Network Video Recorder (NVR)
User Manual

Issue	**V4.7.2**
Date	**2025-03-07**

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 NVR, DVR, and IP 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 NVR, you do not need to forward the port for each camera. Only the ports of the NVR 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 PoE to connect IP cameras to NVR.

IP cameras connected to the NVR using PoE will be isolated from other networks so that they cannot be accessed directly.

13. Network isolation between NVR and IP cameras

We recommend isolating your NVR 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 NVR (Network Video Recorder) device.

Modify Log

ID	Version	Log	Release Time
1	V 4.0	Initial Release	2017/10
2	V 4.1	Add new function	
3	V 4.1.3	Perfect interface, add new models	
4	V 4.1.5	Add reverse playback Open data port 2	2018/01/06
5	V 4.1.6	Add 4 spilt screens of automatic adjusting mainstream or substream. Add private protocol access. Support multi-screen playback. Add the schedule recording function by channel setting Increase the allocation of permissions by channel	
	V 4.2	Add boot wizard Add toolbar Add manual recording and instant playback Add multiple clicks to enlarge Add user lockout Remove the upper right corner to display the alarm warning Add the view of the latest alarm information, modify the manual alarm Modify quick navigation content Preview channel and modify network parameter function on the IPC side	

		Support for copying to some or all channels Remove the full-screen function Add backend backup Add video dual authentication Intelligent motion detection Add the color to distinguish the video type, add the video type search Add sound switch Add instant playback Remove the timeline function Increase intelligence analysis Increase test DDNS function Increase test mail function Modify the time precision to half an hour, and remove the recording plan master switch. Add hardware information Added video dual authentication and boot wizard configuration function Add alarm log Add interval update profile	
6	V 4.2.1	Add the NTP synchronization interval and add the manual NTP synchronization interval. Add access to thermal imaging cameras and display IPC product models Remove auto-hide Add the patrol route and line-scan function Add upgrade IPC, restart IPC, restore factory IPC Increase the selection of main and substream backups Add a playback button to play video Add UI to display detailed intelligent analysis of IPC Add 802.1x functionality Add SNMP function Add upgrade device features Add the timing restart function	

		Add U disk upgrade display the progress bar	
7	V 4.2.4	Increase U-boot and kernel version display Increase P2P status display Increase signal type display Increase the POE icon display Increase SSL access IPC, special models support Optimize username and password-saving methods Increase batch backup Increase fixed-point playback Increase hard disk alarm Optimize the recording expiration time input mode to be editable Add city information for each time zone Add face recognition Add P2P server	
8	V 4.3	Add pattern unlock Add mailbox reset password Increase the secure question reset password Add 1+7 split screen Add channel information display Add 3D dome camera Remove live video type switch Add RAID Add S.M.A.R.T Add formatting (fat32 and NTFS) Support quick download event video backup Add event video backup Add pop-up full screen and send screenshot by email Add IPC intelligent analysis configuration Add manual input automatic logout time Restore factory refinement	
9	V4.4	Support adding POE cameras automatically or	

		manually. Support NVR network provided by 3G/4G modem. Support cloud storage. Add disk detection, disk group, and multi-channel recording. Support license plate recognition management. Support through RTSP to add cameras. Add thermal imaging and face detection functions. Add alarm of IP address conflict and abnormal internet connection.	
10	V4.5	Add disk capacity calculation Add viewing network traffic Add alarm output function Add ROI Add the function of the human body thermometer Add temperature schedule linkage Add smart functions Add smart tracking Add microphone Add the synchronization camera time Add people counting Add IO control push message alarm Add the log of alarm events sent by email	2020/05
11	V4.5.1	Add mask detection configuration Increase people counting configuration Optimize the function of adding camera channels manually Optimize record schedule Optimized auto sequence Increase NAT port settings Increase network packet capture Add advanced settings to monitor the channel when logout	

		Add license plate data import and export Detailed alarm events and logs Add the snapshot of real-time video and playback video	
12	V4.6.1	Add HTTPS port configuration Optimize the logic of IPC WEB jump from external network Add multiple layouts Support selection of preview strategy Add audio playback function at WEB Add event retrieval recording and backing up data through events at WEB Add modification of the IP address and subnet mask of the IPC Support ANR/auto network replenishment Add WDDA function of disk Support HTTPS port, used for https access to WEB pages Add an electronic fence feature to the active deterrent camera Add the allowable phone number and refine the backup authority Add multiple layouts to auto-sequence The system log is saved to flash and hard disk	
13	V4.7	Add local intelligence analysis Add remarks about special functions Add web NAT Add smart motion detection Add failover Update cloud update Modify the pictures Delete WiFi chapter Delete ADAM chapter Delete cloud storage	
14	V4.7.2	Update images and architecture Remove body temperature measurement and	

		masks Add IP speakers	

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

- **POE Device:** The front-end devices of POE are required to be installed indoors.
- **Put On Desktop:** The NVR 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** NVR 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 NVR 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 NVR 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

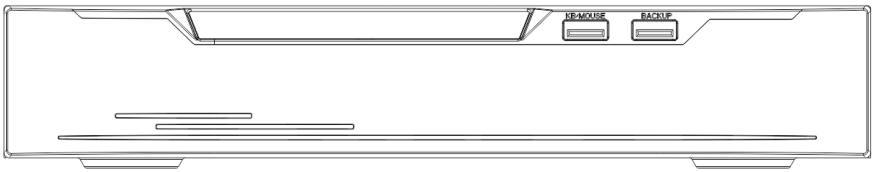


Table 2-1 Front panel function

Port	Description
PWR	When the NVR is operating, the PWR indicator is steady. When the NVR is shut down, the PWR indicator is turned off.
HDD	Hard disk status indicator. This indicator flashes when data is transmitted.
POE	PoE network status indicator. This indicator flashes when data is transmitted.
KB/MOUSE	Only connected to a USB mouse.
BACKUP	Only connected to U disk.

Figure 2-2 Model B

Table 2-2 Front panel function

Port	Description
PWR	When the NVR is operating, the PWR indicator is steady. When the NVR 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.

2.2 Back Panel

The 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 3964E8-P16E-J

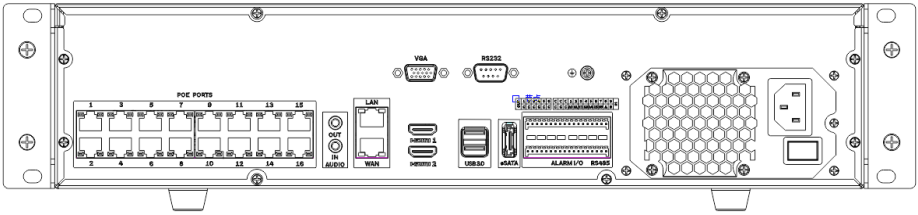


Figure 2-4 3964E4-J

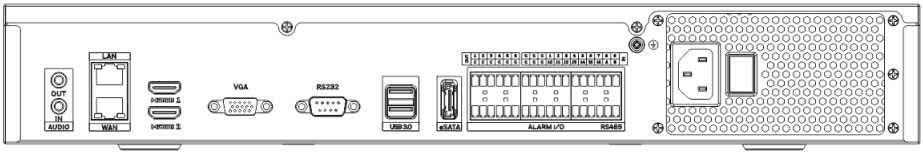
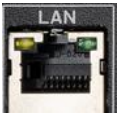
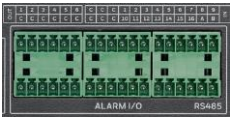


Table 2-3 Rear panel function

Port	Description
 LAN	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 NVR. If there is only a LAN interface, the LAN can be connected to an external Wide Area Network.

 WAN	RJ45 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 NVR.
 Audio output / Audio input	Audio output can be connected to audio output devices such as speakers. Audio input can be connected to audio input devices such as microphones. These interfaces are required for the intercom.
 HDMI/HDMI1/HDMI2	HDMI/HDMI1/HDMI2, 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.
 RS232	Standard RS232 serial communication interface of the device.
 USB port	Only connected to 3.0 U disk.
 ESATA port	Connected external hard disk interface.
 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. A/B represents the two terminals of RS485

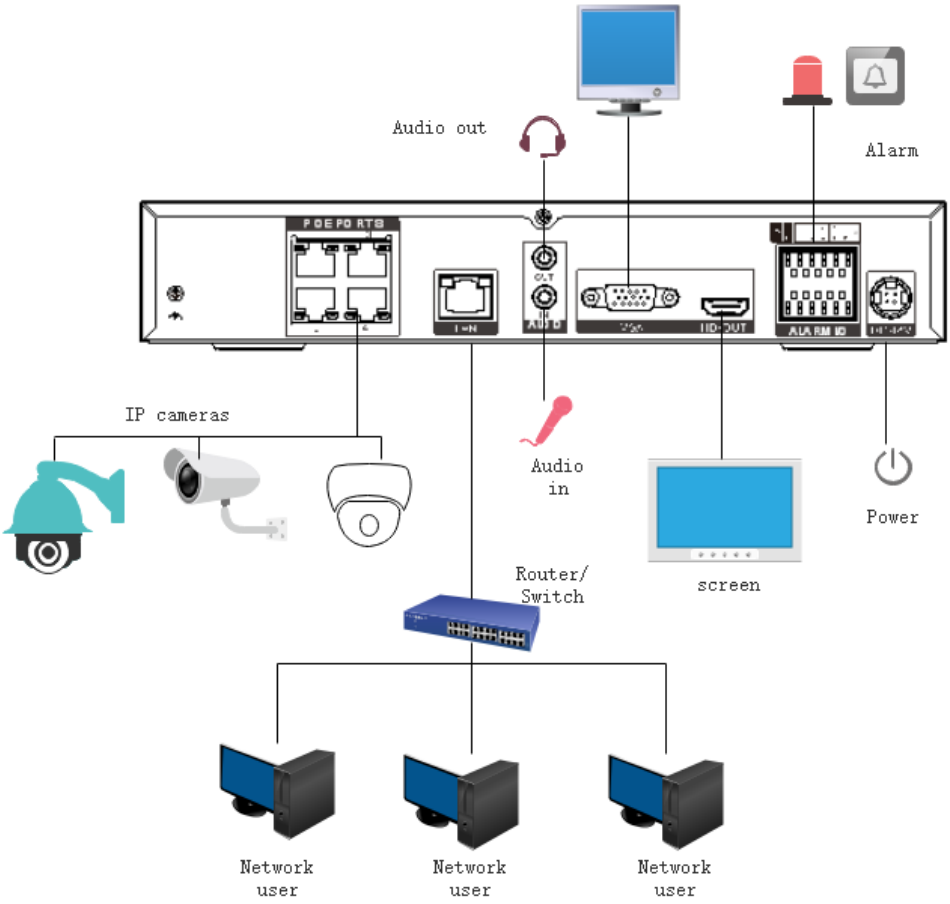
 GND	GND, safety grounding screw.
 POE port	POE network interfaces and cameras can be plugged in directly. It can also support the POE supply.
 Power switch	Power switch
 Power socket	Connected to an external power adapter DC 12V.
 Power socket	AC 110V/220V power input interface
 Power socket	Connected to an external power adapter DC48V.
 Power socket	The redundant power supplies.

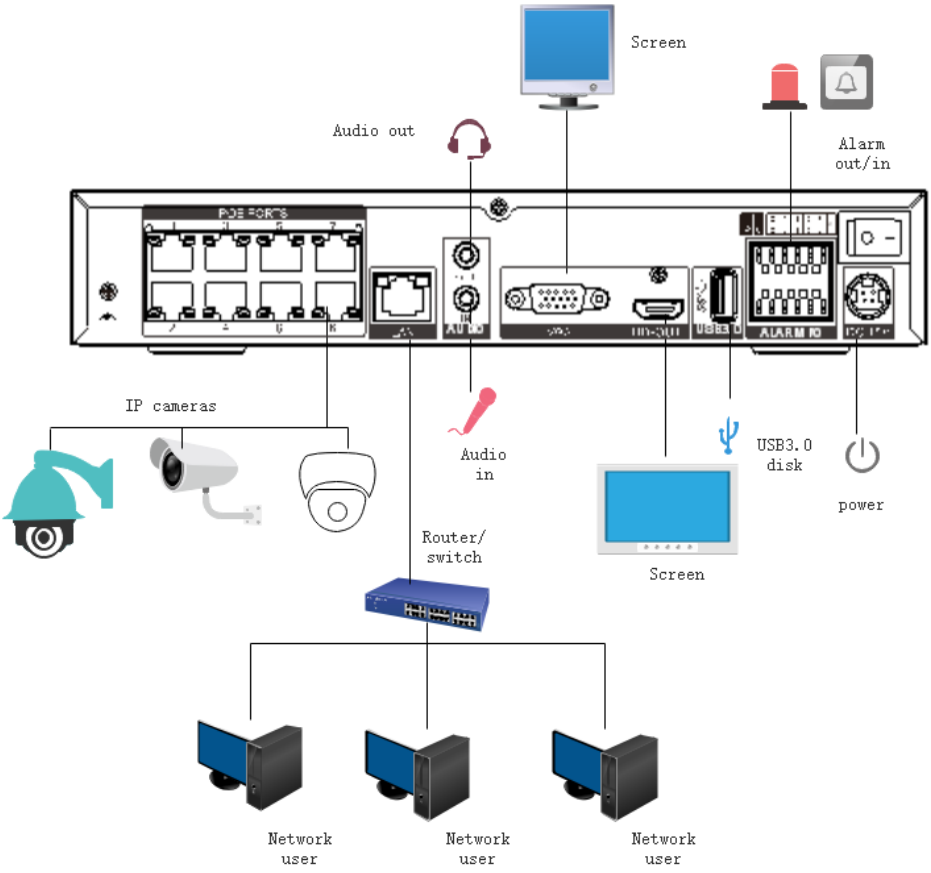
2.3 Connection of NVR

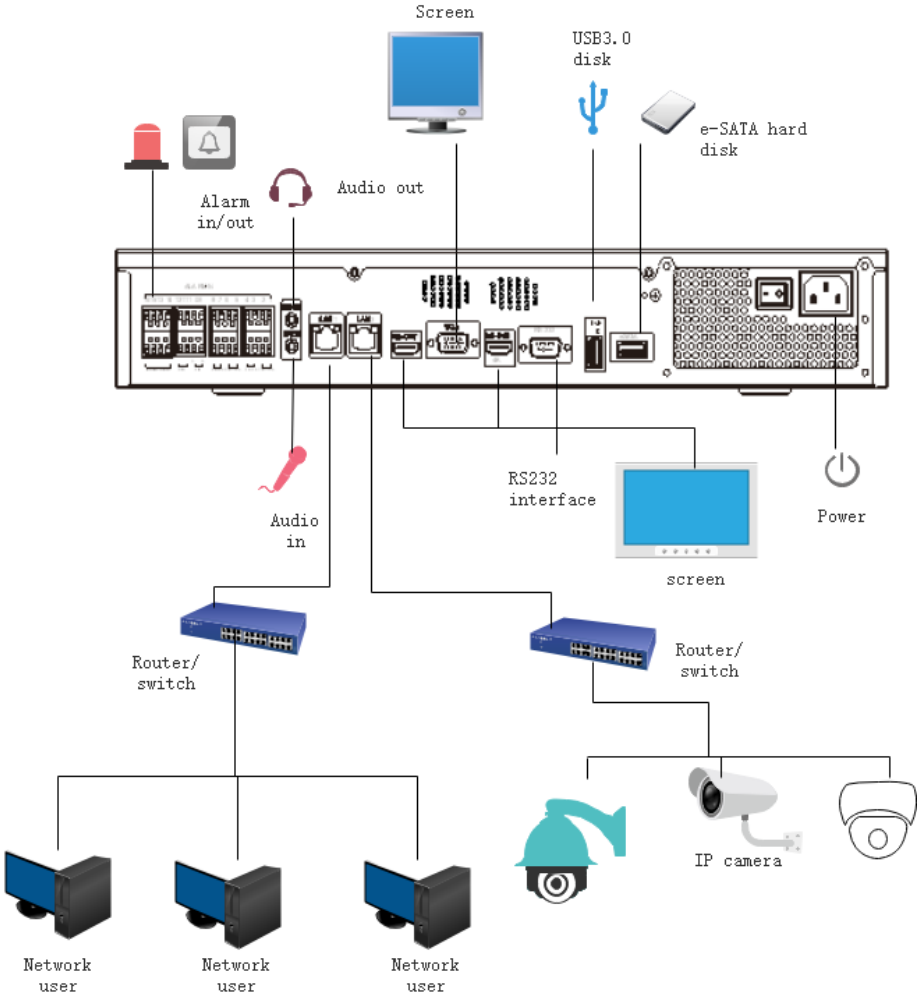
NOTE

The pictures below are for your reference only

Figure 2-5 Connection of NVR




Screen
Audio out
Alarm
out/in
IP cameras
Audio
in
USB3.0
disk
power
Router/
switch
Screen
Network
user
Network
user
Network
user



2.4 Important Notes

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

The NVR 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 NVR 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.

2.5 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 NVR.
- The information in this user manual applies to the full series NVR, **NVR3932E2**, as an example for description.
- **Read this user manual** carefully before using the NVR, and follow the methods described in this manual when using the NVR.
- If you have any doubts when using the NVR, 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.

2.6 Installation Environment and Precautions

Installation environment

Table 2-4 defines the installation environment of the NVR.

Table 2-4 Installation environment

Item	Description
Electromagnetism	The NVR 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 2A(1 HDD non POE) DC 48V 2A(1 HDD) or AC110/ 220V 4A(2 HDDs or more)’ please refer to actual products.
Power consumption	<15W (not including the hard disk)

Installation precautions

Note the following points when installing and operating the NVR:

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

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

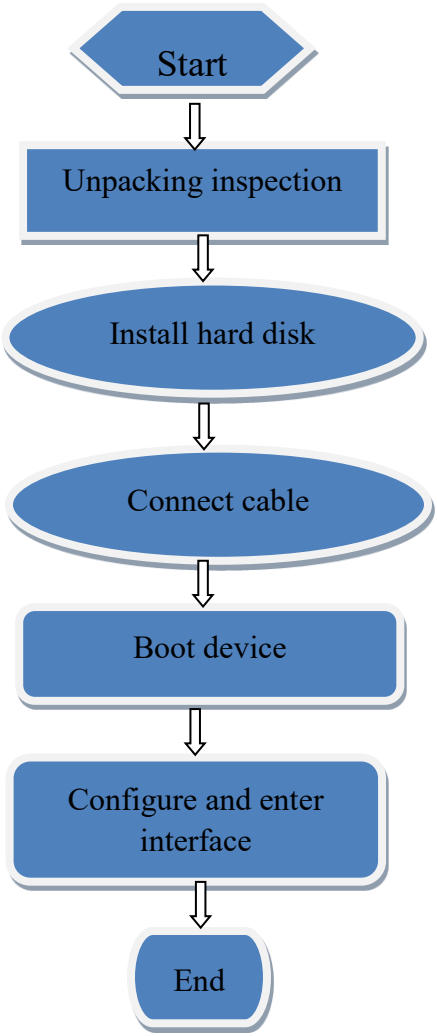
Other Precautions

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

The NVR 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

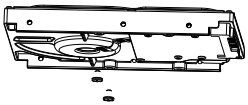
- When replacing the hard disk, please **turn off the power** and then open the device to replace the hard disk.
- Please use the monitoring dedicated SATA hard disk recommended by the hard disk manufacturer.
- Choose the hard disk capacity according to the recording requirements.

3.3.1 Install One Or Two Hard Disks

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

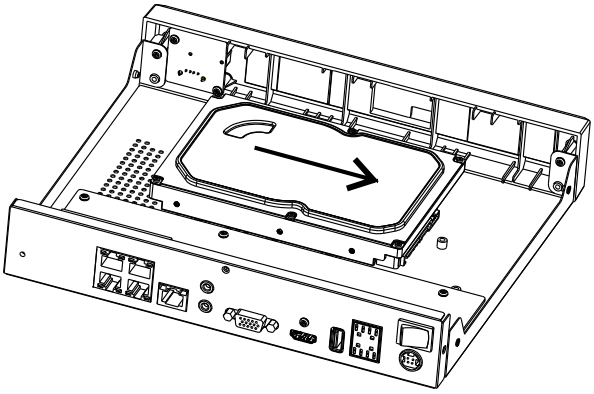
Step 2 Take out the screws and silicone cushion, pass the screws through the silicone cushion, and secure it to the screw holes, as shown in Figure 3-1.

Figure 3-1 Installing the hard disk screws



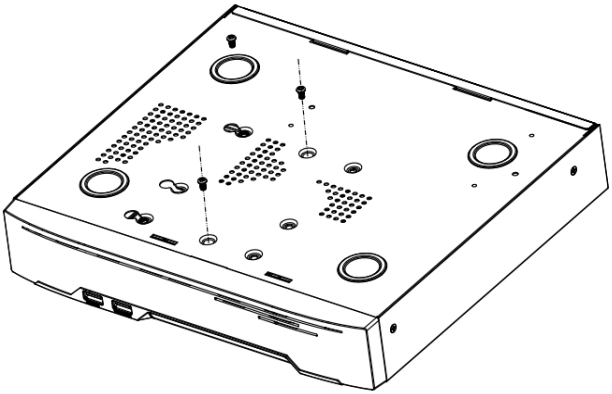
Step 3 Pass the screws through the holes on the base and put the hard disk in place, as shown in Figure 3-2.

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



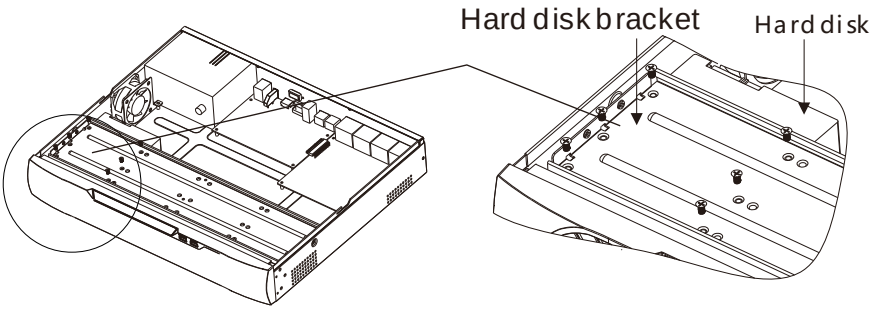
Step 5 Insert the hard disk data cable and power cable, then put back the upper cover and fasten the fixing screws.

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.

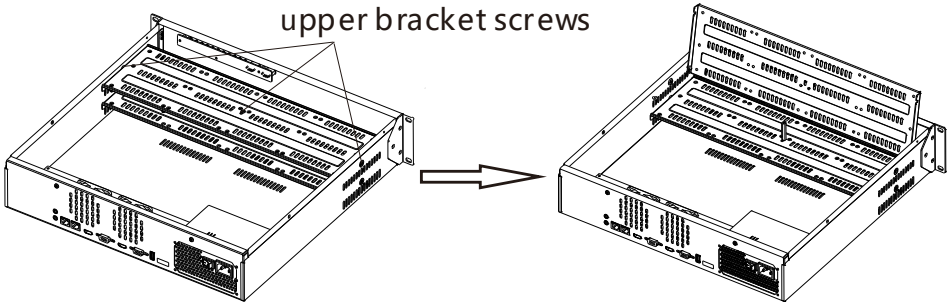
Step 4 Insert the hard disk data cable and power cable, and then put back the upper cover and tighten the fixing screws.

3.3.3 Install Eight Hard disks

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

Step 2 Loosen screws on both sides to lift the upper bracket as shown figure.

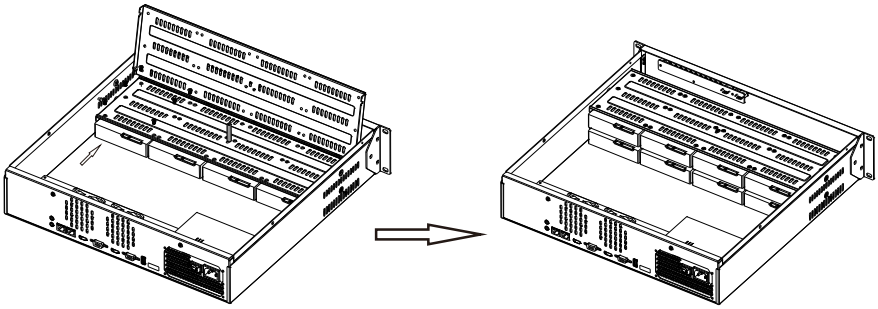
Figure 3-5 Loose screws lift the upper bracket



Step 3 Put the hard disk under the lower bracket, hold the hard disk with one hand, and aim the hard disk hole at the bracket hole, then fix the screws for the hard disk, as shown in Figure 3-6.

Step 4 Pull down the upper bracket and secure it by tightening the screws, then install other hard disks in the upper layer following step 3, as shown in the right figure in Figure 3-6.

Figure 3-6 Unscrew the screws lift the upper bracket



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

NOTE

Users need to provide a hard disk for the NVR. 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 NVR. Format the hard disk.
- The hard disk is damaged.

4 Basic Operations

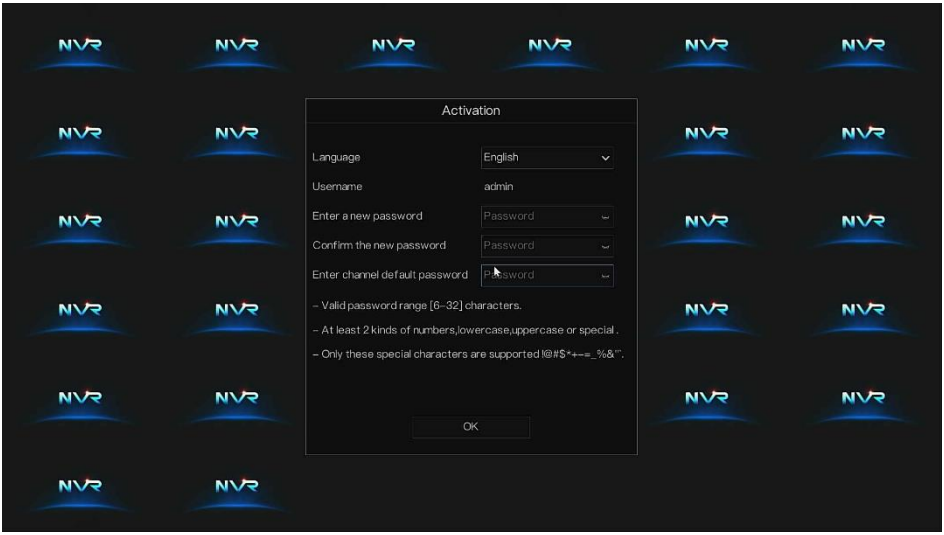
4.1 Power on the Device

CAUTION

- Ensure that the NVR 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 NVR before powering on.
- In some environments, an abnormal power supply may cause the failure of the NVR to work properly and even damage the NVR in severe cases. It is recommended to use a **regulated power supply** to power up the NVR in such environments.

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

Figure 4-1 Real-time video screen



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

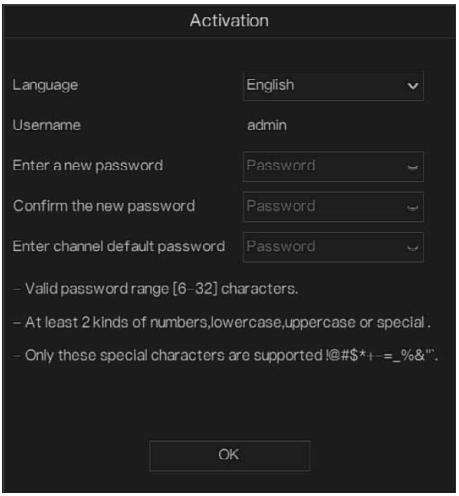
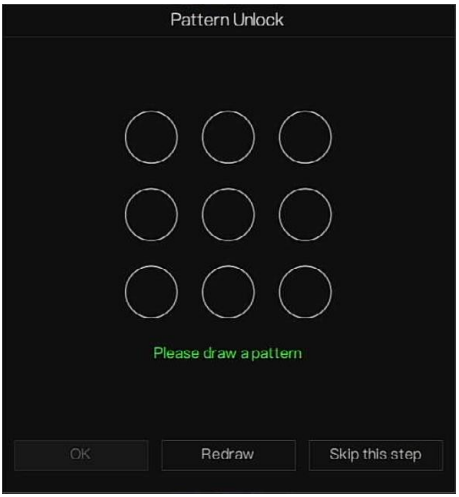


Table 4-1 Description of activation

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 NVR 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

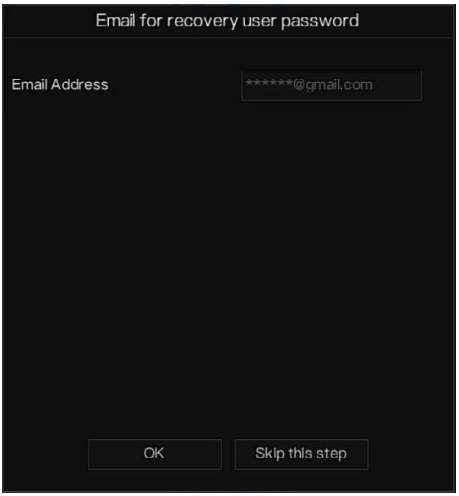


NOTE

- 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

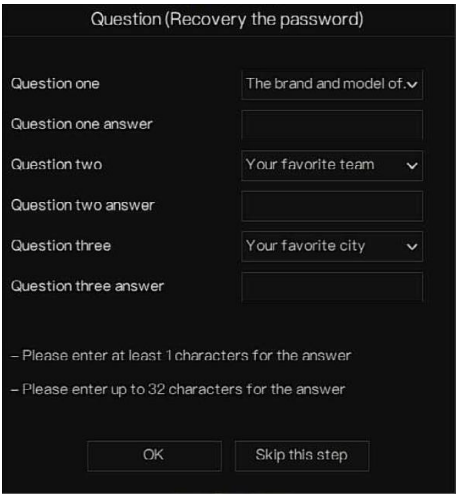


NOTE

- 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



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 NVR; 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

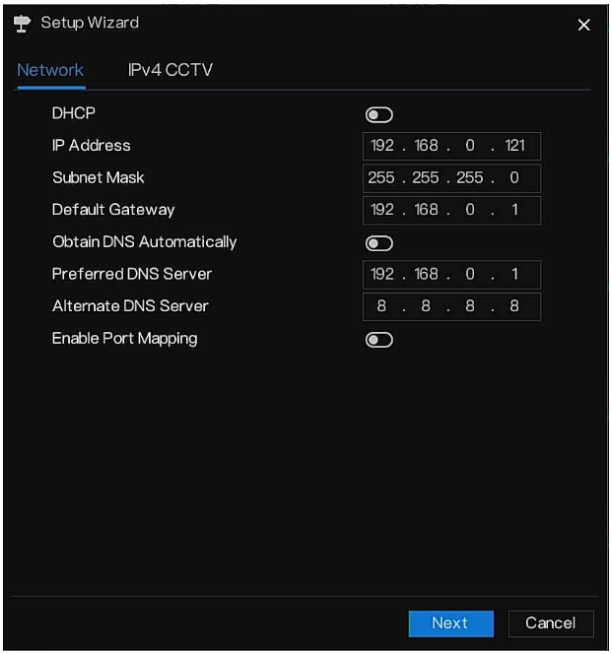
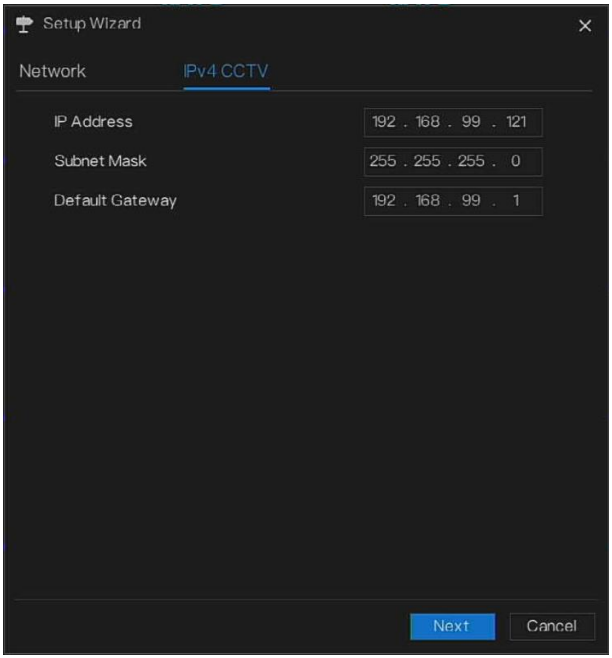


Figure 4-8 IPv4CCTV



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

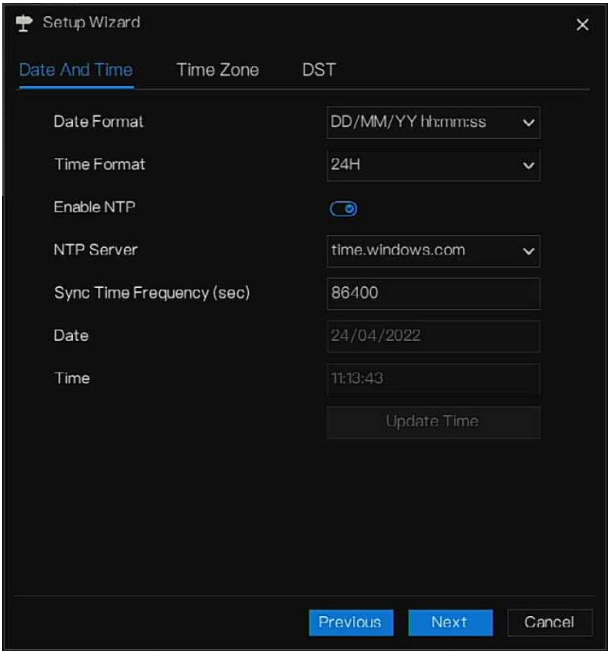
Table 4-1 Network parameter

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
Obtain DNS automatically	Enable the function to get the DNS address automatically.	[Setting method]

Parameter	Description	Configuration
	If you learn about the local DNS server IP, you can input the preferred DNS server and alternate DNS server manually.	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



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

Enable NTP:

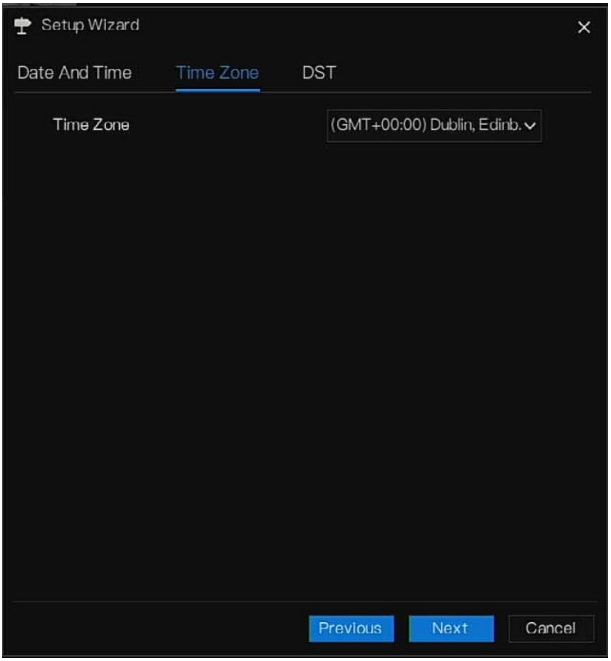
- Click  to synchrony time from the network.

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.

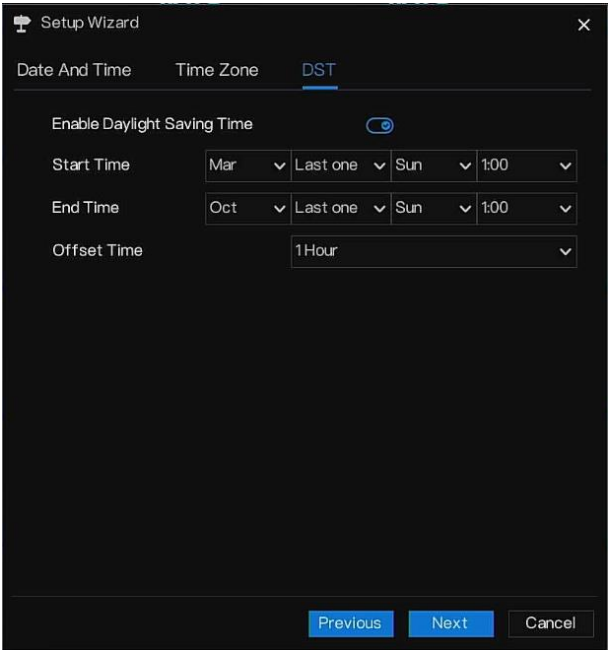
Step 3 Click **Time Zone,** and choose the current time zone from the drop-down list as shown in Figure 4-10.

Figure 4-10 Wizard of time zone



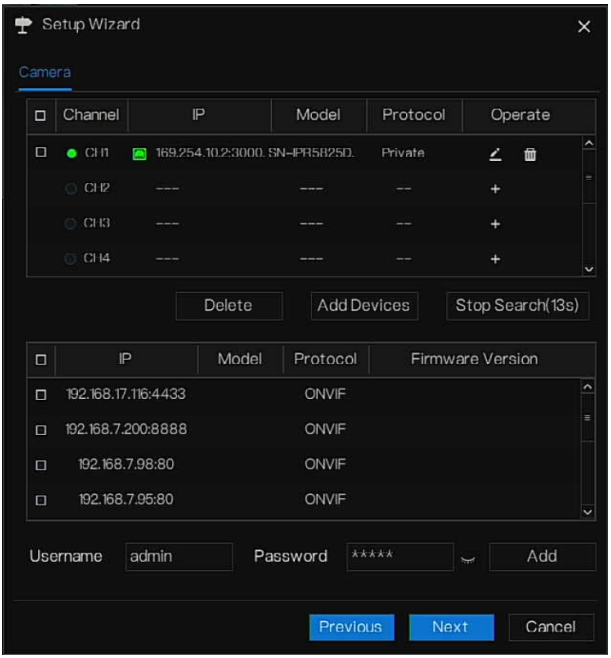
Step 4 Click **DST,** enable the DST, and set the start and the end time. Select offset time from the drop-down list.

Figure 4-11 Wizard of DST



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

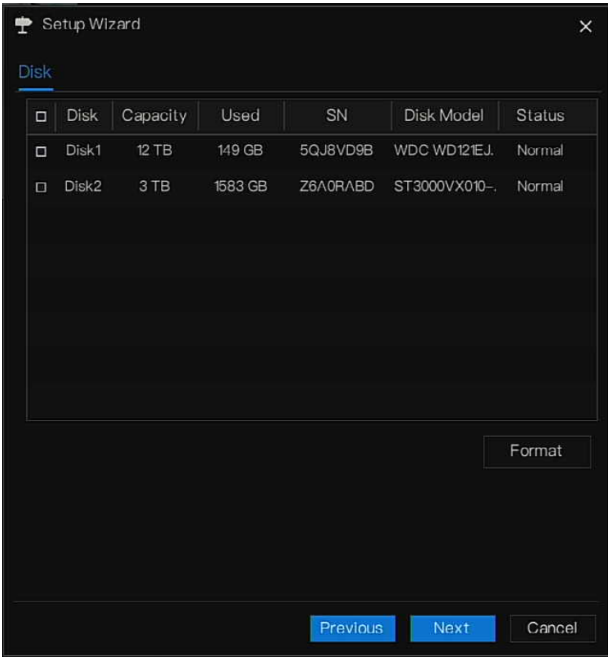
Figure 4-12 Wizard of adding camera



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.

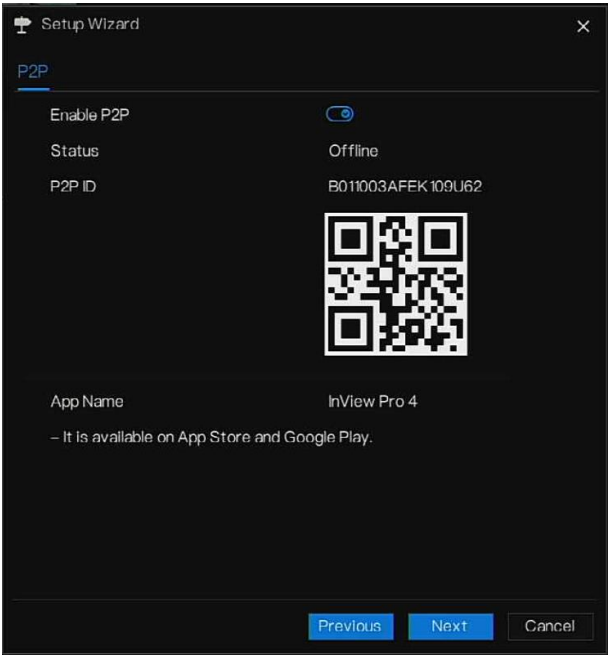
Figure 4-13 Wizard of disk



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

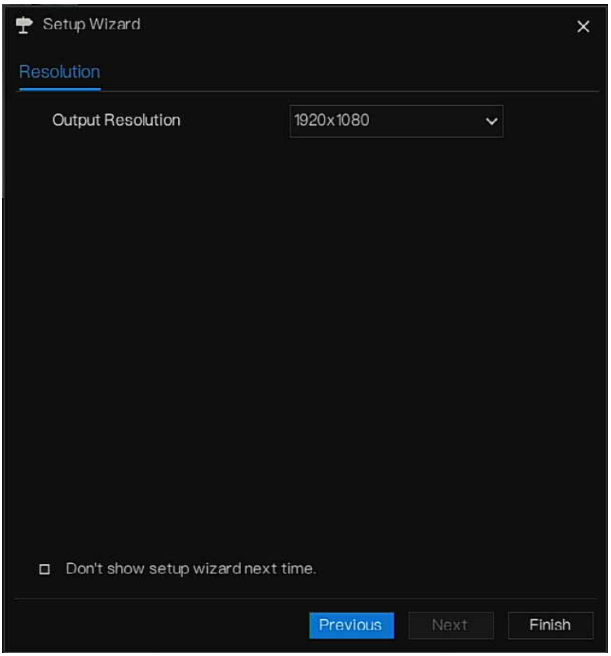


Step 8 Enable the P2P, user can use mobile devices to manage the NVR by scanning the P2P ID if the mobile phone has loaded the (search the APP at the **App Store** or **Google Play**).

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



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 NVR. If there is a power switch on the rear panel of the NVR, you can power off the power switch to disconnect the NVR 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 NVR 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

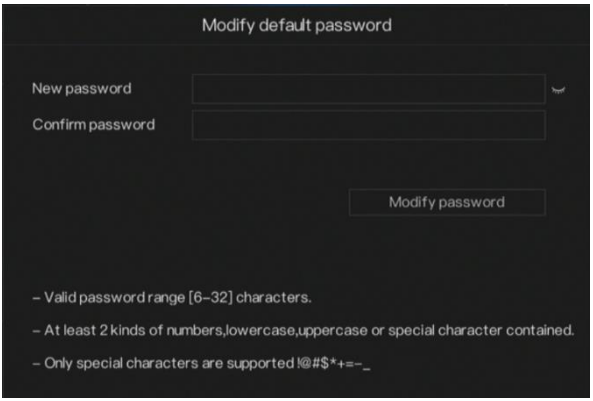
If the password is incorrect more than 3 times, please log in again after 5 minutes. You can also power off and power on to start the device and input the correct password to avoid waiting five minutes.

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.

Step 4 Click Login to access the main User Interface (UI). Modify the default password, as shown in Figure 4-18

Figure 4-18 Modify default password



----End

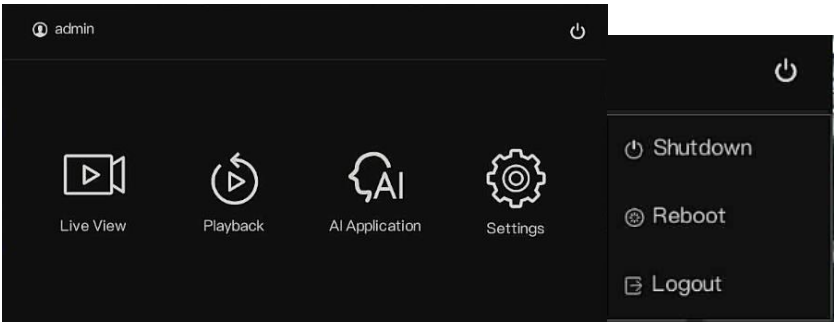
5 Quick Navigation

5.1 Quick Bar

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

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

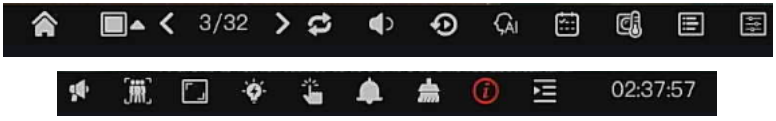
Figure 5-1 Quick home menu



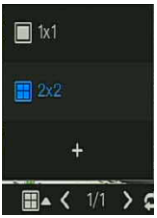
In the middle of the NVR floating menu bar, the video toolbar provides **video window switching**, **auto SEQ, volume, playback,** and **channel information,** as shown in Figure 5-2.

Figure 5-2 Real-time video toolbar

Figure 5-3 Toolbar (recognized mode)

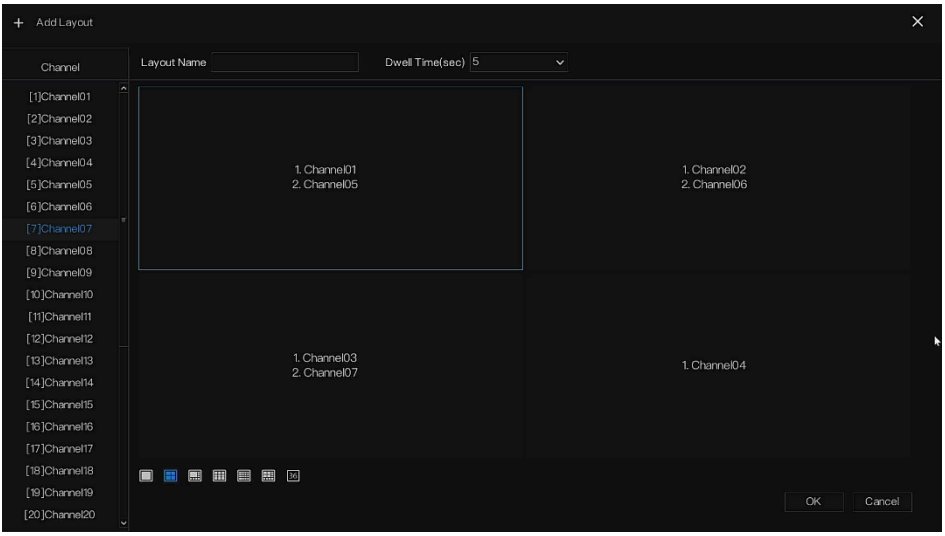


The real-time video toolbar is as follows:



Layout. Users can choose the layout and add new layout strategies as shown in Figure 5-4. Click on the right of the screen-splitting format and choose the channels to view the video. Click + to add a new layout.

Figure 5-4 Add layout



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 the screen is enabled. For how to set the dwell on, please see *Chapter 6.7.5.*

Audio. Click on the icon, and 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.

AI Application. Click the icon to enter the **AI Application** interface. On this page, users can search **face detection**, **license plate detection**, **full-body search**, **vehicle search**, and **people counting**. Set the archive's library of human faces and license plates. If the "Alarm > Local intelligent analysis > General Mode" item is set to **Detection mode**, these human faces and Attendance will **be hidden**.

Attendance. Click the icon to enter the attendance interface.

Thermal. Click the icon to enter the thermal 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 NVR floating menu bar. The main menu quick toolbar provides **Manual alarm, Alarm information, Clean alarm, Information,** and **time**, as shown in Figure 5-5.

Figure 5-5 Main menu quick toolbar

Broadcast. The user adds the speaker to the NVR 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 5-6 Broadcast

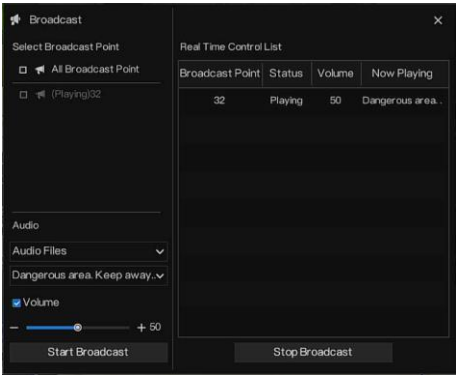
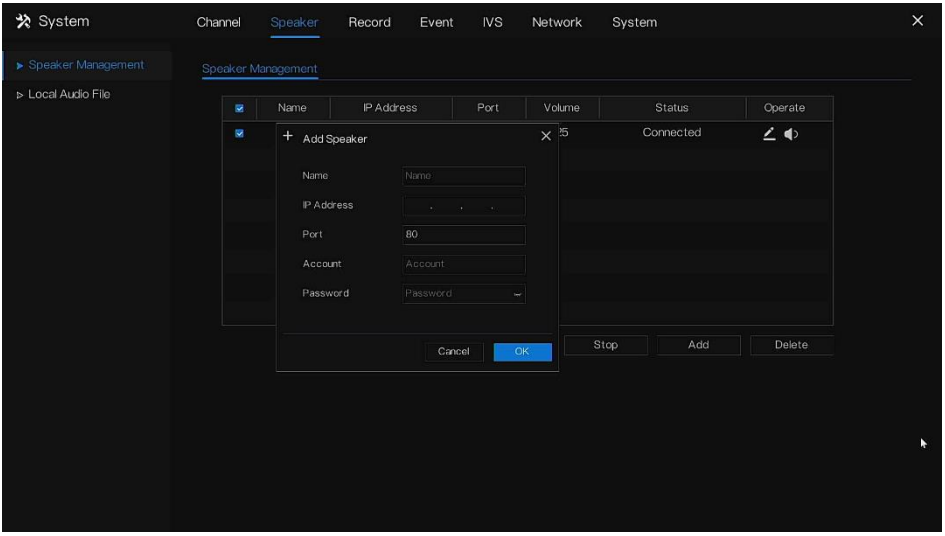


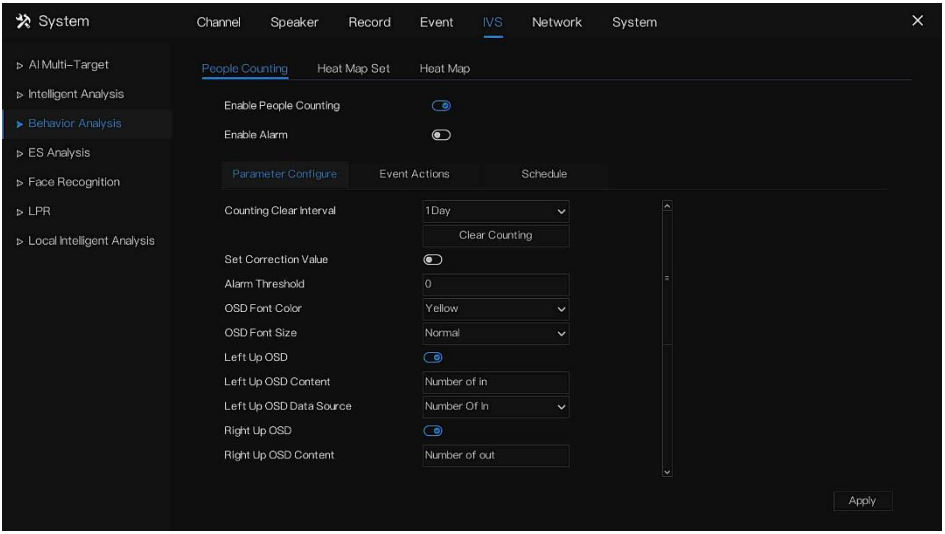
Figure 5-7 Add speaker



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

People counting. Click to show the data of people counting. Click again to close. The style of the show is set on **Settings > IVS > Behavior Analysis > People counting** interface.

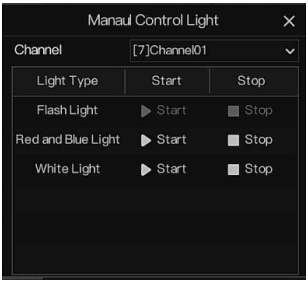
Figure 5-8 People counting



Open original scale. Click the icon to open the original scale; the split screens will play the live video at the original aspect ratio, or else they will play the video at a **16:9 aspect ratio**.

Manual control light. For the camera with the light (**flashlight**, **red and blue light**, or **white light**), click **Start** to open the light manually, and click **Stop** to close the light.

Figure 5-9 Manual control light

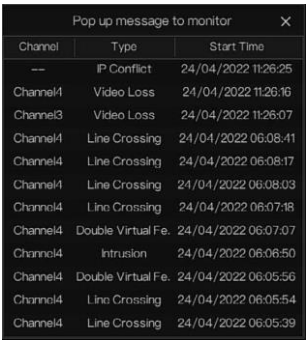


Manual alarm. Click the icon; users can set different channels, and choose alarm out, the window shows in Figure 5-10.

Figure 5-10 Manual alarm

: Event list, click on the icon for more details as shown in Figure 5-11.

Figure 5-11 Event list

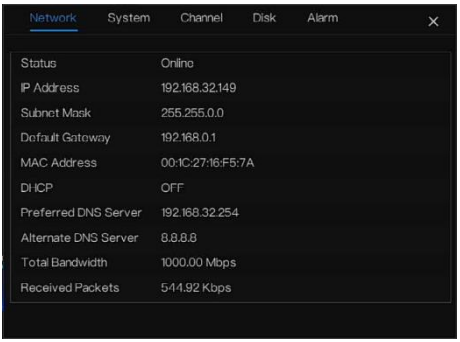


Clean alarm. Click the icon and clear the current alarm actions, like voice and external alarms out.

Information. Click the icon and the general information will show, like **network/system/channel/disk/alarm**, as shown in Figure 5-12.

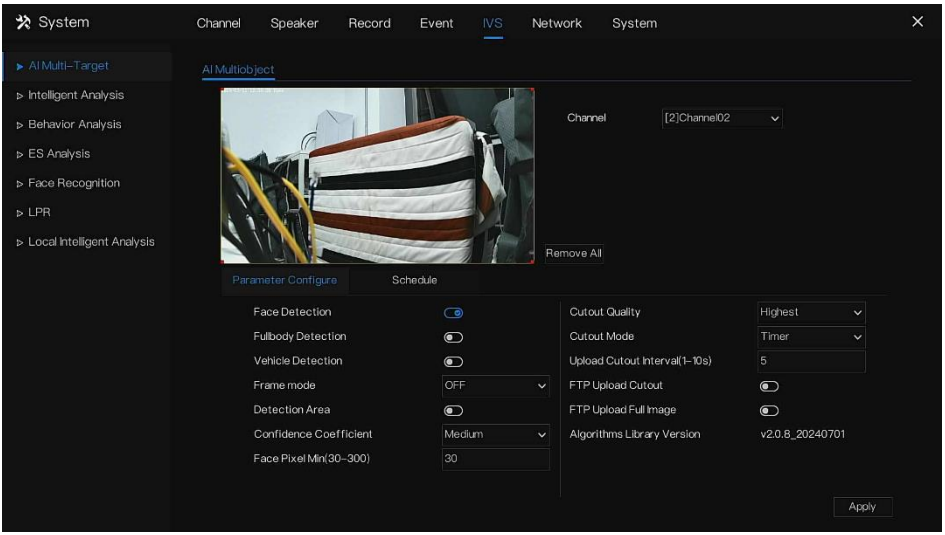
The red icon means the disk needs to be formatted.

Figure 5-12 Information



Disable snapshot list. The snapshot list is enabled by default. If you don't want to see the snapshot of human faces, you can disable it. The cameras should be enabled for the face detection/LPR, and so on.

Figure 5-13 AI multi-object

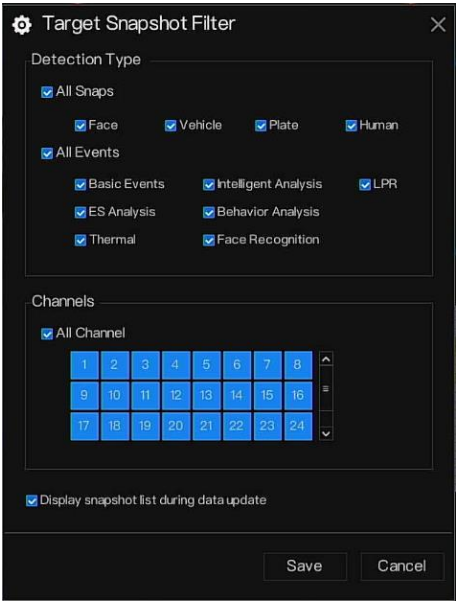


Choose one snapshot to playback, search the result by the picture, and add this one to the list.

Figure 5-14 Snapshot list

You can tick the detection type, such as **face**, **vehicle**, **plate**, or **human**. Choose the event types and channels, as shown in Figure 5-15.

Figure 5-15 Target snapshot filter



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.

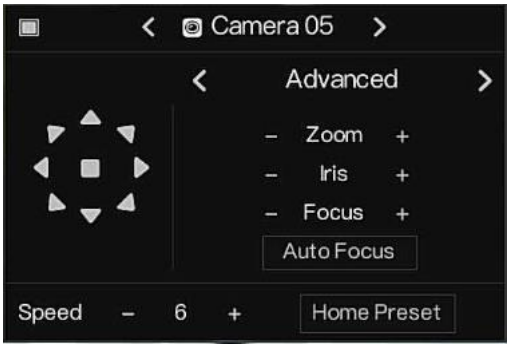
Instant playback: Click the icon, and the window will record the video from five minutes ago.

 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 5-16.

Figure 5-16 PTZ adjust screen



 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.

 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, and 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**.

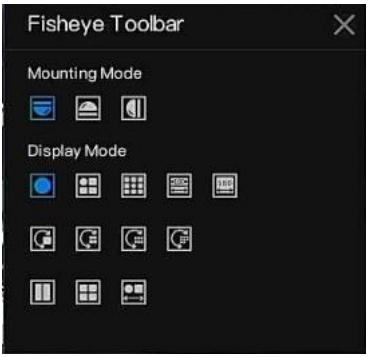
Figure 5-17 Camera picture parameter

Two-way audio. The NVR and camera can talk to each other.

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

Fisheye. Click to switch the fisheye modes for the current channel, as shown in Figure 5-18. Select the mounting mode, and then choose the display mode.

Figure 5-18 Fisheye



 The current channel is recording.

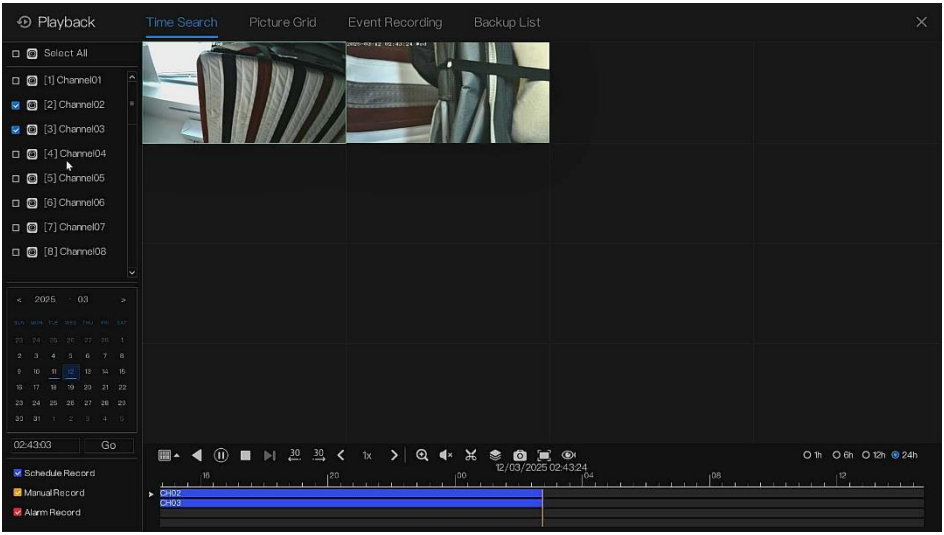
 **Alarm.** The current channel has a motion-detection alarm.

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 5-19.

Figure 5-19 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.

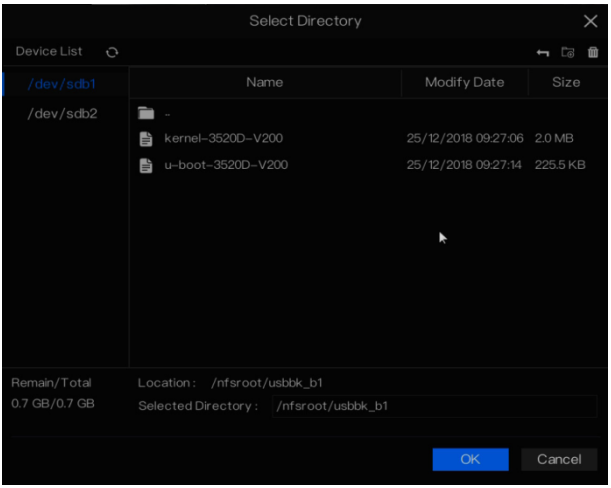
 **Zoom.** Roll the roller of the mouse to zoom in or out.

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 the **saving the file** pop-ups as Figure 5-20. Click **OK** to save.

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

Figure 5-20 Select directory

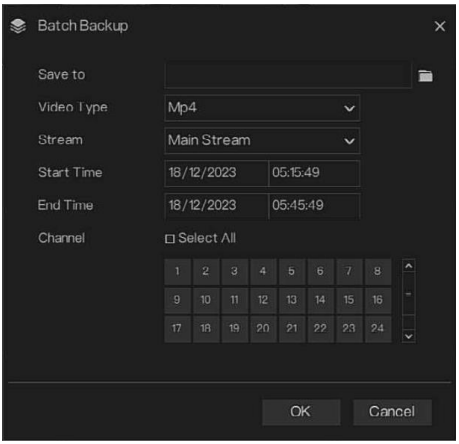


Batch backup.

1. Click the icon to backup multi-channels, as shown in Figure 5-21.
2. Choose the folder to save.
3. Select the stream information from the drop-down list.
4. Set the start time and end time, and select the channels.
5. Click **OK** to backup.

The backup videos are marked by a watermark; you can view them by our player. If the user adds the NAS account, the backup recording can be saved to the NAS.

Figure 5-21 Batch backup



 **Snapshot panorama.** Click to save it to a USB storage device on the NVR.

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

: Type of time bar, recording video can show.

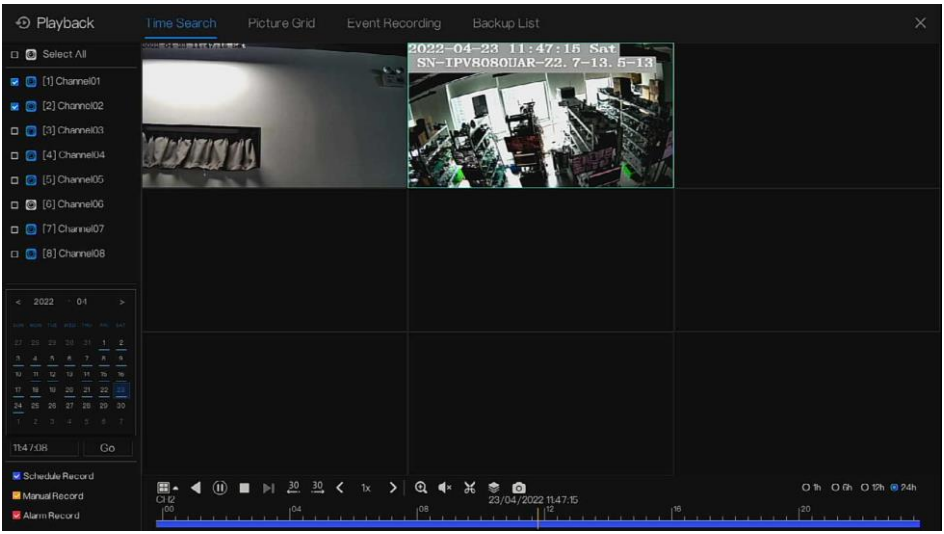
5.3.1 Time Search

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 5-22.

Figure 5-22 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 left-hand 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.

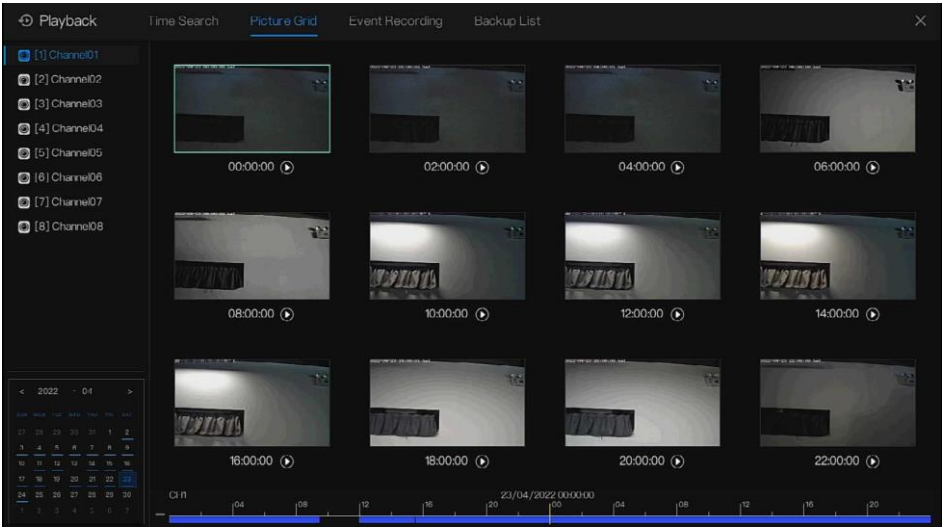
----End

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 5-23.

Figure 5-23 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 interval.

Step 5 Click  to replay the grid individually.

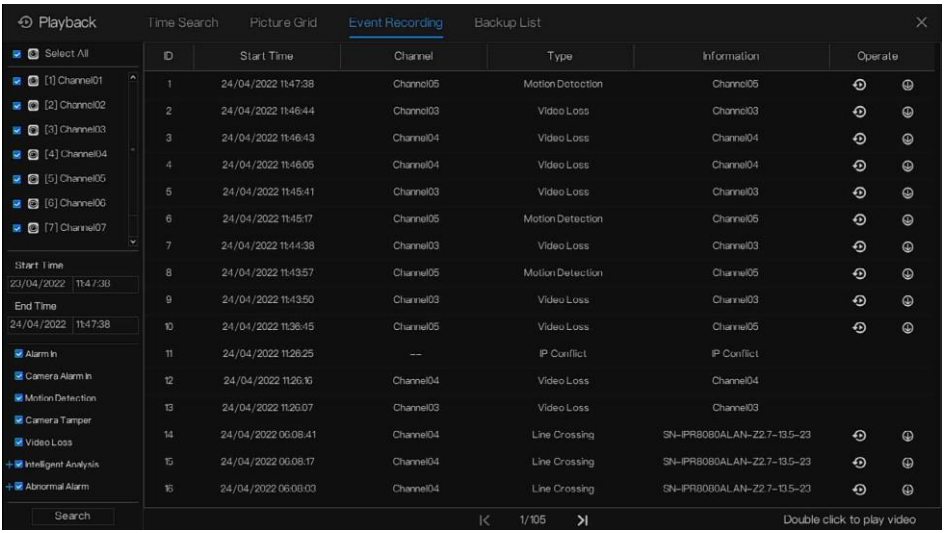
Figure 5-24 Replay

----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 5-25

Figure 5-25 Event screen



Operation Steps

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

Step 2 Set start and end times.

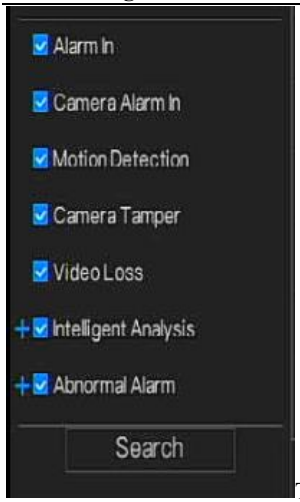
Step 3 Tick the alarm type, such as alarm in, camera alarm in, motion alarm, video loss, intelligent analysis, and abnormal alarm.

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 recorded video.

 Play the recording video.

 Back up the recording video.



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, registered license plate, unregistered license plate, over temperature, low temperature, abnormal temperature, threshold warning, threshold alarm, temperature difference warning, temperature difference alarm, temperature section alarm, low face temperature, normal face temperature, high face temperature, 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.

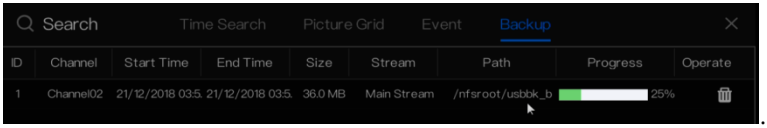
----End

5.3.4 Backup List

Click  on the quick navigation bar, and choose 

at title to access the backup screen, as shown in Figure 5-26.

Figure 5-26 Backup screen



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

----End

5.4 AI Application (Only for Some Models)

At the AI Application interface, we can set the **Smart Search** and **Archives library.**

All snapshots can be added to the libraries according to the real needs.

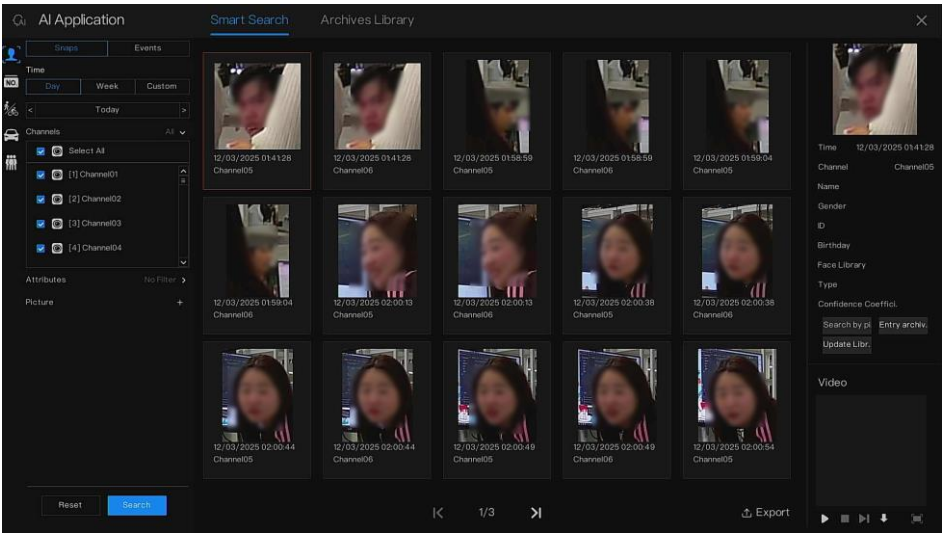
5.4.1 Smart Search

At the Smart Search interface, users can search the **human face, vehicle license plate, full body,** and **car**.

Up to **1000 pictures** can be displayed. Click to see more details and export search results.

5.4.1.1 Human Face Search

Figure 5-27 Human face search



Step 1 Choose Human Face to search at the Smart Search interface.

Step 2 Tick the face recognition camera channels, and set the start and end times.

Step 3 Choose the condition (by picture or by feature). The picture can be selected from the file folder.

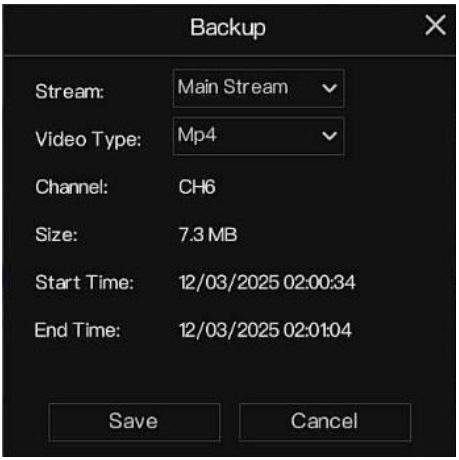
Step 4 Click “Search” to search the snapshot of the human face.

Step 5 The result will show in the middle of the page; click the picture, and the detailed information will show at the top right of the page.

Step 6 The pictures can be added to the library or used to search.

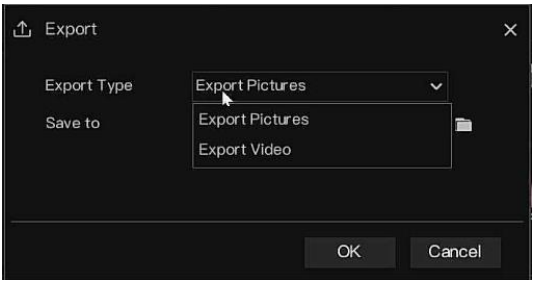
Step 7 Click the play button of the video to play the recording of the snapshot, and click “Backup” to back up the recording videos.

Figure 5-28 Back up



Step 8 Click “Export” to export the result, and choose export-type pictures or videos.

Figure 5-29 Export



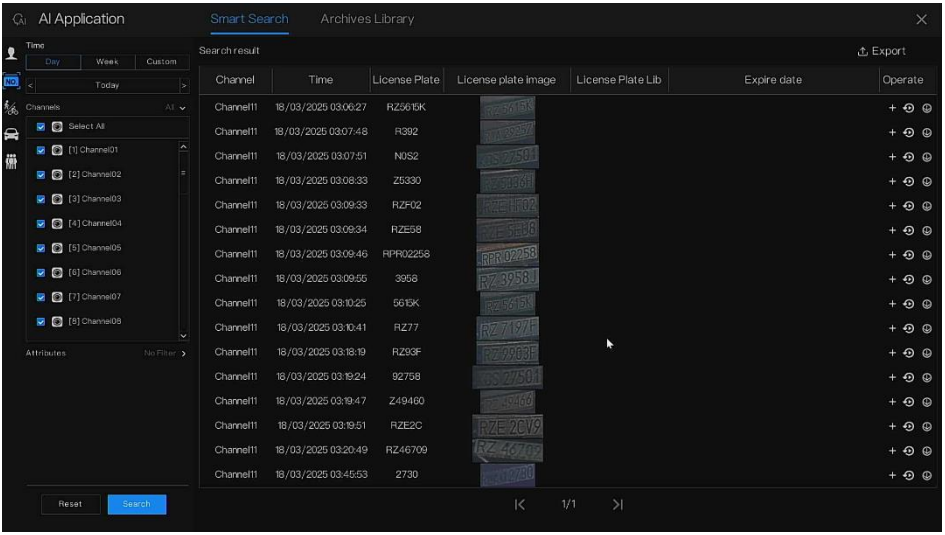
Play a video of the snapshot; it will play a **30-second video** before and after the snapshot.

Snapshot in real-time video: put the cursor on a picture, such as  , and you can add it to **the face library** or **face search**. The cursor is on the snapshotting area, and the pictures are not updated. Move the mouse so that the pictures can be shown in time.

----End

5.4.1.2 Vehicle License Plate Search

Figure 5-30 Vehicle license plate search



Step 1 Choose the vehicle License Plate at the Smart Search interface.

Step 2 Tick the vehicle license plate recognition camera channels, and set the start time and end time.

Step 3 Input the license plate optionally.

Step 4 Click “Search” to search the snapshot of the license plate.

Step 5 The result will show on the page; click “+” to add to the library.

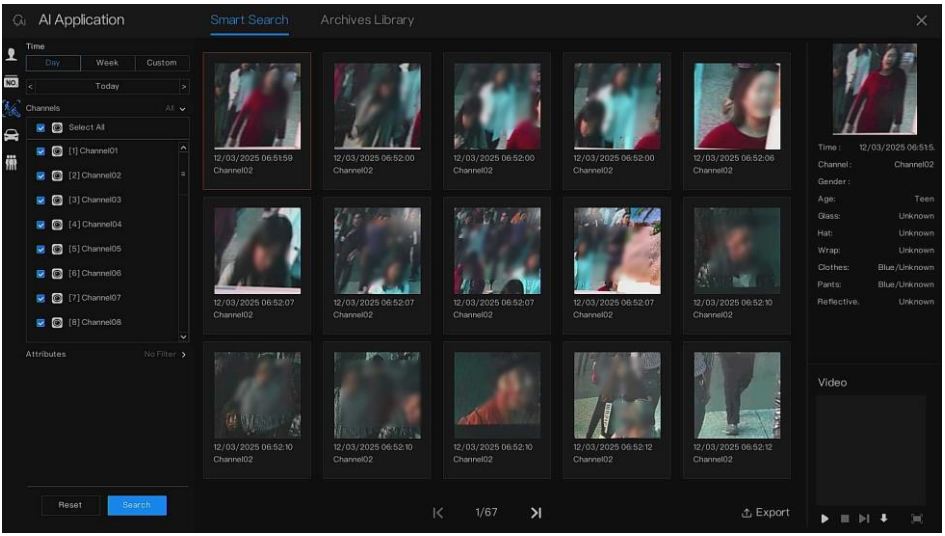
Step 6 Click “Playback” to view the recording video, and click “Backup” to back up the video.

Step 7 Click “Export” to export the result.

----End

5.4.1.3 Full Body Search

Figure 5-31 Full body search



Step 1 Choose Full Body Search at the Smart Search interface.

Step 2 Tick the AI recognition camera channels, and set the start time and end time.

Step 3 Set the gender, and then click cycling or no cycling.

Step 4 Click “Search” to search the snapshot of the human face.

Step 5 The result will show in the middle of the page; click the picture, and the detailed information will show at the top right of the page.

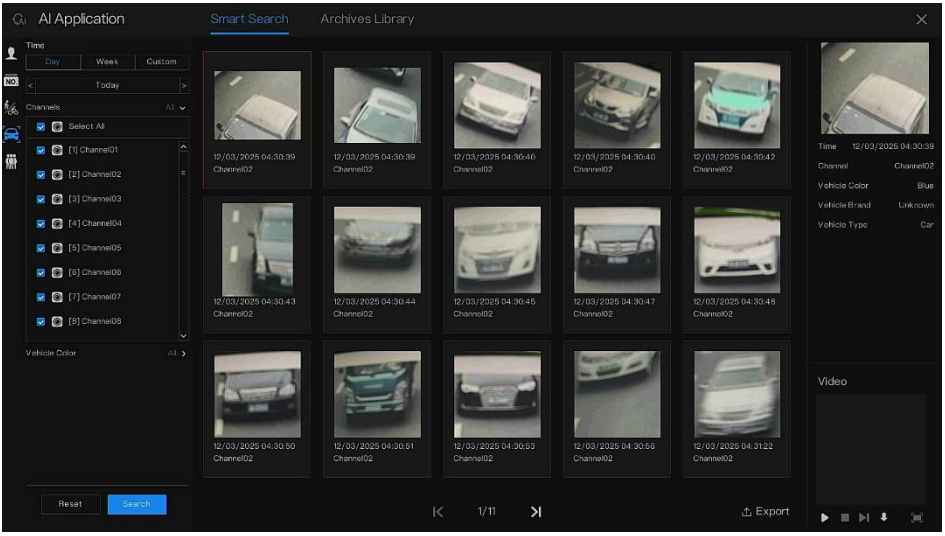
Step 6 Click the play button of the video to play the recording of the snapshot, and click “backup” to back up the video.

Step 7 Click “Export” to export the result.

----End

5.4.1.4 Vehicle Search

Figure 5-32 Vehicle search



Step 1 Choose Vehicle Search at the Smart Search interface.

Step 2 Tick the AI recognition camera channels, and set the start time and end time.

Step 3 Tick the color.

Step 4 Click “Search” to search the snapshot of the human face.

Step 5 The result will be shown in the middle of the page; click the picture and the detailed information shown at the top right of the page.

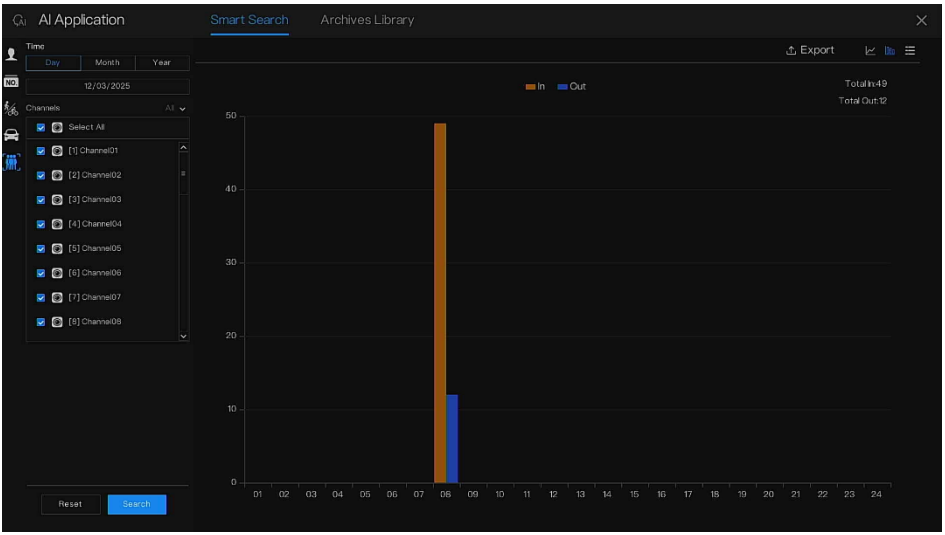
Step 6 Click the play button of the video to play the recording of the snapshot, and click “backup” to back up the video.

Step 7 Click “Export” to export the result.

----End

5.4.1.5 People counting

Figure 5-33 People counting



Step 1 Choose People Counting at the Smart Search interface.

Step 2 Tick the AI recognition camera channels, and set the statistical type and date.

Step 3 Click “Search” to search for the snapshot of the human face.

Step 4 Click “Export” to export the statistics to a USB disk.

Step 5 Click  to view the data in different data tables.

----End

5.4.2 Archives Library

At the archive's library, users can add to or edit the **face library** and **license plate library**.

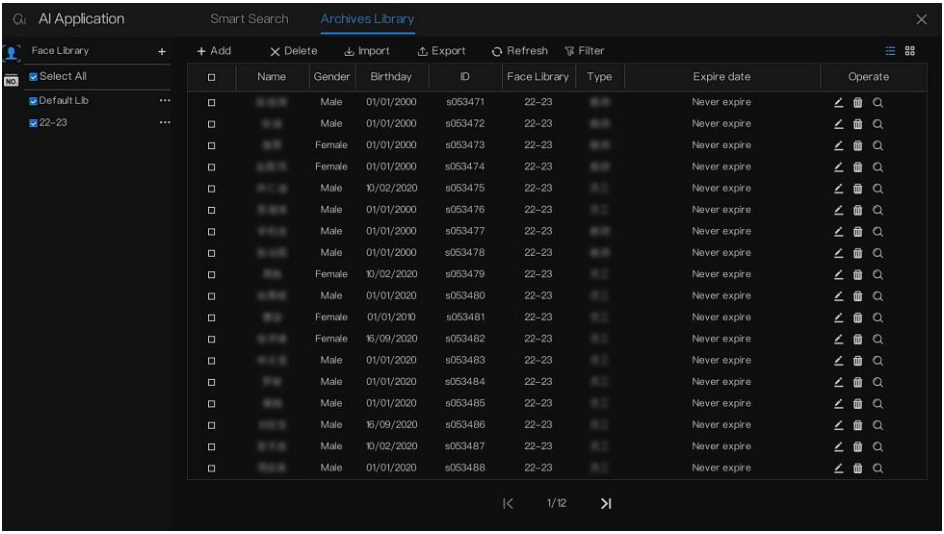
The license plate libraries can be imported to and exported from IP cameras.

5.4.2.1 Face Library

NOTE

The NVRs can save **5000-10000 human faces** in the face library. The detailed number should refer to the device’s performance.

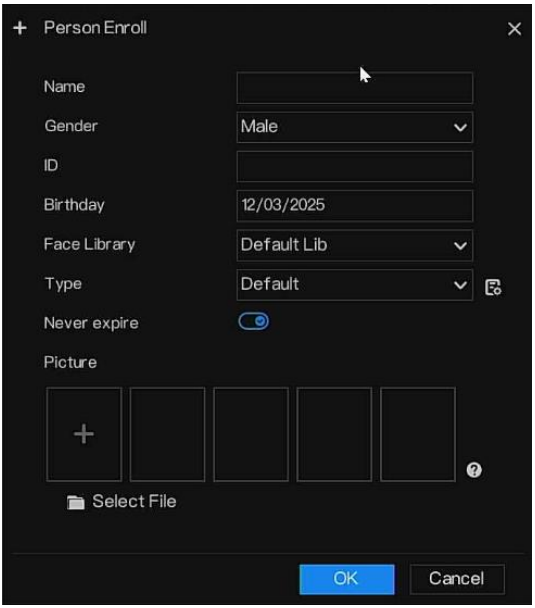
Figure 5-34 Face library



Click “+” to add a new face library.

Click “Add” to add a person's face.

Figure 5-35 Person enroll



Tick the person, and click “Delete” to delete the person.

Click “Import” to add the person batch.

Click “Export” to export all persons in the library.

Click “Filter” to filter all persons in the library, as shown in Figure 5-36.

Figure 5-36 Filter

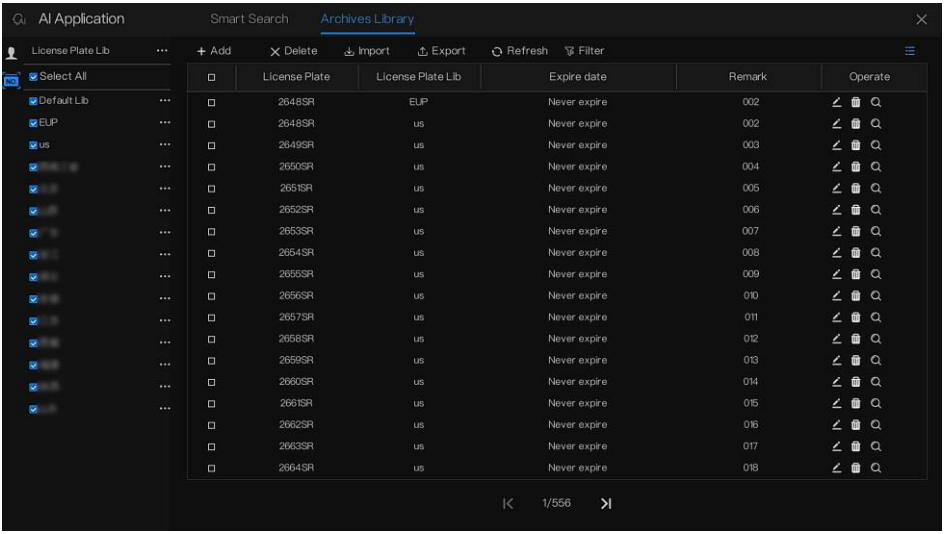
Click the operate icon to edit or delete the chosen person.

----End

5.4.2.2 License Plate Library

At the License Plate library interface, users can **add/delete/operate** the library. It supports the **whitelist** and **blacklist** according to the libraries to **export** and **import** the library to IP cameras.

Figure 5-37 License plate library



Click “+” to **add** a new license plate **library**.

Click “Add” to **add a plate** to the library.

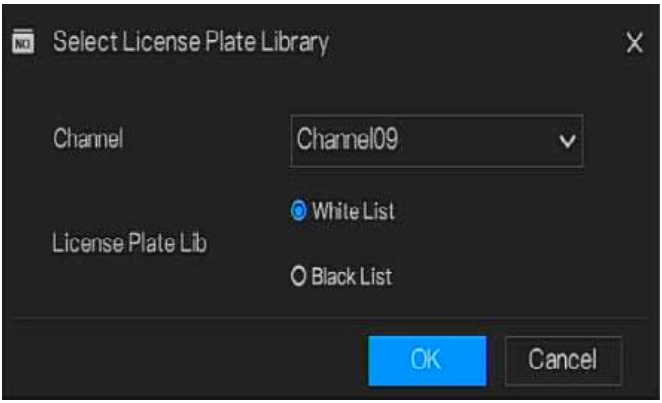
Tick the plate, and click “Delete” to delete the license plate.

Click “Import” to **add** the license plate **batch**.

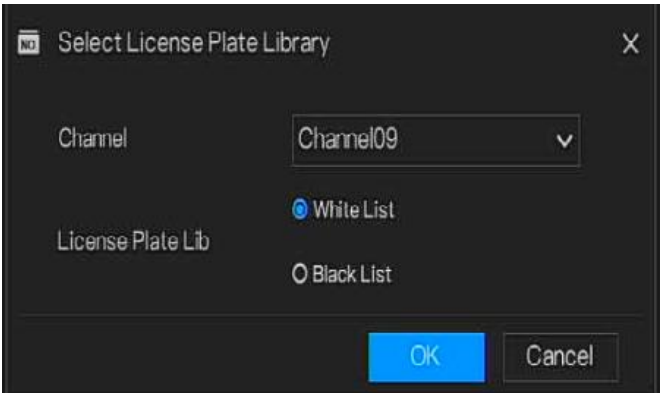
Click “Export” to export the all-license plate library.

Click the operate icon to edit or delete the chosen license plate.

Click “Import from Camera” to select the license plate library for the channel.



Click “Export to Camera” to add the license plate number to the camera.



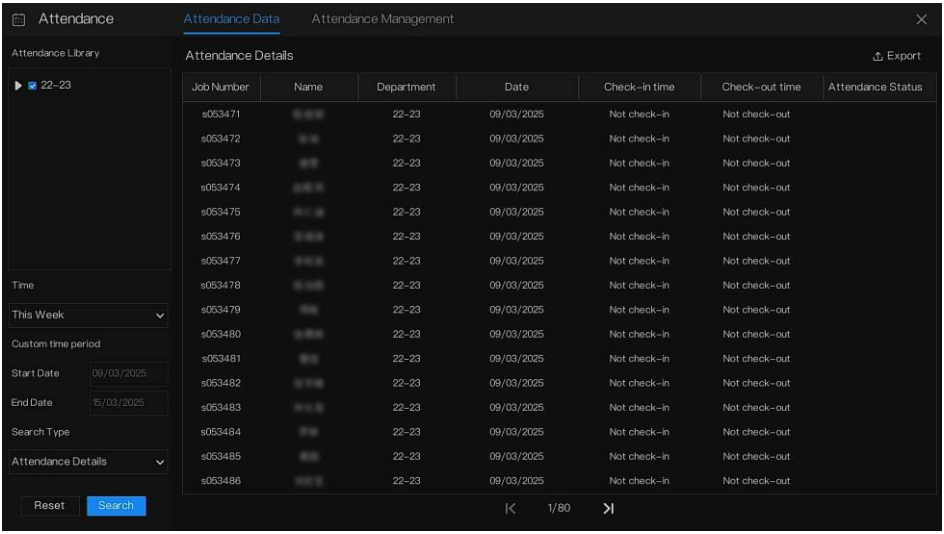
----End

5.5 Attendance (Only for Some Models)

5.5.1 Attendance Data

Click to enter the Attendance Data interface, as shown in Figure 5-38.

Figure 5-38 Attendance data



Operation Steps

Step 1 Tick the Attendance Library. Add an Attendance Library advanced at the **Attendance Management > Attendance Library** page.

Step 2 Choose a time mode, such as today, this week, this month, or custom time.

Step 3 Choose a search type, such as attendance summary and attendance details.

Step 4 Click Search; the result will show in the interface.

Step 5 Click Export to export the query result.

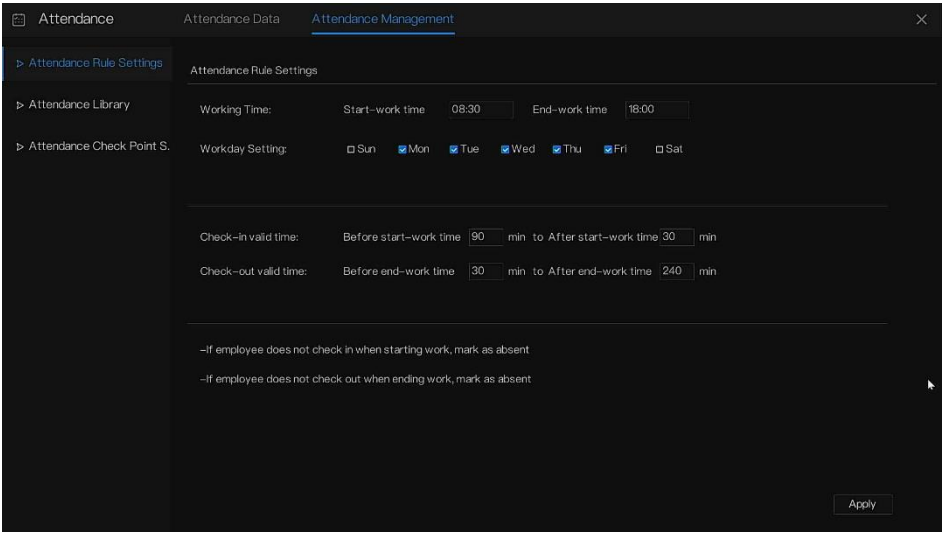
----End

5.5.2 Attendance Management

5.5.2.1 Attendance Rule Settings

In attendance management, users can set **Attendance Rules**, **Library**, and **Check Points**, as shown in Figure 5-39.

Figure 5-39 Attendance rule settings



Operation Steps

Step 1 Set Start-work time and End-work time.

Step 2 Tick the workday.

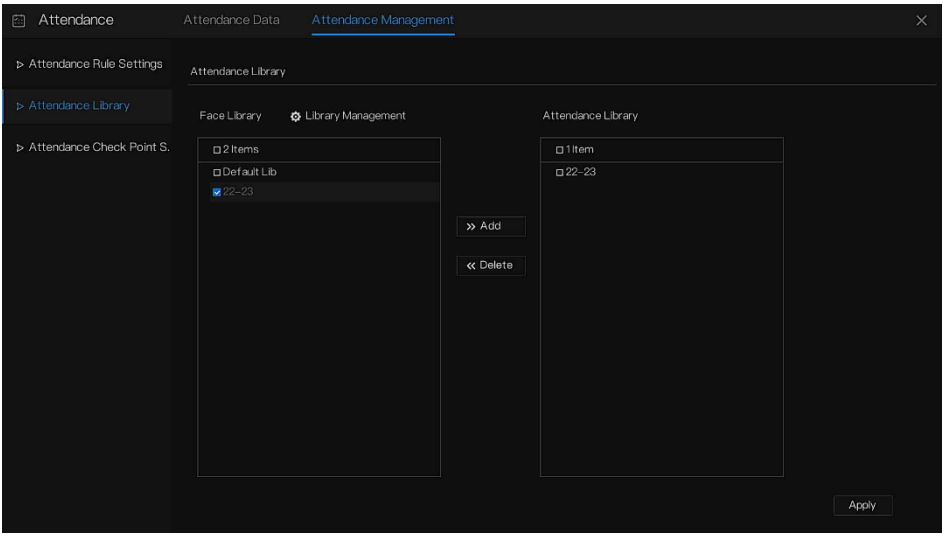
Step 3 Set valid times for check-in and check-out.

Step 4 Click Save to save the setting.

5.5.2.2 Attendance library

Step 1 Click **Attendance Library** to add a library; the attendance library can call the face database directly.

Figure 5-40 Attendance library



Step 2 Tick the library and click Add to add to the attendance library. If you want to modify the library.

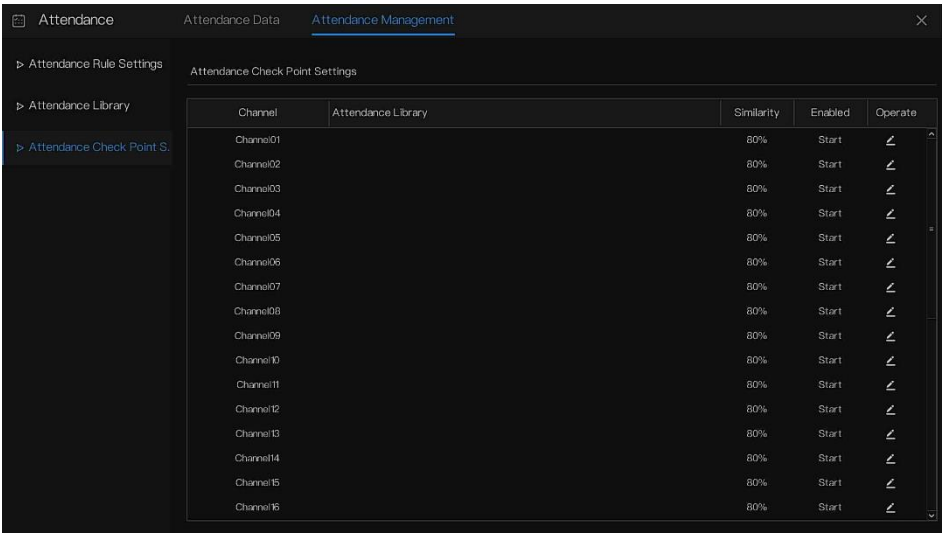
Step 3 Click Database management to enter the face database management to modify the parameter.

Step 4 Click Save to save the setting.

5.5.2.3 Attendance Check Point settings:

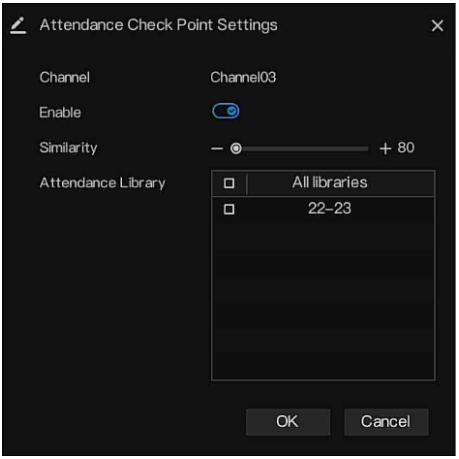
Step 1 Click the **Attendance Check Point** settings to set the point, as shown in Figure 5-41.

Figure 5-41 Attendance checkpoint settings



Step 2 Click  to edit the point setting, as shown in Figure 5-42

Figure 5-42 Checkpoint



Step 3 Enable the function, set **Similarity**, and tick the **Library**. All face detection cameras can set the checkpoints.

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

---End

5.6 Thermal Temperature

NOTE

The Thermal Temperature function is only available for some devices. If the current device does not have the function, please ignore it.

5.6.1 Temperature Parameters

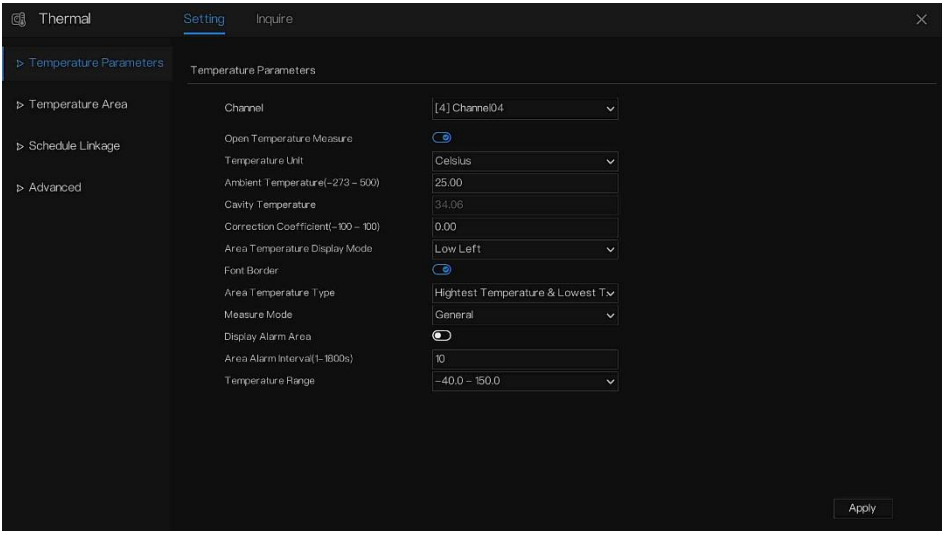
Temperature Parameters include **Temperature Unit**, **Ambient Type**, **Ambient Temperature**, **Cavity Temperature**, C**orrectional Coefficient**, and **Area Temperature Display Mode**.

Operation Procedure

Step 1 Choose **Thermal >Temperature Parameters**.

The **Temperature Parameters** page is displayed, as shown in Figure 5-43.

Figure 5-43 Temperature Parameters interface



Step 2 Configure the settings as per Table 5-1.

Table 5-1 Temperature parameters

Parameter	Description	Setting
Channel	Choose one channel to set.	[Setting method] Select a channel from the drop-down list box.
Open Temperature Measure	Enable temperature measurement.	N/A
Temperature Unit	Celsius and Fahrenheit temperature units are available.	[Setting method] Select a value from the drop-down list box. [Default value] Celsius
Ambient Temperature	The ambient temperature of the camera. It is set when the ambient is outside.	[Setting method] Enter a value manually.
Cavity Temperature	The cavity temperature of the camera.	N/A
Correction Coefficient (-100 ~ 100)	Correction coefficient refers to the deviation between measured object temperature and actual temperature. For example: 1. The measured object temperature is 30, and the actual temperature is 37, so the correction coefficient should be **7.** 2. The measured object temperature is 37, and the actual temperature is 30, so the correction coefficient should be **-7.**	[Setting method] Enter a value manually. [Default value] 0.00
Area Temperature Display Mode	The display position of temperature information on the live video image.	[Setting method] Select a value from the drop-down list box. [Default value] Low left
Font Border	The font will be bolded.	[Setting method] Enable or disable [Default value] disable

Parameter	Description	Setting
Area Temperature Type	There are three types of area temperature.	[Setting method] Select a value from the drop-down list box. [Default value] Highest Temperature
Measure Mode	There are two types of measurement modes.	[Setting method] Select a value from the drop-down list box. [Default value] General
Display Alarm Area	N/A	[Setting method] Enable or disable [Default value] disable
Area Alarm Interval	N/A	[Setting method] Enter a value manually ranging from 1 to 1800. [Default value] 10
Temperature Range	Choose from the drop-down list. The different models have different ranges. -40-150, or -20-120, depending on the performance of the camera.	It will show the default value.

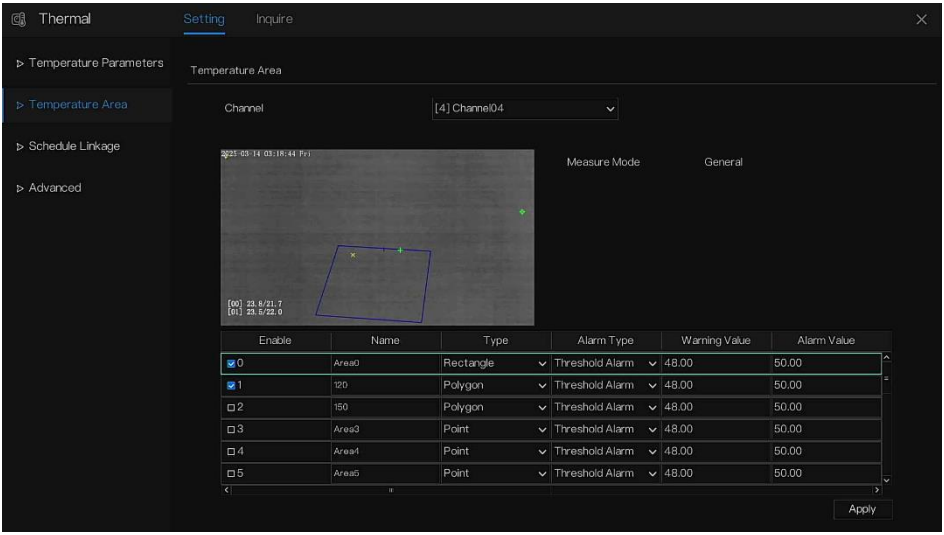
5.6.2 Temperature Area

Operation Procedure

Step 1 Choose **Thermal > Temperature Area**.

The **Temperature Area** page is displayed, as shown in Figure 5-44

Figure 5-44 Temperature area and alarm configuration



Step 2 Set the parameters according to Table 5-2

Table 5-2 Temperature area and alarm configuration

Parameter	Description	Setting
Channel	N/A	[Setting method] Select a value from the drop-down list box. [Default value] 1
Measure Mode	Set at temperature parameter interface. For PTZ bi-spectrum cameras, preset and general can be chosen.	N/A
PTZ Area(only used for PTZ cameras)	Choose or set the preset, and adjust the camera with the PTZ keyboard. All presets can set 20 areas to alarm.	Set the preset manually, or select an existing preset in the drop-down list.
Enable	Tick to enable alarm areas.	N/A
ID	It ranges from 0 to 19.	N/A
Name	Area name of temperature area.	[Setting method] Enter a value manually.

Parameter	Description	Setting
Type	Type of temperature area. ID 0 is the default rectangle area, which is full screen. 20 areas can be set, these are from 0 to 19 area.	[Setting method] Select a value from the drop-down list box. [Default value] Rectangle/Point
Alarm Type	Threshold alarms and Temperature difference alarms are available for alarm type.	[Setting method] Select a value from the drop-down list box. [Default value] Threshold alarm
Warning Value	The camera will warn when the surveillance object's temperature reaches the warning value.	[Setting method] Enter a value manually. [Default value] 48.00
Alarm Value	The camera will alarm when the surveillance object temperature reaches the alarm value.	[Setting method] Enter a value manually. [Default value] 50.00
Maximum Alarm Value	The maximum value of the alarm range, if the alarm value is exceeded, no alarm will be generated.	[Setting method] Enter a value manually. [Default value] 60.00
Emission Rate	The emission rate is the capability of an object to emit or absorb energy. The emission rate should be set only when the target is a special material.	[Setting method] Enter a value manually. [Default value] 0.95
Distance(M)	The distance between the camera and the target.	[Setting method] Enter a value manually. [Default value] 15 NOTE Enter the actual distance when the distance between the camera and the target is less than 15 m. Enter 15 when the distance between the camera and the target is greater than or equal to 15 m.

Parameter	Description	Setting
Alarm	Open or close the alarm output and linkage of the area.	[Setting method] Tick the alarm areas

Step 3 Set temperature area.

1. Tick an area ID.
2. Select the type from the drop-down list.
3. Press and hold the left mouse button, and drag in the video area to draw a temperature area. Right-click to finish the area selection.
4. Click **Apply**, the message “Apply success” is displayed, and the temperature area is set successfully.

Delete a temperature area:

1. Select an area ID.
2. Click the temperature area and right-click.
3. Unselected the area ID.
4. Click **Apply**, the message “Apply success” is displayed, and the temperature area is deleted successfully.

Step 4 Click **Apply**.

Step 5 The message "Apply success" is displayed, and the system saves the settings.

----End

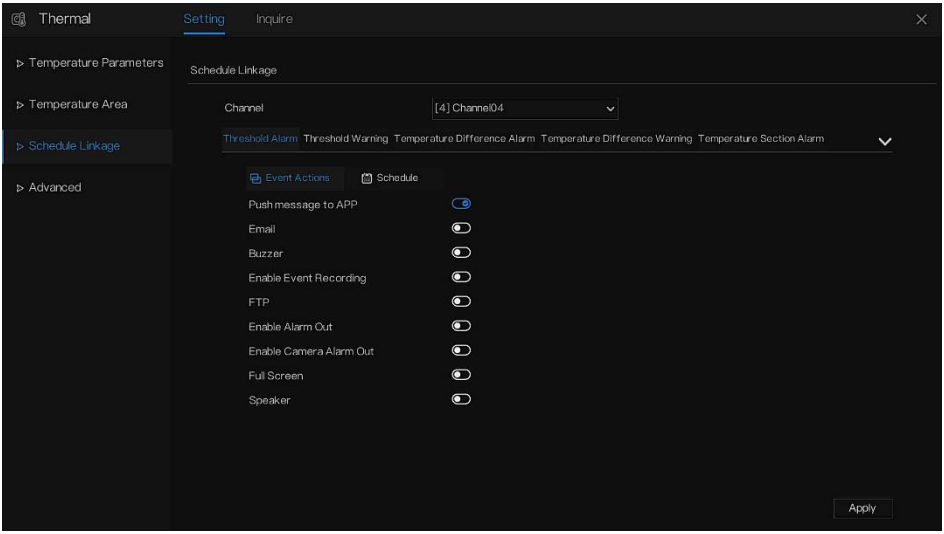
5.6.3 Schedule Linkage

Operation Procedure

Step 1 Choose **Thermal > Schedule Linkage**。

The **Schedule Linkage** page is displayed, as shown in Figure 5-45.

Figure 5-45 Schedule Linkage

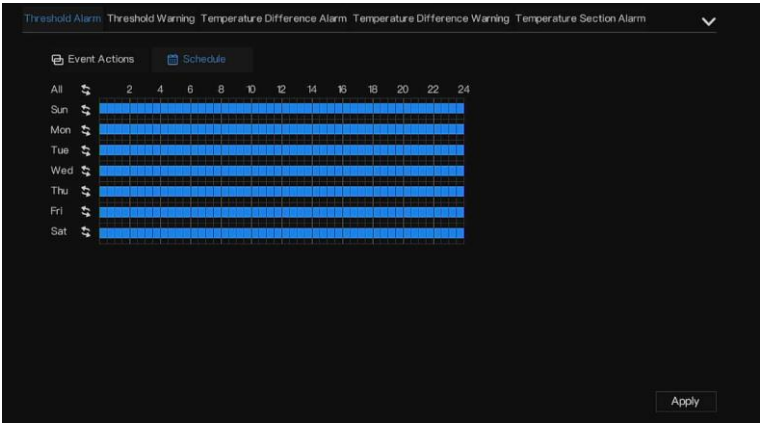


Step 2 Tick the output channel.

Step 3 Enable the "Alarm Record" and "E-mail" buttons.

Step 4 Set Schedule Linkage.

Figure 5-46 Schedule



Method 1: Click the left mouse button to select any time point between 0:00-24:00 from Monday to Sunday, as shown in Figure 5-45.

Method 2: Hold down the left mouse button, drag and release the mouse to select the alarm time from 0:00-24:00 from Sunday to Saturday.

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 alarm time page to select the whole day or the whole week.

Deleting alarm time: Click again or inverse selection to delete the selected alarm time.

Step 5 Click **Apply**. The message "Apply success" is displayed, and the system saves the settings.

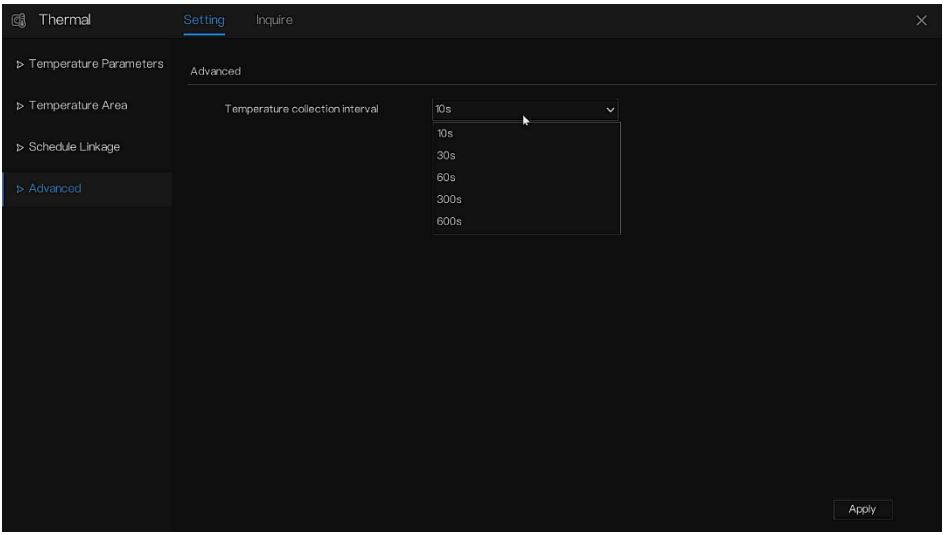
----End

5.6.4 Advanced

Operation Procedure

Step 1 Choose **Thermal** > **Advanced** to enter the advanced interface, as shown in Figure 5-47**.**

Figure 5-47 Advanced



Step 2 Select the **Temperature collection interval** from the drop-down list. The NVR will collect the temperature at the set interval.

Step 3 Click **Apply**. The message "Apply success" is displayed, and the system saves the settings.

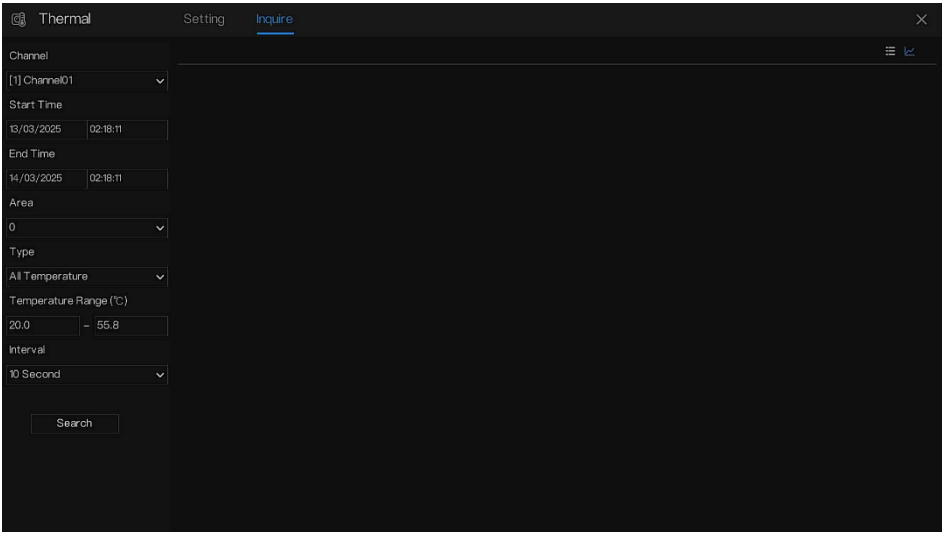
----End

5.6.5 Inquire

Operation Procedure

Step 1 Choose **Thermal** > **Inquire** to enter the inquire interface, as shown in Figure 5-48.

Figure 5-48 Inquire



Step 2 Choose a channel formal the **thermal camera**.

Step 3 Set the **Start** and **End** times.

Step 4 Choose the area, which is set at the temperature area interface. The default area is **0** (**full screen**).

Step 5 Choose the **Type of temperature**, and set the **Temperature Range**.

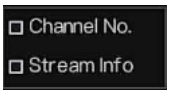
Step 6 Choose the **Interval** of showing, and click **Search** to show the result. There are two modes to show the result: **list** or **picture**.

----End

5.7 Channel Information

Click the  will show as Figure 5-49, and tick the **Channel No**. Or **Stream Info**, the information will show on the live video screen.

Figure 5-49 Channel information

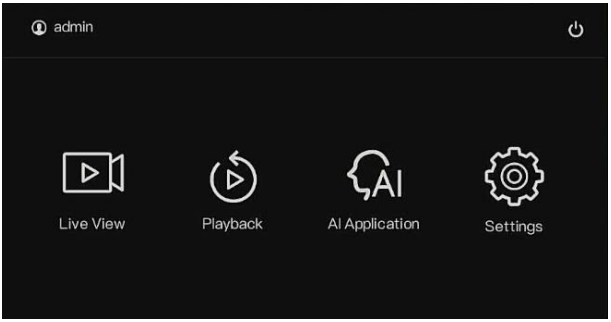


----End

5.8 Main Menu

Right-click on the UI screen, the main menu as shown in Figure 5-50.

Figure 5-50 NVR main menu



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

Channel: Camera, Encode, Image, OSD, Privacy Zone, 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.

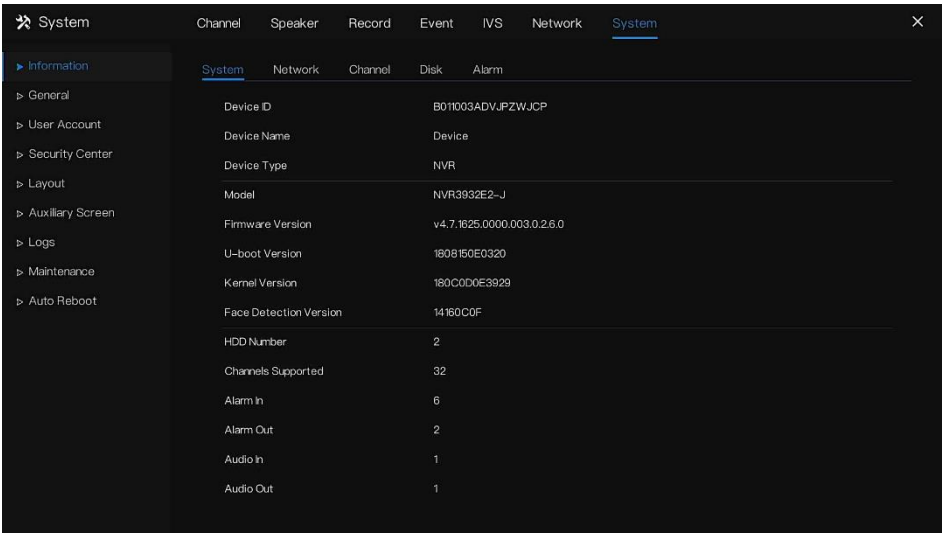
Event: General, Motion Detection, Video Loss, Alarm In, Abnormal Alarm, and Alarm Out.

IVS: AI Multi-Target, Intelligent Analysis, Behavior Analysis, ES Analysis, Face Recognition, **LPR**, 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 5-51 Setting



----End

6 System Setting

NOTE

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

6.1 Channel Management

IP cameras can directly be connected to input channels of the NVR by plugging in a POE port. When IP cameras are insufficient, the NVR can automatically search for and add IP cameras or manually add cameras in the same Local Area Network (LAN).

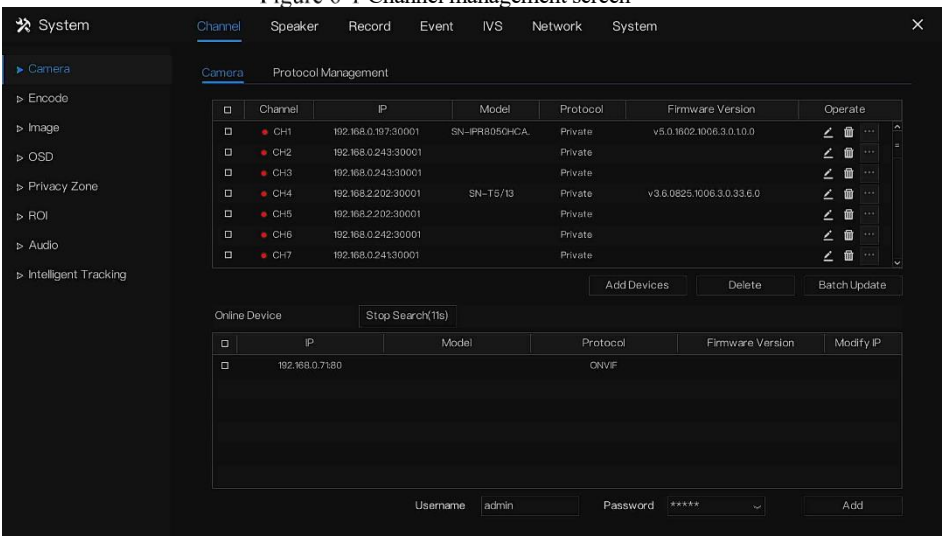
Channel management includes **Adding** or **Deleting a Camera, Encode, Image, OSD, Privacy Zone, ROI, Audio,** and **Intelligent Tracking**.

6.1.1 Camera

Operation Description

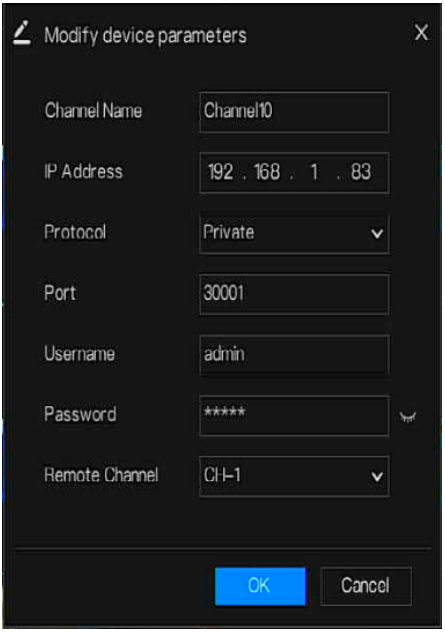
Click **Channel** in the Setting System menu to access the camera management screen, as shown in Figure 6-1 There are four modes for adding cameras: manually add, batch add, search to add, POE add, and automatic add.

Figure 6-1 Channel management screen



 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



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.

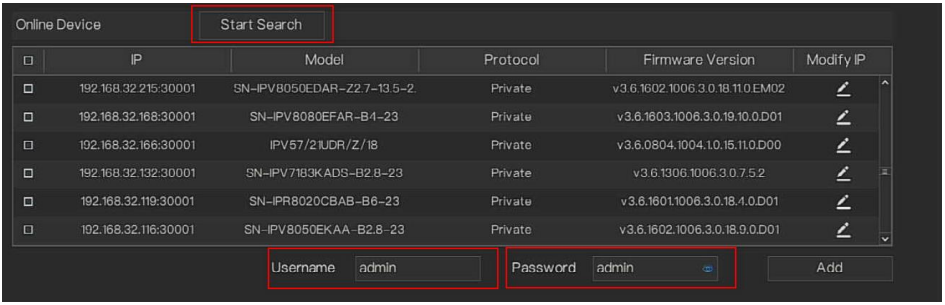
----End

6.1.1.1 Add Camera Automatically

The NVR 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.



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 NVR. 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.

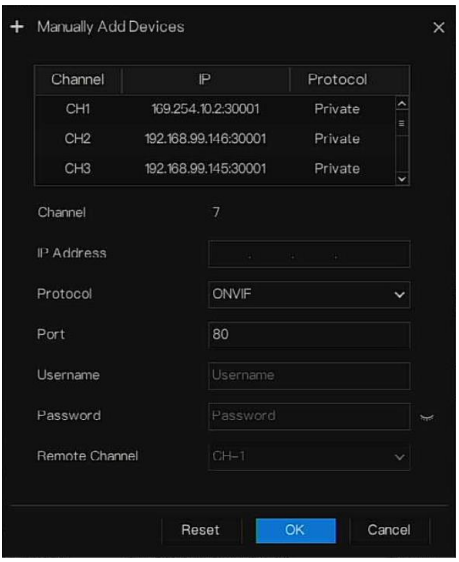
----End

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



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

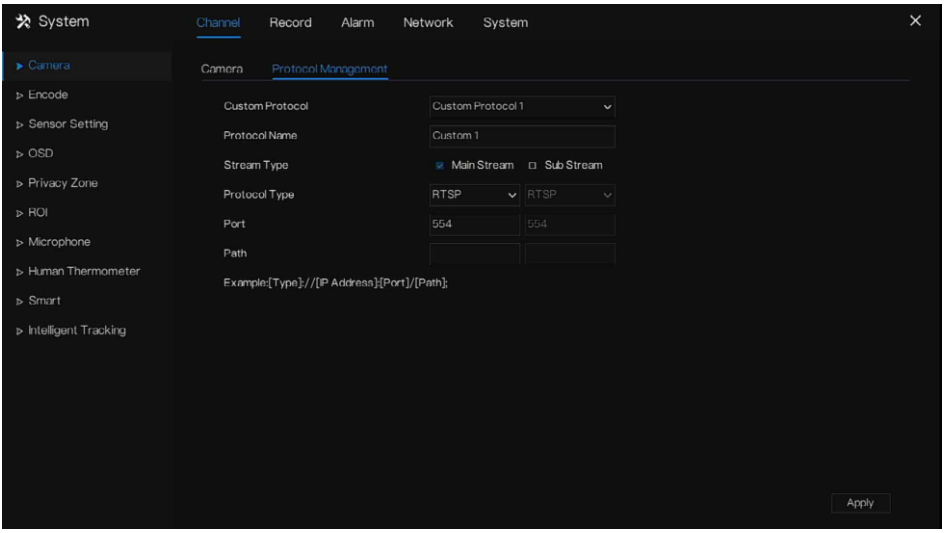
- If all channels of the NVR are connected by cameras, please delete the cameras that you don't need so that you can add more cameras.
- If an IP camera is added manually, input the correct username and password of the camera below the online device list. The camera will be added successfully. If not, 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 NVR, they can copy the IP address, username, and password, only modify the remote channel to add different channels to NVR.

----End

6.1.1.3 Add Camera by RSTP

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

Figure 6-4 Protocol management



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.

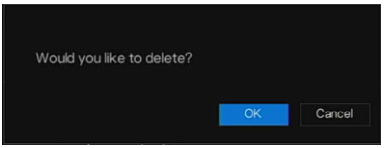
----End

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



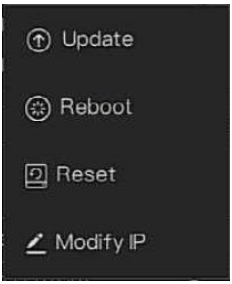
Step 2 Click OK, the camera will be deleted successfully.

The POE cameras are online and can't be deleted directly; you should modify the username or password to make it offline, then click  to delete. The POE channel is deleting; the camera should be unplugged and then plugged in to connect again.

6.1.1.5 Operate Camera

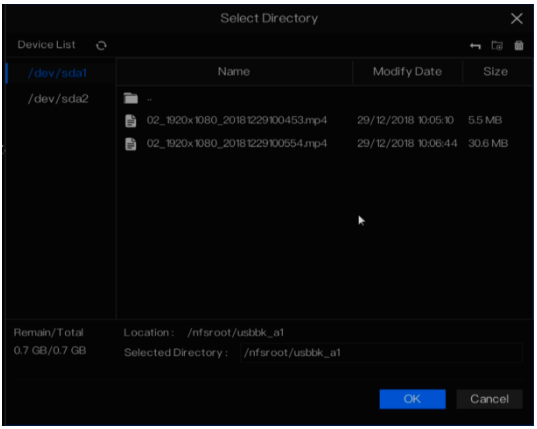
At the camera list, click  to operate the camera as shown in Figure 6-6; users can update, reboot, and reset the camera immediately.

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.

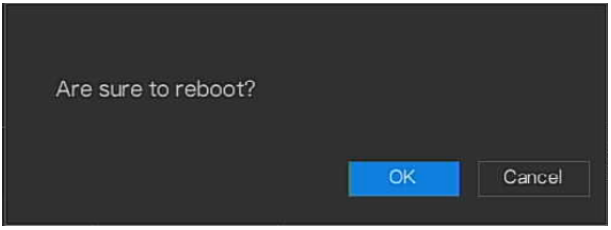
Figure 6-7 Select directory of software.



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

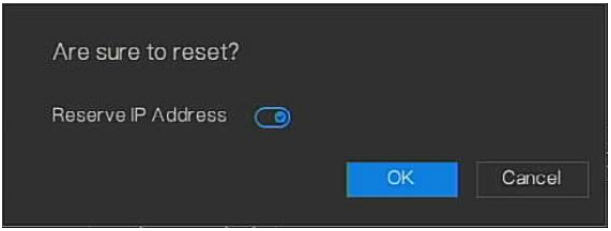
Reboot: Click **Reboot**, and the message **"Are sure to reboot?"** will show, click OK to reboot the camera.

Figure 6-8 Reboot camera



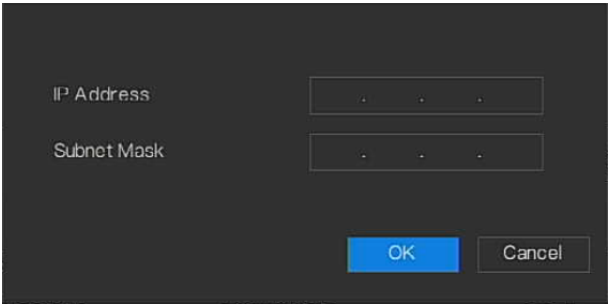
Reset: Click **Reset**, and the message **"Are sure to reset?"** will show, and users can enable the retain IP address function. Click OK to reboot the camera.

Figure 6-9 Reset camera



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

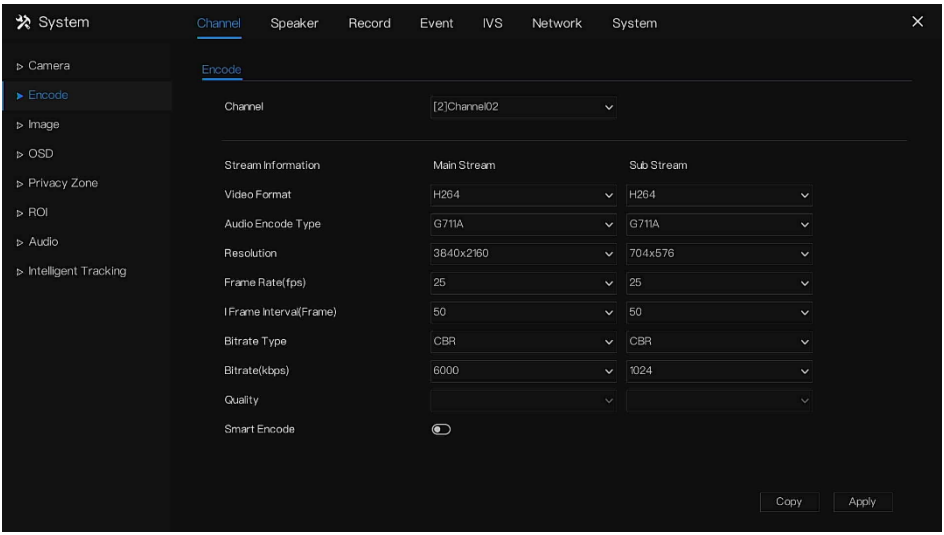
6.1.2 Encode Parameter

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



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**, B**itrate 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

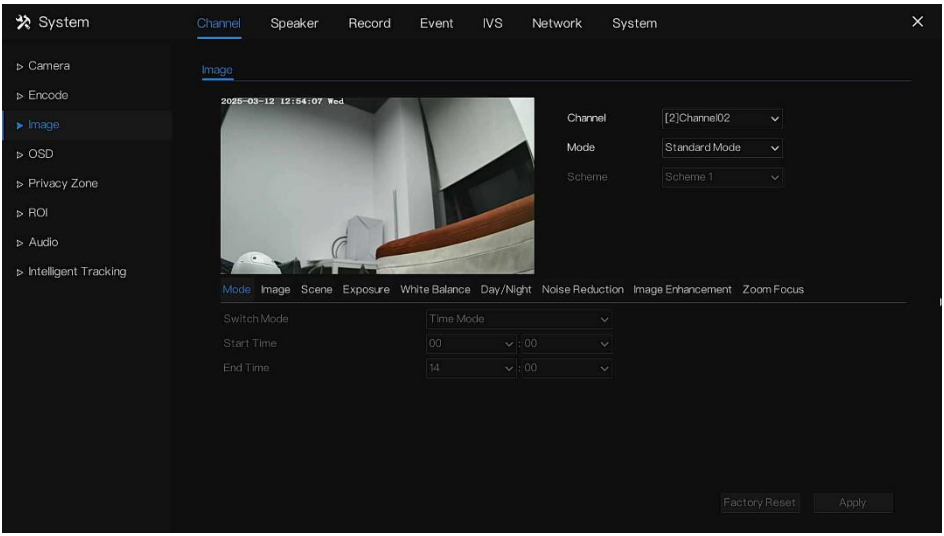
6.1.3 Image

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



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.

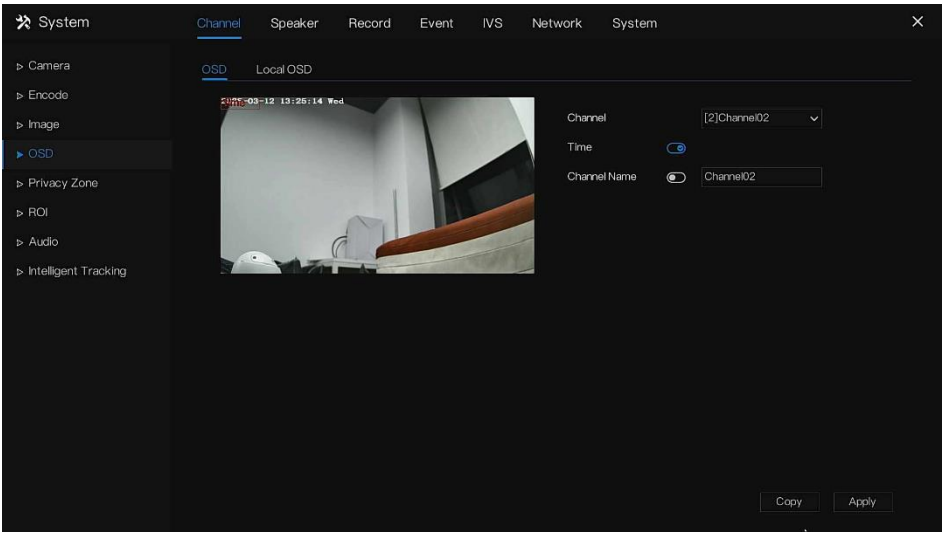
----End

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



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.

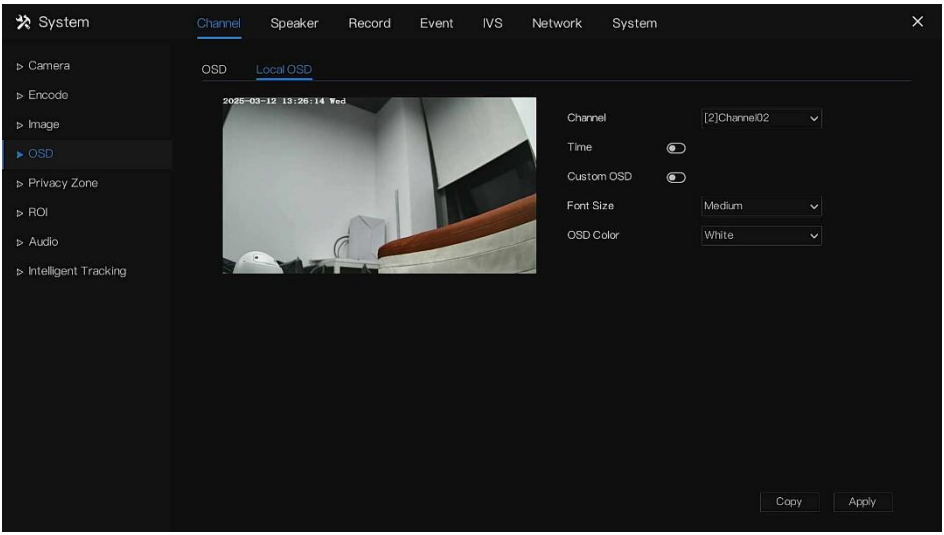
Step 6 Click Copy and select channels, then click OK to apply the OSD settings to cameras in selected channels, and click Apply to save OSD settings.

----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 NVR sets the local OSD.

Figure 6-14 Local OSD



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

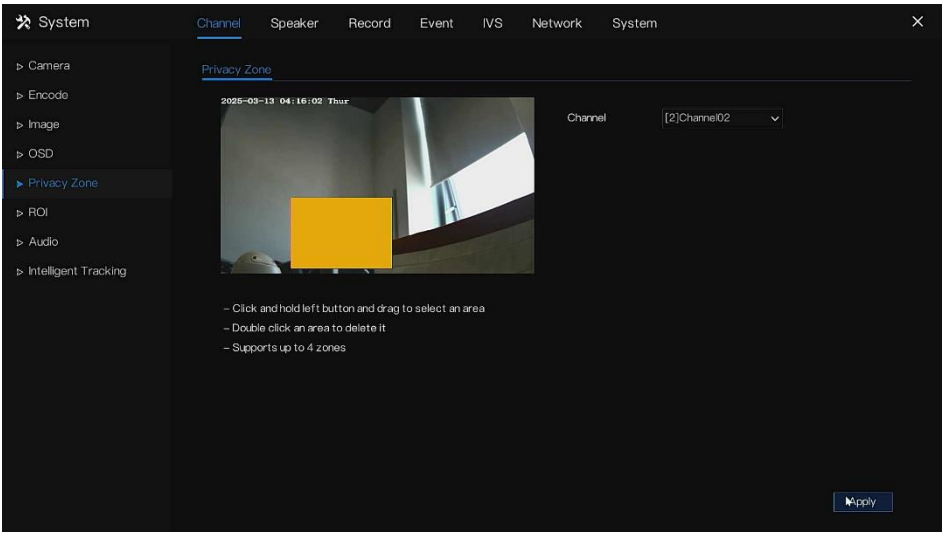
6.1.5 Privacy Zone

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



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 ROI

1. Navigate to **Settings > Channel > ROI** (Region of Interest) as shown in Figure 6-16.

Figure 6-16 ROI

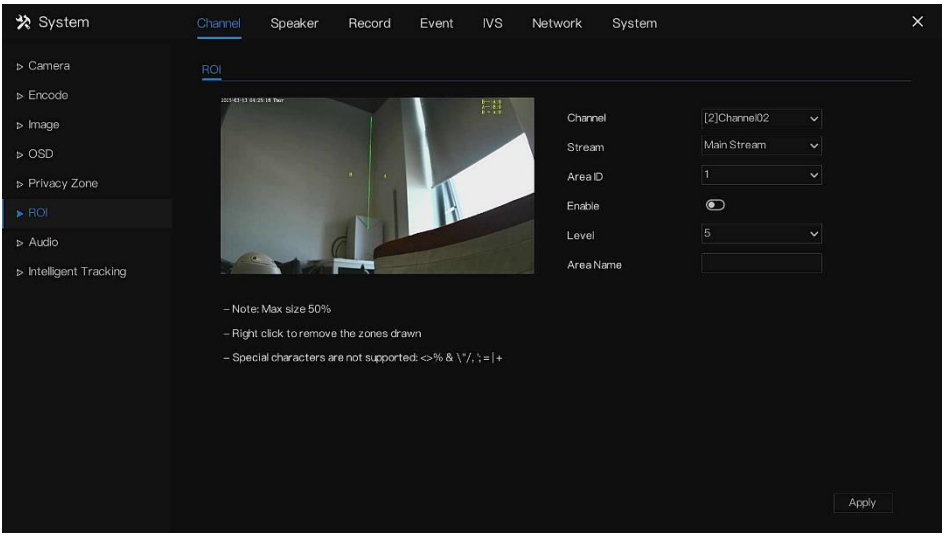


Table 6-1 ROI parameter

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

Parameter	Description	Setting
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
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

6.1.7 Audio (Only for Some Models)

6.1.7.1 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 6-17.
2. Adjust the parameters as per Table 6-2.

Figure 6-17 Audio input

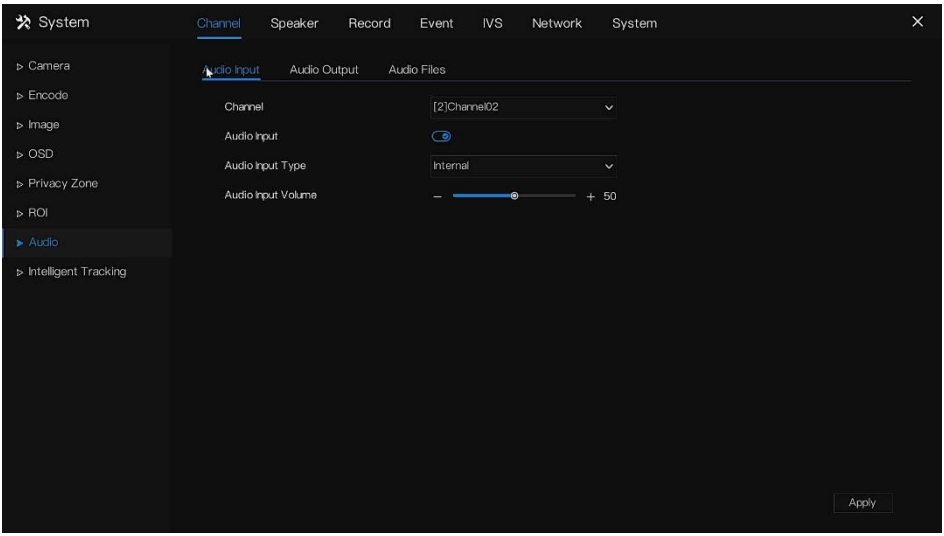


Table 6-2 Audio input

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

6.1.7.2 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 6-18 Audio output

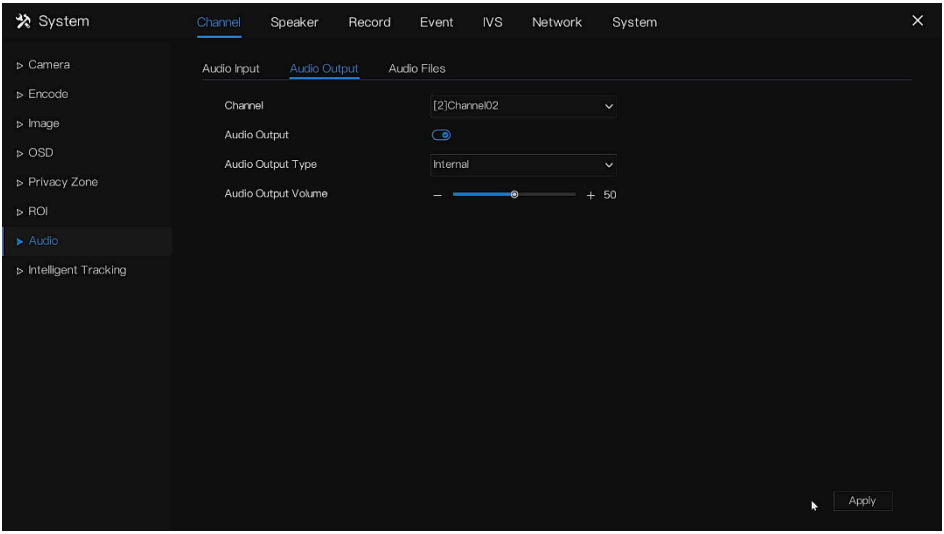


Table 6-3 Audio output

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.

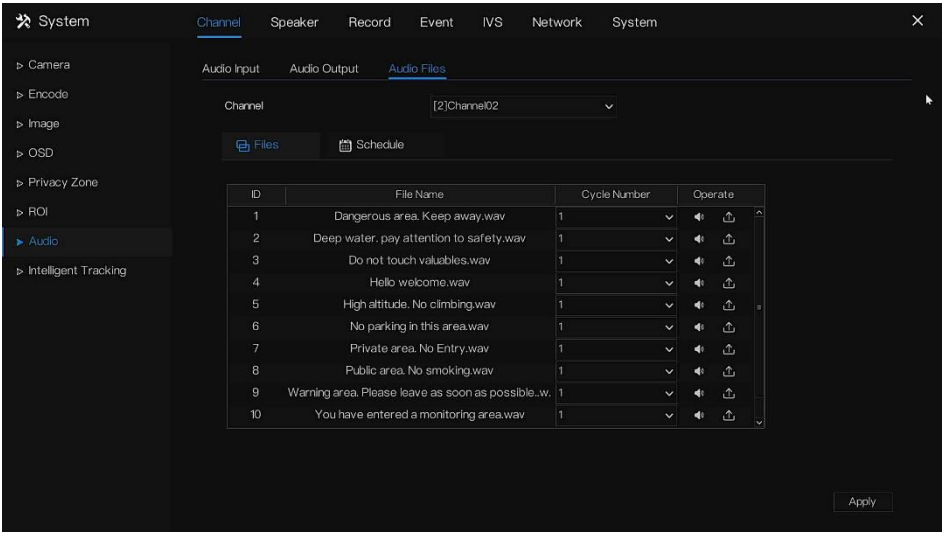
4. Click Apply to save privacy settings.

----End

6.1.7.3 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 6-19 Audio files



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 6-20 Upload audio file

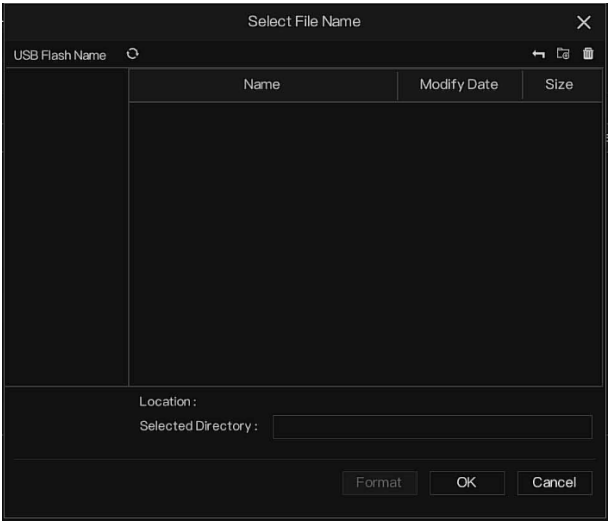
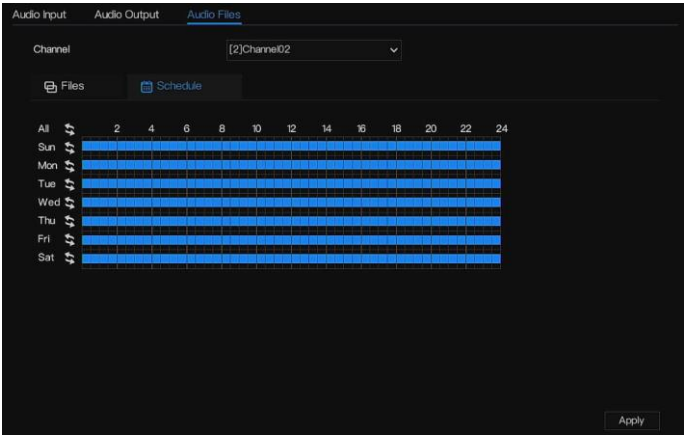


Figure 6-21 Schedule of audio file



6.1.8 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 6-22.
2. Adjust the parameters as per Table 6-4.
3. Click Apply to save settings.

Figure 6-22 Intelligent tracking

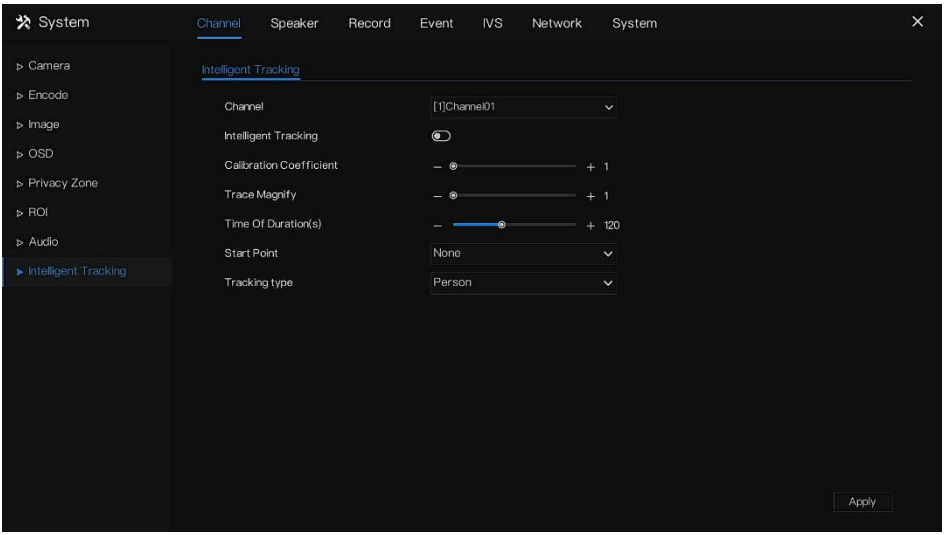


Table 6-4 Intelligent tracking parameters

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

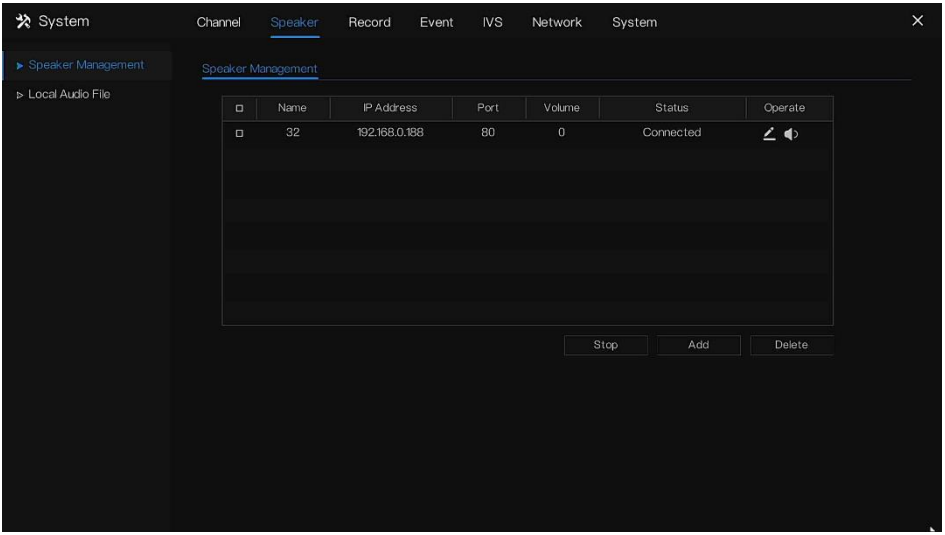
Users can add the speaker to the NVR so that the NVR broadcasts the video files.

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

6.2.1 Speaker Management

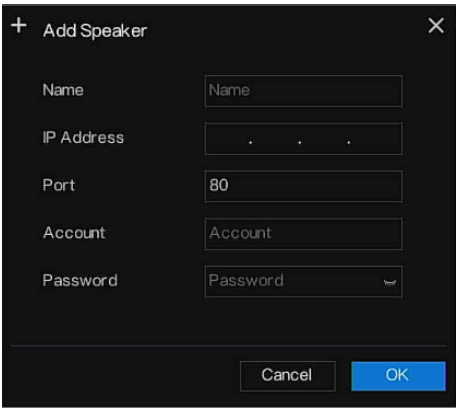
Step 1 Navigate to **Settings > Speaker** as shown in Figure 6-23.

Figure 6-23 Speaker management



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

Figure 6-24 Add speaker

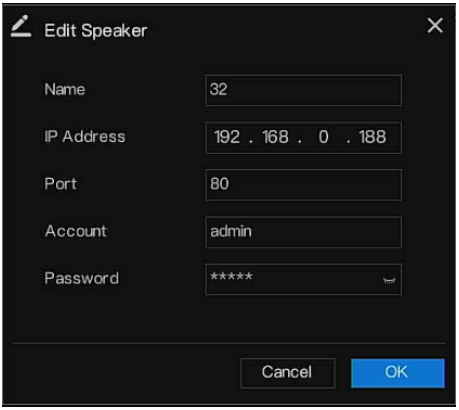


Step 3 Add succeeded. Click to adjust the audio volume.

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.

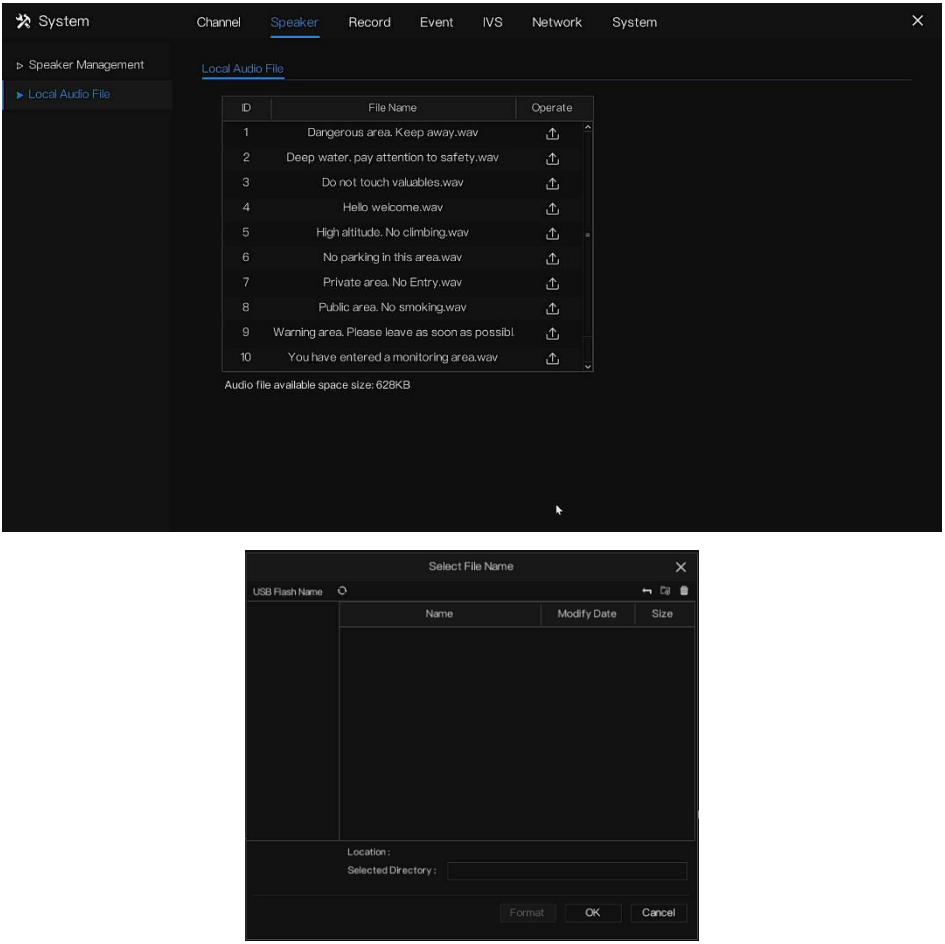
Figure 6-25 Edit speaker



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 1MB. The uploaded audio files should be WAV-type.

Figure 6-26 Local audio file



6.3 Record-Setting

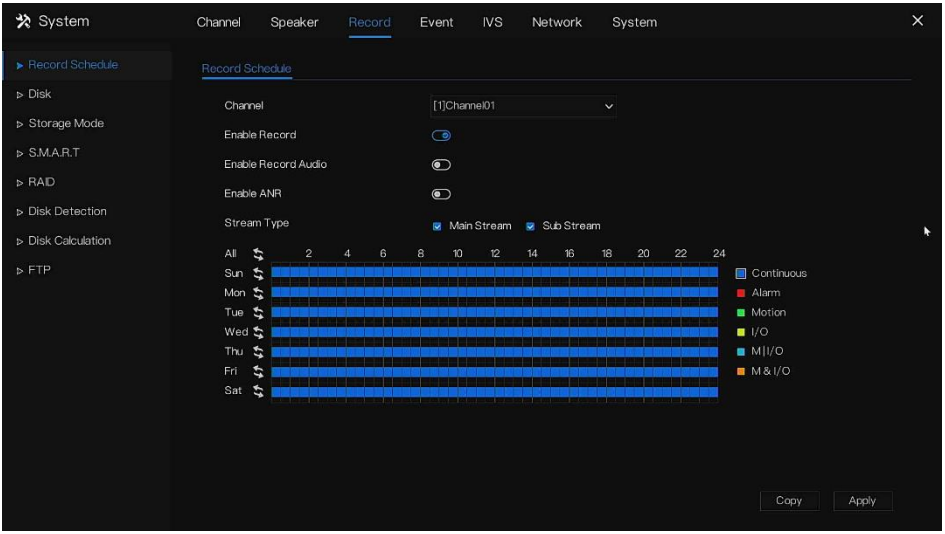
Set the **Record Schedule, Disk, Storage Mode**, **S.M.A.R.T**, **Disk Detection**, **Disk Calculation**, **FTP**, and so on.

6.3.1 Record Schedule

Operation Description

Navigate to **Settings > Record > Record Schedule** as shown in Figure 6-27.

Figure 6-27 Record management screen



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 NVR 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

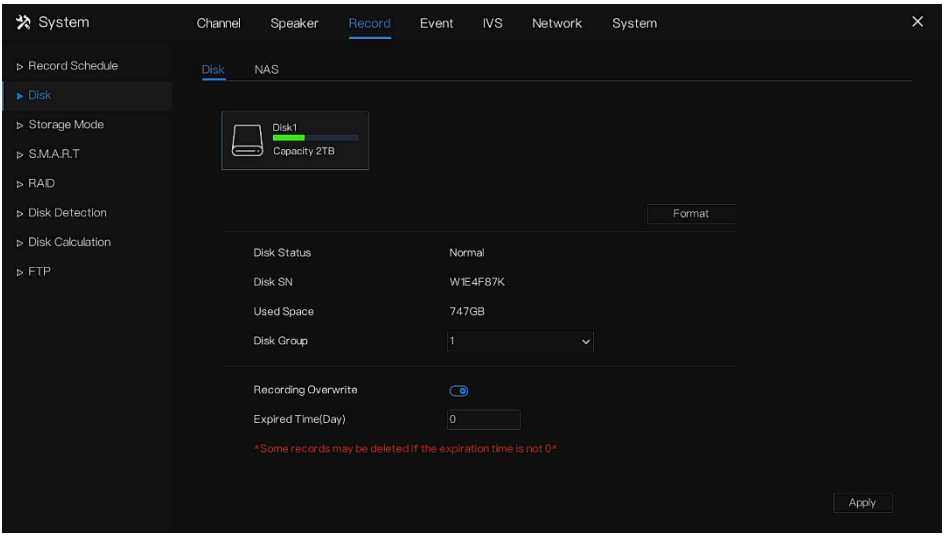
6.3.2.1 Disk

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 6-28.

Figure 6-28 Disk screen



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.

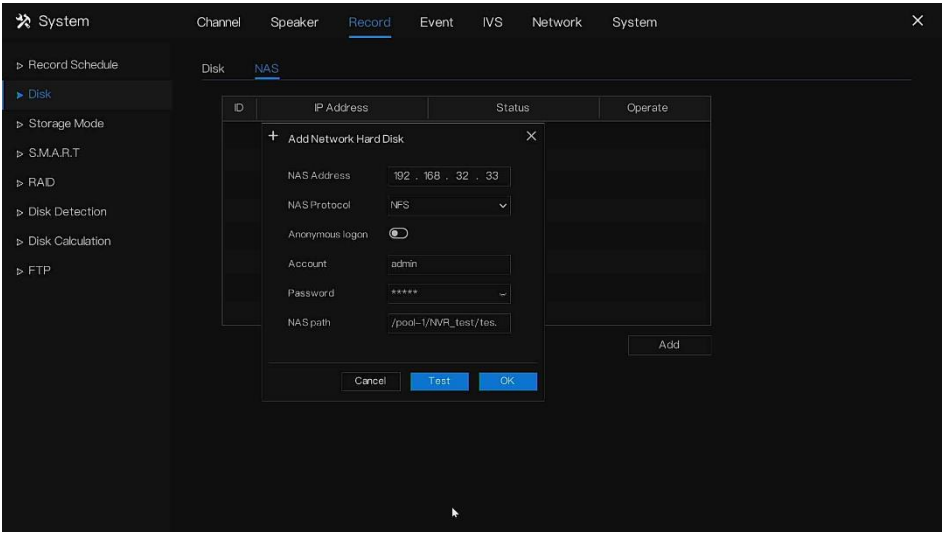
The expired time is 0, which means the disk will be rewritten only when the disk is full.

----End

6.3.2.2 NAS

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

Figure 6-29 NAS



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.

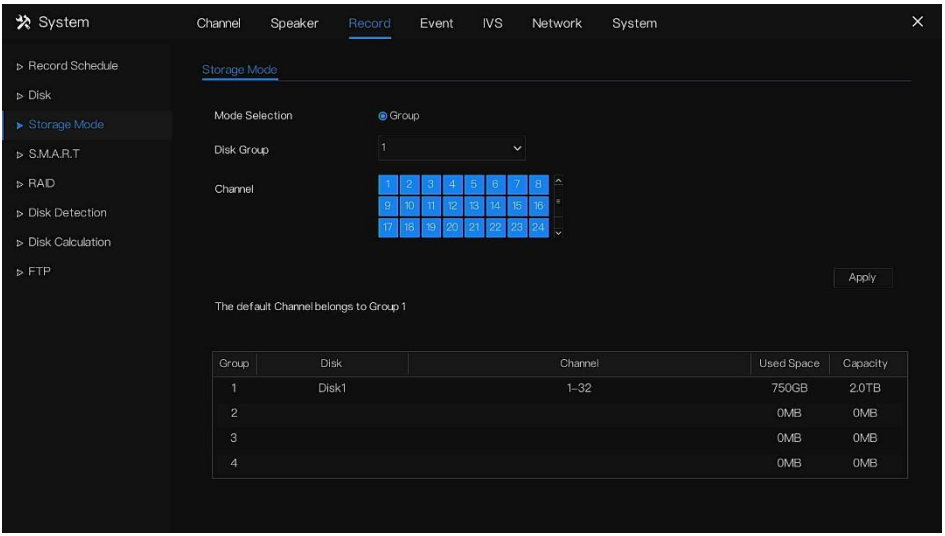
6.3.3 Storage Mode

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 6-30.

Figure 6-30 Storage mode



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 NVR 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.

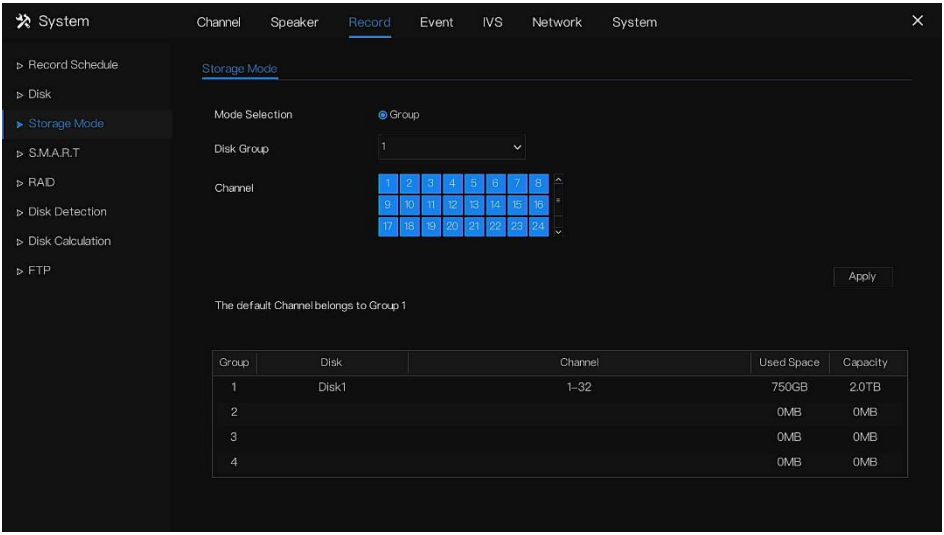
----End

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 6-31.

Figure 6-31 S.M.A.R.T

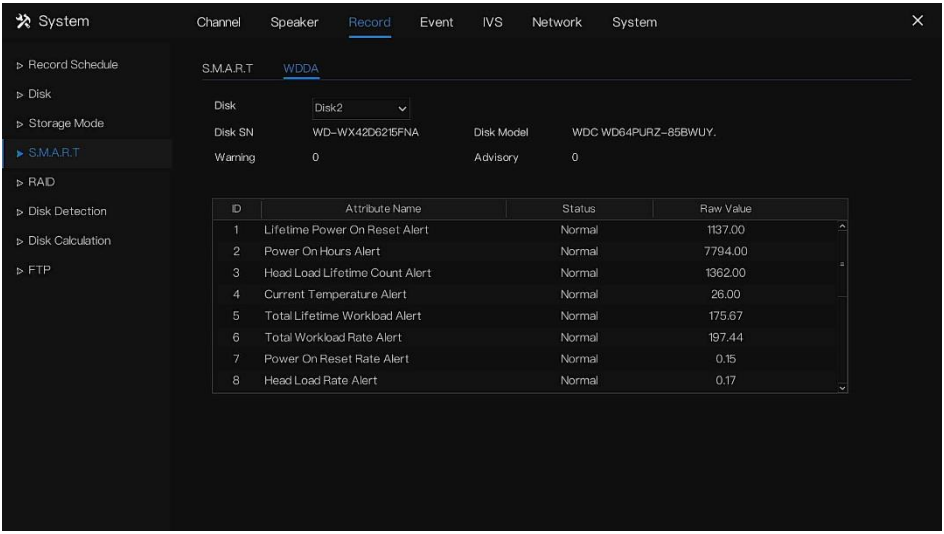


----End

6.3.4.2 WDDA

The **Western Digital disk** has the **WDDA** function, and the NVR can read the information of the disk so that users can view the status of the disk, as shown in Figure 6-32.

Figure 6-32 WDDA



----End

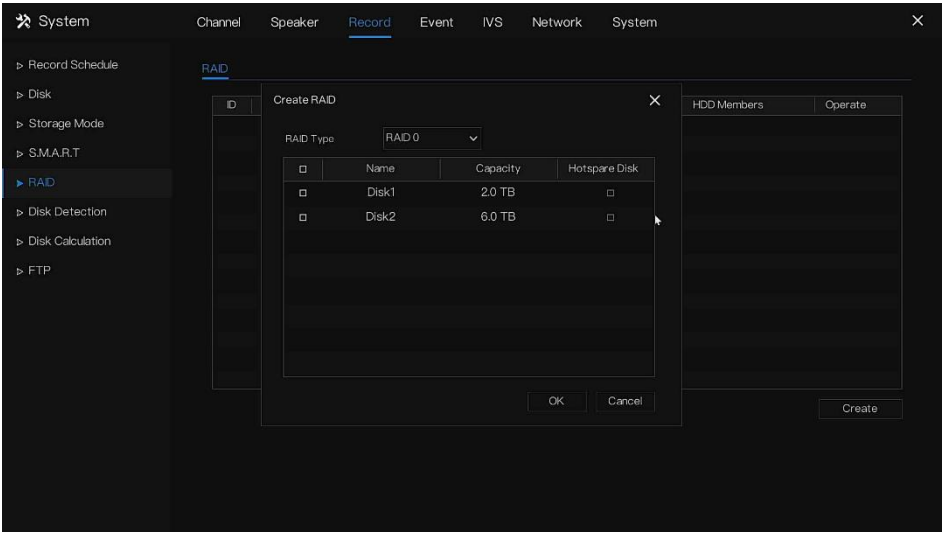
6.3.5 RAID (Only for Some Models)

The NVR supports **building/editing/deleting** the RAID. Users can choose the type of RAID according to the importance of recording.

NOTE

- The disks must be enterprise-level disks. The capacity of disks is the same for efficient use. RAID0/1/5/6/10 are supporting,
- The maximum capacity of RAID cannot exceed 80T.
- RAID5 at least 3 disks can be created. RAID6 at least 4 disks can be created. RAID10 at least 4 disks can be created. Create a hot spare disk that needs more than one disk or double basic disks.

Figure 6-33 RAID



Operation Steps

Step 1 Navigate to **Settings > Record > RAID**

Step 2 Click **Create** to choose a disk to create a new RAID.

Step 3 Tick a **Hot-spare Disk** to back up in case the disk is broken. The number of disks must be more than one.

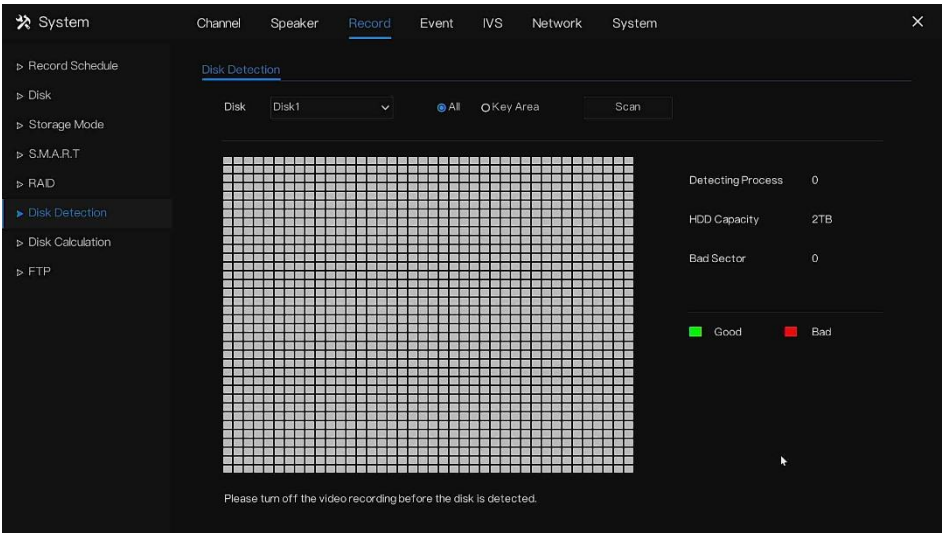
Step 4 Click **OK** to save the creation, and format the new RAID.

----End

6.3.6 Disk Detection

Detect the disk before recording videos so that the data are secure, as shown in Figure 6-34.

Figure 6-34 Disk Detection



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

6.3.7 Disk Calculation

Users can calculate the usage of the disk so that they can set the storage strategy reasonably, as shown in Figure 6-35.

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

Figure 6-35 Disk calculation of capacity

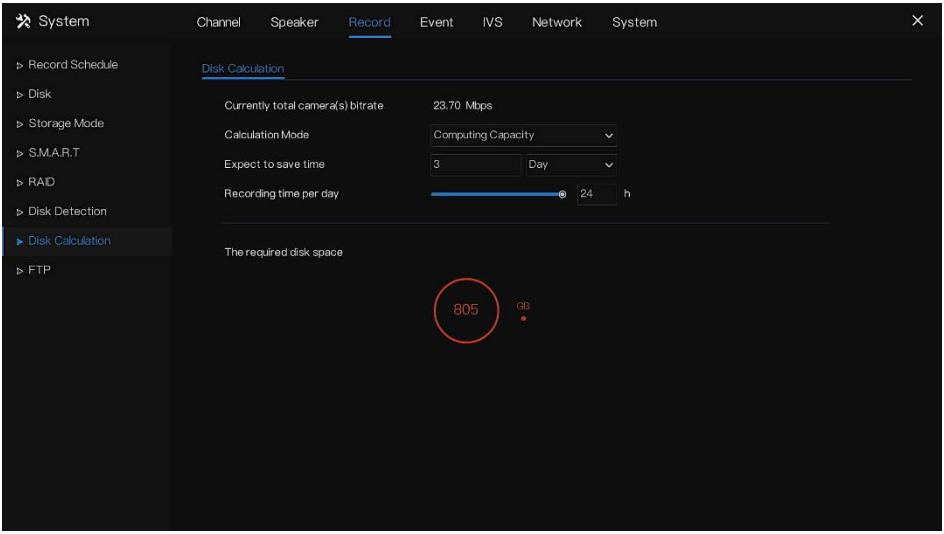
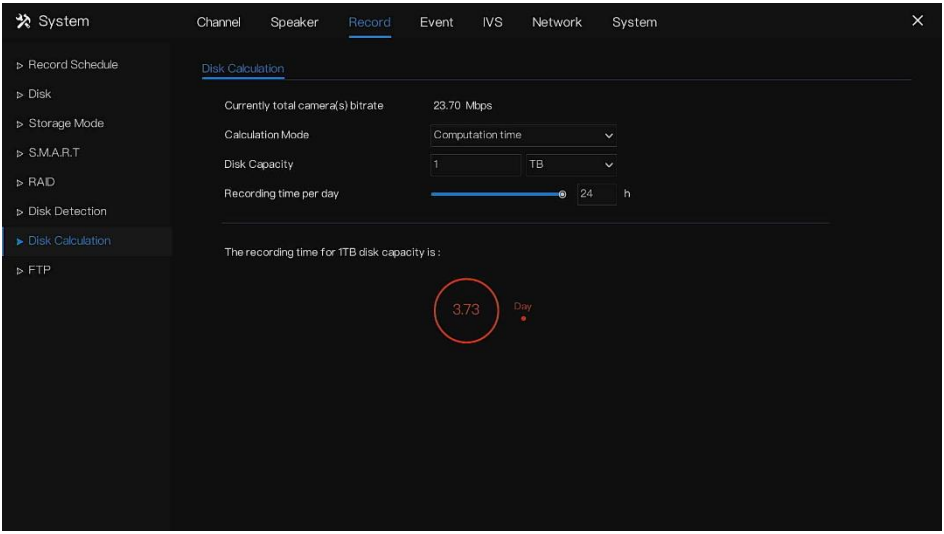


Figure 6-36 Disk calculation of time

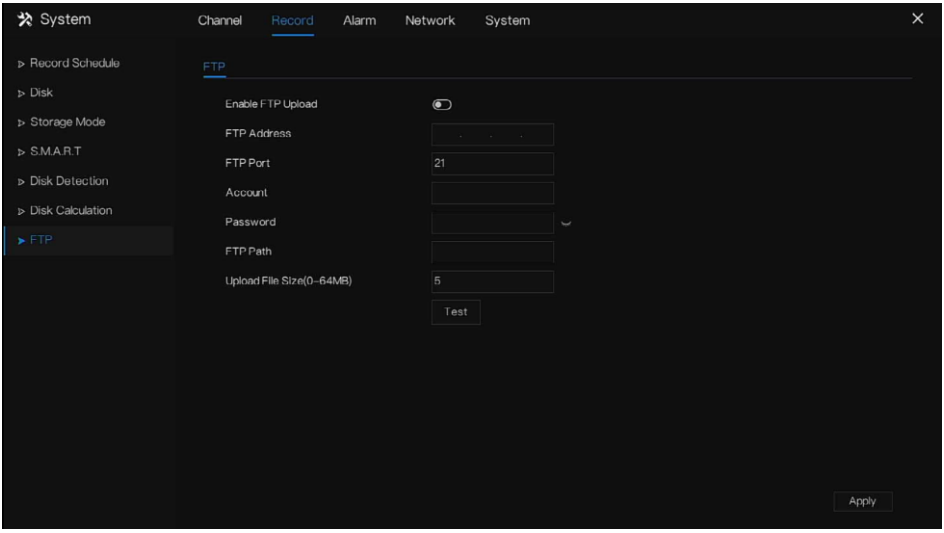


----End

6.3.8 FTP

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

Figure 6-37 FTP



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

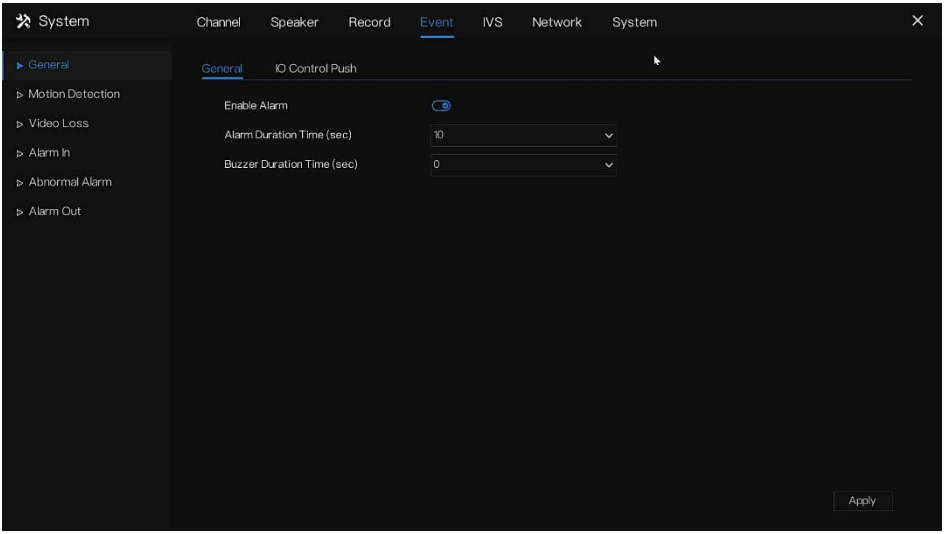
Set the **General**, **Motion Detection**, **Video Loss**, **Alarm In**, **Abnormal Alarm**, and **Alarm Out** in the **Event** screen.

6.4.1 General

6.4.1.1 General

Step 1 Navigate to **Settings > Event > General**, as shown in Figure 6-38.

Figure 6-38 Alarm management screen



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

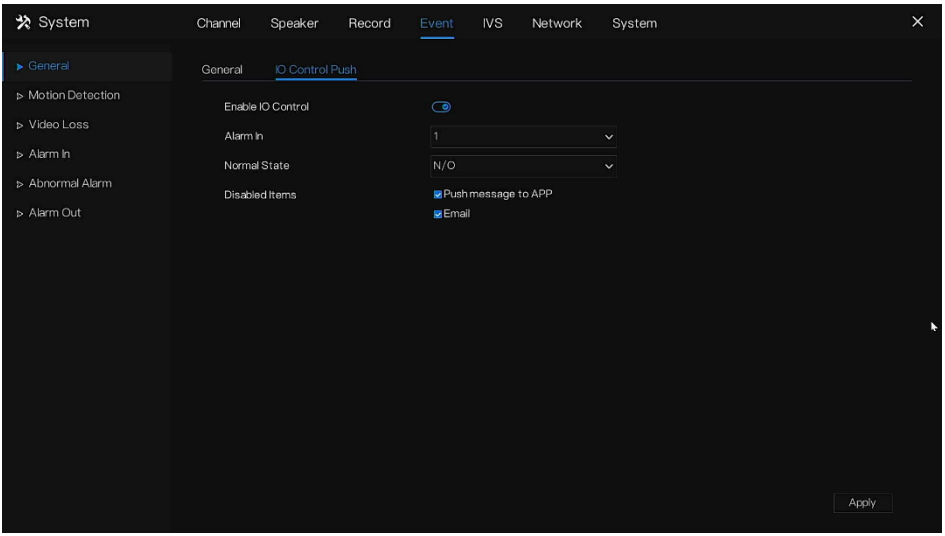
IO control push is to enable the **IO port** of the NVR rear panel. When the IO port receives the match signal, it will be a push message. For example, if you select **Normally Open** and tick the

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 6-39 IO control push



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

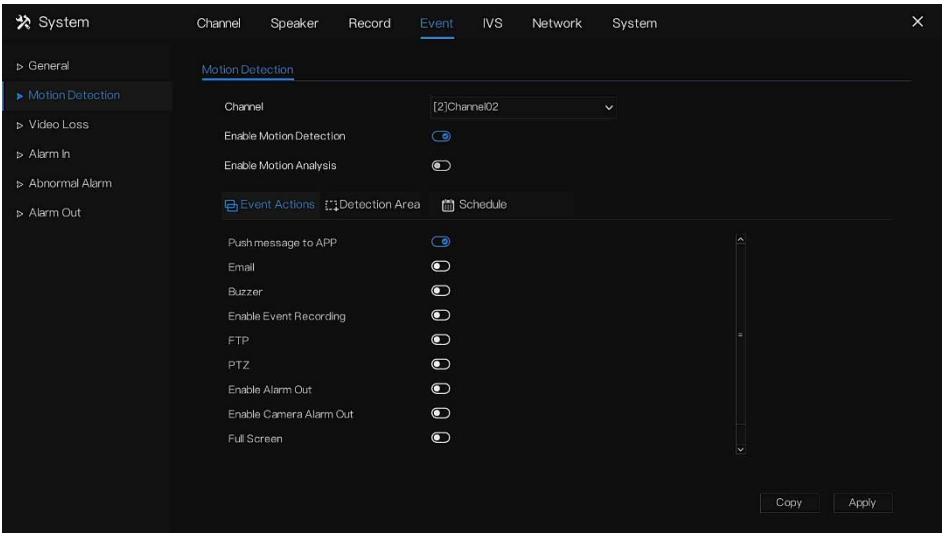
6.4.2 Motion Detection

The NVR 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 6-40.

Figure 6-40 Motion detection screen



Operation Steps

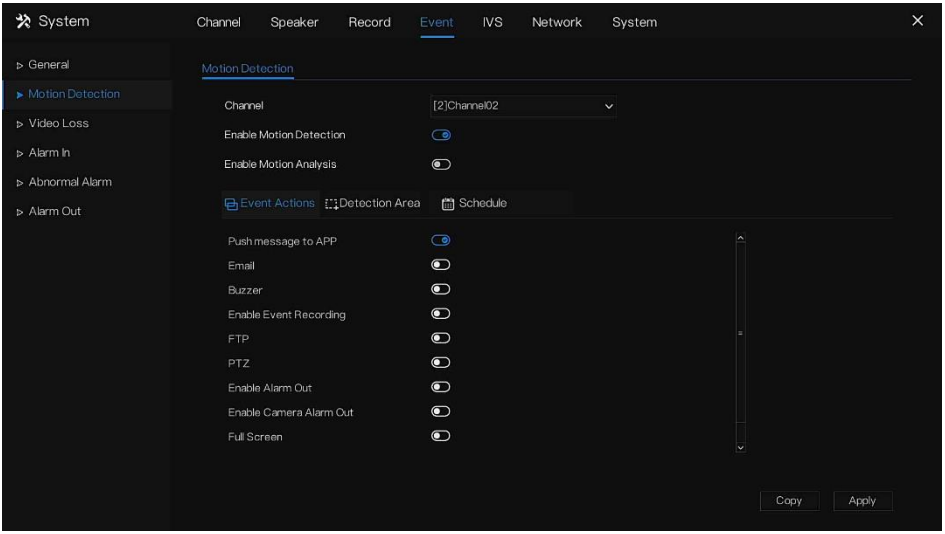
Step 1 Select a channel from the drop-down list of channels.

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 6-41.

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

Table 6-5 Event actions

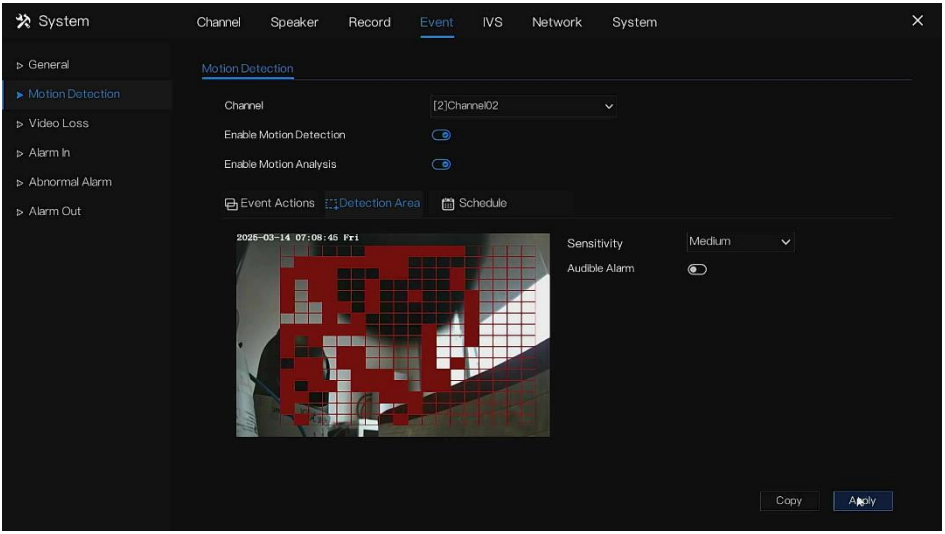


Parameter	Description
Push Message to app	When motion is triggered, you will receive a notification via the mobile app.
Email	When a motion is triggered, a notification will be sent to a designated email address. Note: Email settings must be configured under Network settings (see section *6.6.5 Email*) 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 *6.3.8 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 NVR 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. 

Step 5 Click the Area page to access the motion detection area setting, as shown in Figure 6-41.

Figure 6-41 Motion detection area setting screen



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.

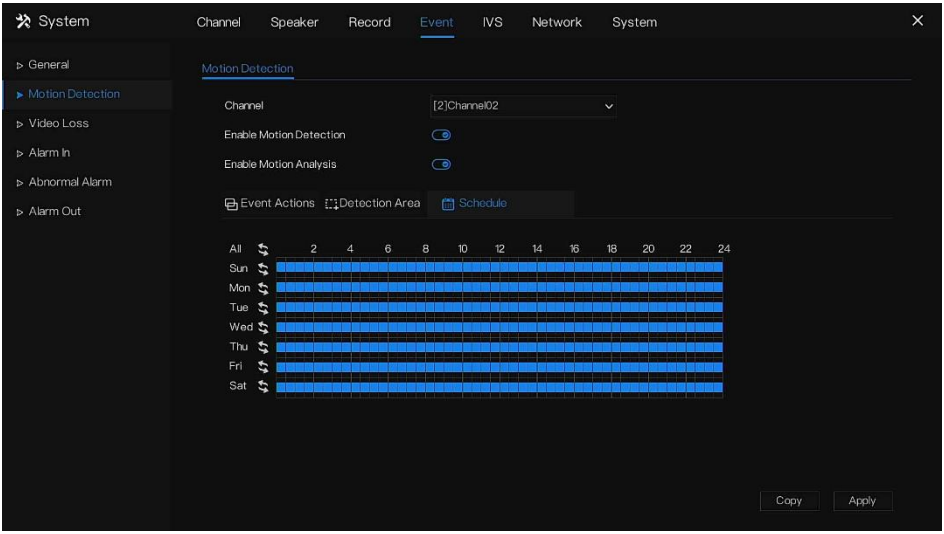
Step 6 Click the **Schedule** page to access the schedule screen. For details, please refer to section *6.3.1 Record Schedule*.

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 6-42 Alarm schedule



----End

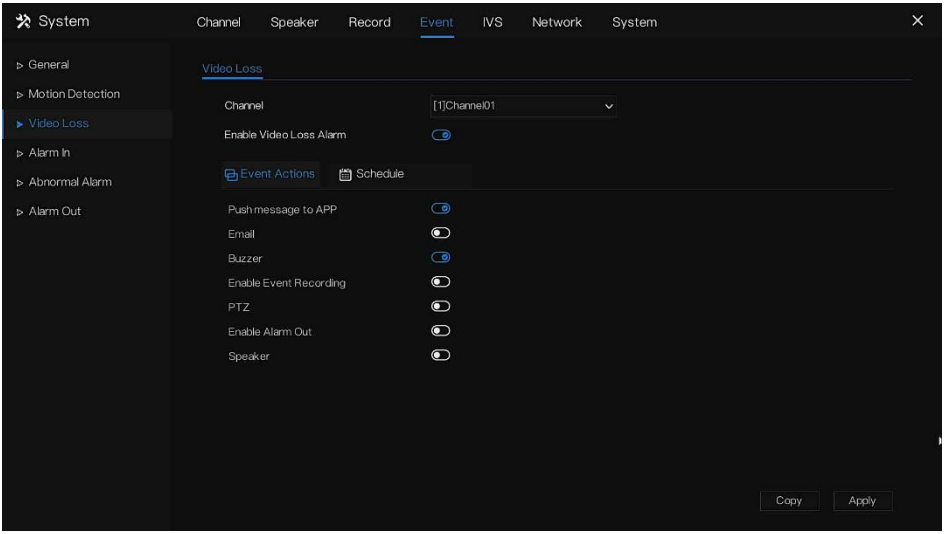
6.4.3 Video Loss

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

Operation Description

Navigate to **Settings > Event** > **Video Loss** as shown in Figure 6-43.

Figure 6-43 Video loss screen



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, Pop-up Message to Monitor, Send Email, Buzzer, FTP, PTZ, Alarm Out, Event Recordings, 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  and select a channel, then click  to apply the parameter settings to cameras in selected channels, and click  to save video loss settings.

----End

6.4.4 Alarm In

NOTE

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

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

Operation Description

Navigate to **Settings > Event > Alarm In** as shown in Figure 6-44.

Figure 6-44 Alarm in screen

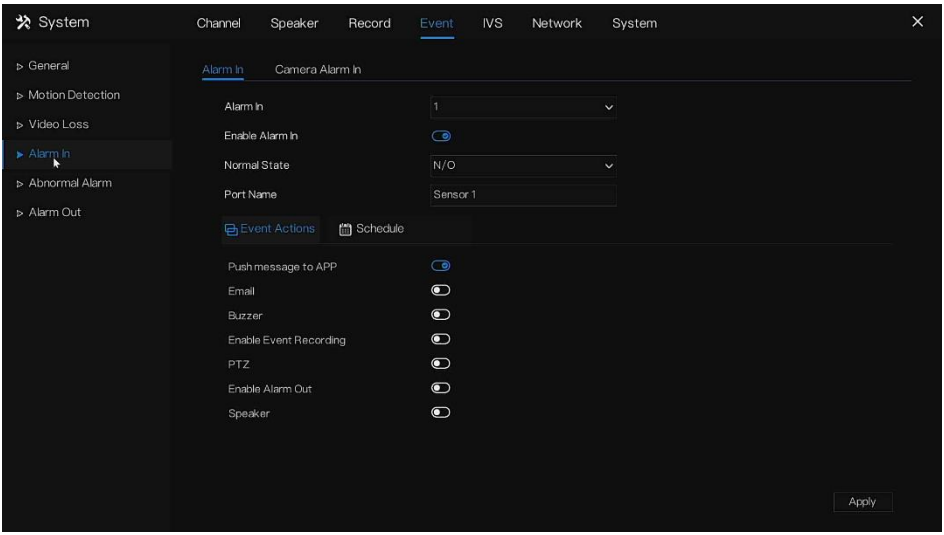
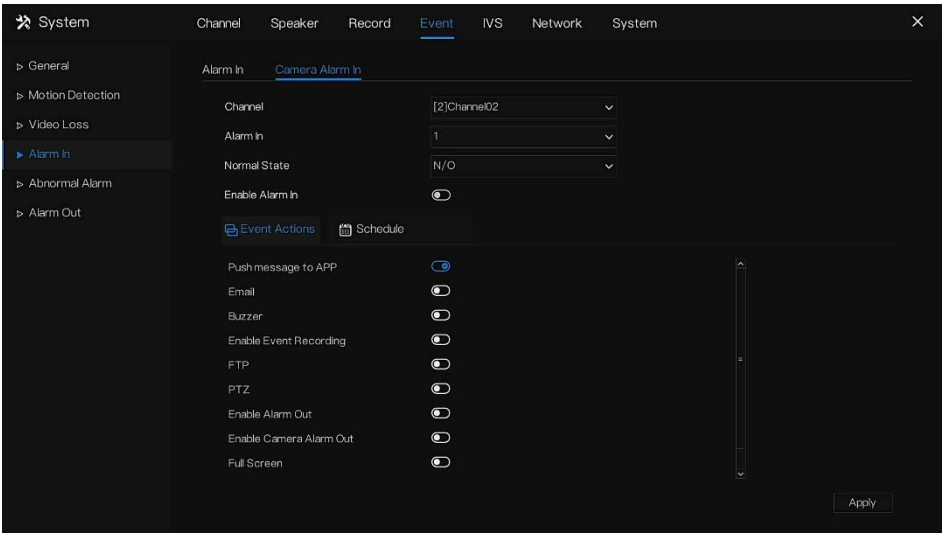


Figure 6-45 Camera alarm in



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, Sendi Email, Buzzer, FTP, PTZ, Full Screen, Alarm Out, Camera Alarm Out, Event Recording, 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 **section *6.3.1 Record Schedule*.**

Step 8 Click 

to save the settings of **Alarm In**.

----End

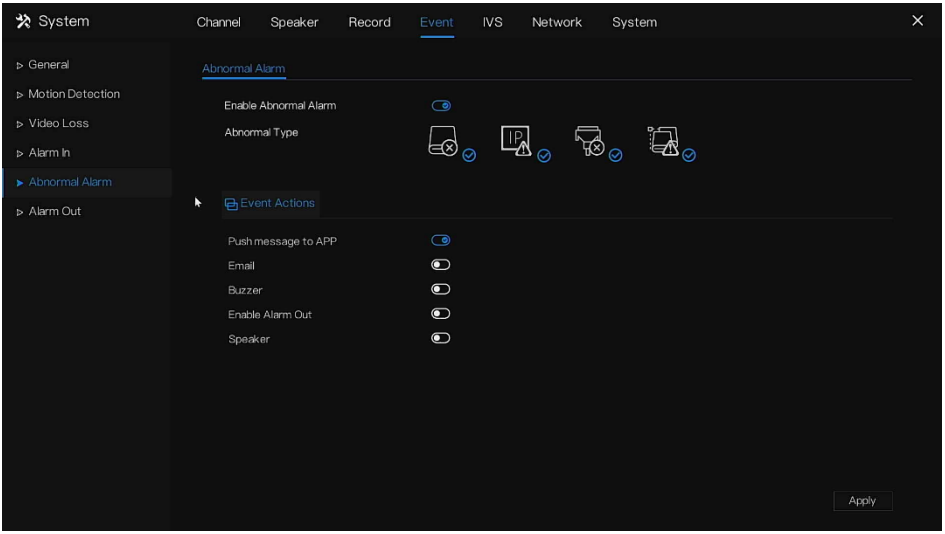
6.4.5 Abnormal Alarm

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

Operation Description

Step 1 Navigate to **Settings > Event > Abnormal Alarm** as shown in Figure 6-46.

Figure 6-46 Abnormal alarm screen



Step 2 Tick the abnormal actions.

Step 3 Enable the event actions to include: Push Message to App, Send Email, Buzzer, 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

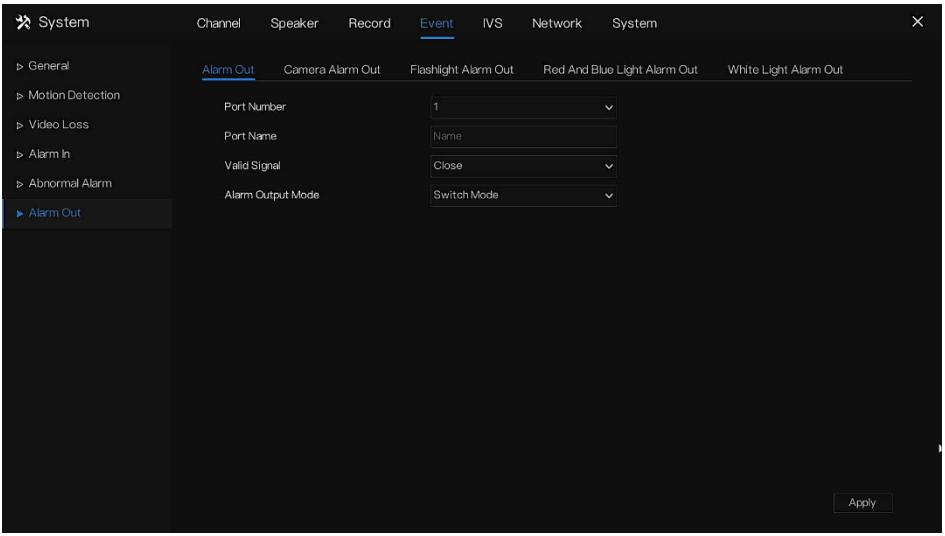
6.4.6 Alarm Out

6.4.6.1 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 6-47 Alarm out



----End

6.4.6.2 Camera Alarm out

NOTE

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

Figure 6-48 Camera alarm out

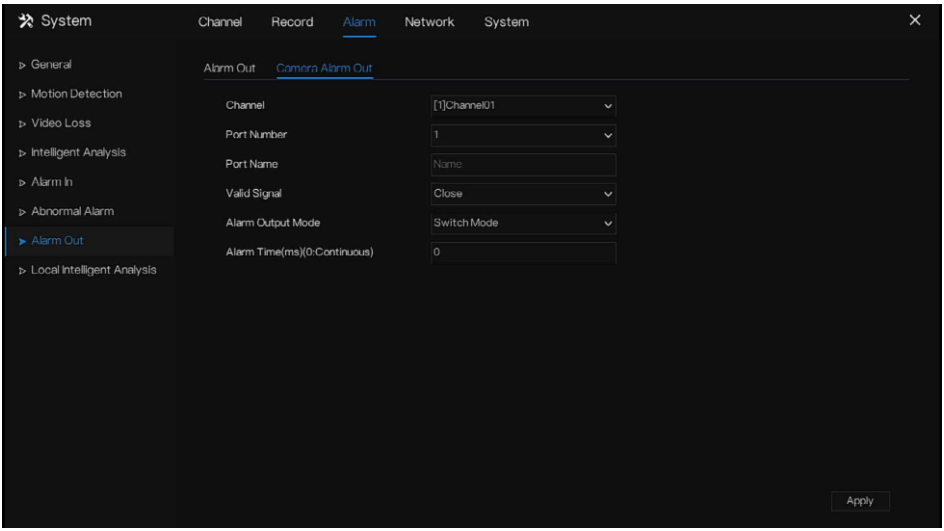


Table 6-6 Camera alarm out

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

6.4.6.3 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 6-49 Flashlight alarm out

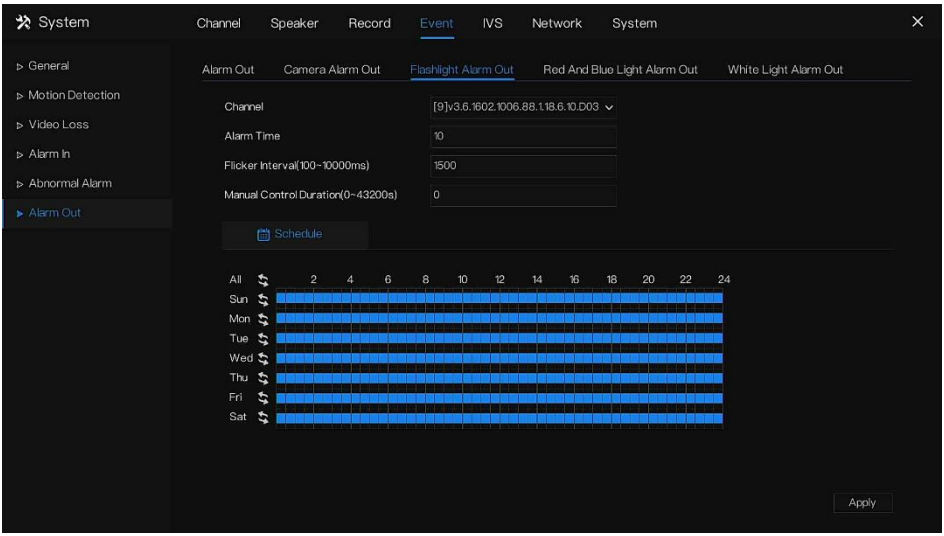


Figure 6-50 Red and blue light Light alarm out

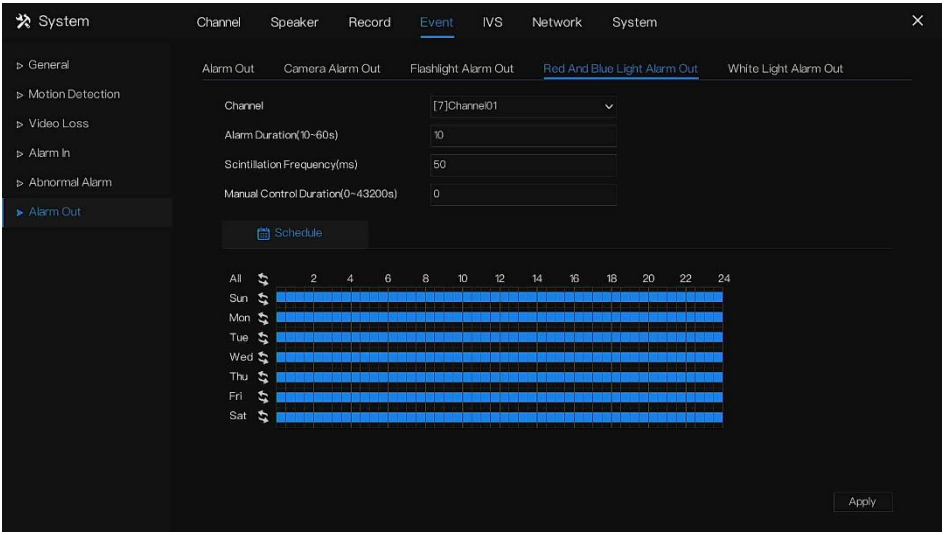


Figure 6-51 White light alarm out

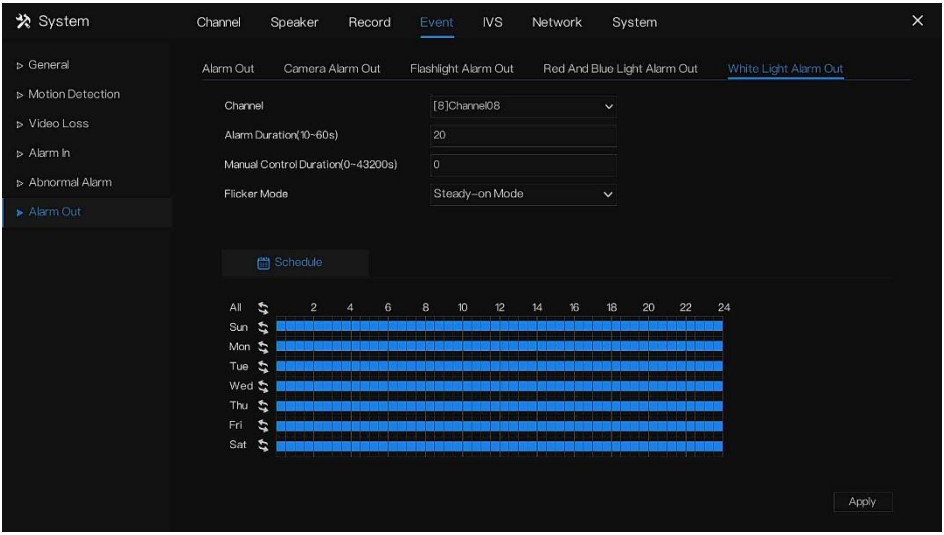


Table 6-7 Camera alarm out

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.

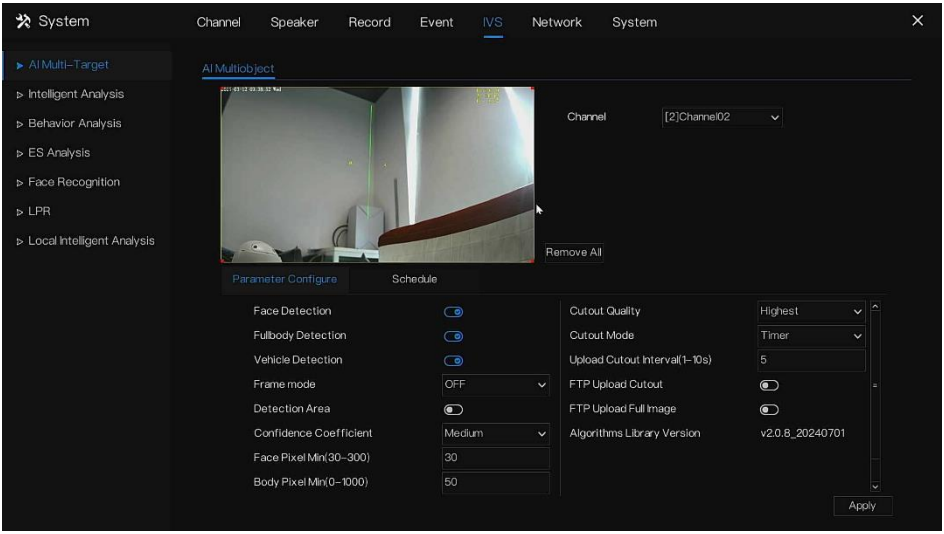
6.5 IVS Configuration

Set the **AI Multi-Target, Intelligent Analysis, Behavior Analysis, ES Analysis (Environmental Safety), Face Recognition, LPR,** and **Local Intelligent Analysis** in the IVS (Intelligent Video System) screen.

6.5.1 AI Multi-Target

1. Navigate to **Settings > IVS > AI Multi-Target** as shown in Figure 6-52.

Figure 6-52 AI Multiobject



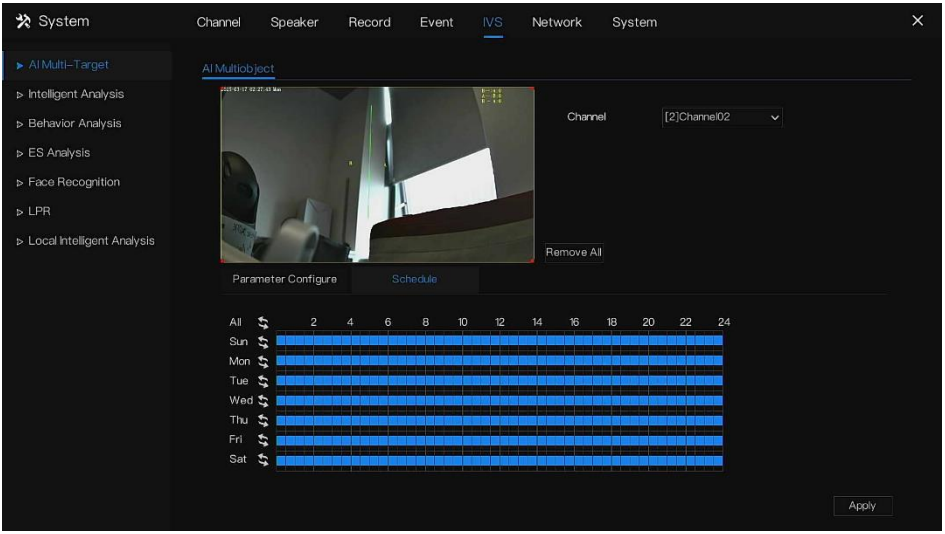
2. Choose the intelligent camera from the drop-down list.
3. Configure the parameters as per Table 6-8.

Table 6-8 AI Multiobject

Parameter	Description	How to set
Face Detection	The camera will snap the face when someone appears in the live video.	Enable
Full body Detection	The camera will snap the whole body when someone appears in the live video.	Enable
License Plate Detection	The camera will snap the license plate when the vehicle's license plate appears in live the video.	Enable
Vehicle Detection	The camera will snap the license plate when the vehicle appears in the live video.	Enable
Display Trace Info	Enable this function and a trace frame will show in the live video. Mode 1:  Mode 2: 	Choose from the drop-down list.
Show Detection area	Enable to set a detection area, and the frame will show in the live video	Enable

Parameter	Description	How to set
Confidence Coefficient	In the range of snap images, there are three types such as high, mid, and low. The higher the confidence, the better the snap quality and the fewer snapshots.	Choose from the drop-down list.
Face pixel min(30-300)	30-300 pixels; the smaller the pixel is set, the more faces will be captured, but it may be mistaken.	Input a value ranges 30 to 300
Body pixel min(30-300)	30-300 pixels; the smaller the pixel is set, the more body will be captured, but it may be mistaken.	Input a value range of 30 to 300
Vehicle pixel min(30-800)	30-300 pixels; the smaller the pixel is set, the more faces will be captured, but it may be mistaken.	Input a value range of 30 to 800
Image matting quality	For the quality of snap images, three modes can be chosen such as low, mid, and high.	Choose from the drop-down list.
Snapshot mode	Three modes can be chosen such as timing, and optimal.	Choose from the drop-down list.
Upload image interval(1-10 s)	At timing mode, set the interval of the uploaded image.	Input a value ranges 1 to 10
FTP upload image matting	**Configuration** > **Network Service** > **FTP** set FTP-related parameters, the captured picture will be sent to the set FTP location.	Enable
FTP upload whole image	Capture a picture and send a whole image.	Enable

Figure 6-53 Schedule



----End

6.5.2 Intelligent Analysis (Only for Some Models)

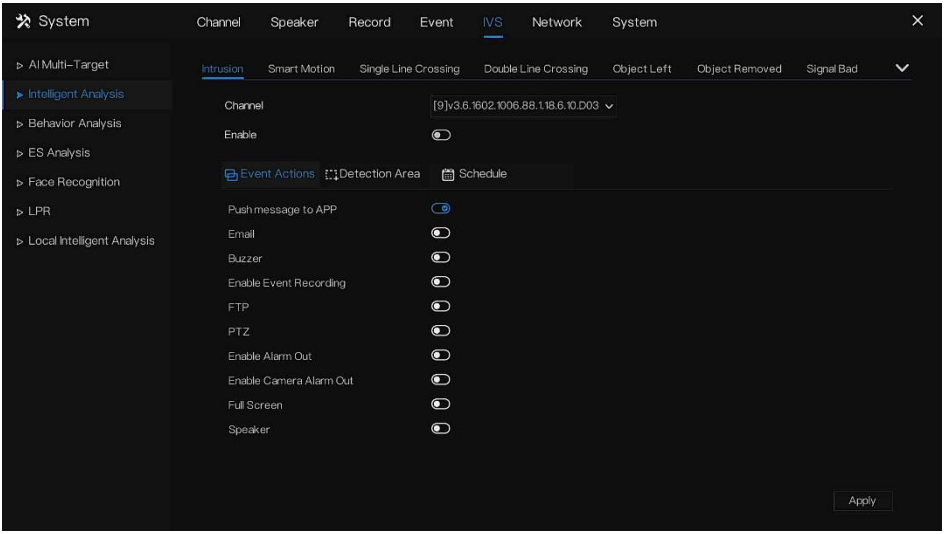
NOTE

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



Step 2 Select one action to set the alarm. (**Intrusion, Smart Motion, Single Line Crossing, Double Line Crossing, Object Left, Object Removed, Signal Bad, Loiter, Multi-loiter, Abnormal Speed, Wrong Way, Illegal Parking, People Counting, Fence, Enter Area, Leave Area, Advanced**).

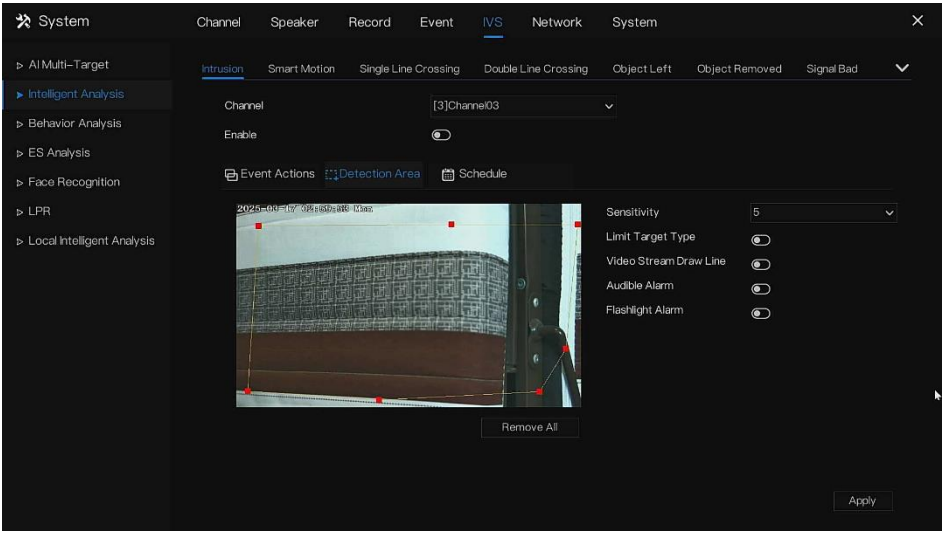
Step 3 Select a channel from the drop-down list of channels.

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*.**

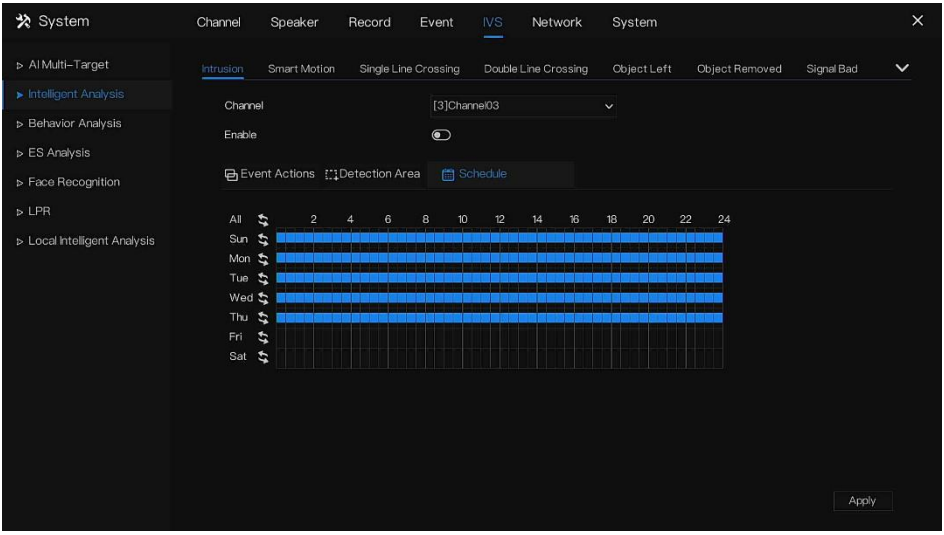
Step 6 Click the Detection Area page to set the detection area. Use the mouse to draw the polygonal region to deploy.

Figure 6-55 Detection area



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

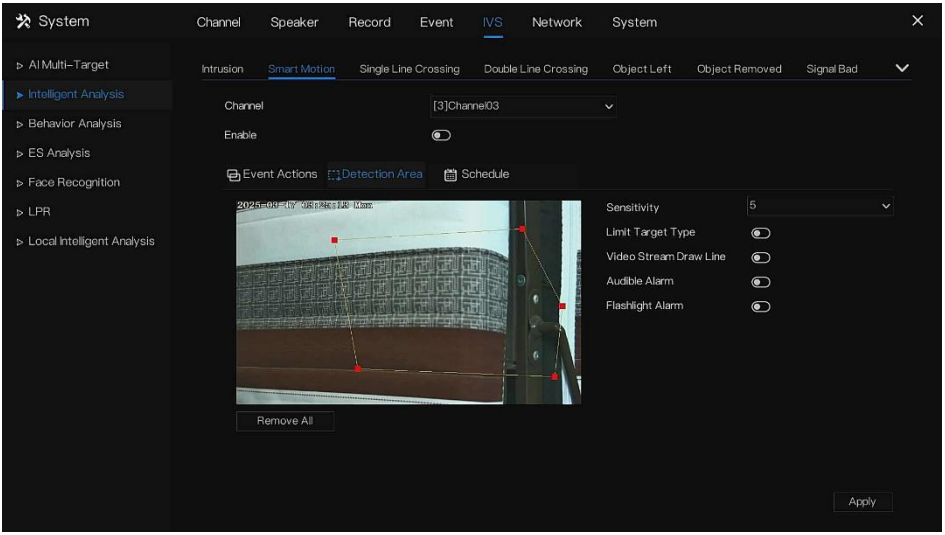


Step 8 Click Apply to save the settings.

6.5.2.2 Smart Motion

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

Figure 6-57 Smart Motion



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 6-9 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

People Counting:

This function is set for the channel cameras.

Figure 6-58 People counting

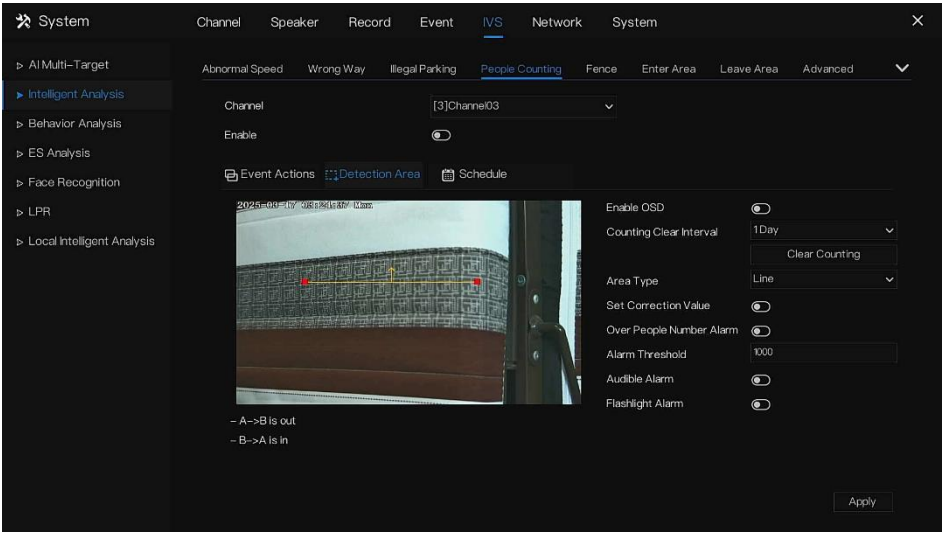


Table 6-10 People counting parameters

Parameter	Description	Setting
Enable	Click the button to enable people counting.	[How to set] Click Enable to enable. [Default value] **OFF**

OSD enables	When enabled the statistical data of people counting will show on OSD	[How to set] Click Enable to enable. [Default value] **OFF**
Counting clear interval	Five modes can be chosen such as 10 min, half-hour, 1 hour, 12-hour, and 1 day.	[Setting method] Choose from the drop-down list [Default value] **7**
Area type	The area to distinguish entry and exit.	[Default value] **Line**

----End

Fence:

It is only available for Fence AI multi-object cameras. When a person or car is found in the detection area, it will alarm.

Users can choose several event actions to alarm.

Figure 6-59 Fence

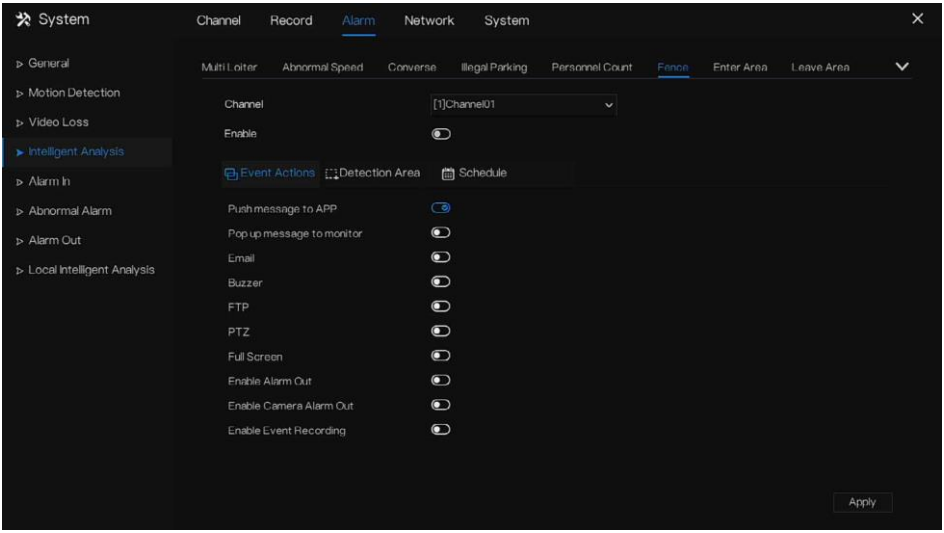
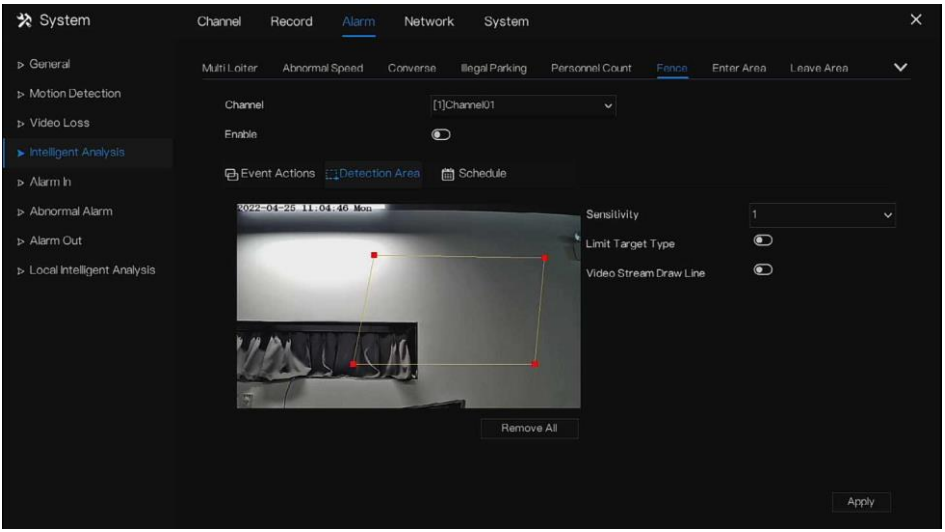


Figure 6-60 Fence detection area



Enable limit target type; choose the type (person or car, person, car).

Enable video stream draw line; when detects the car or person, it will show the blue frame to mark the target.

Use the mouse to draw the detection area. Users can draw serval areas depending on the real condition.

----End

6.5.3 Behavior Analysis

On the Behavior Analysis screen, users can set the people counting, heat map set, and heat map. The heat map is applicable for dual-lens cameras and panoramic cameras.

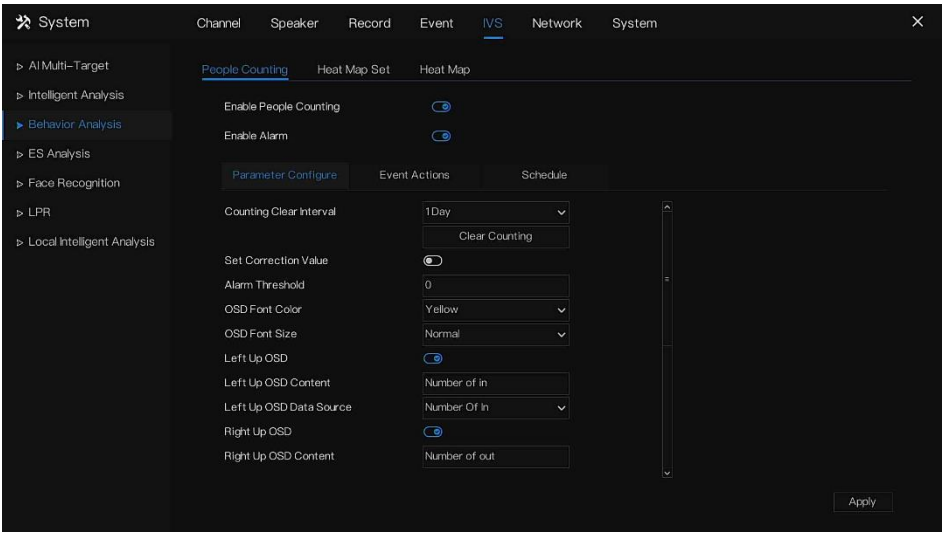
6.5.3.1 People Counting

This function is set for the NVR, the data is from all channels of the NVR, and the OSD will show on the live video of the UI.

Operation Description

Step 1 Navigate to **Settings > IVS > Behavior analysis > People Counting** as shown in Figure 6-61.

Figure 6-61 People counting screen



Step 2 Click  to enable the people counting and alarm.

Step 3 Set the Parameter Configure.

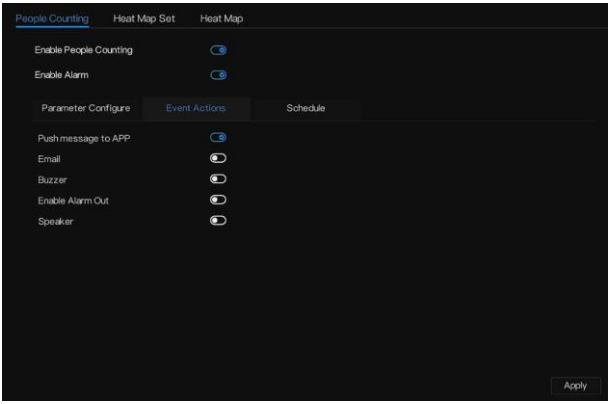
Table 6-11 Parameter Configure

Function	Procedure	Description
Counting Clear Interval	The user can choose the clear interval from the drop-down list: never, 10 min, halt-hour, 1 hour, 12 hours, and one day.	Choose from the drop-down list.
Set Correction Value	Enable and set the count correction value. It can be positive or negative. For example, if 30 people are entering the area before counting, input 30 to correct. If 30 people go out of the area, input -30.	Choose from the drop-down list.
Alarm Threshold	Enable. If the counting number is over the threshold, it will alarm. The threshold of activating the alarm.	Input a value
OSD Font Color	Set the OSD font color; the default color is yellow.	Choose from the drop-down list.
OSD Font Size	Choose the size of OSD font: small/normal/big can be chosen. The default size is normal.	Choose from the drop-down list.
Left Up OSD	Enable. Choose the content and Data source to show on live video.	Input a value ranges 1 to 10

Function	Procedure	Description
Left Up OSD Content Left Up OSD Data Source Right Up OSD Right Up OSD Content Right Up OSD Data Source Left Down OSD Left Down OSD Content Left Down OSD Data Source Right Down OSD Right down OSD Content Right Down OSD Data Source		Enable to show OSD; the content can be costumed as the figure.
OSD Counting Channels	The default is for all channels to count. The channel cameras enable the people counting intelligent analysis.	

Step 4 Set the Event actions.

Figure 6-62 Event actions



Step 5 Set the schedule of People Counting.

Figure 6-63 Set schedule

Step 6 Click Apply to save the settings.

----End

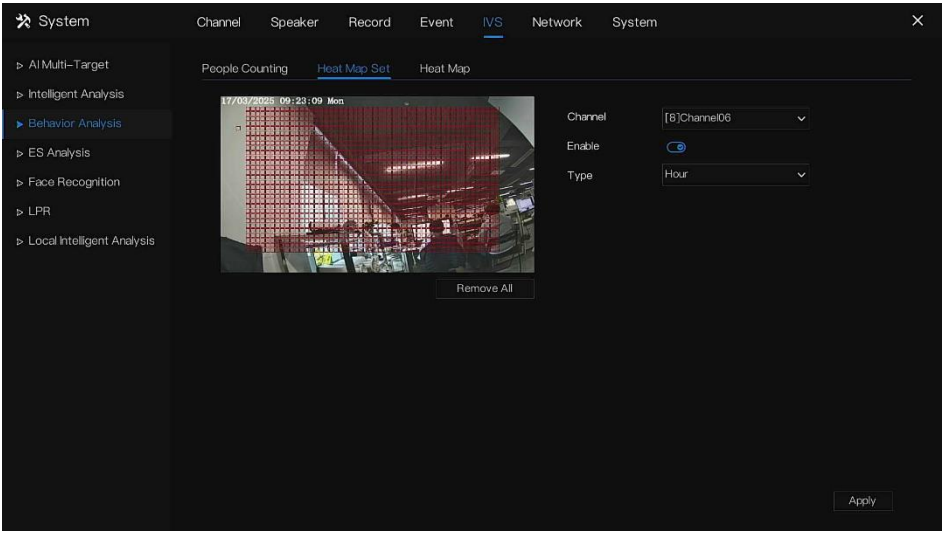
6.5.3.2 Heat Map Set

The Heat Map is a method of data analysis, statistics, and intuitive display, displaying customers' regions, targets, and geographical locations in a specially highlighted form.

After the camera enables the heat map, it will automatically detect and count the flow of personnel in the detection area and identify the relative frequency of flow activities through different colors.

Step 1 Navigate to **Settings > IVS > Behavior Analysis > Heat Map Set,** as shown in Figure 6-64.

Figure 6-64 Heat map set



Step 2 Enable the heat map function. This function is disabled by default and needs to be manually enabled.

Step 3 Set the type. Is it statistical type, Hour (there are 24 pieces of data per day), or Day (there is 1 piece of data per day). The original data will be cleared when the type is switched. Please operate with caution.

Step 4 Click **Apply**. The message "Apply success!" is displayed, and the system will save the settings.

Heat map

Choose **Heat Map** on **Settings > IVS > Behavior Analysis** to access the heat map screen, as shown in Figure 6-65.

Figure 6-65 Heat map

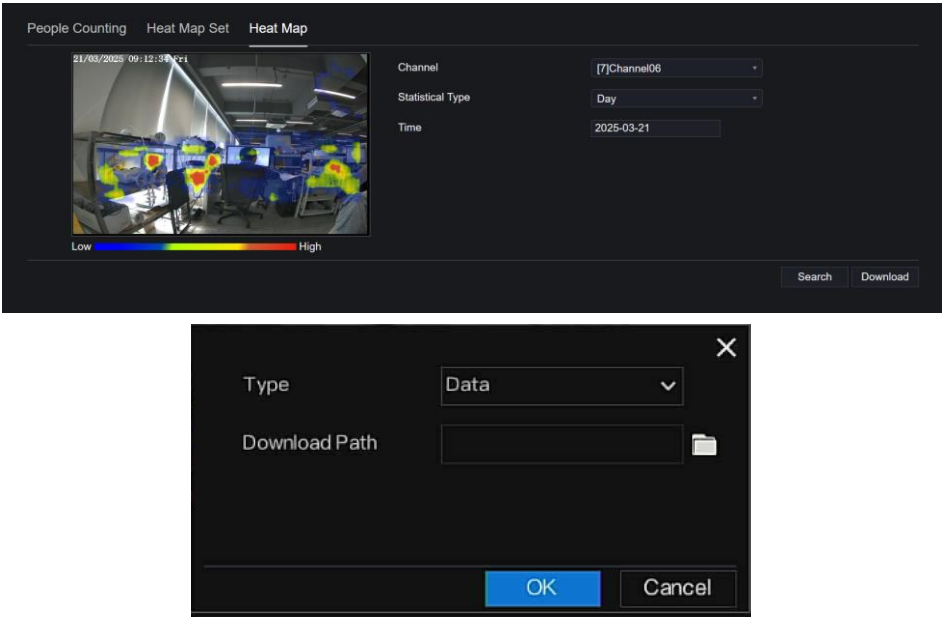


Table 6-12 Parameters of heat map

Parameter	Description	Setting
Type	Choose Data or Picture. Data is presented in numerical form to download; The picture is displayed in different areas with different colors on the downloaded picture.	[How to set] Choose from the drop-down list [Default value] **Normal mode**
Statistics type	Year/ Month/ Day/ Hour can be chosen.	[How to set] Click the button on. [Default value] **OFF**
Time	Select a retail time to search or download heat map data.	[How to set] Choose from the drop-down list
Heat map bar	Distinguish different degrees by different colors. The maximum value is the maximum data of a single area in the heat map at the current set time.	Null

Set the time to search, “Search” or “Download” the relevant heat map statistic.

Click "Search" to view directly or click " Download " to download the data in CSV format to a local folder.

----End

6.5.4 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.

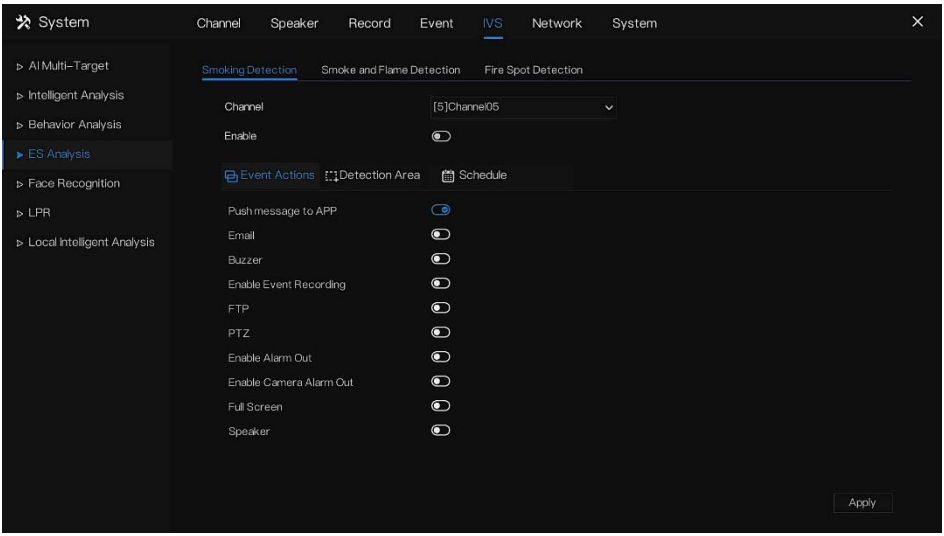
6.5.4.1 Smoking Detection

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 6-66.

Step 2 Choose the thermal camera to enable smoking detection.

Figure 6-66 Smoking detection

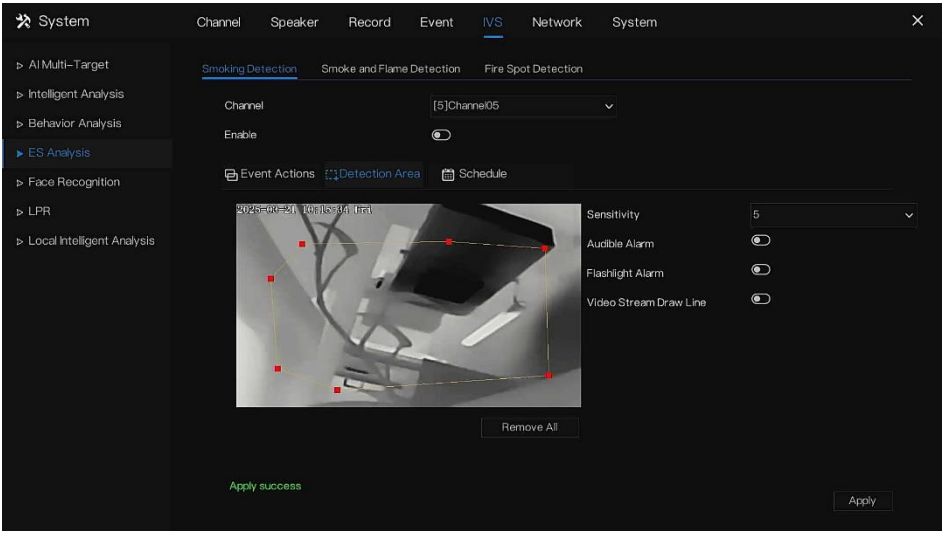


Step 3 Enable the event actions.

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

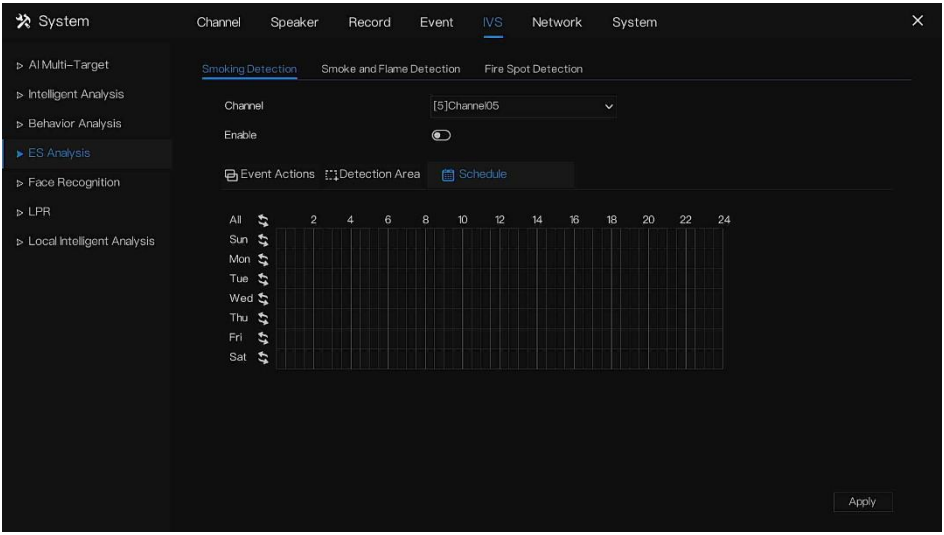
Step 5 For different cameras, you can choose to enable the audible alarm, flashlight alarm, or video stream draw line.

Figure 6-67 Smoking - Detection area



Step 6 Set the schedule to arm.

Figure 6-68 Smoking – Schedule



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

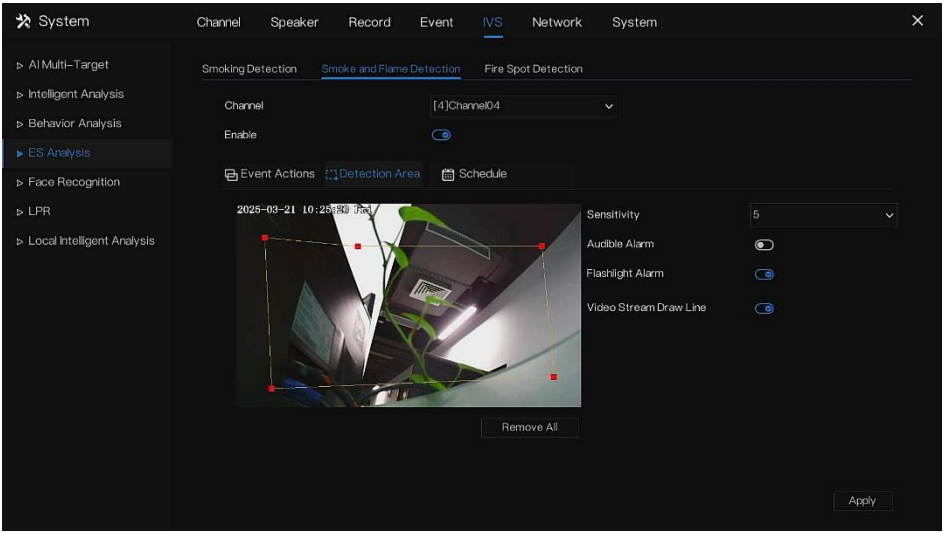
----End

6.5.4.2 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 6-69.

Figure 6-69 Smoke and flame detection



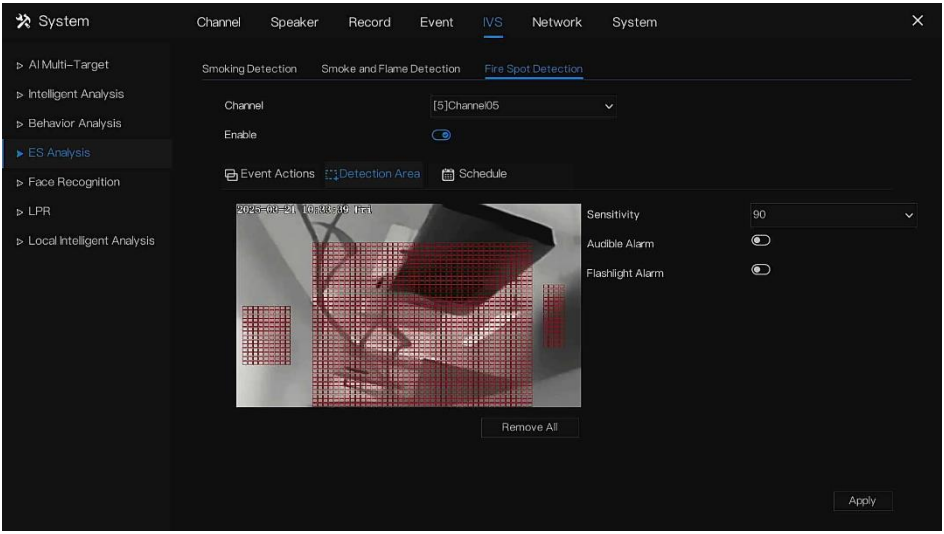
2. For the detailed settings, please refer to ***Chapter 6.5.4.1 Smoking Detection***.

6.5.4.3 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 6-70.

Figure 6-70 Fire spot detection



For the detailed settings, please refer to *Chapter 6.5.4.1 Smoking Detection*.

6.5.5 Face Recognition

At the face comparison interface, users can set different channels' strategies, such as similarity, display comparison results, face library, enable alarming, event action, and arming time.

Navigate to **Settings > IVS > Face Recognition** as shown in Figure 6-71.

Figure 6-71 Face recognition

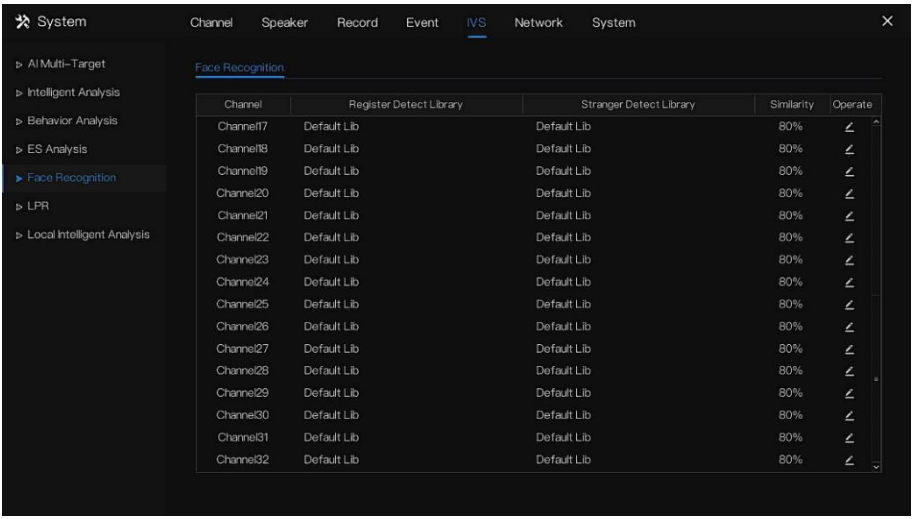


Figure 6-72 Strategy

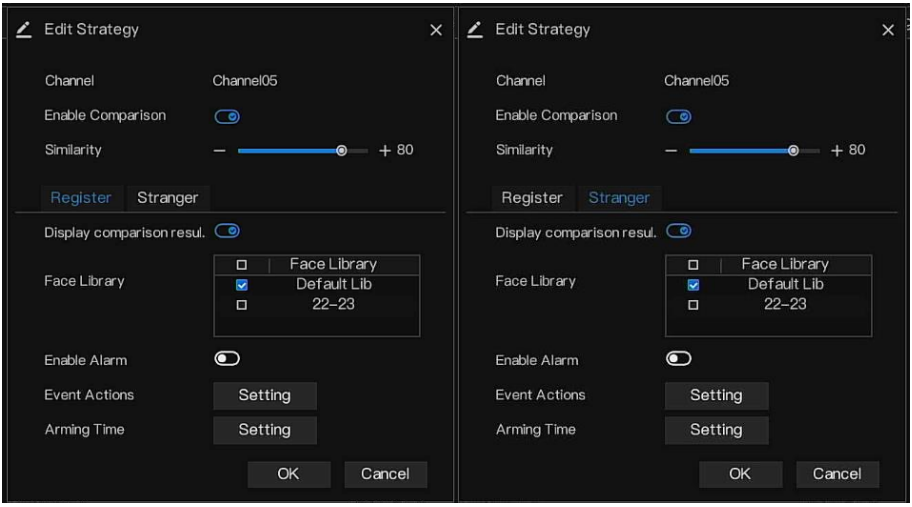


Figure 6-73 Event actions

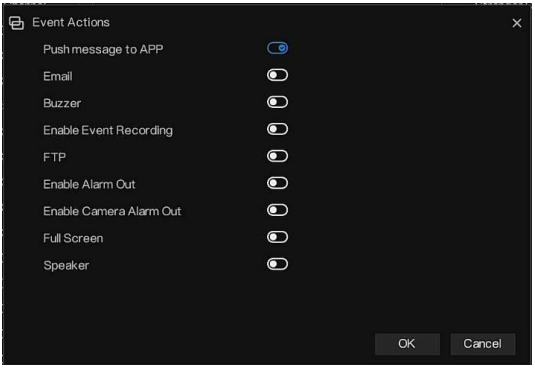


Figure 6-74 Arming time

----End

6.5.6 LPR(License Plate Recognition)

6.5.6.1 Basic setting

1. Navigate to **Settings > IVS** > **LPR basic setting** as shown in Figure 6-75.
2. Configure the basic settings as outlined in Table 6-13 below.

Figure 6-75 License plate recognition

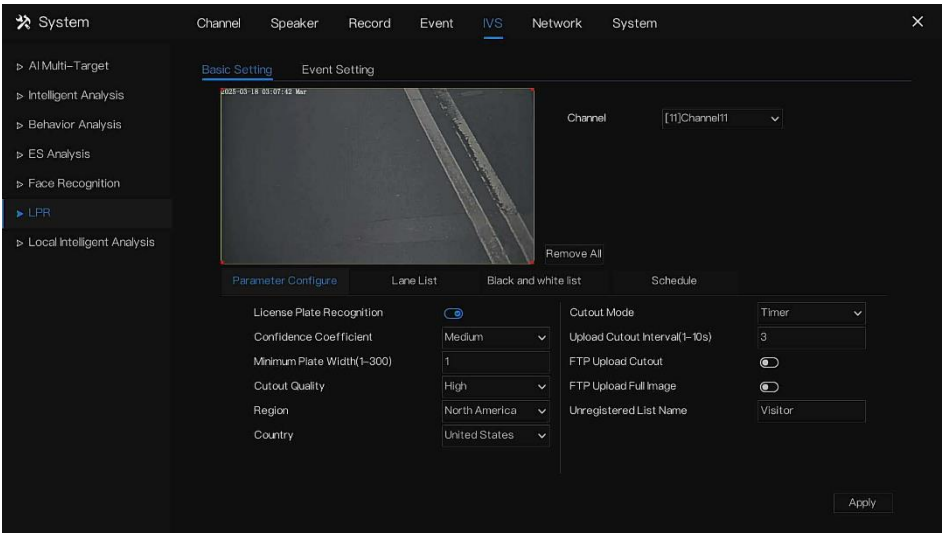


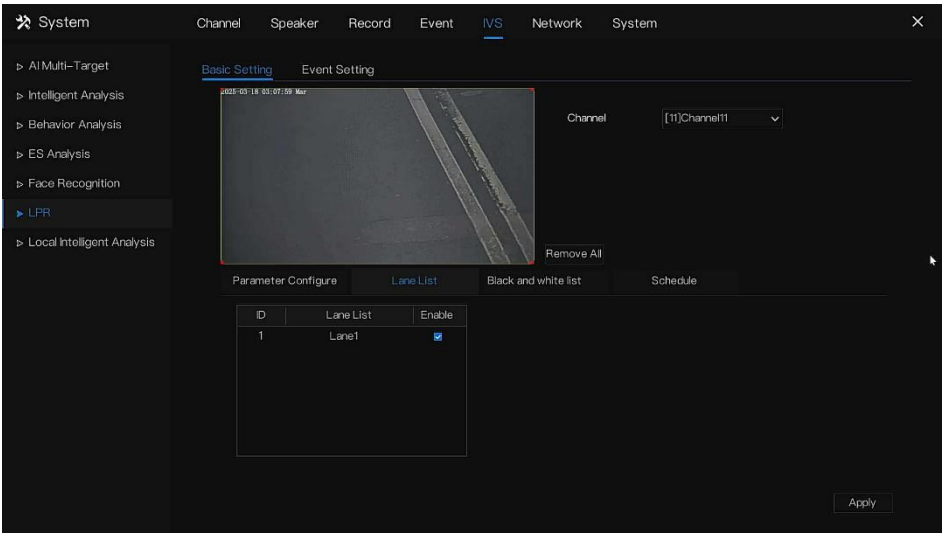
Table 6-13 License plate recognition

Function	Procedure	Description
License Plate Detection	The camera will capture the license plate when the car appears in live video.	[Setting method] Enable
Confidence coefficient	In the range of snapshot images, there are three types: high, mid, and low. The higher the confidence, the better the snapshot quality and the fewer snapshots.	[Setting method] Choose from the drop-down list.
Minimum Plate Width	The smaller the pixel is set, the more plate will be captured, but it may be mistaken.	[Setting method] Input a value ranges 1 to 300
Cutout Quality	For the quality of the snapshot image, three modes can be chosen, low, mid, and high.	[Setting method] Choose from the drop-down list.
Region	The region and country of license plate.	[Setting method] It is costumed
Country		
Cutout mode	Two modes can be chosen, timer and optimal. At timer mode, set the interval of the upload image.	[Setting method] Choose from the drop-down list.

Function	Procedure	Description
FTP Upload Image matting	**Configuration > Network Service > FTP** set FTP-related parameters, the captured picture will be sent to the set FTP location.	[Setting method] Enable
FTP Uploads Whole Image	Capture a picture and send a whole image.	[Setting method] Enable
Unregistered List Name	For the licenses of the unregistered list name, users can set a custom name to display, the default is “Visitor”.	[Setting method] It is costumed

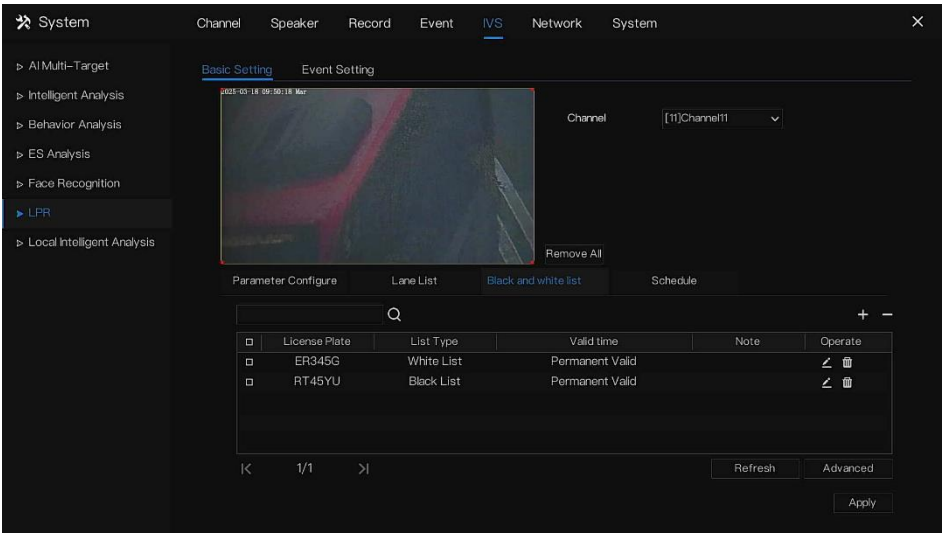
1. Users can set several lanes as the real scene.

Figure 6-76 Lane list



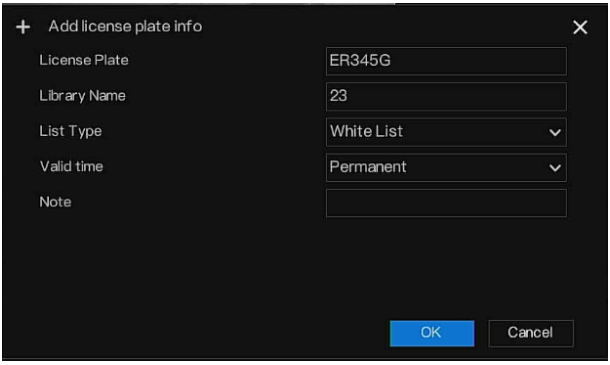
2. Users can add licenses to the list one by one, and the licenses will show on the list, as shown in Figure 6-77.

Figure 6-77 Black and white list



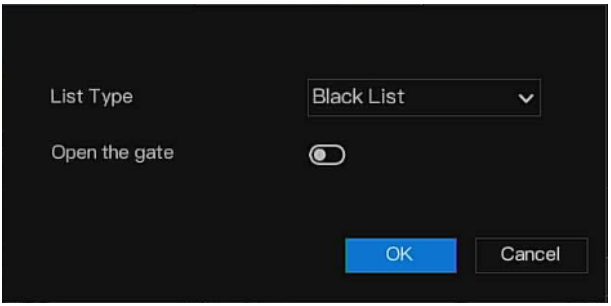
3. Click + to add the license set to the whitelist or blacklist. Tick the license plates, and click – to delete.
4. Click to edit the license plate. Click to delete the current license plate.

Figure 6-78 Add license plate



1. Click Refresh to update the list.
2. Click Advanced to operate the gate.

Figure 6-79 Advanced



6.5.6.2 License Comparison

At the License Plate interface, users can set strategies for different channels of license plate recognition cameras, such as register and unregister, enable alarming, event action, and arming time, as shown in Figure 6-80.

Figure 6-80 License Comparison

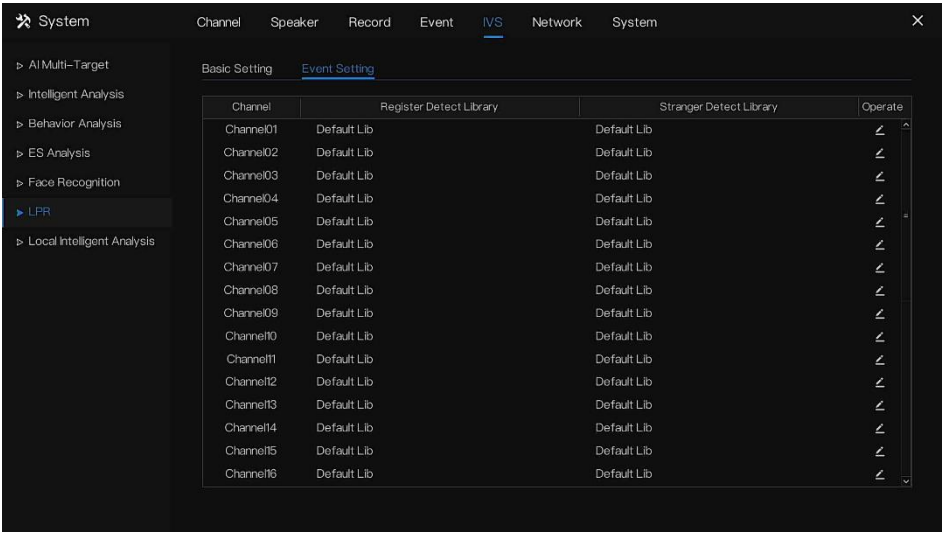


Figure 6-81 Strategy

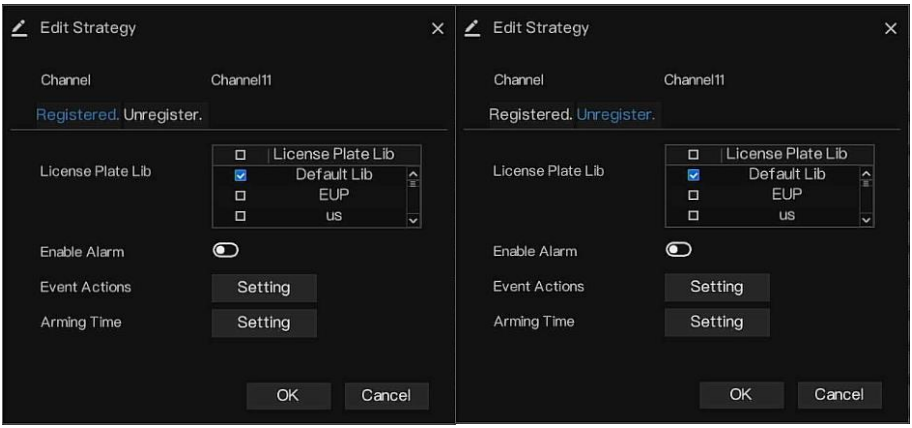


Figure 6-82 Event actions

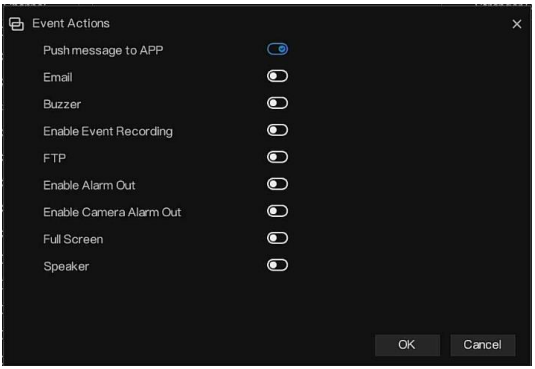


Figure 6-83 Arming time

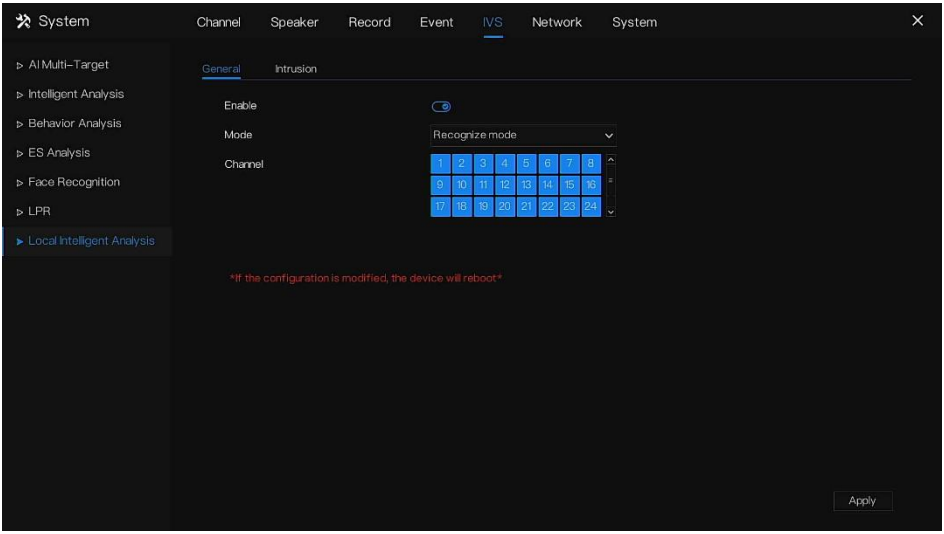
----End

6.5.7 Local Intelligent Analysis

6.5.7.1 General

1. Navigate to **Settings > IVS** > **Local Intelligent Analysis > General** as shown in Figure 6-84.

Figure 6-84 Local intelligent analysis – General



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

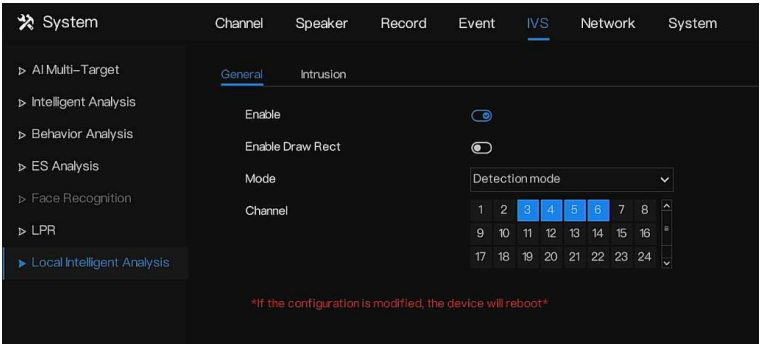
- The NVR3908 and 3916 support all channels' local intelligent analysis.
- The NVR of the model -J has the local intelligent analysis function. The recognize mode is only applicable for the AI multi-target cameras. The detection mode is for the NVR, without relativity with channel cameras.
- Enable or disable the intrusion, modify the channels, and the device will be rebooted**.**

When users choose the mode as recognition mode and choose the channels (all channels can be chosen if the channels support recognition functions) to enable this function, the **AI Recognition**

and **Attendance** interface will be enabled at the quick menu, for detailed information, please refer to **section *5.4*.**

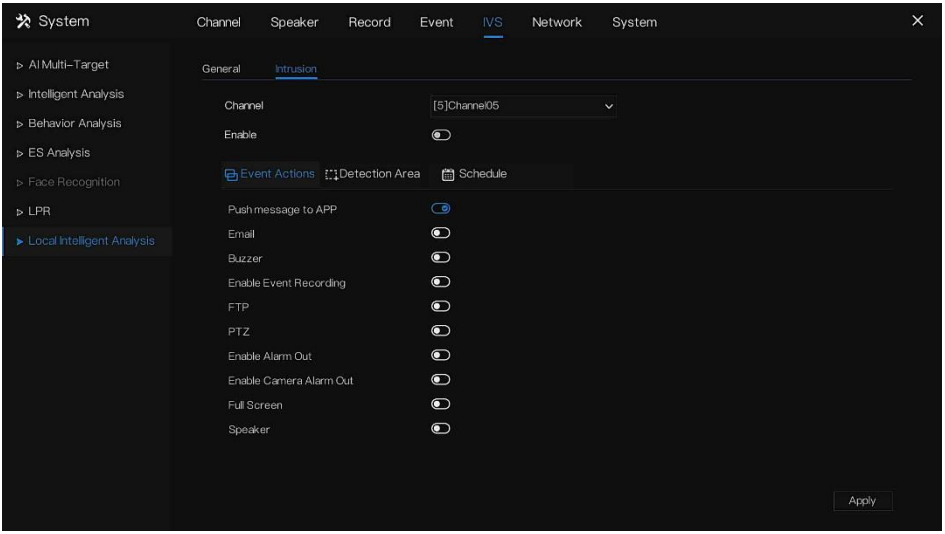
6.5.7.2 Intrusion

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



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

Figure 6-85 Intrusion

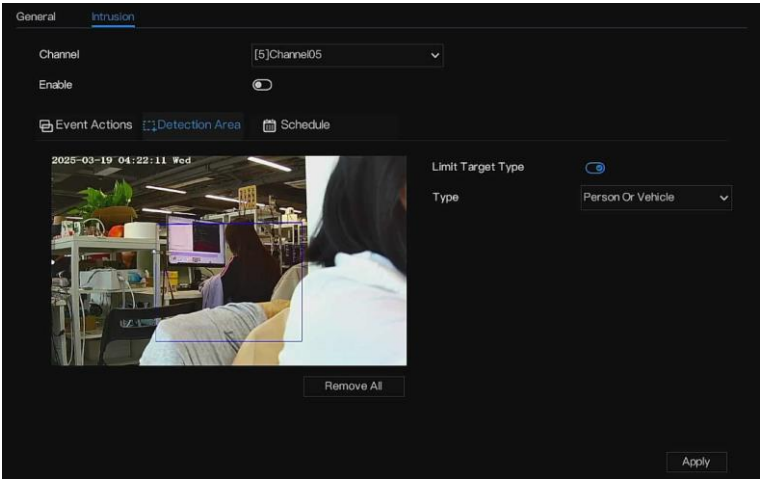


Event action：

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 6-86 Detection area



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/car, or car.

Figure 6-87 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 6-87.

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 6-88.

Figure 6-88 Network management screen

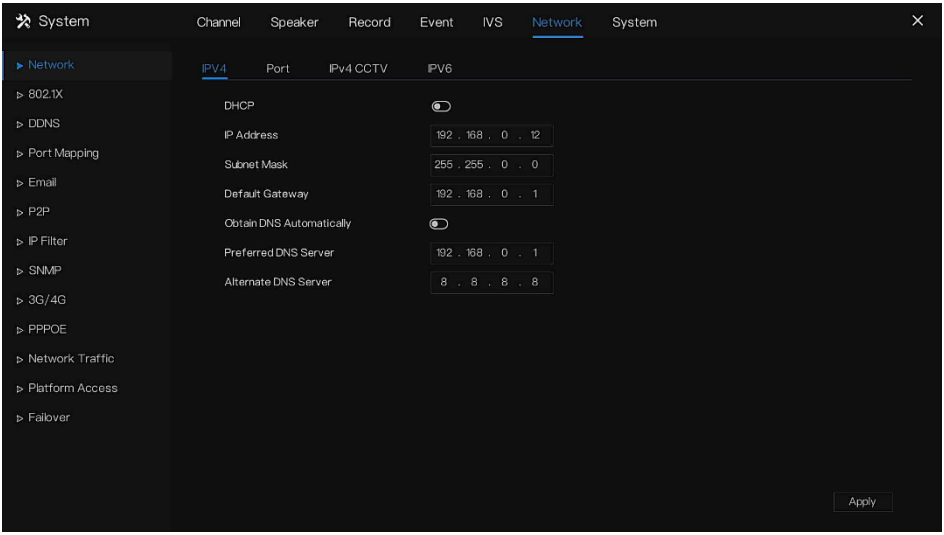


Table 6-14 Network

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

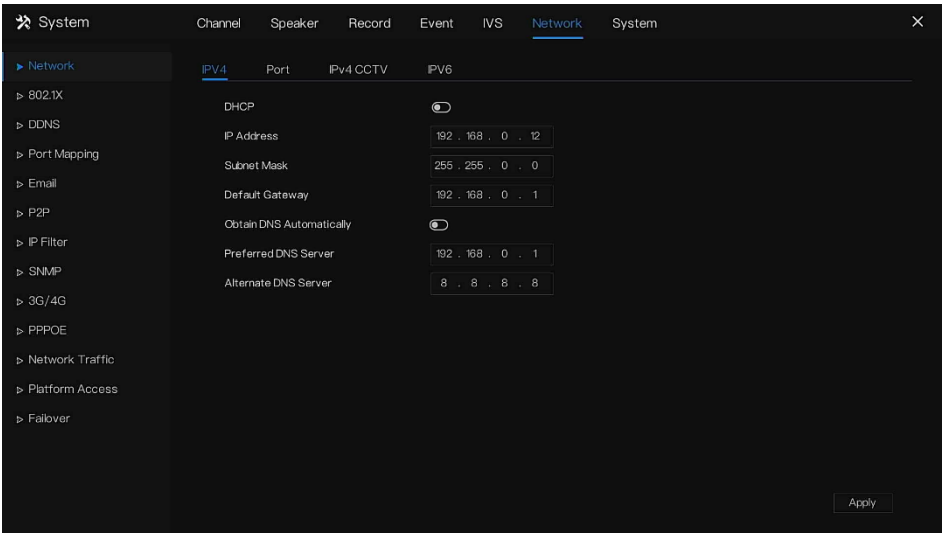
Set **DHCP a**nd **DNS** manually or automatically.

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 NVR is connected should have the DHCP function, and the router distributes an IP to the NVR). The function is disabled by default.

Figure 6-89 Enable DHCP



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  to save IP settings.

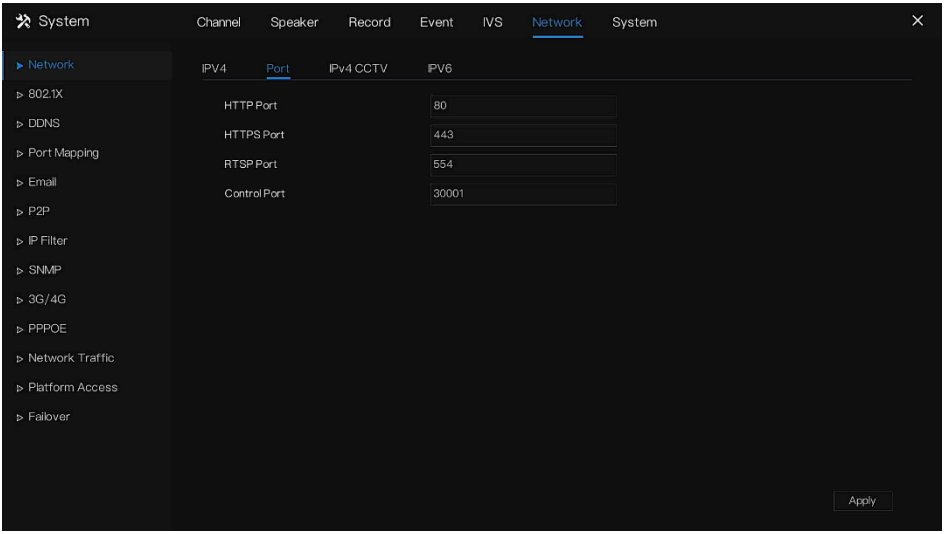
----End

6.6.1.2 Port

Operation Steps

Step 1 Click **the Port** page to access the port setting screen, as shown in Figure 6-90.

Figure 6-90 Port setting screen



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 6-15 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 NVR is connected to the APP InView Pro or the platform 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)

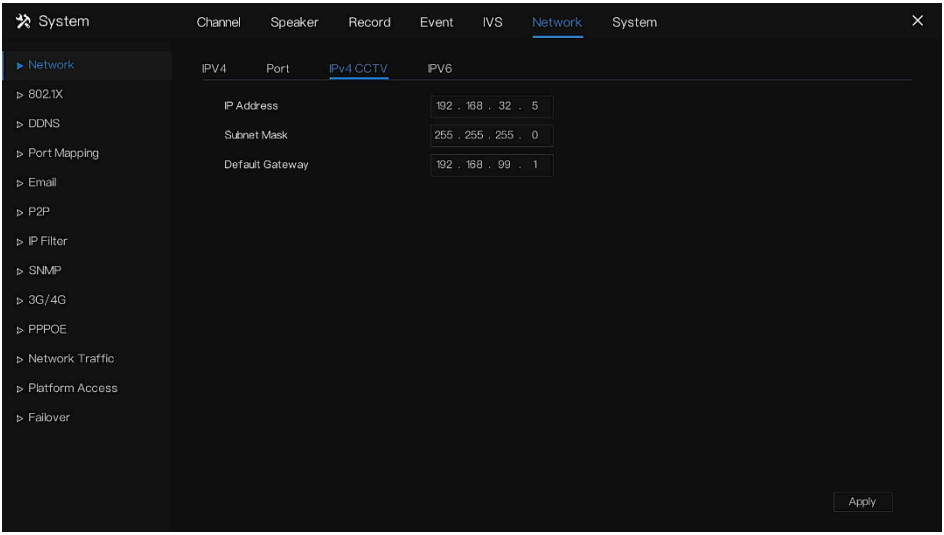
The non-POE device has two network ports, WAN and LAN.

If the user connects to the NVR via the LAN port, they need to use the IPv4 address of the CCTV to access the NVR'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 6-91.

Figure 6-91 IPv4 CCTV



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 NVR 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.

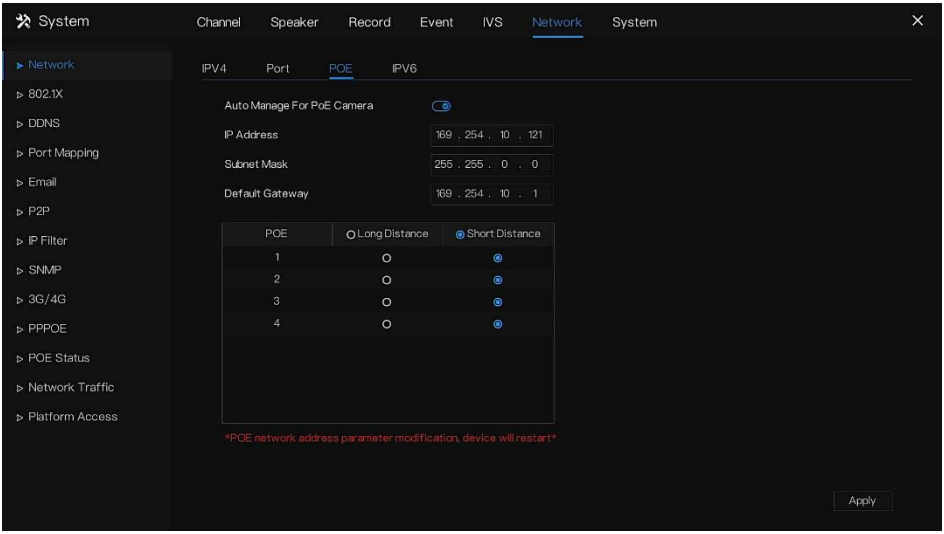
----End

6.6.1.4 POE (Only for Some Models)

Operation Steps

Step 1 Click the **POE** on **Settings > Network > Network** to access the POE setting screen, as shown in Figure 6-92.

Figure 6-92 POE screen



Step 2 The NVR will deploy IP addresses to the cameras connected to POE immediately when the auto-manage for the POE camera is enabled.

Step 3 Users can choose long distance or short distance depending on the real scene. When the network cables are more than 100m, it is recommended to choose the long distance. The long distance can support up to 250 meters; this mode will reduce broadband from 100m to 10m.

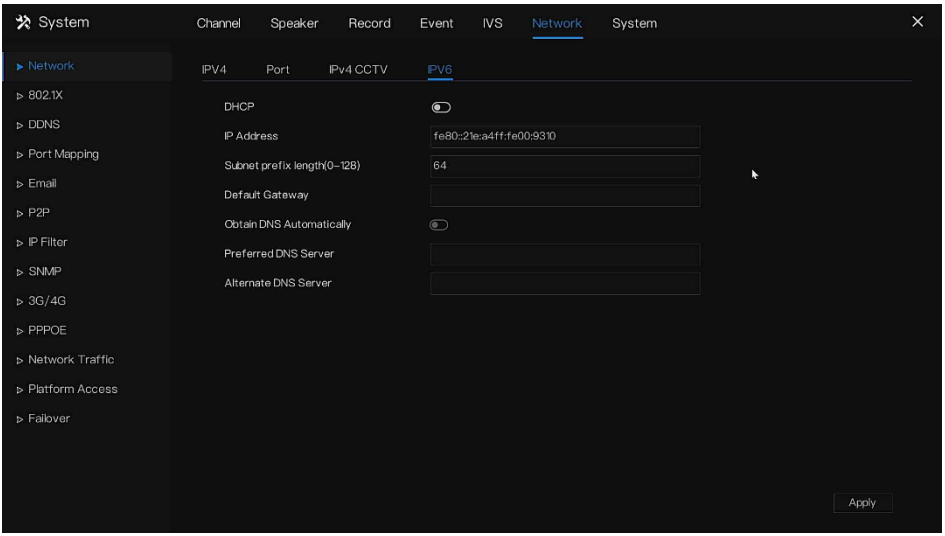
Step 4 Click Apply to set the POE camera IP address successfully.

----End

6.6.1.5 IPV6

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

Figure 6-93 IPV6



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.

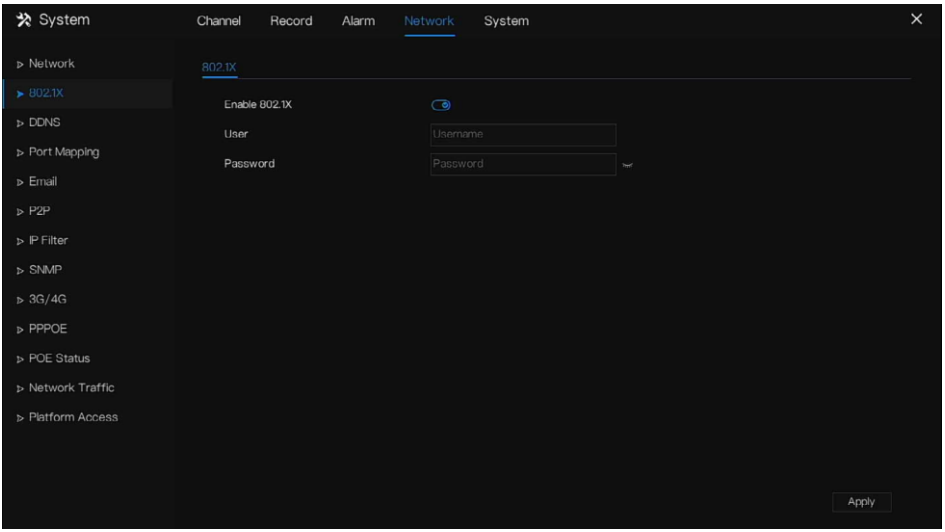
6.6.2 802.1 X

The 802.1X for NVR 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 6-94 802.1 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 NVR needs to input an account to certify.

----End

6.6.3 DDNS

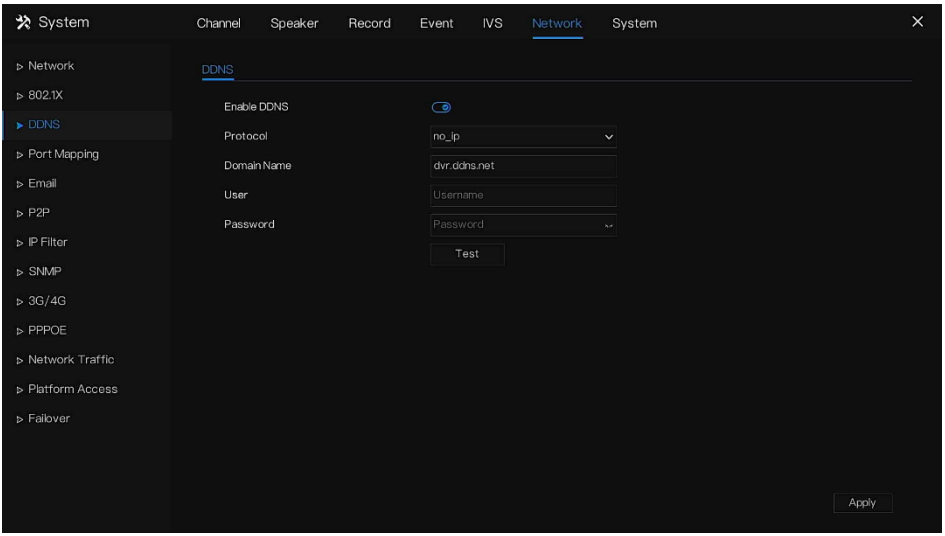
Please make sure to connect the specified camera to the Internet and obtain the user name and password for logging into the dynamic domain name system (DDNS) from the server.

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 6-95.

Figure 6-95 DDNS setting screen



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 NVR via an address that is set in the DDNS settings.

----End

6.6.4 Port Mapping

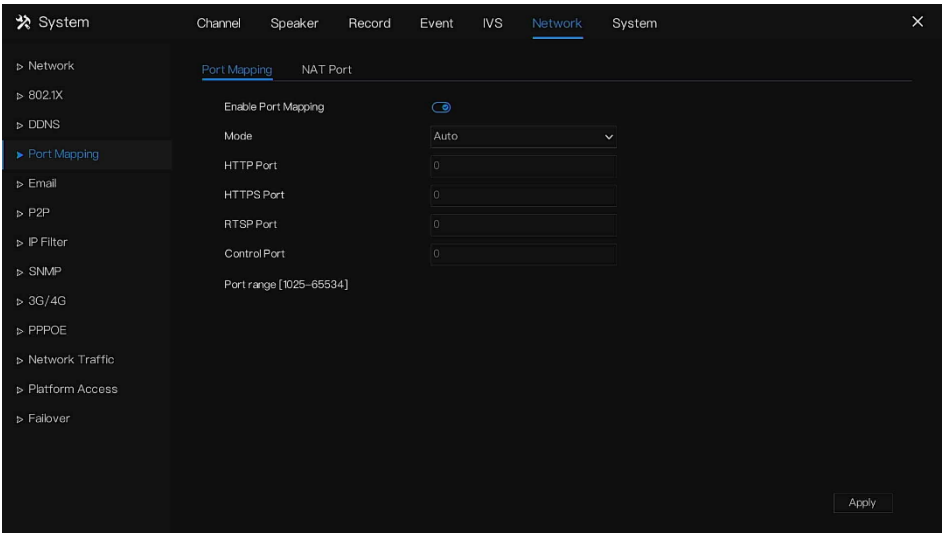
6.6.4.1 Port Mapping

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

Operation Steps

Step 1 Click **Port Mapping** on **Settings > Network** to access the port mapping screen, as shown in Figure 6-96.

Figure 6-96 Port mapping setting screen



Step 2 Select UPnP enable type.

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

Table 6-16 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.

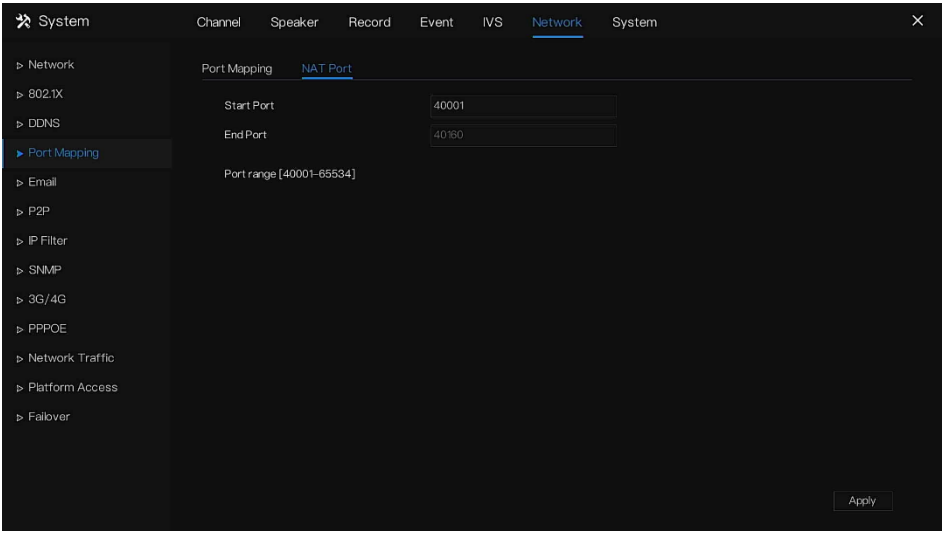
Step 5 Click Apply to save settings.

----End

6.6.4.2 NAT Port

NAT Port (Network Address Translation). Access the NVR channels through the NAT port. Users can set the start port, and it will generate the end port automatically. We will view the NAT port when we access the channel by clicking  icon at the web interface.

Figure 6-97 NAT port



Users can input the IP address and 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

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 6-98.

Step 2 Configure the settings for the email parameters.

Figure 6-98 Email setting screen

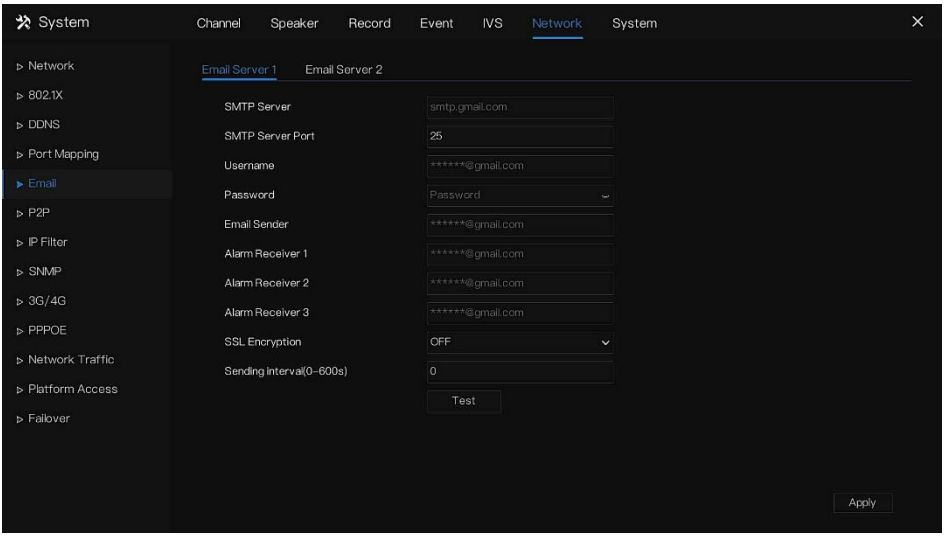


Figure 6-99 Email server 2

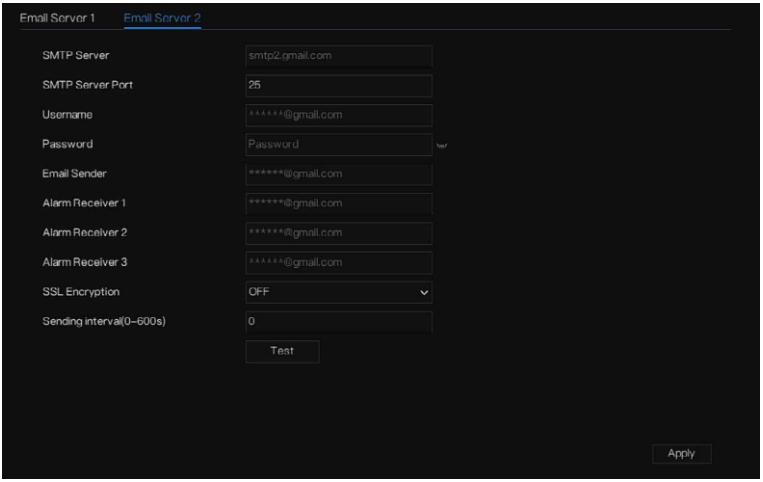


Table 6-17 Email parameters

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

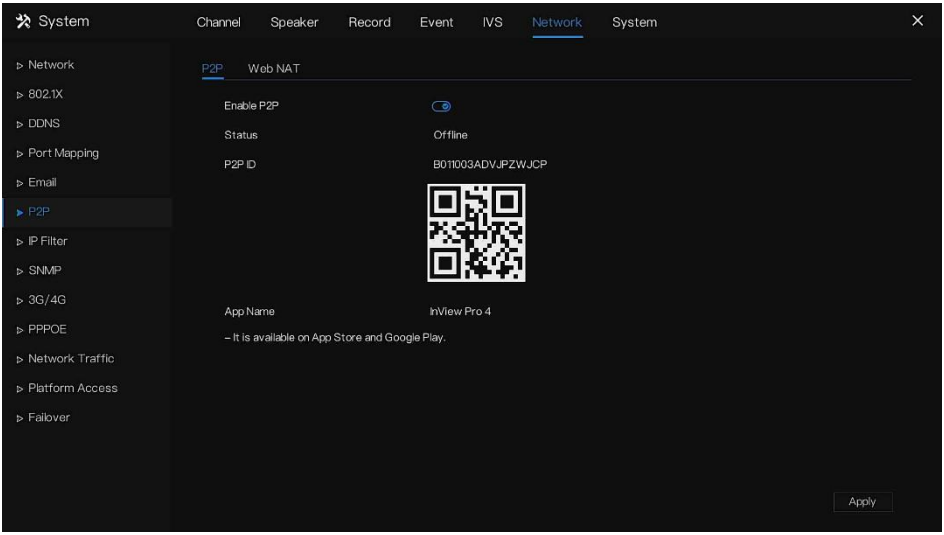
6.6.6.1 P2P

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 6-100.

Figure 6-100 P2P screen



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 **InView Pro4** is installed on a mobile phone, run the APP and scan the QR to add and access the NVR when the device is online.

----End

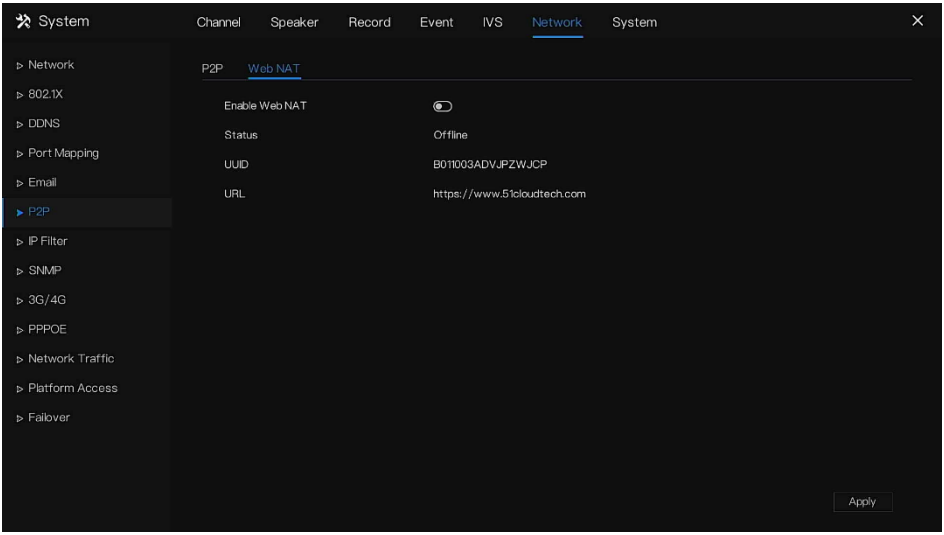
6.6.6.2 Web NAT

This function is used for web access to the NVR.

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 6-101 Web NAT



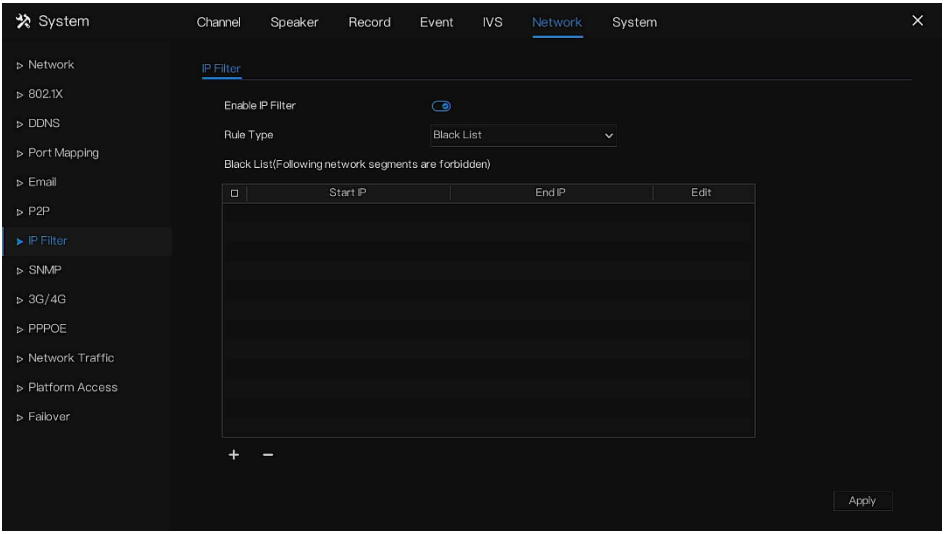
6.6.7 IP Filter

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 6-102.

Figure 6-102 IP Filter setting screen

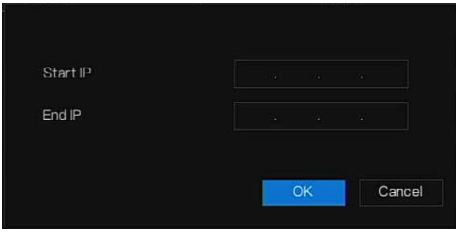


Step 2 Click  next to **IP Filter** to enable the function of IP Filter.

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 6-103.

Figure 6-103 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 6-104.

Figure 6-104 SNMP settings screen

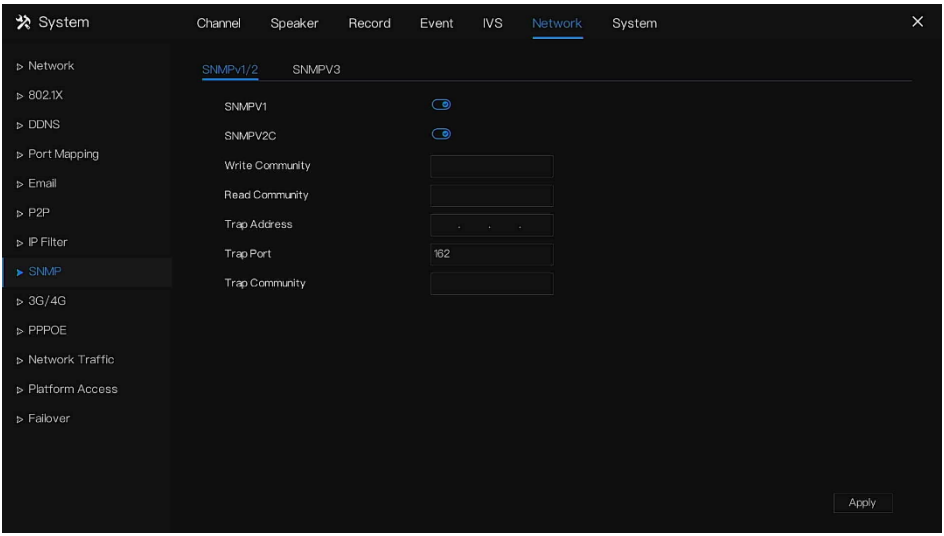
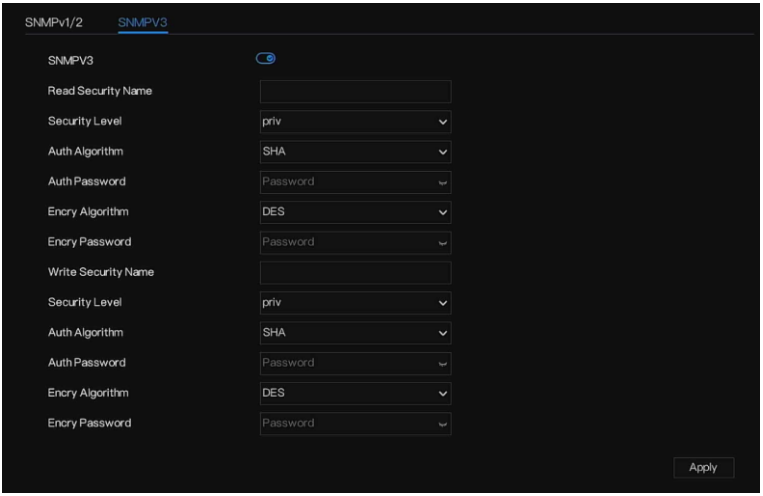


Figure 6-105 SNMPV3



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

	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 6-106.

Figure 6-106 SNMPV 1/2 interface

Table 6-18 SNMP parameters

Step 3 Input the parameters of the protocol.

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

----End

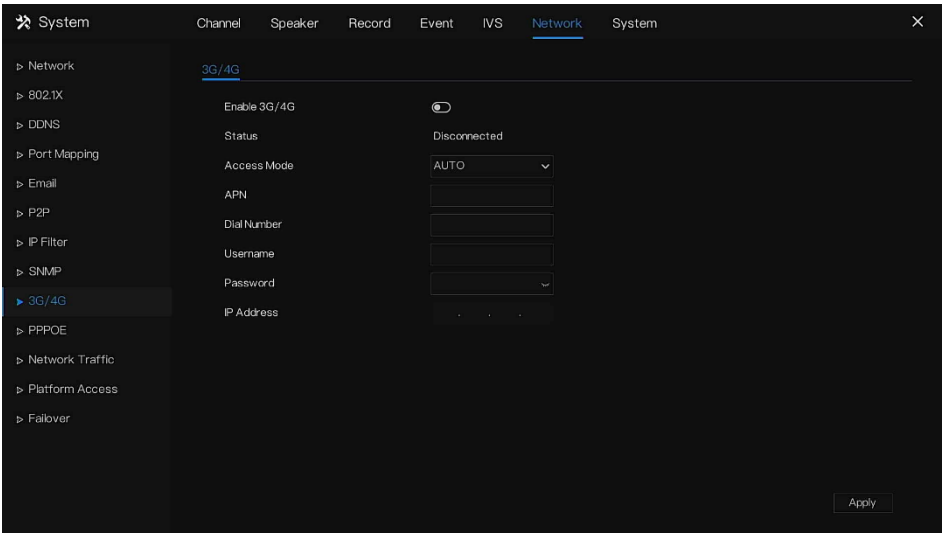
6.6.9 3G/4G

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

Operation Steps

Step 1 Plug the modem into NVR, and enable the 3G/4G function, as shown in Figure 6-107.

Figure 6-107 3G/4G setting screen



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

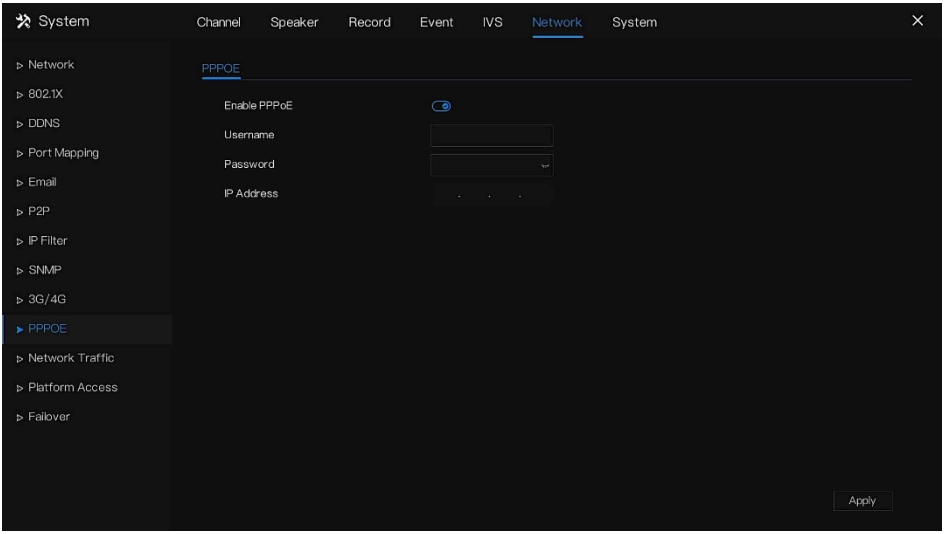
- Modify the access mode of 3G/4G (AUTO, LTE, TD-SCDMA, WCDMA, GSM/GPRS). If you cannot dial within 5 minutes, re-plug the modem.
- Users are familiar with the relevant network (different service provider parameters are different) and modem information before manually switching to other modes; the recommended 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 6-108.

Figure 6-108 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.

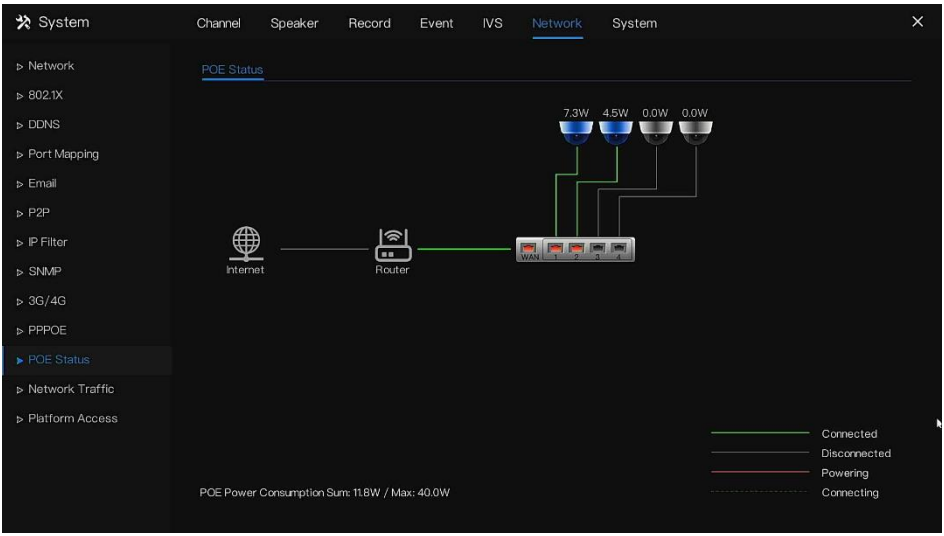
Step 4 Users input the IP to access the NVR web immediately.

----End

6.6.11 POE Status (Only for Some Models)

Users can view the status of POE intuitively, as shown in Figure 6-109.

Figure 6-109 POE status

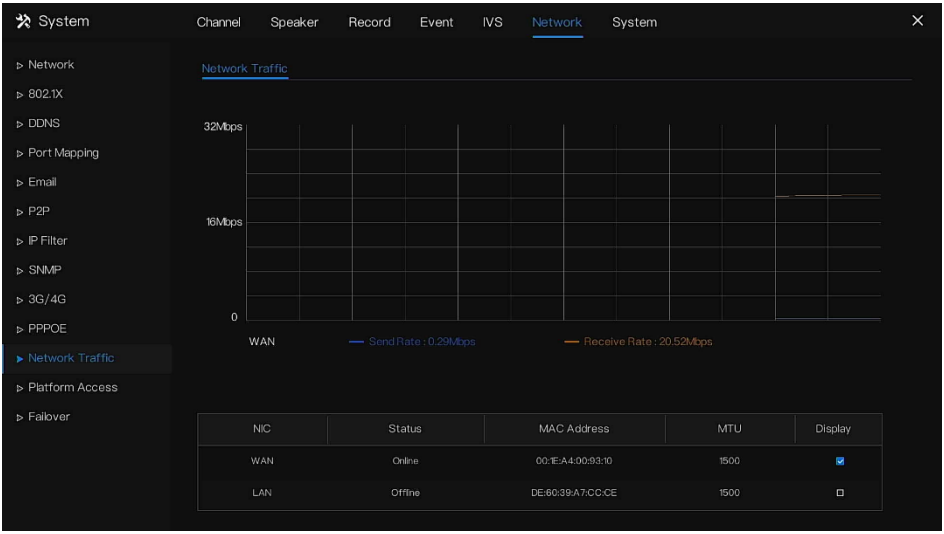


----End

6.6.12 Network Traffic

Users can view the network traffic immediately, as shown in Figure 6-110

Figure 6-110 Network traffic



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

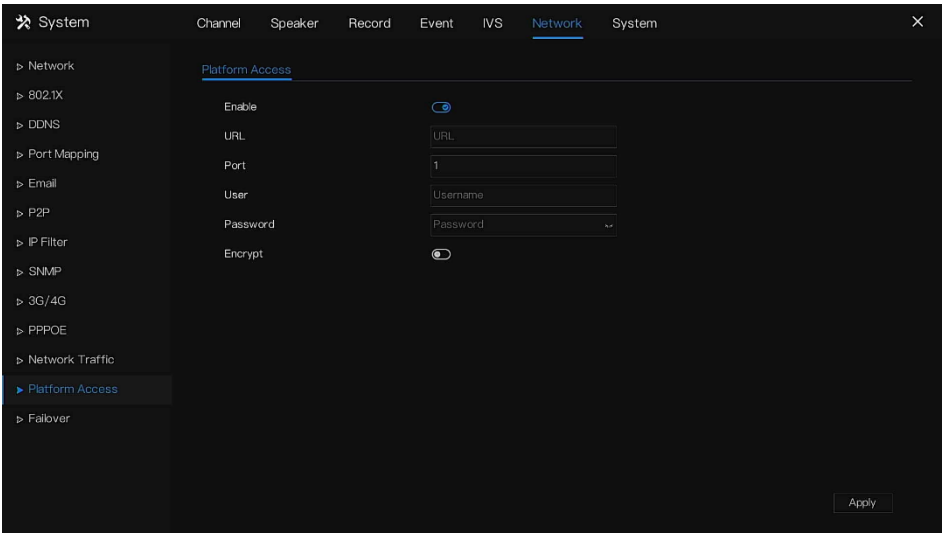
----End

6.6.13 Platform Access

If the NVR and platform system are not on the same local network, ensure the NVR 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 NVR 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 6-111

Figure 6-111 Platform Access page



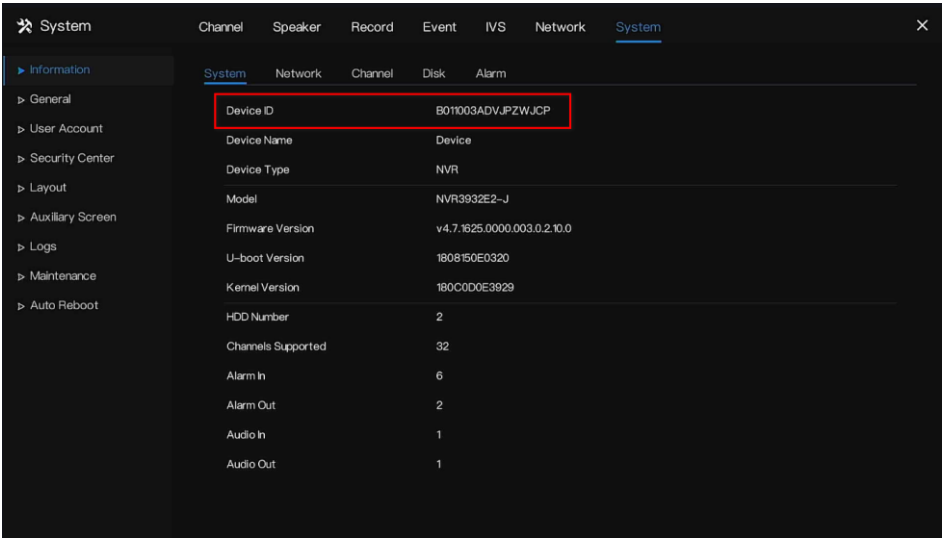
Step 2 Input the parameters. The URL and port are the platform server IP address and port.

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

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

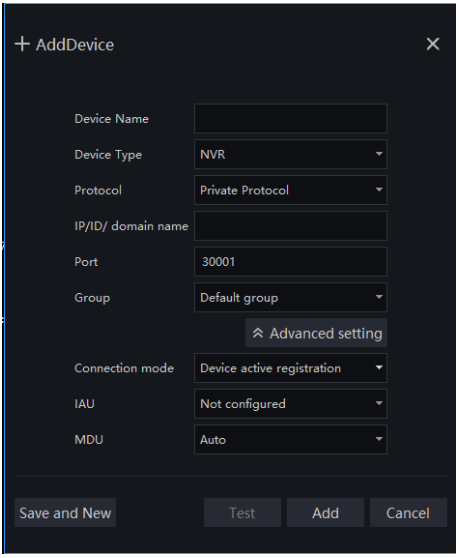
1: IP/ID/Domain name is Device ID of NVR.

Figure 6-112 IP/ID/Domain



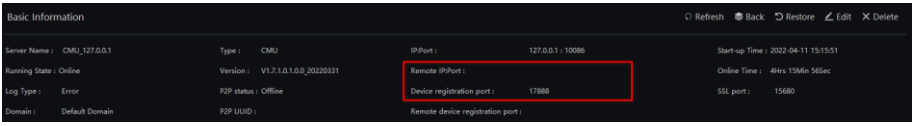
2: The connection mode should be chosen for **Device active registration**.

Figure 6-113 Connect NVR to platform



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

Figure 6-114 URL address/port



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.

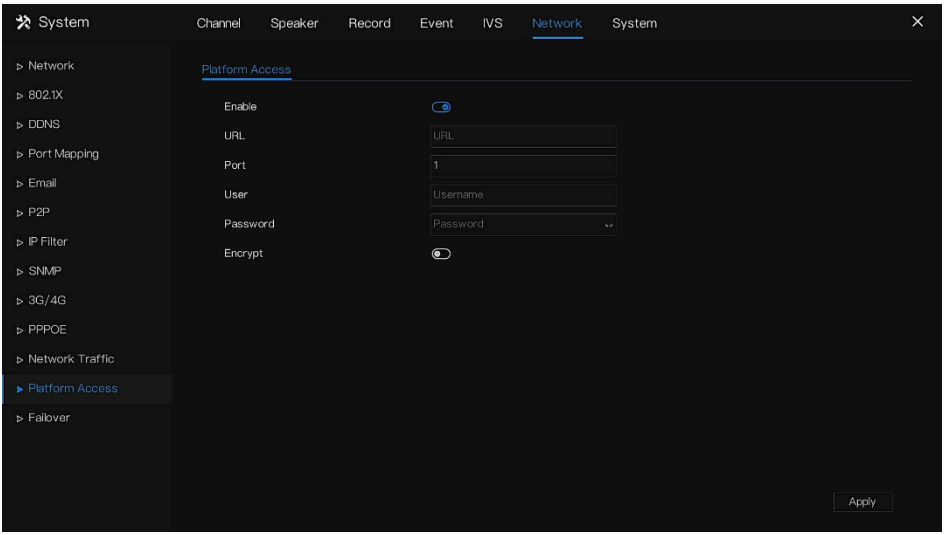
----End

6.6.14 Failover

If users want to keep all recordings working normally, set the NVR to act as redundant NVR, when the primary NVRs are broken down, the redundant can keep working as failover.

Step 1 Choose **Configuration > Network Service > Failover,** The **Failover** page is displayed, as shown in Figure 6-115.

Figure 6-115 Failover



Step 2 Choose the Primary mode and enable primary NVR to unfold for setting the redundant NVR parameters (WAN address, port, username, password). If the connect status is Disconnected / Connection timed out / Username or password error/Redundant NVR does not support failover.

Figure 6-116 Redundant mode

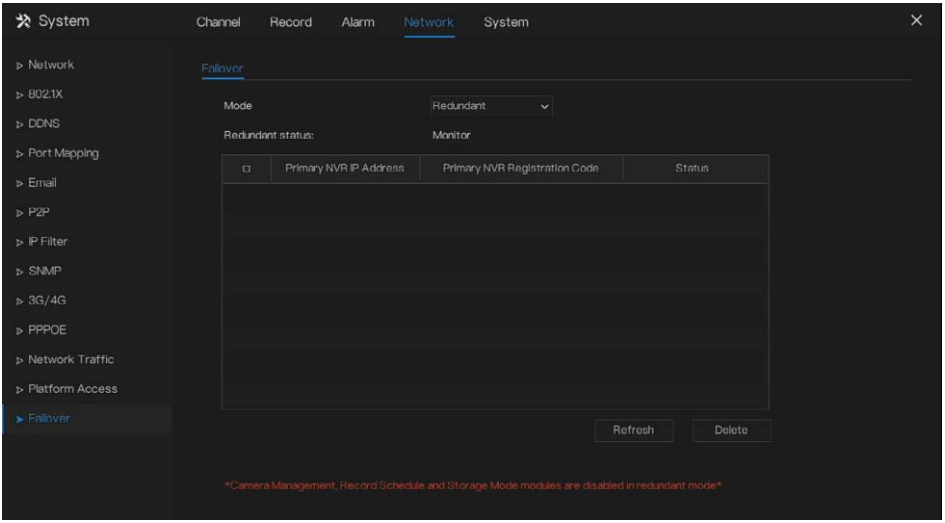


Table 6-19 Primary NVR parameters

Parameter	Description
Enable Primary NVR	Enable to connect to the redundant NVR for security.
Redundant NVR WAN address	The network information of redundant NVR. The channel and disk numbers of redundant NVR cannot be less than that of primary NVR.
Redundant NVR port	
Redundant NVR user	
Redundant NVR password	
Redundant NVR serial No	
Connect status	Disconnected / Connection timed out / Username or password error/Redundant NVR does not support failover.

NOTE

The channel and disk numbers of redundant NVR cannot be less than that of primary NVR.

The time of the primary NVR and redundant NVR must be consistent.

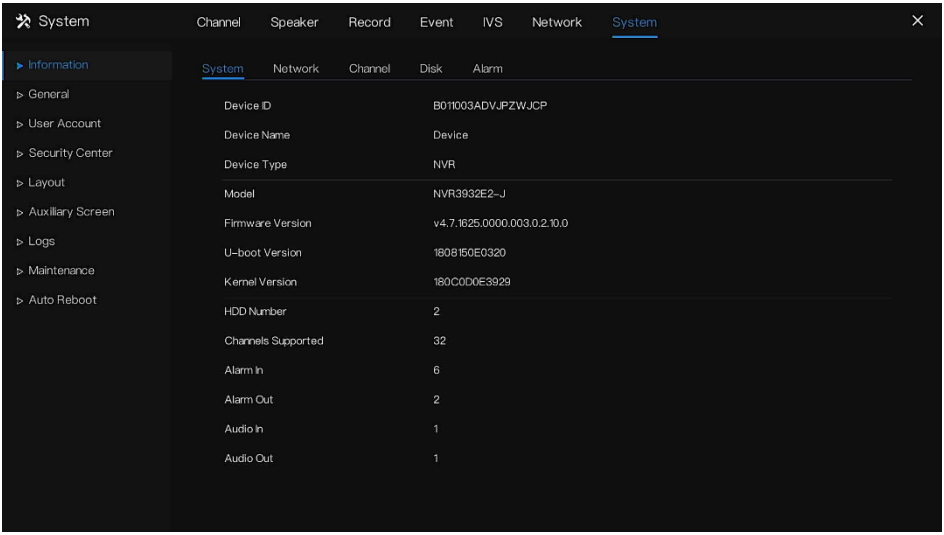
6.7 System Management

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 6-117.

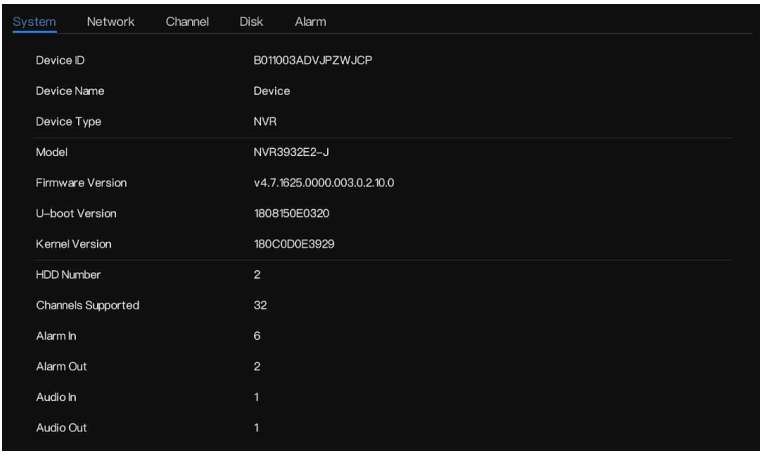
Figure 6-117 System setting screen



6.7.1 Information

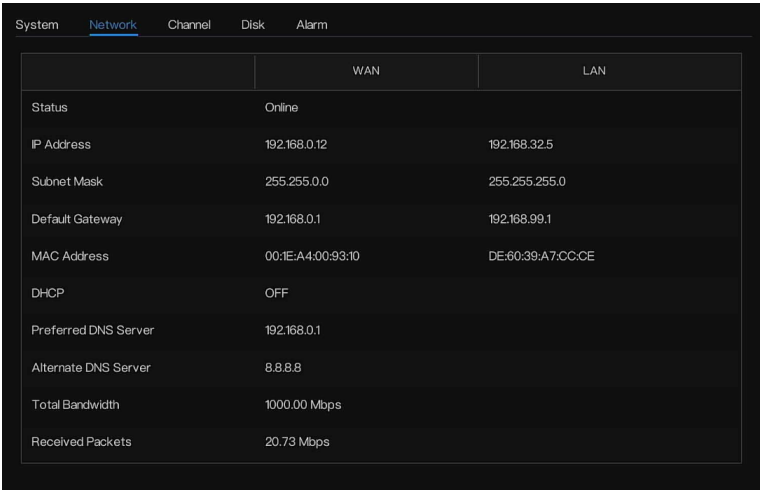
View the device ID, device name, device type, model, firmware version, kernel version, face detection version, HDD volume, channel support, alarm in, alarm out, audio in, and audio out in the **Information** screen, as shown in Figure 6-118.

Figure 6-118 Information-system interface



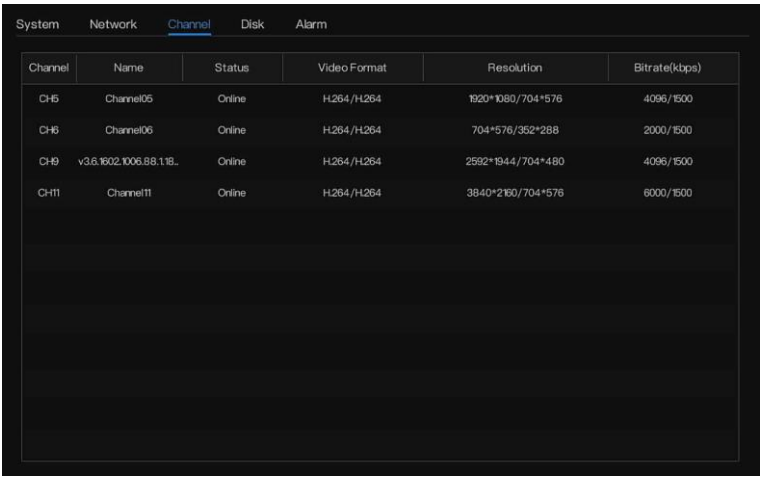
Network: status, IP address, subnet mask, default gateway, MAC address, DHCP, preferred DNS server, Alternate DNS server, total bandwidth, received packets, and so on, as shown in Figure 6-119.

Figure 6-119 Information-network interface



Channel: channel, name, status, video format, resolution, bitrate (kbps), and so on, as shown in Figure 6-120.

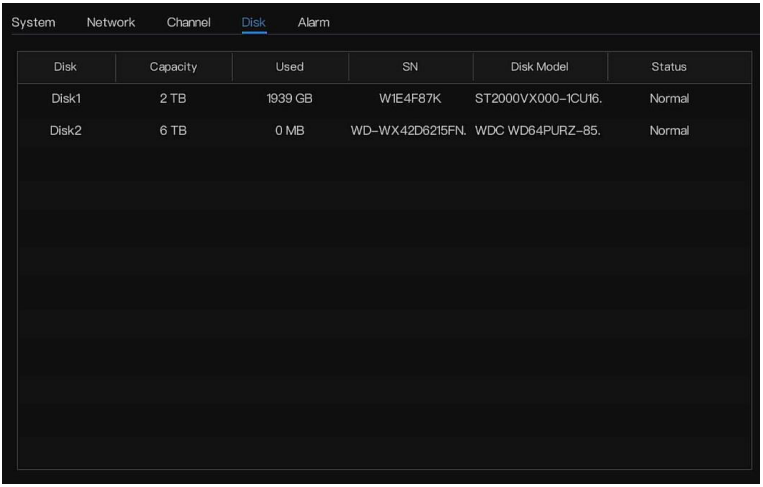
Figure 6-120 Information-channel interface



Disk: disk name, capacity, used, SN, disk model, status, and so on, as shown in Figure 6-121

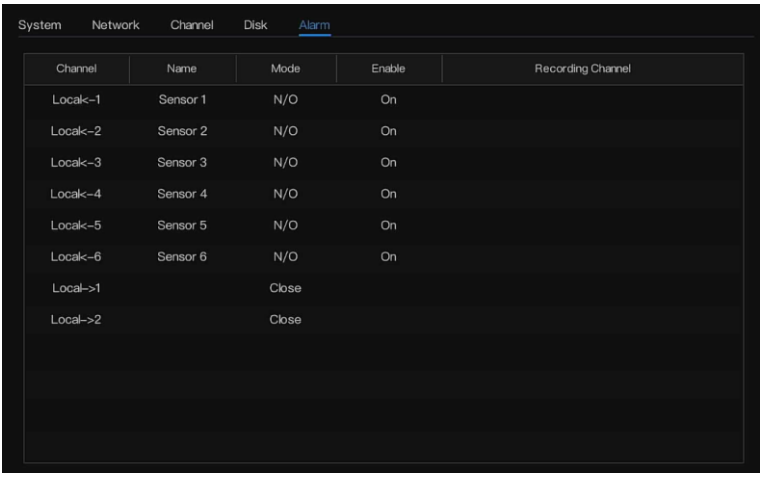
.

Figure 6-121 Information-disk interface



Alarm: channel, name, mode, enable, recording channel, and so on, as shown in Figure 6-122.

Figure 6-122 Information-alarm interface



----End

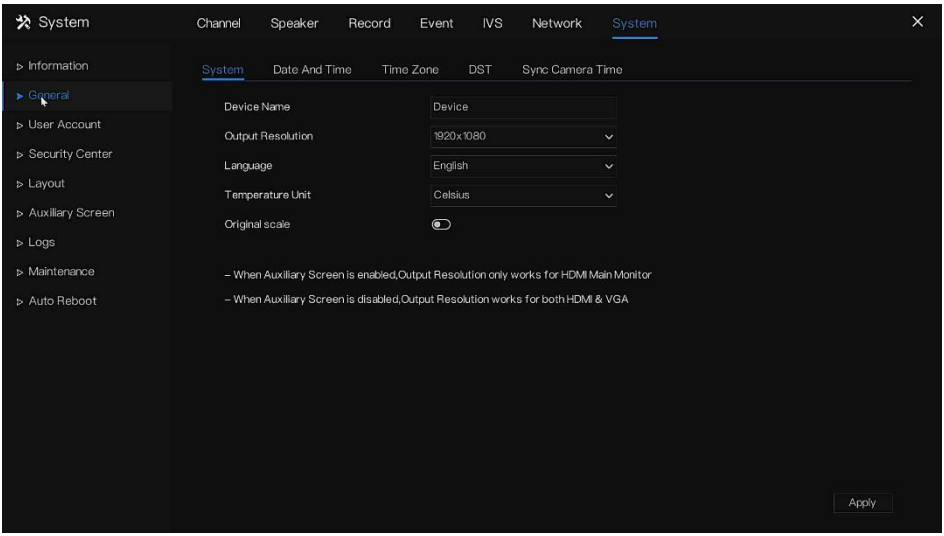
6.7.2 General

6.7.2.1 System

Operation Steps

Step 1 Click **General** on **Settings > System** to access the system screen, as shown in Figure 6-123.

Figure 6-123 system setting screen



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.

Step 6 Enable Original scale. The play video interface will display video with the original aspect ratio. Disable Original Scale and the play video interface will display video with a 16:9 aspect ratio.

NOTE

The NVR 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.

Figure 6-124 Disable Original scale

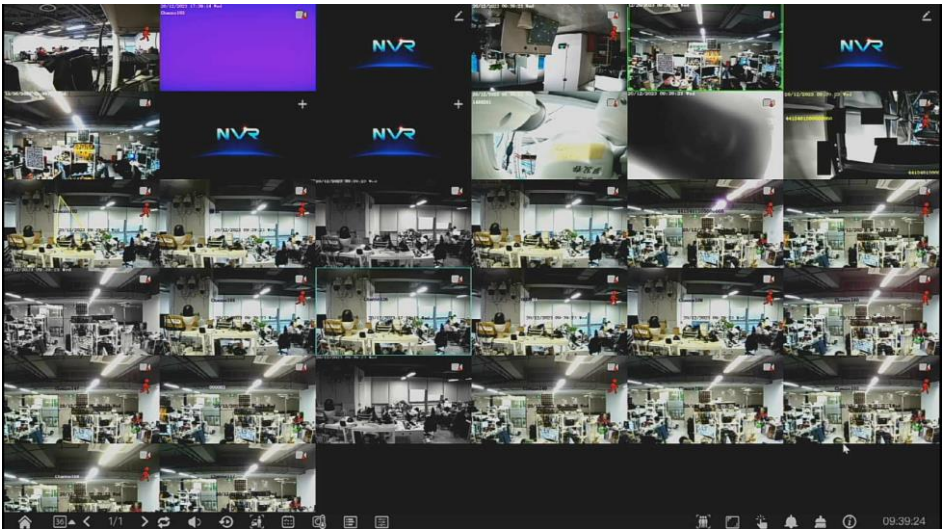


Figure 6-125 Enable Original scale

Step 7 Click Apply to save settings.

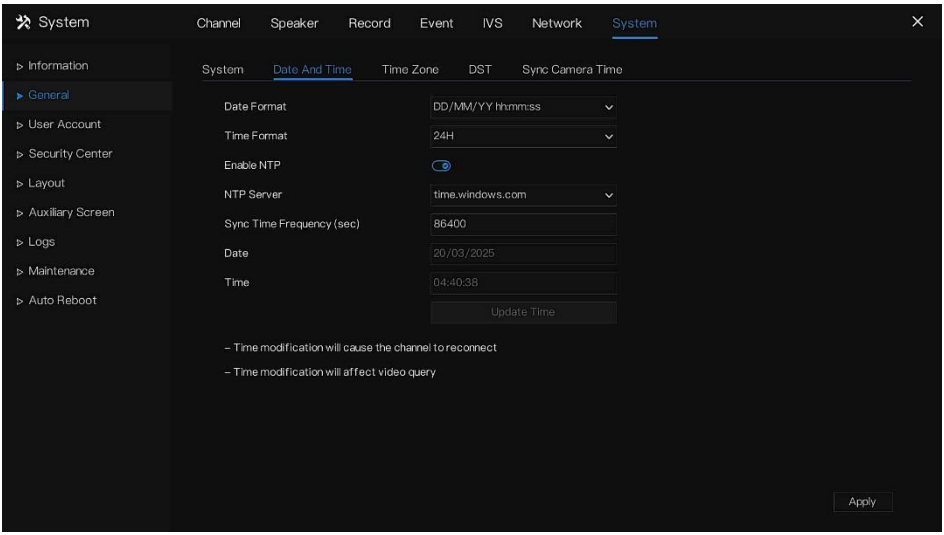
----End

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 6-126.

Figure 6-126 Date and Time setting screen



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 6-20 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.
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.

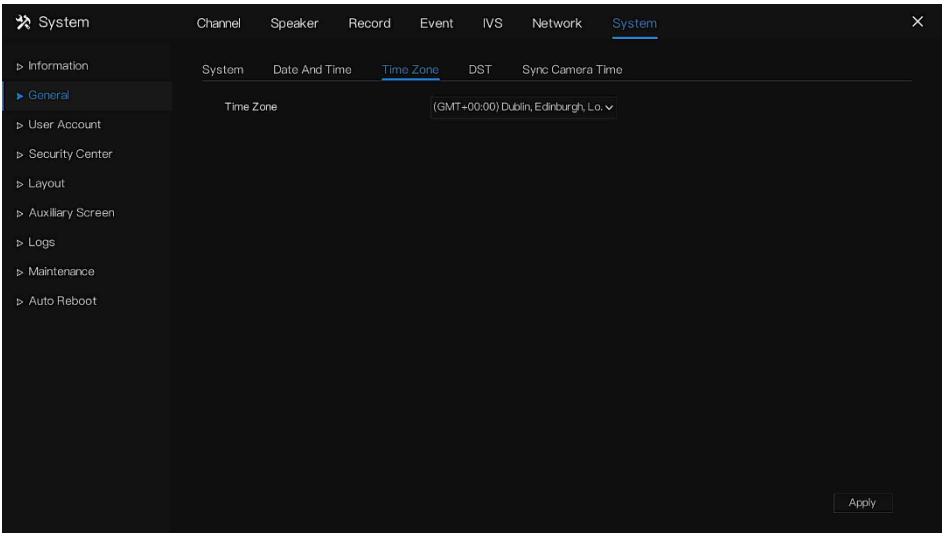
----End

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 6-127.

Figure 6-127 Time zone setting screen



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

Step 3 Click Apply to save settings.

----End

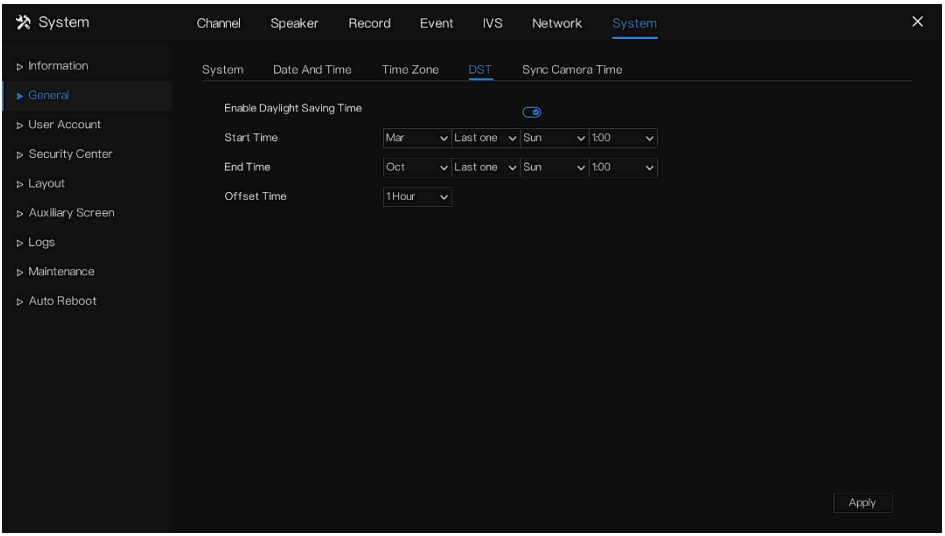
6.7.2.4 DST

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 6-128.

Figure 6-128 DST setting screen



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.

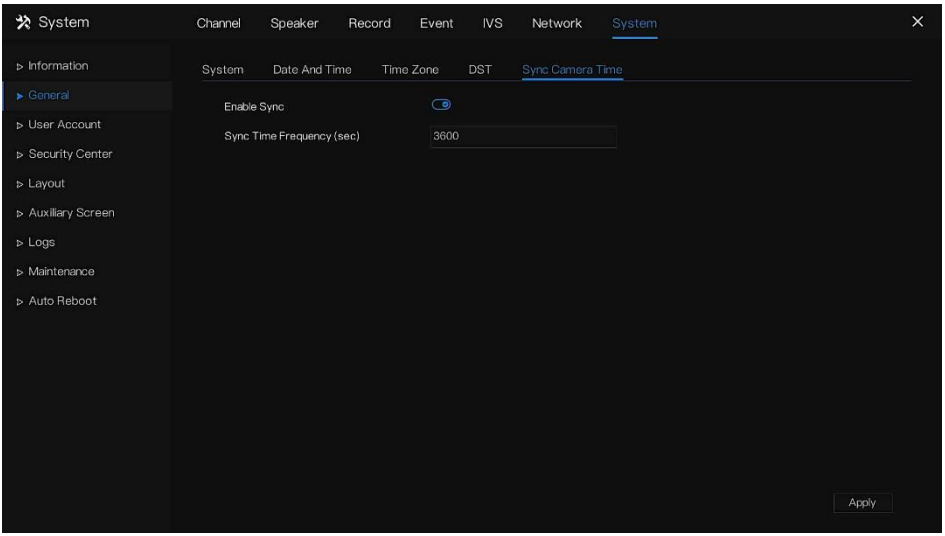
Step 4 Click  to save settings.

----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 6-129 Sync camera Time



----End

6.7.3 User Account

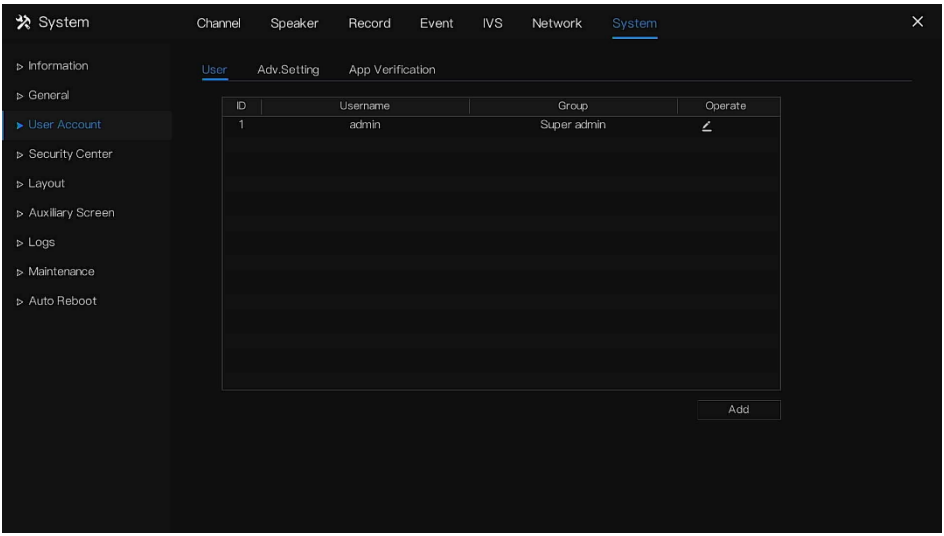
Add, modify, and delete a user and privilege in the user screen. The admin user can dispose of privileges to different users.

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 6-130.

Figure 6-130 User management screen

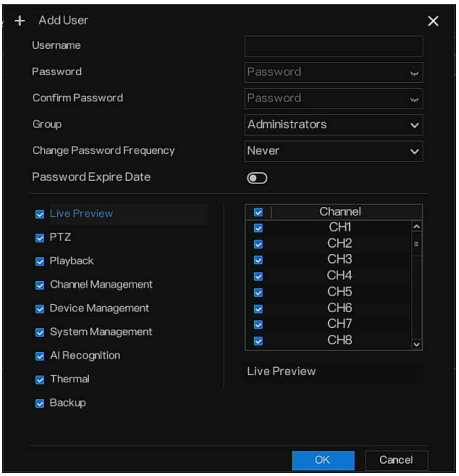


Step 2 Add or delete a user.

- Add a user

  Click **Add** and the **Add User** dialog box appears, as shown in Figure 6-131.

  Figure 6-131 Add user screen



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

Table 6-21 Add interface parameters

Parameter	Description
User Name	Enter a username and password for the account.
Password	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
Confirm password	Re-enter the password.
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.

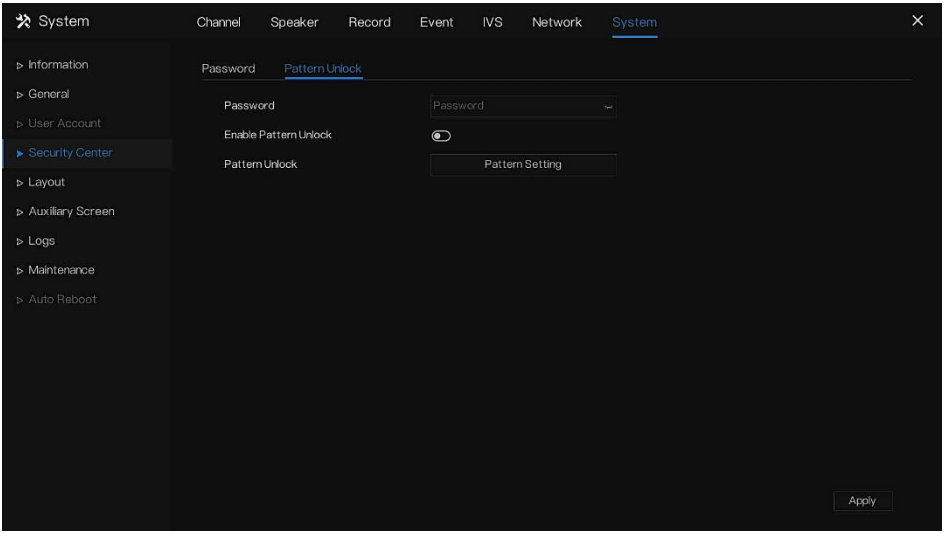
NOTE

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 6-132 General user set pattern to unlock.



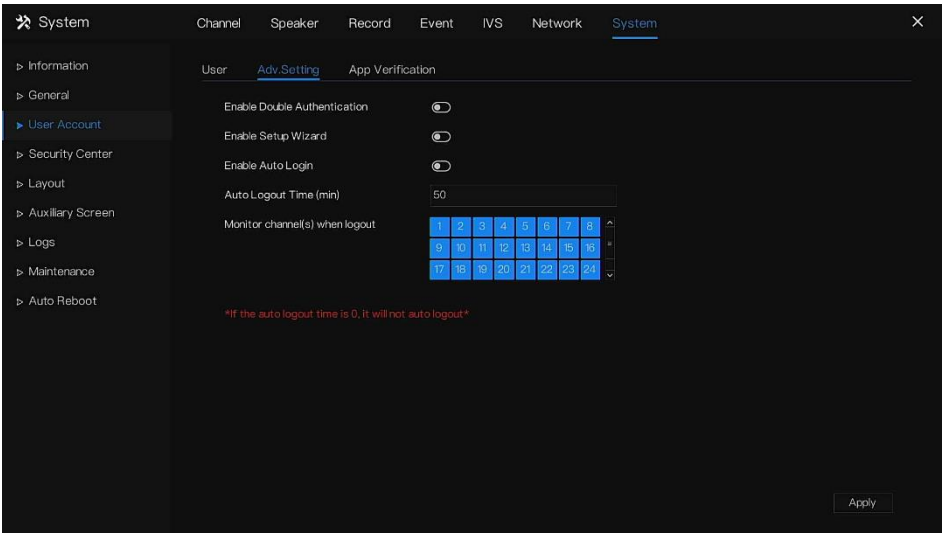
-----End

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 6-133.

Figure 6-133 Advance setting screen



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.

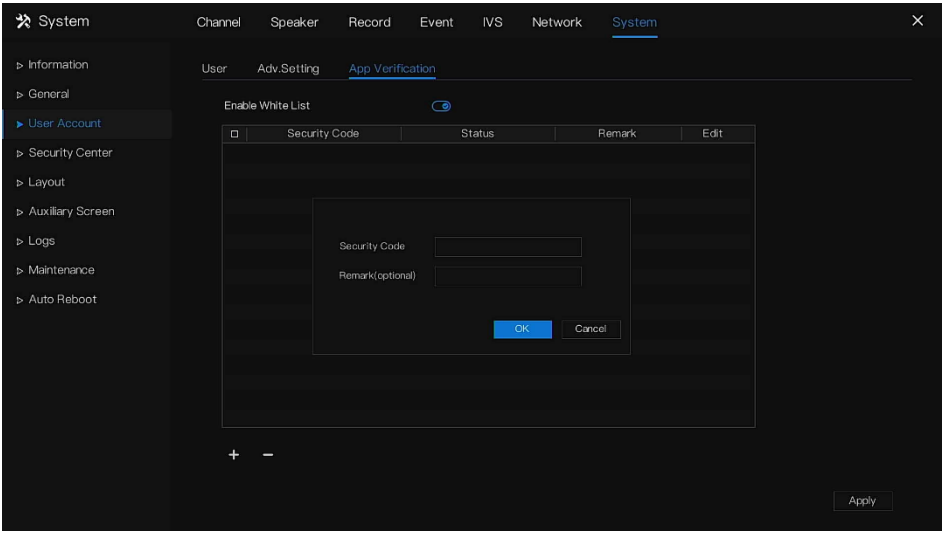
-----End

6.7.3.3 App Verification

Add the digital number to the whitelist. When logging in to the mobile app to manage the NVR, enter a series of numbers in the whitelist for testing and verifying to ensure security.

Click App Verification on **Settings > System** > **User Account to access the** App Verification screen, as shown in Figure 6-134.

Figure 6-134 App verification



Up to 20 groups of security codes can be added and notes can be modified for them.

Tick the numbers, and click "-" to delete the numbers.

Click Apply to save the setting.

----End

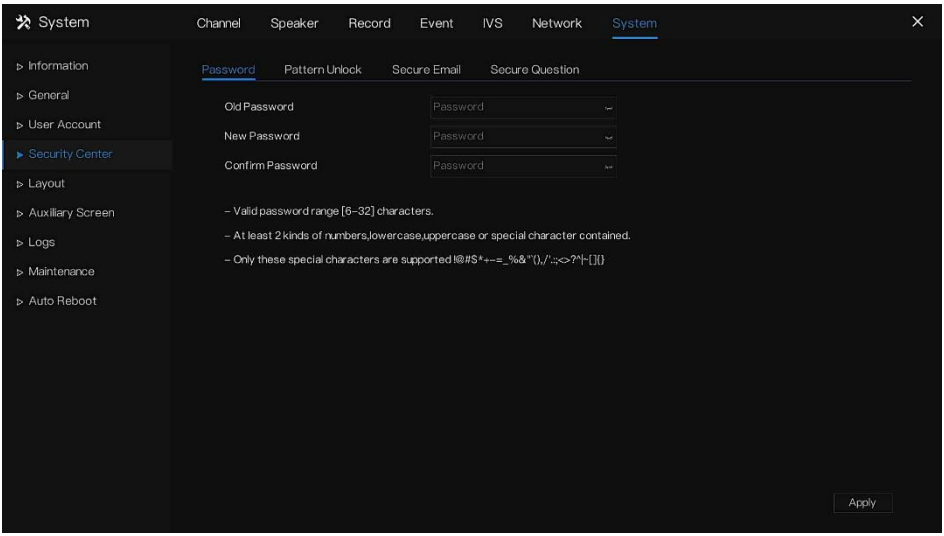
6.7.4 Security Center

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 6-135.

Figure 6-135 Password modification screen



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

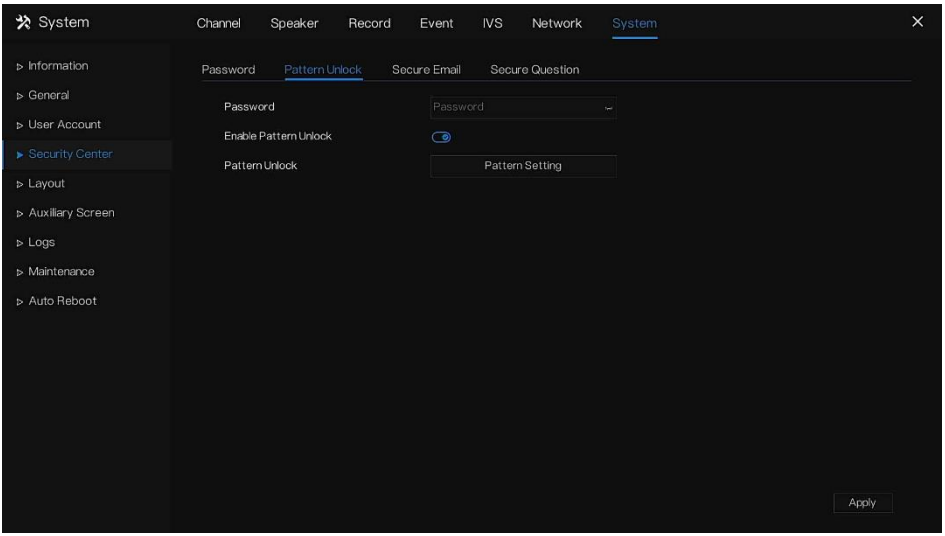
NOTE

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 6-136.

Figure 6-136 Pattern unlock screen



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.

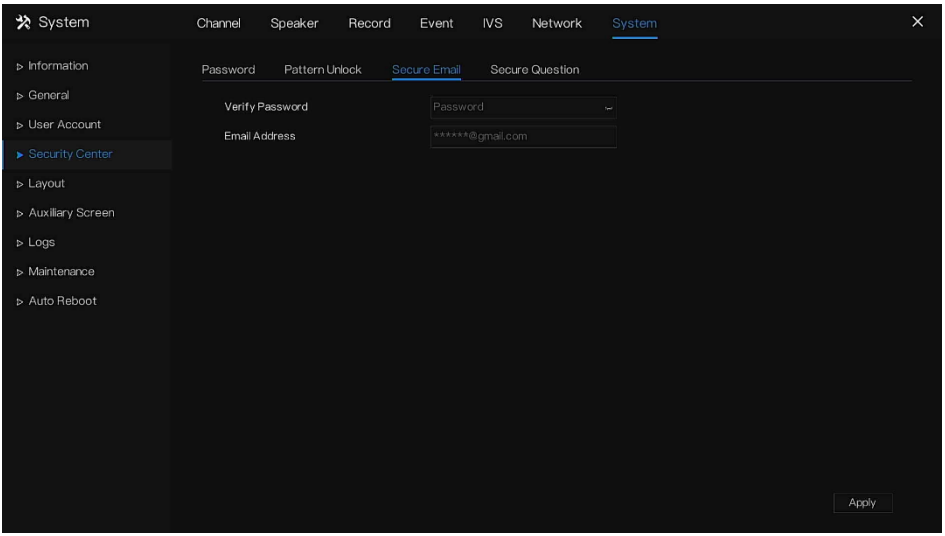
Step 5 Click OK to save the pattern unlock.

----End

6.7.4.3 Secure Email

Set the email to receive the verification code to create a new password, as shown in Figure 6-137.

Figure 6-137 Secure Email



Step 1 Input the password of NVR.

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

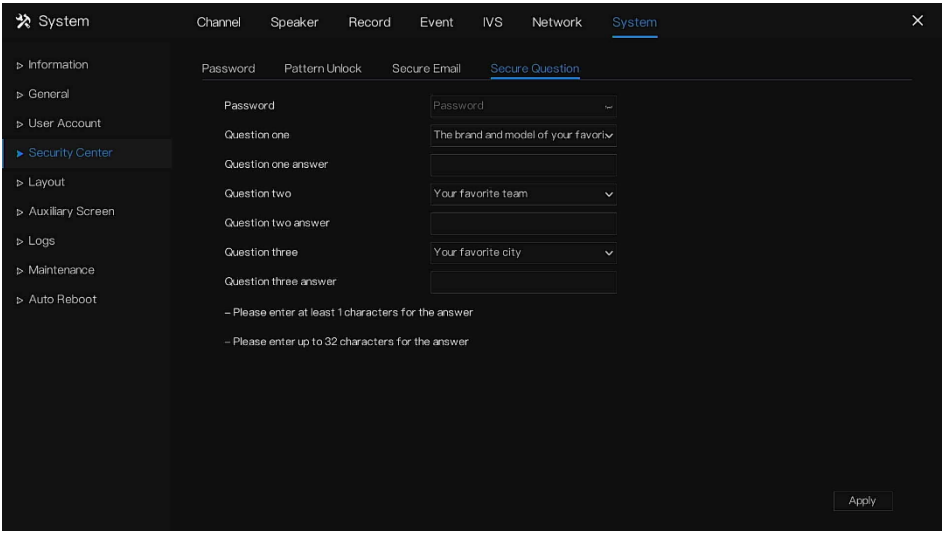
Step 3 Click Apply to save the setting.

----End

6.7.4.4 Secure Question

Set the questions to create a new password, as shown in Figure 6-137.

Figure 6-138 Secure question



Step 1 Input the password of NVR.

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

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

----End

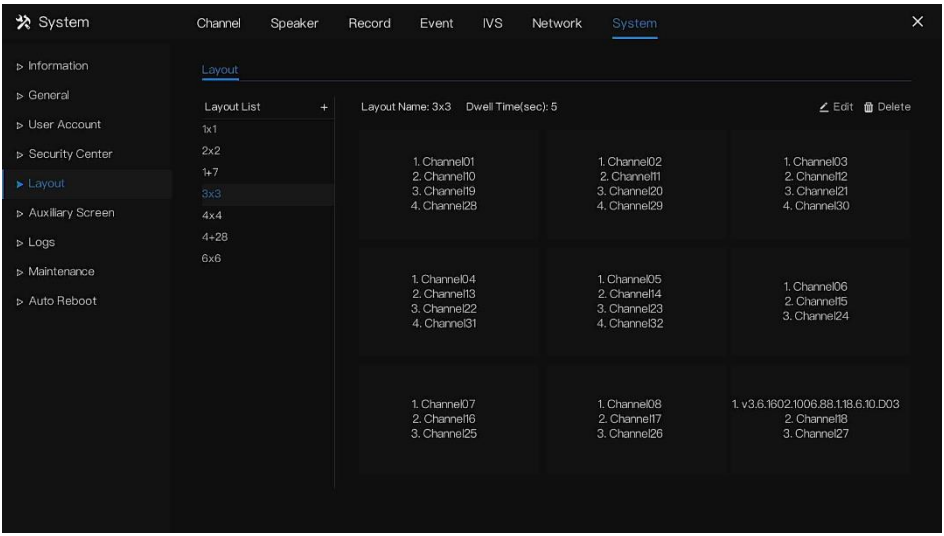
6.7.5 Layout

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

Operation Steps

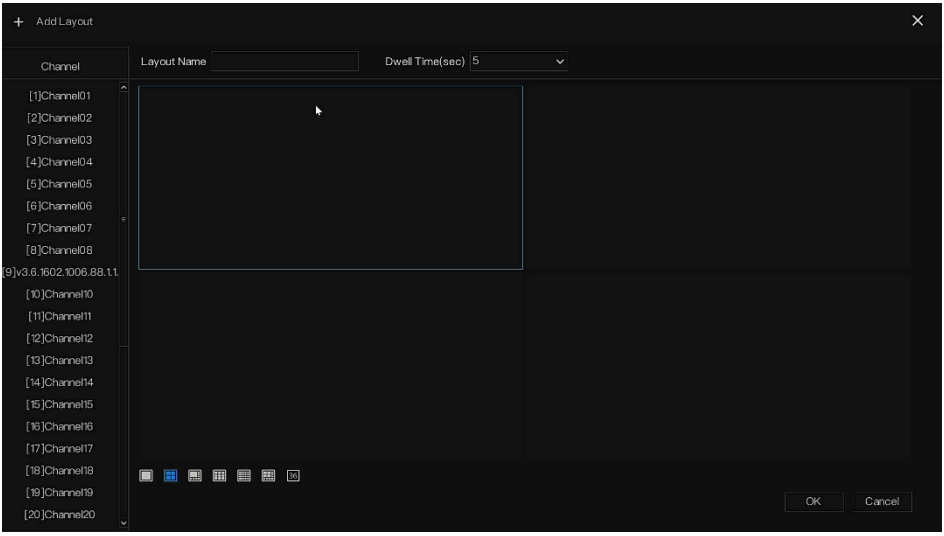
Step 1 Click **Layout** in the Setting System or menu of the system management screen and choose **Layout** to access the display screen, as shown in Figure 6-139.

Figure 6-139 Auto Sequence screen



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

Figure 6-140 Add a new layout

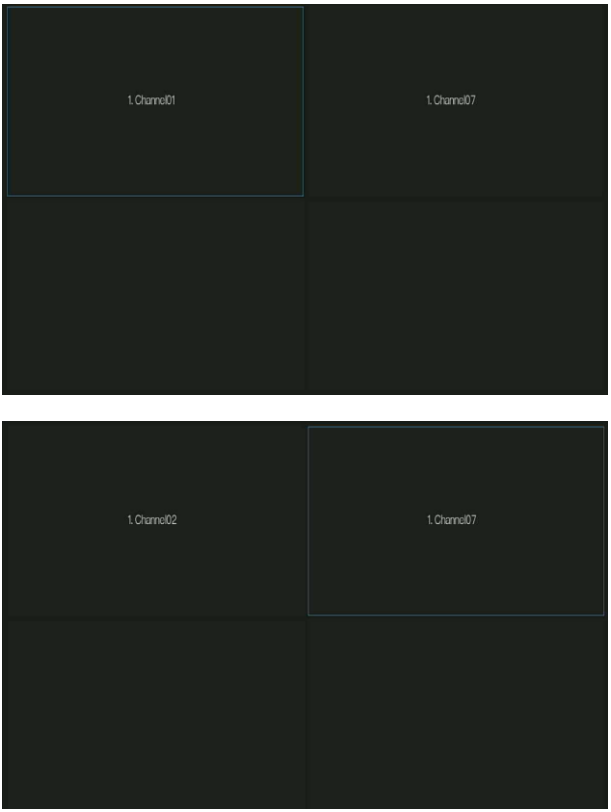


Step 3 Input the layout name, and select dwell time from the **SEQ** Dwell time drop-down list(the display screen will loop play the real-time video according to setting time).

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 6-141 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

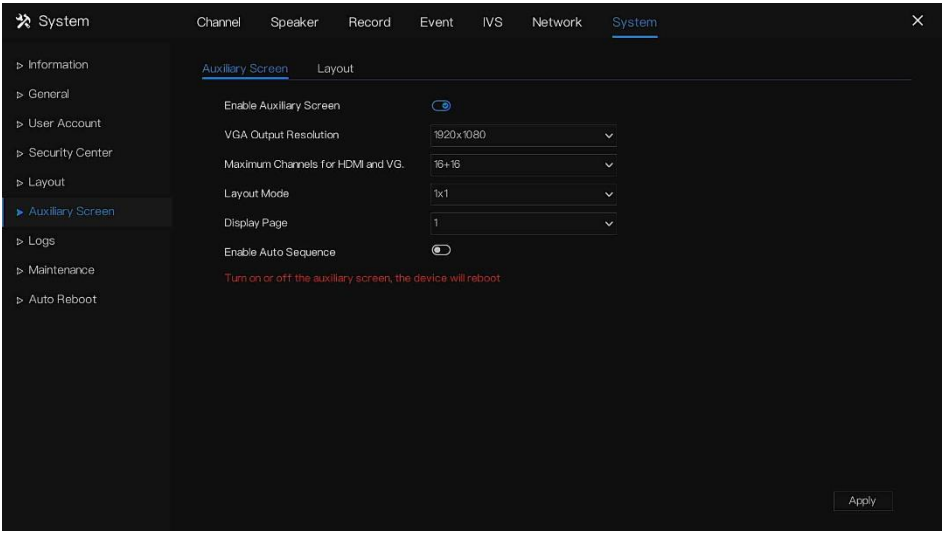
This function can only be used for devices with 8 or more channels. The main screen is connected by HDMI (HD-OUT 2), and the auxiliary screen is connected by VGA.

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 6-142

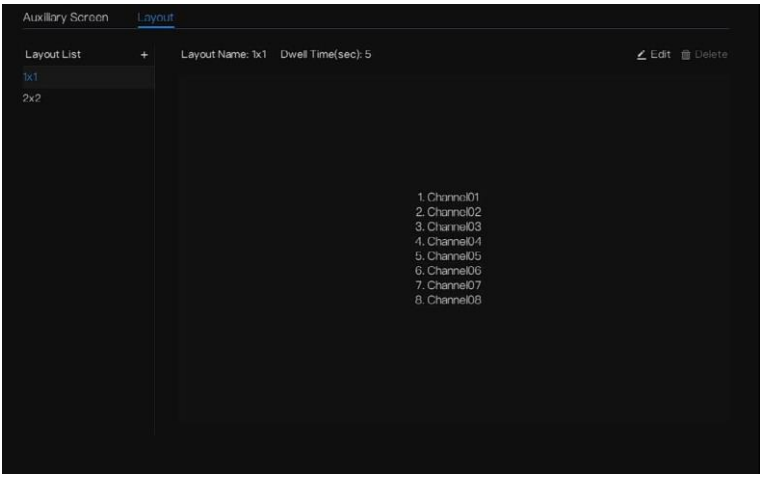
Figure 6-142 Auxiliary screen



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 6-143.

Figure 6-143 The auto sequence of auxiliary screen



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

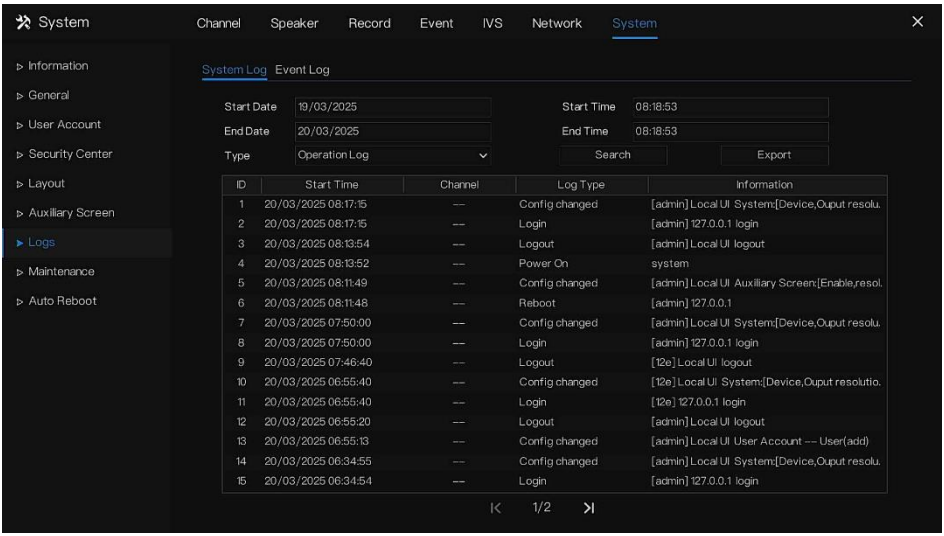
The users should keep the power on when the system parameters are modified. All modifications will be saved for three minutes; otherwise, the setting may fail to be applied.

The operation logs and the alarm logs will be saved to the hard disk when the hard disks are installed, otherwise; the NVR 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 6-144.

Figure 6-144 Log screen



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.

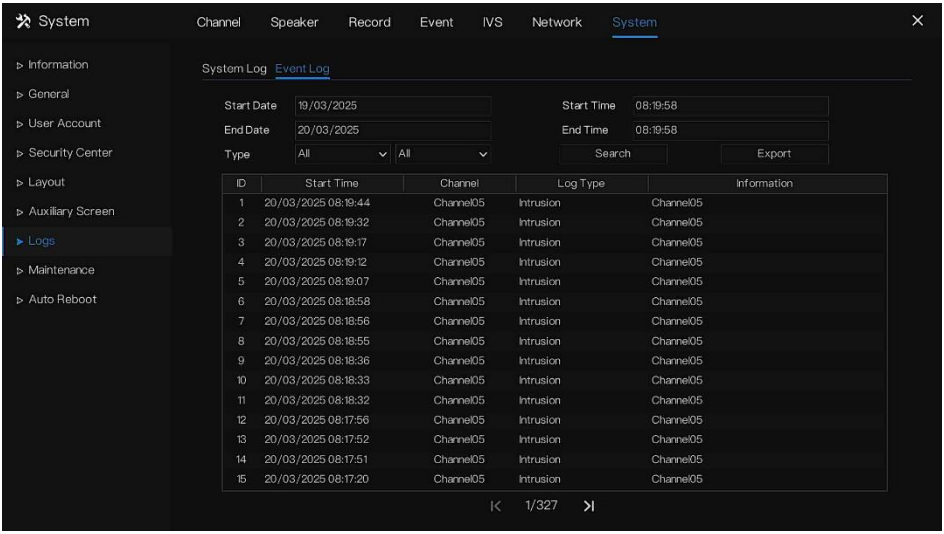
Step 6 The logs can be saved to a flash disk and hard disk at the same time, the newest logs are saved to a flash disk, and the old logs will be transferred to a hard disk.

----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 6-145 Event Log

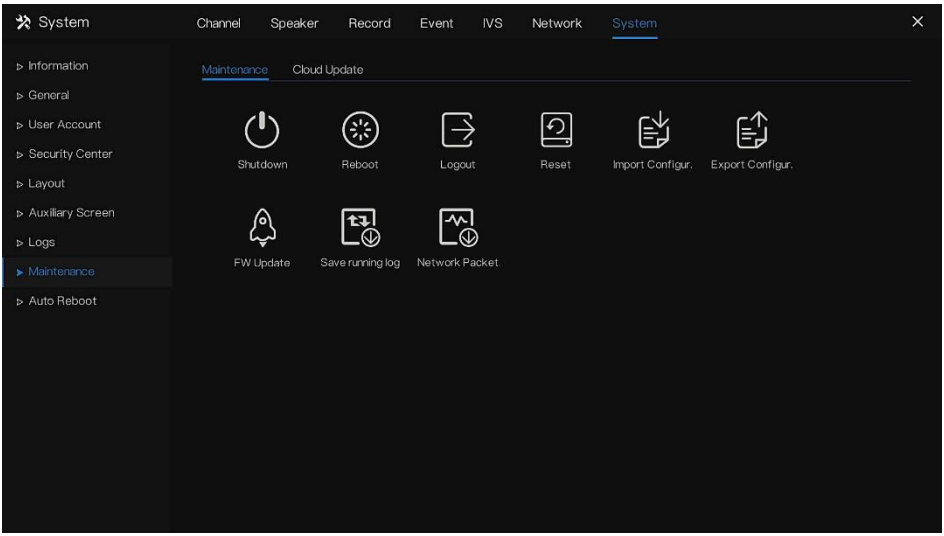


6.7.8 Maintenance

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 6-146.

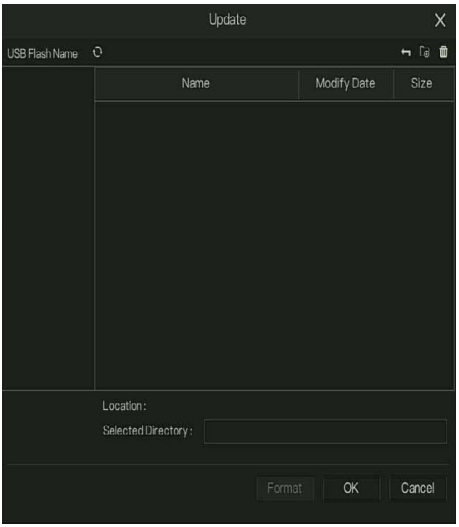
Figure 6-146 Maintenance screen



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

Step 3 Click FW Update to update the firmware.

Figure 6-147 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 NVR 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 NVR 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.

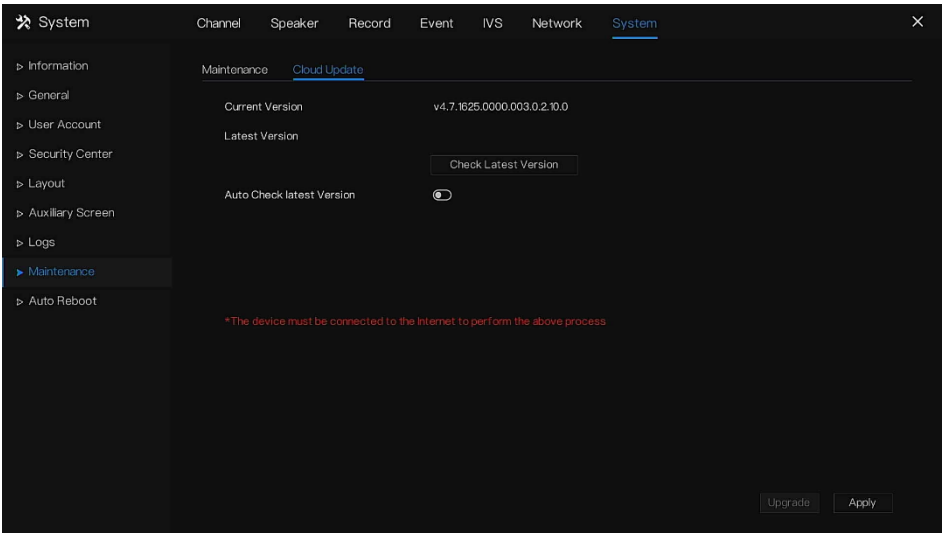
Save running log: In the U disk, save the running log.

----End

6.7.8.2 Cloud Update

When the NVR is connected to the Internet, users can update the software through the Internet. Click **Check Latest Version** to check the latest one, then update. You can also enable auto-check, and the device will check every week.

Figure 6-148 Cloud update



NOTE

The device must be connected to the Internet to perform the above process.

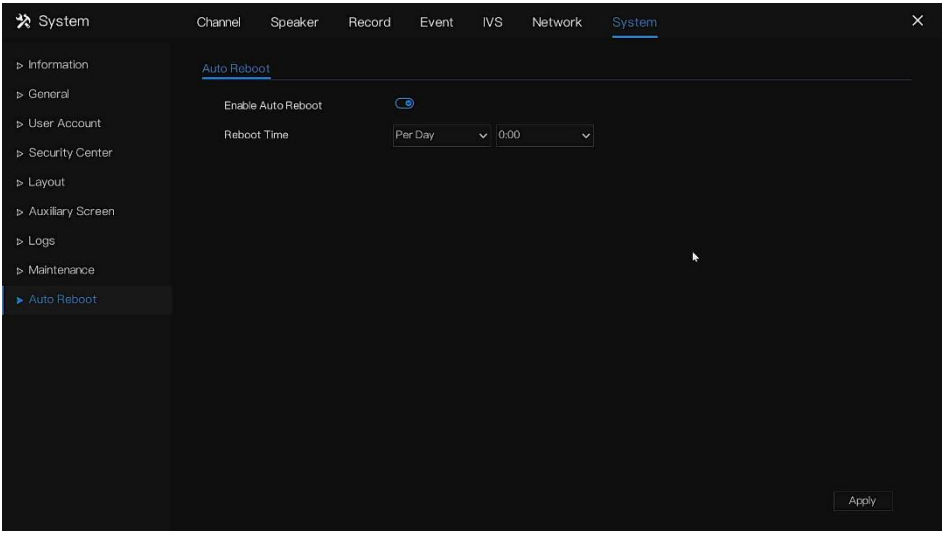
----End

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 6-149.

Figure 6-149 Auto reboot screen



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

.

Step 3 Reboot the NVR per day, week, or month.

Step 4 Select the reboot time from the drop-down list. The NVR 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.

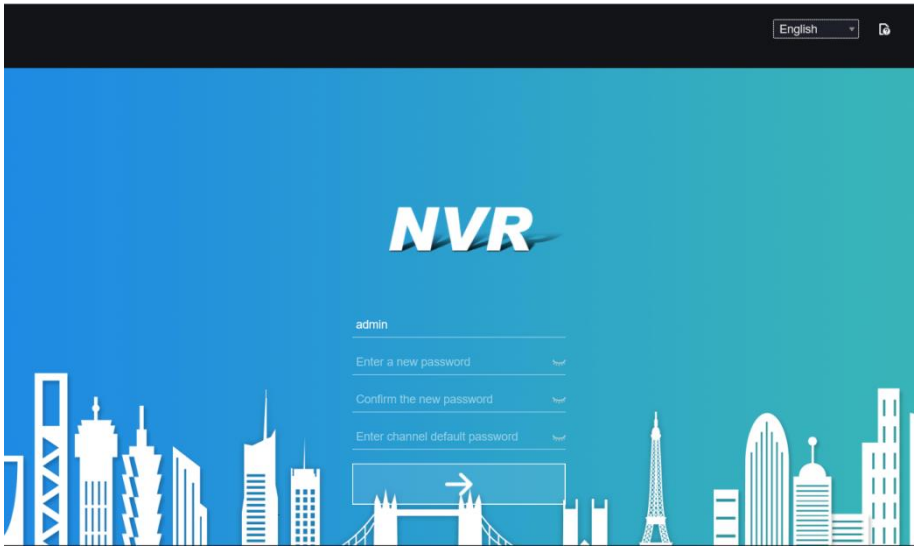
The functions of the web interface are the same as those of the UI system. All functions can be referred to in Chapter 6, UI System Setting.

7.1 Activation

Open the Chrome browser, enter the IP address of the NVR (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

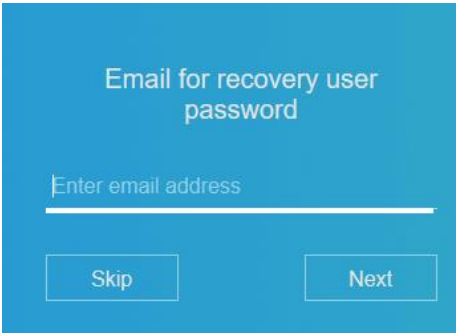


Step 1 Set the password and confirm the password.

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



Step 4 Set the question to recover the password.

Figure 7-3 Question

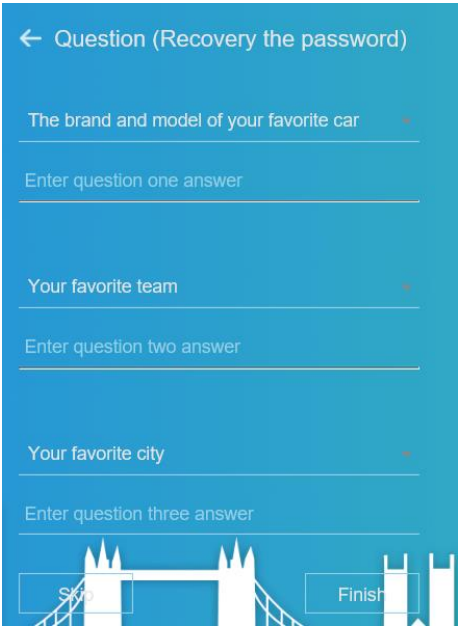
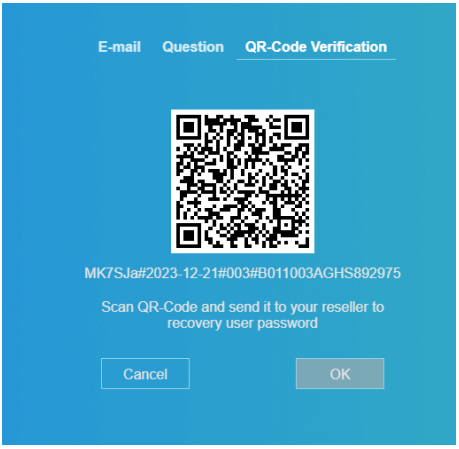


Figure 7-4 QR recovery password



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.

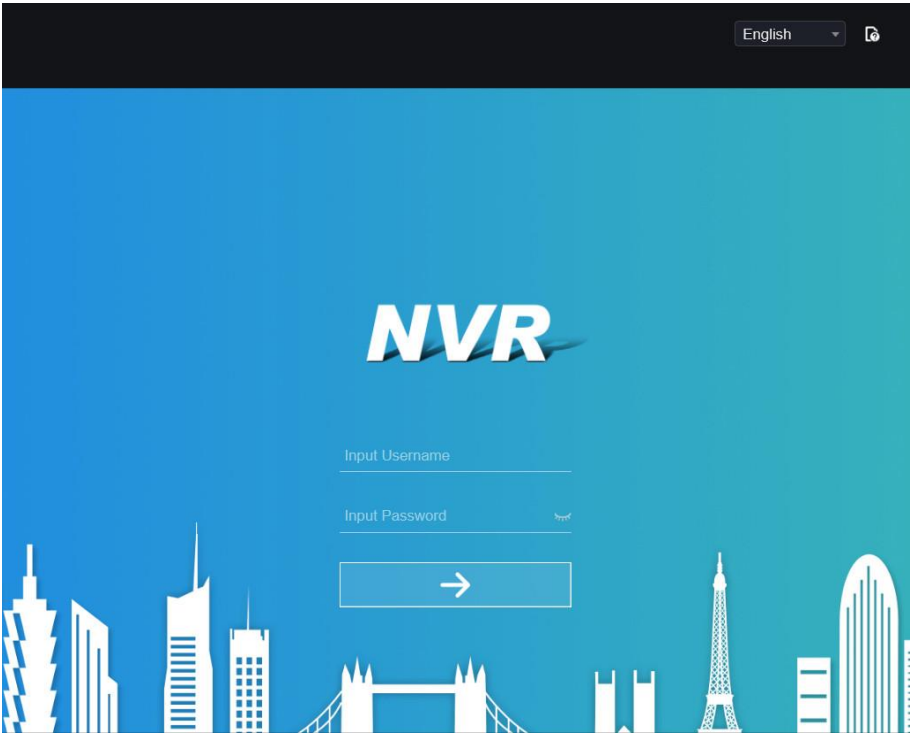
Here we take Chrome as an example for video viewing.

Login

Step 1 Open the Chrome browser, enter the IP address of the NVR (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 NVR for the first time.

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

Figure 7-6 Homepage interface 1

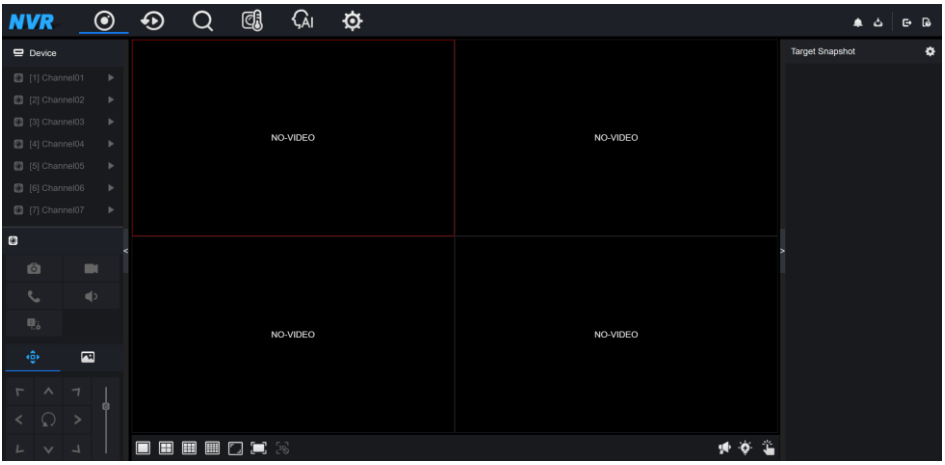


Figure 7-7 Homepage interface 2

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

NVR 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 5-16 shows the overall layout of the interface. For descriptions of the interface, please refer to Table 7-1.

Figure 7-8 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 NVR and the channels managed by the NVR.
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 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 7-11.

8		Broadcast. When you add the IP speakers to the NVR, 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.

Figure 7-9 Help

Figure 7-10 Broadcast

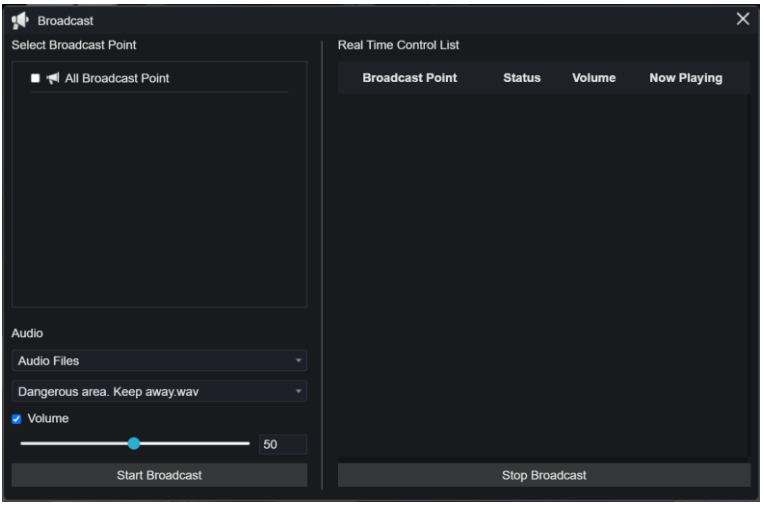
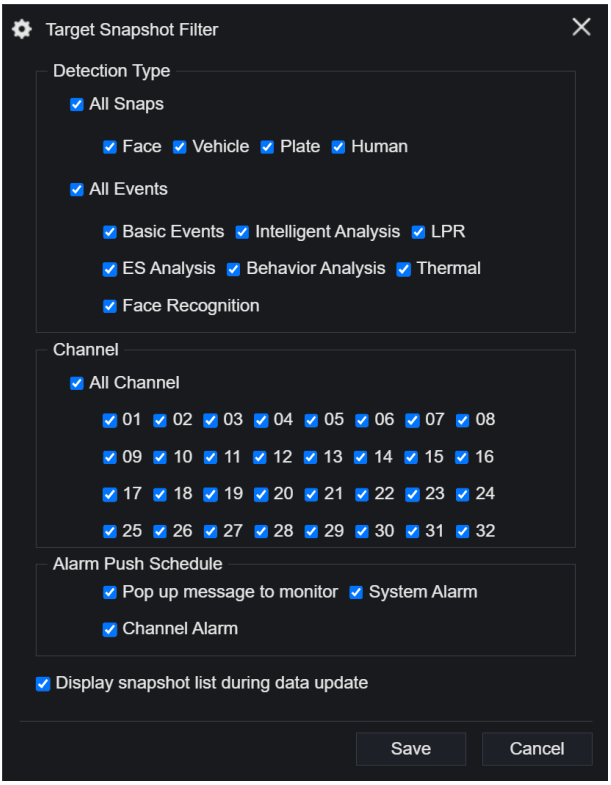


Figure 7-11 Target snapshot filter



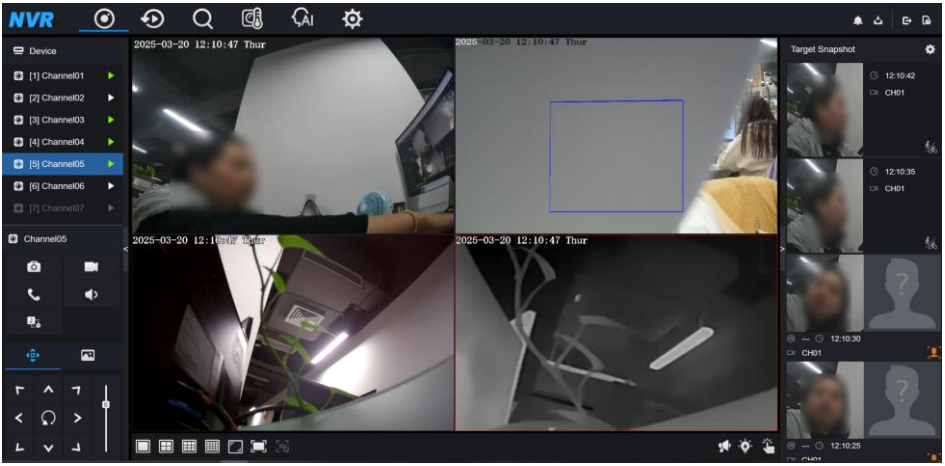
----End

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 7-12.

Figure 7-12 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.
	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).
	Switch stream	Click the button to switch stream 1 (mainstream) and stream 2 (substream).

Buttons	Button description	How to operate
	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 NVR 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 7-13. Table 7-3 describes the operations.

Figure 7-13 PTZ control interface

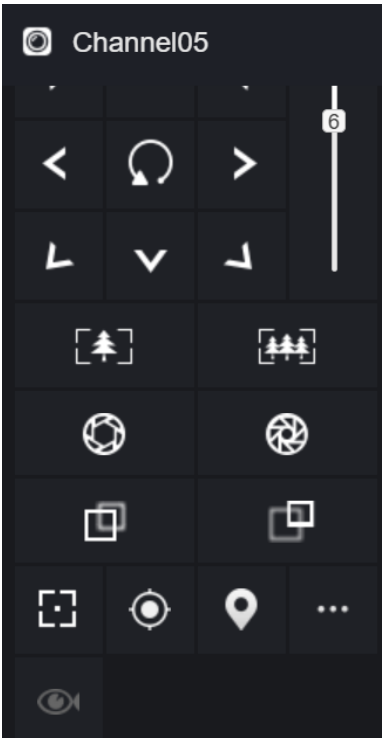
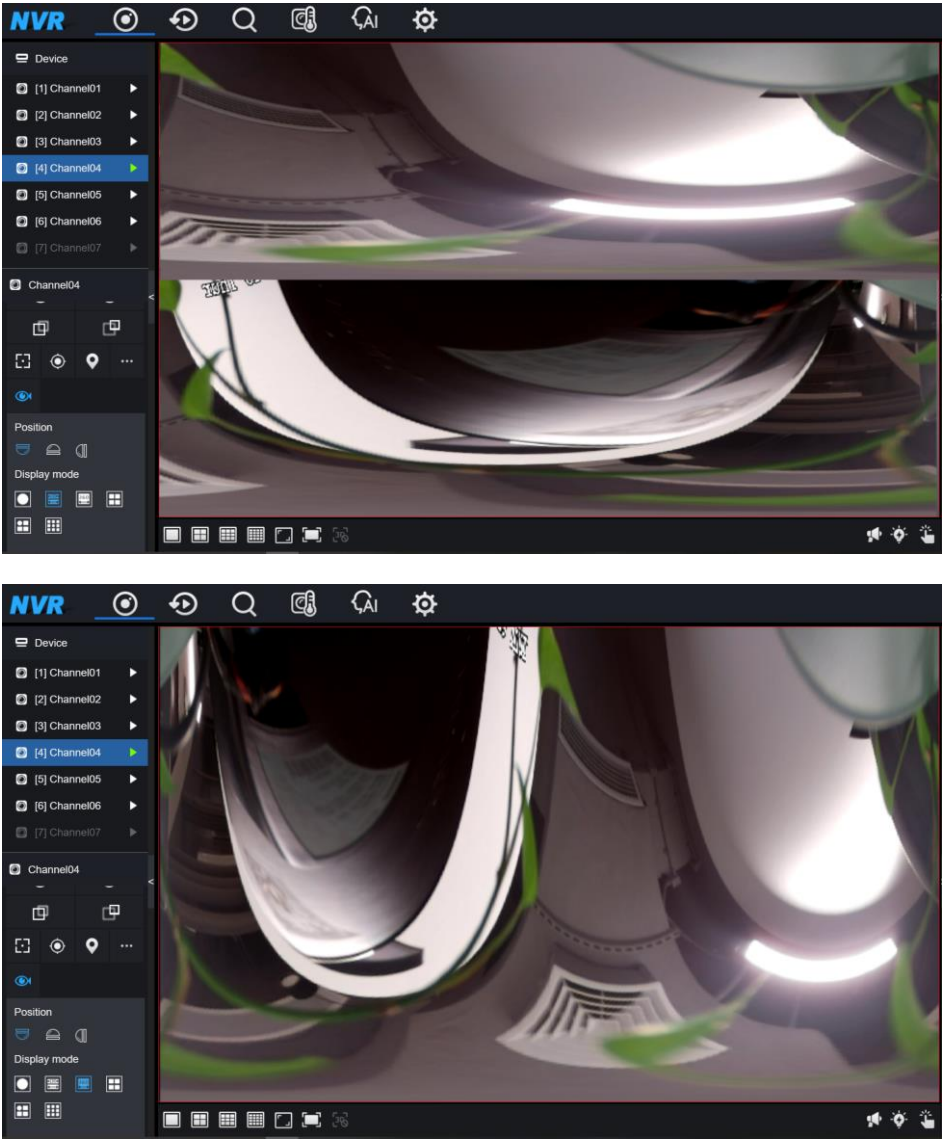


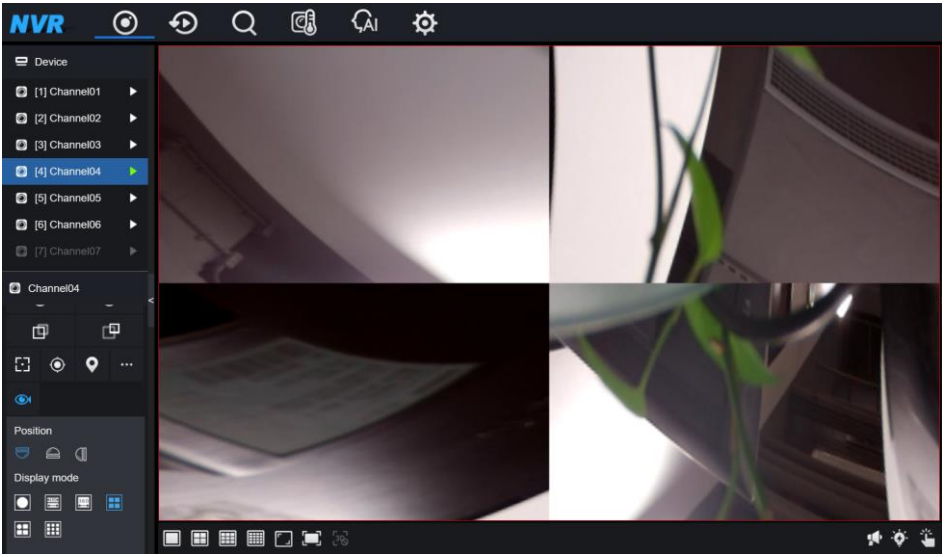
Table 7-3 Device parameters

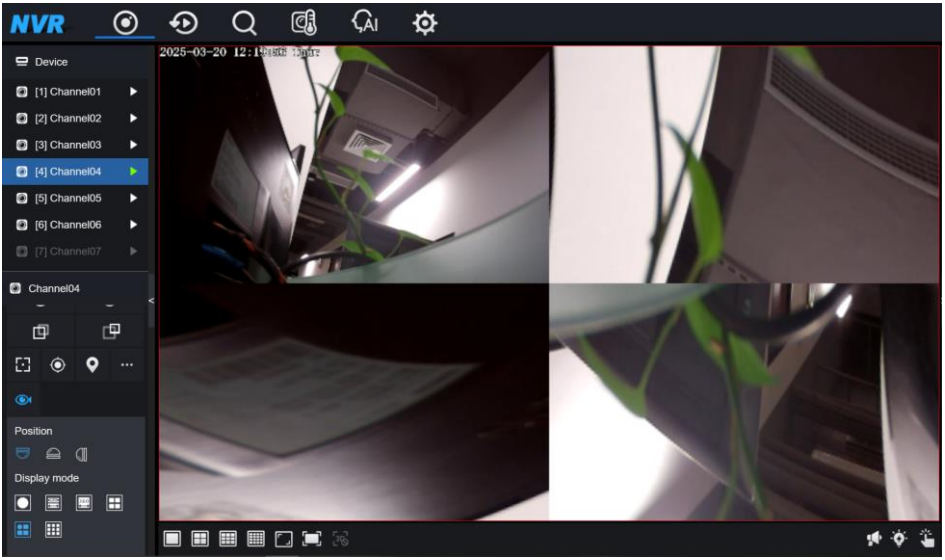
Buttons	Button description	How to operate
	Direction key	Click the button to control the omnidirectional movement of the PTZ.
	Speed slider	Drag the slider to adjust the value of PTZ rotation speed.
	Zoom in	Click the buttons to adjust the focal length.
	Zoom out	

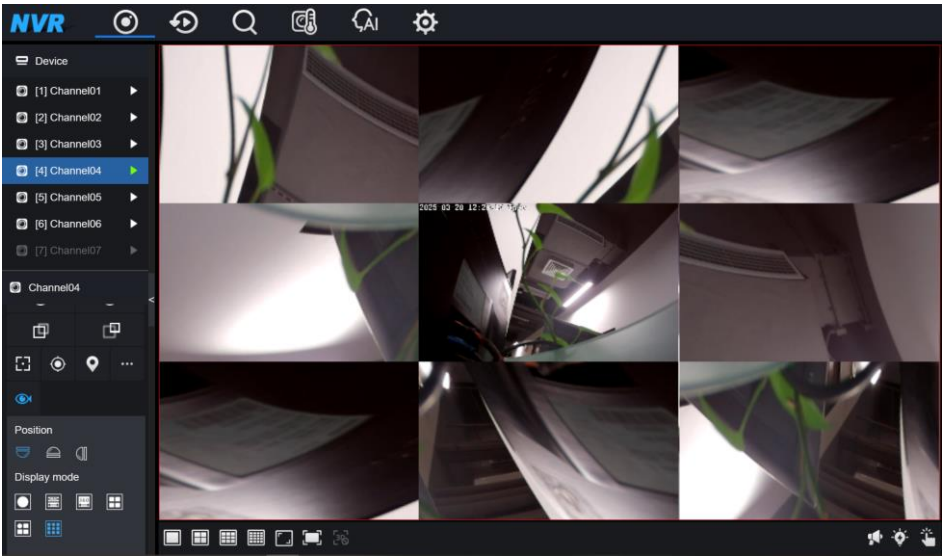
Buttons	Button description	How to operate
	Iris+	Click the buttons to adjust the aperture.
	Iris-	
	Far focus	Click the buttons to adjust the focal length.
	Near focus	
	Autofocus	Click the button to focus automatically.
	Home preset	N/A
	Preset	The camera sets the tour, click the button and the dome camera rotates as the setting.
	More	More settings, scan, and tour
	Fisheye	When the channel is playing in one-screen mode, the fisheye is valid. Click the icon to choose one mode to play. 

Figure 7-14 Fisheye modes




NVR
Device
[1] Channel01
[2] Channel02
[3] Channel03
[4] Channel04
[5] Channel05
[6] Channel06
[7] Channel07
Channel04
Position
Display mode


NVR
Device
[1] Channel01
[2] Channel02
[3] Channel03
[4] Channel04
[5] Channel05
[6] Channel06
[7] Channel07
Channel04
Position
Display mode



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 7-15. Table 7-4 describes the operations.

Figure 7-15 Image parameter interface

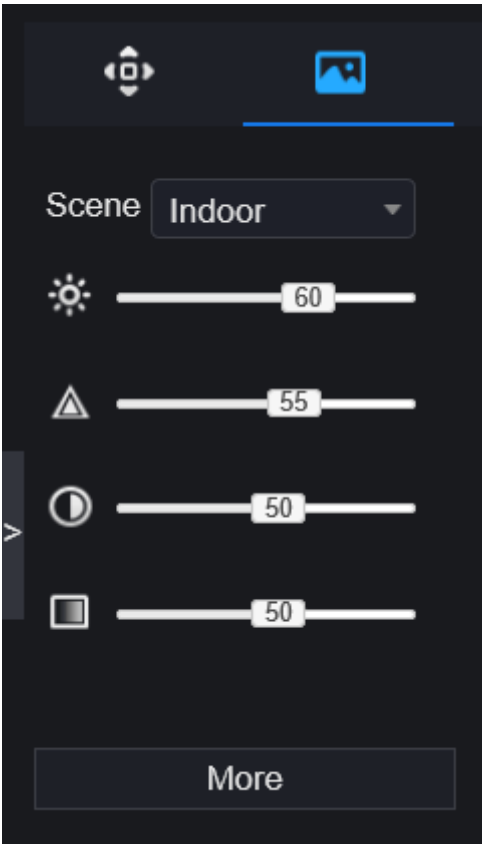
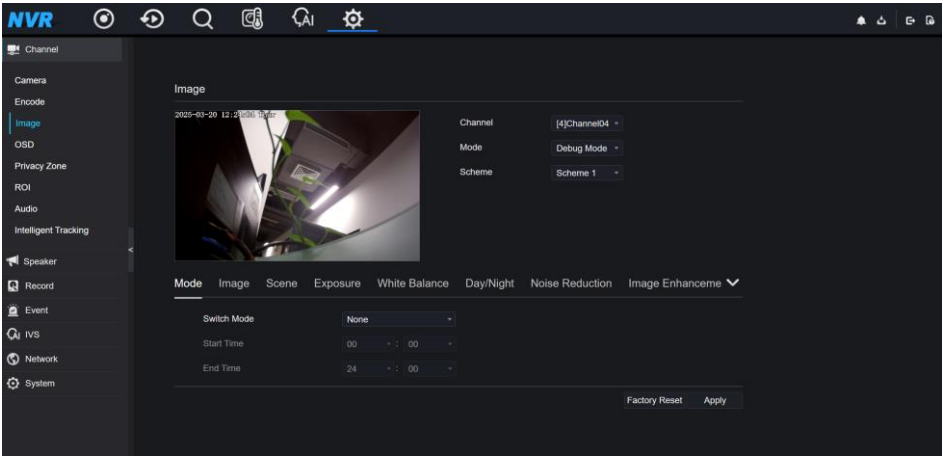


Table 7-4 Device parameters

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 7-16, for more details, please refer to *Chapter 6.1.3* Image.

Figure 7-16 Sensor setting interface



----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

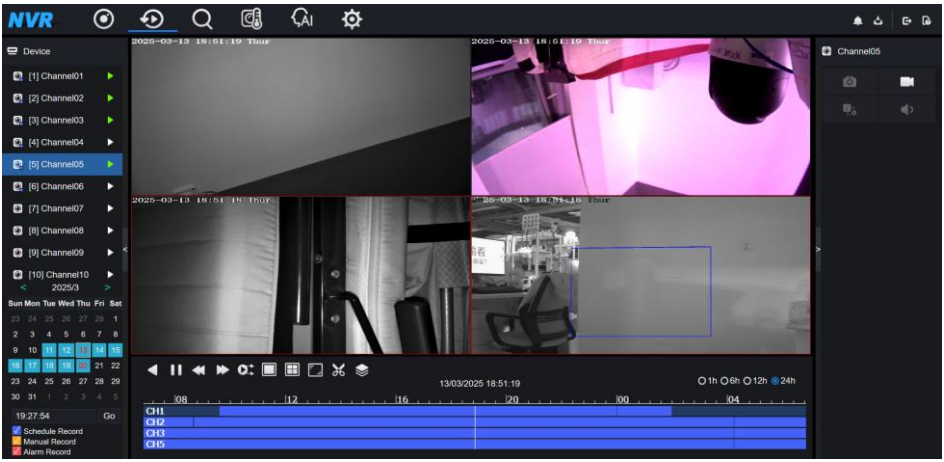
7.3.1 Video Playback

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 7-17.

Figure 7-17 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.

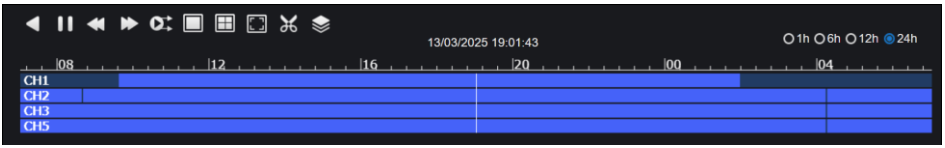
After a device and date are selected, video information is displayed below the video pane. The time scale above the file axis shows the different time points of video recording. The time in blue in the middle is the time of the video playing.

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.

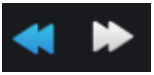
You can play a video after selecting a device and date. Figure 7-18 shows the control bar of video playback.

Figure 7-18 Control bar



 Reversed.

 Play/Pause.

 Triple speed.

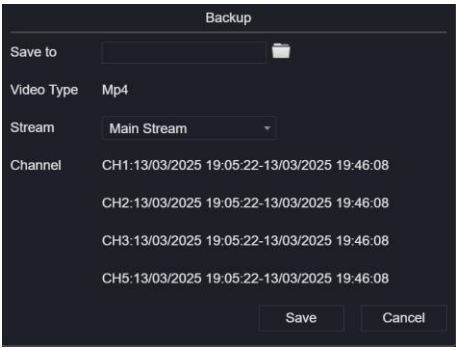
 Sync/Async. You can set the different channels to play synchronously or asynchronously. Sync mode indicates the selected channels play video synchronously. Async mode indicates users play different record periods.

 Split-screen. One or four screens.

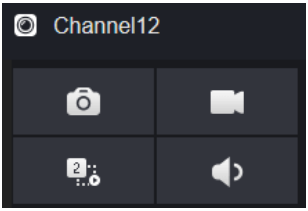
 Open original scale/Close original scale.

 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 7-19 Backup



Types of time bar/interval.



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

----End

7.4 Alarm Search

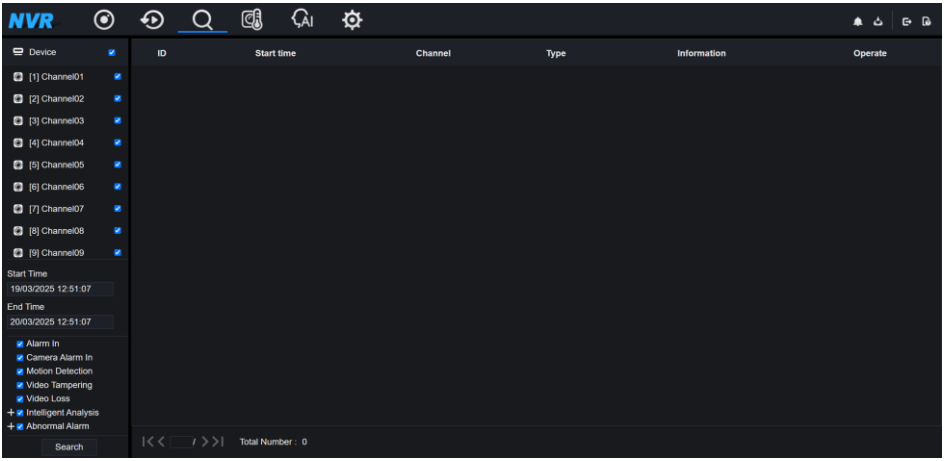
You can search for channel alarms and system alarms in the alarm search interface.

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 7-20.

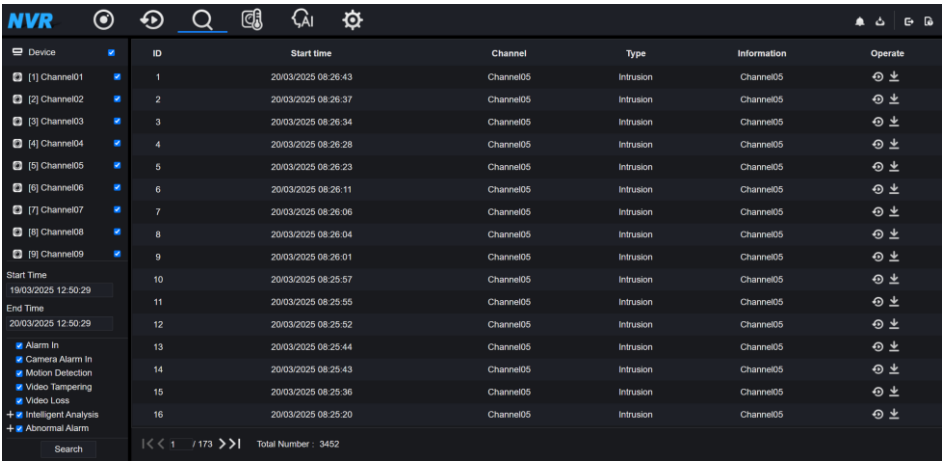
Figure 7-20 Channel alarm interface



Step 2 Choose the alarm type to search.

Step 3 Click **Search**. The result will be displayed as shown in Figure 7-21.

Figure 7-21 Channel alarm result



NOTE

Click  to select the page of the alarm list.

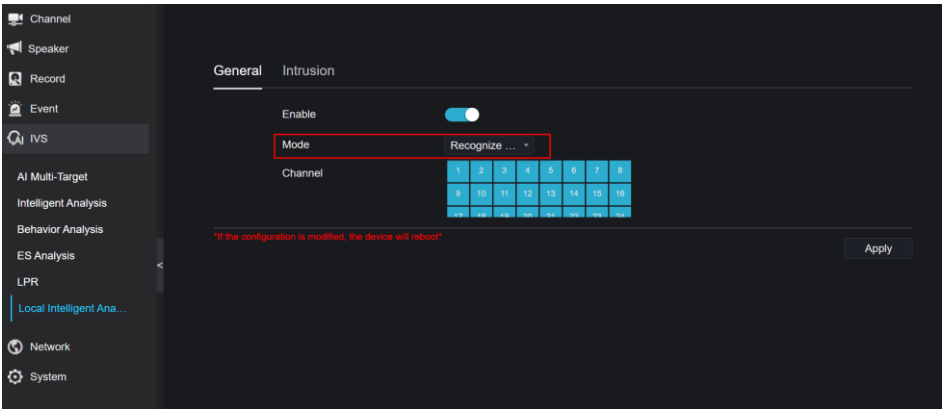
20 alarm messages are shown on every page.

----End

7.5 Attendance (Only for Some Models)

For some models, the local intelligent analysis should be set to Recognize Mode so that the attendance function is unfolded.

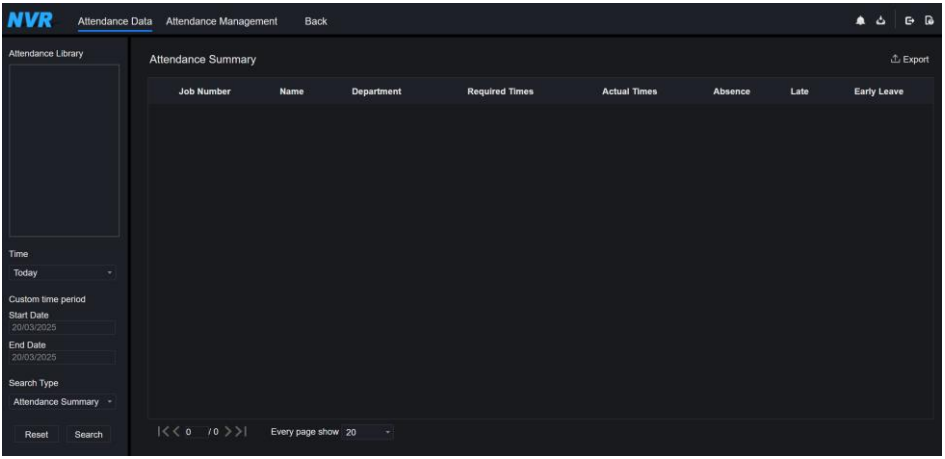
Figure 7-22 Recognize mode



7.5.2 Attendance Data

Click to enter the attendance data interface, as shown in Figure 7-23.

Figure 7-23 Attendance data



Operation Steps

Step 1 Tick the Attendance Library.

Step 2 Choose the time mode, such as today, this week, this month, or custom time.

Step 3 Choose a search type, such as attendance summary and attendance details.

Step 4 Click search. The result will show in the interface.

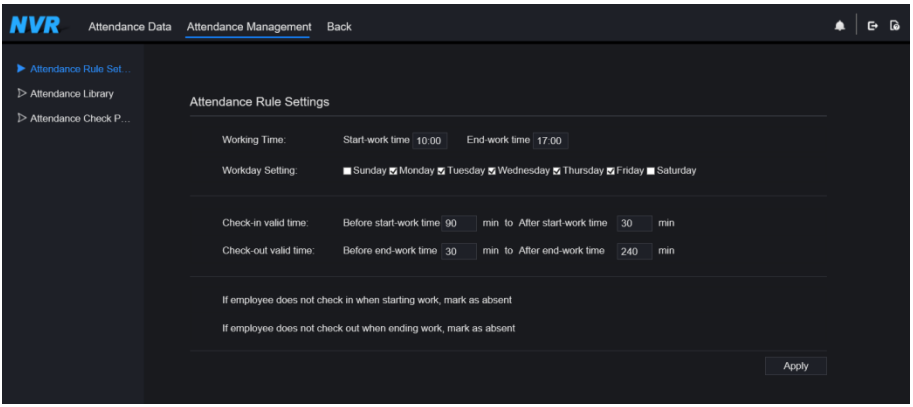
Step 5 Click Export to export the query result.

----End

7.5.3 Attendance Management

In Attendance Management, users can set attendance rules, libraries, and checkpoints, as shown in Figure 7-24.

Figure 7-24 Attendance rule settings



Operation Steps

Step 1 Set start work time and end work time.

Step 2 Tick the workdays.

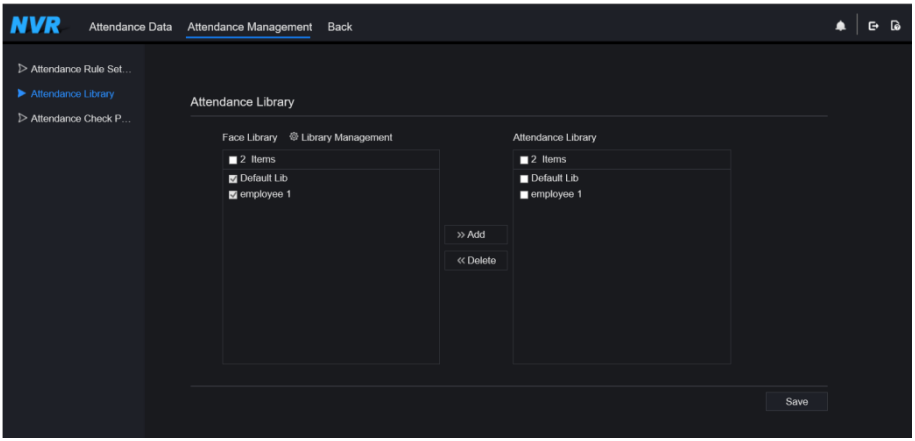
Step 3 Set valid time for check-in and check-out.

Step 4 Click Save to save the setting.

Attendance library

Step 1 Click **Attendance Library** to add a library. The attendance library can call the face database directly.

Figure 7-25 Attendance library



Step 2 Tick the library and click **Add** to add to the attendance library. If you want to modify the library, please enter the library interface to change the parameters.

Step 3 Click 

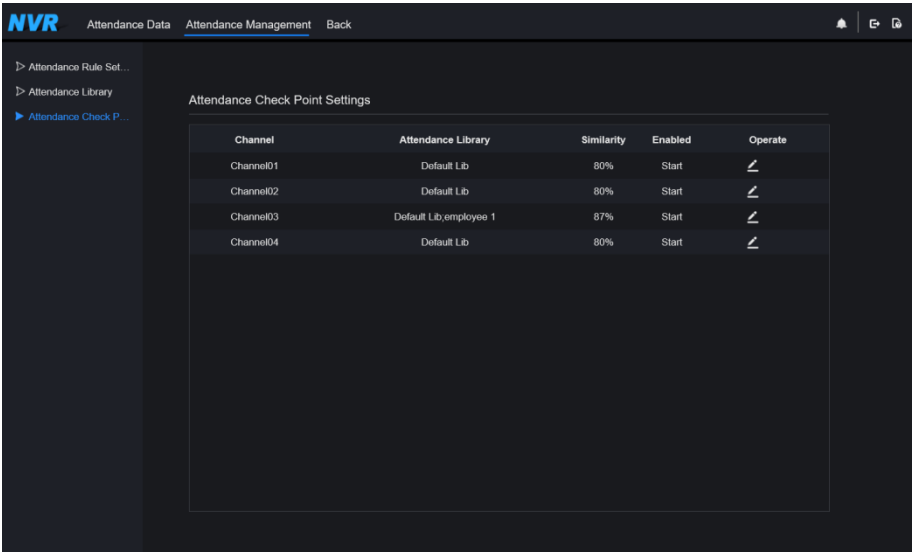
to enter the face database management to modify parameters.

Step 4 Click **Save** to save the setting.

Attendance Checkpoint settings:

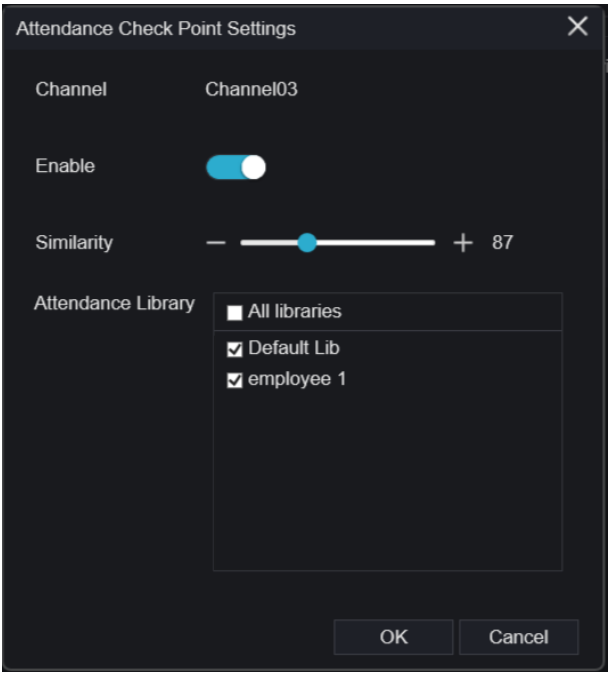
Step 1 Click Attendance Checkpoint Settings to set the point, as shown in Figure 7-26.

Figure 7-26 Attendance checkpoint setting



Step 2 Click  to edit the point setting, as shown in Figure 7-27.

Figure 7-27 Checkpoint



Step 3 Enable the function, set similarity, and tick the library. All face detection cameras can set the checkpoints.

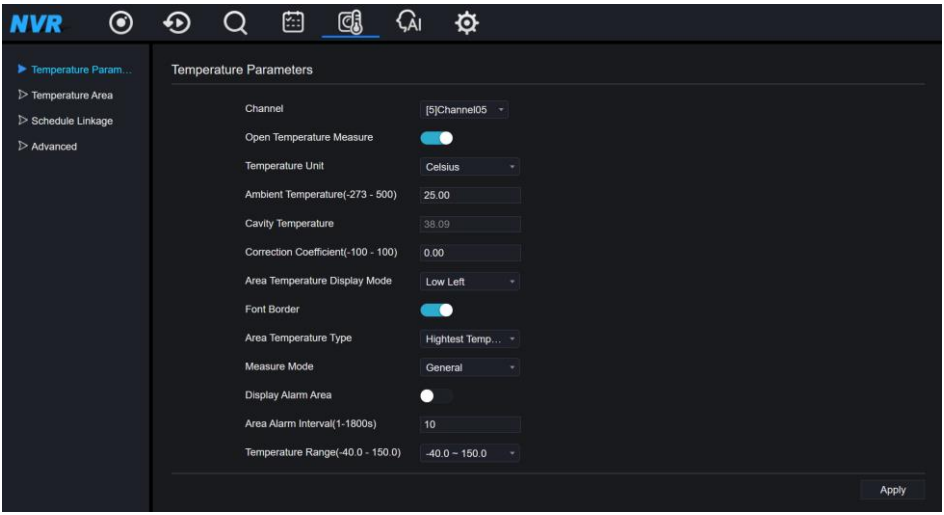
Step 4 Click OK to save the setting.

----End

7.6 Thermal

For thermal camera channels, set the temperature parameters, temperature area, schedule linkage, and advance on the Thermal as shown in Figure 7-28.

Figure 7-28 Thermal



For detailed information please refer to Chapter 5.6 *Thermal Temperature.*

Figure 7-29 Temperature area

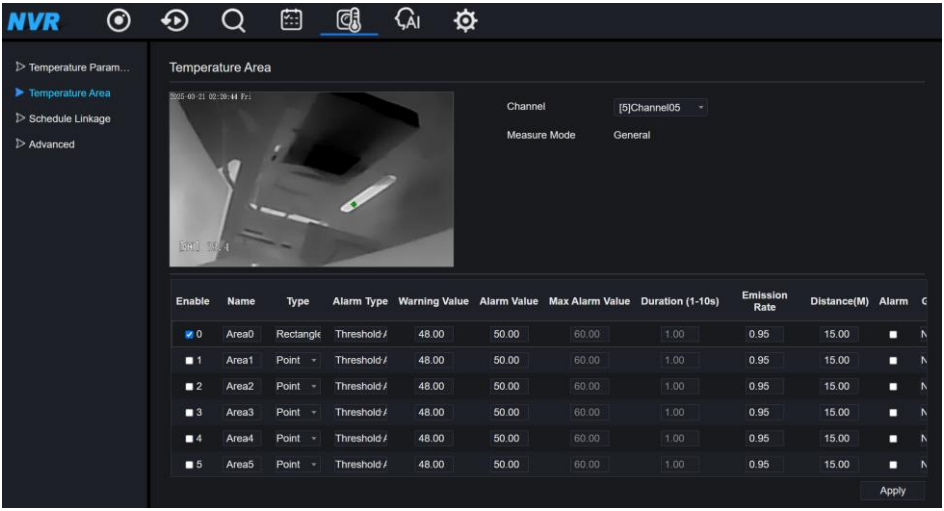


Figure 7-30 Schedule linkage

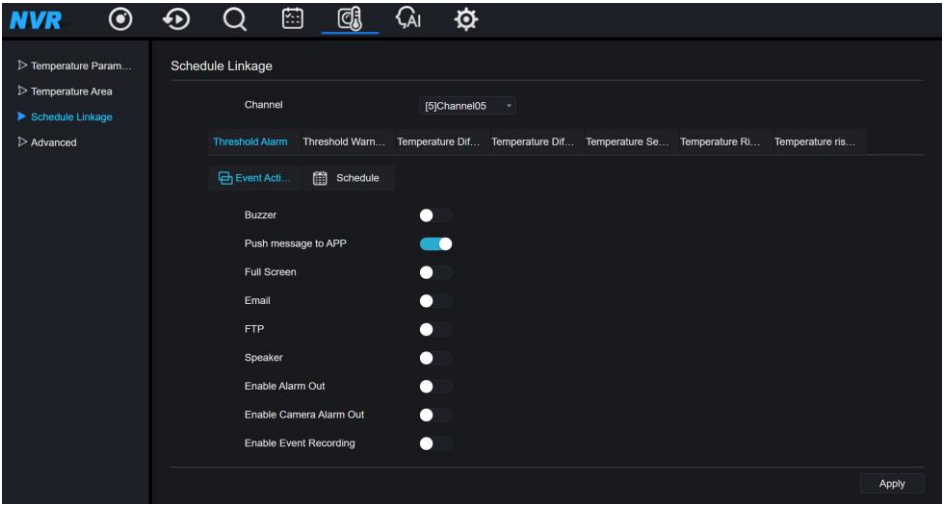
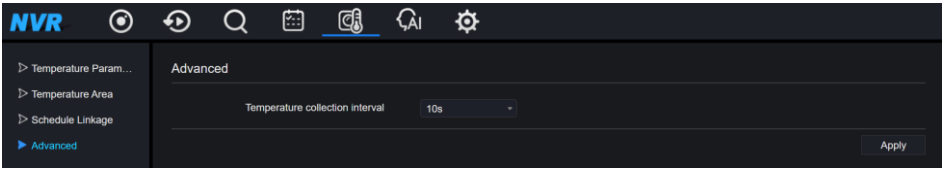


Figure 7-31 Advanced



7.7 AI Application (Only for Some Models)

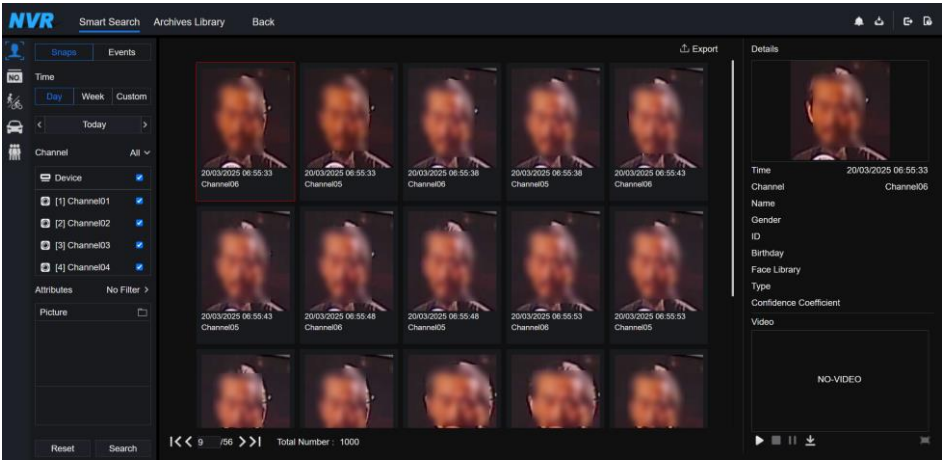
At the AI recognition interface, we can set the **Real-time Comparison, Smart search, Archives library,** and **Comparison configuration**.

7.7.1 Smart Search

At the smart search interface, users can search the human face, vehicle license plate, full body, car, and body temperature.

7.7.1.1 Human Face Search

Figure 7-32 Human face search



Step 1 Choose Human Face to search at the Smart Search interface.

Step 2 Tick the face recognition camera channels, and set the start time and end time.

Step 3 Choose the condition (by picture or by feature). The picture can be chosen from the file folder.

Step 4 Click “Search” to search the snapshot of the human face.

Step 5 The result will show in the middle of the page. Click the picture and detailed information at the top right of the page.

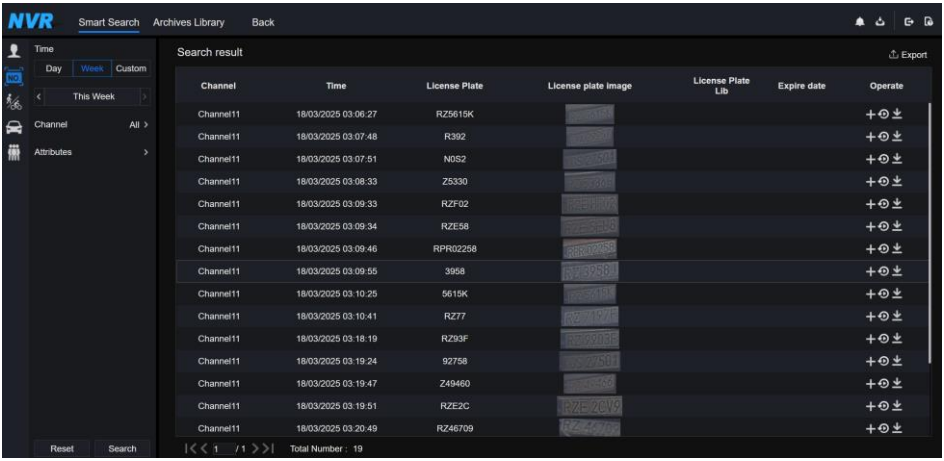
Step 6 Detailed pictures can be used to search or add to the library.

Step 7 Click the play button of the video to play the recordings of the snapshot.

----End

7.7.1.2 Vehicle License Plate Search

Figure 7-33 Vehicle License Plate Search



Step 1 Choose the Vehicle License Plate at the Smart Search interface.

Step 2 Tick the vehicle license plate recognition camera channels, and set the start time and end time.

Step 3 Input the license plate optionally.

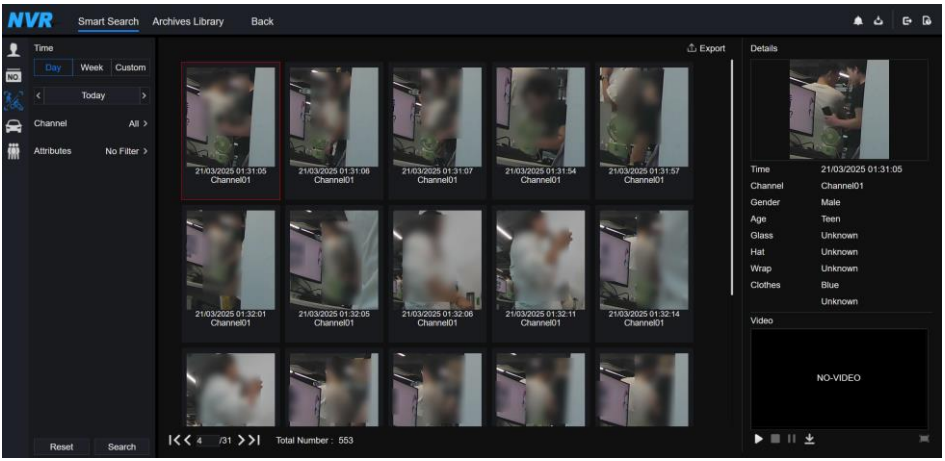
Step 4 Click “Search” to search the snapshot of the license plate.

Step 5 The result will show on the page. Click “+” to add to the library.

----End

7.7.1.3 FullBody Search

Figure 7-34 Full body search



Step 1 Choose Full Body Search at the Smart Search Interface.

Step 2 Tick the AI recognition camera channels, and set the start time and end time.

Step 3 Set the gender and click cycling or no cycling.

Step 4 Click “Search” to search the snapshot of the human face.

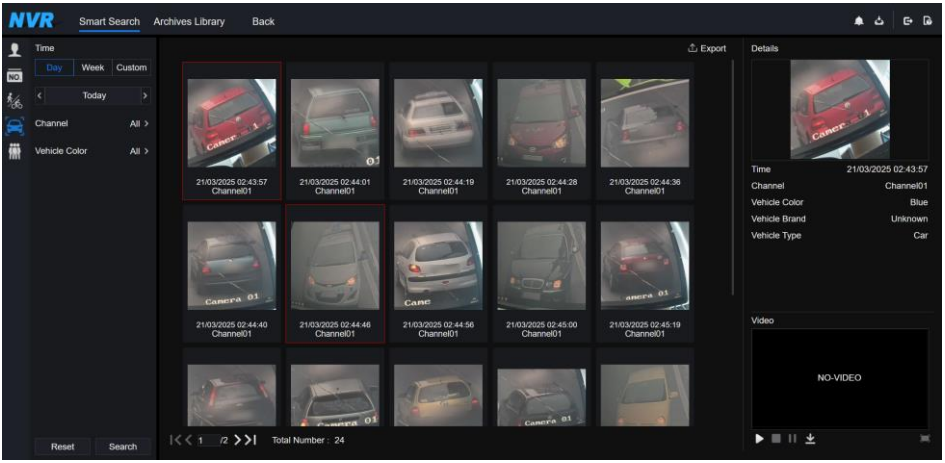
Step 5 The result will show in the middle of the page. Click the picture, and the detailed information will show at the top right of the page.

Step 6 Click the play button of the video to play the recording of the snapshot.

----End

7.7.1.4 Vehicle Search

Figure 7-35 Vehicle search



Step 1 Choose Vehicle Search at the Smart Search Interface.

Step 2 Tick the AI recognition camera channels, and set the start time and end time.

Step 3 Tick the color.

Step 4 Click “Search” to search the snapshot of the human face.

Step 5 The result will show in the middle of the page. Click the picture and detailed information at the top right of the page.

Step 6 Click the play button of the video to play the recordings of the snapshot.

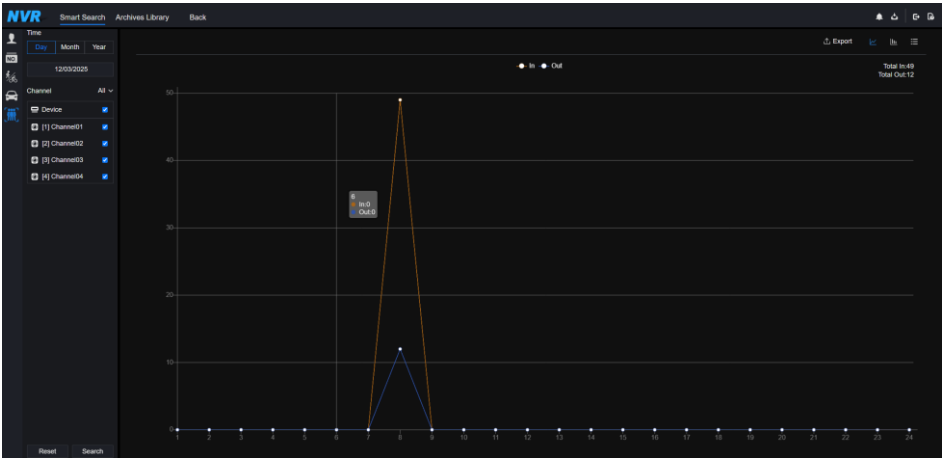
----End

7.7.1.5 People counting

If the AI camera connects to the NVR, the NVR can directly obtain the data of the camera. Set the statistical type (day, month, year), and choose the time to search.

The result can be shown as a line graph, histogram, or list, as shown in Figure 7-36.

Figure 7-36 People counting



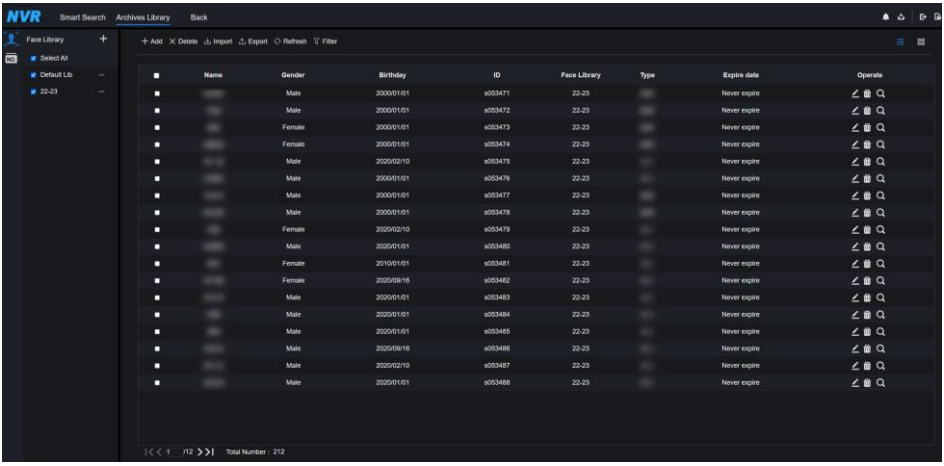
----End

7.7.2 Archives Library

At the Archives library, users can add or edit the face library, and license plate library.

7.7.2.1 Face Library

Figure 7-37 Face library



Click “+” to add a face library.

Click “Add” to add the person to enroll.

Tick the person, and click “Delete” to delete the person.

Click “Import” to add the person batch.

Click “Export” to export all people in the library.

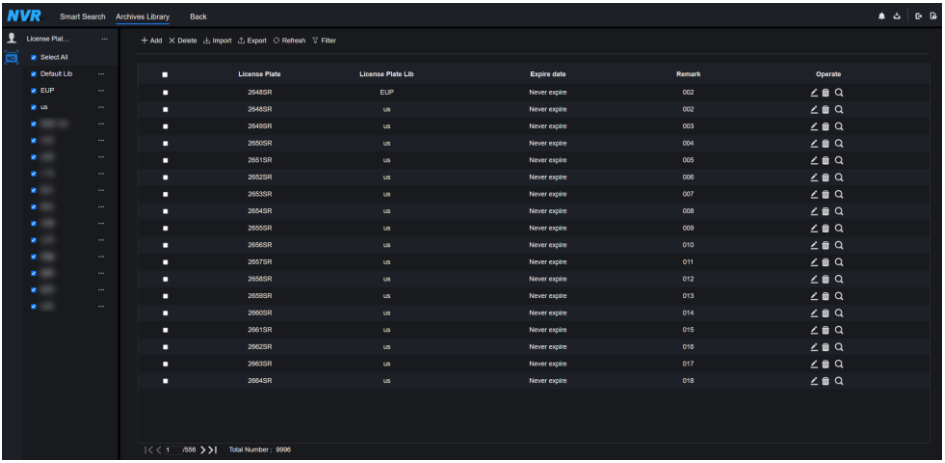
Click the operate icon to edit or delete the chosen person.

To get snapshots in real-time video, put the cursor on a picture, such as  , you can add it to the face library or face search. The cursor is on Area 6, and the pictures are not updated; move the mouse so that the pictures show in time.

----End

7.7.2.2 License Plate Library

Figure 7-38 License plate library



Click “+” to add the license plate library.

Click “Add” to add the plate to the library.

Tick the plate, and click “Delete” to delete the license plate.

Click “Import” to add the license plate batch.

Click “Export” to export the all-license plate library.

Click the operate icon to edit or delete the chosen license plate.

----End

8 System Setting

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

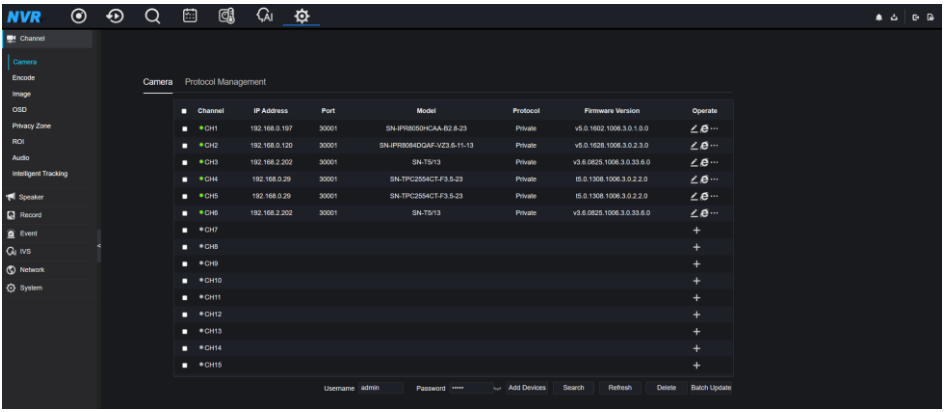
8.1 Channel

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

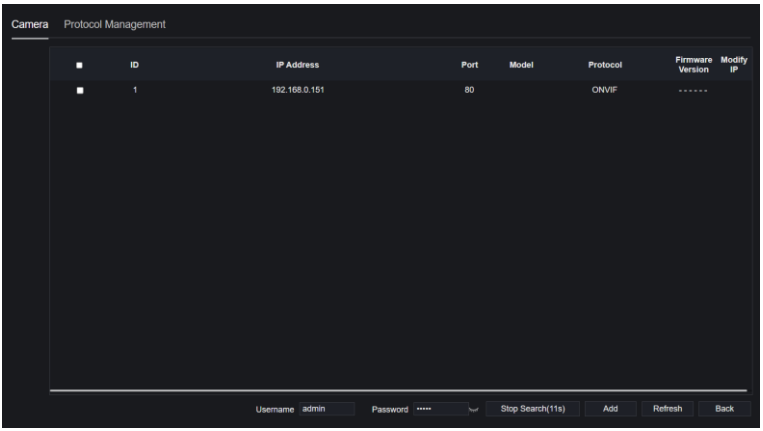


Step 2 Input username and password (the default username and password both are admin), and click/add cameras automatically.

Step 3 Click Search to search cameras at the same LAN as NVR, 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



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

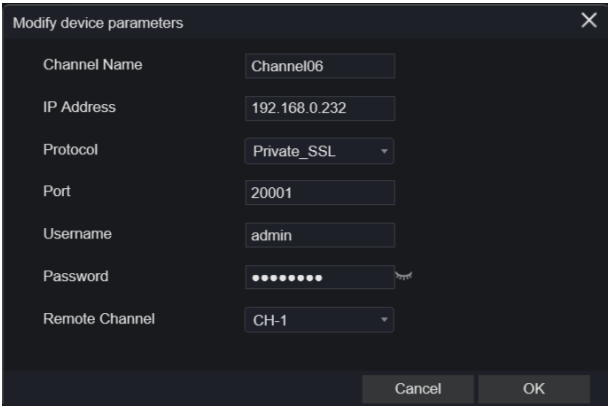
Step 5 Click Refresh to refresh the camera status.

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.

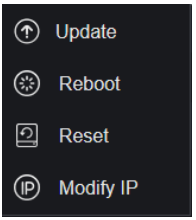
Figure 8-3 Modify device parameters



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.

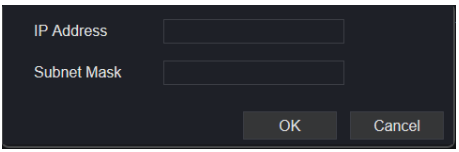
Figure 8-4 Add camera manually

Step 10 Click  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



NOTE

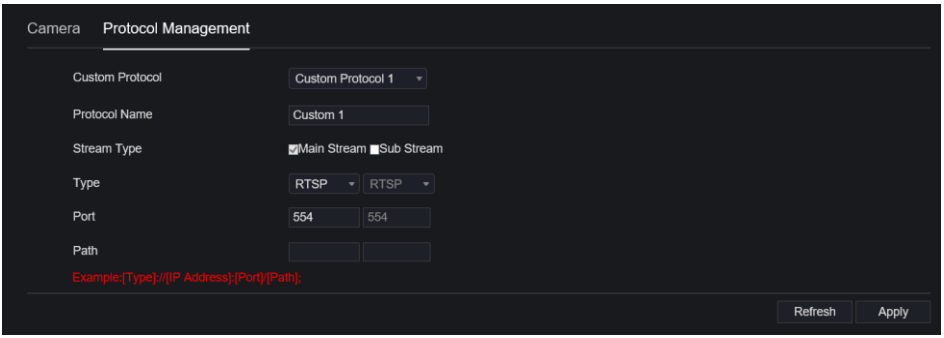
 It indicates the camera is online. Users can view the live video immediately.

 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 NVR.

Figure 8-6 Protocol management



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.

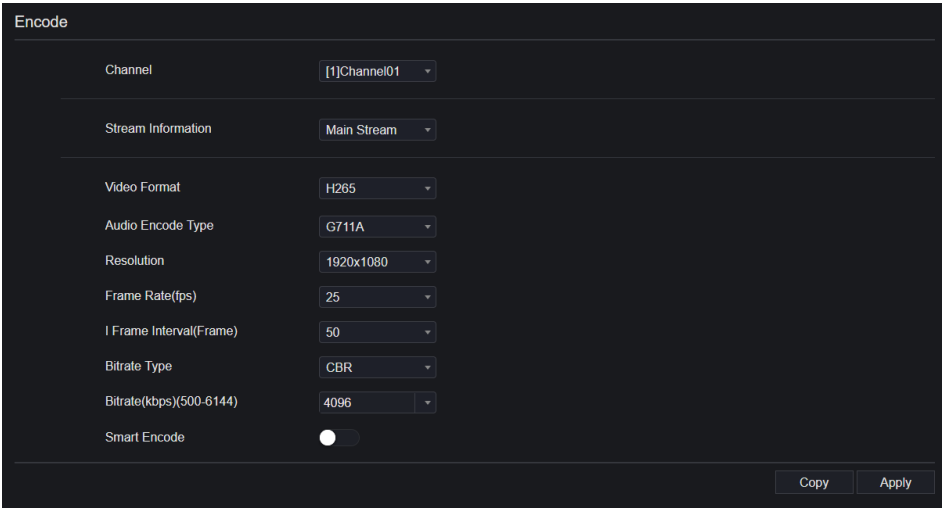
Step 7 Input the path, which is decided by the manufacturer of the cameras.

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



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.

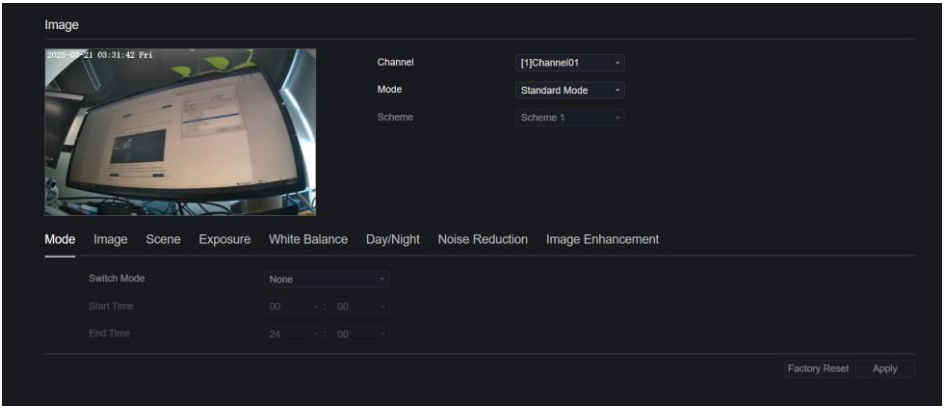
Step 4 Click Copy to choose another camera to copy settings. Click Apply to save the settings.

----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



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

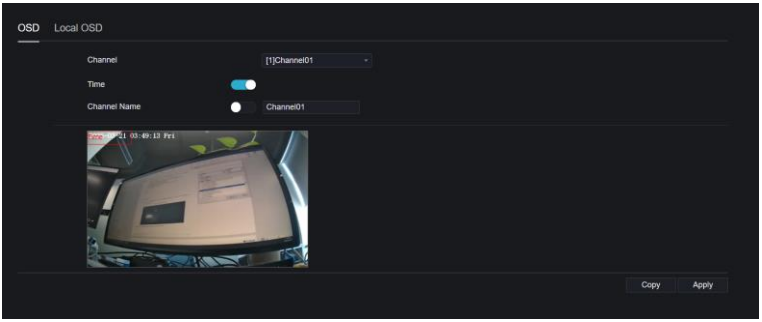
Brightness: It indicates the total brightness of an image. As the value increases, the image becomes brighter.
Sharpness: It indicates the border sharpness of an image. As the value increases, the borders become clearer, and the number of noise points increases.
Saturation: It indicates the color saturation 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

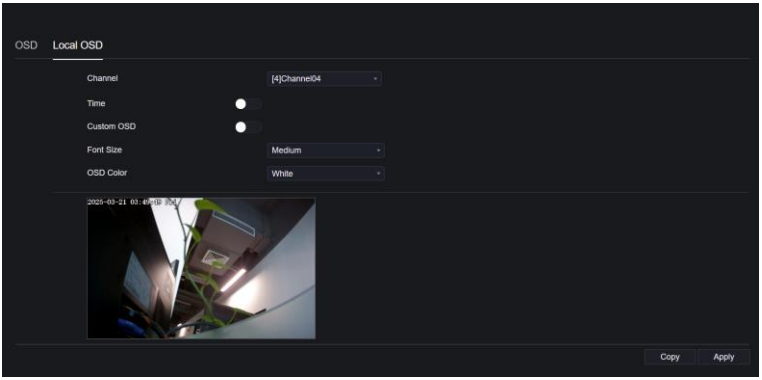


Step 2 Select a channel and scene from the drop-down list.

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



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

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.

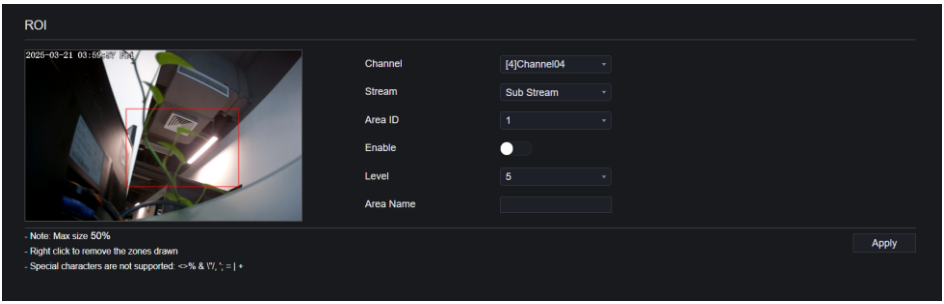
Step 5 Click Copy to choose other cameras to copy settings. Click Apply to save the settings.

----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



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 6.1.7 Audio (Only for Some Models)*.

Figure 8-13 Audio in

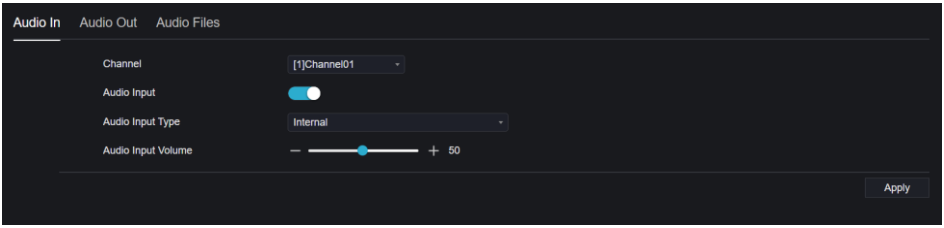


Figure 8-14 Audio out

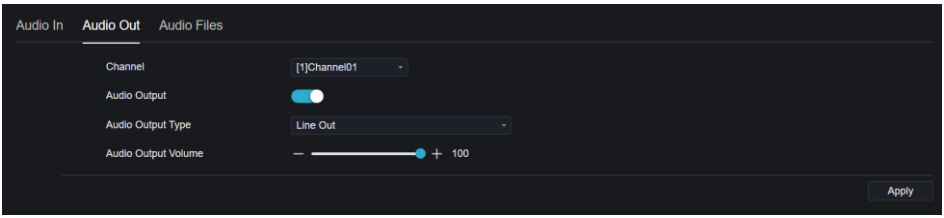
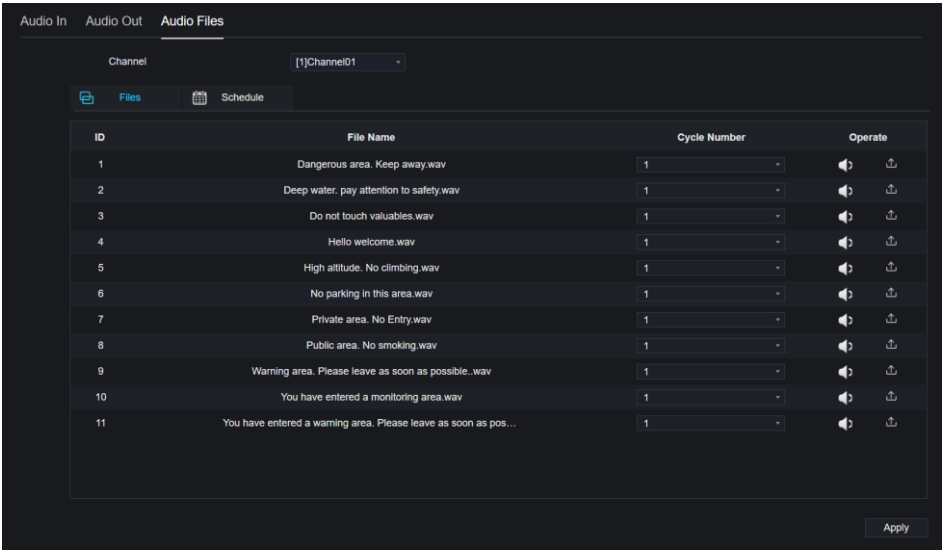


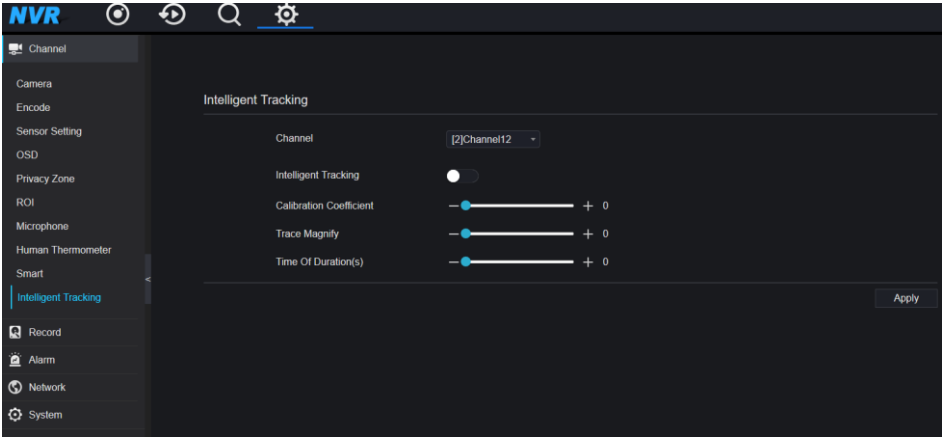
Figure 8-15 Audio files



8.1.8 Intelligent Tracking (Only for Some Models)

This function can only be used for high-speed dome cameras. It works with the PTZ function.

Figure 8-16 Intelligent tracking



The detailed information please refer to the UI configuration setting.

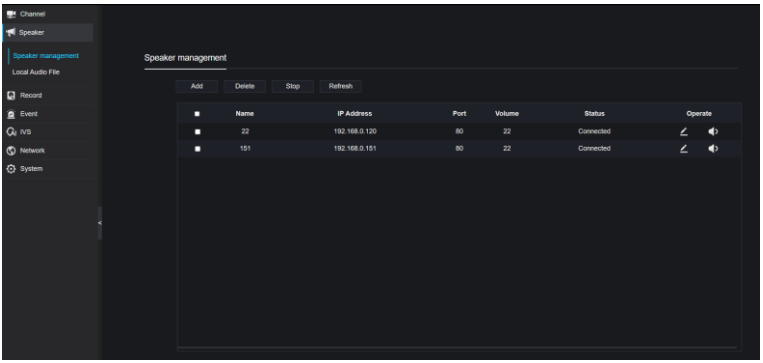
8.2 Speaker

On the Speaker interface, users can add IP speakers to the NVR, and manage the local audio files.

For the detailed information, please refer to *Chapter 6.2 Speaker*.

8.2.1 Speaker Management

Figure 8-17 Speaker management



8.2.2 Local Audio Files

Figure 8-18 Local audio file

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 8-19.

Figure 8-19 Record schedule interface

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 NVR, the NVR 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.

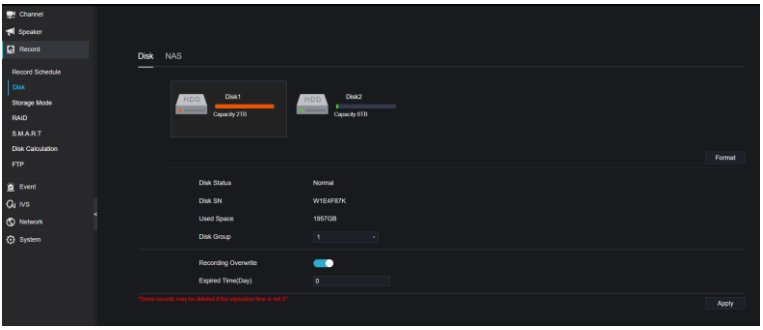
----End

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 8-20.

Figure 8-20 Disk interface



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

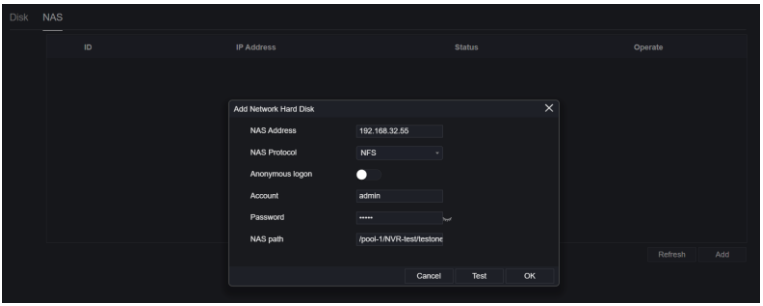
8.3.2.2 NAS

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 8-21 NAS



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.

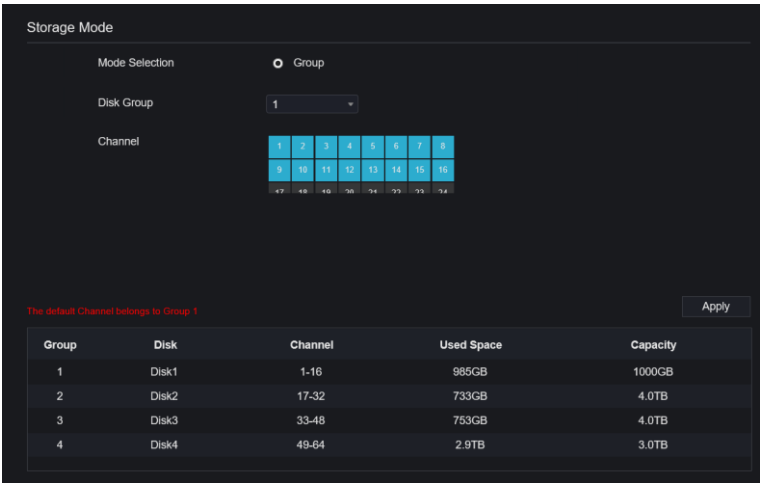
Step 5 Click **Test** to check the parameters, test successfully, and click **OK** to save the settings.

----End

8.3.3 Storage Mode

Distribute channels to different disk groups as needed for efficient use of the disk capacity.

Figure 8-22 Storage Mode



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 RAID (Only for Some Models)

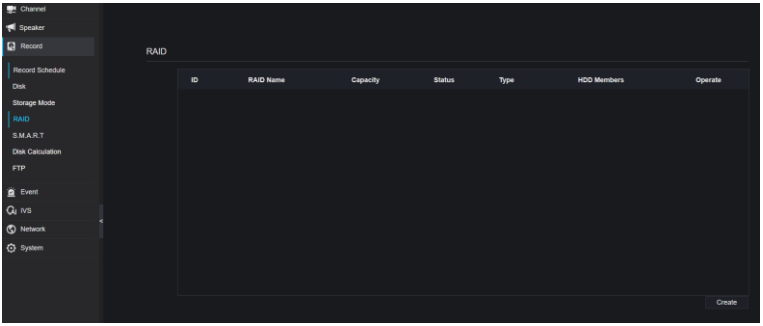
NOTE

The disks must be enterprise-level disks. It is recommended to choose the same capacity for efficient use. Support RAID 0/1/5/6/10.

For RAID5, at least 3 disks can be created. For RAID6, at least 4 disks can be created. For RAID10, at least 4 disks can be created. Creating a hot spare disk requires more disks.

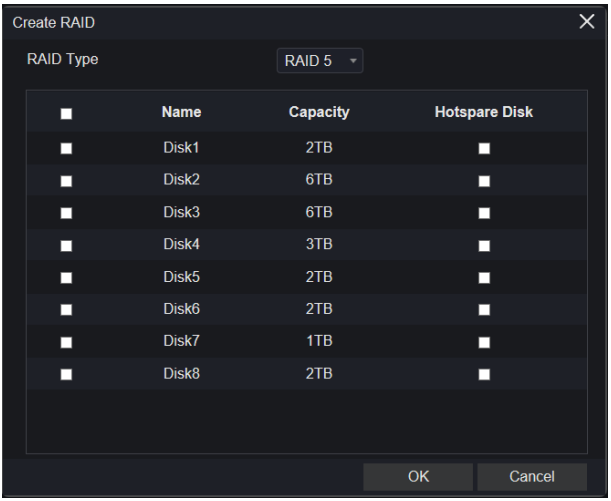
It is recommended to choose the same capacity for efficient use. The RAID with less than 80T capacity can be built.

Figure 8-23 RAID



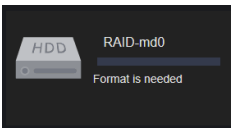
Operation Steps

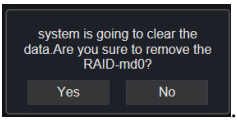
Step 1 Click **RAID** to create the RAID.



Step 2 Click **Create** to choose a disk to create a new RAID.

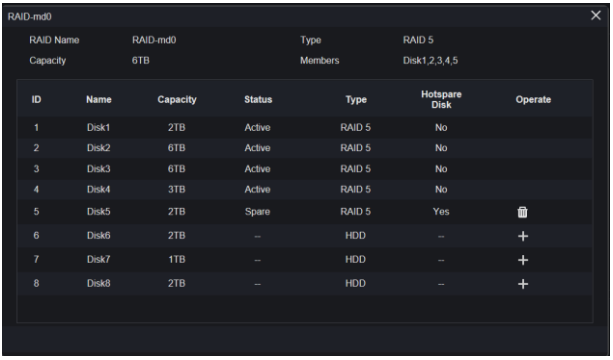
Step 3 Tick the **Hot-Spare Disk** to back up the broken disk in case the number of disks must be more than the basic disks.

Step 4 Click OK to save the operation, format the new RAID 

Step 5 Click **Format** it will show 

.

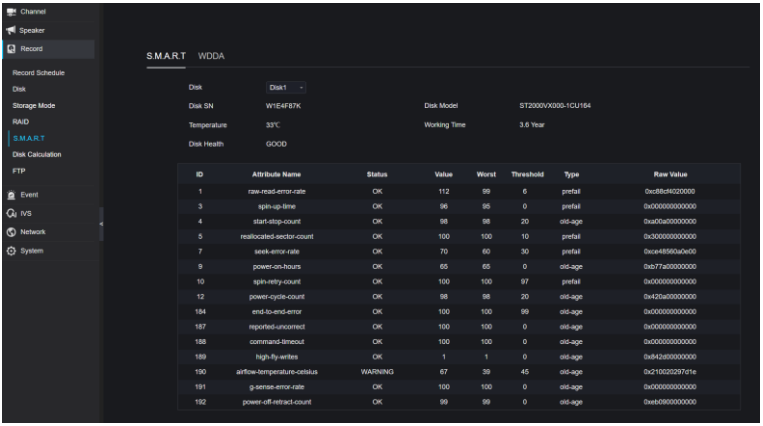
Figure 8-24 Modify the RAID



8.3.5 S.M.A.R.T

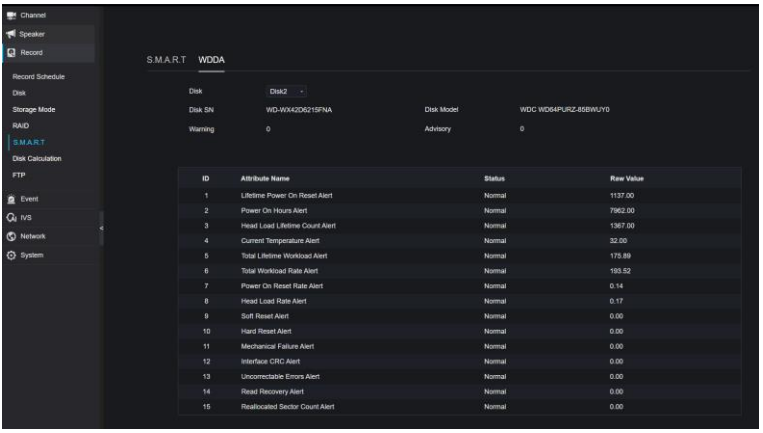
S.M.A.R.T is a Self-Monitoring Analysis and Reporting Technology; users can view the health of the disk, as shown in Figure 8-25.

Figure 8-25 S.M.A.R.T



The disk of Western Digital can be viewed by WDDA, as shown in Figure 8-26.

Figure 8-26 WDDA (Supplied for Some Model)

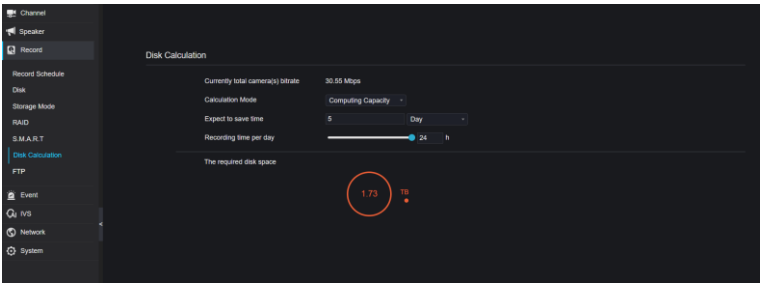


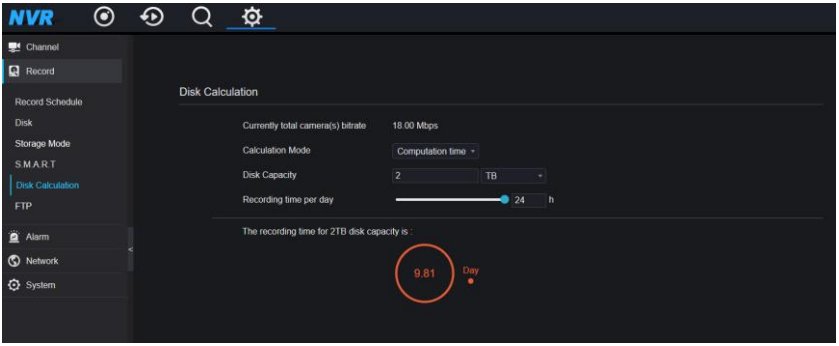
8.3.6 Disk Calculation

There are two modes to calculate the captivity of the disk, as 

shown here.

Figure 8-27 Disk calculation

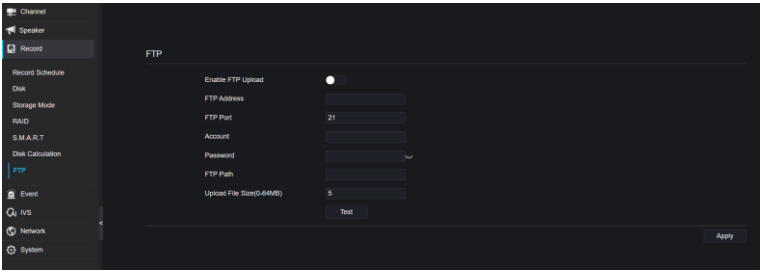




8.3.7 FTP

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



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

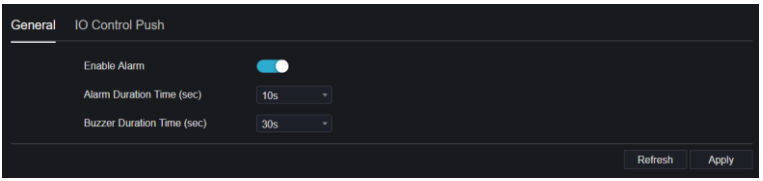
8.4.1.1 General

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



Step 3 Click Apply to save settings. Click Refresh to return to the previous settings.

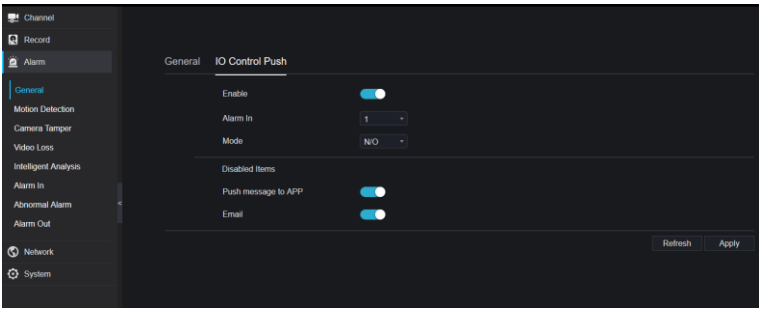
8.4.1.2 IO Control Push

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



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.

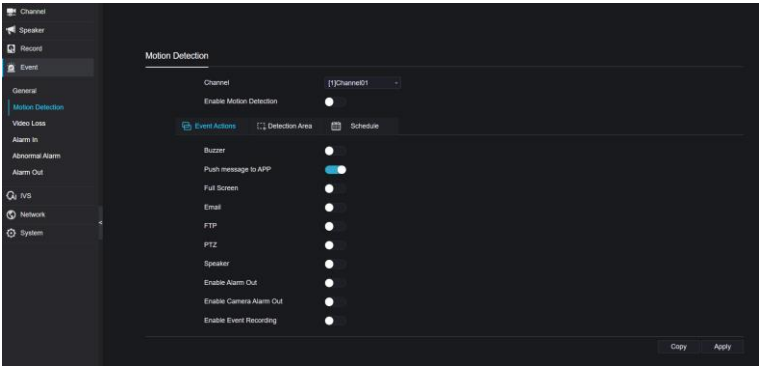
----End

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



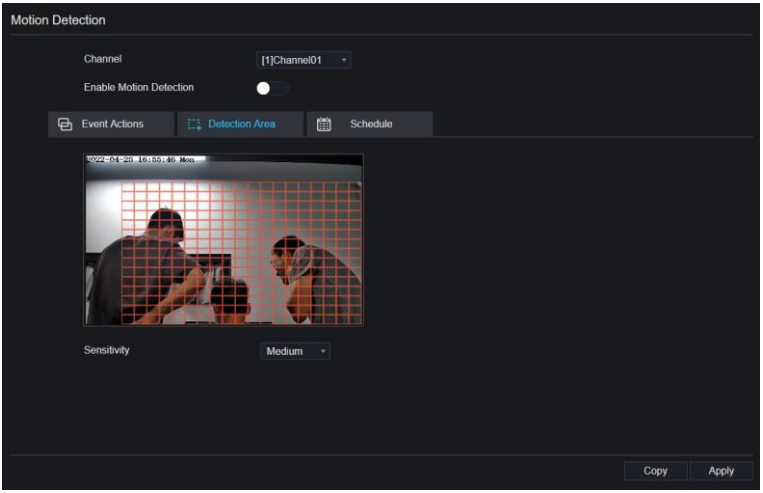
Step 2 Click the channel drop-down list to choose a channel.

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



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

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.

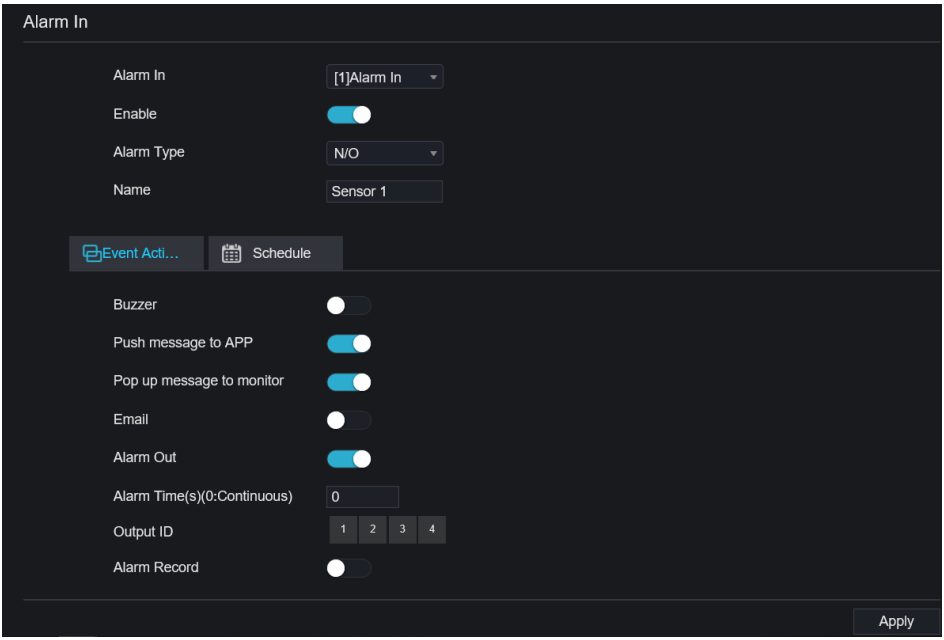
----End

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



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.

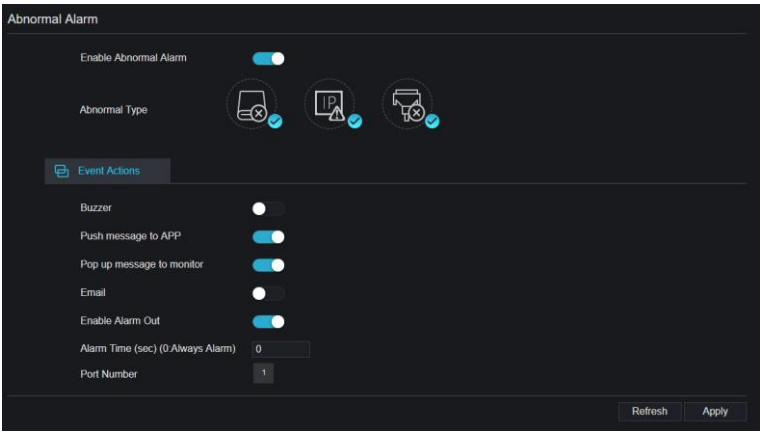
----End

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 5-20.

Figure 8-35 Abnormal alarm interface



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

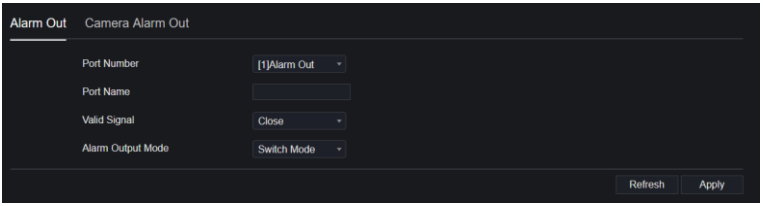
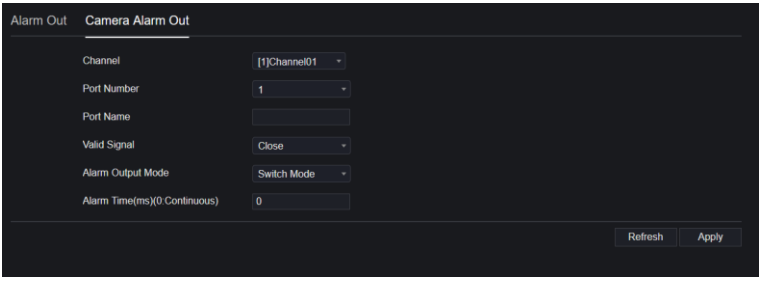


Figure 8-37 Camera alarm out

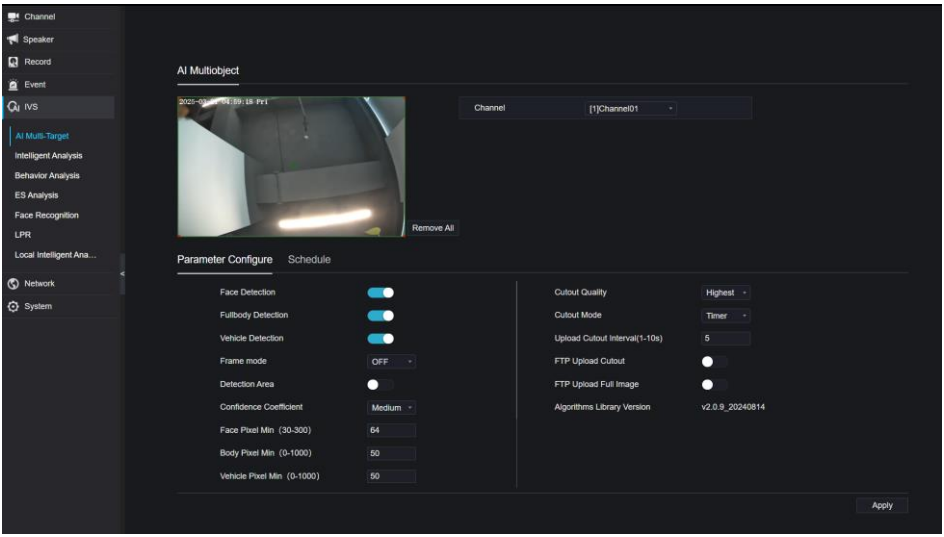


8.5 IVS

On the IVS interface, users can set the AI Multi-Target, Intelligent Analysis, Behavior Analysis, ES Analysis, Face Recognition, LPR, and Local Intelligent Analysis. For detailed information, please refer to *Chapter 6.5 IVS Configuration*.

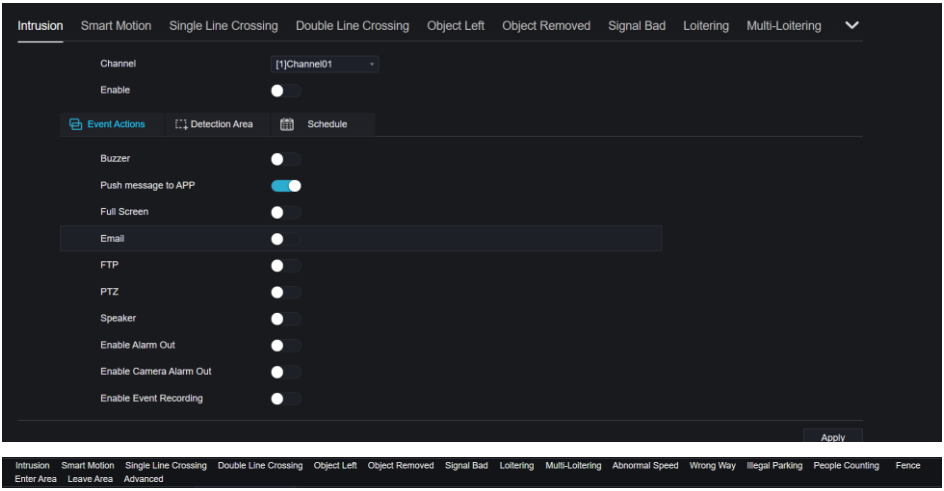
8.5.1 AI Multi-Target

Figure 8-38 AI Multi-Target



8.5.2 Intelligent Analysis (Only for Some Models)

Figure 8-39 Intelligent analysis interface



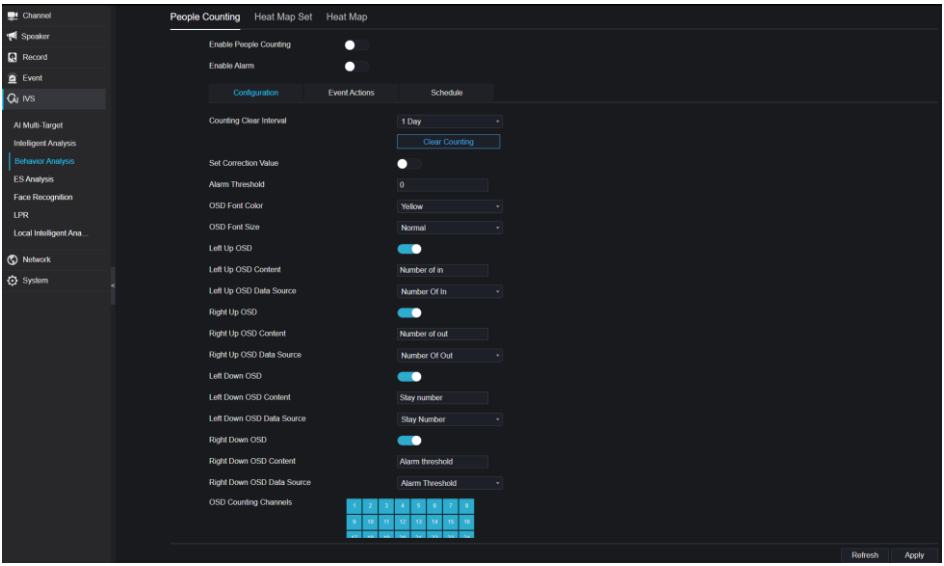
8.5.3 Behavior Analysis

On the Behavior Analysis interface, users can set the people counting of the NVR and heat map.

For detailed information, please refer to *Chapter 6.5.3 Behavior Analysis*.

8.5.3.1 People Counting

Figure 8-40 People counting



8.5.3.2 Heat Map

Figure 8-41 Heat map set

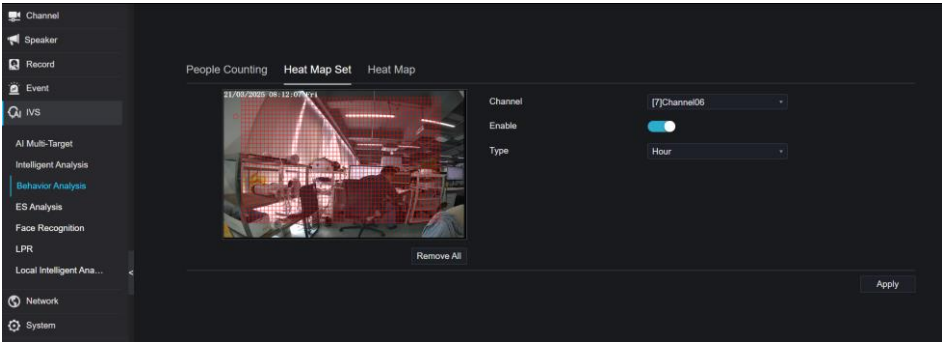


Figure 8-42 Heat map

8.5.4 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 6.5.4 ES Analysis*.

8.5.5 Face Comparison

At the comparison configuration interface, users can set the comparison of human face/license plate/temperature.

Figure 8-43 Face comparison

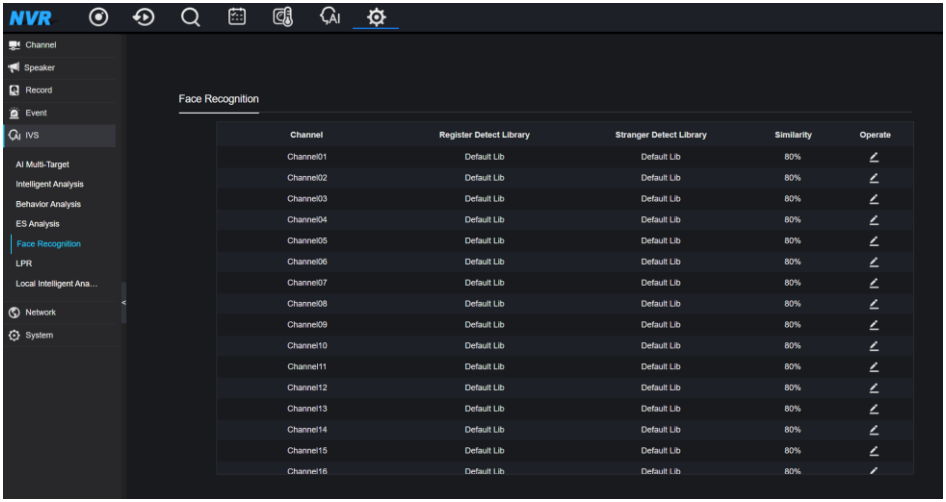


Figure 8-44 Edit Strategy

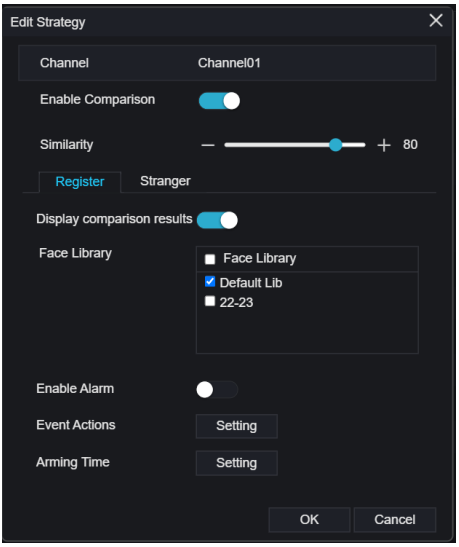


Figure 8-45 Event actions

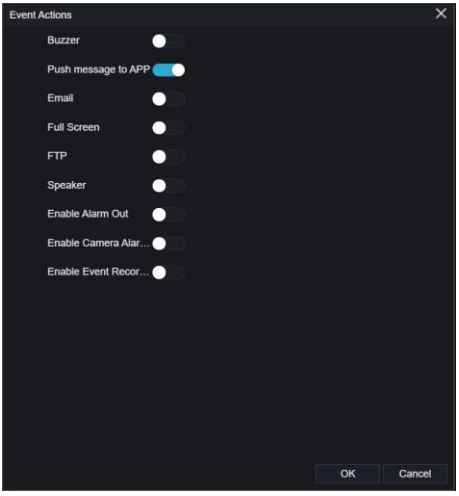
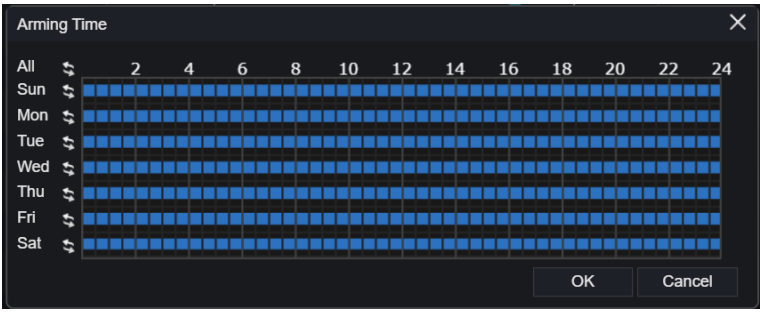


Figure 8-46 Arming time



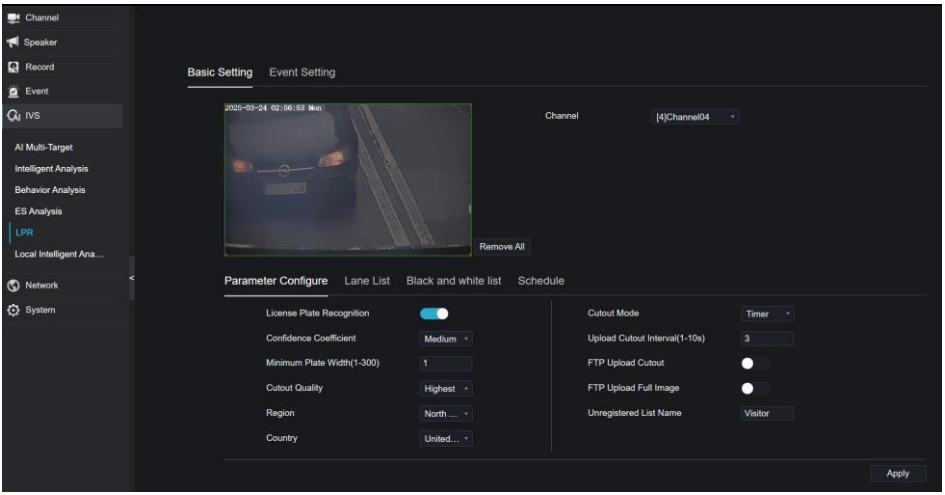
At the Face Comparison interface, users can set different channels' strategies, such as similarity, display comparison results, face library, enable alarming, event action, and schedule, as shown in Figure 6-71.

8.5.6 LPR

8.5.6.1 Basic Setting

For detailed information, please refer to *Chapter 6.5.6 LPR(License Plate Recognition).*

Figure 8-47 License Comparison



At the License Plate interface, users can set strategies for different channels of license plate recognition cameras, such as register and unregister, enabling alarming, event action, and schedule, as shown in Figure 8-47.

Figure 8-48 Event setting

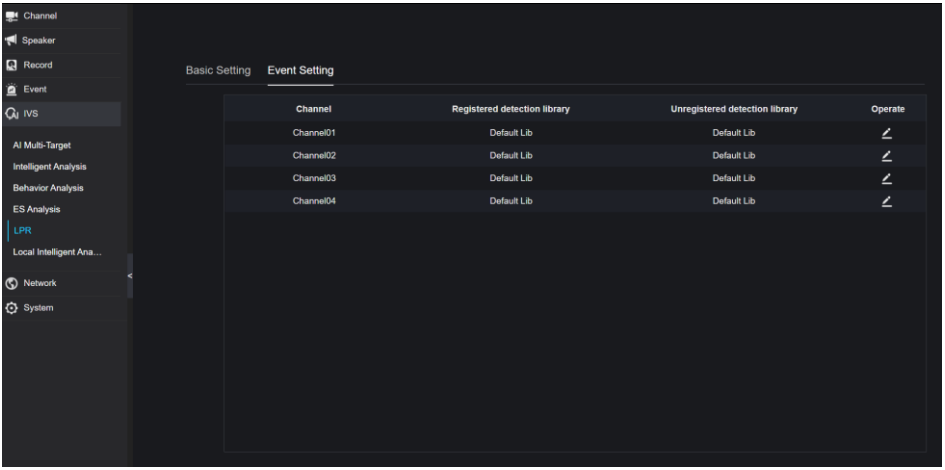
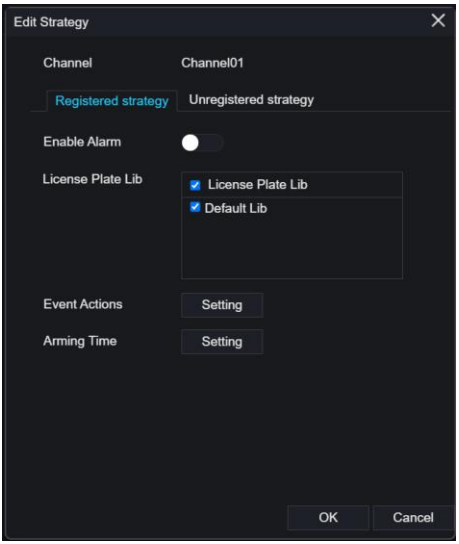


Figure 8-49 Edit strategy



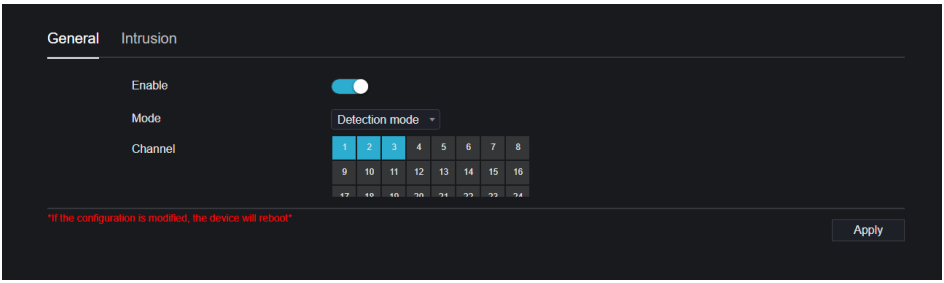
means the library is deleted.

----End

8.5.7 Local Intelligent Analysis

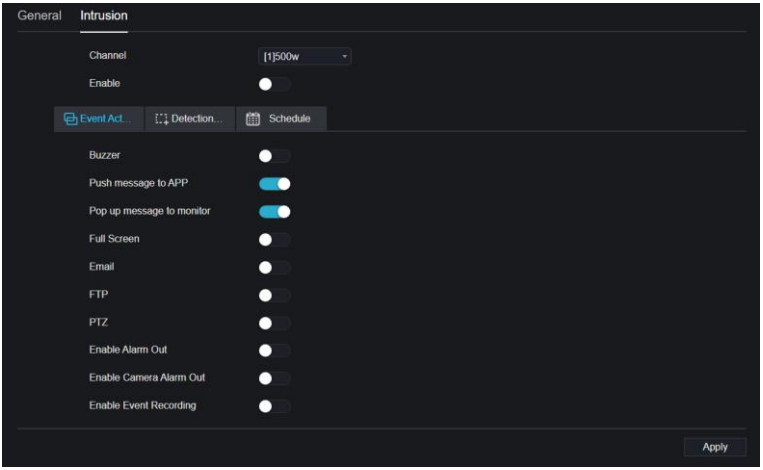
At the Local Intelligent Analysis interface, users can enable and set the mode to detection mode, and choose less than 4 channels to enable intrusion. The chosen channel devices should be AI multi-object cameras.

Figure 8-50 Local intelligent analysis



If the mode is set to recognize mode, the AI icon and Attendance icon will show on the top of the interface; otherwise, it will be hidden.

Figure 8-51 Intrusion



8.6 Network

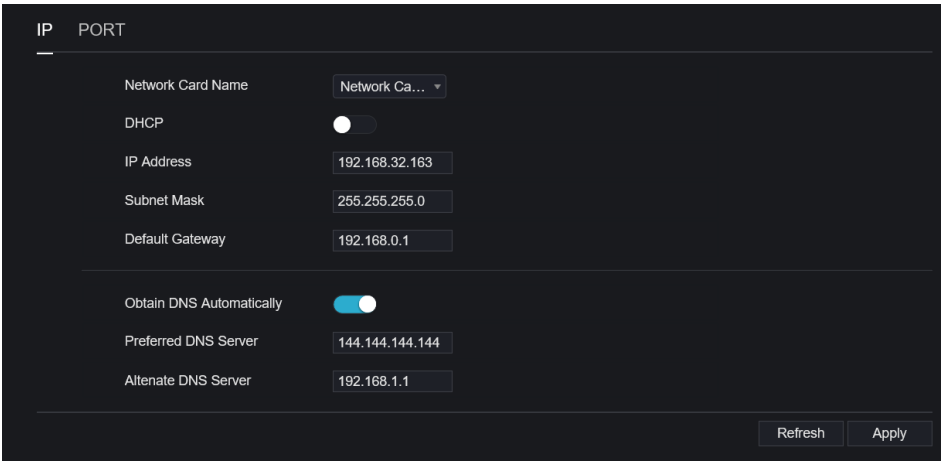
Users can set Network, DDNS, E-mail, UPnP, P2P, IP Filter, 802.1X, SNMP, and Web Mode.

8.6.1 Network

Procedure

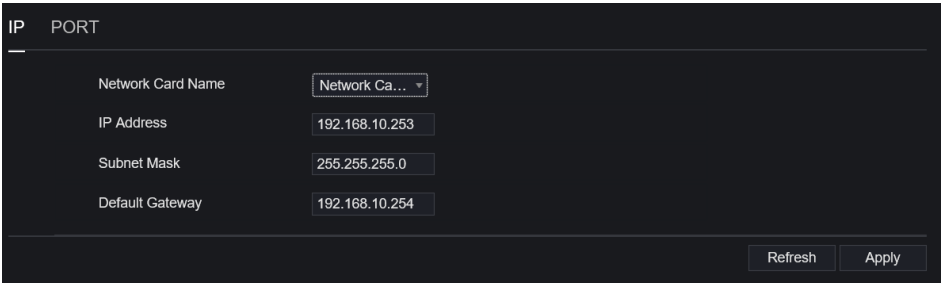
Step 1 On the **System Setting** screen, choose **Network > Network** to access the network interface, as shown in Figure 8-52.

Figure 8-52 Network interface



Step 2 Choose a network card from the drop-down list. Network card I is LAN1, and network card II is LAN2, as shown in Figure 8-53.

Figure 8-53 Network card II



Step 3 Click  next to **IP** to enable or disable the function of automatically getting an IP address. The function is enabled by default.

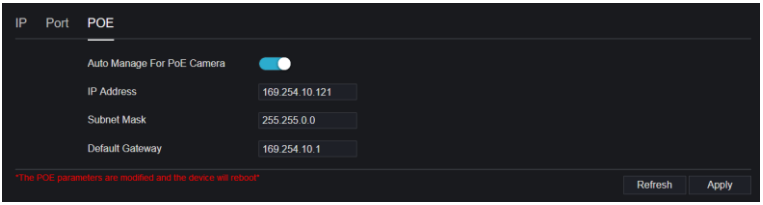
If the function is disabled, click the input boxes next to **IP**, **Subnet Mask**, and **Gateway** to set the parameters as required.

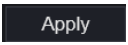
Step 4 Click  next to **Obtain DNS Automatically** to enable or disable the function of automatically getting a DNS address. The function is enabled by default.

If the function is disabled, click the input boxes next to **DNS1** and **DNS2**, delete the original addresses, and enter new addresses.

Step 5 Set **PORT** and **POE** manually, and input the information about these.

Figure 8-54 POE



Step 6 Click  to restore previous settings. Click  to save the settings.

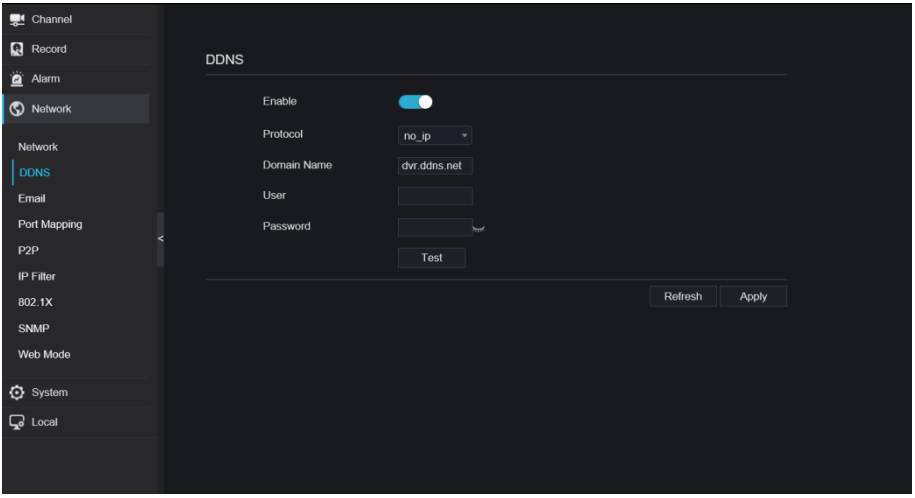
----End

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 8-55.

Figure 8-55 DDNS interface



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 NVR.

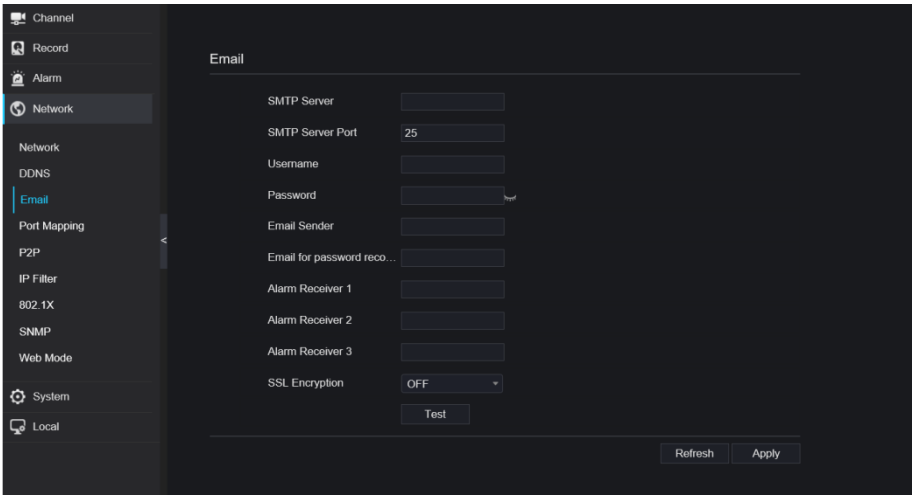
----End

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 8-56

Figure 8-56 Email interface



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

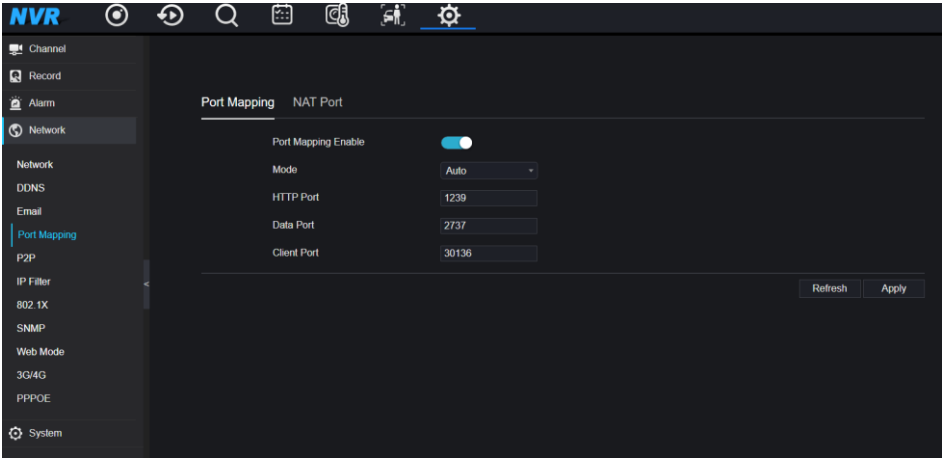
8.6.4 Port Mapping

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 8-57.

Figure 8-57 Port Mapping interface



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.

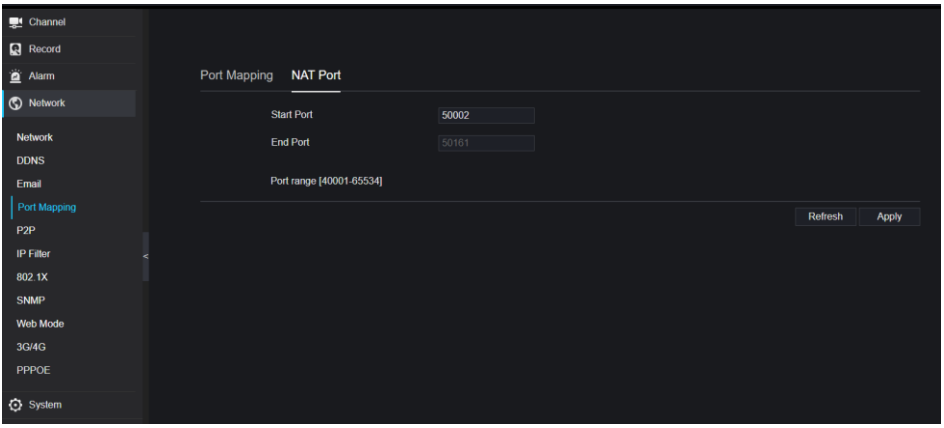
NOTE

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 8-58 NAT port



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

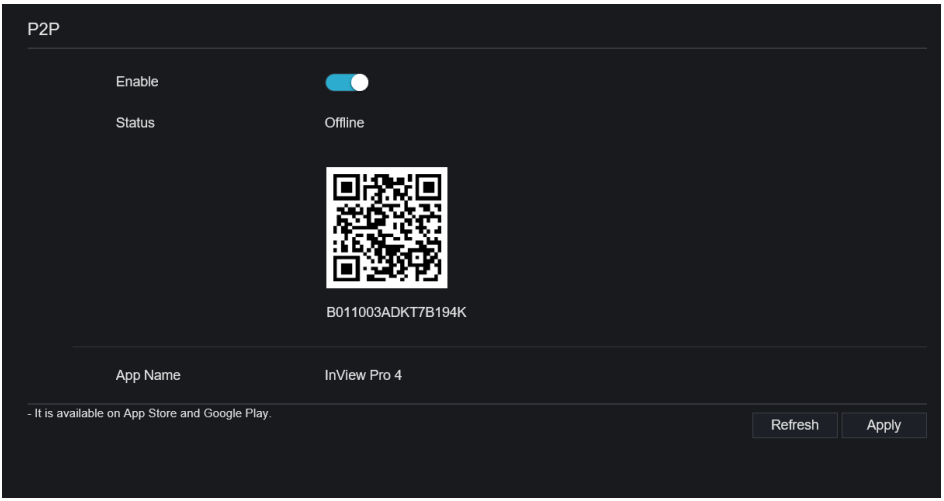
8.6.5 P2P

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 8-59.

Figure 8-59 P2P interface



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 InView Pro 4 on a mobile phone, run the app and scan the UUID QR code to add it. And then access the NVR 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 8-60 Web NAT

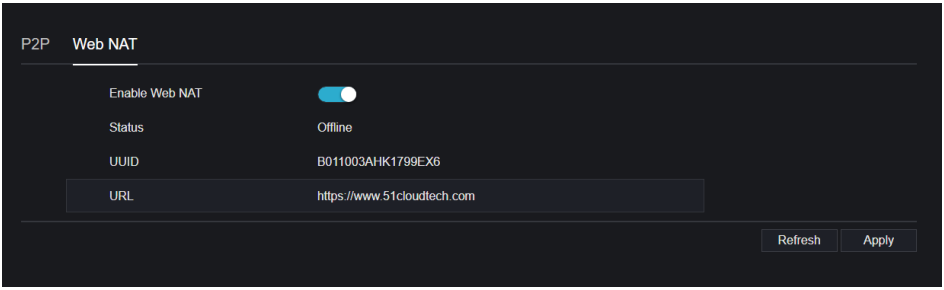
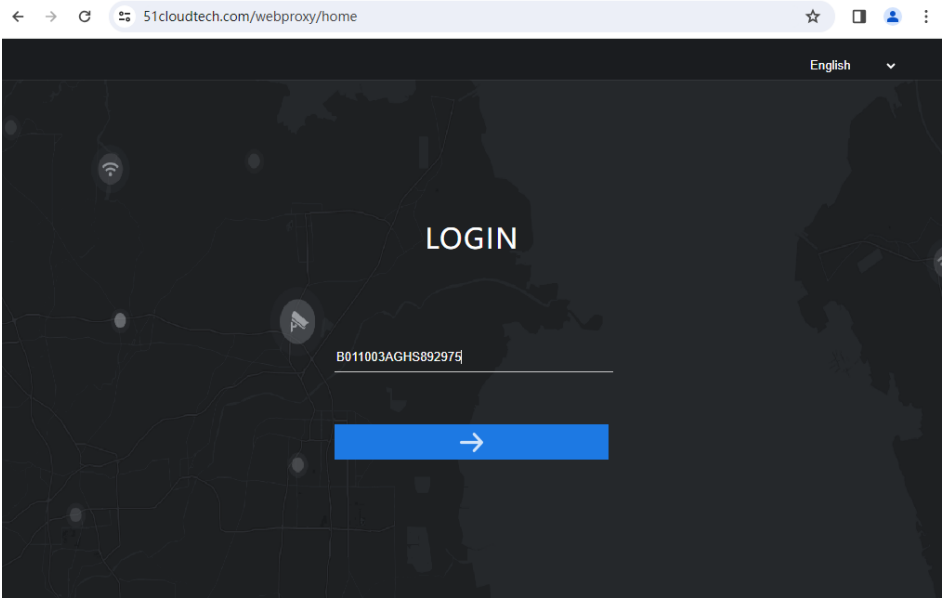


Figure 8-61 URL interface



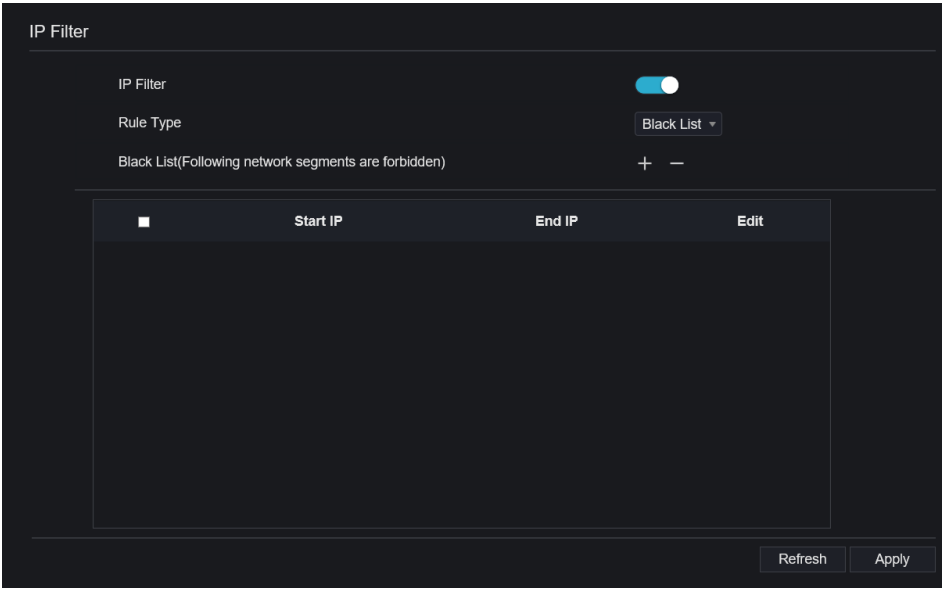
At the login interface, input the UUID of the NVR, and click Enter to enter the web interface of NVR.

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 8-62.

Figure 8-62 IP filter interface



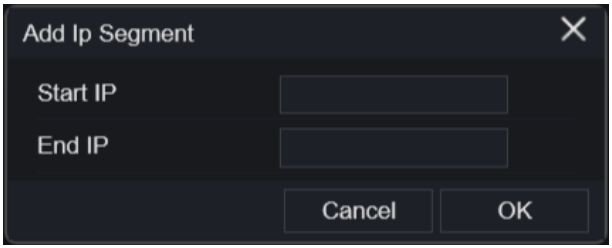
Step 2 Click **Enable** to enable the IP filter function.

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 8-63 Black or white list interface



Step 5 Set start IP and end IP.

Step 6 Click  to deny settings, and click  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.

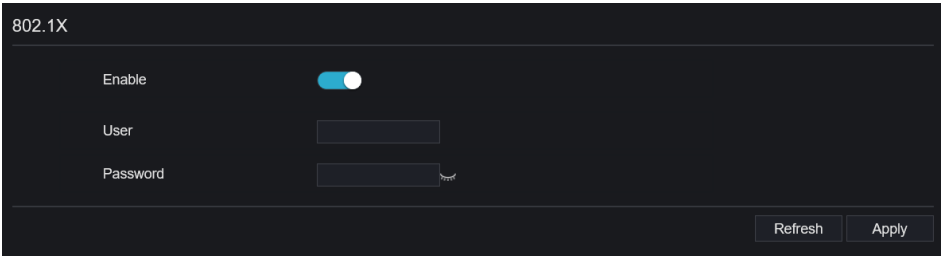
----End

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 8-64.

Figure 8-64 802.1X 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.

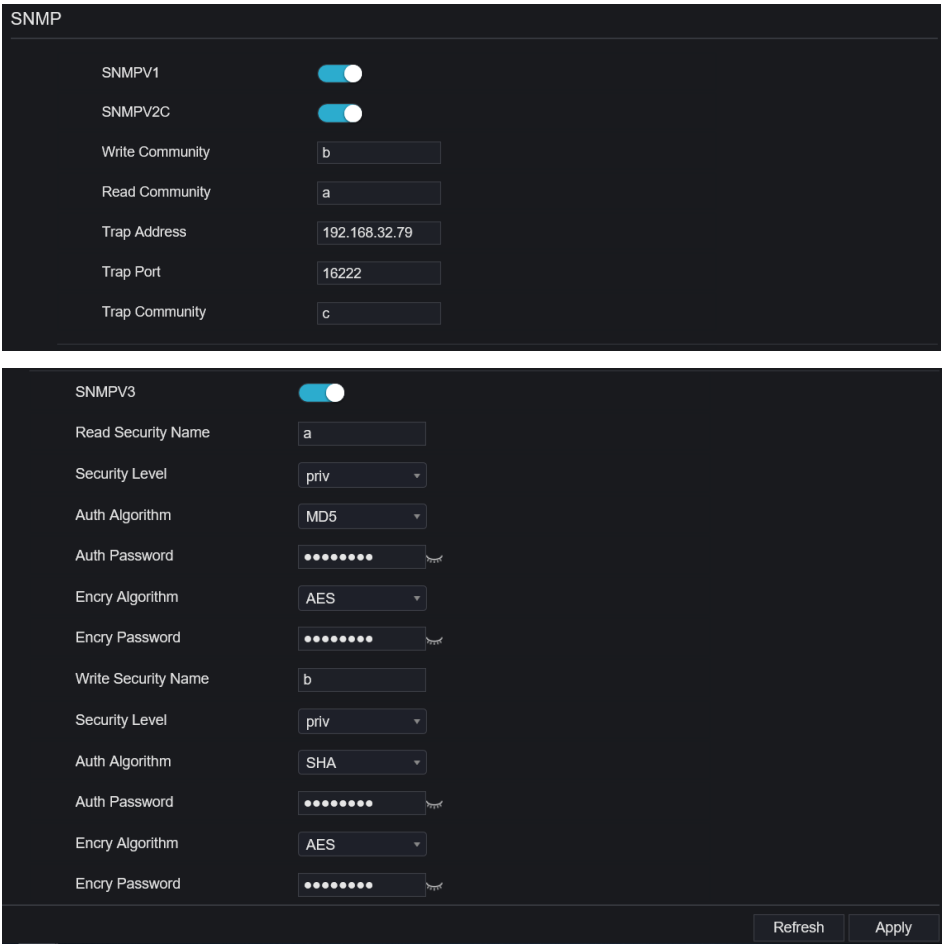
----End

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 8-65.

Figure 8-65 SNMP interface



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

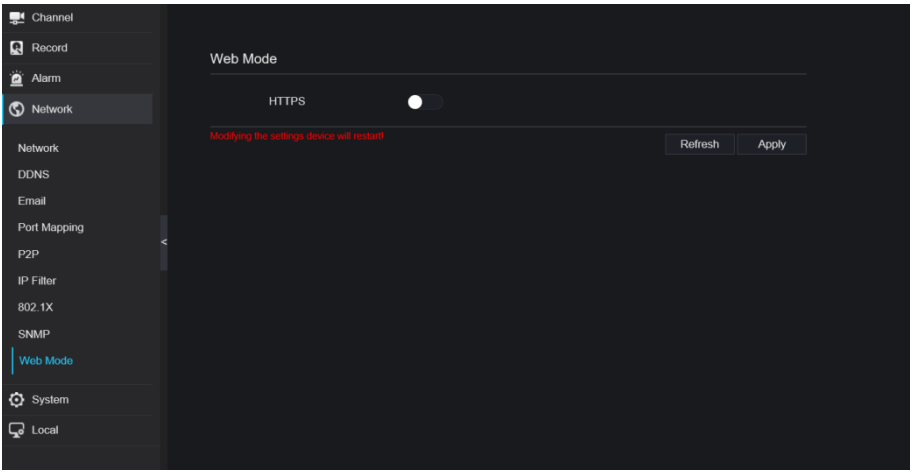
Step 3 Click Refresh to restore previous settings. Click Apply to save the settings.

----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 8-66 Web mode interface



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

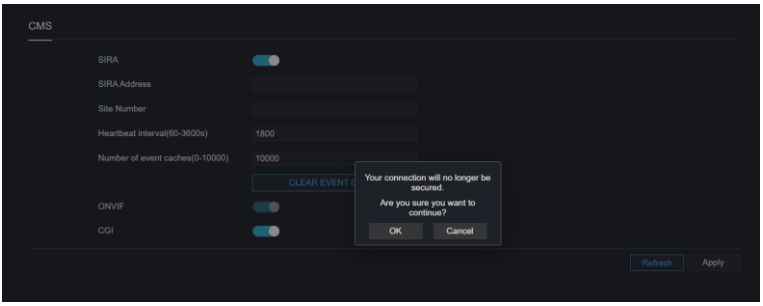
If the user wants to access the NVR via SIRA, ONVIF, or CGI, you can enable these. Enable the SIRA; the ONVIF is enabled automatically. The security of NVR will be reduced, so users should make sure of these actions.

SIRA: The server, the NVR, will sync the time and send some alarm information to this server.

ONVIF: Open Network Video Interface Forum. Users can access the NVR via the ONVIF protocol.

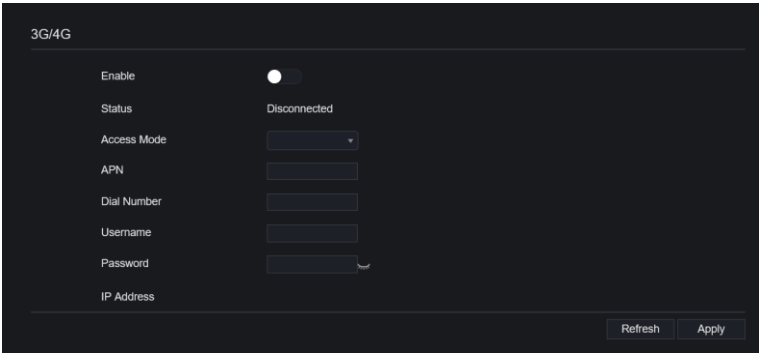
CGI: Common Gateway Interface. Users can access the NVR via CGI command.

Figure 8-67 CMS



8.6.11 3G/4G

Figure 8-68 3G/4G



Step 1 The user plugs the modem into NVR.

Step 2 Enable the 3G/4G.

Step 3 When the status is connected, users can set the access mode. AUTO is recommended.

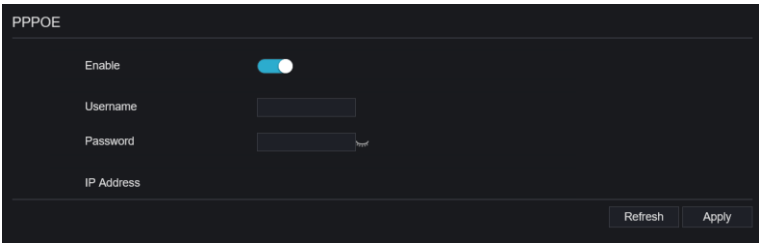
Step 4 If choosing another access mode, users should input the parameter correctly.

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 NVR conveniently.

Figure 8-69 PPPOE



Step 1 Enable the PPPOE.

Step 2 Input the username and password.

Step 3 The IP address is obtained automatically.

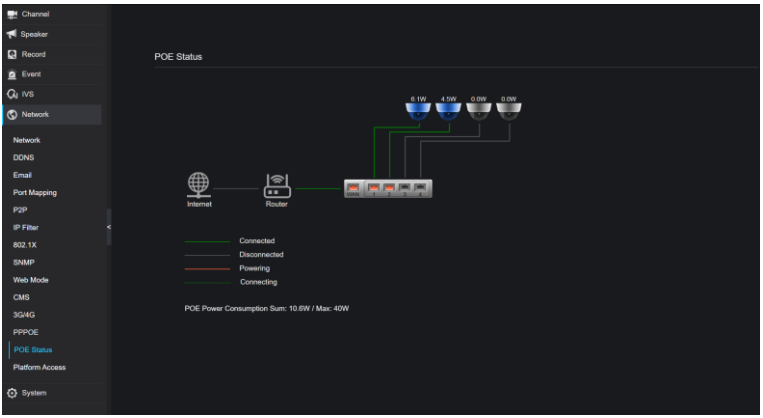
Step 4 Click Refresh to restore previous settings. Click Apply to save the settings.

Step 5 Users can use the IP address to access NVR immediately.

8.6.13 POE Status (Only for Some Models)

Users can view the POE status at this interface, as shown in Figure 8-70.

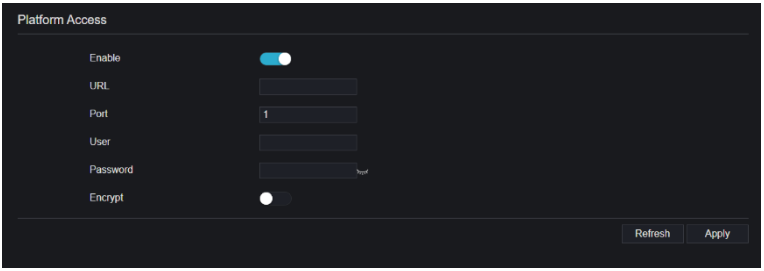
Figure 8-70 POE status



8.6.14 Platform Access

For more details, please refer to the UI interface parameter setting *6.6.13 Platform Access*.

Figure 8-71 Platform access

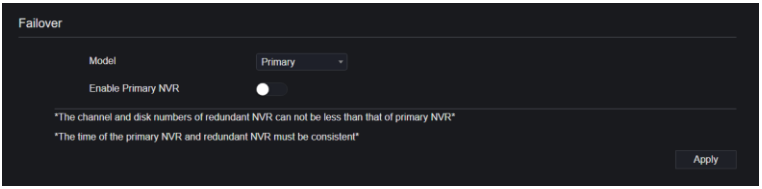


8.6.15 Failover

If users want to keep all recordings working normally, set the NVR to act as a redundant NVR. When the primary NVRs are broken down, the redundant NVR can keep working as a failover.

For more details, please refer to UI interface parameter settings *6.6.14 Failover*.

Figure 8-72 Failover



8.7 System

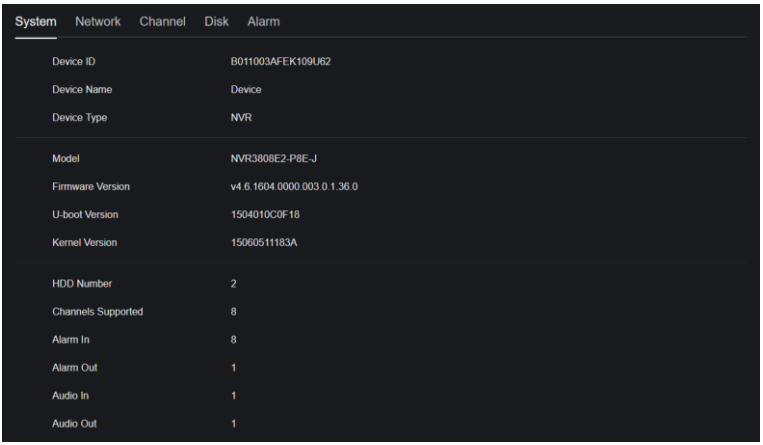
Users can set parameters about information, general, user, password, logs, maintenance, and auto restart.

8.7.1 Device Information

Procedure

Step 1 Click  on the navigation bar, and the device information interface is displayed, as shown in Figure 8-73.

Figure 8-73 Device information interface



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		
Alarm in		
Alarm out		
Audio in		
Audio out		

Figure 8-74 Network

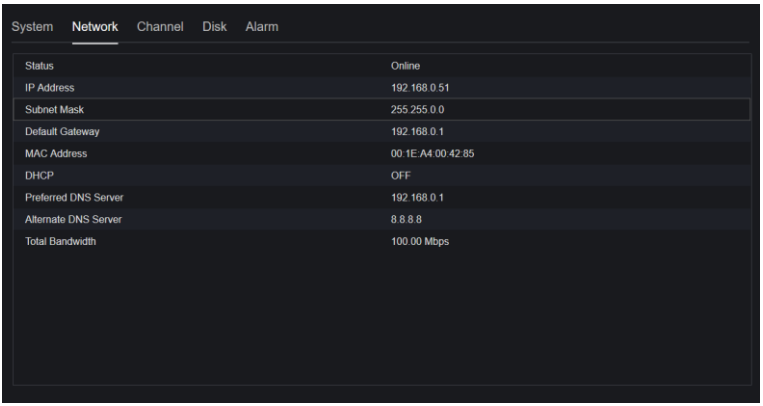


Figure 8-75 Channel

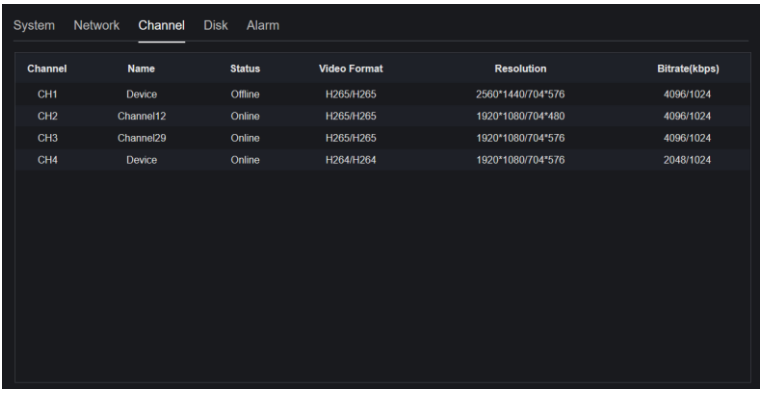


Figure 8-76 Disk

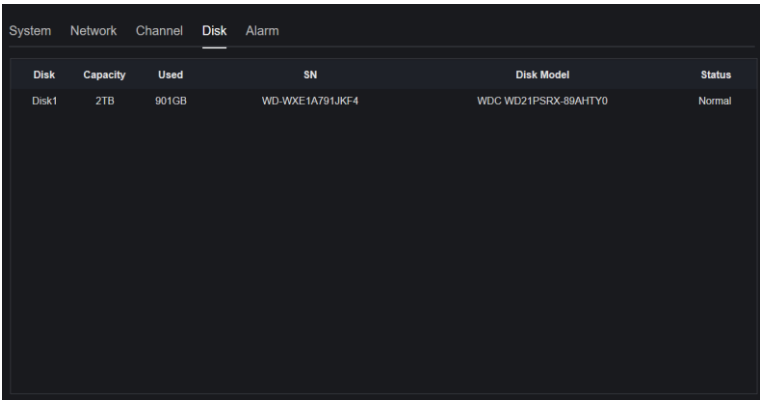
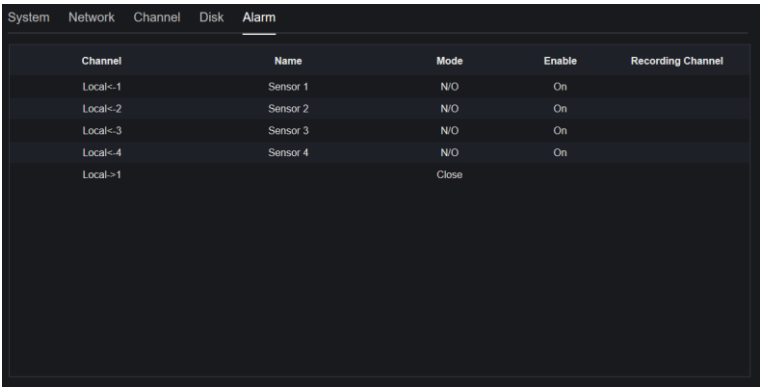


Figure 8-77 Alarm



----End

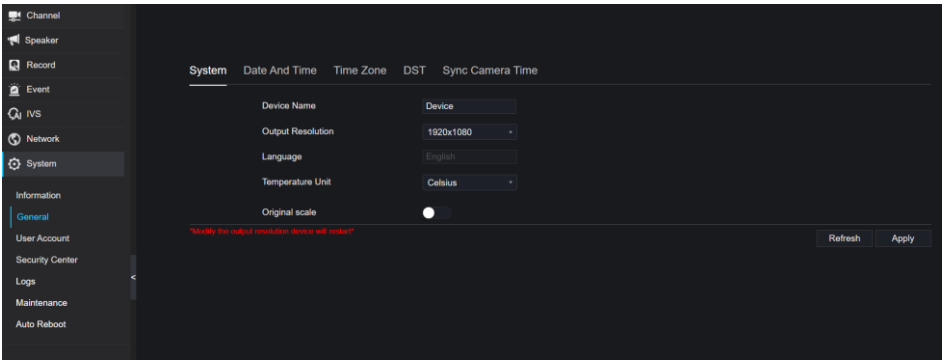
8.7.2 General

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 8-78.

Figure 8-78 Basic setting interface



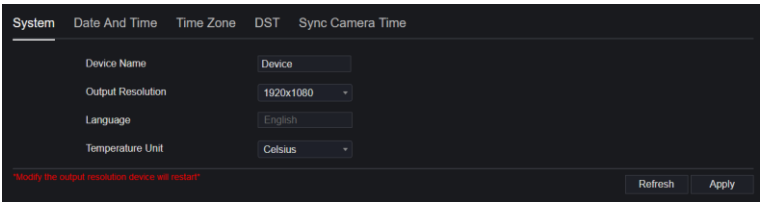
Step 2 Set the system.

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.

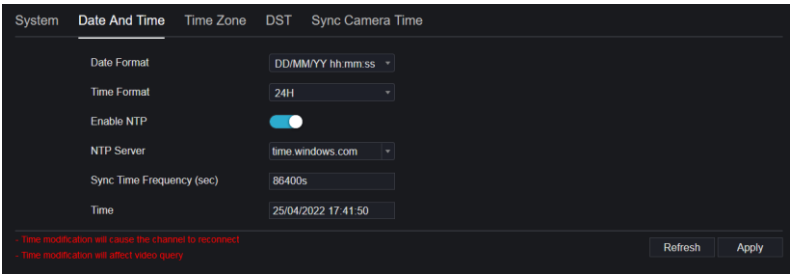
Figure 8-79 System interface



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 8-80.
6. Click the NTP Sync button to disable time synchronization.

7. Async date and time interface.

Figure 8-80 Date and time



Step 4 Set the time zone.

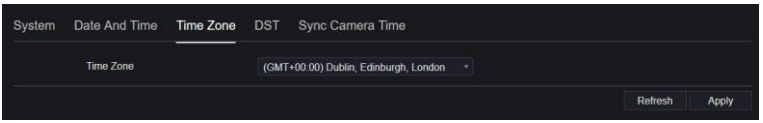
1. Select the date format and time format from the drop-down list.

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 8-81.
Time zone setting interface

Figure 8-81 Time zone



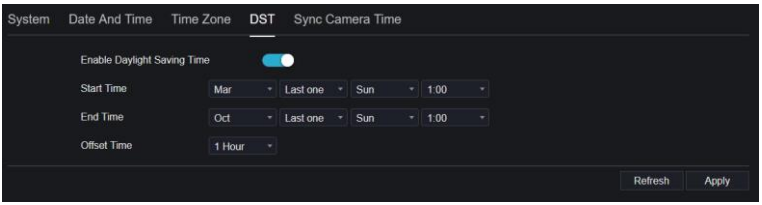
Select a time zone from the drop-down list.

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 8-82. The button is disabled by default.

Figure 8-82 DST setting interface

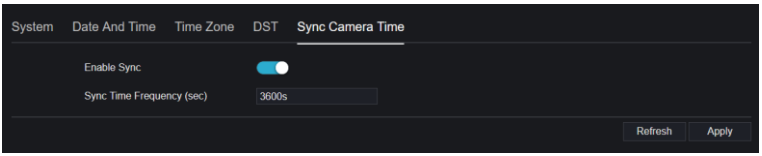


Select a start time from the drop-down list.

Select an end time from the drop-down list.

Select an offset time from the drop-down list.

Figure 8-83 Sync camera time



Enable sync camera time, and the cameras of NVR 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

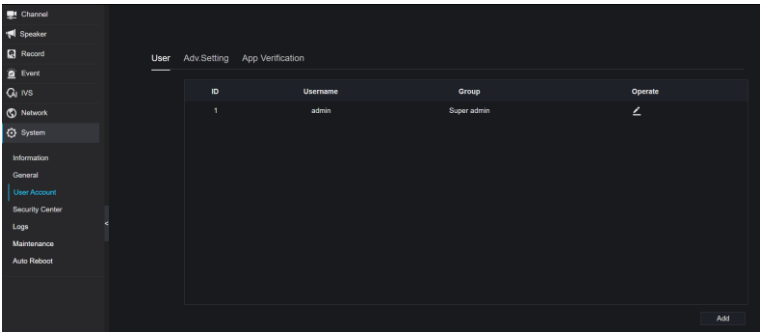
You can create new user accounts to manage the device.

8.7.3.1 Add User

Procedure

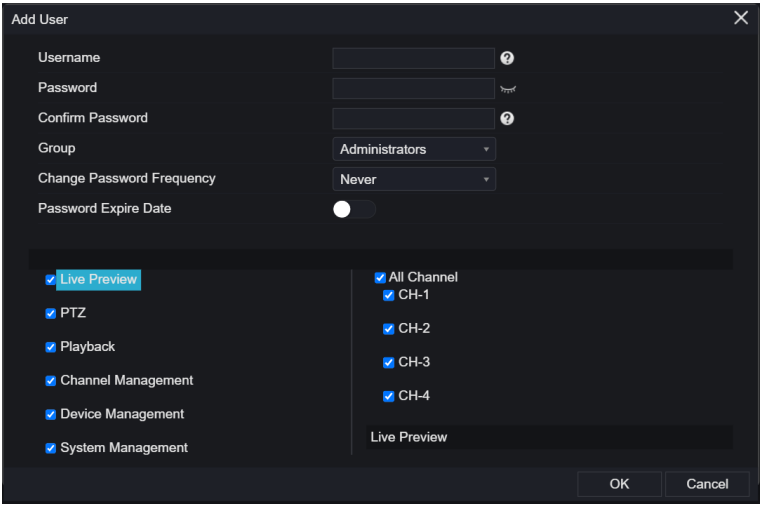
Step 1 On the **System Setting** screen, choose **System > User** to access the **User** interface, as shown in Figure 8-84.

Figure 8-84 User interface



Step 2 Click **Add** to add a new user, as shown in Figure 8-85.

Figure 8-85 Add user



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.

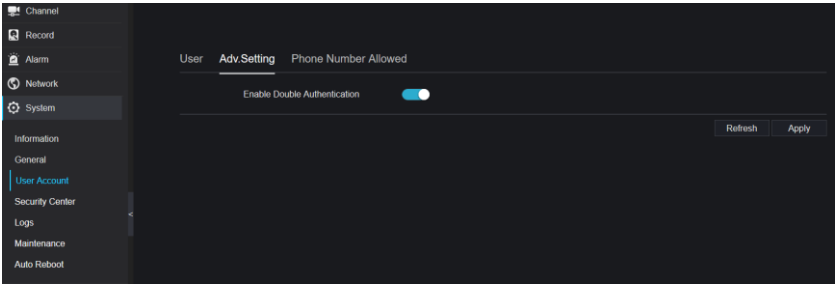
----End

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 8-86 Adv. Setting interface



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.

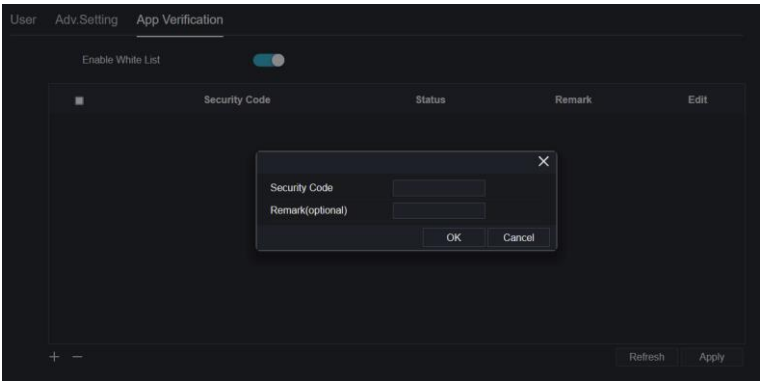
Step 3 Click Apply to save the device time setting. Click Refresh to return to the previous setting.

----End

8.7.3.3 App Verification

Add the digital number to the white list. When the user logs into the cellphone app to manage the NVR, a series of numbers must be added to the whitelist for testing and verification to ensure security.

Figure 8-87 App Verification



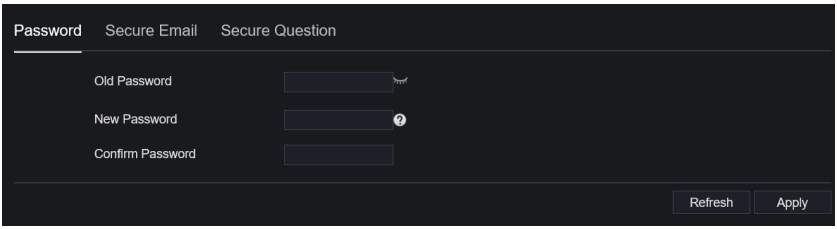
8.7.4 Security Center

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 8-88.

Figure 8-88 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.

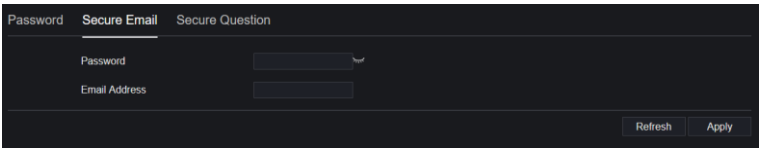
Only these special characters are supported ！ @#&*+=-%&”`(),/’.:;< >?^|~[]{}.

----End

8.7.4.2 Secure Email

The secure email can receive the verification code of NVR if the user forgets the password accidentally.

Figure 8-89 Secure Email

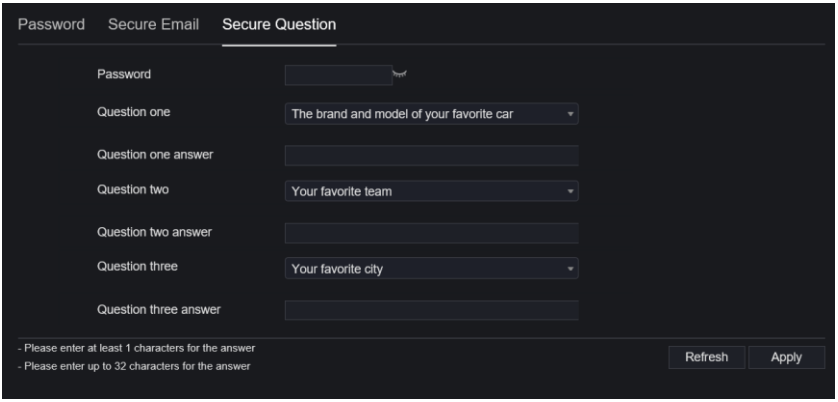


----End

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 NVR.

Figure 8-90 Secure question



----End

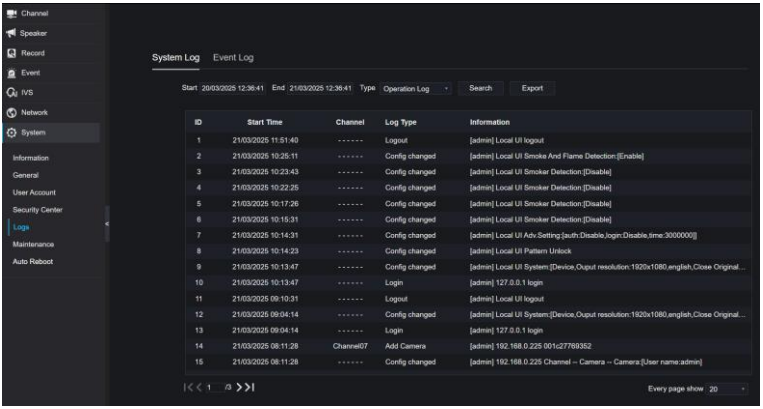
8.7.5 Logs

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 8-91.

Figure 8-91 System log interface



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.

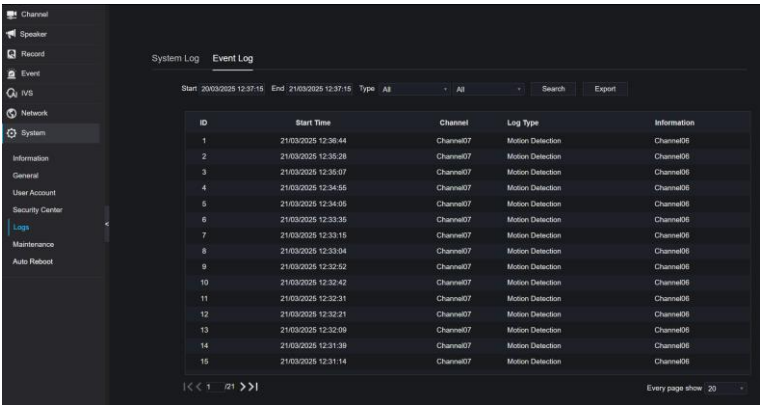
----End

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 8-92.

Figure 8-92 Event log interface



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

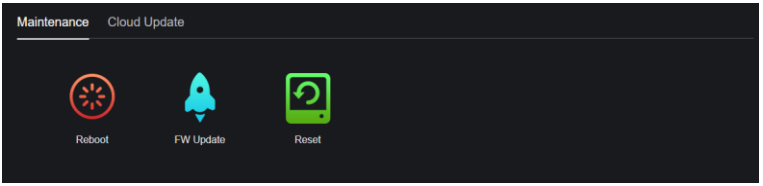
8.7.6 Maintenance

8.7.6.1 Maintenance

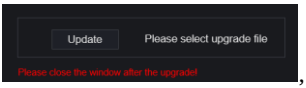
Procedure

Step 1 On the **System Setting** screen, choose **System >Maintenance** to access the maintenance interface, as shown in Figure 8-93.

Figure 8-93 Maintenance interface



Step 2 Click **Reboot**. The pop-up message will show you, click OK to reboot.

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 

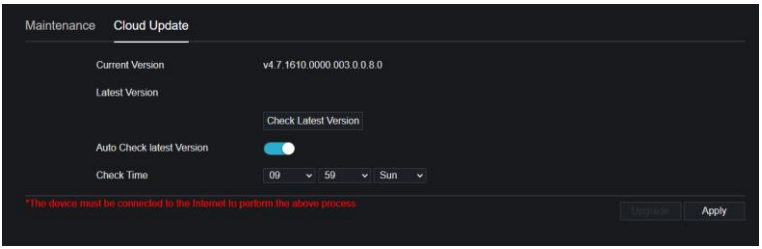
to reset.

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 8-94 Cloud update



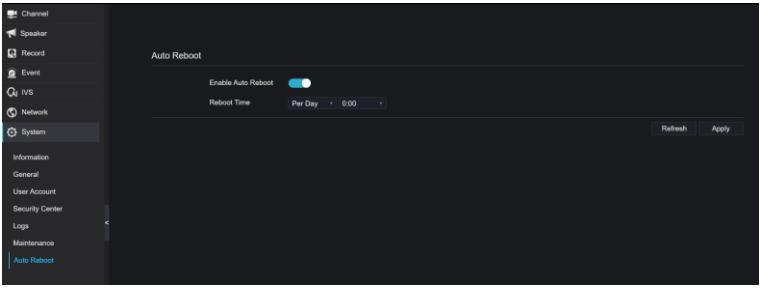
----End

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 8-95.

Figure 8-95 Auto restart



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)