



User Manual

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.

Privacy Protection Reminder:

If you have installed our products, you may be collecting 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, informing the relevant rights holder of the existence of video surveillance areas, and provide corresponding contact information.

About This Document:

- This document is for use with multiple models. The appearance and function of the products are subject to the actual products.
- Any loss caused by failure to follow the instructions in this document is the responsibility of the user.
- This document will be updated in real time according to the laws and regulations of the relevant region. For details, please refer to the product's paper, electronic CD, QR code or official website. If the paper and electronic files are inconsistent, please refer to the electronic file.
- The company reserves the right to modify any information in this document at any time.
- The revised content will be added to the new version of this document without prior notice.

- This document may contain technical inaccuracies, or inconsistencies with product features and operations, or typographical errors.
- If the obtained PDF document cannot be opened, please make sure you are using compatible, up to date PDF reader software.

Network Security Advice

Required measures to ensure basic network security of equipment:

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. Check for latest firmware versions on www.northernvideo.com.

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

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

Forward only 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 certain features required for the particular users.

9. 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.

10. 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.

11. 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.

13. Physically protect your device

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

14. 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 operations of the DVR (Network Video Recorder) device.

Modify Log

ID	Version	Log	Release Time
1	V 4.0	Initial Release	2017
2	V 4.1	Add function	
3	V 4.1.3	Perfect interface, add models	
4	V 4.1.5	Add reverse playback Open data port 2	20180106
5	V 4.1.6	Add 4 split screens of automatic adjusting main stream or sub stream. Add private protocol access. Support multi-screen playback. Add the schedule recording function by channel setting Increase the allocation of permissions by channel	
	V 4.2	Add boot wizard Add toolbar Add manual recording and timely playback Add multiple clicks to enlarge Add user lockout Remove the upper right corner to display the alarm warning Add the view of the latest alarm information, modify the manual alarm Modify quick navigation content	

		<p>Preview channel and modify network parameter function on IPC side</p> <p>Support for copying to some or all channels</p> <p>Remove the full screen function</p> <p>Add background backup</p> <p>Add video dual authentication</p> <p>Intelligent motion detection</p> <p>Add the color to distinguish the video type, increase the video type search</p> <p>Add sound switch</p> <p>Add instant playback</p> <p>Remove the timeline function</p> <p>Increase intelligence analysis</p> <p>Increase test DDNS function</p> <p>Increase test mail function</p> <p>Modify the time precision to half an hour, remove the recording plan master switch</p> <p>Add hardware information</p> <p>Added video dual authentication and boot wizard configuration function</p> <p>Add alarm log</p> <p>Add interval update profile</p>	
6	V 4.2.1	<p>Add the NTP synchronization interval and add the manual NTP synchronization interval.</p> <p>Add access to thermal imaging cameras and display IPC product models</p> <p>Remove auto hide</p> <p>Add the patrol route and line sweep function</p> <p>Add upgrade IPC, restart IPC, restore factory IPC</p> <p>Increase the selection of primary and sub stream backups</p> <p>Add click playback button to play video</p> <p>Add UI display granular IPC intelligence analysis</p> <p>Add 802.1x functionality</p>	

		<p>Add SNMP function</p> <p>Add upgrade device features</p> <p>Add the timing restart function</p> <p>Add U disk upgrade display progress bar</p>	
7	V 4.2.4	<p>Increase U-boot and kernel version display</p> <p>Increase P2P status display</p> <p>Increase signal type display</p> <p>Increase POE icon display</p> <p>Increase SSL access IPC, special models support</p> <p>Optimize username and password saving methods</p> <p>Increase batch backup</p> <p>Increase fixed point playback</p> <p>Increase hard disk alarm</p> <p>Optimized recording expiration time input mode is editable</p> <p>Increase the city after each time zone</p> <p>Increase face recognition</p> <p>Add P2P server</p>	
8	V 4.3	<p>Add pattern unlock</p> <p>Add mailbox reset password</p> <p>Increase the secure question reset password</p> <p>Add 1+7 split screen</p> <p>Add channel information display</p> <p>Add 3D ball machine</p> <p>Remove the video type switch from the scene</p> <p>Add RAID</p> <p>Add S.M.A.R.T</p> <p>Add formatting (fat32 and NTFS)</p> <p>Support event video quick download backup</p> <p>Add event video backup</p> <p>Add the full screen of the bomb and send the screenshot</p> <p>Add IPC intelligent analysis configuration</p>	

		Add manual input automatic logout time Restore factory refinement	
--	--	--	--

Symbol Conventions

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

Symbol	Description
 DANGER	Alerts you to a high risk hazard that could, if not avoided.
 WARNING	Alerts you to a medium or low risk hazard that could, if not avoided, result in moderate or minor injury.
 CAUTION	Alerts you to a potentially hazardous situation that could, if not avoided, 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 uses of the product. To prevent danger and property damage, please read this manual carefully before using the device and strictly comply to the manual when using it. Please save the manual after reading.

Requirements

- The DVR is 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 or around 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.
- Only remove the device cover of the device if installing or replacing Hard Disks, Hard Disks are the only serviceable part inside the device.
- 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 following local recycling laws.
- Only use power supply included with the device.

- 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 plug with the power outlet with a protective ground connection.

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.

Contents

Legal Notice	ii
Network Security Advice	iv
About This Document	vii
Purpose.....	vii
Modify Log	vii
Symbol Conventions	x
Safety Instructions.....	xi
Requirements	xi
Power Requirement.....	xi
Important Statement	xii
Contents.....	xiii
1.2.1 Cloud Upgrade	1
1.2.2 Real-time Monitoring.....	1
1.2.3 Playback.....	1
1.2.4 User Management	2
1.2.5 Storage Function	2
1.2.6 Alarm Function	2
1.2.7 Network Monitoring.....	2
1.2.8 Split Screen	3
1.2.9 Recording Function.....	3
1.2.10 Backup Function	3
1.2.11 External Device Control.....	3
1.2.12 Accessibility.....	3
3.3.1 Install One or Two Hard disks.....	10
6.3.1 Time Search	39
6.3.2 Picture Grid.....	40
6.3.3 Event.....	42
6.3.4 Backup	43
7.3.1 Camera	45

7.3.2 Encode Parameter.....	49
7.3.3 Sensor Setting	50
7.3.4 OSD Settings.....	52
7.3.5 Privacy Zone	53
7.3.6 Channel Type	54
7.4.1 Record Schedule	55
7.4.2 Disk.....	56
7.4.3 S.M.A.R.T.....	58
7.5.1 General.....	59
7.5.2 Motion Detection	60
7.5.3 Camera Tamper	62
7.5.4 Video Loss.....	63
7.5.5 Intelligent Analysis.....	64
7.5.6 Alarm In	65
7.5.7 Abnormal Alarm.....	67
7.6.1 Network.....	69
7.6.2 802.1 X.....	71
7.6.3 DDNS.....	72
7.6.4 E-mail.....	73
7.6.5 Port Mapping.....	74
7.6.6 P2P	74
7.6.7 IP Filter	75
7.7.1 Information	78
7.7.2 General.....	79
7.7.3 User.....	84
7.7.4 Security Center.....	86
7.7.5 Auto Sequence.....	90
7.7.6 Logs	92
7.7.7 Maintenance.....	94
7.7.8 Auto Restart	95
8.3.1 Browsing Real-Time Videos	101
8.3.2 Live Video.....	103

8.3.3 Channel Operation	104
8.3.4 PTZ Control and Setting	105
8.3.5 Sensor Setting	107
8.3.6 Layout	109
8.4.1 Video Playback.....	110
8.5.1 Channel Alarm	112
8.5.2 System Alarm.....	114
9.1.1 Camera	116
9.1.2 Encode	118
9.1.3 Sensor Setting	119
9.1.4 OSD	121
9.1.5 Privacy Zone	121
9.2.1 Record Schedule	122
9.2.2 Disk	123
9.2.3 S.M.A.R.T.....	124
9.3.1 General.....	125
9.3.2 Motion Detection	126
9.3.3 Camera Tamper	128
9.3.4 Video Loss.....	129
9.3.5 Intelligent Analysis.....	130
9.3.6 Alarm In	130
9.3.7 Abnormal Alarm.....	131
9.4.1 Network.....	132
9.4.2 DDNS.....	134
9.4.3 E-mail.....	134
9.4.4 Port Mapping.....	135
9.4.5 P2P	136
9.4.6 IP Filter	137
9.4.7 802.1X.....	139
9.4.8 Web Mode	140
9.5.1 Device Information	140
9.5.2 General.....	142

9.5.3 User 145

9.5.4 Password 147

9.5.5 Logs 148

9.5.6 Maintenance 149

9.5.7 Auto Restart 150

1 Preface

1.1 Product Description

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

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 the device through online upgrade.

1.2.2 Real-time Monitoring

It has a VGA (Video Graphics Array) port and an HDMI (High Definition Media Interface) port. It can be monitored by a monitor screen or monitor, and supports simultaneous output of VGA and HDMI.

1.2.3 Playback

Each channel offers independent real-time recording, and play functions such as retrieval, playback, network monitoring, video query, and download. Please refer to chapter Playback

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

The exact time when the event occurred can be displayed during playback of the recording.

You can select any area of the screen for partial magnification.

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 Function

According to the user's configuration and policies (such as through alarm and timing 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 give corresponding prompts.

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

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

1.2.7 Network Monitoring

Through the network, the audio and video data of the 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 a monitor. 1/4/8/9/16 screen splitting is supported during preview; 1/4/9/16 screen splitting is supported during playback, views are dependent on the amount of channels available on the recorder.

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)

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 be freely set.

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

1.2.12 Accessibility

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

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

Supports record logging.

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

Supports playback of audio and video from remote IPC 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 supports connected to an USB mouse.

Figure 2-2 Real panel

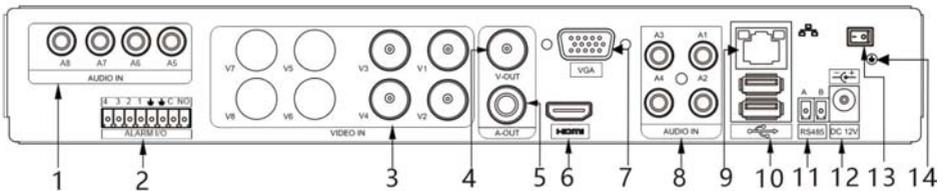


Table 2-2 Real panel function

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	Supports 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 only Surveillance rated Hard Disks in the unit (the quality of hard disks sold on markets varies greatly with different brands and models).
- Always shut down the unit and remove power if needing to inspect, install or replace Hard Disks.

- 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.
- In the case of product upgrade, the information in this document is subject to change without notice.

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 conform to national standards of electromagnetic radiation and does not cause harm to the human body.
Temperature	-10°C to +45°C
Humidity	20% to 80%
Atmospheric pressure	86 Kpa to 106 Kpa
Power supply	DC 12V, 2A / DC 12V, 4A, please refer to actual product.
Power consumption	<15W (excluding the hard disk)

Installation precautions

Note the following points when installing and operating the DVR:

- Install the DVR horizontally.

- Avoid direct sunlight on the DVR and keep away from any heat sources and hot environments.
- Connect the DVR to other devices correctly during installation.
- Depending on the model number, the DVR may or may not include hard disk upon delivery.

The DVR identifies hard disk capacity automatically and supports mainstream hard disk models.

User should use Surveillance or Security level drives.

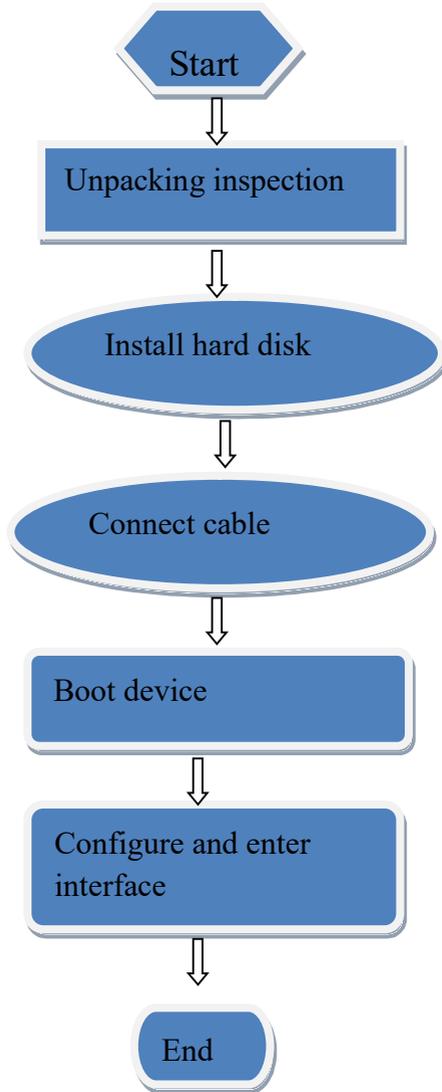
Other precautions

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

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

3 Install Device

3.1 Process



- Step 1 Check the appearance, packaging, and label of the device to ensure there is no damage.
- Step 2 Install the hard disk and fix the hard disk on the device bracket.
- Step 3 Connect the device cable.
- Step 4 After ensuring that the device is connecting correct, connect 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 the transportation company sends network video recorder to you, please check the following table for unpacking. If you have any questions, please contact our sales technicians.

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	<p>Label of device</p> <p>Is the equipment model consistent with the order contract?</p> <p>Whether the label is torn</p> <p> NOTE</p> <p>Do not tear or discard, otherwise warranty service is not guaranteed. When you call the company for sales personnel calls, you will need to provide the serial number of the product on the label.</p>	
3	Cabinet	Package	Is there any obvious damage
		Data cable, power cable, fan power supply,	<p>Is the connection loose?</p> <p> NOTE</p>

		and motherboard	If it is loose, please contact the company's after-sales personnel.
--	--	-----------------	---

3.3 Install Hard Disk

When installing for the first time, first check if the hard disk is installed. It is recommended to use the Security/Surveillance rated Hard Disks.

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



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.

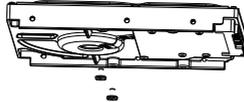
Use a reasonable hard disk capacity according to the recording requirements.

3.3.1 Install One or Two Hard disks

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

Step 2 Take out the screws and install it to the screw holes, as show in Figure 3-1..

Figure 3-1 Installing the hard disk screws



Step 3 Route the screws through the hole on the base, push the hard disk to the appropriate position on the left, as shown in Figure 3-2.

Figure 3-2 Install hard disk



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

Figure 3-3 Install hard disk



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

4 Basic Operations

4.1 Power on the Device

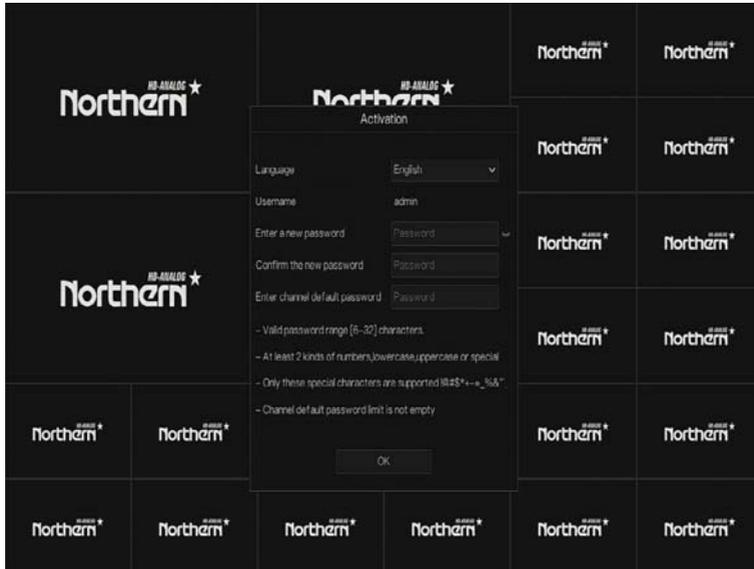


CAUTION

- Ensure that the DVR is correctly connected to the 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 power-on.
- In some locations & environments, abnormal building power fluctuations may cause the failure of the DVR to work properly and even damage the DVR in severe cases. It is recommended to always use battery backup device with surge protection to protect the device if connected to a power source which is prone to Blackouts or Brownouts.

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

Figure 4-1 Real-time video screen



 **NOTE**

For users who install the hard disk for the DVR. The hard disk is 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 the user logs into the device for the first time, or resets 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

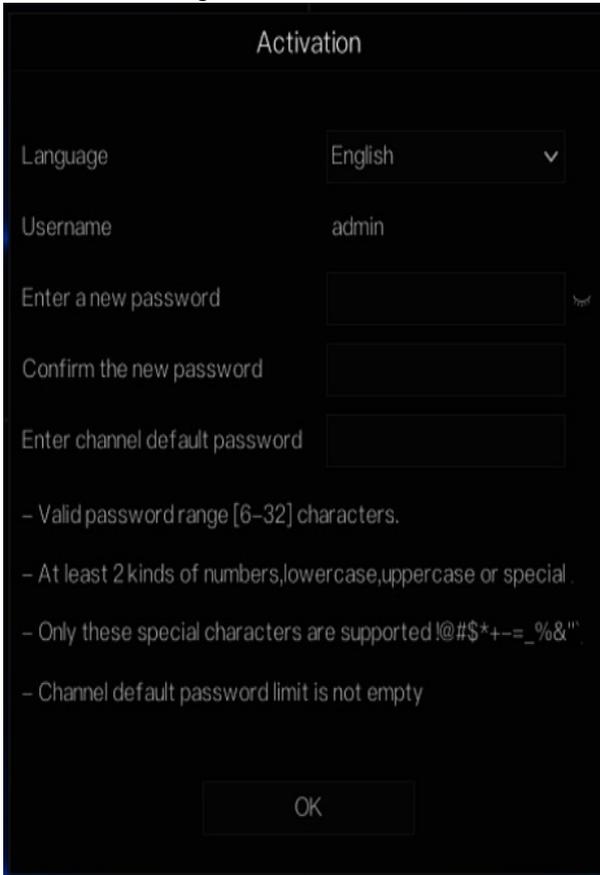
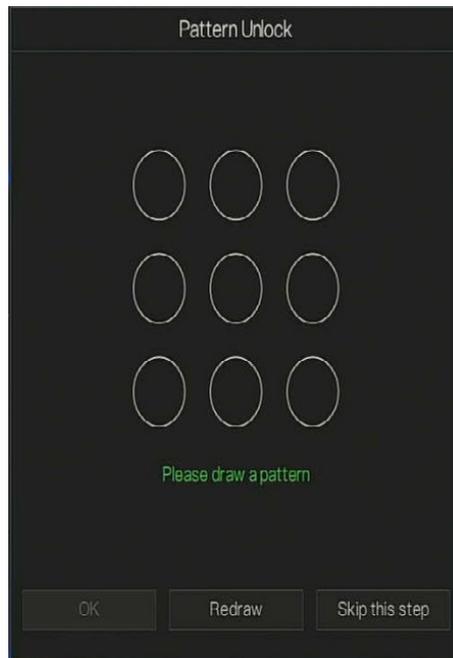


Table 4-1 Description of activation

Name	Description
Username	The default username is admin, and “admin” is super administrator.
Password	Valid password range 6-32 characters.
Confirm password	At least 2 kinds of numbers, lower case, upper case or special characters contained. Only these special characters are supported !@#\$*+ -= _%&” Channel default password limit is not empty.
Channel password	The DVR channel connection password is the camera login password.

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

Figure 4-3 Set pattern unlock



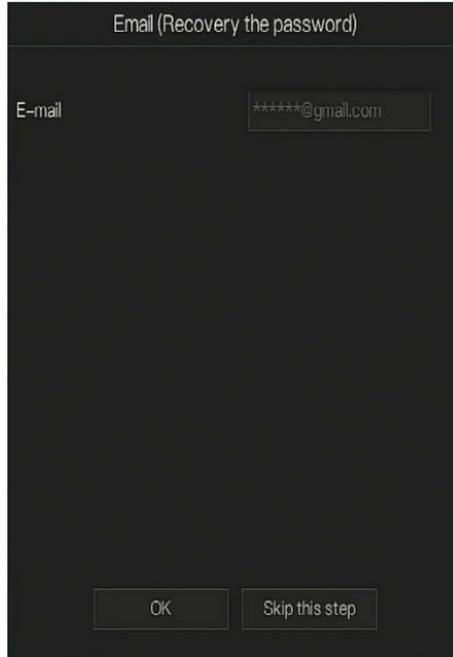
 **NOTE**

After the pattern is unlocked, the system defaults to the pattern unlock login. If the pattern unlock is not set, you will need to input the password to login.

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

Set the Email to receive the verification code if user forget the initial password to create new password, as shown in Figure 4-4.

Figure 4-4 Set Email



 **NOTE**

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

If the email address is not set, you can reply to the secure question or send the QR code to the seller to give 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

Question two Your favorite team ▾

Question two answer

Question three Your favorite city ▾

Question three answer

- Please enter at least 4 characters for the answer

- Please enter up to 32 characters for the answer

OK Skip this step

 **NOTE**

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

Question one can be set: Your favorite animal

Company name of your first job

The name of the first boy/girl you like

Question 2: Your favorite team

Question 3: Your favorite city

The three question options cannot be set to the same issue.

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

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

4.3 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 RPM off the power switch to disconnect the DVR from the power supply.

4.4 Login to the System

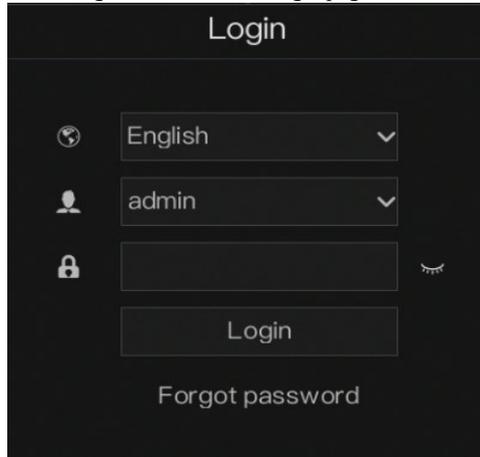
Step 1 Login to the device, there are two modes to login if you set the pattern unlock, as shown in

Figure 4-6 Pattern unlock login page



Step 2 On the DVR login page, click “ Password” to at pattern unlock interface. If user 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 wait and 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. User 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 new password to login .
2. Answer the secure question to create 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

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

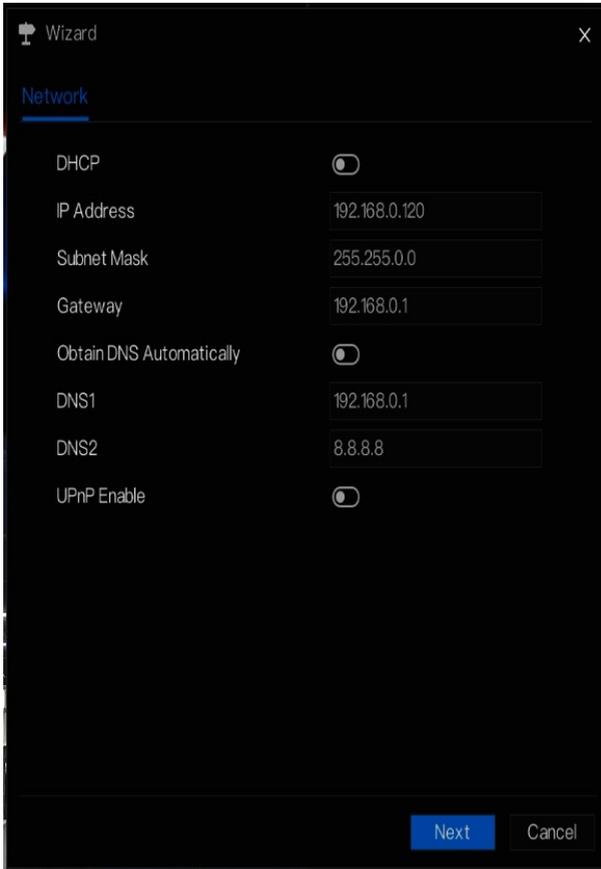
5 Wizard

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 - Network



Step 1 Set the parameter, the details please refer to Table 5-1.

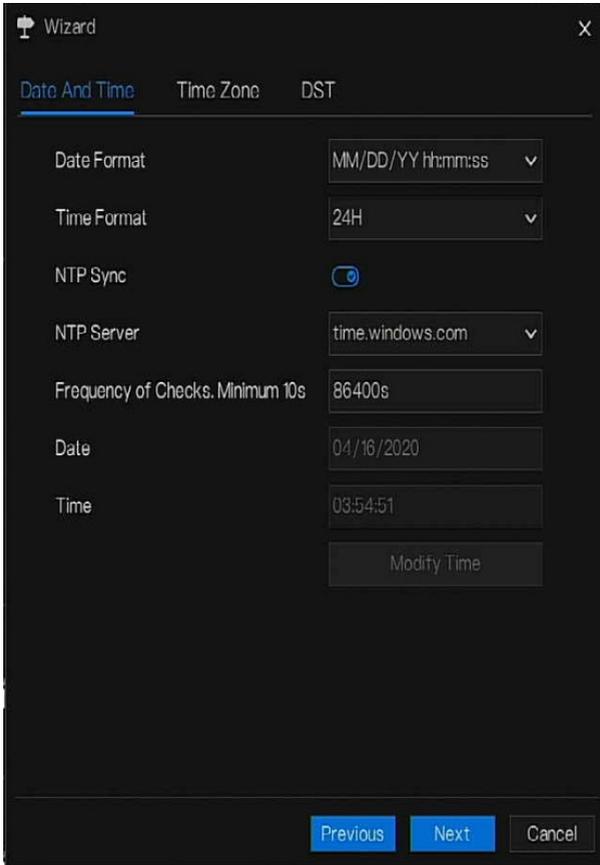
Table 5-1 Network parameter

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 disable	[Setting method] Manual

Parameter	Description	Configuration
Subnet mask	Set the subnet mask of device	[Setting method] Manual [Default value] 255.255.255.0
Gateway	If the user wants to access device, this must be set	[Setting method] Manual [Default value] 192.168.0.1
Obtain DNS automatically	N/A	[Setting method] Enable
DNS 1	N/A	[Setting method] Manual [Default value] 192.168.0.1
DNS 2	N/A	[Setting method] Manual [Default value] 192.168.0.1
UPnP	Auto: device to obtain Web port, data port and client port. Manual: user set the port manually.	[Setting method] Choose type from drop-down list [Default value] Auto
Web Port	N/A	[Setting method] When UPnP is manual, you need to set these.
Data Port	N/A	
Client	N/A	

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

Figure 5-3 Wizard - Date and Time



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

Click  to synchronize time from network.

Disable the NTP-Sync, set time manually.

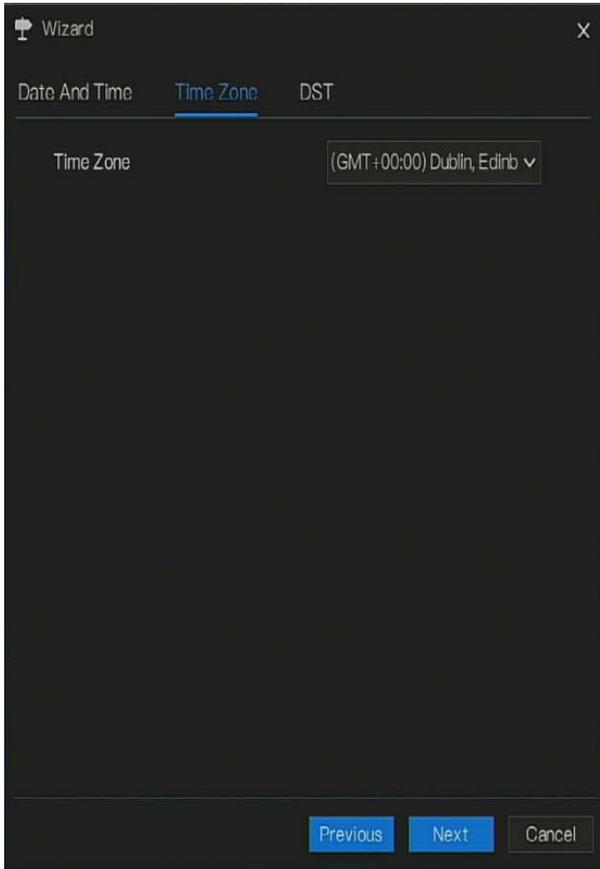
Roll the mouse to choose year, month and day when clicking the date.

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.

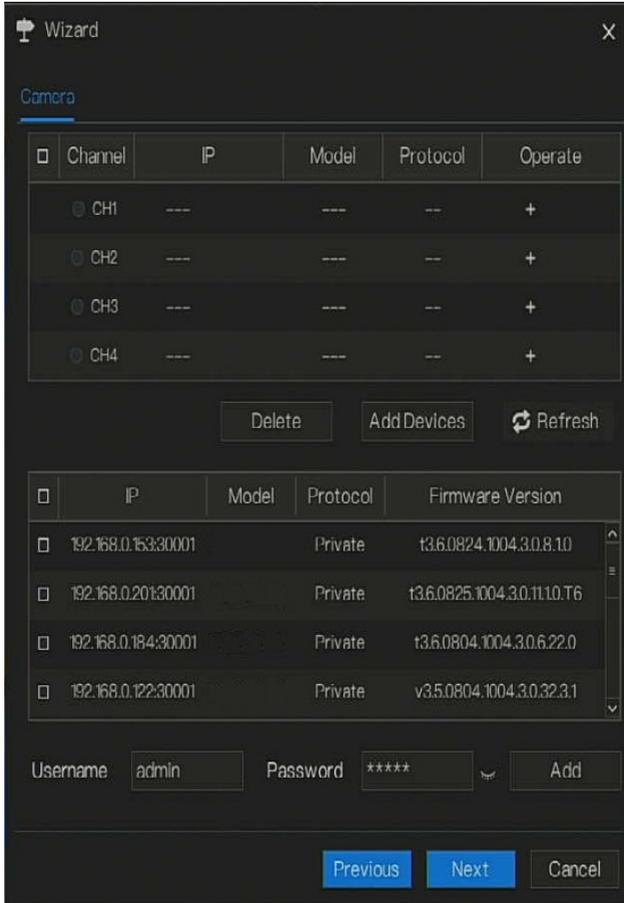
Figure 5-4 Wizard - Time Zone



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

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

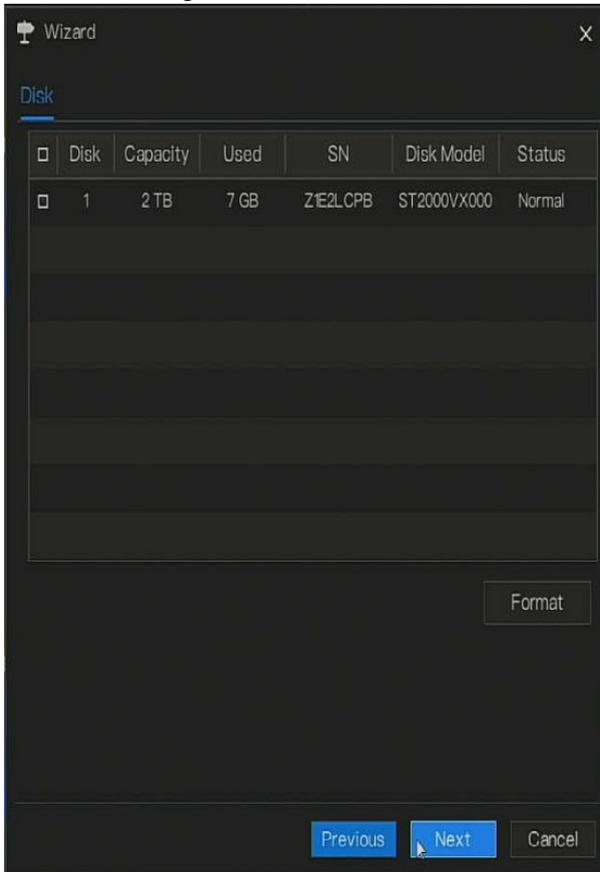
Figure 5-5 Wizard - Adding Camera



The 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.

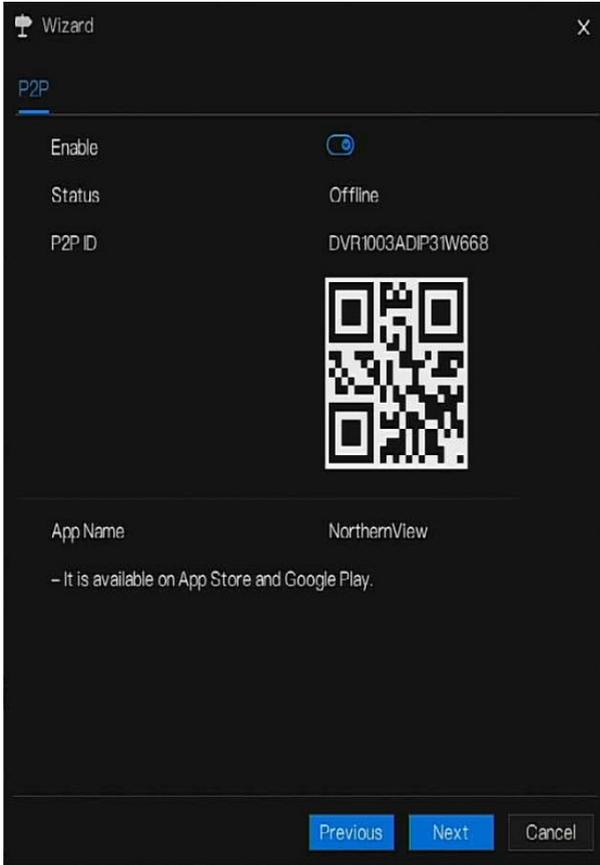
Figure 5-6 Wizard - Disk



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

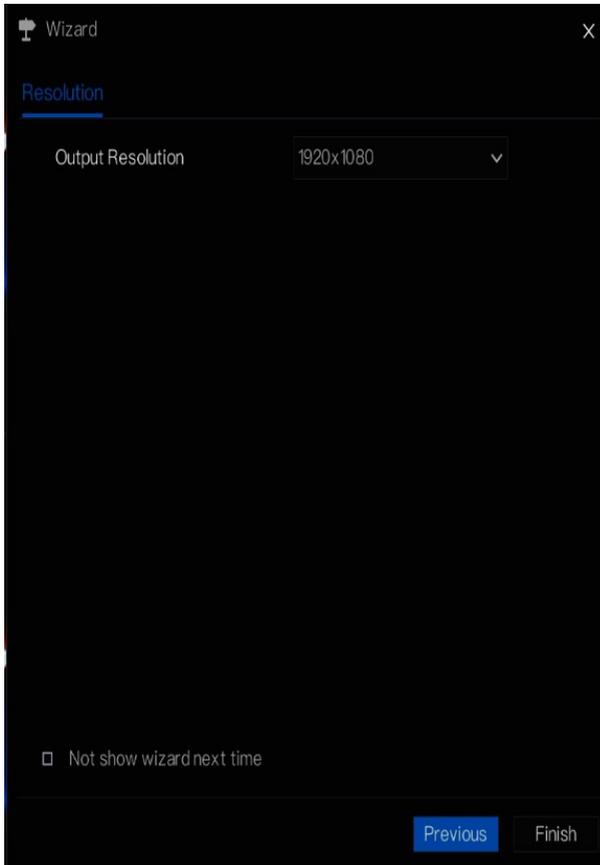
Figure 5-7 Wizard - P2P



Step 8 Enable the P2P, user can use mobile devices to manage the DVR by scanning the P2P ID, if the mobile phone has loaded the NorthernView (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 - Resolution



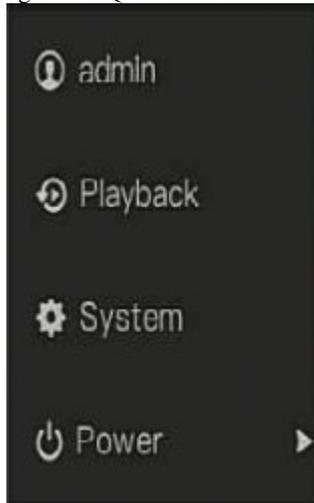
Step 10 Click **Finish** to end the wizard, tick the **Not show this window next time**, wizard would not show at next time. Reopen wizard at **system >user >advance setting**.

6 Quick Navigation

After the DVR operation screen is displaying, move the cursor to the down most position of the DVR screen. The DVR floating menu bar is displaying.

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 **video window switching, auto SEQ, volume, playback, and channel information**, as shown in Figure 6-2.

Figure 6-2 Real-time video toolbar



The real-time video toolbar is described as follows:

Layout. Click the icon, the real-time video window switch between the single-screen mode and multi-screen mode. Click  on the right of screen splitting format and choose the channels to view the video.



: Auto SEQ. click icon, the layout dwell on screen is enabled, for how to set the dwell on, please see *chapter 7.7.5*.



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

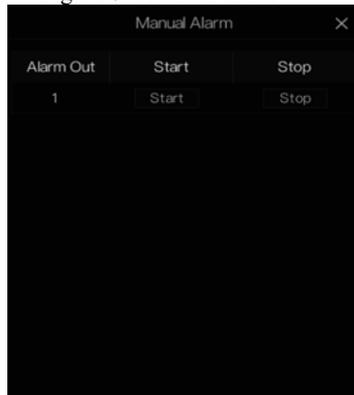
A main menu quick toolbar is display on the right of DVR floating menu bar. The main menu quick toolbar provides **manual alarm, alarm information, clean alarm information** and **time**, as shown in Figure 6-3.

Figure 6-3 Main menu quick toolbar



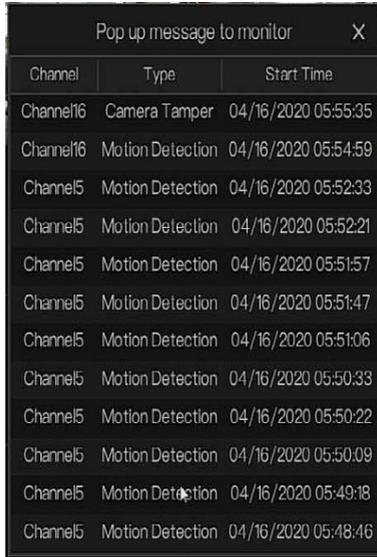
: Manual alarm, click the icon, the window shows in Figure 6-4.

Figure 6-4 Manual alarm



: Alarm message, click icon would show pop-up message window, as shown in 6.1.

6.1 Alarm message



Pop up message to monitor			X
Channel	Type	Start Time	
Channel16	Camera Tamper	04/16/2020 05:55:35	
Channel16	Motion Detection	04/16/2020 05:54:59	
Channel5	Motion Detection	04/16/2020 05:52:33	
Channel5	Motion Detection	04/16/2020 05:52:21	
Channel5	Motion Detection	04/16/2020 05:51:57	
Channel5	Motion Detection	04/16/2020 05:51:47	
Channel5	Motion Detection	04/16/2020 05:51:06	
Channel5	Motion Detection	04/16/2020 05:50:33	
Channel5	Motion Detection	04/16/2020 05:50:22	
Channel5	Motion Detection	04/16/2020 05:50:09	
Channel5	Motion Detection	04/16/2020 05:49:18	
Channel5	Motion Detection	04/16/2020 05:48:46	

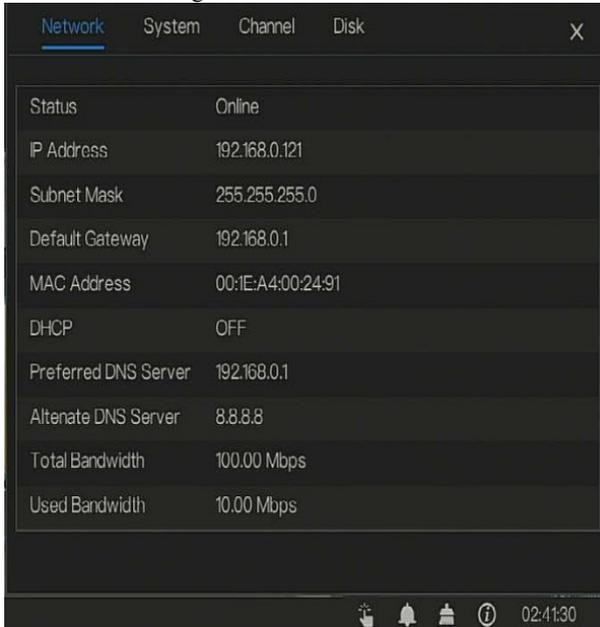


: Clear alarm, click icon and clear the current alarm actions like voice and external alarm out.



: Information, click icon and the general information would show for network, system, channel and disk, as shown in Figure 6-5.

Figure 6-5 Information



Network	System	Channel	Disk
Status	Online		
IP Address	192.168.0.121		
Subnet Mask	255.255.255.0		
Default Gateway	192.168.0.1		
MAC Address	00:1E:A4:00:24:91		
DHCP	OFF		
Preferred DNS Server	192.168.0.1		
Alternate DNS Server	8.8.8.8		
Total Bandwidth	100.00 Mbps		
Used Bandwidth	10.00 Mbps		

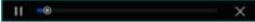
6.2 Real Time Video Bar

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 only is useful for speed dome cameras. You can adjust every parameter as shown in Figure 6-6.

Figure 6-6 PTZ adjust screen



: User adjust direction of IP cameras with PTZ , or adjust the OSD parameters of analog cameras.



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



: click the button to enter the PTZ setting.

Figure 6-7 PTZ setting

Setting	Value
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.

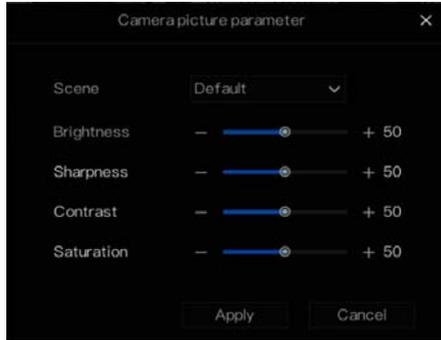


: Zoom in, click zoom in, roll the mouse wheel to zoom in and zoom out. Right-click to exit the zooming.



: Image, click the icon ,as shown in Figure 6-8. Select scene, and drag cursor to adjust value of brightness, sharpness, contrast and saturation.

Figure 6-8 Camera picture parameter

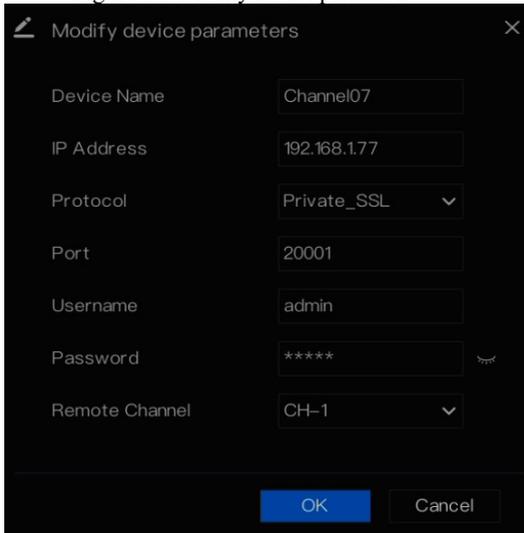


: Two way audio. The DVR and camera can talk to each other.



: Modify device parameters, as shown in Figure 6-9.

Figure 6-9 Modify device parameter

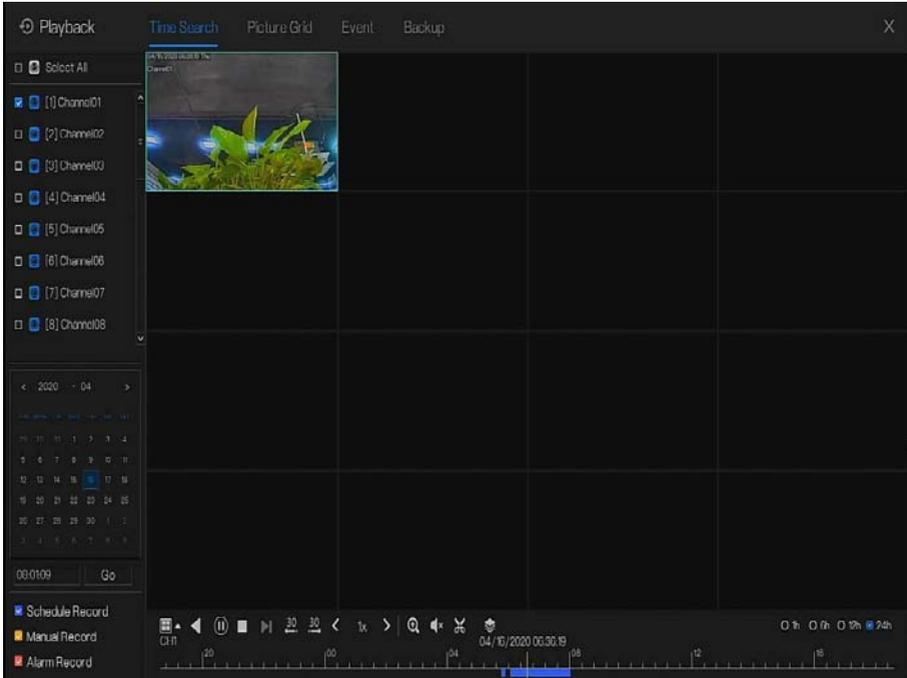


6.3 Playback

Playback refers to playing back a video.

Click  in the quick navigation bar to access the playback screen, as shown in Figure 6-10.

Figure 6-10 Playback screen



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



: Layout.

: Reversed, pause/play, stop.

:30s backward, 30s forward.

:Triple speed, it supports up to 32 times to playback.

: Zoom.

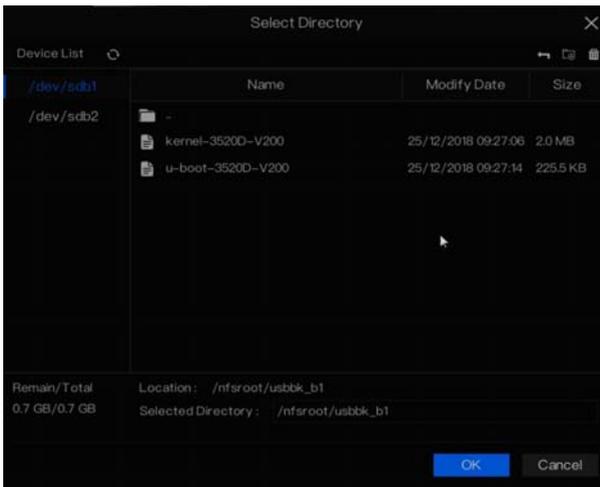
: Audio.

: 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 6-11 . Click **OK** to save.

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

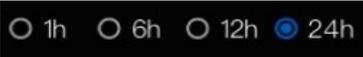
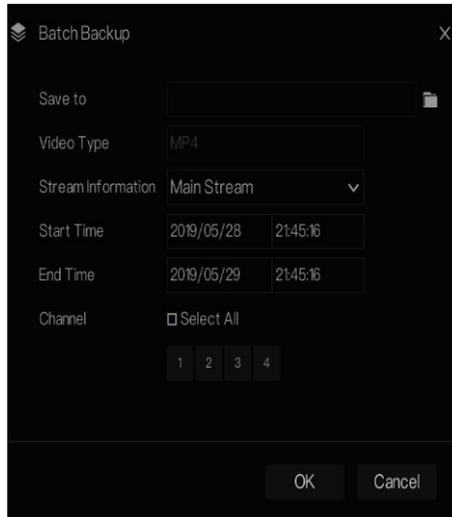
Figure 6-11 Select directory



: Batch backup, click the icon to backup multi-channels, as shown in Figure 6-12.

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.

Figure 6-12 Batch backup



: Type of time bar, recording video can show

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 6-13.

Figure 6-13 Time Search screen



Operation Steps

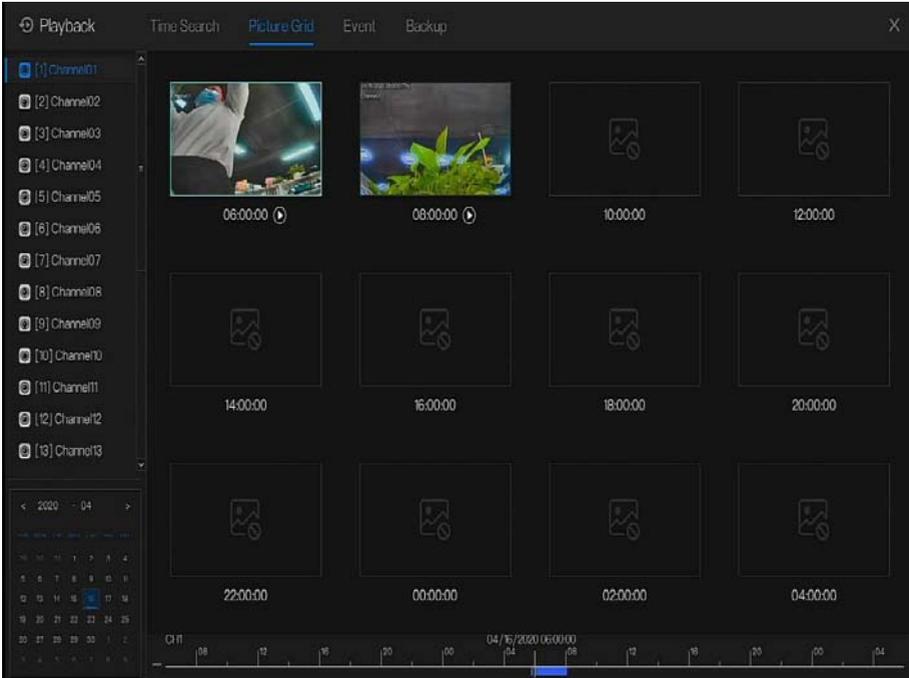
- Step 3 Select a camera in the camera list on the left side of the search screen. The video view of the selected camera is displayed in the play window.
- Step 4 Select a date in the calendar on the left lower side of the search screen.
- Step 5 Choose record type , and search the video quickly.
- Step 6 Choose proper button to adjust video.

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 6-14.

Figure 6-14 Picture grid screen



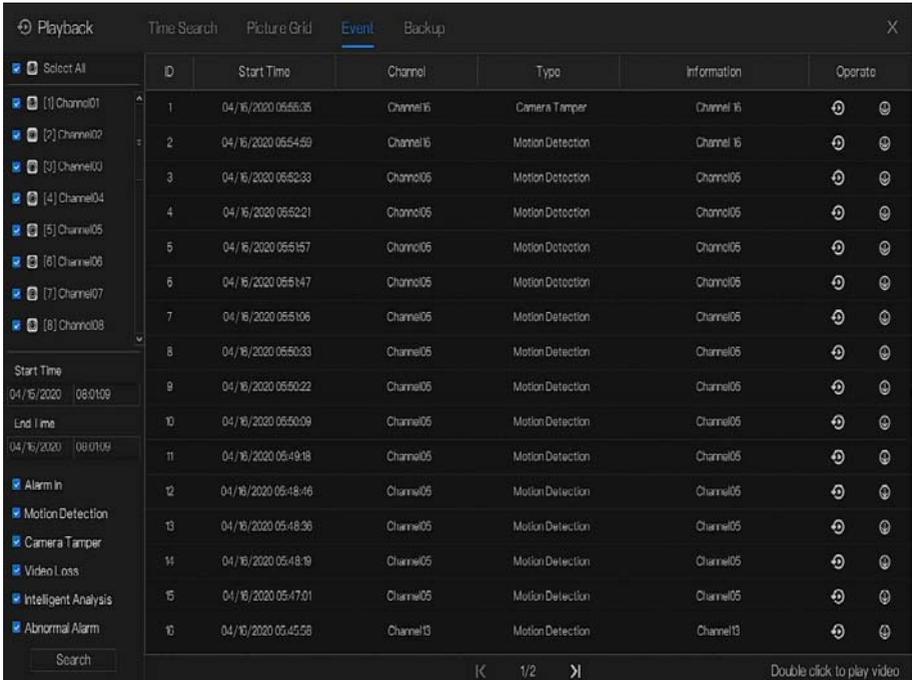
Operation Steps

- Step 1 Select a camera in the camera list on the left side of the picture grid screen. Videos shot by the camera in the earliest time range on the current day are displayed as thumbnails in the window on the right side.
- Step 2 Select a day from calendar.
- Step 3 A day are divided to 12 grids, two hours is 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.

6.3.3 Event

Click  on the quick navigation bar; choose **event** at title to access the alarm event screen, as shown in Figure 6-15

Figure 6-15 Event screen



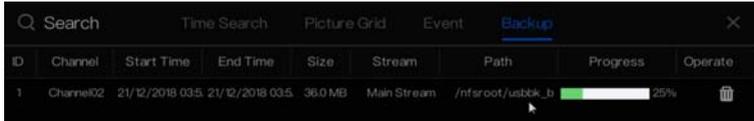
Operation Steps

- 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  to query the event, the result would show at window.
- Step 5 Double click to play video about event. It will play recording video.

6.3.4 Backup

Click  on the quick navigation bar, choose  at title to access the backup screen, as shown in Figure 6-16.

Figure 6-16 Backup screen



The screenshot shows a software interface with a navigation bar at the top containing 'Search', 'Time Search', 'Picture Grid', 'Event', and 'Backup'. Below the navigation bar is a table with the following data:

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

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

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.

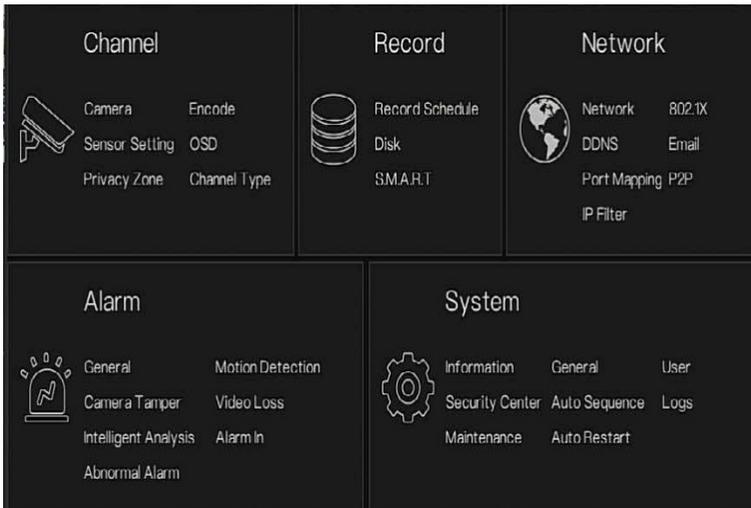
Figure 7-1 Channel information



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



7.3 Channel Management

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

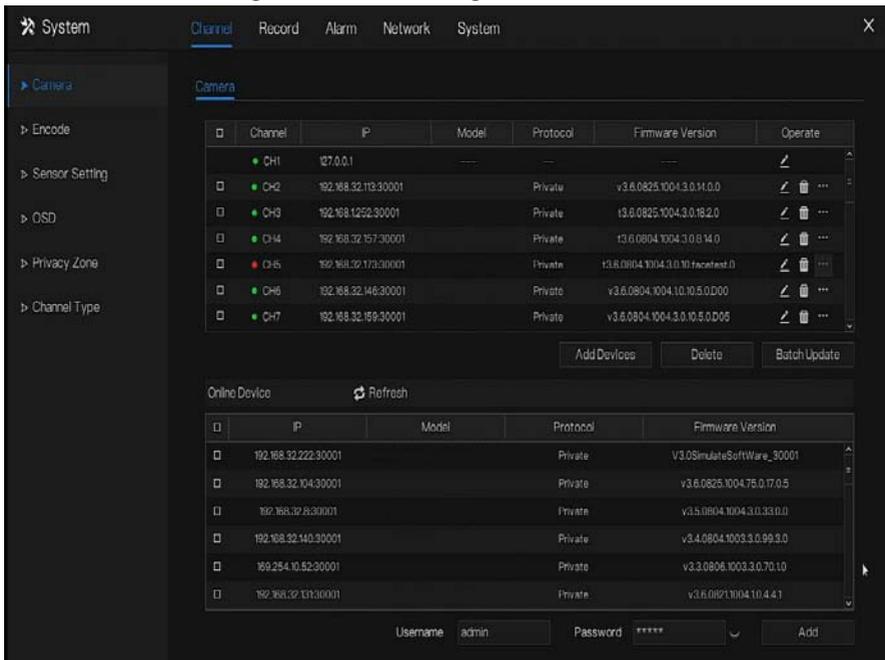
Channel management includes add or delete **Camera**, **Encode**, **Sensor Setting**, **OSD Privacy Zone** and **Channel Type**.

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



7.3.1.1 Add Camera Automatically

The DVR can add automatically cameras to the camera list.

Operation Methods

Method 1: Click  button, the cameras these are the same local area network with DVR will show in list, input username and password. Click , the cameras in the list would be added to channels directly.

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

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



NOTE

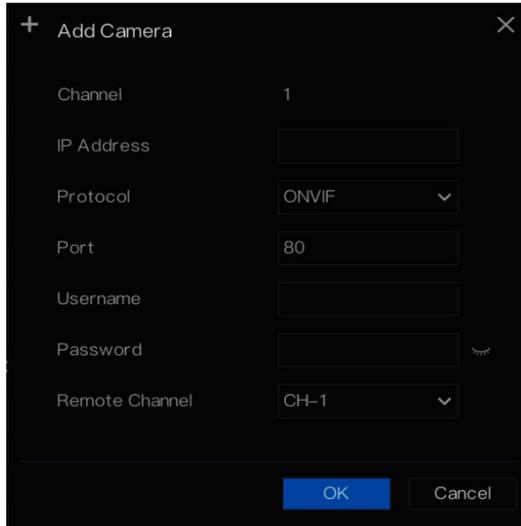
- On the camera management screen, check the status of channel in the camera list. If the status of a channel is , this camera is online. If the status of a channel is , this camera is offline.
- The added cameras should be the same network segment as DVR.

7.3.1.2 Add Camera Manually

Operation Steps

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

Figure 7-4 Add camera screen



+	Add Camera	×
Channel	1	
IP Address	<input type="text"/>	
Protocol	ONVIF	▼
Port	80	
Username	<input type="text"/>	
Password	<input type="password"/>	🔍
Remote Channel	CH-1	▼
OK		Cancel

Step 2 Input IP address, 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 , 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.

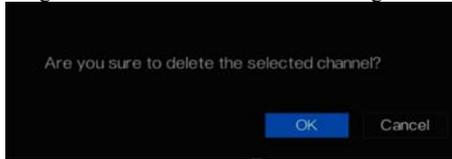
If a IP camera is added manually, input the correct username and password of the camera below the online device list. The camera will be added successfully. If not the camera would be shown on list at offline.

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 displaying, as shown in Figure 7-5.

Figure 7-5 Delete confirmation message

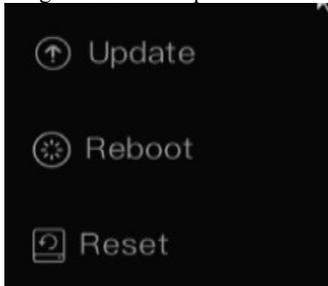


Step 2 Click , the camera is deleted successfully.

7.3.1.4 Operate Camera

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

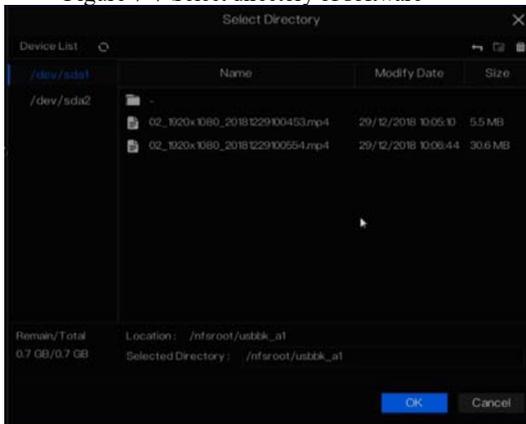
Figure 7-6 More operation



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

Step 2 Set the directory click  to update camera.

Figure 7-7 Select directory of software



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

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

 **NOTE**

Update need upload the software by flash driver.

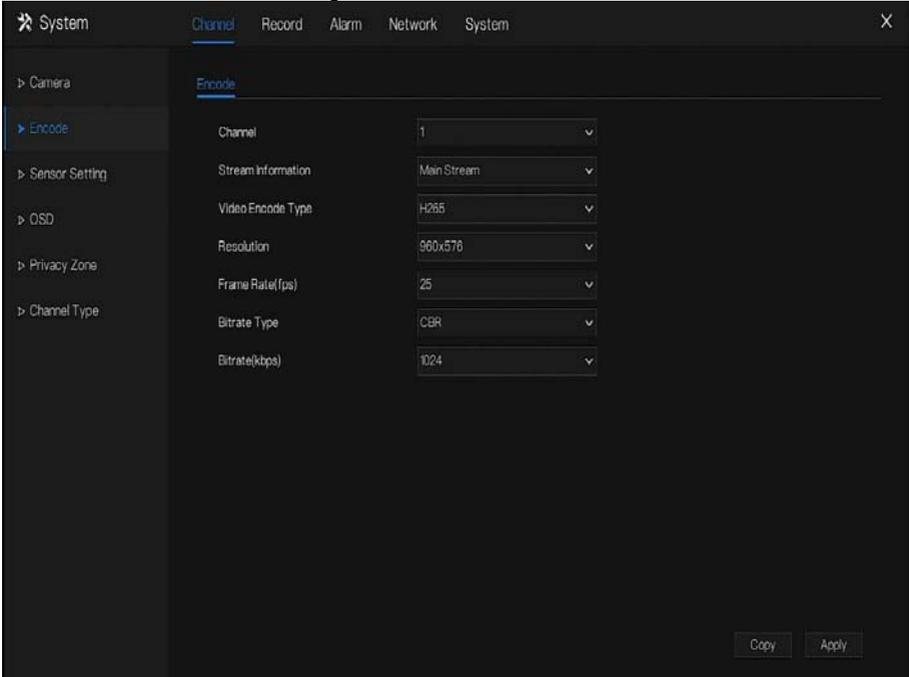
7.3.2 Encode Parameter

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 7-8.

Figure 7-8 Encode screen



Operation Steps

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

Step 2 Select stream information.

Step 3 Select encode type, resolution, frame rate, bitrate type and bitrate size from the drop-down lists.

Step 4 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.

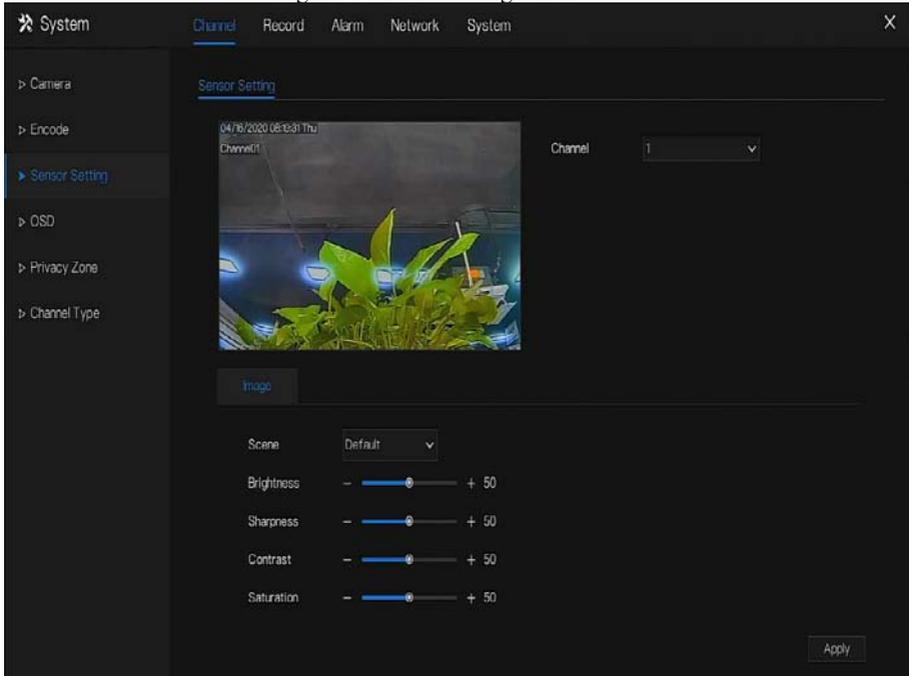
7.3.3 Sensor Setting

Sensor setting refer to basic attributes of pictures, it includes the 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 7-9.

Figure 7-9 Sensor setting screen



The Sensor Setting are 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: user 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: user can zoom and focus.

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.

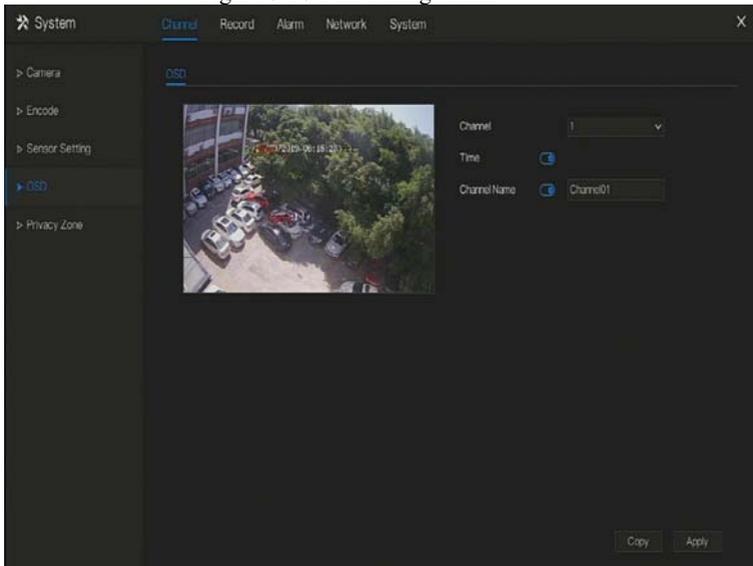
Step 3 Set parameters.

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

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 7-10.

Figure 7-10 OSD setting screen



Operation Steps

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

Step 2 Click **Time** 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  and select channels, then click  to apply the OSD settings to cameras in selected channels , click  to save OSD settings.

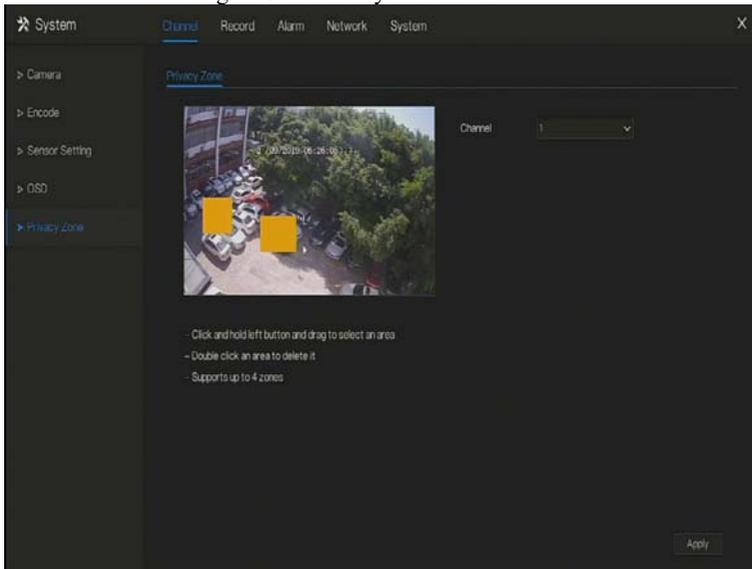
7.3.5 Privacy Zone

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 7-11.

Figure 7-11 Privacy zone screen



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.

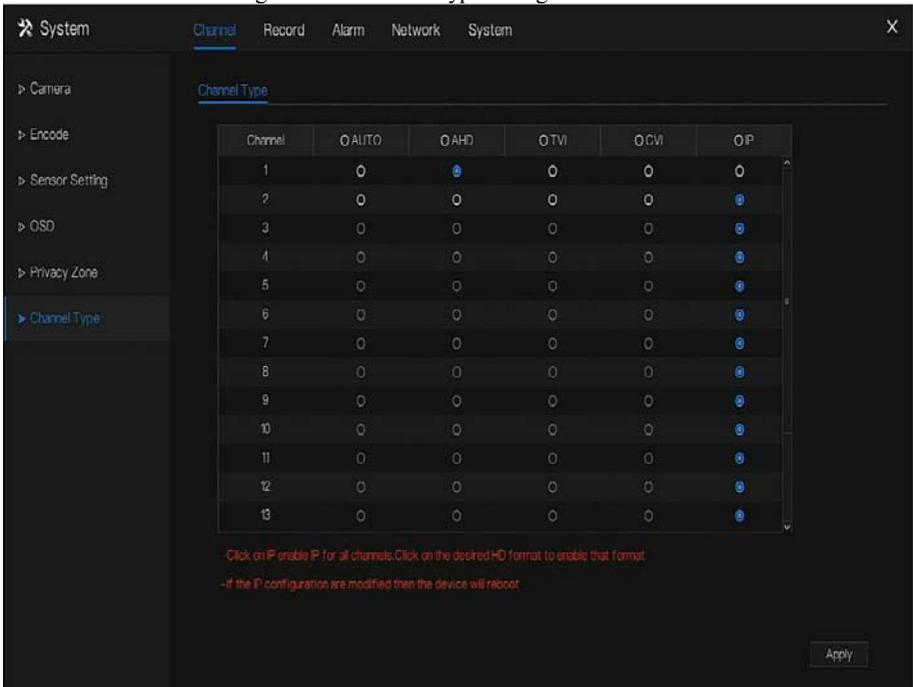
Step 3 Click **Copy** and select channels or tick **all**, then click **OK** to apply the privacy settings to cameras in selected channels , click **Apply** to save privacy settings.

Step 4 Double click privacy area to delete setting.

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 7-12.

Figure 7-12 Channel Type setting screen



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.

7.4 Record Setting

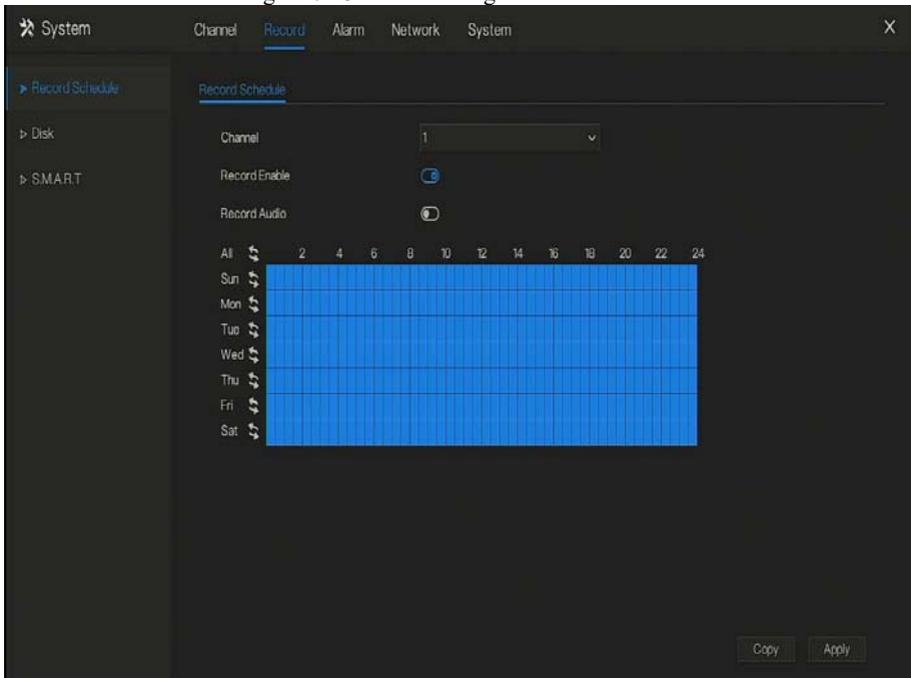
Set the **Record Schedule**, view the disk capacity, examine the record' status.

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 7-13.

Figure 7-13 Record management screen



Operation Steps

- Step 1 Select a channel from the drop-down list of channel.
- Step 2 Enable the record enable.
- Step 3 Enable the record audio.

Step 4 Set the record schedule. **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 is all week.

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

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

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

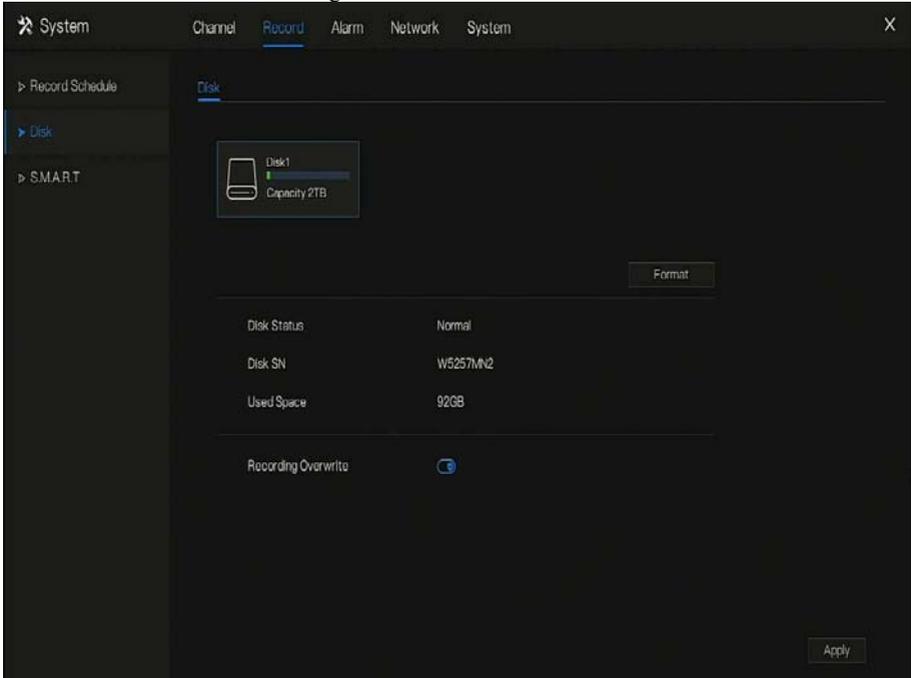
7.4.2 Disk

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 7-14.

Figure 7-14 Disk screen



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

Step 3 Click **OK**, and the disk would be formatted.

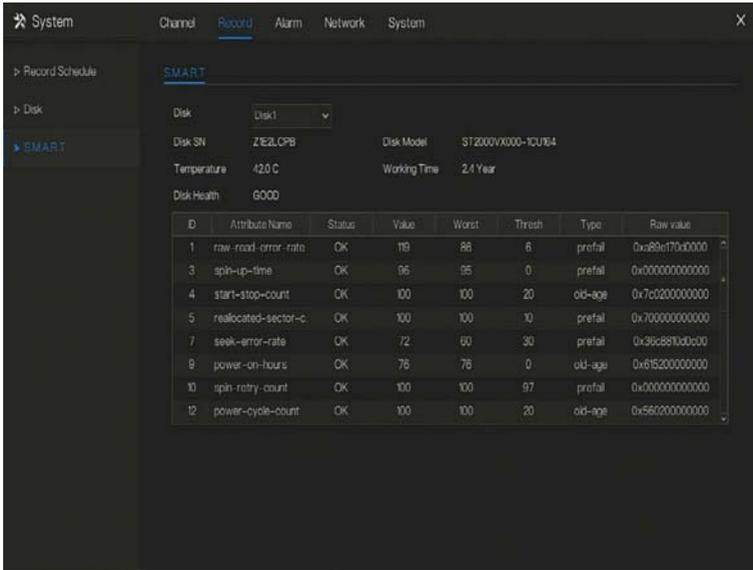
Step 4 Record expiration setting. Select record expiration days from the drop-down list of record expiration.

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

7.4.3 S.M.A.R.T

S.M.A.R.T is Self-Monitoring Analysis and Reporting Technology, user can view the health of disk, as shown in Figure 7-15.

Figure 7-15 S.M.A.R.T



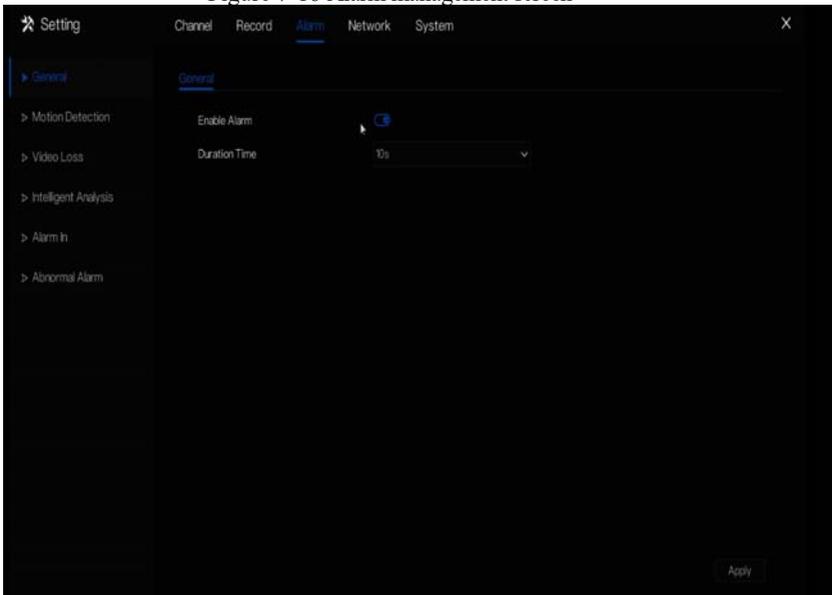
7.5 Alarm Management

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

7.5.1 General

Step 3 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 7-16.

Figure 7-16 Alarm management screen



Step 4 Enable the Enable alarm button.

Step 5 Select a value from the drop-down list of duration time.

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

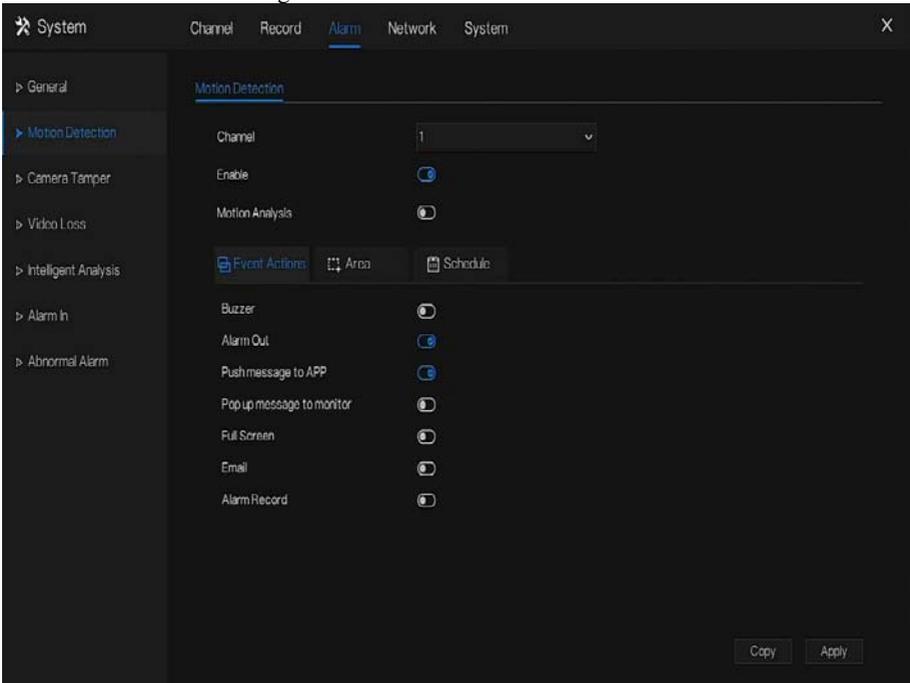
7.5.2 Motion Detection

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 7-17.

Figure 7-17 Motion detection screen



Operation Steps

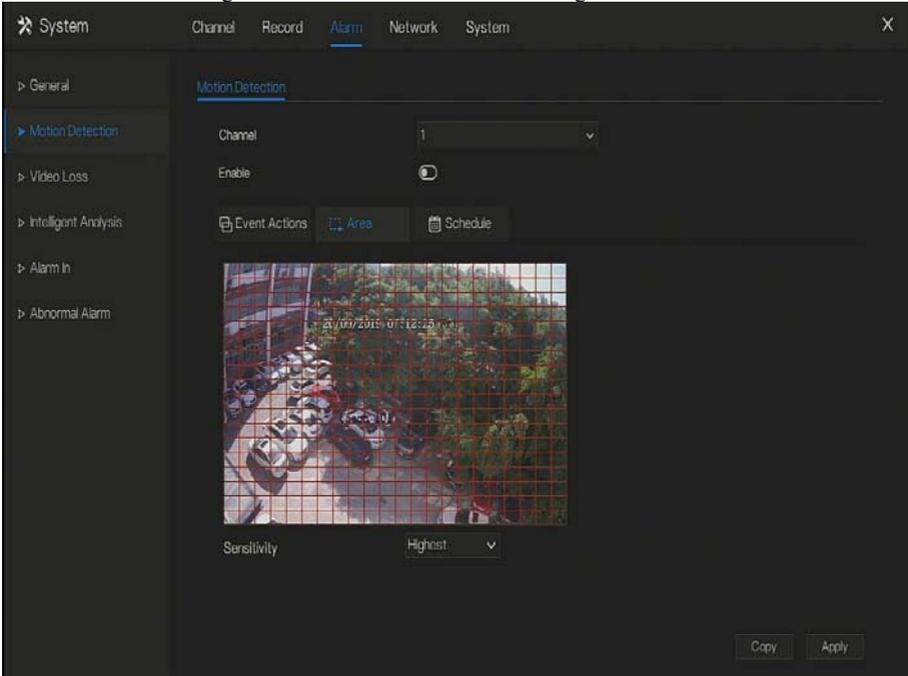
Step 2 Select a channel from the drop-down list of channel.

Step 3 Click  to enable motion detection.

Step 4 Enable the Event actions include: buzzer, alarm out, push message, pop up message, full screen, send E-mail and alarm record.

Step 5 Click Area page to access the motion detection area setting, as shown in Figure 7-18.

Figure 7-18 Motion detection area setting screen



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

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

NOTE

After a motion detection area is selected, double-click it to delete the selected area.

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.

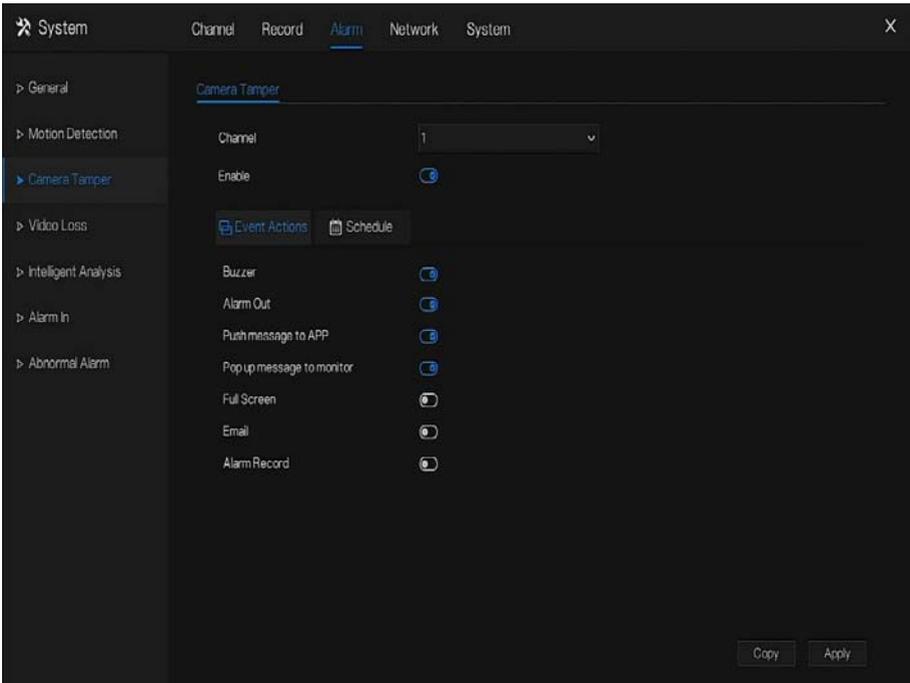
7.5.3 Camera Tamper

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 7-20.

Figure 7-19 Camera Tamper screen



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 include: buzzer, alarm out, push message, pop up message, send E-mail and post recording.

Step 4 Click Schedule page to access the schedule screen.

Step 5 For details, please see 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.

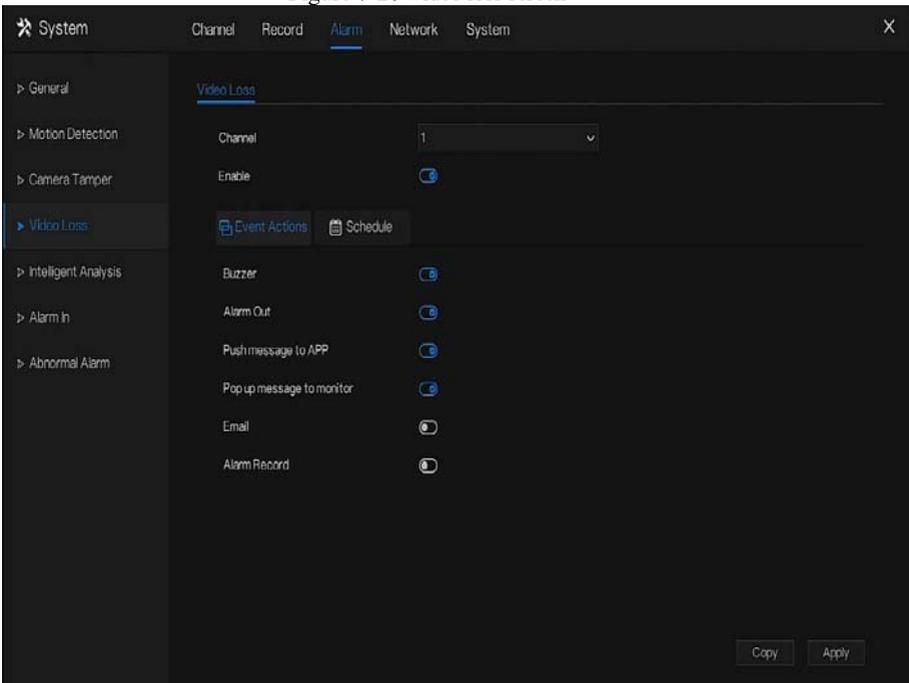
7.5.4 Video Loss

If a camera is disconnected to DVR, it will trigger video loss alarm.

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 7-20.

Figure 7-20 Video loss screen



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 include: buzzer, alarm out, push message, pop up message, send E-mail and post recording.

Step 4 Click Schedule page to access the schedule screen.

Step 5 For details, please see 7.4.1 Record Schedule Set the record schedule.

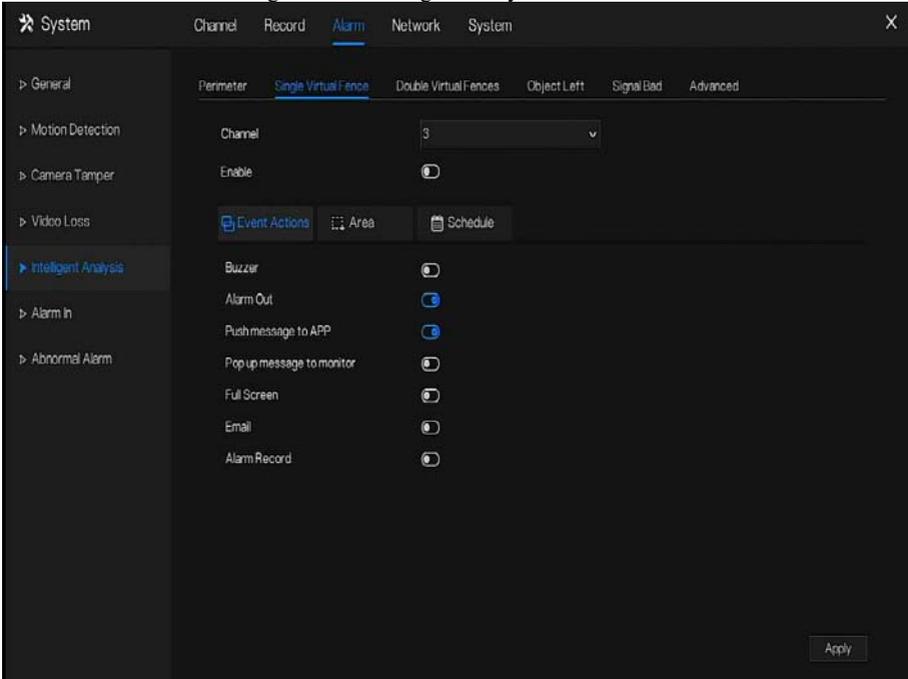
Step 6 Click  and select a channel, then click  to apply the parameter settings to cameras in selected channels, click  to save video loss settings.

7.5.5 Intelligent Analysis

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 7-6.

Figure 7-21 Intelligent Analysis screen



Step 2 Select one action to set the alarm.(perimeter, single virtual fence, double virtual fences, object left, signal bad, advanced)

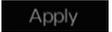
Step 3 Select a channel from the drop-down list of channel.

Step 4 Click  to enable intelligent analysis alarm.

Step 5 Enable the event actions include: buzzer, alarm out, push message, pop up message, send E-mail and post recording.

Step 6 Click Schedule page to access the schedule screen.

Step 7 For details, please see Set the record schedule.

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

7.5.6 Alarm In

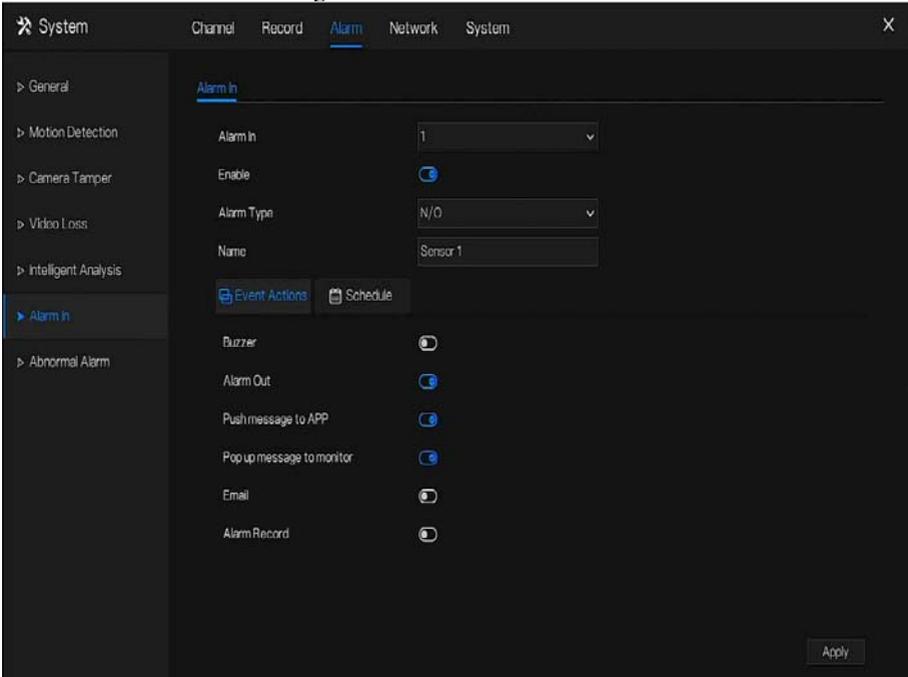
NOTE

Some devices may not have the function.

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 7-22.

Figure 7-22 Alarm in screen



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 include: buzzer, alarm out, push message, pop up message, send E-mail and post 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.

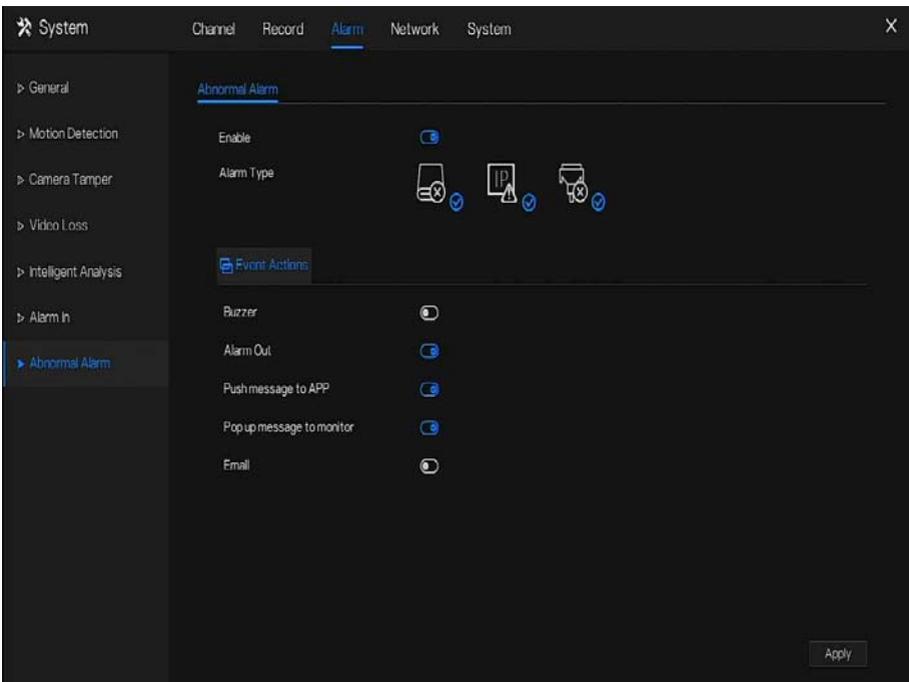
7.5.7 Abnormal Alarm

Camera tamper means that the DVR would send alarm notification while objects cover 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 7-23.

Figure 7-23 Abnormal alarm screen



Operation Steps

Step 2 Tick the abnormal actions.

Step 3 Enable the event actions include: buzzer, alarm out, push message, pop up message, send E-mail and post recording.

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

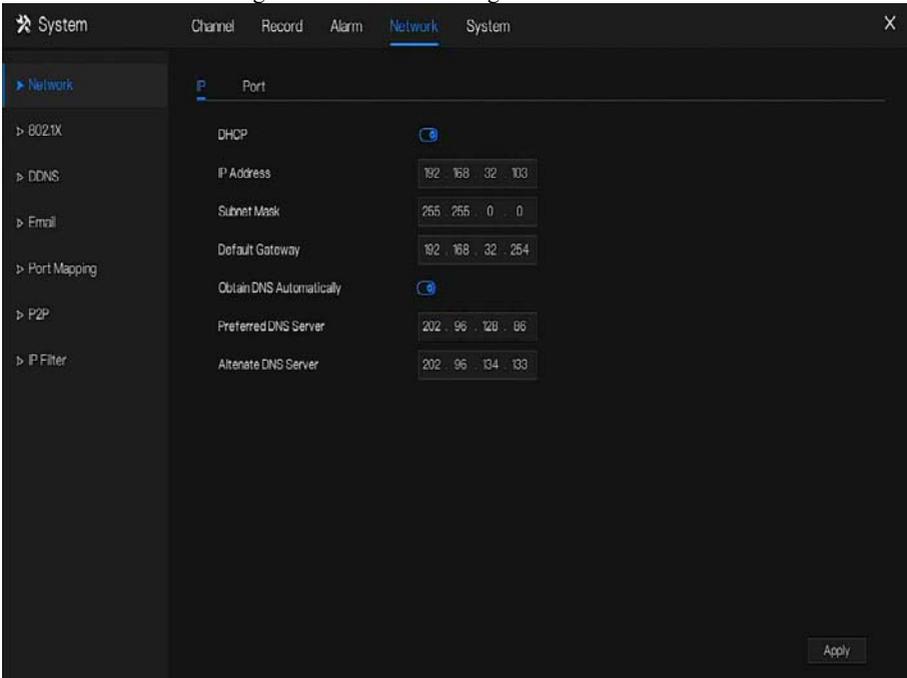
7.6 Network Management

Set the **Network Parameter, 802.1X, DDNS, E-mail, Port Mapping, P2P, IP Filter, 3G/4G** and **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 7-24.

Figure 7-24 Network management screen



7.6.1 Network

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

7.6.1.1 IP

Operation Steps

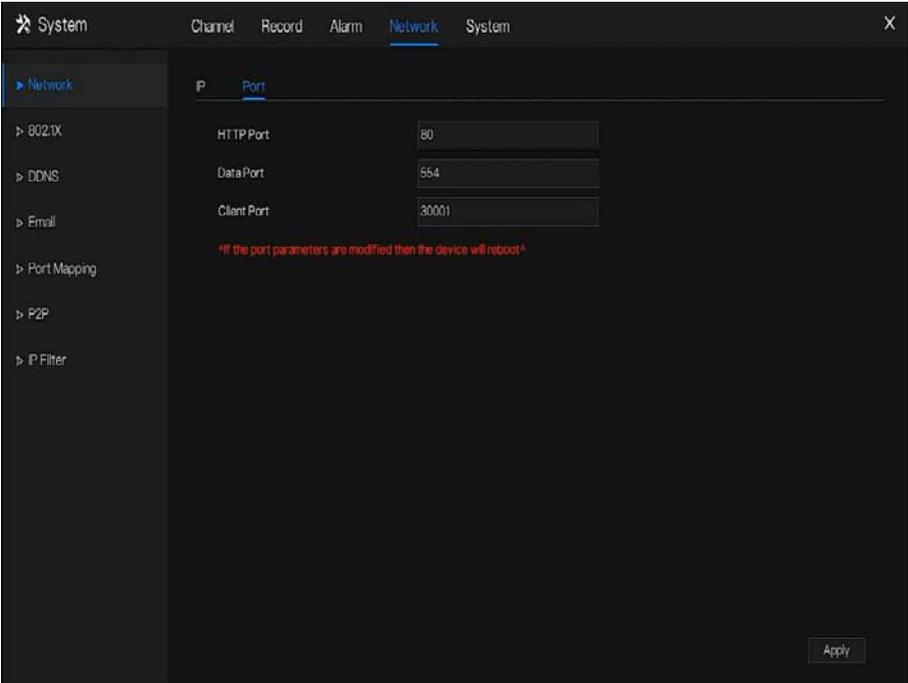
- Step 1 Click  next to **DHCP** to enable or disable the function of automatically getting an IP address. The function is disabled by default.
- Step 2 If the function is disabled, click input boxes next to **IP**, **Subnet mask**, and **Gateway** to set the parameters as required.
- Step 3 Click  next 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 original address, and enter new address.
- Step 5 Click  to save IP settings.

7.6.1.2 Port

Operation Steps

Step 1 Click **Port** page to access the port setting screen, as shown in Figure 7-25.

Figure 7-25 Port setting screen



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

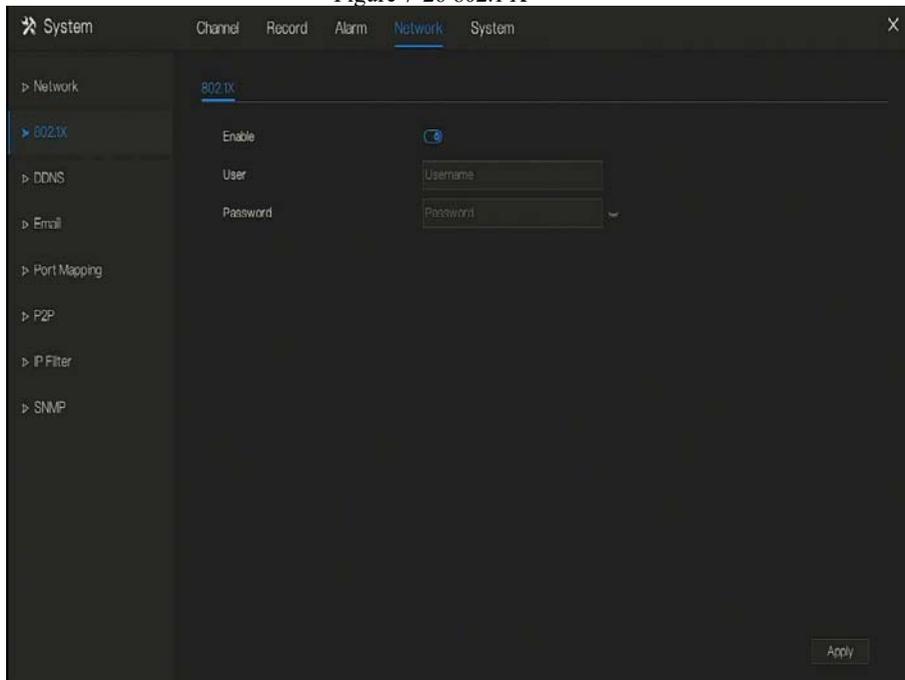
Step 3 Click **Apply** to save port settings.

7.6.2 802.1 X

Operation Steps

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

Figure 7-26 802.1 X



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

Step 3 Click  to save the settings. The visitor to view the DVR need to input account to certify.

7.6.3 DDNS

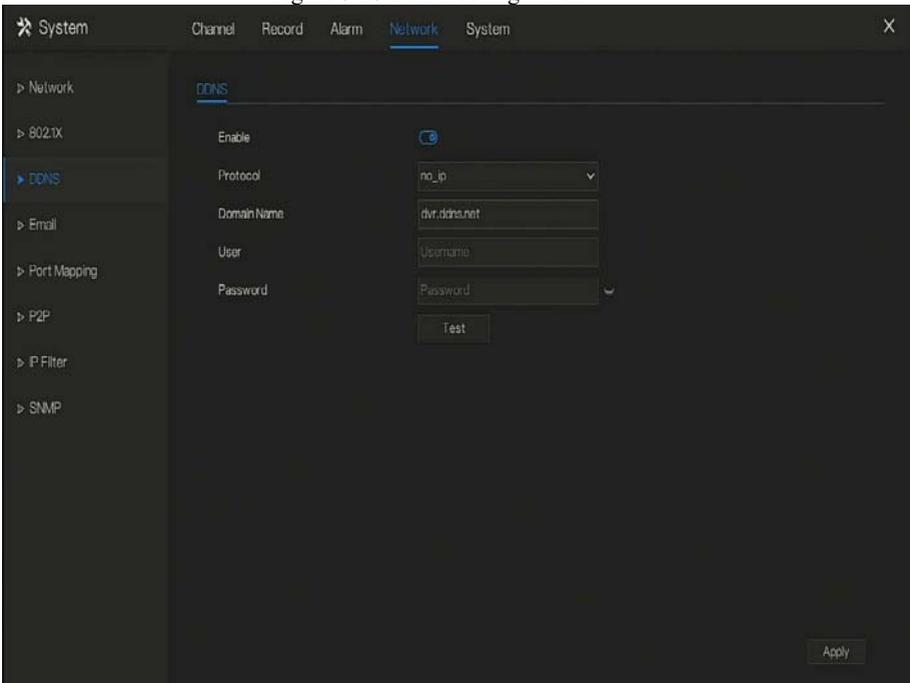
Please make sure of connecting the specified camera to the Internet, and obtain the user name and password for logging into the dynamic domain name system (DDNS) from the server.

Operation Steps

Step 1 Click **DDNS** 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 7-27.

Figure 7-27 DDNS setting screen



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

Step 4 Set domain name, input user and password.

Step 5 Click  to check the domain name.

Step 6 Click  to save DDNS network settings

NOTE

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

7.6.4 E-mail

If the simple mail transfer protocol (SMTP) function is enabling, the device automatically sends alarm information to specified email addresses when an alarm is generated.

Operation Steps

Step 1 Click **E-mail** in the main menu or menu of the network management screen and choose **E-mail** to access the E-mail screen, as shown in Figure 7-28.

Figure 7-28 E-mail setting screen

The screenshot shows the 'E-mail' configuration screen within a 'System' menu. The interface is dark-themed. On the left, a sidebar lists various system settings: Network, 802.1X, DDNS, Email (highlighted), Port Mapping, P2P, IP Filter, and SNMP. The main area is titled 'Email' and contains several input fields: '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), and 'SSL Encryption' (OFF). A 'Test' button is located below the input fields. An 'Apply' button is in the bottom right corner.

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 receive 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 retrieve 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.

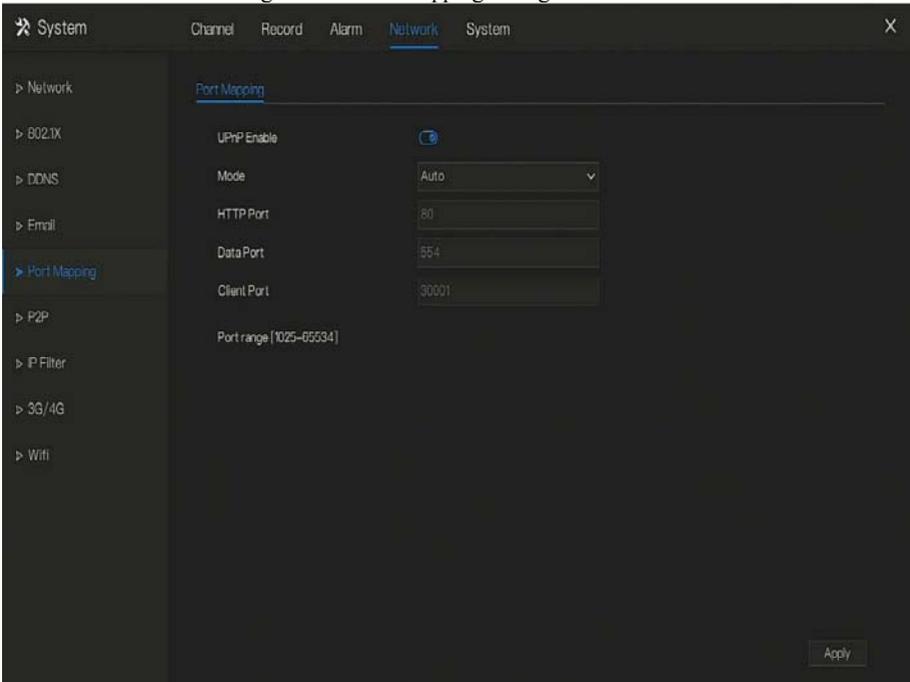
Step 7 Click **Apply** to save settings.

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 7-29.

Figure 7-29 Port mapping setting screen



Step 2 Select UPnP enable type.

Step 3 Manual UPnP: input http port, data port and client port manually.

Step 4 Auto UPnP: device obtain the port automatically.

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

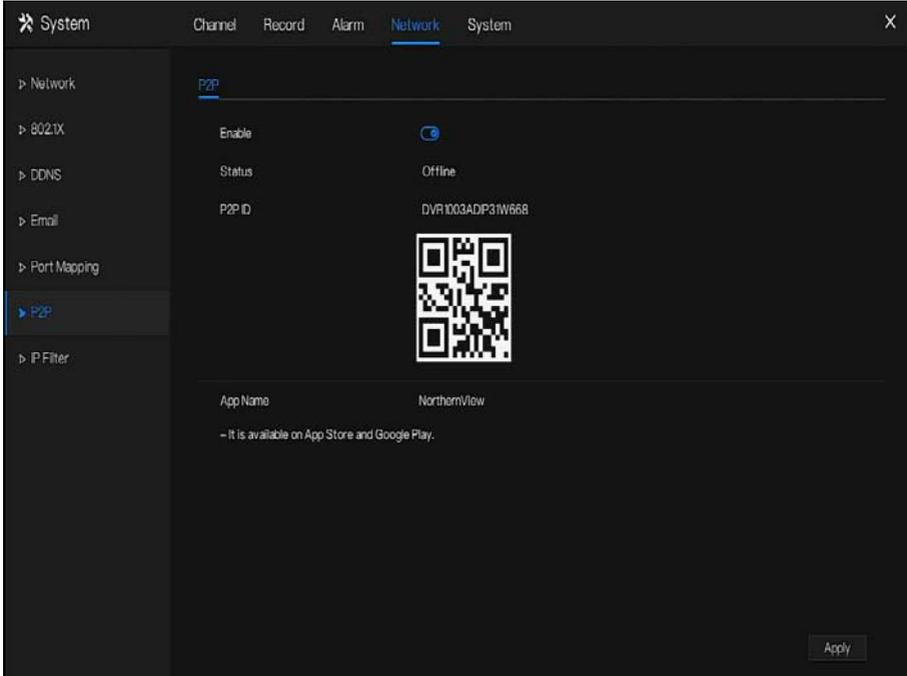
7.6.6 P2P

Show the UDID 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 7-30.

Figure 7-30 P2P screen



Step 2 Click  to enable the P2P function.

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

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

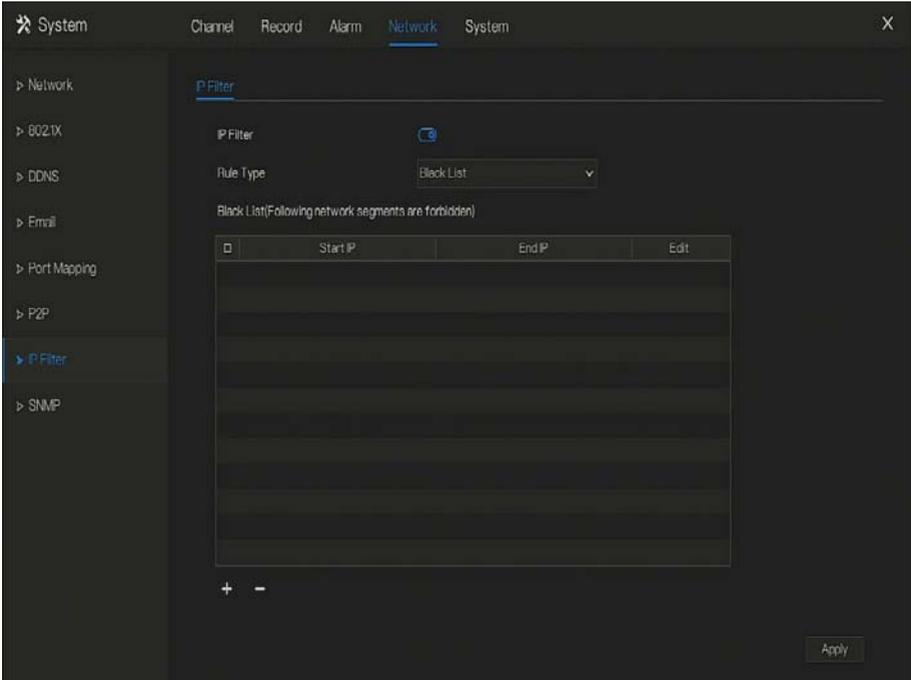
7.6.7 IP Filter

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 7-31.

Figure 7-31 IP Filter setting screen

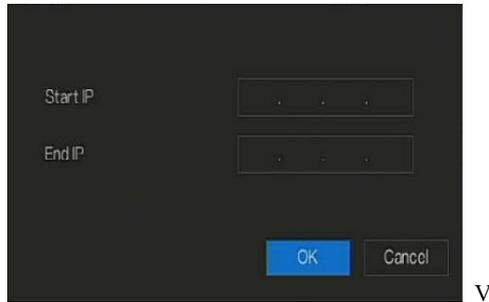


Step 2 Click  next to **IP Filter** to enable the function of IP Filter.

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

Step 4 Click  to set black & white list IP segment screen is displaying, as show in Figure 7-32.

Figure 7-32 IP Address Segment screen



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

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



NOTE

Black list: IP address in specified network segment to prohibit access.

White list: IP address in specified network segment to allow access

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

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

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

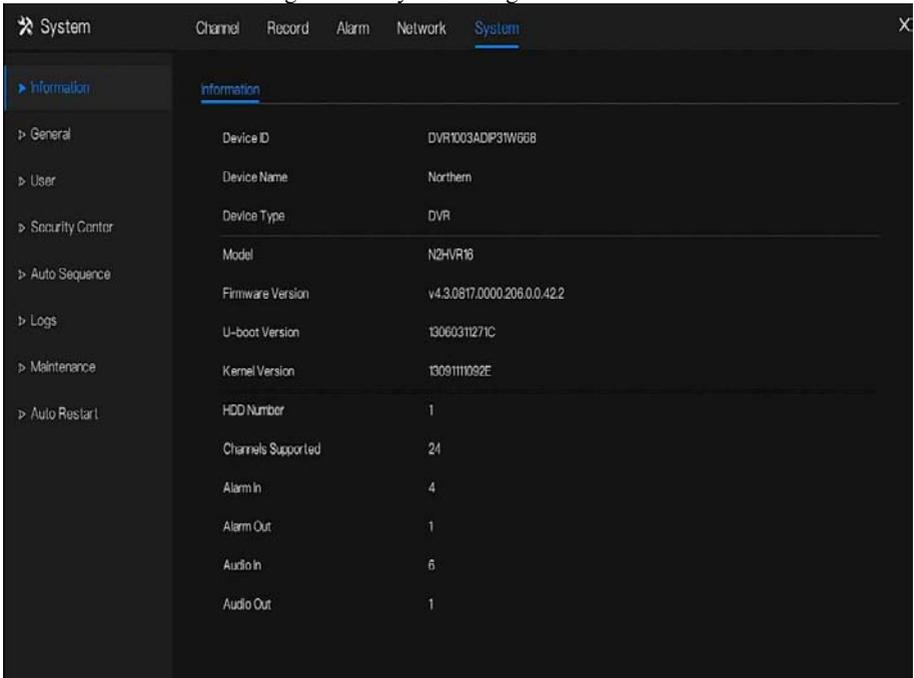
7.7 System Management

View the device **Information** and set **General** information, **User**, **Security Center**, **Auto Sequence**, **Logs**, **Maintenance** and **Auto Restart** 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 7-33.

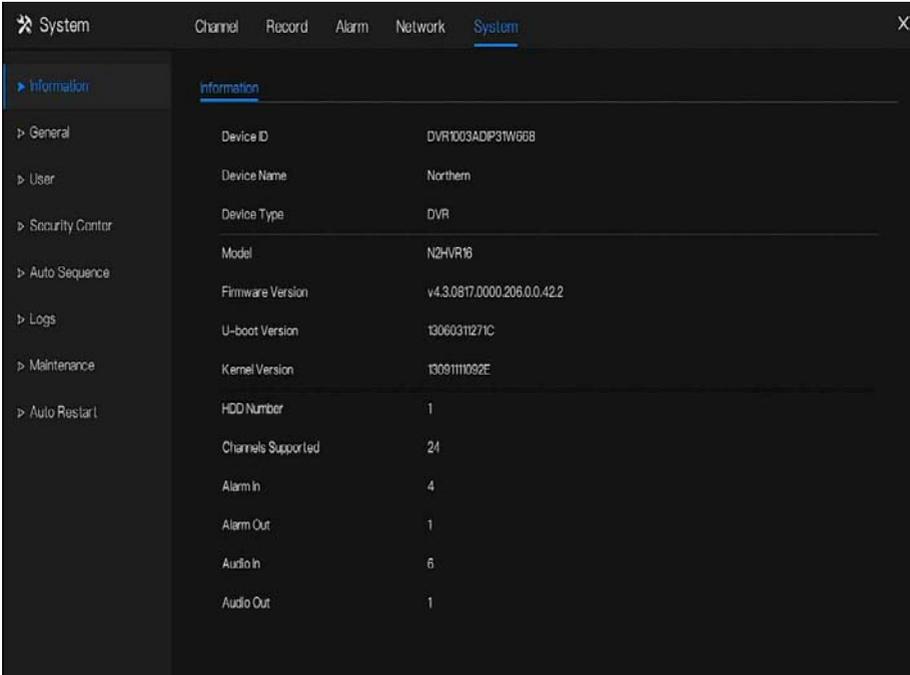
Figure 7-33 System setting screen



7.7.1 Information

View the device ID, device name, device type, model, firmware version, HDD volume, channel support, alarm in, and alarm out, audio in, audio out in **information** screen, as shown in Figure 7-34 .

Figure 7-34 Information interface

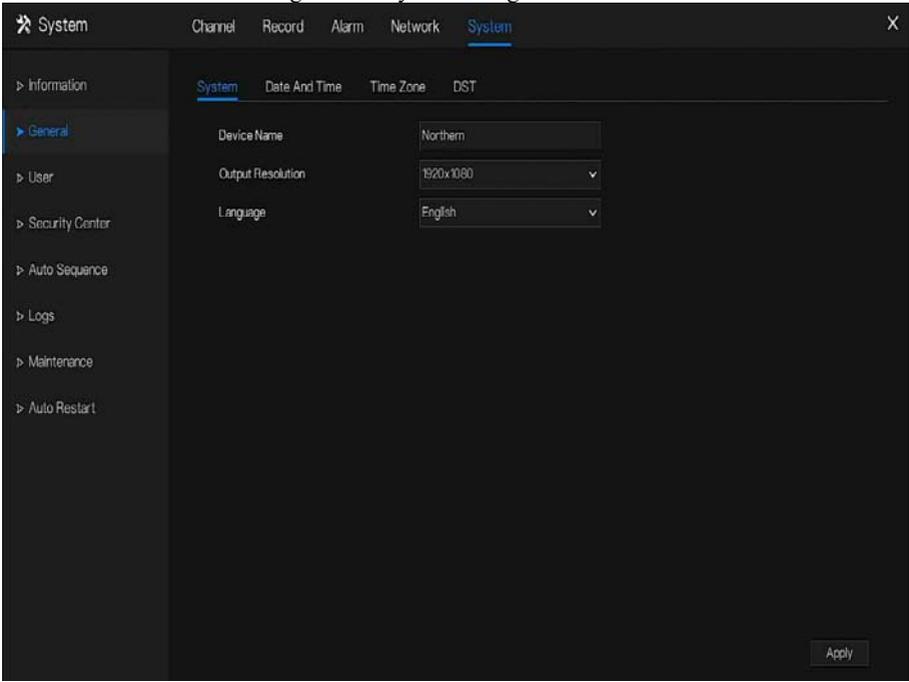


7.7.2 General

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 7-35.

Figure 7-35 system setting screen



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.

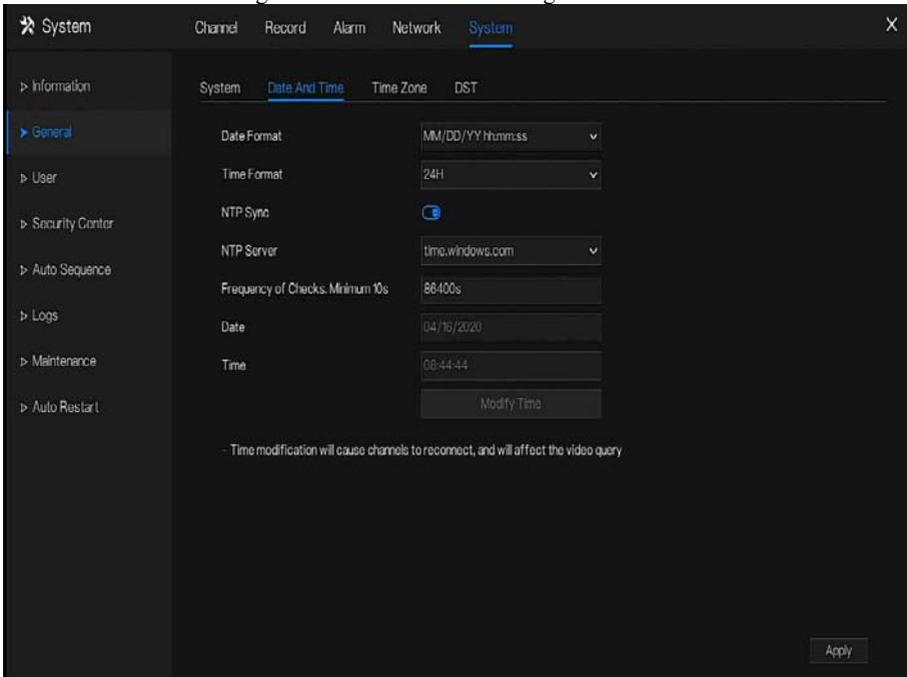
Step 5 Click **Apply** to save settings.

7.7.2.1 Date and Time

Operation Steps

Step 1 Click **Date and Time** page to access the date and time setting screen, as shown in Figure 7-36.

Figure 7-36 Date and Time setting screen



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 scroll the mouse scroll wheel to select the year, month, and date.

Click **Time** and scroll the mouse scroll wheel to select the hour, minute, and second.

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

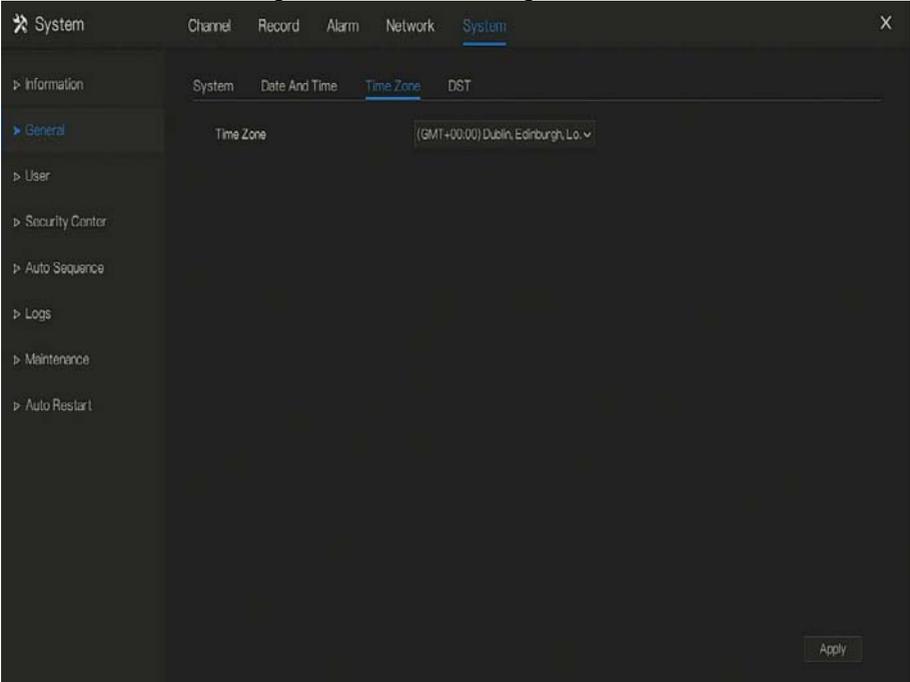
Step 5 Click Apply to save settings.

7.7.2.2 Time Zone

Operation Steps

Step 1 Click **Time zone** page to access the time zone setting screen, as shown in Figure 7-37.

Figure 7-37 Time zone setting screen



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

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

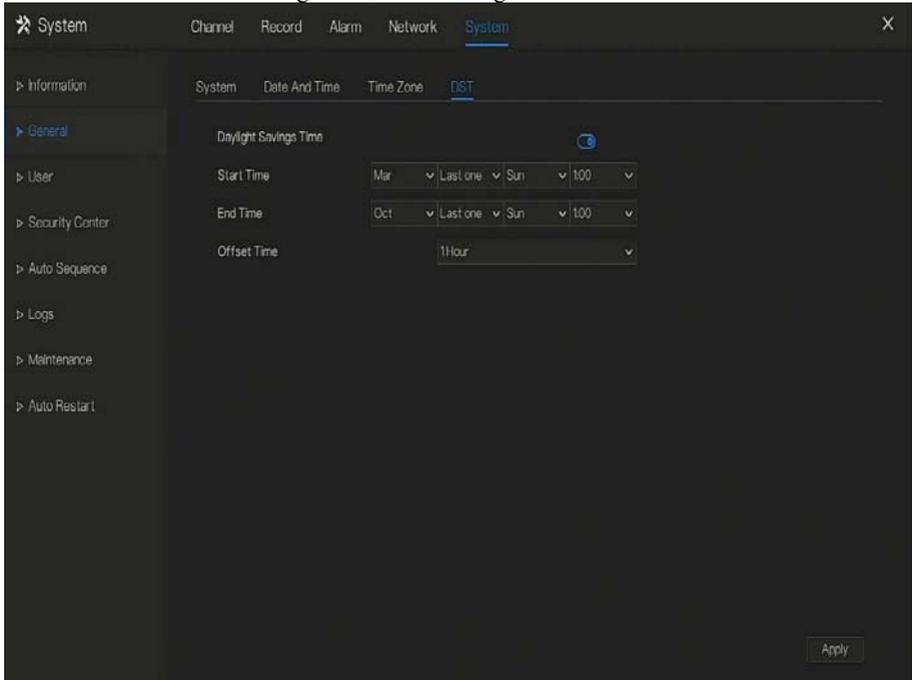
7.7.2.3 DST

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

Operation Steps

Step 1 Click **DST** page to access the DST setting screen, as shown in Figure 7-38.

Figure 7-38 DST setting screen



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 basis on the local rules.

Step 4 Click  to save settings.

7.7.3 User

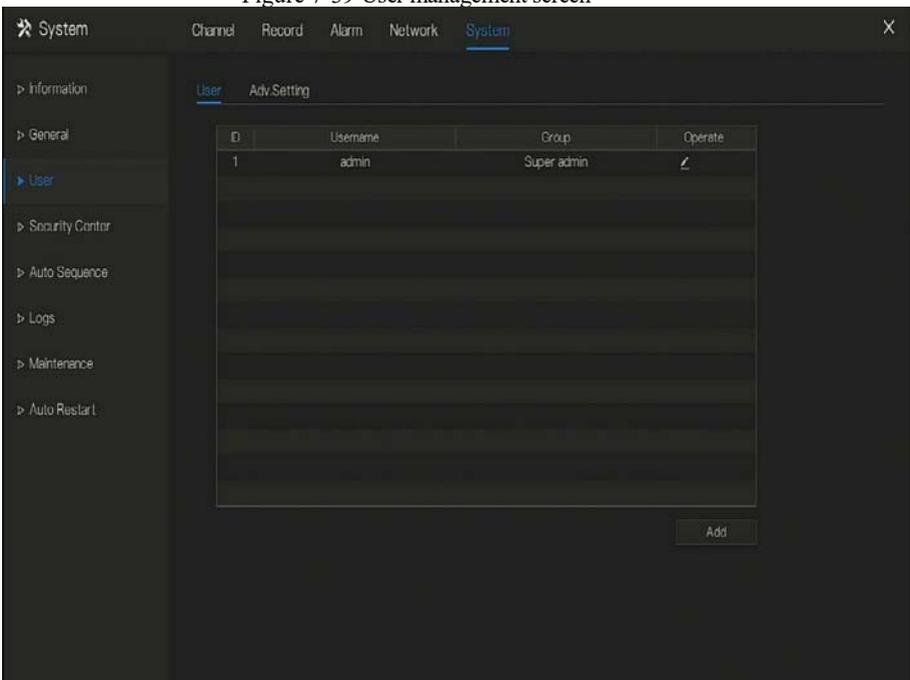
Add, modify, and delete a user and privilege in user screen, admin user can dispose privilege to different user.

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 7-39.

Figure 7-39 User management screen

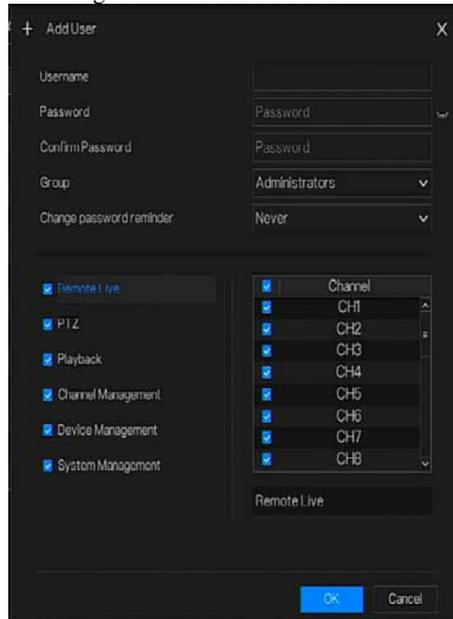


Step 2 Add or delete a user.

- Add a user

Click **Add**, the **Add User** dialog box appears, as shown in Figure 7-40.

Figure 7-40 Add user screen



Input a username, password and confirm password.

 **NOTE**

The password should include letter, character and number, at least two types.

The password should be 6~32 characters.

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 . The user is set successfully.

 **NOTE**

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

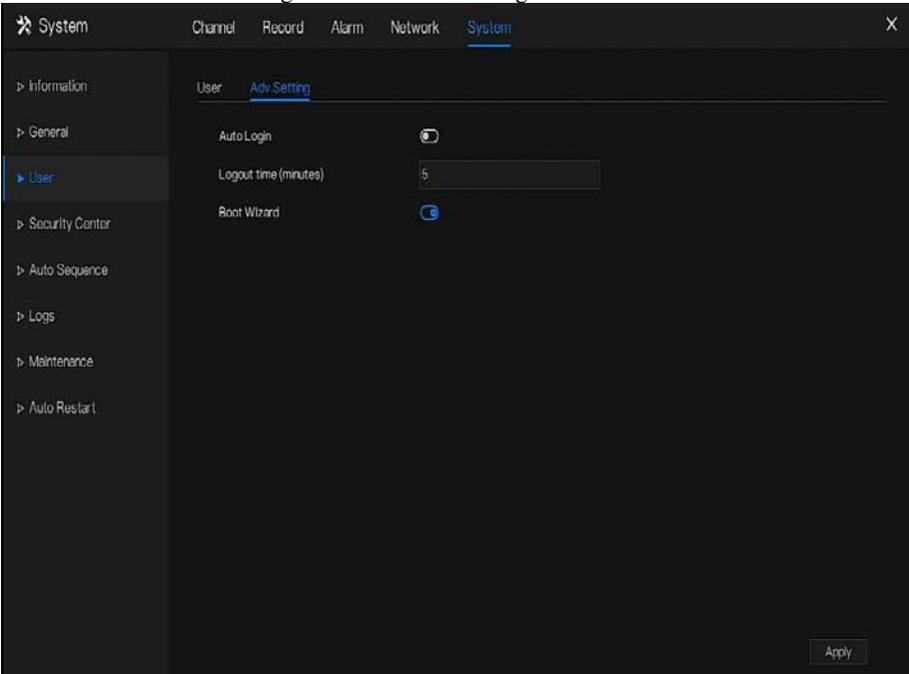
Select a user from user list and click  to edit, or click  to delete a user.

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 9-8.

Figure 7-41 Advance setting screen



Step 2 Enable or disable Auto login, Password double authentication, Boot Wizard. Set the logout time if the user disable the auto login.

Step 3 Click  to save settings.

7.7.4 Security Center

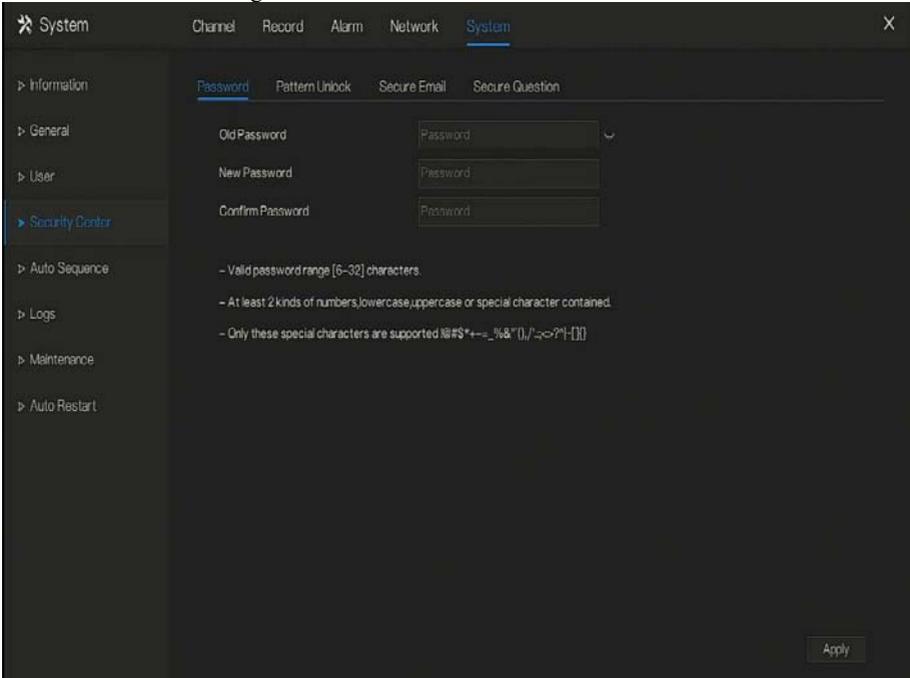
User can modify the password, pattern unlock, secure email, and secure question.

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 7-42.

Figure 7-42 Password modification screen



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

NOTE

The password should include at least two kinds of letter, character and number.

The password should be 6~32 characters.

Only special characters (!@#\$%*+~_-%&*()/_-~<?>[]{} are supported,

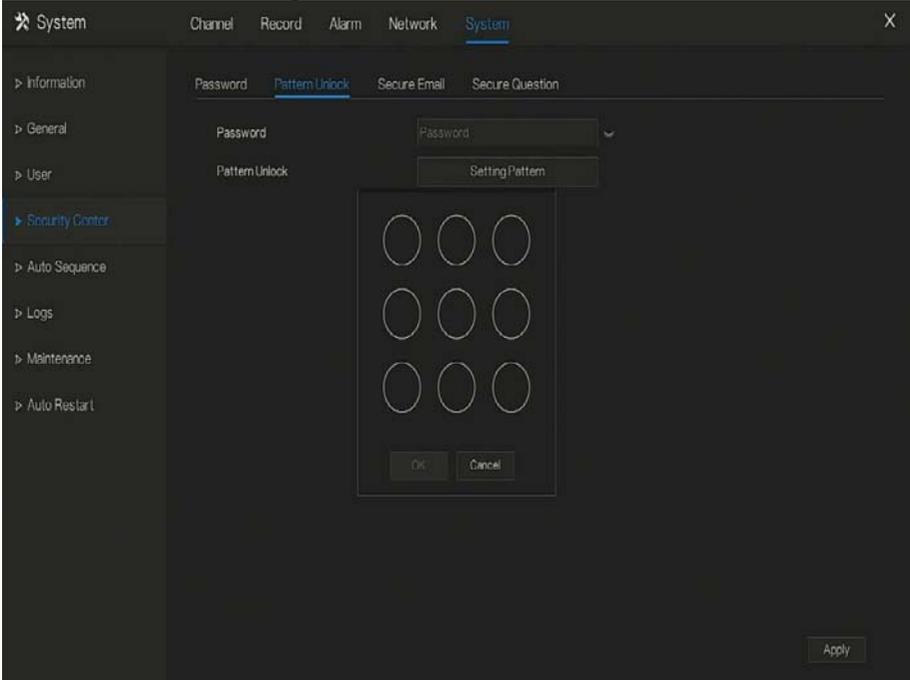
Step 3 Click  to save modified password settings.

7.7.4.2 Pattern Unlock

Operation Steps

Step 1 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 7-43.

Figure 7-43 Pattern unlock screen



Step 2 Input the password, click **Setting Pattern** to set a new pattern unlock.

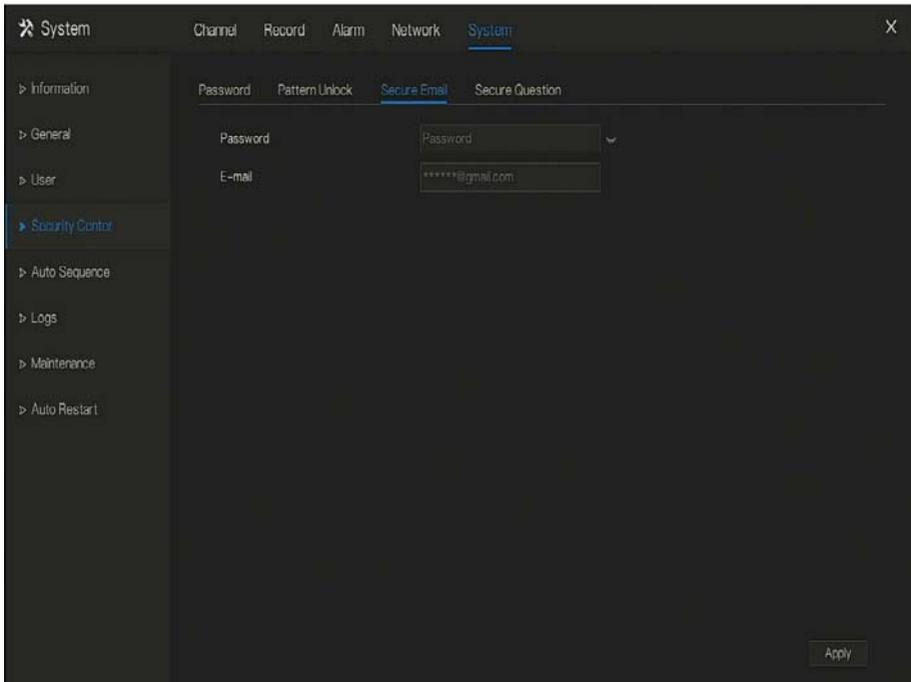
Step 3 Draw the pattern, then it will remind to draw the confirmation pattern again.

Step 4 Click **OK** to save the pattern unlock.

7.7.4.3 Secure Email

Set the email to receive the verification code to create new password, as shown in Figure 7-44.

Figure 7-44 Secure Email



Step 1 Input the password of DVR.

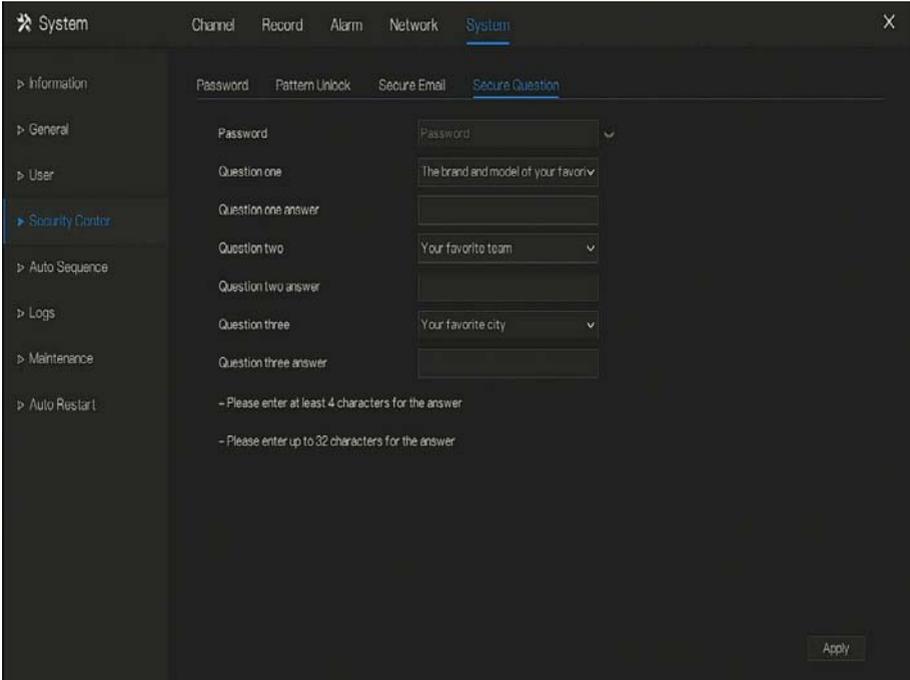
Step 2 Set the Email which will receive email of the verification code.

Step 3 Click **Apply** to save setting.

7.7.4.4 Secure Question

Set the questions to create new password, as shown in Figure 7-44.

Figure 7-45 Secure question



Step 1 Input the password of DVR.

Step 2 Choose the question from drop-down list.

Step 3 Input the answer, click  to save setting.

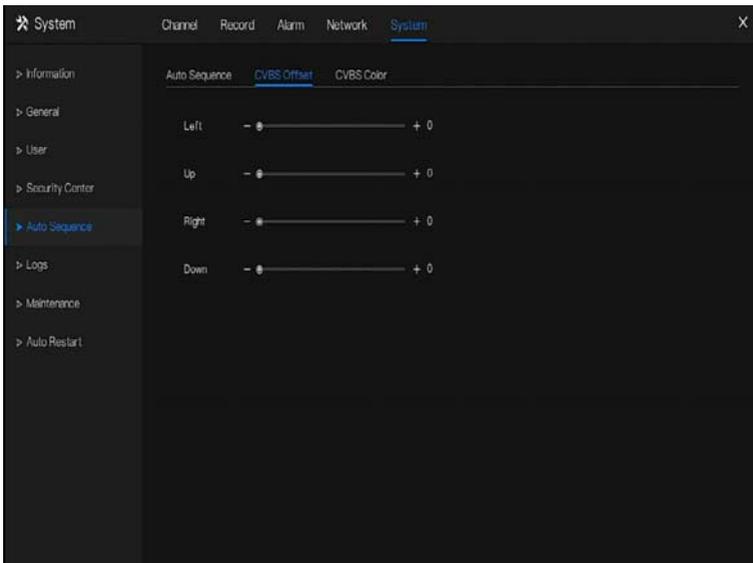
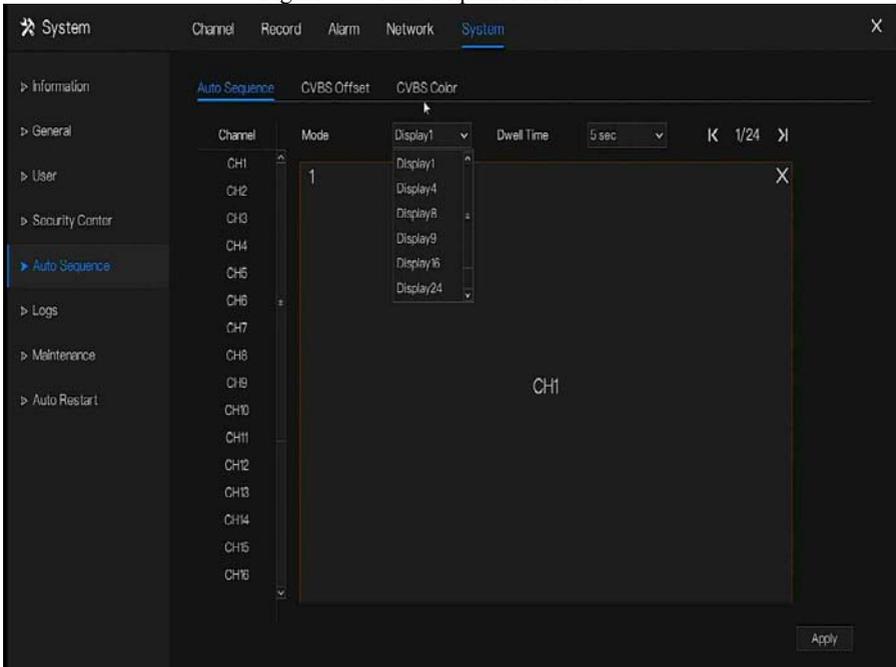
7.7.5 Auto Sequence

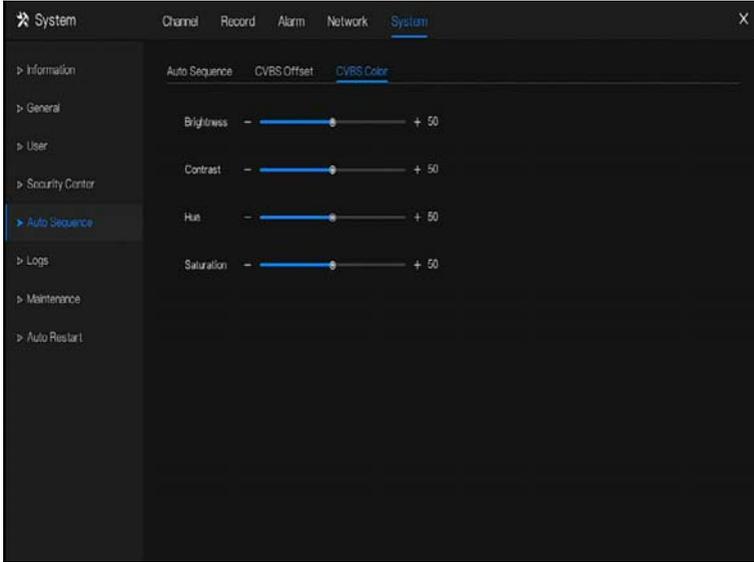
Set video mode, dwell time in display screen.

Operation Steps

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

Figure 7-46 Auto Sequence screen





Step 2 Set mode of display. Select a display mode from the **SEQ** drop-down list.

Step 3 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 If user use CVBS monitor to view live video, adjust the offset position and color

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

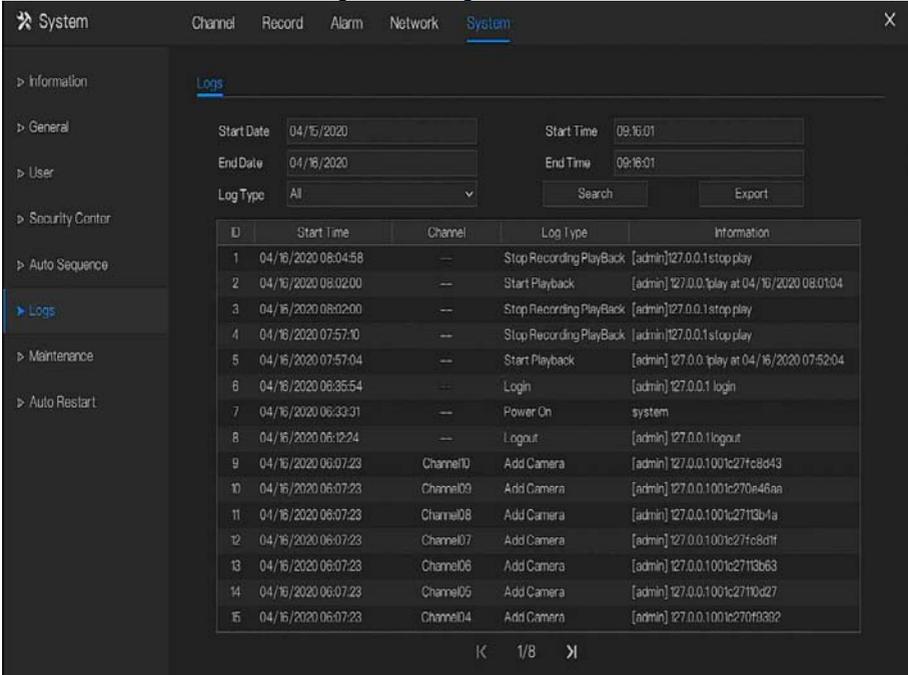
7.7.6 Logs

Search for logs information and export the information.

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 7-47.

Figure 7-47 Log screen



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.

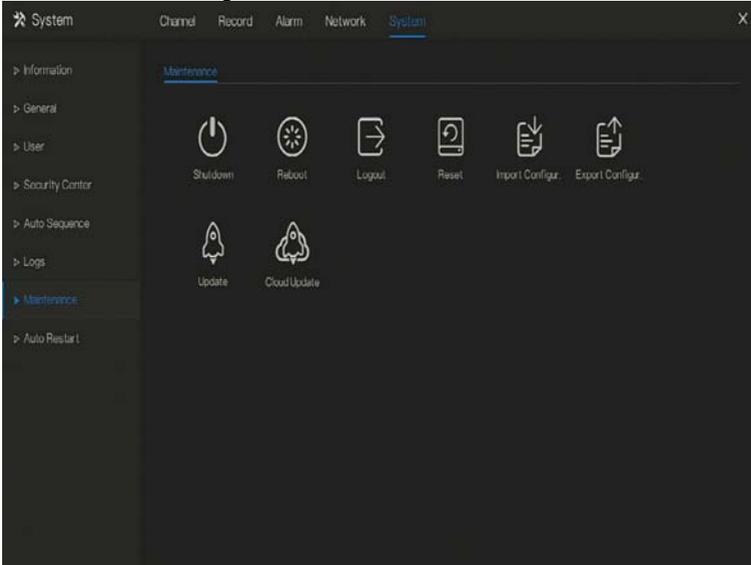
Step 5 Click **Export** to export logs to USB storage.

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 7-48.

Figure 7-48 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 “ **Are you sure to import the configuration?**” user should make 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

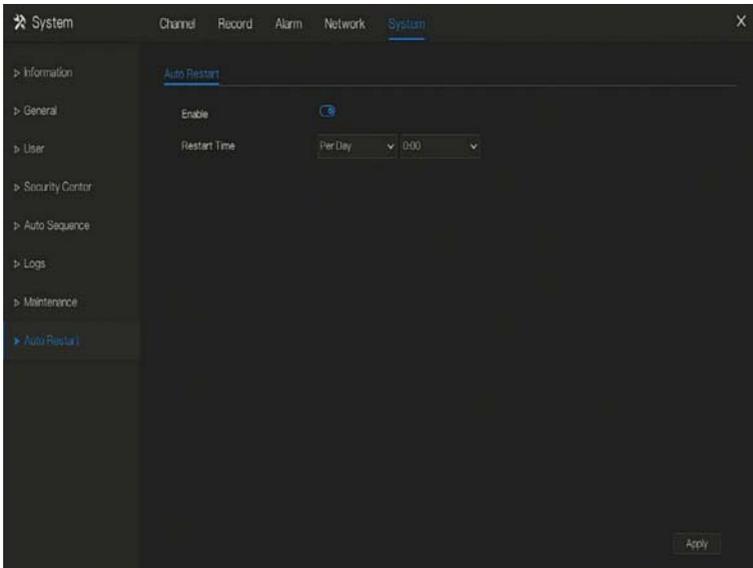
When the DVR finishes updating, the device would restart.

7.7.8 Auto Restart

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 7-48.

Figure 7-49 Auto restart screen



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

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

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

8 WEB Quick Start

8.1 Activation

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

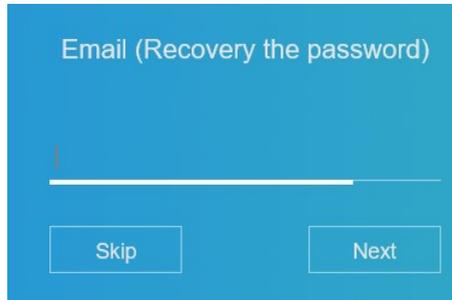


Step 1 Set the password, confirm the password.

Step 2 Input the channel password.

Step 3 Set the email of recovery the password.

Figure 8-2 Email



Step 4 Set the question of recovery the password.

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

Skip Finish

 **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.

Brover 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

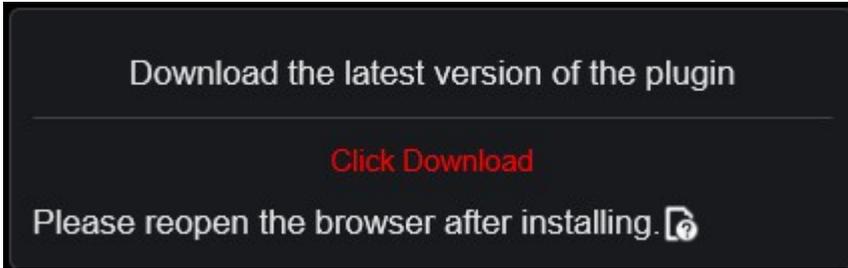
The password incorrect more than 3 times, please login again after 5 minutes.

User 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.

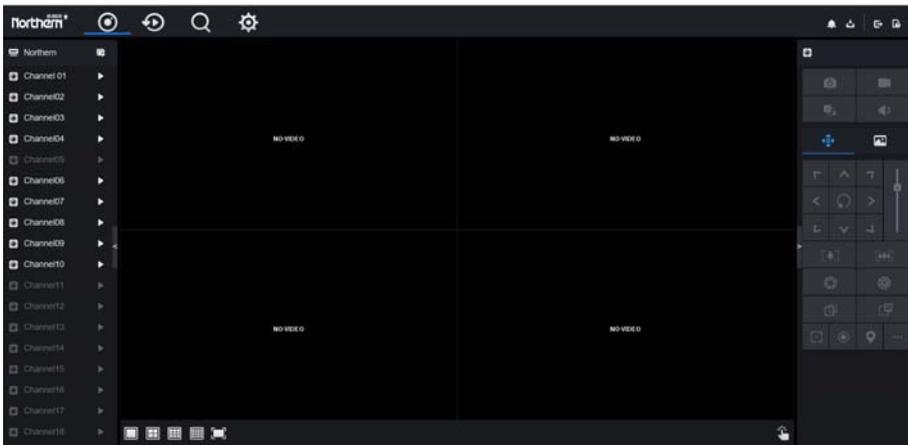
Step 3 Click **Login** to access the homepage, it would show reminder to download the latest version of the plugin, as shown in Figure 6-4.

Figure 8-5 Download the plugin



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  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 6-6 shows the overall layout of the interface. For descriptions of the interface, please refer to Table 8-1.

Figure 8-7 Homepage layout

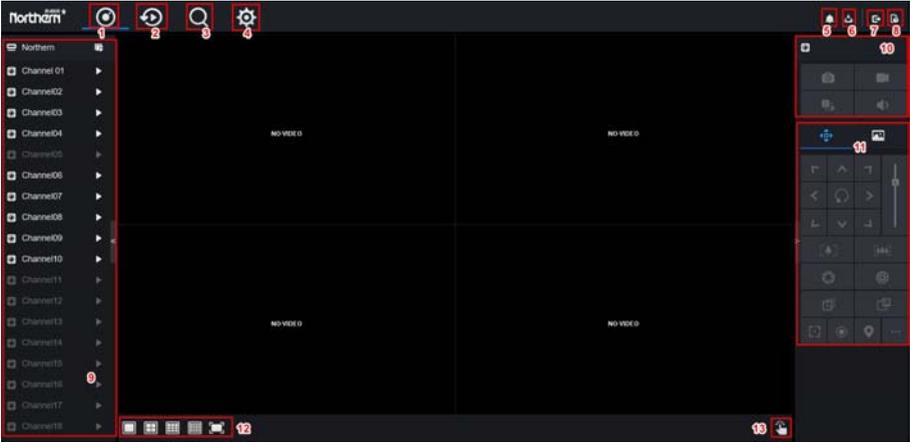


Table 8-1 Descriptions of homepage

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, record, alarm, network, system and local settings.
5	Alarm	Alarm notification. User 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	User 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	 <p>Click  to show PTZ control buttons in zone 10, you can control the PTZ equipment in the current channels. That function only used for IP dome camera.</p>
	Color parameter button	 <p>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.</p>
	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.

8.3 Browsing Videos

8.3.1 Browsing Real-Time Videos

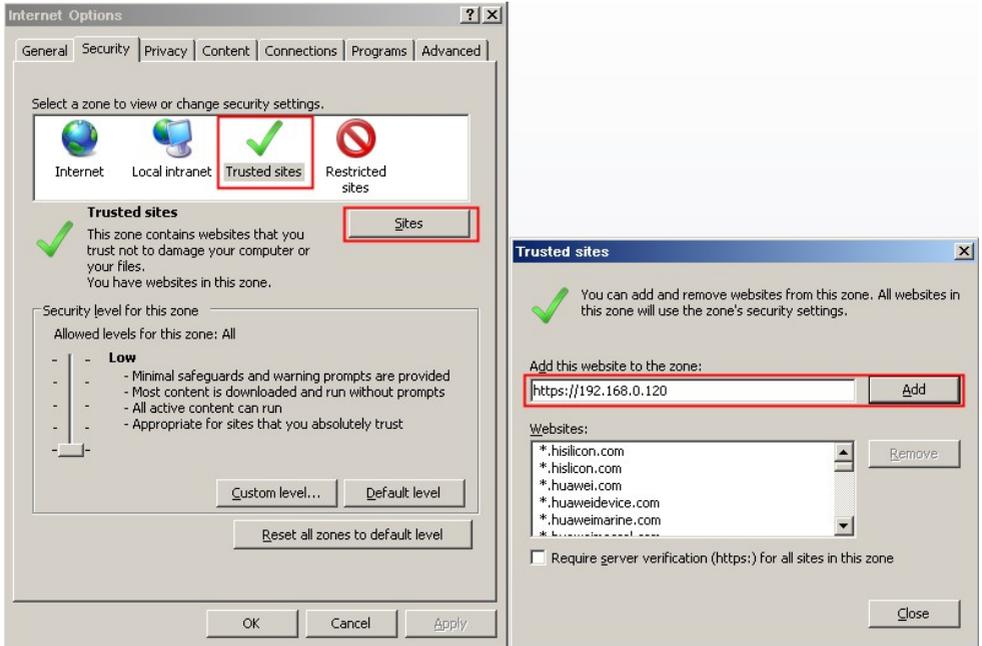
You can browse real-time videos in the web management system.

Preparation

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

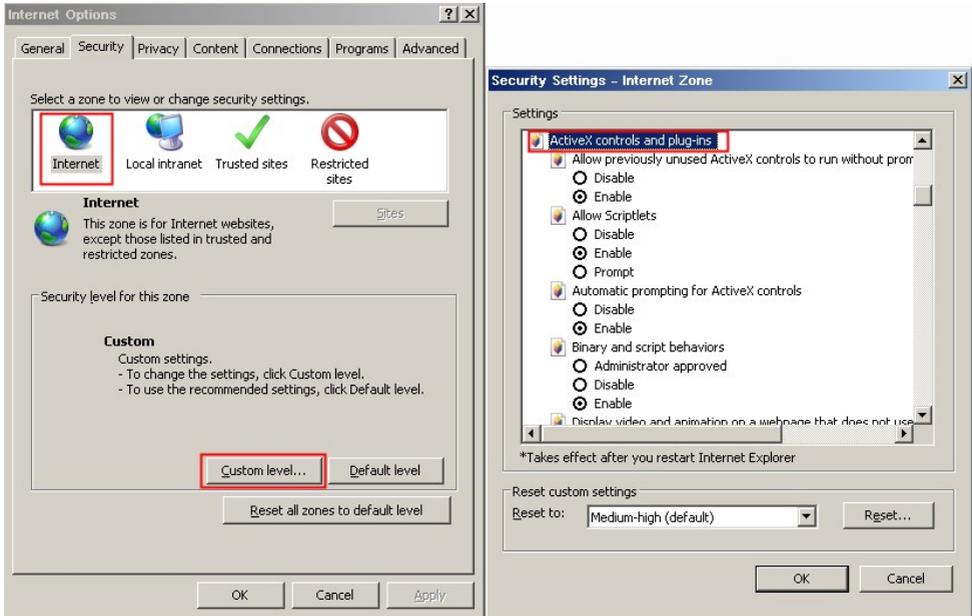
Step 1 Open Internet Explorer. Choose **Tools > Internet Options > Security > Trusted sites > Sites**. In the displayed dialog box, click **Add**, as shown in Figure 8-8.

Figure 8-8 Adding a trusted site



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



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



8.3.3 Channel Operation

Descriptions

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

Table 8-2 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.
	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 disenable the video.

8.3.4 PTZ Control and Setting

Descriptions

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

PTZ Setting

If a Network Dome or a camera connected to PTZ had been added to the DVR channel, user 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 8-3 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

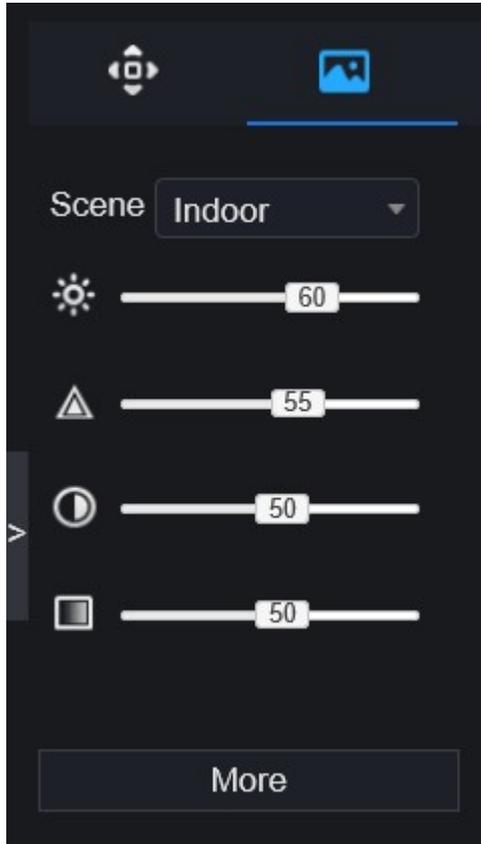


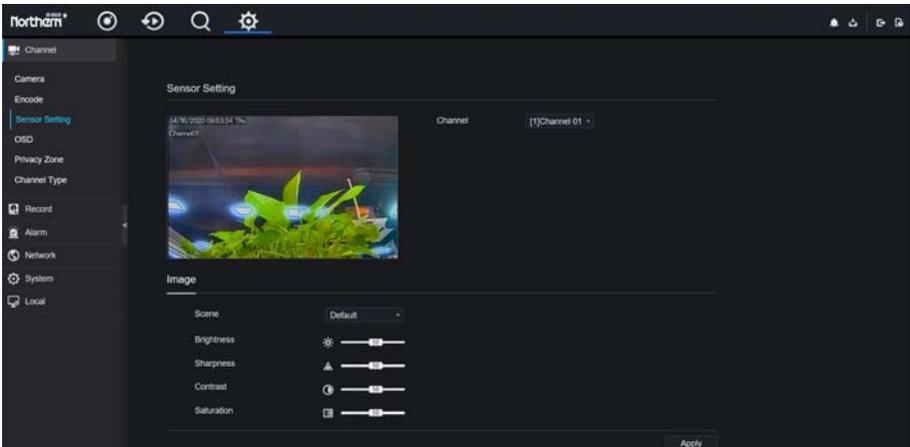
Table 8-4 Device parameters

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



8.3.6 Layout

Click  at the bottom left corner of real-time videos interface, the buttons indicate 1 screen, 4 screens and 9 screens from left to right. More POE port will be 16 screens.

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 exists, grey file axis indicates no video exists.

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 differen channels to play synchronously or asynchronously.

Sync mode indicates the selected channels play video synchronously. Async mode indicates user play different time period record

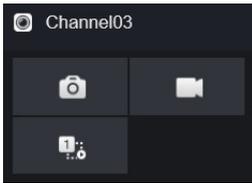
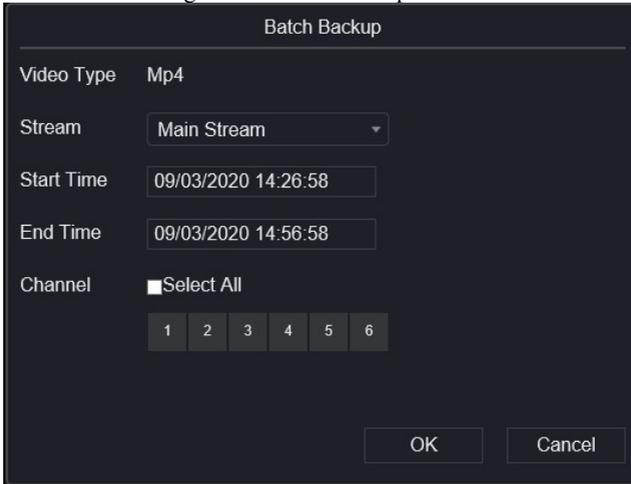


: backup, click the icon to download the recording video, click again to end the download.



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

Figure 8-16 Batch backup



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

8.5 Alarm Search

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

8.5.1 Channel Alarm

Procedure

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

Figure 8-17 Channel alarm interface

ID	Start Time	Channel	Type
1	04/16/2020 05:55:35	Channel 16	Camera Tamper
2	04/16/2020 05:54:59	Channel 16	Motion Detection
3	04/16/2020 05:52:33	Channel05	Motion Detection
4	04/16/2020 05:52:21	Channel05	Motion Detection
5	04/16/2020 05:51:57	Channel05	Motion Detection
6	04/16/2020 05:51:47	Channel05	Motion Detection
7	04/16/2020 05:51:06	Channel05	Motion Detection
8	04/16/2020 05:50:33	Channel05	Motion Detection
9	04/16/2020 05:50:22	Channel05	Motion Detection
10	04/16/2020 05:50:09	Channel05	Motion Detection
11	04/16/2020 05:49:18	Channel05	Motion Detection
12	04/16/2020 05:48:46	Channel05	Motion Detection
13	04/16/2020 05:48:36	Channel05	Motion Detection
14	04/16/2020 05:48:19	Channel05	Motion Detection
15	04/16/2020 05:47:01	Channel05	Motion Detection



Step 2 Click  at the top right corner, select the channel and type, set start time and end time, as shown in Figure 8-18.

Figure 8-18 Set channel alarm

Channel All ▾

Type All ▾

Start Time 2019/01/03 15:13:25

End Time 2019/01/04 15:13:25

Search

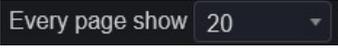
Step 3 Click **Search**, the result will be displayed as shown in Figure 8-19.

Figure 8-19 Channel alarm result



ID	Start Time	Channel	Type
1	10/03/2020 05:21:50	Channel01	Camera Tamper
2	10/03/2020 05:02:21	Channel01	Camera Tamper
3	10/03/2020 04:57:29	Channel01	Camera Tamper
4	10/03/2020 04:55:23	Channel01	Camera Tamper
5	10/03/2020 04:55:06	Channel01	Camera Tamper
6	10/03/2020 04:42:08	Channel01	Camera Tamper
7	10/03/2020 04:40:52	Channel01	Camera Tamper
8	10/03/2020 04:35:24	Channel01	Camera Tamper
9	10/03/2020 00:10:22	Channel01	Camera Tamper
10	10/03/2020 00:03:41	Channel01	Camera Tamper

 **NOTE**

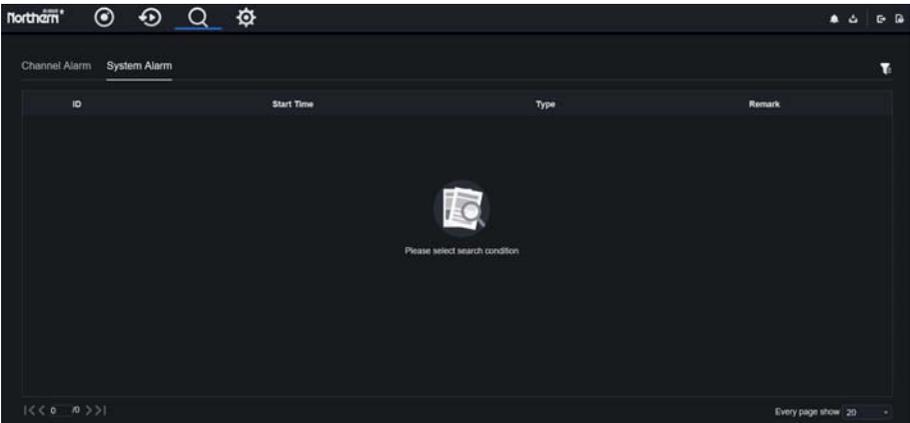
Click  to select the page of alarm list.
 shows the rows shown in every page.

8.5.2 System Alarm

Procedure

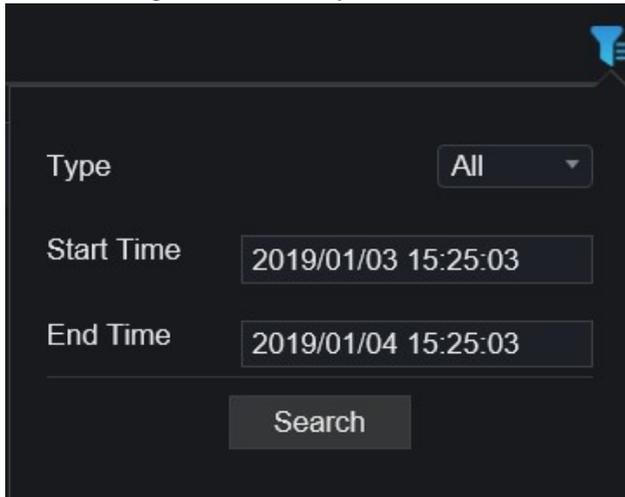
Step 1 Click **System Alarm** in the channel alarm interface, the system alarm is displayed, as shown in Figure 8-20.

Figure 8-20 System alarm result



Step 2 Click  at the top right corner, set the channel, type(alarm in and other), start time and end time, as shown in Figure 8-21.

Figure 8-21 Search system alarm



Step 3 Click **Search**, the result will be displayed.

9 System Setting

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

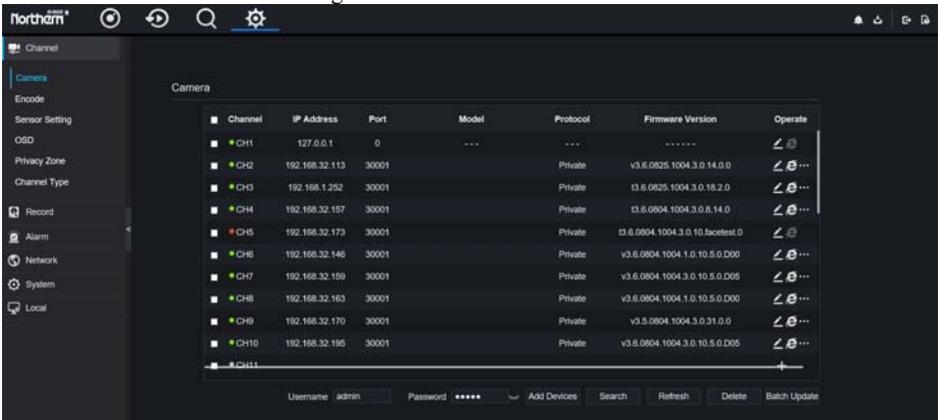
9.1 Channel

User can set parameter about camera, encode, sensor setting, OSD and privacy zone.

9.1.1 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



Step 2 Input username and password, 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 camera.

Figure 9-2 Device search

ID	IP Address	Port	Model	Protocol	Firmware Version
1	192.168.32.140	30001		Private	v3.4.0804.1003.3.0.99.3.0
2	192.168.32.113	30001		Private	v3.6.0825.1004.3.0.14.0.0
3	192.168.32.163	30001		Private	v3.6.0804.1004.1.0.10.5.0.D00
4	192.168.70.179	30001		Private	v3.5.0819.3900.172.0.31.0.109
5	192.168.1.252	30001		Private	t3.6.0825.1004.3.0.18.2.0
6	192.168.32.152	30001		Private	v3.6.0804.1004.1.0.10.5.0.D00
7	192.168.32.130	30001		Private	v3.4.0702.1003.3.0.102.0.0
8	192.168.32.104	30001		Private	v3.6.0825.1004.75.0.17.0.5
9	192.168.32.157	30001		Private	t3.6.0804.1004.3.0.8.14.0
10	192.168.32.158	30001		Private	v3.6.0804.1004.1.0.10.5.0.D00
11	192.168.32.8	30001		Private	v3.5.0804.1004.3.0.33.0.0
12	192.168.32.170	30001		Private	v3.5.0804.1004.3.0.31.0.0

Username: admin Password: ***** Add Refresh Back

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

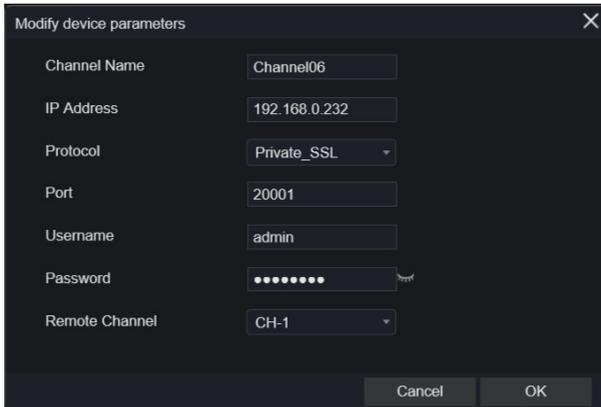
Step 5 Click **Refresh** to refresh cameras status.

Step 6 Choose the cameras and click **Delete** to delete.

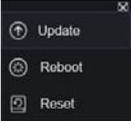
Step 7 Click **Batch Update** to update all selected cameras at once, the pop-up window would show to select software.

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

Figure 9-3 Modify device parameters



Step 9 Click  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, user can view the live video immediately.

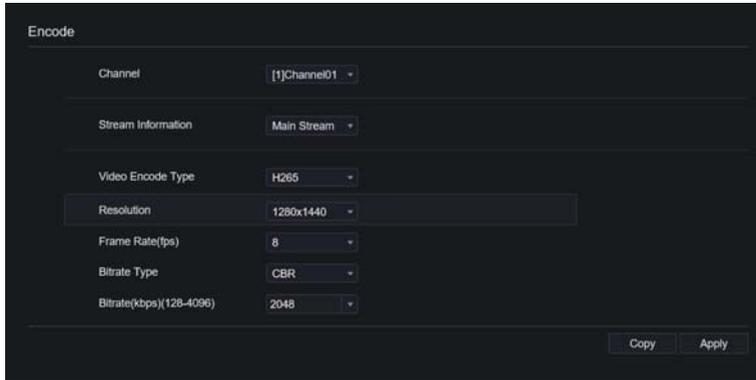


: it indicates the camera is offline, it maybe not connect the network, or the password is incorrect. User access to the modify device parameters interface to change.

9.1.2 Encode

Step 1 On the **System Setting** screen, choose **Channel > Encode** to access the encode interface, as shown in Figure 9-4.

Figure 9-4 Encode interface



Step 2 Select a channel from drop-down list.

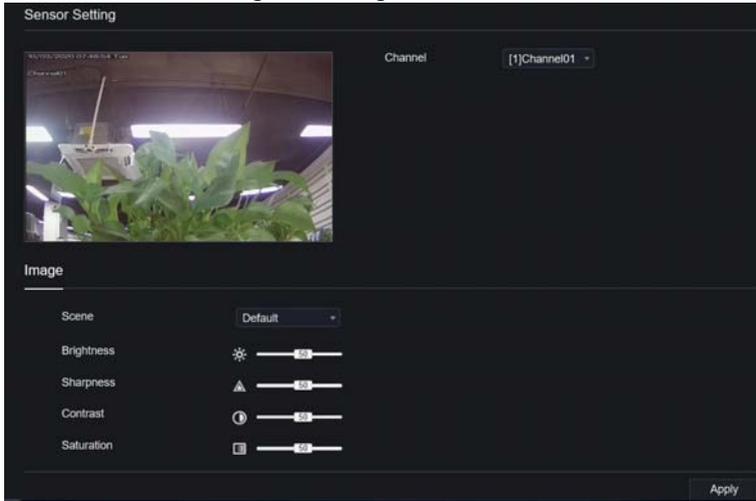
Step 3 Select stream information, encode type, resolution, frame rate, bitrate control and bitrate from drop-down list.

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

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 9-5.

Figure 9-5 Image interface



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 camera's sensor setting, user can refer IP cameras' settings.

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

 **NOTE**

Brightness: It indicates the total brightness of an image. As the value increases, the image becomes brighter.

Sharpness: It indicates the border sharpness of an image. As the value increases, the borders become clearer, and the number of noise points increases.

Saturation: It indicates the color saturation of an image. As the value increases, the image becomes more colorful.

Contrast : It indicates the measurement of different brightness levels between the brightest white and darkest black in an image. The larger the difference range is, the greater the contrast; 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: user can transit day to night, or switch mode.

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

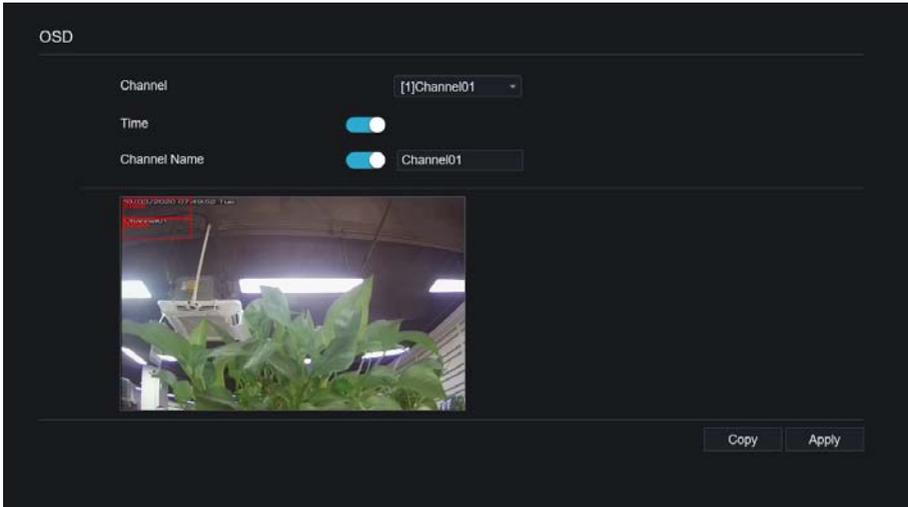
Enhance image: it includes WDR, HLC, BLC, defog and anti-shake.

Zoom focus: user can zoom and focus.

9.1.4 OSD

Step 1 On the **System Setting** screen, choose **Channel >OSD** to access the OSD interface, as shown in Figure 5-4

Figure 9-6 OSD interface



Step 2 Select a channel and scene from drop list.

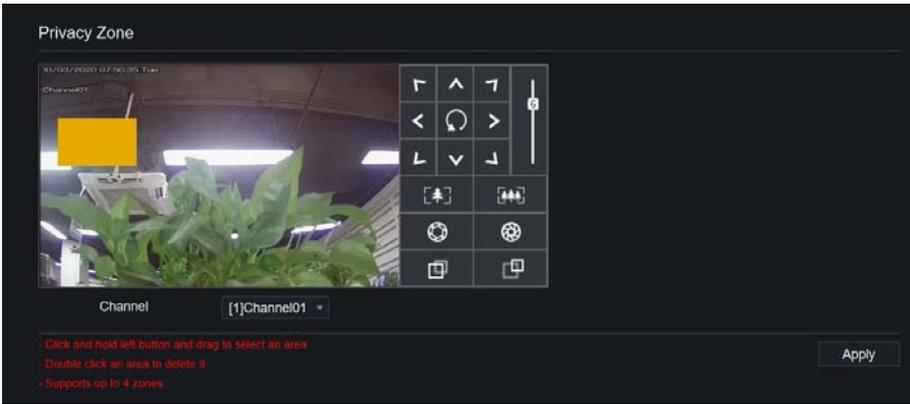
Step 3 Enable time and channel name. You can set channel name. Drag the icon of Channel Name or Date and Time to move, select the location.

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

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 9-7.

Figure 9-7 Privacy interface



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 would delete the area.

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

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

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 9-8.

Figure 9-8 Record schedule interface



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 drag the mouse cursor to choose.

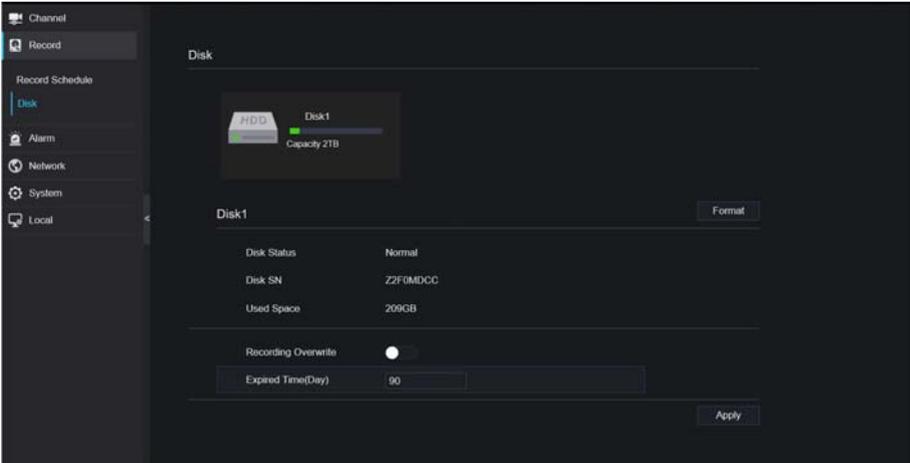
Step 5 Click  to return the previous settings.

Step 6 Click  to choose other camera to copy settings. Click  to save the settings.

9.2.2 Disk

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

Figure 9-9 Disk interface



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.

9.2.3 S.M.A.R.T

S.M.A.R.T is Self-Monitoring Analysis and Reporting Technology, user can view the health of disk, as shown in 7.3.

Figure 9-10 S.M.A.R.T

S.M.A.R.T

Disk: Disk1

Disk SN: W5257MN2 Disk Model: ST2000VX008-2E3164

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	0x506d92060000
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-rtly-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

9.3 Alarm

User can set general, motion detection, video loss, intelligent analysis and alarm in on alarm interface.

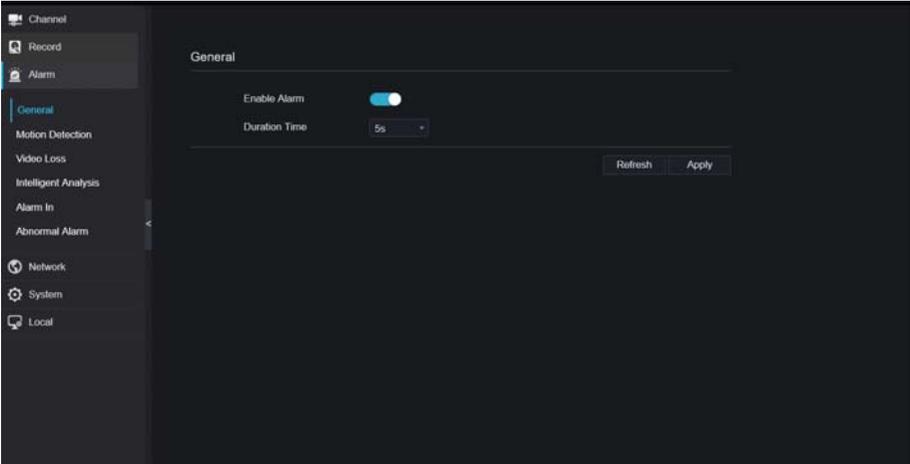
9.3.1 General

Procedure

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

Step 2 Enable alarm to set duration time, as shown in Figure 9-11.

Figure 9-11 General interface



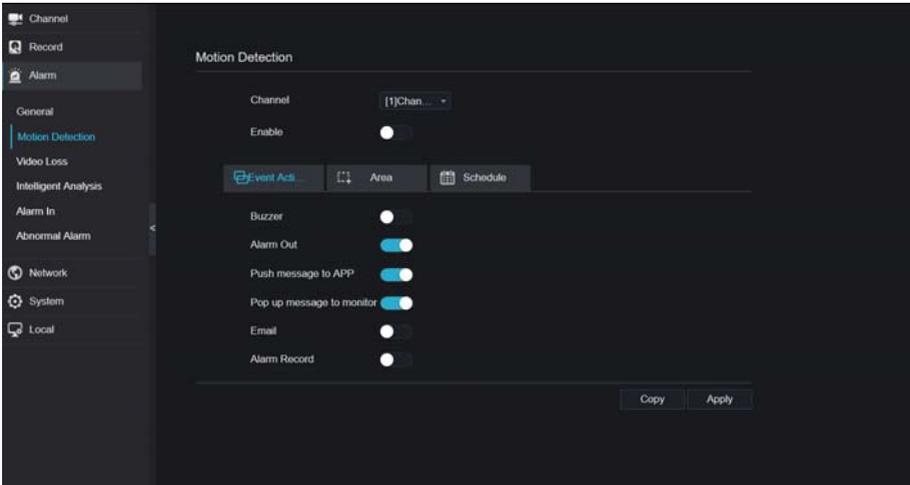
Step 3 Click **Apply** to save settings. Click **Refresh** to return to the previous settings.

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 9-12.

Figure 9-12 Motion detection interface



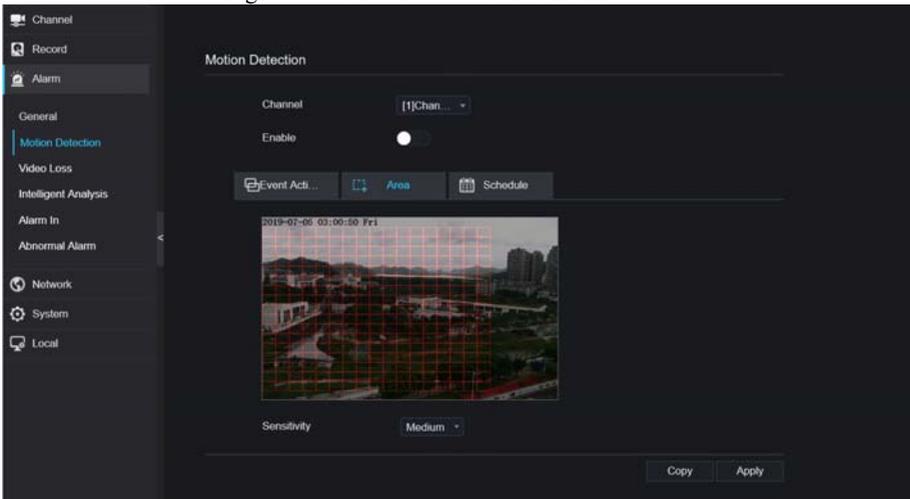
Step 2 Click channel drop-down list to choose channel.

Step 3 Enable motion detection alarm.

Step 4 Set **Event Activity**, includes buzzer, alarm out, push message, pop-up message, send E-mail and alarm record.

Step 5 Click **Area** to access the motion detection area setting, as shown in Figure 9-13.

Figure 9-13 Motion detection area interface



1. Hold down and drag the left mouse button to draw a motion detection area.

2. Select a value from the drop-down list next to **Sensitivity**.

3. Double -click the chosen area to delete.

Step 6 Click **Schedule** to access schedule settings, 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.

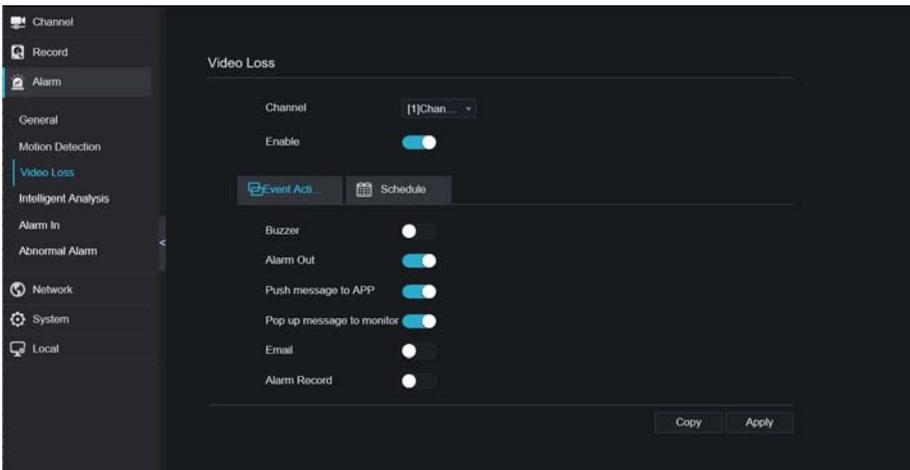
Step 7 Click **Copy** to choose other camera to copy settings. Click **Apply** to save the settings.

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 9-15.

Figure 9-14 Camera tamper interface



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* .

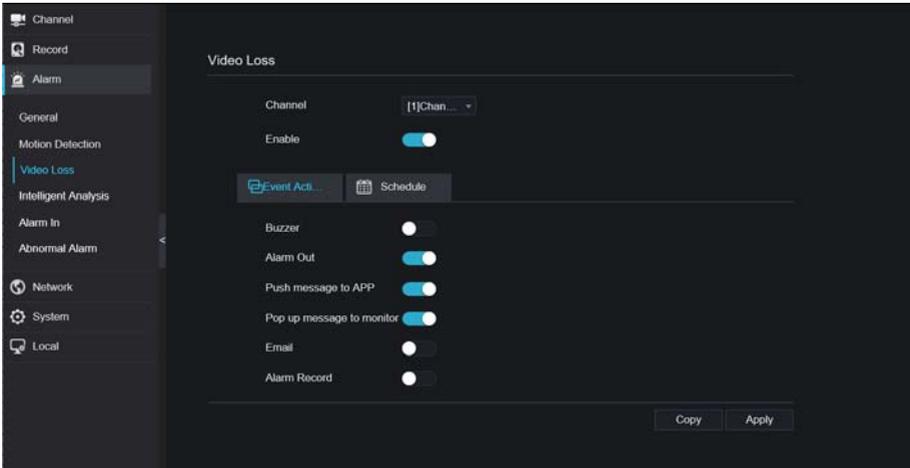
Step 5 Click **Copy** to choose other camera to copy settings. Click **Apply** to save the settings.

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 9-15.

Figure 9-15 Video loss interface



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* .

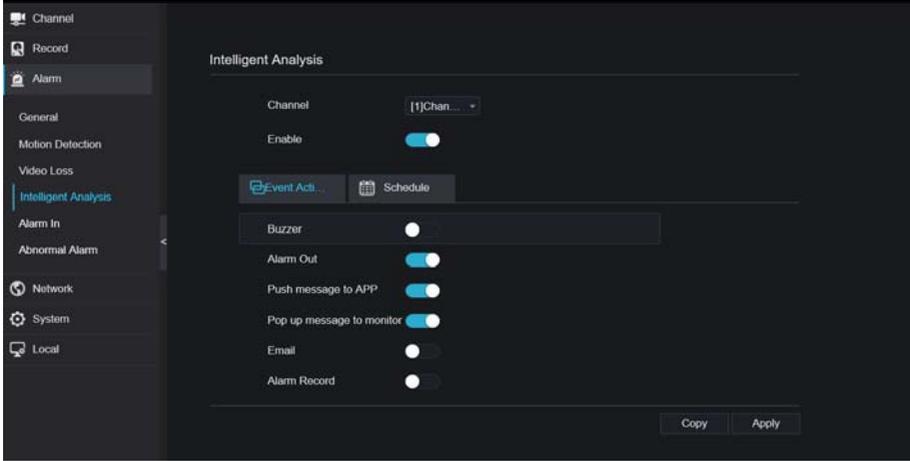
Step 5 Click **Copy** to choose other camera to copy settings. Click **Apply** to save the settings.

9.3.5 Intelligent Analysis

Procedure

Please refer to chapter 7.6.1 *video loss settings*, interface displayed as shown in Figure 9-16.

Figure 9-16 Intelligent analysis interface

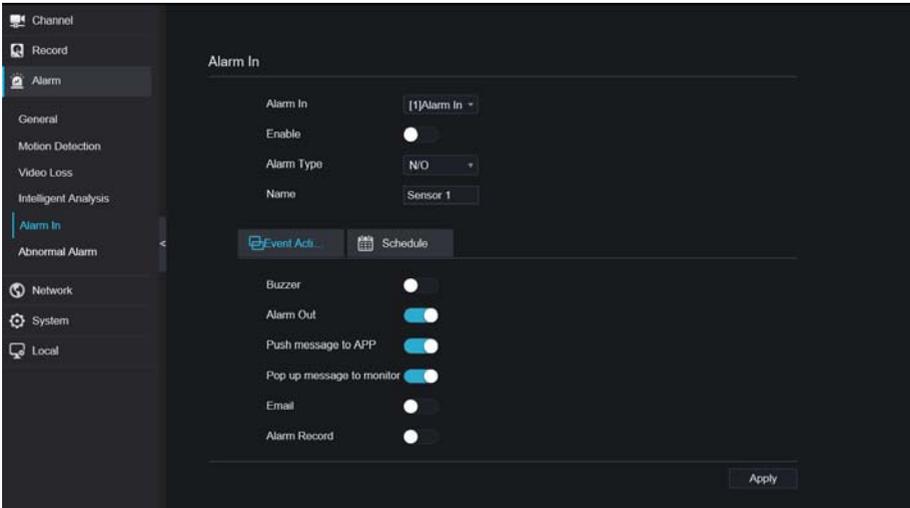


9.3.6 Alarm In

Procedure

Step 1 On the **System Setting** screen, choose **Alarm** > **Alarm In** to access the alarm in interface, as shown in Figure 9-17.

Figure 9-17 Alarm in interface



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

Step 3 Enable the button, choose alarm type.

Step 4 Set name, default is Sensor 1.

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

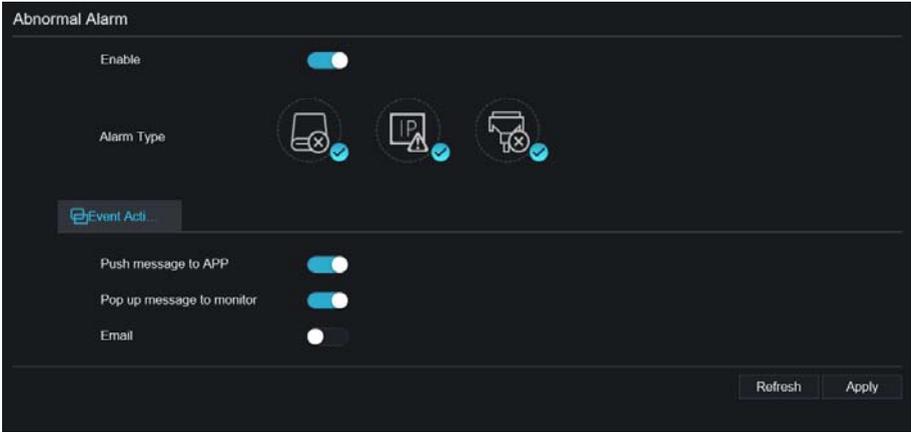
Step 6 Click  to save settings.

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 6-11.

Figure 9-18 Abnormal alarm interface



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

Step 3 Enable the button, tick alarm type.

Step 4 Set name, default is Sensor 1.

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

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

9.4 Network

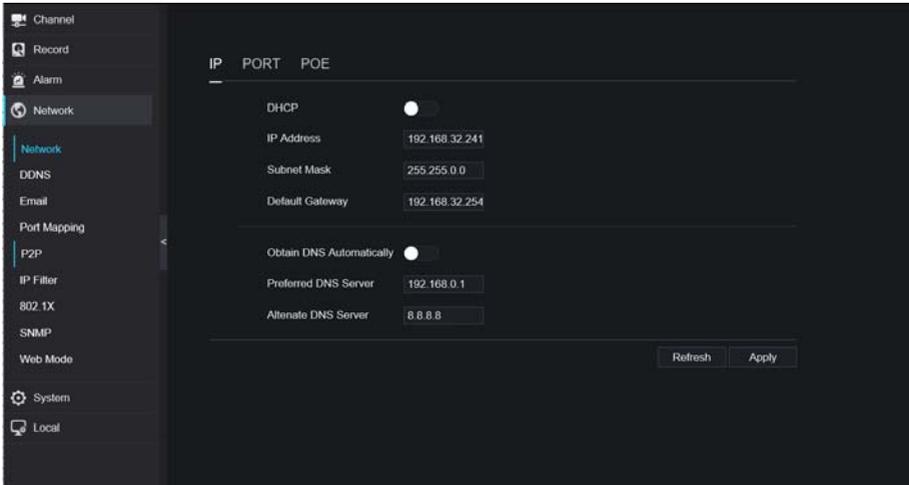
Users can set Network, DDNS, E-mail, UPnP, P2P, IP Filter, 802.1X, SNMP and Web Mode.

9.4.1 Network

Procedure

Step 1 On the **System Setting** screen, choose **Network > Network** to access the network interface, as shown in Figure 9-19.

Figure 9-19 Network interface



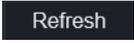
Step 2 Click  next to **IP** to enable or disable the function of automatically getting an IP address. The function is enabled by default.

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** and **POE** manually, input the information about these.

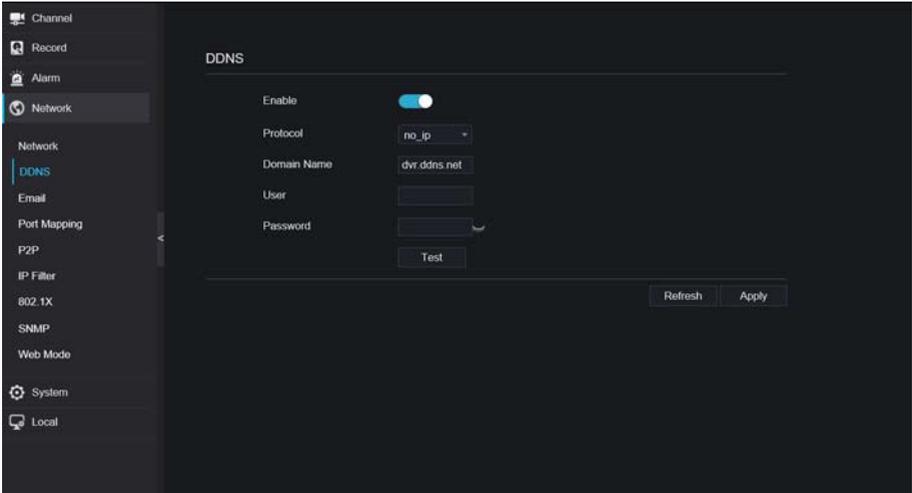
Step 5 Click  to restore previous settings. Click  to save the settings.

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 9-20.

Figure 9-20 DDNS interface



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

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

Step 4 Set domain name, user, and password.

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



NOTE

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

9.4.3 E-mail

Procedure

Step 1 Click **E-mail** in the network interface, choose **Network > E-mail** to access the E-mail interface, as shown in Figure 9-21

Figure 9-21 E-mail interface

The screenshot shows the 'Email' configuration page. The left sidebar has 'Network' selected, with 'E-mail' highlighted. The main content area has the title 'Email' and the following settings:

- SMTP Server: [Text Input]
- SMTP Server Port: 25 [Text Input]
- Username: [Text Input]
- Password: [Password Input]
- Email Sender: [Text Input]
- Email for password reco...: [Text Input]
- Alarm Receiver 1: [Text Input]
- Alarm Receiver 2: [Text Input]
- Alarm Receiver 3: [Text Input]
- SSL Encryption: OFF [Dropdown]

Buttons: Test, Refresh, Apply

Step 2 Set SMTP server and SMTP server port manually.

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

Step 4 Set E-mail for receive alarm the message.

Step 5 Set E-mail for retrieve the password the message.

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

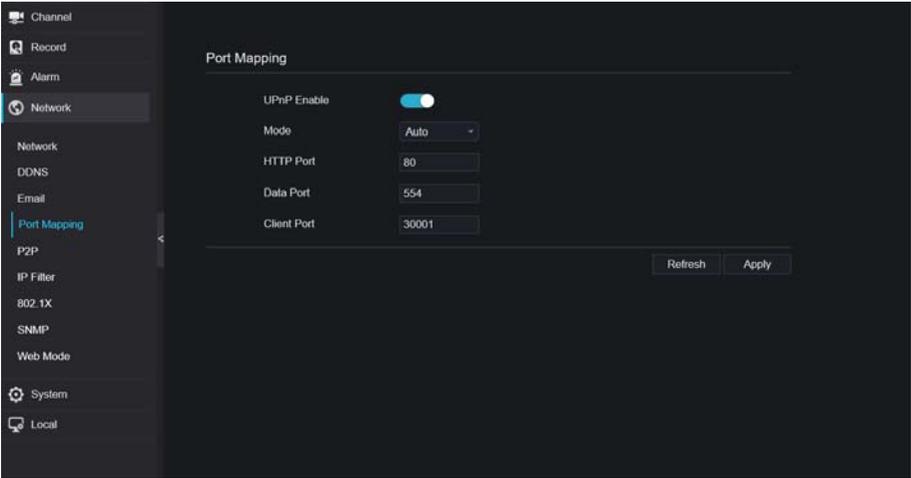
Step 7 Click **Refresh** to restore previous settings. Click **Apply** to save the settings.

9.4.4 Port Mapping

Procedure

Step 1 Click **Port Mapping** in the network interface, choose **Network > Port Mapping** to access the UPnP interface as shown in Figure 9-22.

Figure 9-22 Port Mapping interface



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

Step 3 After **UPnP** is manual, set the Web port, data port and client port manually.

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

 **NOTE**

Auto :system perform UPnP automatically.

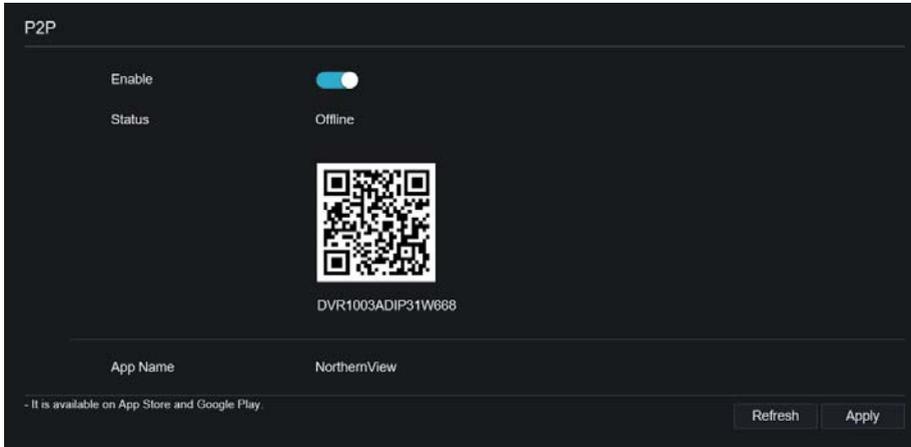
Manual : the ports distribute by router, you need to refer router then input them.

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 9-23.

Figure 9-23 P2P interface



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

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

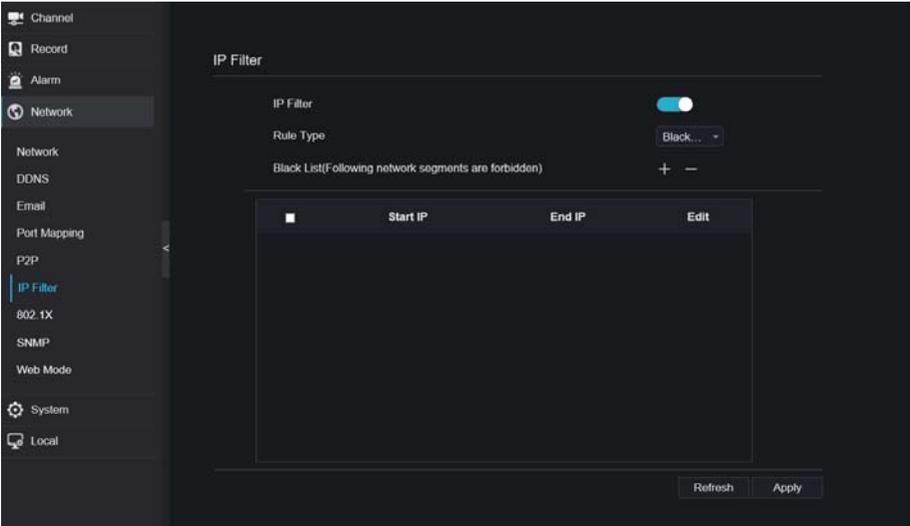
Step 4 After the NorthernView is installed in mobile phone, run the APP and scan the UUID QR code to add then access the DVR when the device is online.

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 9-24.

Figure 9-24 IP filter interface



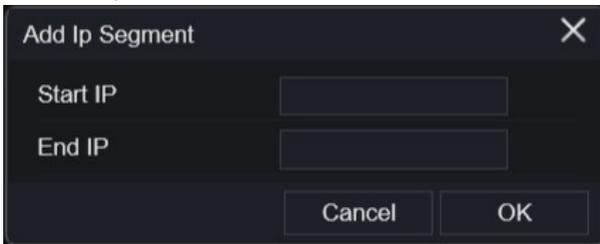
Step 2 Click **Enable** to enable the IP filter function.

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 9-25 Black or white list interface



Step 5 Set start IP and end IP.

Step 6 Click  to deny settings, click  to save the settings.

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

 **NOTE**

Black list: IP address in specified network segment to prohibit access.

White list: IP address in specified network segment to allow access.

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

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

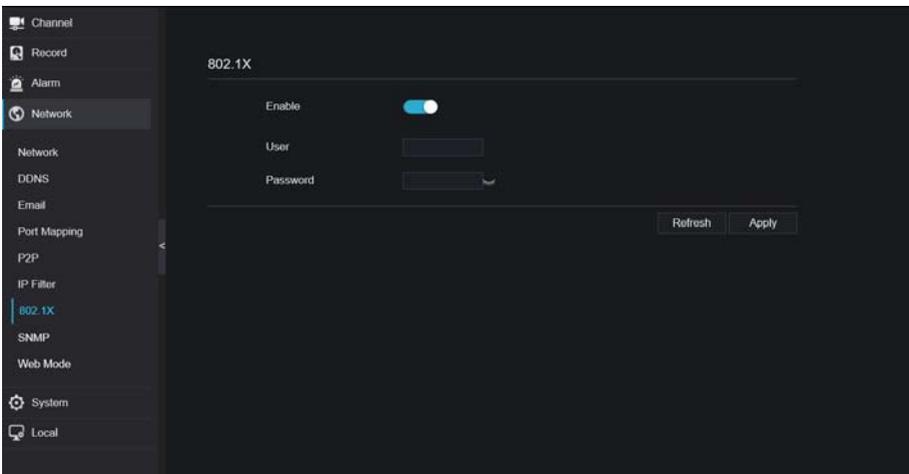
Only one rule type is available, and the last rule type set is efficient.

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 9-26.

Figure 9-26 802.1X interface



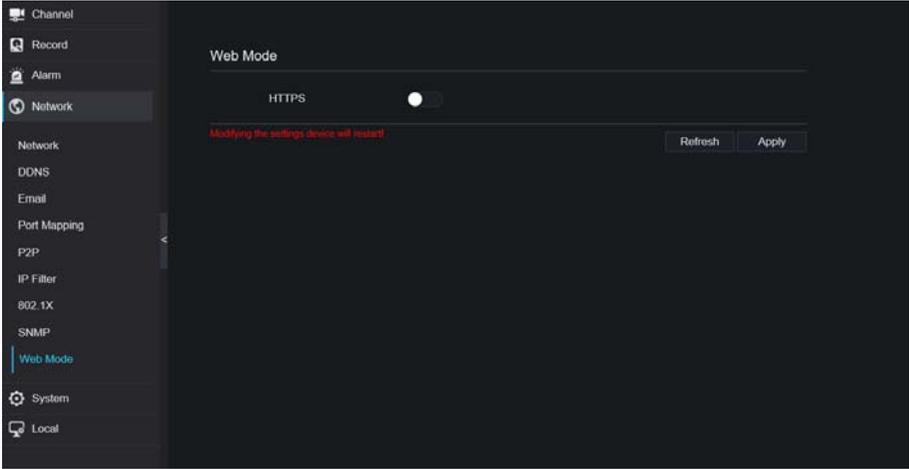
Step 2 Input the user and password of 802.1X authentication.

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

9.4.8 Web Mode

Step 1 Click **Web Mode** in the network interface, Web mode interface is displayed, as shown in Figure 5-1.

Figure 9-27 Web mode interface



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

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

9.5 System

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

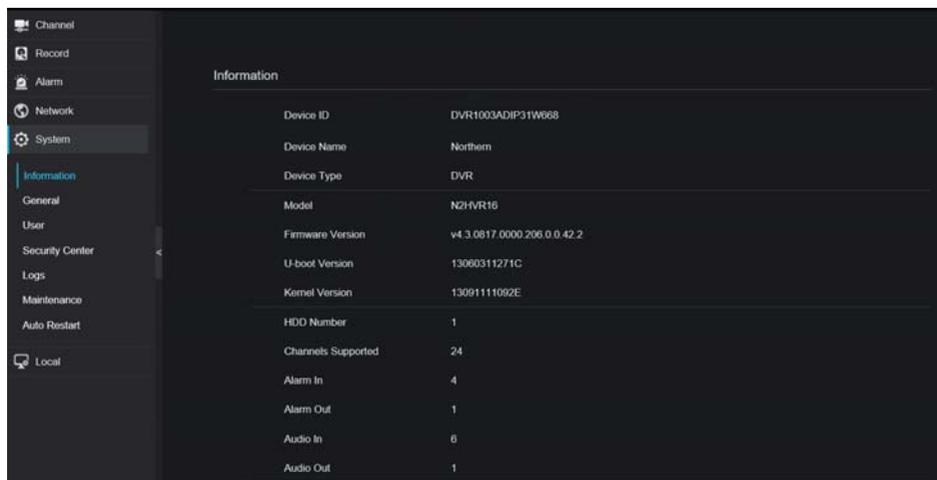
9.5.1 Device Information

Procedure



Step 1 Click **System** on the navigation bar, the device information interface is displayed, as shown in Figure 9-28.

Figure 9-28 Device information interface



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

Table 9-1 Device parameters

Parameter	Description	Setting
Device ID	Unique device identifier used by the platform to distinguish the devices.	[Setting method] The parameter cannot be modified.
Device Name	Name of the device.	[Setting method] System Setting > General Modify the device name.
Device Type	N/A	[Setting method]
Model		These parameters cannot be modified.
Firmware version		
HDD volume		
Channel support		
Alarm in		
Alarm out		
Audio in		

Parameter	Description	Setting
Audio out		

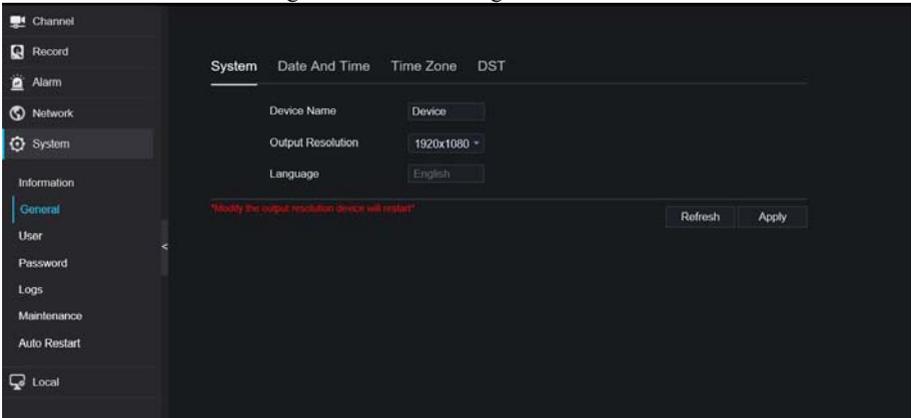
9.5.2 General

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

Procedure

Step 1 On the **System Setting** screen, choose **System >General** to access the general interface, as shown in Figure 9-29.

Figure 9-29 Basic setting interface



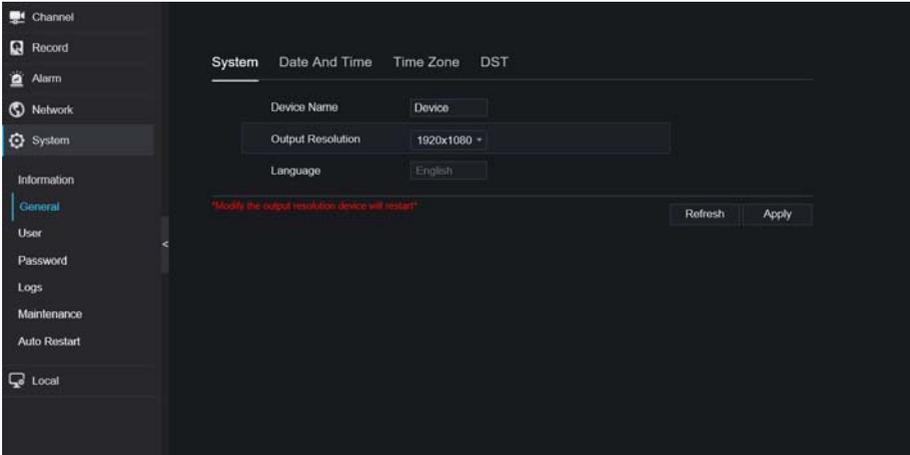
Step 2 Set system.

1. Input the device name.
2. Choose output resolution from drop list.
3. Click  to save the system setting.

Step 3 Set date and time.

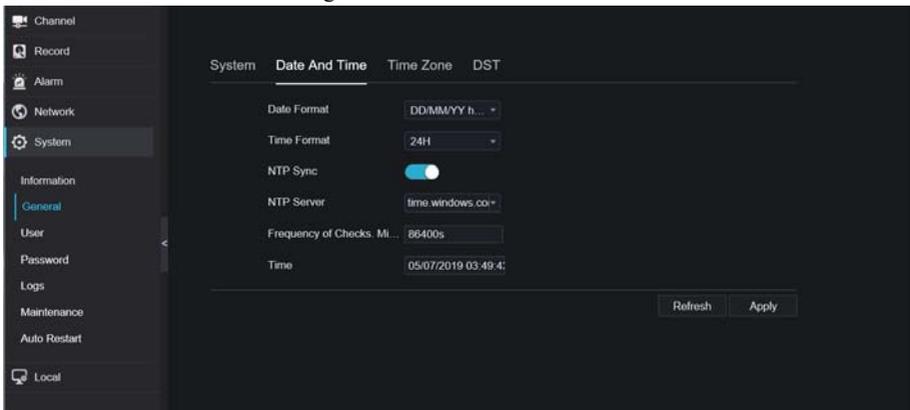
1. Synchronize the time from the NTP server, as shown in Figure 5-8.
2. Click NTP Sync button to enable synchronize time. The default value is enabling.

Figure 9-30 System interface



3. Select NTP server, date format and time format from drop list.
4. Click **Apply** to save date and time setting. The device time will synchronize with NTP server time.
5. Set the device time manually, as shown in Figure 9-31.
6. Click NTP Sync button to disable synchronize time.

Figure 9-31 Date and time



Step 4 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.

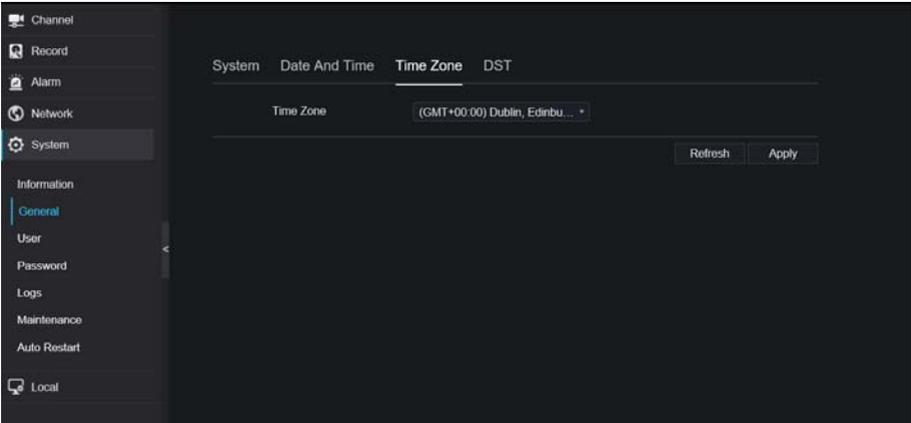
Step 5 Set time zone.

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

32.

Time zone setting interface

Figure 9-32 Time zone



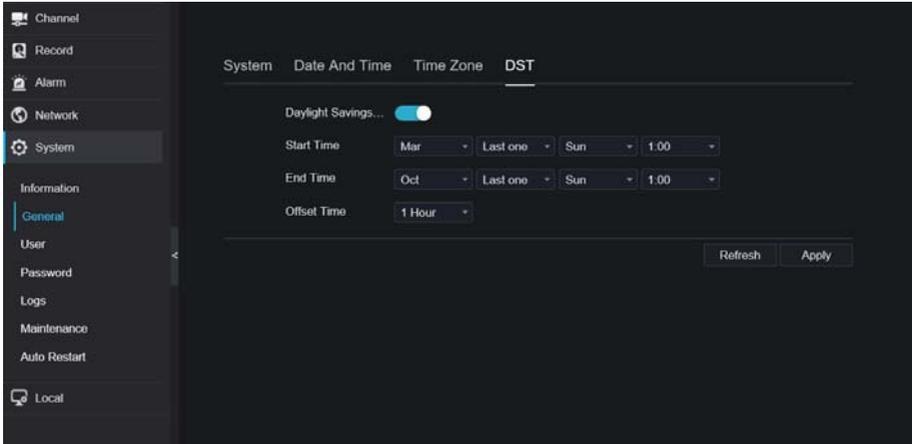
Select a time zone from the drop-down list.

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

Step 6 Set DST.

1. Click **DST** to enter the DST setting interface, click **DST** button to enable, as shown in Figure 9-33. The button is disable by default.

Figure 9-33 DST setting interface



- Select a start time from the drop-down list.
- Select an end time from the drop-down list.
- Select an offset time from the drop-down list.

Click **Apply** to save the DST setting. Click **Refresh** to return to previous setting.

9.5.3 User

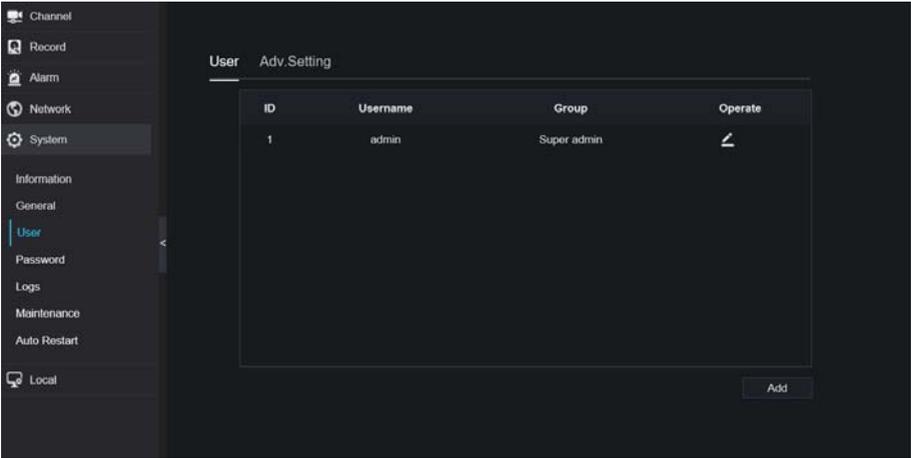
You can create new user accounts to manage the device.

9.5.3.1 Add User

Procedure

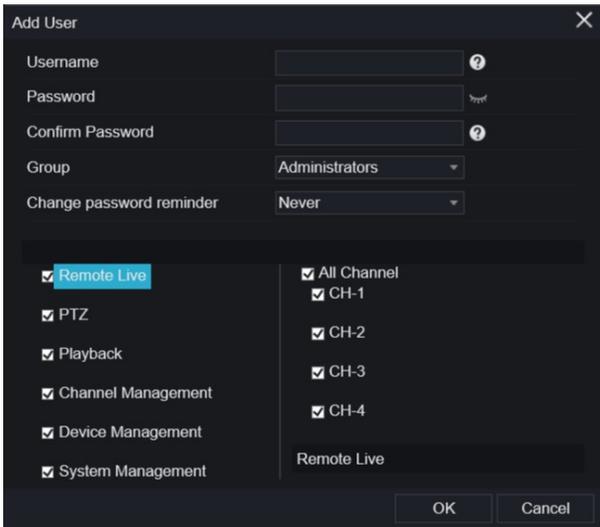
Step 1 On the **System Setting** screen, choose **System > User** to access the **User** interface, as shown in Figure 9-34.

Figure 9-34 User interface



Step 2 Click **Add** to add a new user, as shown in Figure 9-35.

Figure 9-35 Add user

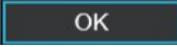


Step 3 Input username, password and confirm password.

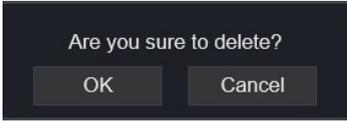
Step 4 Select group and change password reminder from drop-down list.

Step 5 Assign the privilege to user.

Step 6 Select channels to manage.

Step 7 Click , the message “**Add success**” is showed. If the password is not meet the rule, it would show .

Step 8 Click  to edit user’s information.

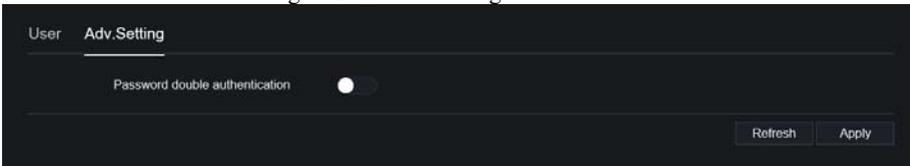
Step 9 Click  to delete the account, it would show , click  to delete.

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 9-36.

Figure 9-36 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.

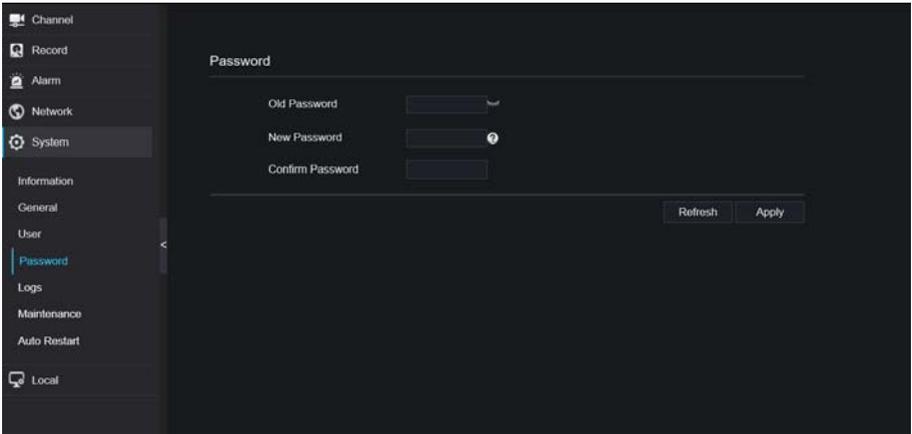
Step 3 Click  to save the device time setting. Click  to return to previous setting.

9.5.4 Password

Procedure

Step 1 On the **System Setting** screen, choose **System >Password** to access password interface, as shown in Figure 9-37.

Figure 9-37 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.

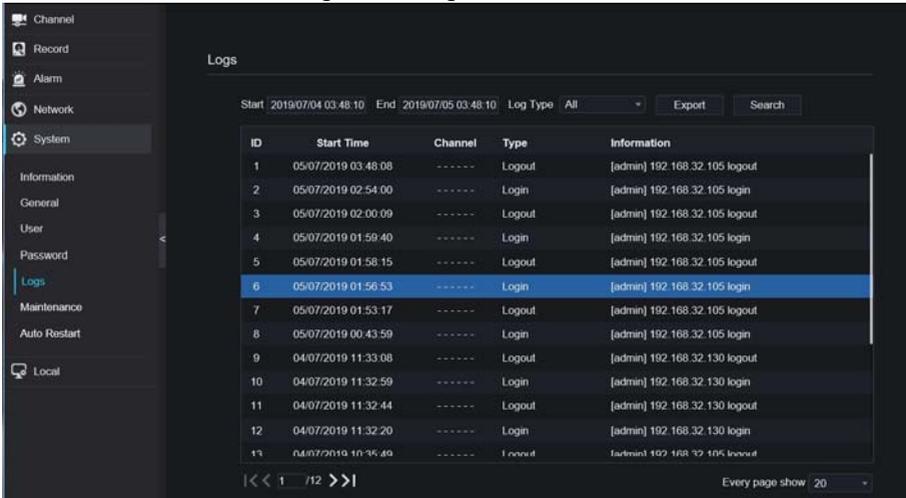
Only special characters are supported: (! @, #, \$, *, +, =, -).

9.5.5 Logs

Procedure

Step 1 On the **System Setting** screen, choose **System > Logs** to access logs interface, as shown in Figure 9-38.

Figure 9-38 Logs interface



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.

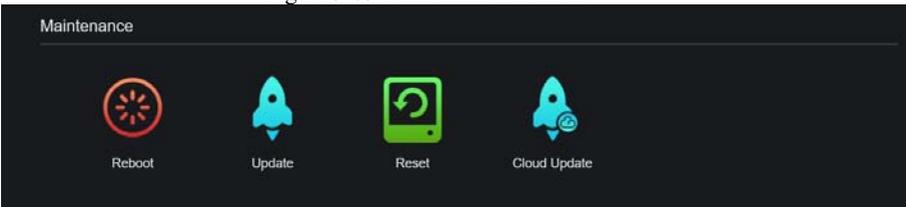
Step 5 Click **Export** to export the logs.

9.5.6 Maintenance

Procedure

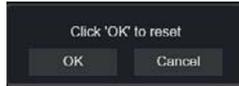
Step 1 On the **System Setting** screen, choose **System >Maintenance** to access maintenance interface, as shown in Figure 9-39.

Figure 9-39 Maintenance interface



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

Step 3 Click **Update**, the message shows **Please select upgrade file**, choose software from specific location to update.



Step 4 Click **Reset**, the pop-up message shows to you, click



to reset.

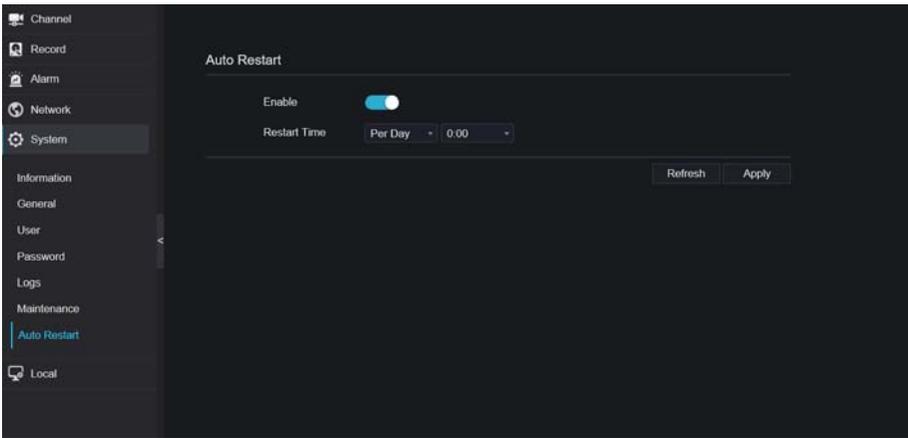
Step 5 If the device is online, and the cloud server has the software, click the **Cloud Update**, it shows ‘make sure to update’, click **OK** to update.

9.5.7 Auto Restart

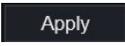
Procedure

Step 1 On the **System Setting** screen, choose **System > Auto Restart** to access auto restart enable the auto restart, the screen as shown in Figure 9-40.

Figure 9-40 Auto restart



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

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

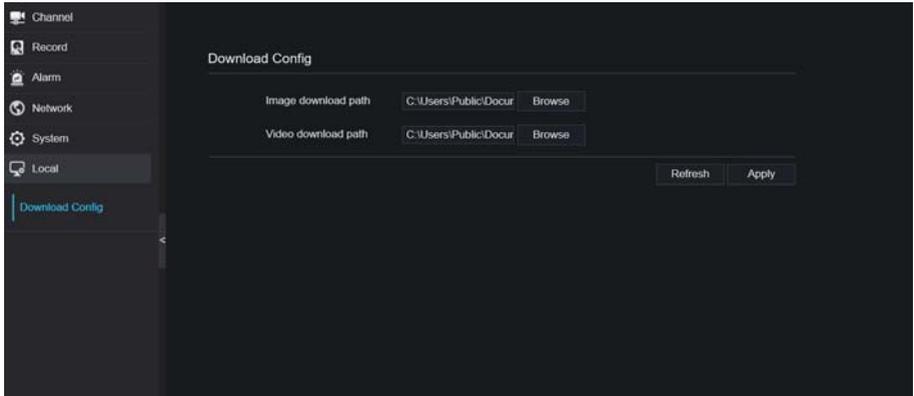
9.6 Local

Set the image download path for snapshot and the record download path for record files in the download configuration interface.

Procedure

Step 1 Click **Local Download Config** in local interface, as shown in Figure 9-41.

Figure 9-41 Local interface



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.