Libert	Y ™	L3NV	RP	OE Ser	ies Al	NVRs
	4	Liberty		/ = =		
	Liberty	-	7			
	Liberty		1			
32 Libe	erty	4040				

User Manual for: L3NVR4POE, L3NVR8POE, L3NVR16POE, L3NVR3216POE



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 several models. The appearance and function of the products are subject to the actual products.

Any loss caused by failure to follow the instructions in this document is the responsibility of the user.

This document will be updated in real time according to the laws and regulations of the relevant region. For details, please refer to the product's paper, electronic CD, QR code or official website. If the paper and electronic files are inconsistent, please refer to the electronic file as.

The company reserves the right to modify any information in this document at any time. The revised content will be added to the new version of this document without prior notice. This document may contain technical inaccuracies, or inconsistencies with product features and operations, or typographical errors, which are subject to the company's final interpretation.

If the obtained PDF document cannot be opened, please use the latest version or the most mainstream reading tool.

Network Security Advice

Required measures to ensure basic network security of equipment:

Modify the password regularly and set a strong password.

Devices that do not change the password regularly 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 NVR, DVR and IP cameras should be updated to the latest version to ensure the latest features and security of the device.

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

1. Change your password regularly

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

2. Modify the default HTTP and data ports

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

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

3. Use HTTPS/SSL encryption

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

4. Enable IP filtering

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

5. Change the ONVIF password

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

6. Only forward the ports that must be used

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

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

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

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

8. Restrict the permissions of the ordinary account

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

UPNP

When the UPnP protocol is enabled, the router will automatically map the intranet ports. Functionally, this is user-friendly, but it causes the system to automatically forward the data of the corresponding port, causing the data that should be restricted to be stolen by others. If you have manually opened HTTP and TCP port mappings on your router, we strongly recommend that you turn this feature off. In actual usage scenarios, we strongly recommend that you do not turn this feature on.

SNMP

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

Multicast

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

v

12. Check logs

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

Physically protect your device

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

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

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

Network isolation between NVR and IP cameras

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

About This Document

Purpose

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

Symbol Conventions

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

Symbol	Description
	It's for warning when a hazard or a hazardous condition is likely to be life-threatening.
	Alerts you to a medium or low risk hazard that, if not avoided, could result in moderate or minor injury.
	Alerts you to a potentially hazardous situation that, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results.
G ≕" 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 NVR device does not support wall mounting.

Do not place and install the device in direct sunlight or near heat-generating equipment.

Do not install the device in a place subject to high humidity, dust or soot.

Please keep the equipment installed horizontally or install the equipment in a stable place, taking care to prevent the product from falling.

Do not drop or spill liquid into the device and ensure that no liquid-filled items are placed on the device to prevent liquid from flowing into the device.

Install the device in a well-ventilated area, and do not block the ventilation openings of the device.

Use the device only within the rated input and output range.

Do not disassemble the device at will.

Please transport, use and store the device within the permissible humidity and temperature range.

Power Requirement

Be sure to use the specified manufacturer's model battery, otherwise there is a danger of explosion!

Be sure to use the battery as required, otherwise there is a danger of the battery catching fire, exploding or burning!

Only use the same model of battery when replacing the battery!

Be sure to dispose of the used battery as the instruction of battery!

Be sure to use the power adapter that meets standard with the device, otherwise the personal injury or equipment damage caused by the user will be borne by the user.

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

Important Statement

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

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

Contents

Legal Noticeii
Network Security Adviceiv
About This Document
Purposevii
Symbol Conventions
Safety instructions
Requirementsviii
Power Requirementviii
Important Statementix
Contents
1 Preface
1.1 Product Description1
1.2 Product Features
1.2.1 Cloud Upgrade1
1.2.2 Real-time Monitoring2
1.2.3 Playback
1.2.4 User Management
1.2.5 Storage Function
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 Control4
1.2.12 Accessibility
2 Product Structure

2.1 Front Panel	
2.2 Back Panel	5
2.3 Important Notes	
2.4 About This User Manual	
2.5 Installation Environment and Precautions	
3 Install device	
3.1 Process	
3.2 Unpacking Inspection	14
3.3 Install Hard Disk	
3.3.1 Install One or Two Hard disks	
4 Basic Operations	
4.1 Power on the Device	
4.2 Activation	
4.3 Power off the Device	
4.4 Login to the System	
5 Wizard	
6 Quick Navigation	
6 Quick Navigation	
6.1 Quick Bar	
6.1 Quick Bar6.2 Real Time Video Bar	
6.1 Quick Bar6.2 Real Time Video Bar6.3 Playback	
 6.1 Quick Bar 6.2 Real Time Video Bar 6.3 Playback 6.3.1 Time Search 	35 39 41 43 44
 6.1 Quick Bar 6.2 Real Time Video Bar 6.3 Playback 6.3.1 Time Search 6.3.2 Picture Grid 	35 39 41 43 44 44 46
 6.1 Quick Bar 6.2 Real Time Video Bar 6.3 Playback 6.3.1 Time Search 6.3.2 Picture Grid 6.3.3 Event Recording 	35 39 41 43 44 44 46 48
 6.1 Quick Bar 6.2 Real Time Video Bar 6.3 Playback 6.3.1 Time Search 6.3.2 Picture Grid 6.3.3 Event Recording 6.3.4 Backup List 	35 39 41 43 44 44 44 46 48 49
 6.1 Quick Bar 6.2 Real Time Video Bar 6.3 Playback 6.3.1 Time Search 6.3.2 Picture Grid 6.3.3 Event Recording 6.3.4 Backup List 6.4 AI Recognition (Only for Some Models) 	35 39 41 43 44 44 46 46 48 49 49
 6.1 Quick Bar 6.2 Real Time Video Bar 6.3 Playback 6.3.1 Time Search 6.3.2 Picture Grid 6.3.3 Event Recording 6.3.4 Backup List 6.4 AI Recognition (Only for Some Models) 6.4.1 Real Time Comparison 	35 39 41 43 44 44 46 46 48 49 49 49
 6.1 Quick Bar 6.2 Real Time Video Bar 6.3 Playback 6.3.1 Time Search 6.3.2 Picture Grid 6.3.3 Event Recording 6.3.4 Backup List 6.4 AI Recognition (Only for Some Models) 6.4.1 Real Time Comparison 6.4.1.1 Human Face 	35 39 41 43 44 44 46 48 49 49 49 49 50
 6.1 Quick Bar 6.2 Real Time Video Bar 6.3 Playback 6.3.1 Time Search 6.3.2 Picture Grid 6.3.2 Picture Grid 6.3.3 Event Recording 6.3.4 Backup List 6.4 AI Recognition (Only for Some Models) 6.4.1 Real Time Comparison 6.4.1.1 Human Face 6.4.1.2 Vehicle and Full Body 	35 39 41 43 43 44 46 48 49 49 49 49 50 50 51
 6.1 Quick Bar 6.2 Real Time Video Bar 6.3 Playback 6.3.1 Time Search 6.3.2 Picture Grid 6.3.2 Picture Grid 6.3.3 Event Recording 6.3.4 Backup List 6.4 AI Recognition (Only for Some Models) 6.4.1 Real Time Comparison 6.4.1.1 Human Face 6.4.1.2 Vehicle and Full Body 6.4.2 Smart Search 	35 39 41 43 44 44 46 48 49 49 49 49 50 50 51 52

6.4.3 Archives Library	
6.4.3.1 Face Library	56
6.4.4 Comparison Configuration	
6.4.4.1 Face Comparison	
6.4.5 Attendance Management	59
6.5 Channel Information	
6.6 Main Menu	
7 UI System Setting	64
7.1 Channel Management	64
7.1.1 Camera	
7.1.1.1 Add Camera Automatically	
7.1.1.2 Add Camera Manually	67
7.1.1.3 Add Camera by RSTP	
7.1.1.4 Delete Camera	
7.1.1.5 Operate Camera	69
7.1.2 Encode Parameter	
7.1.3 Sensor Setting	
7.1.4 OSD Settings	73
7.1.5 Privacy Zone	
7.1.6 ROI	75
7.1.7 Microphone	76
7.1.8 Smart	
7.1.8.1 AI Multiobject	
7.1.9 Intelligent Tracking	
7.2 Record Setting	
7.2.1 Record Schedule	
7.2.2 Disk	
7.2.3 RAID (Only for Some Models)	
7.2.4 Storage Mode	
7.2.5 S.M.A.R.T	
7.2.5.1 S.M.A.R.T	
7.2.5.2 WDDA	

7.2.6 Disk Detection	90
7.2.7 Disk Calculation	92
7.2.8 FTP	93
7.3 Alarm Management	95
7.3.1 General	95
7.3.1.1 General	95
7.3.1.2 IO control push	
7.3.2 Motion Detection	
7.3.3 Video Loss	99
7.3.4 Intelligent Analysis	
7.3.5 Alarm In	
7.3.6 Abnormal Alarm	105
7.3.7 Alarm Out	106
7.3.7.1 Alarm Out	
7.3.7.2 Camera Alarm out	107
7.3.8 Local Intelligent Analysis	
7.3.8.1 General	
7.3.8.1 General 7.3.8.2 Intrusion	109
	109 110
7.3.8.2 Intrusion	
7.3.8.2 Intrusion 7.4 Network Management	109 110 113 114
7.3.8.2 Intrusion 7.4 Network Management 7.4.1 Network	
7.3.8.2 Intrusion 7.4 Network Management 7.4.1 Network 7.4.1.1 IP	
7.3.8.2 Intrusion 7.4 Network Management 7.4.1 Network 7.4.1.1 IP 7.4.1.2 Port	
7.3.8.2 Intrusion 7.4 Network Management 7.4.1 Network 7.4.1.1 IP 7.4.1.2 Port 7.4.1.3 POE	
7.3.8.2 Intrusion 7.4 Network Management 7.4.1 Network 7.4.1.1 IP 7.4.1.2 Port 7.4.1.3 POE 7.4.2 802.1 X	
7.3.8.2 Intrusion 7.4 Network Management 7.4.1 Network 7.4.1.1 IP 7.4.1.2 Port 7.4.1.3 POE 7.4.2 802.1 X 7.4.3 DDNS	
7.3.8.2 Intrusion 7.4 Network Management 7.4.1 Network 7.4.1.1 IP 7.4.1.2 Port 7.4.1.3 POE 7.4.2 802.1 X 7.4.4 Port Mapping	
7.3.8.2 Intrusion 7.4 Network Management 7.4.1 Network 7.4.1.1 IP 7.4.1.2 Port 7.4.1.3 POE 7.4.2 802.1 X 7.4.3 DDNS 7.4.4 Port Mapping 7.4.1 Port Mapping	
7.3.8.2 Intrusion 7.4 Network Management 7.4.1 Network 7.4.1 Network 7.4.1.1 IP 7.4.1.2 Port 7.4.1.3 POE 7.4.2 802.1 X 7.4.4 Dort Mapping 7.4.1 Port Mapping 7.4.2 NAT Port	
7.3.8.2 Intrusion 7.4 Network Management 7.4.1 Network 7.4.1 IP 7.4.1.2 Port 7.4.1.3 POE 7.4.2 802.1 X 7.4.3 DDNS 7.4.4 Port Mapping 7.4.5 Email	

7.4.9 POE Status	
7.4.10 Network Traffic	
7.4.11 Platform Access	
7.5 System Management	
7.5.1 Information	
7.5.2 General	
7.5.2.1 System	
7.5.2.2 Date and Time	
7.5.2.3 Time Zone	
7.5.2.4 DST	
7.5.2.5 Sync Camera Time	
7.5.3 User Account	
7.5.3.1 User	
7.5.3.2 Advance Setting	
7.5.3.3 App Verification	141
7.5.4 Security Center	142
7.5.4.1 Password	
7.5.4.2 Pattern Unlock	
7.5.4.3 Secure Email	
7.5.4.4 Secure Question	
7.5.5 Layout	
7.5.6 Auxiliary Screen (Only for Some Models)	
7.5.7 Logs	
7.5.7.1 System Log	
7.5.7.2 Event Log	151
7.5.8 Maintenance	
7.5.9 Auto Reboot	
WEB Quick Start	
8.1 Activation	
8.2 Login and Logout	
8.3 Browsing Videos	
8.3.1 Browsing Real-Time Videos	

8.3.2 Live Video	164
8.3.3 Channel Operation	
8.3.4 PTZ Control and Setting	
8.3.5 Sensor Setting	
8.3.6 Layout	
8.4 Playback	
8.4.1 Video Playback	171
8.5 Alarm Search	173
8.5.1 Channel Alarm	173
8.6 Attendance	175
8.6.1 Attendance Data	
8.6.2 Attendance Management	176
8.7 AI Recognition	
8.7.1 Real Time Comparison	181
8.7.1.1 Human Face	
8.7.1.2 Vehicle and Full Body	
8.7.1.3 Real Time Body Temperature Filter	
8.7.2 Smart Search	
8.7.2.1 Human Face Search	
8.7.2.2 Full Body Search	
8.7.2.3 Vehicle Search	
8.7.3 Archives Library	
8.7.3.1 Face Library	186
8.7.4 Comparison Configuration	186
9 System Setting	
9.1 Channel	191
9.1.1 Camera	
9.1.1.1 Protocol Management	194
9.1.2 Encode	195
9.1.3 Sensor Setting	
9.1.4 OSD	197
9.1.5 Privacy Zone	

9.1.6 ROI	199
9.1.7 Microphone	
9.1.8 Smart	
9.1.9 Intelligent Tracking (Only for Some Models)	201
9.2 Record	201
9.2.1 Record Schedule	202
9.2.2 Disk	
9.2.3 Storage Mode	
9.2.4 RAID (Only for Some Models)	
9.2.5 S.M.A.R.T	
9.2.6 Disk Calculation	
9.2.7 FTP	
9.3 Alarm	209
9.3.1 General	
9.3.1.1 General	210
9.3.1.2 IO Control Push	
9.3.2 Motion Detection	
9.3.3 Video Loss	213
9.3.4 Intelligent Analysis (Only for Some Models)	
9.3.5 Alarm In	
9.3.6 Abnormal Alarm	216
9.3.7 Alarm out	217
9.4 Network	
9.4.1 Network	
9.4.2 DDNS	
9.4.3 Email	
9.4.4 Port Mapping	222
9.4.4.1 Port Mapping	
9.4.4.2 NAT port	
9.4.5 P2P	
9.4.6 IP Filter	224
9.4.7 802.1X	

xvi

9.4.8 SNMP
9.4.9 Web Mode
9.4.10 POE Status
9.4.11 Platform Access
9.5 System
9.5.1 Device Information
9.5.2 General
9.5.3 User Account
9.5.3.1 Add User
9.5.3.2 Adv.Setting
9.5.3.3 App Verification
9.5.4 Security Center
9.5.4.1 Password
9.5.4.2 Secure Email
9.5.4.3 Secure Question
9.5.5 Logs
9.5.5.1 System Logs241
9.5.5.2 Event
9.5.6 Maintenance
9.5.7 Auto Reboot
9.6 Local (Supplied for IE Browser)

1 Preface

1.1 Product Description

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

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

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

1.2 Product Features

1.2.1 Cloud Upgrade

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

1.2.2 Real-time Monitoring

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

1.2.3 Playback

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

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

The exact time when the event occurred can be displayed during playback of the recording. You can select any area of the screen for partial magnification.

1.2.4 User Management

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

1.2.5 Storage Function

According to the user's configuration and policies (alarm or time settings), the corresponding audio and video data transmitted by the remote device is stored in the NVR device. For details, please refer to 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 NVR device is transmitted to the network terminal for decompression and reproduction. The device supports 8 (or 4) simultaneous online users to perform streaming operations. The audio and video data is transmitted using protocols such as HTTP (Hyper Text Transfer Protocol), TCP (Transmission Control Protocol), UDF (User Datagram Protocol), MULTICAST, RTP (Real-time Transport Protocol), and RTCP (Real Time Streaming Protocol). Use SNMP (Simple Network Management Protocol) for some alarm data or information Support WEB mode access system, applied to WAN, LAN environment.

1.2.8 Split Screen

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

1.2.9 Recording Function

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

1.2.10 Backup Function

Support USB2.0 and eSATA video backup.

1.2.11 External Device Control

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

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

1.2.12 Accessibility

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

Alteration Line) system.

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

Supports for logging recording.

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

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



4

For other functions, please see the following text.

2 Product Structure

2.1 Front Panel

Figure 2-1 One disk/four disks model

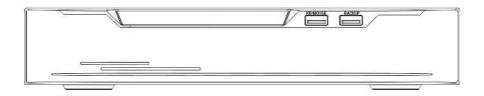


Table 2-1 Front panel function

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

2.2 Back Panel

Figure 2-2 L3NVR4POE

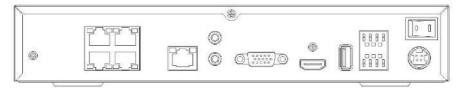


Figure 2-3 L3NVR8POE

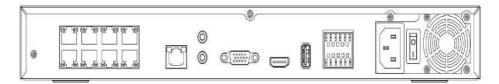
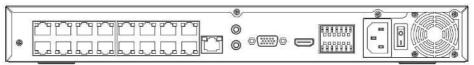


Table 2-2 Real panel function

Port	Description
POE	POE network interfaces
LAN	RJ 45 10/100/1000 Mbps adaptive Ethernet interface
AUDIO OUT / AUDIO IN	Audio output / Audio input
VGA	Video output interface
HDMI	
Alarm I/O	Alarm input/Alarm output
-	GND
DC48V	Connected to an external power adapter

Figure 2-4 L3NVR16POE





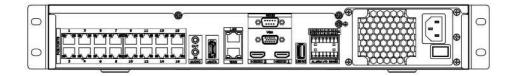
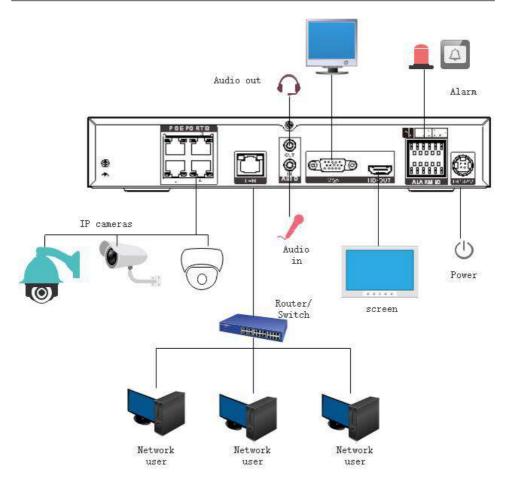
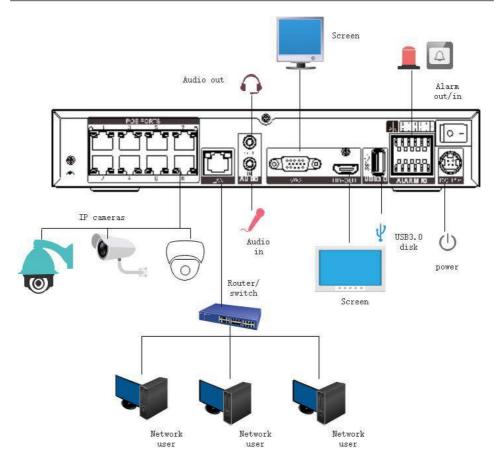
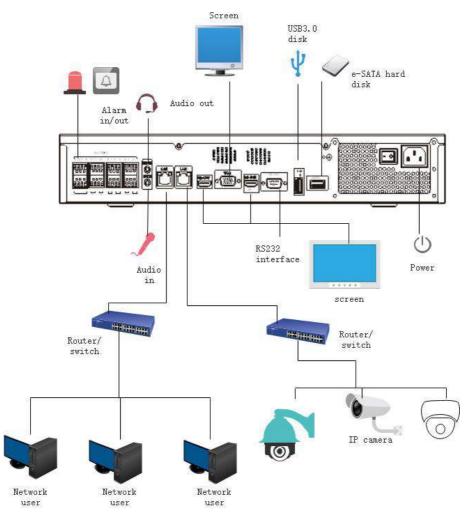


Table 2-3 Real panel function

Port	Description
POE	POE network interfaces
LAN	RJ 45 10/100/1000 Mbps adaptive Ethernet interface
AUDIO OUT / AUDIO IN	Audio output / Audio input
VGA	Video output interface
HDMI	
USB 3.0	Only connected to 3.0 U disk
Alarm I/O	Alarm input/Alarm output
÷	GND
DC48V	Connected to an external power adapter







2.3 Important Notes

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

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

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

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

We are not liable for any video data loss caused by improper installation, configuration, operation, and hard disk errors.

All images in the document are for reference only, please subject to the actual products.

2.4 About This User Manual

Please note the following points before using this user manual:

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

The information in this user manual applies to the full series NVR, NVR as an example for description.

Read this user manual carefully before using the NVR and follow the methods described in this manual when using the NVR.

If you have any doubts when using the NVR, contact your product seller.

As our products are subject to continuous improvement, we reserve the right to modify product manual, without notice and without incurring any obligation.

2.5 Installation Environment and Precautions

Installation environment

Table 2-10 defines the installation environment of the NVR.

Item	Description
Electromagnetism	The NVR conforms to national standards of electromagnetic radiation and does not cause harm to the human body.
Temperature	-10°C to +45°C
Humidity	20% to 80%
Atmospheric pressure	86 Kpa to 106 Kpa
Power supply	DC 12V, DC 48V 2A(1 HDD) or AC110/ 220V 4A(2 HDDs or more), please refer to actual products.
Power consumption	<15W (not including the hard disk)

Table 2-4 Installation environment

Installation precautions

Note the following points when installing and operating the NVR:

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

Install the NVR horizontally.

Avoid direct sunlight on the NVR and keep away from any heat sources and hot environments.

Connect the NVR to other devices correctly during installation.

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

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

You'd better use high-quality hard disk so that the NVR can work stably and reliably. Please

refer to chapter 10 Disk Compatibility

Other precautions

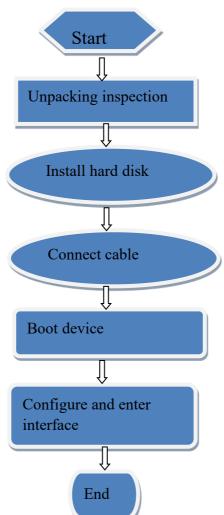
Clean the NVR with a piece of soft and dry cloth. Do not use chemical solvents. Do not place objects on the NVR.

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

Series of NVR

3 Install device

3.1 Process



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

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

- Step 3 Connect the device cable.
- Step 4 Make sure the device is properly connected. Power up and turn on the device.
- Step 5 Configure the initial parameters of the device. The boot wizard contains network configuration, add cameras, and manage disks. For details, please refer to the chapter of Wizard .

3.2 Unpacking Inspection

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

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

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 need to provide the serial number of the product on the label.
3	Cabinet	Package	Is there any obvious damage
		Data cable, power cable, fan power supply, and motherboard	Is the connection loose? NOTE If it is loose, please contact the company's after-sales personnel.

T 1 1 A 1	T T			
Table 3-1	Uni	nackino	1115	nection
raole 5	. 011	Jacking	, 1110	peenon

3.3 Install Hard Disk

Check if the hard disk is installed during the first installation. Please use the recommended hard disk model. For more details, see *10 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.

Choose the hard disk capacity according to the recording requirements.

3.3.1 Install One or Two Hard disks

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

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

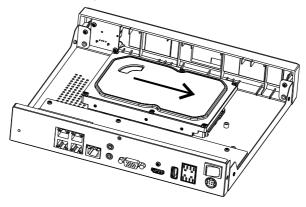
and secure it to the screw holes, as show in Figure 3-1..

Figure 3-2 Installing the hard disk screws

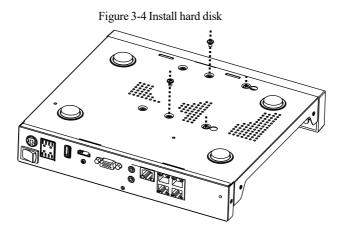


Step 3 Pass the screws through the holes on the base and put the hard disk in place, as shown in Figure 3-2.

Figure 3-3 Install hard disk



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



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

4 Basic Operations

4.1 Power on the Device



Ensure that the NVR is correctly connected to a power supply, and a display is correctly connected to the high-definition multimedia interface (HDMI) or video graphics array (VGA) port of the NVR before power-on.

In some environments, abnormal power supply may cause the failure of the NVR to work properly and even damage the NVR in severe cases. It is recommended to use a regulated power supply to power up the NVR in such environments.

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

Figure 4-1 Real-time video screen

Liberty	Activation			Liberty
	Language	English		
	Usemame	admin		
	Enter a new password			
Liberty	Confirm the new password			
	Enter channel default password			Liberty
	- Valid password range [6-32]	characters.		
	- At least 2 kinds of numbers lo	worcase,uppercase	or special.	
	- Only these special characters	are supported 18#\$	\$*:=_%&~,	
	- Channel default password im	t is not empty		
				Liberty
iberty		3 K		

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

NVR. Format the hard disk.

The hard disk is damaged.

4.2 Activation

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

Basic Operations

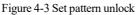
Figure 4-2 Activation

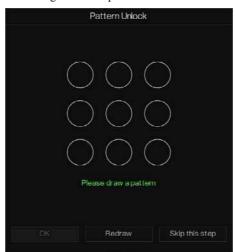
Activa	ation	
Language	English	~
Username	admin	
Enter a new password		
Confirm the new password		
Enter channel default password		
- Valid password range [6-32] ch	aracters.	
- At least 2 kinds of numbers,low	ercase,uppercase or	special.
- Only these special characters a	re supported !@#\$*+	=_%&"`.
- Channel default password limit	is not empty	
Of		

Table 4-1 Description of activation

Name	Description
Username	The default username is admin, and "admin" is super administrator.
Password	Valid password range 6-32 characters.
Confirm password	At least 2 kinds of numbers, lower case, upper case or special characters contained.
	Only these special characters are supported ! @#&*+=- %&"`(),/'.:;<>?^ ~[]{}. Channel default password limit is not empty.
Channel password	The NVR channel connection password is the camera login password.

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





After setting pattern unlock, the system default login will be pattern unlock login. If pattern unlock is not set, you need enter the password to log in.

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

Allow the Mailbox to receive verification code. The password will be reset when you forget it, as shown in Figure 4-4.

Basic Operations

Figure 4-4 Set Email

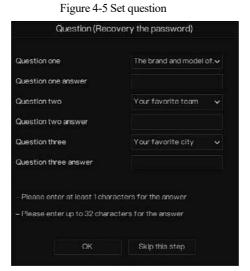
Email for re	overy user password		
Email Address			
04			
OK	Skip this step		

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 get the temporary password to login to the device.

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

Set the secure questions to create a new password in case the user forgets the password.



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

Questions one can be set: Your favorite animal

Company name of your first job

The name of the first boy/girl you like

The worst security question you have ever seen

The funniest worst design you have ever seen

Your favorite team

Your favorite city

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

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

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

4.3 Power off the Device

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

4.4 Login to the System

Step 1 Login to the device (two modes to login). The pattern unlock is as shown in Figure 4-6. Figure 4-6 Pattern unlock login page



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

3)	English	×
1	admin	~
3	Password	
	Login	

Figure 4-7 Password login page

Step 3 Input the username and password.

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, the seller will send you the

verification code to create a new password.

2. Answer the secure question to create new password.

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

in Figure 4-8

Basic Operations

Figure 4-8 Modify default password

	Modify default password	
New password Confirm password		
	Modify password	
– Valid password range (6-32) characters	
	bers,lowercase,uppercase or special character conta	ined.
- Only special character	s are supported 1@#\$*+=	

----End

5 Wizard

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



Figure 5-1 Wizard

Figure 5-2 Wizard of network

DHCP	
IP Address	192 . 168 . 0 . 121
Subnet Mask	255 . 255 . 255 . 0
Default Gateway	192 . 168 . 0 . 1
Obtain DNS Automatically	0
Preferred DNS Server	
Alternate DNS Server	
Enable Port Mapping	
Mode	Auto 🗸
HTTP Port	
HTTPS Port	
RTSP Port	
Control Port	

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

Table 5-1	Network	parameter
-----------	---------	-----------

Parameter	Description	Configuration
DHCP	Enable DHCP, the device will obtain the IP address from the DHCP server.	[Setting method] Enable
IP Address	Set the IP of device when DHCP is disable	[Setting method] Manual
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, he must set that	[Setting method] Manual [Default value] 192.168.0.1
Obtain DNS	N/A	[Setting method]

Parameter	Description	Configuration
automatically		Enable
Preferred DNS Server	N/A	[Setting method] Manual [Default value] 192.168.0.1
Alternate DNS Server	N/A	[Setting method] Manual [Default value] 8.8.8.8
Enable Port Mapping	Enable to set the ports of HTTP, HTTPS, RSTP, Control. Auto: device to obtain Web port, data port and client port. Manual: user set the port manually.	[Setting method] Choose type from drop-down list [Default value] Auto
HTTP Port	N/A	[Setting method]
HTTPS Port	N/A	When Port Mapping
RTSP Port	N/A	is manual, you need to set these.
Control Port	N/A	

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

Figure 5-3 Wizard of date and time

te And Time Time Zone	e DST
Date Format	DD/MM/YY hhmmss 🗸 🗸
Time Format	24H 🗸
Enable NTP	0
NTP Server	time.windows.com 🗸
Sync Time Frequency (sec)	86400
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 5-4.

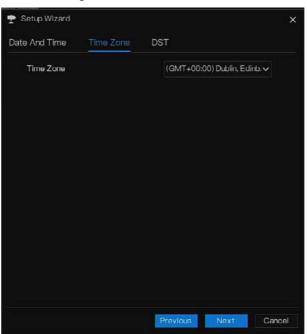


Figure 5-4 Wizard of time zone

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 5-5.

Figure 5-5 Wizard of adding camera

	Channel	6 ().	P	Model	Protocol	Oper	ate
0	• CHI	169.25	4:10:2:3000.		Privata	۷	۵
	© CHS						
	© CH3					+	
	CH4						
			Delete	AddD	Devices	Stop Sear	rch(13s)
0		P	Model	Protocol	Firmw	are Versio	on
۵	192.168.1	7,116:4433		ONVIF			
n	192.168.7	.200:8888		ONVIF			
D	192,168	3.7.98:80		ONVIF			
0	192.168	3.7.95:80		ONVIF			
Use	ername	admin	Pa	ssword		5	Add

The details of adding camera please refer to *chapter 7.1*.

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

31

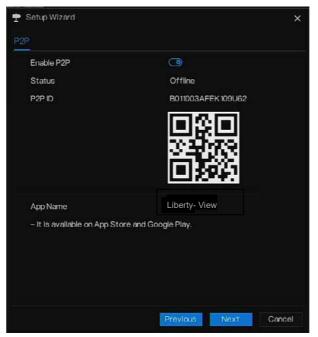
	Disk	Capacity	Used	SN	Disk Model	Status
	Disk1	12 TB	149 GB	5QJ8VD9B		Normal
D	Disk2	3 TB	1583 GB	Z6A0RABD		Normal
						Format

Figure 5-6 Wizard of disk

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

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

Figure 5-7 P2P



- Step 8 Enable the P2P, user can use mobile devices to manage the NVR by scanning the P2P ID, if the mobile phone has loaded the Liberty-View (search the APP at App Store or Google Play).
- Step 9 Click Next to enter the wizard of resolution, as shown in Figure 5-8. Choose resolution from drop-down list. (the highest resolution is 3840*2160)

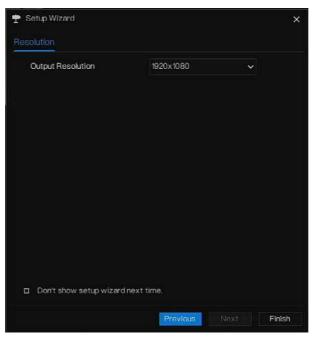


Figure 5-8 Wizard of resolution

Step 10 Click **Finish** to end the wizard, tick the **Don't show setup wizard next time**, it would not show at next time. Reopen wizard at **system > User > Advance setting**.

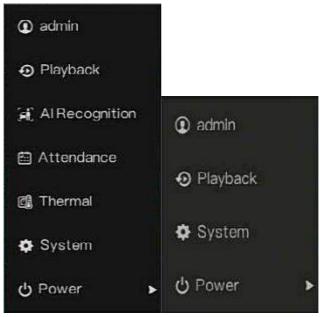
6 Quick Navigation

6.1 Quick Bar

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

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





In the middle of NVR floating menu bar, the video tool bar provides video window switching, auto SEQ, volume, playback, and channel information, as shown in Figure 6-2.

Figure 6-2 Real-time video toolbar



The real-time video toolbar is as follows:



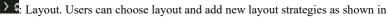


Figure 6-3. Click on the right of screen splitting format and choose the channels to view the video. Click + to add a new layout.

Figure 6-3 Add layout

+ Adduzerst			×
Chanel	Layor News	Ewall Time(sec) 5	
Fürt 29.stannels 3.Stannel28 3.Organ 4.Filter 4.Filter	्रे.स 2. Carretti 3. Charretti 4. सम्ब		
			Cana

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

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

please see chapter 7.5.5.

36

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

lo Channel Il Cricode

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



Preview strategy, users can switch the real-time preview mode according to the network.

There are three modes: fluency, balanced and real-time.

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

Figure 6-4 Main menu quick toolbar



1

: Manual alarm, click the icon, users can set different channels, choose alarm out, the

window shows in Figure 6-5.



Figure 6-5 Manual alarm

: Alarm message, click on the icon for more details as shown in Figure 6-6.

	Pop up message	to monitor 🛛 🗙
Channel	Туре	Start Time
	IP Conflict	24/04/2022 11:26:25
Channel4	Video Loss	24/04/2022 11:26:16
Channel3	Video Loss	24/04/2022 11:26:07
Channel4	Line Crossing	24/04/2022 06:08:41
Channel4	Line Crossing	24/04/2022 06:08:17
Channel4	Line Crossing	24/04/2022 06:08:03
Channel4	Line Crossing	24/04/2022 06:07:18
Channel4	Double Virtual Fe.	24/04/2022 06:07:07
Channel4	Intrusion	24/04/2022 06:06:50
Channel4	Double Virtual Fe.	24/04/2022 06:05:56
Channel4	Line Crossing	24/04/2022 06:05:54
Channel4	Line Crossing	24/04/2022 06:05:39

Figure 6-6 Alarm message



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

out.

(i)

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

channel, disk and alarm, as shown in Figure 6-7.

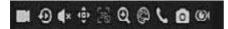
Figure 6-7 Information

Network System	Channel	Disk	Alarm	×
Status	Onine			
IP Address	192.168.32.149			
Subnet Mask	255.255.0.0			
Default Gateway	192.168.0.1			
MAC Address	00:1C:27:16:F5:7			
DHCP	OFF			
Preferred DNS Server	192.168.32.254			
Alternate DNS Server	8.8.8.8			
Total Bandwidth	1000.00 Mbps			
Received Packets	544.92 Kbps			

11

6.2 Real Time Video Bar

Right click at 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 be recording video five minutes ago.

is the time bar of playback.

Audio: open or close the audio.

PTZ: This function is only applied for speed dome cameras. The monitored camera can focus,

zoom or iris at this pop-up window. You can adjust every parameter as shown in Figure 6-8.



Figure 6-8 PTZ adjust screen

₽ Å 4 4 ■ ♪ 4 ₽ ↓

adjust direction of camera.

At this part, perform Advanced, Scan and Tour settings.

: 3D, this function can only 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.

P

: Image, click the icon, as shown in Figure 6-9. Select scene, and drag cursor to adjust value

of brightness, sharpness, contrast and saturation.

Figure 6-9 Camera picture parameter



5

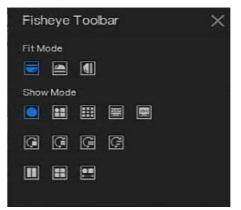
Two way audio. The NVR and camera can talk to each other.

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

: fisheye (only used for fisheye cameras), click to switch the fisheye modes, as shown in

Figure 6-10.

Figure 6-10 Fisheye



6.3 Playback

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

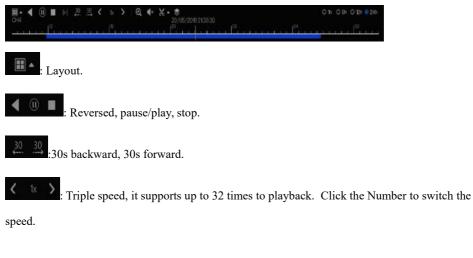
Click finite quick navigation bar to access the playback screen, as shown in Figure 6-11. Figure 6-11 Playback screen

Choose the channels from the channels list, click one day to play (the date has blue line, it means

there is recording video at this day, it doesn't mean for all channels has video.)

It maybe has three color bars on the time bar, the blue one is schedule record, the yellow one is manual record, and the red one is alarm record.

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



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



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

icon again.

The backup type appears. Click **save**. And **saving the file** pop ups as Figure 6-12. Click **OK** to save.

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

Figure 6-12 Select directory

	Select Directo	ry X
Device List C		+• ⊑ Ø
/dev/sdb2	1	
	😫 kemel-35200-V200	
	🔒 u-boot-3520D-V200	
		*
Remain/Total 0.7 GB/0.7 GB	Location: /nfsroot/usbbk_b1 Selected Directory: /nfsroot/us	
		OK Cancel

Batch backup, click the icon to backup multi-channels, as shown in Figure 6-13.

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. The backup videos are marked by watermark, you can view it by our player.

: Snapshot panorama. Click to save it to USB storage device on NVR.

42

Figure 6-13 Batch backup

Save to			ì
Video Type			
StreamInformation	Main Stream		
Start Time	2019/05/28	21:45:16	
End Time	2019/05/29	21:45:16	
Channel	□ Select All		
		OK	Cancel

: Type of time bar, recording video can show

6.3.1 Time Search

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

Operation Description

Click On in the quick navigation bar to access the search screen, as shown in Figure 6-14.

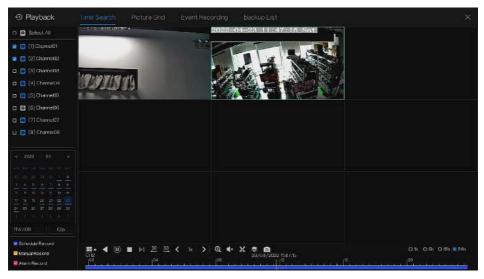


Figure 6-14 Time Search screen

Operation Steps

Step 1 Select a camera or cameras in the camera list on the left side of the search screen. The

video view of the selected camera is 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

44

6.3.2 Picture Grid

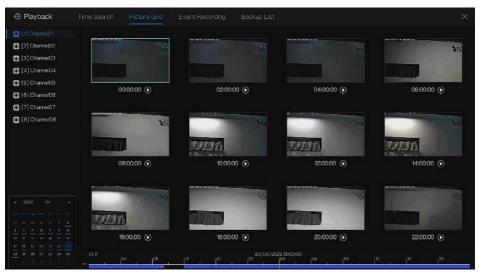
Picture grid refers to evenly dividing the video of a channel by time range and searching for a video based on thumbnails divided by time range.

Click **Ficture Crice** on the quick navigation bar to access the picture grid screen, as shown in Figure 6-15.

Network Video Recorder User Manual

Quick Navigation

Figure 6-15 Picture grid screen

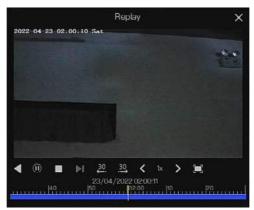


Operation Steps

- Step 1 Select a camera in the camera list on the left side of the picture grid screen. Videos shot by the camera in the earliest time range on the current day are displayed as thumbnails in the window on the right side.
- Step 2 Select a date from calendar.
- Step 3 A day are dividend to 12 grids, every two hours is a grid. Click the image to change the interval.
- Step 4 Select a required thumbnail, double-click it or right-click it and choose Play from the shortcut menu to play the video.

Step 5 Click Step

Figure 6-16 Replay



----End

6.3.3 Event Recording

Click On the quick navigation bar; choose **Event** at title to access the alarm event screen, as shown in Figure 6-17

Quick Navigation

Network Video Recorder User Manual

Figure 6-17 Event screen

• Playback							
🛛 🐼 Select Al			Channel			Oper	
🙎 🙆 [1] Channei01 🔷		24/04/2022 1147:38	Channel05	Mation Detaction	Ghannel05	Ð	۲
🖬 🔀 (2) Chonnelli 2		24/04/2022 1148:44	Channel03		Channel03	9	٩
🖬 🚺 [3] Channel03		24/04/2022 1546:43	Channel04	Video Loss	Channel04	Ð	Ø
😸 🛃 [4] Channel04 👘		24/04/2022 1146/05	Channel04	Video Loss	Charoel04	Ð	Φ
🛛 🗃 (5) Channel06		24/04/2022 11/15/41	Channel03	Video Loss	Channel03	Ð	e
🗃 🞯 [6] ChannelD6							
🛛 🖸 [7] Charne07		24/04/2022 11:45:17	Channel05	Motion Detection	Channel05	Ð	Φ
		24/04/2022 1144:38	Channel03	Video Loss	Channel03	Ð	
Start Time 23/04/2022 1147:38		24/04/2022 10/357	Channel05	Mation Detection	Channel05	Ð	۹
End Time		24/04/2022 11:13:50	Channel03		Channel03	۹	۵
24/04/2022 11:47:38		24/01/2022 11:36:15	Charmel05	Video Loss	Chennel06	Ð	Ð
尾 Alarm in		24/04/2022 1126:25		IP Confiet	IP Conflict		
🗟 Gamera Alarmin		24/04/2022 1120.10	Channel04	Video Loss	Channel04		
Motion Detection		24/04/2022 11:20:07	Channel03	Video Loss	Channel03		
Comera Tamper	14	24/04/2022 00:08:41	Channe/04	Line Crossino		Ð	Φ
Video Loss							
🐱 hteligent Analysis		24/04/2022 00:08:17	Channel04	Line Crossing		Ð	æ
R Abnormal Alarm		24/04/2022 06:08:03	Channel04	Line Crossing		۲	۵
Search				IC 1/105 X	Dox	ble click to pla	video

Operation Steps

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

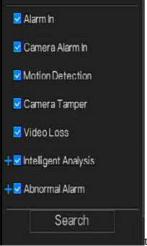
- Step 2 Set start and end time.
- Step 3 Tick the alarm type, such as alarm in, camera alarm in, motion alarm, video loss, intelligent analysis and abnormal alarm
- Step 4 Click Search to query the event, the result would show at window.
- Step 5 Double click to play video about event. It will play recording video.



• play the recording video.



Solution: backup the recording video.



the type of intelligent analysis and abnormal alarm are subdivided,

users can tick Detail Alarm to show.

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

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

User can choose the accurate alarm events to search.

----End

48

6.3.4 Backup List

Click on the quick navigation bar, choose Backup at title to access the backup screen, as shown in Figure 6-18.

Figure 6-18 Backup screen

Q	Search					
1D		End Time			Progress	Operate
4				m /nfsrööt/usbbk_b	25	» ش

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

6.4 AI Recognition (Only for Some Models)

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

The all snapshots is able to be added to the libraries according the real needs

6.4.1 Real Time Comparison

Real time comparison can compare human faces, vehicle license plate, and AI(include riding, vehicle, full body)

6.4.1.1 Human Face

At real time comparison interface, click the to enter the human face comparison interface, choose the cameras with face recognition function to play live video, the snapshots of camera will be compared with the templates which have been registered in libraries, the result shows as in Figure 6-19.

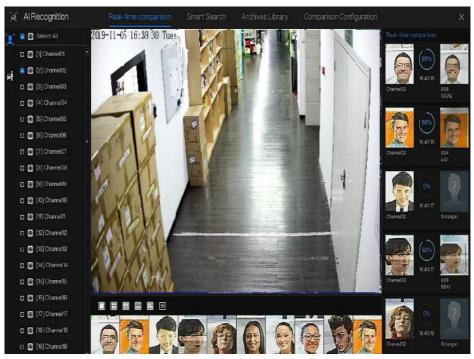


Figure 6-19 Human face comparison

Click the "+" to add the snapshot to face library immediately.

Snapshot in real time video, put the cursor on picture such as **F D**, you can add it to face

library, or face search. The cursor on area and the pictures are not update, move the mouse so that the pictures can be shown in time.

----End

50

6.4.1.2 Vehicle and Full Body

At real time comparison interface, click the **NO** to enter the vehicle license plate comparison interface, choose the AI recognition cameras to play live video, the snapshot of camera will be compared in libraries, the snapshot to vehicle and full body will show at the bottom of page, the result shows as in Figure 6-20.

Quick Navigation

Figure 6-20 Full body





6.4.2 Smart Search

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

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

6.4.2.1 Human Face Search



- Step 1 Choose human face search at smart search interface.
- Step 2 Tick the face recognition camera channels, set the start and end time.
- Step 3 Choose the condition (by picture or by feature), the picture can be selected from the file folder.
- Step 4 Click "Search" to search the snapshot of human face.
- Step 5 The result will show at the middle of page, click the picture and the detail information show at the top right of page.
- Step 6 The pictures can be added to library or used to search.
- Step 7 Click play button of video to play the recording of snapshot, click "Backup" to back up the recording videos.

Quick Navigation

Figure 6-22 Back up

	Backup	
Stream:	Main Stream 🗸 🗸	
Video Type:	Mp4	
Channel:	CH9	
Size:	30.0 MB	
Start Time:	27/04/2020 14:09:37	
End Time:	27/04/2020 14:10:07	
Save	Cancel	

Step 8 Click "Export" to export the result, choose export type pictures or videos.

(2013) (1722) S.S.S.S.S.S.S.S.S.S.S.S.S.S.S.S.S.S.S.	Temenenen -	
Export Type	Export Pictures 🗸	
Save to	Export Pictures	
	Export video	

Figure 6-23 Export

Play video of snapshot, it will play a 30-seconds video before and after the snapshot.

Snapshot in real time video, put the cursor on picture such as + 💭 🔍, you can add it to face

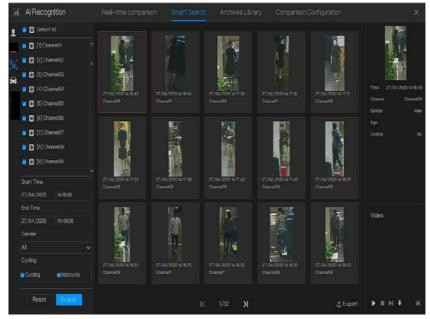


library, or face search. The cursor on area 6 and the pictures is not update, move the mouse so that the pictures can be shown in time.

----End

6.4.2.2 Full Body Search





Step 1 Choose full body search at smart search interface.

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

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

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

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

54

Quick Navigation

Network Video Recorder User Manual

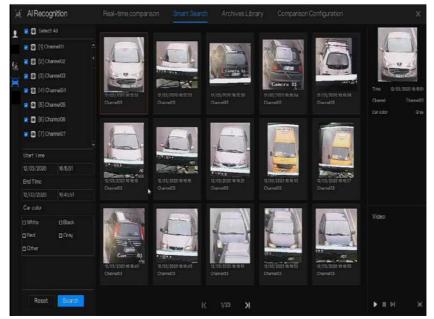
Step 6 Click play button of video to play the recording of snapshot, click "backup" to back up the video.

Step 7 Click "Export" to export the result.

----End

6.4.2.3 Vehicle Search

Figure 6-25 Vehicle search



- Step 1 Choose vehicle search at smart search interface.
- Step 2 Tick the AI recognition camera channels, set the start time and end time.
- Step 3 Tick the color.
- Step 4 Click "Search" to search the snapshot of human face.
- Step 5 The result will be showed at the middle of page, click the picture and the detail information show at the top right of page.
- Step 6 Click play button of video to play the recording of snapshot, click "backup" to back up the video
- Step 7 Click "Export" to export the result.

----End

6.4.3 Archives Library

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

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

6.4.3.1 Face Library

Figure 6-26 Face library

	+ Add	X De	lete 🕁	import.	击 Export	Q Refresh 17	7 Filter		
D Select All		Name	Gender	Birthday			Тура	Expire date	Operate
🛛 Defadi Llu	٥		Male	28/11/2019	i n	urknow	Student	Never expire	2 🛙 Q
			Male	28/11/2019		unknow	Student	Never expire	۵ 🛍 ک
Drve			Male	28/11/2019		unknow	Student	Never expire	∠∎ 0.
etechnology			Mala	28/11/2019		urknow.	Student	Never expire	2∎0
e maga			Male	28/11/2019		unknow	Teacher	Nover expire	∠ @ Q
engineering			Male.	28/11/2019		urknow	Student	Nover expire	∠ 🗈 Q
platform			Mala	28/11/2019		unknow	Student	Never expire:	소 🖬 이,
			Male	20/11/2019		sinknow	Student	Never expire	∠∎ a
Eur know			Male	28/11/2019		unknow	Student	Never expire	∠ tù Q
e lind.			Male	28/11/2019		unknow	Student	Never expire	∠∎ 0.
Phardware .			Male	28/11/2019		unknow	Student	Never expire	2 🖬 Q
download			Molo	28/11/2019		unknow	Student.	Novor expire	2 🛚 Q
			Mile	28/11/2019		unknow	Student	Never expire	2 🗈 Q
			Male	28/11/2019		unknow	Student	Never expire	∠ 🖬 Q
			Male	28/11/2019		unknow	Student	Never expire	∠∎ 0
			Male	28/11/2019		uoknow	Stuckent	Never expire	∠∎ 0
			Male	28/11/2019		unknow	Student	Never expire	∠ ĝ 0,
			Molo.	28/11/2019		unknow	Student	Nover expire	∠ 🖻 Q

Click "+" to add a new face library.

Click "Add" to add person face.

Tick the person, click "Delete" to delete the person.

Click "Import" to add the person batch.

Click "Export" to export the all person in library.

Click "Filter" to filter the all persons in library, as shown in Figure 6-27.

Quick Navigation

Figure 6-27 Filter

Gender	All	
D		
Туре	All	
Picture	All	18

Click operate icon to edit or delete the chosen person.

----End

6.4.4 Comparison Configuration

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

At comparison configuration interface, user can set the comparison of human face/ license

plate/temperature/ mask detection configuration/ personnel count configuration.

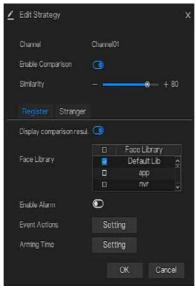
6.4.4.1 Face Comparison

At face comparison interface, users can set different channels' strategy, such as similarity, display comparison result, face library, enable alarming, event action, arming time, as shown in Figure 6-28.

Al Recognition				
Channel	Register Detect Library	Stranger Detect Library	Sminity	Operate
Chamoitt	DefailtLib	DefaultLb	80%	
Chanel2	Defait i in	Clefwatility		۷.
Charrent2		Detautlub		
Channel14	DefaultLib	Defwit Lib		
Ourse/6	Default Lib	DefaultLite	80%	
Channel 15	DefaultLib	DefaultLb	80%	
Channel 17	Defait Lib	Defaut Lb		۷.
Chame/8	Default Lib	Defaut Lib		
Charce/E	Onfailt1.b	Defaulti.b		
Otame(2)	DetaultLib	DefaultUb		
Chane@1	DefaitLb	Default Lb	80%	
Channel22	Default Lib	Default Lb		
Otemei23	Dufault Lib	DefaultLib		
Channel24	Ocfair Lib	Dofout Lib		
Channel25	Octault Lib	DofastLib		۷.
Channel/5	Ueta #1.h	Detwit Lib		۷.
Charrie 2/	UetaitLb	Detwit Lb		
Channe 29	DefaultLib	Default Lb		
Charre 29	DefailtLb	DefadtLib	80%	4

Figure 6-28 Face comparison

Figure 6-29 Strategy



----End

58

6.4.5 Attendance Management

In attendance management, users can set attendance rule, library and check point, as shown in Figure 6-30.



Attendance		×
p-Attendance Rule Settings	Attendance Rule Settings	
⊅-Attendance Library	Working Time: Start-work time 09:30 End-work time 1000	
▷ Attendance Check Point S.	WurkdaySetling: ⊡Sun ∎Mun ∎Toe ∎Wed ∎Thu ∎Fri ⊡Sat	
	Check-in valid time: Before stort-work time 10 min to After stort-work time 30 min Check-out valid time: Before end-work time 10 min to After end-work time 30 min	
	-If employee does not check in when starting work, mark as absent If employee does not check out when ending work, mark as absent	
	Apply	

Operation Steps

Step 1 Set start work time and end work time.

Step 2 Tick the workday

Step 3 Set valid time of check in and check out.

Step 4 Click Save to save the setting.

Attendance library

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

Attendance	Attendance Data Attendance Managem			
> Attendance Rule Settings	Attendance Library			
	Face Library 👩 Library Management		Attendance Library	
> Attendence Check Puint S.	C 12 Rems R Dafnut I. Ib 2 ap 2 of r 2 biotnology 2 b	>> Add « Delete	D 12 litems	Accey

Figure 6-31 Attendance library

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

Step 3 click Database management to enter the face database management to modify

parameter.

Step 4 Click Save to save the setting.

Attendance check point settings:

Step 1 Click Attendance check point settings to set point, as shown in Figure 6-32.

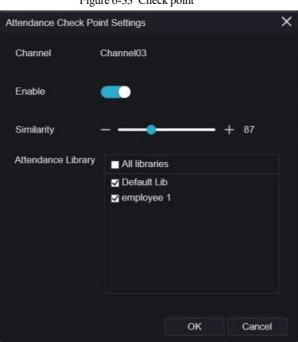
Quick Navigation

Attendance	Attendance Data				
> Attendance Rule Settings	Attendance Check Po	int Settings			
> Attendance Library	Channel	Attendance Litrary	Similarity	Enabled	Operat
	(Jtame01	Default Lib;appminitechnology;mage;engineering;platform;pc;urknow;test/hardw	80%	Start	4
	Charnel02			Start	∠
	Channel03		80%	Start	
	Charrys 104		80%	Start	4
	Charnol05		80%	Start	۷.
	ChannelOfi	Defailt Libpppror, technology;mage, engineeringplatform; pounknow; test; har dw.		Start	4
	Channel07			Start	4
	Chave08	Default Lib;app;//wr.technology;image,engineering;platform;pc;uninow;testUhardw		Start	۷
	Chamel09		80%	Start	1
	Chamel10				
	ChannelT				2
	Chamol12			Start	4
	Channell3			Start	4
	Chame/4			Start	4
	Chamel15		80%	Start	2
	Charnel 16			Start	4

Figure 6-32 Attendance check point setting

Step 2 Click L to edit check point setting, as shown in Figure 6-33

61



- Step 3 Enable the function, set similarity and tick the library, all face detection cameras can be set the check points
- Step 4 Click **OK** to save the setting.

---End

Figure 6-33 Check point

6.5 Channel Information

Click the B will show as Figure 6-34, tick the Channel or Encode, the information will show in

live video screen.





----End

6.6 Main Menu

Right-click on the UI screen, the main menu as shown in Figure 6-35. The main menu includes

Channel, Record, Network, Alarm and System.

Figure 6-35 NVR main menu

	Channel			Record			Network	
Þ	Camera Sensor Setting Privacy Zone Microphone Smort	Encode OSD RCI Intelligent Tracking	0))	Record Schedule Storage Mode Disk Detection FTP	Disk SMART Disk Calculatio.	S	Network DDNS Email IP Filter	802.0X Port Mapping P2P SNMP
	Alarm				System			
	General Video Loss Alarm In Alarm Out	Motion Deter Intelligent An Abnormal Ala Local Intellia	alysis em	Ę,	Information Security Center Loga	General Layout Mainten	ance	User Account Auxiliary Screen Auto Reboot

----End

7 UI System Setting

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

7.1 Channel Management

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

Channel management includes Add or Delete Camera, Encode, Sensor Setting, OSD, Privacy Zone, ROI, Microphone, Human Thermometer, Smart, and Intelligent Tracking.

7.1.1 Camera

Operation Description

Click **Channel** in the main menu to access the camera management screen, as shown in Figure 7-1 There are four modes for adding cameras, manually add, batch add, search to add, POE add, and automatic add.

64

UI System Setting

🗙 System		Record	Alarm I	Network	System					
	Gamora	Protoco	l Management							
> Encode		Chargel			Model			ware Version	Operate	
Sensor Setting		CHI	192,168.32.74:30	1001		Privatu	(3.6.08)	04.1004.278.0.119.1	<u>ک</u> ش ′	
 Sensor Senarg 				001			-36.08		<u>∠</u> 0 -	
▶ 0SD			169.254.10.4.300						2 0 -	
									∠ ∎ -	
» Microphone						Aad	levices	Delete	Batuh Updal	é.
⊳ Maraphana	Onine I	Device	Start	Search		Adul	levices	Delete	Batch Updal	θ.
» Microphono	Orine1 D	Device P		Search Mode		Adul Protocol	levices	Delete Firmware Varsion	Bal ưn Updal Modify F	
> Micropitano > Smart							levices			
		P	154.0000				levices		Modify F	
⊳ Smart		P 192 106 22	154 8888			Protocol	levices	Firmware Version	Modify F	
⊳ Smart		P 192 108 32 192 168 32 1	154.0986 153.30001 132.90001			Protocol ON/F Privale	levices	Firmware Version v38.0804.1004.3.0.119.0	Modify F	
⊳ Smart		. P 192 108 32 192 108 32 1 192 108 32 1	154.0080 153.00001 182.00001 90.00001			Protocol ONVIF Private Private	levices	Firmware Version v38.0804.1004.3.0.115.0 138.0821.1004.3.05.10	Medfy F 2 2 2	
⊳ Smart		P 192 106 32 192 468 32 1 192 468 32 1 192 468 32 1	154.0986 153.00001 182.00001 20.00001 79.00001			Protocol CNVIF Privala Privata Privata	levices	Firmware Version v38.0801.1001.3.0.119.0 t38.0821.1004.3.0.5.10 v3.0.1304.3043.0.410	Modfy F	

Figure 7-1 Channel management screen

Modify device parameters, remote channel is based on cameras (human body

temperature has two remote channels, fisheye cameras have four remote channels) as shown in Figure 7-2.

Channel Name	Channel10
P Address	192 . 168 . 1 . 83
Protocol	Private 🗸 🗸
Port	30001
Username	admin
Password	*****
Remote Channel	CH-1 v

Figure 7-2 Modify device parameter

----End

7.1.1.1 Add Camera Automatically

The NVR can add automatically cameras to the camera list.

Operation Methods

Method 1: Click Start Search button, the cameras in the same network as your recorder will show in list, the search will be lasting for 20 seconds. Input username and password (the default value both are admin) click Add Devices, the cameras in the list would be added to channels directly. Method 2: Select the cameras you want to add, and click Add Devices, 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 channels in the camera list. If the status of a

channel is this camera is online. If the status of a channel is this camera is offline.

The added cameras should be the same network as NVR.

----End

7.1.1.2 Add Camera Manually

Operation Steps

Step 1 Click to add devices as shown in Figure 7-3.

Channel	Р		Protocol	
CH1	169.254.10.2	:30001	Private	< 1
CH2	192.168.99.14	6:30001	Private	
CH3	192.168.99.14	5:30001	Private	÷
Channel				
Address				
rotocol	c	NVIF		~
°or t		o		
Jsername				
assword				
lemote Chan	nel (

Figure 7-3 Add camera screen

- Step 2 Input IP address, port, user name and password of this camera. Double click the online camera IP to copy its configuration. Quick change of other channel's parameters can be done.
- Step 3 Select a protocol from the drop-down list(ONVIF, Private, custom protocols). Remote channel is only used for multi channels cameras, such as human temperature cameras, fisheye cameras, and so on.

Step 4 Click OK, the camera is added successfully.

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

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

The protocol can be chosen the custom protocols these are set at protocol interface.

The user can click the added channel to copy the information to save the time, you can just need to modify difference information, such as the remote channel.

----End

7.1.1.3 Add Camera by RSTP

If the user wants to add the different protocol cameras to NVR, you can set the protocol

management, and add cameras one by one, as shown in Figure 7-4.

Figure 7-4 Protocol management

🛠 System	Channel Record Alarm	Network System	×
	Camera Protocol Management		
> Encode	Custom Protocol	Custom Protocol 1 🗸 🗸	
b Sensor Setting	Protocol Name	Custom 1	
⊳ OSD	Stream Type	🖉 Main Stream 💷 Sub Stream	
 Privacy Zone 	Protocol Type	RTSP V RTSP V	
> ROI	Port		
⊳ Microphono	Path		
	Example(Type)://[IP Address][Port	t]/[Path];	
ъ Smart			
Intelligent Tracking			
			Apply

Step 1 Click Channel > Camera > Protocol Management.

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

UI System Setting

Step 3 Input the protocol name.

- Step 4 Tick main stream and sub stream. The main stream shows image on full screen live video. The sub stream shows image on split screen. If you just tick main stream and the channel will not show image on split screen.
- Step 5 Choose the type of protocol, the default value is RTSP.
- Step 6 Input the port of the IP camera.
- Step 7 Input the path (it may vary with different camera models).
- Step 8 Click Apply to save the settings.

Choose the protocol from the drop-down list, the protocol is set at protocol management interface. The cameras should be confirmed to the protocols.

----End

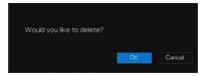
7.1.1.4 Delete Camera

Operation Steps

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

message screen is displaying, as shown in Figure 7-5.

Figure 7-5 Delete confirmation message



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

7.1.1.5 Operate Camera

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

Figure 7-6 More operation

 Update 	
Reboot	
② Reset	
🖌 Modify IP	

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

Step 2 Set the directory click OK to update camera. Figure 7-7 Select directory of software

		>
		-
02_1020x 1080_20181229100453.mp4		
02_1020x 1080_20181229100564 mp4		
	٠	
	GK	Cancel

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

- Step 4 Click **Reset**, message "**Are you sure to reset?**" would show, users can enable the retain IP address function. Click OK to reboot the camera.
- Step 5 Tick the cameras with non-onvif protocol and cameras are online, click **Update** to update all cameras at once.
- Step 6 IP address of the online camera can be modified, click **Modify IP** to modify as shown in following figure, input the new IP address and subnet mask.

Update need upload the firmware by flash driver.

----End

70

7.1.2 Encode Parameter

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

Operation Description

Click **Encode** in the main menu or **Menu** of the channel management screen and choose **Encode** to access the **Encode** screen, as shown in Figure 7-8.

🛠 System	Channel Record Alarm	Network System			
⊳ Camera	Encada				
	Channel	[1]Channel01			
Sensor Setting					
> OSD	Stream Information	Main Stream	Sub Stream		
Privacy Zone	Video Format	H285	H285		
⊳ HOI	Audio Encode Type	G711A			
> Microphone	Resolution	1920×1000	704x576		
	Frame Rate(fps)				
> Smart	Frame Interval(Frame)	50			
Intelligent Tracking	Bitrate Type	CBR	CER		
	Elitrate(kbps)	4096	1024		
	Quality				
	Smart Encode	Ð			
				Сару	Αρρίγ

Figure 7-8 Encode screen

Operation Steps

- Step 1 Select a channel from the drop-down list of channel.
- Step 2 Set video format, audio encode type, resolution, frame rate, bitrate type, bitrate size and quality from the drop-down lists.
- Step 3 Click Copy and select channels or tick all, then click OK to apply the parameter settings to cameras in selected channels , click Apply to save encode parameter settings.

----End

7.1.3 Sensor Setting

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

Operation Description

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

Figure 7-9 Sensor setting screen

🛪 System	Channel Record	Alarm Network	System				×
> Camera	Sensor Setting						
> Encode	2022-04-24 12 54 48 8.0						
		Contraction of the local division of the loc		Channel	[1]Channel01		
⇒ OSD							
> Privacy Zone							
> ROI	1-1 Idulatore	146					
> Microphone							
⊳ Smart	huga S	owa Exposura	White Balance	DayNight	Noise Reduction	Enhance Image	
Intelligent Tracking	Scene	Default 🗸					
	Brightness	•	+ 50				
	Sherpness						
	Contrast						
	Saturation		+ 50				
						Default	Apply

The Sensor Setting are as follows:

Brightness: it indicates brightness or darkness of an image.

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.

72

UI System Setting

Day-night: users can transit day to night, or switch mode. Noise reduction: it includes 2D NR and 3D NR. Enhance image: it includes WDR, HLC, BLC, defog and anti-shake. Zoom focus: users can zoom and focus.

Operation Steps

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

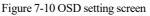
Step 2 Select scene from the drop-down list. The default values of picture parameters vary with scenarios.

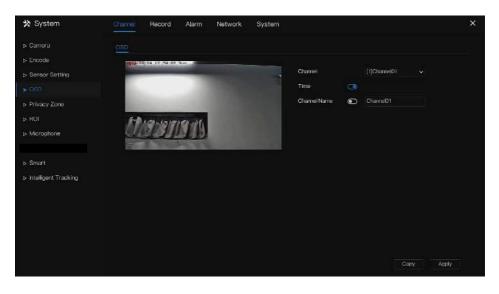
Step 3 Set parameters.

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

7.1.4 OSD Settings

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





Operation Steps

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

- Step 2 Click next to Time to enable or disable OSD time setting.
- Step 3 Click next to Name to enable or disable OSD channel setting.

Step 4 Set the channel name.

- Step 5 In the video window, click and drag time or channel to move to a location.
- Step 6 Click Copy and select channels, then click OK to apply the OSD settings to cameras in selected channels , click Apply to save OSD settings.

----End

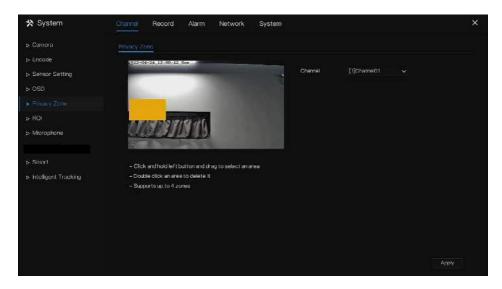
7.1.5 Privacy Zone

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

Operation Description

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

Figure 7-11 Privacy zone screen



Operation Steps

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

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

Step 3 Click Copy and select channels or tick **all**, then click OK to apply the privacy settings to cameras in selected channels , click Apply to save privacy settings. Step 4 Double click privacy area to delete setting.

----End

7.1.6 ROI

UI System Setting

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

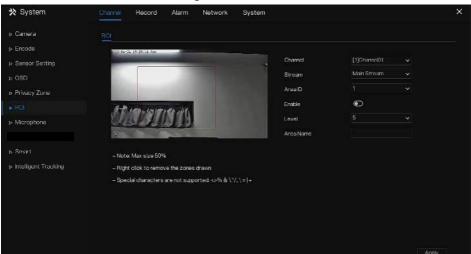


Figure 7-12 ROI

Table 7-2 RIO parameter

	1			
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	The measure result of ROI. The higher the grade, the clearer the area inside and the more vaguer the area outside. There are five levels.	[Setting method] Select a value from the drop-down list box. [Default value] 5
Area Name	The marked name used for areas.	[Setting method] Enter a value manually. The value cannot exceed 32 bytes.

----End

7.1.7 Microphone

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

Network Video Recorder User Manual

UI System Setting

Figure 7-13 Microphone

🛪 System	Chamel Record Alarm	Network System		×
> Camera	Microphone			
> Encode	Channel	[1]ChanneiU1		
Sensor Setting	Microphone	(
⊳ OSD	Microphone Type	Line in		
Privacy Zone	Microphone Volume		+ 50	
> ROI				
≫ Smart				
Intelligent Tracking				
				Apply

Table 7-3 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.

----End

7.1.8 Smart

It is only available for cameras with AI function.

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

7.1.8.1 AI Multiobject

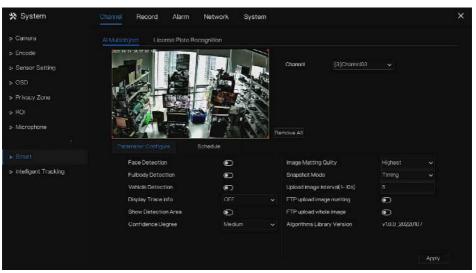


Figure 7-14 AI multiobject

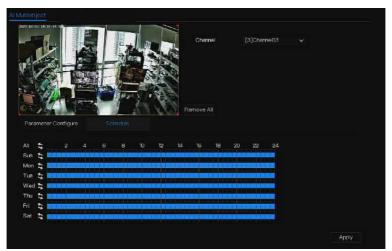
Table 7-4 AI multiobject

Parameter	Description	How to set
Face detection	The camera will snap the face when someone appears in live video.	Enable
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.	Choose from drop list.

UI System Setting

stem Setting Parameter	Description	User Manual How to set
	Mode 1:	
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- down 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 range 30 to 300
Vehicle pixel min(30-800)	30-300 pixels, the smaller the pixel be set, the more face will be captured, but it may be mistaken.	Input a value range 30 to 800
Image matting quality	The quality of snap images, There are three modes can be chosen, such as low, mid and high.	Choose from drop list.
Snapshot mode	There are three modes can be chosen, such as timing, and optimal.	Choose from drop list.
Upload image interval(1-10 s)	At timing mode, set the interval of upload image.	Input a value ranges 1 to 10
FTP upload image matting	Configuration > Network Service > FTP , set FTP related parameters, the captured picture will be sent to the set FTP location	Enable
FTP upload whole image	Capture a picture and send a whole image.	Enable

Figure 7-15 Schedule



----End

7.1.9 Intelligent Tracking

This function is available for high speed camera.

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

UI System Setting

Figure 7-16 Intelligent tracking

🛠 System	Channel Record Alarm	Network Syste		×
⊳ Camera	Intelligent Tracking			
> Encode	Channel			
Sonsor Sotting	intelligent Tracking	G		
> OSD	Calbration Coefficient	- •		
> Privacy Zone	Trace Magnify	-	+ 17	
⊳ ROI	Time Of Duration(s)		9 + 212	
> Microphone				
Human Thermometer				
⊳ Smart				
				Actily

Table 7-5 Intelligent tracking parameters

Parameter	Description	Setting
Enable	Enable the button to enable the intelligent tracking	[How to set] Click Enable to enable. [Default value] OFF
Calibration Coefficient	It is equivalent to a control coefficient, and real-time tracking doubling rate nonlinear positive correlation, usually the higher the installation height, the greater the calibration coefficient value; it ranges from 1 to 30	[Setting method] Drag the slider. [Default value] 1
Trace Magnify	It is the value of lens zoom, it has a large influence on the real-time tracking magnification,	[Setting method] Drag the slider. [Default value] 7

Time of Duration	The maximum time of a tracking period, it ranges from 0 to 300 s.	[Setting method] Drag the slider. [Default value] 120
------------------	---	--

----End

7.2 Record Setting

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

7.2.1 Record Schedule

Operation Description

Click **Record** in the main menu or click the record page of any function screen in the main menu to access the record schedule screen, as shown in Figure 7-17.

Figure 7-17	Record	management screen
	1100010	interine Berreen

	Renord	I Schni	tito												
Jisk	Ch	amei					[1]Chan	nelU1							
Storage Mode	En	able Fie	cord				۲								
SMART	En	able Re	cerd Audi	o			D								
Disk Detection	En	abie AN	R												
Jisk Calculation	AI		2	-4	6	8	10	-12	16	18	20	22	24		
		7 47					10100					NULLER		Continuous	
		n 🎝									201-			📕 Alarm	
		1 1 11									and the second			Motion	
		1 4												∎ м)і/о	
	Fri													□ M&I/O	
	Sa	4					i ei An be s					Market Bark			

Operation Steps

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

Step 2 Enable the record.

Step 3 Enable the record audio.

Step 4 Enable ANR, the camera is installed with SD card, if the camera is disconnected from the network, when the network is recovered, the NVR can read the recording of camera and copy the loss video form the SD card.

Step 5 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.

When you select time by dragging the cursor, the cursor cannot move out of the time area. Otherwise, no time would be selected.

The selected area is blue. The default is all week.

Users can choose alarm type to record, if the chosen alarm is happening at the setting time, it will record. So that it will using the disk effectively to avoid repeating useless recording.

The ANR function can be used only for the cameras with supplementary recording function.

Users can set different alarms to record.

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

Step 6 Deleting record schedule: Click again or inverse selection to delete the selected

record schedule.

Step 7 Click Copy and select channels or tick all, then click OK to apply the record management settings to selected channels , click Apply to save settings.

----End

7.2.2 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 time.

UI System Setting Operation Description

Step 1 Click Record in the main menu or menu of the record screen and choose Disk to access

the disk screen, as shown in Figure 7-18.

🛠 System	Channel Record Alarm	Network System		×
> Record Schedule				
⇒ Storage Mode		nsk2		
⊳ S.M.A.R.T	Cepacity 12TB	Capacity 3TR		
▷ Disk Detection				
» Disk Calculation			Format	
> FTP	Disk Status	Normal		
	Disk SN	5QJ8VD98		
	Used Space	149GB		
	Disk Group			
	Recording Overwrite	G		
	Expired Time(Day)			

Figure 7-18 Disk screen

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

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

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

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

Step 6 Record expiration setting. Select record expiration days from the drop-down list of record expiration. The expired time is not 0, the records will be deleted when the time is over the setting value.

Step 7 Click Apply to save the settings.

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

The expired time is 0, it means the disk will be rewrite only when the disk is full .

----End

7.2.3 RAID (Only for Some Models)

The NVR support to build/ edit/ delete the RAID. Users can choose the type of RAID according to the importance of recording.

RAID is only used for the device with 4 disks or more. And the disks must be enterprise level disks. The capacity of disks is the same for efficient using.

The maximum capacity of RAID cannot exceed 100T.

RAID5 at least 3 disks can be created. RAID6 at least 4 disks can be created. RAID10 at least 4

disks can be created. Create hot spare disk need more one disk or double basic disks.

The capacity of disks is the same for efficient using

Figure 7-19 RAID

	Channel Recor	d Alarm Netw	ork System		
> Record Schedule	RAD				
> Disk	D Creat	e RAD		×	Operate
		D Type RAD 5			
▶ SMART		Name	Capacity	Hotspare Disk	
		Disk1	1TB		
		Disk3			
		Disk4			
				OK Cancel	Create

Operation Steps

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

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

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

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

7.2.4 Storage Mode

Users need to distribute the channels to different disk groups, and use disk capacity reasonably, as shown in Figure 7-20

Figure 7-20 Storage mode

🗞 System	Channel Recor	d Alarm	Network	System		
Record Schedule						
Disk						
	Mode Selection	20	Group			
SMART	Disk Group					
Disk Detection	Channel			5 0 7 8		
Disk Galduation						
Disk Cabulation						Apply
	The default Charn	el belanas tu Gr	anto 1			Αρρίγ
	The default Charn	el belonge to Gri	uup 1			Αρρίγ
	The defadi Charn Group	el belangs to Gr Disk	uup 1	Charned	ປຣສຕ໌ ຣິດສຸດອ	Appiy Capacity
			хр1	Charnel 1-4	Used Space 14908	
	Group	Disk	sup 1			Capacity
	Group 1	Disk Disk1	эцр 1	1.4	149GB	Capacity 120TB

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 record these channels, please make sure that all channels are in list.

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

----End

88

7.2.5 S.M.A.R.T

7.2.5.1 S.M.A.R.T

S.M.A.R.T is Self-Monitoring Analysis and Reporting Technology, u which is able to check the disk as shown in Figure 7-21.

UI System Setting

Figure 7-21 S.M.A.R.T

Disk Detection	Temper Disk Hei			Disk Model Working Time	2.9 Month				
Disk Calculation		Attribute Name	Status	Value		Threshold	Түре	Raw Value	
		raw-read-error-rate	OK	100	100	16	prefail	0x000000000000	
		throughput-performe.					old-age	0x60000000000	
		spin-up-time	OK				prefail	0x95019e010800	
		start-stop-count		100			oki-age	0x240000000000	
		reallocated-sector-c.		100	100		prefail	0x000000000000	
		seek-error-rate			100		old-age	0×0000000000000	
		seek-time-performa.			140		old-age	0x0100000000000	
		powar-on-hours			100		old-aga	0x270800000000	

----End

7.2.5.2 WDDA

The western digital disk has the WDDA function, the NVR can read the information of disk, so that users can view the status of disk, as shown in Figure 7-22.

Figure 7-22 WDDA

 Record Schedule 	S.M.A.R.T	WDDA				
Disk	Disk	Disk1 🗸				
Storage Mode	Disk SN	Disk1	Disk Model			
	Warning		Advisory			
Disk Detection						
> Disk Calculation		AttributeName		Status	Raw Value	
		Lifetime Power On Reset Alert		Normal	22.00	
		Power On Hours Alert		Normal	2087.00	
		Head Load Lifetime Count Alert		Normal	79.00	
		Current Temperature Alert		Normal		
		Total Lifetime Workload Alert		Normal		
		Total Workload Rate Alert		Normal	114.72	
		Power On Reset Rate Alert.		Normal		
		Head Load Bate Akrt			0.04	

----End

7.2.6 Disk Detection

Detect the disk before recording videos so that the data are secure as shown in Figure 7-23.

UI System Setting

Figure 7-23 Disk Detection

🛠 System	Channel		Alarm	Network	System				×
➢ Record Schedule	Dink Deter	tion							
⊳ Disk	Disk				⊕Eey Area ₩	Cancel			
▹ Storage Mode									
▶ RAD							DetectingProcess	5.52%	
▶ SMART						9999539 9999955 9999955 1999955	HDD Capacity	3TB	
							Bad Sector		
 Cloud Storage 						3222255 222255 222555 2225555 22255555 222555555			
	8 8 8 8 8 8 8 8 8 9 8 8	100001050 800000050 800000000 8000000000 800000000	(日本) (日本) (日本) (日本) (日本) (日本) (日本) (日本)			第三句後の名号 第三句をのからこ 第四句でがらこ 第四句をのからこ	📕 Good 📕	Bad	
						2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2			
	550					0 2 0 0 0 0 0 0 2 0 0 0 0 0 0 2 0 0 0 0			
						83556888 2336888 2336888 2336888 2336888 2336888 2336888 234688 23568 23568 2556 2556 2556 2556 2556 2556 2556 2			
	8881								
	Please	turn off the v	vedio recordin	gbefore the dis	k is detected.				

Operation Steps

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

Step 2 Tick All or key Area to detect the disk. It will take some several 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.

----End

7.2.7 Disk Calculation

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

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

Figure 7-24 Disk calculation of capacity

🛠 System	Channel Record Alarm 1	Network System		×
Record Schedule	Disk Galesiation			
> Disk	Currently total camera(s) bitrate	32.45 Mbps		
Storage Mode	Calculation Mode	Computing Capacity		
> SMART	Expect to save time	10 Day		
> Disk Detection	Recording time per day		-e 24 li	
>TTP	The required disk space			

Network Video Recorder User Manual

UI System Setting

Figure 7-25 Disk calculation of time

🛠 System	Channel Record Alarm	Network System	×
Record Schedule	Disk Calculation		
ъ Disk	Currently total camera(s) bitrate	32.45 Mbps	
t⊧ Storage Mode	Calculation Mode	Computation time	
> SMAR.T	Disk Capacity		
 Disk Detection 	Recording time per day	0 2/	
	The recording time for 10TB disk orp	ecty is:	



7.2.8 FTP

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

Figure 7-26 FTP

🛠 System	Channel Hecord Alarm	Network System	×
Record Schedule	ETP		
⇒ Disk	Enable F 1 P Upload	Ō	
⊳ Storage Mode	FTP Address		
⊳ SMART	FTP Port		
▷ Disk Detection	Account		
» Disk Calculation	Password		
	FTP Peth		
	Upload File Size((1–64MB)		
		Test	
			Apply

Step 1 Enable the FTP upload.

Step 2 Input the FTP address and port.

Step 3 Input the account, password and FTP path.

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

Step 5 Click "Test" to test the parameters. After the test is successful, click "Apply" to save the settings

----End

7.3 Alarm Management

Set the General alarm information, Motion Detection, Video Loss, Intelligent Analysis,

Alarm In, Abnormal Alarm, Alarm out and Local intelligent analysis in alarm management screen.

7.3.1 General

7.3.1.1 General

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

Figure 7-27 Alarm management screen

🛠 System	Channel	Record	Alarm	Network	System		×
	Genoral	ID Control	Push				
> Motion Detection	Enable /	Alarm		Q			
> Video Loss	Alarm D	uration Time	(sec)				
> Intelligent Analysis	Buzzert	Duration Time	r(sec)				
⊳ Alarm h							
⊳ Abnormal Alarm							
> Alarm Out							
> Local Intelligent Analysis							
							Apply

Step 2 Click to enable the alarm function.

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

Step 4 Click Apply to save alarm settings.

7.3.1.2 IO control push

If you select normally open and tick the disabled items, the alarm input 1 will not push message.

Only when the alarm in 1 is in the normally closed, it can push alarm message.

Step 1 Enable the IO control push.

Figure	7-28	Ю	control	pus	h
1 igaie	/ 20	10	00110101	pab	-

🛪 System	Channel Record Alarin	Network System	×
> General	General ID Control Push		
 > Motion Detection > Video Loss > Intelligent Ansiyals > Alarm In > Alarm Anal Alarm > Alarm Out 	Enable IO Control Alorm In Normal State Disabled itams	C 1 N/O Poshmessage to AFP €Email	
.p. Local intelligent Analysis			
			Acply

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

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

----End

7.3.2 Motion Detection

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

Operation Description

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

▶ Mation Detection	Channel	(1)Channel01	
	Enable Video Loss Alarm		
Advanced Intelligent Analy.			
 Intelligent Analysis 	Event Actions 🛗 Schedu		
> Alam In	Push message to APP		
 Abnormal Alarm 	Pop up message to monitor		
Alerm Out	Email	Ξ	
ADAM		•	
 Local Intelligent Analysis 		•	
Cocarinteligent Analysis	Enable Alarm Out Erable Remote IO	•	
	Enable Remaile IO Enable Event Recording	•	
	entencevan biasatang		

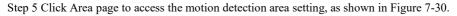
Figure 7-29 Motion detection screen

For Email, FTP, you should set the parameters of these in advance.

Enable Remote IO, the users connect the ADAM (data acquisition modules) to NVR in advanced. Alarm time, the alarm will be duration. Remote ID, the ADAM is connected to NVR'S ID.

Port number, the alarm device is plugged to ADAM's ID. elation Steps

- Step 1 Select a channel from the drop-down list of channel.
- Step 2 Click **O** to enable motion detection.
- Step 3 Enable motion analysis if the camera detects the motion action, the area will be block as shown in Figure 7-30.
- Step 4 Enable the Event actions include: push messages to App, pop up messages to monitor, send Email, buzzer, FTP, PTZ, full screen, alarm out, camera alarm out, enable remote IO, event recordings and so on.



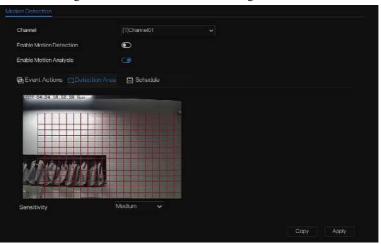


Figure 7-30 Motion detection area setting screen

Area :

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

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

Step 6 Click Schedule page to access the schedule screen. For details, please see 7.2.1 Record

Schedule Figure 7-23Step 5 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.

Double click 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.

Enable the alarm out, users need to set alarm time and output ID, four ID are corresponding to back panel's alarm out, 1 A and 1 B, 2 A and 2 B, 3 A and 3 B, 4 A and 4 B.

Channel alarm out is corresponding to alarm port of camera.

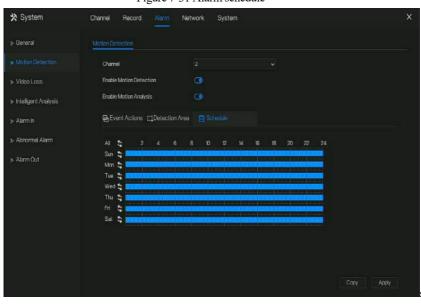


Figure 7-31 Alarm schedule

----End

7.3.3 Video Loss

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

Operation Description

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

Figure 7-32 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: push message to App, pop up message to monitor, send Email, buzzer, FTP, PTZ, alarm out, enable remote IO, event recording and so on.
- Step 4 Click Schedule page to access the schedule screen.
- Step 5 For details, please see 7.2.1 Record Schedule Figure 7-23Step 5 Set the record schedule.
- Step 6 Click Copy and select a channel, then click OK to apply the parameter settings to cameras in selected channels, click Apply to save video loss settings.
- ----End

7.3.4 Intelligent Analysis

The channel camera can set the intelligent analysis which are depended on the performance of cameras.

Operation Description

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

🛠 System	Channel Record Alarm Ne	twork System	×
⊳ General	Perimeter Single Virtual Fence Doubl	le Virtual Fences Multi Loitering Wrong Way People Counting	~
» Motion Detection	Chamel	[1]Chame(U) 🗸	
p Video Loss	Enable	Ð	
🔹 Intelligent Analysis	Event Action 1 Contention Area	i 🛗 Schechile	
⊳ Alarm h			
> Abnormal Alarm		•	
> Alarm Out			
> Alerm Cut	Buzzer	\odot	
tananan ar			
 Local Intelligent Analysis 			
	Full Screen	Ð	
	Enable Alarm Out	•	
	Enable Camera Alarm Out	0	
	Enable Remote IO		
	Enable Event Recording	•	

Figure 7-33 Intelligent Analysis screen

- Step 2 Select one action to set the alarm.(Intrusion, Line crossing, Single virtual fence, Double virtual fences, Object left, Object removed, Signal bad, Loiter, Multi loiter, Abnormal speed, Converse, Illegal parking, Personnel count, Fence, Enter area, Leave area, Advanced).
- Step 3 Select a channel from the drop-down list of channel.

101

Step 4 Click **(** to enable intelligent analysis alarm.

Step 5 Enable the event actions include: push message to App, pop up message to monitor, send Email, buzzer, FTP, PTZ, full screen, alarm out, camera alarm out, enable remote IO, event recording and so on.

Step 6 Click Schedule page to access the schedule screen.

Step 7 For details, please see Figure 7-23Step 5 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.

🛠 System	Channel Record A	arm Network System			×
▶ General	Perimeter Single Virtual Fend	e Double Virtual Fences Multi Loitering	g Wrong Way People Counting		~
▷ Motion Detection	Channel	(3)Channel03			
> Video Loss	Envible	Ð			
⇒ Akirm h	CEVent Actions	stection Area 🛗 Schedule			
⊳ Abnormal Alarm	2022-04-26 11:08.44		Enable OSD	Ð	
15 Alarm Out	- the		Counting Clear Interval	1Day	
> Local Intelligent Analysis			Ares Type	Line	
	1.0	Sales Harris	Set Correction Value	۲	
			Over Perpla Number Alarm	•	
		ALL NO	Alarm Threshold	1000	
	Control 1	A STATEMENT			
	- A->Bis out				
	- B->A is in				
				Apply	

Figure 7-34 Personnel count

Table 7-6 Personnel count parameters

Parameter	Description	Setting
Enable	Click the button to enable personnel count.	[How to set] Click Enable to enable. [Default value] OFF

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

----End

7.3.5 Alarm In



This function requires access to a camera that supports external alarm in.

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

Operation Description

Click **Alarm in** in the main menu or menu of the alarm management screen and choose **Alarm** in to access the alarm in screen, as shown in Figure 7-35.

🛪 System	Channel Record Alarm	Network System	×
.≽ General	Alarm In Carnera Alarm In		
 Motion Detection Video Loss 	Alarmin		
	Enable Alarm In Normal State	N/0	
> Intelligent Analysis > Alarm In	Port Name		
Abnormal Alarm	G Evint Antiwei 🛛 🖨 Scherke		
⊳ Alarm Out	Push message to APP Popus message to monitor	0 (1)	
▹ LocalIntelligent Analysis		•	
	PTZ Enable Alarm Out	•	
	Endle Event Recording	•	
			Apply

Figure 7-35 Alarm in screen

Figure 7-36 Camera alarm in

🛠 System	Channel Record Alerm	Network System		×
≽ General	Alarm In Comora Alarm In			
▶ Motion Detection	Channel	[1]ChannelU1		
Video Loss	Alamin			
	Normal State			
⇒ Intelligent Analysis	Enable Alarmin	۲		
 Alarm In Abnormal Alarm 	🔁 Evant Action 🔲 Schedu	le.		
 Abrm Out 	Email	Ð		
		©		
		O		
 Local Intelligent Analysis 		Ð		
	Full Screen	\odot		
	Enable Alarm Out	O		
	Enable Camera Alarm Out	Ð		
	Enable Remote IO	Ð		
	Enable Event Recording	Ð		

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: push message to App, pop up message to monitor, send Email, buzzer, FTP, PTZ, full screen, alarm out, camera alarm out, enable remote IO, event recording and so on.
- Step 6 Click **Schedule** page to access the schedule screen. For details, please see 7.2.1 Record Schedule Figure 7-17Step 5 Set the record schedule.

Step 7 Click Apply to save settings of Alarm in.

7.3.6 Abnormal Alarm

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

105

Operation Description

Step 1 Click **Abnormal Alarm** in the main menu or menu of the alarm management screen and choose **Abnormal Alarm** to access the abnormal alarm screen, as shown in Figure 7-39.

🛠 System	Channel Record Alarm	Network System	×
> General	Abnormal Alarm		
 Motion Detection Video Loss 	Enable Abnormal Alarm Abnormal Type		
⇒ Intelligent Analysis ≫ Alarm In			
	Pushmessage to APP	3	
 ▶ Alarm Out ▶ Local Intelligent Analysis 	Papup message to monitor Email Rutzor Enable Alarm Cur Enable Hemote IO	3 D D D	
			Apply

Figure 7-37 Abnormal alarm screen

Step 2 Tick the abnormal actions.

Step 3 Enable the event actions include: push message to App, pop up message to monitor, send

Email, buzzer, alarm out, enable remote IO and so on.

Step 4 Click Apply to save abnormal alarm settings.

7.3.7 Alarm Out

7.3.7.1 Alarm Out

Choose one output ID as the output interface.

Figure 7-38 Alarm out

🛠 System	Channel Record Alarm	Network System	×
> General	Alarm Out Camora Alarm Out		
> Motion Detection > Video Loss > Intelligent Analysis > Alarm In > Alarm In	Port Namber Port Name Valid Signal Alarm Output Mode	1 Name Close Switch Mode	
 Nami Out: Local Intelligent Analysis 			
			Арруу

----End

7.3.7.2 Camera Alarm out

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

🛠 System	Channel Record Alarm	Network System	×
⇒ General	Alarm Out	Flashlight Alarm Out	
⋟ Motion Detection	Chamel	(1)ChameU1	
⊳ Video Loss	Port Number		
> intelligent Analysis	Port Name		
⊳ Alarm In	Valid Signal	Close	
 Abnormal Alarm 	Alarm Output Mode	Switch Mode	
	Alarm Time(ms)(0:Continuous)		
Local Intelligent Analysis			
			Apply

Figure 7-39 Camera alarm out

Table 7-7 Camera alarm out

Parameter	Description	Setting
Alarm Output	ID of the alarm output channel. NOTE The number of alarm output channels depends on the device model.	[Setting method] Select a value from the drop-down list box. [Default value] 1
Name	Alarm output channel name.	[Value range] 0 to 32 bytes
Valid Signal	The options are as follows: Close : An alarm is generated when an external alarm signal is received. Open : An alarm is generated when no external alarm signal is received.	[Setting method] Select a value from the drop-down list box. [Default value] Close

Parameter	Description	Setting
Alarm Output Mode	When the device receives I/O alarm signals, it will send the alarm information to an external alarm device in the mode specified by this parameter. The options include the switch mode and pulse mode.	[Setting method] Select a value from the drop-down list box. [Default value] Switch Mode
	NOTE If the switch mode is used, the alarm frequency of the device must be the same as that of the external alarm device.	
	If the pulse mode is used, the alarm frequency of the external alarm device can be configured.	
Alarm Time(ms) (0: Continuous)	Alarm output duration. The value 0 indicates that the alarm remains continuous valid.	[Setting method] Enter a value manually. [Default value] 0 [Value range] 0 to 86400 seconds
Manual Control	Control the alarm output.	N/A

----End

7.3.8 Local Intelligent Analysis

7.3.8.1 General

At "Alarm > Local Intelligent Analysis > General" interface, enable the local intelligent analysis to set the local intrusion, as shown in Figure 7-40.

🛠 System	Channel Record Alarm	Network System	×
⊳ General	Perimeter		
 Motion Detection Video Loss Intelligent Analysis Abrem In Abrormal Alarm Alarm Out Loss Intelligent Analysis 	Enable Fraithe Draw Rect Modo Charnel	C Detection mode 2 2 2 5 5 7 8 the device will reboot+	
			Apely

Figure 7-40 Local intelligent analysis - General

Enable the alarm function.

Enable Draw Rectangle, the detection rectangle will be shown on the live video of intrusion.

Choose the channels, support up to 4 channels.

Enable or disable the intrusion, modify the channels, click the "Apply" and the device will be rebooted.

7.3.8.2 Intrusion

At "Alarm > Local Intelligent Analysis > Intrusion" interface to set the parameter of local intrusion.

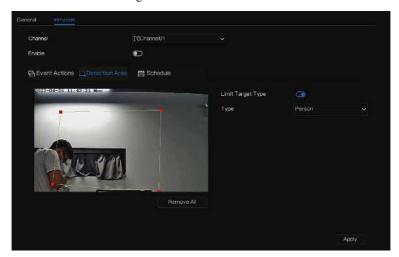
The "Intrusion" refers to that an alarm is generated when the targets of specified types (such as person, car, and both person and car) enter the detection area.

Figure 7-41 Intrusion

General	General Intrusing		
Motion Detection	Channel	[1]Channel01 v	
Video Loss	Fneble	۲	
Intelligent Analysis	Event Actions	Area 📋 Schedule	
Alarm In	Push message to APP		
Abriormal Alarm	Propup message to monitor	O	
Alarm Out	Email	\odot	
	Buzzer	O	
		۲	
		Θ	
		Đ	
	Enable Alarm Out	Ο	
	Enable Camera Alarm Cut	۲	
	Enable Remote IO		
	Enable Event Recording	0	

Event action:

Choose the channel to enable the intrusion, enable the event actions (such as push message to App, Pop up message to monitor, Email, Buzzer, FTP, PTZ, Full screen, Alarm out, Camera alarm out, enable remote IO, Event recording, and so on). Click "Apply" to save the settings. Figure 7-42 Detection area



Detection area:

Move the cursor to the drawing interface and click to generate a point, move the cursor to draw a

line, and then click to generate another point. This is how a line is generated. In this way,

continue to draw lines to form any shape, and right-click to finish line drawing.

A drawn line cannot cross another one, or the line drawing fails.

Any shape with 8 sides at most can be drawn.

The quantity of detection areas is not limited yet and will be described in future when a limit is applied.

Choose Limit target from the drop-down list, person/ person or car / car.

Chanr	el)Channe							
Frvible					e	D							
ΒEV	ent A	ctions	[]]Dete	ction Ar	88								
	42										20	24	
Sun		let thin					a sian	< Altered					
Mon	45				o sua o						00700		
Tuc	44												
Wed									Par Pille				
	44												
					27 M H								
Sat	4	et al sub			SUL.	ur oligie.				111			

Figure 7-43 Set schedule

Set schedule:

Method 1: Click left mouse button to select any time point within 0:00-24:00 from Monday to Sunday as shown in Figure 7-63.

Method 2: Hold down the left mouse button, drag and release mouse to select the schedule within 0:00 -24:00 from Monday to Sunday.

When you select time by dragging the cursor, the cursor cannot be moved out of the time area. Otherwise, no time can be selected. Method 3: Click in the schedule page to select the whole day or whole week. Deleting schedule: Click again or inverse selection to delete the selected schedule. ----End

7.4 Network Management

Set the Network Parameter, 802.1X, DDNS, E-mail, Port Mapping, P2P, IP Filter, SNMP 3G/4G and PPPOE, Network Traffic in the network management screen.

Operation Description

Step 1 Click **Network** in the main menu (or click the network page of any function screen in the main menu) to access the network management screen, as shown in Figure 7-44.

Figure 7-44 Network management screen

🛠 System	Channel Record Alarm	Network System	×
	Port POE		
> 602.0X > DDNS > Port Mapping > Email > P2P > IP Filter > SNMP	DI IOP P Address Subnet Mask Default Gateway Obtain DNS Automaticatly Preferrari DNS Server Alternatic DNS Server	102 168 32 149 256 255 0 0 102 168 0 1 109 168 32 254	
 POE Status Network Traffic Platform Access 			Apply

7.4.1 Network

Set DHCP and DNS manually or automatically.

7.4.1.1 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 a new address.

Step 5 Click Apply to save IP settings. ----End

7.4.1.2 Port

Operation Steps

Step 1 Click Port page to access the port setting screen, as shown in Figure 7-45.

Figure 7-45 Port setting screen

🛠 System	Channel Record Alam	n <u>Network</u> System	×
	P Port POE		
> B02.1X > DDNS	HTTP Port		
» Port Mapping	RTSP Port	554	
> Email > P2P	Control Port	30001	
> P Filter			
⊳ SNMP			
> POE Status			
> Network Traffic			
> Platform Access			
			Apply

Step 2 Set the HTTP port, HTTPS port, RTSP port and Control port.

Step 3 Click Apply to save port settings.

7.4.1.3 POE

Operation Steps

Step 1 Click POE page to access the POE setting screen, as shown in Figure 7-46.

🛠 System	Channel Record Alarm <u>Network</u> System	×
	IP Port POE	
 b 802.1X b DDNS b Port Mapping b Email p. P2P p. IP Filter 	Auto Manage For Poli: Camera IP Ankiness IP Ankiness Submot Mask 266: 256: 0 0 Default Gateway 99: 254: 10 1 *The PCE parameters are modified and the perior will inducet*	
 > SNMP > POE Status > Network Traffic 		
 Platform Access 		yiqA

Figure 7-46 POE screen

Step 2 The NVR will deploy IP addresses to the cameras connected to POE immediately.

Step 3 Click Apply to set POE camera IP address successfully.

----End

7.4.2 802.1 X

Operation Steps

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

System Channel Record Alarm Network System Network BD2.1X	×
> Network B021X	
> 802.1X Ca	
> DDNS User Distribution	
> Port Mapping Password Password ++++	
> Enail	
> P2P	
⊳ P ∩iter	
⇒ SMMP	
> POE Status	
p- Network Traffic	
> Pletform Access	
	Apply

Figure 7-47 802 1 X

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 NVR need to input account to certify.

----End

7.4.3 DDNS

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

Operation Steps

- Step 1 Click **DDNS** in the main menu or menu of the network management screen and choose **DDNS** to access the DDNS screen.
- Step 2 Click next to **Enable** to enable the DDNS function. It is disabled by default, as shown in Figure 7-48.

🛠 System	Channel Record Alam	n <u>Network</u> System	×
> Network	DDNS		
⇒ 802.1X	Enable DONS	0	
	Protocol	na_p 🗸	
▷ Port Mapping			
⊳ Email	Domain Name	dvr.ddns.net	
▶ P2P	User		
> P Filter	Password	Massword	
> SNMP			
p⊢POE Status			
⊳ Network Traffic			
> Platform Access			
			Apply

Figure 7-48 DDNS setting screen

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

Step 4 Set domain name, input user and password.

Step 5 Click Test to check the domain name.

Step 6 Click Apply to save DDNS network settings

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

----End

7.4.4 Port Mapping

7.4.4.1 Port Mapping

Operation Steps

Step 1 Click **Port Mapping** in the main menu or menu of the network management screen and choose **Port Mapping** to access the port mapping screen, as shown in Figure 7-49.

🛠 System	Channel Record Alarm	Network System	×
▶ Network	Port Mapping NAT Port		
⊳ 802.1X	Enable Port Mapping	0	
> DDNS	Mode		
	HTTP Port		
> Email	HTTPS Parl		
> P2P	RTSP Part		
> P Filter	Control Port		
> SNMP	Port range [1025-65534]		
> POE Status			
> Network Traffic			
> Platform Access			
			Apply

Figure 7-49 Port mapping setting screen

Step 2 Select UPnP enable type.

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

Step 4 Auto UPnP: device obtain the port automatically.

Step 5 Click Apply to save settings. ----End

7.4.4.2 NAT Port

NAT Port (Network Address Translation). Access the NVR channels through the NAT port. Users can set the start port, and it will generate the end port automatically. We will view the NAT port

when we access the channel through clicking $\angle e^{\cdots}$ icon at Web interface.

🛠 System	Channel Record Alarm	Network System	×
⊳ Network	Port Mapping NAT Port		
⊳ 802.1X	Start Port	40001	
⊳ DDNS	EndPort		
	Port range [40001-65534]		
> Email	i-ou ranĝa [acooeposa-]		
⊳ P Filter			
⊳ SNMP			
POE Status			
> Network Traffic			
> Platform Access			
			Арру

Figure 7-50 NAT port

----End

7.4.5 Email

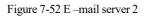
If the simple mail transfer protocol (SMTP) function is enabled, the device automatically sends alarm information to specified email addresses when an alarm is generated. Two mailboxes can be set as receivers.

Operation Steps

Step 1 Click **E-mail** in the main menu or menu of the network management screen and choose **E-mail** to access the E-mail screen, as shown in Figure 7-51.

🛪 System	Channel Record Alarm	Network System	>	<
⊳ Network	Email Server 1 Email Server 2			
ı⊳ 902,1X	SMTP Server			
⊅- DDNS	SMTP Server Port			
Port Mapping	Usomamo			
≱ Email	Password			
p P2P	Email Sender			
▷ IP Filter	Alerm Receiver 1			
⊳.SNMP	Alarm Receiver 2			
	Alarm Receiver 3			
NARAWARKA	SSL Encryption			
⊯ POE Status	Sending Interval(0-600s)			
> Network Traffic		Test		
 Platform Access 				
			Apply	

Figure 7-51 E-mail setting screen



SMTP Server		
SMTP Server Port		
Usemane		
Password		
Email Sender		
Alarm Receiver 1		
Alarm Receiver 2		
Alarm Receiver 3		
SSL Encryption	CFF	
Sending interval(0-600s)		
		Ap

Step 2 Set SMTP server address and SMTP server port manually.

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

- Step 4 Set E-mail for receiving 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, E-mail is set successfully.

Step 6 Set SSL encryption for encrypting mail or not, set sending interval.

Step 7 Click Apply to save settings. ----End

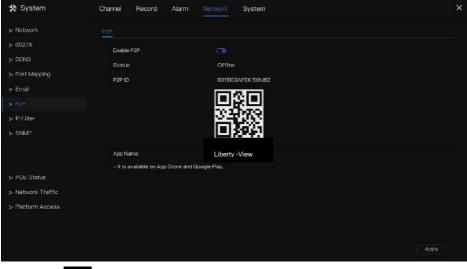
7.4.6 P2P

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 7-53.

Figure 7-53 P2P screen



Step 2 Click to enable the P2P function.

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

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

----End

7.4.7 IP Filter

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

Operation Steps

Step 1 Click IP Filter in the main menu or menu of the network management screen and choose

IP Filter to access the IP filter screen, as shown in Figure 7-54.

Figure 7-54 IP Filter setting screen

🛠 System	Channel Red	ord Alarm	Network Syste	am		×
▷ Network	IP Fillor					
⊳ 802.1X	Enable P Filte		C			
> DDNS	Ruio Type		Black List			
▶ Port Mapping	Black List(Fo	lowing network segn	ients are forbidden)			
> Enal		Start IP		End IP	Edit	
⊳ P2P						
▶ SNMP						
» POE Status						
» Network Traffic						
> Platform Access						
	+ -					
						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 **set** to set black & white list IP segment screen is displaying, as show in Figure 7-

55.

Figure 7-55 IP Address Segment screen

Start IP		
End IP		

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: A list of IP addresses in specified network segment that are regarded as unacceptable or untrustworthy and should be excluded or avoided.

White list: a list of addresses in specified network segment considered to be acceptable or trustworthy.

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

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

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

----End

7.4.8 SNMP

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

Operation Steps

Step 1 Click **IP Filter** in the main menu or menu of the network management screen and choose **IP Filter** to access the IP filter screen, as shown in Figure 7-56.

🛠 System	Channel Record Alarr	m Network System	>
Network	SMMPV1/2 SNMPV3		
5 602.1X	SNMPV1		
> DONS	SNMPV2C		
Port Mapping	Write Community		
∘ Email	Read Community		
≥ P2P	Trap Address		
⊳ IP Filter	Trap Port	152	
	Trap Community		
> POE Status			
 Network Traffic 			
 Platform Access 			
			Apply

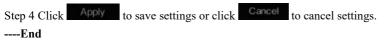
Figure 7-56 SNMP settings screen

Step 2 Click next to **SNMPV 1** to enable the function . The interface is shown as Figure 7-59.

SNMPV1		
SNMPV2C	۲	
Write Community		
Read Community		
Trap Address		
Trap Port		
Trap Community		

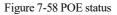
Figure 7-57 SNMPV 1/2 interface

Step 3 Input the parameters of protocol.



7.4.9 POE Status

Users can view the status of POE intuitively, as shown in Figure 7-58.





----End

7.4.10 Network Traffic

Users can view the network traffic immediately, as shown in Figure 7-59

* System	Channel R	ecord Alarm	Network	System	×
⊳ Network	Natwork Traffi	q			
⊳ 802,1X					
⊳ DDNS	16Mbps				
▷ Port Mapping					
⊳ Email					
▶ P2P	8Mbps				
⊳ IP Filter					
⊳ SNMP					
	0 LAN1				
POE Status	Forth				
> Platform Access			Status	MAC Address	Display
			Online	00:1C:27:18:F8:7A	

There are two rates, transmit rate and receive rate. The status of LAN(s) show on list.

----End

7.4.11 Platform Access

If the NVR and platform system are not at the same local network, ensure the NVR is connected to the same external server as the platform system. You should build a server for platform in advanced, platform's remote IP/Port and NVR are mapping port to external network.

Step 1 Choose Configuration > Network Service > Platform Access.

The Platform Access page is displayed, as shown in Figure 7-60

🛪 System	Channel Record Alarm	Network System	×
⊳ Network	Platform Access		
> 6021X > DDNS > Port Mapping > Enuil > P2P > IP Filter > SNMP	Envible URL Port Usar Password Encrypt	C3 LRL User name Passeorr	
 Network Traffic ⇒ Platform Access 			
			Apply

Figure 7-60 Platform Access page

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

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

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

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

🛪 System Channel Record Alarm Network. Channel Device D D011003AFEK109U62 Device Name Device Device Type NVP Model L3NVR8POE v4.6.1604.0000.003.0.136.0 U-boot Version 1504010C0F18 Kernel Version 15060511183A » Auto Roboot HDD Number Channels Supported Alarm Out Audio In Audio Out

Figure 7-61 IP/ID/Domain

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

Figure 7-62 Connect NVR to platform

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

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

Figure 7-63 URL address / port

Basic Inform	nation			O Refeish @ Back O Bestone ∠ fuit - X Delere
Server Name :			12/.001-1000	24art-up intel; 2002-04-11:1515651
Running States	Osisc	Resource (P.Dont)		Codine Time : 4465 15045 5666
tog Type i		Device registration (1011)	17838	551 (Avr.) 15685
Demain :	Default Domain	Service device registration po	#:	

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

Step 6 Click Apply.

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

----End

7.5 System Management

View the device **Information** and set **General** information, **User Account**, **Security Center**, **Layout**, **Logs**, **Maintenance** and **Auto Reboot** for the system setting.

Operation Description

Click **System** in the main menu (or click the system page of any function screen in the main menu) to access the system setting screen, as shown in Figure 7-64.

Information System Network Channel Diek Ahrm > General Device D BUTRUSAL-EK199052 <th>🛠 System</th> <th>Channel Record Alarm Network</th> <th>×</th>	🛠 System	Channel Record Alarm Network	×
Device D BUTRUDAL-EK 1980/62 >- User Account Device Name Device Name Device > Sacurity Center Device Type > Layout NVR		System Network Channel Disk Alarm	
Auxiliary Screen Firmware Version VALUEPOE > Logs U-boot Version V4.6.1904.0000.003.0.136.0 > Maintenance U-boot Version 150401000°16 > Auxio Roboot HDD Number 2 Charnels Supported 8 Alarmin Alarmin Cuit 1 Audio Intension Audio Int 1 Audio Intension	> General > User Account > Security Center > Layoul > Auxiliary Screen > Logs > Maintenance	Device ID BUTRUUSAFEK108U62 Device Name Device Device Type M/R Modul LINVREPOE Firmware Version V4.6.1004.000.003.0.136.0 U-boot Version 1504.010007.18 Kernel Varsion 1504010007.18 HDD Number 2 Chamels Supported 8 Alarm In 0 Alarm Out 1	

Figure 7-64 System setting screen

7.5.1 Information

View the device ID, device name, device type, model, firmware version, kernel version, face detection version, HDD volume, channel support, alarm in, and alarm out, audio in, audio out in **information** screen, as shown in Figure 7-65.

Device Name Device Type NVR NVR NVR Type NVR Lasvy Firmware Version V4.0.1 U-boot Version 15040	IUGA/LK/09U62 In IRNFOE IRNFOE INCOL0000.003.0,130.0 IDCOF16
Device Type NVR Mudel L3NV Firmware Version v4.6.3 U-boot Version 15040 Kernet Version 15060 HDD Number 2	RSPOE
Model LINV Firmware Version v4.6.1 U-boot Version 55640 Kernel Version 5660 HDD Number 2	804.000.003.0.136.0
LISV Firmware Version v4.0.1 U-boot Version 15040 Kernel Version 15060 HDD Number 2	804.000.003.0.136.0
U-boot Version 15040 Kernel Version 15060 HDD Number 2	
Kernel Version 15060 HDD Number 2	1000F18
HDD Number 2	
	05111B3A
Channels Supported 8	
Alarm In 8	
Alarm Out 1	
Audio In 1	
Audio Out 1	

Figure 7-65 Information-system interface

Network: status, IP address, subnet mask, default gateway, MAC address, DHCP, preferred DNS server, Alternate DNS server, total band width, received packets, and so on, as shown in Figure 7-66.

System <u>Network</u> Channel	Diak Alarm
Status	Online
IP Address	192168.32149
Subnet Mask	255,255,0,0
Default Gateway	192.168.0.1
MAC Address	00:1C:27:16:F5:7A
DHCP	OFF
Preferred DNS Server	192168.32.254
Alternate DNS Server	
Total Bandwidth	1000.00 Maps
Received Packets	11.53 Mbps

Figure 7-66 Information-network interface

Channel: channel, name, status, video format, resolution, bitrate (kbps), and so on, as shown in Figure 7-67.

Dame Estatus Vision Format: Estatus Estatus CH Obanuelli Otanu Hote/Estatus Edit/1065 Edit/1067/04576 4656/024 D2P Obwenit/P Hifter Hote/Hote/Estatus Edit/1068 Edit/1061/047576 4656/024 D2P Obwenit/P Hifter Hote/Hote/Estatus Edit/1061/047576 4656/024 D4 Chowenitis Chowenitis Edit/1068 Edit/1068 2656/1024/024 CH Chowenitis Ofen Hote/Hotes 2656/1025 2557/680/704/963 4006/024 CH Chowenitis Ofen Hote/Hotes 1026/1425 1026/1680 4006/024 CH Chowenitis Ofen Hote/Hotes 1026/1425 1026/120/024 2000/024 CH Chowenitis Unit### Hote/Hotes 1026/1425 2000/024 2000/024 CH Chowenitis Unit## Hote/Hotes 3026/1425 3020/0707/07570 3000/024 CH Chowenitis Otalex85 3026/07007/0	lystem	Notwork <u>c</u>	Disk	Alarm		
D-27 Cheered/2 Effense F10990/LPAA Stitut/TM02/20/93/96 4004/199 D-31 Cheered/2 Debr H.396/H.485 Stitut/TM02/20/93/96 4004/199 D-41 Chevred/2 Debr H.396/H.485 Stitut/TM04/96 4004/199 D-45 Chevred/2 Debr H.305/H.205 Stitut/TM04/96 4004/199 D-45 Chevred/2 Debr H.305/H.205 9529/H.201/34/93 4004/024	Charnal			Viceo Format		Bitrate0dopo)
Cheverentics Cheverenics Cheverentics Cheverentics </td <td></td> <td>Channel01</td> <td>Online</td> <td>H.265/H.265</td> <td>000*1060/704*576</td> <td>4036/1024</td>		Channel01	Online	H.265/H.265	000*1060/704*576	4036/1024
CH4 Charveto4 Craine H355/H325 2592*6207/04*040 4496/7024 G=6 Charveto5 Craine H355/H305 H320*E30/70#430 4606/024 G=6 Charveto5 Craine H355/H305 H320*E30/70#430 4606/024 G=6 Charveto5 Craine H305/H305 H305/H305 H305/H305 G=6 Charveto5 Craine H305/H305 H305/H305 H305/H305		Chemel 12				
Ch-6 Charvellot Crefm H305/H205 H302/H205 H302/H205 4000/1024 CH-6 Charvellot Unit# H305/H205 JOINT 100/J01/200 S000/1025		Channel38				
0-13 Chemel(6 Unive 11/2/5,11/25 70.4*180/5/240 20/0)/1/24		Channel64				
		Chamel05	Crief-rei	H.265/H.265	102011080/704+480	
CH8 ChemeK8 DIThie H255/H255 98404280/7254576 4696/768		Channel06	Online			
	049	ChanneR66			084042360/7204578	

Figure 7-67 Information-channel interface

Disk: disk name, capacity, used, SN, disk model, status, and so on, as shown in Figure 7-68

Figure 7-68	Information-disk interface
-------------	----------------------------

System Notw	ork Channel	Dok Alton		
	Capacity			
Diskt.	12 TB		5GJ&VD9B	Normal
Disk2			26A0RABD	Normal

Alarm: channel, name, mode, enable, recording channel, and so on, as shown in Figure 7-69.

lystom	Network	Channel	Disk Alarm		
Cha		Name	Mode.	Enable	Recording Channel
	ik-1	Sensor 1			
Loca		Sensor 2			
Loca	ik-3	Sensor 3			
Loca		Sensor 4			
Loca	#⊢>1		Close		

Figure 7-69 Information-alarm interface

----End

7.5.2 General

7.5.2.1 System

Operation Steps

Step 1 Click **General** in the main menu or menu of the system management screen and choose **General** to access the system screen, as shown in Figure 7-70.

🗙 System	Channel Record Alarm	Network System		
Information	System Date And Time	Tima Zona DST Syna	Camera Time	
	Device Name	Device		
5 Liser Account	Output Resolution	1920×1080		
 Security Center 	Language	English		
⊳ Layout	Temperature Unit	Celsius		
Þ Logs				
> Maintenance				
Auto Reboot				
				Apply

Figure 7-70 system setting screen

Step 2 Enter the name of the selected device.

Step 3 Select a proper resolution from the output resolution drop-down list.

Step 4 Select a required language from the Language drop-down list.

Step 5 Set the temperature unit.

Step 6 Click Apply to save settings.

7.5.2.2 Date and Time

Operation Steps

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

7-71.

	Date Format	DD/MM/YY Hitmmiss	
Liser Account	Time Format		
Security Center	Enable NTP	Q	
> Layout	NTP Server	time.windows.com	
	Sync Time Frequency (sec)	86400	
	Dete		
> Maintenance	Time		
> Auto Reboot			
	- Time modification will cause the	channel to reconnect	
	- Time modification will affect vid	ao avery	

Figure 7-71 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 use the scroll wheel to select the year, month, and date.

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

Click Modify Time to save the time settings.

Step 5 Click Apply to save settings.

----End

7.5.2.3 Time Zone

Operation Steps

Step 1 Click Time zone page to access the time zone setting screen, as shown in Figure 7-72.

🛠 System	Channel Record Alarm Network System	x
> Information	System Date And Time Time Zone DST Sync Comoro Time	
	Time Zone (GMT+00:00) Dublin, Edinburgh, Lo. v	
> User Account		
> Security Center		
> Layout		
> Logs		
> Maintenanca		
» Auto Reboot		
		Actoly
		10661/

Figure 7-72 Time zone setting screen

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

Step 3 Click Apply to save settings.

7.5.2.4 DST

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

Operation Steps

Step 1 Click DST page to access the DST setting screen, as shown in Figure 7-73.

	1 igure 7-75 D5	1 bound boroom
🛠 System	Channel Record Alarm Netwo	ork System X
> Information	Systam Date And Time Time Zone	05T Sync Camora Timo
	Enable Daylight Saving Time	G
» Liser Account	Start Time Mar	✓ Last one ✓ Sun → 100 ✓
Security Center	End Time Oct	v Lastone v Sun v 100 v
> Layout	Offset Time 1Hour	
» Maintenance		
> Auto Reboot		
		Aggiy

Figure 7-73 DST setting screen

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

Step 3 Select start time, end time, offset time from the drop-down list respectively, that basis on

the local rules.

Step 4 Click Apply to save settings.

----End

7.5.2.5 Sync Camera Time

Enable the sync camera time, the channels will show the sync time, and set the frequency of check

System	Date And Time	Timo Zono	DST	Syna Camero Timo
Enable	Sync	G		
Sync Ti	ime Frequency (sec)		10	

----End

7.5.3 User Account

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

7.5.3.1 User

Operation Steps

Step 1 Click User in the main menu or menu of the system management screen and choose User to access the user screen, as shown in Figure 7-74.

🛠 System	Channel	Record Alarm	Network				×
Information	Usor	Adv.Setting App. V	erification				
⊳ General		Useman	ia.	Grau	p	Operate	
		admin		Super a		۷	
> Security Center							
⊳ Layout							
Auxiliary Screen							
⊳ Logs							
> Maintenance							
> Auto Reboot							
						Add	

Figure 7-74 User management screen

Step 2 Add or delete a user.

Add a user

Click Add, the Add User dialog box appears, as shown in Figure 7-75. Figure 7-75 Add user screen

Password			
Confirm Password			
	Administrat	ors	
Change Password Frequency	Never		Ŷ
Password Expire Date	۲		
🛛 Live Freview	3	Channel	
PTZ	2	CHI	
	2	CH2	
🗑 Playback	<u> </u>	CH3	
Channel Management	2	CH4 CH5	
😴 Device Management		CHS	
Cevice ivial agement		CH7	
🛃 System Management	÷.	CH8	
Backup	Live Previe		

139

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

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

The password should be 6~32 characters long.

- Step 3 Select a Group from the drop-down list box.
- Step 4 Select a Change password reminder value from the drop-down list box.
- Step 5 Enable the expire date to set the new user's authority time.
- Step 6 Select the operation privileges and channels in the list of the add user screen.
- Step 7 Click OK. The user is set successfully.

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

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

----End

7.5.3.2 Advance Setting

Operation Steps

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

🛠 System	Channel Record Alarm	Network System	×
> Information	User . <u>Adv.Setting</u> . App Veri	fication	
> General	Enable Double Authentication	Ð	
	Enable Setup Wizard	a	
> Security Center	Enable Auto Login		
	Auto Logoal Time (min)	5	
> Auxiliary Screen			
⊳ Logs	Monitor channel(s) when logout		
> Maintenance			
⊳ Auto Reboet			
			Apply

Figure 7-76 Advance setting screen

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

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

Step 4 Click Apply to save settings.

-----End

7.5.3.3 App Verification

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

X System	Channel	Record Alarm N	Vetwork System		
Information	Liser A	dv.Sotting APP V			
> General	Enable V	/hite List	3		
		Phone Number	Status	Remark,	
> Security Center					
> Layout					
		Phone Network			
Maintenance		Remark(options			
Auto Reboot					
			CK .	Candel	
	1	_			
	T S	72			

Figure 7-77 App verification

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

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

Click Apply to save the setting. ----End

7.5.4 Security Center

7.5.4.1 Password

Operation Steps

Step 1 Click **Security Center** in the main menu or menu of the system management screen and choose **Password** to access the modify password screen, as shown in Figure 7-78.

🛪 System	Channel Record	Alarm Network	System	×
> Information	Password Pattern Uni	ock Socure Email	Secure Question	
 Filtermation General User Account Security Center Layout Auxiliary Screen Logs Metritermose Auto Relatort 	Old Password New Password Confirm Password – Valid password range – At least 2 kinds of run	Passw Paniw Pascw 6–32) characters, bers,lowercase, uppercas		
				Асру

Figure 7-78 Password modification screen

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



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

The password should be $6 \sim 32$ characters.

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

Step 3 Click Apply to save modified password settings.

----End

7.5.4.2 Pattern Unlock

Operation Steps

Step 1 Click Security Center in the main menu or menu of the system management screen and choose Pattern Unlock to access the modify pattern unlock screen, as shown in Figure 7-79.

🛠 System	Channel Record Alarm	Network System	×
⊳ Information	Password Pattern Unlock	Secure Email Secure Question	
⊳ General	Password		
> User Account	Enable Pattern Unlock	•	
	Pattern Unlock	Pattern Setting	
▶ Layoul			
 Auxiliary Screen 			
.p. Logs			
⊳ Maintenance			
⊳ Auto Roboot			
			Apply
			C1407

Figure 7-79 Pattern unlock screen

Step 2 Input the password, enable pattern unlock.

Step 3 Click Setting Pattern to set an new pattern unlock.

Step 4 Draw the pattern, then it will remind to draw the confirmation pattern again.

Step 5 Click OK to save the pattern unlock.

----End

7.5.4.3 Secure Email

Set the email to receive the verification code to create new password, as shown in Figure 7-80.

🛠 System	Channel Record Alam	n Network System		×
» Information	Password Pattern Unlock	Socure Email Secure Queatic	an.	
» General	Verity Password			
> User Account	Email Address			
Security Center				
» Layout				
▶ Auxiliary Screen				
⊳ Logs				
⊳ Maintenance				
» Auto Roboot				
				Αρργ

Figure 7-80 Secure Email

Step 1 Input the password of NVR.

Step 2 Set the Email address to receive verification code.

Step 3 Click Apply to save setting.

----End

7.5.4.4 Secure Question

Set the questions to create new password, as shown in Figure 7-80.

🛪 System	Channel Record Alarm N	letwork System	×
▷ Information	Password Pattern Unlock Sec	ure Email Secure Question	
▷ General ▷ User Account	Password		
	Question one answer	The brand and model of your favorix	
⊳ Layout ⊳ Auxiliary Screan	Question two	Your favorite team 🗸 🗸	
> Logs > Maintenance	Guestion three	Your favorite city 🗸 🗸	
⊳ Auto Roboot	Question three answer - Please enter at least 1 characters fo	r the answer	
	- Please enter up to 32 characters for	the enginer	
			Apply

Figure 7-81 Secure question

Step 1 Input the password of NVR.

Step 2 Choose the question from drop-down list.

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

----End

7.5.5 Layout

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

Operation Steps

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

🛪 System	Channel Record	Alarm Network System	×
▶ Information	Layout		
▶ General	Layout List	+ Layout Name: 1x1 Dwell Fime(sec); 5	∠ Edit @ Delete
≱ User Account			
> Security Center	2x2		
 Auxiliary Screen 			
⊳ Logs			
 Maintenance 		1. Channel01 2. Channel02	
		3. Chamel03 4. Chamel04	
⊳ Auto Rehoot		5. Channel05	
		6. Channel06 7. Channel07	
		8. Channel08	

Figure 7-82 Auto Sequence screen

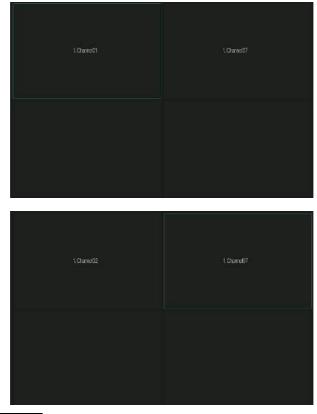
Step 2 Click "+" to add a new layout. The default layout is one splitting screen.

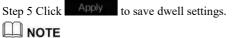
Figure 7-83 Add a new layout

+ AddLayout				×
Channel	Layout Name	Dwel Time(sec) S		
[1]Ohannel01 [2]Channel02 [3]Channel03 [4]Channel04 [5]Channel05 [6]Channel05 [6]Channel05 [7]Channel03 [7]Channel03 [4]Ehrety				
				Gancel

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

Step 4 Select split screen mode at the bottom of the page. Set the channel display by dragging the channel to specific position, or select the position first, then click the channel. A split screen can play multiple channels. Auto sequence means it will play according to the setting. For example, the first split screen is set as two pages (channel 1 and 2), the second split screen is set as one page (channel 3). When auto sequence is enabled, channel 1 and channel 3 are displayed, then channel 2 and channel 3 are displayed. Figure 7-84 Auto sequence





User can add up to 16 layouts.

----End

7.5.6 Auxiliary Screen (Only for Some Models)

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

Operation Steps

Step 1 Click Auxiliary Screen in the main menu or menu of the system management screen.

Step 2 Enable the auxiliary screen, as shown in Figure 7-87

🛠 System	Channel Record Alarm Ne	atwork. System	×
> Information	Auxiliary Scroon Layout		
> General	Enable Auxiliary Screen	0	
:> User Account	VGA Output Besolution	1020x1080	
Security Center	Maximum Channel for HDMI and VGA	414	
> Layout	Layout Mode	5x1	
	Display Page		
t> Logs	Enable Auto Sequence	۲	
> Maintenance			
⊳ Auto Reboot			
			Αρργ

Figure 7-85 Auxiliary screen

Step 3 Set the Output Resolution, Decoding Ability(main + auxiliary), Layout Mode, Display Channel.

Step 4 Enable tour to set Auto Sequence of auxiliary screen as shown in.

Advinary acroent	Latyca			
Auxiliary Serteen Layout List UI 2x2		Dwell Time(sec): 5	1. Charnel01 2. Charnel02 3. Charnel03 4. Charnel05 5. Charnel05 6. Charnel05 6. Charnel05 8. Charnel08	∠ Edit (ĝi Deens

Figure 7-86 Auto sequence of auxiliary screen

Step 5 Click Apply to save settings.

The auxiliary screen shows different channels with main screen, and the auto sequence show all channels.

The auxiliary screen will show the personnel counting information if it is enabling.

----End

7.5.7 Logs

7.5.7.1 System Log

Search for logs information and export the information of logs.

Operation Steps

Step 1 Click **Logs** in the main menu or menu of the system management screen and choose **Logs** to access the log screen, as shown in Figure 7-87.

🛠 System	Channel Re	cord Alarm	Network Sys				>
Information	System Log Ex						
> General	Start Date	24/04/2022		Start Time	15:21:16		
User Account	End Date	25/04/2022		End Time			
 Security Center 	Туре	Operation Log		Searc		Export	
Layout		Start Time	Channel	LogType		Information	
Auxiliary Screen	1 25/0	01/2022 15:02:40		Login	[admin] 127	.0.0.1 login	
- Moxiliar y Screen	2 25/0	14/2022 15:02:00		Logout	[admin] 12/	.0.0 Negaut	
		04/2022 14:40:35		Login	[admin] 127	.0.0.1 login	
 Maintenance 	4 25/0	14/2022 13:10:17		Logout	[admin] 127	.0.0.1logaut	
2 Wolffoorting G	5 25/0	14/2022 12:56:10		Login	[admin] 127	.0.0.1 login	
Auto Reboot	6 25/0	14/2022 12:39:20		Logoul	[admin] 127	.0.0.1logout	
	7 25/0	14/2022.12:32:43		Login	[admin] 727	0.0.1 login	
	8 25/0	14/2022 12:32:00		Logoul	(admin) 192	.188.0.157 logoul	
	9 25/0	14/2022 12:29:30		Logout	[admin] 127	.0.0.1 logaut	
	10 25/0	14/2022 12:14:25		Login	[admin] 192	.168.0.157 login	
	11 25/0	04/2022 12:13:41		Login	admin 127	.0.0.1 login	
		14/2022 12:07:03		Logout	[admin] 127	.0.0.1logaut	
	13 25/0	14/2022 11:4:55		Login	[admin] 127	.0.0.1 login	
	14 25/0	4/2022 11:41:50		Logout	[admin] 127	.0.0.1logeut	
	15 25/0	04/2022 11:41:49		Power On	system		

Figure 7-87 Log screen

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

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

Step 4 Click Search to query logs.

Step 5 Click Export to export logs to flash disk.

Step 6 the logs can be saved to flash disk and hard disk at the same time, the newest logs is saved

to flash disk, and the old logs will be transferred to hard disk.

----End

7.5.7.2 Event Log

Event logs are divided into more detailed types, which can be found quickly. Its operation is the same as the system log, please refer to chapter 7.5.7.1.

Information	System Log	vont Liog				
> General	Start Date	24/04/2022		Start Time	15:22:32	
⊳ User Account	End Date	25/04/2022		End Time	15.22.32	
> Security Center	Туре	AL	v Al v	Searc		Export
Layout		Start Time	Channel	Log Type		formation
> Auxiliary Screen		04/2022 15:20:18 04/2022 15:19:56	Channel05 Channel05	Motion Detection Motion Detection	Channel05 Channel05	
	3 25/0	04/2022 15:19:43	Channe/05	Motion Detection	Channo/05	
> Maintenance		04/202215:19:27 04/202215:10:15	Channel05 Channel05	Motion Detection Motion Detection	Channel05 Channel05	
⊳ Auto Reboot	6 25/0	04/2022 15:18:25	Channel05	Motion Detection	Chane/05	
		04/2022 15:17:40	Channel05	Motion Detection	Channel05	
		04/2022 15:17:26 04/2022 15:17:02	Channel05 Channel05	Mation Detection Motion Detection	Channel05 Channel05	
		04/2022 15:17:02 04/2022 15:16:37	Channel05	Motion Detection	Channel05 Channel06	
		04/2022 15:16:24	Channel05	Motion Detection	Channel05	
		04/2022 15:15:53	Channel05	Motion Detection	Channel06	
		04/2022 15:14:46	Channel05	Motion Detection	Charne/05	
	14 25/0	04/2022 15:12:11	Channel05	Motion Detection	Channel05	
	15 25/0	04/2022 15:11:00	Channel05	Motion Detection	Charmei05	

Figure 7-88 Event

7.5.8 Maintenance

Operation Steps

Step 1 Click **Maintenance** in the main menu or menu of the system management screen and choose **Maintenance** to access the maintenance screen, as shown in Figure 7-89.

🛠 System	Channel Reco	ord Alarm	Network Sys				×
> Information	Maintenanae						
⊳ General							
> User Account	()	()	\Box	Ð,	Ē,	E,	
> Security Center	Shutdown	Reboot	Logout	Reset	Import Configur.	Export Configur.	
⊳ Layout							
Auxiliary Screen	ద్రి	(P)	t₽ ⊕	∽			
> Logs		(لپ)					
	FW Update	Cloud Update	Save running log	Network Packet			
⊳ Auto Rebont							

Figure 7-89 Maintenance screen

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

	🛏 îg 🛱
Modify Date	
ск	Cancel
	Format OK

Figure 7-90 Firmware update

Step 3 Click import configuration or export configuration to view the message " Are you sure to import the configuration?" Make sure the flash driver is working.

Step 4 The tips 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 NVR finishes updating, the device would restart.

Network packet capture: the NVR is plugged into the USB disk, click the network packet capture,

and set the relevant parameters of the packet capture. The captured data can be downloaded and used for device problem analysis.

FW Update, firmware update; Plug in the U disk with the update software, choose the file to update.

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

----End

7.5.9 Auto Reboot

Operation Steps

Step 1 Click **Auto reboot** in the main menu or menu of the system management screen and choose **Auto reboot** to access the maintenance screen, as shown in Figure 7-91.

🛪 System	Channel Record Alarm	Network	System	×
> Information	Auto Roboot			
≽ General	Enable Auto Reboot	•		
» User Account	Reboot Time	Per Day	v 0:00 v	
 Security Center 				
> Layout				
> Logs				
» Maintenance				
Auto Reboot				
				Apply

Figure 7-91 Auto restart screen

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

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

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

----End

8 WEB Quick Start

The functions of Web are the same as those of UI system, all functions can be referred to chapter 7 UI system setting.

8.1 Activation

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



Step 1 Set the password, and confirm the password.

Step 2 Input the channel password.

Step 3 Set the email to recovery the password.

Figure 8-2 Email

	passw
	er email address
Next	
	Skip

Step 4 Set the question to recovery the password.

Figure 8-3 Question

Your favorite team	
Your favorite city	

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

8.2 Login and Logout

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

The win 7/ win 10 system supports Firefox/Chrome, but the XP system does not.

Brower supports 32 bits systems.

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.

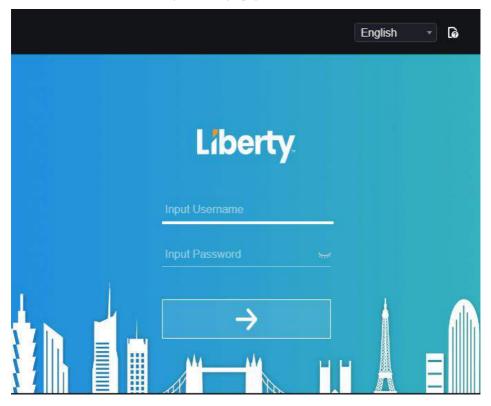
Here we take IE 10 as an example for videos viewing.

Login

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

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

Figure 8-4 Login page interface



Step 2 Input the user name and password.

The default user name and password both are admin. The password is incorrect more than 3 times, please log in 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 NVR for the first time.

Step 3 Click Login to access the homepage, as shown in Figure 8-5.

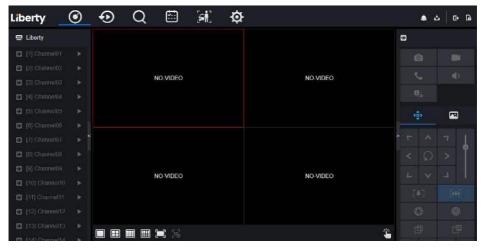
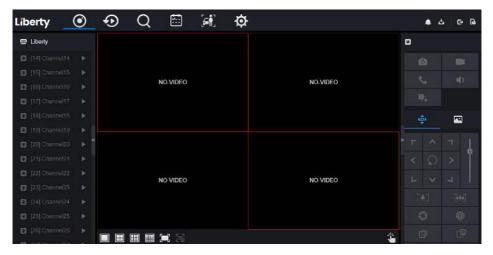


Figure 8-5 Homepage interface 1

Figure 8-6 Homepage interface 2



Logout

To logout of the system, click in the upper right corner of the homepage. The pop-up
message shows "Would you like to exit?" Click OK and the login page will display.
Homepage Layout

NVR allows you to use the Web interface in a PC for implementation of such functions as live video, playback, retrieval, setting, image parameters access, configuration, PTZ control and so on. Figure 6-8 shows the overall layout of the interface. For descriptions of the interface, please refer to Table 8-1.

Figure 8-7 Homepage layout

Liberty	۲	Ð	Q	2	ø			
Device Channel01 Channel02 Channel03 Channel04	(<mark>6</mark>)			NO VIDEO		NO MDEG		
				NO-VIDEO		ND-INDEQ		× ⊣ –
			11					

No.	Function	Description			
INO.	Function	Description			
1	Function navigation bar	Main functions navigation bar of the device, it includes Live Video, Playback, Alarm Search, Face Recognition, Attendance and System Setting.			
2	Alarm	Alarm notification. User can tick pop-up message to monitor, system alarm and channel alarm.			
3	Logout button	User can click Logout to exit the current account and return to the login interface.			
4	Help	Help for running environment, plug-in installation and activation.			
5	Device's list	Display a list of the channels of the managed NVR and the channels managed by NVR.			
6	Real-time video	Display the real-time videos of the channels managed by NVR.			
7	Channel Operation	Include snapshot, record, stream switch and audio on/off.			
8	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 uses for IP dome camera.			
9	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.			
10	Operation zone	The operation zone of PTZ control and image parameter setting.			
11	Layouts	Select the one-screen, four-screen, nine-screen or sixteen- screen to switch the layout.			
12	Manual alarm	Trigger and close the external alarm device manually.			

----End

8.3 Browsing Videos

8.3.1 Browsing Real-Time Videos

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

Preparation

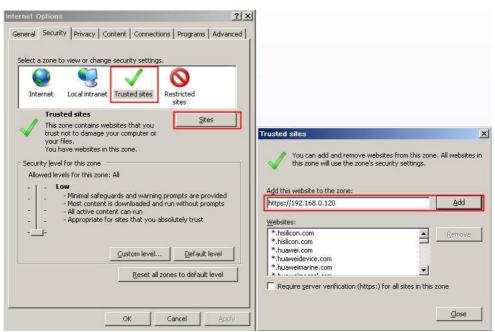
To ensure that real-time videos can be played properly, perform the following operations when

you log in to the web management system for the first time:

Step 1 Open Internet Explorer. Choose Tools > Internet Options > Security > Trusted sites >

Sites. In the displayed dialog box, click Add, as shown in Figure 8-8.

Figure 8-8 Adding a trusted site



Step 2 In Internet Explorer, choose **Tools > Internet Options > Security > Customer level**, and set Download unsigned ActiveX controls and Initialize and script ActiveX controls not

marked as safe for scripting under ActiveX controls and plug-ins to Enable, as shown in Figure 8-9.

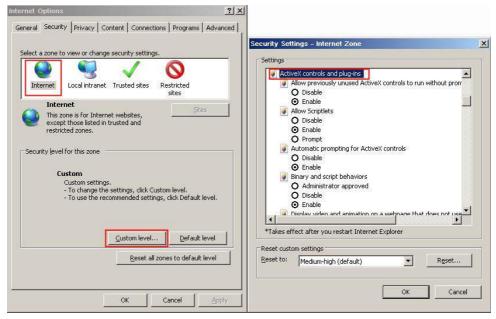


Figure 8-9 Configuring ActiveX controls and plug-ins

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

the browser.

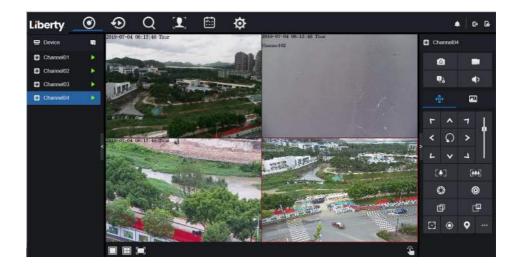
If the repair tips displayed when installing the control, close the browser and continue the installation, reopen the login page when the control is installed.

8.3.2 Live Video

Descriptions

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

Figure 8-10 Real-time videos interface



----End

8.3.3 Channel Operation

Descriptions

Channel operation includes snapshot, record, stream switch and audio on/off. Table 8-3 describes the operations.

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

8.3.4 PTZ Control and Setting

Descriptions

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

PTZ Setting

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

Click Click, the PTZ operation and setting interface is as shown in Figure 8-11. Table 8-4 describes the operations.



Figure 8-11 PTZ control interface

Table 8-4 Device parameters

Buttons	Button description	How to operate
F ^ 7 < 0 > L ~ 4	Direction key	Click button to control omni-directional movement of the PTZ.
5	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.
®	Iris-	
Ф	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, scan and tour

8.3.5 Sensor Setting

Descriptions

The sensor setting can adjust scene, brightness, sharpness, contrast and saturation, click to access image setting, as shown in Figure 8-12. Table 8-5 describes the operations.

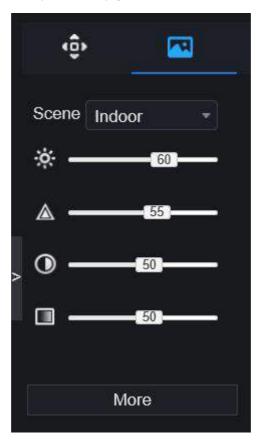
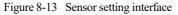


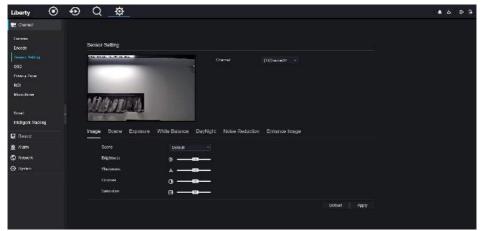
Figure 8-12 Image parameter interface

Table 8-5 Device	parameters
------------------	------------

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

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





----End

8.3.6 Layout



at the bottom left conner of real-time videos interface, the buttons

indicate 1 screen, 4 screens and 9 screens from left to right. The device with more POE ports can support 16 screens layout.

8.4 Playback

8.4.1 Video Playback

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

Procedure

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

shown in Figure 8-14.



Figure 8-14 Video playback

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

The unselected device is marked with

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

Step 4 Tick the type of record, such as schedule record, manual record and alarm record. Step 5 Display videos. After a device and date are selected, video information is displayed below the video pane. The time scale above the file axis shows the different time points of video recording. The time in blue in the middle is the time of the video playing.

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

You can drag the axis to play recording quickly.

Step 6 Play a video.

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

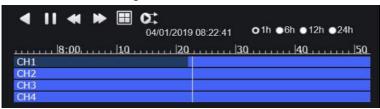


Figure 8-15 Control bar



reversed.



: triple speed.



: split screen. One or four screens.

0;

: 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 users play different time period record

●1h ●6h ●12h **0**24h

types of time bar.



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

----End

8.5 Alarm Search

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

8.5.1 Channel Alarm

Procedure

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

shown in Figure 8-16.

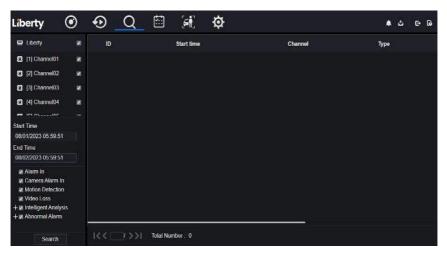


Figure 8-16 Channel alarm interface

Step 2 Choose the alarm type to search.

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

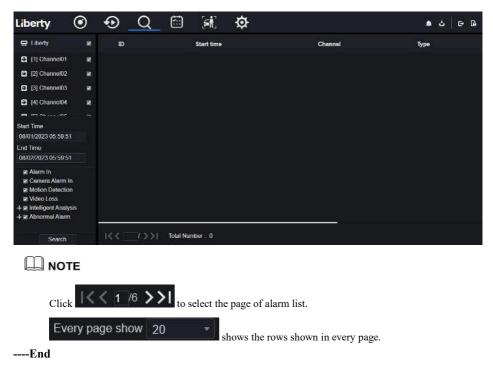


Figure 8-17 Channel alarm result

8.6 Attendance

8.6.1 Attendance Data

Click to enter attendance data interface, as shown in Figure 8-18.

175

tlendance Library	Attendance Summa	iv.						් Espo
	Job Number	Name	Department	Required Times	Actual Times	Absence	Late	Early Leave
ne oday +								
istom time period art Date 1/02/2023								
d Date 8/02/2023								
arch Type Bendance Summary								

Figure 8-18 Attendance data

Operation Steps

Step 1 Tick the attendance library.

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

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

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

Step 5 Click Export to export the query result.

----End

8.6.2 Attendance Management

In attendance management, user can set attendance rule, library and check point, as shown in Figure 8-19.

Figure 8-19 Attendance rule settings

Liberty Attendance	Data Attendance Management Back	د ه	e	G
Attendance: Rule Set. Attendance Library Attendance Check P	Attondanco Rulo Sottings Warking Iran: Startwork time 08.30 Endwark time 18.00 Warking Setting Saturday Wooday ar Tuesday ar Wodesclay ar Thursday ar Enday			
	Check-bryold time: Floton start-work t 99 min to After stars-work time, 30 min Check-but valid time: Before and voek t 90 min to After and work time 240 min			
	H emplayee does not check in when starting work, mark as absent - # emplayee does not check out when ending work, mark as absent			
	Арру			

Operation Steps

Step 1 Set start work time and end work time.

Step 2 Tick the workdays.

Step 3 Set valid time of check in and check out.

Step 4 Click Save to save the setting.

Attendance library

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

D Attendance Role Set	Attendance Library					
► Attentinues Eduary > Attentinues Check P	Face Library 🔅 Library Management	ः And « Delete	Atondance Library			
				Save		

- Step 2 Tick the library and click **Add** to add to attendance library. If you want to modify the library, please enter to library interface to change parameters..
- Step 3 click Database management to enter the face database management to modify

parameter.

Step 4 Click Save to save the setting.

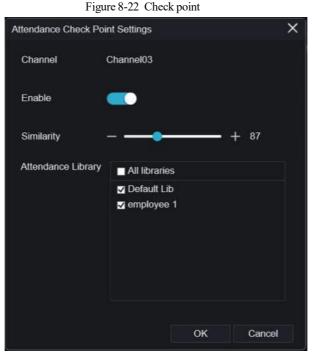
Attendance check point settings:

Step 1 Click Attendance check point settings to set point, as shown in Figure 8-21.

▷ Attendance Rule Set	Attendance Check Point Setting	5				
D Attendance Library						
	Channel	Attendance Library	Similarity	Enabled	Operate	
	Channel01		80%	Start	۷.	
	Channel02		80%	Start	∠	
	Channel03		80%	Start	∠	
	Channel04		80%	Start	∠	
	Channel05		80%	Start	۷	
	Charmel06		80%	Start	4	
	Channel07		80%	Start	۷.	
	Channel08		80%	Start	2	
	Channel09		80%	Start	∠	
	Channel10		80%	Slart	۷	
	Channel 11		83%	Start	2	
	Channel12		80%	Start	∠	
	Channel13		80%	Start	2	

Figure 8-21 Attendance check point setting

Step 2 Click Lo edit check point setting, as shown in Figure 8-22



Step 3 Enable the function, set similarity and tick the library, all face detection cameras can be set the check points.

Step 4 Click OK to save the setting.

----End

8.7 AI Recognition

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

8.7.1 Real Time Comparison

Real time comparison can compare human face, vehicle license plate, and AI(include riding,

vehicle, full body)

8.7.1.1 Human Face

At real time comparison interface, click the **D** to enter the human face comparison interface, choose the cameras with face recognition function to play live video, the snapshot of camera will be compared with libraries, the result shows as in Figure 8-23.



Figure 8-23 Human face comparison

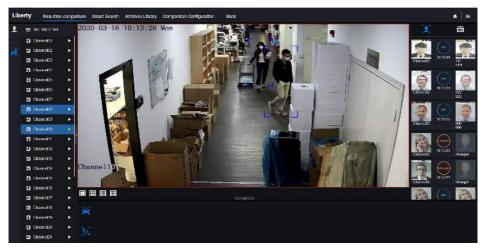
Click the "+" to add the snapshot to face library immediately.

----End

8.7.1.2 Vehicle and Full Body

At real time comparison interface, click the **NO** to enter the vehicle license plate comparison interface, choose the AI recognition cameras to play live video, the snapshot of camera will compare with libraries, the snapshot to vehicle and full body will show at the bottom of page, the result shows as in Figure 8-25.

Figure 8-24 Full body

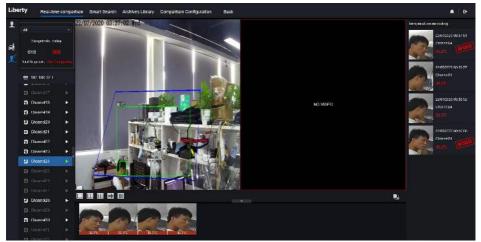


8.7.1.3 Real Time Body Temperature Filter

The real time body temperature will show the snapshot of device, it shows the over temperature and snapshot to human face.

Snapshot will show the characteristic such as no mask (the mask detection configuration can be

set at comparison configuration interface () Figure 8-25 Body temperature



8.7.2 Smart Search

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

body temperature.

8.7.2.1 Human Face Search

Figure 8-26 Human face search



Step 1 Choose human face search at smart search interface.

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

- Step 3 Choose the condition (by picture or by feature), the picture can be chosen from the file folder.
- Step 4 Click "Search" to search the snapshot of human face.
- Step 5 The result will show at the middle of page, click the picture and detailed information at the top right of page.

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

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

8.7.2.2 Full Body Search

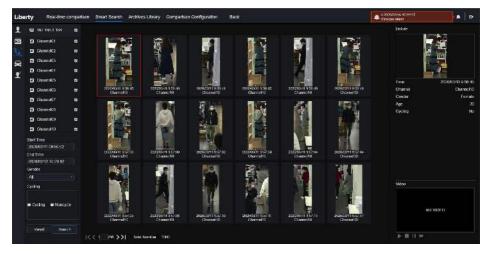


Figure 8-27 Full body search

Step 1 Choose full body search at smart search interface.

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

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

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

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

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

8.7.2.3 Vehicle Search

Figure 8-28 V	/ehicle search
---------------	----------------

								Helida	
😑 197 198 S 194								THE OTHER	
a itemeti								and the second	-
Silennei02				1 2 3				a statistics	the second se
Channel03	-	and the second second	Column Street	1000	and the second	CARD OF THE OWNER	Concession in which the local division in which the local division is not the local division in the local dint		
🖸 Channellé			100	and a		100	A DESCRIPTION OF	10.00	
1 Damstin								Tim	2020/03/02 11:50
Channol06	•	31311040 H 50.56 Charrenti	2000/1110 1.9155 Chappel66	2000/00/01 41:50:57 Channel76	SUSSICHO 11 20:57 Charrel05	2020/01190 14:50 57 Channel 08	2000-00400 (11.51.53 Channel08	Chantiel	Channel
Chantel07	-							Car zolor	E
🛱 CleanelCS		120		The second second	-				
D Commette		-	No. of Concession, Name	4	100	200	The second		
3 Channel 10		Comments of	Contraction of the local division of the loc	Sector Sector	low al	-0	-0		
Set Ime		Statistics.		Statement of the local division of the local	Salar Mi	Contraction of the second			
2020/03/03/09/06/54 42		202002049 11 52 09	2020/03/09 11:52:52	202040303 11:50 12	20202040 11 24 00	202011109-11-51-00	20209303115101		
2017003/13 10:24:42		Channel03	Channel R8	Channel08	Channel08	Channel08	Channel 38		
Che rates									
White Block			And in case of the local diversion of		-		1000		
■ Red ■ Hory		Sector 1	and to	and the second s	and the	and the second s	1000	Witer	
Citier		200	C. C. C. C.	Same and	and a second	-	1		
									NO-VIDEO
		Charlette	Channel 19	205200-03-11-Sert3 Channel 9	202030-08-11-54-02 Chartochile	ononative instate. Chancelle	Precedentis 11/5/21 Charlos (8		
Toped See									

Step 1 Choose vehicle search at smart search interface.

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

Step 3 Tick the color.

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

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

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

----End

8.7.3 Archives Library

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

8.7.3.1 Face Library

B Select A1	Final X I			nisen Configuration	Back.			A 2022/04/16 (Dos203 Regelered positificitation	
		elete 🔿 Refresi							
Ø Dekattion -									
		turne 🔰	Sender	Birthday		Focu Library	Туре	Expire date	Operate
C Indusing			Make	2020/05/14	1111	download	Teacher	Nover copite	∠ 00
ti maga -			Мон	202000014		itownkrodf	leaster	Минескортон	∠ 0
e englacering	0		Famale	2020/05/14		downhad	Teachar	Never copine	∠ 00
Б нар			Formalio	2020/05/14		download	leacher	Novor oxpiro	∠ 0
S 114		505	lemale.	202053514	hab	downhood	necteri	Nezes exprae	∠ 0
mottelq in		066	Female	2020/05/14	069	downkiad	Teacher	Nover expire	∠ 00
n in -			Maxi	20200314		download	loaches	Noves copins	∠ 00
g introv		868	Mon	2020/05/14	838	downhood	Shoel	Мизия нарти	<u> </u>
S lest -	(in 1)	959	Fomalo	2020/05/14	939	download	Student	Never expire	∠ 00
Bi handware	100		Мен	202003314		downinsd	Sinched	Хагаес кортн	<u>∠ 0</u>
a downional -									

Figure 8-29 Face library

Click "+" to add face library.

Click "Add" to add person enroll.

Tick the person, click "Delete" to delete the person.

Click "Import" to add the person batch.

Click "Export" to export all people in library.

Click operate icon to edit or delete the chosen person.

face library, or face search. The cursor on area 6 and the pictures are not update, move the mouse so that the pictures show in time.

----End

8.7.4 Comparison Configuration

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

Figure 8-30 Face comparison

	Edli Strategy		×	
	Channel	Channal01		
Channel01	Enable Comparison			
	Enable Comparison			
Chame03	Similarty	+ 00		
	Register. Stran	liet :		
	Display comparison res	uts 📺		
	Face Library	gr Face Library		
	Enable Alarm			
	Event Actions	Setting		
	Aming Time	Satting		
		OK Cancel		
	Default Lite	Default		

Event Actions			×
Buzzer			
Push message to APP			
Pop up message to monitor			
Email			
Full Screen			
Cloud Storage	•		
Alarm Out			
Alarm Time(s)(0 Continuous)	0		
Output ID			
Camera Alarm Out			
Alarm Record			
		ОК	Cancel

At face comparison interface, users can set different channels' strategy, such as similarity, display comparison result, face library, enable alarming, event action, schedule, as shown in Figure 6-35.

Liberty	Real-time comparison Smart B	earch Archives Library Comparison Configuration Back	Rappi Manajpassare Indere A Strattform All service	• •	*
1	channo.12	A LULUA Debartub	A LULUA Cosof Lin	2	
	channell 3	LUCUND: See LIB	A DUDUA;Detauk Lib	۷	
T	cranic14	A EV, EU, D-Ituri Lib	A EU EU/Defait LE		
	channelti	A EUEUA Defaal Lib	A EURIA Defait Lite		
	о (филин 18	A FUTUR Default is	A FUELA Datast in		
	channel17	U of soul Lab	Default Lite	2	
	prese Bi) Satard Fids	Dokal Im	۷	
	channel19	DefaultLb	Default Lib		
	channe(2)	Ustaul Lit	Default Lip	4	
	.cheme/21	Gebent) de	Debuilt in		
	channe 22	Default_D	Default Lib		
	ctanue/20	Ustani (), di	Detect Let	4	
	chanter24	Defect Ch	Defect th	4	
	channe (25	UctoutLb	Detault Up	4	
	grame 24	(bearf) di	Default 1 m		
	channel27	Behallub	Default Lib	۷	
	chantel@J	Uthod Lb	Default Las		
	idente 28	Cebert? dt	Detect Fit		
	channel 90	DefaultLb	Default Ub	۷	
	channe 31	Unantito	Detail Us	2	
	Chernel 20	Todon11 h	Delect Fite	2	

Figure 8-31 License comparison

At license plate interface, users can set strategies of different channels of license plate

recognition cameras, such as register and unregister, enable alarming, event action, schedule, as shown in Figure 8-31.

means the library is deleted.

Figure 8-32 Temperature comparison

Liberty	Real-time comparison Smart Sea	ach	Archiv	es Libra	ck.			2 2009/12/15 30.42.20 Strange + 6.00	e e	
	imparature Configuration									
803	Low lange state the shid(): 1-00.9)									
in the	High temperature threshold (0.1-99.9)									
	Normal temperature (0.1.60.0)									
						Refred	Apply			

At temperature comparison interface, users can set low temperature threshold, high temperature threshold, normal temperature, as shown in Figure 8-33.

		I Igui	8-55 Strategy	
2	Edit Strategy		×	
	Channel	Channel11	🗾 Edit Strategy	x
	Similarity		Channel Channel13	
	Register Stranger		Registered Unregister.	
	Display comparison resul		License F	
		E Face Library	License Plate Lib EL	
	Face Library	🗵 🛛 Default Lib 🔉	🗆 EU 🔽 Defau	
		□ app	Unita	
		nvr 🗸	Enable Alarm 💽	
	Enable Alarm		Event Actions Setting	
	Event Actions	Setting	Arming Time Setting	
	Arming Time	Setting		
		OK Cancel	OK	Cancel

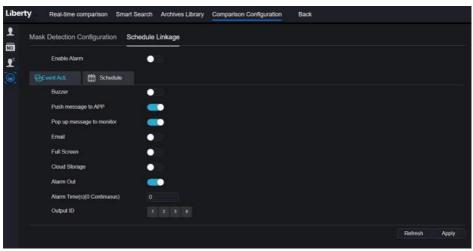
Mask detection configuration: enable mask detection, set the mode (wear mask, no mask). Set confidence degree, the default value is 90. Click "apply" to save the settings.

Figure 8-34 Mask detection configuration

y Real-time comparison Sma		
Mask Detection Configuration	Schedule Linkage	
Mask Detection Enable	-	
Mode	No Mask +	
Confidence Degree	+ 90	
		Refresh Apply

Enable mask alarm linkage, set the event action and schedule.

Figure 8-35 Schedule linkage



The alarm information is relevant to mask detection configuration.

9 System Setting

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

9.1 Channel

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

9.1.1 Camera

Step 0 On the System Setting screen, choose Channel > Camera to access the camera interface,

as shown in Figure 9-1.

Liberty	۲	Ð	Q		Ci (1	ø					• G
E Claund											
Camora Lucode			Camera	RTSP Con	naction						
Service Setting				Channel	IP Addrese	Port	Nodel	Protocol	Firmware Vension	Operate	
OSD Fittacy Zone				- ant	192 165 32 195	90001		Druste	15 6 0001 1004 5 0 10:0 0_AD_IVS1ext2	∠.e	
ROI				CH2	192 168 32 222	30001		Preside:	VS (IS matriceSciPASe = 3002)	2.0	
Niclophone				• CH3	192 168 32 5	30001		Private	v3 6 0804 1004 3.0 10 7 0	∠.ø…	
				CHA	192,168,32,175	30001		Private	13 8 0504 1004 3.0 10 10.0	2₫	
Scient				СНБ	192,168,32,166	20001		Privato.	V2.6.0807 1004.1.0.32.3.1	∠.@	
Record				Cite	192,168,32,171	30001		Private	¥3.6.0304.1004.3.0.10.11.0	∠.e	
				с фант	192,106,32,162	30001		Private	15 6 0804 1004 3 0 11.0.0	∠,⊝	
Airm				т (фена	192 188 32 181	30001		Printe	v3.5.0812 1084 3 0.58 0,0	∠.⊖	
S Novork				СНЯ	192.168.32.145	30001		Printe	13.6 0819 1004 S.0 10 S.D	∠⊘	
💮 Syslem				CH10	192 168 32 131	30001		Private	v8.6.0004 1004 3.0 10:11 0.005	∠ø…	
				Сни	192.108.32.157	30001		Private	v3.4.0702.1003.3.0.162.0.0	∠.©	
				• CI112	192.168.52.150			CINVIF	x0.5 0804 1004 08.1.50 7.14	∠e	
			1	- Arms	102 101 111 120						
						Jsomamo H	Hassword	Aukt Dava	on Smith Refere Drivin	Batch Update	

Figure 9-1 Camera interface

Step 1 Input username and password (the default username and password both are admin), and

click

Click To Add add cameras automatically.

191

Search

Step 2 Click

to search cameras at the same LAN as NVR, as shown in Figure 9-2.

Choose the cameras, input username and password, click **Add** to add new cameras. Figure 9-2 Device search

	Protocol I	Management				
	ID	IP Address	Port	Model	Protocol	Firmware Version
		192.168.99.14	30001	IPS57/30BDR/ZSD30/28	Private	13.6.0804.1004.3.0.8.12.0
		192.168.70.177	30001	C81031-W	Private	v3.5.0819.3900.172.0.31.0.10
		192.168.70.176	30001	C81041-W	Private	v3.5.0819.3900.172.0.31.0.10
		192.168.10.249	30044	IPR57/08ALDN/Z3.3-12/23	Private	v3.5.0819.1004.3.0.33.3.0
		192.168.10.208	30001		Private	t3.8.0825.1004.3.0.13.4.0
		192,168,10,127	80		ONVIF	
		192,168.10.126	80		ONVIF	
	8	192.168.10.8	30001		Private	t3.6.0804.1004.3.0.6.90.0
5 3 Cl			J OUCK IO	camera interface.		
14 Cl	ick	Refresh to	refresh ca	meras status		
		10		meras status.		
		Refresh to		meras status. Delete to delete		
o 5 Cł	noose th	ne cameras an	d click	Doloto		-up window would
p 6 Cl	noose th ick Bat	ne cameras an	d click update all	Delete to delete		-up window would

Figure 9-3 Modify device parameters

Modify device parameters			×
Channel Name	Channel06		
IP Address	192 168 0.232		
Protocol	Private_SSL		
Port	20001		
Username	admin		
Password	•••••	755	
Remote Channel	CH-1		
		Cancel	ок

Step 8 Click

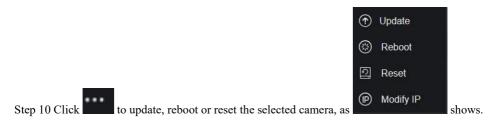
to add camera manually, click the added channel to copy information to add,

so that user just modify some information quickly, as shown in Figure 9-4.

Figure 9-4 Add camera manually

Channel	IP	Protocol
CH1	192.168.32.196.30001	Private
CH2	192 168 32 222 30001	Private
СНЗ	192.168.32.5:30001	Private
CH4	192.168.32.175.30001	Private
Channel	32	
IP Address	192.168.32.5	
Protocol	Private *	
Port	30001	
Username	admin	
Password	····· \>	
Remote Channel	CH-1 *	

Step 9 Click to access web immediately.



The pop-up message "Are you sure to restart the device?" "Are you sure to reset?

Reserve IP Address" would respectively show.

Figure 9-5 Modify IP

IP Address		1
Subnet Mask		
	ок	Cancel

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

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

9.1.1.1 Protocol Management

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

Figure 9-6 Protocol management

Custom Protocol	Custom Protocol 1 *	
Protocol Name	Custom 1	
Stream Type	IgMain Stream ■Sub Stream	
Туре	RTSP • RTSP •	
Port	554 564	
Path		

Step 1 Click Channel > Camera > RTSP Connection.

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

Step 3 Input the protocol name.

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

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

Step 6 Input the port of the IP camera.

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

Step 8 Click Apply to save the settings.

9.1.2 Encode

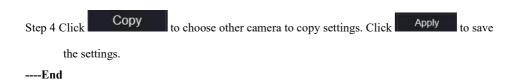
Step 1 On the **System Setting** screen, choose **Channel > Encode** to access the encode interface, as shown in Figure 9-7.

ode		
Channel	[1]Channel01 -	
Stream Information	Main Stream +	
Video Format	H265 +	
Audio Encode Type	G711A *	
Resolution	1920x1080 +	
Frame Rate(tps)		
I Frame Interval(Frame)	- 50 -	
Bitrate Type	CBR +	
Bitrate(kbps)(500-6144)	4096 *	
Smart Encode		
		Copy Λρ

```
Figure 9-7 Encode interface
```

Step 2 Select a channel from drop-down list.

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



9.1.3 Sensor Setting

Step 1 On the System Setting screen, choose Channel >Sensor Setting to access the sensor

setting interface, as shown in Figure 9-8.

Figure 9-8 Image interface

		Channel	[3]Channel29 -	
4/01/2023 05 Commit 207				
ge Scene Expor		nt Noise Redu	tion Enhance Image	
ge Scene Expor	sure White Balance DayNig	nt Noise Redui	tion Enhance Image	
		ht Noise Redu	tion Enhance Image	
Scene	Default -	ht Noise Redu	ction Enhance Image	
Scene Brightness	Default -	ht Noise Redu	ction Enhance Image	

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, please refer IP cameras' settings.



the settings.

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

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

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

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

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

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

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

Day-night: it 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**: zoom and focus.

----End

9.1.4 OSD

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

shown in Figure 5-4

D						
Channel		(1)Channel()1 -				
Time						
Channel Nan	e U	Channel01				
022-04-26-1	ga 1990 www					
Terre		T				
1.0						
Par Press						
1119	TTAXA					
- /	and the second					
					Сору	Αρρ

Figure 9-9 OSD interface

Step 2 Select a channel and scene from drop down 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 cameras to copy settings. Click Apply to

save the settings.

----End

9.1.5 Privacy Zone

Step 1 On the System Setting screen, choose Channel >Privacy Zone to access the privacy

zone interface, as shown in Figure 9-10.

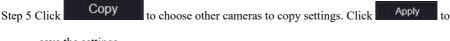
Figure 9-10 Privacy interface

Liberty (•	0 Q @					
📑 Channel							
Camera Encode		Privacy Zone					
Sensor Setting OSD Privacy Zone		96/14/2021 99:49:50 Pet	F ^ < 0	→ 	Channel	[2]Channel12 -	
ROI Microphone			- L V [4]	 			
Smart			O U	@ [P			
Intelligent Tracking		Click and hold left button and drag to s - Double click an area to dolete it - Supports up to 4 zones	elect an area				Apply
Record		Condition of the America					
System							

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.

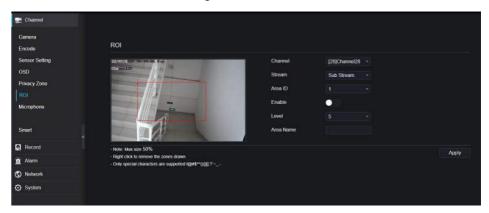


save the settings.

9.1.6 ROI

ROI(Region of interest), choose channel, stream, area ID and draw the area. Set the level, there are five levels can be chosen. Set area name, click "Apply" to save the settings.

Figure 9-11 ROI



9.1.7 Microphone

Users can set the microphone parameters of channel.

Figure 9-12 Microphone

Carrena Encode Microphone Setting Charnel J1/CharneO1 -
Sensor Selling Channel HV Sensort
050
- Privacy Zone Microphone 🦲
ROI Microphone Type Line In -
Microphone Witane
Smart c
R Horord
🚊 Alami
🛇 Notraurk
O System

9.1.8 Smart

At smart interface, users can set AI multiobject, license plate recognition, face detection.

Figure 9-13 Smart interface Chan Camera Al Multiobject License Plate Recognition Face Detection Encod Sensor Settin Charles [3]Channel03 -OSL Protect **PO** Men CI Record Parameter Configure Alarmi tedule S Network Fore Detertion Image Metting Culty Medium O System Fulfoody Detection Allabate of Mod Openial w Degree(II-90) 80 Display Trace Info Till Dei e(0.80) 60 (0.90 60 ni Unani inked many mat ace Pixel Min(30-300) el Mantan an

9.1.9 Intelligent Tracking (Only for Some Models)

This function can only be used for high speed dome camera. It works with PTZ function.

Figure 9-14 Intelligent tracking

Liberty	۲	Ð	Q		[#]	ø		. a ⊖ G
🛒 Channel								
Carnera Encode			Intelligent	Tracking				
Sensor Setting				Channel				
OSD							Apply	
Privacy Zone								
RO								
Microphone								
Smart								
Intelligent Trackle								
Record								
🚊 Alarm								
S Network								
O System								

The detailed information please refer to UI configuration setting.

9.2 Record

Users can set record policy in storage interface.

9.2.1 Record Schedule

Procedure

Step 1 On the System Setting screen, choose Record > Record schedule to access the record

schedule interface, as shown in Figure 9-15.

Figure 9-15 Record schedule interface

🛃 Channel	
Record	
Record Schedule	Record Schedule
Disk	Channel [1]juit +
Storage Mode S M A R T Disk Calculation FTP	Eriable Rocord Enable Rocord Audio Eriable ANR C
🧕 Alarm	All \$ 2 4 6 8 10 12 14 16 18 20 22 24 Sun \$
S Network	Mon E Continuous
O System	Too to the second secon
	Copy Refresh Apply

Step 2 Select a channel.

Step 3 Enable the record, then enable record audio.

Step 4 Enable ANR, when the IP cameras support the ANR, if the cameras are disconnected to NVR, the NVR can copy the loss video recordings from SD card installed in cameras.

Step 5 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. Users can set the alarm recording to save the space of disk.

Step 6 Click Refresh to return the previous settings.

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

----End

9.2.2 Disk

Step 1 On the System Setting screen, choose Record >Disk to access the disk interface, as

shown in Figure 9-16.

Figure	9-16	Disk	inter	face
riguie	9-10	DISK	muci	lace

Disk			r.
	Disk1 Capacity 2TB		
			Format
	Disk Status	Normal	
	Disk SN	WD WXE1A791JKF4	
	Used Space	434GB	
	Disk Group		
	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 users will view pop-up window

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

Cancel to quit.

Step 4 Choose the disk group from drop-down list, there are four disk groups.

Step 5 Enable the recording overwrite, set the expired time. (If the expired time is 0, it means the disk is full, then the recording will be rewrite. It the expired time is 5 days, the recording video will be rewrite when it reaches the expiration date..)

Step 6 If the recording overwrite is disable, set the expired time, it is up to 90 days.

----End

9.2.3 Storage Mode

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

	Mode Selection	o g	roup							
	Disk Group									
	Channel			1	4	6	7	3		
			0 1	1 12	16	14	15	16		
		17	iā 1	o 10	24	22	22			
	annel belongs to Group 1									Арј
e dottan Ch Group	Disk		nann	el				Used Space	Capacity	Ар
			nann 1-16	el				Used Space 985GB	Capacity 1000GB	Ар
Group	Disk									Ар
Group 1	Disk Disk1	1	1-16					985GB	1000GB	Ap

Figure 9-17 Storage Mode

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.

9.2.4 RAID (Only for Some Models)

RAID is only used for the device with 4 disks or more. And the disks must be enterprise level disks. It is recommended to choose the same capacity for efficient use.

For Raid5, at least 3 disks can be created. For RAID6, at least 4 disks can be created. For RAID10, at least 4 disks can be created. Creating a hot spare disk requires more disks.

It is recommended to choose the same capacity for efficient use. The RAID with less than 100T capacity can be built.

Liberty	\odot	€	Q		(et)	¢					٠	۵	G 6
🛃 Channal													
Record			RAID										
Record Schooluin Disk Storage Mode RAD S.M.A.R.T Disk Calculation FTP		-	ID	RAIE) Næme	Capacity	Status	Туре	HDD Members	Operate			
Alanm S Network System													
										Create			

Figure 9-18 RAID

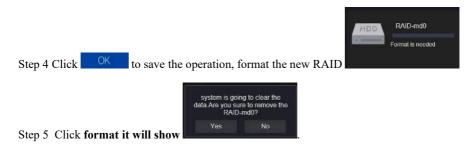
Operation Steps

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

reate RAID				>
RAID Type		RAID 5 +		
Q	Name	Capacity	Hotsp	are Disk
	Disk1	2TB		
	Disk2	6TB		
	Disk3	6TB		
	Disk4	3TB		
	Disk5	2TB		
	Disk6	2TB		
	Disk7	1TB		
	Disk8	2TB		
			ок	Cancel

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

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



mati						
RAID N	ame	RAID md0		Туре	RAID 5	
Capacil		бТВ		Members	Disk1,2,3,4,5	
ID.	Name	Capacity	Status	Туре	Hotspare Disk	Operate
	Disk1		Activo	RAID 5	Na	
	Des2		Active	RAID 5		
	Disk3	бТВ	Actve	RAID 5	No	
	Disk4		Active	RAID 5		
	Disk5	27B	Spere	RAID 5	Yes	1
6	Disk6			нор		
	Dek7			HOD		+
	Disk8	2TB		HDD		

Figure 9-19 Modify the RAID

9.2.5 S.M.A.R.T

S.M.A.R.T is Self-Monitoring Analysis and Reporting Technology, users can view the health of disk, as shown in Figure 9-20.

Figure 9	9-20 S	.M.A.I	۲.S
----------	--------	--------	-----

Liberty 💽	Ð	Q¢								
🛒 Cherand										
👷 Geord										
Record Schodule		S.M.A.R.T WDDA								
Record Schooler										
Sloraco Niedo		Disk	Diski -							
SMART		Dak SN	WD-WXF14791UKF4			DiskMo	de i	WEC WD21P	5RX.09/417/0	
Disk Calculation		lengestae	2010			Working	Time	2 t Month		
Line Cartalonia						10-104				
		Usk Roath	6000							
🙆 //am		ю	Athributa Name	Status	Value	Wood	Thresh	Туре	Rate value	
Stobwerk						200				
O System			onvosularitariada	CK.	208	101		prefeit	Ge0000000000 Gat-5000000000	
		4	spin up time start-stop-count	СК	106	100		precial old-age	CK620+0000000	
		* 5)	realization sector count	UK:	2010	000	140		Californionomo	
								pre-et	0.00000000000	
			der-terre-size	ок	200 98	200 98		old ago	0x40560000000	
			powerandous					old-oge		
			spen beby count	OK.	500	1967		okt ege	Ca10(1000000000	
			colloraden-retry-count					old-ago	Cx0000000000	
			hower ritige count			100		opt rafe	Carphonometrication	
			power-off-relitact-count		200	200		old-ago	CK03010000000	
			Indepheotof		200	700		chi-que	Ca01000000000	
			hemiseratum contacts 2					old sam	04240340042040000	

The disk of Western Digital can be viewed by WDDA, as shown in Figure 9-21.

iberty 💿 Đ) Q 🕸				
Channel					
Record					
Record Schedule	S.M.A.R.T WDDA				
Disk Storage Mode S M A.R.T	Disk Disk SN	Diskt •	Disk Model	WDC W	D21PSRX.89AHTY0
SMART Disk Calculation FTP	Warning		Advisory		
Alarm	ID Attribute	Name		Status	Raw value
S Network	1 Lifetime	Power On Reset Alert		Normal	354
) System	2 Power 0	n Hours Alert		Normal	1481
	3 Head Lo	ad Lifetime Count Alert		Normal	354
	4 Current	emperature Alert		Normal	
	5 Total Life	time Workload Alert		Normal	3.2302463
	6. Total Wo	rkload Rate Alert		Normal	19 106655
	7 Power 0	n Reset Rate Alert		Normal	0.23902768
	8 Head Lo	ad Rate Alert		Normal	0.23902768
	9 Soft Res	et Alert		Normal	
	10 Hard Re	set Alert		Normal	
	11 Mechani	al Failure Alert		Normal	
	12 Interface	CRC Alert		Normal	

Figure 9-21 WDDA (Supplied for Some Model)

9.2.6 Disk Calculation

There are two modes to calculate the captivity of disk, as Computing Capacity Computation time shown in.

Figure 9-22 Disk calculation

Liberty	۲	۲	Q		(e i)	¢					4	4	G	6
🛃 Channel														
Record			Disk Calcu	1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.										
Record Schodule Diek Siorage Mode RAID S.M.A.R.T Diek Calculation FTP					lode 14 time 14 per day	itrate 0.00 Mbps Computing G	• Day	• 24 h						
Alaim							GB							
S Network						\sim								
💮 System														

Liberty	۲	Ð	Q	[=]]	<u>_</u>	* 4 B B
📑 Channel						
Record						
Racord Schedula Diek Storage Mode (KAI) S.M.A.R.T Diek Calculation FTP Alern O. Network O. Network				Aodia ve time ne per day	bitraic 0 00 Mbgs Computing • 0 Dey • 24 b	

9.2.7 FTP

Set the FTP path to receive the alarm information, as shown in Figure 9-23. More detail information please refer to UI interface parameters.

Figure 9-23 FTP

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

9.3 Alarm

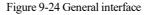
Users can set general, motion detection, video loss, intelligent analysis and alarm in on alarm interface.

9.3.1 General

9.3.1.1 General

Procedure

Step 1 On the **System Setting** screen, choose **Alarm > General** to access the general interface. Step 2 Enable alarm to set duration time and buzzer duration time, as shown in Figure 9-24.



Enable Alarm				
Alarm Duration Time (sec)	10s			
Buzzer Duration Time (sec)	30s			
			Refres	h Apply

9.3.1.2 IO Control Push

Procedure

Step

- Step 1 On the **System Setting** screen, choose **Alarm > General > IO Control Push** to access the general interface.
- Step 2 Enable the IO control push, as shown in Figure 9-25.

Figure 9-25 IO control push interface

Channel Record	General	IO Control Push				
Ceneral Motion Detection Camera Temper Video Loss Intelligent Analysis Alarm In Abnormal Alarm Alarm Out		Enable Alarm In Mode Disabled Items Push message to APP Email	NO P			
Network O System					Refresh	Apply

Step 3 Choose one alarm in and mode (N/C, N/O).

Step 4 Tick the disable items, click "Apply" to save settings.

----End

9.3.2 Motion Detection

Procedure

Step 1 On the **System Setting** screen, choose **Alarm > Motion Detection** to access the motion detection interface, as shown in Figure 9-26.

Motion Dete	oction		
	Chennel	(1)Channel01 -	
	Enable Motion Detection	00	
9	Event Actions [1] Detection	n Area 🛗 Schedule	
	Buzzer	•	
	Push message to APP		
	Pop up message to monitor		
	Full Screen	(1)	
	Email		
	FTP		
	PTZ		
	Enable Alarm Out		
	Enable Camera Alarm Out		
	Enable Event Recording		
		Copy Appl	

Figure 9-26 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, push message to APP, pop-up message to monitor, full screen, Email, cloud storage, alarm out (the back panel), channel alarm out (the port of cameras), and alarm record.
- Step 5 Click Area to access the motion detection area setting, as shown in Figure 9-27.

Motion Dete	sction		
	Channel	(1)Channel01 +	
	Enable Motion Detection		
Ð	Event Actions	n Area 🛗 Schedule	
	2722-01-25 16:55:46 Mon		
		X	
	Sensitivity	Medium	
			Copy Apply

Figure 9-27 Motion detection area interface

- 1. Hold down and drag the left mouse button to draw a motion detection area.
- 2. Select a value from the drop-down list next to Sensitivity.
- 3. Double -click the chosen area to delete.
- Step 6 Click **Schedule** to access schedule settings, drag and release mouse to select the alarming time within 00:00-24:00 from Monday to Sunday. Click the chosen area can cancel. The settings of alarm schedule are same as disk schedule.

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

save the settings.

---End

9.3.3 Video Loss

Procedure

Step 1 On the System Setting screen, choose Alarm > Video Loss to access the video loss interface, as shown in Figure 9-28.

Figure 9-28 Video loss interface



Step 2 Click drop-down list to choose channel.

Step 3 Enable the video loss alarm.

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

Step 5 Click	Сору	to choose other camera to copy settings. Click	Apply	to save

the settings.

----End

9.3.4 Intelligent Analysis (Only for Some Models)

Procedure

Please refer to chapter 7.4.1 video loss settings, interface displayed as shown in Figure 9-29.

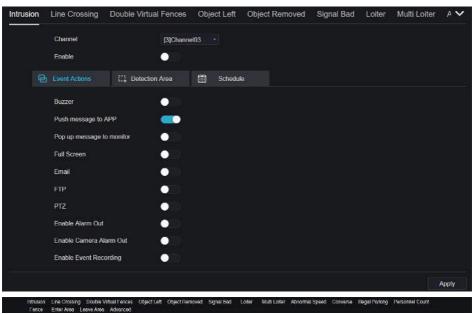


Figure 9-29 Intelligent analysis interface

9.3.5 Alarm In

Procedure

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

Alarm In	
Alarm In	[1]Alarm In 🔹
Enable	
Alarm Type	N/O *
Name	Sensor 1
Event Acti III Schedule	
Buzzer	
Push message to APP	
Pop up message to monitor	
Email	
Alarm Out	
Alarm Time(s)(0:Continuous)	
Output ID	
Alarm Record	

Figure 9-30 Alarm in interface

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

Step 3 Enable the button, choose alarm type.

Step 4 Set name, default as Sensor 1.

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

Step 6 Click Apply to save settings.

----End

9.3.6 Abnormal Alarm

Procedure

Step 1 On the System Setting screen, choose Alarm > Abnormal Alarm to access the abnormal alarm interface, as shown in Figure 6-12.



Abnormal Alarm					
Enable Abnormal Alarm					
Abnormal Type		~ ₽øø			
Buzzer	•				
Push message to APP					
Pop up message to monitor					
Email					
Enable Alarm Out					
Alarm Time (sec) (0 Always Alarm)					
Port Number					
				Refresh	Apply

Step 2 Enable the button, tick alarm type.

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

Step 4 Click Apply to save settings.

----End

9.3.7 Alarm out

Set the alarm out, the camera alarm out.

Figure 9-32 Alarm out

Alarm Out	Camera Alarm Out				
	Port Number Port Name	[1]Alarm Out			
	Valid Signal	Close			
	Alarm Output Mode	Switch Mode		Refresh	Apply

Figure 9-33 Camera alarm out

	larm Out	Camera Alarm Out					
Close + Mode Switch Mode -		Channel	[1]Channel01				
Mode Switch Mode -		Port Number					
Mode Switch Mode -		Port Name					
		Valid Signal	Close				
e)(0 Continuous) D		Alarm Output Mode	Switch Mode				
		Alarm Time(ms)(0 Continuous)					
		Alarm Output Mode	Switch Mode				

9.4 Network

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

9.4.1 Network

Procedure

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

Figure 9-34 Network interface

300 AN			
	Network Card Name	Network Ca *	
	DHCP		
	IP Address	192.168.32.163	
	Subnet Mask	255.255.255.0	
	Default Gateway	192.168.0.1	
	Obtain DNS Automatically		
	Preferred DNS Server	144, 144, 144, 144	
	Altenate DNS Server	192.168.1.1	
			Refresh Apply

Step 2 Choose network card from the drop-down list. Network card I is LAN1, network card II is LAN2, as shown in Figure 9-35.

Figure 9-35 Network card II

PORT			
Network Card Name	Network Ca *		
IP Address	192.168.10.253		
Subnet Mask	255.255.255.0		
Default Gateway	192.168.10.254		
		Refresh	Apply

Step 3 Click next to IP to enable or disable the function of automatically getting an IP

address. The function is enabled by default.

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

Step 4 Click next to Obtain DNS Automatically to enable or disable the function of

automatically getting a DNS address. The function is enabled by default.

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

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

Figure 9-36 POE

IP Por	t POE			
	Auto Manage For PoE Camera	_		
	IP Address	169,254 10 121		
	Subnet Mask	255.255.0.0		
	Default Gateway	169.254.10.1		
(100-1436-p)	naneten an mathetaria he desce all'm	een:	Refresh	Αρρίγ
Step 6 Click	Refresh to restor	re previous settings. Cli	ck Apply to sav	e the settings
End				

9.4.2 DDNS

Procedure

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

interface as shown in Figure 9-37.

Figure 9-37 DDNS interface

🛒 Channel						
Record	DDNS					
🧕 Alarm	DDNG					
S Network		Enable				
Network		Protocol	no_ip =			
DDNS		Domain Name	dvr ddns net			
Email		User				
Port Mapping		Password				
			Test			
IP Filler 802.1X				Refresh	Apply	
SNMP						
Web Mode						
System						
G 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.

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

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

----End

9.4.3 Email

Procedure

Step 1 Click Email in the network interface, choose Network > Email to access the E-mail

interface, as shown in Figure 9-38



🛒 Channel					
Q Record En	and .				
2 Alarm	lan.				
S Network	SMTP Server				
Network	SMTP Server Port				
DDNS	Username				
Email	Password				
Port Mapping	Email Sender				
P2P <	Email for password reco.				
IP Filter	Alarm Receiver 1				
802.1X	Alarm Receiver 2				
SNMP Web Mode	Alarm Receiver 3				
	SSL Encryption	OFF			
System		Test			
⊊ Local					
				Refresh Ap	ply

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 receiving the alarm message.

Step 5 Set E-mail for retrieving the password.

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

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

System Setting

----End

9.4.4 Port Mapping

9.4.4.1 Port Mapping

Procedure

Step 1 Click Port Mapping in the network interface, choose Network > Port Mapping to

access the UPnP interface as shown in Figure 9-39.

Figure 9-39 Port Mapping interface

Liberty	۲	•	Q	. 🗇	۶ť)	ø							3 D)
🛃 Channel													
Record													
🙍 Nam			Port Ma	pping NA	T Port								
S Network				Enable Por	t Mapping								
Natwork				Mode		Auto							
DONS				HTTP Port									
Email				HITPS Po	t								
Port Mapping				RTSP Part									
P2P				Control Por									
IP Filter 802 1X									Retresh	 ely.			
SINMP									Kalinan	 197			
Web Mode													
POE Status													
Platform Access													
💮 System													

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

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

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

Auto: System perform UPnP automatically. Manual: The ports are distributed by the router. Input them according to the router.

9.4.4.2 NAT port

NAT (Network Address Translation), users can browse the web of camera by NAT port. There are five ports can be assigned to each camera. Input the start port, the system will compute the end port automatically.

Figure 9-40 NAT port

🛒 Channel						
Record						
a Alarm	Port Mapping	NAT Port				
S Network	9	art Port	50002			
		un en en e				
Network	En	id Port				
DDNS						
Email	Po	ort range [40001-65534]				
Port Mapping						
P2P					Refresh	Apply
IP Filler						
802.1X						
SNMP						
Web Mode						
36/46						
PPPOE						
System						

----End

9.4.5 P2P

Procedure

Step 1 Click P2P in the network interface, choose Network > P2P to access the P2P interface, as shown in Figure 9-41.

Figure	9-41	P2P	interface
--------	------	-----	-----------

P2P				
Enable P2		-		
Status		Online		
		B011003ACH51729NA		
App Name		Liberty-View		
- It is available on App Store	and Google Play		Refresh	Apply

Step 2 Click Enable to enable the P2P function.

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

Step 4 After installing Liberty-View in mobile phone, run the app and scan the UUID QR code to add it. And then access the NVR while the device is online.

----End

9.4.6 IP Filter

Procedure

Step 1 Click **IP Filter** in the network interface, choose **Network > IP Filter** to access the IP filter interface, as shown in Figure 9-42.

Figure 9-42 IP filter interface

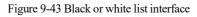
IP Filter						
	IP Filter					
	Rule Type			Black List 👻		
	Black List(Followi	ing network segments are forbidden)		+ -		
		Start IP	End IP	Ed	it	
					Refresh	Apply

Step 2 Click Enable to enable the IP filter function.

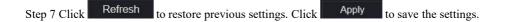
Step 3 Click drop-down list of rule type to choose black list or white list.

Step 4 Click ,view the pop-up windows to set black list or white list, as shown in 7.5.5.

Click to delete the list.



Add Ip Segment		×
Start IP		
End IP		
	Cancel	ок
Step 5 Set start IP and end IP.		
Step 6 Click Cancel to deny settings	, click OK	to save the settings.



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

9.4.7 802.1X

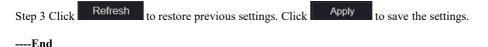
Procedure

Step 1 Click **802.1X** in the network interface, 802.1X interface is displayed, enable the button, as shown in Figure 9-44.

802.1X				
	Enable	-		
	User			
	Password	Yind .		
			Refresh	Apply

Figure 9-44 802.1X interface

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



9.4.8 SNMP

Procedure

Step 1 Click SNMP in the network interface, SNMP interface is displayed, enable the button

next to SNMPV1, as shown in Figure 9-45.

SNMP			
SNMPV1	_		
SNMPV2C			
Write Community	b		
Read Community	а		
Trap Address	192.168.32.79		
Trap Port	16222		
Trap Community			
SNMPV3			
Read Security Name	а		
Security Level	priv		
Auth Algorithm	MD5		
Auth Password	*******		
		<u> </u>	
Encry Algorithm	AES		
Encry Password	******		
Write Security Name	b		
Security Level	priv		
Auth Algorithm	SHA		
Auth Password	*******	Sect	
Encry Algorithm	AES		
Encry Password	*******		
			Defeat
			Refresh Apply

Step 2 Input the information of SNMP (simple network management protocol). there are three types of that function. Users can apply that if need.

Parameter	Description	Setting
SMTP Server Address	IP address of the SMTP server.	[Setting method] Enter a value manually.
SMTP Server Port	Port number of the SMTP server.	[Setting method] Enter a value manually. [Default value] 25
User Name	User name of the mailbox for sending emails.	[Setting method] Enter a value manually.
Password	Password of the mailbox for sending emails.	[Setting method] Enter a value manually.
Sender E-mail Address	Mailbox for sending emails.	[Setting method] Enter a value manually.
Recipient_E- mail_Address1	(Mandatory) Email address of recipient 1.	[Setting method] Enter a value manually.
Recipient_E- mail_Address2	(Optional) Email address of recipient 2.	
Recipient_E- mail_Address3	(Optional) Email address of recipient 3.	
Recipient_E- mail_Address4	(Optional) Email address of recipient 4.	
Recipient_E- mail_Address5	(Optional) Email address of recipient 5.	
Attachment Image Quality	A higher-quality image means more storage space. Set this parameter based on the site requirement.	N/A
Transport Mode	Email encryption mode. Set this parameter based on the encryption modes supported by the SMTP server.	[Setting method] Select a value from the drop-down list box. [Default value] No Encrypted

Table 9-2 SNMP	parameters
----------------	------------

Step 3 Click

Refresh

to restore previous settings. Click

Apply to save th

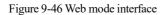
to save the settings.

----End

9.4.9 Web Mode

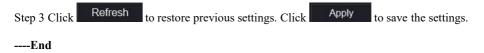
Step 1 Click Web Mode in the network interface, Web mode interface is displayed, as shown in

Figure 9-46.



😴 Channel		
Record	Web Mode	
🚊 Alarm		
S Network	HTTPS	
Network		Refresh Apply
DDNS		
Email		
Port Mapping		
P2P		
IP Filter		
802.1X		
SNMP		
Web Mode		
System		
🖵 Local		

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



9.4.10 POE Status

Users can view the POE status at this interface, as shown in Figure 9-47.

Figure 9-	7 POE status
-----------	--------------

Connected Bit Chained Connected Bit Chained Bit Chain	Liberty	۲	Ð	Q	Ø	8			
Alarm POE Status Network DONS Emeil Port Mapping P2P IP Fater Status Mode Connected	🔜 Channel								
	Record								
Network DDNS Email Port Mapping P2P IP Filtor B02.1X SNMP Web Mode Connected	🚊 Alarm			POE St	atus				
Network DDNS Email Port Mapping P2P IP Filter B02.1X SNMP Web Mode Connected	S Network								
Pole Statua POE Power Consumption Sum: 1 6W / Max: 40W	DDNS Email Port Mapping P2P IP Filter 802:1X SNMP Web Mode POE Status					Router Connected Disconnected Powering Connecting			

9.4.11 Platform Access

For more detail, please refer to UI interface parameter setting 7.4.13 Platform Access. Figure 9-48 Platform access

Enable		
URL		
Port		
User		
Password		
Encrypt		

9.5 System

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

9.5.1 Device Information

Procedure

Step 1 Click



on the navigation bar, the device information interface is displayed, as

shown in Figure 9-49.

System Network Channel	l Disk Alarm
Device ID	B011003AFEK109U62
Device Name	Device
Device Type	NVR
Model	L3NVR8POE
Firmware Version	v4 6 1604 0000 003 0 1 36 0
U-boot Version	1504010C0F18
Kernel Version	15080511183A
HDD Number	
Channels Supported	
Alarm In	
Alarm Out	
Audio In	
Audio Out	

Figure 9-49 Device information interface

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

Table 9-3 Device	parameters
------------------	------------

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

Parameter	Description	Setting
Alarm in		
Alarm out		
Audio in		
Audio out		

Figure 9-50 Network

Status Online IP Address 162, 168, 0.51 Stubret Mask 255, 255, 0.0 Default Gateway 162, 168, 0.01 MACA Address 00.1E, A4, 00.42, 85 DHCP OFF Prefored DNS Server 162, 168, 0.1 Atternate DNS Server 8.8, 8.8 Tetal Bandwidth 100, 00 Mpcs	ystem Network Channel Disk Alarm		
Subnet Mask 255.250.0 Default Gateway 162.168.0.1 MAC Address 001E:A4.00.42.85 DHCP OFF Preferred DNS Server 162.168.0.1 Attemate DNS Server 8.8.8	Status	Online	
Default Gateway 162.168.0 1 MAC Address 001E.A4.0042.85 DHCP OFF Preferred DNS Server 152.168.0 1 Attemate DNS Server 8.8.8	IP Address	192 168 0 51	
MAC Address 00 1E A4 00 42 85 DHCP OFF Preterred DNS Server 162 168 0.1 Attemate DNS Server 8.8.8	Subnet Mask	255.255.0.0	
DHOP OFF Preferred DNS Server 162 168 0.1 Alternate DNS Server 888.8	Default Gateway	192.168.0.1	
Preferred DNS Server 162 166 0.1 Attemate DNS Server 8.8.8	MAC Address	00.1E.A4.00.42.85	
Atternate DNS Server 8888	DHCP		
	Preferred DNS Server	192.168.0.1	
Total Bandwidth 100.00 Mbps	Alternate DNS Server	8.8.8	
	Total Bandwidth	100 00 Mbps	

Figure 9-51 Channel

Channel	Name	Status	Video Format	Resolution	Bitrate(kbps)
CH1	Device	Offline	H265/H265	2560*1440/704*576	4096/1024
CH2	Channel12	Online	H265/H265	1920*1080/704*480	4096/1024
СНЗ	Channel29	Online	H265/H265	1920*1080/704*576	4096/1024
	Device	Online	H264/H264	1920*1080/704*576	2048/1024

Figure 9-52 Disk

System	Network	Channel	Disk	Alarm		
Disk	Capacity	Used		SN	Disk Model	Status
Diskt	278	901GB				Normal

Figure 9-53 Alarm

ystem Network Channel	Disk Alarm			
Channel	Name	Mode	Enable	Recording Channel
Local<-1	Sensor 1	NO		
Local<-2	Sensor 2	NO		
Local<-3	Sensor 3	N/O		
Local<-4	Sensor 4	NO		
Local⇒1		Close		

----End

9.5.2 General

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

Procedure

Step 1 On the **System Setting** screen, choose **System >General** to access the general interface, as shown in Figure 9-54.

Figure 9-54 Basic setting interface

📑 Channel				
Record				
🚊 Alarm	System	Date And Time Tin	ne Zone DST Sync Camera Time	
S Network		Device Name	Device	
System		Output Resolution	1920x1060 *	
Information		Language		
General User Account		Temperature Unit	Celsius +	
Security Center				Retresh Apply
Logs				
Maintenance				
Auto Reboot				



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

Step 3 Set date and time.

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

Figure 9-55 System interface

System	Date And Time Time Zone	DST Sync Camera Time		
	Device Name	Device		
	Output Resolution	1920x1080 +		
	Language			
	Temperature Unit	Celsius +		
			Refresh	Apply

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

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

- 5. Set the device time manually, as shown in Figure 9-56.
- 6. Click NTP Sync button to disable synchronize time.

7. Async date and time interface

Figure 9-56 Date and time

Date Format	DD/MM/YY hh.mm.ss +	
Time Format	24H +	
Enable NTP		
NTP Server	time windows com +	
Sync Time Frequency (sec)	86400s	
Time	25/04/2022 17:41:50	

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 s	etting.			

Step 5 Set time zone.

Click **Time Zone** to enter the time zone setting interface, as shown in Figure 9-57. Time zone setting interface

Figure 9-57 Time zone

System	Date And Time	Time Zone	DST	Sync	Camera	Time				
	Time Zone		(GMT	+00:00)1	Dublin, Ed	inburgh, Lo	ondon			
									Refresh	Apply

Select a time zone from the drop-down list.

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

Step 6 Set DST.

1. Click DST to enter the DST setting interface, click DST button to enable, as shown in Figure 9-60. The button is disabled by default.



Enable Daylight Saving	Time	•						
Start Time	Mar		Last one	Sun				
End Time	Oct		Last one	Sun	1.00			
Offset Time	1 Hour							

Select a start time from the drop-down list.

Select an end time from the drop-down list.

Select an offset time from the drop-down list.

Figure 9-59 Sync camera time

System	Date And Time	Time Zone	DST	Sync Carnera Time		
	Enable Sync		-			
	Sync Time Freque	ncy (sec)	3600s			
					Refresh	Apply

Enable sync camera time, the cameras of NVR 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.				
End				

9.5.3 User Account

You can create new user accounts to manage the device.

9.5.3.1 Add User

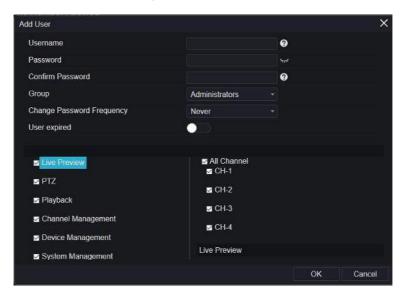
Procedure

Step 1 On the **System Setting** screen, choose **System >User** to access the **User** interface, as shown in Figure 9-60.

Figure 9-60 User interface

Record					
i Abun	User	Adv. Setting	Phone Number Allowed		
🕽 Network					
System		D	Username	Group	Operate
Information		1	aquiti	Super admin	4
General					
Security Center					
logs					
Maintenance					
Auto Robert					
					Ari.

Step 2 Click Add to add a new user, as shown in Figure 9-61. Figure 9-61 Add user



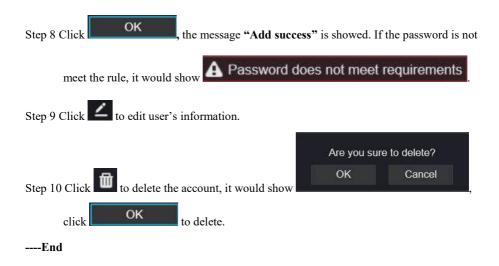
Step 3 Input username, password and confirm password.

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

Step 5 Assign the privilege to the user.

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

Step 7 Select channels to manage.



9.5.3.2 Adv.Setting

Procedure

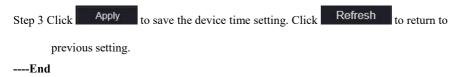
Step 1 On the System Setting screen, choose System > User > Adv. Setting to access interface,

as shown in Figure 9-62.



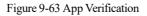
👮 Channel							
Record							
🚊 Alam	User	Adv.Setting	Phone Number /	Allowed			
S Network			ouble Authentication	_			
🗇 System		Liable C	ouble Aublent cabon				
vioreation						Refresh	Apply
General							
User Account							
Security Center							
Logs							
Mantenance							
Auto Rebort							

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



9.5.3.3 App Verification

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



User Adv.Setting Ap	p Verification				2
			Status	Remark	
		Security Code Remark(optional)	OK	Cancel	

9.5.4 Security Center

9.5.4.1 Password

Procedure

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

interface, as shown in Figure 9-64.

Figure 9-64 Password interface

-				
c	Did Password			
N	vew Password	0		
c	Confirm Password			

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

239



Valid password range [6-32] characters.

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

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

----End

9.5.4.2 Secure Email

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

Figure	9-65	Secure	Email
--------	------	--------	-------

Password	Secure Email	Secure Que	stion				
	Password						
	Email Address						
						Refresh	Apply

----End

9.5.4.3 Secure Question

If the user forgets the password and answers the security question correctly, the user can change the password to log in to the NVR..

Password	Secure Email	Secure Question		
	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	r		
	t least 1 characters for the p to 32 characters for the		Refresh	Apply

----End

9.5.5 Logs

9.5.5.1 System Logs

Procedure

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

in Figure 9-66.

Channel						
Record						
Alama	System Log Eve	nt Log				
) Network						
) Syskan	Start 24/04/202	2 17 19:09 Find 25/04/2022 17:49:08	Type Operation	Lag -	Search Export	
information	D	Stert Time	Channel	Log Type	Information	
General		25/04/2022 17:06:53		Logout	(admin) 192 168.32 199 logoul	
User Account		25/04/2022 17:05:19		Login	jadminj 192 168.32 199 login	
Security Center		25/04/2022 17.05.18		Logoul	[admin] 192.168.32.199 logout	
		25/04/2022 17:06:18		Login	(admin) 192 168 32 199 login	
Maintenance		25/04/2022 15:53:25		Login	(admin) 192 168 0 157 login	
Auto Rehool		25/04/2022 15:32:03		Logout	(admin) 127.0.0.1 logout	
runa manage		25/04/2022 15:02:40		Login	(admin) 127 0 0 1 login	
	8	25/04/2022 15:02:00		Logout	[admin] 127.0.0.1 logout	
		25/04/2022 14 40 35		Login	(admin) 127 0.0 1 login	
		25/04/2022 13:10:17		Logout	(admin) 127.0.0.1 logout	
		25/04/2022 12 56 10		Logia	(admin) 127.0.0 1 login	
		25/04/2022 12:39:20		Logout	[admin] 127.0.0.1 logout	
		25/04/2022 12:32:43		Login	(admin) 127 0.0 1 login	

Figure 9-66 System log interface

Step 2 Set start and end time from calendar.

Step 3 Select log type from drop-down list.

Step 4 Click Search to acquire log information.

Step 5 Click Export to export the logs.

----End

9.5.5.2 Event

Procedure

Step 1 On the System Setting screen, choose System >Logs > Event to access logs interface, as shown in Figure 9-67.

Figure	9-67	Event	log	interface
1.9	/ 0/		8	

Channel					
Record					
Alarm	System Log	Event Log			
Network					
System	Start 24	04/2022 17:50:26 End 25/04/2022 17:50:26	Type All -		Search Export
nformation	ю	Start Time	Channel	Log Type	Information
leneral		25/04/2022 17:50:23	Channel05	Motion Detection	Channel05
ser Account		25/04/2022 17:49:09	Channel05	Motion Detection	Channel05
ecurity Center		25/04/2022 17:48:47	Channel05	Motion Detection	Channel05
igs		25/04/2022 17:41:03	Channel05	Motion Detection	Channel05
aintenance		25/04/2022 17:37:29	Channe/05	Motion Detection	Channel05
to Reboot		25/04/2022 17:37:02	Channel05	Motion Detection	Channel05
au rebutui		25/04/2022 17:33:55	Channe/05	Motion Detection	Channel05
		25/04/2022 17:32:07	Channel05	Motion Detection	Channel05
		25/04/2022 17:31:06	Channel05	Motion Detection	Channel05
		25/04/2022 17:29:06	Channel05	Motion Detection	Channel05
		25/04/2022 17:28 16	Channel05	Motion Detection	Channel05
		25/04/2022 17:28:01	Channel05	Motion Detection	Channel05
		25/04/2022 17:25 15	Channel05	Motion Detection	Channel05

Step 2 Set start and end time from calendar.

Step 3 Select event type from drop-down list.

Step 4 Click Search to acquire log information.

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

----End

9.5.6 Maintenance

Procedure

Step 1 On the **System Setting** screen, choose **System >Maintenance** to access maintenance interface, as shown in Figure 9-68.

Figure 9-68 Maintenance interface

Maintenance
Reboot FW Update Reset
Cloud Update
Step 2 Click Reboot , the pop-up message will show you, click OK to reboot.
Step 3 Click Update , the message shows
specific location to update.
Step 4 Click Reset , the pop-up message
OK to reset.
Step 5 If the device is online, and the cloud server has the software, click the Cloud Update, it

----End

9.5.7 Auto Reboot

Procedure

Step 1 On the **System Setting** screen, choose **System > Auto Reboot** to access auto restart enable the auto restart, the screen as shown in Figure 9-69.

shows 'make sure to update', click OK to update.

Figure 9-69 Auto restart

📰 Channel				
Record				
🚊 Alam	Auto	Reboot		
S Notwork		Luske Aula Reboti 🚛		
 System 		Rehod Time Par Day + 0 OII +		
Information Centeral			Retresh	Apply
User Account				
Security Center				
Logs				
Maintenance				
Auto Bebont				

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

Step 3 Click	Apply	to save settings.	Click	Refresh	to return to previo	ous setting.
End						

9.6 Local (Supplied for IE Browser)

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

This function is only used for IE browser.

Procedure

Step 1 Click Local Download Config in local interface, as shown in Figure 9-70.

Figure 9-70 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		
Je Local				Refresh	Apply
Download Config					

Step 2 Enter the image download path.

Step 3 Enter the record download path.

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

----End