Abnormal Alarm

Search

ID	Start Time	Channel	Type	Information	Operate
1	24/04/2022 11:47:38	Channel05	Motion Detection	Channel05	↺ ⊕
2	24/04/2022 11:46:44	Channel03	Video Loss	Channel03	↺ ⊕
3	24/04/2022 11:46:43	Channel04	Video Loss	Channel04	↺ ⊕
4	24/04/2022 11:46:05	Channel04	Video Loss	Channel04	↺ ⊕
5	24/04/2022 11:45:41	Channel03	Video Loss	Channel03	↺ ⊕
6	24/04/2022 11:45:17	Channel05	Motion Detection	Channel05	↺ ⊕
7	24/04/2022 11:44:38	Channel03	Video Loss	Channel03	↺ ⊕
8	24/04/2022 11:43:57	Channel05	Motion Detection	Channel05	↺ ⊕
9	24/04/2022 11:43:50	Channel03	Video Loss	Channel03	↺ ⊕
10	24/04/2022 11:36:45	Channel05	Video Loss	Channel05	↺ ⊕
11	24/04/2022 11:26:25	--	IP Conflict	IP Conflict	
12	24/04/2022 11:26:16	Channel04	Video Loss	Channel04	
13	24/04/2022 11:26:07	Channel03	Video Loss	Channel03	
14	24/04/2022 06:08:41	Channel04	Line Crossing		↺ ⊕
15	24/04/2022 06:08:17	Channel04	Line Crossing		↺ ⊕
16	24/04/2022 06:08:03	Channel04	Line Crossing		↺ ⊕

|< 1/105 >|

Double click to play video

Operation Steps

Step 1 Select cameras in the camera list on the left.

Step 2 Set start and end times.

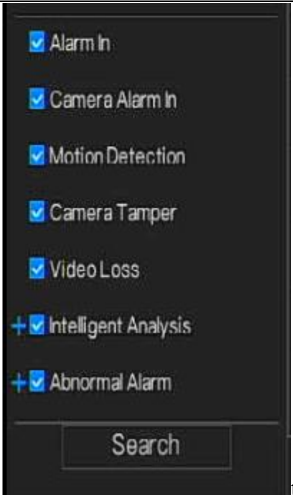
Step 3 Tick the alarm type, such as alarm in, camera alarm in, motion alarm, video loss, intelligent analysis, and abnormal alarm.

Step 4 Click Search to query the event, the result will show in the window.

Step 5 Double-click to play a video about the event. It will play a recording video.

↺: play the recording video.

⊕: back up the recording video.



☑ Alarm In

☑ Camera Alarm In

☑ Motion Detection

☑ Camera Tamper

☑ Video Loss

+ ☑ Intelligent Analysis

+ ☑ Abnormal Alarm

the type of intelligent analysis and abnormal alarm are subdivided, users can tick **Detail Alarm** to show.

The intelligent analysis includes intrusion, single line crossing, double line crossing, loitering, multi-loitering, object left, object removed, abnormal speed, wrong way, illegal parking, signal bad, register, stranger, wear mask, no mask, fence alarm, people counting threshold alarm, people counting threshold alarm(IPC), enter area, leave area, smoking detection, smoke and flame detection, fire spot detection, smart motion.

Abnormal alarms include disk error, full disk, IP conflict, network disconnected, fan alarm, power alarm, failover normal alarm, and failover spare alarm.

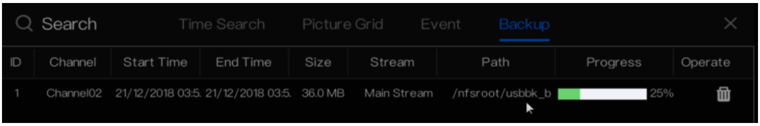
Users can choose the accurate alarm events to search.

----End

5.3.4 Backup List

Click on the quick navigation bar, and choose Backup at title to access the backup screen, as shown in Figure 5-25.

Figure 5-25 Backup screen



ID	Channel	Start Time	End Time	Size	Stream	Path	Progress	Operate
1	Channel02	21/12/2018 03:5.	21/12/2018 03:5.	36.0 MB	Main Stream	/nfsroot/usbbk_b	25%	🗑

.

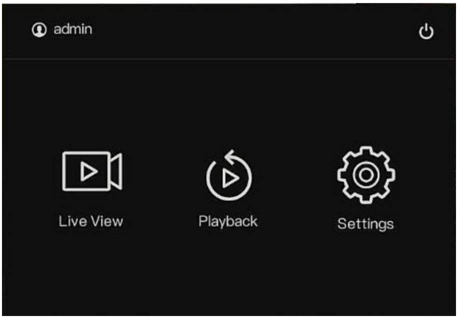
View detailed information on backup. Click on **Delete** to quit the download.

----End

5.4 Main Menu

Right-click on the UI screen, the main menu as shown in Figure 5-26.

Figure 5-26 DVR main menu



Choose the Settings to set the **Channel, Speaker, Record, Event, IVS, Network,** and **System**.

Channel: Camera, Encode, Image, OSD, Privacy Zone, Channel Type, ROI, Audio, and Intelligent Tracking.

Speaker: Speaker Management, and Local Audio File.

Record: Record schedule, Disk, Storage Mode, S.M.A.R.T, Disk Detection, Disk Calculation, and FTP.

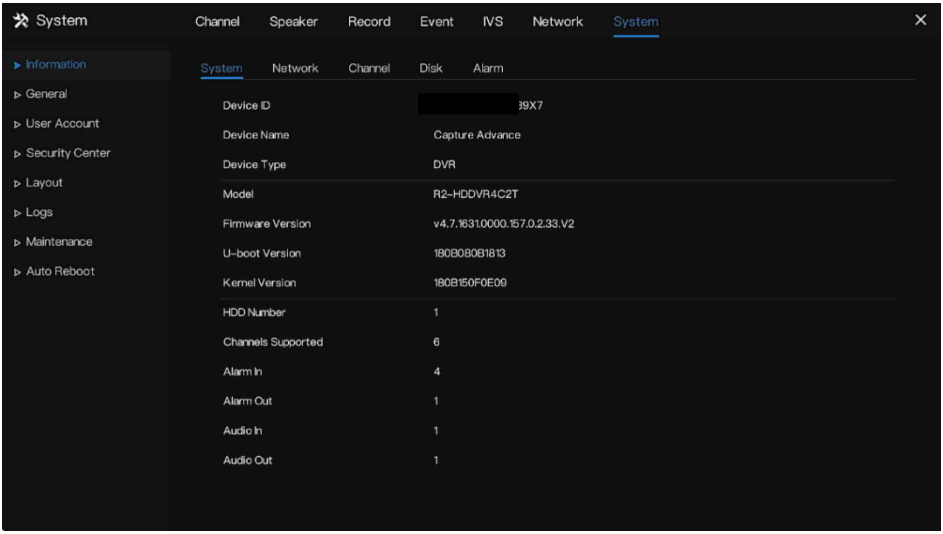
Event: General, Motion Detection, Video Tampering, Video Loss, Alarm In, Abnormal Alarm, and Alarm Out.

IVS: Intelligent Analysis, ES Analysis, and Local Intelligent Analysis.

Network: Network, 8012.1X, DDNS, Port Mapping, Email, P2P, IP Filter, SNMP, 3G/4G, PPPOE, Network Traffic, Platform Access, and Failover.

System: Information, General, User Account, Security Center, Layout, Auxiliary Screen, Logs, Maintenance, and Auto Reboot.

Figure 5-27 Setting



Device ID	[redacted]9X7
Device Name	Capture Advance
Device Type	DVR
Model	R2-HDDVR4C2T
Firmware Version	v4.7.1631.0000.157.0.2.33.V2
U-boot Version	180B080B1813
Kernel Version	180B150F0E09
HDD Number	1
Channels Supported	6
Alarm In	4
Alarm Out	1
Audio In	1
Audio Out	1

----End

6 System Setting

NOTE

Different devices may have different functions; please refer to actual products.

6.1 Channel Management

The analog cameras can directly be connected to input channels of the DVR by coaxial cables. There are some channels can connect IP cameras, the DVR can automatically search for and add IP cameras or manually add cameras in the same Local Area Network (LAN).

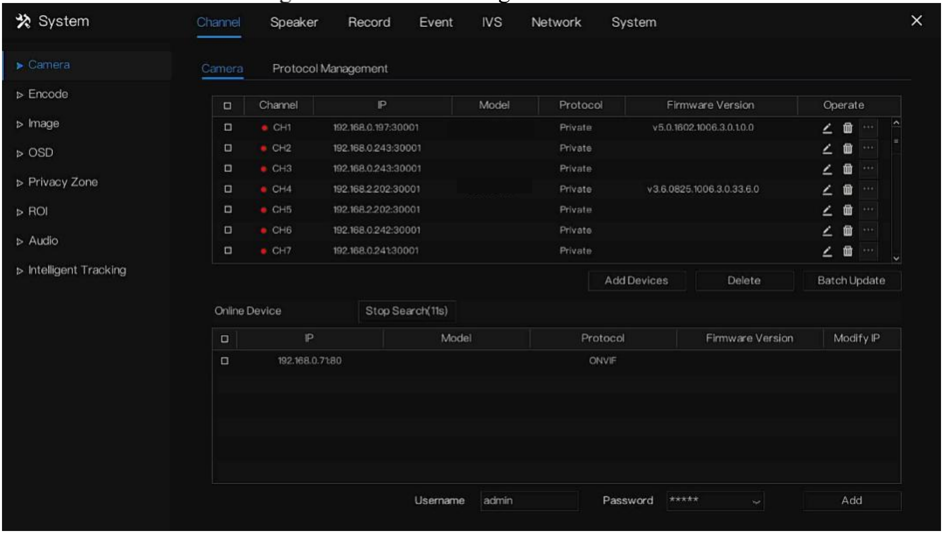
Channel management includes **Adding** or **Deleting a Camera, Encode, Image, OSD, Privacy Zone, Channel Type, ROI, Audio,** and **Intelligent Tracking**.

6.1.1 Camera

Operation Description

Click **Channel** in the Setting System menu to access the camera management screen, as shown in Figure 6-1 There are four modes for adding cameras: manually add, batch add, search to add, coaxial cable add analog cameras, and automatic add.

Figure 6-1 Channel management screen



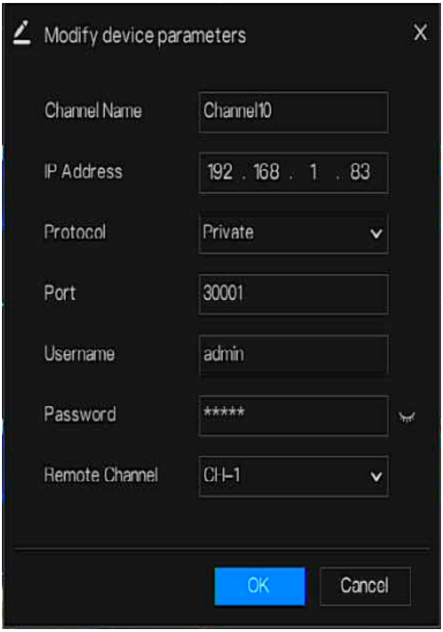
□	Channel	IP	Model	Protocol	Firmware Version	Operate
□	● CH1	192.168.0.197:30001	[redacted]	Private	v5.0.1602.1006.3.0.1.0.0	
□	● CH2	192.168.0.243:30001		Private		
□	● CH3	192.168.0.243:30001		Private		
□	● CH4	192.168.2.202:30001	[redacted]	Private	v3.6.0825.1006.3.0.33.6.0	
□	● CH5	192.168.2.202:30001		Private		
□	● CH6	192.168.0.242:30001		Private		
□	● CH7	192.168.0.241:30001		Private		

□	IP	Model	Protocol	Firmware Version	Modify IP
□	192.168.0.71:80		ONVIF		

Username admin Password *****

Modify device parameters; the remote channel is based on cameras (human body temperature has two remote channels, and fisheye cameras have four remote channels), as shown in Figure 6-2.

Figure 6-2 Modify device parameter



Modify device parameters

Channel Name: Channel10

IP Address: 192 . 168 . 1 . 83

Protocol: Private

Port: 30001

Username: admin

Password: *****

Remote Channel: CH-1

Add Devices: It is to add cameras automatically.

Delete: Choose the camera, and click the Delete button to delete.

Tick the online non-ONVIF channels on the list and click Batch Update to access the directory of software. It will update the channels at once.

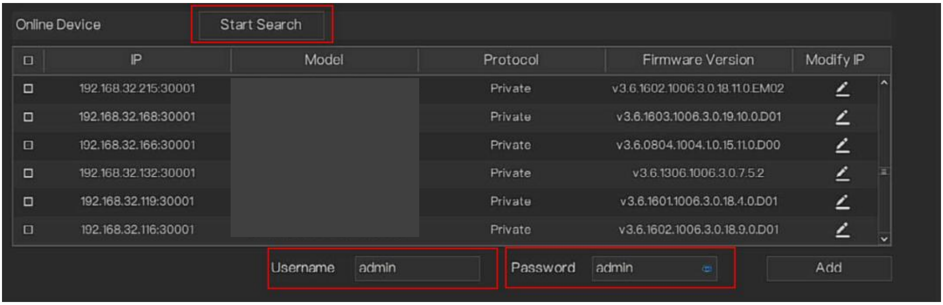
----End

6.1.1.1 Add Camera Automatically

The DVR can automatically add cameras to the camera list.

Operation Methods

Method 1: Click Start Search, and the cameras in the same network as your recorder will show in the list, the search will last for 20 seconds. Input username and password (the default value is both admin) and click **Add Devices**, the cameras that are top-ranked in the list of devices will be added to channels directly.



Online Device Start Search

□	IP	Model	Protocol	Firmware Version	Modify IP
□	192.168.32.215:30001	[redacted]	Private	v3.6.1602.1006.3.0.18.11.0.EM02	✎
□	192.168.32.168:30001	[redacted]	Private	v3.6.1603.1006.3.0.19.10.0.D01	✎
□	192.168.32.166:30001	[redacted]	Private	v3.6.0804.1004.1.0.15.11.0.D00	✎
□	192.168.32.132:30001	[redacted]	Private	v3.6.1306.1006.3.0.7.5.2	✎
□	192.168.32.119:30001	[redacted]	Private	v3.6.1601.1006.3.0.18.4.0.D01	✎
□	192.168.32.116:30001	[redacted]	Private	v3.6.1602.1006.3.0.18.9.0.D01	✎

Username admin Password admin Add

Method 2: Select the cameras you want to add, and click Add. The selected cameras will be added to the camera list.

NOTE

- On the camera management screen, check the status of channels in the camera list. If the status of a channel is 🟩, this camera is online. If the status of a channel is 🟥, this camera is offline.
- The added cameras should be on the same network as the DVR. For WAN and LAN, LAN is used for the internal network. The LAN port is only allowed to connect cameras, and it cannot connect to the Internet. WAN connects to the Internet, and users can manage the cameras through WAN.

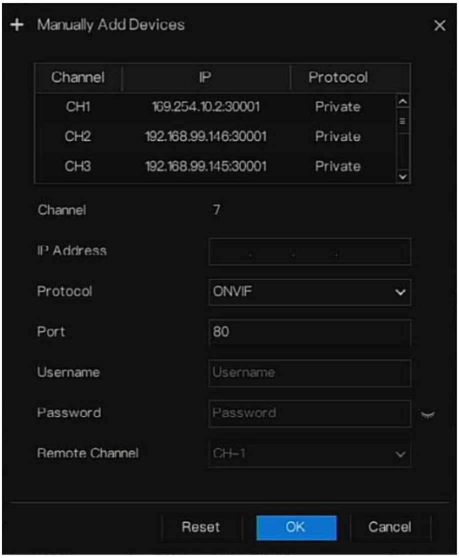
----End

6.1.1.2 Add Camera Manually

Operation Steps

Step 1 Click + to add devices as shown in Figure 6-3.

Figure 6-3 Add camera screen



Manually Add Devices

Channel	IP	Protocol
CH1	169.254.10.2:30001	Private
CH2	192.168.99.146:30001	Private
CH3	192.168.99.145:30001	Private

Channel 7

IP Address . . .

Protocol ONVIF

Port 80

Username Username

Password Password

Remote Channel CH-1

Step 2 Input the **IP address**, **Port**, **Username**, and **Password** of the camera. Double-click the online camera IP to copy its configuration. Quick changes to other channels' parameters can be made.

Step 3 Select a protocol from the drop-down list (**ONVIF, Private, Custom Protocols**). **Remote channel** is only used for multi-channel cameras, such as bi-spectrum thermal cameras, fisheye cameras, and so on.

Step 4 Click OK, the camera is added successfully.

NOTE

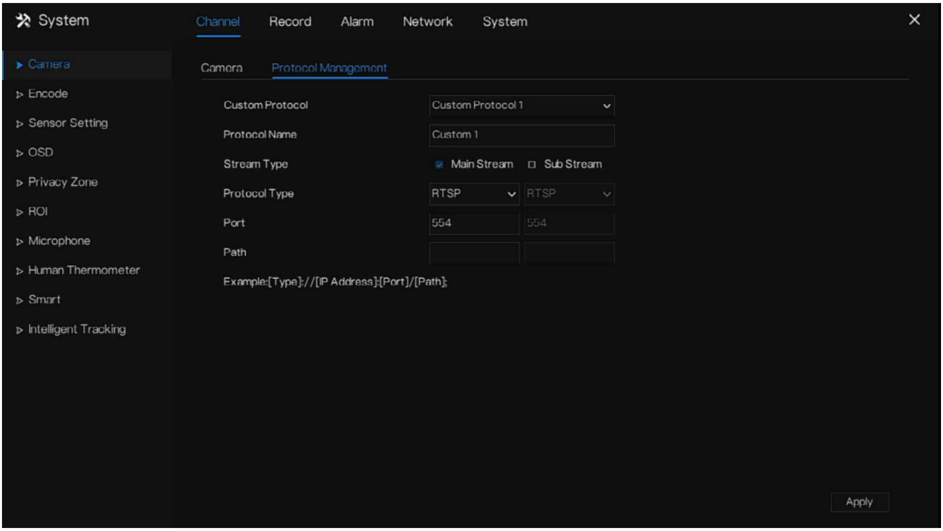
- If all channels of the DVR are connected by cameras, please delete the cameras that you don't need so that you can add more cameras.
- If an IP camera is added manually, input the correct username and password of the camera below the online device list. The camera will be added successfully. If not, the camera would be shown on the list as offline.
- The protocol can be chosen by the custom protocols; these are set at the protocol interface.
- For the Bi-spectrum camera, there are two channels; you should add both channels. The user can click the added channel to copy the information to save time; you just need to modify different information, such as the remote channel. If the remote channel is CH-1, the visible channel is added; remote channel is CH-2, the thermal channel is added. If users add DVR channels to DVR, they can copy the IP address, username, and password, only modify the remote channel to add different channels to DVR.

----End

6.1.1.3 Add Camera by RSTP

If the user wants to add the different protocol cameras to the DVR, you can set the **Protocol Management**, and add cameras one by one, as shown in Figure 6-4.

Figure 6-4 Protocol management



Custom Protocol: Custom Protocol 1

Protocol Name: Custom 1

Stream Type: ☑ Main Stream □ Sub Stream

Protocol Type: RTSP RTSP

Port: 554 554

Path:

Example:[Type]://[IP Address]:[Port]/[Path];

Step 1 Click **Settings > Channel > Camera > Protocol Management.**

Step 2 Choose the **Custom Protocol** from the drop-down list; 16 kinds of protocols can be set.

Step 3 Input the **protocol name**.

Step 4 Tick mainstream and substream. The mainstream shows the image on full-screen live video. The substream shows the image on the split screen. If you just tick mainstream, the channel will not show the image on a split screen.

Step 5 Choose the **Type of Protocol**, the default value is **RTSP**.

Step 6 Input the **Port** of the IP camera.

Step 7 Input the P**ath** (it may vary with different camera models).

Step 8 Click **Apply** to save the settings.

NOTE

Choose the protocol from the drop-down list; the protocol is set at the protocol management interface. The cameras should be confirmed according to the protocols.

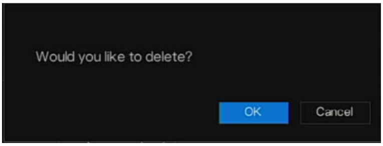
----End

6.1.1.4 Delete Camera

Operation Steps

Step 1 Select a camera to delete in the camera list and click 🗑. The delete confirmation message screen is displayed, as shown in Figure 6-5.

Figure 6-5 Delete confirmation message



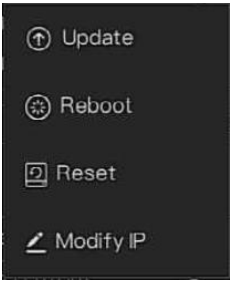
Would you like to delete?

Step 2 Click OK, the camera will be deleted successfully.

6.1.1.5 Operate Camera

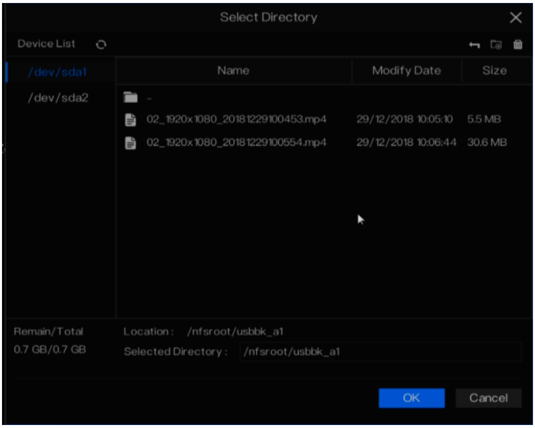
At the camera list, click ••• to operate the camera as shown in Figure 6-6; users can update, reboot, and reset the camera immediately.

Figure 6-6 More operation



Update: Click **Update**. A pop-up window will appear to select software, as shown in Figure 6-7. Set the directory and click OK to update the camera.

Figure 6-7 Select directory of software.



/dev/sda1
/dev/sda2

Name	Modify Date	Size
..		
02_1920x1080_20181229100453.mp4	29/12/2018 10:05:10	5.5 MB
02_1920x1080_20181229100554.mp4	29/12/2018 10:06:44	30.6 MB

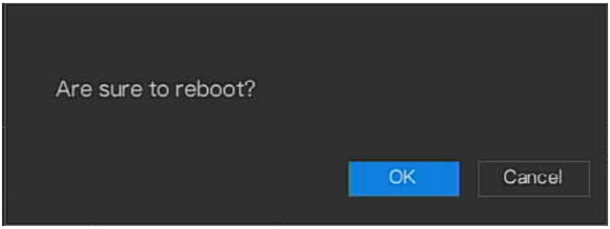
Remain/Total
0.7 GB/0.7 GB

Location : /nfsroot/usbbk_a1
Selected Directory : /nfsroot/usbbk_a1

Batch Update: Tick the cameras with non-ONVIF protocol and cameras are online; click **Update** to update all cameras at once.

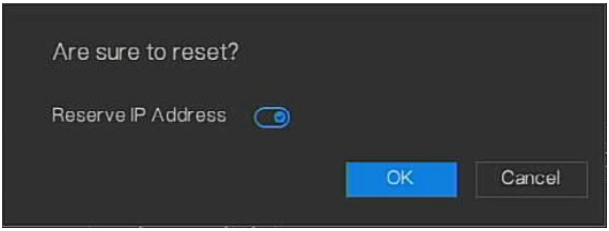
Reboot: Click **Reboot**, and the message **"Are sure to reboot?"** will show, click OK to reboot the camera.

Figure 6-8 Reboot camera


Are sure to reboot?

Reset: Click **Reset**, and the message **"Are sure to reset?"** will show, and users can enable the retain IP address function. Click OK to reboot the camera.

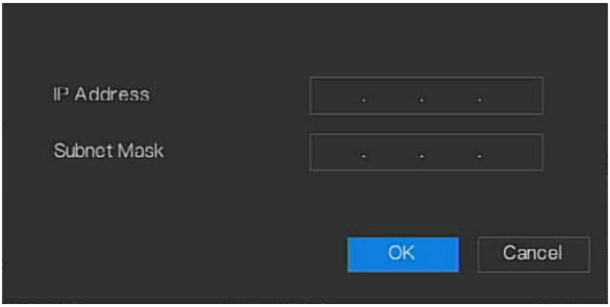
Figure 6-9 Reset camera


Are sure to reset?

Reserve IP Address

Modify IP: The IP address of the online camera can be modified. Click **Modify IP** to modify as shown in the following figure, and input the new IP address and subnet mask.

Figure 6-10 **Modify IP**



NOTE

The update needs to upload the firmware by the flash drive.

----End

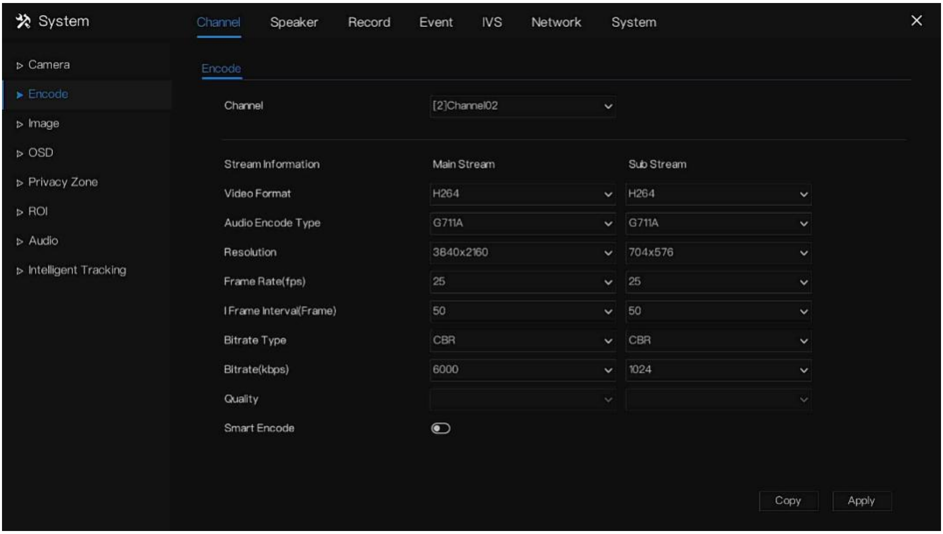
6.1.2 Encode Parameter

The system allows setting the **Stream Information**, **Encode Type**, **Resolution**, **Frame Rate**, **Bitrate Control**, **Bitrate**, and **Quality** for cameras in a channel in the **Encode Parameter** screen.

Operation Description

Navigate to **Settings > Channel > Encode** as shown in Figure 6-11.

Figure 6-11 Encode screen



Channel: [2]Channel02

Stream Information	Main Stream	Sub Stream
Video Format	H264	H264
Audio Encode Type	G711A	G711A
Resolution	3840x2160	704x576
Frame Rate(fps)	25	25
I Frame Interval(Frame)	50	50
Bitrate Type	CBR	CBR
Bitrate(kbps)	6000	1024
Quality		
Smart Encode	○	

Operation Steps

Step 1 Select a channel from the drop-down list of channels.

Step 2 Set **Video Format**, **Audio Encode Type**, **Resolution**, **Frame Rate**, **Bitrate Type**, **Bitrate Size**, and **Quality** from the drop-down lists.

Step 3 Click Copy and select channels or tick **all**, then click OK to apply the parameter settings to cameras in selected channels, and click Apply to save encode parameter settings.

----End

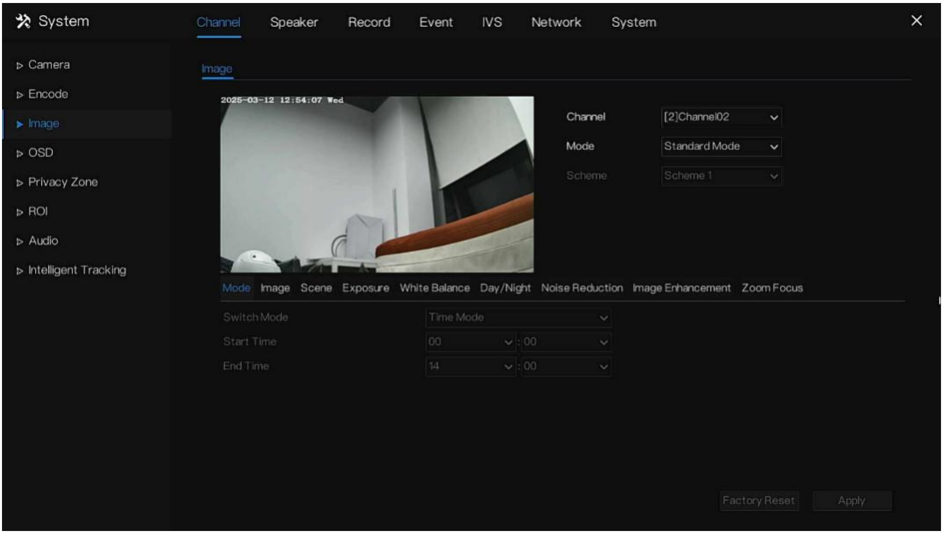
6.1.3 Image

Image refers to the basic attributes of pictures, it includes **brightness, sharpness, contrast**, and **saturation**. You can set picture parameters for each channel based on the scene.

Operation Description

Navigate to **Settings > Channel > Image** as shown in Figure 6-12.

Figure 6-12 Image screen



Channel: [2]Channel02

Mode: Standard Mode

Scheme: Scheme 1

Switch Mode: Time Mode

Start Time: 00 : 00

End Time: 14 : 00

The image settings are as follows: **mode, image, scene, exposure, white balance, day/night, noise reduction, image enhancement, and zoom focus** (it is applied to the monitored lens). For thermal cameras, users can set the **mode, image, scene, pseudocolor, FFC control, noise reduction, and image enhancement.**

- **Brightness**: It indicates the brightness or darkness of an image.
- **Sharpness**: It indicates the picture's clarity.
- **Contrast**: It refers to the brightest white and darkest black in an image.
- **Saturation**: It indicates the brilliance of the picture color.

Other parameters are image settings of IP cameras, like **scene, exposure, white balance, day-night, noise reduction, enhance image, zoom focus**, etc.

- **Scene**: It includes **indoor, outdoor**, and default. Mirror includes **normal, horizontal, vertical, horizontal + vertical**.
- **Exposure**: It includes mode, max shutter, meter area, and max gain.
- **White balance**: It includes tungsten, fluorescent, daylight, shadow, manual, etc.
- **Day/night**: Users can transit day to night or switch modes.
- **Noise reduction**: It includes 2D NR and 3D NR.
- **Enhance image**: It includes WDR, HLC, BLC, defog, and anti-shake.
- **Zoom focus**: Users can zoom and focus.

Operation Steps

Step 1 Select a channel from the drop-down list of channels. Select the **Debug Mode** to modify the settings. **Four schemes** can be set. The default scheme is **Scheme 1**.

Step 2 Select the **Scene** from the drop-down list. The default values of picture parameters vary with scenarios.

Step 3 Set parameters.

Step 4 Click Factory Reset to reset to factory settings if the setting is invalid; click Apply to save modified settings.

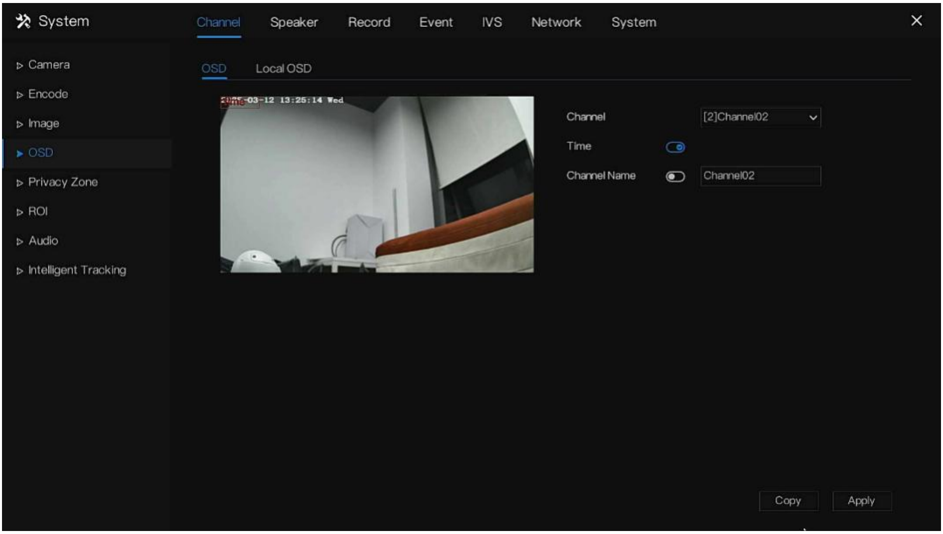
----End

6.1.4 OSD Settings

6.1.4.1 OSD

Navigate to **Settings > Channel > OSD** as shown in Figure 6-13.

Figure 6-13 OSD setting screen



Channel [2]Channel02

Time ●

Channel Name ○ Channel02

Operation Steps

Step 1 Select a channel from the drop-down list of channels.

Step 2 Click ○ next to Time to enable or disable the OSD time setting.

Step 3 Click ○ next to Name to enable or disable the OSD channel setting.

Step 4 Set the **Channel Name**.

Step 5 In the video window, click and drag the time or channel to move to a location.

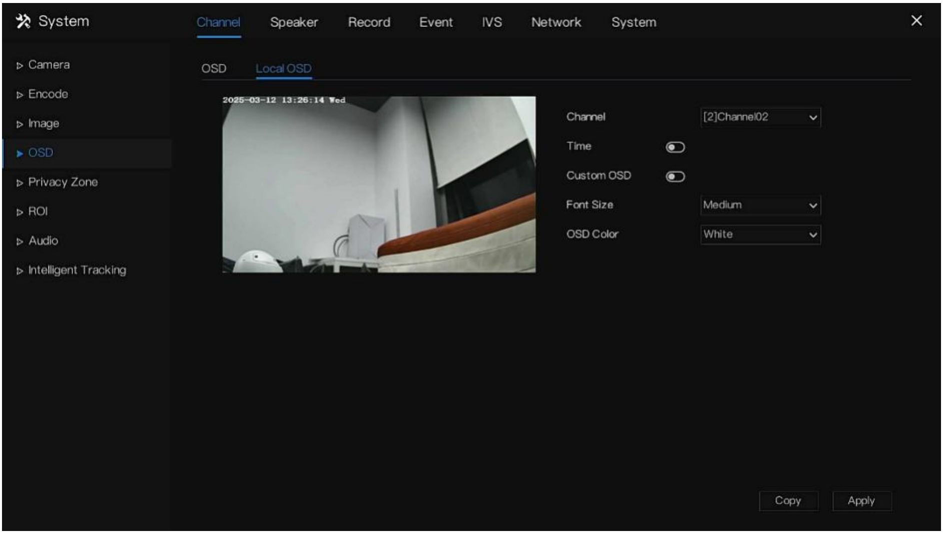
Step 6 Click Copy and select channels, then click OK to apply the OSD settings to cameras in selected channels, and click Apply to save OSD settings.

----End

6.1.4.2 Local OSD

Navigate to **Settings > Channel > OSD > Local OSD** as shown in Figure 6-14. It is used to the IPC without OSD, so the DVR sets the local OSD.

Figure 6-14 Local OSD



Channel: [2]Channel02
Time: ○
Custom OSD: ○
Font Size: Medium
OSD Color: White

Operation Steps

Step 1 Select a channel from the drop-down list of channels.

Step 2 Click ○ next to Time to enable or disable the OSD time setting.

Step 3 Click ○ next to Custom OSD to enable or disable the Custom OSD, and input the custom characters into the table; it will show on the live video.

Step 4 Set the font size and OSD color from the drop-down list.

Step 5 Click Copy and select channels, then click OK to apply the OSD settings to cameras in selected channels, and click Apply to save OSD settings.

----End

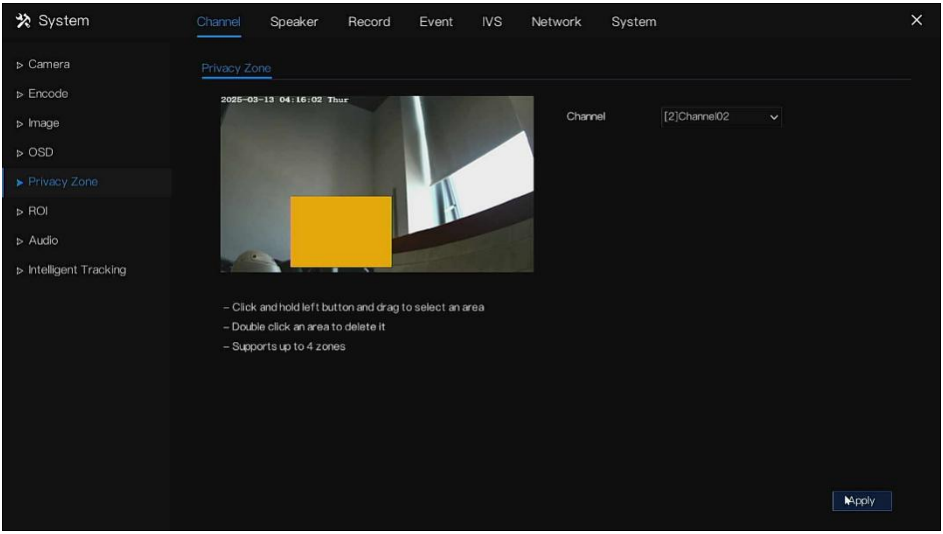
6.1.5 Privacy Zone

The system allows you to **mask images** in a specified zone, which is called a **Privacy Zone**.

Operation Description

Navigate to **Settings > Channel > Privacy Zone** as shown in Figure 6-15.

Figure 6-15 Privacy zone screen



Channel [2]Channel02

- Click and hold left button and drag to select an area
- Double click an area to delete it
- Supports up to 4 zones

Operation Steps

Step 1 Select a channel from the drop-down list of channels.

Step 2 In the video window, hold down and drag the left mouse button to draw a privacy area.

Step 3 Click Copy and select channels or tick **all**, then click OK to apply the privacy settings to cameras in selected channels, and click Apply to save privacy settings.

Step 4 Double-click the privacy area to delete the setting.

----End

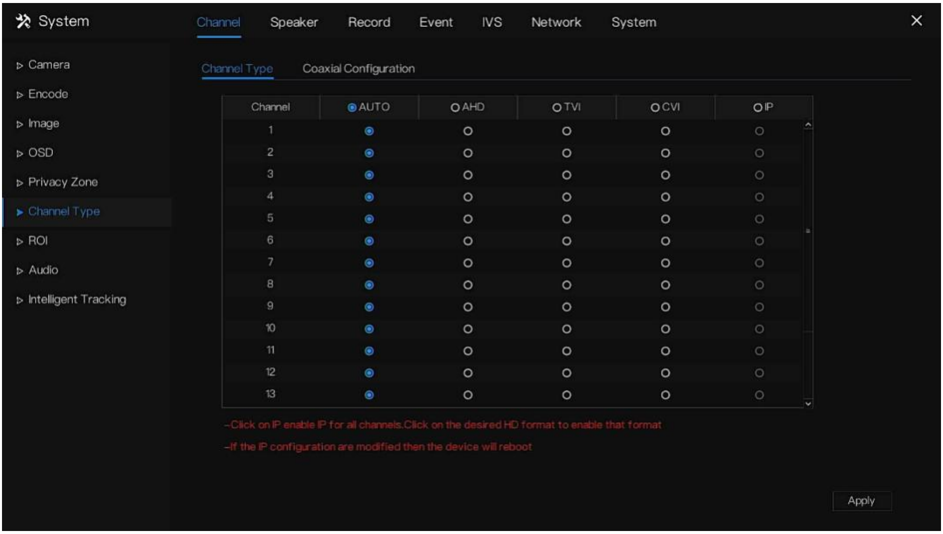
6.1.6 Channel Type

6.1.6.1 Channel Type

For the analog cameras, users can set the channel type to AUTO, AHD, TVI, CVI, or IP. If the IP mode is enabled, it works for all channels. The IP configuration is modified, and then the device will reboot.

Navigate to **Settings > Channel > Channel Type** as shown in Figure 6-16.

Figure 6-16 Channel Type setting screen



Channel	● AUTO	○ AHD	○ TVI	○ CVI	○ IP
1	●	○	○	○	○
2	●	○	○	○	○
3	●	○	○	○	○
4	●	○	○	○	○
5	●	○	○	○	○
6	●	○	○	○	○
7	●	○	○	○	○
8	●	○	○	○	○
9	●	○	○	○	○
10	●	○	○	○	○
11	●	○	○	○	○
12	●	○	○	○	○
13	●	○	○	○	○

-Click on IP enable IP for all channels.Click on the desired HD format to enable that format

-If the IP configuration are modified then the device will reboot

Operation Steps

Step 1 Choose a channel to set the Channel Type.

Step 2 Some devices have N+0.5N channels. N means the maximum number of connected coaxial cameras. 0.5N is the minimum number of IP cameras.

NOTE

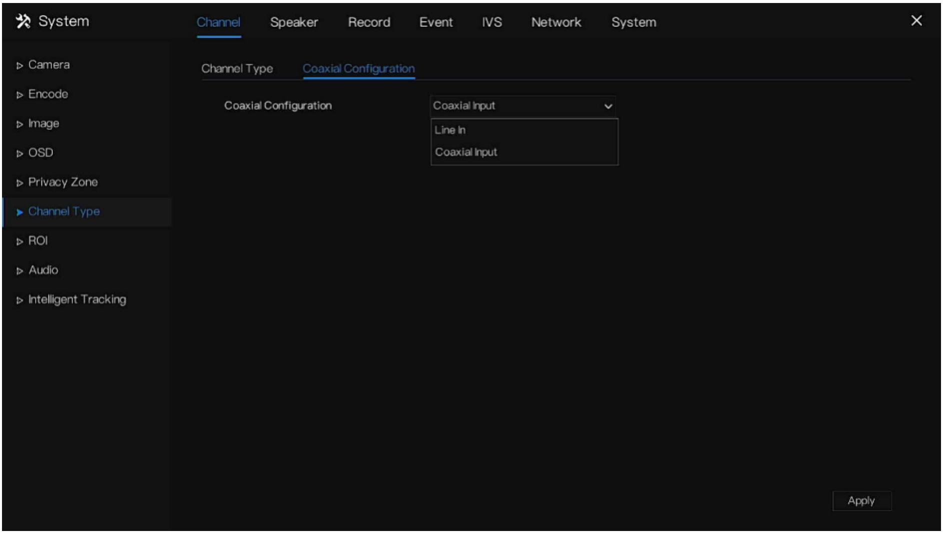
Click on IP to enable IP for all channels. Click on the desired HD format to enable that format.

If the IP configuration is modified, the device will reboot.

6.1.6.2 Coaxial Configuration

Set the Audio Input Type. The Line In means the audio input is by the audio input port on the DVR panel. The Coaxial Input means that the analog cameras need to have the built-in microphones, and the mode chosen is TVI on the OSD menu.

Figure 6-17 Coaxial Configuration

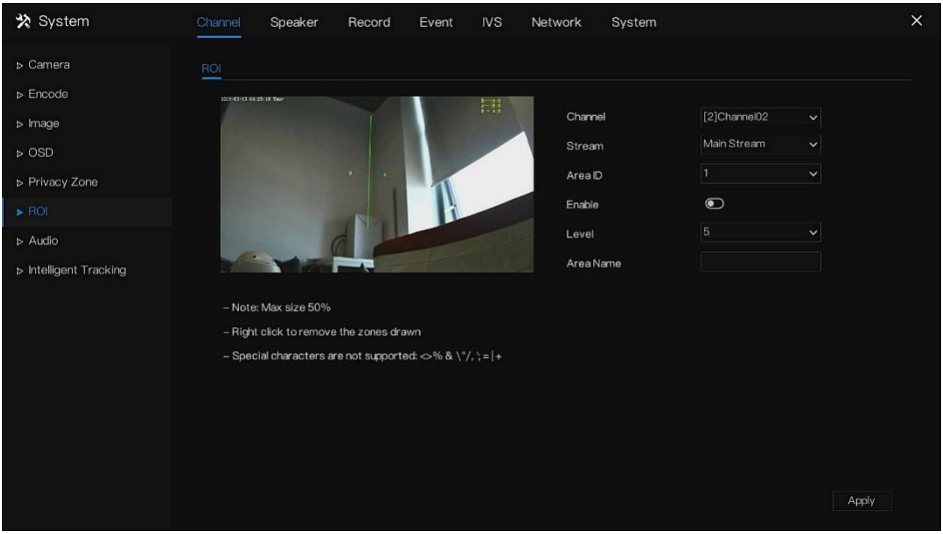


Coaxial Configuration: Coaxial Input

6.1.7 ROI

1. Navigate to **Settings > Channel > ROI** (Region of Interest) as shown in Figure 6-18.

Figure 6-18 ROI



Channel: [2]Channel02

Stream: Main Stream

Area ID: 1

Enable

Level: 5

Area Name

– Note: Max size 50%

– Right click to remove the zones drawn

– Special characters are not supported: <>% & \"/, ';=|+

Table 6-1 ROI parameter

Parameter	Description	Setting
Stream	Stream ID.	[Setting method] Select a value from the drop-down list box. [Default value] Stream 1
Enable	Enable the ROI	[Setting method] Click the button. [Default value] OFF
Area ID	ROI area ID, there are 8 area	[Setting method] Select a value from the drop-down list box. [Default value] 1
Level	The measured result of ROI. The higher the grade, the clearer the area inside and the more vaguer the area outside. There are five levels.	[Setting method] Select a value from the drop-down list box. [Default value] 5

Parameter	Description	Setting
Area Name	The marked name is used for areas.	[Setting method] Enter a value manually. The value cannot exceed 32 bytes.

2. Click Apply to save ROI settings.

----End

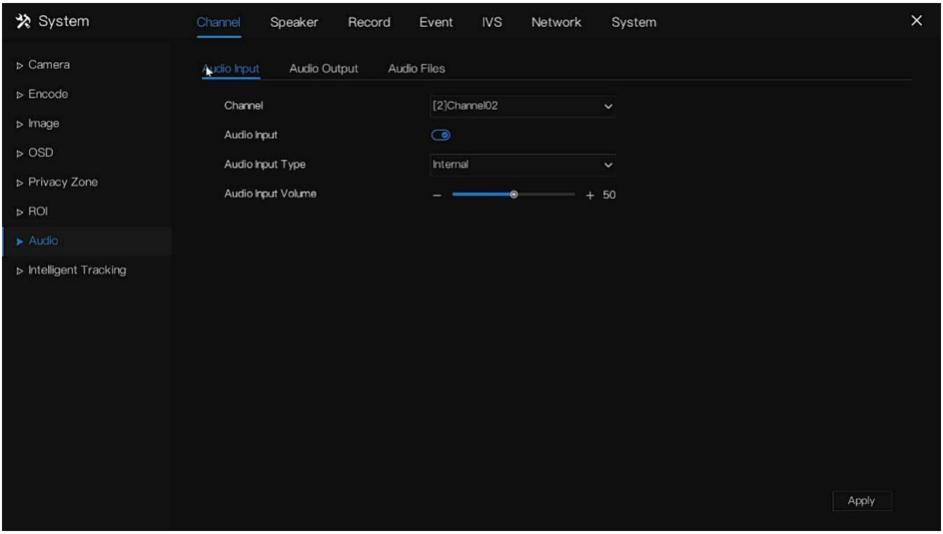
6.1.8 Audio (Only for Some Models)

6.1.8.1 Audio Input

Set the audio input parameters, an audio input device such as the **microphone**.

1. Navigate to **Settings > Channel > Audio > Audio Input** as shown in Figure 6-19.
2. Adjust the parameters as per Table 6-2.

Figure 6-19 Audio input



Channel: [2]Channel02

Audio Input: ●

Audio Input Type: Internal

Audio Input Volume: − + 50

Table 6-2 Audio input

Parameter	Description	Setting
Channel	Choose one channel to set.	[Setting method] Select a channel from the drop-down list box.
Enable Audio Input	Indicates whether to enable the microphone function.	[Setting method] Click the button to enable the microphone.
Audio Input Type	Audio input types include: ● Line In An active audio input is required. ● Internal The cameras have a built-in microphone.	[Setting method] Select a value from the drop-down list box.

Parameter	Description	Setting
Audio Input Volume	Allows you to adjust the audio input volume.	[Setting method] Slide the slider left or right. [Default value] 50 NOTE The value ranges from 0 to 100.

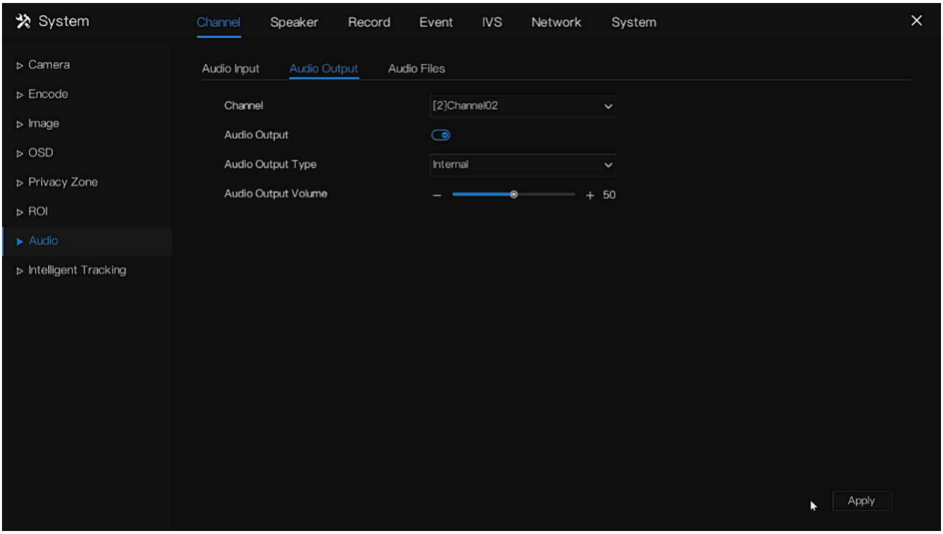
3. Click Apply to save privacy settings.

----End

6.1.8.2 Audio Output

1. Navigate to **Settings > Channel > Audio > Audio Output.**
2. Select **Audio Output**, set the audio output parameters, and select an audio output device such as a speaker.
3. Adjust the parameters as per Table 6-3.

Figure 6-20 Audio output



Channel: [2]Channel02

Audio Output: on

Audio Output Type: Internal

Audio Output Volume: − + 50

Table 6-3 Audio output

Parameter	Description	Setting
Channel	Choose one channel to set.	[Setting method] Select a channel from the drop-down list box.
Enable Audio output	Indicates whether to enable the speaker function.	[Setting method] Click the button to enable the microphone.
Audio output Type	Audio output types include: ● Line In An active audio output is required. ● Internal The cameras have a built-in speaker.	[Setting method] Select a value from the drop-down list box.
Audio output Volume	Allows you to adjust the audio output volume.	[Setting method] Slide the slider left or right. [Default value] 50 NOTE The value ranges from 0 to 100.

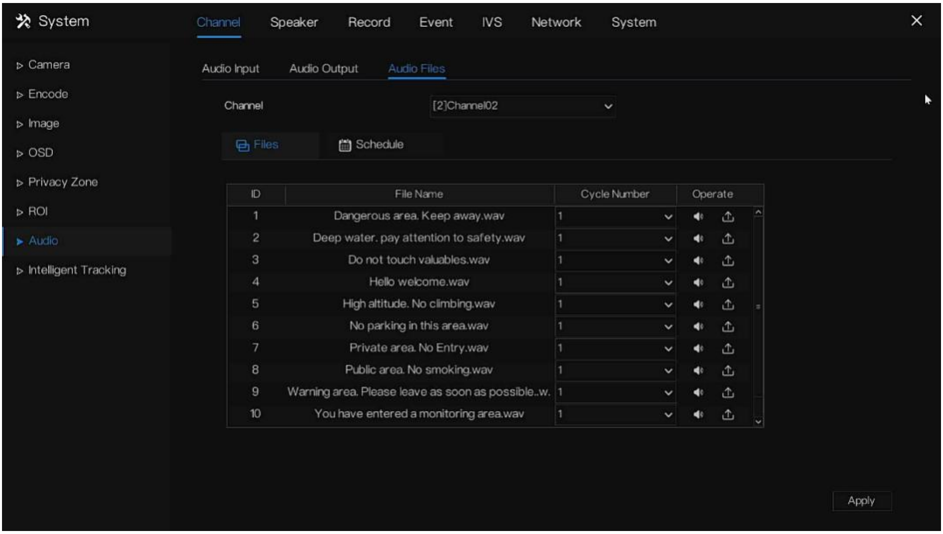
4. Click Apply to save privacy settings.

----End

6.1.8.3 Audio Files

1. Navigate to **Settings > Channel > Audio.**
2. Select **Audio Files**, and set the audio files. The user can upload the audio files, and when the alarm is triggered, you can enable the audio alarm to play the audio to warn.

Figure 6-21 Audio files



Channel: [2]Channel02

ID	File Name	Cycle Number	Operate
1	Dangerous area. Keep away.wav	1	🔊 ⇪
2	Deep water. pay attention to safety.wav	1	🔊 ⇪
3	Do not touch valuables.wav	1	🔊 ⇪
4	Hello welcome.wav	1	🔊 ⇪
5	High altitude. No climbing.wav	1	🔊 ⇪
6	No parking in this area.wav	1	🔊 ⇪
7	Private area. No Entry.wav	1	🔊 ⇪
8	Public area. No smoking.wav	1	🔊 ⇪
9	Warning area. Please leave as soon as possible..w.	1	🔊 ⇪
10	You have entered a monitoring area.wav	1	🔊 ⇪

3. Choose a channel from the drop-down list.
4. Select one audio file, set the cycle number, and click 🔊 to play.
5. Users can customize the audio file to play. Click ⇪ to select the file to upload.
6. Click Apply to save settings.

NOTE

- The type should be WAV, the size must be **less than 250 KB**, and the bit rate should be **128 kbps**.
- The schedule of the audio file is the general set for **all linkage audio alarms**. It is out of the schedule; the audio alarm is invalid.

Figure 6-22 Upload audio file

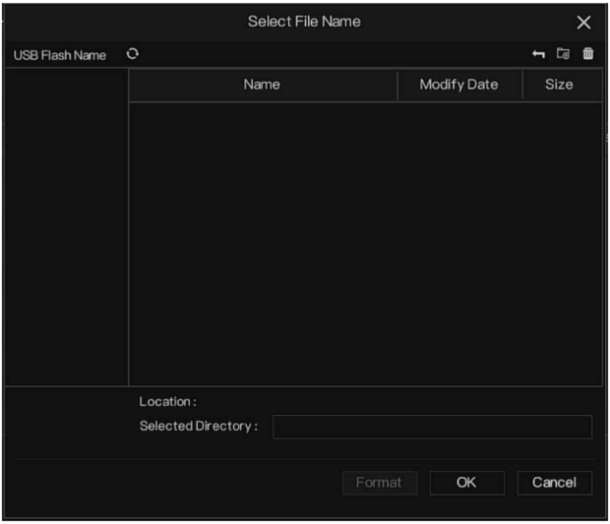
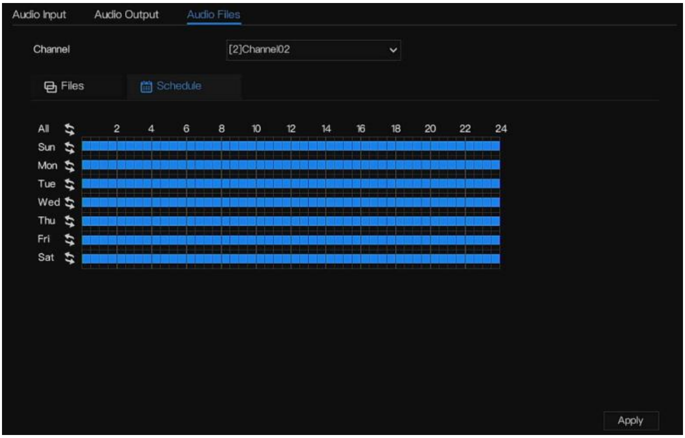


Figure 6-23 Schedule of audio file



6.1.9 Intelligent Tracking (Only for Some Models)

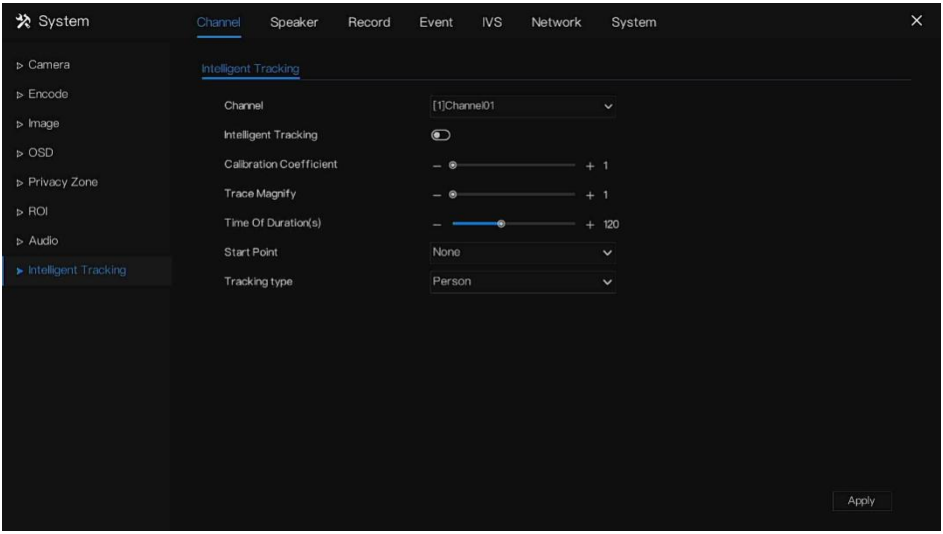
NOTE

This function is available for high-speed cameras.

The **Intelligent Tracking** function is that the dome camera can continuously track the moving target of the pre-made scene and automatically adjust the camera zoom focus according to the moving target distance, and the dome automatically returns to the preset scene when the moving target disappears.

1. Navigate to **Settings > Channel > Intelligent Tracking** as shown in Figure 6-24.
2. Adjust the parameters as per Table 6-4.
3. Click Apply to save settings.

Figure 6-24 Intelligent tracking



Channel [1]Channel01
Intelligent Tracking
Calibration Coefficient 1
Trace Magnify 1
Time Of Duration(s) 120
Start Point None
Tracking type Person

Table 6-4 Intelligent tracking parameters

Parameter	Description	Setting
Channel	Choose one channel to set.	[Setting method] Select a channel from the drop-down list box.

Enable	Enable the button to enable intelligent tracking	[How to set] Click Enable to enable. [Default value] OFF
Calibration Coefficient	It is equivalent to a control coefficient, and real-time tracking doubling rate nonlinear positive correlation, usually the higher the installation height, the greater the calibration coefficient value; it ranges from 1 to 30	[Setting method] Drag the slider. [Default value] **1**
Trace Magnify	It is the value of lens zoom, it has a large influence on the real-time tracking magnification,	[Setting method] Drag the slider. [Default value] **7**
Time of Duration	The maximum time of a tracking period ranges from 0 to 300 s.	[Setting method] Drag the slider. [Default value] **120**
Start Point	At the start point of the tracking, you can choose the preset or none. The preset should be set in advance.	[Setting method] Choose from the drop-down list. [Default value] **None**
Tracking Type	Choose the tracking type, person, or car.	[Setting method] Choose from the drop-down list. [Default value] **Person**

----End

6.2 Speaker

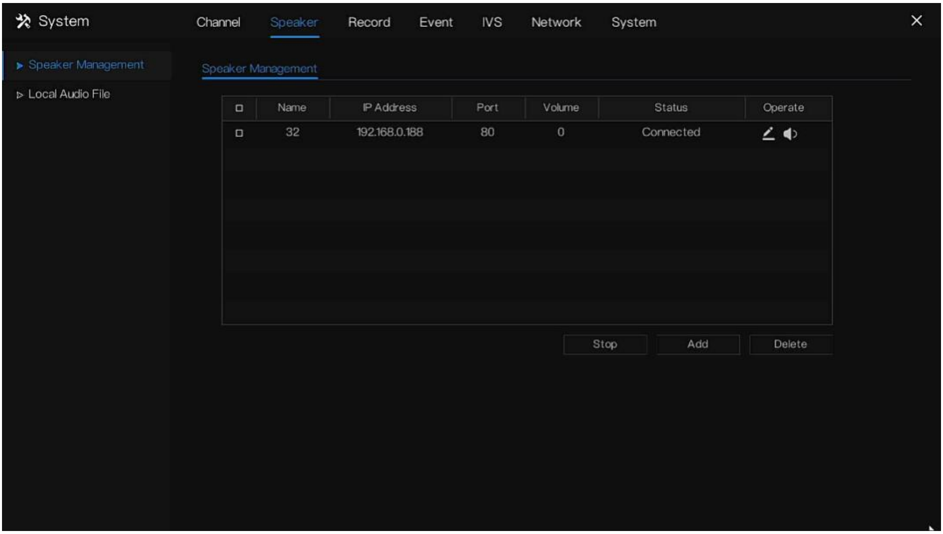
Users can add the speaker to the DVR so that the DVR broadcasts the video files.

Click **Speaker Management** on **Settings > Speaker** to access the record schedule screen.

6.2.1 Speaker Management

Step 1 Navigate to **Settings > Speaker** as shown in Figure 6-25.

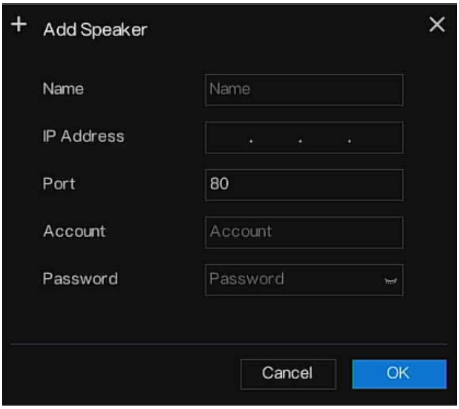
Figure 6-25 Speaker management



□	Name	IP Address	Port	Volume	Status	Operate
□	32	192.168.0.188	80	0	Connected	✎ 🔈

Step 2 Click **Add** to add the speaker to the DVR. Input the parameters of the speaker. Click **OK** to add.

Figure 6-26 Add speaker



Add Speaker

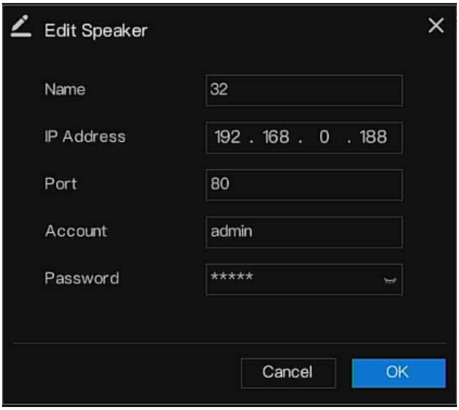
Name	Name
IP Address	. . .
Port	80
Account	Account
Password	Password

Step 3 Add succeeded. Click 🔈 to adjust the audio volume.

Step 4 Tick the speaker, and click **Delete** to delete the chosen speaker. When the speaker is triggered by the event alarm, click **Stop** to end the broadcast.

Step 5 Click ✎ to edit the speaker.

Figure 6-27 Edit speaker



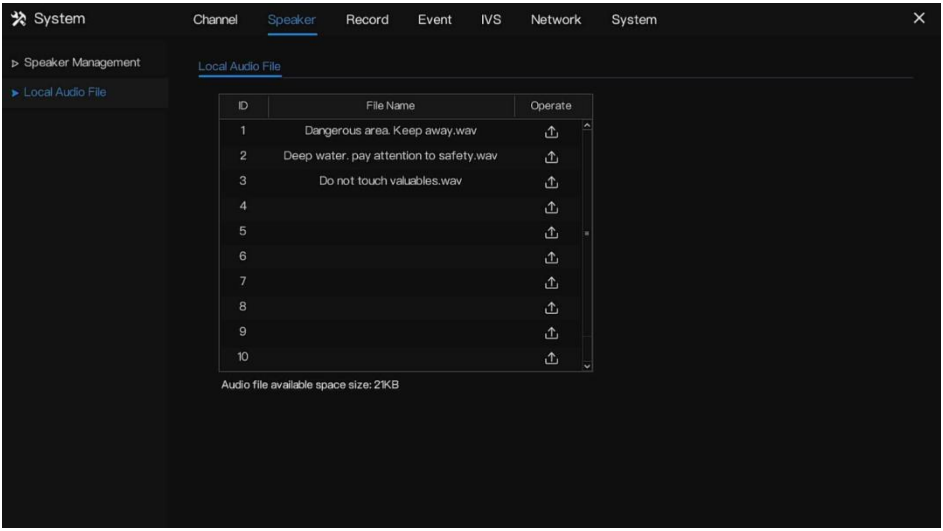
Edit Speaker

Name	32
IP Address	192 . 168 . 0 . 188
Port	80
Account	admin
Password	*****

6.2.1.2 Local Audio File

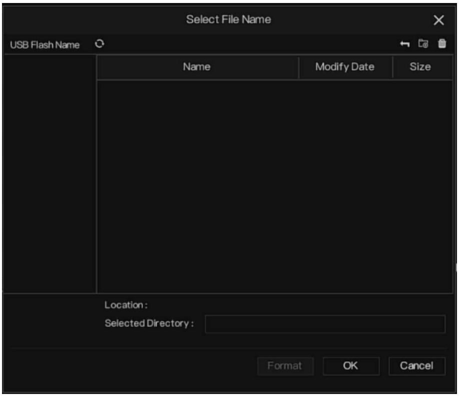
Users can upload **11 audio files** one by one or use the default audio file. The sum size of all files can’t exceed 128 Kb. The uploaded audio files should be WAV-type.

Figure 6-28 Local audio file



ID	File Name	Operate
1	Dangerous area. Keep away.wav	⇪
2	Deep water. pay attention to safety.wav	⇪
3	Do not touch valuables.wav	⇪
4		⇪
5		⇪
6		⇪
7		⇪
8		⇪
9		⇪
10		⇪

Audio file available space size: 21KB



6.3 Record-Setting

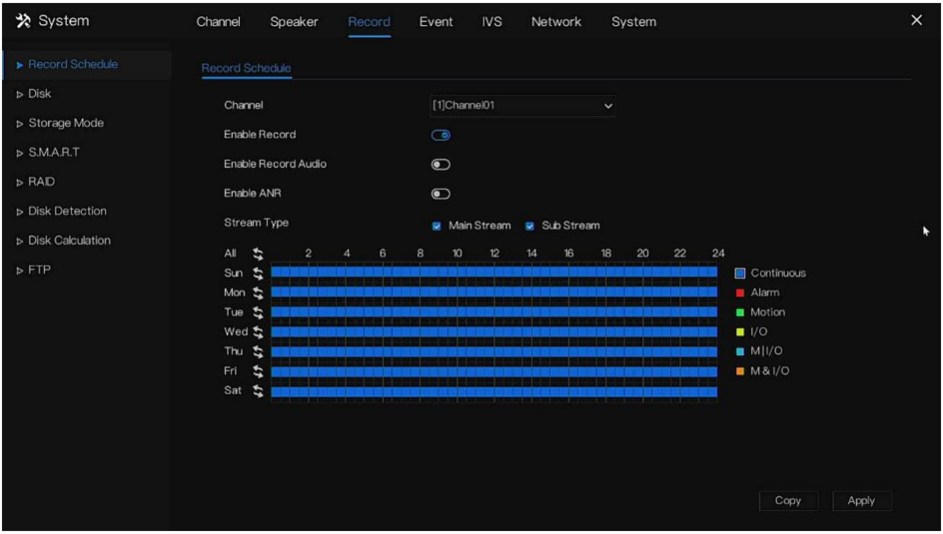
Set the **Record Schedule, Disk, Storage Mode**, **S.M.A.R.T**, **Disk Detection**, **Disk Calculation**, **FTP**, and so on.

6.3.1 Record Schedule

Operation Description

Navigate to **Settings > Record > Record Schedule** as shown in Figure 6-29.

Figure 6-29 Record management screen



Channel [1]Channel01

Enable Record

Enable Record Audio

Enable ANR

Stream Type ☑ Main Stream ☑ Sub Stream

Operation Steps

Step 1 Select a channel from the drop-down list of channel option.

Step 2 Enable the Record.

Step 3 Enable the Recorded Audio.

Step 4 Enable ANR. The camera is installed with an SD card If the camera is disconnected from the network, when the network is recovered, the DVR can read the recording of the camera and copy the lost video from the SD card.

Step 5 Tick to choose mainstream or substream to record.

Step 6 Set the record schedule.

- **Method 1**: Hold down the left mouse button, drag, and release the mouse to select the arming time between 00:00 and 24:00 from Monday to Sunday.

NOTE

- When you select time by dragging the cursor, the cursor cannot move out of the time area. Otherwise, no time would be selected.
- The selected area is **blue**. The default is **all week**.
- Users can choose an alarm type to record; if the chosen alarm is happening at the set time, it will record. So that it will be using the disk effectively to avoid repeating useless recordings.
- The **ANR function** can be used only for the cameras with a supplementary recording function.
- Users can set different alarms to record.

- **Method 2**: Click ⇅ on the record schedule page to select the whole day or whole week.

Step 7 Deleting record schedule: Click ⇅ again or inverse selection to delete the selected record schedule.

Step 8 Click Copy and select channels or tick **all**, then click OK to apply the record management settings to selected channels, and click Apply to save settings.

----End

6.3.2 Disk

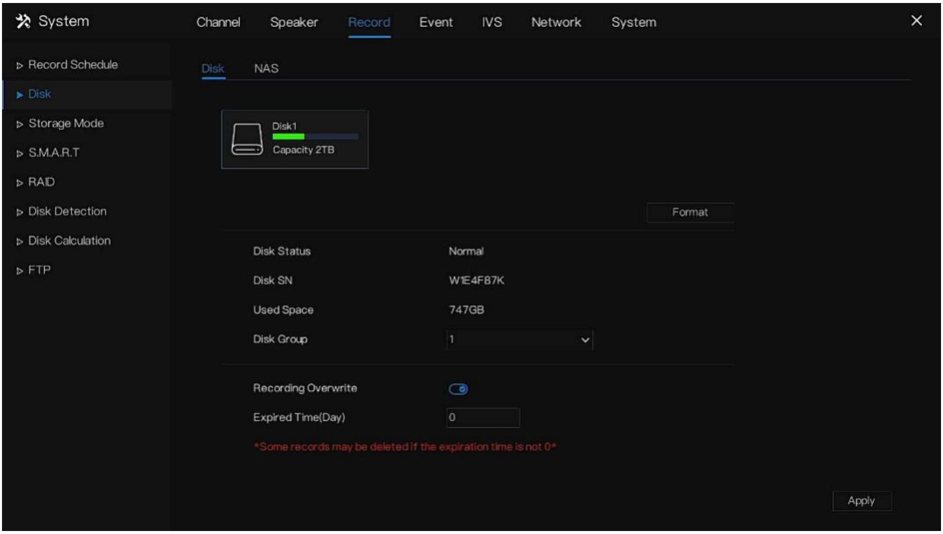
6.3.2.1 Disk

View the total **capacity** of the disk, disk **status**, disk **SN code**, and **storage space** of the disk. You can **format** the disk and set a record **expiration time**.

Operation Description

Step 1 Navigate to **Record > Disk** as shown in Figure 6-30.

Figure 6-30 Disk screen



Disk Status Normal

Disk SN W1E4F87K

Used Space 747GB

Disk Group 1

Recording Overwrite

Expired Time(Day) 0

Some records may be deleted if the expiration time is not 0

Step 2 Click **Format**. The message **"Are you sure to format the disk? Your data will be lost"** is displayed.

Step 3 Choose the **Disk Group**; there are **four groups**.

Step 4 Click OK, and the disk will be formatted.

Step 5 Enable recording to **Overwrite**; the disk will be overwritten automatically.

Step 6 Record expiration setting. Select record expiration days from the drop-down list of record expiration. If the expired time is **not 0**, the records will **be deleted** when the time is over the setting value.

Step 7 Click Apply to save the settings.

NOTE

The disk groups can keep the recording of channels at different disks, which will improve the storage efficiency.

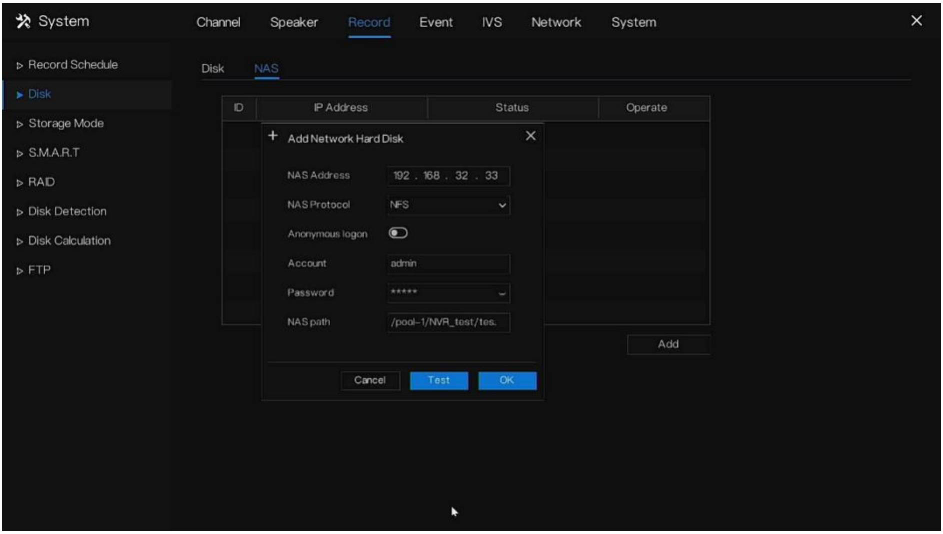
The expired time is 0, which means the disk will be rewritten only when the disk is full.

----End

6.3.2.2 NAS

If users have NAS accounts, set the settings of NAS for saving the backup recording.

Figure 6-31 NAS



Add Network Hard Disk

NAS Address: 192 . 168 . 32 . 33

NAS Protocol: NFS

Anonymous logon

Account: admin

Password: *****

NAS path: /pool-1/NVR_test/tes.

Step 1 Navigate to **Record > Disk > NAS** to enter the NAS interface.

Step 2 Click **ADD** to add an account, then input the **NAS address** (the NAS protocol is default NFS, and enter the account and password. If the anonymous logon is on, the account and password are invalid). Input **NAS path** (the path can be viewed at the NAS interface)

Step 3 Click **Test** to test for verifying the parameters; if it tests successfully, click **OK** to save the settings.

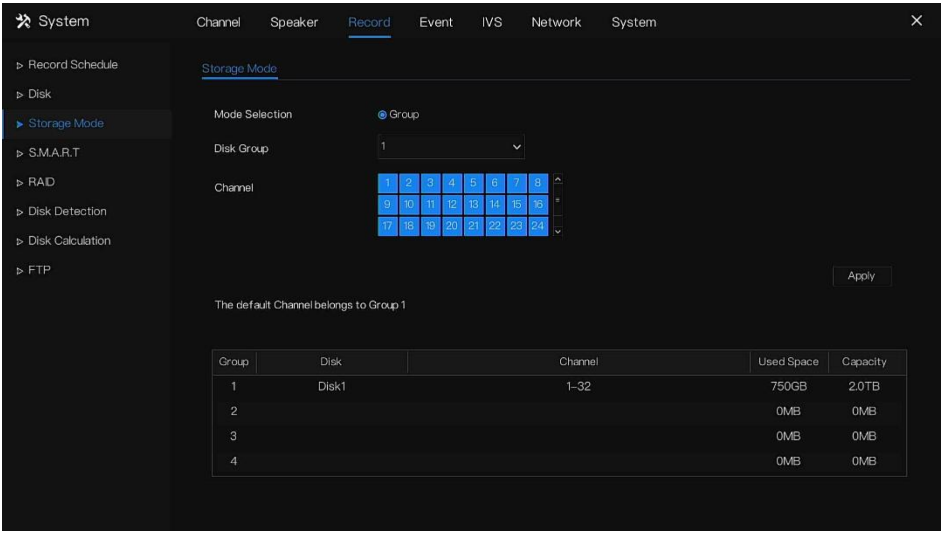
6.3.3 Storage Mode

Users need to distribute the channels to different disk groups and use disk capacity reasonably.

Operation Steps

Step 1 Navigate to **Settings > Record > Storage** as shown in Figure 6-32.

Figure 6-32 Storage mode



Mode Selection ● Group

Disk Group 1

Channel 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

The default Channel belongs to Group 1

Group	Disk	Channel	Used Space	Capacity
1	Disk1	1–32	750GB	2.0TB
2			0MB	0MB
3			0MB	0MB
4			0MB	0MB

Step 2 Choose the Disk Group.

Step 3 Select the channel to record to a disk group.

Step 4 Click **Apply** to save the settings.

Step 5 The group list will show the detailed information.

NOTE

- If the channels are not in the list, it means the DVR will not record these channels; please make sure that all channels are in the list.
- Choose the number of channels. You should consider the capacity of the disk group.

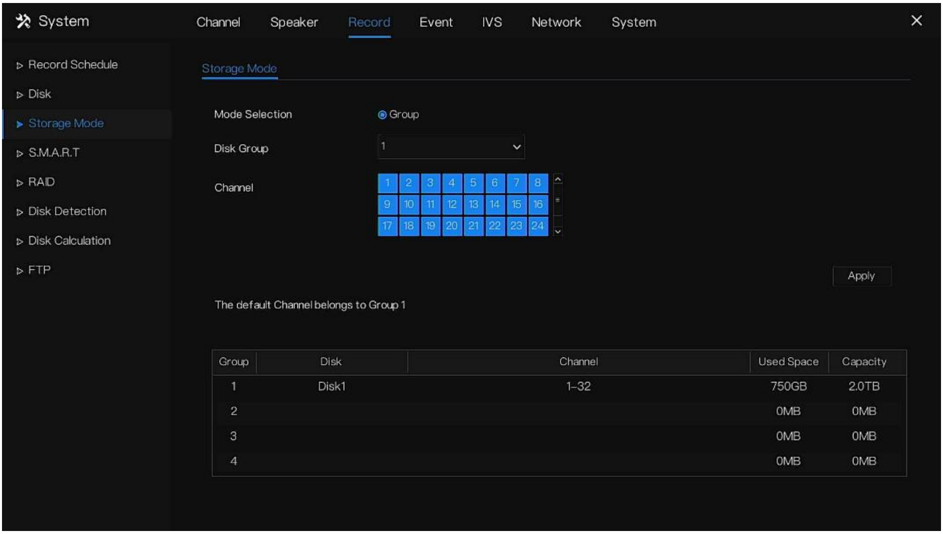
----End

6.3.4 S.M.A.R.T

6.3.4.1 S.M.A.R.T

S.M.A.R.T is a **Self-Monitoring Analysis and Reporting Technology**, which can check the disk as shown in Figure 6-33.

Figure 6-33 S.M.A.R.T



Mode Selection ● Group

Disk Group 1

Channel

The default Channel belongs to Group 1

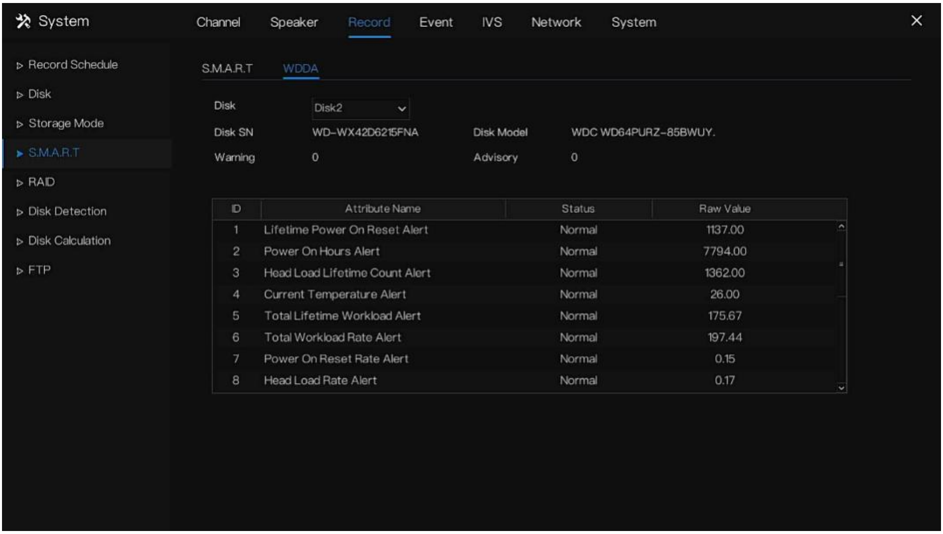
Group	Disk	Channel	Used Space	Capacity
1	Disk1	1-32	750GB	2.0TB
2			0MB	0MB
3			0MB	0MB
4			0MB	0MB

----End

6.3.4.2 WDDA

The **Western Digital disk** has the **WDDA** function, and the DVR can read the information of the disk so that users can view the status of the disk, as shown in Figure 6-34.

Figure 6-34 WDDA



Disk: Disk2

Disk SN: WD-WX42D6215FNA

Disk Model: WDC WD64PURZ-85BWUY.

Warning: 0

Advisory: 0

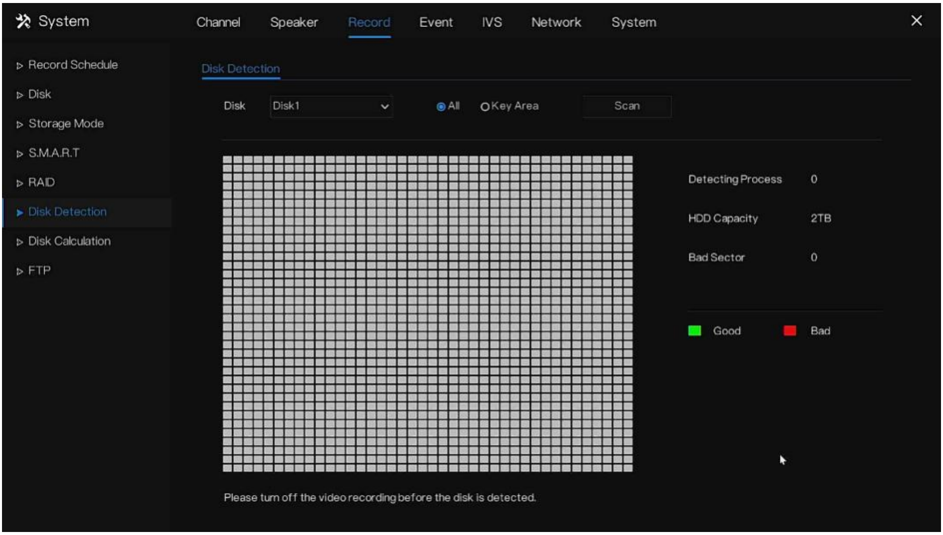
ID	Attribute Name	Status	Raw Value
1	Lifetime Power On Reset Alert	Normal	1137.00
2	Power On Hours Alert	Normal	7794.00
3	Head Load Lifetime Count Alert	Normal	1362.00
4	Current Temperature Alert	Normal	26.00
5	Total Lifetime Workload Alert	Normal	175.67
6	Total Workload Rate Alert	Normal	197.44
7	Power On Reset Rate Alert	Normal	0.15
8	Head Load Rate Alert	Normal	0.17

----End

6.3.5 Disk Detection

Detect the disk before recording videos so that the data are secure, as shown in Figure 6-35.

Figure 6-35 Disk Detection



Disk Disk1

● All ○ Key Area

Detecting Process 0

HDD Capacity 2TB

Bad Sector 0

🟩 Good 🟥 Bad

Please turn off the video recording before the disk is detected.

Operation Steps

Step 1 Navigate to **Settings** > **Record** > **Disk Detection.**

Step 2 Choose the disk from the drop-down list.

Step 3 Tick **All** or **Key Area** to detect the disk. It will take several minutes.

Step 4 Click Scan to scan the disk.

Step 5 The result of the disk will show in the interface.

NOTE

- The green block means good and the red block means bad. If the red blocks are too much or at the key section, please change the disk immediately.
- Please turn off the video recording before the disk is detected; otherwise, the recording of the video may be lost.

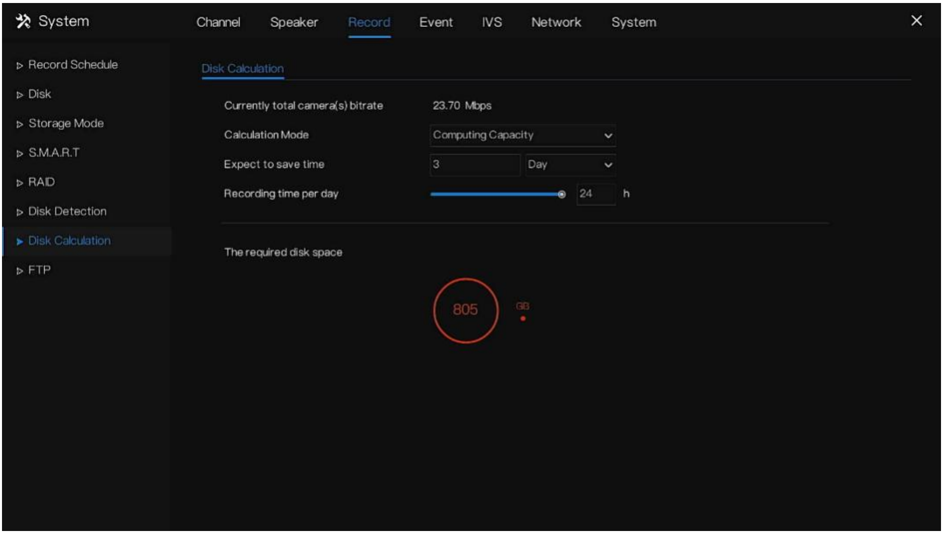
----End

6.3.6 Disk Calculation

Users can calculate the usage of the disk so that they can set the storage strategy reasonably, as shown in Figure 6-36.

Two modes can be set: **Computing Capacity** and **Computing Time**.

Figure 6-36 Disk calculation of capacity



Currently total camera(s) bitrate 23.70 Mbps

Calculation Mode Computing Capacity

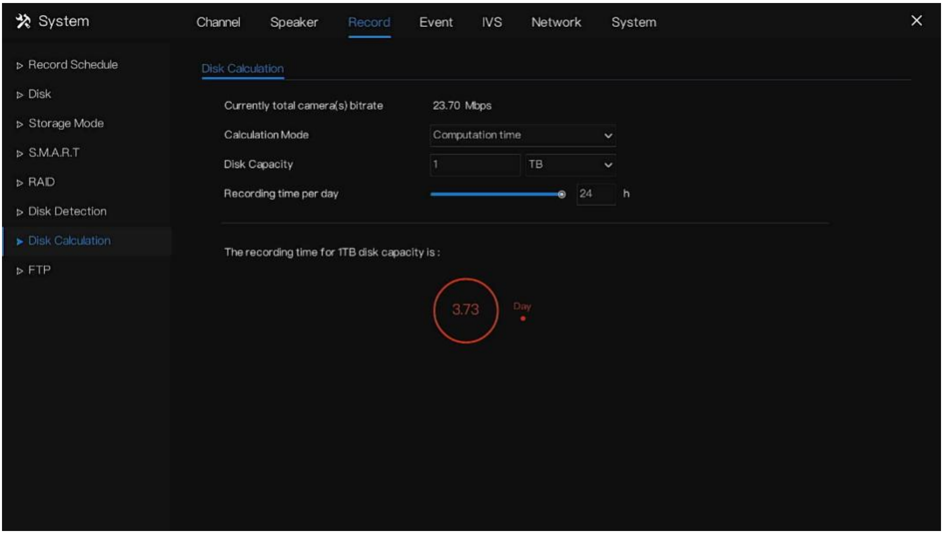
Expect to save time 3 Day

Recording time per day 24 h

The required disk space

805 GB

Figure 6-37 Disk calculation of time



Currently total camera(s) bitrate 23.70 Mbps

Calculation Mode Computation time

Disk Capacity 1 TB

Recording time per day 24 h

The recording time for 1TB disk capacity is :

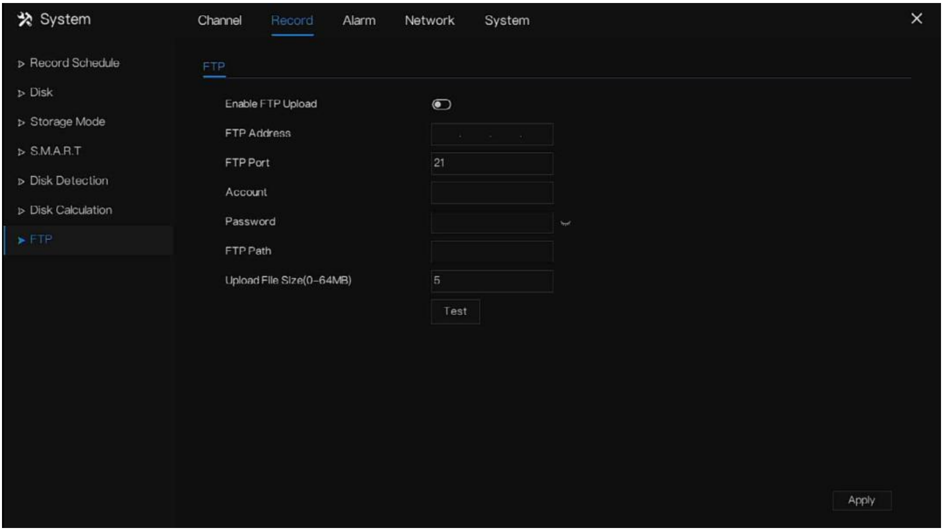
3.73 Day

----End

6.3.7 FTP

Enable FTP upload; when the alarm happens, users can link the FTP upload to save the alarm recordings.

Figure 6-38 FTP



Enable FTP Upload

FTP Address . . .

FTP Port 21

Account

Password

FTP Path

Upload File Size(0-64MB) 5

Step 1 Navigate to **Settings > Event > FTP.**

Step 2 **Enable** the FTP upload.

Step 3 Input the FTP address and port.

Step 4 Input the **account, password**, and **FTP path**.

Step 5 Set the upload file size, which ranges from **0 to 64 MB**.

Step 6 Click **Test** to test the parameters. After the test is successful, click **Apply** to save the settings.

----End

6.4 Event Management

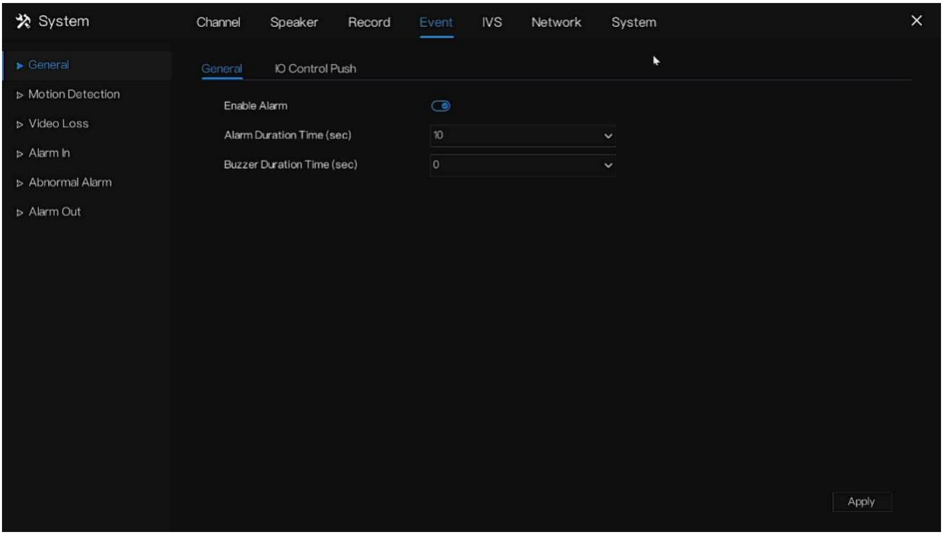
Set the **General**, **Motion Detection**, **Video Loss**, **Alarm In**, **Video Tampering**, **Abnormal Alarm**, and **Alarm Out** in the **Event** screen.

6.4.1 General

6.4.1.1 General

Step 1 Navigate to **Settings > Event > General**, as shown in Figure 6-39.

Figure 6-39 Alarm management screen



Enable Alarm

Alarm Duration Time (sec) 10

Buzzer Duration Time (sec) 0

Step 2 Click to **Enable** the alarm function.

Step 3 Select a value from the drop-down list of **Duration Times**.

Step 4 Click Apply to save alarm settings.

----End

6.4.1.2 IO control push

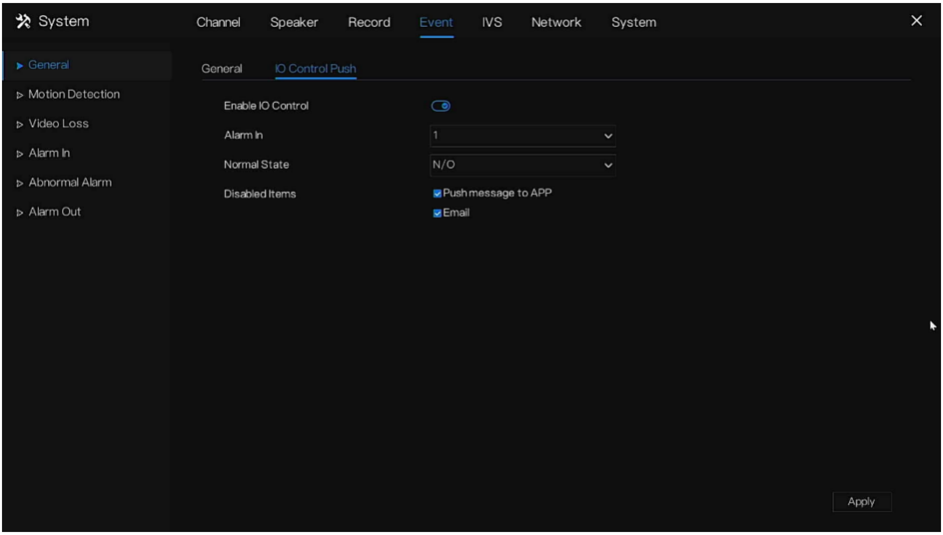
IO control push is to enable the **IO port** of the DVR rear panel. When the IO port receives the match signal, it will be a push message. For example, if you select **Normally Open** and tick the

Disabled Items, the alarm input 1 will not push the message. Only when the alarm in 1 is **Normally Closed**, it can **push** the alarm message.

Step 1 Navigate to **Settings > Event > General** > **IO Control Push**.

Step 2 Enable the IO control push.

Figure 6-40 IO control push



Enable IO Control ●

Alarm In 1

Normal State N/O

Disabled Items ☑ Push message to APP ☑ Email

Step 3 Choose one **Alarm In ID**. Choose the **normal state** (N/C, N/O).

Step 4 Tick the **Disabled Items** (the disabled item will affect **all alarms**; this push item will be invalid, and the alarm will not push a message to the app or email)

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

----End

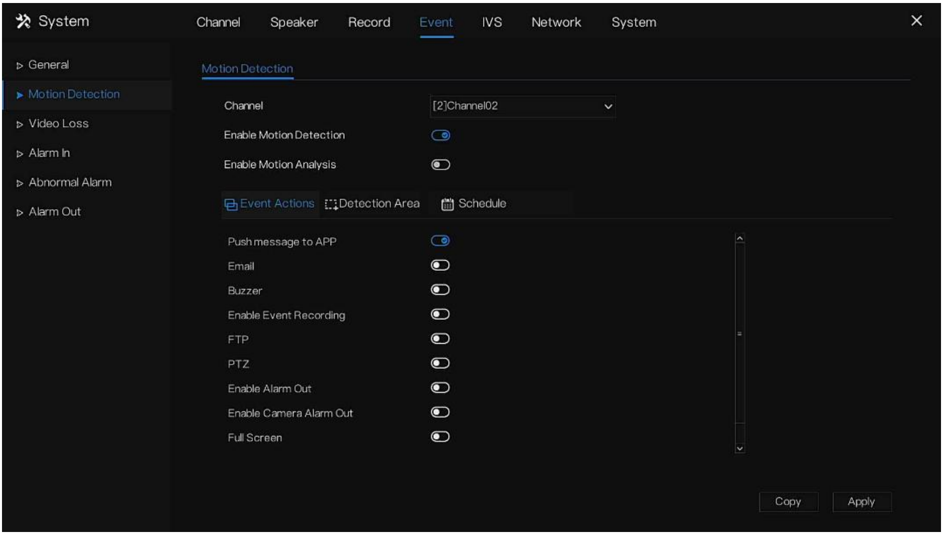
6.4.2 Motion Detection

The DVR will send a motion detection alarm while something is moving in the specific view of the camera.

Operation Description

Step 1 Navigate to **Settings > Event > Motion Detection** as shown in Figure 6-41.

Figure 6-41 Motion detection screen



Channel [2]Channel02

Enable Motion Detection ●

Enable Motion Analysis ○

Push message to APP ●

Email ○

Buzzer ○

Enable Event Recording ○

FTP ○

PTZ ○

Enable Alarm Out ○

Enable Camera Alarm Out ○

Full Screen ○

Operation Steps

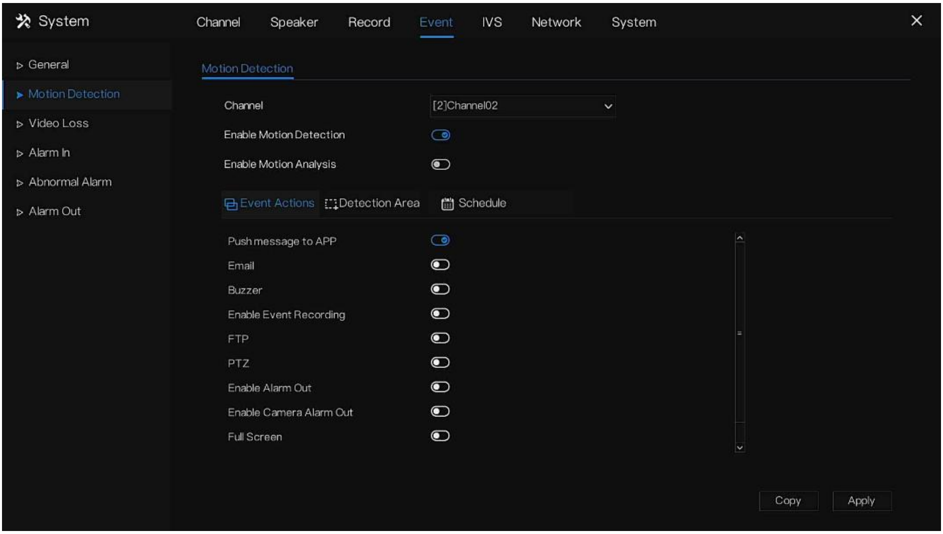
Step 1 Select a channel from the drop-down list of channels.

Step 2 Click ○ to enable motion detection.

Step 3 Enable motion analysis if the camera detects the motion action, the **motion area** will be blocked completely, as shown in Figure 6-42.

Step 4 Enable the Event Actions including **Push Messages to App**, **Email**, **Buzzer**, **Enable Event Recordings**, **FTP**, **PTZ**, **Enable Alarm Out**, **Full Screen**, **Speaker** and so on. Configure the settings as per Table 6-5.

Table 6-5 Event actions



Channel [2]Channel02

Enable Motion Detection ●

Enable Motion Analysis ○

Push message to APP ●

Email ○

Buzzer ○

Enable Event Recording ○

FTP ○

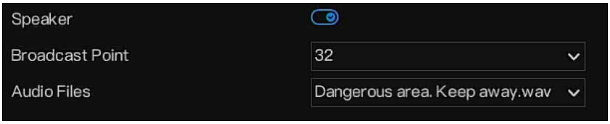
PTZ ○

Enable Alarm Out ○

Enable Camera Alarm Out ○

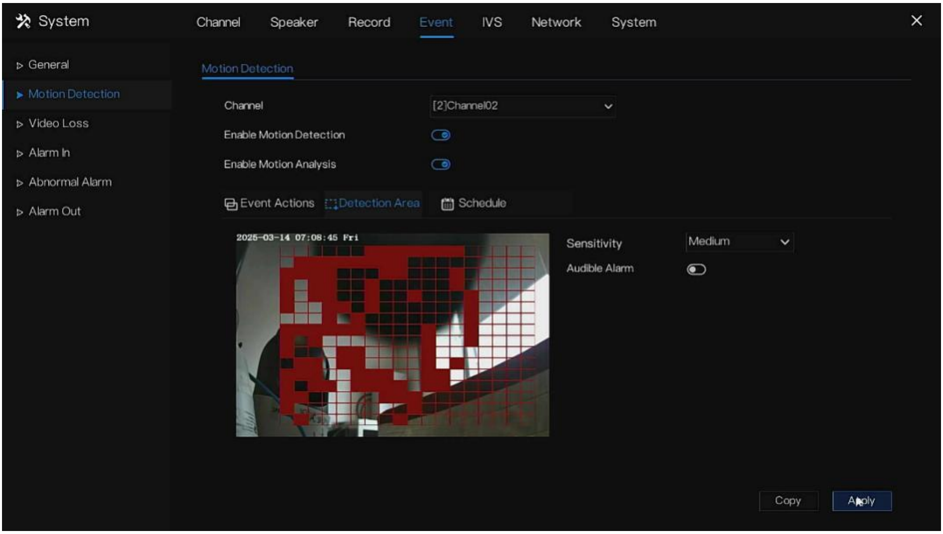
Full Screen ○

Parameter	Description
Push Message to app	When motion is triggered, you will receive a notification via the mobile app.
Email	When a motion is triggered, a notification will be sent to a designated email address. Note: Email settings must be configured under Network settings (see section *6.6.5 Email*) before enabling this option.
Buzzer	When motion is triggered, a buzzer will sound.
Enable Event Recording	When motion is triggered, enable to record when the alarm is occurred. Post-record(sec): choose the duration of other channels to record the alarm video. Recording channel: choose the channels to record.
FTP	When motion is triggered, a snapshot will be saved via FTP. Note: FTP settings must be configured under Recording settings (see section *6.3.7 FTP*) before enabling this option.
PTZ	When motion is triggered a designated PTZ camera will execute a designated preset function. Note the preset operation must be configured in the PTZ camera settings (it will be related to the PTZ camera's preset) before enabling this option. Supporting camera required.
Enable Alarm Out	When motion is triggered, it will enable the alarm out port of the rear panel.
Enable Camera Alarm Out	When motion is triggered, enable to linkage of the alarm out port of the camera.
Full Screen	When motion is triggered the live view from the DVR will display the camera in full screen.
Speaker	When motion is triggered, it will enable the speaker to play the

	set audio file by the chosen broadcast point.  Speaker Broadcast Point 32 Audio Files Dangerous area. Keep away.wav

Step 5 Click the Area page to access the motion detection area setting, as shown in Figure 6-42.

Figure 6-42 Motion detection area setting screen



Channel [2]Channel02

Enable Motion Detection

Enable Motion Analysis

Sensitivity Medium

Audible Alarm

Area :

1. Hold down and drag the left mouse button to draw a motion detection area. You can configure several regions. Hold down and drag the left mouse button to draw a motion detection area; the default area is **full screen**.
2. Drag on the screen to select the region that you want to detect. When any of the several regions activates the motion detect alarm, the channel where this region belongs will activate the motion detect alarm.
3. Select a value from the drop-down list next to **Sensitivity**. **Sensitivity**: four levels can be chosen – **Low, Medium, High, and Highest** – but it is not consistent with IPC. The higher the chosen is, the easier the alarms can be activated.
4. If the camera has a **built-in speaker**, you can enable the audio alarm. If the camera has a **flashlight**, you can enable the flashlight alarm.

Step 6 Click the **Schedule** page to access the schedule screen. For details, please refer to section

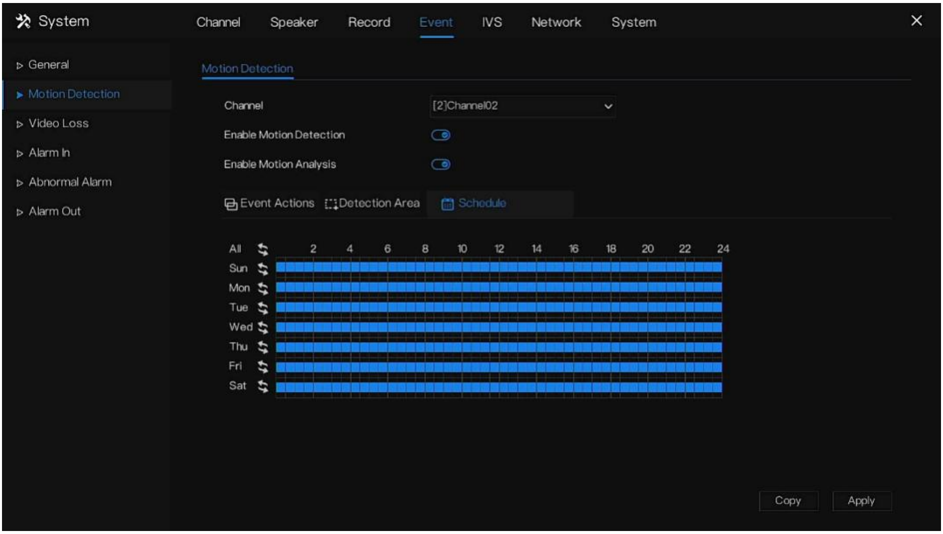
6.3.1 Record Schedule.

Step 7 Click Copy and select channels or tick **all**, then click OK to apply the motion detection settings to cameras in selected channels, and click Apply to save motion detection alarm settings.

NOTE

- Double-click to delete the selected area.
- The default area is the whole area.
- If you leave the page without applying, the tip "Do you want to save?" will show. Click Save to save the settings. Click Cancel to quit the settings.
- To enable the alarm out, users need to set alarm time and output ID, four IDs corresponding to the back panel's alarm out, 1 A and 1 B, 2 A and 2 B, 3 A and 3 B, 4 A and 4 B.
- The channel alarm out corresponds to the alarm port of the camera.

Figure 6-43 Alarm schedule



Channel: [2]Channel02

Enable Motion Detection: ●

Enable Motion Analysis: ●

----End

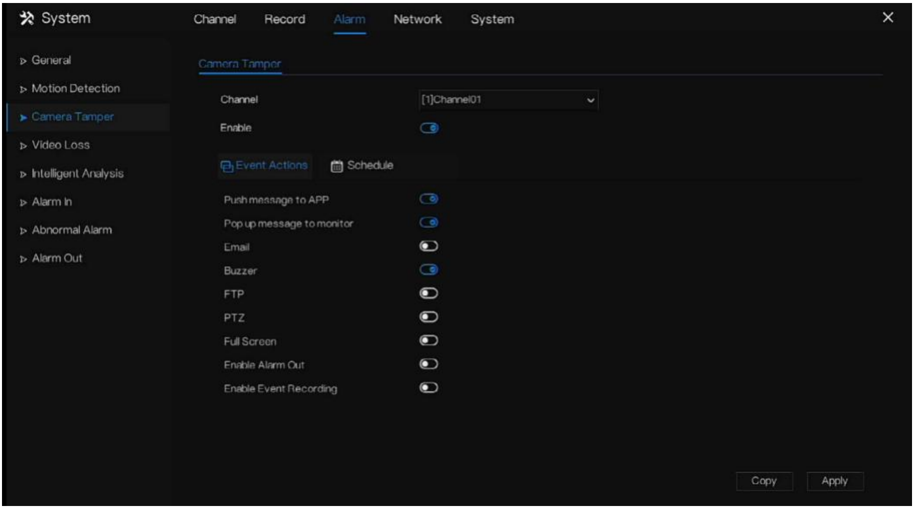
6.4.3 Video Tamper

The camera is blocked by something, and live video cannot clearly monitor the scene, that will trigger video tamper alarm.

Operation Description

Click **Video Tamper** in the main menu or menu of the alarm management screen and choose **Video Tamper** to access the video loss screen, as shown in Figure 6-44.

Figure 6-44 Camera Tamper screen



Channel	[1]Channel01
Enable	●
Push message to APP	●
Pop up message to monitor	●
Email	○
Buzzer	●
FTP	○
PTZ	○
Full Screen	○
Enable Alarm Out	○
Enable Event Recording	○

Operation Steps

Step 1 Navigate to **Settings > Event** > **Video tamper**

Step 2 Select a channel from the drop-down list of channel.

Step 3 Click ○ to enable camera tamper alarm.

Step 4 Enable the Event actions including: **Push message to App, Email, Buzzer, Enable event recording, FTP, PTZ, Enable alarm out, Full screen,** and **Speaker**.

Step 5 Click Schedule page to access the schedule screen.

Step 6 For details, please refer to *6.3.1 Record Schedule Tick to choose mainstream* or substream to record.

Step 7 Set the record schedule.

Step 8 Click Copy and select a channel, then click OK to apply the parameter settings to cameras in selected channels, click Apply to save video loss settings.

---End

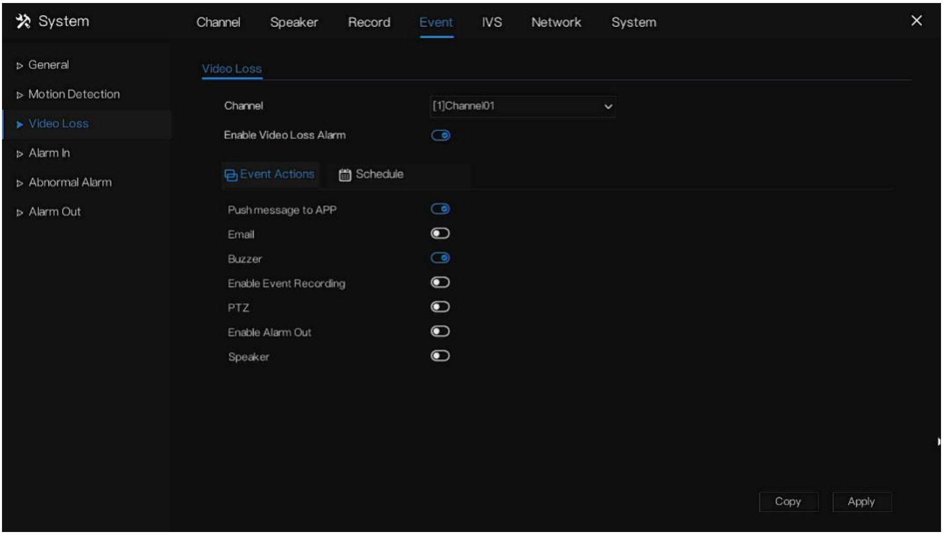
6.4.4 Video Loss

If a camera is **disconnected** from the DVR, it will trigger a video loss alarm.

Operation Description

Navigate to **Settings > Event** > **Video Loss** as shown in Figure 6-45.

Figure 6-45 Video loss screen



Channel [1]Channel01

Enable Video Loss Alarm ●

Push message to APP ●

Email ○

Buzzer ●

Enable Event Recording ○

PTZ ○

Enable Alarm Out ○

Speaker ○

Operation Steps

Step 1 Select a channel from the drop-down list of channels.

Step 2 Click ○ to enable the video loss alarm.

Step 3 Enable the Event Actions including **Push Messages to App, Email, Buzzer, Enable Event Recording, PTZ, Enable Alarm Out, Speaker,** and so on.

Step 4 Click the **Schedule** to access the schedule screen. For details, please refer to the section ***6.3.1 Record Schedule***.

Step 5 Click Copy and select a channel, then click OK to apply the parameter settings to cameras in selected channels, and click Apply to save video loss settings.

----End

6.4.5 Alarm In

NOTE

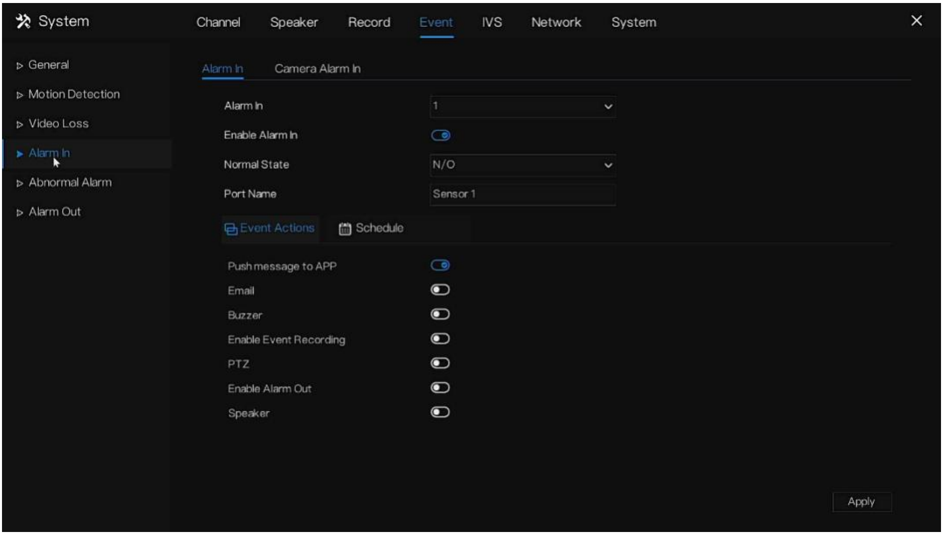
This function requires that the device be connected to an external alarm.

There are two types of alarm: one is the **DVR's alarm**, and the other is the **camera channel's alarm**.

Operation Description

Navigate to **Settings > Event > Alarm In** as shown in Figure 6-46.

Figure 6-46 Alarm in screen



Alarm In: 1

Enable Alarm In: ●

Normal State: N/O

Port Name: Sensor 1

Push message to APP: ●

Email: ○

Buzzer: ○

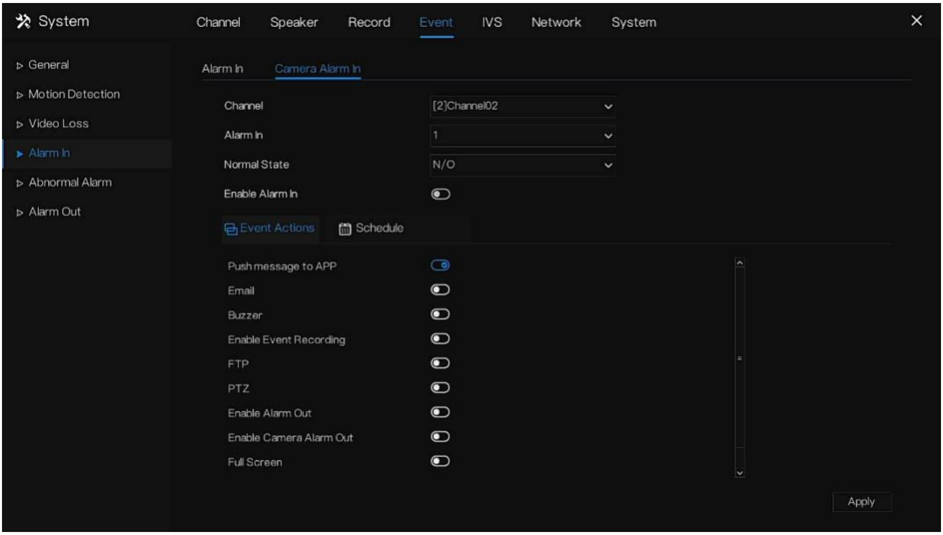
Enable Event Recording: ○

PTZ: ○

Enable Alarm Out: ○

Speaker: ○

Figure 6-47 Camera alarm in



Channel: [2]Channel02

Alarm In: 1

Normal State: N/O

Enable Alarm In: ○

Push message to APP: ●

Email: ○

Buzzer: ○

Enable Event Recording: ○

FTP: ○

PTZ: ○

Enable Alarm Out: ○

Enable Camera Alarm Out: ○

Full Screen: ○

Operation Steps

Step 1 Navigate to **Settings > Event > Alarm In** > **Camera Alarm In**

Step 2 Select a channel in **Alarm In**.

Step 3 Click ○ to enable or disable the functions.

Step 4 Select the **Alarm Type** from the drop-down list.

NOTE

- **NC:** Normal Close Alarm
- **NO:** Normal Open Alarm

Step 5 Set a **Name**.

Step 6 Enable the event actions including **Push message to App, Email, Buzzer, Enable Event Recording, PTZ, Enable Alarm Out, Speaker,** and so on. For the detailed operation, please refer to ***section 6.4.2 Motion Detection***.

Step 7 Click the **Schedule** page to access the schedule screen. For details, please refer to s**ection *6.3.1 Record Schedule.***

Step 8 Click Apply to save the settings of **Alarm In**.

----End

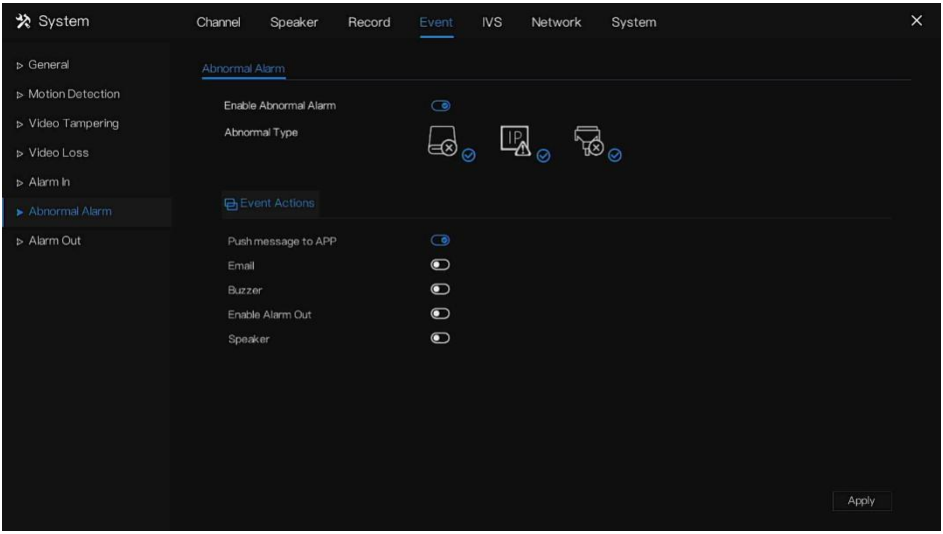
6.4.6 Abnormal Alarm

Abnormal alarms include **Disk Alarms**, **IP Conflicts** and **Network Disconnected.**

Operation Description

Step 1 Navigate to **Settings > Event > Abnormal Alarm** as shown in Figure 6-48.

Figure 6-48 Abnormal alarm screen



Enable Abnormal Alarm ●

Abnormal Type ✓ ✓ ✓

Push message to APP ●

Email ○

Buzzer ○

Enable Alarm Out ○

Speaker ○

Step 2 Tick the abnormal actions.

Step 3 Enable the event actions to include: **Push Message to App, Email, Buzzer, Enable Alarm Out, Speaker**, and so on. For the detailed operation, please refer to ***section 6.4.2 Motion Detection*.**

Step 4 Click Apply to save abnormal alarm settings.

----End

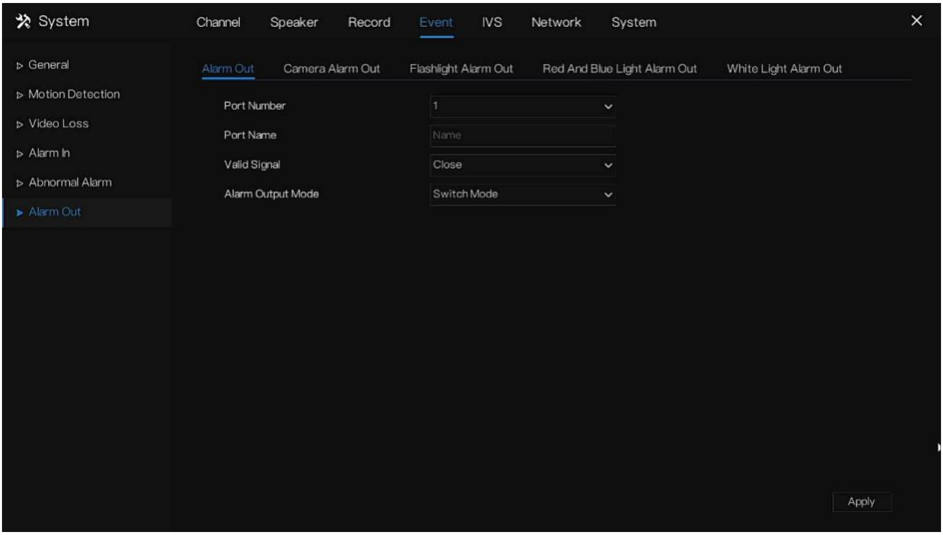
6.4.7 Alarm Out

6.4.7.1 Alarm Out

1. Navigate to **Settings > Event > Alarm out**
2. Choose one Output ID as the output interface.

3. Click Apply to save abnormal alarm settings.

Figure 6-49 Alarm out



Port Number: 1
Port Name: Name
Valid Signal: Close
Alarm Output Mode: Switch Mode

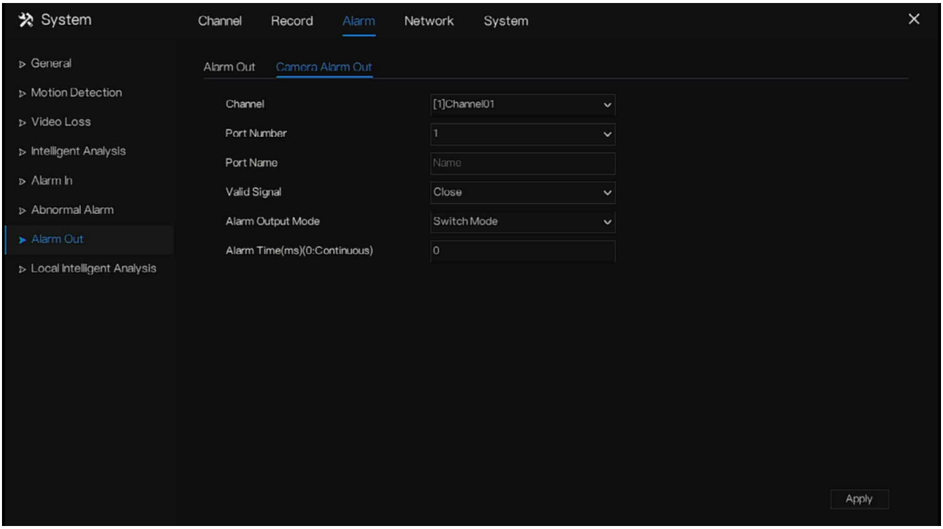
----End

6.4.7.2 Camera Alarm out

NOTE

This function requires access to a camera that is connected to an external alarm-out device.

Figure 6-50 Camera alarm out



Channel: [1]Channel01

Port Number: 1

Port Name: Name

Valid Signal: Close

Alarm Output Mode: Switch Mode

Alarm Time(ms)(0:Continuous): 0

Table 6-6 Camera alarm out

Parameter	Description	Setting
Alarm Output	ID of the alarm output channel. NOTE The number of alarm output channels depends on the device model.	[Setting method] Select a value from the drop-down list box. [Default value] 1
Name	Alarm output channel name.	[Value range] 0 to 32 bytes
Valid Signal	The options are as follows: ● **Close**: An alarm is generated when an external alarm signal is received. ● **Open**: An alarm is generated when no external alarm signal is received.	[Setting method] Select a value from the drop-down list box. [Default value] Close

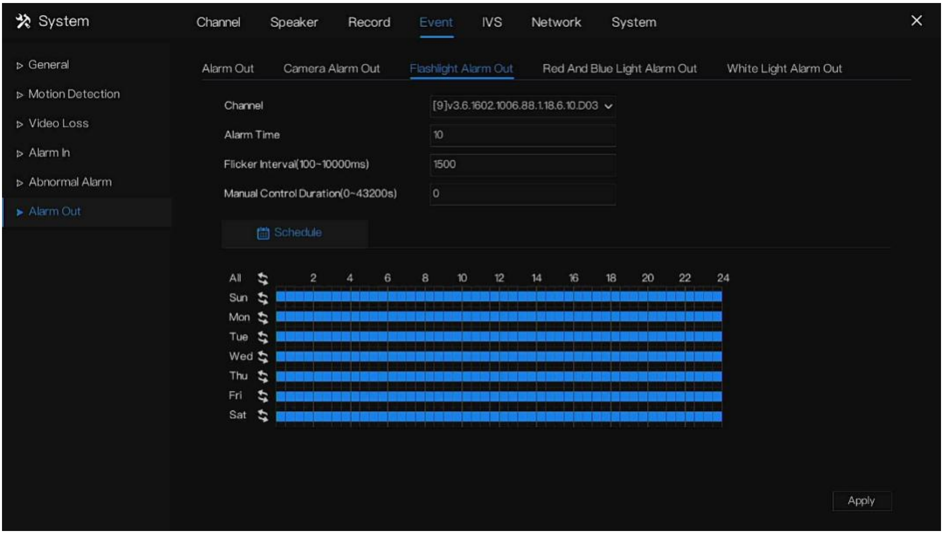
Parameter	Description	Setting
Alarm Output Mode	When the device receives I/O alarm signals, it will send the alarm information to an external alarm device in the mode specified by this parameter. The options include the switch mode and pulse mode. NOTE ● If the switch mode is used, the alarm frequency of the device must be the same as that of the external alarm device. ● If the pulse mode is used, the alarm frequency of the external alarm device can be configured.	[Setting method] Select a value from the drop-down list box. [Default value] Switch Mode
Alarm Time(ms) (0: Continuous)	Alarm output duration. The value **0** indicates that the alarm remains continuously valid.	[Setting method] Enter a value manually. [Default value] 0 [Value range] 0 to 86400 seconds
Manual Control	Control the alarm output.	N/A

----End

6.4.7.3 Light Alarm Out

For the camera with the light (flashlight, red and blue light, or white light), you can set the alarm settings as shown in the figures.

Figure 6-51 Flashlight alarm out



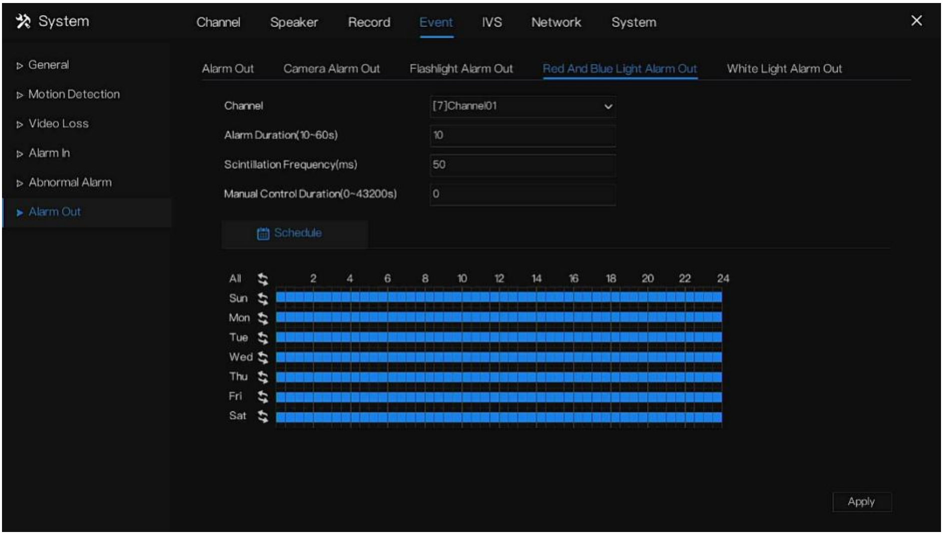
Channel [9]v3.6.1602.1006.88.1.18.6.10.D03

Alarm Time 10

Flicker Interval(100~10000ms) 1500

Manual Control Duration(0~43200s) 0

Figure 6-52 Red and blue light Light alarm out



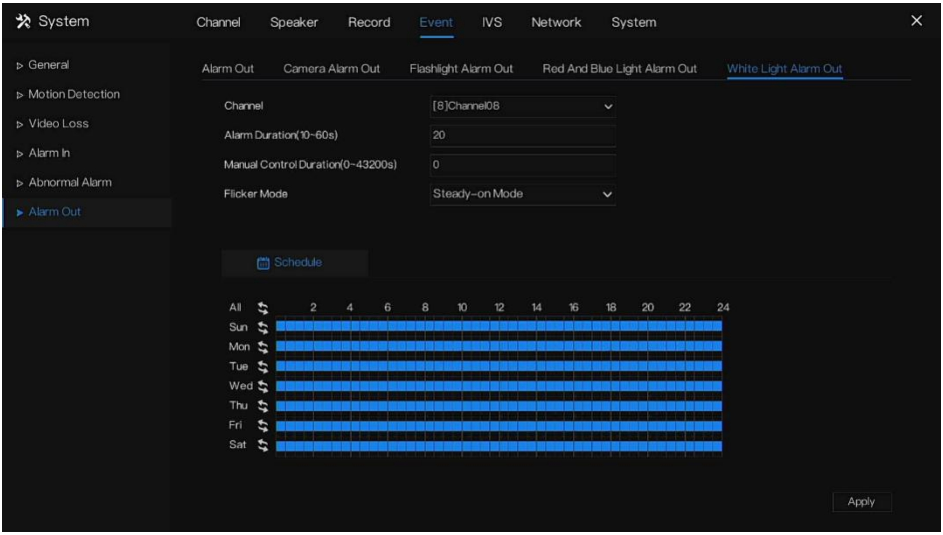
Channel [7]Channel01

Alarm Duration(10~60s) 10

Scintillation Frequency(ms) 50

Manual Control Duration(0~43200s) 0

Figure 6-53 White light alarm out



Channel: [8]Channel08

Alarm Duration(10~60s): 20

Manual Control Duration(0~43200s): 0

Flicker Mode: Steady-on Mode

Table 6-7 Camera alarm out

Parameter	Description	Setting
Channel	Choose one channel with light to set.	[Setting method] Select a channel from the drop-down list box.
Alarm Time	For flashlight cameras, When the alarm is triggered, the light will last for the set time.	[Setting method] Enter a value manually.
Flicker interval(100-10000ms)	For flashlight cameras, set the flicker interval of the flashlight.	[Setting method] Enter a value manually.
Alarm Duration(10-60s)	The light alarm will be duration.	[Value range] 10 to 60s
Scintillation frequency (ms)	For red and blue light cameras, set the scintillate frequency of the red and blue light.	[Setting method] Enter a value manually.

Parameter	Description	Setting
Manual Control Duration (0-43200s)	When the user manually opens the light, it will last for the set time.	[Setting method] Enter a value manually.
Flicker Mode	The white light has two modes of flicker: flicker mode and steady-on mode. The flicker mode means the light is flashing. The steady-on mode means the light is always on.	[Setting method] Select one from the drop-down list box.

6.5 IVS Configuration

Set the **Intelligent Analysis, ES Analysis (Environmental Safety),** and **Local Intelligent Analysis** in the IVS (Intelligent Video System) screen.

6.5.1 Intelligent Analysis (Only for Some Models)

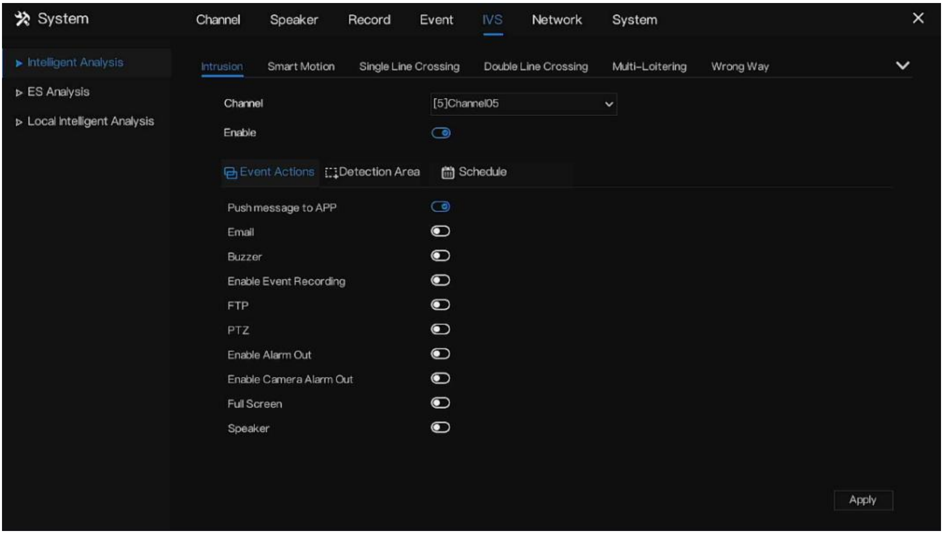
NOTE

The channel camera can set the Intelligent Analysis, which is dependent on the performance of the cameras.

Operation Description

Step 1 Navigate to **Settings > IVS > Intelligent Analysis** as shown in Figure 6-54.

Figure 6-54 Intelligent Analysis screen



Channel [5]Channel05

Enable

Push message to APP

Email

Buzzer

Enable Event Recording

FTP

PTZ

Enable Alarm Out

Enable Camera Alarm Out

Full Screen

Speaker

Step 2 Select one action to set the alarm. (**Intrusion, Smart Motion, Single Line Crossing, Double Line Crossing, Multi-loitering, Wrong Way, People Counting**).

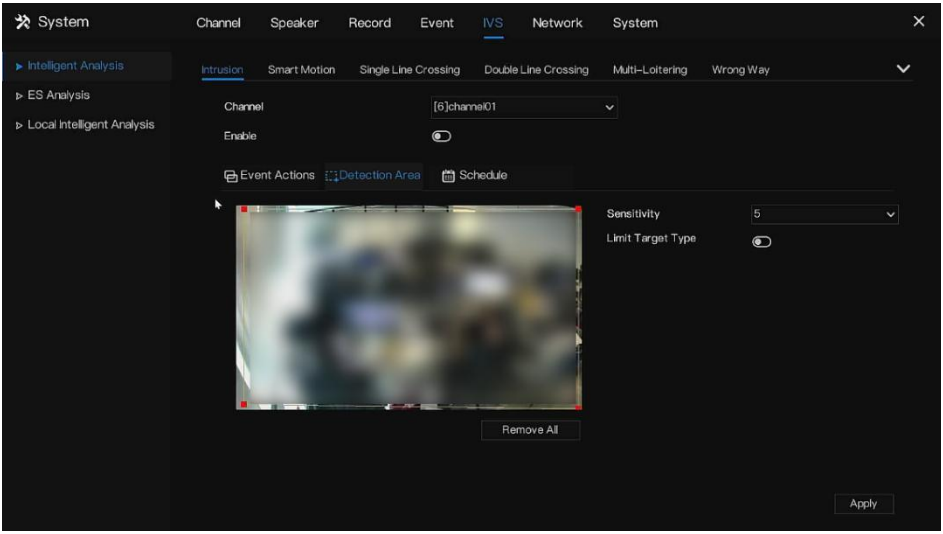
Step 3 Select a channel from the drop-down list of channels.

Step 4 Click to enable the intelligent analysis alarm.

Step 5 Enable the event actions including **Push Message to App**, **Pop-up Message to Monitor**, **Send Email**, **Buzzer**, **FTP**, **PTZ**, **Full Screen**, **Alarm Out**, **Camera Alarm Out**, **Event Recordings**, and so on. For the detailed operation, please refer to ***section 6.4.2 Motion Detection*.**

Step 6 Click the Detection Area page to set the detection area. Use the mouse to draw the polygonal region to deploy.

Figure 6-55 Detection area



System

Channel Speaker Record Event IVS Network System

- Intelligent Analysis
- ES Analysis
- Local Intelligent Analysis

Intrusion Smart Motion Single Line Crossing Double Line Crossing Multi-Loitering Wrong Way

Channel [6]channel01

Enable

Event Actions Detection Area Schedule

Sensitivity 5

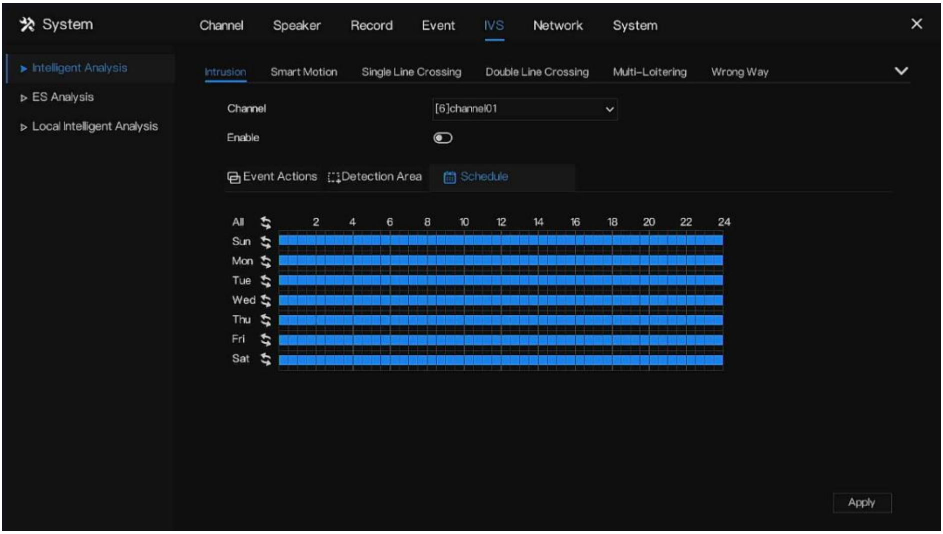
Limit Target Type

Remove All

Apply

Step 7 Click the Schedule page to access the schedule screen. For details, please refer to section *6.3.1 Record Schedule.*

Figure 6-56 Set schedule



System

Channel Speaker Record Event IVS Network System

- Intelligent Analysis
- ES Analysis
- Local Intelligent Analysis

Intrusion Smart Motion Single Line Crossing Double Line Crossing Multi-Loitering Wrong Way

Channel [6]channel01

Enable

Event Actions Detection Area Schedule

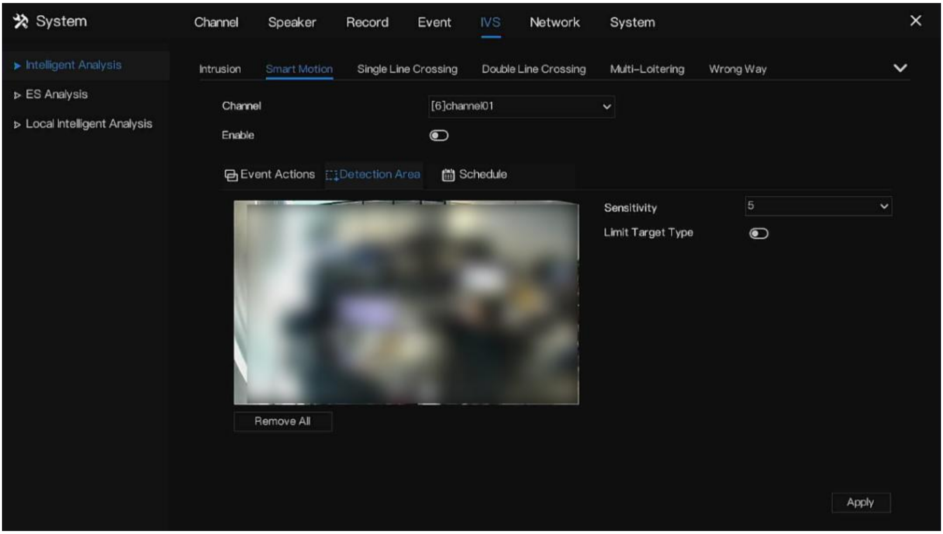
Apply

Step 8 Click Apply to save the settings.

6.5.1.2 Smart Motion

If the AI multi-object cameras are connected to the DVR, users can set the limit target (person or car) to be detected.

Figure 6-57 Smart Motion



Channel: [6]channel01
Enable
Sensitivity: 5
Limit Target Type

Step 1 Select a channel from the drop-down list of channels.

Step 2 Click ● to enable smart motion.

Step 3 Enable some event actions. For the detailed operation, please refer to *section 6.4.2 Motion Detection.*

Step 4 Set the detection area.

Move the cursor to the drawing interface and click to generate a point. Move the cursor to draw a line, and then click to generate another point. This is how a line is generated. In this way, continue to draw lines to form any shape, and right-click to finish the drawing.

Step 5 Choose the sensitivity, and enable the limit target type.

Table 6-8 Smart motion area

Parameter	Description
Sensitivity	Every region of every channel has an individual sensitivity value. The range is 0-100. The bigger the value is, the easier the alarms can be activated.

Parameter	Description
Type	Person: only detects people Vehicle: only detects cars Person or vehicle: detects person and car at the same time

Step 6 Click Apply to save settings.

----End

6.5.2 ES Analysis

On the Environmental Safety Analysis interface, users can set the parameters of smoking detection, smoke and flame detection, and fire spot detection. Enable the linkage actions; the alarm information can be sent to the user by the linkage.

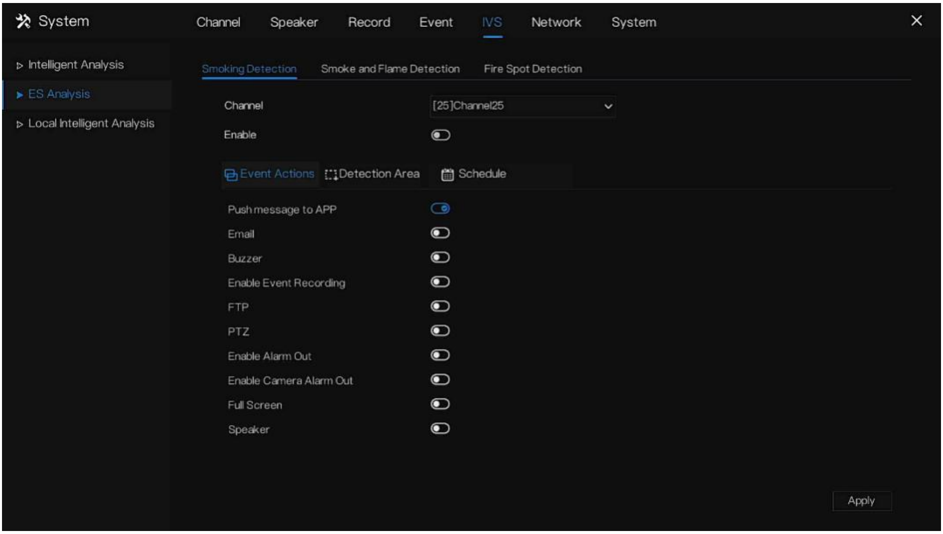
6.5.2.1 Smoking Detection

Smoking detection functionality is widely used in areas where smoking is prohibited, assisting managers in real-time monitoring of smoking behaviors to ensure safety and compliance. Through automatic alerts or recordings, it can effectively reduce health issues, safety risks, and violations caused by smoking.

Step 1 Navigate to **Settings** > **IVS** > **ES Analysis** > **Smoking**, as shown in Figure 6-58.

Step 2 Choose the thermal camera to enable smoking detection.

Figure 6-58 Smoking detection



Channel [25]Channel25

Enable ○

Push message to APP ●

Email ○

Buzzer ○

Enable Event Recording ○

FTP ○

PTZ ○

Enable Alarm Out ○

Enable Camera Alarm Out ○

Full Screen ○

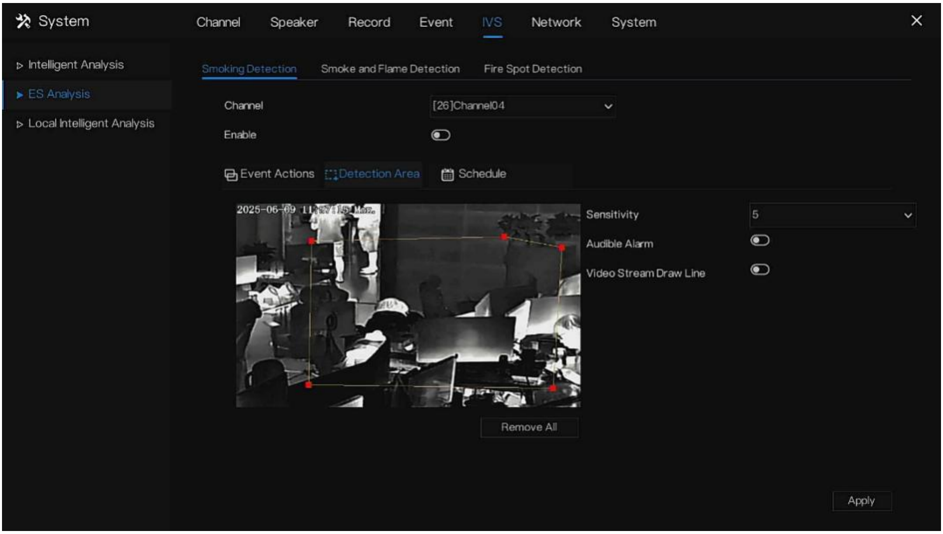
Speaker ○

Step 3 Enable the event actions.

Step 4 Set the detection areas. Use the mouse to draw the area.

Step 5 For different cameras, you can choose to enable the audible alarm, flashlight alarm, or video stream draw line.

Figure 6-59 Smoking - Detection area



System

Channel Speaker Record Event IVS Network System

Intelligent Analysis
ES Analysis
Local Intelligent Analysis

Smoking Detection Smoke and Flame Detection Fire Spot Detection

Channel: [26]Channel04

Enable

Event Actions Detection Area Schedule

2025-06-09

Sensitivity: 5

Audible Alarm

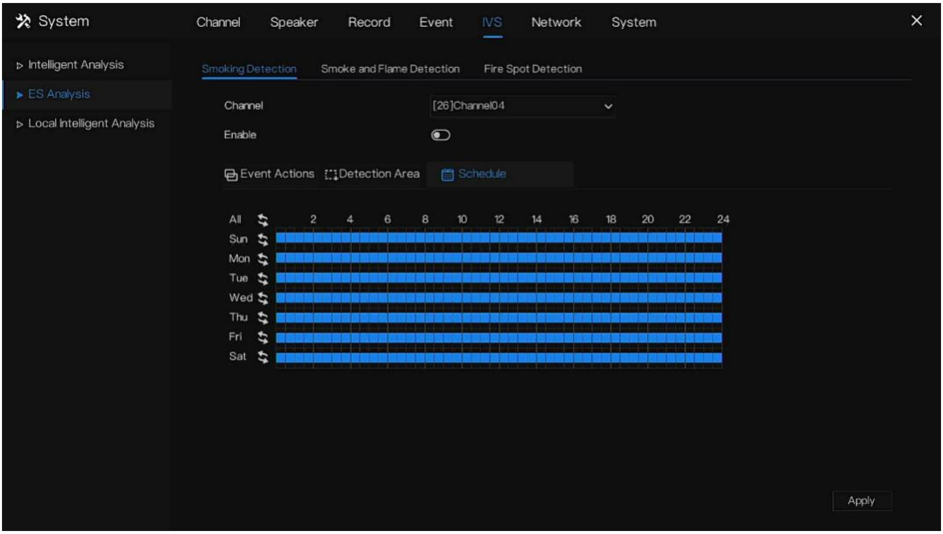
Video Stream Draw Line

Remove All

Apply

Step 6 Set the schedule to arm.

Figure 6-60 Smoking – Schedule



System

Channel Speaker Record Event IVS Network System

Intelligent Analysis
ES Analysis
Local Intelligent Analysis

Smoking Detection Smoke and Flame Detection Fire Spot Detection

Channel: [26]Channel04

Enable

Event Actions Detection Area Schedule

Step 7 Click Apply. The message "Apply success!" is displayed, and the system will save the settings

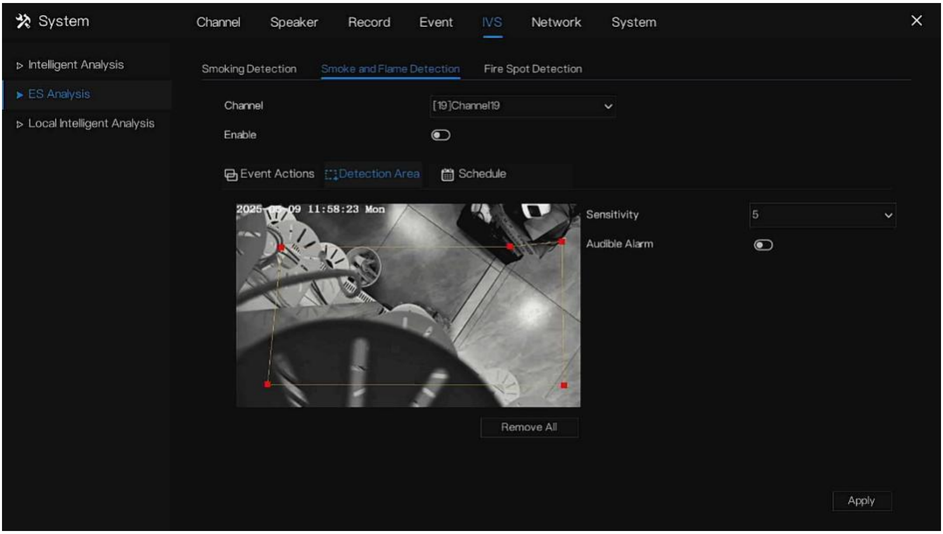
----End

6.5.2.2 Smoke and Flame Detection

The Smoke and Flame Detection function refers to that an alarm is generated when something is smoking or generating flame at the deployment area.

1. Navigate to **Settings > IVS > ES Analysis > Smoke and Flame Detection** as shown in Figure 6-61.

Figure 6-61 Smoke and flame detection



Channel: [19]Channel19
Enable
Sensitivity: 5
Audible Alarm

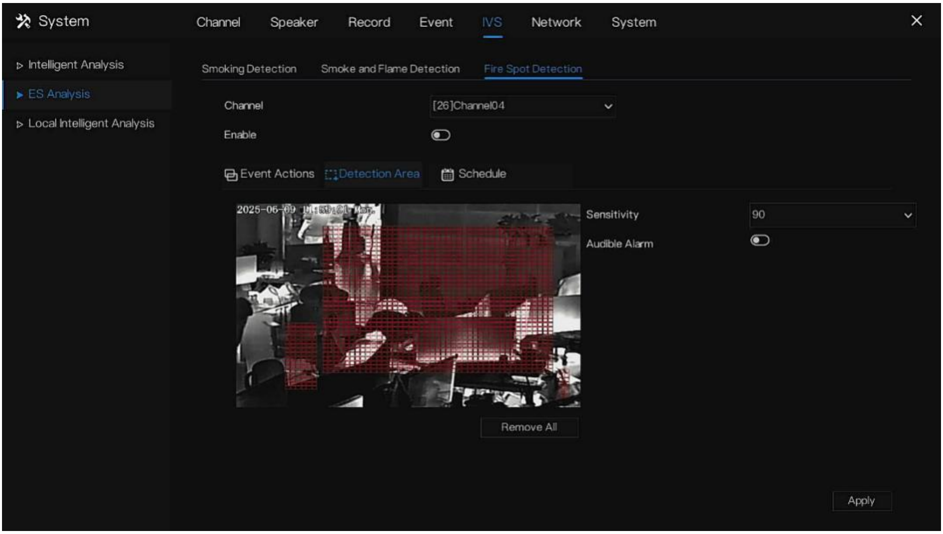
2. For the detailed settings, please refer to ***Chapter 6.5.2.1 Smoking Detection***.

6.5.2.3 Fire Spot Detection

The Fire Spot Detection function is when an alarm is generated when something is on fire at the deployment area.

Navigate to **Settings > IVS > ES Analysis > Fire Spot Detection** as shown in Figure 6-62.

Figure 6-62 Fire spot detection



Channel: [26]Channel04

Enable

Sensitivity: 90

Audible Alarm

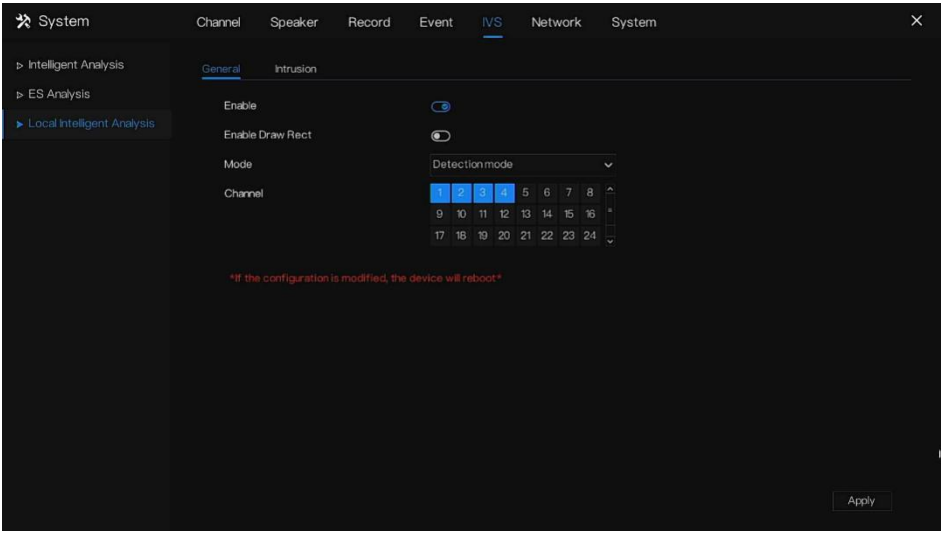
For the detailed settings, please refer to *Chapter 6.5.2.1 Smoking Detection*.

6.5.3 Local Intelligent Analysis

6.5.3.1 General

1. Navigate to **Settings > IVS** > **Local Intelligent Analysis > General** as shown in Figure 6-63.

Figure 6-63 Local intelligent analysis – General



Enable ●
Enable Draw Rect ○
Mode: Detection mode
Channel: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

If the configuration is modified, the device will reboot

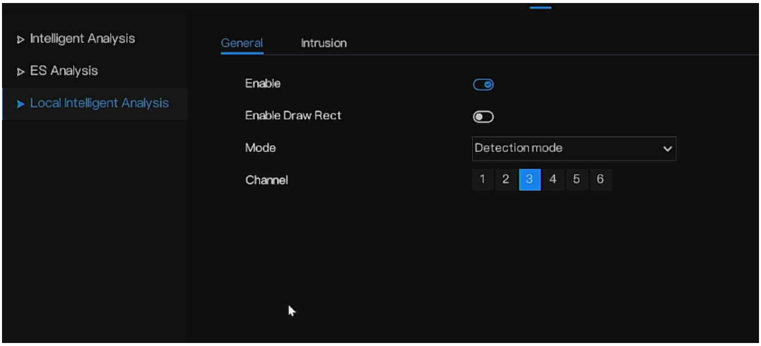
2. Enable the alarm function.
3. Enable Draw Rectangle, and the detection rectangle will be shown on the live video of the intrusion.
4. Choose the channels; up to 4 channels can be chosen.

NOTE

- Only the analog cameras support this function.

6.5.3.2 Intrusion

Navigate to **Settings** > **IVS** > **Local Intelligent Analysis** > **Intrusion**. In general, the mode should be **Detection Mode**.



Enable: on

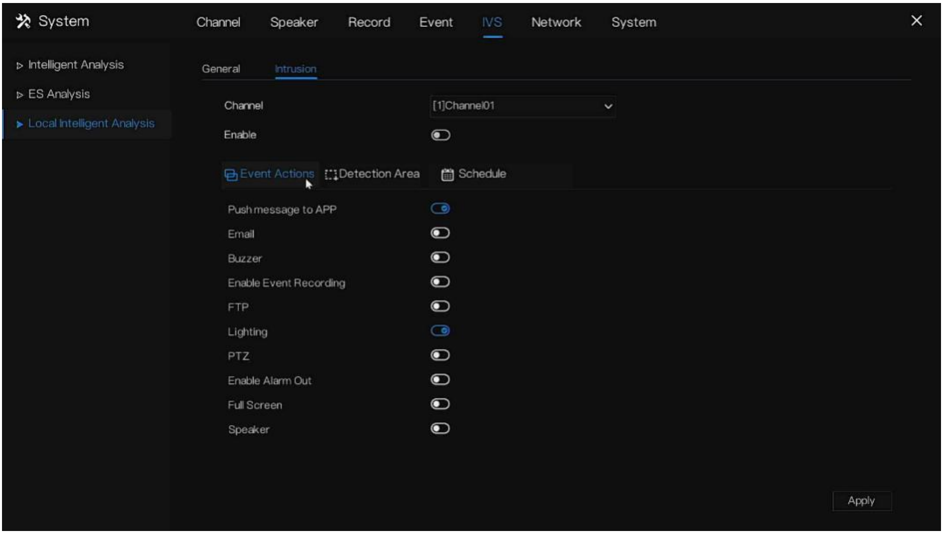
Enable Draw Rect: off

Mode: Detection mode

Channel: 1 2 3 4 5 6

Intrusion refers to an alarm generated when the targets of specified types (such as **person, vehicle , and both person and vehicle**) enter the detection area. It is the intrusion of the DVR, not related to the cameras. It is the algorithm of the DVR, and the DVR analyzes the data coming from the cameras.

Figure 6-64 Intrusion



Channel: [1]Channel01

Enable: off

Push message to APP: on

Email: off

Buzzer: off

Enable Event Recording: off

FTP: off

Lighting: on

PTZ: off

Enable Alarm Out: off

Full Screen: off

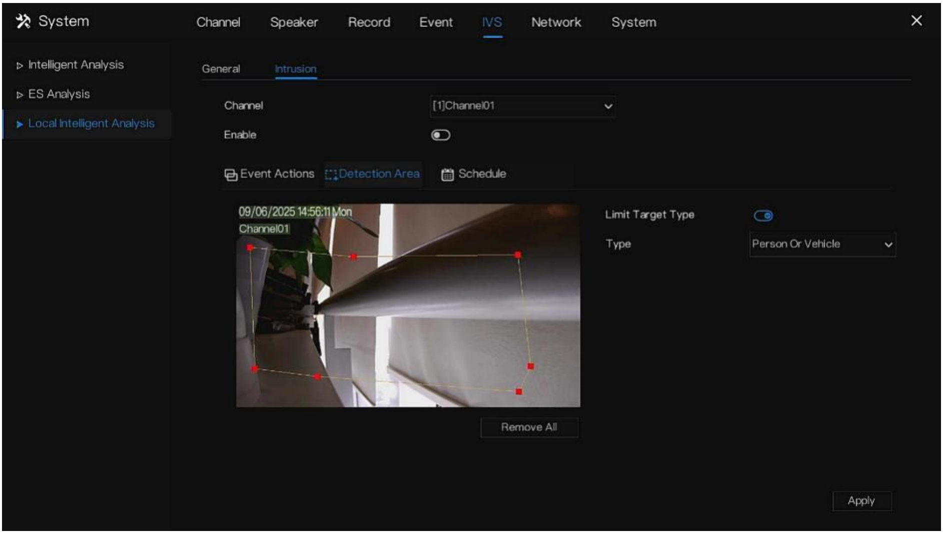
Speaker: off

Event action：

Choose the channel to enable the intrusion, and enable the event actions (such as Push message to App, Pop-up Message to Monitor, Email, Buzzer, FTP, PTZ, Full Screen, Alarm Out, Camera Alarm out, Event Recording, and so on). For the detailed operation, please refer to *section 6.4.2 Motion Detection*.

Click “Apply” to save the settings.

Figure 6-65 Detection area



Channel [1]Channel01

Enable

Limit Target Type

Type Person Or Vehicle

Detection area:

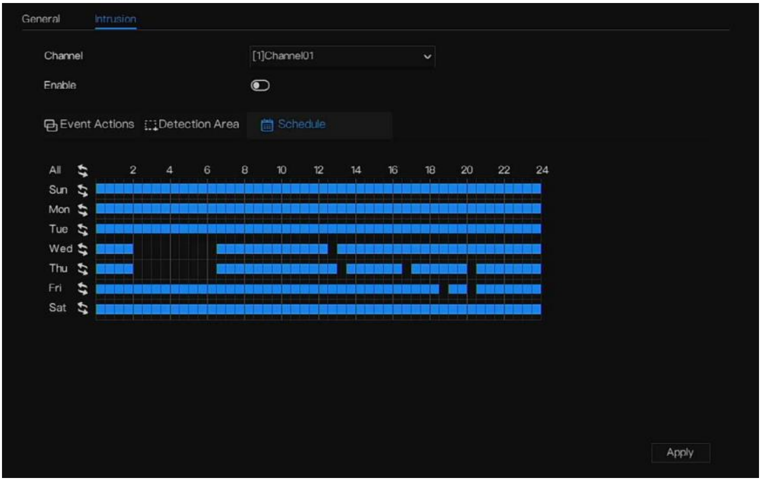
Move the cursor to the drawing interface and click to generate a point, move the cursor to draw a line, and then click to generate another point. This is how a line is generated. In this way, continue to draw lines to form any shape, and right-click to finish the drawing.

NOTE

- A drawn line cannot cross another one, or the line drawing fails.
- Any shape with 8 sides at most can be drawn.
- The quantity of detection areas is not limited yet and will be described in the future when a limit is applied.

Choose a Limit Target from the drop-down list: person, person/ vehicle, or vehicle.

Figure 6-66 Set schedule



Set schedule:

Method 1： Click the left mouse button to select any time point within 0:00-24:00 from Monday to Sunday as shown in Figure 6-66.

Method 2： Hold down the left mouse button, drag, and release the mouse to select the schedule between 0:00 and 24:00 from Monday to Sunday.

NOTE

- When you select time by dragging the cursor, the cursor cannot be moved out of the time area. Otherwise, no time can be selected.

Method 3： Click ⟳ on the schedule page to select the whole day or whole week.

Deleting schedule: Click ⟳ again or inverse selection to delete the selected schedule.

----End

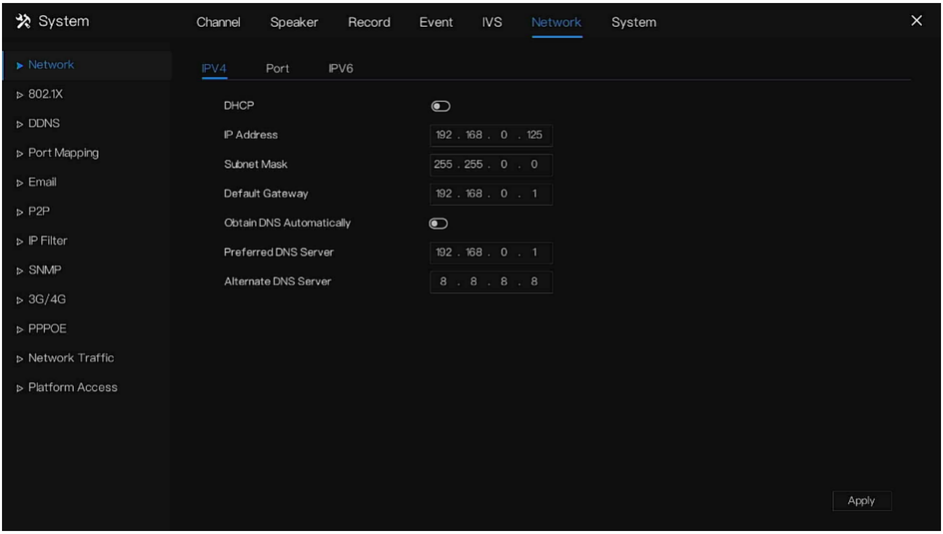
6.6 Network Management

Set the **Network Parameter, 802.1X, DDNS, E-mail, Port Mapping, P2P, IP Filter, SNMP 3G/4G, PPPOE,** and **Network Traffic** in the network management screen.

Operation Description

Step 1 Click **Network** on **Settings > Network** to access the network management screen, as shown in Figure 6-67.

Figure 6-67 Network management screen



DHCP
IP Address 192 . 168 . 0 . 125
Subnet Mask 255 . 255 . 0 . 0
Default Gateway 192 . 168 . 0 . 1
Obtain DNS Automatically
Preferred DNS Server 192 . 168 . 0 . 1
Alternate DNS Server 8 . 8 . 8 . 8

Table 6-9 Network

Parameter	Description
DHCP	Enable the DHCP function. The IP address, subnet mask, and default gateway are not available for configuration once DHCP is enabled. • If DHCP is effective, the obtained information will be displayed in the **IP Address** box, **Subnet Mask** box, and **Default Gateway** box. • If you want to manually configure the IP information, disable the DHCP function first. If the PPPoE connection is successful, the IP address, subnet mask, default gateway, and DHCP are not available for configuration.

Parameter	Description
IP Address	Enter the IP address and configure the corresponding subnet mask and default gateway. The IP address and default gateway must be in the same network segment.
Subnet Mask	
Default Gateway	
Obtain DNS automatically	Enable the function to get the DNS address automatically. If you learn about the local DNS server IP, you can input the preferred DNS server and alternate DNS server manually.
Preferred DNS	In the **Preferred DNS** box, enter the IP address of the DNS.
Alternate DNS	In the **Alternate DNS** box, enter the IP address of the alternate DNS.

6.6.1 Network

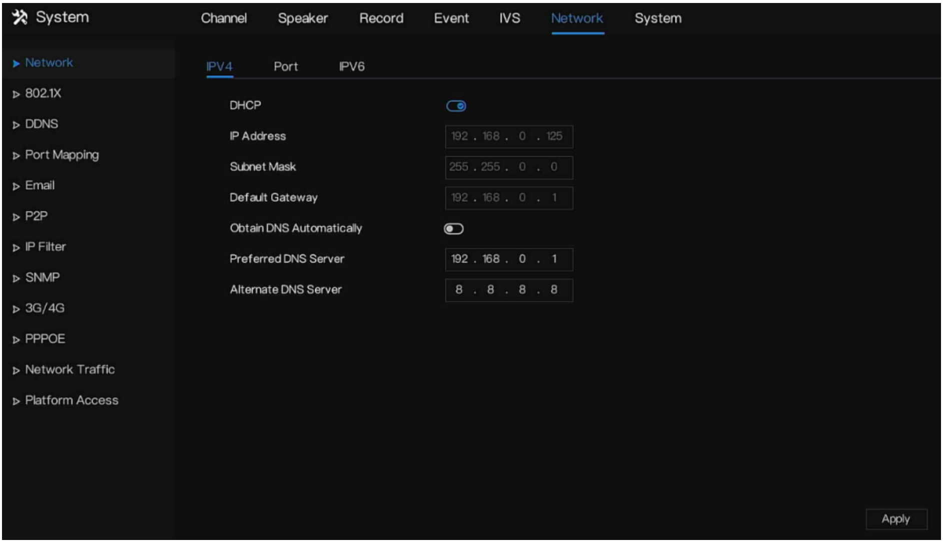
Set **DHCP and DNS** manually or automatically.

6.6.1.1 IPv4

Operation Steps

Step 1 Click ○ next to **DHCP** to enable or disable the function of automatically getting an IP address (the router where the DVR is connected should have the DHCP function, and the router distributes an IP to the DVR). The function is disabled by default.

Figure 6-68 Enable DHCP



DHCP
IP Address 192 . 168 . 0 . 125
Subnet Mask 255 . 255 . 0 . 0
Default Gateway 192 . 168 . 0 . 1
Obtain DNS Automatically
Preferred DNS Server 192 . 168 . 0 . 1
Alternate DNS Server 8 . 8 . 8 . 8

Step 2 If the function is disabled, click the input boxes next to **IP**, **Subnet Mask**, and **Gateway** to set the parameters as required. For the format, please refer to the router's network.

Step 3 Click next to **Obtain DNS Automatically** to enable or disable the function of automatically getting a DNS address. The function is enabled by default.

Step 4 If the function is disabled, click the input boxes next to **DNS 1 (default 192.168.0.1)** and **DNS 2 (default 8.8.8.8)**, delete the original address, and enter a new address.

Step 5 Click Apply to save IP settings.

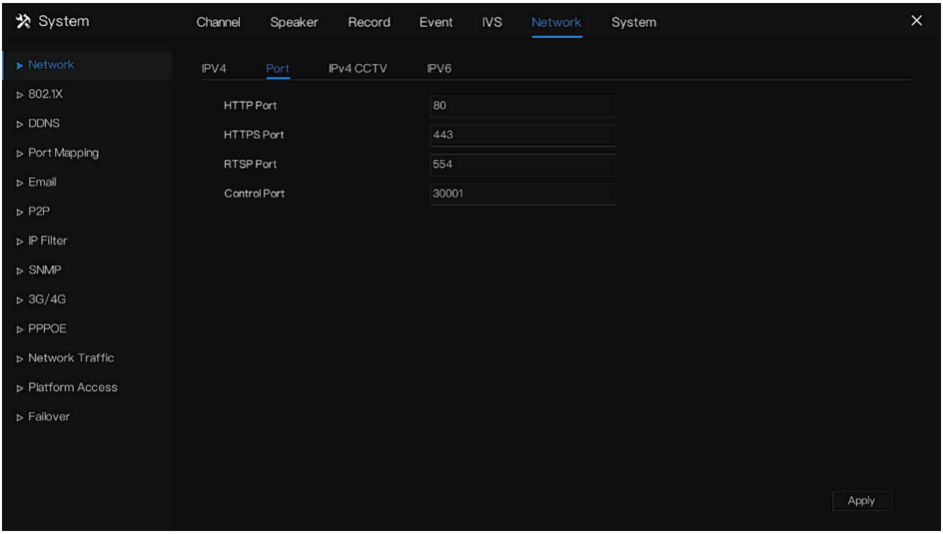
----End

6.6.1.2 Port

Operation Steps

Step 1 Click **the Port** page to access the port setting screen, as shown in Figure 6-69.

Figure 6-69 Port setting screen



HTTP Port 80

HTTPS Port 443

RTSP Port 554

Control Port 30001

Step 2 Set the HTTP port, HTTPS port, RTSP port, and Control port. If the users use these ports to log in, and the ports are changed, inputting the changed ports is necessary.

Table 6-10 Port

Parameter	Description
HTTP Port	The default value setting is 80. You can enter the value according to your actual situation. If you enter another value, for example, 8080, you should enter 8080 after the IP address when logging in to the device by browser. For example, http://192.168.0.121:8080.
HTTPS Port	HTTPS communication port. The default value setting is 443. You can enter the value according to your actual situation. For example, https://192.168.0.121:443.
RTSP Port	Real-Time Streaming Protocol. The default value setting is 554. You can select the value according to your actual situation. For example, rtsp://192.168.0.121:554/4/1.
Control port	The default value setting is 30413. You can enter the value according to your actual situation. When the DVR is connected to the APP Capture ADV or the platform Capture ADV CMS, the control port is necessary to input these systems.

Step 3 Click Apply to save port settings.

----End

6.6.1.3 IPv4CCTV (Only for Some Models)

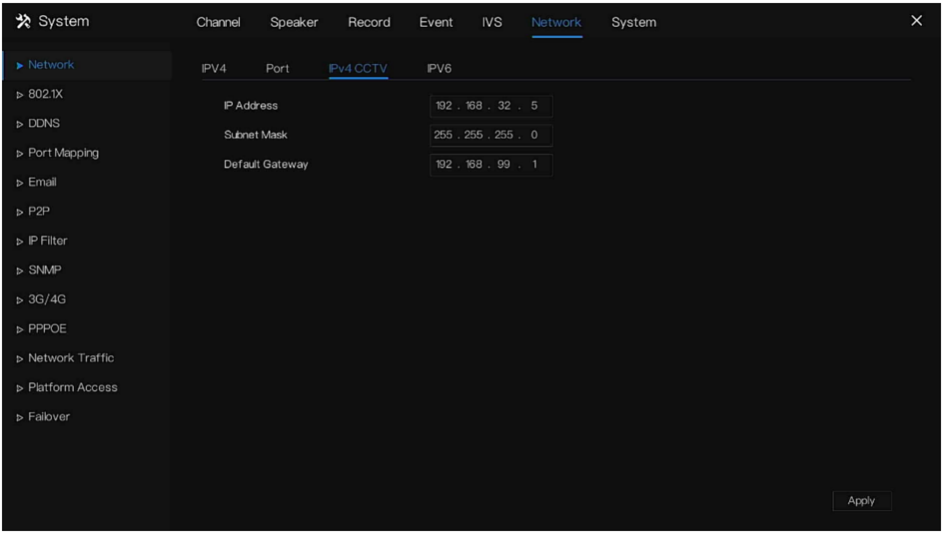
Some models have two network ports, WAN and LAN.

If the user connects to the DVR via the LAN port, they need to use the IPv4 address of the CCTV to access the DVR's web interface. This method is only for LAN access and does not support Internet access.

Operation Steps

Step 1 Click **the IPv4 CCTV** page to access the LAN setting screen, as shown in Figure 6-70.

Figure 6-70 IPv4 CCTV



IP Address 192 . 168 . 32 . 5

Subnet Mask 255 . 255 . 255 . 0

Default Gateway 192 . 168 . 99 . 1

Step 2 Input the IP address, subnet mask, and default gateway.

Step 3 Click Apply to save the settings.

NOTE

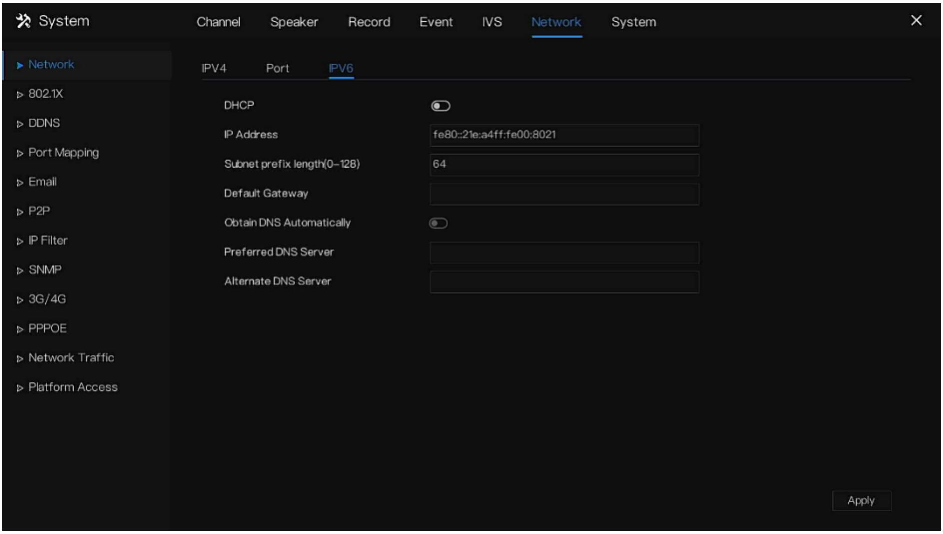
WAN and LAN can be connected to different networks so that DVR can add more cameras. WAN usually is connected to the external network to connect to the Internet; it is the default gateway. LAN connects to the internal network to add the cameras.

----End

6.6.1.4 IPV6

If the users' network router can be connected to IPv6, users can access the web through the IPv6 IP address.

Figure 6-71 IPV6



DHCP

IP Address: fe80::21e:a4ff:fe00:8021

Subnet prefix length(0–128): 64

Default Gateway:

Obtain DNS Automatically

Preferred DNS Server:

Alternate DNS Server:

The settings are the same as IPv4, but the input IP address is different; type as http://[fe80::21e:a4ff:fe00:6978]:port, the content of [] is IPv6 IP address, the port is the network port.

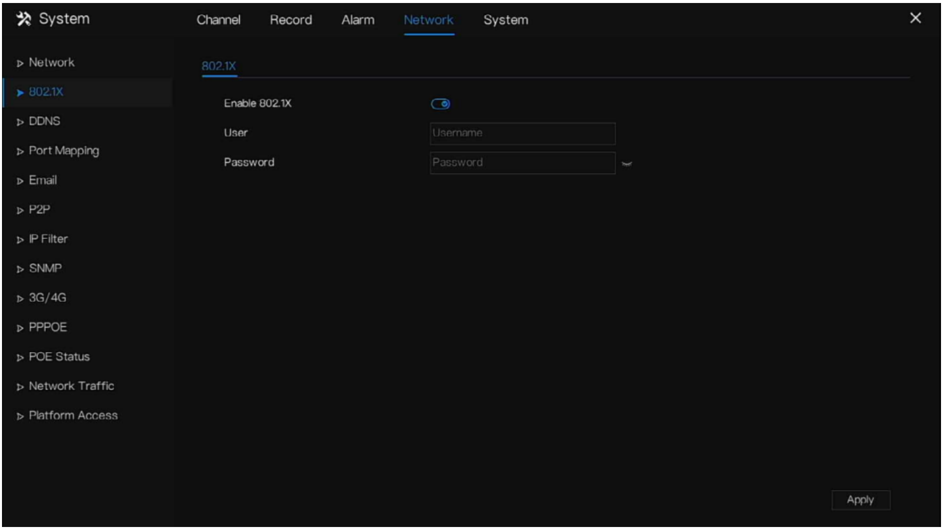
6.6.2 802.1 X

The 802.1X for DVR only offers the 802.1X interface and is the client-side; the users should provide the switch with the 802.1X function and **RADIUS** server configuration.

Operation Steps

Step 1 Click ○ next to **802.1 X** to enable or disable the function. The default is disabled.

Figure 6-72 802.1 X



Step 2 Input the user and password of 802.1X, the account is created by the user.

Step 3 Click Apply to save the settings. The visitor to view the DVR needs to input an account to certify.

----End

6.6.3 DDNS

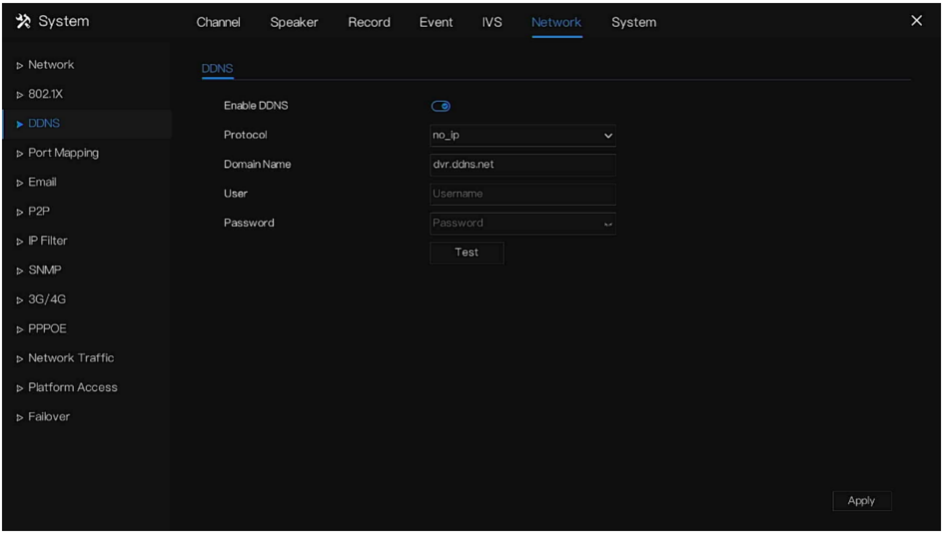
Please make sure to connect the specified camera to the Internet and obtain the user name and password for logging into the dynamic domain name system (DDNS) from the server.

Operation Steps

Step 1 Click **DDNS** on **Settings > Network** to access the DDNS screen.

Step 2 Click ○ next to **Enable** to enable the DDNS function. It is disabled by default, as shown in Figure 6-73.

Figure 6-73 DDNS setting screen



Enable DDNS

Protocol: no_ip

Domain Name: dvr.ddns.net

User: Username

Password: Password

Step 3 Select a required value from the protocol drop-down list.

Step 4 Set domain name, input user, and password.

Step 5 Click Test to check the domain name.

Step 6 Click Apply to save DDNS network settings.

NOTE

An external network can access the DVR via an address that is set in the DDNS settings.

----End

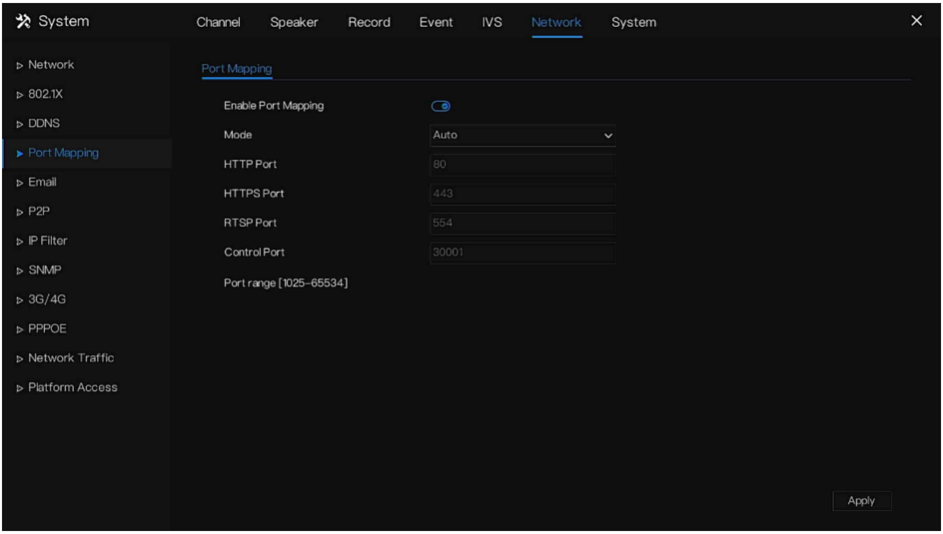
6.6.4 Port Mapping

Configure the port mapping, and you can access the DVR via the different ports.

Operation Steps

Step 1 Click **Port Mapping** on **Settings > Network** to access the port mapping screen, as shown in Figure 6-74.

Figure 6-74 Port mapping setting screen



Enable Port Mapping ●

Mode Auto

HTTP Port 80

HTTPS Port 443

RTSP Port 554

Control Port 30001

Port range [1025-65534]

Step 2 Select UPnP enable type.

Step 3 Manual UPnP: Input the HTTP port, data port, and client port manually.

Table 6-11 Port

Parameter	Description
HTTP Port	The default value setting is 80. You can enter the value according to your actual situation. If you enter another value, for example, 70, then you should enter 70 after the IP address when logging in to the device by browser.
HTTPS Port	HTTPS communication port. The default value setting is 443. You can enter the value according to your actual situation.
RTSP Port	Real-Time Streaming Protocol. The default value setting is 554. You can enter the value according to your actual situation.
Control port	The default value setting is 30413. You can enter the value according to your actual situation.

Step 4 Auto-UPnP: The device obtains the port automatically.

Step 5 Click Apply to save settings.

----End

6.6.5 Email

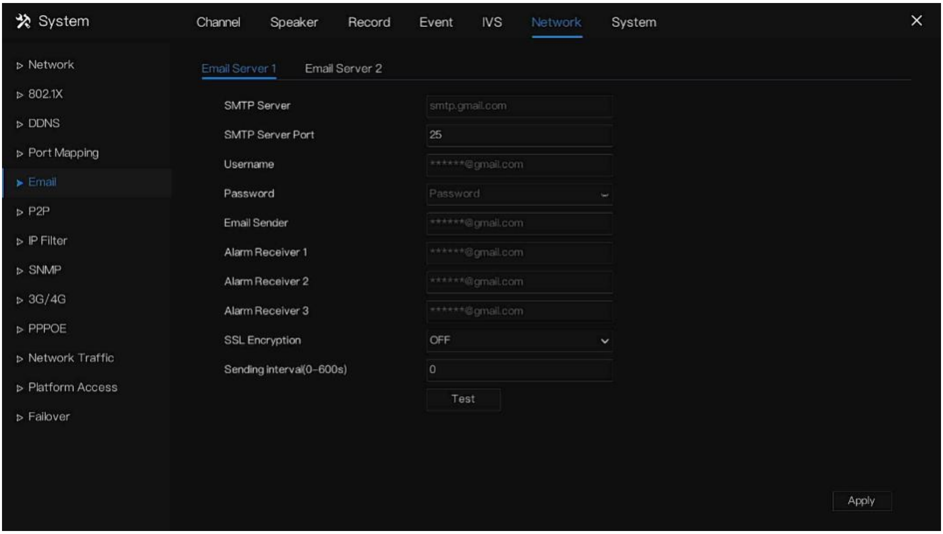
If the Simple Mail Transfer Protocol (SMTP) function is enabled, the device automatically sends alarm information to specified email addresses when an alarm is generated. Two mailboxes can be set as receivers.

Operation Steps

Step 1 Click **Email** on **Settings > Network** to access the E-mail screen, as shown in Figure 6-75.

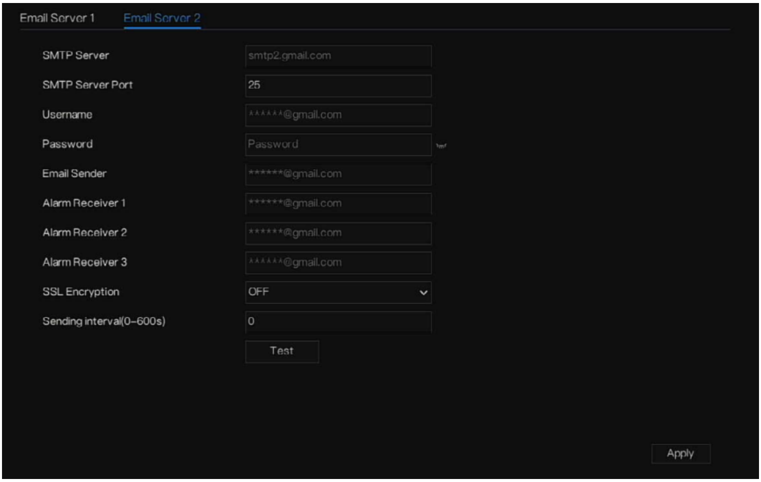
Step 2 Configure the settings for the email parameters.

Figure 6-75 Email setting screen



SMTP Server: smtp.gmail.com
SMTP Server Port: 25
Username: ******@gmail.com
Password: Password
Email Sender: ******@gmail.com
Alarm Receiver 1: ******@gmail.com
Alarm Receiver 2: ******@gmail.com
Alarm Receiver 3: ******@gmail.com
SSL Encryption: OFF
Sending interval(0-600s): 0

Figure 6-76 Email server 2



SMTP Server: smtp2.gmail.com
SMTP Server Port: 25
Username: ******@gmail.com
Password: Password
Email Sender: ******@gmail.com
Alarm Receiver 1: ******@gmail.com
Alarm Receiver 2: ******@gmail.com
Alarm Receiver 3: ******@gmail.com
SSL Encryption: OFF
Sending interval(0–600s): 0

Table 6-12 Email parameters

Parameter	Description
SMTP server	Enter the address of the SMTP server of the sender’s email account.
SMTP server port	Enter the port value of the SMTP server. The default value setting is 25. You can enter the value according to your actual situation.
Username	Enter the username and password of the sender’s email account.
Password	
Email sender	Enter the email address of the sender’s email account.
Alarm Receivers	Enter the emails of the receivers that you want to receive the notification. The Device supports up to three mail receivers.
TLS encryption	Select the encryption type: **TLS** (default value), **StartTLS**, and **Off**. Set the parameter based on the encryption mode supported by the SMTP server.
Sending Interval(0-600s)	This is the interval that the system sends an email for the same type of alarm event, which means, the system does not send emails caused by frequent alarm events. The value ranges from 0 to 600. 0 means that there is no interval.

Parameter	Description
TEST	Click **TEST** to test the email-sending function. If the configuration is correct, the receiver's email account will receive the email. Before testing, click **Apply** to save the settings.

Step 3 Click Apply to save settings.

----End

6.6.6 P2P

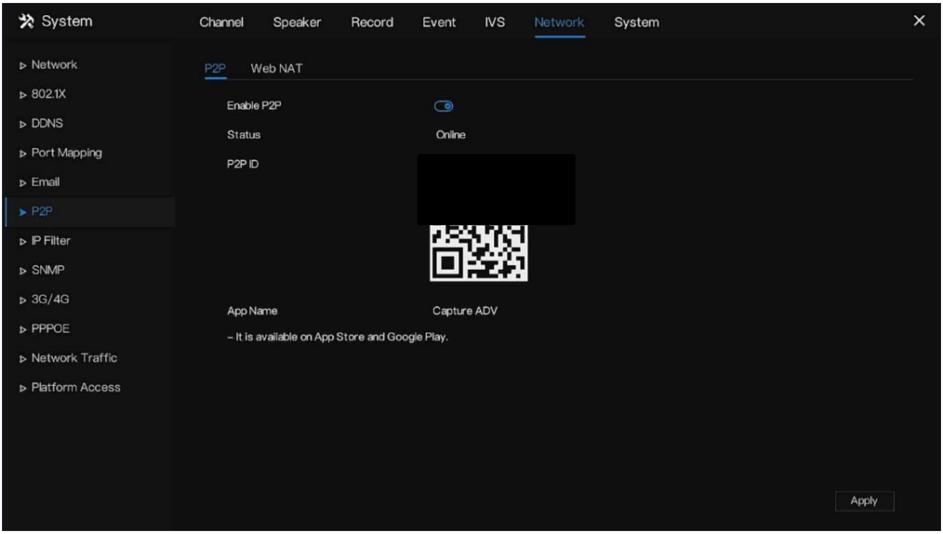
6.6.6.1 P2P

Show the UUID code and set the P2P status of the device.

Operation Steps

Step 1 Click **P2P** on **Settings > Network** to access the P2P screen, as shown in Figure 6-77.

Figure 6-77 P2P screen



Enable P2P ●

Status Online

P2P ID [redacted]

App Name Capture ADV

– It is available on App Store and Google Play.

Step 2 Click ○ to enable the P2P function.

Step 3 Click Apply to save P2P network settings or click **Cancel** to cancel settings.

Step 4 After the **Capture ADV** is installed on a mobile phone, run the APP and scan the QR to add and access the DVR when the device is online.

----End

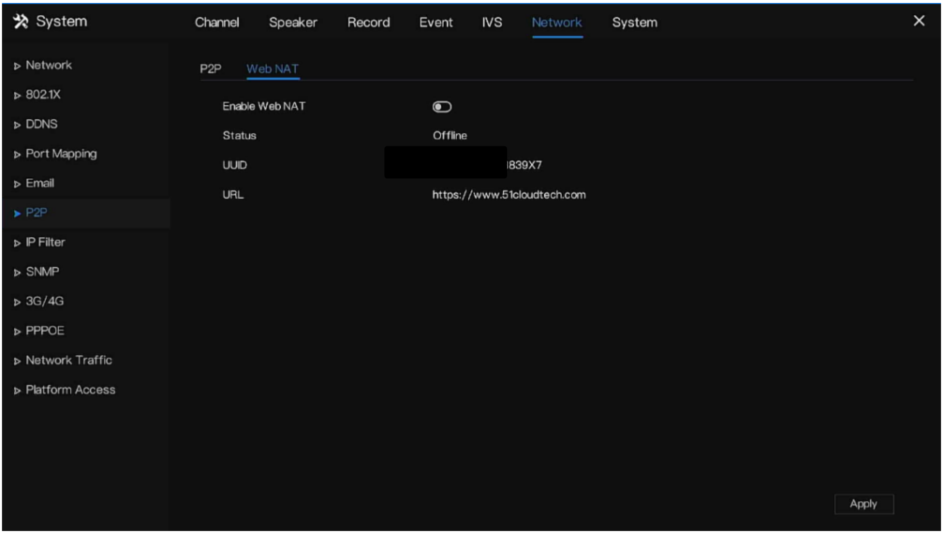
6.6.6.2 Web NAT

This function is used for web access to the DVR.

The web NAT uses URL and UUID to log in to the web interface.

Enable Web NAT; when the status is online, copy the URL to enter the browser, and it will jump to the URL interface.

Figure 6-78 Web NAT



Enable Web NAT ○

Status Offline

UUID [redacted]839X7

URL https://www.51cloudtech.com

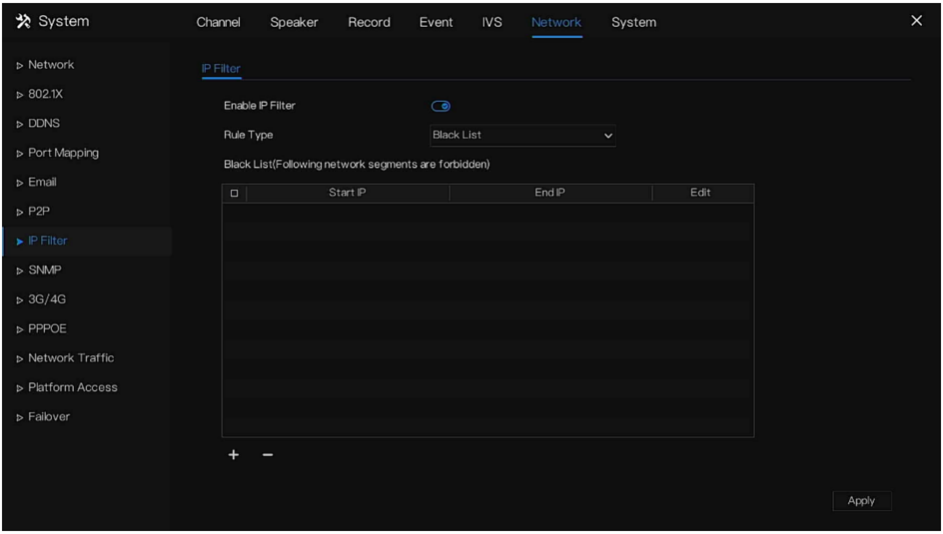
6.6.7 IP Filter

Set the IP address in a specified network segment to allow or prohibit access.

Operation Steps

Step 1 Click the **IP Filter** on **Settings > Network** to access the IP filter screen, as shown in Figure 6-79.

Figure 6-79 IP Filter setting screen

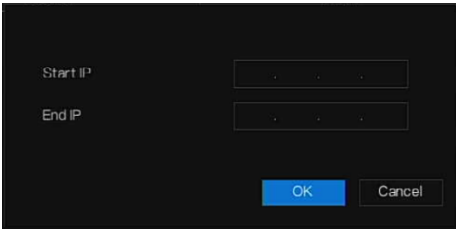


Step 2 Click ⬤ next to **IP Filter** to enable the function of IP Filter.

Step 3 Select blacklist or whitelist drop-down list.

Step 4 Click + to set the blacklist &whitelist IP segment screen is displaying, as shown in Figure 6-80.

Figure 6-80 IP Address Segment screen



Step 5 Enter value manually for start IP address and end IP address.

Step 6 Click OK. The system saves the settings. The black and white lists IP segment are listed in the black (white) list.

NOTE

Blacklist: A list of IP addresses in specified network segments that are regarded as unacceptable or untrustworthy and should be excluded or avoided.

Whitelist: A list of addresses in a specified network segment considered to be acceptable or trustworthy.

Select a name in the list and click **Delete** to delete the name from the list.

Select a name in the list and click **Edit** to edit the name in the list.

Only one rule type is available, and the last rule type set is efficient.

----End

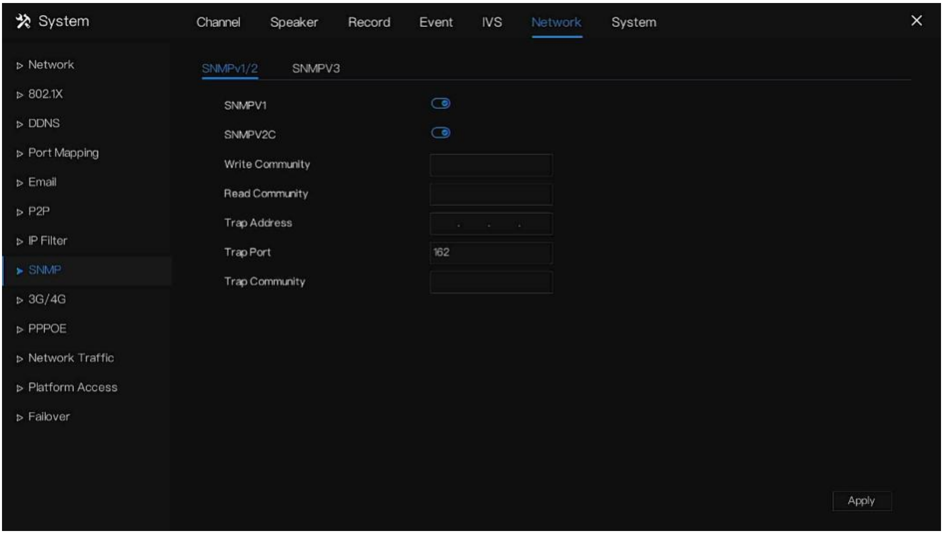
6.6.8 SNMP

There are three versions of Simple Network Management Protocols at the interface.

Operation Steps

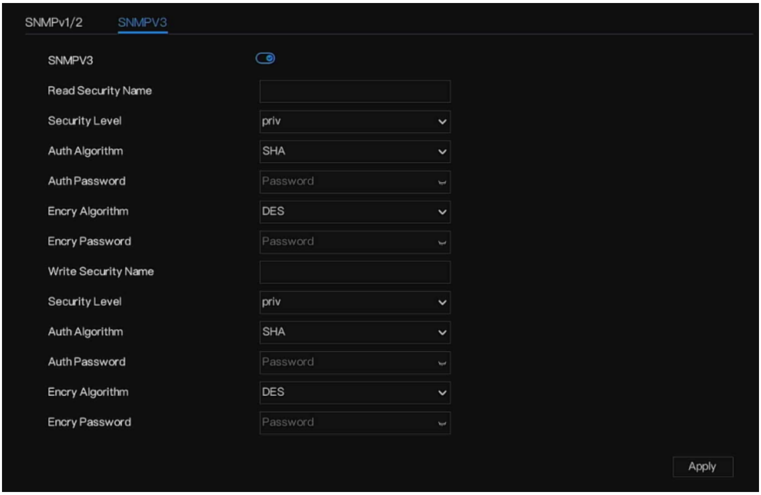
Step 1 Click the **IP Filter** in the Setting System or menu of the network management screen and choose **IP Filter** to access the IP filter screen, as shown in Figure 6-81.

Figure 6-81 SNMP settings screen



SNMPV1
SNMPV2C
Write Community
Read Community
Trap Address . . .
Trap Port 162
Trap Community

Figure 6-82 SNMPV3



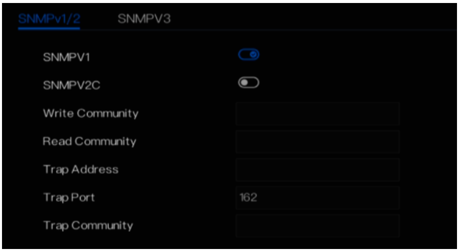
SNMPV3
Read Security Name
Security Level priv
Auth Algorithm SHA
Auth Password Password
Encry Algorithm DES
Encry Password Password
Write Security Name
Security Level priv
Auth Algorithm SHA
Auth Password Password
Encry Algorithm DES
Encry Password Password

Parameter	Description
SNMPV1	The version of SNMP. SNMPV1 and SNMPV2C use communities to establish trust between managers and agents. Agents support three
SNMPV2C	

Parameter	Description
	community names, write community, read community, and trap.
Write community	Name of writing community.
Read community	The write community only can modify data.
Trap address	Name of the reading community.
Trap port	The writing community only can read data.
Trap community	IP address of the trap.
SNMPV3	Management port of accepting messages from the trap.
Read security name	community string of traps.
Write security name	The trap community string allows the manager to receive asynchronous information from the agent.
Security level	The version of SNMP.
Auth algorithm	SNMPv3 uses community strings but allows for secure authentication and communication between the SNMP manager and agent.
Auth password	Name of read security.
Encry algorithm	Name of write security.
Encry password	Security Level between SNMP manager and agent includes three levels:

Step 2 Click ◯ next to **SNMPV 1** to enable the function. The interface is shown in Figure 6-83.

Figure 6-83 SNMPV 1/2 interface



SNMPv1/2 SNMPV3

SNMPV1 ●

SNMPV2C ○

Write Community

Read Community

Trap Address

Trap Port 162

Trap Community

Table 6-13 SNMP parameters

Step 3 Input the parameters of the protocol.

Step 4 Click Apply to save settings or click Cancel to cancel settings.

----End

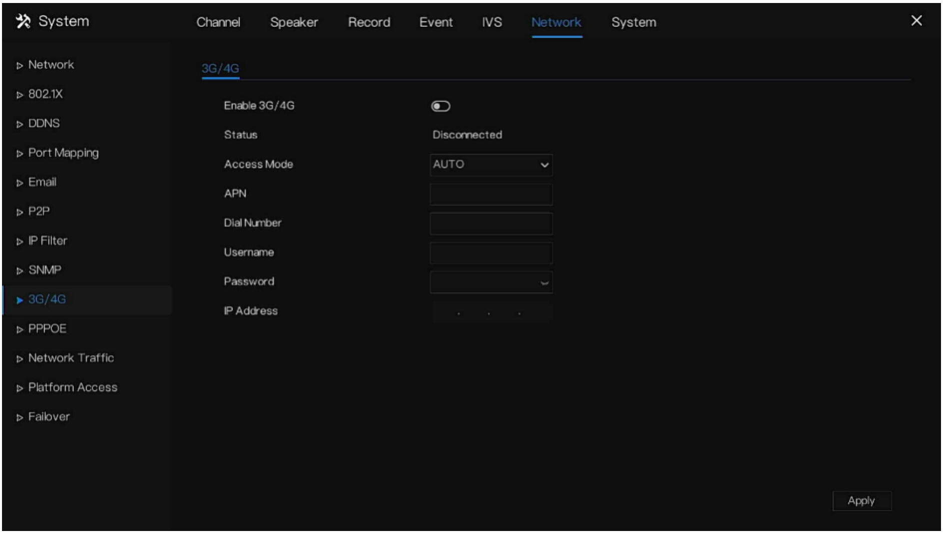
6.6.9 3G/4G

Users can connect DVR to the data network using a modem.

Operation Steps

Step 1 Plug the modem into DVR, and enable the 3G/4G function, as shown in Figure 6-84.

Figure 6-84 3G/4G setting screen



Enable 3G/4G	○
Status	Disconnected
Access Mode	AUTO
APN	
Dial Number	
Username	
Password	
IP Address	. . .

Step 2 If the connection is successful, set other parameters.

Step 3 Choose access mode; the default is AUTO. Five modes can be chosen, such as AUTO, LTE, TD-SCDMA, WCDMA, and GSM/GPRS.

Step 4 Input the APN, dial number, username, password, and IP address. In auto mode, all these parameters can be obtained automatically.

Step 5 Click Apply to save settings.

NOTE

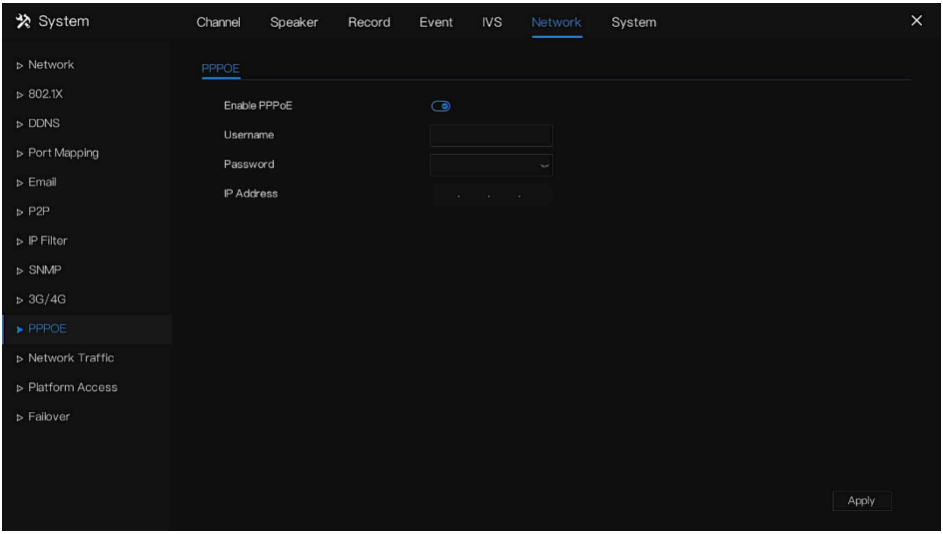
- Modify the access mode of 3G/4G (AUTO, LTE, TD-SCDMA, WCDMA, GSM/GPRS). If you cannot dial within 5 minutes, re-plug the modem.
- Users are familiar with the relevant network (different service provider parameters are different) and modem information before manually switching to other modes; the recommended mode is **Auto**.
- When using the 3G/4G function, you need to manually close the PPPOE function. Only one function can be used at a time.
- If the Internet access type is LTE (4G network), you do not need to dial the number, user name, and password.

----End

6.6.10 PPPOE

PPPOE Point-to-Point protocol Ethernet; the user uses the PPPOE to access the network immediately, as shown in Figure 6-85.

Figure 6-85 PPPOE



Step 1 Enable the PPPOE function.

Step 2 Input the **username**, and **password** (provided by network operator).

Step 3 Click Apply to save settings, and the IP is obtained automatically.

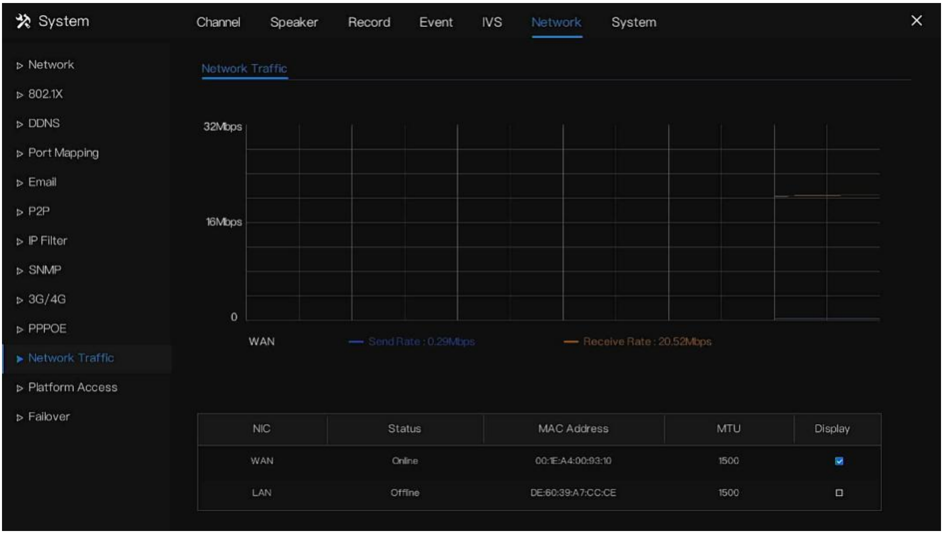
Step 4 Users input the IP to access the DVR web immediately.

----End

6.6.11 Network Traffic

Users can view the network traffic immediately, as shown in Figure 6-86

Figure 6-86 Network traffic



NIC	Status	MAC Address	MTU	Display
WAN	Online	00:1E:A4:00:93:10	1500	☑
LAN	Offline	DE:60:39:A7:CC:CE	1500	□

There are two rates: transmit rate and receive rate. The status of LAN(s) is shown on the list.

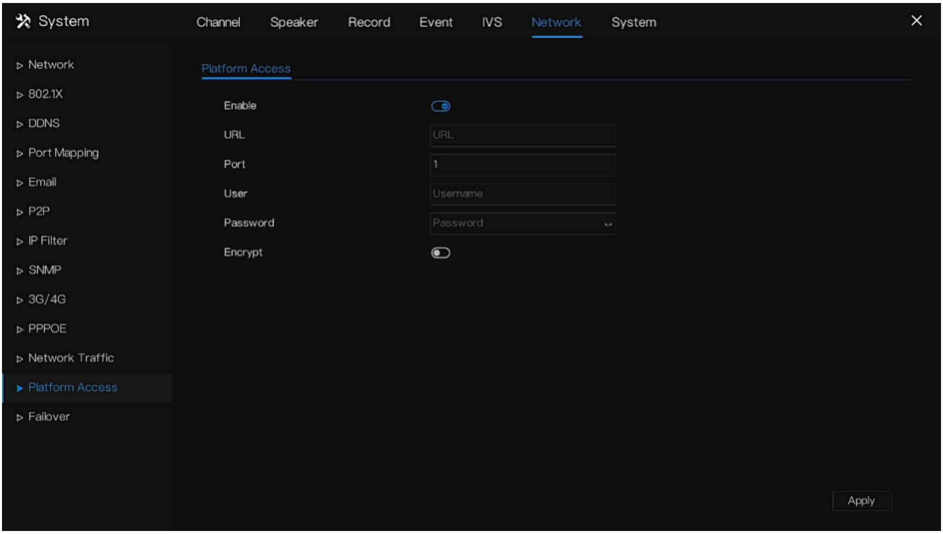
----End

6.6.12 Platform Access

If the DVR and platform system are not on the same local network, ensure the DVR is connected to the same external server as the platform system. You should build a server for the platform in advance; the platform's remote IP/Port and DVR are mapping the port to the external network.

Step 1 Click **Platform Access** on **Settings > Network Service** to access the **Platform Access** page, as shown in Figure 6-87

Figure 6-87 Platform Access page



URL: URL
Port: 1
User: Username
Password: Password

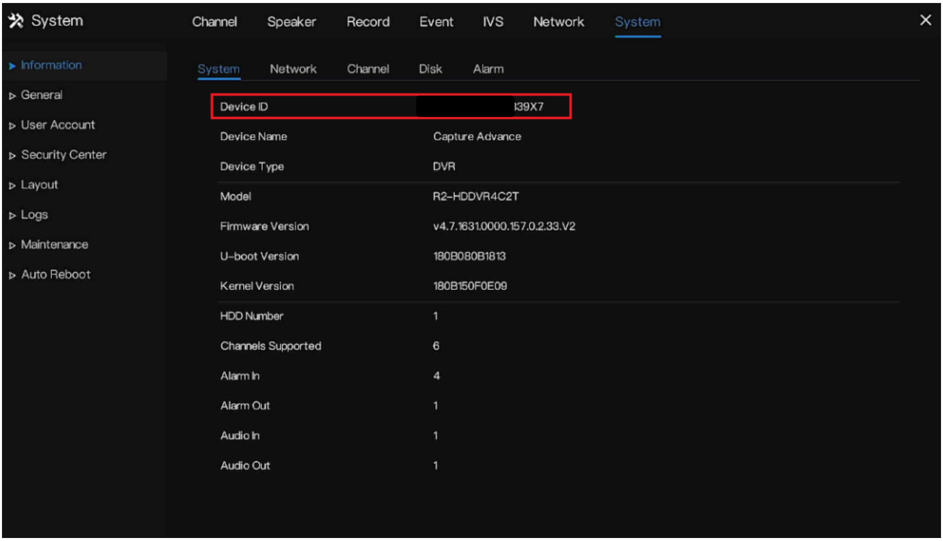
Step 2 Input the parameters. The URL and port are the platform server IP address and port.

Step 3 The name and port are the platform's login name and password.

Step 4 Add the DVR to the platform. You should input the following information.

1: IP/ID/Domain name is Device ID of DVR.

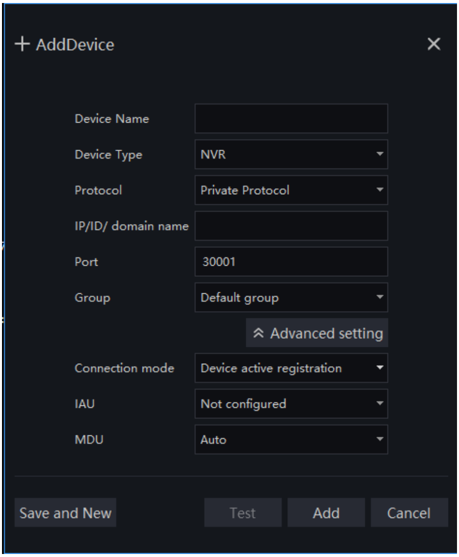
Figure 6-88 IP/ID/Domain



Device ID	[redacted]39X7
Device Name	Capture Advance
Device Type	DVR
Model	R2-HDDVR4C2T
Firmware Version	v4.7.1631.0000.157.0.2.33.V2
U-boot Version	180B080B1813
Kernel Version	180B150F0E09
HDD Number	1
Channels Supported	6
Alarm In	4
Alarm Out	1
Audio In	1
Audio Out	1

2: The connection mode should be chosen for **Device active registration**.

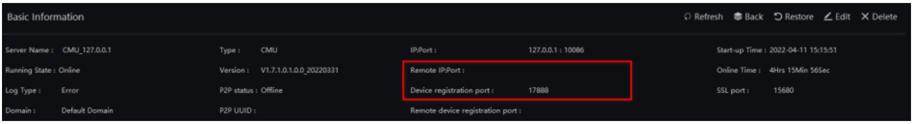
Figure 6-89 Connect DVR to platform



Device Name	
Device Type	NVR
Protocol	Private Protocol
IP/ID/ domain name	
Port	30001
Group	Default group
Connection mode	Device active registration
IAU	Not configured
MDU	Auto

3: the CMU, MDU, and IAU servers of the platform should be mapped to the ports of the external network in advance.

Figure 6-90 URL address/port



Server Name : CMU_127.0.0.1
Running State : Online
Log Type : Error
Domain : Default Domain
Type : CMU
Version : V1.7.1.0.1.0.0_20220331
P2P status : Offline
P2P UUID :
IP:Port : 127.0.0.1 : 10086
Remote IP:Port :
Device registration port : 17888
Remote device registration port :
Start-up Time : 2022-04-11 15:15:51
Online Time : 4Hrs 15Min 56Sec
SSL port : 15680

Step 5 If you want to encrypt the access, you can enable the Encrypt.

Step 6 Click **Apply**.

The message "Apply success!" is displayed, and the system saves the settings.

----End

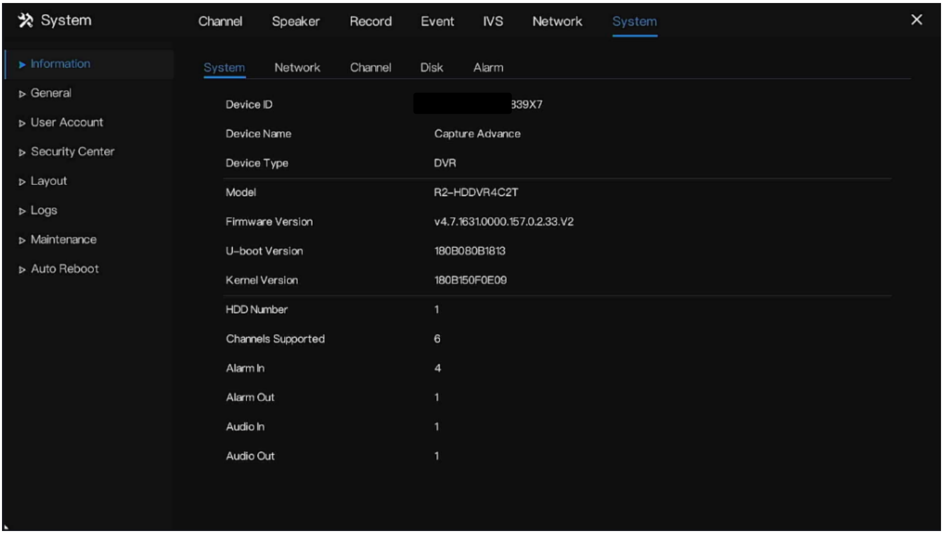
6.7 System Management

View the device **Information** and set **General** information, **User Account**, **Security Center**, **Layout**, **Logs**, **Maintenance,** and **Auto Reboot** for the system setting.

Operation Description

Click **System** in the Setting System (or click the system page of any function screen in the Setting System) to access the system setting screen, as shown in Figure 6-91.

Figure 6-91 System setting screen

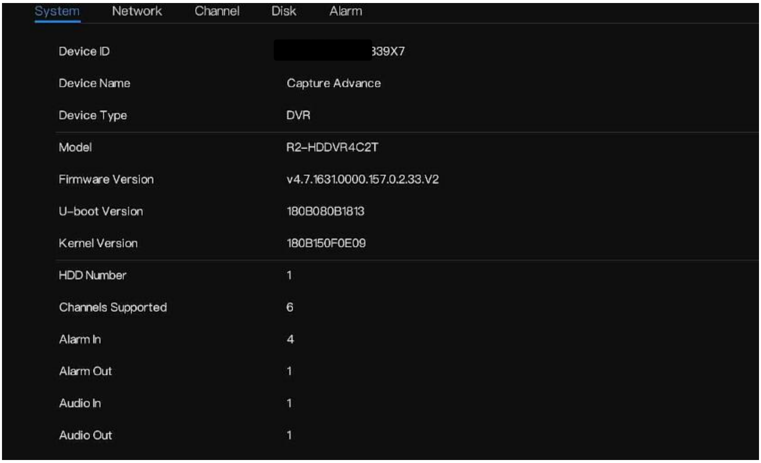


Device ID	[redacted]39X7
Device Name	Capture Advance
Device Type	DVR
Model	R2-HDDVR4C2T
Firmware Version	v4.7.1631.0000.157.0.2.33.V2
U-boot Version	180B080B1813
Kernel Version	180B150F0E09
HDD Number	1
Channels Supported	6
Alarm In	4
Alarm Out	1
Audio In	1
Audio Out	1

6.7.1 Information

View the device ID, device name, device type, model, firmware version, kernel version, face detection version, HDD volume, channel support, alarm in, alarm out, audio in, and audio out in the **Information** screen, as shown in Figure 6-92.

Figure 6-92 Information-system interface

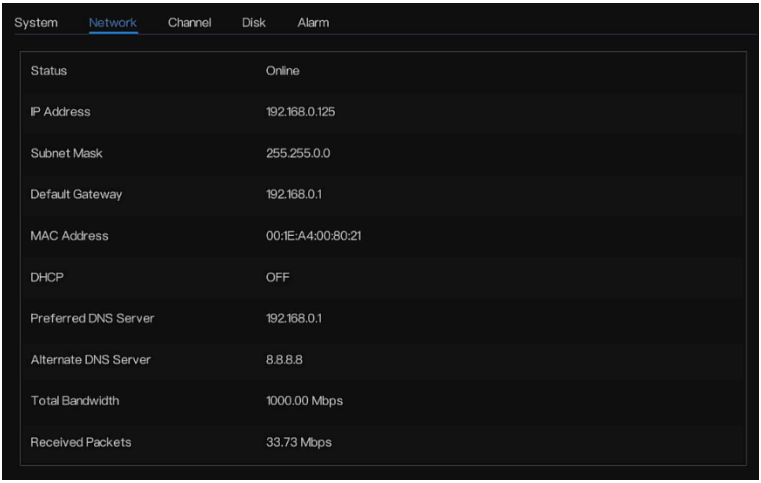


System Network Channel Disk Alarm

Device ID	[redacted]39X7
Device Name	Capture Advance
Device Type	DVR
Model	R2-HDDVR4C2T
Firmware Version	v4.7.1631.0000.157.0.2.33.V2
U-boot Version	180B080B1813
Kernel Version	180B150F0E09
HDD Number	1
Channels Supported	6
Alarm In	4
Alarm Out	1
Audio In	1
Audio Out	1

Network: status, IP address, subnet mask, default gateway, MAC address, DHCP, preferred DNS server, Alternate DNS server, total bandwidth, received packets, and so on, as shown in Figure 6-93.

Figure 6-93 Information-network interface

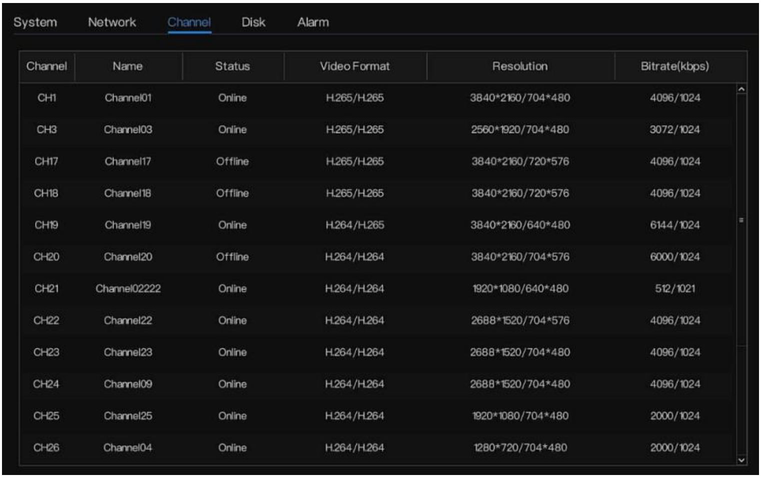


System Network Channel Disk Alarm

Status	Online
IP Address	192.168.0.125
Subnet Mask	255.255.0.0
Default Gateway	192.168.0.1
MAC Address	00:1E:A4:00:80:21
DHCP	OFF
Preferred DNS Server	192.168.0.1
Alternate DNS Server	8.8.8.8
Total Bandwidth	1000.00 Mbps
Received Packets	33.73 Mbps

Channel: channel, name, status, video format, resolution, bitrate (kbps), and so on, as shown in Figure 6-94.

Figure 6-94 Information-channel interface

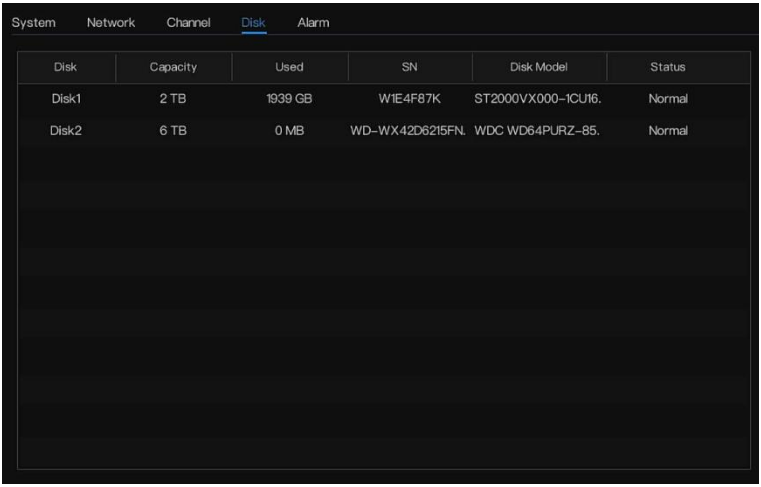


Channel	Name	Status	Video Format	Resolution	Bitrate(kbps)
CH1	Channel01	Online	H.265/H.265	3840*2160/704*480	4096/1024
CH3	Channel03	Online	H.265/H.265	2560*1920/704*480	3072/1024
CH17	Channel17	Offline	H.265/H.265	3840*2160/720*576	4096/1024
CH18	Channel18	Offline	H.265/H.265	3840*2160/720*576	4096/1024
CH19	Channel19	Online	H.264/H.265	3840*2160/640*480	6144/1024
CH20	Channel20	Offline	H.264/H.264	3840*2160/704*576	6000/1024
CH21	Channel02222	Online	H.264/H.264	1920*1080/640*480	512/1021
CH22	Channel22	Online	H.264/H.264	2688*1520/704*576	4096/1024
CH23	Channel23	Online	H.264/H.264	2688*1520/704*480	4096/1024
CH24	Channel09	Online	H.264/H.264	2688*1520/704*480	4096/1024
CH25	Channel25	Online	H.264/H.264	1920*1080/704*480	2000/1024
CH26	Channel04	Online	H.264/H.264	1280*720/704*480	2000/1024

Disk: disk name, capacity, used, SN, disk model, status, and so on, as shown in Figure 6-95

.

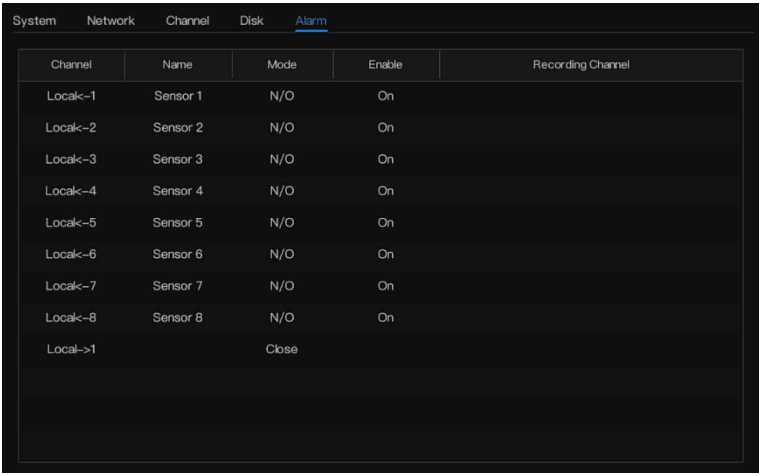
Figure 6-95 Information-disk interface



Disk	Capacity	Used	SN	Disk Model	Status
Disk1	2 TB	1939 GB	W1E4F87K	ST2000VX000-1CU16.	Normal
Disk2	6 TB	0 MB	WD-WX42D6215FN.	WDC WD64PURZ-85.	Normal

Alarm: channel, name, mode, enable, recording channel, and so on, as shown in Figure 6-96.

Figure 6-96 Information-alarm interface



Channel	Name	Mode	Enable	Recording Channel
Local<-1	Sensor 1	N/O	On	
Local<-2	Sensor 2	N/O	On	
Local<-3	Sensor 3	N/O	On	
Local<-4	Sensor 4	N/O	On	
Local<-5	Sensor 5	N/O	On	
Local<-6	Sensor 6	N/O	On	
Local<-7	Sensor 7	N/O	On	
Local<-8	Sensor 8	N/O	On	
Local->1		Close		

----End

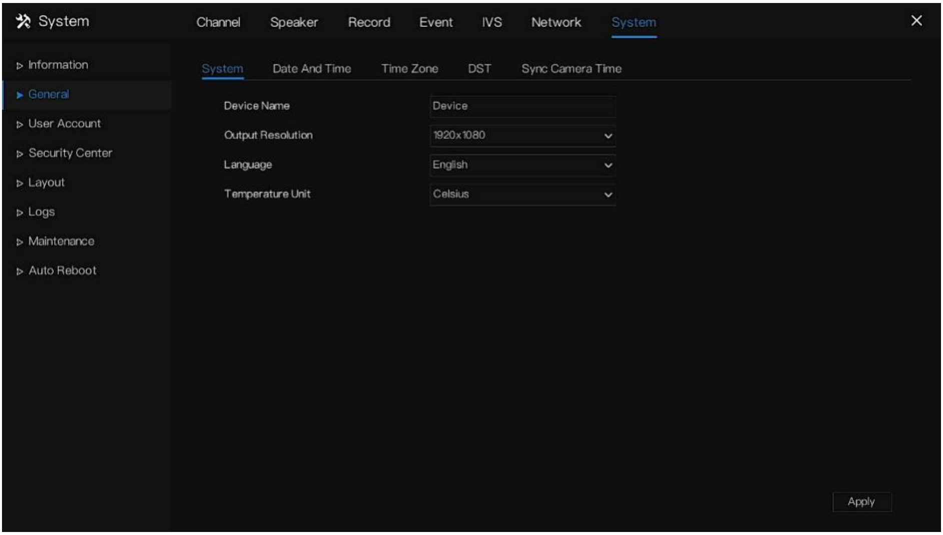
6.7.2 General

6.7.2.1 System

Operation Steps

Step 1 Click **General** on **Settings > System** to access the system screen, as shown in Figure 6-97.

Figure 6-97 system setting screen



Device Name: Device

Output Resolution: 1920x1080

Language: English

Temperature Unit: Celsius

Step 2 Enter the name of the selected device.

Step 3 Select a proper resolution from the output resolution drop-down list.

Step 4 Select a required language from the Language drop-down list.

Step 5 Set the temperature unit.

NOTE

The DVR supports the following languages, Arabi, Danish, Finnish, Hungarian, Korean, Russian, Turkish, Chinese, Dutch, French, Indonesian Language, Slovakia, Vietnamese, Traditional Chinese, Chinese, English, German, Italian, Polish, Spanish, Czech, Farsi, Hebrew, Japanese, Portuguese, Thai.

Step 6 Click Apply to save settings.

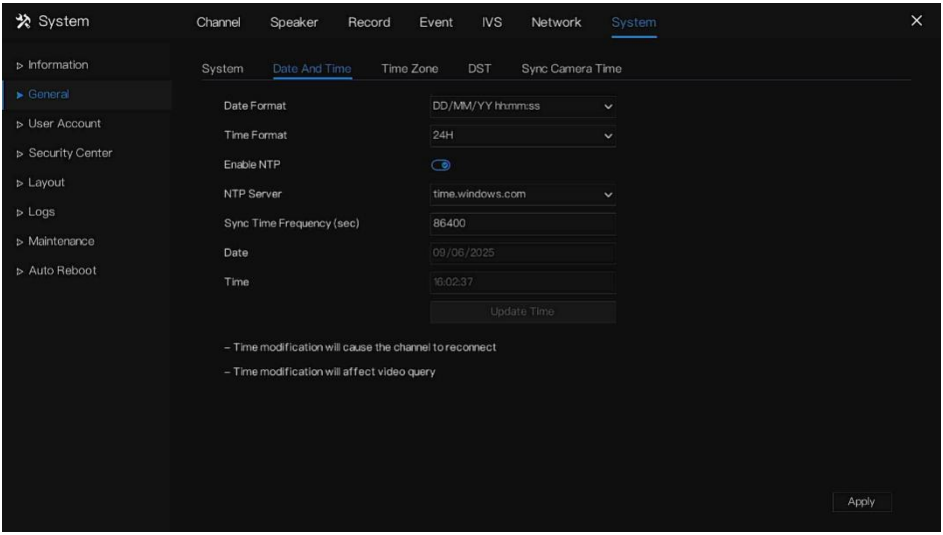
----End

6.7.2.2 Date and Time

Operation Steps

Step 1 Click the **Date and Time** on **Settings > System** > **General** to access the date and time setting screen, as shown in Figure 6-98.

Figure 6-98 Date and Time setting screen



Date Format: DD/MM/YY hh:mm:ss

Time Format: 24H

Enable NTP: ●

NTP Server: time.windows.com

Sync Time Frequency (sec): 86400

Date: 09/06/2025

Time: 16:02:37

– Time modification will cause the channel to reconnect

– Time modification will affect video query

Step 2 Select the required format from the Date Format and Time Format drop-down list.

Step 3 Click next to NTP Sync to disable time synchronization. Time synchronization is enabled by default. Time is synchronized with the NTP.

Step 4 After NTP Sync is disabled, you can manually set the system time:

Click **Date** and use the scroll wheel to select the year, month, and date.
Click **Time** and use the scroll wheel to select the hour, minute, and second.
Click **Modify Time** to save the time settings.

Table 6-14 Data and time parameters

Parameter	Description
Date format	Select a date format for the system.
Time format	Select **12H** or **24H** for the time display style.
Enable NTP	Enable the NTP function to sync the Device time with the NTP server. ⚠ **If NTP is enabled, device time will be automatically synchronized with the server.**
Enable NTP encryption	Enable the NTP to keep safe.

Parameter	Description
NTP server	Choose the NTP server to synchronize. If at **Network > Access platform** interface, enable SIRA, the NTP server will be updated automatically**.**
Sync time frequency (sec)	Sync the NTP server for the setting time. ⚠ **Do not change the system time randomly; otherwise, the recorded video cannot be searched. It is recommended to avoid the recording period or stop recording first before you change the system time.**
Date (Time)	If the user doesn't enable the sync time, you can modify the Date (Time) manually.

Step 5 Click Apply to save settings.

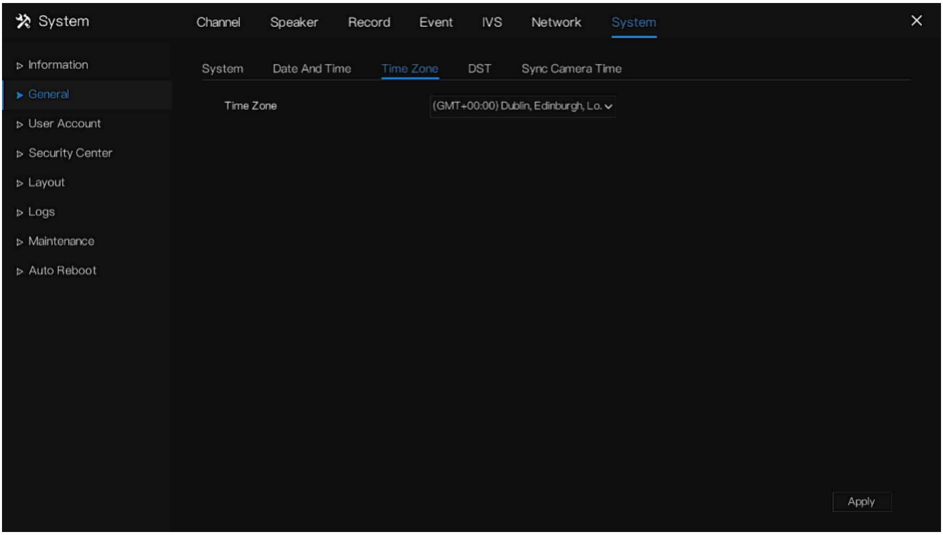
----End

6.7.2.3 Time Zone

Operation Steps

Step 1 Click **the Time Zone** on **Settings > System** > **General** to access the time zone setting screen, as shown in Figure 6-99.

Figure 6-99 Time zone setting screen



Time Zone (GMT+00:00) Dublin, Edinburgh, Lo.

Step 2 Select a required time zone from the Time Zone drop-down list.

Step 3 Click Apply to save settings.

----End

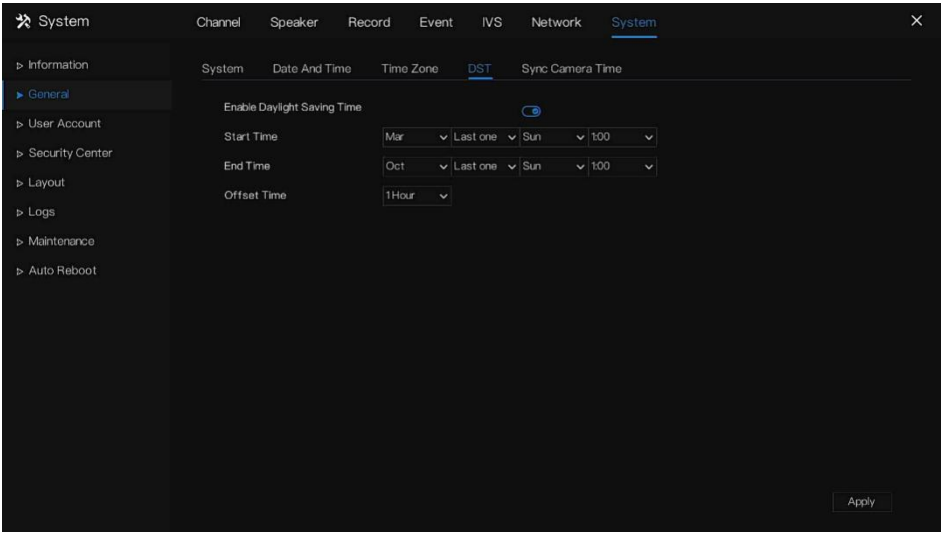
6.7.2.4 DST

When the DST start time arrives, the device time automatically goes forward one hour (offset time). When the DST end time arrives, the device time automatically goes backward one hour. The offset time can change if the local rule is different.

Operation Steps

Step 1 Click the **DST** on **Settings > System** > **General** to access the DST setting screen, as shown in Figure 6-100.

Figure 6-100 DST setting screen



Enable Daylight Saving Time

Start Time Mar Last one Sun 1:00

End Time Oct Last one Sun 1:00

Offset Time 1Hour

Step 2 Click ◯ next to **DST** to enable DST.

Step 3 Select start time, end time, and offset time from the drop-down list respectively, that basis on the local rules.

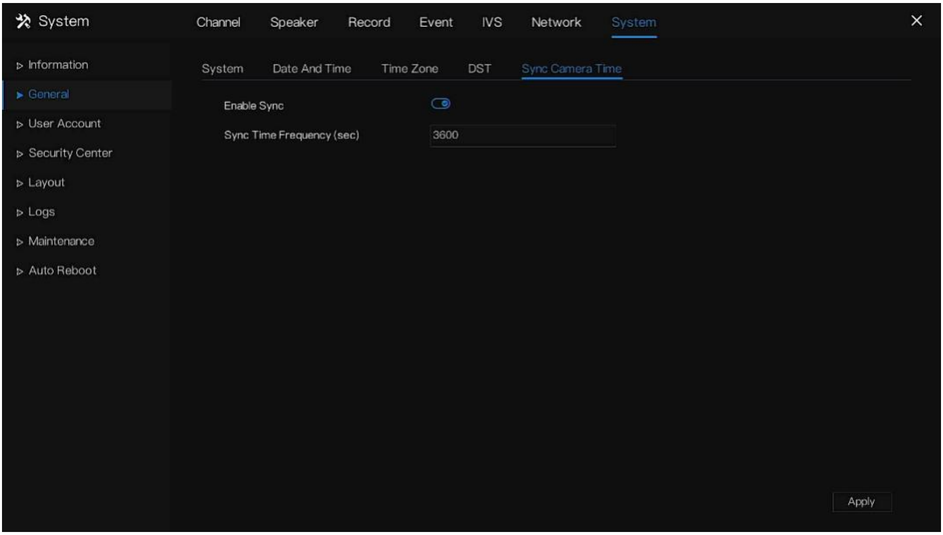
Step 4 Click Apply to save settings.

----End

6.7.2.5 Sync Camera Time

Click the **Sync Camera Time** on **Settings > System** > **General**. Enable the sync camera time, the channels will show the sync time and set the frequency of the check.

Figure 6-101 Sync camera Time



Enable Sync

Sync Time Frequency (sec) 3600

----End

6.7.3 User Account

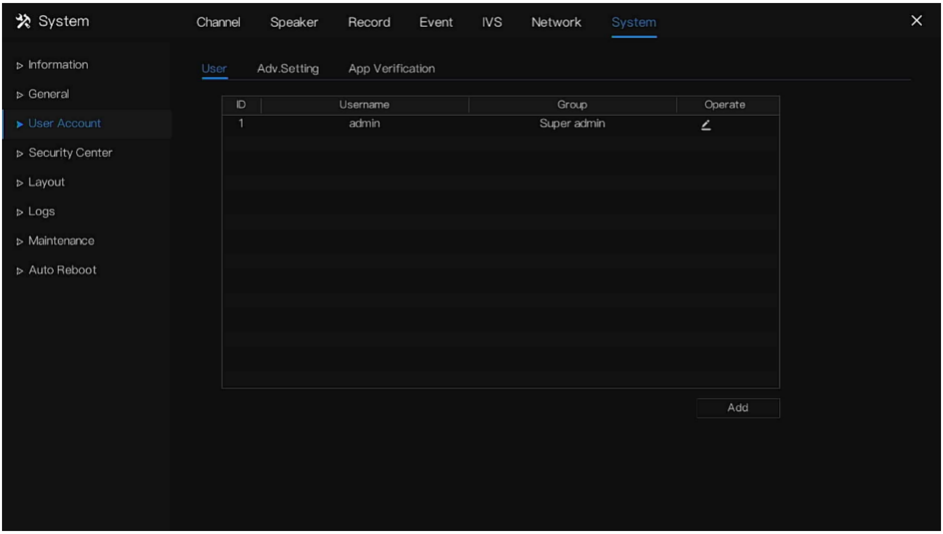
Add, modify, and delete a user and privilege in the user screen. The admin user can dispose of privileges to different users.

6.7.3.1 User

Operation Steps

Step 1 Click **User** on **Settings > System** > User Account to access the user screen, as shown in Figure 6-102.

Figure 6-102 User management screen



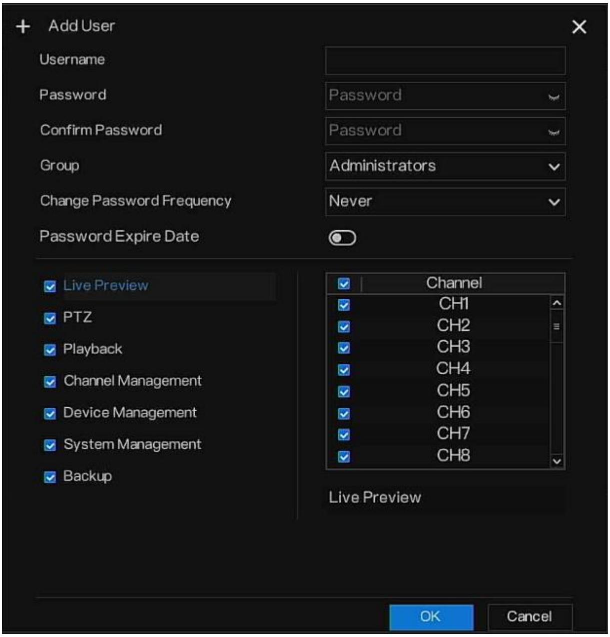
ID	Username	Group	Operate
1	admin	Super admin	✎

Step 2 Add or delete a user.

- Add a user

  Click **Add** and the **Add User** dialog box appears, as shown in Figure 6-103.

Figure 6-103 Add user screen



+ Add User

Username

Password: Password

Confirm Password: Password

Group: Administrators

Change Password Frequency: Never

Password Expire Date

☑ Live Preview
☑ PTZ
☑ Playback
☑ Channel Management
☑ Device Management
☑ System Management
☑ Backup

☑	Channel
☑	CH1
☑	CH2
☑	CH3
☑	CH4
☑	CH5
☑	CH6
☑	CH7
☑	CH8

Live Preview

Input a username, and password and confirm the password, choose group and change password reminder, and set the expiration date.

Table 6-15 Add interface parameters

Parameter	Description
User Name	Enter a username and password for the account. For user name should meet the rules: only these special characters are supported !@#$*+-=%&”`()./’.:;<>?^\|~[] Password requirement; -The password must be between 8 to 20 -Upper & lower case letters -At least on the number -Support the symbol -_@%^.~?#$=+”:,& only and must contain at least one of them -The first character must be a number or letter -No space
Password	
Confirm password	Re-enter the password.

Parameter	Description
Group	Select a group for the account, there are three groups, administer/ operator /media user. The user rights must be within the group's permission.
Change password frequency	To keep the safety of the device modify the password regularly.
Password expire date	Enable to set the duration of the user account.

Step 3 Select a **Group** from the drop-down list box.

Step 4 Select a **Change password reminder** value from the drop-down list box.

Step 5 Enable the expiration date to set the new user’s authority time.

Step 6 Select the operation privileges and channels in the list of the add user screen.

Step 7 Click OK. The user is set successfully.

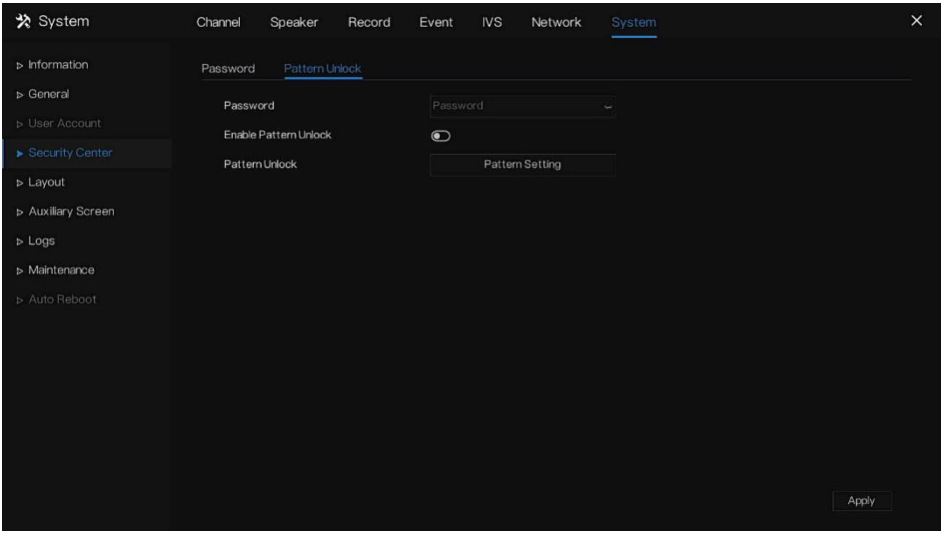
NOTE

The default user is the **admin** and cannot be deleted or modified.

Select a user from the user list and click ✎ to edit, or click 🗑 to delete a user.

The general user can also set pattern unlock to log on.

Figure 6-104 General user set pattern to unlock.

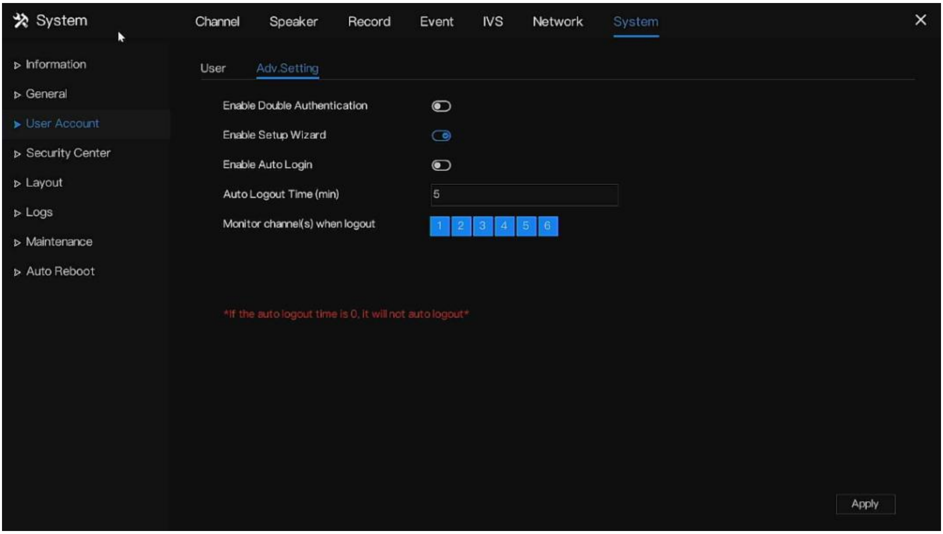


6.7.3.2 Advance Setting

Operation Steps

Step 1 Click **Adv Setting** on **Settings > System** > **User Account** to access the Advanced setting screen, as shown in Figure 6-105.

Figure 6-105 Advance setting screen



Enable Double Authentication ○

Enable Setup Wizard ●

Enable Auto Login ○

Auto Logout Time (min) 5

Monitor channel(s) when logout 1 2 3 4 5 6

If the auto logout time is 0, it will not auto logout

Step 2 Enable or disable **Double Authentication, Auto login, and Setup Wizard**. Set the logout time if the user disables the auto-login.

Step 3 Choose monitor channels when logging out, the default is all channels.

Step 4 Click Apply to save settings.

-----End

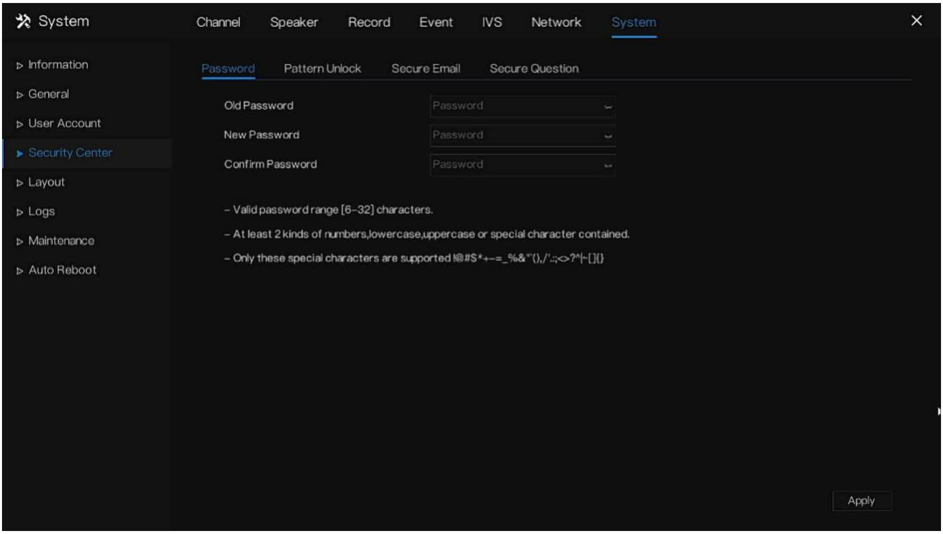
6.7.4 **Security Center**

6.7.4.1 Password

Operation Steps

Step 1 Click **Security Center** on **Settings > System** to access the modified password screen, as shown in Figure 6-106.

Figure 6-106 Password modification screen



Old Password: Password

New Password: Password

Confirm Password: Password

- Valid password range [6-32] characters.
- At least 2 kinds of numbers,lowercase,uppercase or special character contained.
- Only these special characters are supported !@#$*+-=_%&"(),/'.:;<>?^|~[]{}

Step 2 Input the correct old password, and the new password, and confirm the password.

NOTE

The password should include at least two kinds of letters, characters, and numbers.

The password should be 6~32 characters.

Only special characters (! @#&*+=-%&"`(),/'.:;< >?^|~[]{}) are supported,

Step 3 Click Apply to save modified password settings.

----End

6.7.4.2 Pattern Unlock

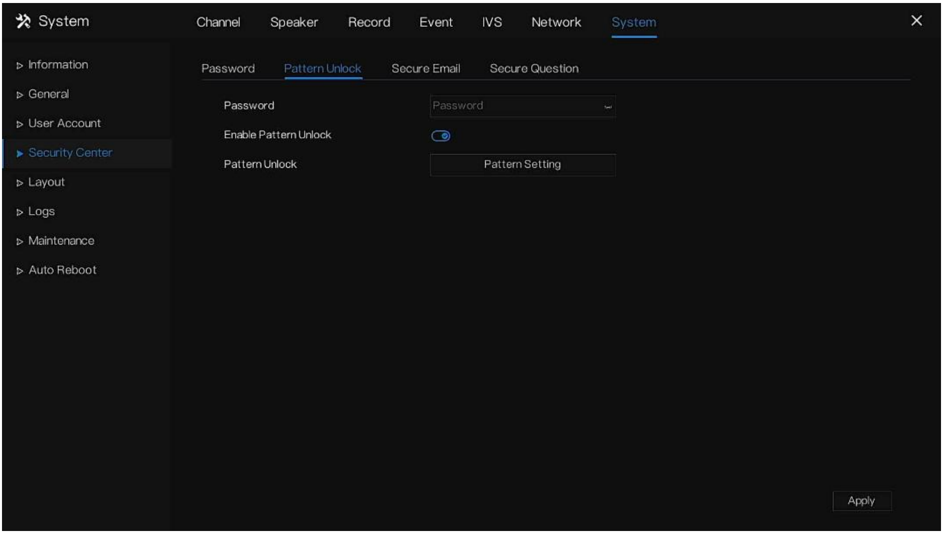
NOTE

The general users can also set pattern unlock to log on.

Operation Steps

Step 1 Click **Security Center** on **Settings > System** and choose **Pattern Unlock** to access the modified pattern unlock screen, as shown in Figure 6-107.

Figure 6-107 Pattern unlock screen



Password: Password

Enable Pattern Unlock: ●

Pattern Unlock: Pattern Setting

Step 2 Input the password, and enable pattern unlock.

Step 3 Click **Setting Pattern** to set a new pattern to unlock.

Step 4 Draw the pattern, then it will remind you to draw the confirmation pattern again.

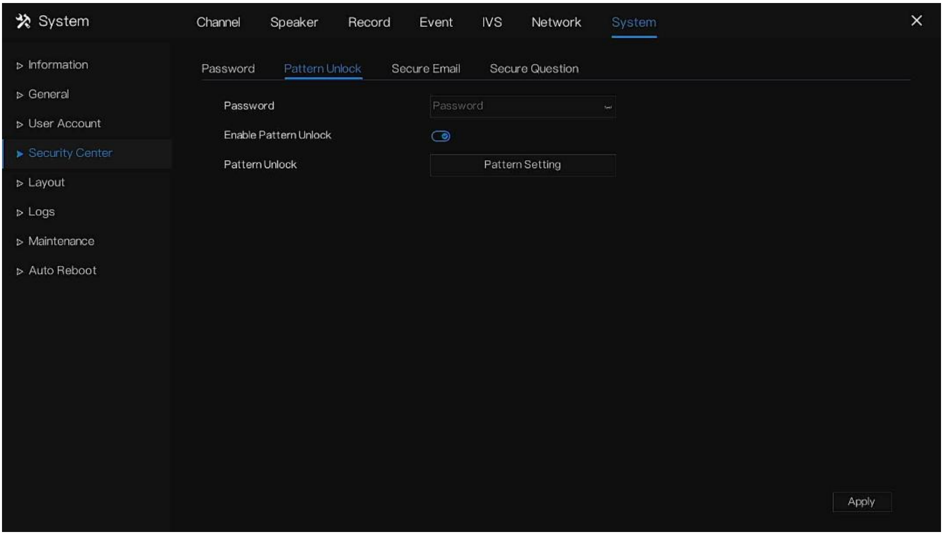
Step 5 Click OK to save the pattern unlock.

----End

6.7.4.3 Secure Email

Set the email to receive the verification code to create a new password, as shown in Figure 6-108.

Figure 6-108 Secure Email



Password: Password

Enable Pattern Unlock: ●

Pattern Unlock: Pattern Setting

Step 1 Input the password of DVR.

Step 2 Set the Email address to receive the verification code.

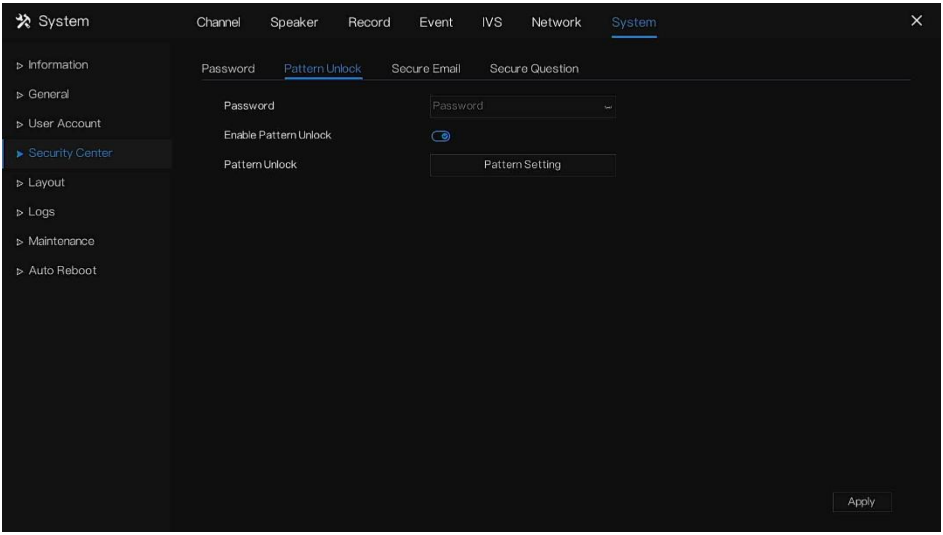
Step 3 Click Apply to save the setting.

----End

6.7.4.4 Secure Question

Set the questions to create a new password, as shown in Figure 6-108.

Figure 6-109 Secure question



Password: Password

Enable Pattern Unlock: ●

Pattern Unlock: Pattern Setting

Step 1 Input the password of DVR.

Step 2 Choose the question from the drop-down list.

Step 3 Input the answer, and click Apply to save the setting.

----End

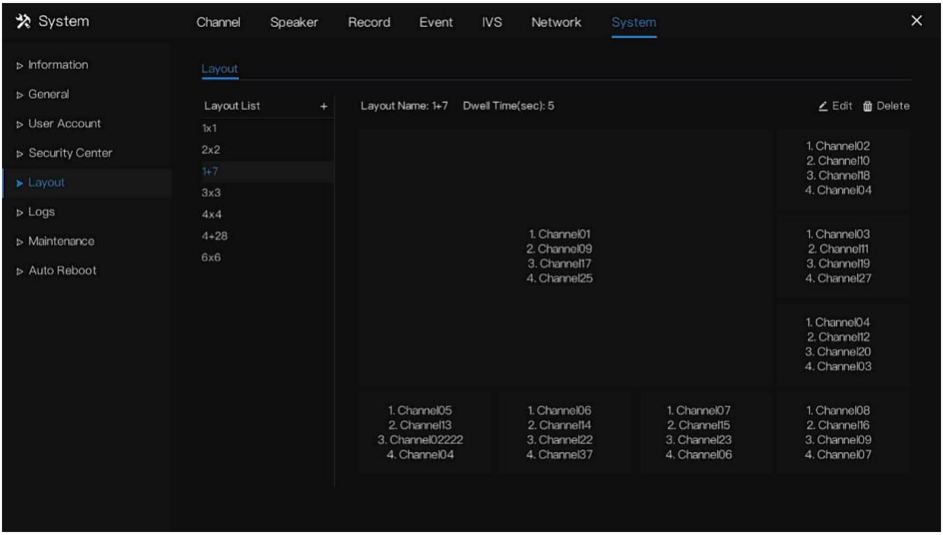
6.7.5 Layout

Set viewing video mode, and dwell time in the display screen. The layout is set as auto sequence multiple screens.

Operation Steps

Step 1 Click **Layout** in the Setting System or menu of the system management screen and choose **Layout** to access the display screen, as shown in Figure 6-110.

Figure 6-110 Auto Sequence screen



Layout Name: 1+7 Dwell Time(sec): 5

1. Channel01
2. Channel09
3. Channel17
4. Channel25

1. Channel02
2. Channel10
3. Channel18
4. Channel04

1. Channel03
2. Channel11
3. Channel19
4. Channel27

1. Channel04
2. Channel12
3. Channel20
4. Channel03

1. Channel05
2. Channel13
3. Channel02222
4. Channel04

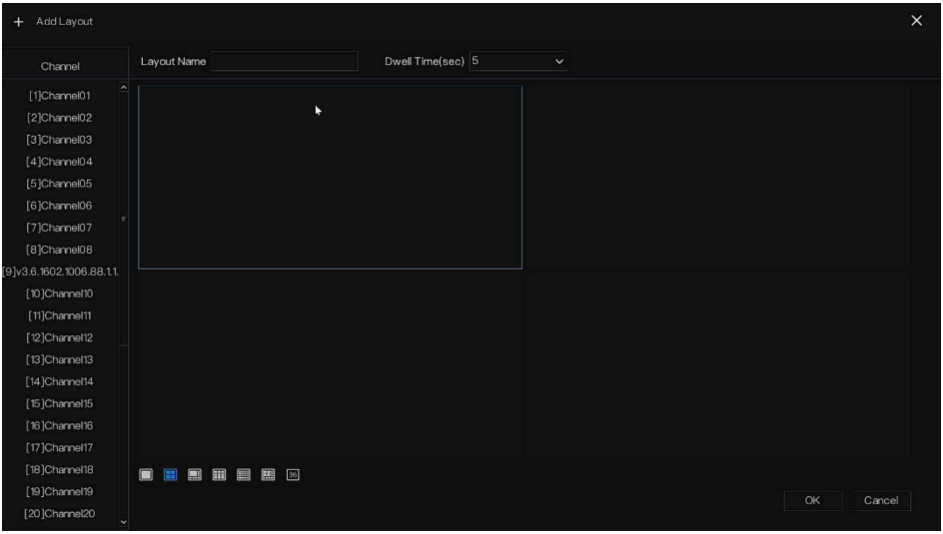
1. Channel06
2. Channel14
3. Channel22
4. Channel37

1. Channel07
2. Channel15
3. Channel23
4. Channel06

1. Channel08
2. Channel16
3. Channel09
4. Channel07

Step 2 Click "+" to add a new layout. The default layout is one splitting screen.

Figure 6-111 Add a new layout



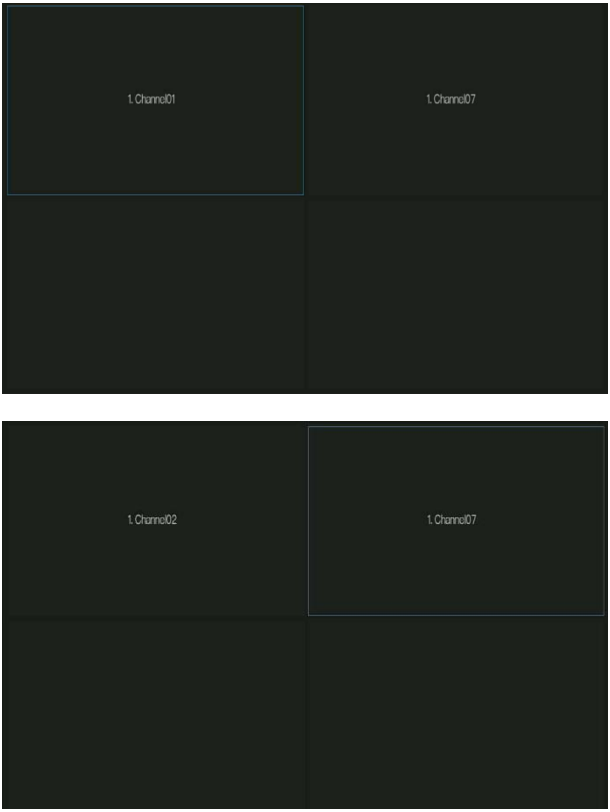
Layout Name

Dwell Time(sec) 5

Step 3 Input the layout name, and select dwell time from the **SEQ** Dwell time drop-down list(the display screen will loop play the real-time video according to setting time).

Step 4 Select split-screen mode at the bottom of the page. Set the channel display by dragging the channel to a specific position, or select the position first, then click the channel. A split screen can play multiple channels. Auto sequence means it will play according to the setting. For example, the first split screen is set as two pages (channels 1 and 2), and the second split screen is set as one page (channel 3). When the auto sequence is enabled, channel 1 and channel 3 are displayed, then channel 2 and channel 3 are displayed.

Figure 6-112 Auto sequence



Step 5 Click Apply to save dwell settings.

NOTE

Users can add up to 16 layouts.

----End

6.7.6 Auxiliary Screen (Only for Some Models)

NOTE

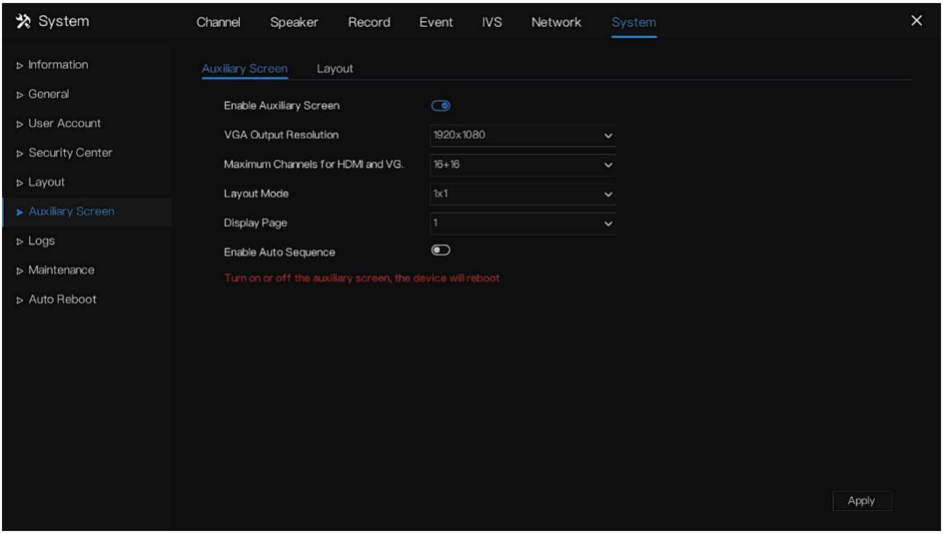
This function can only be used for some DVR devices. The main screen is connected by HDMI (HD-OUT 2), and the auxiliary screen is connected by VGA.

Operation Steps

Step 1 Click the **Auxiliary Screen** in the Setting System or menu of the system management screen.

Step 2 Enable the auxiliary screen, as shown in Figure 6-113

Figure 6-113 Auxiliary screen

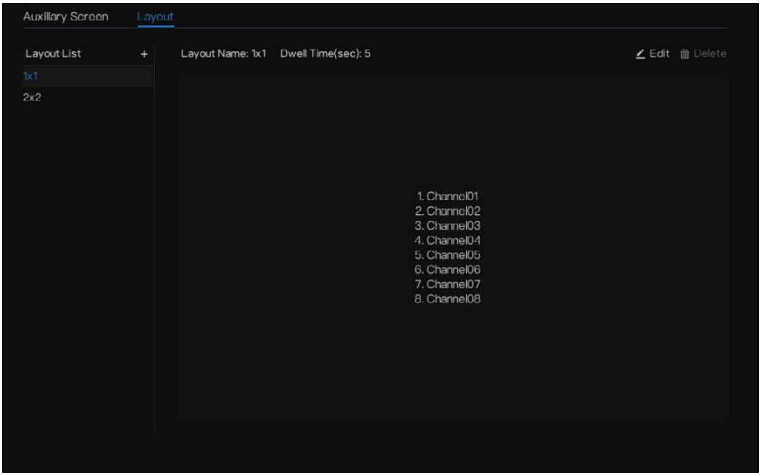


Enable Auxiliary Screen: ●
VGA Output Resolution: 1920x1080
Maximum Channels for HDMI and VG.: 16+16
Layout Mode: 1x1
Display Page: 1
Enable Auto Sequence: ○
Turn on or off the auxiliary screen, the device will reboot

Step 3 Set the Output Resolution, Decoding Ability(main + auxiliary), Layout Mode, and Display Channel.

Step 4 Enable tour to set **Auto Sequence** of the auxiliary screen as shown in Figure 6-114.

Figure 6-114 The auto sequence of auxiliary screen



Layout Name: 1x1 Dwell Time(sec): 5

1. Channel01
2. Channel02
3. Channel03
4. Channel04
5. Channel05
6. Channel06
7. Channel07
8. Channel08

Step 5 Click Apply to save settings.

NOTE

The auxiliary screen shows different channels from the main screen, and the auto sequence shows all channels.

The auxiliary screen will show the people counting information if it is enabled

----End

6.7.7 Logs

6.7.7.1 System Log

Search for log information and export the information of logs.

NOTE

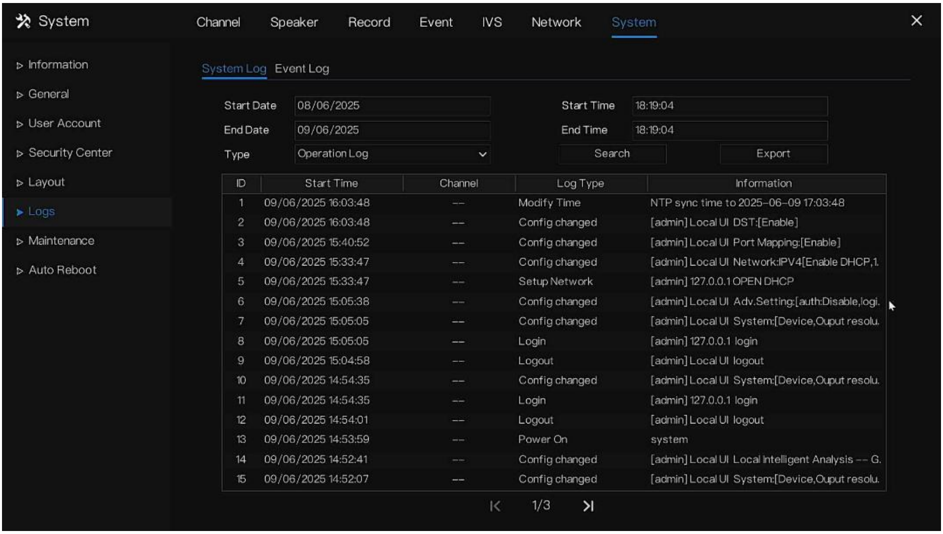
The users should keep the power on when the system parameters are modified. All modifications will be saved for three minutes; otherwise, the setting may fail to be applied.

The operation logs and the alarm logs will be saved to the hard disk when the hard disks are installed, otherwise; the DVR only saves 500 of the latest logs for each log (the operation log and the alarm log), and other logs would be discarded.

Operation Steps

Step 1 Click **Logs** on **Settings > System** to access the logs screen, as shown in Figure 6-115.

Figure 6-115 Log screen



Start Date 08/06/2025
End Date 09/06/2025
Type Operation Log
Start Time 18:19:04
End Time 18:19:04

ID	Start Time	Channel	Log Type	Information
1	09/06/2025 16:03:48	---	Modify Time	NTP sync time to 2025-06-09 17:03:48
2	09/06/2025 16:03:48	---	Config changed	[admin] Local UI DST:[Enable]
3	09/06/2025 15:40:52	---	Config changed	[admin] Local UI Port Mapping:[Enable]
4	09/06/2025 15:33:47	---	Config changed	[admin] Local UI Network:IPV4[Enable DHCP,1.
5	09/06/2025 15:33:47	---	Setup Network	[admin] 127.0.0.1 OPEN DHCP
6	09/06/2025 15:05:38	---	Config changed	[admin] Local UI Adv.Setting:[auth:Disable,logi.
7	09/06/2025 15:05:05	---	Config changed	[admin] Local UI System:[Device,Ouput resolu.
8	09/06/2025 15:05:05	---	Login	[admin] 127.0.0.1 login
9	09/06/2025 15:04:58	---	Logout	[admin] Local UI logout
10	09/06/2025 14:54:35	---	Config changed	[admin] Local UI System:[Device,Ouput resolu.
11	09/06/2025 14:54:35	---	Login	[admin] 127.0.0.1 login
12	09/06/2025 14:54:01	---	Logout	[admin] Local UI logout
13	09/06/2025 14:53:59	---	Power On	system
14	09/06/2025 14:52:41	---	Config changed	[admin] Local UI Local Intelligent Analysis -- G.
15	09/06/2025 14:52:07	---	Config changed	[admin] Local UI System:[Device,Ouput resolu.

Step 2 Set the start date, end date, start time, and end time of the logs on the log screen.

Step 3 Select the logs type from the drop-down list.

Step 4 Click Search to query logs.

Step 5 Click Export to export logs to flash disk.

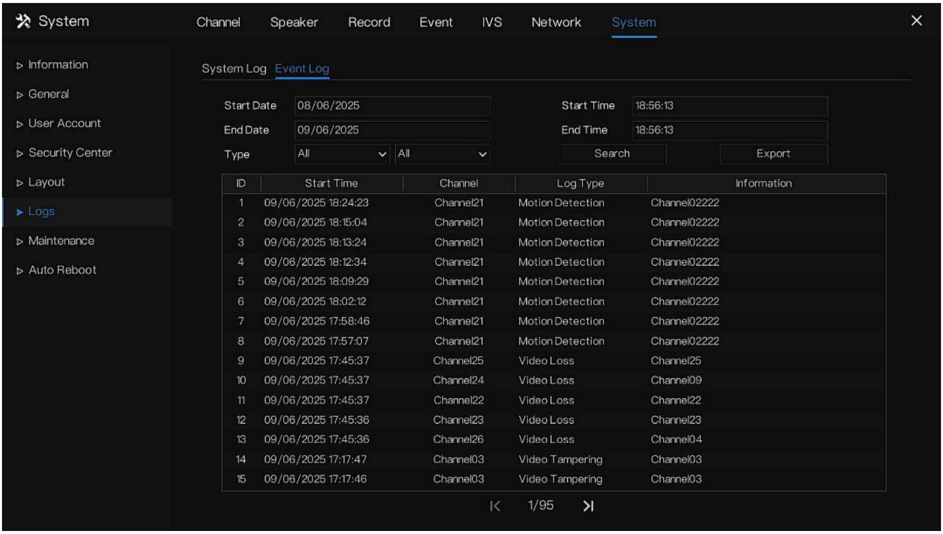
Step 6 The logs can be saved to a flash disk and hard disk at the same time, the newest logs are saved to a flash disk, and the old logs will be transferred to a hard disk.

----End

6.7.7.2 Event Log

Event logs are divided into more detailed types which can be found quickly. Its operation is the same as the system log; please refer to Chapter 6.7.7.1.

Figure 6-116 Event Log



Start Date 08/06/2025

End Date 09/06/2025

Type All All

Start Time 18:56:13

End Time 18:56:13

ID	Start Time	Channel	Log Type	Information
1	09/06/2025 18:24:23	Channel21	Motion Detection	Channel02222
2	09/06/2025 18:15:04	Channel21	Motion Detection	Channel02222
3	09/06/2025 18:13:24	Channel21	Motion Detection	Channel02222
4	09/06/2025 18:12:34	Channel21	Motion Detection	Channel02222
5	09/06/2025 18:09:29	Channel21	Motion Detection	Channel02222
6	09/06/2025 18:02:12	Channel21	Motion Detection	Channel02222
7	09/06/2025 17:58:46	Channel21	Motion Detection	Channel02222
8	09/06/2025 17:57:07	Channel21	Motion Detection	Channel02222
9	09/06/2025 17:45:37	Channel25	Video Loss	Channel25
10	09/06/2025 17:45:37	Channel24	Video Loss	Channel09
11	09/06/2025 17:45:37	Channel22	Video Loss	Channel22
12	09/06/2025 17:45:36	Channel23	Video Loss	Channel23
13	09/06/2025 17:45:36	Channel26	Video Loss	Channel04
14	09/06/2025 17:17:47	Channel03	Video Tampering	Channel03
15	09/06/2025 17:17:46	Channel03	Video Tampering	Channel03

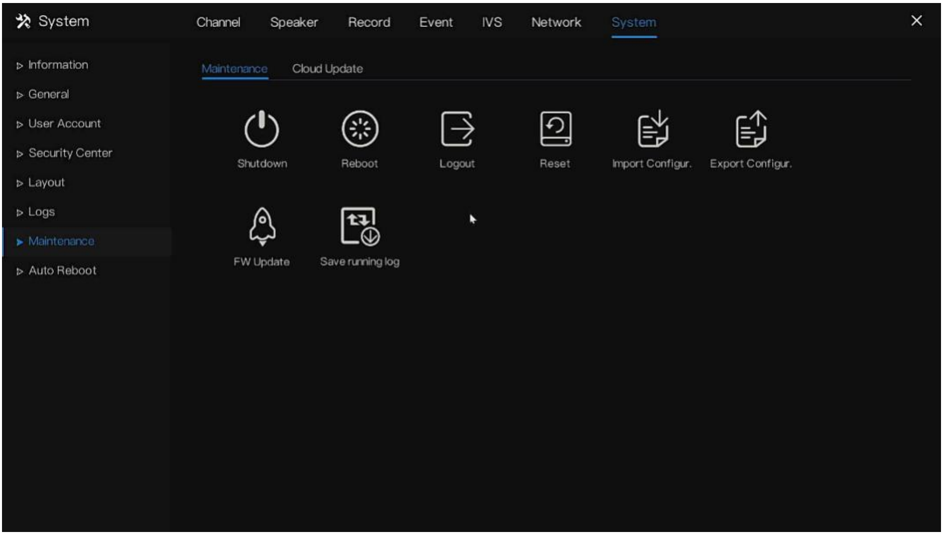
1/95

6.7.8 Maintenance

Operation Steps

Step 1 Click **Maintenance** in the Setting System or menu of the system management screen and choose **Maintenance** to access the maintenance screen, as shown in Figure 6-117.

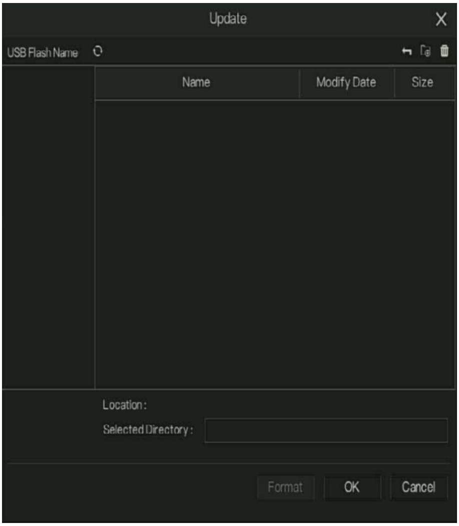
Figure 6-117 Maintenance screen



Step 2 Click **Shutdown, Reboot, Logout, Exit system, Reset, or Update** to operate the DVR if you need to.

Step 3 Click **FW Update** to update the firmware.

Figure 6-118 Firmware update



Step 4 Click **Import Configuration** or **Export Configuration** to view the message "**Are you sure to import the configuration?"** Make sure the flash drive is working.

Step 5 The tips will show on the screen. Click **OK** to ensure choice.

Step 6 Click **Import Config** to import the configuration to the flash drive.

Step 7 Import the configuration, the device will restart immediately.

Step 8 Click **Export Config** to export the configuration from the flash drive.

NOTE

When the DVR finishes updating, the device will restart. It takes about five minutes to update firmware and then will jump to the login interface automatically. If you don't want to wait for five minutes, when the pop-up window shows update 99%, press F5 to refresh the web to go to the login interface.

Network packet capture: the DVR is plugged into the USB disk, the network packet capture, and the relevant parameters of the packet capture. The captured data can be downloaded and used for device problem analysis.

FW Update, firmware update: Plug in the U disk with the update software, and choose the file to update.

Save running log: In the U disk, save the running log.

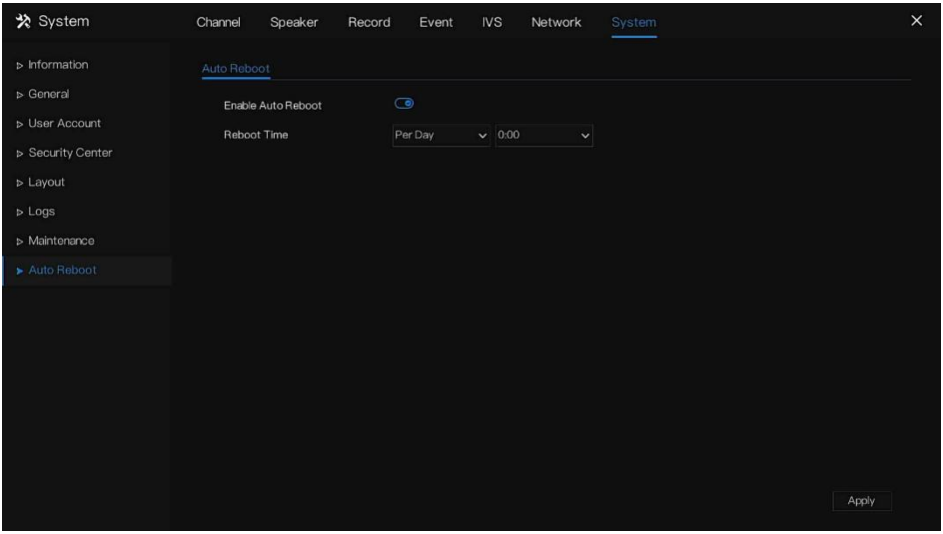
----End

6.7.9 Auto Reboot

Operation Steps

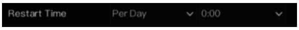
Step 1 Click **Auto Reboot** in the Setting System or menu of the system management screen and choose **Auto Reboot** to access the maintenance screen, as shown in Figure 6-119.

Figure 6-119 Auto reboot screen



Enable Auto Reboot ●

Reboot Time Per Day 0:00

Step 2 Enable the function, restart time is showing as figure .

Restart Time Per Day 0:00

Step 3 Reboot the DVR per **day**, **week**, or **month**.

Step 4 Select the reboot time from the drop-down list. The DVR will be rebooted at the set time.

----End

7 WEB Quick Start

It describes how to access Network Video Recorder remotely using a browser-based web client.

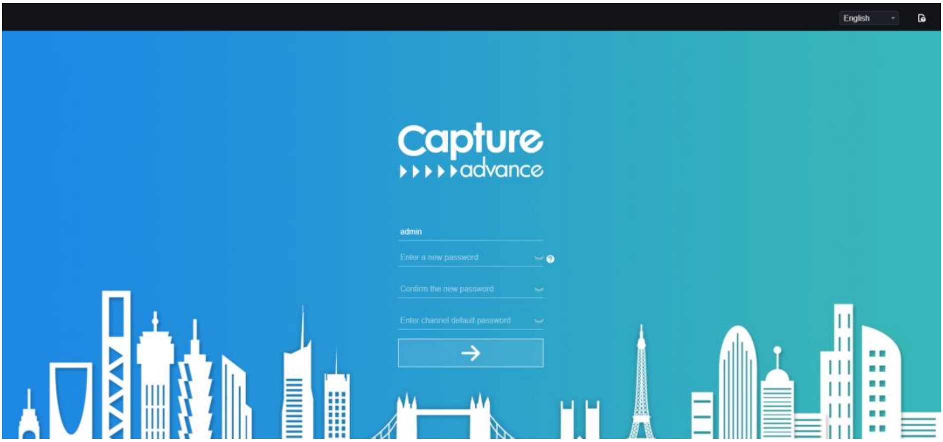
The functions of the web interface are the same as those of the UI system. All functions can be referred to in Chapter 5, UI System Setting.

7.1 Activation

Open the Chrome browser, enter the IP address of the DVR (the default value is 192.168.0.121) in the address box, and press **Enter**.

If you don't set the password at the UI interface, the user needs to activate the device, as shown in

Figure 7-1 Activation

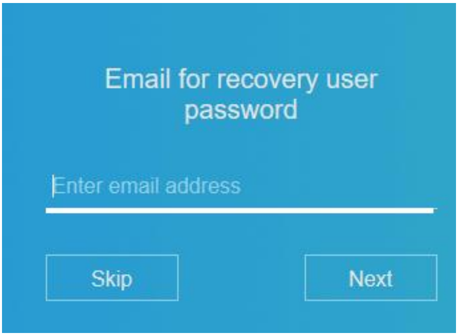


Step 1 Set the password and confirm the password.

Step 2 Input the channel password.

Step 3 There are three methods to recover the password: Setting Email, Security Questions, and QR Code Verification.

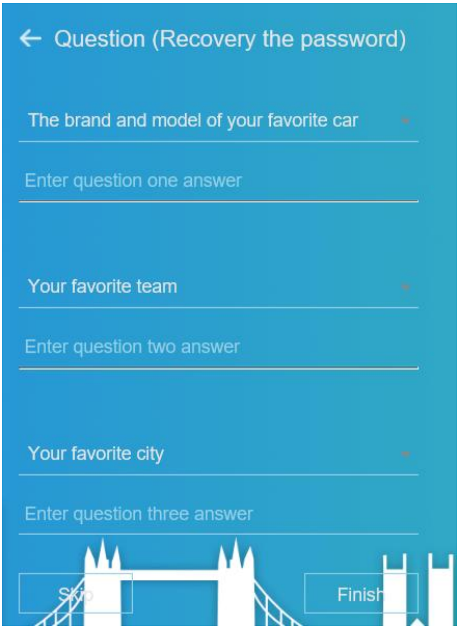
Figure 7-2 Email



Email for recovery user password

Step 4 Set the question to recover the password.

Figure 7-3 Question



Question (Recovery the password)

The brand and model of your favorite car

Enter question one answer

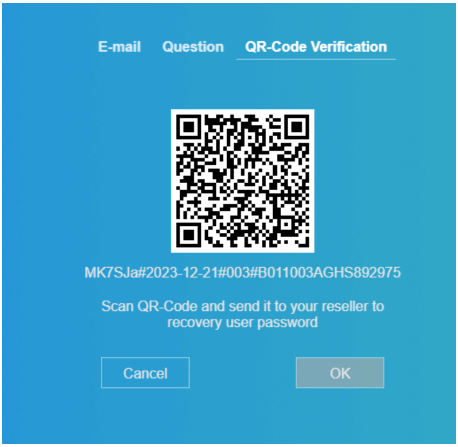
Your favorite team

Enter question two answer

Your favorite city

Enter question three answer

Figure 7-4 QR recovery password



MK7SJa#2023-12-21#003#B011003AGHS892975

Scan QR-Code and send it to your reseller to recovery user password

NOTE

If you don't set the email or question, you can skip the steps.

7.2 Login and Logout

⚠ **CAUTION**

You can use Firefox, Chrome, or Edge to access the web interface.

The Win 7/Win 10 system supports Firefox/Chrome, but the XP system does not.

Browser supports 32-bit systems.

Descriptions of browsers:

To access the client by using Chrome, you need to manually enable NPAPI in the browser according to the following steps:

- In the Chrome address bar, enter chrome://flag/#enable-npapi.
- Go to the experimental features' management page.
- Enable NPAPI Mac and Windows.
- Click **Enable** (NPAPI plugin is enabled).
- Re-launch Chrome.

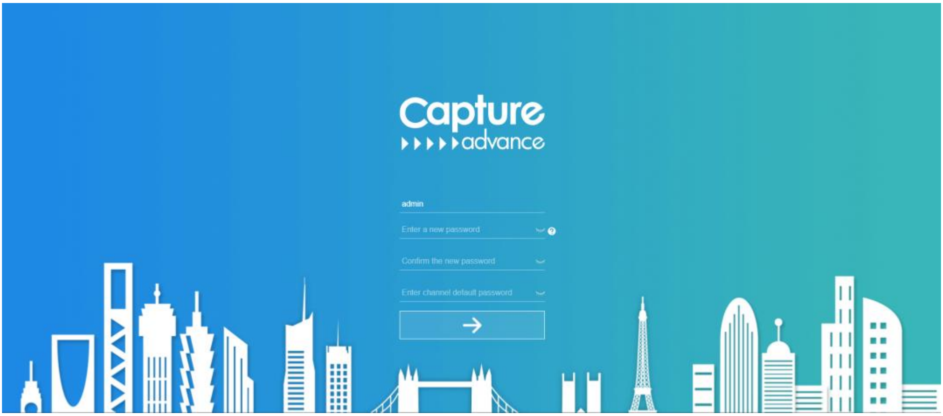
Here we take Chrome as an example for video viewing.

Login

Step 1 Open the Chrome browser, enter the IP address of the DVR (default value: 192.168.0.121) in the address box, and press **Enter**.

The login page is displayed, as shown in Figure 7-5.

Figure 7-5 Login page interface



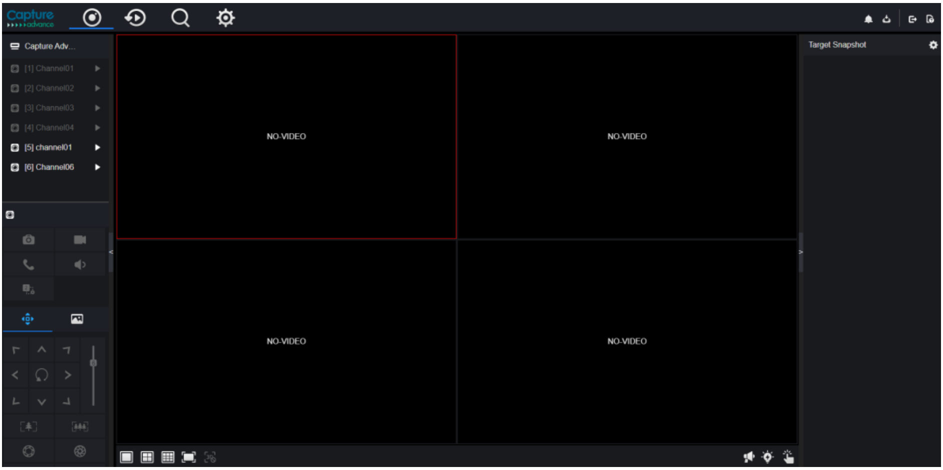
Step 2 Input the user name and password.

NOTE

- The default user name and password are both admin. The password is incorrect more than 3 times: please login again after 5 minutes.
- Users can change the system display language on the login page.
- The modify password page pop-up window would show when logging into the DVR for the first time.

Step 3 Click **Login** to access the homepage, as shown in Figure 7-6.

Figure 7-6 Homepage interface



Logout

To log out of the system, click in the upper right corner of the homepage. The pop-up message shows, "**Would you like to exit?**" Click OK and the login page will display.

Homepage Layout

DVR allows you to use the web interface on a PC for the implementation of such functions as live video, playback, retrieval, setting image parameters access, configuration, PTZ control, and so on. Figure 5-14 shows the overall layout of the interface. For descriptions of the interface, please refer to Table 7-1.

Figure 7-7 Homepage layout

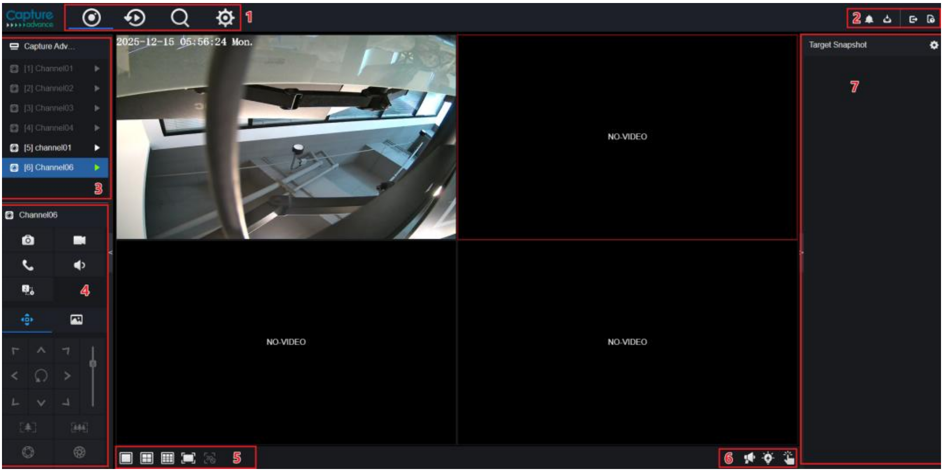


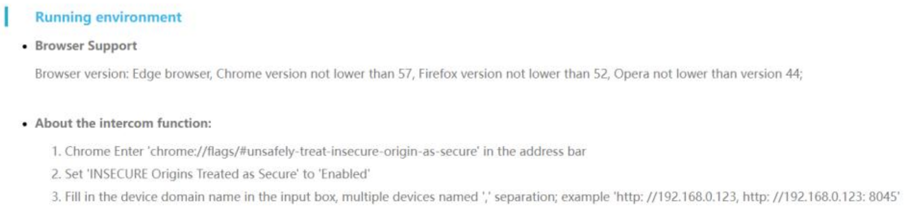
Table 7-1 Descriptions of homepage

No.	Function	Description
1	Function navigation bar	The main functions navigation bar of the device include Live Video, Playback, Event Recording, Attendance, Thermal, AI Application, and System Setting.

2	Alarm	🔔 Alarm notification. Users can tick pop-up messages to monitor system alarms and channel alarms. 📥 Backup download list. ⎋ Logout. Users can click **Logout** to exit the current account and return to the login interface. ❓ Help. Help with the running environment, plug-in installation, and activation.
3	Device’s list	Display a list of the channels of the managed DVR and the channels managed by the DVR.
4	Channel Operation	Includes snapshot, record, stream switch, and audio on/off. PTZ control button. Click ✥ to show PTZ control buttons in zone 10; you can control the PTZ equipment in the current channels. That function is only used for IP dome cameras. Image parameter button. Click 🖼 to show color parameter setting buttons in zone 9, you can set and adjust the color parameters, for example, brightness, contrast, saturation, and sharpness. Click **More** to access image settings.
5	Layouts	Select the one-screen, four-screen, nine-screen, or sixteen-screen to switch the layout.
6	Manual Operations	📢 Broadcast. When you add the IP speakers to the DVR, users can broadcast the local audio file to the alarm. 💡 Manual control light, support flashlight, red and blue light, and white light. If the camera has a light, you can control the light manually. 👆 Manual alarm. Trigger and close the external alarm device manually.

7	Target snapshot	The snapshots will show on live video; you can click ⚙ to set the target snapshot filter, as shown in Figure 7-10.

Figure 7-8 Help



Running environment

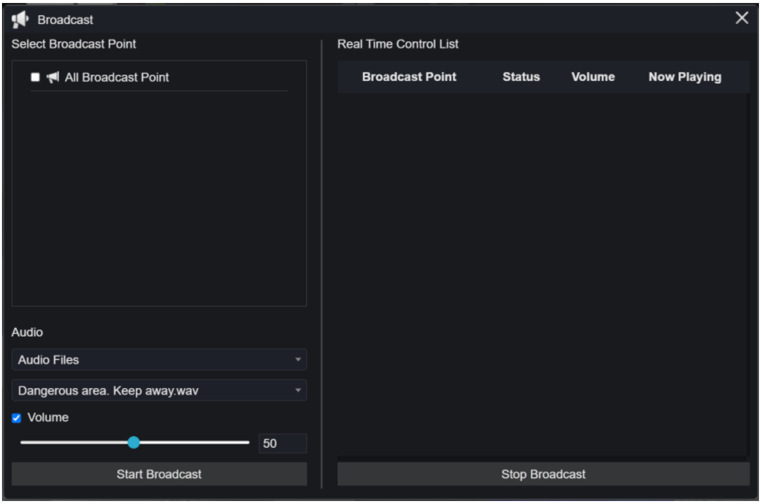
- **Browser Support**

  Browser version: Edge browser, Chrome version not lower than 57, Firefox version not lower than 52, Opera not lower than version 44;

- **About the intercom function:**

  1. Chrome Enter 'chrome://flags/#unsafely-treat-insecure-origin-as-secure' in the address bar
  2. Set 'INSECURE Origins Treated as Secure' to 'Enabled'
  3. Fill in the device domain name in the input box, multiple devices named ',' separation; example 'http: //192.168.0.123, http: //192.168.0.123: 8045'

Figure 7-9 Broadcast

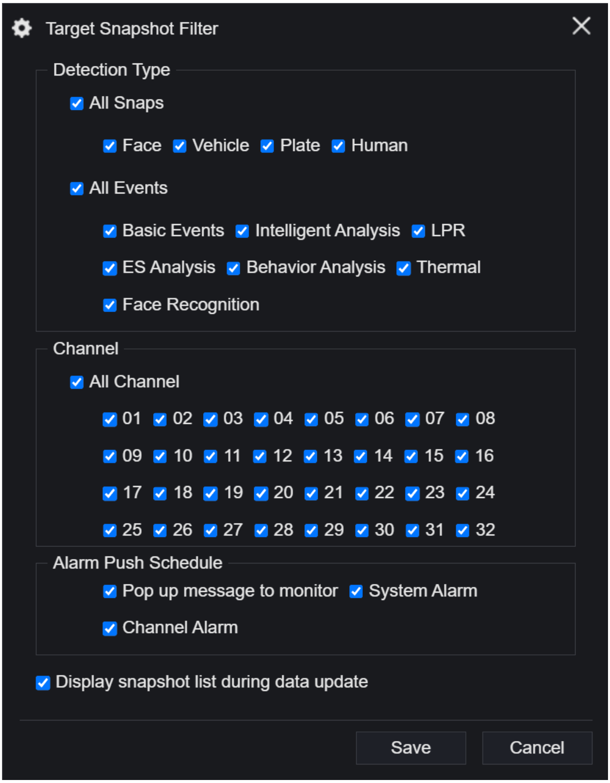


Audio: Audio Files

Dangerous area. Keep away.wav

☑ Volume: 50

Figure 7-10 Target snapshot filter



Target Snapshot Filter

Detection Type

☑ All Snaps

☑ Face ☑ Vehicle ☑ Plate ☑ Human

☑ All Events

☑ Basic Events ☑ Intelligent Analysis ☑ LPR

☑ ES Analysis ☑ Behavior Analysis ☑ Thermal

☑ Face Recognition

Channel

☑ All Channel

☑ 01 ☑ 02 ☑ 03 ☑ 04 ☑ 05 ☑ 06 ☑ 07 ☑ 08

☑ 09 ☑ 10 ☑ 11 ☑ 12 ☑ 13 ☑ 14 ☑ 15 ☑ 16

☑ 17 ☑ 18 ☑ 19 ☑ 20 ☑ 21 ☑ 22 ☑ 23 ☑ 24

☑ 25 ☑ 26 ☑ 27 ☑ 28 ☑ 29 ☑ 30 ☑ 31 ☑ 32

Alarm Push Schedule

☑ Pop up message to monitor ☑ System Alarm

☑ Channel Alarm

☑ Display snapshot list during data update

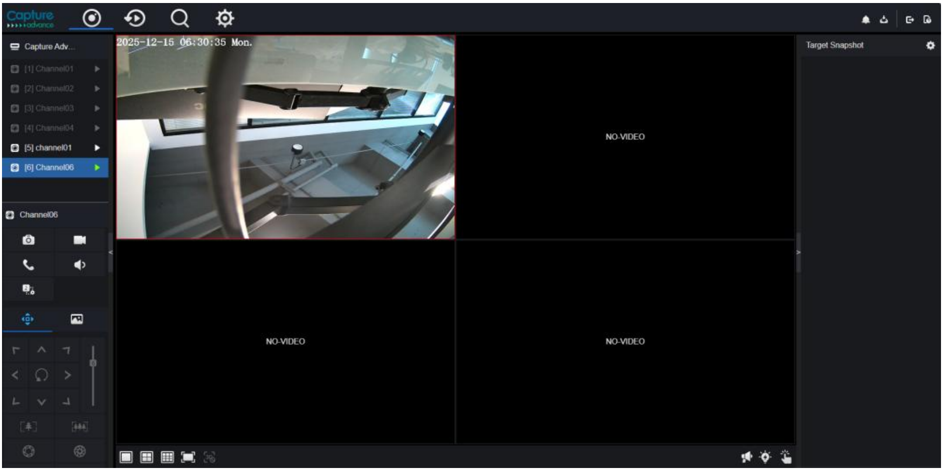
----End

7.2.2 Live Video

Descriptions

After logging in to the device, click online channel; you can view the real-time videos, as shown in Figure 7-11.

Figure 7-11 Real-time videos interface



----End

7.2.3 Channel Operation

Descriptions

Channel operation includes snapshot, record, stream switch, and audio on/off. Table 7-2 describes the operations.

Table 7-2 Descriptions of homepage

Buttons	Button description	How to operate
📷	Snapshot	Click the button to take snapshots of the current image.
🎥	Record	Click the button to start recording, and click the button again to stop recording.

Buttons	Button description	How to operate
☎	Talkback	If the channel cameras have a louder mic, click talk back and communicate with the camera at the web interface. The web should set the intercom function in advance (refer to Help).
2	Switch stream	Click the button to switch stream 1 (mainstream) and stream 2 (substream).
🔈	Enable/Disable video.	Click the button to enable the audio, and click again to disable the audio.

----End

7.2.4 PTZ Control and Setting

Descriptions

The PTZ control and setting function applies only to the network dome or camera connected to an external PTZ.

PTZ Setting

If a network dome or a camera connected to PTZ had been added to the DVR channel, users can control the PTZ rotation to adjust their shooting angle when they are viewing the video. This allows you to perform omnidirectional video surveillance.

Click ✥; the PTZ operation and setting interface is as shown in Figure 7-12. Table 7-3 describes the operations.

Figure 7-12 PTZ control interface

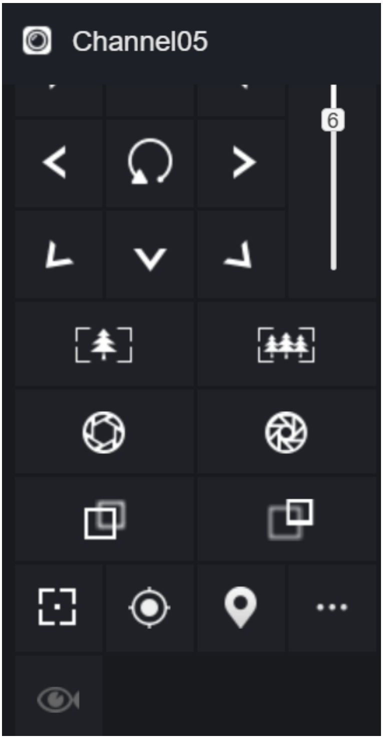
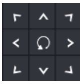


Table 7-3 Device parameters

Buttons	Button description	How to operate
	Direction key	Click the button to control the omnidirectional movement of the PTZ. : For analog cameras, click to enter the main menu of cameras.
	Speed slider	Drag the slider to adjust the value of PTZ rotation speed.
	Zoom in	Click the buttons to adjust the focal length.

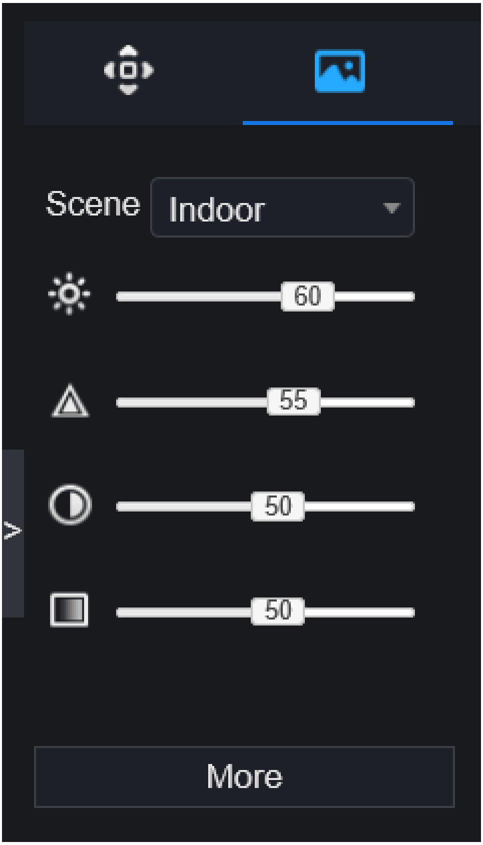
Buttons	Button description	How to operate
⛶	Zoom out	
◎	Iris+	Click the buttons to adjust the aperture.
⊛	Iris-	
⧉	Far focus	Click the buttons to adjust the focal length.
⧉	Near focus	
⛶	Autofocus	Click the button to focus automatically.
◎	Home preset	N/A
📍	Preset	The camera sets the tour, click the button and the dome camera rotates as the setting.
…	More	More settings, scan, and tour
👁	Fisheye	The DVR can support this function.

7.2.5 Image Setting

Descriptions

The image setting can adjust the scene, brightness, sharpness, contrast, and saturation. Click 🖼 to access the image setting, as shown in Figure 7-13. Table 7-4 describes the operations.

Figure 7-13 Image parameter interface



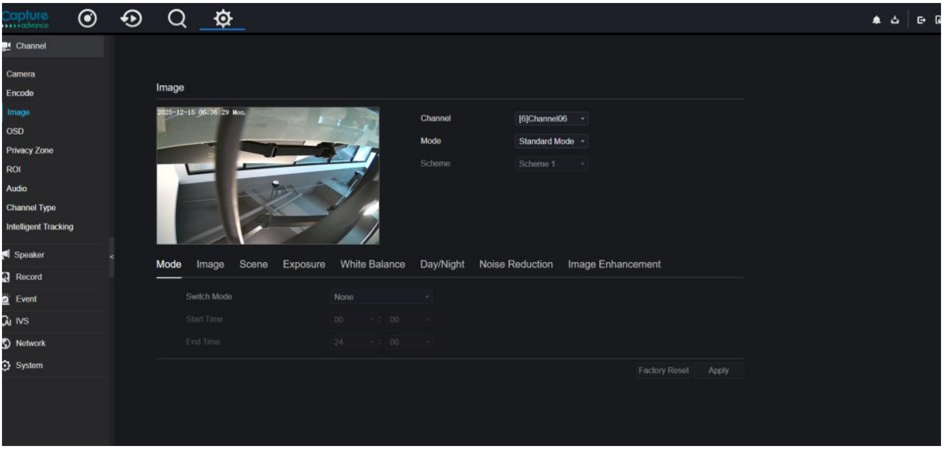
Scene Indoor

Table 7-4 Device parameters

Buttons	Button description	How to operate
☼	Brightness	Click the button to adjust the image brightness.
△	Sharpness	Click the button to adjust the image definition.
◐	Contrast	Click the button to adjust the transparency of the image.
▣	Saturation	Click the button to adjust the chromatic purity of the image.

Clicking More will give you access to the system sensor settings. As shown in Figure 7-14, for more details, please refer to *Chapter 6.1.3* Image.

Figure 7-14 Image setting interface



Channel [6]Channel06
Mode Standard Mode
Scheme Scheme 1

Switch Mode None
Start Time 00 : 00
End Time 24 : 00

----End

7.2.6 Layout

Click □ ⊞ ▦ ▦ at the bottom left corner of the real-time videos interface; the buttons indicate 1 screen, 4 screens, 9 screens, and 16 screens from left to right. The device with more channels can support 16-screen layouts.

----End

7. 3 Playback

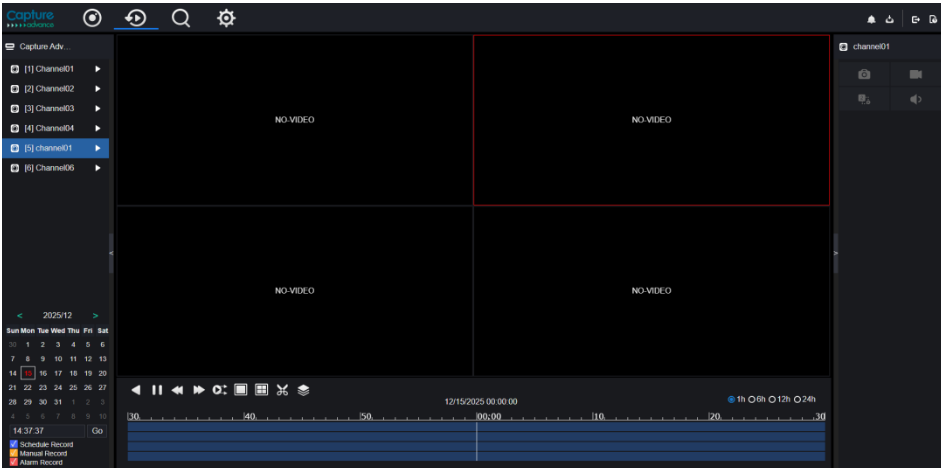
7.3.1 Video Playback

Video playback refers to the playing of videos stored on local hard disks.

Procedure

Step 1 Click In the function navigation bar, the video playback interface is displayed, as shown in Figure 7-15.

Figure 7-15 Video playback



Step 2 Select a channel. Click a device in the device list. A selected device is marked with ▶.

The unselected device is marked with ▶.

Step 3 Select a date from the calendar at the left bottom. The date will be colored if it has a record as shown in the upper figure.

Step 4 Tick the type of record, such as schedule record, manual record, and alarm record.

Step 5 Display videos.

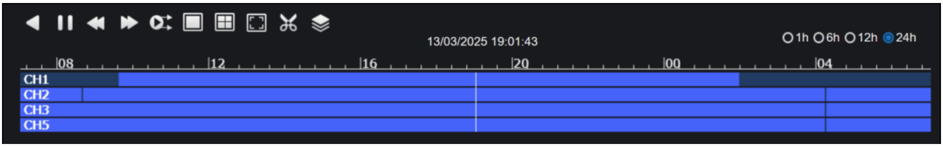
After a device and date are selected, video information is displayed below the video pane. The time scale above the file axis shows the different time points of video recording. The time in blue in the middle is the time of the video playing.

The file axis displays videos. The blue file axis indicates video exists; the grey file axis indicates no video exists. You can drag the axis to play the recording quickly.

Step 6 Play a video.

You can play a video after selecting a device and date. Figure 7-16 shows the control bar of video playback.

Figure 7-16 Control bar



◀ Reversed.

❚❚ Play/Pause.

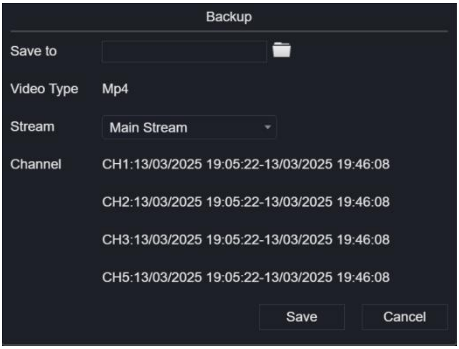
⏪ ⏩ Triple speed.

⇄ Sync/Async. You can set the different channels to play synchronously or asynchronously. Sync mode indicates the selected channels play video synchronously. Async mode indicates users play different record periods.

⊞ Split-screen. One or four screens.

✂ Backup. Click the icon to start up the recording and drag the time bar to quickly back up. Click again to make sure of the backup.

Figure 7-17 Backup



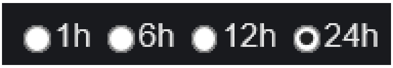
Backup

Save to

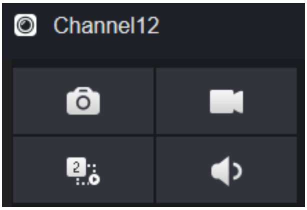
Video Type: Mp4

Stream: Main Stream

Channel: CH1:13/03/2025 19:05:22-13/03/2025 19:46:08
CH2:13/03/2025 19:05:22-13/03/2025 19:46:08
CH3:13/03/2025 19:05:22-13/03/2025 19:46:08
CH5:13/03/2025 19:05:22-13/03/2025 19:46:08



Types of time bar/interval.



The user can operate the record as same as live video.

----End

7.4 Alarm Search

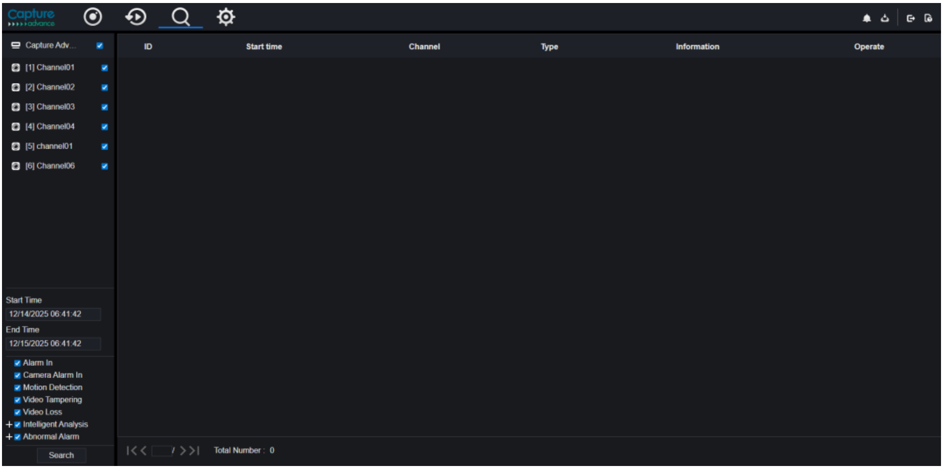
You can search for channel alarms and system alarms in the alarm search interface.

7.4.1 Channel Alarm

Procedure

Step 1 Click on the function navigation bar and the channel alarm interface is displayed, as shown in Figure 7-18.

Figure 7-18 Channel alarm interface



☑ Capture Adv...
[1] Channel01 ☑
[2] Channel02 ☑
[3] Channel03 ☑
[4] Channel04 ☑
[5] channel01 ☑
[6] Channel06 ☑

Start Time: 12/14/2025 06:41:42
End Time: 12/15/2025 06:41:42

☑ Alarm In
☑ Camera Alarm In
☑ Motion Detection
☑ Video Tampering
☑ Video Loss
+ ☑ Intelligent Analysis
+ ☑ Abnormal Alarm

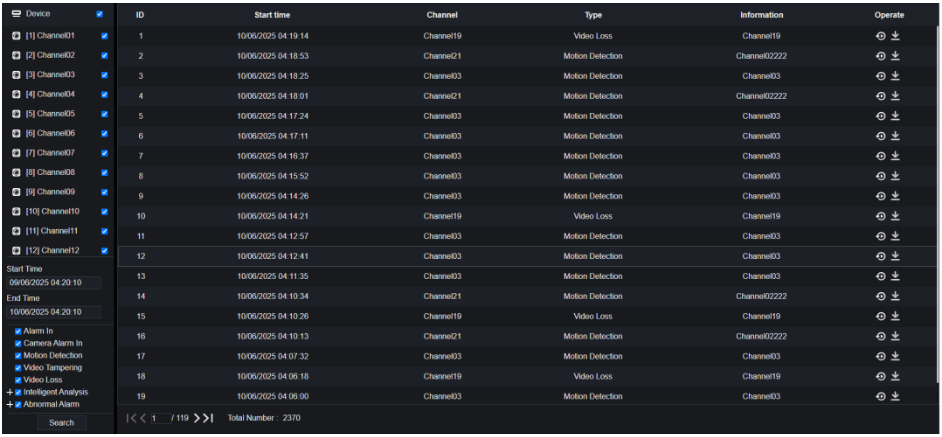
ID	Start time	Channel	Type	Information	Operate

Total Number : 0

Step 2 Choose the alarm type to search.

Step 3 Click **Search**. The result will be displayed as shown in Figure 7-19.

Figure 7-19 Channel alarm result



Device ☑
- [1] Channel01 ☑
- [2] Channel02 ☑
- [3] Channel03 ☑
- [4] Channel04 ☑
- [5] Channel05 ☑
- [6] Channel06 ☑
- [7] Channel07 ☑
- [8] Channel08 ☑
- [9] Channel09 ☑
- [10] Channel10 ☑
- [11] Channel11 ☑
- [12] Channel12 ☑

Start Time: 09/06/2025 04:20:10

End Time: 10/06/2025 04:20:10

- ☑ Alarm In
- ☑ Camera Alarm In
- ☑ Motion Detection
- ☑ Video Tampering
- ☑ Video Loss
- + ☑ Intelligent Analysis
- + ☑ Abnormal Alarm

Search

ID	Start time	Channel	Type	Information	Operate
1	10/06/2025 04:19:14	Channel19	Video Loss	Channel19	↺ ⤓
2	10/06/2025 04:18:53	Channel21	Motion Detection	Channel02222	↺ ⤓
3	10/06/2025 04:18:25	Channel03	Motion Detection	Channel03	↺ ⤓
4	10/06/2025 04:18:01	Channel21	Motion Detection	Channel02222	↺ ⤓
5	10/06/2025 04:17:24	Channel03	Motion Detection	Channel03	↺ ⤓
6	10/06/2025 04:17:11	Channel03	Motion Detection	Channel03	↺ ⤓
7	10/06/2025 04:16:37	Channel03	Motion Detection	Channel03	↺ ⤓
8	10/06/2025 04:15:52	Channel03	Motion Detection	Channel03	↺ ⤓
9	10/06/2025 04:14:26	Channel03	Motion Detection	Channel03	↺ ⤓
10	10/06/2025 04:14:21	Channel19	Video Loss	Channel19	↺ ⤓
11	10/06/2025 04:12:57	Channel03	Motion Detection	Channel03	↺ ⤓
12	10/06/2025 04:12:41	Channel03	Motion Detection	Channel03	↺ ⤓
13	10/06/2025 04:11:35	Channel03	Motion Detection	Channel03	↺ ⤓
14	10/06/2025 04:10:34	Channel21	Motion Detection	Channel02222	↺ ⤓
15	10/06/2025 04:10:26	Channel19	Video Loss	Channel19	↺ ⤓
16	10/06/2025 04:10:13	Channel21	Motion Detection	Channel02222	↺ ⤓
17	10/06/2025 04:07:32	Channel03	Motion Detection	Channel03	↺ ⤓
18	10/06/2025 04:06:18	Channel19	Video Loss	Channel19	↺ ⤓
19	10/06/2025 04:06:00	Channel03	Motion Detection	Channel03	↺ ⤓

|< < 1 / 119 > >| Total Number : 2370

NOTE

Click |< < 1 /6 > >| to select the page of the alarm list.

20 alarm messages are shown on every page.

----End

8 System Setting

The system setting allows you to set Channel, Speaker, Record, Event, IVS, Network, and System.

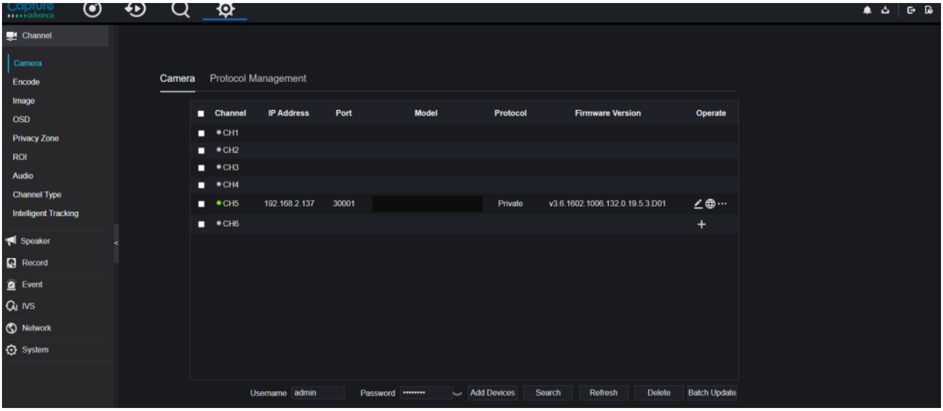
8.1 Channel

Users can set parameters about the camera, encode, sensor settings, OSD, and privacy zone.

8.1.1 Camera

Step 1 On the **System Setting** screen, choose **Channel > Camera** to access the camera interface, as shown in Figure 8-1.

Figure 8-1 Camera interface



□	Channel	IP Address	Port	Model	Protocol	Firmware Version	Operate
□	● CH1						
□	● CH2						
□	● CH3						
□	● CH4						
□	● CH5	192.168.2.137	30001	[redacted]	Private	v3.6.1602.1006.132.0.19.5.3.D01	
□	● CH6						+

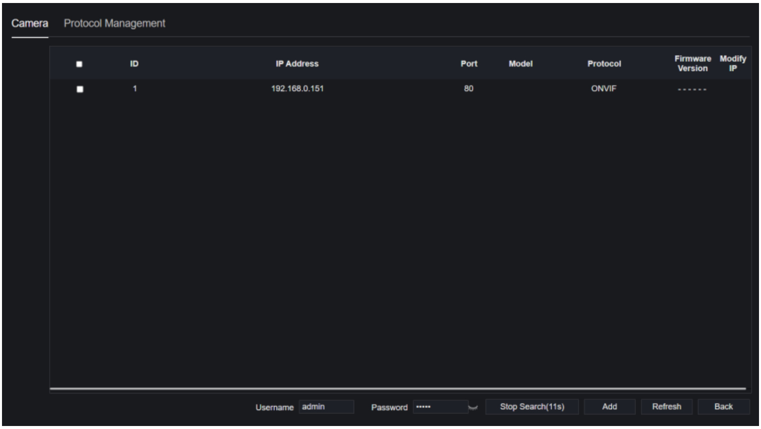
Username admin Password ••••••••

Step 2 Input username and password (the default username and password both are admin), and click/add cameras automatically.

Step 3 Click Search to search cameras at the same LAN as DVR, as shown in Figure 8-2.

Choose the cameras, input the username and password, and click **Add** to add new cameras.

Figure 8-2 Device search



■	ID	IP Address	Port	Model	Protocol	Firmware Version	Modify IP
■	1	192.168.0.151	80		ONVIF	------	

Username admin Password •••••

Step 4 Click Back to go back to the camera interface.

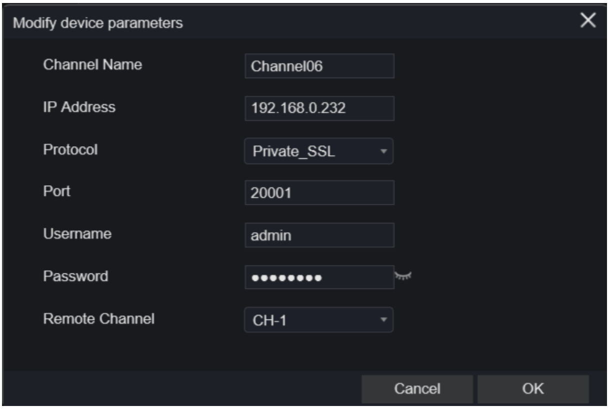
Step 5 Click Refresh to refresh the camera status.

Step 6 Choose the cameras and click Delete to delete.

Step 7 Click Batch Update to update all selected cameras at once; the pop-up window will show to select software.

Step 8 Click ✎ to modify the information of device parameters, as shown in Figure 8-3.

Figure 8-3 Modify device parameters



Channel Name: Channel06

IP Address: 192.168.0.232

Protocol: Private_SSL

Port: 20001

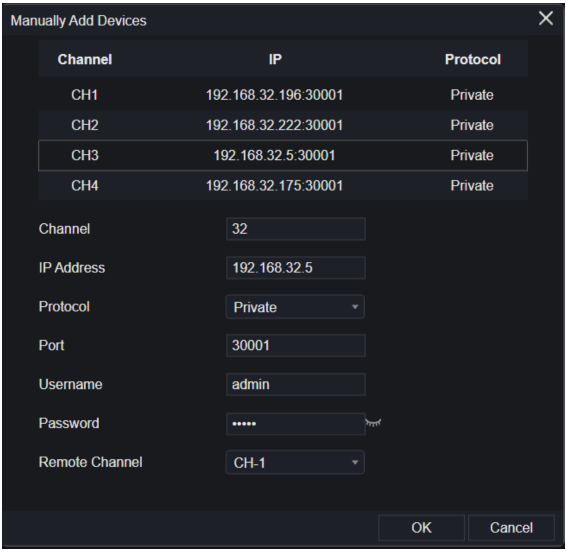
Username: admin

Password: ●●●●●●●●●

Remote Channel: CH-1

Step 9 Click + to add the camera manually, and click the added channel to copy information to add so that the user just modifies some information quickly, as shown in Figure 8-4.

Figure 8-4 Add camera manually



Channel	IP	Protocol
CH1	192.168.32.196:30001	Private
CH2	192.168.32.222:30001	Private
CH3	192.168.32.5:30001	Private
CH4	192.168.32.175:30001	Private

Channel: 32

IP Address: 192.168.32.5

Protocol: Private

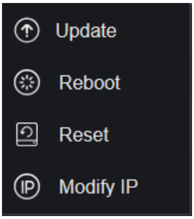
Port: 30001

Username: admin

Password: •••••

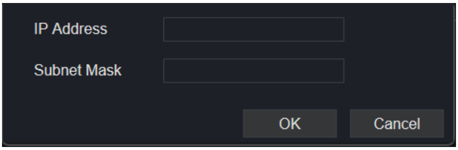
Remote Channel: CH-1

Step 10 Click e to access the web immediately.



Step 11 Click ••• to update, reboot, or reset the selected camera, as shows. The pop-up message "Are you sure to restart the device?" "Are you sure to reset? Reserve IP Address" would respectively show.

Figure 8-5 Modify IP



IP Address

Subnet Mask

OK Cancel

NOTE

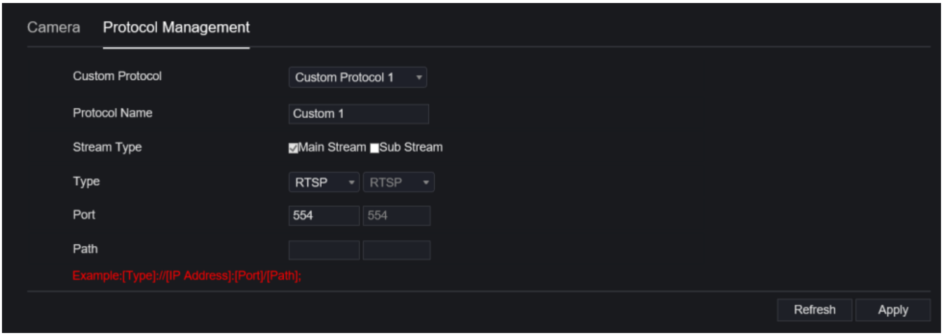
● It indicates the camera is online. Users can view the live video immediately.

● It indicates the camera is offline. It may not be connected to the network, or the password may be incorrect. Access to the modified device parameters interface to change.

8.1.1.1 Protocol Management

Set the Protocol Management; users can add different protocol cameras to the DVR.

Figure 8-6 Protocol management



Camera | Protocol Management

Custom Protocol: Custom Protocol 1

Protocol Name: Custom 1

Stream Type: ☑Main Stream ■Sub Stream

Type: RTSP RTSP

Port: 554 554

Path:

Example:[Type]://[IP Address]:[Port]/[Path];

Refresh Apply

Step 1 Click **Channel > Camera > RTSP Connection.**

Step 2 Choose the Custom Protocol from the drop-down list; 16 kinds of protocols can be set.

Step 3 Input the protocol name.

Step 4 Tick mainstream and substream. The mainstream shows the image on full-screen live video. The substream shows the image on the split screen. If you just tick mainstream, the channel will not show the image on the split screen.

Step 5 Choose the type of protocol. The default value is RTSP.

Step 6 Input the port of the IP camera.

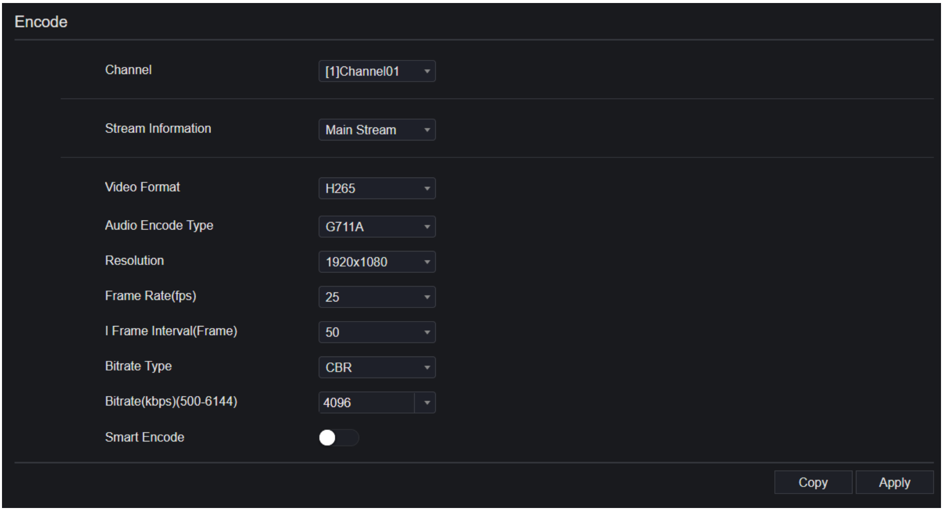
Step 7 Input the path, which is decided by the manufacturer of the cameras.

Step 8 Click Apply to save the settings.

8.1.2 Encode

Step 1 On the **System Setting** screen, choose **Channel > Encode** to access the encode interface, as shown in Figure 8-7.

Figure 8-7 Encode interface



Encode

Channel: [1]Channel01

Stream Information: Main Stream

Video Format: H265

Audio Encode Type: G711A

Resolution: 1920x1080

Frame Rate(fps): 25

I Frame Interval(Frame): 50

Bitrate Type: CBR

Bitrate(kbps)(500-6144): 4096

Smart Encode: ○

Step 2 Select a channel from the drop-down list.

Step 3 Select stream information, encode type, resolution, frame rate, bitrate control, and bitrate from the drop-down list.

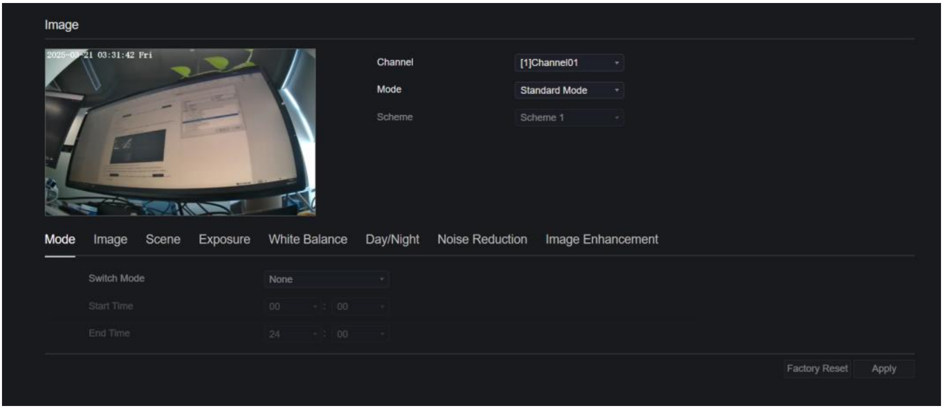
Step 4 Click Copy to choose another camera to copy settings. Click Apply to save the settings.

----End

8.1.3 Image

Step 1 On the **System Setting** screen, choose **Channel > Image** to access the Image interface, as shown in Figure 8-8.

Figure 8-8 Image interface



Image

Channel: [1]Channel01

Mode: Standard Mode

Scheme: Scheme 1

Mode | Image | Scene | Exposure | White Balance | Day/Night | Noise Reduction | Image Enhancement

Switch Mode: None

Start Time: 00 : 00

End Time: 24 : 00

Factory Reset | Apply

Step 2 Select a channel and scene from the drop-down list. Choose the Debug mode to modify the parameters of the image.

Step 3 Set image parameters, like mode, image, scene, exposure, white balance, day/night, noise reduction, image enhancement, and so on. For the detailed information, please refer to the IP cameras' image settings.

Step 4 Click Factory Reset to reset the image settings. Click Apply to save the settings.

NOTE

Brightness: It indicates the total brightness of an image. As the value increases, the image becomes brighter.

Sharpness: It indicates the border sharpness of an image. As the value increases, the borders become clearer, and the number of noise points increases.

Saturation: It indicates the color saturation of an image. As the value increases, the image becomes more colorful.

Contrast: It indicates the measurement of different brightness levels between the brightest white and darkest black in an image. The larger the difference range is, the greater the contrast is; the smaller the difference range is, the smaller the contrast is.

Scene: it includes indoor, outdoor, and default. Mirror includes normal, horizontal, vertical, horizontal + vertical.

Exposure: It includes mode, max shutter, meter area, and max gain.

White balance: It includes tungsten, fluorescent, daylight, shadow, manual, etc.

Day-night: It transits from day to night or switches modes.

Noise reduction: It includes 2D NR and 3D NR.

Enhance image: It includes WDR, HLC, BLC, defog, and anti-shake.

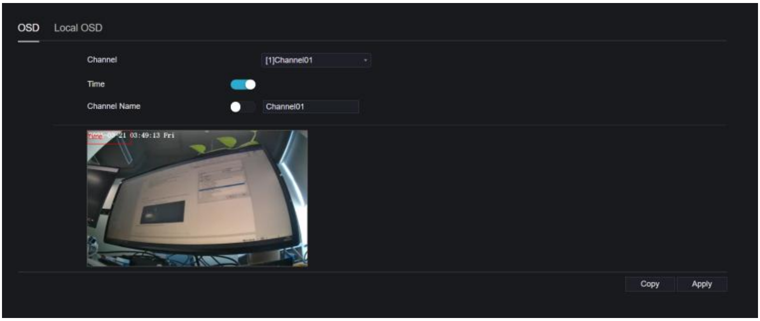
Zoom focus: Zoom and focus.

----End

8.1.4 OSD

Step 1 On the **System Setting** screen, choose **Channel > OSD** to access the OSD interface, as shown in Figure 4-10

Figure 8-9 OSD interface



Channel [1]Channel01

Time ●

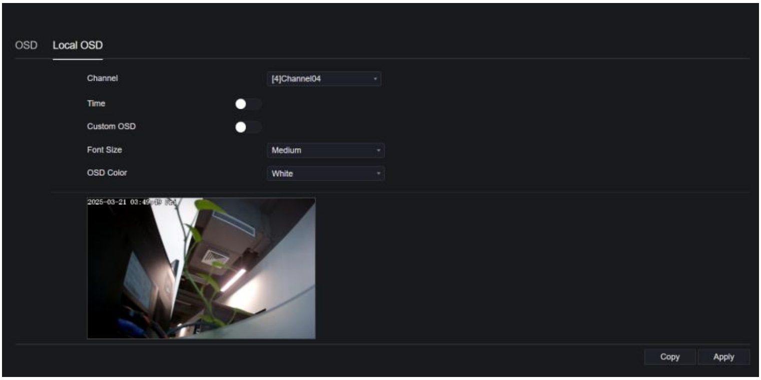
Channel Name ○ Channel01

Step 2 Select a channel and scene from the drop-down list.

Step 3 Enable time and channel name. You can set the channel name. Drag the icon of the Channel Name or Date and Time to move, and select the location.

Step 4 Click Copy to choose other cameras to copy settings. Click Apply to save the settings.

Figure 8-10 Local OSD



Channel: [4]Channel04

Time

Custom OSD

Font Size: Medium

OSD Color: White

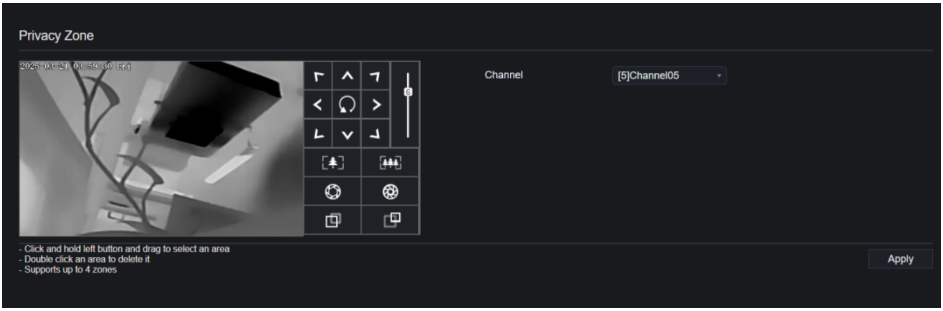
Users can enable the time and custom OSD on local videos; this OSD can’t be shown on the backup recording.

----End

8.1.5 Privacy Zone

Step 1 On the **System Setting** screen, choose **Channel > Privacy Zone** to access the privacy zone interface, as shown in Figure 8-11.

Figure 8-11 Privacy interface



Privacy Zone

Channel [5]Channel05

- Click and hold left button and drag to select an area
- Double click an area to delete it
- Supports up to 4 zones

Step 2 Select a channel from the drop-down list.

Step 3 Drag the mouse to select an area to cover with a rectangular frame. You can set less than four areas to be covered. A double click would delete the area.

Step 4 PTZ can be used for adjusting the IP dome cameras.

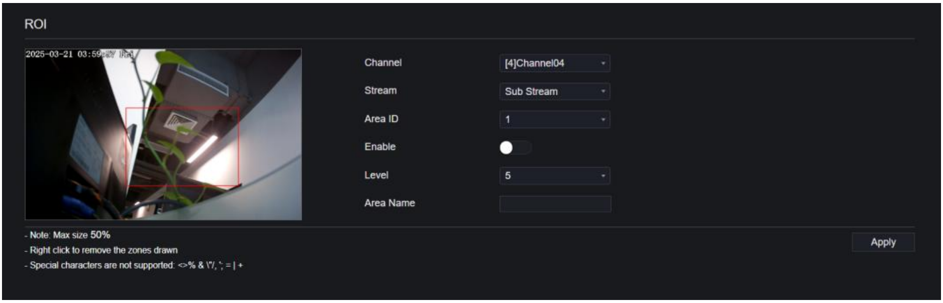
Step 5 Click Copy to choose other cameras to copy settings. Click Apply to save the settings.

----End

8.1.6 ROI

ROI (Region of Interest). Choose channel, stream, and area ID, and draw the area. Set the level; five levels can be chosen. Set the area name, and click “Apply” to save the settings.

Figure 8-12 ROI



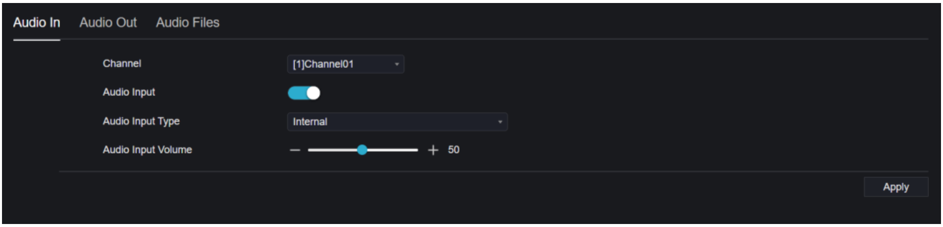
Channel: [4]Channel04
Stream: Sub Stream
Area ID: 1
Enable: ○
Level: 5
Area Name:

- Note: Max size 50%
- Right click to remove the zones drawn
- Special characters are not supported: <>% & \"/, '; = | +

8.1.7 Audio (Only for Some Models)

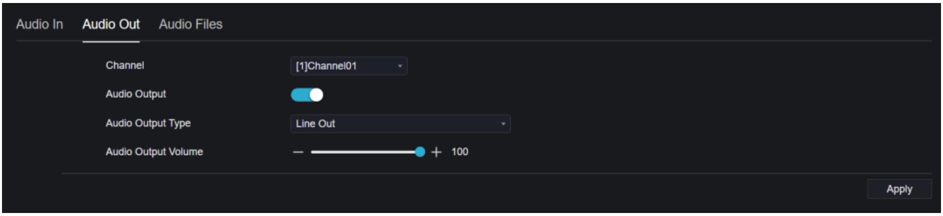
Users can set the audio parameters of the channel. Audio in, audio out, and audio files. For detailed information, please refer to *Chapter 6.1.8 Audio (Only for Some Models)*.

Figure 8-13 Audio in



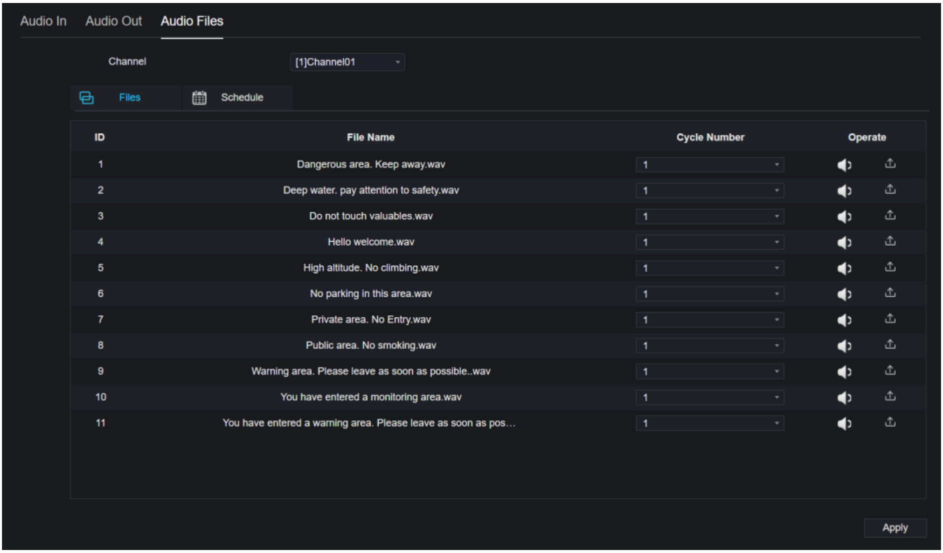
Channel: [1]Channel01
Audio Input: ●
Audio Input Type: Internal
Audio Input Volume: 50

Figure 8-14 Audio out



Channel: [1]Channel01
Audio Output: ●
Audio Output Type: Line Out
Audio Output Volume: 100

Figure 8-15 Audio files



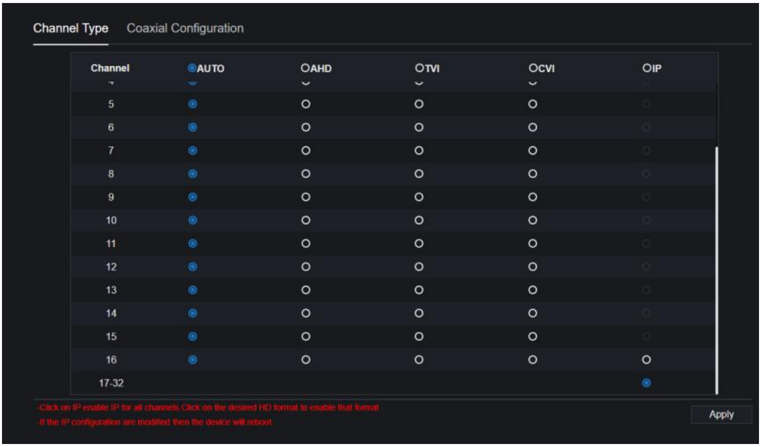
Channel [1]Channel01

ID	File Name	Cycle Number	Operate
1	Dangerous area. Keep away.wav	1	🔈 ⇪
2	Deep water. pay attention to safety.wav	1	🔈 ⇪
3	Do not touch valuables.wav	1	🔈 ⇪
4	Hello welcome.wav	1	🔈 ⇪
5	High altitude. No climbing.wav	1	🔈 ⇪
6	No parking in this area.wav	1	🔈 ⇪
7	Private area. No Entry.wav	1	🔈 ⇪
8	Public area. No smoking.wav	1	🔈 ⇪
9	Warning area. Please leave as soon as possible..wav	1	🔈 ⇪
10	You have entered a monitoring area.wav	1	🔈 ⇪
11	You have entered a warning area. Please leave as soon as pos…	1	🔈 ⇪

8.1.8 Channel Type

For the analog cameras, users can set the channel type for these, AUTO, AHD, TVI, CVI, or IP. If the IP mode is enabling, it works for all channels. The IP configuration are modified then the device will be reboot.

Figure 8-16 Channel type



Channel Type Coaxial Configuration

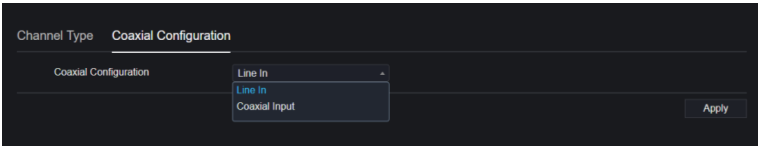
Channel	●AUTO	○AHD	○TVI	○CVI	○IP
5	●	○	○	○	○
6	●	○	○	○	○
7	●	○	○	○	○
8	●	○	○	○	○
9	●	○	○	○	○
10	●	○	○	○	○
11	●	○	○	○	○
12	●	○	○	○	○
13	●	○	○	○	○
14	●	○	○	○	○
15	●	○	○	○	○
16	●	○	○	○	○
17-32					●

-Click on IP enable IP for all channels.Click on the desired HD format to enable that format

-If the IP configuration are modified then the device will reboot

Apply

Figure 8-17 Coaxial configuration



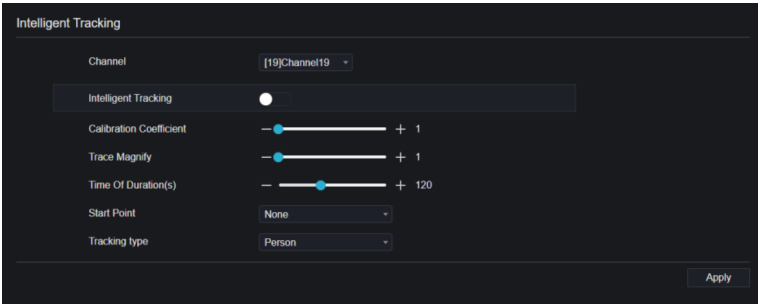
Channel Type Coaxial Configuration

Coaxial Configuration: Line In

8.1.9 Intelligent Tracking (Only for Some Models)

This function can only be used for high-speed dome cameras. It works with the PTZ function.

Figure 8-18 Intelligent tracking



Intelligent Tracking

Channel: [19]Channel19

Intelligent Tracking: ○

Calibration Coefficient: 1

Trace Magnify: 1

Time Of Duration(s): 120

Start Point: None

Tracking type: Person

The detailed information please refer to the UI configuration setting.

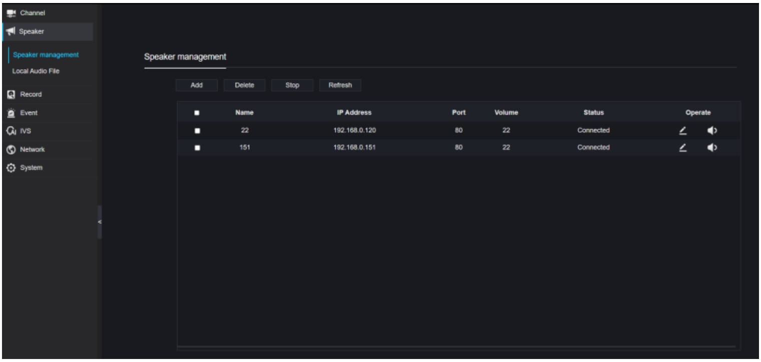
8.2 Speaker

On the Speaker interface, users can add IP speakers to the DVR, and manage the local audio files.

For the detailed information, please refer to *Chapter 6.2 Speaker*.

8.2.1 Speaker Management

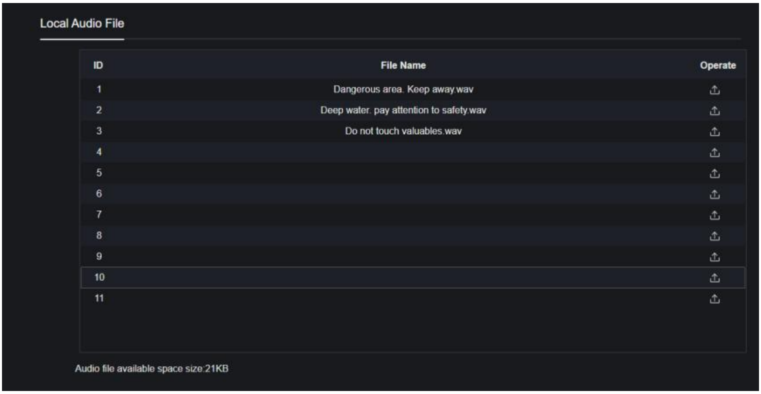
Figure 8-19 Speaker management



■	Name	IP Address	Port	Volume	Status	Operate
■	22	192.168.0.120	80	22	Connected	
■	151	192.168.0.151	80	22	Connected	

8.2.2 Local Audio Files

Figure 8-20 Local audio file



Local Audio File

ID	File Name	Operate
1	Dangerous area. Keep away.wav	⇧
2	Deep water. pay attention to safety.wav	⇧
3	Do not touch valuables.wav	⇧
4		⇧
5		⇧
6		⇧
7		⇧
8		⇧
9		⇧
10		⇧
11		⇧

Audio file available space size:21KB

8.3 Record

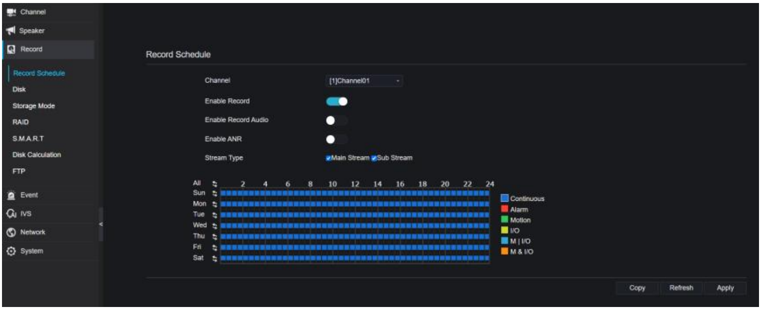
Users can set record policies in the Storage interface.

8.3.1 Record Schedule

Procedure

Step 1 On the **System Setting** screen, choose **Record > Record Schedule** to access the record schedule interface, as shown in Figure 8-21.

Figure 8-21 Record schedule interface



Record Schedule

Channel: [1]Channel01

Enable Record: ●

Enable Record Audio: ○

Enable ANR: ○

Stream Type: ☑Main Stream ☑Sub Stream

Step 2 Select a channel.

Step 3 Enable the record, then enable record audio.

Step 4 Enable ANR. When the IP cameras support the ANR, if the cameras are disconnected from the DVR, the DVR can copy the lost video recordings from the SD card installed in the cameras.

Step 5 To set the record schedule, you can drag the mouse to choose an area or click ⇅ to choose all day or all week. You can also click one by one to set the schedule. Or drag the mouse cursor to choose. Users can set the alarm recording to save the space of the disk.

Step 6 Click Refresh to return the previous settings.

Step 7 Click Copy to choose other cameras to copy settings. Click Apply to save the settings.

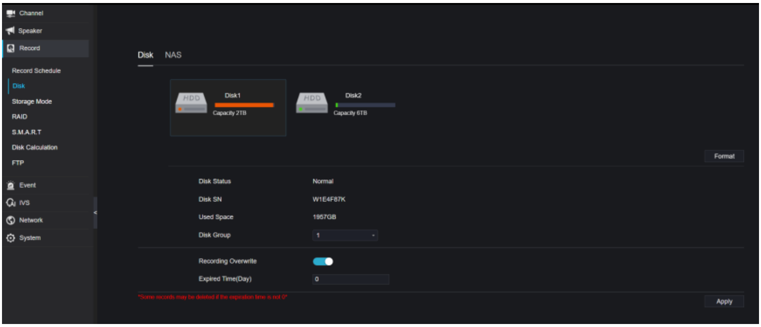
----End

8.3.2 Disk

8.3.2.1 Disk

Step 1 On the **System Setting** screen, choose **Record > Disk** to access the disk interface, as shown in Figure 8-22.

Figure 8-22 Disk interface



Disk1 Capacity 2TB
Disk2 Capacity 6TB

Disk Status: Normal
Disk SN: W1E4F87K
Used Space: 1967GB
Disk Group: 1
Recording Overwrite: ●
Expired Time(Day): 0

Some records may be deleted if the expiration time is not 0

Step 2 You can view information like capacity, disk status, disk SN code, and used space.

Step 3 Click Format to delete all data. Before deleting the data, users will view a pop-up window "Are you sure to format disk? Your data will be lost". Click OK to delete, and click Cancel to quit.

Step 4 Choose the disk group from the drop-down list; there are four disk groups.

Step 5 Enable the recording overwrite, and set the expired time. (If the expired time is 0, it means the disk is full, and then the recording will be rewritten. If the expiration time is 5 days, the recording video will be rewritten when it reaches the expiration date.)

Step 6 If the recording overwrite is disabled, set the expired time; it is up to 90 days.

----End

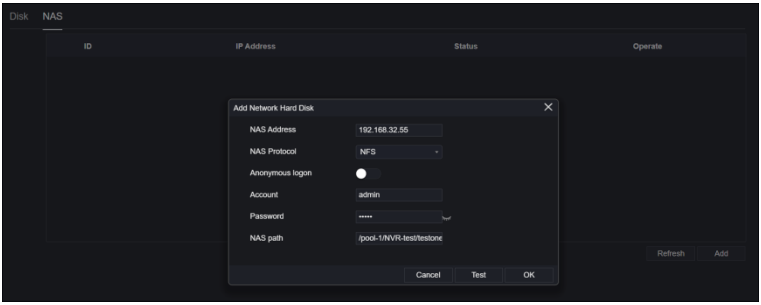
8.3.2.2 NAS

If users have a NAS account, they can add the NAS as a network hard disk for saving backup recordings.

Step 1 On the **System Setting** screen, choose **Record > Disk > NAS** to access the NAS interface.

Step 2 Click Add to add a NAS account.

Figure 8-23 NAS



Add Network Hard Disk

NAS Address: 192.168.32.55

NAS Protocol: NFS

Anonymous logon: ○

Account: admin

Password: •••••

NAS path: /pool-1/NVR-test/testone

Step 3 Input the NAS address. The protocol is default NFS. Enable anonymous login, the account and password are invalid; else input the account and password.

Step 4 Input the NAS path, the path can be viewed at the NAS interface.

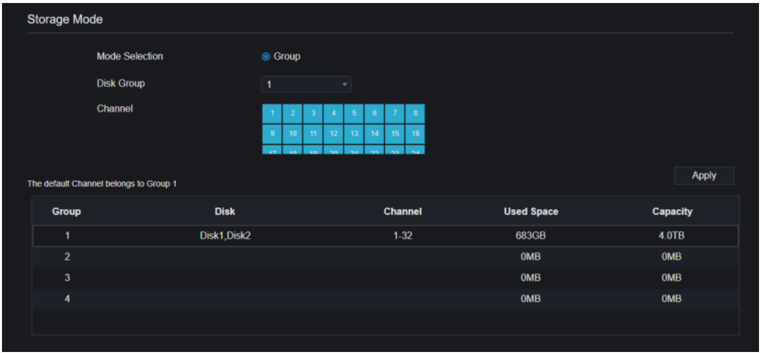
Step 5 Click **Test** to check the parameters, test successfully, and click **OK** to save the settings.

----End

8.3.3 Storage Mode

Distribute channels to different disk groups as needed for efficient use of the disk capacity.

Figure 8-24 Storage Mode



Storage Mode

Mode Selection: ● Group

Disk Group: 1

Channel

The default Channel belongs to Group 1

Group	Disk	Channel	Used Space	Capacity
1	Disk1,Disk2	1-32	683GB	4.0TB
2			0MB	0MB
3			0MB	0MB
4			0MB	0MB

Operation Steps

Step 1 Choose the disk group.

Step 2 Select the channel to record to the disk group.

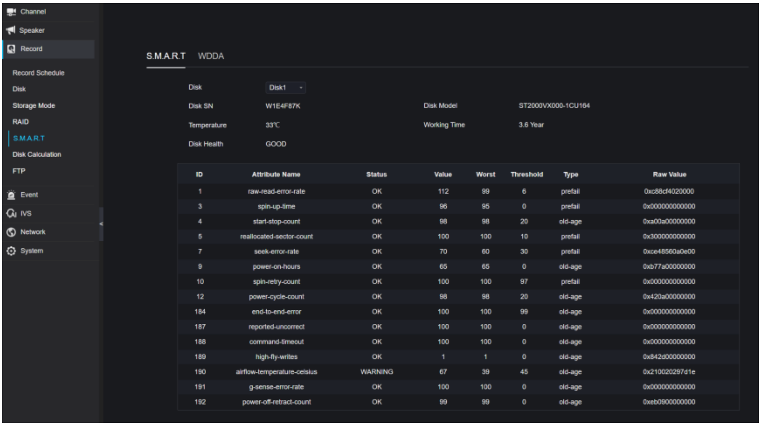
Step 3 Click Apply to save the settings.

Step 4 The group list will show the detailed information.

8.3.4 S.M.A.R.T

S.M.A.R.T is a Self-Monitoring Analysis and Reporting Technology; users can view the health of the disk, as shown in Figure 8-25.

Figure 8-25 S.M.A.R.T



Disk: Disk1

Disk SN: W1E4F87K

Disk Model: ST2000VX000-1CU164

Temperature: 33℃

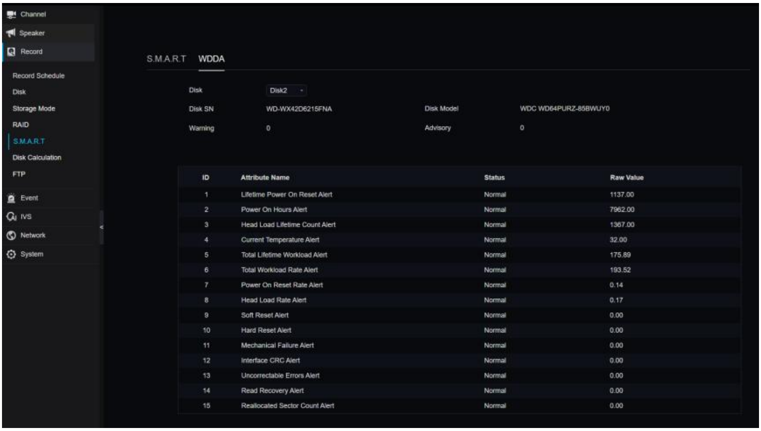
Working Time: 3.6 Year

Disk Health: GOOD

ID	Attribute Name	Status	Value	Worst	Threshold	Type	Raw Value
1	raw-read-error-rate	OK	112	99	6	prefail	0xc88cf4020000
3	spin-up-time	OK	96	95	0	prefail	0x000000000000
4	start-stop-count	OK	98	98	20	old-age	0xa00a00000000
5	reallocated-sector-count	OK	100	100	10	prefail	0x300000000000
7	seek-error-rate	OK	70	60	30	prefail	0xce48560a0e00
9	power-on-hours	OK	65	65	0	old-age	0xb77a00000000
10	spin-retry-count	OK	100	100	97	prefail	0x000000000000
12	power-cycle-count	OK	98	98	20	old-age	0x420a00000000
184	end-to-end-error	OK	100	100	99	old-age	0x000000000000
187	reported-uncorrect	OK	100	100	0	old-age	0x000000000000
188	command-timeout	OK	100	100	0	old-age	0x000000000000
189	high-fly-writes	OK	1	1	0	old-age	0x842d00000000
190	airflow-temperature-celsius	WARNING	67	39	45	old-age	0x210020297d1e
191	g-sense-error-rate	OK	100	100	0	old-age	0x000000000000
192	power-off-retract-count	OK	99	99	0	old-age	0xeb0900000000

The disk of Western Digital can be viewed by WDDA, as shown in Figure 8-26.

Figure 8-26 WDDA (Supplied for Some Model)



Disk: Disk2

Disk SN: WD-WX42D6215FNA

Disk Model: WDC WD64PURZ-85BWUY0

Warning: 0

Advisory: 0

ID	Attribute Name	Status	Raw Value
1	Lifetime Power On Reset Alert	Normal	1137.00
2	Power On Hours Alert	Normal	7962.00
3	Head Load Lifetime Count Alert	Normal	1367.00
4	Current Temperature Alert	Normal	32.00
5	Total Lifetime Workload Alert	Normal	175.89
6	Total Workload Rate Alert	Normal	193.52
7	Power On Reset Rate Alert	Normal	0.14
8	Head Load Rate Alert	Normal	0.17
9	Soft Reset Alert	Normal	0.00
10	Hard Reset Alert	Normal	0.00
11	Mechanical Failure Alert	Normal	0.00
12	Interface CRC Alert	Normal	0.00
13	Uncorrectable Errors Alert	Normal	0.00
14	Read Recovery Alert	Normal	0.00
15	Reallocated Sector Count Alert	Normal	0.00

8.3.5 Disk Calculation

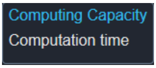
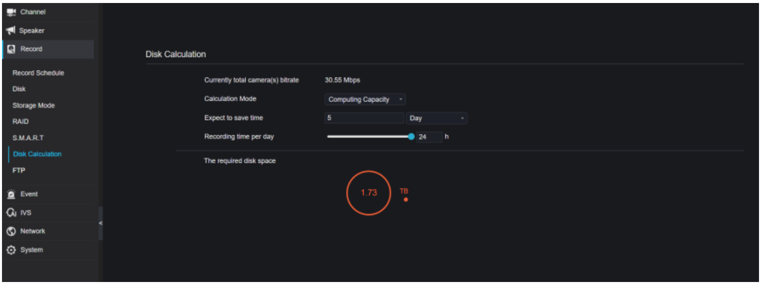
There are two modes to calculate the captivity of the disk, as  shown here.

Figure 8-27 Disk calculation



Disk Calculation

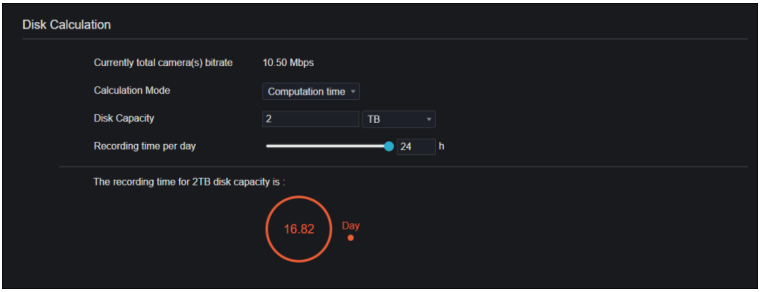
Currently total camera(s) bitrate: 30.55 Mbps

Calculation Mode: Computing Capacity

Expect to save time: 5 Day

Recording time per day: 24 h

The required disk space: 1.73 TB



Disk Calculation

Currently total camera(s) bitrate: 10.50 Mbps

Calculation Mode: Computation time

Disk Capacity: 2 TB

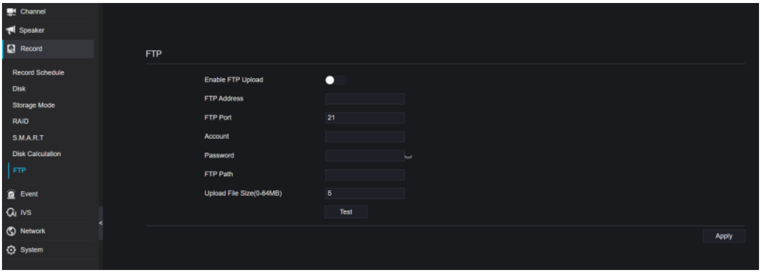
Recording time per day: 24 h

The recording time for 2TB disk capacity is : 16.82 Day

8.3.6 FTP

Set the FTP path to receive the alarm information, as shown in Figure 8-28. For more detailed information, please refer to UI interface parameters.

Figure 8-28 FTP



FTP

Enable FTP Upload: ○

FTP Address:

FTP Port: 21

Account:

Password:

FTP Path:

Upload File Size(0-64MB): 5

8.4 Event

Users can set general, motion detection, video loss, alarm in, abnormal alarm, and alarm out on the alarm interface. For detailed information, please refer to *Chapter 6.4 Event Management*.

8.4.1 General

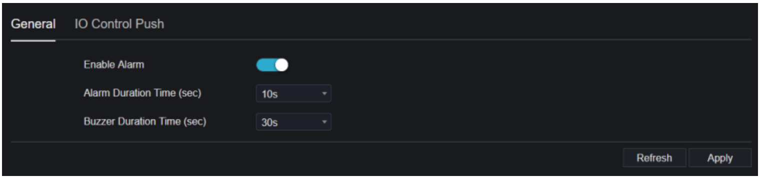
8.4.1.1 General

Procedure

Step 1 On the **System Setting** screen, choose **Alarm > General** to access the General interface.

Step 2 Enable the alarm to set the duration time and buzzer duration time, as shown in Figure 8-29.

Figure 8-29 General interface



Enable Alarm: on
Alarm Duration Time (sec): 10s
Buzzer Duration Time (sec): 30s

Step 3 Click Apply to save settings. Click Refresh to return to the previous settings.

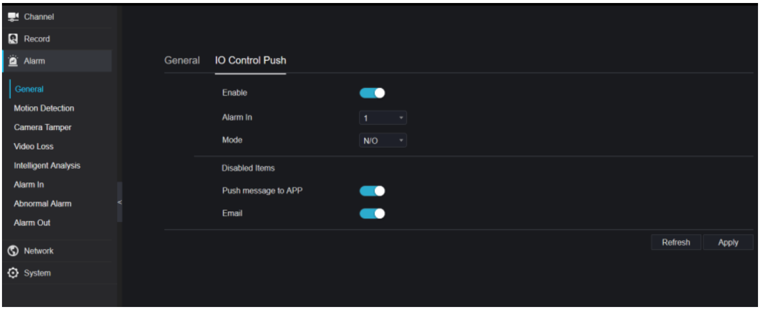
8.4.1.2 IO Control Push

Procedure

Step 1 On the **System Setting** screen, choose **Alarm > General** > **IO Control Push** to access the general interface.

Step 2 Enable the IO control push, as shown in Figure 8-30.

Figure 8-30 IO control push interface



Enable: on
Alarm In: 1
Mode: N/O
Disabled Items
Push message to APP: on
Email: on

Step 3 Choose one alarm in and the mode (N/C, N/O).

Step 4 Tick the disable items (it will affect all alarm push messages), and click “Apply” to save settings.

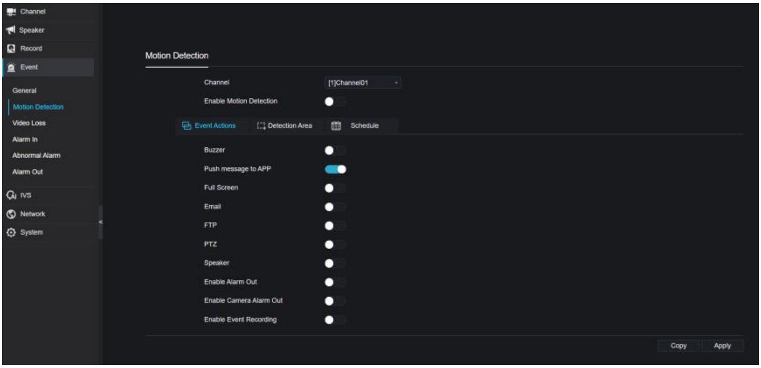
----End

8.4.2 Motion Detection

Procedure

Step 1 On the **System Setting** screen, choose **Alarm > Motion Detection** to access the motion detection interface, as shown in Figure 8-31.

Figure 8-31 Motion detection interface



Channel: [1]Channel01

Enable Motion Detection ○

Buzzer ○

Push message to APP ●

Full Screen ○

Email ○

FTP ○

PTZ ○

Speaker ○

Enable Alarm Out ○

Enable Camera Alarm Out ○

Enable Event Recording ○

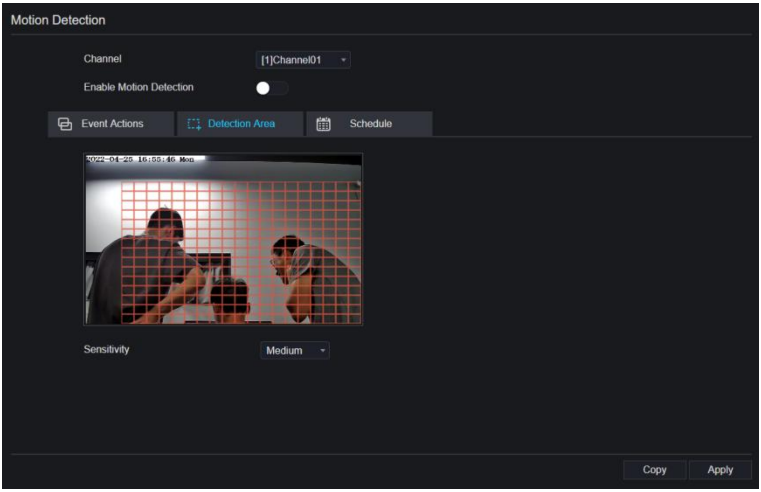
Step 2 Click the channel drop-down list to choose a channel.

Step 3 Enable motion detection alarm.

Step 4 Set **Event Activity**, which includes buzzer, push message to APP, pop-up message to monitor, full screen, email, cloud storage, alarm out (the back panel), channel alarm out (the port of cameras), and alarm record.

Step 5 Click **Area** to access the motion detection area setting, as shown in Figure 8-32.

Figure 8-32 Motion detection area interface



Motion Detection

Channel [1]Channel01

Enable Motion Detection

Sensitivity Medium

1. Hold down and drag the left mouse button to draw a motion detection area.
2. Select a value from the drop-down list next to **Sensitivity**.
3. Double-click the chosen area to delete.

Step 6 Click **Schedule** to access schedule settings, and drag and release the mouse to select the alarming time between 00:00 and 24:00 from Monday to Sunday. Clicking the chosen area can cancel it. The settings of the alarm schedule are the same as the disk schedule.

Step 7 Click Copy to choose other cameras to copy settings. Click Apply to save the settings.

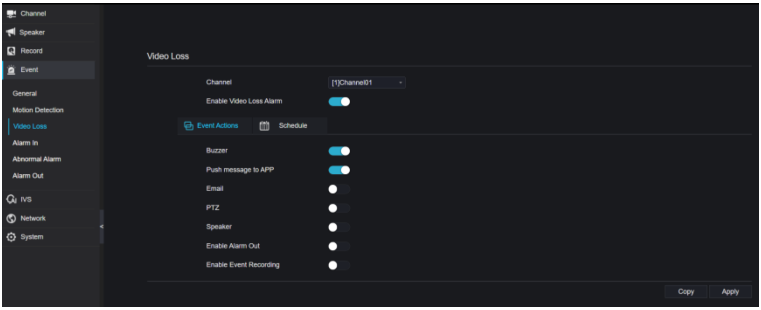
---End

8.4.3 Video Loss

Procedure

Step 1 On the **System Setting** screen, choose **Alarm > Video Loss** to access the video loss interface, as shown in Figure 8-33.

Figure 8-33 Video loss interface



Video Loss

Channel: [1]Channel01

Enable Video Loss Alarm ☑

Buzzer ☑

Push message to APP ☑

Email ☐

PTZ ☐

Speaker ☐

Enable Alarm Out ☐

Enable Event Recording ☐

Step 2 Click the drop-down list to choose a channel.

Step 3 Enable the video loss alarm.

Step 4 For setting event activity and schedule, please refer to *Figure 4-6 motion detection settings*.

Step 5 Click Copy to choose other cameras to copy settings. Click Apply to save the settings.

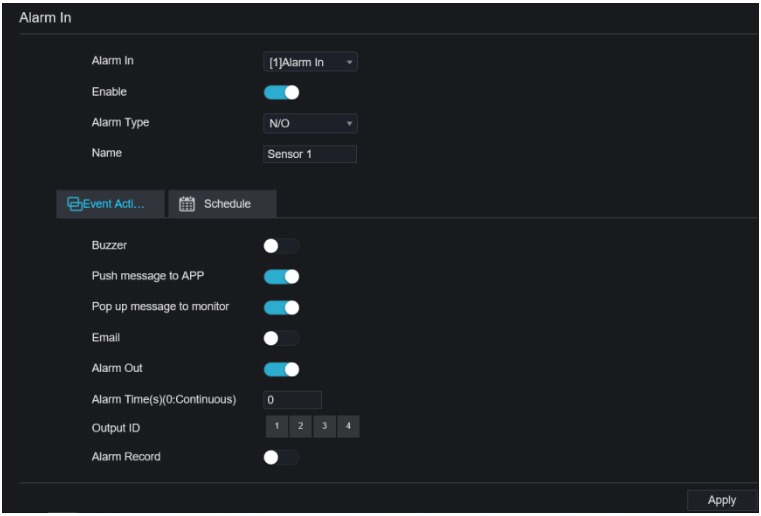
----End

8.4.4 Alarm In

Procedure

Step 1 On the **System Setting** screen, choose **Alarm > Alarm In** to access the alarm in the interface, as shown in Figure 8-34.

Figure 8-34 Alarm in interface



Alarm In

Alarm In: [1]Alarm In

Enable: ☑

Alarm Type: N/O

Name: Sensor 1

Buzzer: ☐

Push message to APP: ☑

Pop up message to monitor: ☑

Email: ☐

Alarm Out: ☑

Alarm Time(s)(0:Continuous): 0

Output ID: 1 2 3 4

Alarm Record: ☐

Step 2 Click the drop-down list to choose alarm in.

Step 3 Enable the button and choose the alarm type.

Step 4 Set name, default as Sensor 1.

Step 5 For setting event activity and schedule, please refer to *motion detection settings*.

Step 6 Click Apply to save settings.

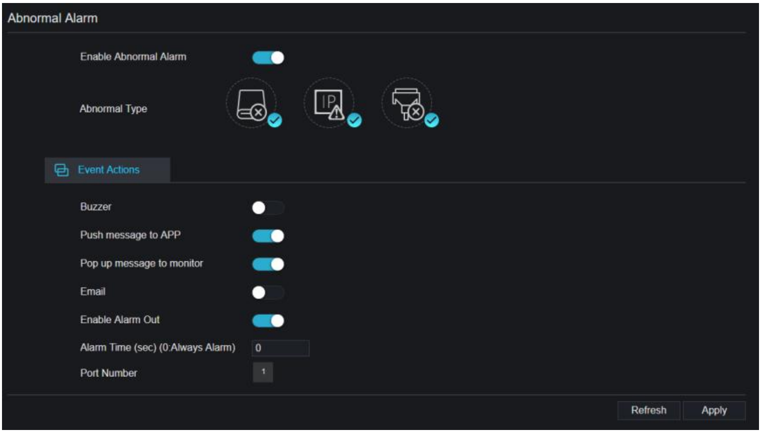
----End

8.4.5 Abnormal Alarm

Procedure

Step 1 On the **System Setting** screen, choose **Alarm > Abnormal Alarm** to access the abnormal alarm interface, as shown in Figure 5-19.

Figure 8-35 Abnormal alarm interface



Abnormal Alarm

Enable Abnormal Alarm ☑

Abnormal Type

Event Actions

Buzzer ☐

Push message to APP ☑

Pop up message to monitor ☑

Email ☐

Enable Alarm Out ☑

Alarm Time (sec) (0:Always Alarm) 0

Port Number 1

Step 2 Enable the button and tick alarm type.

Step 3 For setting event activity and schedule, please refer to *motion detection settings*.

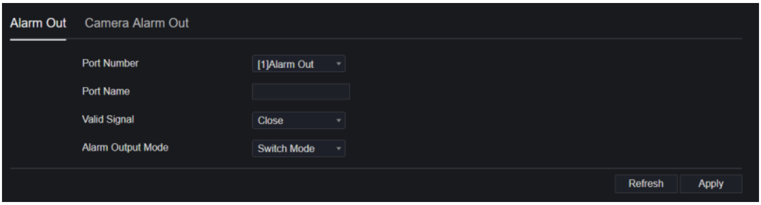
Step 4 Click Apply to save settings.

----End

8.4.6 Alarm out

Set the alarm out and the camera alarm out.

Figure 8-36 Alarm out



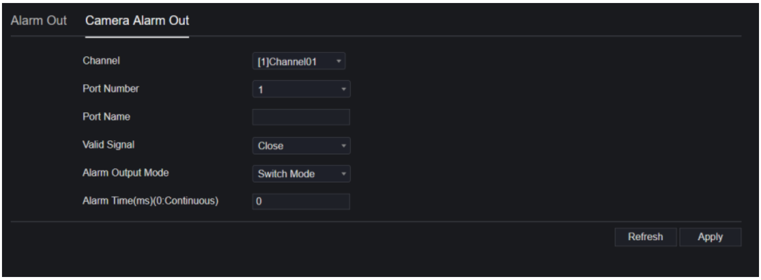
Port Number: [1]Alarm Out

Port Name:

Valid Signal: Close

Alarm Output Mode: Switch Mode

Figure 8-37 Camera alarm out



Channel: [1]Channel01

Port Number: 1

Port Name:

Valid Signal: Close

Alarm Output Mode: Switch Mode

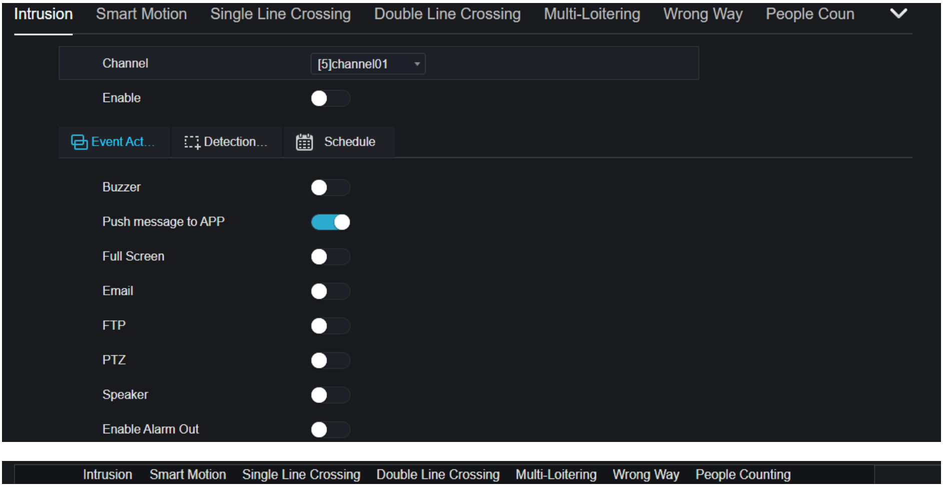
Alarm Time(ms)(0:Continuous): 0

8.5 IVS

On the IVS interface, users can set the Intelligent Analysis, ES Analysis, and Local Intelligent Analysis. For detailed information, please refer to *Chapter 6.5 IVS Configuration*.

8.5.1 Intelligent Analysis (Only for Some Models)

Figure 8-38 Intelligent analysis interface



Channel: [5]channel01

Enable ○

Buzzer ○

Push message to APP ●

Full Screen ○

Email ○

FTP ○

PTZ ○

Speaker ○

Enable Alarm Out ○

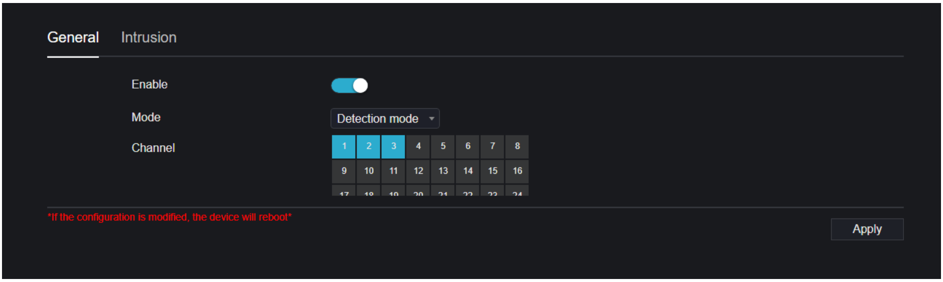
8.5.2 ES Analysis

ES Analysis (Environmental Safety Analysis) includes smoking detection, smoke and flame detection, and fire spot detection; these functions apply to thermal cameras. For detailed information, please refer to *Chapter 6.5.2 ES Analysis.*

8.5.3 Local Intelligent Analysis

At the Local Intelligent Analysis interface, users can enable and set the mode to detection mode, and choose less than 4 channels to enable intrusion. The chosen channel devices should be AI multi-object cameras.

Figure 8-39 Local intelligent analysis



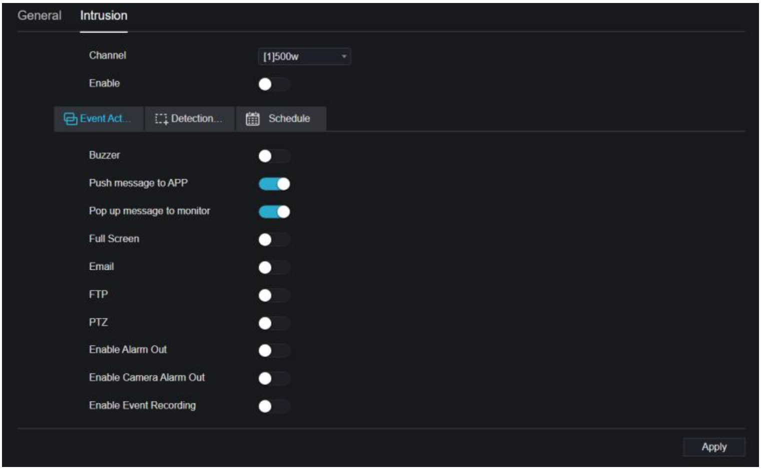
Enable ☑

Mode: Detection mode

Channel: 1 ☑, 2 ☑, 3 ☑, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24

If the configuration is modified, the device will reboot

Figure 8-40 Intrusion



Channel: [1]500w

Enable □

Buzzer □

Push message to APP ☑

Pop up message to monitor ☑

Full Screen □

Email □

FTP □

PTZ □

Enable Alarm Out □

Enable Camera Alarm Out □

Enable Event Recording □

8.6 Network

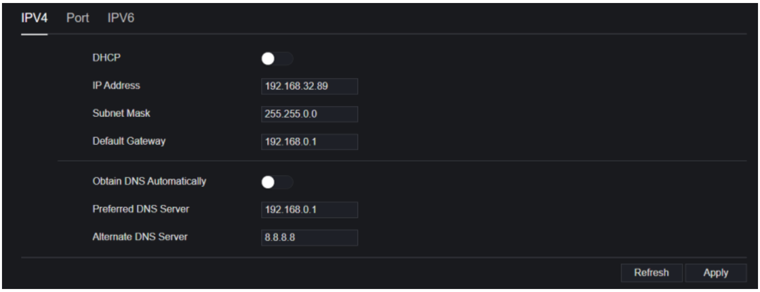
Users can set Network, DDNS, E-mail, UPnP, P2P, IP Filter, 802.1X, SNMP, and Web Mode.

8.6.1 Network

Procedure

Step 1 On the **System Setting** screen, choose **Network > Network** to access the network interface, as shown in Figure 8-41.

Figure 8-41 Network interface



IPV4 Port IPV6

DHCP ●

IP Address: 192.168.32.89

Subnet Mask: 255.255.0.0

Default Gateway: 192.168.0.1

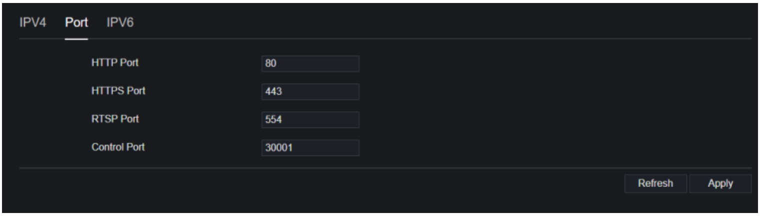
Obtain DNS Automatically ●

Preferred DNS Server: 192.168.0.1

Alternate DNS Server: 8.8.8.8

Refresh Apply

Figure 8-42 Port



IPV4 Port IPV6

HTTP Port: 80

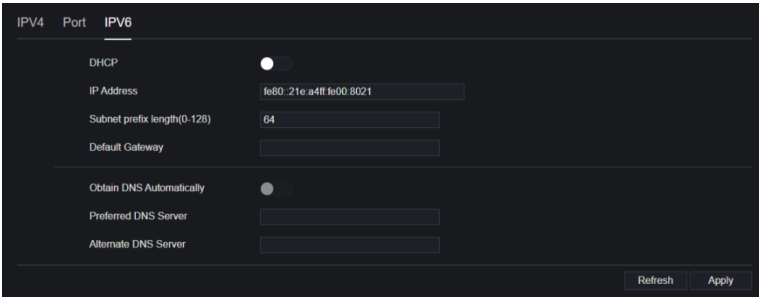
HTTPS Port: 443

RTSP Port: 554

Control Port: 30001

Refresh Apply

Figure 8-43 IPV6



IPV4 Port IPV6

DHCP ●

IP Address: fe80::21e:a4ff:fe00:8021

Subnet prefix length(0-128): 64

Default Gateway:

Obtain DNS Automatically ●

Preferred DNS Server:

Alternate DNS Server:

Refresh Apply

Step 2 Click ○ next to **IP** to enable or disable the function of automatically getting an IP address. The function is enabled by default.

If the function is disabled, click the input boxes next to **IP**, **Subnet Mask**, and **Gateway** to set the parameters as required.

Step 3 Click ○ next to **Obtain DNS Automatically** to enable or disable the function of automatically getting a DNS address. The function is enabled by default.

If the function is disabled, click the input boxes next to **DNS1** and **DNS2**, delete the original addresses, and enter new addresses.

Step 4 Set **Port** and **IPV6** manually, and input the information about these.

Step 5 Click Refresh to restore previous settings. Click Apply to save the settings.

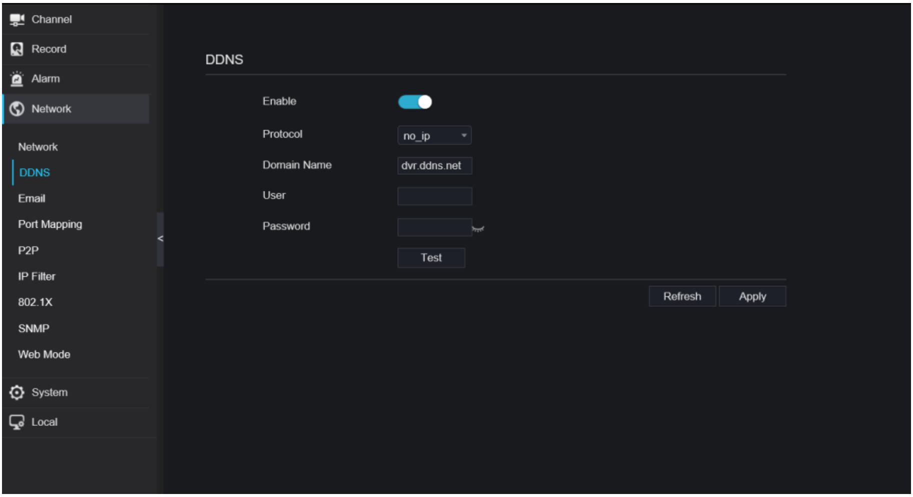
----End

8.6.2 DDNS

Procedure

Step 1 Click **DDNS** in the network interface, and choose **Network > DDNS** to access the DDNS interface as shown in Figure 8-44.

Figure 8-44 DDNS interface



DDNS

Enable

Protocol: no_ip

Domain Name: dvr.ddns.net

User

Password

Step 2 Click the button to enable the DDNS function. It is disabled by default.

Step 3 Select a required value from the **protocol** drop-down list.

Step 4 Set domain name, user, and password.

Step 5 Click Refresh to restore previous settings. Click Apply to save the settings.

NOTE

An external network can access an address specified in the DDNS settings to access the DVR.

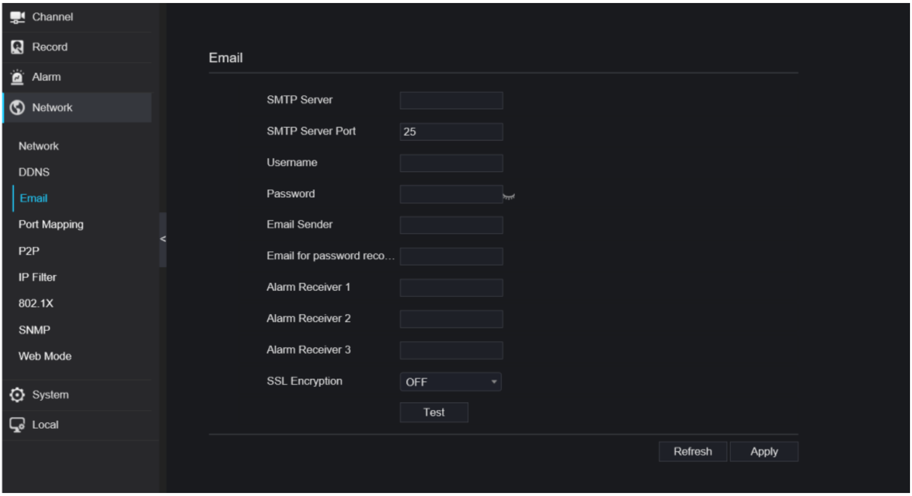
----End

8.6.3 Email

Procedure

Step 1 Click **Email** in the network interface, and choose **Network > Email** to access the Email interface, as shown in Figure 8-45

Figure 8-45 Email interface



SMTP Server
SMTP Server Port 25
Username
Password
Email Sender
Email for password reco...
Alarm Receiver 1
Alarm Receiver 2
Alarm Receiver 3
SSL Encryption OFF

Step 2 Set the SMTP server and SMTP server port manually.

Step 3 Set the sender's email address, username, and password manually.

Step 4 Set the email address for receiving the alarm message.

Step 5 Set the email for retrieving the password.

Step 6 Click the **SSL Encryption** drop-down list to enable the safeguard of email.

Step 7 Click Refresh to restore previous settings. Click Apply to save the settings.

----End

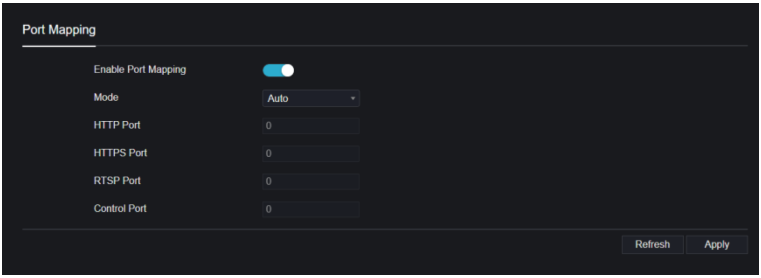
8.6.4 Port Mapping

8.6.4.1 Port Mapping

Procedure

Step 1 Click **Port Mapping** in the network interface, and choose **Network > Port Mapping** to access the UPnP interface as shown in Figure 8-46.

Figure 8-46 Port Mapping interface



Port Mapping

Enable Port Mapping	●
Mode	Auto
HTTP Port	0
HTTPS Port	0
RTSP Port	0
Control Port	0

Step 2 Select the manner from UPnP to enable the drop-down list. The default value is auto.

Step 3 After **UPnP** is manual, set the web port, data port, and client port manually.

Step 4 Click Refresh to restore previous settings. Click Apply to save the settings.

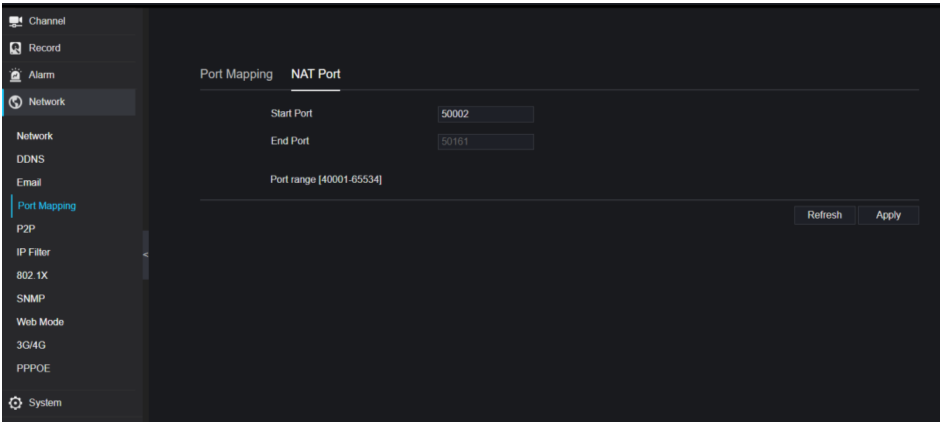
NOTE

Auto: The system performs UPnP automatically.
Manual: The ports are distributed by the router. Input them according to the router.

8.6.4.2 NAT port

NAT (Network Address Translation), users can browse the web of the camera by NAT port. Five ports can be assigned to each camera. Input the start port, and the system will compute the end port automatically.

Figure 8-47 NAT port

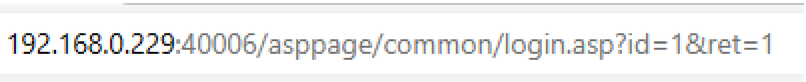


Start Port 50002

End Port 50161

Port range [40001-65534]

Users can input the http://IP address:port for example http://192.168.0.229:40006/ to access the camera's web interface.



192.168.0.229:40006/asppage/common/login.asp?id=1&ret=1

----End

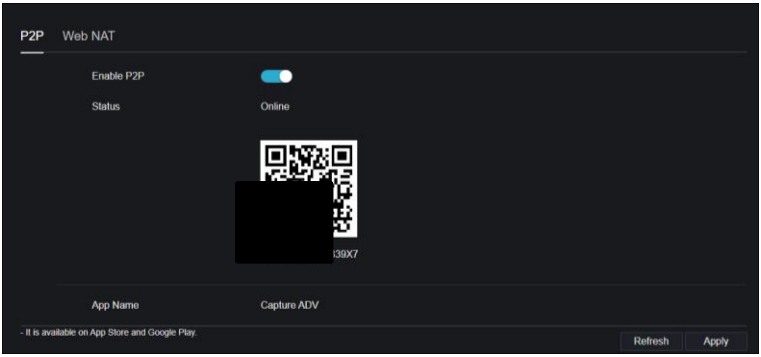
8.6.5 P2P

8.6.5.1 P2P

Procedure

Step 1 Click **P2P** in the network interface, and choose **Network > P2P** to access the P2P interface, as shown in Figure 8-48.

Figure 8-48 P2P interface



P2P Web NAT

Enable P2P

Status Online

[redacted]

App Name Capture ADV

- It is available on App Store and Google Play.

Refresh Apply

Step 2 Click **Enable** to enable the P2P function.

Step 3 Click Refresh to restore previous settings. Click Apply to save the settings.

Step 4 After installing Capture ADV on a mobile phone, run the app and scan the UUID QR code to add it. And then access the DVR while the device is online.

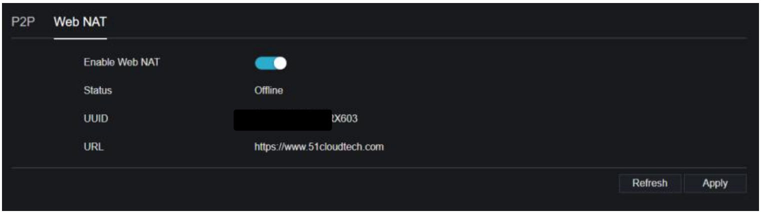
----End

8.6.5.2 Web NAT

The web NAT uses URL and UUID to log in to the web interface.

Enable Web NAT. When the status is online, copy the URL to enter the browser, and it will jump to the URL interface.

Figure 8-49 Web NAT



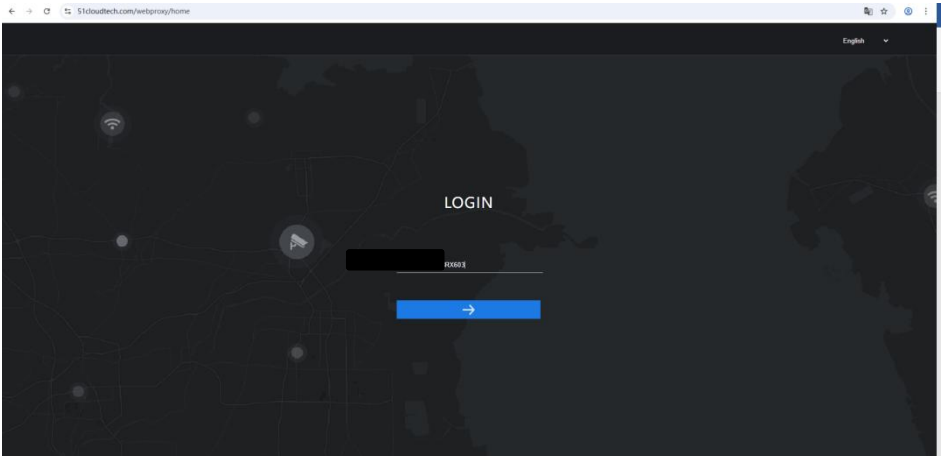
Enable Web NAT: on

Status: Offline

UUID: [redacted]X603

URL: https://www.51cloudtech.com

Figure 8-50 URL interface



[redacted]RX603

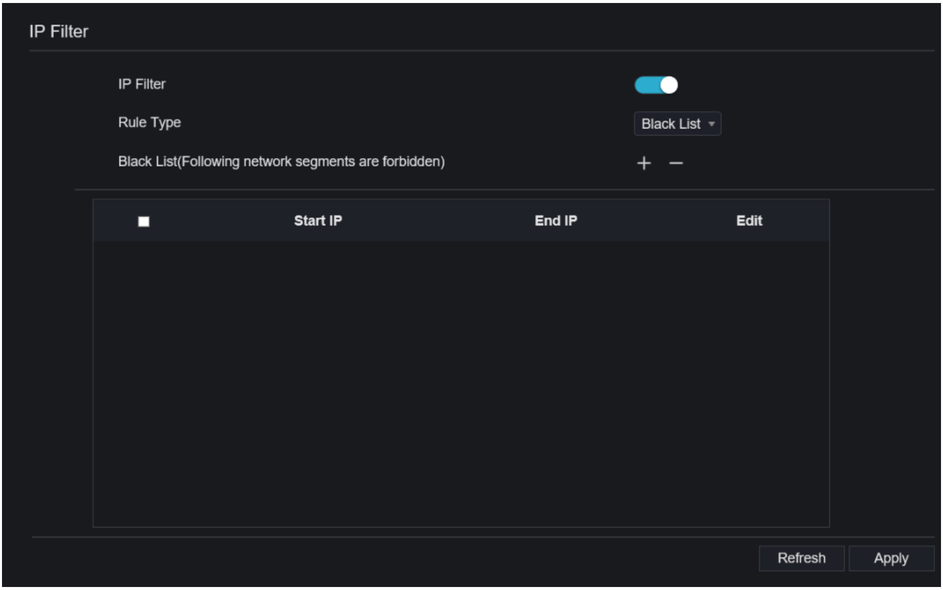
At the login interface, input the UUID of the DVR, and click Enter to enter the web interface of DVR.

8.6.6 IP Filter

Procedure

Step 1 Click **IP Filter** in the network interface, and choose **Network > IP Filter** to access the IP filter interface, as shown in Figure 8-51.

Figure 8-51 IP filter interface



IP Filter

IP Filter: ●

Rule Type: Black List ▾

Black List(Following network segments are forbidden) + −

■	Start IP	End IP	Edit

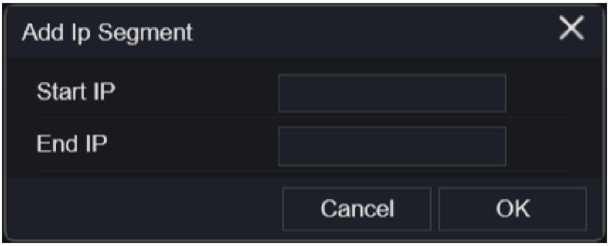
Step 2 Click **Enable** to enable the IP filter function.

Step 3 Click the drop-down list of rule types to choose blacklist or whitelist.

Step 4 Click +, view the pop-up windows to set a blacklist or whitelist, as shown in 6.7.5.

Click − to delete the list.

Figure 8-52 Black or white list interface



Add Ip Segment

Start IP:

End IP:

Step 5 Set start IP and end IP.

Step 6 Click Cancel to deny settings, and click OK to save the settings.

Step 7 Click Refresh to restore previous settings. Click Apply to save the settings.

NOTE

Blacklist: IP address in specified network segment to prohibit access.
Whitelist: IP address in specified network segment to allow access.
Select a name in the list and click Delete to delete the name from the list.
Select a name in the list and click Edit to edit the name in the list.
Only one rule type is available, and the last rule type set is efficient.

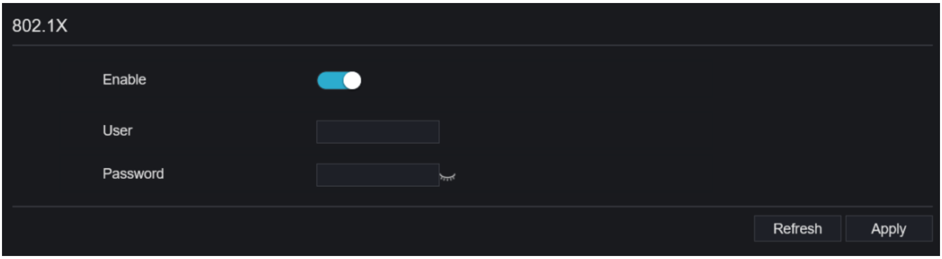
----End

8.6.7 802.1X

Procedure

Step 1 Click **802.1X** in the network interface. The 802.1X interface is displayed Enable the button, as shown in Figure 8-53.

Figure 8-53 802.1X interface



Step 2 Input the user and password of 802.1X authentication.

Step 3 Click Refresh to restore previous settings. Click Apply to save the settings.

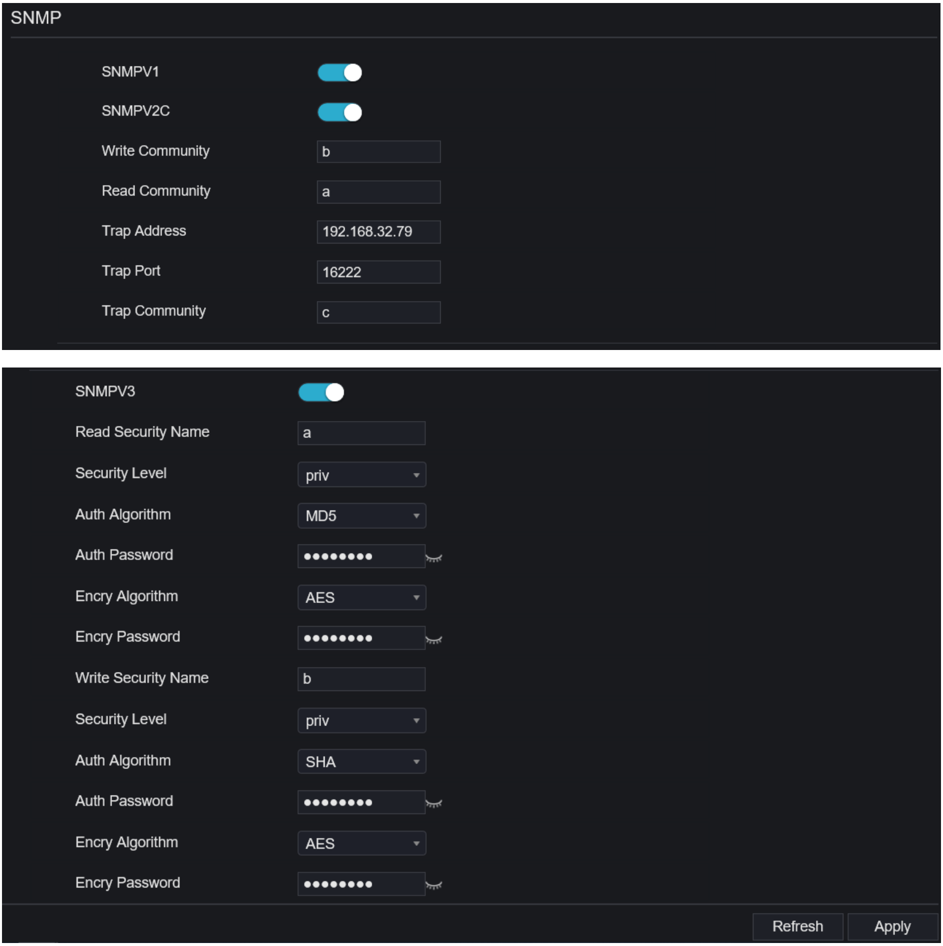
----End

8.6.8 SNMP

Procedure

Step 1 Click **SNMP** in the network interface. The SNMP interface is displayed. Enable the button next to SNMPV1, as shown in Figure 8-54.

Figure 8-54 SNMP interface



SNMP

SNMPV1	●
SNMPV2C	●
Write Community	b
Read Community	a
Trap Address	192.168.32.79
Trap Port	16222
Trap Community	c
SNMPV3	●
Read Security Name	a
Security Level	priv
Auth Algorithm	MD5
Auth Password	●●●●●●●●
Encry Algorithm	AES
Encry Password	●●●●●●●●
Write Security Name	b
Security Level	priv
Auth Algorithm	SHA
Auth Password	●●●●●●●●
Encry Algorithm	AES
Encry Password	●●●●●●●●

Step 2 Input the information of SNMP (Simple Network Management Protocol). There are three types of that function. Users can apply that if needed.

Table 8-1 SNMP parameters

Parameter	Description	Setting
SMTP Server Address	IP address of the SMTP server.	[Setting method] Enter a value manually.
SMTP Server Port	Port number of the SMTP server.	[Setting method] Enter a value manually. [Default value] 25
User Name	User name of the mailbox for sending emails.	[Setting method] Enter a value manually.
Password	Password of the mailbox for sending emails.	[Setting method] Enter a value manually.
Sender E-mail Address	Mailbox for sending emails.	[Setting method] Enter a value manually.
Recipient_E-mail_Address1	(Mandatory) Email address of recipient 1.	[Setting method] Enter a value manually.
Recipient_E-mail_Address2	(Optional) Email address of recipient 2.	
Recipient_E-mail_Address3	(Optional) Email address of recipient 3.	
Recipient_E-mail_Address4	(Optional) Email address of recipient 4.	
Recipient_E-mail_Address5	(Optional) Email address of recipient 5.	
Attachment Image Quality	A higher-quality image means more storage space. Set this parameter based on the site requirement.	N/A
Transport Mode	Email encryption mode. Set this parameter based on the encryption modes supported by the SMTP server.	[Setting method] Select a value from the drop-down list box. [Default value] No Encrypted

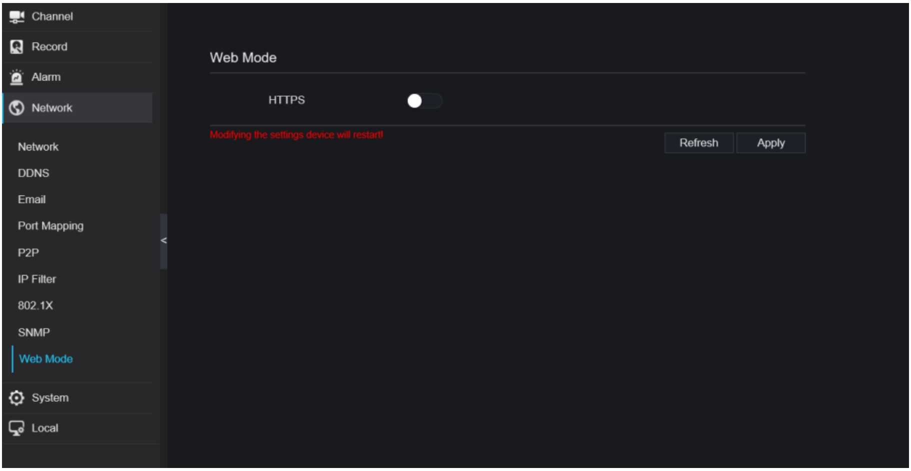
Step 3 Click Refresh to restore previous settings. Click Apply to save the settings.

----End

8.6.9 Web Mode

Step 1 Click **Web Mode** in the network interface. The Web Mode interface is displayed, as shown in Figure 4-6.

Figure 8-55 Web mode interface



Web Mode

HTTPS

Modifying the settings device will restart!

Step 2 Enable the HTTPS. The device will restart and start HTTPS secure.

Step 3 Click Refresh to restore previous settings. Click Apply to save the settings.

----End

8.6.10 CMS

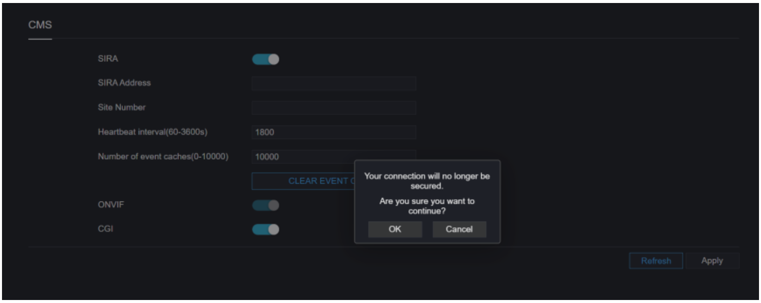
If the user wants to access the DVR via SIRA, ONVIF, or CGI, you can enable these. Enable the SIRA; the ONVIF is enabled automatically. The security of DVR will be reduced, so users should make sure of these actions.

SIRA: The server, the DVR, will sync the time and send some alarm information to this server.

ONVIF: Open Network Video Interface Forum. Users can access the DVR via the ONVIF protocol.

CGI: Common Gateway Interface. Users can access the DVR via CGI command.

Figure 8-56 CMS



CMS

SIRA

SIRA Address

Site Number

Heartbeat interval(60-3600s) 1800

Number of event caches(0-10000) 10000

CLEAR EVENT C

ONVIF

CGI

Your connection will no longer be secured.

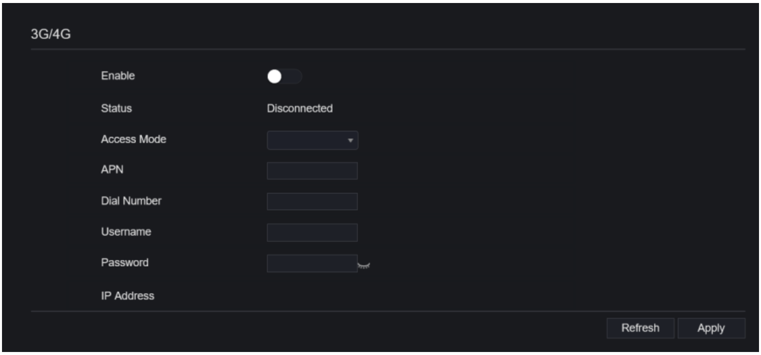
Are you sure you want to continue?

OK Cancel

Refresh Apply

8.6.11 3G/4G

Figure 8-57 3G/4G



3G/4G

Enable

Status Disconnected

Access Mode

APN

Dial Number

Username

Password

IP Address

Refresh Apply

Step 1 The user plugs the modem into DVR.

Step 2 Enable the 3G/4G.

Step 3 When the status is connected, users can set the access mode. AUTO is recommended.

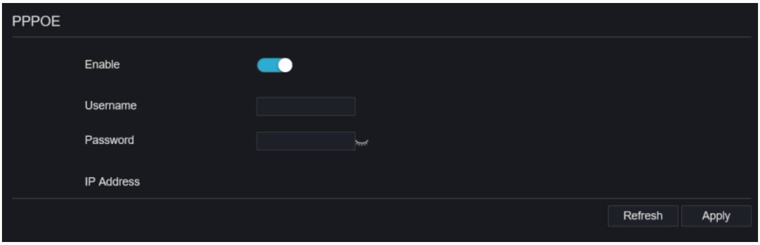
Step 4 If choosing another access mode, users should input the parameter correctly.

Step 5 Click Refresh to restore previous settings. Click Apply to save the settings.

8.6.12 PPPOE

Users can use the PPPOE function to manage the DVR conveniently.

Figure 8-58 PPPOE



PPPOE

Enable: on

Username

Password

IP Address

Step 1 Enable the PPPOE.

Step 2 Input the username and password.

Step 3 The IP address is obtained automatically.

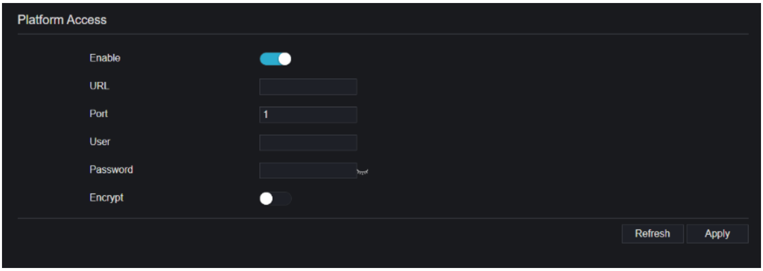
Step 4 Click Refresh to restore previous settings. Click Apply to save the settings.

Step 5 Users can use the IP address to access DVR immediately.

8.6.13 Platform Access

For more details, please refer to the UI interface parameter setting *6.6.12 Platform Access.*

Figure 8-59 Platform access



Platform Access

Enable: on

URL

Port: 1

User

Password

Encrypt: off

8.7 System

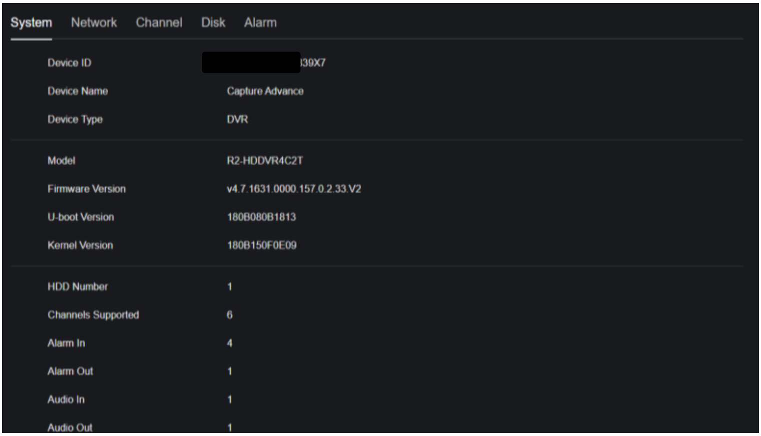
Users can set parameters about information, general, user, password, logs, maintenance, and auto restart.

8.7.1 Device Information

Procedure

Step 1 Click ⚙ on the navigation bar, and the device information interface is displayed, as shown in Figure 8-60.

Figure 8-60 Device information interface



Device ID	[redacted]
Device Name	Capture Advance
Device Type	DVR
Model	R2-HDDVR4C2T
Firmware Version	v4.7.1631.0000.157.0.2.33.V2
U-boot Version	180B080B1813
Kernel Version	180B150F0E09
HDD Number	1
Channels Supported	6
Alarm In	4
Alarm Out	1
Audio In	1
Audio Out	1

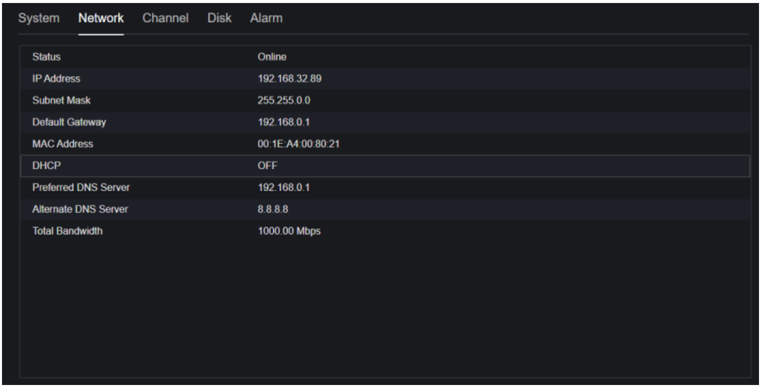
Step 2 Set the device name according to Table 8-2.

Table 8-2 Device parameters

Parameter	Description	Setting
Device ID	A unique device identifier is used by the platform to distinguish the devices.	[Setting method] The parameter cannot be modified.
Device Name	Name of the device.	[Setting method] **System Setting > General** Modify the device name.
Device Type	N/A	[Setting method] These parameters cannot be modified.
Model		
Firmware version		
HDD volume		
Channel support		

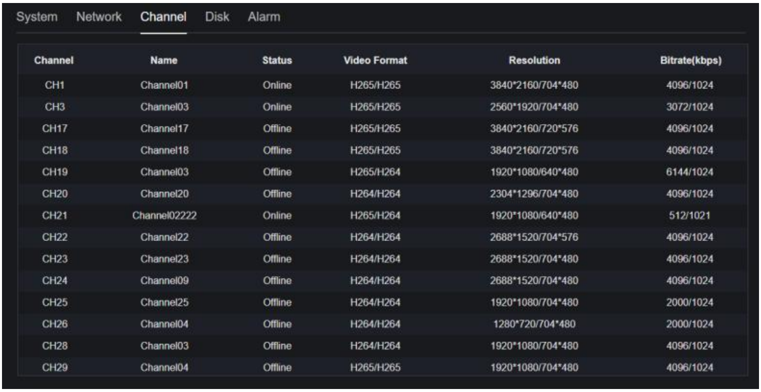
Parameter	Description	Setting
Alarm in		
Alarm out		
Audio in		
Audio out		

Figure 8-61 Network



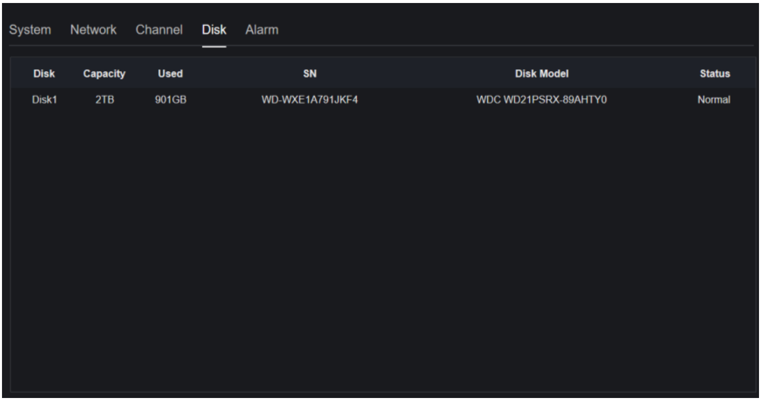
Status	Online
IP Address	192.168.32.89
Subnet Mask	255.255.0.0
Default Gateway	192.168.0.1
MAC Address	00:1E:A4:00:80:21
DHCP	OFF
Preferred DNS Server	192.168.0.1
Alternate DNS Server	8.8.8.8
Total Bandwidth	1000.00 Mbps

Figure 8-62 Channel



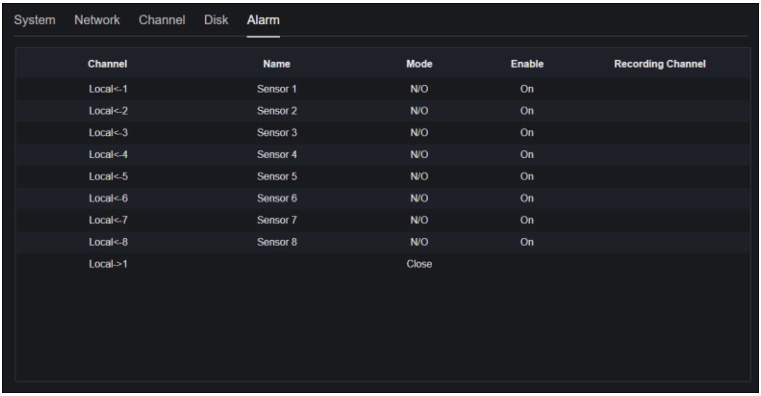
Channel	Name	Status	Video Format	Resolution	Bitrate(kbps)
CH1	Channel01	Online	H265/H265	3840*2160/704*480	4096/1024
CH3	Channel03	Online	H265/H265	2560*1920/704*480	3072/1024
CH17	Channel17	Offline	H265/H265	3840*2160/720*576	4096/1024
CH18	Channel18	Offline	H265/H265	3840*2160/720*576	4096/1024
CH19	Channel03	Offline	H265/H264	1920*1080/640*480	6144/1024
CH20	Channel20	Offline	H264/H264	2304*1296/704*480	4096/1024
CH21	Channel02222	Online	H265/H264	1920*1080/640*480	512/1021
CH22	Channel22	Offline	H264/H264	2688*1520/704*576	4096/1024
CH23	Channel23	Offline	H264/H264	2688*1520/704*480	4096/1024
CH24	Channel09	Offline	H264/H264	2688*1520/704*480	4096/1024
CH25	Channel25	Offline	H264/H264	1920*1080/704*480	2000/1024
CH26	Channel04	Offline	H264/H264	1280*720/704*480	2000/1024
CH28	Channel03	Offline	H264/H264	1920*1080/704*480	4096/1024
CH29	Channel04	Offline	H265/H265	1920*1080/704*480	4096/1024

Figure 8-63 Disk



Disk	Capacity	Used	SN	Disk Model	Status
Disk1	2TB	901GB	WD-WXE1A791JKF4	WDC WD21PSRX-89AHTY0	Normal

Figure 8-64 Alarm



Channel	Name	Mode	Enable	Recording Channel
Local<-1	Sensor 1	N/O	On	
Local<-2	Sensor 2	N/O	On	
Local<-3	Sensor 3	N/O	On	
Local<-4	Sensor 4	N/O	On	
Local<-5	Sensor 5	N/O	On	
Local<-6	Sensor 6	N/O	On	
Local<-7	Sensor 7	N/O	On	
Local<-8	Sensor 8	N/O	On	
Local->1		Close		

----End

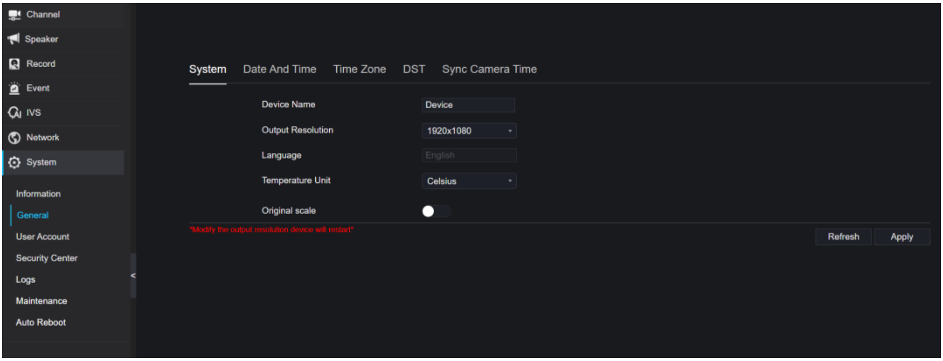
8.7.2 General

You can set the system settings, date and time, time zone, and DST general interface.

Procedure

Step 1 On the **System Setting** screen, choose **System > General** to access the general interface, as shown in Figure 8-65.

Figure 8-65 Basic setting interface



Device Name: Device

Output Resolution: 1920x1080

Language: English

Temperature Unit: Celsius

Original scale

"Modify the output resolution device will restart"

Step 2 Set the system.

1. Input the device name.

2. Choose output resolution from the drop-down list.

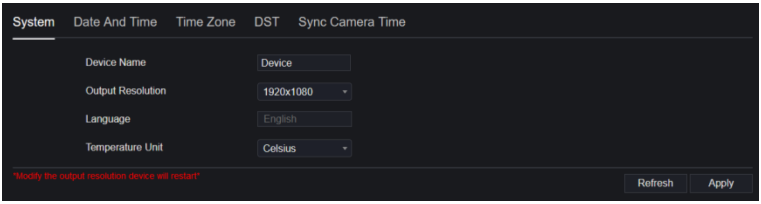
3. Click Apply to save the system setting.

Step 3 Set date and time.

1. Synchronize the time from the NTP server.

2. Click the NTP Sync button to enable time synchronization. The default value is enabled.

Figure 8-66 System interface



Device Name: Device

Output Resolution: 1920x1080

Language: English

Temperature Unit: Celsius

"Modify the output resolution device will restart"

3. Select the NTP server, date format, and time format from the drop-down list.

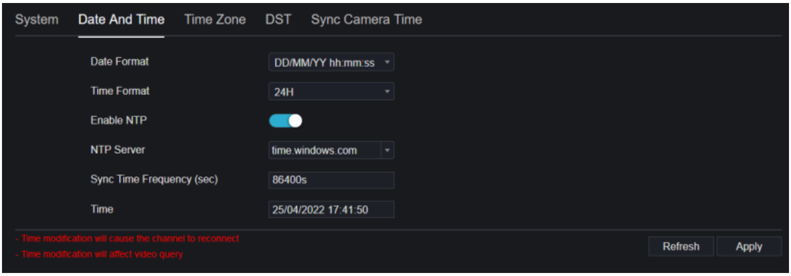
4. Click Apply to save the date and time setting. The device time will synchronize with the NTP server time.

5. Set the device time manually, as shown in Figure 8-67.

6. Click the NTP Sync button to disable time synchronization.

7. Async date and time interface.

Figure 8-67 Date and time



Date Format: DD/MM/YY hh:mm:ss
Time Format: 24H
Enable NTP: On
NTP Server: time.windows.com
Sync Time Frequency (sec): 86400s
Time: 25/04/2022 17:41:50

- Time modification will cause the channel to reconnect
- Time modification will affect video query

Step 4 Set the time zone.

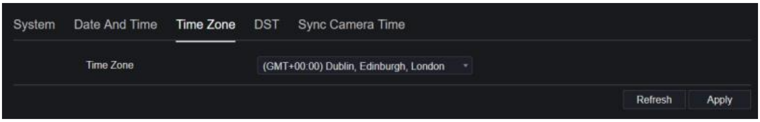
1. Select the date format and time format from the drop-down list.

2. Click Apply to save the device time setting. Click Refresh to return to the previous setting.

Step 5 Set time zone.

Click **Time Zone** to enter the time zone setting interface, as shown in Figure 8-68.
Time zone setting interface

Figure 8-68 Time zone



Time Zone: (GMT+00:00) Dublin, Edinburgh, London

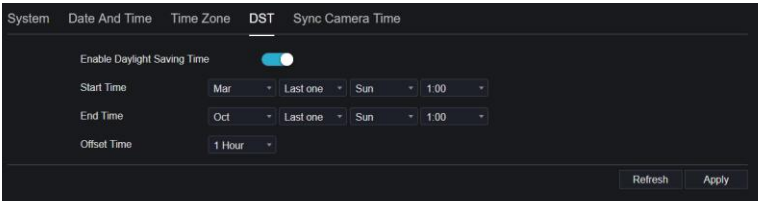
Select a time zone from the drop-down list.

Click Apply to save the time zone setting. Click Refresh to return to the previous setting.

Step 6 Set DST.

1. Click DST to enter the DST setting interface, and click the DST button to enable, as shown in Figure 8-69. The button is disabled by default.

Figure 8-69 DST setting interface



Enable Daylight Saving Time

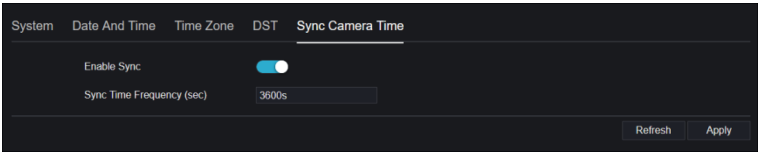
Start Time Mar Last one Sun 1:00

End Time Oct Last one Sun 1:00

Offset Time 1 Hour

Select a start time from the drop-down list.
Select an end time from the drop-down list.
Select an offset time from the drop-down list.

Figure 8-70 Sync camera time



Enable Sync

Sync Time Frequency (sec) 3600s

Enable sync camera time, and the cameras of DVR management will be showing at the same time.
Set the frequency of checks (minimum 10s).

Step 7 Click Apply to save the DST setting. Click Refresh to return to the previous setting.

----End

8.7.3 User Account

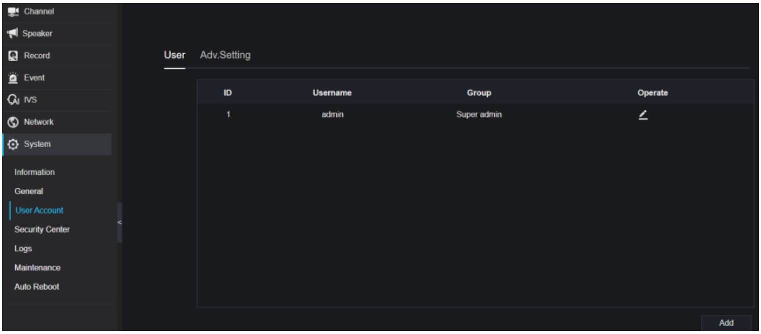
You can create new user accounts to manage the device.

8.7.3.1 Add User

Procedure

Step 1 On the **System Setting** screen, choose **System > User** to access the **User** interface, as shown in Figure 8-71.

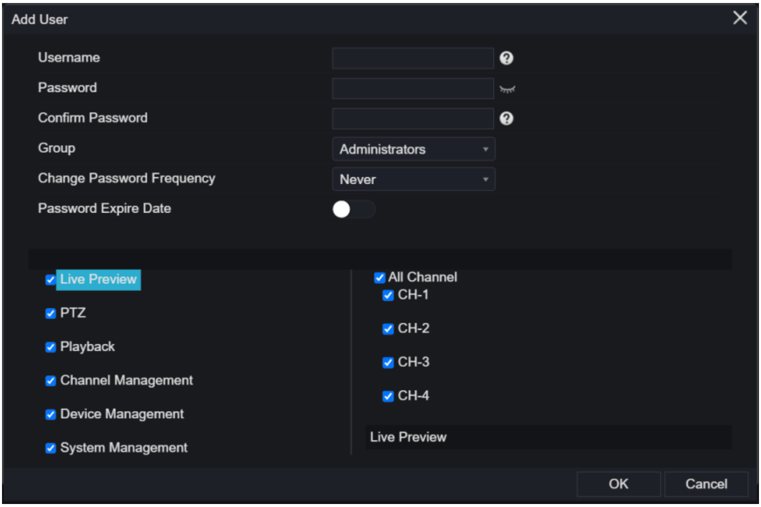
Figure 8-71 User interface



ID	Username	Group	Operate
1	admin	Super admin	

Step 2 Click **Add** to add a new user, as shown in Figure 8-72.

Figure 8-72 Add user



Username	
Password	
Confirm Password	
Group	Administrators
Change Password Frequency	Never
Password Expire Date	○

☑ Live Preview
☑ PTZ
☑ Playback
☑ Channel Management
☑ Device Management
☑ System Management

☑ All Channel
☑ CH-1
☑ CH-2
☑ CH-3
☑ CH-4

Live Preview

Step 3 Input username, password, and confirm password.

Step 4 Select a group and change the password reminder from the drop-down list.

Step 5 Assign the privilege to the user.

Step 6 Enable the expiration date to set the new user’s authority time.

Step 7 Select channels to manage.

Step 8 Click OK**, and** the message **"Add success"** is shown. If the password does not meet the rule, it will show ⚠ Password does not meet requirements.

Step 9 Click ✎ to edit the user's information.

Step 10 Click 🗑 to delete the account, it will show "Are you sure to delete? OK Cancel", click OK to delete.

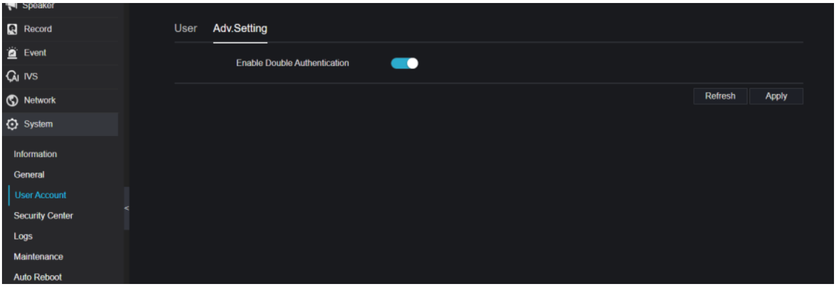
----End

8.7.3.2 Adv.Setting

Procedure

Step 1 On the **System Setting** screen, choose **System > User** > **Adv. Setting** to access interface, as shown in Table 6-3.

Figure 8-73 Adv. Setting interface



Enable Double Authentication ●

Step 2 Enable the **Password Double Authentication**. If the user wants to play back a video, he needs to input another username and password to authenticate.

Step 3 Click Apply to save the device time setting. Click Refresh to return to the previous setting.

----End

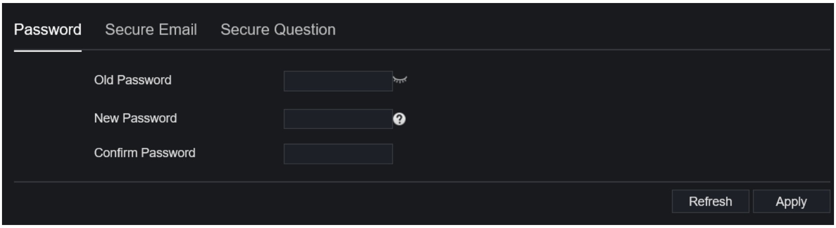
8.7.4 Security Center

8.7.4.1 Password

Procedure

Step 1 On the **System Setting** screen, choose **System > Security Center** to access the password interface, as shown in Figure 8-74.

Figure 8-74 Password interface



Step 2 Input the old password, and the new password and confirm the password.

Step 3 Click Apply to save settings. Click Refresh to return to the previous setting.

NOTE

The valid password range is [6-32] characters.

At least 2 kinds of numbers, lowercase, uppercase, or special characters contained.

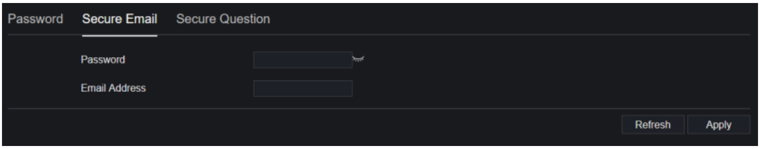
Only these special characters are supported！ @#&*+=-%&”`(),/’.:;< >?^|~[]{}.

----End

8.7.4.2 Secure Email

The secure email can receive the verification code of DVR if the user forgets the password accidentally.

Figure 8-75 Secure Email

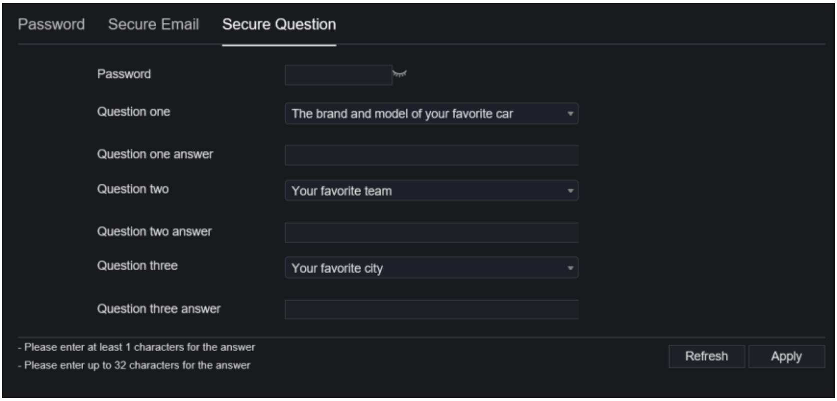


----End

8.7.4.3 Secure Question

If the user forgets the password and answers the security question correctly, the user can change the password to log in to the DVR.

Figure 8-76 Secure question



Password

Question one: The brand and model of your favorite car

Question one answer

Question two: Your favorite team

Question two answer

Question three: Your favorite city

Question three answer

- Please enter at least 1 characters for the answer
- Please enter up to 32 characters for the answer

----End

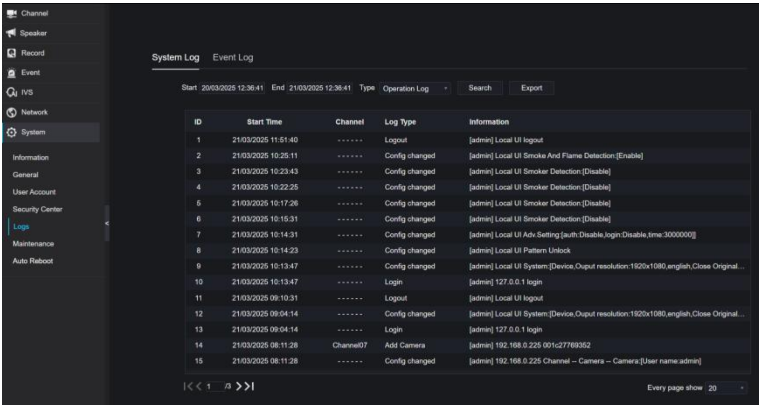
8.7.5 Logs

8.7.5.1 System Logs

Procedure

Step 1 On the **System Setting** screen, choose **System > Logs** to access the logs interface, as shown in Figure 8-77.

Figure 8-77 System log interface



Start 20/03/2025 12:36:41 End 21/03/2025 12:36:41 Type Operation Log

ID	Start Time	Channel	Log Type	Information
1	21/03/2025 11:51:40	------	Logout	[admin] Local UI logout
2	21/03/2025 10:25:11	------	Config changed	[admin] Local UI Smoke And Flame Detection:[Enable]
3	21/03/2025 10:23:43	------	Config changed	[admin] Local UI Smoker Detection:[Disable]
4	21/03/2025 10:22:25	------	Config changed	[admin] Local UI Smoker Detection:[Disable]
5	21/03/2025 10:17:26	------	Config changed	[admin] Local UI Smoker Detection:[Disable]
6	21/03/2025 10:15:31	------	Config changed	[admin] Local UI Smoker Detection:[Disable]
7	21/03/2025 10:14:31	------	Config changed	[admin] Local UI Adv.Setting:[auth:Disable,login:Disable,time:3000000]]
8	21/03/2025 10:14:23	------	Config changed	[admin] Local UI Pattern Unlock
9	21/03/2025 10:13:47	------	Config changed	[admin] Local UI System:[Device,Ouput resolution:1920x1080,english,Close Original...
10	21/03/2025 10:13:47	------	Login	[admin] 127.0.0.1 login
11	21/03/2025 09:10:31	------	Logout	[admin] Local UI logout
12	21/03/2025 09:04:14	------	Config changed	[admin] Local UI System:[Device,Ouput resolution:1920x1080,english,Close Original...
13	21/03/2025 09:04:14	------	Login	[admin] 127.0.0.1 login
14	21/03/2025 08:11:28	Channel07	Add Camera	[admin] 192.168.0.225 001c27769352
15	21/03/2025 08:11:28	------	Config changed	[admin] 192.168.0.225 Channel -- Camera -- Camera:[User name:admin]

1 /3

Every page show 20

Step 2 Set start time and end time from the calendar.

Step 3 Select the log type from the drop-down list.

Step 4 Click **Search** to acquire log information.

Step 5 Click **Export** to export the logs.

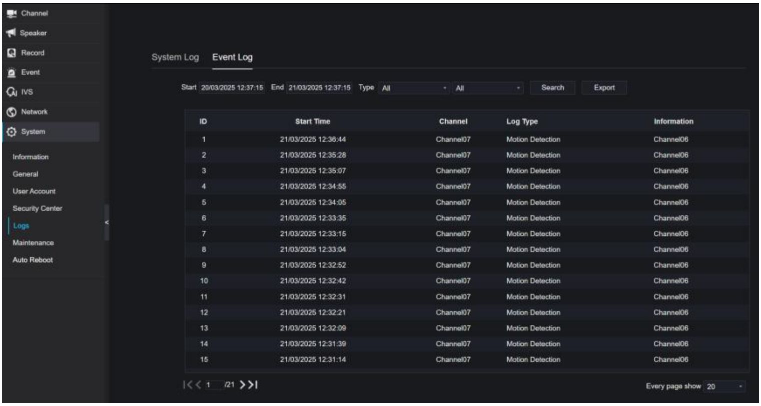
----End

8.7.5.2 Event

Procedure

Step 1 On the **System Setting** screen, choose **System >Logs > Event** to access the logs interface, as shown in Figure 8-78.

Figure 8-78 Event log interface



Start 20/03/2025 12:37:15 End 21/03/2025 12:37:15 Type All All

ID	Start Time	Channel	Log Type	Information
1	21/03/2025 12:36:44	Channel07	Motion Detection	Channel06
2	21/03/2025 12:35:28	Channel07	Motion Detection	Channel06
3	21/03/2025 12:35:07	Channel07	Motion Detection	Channel06
4	21/03/2025 12:34:55	Channel07	Motion Detection	Channel06
5	21/03/2025 12:34:05	Channel07	Motion Detection	Channel06
6	21/03/2025 12:33:35	Channel07	Motion Detection	Channel06
7	21/03/2025 12:33:15	Channel07	Motion Detection	Channel06
8	21/03/2025 12:33:04	Channel07	Motion Detection	Channel06
9	21/03/2025 12:32:52	Channel07	Motion Detection	Channel06
10	21/03/2025 12:32:42	Channel07	Motion Detection	Channel06
11	21/03/2025 12:32:31	Channel07	Motion Detection	Channel06
12	21/03/2025 12:32:21	Channel07	Motion Detection	Channel06
13	21/03/2025 12:32:09	Channel07	Motion Detection	Channel06
14	21/03/2025 12:31:39	Channel07	Motion Detection	Channel06
15	21/03/2025 12:31:14	Channel07	Motion Detection	Channel06

1 /21

Every page show 20

Step 2 Set start time and end time from the calendar.

Step 3 Select the event type from the drop-down list.

Step 4 Click **Search** to acquire log information.

Step 5 Click **Export** to export the event logs.

----End

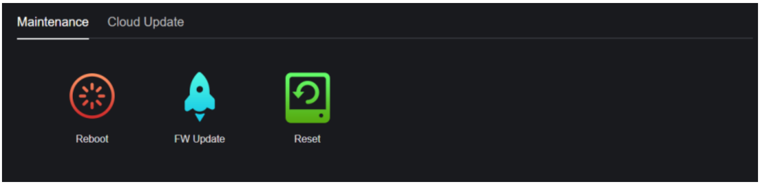
8.7.6 Maintenance

8.7.6.1 Maintenance

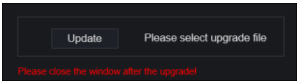
Procedure

Step 1 On the **System Setting** screen, choose **System >Maintenance** to access the maintenance interface, as shown in Figure 8-79.

Figure 8-79 Maintenance interface



Step 2 Click **Reboot**. The pop-up message will show you, click OK to reboot.



Update Please select upgrade file

Please close the window after the upgrade!

Step 3 Click **Update**. The message shows , choose software from a specific location to update.

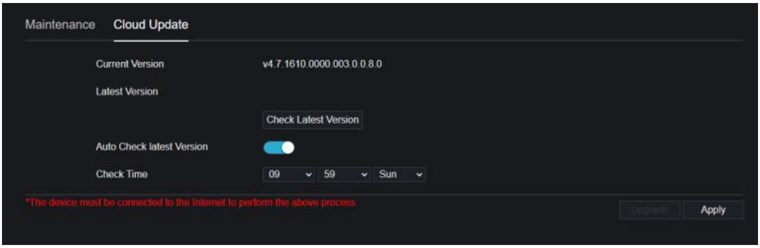
Step 4 Click **Reset**, and the pop-up message/will show you, click OK to reset.

8.7.6.2 Cloud Update

If the device is online and the cloud server has the latest software, click **Check Latest Version** to check the latest software, and click **Update** to start updating.

Users can set auto-checking every week at the same time.

Figure 8-80 Cloud update



Current Version v4.7.1610.0000.003.0.0.8.0

Latest Version

Auto Check latest Version

Check Time 09 59 Sun

*The device must be connected to the Internet to perform the above process

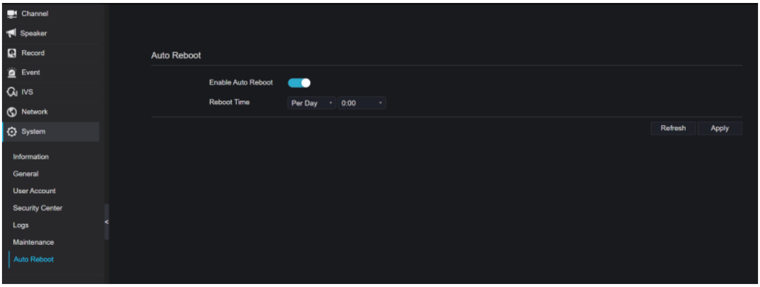
----End

8.7.7 Auto Reboot

Procedure

Step 1 On the **System Setting** screen, choose **System > Auto Reboot** to access auto restart and enable the auto restart, the screen as shown in Figure 8-81.

Figure 8-81 Auto restart



Auto Reboot

Enable Auto Reboot ●

Reboot Time Per Day 0:00

Step 2 Select one type of restart time from the drop-down list.

Step 3 Click Apply to save settings. Click Refresh to return to the previous setting.

----End

9 Disk Compatibility

The hard disks in the following list are tested and certified by our company. If you want to use other hard disks, please consult our technical staff.

Table 9-1 Disk specification

Hard Disk Brand	Type	Model	Capacity	Verification of Platform
WD (Western Digital)	Monitoring-grade	WD221PURP	22TB	All platform
		WD10EJRX	1TB	
		WD30PURZ	3TB	
		WD20EJRX	2TB	
		WD121EJRX	12TB	
		WD82EJRX	8TB	
		WD60PURX	6TB	
		WD30PURX	3TB	
		WD40EJRX	4TB	
		WD10EZEX	1TB	
		WD30EURS	3TB	
		WD20EURS	2TB	
		WD40PURX	4TB	
		WD30EJRX	3TB	
		WD84EJRX	8TB	
		WD102EJRX	10TB	
		WD180EJRX	18TB	
		WD23PURZ	2TB	
		WD64PURZ	6TB	

		WD85PURZ	8TB	
		WD11PURZ	1TB	
		WD43PURZ	4TB	
		WD10PURZ	1TB	
		WD40PURZ	4TB	
		WD22PURZ	2TB	
		WD63PURZ	6TB	
		WD84PURZ	8TB	
		WD101PURP	10TB	
Seagate	Monitoring-grade	ST3000VX010	3TB	
		ST2000VX008	2TB	
		ST4000VX000	4TB	
		ST8000VX0002	8TB	
		ST31000528AS	1TB	
		ST2000VX000	2TB	
		ST6000VX0001	6TB	
		ST1000VM002	1TB	
		ST1000VX005	1TB	
		ST2000VM005	3TB	
		ST3000VM006	3TB	
		ST3000VX009	3TB	
		ST4000VM004	4TB	
		ST4000VX007	4TB	
		ST8000VX004	4TB	
		ST10000VE0008	10TB	
Toshiba	Monitoring level grade	DT02ABA600VH	6TB	
		DT02ABA400V	4TB	
		HDKJB01QAA01	1TB	
		DT01ABA100V	1TB	
		HDWT720	2TB	
		HDWT860	4TB	
		WUS721010ALE6L4	10TB	

WD (Western Digital)	Enterprise-grade	HUS728T8TALE6L4	8TB	
		HUS722T2TALA604	2TB	
		HUS726T4TALEL	4TB	
Seagate	Enterprise-grade	ST2000NM000B	2TB	
		ST4000NM024B	4TB	
		ST8000NM017B	8TB	
		ST8000NM000A	8TB	
		ST10000NM017B	10TB	
		WUH721816ALE6L4	16TB	

Video recording size per channel per hour =bitrate (kbps)*3600/1200/8 (M)

Recording duration =Total hard disk capacity (M) / Video recording size per channel per hour/number channels (H)