L3HVR Series Recorders

User Manual for:
L3HVR4, L3HVR8, L3HVR16

Rev. 08/21/2023

Liberty Wire & Cable, Inc. 1490 Garden of the Gods Rd, Ste F Colorado Springs, CO 80907 — 855.388.7422

Legal Notice

Trademark Statement：

VGA is trademark of IBM Corporation.

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

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

Responsibility statement：

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

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

Privacy Protection Reminder:

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

About This Document：

- This document is for use with several models. The appearance and function of the products are subject to the actual products.
- Any loss caused by failure to follow the instructions in this document is the responsibility of the user.
- This document will be updated in real time according to the laws and regulations of the relevant region. For details, please refer to the product's paper, electronic CD, QR code or

official website. If the paper and electronic files are inconsistent, please refer to the electronic file as.

- The company reserves the right to modify any information in this document at any time.
- The revised content will be added to the new version of this document without prior notice.
- This document may contain technical inaccuracies, or inconsistencies with product features and operations, or typographical errors, which are subject to the company's final interpretation.
- If the obtained PDF document cannot be opened, please use the latest version or the most mainstream reading tool.

Network Security Advice

Required measures to ensure basic network security of equipment:

Modify the factory default password and use a strong password

Devices that do not change the factory default password or use a weak password are the easiest to be hacked. Users are advised to modify the default password and use strong passwords whenever possible (minimum of 6 characters, including uppercase, lowercase, number, and symbol).

Update firmware

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

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

1. **Change your password regularly**

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

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

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

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

3. **Use HTTPS/SSL encryption**

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

4. **Enable IP filtering**

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

5. **Change the ONVIF password**

For some old versions of the IP camera firmware, after the system's master password is changed, the ONVIF password will not be automatically changed. You must update the camera's firmware or manually update the ONIVF password.

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

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

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

7. Use a different username and password on the video surveillance system.

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

8. Restrict the permissions of the ordinary account

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

UPNP

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

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

SNMP

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

Multicast

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

12. Check logs

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

Physically protect your device

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

It is highly recommended that you use PoE to connect IP cameras to DVR.

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

Network isolation between DVR and IP cameras

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

About This Document

Purpose

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

Symbol Conventions

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

Symbol	Description
⚠ DANGER	It's for warning when a hazard or a hazardous condition is likely to be life-threatening
⚠ WARNING	Alerts you to a medium or low risk hazard that, if not avoided, could result in moderate or minor injury.
⚠ CAUTION	Alerts you to a potentially hazardous situation that, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results.
🔑 TIP	Provides a tip that may help you solve a problem or save time.
📖 NOTE	Provides additional information to emphasize or supplement important points in the main text.

Safety Instructions

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

Requirements

- The front-end devices of POE are required to be installed indoors.
- The DVR device does not support wall mounting.
- Do not place and install the device in direct sunlight or near heat-generating equipment.
- Do not install the device in a place subject to high humidity, dust or soot.
- Please keep the equipment installed horizontally or install the equipment in a stable place, taking care to prevent the product from falling.
- Do not drop or spill liquid into the device and ensure that no liquid-filled items are placed on the device to prevent liquid from flowing into the device.
- Install the device in a well-ventilated area, and do not block the ventilation openings of the device.
- Use the device only within the rated input and output range.
- Do not disassemble the device at will.
- Please transport, use and store the device within the permissible humidity and temperature range.

Power Requirement

- Be sure to use the specified manufacturer's model battery, otherwise there is a danger of explosion!
- Be sure to use the battery as required, otherwise there is a danger of the battery catching fire, exploding or burning!
- Only use the same model of battery when replacing the battery!
- Be sure to dispose of the used battery as the instruction of battery!
- Be sure to use the power adapter that meets standard with the device, otherwise the personal injury or equipment damage caused by the user will be borne by the user.

- Use a power supply that meets the SELV (Safety Extra Low Voltage) requirements and supply power according to the rated voltage of IEC60950-1 in accordance with the Limited Power Source. The specific power supply requirements are based on the equipment label.
- Connect the Class I product to the power outlet with a protective ground connection.
- The appliance is coupled to the port unit. Keep it at a proper angle for normal use.

Important Statement

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

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

Contents

1 Preface

1.1 Product Description

This product is a high-performance DVR device. The product has multiple functions: preview, split view, real-time video storage, mouse quick operation, remote management and control.

This product supports three storage methods: central storage, front-end storage, and client storage. The front-end monitoring point can be located anywhere in the network without geographical restrictions. It is combined with other front-end devices such as network cameras, network construction of video server, and professional video surveillance systems to form a powerful security monitoring network. In the networked deployment system of this product, the central point and the monitoring point need only one network cable to connect There is no need to connect video and audio cables. The operation is simple, and the cost of wiring and maintenance cost is low.

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

1.2 Product Features

1.2.1 Cloud Upgrade

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

1.2.2 Real-time Monitoring

It has a VGA (Video Graphics Array) port and an HDMI (High Definition Media Interface) port. It can realize monitoring function through monitor and display, and support VGA and HDMI output at the same time.

1.2.3 Playback

Each channel can record video independently in real time and perform functions such as retrieval, playback, network monitoring, video query and download. For more details, please refer to chapter Playback

Multiple playback modes: slow release, fast release, reverse playback, and frame-by-frame playback.

The exact time of events can be displayed when playing back the video.

You can select any area of the screen to partially zoom in.

1.2.4 User Management

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

1.2.5 Storage Funtion

According to the user's configuration and policies (alarm or time settings), the corresponding audio and video data transmitted by the remote device is stored in the DVR device. For details, please refer to chapter Storage Management.

Users can record by WEB mode as needed. The video files are stored on the computer where the client is located. Please refer to chapter Storage.

1.2.6 Alarm Function

Real-time response to external alarm input, correct processing according to the user's preset linkage settings and giving corresponding prompts.

The setting options of the central alarm receiving server are provided, so that the alarm information can be actively and remotely notified, and the alarm input can come from various external devices connected.

The alarm information can be notified to the user by mail or APP.

1.2.7 Network Monitoring

Through the network, the audio and video data of the IP camera or NVS (Network Video Server) of the DVR device is transmitted to the network terminal for decompression and reproduction.

The device supports 8 simultaneous online users to perform streaming operations.

The audio and video data is transmitted using protocols such as HTTP (Hyper Text Transfer Protocol), TCP (Transmission Control Protocol), UDF (User Datagram Protocol), MULTICAST, RTP (Real-time Transport Protocol), and RTCP (Real Time Streaming Protocol).

Use SNMP (Simple Network Management Protocol) for some alarm data or information

Support WEB mode access system, applied to WAN, LAN environment.

1.2.8 Split Screen

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

1.2.9 Recording Function

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

1.2.10 Backup Function

Support USB2.0 and eSATA video backup.

1.2.11 External Device Control

The peripheral control function is supported, and the control protocol and connection interface of each peripheral can set as you need.

Support transparent data transmission of multiple interfaces, such as: RS232, RS485.

1.2.12 Accessibility

Supports video NTSL (Nation Television Standards Committee) system and PAL (Phase Alteration Line) system.

Supports system resource information and real-time display of running status.

Supports for logging recording.

Supports local GUI (Graphical User Interface) output and quick menu operation via mouse.

Supports playback of audio and video from remote IPC or NVS devices.

📖 **NOTE**

For other functions, please see the following text.

2 Product Structure

2.1 Front Panel

Figure 2-1 One disk/two disks model

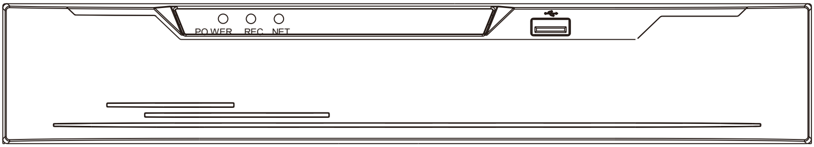


Table 2-1 Front panel function

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

Figure 2-2 Rear panel

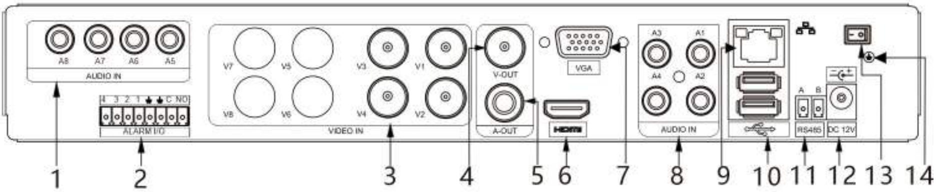


Table 2-2 Rear panel function

No.	Port	Description
1	AUDIO IN	Audio input, such as microphone.

2	ALARM I/O	Alarm input and alarm output.
3	VIDEO IN	Analog video signal access.
4	CVBS	CVBS output.
5	A-OUT	Audio output.
6	VGA	Video output interface.
7	HDMI	
8	AUDIO IN	Audio input, such as microphone.
9	LAN	RJ 45 10/100/1000 Mbps adaptive Ethernet interface
10	USB 3.0	Can be connected to USB device, such as mouse, keyboard. the bottom port only support U disk, the upper and front panel USB port cannot be used as the same time.
11	RS485	Standard RS485 serial communication interface of the device.
12	DC 12	DC Power 12 V.
13	⊟	Power switch (some models do not have switch).
14	⏚	Safe ground screw of the device.

2.2 Important Notes

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

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

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

- Use Monitoring dedicated hard disks as the storage devices of the DVR with high stability and competitive price/performance ratios (the quality of hard disks sold on markets varies greatly with different brands and models).
- Do not open the enclosure of this product unless performed by a professional person to avoid damage and electric shock.

- We are not liable for any video data loss caused by improper installation, configuration, operation, and hard disk errors.
- All images in the document are for reference only, please subject to the actual products.

2.3 About This User Manual

Please note the following points before using this user manual:

- This user manual is intended for persons who operate and use the DVR.
- The information in this user manual applies to the full series DVR, DVR as an example for description.
- Read this user manual carefully before using the DVR and follow the methods described in this manual when using the DVR.
- If you have any doubts when using the DVR, contact your product seller.
- As our products are subject to continuous improvement, we reserve the right to modify product manual, without notice and without incurring any obligation.

2.4 Installation Environment and Precautions

Installation environment

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

Table 2-3 Installation environment

Item	Description
Electromagnetism	The DVR meets the national standards for electromagnetic radiation. It will not cause harm to humans.
Temperature	–10°C to +45°C
Humidity	20% to 80%
Atmospheric pressure	86 Kpa to 106 Kpa
Power supply	DC 12V, 2A / DC 12V, DC220V, the current should not to be less than 3A, please refer to actual product.
Power consumption	<15W (not including the hard disk)

Installation precautions

Note the following points when installing and operating the DVR:

- The power adapter of the DVR uses DC48V±20% input. Do not use the DVR when voltage is too high or too low.
- Install the DVR horizontally.
- Avoid direct sunlight on the DVR and keep it away from any heat sources and hot environments.
- Connect the DVR to other devices correctly during installation.
- The DVR is not configured with any hard disk upon delivery. Install one or more hard disks when using the DVR for the first time.

lease choose high-quality hard drives to enable stable and reliable operation of the DVR. For more details, please refer to chapter 10 Disk Compatibility

Other precautions

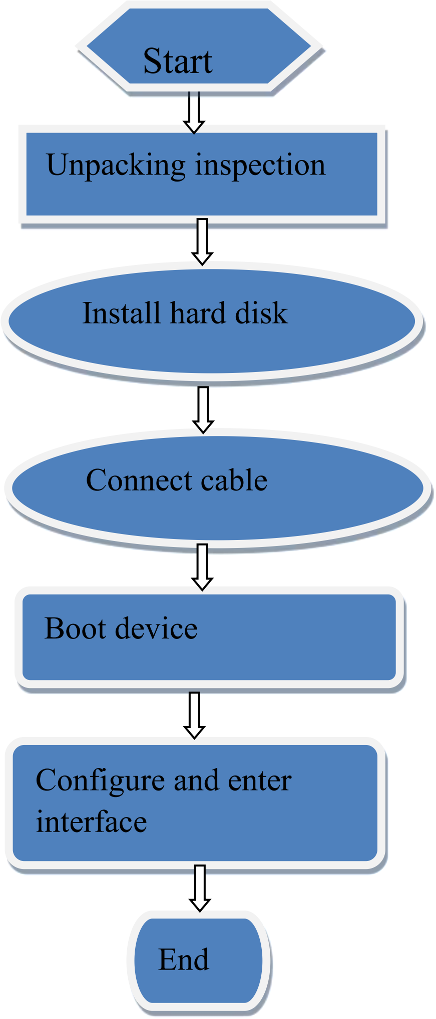
- Clean the DVR with a piece of soft and dry cloth. Do not use chemical solvents.
- Do not place objects on the DVR.

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

Series of DVR

3 Install Device

3.1 Process



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

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

Step 3 Connect the device cable.

Step 4 After ensuring that the device is connecting correct, connected the power and turn on the device.

Step 5 Configure the initial parameters of the device. The boot wizard contains network configuration, add cameras, and manage disks. For details, please refer to the chapter of Wizard .

3.2 Unpacking Inspection

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

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

Table 3-1 Unpacking inspection

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

		cable, fan power supply, and motherboard	NOTE If it is loose, please contact the company's after-sales personnel.

3.3 Install Hard Disk

Please use the recommended hard disk model. For more details, see *10 Disk Compatibility*.

It is not recommended to use a PC dedicated hard disk.

CAUTION

When replacing the hard disk, please turn off the power and then open the device to replace the hard disk.

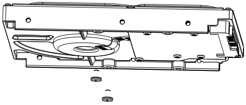
Please use the monitoring dedicated SATA hard disk recommended by the hard disk manufacturer.

Choose the hard disk capacity according to the recording requirements.

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

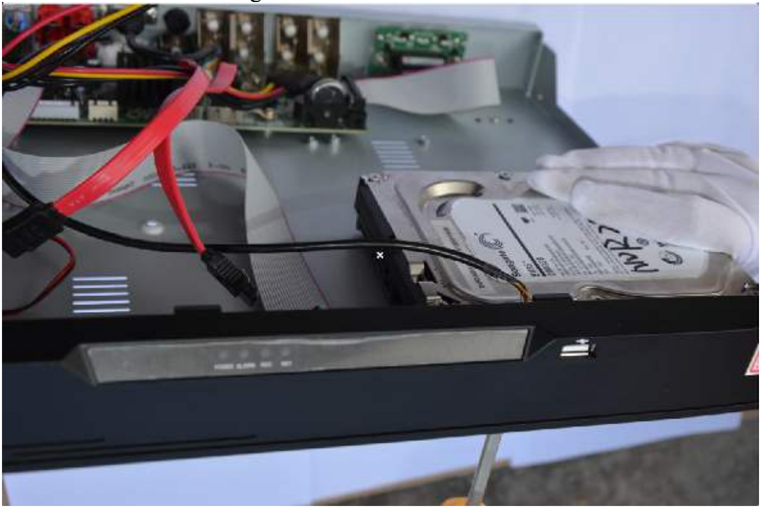
Step 2 Take out the screws and silicone cushion, pass the screws through the silicone cushion, and secure it to the screw holes, as show in Figure 3-1..

Figure 3-2 Installing the hard disk screws



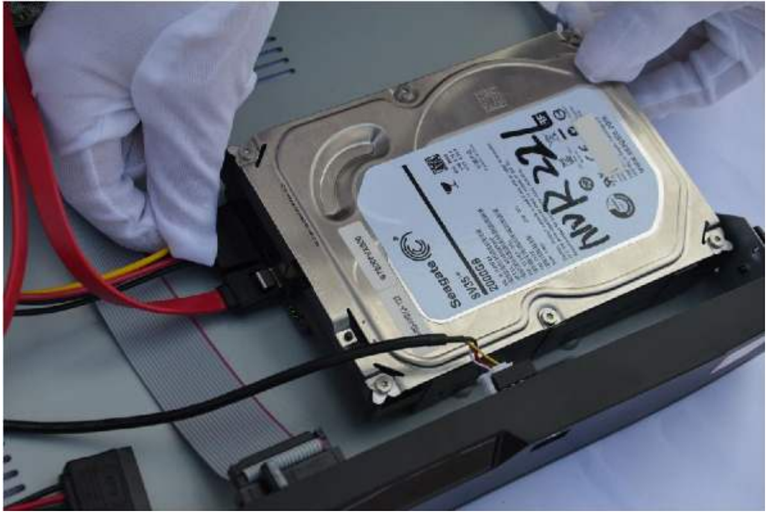
Step 3 Pass the screws through the holes on the base and put the hard disk in place, as shown in Figure 3-2.

Figure 3-3 Install hard disk



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

Figure 3-4 Install hard disk



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

4 Basic Operations

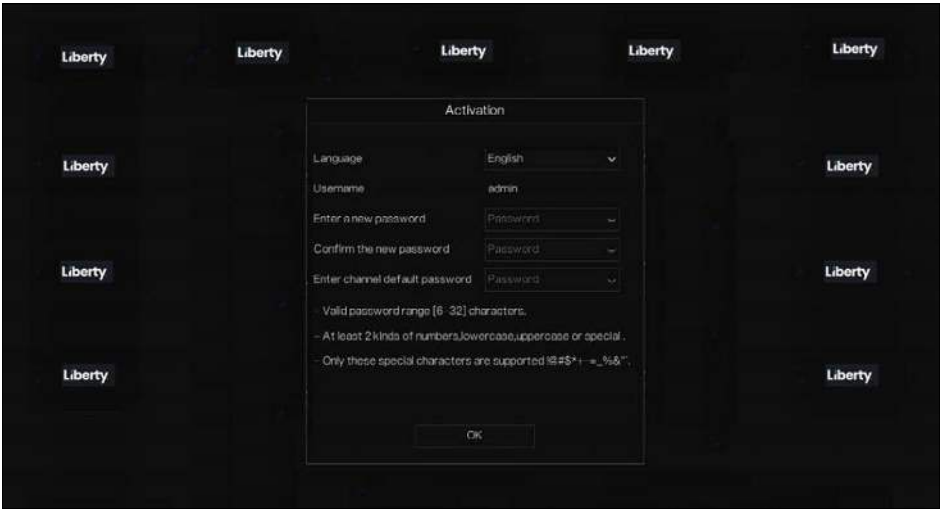
4.1 Power on the Device

CAUTION

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

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

Figure 4-1 Real-time video screen



Activation

Language: English

Username: admin

Enter a new password: Password

Confirm the new password: Password

Enter channel default password: Password

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

NOTE

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

The hard disk is new and is not formatted. Login to the system and format the hard disk.

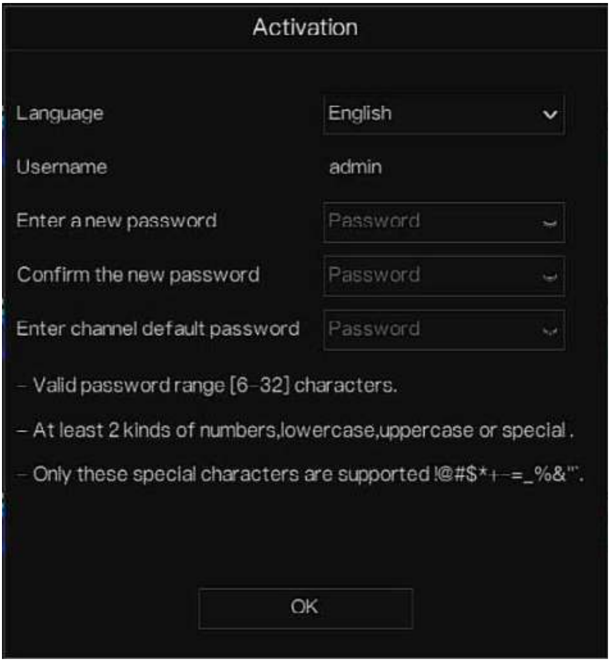
The hard disk is formatted, but the file system is inconsistent with the file system supported by the DVR. Format the hard disk.

The hard disk is damaged.

4.2 Activation

When login the device at first time, or reset the DVR, you need to activate the device and set login and channel default password, as shown in Figure 4-2.

Figure 4-2 Activation



Activation

Language: English

Username: admin

Enter a new password: Password

Confirm the new password: Password

Enter channel default password: Password

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

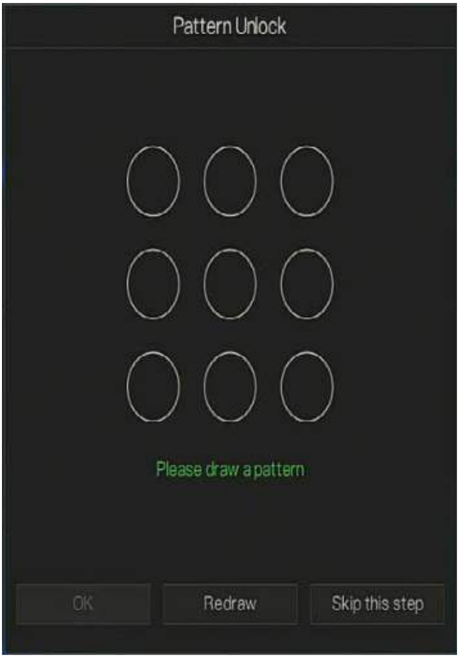
Table 4-1 Description of activation

Name	Description
Username	The default username is admin, and “admin” is super administrator.

Password	Valid password must be 6-32 characters long. At least 2 kinds of numbers, lower case, upper case or special characters contained. Only these special characters are supported !@#$*+-=_%&”
Confirm password	
Channel password	The DVR channel connection password is the camera login password.

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

Figure 4-3 Set pattern unlock



Please draw a pattern

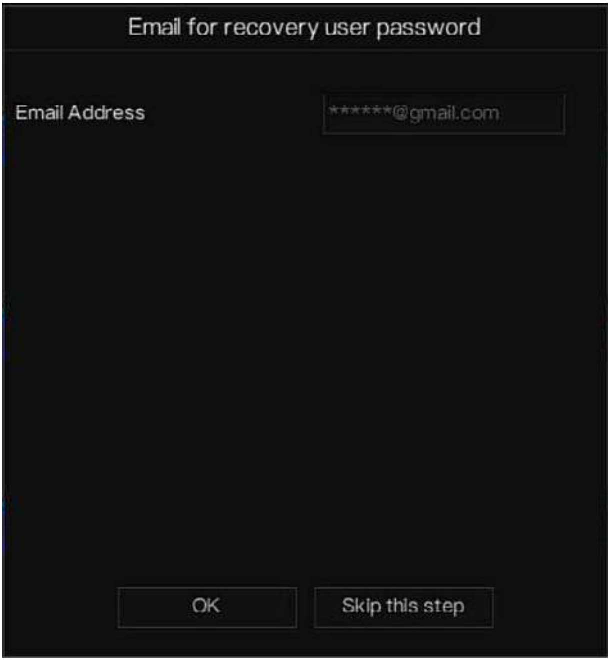
NOTE

After setting pattern unlock, the system default login will be pattern unlock login. If pattern unlock is not set, you need 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 verification code. The password will be reset when you forget it, as shown in Figure 4-4.

Figure 4-4 Set Email



Email for recovery user password

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

NOTE

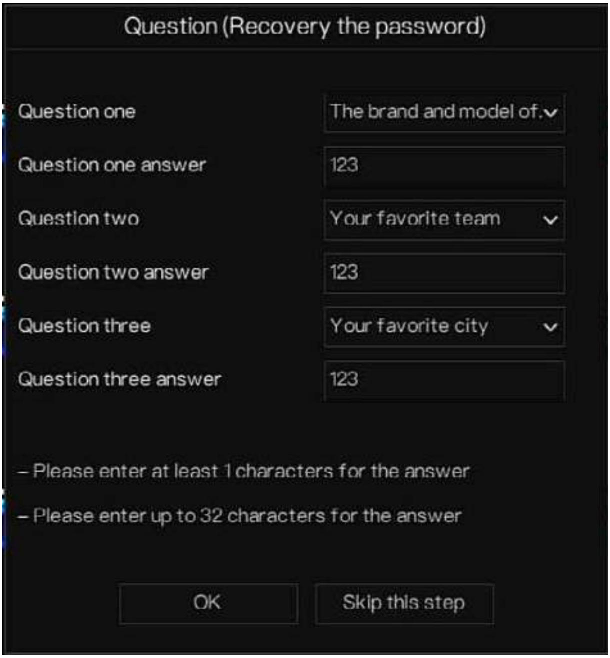
Set the email address, if you forget the password, you can receive the verification, and reset the password.

If the email address is not set, you can reply to the secure question or send the QR code to the seller to get the temporary password to login to the device.

If you don't need to set the email, click "**Skip this step**".

Set the secure question, if user forgot the password can through the secure questions to create new password to login the device.

Figure 4-5 Set question



Question (Recovery the password)

Question one: The brand and model of.

Question one answer: 123

Question two: Your favorite team

Question two answer: 123

Question three: Your favorite city

Question three answer: 123

– Please enter at least 1 characters for the answer

– Please enter up to 32 characters for the answer

NOTE

The users can set three questions, and if they forget the password, they can answer the question and enter the reset password interface.

Question 1 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 most funning/worst design you have ever seen

Question 2: Your favorite team

Question 3: Your favorite city

The three question options cannot be set to the same.

The answer requires a minimum of four characters and a maximum of 32 characters.

If you do not want to set a password question, you can click **Skip this step**.

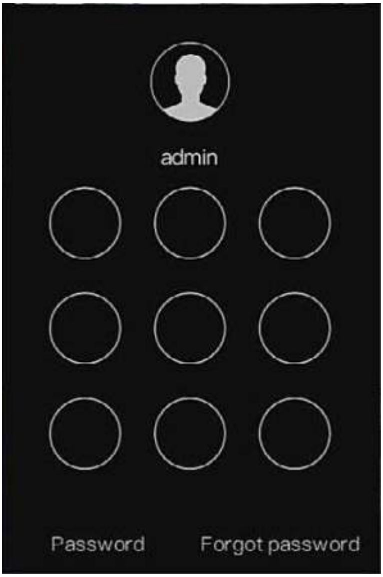
4.3 Power off the Device

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

4.4 Login to the System

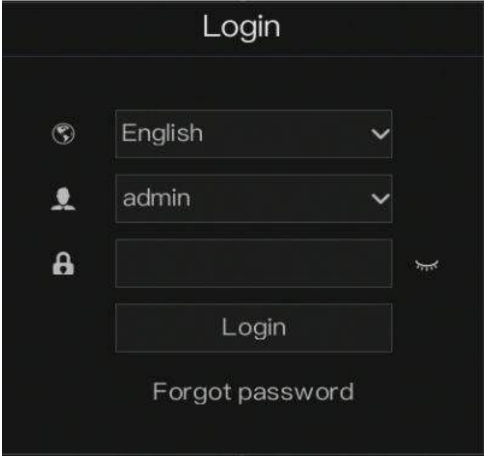
Step 1 Login to the device, there are two modes to login if you set the pattern unlock, as shown in Figure 4-6.

Figure 4-6 Pattern unlock login page



Step 2 On the DVR login page, click " Password" to at pattern unlock interface. If users don't set the pattern unlock it will show password to login interface directly, select the language, as shown in Figure 4-7.

Figure 4-7 Password login page



Step 3 Input the username and password.

NOTE

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

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

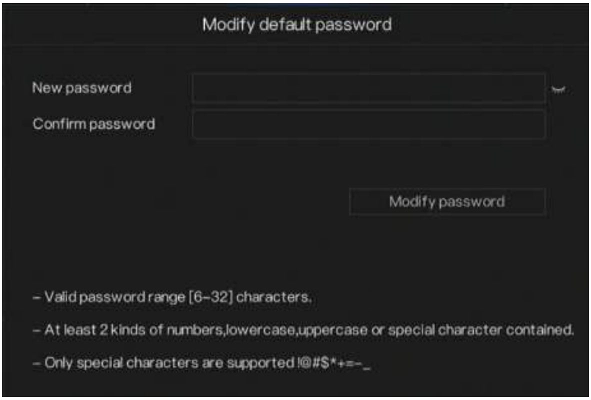
1. Scan the QR code and send the QR code to your seller, seller send the verification code to user and set a new password to login .

2. Answer the secure question to create a new password.

Step 4 Click Login to access the main User Interface (UI).

Step 5 Modify the default password, as shown in Figure 4-8

Figure 4-8 Modify default password



Modify default password

New password

Confirm password

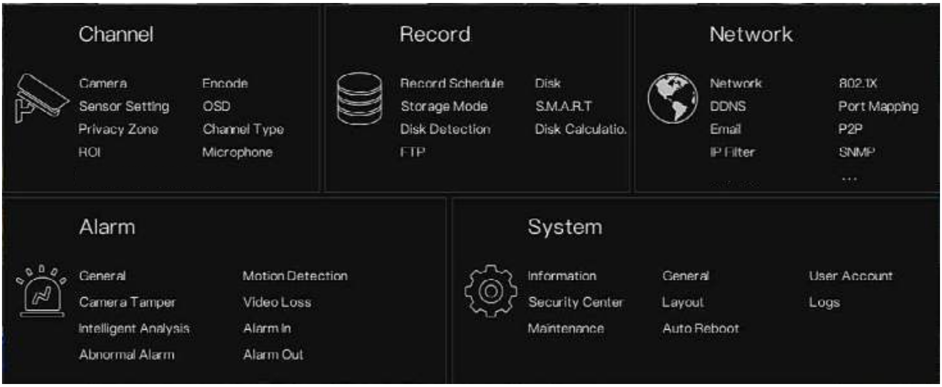
Modify password

- Valid password range [6-32] characters.

- At least 2 kinds of numbers,lowercase,uppercase or special character contained.

- Only special characters are supported !@#$*+=-_

Figure 4-9 Main menu



----End

5 Wizard

Login the DVR, the wizard is showing on live video, click **Start Wizard,** the pop-up window will show as Figure 5-1.

Figure 5-1 Wizard

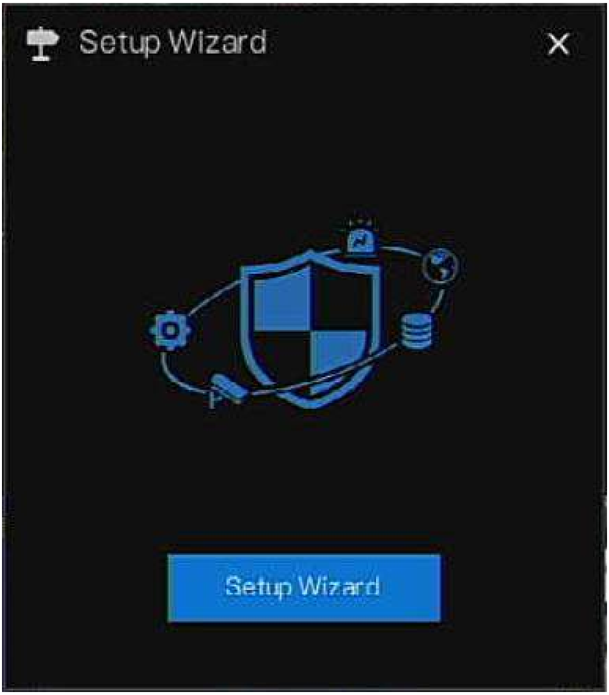
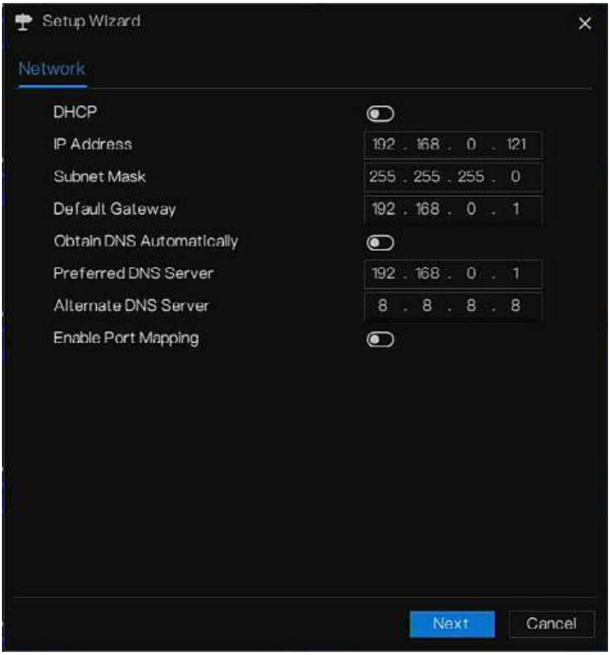


Figure 5-2 Wizard of network



DHCP
IP Address 192 . 168 . 0 . 121
Subnet Mask 255 . 255 . 255 . 0
Default Gateway 192 . 168 . 0 . 1
Obtain DNS Automatically
Preferred DNS Server 192 . 168 . 0 . 1
Alternate DNS Server 8 . 8 . 8 . 8
Enable Port Mapping

Step 1 Set parameters, for more details please refer to Table 5- 1.

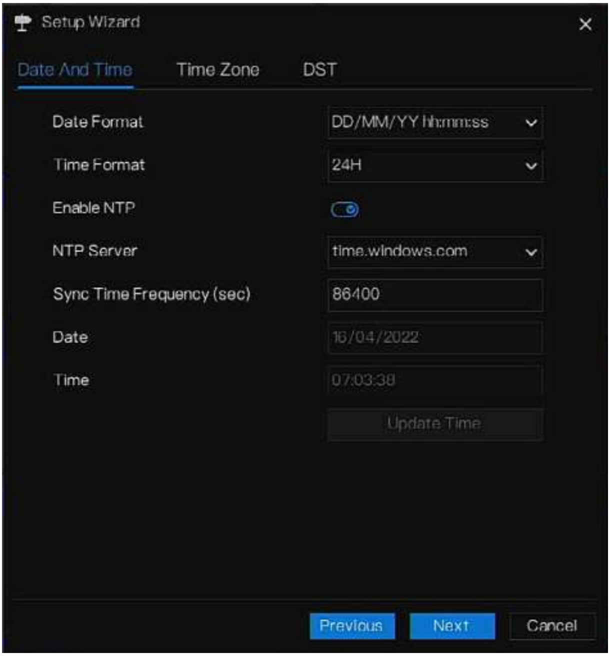
Table 5- 1 Network parameter

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

Parameter	Description	Configuration
	he must set that	Manual [Default value] 192.168.0.1
Obtain DNS automatically	N/A	[Setting method] Enable
Preferred DNS Server	N/A	[Setting method] Manual [Default value] 192.168.0.1
Alternate DNS Server	N/A	[Setting method] Manual [Default value] 192.168.0.1
Enable Port Mapping	Auto: Obtain HTTP port, HTTPS port, RTSP port and Control Port. Manual: Set the port manually.	[Setting method] Choose type from drop-down list [Default value] Auto
HTTP Port	N/A	[Setting method] When UPnP is manual, you need to set these.
HTTPS Port	N/A	
RTSP	N/A	
Control Port	N/A	

Step 2 Click Next to view the basic information about device, as shown in Figure 5-3.

Figure 5-3 Wizard of date and time



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

Time Format: 24H

Enable NTP

NTP Server: time.windows.com

Sync Time Frequency (sec): 86400

Date: 16/04/2022

Time: 07:03:38

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

Click to synchronize time from network.

Disable the NTP-Sync, set time manually.

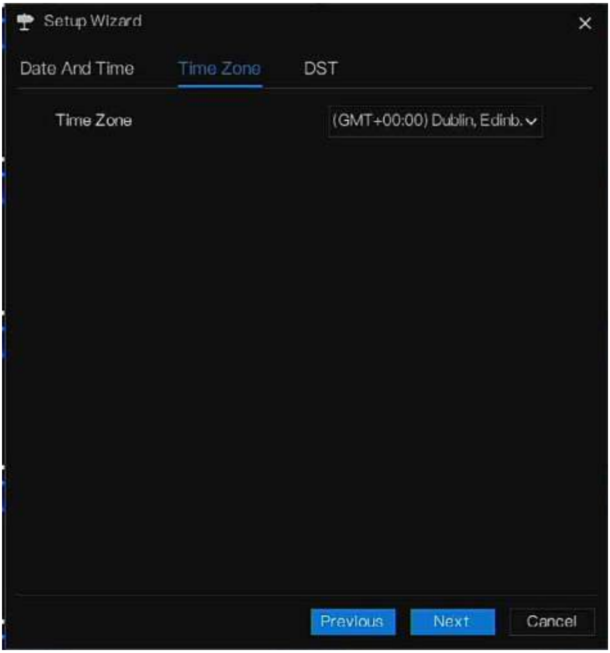
Roll the mouse to choose year, month and day when clicking the date.

Roll the mouse to choose hour, minute and second when clicking the date.

Click **Modify Time** to save the time.

Step 3 Click **Time Zone,** choose the current time zone from drop-down list, as shown in Figure 5-4.

Figure 5-4 Wizard of time zone

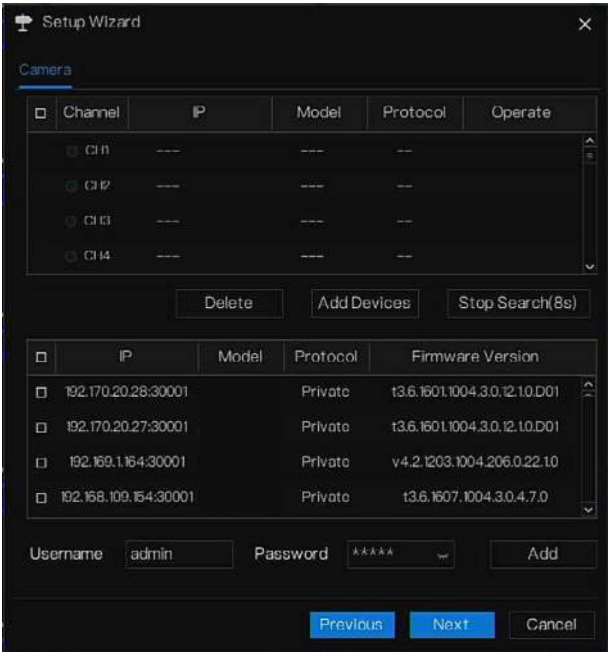


Time Zone (GMT+00:00) Dublin, Edinb.

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

Step 5 Click Next to add cameras, as shown in Figure 5-5.

Figure 5-5 Wizard of adding camera



Setup Wizard

Camera

□	Channel	IP	Model	Protocol	Operate
	CH1	----	----	--	
	CH2	----	----	--	
	CH3	----	----	--	
	CH4	----	----	--	

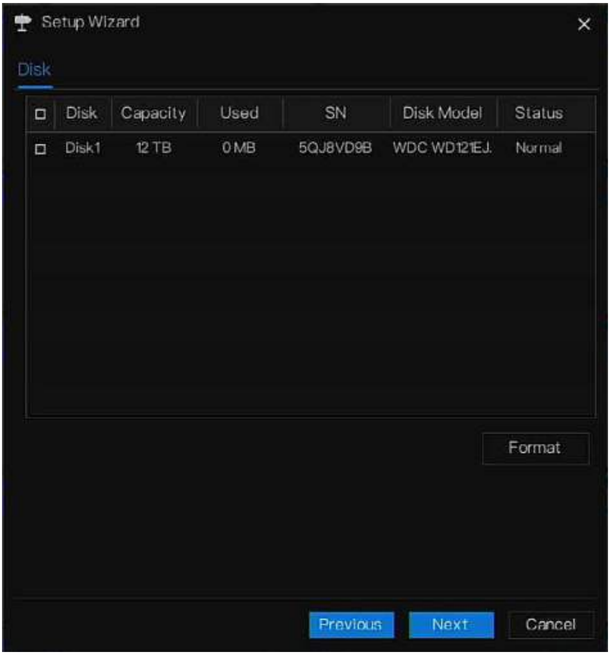
□	IP	Model	Protocol	Firmware Version
□	192.170.20.28:30001		Private	t3.6.1601.1004.3.0.12.1.0.D01
□	192.170.20.27:30001		Private	t3.6.1601.1004.3.0.12.1.0.D01
□	192.169.1.164:30001		Private	v4.2.1203.1004.206.0.22.1.0
□	192.168.109.154:30001		Private	t3.6.1607.1004.3.0.4.7.0

Username admin Password *****

For more details of adding camera please refer to *chapter 7.3*.

Step 6 Click Next to enter wizard of disk, as shown in Figure 5-6.

Figure 5-6 Wizard of disk

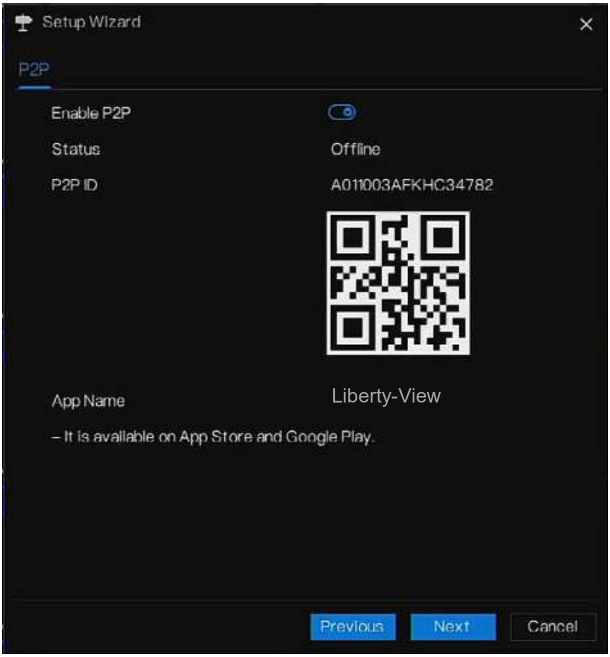


□	Disk	Capacity	Used	SN	Disk Model	Status
□	Disk1	12 TB	0 MB	5QJ8VD9B	WDC WD121EJ.	Normal

You can view the general information of disk. You can also format the disk.

Step 7 Click Next to enter wizard of P2P, as shown in Figure 5-7

Figure 5-7 P2P



Enable P2P

Status Offline

P2P ID A011003AFKHC34782

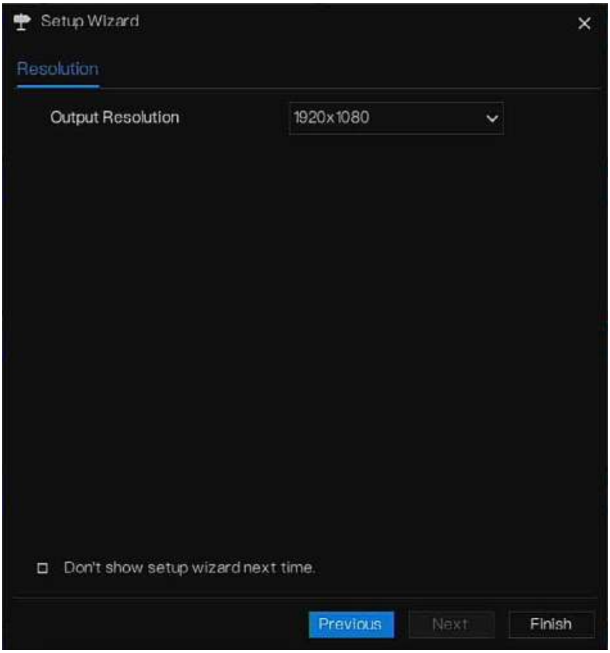
App Name Liberty-View

– It is available on App Store and Google Play.

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

Step 9 Click Next to enter the wizard of resolution , as shown in Figure 5-8. Choose resolution from drop-down list.

Figure 5-8 Wizard of resolution



Output Resolution: 1920x1080

□ Don't show setup wizard next time.

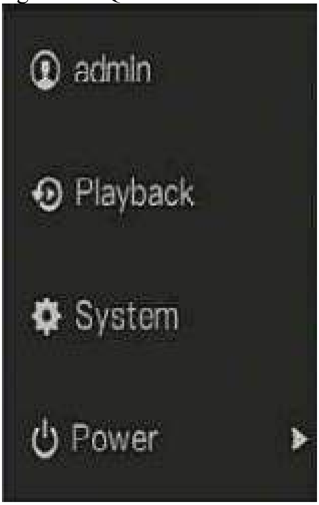
Step 10 Click Finish to end the wizard, tick the **Not show this window next time,** wizard would not show at next time. Reopen wizard at **System >User Account > Adv. Setting.**

6 Quick Navigation

The DVR operation interface appears. Move the cursor to the bottom of the screen to display the DVR's floating menu.

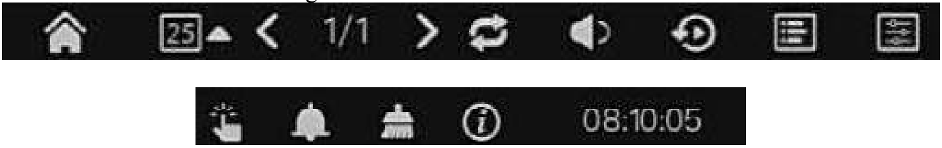
Click 🏠 in the left of DVR floating menu bar. The quick home menu is showing. The quick home menu provides **Playback**, **System and Power (Shutdown, Reboot and Logout)** as shown in Figure 6-1.

Figure 6-1 Quick home menu

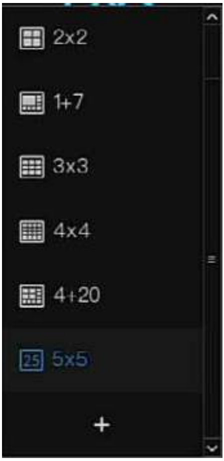


In the middle of DVR floating menu bar, the video tool bar provides **Split screen**, **switch page, Auto Sequence, Volume, Playback, Channel Information,** and **Live View Strategy** as shown in Figure 6-2.

Figure 6-2 Real-time video toolbar

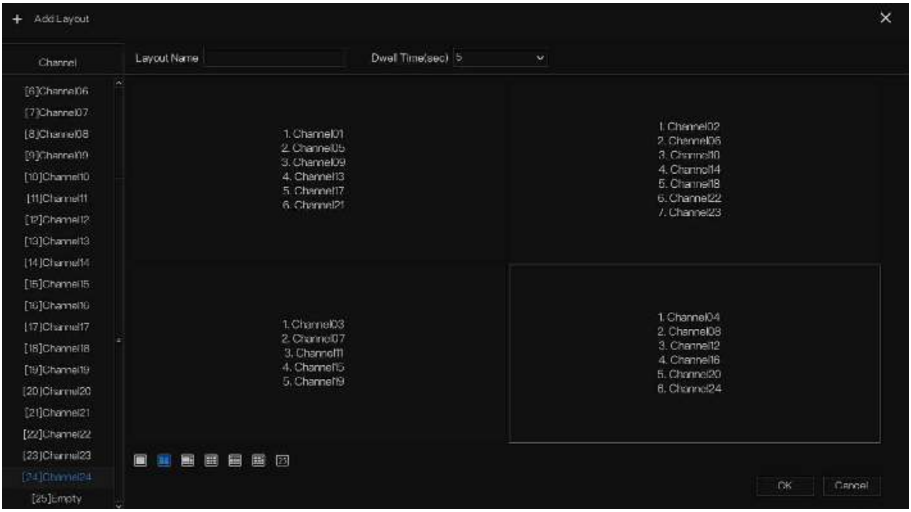


The real-time video toolbar is described as follows:



: Layout. Users can choose layout and add new layout strategies as shown in Figure 6-3. Click ▲ on the right of screen splitting format and choose the channels to view the video.

Figure 6-3 Add layout



Layout Name

Dwell Time(sec) 5

1. Channel01
2. Channel05
3. Channel09
4. Channel13
5. Channel17
6. Channel21

1. Channel02
2. Channel06
3. Channel10
4. Channel14
5. Channel18
6. Channel22
7. Channel23

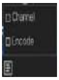
1. Channel03
2. Channel07
3. Channel11
4. Channel15
5. Channel19

1. Channel04
2. Channel08
3. Channel12
4. Channel16
5. Channel20
6. Channel24

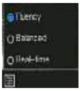
Input the layout name, choose the dwell time, and choose the splitting format. Choose one channel or many channels to add on screen.

: Auto Sequence. Click on the icon, the layout dwell on screen is enabled, for how to set the dwell on, please refer to *chapter 7.7.5*.

: Audio. Click on the icon, the audio setting screen is displaying, which you can choose the channel and adjust the volume.



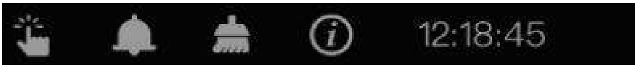
: Channel information, tick the channel or encode, the live video will show the channel information.



: Live view strategy, users can depend on the network to switch the strategy, there are three modes, such as fluency, balanced and real-time.

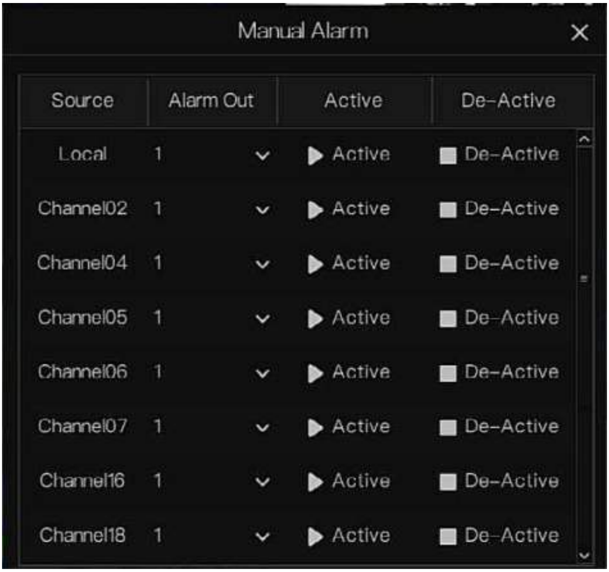
A main menu quick toolbar is display on the right of DVR floating menu bar. The main menu quick toolbar provides **Manual Alarm, Alarm Information, Clean Alarm Information** and **Time**, as shown in Figure 6-4.

Figure 6-4 Main menu quick toolbar



: Manual alarm, Click on the icon, the window shows in Figure 6-5.

Figure 6-5 Manual alarm



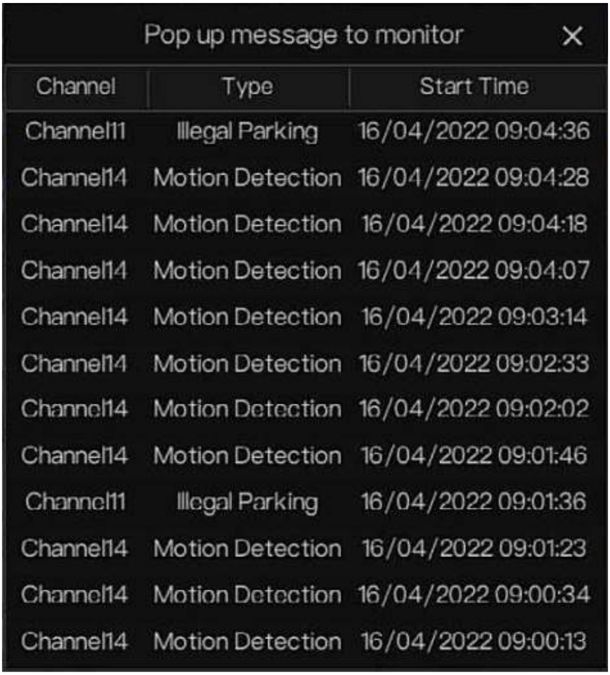
Manual Alarm

Source	Alarm Out	Active	De-Active
Local	1	▶ Active	■ De-Active
Channel02	1	▶ Active	■ De-Active
Channel04	1	▶ Active	■ De-Active
Channel05	1	▶ Active	■ De-Active
Channel06	1	▶ Active	■ De-Active
Channel07	1	▶ Active	■ De-Active
Channel16	1	▶ Active	■ De-Active
Channel18	1	▶ Active	■ De-Active

🔔: Alarm message, Click on the icon to display a pop-up message window, as shown in Figure 6-6.

6.1 Alarm message

Figure 6-6 Alarm message



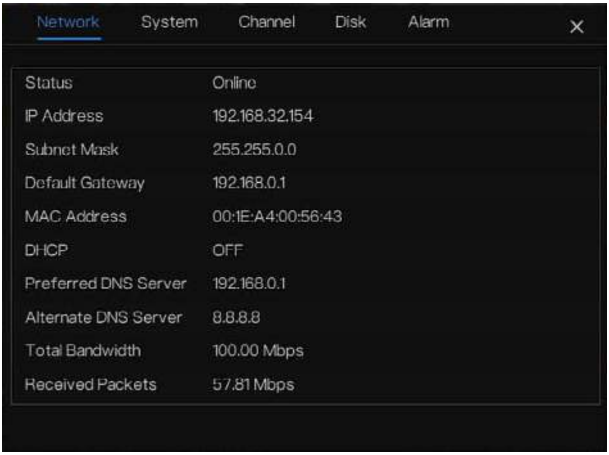
Pop up message to monitor

Channel	Type	Start Time
Channel11	Illegal Parking	16/04/2022 09:04:36
Channel14	Motion Detection	16/04/2022 09:04:28
Channel14	Motion Detection	16/04/2022 09:04:18
Channel14	Motion Detection	16/04/2022 09:04:07
Channel14	Motion Detection	16/04/2022 09:03:14
Channel14	Motion Detection	16/04/2022 09:02:33
Channel14	Motion Detection	16/04/2022 09:02:02
Channel14	Motion Detection	16/04/2022 09:01:46
Channel11	Illegal Parking	16/04/2022 09:01:36
Channel14	Motion Detection	16/04/2022 09:01:23
Channel14	Motion Detection	16/04/2022 09:00:34
Channel14	Motion Detection	16/04/2022 09:00:13

🧹: Clean alarm, Click on the icon to clear current alarm actions like voice and external alarm.

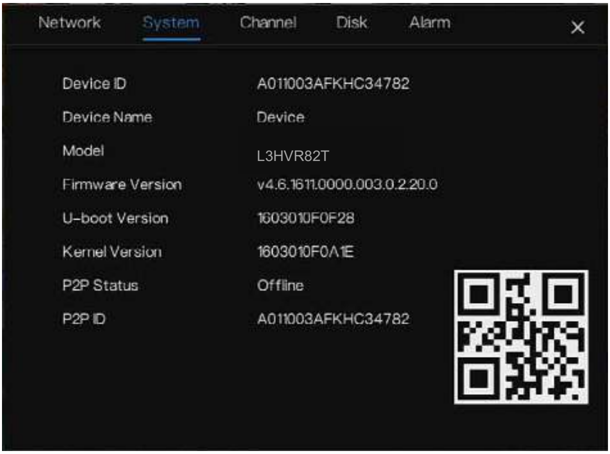
ⓘ: Information, click on the icon and the genreal information would show, like network, system, channel and disk, as shown in Figure 6-7.

Figure 6-7 Information



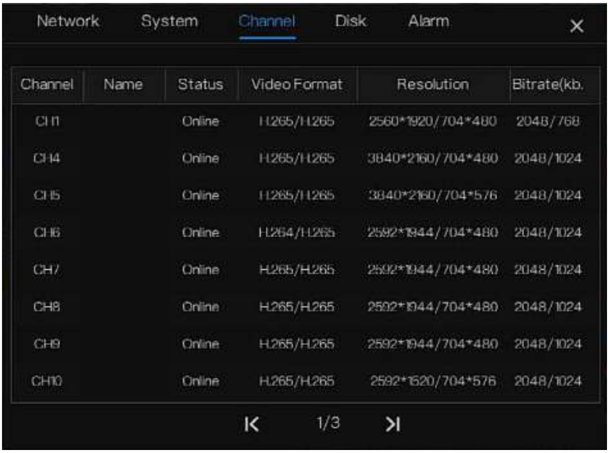
Status	Online
IP Address	192.168.32.154
Subnet Mask	255.255.0.0
Default Gateway	192.168.0.1
MAC Address	00:1E:A4:00:56:43
DHCP	OFF
Preferred DNS Server	192.168.0.1
Alternate DNS Server	8.8.8.8
Total Bandwidth	100.00 Mbps
Received Packets	57.81 Mbps

Figure 6-8 System



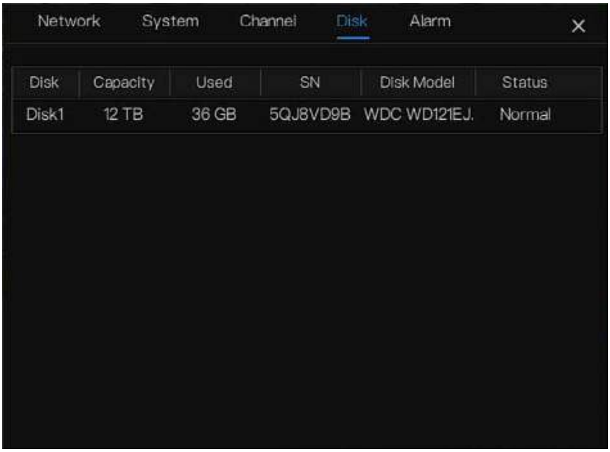
Device ID	A011003AFKHC34782
Device Name	Device
Model	L3HVR82T
Firmware Version	v4.6.1611.0000.003.0.2.20.0
U-boot Version	1603010F0F28
Kernel Version	1603010F0A1E
P2P Status	Offline
P2P ID	A011003AFKHC34782

Figure 6-9 Channel



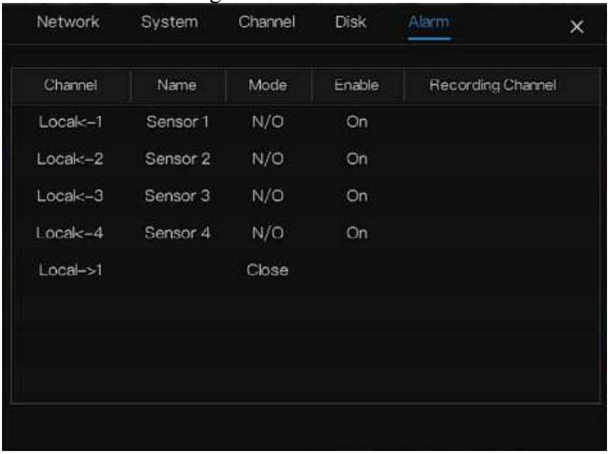
Channel	Name	Status	Video Format	Resolution	Bitrate(kb.
CH1		Online	H.265/H.265	2560*1920/704*480	2048/768
CH4		Online	H.265/H.265	3840*2160/704*480	2048/1024
CH5		Online	H.265/H.265	3840*2160/704*576	2048/1024
CH6		Online	H.264/H.265	2592*1944/704*480	2048/1024
CH7		Online	H.265/H.265	2592*1944/704*480	2048/1024
CH8		Online	H.265/H.265	2592*1944/704*480	2048/1024
CH9		Online	H.265/H.265	2592*1944/704*480	2048/1024
CH10		Online	H.265/H.265	2592*1520/704*576	2048/1024

Figure 6-10 Disk



Disk	Capacity	Used	SN	Disk Model	Status
Disk1	12 TB	36 GB	5QJ8VD9B	WDC WD121EJ.	Normal

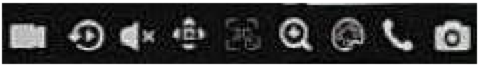
Figure 6-11 Alarm



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->1		Close		

6.2 Real Time Video Bar

Click realtime image, the quick setting will show as figure.



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

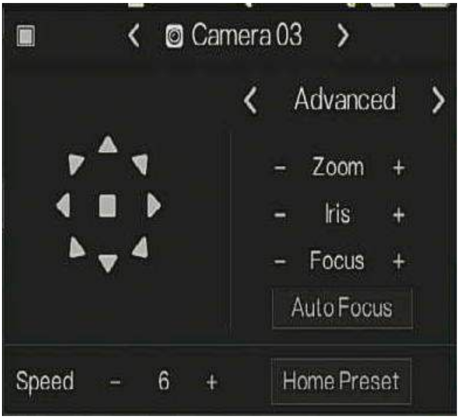
Instant playback: Click the icon, the window will play previous five minutes record video.

is the time bar of playback.

Audio: Open or close the audio.

PTZ: This function is only useful for speed dome cameras. You can adjust every parameter as shown in Figure 6-12.

Figure 6-12 PTZ adjust screen



Speed - 6 +

: Users adjust direction of camera.

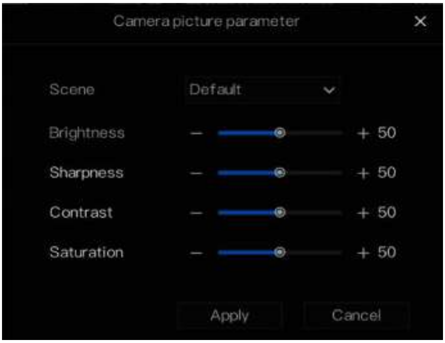
: At this part, users can set **Advanced, Scan** and **Tour** settings.

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

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

: Image, click on the icon,as shown in Figure 6-15. Select scene, and drag cursor to adjust value of brightness, sharpness, contrast and saturation.

Figure 6-13 Camera picture parameter



Camera picture parameter

Scene: Default

Brightness: 50

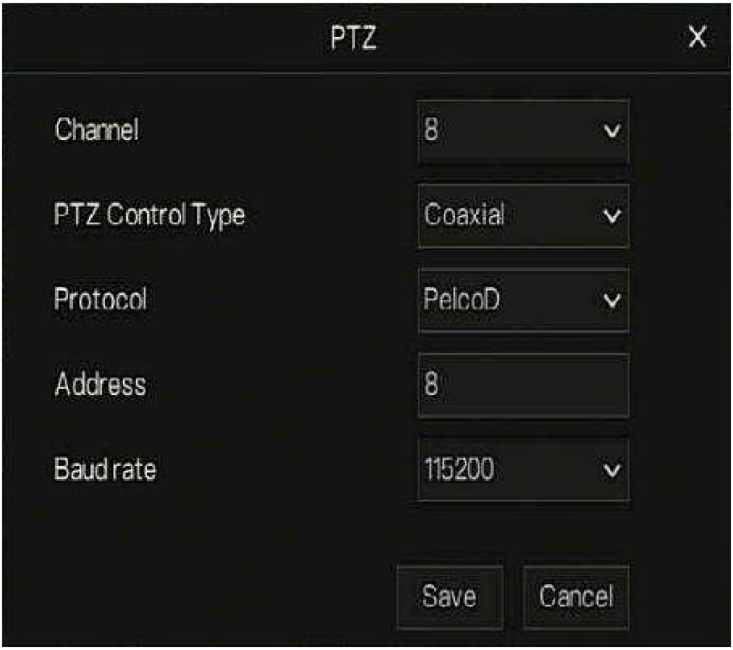
Sharpness: 50

Contrast: 50

Saturation: 50

⚙: click the button to enter the PTZ setting, as shown in Figure 6-14.

Figure 6-14 PTZ setting



PTZ

Channel: 8

PTZ Control Type: Coaxial

Protocol: PelcoD

Address: 8

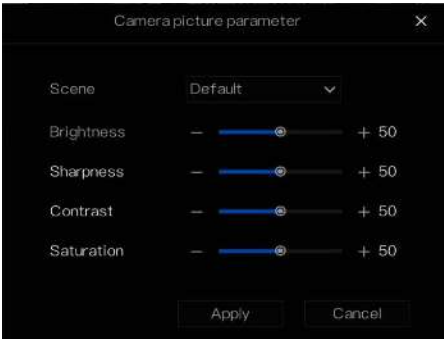
Baud rate: 115200

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

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

🎨: Image, click on the icon ,as shown in Figure 6-15. Select scene, and drag cursor to adjust value of brightness, sharpness, contrast and saturation.

Figure 6-15 Camera picture parameter



Camera picture parameter

Scene: Default

Brightness: 50

Sharpness: 50

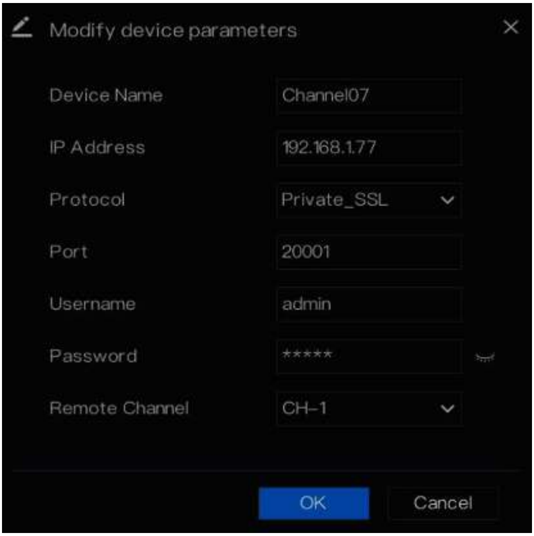
Contrast: 50

Saturation: 50

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

✎: Modify device parameters, as shwon in Figure 6-16.

Figure 6-16 Modify device parameter



Modify device parameters

Device Name: Channel07

IP Address: 192.168.1.77

Protocol: Private_SSL

Port: 20001

Username: admin

Password: *****

Remote Channel: CH-1

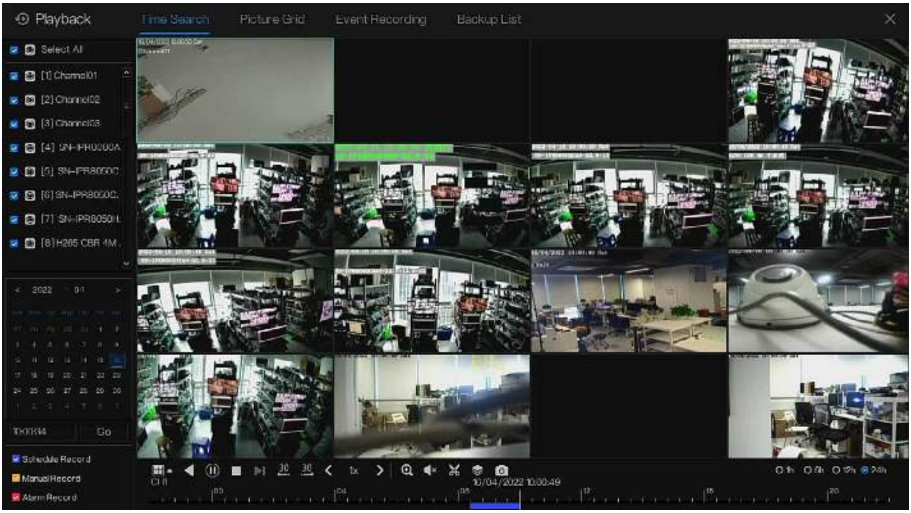
: snapshot panorama (the USB drive is plugged into the DVR).

6.3 Playback

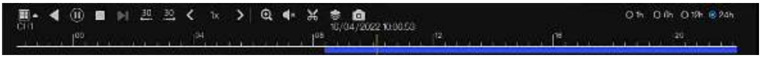
Playback refers to playing back a video.

Click in the quick navigation bar to access the playback screen, as shown in Figure 6-17.

Figure 6-17 Playback screen



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



▦▲: Layout.

◀ ⏸ ■: Reversed, pause/play, stop.

30 30:30s backward, 30s farward.

❮ 1x ❯:Triple speed, it supports up to 32x to playback.

🔍: Zoom.

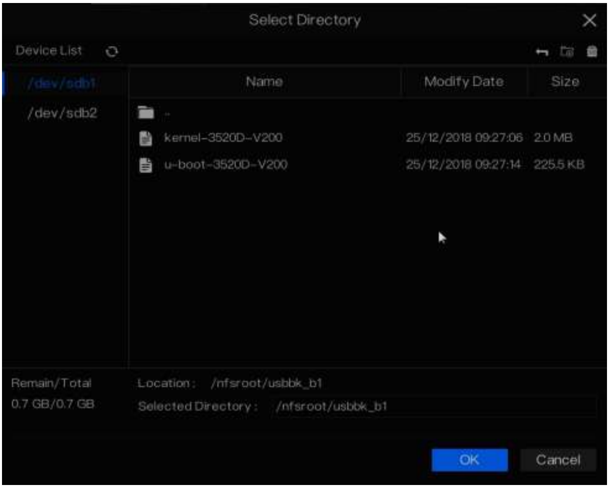
🔇: Audio.

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

The backup type shows, click **Save**, then saving the file pop-up windows would show as Figure 6-18 . Click **OK** to save.

This function is available after a USB disk is plugging in the device.

Figure 6-18 Select directory



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

Remain/Total
0.7 GB/0.7 GB

Location: /nfsroot/usbbk_b1

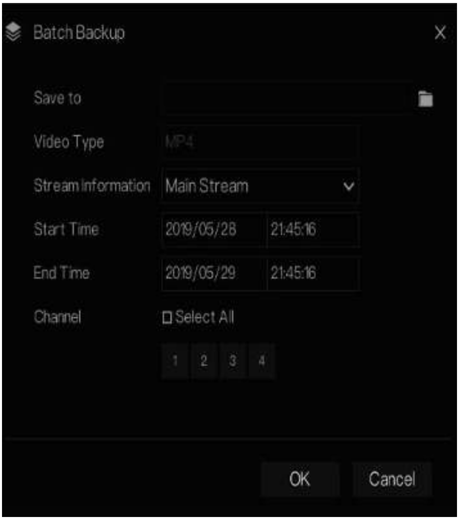
Selected Directory: /nfsroot/usbbk_b1

: Batch backup, click the icon to backup multi-channels, as shown in Figure 6-19.

Choose the folder to save, select the stream information from drop-down list, set the start time and end time, select the channels, Click **OK** to backup.

: Get a snapshot of the playback video's panorama if the USB disk is plugged in the DVR.

Figure 6-19 Batch backup



Batch Backup

Save to:

Video Type: MP4

Stream Information: Main Stream

Start Time: 2019/05/28 21:45:16

End Time: 2019/05/29 21:45:16

Channel: □ Select All

1 2 3 4

OK Cancel

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

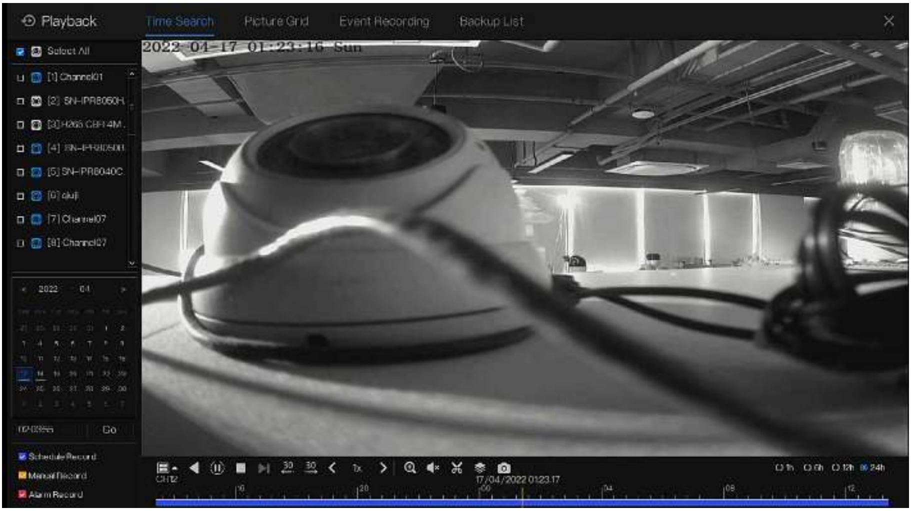
6.3.1 Time Search

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 6-20.

Figure 6-20 Time Search screen



Operation Steps

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

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

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

Step 4 Choose proper button to adjust video.

----End

6.3.2 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 6-21.

Figure 6-21 Picture grid screen

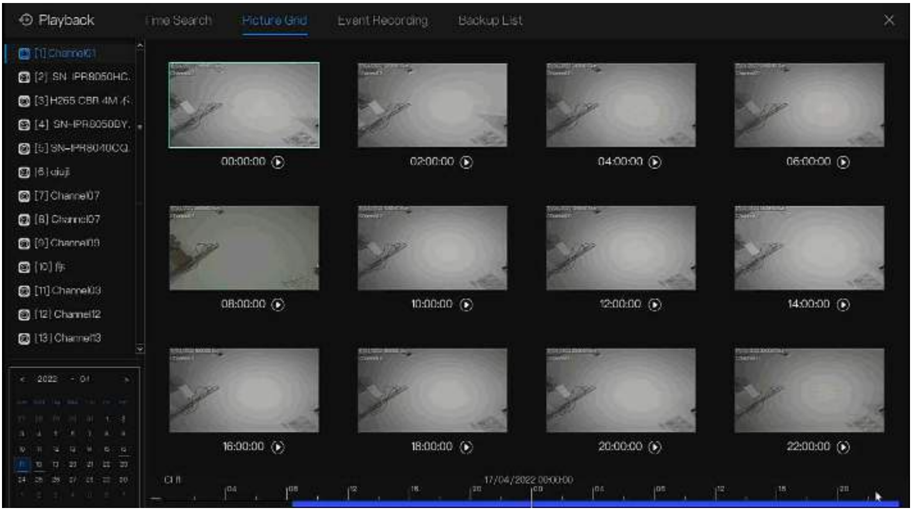
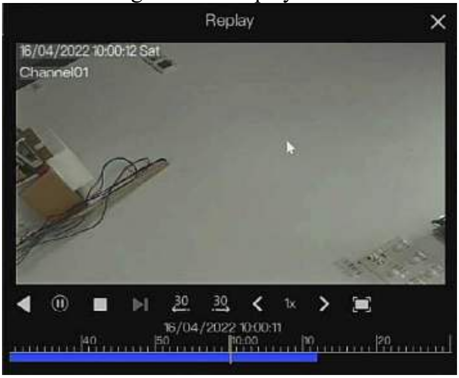


Figure 6-22 Replay



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 day from calendar.

Step 3 One day dividends for 12 grids, two hours for one grid.

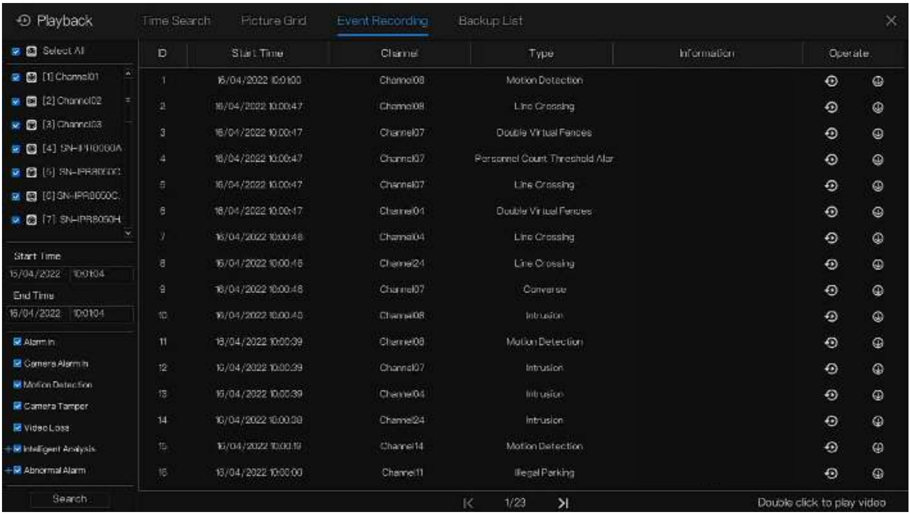
Step 4 Select a required thumbnail, double-click it or right-click it and choose Play from the shortcut menu to play the video.

----End

6.3.3 Event Recording

Click on the quick navigation bar; choose **Event Recording** at title to access the alarm event screen, as shown in Figure 6-23.

Figure 6-23 Event screen



- ☑ Select All
- ☑ [1] Channel01
- ☑ [2] Channel02
- ☑ [3] Channel03
- ☑ [4] SN-IPH8000A
- ☑ [5] SN-IPR8000C
- ☑ [6] SN-IPR8050C
- ☑ [7] SN-IPR8050H

Start Time
15/04/2022 10:01:04

End Time
16/04/2022 10:01:04

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

Search

ID	Start Time	Channel	Type	Information	Operate
1	16/04/2022 10:01:00	Channel08	Motion Detection		
2	16/04/2022 10:00:47	Channel08	Line Crossing		
3	16/04/2022 10:00:47	Channel07	Double Virtual Fences		
4	16/04/2022 10:00:47	Channel07	Personnel Count Threshold Alar		
5	16/04/2022 10:00:47	Channel07	Line Crossing		
6	16/04/2022 10:00:47	Channel04	Double Virtual Fences		
7	16/04/2022 10:00:48	Channel04	Line Crossing		
8	16/04/2022 10:00:46	Channel24	Line Crossing		
9	16/04/2022 10:00:48	Channel07	Converse		
10	16/04/2022 10:00:40	Channel08	Intrusion		
11	16/04/2022 10:00:39	Channel08	Motion Detection		
12	16/04/2022 10:00:39	Channel07	Intrusion		
13	16/04/2022 10:00:39	Channel04	Intrusion		
14	16/04/2022 10:00:38	Channel24	Intrusion		
15	16/04/2022 10:00:19	Channel14	Motion Detection		
16	16/04/2022 10:00:00	Channel11	Illegal Parking		

1/23

Double click to play video

Operation Steps

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

Step 2 Set start and end time.

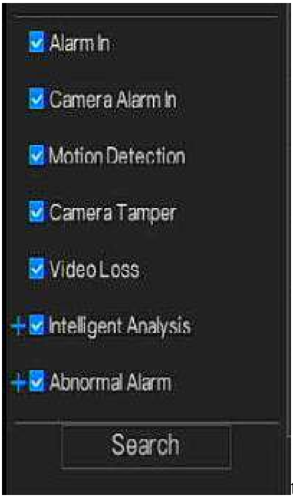
Step 3 Tick the alarm type, such as alarm in, motion alarm, block alarm, video loss and intelligent analysis.

Step 4 Click Search to query the event, the result would show at window.

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

: Play the recording video.

: Backup the recording video.



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

Search

the type of intelligent analysis and abnormal alarm are subdivided, Users can tick the detail alarm to show.

Intelligent analysis includes perimeter, single virtual fence, double virtual fences, loiter, multi loiter, object left, object removed, abnormal speed, converse, illegal parking, signal bad, register, stranger, registered license plate, over temperature, low temperature, abnormal temperature, threshold warning, threshold alarm, temperature difference warning, temperature difference alarm, temperature section alarm, face temperature, wear mask, no mask, personnel count threshold alarm, personnel count threshold alarm(IPC) .

Abnormal alarm includes disk error, IP conflict, network disconnected.

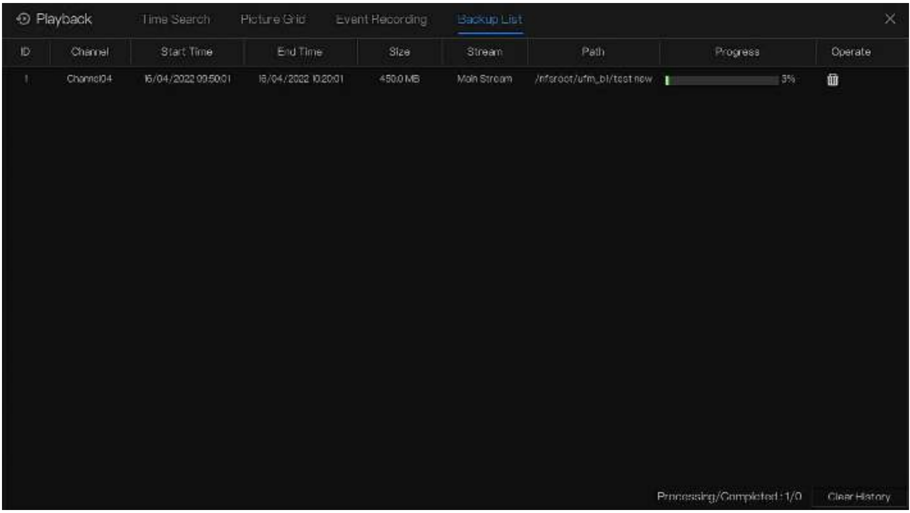
Users can choose the accurate alarm events to search.

----End

6.3.4 Backup List

Click ⟲ on the quick navigation bar, choose Backup List at title to access the backup screen, as shown in Figure 6-6.

Figure 6-24 Backup list screen



ID	Channel	Start Time	End Time	Size	Stream	Path	Progress	Operate
1	Channel04	16/04/2022 09:50:01	16/04/2022 10:20:01	450.0 MB	Main Stream	/nfsroot/ufm_bl/test.new	3%	🗑

Processing/Completed : 1/0

You can view the detail information of backup. Click delete button to quit the download.

----End

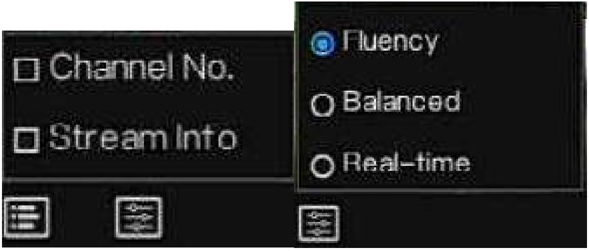
7 UI System Setting

7.1 Channel Information

Click the ☰ will show as Figure 7-1, tick the Channel or Encode, the information will show in live video screen.

Click ☰ to switch the live video strategy based on actual scene.

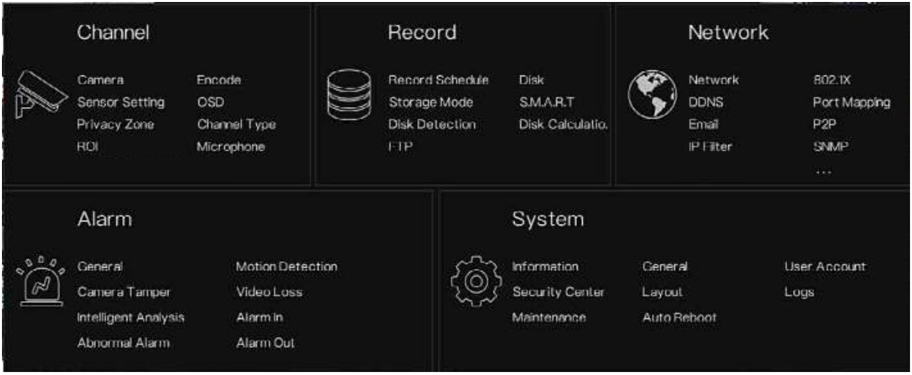
Figure 7-1 Channel information



7.2 Main Menu

Right-click on UI screen, the main menu as shown in Figure 7-2. The main menu includes **Channel**, **Record, Network, Alarm** and **System**.

Figure 7-2 DVR main menu



----End

7.3 Channel Management

Analog cameras can directly connect to input channels of the DVR by cables to connect. When analog cameras are insufficient, the DVR can automatically search for and adds IP cameras or manually add cameras in the same Local Area Network (LAN).

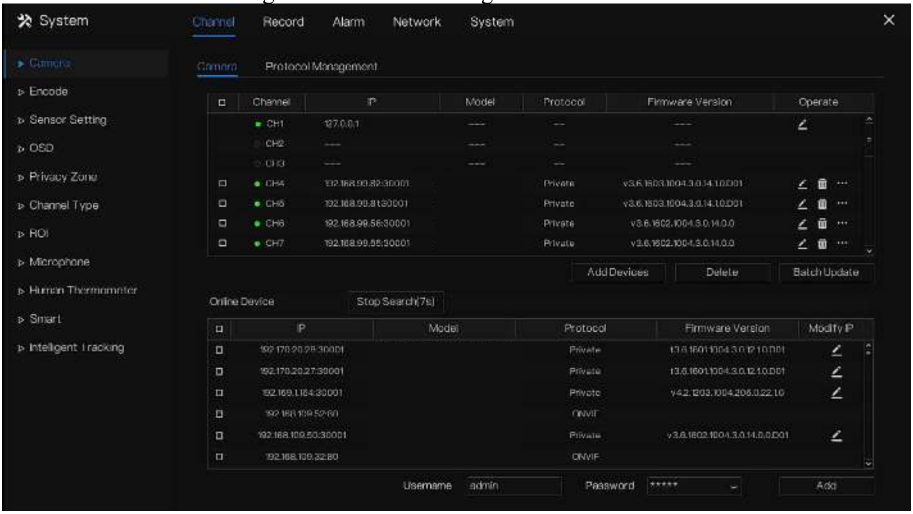
Channel management includes add or delete **Camera, Encode, Sensor Setting, OSD Privacy Zone**, **Channel Type, ROI, Microphone, Human Thermometer, Smart, Intelligent Tracking and so on.**

7.3.1 Camera

Operation Description

Click **Channel** in the main menu to access the camera management screen, as shown in Figure 7-3 .

Figure 7-3 Channel management screen



□	Channel	IP	Model	Protocol	Firmware Version	Operate
	● CH1	127.0.0.1	----	--	----	✎
	○ CH2	----	----	--	----	
	○ CH3	----	----	--	----	
□	● CH4	192.168.99.82:30001		Private	v3.6.1603.1004.3.0.14.10.D01	✎ 🗑 ···
□	● CH5	192.168.99.81:30001		Private	v3.6.1603.1004.3.0.14.10.D01	✎ 🗑 ···
□	● CH6	192.168.99.56:30001		Private	v3.6.1602.1004.3.0.14.0.0	✎ 🗑 ···
□	● CH7	192.168.99.55:30001		Private	v3.6.1602.1004.3.0.14.0.0	✎ 🗑 ···

□	IP	Model	Protocol	Firmware Version	Modify IP
□	192.170.20.28:30001		Private	t3.6.1601.1004.3.0.12.1.0.D01	✎
□	192.170.20.27:30001		Private	t3.6.1601.1004.3.0.12.1.0.D01	✎
□	192.169.1.184:30001		Private	v4.2.1203.1004.206.0.22.1.0	✎
□	192.168.109.52:80		ONVIF		
□	192.168.109.50:30001		Private	v3.6.1602.1004.3.0.14.0.0.D01	✎
□	192.168.109.32:80		ONVIF		

Username: admin
Password: *****

7.3.1.1 Add Camera Automatically

The DVR can add automatically cameras to the camera list.

Operation Methods

Method 1: Click Refresh button, the cameras that are on the same network as the DVR will show in list, input username and password (the default value both are admin), click Add Devices, the cameras in the list would be added to channels directly.

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

Tick the online non-onvif channels at list and click Batch Update to access the directory of software; it would to update the channels at once.

NOTE

On the camera management screen, check the status of channel 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 segment as DVR.

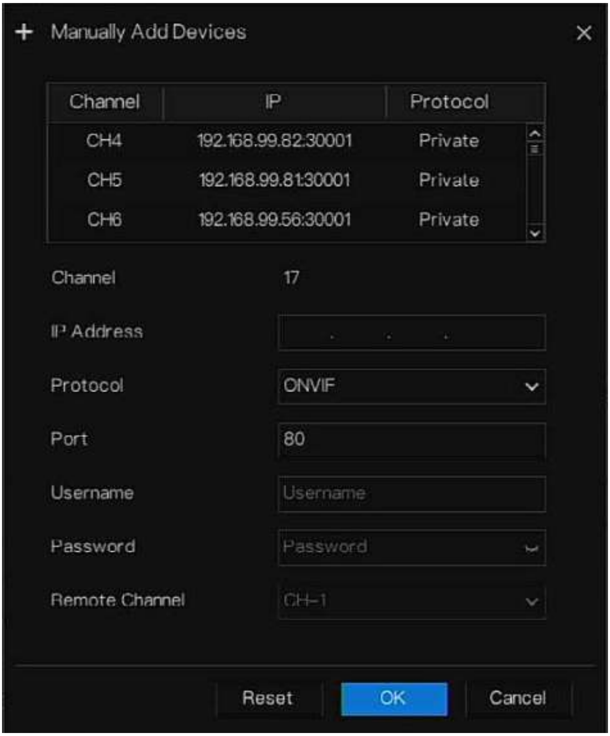
----End

7.3.1.2 Add Camera Manually

Operation Steps

Step 1 Click +, the screen to add devices manually is displayed, as shown in Figure 7-4.

Figure 7-4 Add camera screen



Channel	IP	Protocol
CH4	192.168.99.82:30001	Private
CH5	192.168.99.81:30001	Private
CH6	192.168.99.56:30001	Private

Channel 17

IP Address . . .

Protocol ONVIF

Port 80

Username Username

Password Password

Remote Channel CH-1

Step 2 Input IP address (click the on list, modify the IP to enter address quickly), port, user name and password of camera.

Step 3 Select a protocol from the drop-down list. Remote channel is only used for thermal imaging cameras.

Step 4 Click OK, the camera is added successfully.

NOTE

If all channels of the DVR are connected by cameras, please delete the cameras that you don't need, so that you can add more cameras.

If an IP camera is added manually, input the correct username and password of the camera below the online device list. The camera will be added successfully. If not, the camera will show on list at offline.

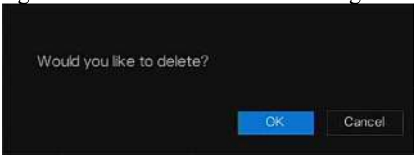
----End

7.3.1.3 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 7-5.

Figure 7-5 Delete confirmation message



Would you like to delete?

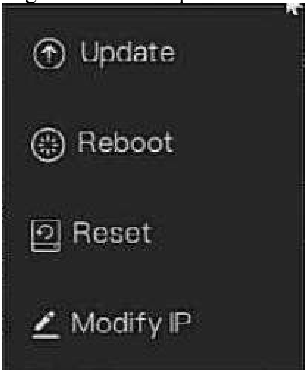
Step 2 Click OK, the camera is deleted successfully.

----End

7.3.1.4 Operate Camera

At camera list, click ••• to operate camera as shown in Figure 7-6, users can update, reboot and reset the camera immediately.

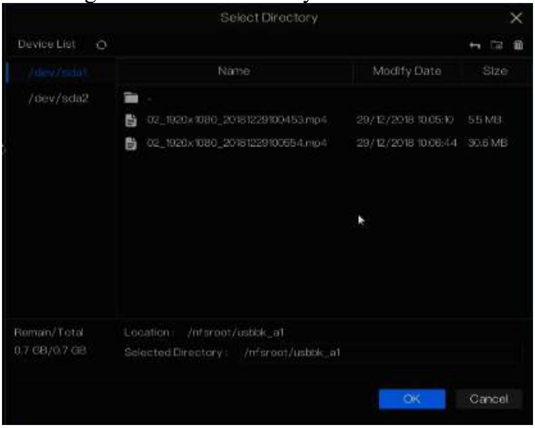
Figure 7-6 More operation



Step 1 Click **Update,** and select the software in pop-up window, as shown in Figure 7-7.

Step 2 Set the directory and click OK to update camera.

Figure 7-7 Select directory of software



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

Remain/Total
0.7 GB/0.7 GB

Location : /nfsroot/usbbk_a1

Selected Directory : /nfsroot/usbbk_a1

Step 3 Click **Reboot,** message “**Are you sure to reboot?** ” would show, click OK to reboot the camera.

Step 4 Click **Reset,** message “**Are you sure to reset?**” would show, users can enable the retain IP address function. Click OK to reset the camera.

Step 5 Tick the cameras with non-onvif protocol and cameras are online, click **Update** to update all cameras at once.

Step 6 The IP of online cameras can be modified, click **Modify IP** to modify as shown in following figure, input the new IP address and subnet mask.

NOTE

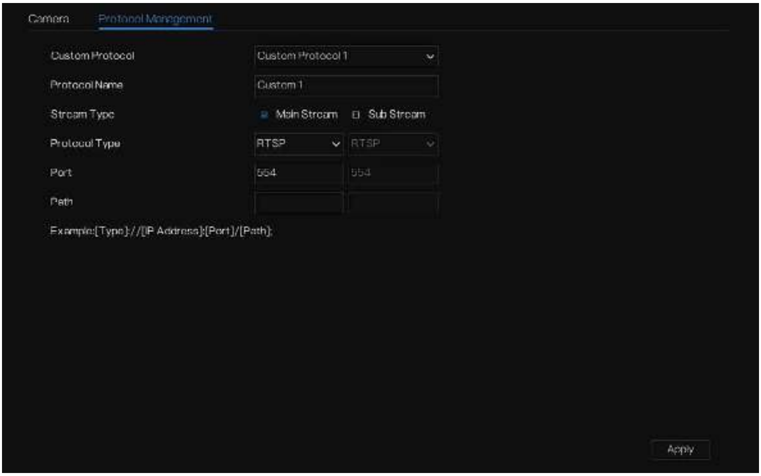
Update need upload the software by flash driver.

----End

7.3.1.5 Protocol Management

Set the protocol management, users can add different protocol cameras to DVR

Figure 7-8 Protocol management



Custom Protocol: Custom Protocol 1

Protocol Name: Custom 1

Stream Type: ☑ Main Stream ☐ Sub Stream

Protocol Type: RTSP | RTSP

Port: 554 | 554

Path:

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

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

Step 2 Choose the custom protocol from the drop-down list, there are 16 kinds of protocols can be set.

Step 3 Input the protocol name.

Step 4 Tick main stream and sub stream. The main stream shows image on full screen live video. The sub stream shows image on split screen. If you just tick main stream and the channel will not show image on split screen.

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

Step 6 Input the port, it depends on the IP camera.

Step 7 Input the path, it depends on the manufacturer of cameras.

Step 8 Click Apply to save the settings

----End

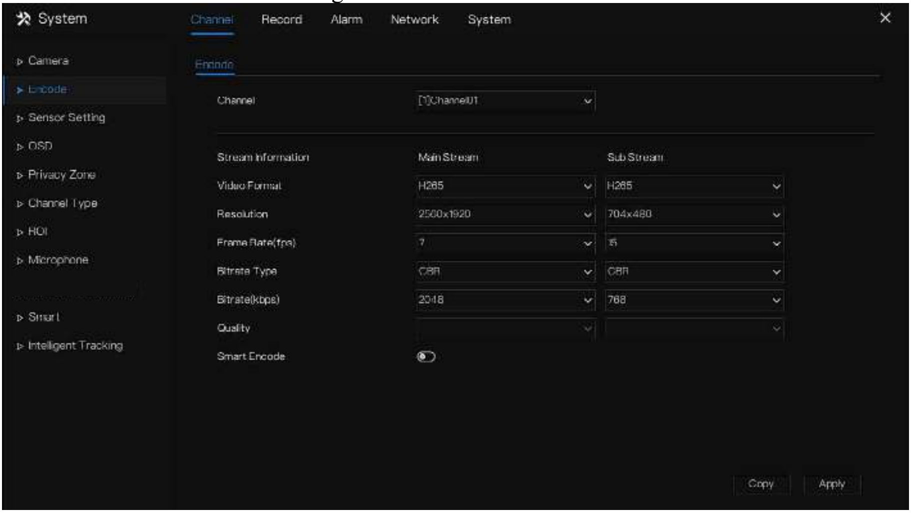
7.3.2 Encode Parameter

The system allows setting the stream information, encoding type, resolution, frame rate, bitrate control, bitrate and quality for cameras in a channel in **Encode Parameter** screen.

Operation Description

Click **Encode** in the main menu or **Menu** of the channel management screen and choose **Encode** to access the **Encode** screen, as shown in Figure 7-9.

Figure 7-9 Encode screen



Channel: [1]Channel01

Stream Information	Main Stream	Sub Stream
Video Format	H265	H265
Resolution	2560x1920	704x480
Frame Rate(fps)	7	15
Bitrate Type	CBR	CBR
Bitrate(kbps)	2048	768
Quality		
Smart Encode	○	

Operation Steps

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

Step 2 Set video format, audio encode type, resolution, frame rate, bitrate type, bitrate size and quality (for VBR) 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, click Apply to save encode parameter settings.

----End

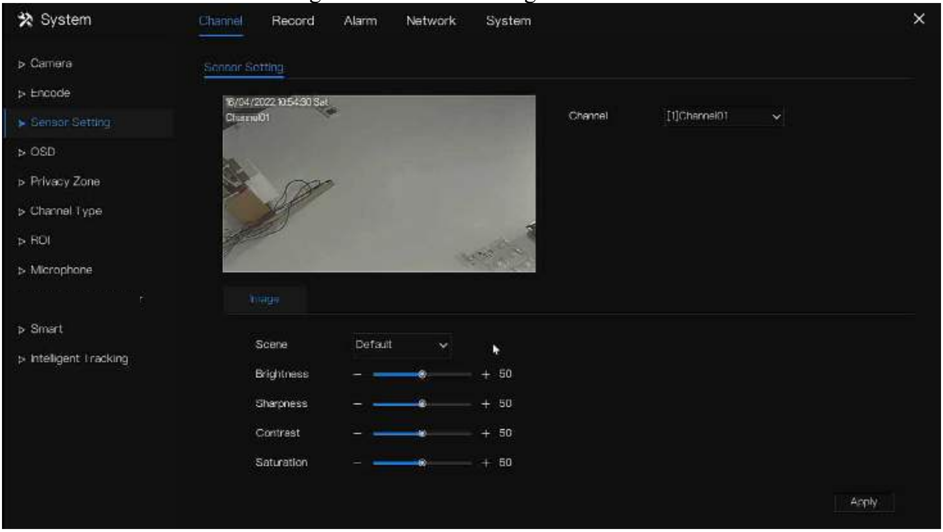
7.3.3 Sensor Setting

Sensor setting refer to basic attributes of pictures, it includes brightness, sharpness, contrast and saturation. You can set picture parameters for each channel based on scene.

Operation Description

Click **Sensor Setting** in the main menu or click menu of the channel management screen and choose **Sensor Setting** to access the Sensor Setting screen, as shown in Figure 7-10.

Figure 7-10 Sensor setting screen



Channel [1]Channel01

Scene Default

Brightness 50

Sharpness 50

Contrast 50

Saturation 50

The Sensor Setting is as follows:

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

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

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

NOTE

The analog cameras can only adjust the image parameters.

Operation Steps

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

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

Step 3 Set parameters.

Step 4 Click Default to reset to factory settings, click Apply to save image settings.

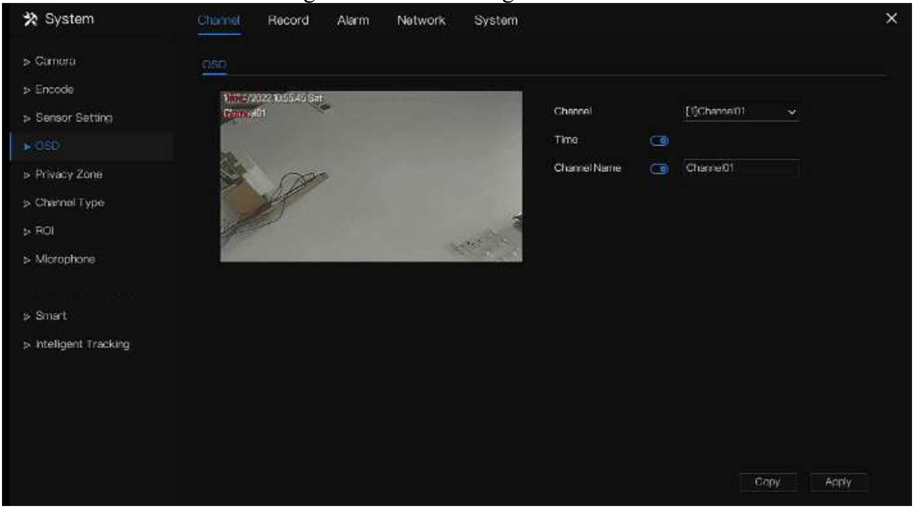
----End

[redacted]

7.3.4 OSD Settings

Click **OSD** in the main menu or menu of the channel management screen and choose **OSD** to access the OSD screen, as shown in Figure 7-11.

Figure 7-11 OSD setting screen



Channel [1]Channel01

Time ○

Channel Name ○ Channel01

Operation Steps

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

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

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

Step 4 Set the channel name.

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

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

----End

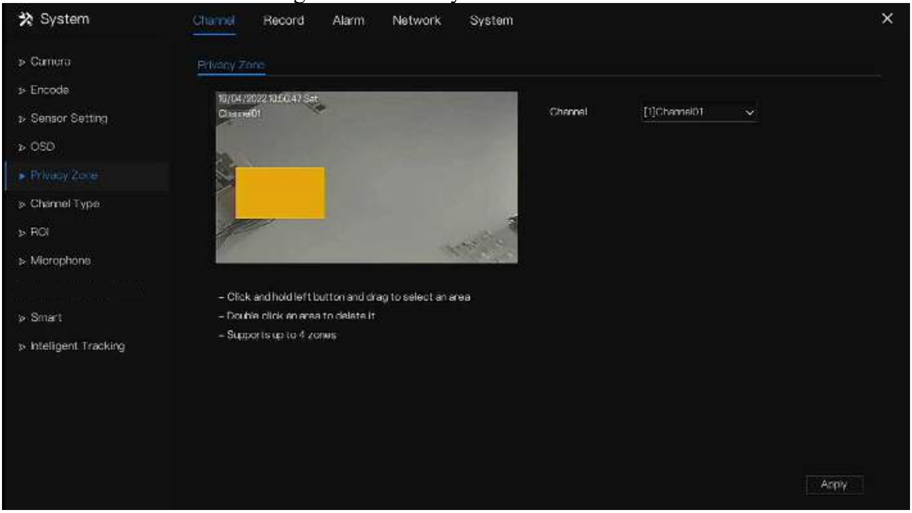
7.3.5 Privacy Zone

The system allows you to mask images in a specified zone and this zone is called privacy zone.

Operation Description

Click **Privacy Zone** in the main menu or menu of the channel management screen and choose privacy zone to access the **Privacy Zone** screen, as shown in Figure 7-12.

Figure 7-12 Privacy zone screen



Channel [1]Channel01

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

Operation Steps

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

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

Step 3 Click Apply to save privacy settings.

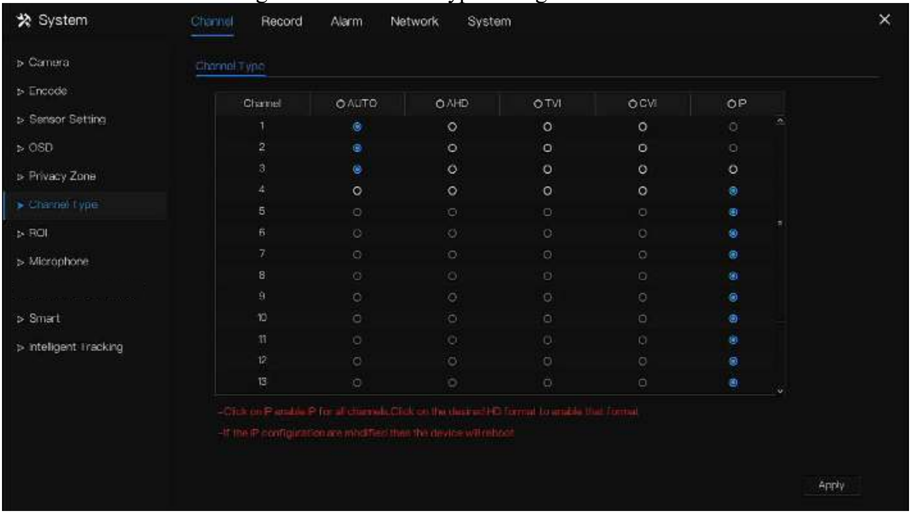
Step 4 Double click privacy area to delete setting.

----End

7.3.6 Channel Type

Click **Channel Type** in the main menu or menu of the channel management screen and choose **Channel Type** to access the Channel Type screen, as shown in Figure 7-13.

Figure 7-13 Channel Type setting screen



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

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

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

Operation Steps

Step 1 Choose channel to set channel type.

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

NOTE

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

If the IP configuration are modified the device will reboot.

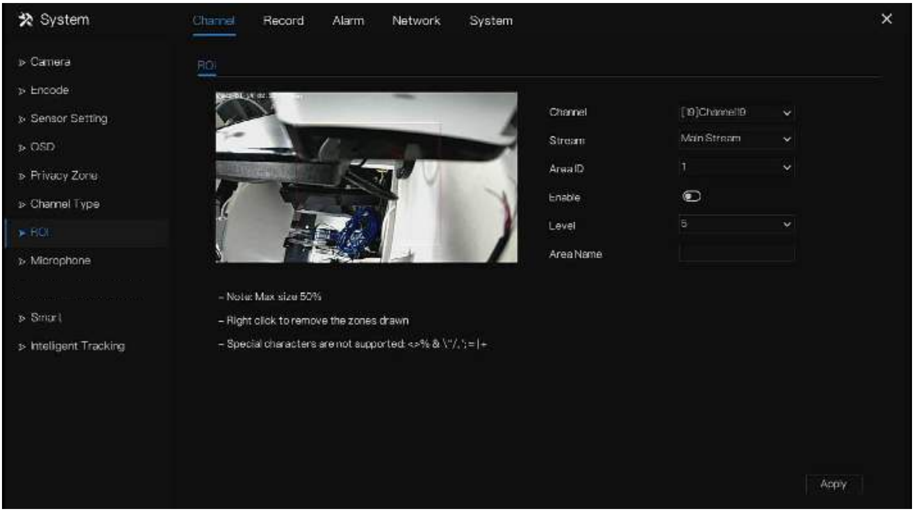
7.3.7 ROI

NOTE

This function can only be used for IP cameras.

Click **ROI** in the main menu or menu of the channel management screen and choose **ROI** to access the ROI screen, as shown in Figure 7-14.

Figure 7-14 ROI



Channel [19]Channel19

Stream Main Stream

Area ID 1

Enable

Level 5

Area Name

- Note: Max size 50%
- Right click to remove the zones drawn
- Special characters are not supported: <>% & \"/,';=|+

Table 7-1 RIO parameter

Parameter	Description	Setting
Stream	Stream ID.	[Setting method] Select a value from the drop-down list box. [Default value] Stream 1
Enable	Enable the ROI	[Setting method] Click the button. [Default value] OFF
Area ID	ROI area ID, there are 8 areas.	[Setting method] Select a value from the drop-down list box. [Default value] 1

Parameter	Description	Setting
Level	Visual effect of ROI. The higher the grade is, the clearer areas inside and the vaguer areas outside are. There are five levels.	[Setting method] Select a value from the drop-down list box. [Default value] 5
Area Name	The marked name used for areas.	[Setting method] Enter a value manually. The value cannot exceed 32 bytes.

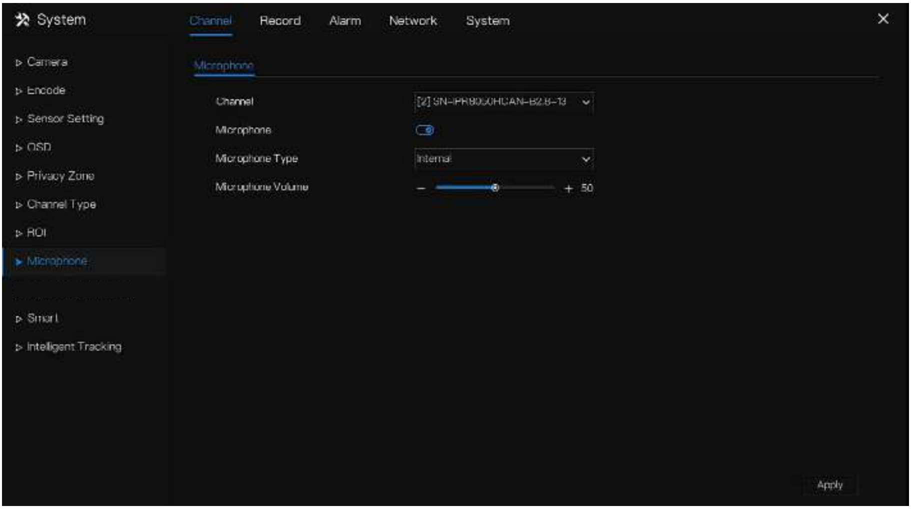
7.3.8 Microphone

NOTE

This function can only be used for IP cameras with microphone or the external microphone.

Click **Microphone** in the main menu or menu of the channel management screen and choose **Microphone** to access the Microphone screen, as shown in Figure 7-15.

Figure 7-15 Microphone



Channel [2] SN-IPR8050HCAN-B2.8-13

Microphone

Microphone Type Internal

Microphone Volume − + 50

Table 7-2 Microphone

Parameter	Description	Setting
Enable Microphone	Indicates whether to enable the microphone function.	[Setting method] Click the button on to enable microphone.
Microphone Type	Microphone types include: ● Line In, an active audio input is required. ● Internal, the cameras are with microphone.	[Setting method] Select a value from the drop-down list box.
Microphone Volume	Allows you to adjust the microphone volume.	[Setting method] Slide the slider left or right. [Default value] 50 NOTE The value ranges from 0 to 100.

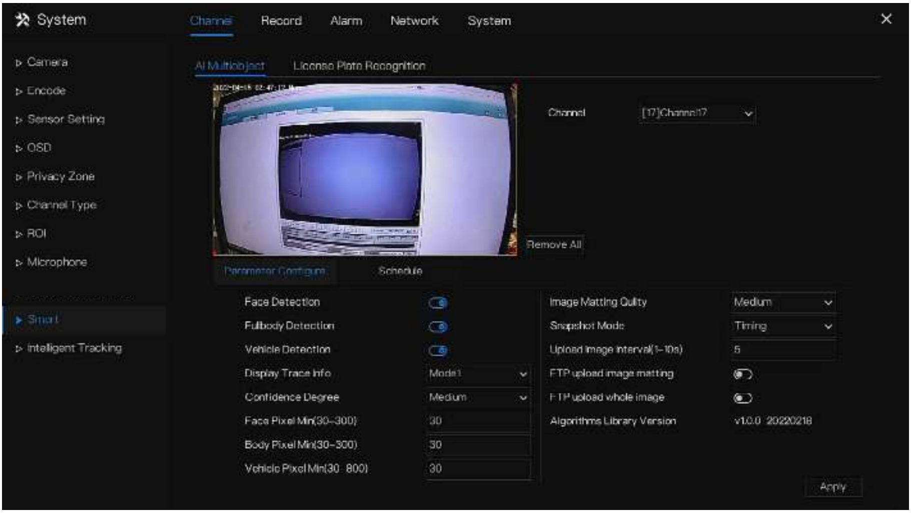
7.3.9 Smart

NOTE

The comparison function is only for AI multiobject cameras, please refer to actual cameras.

7.3.9.1 AI Multiobject

Figure 7-16 AI multiobject



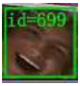
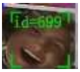
Channel [17]Channel17

Face Detection: on
Fulbody Detection: on
Vehicle Detection: on
Display Trace Info: Mode1
Confidence Degree: Medium
Face Pixel Min(30~300): 30
Body Pixel Min(30~300): 30
Vehicle Pixel Min(30~800): 30

Image Matting Qulity: Medium
Snapshot Mode: Timing
Upload Image interval(1~10s): 5
FTP upload image matting: off
FTP upload whole image: off
Algorithms Library Version: v1.0.0 20220218

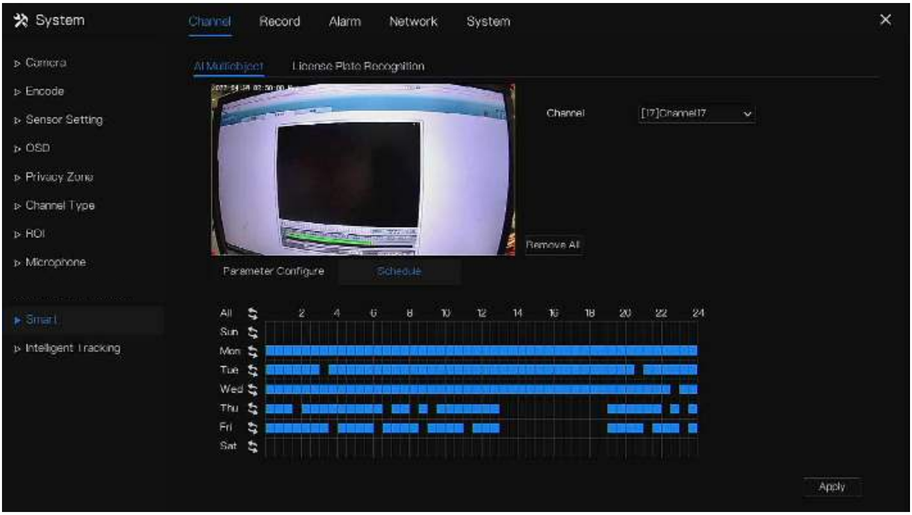
Table 7-3 AI multiobject

Parameter	Description	How to set
Face detection	The camera will capture the face when someone appears in live video.	Enable
Full body detection	The camera will capture the whole body when someone appears in live video.	Enable
Vehicle detection	The camera will capture the licence when the vehicle appears in live video.	Enable

Parameter	Description	How to set
Display trace info	Enable the function and a trace frame will show at live video. Mode 1:  Mode 2: 	Choose from drop list.
Show detection area	Enable to set a detection area, and the frame will show at live video	Enable
Confidence coefficient	The range of snap image, there are three type, such as high, mid and low. The higher the confidence, the better the snap quality and the fewer snapshots.	Choose from drop list.
Face pixel min(30-300)	30-300 pixels, the smaller the pixel be set, the more faces will be captured, but it may be mistaken.	Input a value ranges 30 to 300
Body pixel min(30-300)	30-300 pixels, the smaller the pixel be set, the more bodies will be captured, but it may be wrong.	Input a value range 30 to 300
Plate pixel min(30-300)	30-300 pixels, the smaller the pixel be set, the more face will be captured, but it may be mistaken.	Input a value range 30 to 300
Vehicle pixel min(30-300)	30-300 pixels, the smaller the pixel be set, the more license plates will be captured, but it may be wrong.	Input a value ranges 30 to 300
Image matting quality	The quality of snap image, There are three mode can be chosen, such as low, mid and high.	Choose from drop list.
Attribute	Click to enable, the screenshot can display the	Enable

Parameter	Description	How to set
	relevant basic information of the vehicle. Such as the age of people, gender, etc. The color, model of the car.	
Snapshot mode	There are two modes can be chosen, such as timing, and optimal.	Choose from drop list.
Upload image interval(1-10 s)	At timing mode, set the interval of upload image.	Input a value ranges 1 to 10
FTP upload image matting	**Configuration > Network Service > FTP**, set FTP related parameters, the captured picture will be sent to the set FTP location	Enable
FTP upload whole image	Capture a picture and send a whole image.	Enable

Figure 7-17 Schedule


Channel: [17]Channel17

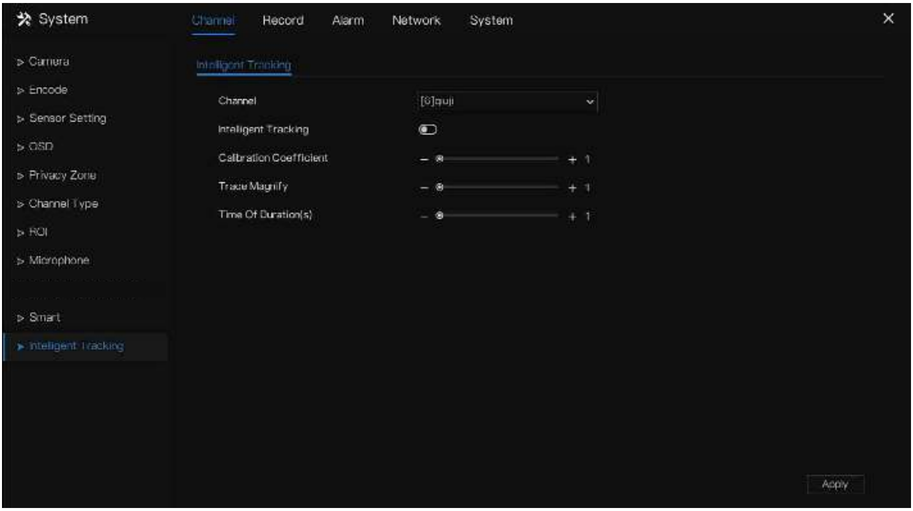
7.3.10 Intelligent Tracking (Only for Some Model)

NOTE

This function can only be used for high speed PTZ cameras.

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

Figure 7-18 Intelligent tracking



Channel [6]quji

Intelligent Tracking

Calibration Coefficient – + 1

Trace Magnify – + 1

Time Of Duration(s) – + 1

Table 7-4 Intelligent tracking parameters

Parameter	Description	Setting
Enable	Enable the button to enable the 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, it ranges from 0 to 300 s.	[Setting method] Drag the slider. [Default value] **120**

7.4 Record Setting

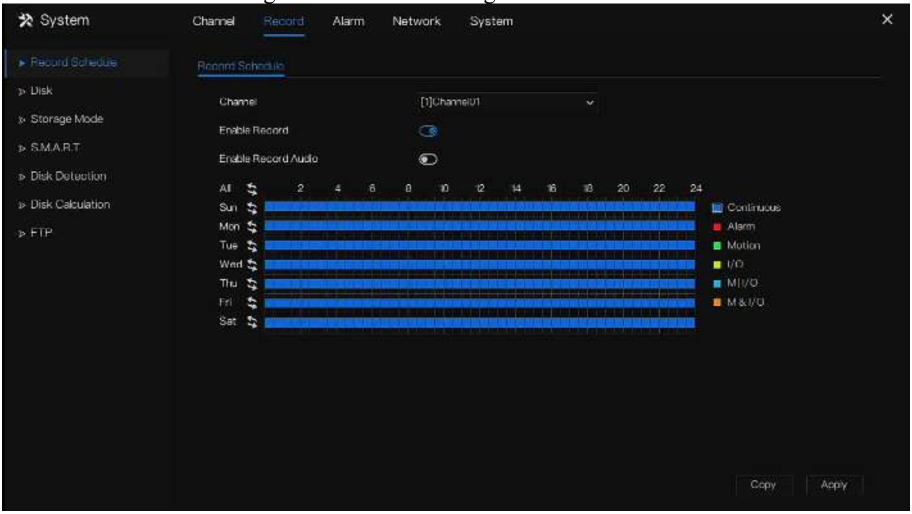
Set the **Record Schedule**, **Disk, Storage Mode, S.M.A.R.T, Disk Detection, Disk Calculation,** and **FTP**.

7.4.1 Record Schedule

Operation Description

Click **Record** in the main menu or click the record page of any function screen in the main menu to access the record schedule screen, as shown in Figure 7-19.

Figure 7-19 Record management screen



Channel [1]Channel01

Enable Record

Enable Record Audio

Operation Steps

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

Step 2 Enable the record.

Step 3 Enable the record audio.

Step 4 Set the record schedule. The different alarm schedules are showing different colors, but for recording video only three colors show alarm information.

Method 1: Hold down the left mouse button, drag and release mouse to select the arming time within 00:00-24:00 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 schedule is **All**.
- Users can choose one alarm type to record, if the chosen alarm is happening at the setting time, it will record. So that it will using the disk effectively to avoid repeating useless recording.
- Users can set different alarms to record.

Method 2: Click ⇆ in the record schedule page to select whole day or whole week.

Step 5 Deleting record schedule: Click ⇆ again or inverse selection to delete the selected record schedule.

Step 6 Click Copy and select channels or tick **all**, then click OK to apply the record management settings to selected channels , click Apply to save settings.

----End

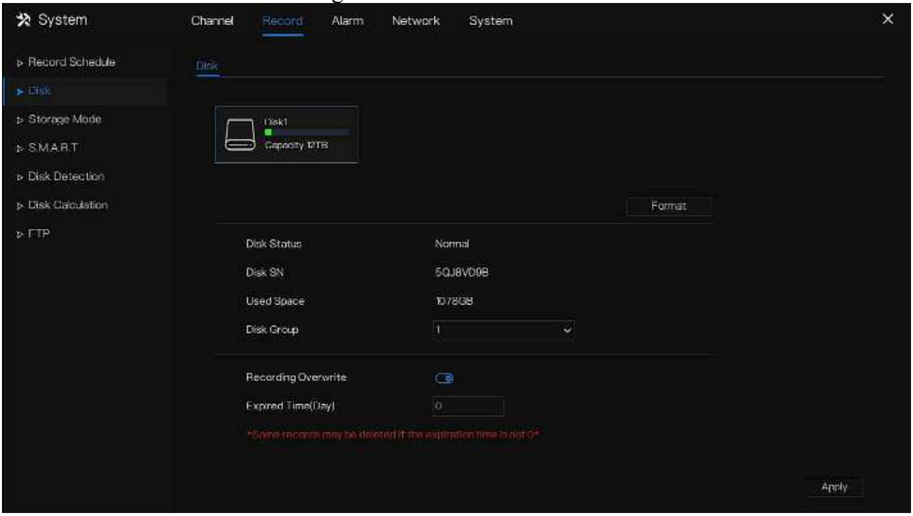
7.4.2 Disk

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

Operation Description

Step 1 Click **Record** in the main menu or menu of the record screen and choose **Disk** to access the disk screen, as shown in Figure 7-20.

Figure 7-20 Disk screen



Disk Status Normal

Disk SN 5QJ8VD9B

Used Space 1078GB

Disk Group 1

Recording Overwrite

Expired Time(Day) 0

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

Step 2 Click **Format**. The message “Are you sure to format disk? Your data will be lost” is displaying.

Step 3 Choose the disk group, there are four groups.

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

Step 5 Enable recording overwrite, the disk will be overwrite automatically.

Step 6 Record expiration setting. Select record expiration days from the drop-down list of record expiration. 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.

----End

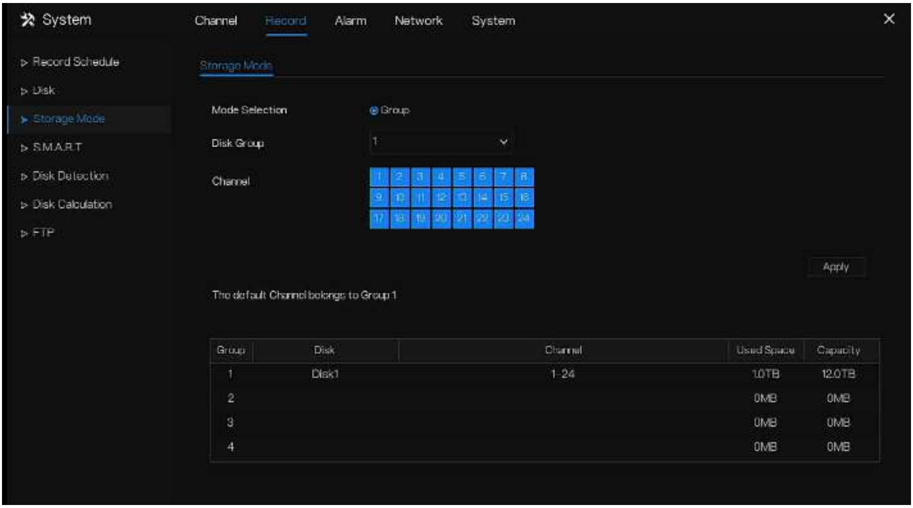
7.4.3 Storage Mode

NOTE

Group is used for multiple disks models, if you want to manage disk quickly and easily, grouping accords to actual application scenarios.

User is based on need to distribute the channels to different disk group, and use disk capacity reasonably, as shown in Figure 7-21.

Figure 7-21 Storage mode



Mode Selection ● Group

Disk Group 1

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

The default Channel belongs to Group 1

Group	Disk	Channel	Used Space	Capacity
1	Disk1	1-24	1.0TB	12.0TB
2			0MB	0MB
3			0MB	0MB
4			0MB	0MB

Operation Steps

Step 1 Choose the disk group.

Step 2 Select the channel recorded to the disk group.

Step 3 Click **Apply** to save the settings.

Step 4 The group list will show the detail information.

NOTE

If the channels are not in list, it means DVR will not to record these channels, please make sure about all channels are in list.

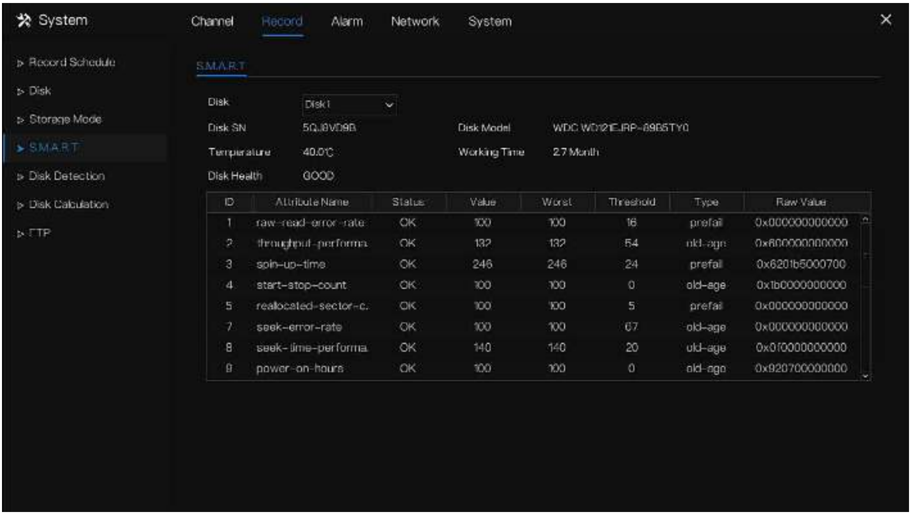
Choose number of channel number you should consider the capacity of disk group.

----End

7.4.4 S.M.A.R.T

S.M.A.R.T is Self-Monitoring Analysis and Reporting Technology, users can view the health of disk, as shown in Figure 7-22.

Figure 7-22 S.M.A.R.T



Disk	Disk1
Disk SN	5QJ8VD9B
Disk Model	WDC WD121EJRP-89B5TY0
Temperature	40.0℃
Working Time	2.7 Month
Disk Health	GOOD

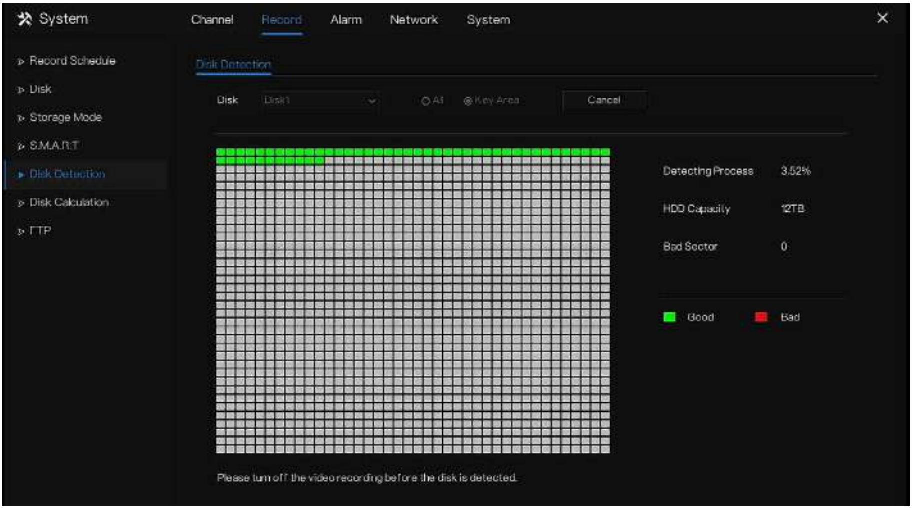
ID	Attribute Name	Status	Value	Worst	Threshold	Type	Raw Value
1	raw-read-error-rate	OK	100	100	16	prefail	0x000000000000
2	throughput-performa	OK	132	132	54	old-age	0x600000000000
3	spin-up-time	OK	246	246	24	prefail	0x6201b5000700
4	start-stop-count	OK	100	100	0	old-age	0x1b0000000000
5	reallocated-sector-c.	OK	100	100	5	prefail	0x000000000000
7	seek-error-rate	OK	100	100	67	old-age	0x000000000000
8	seek-time-performa	OK	140	140	20	old-age	0x0f0000000000
9	power-on-hours	OK	100	100	0	old-age	0x920700000000

----End

7.4.5 Disk Detection

Before recording the video, users need to detect the disk to keep the data safety, as shown in Figure 7-23.

Figure 7-23 Disk Detection



Disk: Disk1

○ All ● Key Area

Detecting Process 3.52%

HDD Capacity 12TB

Bad Sector 0

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

Operation Steps

Step 1 Choose the disk from the drop-down list.

Step 2 Tick all or key to detect the disk. Detecting all need some time, and detecting key section maybe need a few minutes.

Step 3 Click **Scan** to scan the disk.

Step 4 Click **Cancel** to quit scanning, the pop-up window shows "Would you like to stop disk detection?", click **OK** to quit.

Step 5 The disk analysis will show on this page.

NOTE

The green block means good, the red block means bad, if the red blocks are too much or at key section, please change the disk immediately

Please turn off the video recording before the disk is detected, otherwise the recording of video maybe lost.

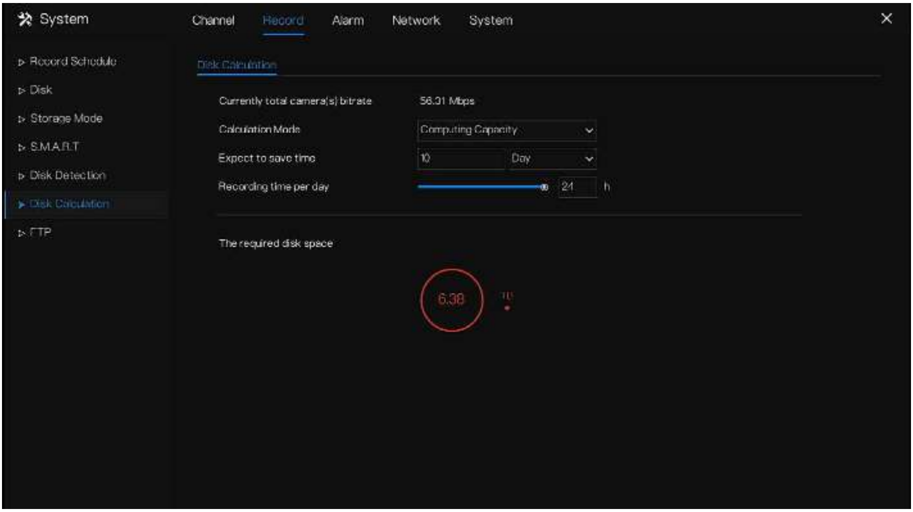
----End

7.4.6 Disk Calculation

Users can calculate the usage of disk, so that he can set the storage strategy reasonably, as shown in Figure 7-24.

There are two modes can be set, computing capacity and computing time

Figure 7-24 Disk calculation of capacity



Currently total camera(s) bitrate 56.31 Mbps

Calculation Mode Computing Capacity

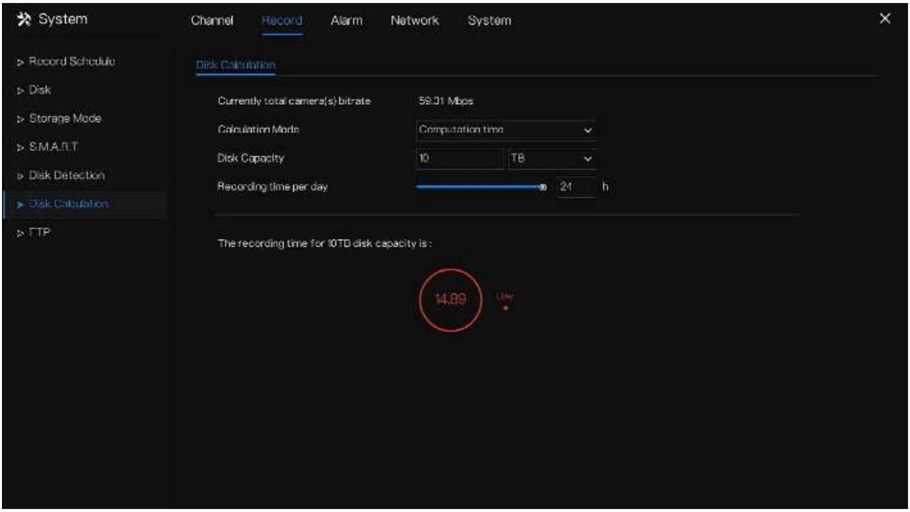
Expect to save time 10 Day

Recording time per day 24 h

The required disk space

6.38 TB

Figure 7-25 Disk calculation of time



Currently total camera(s) bitrate 59.31 Mbps

Calculation Mode Computation time

Disk Capacity 10 TB

Recording time per day 24 h

The recording time for 10TB disk capacity is :

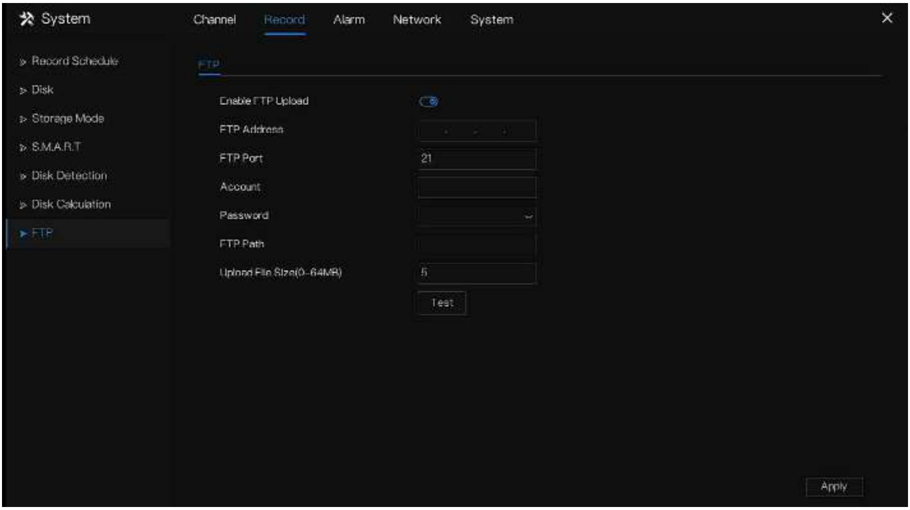
14.89 Day

----End

7.4.7 FTP

Enable FTP upload, when the alarm is happens, users can linkage the **FTP upload** to save the alarm recordings.

Figure 7-26 FTP



Enable FTP Upload
FTP Address
FTP Port: 21
Account
Password
FTP Path
Upload File Size(0-64MB): 5

Step 1 Enable the FTP upload.

Step 2 Input the FTP address and port.

Step 3 Input the account, password and FTP path.

Step 4 Set the upload file size, it ranges from 0 to 64 MB.

Step 5 Click "**Test**" to test the parameters, if test successfully, click "**Apply**" to save the settings.

----End

7.5 Alarm Management

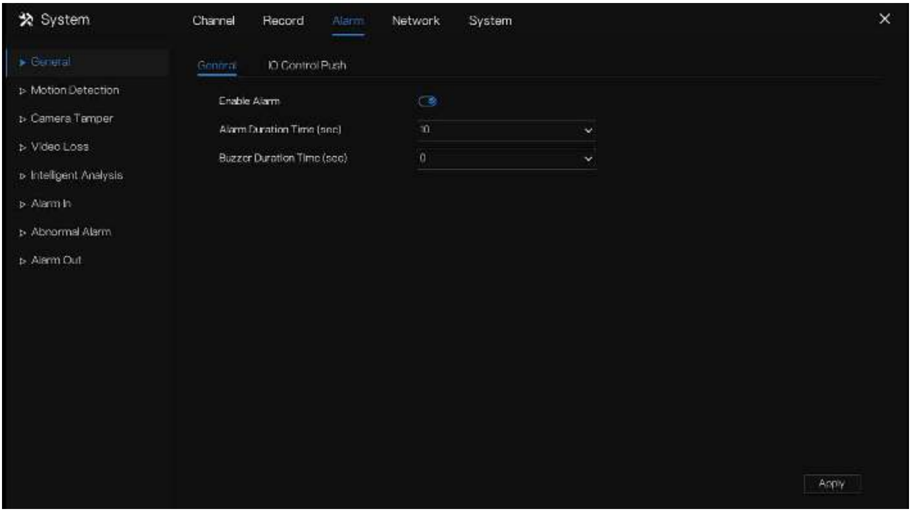
Set the **General alarm information, Motion Detection, Camera Tamper, Video Loss, Intelligent Analysis, Alarm In, Abnormal Alarm** and **Alarm Out** in alarm management screen.

7.5.1 General

7.5.1.1 General

Step 1 Click **Alarm** in the main menu (or click the alarm page of any function screen in the main menu) to access the alarm management screen, as shown in Figure 7-27.

Figure 7-27 Alarm management screen



Enable Alarm ●
Alarm Duration Time (sec) 10
Buzzer Duration Time (sec) 0

Step 2 Enable the Enable alarm button.

Step 3 Select a value from the drop-down list of duration time.

Step 4 Click Apply to save alarm settings.

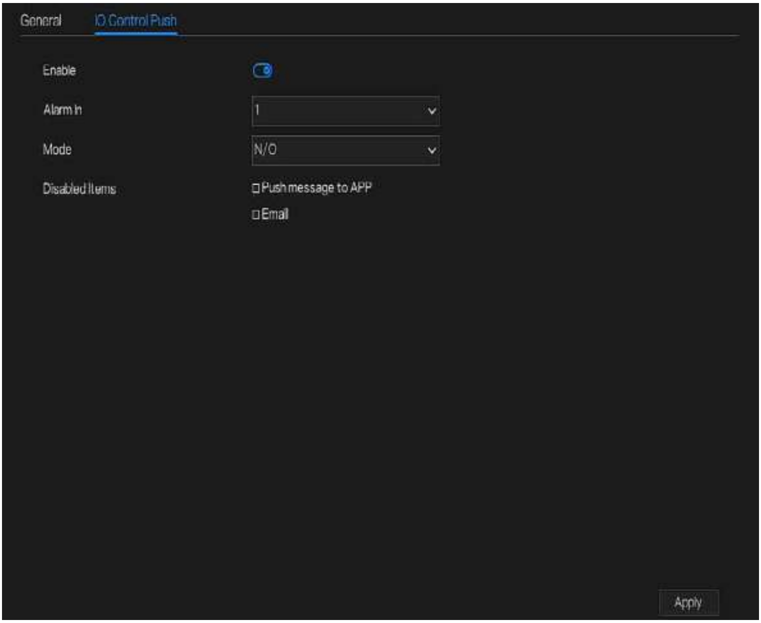
----End

7.5.1.2 IO control push

If you select normally open and tick the disabled items, alarm input 1 will not push the message when it is normally open. Only when the alarm in 1 is in the normally closed, it can push an alarm message.

Step 1 Enable the IO control push, as shown in Figure 7-28.

Figure 7-28 IO control push interface



Enable ●

Alarm In 1

Mode N/O

Disabled Items □Push message to APP
□Email

Step 2 Choose one alarm in and mode(N/C, N/O).

Step 3 Tick the disable items, click “Apply” to save settings.

----End

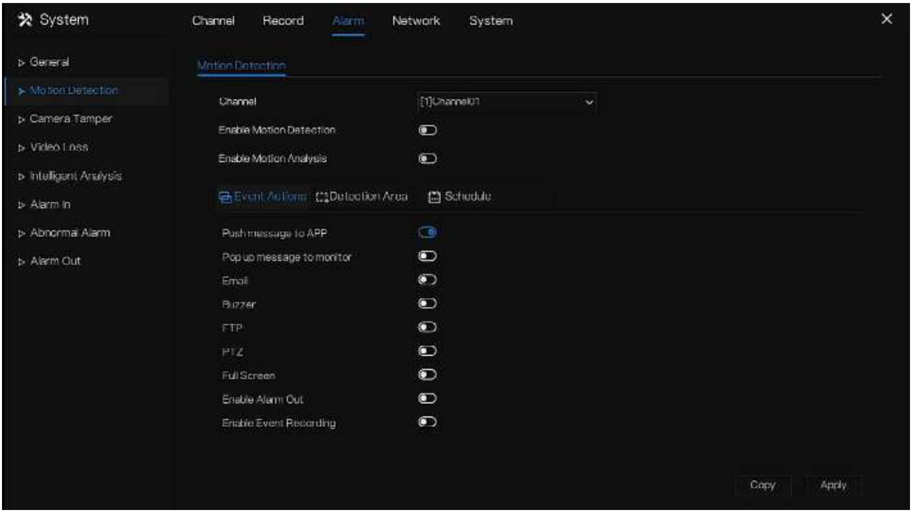
7.5.2 Motion Detection

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

Operation Description

Step 1 Click **Motion Detection** in the main menu or menu of the alarm management screen and choose **Motion Detection** to access the Motion Detection screen, as shown in Figure 7-29.

Figure 7-29 Motion detection screen



Channel [1]Channel01

Enable Motion Detection

Enable Motion Analysis

Push message to APP

Pop up message to monitor

Email

Buzzer

FTP

PTZ

Full Screen

Enable Alarm Out

Enable Event Recording

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

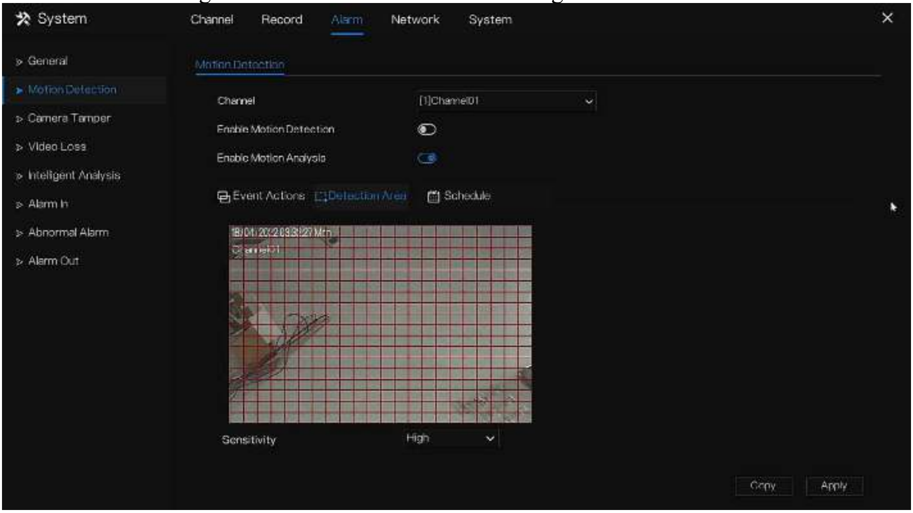
Step 3 Click ● to enable motion detection.

Step 4 Enable motion analysis, if the camera detects the motion action, the area will be block.

Step 5 Enable the Event actions including: Push message to App, Pop up message to monitor, Email, Buzzer, FTP, PTZ, Full screen, Enable alarm out and Enable event recording.

Step 6 Click Area page to access the motion detection area setting, as shown in Figure 7-30.

Figure 7-30 Motion detection area setting screen



Channel: [1]Channel01

Enable Motion Detection

Enable Motion Analysis

Sensitivity: High

Area :

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**.

Step 7 Click **Schedule** page to access the schedule screen. For details, please see 7.4.1 Record Schedule Set the record schedule.

Step 8 Click Copy and select channels or tick **all**, then click OK to apply the motion detection settings to cameras in selected channels, click Apply to save motion detection alarm settings.

NOTE

Click to select the motion detection area, and double click to cancel.

The default area is whole area.

If you leave the page without applying, the tip “Do you want to save?” would show. Click **Save** to save the settings. Click cancel to quit the settings.

----End

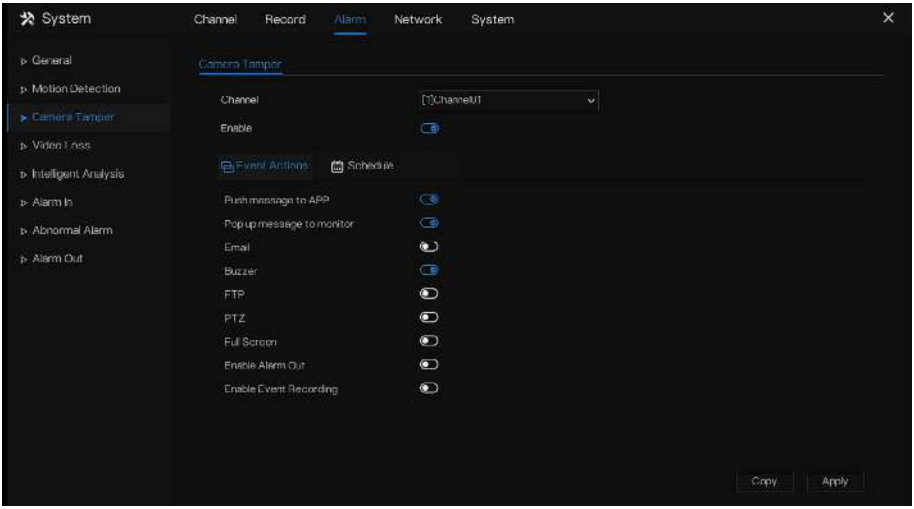
7.5.3 Camera Tamper

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

Operation Description

Click **Camera Tamper** in the main menu or menu of the alarm management screen and choose **Camera Tamper** to access the video loss screen, as shown in Figure 7-31.

Figure 7-31 Camera Tamper screen



Channel [1]Channel01

Enable ●

Push message to APP ●

Pop up message to monitor ●

Email ○

Buzzer ●

FTP ○

PTZ ○

Full Screen ○

Enable Alarm Out ○

Enable Event Recording ○

Operation Steps

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

Step 2 Click ○ to enable camera tamper alarm.

Step 3 Enable the Event actions including: **Push message to App, Pop up message to monitor, Email, Buzzer, FTP, PTZ, Full screen, Enable alarm out** and **Enable event recording**.

Step 4 Click Schedule page to access the schedule screen.

Step 5 For details, please refer to *7.4.1 Record Schedule Set the record schedule.*

Step 6 Click Copy and select a channel, then click OK to apply the parameter settings to cameras in selected channels, click Apply to save video loss settings.

---End

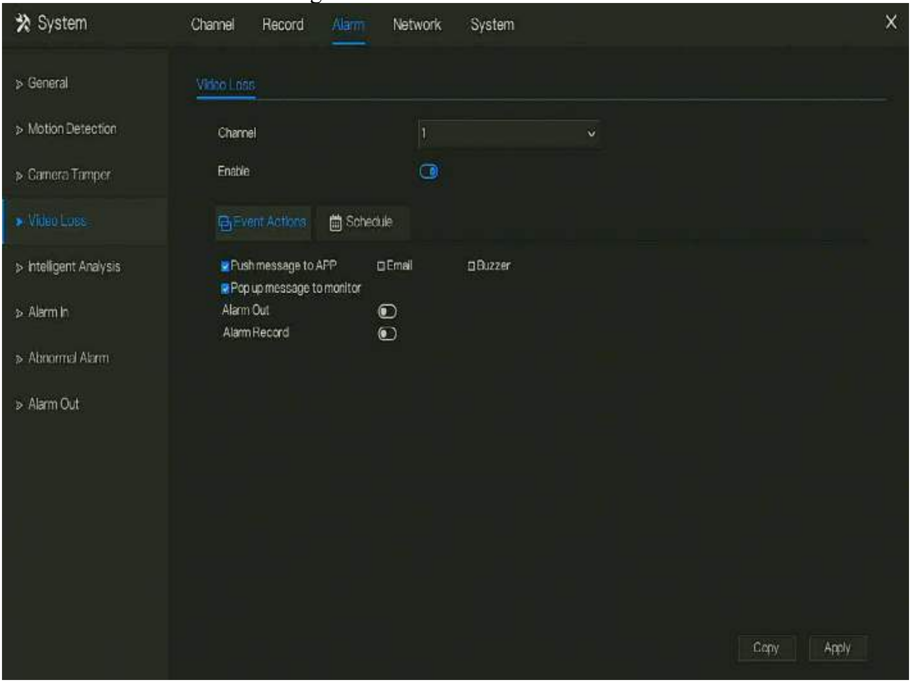
7.5.4 Video Loss

If the camera is disconnected from the DVR, a video loss alarm will be triggered.

Operation Description

Click **Video Loss** in the main menu or menu of the alarm management screen and choose **video Loss** to access the video loss screen, as shown in Figure 7-32.

Figure 7-32 Video loss screen



Channel 1

Enable ●

☑ Push message to APP ☐ Email ☐ Buzzer

☑ Pop up message to monitor

Alarm Out ○

Alarm Record ○

Operation Steps

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

Step 2 Click ○ to enable video loss alarm.

Step 3 Enable the Event actions including: **Push message to App, Pop up message to monitor, Email, Buzzer, FTP, PTZ, Enable alarm out** and **Enable event recording**.

Step 4 Click Schedule page to access the schedule screen.

Step 5 For details, please refer to *7.4.1 Record Schedule Set the record schedule.*

Step 6 Click Copy and select a channel, then click OK to apply the parameter settings to cameras in selected channels, click Apply to save video loss settings.

---End

7.5.5 Intelligent Analysis

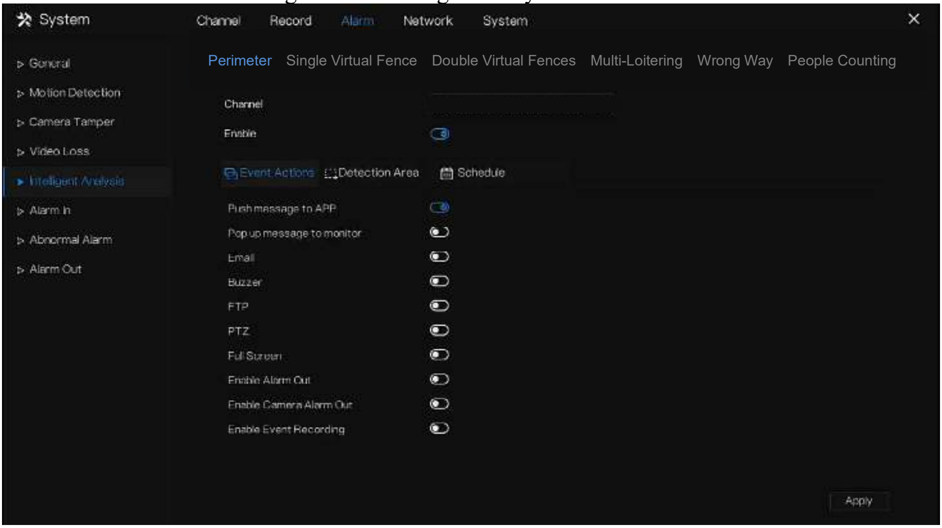
NOTE

This function can only be used for IP cameras. T Different cameras may have different types of intelligent analysis, please refer to the actual product.

Operation Description

Step 1 Click **Intelligent Analysis** in the main menu or menu of the alarm management screen and choose **Intelligent Analysis** to access intelligent analysis screen, as shown in Figure 7-33.

Figure 7-33 Intelligent Analysis screen



Channel

Enable

Push message to APP

Pop up message to monitor

Email

Buzzer

FTP

PTZ

Full Screen

Enable Alarm Out

Enable Camera Alarm Out

Enable Event Recording

Step 2 Select one action to set the alarm.(perimeter, single virtual fence, double virtual fences, object left, signal bad, loiter, multi loiter. For some cameras, **Abnormal Speed, Converse, Illegal Parking, Advanced** can be set.

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

Step 4 Click to enable intelligent analysis alarm.

Step 5 Enable the event actions including: **Push message to App, Pop up message to monitor, Email, Buzzer, FTP, PTZ, Full screen, Enable alarm out** and **Enable event recording**.

Step 6 Click Schedule page to access the schedule screen.

Step 7 For details, please refer to *7.4.1 Record Schedule Set the record schedule.*

Step 8 Click Apply to save video loss settings.

----End

7.5.6 Alarm In

There are two types alarm in, one is the DVR's alarm in, the other is the camera channel's alarm in.

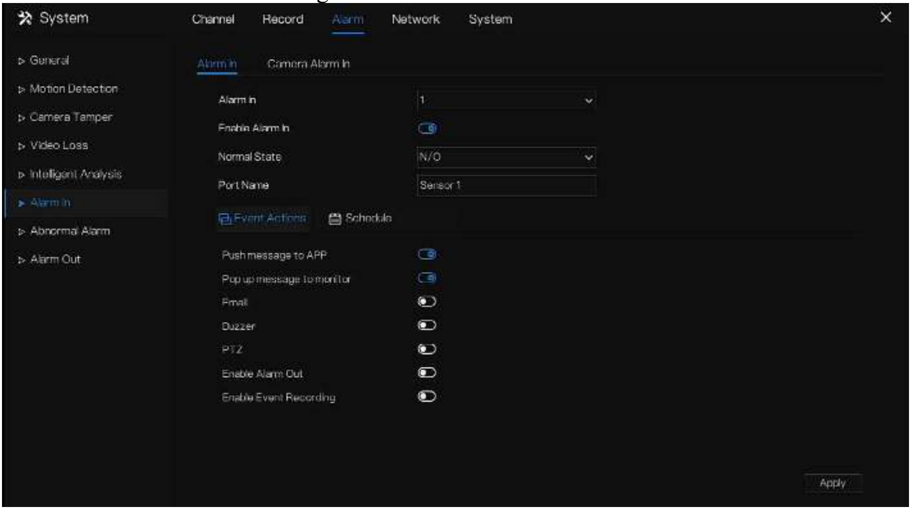
NOTE

Some cameras may not have the function, please refer to actual products.

Operation Description

Click **Alarm in** in the main menu or menu of the alarm management screen and choose **Alarm in** to access the alarm in screen, as shown in Figure 7-34.

Figure 7-34 Alarm in screen



Alarm In: 1

Enable Alarm In: ●

Normal State: N/O

Port Name: Sensor 1

Push message to APP: ●

Pop up message to monitor: ●

Email: ○

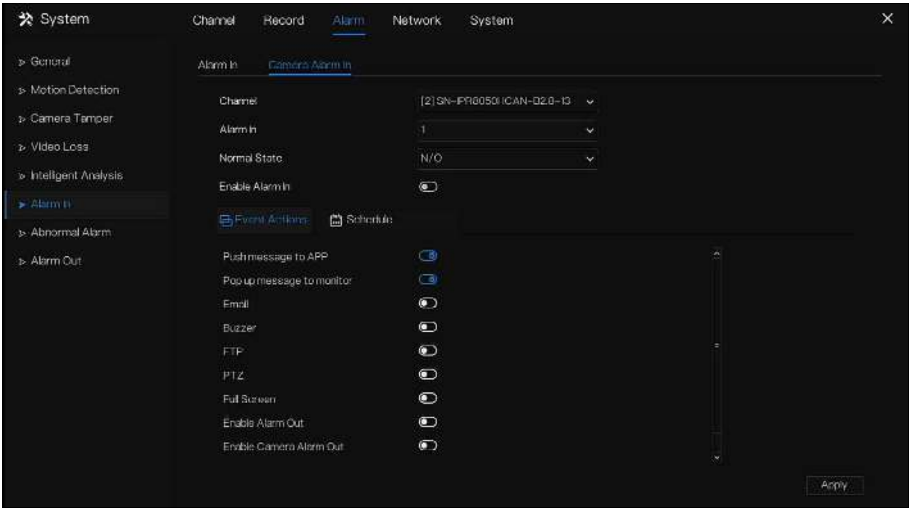
Buzzer: ○

PTZ: ○

Enable Alarm Out: ○

Enable Event Recording: ○

Figure 7-35 Channel alarm in screen



Channel: [2] SN-IPR8050ICAN-B2.8-13

Alarm In: 1

Normal State: N/O

Enable Alarm In: off

Push message to APP: on

Pop up message to monitor: on

Email: off

Buzzer: off

FTP: off

PTZ: off

Full Screen: off

Enable Alarm Out: off

Enable Camera Alarm Out: off

Operation Steps

Step 1 Select a channel in **alarm in**.

Step 2 Click ○ to enable or disable the functions.

Step 3 Select **Alarm type** from the drop-down list.

NOTE

NC: Normal close the alarm

NO: Normal open the alarm

Step 4 Set **name**.

Step 5 Enable the event actions including: **Push message to App, Pop up message to monitor, Email, Buzzer, FTP, PTZ, Full screen, Enable alarm out** and **Enable event recording**.

Step 6 Click **Schedule** page to access the schedule screen. For details, please see *7.4.1 Record Schedule Set the record schedule.*

Step 7 Click Apply to save alarm in settings.

----End

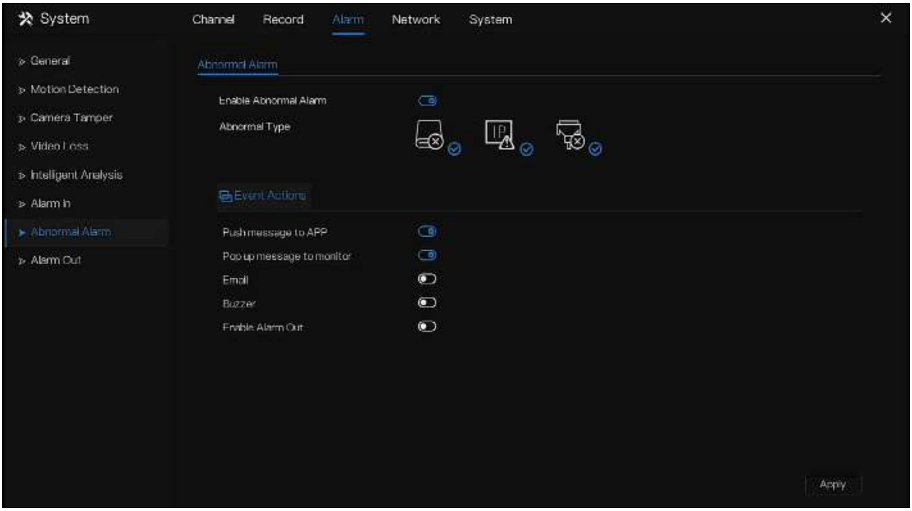
7.5.7 Abnormal Alarm

Camera tamper means that the DVR would send alarm notification while objects cover IP cameras.

Operation Description

Step 1 Click **Abnormal Alarm** in the main menu or menu of the alarm management screen and choose **Abnormal Alarm** to access the abnormal alarm screen, as shown in Figure 7-36.

Figure 7-36 Abnormal alarm screen



Enable Abnormal Alarm ●

Abnormal Type ✓ ✓ ✓

Push message to APP ●

Pop up message to monitor ●

Email ○

Buzzer ○

Enable Alarm Out ○

Operation Steps

Step 2 Tick the abnormal actions.

Step 3 Enable the event actions include: Push message to App, Pop up message to monitor, Email, Buzzer and Enable alarm out.

Step 4 Click Apply to save abnormal alarm settings.

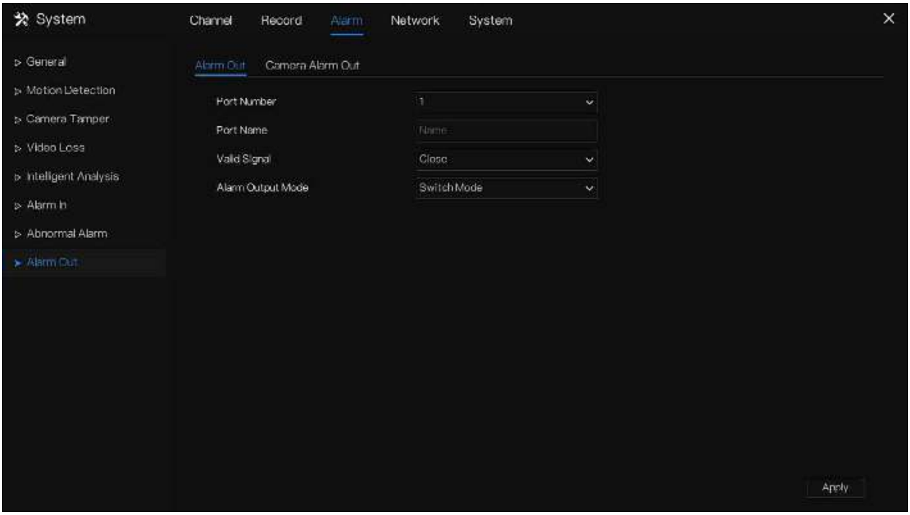
----End

7.5.8 Alarm Out

7.5.8.1 Alarm Out

Choose one output ID as the output interface, as shown in Figure 7-37. Choose the **Valid Signal** and **Alarm Output Mode** according to the connection of external alarm devices.

Figure 7-37 Alarm out screen



Port Number: 1

Port Name: Name

Valid Signal: Close

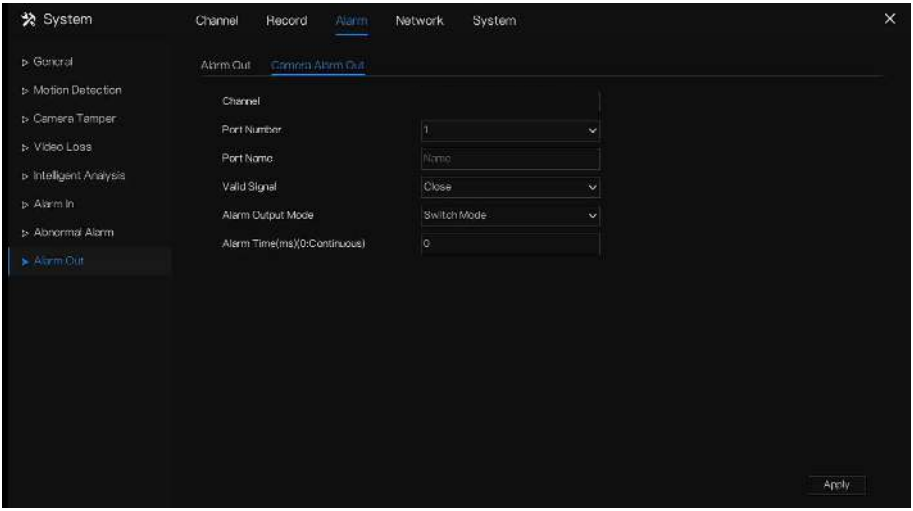
Alarm Output Mode: Switch Mode

7.5.8.2 Camera Alarm out

NOTE

This function is only used for IP cameras.

Figure 7-38 Camera alarm out



Channel

Port Number: 1

Port Name: Name

Valid Signal: Close

Alarm Output Mode: Switch Mode

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

Table 7-5 Camera alarm out parameters

Parameter	Description	Setting
Channel	Choose one channel to set, the camera should have the alarm out port.	
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, the device sends 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 continuous 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

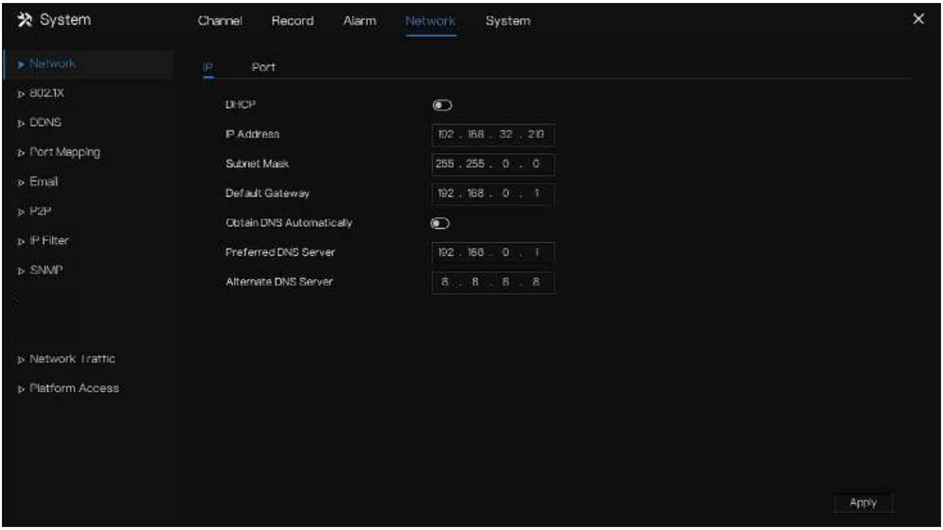
7.6 Network Management

Set the **Network Parameter, 802.1X, DDNS, E-mail, Port Mapping, P2P, IP Filter, Network Traffic, Platform Access** or **WiFi** in the network management screen.

Operation Description

Step 1 Click **Network** in the main menu (or click the network page of any function screen in the main menu) to access the network management screen, as shown in Figure 7-39.

Figure 7-39 Network management screen



DHCP	○
IP Address	192 . 168 . 32 . 210
Subnet Mask	255 . 255 . 0 . 0
Default Gateway	192 . 168 . 0 . 1
Obtain DNS Automatically	○
Preferred DNS Server	192 . 168 . 0 . 1
Alternate DNS Server	8 . 8 . 8 . 8

7.6.1 Network

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

7.6.1.1 IP

Operation Steps

Step 1 Click ○ next to **DHCP** to enable or disable the function of automatically getting an IP address. The function is disabled by default.

Step 2 If the function is disabled, click input boxes next to **IP**, **Subnet mask**, and **Gateway** to set the parameters as required.

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

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

Step 5 Click Apply to save IP settings.

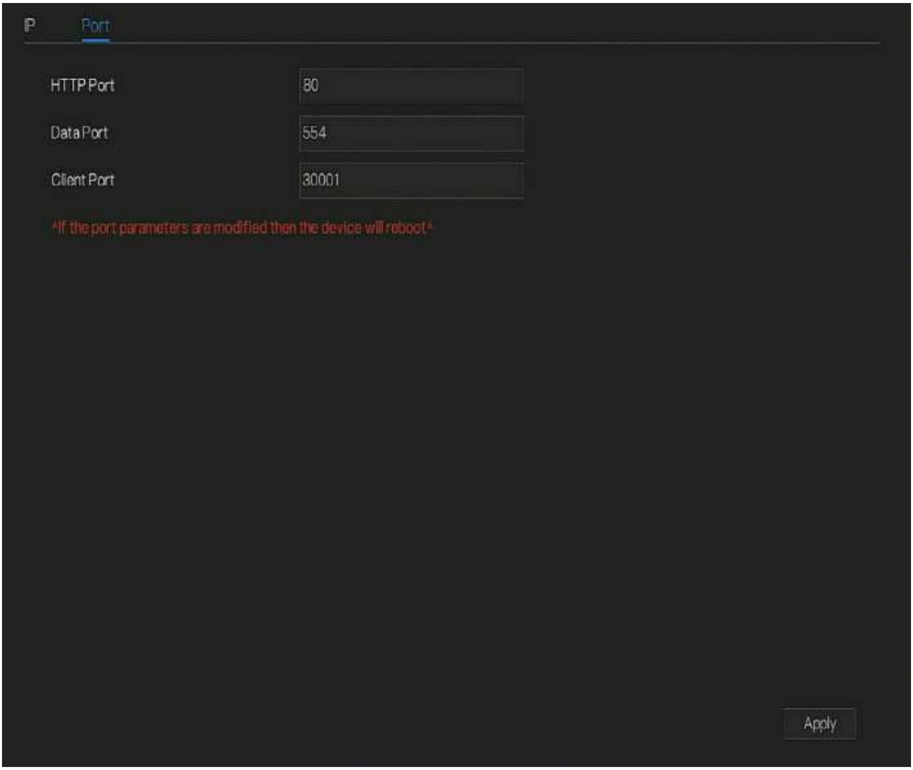
----End

7.6.1.2 Port

Operation Steps

Step 1 Click **Port** page to access the port setting screen, as shown in Figure 7-40.

Figure 7-40 Port setting screen



HTTP Port: 80

Data Port: 554

Client Port: 30001

If the port parameters are modified then the device will reboot

Step 2 Set the web port, data port and client port.

Step 3 Click Apply to save port settings.

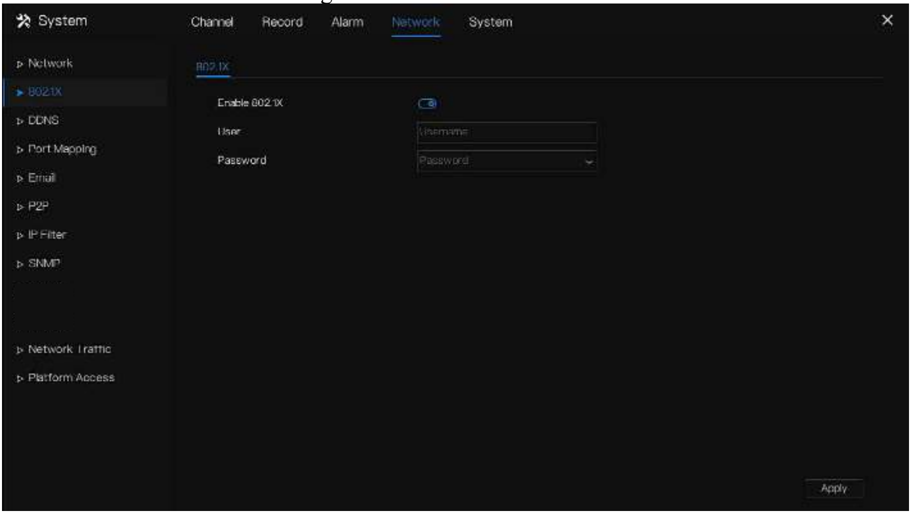
----End

7.6.2 802.1 X

Operation Steps

Step 1 Click ○ next to **802.1 X** to enable or disable the function, as shown in Figure 7-41. The default is disabled.

Figure 7-41 802.1 X screen



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

Step 3 Click Apply to save the settings. The visitor who view the DVR need to enter the account for authentication.

7.6.3 DDNS

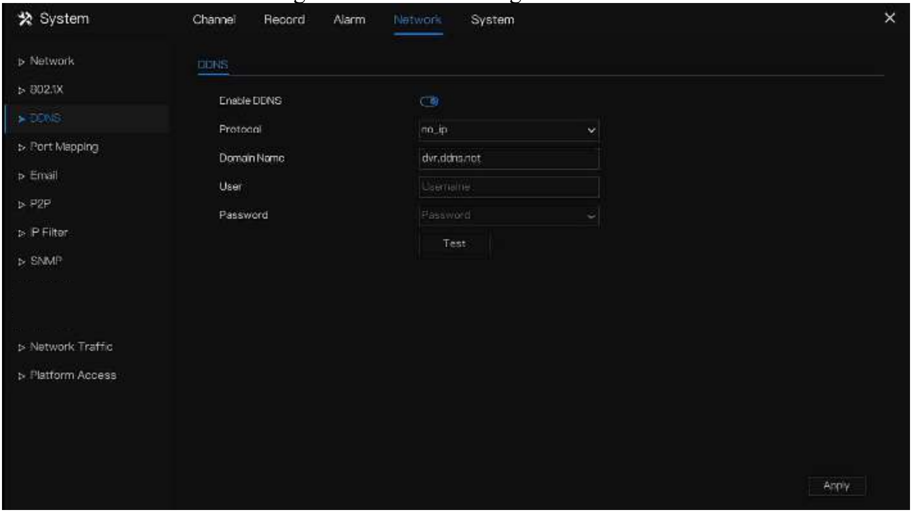
Please make sure the specified camera is connected to the Internet, and obtain the user name and password for logging into the dynamic domain name system (DDNS) from the server.

Operation Steps

Step 1 Click **DDNS** in the main menu or menu of the network management screen and choose **DDNS** 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 7-42.

Figure 7-42 DDNS setting screen



Enable DDNS ●

Protocol no_ip

Domain Name dvr.ddns.net

User Username

Password Password

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

Step 4 Set a domain name, input username and password.

Step 5 Click Test to check the domain name.

Step 6 Click Apply to save DDNS network settings

NOTE

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

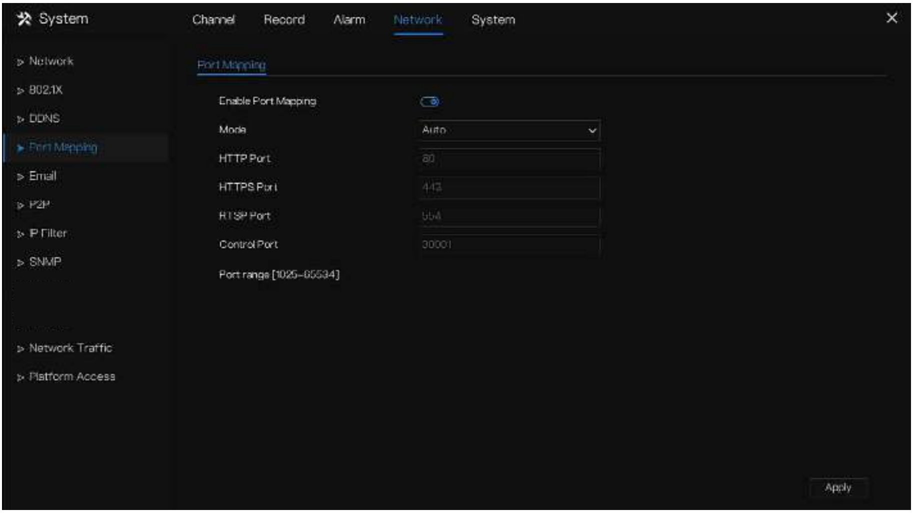
----End

7.6.4 Port Mapping

Operation Steps

Step 1 Click **Port Mapping** in the main menu or menu of the network management screen and choose **Port Mapping** to access the port mapping screen, as shown in Figure 7-43.

Figure 7-43 Port mapping setting screen



Enable Port Mapping

Mode: Auto

HTTP Port: 80

HTTPS Port: 443

RTSP Port: 554

Control Port: 30001

Port range [1025–65534]

Step 2 Select UPnP enable type.

Step 3 Manual UPnP: input HTTP port, HTTPS port, RSTP port and Control Port manually.

Step 4 Auto Port Mapping: The device obtain the port automatically.

Step 5 Click Apply to save settings.

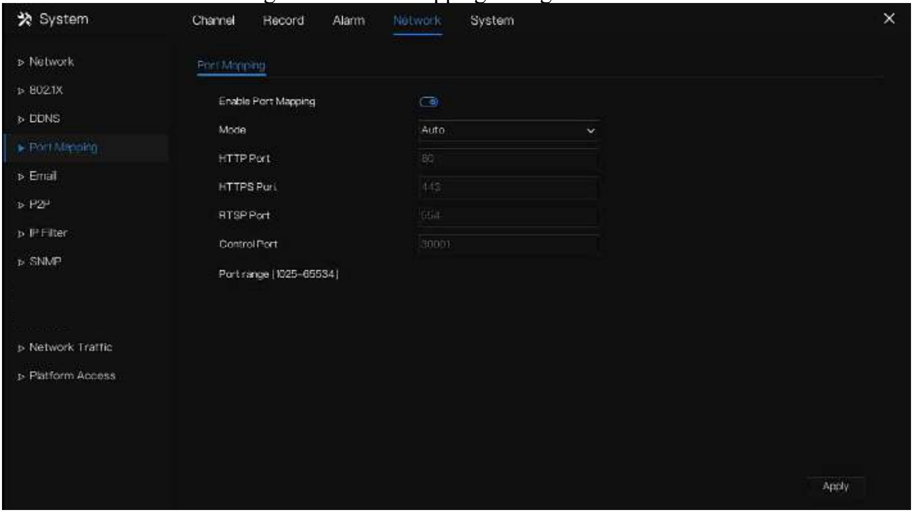
----End

7.6.5 Port Mapping

Operation Steps

Step 1 Click **Port Mapping** in the main menu or menu of the network management screen and choose **Port Mapping** to access the port mapping screen, as shown in Figure 7-44.

Figure 7-44 Port mapping setting screen



Enable Port Mapping

Mode: Auto

HTTP Port: 80

HTTPS Port: 443

RTSP Port: 554

Control Port: 30001

Port range (1025-65534)

Step 2 Select Port Mapping enable type.

Step 3 Manual Port Mapping: input HTTP port, HTTPS port, RTSP port and Control port manually. Port range is 1025-65534.

Step 4 Auto Port Mapping: The device obtain the port automatically.

Step 5 Click Apply to save settings.

----End

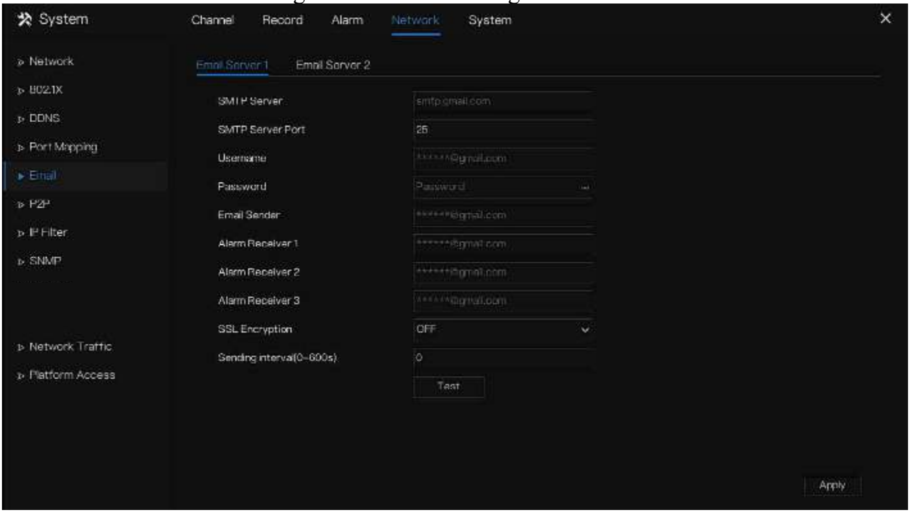
7.6.6 Email

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.

Operation Steps

Step 1 Click **Email** in the main menu or menu of the network management screen and choose **Email** to access the Email screen, as shown in Figure 7-45.

Figure 7-45 E-mail setting screen



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

Step 2 Set SMTP server and SMTP server port manually.

Step 3 Input E-mail sender, user name and password manually.

Step 4 Set E-mail for receiving the alarm. the message “**Mail has been sent, please check**” is displaying. Open the mail, if the verification code is received, that shows the E-mail is set successfully.

Step 5 Set E-mail for retrieving the password. the message “Mail has been sent, please check” is displaying. Open the mail, if the verification code is received, that shows the E-mail is set successfully.

Step 6 Set SSL encryption for encrypting mail or not.

Step 7 Click Apply to save settings. You can set two servers to send and receive the alarm information.

----End

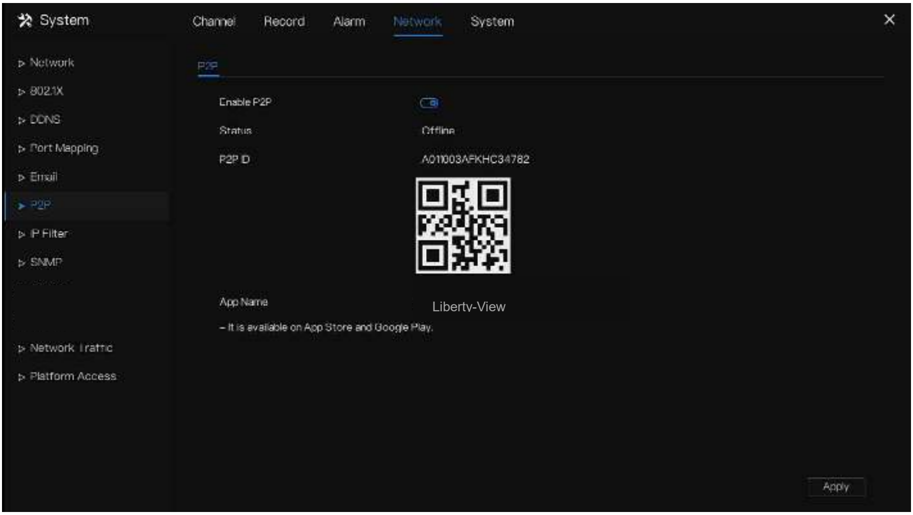
7.6.7 P2P

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

Operation Steps

Step 1 Click **P2P** in the main menu or menu of the network management screen and choose **P2P** to access the P2P screen, as shown in Figure 7-46.

Figure 7-46 P2P screen



Enable P2P

Status Offline

P2P ID A011003AFKHC34782

App Name Liberty-View

– It is available on App Store and Google Play.

Step 2 Click ○ to enable the P2P function.

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

Step 4 After the **Liberty-View** is installed in mobile phone, run the APP and scan the QR to add and access the DVR when the device is online.

----End

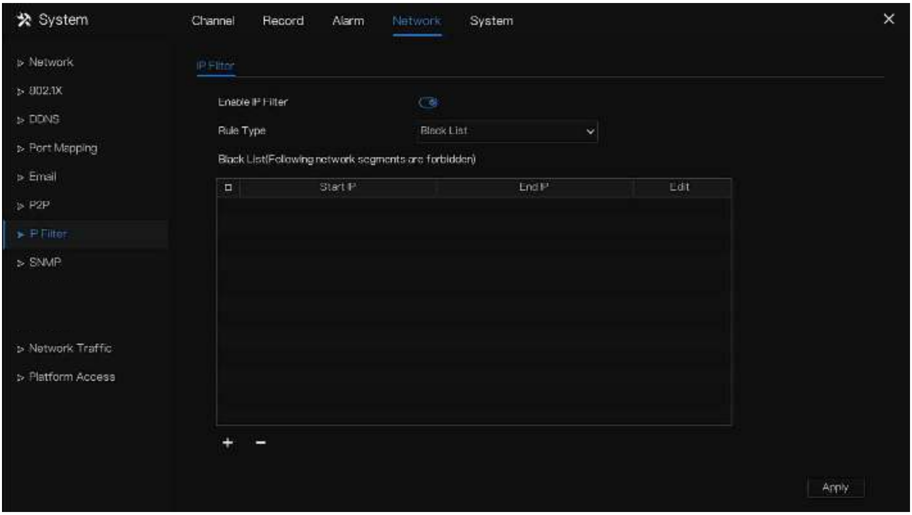
7.6.8 IP Filter

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

Operation Steps

Step 1 Click **IP Filter** in the main menu or menu of the network management screen and choose **IP Filter** to access the IP filter screen, as shown in Figure 7-47.

Figure 7-47 IP Filter setting screen



Enable IP Filter ●

Rule Type: Black List

Black List(Following network segments are forbidden)

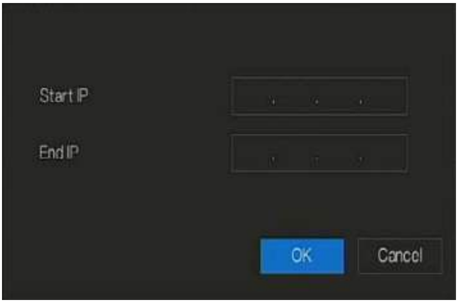
□	Start IP	End IP	Edit

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

Step 3 Select black list or white list drop-down list.

Step 4 Click + to set black &white list, The IP segment screen is as show in Figure 7-48.

Figure 7-48 IP Address Segment screen



Start IP . . .

End IP . . .

V

Step 5 Enter values of start IP address, end IP address.

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

NOTE

Black list: A list of IP addresses that are regarded as unacceptable or untrustworthy and should be excluded or avoided.

White list: A list of IP addresses 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

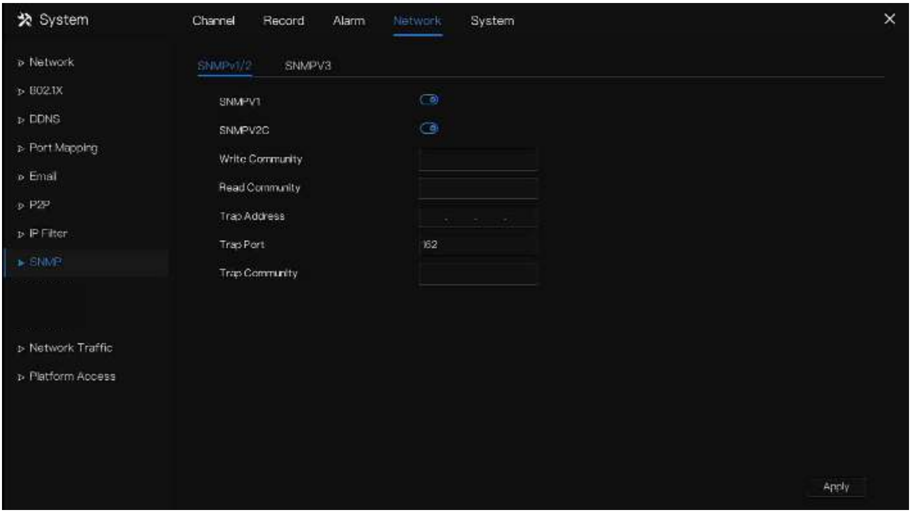
7.6.9 SNMP

There are three versions of simple network management protocol at interface.

Operation Steps

Step 1 Click **IP Filter** in the main menu or menu of the network management screen and choose **IP Filter** to access the IP filter screen, as shown in Figure 7-49.

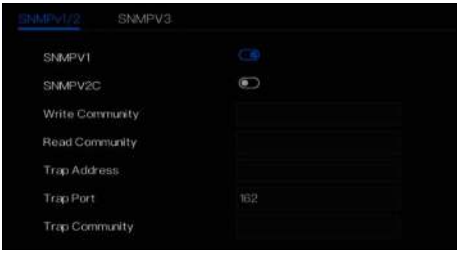
Figure 7-49 SNMP settings screen



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

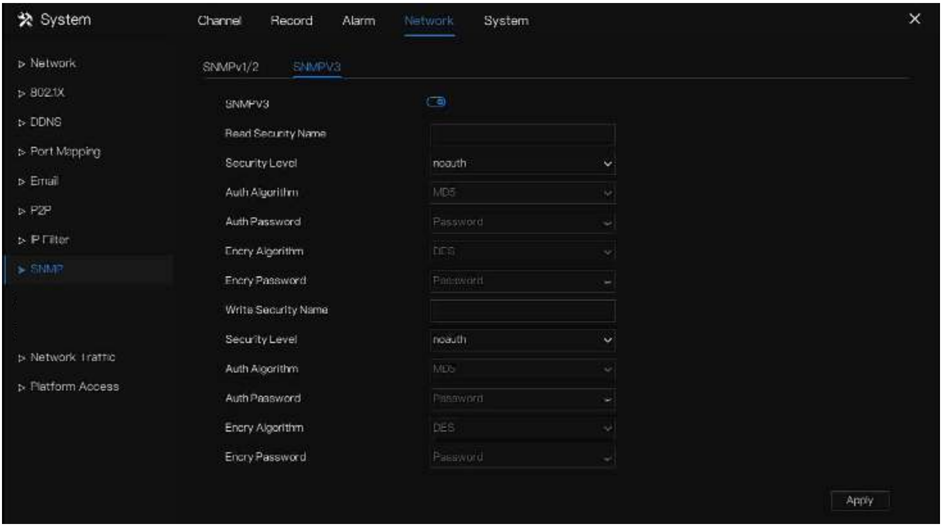
Step 2 Click ○ next to **SNMPV 1** to enable the function . The interface is shown as Figure 7-52.

Figure 7-50 SNMPV 1/2 interface



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

Figure 7-51 SNMPV3



SNMPV3
Read Security Name
Security Level noauth
Auth Algorithm MD5
Auth Password Password
Encry Algorithm DES
Encry Password Password
Write Security Name
Security Level noauth
Auth Algorithm MD5
Auth Password Password
Encry Algorithm DES
Encry Password Password

Step 3 Input the parameters of protocol.

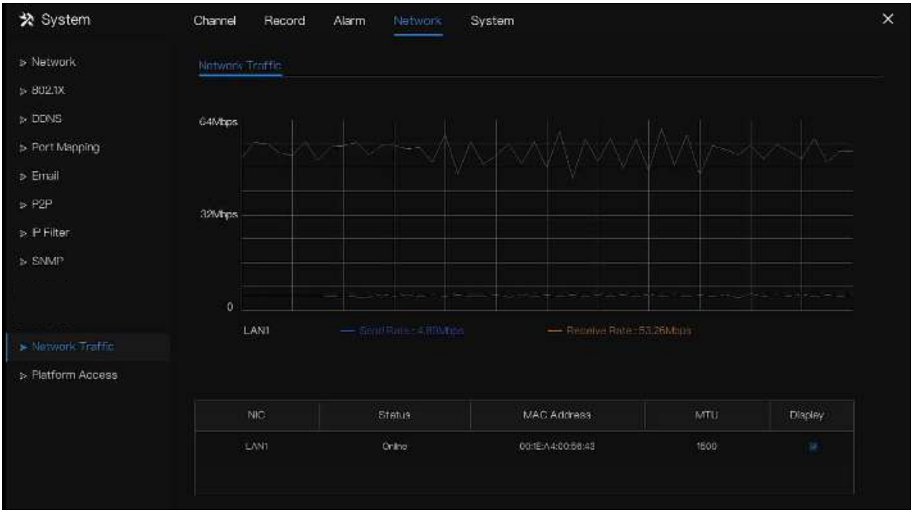
Step 4 Click Apply to save settings or click Cancel to cancel settings.

----End

7.6.10 Network Traffic

Users can view the network traffic immediately, as shown in Figure 7-52.

Figure 7-52 Network traffic screen



NIC	Status	MAC Address	MTU	Display
LAN1	Online	00:1E:A4:00:58:43	1500	☑

There are two rates, transmit rate and receive rate (the web interface shows live video).

----End

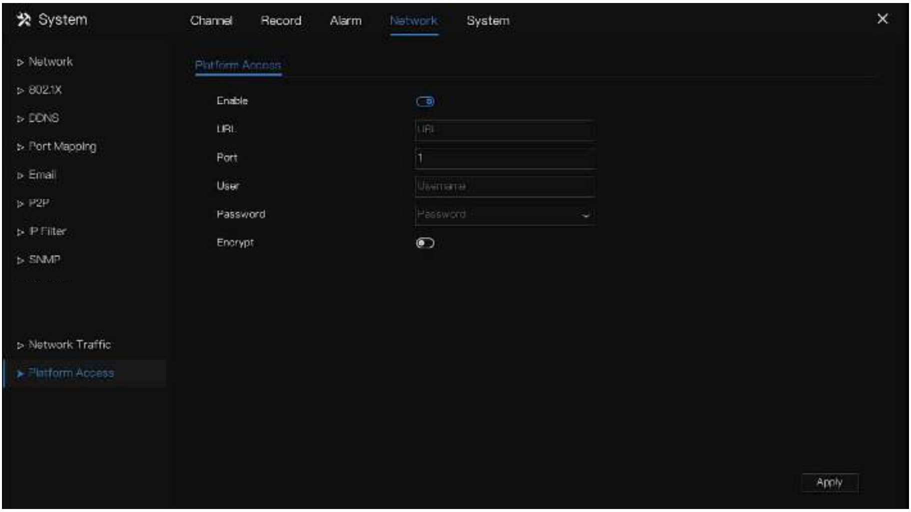
7.6.11 Platform Access

If the DVR and platform system are not at the same local network, you can connect the device and the platform system to an external server.. You should build a server for platform in advance, platform's remote IP/Port and DVR are mapping port to external network.

Step 1 Choose **Configuration > Network Service > Platform Access**.

The **Platform Access** page is displayed, as shown in Figure 7-53

Figure 7-53 Platform Access page



Enable	
URL	URL
Port	1
User	Username
Password	Password
Encrypt	

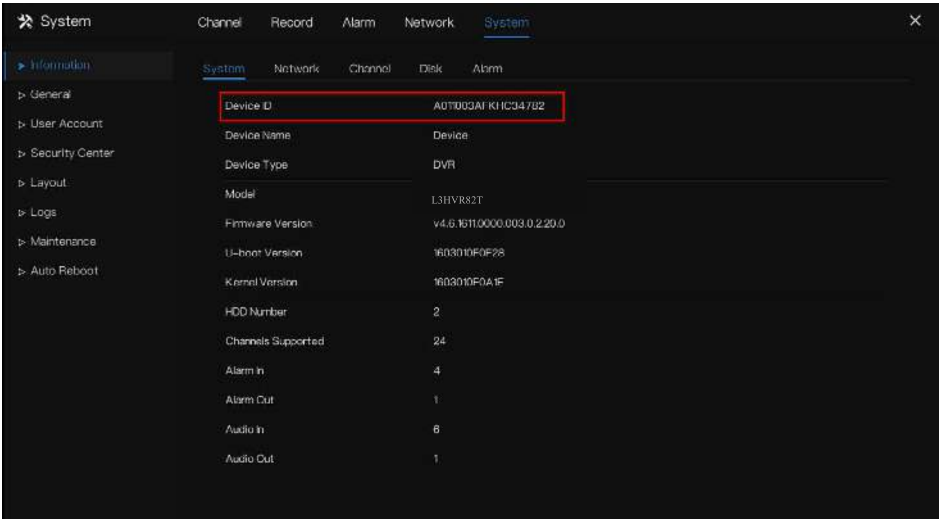
Step 2 Input the parameters. The URL and port are the the IP address and port of the platform server.

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

Step 4 Add the DVR to platform, you should input the following information

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

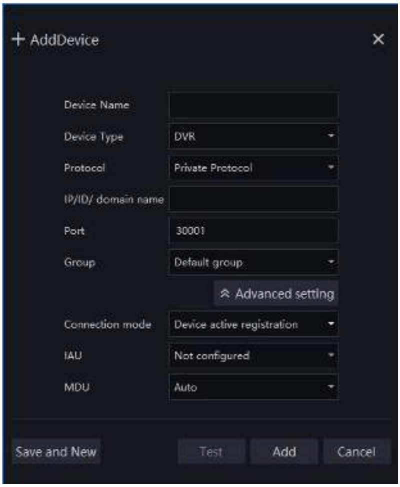
Figure 7-54 IP/ID/Domain



Device ID	A011003AFKHC34782
Device Name	Device
Device Type	DVR
Model	L3HVR82T
Firmware Version	v4.6.1611.0000.003.0.2.20.0
U-boot Version	1603010F0F28
Kernel Version	1603010F0A1F
HDD Number	2
Channels Supported	24
Alarm In	4
Alarm Out	1
Audio In	6
Audio Out	1

2: The connection mode should be selected as **Device active registration**.

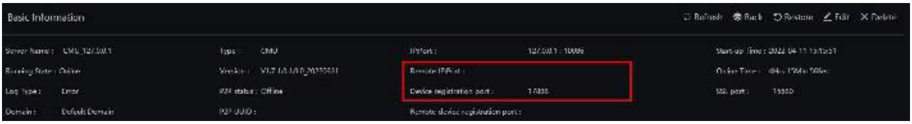
Figure 7-55 Connect DVR to platform



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

3: the CMU, MDU and IAU servers of platform should port map to external network in advance.

Figure 7-56 URL address / port



Server Name : CMU_127.0.0.1
Type : CMU
IP/Port : 127.0.0.1 : 10086
Start-up Time : 2022-04-11 15:15:51
Running State : Online
Version : V1.7.1.0.1.0.0_20220331
Remote IP/Port :
Online Time : d4h 15Min 50Sec
Log Type : Error
P2P status : Offline
Device registration port : 17000
SSL port : 15550
Domain : Default Domain
P2P UUID :
Remote device registration port :

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

Step 6 Click **Apply**.

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

----End

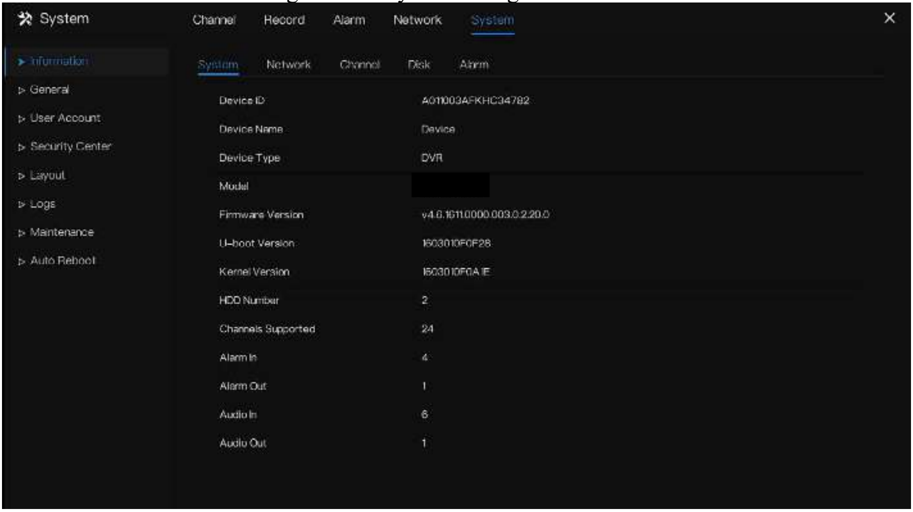
7.7 System Management

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 main menu (or click the system page of any function screen in the main menu) to access the system setting screen, as shown in Figure 7-57.

Figure 7-57 System setting screen

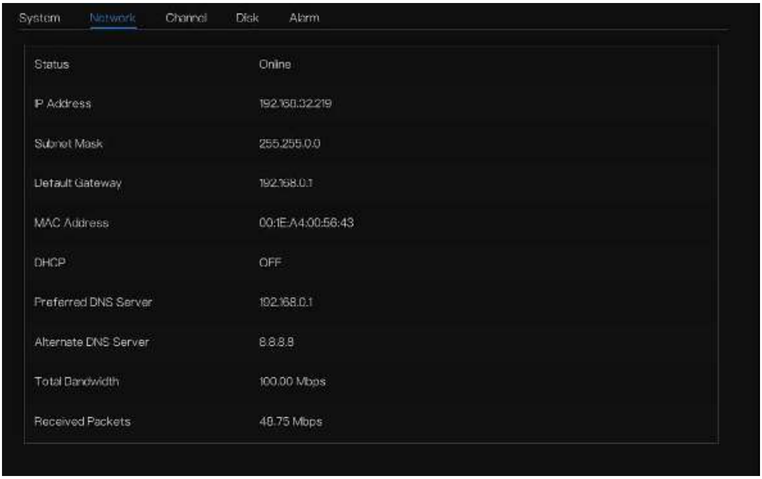


Device ID	A011003AFKHC34782
Device Name	Device
Device Type	DVR
Model	[redacted]
Firmware Version	v4.6.1611.0000.003.0.2.20.0
U-boot Version	1603010F0F28
Kernel Version	1603010F0A1E
HDD Number	2
Channels Supported	24
Alarm In	4
Alarm Out	1
Audio In	6
Audio Out	1

7.7.1 Information

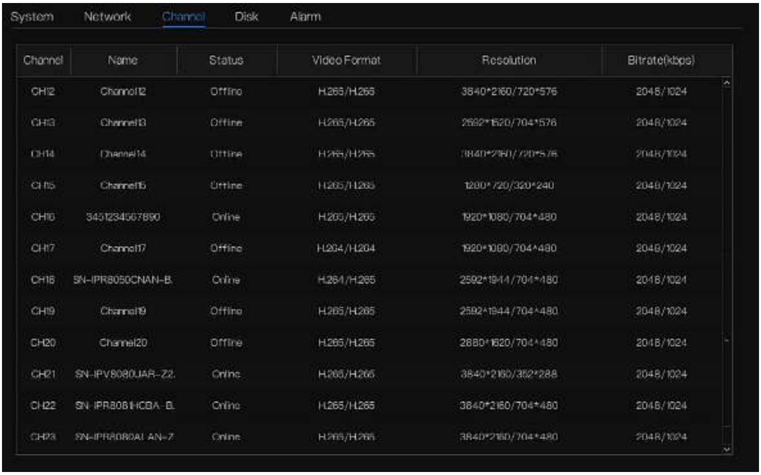
Information includes System, Network, Channel, Disk, Alarm, as shown in Figure 7-58 .

Figure 7-58 Information interface



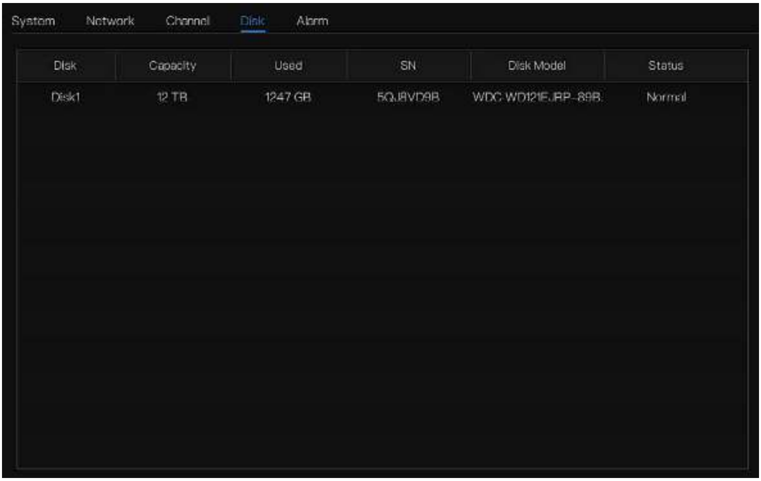
Status	Online
IP Address	192.168.32.219
Subnet Mask	255.255.0.0
Default Gateway	192.168.0.1
MAC Address	00:1E:A4:00:56:43
DHCP	OFF
Preferred DNS Server	192.168.0.1
Alternate DNS Server	8.8.8.8
Total Bandwidth	100.00 Mbps
Received Packets	48.75 Mbps

Figure 7-59 Channel



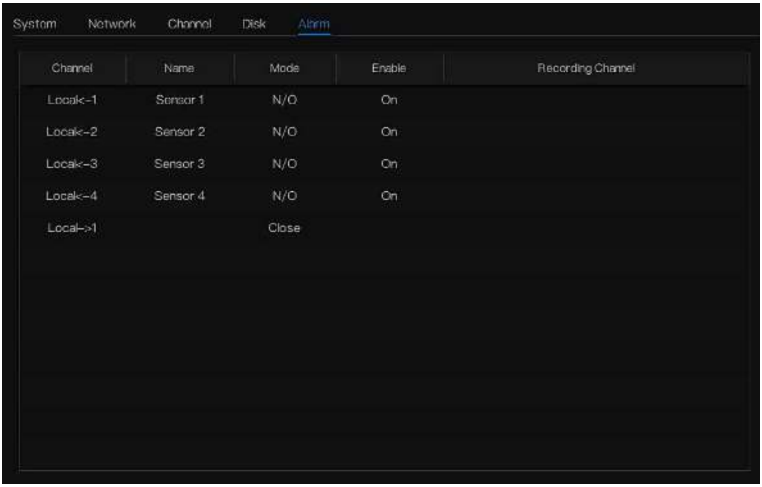
Channel	Name	Status	Video Format	Resolution	Bitrate(kbps)
CH12	Channel12	Offline	H.265/H.265	3840*2160/720*576	2048/1024
CH13	Channel13	Offline	H.265/H.265	2592*1520/704*576	2048/1024
CH14	Channel14	Offline	H.265/H.265	3840*2160/720*576	2048/1024
CH15	Channel15	Offline	H.265/H.265	1280*720/320*240	2048/1024
CH16	3451234567890	Online	H.265/H.265	1920*1080/704*480	2048/1024
CH17	Channel17	Offline	H.264/H.264	1920*1080/704*480	2048/1024
CH18	SN-IPR8050CNAN-B.	Online	H.264/H.265	2592*1944/704*480	2048/1024
CH19	Channel19	Offline	H.265/H.265	2592*1944/704*480	2048/1024
CH20	Channel20	Offline	H.265/H.265	2880*1620/704*480	2048/1024
CH21	SN-IPV8080UAR-Z2.	Online	H.265/H.265	3840*2160/352*288	2048/1024
CH22	SN-IPR8081HCBA-B.	Online	H.265/H.265	3840*2160/704*480	2048/1024
CH23	SN-IPR8080ALAN-Z.	Online	H.265/H.265	3840*2160/704*480	2048/1024

Figure 7-60 Disk



Disk	Capacity	Used	SN	Disk Model	Status
Disk1	12 TB	1247 GB	5QJ8VD9B	WDC WD121EJRP-89B.	Normal

Figure 7-61 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->1		Close		

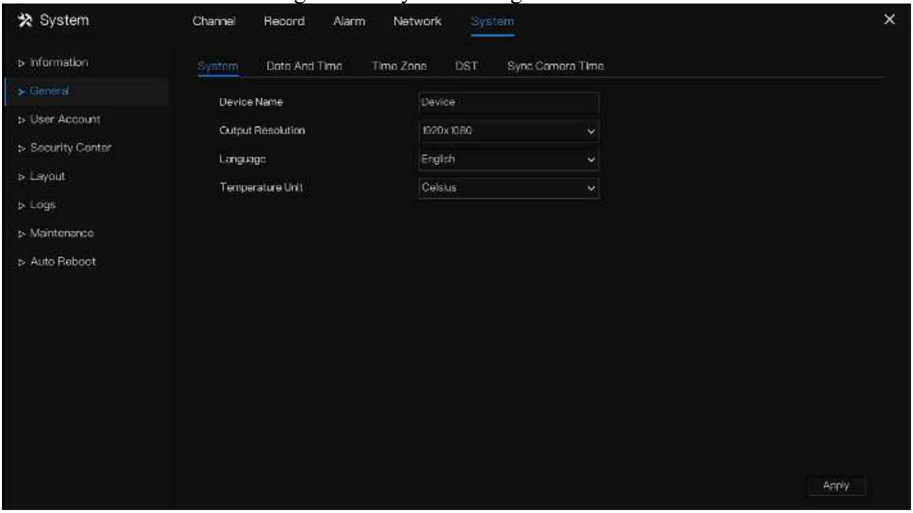
7.7.2 General

7.7.2.1 System

Operation Steps

Step 1 Click **General** in the main menu or menu of the system management screen and choose **General** to access the system screen, as shown in Figure 7-62.

Figure 7-62 system setting screen



Device Name: Device
Output Resolution: 1920x1080
Language: English
Temperature Unit: Celsius

Step 2 Enter device name for 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 Click Apply to save settings.

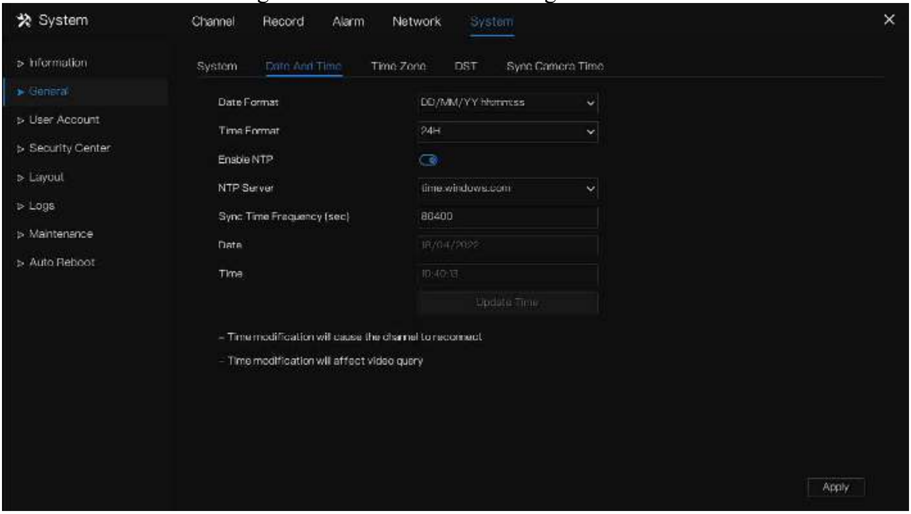
----End

7.7.2.2 Date and Time

Operation Steps

Step 1 Click **Date and Time** page to access the date and time setting screen, as shown in Figure 7-63.

Figure 7-63 Date and Time setting screen



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

Time Format 24H

Enable NTP

NTP Server time.windows.com

Sync Time Frequency (sec) 86400

Date 18/04/2022

Time 10:40:13

- Time modification will cause the channel to reconnect

- Time modification will affect video query

Step 2 Select 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.

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

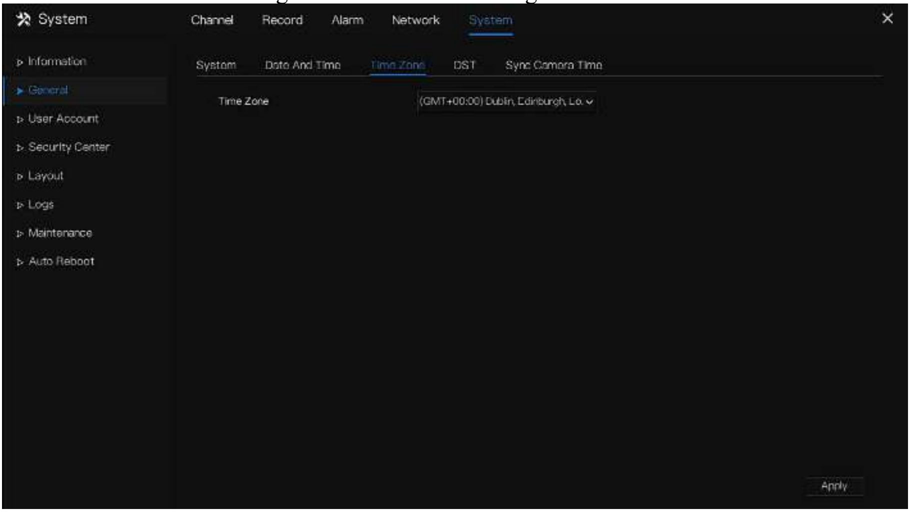
----End

7.7.2.3 Time Zone

Operation Steps

Step 1 Click **Time zone** page to access the time zone setting screen, as shown in Figure 7-64.

Figure 7-64 Time zone setting screen



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

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

Step 2 Click Apply to save settings.

----End

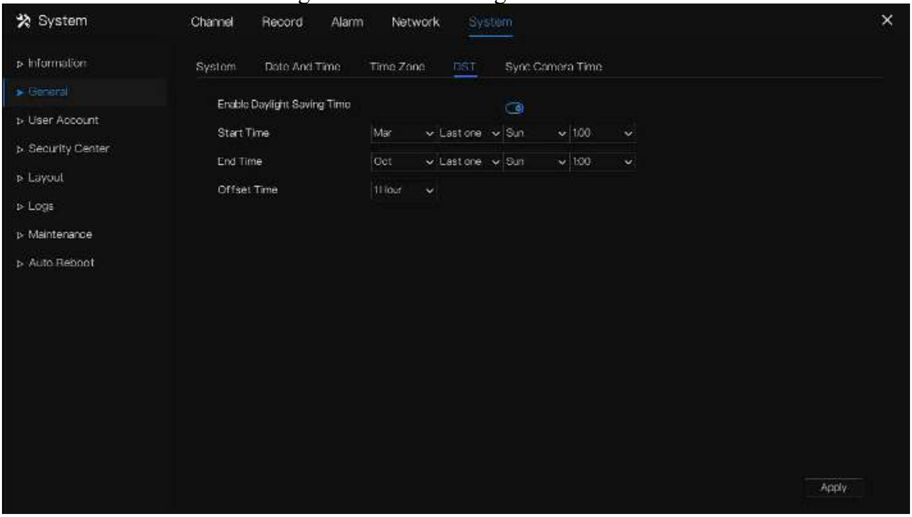
7.7.2.4 DST

Daylight saving time begins in the spring, when the device clock is set one hour ahead automatically. It is then set one hour back in the fall. The offset time can be changed as local rules.

Operation Steps

Step 1 Click **DST** page to access the DST setting screen, as shown in Figure 7-65.

Figure 7-65 DST setting screen



Enable Daylight Saving Time ●

Start Time Mar Last one Sun 1:00

End Time Oct Last one Sun 1:00

Offset Time 1Hour

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

Step 3 Select start time, end time, offset time from the drop-down list respectively, that according to the local rules.

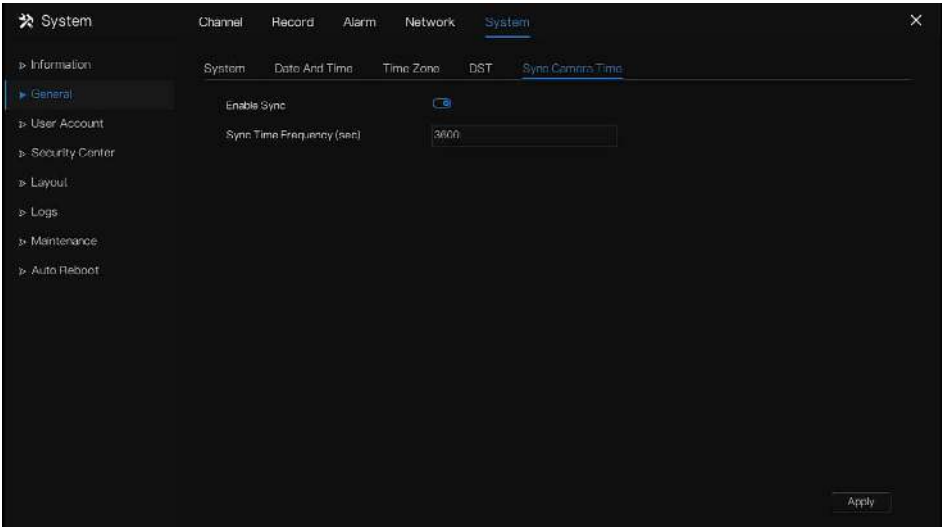
Step 4 Click Apply to save settings.

----End

7.7.2.5 Sync Camera Time

Users enable the sync camera time, the channels will show the sync time, and set the frequency of check.

Figure 7-66 Sync camera time



Enable Sync

Sync Time Frequency (sec) 3600

7.7.3 User

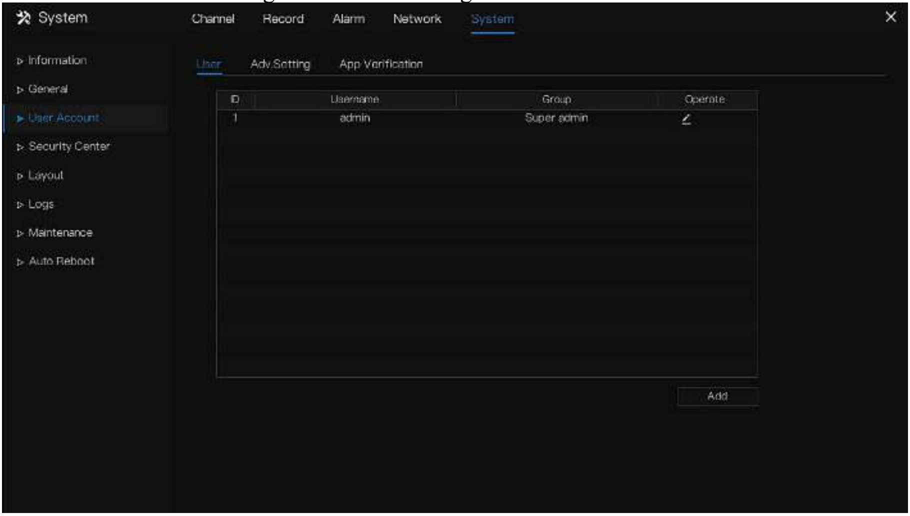
Add, modify, and delete a user and privilege in user screen, admin users can dispose privilege to different users.

7.7.3.1 User

Operation Steps

Step 1 Click **User** in the main menu or menu of the system management screen and choose **User** to access the user screen, as shown in Figure 7-76.

Figure 7-67 User management screen



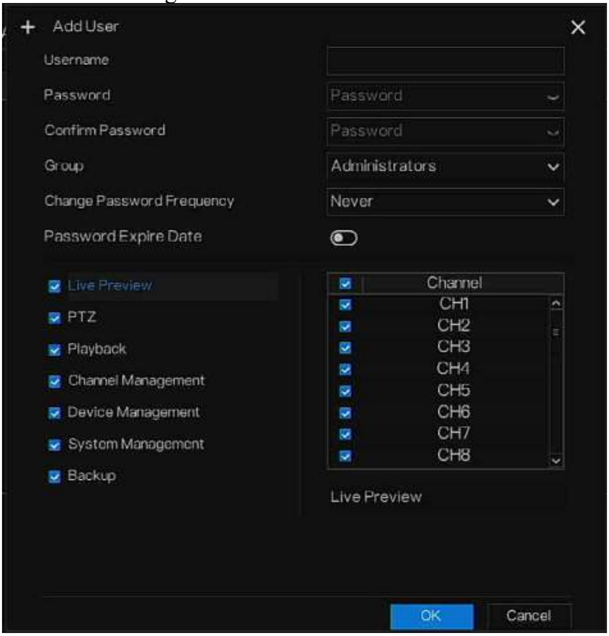
ID	Username	Group	Operate
1	admin	Super admin	✎

Step 2 Add or delete a user.

- Add a user

  Click **Add**, the **Add User** dialog box appears, as shown in Figure 7-77.

Figure 7-68 Add user screen



+ Add User ✕

Username

Password: Password

Confirm Password: Password

Group: Administrators

Change Password Frequency: Never

Password Expire Date: ○

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

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

Live Preview

OK Cancel

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

NOTE

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

The password should be 6~32 characters long.

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

Step 6 Click OK. The user is set successfully.

NOTE

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

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

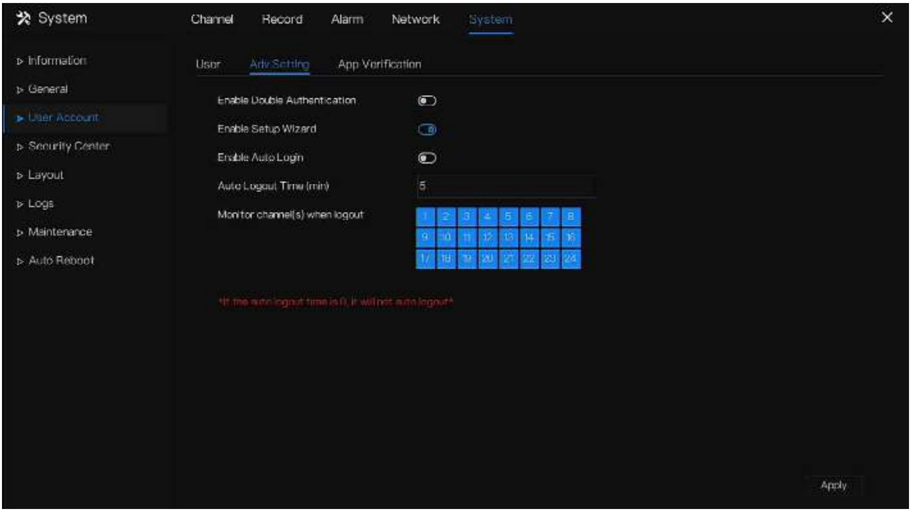
-----End

7.7.3.2 Advance Setting

Operation Steps

Step 1 Click **User** in the main menu or menu of the system management screen and choose **Adv Setting** to access the user screen, as shown in Figure 7-78.

Figure 7-69 Advance setting screen



Enable Double Authentication ○
Enable Setup Wizard ●
Enable Auto Login ○
Auto Logout Time (min) 5
Monitor channel(s) when logout 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

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

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

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

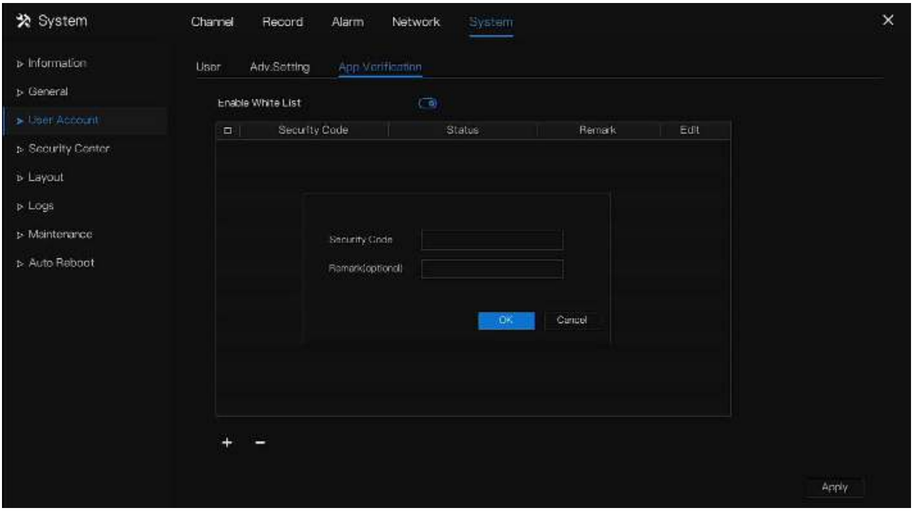
Step 4 Click Apply to save settings.

-----End

7.7.3.3 App Verification

Add the digital number to white list, when the user login the cellphone App to manage the DVR, A series of numbers must be entered in the whitelist for testing and verification to ensure security.

Figure 7-70 Phone number allowed



Up to 20 phone numbers can be added, and remarks of them can be modified.

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

Click Apply to save the setting.

-----End

7.7.4 Security Center

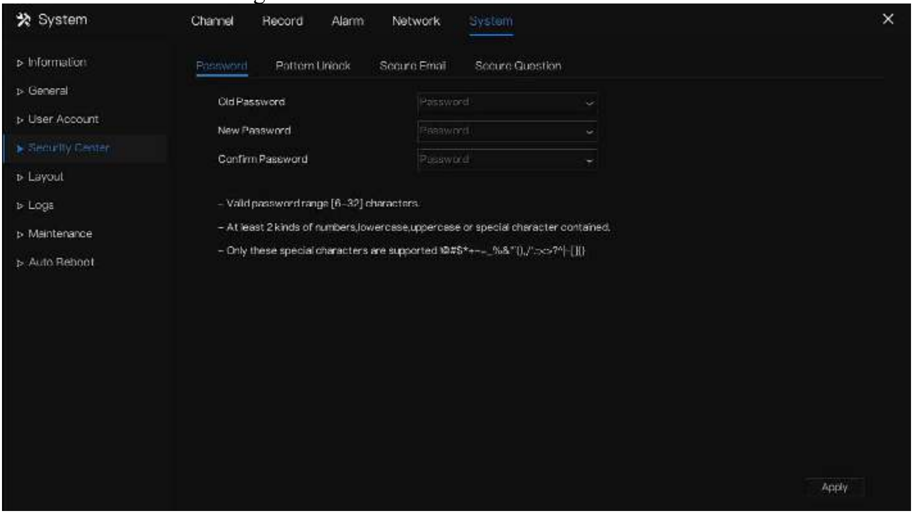
Users can modify the password, pattern unlock, secure email, and secure question.

7.7.4.1 Password

Operation Steps

Step 1 Click **Security Center** in the main menu or menu of the system management screen and choose **Password** to access the modify password screen, as shown in Figure 7-80.

Figure 7-71 Password modification screen



Old Password: Password

New Password: Password

Confirm Password: Password

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

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

NOTE

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

The password should be 6~32 characters long.

Only special characters (! @#$*+=-) are supported,

Step 3 Click Apply to save modified password settings.

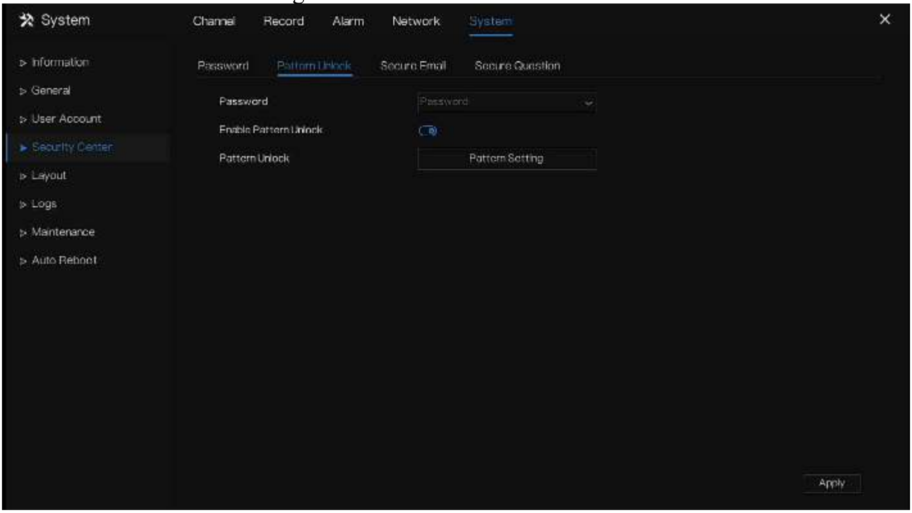
----End

7.7.4.2 Pattern Unlock

Operation Steps

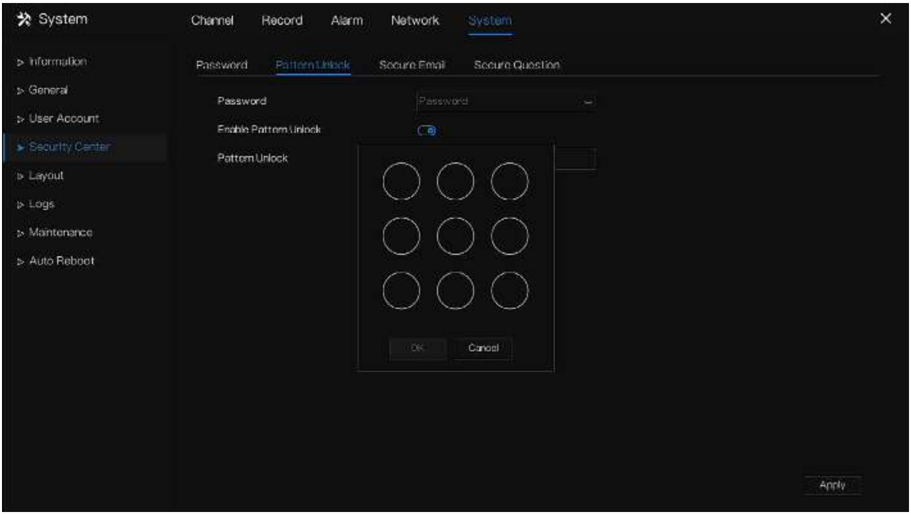
Step 4 Click **Security Center** in the main menu or menu of the system management screen and choose **Pattern Unlock** to access the modify pattern unlock screen, as shown in Figure 7-81.

Figure 7-72 Pattern unlock screen



Step 5 Input the password, click **Setting Pattern** to set an new pattern unlock.

Figure 7-73 Set pattern



Step 6 Draw the pattern, then it will remind to draw the confirmation pattern again.

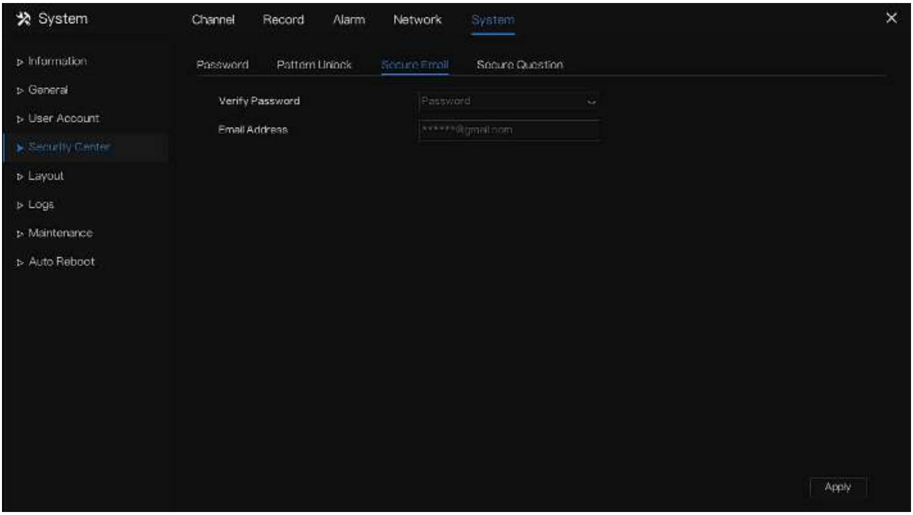
Step 7 Click OK to save the pattern unlock.

----End

7.7.4.3 Secure Email

Set the email to receive the verification code to create a new password, as shown in Figure 7-83.

Figure 7-74 Secure Email screen



Verify Password: Password

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

Step 1 Input the password of DVR.

Step 2 Set the Email which will receive email of the verification code.

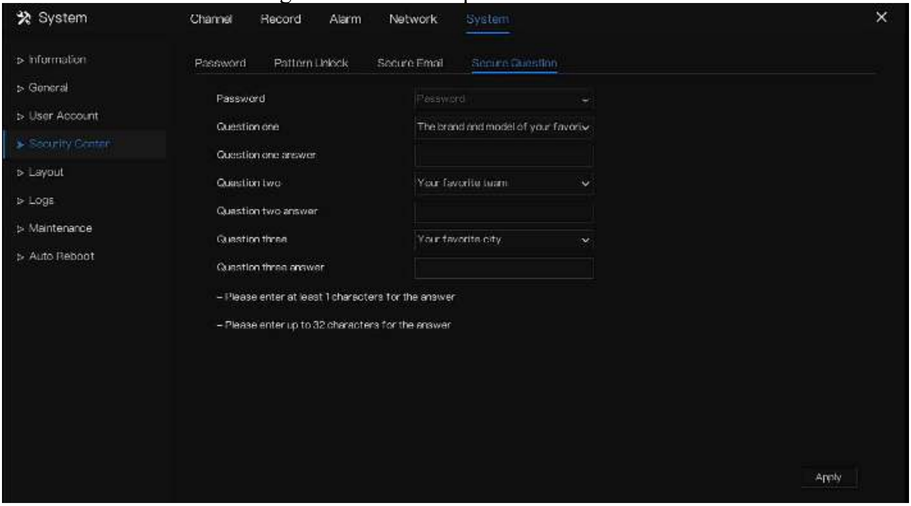
Step 3 Click Apply to save setting.

----End

7.7.4.4 Secure Question

Set the questions to create a new password, as shown in Figure 7-84.

Figure 7-75 Secure question screen



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:

- Please enter at least 1 characters for the answer

- Please enter up to 32 characters for the answer

Step 4 Input the password of DVR.

Step 5 Choose the question from drop-down list.

Step 6 Input the answer, click Apply to save settings.

----End

7.7.5 Layout

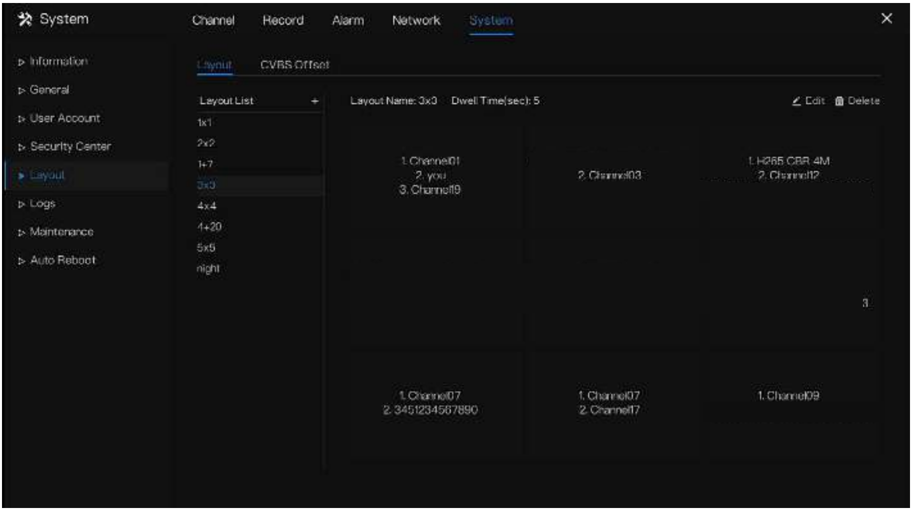
7.7.5.1 Layout

Set viewing video mode, dwell time in display screen. The layout is set as multi-page auto sequence.

Operation Steps

Step 1 Click **Layout** in the main menu or menu of the system management screen and choose **Layout** to access the display screen, as shown in Figure 7-85.

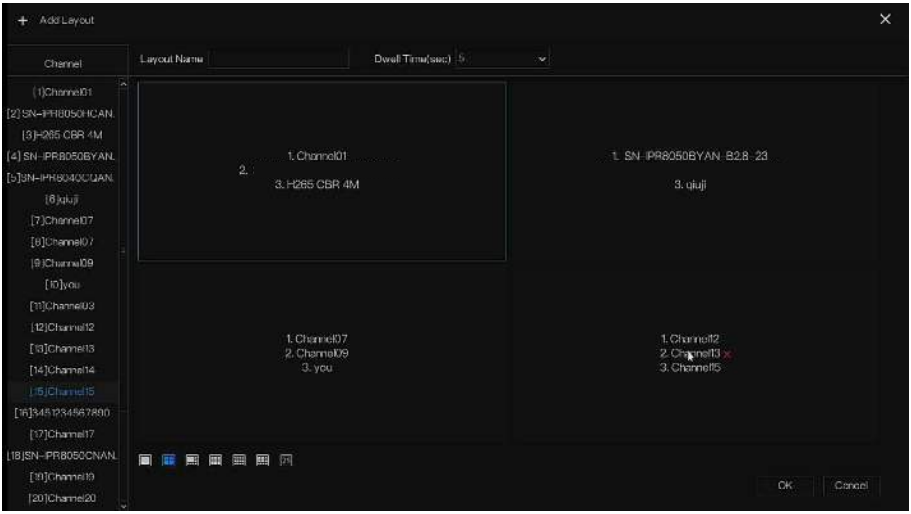
Figure 7-76 Auto Sequence screen



Layout Name: 3x3 Dwell Time(sec): 5

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

Figure 7-77 Add a new layout



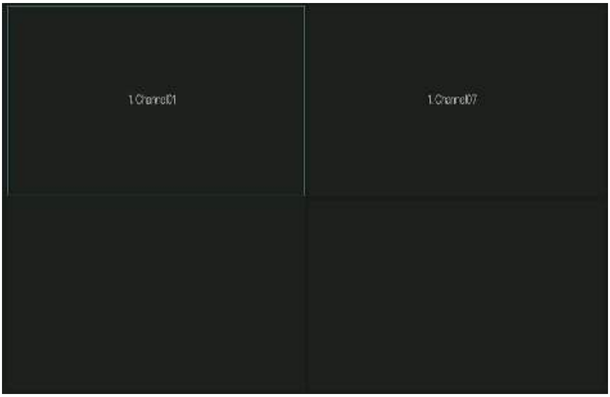
Layout Name

Dwell Time(sec) 5

Step 3 Input the layout name, 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 Choose the mode of splitting screen at the page bottom; set the display mode of channels by dragging channel to the specific location, or choose the location first, then click the channels to place. One splitting screen can play several channels, the auto sequence is played by the set pages, for example the first split screen is set as two pages (channel 1 and 2), the second split screen is set as one page (channel 3), when enable to auto sequence, channel 1 and channel 3, then show channel 2 and channel 3.

Figure 7-78 Auto sequence



Step 5 Click Apply to save dwell settings.

NOTE

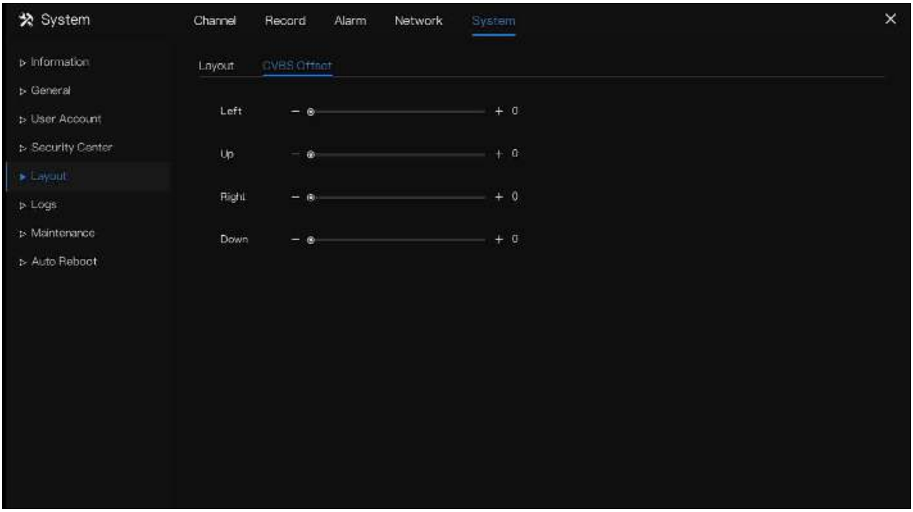
The layout can be added up to 16 layouts.

---End

7.7.5.2 CVBS Offset

The DVR is connected to CVBS monitor via V-out port. Adjust the directions value to set the CVBS monitor’s display.

Figure 7-79 CVBS Offset



Left − + 0

Up − + 0

Right − + 0

Down − + 0

---End

7.7.6 Logs

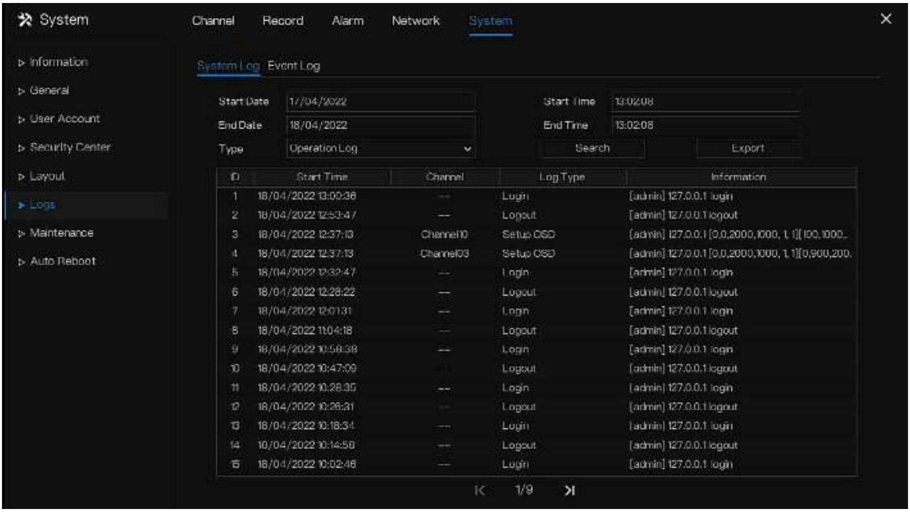
7.7.6.1 System Log

Search for logs information and export the information of logs.

Operation Steps

Step 1 Click **Logs** in the main menu or menu of the system management screen and choose **Logs** to access the log screen, as shown in Figure 7-80.

Figure 7-80 System Log screen



Start Date 17/04/2022
Start Time 13:02:08
End Date 18/04/2022
End Time 13:02:08
Type Operation Log

ID	Start Time	Channel	Log Type	Information
1	18/04/2022 13:00:38	---	Login	[admin] 127.0.0.1 login
2	18/04/2022 12:53:47	---	Logout	[admin] 127.0.0.1 logout
3	18/04/2022 12:37:13	Channel10	Setup OSD	[admin] 127.0.0.1 [0,0,2000,1000, 1, 1][100,1000..
4	18/04/2022 12:37:13	Channel03	Setup OSD	[admin] 127.0.0.1 [0,0,2000,1000, 1, 1][0,900,200.
5	18/04/2022 12:32:47	---	Login	[admin] 127.0.0.1 login
6	18/04/2022 12:28:22	---	Logout	[admin] 127.0.0.1 logout
7	18/04/2022 12:01:31	---	Login	[admin] 127.0.0.1 login
8	18/04/2022 11:04:18	---	Logout	[admin] 127.0.0.1 logout
9	18/04/2022 10:58:38	---	Login	[admin] 127.0.0.1 login
10	18/04/2022 10:47:09	---	Logout	[admin] 127.0.0.1 logout
11	18/04/2022 10:28:35	---	Login	[admin] 127.0.0.1 login
12	18/04/2022 10:26:31	---	Logout	[admin] 127.0.0.1 logout
13	18/04/2022 10:18:34	---	Login	[admin] 127.0.0.1 login
14	18/04/2022 10:14:58	---	Logout	[admin] 127.0.0.1 logout
15	18/04/2022 10:02:46	---	Login	[admin] 127.0.0.1 login

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

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

Step 4 Click Search to query logs.

Step 5 Click Export to export logs to flash disk.

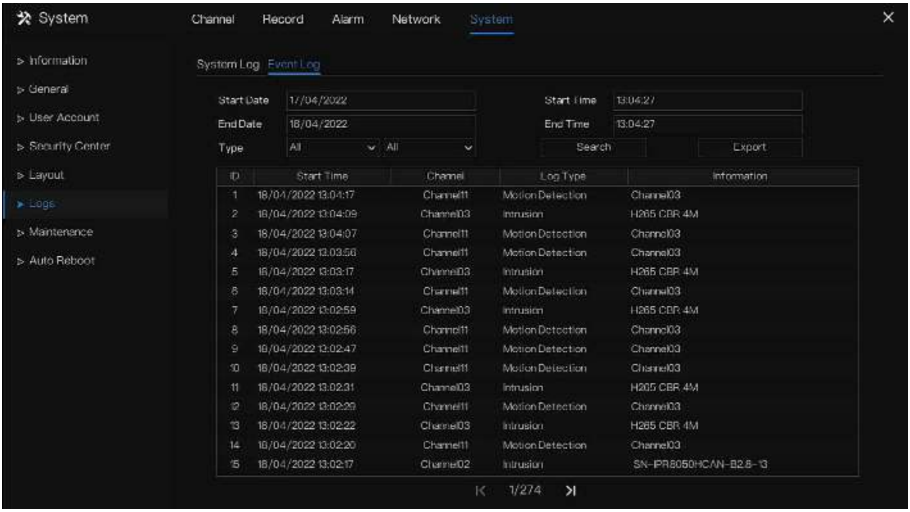
Step 6 Logs can be saved to both flash drive and hard disk, the latest logs are saved to flash drive and the old logs will be transferred to hard disk.

----End

7.7.6.2 Event Log

The event logs are divided into more detailed types, users can find the information quickly. The operation is the same as system logs, please refer to chapter *7.7.6.1*.

Figure 7-81 Event



Start Date 17/04/2022

End Date 18/04/2022

Type All All

Start Time 13:04:27

End Time 13:04:27

ID	Start Time	Channel	Log Type	Information
1	18/04/2022 13:04:17	Channel11	Motion Detection	Channel03
2	18/04/2022 13:04:09	Channel03	Intrusion	H265 CBR 4M
3	18/04/2022 13:04:07	Channel11	Motion Detection	Channel03
4	18/04/2022 13:03:56	Channel11	Motion Detection	Channel03
5	18/04/2022 13:03:17	Channel03	Intrusion	H265 CBR 4M
6	18/04/2022 13:03:14	Channel11	Motion Detection	Channel03
7	18/04/2022 13:02:59	Channel03	Intrusion	H265 CBR 4M
8	18/04/2022 13:02:56	Channel11	Motion Detection	Channel03
9	18/04/2022 13:02:47	Channel11	Motion Detection	Channel03
10	18/04/2022 13:02:39	Channel11	Motion Detection	Channel03
11	18/04/2022 13:02:31	Channel03	Intrusion	H265 CBR 4M
12	18/04/2022 13:02:29	Channel11	Motion Detection	Channel03
13	18/04/2022 13:02:22	Channel03	Intrusion	H265 CBR 4M
14	18/04/2022 13:02:20	Channel11	Motion Detection	Channel03
15	18/04/2022 13:02:17	Channel02	Intrusion	SN-IPR8050HCAN-B2.8-13

1/274

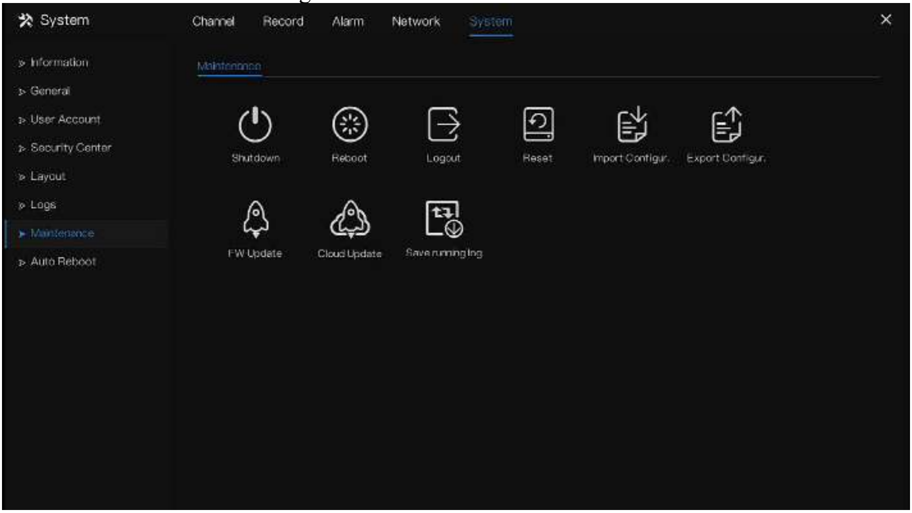
----End

7.7.7 Maintenance

Operation Steps

Step 1 Click **Maintenance** in the main menu or menu of the system management screen and choose **Maintenance** to access the maintenance screen, as shown in Figure 7-82.

Figure 7-82 Maintenance screen



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

Step 3 Click import configuration or export configuration to view the message “ A**re you sure to import the configuration?”** Make sure that the flash driver is working.

Step 4 The tip will show on screen, click **OK** to ensure choice.

Step 5 Click **Import Config** to import the configuration to flash drive.

Step 6 Import the configuration, the device would restart immediately.

Step 7 Click **Export Config** to export the configuration from flash drive.

NOTE

When the DVR finishes updating, the device would restart.

If the device is malfunction, you can save the running log and send it to our technicians who can analyze the cause of the error.

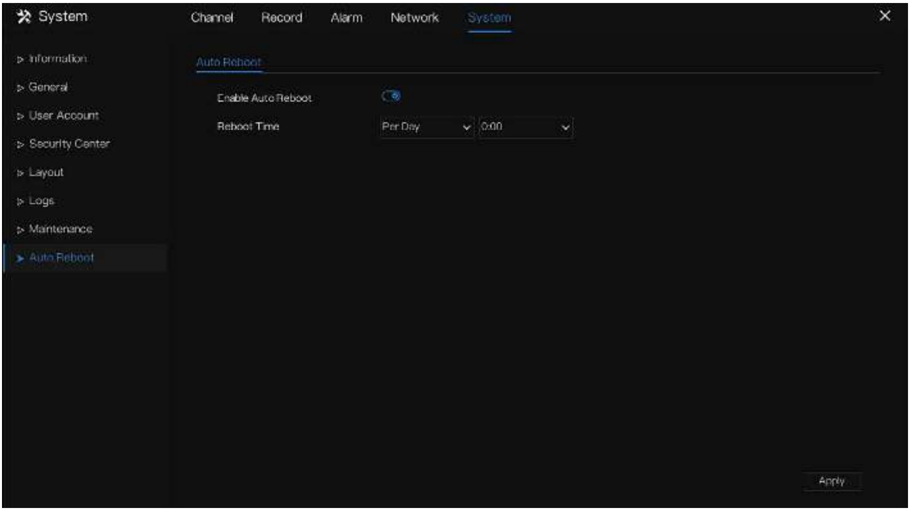
----End

7.7.8 Auto Reboot

Operation Steps

Step 1 Click **Auto restart** in the main menu or menu of the system management screen and choose **Auto restart** to access the maintenance screen, as shown in Figure 7-83.

Figure 7-83 Auto restart screen



Enable Auto Reboot: on

Reboot Time: Per Day, 0:00

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

Restart Time: Per Day, 0:00

Step 3 Restart the DVR per day, week or month.

Step 4 Select the restart time from the drop-down list.

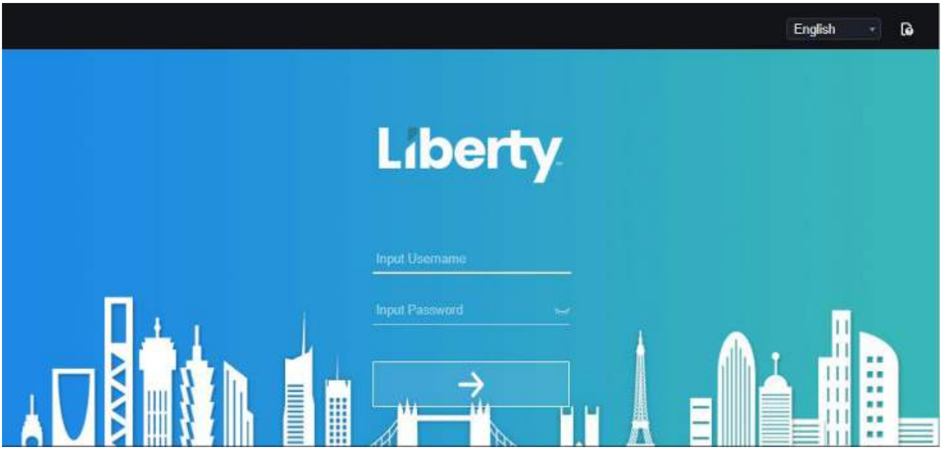
----End

8 WEB Quick Start

8.1 Activation

If you don't set the password at UI interface, activate the device, as shown in Figure 8-1.

Figure 8-1 Activation interface

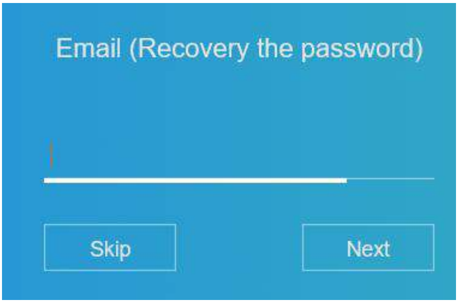


Step 1 Set the password, confirm the password.

Step 2 Input the channel password.

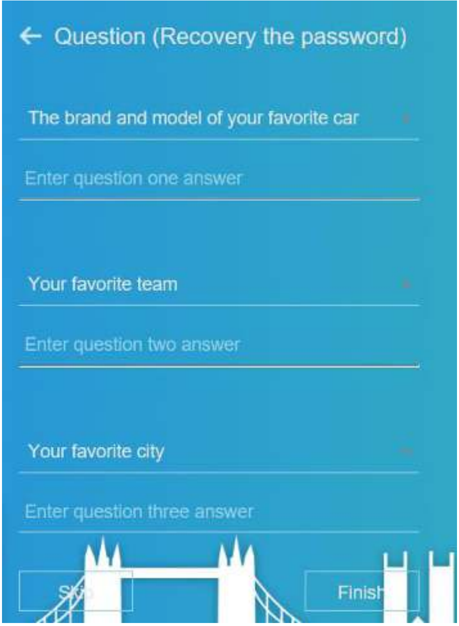
Step 3 Set the email for recovering the password, as shown in Figure 8-2.

Figure 8-2 Email



Step 4 Set the question of recovering the password, as shown in Figure 8-3.

Figure 8-3 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

NOTE

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

8.2 Login and Logout

CAUTION

You must use below Firefox 53 or below Chrome 45 to access the Web interface. Otherwise, the interface functions cannot be used normally.

The win 7/ win 10 system supports IE 8 or more, but the XP system does not.

Brower supports 32 bits.

Descriptions of browser:

To access the client by using Chrome 42-44, you need to enable manually Npapi in the browser according to following steps:

- In the Chrome address bar, enter chrome://flag/#enable-npapi.

- Go to the experimental features' management page.
- Enable NAPAPI Mac, Windows.
- Click **Enable** (NPAPI plugin is enabled).
- Re-launch Chrome.

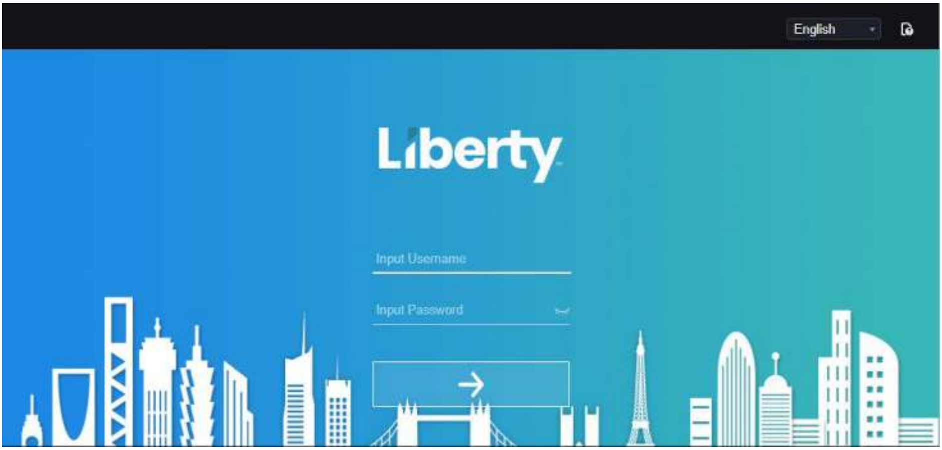
Here we take IE 10 as an example for videos viewing.

Login

Step 1 Open IE browser, enter the IP address of the DVR (DHCP is on by default) in the address box, and press **Enter**.

The login page is displayed, as shown in Figure 8-4.

Figure 8-4 Login page interface



Step 2 Input the user name and password.

NOTE

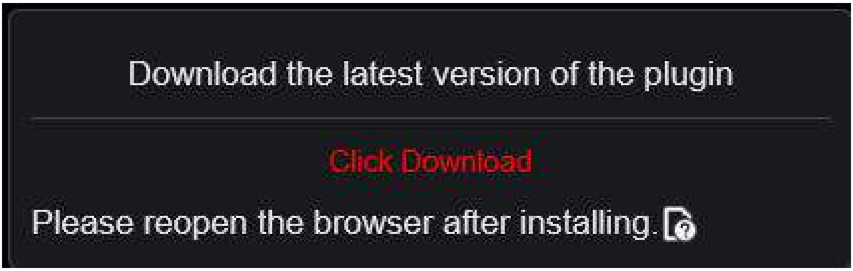
The default user name and password are admin. If the password is wrong more than 3 times, please login again after 5 minutes.

Users can change the system display language on the login page.

The modify password page pop-up window would show when login the DVR for the first time.

Step 3 Click **Login** to access the homepage, it would show reminder to download the latest version of the plugin, as shown in Figure 8-5. Only IE browser need to load the plugin.

Figure 8-5 Download the plugin



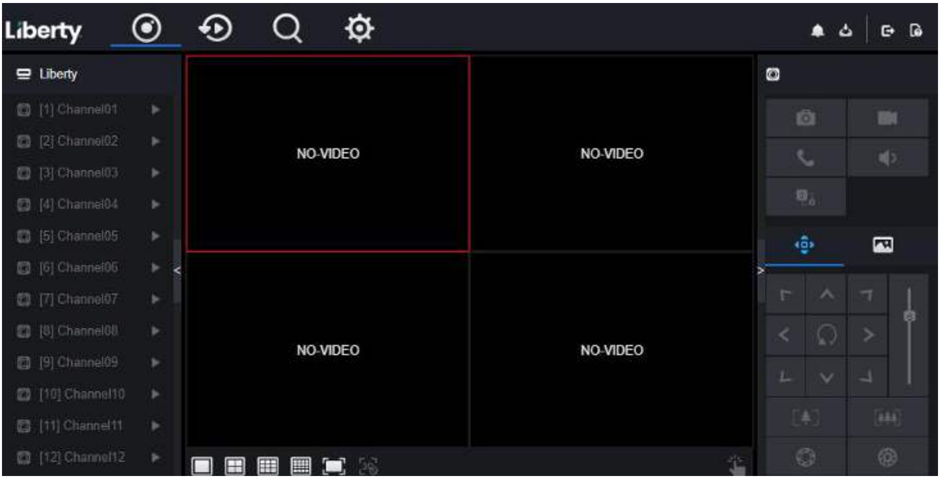
Download the latest version of the plugin

Click Download

Please reopen the browser after installing.

Step 4 Install the latest plugin, reopen the browser and the homepage is displaying as shown in Figure 8-6.

Figure 8-6 Homepage interface



Logout

To logout of the system, click ⇨ in the upper right corner of the homepage. The pop-up message shows “**Do you want to exit?**” Click OK and the login page will display.

Homepage Layout

DVR allows you to use the Web interface in a PC for implementation of such functions as live video, playback, retrieval, setting, image parameters access, configuration, PTZ control and so on.

Figure 8-7 shows the overall layout of the interface. For descriptions of the interface, please refer to Table 8-1.

Figure 8-7 Homepage layout

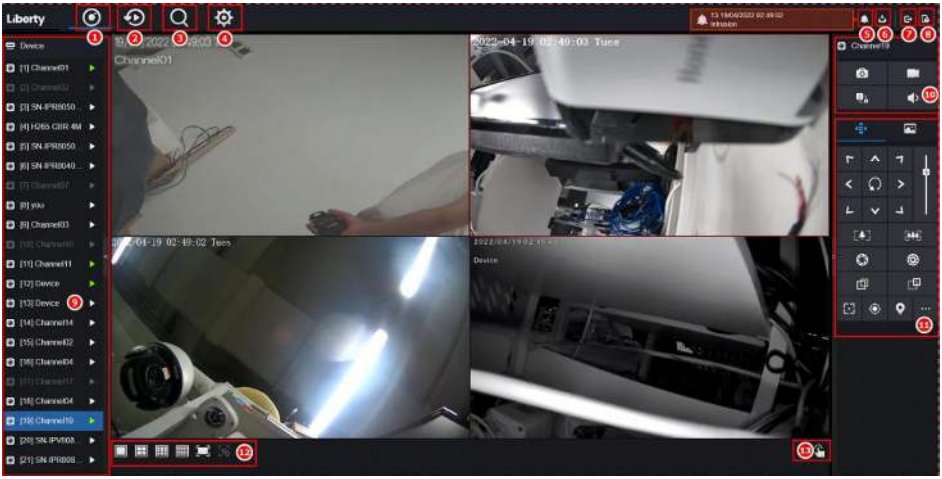


Table 8-2 Descriptions of homepage

No.	Function	Description
1	Live video	Display the real-time videos of the channels managed by DVR
2	Playback	Click to enter playback interface.
3	Alarm search	Click to enter alarm search interface to search channel alarm or system alarm.
4	System setting	Click to enter system setting interface, set channel, recorded, alarm, network, system and local settings.
5	Alarm	Alarm notification. Users can tick pop-up message to monitor, system alarm and channel alarm.
6	Download backup	The histories of backup, and the process of download.
7	Logout button	Users can click **Logout** to exit the current account and return to the login interface.
8	Help	Help for running environment, plug-in installation and activation.

9	Devices list	Display a list of the channels of the managed DVR and the channels managed by DVR.
10	Channel Operation	Include snapshot, record, stream switch and audio on/off.
11	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.
	Color 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.
	Operation zone	The operation zone of PTZ control and image parameter setting.
12	Layouts	Select the one-screen, four-screen, nine-screen or sixteen- screen to switch the layout.
13	Manual alarm	Trigger and close the external alarm device manually.

----End

8.3 Browsing Videos

8.3.1 Browsing Real-Time Videos

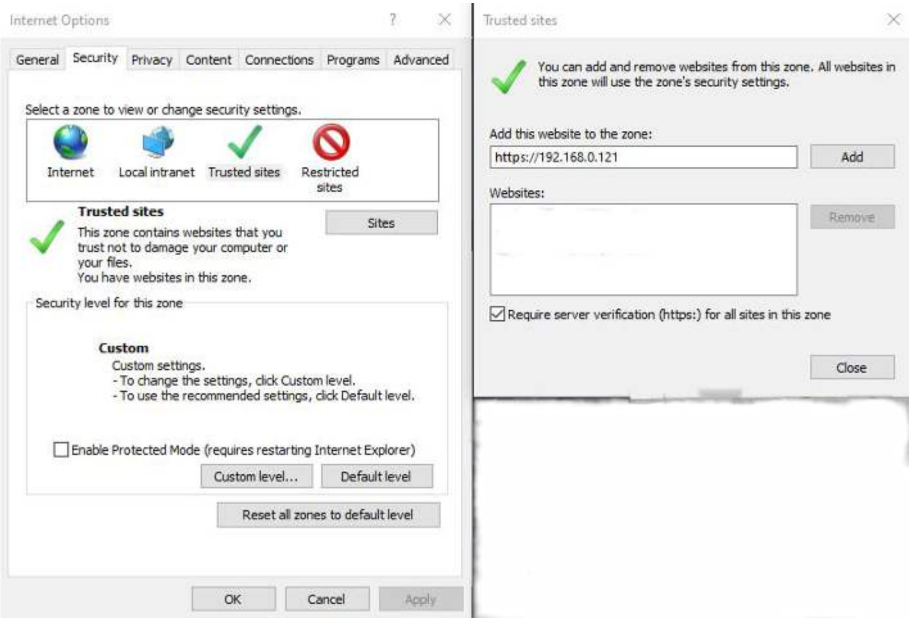
You can browse real-time videos in the web management system.

Preparation

To ensure that real-time videos can be played properly, users must perform the following operations when you log in to the web management system for the first time:

Step 1 Open Internet Explorer. Choose **Tools > Internet Options > Security > Trusted sites > Sites**. In the displayed dialog box, click **Add**, as shown in Figure 8-8.

Figure 8-8 Adding a trusted site



Select a zone to view or change security settings.

Trusted sites

This zone contains websites that you trust not to damage your computer or your files.
You have websites in this zone.

Security level for this zone

Custom

Custom settings.
- To change the settings, click Custom level.
- To use the recommended settings, click Default level.

□ Enable Protected Mode (requires restarting Internet Explorer)

You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

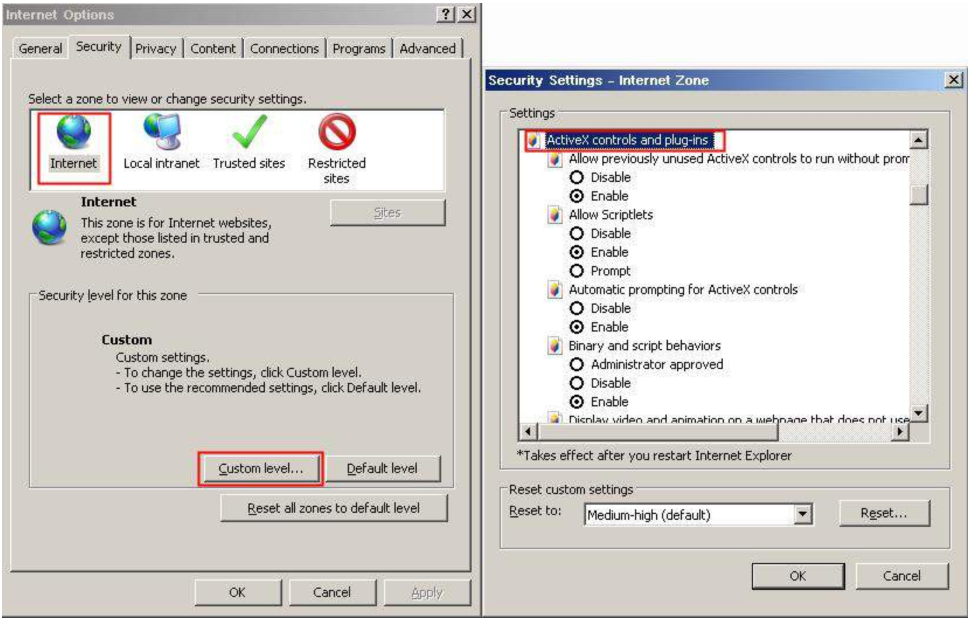
Add this website to the zone:
https://192.168.0.121

Websites:

☑ Require server verification (https:) for all sites in this zone

Step 2 In Internet Explorer, choose **Tools > Internet Options > Security > Customer level**, and set Download unsigned ActiveX controls and Initialize and script ActiveX controls not marked as safe for scripting under ActiveX controls and plug-ins to Enable, as shown in Figure 8-9.

Figure 8-9 Configuring ActiveX controls and plug-ins



Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

Select a zone to view or change security settings.

Internet | Local intranet | Trusted sites | Restricted sites

Internet

This zone is for Internet websites, except those listed in trusted and restricted zones.

Sites

Security level for this zone

Custom

Custom settings.

- To change the settings, click Custom level.
- To use the recommended settings, click Default level.

Custom level... | Default level

Reset all zones to default level

OK | Cancel | Apply

Security Settings - Internet Zone

Settings

ActiveX controls and plug-ins

Allow previously unused ActiveX controls to run without prom

○ Disable
● Enable

Allow Scriptlets

○ Disable
● Enable
○ Prompt

Automatic prompting for ActiveX controls

○ Disable
● Enable

Binary and script behaviors

○ Administrator approved
○ Disable
● Enable

Display video and animation on a webpage that does not use

*Takes effect after you restart Internet Explorer

Reset custom settings

Reset to: Medium-high (default)

Reset...

OK | Cancel

Step 3 Download and install the player control as prompted. During installing, you need to close the browser.

NOTE

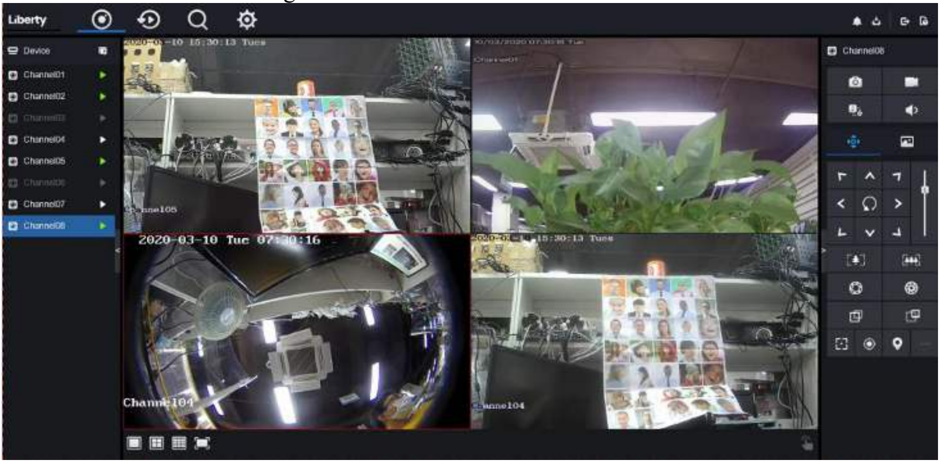
If the repair tips displayed when installing the control , close the browser and continue the installation, reopen the login page when the control is installed.

8.3.2 Live Video

Descriptions

After login the device, click online channel, you can view the real-time videos, as shown in Figure 8-10.

Figure 8-10 Real-time videos interface



----End

8.3.3 Channel Operation

Descriptions

Channel operation includes snapshot, record, stream switch and audio on/off. Table 8-2 describes the operations.

Table 8-3 Descriptions of homepage

Buttons	Button description	How to operate
📷	Snapshot	Click button to take snapshots of the current image.
📹	Record	Click button to start recording and click button again to stop recording.
2	Switch stream	Click button to switch stream 1 (main stream) and stream 2(sub stream).
🔈	Enable/Disable video	Click button to enable the audio and click again to disable the video.

----End

8.3.4 PTZ Control and Setting

NOTE

The PTZ control is only used for some cameras, such as high speed cameras which rotate and adjust the lens. For monitored lens cameras can zoom /focus /iris. For actual operations please refer to actual product.

Descriptions

The PTZ control and setting function only applies to Network Dome or cameras connected to an external PTZ.

PTZ Setting

If a Network Dome or a camera connected to PTZ had been added to the DVR channel, users can control the PTZ rotation to adjust their shooting angle when you are viewing the video. This allows you to perform Omni-directional video surveillance.

Click , the PTZ operation and setting interface is displaying, as shown in Figure 8-11. Table 8-3 describes the operations.

Figure 8-11 PTZ control interface

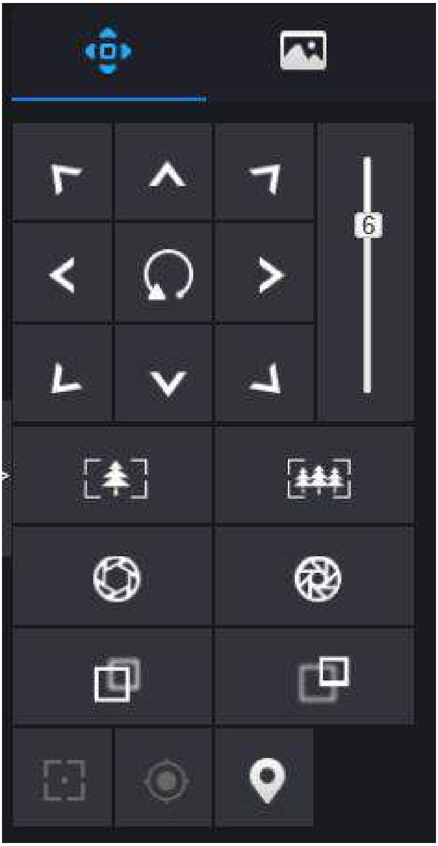
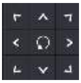
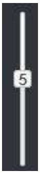


Table 8-4 Device parameters

Buttons	Button description	How to operate
	Direction key	Click button to control omni-directional movement of the PTZ.
	Speed slider	Drag the slider to adjust the value of PTZ rotation speed.

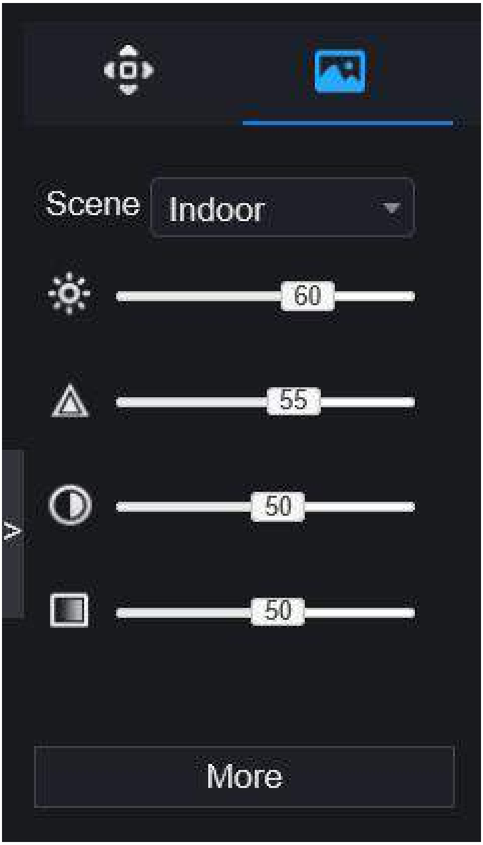
Buttons	Button description	How to operate
🌲	Zoom in	Click buttons to adjust the focal length.
🌲🌲🌲	Zoom out	
◎	Iris+	Click buttons to adjust the aperture.
◎	Iris-	
⧉	Far focus	Click buttons to adjust the focal length.
⧉	Near focus	
⛶	Auto focus	Click button to focus automatically.
◉	Home preset	N/A
📍	Preset	The camera is set the tour, click the button and dome camera rotate as the setting.
···	More	More settings

8.3.5 Sensor Setting

Descriptions

The sensor setting can adjust scene, brightness, sharpness, contrast and saturation, Click 🖼 to access image setting, as shown in Figure 8-12. Table 8-4 describes the operations.

Figure 8-12 Image parameter interface



Scene Indoor

☼ 60

△ 55

◐ 50

▣ 50

More

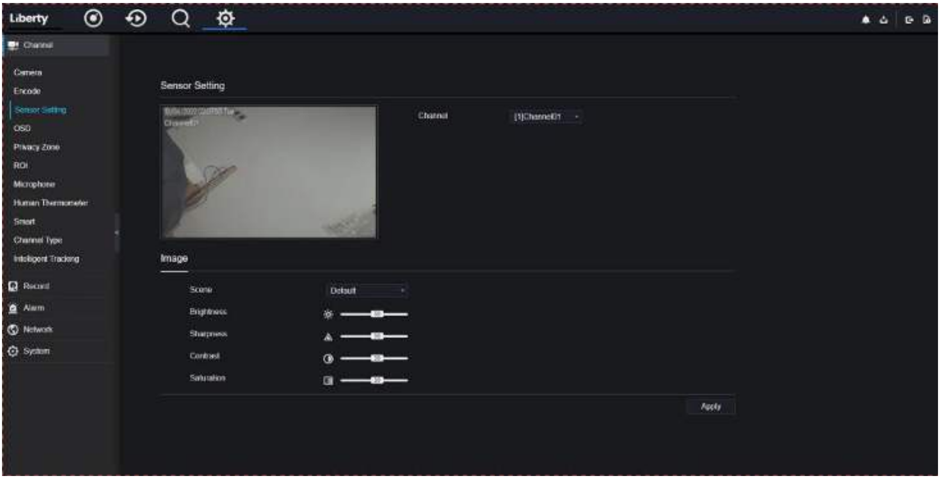
Table 8-5 Device parameters

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

Buttons	Button description	How to operate
▨	Saturation	Click button to adjust the chromatic purity of the image.

Click more will be access to system sensor setting. As shown in Figure 8-13, more detail please refer to *chapter Figure 4-7*.

Figure 8-13 Sensor setting interface



Channel [1]Channel01

Scene Default

Brightness

Sharpness

Contrast

Saturation

----End

8.3.6 Layout

Click □ ⊞ ▦ at the bottom left conner of real-time videos interface, the buttons indicate 1 screen, 4 screens and 9 screens from left to right. 16 screens need more ports.

----End

8. 4 Playback

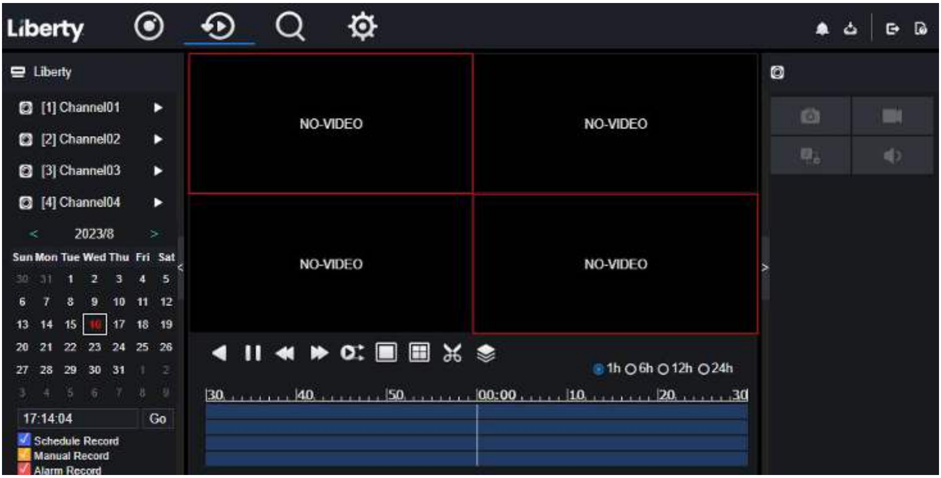
8.4.1 Video Playback

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

Procedure

Step 1 Click in the function navigation bar, the video playback interface is displayed, as shown in Figure 8-14.

Figure 8-14 Video playback



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

An unselected device is marked with ▶.

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

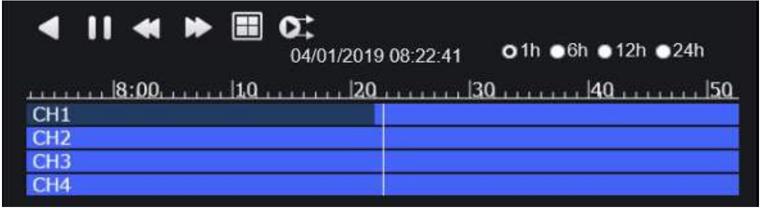
The file axis displays videos. The blue file axis indicates a video exits, grey file axis indicates no video exits.

You can drag the axis to play recording quickly.

Step 6 Play a video.

You can play a video after selecting a device and date. Figure 8-15 shows the control bar of video playback.

Figure 8-15 Control bar



◀: Reversed.

❚❚: Play/pause.

⏪ ⏩: Triple speed.

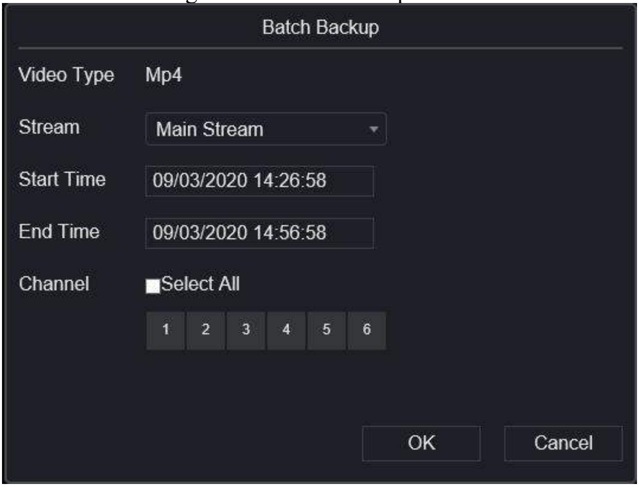
⊞: Split screen. One or four screens.

: Sync/async. You can set the different channels to play synchronously or asynchronous. Sync mode indicates the selected channels play video synchronously. Async mode indicates user play different time period record

✂ : Backup, click the icon to download the recording video, click again to end the download.

: Batch backup, click the icon to backup many channels' recording videos, as shown in Figure 8-16.

Figure 8-16 Batch backup



Batch Backup

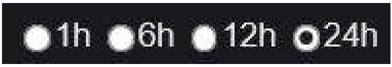
Video Type Mp4

Stream: Main Stream

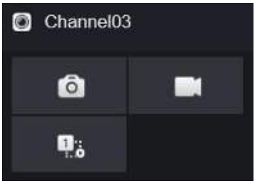
Start Time: 09/03/2020 14:26:58

End Time: 09/03/2020 14:56:58

Channel: ■Select All



: Types of time bar.



: Users can operate the record as same as live video.

----End

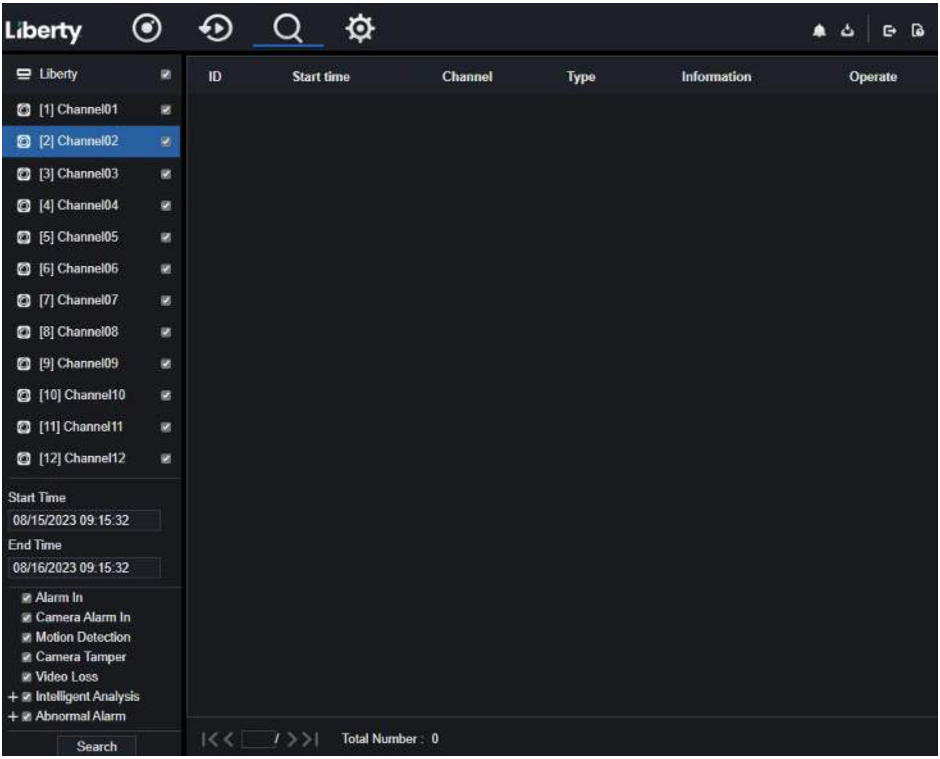
8.5 Alarm Search

You can search for different alarm messages at the alarm search interface.

Procedure

Step 1 Click 🔍 in the function navigation bar, the channel alarm interface is displayed, as shown in Figure 8-17.

Figure 8-17 Alarm search interface



Liberty

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

Start Time: 08/15/2023 09:15:32

End Time: 08/16/2023 09:15:32

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

Search

ID	Start time	Channel	Type	Information	Operate

|< < / > >| Total Number : 0

Step 2 Tick channels and types, set start time and end time.

Step 3 Click **Search**, the result will be displayed as shown in Figure 8-17.

Step 4 Click ⟲ to play the recording.

Step 5 Click ⤓ to download the recording.

NOTE

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

Every page show 20 ▾ shows the rows shown in every page.

----End

9 System Setting

The system setting allows you to set system, channel, record, alarm, network and local setting.

9.1 Channel

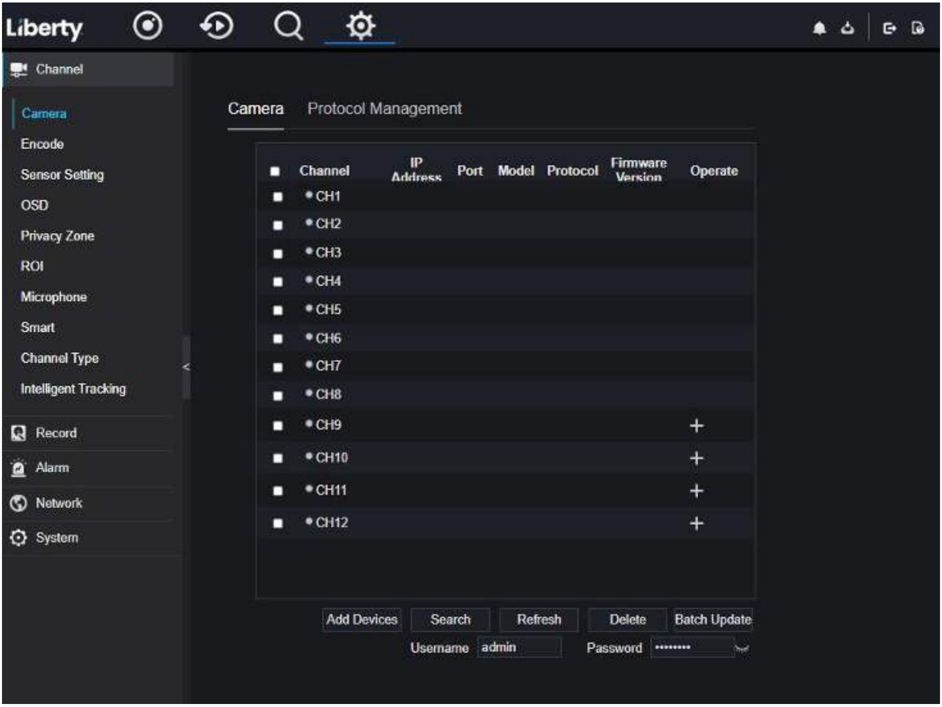
Users can set parameters about camera, encode, sensor setting, OSD and privacy zone.

9.1.1 Camera

9.1.1.1 Camera

Step 1 On the **System Setting** screen, choose **Channel > Camera** to access the camera interface, as shown in Figure 9-1.

Figure 9-1 Camera interface



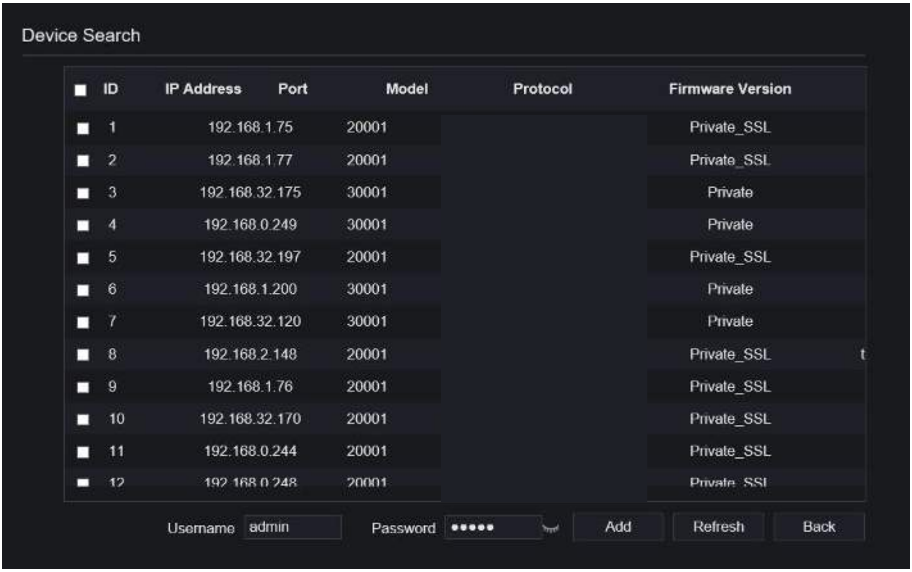
■	Channel	IP Address	Port	Model	Protocol	Firmware Version	Operate
■	• CH1						
■	• CH2						
■	• CH3						
■	• CH4						
■	• CH5						
■	• CH6						
■	• CH7						
■	• CH8						
■	• CH9						+
■	• CH10						+
■	• CH11						+
■	• CH12						+

Username admin Password ••••••••

Step 2 Input username and password (both default values are admin), and click Click To Add add cameras automatically.

Step 3 Click Search to search cameras at the same LAN as DVR, as shown in Figure 9-2. Choose the camera, input username and password, click **Add** to add new cameras.

Figure 9-2 Device search



Device Search

■	ID	IP Address	Port	Model	Protocol	Firmware Version
■	1	192.168.1.75	20001			Private_SSL
■	2	192.168.1.77	20001			Private_SSL
■	3	192.168.32.175	30001			Private
■	4	192.168.0.249	30001			Private
■	5	192.168.32.197	20001			Private_SSL
■	6	192.168.1.200	30001			Private
■	7	192.168.32.120	30001			Private
■	8	192.168.2.148	20001			Private_SSL
■	9	192.168.1.76	20001			Private_SSL
■	10	192.168.32.170	20001			Private_SSL
■	11	192.168.0.244	20001			Private_SSL
■	12	192.168.0.248	20001			Private_SSL

Username admin Password ●●●●●

Step 4 Click Back to back to camera interface.

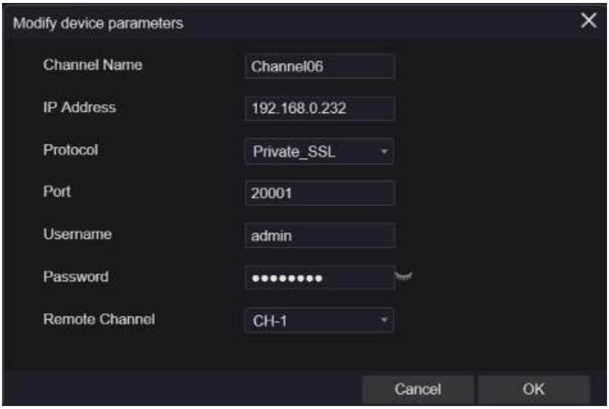
Step 5 Click Refresh to refresh cameras status.

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 would show to select software.

Step 8 Click ✎ to modify the information of device parameters, as shown in Figure 9-3.

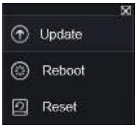
Figure 9-3 Modify device parameters



Modify device parameters

Channel Name	Channel06
IP Address	192.168.0.232
Protocol	Private_SSL
Port	20001
Username	admin
Password	●●●●●●●●●
Remote Channel	CH-1

Step 9 Click e to access web immediately.

Step 10 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.

NOTE

🟢: it indicates the camera is online, users can view the live video immediately.

🔴: it indicates the camera is offline, it maybe not connected to the network, or the password is incorrect. User access to the modify device parameters interface to change.

9.1.1.2 Protocol Management

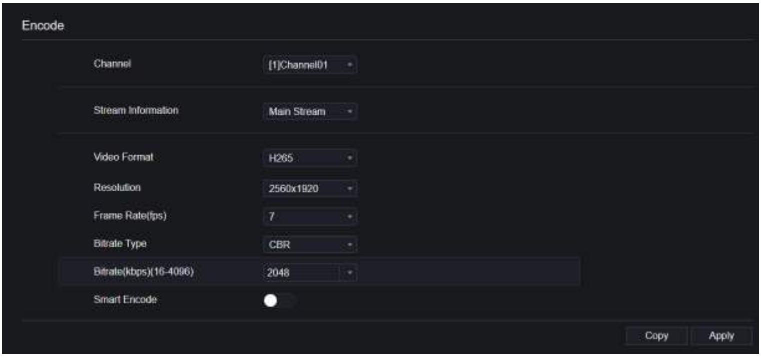
At protocol management, you can set the custom protocol for adding cameras. For more details please refer *7.3.1.5Protocol Management*

Figure 9-4 Protocol management

9.1.2 Encode

Step 1 On the **System Setting** screen, choose **Channel > Encode** to access the encode interface, as shown in Figure 9-5.

Figure 9-5 Encode interface



Encode

Channel: [1]Channel01

Stream Information: Main Stream

Video Format: H265

Resolution: 2560x1920

Frame Rate(fps): 7

Bitrate Type: CBR

Bitrate(kbps)(16-4096): 2048

Smart Encode: ●

Step 2 Select a channel from drop-down list.

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

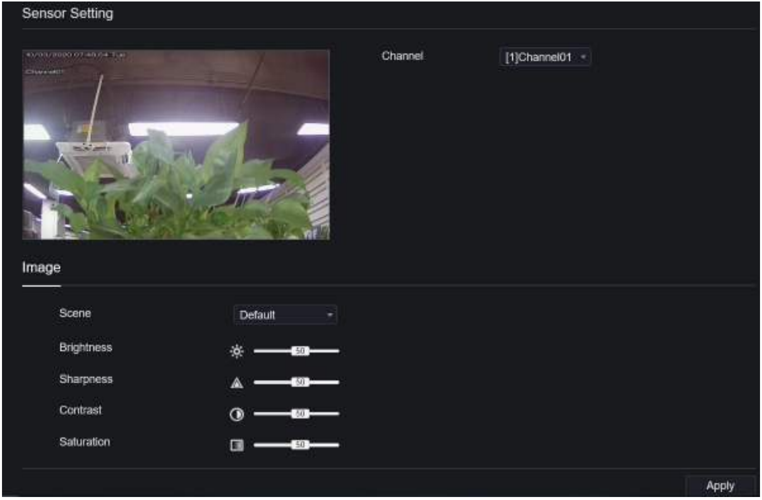
Step 4 Click Copy to choose other cameras to copy settings. Click Apply to save the settings.

----End

9.1.3 Sensor Setting

Step 1 On the **System Setting** screen, choose **Channel >Sensor Setting** to access the sensor setting interface, as shown in Figure 9-6.

Figure 9-6 Image interface



Sensor Setting

Channel [1]Channel01

Image

Scene Default

Brightness 50

Sharpness 50

Contrast 50

Saturation 50

Apply

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

Step 3 Set image parameters, like scene, brightness, sharpness, contrast and saturation.

Step 4 Other parameters are for camera's sensor setting, please refer IP cameras' settings.

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

NOTE

The analog cameras can only adjust the image parameters.

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; the smaller the difference range is, the smaller the contrast.

Scene: It includes indoor, outdoor, default. Mirror includes normal, horizontal, vertical, horizontal + vertical.

Exposure: It includes mode, max shutter, meter area and max gain.

White balance: It includes tungsten, fluorescent, daylight, shadow, manual, etc.

Day-night: Users can transit day to night, or switch mode.

Noise reduction: It includes 2D NR and 3D NR.

Enhance image: It includes WDR, HLC, BLC, defog and anti-shake.

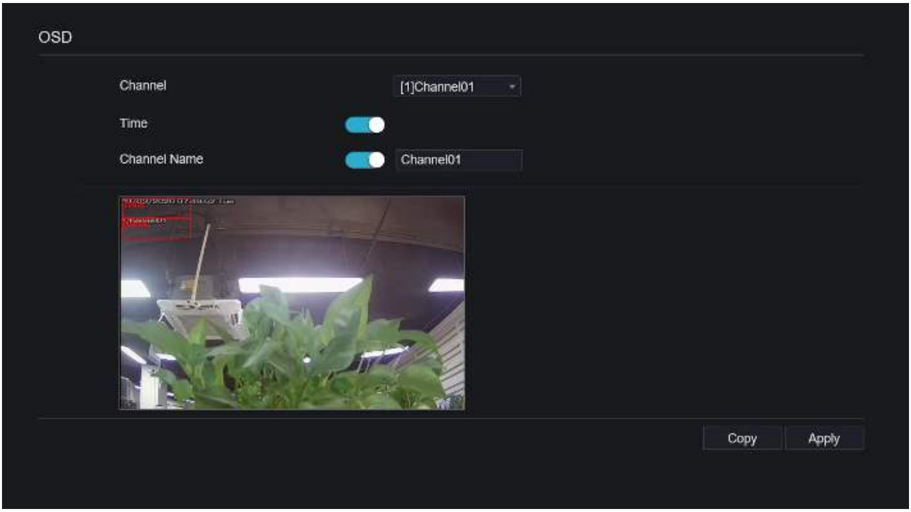
Zoom focus: Users can zoom and focus.

----End

9.1.4 OSD

Step 1 On the **System Setting** screen, choose **Channel >OSD** to access the OSD interface, as shown in Figure 9-7.

Figure 9-7 OSD interface



OSD

Channel: [1]Channel01

Time: ●

Channel Name: ● Channel01

Step 2 Select a channel and scene from drop list.

Step 3 Enable time and channel name. You can set channel name. Drag the icon of Channel Name or Date and Time to move, select the location.

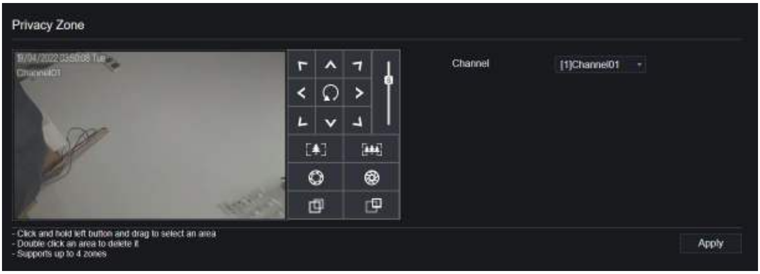
Step 4 Click Copy to copy settings to other cameras. Click Apply to save the settings.

----End

9.1.5 Privacy Zone

Step 1 On the **System Setting** screen, choose **Channel > Privacy Zone** to access the privacy zone interface, as shown in Figure 9-8.

Figure 9-8 Privacy interface



Privacy Zone

Channel [1]Channel01

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

Apply

Step 2 Select a channel from drop-down list .

Step 3 Drag the mouse to select area to cover with rectangle frame. You can set less than four areas to be covered. Double click to delete the area.

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

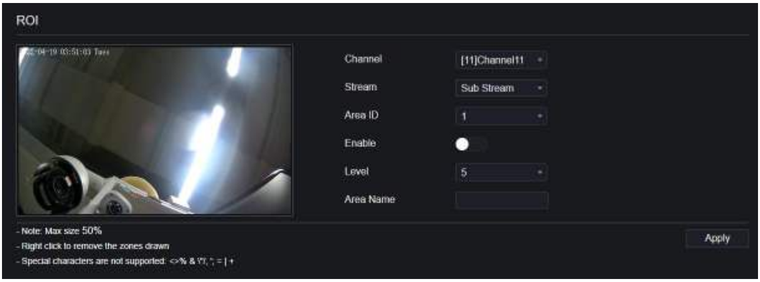
Step 5 Click Copy to copy settings to other cameras. Click Apply to save the settings.

----End

9.1.6 ROI

ROI(Region of interest), choose channel, stream, area ID and draw the area, as shown in Figure 9-9. Set the level, there are five levels can be chosen. Set area name, click “Apply” to save the settings.

Figure 9-9 ROI interface



ROI

Channel: [11]Channel11

Stream: Sub Stream

Area ID: 1

Enable: ○

Level: 5

Area Name:

- Note: Max size 50%
- Right click to remove the zones drawn
- Special characters are not supported: <>% & \'/, "; = | +

Apply

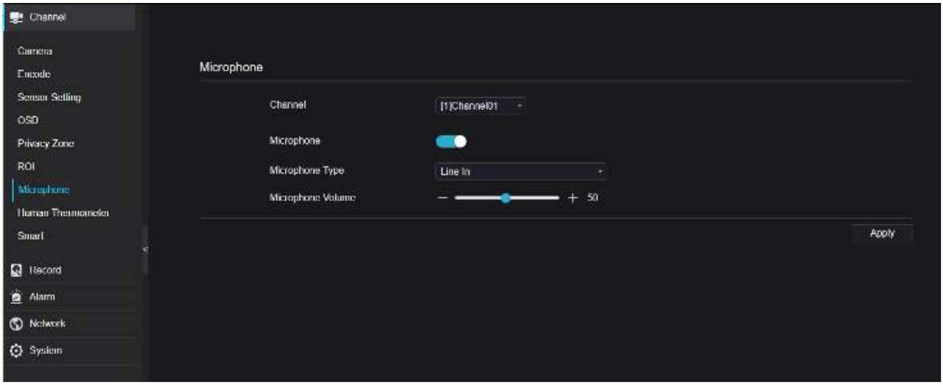
9.1.7 Microphone

NOTE

This function is only applicable to some models with microphone.

Users can set the microphone parameters of channel, as shown in Figure 9-10.

Figure 9-10 Microphone interface



Microphone

Channel: [1]Channel01

Microphone: ●

Microphone Type: Line In

Microphone Volume: − + 50

Apply

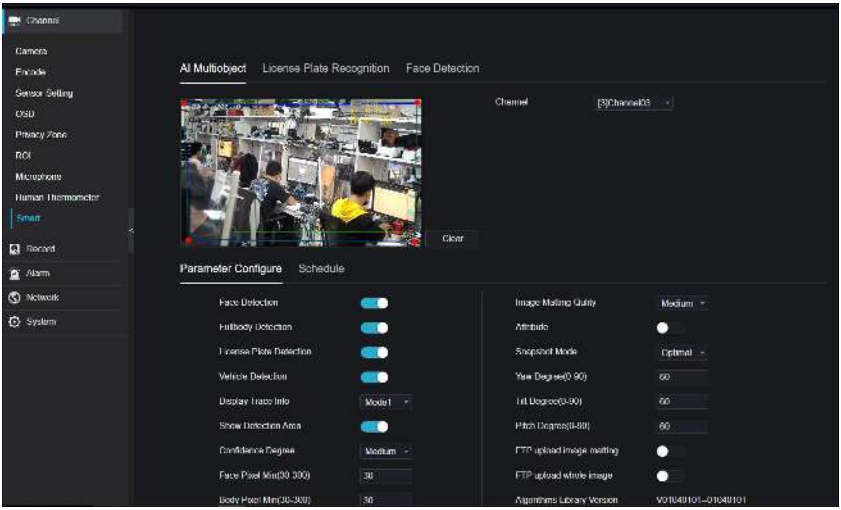
9.1.8 Smart

NOTE

This function is only applicable to some models.

At smart interface, users can set AI multiobject, license plate recognition, face detection, as shown in Figure 9-11.

Figure 9-11 Smart interface



Channel [3]Channel03

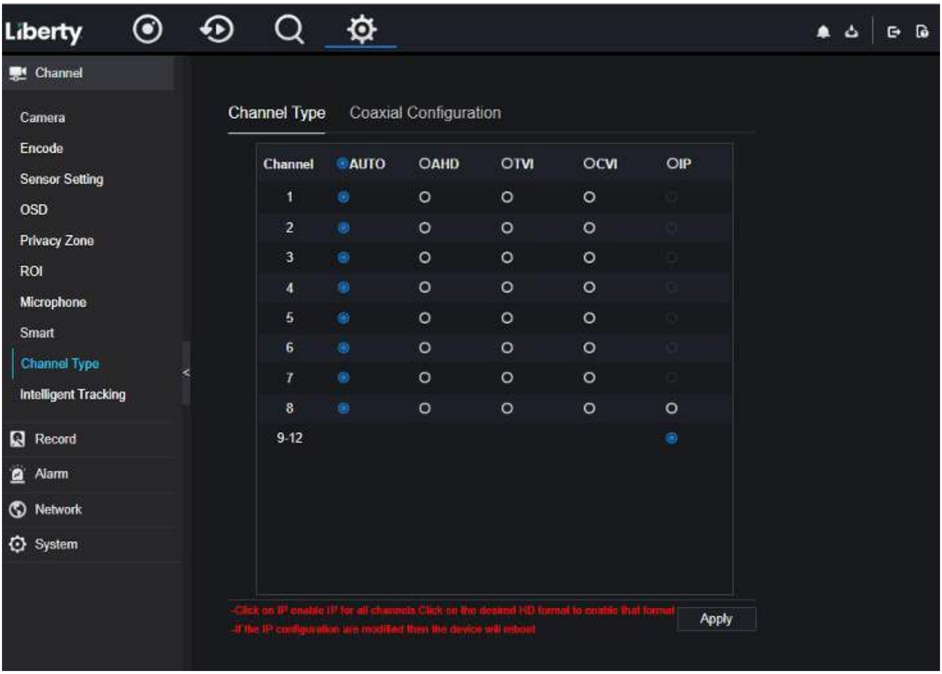
Face Detection ●
Fullbody Detection ●
License Plate Detection ●
Vehicle Detection ●
Display Trace Info Mode1
Show Detection Area ●
Confidence Degree Medium
Face Pixel Min(30-300) 30
Body Pixel Min(30-300) 30

Image Matting Qulity Medium
Attribute ○
Snapshot Mode Optimal
Yaw Degree(0-90) 60
Tilt Degree(0-90) 60
Pitch Degree(0-90) 60
FTP upload image matting ○
FTP upload whole image ○
Algorithms Library Version V01040101--01040101

9.1.9 Channel Type

Set the analog channels type, the bottom channel should be set first, or set all analog channels at once.

Figure 9-12 Channel type interface



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

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

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

----End

9.1.10 Intelligent Tracking

NOTE

This function is only applicable to some models (high speed PTZ camera).

More detail information please refer to *7.3.11 Intelligent Tracking (Only for Some Model)*

9.2 Record

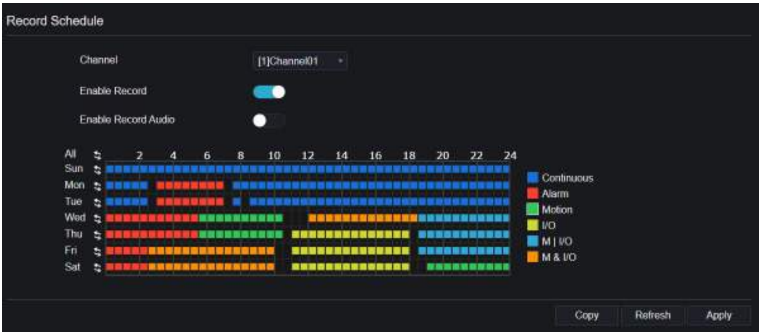
Users can set record policy in storage interface.

9.2.1 Record Schedule

Procedure

Step 1 On the **System Setting** screen, choose **Record > Record schedule** to access the record schedule interface, as shown in Figure 9-13.

Figure 9-13 Record schedule interface



Record Schedule

Channel [1]Channel01

Enable Record

Enable Record Audio

Step 2 Select a channel .

Step 3 Enable the record, then enable record audio.

Step 4 Set the record schedule, you can drag the mouse to choose area, click ⇅ to choose all day or all week, you can also click one by one to set the schedule. Or dray the mouse cursor to choose. Users can set the alarm recording to save the space of disk.

Step 5 Click Refresh to return the previous settings.

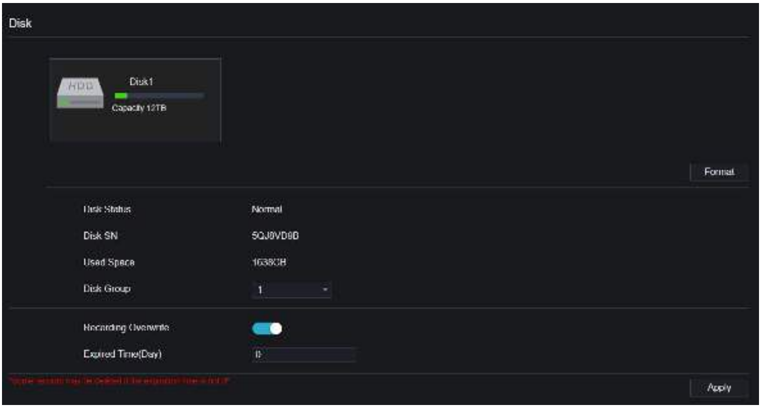
Step 6 Click Copy to copy settings to other cameras. Click Apply to save the settings.

----End

9.2.2 Disk

Step 1 On the **System Setting** screen, choose **Record >Disk** to access the disk interface, as shown in Figure 9-14.

Figure 9-14 Disk interface



Disk Status: Normal

Disk SN: 5QJ8VD8B

Used Space: 1638GB

Disk Group: 1

Recording Overwrite: ●

Expired Time(Day): 0

Step 2 You can view the information like capacity, disk status, disk SN code and used space.

Step 3 Click Format to delete all data. Before deleting data user will view pop-up window

“ Are you sure to format disk? Your data will be lost”. Click OK to delete, click

Cancel to quit.

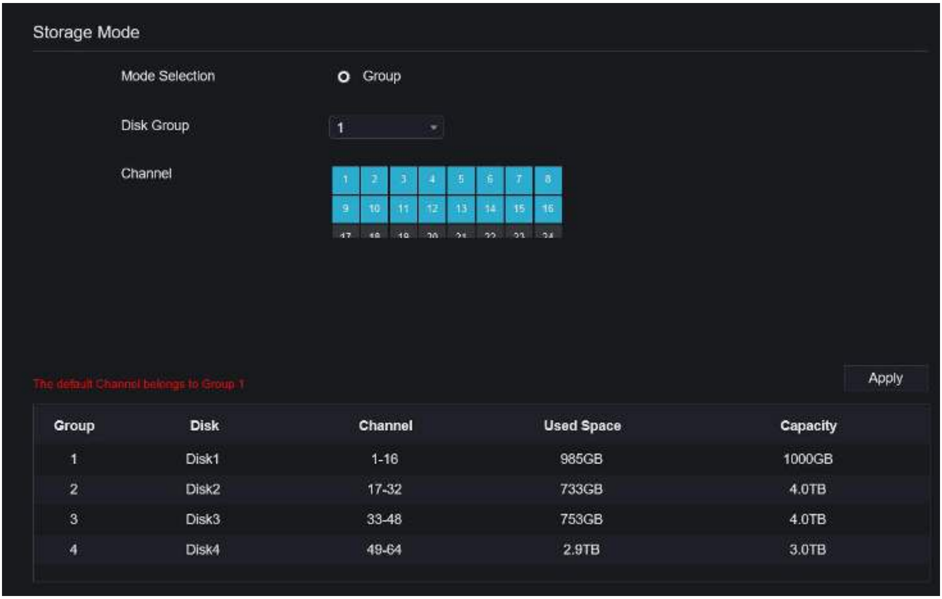
Step 4 Set the expired time, it is up to 90 days.

----End

9.2.3 Storage Mode

Divide channels into different disk groups as needed and using the disk capacity efficiently, as shown in Figure 9-15.

Figure 9-15 Storage Mode interface



Storage Mode

Mode Selection ○ Group

Disk Group 1

Channel

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

The default Channel belongs to Group 1

Group	Disk	Channel	Used Space	Capacity
1	Disk1	1-16	985GB	1000GB
2	Disk2	17-32	733GB	4.0TB
3	Disk3	33-48	753GB	4.0TB
4	Disk4	49-64	2.9TB	3.0TB

Operation Steps

Step 1 Choose the disk group.

Step 2 Select the channel to recorded to disk group.

Step 3 Click **Apply** to save the settings.

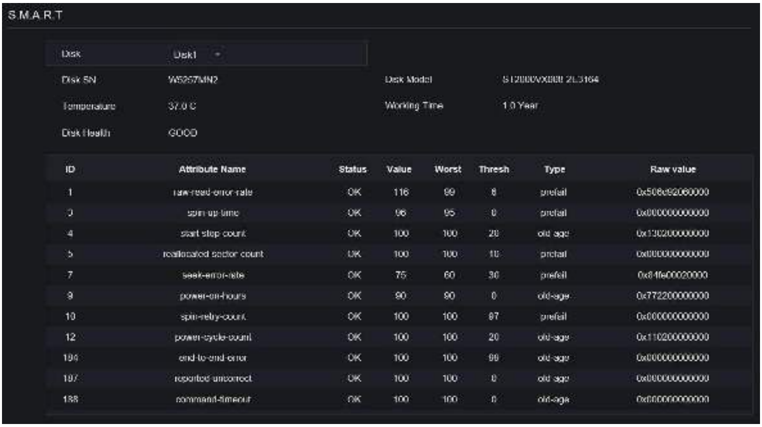
Step 4 The group list will show the detail information.

----End

9.2.4 S.M.A.R.T

S.M.A.R.T is Self-Monitoring Analysis and Reporting Technology, users can view the health of disk, as shown in Figure 9-16.

Figure 9-16 S.M.A.R.T interface



S.M.A.R.T

Disk: Disk1

Disk SN: W5257MN2

Disk Model: ST2000VX008 2L3164

Temperature: 37.0 C

Working Time: 1.0 Year

Disk Health: GOOD

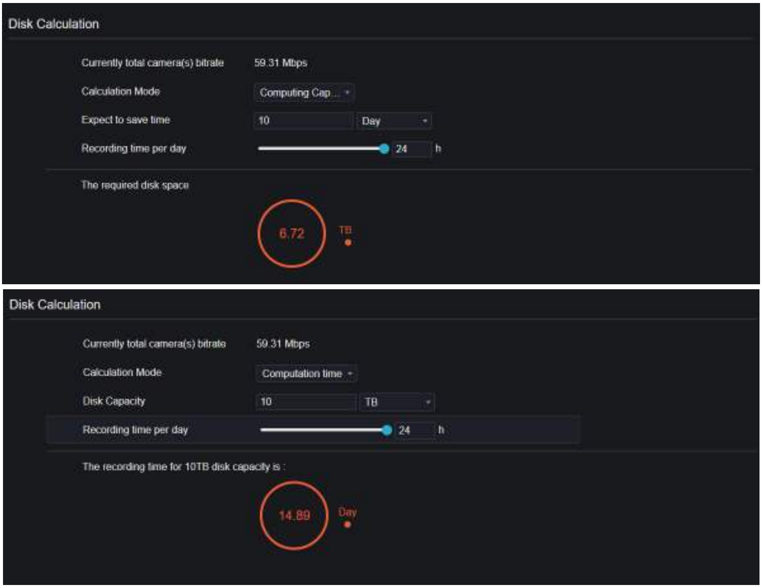
ID	Attribute Name	Status	Value	Worst	Thresh	Type	Raw value
1	raw-read-error-rate	OK	116	99	6	prefail	0x508d92060000
3	spin-up-time	OK	96	95	0	prefail	0x000000000000
4	start stop count	OK	100	100	20	old age	0x130200000000
5	reallocated sector count	OK	100	100	10	prefail	0x000000000000
7	seek-error-rate	OK	75	60	30	prefail	0x84fe00020000
9	power-on-hours	OK	90	90	0	old-age	0x772200000000
10	spin-retry-count	OK	100	100	97	prefail	0x000000000000
12	power-cycle-count	OK	100	100	20	old-age	0x110200000000
184	end-to-end-error	OK	100	100	99	old-age	0x000000000000
187	reported-uncorrect	OK	100	100	0	old age	0x000000000000
188	command-timeout	OK	100	100	0	old-age	0x000000000000

----End

9.2.5 Disk Calculation

You can choose different calculation, computing capacity and computation time.

Figure 9-17 Disk Calculation



Disk Calculation

Currently total camera(s) bitrate: 59.31 Mbps

Calculation Mode: Computing Cap...

Expect to save time: 10 Day

Recording time per day: 24 h

The required disk space

6.72 TB

Disk Calculation

Currently total camera(s) bitrate: 59.31 Mbps

Calculation Mode: Computation time

Disk Capacity: 10 TB

Recording time per day: 24 h

The recording time for 10TB disk capacity is :

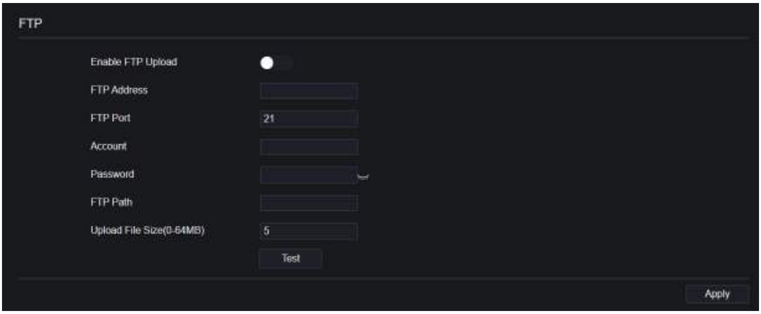
14.89 Day

----End

9.2.6 FTP

Set the FTP path to receive the alarm information, as shown in Figure 9-18. For more details, please refer to *7.4.7 FTP*.

Figure 9-18 FTP



FTP

Enable FTP Upload ○

FTP Address

FTP Port 21

Account

Password

FTP Path

Upload File Size(0-64MB) 5

9.3 Alarm

Users can set **General**, **Motion Detection, Camera Tamper, Video Loss, Intelligent Analysis** and **Alarm in** on alarm interface.

9.3.1 General

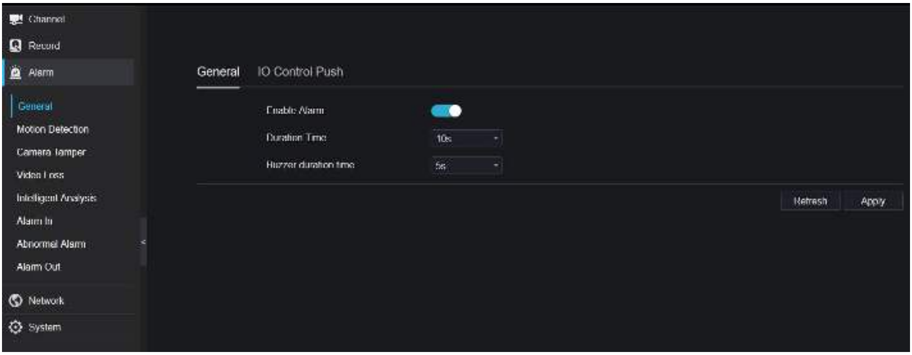
9.3.1.1 General

Procedure

Step 1 On the **System Setting** screen, choose **Alarm > General** to access the general interface.

Step 2 Enable alarm to set duration time and buzzer duration time, as shown in Figure 9-19.

Figure 9-19 General interface



Enable Alarm ●

Duration Time 10s

Buzzer duration time 5s

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

----End

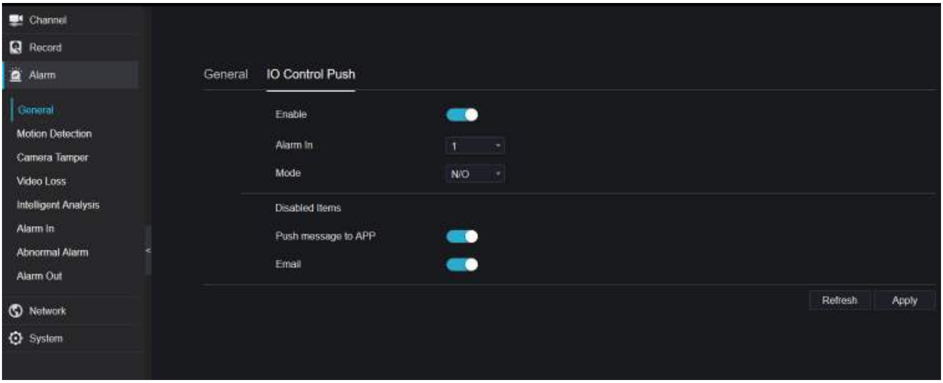
9.3.1.2 IO Control Push

Procedure

Step 4 On the **System Setting** screen, choose **Alarm > General** > **IO Control Push** to access the general interface.

Step 5 Enable the IO control push, as shown in Figure 9-20.

Figure 9-20 IO control push interface



Enable: on

Alarm In: 1

Mode: N/O

Disabled Items

Push message to APP: on

Email: on

Step 6 Choose one alarm in and mode(N/C, N/O).

Step 7 Tick the disable items, click "Apply" to save setting.

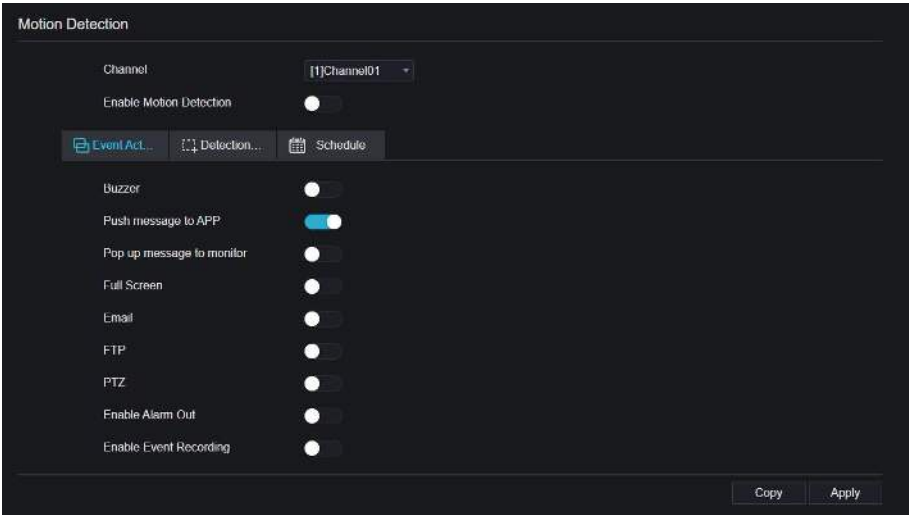
----End

9.3.2 Motion Detection

Procedure

Step 1 On the **System Setting** screen, choose **Alarm > Motion Detection** to access the motion detection interface, as shown in Figure 9-21.

Figure 9-21 Motion detection interface



Motion Detection

Channel [1]Channel01

Enable Motion Detection ○

Buzzer ○

Push message to APP ●

Pop up message to monitor ○

Full Screen ○

Email ○

FTP ○

PTZ ○

Enable Alarm Out ○

Enable Event Recording ○

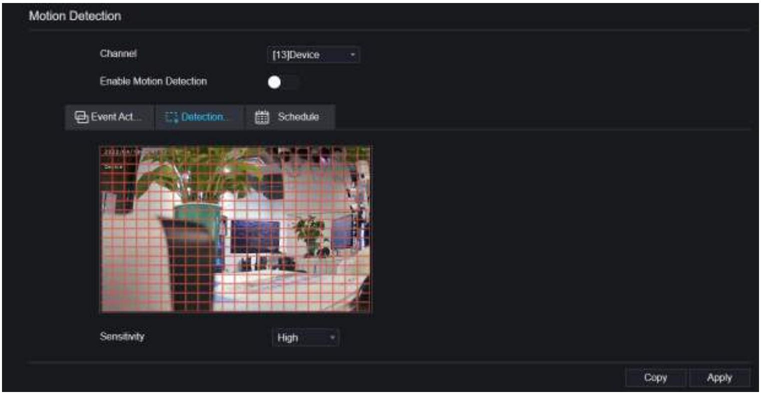
Step 2 Click channel drop-down list to choose channel.

Step 3 Enable motion detection alarm.

Step 4 Set **Event Activity**.

Step 5 Click **Area** to access the motion detection area setting, as shown in Figure 9-22.

Figure 9-22 Motion detection area interface



Motion Detection

Channel [13]Device

Enable Motion Detection ○

Sensitivity High

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 it.

Step 6 Click **Schedule** to access schedule settings, drag and release mouse to select the alarming time within 00:00-24:00 from Monday to Sunday. Click the chosen area can cancel. The settings of alarm schedule are same as disk schedule.

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

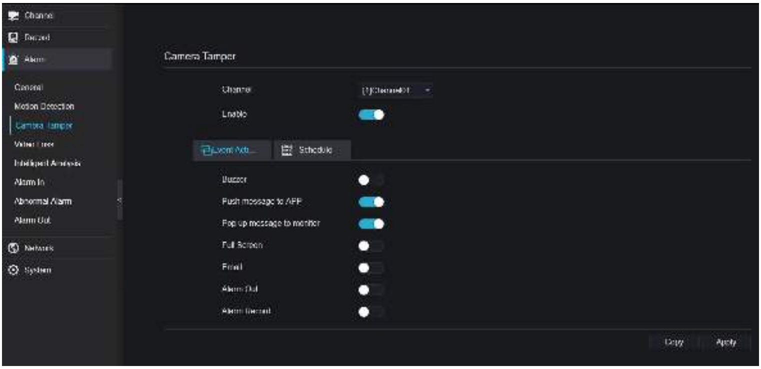
---End

9.3.3 Camera Tamper

Procedure

Step 1 On the **Camera Tamper** screen, choose **Alarm > Camera Tamper** to access the Camera Tamper interface, as shown in Figure 9-23.

Figure 9-23 Camera tamper interface



Camera Tamper

Channel [1]Channel01

Enable ☑

Buzzer ☐

Push message to APP ☑

Pop up message to monitor ☑

Full Screen ☐

Email ☐

Alarm Out ☐

Alarm Record ☐

Step 2 Click drop-down list to choose channel.

Step 3 Enable the camera tamper alarm.

Step 4 Set event activity and schedule please refer to *Figure 5-1 motion detection settings* .

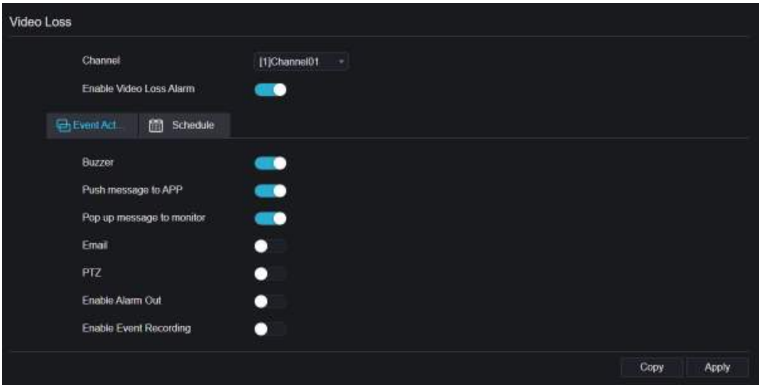
Step 5 Click Copy to copy settings to other cameras. Click Apply to save the settings.

9.3.4 Video Loss

Procedure

Step 1 On the **System Setting** screen, choose **Alarm > Video Loss** to access the video loss interface, as shown in Figure 9-24.

Figure 9-24 Video loss interface



Channel: [1]Channel01

Enable Video Loss Alarm ☑

Buzzer ☑

Push message to APP ☑

Pop up message to monitor ☑

Email ☐

PTZ ☐

Enable Alarm Out ☐

Enable Event Recording ☐

Step 2 Click drop-down list to choose channel.

Step 3 Enable the video loss alarm.

Step 4 Set event activity and schedule please refer to *Figure 5-1 motion detection settings* .

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

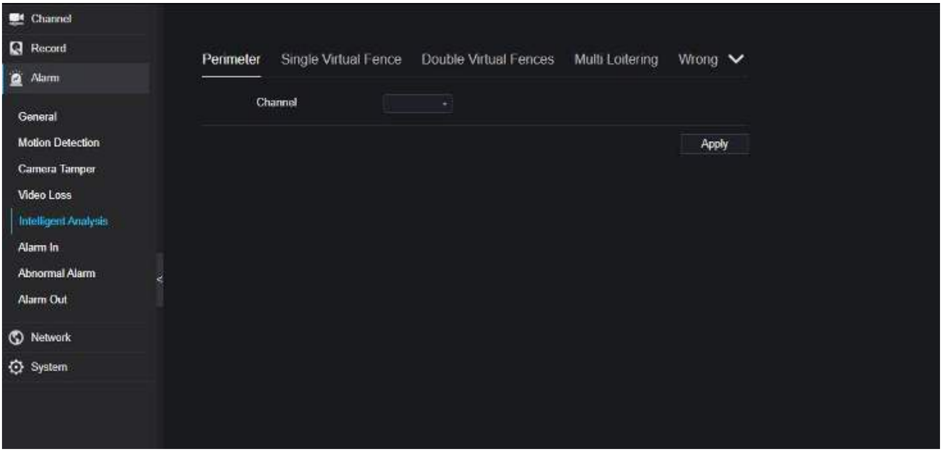
----End

9.3.5 Intelligent Analysis

Procedure

Please refer to chapter *7.6.1 video loss settings,* interface displayed as shown in Figure 9-25.

Figure 9-25 Intelligent analysis interface

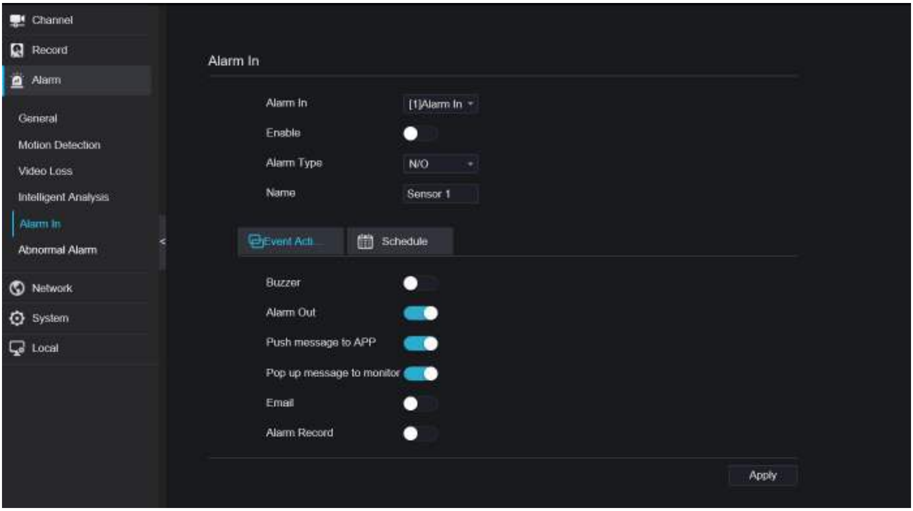


9.3.6 Alarm In

Procedure

Step 1 On the **System Setting** screen, choose **Alarm > Alarm In** to access the alarm in interface, as shown in Figure 9-26.

Figure 9-26 Alarm in interface



Alarm In

Alarm In	[1]Alarm In
Enable	○
Alarm Type	N/O
Name	Sensor 1
Buzzer	○
Alarm Out	●
Push message to APP	●
Pop up message to monitor	●
Email	○
Alarm Record	○

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

Step 3 Enable the button, choose alarm type.

Step 4 Set name, the default is Sensor 1.

Step 5 Set event activity and schedule, please refer to *motion detection settings* .

Step 6 Click Apply to save settings.

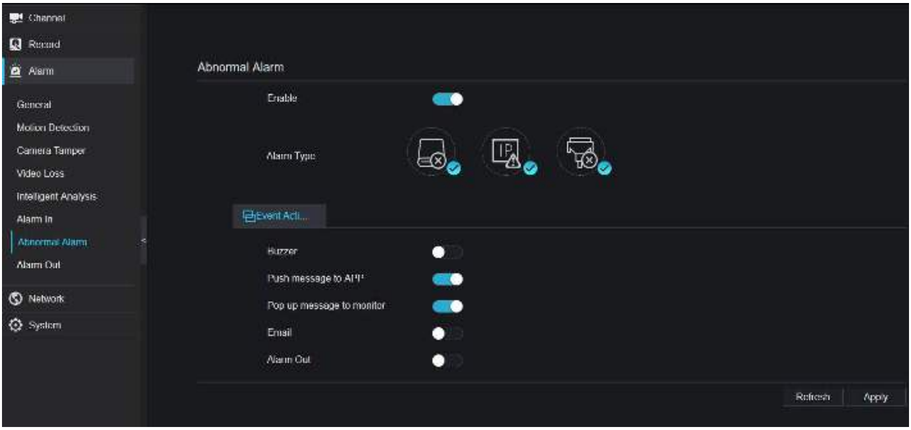
----End

9.3.7 Abnormal Alarm

Procedure

Step 1 On the **System Setting** screen, choose **Alarm > Abnormal Alarm** to access the abnormal alarm interface, as shown in Figure 6-18.

Figure 9-27 Abnormal alarm interface



Abnormal Alarm

Enable ●

Alarm Type ✓ ✓ ✓

Buzzer ○

Push message to APP ●

Pop up message to monitor ●

Email ○

Alarm Out ○

Step 2 Enable the button, tick alarm type.

Step 3 Set event activity and schedule please refer to *motion detection settings* .

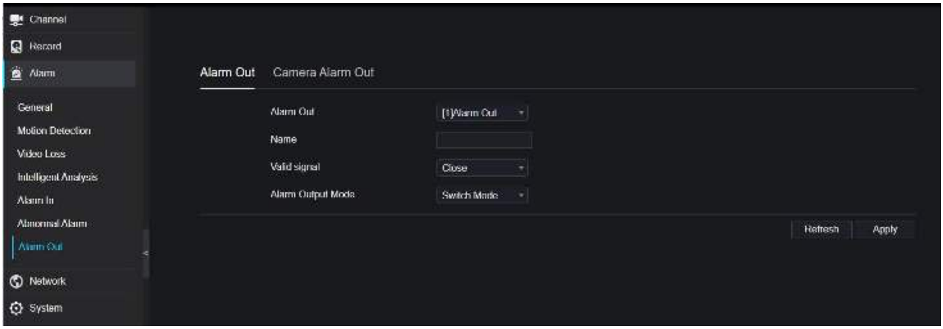
Step 4 Click Apply to save settings.

----End

9.3.8 Alarm out

Set the alarm out, the devices and cameras, as shown in Figure 9-28 and Figure 9-29.

Figure 9-28 Alarm out interface



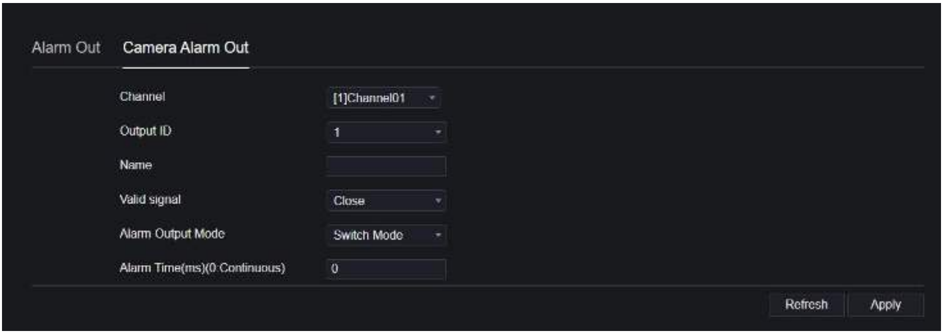
Alarm Out: [1]Alarm Out

Name:

Valid signal: Close

Alarm Output Mode: Switch Mode

Figure 9-29 Camera alarm out interface



Channel: [1]Channel01

Output ID: 1

Name:

Valid signal: Close

Alarm Output Mode: Switch Mode

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

9.4 Network

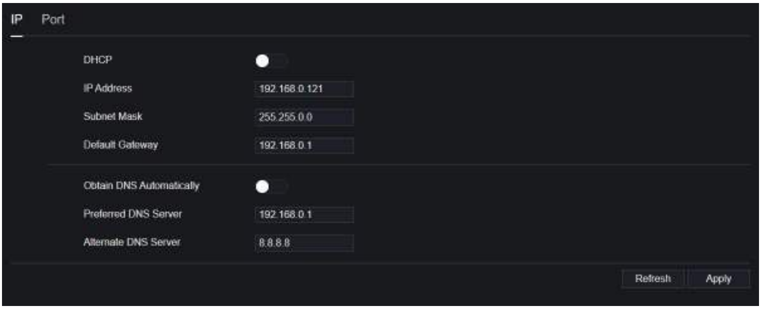
Users can set Network, DDNS, E-mail, UPnP, P2P, IP Filter, 802.1X, SNMP and Web Mode.

9.4.1 Network

Procedure

Step 1 On the **System Setting** screen, choose **Network > Network** to access the network interface, as shown in Figure 9-30.

Figure 9-30 Network interface



DHCP ○

IP Address: 192.168.0.121

Subnet Mask: 255.255.0.0

Default Gateway: 192.168.0.1

Obtain DNS Automatically ○

Preferred DNS Server: 192.168.0.1

Alternate DNS Server: 8.8.8.8

Step 2 Click ○ next to **IP** to enable or disable the function of automatically getting an IP address. The function is enabled by default.

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

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

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

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

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

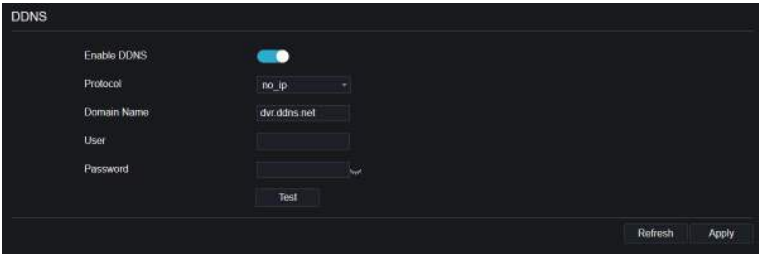
----End

9.4.2 DDNS

Procedure

Step 1 Click **DDNS** in the network interface, choose **Network > DDNS** to access the DDNS interface as shown in Figure 9-31.

Figure 9-31 DDNS interface



DDNS

Enable DDNS

Protocol: no_ip

Domain Name: dvr.ddns.net

User

Password

Test

Refresh Apply

Step 2 Click the button to enable the DDNS function. It is disabled by default.

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

Step 4 Set domain name, user, and password.

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

NOTE

An external network can access an address specified in the DDNS settings to access the DVR.

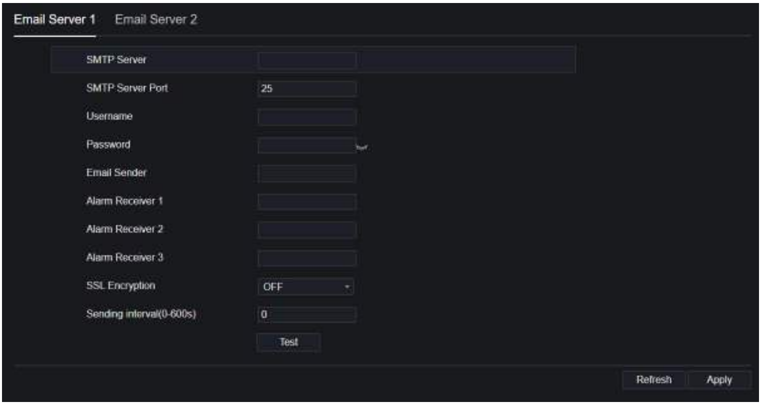
----End

9.4.3 Email

Procedure

Step 1 Click **Email** in the network interface, choose **Network > Email** to access the Email interface, as shown in Figure 9-32

Figure 9-32 Email interface



Email Server 1 Email Server 2

SMTP Server

SMTP Server Port: 25

Username

Password

Email Sender

Alarm Receiver 1

Alarm Receiver 2

Alarm Receiver 3

SSL Encryption: OFF

Sending interval(0-600s): 0

Test

Refresh Apply

Step 2 Set SMTP server and SMTP server port manually.

Step 3 Set sender Email, user name and password manually.

Step 4 Set Email for receiving alarm the message.

Step 5 Set Email for retrieving the password the message.

Step 6 Click **SSL Encryption** drop-down list to enable safeguard of email.

Step 7 Click Refresh to restore previous settings. Click Apply to save the settings.

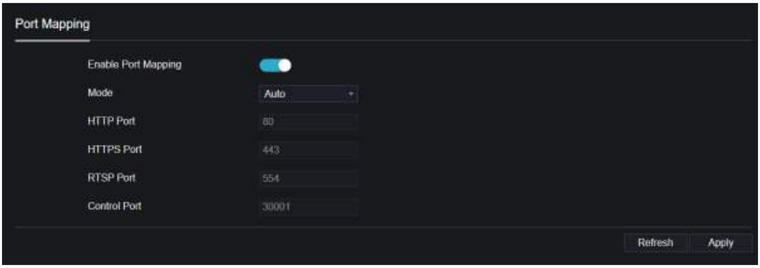
----End

9.4.4 Port Mapping

Procedure

Step 1 Click **Port Mapping** in the network interface, choose **Network > Port Mapping** to access the Port Mapping interface as shown in Figure 9-33.

Figure 9-33 Port Mapping interface



Enable Port Mapping: on

Mode: Auto

HTTP Port: 80

HTTPS Port: 443

RTSP Port: 554

Control Port: 30001

Step 2 Select manner from UPnP enable drop list. The default value is auto.

Step 3 After **Mode** is manual, set the HTTP port, HTTPS port, RTSP port and Control port manually.

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

NOTE

Auto: The system perform Port Mapping automatically.

Manual: The ports are distributed by the router. Please refer to the information on the router when entering them.

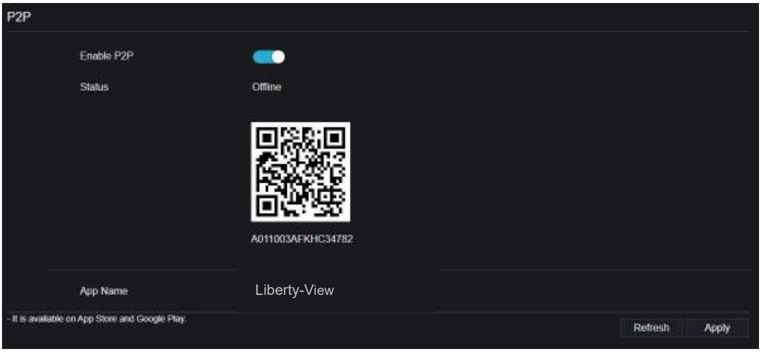
----End

9.4.5 P2P

Procedure

Step 1 Click **P2P** in the network interface, choose **Network > P2P** to access the P2P interface, as shown in Figure 9-34.

Figure 9-34 P2P interface



P2P

Enable P2P: on

Status: Offline

A011003AFKHC34782

App Name: Liberty-View

- It is available on App Store and Google Play.

Step 2 Click **Enable** to enable the P2P function.

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

Step 4 After the Liberty-View is installed in mobile phone, run the APP and scan the UUID QR code to add then access the DVR when the device is online.

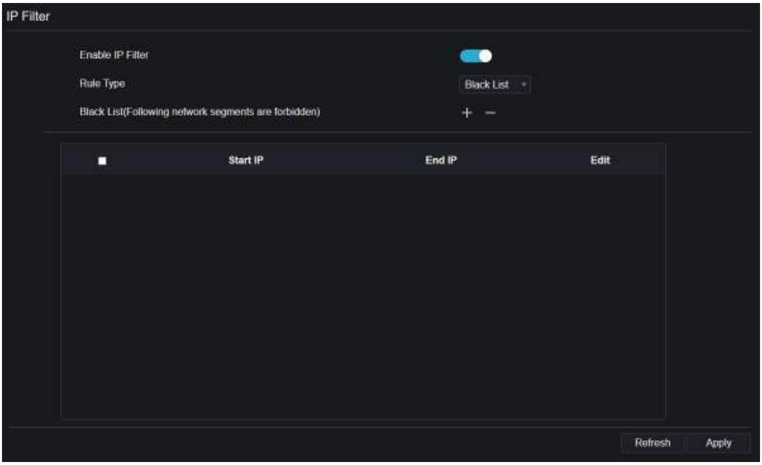
----End

9.4.6 IP Filter

Procedure

Step 1 Click **IP Filter** in the network interface, choose **Network > IP Filter** to access the IP filter interface, as shown in Figure 9-35.

Figure 9-35 IP filter interface



IP Filter

Enable IP Filter ●

Rule Type: Black List

Black List(Following network segments are forbidden) + −

■	Start IP	End IP	Edit

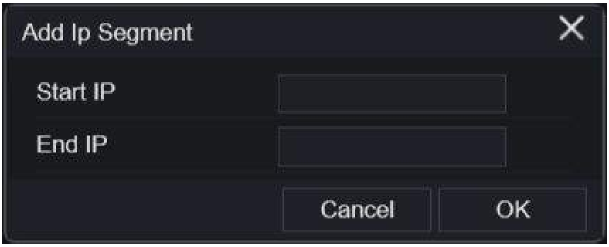
Step 2 Click **Enable** to enable the IP filter function.

Step 3 Click drop-down list of rule type to choose black list or white list.

Step 4 Click + ,view the pop-up windows to set black list or white list, as shown in 7.7.5.

Click − to delete the list.

Figure 9-36 Black or white list interface



Add Ip Segment

Start IP:

End IP:

Step 5 Set start IP and end IP.

Step 6 Click Cancel to cancel settings, click OK to save the settings.

Step 7 Click Refresh to restore previous settings. Click Apply to save the settings.

NOTE

Black list: A list of IP addresses that are regarded as unacceptable or untrustworthy and should be excluded or avoided.

White list: A list of IP addresses 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.

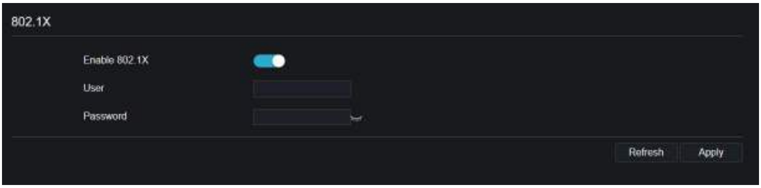
----End

9.4.7 802.1X

Procedure

Step 1 Click **802.1X** in the network interface, 802.1X interface is displayed, enable the button, as shown in Figure 9-37.

Figure 9-37 802.1X interface



Step 2 Input the user and password of 802.1X authentication.

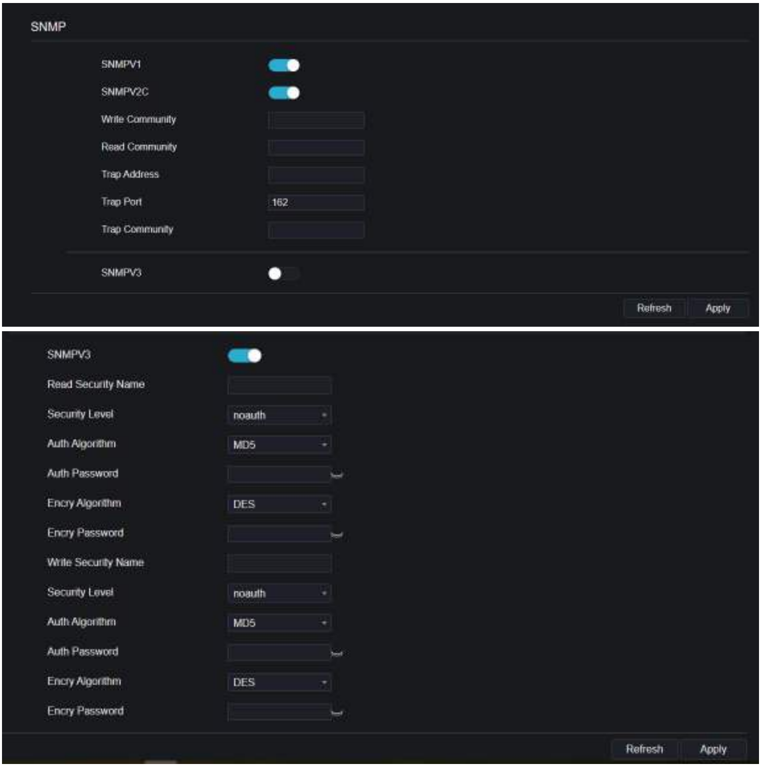
Step 3 Click Refresh to restore previous settings. Click Apply to save the settings.

----End

9.4.8 SNMP

There are three versions of simple network management protocol at interface.

Figure 9-38 SNMP interface



SNMP

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

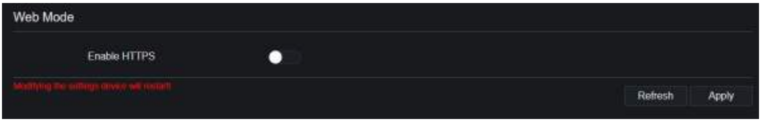
SNMPV3 ○

SNMPV3 ●
Read Security Name
Security Level noauth
Auth Algorithm MD5
Auth Password
Encry Algorithm DES
Encry Password
Write Security Name
Security Level noauth
Auth Algorithm MD5
Auth Password
Encry Algorithm DES
Encry Password

9.4.9 Web Mode

Step 1 Click **Web Mode** in the network interface, Web mode interface is displayed, as shown in Figure 9-39.

Figure 9-39 Web mode interface



Web Mode

Enable HTTPS ○

Modifying the settings device will restart!

Step 2 Enable the https, the device will restart and start https secure.

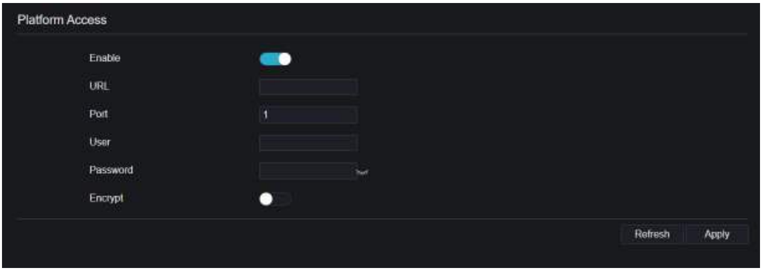
Step 3 Click Refresh to restore previous settings. Click Apply to save the settings.

----End

9.4.10 Platform Access

For more details please refer to *7.6.13 Platform Access*.

Figure 9-40 Platform access



Platform Access

Enable: ●

URL:

Port: 1

User:

Password:

Encrypt: ○

9.5 System

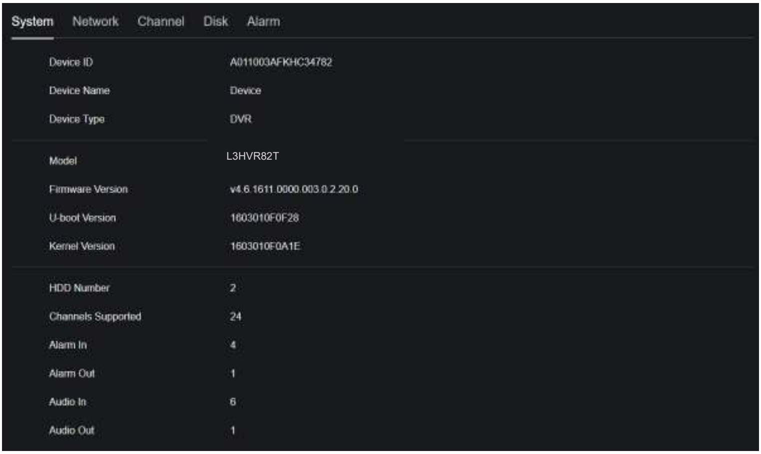
Users can set parameters about information, general, user, password, logs, maintenance and auto restart.

9.5.1 Device Information

Procedure

Step 1 Click ⚙ on the navigation bar, the device information interface is displayed, as shown in Figure 9-41.

Figure 9-41 Device information interface



Device ID A011003AFKHC34782

Device Name Device

Device Type DVR

Model L3HVR82T

Firmware Version v4.6.1611.0000.003.0.2.20.0

U-boot Version 1603010F0F28

Kernel Version 1603010F0A1E

HDD Number 2

Channels Supported 24

Alarm In 4

Alarm Out 1

Audio In 6

Audio Out 1

Step 2 Set the device name according to Table 9-1.

Table 9-2 Device parameters

Parameter	Description
System	The basic information of device.
Network	The network information of the device.
Channel	The status of channels
Disk	The status of disk(s)
Alarm	The information of IO alarm port.

----End

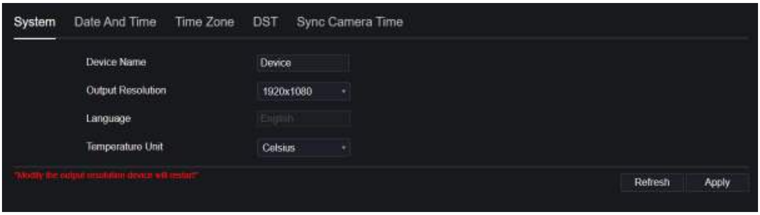
9.5.2 General

You can set system, date and time, time zone, DST and sync camera time general interface.

Procedure

Step 1 On the **System Setting** screen, choose **System >General** to access the general interface, as shown in Figure 9-42.

Figure 9-42 Basic setting interface



Device Name: Device

Output Resolution: 1920x1080

Language: English

Temperature Unit: Celsius

"Modify the output resolution device will restart"

Step 2 Set system.

1. Input the device name.

2. Choose output resolution from drop list.

3. Set the temperature unit.

4. Click Apply to save the system setting.

Step 3 Set date and time.

1. Synchronize the time from the NTP server.

2. Click NTP Sync button to enable synchronize time. The default value is enabling.

Step 4 Enable NTP.

1. Select NTP server, date format and time format from drop list.

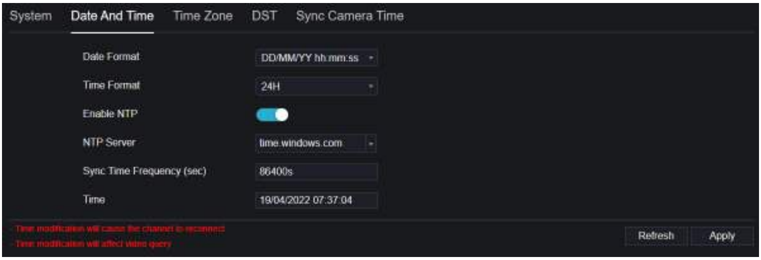
2. Click Apply to save date and time setting. The device time will synchronize with NTP server time.

3. Set the device time manually, as shown in Figure 9-43.

4. Click NTP Sync button to disable synchronize time.

5. Async date and time interface

Figure 9-43 Date and time



Date Format	DD/MM/YY hh:mm:ss
Time Format	24H
Enable NTP	●
NTP Server	time.windows.com
Sync Time Frequency (sec)	86400s
Time	19/04/2022 07:37:04

- Time modification will cause the channel to reconnect
- Time modification will affect video query

Step 5 Set the time zone.

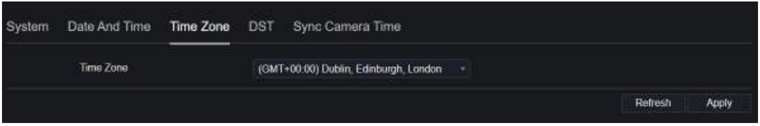
1. Select date format and time format from the drop-down list.

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

Step 6 Set time zone.

Click **Time Zone** to enter the time zone setting interface, as shown in Figure 9-44. Time zone setting interface

Figure 9-44 Time zone



Time Zone	(GMT+00:00) Dublin, Edinburgh, London

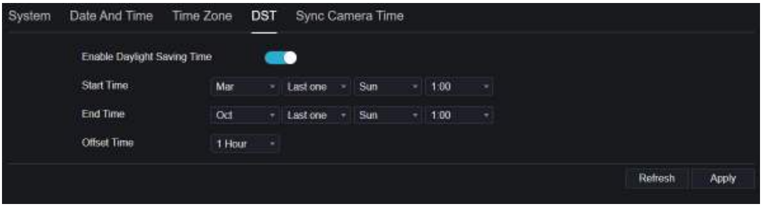
Select a time zone from the drop-down list.

Click Apply to save the time zone setting. Click Refresh to return to previous setting.

Step 7 Set DST.

1. Click DST to enter the DST setting interface, click DST button to enable, as shown in Figure 9-45. The button is disable by default.

Figure 9-45 DST setting interface



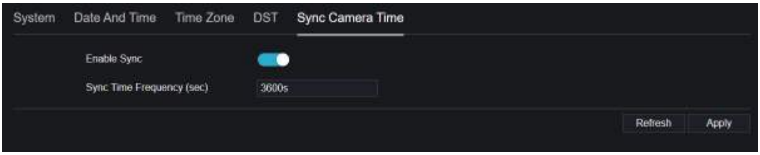
Enable Daylight Saving Time	●			
Start Time	Mar	Last one	Sun	1:00
End Time	Oct	Last one	Sun	1:00
Offset Time	1 Hour			

Select a start time from the drop-down list.

Select an end time from the drop-down list.

Select an offset time from the drop-down list.

Figure 9-46 Sync camera time



Enable Sync: ●

Sync Time Frequency (sec): 3600s

Enable sync camera time, the cameras of DVR management will show at the same time.

Set the frequency of checks (minimum 10s).

Step 8 Click Apply to save the DST setting. Click Refresh to return to previous setting.

9.5.3 User

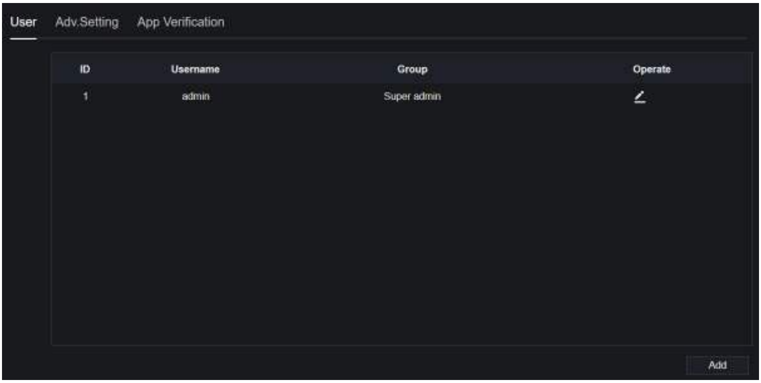
You can create new user accounts to manage the device.

9.5.3.1 Add User

Procedure

Step 1 On the **System Setting** screen, choose **System >User** to access the **User** interface, as shown in Figure 9-50.

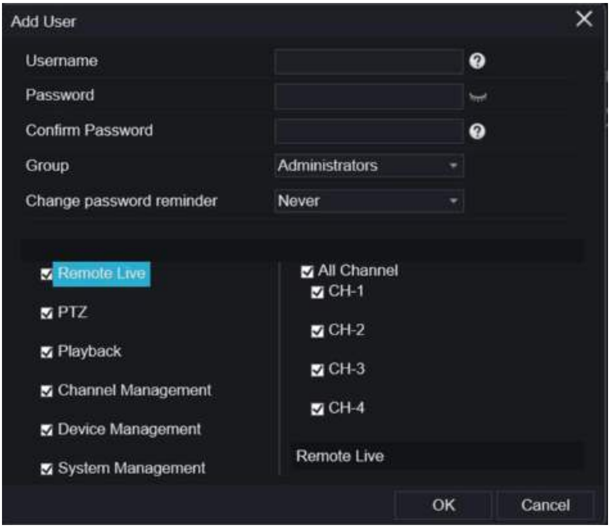
Figure 9-47 User interface



ID	Username	Group	Operate
1	admin	Super admin	✎

Step 2 Click **Add** to add a new user, as shown in Figure 9-48.

Figure 9-48 Add user



Add User ✕

Username

Password

Confirm Password

Group: Administrators

Change password reminder: Never

☑ Remote Live

☑ PTZ

☑ Playback

☑ Channel Management

☑ Device Management

☑ System Management

☑ All Channel

☑ CH-1

☑ CH-2

☑ CH-3

☑ CH-4

Remote Live

OK Cancel

Step 3 Input username, password and confirm password.

Step 4 Select group and change password reminder from drop-down list.

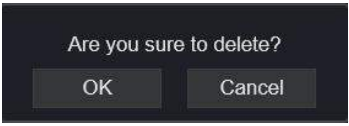
Step 5 Assign the privilege to users.

Step 6 Select channels to manage.

Step 7 Click OK, the message **"Add success"** shows. If the password does not meet the rule, it would show ⚠ Password does not meet requirements.

Step 8 Click ✎ to edit user's information.

Step 9 Click 🗑 to delete the account, it woud show



Are you sure to delete?

OK Cancel

, click OK to delete.

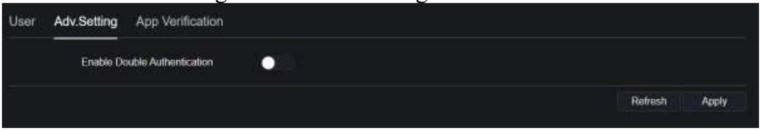
----End

9.5.3.2 Adv.Setting

Procedure

Step 1 On the **System Setting** screen, choose **System >User** > **Adv. Setting** to access interface, as shown in Figure 9-49.

Figure 9-49 Adv. Setting interface



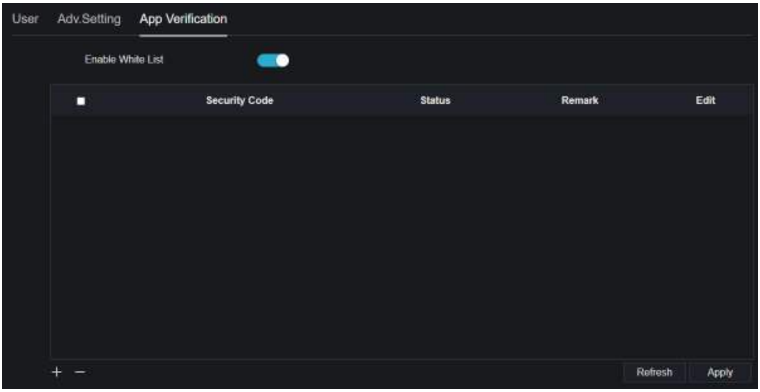
Step 2 Enable the **Password double authentication**. If the user want to playback video, he need input another username and password to authenticate.

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

9.5.3.3 App Verification

For more details information please refer to *7.7.3.3 App Verification.*

Figure 9-50 App Verification interface



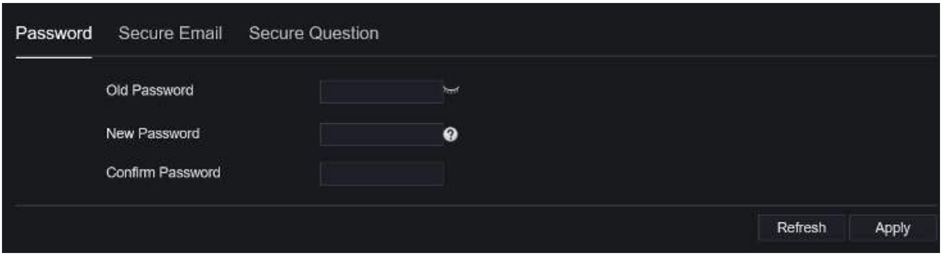
9.5.4 Security Center

9.5.4.1 Password

Procedure

Step 1 On the **System Setting** screen, choose **System >Security Center** to access password interface, as shown in Figure 9-51.

Figure 9-51 Password interface



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

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

NOTE

Valid password range [6-32] characters.

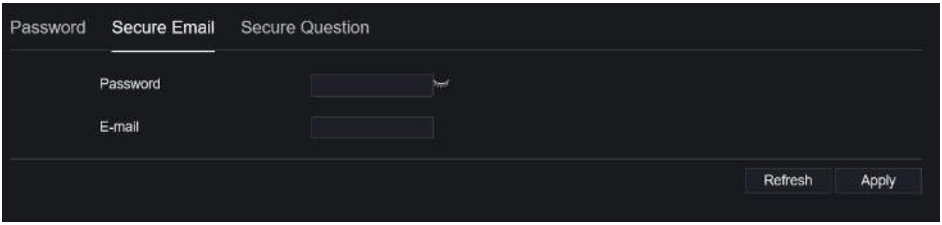
At least 2 kinds of numbers, lowercase, uppercase or special character contained.

Only special characters are support !@#$*+=-.

----End

9.5.4.2 Secure Email

The secure email can receive the verification code of DVR, if users forgot the password accidentally.

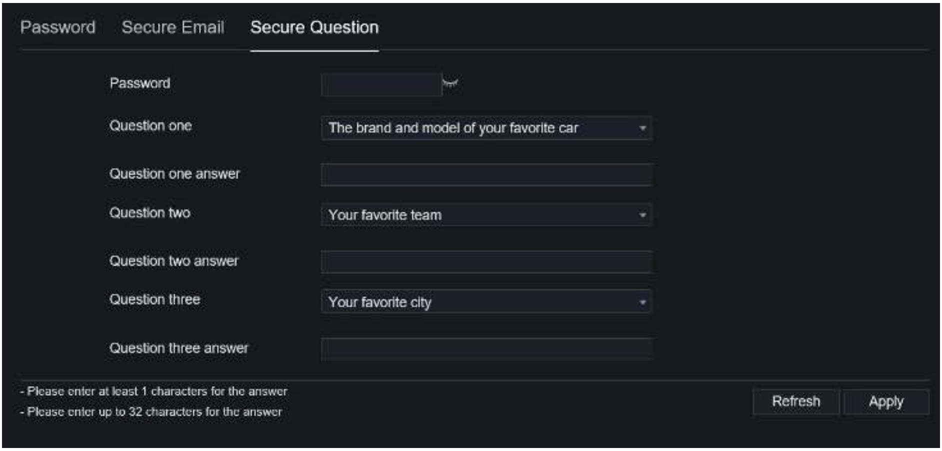


Password

E-mail

9.5.4.3 Secure Question

Users can modify the password to login the DVR if user forgot the password and answer correctly the secure questions.



Password

Question one: The brand and model of your favorite car

Question one answer

Question two: Your favorite team

Question two answer

Question three: Your favorite city

Question three answer

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

----End

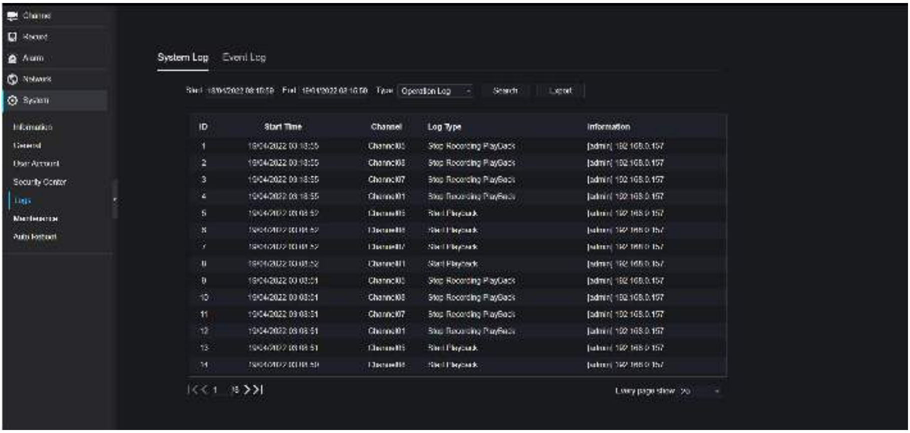
9.5.5 Logs

9.5.5.1 System Logs

Procedure

Step 1 On the **System Setting** screen, choose **System >Logs** to access logs interface, as shown in Figure 9-52.

Figure 9-52 Logs interface



Start 18/04/2022 08:10:59 End 19/04/2022 08:10:59 Type Operation Log

ID	Start Time	Channel	Log Type	Information
1	19/04/2022 08:18:55	Channel05	Stop Recording PlayBack	[admin] 192.168.0.157
2	19/04/2022 08:18:55	Channel08	Stop Recording PlayBack	[admin] 192.168.0.157
3	19/04/2022 08:18:55	Channel07	Stop Recording PlayBack	[admin] 192.168.0.157
4	19/04/2022 08:18:55	Channel01	Stop Recording PlayBack	[admin] 192.168.0.157
5	19/04/2022 08:08:52	Channel05	Start Playback	[admin] 192.168.0.157
6	19/04/2022 08:08:52	Channel08	Start Playback	[admin] 192.168.0.157
7	19/04/2022 08:08:52	Channel07	Start Playback	[admin] 192.168.0.157
8	19/04/2022 08:08:52	Channel01	Start Playback	[admin] 192.168.0.157
9	19/04/2022 08:08:51	Channel05	Stop Recording PlayBack	[admin] 192.168.0.157
10	19/04/2022 08:08:51	Channel08	Stop Recording PlayBack	[admin] 192.168.0.157
11	19/04/2022 08:08:51	Channel07	Stop Recording PlayBack	[admin] 192.168.0.157
12	19/04/2022 08:08:51	Channel01	Stop Recording PlayBack	[admin] 192.168.0.157
13	19/04/2022 08:08:51	Channel05	Start Playback	[admin] 192.168.0.157
14	19/04/2022 08:08:50	Channel08	Start Playback	[admin] 192.168.0.157

Every page show 20

Step 2 Set start and end time from calendar.

Step 3 Select log type from drop-down list.

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

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

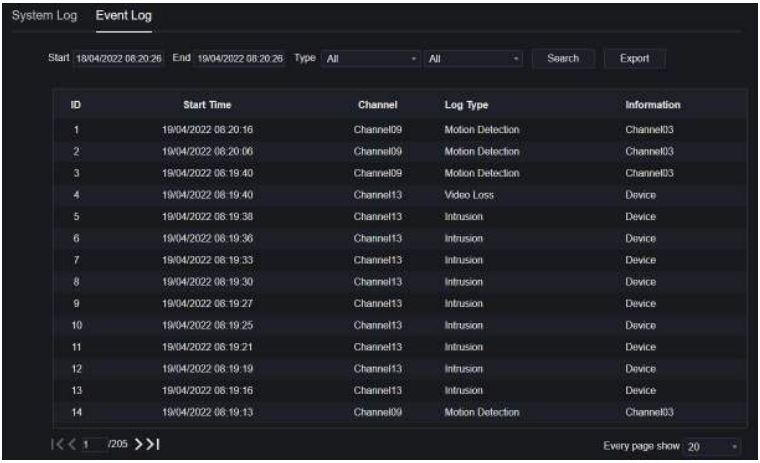
----End

9.5.5.2 Event Log

Procedure

Step 6 On the **System Setting** screen, choose **System > Logs > Event Log** to access logs interface, as shown in Figure 9-53.

Figure 9-53 Event interface



Start 18/04/2022 08:20:26 End 19/04/2022 08:20:26 Type All All Search Export

ID	Start Time	Channel	Log Type	Information
1	19/04/2022 08:20:16	Channel09	Motion Detection	Channel03
2	19/04/2022 08:20:06	Channel09	Motion Detection	Channel03
3	19/04/2022 08:19:40	Channel09	Motion Detection	Channel03
4	19/04/2022 08:19:40	Channel13	Video Loss	Device
5	19/04/2022 08:19:38	Channel13	Intrusion	Device
6	19/04/2022 08:19:36	Channel13	Intrusion	Device
7	19/04/2022 08:19:33	Channel13	Intrusion	Device
8	19/04/2022 08:19:30	Channel13	Intrusion	Device
9	19/04/2022 08:19:27	Channel13	Intrusion	Device
10	19/04/2022 08:19:25	Channel13	Intrusion	Device
11	19/04/2022 08:19:21	Channel13	Intrusion	Device
12	19/04/2022 08:19:19	Channel13	Intrusion	Device
13	19/04/2022 08:19:16	Channel13	Intrusion	Device
14	19/04/2022 08:19:13	Channel09	Motion Detection	Channel03

1 /205

Every page show 20

Step 7 Set start and end time from calendar.

Step 8 Select event type from drop-down list.

Step 9 Click **Search** to acquire log information.

Step 10 Click **Export** to export the event logs.

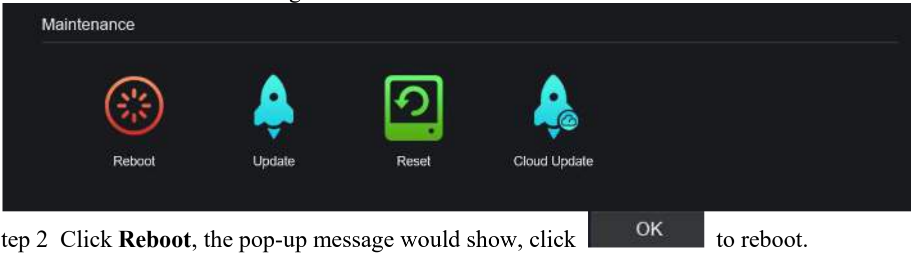
----End

9.5.6 Maintenance

Procedure

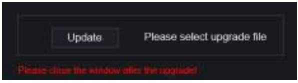
Step 1 On the **System Setting** screen, choose **System >Maintenance** to access maintenance interface, as shown in Figure 9-54.

Figure 9-54 Maintenance interface

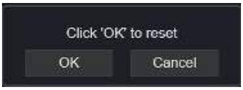


Step 2 Click **Reboot**, the pop-up message would show, click OK to reboot.

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


Update Please select upgrade file

Please close the window after the upgrade!

Step 4 Click **Reset**, the pop-up message  shows, click OK to reset.

Click 'OK' to reset

Step 5 If the device is online, and the cloud server has the software, click **Cloud Update, it shows** 'make sure to update' **,** click **OK** to update.

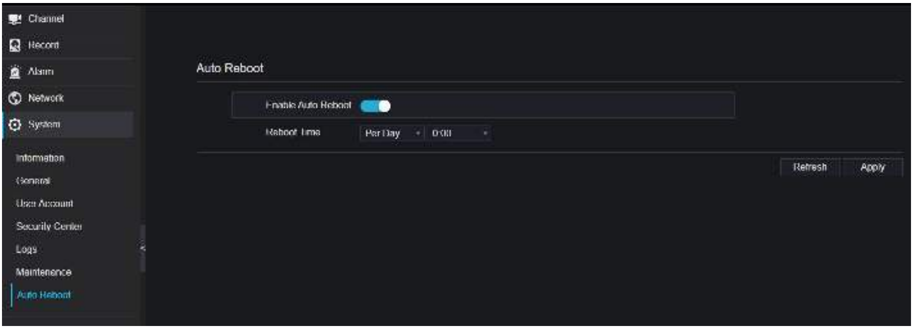
----End

9.5.7 Auto Reboot

Procedure

Step 1 On the **System Setting** screen, choose **System > Auto Reboot** to access auto restart enable the auto restart, the screen as shown in Figure 9-55.

Figure 9-55 Auto restart



Auto Reboot

Enable Auto Reboot: on

Reboot time: Per Day 0:00

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

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

9.6 Local

Set the image download path for snapshots and the record download path for record files in the download configuration interface. It is only used for IE browser.

Procedure

Step 1 Click **Local Download Config** in local interface, as shown in Figure 9-56.

Figure 9-56 Local interface

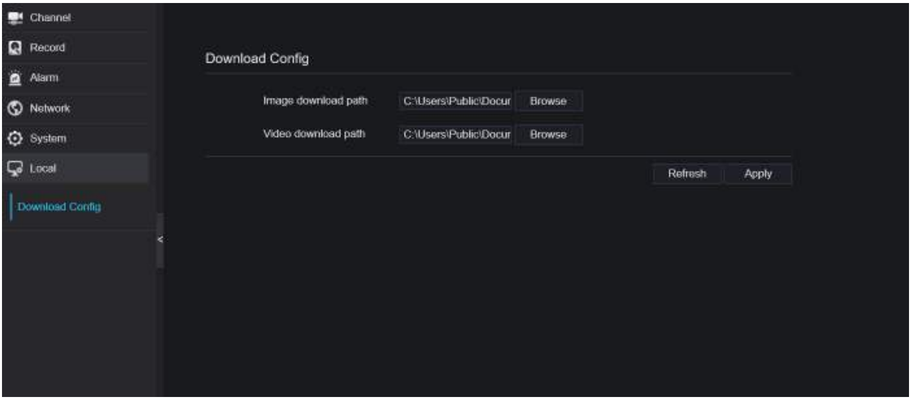


Image download path C:\Users\Public\Docur

Video download path C:\Users\Public\Docur

Step 2 Enter the image download path.

Step 3 Enter the record download path.

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

----End