

Digital Video Recorder (DVR) User Manual

Issue

V4.5

Date

2022-03-01

Legal Notice

Trademark Statement:

VGA is trademark of IBM Corporation.

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

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

Responsibility statement:

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

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

Privacy Protection Reminder:

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

About This Document:

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

Network Security Advice

Required measures to ensure basic network security of equipment:

Modify the factory default password and use a strong password

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

Update firmware

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

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

1. Change your password regularly

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

2. Modify the default HTTP and data ports

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

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

3. Use HTTPS/SSL encryption

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

4. Enable IP filtering

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

5. Change the ONVIF password

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 its permissions.

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 boring operations. We recommend that you place the device in a locked room and place it in a locked cabinet with a locked box.

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

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

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.

Symbol Conventions

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

Symbol	Description	
	Alerts you to a high risk hazard that could, if not avoided.	
Alerts you to a medium or low risk hazard that could, if no avoided, result in moderate or minor injury.		
	Alerts you to a potentially hazardous situation that could, if not avoided, result in equipment damage, data loss, performance deterioration, or unanticipated results.	
Ge=™ TIP	Provides a tip that may help you solve a problem or save time.	
	Provides additional information to emphasize or supplement important points in the main text.	

Safety Instructions

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

Requirements

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

Power Requirement

- Be sure to use the specified manufacturer's model battery, otherwise there is a danger of explosion!
- Be sure to use the battery as required, otherwise there is a danger of the battery catching fire, exploding or burning!
- Only use the same model of battery when replacing the battery!
- Be sure to dispose of the used battery as the instruction of battery!
- Be sure to use the power adapter that meets standard with the device, otherwise the personal injury or equipment damage caused by the user will be borne by the user.
- Use a power supply that meets the SELV (Safety Extra Low Voltage) requirements and supply power according to the rated voltage of IEC60950-1 in accordance with the Limited Power Source. The specific power supply requirements are based on the equipment label.
- Connect the Class I product to plug with the power outlet with a protective ground connection.
- The appliance is coupled to the port unit. Keep it at an easy angle for normal use.

Important Statement

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

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

Contents

Legal Noticei
Network Security Adviceii
About This Documentiv
Purposeiv
Symbol Conventions iv
Safety Instructionsv
Requirements v
Power Requirement v
Important Statement v
Contentsvi
1 Preface1
1.1 Product Description
1.2 Product Features
1.2.1 Cloud Upgrade 1
1.2.2 Real-time Monitoring 1
1.2.3 Playback
1.2.4 User Management
1.2.5 Storage Funtion
1.2.6 Alarm Function
1.2.7 Network Monitoring
1.2.8 Split Screen
1.2.9 Recording Function
1.2.10 Backup Function
1.2.11 External Device Control
1.2.12 Accessibility
Product Structure
1.3 Front Panel 5
1.4 Important Notes
1.5 About This User Manual7

1.6 Installation Environment and Precautions7
2 Install Device
2.1 Process
2.2 Unpacking Inspection
2.3 Install Hard Disk 11
2.3.1 Install One or Two Hard disks11
2.3.2 Install Four Hard disks 13
3 Basic Operations 14
3.1 Power on the Device
3.2 Activation
3.3 Power off the Device
3.4 Login to the System
4 Wizard
5 Quick Navigation
5.1 Alarm message
5.2 Real Time Video Bar
5.3 Playback
5.3.1 Time Search
5.3.2 Picture Grid
5.3.3 Event
5.3.4 Backup
6 UI System Setting 44
6.1 Channel Information
6.2 Main Menu
Channel Management
6.2.1 Camera
6.2.1.1 Add Camera Automatically
6.2.1.2 Add Camera Manually 48
6.2.1.3 Delete Camera
6.2.1.4 Operate Camera 49
6.2.2 Encode Parameter
6.2.3 Sensor Setting

6.2.4 OSD Settings	53
6.2.5 Privacy Zone	54
6.2.6 Channel Type	56
6.2.7 ROI	56
6.2.8 Microphone	58
6.2.9 Smart	60
6.2.9.1 AI Multiobject	60
6.3 Record Setting	64
6.3.1 Record Schedule	64
6.3.2 Disk	65
6.3.3 Storage Mode	66
6.3.4 S.M.A.R.T	68
6.3.5 Disk Detection	68
6.3.6 Disk Calculation	70
6.4 Alarm Management	
6.4.1 General	
6.4.1.1 General	
6.4.1.2 IO control push	
6.4.2 Motion Detection	
6.4.3 Camera Tamper	
6.4.4 Video Loss	
6.4.5 Intelligent Analysis	
6.4.6 Alarm In	80
6.4.7 Abnormal Alarm	82
6.4.8 Alarm Out	83
6.4.8.1 Alarm Out	83
6.4.8.2 Camera Alarm out	83
6.5 Network Management	86
6.5.1 Network	
6.5.1.1 IP	87
6.5.1.2 Port	87
6.5.2 802.1 X	

6.5.3 DDNS	89
6.5.4 E-mail	90
6.5.5 Port Mapping	92
6.5.6 P2P	92
6.5.7 IP Filter	93
6.5.8 3G/4G	95
6.5.9 Network Traffic	97
6.6 System Management	97
6.6.1 Information	98
6.6.2 General	99
6.6.2.1 System	99
6.6.2.2 Date and Time	. 100
6.6.2.3 Time Zone	. 101
6.6.2.4 DST	. 102
6.6.3 User	. 103
6.6.3.1 User	. 104
6.6.3.2 Advance Setting	. 106
6.6.4 Security Center	. 106
6.6.4.1 Password	. 107
6.6.4.2 Pattern Unlock	. 108
6.6.4.3 Secure Email	. 108
6.6.4.4 Secure Question	. 109
6.6.5 Auto Sequence	110
6.6.6 Logs	111
6.6.7 Maintenance	112
6.6.8 Auto Restart	113
7 WEB Quick Start	115
7.1 Activation	. 115
7.2 Login and Logout	. 116
7.3 Browsing Videos	. 120
7.3.1 Browsing Real-Time Videos	. 120
7.3.2 Live Video	. 122

7.3.3 Channel Operation	
7.3.4 PTZ Control and Setting	
7.3.5 Sensor Setting	
7.3.6 Layout	
7. 4 Playback	
7.4.1 Video Playback	
7.5 Alarm Search	
7.5.1 Channel Alarm	
7.5.2 System Alarm	
8 System Setting	
8.1 Channel	
8.1.1 Camera	
8.1.2 Encode	
8.1.3 Sensor Setting	
8.1.4 OSD	
8.1.5 Privacy Zone	
8.1.6 ROI	
8.1.7 Microphone	
8.1.8 Smart	
8.1.9 Channel Type	
8.2 Record	
8.2.1 Record Schedule	
8.2.2 Disk	
8.2.3 Storage Mode	
8.2.4 S.M.A.R.T	
8.3 Alarm	
8.3.1 General	
8.3.1.1 General	
8.3.1.2 IO Control Push	
8.3.2 Motion Detection	
8.3.3 Camera Tamper	
8.3.4 Video Loss	

8.3.5 Intelligent Analysis	3
8.3.6 Alarm In 154	4
8.3.7 Abnormal Alarm 155	5
8.3.8 Alarm out	5
8.4 Network	5
8.4.1 Network	5
8.4.2 DDNS	3
8.4.3 E-mail	3
8.4.4 Port Mapping 159	9
8.4.5 P2P	0
8.4.6 IP Filter	1
8.4.7 802.1X	3
8.4.8 Web Mode	
8.4.9 3G/4G	4
8.4.10 PPPOE	5
8.5 System	5
8.5.1 Device Information	5
8.5.2 General	
8.5.3 User	1
8.5.3.1 Add User	1
8.5.3.2 Adv.Setting	3
8.5.4 Security Center	
8.5.4.1 Password	
8.5.4.2 Secure Email 174	4
8.5.4.3 Secure Question	
8.5.5 Logs	
8.5.5.1 Logs	
8.5.5.2 Event	
8.5.6 Maintenance	
8.5.7 Auto Restart	
8.6 Local	

1 Preface

1.1 Product Description

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

This product supports three storage methods: central storage, front-end storage, and client storage. The front-end monitoring point can be located anywhere in the network without geographical restrictions. It is combined with other front-end devices such as network cameras, network video server networks, and professional video surveillance systems to form a powerful security monitoring network. In the networked deployment system of this product, the central point and the monitoring point need only one network cable to connect. It is not necessary to set up visual and audio lines to the monitoring point, and the construction is simple, and the wiring cost and maintenance cost are low.

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

1.2 Product Features

1.2.1 Cloud Upgrade

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

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 IP camera or NVS (Network Video Server) of the DVR device is transmitted to the network terminal for decompression and reproduction. The device supports 8 simultaneous online users to perform streaming operations. The audio and video data is transmitted using protocols such as HTTP (Hyper Text Transfer Protocol), TCP (Transmission Control Protocol), UDF (User Datagram Protocol), MULTICAST, RTP (Real-time Transport Protocol), and RTCP (Real Time Streaming Protocol). Use SNMP (Simple Network Management Protocol) for some alarm data or information Support WEB mode access system, applied to WAN, LAN environment.

1.2.8 Split Screen

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

1.2.9 Recording Function

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

1.2.10 Backup Function

Support USB2.0 and eSATA video backup.

1.2.11 External Device Control

The peripheral control function is supported, and the control protocol and connection interface of each peripheral can be freely set.

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

1.2.12 Accessibility

Support video NTSL (Nation Television Standards Committee) system and PAL (Phase

Alteration Line) system.

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

Support for logging recording.

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

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

For other functions, please see the following text.

Product Structure

1.3 Front Panel





Table 1-1 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.	
-	DVK is shut down, the f wik indicator is turned on.	
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 1-2 Real panel

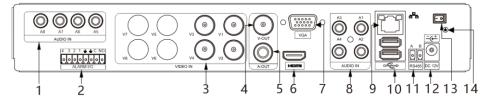


Table 1-2 Real panel function

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	- o]	Power switch (some models do not have switch)	
14	÷	Safe ground screw of the device	

1.4 Important Notes

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

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

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

• Use Monitoring dedicated hard disks as the storage devices of the DVR with high stability and competitive price/performance ratios (the quality of hard disks sold on markets varies greatly with different brands and models).

• Do not open the enclosure of this product unless performed by a professional person to avoid damage and electric shock.

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

1.5 About This User Manual

Please note the following points before using this user manual:

- This user manual is intended for persons who operate and use the 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.

1.6 Installation Environment and Precautions

Installation environment

Table 1-3 defines the installation environment of the DVR.

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 $+45^{\circ}$ 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)	

Table 1-3 Installation environment

Installation precautions

Note the following points when installing and operating the DVR:

• The power adapter of the DVR uses DC48V \pm 20% input. Do not use the DVR when voltage is too high or too low.

- Install the DVR horizontally.
- Avoid direct sunlight on the DVR and keep away from any heat sources and hot environments.
- Connect the DVR to other devices correctly during installation.

• The DVR is not configured with any hard disk upon delivery. Install one or more hard disks when using the DVR for the first time.

The DVR identifies hard disk capacity automatically and supports mainstream hard disk models. User should use good brands of hard disk so that the DVR can operate stably and reliably, please refer to chapter 错误!未找到引用源。错误!未找到引用源。

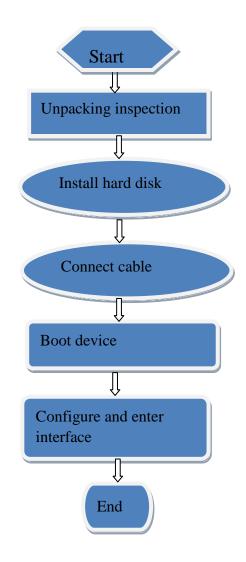
Other precautions

- 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.

2 Install Device

2.1 Process



- Step 1 Check the appearance, packaging, and label of the device to ensure which 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 .

2.2 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.

No	Item		Check content
1	Overall	Appearance	Is there any obvious damage
	packaging	Package	Is there accidental impact
		Accessories	Is it complete
2	Label	Label of device	Is the equipment model consistent with the order contract? Whether the label is torn 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.
3	Cabinet	Package	Is there any obvious damage
		Data cable, power	Is the connection loose?

Table 2-1 Unpacking inspection

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

2.3 Install Hard Disk

When installing for the first time, first check if the hard disk is installed. It is recommended to use the company recommended hard disk model 9 disk compatibility.

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.

2.3.1 Install One or Two Hard disks

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

Step 2 Take out the screws and silicone cushion, route the screws through the silicone cushion,

and install it to the screw holes, as show in Figure 2-1.

Figure 2-1 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 2-2.





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

Figure 2-3 Install hard disk



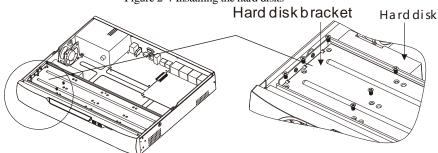
Step 5 Insert the hard disk data cable and power cable, then put on the upper cover and fasten the fixing screws.

2.3.2 Install Four Hard disks

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

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

Figure 2-4 Installing the hard disks



Step 3 Install other hard disks following step 2.

Step 4 Insert the hard disk data cable and power cable, then put on the upper cover and fasten the

fixing screws.

3 Basic Operations

3.1 Power on the Device



CAUTION

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

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 3-1.

Figure 3-1 Real-time video screen

	Activa	ation	SVG
	Language	English 🗸	
	Username	admin	
	Enter a new password		
	Confirm the new password		
	Enter channel default password		DVA
	- Valid password range [6-32] ch		
	 At least 2 kinds of numbers, low Only these special characters a 		
	 Only these special characters a Channel default password limit i 		
الحورية وحدولة المحا			
	OK		

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

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

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

DVR. Format the hard disk.

The hard disk is damaged.

3.2 Activation

When the user login the device at first time, or reset the DVR, you need to activate the device and set login and channel default password, as shown in Figure 3-2.



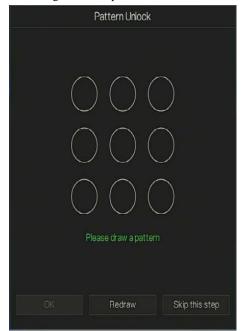
Activation				
Language		English	~	
Username		admin		
Enter a new passwor	d			
Confirm the new pas	sword			
Enter channel default	password			
– Valid password range [6–32] characters.				
- At least 2 kinds of numbers, lowercase, uppercase or special.				
– Only these special characters are supported !@#\$*+==_%&"`_				
- Channel default password limit is not empty				
	OK			

Table 3-1 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.
Channel password	Password length must be at least 8 characters.
	Password cannot contain special characters

The DVR channel connection password is for authenticating the camera.

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



🛄 ΝΟΤΕ

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 3-4.

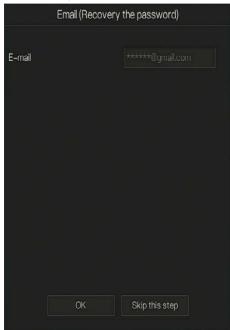


Figure 3-4 Set Email

Set the email address, if you forget the password, you can though 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.

Question (Reco	overy the password)	
Question one	The brand and model of	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 char	acters for the answer	
- Please enter up to 32 chara	cters for the answer	
OK	Skip this step	

Figure 3-5 Set question

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

The worst security question you have ever seen

The most funning/worst design you have ever seen

Question 2: Your favorite team

Question 3: Your favorite city

The three question options cannot be set to the same.

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

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

3.3 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.

3.4 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 3-6.

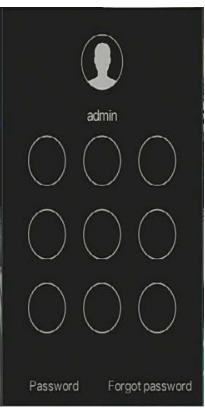


Figure 3-6 Pattern unlock login page

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 3-7.

Fi	gure 3-7 Password lo	ogin page	
	Login		
٩	English	~	
٤	admin	~	
a).
	Logir	1	
	Forgot pas	sword	

Step 3 Input the username and password.

\square	NOTE
-----------	------

The password incorrect more than 3 times, please login again after 5 minutes. You can also power off, and power on to start on the device, input the correct password to avoid waiting five minutes. If user forget password, click Forgot password. User can choose a way to create new password:

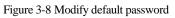
1. Scan the QR code and send the QR code to your seller, seller send the verification

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 3-8



	Modify default password		
New password Confirm password			
	Modify password		
	6-32] characters. bers,lowercase,uppercase or special character contail s are supported !@#\$*+=	ned.	

----End

4 Wizard

Login the DVR, the wizard is showing on live video, click **Start Wizard**, the pop-up window will show as Figure 4-1.



Figure 4-1 Wizard

I Igure 4-2 Wizard	of network
🕈 Wizard	×
Network	
DHCP	
IP Address	192.168.0.120
Subnet Mask	255.255.0.0
Gateway	192.168.0.1
Obtain DNS Automatically	
DNS1	192.168.0.1
DNS2	8.8.8.8
UPnP Enable	
	Next Cancel

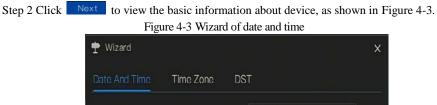
Figure 4-2 Wizard of network

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

Table 4-1 Network	parameter
-------------------	-----------

Parameter	Description	Configuration
DHCP	Enable DHCP, the device will obtain the IP address from the DHCP server.	[Setting method] Enable
IP Address	Set the IP of 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,	[Setting method]
	he must set that	Manual
		[Default value]
		192.168.0.1
Obtain DNS	N/A	[Setting method]
automatically		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,	[Setting method]
	data port and client port.	Choose type from
	Manual: user set the port manually.	drop-down list
		[Default value]
		Auto
Web Port	N/A	[Setting method]
Data Port	N/A	When UPnP is
Client	N/A	manual, you need to set these.



Date Format	DD/MM/YY hh:mm:ss	Y	
Time Format	24H	v	
NTP Sync	•		
NTP Server	time.windows.com	~	
Frequency of Checks. Minimum 10s	86400s		
Date			
Time			

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

Click to synchrony 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 4-4.

Figure 4-4 Wizard of 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 4-5.

	Channel	IF		Model	Protocol	Operate
	CH1					+
	CH2					+
	CH3					+
	CH4					+
.0	P		Dele	te 4 Protocol	Add Devices	C Refres
	192.168.0.1	53:30001	moder	Private		1004.3.0.8.1.0
٥	192.168.0.2	201:30001		Private	t3.6.0825.10	04.3.0.11.10.T6
	192.168.0.1	84:30001		Private	t3.6.0804.1	004.3.0.6.22.0
	192.168.0.1	22:30001		Private	v3.5.0804.1	004.3.0.32.3.1
Use	ername	admin	Pa	ssword *	****	Add

Figure 4-5 Wizard of adding camera

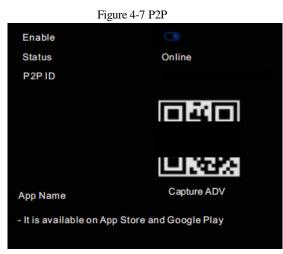
Step 6 Click Next to enter wizard of disk, as shown in Figure 4-6.

Figure 4-6 Wizard of disk

Ŧ	🕈 Wizard							
Dis	sk							
1		Disk	Capacity	Used	SN	Disk Model	Status	
[2 TB	7 GB	Z1E2LCPB	ST2000VX000	Normal	
							Format	
					Previous	Next	Cancel	

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

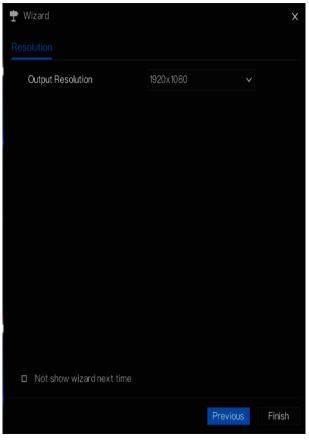
Step 7 Click Next to enter wizard of P2P, as shown in Figure 4-7



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 Capture ADV(search the APP at App Store or Google Play).

Step 9 Click Next to enter the wizard of resolution , as shown in Figure 4-8. Choose resolution from drop-down list.

Figure 4-8 Wizard of 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**.

5 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 **1** 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 5-1.



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 5-2.

Figure 5-2 Real-time video toolbar



The real-time video toolbar is described as follows:



between the single-screen mode and multi-screen mode. Click in on the right of screen splitting

format and choose the channels to view the video.

EXAuto SEQ. click icon, the layout dwell on screen is enabled, for how to set the dwell on,

please see chapter 6.6.5.

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 5-3.

Figure 5-3 Main menu quick toolbar



: Manual alarm, click the icon, the window shows in Figure 5-4.

	Manual Alarm	×
Alarm Out	Start	Stop
1		

Figure 5-4 Manual alarm

Alarm message, click icon would show pop-up message window, as shown in 5.1.

5.1 Alarm message

Pop–Up message X					
		Start time			
Channel8	Motion Detection	27/12/2018 17:32:57			
Channel8	Motion Detection	27/12/2018 17:32:42			
Channel8	Motion Detection	27/12/2018 17:31:53			
Channel8	Motion Detection	27/12/2018 17:31:11			
Channel8	Motion Detection	27/12/2018 17:29:23			
Channel8	Motion Detection	27/12/2018 17:23:46			
Channel8	Motion Detection	27/12/2018 17:23:35			
Channel8	Motion Detection	27/12/2018 17:23:24			
Channel8	Motion Detection	27/12/2018 17:23:13			
Channel8	Motion Detection	27/12/2018 17:18:14			



Clean alarm, click icon and clean the current alarm actions like vioce and external alarm

out.



Information, click icon and the genreal information would show, like network, system,

channel and disk, as shown in Figure 5-5.

Network	System	Channel	Disk		×
Status		Online			
IP Address		192.168.0.121			
Subnet Mask		255.255.255.0			
Default Gatewa	ay	192.168.0.1			
MAC Address		00:1E:A4:00:24	1:91		
DHCP		OFF			
Preferred DNS	Server	192.168.0.1			
Altenate DNS S	Server	8.8.8			
Total Bandwidt	h	100.00 Mbps			
Used Bandwidt	h	10.00 Mbps			

Figure 5-5 Information

II -0

5.2 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 5-6.

Figure 5-6 PTZ adjust screen

Figure 5-6 PTZ adjust screen

Advanced

Advanced

- Zoom +

- Iris +

- Focus +

Auto Focus

Speed - 6 + Home Preset



User adjust direction of camera.



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



: click the button to enter the PTZ setting, as shown in Figure 5-7.

Figure 5-7 PTZ setting

Channel	8	~
PTZ Control Type	Coaxial	~
Protocol	PelcoD	~
Address	8	
Baudrate	115200	~
	Save	Cancel

: 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.

E Image, click the icon ,as shown in Figure 5-8. Select scene, and drag cursor to adjust value of brightness, sharpness, contrast and saturation.

Figure 5-8 Camera picture parameter





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

: Modify device parameters, as shwon in Figure 5-9.

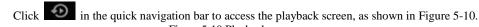
<u>~</u>	Modify device parameters					
	Device Name	Channel07				
	IP Address	192.168.1.77				
	Protocol	Private_SS				
	Port	20001				
	Username	admin				
	Password					
	Remote Channel	CH-1	~			
		OK	Cance	el		

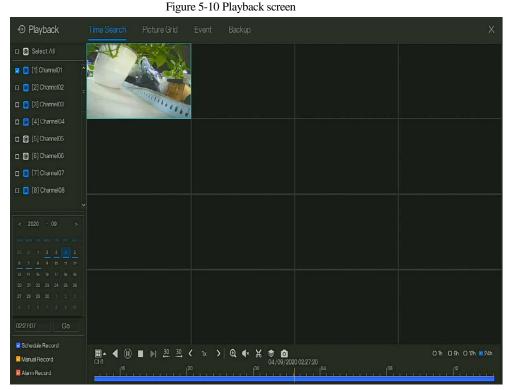
Figure 5-9 Modify device parameter

o: snapshot panorama if the USB disk is plugging in the DVR.

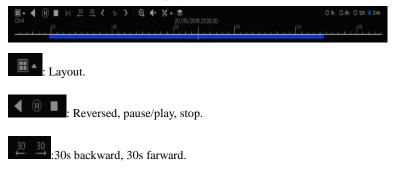
5.3 Playback

Playback refers to playing back a video.





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



(1x):Triple speed, it supports up to 32 times to playback.

C: Zoom.

• : Audio.

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

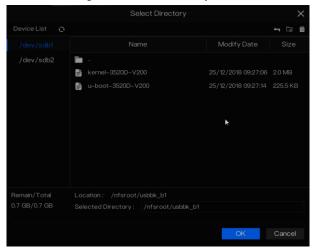
icon again.

The backup type shows, click save, then saving the file pop-up windows would show as Figure

5-11 . Click OK to save.

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

Figure 5-11 Select directory



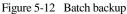


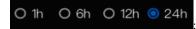
Batch backup, click the icon to backup multi-channels, as shown in Figure 5-12.

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.

1: snapshot the playback video's panorama if the USB disk is plugging in the DVR.

📚 🛛 Batch Backup			Х
Save to			Î
Video Type			
Stream Information	Main Stream		
Start Time	2019/05/28	21:45:16	
End Time	2019/05/29	21:45:16	
Channel	Select All		
		OK	Cancel
		OK	Cancel





Type of time bar, recording video can be showed.

5.3.1 Time Search

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

Operation Description

Click On in the quick navigation bar to access the search screen, as shown in Figure 5-13.



Operation Steps

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

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

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

Step 4 Choose proper button to adjust video.

----End

5.3.2 Picture Grid

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

Click

on the quick navigation bar to access the picture grid screen, as shown in

Figure 5-14.



Figure 5-14 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 dividend 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.

----End

5.3.3 Event

Click **w** on the quick navigation bar; choose **event** at title to access the alarm event screen, as shown in Figure 5-15

	Figure 5-15 E	event scree	n		
Q Search					×
🛃 🔘 Smart Choice					Operate
[1] Channel01					Ð
[2] Channel02					Ð
[3] Channel03					Ð
[4] Channel04					Ð
 (5) Channel05 (6) Channel06 					Ð
 [0] [0] Channel07 					Ð
(8) Channel08					Ð
					Ð
Start Time 14/12/2018 09:26:42	27/12/2018 17:23:13				Ð
End Time	27/12/2018 17:18:14				Ð
	27/12/2018 17:05:37				Ð
Alarm In	27/12/2018 17:03:05				Ð
Motion Alarm	27/12/2018 17:02:42	Channel08		Channel08	Ð
Block Alarm	27/12/2018 17:01:55				Ð
Video Loss	27/12/2018 16:59:40				Ð
Intelligent Analysis	27/12/2018 16:56:41				Ð
Search	277 87 2010 10.00.41	< 1/14	>I	Double click t	

Figure 5 15 Event corport

Operation Steps

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

Step 2 Set start and end time.

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

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

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

----End

5.3.4 Backup

Click on the quick navigation bar, choose **Backup** at title to access the backup screen, as shown in Figure 5-16.

Figure 5-16 Backup screen								
Search								×
								Operate
				Main Strea		ot/usbbk_b 📕	25%	<u>ل</u>

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

----End

6 UI System Setting

6.1 Channel Information

Click the 🗐 will show as Figure 6-1, tick the Channel or Encode, the information will show in

live video screen.





6.2 Main Menu

Right-click on UI screen, the main menu as shown in Figure 6-2. The main menu includes **Channel, Record, Network, Alarm** and **System**.

UI System Setting

		Figure 6-2 D	VR main menu			
	Channel	Re	ecord		Network	
R	Camera Encode Sensor Setting OSD Privacy Zone Channel Ty. ROI Microphone	Sto S.M	cord Schedule Disk rage Mode – Disk Calc. I.A.R.T k Detection	\$	Network DDNS Port Mapping IP Filter PPPOE	802.1X Email P2P 3G/4G Network T.
م م م	Alarm General Motion Camera Tamper Video Intelligent Analysis Alarm Abnormal Alarm Alarm	'n	Syste Informatic Security (Maintenar	on Ger Center Aut		ser ogs

----End

Channel Management

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

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

6.2.1 Camera

Operation Description

Click **Channel** in the main menu to access the camera management screen, as shown in Figure 6--3.

UI System Setting

🗙 System		Record	Alarm Netwo	rk System					
	Camera	RTSP C	onnection						
⊳ Encode		Channel		Model		Firmv	vare Version	Opera	
Sensor Setting		• CH1	127.0.0.1					2	
s sensor setting			192.168.32.222:30001	I IIIIIII	Private	V3.0Simulate	SoftWare_30001	∠ 🛍	
> OSD			192.168.32.195:30001		Private	t3.6.0804		∠ 🛍	
					Private			∠ û	
Privacy Zone		CH5	192.168.32.171:30071	1		t3.5.0807.	1004.3.0.33.6.0	∠ û	
⊳ Channel Type		• CH6	192.168.32.152:30001	persistential.			1004.3.0.33.17.0	∠ ŵ	
p channer rype		• CH7	192.168.32.151:30001			v3.6.0804	1004.3.0.10.11.0	∠ 🛍	
⊳ ROI					Ad	dDevices	Delete	Batchl	Jpdate
⊳ Microphone	Online	Device	Start Search						
				Model	Protoco			rsion	
		192.168.32.1	79:30001		Private		v3.5.0806.1004.3	0.33.0.0	
> Smart		192.168.32							
		192.168.8.1	7:30001		Private		v3.6.0825.1004.3		
▷ Intelligent Tracking		192.168.1.2			ONVIF				
			Userr	ame admin	Pa	ssword ****	*	A	ld

6.2.1.1 Add Camera Automatically

The DVR can add automatically cameras to the camera list.

Operation Methods

Method 1: Click Refresh button, the cameras these are the same local area network with DVR will show in list, input username and password (the default value both are admin)click

, the cameras in the list would be added to channels directly.

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

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

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.

6.2.1.2 Add Camera Manually

Operation Steps

Step 1 Click **t**, the screen to add devices manually is displaying, as shown in Figure 6-4.

+	Add Camera			×
	Channel			
	IP Address			
	Protocol	ONVIF	\sim	
	Port	80		
	Username			
	Password			
	Remote Channel	CH-1	~	
		OK	Car	ncel

Figure 6-4 Add camera screen

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 OK, the camera is added successfully.

🛄 ΝΟΤΕ

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.

6.2.1.3 Delete Camera

Operation Steps

Step 1 Select a camera to delete in the camera list and click in, the delete confirmation

message screen is displaying, as shown in Figure 6-5.



6.2.1.4 Operate Camera

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



Step 1 Click Update, pop-up window to select software, as shown in Figure 6-7.

Step 2 Set the directory click OK to update camera.



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

- Step 4 Click **Reset**, message "**Are you sure to reset?**" would show, user can enable the retain IP address function. click
- Step 5 Tick the cameras with non-onvif protocol and cameras are online, click **Update** to update all cameras at once.

📖 ΝΟΤΕ

Update need upload the software by flash driver.

6.2.2 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 6-8.

UI System Setting

	Figure	6-8 Encode screen	l	
🛪 System	Channel Record Alarm	Network System		×
⊳ Camera	Encode			
	Channel			
▷ Sensor Setting	Stream Information	Main Stream		
⊳ OSD	Video Encode Type	H265		
▷ Privacy Zone	Resolution	2560×1920		
> Channel Type	Frame Rate(fps)			
	Bitrate Type			
⊳ ROI	Bitrate(kbps)(16-2048)	2048		
▷ Microphone	Quality			
	Smart Encode			
⊳ Smart				
▷ Intelligent Tracking				
				Copy Apply

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(VBR can switch the Quality, CBR can adjust quality.) and bitrate size from the drop-down lists. Or enable smart encode to adjust automatically.
- 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.
- ----End

6.2.3 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 6-9.

		Fig	gure 6-9	9 Sensor	setting scr	reen	0		
🛠 System		Record	Alarm	Network	System				×
⊳ Camera	Sensor Se	tting							
⊳ Encode			Q			Channel			
⊳ OSD			08/09/2020	11:05:01 Hes					
▷ Privacy Zone		Chai	nne101						
▷ Channel Type									
⊳ ROI					14F				
▷ Microphone			Scene	Exposure	White Balance	DayNight	Noise Reduction	Enhance Image	Zoom Focus
		Scene	Defaul						
⊳ Smart		Brightness		•	+ 50				
Intelligent Tracking		Sharpness							
P Intelligent frackling		Contrast			+ 50				
		Saturation		0	+ 50				
								Default	Apply

The Sensor Settings 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.

The analog cameras can only adjust the image parameters.

Operation Steps

- Step 1 Select a channel from the drop-down list of channel.
- Step 2 Select scene from the drop-down list. The default values of picture parameters vary with scenarios.

Step 3 Set parameters.

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

6.2.4 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 6-10.

🛠 System	Channel Record Alarm Network System	×
⊳ Camera	050	
⊳ Encode	Channel 1 V	
▷ Sensor Setting	Time 💿	
	Charnel Name 👩 Charnel01	
▷ Privacy Zone		
▷ Channel Type	110000	
⊳ ROI		
⊳ Microphone		
1		
⊳ Smart		
▹ Intelligent Tracking		
	Copy Appl	

Figure 6-10 OSD setting screen

Operation Steps

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

- Step 2 Click next to Time to enable or disable OSD time setting.
- Step 3 Click next to Name to enable or disable OSD channel setting.
- Step 4 Set the channel name.
- Step 5 In the video window, click and drag time or channel to move to a location.

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

----End

6.2.5 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 6-11.

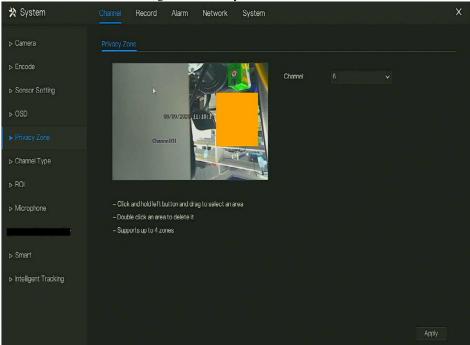


Figure 6-11 Privacy zone screen

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.

----End

6.2.6 Channel Type

Click Channel Type in the main menu or menu of the channel management screen and choose

🛠 System	Channel Re	cord Alarm	Network	System			
⊳ Camera	Channel Type						
⊳ Encode	Channe	el OAUTO	OA	HD OTVI	OCVI	OP	
Sensor Setting			o	0	0	0	
		0	C	0	0		
OSD			C				
Privacy Zone							
Privacy Zone							
			C				
ROI							
Microphone			O				
Smart							
olliait							
Intelligent Tracking							Apply

Channel Type to access the Channel Type screen, as shown in Figure 6-12.

Figure 6-12 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.

6.2.7 ROI

Click **ROI** in the main menu or menu of the channel management screen and choose **ROI** to access the ROI screen, as shown in Figure 6-13.

UI System Setting

System Channel Record Alarm Network System	
	×
⊳ Camera ROI	
> Encode Channel 19	
▷ Sensor Setting ▷ Sensor Setting Stream Main Stream ✓	
⊳ OSD Area D 1 v	
⊳ Privacy Zone Enable	
> Channel Type	
▶ ROI	
⊳ Microphone – Note: Max size 50%	
- Right click to remove the zones drawn	
– Special characters are not supported: ∽%&*/,;= +	
⊳ Smart	
⊳ Intelligent Tracking	
그는 것 같은 것 같은 것 같아요. 그는 말 같이 많이	
1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1	
Apply	

Table 6-1 RIO parameter

Parameter	Description	Setting
Stream	Stream ID.	[Setting method]
		Select a value from the drop-down
		list box.
		[Default value]
		Stream 1
Enable	Enable the ROI	[Setting method]
		Click the button.
		[Default value]
		OFF

Parameter	Description	Setting
Area ID	ROI area ID, there are 8 area	[Setting method] Select a value from the drop-down list box. [Default value] 1
Level	Visual effect of ROI. The higher the grade is, the more clearly areas inside and the vaguer areas outside are. There are five levels.	[Setting method] Select a value from the drop-down list box. [Default value] 5
Area Name	The marked name used for areas.	[Setting method] Enter a value manually. The value cannot exceed 32 bytes.

6.2.8 Microphone

Click **Microphone** in the main menu or menu of the channel management screen and choose **Microphone** to access the Microphone screen, as shown in Figure 6-14.

Figure 6-14 Microphone

🗙 System		Record	Alarm	Network	System			×
⊳ Camera	Microphon	e						
▷ Encode	Channe	el						
▷ Sensor Setting	Microp	nhone		٩				
⊳ OSD	Microp	hone Type		Line In				
▷ Privacy Zone	Microp	ihone Volume				+ 50		
⊳ ROI								
► Microphone								
⊳ Smart								
Intelligent Tracking								
								Annhi
								Apply

Table 6-2 Microphone

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

6.2.9 Smart

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

6.2.9.1 AI Multiobject

🛠 System	Channel Record	Alarm	Network	System					Х
⊳ Camera	Al Multiobject								
⊳ Encode	Chupe113			9-1	Channel 1				
▹ Sensor Setting		L Mon							
⊳ OSD									
▷ Privacy Zone	10s								
> ROI					Clear				
≽ Microphone		re So	hedule						
	Face Detection	n	0		Image Matting Qulity		Medium		
	Fullbody Detec	tion	٩		Attribute		lacksquare		
	License Plate	Detection	0		Snapshot Mode		Optimal		
Intelligent Tracking	Vehicle Detec	tion	٢		Yaw Degree(0-90)				
	Display Trace	Info	Mode1		Tilt Degree(0-90)				
	Show Detection	on Area	9		Pitch Degree(0-90)				
	Confidence De	egree	Mediu		FTP upload image ma	atting	▣		
	Face Pixel Min	(30–300)			FTP upload whole im	age	O		
								Apply	

Figure 6-15 AI multiobject

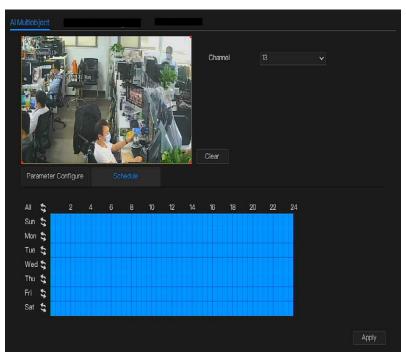
Parameter	Description	How to set
Face detection	The camera will snap the face when someone	Enable

UI System Setting

Parameter	Description	How to set
	appears in live video.	
Full body detection	The camera will snap the whole body when someone appears in live video.	Enable
Licence plate detection	The camera will snap the licence when the vehicle's licence appears in live video.	Enable
Vehicle detection	The camera will snap the licence when the vehicle appears in live video.	Enable
Display trace info	Enable the function and a trace frame will show at live video. Mode 1:	Choose from drop list.
Show detection area	Enable to set a detection area, and the frame will show at live video	Enable
Confidence coefficient	The range of snap image, there are three type, such as high, mid and low. The higher the confidence, the better the snap quality and the fewer snapshots.	Choose from drop list.
Face pixel min(30-300)	30-300 pixels, the smaller the pixel be set, the more face will be captured, but it may be mistaken.	Input a value ranges 30 to 300
Body pixel min(30-300)	30-300 pixels, the smaller the pixel be set, the more body will be captured, but it may be mistaken.	Input a value ranges 30 to 300
Plate pixel min(30-300)	30-300 pixels, the smaller the pixel be set, the more face will be captured, but it may be	Input a value ranges 30 to 300

Parameter	Description	How to set
	mistaken.	
Vehicle pixel min(30-300)	30-300 pixels, the smaller the pixel be set, the more face will be captured, but it may be mistaken.	Input a value ranges 30 to 300
Image matting quality	The quality of snap image, There are three mode can be chosen, such as low, mid and high.	Choose from drop list.
Attribute	Click to enable, the screenshot can display the relevant basic information of the vehicle. Such as the age of people, gender, etc. The color, model of the car.	Enable
Snapshot mode	There are three mode can be chosen, such as timing, and optimal.	Choose from drop list.
Upload image interval(1-10 s)	At timing mode, set the interval of upload image.	Input a value ranges 1 to 10
Snapshot count	At optimal mode, set the number of snapshot image	Input a value ranges 1 to 5
Yaw degree(0- 90)	Both eyes appear on the screen, offset in the left and right direction	
Tilt degree(0-90)	The face is deflected, and both eyes cannot appear in the picture.	Input a value ranges 0 to 90
Pitch degree(0- 90)	Face is moving up and down	
FTP upload image matting	Configuration > Network Service > FTP , set FTP related parameters, the captured picture will be sent to the set FTP location	Enable
FTP upload whole image	Capture a picture and send a whole image.	Enable

Figure 6-16 Schedule



6.3 Record Setting

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

6.3.1 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 6-17.

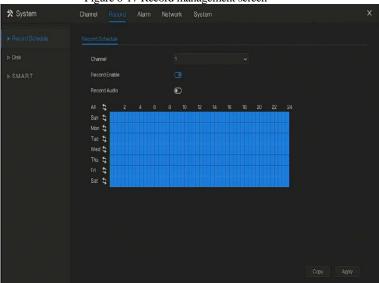


Figure 6-17 Record management screen

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 is again or inverse selection to delete the selected record schedule. Step 6 Click Copy and select channels or tick all, then click K to apply the record management settings to cameras in selected channels , click Apply to save settings.

6.3.2 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 6-18.

		Figur	e 6-18 Di	sk screen			
🗙 System	Channel	Record Alarm	Network	System			×
▷ Record Schedule	Disk						
⊳ SMAR.T		Disk1 Cepacity 2TB			Format		
	Di	sk Status	No	rmal			
	Dis	sk SN	W	5257MN2			
	Us	ed Space	92	GB			
	Re	cording Overwrite	C				
						Appl	

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.

----End

6.3.3 Storage Mode

User is based on need to distribute the channels to different disk group, and use disk capacity reasonably, as shown in Figure 6-19.

UI System Setting

Figure 6-19 Storage mode						
🗙 System	Channel Record	Alarm Network	x System		Х	
▷ Record Schedule	Storage Mode					
⊳ Disk	Mode Selection	@ Group				
► Storage Mode	Disk Group					
⊳ RAID	Channel	123	4 5 6 7 8			
⊳ S.M.A.R.T			2 13 14 15 16			
▷ Disk Detection		17 10 19 2	10 21 22 23 24 🥁			
▷ Cloud Storage					Apply	
	The default Channel L	pelongs to Group 1				
	Group	Disk	Channel	Used Space	Capacity	
		Disk1	1–16	677GB	1.0TB	
		Disk2	17–32	448GB		
		Disk3	33-48	753GB		
		Disk4	49–64	3.0TB	3.0TB	

Operation Steps

Step 1 Choose the disk group.

Step 2 Select the channel to record to disk group.

Step 3 Click Apply to save the settings.

Step 4 The group list will show the detail information.

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

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

6.3.4 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 6-20.

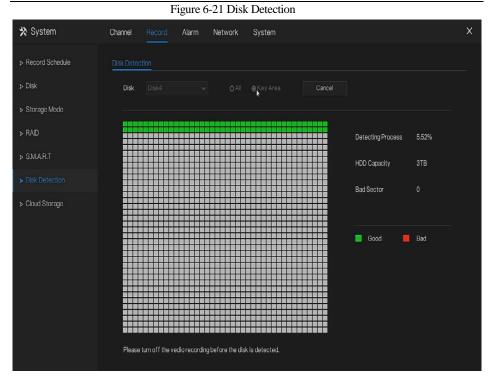
🕉 System	Channel	Record Alarm	Network	System					
	Disk								
	Disk SN	Z1E2LCPB		Disk Model	ST2000V	K000-1CU164			
	Temper	ature 42.0 C		Working Time	2.4 Year				
	Disk He	aith GOOD							
		raw-read-error-rate	OK	119	86		prefail	0xa89e170d0000	
		start-stop-count					old-age	0x7c020000000	
		reallocated-sector-							
		seek-error-rate						0x36c8810d0c00	
								0x0000000000000	
							old-age		

Figure 6-20 S.M.A.R.T

6.3.5 Disk Detection

Before the recording the video, user need to detect the disk to keep the data safety, as shown in Figure 6-21.

UI System Setting



Operation Steps

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

- Step 2 Tick all or key to detect the disk. Detect all need some time, detect key section maybe need a few minutes.
- Step 3 Click Scan to scan the disk.
- Step 4 The result of disk will show in interface

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

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

6.3.6 Disk Calculation

User can calculate the usage of disk, so that he can set the storage strategy reasonably, as shown in Figure 6-22.

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

Figure 6-22 Disk calculation of capacity

🗙 System	Channel Record Alarm	Network System	×
▷ Record Schedule	Disk Calculation		
⊳ Disk	Mode Selection	Computing Capacity 🗸	
⊳ Storage Mode	Expect to save time	1 Day 🗸	
▶ RAD	The daily video time	● 24 h	
⊳ SMA.R.T	The required disk space		
▶ Disk Detection	The required disk space		
▹ Cloud Storage		(182.7) 68	
Disk Calculation	٠	\bigcirc	

UI System Setting

Figure 6-23 Disk calculation of time

🗙 System	Channel Record Alarm	Network System	×
Record Schedule	Disk Calculation		
⊳ Disk	Mode Selection	Computation time V	
▷ Storage Mode	Disk Size		
▶ RAID	The daily video time	124 h	
⊳ SMA.R.T			
Disk Detection	Video can be save time		
▷ Cloud Storage		141 Day Week Month	
Disk Calculation		\bigcirc	
		*	
		Г	

6.4 Alarm Management

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

6.4.1 General

6.4.1.1 General

Step 1 Click **Alarm** in the main menu (or click the alarm page of any function screen in the main menu) to access the alarm management screen, as shown in Figure 6-24.

Figure 6-24 Alarm management screen

🗙 System	Channel Re	ecord Alarm	Network	System	×
	General K) Control Push			
▷ Motion Detection	Enable Alarr	n	٢		
⊳ Video Loss	Duration Tin	ne		×	
▶ Intelligent Analysis	Buzzer dura	ition time		Ŷ	
⊳ Alarm In					
⊳ Abnormal Alarm					
⊳ Alarm Out					
					Apply

Step 2 Enable the Enable alarm button.

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

Step 4 Click Apply to save alarm settings.

6.4.1.2 IO control push

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

Step 1 Enable the IO control push, as shown in Figure 6-25.

Enable Image: Comparison of the second s	Enable Enable Image: Constraint of the state of the	
Alam In 1 Mode N/O Disabled Items Push message to APP Email	Alarm In 1 Mode N/O Disabled Items □ Push message to APP	
Mode N/O V Disabled Items Dush message to APP Email	Mode N/O V Disabled Items DPush message to APP	
Disabled Items Push message to APP Email	Disabled Items Disabled Items	
□ Email		
	⊟Email	
Anniv		
Ander		
Ande		
Anniv		
Anniv		
Andv		
Anniv		
Anniv		
Anniv		
Angly		
Anniv		
Anniv		
Analy		
Anniv		
Analy		
Anniv		
Apply		

Figure 6-25 IO control push interface

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

Step 3 Tick the disable items, click "Apply" to save setting.

----End

6.4.2 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

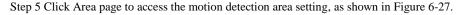
choose **Motion Detection** to access the Motion Detection screen, as shown in Figure 6-26. Figure 6-26 Motion detection screen

🛠 System	Channel Record Alarm Network System	×
⊳ General	Motion Detection	
► Motion Detection	Channel 1	
⊳ Camera Tamper	Enzble	
▹ Video Loss	Mation Analysis	
▷ Intelligent Analysis	Event Actions 🔛 Area	
⊳ Alarm In	∎Push message to APP ⊡Email ⊡Buzzer ⊡Popup message to monitor ⊡Full Screen	
⊳ Abnormal Alarm	Alarm Record I	
⊳ Alarm Out		
	Сору Арріу	_

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

Step 3 Click **O** 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.



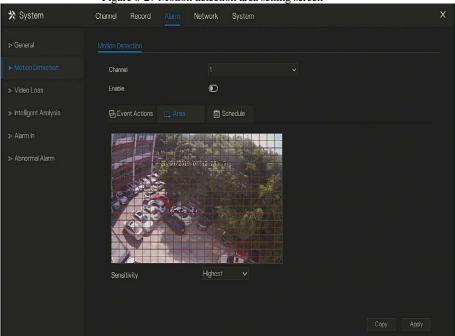


Figure 6-27 Motion detection area setting screen

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 6.3.1 Record

d 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.

📖 ΝΟΤΕ

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.

----End

6.4.3 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 6-28.

* System Channel Record Network System ▷ General Channel Enable ▷ Intelligent Analysis Push message to APP □ Email Buzzer Pop up message to monitor Deful Screen Alarm Out \mathbf{O} Alarm Record \odot

Figure 6-28 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 6.3.1 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.

6.4.4 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 6-29.

🗙 System	Channel Record Alarm Network System	X
⊳ General	Video Loss	
▷ Motion Detection	Chamel 1	
▷ Camera Tamper	Enable 🕜	
➤ Video Loss	Event Actions	
▷ Intelligent Analysis		
⊳ Alarm In	Alarm Record	
⊳ Abnormal Alarm		
⊳ Alarm Out		
	Сору	Apply

Figure 6-29 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 6.3.1 Record Schedule Set the record schedule.

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

----End

6.4.5 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 6--30.

- Ale Locale and	Figure 6-50 Interligent Analysis screen	1000
🗙 System	Channel Record Alarm Network System	Х
⊳ General	Perimeter Single Virtual Fence Double Virtual Fences Object Left Object Removed Signal Bad Lotter Multi Lotter Abnormal Speed Converse Illegal Parking Personnel Count Advanced	
Motion Detection		
⊳ Camera Tamper	Chamel 6 v	
▹ Video Loss		
► Intelligent Analysis	Event Actions ::: Area 🛗 Schedule	
⊳ Alarm In	■Push message to APP □Email □Buzzer □ Pop up message to monitor □ Full Screen Alarm Out	
> Abnormal Alarm	Camera Alarm Out C Alarm Record C	
⊳ Alarm Out		
	Apply	

20 T / 11' / A 1 '

Step 2 Select one action to set the alarm.(perimeter, single virtual fence, double virtual fences, object left, signal bad, loiter, multi loiter, abnormal speed, converse, illegal parking, 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 Copy and select a channel, then click oK to apply the parameter settings to cameras in selected channels, click Apply to save video loss settings.

----End

6.4.6 Alarm In

There two types alarm in, one is the NVR's alarm in, another is the camera channel's alarm in.

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 6-31.

and the second second	Figure 6-31 Alarm	
🛪 System	Channel Record Alarm Network	System X
⊳ General	Alarm In Comera Alarm In	
Motion Detection	Alarm In 1	
⊳ Camera Tamper	Enable 💽	
▹ Video Loss	Mode N/O	
▷ Intelligent Analysis	Name Sensor 1	
⊳ Abnormal Alarm		Bluzzer
⊳ Alarm Out	Alarm Record	
		Apply

🗙 System	Channel Record Alarm	Network System		×
⊳ General	Alarm in Channel Alarm in			
Motion Detection	Channel			
⊳ Video Loss	Alarm In			
▶ Intelligent Analysis	Alarm Type			
	Enable	٢		
⊳ Abnormal Alarm	Event Actions 🛗 Sch	edule	k	
		Email DBuzzer DFull Storeen DCloud Storage 1 2 3 4		
				Apply

Figure 6-32 Channel 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.

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 6.3.1 Record

d Schedule Set the record schedule.

Step 7 Click Apply to save alarm in settings.

----End

6.4.7 Abnormal Alarm

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

Operation Description

Step 1 Click Abnormal Alarm in the main menu or menu of the alarm management screen and choose Abnormal Alarm to access the abnormal alarm screen, as shown in Figure 6-33. Figure 6-33 Abnormal alarm screen

🗙 System	Channel Record Alarm Network System	×
⊳ General	Abnormal Alarm	
Motion Detection	Enable 🕒	
⊳ Camera Tamper	Alarm Type	
▹ Video Loss		
▷ Intelligent Analysis		
⊳ Alarm In	■ Push message to APP □ Email □ Buzzer ■ Popup message to monitor	
► Abnormal Alarm	Alarm Out 💽	
⊳ Alarm Out		
والبر كالم		
	Apply	

Operation Steps

Step 2 Tick the abnormal actions.

UI System Setting

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.

----End

6.4.8 Alarm Out

6.4.8.1 Alarm Out

Choose one output ID as the output interface, as shown in Figure 6-34.

Figure 6-34 Alarm out screen

🗙 System	Channel	Record	Alarm	Network	System		×
⊳ General	Alarm Out	Camera A	larm Out				
Motion Detection	Output						
⊳ Video Loss							
▹ Intelligent Analysis							
⊳ Alarm In							
Abnormal Alarm							
► Alarm Out							
							Apply

6.4.8.2 Camera Alarm out

Digital Video Recorder User Manual

Figure 6-35 Camera alarm out

🛠 System	Channel Record Alarm	Network System	×
⊳ General	Alarm Out Camera Alarm Out		
▷ Motion Detection	Channel		
⊳ Video Loss	Output ID		
⊳ Intelligent Analysis	Name		
⊳ Alarm In	Valid signal	Close	
⊳ Abnormal Alarm	Alarm Output Mode	Switch Mode	
	Alarm Time(s)(0:Continuous)		
			Apply

Table 6-4 Camera alarm out

Parameter	Description	Setting
Alarm Output	ID of the alarm output channel. NOTE The number of alarm output channels depends on the device model.	[Setting method] Select a value from the drop-down list box. [Default value] 1
Name	Alarm output channel name.	[Value range] 0 to 32 bytes

Parameter	Description	Setting
Valid Signal Alarm Output Mode	 The options are as follows: Close: An alarm is generated when an external alarm signal is received. Open: An alarm is generated when no external alarm signal is received. When the device receives I/O alarm signals, the device sends the alarm information to an external alarm device in the mode specified by this parameter. The options include the switch mode and pulse mode. NOTE If the switch mode is used, the alarm frequency of the device must be the same as that of the external alarm device. If the pulse mode is used, the alarm device. 	[Setting method] Select a value from the drop-down list box. [Default value] Close [Setting method] Select a value from the drop-down list box. [Default value] Switch Mode
	frequency of the external alarm device can be configured.	
Alarm Time(ms) (0: Continuous)	Alarm output duration. The value 0 indicates that the alarm remains continuous valid.	[Setting method] Enter a value manually. [Default value] 0 [Value range] 0 to 86400 seconds
Manual Control	Control the alarm output.	N/A

----End

6.5 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 6-36.

🛠 System	Channel Record Alarm	Network System	
	P Port		
⊳ 802.1X	DHCP		
> DDNS	IP Address		
⊳ Email	Subnet Mask		
▷ Port Mapping	Default Gateway		
	Obtain DNS Automatically		
	Preferred DNS Server		
▷ IP Filter	Altenate DNS Server		
⊳ 3G/4G			
			Apply

Figure 6-36 Network management screen

6.5.1 Network

Set DHCP and DNS manually or automatically.

6.5.1.1 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 Apply to save IP settings.

----End

6.5.1.2 Port

Operation Steps

Step 1 Click Port page to access the port setting screen, as shown in Figure 6-37.

P Port		
HTTP Port		
DataPort	554	
Client Port	30001	
		Apply

Figure 6-37 Port setting screen

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

Step 3 Click to save port settings.

----End

6.5.2 802.1 X

Operation Steps

Step 1 Click next to **802.1 X** to enable or disable the function , as shown in Figure 6-38. The default is disabled.

Figure 6-38 802.1 X screen				
🗙 System	Channel Record Alarm	Network System	Х	
▷ Network	<u>802:1X</u>			
	Enable			
▶ DDNS	User			
⊳ Email	Password			
▷ Port Mapping				
⊳ P2P				
▷ IP Filter				
⊳ SNMP				
			Apply	

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

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

6.5.3 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 6-39.

	Figure 6-39 DDNS setting screen				
🗙 System	Channel Record Alarr	n Network System	×		
⊳ Network	DDNS				
⊳ 802.1X	Enable				
	Protocol	no_ip 🗸			
⊳ Email	Domain Name				
▷ Port Mapping	User				
⊳ P2P	Password	Password 🚽			
⊳ IP Filter					
⊳ SNMP					
			Apply		

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

...

Step 4 Set domain name, input user and password.

Step 5 Click Test to check the domain name. Step 6 Click Apply to save DDNS network settings

NOTE

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

----End

6.5.4 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 6-40.

🛠 System		larm Network System		X
⊳ Network	Email			
⊳ 802.1X	SMTP Server			
⊳ DDNS	SMTP Server Port			
	Usemame			
▷ Port Mapping	Password			
	Email Sender			
> P2P	Alarm Receiver 1			
▷ IP Filter	Alarm Receiver 2			
⊳ SNMP	Alarm Receiver 3			
	SSL Encryption	OFF		
			Ар	ply

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.

----End

6.5.5 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 6-41.

Figure 6-41 Port mapping setting screen

🗙 System	Channel Record Alarm Netw	vork System	X
▷ Network	Port Mapping		
⊳ 802.1X	UPnP Enable		
> DDNS	Mode		
⊳ Email	HTTP Port		
	DataPort		
> P2P	Client Port		
⊳ IP Filter	Port range [1025-65534]		
⊳ 3G/4G			
⊳ Wifi			

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.

----End

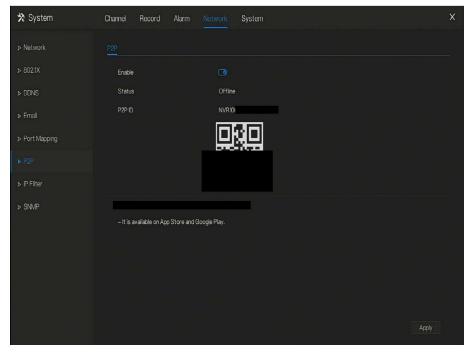
6.5.6 P2P

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

Operation Steps

Step 1 Click **P2P** in the main menu or menu of the network management screen and choose **P2P** to access the P2P screen, as shown in Figure 6-42.

Figure 6-42 P2P screen



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

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

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

----End

6.5.7 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 6-43.

Figure 6-43 IP Filter setting screen

🛠 System	Channel Record Alarm Network System	Х
▷ Network	PFilter	
⊳ 802.1X	P Filter 🕜	
> DDNS	Rule Type Black List 🗸	
▹ Email	Black List(Following network segments are forbidden)	
▷ Port Mapping		
> P2P		
► IP Filter		
▷ SNMP		
	+ -	
	Apply	

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 6-

-44.

Figure 6-44 IP Address Segment screen

Start IP			
End IP			
	OK	Car	ncel
			1

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

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

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.

----End

6.5.8 3G/4G

User can use modem to connect to data network.

📖 ΝΟΤΕ

Some devices may not have the function.

Operation Steps

Step 1 Plug the modem to DVR, and enable the 3G/4G function, as shown in Figure 6-45.

	Figure 6-45	5 3G/4G setting screen	
🛠 System	Channel Record Alarm	Network System	×
▷ Network	<u>36/46</u>		
⊳ 802.1X	Enable		
⊳ DDNS	Status	Disconnected	
⊳ Email	Access Mode		
▷ Port Mapping	APN Dial Number		
⊳ P2P	Username		
▶ IP Filter	Password		
▶ 3G/4G	IP Address		
⊳ Wifi			
			Apply

Step 2 The status is connected to set the other parameters.

- Step 3 Choose access mode, the default is AUTO. There are five modes can be chosen, such as AUTO, LTE, TD-SCDMA, WCDMA, GSM/GPRS.
- Step 4 Input the APN, dial number, username, password, IP address. At auto mode, all these parameters can obtain automatically.

Step 5 Click Apply to save settings.

Modify the access mode, if the status is all disconnected in five minutes, please unplug the modem to restart the modem immediately.

Users are familiar with the relevant network (different service provider parameters are different) and modem information before manually switching to other modes, we recommend access mode to choose auto.

When using the 3G / 4G function, you need to manually close the PPPOE function. Only one function can be used at a time.

If the Internet access type is LTE (4G network), you do not need to dial the number, user name and password.

----End

6.5.9 Network Traffic

User can view the network traffic immediately, as shown in Figure 6-46.

Figure 6-46 Network traffic screen

🛠 System	Chan	nel Reco	ord Alarm		System			>
⊳ Network	Netv	vork Traffic						
⊳ 802.1X	12	8Mbps						
⊳ DDNS								
⊳ Email								
▷ Port Mapping			~~~	~/~			~	
⊳ P2P								
⊳ IP Filter								
⊳ SNMP								
⊳ 3G/4G		_AN1						
▷ PPPOE								
		NIC	Status		VAC Address	мти	NIC TYPE	Display
		LANI	Online		00:1C:27:11:9F:32	1500	Self ∧ daptive	

There are two rates, transmit rate and receive rate.

----End

6.6 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 6-47.

Figure 6-47 System setting screen					
🛠 System	Channel Record Alarm	Network System	×		
	Information				
⊳ General	Device ID				
	Device Name	Device			
Security Center	Device Type	DVR			
▷ Auto Sequence	Model				
	Firmware Version	v4.5.0817.0000.003.10.32.1			
▶ Logs	U-boot Version	140509 1000 10			
» Maintenance	Kernel Version	140408082A36			
⊳ Auto Restart	HDD Number				
	Channels Supported	24			
	Alarm In				
	Alarm Out				
	Audio In				
	Audio Out				

6.6.1 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 6-48.

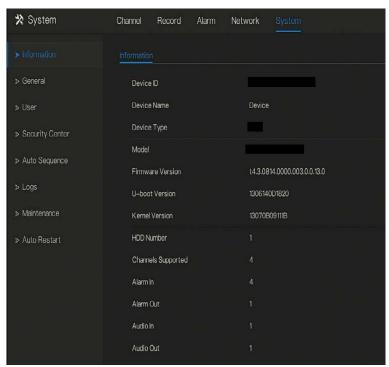


Figure 6-48 Information interface

6.6.2 General

6.6.2.1 System

Operation Steps

Step 1 Click **General** in the main menu or menu of the system management screen and choose **General** to access the system screen, as shown in Figure 6-49.

	Figure 6-2	19 system setting s	screen	
🗙 System	Channel Record Alarm	Network System		×
▷ Information	System Date And Time	Time Zone DST		
	Device Name			
⊳ User	Output Resolution			
Security Center	Language	English		
⊳ Auto Sequence				
⊳ Logs				
▷ Maintenance				
⊳ Auto Restart				
				Apply

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.

6.6.2.2 Date and Time

Operation Steps

Step 1 Click **Date and Time** page to access the date and time setting screen, as shown in Figure 6-50.

🛠 System	Channel Record Alarm Ne	etwork System	X
▷ Information	System Date And Time Time Z	fone DST	
	Date Format	DD/MM/YY hhmm.ss 🗸	
⊳ Úser	Time Format		
▹ Security Center	NTP Sync	G	
⊳ Auto Sequence	NTP Server		
⊳ Logs	Frequency of Checks. Minimum 10s	86400s	
	Date		
▷ Maintenance	Time		
▷ Auto Restart			
	 Time modification will cause channels 	s to reconnect, and will affect the video query	
		Apply	

Figure 6-50 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.

----End

6.6.2.3 Time Zone

Operation Steps

Step 1 Click **Time zone** page to access the time zone setting screen, as shown in Figure 6-51.

	Figure 6-:	51 Time zone setting screen	
🗙 System	Channel Record Alar	rm Network System	x
> Information	System Date And Time	Time Zone DST	
► General	Time Zone	(GMT+00:00) Dublin, Edinburgh, Lo. 🗸	
⊳ User			
▹ Security Center			
⊳ Auto Sequence			
⊳ Logs			
⊳ Maintenance			
⊳ Auto Restart			
			Apply

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

Step 3 Click Apply to save settings.

6.6.2.4 DST

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

Operation Steps

Step 1 Click DST page to access the DST setting screen, as shown in Figure 6-52.

Figure 6-52 DST setting screen						
🛠 System	Channel Record Alarm Network System	×				
▷ Information	System Date And Time Time Zone DST					
▶ General	Daylight Savings Time					
⊳ User	Start Time Mar v Last one v Sun v 100 v					
Security Center	End Time Oct v Last one v Sun v 100 v					
⊳ Auto Sequence	Offset Time 1Hour v					
⊳ Logs						
▷ Maintenance						
⊳ Auto Restart						
		pply				

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 Apply to save settings.

6.6.3 User

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

6.6.3.1 User

Operation Steps

Step 1 Click User in the main menu or menu of the system management screen and choose User

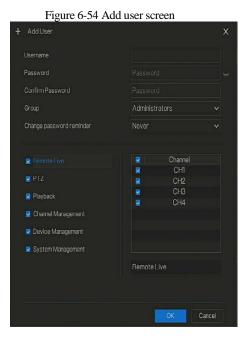
to access the user screen, as shown in Figure 6-53.

	Figure 6-53 User management screen						
🛠 System	Channel Record	Alarm Network	System		×		
▶ Information	User Adv.Settin						
⊳ General		Username		Operate			
		admin	Super admin	۷			
▹ Security Center							
▷ Auto Sequence							
⊳ Logs							
⊳ Maintenance							
▹ Auto Restart							
				Add			

Step 2 Add or delete a user.

Add a user

Click Add, the Add User dialog box appears, as shown in Figure 6-54.



Input a username, password and confirm password.

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 OK. The user is set successfully.

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

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

-----End

6.6.3.2 Advance Setting

Operation Steps

Step 1 Click User in the main menu or menu of the system management screen and choose Adv

Figure 6 55 Advance setting series

Setting to access the user screen, as shown in Figure 6-55.

	Figure 0-55	Advance setting screen	
🛠 System	Channel Record Alarm	Network System	X
▷ Information	User Adv.Setting		
⊳ General	Auto Login	Đ	
	Logout time (minutes)		
▹ Security Center	Password double authentication	Đ	
⊳ Auto Sequence	Boot Wizard		
⊳ Logs			
▷ Maintenance			
▹ Auto Restart			
			Apply

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 Apply to save settings.

6.6.4 Security Center

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

6.6.4.1 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 6-56.

🛠 System	Channel Record Alarm Ne	twork System		Х
▷ Information	Password Pattern Unlock Secu	re Email Secure Question		
⊳ General	Old Password			
⊳ User	New Password			
 Security Center 	Confirm Password			
⊳ Auto Sequence	– Valid password range [6–32] characti	ers.		
⊳ Logs	- At least 2 kinds of numbers, lowercase			
⊳ Maintenance	 Only these special characters are sup 	ported !@#\$*+-=_%&"'(),/'.:;<>?^ -[]{}		
▷ Auto Restart				
			Apply	

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

🛄 ΝΟΤΕ

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

The password should be 6~32 characters.

 $Backslash \setminus cannot \ be \ used.$

Step 3 Click Apply to save modified password settings.

----End

6.6.4.2 Pattern Unlock

Operation Steps

Step 4 Click **Security Center** in the main menu or menu of the system management screen and choose **Pattern Unlock** to access the modify pattern unlock screen, as shown in Figure 6--57.

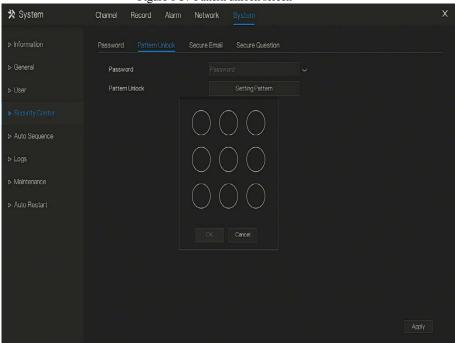


Figure 6-57 Pattern unlock screen

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

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

Step 7 Click OK to save the pattern unlock.

----End

6.6.4.3 Secure Email

Set the email to receive the verification code to create new password, as shown in Figure 6-58.

🛪 System	Channel Record Alarm Ne	twork System		х
▶ Information	Password Pattern Unlock Secu	re Email Secure Question		
⊳ General	Password			
⊳ User	E-mail			
 Security Center 				
▷ Auto Sequence				
⊳ Logs				
▷ Maintenance				
▹ Auto Restart				
			Apply	

Figure 6-58 Secure Email screen

Step 8 Input the password of DVR.

Step 9 Set the Email which will receive email of the verification code.

Step 10 Click Apply to save setting.

----Ena

6.6.4.4 Secure Question

Set the questions to create new password, as shown in Figure 6-59.

🗙 System	Channel Record Alarm Ne	twork System	×
▷ Information	Password Pattern Unlock Secu	re Email Secure Question	
⊳ General	Password		
	Question one	The brand and model of your favoriv	
	Question one answer		
⊳ Auto Sequence	Question two	Your favorite team 🗸 🗸	
⊳ Logs	Question two answer		
	Question three	Your favorite city 🗸	
▷ Maintenance	Question three answer		
▷ Auto Restart	- Please enter at least 4 characters for		
	– Please enter up to 32 characters for t	ne answer	
			Apply

Figure 6-59 Secure question screen

Step 11 Input the password of DVR.

Step 12 Choose the question from drop-down list.

Step 13 Input the answer, click Apply to save setting. ----End

6.6.5 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 6-60.

	F	igure 6-60	Auto Sequ	ence screei	1		
🛪 System	Channel Rec	cord Alarm	Network Sy				×
> Information	Auto Sequence						
⊳ General	Channel	Mode	Display4 🗸	Dwell Time		к 1/1 н	
⊳ User			Display1 Display4	X 2			
▷ Security Center	CH3 CH4						
► Auto Sequence	CH4		CH1		CH2		
⊳ Logs							
▷ Maintenance							
⊳ Auto Restart							
			CH3		CH4		
							Apply

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 Click Apply to save dwell settings.

6.6.6 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 6-61.

🞗 System	Channel Rec	cord Alarm	Network Sys			
⊳ General	Start Date			Start Time		
⇒ User	End Date			End Time		
	LogType					
> Auto Sequence		09/2019 06:23:53	Channel04	Add Camera	[admin] 192.168.0.254 001c	27123898
			Channel04	Delete Camera	[admin] 192.168.0.254 001c	
Maintenance		09/2019 06:23:35	Channel02		[admin] 192.168.0.254 001c	
Auto Restart			Channel01	Add Camera	[admin] 127.0.0.1001c270e	46ba
			Channel02	Delete Camera	[admin] 127.0.0.1001c27121	0ab
				Stop Recording PlayBa		
				Stop Recording PlayBa	k [admin]127.0.0.1 stop play	
				Stop Recording PlayBa		
		09/2019 03:58:19		Start Playback	[admin] 127.0.0.1play at 19/	

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.

----End

6.6.7 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 6-62.

	Figur	e 6-62 M	laintenan	ce scree	en		
🛠 System	Channel Record	Alarm Ne	etwork Syste				×
	Maintenance						
⊳ General		\sim	Ģ		cyle	<u>ح</u> ۸	
	\odot		Þ	Ð,	Ē	Ē	
	Shutdown	Reboot	Logout	Reset	Import Configur.		
	A	A					
	لچک Update	(ليپ) Cloud Update					
	apublo	Cipper of hears					
> Auto Restart							

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.

When the DVR finishes updating, the device would restart.

----End

6.6.8 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 6-63.

🛠 System	Channel Record Alari	n Network System	×
X Olorom			
Information			
⊳ General	Enable		
▶ User	Restart Time		
▶ Security Center			
▷ Auto Sequence			
⊳ Logs			
▶ Maintenance			
► Auto Restart			
			Apply

Figure 6-63 Auto restart screen

Step 2 Enable the function, restart time is showing as figure Restart Time Por Day V 000 V

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

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

----End

7 WEB Quick Start

7.1 Activation

If you don't set the password at UI interface, user need activate the device, as shown in Figure 7--1.

Figure 7-1 Activation interface

Step 1 Set the password, confirm the password.

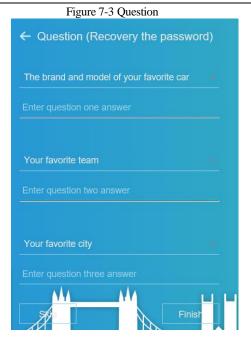
Step 2 Input the channel password.

Step 3 Set the email of recovery the password, as shown in Figure 7-2.

Figure 7-2 Email

Email (Recovery tl	ne password)
1	
Skip	Next

Step 4 Set the question of recovery the password, as shown in Figure 7-3.



🛄 NOTE

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

7.2 Login and Logout

\triangle caution

You must use below Firefox 53 or below Chrome 45 to access the Web interface.

Otherwise, the interface functions cannot be used normally.

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

Brower supports 32 bits.

Descriptions of browser:

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

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

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

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

Login

Step 1 Open IE browser, enter the IP address of the DVR (DHCP is on by default) in the address

box, and press Enter.

The login page is displayed, as shown in Figure 7-4.

Figure 7-4 Login page interface



Step 2 Input the user name and password.

🛄 ΝΟΤΕ

The default user name and password both are admin. The password incorrect more than 3 times, please login again after 5 minutes.

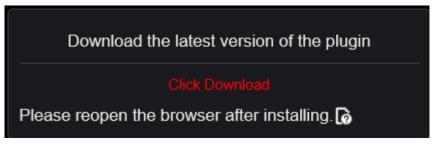
User can change the system display language on the login page.

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 7-5.

Figure 7-5 Download the plugin



Step 4 Install the latest plugin, reopen the browser and the homepage is displaying as shown in

Figure 7-6.

DVR	۲	Ð	Q	ø				د 🔺	G	ß
Device	8						8			
Channel01										
Channel02										
Channel03										
Channel04					NO-VIDE0	N0-VIDE0			~ R	
Channel05										
Channel06										4
Channel07										
Channel08										I.
	۲						>			3
										1
					NO-VIDEO	NO-VIDEO				

Figure 7-6 Homepage interface

Logout

To logout of the system, click in the upper right corner of the homepage. The pop-up
message shows " Do you want to exit? " Click OK and the login page will display.
Homepage Layout
DVR allows you to use the Web interface in a PC for implementation of such functions as live
video, playback, retrieval, setting, image parameters access, configuration, PTZ control and so on
Figure 7-7 shows the overall layout of the interface. For descriptions of the interface, please refer

to Table 7-1.

Figure 7-7 Homepage layout

DVR 1	2 Đ 3 Q 4 Ờ		
🗆 Desilee 🛛 🗬			× 10
😋 Channe 01 🛛 🕨			iei ini
🖸 Deceltz 🛛 🕨			Bia ada
C3 Channe 03 ►			
🔄 Uhannolli 🛛 🕨	NO-3072	K0/2000	<u>ூ</u> 11
CS Chanacole 9 🕨			~ ~ ~
			≺ ດ ≻ ໃ
			6 V 4
			141
			0 0
			요 🔍 🔍 🗠
	кран т	KR2 HER	
	■ ■ Ⅲ ≈ 12	Č	13

Table 7-1 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 serach interface to search channel alarm or system alarm.
4	System setting	Click to enter system setting interface, set channel, recored, 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	Click to show PTZ control buttons in zone 10, you can control the PTZ equipment in the current channels. That function only use for IP dome camera.
	Color parameter button	Click to show color parameter setting buttons in zone 9, you can set and adjust the color parameters, for example, brightness, contrast, saturation, and sharpness. Click More to access image settings.
	Operation zone	The operation zone of PTZ control and image parameter setting.
12	Layouts	Select the one-screen, four-screen, nine-screen or sixteen- screen to switch the layout.
13	Manual alarm	Trigger and close the external alarm device manually.

----End

7.3 Browsing Videos

7.3.1 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 7-8.

Figure 7-8 Adding a	trusted site
Internet Options ? ×	Trusted sites \times
General Security Privacy Content Connections Programs Advanced	You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.
Select a zone to view or change security settings.	Add this website to the zone: https://192.168.0.121 Add Websites:
Trusted sites Sites This zone contains websites that you trust not to damage your computer or your files. You have websites in this zone. Sites	Remove
Custom Custom settings. - To change the settings, click Custom level. - To use the recommended settings, click Default level.	Close
Enable Protected Mode (requires restarting Internet Explorer) Custom level Default level Reset all zones to default level	
OK Cancel Apply	

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 7-9.

Issue V4.5 (2020-09-07)

Figure 7-9 Configuring Active	X controls and plug-ins
Internet Options	
General Security Privacy Content Connections Programs Advanced	
Select a zone to view or change security settings. Image: Security settings Image: Security settings Image: Security level for this zone Image: Security level for this zone Security level for this zone Image: Security level for this zone Image: Security level for this zone Image: Security level for this zone Image: Security level for this zone Image: Security level for this zone Image: Security level for this zone Image: Security level for this zone Image: Security level for this zone Image: Security level for this zone Image: Security level for this zone Image: Security level for this zone Image: Security level for this zone Image: Security level for this zone Image: Security level for this zone Image: Security level Image: Security level for this zone Image: Security level Image: Security level for this zone Image: Security level Image: Security level for this zone Image: Security level Image: Security level for this zone Image: Security level Image: Security level Image: Security level Image: Security level Image: Security level Image: Security level Image: Security level Image: Security level	Security Settings - Internet Zone
OK Cancel Apply	OK Cancel

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

the browser.

🛄 ΝΟΤΕ

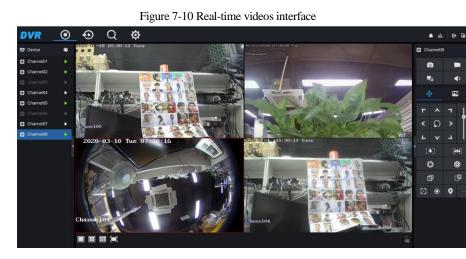
If the repair tips displayed when installing the control, close the browser and continue the installation, reopen the login page when the control is installed.

7.3.2 Live Video

Descriptions

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

Figure 7-10.



----End

7.3.3 Channel Operation

Descriptions

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

Buttons	Button description	How to operate
Ô	Snapshot	Click button to take snapshots of the current image.
	Record	Click button to start recording and click button again to stop recording.
2.6	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.

Table 7-2 Descriptions of homepage

----End

7.3.4 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 7-11.

Table 7-3 describes the operations.

Figure 7-11 PTZ control interface

¢			
٢	^	7	Ţ
<	S	>	6
L	×	7	
	[‡]		
¢	٩		3
Ð		۵	9
	۲	Q	

Table 7-3 Device parameters

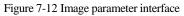
Buttons	Button description	How to operate
r ~ <	Direction key	Click button to control omni-directional movement of the PTZ.
6 	Speed slider	Drag the slider to adjust the value of PTZ rotation speed.

Buttons	Button description	How to operate
[♠]	Zoom in	Click buttons to adjust the focal length.
[** *]	Zoom out	
\bigcirc	Iris+	Click buttons to adjust the aperture.
X	Iris-	
₫	Far focus	Click buttons to adjust the focal length.
Ð	Near focus	
	Auto focus	Click button to focus automatically.
۲	Home preset	N/A
•	Preset	The camera is set the tour, click the button and dome camera rotate as the setting.
	More	More settings

7.3.5 Sensor Setting

Descriptions

The sensor setting can adjust scene, brightness, sharpness, contrast and saturation, Click to access image setting, as shown in Figure 7-12. Table 7-4 describes the operations.



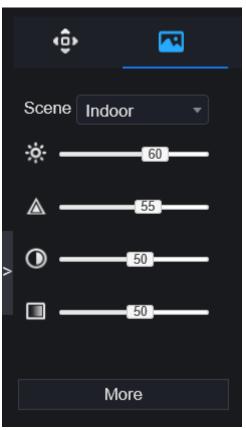


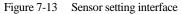
Table 7-4 Device	parameters
------------------	------------

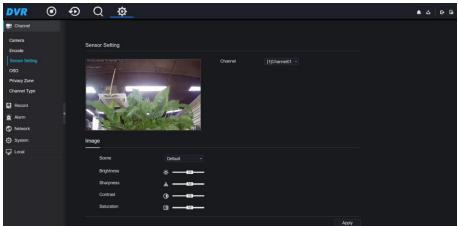
Buttons	Button description	How to operate
÷.	Brightness	Click button to adjust the image brightness.
	Sharpness	Click button to adjust the image definition.
	Contrast	Click button to adjust the transparency of the image.

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 7-13, more detail please

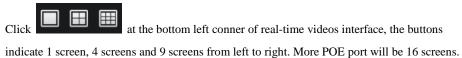
refer to chapter Figure 3-7.





----End

7.3.6 Layout



----End

7.4 Playback

7.4.1 Video Playback

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

Procedure

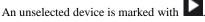
Step 1 Click in the function navigation bar, the video playback interface is displayed,

as shown in Figure 7-14.



Figure 7-14 Video playback

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



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

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

Step 5 Display videos.

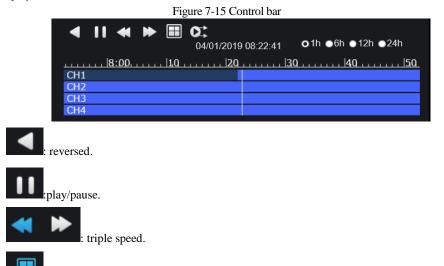
After a device and date are selected, video information is displayed below the video pane. The time scale above the file axis shows the different time points of video recording. The time in blue in the middle is the time of the video playing.

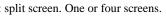
The file axis displays videos. The blue file axis indicates a video exits, grey file axis indicates no video exits.

You can drag the axis to play recording quickly.

Step 6 Play a video.

You can play a video after selecting a device and date. Figure 7-15 shows the control bar of video playback.







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



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



E : batch backup, click the icon to backup many channels' recording videos, as shown in Figure 7-16.

	Figure 7-16 Batch backup									
		Batch Backup								
	Video Type	Mp4								
	Stream	Ma	in Str	eam						
	Start Time	09/	03/20	20 1 [,]	4:26:	58				
	End Time	09/	03/20	20 1 [,]	4:56:	58				
	Channel	∎Se	lect /	AII						
					4		6			
								ОК		Cancel
●1h ●6	h ⊙ 12h (0 2	4h	: ty	pes (of tin	ne ba	ır.		
Channel03										
Ó										
Q .;	: use	r car	1 ope	erate	the	recoi	rd as	same as	live	video.
End										

-

7.5 Alarm Search

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

7.5.1 Channel Alarm

Procedure

Step 1 Click I in the function navigation bar, the channel alarm interface is displayed, as

shown in Figure 7-17.

VR 🎯	• •• <u> </u>		<u>ه</u> ځ و
Channel Alarm	System Alarm		
	Start Time	Channel	Туре
	10/03/2020 06:33:34	Channel07	Video Loss
	10/03/2020 06:13:00	Channel07	Video Loss
	10/03/2020 05:21:50	Channel01	Carnera Tamper
	10/03/2020 05:02:21	Channel01	Camera Tamper
	10/03/2020 04:57:29	Channel01	Camera Tamper
	10/03/2020 04:55:23	Channel01	Camera Tamper
	10/03/2020 04:55:08	Channel01	Camera Tamper
	10/03/2020 04:42:08	Channel01	Camera Tamper
	10/03/2020 04:40:52	Channel01	Camera Tamper
	10/03/2020 04:35:24	Channel01	Camera Tamper
	10/03/2020 02:38:20	Channel03	Video Loss
	10/03/2020 02:36:22	Channel07	Video Loss
	10/03/2020 02:35:48	Channel07	Perimeter
	10/03/2020 02:34:36	Channel07	Perimeter
15	10/03/2020 02:32:38	Channel07	Perimeter

Figure 7-17 Channel alarm interface

Step 2 Click at the top right conner, select the channel and type, set start time and end time, as shown in Figure 7-18.



Channel		All •
Туре	All	•
Start Time	2019/01/03 15:1	3:25
End Time	2019/01/04 15:1	3:25
	Search	

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

Figure 7-19	Channel alarm result
-------------	----------------------

	-		
Channel Alarm	System Alarm		T
D	Start Time	Channel	Туре
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 04:55:08	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
I<< <u>1</u> /1 >>			Every page show 20 *
	1/6 >>I to se	elect the page of alarm list.	
Ever	y page show 20	shows the rows shown in evo	ery page.

7.5.2 System Alarm

Procedure

Step 1 Click **System Alarm** in the channel alarm interface, the system alarm is displayed, as shown in Figure 7-20.

Figure 7-20 System alarm res	alt	
------------------------------	-----	--

DVR 💿	• • <u> </u>		ه ٢ ٦
Channel Alarm	System Alarm		T
D	Start Time	Туре	Remark
1	10/03/2020 07:26:45	IP conflict	IP Conflict
2	10/03/2020 07:22:05	IP conflict	IP Conflict
3			IP Conflict
4	10/03/2020 07:16:01	IP conflict	IP Conflict
5	10/03/2020 06:48:35	IP conflict	IP Conflict
6	10/03/2020 06:41:07	IP conflict	IP Conflict
7	10/03/2020 06:30:46	IP conflict	IP Conflict
8	10/03/2020 06:11:37	IP conflict	IP Conflict
9	10/03/2020 06:09:03	IP conflict	IP Conflict
10	10/03/2020 06:06:57	IP conflict	IP Conflict
11	10/03/2020 06:05:28	IP conflict	IP Conflict
12	10/03/2020 05:48:03	IP conflict	IP Conflict
13	10/03/2020 05:46:59	IP conflict	IP Conflict
14	10/03/2020 05:27:45	IP conflict	IP Conflict
15	10/03/2020 05:26:44	IP conflict	IP Conflict
I<< 1_/7 >>I	1		Every page show 20 +

Step 2 Click at the top right conner, set the channel, type(alarm in and other), start time

and end time, as shown in Figure 7-21.



Туре		All	
Start Time	2019/01/03 15	5:25:03	
End Time	2019/01/04 15	5:25:03	
	Search		

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

----End

8 System Setting

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

8.1 Channel

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

8.1.1 Camera

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

DVR	۲	€	Q	<u> </u>						
🛃 Channel										
Camera			Camera							
Sensor Setting				Channel	IP Address	Port	Model	Protocol	Firmware Version	Operate
OSD				CH1	127.0.0.1					∠.©
Privacy Zone				CH2	192.168.32.101	30001		Private	13.6.0804.1004.3.0.6.12.0	∠.e
Channel Type				 CH3 	192.168.32.130	30001	_	Private	v3.4.0702.1003.3.0.102.0.0	∠.@
Record				CH4	192.168.3.174	30001	_	Private	v3.5.0819.1004.3.0.32.2.1	∠.ē…
🙆 Alarm				CH5	192.168.32.188	30001		Private	13.6.0804.1004.3.0.8.7.0	∠.e
Network				CH6	192.168.32.53	30001		Private	v3.5.0819.3900.172.0.31.0.53	2.©
System				 CH7 	192.168.32.109	30001		Private	V3.6.0804.1004.3.0.7.1.0.D05	∠.e…
🗣				CH8	192.168.18.139			ONVIF	V5.2.1 build 141120	∠.©
					Username admir		Password •••••	here Add Devices	Search Refresh Delete	Batch Update

Figure 8	8-1	Camera	interface
I Iguie (J I	Cumera	mernee

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 8-2.

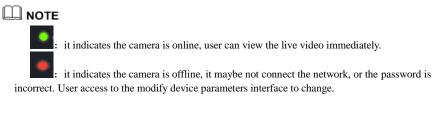
Choose the camera, input username and password, click Add to add new camera.

		Figure 8-2	2 Device search		
Device Search	ı				
■ ID	IP Address	Port M	odel Protoc	col Firmware Versior	n
1	192.168.1			Private_SSL	
2	192.168.1			Private_SSL	
3	192.168.32			Private	
4	192.168.0			Private	
5	192.168.32			Private_SSL	
— 6	192.168.1	.200 30001		Private	
7	192.168.32			Private	
8	192.168.2	.148 20001		Private_SSL	t
9	192.168.1	.76 20001		Private_SSL	
1 0	192.168.32	2.170 20001		Private_SSL	
1 1	192.168.0	.244 20001		Private_SSL	
1 2	192 168 0	248 20001		Private SSI	
	Username adr	nin Pas	sword ••••	Add Refresh	Back
94 Click	Back	to back to car	nera interface.		
5 Click	Refresh to	o refresh came	eras status.		
6 Choose	the cameras ar	nd click	Delete to del	lete.	
7 Click B	atch Update to) update all se	elected cameras a	t once, the pop-up wind	ow wou
w to select s	oftware.				

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

	Figure 8-3 Mo	dify device para	meters		
M	odify device parameters			×	
	Channel Name	Channel06			
	IP Address	192.168.0.232			
	Protocol	Private_SSL •			
	Port	20001			
	Username	admin			
	Password	•••••	ب ہر		
	Remote Channel	CH-1			
			Cancel	ок	
Step 9 Click	to access web immed	liately.			
				① Update	×
				🛞 Reboot	
Step 10 Click	to update, reboot or	reset the selecte	ed camera, as	ମ୍ରି Reset	shows.

The pop-up message "Are you sure to restart the device?" "Are you sure to reset? Reserve IP Address" would respectively show.



8.1.2 Encode

Step 1 On the **System Setting** screen, choose **Channel** > **Encode** to access the encode interface, as shown in Figure 8-4.

Figure 8-4 Encode interface

Encod	de	
	Channel	[1]Channei01 ·
	Stream Information	Main Stream ·
	Video Encode Type	H265 ·
	Resolution	1280x1440 *
	Frame Rate(fps)	
	Bitrate Type	CBR •
	Bitrate(kbps)(128-4096)	2048 🔹
		Copy Apply

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	Сору	to choose other camera to copy settings. Click	Apply	to
save the	settings.			

----End

8.1.3 Sensor Setting

Step 1 On the **System Setting** screen, choose **Channel** >**Sensor Setting** to access the sensor setting interface, as shown in Figure 8-5.

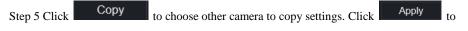
Figure 8-5 Image interface

Sensor Setting				
Contract of the time of the ti		Channel	[1]Channel01 •	
Scene	Default +			
Brightness	÷			
Sharpness	A <u>50</u>			
Contrast	0			
Saturation	II			
				Apply

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

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

Step 4 Other parameters are camera's senor setting, user can refer IP cameras' settings.



save the settings.

🛄 ΝΟΤΕ

The analog cameras can only adjust the image parameters.

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

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

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

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

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

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

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

Day-night: 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.

----End

8.1.4 OSD

Step 1 On the System Setting screen, choose Channel >OSD to access the OSD interface, as

shown in Figure 8-6.

Figure 8-6 OSD interface

OSD			
	Channel	[1]Channel01 •	
	Time 🦲		
	Channel Name	Channel01	
			Copy Apply

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.

----End

8.1.5 Privacy Zone

Step 1 On the **System Setting** screen, choose **Channel** >**Privacy Zone** to access the privacy zone interface, as shown in Figure 8-7.

Figure 8-7 Privacy interface

SQ/DB/2000 07 Giblish Turi		 ► ▲ ↓ ↓		
Channel	[1]Channel01 🔻			

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.

----End

8.1.6 ROI

ROI(Region of interest), choose channel, stream, area ID and draw the area, as shown in Figure

8-8. Set the level, there are five levels can be chosen. Set area name, click "Apply" to save the settings.

Figure 8-8 ROI interface

🚅 Channel							
Carnera Encode	ROI						
Sensor Setting		7/2020 06159:04 Vol.		Channel	[28]Channel28		
OSD	Classe	pe128		Stream	Sub Stream		
Privacy Zone	100			Area ID			
ROI				Enable			
Microphone		-		Level			
Smart	2			Area Name			
Record	- Note	: Max size 50%				Apply	
🚊 Alarm		It click to remove the zones drawn special characters are supported I@#\$**	*090?~			Афру	
S Network							
System							

8.1.7 Microphone

User can set the microphone parameters of channel, as shown in Figure 8-9. Figure 8-9 Microphone interface

📑 Channel			
Carnera Encode	Microphone	9	
Sensor Setting OSD		Channel	[1]Channel01 ·
Privacy Zone		Microphone	-
ROI Microphone		Microphone Type	Line In -
Microphone		Microphone Volume	
Smart			Apply
Record			
🚊 Alarm			
S Network			
O System			

8.1.8 Smart

At smart interface, user can set AI multiobject, as shown in Figure 8-10.

Figure 8-10 Smart interface

Channel				
Camera				
Encode	Al Multiobject			
Sensor Setting		-	Channel [3]Channel0	1 -
OSD			Constituer (Stongaliero	
Privacy Zone		In Maria		
ROI				
Microphone				
Smart		Clear		
Record		Clear		
🚊 Alarm	Parameter Configure Schedule			
S Network	Face Detection		Image Matting Qulity	Medium +
System	Fullbody Detection	-	Attribute	
	License Plate Detection		Snapshot Mode	Optimal -
	Vehicle Detection	-	Yaw Degree(0-90)	60
	Display Trace Info	Mode1 -	Tilt Degree(0-90)	60
	Show Detection Area		Pitch Degree(0-90)	
	Confidence Degree	Medium -	FTP upload image matting	•
	Face Pixel Min(30-300)		FTP upload whole image	
	Body Pixel Min(30-300)	30	Algorithms Library Version	V0104010101040101

8.1.9 Channel Type

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

									,	
				Figu	re 8-11 Cha	nnel type in	terface			
DVR	۲	€	Q	ø						
💻 Channel										
Carnera										
Encode			Channe	Гуре						
Sensor Setting				Channel	Oauto	OAHD	Оти	Осчі	OIP	
OSD										
Privacy Zone										
ROI										
Microphone										
Smart										
Record										
🚊 Alarm										
Network										
System										
-Cystein										
										Apply
										Apply

----End

8.2 Record

Users can set record policy in storage interface.

8.2.1 Record Schedule

Procedure

Step 1 On the **System Setting** screen, choose **Record** > **Record** schedule to access the record schedule interface, as shown in Figure 8-12.

System Setting

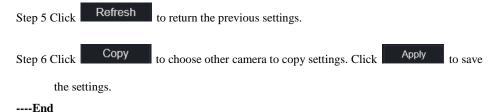
Record		
	Record Schedule	
Disk	Channel [1]Channel01 -	
Storage Mode RAID	Record Enable	
S.M.A.R.T	Record Audio	
Cloud Storage	All \$ 2 4 6 8 10 12 14 16 18 20 22 24 Sun \$	
🚊 Alarm	Mon t	
S Network <	Wed to	
System		
	Sat S	
	Copy Refresh Apply	

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 **w** to choose all

day or all week, you can also click one by one to set the schedule. Or dray the mouse cursor to choose. User can set the alarm recording to save the space of disk.



8.2.2 Disk

Step 1 On the **System Setting** screen, choose **Record** >**Disk** to access the disk interface, as shown in Figure 8-13.

Figure 8-13 Disk interface

🛒 Channel				
Record	Dis	sk		
Record Schedule				
Disk		HDD Disk1		
🚊 Alarm		Capacity 2TB		
S Network				
System				
🖵 Local		Disk1		Format
		Disk Status	Normal	
		Disk SN	Z2F0MDCC	
		Used Space	209GB	
		Recording Overwrite		
		Expired Time(Day)		
				Apply

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



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

----End

8.2.3 Storage Mode

User is based on need to distribute the channels to different disk group, and use disk capacity reasonably, as shown in Figure 8-14.

Figure 8-14 Storage Mode interface

Storage M	lode							
	Mode Selection	O Group						
	Disk Group							
	Channel	1 2 :	3 4	5 (7	8		
		9 10 1 17 19 1	1 12 a 20	13 1 21 2		16		
		- 17 - 18 - 1	- m					
								Apply
Group	Disk	Chann	el			Used Space	Capacity	
	Disk1	1-16				985GB	1000GB	
2	Disk2	17-32				733GB	4.0TB	
	Disk3	33-48				753GB	4.0TB	
4	Disk4	49-64				2.9TB	3.0TB	

Operation Steps

Step 1 Choose the disk group.

Step 2 Select the channel to record to disk group.

Step 3 Click Apply to save the settings.

Step 4 The group list will show the detail information.

----End

8.2.4 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 8-15.

Figure 8-15 S.M.A.R.T interface

M.A.R.T							
Disk	Disk1 *						
Disk SN	W5257MN2		Disk Moo	lel	ST20	000VX008-2E3164	
Temperature	37.0 C		Working	Time	1.0 Y	'ear	
Disk Health	GOOD						
ID	Attribute Name	Status	Value	Worst	Thresh	Туре	Raw value
	raw-read-error-rate	ок	116	99		prefail	0x506d92060000
	spin-up-time	ок	96			prefail	0x00000000000
	start-stop-count	ок	100	100		old-age	0x13020000000
	reallocated-sector-count	ок	100	100		prefail	0x0000000000000
	seek-error-rate	ок		60		prefail	0x84fe00020000
	power-on-hours	ок	90	90		old-age	0x772200000000
	spin-retry-count	ок	100	100		prefail	0x00000000000
	power-cycle-count	ок	100	100		old-age	0x110200000000
184	end-to-end-error	ок	100	100	99	old-age	0x00000000000
	reported-uncorrect	ОК	100	100		old-age	0x00000000000
188	command-timeout	ок	100	100		old-age	0x00000000000

----End

8.3 Alarm

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

8.3.1 General

8.3.1.1 General

Procedure

Step 1 On the **System Setting** screen, choose **Alarm** > **General** to access the general interface. Step 2 Enable alarm to set duration time and buzzer duration time, as shown in Figure 8-16.

Figure 8-16 General interface

L Channel								
Record								
🚊 Alarm		General	IO Control Push					
General			Enable Alarm	_				
Motion Detection			Duration Time	105				
Camera Tamper			Buzzer duration time					
Video Loss			Buzzer duration time					
Intelligent Analysis							Refresh	Apply
Alarm In								
Abnormal Alarm								
Alarm Out								
S Network								
System								
	Ap	plv			Refresh			
Step 3 Click	141		to save settings.			to return to the pr	revious	settings

----End

8.3.1.2 IO Control Push

Procedure

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

Step 5 Enable the IO control push, as shown in Figure 8-17.

Figure 8-17 IO control push interface

📜 Channel				
Record				
🚊 Alarm	General	IO Control Push		
General Motion Detection Camera Tamper Video Loss		Enable Alarm In Mode	1 • NO •	
Intelligent Analysis Alarm In Abnormal Alarm Alarm Out		Disabled Items Push message to APP Email	-	
NetworkSystem				Refresh Apply

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

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

----End

8.3.2 Motion Detection

Procedure

Step 1 On the **System Setting** screen, choose **Alarm > Motion Detection** to access the motion detection interface, as shown in Figure 8-18.

		0					
👮 Channel							
Record							
🚊 Alarm	Motion	Detection					
General Motion Detection		Channel		[1]Channel01			
Carnera Tamper		Enable					
Video Loss			[]] Area	Schedule			
Intelligent Analysis Alarm In		Buzzer		•			
Abnormal Alarm		Push message	to APP				
Alarm Out		Pop up messa	ge to monitor	\bullet			
S Network		Full Screen		\bullet			
System		Email		$\bullet \blacksquare$			
		Alarm Out		\bullet			
		Alarm Record		$\bullet \blacksquare$			
						Сору	Apply

Figure 8-18 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 Email and alarm record.
- Step 5 Click Area to access the motion detection area setting, as shown in Figure 8-19.

Figure 8-19 Motion detection area interface

💻 Channel		
Record	Motion Detection	
🚊 Alarm		
General	Channel [1]Chan *	
Motion Detection	Enable	
Video Loss	D = 100 m = 100 m = 100	
Intelligent Analysis	Event Acti 🔛 Area 🛗 Schedule	
Alarm In	2019-07-06 03:00:50 Fri	
Abnormal Alarm <	- Aller - Aller	
S Network		
System		
🖵 Local		
	Sensitivity Medium *	
	Copy Apply	

- 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.

---End

8.3.3 Camera Tamper

Procedure

Step 1 On the Camera Tamper screen, choose Alarm > Camera Tamper to access the Camera

Tamper interface, as shown in Figure 8-20.



🛒 Channel		
Record		
🚊 Alarm	Camera Tamper	
General	Channel [1]Channel01 -	
Motion Detection Camera Tamper	Enable	
Video Loss	Event Acti 🛗 Schedule	
Intelligent Analysis	Buzzer	
Alarm In		
Abnormal Alarm	< Push message to APP	
Alarm Out	Pop up message to monitor	
S Network	Full Screen	
System	Email	
	Alarm Out	
	Alarm Record	
		Copy Apply

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 4-1 motion detection settings .

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

save the settings.

8.3.4 Video Loss

Procedure

Step 1 On the System Setting screen, choose Alarm > Video Loss to access the video loss

interface, as shown in Figure 8-21.

Figure 8-21 Video loss interface

🛒 Channel		
Record	Video Loss	
🚊 Alarm		
General	Channel [1]Chan *	
Motion Detection	Enable 💽	
Video Loss	Event Acti	
Intelligent Analysis		
Alarm In	Buzzer	
Abnormal Alarm	Alarm Out 📃	
S Network	Push message to APP	
System	Pop up message to monitor 🛑	
G Local	Email	
	Alarm Record	
	Copy Apply	

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 4-1 motion detection settings .

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

save the settings.

----End

8.3.5 Intelligent Analysis

Procedure

Please refer to chapter 6.5.1 video loss settings, interface displayed as shown in Figure 8-22.

T .	0 00	T / 11* /	1 .	·
Highre	8-77	Intelligent	analysis	interface
1 iguic	0 22	memgent	unu yong	mucruce

🛃 Channel												
Record												
🚊 Alarm	Р	erimeter	Single \	/irtual Fence	Double Virtua	Fences	Object Left	Object Removed	Signal Bad	Loiter	Mult	~
General	-		Channel		[10]Ch	annel10 -						
Motion Detection			Enable									
Camera Tamper				Area	E Schedule							
Video Loss												
Intelligent Analysis			Buzzer									
Alarm In			Push me	sage to APP								
Abnormal Alarm			Pop up m	essage to monitor								
Alarm Out			Full Scree	-)n								
S Network			Email									
System			Alarm Ou									
			Alarm Re	cord								
											Ар	ply

8.3.6 Alarm In

Procedure

Step 1 On the System Setting screen, choose Alarm > Alarm In to access the alarm in interface,

as shown in Figure 8-23.

T .'	0.00	4.1		• • •
Figure	8-23	Alarm	1n	interface

🛒 Channel		
Record	Alarm In	
🚊 Alarm		
General	Alarm In [1]Alarm In *	
Motion Detection	Enable	
Video Loss	Alarm Type N/O *	
Intelligent Analysis	Name Sensor 1	
Alarm In	Event Acti Schedule	
Abnormal Alarm		
S Network	Buzzer	
🧿 System	Alarm Out	
🖵 Local	Push message to APP	
	Pop up message to monitor	
	Email	
	Alarm Record	
	Apply	

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 Apply to save settings.

----End

8.3.7 Abnormal Alarm

Procedure

Step 1 On the System Setting screen, choose Alarm > Abnormal Alarm to access the

abnormal alarm interface, as shown in Figure 5-11.

Figure 8-24 Abnormal alarm interface

🛒 Channel							
Record							
🚊 Alarm	Abnorm	nal Alarm					
General		Enable	-				
Motion Detection							
Camera Tamper		Alarm Type			₲₽₽		
Video Loss				N	<u> </u>		
Intelligent Analysis							
Alarm In							
Abnormal Alarm		Buzzer					
Alarm Out		Push message to APP					
S Network		Pop up message to monitor					
System		Email					
		Alarm Out					
						Refresh	Apply

Step 2 Enable the button, tick alarm type.

Step 3 Set name, default is Sensor 1.

Step 4 Set event activity and schedule please refer to motion detection settings .

Step 5 Click Apply to save settings.

----End

Issue V4.5 (2020-09-07)

8.3.8 Alarm out

Set the alarm out, the device and cameras, as shown in Figure 8-25 and Figure 8-26.

Figure 8-25 Alarm out interface

💻 Channel						
Record						
🚊 Alarm	Alarm Out	Camera Alarm Out				
General Motion Detection		Alarm Out Name	[1]Alarm Out			
Video Loss		Valid signal	Close			
Intelligent Analysis Alarm In		Alarm Output Mode	Switch Mode			
Abnormal Alarm					Refresh	Apply
Alarm Out						
S Network						
🧿 System						

Figure 8-26 Camera alarm out interface

Alarm Out	Camera Alarm Out	
	Channel	[1]Channel01 ·
	Output ID	
	Name	
	Valid signal	Close *
	Alarm Output Mode	Switch Mode •
	Alarm Time(ms)(0:Continuous)	
		Refresh Apply

8.4 Network

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

8.4.1 Network

Procedure

Step 1 On the **System Setting** screen, choose **Network > Network** to access the network interface, as shown in Figure 8-27.

Figure 8-27 Network interface

👥 Channel					
Record	IP	PORT POE			
🖻 Alarm	-	FORT FOE			
S Network		DHCP			
Network		IP Address	192.168.32.241		
DDNS		Subnet Mask	255.255.0.0		
Email		Default Gateway	192.168.32.254		
Port Mapping	4				
P2P		Obtain DNS Automatically			
IP Filter		Preferred DNS Server	192.168.0.1		
802.1X		Altenate DNS Server	8.8.8		
SNMP					
Web Mode				Refresh	Apply
System					
🖵 Local					

Step 2 Click next to **IP** to enable or disable the function of automatically getting an IP

address. The function is enabled by default.

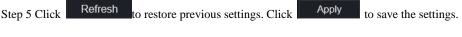
If the function is disabled, click input boxes next to **IP**, **Subnet mask**, and **Gateway** to set the parameters as required.

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.



----End

8.4.2 DDNS

Procedure

Step 1 Click **DDNS** in the network interface, choose **Network > DDNS** to access the DDNS

```
interface as shown in Figure 8-28.
```

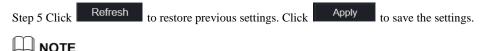
```
Figure 8-28 DDNS interface
```

📑 Channel					
Record	DDNS				
🖻 Alarm					
S Network		Enable			
Network		Protocol	no_ip *		
		Domain Name	dvr.ddns.net		
Email		User			
Port Mapping <		Password			
P2P			Test		
IP Filter				Refresh	Apply
802.1X SNMP					. 419.9
Web Mode					
System					
Local					

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.



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

8.4.3 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 8-29

-	Channel						
E	Record	Email					
Ē	Alarm						
G) Network		SMTP Server				
	Network		SMTP Server Port				
	DDNS		Username				
1.1			Password				
1	Port Mapping		Email Sender				
1	~ ?2P		Email for password reco				
1	P Filter		Alarm Receiver 1				
	302.1X SNMP		Alarm Receiver 2				
	Neb Mode		Alarm Receiver 3				
0	System		SSL Encryption	OFF 👻			
-	Local			Test			
					Refresh	Apply	

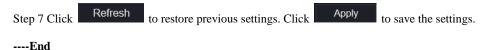
Step 2 Set SMTP server and SMTP server port manually.

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.



8.4.4 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 8-30.

Figure 8-30 Port Mapping interface

♀ Record ▲ Aarm ♥ Network DDNS Email Port Mapping Client Port B0 Data Port 554 Port Mapping Client Port 802.1X SNMP Web Mode	🚅 Channel			
Alarm Alarm Vetwork UPnP Enable UPnP Enab	Record	Port Mapping		
Network Mode Auto Network HTTP Port 80 DDNS Data Port 554 Port Mapping Client Port 30001 P2P Refresh Apply iP Filter 802.1X SNMP Web Mode Veb Mode Veb Mode	🚊 Alarm			
Network HTTP Port 80 DDNS Data Port 554 Email Data Port 554 Port Mapping Client Port 30001 P2P Refresh Apply 802.1X SNMP Web Mode Veb Mode	S Network	UPnP Enable	-	
DDNS HTTP Port 80 Email Data Port 554 Port Mapping Client Port 30001 P2P BP2 Refresh Apply Web Mode © System	Network	Mode	Auto *	
Email Data Port 554 Port Mapping Client Port 30001 IP Filter 802.1X SNMP Web Mode © System		HTTP Port		
P2P P2P Refresh Apply IP Filter 802.1X SNMP Web Mode \$\$ System		Data Port	554	
P2P Refresh Apply IP Filter 802.1X SNMP Web Mode Veb Mode	Port Mapping		30001	
IP Filter 802.1X SNMP Web Mode O System	P2P		Refresh	Apply
SNMP Web Mode © System			Tonsii	
Web Mode System	IP Filter			
🔁 System	802.1X			
	802.1X SNMP			
	802.1X SNMP			
	802.1X SNMP Web Mode			
	802.1X SNMP Web Mode			

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 Re	efresh to restore previ	ous settings. Click	Apply	to save the settings.
-----------------	-------------------------	---------------------	-------	-----------------------

Auto :system perform UPnP automatically.

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

----End

8.4.5 P2P

Procedure

Step 1 Click P2P in the network interface, choose Network > P2P to access the P2P interface, as shown in Figure 8-31.

Figure 8-31 P2P interface

👥 Channel				
Record	P2P			
🚊 Alarm				
S Network	Enable			
Network	Status	Offline		
DDNS				
Email		大学が出		
Port Mapping				
P2P				
IP Filter				
802.1X	App Name			
SNMP	- It is available on App Store and Goop	gle Play.	Refresh Apply	
Web Mode				
O System				
G Local				

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 Capture ADV is installed in mobile phone, run the APP and scan the UUID QR code to add then access the DVR when the device is online.

----End

8.4.6 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 8-32.

Figure 8-32 IP filter interface

💻 Channel					
Record	IP Filter				
🙋 Alarm					
S Network	IP Filter				
Network	Rule Type			Black *	
DDNS	Black List(Foll	owing network segments are f	orbidden)		
Email		Start IP	End IP	Edit	
Port Mapping <		ount in	LIGH	Eun	
P2P					
IP Filter					
802.1X					
SNMP Web Mode					
O System					
G Local					
				Refresh	Apply

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 window	s to set black list o	or white list, as sl	hown in 6.6.5.
Click	to delete the list.			
	Figure 8-33 Black	or white list interfac	xe	
	Add Ip Segment		×	
	Start IP			
	End IP			
		Cancel	OK	
Step 5 Set start II	P and end IP.			
Step 6 Click	Cancel to deny settings,	click OK	to save the s	settings.
Step 7 Click	Refresh to restore previou	is settings. Click	Apply to s	save the settings.

🛄 ΝΟΤΕ

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.

----End

8.4.7 802.1X

Procedure

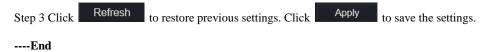
Step 1 Click 802.1X in the network interface, 802.1X interface is displayed, enable the button, as

shown in Figure 8-34.

💻 Channel		
Record	802.1X	
🖻 Alarm		
S Network	Enable	
Network	User	
DDNS	Password	
Email		
Port Mapping		Refresh Apply
P2P		
IP Filter		
802.1X		
SNMP		
Web Mode		
🗿 System		
🖵 Local		

Figure 8-34 802.1X interface

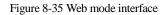
Step 2 Input the user and password of 802.1X authentication.



8.4.8 Web Mode

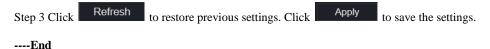
Step 1 Click Web Mode in the network interface, Web mode interface is displayed, as shown in

Figure 8-35.



Lannel		
Record	Web Mode	
🚊 Alarm		
S Network	нттря	
Network	Modifying the settings device will restart! Refresh Apply	
DDNS		
Email		
Port Mapping		
P2P		
IP Filter		
802.1X		
SNMP		
Web Mode		
😧 System		
G Local		

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



8.4.9 3G/4G

Step 1 Click **3G/4G** in the network interfac, as shown in Figure 8-36.

Figure 8-36 3G/4G interface

3G/4G				
	Enable			
	Status	Disconnected		
	Access Mode			
	APN			
	Dial Number			
	Username			
	Password			
	IP Address			
			Refresh	Apply

Step 2 The user plug the modem to DVR.

Step 3 Enable the 3G/4G.

Step 4 When the status is connection, user can set the access mode, AUTO is recommended.

Step 5 If choose other access mode, user should input the parameter correctly.

Step 6 Click	Refresh	to restore previous settings. Click	Apply	to save the settings.
End				

8.4.10 PPPOE

User can use PPPOE function to manage the NVR conveniently, as shown in Figure 8-37.

Figure 8-37 PPPOE interface

PPPOE				
	Enable	•		
	Username			
	Password			
	IP Address			
			Refresh	Apply

Step 1 Enable the PPPOE.

Step 2 Input the username and password.

Step 3 The IP address is obtained automatically.

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

Step 5 User use the IP address to access NVR immediately.

----End

8.5 System

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

8.5.1 Device Information

Procedure



Ø

Click on the navigation bar, the device information interface is displayed, as shown in Figure 8-38.

Figure 8-38 Device information interface

		0	
E Channel			
Record			
🚊 Alarm	Information		
S Network		Device ID	DVRJYBACJW62W171
😧 System		Device Name	Device
Information		Device Type	-
General		Model	
User		Firmware Version	v4.5.0817.0000.003.1.0.32.1
Security Center		U-boot Version	140509100010
Logs		Kernel Version	140408062A36
Maintenance		Kenner version	1404000022430
Auto Restart		HDD Number	1
		Channels Supported	24
		Alarm In	4
		Alarm Out	1
		Audio In	6
		Audio Out	1

Step 2 Set the device name according to Table 8-1.

Parameter	Description	Setting
Device ID	Unique device identifier used by the	[Setting method]
	platform to distinguish the devices.	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
Firmware version		modified.
HDD volume		
Channel support		
Alarm in		
Alarm out		
Audio in		
Audio out		

Table 8-1 Device parameters

----End

8.5.2 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 8-39.

Figure 8-39 Basic setting interface 🚅 Channel Record System Date And Time Time Zone 📋 Alarm S Network Device Name Device 🗿 System Output Resolution 1920x1080 -Language Information Refresh Apply User Password Maintenance Auto Restart G Local

Step 2 Set system.

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

Figure 8-40	System	interface
-------------	--------	-----------

🚅 Channel		
Record	System Date And Time Time Zone DST	
🚊 Alarm		
S Network	Device Name Device	
🧿 System	Output Resolution 1920x1080 -	
Information	Language English	
General		Refresh Apply
User <		
Password		
Logs		
Maintenance		
Auto Restart		
🖵 Local		

Step 3 Set date and time.

- 1. Synchronize the time from the NTP server.
- 2. Click NTP Sync button to enable synchronize time. The default value is enabling.

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

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

3. Set the device time manually, as shown in Figure 8-41.

4. Click NTP Sync button to disable synchronize time.

5. Async date and time interface

	8		
💻 Channel			
Record	System Date And Time Time Zone	TST	
🖻 Alarm			
S Network	Date Format DD/MM/YY		
🧿 System	Time Format 24H		
Information	NTP Sync		
General	NTP Server time.windows		
User <	Frequency of Checks. Mi 86400s		
Password	Time 05/07/2019 0	3:49:4:	
Logs			
Maintenance		Refresh	Apply
Auto Restart			
🖵 Local			

Figure 8-41 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 set	tting.				

Step 5 Set time zone.

Click **Time Zone** to enter the time zone setting interface, as shown in Figure 8-42. Time zone setting interface

Figure 8-42 Time zone

E Channel		
Record	System Date And Time Time Zone DST	
🖻 Alarm		
S Network	Time Zone (GMT+00:00) Dublin, Edinbu *	
🧿 System	Refresh Apply	
Information		
General		
User		
Password		
Logs		
Maintenance		
Auto Restart		
🖵 Local		

Select a time zone from the drop-down list.

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

Step 6 Set DST.

1. Click DST to enter the DST setting interface, click DST button to enable, as shown in Figure 8-43. The button is disable by default.

Figure 8-43 DST setting interface

💻 Channel								
Record	System	Date And Time	Time Zo	one DST				
🚊 Alarm	Gystein		Time Z					
S Network		Daylight Savings						
🗿 System		Start Time	Mar	Last one	Sun -	1:00		
Information		End Time	Oct	* Last one	Sun -	1:00		
General		Offset Time	1 Hour					
User							Refresh	Apply
Password								
Logs								
Maintenance								
Auto Restart								
🖵 Local								

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

Figure 8-44 Sync camera time

🛒 Channel		
Record		
🚊 Alarm	System Date And Time Time Zone DST Sync Camera Time	
S Network	Sync Camera Time	
System		
	Frequency of Checks. Minimum 10s 3600s	
Information		
General		Refresh Apply
User		
056		
Security Center		
Logs		
Maintenance		
Maintenance Auto Restart		

Enable sync camera time, the cameras of DVR management will be showing the same time. Set the frequency of checks(minimum 10s).

Step 7 Click	Apply	to save the DST setting. Click	Refresh	to return to previous

setting.

8.5.3 User

You can create new user accounts to manage the device.

8.5.3.1 Add User

Procedure

Step 1 On the **System Setting** screen, choose **System** >**User** to access the **User** interface, as shown in Figure 8-45.

Figure 8-45 User interface

_ C	Channel					
R R	Record	User	Adv.Set	ting		
<u>.</u> 1	Varm		Auv.Sei			
s v	letwork		ID	Username	Group	Operate
😳 s	System			admin	Super admin	۷
Info	rmation					
Gen	neral					
Use		<				
Pas	sword					
Log						
	ntenance					
Auto	o Restart					
Տ ԵՐ	ocal					Add

Step 2 Click Add to add a new user, as shown in Figure 8-46.

Figure 8-46 Add user

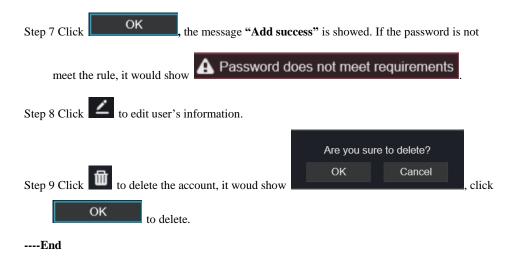
Add User			X
Username Password Confirm Password Group	Administrators	9 	
Change password reminder	Never		
 Remote Liva PTZ Playback Channel Management Device Management System Management 	♥ All Channel ♥ CH-1 ♥ CH-2 ♥ CH-3 ♥ CH-4 Remote Live		
		ок	Cancel

Step 3 Input username, password and confirm password.

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

Step 5 Assign the privilege to user.

Step 6 Select channels to manage.



8.5.3.2 Adv.Setting

Procedure

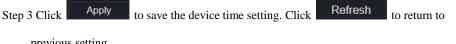
Step 1 On the System Setting screen, choose System >User > Adv. Setting to access interface,

as shown in Figure 8-47.

Figure 8-47 Adv. Setting interface

User	Adv.Setting					
	Password double authentication					
					Refresh	Apply

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



previous setting.

8.5.4 Security Center

8.5.4.1 Password

Procedure

Step 1 On the System Setting screen, choose System >Security Center to access password

interface, as shown in Figure 8-48.

Figure 8-48 Password interface

Password	Secure Email	Secure C	Question				
	Old Password			¥			
	New Password			Ø			
	Confirm Password						
						Refresh	Apply

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

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

Valid password range [6-32] characters.

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

 $Backslash \setminus cannot \ be \ used.$

----End

8.5.4.2 Secure Email

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

Password	Secure Email	Secure Question	
	Password		
	E-mail		
		Refresh Ap	ply

8.5.4.3 Secure Question

User can modify the password to login the NVR if user forgot the password and answer correctly the secure questions.

Password	Secure Email	Secure C	luestion			
	Password					
	Question one		The brand and model of your favorite car			
	Question one answer					
	Question two		Your favorite team			
	Question two answer					
	Question three		Your favorite city			
	Question three answe	er				
	It least 1 characters for the point of the p				Refresh	Apply

----End

8.5.5 Logs

8.5.5.1 Logs

Procedure

Step 1 On the System Setting screen, choose System >Logs to access logs interface, as shown in

Figure 8-49.

Figure 8-49 Logs interface

L Channel						
Record						
ä Alarm	Logs Event					
S Network						
System	Start 08/09/20	120 06 18:21 End 09/09/2020 06	18:21 Type Operat	ion Log 🔹	Search Export	
Information	ID	Start Time	Channel	Log Type	Information	
General		09/09/2020 05:25:27	Channel12	Online	[admin] 127.0.0.1 001c27110d22	
User		09/09/2020 05:24:48	Channel11	Online	[admin] 127.0.0.1 001c271207bf	
Security Center		09/09/2020 05:18:53	Channel12	Online	[admin] 127.0.0.1 001c27110d22	
		09/09/2020 05:18:53	Channel11	Online	[admin] 127.0.0.1 001c271207bf	
		09/09/2020 05:05:23	Channel12	Online	[admin] 127.0.0.1 001c27110d22	
Maintenance		09/09/2020 05:03:37	Channel12	Online	[admin] 127.0.0.1 001c27110d22	
Auto Restart		09/09/2020 05:03:35	Channel11	Online	[admin] 127.0.0.1 001c271207bf	
		09/09/2020 05:02:02	Channel11	Online	[admin] 127.0.0.1 001c271207bf	
		09/09/2020 05:02:01	Channel12	Online	[admin] 127.0.0.1 001c27110d22	
		09/09/2020 05:02:00	Channel19	Online	[admin] 127.0.0.1 001c270e46aa	
		09/09/2020 04:58:16	Channel10	Online	[admin] 127.0.0.1 001c27fff333	
		09/09/2020 04:40:06	Channel12	Online	[admin] 127.0.0.1 001c27110d22	
		09/09/2020 04:29:23		Logout	[admin] 192.168.0.254 logout	
		4 >>1			Every page show 20	

Step 2 Set start and end time from calendar.

Step 3 Select log type from drop-down list.

Step 4 Click Search to acquire log information.

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

----End

8.5.5.2 Event

Procedure

Step 6 On the System Setting screen, choose System >Logs > Event to access logs interface, as

shown in Figure 8-50.

Figure 8-50 Event interface

💻 Channel						
Record						
🚊 Alarm	Logs	Event				
S Network						
System		Start 07/09/2020 06:18:2	1 End 09/09/2020 06:18:21	Type All *		Search Export
Information		ID	Start Time	Channel	Log Type	Information
General			08/09/2020 03:20:32	Channel09	Video Loss	Channel09
User			08/09/2020 03:20:32	Channel08	Video Loss	Channel08
Security Center			08/09/2020 03:20:32	Channel22	Video Loss	Channel22
			08/09/2020 03:20:32	Channel18	Video Loss	Channel18
Maintenance			08/09/2020 03:20:23	Channel18	Video Loss	Channel18
			08/09/2020 03:20:23	Channel06	Video Loss	Channel06
Auto Restart			08/09/2020 03:20:23	Channel22	Video Loss	Channel22
			08/09/2020 03:20:22	Channel15	Video Loss	Channel15
			08/09/2020 03:20:22	Channel12	Video Loss	Channel12
			08/09/2020 03:20:22	Channel17	Video Loss	Channel17
			08/09/2020 03:20:20	Channel11	Video Loss	Channel11
			08/09/2020 03:20:18	Channel09	Video Loss	Channel09
			08/09/2020 03:20:17	Channel10	Video Loss	Channel10
		I<< 1_/45 >>I				Every page show 20 -

Step 7 Set start and end time from calendar.Step 8 Select event type from drop-down list.Step 9 Click Search to acquire log information.Step 10 Click Export to export the event logs.----End

8.5.6 Maintenance

Procedure

Step 1 On the System Setting screen, choose System >Maintenance to access maintenance

interface, as shown in Figure 8-51.

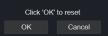
Mainte	enance	Figure	5-51 Walltena	ice interface			
		â	0	â			
	Reboot	Update	Reset	Cloud Update			
Step 2 Cli	ck Reboot , t	he pop-up mes	ssage would sh	now you, click	ОК	to reboot.	

Figure 8-51 Maintenance interface

choose software from

shows to you, click

Step 3 Click **Update**, the message shows specific location to update.



Update

Please select upgrade file

Step 4 Click Reset, the pop-up message

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.

----End

8.5.7 Auto Restart

OK

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 8-52.

Figure 8-52 Auto restart

🚅 Channel		
Record	Auto Restart	
🖻 Alarm		
S Network	Enable 📃	
System	Restart Time Per Day * 0:00 *	
Information	Refresh Apply	
General		
User <		
Password		
Logs		
Maintenance		
Auto Restart		
🖵 Local		

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



8.6 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 8-53. Figure 8-53 Local interface

💻 Channel	
Record	Download Config
🚊 Alarm	
S Network	Image download path C:\Users\Public\Docur Browse
System	Video download path C:\Users\Public\Docur Browse
🖵 Local	Refresh Apply

Step 2 Enter the image download path.

Step 3 Enter the record download path.

Step 4 Click	Refresh	to return the previou	s settings.	Click	Apply	to save the
settings.						
End						