

User Manual

Network Video Recorder (NVR)

BNR-004 / BNR-008

About This Document

Purpose

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

Symbol Conventions

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

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

About This Document	ii
Contents.....	iii
1 Product Structure.....	8
1.1 Back Panel	8
1.2 Hard Disk Installation	9
2 Basic Operations	11
2.1 Power on the Device.....	11
2.2 Activation	12
2.3 Wizard	16
2.4 Power off the Device	25
2.5 Login to the System.....	25
3 Quick Navigation	27
3.1 Quick Bar	27
3.2 Real-Time Video Bar	33
3.3 Playback	35
3.3.1 Time Search.....	38
3.3.2 Picture Grid	39
3.3.3 Event Recording.....	41
3.3.4 Backup List	43
3.4 Channel Information.....	43
3.5 Main Menu	44
4 System Setting	45
4.1 Channel Management.....	45
4.1.1 Camera	45
4.1.2 Encode Parameter.....	52
4.1.3 Image.....	53
4.1.4 OSD Settings	55
4.1.5 Privacy Zone	56
4.1.6 ROI.....	57

4.1.7 Audio	59
4.1.8 Intelligent Tracking	64
4.2 Speaker	66
4.2.1 Speaker Management	66
4.3 Record-Setting.....	68
4.3.1 Record Schedule	68
4.3.2 Disk	70
4.3.3 Storage Mode	72
4.3.4 S.M.A.R.T	73
4.3.5 Disk Detection.....	75
4.3.6 Disk Calculation.....	76
4.3.7 FTP.....	78
4.4 Event Management.....	79
4.4.1 General	79
4.4.2 Motion Detection	80
4.4.3 Video Loss.....	85
4.4.4 Alarm In	86
4.4.5 Abnormal Alarm.....	89
4.4.6 Alarm Out.....	89
4.5 IVS Configuration	95
4.5.1 Intelligent Analysis	95
4.6 Network Management	102
4.6.1 Network.....	103
4.6.2 802.1 X.....	107
4.6.3 DDNS.....	108
4.6.4 Port Mapping.....	109
4.6.5 Email	111
4.6.6 IP Filter.....	114
4.6.7 SNMP	115
4.6.8 PPPOE.....	118
4.6.9 Network Traffic.....	118
4.7 System Management	119
4.7.1 Information.....	120

4.7.2 General	123
4.7.3 User Account.....	130
4.7.4 Security Center	134
4.7.5 Layout	138
4.7.6 Logs.....	141
4.7.7 Maintenance	142
4.7.8 Auto Reboot	144
5 WEB Quick Start.....	146
5.1 Activation	146
5.2 Login and Logout	148
5.2.2 Live Video	153
5.2.3 Channel Operation	153
5.2.4 PTZ Control and Setting	154
5.2.5 Image Setting	156
5.2.6 Layout	158
5.3 Playback	159
5.3.1 Video Playback.....	159
5.4 Alarm Search.....	161
5.4.1 Channel Alarm	161
6 System Setting	163
6.1 Channel.....	163
6.1.1 Camera	163
6.1.2 Encode.....	168
6.1.3 Image.....	168
6.1.4 OSD.....	169
6.1.5 Privacy Zone	171
6.1.6 ROI.....	171
6.1.7 Audio	172
6.1.8 Intelligent Tracking	173
6.2 Speaker	173
6.2.1 Speaker Management	174
6.2.2 Local Audio Files	174
6.3 Record	174

6.3.1 Record Schedule	175
6.3.2 Disk	176
6.3.3 Storage Mode	177
6.3.4 S.M.A.R.T	178
6.3.5 Disk Calculation.....	179
6.3.6 FTP.....	180
6.4 Event.....	181
6.4.1 General	181
6.4.2 Motion Detection	181
6.4.3 Video Loss.....	183
6.4.4 Alarm In	184
6.4.5 Abnormal Alarm.....	184
6.4.6 Alarm out.....	185
6.5 IVS.....	185
6.6 Network	189
6.6.1 Network.....	189
6.6.2 DDNS.....	190
6.6.3 Email	191
6.6.4 Port Mapping.....	192
6.6.5 IP Filter.....	194
6.6.6 802.1X.....	196
6.6.7 SNMP	196
6.6.8 Web Mode	197
6.6.9 CMS	198
6.6.10 PPPOE.....	198
6.7 System	199
6.7.1 Device Information	199
6.7.2 General	202
6.7.3 User Account.....	205
6.7.4 Security Center.....	207
6.7.5 Logs.....	209
6.7.6 Maintenance	210
6.7.7 Auto Reboot	211

Regulatory Information	213
Warning	215
Battery Removal Instruction	215

1 Product Structure

1.1 Back Panel

This chapter explains the functions of all interfaces :

Figure 1-1 NVR Rear Panel

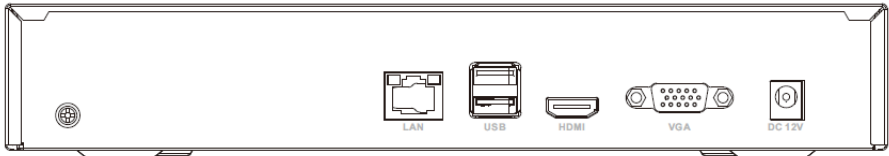
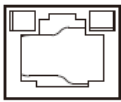
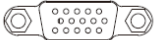


Table 1-1 Rear panel function

Port	Description
 LAN	RJ45 10/100 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.
 HDMI	HDMI/, video output interface; users use an HDMI cable to connect to the monitor.
 VGA	Video output interface; users use a VGA cable to connect to the monitor. If the device has an auxiliary screen function, the VGA will show the content of the auxiliary screen.
 USB	Only connected to Mouse or USB flash drive.

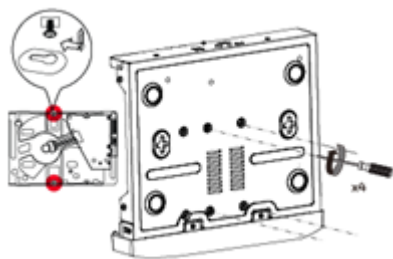
	GND, safety grounding screw.
	Connected to an external power adapter DC 12V.

1.2 Hard Disk Installation

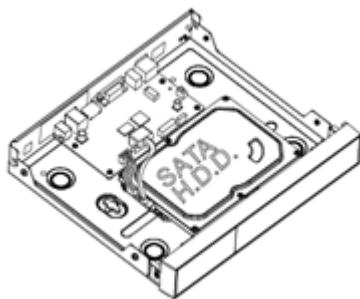
Step 1: Remove the screws on the upper cover and remove the cover.

Step 2: Remove the screws and silicone cushion, pass the screws through the silicone cushion, and secure it to the screw holes.

Step 3: Pass the screws through the holes on the base and put the hard disk in place.



Step 4: Insert the hard disk data cable and power cable.



Step 5: Replace the upper cover and fasten.



CAUTION

- Please check HDD compatibility list to know what hard disk is recommended.
- When replacing the hard disk, please **turn off the power** and then open the device to replace the hard disk.
- Please check HDD compatibility list
- Choose the hard disk capacity according to the recording requirements.



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.

2 Basic Operations

2.1 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 real-time video screen is displayed as shown in Figure 2-1.

Figure 2-1 Real-time video screen



2.2 Activation

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

Figure 2-2 Activation

The screenshot shows a dark-themed 'Activation' window. It contains the following elements:

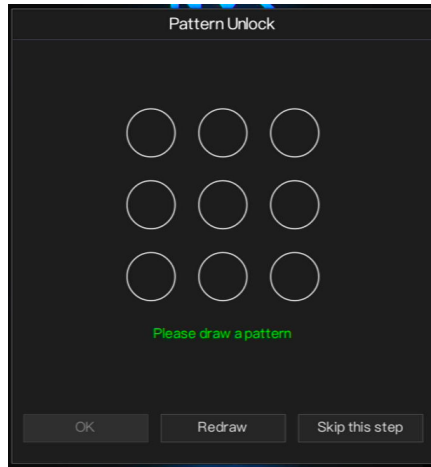
- Language:** A dropdown menu currently set to 'English'.
- Username:** A text field containing the default value 'admin'.
- Enter a new password:** A password input field with a 'Password' label and a visibility toggle.
- Confirm the new password:** A second password input field with a 'Password' label and a visibility toggle.
- Enter channel default password:** A third password input field with a 'Password' label and a visibility toggle.
- Requirements:** A list of rules for the password:
 - Valid password range [8–32] characters.
 - Must not be identical to publicly visible information such as lo.
 - At least 3 kinds of numbers, lowercase, uppercase or special .
 - Only these special characters are supported !@#*\$*+=-_%&'".
- OK Button:** A button at the bottom center to confirm the activation.

Table 2-1 Description of activation

Name	Description
Username	The default username is admin , and “admin” is super administrator.
Password	Valid password range 8-32 characters.
Confirm password	At least 3 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.
Channel default password	Enter channel default password for IP camera connection.

Users can set the pattern unlock to log in to the device, as shown in Figure 2-3.

Figure 2-3 Set pattern unlock

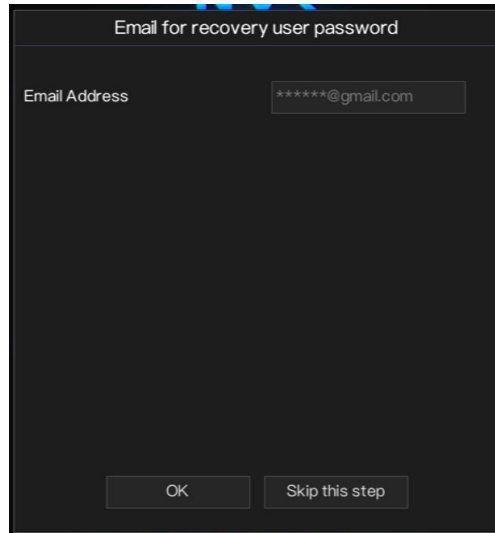


NOTE

- 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 2-4.

Figure 2-4 Set Email



Email for recovery user password

Email Address *****@gmail.com

OK Skip this step



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 reseller to get **the temporary password** and 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 2-5 Set question

Question (Recovery the password)

Question one The brand and model of. ▾

Question one answer

Question two Your favorite team ▾

Question two answer

Question three Your favorite city ▾

Question three answer

- Please enter at least 1 characters for the answer

- Please enter up to 32 characters for the answer

OK Skip this step

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
- The three question options cannot be set to the same issue.
- The answer requires a minimum of 1 character and a maximum of 32 characters.
- If you do not want to set a password question, you can click Skip this step.

2.3 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 2-6.

Figure 2-6 Setup Wizard

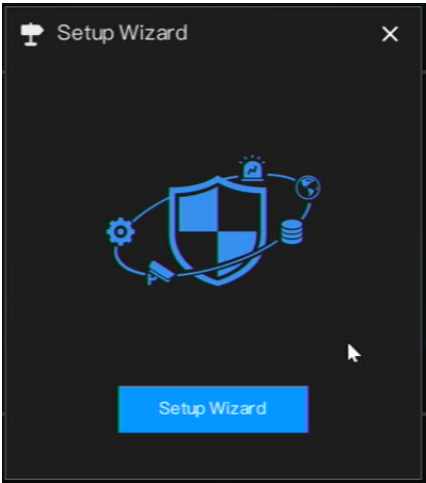
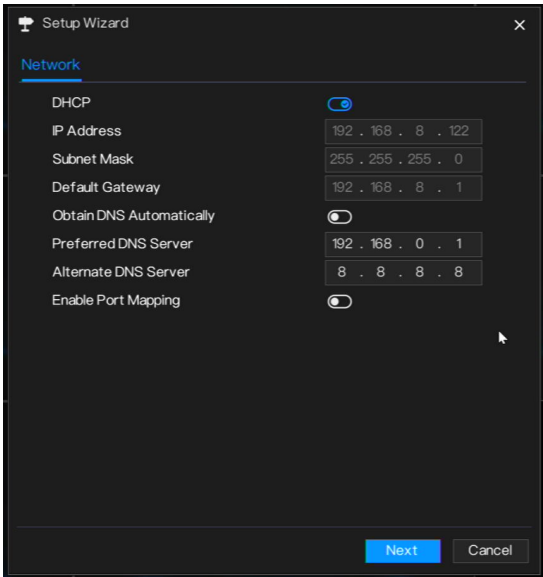


Figure 2-7 Network Setting



Step 1 Contains the parameter, details please refer to Table 2-1.

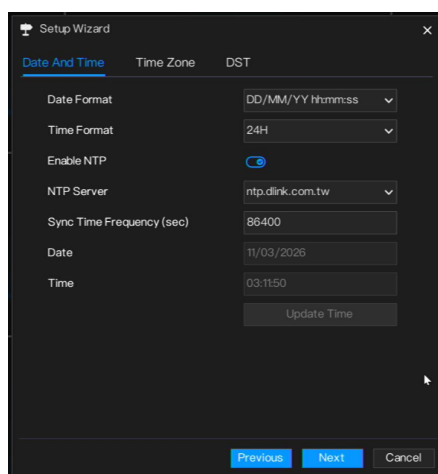
Table 2-1 Network setting parameter

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

Parameter	Description	Configuration
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 Date and Time settings, as shown in Figure 2-88.

Figure 2-8 Date and time setting



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

Enable NTP:

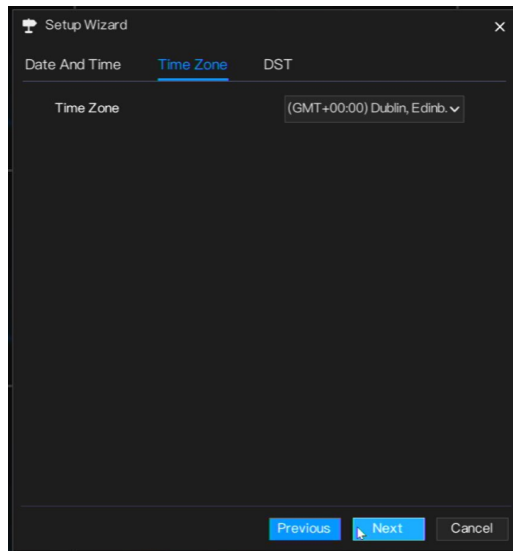
- Click  to synchrony time from the network.

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.

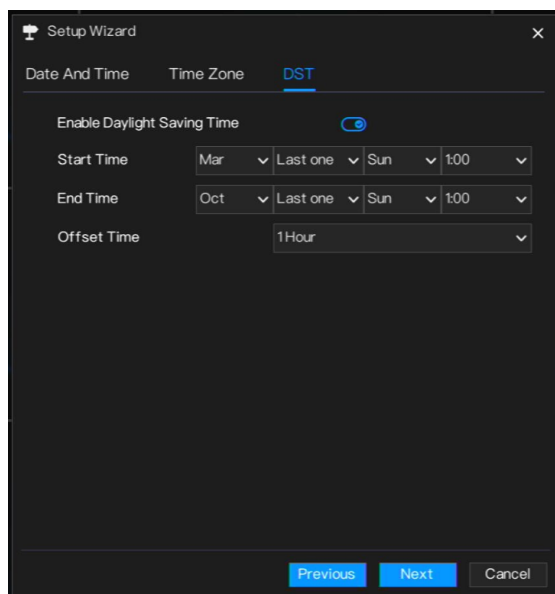
Step 3 Click **Time Zone**, and choose the current time zone from the drop-down list as shown in Figure 2-99.

Figure 2-9 Time zone setting



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

Figure 2-10 DST setting



Step 5 Click **Next** to enter the adding camera wizard, as shown in Figure 2-111.

Figure 2-11 Adding camera

Setup Wizard

Camera

☐	Channel	IP	Model	Protocol	Operate
☒	CH1	---	---	--	+
☒	CH2	---	---	--	+
☒	CH3	---	---	--	+
☒	CH4	---	---	--	+

Delete Add Devices Stop Search(16s)

☐	IP	Model	Protocol	Firmware Version
☐	192.168.8.135:30001	DCS-4618E	Private	v10122
☐	192.168.8.134:30001	DCS-4618E	Private	v10122
☐	192.168.8.133:30001	DCS-4718E	Private	v10132
☐	192.168.8.131:30001	DCS-4712E	Private	v100.11

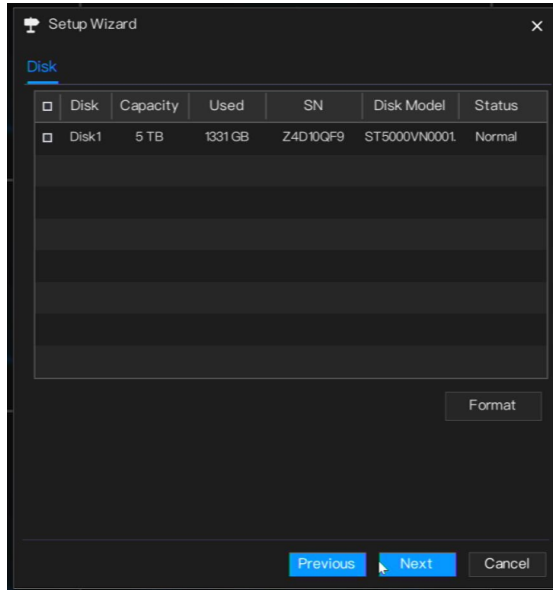
Username admin Password Password Add

Previous Next Cancel

For the details of adding cameras please refer to *chapter 4.1*

Step 6 Click **Next** to enter the wizard of disk, as shown in Figure 2-122.

Figure 2-12 Disk setting

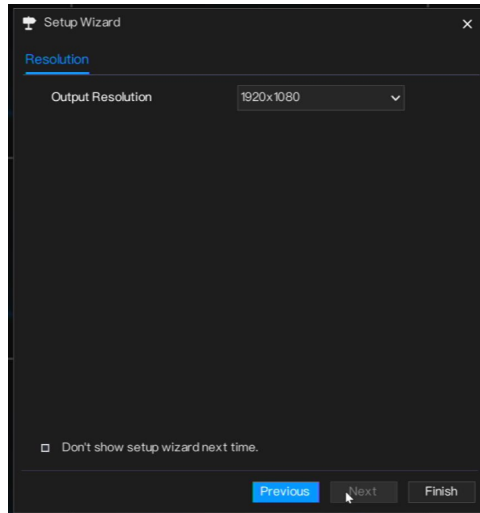


You can view the general information about the disk. You can also format the disk. If you plug the disk into the device for the first time, you must format the disk.

Step 7 Click **Next** to enter the wizard of resolution, as shown in Figure 2-133. 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 2-13 Resolution setting



Step 8 Click **Finish** to end the wizard, click the **Don't show setup wizard next time**, it would not show at next time. Reopen the wizard at **System > User > Advance setting**.

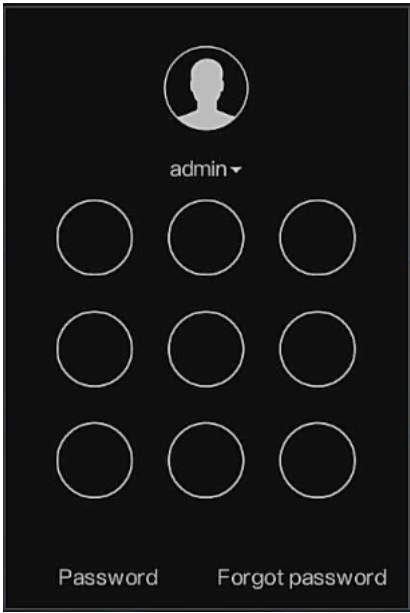
2.4 Power off the Device

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.

2.5 Login to the System

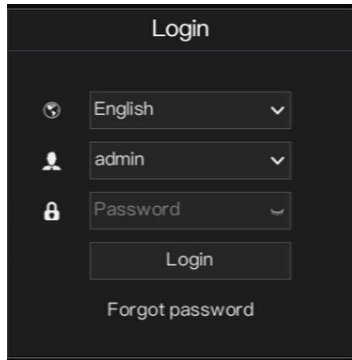
Step 1 Login to the device (two modes to login). The pattern unlock is shown in Figure 2-144.

Figure 2-14 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 2-15.

Figure 2-15 Password login page

The image shows a login interface with a dark background. At the top, the word "Login" is centered in a light-colored font. Below it, there are three input fields, each with a light-colored icon on the left and a dropdown arrow on the right. The first field has a globe icon and contains the text "English". The second field has a person icon and contains the text "admin". The third field has a lock icon and contains the text "Password". Below these fields is a light-colored button with the text "Login". At the bottom, there is a link that says "Forgot password" in a light-colored font.

Step 3 Input the username and password.



NOTE

If the password is incorrect more than 3 times, please log in again after 1 minute. 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).

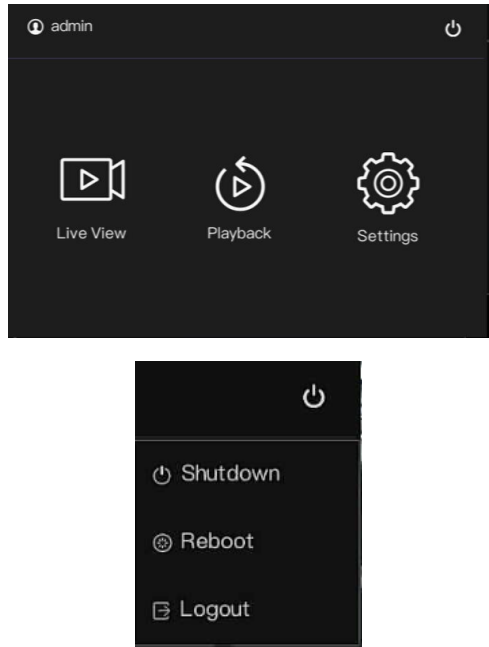
3 Quick Navigation

3.1 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.

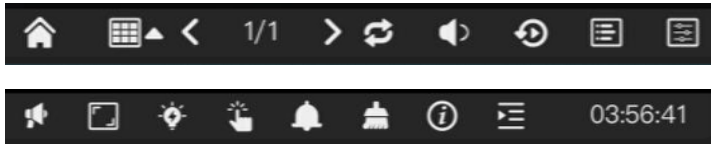
Click  on the left of the NVR floating menu bar. The quick home menu is showing. The quick home menu contains **Live View**, **Playback**, **Settings**, and **Power (Shutdown, Reboot, and Logout)**, as shown in Figure 3-1.

Figure 3-1 Quick home menu

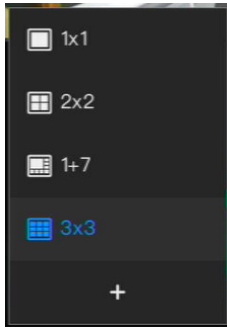


In the middle of the NVR floating menu bar, the video toolbar provides **video window switching**, **auto SEQ**, **volume**, **playback**, and **channel information**, and **Live View Strategy** as shown in Figure 3-2.

Figure 3-2 Real-time video toolbar



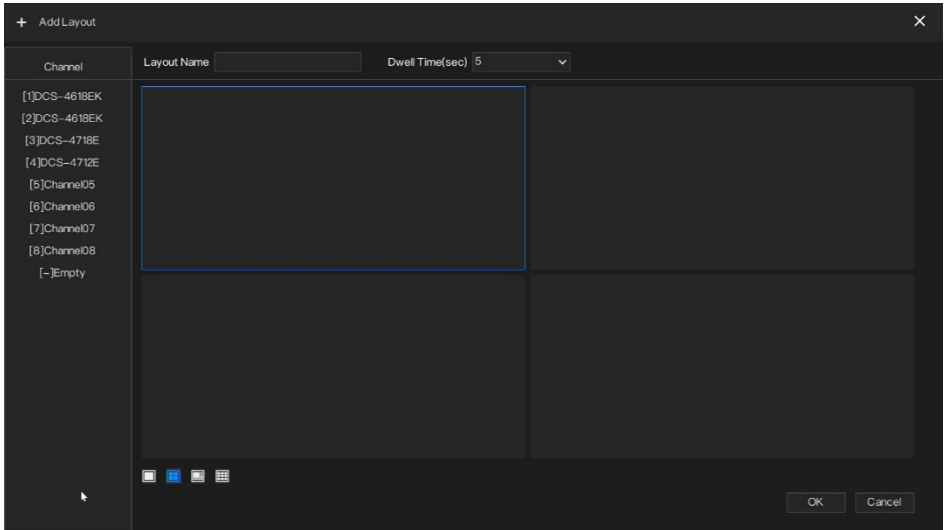
The real-time video toolbar is as follows:



Layout (Depends on NVR mode, channel quantity is very). Users can

choose the layout and add new layout strategies as shown in Figure 3-33. Click  on the right of the screen-splitting format and choose the channels to view the video. Click + to add a new layout.

Figure 3-3 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.



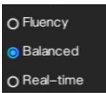
Audio. Click on the icon, and the audio setting screen will be displayed, where you can choose the channel and adjust the volume.



Playback. Click the icon to enter the playback interface.



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**, **Event List**, **Clean alarm**, **Information**, and **Time**, as shown in Figure 3-44.

Figure 3-4 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 3-5 Broadcast

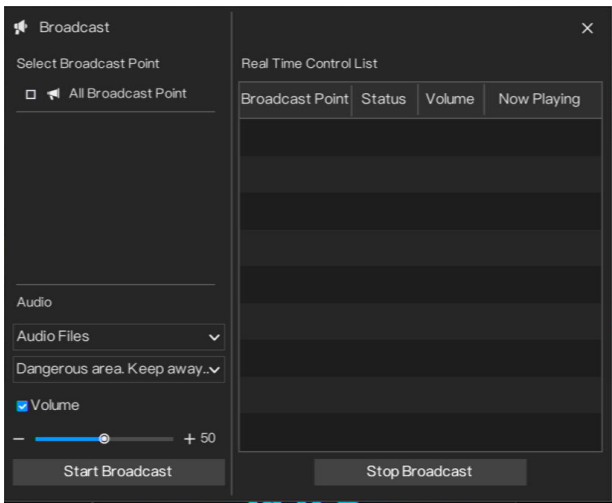
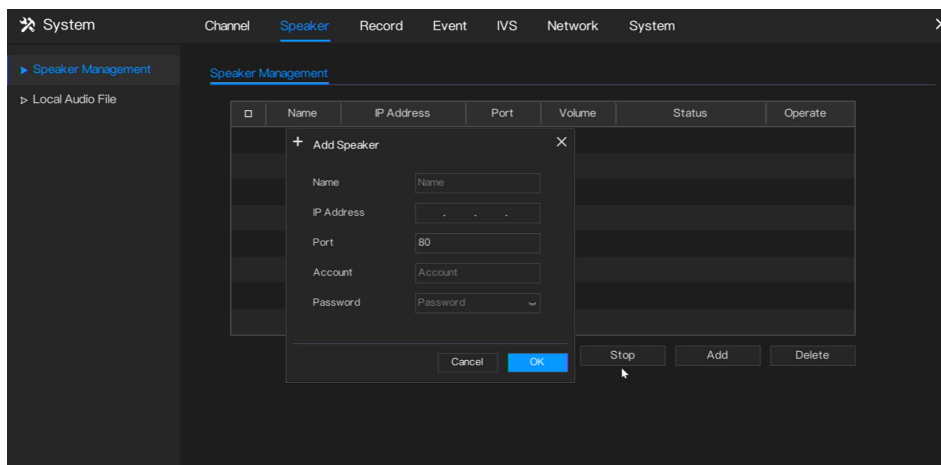


Figure 3-6 Add speaker



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



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 3-7 Manual control light



Manual alarm. Click the icon; users can set different channels, and choose alarm out, the window shows in Figure 3-88.

Figure 3-8 Manual alarm

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



: Event list, click on the icon for more details as shown in Figure 3-99.

Figure 3-9 Event list

Pop up message to monitor		
Channel	Type	Start Time
Channel2	Video Loss	12/03/2026 03:25:48
Channel1	Video Loss	12/03/2026 03:25:48
Channel3	Video Loss	12/03/2026 03:25:47
Channel4	Video Loss	12/03/2026 03:25:47
--	Network Disconn.	12/03/2026 03:25:44
--	Network Disconn.	12/03/2026 03:21:03
Channel1	Video Loss	12/03/2026 03:21:01
Channel2	Video Loss	12/03/2026 03:21:01
Channel4	Video Loss	12/03/2026 03:21:01
Channel3	Video Loss	12/03/2026 03:21:01
Channel2	Video Loss	11/03/2026 09:04:18
Channel1	Video Loss	11/03/2026 09:04:18



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 3-100.



The red icon means the disk needs to be formatted.

Figure 3-10 Information

Network	System	Channel	Disk	
Status	Online			
IP Address	192.168.8.156			
Subnet Mask	255.255.255.0			
Default Gateway	192.168.8.1			
MAC Address	00:1C:27:27:76:5B			
DHCP	On			
Preferred DNS Server	192.168.0.1			
Alternate DNS Server	8.8.8.8			
Total Bandwidth	100.00 Mbps			
Received Packets	35.28 Mbps			



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.

3.2 Real-Time Video Bar

Click on the real-time image and the quick setting will show the bar as Figure 3-11 :

Figure 3-11 Real Time Video Bar



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.

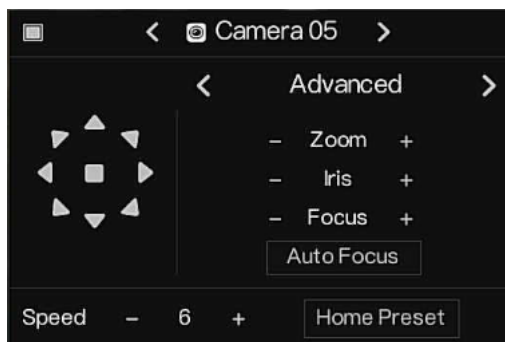


is the time bar of playback.

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 3-121.

Figure 3-12 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.

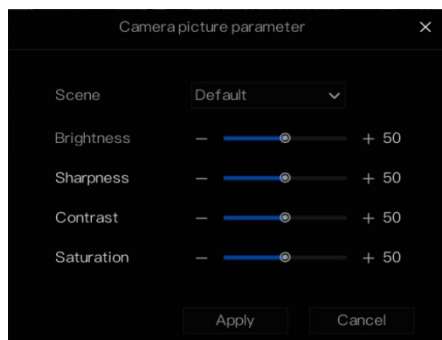


Zoom In. Click Zoom In, and roll the mouse wheel to zoom in and zoom out. Right-click to exit the zooming.



Image. Click the icon, as shown in Figure 3-132. Select the scene, and drag the cursor to adjust the value of **brightness**, **sharpness**, **contrast**, and **saturation**.

Figure 3-13 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.



The current channel is recording.



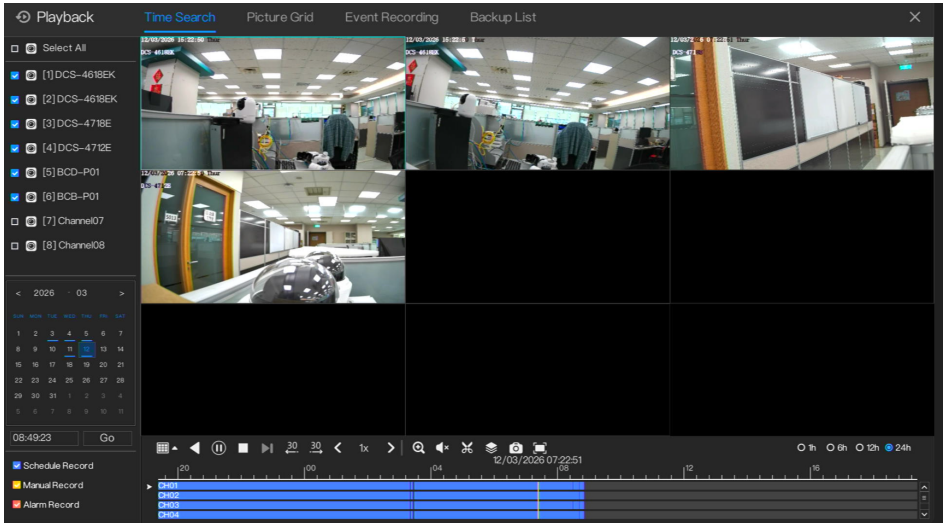
Alarm. The current channel has a motion-detection alarm.

3.3 Playback

Playback refers to playing back a video, fixed-point playback, or playback of the search type.

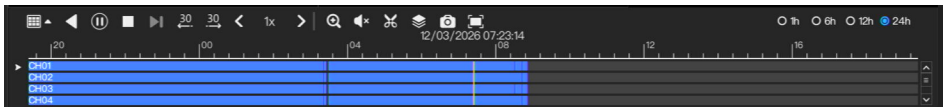
Click  in the quick navigation bar to access the playback screen, as shown in Figure 3-144.

Figure 3-14 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.



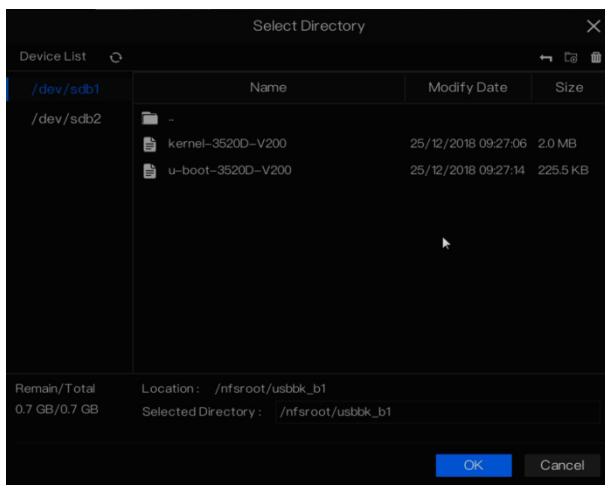
Audio.



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 3-1515. Click **OK** to save.

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

Figure 3-15 Select directory

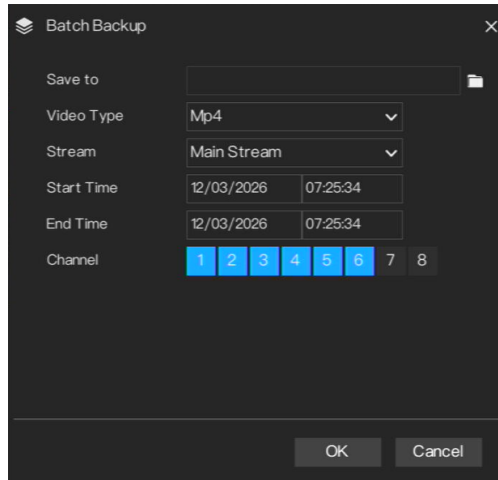


Batch backup.

1. Click the icon to backup multi-channels, as shown in Figure 3-1616.
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.

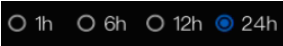
Figure 3-16 Batch backup



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.

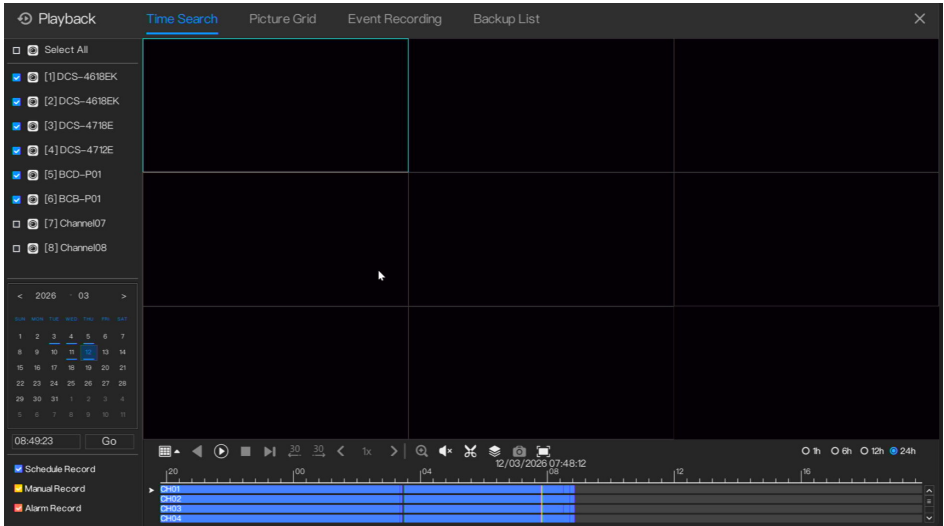
3.3.1 Time Search

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 3-1717.

Figure 3-17 Time Search screen



Operation Steps

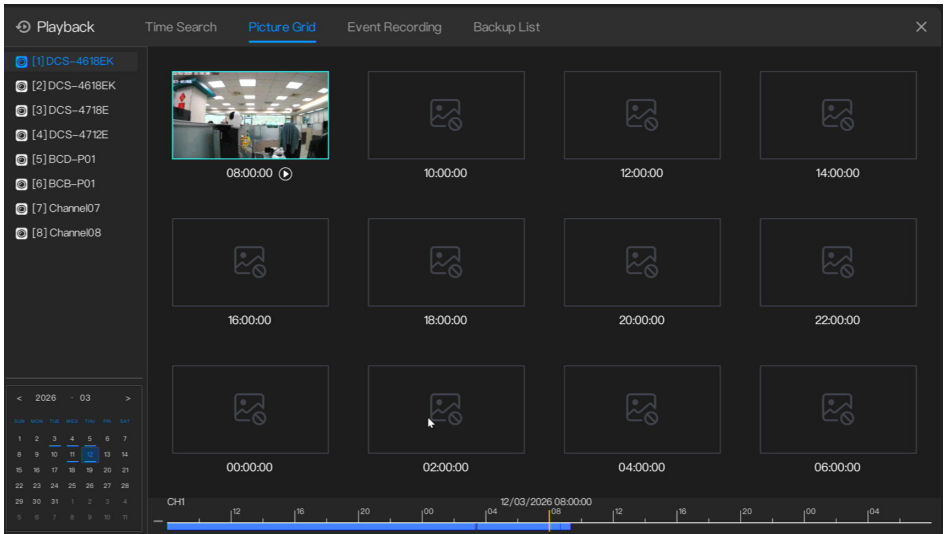
- Step 1** Select a camera or cameras in the camera list on the left side of the search screen. The video view of the selected camera is displayed in the play window.
- Step 2** Select a date in the calendar on the left-hand side of the search screen.
- Step 3** Choose the record type, and search the video quickly.
- Step 4** Choose the proper button to adjust the video.

3.3.2 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 3-1818.

Figure 3-18 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.

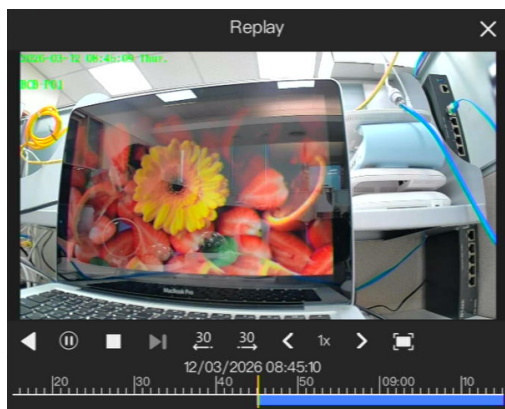
Step 2 Select a date from the calendar.

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 3-19 Replay



3.3.3 Event Recording

Click  on the quick navigation bar; choose **Event Recording** at title to access the alarm event screen, as shown in Figure 3-200

Figure 3-20 Event screen

Playback Time Search Picture Grid Event Recording Backup List

ID	Start Time	Channel	Type	Information	Operate
[1] DCS-461BEK	12/03/2026 08:44:07	Channel03	Video Loss	DCS-471BE	🔍 🔄
[2] DCS-461BEK	12/03/2026 08:44:07	Channel01	Video Loss	DCS-461BEK	🔍 🔄
[3] DCS-471BE	12/03/2026 08:44:07	Channel02	Video Loss	DCS-461BEK	🔍 🔄
[4] DCS-471ZE	12/03/2026 08:43:40	Channel02	Video Loss	DCS-461BEK	🔍 🔄
[5] BCD-P01	12/03/2026 08:43:40	Channel03	Video Loss	DCS-471BE	🔍 🔄
[6] BCB-P01	12/03/2026 08:43:40	Channel04	Video Loss	DCS-471ZE	🔍 🔄
[7] Channel07	12/03/2026 08:43:40	Channel01	Video Loss	DCS-461BEK	🔍 🔄
	12/03/2026 08:29:29	Channel03	Video Loss	DCS-471BE	🔍 🔄
	12/03/2026 08:29:29	Channel02	Video Loss	DCS-461BEK	🔍 🔄
	12/03/2026 08:29:28	Channel04	Video Loss	DCS-471ZE	🔍 🔄
	12/03/2026 08:29:28	Channel01	Video Loss	DCS-461BEK	🔍 🔄
	12/03/2026 08:29:20	--	Network Disconnect	Cable Disconnected	
	12/03/2026 03:25:48	Channel02	Video Loss	DCS-461BEK	🔍 🔄
	12/03/2026 03:25:48	Channel01	Video Loss	DCS-461BEK	🔍 🔄
	12/03/2026 03:25:47	Channel03	Video Loss	DCS-471BE	🔍 🔄
	12/03/2026 03:25:47	Channel04	Video Loss	DCS-471ZE	🔍 🔄

Start Time
11/03/2026 08:49:53
End Time
12/03/2026 08:49:53

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

Search

Double click to play video

Operation Steps

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

Step 2 Set start and end times.

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

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

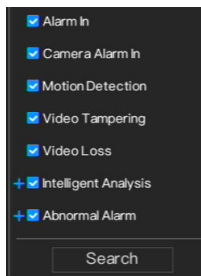
Step 5 Double-click to play a video about the event. It will play a recorded video.



Play the recording video.



Back up the recording video.



The types 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, wrong way, illegal parking, people counting threshold alarm, and smart motion. **Abnormal alarms** include disk error, full disk, IP conflict, network disconnected, fan alarm, power alarm. Users can choose the accurate alarm events to search.

3.3.4 Backup List

Click  on the quick navigation bar, and choose  at title to access the backup screen, as shown in Figure 3-211.

Figure 3-21 Backup screen

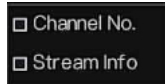
ID	Channel	Start Time	End Time	Size	Stream	Path	Progress	Operate
1	Channel02	21/12/2018 03:5	21/12/2018 03:5	36.0 MB	Main Stream	/nfsroot/usb_bk_b	25%	

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

3.4 Channel Information

Click the  will show as Figure 3-2222, and tick the **Channel No. Or Stream Info**, the information will show on the live video screen.

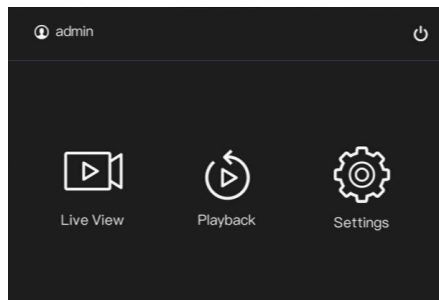
Figure 3-22 Channel information



3.5 Main Menu

Right-click on the UI screen, the main menu as shown in Figure 3-2323.

Figure 3-23 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.

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: Intelligent Analysis settings.

Network: Network, 8012.1X, DDNS, Port Mapping, Email, IP Filter, SNMP, PPPOE, Network Traffic.

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

4 System Setting

4.1 Channel Management

NVR can automatically search for and add IP cameras or manually add cameras in the same Local Area Network (LAN).

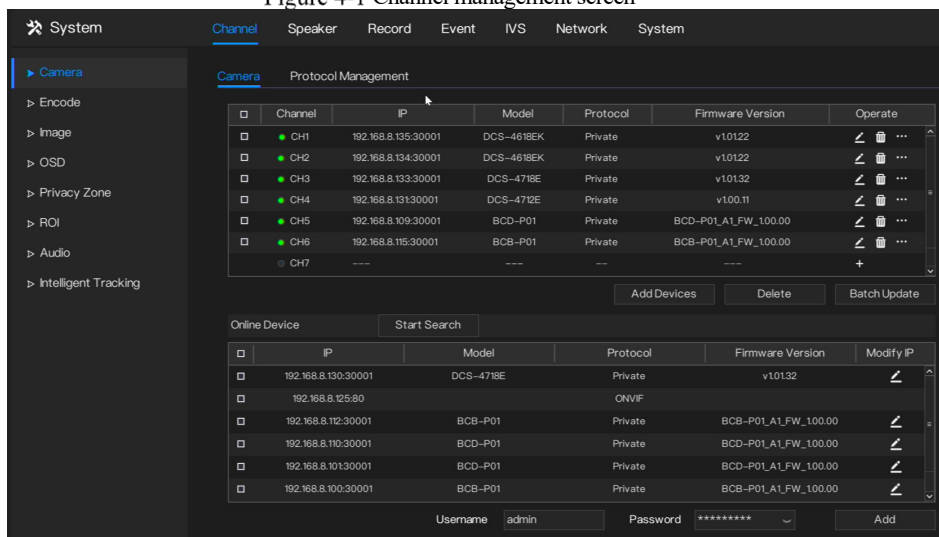
Channel management includes **Adding or Deleting a Camera, Encode, Image, OSD, Privacy Zone, ROI and Audio.**

4.1.1 Camera

Operation Description

Click **Channel** in the Setting System menu to access the camera management screen, as shown in Figure 4-1.

Figure 4-1 Channel management screen



Click  icon to Modify device parameters as shown in Figure 4-2.

Figure 4-2 Modify device parameter

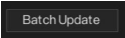
The 'Modify device parameters' dialog box is shown. It contains the following fields and values:

- Channel Name: DCS-4618EK
- IP Address: 192 . 168 . 8 . 135
- Protocol: Private (dropdown)
- Port: 30001
- Username: admin
- Password: ***** (masked)
- Remote Channel: CH-1 (dropdown)

At the bottom, there are 'OK' and 'Cancel' buttons.

Add Devices: It is to add cameras automatically.

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

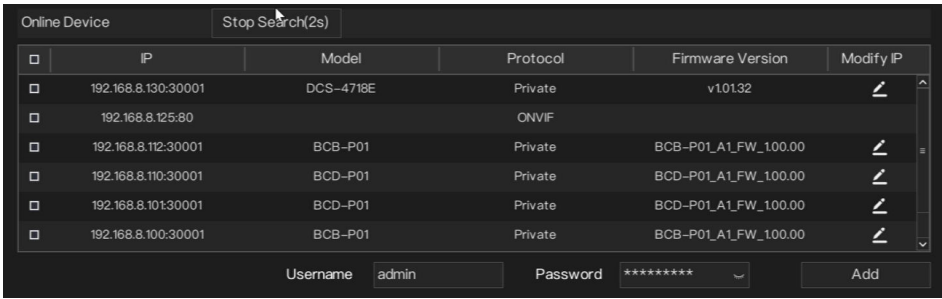
Tick the online non-ONVIF channels on the list and click  to access the directory of software. It will update the channels at once.

4.1.1.1 Add Camera Automatically

The NVR can automatically add cameras to the camera list.

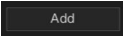
Operation Methods

Method 1: Click , 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.



	IP	Model	Protocol	Firmware Version	Modify IP
☐	192.168.8.130:30001	DCS-4718E	Private	v10132	
☐	192.168.8.125:80		ONVIF		
☐	192.168.8.112:30001	BCB-P01	Private	BCB-P01_A1_FW_100.00	
☐	192.168.8.110:30001	BCD-P01	Private	BCD-P01_A1_FW_100.00	
☐	192.168.8.101:30001	BCD-P01	Private	BCD-P01_A1_FW_100.00	
☐	192.168.8.100:30001	BCB-P01	Private	BCB-P01_A1_FW_100.00	

Username Password 

Method 2: Select the cameras you want to add, and click . 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.

4.1.1.2 Add Camera Manually

Operation Steps

Step 1 Click  to add devices as shown in Figure 4-3.

Figure 4-3 Add camera screen

Manually Add Devices

Channel	IP	Protocol
CH1	192.168.8.135:30001	Private
CH2	192.168.8.134:30001	Private
CH3	192.168.8.133:30001	Private

Channel

7

IP Address

Protocol

ONVIF

Port

80

Username

Username

Password

Password

Remote Channel

CH-1

Reset

OK

Cancel

- 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 , the camera is added successfully.

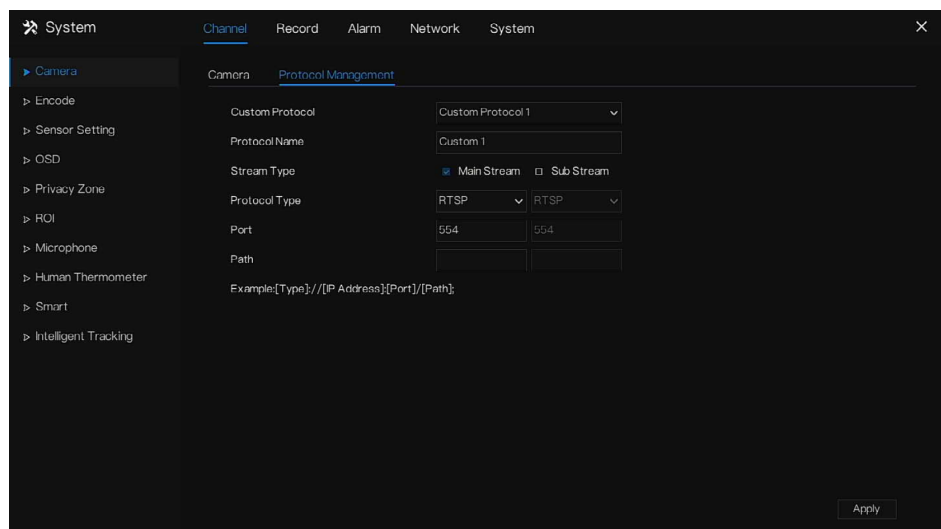
NOTE

- 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.

4.1.1.3 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 4-4.

Figure 4-4 Protocol management



The screenshot displays the 'Protocol Management' configuration window. On the left, a sidebar lists system settings, with 'Camera' expanded to show 'Protocol Management'. The main configuration area includes a 'Custom Protocol' dropdown set to 'Custom Protocol 1', a 'Protocol Name' field with 'Custom 1', and 'Stream Type' checkboxes for 'Main Stream' (checked) and 'Sub Stream'. The 'Protocol Type' is set to 'RTSP' in a dropdown menu. Below this, 'Port' and 'Path' fields both contain the value '554'. An example URL format is shown: 'Example:[Type]://[IP Address]:[Port]/[Path]'. An 'Apply' button is located in the bottom right corner.

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 **Protocol Type**, the default value is **RTSP**.

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

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

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

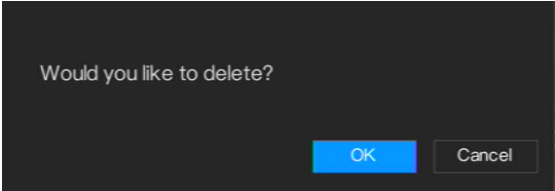
4.1.1.4 Delete Camera

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 4-5.

Step 2

Figure 4-5 Delete confirmation message

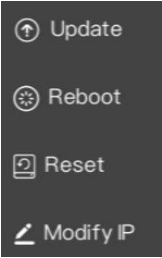


Step 3 Click , the camera will be deleted successfully.

4.1.1.5 Operate Camera

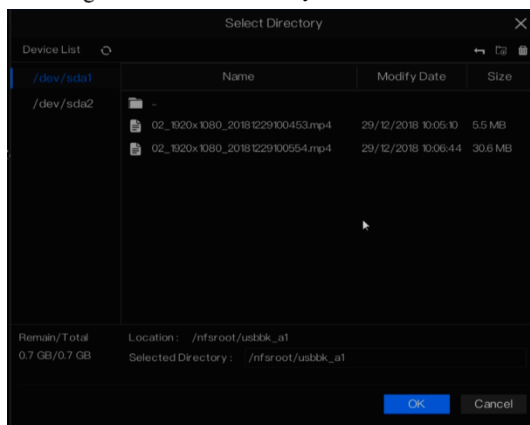
At the camera list, click  to operate the camera as shown in Figure 4-6; users can update, reboot, and reset the camera immediately.

Figure 4-6 More operation



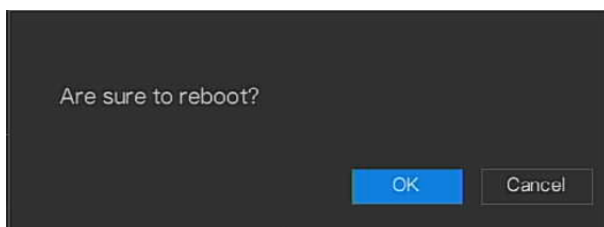
Update: Click **Update**. A pop-up window will appear to select software, as shown in Figure 4-7. Set the directory and click  to update the camera.

Figure 4-7 Select directory of software.



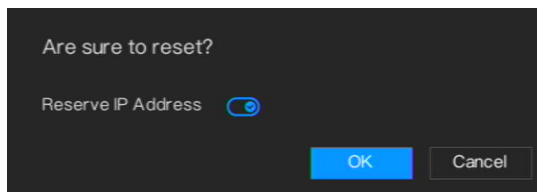
Reboot: Click **Reboot**, and the message “Are sure to reboot?” will show, click  to reboot the camera.

Figure 4-8 Reboot camera



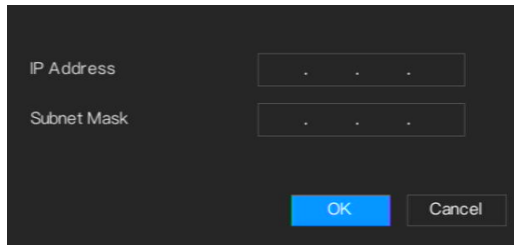
Reset: Click **Reset**, and the message “Are sure to reset?” will show, and users can enable the retain IP address function. Click  to reboot the camera.

Figure 4-9 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 4-10 **Modify IP**

A dark-themed dialog box titled "Modify IP". It contains two input fields: "IP Address" and "Subnet Mask". Each field is a rectangular box with a light gray border and contains three dots, indicating a dotted decimal notation. Below the input fields are two buttons: a blue "OK" button and a gray "Cancel" button.

IP Address

Subnet Mask

OK Cancel

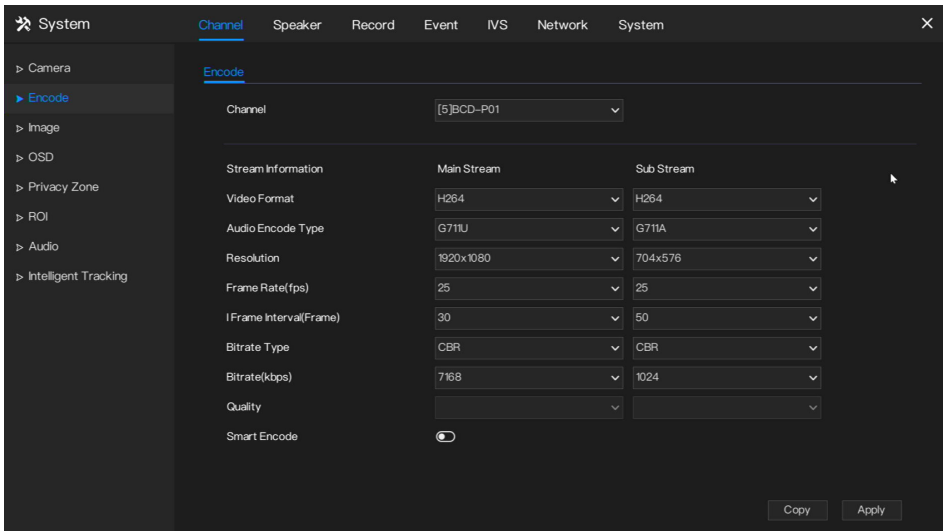
4.1.2 Encode Parameter

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

Operation Description

Navigate to **Settings > Channel > Encode** as shown in Figure 4-11.

Figure 4-11 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**, **Bitrate**, 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.

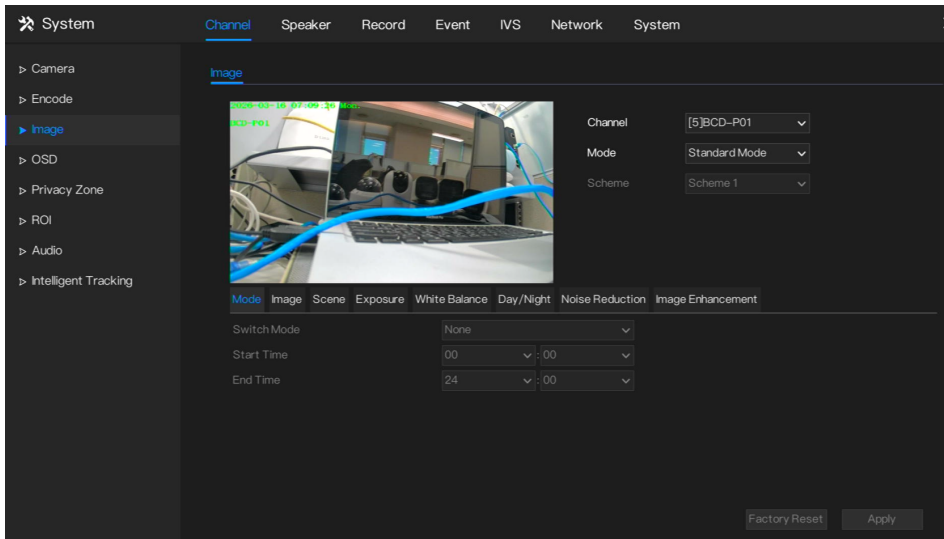
4.1.3 Image

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 4-12.

Figure 4-12 Image screen



The image settings are as follows: **mode, image, scene, exposure, white balance, day/night, noise reduction and image enhancement.**

- **Scene:** It includes **indoor, outdoor**, and default. Mirror includes **normal, horizontal, vertical, horizontal + vertical**.
- **Exposure:** It includes exposure 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 and defog.

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.

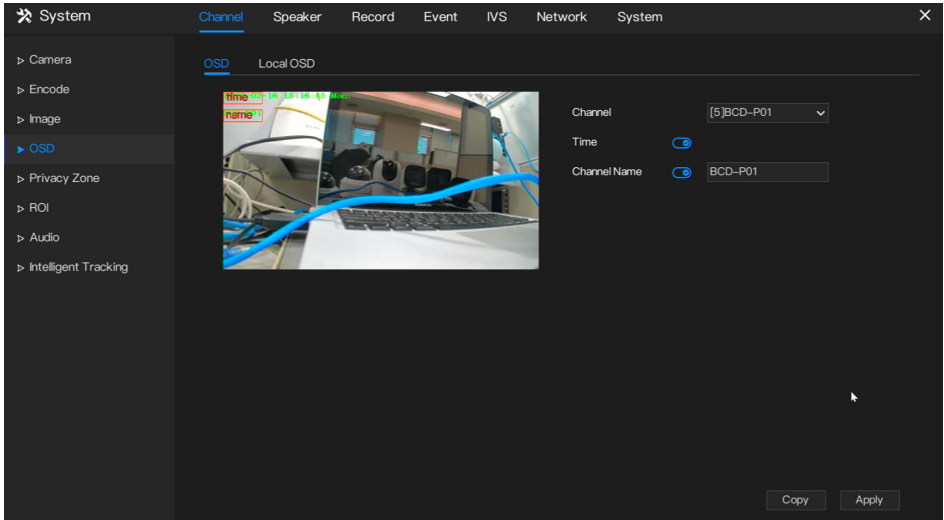
Step 4 Click **Factory Reset** to reset to factory settings if the setting is invalid; click **Apply** to save modified settings.

4.1.4 OSD Settings

4.1.4.1 OSD

Navigate to **Settings > Channel > OSD** as shown in Figure 4-13.

Figure 4-13 OSD setting screen



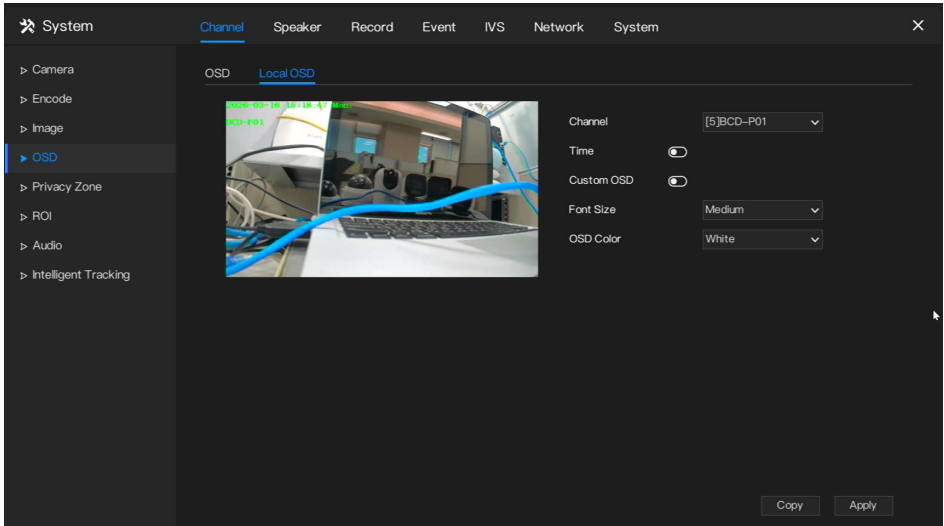
Operation Steps

- 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  and select channels, then click  to apply the OSD settings to cameras in selected channels, and click  to save OSD settings.

4.1.4.2 Local OSD

Navigate to **Settings > Channel > OSD > Local OSD** as shown in Figure 4-14. It is used to the IPC without OSD, so the NVR sets the local OSD.

Figure 4-14 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  and select channels, then click  to apply the OSD settings to cameras in selected channels, and click  to save OSD settings.

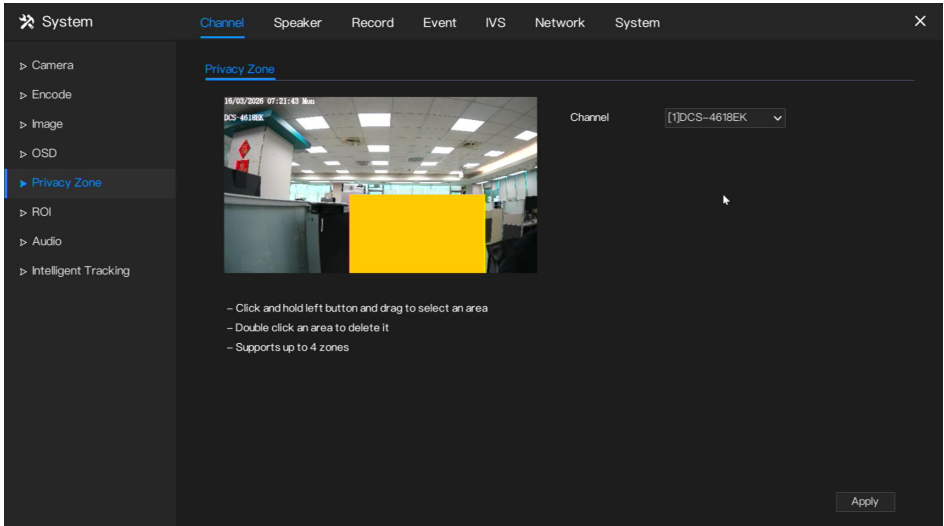
4.1.5 Privacy Zone

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 4-15.

Figure 4-15 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.

4.1.6 ROI

1. Navigate to **Settings > Channel > ROI** (Region of Interest) as shown in Figure 4-16.

Figure 4-16 ROI

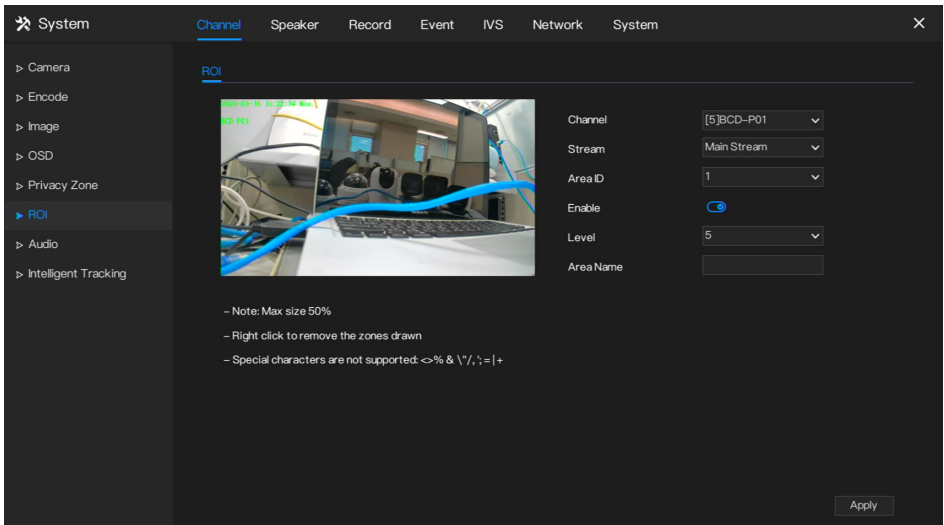


Table 4-1 ROI parameter

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

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

- Click **Apply** to save ROI settings.

4.1.7 Audio

4.1.7.1 Audio Input

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

- Navigate to **Settings > Channel > Audio > Audio Input** as shown in Figure 4-17.
- Adjust the parameters as per Table 4-2.
-

Figure 4-17 Audio input

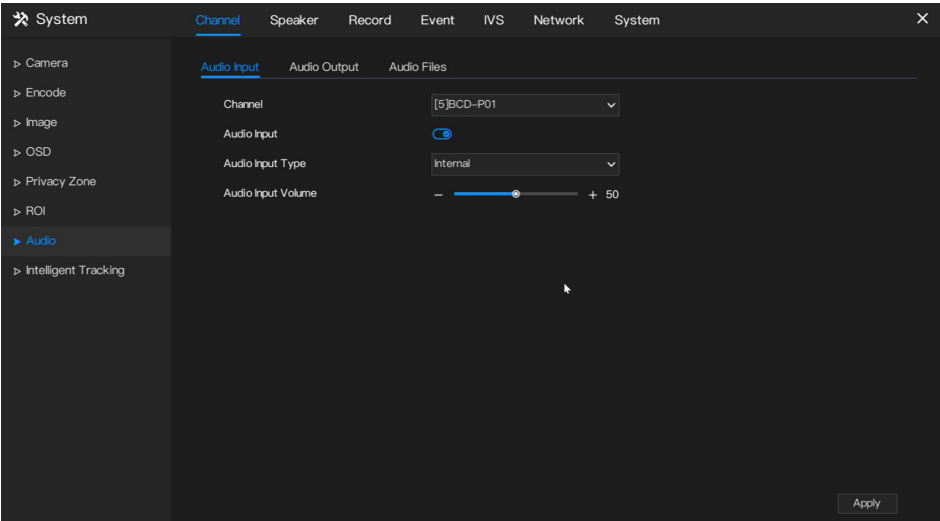


Table 4-2 Audio input

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.

Parameter	Description	Setting
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.
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.

- Click  to save privacy settings.

4.1.7.2 Audio Output

- Navigate to **Settings > Channel > Audio > Audio Output**.
- Select **Audio Output**, set the audio output parameters, and select an audio output device such as a speaker.
- Adjust the parameters as per Table 4-3.

Figure 4-18 Audio output

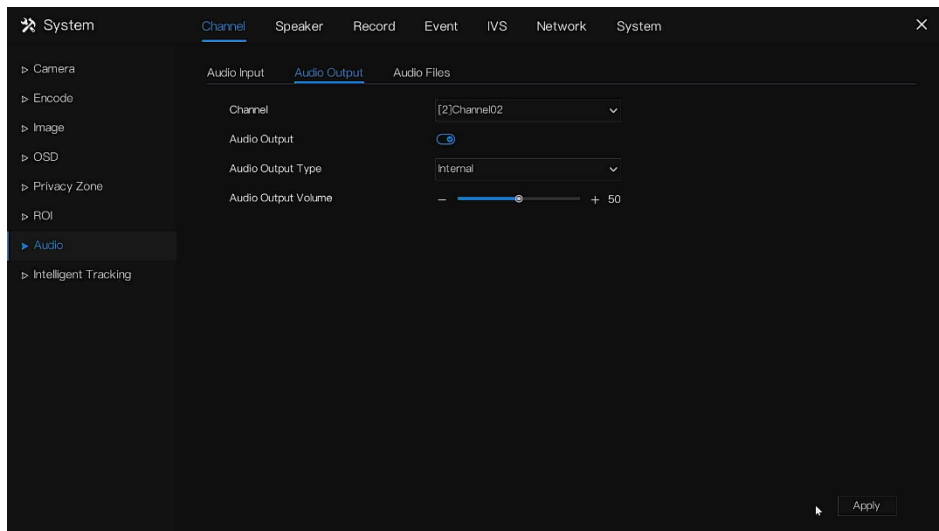


Table 4-3 Audio output

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.

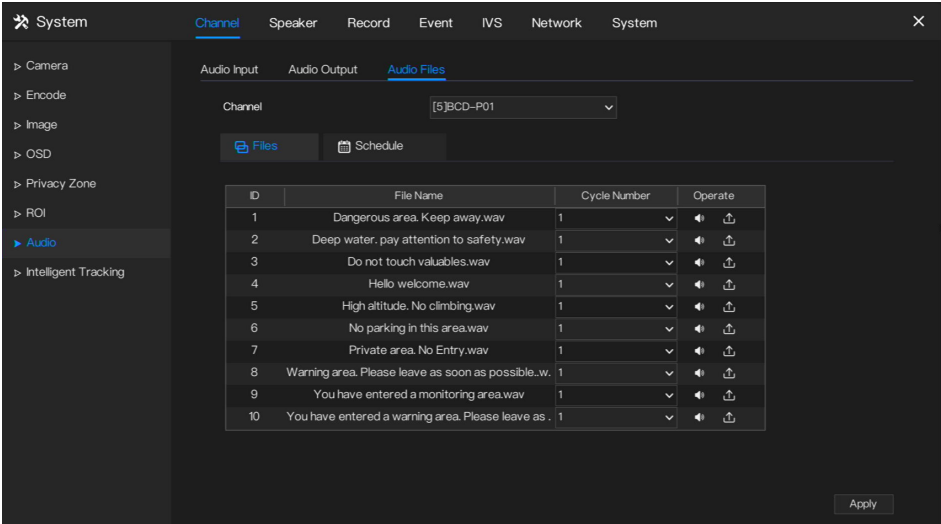
Parameter	Description	Setting
Audio output Volume	Allows you to adjust the audio output volume.	[Setting method] Slide the slider left or right. [Default value] 50 NOTE The value ranges from 0 to 100.

4. Click  to save privacy settings.

4.1.7.3 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 4-19 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  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**.

Figure 4-20 Upload audio file

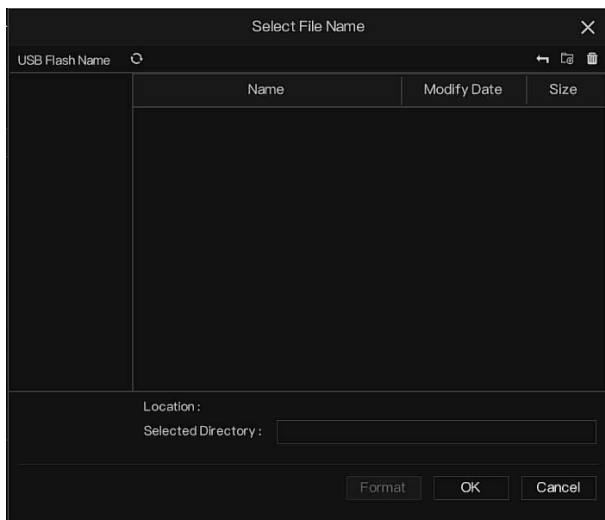
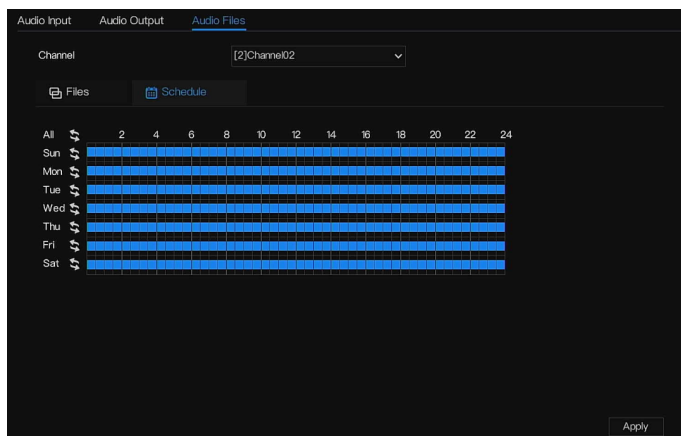


Figure 4-21 Schedule of audio file



4.1.8 Intelligent Tracking

 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 4-22.
2.

Adjust the parameters as per Table 4-4.
3.

Click  to save settings.

Figure 4-22 Intelligent tracking

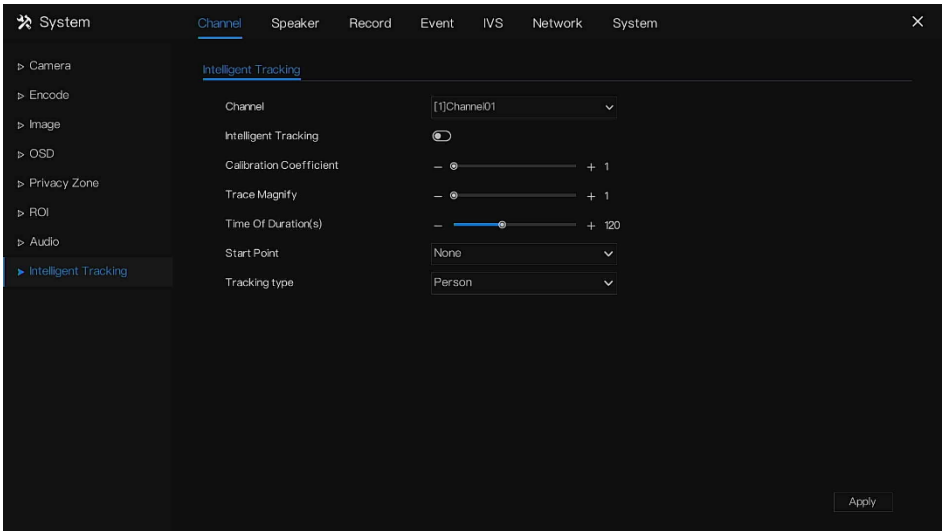


Table 4-4 Intelligent tracking parameters

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

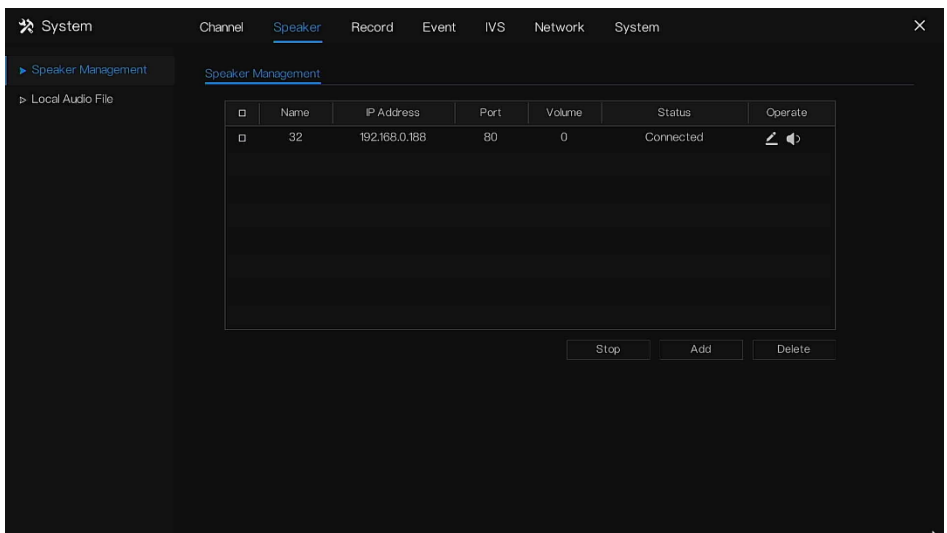
4.2 Speaker

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.

4.2.1 Speaker Management

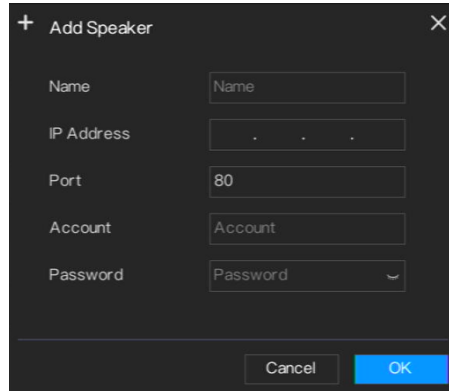
Step 1 Navigate to **Settings > Speaker** as shown in Figure 4-23.

Figure 4-23 Speaker management



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

Figure 4-24 Add speaker

A dark-themed dialog box titled "Add Speaker" with a plus icon on the left and a close icon on the right. It contains five input fields: "Name" (placeholder: Name), "IP Address" (placeholder: . . .), "Port" (placeholder: 80), "Account" (placeholder: Account), and "Password" (placeholder: Password with a dropdown arrow). At the bottom are "Cancel" and "OK" buttons.

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

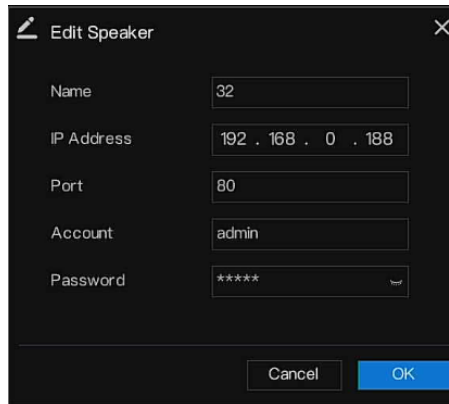
Cancel OK

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 4-25 Edit speaker

A dark-themed dialog box titled "Edit Speaker" with an edit icon on the left and a close icon on the right. It contains five input fields: "Name" (value: 32), "IP Address" (value: 192 . 168 . 0 . 188), "Port" (value: 80), "Account" (value: admin), and "Password" (value: ***** with a dropdown arrow). At the bottom are "Cancel" and "OK" buttons.

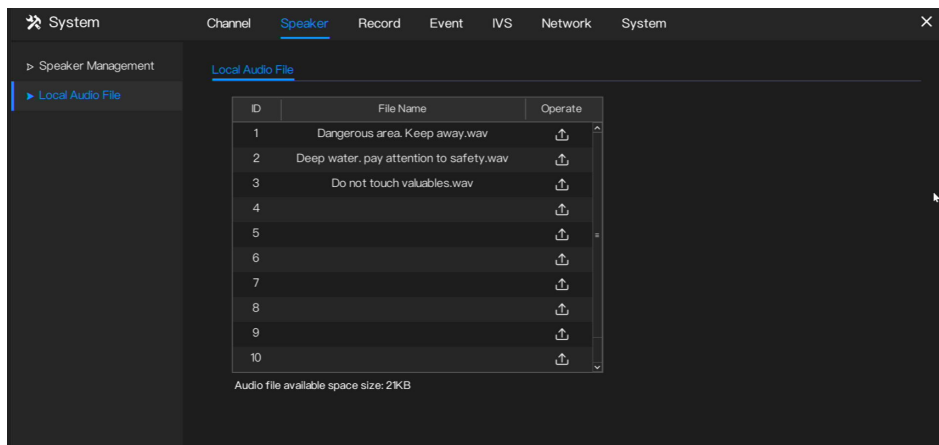
Name	32
IP Address	192 . 168 . 0 . 188
Port	80
Account	admin
Password	*****

Cancel OK

4.2.1.2 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 4-26 Local audio file



4.3 Record-Setting

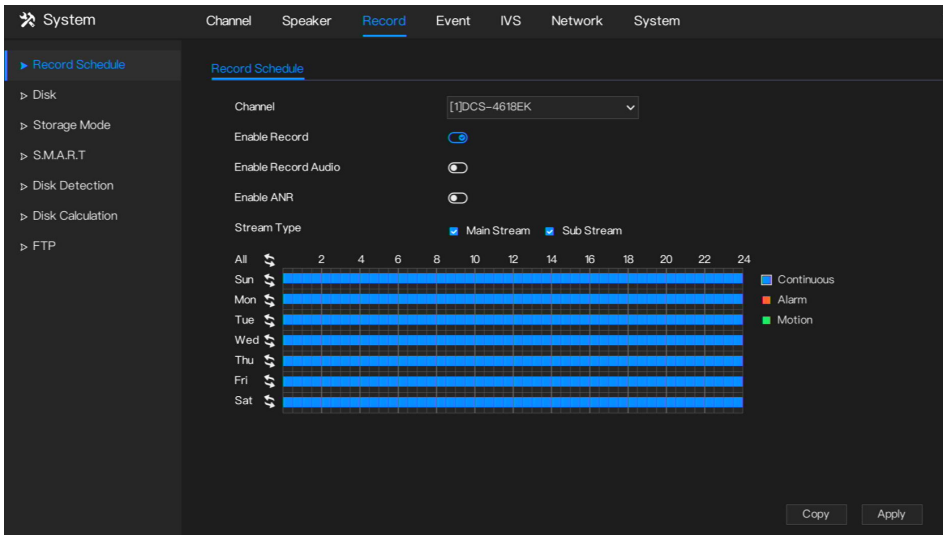
Set the **Record Schedule**, **Disk**, **Storage Mode**, **S.M.A.R.T**, **Disk Detection**, **Disk Calculation** and **FTP**.

4.3.1 Record Schedule

Operation Description

Navigate to **Settings > Record > Record Schedule** as shown in Figure 4-27.

Figure 4-27 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  and select channels or tick **all**, then click  to apply the record management settings to selected channels, and click  to save settings.

4.3.2 Disk

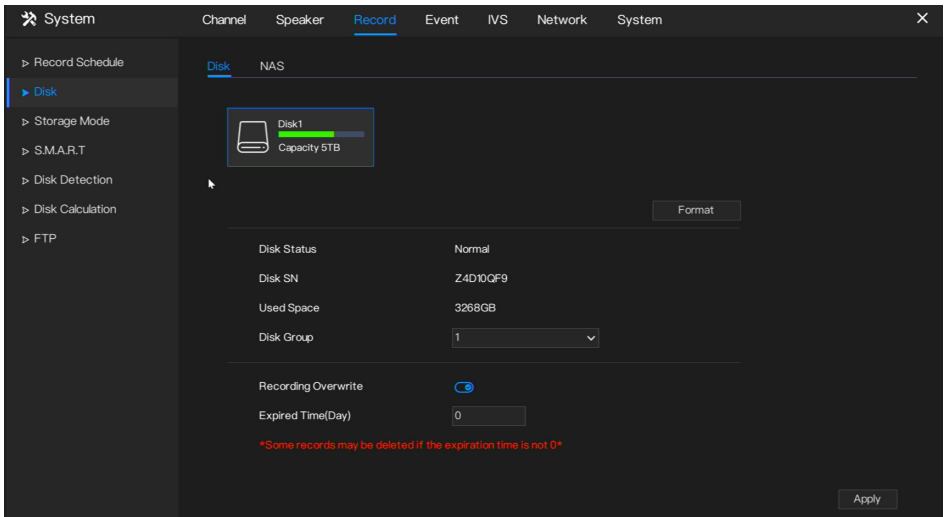
4.3.2.1 Disk

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 4-28.

Figure 4-28 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**.

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

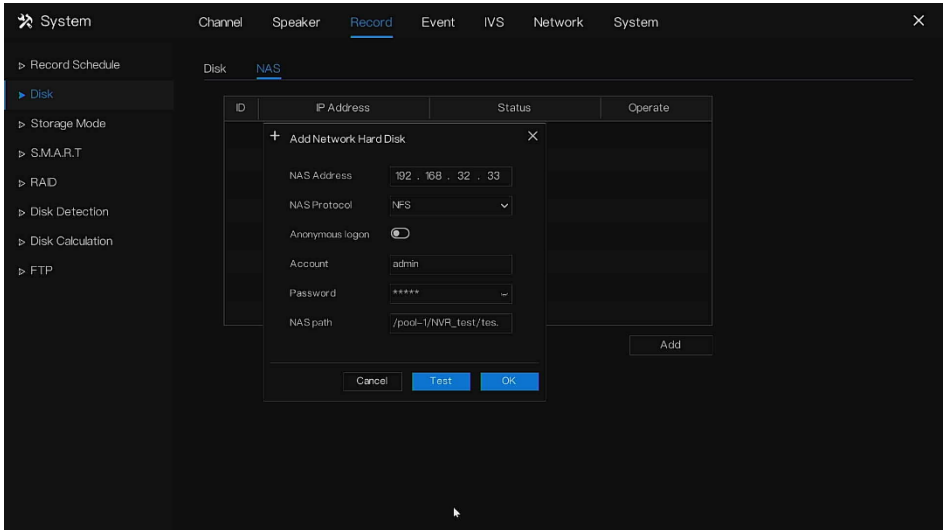
The disk groups can keep the recording of channels at different disks, which will improve the storage efficiency. One driver

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

4.3.2.2 NAS

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

Figure 4-29 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.

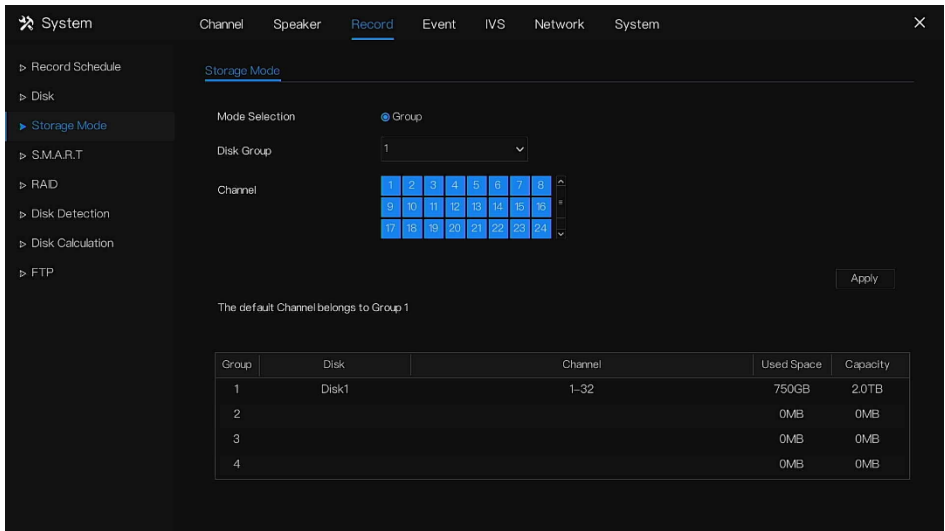
4.3.3 Storage Mode

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 4-30.

Figure 4-30 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.

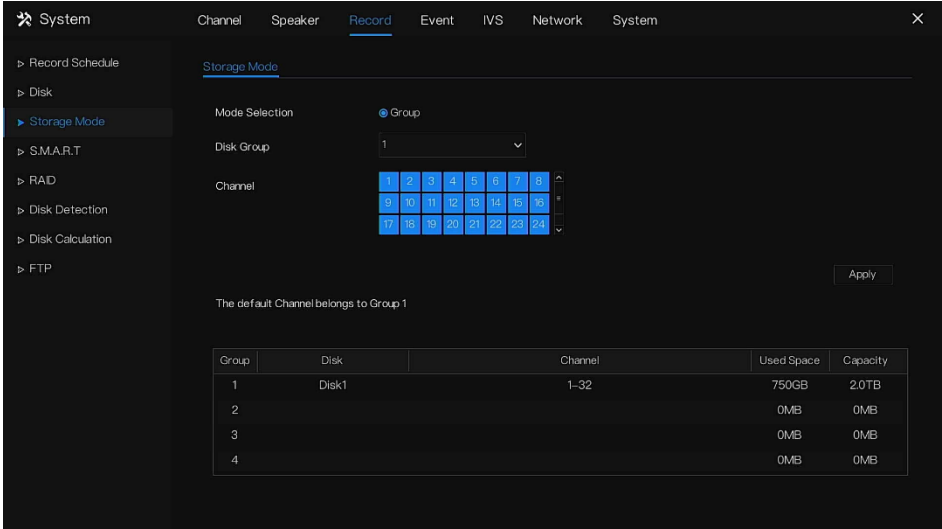
----End

4.3.4 S.M.A.R.T

4.3.4.1 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 4-31.

Figure 4-31 S.M.A.R.T



----End

4.3.4.2 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 4-32.

Figure 4-32 WDDA

S.M.A.R.T WDDA

Disk: Disk2

Disk SN: WD-WX42D6215FNA Disk Model: WDC WD64PURZ-85BWUJ

Warning: 0 Advisory: 0

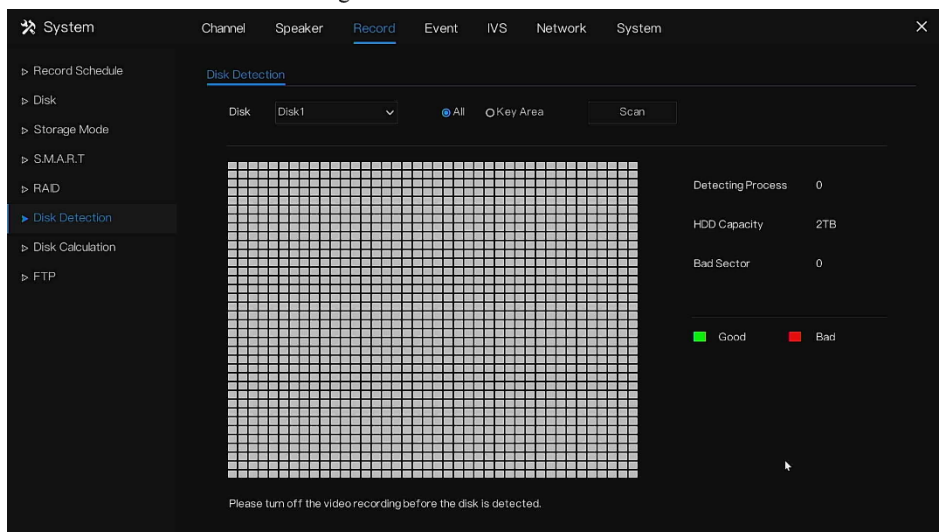
ID	Attribute Name	Status	Raw Value
1	Lifetime Power On Reset Alert	Normal	1137.00
2	Power On Hours Alert	Normal	7794.00
3	Head Load Lifetime Count Alert	Normal	1362.00
4	Current Temperature Alert	Normal	26.00
5	Total Lifetime Workload Alert	Normal	175.67
6	Total Workload Rate Alert	Normal	197.44
7	Power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

----End

4.3.5 Disk Detection

Detect the disk before recording videos so that the data are secure, as shown in Figure 4-33.

Figure 4-33 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

4.3.6 Disk Calculation

Users can calculate the usage of the disk so that they can set the storage strategy reasonably, as shown in Figure 4-34.

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

Figure 4-34 Disk calculation of capacity

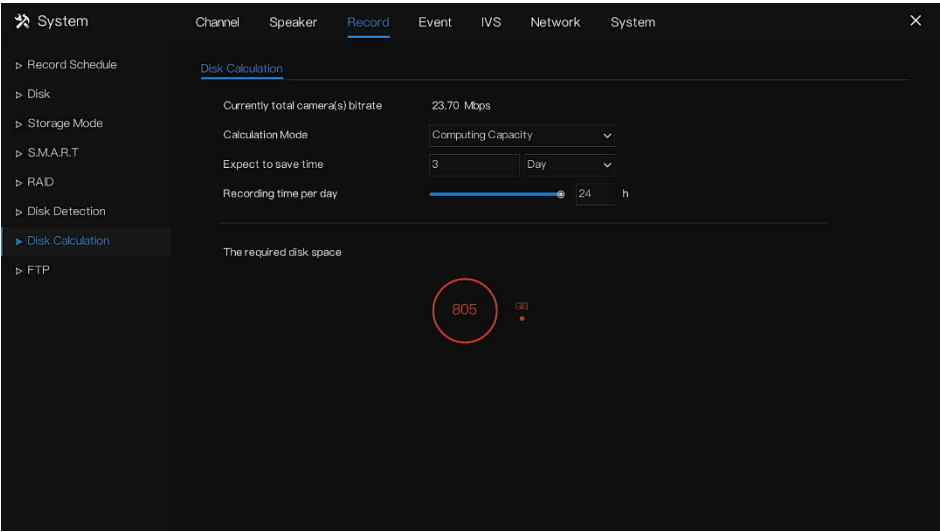
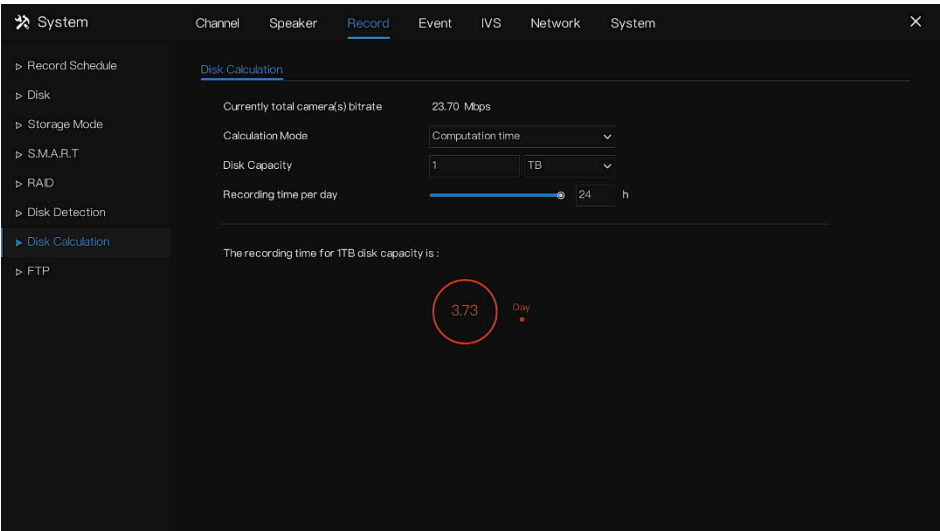


Figure 4-35 Disk calculation of time

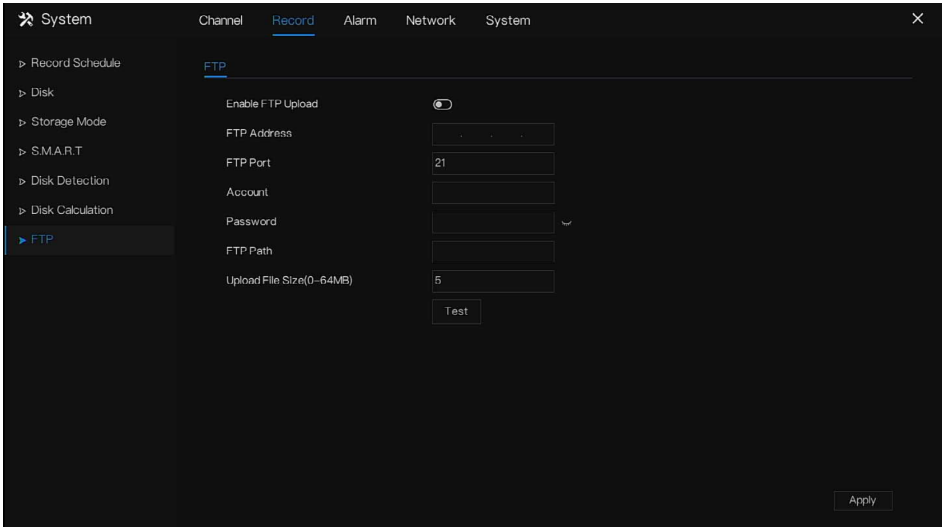


----End

4.3.7 FTP

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

Figure 4-36 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

4.4 Event Management

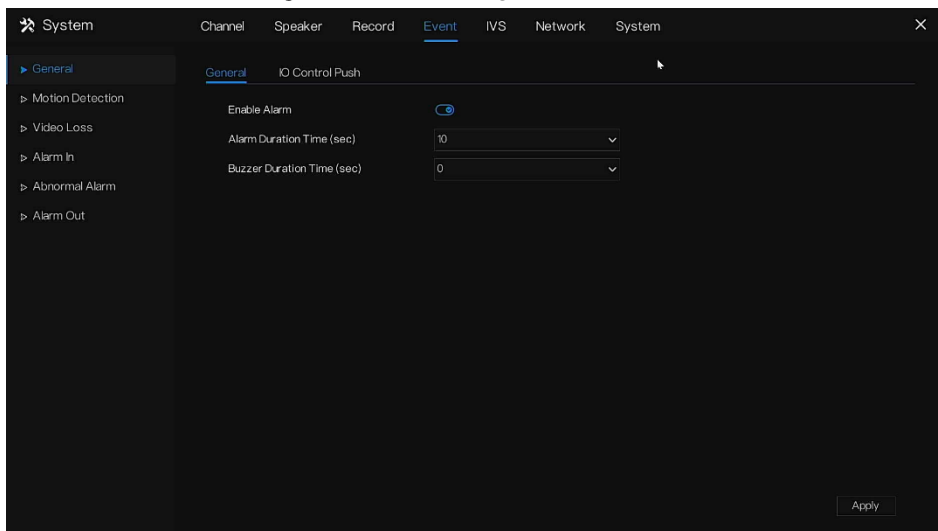
Set the **General**, **Motion Detection**, **Video Loss**, **Alarm In**, **Abnormal Alarm**, and **Alarm Out** in the **Event** screen.

4.4.1 General

4.4.1.1 General

Step 1 Navigate to **Settings > Event > General**, as shown in Figure 4-37.

Figure 4-37 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

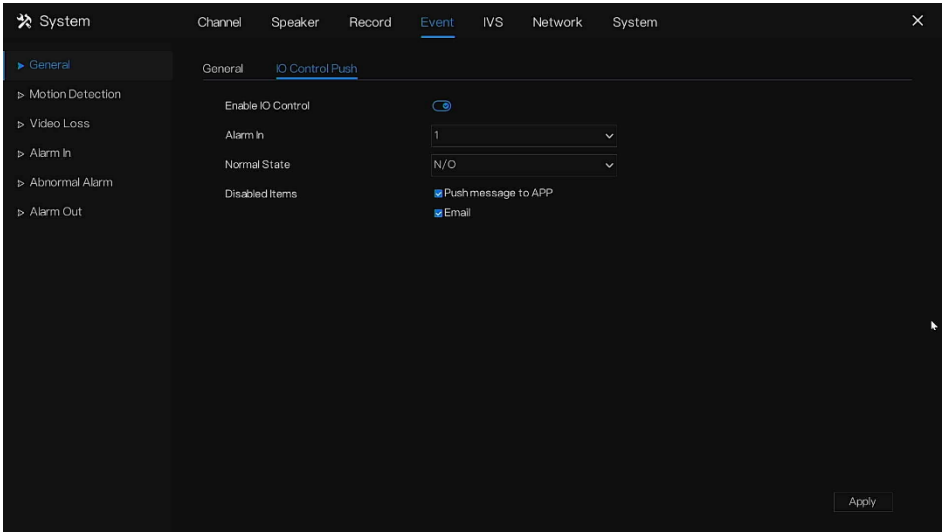
4.4.1.2 IO control push

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 4-38 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

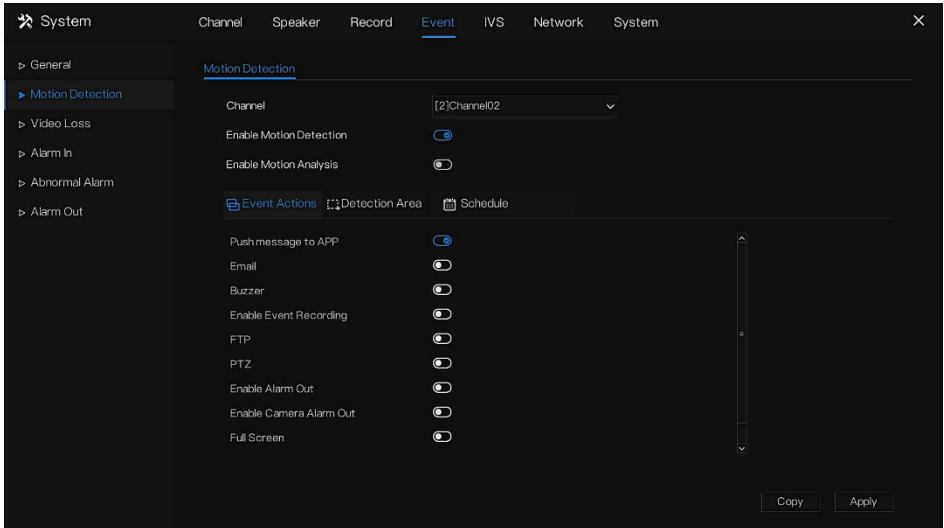
4.4.2 Motion Detection

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 4-39.

Figure 4-39 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 4-40.

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 4-5.

Table 4-5 Event actions

System

Channel

Speaker

Record

Event

IVS

Network

System

✕

▸ General

▸ Motion Detection

▸ Video Loss

▸ Alarm In

▸ Abnormal Alarm

▸ Alarm Out

Motion Detection

Channel

[2]Channel02

▼

Enable Motion Detection

☒

Enable Motion Analysis

☐

Event Actions

Detection Area

Schedule

Push message to APP

☒

Email

☐

Buzzer

☐

Enable Event Recording

☐

FTP

☐

PTZ

☐

Enable Alarm Out

☐

Enable Camera Alarm Out

☐

Full Screen

☐

Copy

Apply

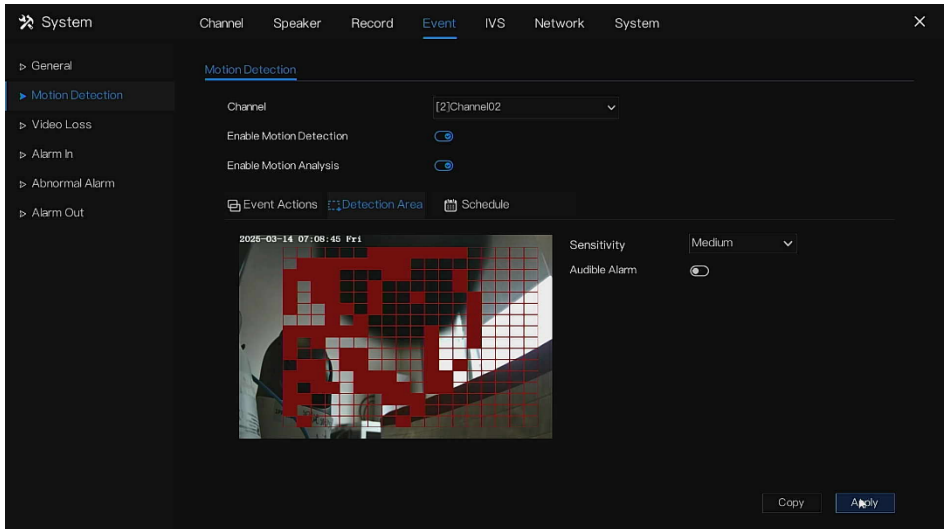
Parameter	Description
Push Message to app	When motion is triggered, you will receive a notification via the mobile app.
Email	When a motion is triggered, a notification will be sent to a designated email address. Note: Email settings must be configured under Network settings (see section 4.6.5 <i>Email</i>) 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 4.3.7 <i>FTP</i>) 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.

Speaker	☒
Broadcast Point	32
Audio Files	Dangerous area. Keep away.wav

Step 5 Click the Area page to access the motion detection area setting, as shown in Figure 4-40.

Figure 4-40 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.

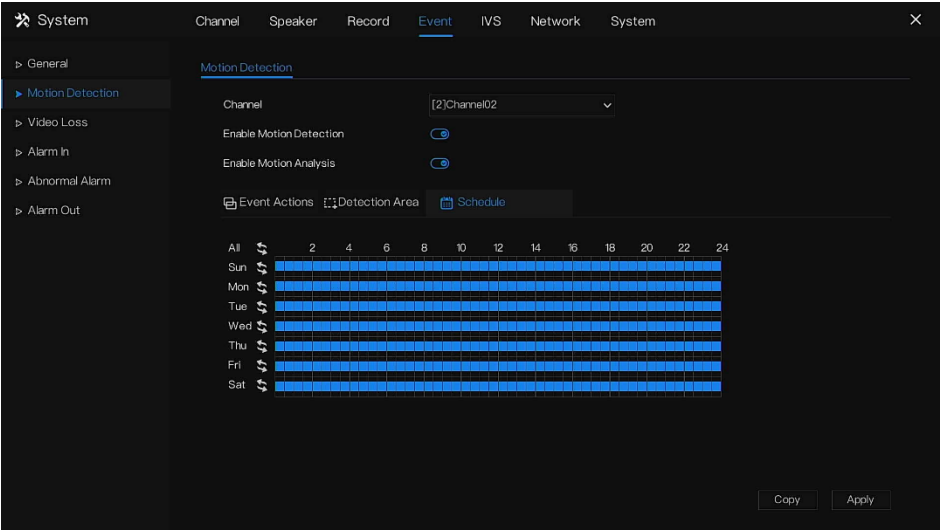
Step 6 Click the **Schedule** page to access the schedule screen. For details, please refer to section 4.3.1 *Record Schedule*.

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 4-41 Alarm schedule



----End

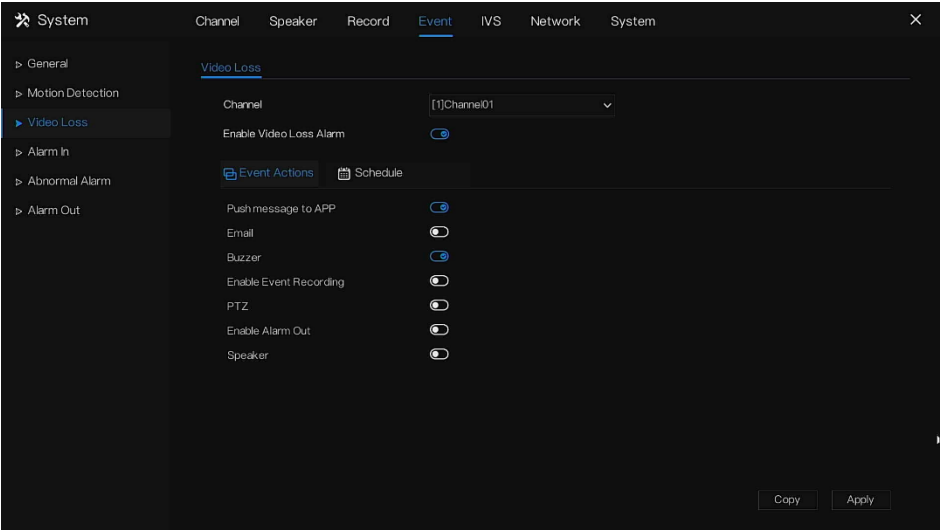
4.4.3 Video Loss

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 4-42.

Figure 4-42 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 *4.3.1 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

4.4.4 Alarm In

NOTE

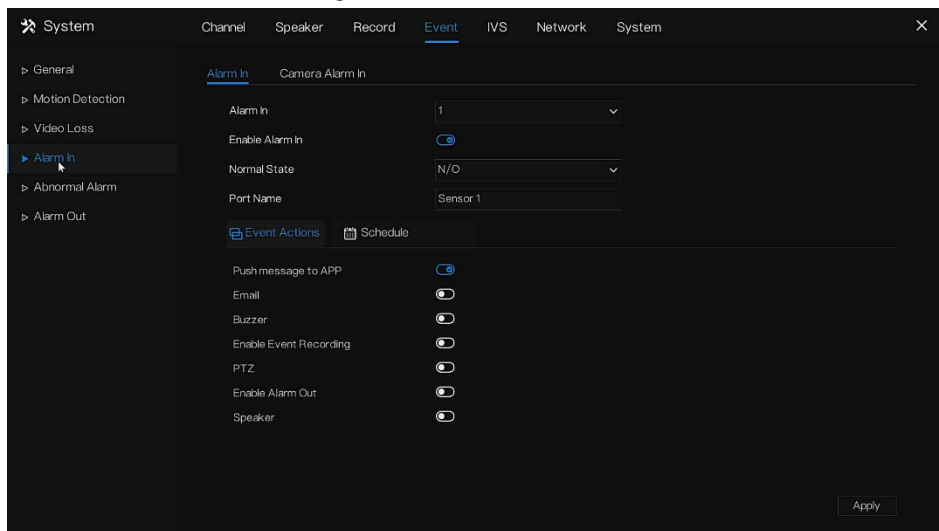
This function requires that the device be connected to an external alarm.

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 4-43.

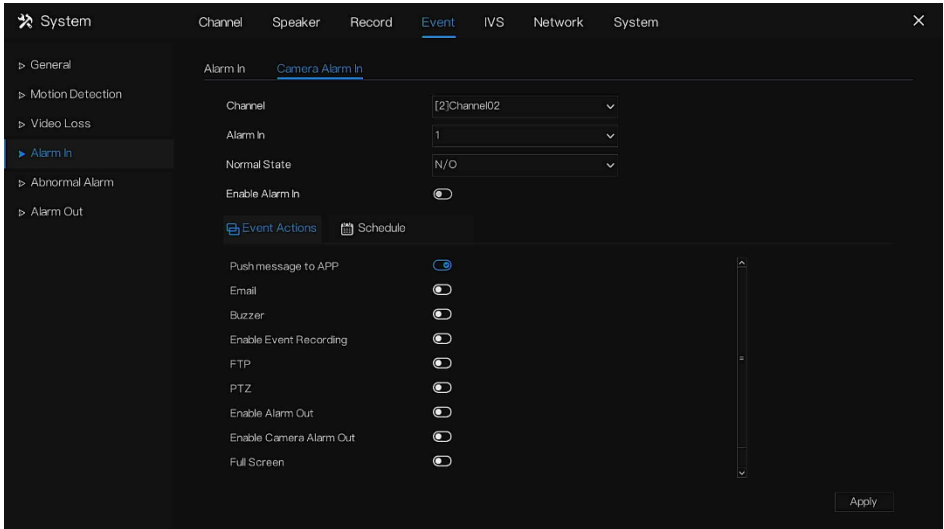
Figure 4-43 Alarm in screen



The screenshot shows the 'Alarm In' configuration screen within the 'Event' settings. The left sidebar lists navigation options: General, Motion Detection, Video Loss, Alarm In (selected), Abnormal Alarm, and Alarm Out. The main area has tabs for 'Alarm In' and 'Camera Alarm In'. Under 'Alarm In', there are fields for 'Alarm In' (set to 1), 'Enable Alarm In' (toggle on), 'Normal State' (set to N/O), and 'Port Name' (set to Sensor 1). Below these are two tabs: 'Event Actions' and 'Schedule'. The 'Event Actions' tab is active, showing a list of actions with toggle switches: 'Push message to APP' (on), 'Email' (off), 'Buzzer' (off), 'Enable Event Recording' (off), 'PTZ' (off), 'Enable Alarm Out' (off), and 'Speaker' (off). An 'Apply' button is located at the bottom right.

Setting	Value/Status
Alarm In	1
Enable Alarm In	On
Normal State	N/O
Port Name	Sensor 1
Push message to APP	On
Email	Off
Buzzer	Off
Enable Event Recording	Off
PTZ	Off
Enable Alarm Out	Off
Speaker	Off

Figure 4-44 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, Send 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 4.4.2 Motion Detection**.

Step 7 Click the **Schedule** page to access the schedule screen. For details, please refer to **section 4.3.1 Record Schedule**.

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

----End

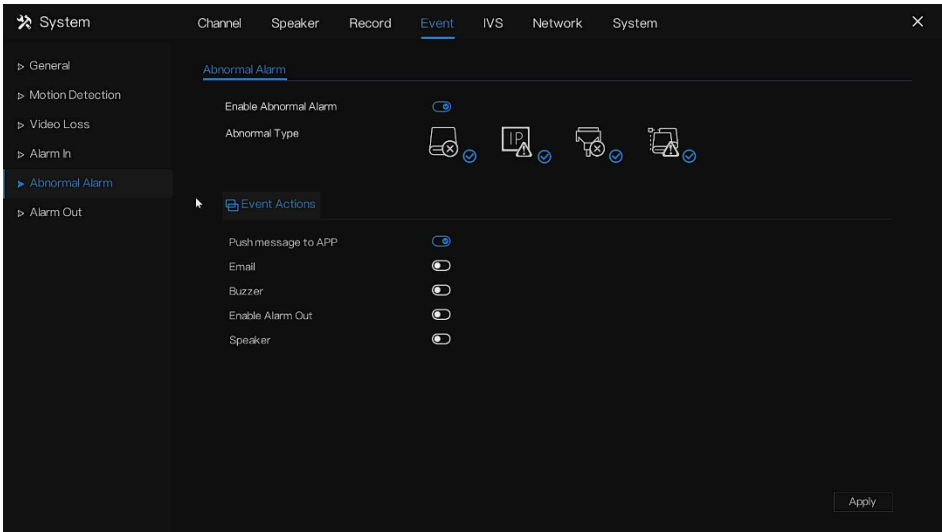
4.4.5 Abnormal Alarm

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 4-45.

Figure 4-45 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 4.4.2 Motion Detection*.

Step 4 Click **Apply** to save abnormal alarm settings.

----End

4.4.6 Alarm Out

4.4.6.1 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 4-46 Alarm out

System

Channel

Speaker

Record

Event

IVS

Network

System

General

Motion Detection

Video Loss

Alarm In

Abnormal Alarm

Alarm Out

Alarm Out

Camera Alarm Out

Flashlight Alarm Out

Red And Blue Light Alarm Out

White Light Alarm Out

Port Number

Port Name

Valid Signal

Alarm Output Mode

1

Name

Close

Switch Mode

Apply

----End

4.4.6.2 Camera Alarm out

 NOTE

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

Figure 4-47 Camera alarm out

Table 4-6 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

4.4.6.3 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 4-48 Flashlight alarm out

System Channel Speaker Record **Event** IVS Network System

General
Motion Detection
Video Loss
Alarm In
Abnormal Alarm
Alarm Out

Alarm Out Camera Alarm Out **Flashlight Alarm Out** Red And Blue Light Alarm Out White Light Alarm Out

Channel [9]3.6.1602.1006.88.118.6.10.D03

Alarm Time 10

Flicker Interval(100~1000ms) 1500

Manual Control Duration(0~43200s) 0

Schedule

All 2 4 6 8 10 12 14 16 18 20 22 24

Sun

Mon

Tue

Wed

Thu

Fri

Sat

Apply

Figure 4-49 Red and blue light Light alarm out

System Channel Speaker Record **Event** IVS Network System

General
Motion Detection
Video Loss
Alarm In
Abnormal Alarm
Alarm Out

Alarm Out Camera Alarm Out Flashlight Alarm Out **Red And Blue Light Alarm Out** White Light Alarm Out

Channel [7]Channel01

Alarm Duration(10~60s) 10

Scintillation Frequency(ms) 50

Manual Control Duration(0~43200s) 0

Schedule

All 2 4 6 8 10 12 14 16 18 20 22 24

Sun

Mon

Tue

Wed

Thu

Fri

Sat

Apply

Figure 4-50 White light alarm out

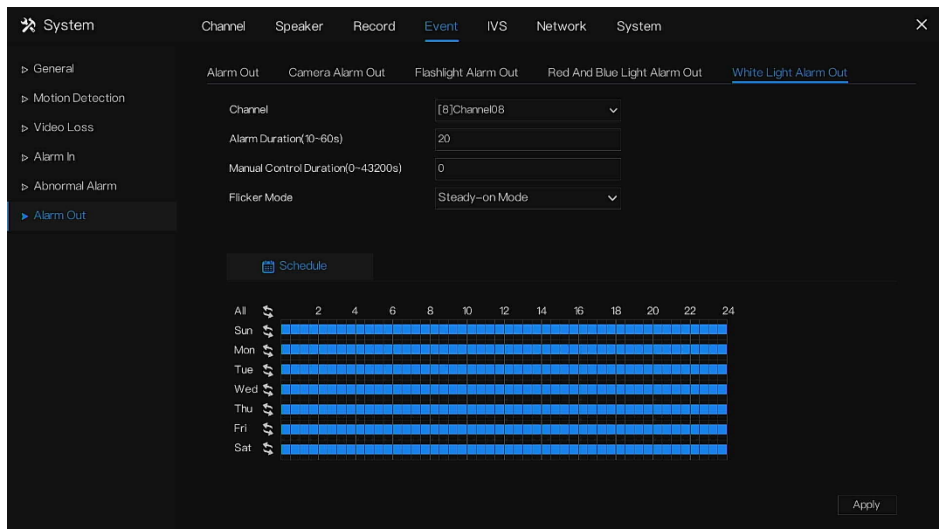


Table 4-7 Camera alarm out

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.
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.

Parameter	Description	Setting
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.

4.5 IVS Configuration

4.5.1 Intelligent Analysis



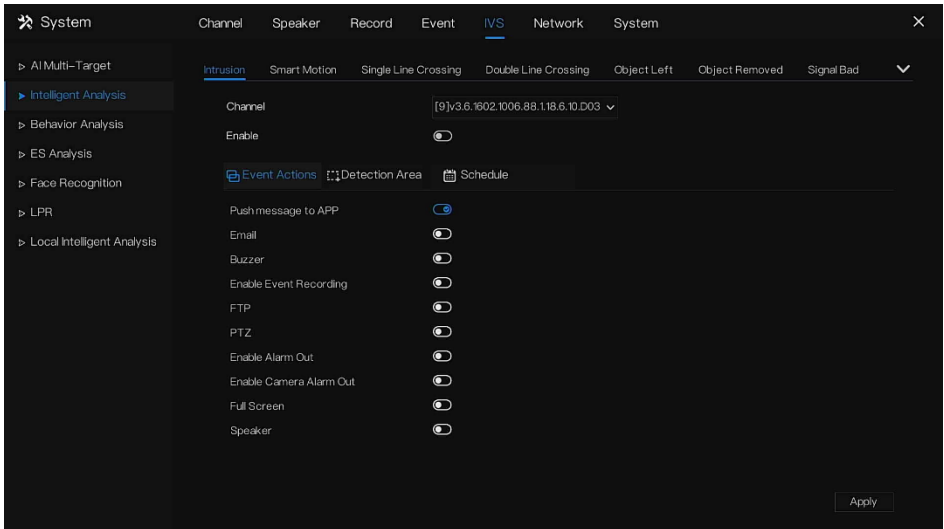
NOTE

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 4-51.

Figure 4-51 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**).

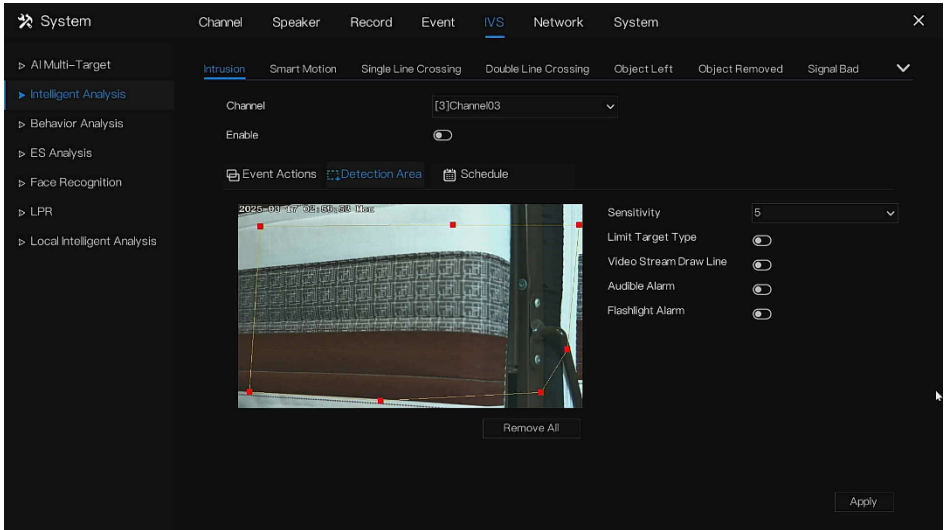
Step 3 Select a channel from the drop-down list of channels.

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 4.4.2 Motion Detection*.

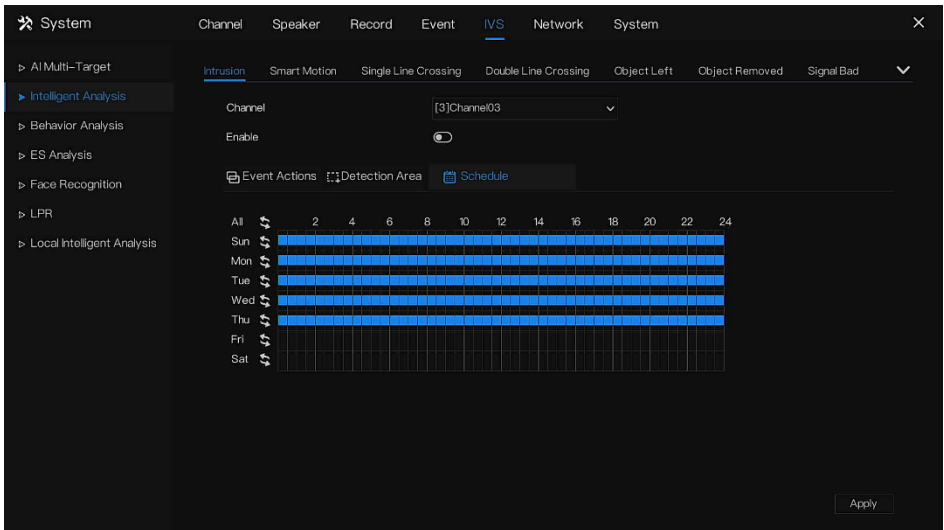
Step 6 Click the Detection Area page to set the detection area. Use the mouse to draw the polygonal region to deploy.

Figure 4-52 Detection area



Step 7 Click the Schedule page to access the schedule screen. For details, please refer to section *4.3.1 Record Schedule*.

Figure 4-53 Set schedule

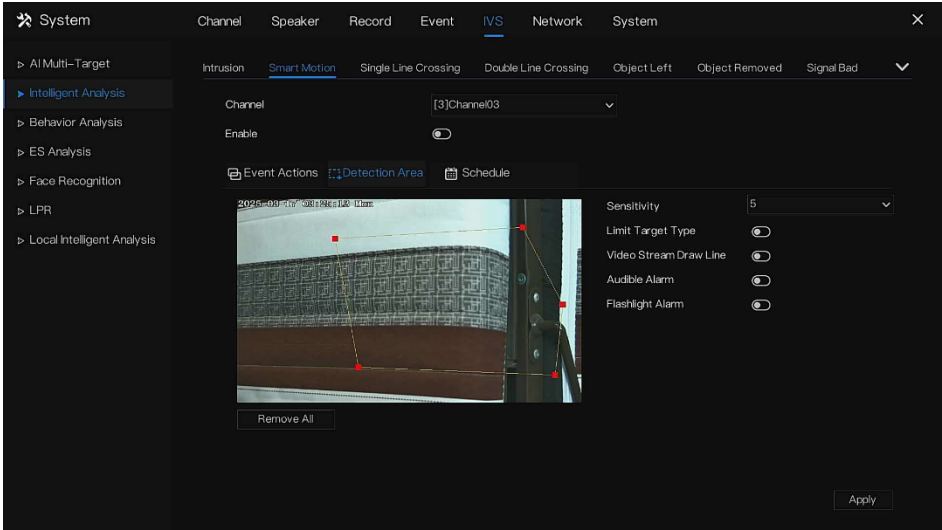


Step 8 Click **Apply** to save the settings.

4.5.1.2 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 4-54 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 4.4.2 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 4-8 Smart motion area

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

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

Step 6 Click **Apply** to save settings.

----End

People Counting:

This function is set for the channel cameras.

Figure 4-55 People counting

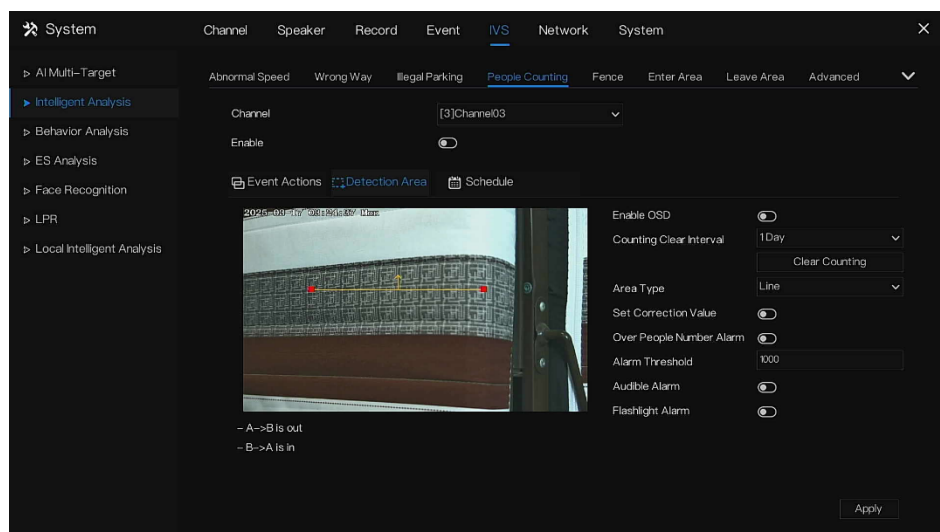


Table 4-9 People counting parameters

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 4-56 Fence

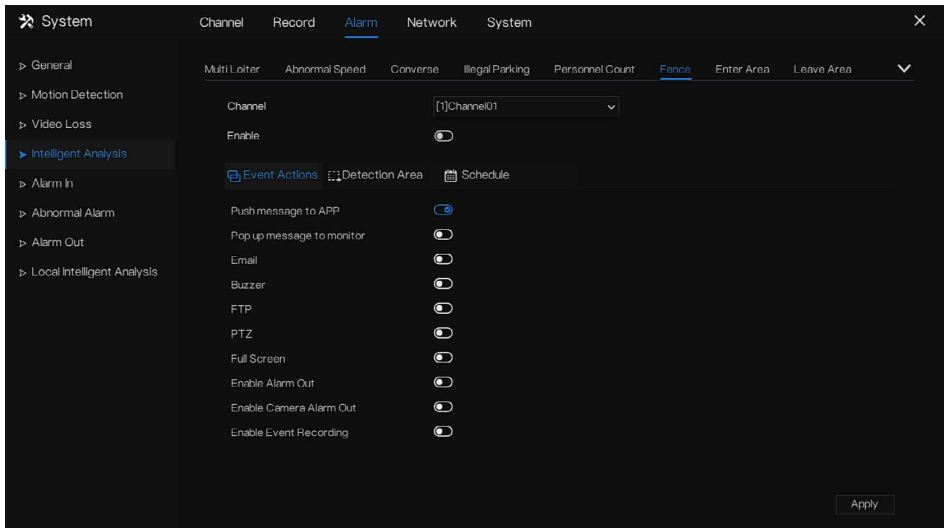
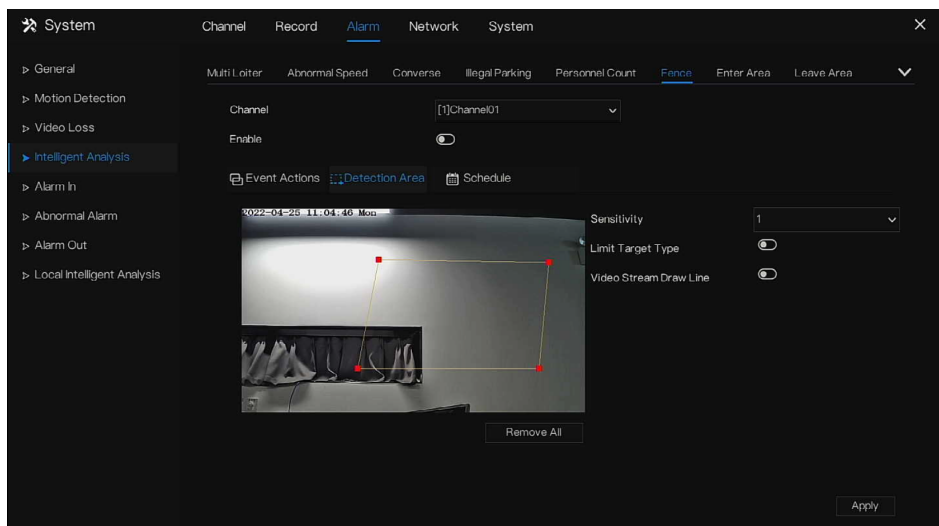


Figure 4-57 Fence detection area



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

4.6 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 4-58.

Figure 4-58 Network management screen

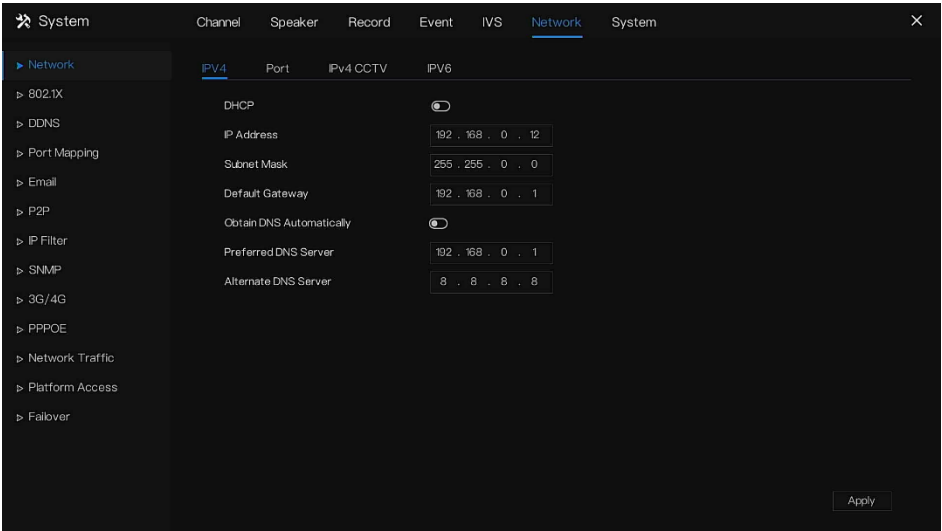


Table 4-10 Network

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.
IP Address	

Parameter	Description
Subnet Mask	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.
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.

4.6.1 Network

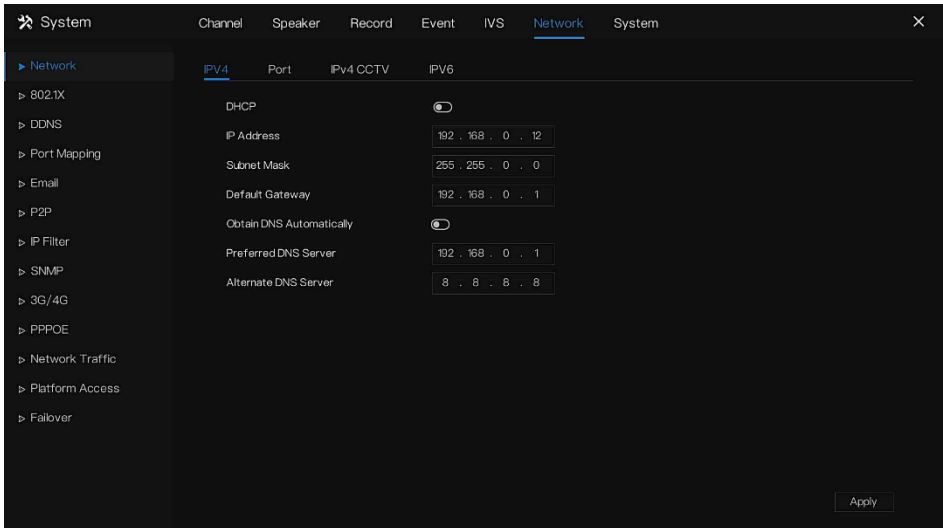
Set **DHCP** and **DNS** manually or automatically.

4.6.1.1 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 4-59 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.

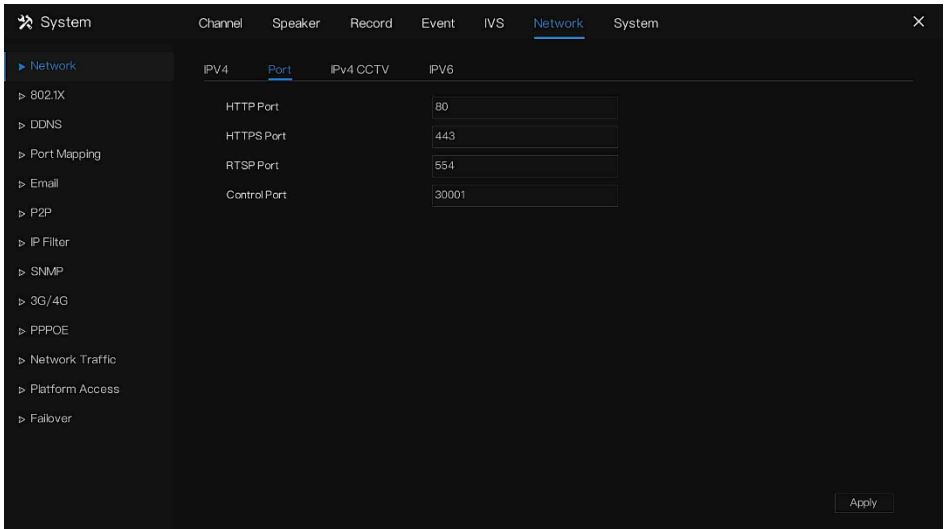
----End

4.6.1.2 Port

Operation Steps

Step 1 Click the **Port** page to access the port setting screen, as shown in Figure 4-60.

Figure 4-60 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 4-11 Port

Parameter	Description
HTTP Port	The default value setting is 80. You can enter the value according to your actual situation. If you enter another value, for example, 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  to save port settings.

----End

4.6.1.3 IPv4CCTV (Only for Some Models)

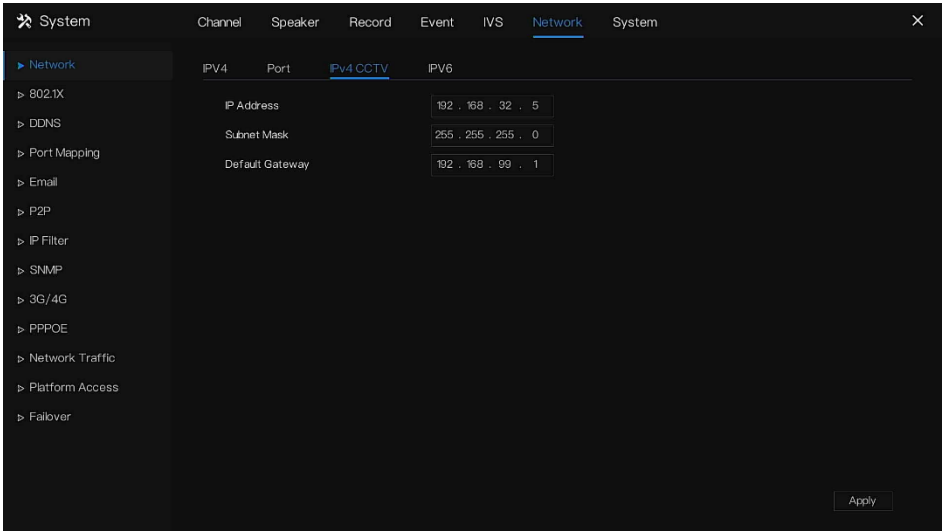
The non-POE device has two network ports, WAN and LAN.

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.

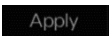
Operation Steps

Step 1 Click the **IPv4 CCTV** page to access the LAN setting screen, as shown in Figure 4-61.

Figure 4-61 IPv4 CCTV



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

Step 3 Click  to save the settings.

NOTE

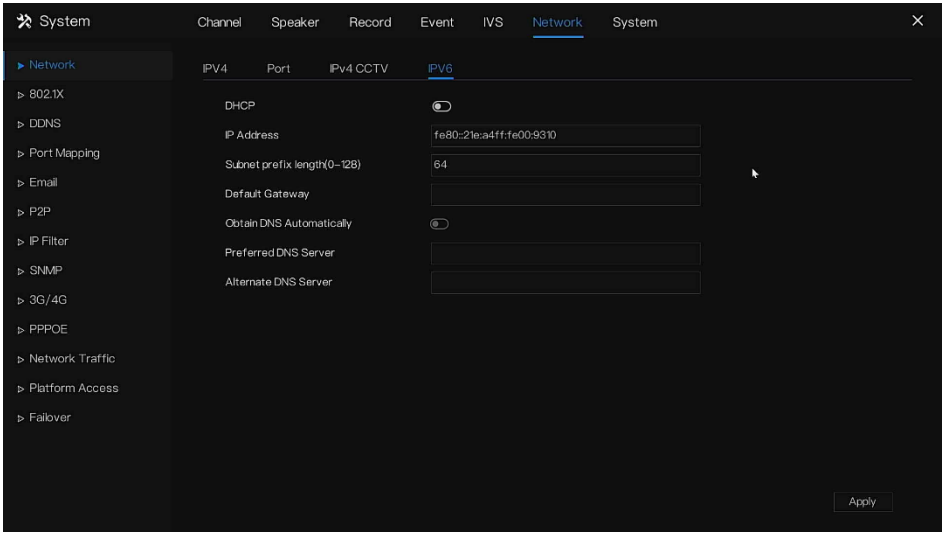
WAN and LAN can be connected to different networks so that NVR can add more cameras. WAN usually is connected to the external network to connect to the Internet; it is the default gateway. LAN connects to the internal network to add the cameras.

----End

4.6.1.4 IPV6

If the users' network router can be connected to IPV6, users can access the web through the IPV6 IP address.

Figure 4-62 IPV6



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

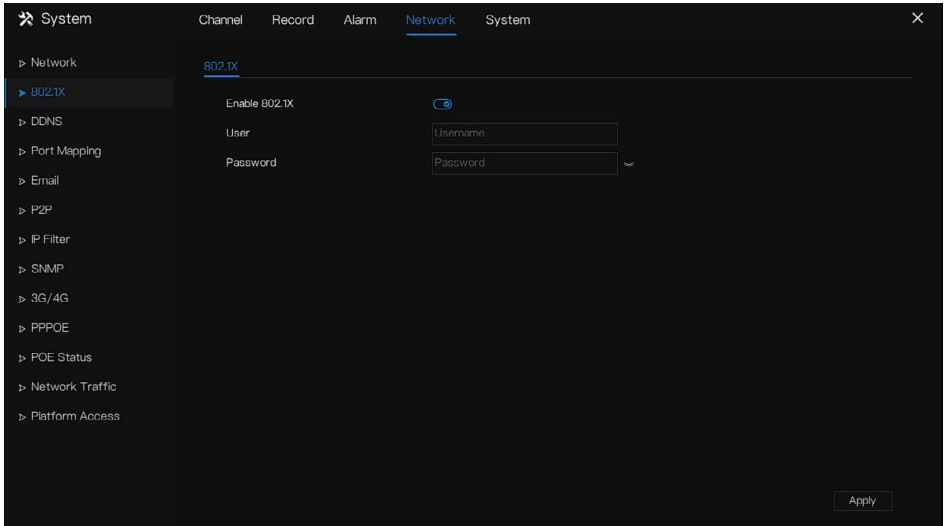
4.6.2 802.1 X

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 4-63 802.1X



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

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

----End

4.6.3 DDNS

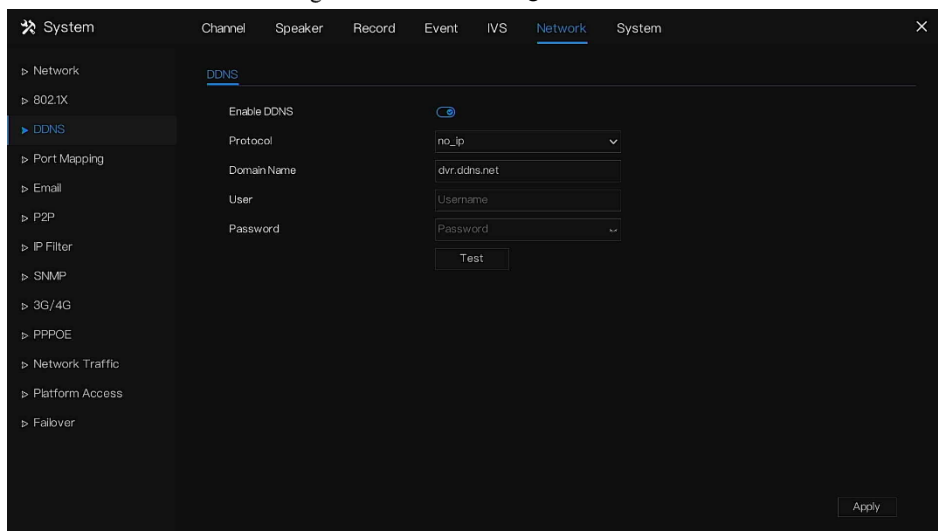
Please make sure to connect the specified camera to the Internet and obtain the user name and password for logging into the dynamic domain name system (DDNS) from the server.

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 4-64.

Figure 4-64 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

4.6.4 Port Mapping

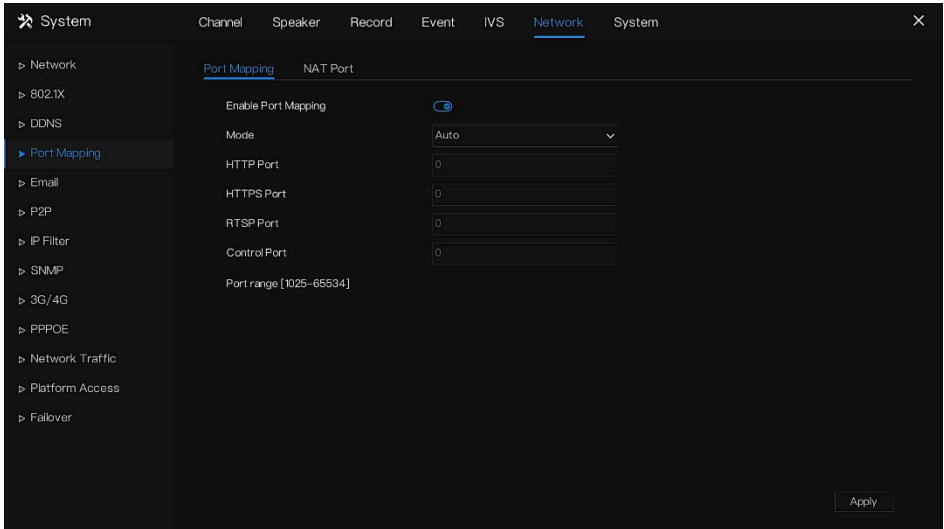
4.6.4.1 Port Mapping

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 4-65.

Figure 4-65 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 4-12 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.

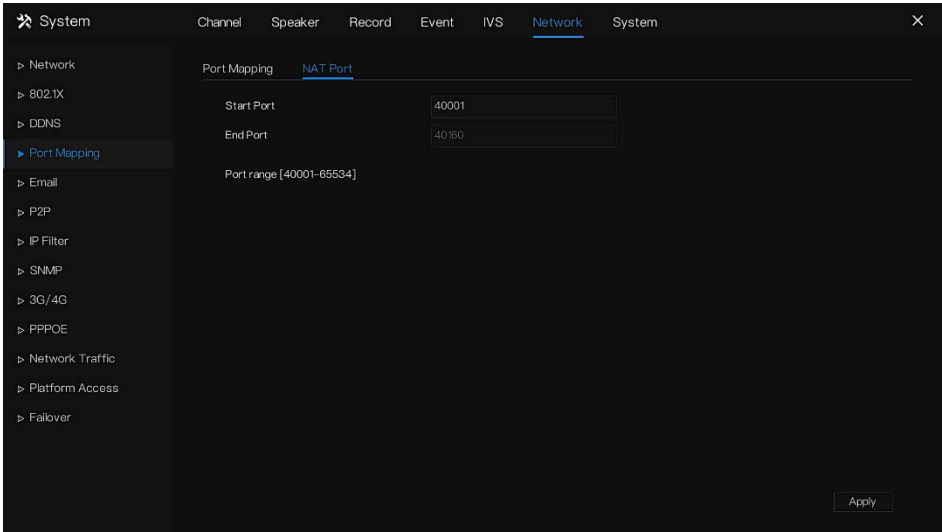
Step 5 Click  to save settings.

----End

4.6.4.2 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 4-66 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

4.6.5 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 4-67.

Step 2 Configure the settings for the email parameters.

Figure 4-67 Email setting screen

The screenshot shows a web-based configuration interface for a network device. The top navigation bar includes 'System', 'Channel', 'Speaker', 'Record', 'Event', 'IVS', 'Network' (highlighted), and 'System'. A left sidebar lists various settings: Network, 802.1X, DDNS, Port Mapping, Email (highlighted), P2P, IP Filter, SNMP, 3G/4G, PPPOE, Network Traffic, Platform Access, and Failover. The main content area is titled 'Email Server 1' and 'Email Server 2'. It contains the following fields and values:

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

Below the fields are two buttons: 'Test' and 'Apply'.

Figure 4-68 Email server 2

The screenshot shows a configuration window for 'Email Server 2'. It contains the following fields and values:

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

Buttons: 'Test' and 'Apply'.

Table 4-13 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  to save settings.

----End

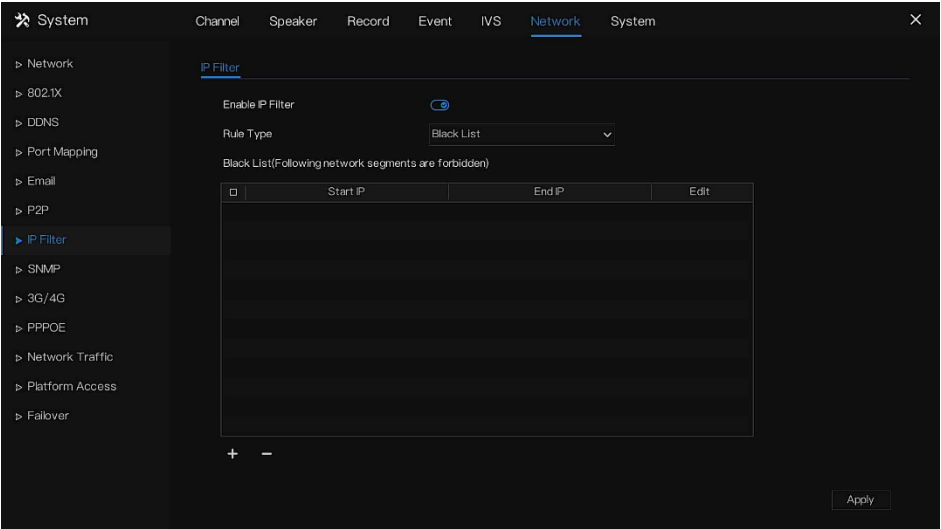
4.6.6 IP Filter

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 4-69.

Figure 4-69 IP Filter setting screen

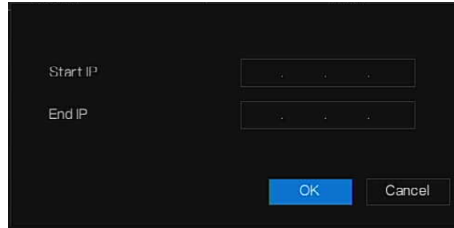


Step 2 Click  next to **IP Filter** to enable the function of IP Filter.

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 4-70.

Figure 4-70 IP Address Segment screen

The image shows a dark-themed dialog box titled "IP Address Segment". It contains two input fields: "Start IP" and "End IP", each with a dotted placeholder for an IP address. At the bottom right, there are two buttons: a blue "OK" button and a grey "Cancel" button.

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

Step 6 Click . 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

4.6.7 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 4-71.

Figure 4-71 SNMP settings screen

The screenshot shows the 'System' settings interface with the 'Network' tab selected. Under the 'Network' tab, the 'SNMPv1/2' sub-tab is active. The settings are as follows:

Parameter	Value
SNMPv1	☐
SNMPv2C	☐
Write Community	
Read Community	
Trap Address	<input "="" type="text" value="."/>
Trap Port	162
Trap Community	

An 'Apply' button is located at the bottom right.

Figure 4-72 SNMPV3

The screenshot shows the 'SNMPv3' sub-tab under the 'Network' tab. The settings are as follows:

Parameter	Value
SNMPv3	☐
Read Security Name	
Security Level	priv
Auth Algorithm	SHA
Auth Password	Password
Encry Algorithm	DES
Encry Password	Password
Write Security Name	
Security Level	priv
Auth Algorithm	SHA
Auth Password	Password
Encry Algorithm	DES
Encry Password	Password

An 'Apply' button is located at the bottom right.

Parameter	Description
SNMPV1	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.
SNMPV2C	

Parameter	Description
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 4-73.

Figure 4-73 SNMPV 1/2 interface



Table 4-14 SNMP parameters

Step 3 Input the parameters of the protocol.

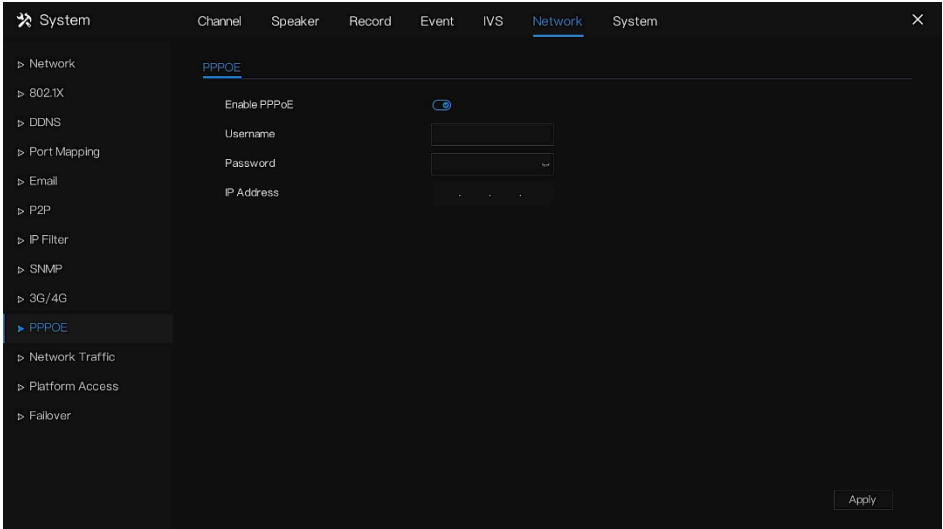
Step 4 Click  to save settings or click  to cancel settings.

----End

4.6.8 PPPOE

PPPOE Point-to-Point protocol Ethernet; the user uses the PPPOE to access the network immediately, as shown in Figure 4-74.

Figure 4-74 PPPOE

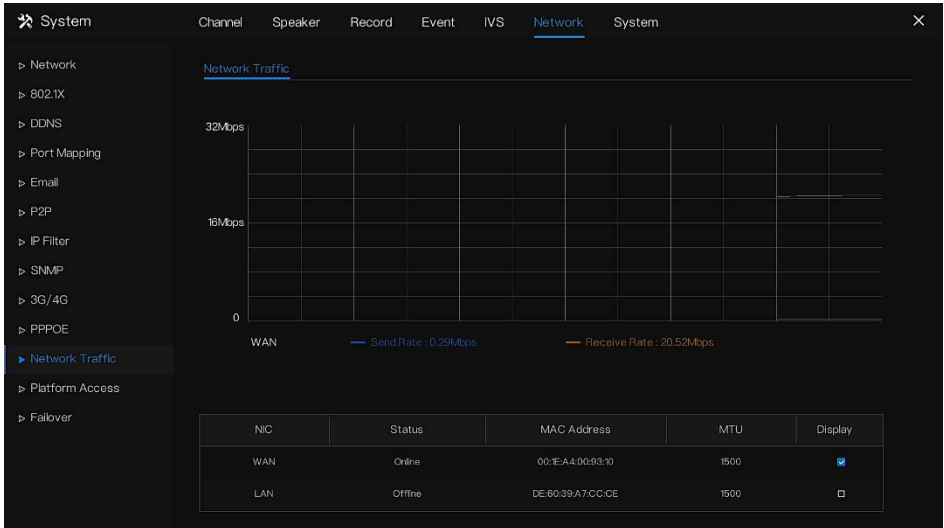


- Step 1** Enable the PPPOE function.
 - Step 2** Input the username, and password (provided by network operator).
 - Step 3** Click **Apply** to save settings, and the IP is obtained automatically.
 - Step 4** Users input the IP to access the NVR web immediately.
- End

4.6.9 Network Traffic

Users can view the network traffic immediately, as shown in Figure 4-75

Figure 4-75 Network traffic



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

----End

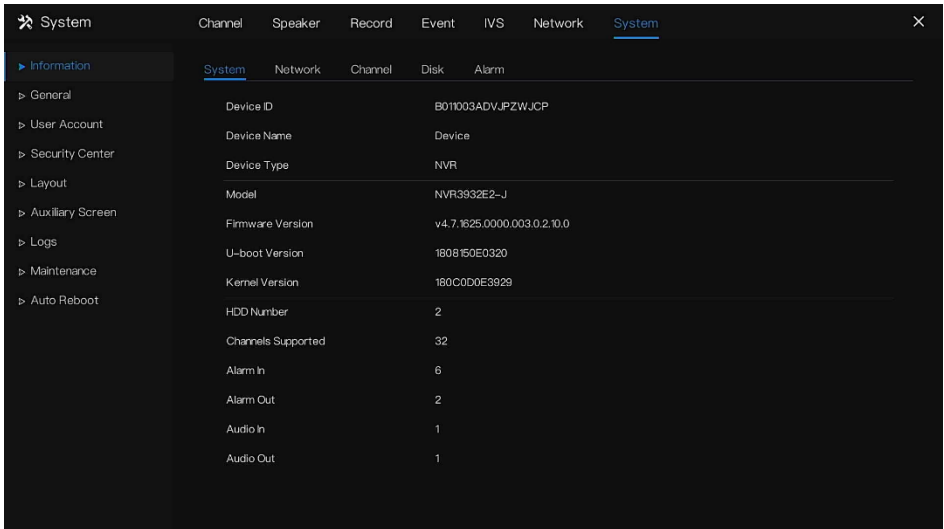
4.7 System Management

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 4-76.

Figure 4-76 System setting screen



4.7.1 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 4-77.

Figure 4-77 Information-system interface

System	Network	Channel	Disk	Alarm
Device ID	B011003ADVJPZWJCP			
Device Name	Device			
Device Type	NVR			
Model	NVR3932E2-J			
Firmware Version	v4.7.1625.0000.003.0.2.10.0			
U-boot Version	1808150E0320			
Kernel Version	180C0D0E3929			
HDD Number	2			
Channels Supported	32			
Alarm In	6			
Alarm Out	2			
Audio In	1			
Audio Out	1			

Network: status, IP address, subnet mask, default gateway, MAC address, DHCP, preferred DNS server, Alternate DNS server, total bandwidth, received packets, and so on, as shown in Figure 4-78.

Figure 4-78 Information-network interface

System	Network	Channel	Disk	Alarm
	WAN		LAN	
Status	Online			
IP Address	192.168.0.12	192.168.32.5		
Subnet Mask	255.255.0.0	255.255.255.0		
Default Gateway	192.168.0.1	192.168.99.1		
MAC Address	00:1E:A4:00:93:10	DE:60:39:A7:CC:CE		
DHCP	OFF			
Preferred DNS Server	192.168.0.1			
Alternate DNS Server	8.8.8.8			
Total Bandwidth	1000.00 Mbps			
Received Packets	20.73 Mbps			

Channel: channel, name, status, video format, resolution, bitrate (kbps), and so on, as shown in Figure 4-79.

Figure 4-79 Information-channel interface

[illegible]

Disk: disk name, capacity, used, SN, disk model, status, and so on, as shown in Figure 4-80

Figure 4-80 Information-disk interface

[illegible]

Alarm: channel, name, mode, enable, recording channel, and so on, as shown in Figure 4-81.

Figure 4-81 Information-alarm interface

System	Network	Channel	Disk	Alarm
Channel	Name	Mode	Enable	Recording Channel
Local<-1	Sensor 1	N/O	On	
Local<-2	Sensor 2	N/O	On	
Local<-3	Sensor 3	N/O	On	
Local<-4	Sensor 4	N/O	On	
Local<-5	Sensor 5	N/O	On	
Local<-6	Sensor 6	N/O	On	
Local->1		Close		
Local->2		Close		

----End

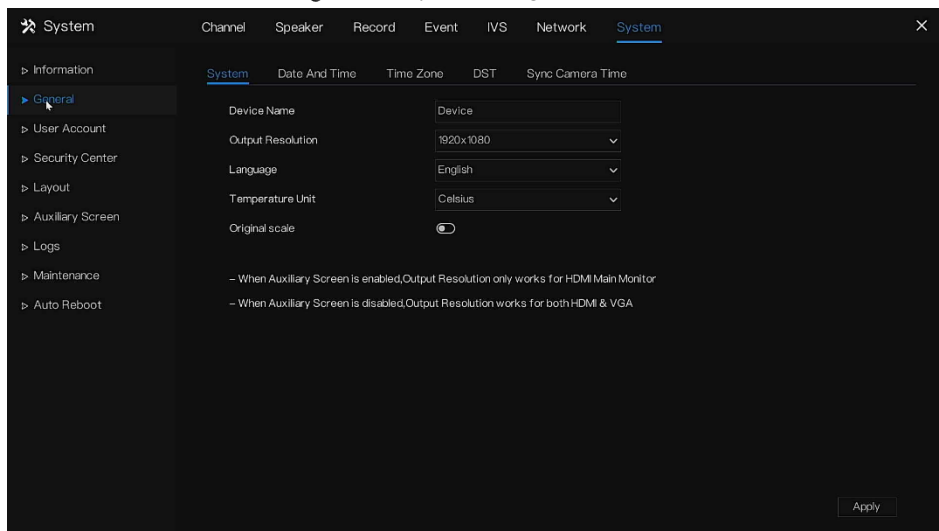
4.7.2 General

4.7.2.1 System

Operation Steps

Step 1 Click **General** on **Settings > System** to access the system screen, as shown in Figure 4-82.

Figure 4-82 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 4-83 Disable Original scale

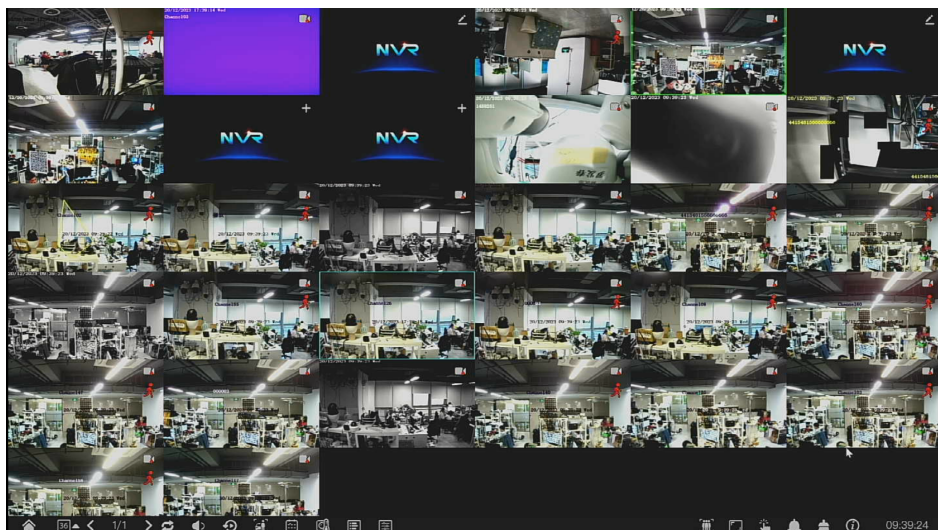
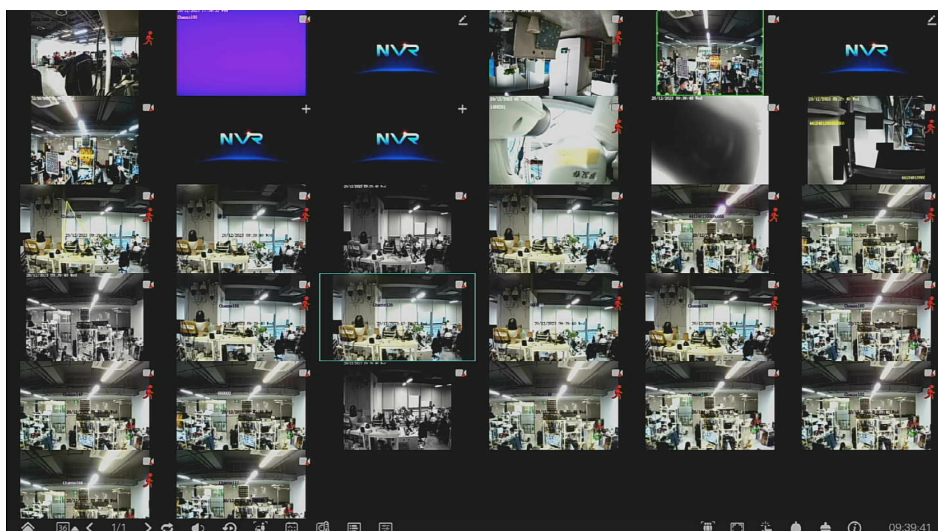


Figure 4-84 Enable Original scale



Step 7 Click **Apply** to save settings.

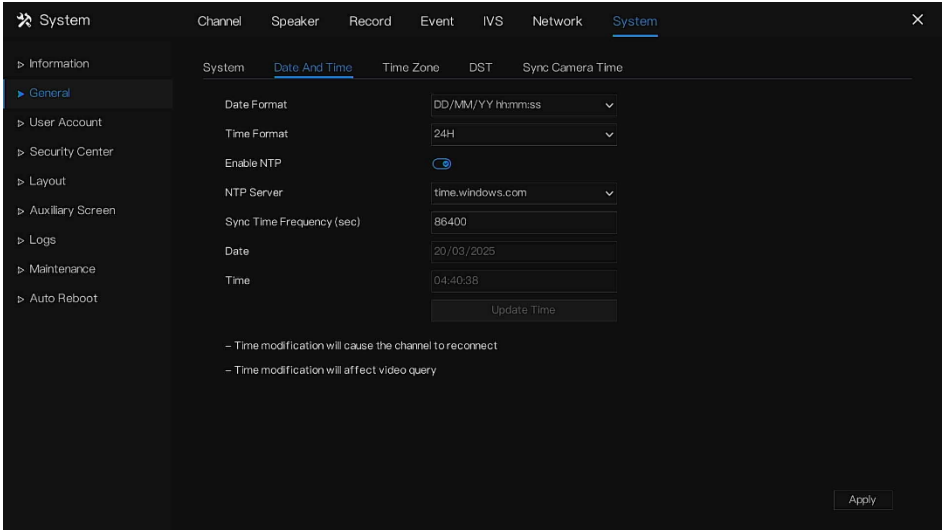
---End

4.7.2.2 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 4-85.

Figure 4-85 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 4-15 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.

Parameter	Description
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.

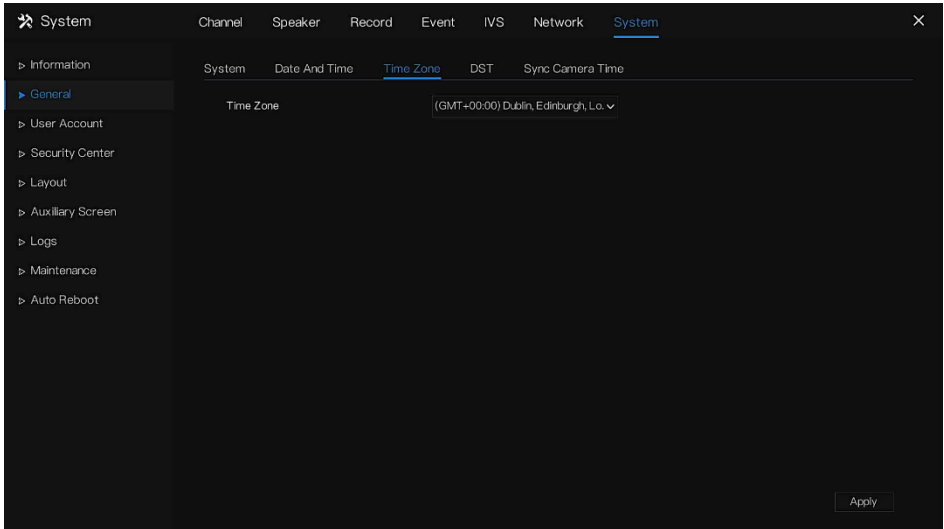
---End

4.7.2.3 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 4-86.

Figure 4-86 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

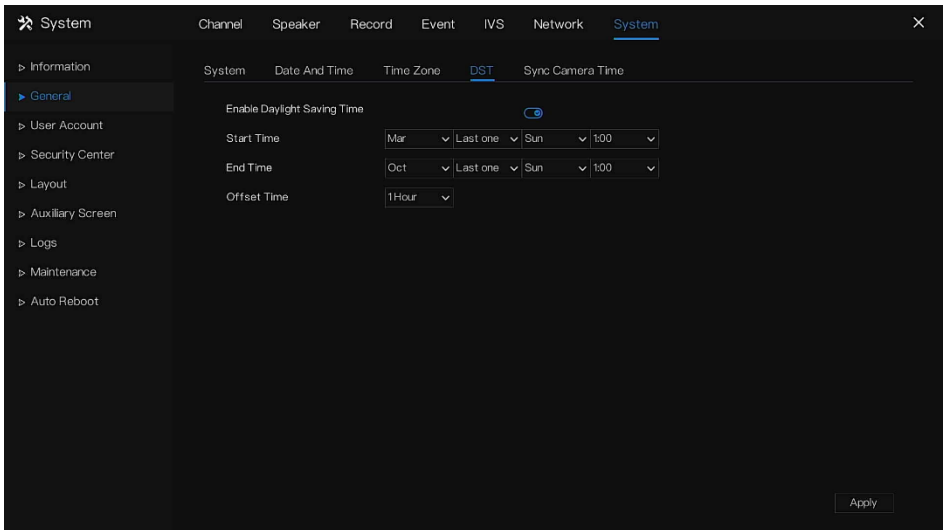
4.7.2.4 DST

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 4-87.

Figure 4-87 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.

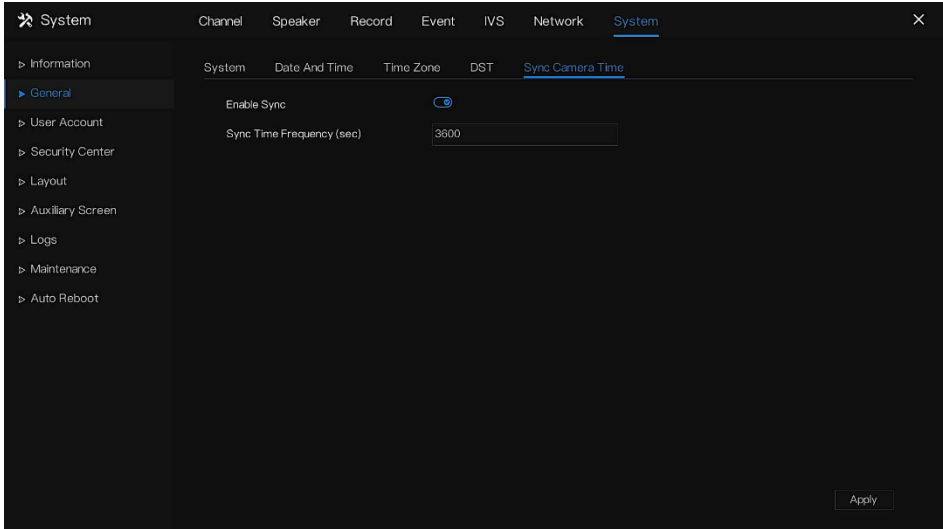
Step 4 Click  to save settings.

---End

4.7.2.5 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 4-88 Sync camera Time



---End

4.7.3 User Account

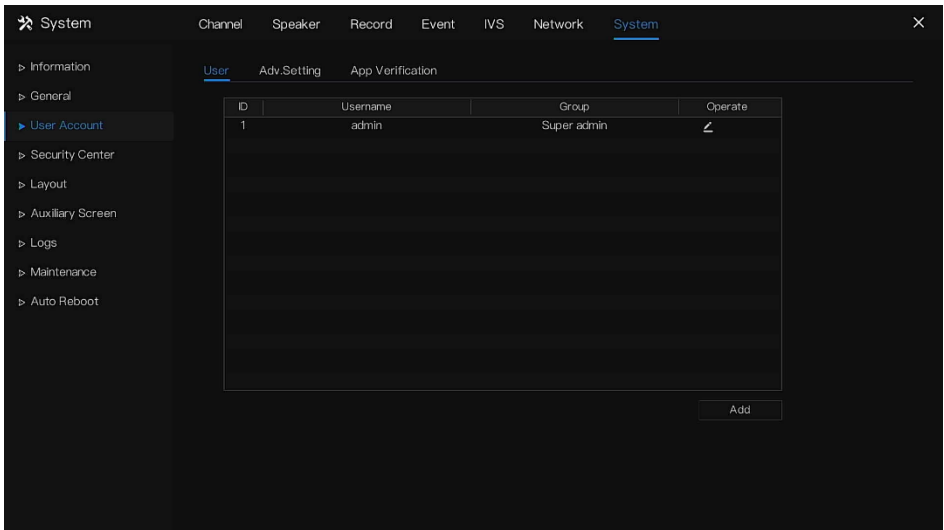
Add, modify, and delete a user and privilege in the user screen. The admin user can dispose of privileges to different users.

4.7.3.1 User

Operation Steps

Step 1 Click **User** on **Settings > System > User Account** to access the user screen, as shown in Figure 4-89.

Figure 4-89 User management screen

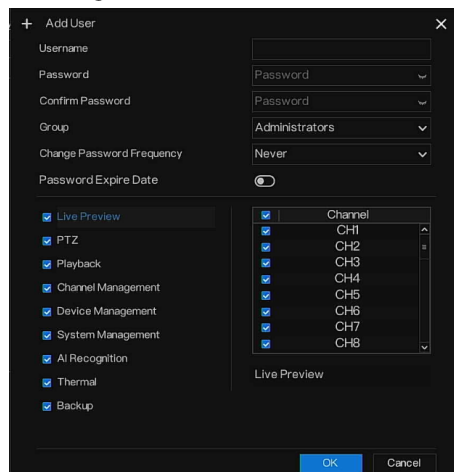


Step 2 Add or delete a user.

- Add a user

Click **Add** and the **Add User** dialog box appears, as shown in Figure 4-90.

Figure 4-90 Add user screen



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

Table 4-16 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 . The user is set successfully.

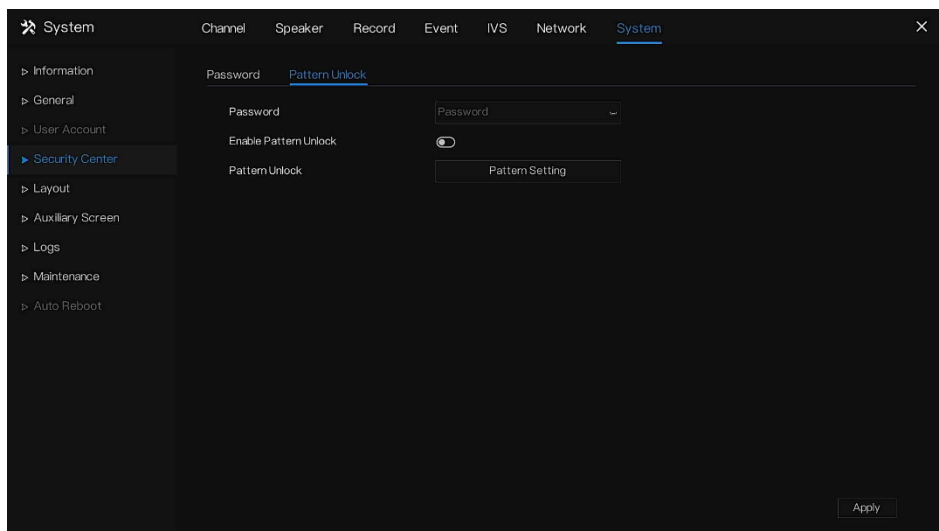
NOTE

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 4-91 General user set pattern to unlock.



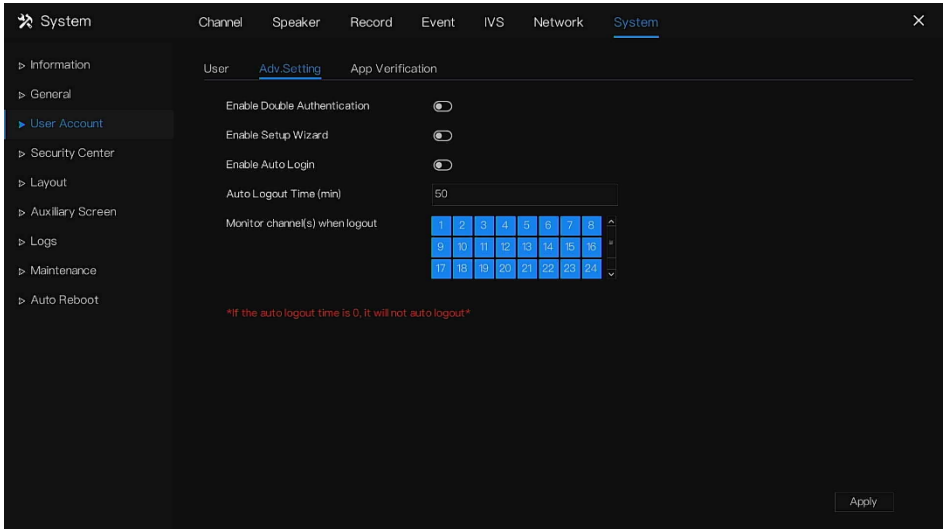
-----End

4.7.3.2 Advance Setting

Operation Steps

Step 1 Click **Adv Setting** on **Settings > System > User Account** to access the Advanced setting screen, as shown in Figure 4-92.

Figure 4-92 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  to save settings.

-----End

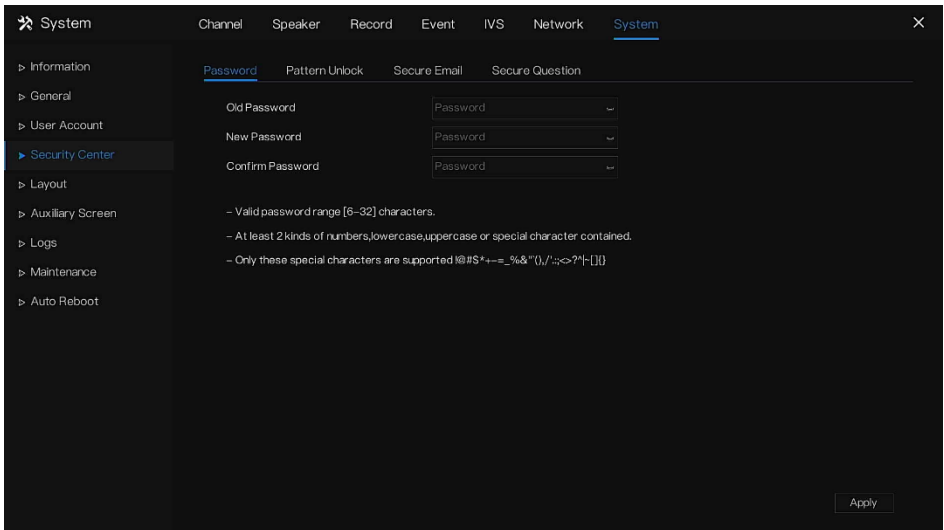
4.7.4 Security Center

4.7.4.1 Password

Operation Steps

Step 1 Click **Security Center** on **Settings > System** to access the modified password screen, as shown in Figure 4-93.

Figure 4-93 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  to save modified password settings.

----End

4.7.4.2 Pattern Unlock



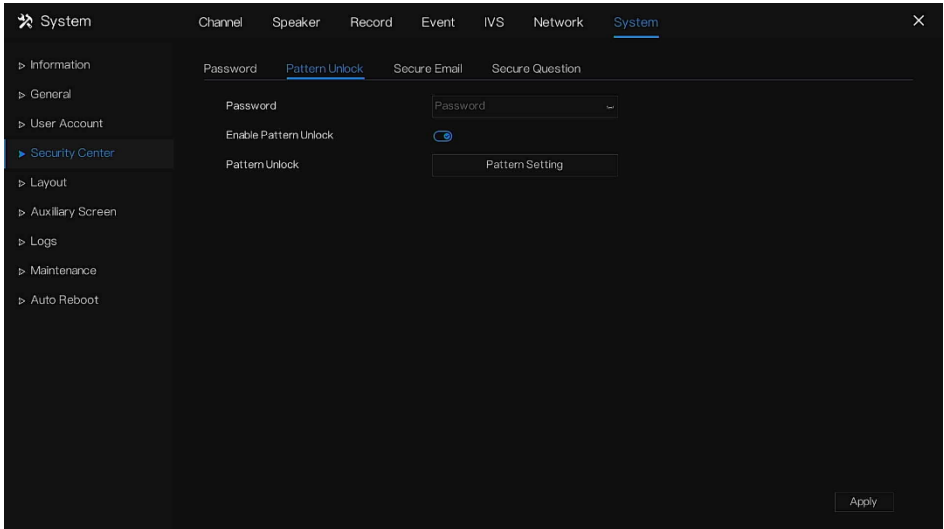
NOTE

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 4-94.

Figure 4-94 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**

4.7.4.3 Secure Email

Set the email to receive the verification code to create a new password, as shown in Figure 4-95.

Figure 4-95 Secure Email

The screenshot shows a web interface for system configuration. At the top, there is a navigation bar with tabs: Channel, Speaker, Record, Event, IVS, Network, and System (which is selected). Below the navigation bar, there is a left sidebar with a tree view containing: Information, General, User Account, Security Center (highlighted), Layout, Auxiliary Screen, Logs, Maintenance, and Auto Reboot. The main content area is titled 'Secure Email' and has sub-tabs: Password, Pattern Unlock, Secure Email (selected), and Secure Question. Under the 'Secure Email' sub-tab, there are two fields: 'Verify Password' and 'Email Address'. The 'Verify Password' field has a dropdown menu showing 'Password'. The 'Email Address' field contains the text '*****@gmail.com'. At the bottom right of the main content area, there is an 'Apply' button.

Step 1 Input the password of NVR.

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

Step 3 Click  to save the setting.

----End

4.7.4.4 Secure Question

Set the questions to create a new password, as shown in Figure 4-95.

Figure 4-96 Secure question

The screenshot shows a web-based system management interface. At the top, there is a navigation bar with tabs: Channel, Speaker, Record, Event, IVS, Network, and System (which is currently selected). Below the navigation bar, on the left, is a sidebar menu with options: Information, General, User Account, Security Center (highlighted), Layout, Auxiliary Screen, Logs, Maintenance, and Auto Reboot. The main content area is titled 'Secure Question' and contains the following fields:

Field	Value
Password	Password
Question one	The brand and model of your favori
Question one answer	
Question two	Your favorite team
Question two answer	
Question three	Your favorite city
Question three answer	

Below the questions, there are two instructions:

- Please enter at least 1 characters for the answer
- Please enter up to 32 characters for the answer

An 'Apply' button is located at the bottom right of the form.

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

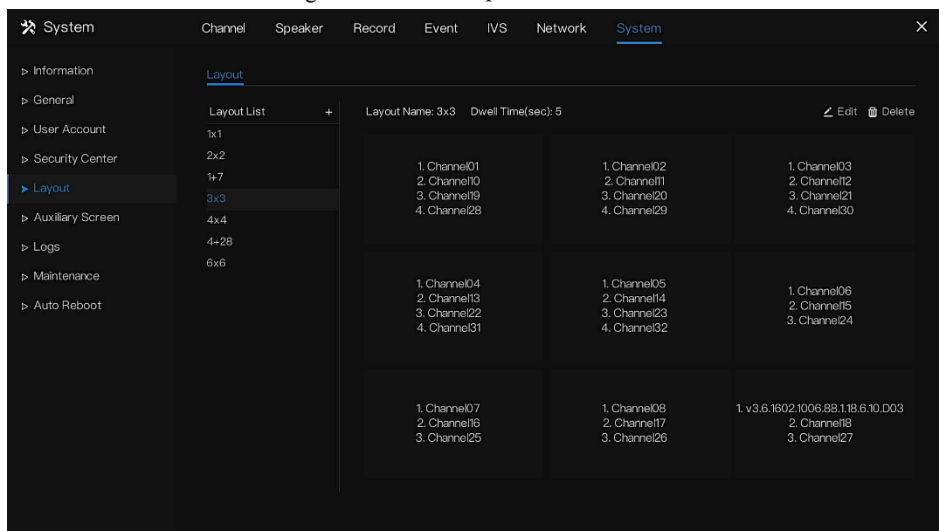
4.7.5 Layout

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

Operation Steps

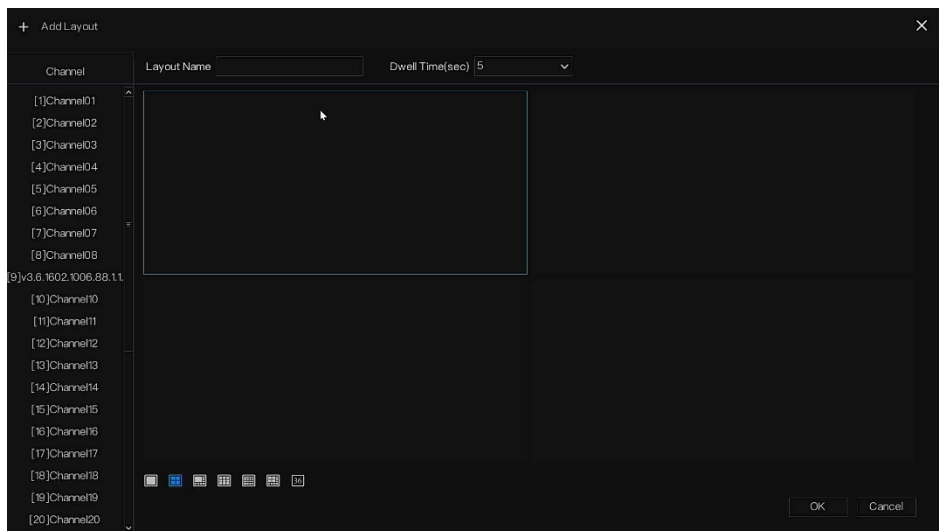
Step 1 Click **Layout** in the Setting System or menu of the system management screen and choose **Layout** to access the display screen, as shown in Figure 4-97.

Figure 4-97 Auto Sequence screen



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

Figure 4-98 Add a new layout

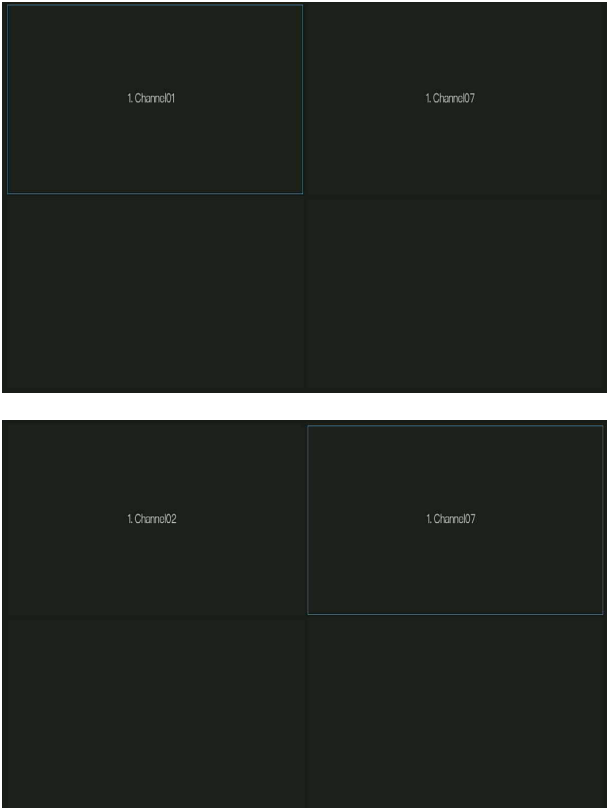


Step 3 Input the layout name, and select dwell time from the **SEQ** Dwell time drop-down list(the display screen will loop play the real-time video according to setting time).

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 4-99 Auto sequence



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

 NOTE

Users can add up to 16 layouts.

----End

4.7.6 Logs

4.7.6.1 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 4-100.

Figure 4-100 Log screen

System
Channel
Speaker
Record
Event
IVS
Network
System

Information
System Log
Event Log

General
Start Date: 19/03/2025
Start Time: 08:18:53

User Account
End Date: 20/03/2025
End Time: 08:18:53

Security Center
Type: Operation Log
Search
Export

Layout

Auxiliary Screen

Logs

Maintenance

Auto Reboot

ID	Start Time	Channel	Log Type	Information
1	20/03/2025 08:17:15	--	Config changed	[admin] Local UI System[Device,Output resolu
2	20/03/2025 08:17:15	--	Login	[admin] 127.0.0.1 login
3	20/03/2025 08:18:54	--	Logout	[admin] Local UI logout
4	20/03/2025 08:18:52	--	Power On	system
5	20/03/2025 08:11:49	--	Config changed	[admin] Local UI Auxiliary Screen[Enable,resol
6	20/03/2025 08:11:48	--	Reboot	[admin] 127.0.0.1
7	20/03/2025 07:50:00	--	Config changed	[admin] Local UI System[Device,Output resolu
8	20/03/2025 07:50:00	--	Login	[admin] 127.0.0.1 login
9	20/03/2025 07:48:40	--	Logout	[12e] Local UI logout
10	20/03/2025 06:55:40	--	Config changed	[12e] Local UI System[Device,Output resolutio
11	20/03/2025 06:55:40	--	Login	[12e] 127.0.0.1 login
12	20/03/2025 06:55:20	--	Logout	[admin] Local UI logout
13	20/03/2025 06:55:13	--	Config changed	[admin] Local UI User Account -- User(add)
14	20/03/2025 06:34:55	--	Config changed	[admin] Local UI System[Device,Output resolu
15	20/03/2025 06:34:54	--	Login	[admin] 127.0.0.1 login

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 to query logs.

Step 5 Click **Export** to export logs to flash disk.

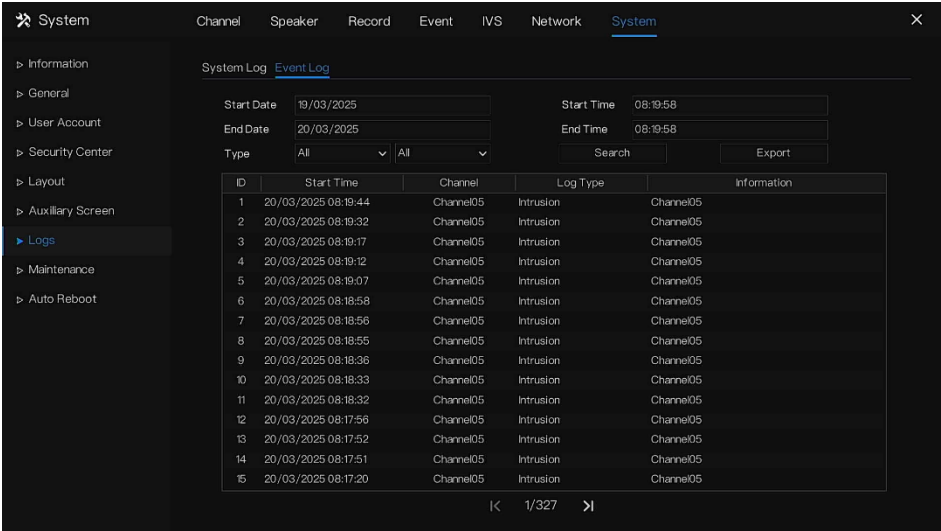
Step 6 The logs can be saved to a flash disk and hard disk at the same time, the newest logs are saved to a flash disk, and the old logs will be transferred to a hard disk.

----End

4.7.6.2 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 4.7.6.1.

Figure 4-101 Event Log

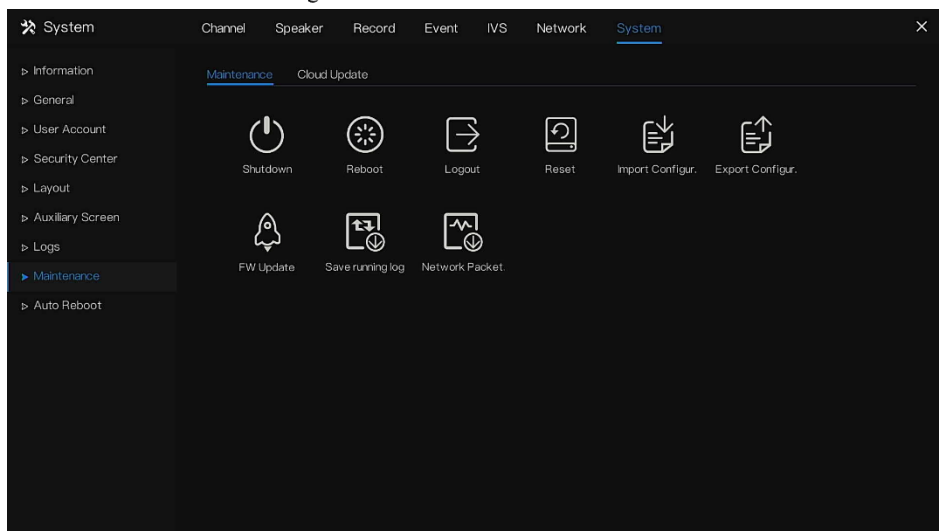


4.7.7 Maintenance

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 4-102.

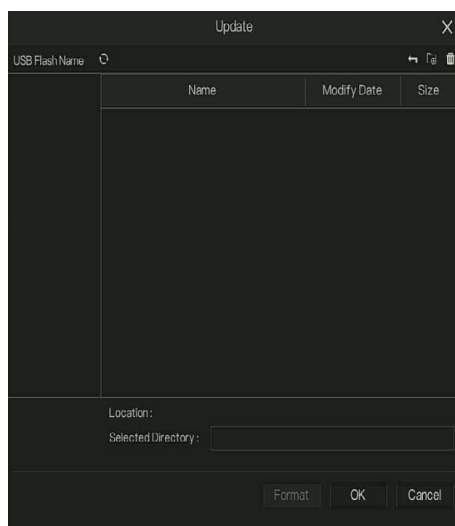
Figure 4-102 Maintenance screen



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 4-103 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.

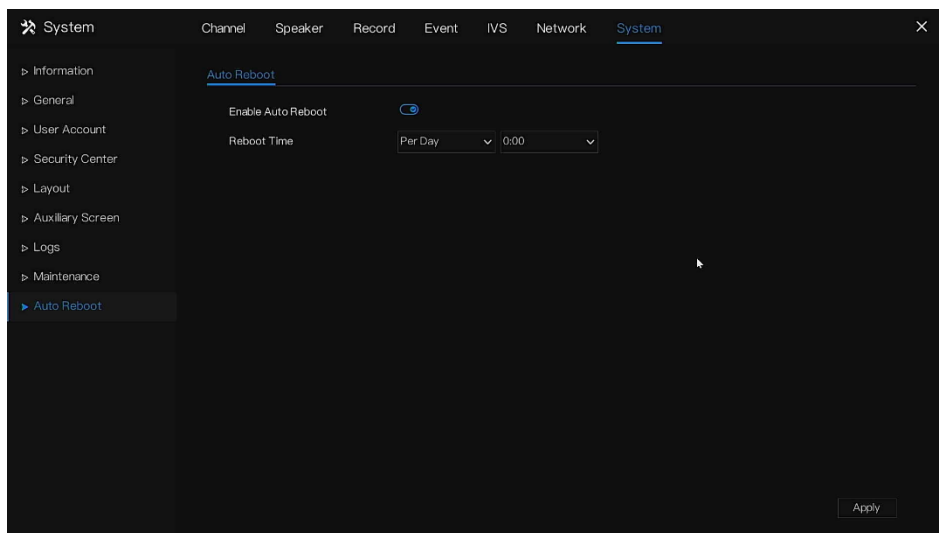
----End

4.7.8 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 4-104.

Figure 4-104 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

5 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.

5.1 Activation

Open the browser, enter the IP address of the NVR (the default value is `https://192.168.0.21`) 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 5-1 Activation

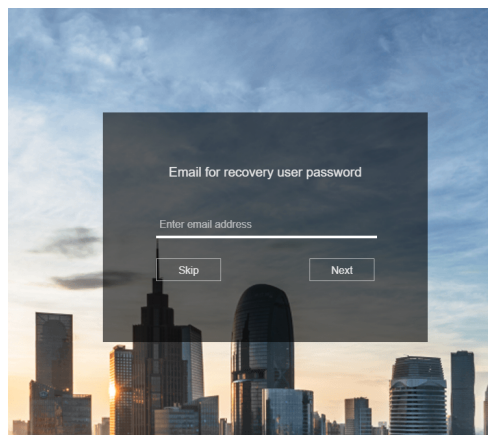


Step 1 Set the password and confirm the password.

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 5-2 Email



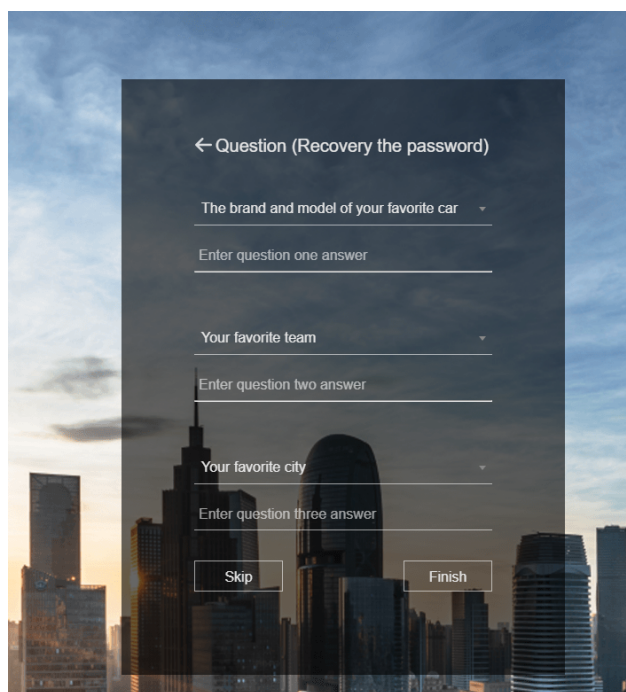
Email for recovery user password

Enter email address

Skip Next

Step 4 Set the question to recover the password.

Figure 5-3 Question



← Question (Recovery the password)

The brand and model of your favorite car

Enter question one answer

Your favorite team

Enter question two answer

Your favorite city

Enter question three answer

Skip Finish

NOTE

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

5.2 Login and Logout



CAUTION

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

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: `https://192.168.0.21`) in the address box, and press **Enter**.

The login page is displayed, as shown in Figure 5-4.

Figure 5-4 Login page interface



Step 2 Input the user name and password.



NOTE

- The default user name. The password is incorrect more than 5 times: please login again after 1 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 5-5.

Figure 5-5 Homepage interface 1

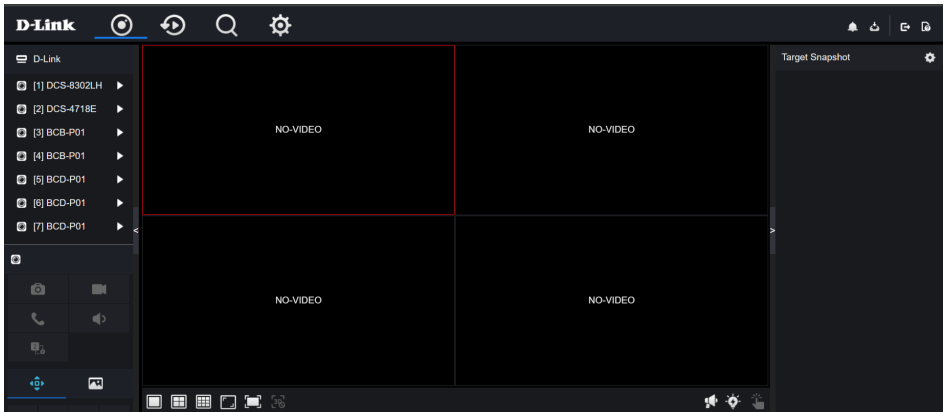
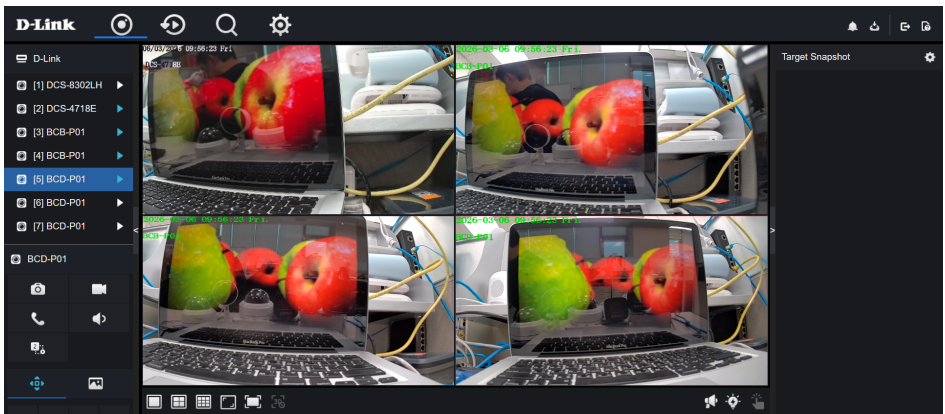


Figure 5-6 Homepage interface 2



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  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, snapshot, setting image parameters access, configuration, PTZ control, and so on. Figure 3-128 shows the overall layout of the interface. For descriptions of the interface, please refer to Table 5-1.

Figure 5-7 Homepage layout

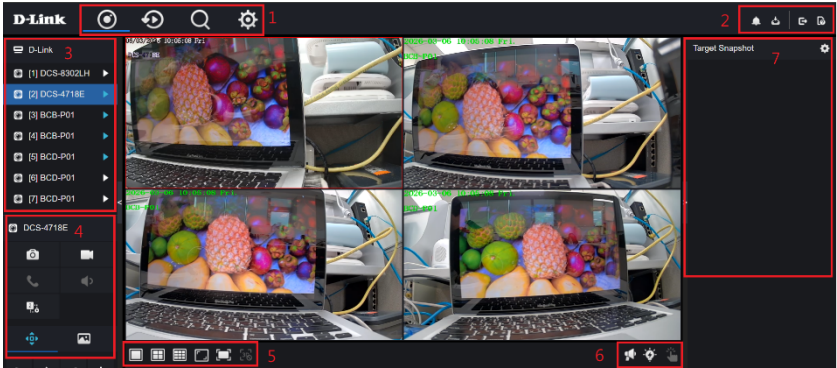


Table 5-1 Descriptions of homepage

No.	Function	Description
1	Function navigation bar	The main functions navigation bar of the device include Live Video, Playback, Event Recording, 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	Depend on NVR support video channel quantity, 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 錯誤! 找不到參照來源。

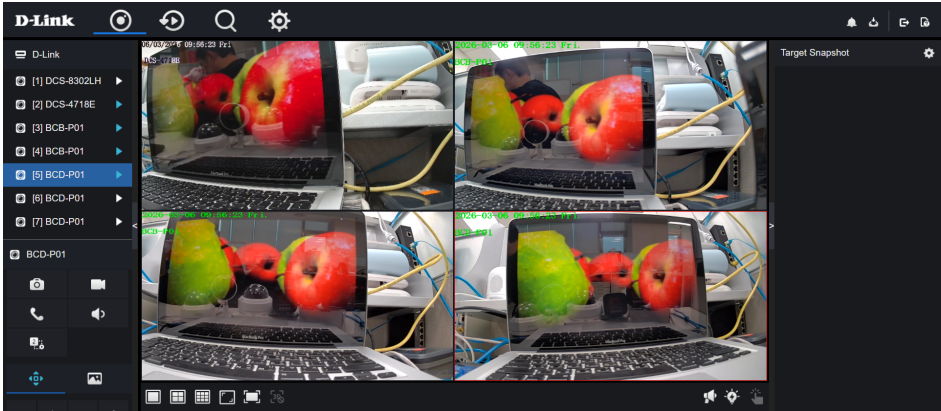
8		 Broadcast. When you add the IP speakers to the NVR, users can broadcast the local audio file to the alarm.  Manual control light, support flashlight, red and blue light, and white light. If the camera has a light, you can control the light manually.  Manual alarm. Trigger and close the external alarm device manually.
---	--	---

5.2.2 Live Video

Descriptions

After logging in to the device, click online channel; you can view the real-time videos, as shown in Figure 5-89.

Figure 5-8 Real-time videos interface



5.2.3 Channel Operation

Descriptions

Channel operation includes snapshot, record, stream switch, and audio on/off. Table 5-2 describes the operations.

Table 5-2 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).
	Enable/Disable video.	Click the button to enable the audio, and click again to disable the audio.

5.2.4 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 5-9. Table 5-3 describes the operations.

Figure 5-9 PTZ control interface

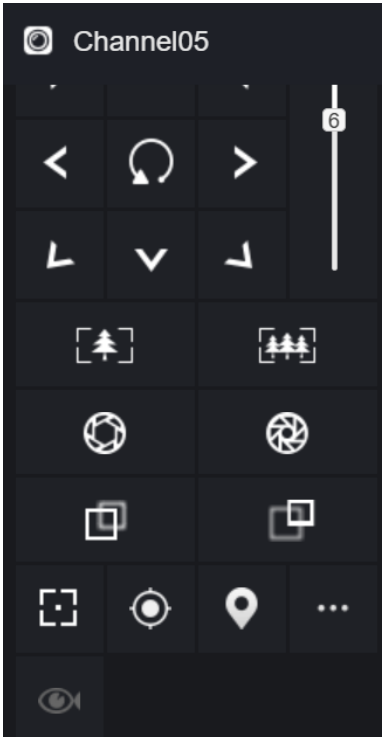


Table 5-3 Device parameters

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.

5.2.5 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 5-101. Table 5-4 describes the operations.

Figure 5-10 Image parameter interface

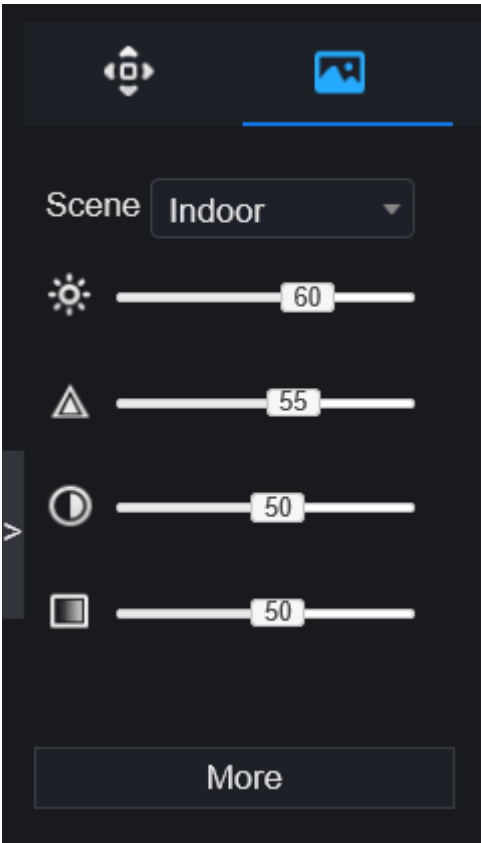
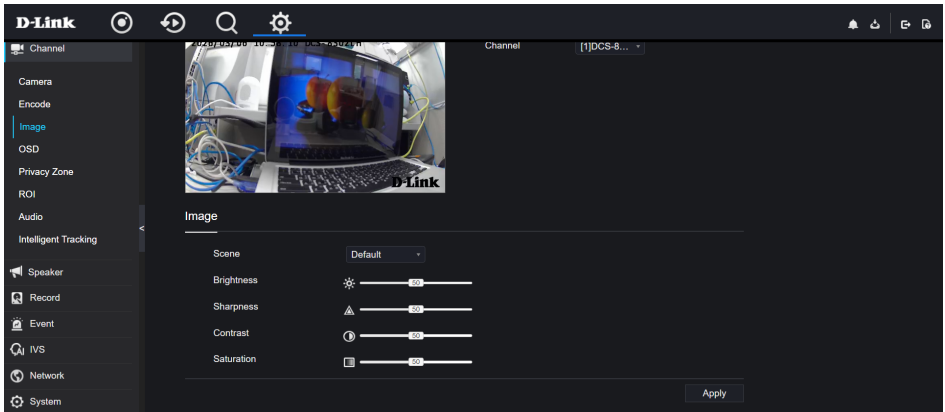


Table 5-4 Device parameters

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 5-112.

Figure 5-11 Sensor setting interface



5.2.6 Layout



Click    at the bottom left corner of the real-time videos interface; Depend on NVR support video channel quantity, the buttons indicate 1 screen, 4 screens, 9 screens from left to right.

5. 3 Playback

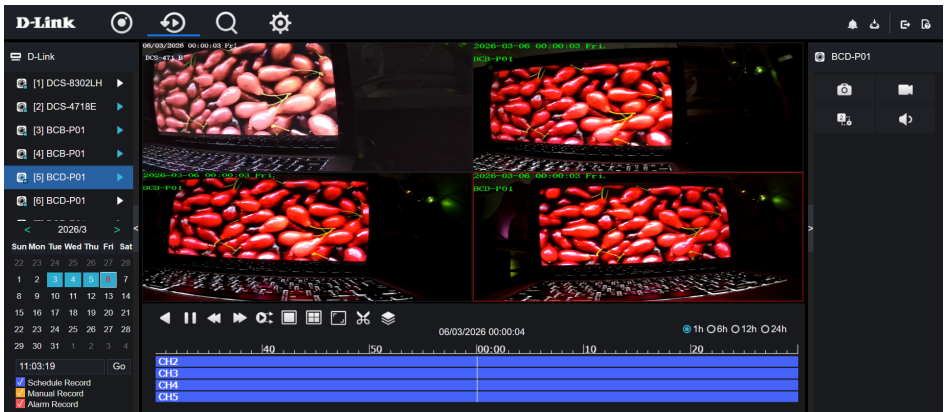
5.3.1 Video Playback

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 5-123.

Figure 5-12 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.

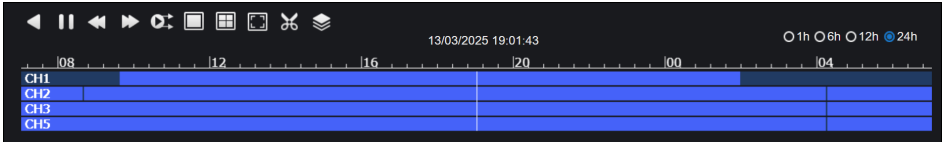
After a device and date are selected, video information is displayed below the video pane. The time scale above the file axis shows the different time points of video recording. The time in blue in the middle is the time of the video playing.

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 5-134 shows the control bar of video playback.

Figure 5-13 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.

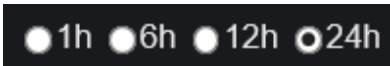
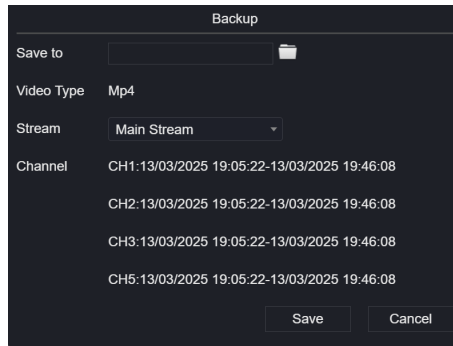


Open original scale/Close original scale.

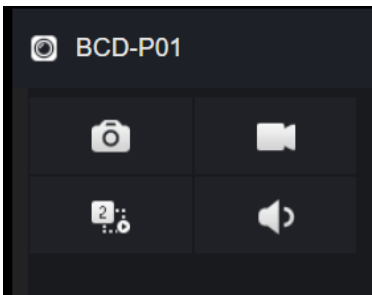


Backup. Click the icon to start up the recording and drag the time bar to quickly back up. Click again to make sure of the backup.

Figure 5-14 Backup



Types of time bar/interval.



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

5.4 Alarm Search

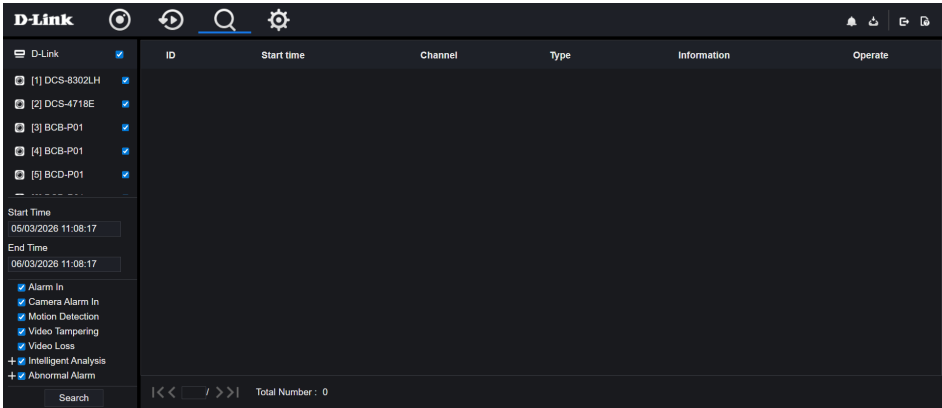
You can search for channel alarms and system alarms in the alarm search interface.

5.4.1 Channel Alarm

Procedure

Step 1 Click  on the function navigation bar and the channel alarm interface is displayed, as shown in Figure 5-1516.

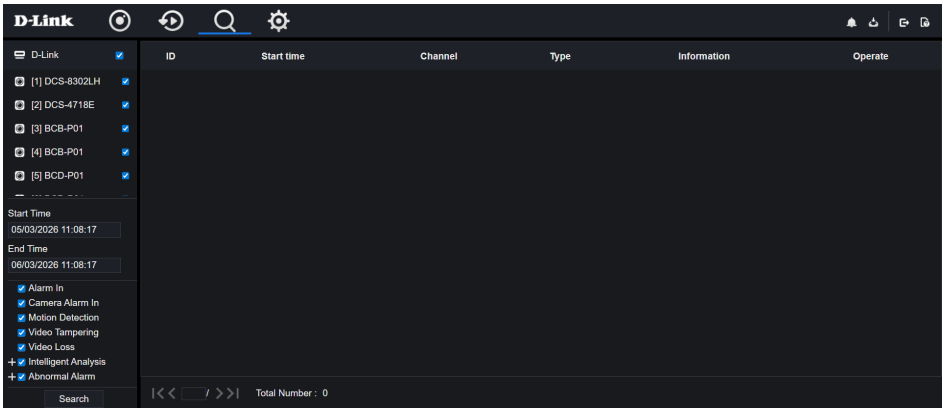
Figure 5-15 Channel alarm interface



Step 2 Choose the alarm type to search.

Step 3 Click **Search**. The result will be displayed as shown in Figure 5-1617.

Figure 5-16 Channel alarm result



NOTE

Click  to select the page of the alarm list.

20 alarm messages are shown on every page.

6 System Setting

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

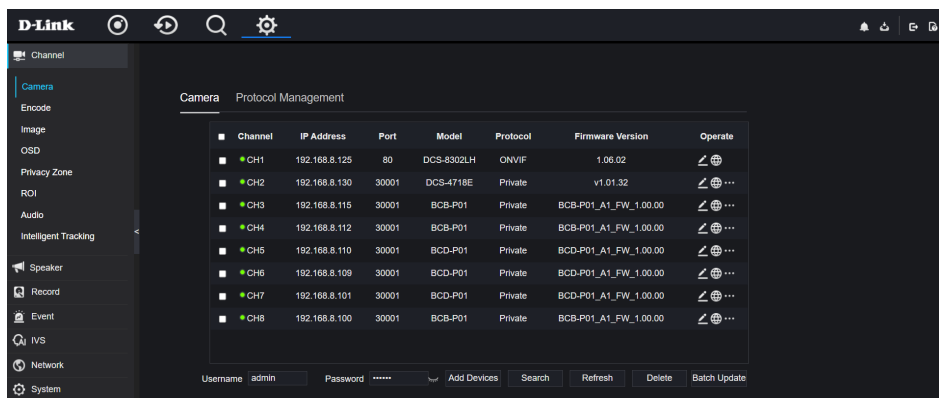
6.1 Channel

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

6.1.1 Camera

Step 1 On the **System Setting** screen, choose **Channel > Camera** to access the camera interface, as shown in Figure 6-1.

Figure 6-1 Camera interface

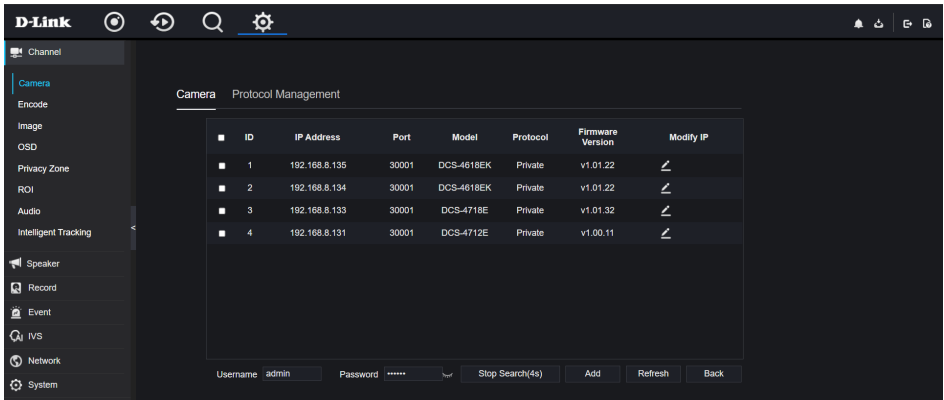


Step 2 Input username and password, and click/add cameras automatically.

Step 3 Click **Search** to search cameras at the same LAN as NVR, as shown in Figure 6-2.

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

Figure 6-2 Device search



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

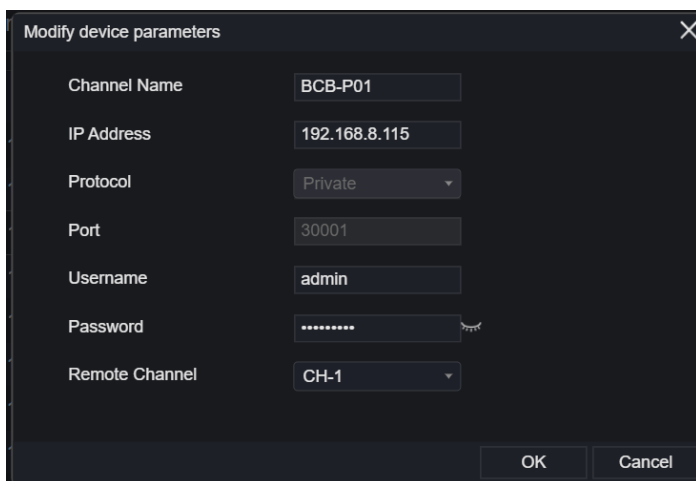
Step 5 Click **Refresh** to refresh the camera status.

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 6-3.

Figure 6-3 Modify device parameters



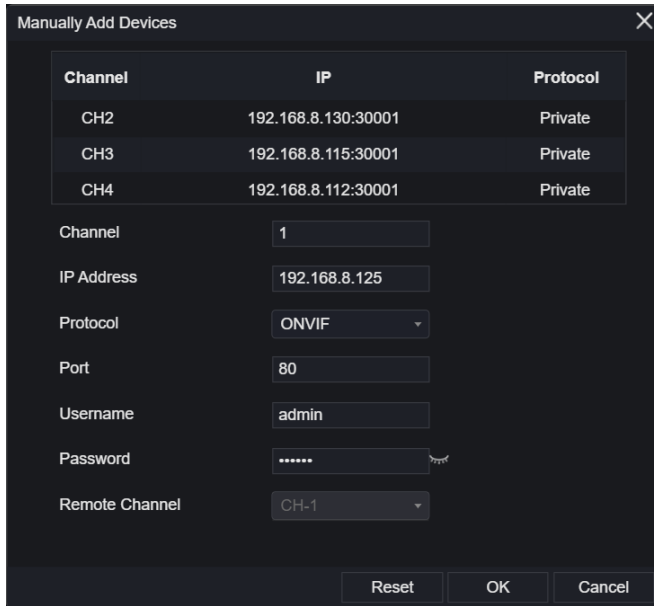
The screenshot shows a dark-themed dialog box titled "Modify device parameters" with a close button (X) in the top right corner. The dialog contains several input fields and dropdown menus:

- Channel Name: BCB-P01
- IP Address: 192.168.8.115
- Protocol: Private (dropdown menu)
- Port: 30001
- Username: admin
- Password: masked with asterisks (password icon on the right)
- Remote Channel: CH-1 (dropdown menu)

At the bottom right of the dialog are two buttons: "OK" and "Cancel".

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 6-4.

Figure 6-4 Add camera manually



Channel	IP	Protocol
CH2	192.168.8.130:30001	Private
CH3	192.168.8.115:30001	Private
CH4	192.168.8.112:30001	Private

Channel	1
IP Address	192.168.8.125
Protocol	ONVIF
Port	80
Username	admin
Password	*****
Remote Channel	CH-1

Step 10 Click  to access the web immediately.

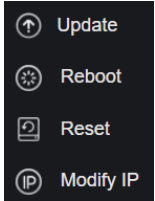
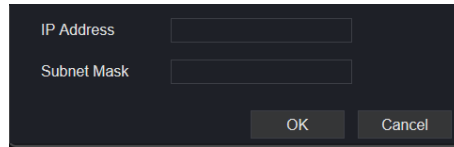
Step 11 Click  to update, reboot, or reset the selected camera, as  shows. The pop-up message “Are you sure to restart the device?” “Are you sure to reset? Reserve IP Address” would respectively show.

Figure 6-5 Modify IP



 NOTE



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

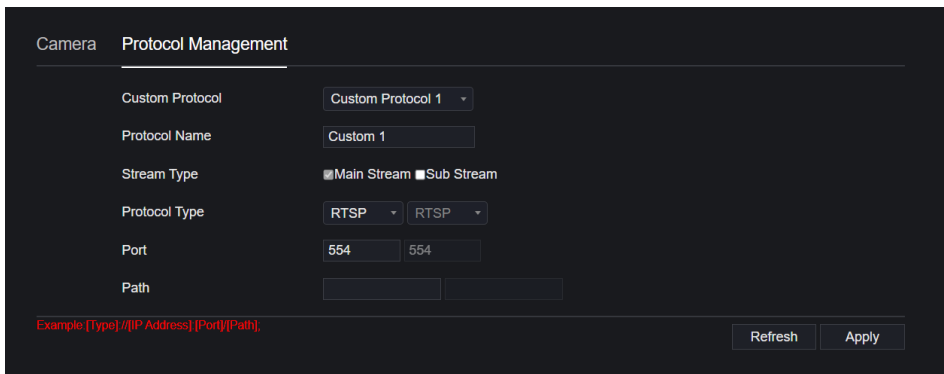


It indicates the camera is offline. It may not be connected to the network, or the password may be incorrect. Access to the modified device parameters interface to change.

6.1.1.1 Protocol Management

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

Figure 6-6 Protocol management



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

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

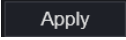
Step 3 Input the protocol name.

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 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  to save the settings.

6.1.2 Encode

Step 1 On the **System Setting** screen, choose **Channel > Encode** to access the encode interface, as shown in Figure 6-7.

Figure 6-7 Encode interface

The screenshot shows the 'Encode' configuration interface. It features a dark background with white text and light gray borders. The interface is organized into a table-like structure with two columns: a label column and a value column. The values are displayed in light gray boxes with a small downward arrow on the right, indicating they are dropdown menus. At the bottom right, there are two buttons: 'Copy' and 'Apply'.

Encode	
Channel	[1]Channel01
Stream Information	Main Stream
Video Format	H264
Resolution	1920x1080
Frame Rate(fps)	30
Bitrate Type	CBR
Bitrate(kbps)(1000-2000)	1680
CopyApply	

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

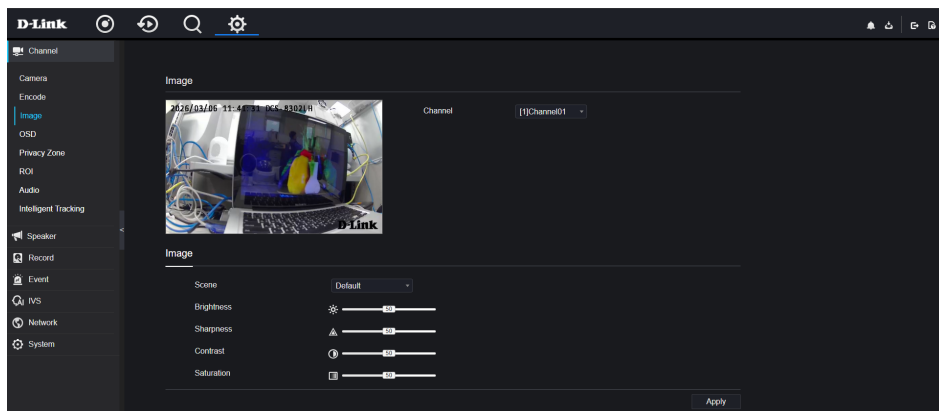
Step 3 Select stream information, resolution, frame rate, bitrate type, and bitrate from the drop-down list.

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

6.1.3 Image

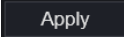
Step 1 On the **System Setting** screen, choose **Channel > Image** to access the Image interface, as shown in Figure 6-8.

Figure 6-8 Image interface



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

Step 3 Set image parameters.

Step 4 Click  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.

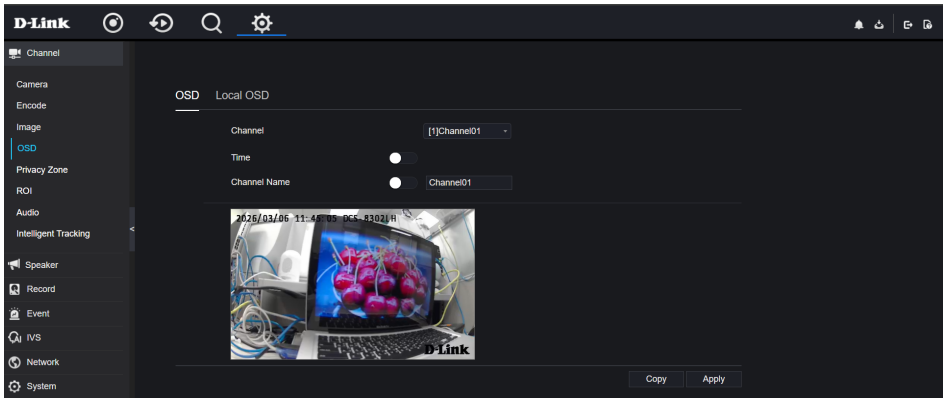
Contrast: It indicates the measurement of different brightness levels between the brightest white and darkest black in an image. The larger the difference range is, the greater the contrast is; the smaller the difference range is, the smaller the contrast is.

Scene: it includes indoor, outdoor, and default.

6.1.4 OSD

Step 1 On the **System Setting** screen, choose **Channel > OSD** to access the OSD interface, as shown in Figure 2-99

Figure 6-9 OSD interface

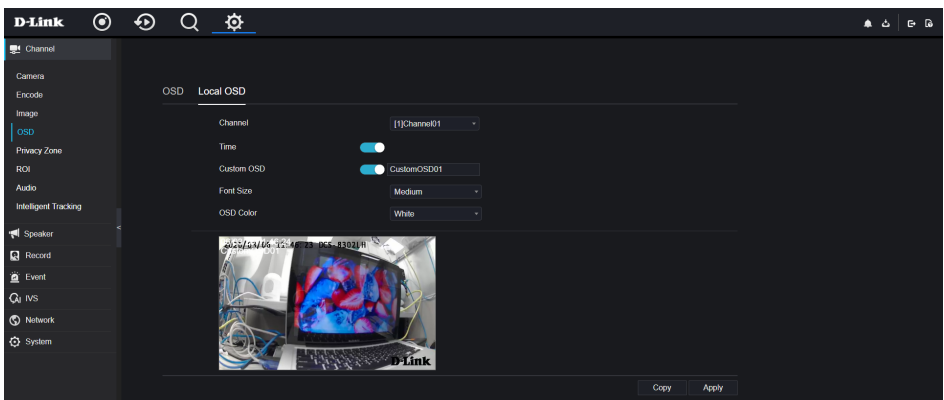


Step 2 Select a channel from the drop-down list.

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 6-10 Local OSD

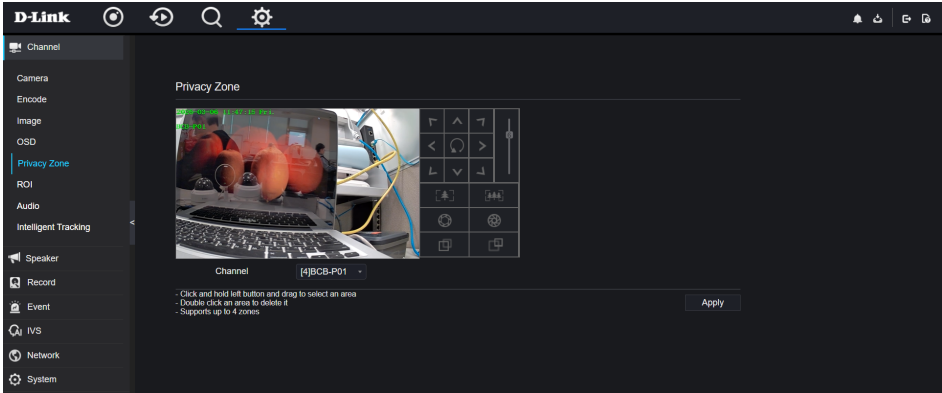


Users can enable the time and custom OSD on local videos; this OSD can't be shown on the backup recording.

6.1.5 Privacy Zone

Step 1 On the **System Setting** screen, choose **Channel > Privacy Zone** to access the privacy zone interface, as shown in Figure 6-11.

Figure 6-11 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.

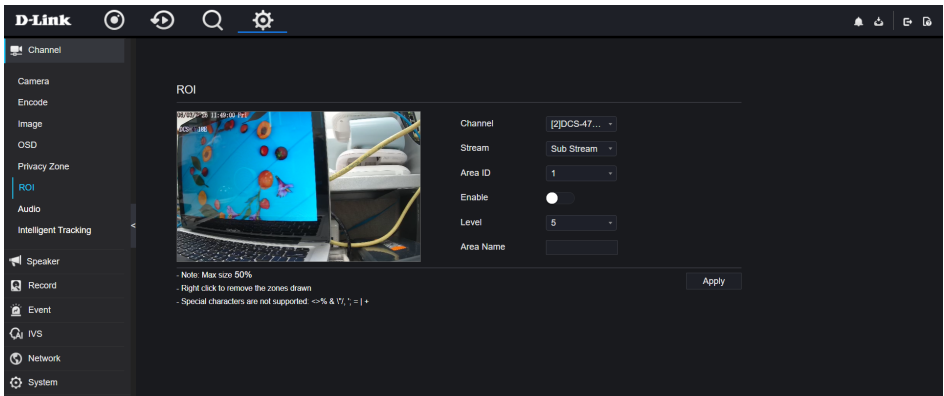
Step 4 PTZ can be used for adjusting the IP dome cameras.

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

6.1.6 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 6-12 ROI



6.1.7 Audio

Users can set the audio parameters of the channel. Audio in, audio out, and audio files.

Figure 6-13 Audio in

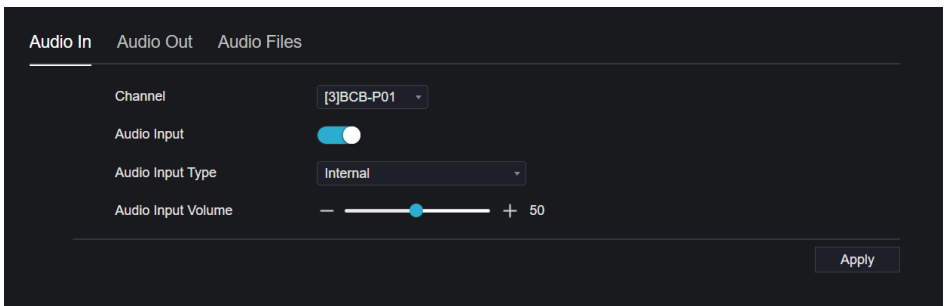


Figure 6-14 Audio out

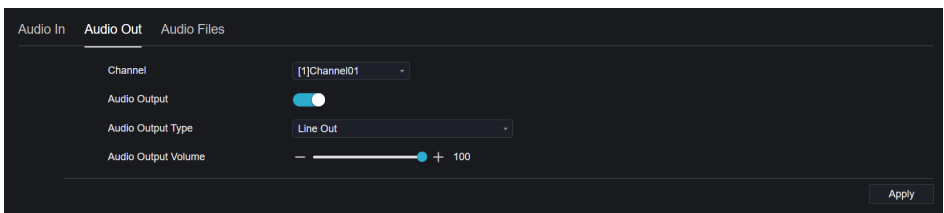
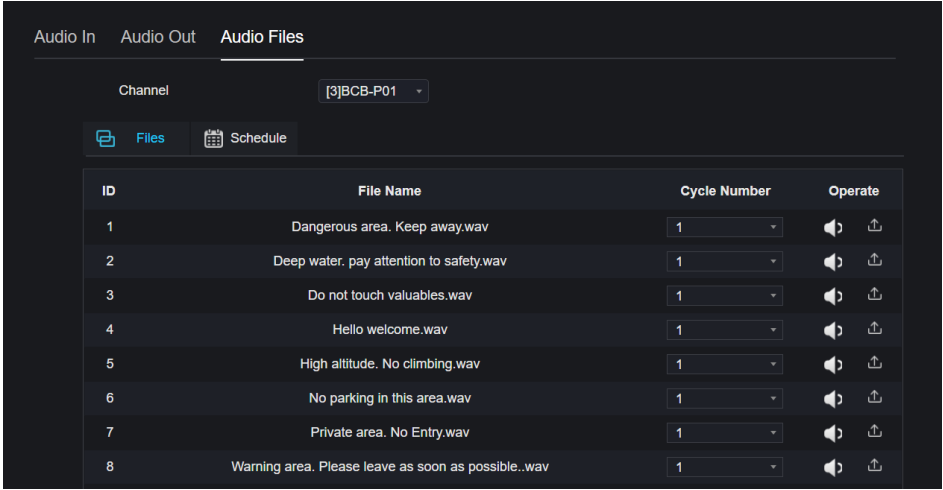


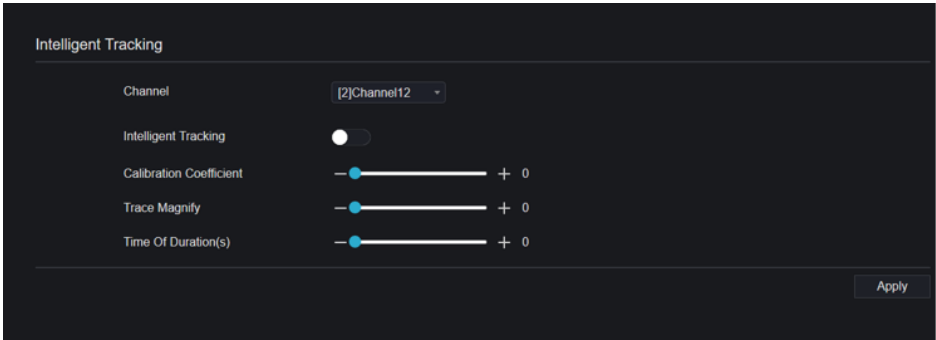
Figure 6-15 Audio files



6.1.8 Intelligent Tracking

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

Figure 6-16 Intelligent tracking

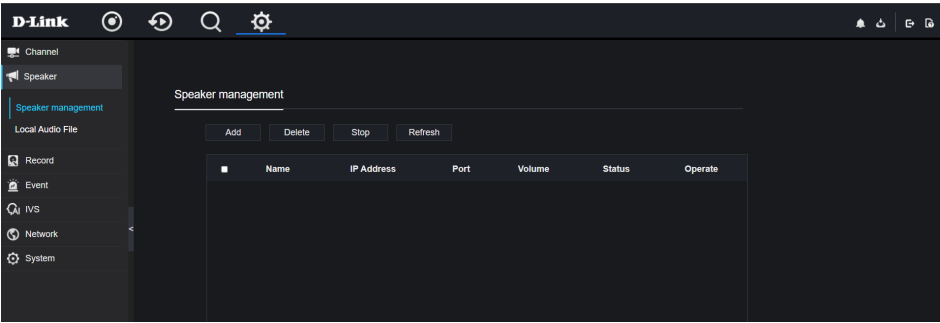


6.2 Speaker

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

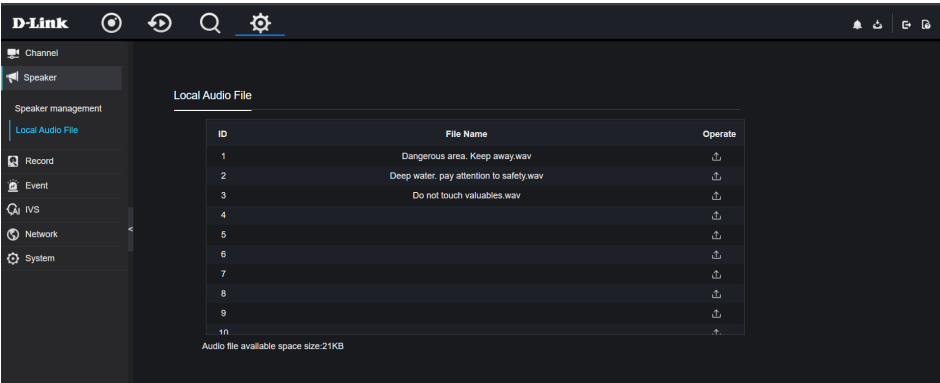
6.2.1 Speaker Management

Figure 6-17 Speaker management



6.2.2 Local Audio Files

Figure 6-18 Local audio file



6.3 Record

Users can set record policies in the Storage interface.

6.3.1 Record Schedule

Procedure

Step 1 On the **System Setting** screen, choose **Record > Record Schedule** to access the record schedule interface, as shown in Figure 6-19.

Figure 6-19 Record schedule interface



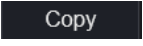
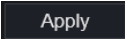
Step 2 Select a channel.

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  to return the previous settings.

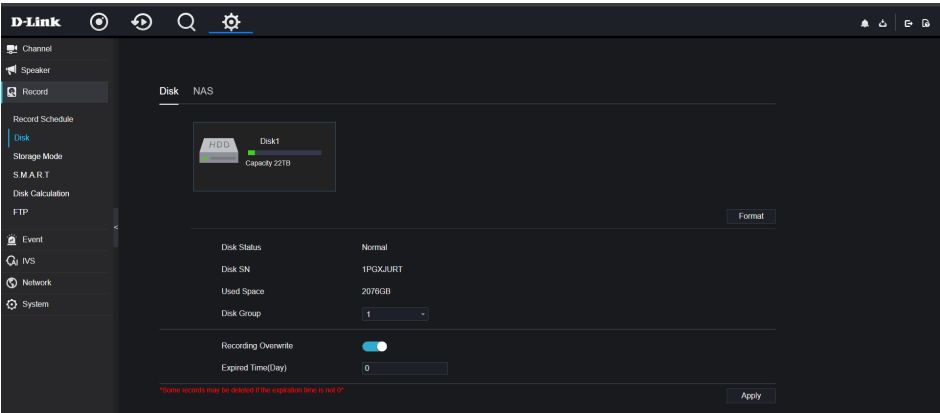
Step 7 Click  to choose other cameras to copy settings. Click  to save the settings.

6.3.2 Disk

6.3.2.1 Disk

Step 1 On the **System Setting** screen, choose **Record > Disk** to access the disk interface, as shown in Figure 6-20.

Figure 6-20 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.

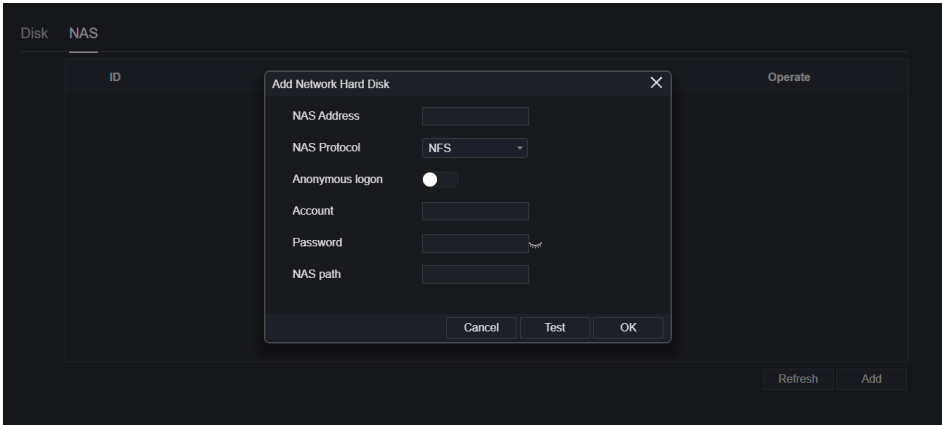
6.3.2.2 NAS

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 6-21 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.

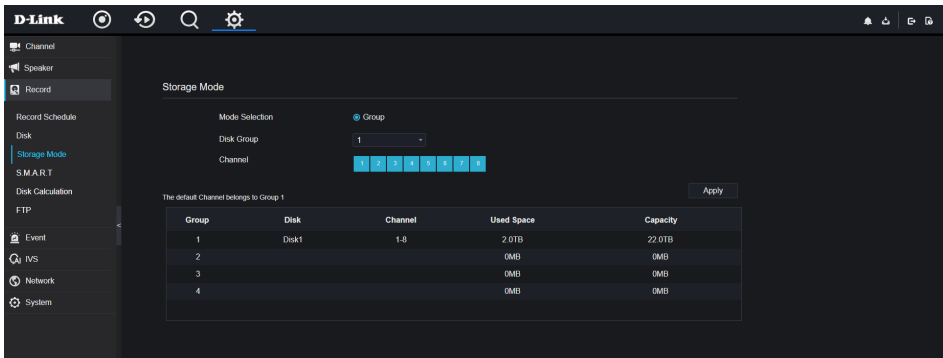
Step 4 Input the NAS path, the path can be viewed at the NAS interface.

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

6.3.3 Storage Mode

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

Figure 6-22 Storage Mode



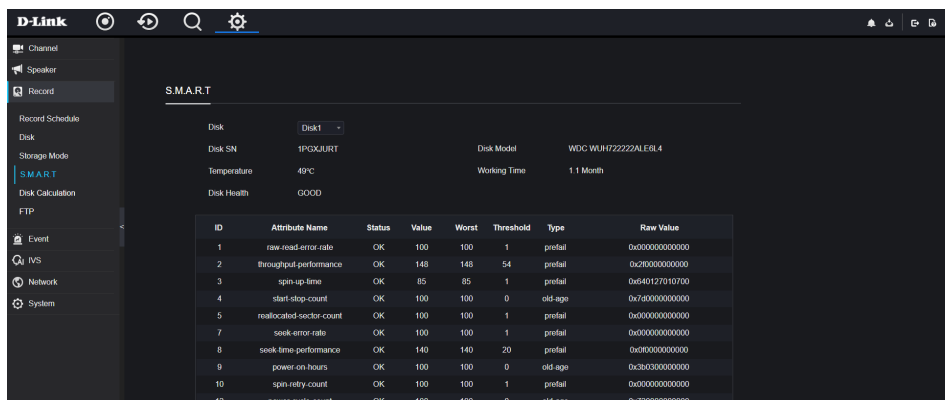
Operation Steps

- 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.

6.3.4 S.M.A.R.T

S.M.A.R.T is a Self-Monitoring Analysis and Reporting Technology; users can view the health of the disk, as shown in Figure 6-233.

Figure 6-23 S.M.A.R.T



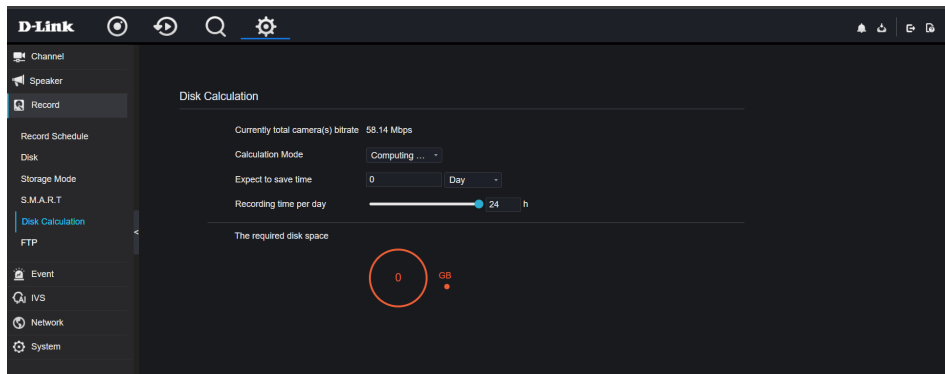
6.3.5 Disk Calculation

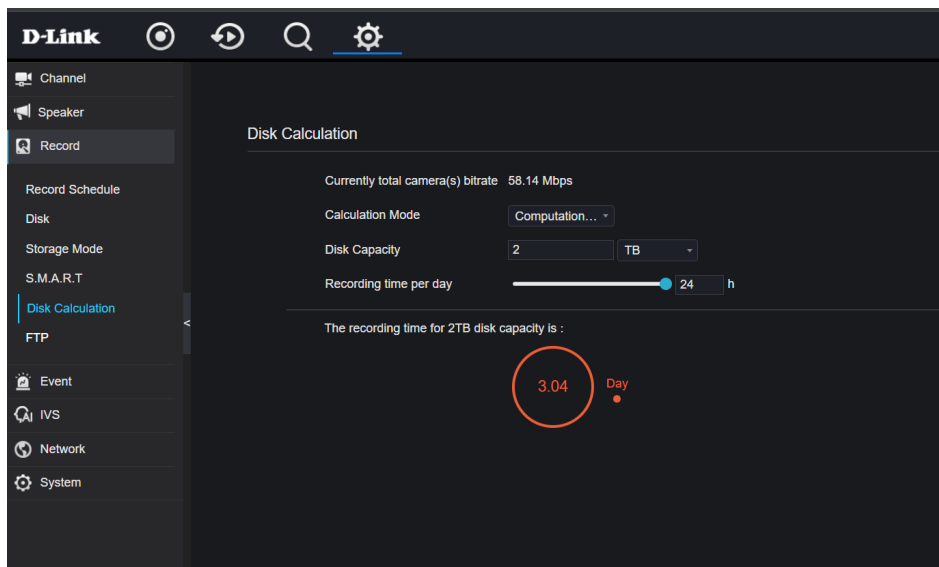
There are two modes to calculate the captivity of the disk, as

Computing Capacity
Computation time

shown here.

Figure 6-24 Disk calculation

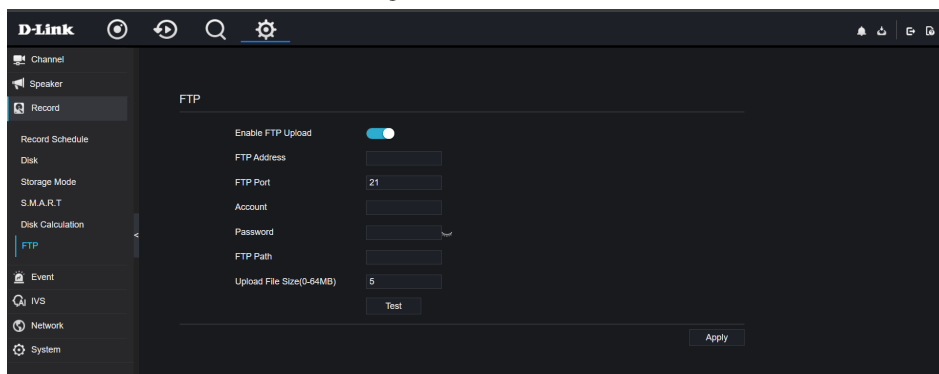




6.3.6 FTP

Set the FTP path to receive the alarm information, as shown in Figure 6-255. For more detailed information, please refer to UI interface parameters.

Figure 6-25 FTP



6.4 Event

Users can set general, motion detection, video loss, alarm in, abnormal alarm, and alarm out on the alarm interface.

6.4.1 General

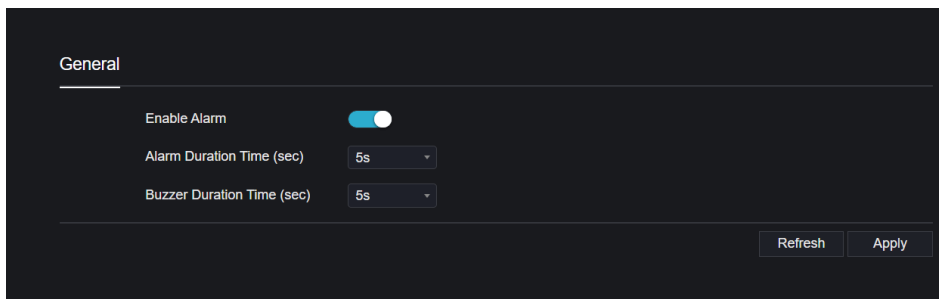
6.4.1.1 General

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 6-266.

Figure 6-26 General interface



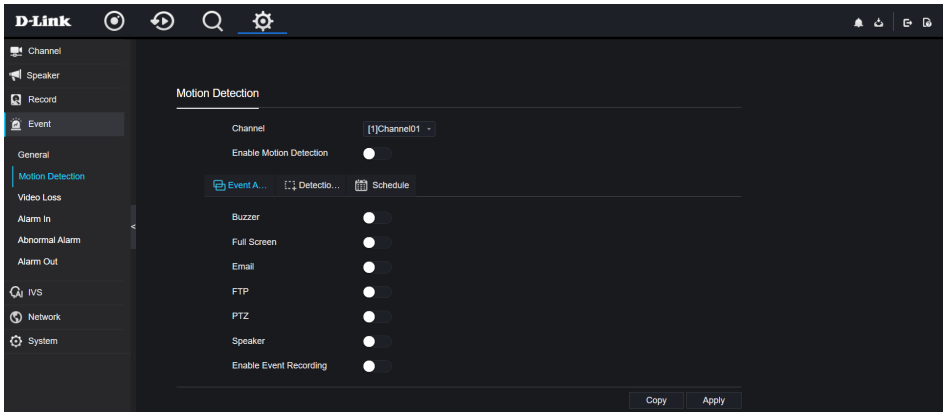
Step 3 Click **Apply** to save settings. Click **Refresh** to return to the previous settings.

6.4.2 Motion Detection

Procedure

Step 1 On the **System Setting** screen, choose **Event > Motion Detection** to access the motion detection interface, as shown in Figure 6-2727.

Figure 6-27 Motion detection interface



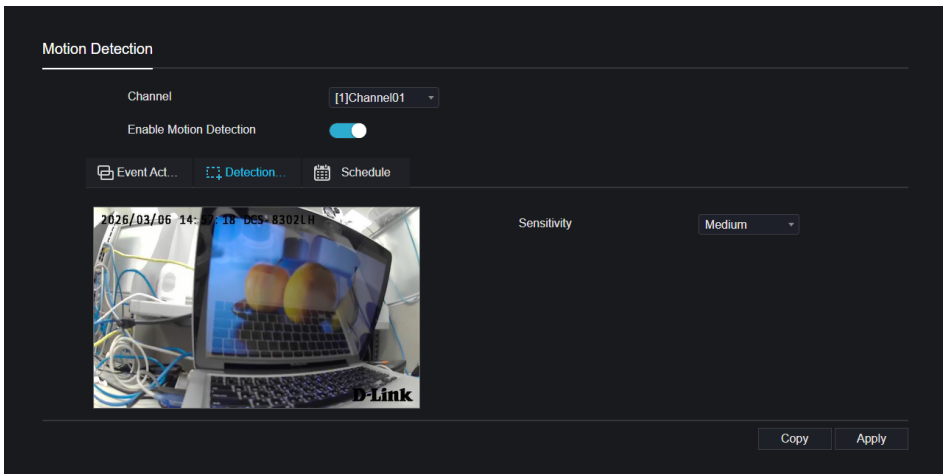
Step 2 Click the channel drop-down list to choose a channel.

Step 3 Enable motion detection alarm.

Step 4 Set **Event Activity**, which includes buzzer, full screen, email, FTP, PTZ, Speaker and Event Record.

Step 5 Click **Area** to access the motion detection area setting, as shown in Figure 6-28.

Figure 6-28 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.

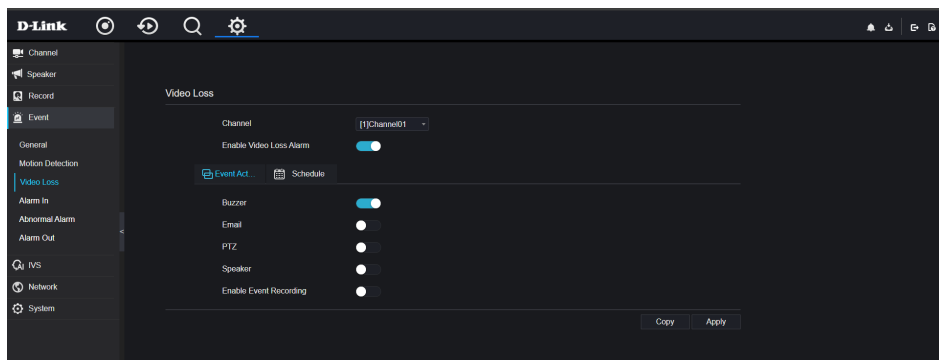
Step 7 Click **Copy** to choose other cameras to copy settings. Click **Apply** to save the settings.

6.4.3 Video Loss

Procedure

Step 1 On the **System Setting** screen, choose **Event > Video Loss** to access the video loss interface, as shown in Figure 6-2929.

Figure 6-29 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 2-6 motion detection settings*.

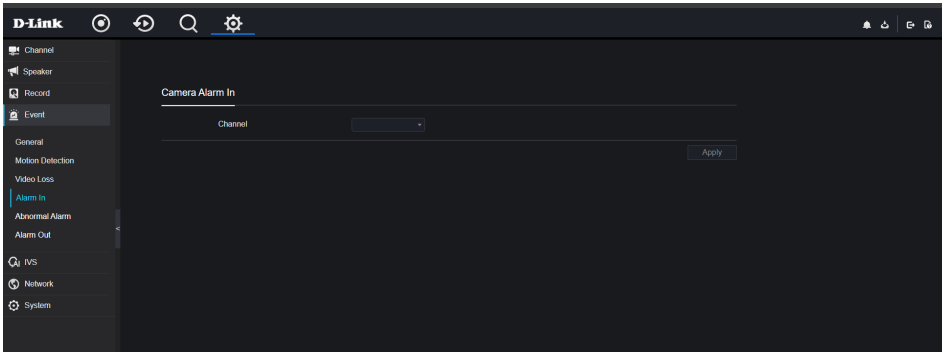
Step 5 Click **Copy** to choose other cameras to copy settings. Click **Apply** to save the settings.

6.4.4 Alarm In

Procedure

Step 1 On the **System Setting** screen, choose **Event > Alarm In** to access the alarm in the interface, as shown in Figure 6-300.

Figure 6-30 Alarm in interface

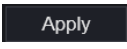


Step 2 Click the drop-down list to choose alarm in.

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  to save settings.

6.4.5 Abnormal Alarm

Procedure

Step 1 On the **System Setting** screen, choose **Event > Abnormal Alarm** to access the abnormal alarm interface, as shown in Figure 3-1531.

Figure 6-31 Abnormal alarm interface



Step 2 Enable the button and tick alarm type.

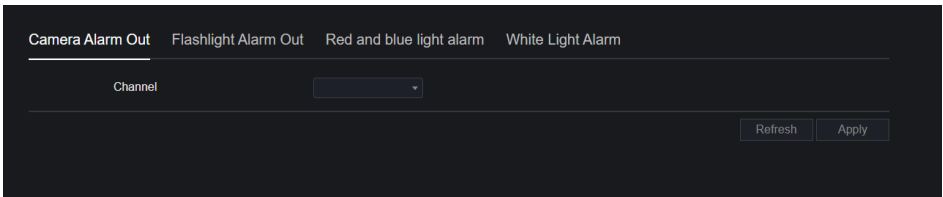
Step 3 For setting event activity and schedule, please refer to *motion detection settings*.

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

6.4.6 Alarm out

Set the alarm out and the camera alarm out.

Figure 6-32 Camera Alarm out



6.5 IVS

The NVR will send a detection alarm while something is detected in the specific view of the camera.

Operation Description

- Step 1** Navigate to **Settings > IVS > Intelligent Analysis** as shown in Figure 4-3933. Select one action to set the alarm. (**Intrusion, Smart Motion, Single Line Crossing, Double Line Crossing, Loiter, Multi-loitering, Wrong Way, Illegal Parking, People Counting**).
- Step 2** Select a channel from the drop-down list of channels.
- Step 3** Click  to enable specific IVS detection feature.
- Step 4** Click the Detection Area page to set the detection area. Use the mouse to draw the polygonal region to deploy as shown in Figure 4-3934.
- Step 5** Click the Schedule page to access the schedule screen, as shown in Figure 4-3935.
- Step 6** Enable the Event Actions including **Buzzer, Full Screen, Send Email, FTP, PTZ, Speaker** and **Event Recordings** and so on. Configure the settings as per Table 4-51.

Figure 6-33 Intelligent analysis interface

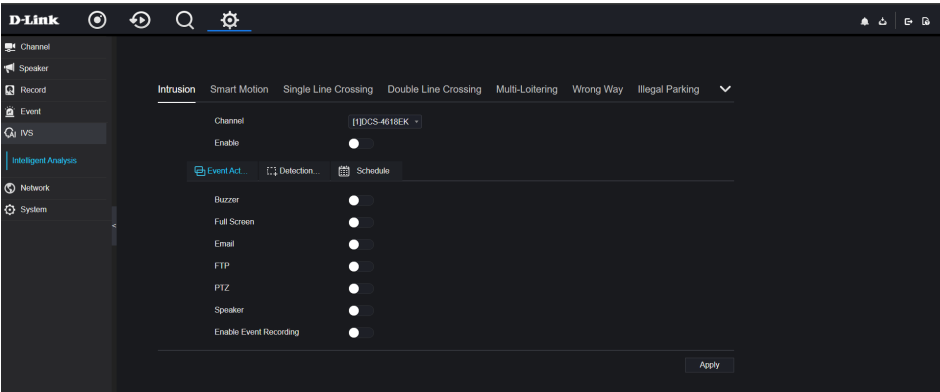


Table 6-1 Event Action Setting

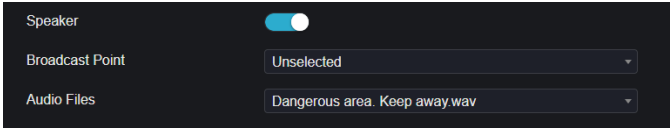
Parameter	Description
Buzzer	When motion is triggered, a buzzer will sound.
Full Screen	When motion is triggered the live view from the NVR will display the camera in full screen.
Email	When a motion is triggered, a notification will be sent to a designated email address. Note: Email settings must be configured under Network settings before enabling this option.
FTP	When motion is triggered, a snapshot will be saved via FTP. Note: FTP settings must be configured under Recording settings (see section 4.3.7 <i>FTP</i>) 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.
Speaker	When a detection is triggered, it will enable the speaker to play the set audio file by the chosen broadcast point. 
Enable Event Recording	When a detection 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.

Figure 6-34 Detection Area Setting

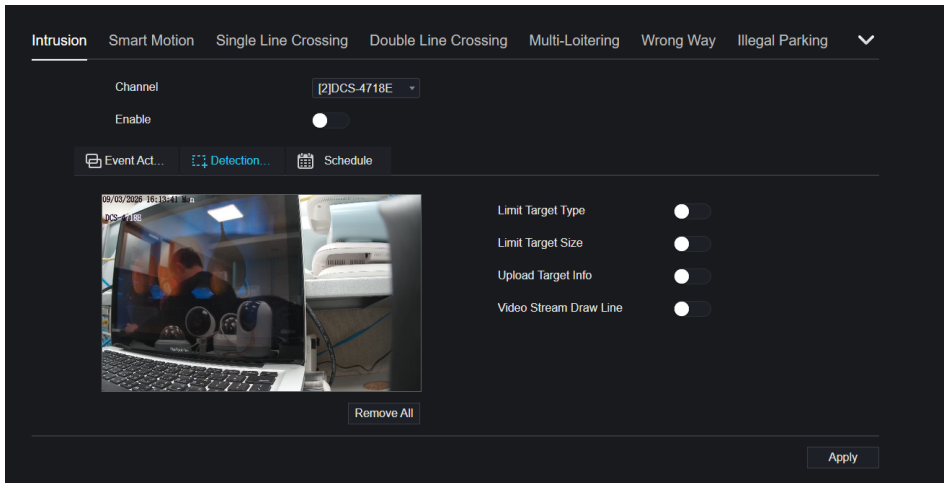
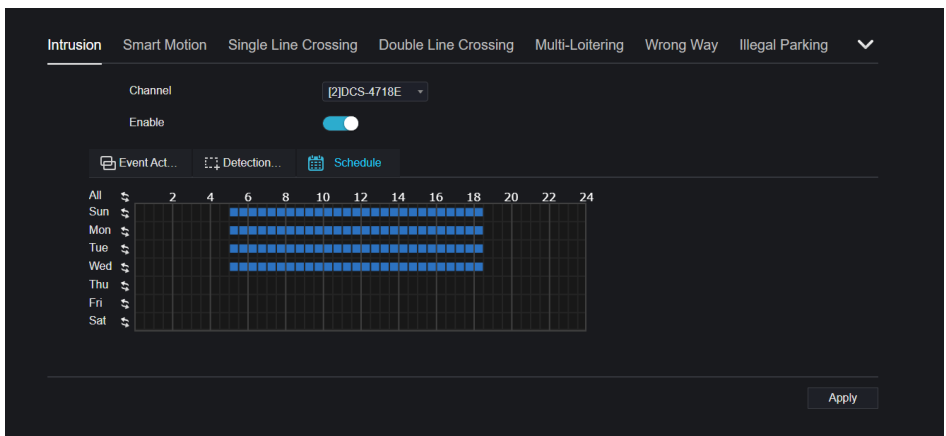


Figure 6-35 Schedule Setting



6.6 Network

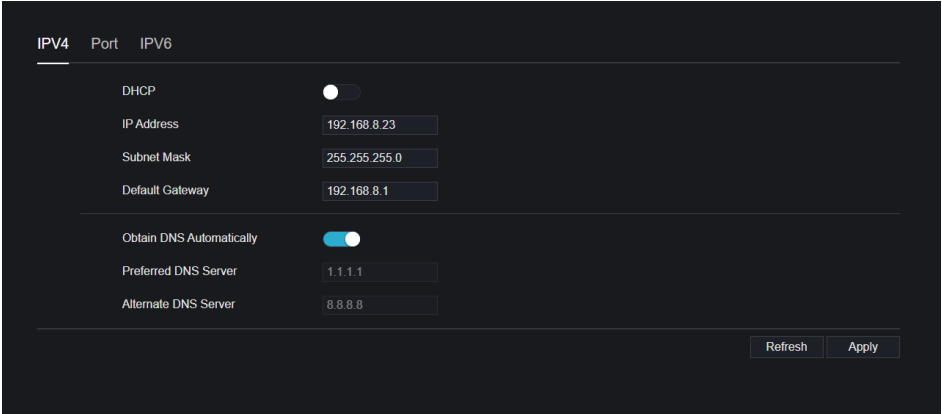
6.6.1 Network

Users can set Network, DDNS, E-mail, Port Mapping, IP Filter, 802.1X, SNMP, Web Mode, CMS and PPPoE.

Procedure

Step 1 On the **System Setting** screen, choose **Network > Network** to access the network interface, as shown in Figure 6-3647.

Figure 6-36 Network interface



Step 2 Click  next to **DHCP** 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 Address**, **Subnet Mask**, and **Default Gateway** to set the parameters as required.

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

If the function is disabled, click the input boxes next to **Preferred DNS Server** and **Alternate DNS Server**, delete the original addresses, and enter new addresses.

Step 4 Set **PORT** and **POE** manually, and input the information about these.

Figure 6-37 POE

The screenshot shows a network configuration interface with tabs for IPv4, Port, and IPv6. The IPv6 tab is active. It contains a DHCP section with a toggle switch (currently off), an IP Address field (fe80::21c:27ff:fe27:765f), a Subnet prefix length(0-128) field (64), and a Default Gateway field. Below this is an 'Obtain DNS Automatically' section with a toggle switch (currently off), and two empty input fields for Preferred DNS Server and Alternate DNS Server. At the bottom right are 'Refresh' and 'Apply' buttons.

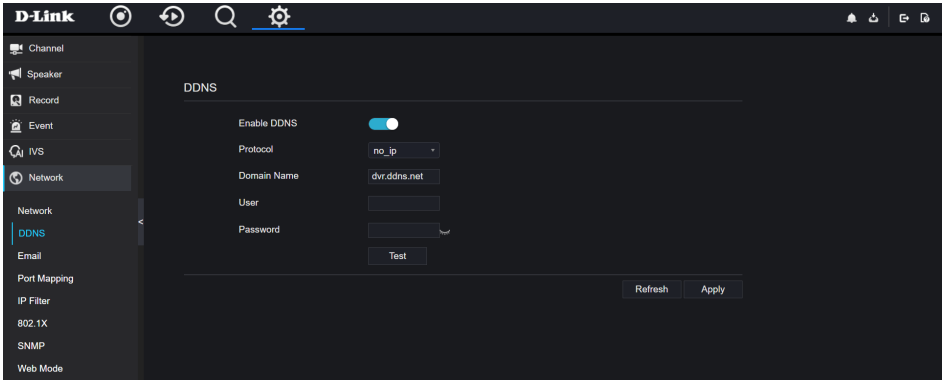
Step 5 Click **Refresh** to restore previous settings. Click **Apply** to save the settings.

6.6.2 DDNS

Procedure

Step 1 Click **DDNS** in the network interface, and choose **Network > DDNS** to access the DDNS interface as shown in Figure 6-3849.

Figure 6-38 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.

6.6.3 Email

Procedure

Step 1 Click **Email** in the network interface, and choose **Network > Email** to access the Email interface, as shown in Figure 6-390

Figure 6-39 Email interface

The screenshot shows the D-Link web interface for configuring email settings. The left sidebar has a menu with options: Channel, Speaker, Record, Event, IVS, Network, DNS, Email, Port Mapping, IP Filter, 802.1X, SNMP, and Web Mode. The 'Email' option is selected. The main content area is titled 'Email Server 1' and 'Email Server 2'. It contains the following fields and values:

Field	Value
SMTP Server	smtp.gmail.com
SMTP Server Port	465
Username	chien@gmail.com
Password	*****
Email Sender	chien@gmail.com
Alarm Receiver 1	chris@dlinkcorp.com
Alarm Receiver 2	
Alarm Receiver 3	
SSL Encryption	SSL
Sending interval(0-600s)	0

At the bottom right, there is a 'Test' button.

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.

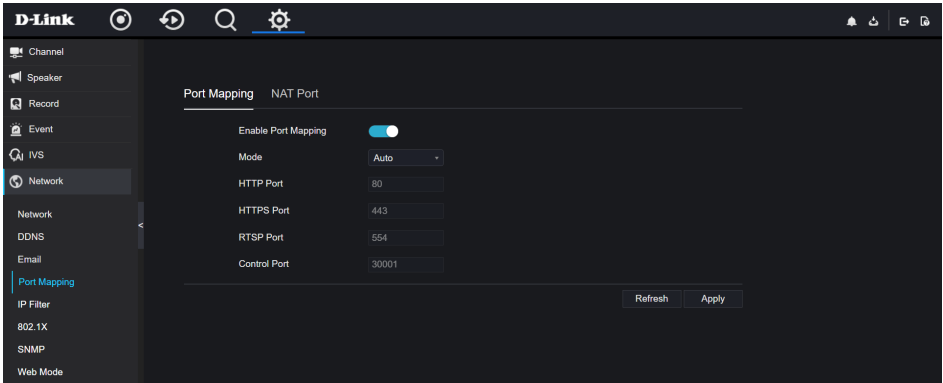
6.6.4 Port Mapping

6.6.4.1 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 6-401.

Figure 6-40 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

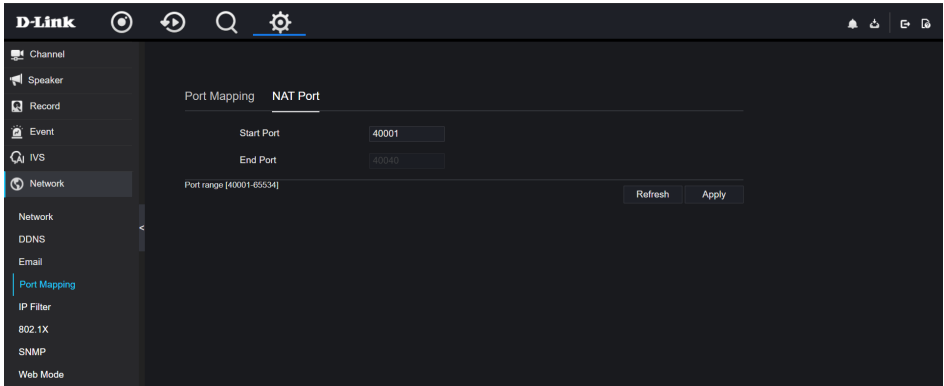
Auto: The system performs UPnP automatically.

Manual: The ports are distributed by the router. Input them according to the router.

6.6.4.2 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 6-41 NAT port



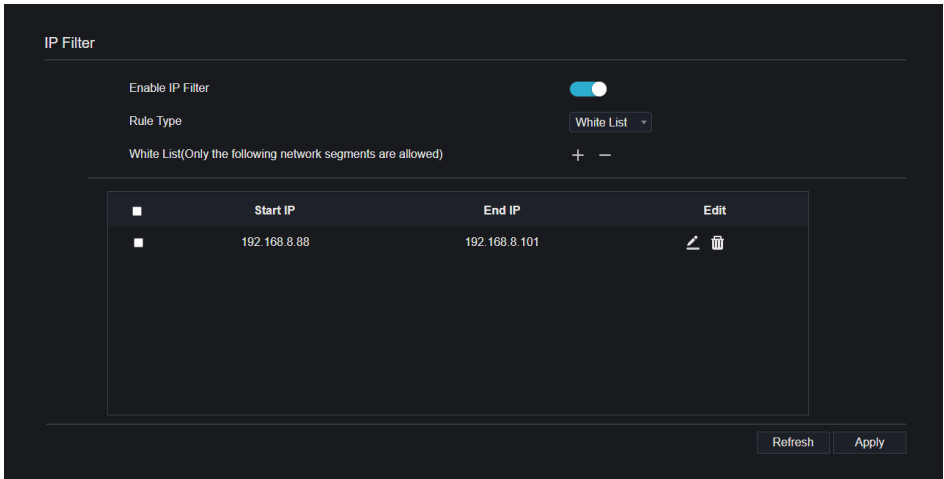
Users can input the https://IP address:port for example <https://192.168.0.229:40006/> to access the camera's web interface.

6.6.5 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 6-4253.

Figure 6-42 IP filter interface

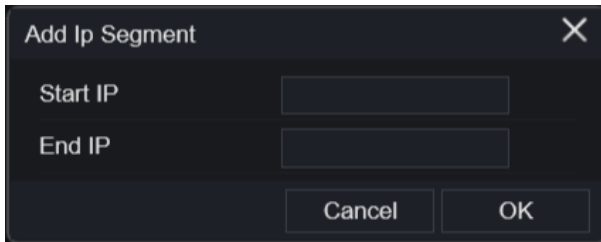


Step 2 Click **Enable** to enable the IP filter function.

Step 3 Click the drop-down list of rule types to choose blacklist or whitelist.

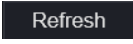
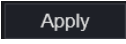
Step 4 Click  to view the pop-up windows to set a blacklist or whitelist 4.7.5. Click  to delete the list.

Figure 6-43 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  to restore previous settings. Click  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.

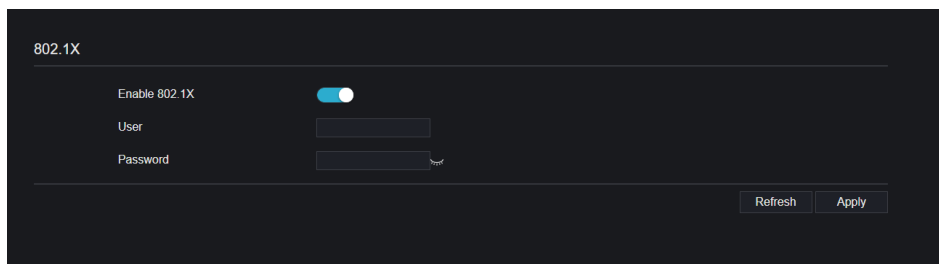
Only one rule type is available, and the last rule type set is efficient.

6.6.6 802.1X

Procedure

Step 1 Click **802.1X** in the network interface. The 802.1X interface is displayed. Enable the button, as shown in Figure 6-4455.

Figure 6-44 802.1X 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.

6.6.7 SNMP

Procedure

Step 1 Click **SNMP** in the network interface. The SNMP interface is displayed. Enable the button next to SNMPV, SNMPV2C or SNMPV3, as shown in Figure 6-4556.

Figure 6-45 SNMP interface

SNMP

SNMPV1

SNMPV2C

Write Community

Read Community

Trap Address

Trap Port

162

Trap Community

SNMPV3

Refresh

Apply

SNMPV3

Read Security Name

Security Level

priv

Auth Algorithm

SHA

Auth Password

Encry Algorithm

DES

Encry Password

Write Security Name

Security Level

priv

Auth Algorithm

SHA

Auth Password

Encry Algorithm

DES

Encry Password

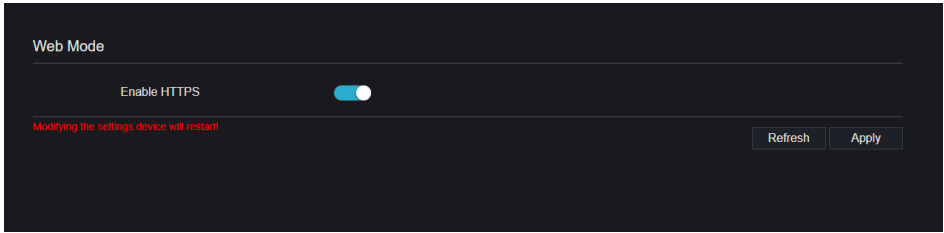
Refresh

Apply

6.6.8 Web Mode

Step 1 Click **Web Mode** in the network interface. The Web Mode interface is displayed, as shown in Figure 2-657.

Figure 6-46 Web mode interface



Step 2 Enable or disable HTTPS.

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

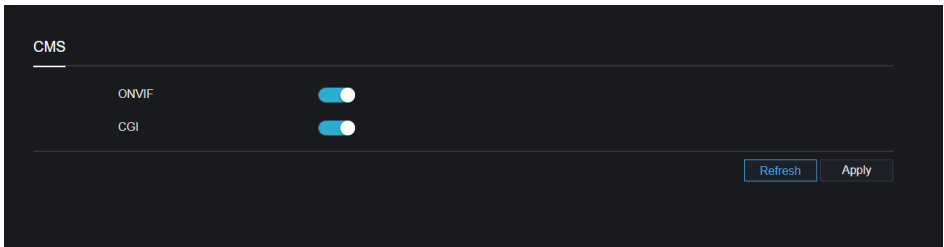
6.6.9 CMS

If the user wants to access the NVR ONVIF, or CGI, you can enable these.

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.

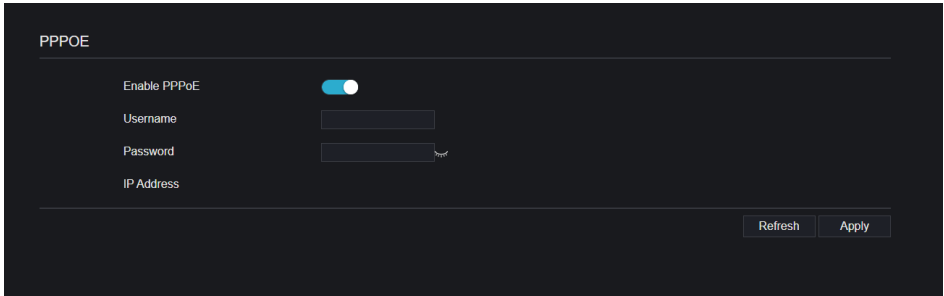
Figure 6-47 CMS



6.6.10 PPPOE

Users can use the PPPOE function to manage the NVR conveniently.

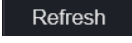
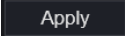
Figure 6-48 PPPOE



Step 1 Enable the PPPOE.

Step 2 Input the username and password.

Step 3 The IP address is obtained automatically.

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

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

6.7 System

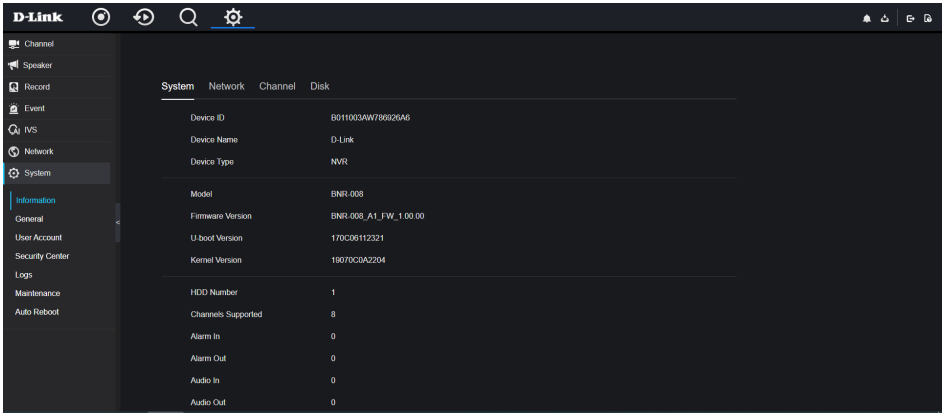
Users can set parameters about information, general, user, password, logs, maintenance, and auto restart.

6.7.1 Device Information

Procedure

Step 1 Click  on the navigation bar, and the device information interface is displayed, as shown in Figure 6-4960.

Figure 6-49 Device information interface



Step 2 Set the device name according to Table 6-11.

Table 6-1 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 6-50 Network

D-Link	Channel	System	Network	Channel	Disk
Channel	Speaker	Record	Event	I/V	Network
System	Information	General	User Account	Security Center	Logs
Maintenance	Auto Reboot				

Status	Online
IP Address	192.168.8.23
Subnet Mask	255.255.255.0
Default Gateway	192.168.8.1
MAC Address	00:1C:27:27:76:5F
DHCP	OFF
Preferred DNS Server	1.1.1.1
Alternate DNS Server	8.8.8.8
Total Bandwidth	100.00 Mbps

Figure 6-51 Channel

D-Link	Channel	System	Network	Channel	Disk
Channel	Speaker	Record	Event	I/V	Network
System	Information	General	User Account	Security Center	Logs
Maintenance	Auto Reboot				

Channel	Name	Status	Video Format	Resolution	Bitrate(kbps)
CH1	Channel01	Online	H264/H264	1920*1080/640*360	1680/512
CH2	DCS-4718E	Online	H264/H264	3840*2160/640*360	7168/1024
CH3	BCS-P01	Online	H264/H264	1920*1080/704*480	7168/1024
CH4	BCS-P01	Online	H264/H264	1920*1080/704*576	7168/1024
CH5	BCD-P01	Online	H264/H264	1920*1080/704*480	7168/1024
CH6	BCD-P01	Online	H264/H264	1920*1080/704*576	7168/1024
CH7	BCD-P01	Online	H264/H264	1920*1080/704*480	7168/1024
CH8	BCS-P01	Online	H264/H264	1920*1080/704*480	7168/1024

Figure 6-52 Disk

D-Link	Channel	System	Network	Channel	Disk
Channel	Speaker	Record	Event	I/V	Network
System	Information	General	User Account	Security Center	Logs
Maintenance	Auto Reboot				

Disk	Capacity	Used	SN	Disk Model	Status
Disk1	22TB	2120GB	1PGXJURT	WDC WUJ172222ALESL4	Normal

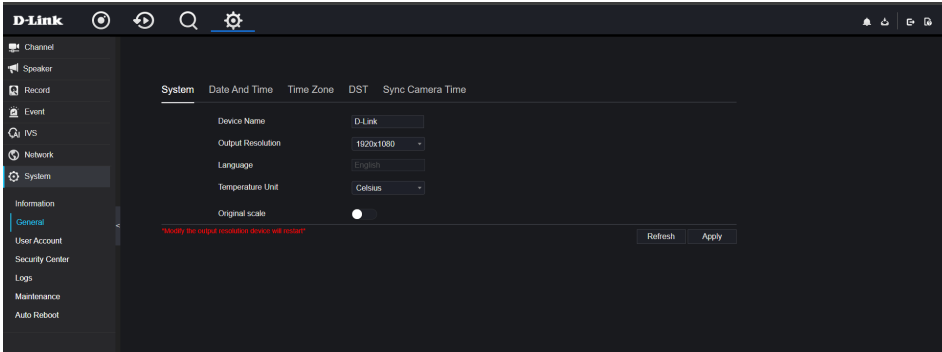
6.7.2 General

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 6-5364.

Figure 6-53 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.

System	Date And Time	Time Zone	DST	Sync Camera Time
	Date Format	DD/MM/YY hh:mm:ss		
	Time Format	24H		
	Enable NTP	☒		
	NTP Server	ntp.dlink.com.tw		
	Sync Time Frequency (sec)	86400s		
	Time	06/03/2026 16:08:00		
- Time modification will cause the channel to reconnect - Time modification will affect video query Refresh Apply				

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 6-5465.
6. Click the NTP Sync button to disable time synchronization.
7. Async date and time interface.

Figure 6-54 Date and time

System	Date And Time	Time Zone	DST	Sync Camera Time
	Date Format	DD/MM/YY hh:mm:ss		
	Time Format	24H		
	Enable NTP	☐		
	Time	06/03/2026 16:10:16		
- Time modification will cause the channel to reconnect - Time modification will affect video query Refresh Apply				

Step 4 Set the time zone.

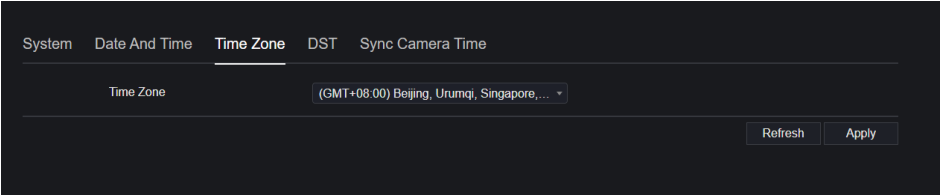
1. Select the date format and time format from the drop-down list.
2. Click **Apply** to save the device time setting. Click **Refresh** to return to the previous setting.

Step 5 Set time zone.

Click **Time Zone** to enter the time zone setting interface, as shown in Figure 6-5566.

Time zone setting interface

Figure 6-55 Time zone



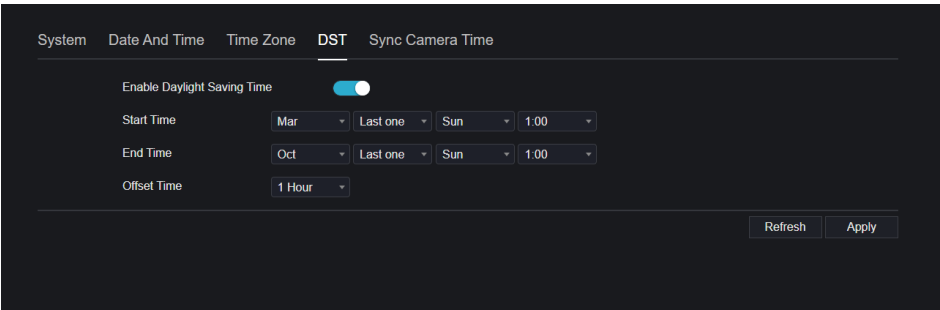
Select a time zone from the drop-down list.

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 6-5667. The button is disabled by default.

Figure 6-56 DST setting interface

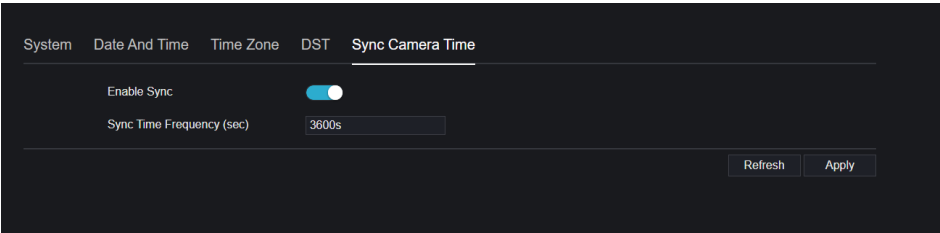


Select a start time from the drop-down list.

Select an end time from the drop-down list.

Select an offset time from the drop-down list.

Figure 6-57 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.

6.7.3 User Account

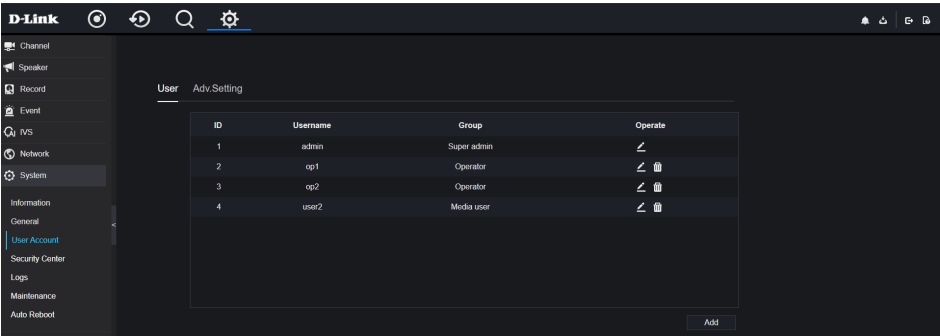
You can create new user accounts to manage the device.

6.7.3.1 Add User

Procedure

Step 1 On the **System Setting** screen, choose **System > User** to access the **User** interface, as shown in Figure 6-5869.

Figure 6-58 User interface



Step 2 Click **Add** to add a new user, as shown in Figure 6-5970.

Figure 6-59 Add user

Add User

Username ?

Password

Confirm Password ?

Group

Change Password Frequency

Password Expire Date ☐

☒ Live Preview

☒ PTZ

☒ Playback

☒ Channel Management

☒ Device Management

☒ System Management

☒ All Channel

☒ CH-1

☒ CH-2

☒ CH-3

☒ CH-4

Live Preview

OK Cancel

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.

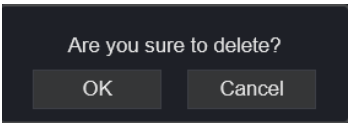
Step 6 Enable the expiration date to set the new user's authority time.

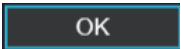
Step 7 Select channels to manage.

Step 8 Click , 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 , click

 to delete.

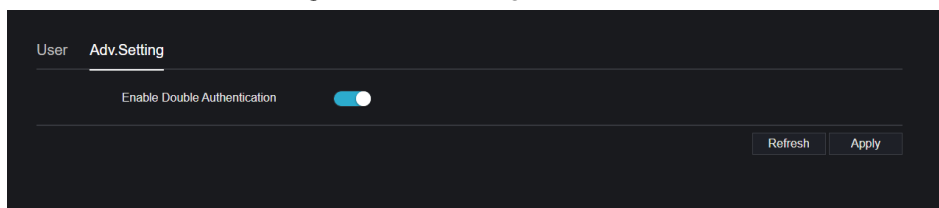
----End

6.7.3.2 Adv.Setting

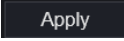
Procedure

Step 1 On the **System Setting** screen, choose **System > User > Adv. Setting** to access interface, as shown in 6-71.

Figure 6-60 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  to save the device time setting. Click  to return to the previous setting.

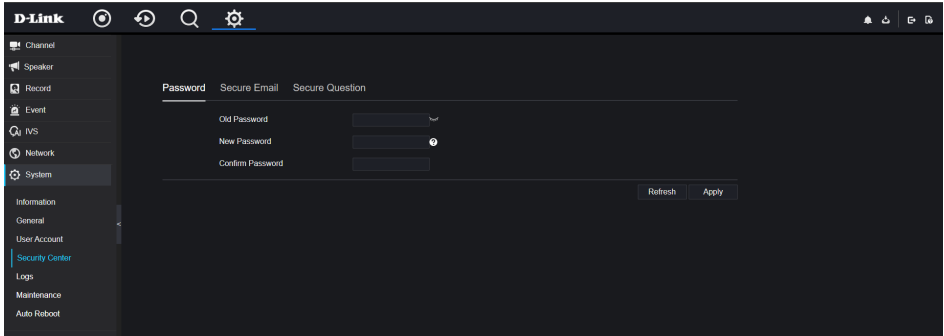
6.7.4 Security Center

6.7.4.1 Password

Procedure

Step 1 On the **System Setting** screen, choose **System > Security Center** to access the password interface, as shown in Figure 6-6172.

Figure 6-61 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 is at least 8 characters.

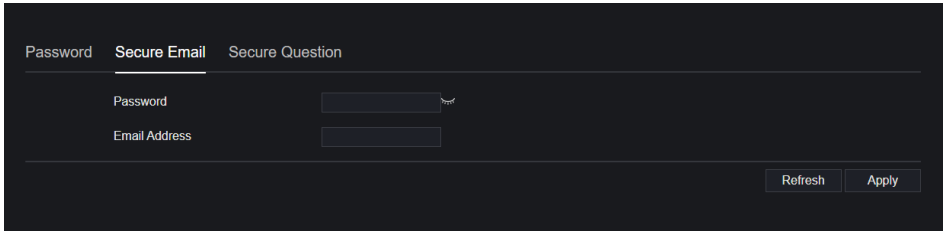
At least 3 kinds of numbers, lowercase, uppercase, or special characters contained.

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

6.7.4.2 Secure Email

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

Figure 6-62 Secure Email



6.7.4.3 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 6-63 Secure question

Password

Secure Email

Secure Question

Password

Question one

Question one answer

Question two

Question two answer

Question three

Question three answer

- Please enter at least 1 characters for the answer

- Please enter up to 32 characters for the answer

Refresh

Apply

6.7.5 Logs

6.7.5.1 System Logs

Procedure

Step 1 On the **System Setting** screen, choose **System > Logs** to access the logs interface, as shown in Figure 6-6475.

Figure 6-64 System log interface

D-Link

Channel

Speaker

Record

Event

NS

Network

System

Information

General

User Account

Security Center

Logs

Maintenance

Auto Reboot

System Log

Event Log

Start 05/03/2026 16:21:47

End 06/03/2026 16:21:47

Type Operation Log

Search

Export

ID	Start Time	Channel	Log Type	Information
1	06/03/2026 14:19:08	-----	Login	[admin] 192.168.8.148 login
2	06/03/2026 14:18:58	-----	Login	[admin] 192.168.8.148 login
3	06/03/2026 14:16:22	-----	Login	[admin] 192.168.8.148 login
4	06/03/2026 11:57:01	-----	Logout	[admin] 192.168.8.148 logout
5	06/03/2026 11:30:06	Channel01	Add Camera	[admin] 192.168.8.148 Unknown_SN_01
6	06/03/2026 11:28:07	Channel01	Delete Camera	[admin] 192.168.8.148 B0C25459/5C0
7	06/03/2026 11:08:16	Channel06	Stop Recording PlayBack	[admin] 192.168.8.148
8	06/03/2026 11:08:16	Channel05	Stop Recording PlayBack	[admin] 192.168.8.148
9	06/03/2026 11:08:16	Channel04	Stop Recording PlayBack	[admin] 192.168.8.148
10	06/03/2026 11:08:16	Channel03	Stop Recording PlayBack	[admin] 192.168.8.148
11	06/03/2026 11:06:54	Channel06	Start Playback	[admin] 192.168.8.148
12	06/03/2026 11:06:53	Channel05	Start Playback	[admin] 192.168.8.148

<< < > >>

Every page show 20

Step 2 Set start time and end time from the calendar.

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

Step 4 Click **Search** to acquire log information.

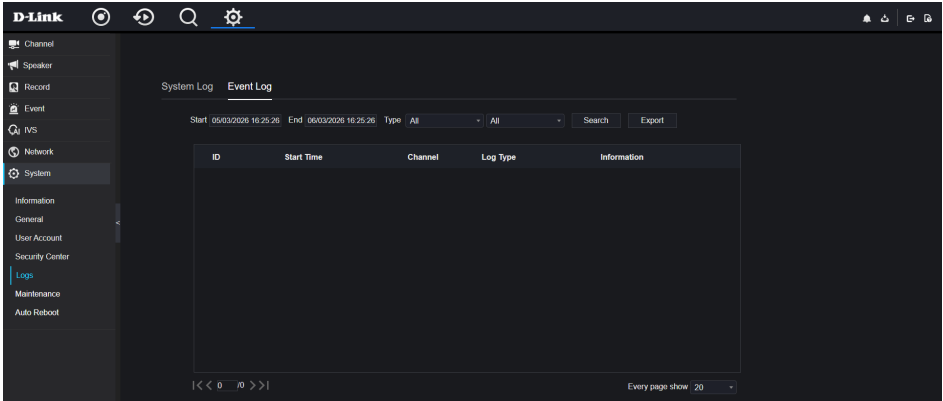
Step 5 Click **Export** to export the logs.

6.7.5.2 Event

Procedure

Step 1 On the **System Setting** screen, choose **System >Logs > Event** to access the logs interface, as shown in Figure 6-6576.

Figure 6-65 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.

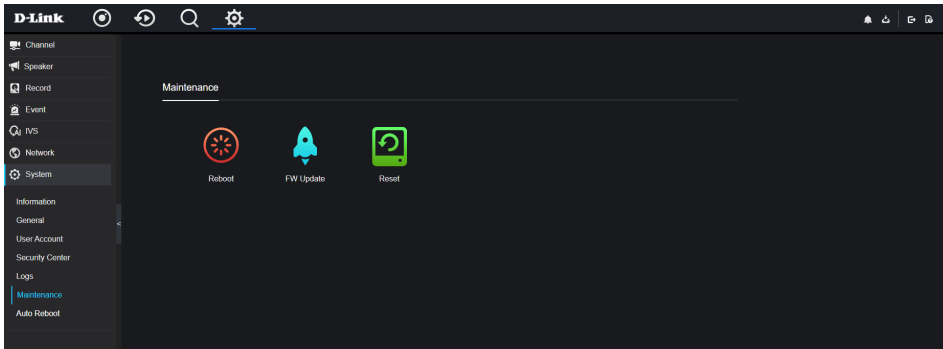
6.7.6 Maintenance

6.7.6.1 Maintenance

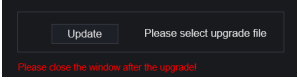
Procedure

Step 1 On the **System Setting** screen, choose **System >Maintenance** to access the maintenance interface, as shown in Figure 6-6677.

Figure 6-66 Maintenance interface



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

Step 3 Click **Update**. The message shows , choose software from a specific location to update.

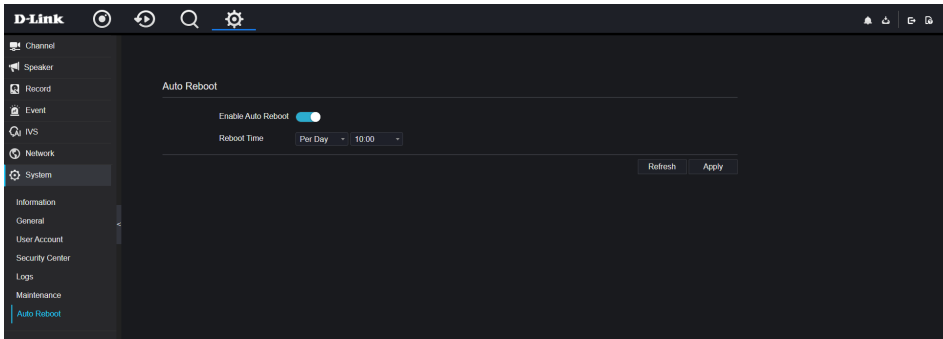
Step 4 Click **Reset**, and the pop-up message/will show you, click  to reset.

6.7.7 Auto Reboot

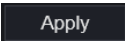
Procedure

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 6-6778.

Figure 6-67 Auto restart



Step 2 Select one type of restart time from the drop-down list.

Step 3 Click  to save settings. Click  to return to the previous setting.

Regulatory Information

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Non-modification Statement

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Caution

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

CE EMI Class A Warning

This equipment is compliant with Class A of CISPR 32. In a residential environment this equipment may cause radio interference.

SAFETY INSTRUCTIONS

The following general safety guidelines are provided to help ensure your own personal safety and protect your product from potential damage. Remember to consult the product user instructions for more details.

Static electricity can be harmful to electronic components. Discharge static electricity from your body (i.e. touching grounded bare metal) before touching the product.

Do not attempt to service the product and never disassemble the product. For some products with a user replaceable battery, please read and follow the instructions in the user manual.

Do not spill food or liquid on your product and never push any objects into the openings of your product.

Do not use this product near water, areas with high humidity, or condensation unless the product is specifically rated for outdoor application.

Keep the product away from radiators and other heat sources.

Always unplug the product from mains power before cleaning and use a dry lint free cloth only.

Warning

Replacement of a battery with an incorrect type that can defeat a safeguard (for example, in the case of some lithium battery types);

Disposal of a battery into fire or a hot oven, or mechanically crushing or cutting of a battery, that can result in an explosion;

Leaving a battery in an extremely high temperature surrounding environment that can result in an explosion or the leakage of flammable liquid or gas;

A battery subjected to extremely low air pressure that may result in an explosion or the leakage of flammable liquid or gas.

Battery Removal Instruction

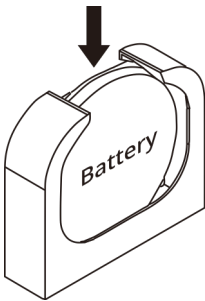
This product contains a rechargeable lithium-ion battery pack located inside the housing.

To remove the battery:

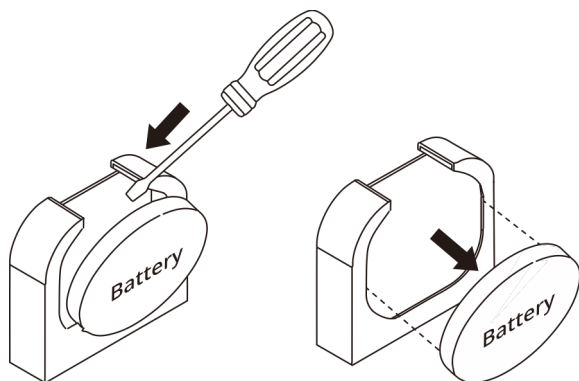
Step 1: Powered off the devices.

Step 2: Remove the screws and top cover.

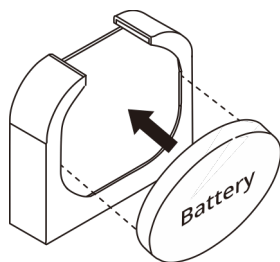
Step 3: Locate the battery cell on the motherboard



Step 4: using a flathead screwdriver to gently pry the battery. Lift the battery up and remove it from holder.



Step 5: Insert the new battery into the holder with the “+” side facing up.



Warning: Do not short-circuit, puncture, or incinerate the battery. Always dispose of used batteries at certified recycling centers. If the battery cannot be removed safely by the user, please contact a qualified technician or authorized service provider.