

HIKVISION



Network Video Recorder

User Manual

UD.6L0202D1984A01

Quick Start Guide

COPYRIGHT ©2015 Hangzhou Hikvision Digital Technology Co., Ltd.

ALL RIGHTS RESERVED.

Any and all information, including, among others, wordings, pictures, graphs are the properties of Hangzhou Hikvision Digital Technology Co., Ltd. or its subsidiaries (hereinafter referred to be “Hikvision”). This user manual (hereinafter referred to be “the Manual”) cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision. Unless otherwise stipulated, Hikvision does not make any warranties, guarantees or representations, express or implied, regarding to the Manual.

About this Manual

This Manual is applicable to WIFI NVR (Network Video Recorder).

The Manual includes instructions for using and managing the product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version in the company website (<http://overseas.hikvision.com/en/>).

Please use this user manual under the guidance of professionals.

Trademarks Acknowledgement

HIKVISION and other Hikvision’s trademarks and logos are the properties of Hikvision in various jurisdictions. Other trademarks and logos mentioned below are the properties of their respective owners.

Legal Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, IS PROVIDED “AS IS”, WITH ALL FAULTS AND ERRORS, AND HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY. IN NO EVENT WILL HIKVISION, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA OR DOCUMENTATION, IN CONNECTION WITH THE USE OF THIS PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS THE APPLICABLE LAW. HIKVISION SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Regulatory information

FCC information

FCC compliance: Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: This product has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This product generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this product does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.

FCC conditions

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

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

EU Conformity Statement



This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the Low Voltage Directive 2006/95/EC, the R&TTE Directive 1999/5/EC, the RoHS Directive 2011/65/EU.



2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info.



2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: www.recyclethis.info.

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (B)/NMB-3(B) standards requirements.

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

- 1) this device may not cause interference, and
- 2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radioexempts de licence.

L'exploitation est autorisée aux deux conditions suivantes :

- 1) l'appareil ne doit pas produire de brouillage, et
- 2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

Preventive and Cautionary Tips

Before connecting and operating your device, please be advised of the following tips:

- Ensure unit is installed in a well-ventilated, dust-free environment.
- Unit is designed for indoor use only.
- Keep all liquids away from the device.
- Ensure environmental conditions meet factory specifications.
- Ensure unit is properly secured to a rack or shelf. Major shocks or jolts to the unit as a result of dropping it may cause damage to the sensitive electronics within the unit.
- Use the device in conjunction with an UPS if possible.
- Power down the unit before connecting and disconnecting accessories and peripherals.
- A factory recommended HDD should be used for this device.

Table 1. 1 Recommended HDDs

Manufacturer	Type	Capacity
Seagate	WD5000LUCT	500G
Seagate	WD10JUCT	1T
Toshiba	MQ01ABD050V	500G
Toshiba	MQ01ABD100V	1T

-
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the manufacturer.

Product Key Features

General

- Connectable to network cameras, network dome and encoders.
- Connectable to the third-party network cameras like ACTI, Arecont, AXIS, Bosch, Brickcom, Canon, PANASONIC, Pelco, SAMSUNG, SANYO, SONY, Vivotek and ZAVIO, and cameras that adopt ONVIF or PSIA protocol.
- Connectable to the smart IP cameras.
- Each channel supports dual-stream.
- Up to 8 network cameras can be connected.
- Independent configuration for each channel, including resolution, frame rate, bit rate, image quality, etc.
- The quality of the input and output record is configurable.

Local Monitoring

- Support HDMI™ output.
- HDMI™ output at up to 1920×1080 resolution.
- Multiple screen display in live view is supported, and the display sequence of channels is adjustable.
- Live view screen can be switched in group, and manual switch and automatic switch live view are also provided, and the interval of automatic switch can be adjusted.
- Quick setting menu is provided for live view.
- Motion detection, video tampering, VCA (Video Content Analysis) alarm, video exception alert and video loss alert functions.
- Privacy mask.
- Multiple PTZ protocols supported; PTZ preset, patrol and pattern.
- Zooming in by clicking the mouse and PTZ tracing by dragging mouse.

HDD Management

- Two kinds of HDD capacity are selectable: 500G and 1T.
- Support S.M.A.R.T. and bad sector detection.
- HDD quota management; different capacity can be assigned to different channel.

Recording and Playback

- Holiday recording schedule configuration.
- Continuous and event video recording parameters.
- Multiple recording types: manual, continuous, alarm, motion, motion | alarm, motion & alarm, and VCA.
- 8 recording time periods with separated recording types each day.
- Pre-record and post-record for alarm, motion detection for recording, and pre-record time for schedule and manual recording.
- Searching record files by events (alarm input/motion detection/VCA).
- Tag adding for record files, searching and playing back by tags.
- Locking and unlocking record files.
- Provide a playback interface with easy and flexible operation.
- Searching and playing back record files by camera No., recording type, start time, end time, etc.
- Smart search for the selected area in the video.
- Zooming in when playback.
- Reverse playback of multi-channel.
- Supports pause, play reverse, speed up, speed down, skip forward, and skip backward when playback, and locating by dragging the mouse.
- Up to 8-ch synchronous playback.

Backup

- Export video data by USB device.
- Export video clips when playback.
- Management and maintenance of backup devices.

Alarm and Exception

- Configurable arming time of alarm input/output.
- Alarm for video loss, motion detection, VCA, video tampering, HDD full, HDD error, network disconnected, IP confliction, illegal login and abnormal record.
- Alarm triggers full screen monitoring, audible warning, notifying surveillance center, sending email and alarm output.
- Manually restore default when system is abnormal.

Other Local Functions

- Operable by mouse.
- Three-level user management; admin user is allowed to create many operating accounts and define their operating permission, which includes the limit to access any channel.
- Operation, alarm, exceptions and log recording and searching.
- Manually triggering and clearing alarms.
- Import and export of device configuration information.

Network Functions

- 1 self-adaptive 10M/100M network interfaces is provided.
- IPv6 is supported.
- TCP/IP protocol, PPPoE, DHCP, DNS, DDNS, NTP, SADP, SMTP, SNMP, NFS, and iSCSI are supported.
- TCP, UDP and RTP for unicast.
- Auto/Manual port mapping by UPnP™.
- Extranet access by HiDDNS and EZVIZ Cloud P2P.
- Remote reverse playback via RTSP.
- Support accessing by the platform via ONVIF.
- Remote search, playback, download, locking and unlocking of the record files, and the breakpoint resume is supported for downloading files.
- Remote parameters setup; remote import/export of device parameters.
- Remote view of the device status, system logs and alarm status.
- Remote HDD formatting and program upgrading.
- Remote system restart and shutdown.
- Alarm and exception information can be sent to the remote host
- Remotely start/stop recording.
- Remotely start/stop alarm output.
- Remote PTZ control.
- Voice broadcasting.
- Embedded WEB server.

Development Scalability:

- SDK for Windows and Linux system.
- Source code of application software for demo.
- Development support and training for application system.

TABLE OF CONTENTS

Product Key Features	5
Chapter 1 Introduction	11
1.1 Front Panel and Rear Panel	12
1.2 USB Mouse Operation	13
1.3 Input Method Description	14
Chapter 2 Getting Started	15
2.1 Starting Up and Shutting Down the NVR	16
2.2 Setting Admin Password	17
2.3 Using the Wizard for Basic Configuration	18
2.4 Adding and Connecting the IP Cameras	23
2.4.1 Activating the IP Camera	23
2.4.2 Adding the Online IP Cameras	24
2.4.3 Editing Connected IP Cameras and Customized Protocols	28
Chapter 3 Live View	31
3.1 Introduction of Live View	32
3.2 Operations in Live View Mode	33
3.2.1 Using the Mouse in Live View	33
3.2.2 Quick Setting Toolbar in Live View Mode	34
3.3 Adjusting Live View Settings	37
Chapter 4 PTZ Controls	39
4.1 Configuring PTZ Settings	40
4.2 PTZ Control Panel	42
4.3 Setting PTZ Presets, Patrols & Patterns	43
4.3.1 Customizing Presets	43
4.3.2 Calling Presets	43
4.3.3 Customizing Patrols	44
4.3.4 Calling Patrols	45
4.3.5 Customizing Patterns	46
4.3.6 Calling Patterns	46
4.3.7 Customizing Linear Scan Limit	47
4.3.8 Calling Linear Scan	48
4.3.9 One-touch Park	48
Chapter 5 Recording Settings	50
5.1 Configuring Parameters	51
5.2 Configuring Recording Schedule	53
5.3 Configuring Motion Detection Recording	56
5.4 Configuring Alarm Triggered Recording	58
5.5 Configuring VCA Event Recording	60
5.6 Manual Recording	62
5.7 Configuring Holiday Recording	63
5.8 Files Protection	64
Chapter 6 Playback	66

6.1	Playing Back Record Files	67
6.1.1	Playing Back by Channel.....	67
6.1.2	Playing Back by Time.....	69
6.1.3	Playing Back by Event Search.....	69
6.1.4	Playing Back by Tag	71
6.1.5	Smart Playback	73
6.1.6	Playing Back by System Logs	75
6.1.7	Playing Back External File	76
6.2	Auxiliary Functions of Playback	78
6.2.8	Playing Back Frame by Frame.....	78
6.2.9	Digital Zoom.....	78
6.2.10	Reverse Playback of Multi-channel	78
Chapter 7	Backup	80
7.1	Backing up Record Files	81
7.1.1	Quick Export.....	81
7.1.2	Backing up by Normal Video Search.....	82
7.1.3	Backing up by Event Search	86
7.1.4	Backing up Video Clips	87
7.2	Managing Backup Devices.....	89
Chapter 8	Alarm Settings	92
8.1	Setting Motion Detection Alarm.....	93
8.2	Setting Sensor Alarms	95
8.3	Detecting Video Loss Alarm.....	98
8.4	Detecting Video Tampering Alarm	100
8.5	Handling Exceptions Alarm.....	102
8.6	Setting Event Hint Display.....	105
8.7	Triggering or Clearing Alarm Output Manually	106
Chapter 9	VCA Alarm.....	107
9.1	Face Detection	108
9.2	Vehicle Detection	109
9.3	Line Crossing Detection	111
9.4	Intrusion Detection	113
9.5	Region Entrance Detection.....	115
9.6	Region Exiting Detection	116
9.7	Loitering Detection.....	116
9.8	People Gathering Detection.....	116
9.9	Fast Moving Detection	116
9.10	Parking Detection	117
9.11	Unattended Baggage Detection	117
9.12	Object Removal Detection.....	117
9.13	Audio Exception Detection	118
9.14	Sudden Scene Change Detection	119
9.15	Defocus Detection	119
9.16	PIR Alarm	119

Chapter 10	VCA Search	120
10.1	Face Search	121
10.2	Behavior Search	123
10.3	Plate Search	124
10.4	People Counting	125
10.5	Heat Map	127
Chapter 11	Network Settings	128
11.1	Configuring General Settings	129
11.2	Configuring Advanced Settings	130
11.2.1	Configuring Wireless Network	130
11.2.2	Configuring EZVIZ Cloud P2P	131
11.2.3	Configuring DDNS	132
11.2.4	Configuring NTP Server	136
11.2.5	Configuring SNMP	137
11.2.6	Configuring Remote Alarm Host	137
11.2.7	Configuring Multicast	138
11.2.8	Configuring RTSP	138
11.2.9	Configuring Server and HTTP Ports	139
11.2.10	Configuring Email	139
11.2.11	Configuring NAT	141
11.3	Checking Network Traffic	144
11.4	Configuring Network Detection	145
11.4.1	Testing Network Delay and Packet Loss	145
11.4.2	Exporting Network Packet	145
11.4.3	Checking the Network Status	146
11.4.4	Checking Network Statistics	147
Chapter 12	HDD Management.....	149
12.1	Initializing HDD.....	150
12.2	Configuring Quota Mode.....	152
12.3	Checking HDD Status	153
12.4	HDD Detection.....	154
12.5	Configuring HDD Error Alarms	156
Chapter 13	Camera Settings	157
13.1	Configuring OSD Settings.....	158
13.2	Configuring Privacy Mask.....	159
13.3	Configuring Video Parameters	160
Chapter 14	NVR Management and Maintenance	161
14.1	Viewing System Information.....	162
14.1.1	Viewing Device Information.....	162
14.2	Searching & Export Log Files	163
14.3	Importing/Exporting IP Camera Info	166
14.4	Importing/Exporting Configuration Files	167
14.5	Upgrading System	168
14.5.1	Upgrading by Local Backup Device	168

14.5.2	Upgrading by FTP	168
14.6	Restoring Default Settings.....	170
Chapter 15	Others.....	171
15.1	Configuring General Settings	172
15.2	Configuring DST Settings	173
15.3	Configuring More Settings for NVR	174
15.4	Managing User Accounts.....	175
15.4.1	Adding a User	175
15.4.2	Deleting a User	177
15.4.3	Editing a User	178
Chapter 16	Appendix	180
16.1	Glossary.....	181
16.2	Troubleshooting.....	182
16.3	Summary of Changes	188
16.4	List of Compatible IP Cameras.....	190
	List of Hikvision IP Cameras	190
	List of Third-party IP Cameras	191

Chapter 1 Introduction

1.1 Front Panel and Rear Panel

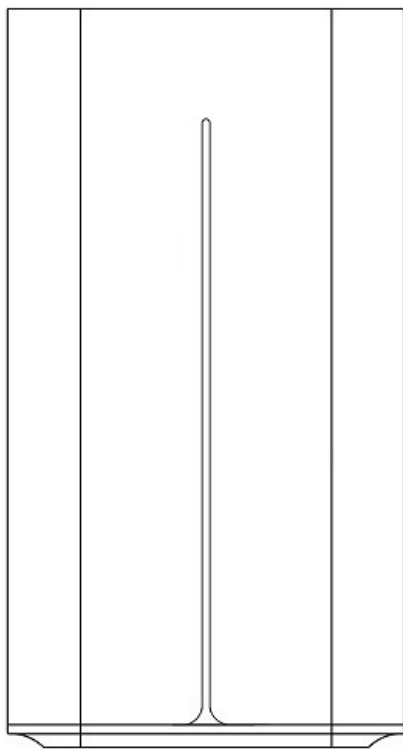


Figure 1. 1 Front Panel

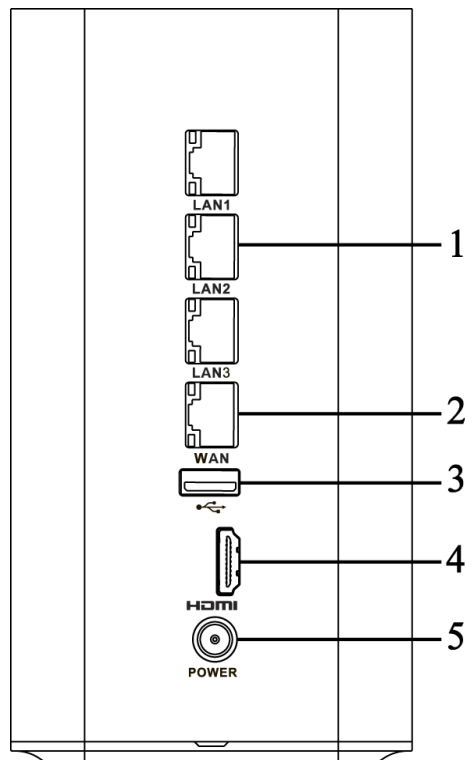


Figure 1. 2 Rear Panel

Table 1. 1 Description of Rear Panel Interface

No.	Name	Description
1	LAN Interface (1 ~ 3)	3 RJ-45 10 /100Mbps network interfaces for LAN (Local Area Networks).
2	WAN Interface	1 RJ-45 10 /100 Mbps network interface for WAN (Wide Area Networks).
3	USB Interface	Universal Serial Bus (USB) ports for additional devices such as USB mouse and USB writer.
4	HDMI	HDMI video output connector.
5	POWER	12VDC Power supply.

1.2 USB Mouse Operation

A regular 3-button (Left/Right/Scroll-wheel) USB mouse can also be used with this NVR. To use a USB mouse:

1. Plug USB mouse into the USB interface on the rear panel of the NVR.
2. The mouse should automatically be detected. If in a rare case that the mouse is not detected, the possible reason may be that the two devices are not compatible, please refer to the recommended the device list from your provider.

The operation of the mouse:

Table 1. 2 Description of the Mouse Control

Name	Action	Description
Left-Click	Single-Click	Live view: Select channel and show the quick set menu. Menu: Select and enter.
	Double-Click	Live view: Switch between single-screen and multi-screen.
	Click and Drag	PTZ control: pan, tilt and zoom. Video tampering, privacy mask and motion detection: Select target area. Digital zoom-in: Drag and select target area. Live view: Drag channel/time bar.
Right-Click	Single-Click	Live view: Show menu. Menu: Exit current menu to upper level menu.
Scroll-Wheel	Scrolling up	Live view: Previous screen. Menu: Previous item.
	Scrolling down	Live view: Next screen. Menu: Next item.

1.3 Input Method Description



Figure 1.3 Soft Keyboard (1)



Figure 1.4 Soft Keyboard (2)

Description of the buttons on the soft keyboard:

Table 1.3 Description of the Soft Keyboard Icons

Figure 1.5

Icon	Description	Icon	Description
	Number		English letter
	Lowercase/Uppercase		Backspace
	Switch the keyboard		Space
	Positioning the cursor		Exit
	Symbols		Reserved

Chapter 2 Getting Started

2.1 Starting Up and Shutting Down the NVR

Purpose:

Proper startup and shutdown procedures are crucial to expanding the life of the NVR.

Before you start:

1. Establish the connection between the NVR and Internet via the WAN interface.
2. Check that the voltage of the extra power supply is the same with the NVR's requirement, and the ground connection is working properly.

Starting up the NVR:

Step:

Check the power supply is plugged into an electrical outlet. It is **HIGHLY** recommended that an Uninterruptible Power Supply (UPS) be used in conjunction with the device.

During the starting up program, a splash screen appears on the monitor.

Shutting down the NVR

Steps:

1. Enter the Shutdown menu.

Menu > Shutdown

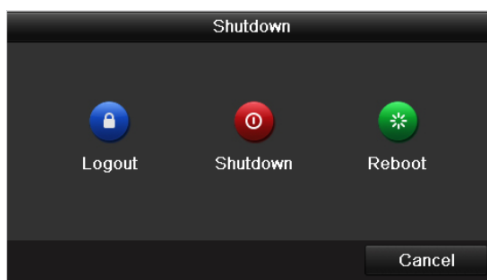


Figure 2. 1 Shutdown Menu

2. Click the **Shutdown** button.
3. Click the **Yes** button.
4. Unplug the power supply when the attention pops up.

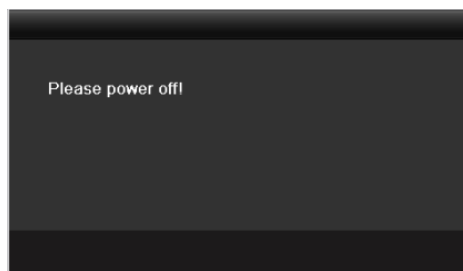


Figure 2. 2 Shutdown Attention

Rebooting the NVR

In the Shutdown menu, you can also reboot the NVR.

Steps:

1. Enter the **Shutdown** menu by clicking Menu > Shutdown.
2. Click the **Logout** button to lock the NVR or the **Reboot** button to reboot the NVR.

2.2 Setting Admin Password

Purpose:

For the first-time access, you need to activate the device by setting an admin password. No operation is allowed before activation.

Steps:

1. Input the same password in the text field of **Create New Password** and **Confirm New Password**.

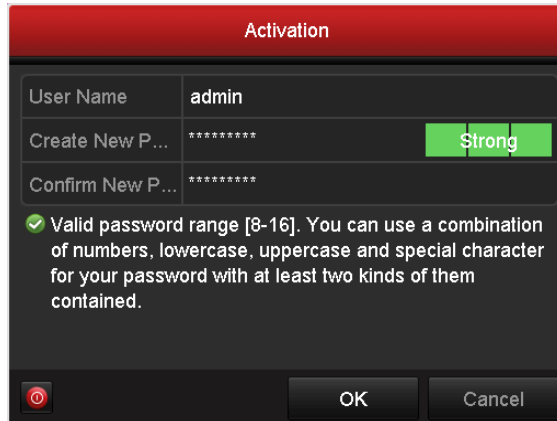
The image shows a dialog box titled "Activation" with a red header bar. It contains three input fields: "User Name" with the value "admin", "Create New P..." with masked characters "*****" and a green "Strong" indicator, and "Confirm New P..." also with masked characters "*****". Below the fields is a green checkmark icon and a message: "Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained." At the bottom are three buttons: a red power button icon, "OK", and "Cancel".

Figure 2. 3 Settings Admin Password



STRONG PASSWORD RECOMMENDED— We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

2. Click **OK** to save the password and activate the device.



For the old version device, if you update it to the new version, the following dialog box will pop up once the device starts up. You can click **YES** and follow the wizard to set a strong password.

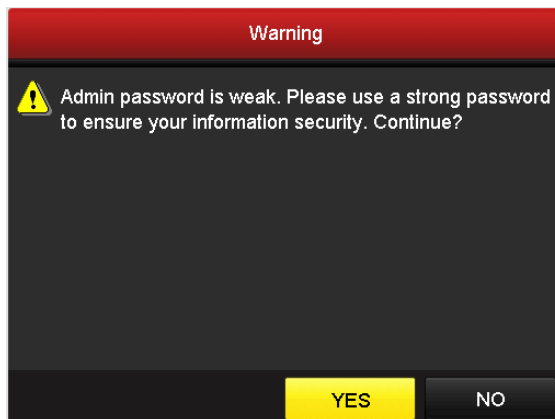
The image shows a dialog box titled "Warning" with a red header bar. It contains a yellow triangle warning icon and the text: "Admin password is weak. Please use a strong password to ensure your information security. Continue?". At the bottom are two buttons: "YES" (yellow) and "NO" (black).

Figure 2. 4 Warning

2.3 Using the Wizard for Basic Configuration

Purpose:

After admin password is set, the setup wizard pops up automatically. It can walk you through some basic settings of the NVR.

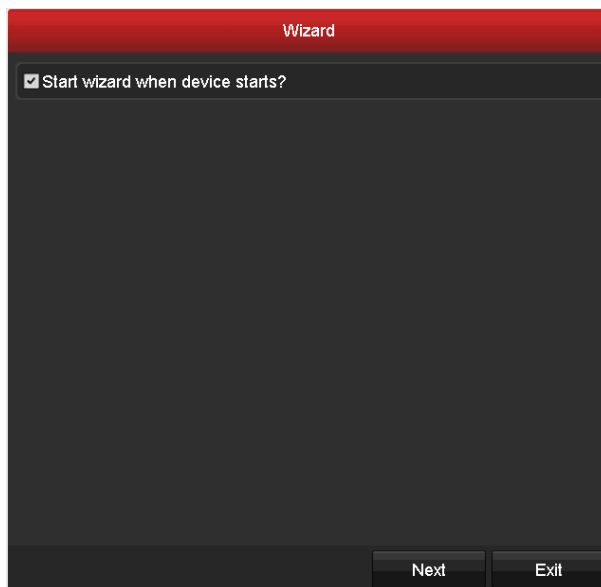


Figure 2. 5 Start Wizard Interface

Steps:

1. If you don't want to use the setup wizard at that moment, click the **Exit** button. You can also choose to use the Setup Wizard next time by leaving the "Start wizard when the device starts?" checkbox checked.
2. Click the **Next** button to enter the **Date and Time Settings** interface.

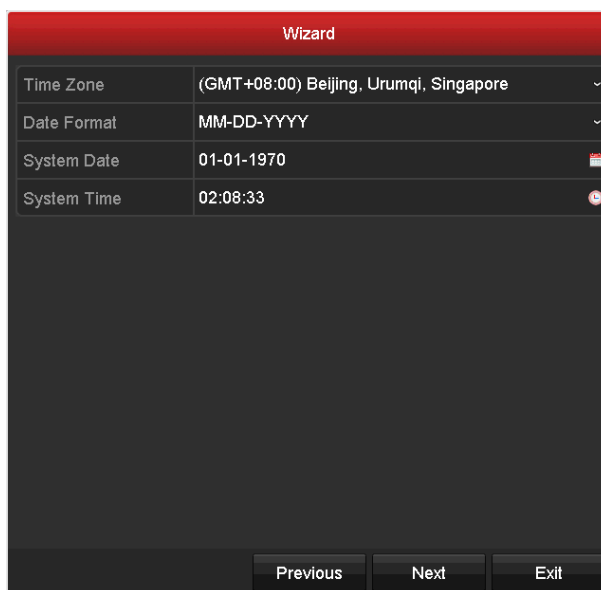


Figure 2. 6 Date and Time Settings

3. After the time settings, click **Next** button which takes you to the WAN Setup Wizard window.

Wizard	
Please select the network connection mode to access the internet:	
Connection Mode	<input checked="" type="radio"/> PPPOE <input type="radio"/> Dynamic IP Address <input type="radio"/> Statistic IP Address
Account	Account A
Password	*****
<div>Previous Next Exit</div>	

Figure 2. 7 WAN Settings

4. Select the **Connection Mode** as **PPPoE** and input **Account** and **Password**.
5. Click **Next** button to enter WIFI settings interface.

Wizard	
Set up wireless network:	
SSID	NVR489794994
Security Mode	WPA2-PSK
Key	264EQJWE
<div>Previous Next Exit</div>	

Figure 2. 8 WIFI Settings

6. Edit **SSID** and select **Security Type**. Input **Network Security Key** if Security Type does not set as **Disable**.
7. Click **Next** button which takes you to the General Network Configuration window.

Wizard	
NIC Type	10M/100M Self-adaptive
Enable DHCP	<input type="checkbox"/>
IPv4 Address	192.168.254.100
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	192.168.254.1
Preferred DNS Serv...	192.168.254.1
Alternate DNS Server	
<div>Previous Next Exit</div>	

Figure 2. 9 General Network Configuration

- Click **Next** button after you configured the general network parameters. Then you will enter the **EZVIZ Cloud P2P** interface. Configure the EZVIZ Cloud P2P according to your needs.

Wizard	
Enable	<input type="checkbox"/>
Access Type	EZVIZ Cloud P2P
Server Address	dev.ezviz7.com <input type="checkbox"/> Custom
Enable Stream Encr...	<input type="checkbox"/>
Verification Code	
Status	Offline
<div>Previous Next Exit</div>	

Figure 2. 10 EZVIZ Cloud P2P interface

- Click **Next** button to enter the **Advanced Network Parameter** interface. You can enable UPnP, enable DDNS and set other ports according to your need.

Wizard	
Server Port	8000
HTTP Port	80
RTSP Port	554
Enable UPnP	<input checked="" type="checkbox"/>
Enable DDNS	<input checked="" type="checkbox"/>
DDNS Type	HiDDNS
Area/Country	Custom
Server Address	www.hik-online.com
Device Domain Name	
Status	Connecting the address server failed.
User Name	
Password	
<div>Previous Next Exit</div>	

Figure 2. 11 Advanced Network Parameters

10. After configuration finishes, click **Next** button to enter **HDD Management** interface.

Wizard					
L...	Capacity	Status	Property	Type	Free Space
1	465.77GB	Normal	R/W	Local	456.00GB

Init

Previous Next Exit

Figure 2. 12 HDD Management

11. To initialize the HDD, click the **Init** button. Initialization removes all the data saved in the HDD.
12. Click **Next** button. You enter the Adding IP Camera interface.
13. Click **Next** button to enter the **IP Camera Management** interface.
14. Click **Search** to search the online IP Camera and the **Security** status shows whether it is active or inactive.
Before adding the camera, make sure the IP camera to be added is in active status.
If the camera is in inactive status, you can click the inactive icon of the camera to set the password to activate it. You can also select multiple cameras from the list and click the **One-touch Activate** to activate the cameras in batch.
Click the **Add** to add the camera.



Figure 2. 13 IP Camera Management

15. Click **Next** button. Configure the recording for the added IP Cameras.

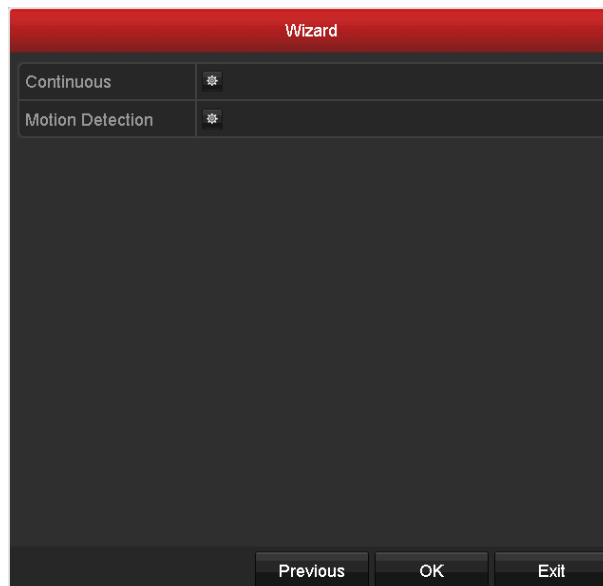


Figure 2. 14 Record Settings

16. Click **OK** to complete the startup Setup Wizard.

2.4 Adding and Connecting the IP Cameras

2.4.1 Activating the IP Camera

Purpose:

Before adding the camera, make sure the IP camera to be added is in active status.

Steps:

1. Enter the IP Camera management interface.

Menu > Camera > Camera

For the IP camera detected online in the same network segment, the **Security** status shows whether it is active or inactive.



Figure 2. 15 IP Camera Management Interface

2. Click the inactive icon of the camera to enter the following interface to activate it. You can also select multiple cameras from the list and click the **One-touch Activate** to activate the cameras in batch.

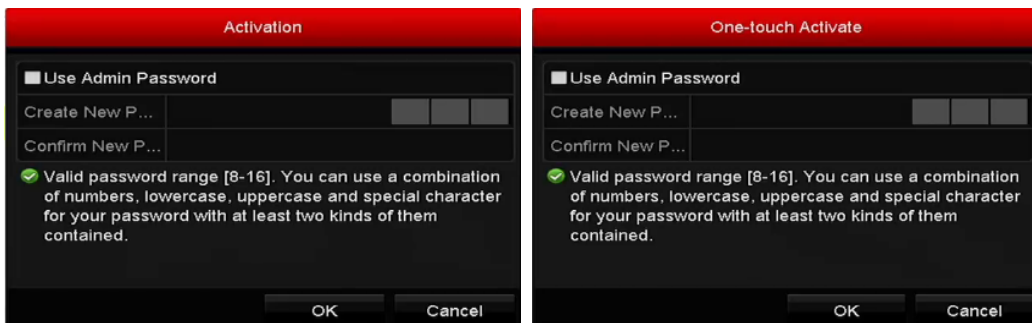


Figure 2. 16 Activate the Camera

3. Set the password of the camera to activate it.

Use Admin Password: when you check the checkbox, the camera (s) will be configured with the same admin password of the operating NVR.



Figure 2. 17 Set New Password

Create New Password: If the admin password is not used, you must create the new password for the camera and confirm it.



STRONG PASSWORD RECOMMENDED– We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

4. Click OK to finish the activating of the IP camera. And the security status of camera will be changed to Active.

2.4.2 Adding the Online IP Cameras

Purpose:

The one of the main functions of the NVR is to connect the network cameras and save the video got from it. So before you can get a live view or record of the video, you should add the network cameras to the connection list of the device.

Before you start:

Establish the network connection between IPC and the NVR via wired or wireless network.

Wired network: connect the Ethernet port of computer to the LAN interface of NVR. And configure the IP address of computer on the principle that the network segment is the same with NVR, that is 192.168.254. x.x.x.

Wireless network: the default SSID and key of wireless network provided by NVR is in the tag of device.



Hikvision WIFI IP camera which has default user name and password and is within 2m distance from the NVR will be added automatically.

Ensure the network connection is valid and correct. For detailed checking and configuring of the network, please see *Chapter 11.3 Checking Network Traffic* and *Chapter 11.4 Configuring Network Detection*.

• **OPTION 1:**

Steps:

1. Right-click the mouse when you in the live view mode to show the right-click menu.

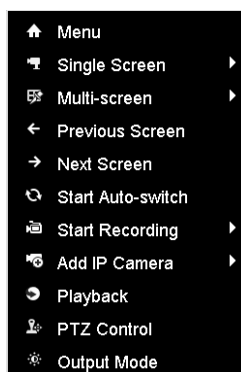


Figure 2. 18 Right-click Menu

2. Positioning the cursor to the **Add IP Camera** and click to select **Manual** in the pop-up menu to enter the IP Camera Management interface.

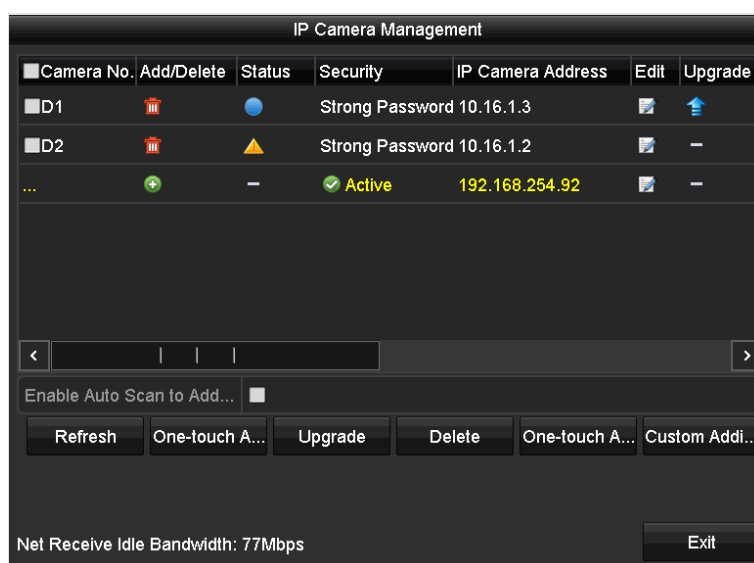









Figure 2. 19 Adding IP Camera Interface



3. Select the IP camera from the list and click the  button to add the camera (with the same admin password of the NVR). Or you can click the **One-touch Adding** button to add all cameras (with the same admin password) from the list.



Make sure the camera to add has already been activated by setting the admin password, and the admin password of the camera is the same with the NVR.

Table 2. 1 Explanation of the icons

Icon	Explanation	Icon	Explanation
	Edit basic parameters of the camera		Add the detected IP camera.
	The camera is connected.		The camera is disconnected; you can click the icon to get the exception information of camera.
	Advanced settings of the camera.		Delete the IP camera

Icon	Explanation	Icon	Explanation
	Upgrade the connected IP camera.		Show the security status of the camera to be active/inactive or the password strength (strong/medium/weak/risk)

4. To add other IP cameras:

- 1) Click the **Custom Adding** button to pop up the Add IP Camera (Custom) interface.

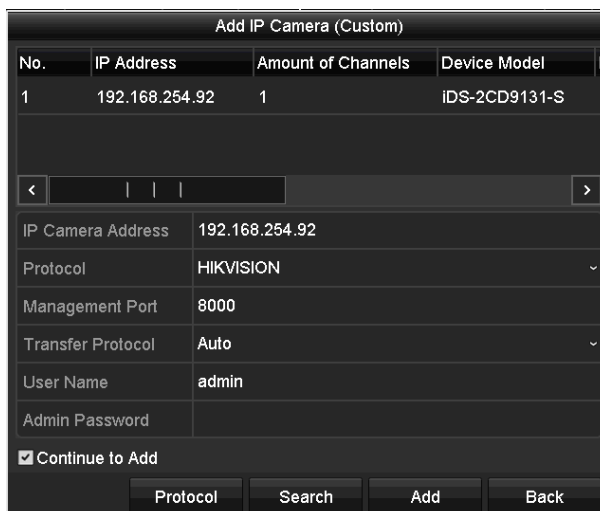


Figure 2. 20 Custom Adding IP Camera Interface

- 2) You can edit the IP address, protocol, management port, and other information of the IP camera to be added.

- 3) Click **Add** to add the camera.

• **OPTION 2:**

Steps:

1. Enter the Camera Management interface.

Menu > Camera > Camera

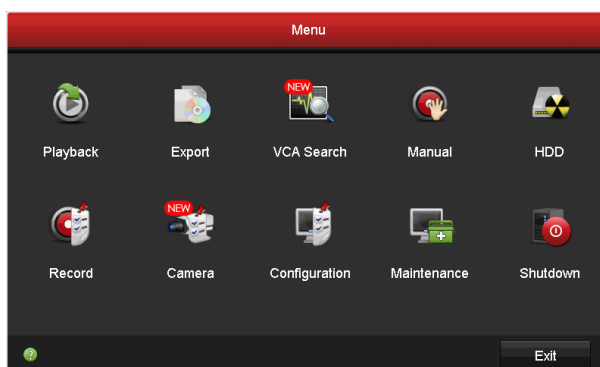


Figure 2. 21 Main Menu

2. Repeat the step 3 and 4 of OPTION 1 to add the camera.



Figure 2.22 IP Camera Management Interface

Table 2.2 Explanation of the icons

Icon	Explanation	Icon	Explanation
	Edit basic parameters of the camera		Add the detected IP camera.
	The camera is connected; you can click the icon to get the live view of the camera.		The camera is disconnected; you can click the icon to get the exception information of camera.
	Advanced settings of the camera.		Delete the IP camera
	Upgrade the connected IP camera.	Security	Show the security status of the camera to be active/inactive or the password strength (strong/weak/risk)

- (For the encoders with multiple channels only) check the checkbox of Channel No. in the pop-up window, as shown in the following figure, and click **OK** to finish adding.




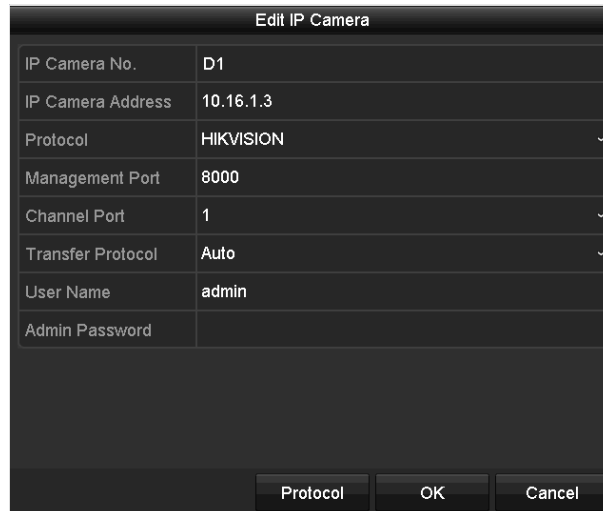
Figure 2.23 Selecting Multiple Channels

2.4.3 Editing Connected IP Cameras and Customized Protocols

After the adding of the IP cameras, the basic information of the camera lists in the page, you can configure the basic setting of the IP cameras.

Steps:

1. Click the  icon to edit the parameters; you can edit the IP address, protocol and other parameters.




Edit IP Camera	
IP Camera No.	D1
IP Camera Address	10.16.1.3
Protocol	HIKVISION
Management Port	8000
Channel Port	1
Transfer Protocol	Auto
User Name	admin
Admin Password	
<div> Protocol OK Cancel </div>	

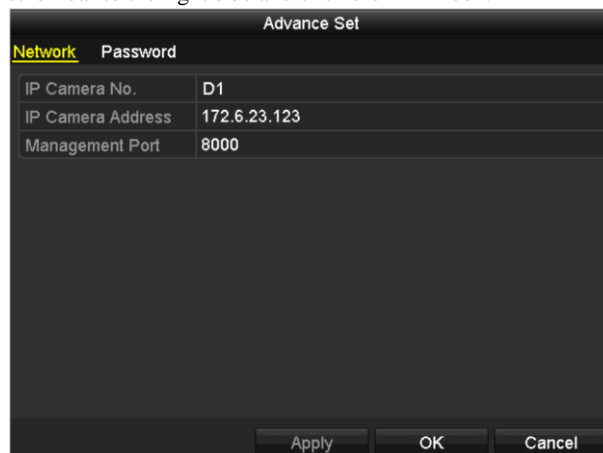
Figure 2. 24 Edit the Parameters

2. Click **OK** to save the settings and exit the editing interface.

To edit advanced parameters:

Steps:

1. Drag the horizontal scroll bar to the right side and click the  icon.



Advance Set	
Network	Password
IP Camera No.	D1
IP Camera Address	172.6.23.123
Management Port	8000
<div> Apply OK Cancel </div>	

Figure 2. 25 Network Configuration of Camera

2. You can edit the **Network** information and the **Password** of the camera.
3. Click **Apply** to save the settings and click **OK** to exit the interface.

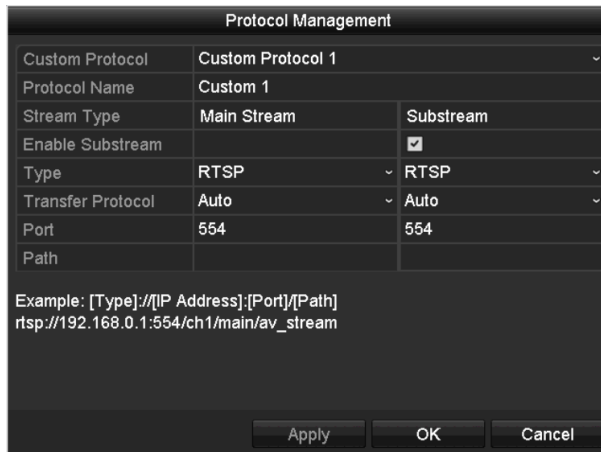
Configuring the customized protocols

Purpose:

To connect the network cameras which are not configured with the standard protocols, you can configure the customized protocols for them.

Steps:

1. Click the **Protocol** button in the custom adding IP camera interface to enter the protocol management interface.



The screenshot shows a 'Protocol Management' dialog box. It contains a table with the following fields:

Protocol Management		
Custom Protocol	Custom Protocol 1	
Protocol Name	Custom 1	
Stream Type	Main Stream	Substream
Enable Substream		<input checked="" type="checkbox"/>
Type	RTSP	RTSP
Transfer Protocol	Auto	Auto
Port	554	554
Path		

Below the table, there is an example URL: `Example: [Type]://[IP Address]:[Port]/[Path]`
`rtsp://192.168.0.1:554/ch1/main/av_stream`

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

Figure 2. 26 Protocol Management Interface

There are 16 customized protocols provided in the system, you can edit the protocol name; and choose whether to enable the sub-stream.

2. Choose the protocol type of transmission and choose the transfer protocols.



Before customizing the protocol for the network camera, you have to contact the manufacturer of the network camera to consult the URL (uniform resource locator) for getting main stream and sub-stream.

The format of the URL is: [Type]://[IP Address of the network camera]:[Port]/[Path].

Example: `rtsp://192.168.1.55:554/ch1/main/av_stream`.

- **Protocol Name:** Edit the name for the custom protocol.
- **Enable Substream:** If the network camera does not support sub-stream or the sub-stream is not needed leave the checkbox empty.
- **Type:** The network camera adopting custom protocol must support getting stream through standard RTSP.
- **Transfer Protocol:** Select the transfer protocol for the custom protocol.
- **Port:** Set the port No. for the custom protocol.
- **Path:** Set the resource path for the custom protocol. E.g., `ch1/main/av_stream`.



The protocol type and the transfer protocols must be supported by the connected network camera.

After adding the customized protocols, you can see the protocol name is listed in the drop-down list, please refer to Figure 2. 27.

No.	IP Address
1	172.6.23.124

PELCO
 PSIA
 SAMSUNG
 SANYO
 SONY
 VIVOTEK
 ZAVIO
 Custom 1
 Custom 2
 Custom 3

IP Camera Address
 Protocol: ONVIF
 Management Port: 80
 User Name: admin
 Admin Password:

Protocol Search Add Back

Figure 2. 27 Protocol Setting

3. Choose the protocols you just added to validate the connection of the network camera.

Chapter 3 Live View





3.1 Introduction of Live View

Live view shows you the video image getting from each camera in real time. The NVR automatically enters Live View mode when powered on. It is also at the very top of the menu hierarchy.

Live View Icons

In the live view mode, there are icons at the upper-right of the screen for each channel, showing the status of the record and alarm in the channel, so that you can know whether the channel is recorded, or whether there are alarms occur as soon as possible.

Table 3. 1 Description of Live View Icons

Icons	Description
	Alarm (video loss, video tampering, motion detection, alarm or VCA alarm)
	Record (manual record, continuous record, motion detection, alarm record or VCA alarm triggered record)
	Alarm & Record
	Event/Exception (motion detection, alarm, VCA alarm or exception information, appears at the lower-left corner of the screen. Please refer to <i>Chapter 8.6 Setting Alarm Response Actions</i> for details.)

3.2 Operations in Live View Mode

In live view mode, there are many functions provided. The functions are listed below.

- **Single Screen:** showing only one screen on the monitor.
- **Multi-screen:** showing multiple screens on the monitor simultaneously.
- **Auto-switch:** the screen is auto switched to the next one. And you must set the dwell time for each screen on the configuration menu before enabling the auto-switch.

Menu>Configuration>Live View>Dwell Time.

- **Start Recording:** continuous record and motion detection record are supported.
- **Output Mode:** select the output mode to Standard, Bright, Gentle or Vivid.
- **Playback:** playback the recorded videos for current day.
- **PTZ Control:** enter PTZ control interface to rotate the PTZ.
- **Add IP Camera:** the shortcut to the IP camera management interface.

3.2.1 Using the Mouse in Live View

Table 3. 2 Mouse Operation in Live View

Name	Description
Menu	Enter the main menu of the system by right-clicking the mouse.
Single Screen	Switch to the single full screen by choosing channel number from the drop-down list.
Multi-screen	Adjust the screen layout by choosing from the drop-down list.
Previous Screen	Switch to the previous screen.
Next Screen	Switch to the next screen.
Start/Stop Auto-switch	Enable/disable the auto-switch of the screens.
Start Recording	Start continuous recording or motion detection recording of all channels.
Add IP Camera	Enter the IP Camera management interface, and manage the cameras.
Playback	Enter the playback interface and start playing back the video of the selected channel immediately.
PTZ Control	Enter PTZ control interface to rotate the PTZ to desired view.
Output Mode	Four modes of output supported, including Standard, Bright, Gentle and Vivid.



The *dwell time* of the live view configuration must be set before using **Start Auto-switch**.

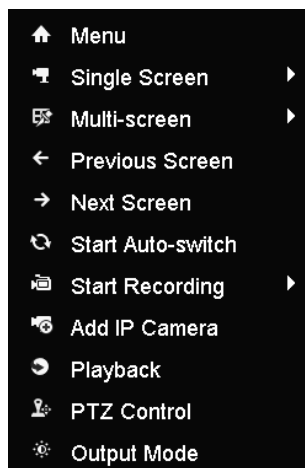


Figure 3. 1 Right-click Menu

3.2.2 Quick Setting Toolbar in Live View Mode

On the screen of each channel, there is a quick setting toolbar which shows when you single-click the mouse in the corresponding screen.



Figure 3. 2 Quick Setting Toolbar

Table 3. 3 Description of Quick Setting Toolbar Icons

Icon	Description	Icon	Description	Icon	Description
	Enable/Disable Manual Record		Instant Playback		Mute/Audio on
	PTZ Control		Digital Zoom		Image Settings
	Face Detection		Live View Strategy		Information
	Close				



Instant Playback only shows the record in last five minutes. If no record is found, it means there is no record during the last five minutes.



Digital Zoom can zoom in the selected area to the full screen. You can left-click and draw to select the area to zoom in, as shown in Figure 3. 3.



Figure 3.3 Digital Zoom



Image Settings icon can be selected to enter the Image Settings menu.

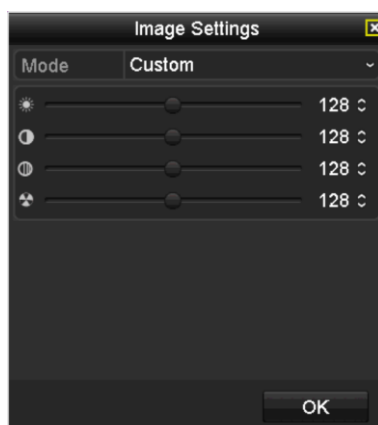


Figure 3.4 Image Settings- Preset

You can set the image parameters like brightness, contrast, saturation and hue.

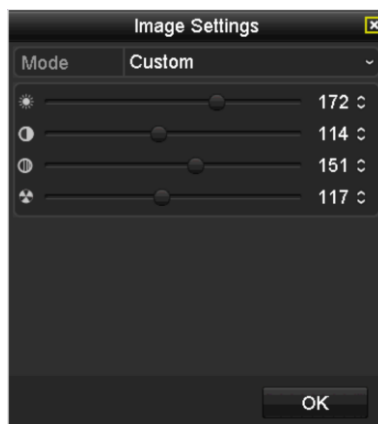


Figure 3.5 Image Settings- Customize



Live View Strategy can be selected to set strategy, including Real-time, Balanced, Fluency.

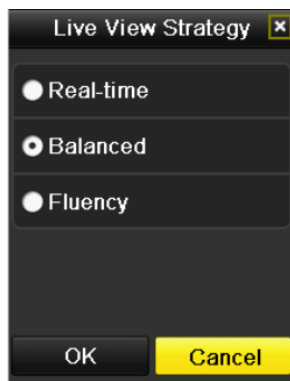


Figure 3. 6 Live View Strategy

3.3 Adjusting Live View Settings

Purpose:

Live View settings can be customized according to different needs. You can configure the output interface, dwell time for screen to be shown, mute or turning on the audio, the screen number for each channel, etc.

Steps:

1. Enter the Live View Settings interface.

Menu > Configuration > Live View

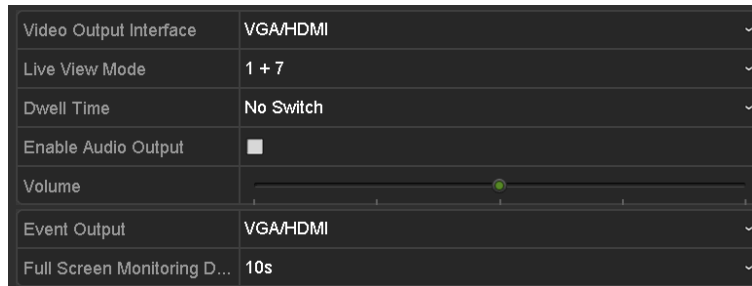


Figure 3. 7 Live View Settings


The settings available in this menu include:


- **Video Output Interface:** Designates the output to configure the settings for, and only HDMI™ is selectable.
- **Live View Mode:** Designates the display mode to be used for live view.
- **Dwell Time:** The time in seconds to dwell between switching of channels when enabling auto-switch in live view.
- **Enable Audio Output:** Enable/disable audio output for the selected video output.
- **Volume:** Adjust the volume of live view, playback and two-way audio for the selected output interface.
- **Event Output:** Designates the output to show event video.
- **Full Screen Monitoring Dwell Time:** The time in seconds to show alarm event on full screen.



2. Setting Cameras Order



Figure 3. 8 Live View Camera Order

- 1) Select a **View** mode in .
- 2) Select the small window, and double-click on the channel number to display the channel on the window.

If you do not want the camera to be displayed on the live view interface, click the corresponding  to stop it.

You can also click  button to start live view for all the channels and click  to stop all the live view.
- 3) Click the **Apply** button to save the setting.

Chapter 4 PTZ Controls

4.1 Configuring PTZ Settings

Purpose:

Follow the procedure to set the parameters for PTZ. The configuring of the PTZ parameters should be done before you control the PTZ camera.

Steps:

1. Enter the PTZ Settings interface.

Menu > Camera > PTZ



Figure 4. 1 PTZ Settings

2. Click the **PTZ Parameter Settings** button to set the RS-485 parameters.



Figure 4. 2 PTZ General Settings

3. Choose the camera for PTZ setting in the **Camera** drop-down list.
4. Enter the parameters of the PTZ camera.



All the parameters should be exactly the same as the PTZ camera parameters.

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

4.2 PTZ Control Panel

To enter the PTZ control panel, there are two ways supported.

OPTION 1:

In the PTZ settings interface, click the **PTZ** button on the lower-right corner.

OPTION 2:

In the Live View mode, click the PTZ Control icon  on quick settings bar, or select the PTZ Control in the right-click menu.

Click the **Configuration** button on the control panel, and you can enter the PTZ Settings interface.










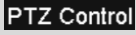

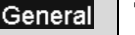






In PTZ control mode, the PTZ panel will be displayed when a mouse is connected with the device. If no mouse is connected, the **PTZ** icon appears in the lower-left corner of the window, indicating that this camera is in PTZ control mode.



Figure 4. 3 PTZ Panel

Table 4. 1 Description of the PTZ panel icons

Icon	Description	Icon	Description	Icon	Description
	Direction buttons and auto-cycle button		Zoom+, Focus+, Iris+		Zoom-, Focus-, Iris-
	The speed of the PTZ movement		Light on/off		Wiper on/off
	3D-Zoom		Image Centralization		Menu
	Switch to the PTZ control interface		Switch to the one-touch control interface		Switch to the general settings interface
	Previous item		Next item		Exit
	Minimize windows				

4.3 Setting PTZ Presets, Patrols & Patterns

Before you start:

Please make sure that the presets, patrols and patterns are supported by PTZ protocols.

4.3.1 Customizing Presets

Purpose:

Follow the steps to set the Preset location which you want the PTZ camera to point to when an event takes place.

Steps:

1. Enter the PTZ Control interface.

Menu > Camera > PTZ



Figure 4. 4 PTZ Settings

2. Use the directional button to wheel the camera to the location where you want to set preset; and the zoom and focus operations can be recorded in the preset as well.
3. Enter the preset No. (1~255) in the preset text field, and click the **Set** button to link the location to the preset. Repeat the steps 2-3 to save more presets.

You can click the **Clear** button to clear the location information of the preset, or click the **Clear All** button to clear the location information of all the presets.

4.3.2 Calling Presets

Purpose:

This feature enables the camera to point to a specified position such as a window when an event takes place.

Steps:


1. Enter PTZ Control interface. For details, please refer to *4.2 PTZ Control Panel*.
2. Choose **Camera** in the drop-down list.
3. Click the  button to show the general settings of the PTZ control.



Figure 4. 5 PTZ Panel - General

4. Input the preset No. in the corresponding text field.
5. Click the **Call Preset** button to call it.

4.3.3 Customizing Patrols

Purpose:

Patrols can be set to move the PTZ to different key points and have it stay there for a set duration before moving on to the next key point. The key points are corresponding to the presets. The presets can be set following the steps above in *Customizing Presets*.

Steps:

1. Enter the PTZ Control interface.
Menu > Camera > PTZ



Figure 4. 6 PTZ Settings

2. Select patrol No. in the drop-down list of patrol.
3. Click the **Set** button to add key points for the patrol.

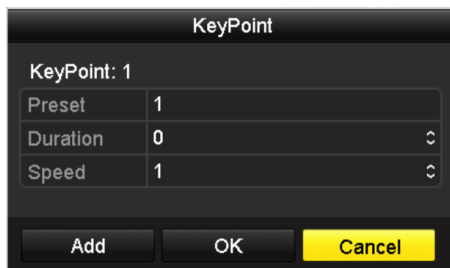


Figure 4.7 Key point Configuration

4. Configure key point parameters, including the **Preset** No., **Duration** of staying for one key point and **Speed** of patrol.
KeyPoint No.: determines the order at which the PTZ will follow while cycling through the patrol.
Preset: PTZ will rotate automatically to the set preset No. when execute the keypoint.
Duration: refers to the time span to stay at the corresponding key point.
Speed: defines the speed at which the PTZ will move from one key point to the next.
5. Click the **Add** button to add the next key point to the patrol, and you can click the **OK** button to save the key point to the patrol.
You can delete all the key points by clicking the **Clear** button for the selected patrol, or click the **Clear All** button to delete all the key pints for all patrols.

4.3.4 Calling Patrols

Purpose:

Calling a patrol makes the PTZ to move according the predefined patrol path.

Steps:


1. Enter PTZ Control interface. For details, please refer to 4.2 PTZ Control Panel.
2. Click the  button to show the general settings of the PTZ control.



Figure 4.8 PTZ Panel - General

3. Select a patrol in the drop-down list and click the **Call Patrol** button to call it.
4. You can click the **Stop Patrol** button to stop calling it.

4.3.5 Customizing Patterns

Purpose:

Patterns can be set by recording the movement of the PTZ. You can call the pattern to make the PTZ movement according to the predefined path.

Steps:

1. Enter the PTZ Control interface.

Menu > Camera > PTZ



Figure 4. 9 PTZ Settings

2. Choose pattern number in the drop-down list.
3. Click the **Start** button and click corresponding buttons in the control panel to move the PTZ camera, and click the **Stop** button to stop it.


The movement of the PTZ is recorded as the pattern.

4.3.6 Calling Patterns

Purpose:

Follow the procedure to move the PTZ camera according to the predefined patterns.

Steps:

1. Enter PTZ Control interface. For details, please refer to 4.2 PTZ Control Panel.
2. Click the  button to show the General settings interface.

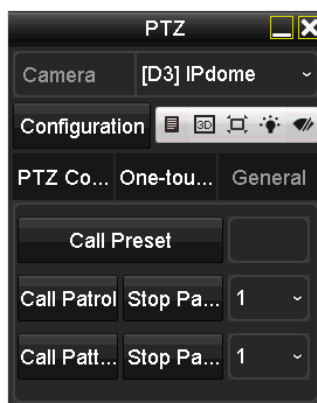


Figure 4.10 PTZ Panel - General

3. Click the **Call Pattern** button to call it.
4. Click the **Stop Pattern** button to stop calling it.

4.3.7 Customizing Linear Scan Limit

Purpose:

The Linear Scan can be enabled to trigger the scan in the horizontal direction in the predefined range.



This function is supported by some certain IP cameras.

Steps:

1. Enter the PTZ Control interface.
Menu > Camera > PTZ



Figure 4.11 PTZ Settings

2. Use the directional buttons to wheel the camera to the location where you want to set the limit, and click the

Left Limit or **Right Limit** button to link the location to the corresponding limit.



The speed dome starts linear scan from the left limit to the right limit, and you must set the left limit on the left side of the right limit, as well the angle from the left limit to the right limit should be no more than 180°.

4.3.8 Calling Linear Scan

Purpose:

Follow the procedure to call the linear scan in the predefined scan range.

Steps:

1. Enter PTZ Control interface. For details, please refer to *4.2 PTZ Control Panel*.
2. Click the button to show the one-touch function of the PTZ control.



Figure 4. 12 PTZ Panel - One-touch

3. Click **Linear Scan** button to start the linear scan and click the Linear Scan button again to stop it.
You can click the **Restore** button to clear the defined left limit and right limit data and the dome needs to reboot to make settings take effect.

4.3.9 One-touch Park

Purpose:

For some certain model of the speed dome, it can be configured to start a predefined park action (scan, preset, patrol and etc.) automatically after a period of inactivity (park time).

Steps:

1. Enter PTZ Control interface. For details, please refer to *4.2 PTZ Control Panel*.
2. Click the button to show the one-touch interface.



Figure 4. 13 PTZ Panel - One-touch

3. There are 3 one-touch park types selectable, click the corresponding button to activate the park action.

Park (Quick Patrol): The dome starts patrol from the predefined preset 1 to preset 32 in order after the park time. The undefined preset will be skipped.

Park (Patrol 1): The dome starts moving according to the predefined patrol 1 after the park time.

Park (Preset 1): The dome moves to the predefined preset 1 location after the park time.



The park time can only be set through the speed dome configuration interface, by default the value is 5s.

4. Click the button again to inactivate it.

Chapter 5 Recording Settings

5.1 Configuring Parameters

Purpose:

By configuring the parameters you can define the parameters which affect the image quality, such as the transmission stream type, the resolution and so on.

Before you start:

1. Make sure that the HDD has already been installed. If not, please install a HDD and initialize it. (Menu > HDD > General)

HDD Information									
L...	Capacity	Status	Property	Type	Free Space	Gr...	Edit	Del...	
1	465.77GB	Normal	R/W	Local	457.00GB	1	-	-	

Figure 5. 1 HDD- General

2. Check the storage mode of the HDD.
 - 1) Click **Advanced** to check the storage mode of the HDD.
 - 2) Please set the maximum record capacity For detailed information, see *12.1 Configuring Quota Mode*.

Steps:

1. Enter the Record settings interface to configure the recording parameters.

Menu > Record > Parameters

Record Substream		
Camera	[D1] Camera 01	
Encoding Parameters	Main Stream(Continuous)	Main Stream(Event)
Stream Type	Video	Video
Resolution	1280*720(HD720P)	1280*720(HD720P)
Bitrate Type	Constant	Constant
Video Quality	Medium	Medium
Frame Rate	Full Frame	Full Frame
Max. Bitrate Mode	General	General
Max. Bitrate(Kbps)	2048	2048
Max. Bitrate Range Reco...	2304~3840(Kbps)	2304~3840(Kbps)
More Setting...		

Figure 5. 2 Recording Parameters

2. Parameters Setting for Recording

- 1) Select **Record** tab page to configure. You can configure the stream type, the resolution, and other parameters on your demand.
- 2) Click the **More Settings** button to set the advanced parameters for recording and then click **OK** button to finish editing.



Figure 5. 3 Recording Parameters-More Settings

- **Pre-record:** The time you set to record before the scheduled time or event. For example, when an alarm triggered the recording at 10:00, if you set the pre-record time as 5 seconds, the camera records it at 9:59:55.
- **Post-record:** The time you set to record after the event or the scheduled time. For example, when an alarm triggered the recording ends at 11:00, if you set the post-record time as 5 seconds, it records till 11:00:05.
- **Expired Time:** The expired time is the longest time for a record file to be kept in the HDD, if the deadline is reached, the file will be deleted. You can set the expired time to 0, and then the file will not be deleted. The actual keeping time for the file should be determined by the capacity of the HDD.
- **Record Audio:** Check the checkbox to enable or disable audio recording.
- **Video Stream:** Main stream and sub-stream are selectable for recording. When you select sub-stream, you can record for a longer time with the same storage space.

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



The Stream Type, Resolution, Bitrate Type and Video Quality of Main Stream (Event) are read-only.

3. Set parameters for sub-stream.

1) Enter the Sub-stream tab.

Record	Substream
Camera	[D1] Camera 01
Stream Type	Video
Resolution (max.: 720P)	352*288(CIF)
Bitrate Type	Constant
Video Quality	Medium
Frame Rate	Full Frame
Max. Bitrate Mode	General
Max. Bitrate (Kbps) (max....	512
Max. Bitrate Range Reco...	384~640(Kbps)

Figure 5. 4 Sub-stream Parameters

- 2) Configure the parameters of the camera.
- 3) Click **Apply** to save the settings.

5.2 Configuring Recording Schedule

Purpose:

Set the recording schedule, and then the camera automatically starts/stops recording according to the configured schedule.

Steps:

1. Enter the Record Schedule interface.

Menu > Record > Schedule

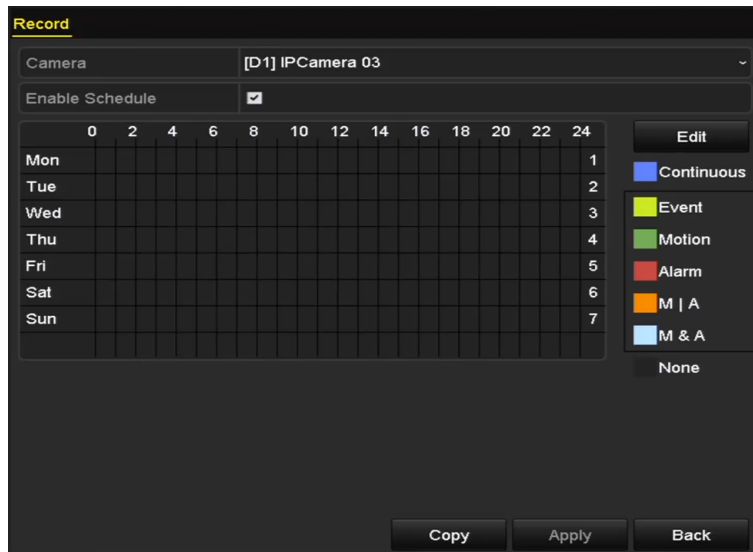


Figure 5. 5 Record Schedule



Different recording types are marked in different color icons.

Continuous: scheduled recording.

Event: recording triggered by all event triggered alarm.

Motion: recording triggered by motion detection.

Alarm: recording triggered by alarm.

M/A: recording triggered by either motion detection or alarm.

M&A: recording triggered by motion detection and alarm.

2. Configure Record Schedule

- 1) Choose the camera to configure.
- 2) Check the checkbox of **Enable Schedule**.
- 3) Edit or draw schedule.

Edit the schedule:

- I. In the message box, select the day to set schedule in the drop-down list of Schedule.

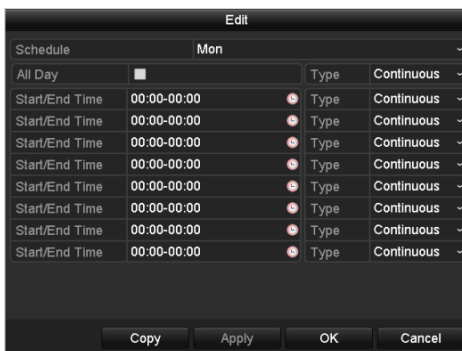



Figure 5. 6 Recording Schedule Interface

You can click the  button to set the accurate time of the schedule.

- II. To schedule an all-day recording, check the checkbox after the **All Day** item.

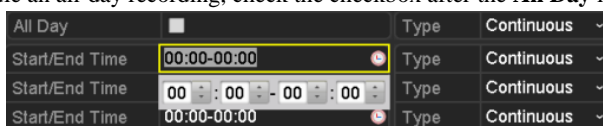


Figure 5. 7 Edit Schedule

- III. To arrange other schedule, leave the **All Day** checkbox blank and set the Start/End time.



Up to 8 periods can be configured for each day. And the time periods cannot be overlapped each other.

- IV. Select the record type in the drop-down list.



To enable Event, Motion, Alarm, M | A (motion or alarm) and M & A (motion and alarm) triggered recording, you must configure the motion detection settings, alarm input settings or VCA settings as well. For detailed information, refer to *8.1 Setting Motion Detection Alarm*, *8.2 Setting Sensor Alarms* and *8.3 Detecting Video Loss Alarm*.

The VCA settings are only available to the smart IP cameras.

Repeat the above steps to schedule recording for other days in the week. Or click **Copy** to copy the schedule settings to other days

- V. Click **Apply** in the Record Schedule interface to save the settings.

Draw the schedule:

- I. Click on a color icon, you can choose the schedule type as continuous or event.

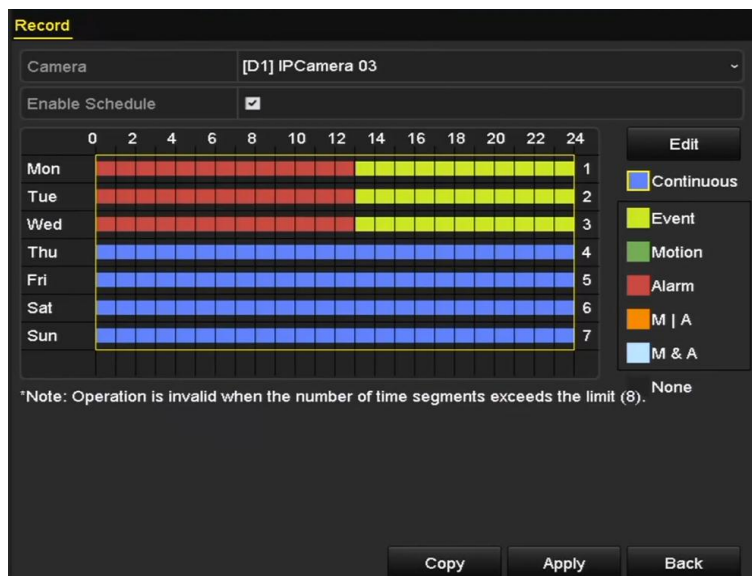


Figure 5. 8 Draw the Schedule

- II. Click the **Apply** button to validate the settings.
3. (Optional) If the settings can also be used to other channels, click **Copy**, and then choose the channel to which you want to copy.
4. Click **Apply** to save the settings.

5.3 Configuring Motion Detection Recording

Purpose:

In the live view mode, once a motion detection event takes place, the NVR can analyze it and do many actions to handle it. Enabling motion detection function can trigger certain channels to start recording, or trigger full screen monitoring, audible warning, notify the surveillance center and so on. In this chapter, you can follow the steps to schedule a record which triggered by the detected motion.

Steps:

1. Enter the Motion Detection interface.

Menu > Camera > Motion

2. Configure Motion Detection.

- 1) Choose camera to configure.
- 2) Check the checkbox of **Enable Motion Detection**.
- 3) Use the mouse to drag and draw the motion detection area in the right live view window.

If you want to set the motion detection for all the area shot by the camera, click **Full Screen**.

To clear the motion detection area, click **Clear**.

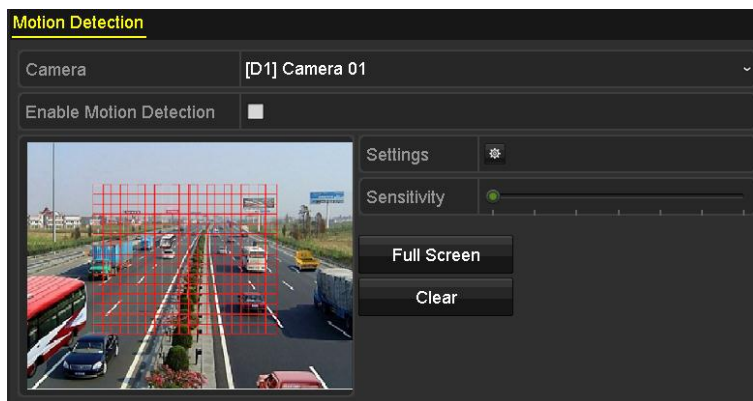


Figure 5. 9 Motion Detection- Mask

- 4) Click **Settings**, and the message box for channel information pop up.

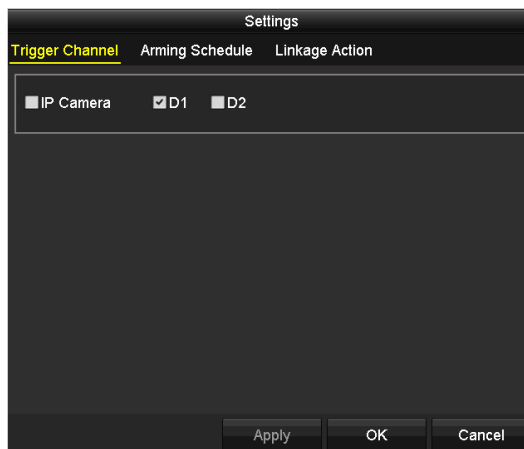


Figure 5. 10 Motion Detection Settings

- 5) Select the channels which you want the motion detection event to trigger recording.

- 6) Click **Apply** to save the settings.
 - 7) Click **OK** to back to the upper level menu.
 - 8) Exit the Motion Detection menu.
- 3.** Edit the Motion Detection Record Schedule. For the detailed information of schedule configuration, see section 5.2 *Configuring Recording Schedule*.

5.4 Configuring Alarm Triggered Recording

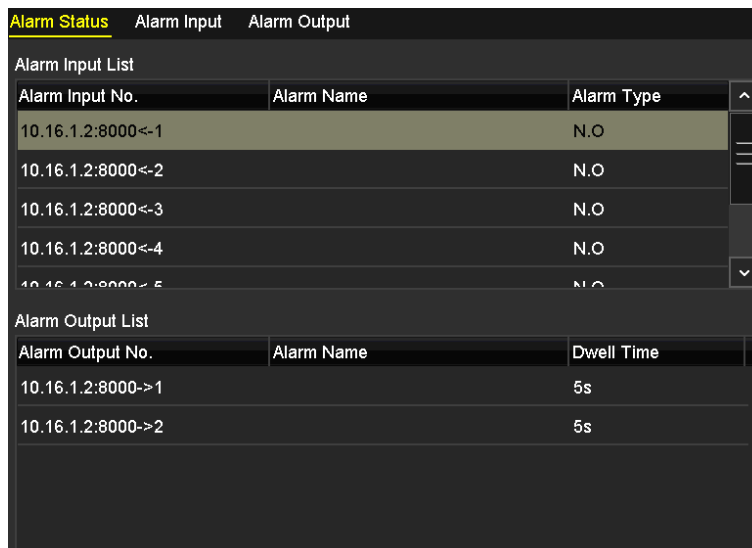
Purpose:

Follow the procedure to configure alarm triggered recording.

Steps:

1. Enter the Alarm setting interface.

Menu > Configuration > Alarm



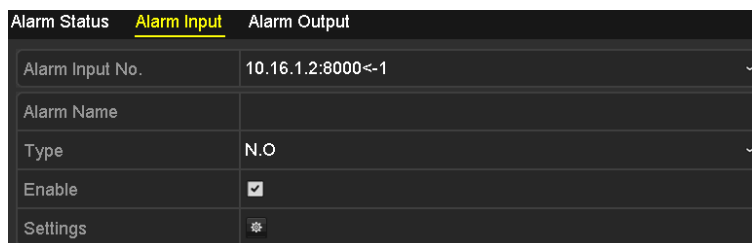
The screenshot shows the 'Alarm Status' tab selected. It contains two sections: 'Alarm Input List' and 'Alarm Output List'.

Alarm Input No.	Alarm Name	Alarm Type
10.16.1.2:8000<-1		N.O
10.16.1.2:8000<-2		N.O
10.16.1.2:8000<-3		N.O
10.16.1.2:8000<-4		N.O
10.16.1.2:8000<-5		N.O

Alarm Output No.	Alarm Name	Dwell Time
10.16.1.2:8000->1		5s
10.16.1.2:8000->2		5s

Figure 5. 11 Alarm Settings

2. Click **Alarm Input** tab and set the alarm parameters.



The screenshot shows the 'Alarm Input' tab selected. It contains the following fields:



Alarm Input No.	10.16.1.2:8000<-1
Alarm Name	
Type	N.O
Enable	<input checked="" type="checkbox"/>
Settings	

Figure 5. 12 Alarm Settings- Alarm Input

- 1) Select **Alarm Input No.**
- 2) Choose N.O (Normally Open) or N.C (Normally Closed) for alarm type.
- 3) Check the checkbox for Enable.
- 4) Click the  icon after Settings.

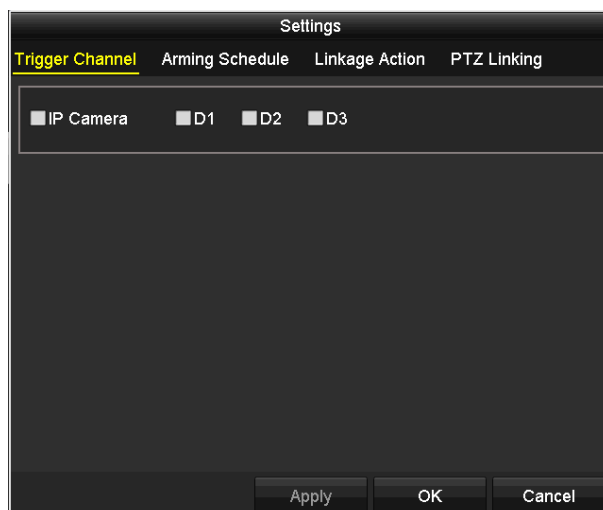


Figure 5. 13 Alarm Settings

- 5) Check the checkbox of IP camera. So the selected camera will be triggered to record when alarm occurs.
- 6) Click **Apply** to save settings.
- 7) Click **OK** to back to the upper level menu.

Repeat the step 2 to configure parameters for other alarm inputs.

If the settings are suitable for other alarm inputs, click **Copy** and choose the alarm input number.

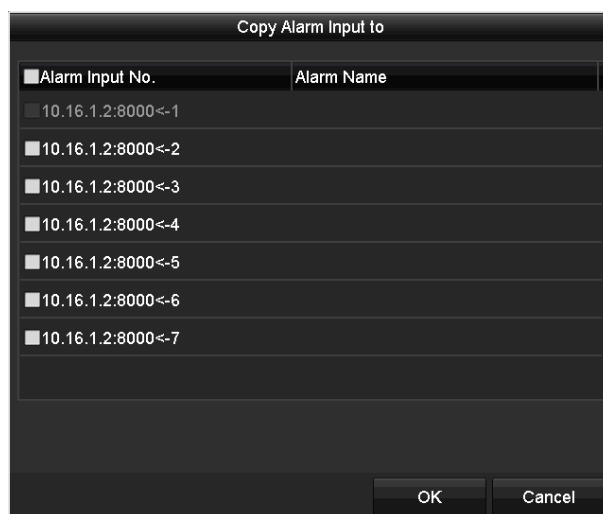


Figure 5. 14 Copy Alarm Input

3. Edit the Alarm triggered record in the Record Schedule setting interface. For the detailed information of schedule configuration, see 5.2 *Configuring Recording Schedule*.

5.5 Configuring VCA Event Recording

Purpose:

The event triggered recording can be configured through the menu. Then events include the motion detection, alarm and VCA events (face detection/face capture, line crossing detection, intrusion detection, region entrance detection, region exiting detection, loitering detection, people gathering detection, fast moving detection, parking detection, unattended baggage detection, object removal detection, audio loss exception detection, sudden change of sound intensity detection, and defocus detection).

Steps:

1. Enter the VCA settings interface and select a camera for the VCA settings.

Menu > Camera > VCA

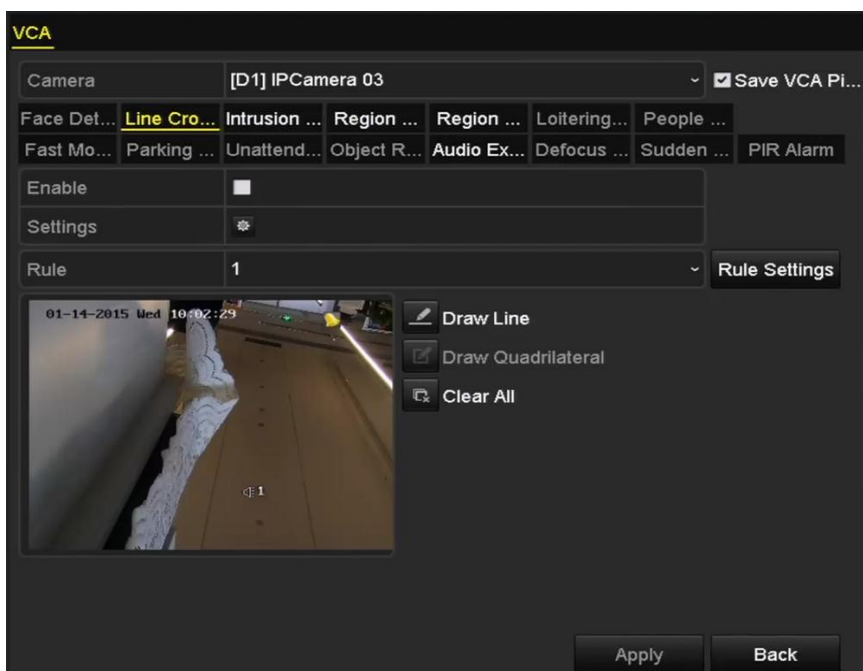


Figure 5. 15 VCA Settings


2. Configure the detection rules for VCA events. For details, see the step 2 in *Chapter 9 VCA Alarm*.
3. Click the icon  to configure the alarm linkage actions for the VCA events.
Select **Trigger Channel** tab and select one or more channels which will start to record when VCA alarm is triggered.
Click **Apply** to save the settings



Figure 5. 16 Set Trigger Camera of VCA Alarm



The PTZ Linking function is only available for the VCA settings of IP cameras.

4. Enter Record Schedule settings interface (Menu > Record > Schedule > Record Schedule), and then set VCA as the record type. For details, see step 2 in 5.2 *Configuring Recording Schedule*.

5.6 Manual Recording

Purpose:

Follow the steps to set parameters for the manual record. Using manual record, you need to manually cancel the record. The manual recording is prior to the scheduled recording.

Steps:

1. Enter the Manual settings interface.

Menu > Manual

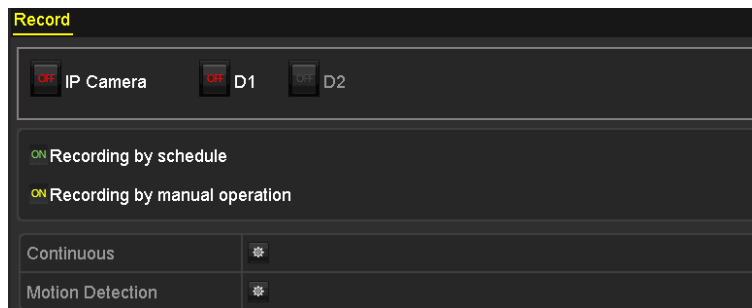


Figure 5. 17 Manual Record

2. Enable the Manual Record.

- 1) Select **Record** on the left bar.
- 2) Click the status button before camera number to switch **OFF** to **ON**.

3. Disable manual record.

Click the status button to switch **ON** to **OFF**.



Green icon **ON** means that the channel is configured the record schedule.

After rebooting, all the manual records enabled will be canceled.

5.7 Configuring Holiday Recording

Purpose:

Follow the steps to configure the record schedule on holiday for the year. You may want to have different plan for recording on holiday.

Steps:

1. Enter the Record setting interface.

Menu > Record > Holiday

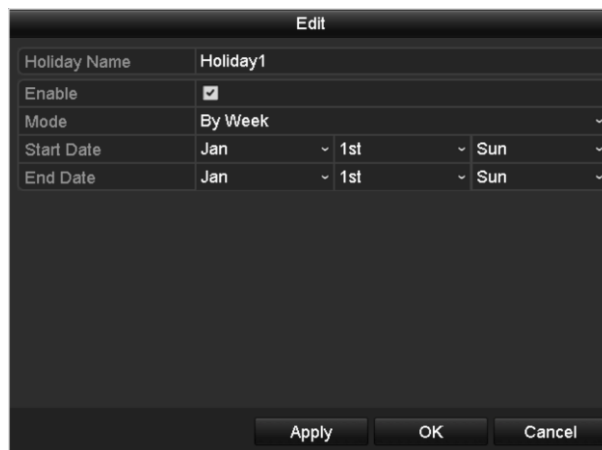


No.	Holiday Name	Status	Start Date	End Date	Edit
1	Holiday1	Disabled	1.Jan	1.Jan	
2	Holiday2	Disabled	1.Jan	1.Jan	
3	Holiday3	Disabled	1.Jan	1.Jan	
4	Holiday4	Disabled	1.Jan	1.Jan	
5	Holiday5	Disabled	1.Jan	1.Jan	
6	Holiday6	Disabled	1.Jan	1.Jan	
7	Holiday7	Disabled	1.Jan	1.Jan	
8	Holiday8	Disabled	1.Jan	1.Jan	
9	Holiday9	Disabled	1.Jan	1.Jan	
10	Holiday10	Disabled	1.Jan	1.Jan	
11	Holiday11	Disabled	1.Jan	1.Jan	

Figure 5. 18 Holiday Settings

2. Enable Edit Holiday schedule.

- 1) Click to enter the Edit interface.



Edit

Holiday Name	Holiday1		
Enable	<input checked="" type="checkbox"/>		
Mode	By Week		
Start Date	Jan	1st	Sun
End Date	Jan	1st	Sun

Apply
OK
Cancel

Figure 5. 19 Edit Holiday Settings

- 2) Check the checkbox after **Enable Holiday**.
- 3) Select **Mode** from the drop-down list.
There are three different modes: **By Date**, **By Week** and **By Month**.
- 4) Set the **Start Date** and **End Date**.
- 5) Click **Apply** to save settings.
- 6) Click **OK** to exit the Edit interface.
3. Enter Record Schedule settings interface to edit the holiday recording schedule. See *section 5.2 Configuring Recording Schedule*.

5.8 Files Protection

Purpose:

You can lock the recorded files to protect the record files from being overwritten.

Steps:

1. Enter Export setting interface.



Menu > Export

Figure 5. 20 Export

2. Select the cameras to protect by checking the checkbox.
3. Configure the **Record Type**, **File Type**, **Start Time** and **End Time**.
4. Click **Search** to show the results and click **List** tab.



Figure 5. 21 Export- Search Result

5. Protect the record files.

- 1) Click the  icon of a file to switch it to , indicating that the file is locked.



The record files of which the recording is still not completed cannot be locked.

- 2) Click  to change it to  to unlock the file and the file is not protected.

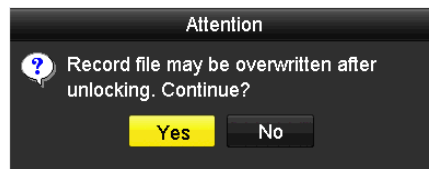


Figure 5. 22 Unlocking Attention

Chapter 6 Playback

6.1 Playing Back Record Files

6.1.1 Playing Back by Channel

Purpose:

Play back the recorded video files of a specific channel in the live view mode. Channel switch is supported.

Instant playback by channel

Steps:

In the live view mode, click to select a channel to pop up quick setting toolbar and click the  button.



Only record files recorded during the last five minutes on this channel will be played back.



Figure 6. 1 Instant Playback Interface

Playback by channel

1. Enter the Playback interface.

In live view mode, right-click a channel and click **Playback** the menu, as shown in Figure 6. 2.

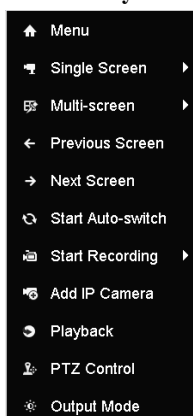


Figure 6. 2 Right-click Menu

2. Playback management.

Check the checkbox of the cameras to execute simultaneous playback for multiple channels.



Figure 6. 3 Playback Interface

The toolbar in the bottom of Playback interface can be used to control playing progress.



Figure 6. 4 Toolbar of Playback



Use the mouse to click any point of the progress bar or drag the progress bar to locate in special frames.

The 04-21-2015 14:13:58 -- 04-21-2015 14:22:04 indicates the start and end time of the record.

Table 6. 1 Detailed Explanation of Playback Toolbar

Button	Operation	Button	Operation	Button	Operation
	Audio on/ Mute		Start/Stop clipping		Lock File
	Add default tag		Add customized tag		File management for video clips, captured pictures, locked files and tags
	Reverse play/ Pause		Stop		Digital Zoom
	30s forward		30s reverse		Pause / Play
	Fast forward		Previous day		Slow forward
	Full Screen		Exit		Next day
	Save the clips		Process bar		Scaling up/down the time line

6.1.2 Playing Back by Time

Purpose:

Play back video files recorded in specified time duration. Multi-channel simultaneous playback and channel switch are supported.

Steps:

1. Enter playback interface.

Menu > Playback



2. Check the checkbox of channel(s) in the channel list and then double-click to select a date on the calendar.

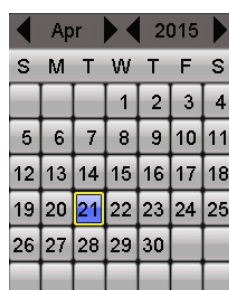


Figure 6. 5 Playback Calendar



In calendar, the dates who have record files for selected camera will show as 21, otherwise it will show as 21.

6.1.3 Playing Back by Event Search

Purpose:

Play back record files of one or several channels searched out by restricting event type (e.g. alarm input and motion detection).

Steps:

1. Enter the Playback interface.
Menu > Playback
2. Select the **Event** in the drop-down list on the top-left side.

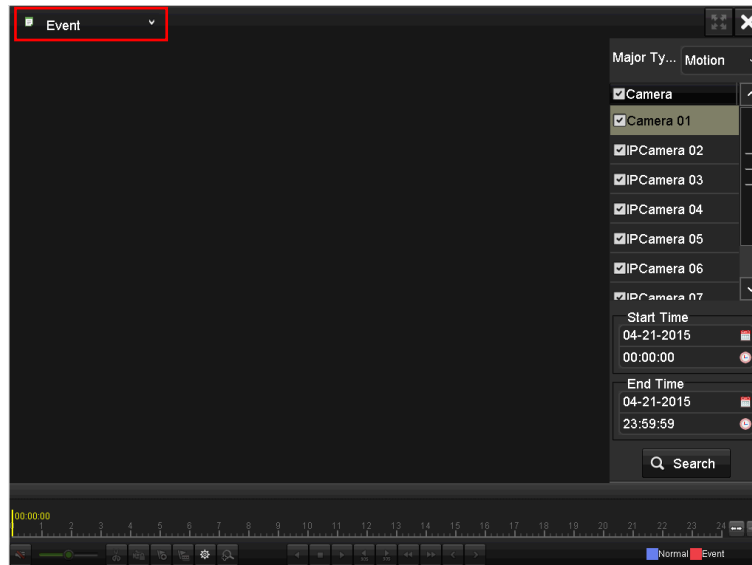


Figure 6. 6 Motion Search Interface

3. Select the **Major Type** as **Alarm Input**, **Motion** or **VCA**.
4. Set the **Start Time** and **End Time**.



Here we take playback by motion as the example.

5. Click **Search** button to get the search result, as shown below.

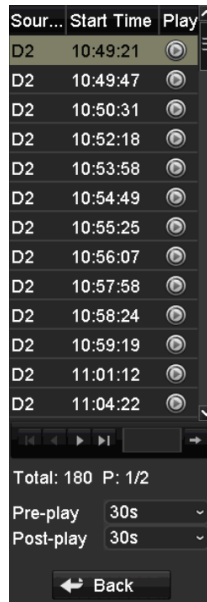



Figure 6. 7 Search Result Bar

6. Click  button to play back the file.



Pre-play and **post-play** can be configured.



Figure 6. 8 Interface of Playback by Event

7. You can click the **Back** button to back to the search interface.

6.1.4 Playing Back by Tag

Purpose:

Video tag allows you to record related information, like people and location, of a certain time point during playback. You are also allowed to use video tag(s) to search for record files and position time point.

You need to add tags before playing back them.

Before you start:

1. Enter Playback interface.
Menu > Playback
2. Search and play back the record file(s). For details, please refer to section 6.1.1 *Playing Back by Channel*.
3. Add tag.

Add default tag: click button in toolbar.

Add customized tag: click button in toolbar and input tag name.



Max. 64 tags can be added to each single video file.

4. Tag management.

Click button to check, edit or delete tag(s).

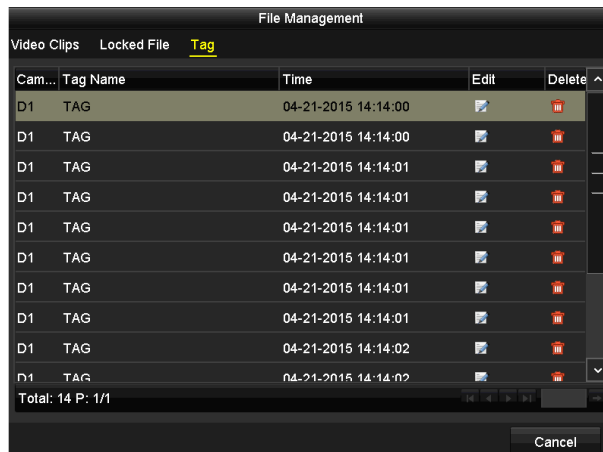


Figure 6.9 Tag Management Interface

Steps:

1. Select the **Tag** from the drop-down list in the Playback interface.

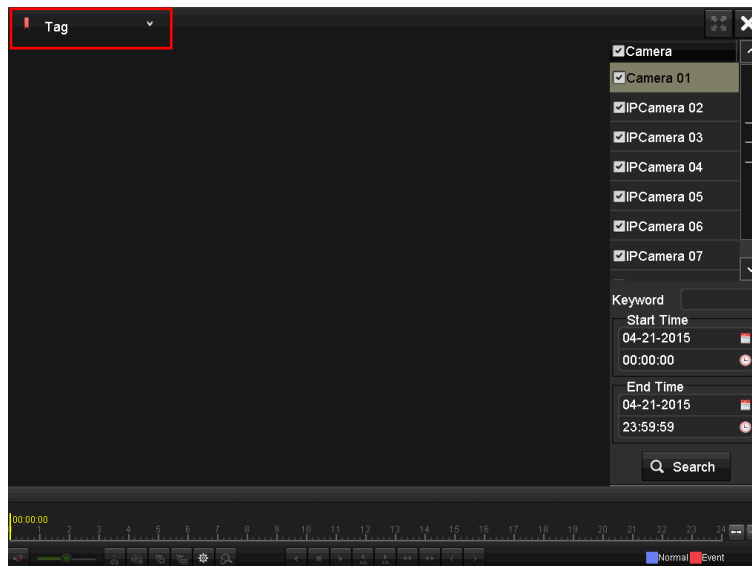



Figure 6.10 Video Search by Tag

2. Check the checkbox of cameras.
3. Edit **Start Time** and **End Time**.
4. Optionally, you can input **Keyword** to search the tag on your demand.
5. Click **Search** to enter Search Result interface.
6. Click  button to play back the file.



Pre-play and post-play can be configured.



Figure 6.11 Interface of Playback by Tag

7. Click the **Back** button to back to the search interface.

6.1.5 Smart Playback

Purpose:

The smart playback function provides an easy way to get through the less effective information. When you select the smart playback mode, the system will analyze the video containing the motion or VCA information, mark it with green color and play it in the normal speed while the video without motion will be played in the 16-time speed. The smart playback rules and areas are configurable.

Before you start:

To get the smart search result, the corresponding event type must be enabled and configured on the IP camera.

Here we take the intrusion detection as an example.

1. Log in the IP camera by the web browser, and enable the intrusion detection by checking the checkbox of it. You may enter the motion detection configuration interface by Configuration > Advanced Configuration > Events > Intrusion Detection.



Figure 6.12 Setting Intrusion Detection on IP Camera

2. Configure the required parameters of intrusion detection, including area, arming schedule and linkage methods. Refer to the user manual of smart IP camera for detailed instructions.

Steps:













1. Enter Playback interface.
Menu > Playback
2. Select the **Smart** in the drop-down list on the top-left side.
3. Select a camera in the camera list.

4. Select a date in the calendar and click the  button on the left toolbar to play the video file.




Figure 6.13 Smart Playback Interface

Table 6.2 Detailed Explanation of Smart Playback


Button	Operation	Button	Operation	Button	Operation
	Draw line for the line crossing detection		Draw quadrilateral for the intrusion detection		Draw rectangle for the motion detection
	Set full screen for motion detection		Clear all		Start/Stop clipping
	File management for video clips		Stop playing		Pause playing / Play
	Smart settings		Search matched video files		Filter video files by setting the target characters

5. Set the rules and areas for smart search of VCA event or motion event.


Line Crossing Detection


Select the  button, and click on the image to specify the start point and end point of the line.


Intrusion Detection

Click the  button, and specify 4 points to set a quadrilateral region for intrusion detection. Only one region can be set.

Motion Detection

Click the  button and then click and draw the mouse to set the detection area manually. You can also

click the  button to set the full screen as the detection area.

6. You can click  to configure the smart settings.

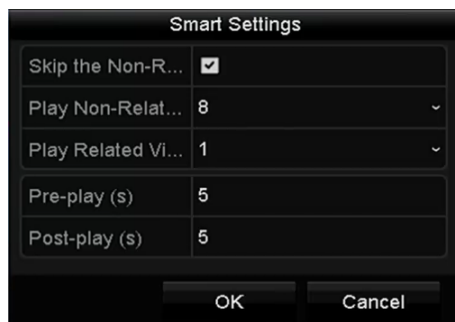


Figure 6. 14 Smart Settings

Skip the Non-Related Video: The non-related video will not be played if this function is enabled.

Play Non-Related Video at: Set the speed to play the non-related video. Max./8/4/1 are selectable.

Play Related Video at: Set the speed to play the related video. Max./8/4/1 are selectable.



Pre-play and post-play is not available for the motion event type.

- Click to search and play the matched video files.
- (Optional) You can click to filter the searched video files by setting the target characters, including the gender and age of the human and whether he/she wears glasses.



Figure 6. 15 Set Result Filter

6.1.6 Playing Back by System Logs

Purpose:

Play back record file(s) associated with channels after searching system logs.

Steps:

- Enter Log Information interface.
Menu > Maintenance > Log Information
- Click **Log Search** tab to enter Playback by System Logs.
- Set the precondition, including **Start Time**, **End Type**, **Major type** and **Minor Type**.
- Click **Search** button.

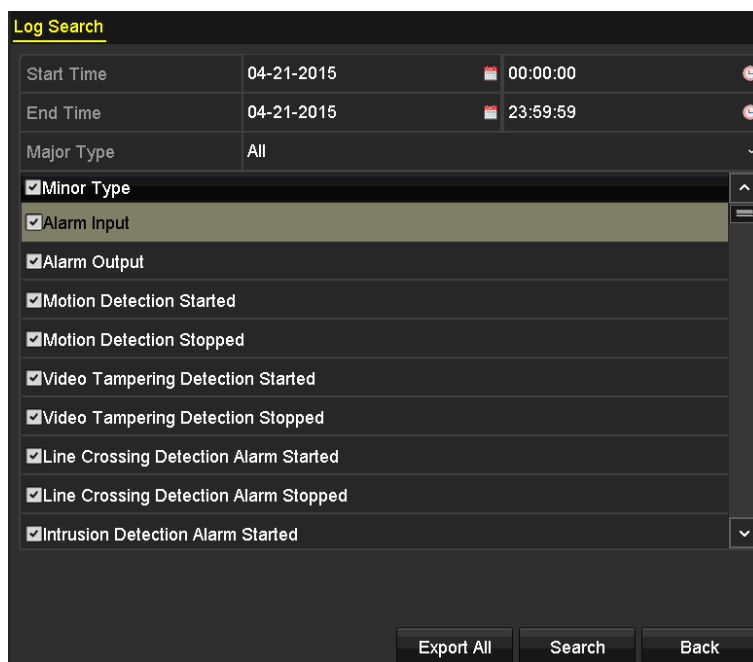


Figure 6. 16 System Log Search Interface

5. Choose a log with record file and click  button to enter Playback interface.



If there is no record file at the time point of the log, the message box “No result found” will pop up.

No.	Major Type	Time	Minor Type	Parameter	Play	Details
187	Alarm	12-26-2013 11:25:54	Video Tamperin...	N/A		✓
188	Alarm	12-26-2013 11:26:01	Video Tamperin...	N/A		✓
189	Alarm	12-26-2013 11:26:12	Video Tamperin...	N/A		✓
190	Alarm	12-26-2013 11:26:17	Video Tamperin...	N/A		✓
191	Alarm	12-26-2013 11:26:23	Video Tamperin...	N/A		✓
192	Information	12-26-2013 11:26:51	System Running...	N/A	—	✓
193	Information	12-26-2013 11:27:02	System Running...	N/A	—	✓
194	Operation	12-26-2013 11:27:12	Remote Operati...	IP Camera	—	✓
195	Operation	12-26-2013 11:27:12	Remote Operati...	N/A	—	✓
196	Operation	12-26-2013 11:27:12	Remote Operati...	Device	—	✓
197	Operation	12-26-2013 11:30:12	Remote Operati...	IP Camera	—	✓
198	Operation	12-26-2013 11:30:12	Remote Operati...	N/A	—	✓
199	Operation	12-26-2013 11:30:12	Remote Operati...	Device	—	✓
200	Operation	12-26-2013 11:33:11	Remote Operati...	IP Camera	—	✓
Total: 1067 P: 2/11						

Figure 6. 17 Result of System Log Search

6.1.7 Playing Back External File

Purpose:

Perform the following steps to review and play back files in the external devices.

Steps:

1. Enter Tag Search interface.

Menu > Playback

2. Select the **External File** in the drop-down list on the top-left side.

The files are listed in the right-side list.

You can click the  Refresh button to refresh the file list.

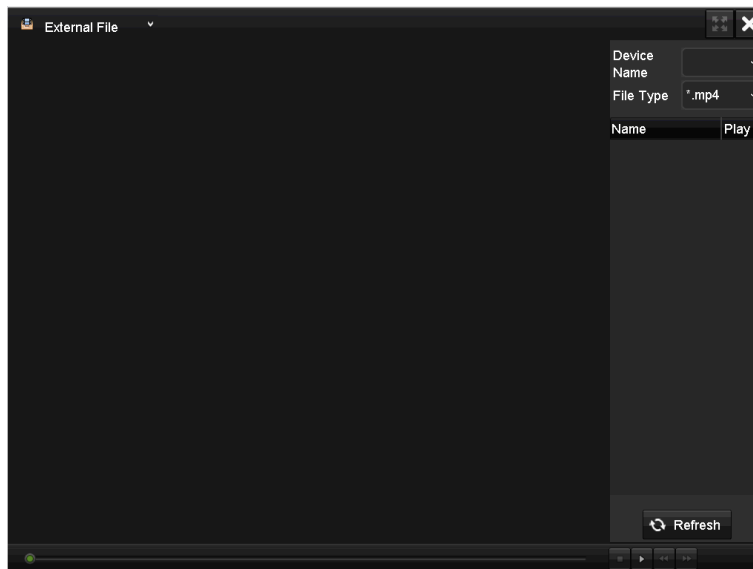





Figure 6. 18 Interface of External File Playback

3. Select the external device and **File Type** in respective dropdown lists.
4. Click the  button to play back record file.
5. You can adjust the playback speed by clicking  and .

6.2 Auxiliary Functions of Playback

6.2.8 Playing Back Frame by Frame

Purpose:


Play video files frame by frame, in case of checking image details of the video when abnormal events happen.



Steps:

1. Enter Playback interface.

Menu > Playback

2. Start signal frame playback.

Playback: click button  until the speed changes to **Single Frame** and one click on the playback screen to play back by one frame.

Reverse playback: click button  until the speed changes to Single frame and one click on the playback screen to reversely play back by one frame. It is also feasible to use button  in toolbar.

6.2.9 Digital Zoom

Steps:


1. Click the  button on the playback toolbar to enter Digital Zoom interface.
2. Use the mouse to draw a red rectangle and the image within it will be enlarged up to 16 times.



Figure 6. 19 Draw Area for Digital Zoom

3. Right-click the image to exit the digital zoom interface.

6.2.10 Reverse Playback of Multi-channel

Purpose:

You can play back record files of multi-channel reversely. Up to 8-ch (with 1280*720 resolution) simultaneous

reverse playback is supported and up to 6-ch (with 1920*1080P resolution) simultaneous reverse playback is supported.

Steps:


1. Enter Playback interface.

Menu > Playback

2. Check more than one checkbox to select multiple channels and click to select a date on the calendar.



Figure 6. 20 4-ch Synchronous Playback Interface

3. Click  to play back the record files reversely.

Chapter 7 Backup

7.1 Backing up Record Files

7.1.1 Quick Export

Purpose:

Export record files to backup device(s) quickly.

Before you start:

You can connect a USB hub to the signal USB interface in rear panel, thus to expand it.

Steps:

1. Enter Video Export interface.
Menu > Export > Normal
2. Choose the channel(s) to back up and click **Quick Export** button.



The time duration of record files on a specified channel cannot exceed one day. Otherwise, the message box “Max. 24 hours are allowed for quick export.” will pop up.

Figure 7. 1 Quick Export Interface

3. Click on the **Export** button to start exporting.



Here we use USB Flash Drive as the example and please refer to the *7.1.2 Backing up by Normal Video Search* for more backup devices supported by the NVR.

Figure 7. 2 Quick Export using USB1-1

Stay in the Exporting interface until all record files are exported.

4. Check backup result.



The Player player.exe will be exported automatically during record file export.

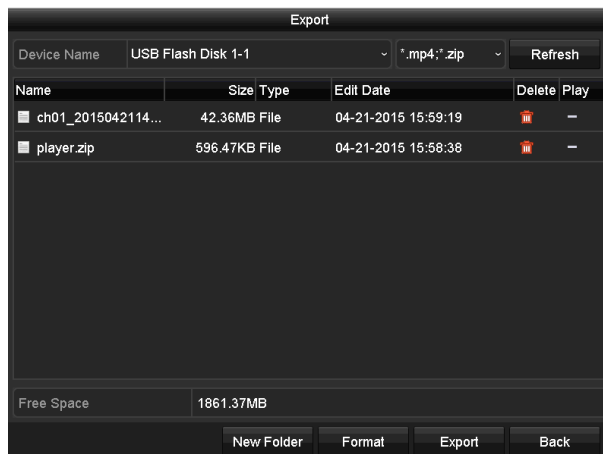


Figure 7. 3 Checkup of Quick Export Result Using USB1-1

7.1.2 Backing up by Normal Video Search

Purpose:

The record files can be backed up to various devices, such as USB flash drives, USB HDDs and USB writer.

Backup using USB flash drives and USB HDDs

Steps:

1. Enter Export interface.
Menu > Export > Normal
2. Set search condition and click **Search** button to enter the search result interface.

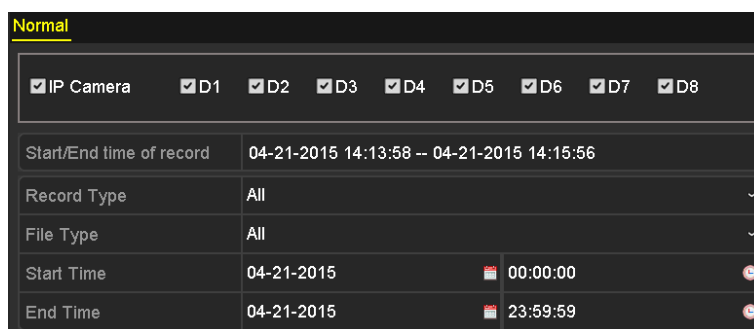


Figure 7. 4 Normal Video Search for Backup

3. Click **List** tab and select record files to back up.

Check the checkboxes before the record files to back up.



The size of the currently selected files is displayed in the lower-left corner of the window.

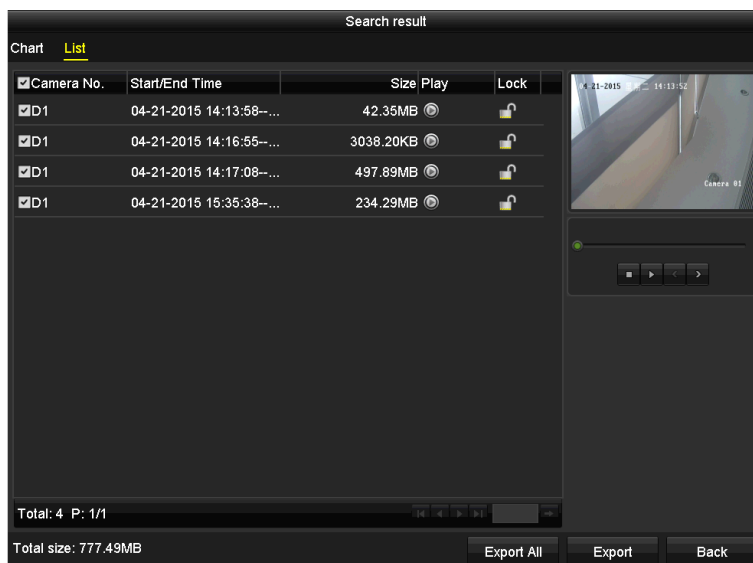


Figure 7. 5 Result of Normal Video Search for Backup

4. Export.

Click **Export All** button to export all the record files.

Or you can select record files to back up, and click **Export** button to enter Export interface.



If the inserted USB device is not recognized:

- Click the **Refresh** button.
- Reconnect device.
- Check for compatibility from vendor.

You can also format USB flash drives or USB HDDs via the device.



Figure 7. 6 Export by Normal Video Search using USB Flash Drive

Stay in the Exporting interface until all record files are exported with pop-up message box "Export finished".

5. Check backup result.



The Player player.exe will be exported automatically during record file export.

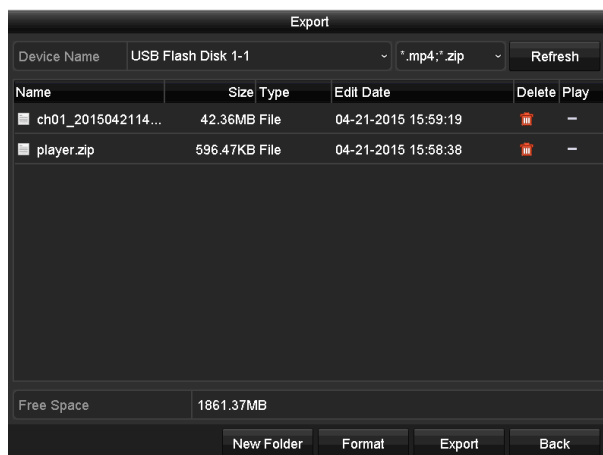


Figure 7. 7 Checkup of Export Result using USB Flash Drive

Backup using USB writer

Steps:

1. Enter Export interface.
Menu > Export > Normal
2. Set search condition and click **Search** button to enter the search result interface.

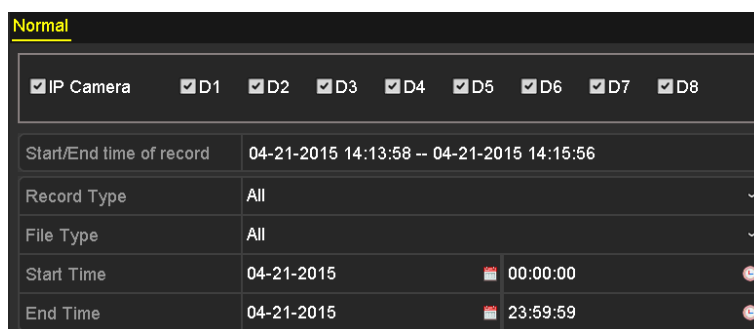


Figure 7. 8 Normal Video Search for Backup

3. Click **list** tab and select record files to back up.

Click button to play the record file to check it.

Check the checkbox before the record files to back up.



The size of the currently selected files is displayed in the lower-left corner of the window.

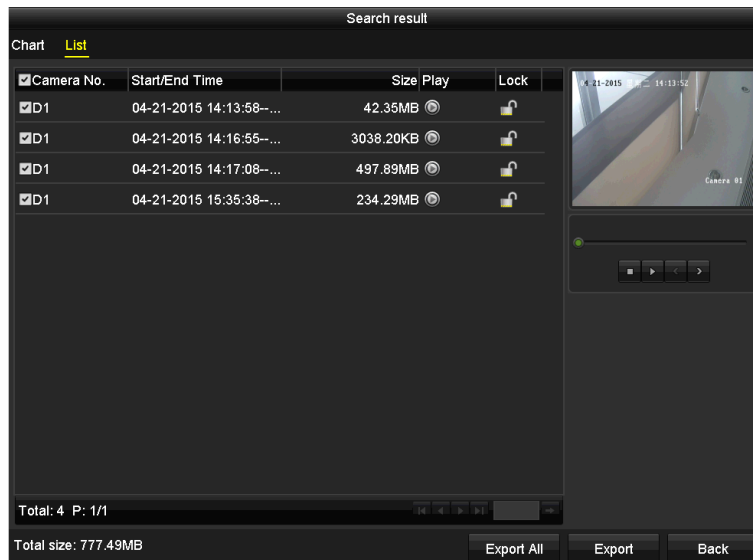


Figure 7. 9 Result of Normal Video Search for Backup

4. Export.

Click **Export** button and start backup.



If the inserted USB writer is not recognized:

- Click the **Refresh** button.
- Reconnect device.
- Check for compatibility from vendor.

Stay in the Exporting interface until all record files are exported with pop-up message box "Export finished".

5. Check backup result.



The Player player.exe will be exported automatically during record file export.

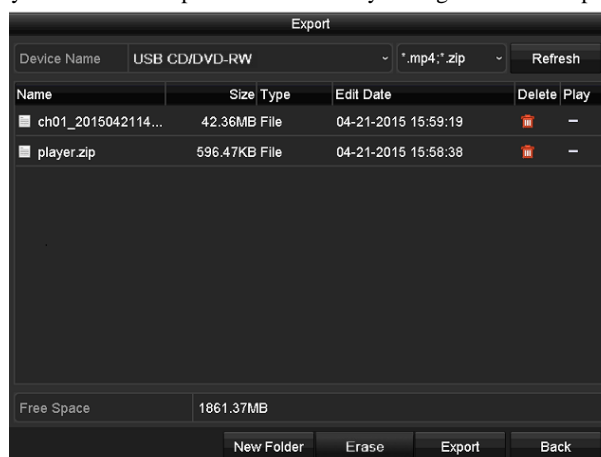


Figure 7. 10 Checkup of Export Result using USB Writer

7.1.3 Backing up by Event Search

Purpose:

Back up events related record files using USB devices (USB flash drives, USB HDDs, USB writer). Quick Backup and Normal Backup are supported.

We take the backing up alarm input events as an example.

Steps:

1. Enter Export interface.
Menu > Export > Event
2. Set the search precondition.
 - 1) Select **Major Type** as **Motion**, **Alarm Input** or **VCA** from the drop-down list.
We take **Motion** as the example to describe the following steps.
 - 2) Select the **Alarm Input No.**, **Start Time** and **End Time**.
 - 3) Click **Search** button to enter the Search Result interface.

Major Type	Motion		
Start Time	04-22-2015	00:00:00	
End Time	04-22-2015	23:59:59	
Pre-play	30s		
Post-play	30s		
<input checked="" type="checkbox"/> IP Camera <input checked="" type="checkbox"/> D1 <input checked="" type="checkbox"/> D2 <input checked="" type="checkbox"/> D3 <input checked="" type="checkbox"/> D4 <input checked="" type="checkbox"/> D5 <input checked="" type="checkbox"/> D6 <input checked="" type="checkbox"/> D7 <input checked="" type="checkbox"/> D8			

Figure 7. 11 Event Search for Backup

3. Click **List** tab.

Source	Camera No.	HDD	Event Time	Size	Play
D1	D1	1	04-22-2015 10:49:55-...	6005.83KB	
D1	D2	1	04-22-2015 10:49:55-...	770.43KB	
D1	D1	1	04-22-2015 10:54:18-...	4956.52KB	
D1	D2	1	04-22-2015 10:54:18-...	2173.51KB	
D1	D1	1	04-22-2015 11:10:42-...	4938.85KB	
D1	D1	1	04-22-2015 11:10:42-...	5018.83KB	
D1	D2	1	04-22-2015 11:10:42-...	2696.05KB	
D1	D2	1	04-22-2015 11:10:42-...	609.68KB	
D1	D1	1	04-22-2015 11:11:06-...	4938.85KB	
D1	D1	1	04-22-2015 11:11:06-...	5018.83KB	
D1	D2	1	04-22-2015 11:11:06-...	2696.05KB	
D1	D2	1	04-22-2015 11:11:06-...	609.68KB	
D3	D3	1	04-22-2015 10:44:35-...	2891.91KB	

Total: 81 P: 1/1

Total size: 0B

Export All Export Back

Figure 7. 12 Result of Event Search

4. Export record file.
Click **Export All** button to export all the record files.
Or you can select record files to back up, and click **Export** button to enter Export interface.

5. Click **Export** in the Export interface.



If the inserted USB device is not recognized:

- Click the Refresh button.
- Reconnect device.
- Check for compatibility from vendor.

You can also format USB flash drive or USB HDDs via the device.



Figure 7. 13 Export by Event Using USB Flash Drive

Stay in the Exporting interface until all record files are exported with pop-up message “Export finished”.

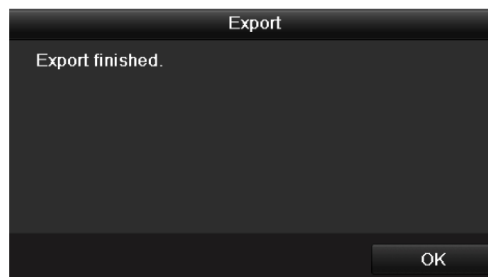


Figure 7. 14 Export Finished

6. Check backup result.



The Player player.exe will be exported automatically during record file export.

7.1.4 Backing up Video Clips




Purpose:

You may also select video clips to export directly during Playback, using USB devices (USB flash drives, USB HDDs, USB writer).

Steps:

1. Enter Playback interface.

Please refer to *Chapter 6.1 Playing Back Record Files*.

2. Click the  button in playback toolbar to start clipping current playback file.
3. Click  stop clipping.
4. Click  to enter Export interface.

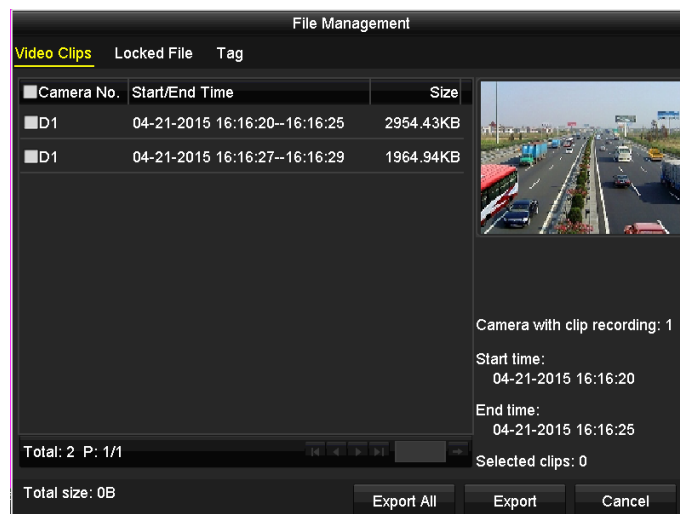


Figure 7.15 Clips Export Interface

5. Select files you want to export.
 6. Click **Export** to enter backup interface.
 7. Select external device and file type in respective dropdown lists and click **Export** to back up files.
- Stay in the Exporting interface until all record files are exported with pop-up message “Export finished”.



If the inserted USB device is not recognized:

- Click the **Refresh** button.
- Reconnect device.
- Check for compatibility from vendor.

You can also format USB flash drive or USB HDDs via the device.



Figure 7.16 Export Video Clips Using USB Flash Drive

7.2 Managing Backup Devices

Management of USB flash drives and USB HDDs

Steps:

1. Enter Search Result interface of record files.
Menu > Export > Normal
2. Set search conditions, including **IP Camera**, **Record Type**, **File Type**, **Start Time** and **End Time**.
3. Click **Search** button to enter Search Result interface.

Figure 7. 17 Normal Video Search for Backup

4. Click to select the **List** tab.
 5. Click **Export All** button to export all the record files.
- Or you can select record files to back up, and click **Export** button to enter Export interface.

Figure 7. 18 Result of Normal Video Search for Backup

6. Backup device management.
 - Select external device and file type in respective dropdown lists.
 - Click **New Folder** button if you want to create a new folder in the backup device.
 - Select a record file or folder in the backup device and click button if you want to delete it.
 - Click **Format** button to format the backup device.



If the inserted USB device is not recognized:

- Click the **Refresh** button.
- Reconnect device.
- Check for compatibility from vendor.



Figure 7. 19 USB Flash Drive Management

Management of USB writers

1. Enter Search Result interface of record files.

Menu > Export > Normal

2. Set search condition.
3. Click **Search** button to enter Search Result interface.

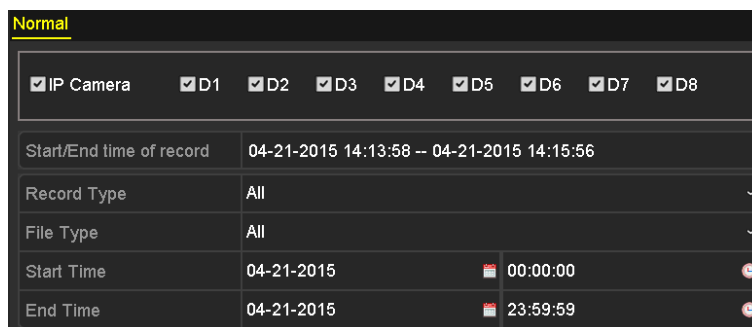


Figure 7. 20 Normal Video Search for Backup

4. Click to select the **List** tab.
5. Select record files you want to back up.
Click **Export All** button to export all the record files.
Or you can select record files to back up, and click **Export** button to enter Export interface.

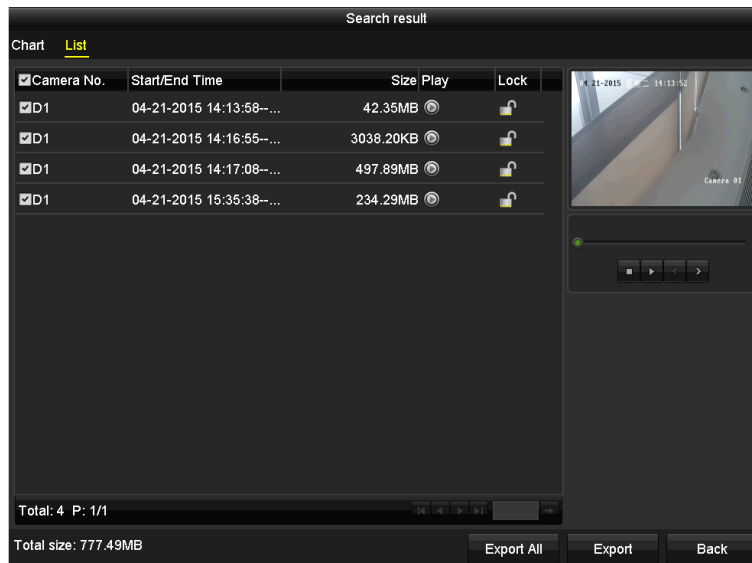


Figure 7. 21 Result of Normal Video Search for Backup

6. Backup device management.

Click **Erase** button if you want to erase the files from a re-writable CD/DVD.



There must be a re-writable CD/DVD when you make this operation.

If the inserted USB writer is not recognized:

- Click the **Refresh** button.
- Reconnect device.
- Check for compatibility from vendor.

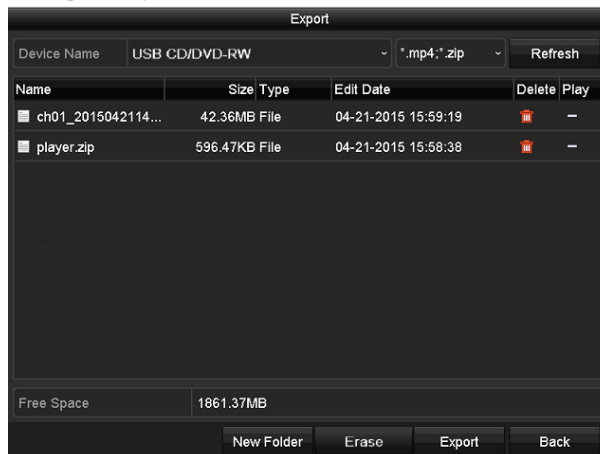


Figure 7. 22 USB Writer Management

Chapter 8 Alarm Settings

8.1 Setting Motion Detection Alarm

Steps:

1. Enter Motion Detection interface of Camera Management.
Menu > Camera > Motion
2. Select a **Camera** to set up motion detection from the drop-down list.
3. Check **Enable Motion Detection** checkbox.
4. Use the mouse to draw detection area(s) in the right live view window.
5. Drag the scroll bar to set the **Sensitivity**.



By default, the motion detection is enabled and configured in full screen.

6. Click button to set alarm response actions.

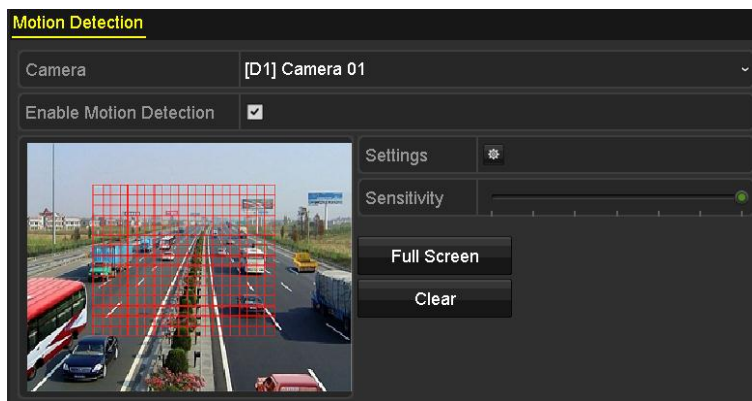


Figure 8. 1 Motion Detection Setup Interface

7. Click **Trigger Channel** tab and select one or more channels which will start to record or become full-screen monitoring when motion alarm is triggered, and click **Apply** to save the settings.



Figure 8. 2 Set Trigger Camera of Motion Detection

8. Configure Arming Schedule of the channel.
 - 1) Select **Arming Schedule** tab.

- 2) Choose one day of a **Week**. Up to eight periods can be set within each day.
- 3) Click **Apply** to save the settings



Time periods shall not be repeated or overlapped.

Week	Mon
1	00:00-24:00
2	00:00-00:00
3	00:00-00:00
4	00:00-00:00
5	00:00-00:00
6	00:00-00:00
7	00:00-00:00
8	00:00-00:00

Figure 8. 3 Set Arming Schedule of Motion Detection

9. Click **Linkage Action** tab to configure alarm response actions. For details, please refer to 8.5 *Handling Exceptions Alarm*.
10. If you want to set motion detection for another channel, repeat the above steps or click **Copy** in the Motion Detection interface to copy the above settings to it.

8.2 Setting Sensor Alarms

Purpose:

Set the handling action of an external sensor alarm.

Steps:

1. Enter Alarm Settings of System Configuration.
Menu > Configuration > Alarm
2. Select **Alarm Input** tab to enter Alarm Input Settings interface.

Alarm Status	Alarm Input	Alarm Output
Alarm Input No.	10.16.1.243:8000<-1	
Alarm Name		
Type	N.O	
Enable	<input checked="" type="checkbox"/>	
Settings		

Figure 8. 4 Alarm Input Setup Interface

3. Select **Alarm Input No.** in the drop-down list.
4. Check the **Enable** checkbox.
5. Click the button after **Settings** to set up its alarm response actions.
6. Select **Trigger Channel** tab and select one or more channels which will start to record or become full-screen monitoring when an external alarm is input, and click **Apply** to save the settings.

Settings

Trigger Channel Arming Schedule Linkage Action PTZ Linking

☒ IP Camera ☐ D1 ☐ D2 ☐ D3

Figure 8. 5 Trigger Channel Settings

7. Select **Arming Schedule** tab to set the arming schedule of handling actions.
 - 1) Choose one day of a week. Up to eight periods can be set within each day
 - 2) Click **Apply** to save the settings.



Time periods cannot be repeated or overlapped.

- 3) Repeat the above steps to set up arming schedule of other days of a week. You can also use Copy button to copy an arming schedule to other days.

Trigger Channel	Arming Schedule	Linkage Action	PTZ Linking
Week	Mon		
1	00:00-24:00	<input type="checkbox"/>	<input type="checkbox"/>
2	00:00-00:00	<input type="checkbox"/>	<input type="checkbox"/>
3	00:00-00:00	<input type="checkbox"/>	<input type="checkbox"/>
4	00:00-00:00	<input type="checkbox"/>	<input type="checkbox"/>
5	00:00-00:00	<input type="checkbox"/>	<input type="checkbox"/>
6	00:00-00:00	<input type="checkbox"/>	<input type="checkbox"/>
7	00:00-00:00	<input type="checkbox"/>	<input type="checkbox"/>
8	00:00-00:00	<input type="checkbox"/>	<input type="checkbox"/>

Figure 8. 6 Set Arming Schedule of Alarm Input

8. Select **Linkage Action** tab to configure alarm response actions. For details, please refer to section 8.5 *Handling Exceptions Alarm*.
9. If necessary, select **PTZ Linking** tab to set PTZ linkage for the alarm input.



Before the setting, check whether the selected speed dome supports PTZ linkage or not.

Trigger Channel	Arming Schedule	Linkage Action	PTZ Linking
PTZ Linking	[D2] Camera 01		
Call Preset	<input type="radio"/>		
Preset	1		
Call Patrol	<input type="radio"/>		
Patrol	1		
Call Pattern	<input type="radio"/>		
Pattern	1		

Figure 8. 7 Set PTZ Linking of Alarm Input

10. Click **OK** to save the settings.
One alarm input can trigger presets, patrol or pattern of more than one channel. But presets, patrols and patterns are exclusive.
11. If you want to set handling action of another alarm input, repeat the above steps.
Or click the **Copy** on the Alarm Input Setup interface and check the checkbox of alarm inputs to copy the settings to them.

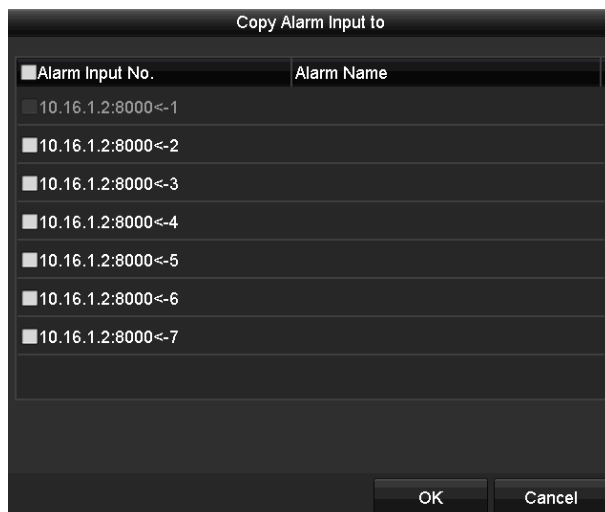


Figure 8. 8 Copy Settings of Alarm Input

8.3 Detecting Video Loss Alarm

Purpose:

Detect video loss of a channel and take alarm response action(s).

Steps:

1. Enter Video Loss interface of Camera Management.

Menu > Camera > Video Loss

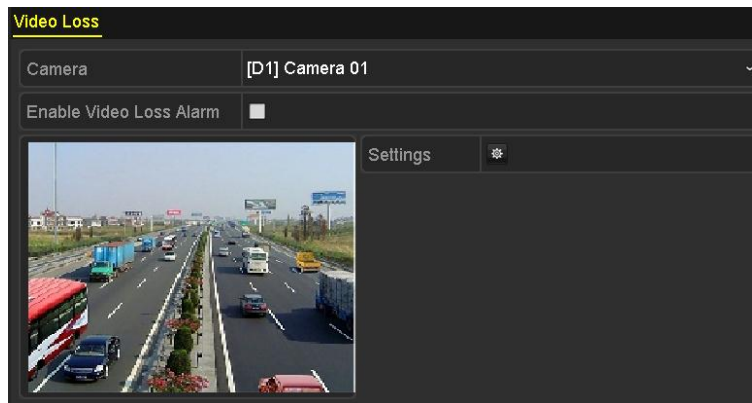



Figure 8. 9 Video Loss Setup Interface

2. Select a **Camera** in the drop-down list.
3. Check the checkbox of **Enable Video Loss Alarm**.
4. Click  button after **Settings** to configure handling action of video loss.
5. Configure **Arming schedule** for the Linkage Actions.
 - 1) Click **Arming Schedule** tab.
 - 2) Choose one day of a **Week**. Up to eight periods can be set within each day.
 - 3) Click **Apply** button to save the settings.



Time periods shall not be repeated or overlapped.

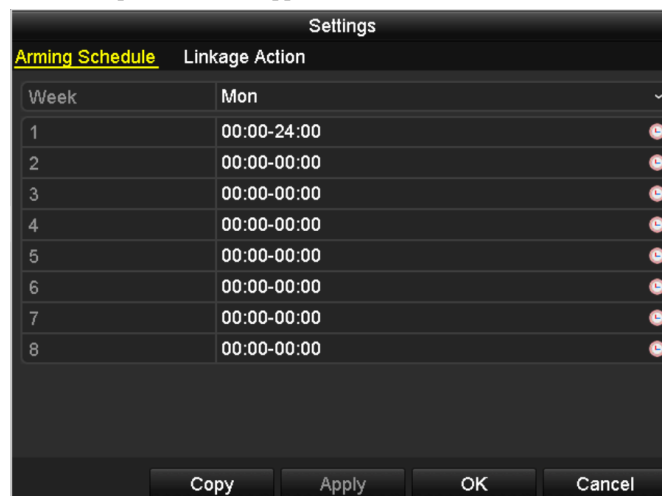


Figure 8. 10 Set Arming Schedule of Video Loss

6. Select **Linkage Action** tab to configure alarm response action. For details, please refer to 8.5 *Handling Exceptions Alarm*.
7. Click the **OK** button to save the settings.

8.4 Detecting Video Tampering Alarm

Purpose:

Trigger alarm when the lens is covered and take alarm response action(s).

Steps:

1. Enter Video Tampering interface.

Menu > Camera > Video Tampering

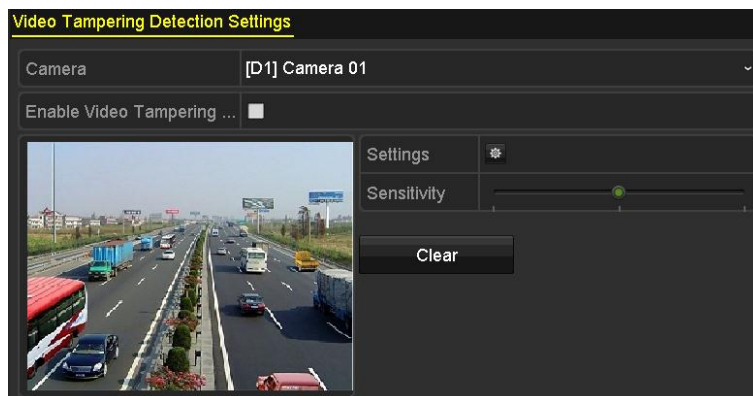



Figure 8. 11 Video Tampering Setup Interface

2. Select the **Camera** in the drop-down list.
3. Check the checkbox of **Enable Video Tampering Detection**.
4. Drag the scroll bar to set the **Sensitivity**.
5. Use the mouse to draw an area in the right live view window to detect video tampering.
6. Click  button to configure handling action.
7. Set **Arming Schedule** parameters.
 - 1) Click **Arming Schedule** tab.
 - 2) Choose one day of a **Week**. Up to eight periods can be set within each day.
 - 3) Click **Apply** button to save the settings.



Time periods cannot be repeated or overlapped.

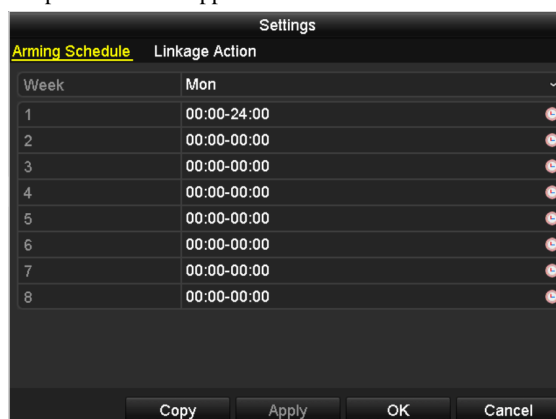


Figure 8. 12 Set Arming Schedule of Video Tampering

8. Select **Linkage Action** tab to configure alarm response actions. For details, please refer to 8.5 *Handling Exceptions Alarm*.
9. Click the **OK** button to save the settings.

8.5 Handling Exceptions Alarm

Purpose:

Exception settings refer to the handling action of various exceptions.

Steps:

1. Enter Exception settings interface.

Menu > Configuration > Exception

Exception	
Enable Event Hint	<input checked="" type="checkbox"/>
Event Hint Settings	
Exception Type	HDD Full
Audible Warning	<input type="checkbox"/>
Notify Surveillance Center	<input type="checkbox"/>
Send Email	<input type="checkbox"/>
Trigger Alarm Output	<input type="checkbox"/>

Figure 8. 13 Exception Settings

2. Select the Exception Type in the drop-down list. Up to 6 kinds types are available.

- **HDD Full:** The HDD is full.
- **HDD Error:** Writing HDD error or unformatted HDD.
- **Network Disconnected:** Disconnected network cable.
- **IP Conflicted:** Duplicated IP address.
- **Illegal Login:** Incorrect user ID or password.
- **Record Exception:** No space for saving recorded files.

3. Check the checkbox of linkage action. Up to 4 linkage actions are available.

- **Audible Warning**

Trigger an audible *beep* when an alarm is detected.

- **Notify Surveillance Center**

Sends an exception or alarm signal to remote alarm host when an event occurs. The alarm host refers to the PC installed with Remote Client.



The alarm signal will be transmitted automatically at detection mode when remote alarm host is configured. Please refer to *11.2.6 Configuring Remote Alarm Host* for details of alarm host configuration.

- **Send Email**

Send an email with alarm information to a user or users when an alarm is detected.

Please refer to *11.2.10 Configuring Email* for details of Email configuration.

- **Trigger Alarm Output**

Trigger an alarm output when an alarm occurs.

You need to configure the dwell time and arming schedule for the alarm output.

- a) Enter Alarm Output interface.

Menu > Configuration > Alarm > Alarm Output

- b) Select an **Alarm Output No.**

- c) Input the **Alarm Name** and set the **Dwell Time**.



If **Manually Clear** is selected for **Dwell Time**, it only be cleared in Menu > Manual > Alarm.

Alarm Status	Alarm Input	Alarm Output
Alarm Output No.	10.16.1.2:8000->1	
Alarm Name		
Dwell Time	5s	
Settings		

Figure 8. 14 Alarm Output Setup Interface

- d) Set the Arming Schedule.

- i. Click the button after Settings.
- ii. Choose one day of a **Week**. Up to 8 periods can be set within each day.



Time periods shall not be repeated or overlapped.

Settings	
Arming Schedule	
Week	Mon
1	00:00-24:00
2	00:00-00:00
3	00:00-00:00
4	00:00-00:00
5	00:00-00:00
6	00:00-00:00
7	00:00-00:00
8	00:00-00:00

Figure 8. 15 Set Arming Schedule of Alarm Output

- iii. Repeat the above steps to configure arming schedule for other days. You can also click **Copy** to copy the arming schedule to other days.
 - iv. Click the **OK** button to save the settings and back to Alarm Output interface.
- e) Optionally, click **Copy** to copy the above settings to other alarm outputs.

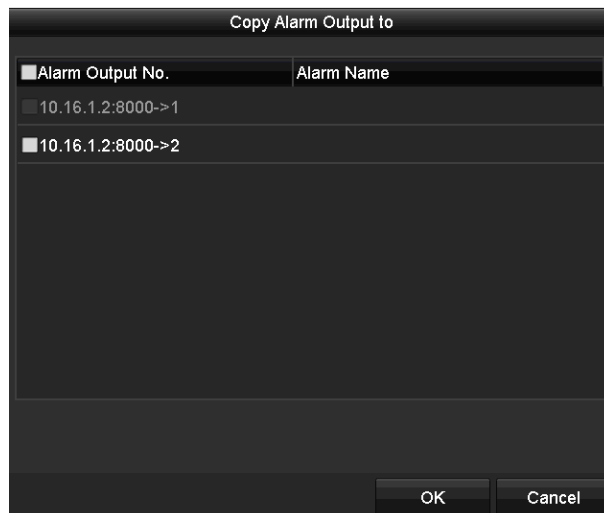


Figure 8. 16 Copy Settings of Alarm Output

8.6 Setting Event Hint Display

Purpose:

When an event or exception happens, a hint will display on the lower-left corner of live view image. And you can click the hint icon to check the details. Besides, the event to be displayed is configurable.

Steps:

1. Enter the Exception settings interface.
Menu > Configuration > Exceptions
2. Check the checkbox of **Enable Event Hint**.



Figure 8. 17 Event Hint Settings Interface


3. Click the  to set the type of event to be displayed on the image.



Figure 8. 18 Event Hint Settings Interface

4. Check the checkbox of events to hint.
5. Click the **OK** button to save the settings.

8.7 Triggering or Clearing Alarm Output Manually

Purpose:

Sensor alarm can be triggered or cleared manually. If Manually Clear is selected in the drop-down list of dwell time of an alarm output, the alarm can be cleared only by clicking **Clear** button in the following interface.

Steps:

1. Select the alarm output you want to trigger or clear and make related operations.

Menu > Manual > Alarm

2. Trigger / clear an alarm output.

- 1) Click to select an Alarm Output No..
- 2) Click **Trigger** or **Clear** to trigger or clear the alarm output.

3. Click **Trigger All** to trigger all and click Clear All to clear all alarm outputs.

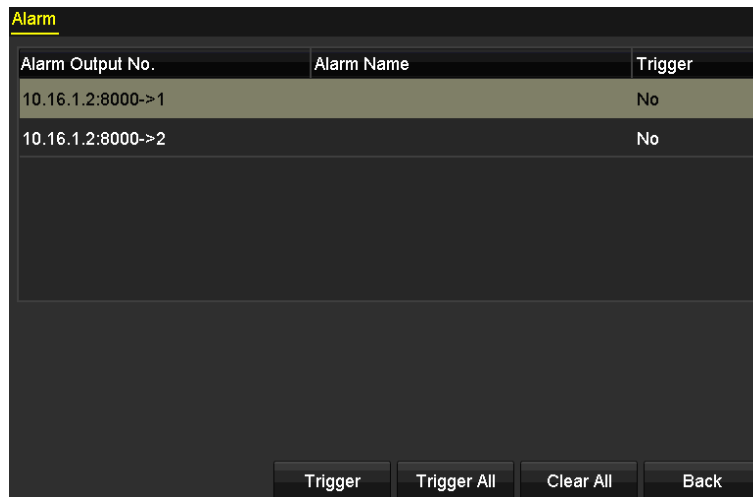


Figure 8. 19 Clear or Trigger Alarm Output Manually

Chapter 9 VCA Alarm



All VCA detection must be supported by the connected IP camera.

Face detection and vehicle detection are supported by DS-8600NI-E8 and DS-7700NI-E4 series.

9.1 Face Detection

Purpose:

Face detection function detects the face appears in the surveillance scene, and some certain actions can be taken when the alarm is triggered.

Steps:

1. Enter the VCA settings interface.
Menu> Camera> VCA
2. Select the camera to configure the VCA.

You can click the checkbox of **Save VCA Picture** to save the captured pictures of VCA detection.

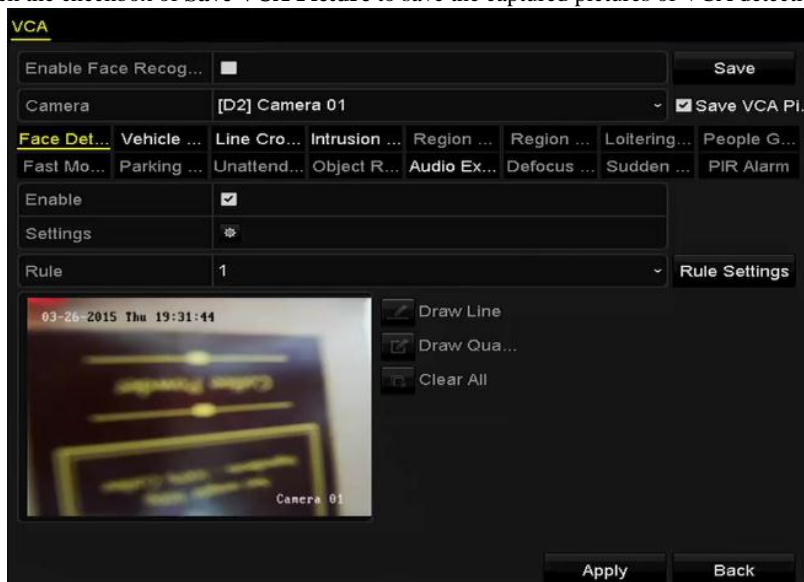


Figure 9. 1 Face Detection

3. Select the VCA detection type to **Face Detection**.
4. Click to enter the face detection settings interface. Configure the trigger channel, arming schedule and linkage action for the face detection alarm. Please refer to step3~step5 of 8.1 Setting Motion Detection Alarm for detailed instructions.
5. Click the **Rule Settings** button to set the face detection rules. You can click-and-drag the slider to set the detection sensitivity.

Sensitivity: Range [1-5]. The higher the value is, the more easily the face can be detected.

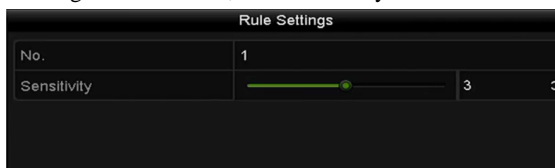


Figure 9. 2 Set Face Detection Sensitivity

6. Click Apply to activate the settings.

9.2 Vehicle Detection

Purpose:

Vehicle Detection is available for the road traffic monitoring. In Vehicle Detection, the passed vehicle can be detected and the picture of its license plate can be captured. You can send alarm signal to notify the surveillance center and upload the captured picture to FTP server.

Steps:

1. Enter the VCA settings interface.
Menu > Camera > VCA
2. Select the camera to configure the VCA.
You can click the checkbox of **Save VCA Picture** to save the captured pictures of VCA detection.
3. Select the VCA detection type to **Vehicle Detection**.
4. Check the **Enable** checkbox to enable this function.

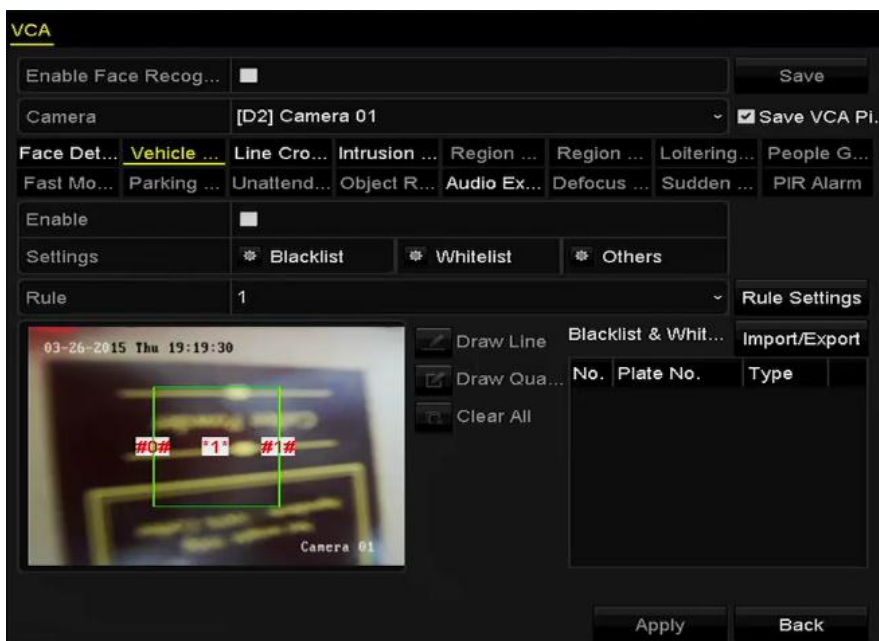




Figure 9. 3 Set Vehicle Detection

5. Click  to configure the trigger channel, arming schedule and linkage actions for the Blacklist, Whitelist and Others.
6. Click the **Rule Settings** to enter the rule settings interface. Configure the lane, upload picture and overlay content settings. Up to 4 lanes are selectable.



Rule Settings	
Basic Picture Overlay Content	
No.	1
Scene No.	Vehicle Detection Scene 1
Scene Name	
Lane Number	1

Apply OK Cancel

Figure 9. 4 Rule Settings

-
7. Click **Save** to save the settings.




Please refer to the User Manual of Network Camera for the detailed instructions for the vehicle detection.

9.3 Line Crossing Detection

Purpose:

This function can be used for detecting people, vehicles and objects cross a set virtual line. The line crossing direction can be set as bidirectional, from left to right or from right to left. And you can set the duration for the alarm response actions, such as full screen monitoring, audible warning, etc.

Steps:

1. Enter the VCA settings interface.
Menu> Camera> VCA
2. Select the camera to configure the VCA.
You can click the checkbox of **Save VCA Picture** to save the captured pictures of VCA detection.
3. Select the VCA detection type to **Line Crossing Detection**.
4. Check the **Enable** checkbox to enable this function.
5. Click  to configure the trigger channel, arming schedule and linkage actions for the line crossing detection alarm.
6. Click the **Rule Settings** button to set the line crossing detection rules.
 - 1) Select the direction to A<->B, A->B or A<-B.



A<->B: Only the arrow on the B side shows; when an object going across the configured line with both direction can be detected and alarms are triggered.

A->B: Only the object crossing the configured line from the A side to the B side can be detected.

B->A: Only the object crossing the configured line from the B side to the A side can be detected.
 - 2) Click-and-drag the slider to set the detection sensitivity.
Sensitivity: Range [1-100]. The higher the value is, the more easily the detection alarm can be triggered.
 - 3) Click-**OK** to save the rule settings and back to the line crossing detection settings interface.



Figure 9. 5 Set Line Crossing Detection Rules

7. Click  and set two points in the preview window to draw a virtual line.
You can use the  to clear the existing virtual line and re-draw it.



Up to 4 rules can be configured.

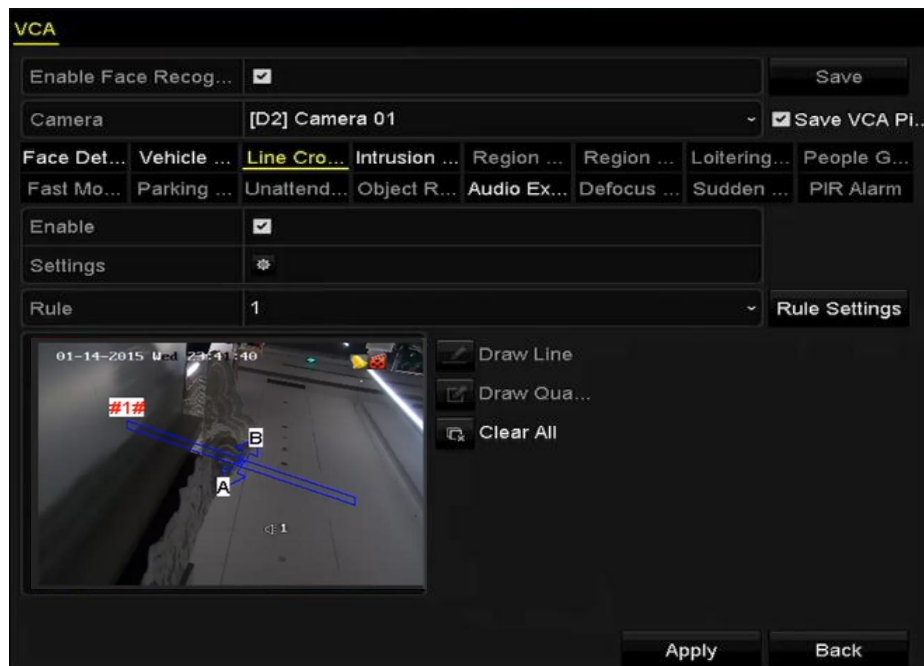


Figure 9. 6 Draw Line for Line Crossing Detection

8. Click **Apply** to activate the settings.

9.4 Intrusion Detection

Purpose:

Intrusion detection function detects people, vehicle or other objects which enter and loiter in a pre-defined virtual region, and some certain actions can be taken when the alarm is triggered.

Steps:




1. Enter the VCA settings interface.
Menu> Camera> VCA
2. Select the camera to configure the VCA.
You can click the checkbox of **Save VCA Picture** to save the captured pictures of VCA detection.
3. Select the VCA detection type to **Intrusion Detection**.
4. Check the **Enable** checkbox to enable this function.
5. Click  to configure the trigger channel, arming schedule and linkage actions for the line crossing detection alarm.
6. Click the **Rule Settings** button to set the intrusion detection rules. Set the following parameters.
 - 1) **Threshold:** Range [1s-10s], the threshold for the time of the object loitering in the region. When the duration of the object in the defined detection area is longer than the set time, the alarm will be triggered.
 - 2) Click-and-drag the slider to set the detection sensitivity.
Sensitivity: Range [1-100]. The value of the sensitivity defines the size of the object which can trigger the alarm. The higher the value is, the more easily the detection alarm can be triggered.
 - 3) **Percentage:** Range [1-100]. Percentage defines the ratio of the in-region part of the object which can trigger the alarm. For example, if the percentage is set as 50%, when the object enters the region and occupies half of the whole region, the alarm is triggered.



Figure 9. 7 Set Intrusion Crossing Detection Rules

- 4) Click-**OK** to save the rule settings and back to the line crossing detection settings interface.
7. Click  and draw a quadrilateral in the preview window by specifying four vertexes of the detection region, and right click to complete drawing. Only one region can be configured.

You can use the  to clear the existing virtual line and re-draw it.



Up to 4 rules can be configured.

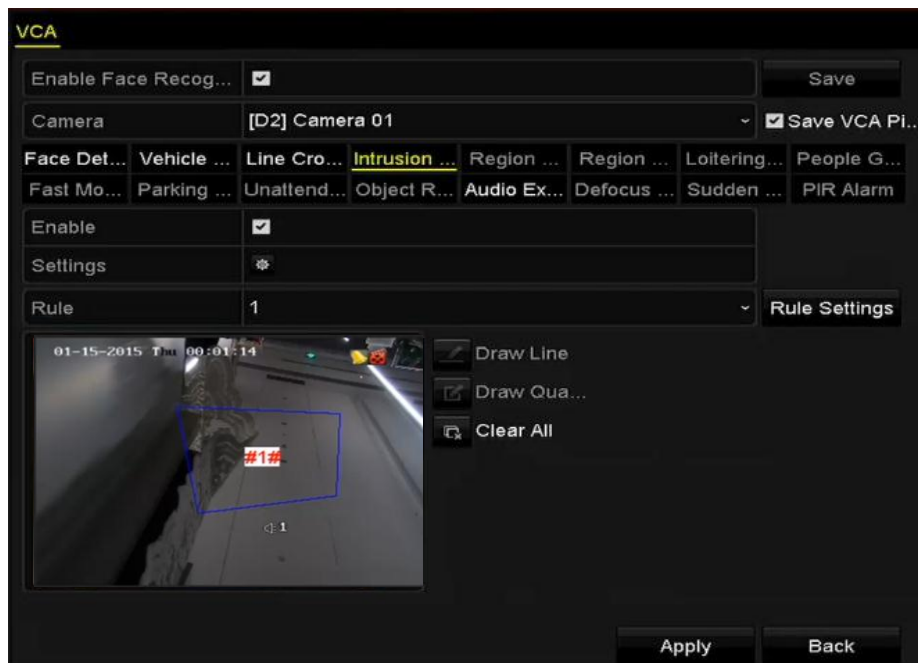


Figure 9. 8 Draw Area for Intrusion Detection




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

9.5 Region Entrance Detection

Purpose:

Region entrance detection function detects people, vehicle or other objects which enter a pre-defined virtual region from the outside place, and some certain actions can be taken when the alarm is triggered.

Steps:

1. Enter the VCA settings interface.
Menu> Camera> VCA
2. Select the camera to configure the VCA.
You can click the checkbox of **Save VCA Picture** to save the captured pictures of VCA detection.
3. Select the VCA detection type to **Region Entrance Detection**.
4. Check the **Enable** checkbox to enable this function.
5. Click  to configure the trigger channel, arming schedule and linkage actions for the line crossing detection alarm.
6. Click the **Rule Settings** button to set the sensitivity of the region entrance detection.
Sensitivity: Range [0-100]. The higher the value is, the more easily the detection alarm can be triggered.
7. Click  and draw a quadrilateral in the preview window by specifying four vertexes of the detection region, and right click to complete drawing. Only one region can be configured.
You can use the  to clear the existing virtual line and re-draw it.

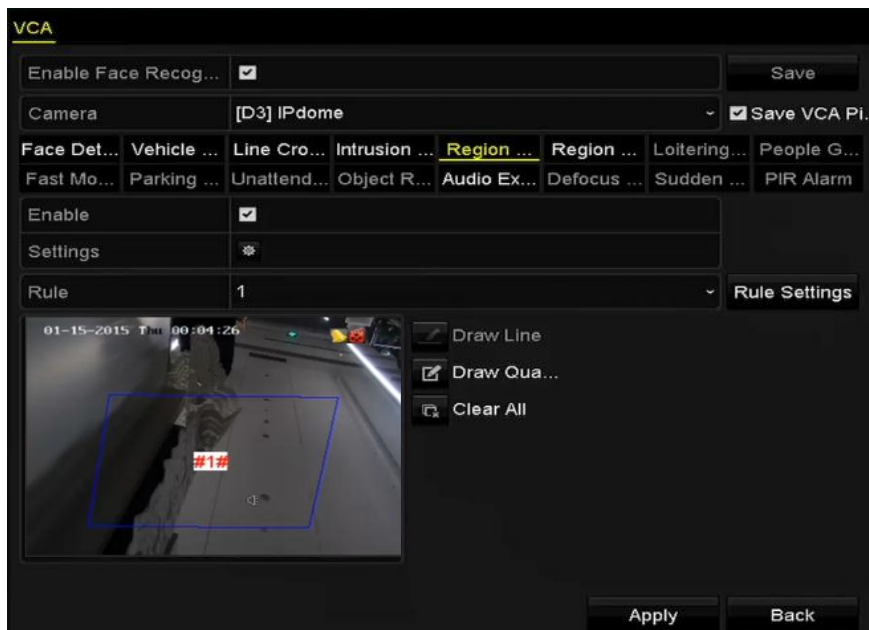


Figure 9. 9 Set Region Entrance Detection



Up to 4 rules can be configured.

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

9.6 Region Exiting Detection

Purpose:

Region exiting detection function detects people, vehicle or other objects which exit from a pre-defined virtual region, and some certain actions can be taken when the alarm is triggered.



Please refer to the *Chapter 9.5 Region Entrance Detection* for operating steps to configure the region exiting detection.

Up to 4 rules can be configured.

9.7 Loitering Detection

Purpose:

Loitering detection function detects people, vehicle or other objects which loiter in a pre-defined virtual region for some certain time, and a series of actions can be taken when the alarm is triggered.



Please refer to the *Chapter 9.4 Intrusion Detection* for operating steps to configure the loitering detection.

The **Threshold** [1s-10s] in the Rule Settings defines the time of the object loitering in the region. If you set the value as 5, alarm is triggered after the object loitering in the region for 5s; and if you set the value as 0, alarm is triggered immediately after the object entering the region.

Up to 4 rules can be configured.

9.8 People Gathering Detection

Purpose:

People gathering detection alarm is triggered when people gather around in a pre-defined virtual region, and a series of actions can be taken when the alarm is triggered.



Please refer to the *Chapter 9.4 Intrusion Detection* for operating steps to configure the people gathering detection.

The **Percentage** in the Rule Settings defines the gathering density of the people in the region. Usually, when the percentage is small, the alarm can be triggered when small number of people gathered in the defined detection region.

Up to 4 rules can be configured.

9.9 Fast Moving Detection

Purpose:

Fast moving detection alarm is triggered when people, vehicle or other objects move fast in a pre-defined virtual region, and a series of actions can be taken when the alarm is triggered.



Please refer to the *Chapter 9.4 Intrusion Detection* for operating steps to configure the fast moving detection. The **Sensitivity** in the Rule Settings defines the moving speed of the object which can trigger the alarm. The higher the value is, the more easily a moving object can trigger the alarm. Up to 4 rules can be configured.

9.10 Parking Detection

Purpose:

Parking detection function detects illegal parking in places such as highway, one-way street, etc., and a series of actions can be taken when the alarm is triggered.



Please refer to the *Chapter 9.4 Intrusion Detection* for operating steps to configure the parking detection. The **Threshold**[5s-20s] in the Rule Settings defines the time of the vehicle parking in the region. If you set the value as 10, alarm is triggered after the vehicle stay in the region for 10s. Up to 4 rules can be configured.

9.11 Unattended Baggage Detection

Purpose:

Unattended baggage detection function detects the objects left over in the pre-defined region such as the baggage, purse, dangerous materials, etc., and a series of actions can be taken when the alarm is triggered.



Please refer to the *Chapter 9.4 Intrusion Detection* for operating steps to configure the unattended baggage detection. The **Threshold**[5s-20s] in the Rule Settings defines the time of the objects left over in the region. If you set the value as 10, alarm is triggered after the object is left and stay in the region for 10s. And the **Sensitivity** defines the similarity degree of the background image. Usually, when the sensitivity is high, a very small object left in the region can trigger the alarm. Up to 4 rules can be configured.

9.12 Object Removal Detection

Purpose:

Object removal detection function detects the objects removed from the pre-defined region, such as the exhibits on display, and a series of actions can be taken when the alarm is triggered.



Please refer to the *Chapter 9.4 Intrusion Detection* for operating steps to configure the object removal

detection.

The **Threshold** [5s-20s] in the Rule Settings defines the time of the objects removed from the region. If you set the value as 10, alarm is triggered after the object disappears from the region for 10s. And the **Sensitivity** defines the similarity degree of the background image. Usually, when the sensitivity is high, a very small object taken from the region can trigger the alarm.


Up to 4 rules can be configured.

9.13 Audio Exception Detection

Purpose:

Audio exception detection function detects the abnormal sounds in the surveillance scene, such as the sudden increase / decrease of the sound intensity, and some certain actions can be taken when the alarm is triggered.

Steps:

1. Enter the VCA settings interface.
Menu> Camera> VCA
2. Select the camera to configure the VCA.
You can click the checkbox of **Save VCA Picture** to save the captured pictures of VCA detection.
3. Select the VCA detection type to **Audio Exception Detection**.
4. Click  to configure the trigger channel, arming schedule and linkage action for the face detection alarm.
5. Click the **Rule Settings** button to set the audio exception rules.

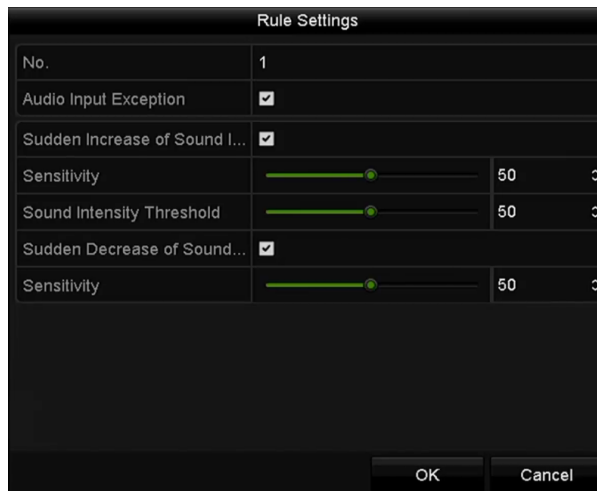


Figure 9. 10 Set Audio Exception Detection Rules

- 1) Check the checkbox of **Audio Input Exception** to enable the audio loss detection function.
- 2) Check the checkbox of **Sudden Increase of Sound Intensity Detection** to detect the sound steep rise in the surveillance scene. You can set the detection sensitivity and threshold for sound steep rise.
Sensitivity: Range [1-100], the smaller the value is, the more severe the change should be to trigger the detection.
Sound Intensity Threshold: Range [1-100], it can filter the sound in the environment, the louder the environment sound, the higher the value should be. You can adjust it according to the real environment.
- 3) Check the checkbox of **Sudden Decrease of Sound Intensity Detection** to detect the sound steep drop in the surveillance scene. You can set the detection sensitivity[1-100] for sound steep drop.
6. Click **Apply** to activate the settings.

9.14 Sudden Scene Change Detection

Purpose:

Scene change detection function detects the change of surveillance environment affected by the external factors; such as the intentional rotation of the camera, and some certain actions can be taken when the alarm is triggered.



Please refer to the *Chapter 9.1 Face Detection* for operating steps to configure the scene change detection.

The **Sensitivity** in the Rule Settings ranges from 1 to 100, and the higher the value is, the more easily the change of scene can trigger the alarm.

9.15 Defocus Detection

Purpose:

The image blur caused by defocus of the lens can be detected, and some certain actions can be taken when the alarm is triggered.



Please refer to the *Chapter 9.1 Face Detection* for operating steps to configure the defocus detection.


The **Sensitivity** in the Rule Settings ranges from 1 to 100, and the higher the value is, the more easily the defocus image can trigger the alarm.

9.16 PIR Alarm

Purpose:

A PIR (Passive Infrared) alarm is triggered when an intruder moves within the detector's field of view. The heat energy dissipated by a person, or any other warm blooded creature such as dogs, cats, etc., can be detected.

Steps:

1. Enter the VCA settings interface.
Menu> Camera> VCA
2. Select the camera to configure the VCA.
You can click the checkbox of **Save VCA Picture** to save the captured pictures of VCA detection.
3. Select the VCA detection type to **PIR Alarm**.
4. Click  to configure the trigger channel, arming schedule and linkage action for the PIR alarm.
5. Click the **Rule Settings** button to set the rules. Please refer to the *Chapter 9.1 Face Detection* for instructions.
6. Click **Apply** to activate the settings.

Chapter 10 VCA Search

With the configured VCA detection, the NVR supports the VCA search for the behavior analysis, face capture, people counting and heat map results.



The DS-7600 series NVR supports the behavior search only.

10.1 Face Search

Purpose:

When there are detected face picture captured and saved in HDD, you can enter the Face Search interface to search the picture and play the picture related video file according to the specified conditions.

Before you start:

Please refer to *Section 9.1 Face Detection* for configuring the face detection.

Steps:

1. Enter the **Face Search** interface.
Menu>VCA Search> Face Search
2. Select the camera (s) for the face search.

Face Search								
<input checked="" type="checkbox"/> IP Camera	<input checked="" type="checkbox"/> D1	<input checked="" type="checkbox"/> D2	<input checked="" type="checkbox"/> D3	<input checked="" type="checkbox"/> D4	<input checked="" type="checkbox"/> D5	<input checked="" type="checkbox"/> D6	<input checked="" type="checkbox"/> D7	<input checked="" type="checkbox"/> D8
Start Time	11-12-2014		00:00:00					
End Time	02-12-2015		23:59:59					
				<input type="button" value="Search"/> <input type="button" value="Back"/>				

Figure 10. 1 Face Search

3. Specify the start time and end time for search the captured face pictures or video files.
4. Click **Search** to start searching. The search results of face detection pictures are displayed in list or in chart.

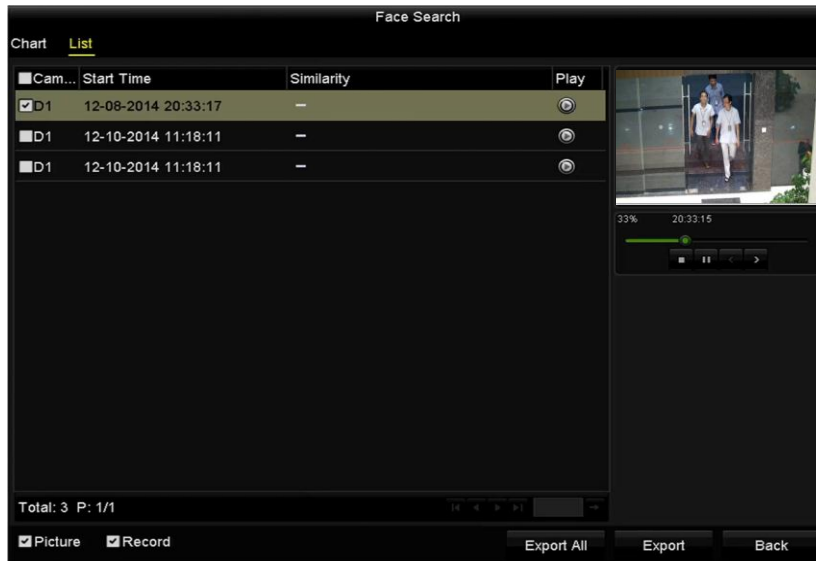


Figure 10. 2 Face Search Interface

5. Play the face picture related video file.

You can double click on a face picture to play its related video file in the view window on the top right, or select a picture item and click to play it.

You can also click to stop the playing, or click to play the previous/next file.

6. If you want to export the captured face pictures to local storage device, connect the storage device to the device and click **Export All** to enter the Export interface.

Click **Export** to export all face pictures to the storage device.

Please refer to *Chapter 7 Backup* for the operation of exporting files.



Figure 10. 3 Export Files

10.2 Behavior Search

Purpose:

The behavior analysis detects a series of suspicious behavior based on VCA detection, and certain linkage methods will be enabled if the alarm is triggered.

Steps:

1. Enter the **Behavior Search** interface.
Menu>VCA Search> Behavior Search
2. Select the camera (s) for the behavior search.
3. Specify the start time and end time for searching the matched pictures.

Figure 10. 4 Behavior Search Interface

4. Select the VCA detection type from the dropdown list, including the line crossing detection, intrusion detection, unattended baggage detection, object removal detection, region entrance detection, region exiting detection, parking detection, loitering detection, people gathering detection and fast moving detection.
5. Click **Search** to start searching. The search results of pictures are displayed in list or in chart.

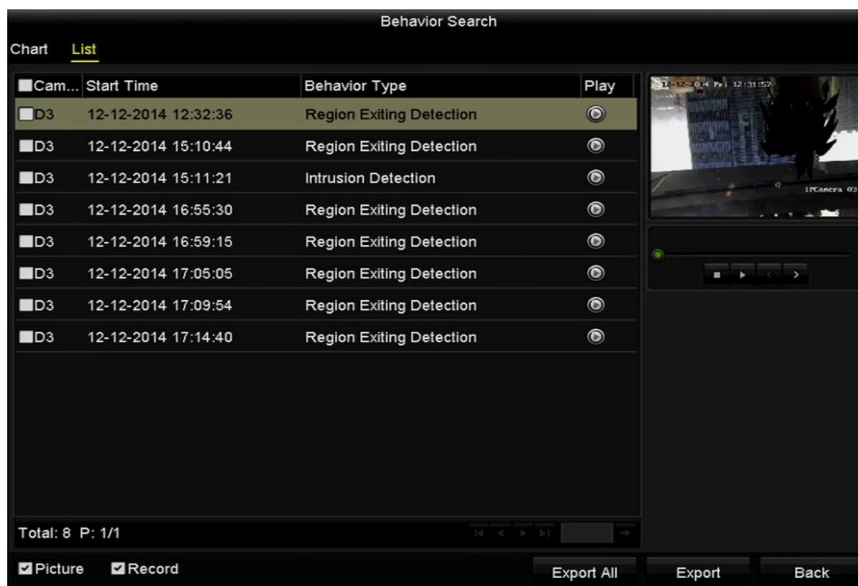


Figure 10. 5 Behavior Search Results

6. Play the behavior analysis picture related video file.

You can double click on a picture from the list to play its related video file in the view window on the top right, or select a picture item and click [Play Icon] to play it.

You can also click [Stop Icon] to stop the playing, or click [Previous Icon] [Next Icon] to play the previous/next file.

7. If you want to export the captured pictures to local storage device, connect the storage device to the device and click **Export All** to enter the Export interface.

Click **Export** to export all pictures to the storage device.

10.3 Plate Search

Purpose: You can search and view the matched captured vehicle plate picture and related information according to the plate searching conditions including the start time/end time, country and plate No..

Steps:

1. Enter the **Plate Search** interface.

Menu > VCA Search > Plate Search

2. Select the camera (s) for the plate search.

3. Specify the start time and end time for searching the matched plate pictures.

Figure 10. 6 Plate Search

4. Select the country from the drop-down list for searching the location of the vehicle plate.
5. Input the plate No. in the field for search.
7. Click **Search** to start searching. The search results of detected vehicle plate pictures are displayed in list or in chart.



Please refer to the Step7-Step8 of *Section 10.1 Face Search* for the operation of the search results.

10.4 People Counting

Purpose:

The People Counting is used to calculate the number of people entered or left a certain configured area and form in daily/weekly/monthly/annual reports for analysis.

Steps:

1. Enter the **People Counting** interface.
Menu>VCA Search> People Counting
2. Select the camera for the people counting.
3. Select the report type to Daily Report, Weekly Report, Monthly Report or Annual Report.
4. Set the statistics time.
5. Click the **Counting** button to start people counting statistics.

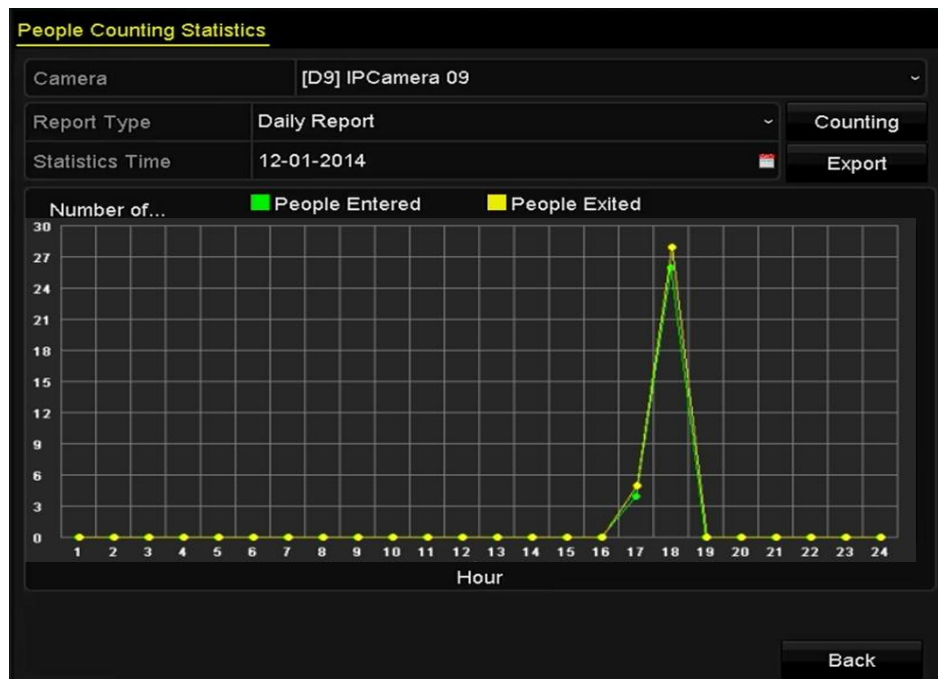


Figure 10. 7 People Counting Interface

6. You can click the **Export** button to export the statistics report in excel format.

10.5 Heat Map

Purpose:

Heat map is a graphical representation of data represented by colors. The heat map function is usually used to analyze the visit times and dwell time of customers in a configured area.



The heat map function must be supported by the connected IP camera and the corresponding configuration must be set.

Steps:

1. Enter the **Heat Map** interface.
Menu>VCA Search> Heat Map
2. Select the camera for the heat map processing.
3. Select the report type to Daily Report, Weekly Report, Monthly Report or Annual Report.
4. Set the statistics time.

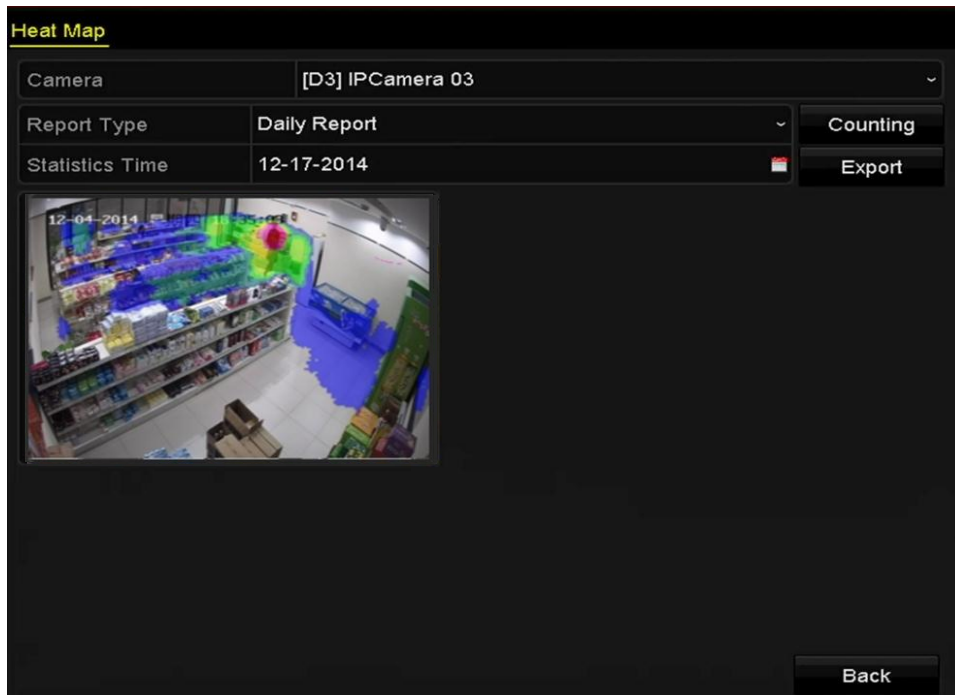


Figure 10. 8 Heat Map Interface

5. Click the **Counting** button to export the report data and start heat map statistics, and the results are displayed in graphics marked in different colors.



As shown in the figure above, red color block (255, 0, 0) indicates the most welcome area, and blue color block (0, 0, 255) indicates the less-popular area.

You can click the **Export** button to export the statistics report in excel format.

Chapter 11 Network Settings

11.1 Configuring General Settings

Purpose:

Network settings must be properly configured before you operate NVR over network.

Steps:

1. Enter the Network Settings interface.

Menu > Configuration > Network

2. Select the **General** tab.

NIC Type	10M/100M Self-adaptive		
Enable DHCP	<input type="checkbox"/>		
IPv4 Address...	10 .16 .1 .20	IPv6 Address...	fe80::c256:e3ff:fe21:86e7/64
IPv4 Subn...	255 .255 .255 .0	IPv6 Address...	
IPv4 Defa...	192 .168 .254 .1	IPv6 Defa...	
MAC Address	c0:56:e3:21:86:e7		
MTU(Bytes)	1500		
Preferred DNS Server	192.168.254.1		
Alternate DNS Server			

Figure 11. 1 Network Settings Interface

3. In the **General Settings** interface, you can configure the following settings: **NIC Type**, **IPv4 Address**, **IPv4 Gateway**, **MTU** and **DNS Server**.



The valid value range of MTU is 500 ~ 9676.

If the DHCP server is available, you can check the checkbox of **Enable DHCP** to automatically obtain an IP address and other network settings.

4. Click **Apply** button to save the settings.

11.2 Configuring Advanced Settings

11.2.1 Configuring Wireless Network

Configuring WAN Settings

Purpose:

The device provides you with wired and wireless network features, just as a wireless router. You can access to internet via NVR instead of a router.

Before you start:

Establish the connection between the NVR and Internet via the WAN interface.

Steps:

1. Enter WAN configuration interface.

Menu > Configuration > WIFI

Figure 11. 2 WAN Configuration Interface

2. Select the **Connection Mode** as **PPPoE**.
3. Input **Account** and **Password** in the text field.
4. Click **Apply** to dial up.

Configuring WIFI Settings

Steps:

1. Enter WIFI configuration interface.

Menu > Configuration > WIFI

Figure 11. 3 WIFI Configuration Interface

2. Click the **WIFI** tab to enter WIFI configuration interface.
3. Input **SSID** in the text field.

SSID: the name of WIFI.

4. Select **Working Channel** and **Security Type** in the drop-down list.
5. If **Security Type** is set other one of the four types except **Disable**, select **Encryption Type** and input **Network Security Key**.



WPA2-PSK and **AES** is more secure than **WPA-PSK** and **TKIP**. However, there may terminals which do not support **WPA2-PSK** and **AES**. When you not sure whether terminals support or not, you can select **WPA-PSK/ WPA2-PSK** and **TKIP/AES** to make NVR do the adaptive selection.

6. Click **Apply** to set up a wireless network.

11.2.2 Configuring EZVIZ Cloud P2P

Purpose:

EZVIZ Cloud P2P provides the mobile phone application and as well the service platform page to access and manage your connected NVR, which enables you to get a convenient remote access to the surveillance system.

Steps:

1. Enter the Network Settings interface.
Menu > Configuration > Network
2. Select the **Platform Access** tab to enter the EZVIZ Cloud P2P Settings interface.
3. Check the **Enable** checkbox to activate this feature.
4. If required, select the checkbox of **Custom** and input the **Server Address**.
5. To turn the **Enable Stream Encryption** on, you can select its checkbox.
6. Enter the **Verification Code** of the device.



The Verification Code consists of 6 capital letters and is located at the bottom of the NVR.

Enable	<input type="checkbox"/>
Access Type	EZVIZ Cloud P2P
Server Address	dev.ezviz7.com <input type="checkbox"/> Custom
Enable Stream Encryption	<input type="checkbox"/>
Verification Code	
Status	Offline

Figure 11. 4 EZVIZ Cloud P2P Settings Interface

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

After configuration, you can access and manage the NVR by your mobile phone on which the EZVIZ Cloud P2P application is installed or by the EZVIZ website (www.ezviz7.com).



For more operation instructions, please refer to the help file on the EZVIZ official website (www.ezviz7.com).

11.2.3 Configuring DDNS

Purpose:

If your NVR is set to use PPPoE as its default network connection, you may set Dynamic DNS (DDNS) to be used for network access.

Prior registration with your ISP is required before configuring the system to use DDNS.

Steps:

1. Enter the Network Settings interface.
Menu > Configuration > Network
2. Select the **DDNS** tab to enter the DDNS Settings interface.
3. Check the **Enable DDNS** checkbox to enable this feature.
4. Select **DDNS Type**. Five different DDNS types are selectable: IPServer, DynDNS, PeanutHull, NO-IP and HiDDNS.
 - **IPServer:** Enter **Server Address** for IPServer.

Enable DDNS	<input checked="" type="checkbox"/>
DDNS Type	IPServer
Area/Country	Custom
Server Address	
Device Domain Name	
Status	Connecting the address server failed.
User Name	
Password	

Figure 11. 5 IPServer Settings Interface

- **DynDNS:**
 - 1) Enter **Server Address** for DynDNS (i.e. members.dyndns.org).
 - 2) In the NVR Domain Name text field, enter the domain obtained from the DynDNS website.
 - 3) Enter the **User Name** and **Password** registered in the DynDNS website.

Enable DDNS	<input checked="" type="checkbox"/>
DDNS Type	DynDNS
Area/Country	Custom
Server Address	
Device Domain Name	
Status	Connecting the address server failed.
User Name	
Password	

Figure 11. 6 DynDNS Settings Interface

- **PeanutHull:** Enter the **User Name** and **Password** obtained from the PeanutHull website.

Enable DDNS	<input checked="" type="checkbox"/>
DDNS Type	PeanutHull
Area/Country	Custom
Server Address	
Device Domain Name	
Status	Connecting the address server failed.
User Name	
Password	

Figure 11. 7 PeanutHull Settings Interface

- **NO-IP:**

Enter the account information in the corresponding fields. Refer to the DynDNS settings.

- 1) Enter **Server Address** for NO-IP.
- 2) In the NVR Domain Name text field, enter the domain obtained from the NO-IP website (www.no-ip.com).
- 3) Enter the **User Name** and **Password** registered in the NO-IP website.

Enable DDNS	<input checked="" type="checkbox"/>
DDNS Type	NO-IP
Area/Country	Custom
Server Address	
Device Domain Name	
Status	Connecting the address server failed.
User Name	
Password	

Figure 11. 8 NO-IP Settings Interface

- **HiDDNS:**

- 1) Select the continent/country of the server on which the device is registered.
- 2) The **Server Address** of the HiDDNS server appears by default: www.hik-online.com.
- 3) Enter the **Device Domain Name**. You can use the alias you registered in the HiDDNS server or define a new device domain name. If a new alias of the device domain name is defined in the NVR, it will replace the old one registered on the server. You can register the alias of the device domain name in the HiDDNS server first and then enter the alias to the **Device Domain Name** in the NVR; you can also enter the domain name directly on the NVR to create a new one.

Enable DDNS	<input checked="" type="checkbox"/>
DDNS Type	HiDDNS
Area/Country	Custom
Server Address	www.hik-online.com
Device Domain Name	
Status	Connecting the address server failed.
User Name	
Password	

Figure 11. 9 HiDDNS Settings Interface

➤ **Register the device on the HiDDNS server.**

- 1) Go to the HiDDNS website: www.hik-online.com.

Figure 11. 10 Register an Account

- 2) Click **Register** to register an account if you do not have one and use the account to log in.

Figure 11. 11 Register an Account

- 3) In the Device Management interface, click **Add** to register the device.

Figure 11. 12 Register the Device

- 4) Input **Device Serial No.**, **Device Domain (Device Name)** and **HTTP Port**. And click **OK** to add the device.

➤ **Access the Device via Web Browser or Client Software**

After having successfully registered the device on the HiDDNS server, you can access your device via web browser or Client Software with the **Device Domain Name (Device Name)**.

OPTION 1: Access the Device via Web Browser

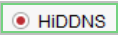
Open a web browser, and enter <http://www.hik-online.com/alias> in the address bar. Alias refers to the **Device Domain Name** on the device or the **Device Name** on the HiDDNS server.

Example: <http://www.hik-online.com/nvr>



If you mapped the HTTP port on your router and changed it to port No. except 80, you have to enter <http://www.hik-online.com/alias:HTTP port> in the address bar to access the device. You can refer to *Chapter 9.2.11* for the mapped HTTP port No.

OPTION 2: Access the devices via iVMS-4200

For iVMS-4200, in the Add Device window, select  and then edit the device information.

Nickname: Edit a name for the device as you want.

Server Address: www.hik-online.com

Device Domain Name: It refers to the **Device Domain Name** on the device or the **Device Name** on the HiDDNS server you created.

User Name: Enter the user name of the device.

Password: Enter the password of the device.

Figure 11. 13 Access Device via iVMS-4200

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

After setting all the required parameters for the DDNS, you can view the connecting status of the device by checking the **Status** information.

11.2.4 Configuring NTP Server

Purpose:

Ensure the network connection of the PC (running FTP server) and the device is valid and correct. Run the FTP server on the PC and copy the firmware into the corresponding directory of your PC.



Refer to the user manual of the FTP server to set the FTP server on your PC and put the firmware file into the directory as required.

Steps:

1. Enter the Network Settings interface.
Menu > Configuration > Network
2. Select the **NTP** tab to enter the NTP Settings interface, as shown in Figure 11. 14.

Enable NTP	<input checked="" type="checkbox"/>
Interval (min)	60
NTP Server	129.6.15.28
NTP Port	123

Figure 11. 14 NTP Settings Interface

3. Check the **Enable NTP** checkbox to enable this feature.
4. Configure the following NTP settings:
 - **Interval:** Time interval between the two synchronizing actions with NTP server. The unit is minute.
 - **NTP Server:** IP address of NTP server.
 - **NTP Port:** Port of NTP server.
5. Click the **Apply** button to save and exit the interface.



The time synchronization interval can be set from 1 to 10080min, and the default value is 60min. If the NVR is connected to a public network, you should use a NTP server that has a time synchronization function, such as the server at the National Time Center (IP Address: 210.72.145.44). If the NVR is setup in a more customized network, NTP software can be used to establish a NTP server used for time synchronization.

11.2.5 Configuring SNMP

Purpose:

You can use SNMP protocol to get device status and parameters related information.

Steps:

1. Enter the Network Settings interface.
Menu > Configuration > Network
2. Select the **SNMP** tab to enter the SNMP Settings interface, as shown in Figure 11. 15.

Enable SNMP	<input checked="" type="checkbox"/>
SNMP Version	V2
SNMP Port	161
Read Community	public
Write Community	private
Trap Address	
Trap Port	162

Figure 11. 15 SNMP Settings Interface

3. Check the **SNMP** checkbox to enable this feature.
4. Configure the following SNMP settings.
 - **Trap Address:** IP Address of SNMP host.
 - **Trap Port:** Port of SNMP host.
5. Click the **Apply** button to save and exit the interface.



Before setting the SNMP, please download the SNMP software and manage to receive the device information via SNMP port. By setting the Trap Address, the NVR is allowed to send the alarm event and exception message to the surveillance center.

11.2.6 Configuring Remote Alarm Host

Purpose:

With a remote alarm host configured, the NVR will send the alarm event or exception message to the host when an alarm is triggered. The remote alarm host must have the Network Video Surveillance software installed.

Steps:

1. Enter the Network Settings interface.
Menu > Configuration > Network
2. Select the **More Settings** tab to enter the More Settings interface, as shown in Figure 11. 16.

Alarm Host IP	
Alarm Host Port	0
Server Port	8000
HTTP Port	80
Multicast IP	
RTSP Port	554
Enable High-speed Dow...	<input type="checkbox"/>

Figure 11. 16 More Settings Interface

3. Enter **Alarm Host IP** and **Alarm Host Port** in the text fields.

The **Alarm Host IP** refers to the IP address of the remote PC on which the Network Video Surveillance Software (e.g., iVMS-4200) is installed, and the **Alarm Host Port** must be the same as the alarm monitoring port configured in the software.

4. Click the **Apply** button to save and exit the interface.

11.2.7 Configuring Multicast

Purpose:

The multicast can be configured to realize live view for more than 128 connections through network for the device. A multicast address spans the Class-D IP range of 224.0.0.0 to 239.255.255.255. It is recommended to use the IP address ranging from 239.252.0.0 to 239.255.255.255.

Steps:

1. Enter the Network Settings interface.
Menu > Configuration > Network
2. Select the **More Settings** tab to enter the More Settings interface, as shown in Figure 11. 16.
3. Set **Multicast IP**, as shown in Figure 11. 17. When adding a device to the Network Video Surveillance Software, the multicast address must be the same as the NVR's multicast IP.

Server Port	8000
HTTP Port	80
Multicast IP	239.221.2.78

Figure 11. 17 Configure Multicast

4. Click the **Apply** button to save and exit the interface.



The multicast function should be supported by the network switch to which the NVR is connected.

11.2.8 Configuring RTSP

Purpose:

The RTSP (Real Time Streaming Protocol) is a network control protocol designed for use in communication systems to control streaming media servers.

Steps:

1. Enter the Network Settings menu
Menu >Configuration> Network
2. Select the **More Settings** tab to enter the More Settings menu, as shown in Figure 11. 16.

RTSP Port	554
-----------	-----

Figure 11. 18 RTSP Settings Interface

3. Enter the RTSP port in the text field of **RTSP Service Port**. The default RTSP port is 554, and you can change it according to different requirements.
4. Click the **Apply** button to save and exit the menu.

11.2.9 Configuring Server and HTTP Ports

Purpose:

You can change the server and HTTP ports in the Network Settings menu. The default server port is 8000 and the default HTTP port is 80.

Steps:

1. Enter the Network Settings interface.
Menu >Configuration> Network
2. Select the **More Settings** tab to enter the More Settings interface, as shown in Figure 11. 16.
3. Enter new **Server Port** and **HTTP Port**.

Server Port	8000
HTTP Port	80
Multicast IP	239.221.2.78

Figure 11. 19 Host/Others Settings Menu

4. Enter the Server Port and HTTP Port in the text fields. The default Server Port is 8000 and the HTTP Port is 80, and you can change them according to different requirements.
5. Click the **Apply** button to save and exit the interface.



The Server Port should be set to the range of 2000-65535 and it is used for remote client software access. The HTTP port is used for remote web browser access.

11.2.10 Configuring Email

Purpose:

The system can be configured to send an Email notification to all designated users if an alarm event is detected, etc., an alarm or motion event is detected or the administrator password is changed.

Before configuring the Email settings, the NVR must be connected to a local area network (LAN) that maintains an SMTP mail server. The network must also be connected to either an intranet or the Internet depending on the location of the e-mail accounts to which you want to send notification.

Steps:

1. Enter the Network Settings interface.
Menu > Configuration > Network
2. Set the IPv4 Address, IPv4 Subnet Mask, IPv4 Gateway and the Preferred DNS Server in the Network Settings menu, as shown in Figure 11. 20.

NIC Type	10M/100M/1000M Self-adaptive		
Enable DHCP	<input type="checkbox"/>		
IPv4 Address	10 .16 .1 .20	IPv6 Address	fe80::c256:e3ff:fe21:86e7/64
IPv4 Subnet	255 .255 .255 .0	IPv6 Address	
IPv4 Default	192 .168 .254 .1	IPv6 Default	
MAC Address	c0:56:e3:21:86:e7		
MTU(Bytes)	1500		
Preferred DNS Server	192.168.254.1		
Alternate DNS Server			

Figure 11. 20 Network Settings Interface

3. Click **Apply** to save the settings.
4. Select the Email tab to enter the Email Settings interface.

Enable Se...	<input type="checkbox"/>	SMTP Ser...	
User Name		SMTP Port	25
Password		Enable SSL	<input type="checkbox"/>
Sender			
Sender's Address			
Select Receivers	Receiver 1		
Receiver			
Receiver's Address			
Enable Attached Picture	<input type="checkbox"/>		
Interval	2s		

Figure 11. 21 Email Settings Interface

5. Configure the following Email settings:
 - Enable Server Authentication (optional):** Check the checkbox to enable the server authentication feature.
 - User Name:** The user account of sender's Email for SMTP server authentication.
 - Password:** The password of sender's Email for SMTP server authentication.
 - SMTP Server:** The SMTP Server IP address or host name (e.g., smtp.263xmail.com).
 - SMTP Port No.:** The SMTP port. The default TCP/IP port used for SMTP is 25.
 - Enable SSL (optional):** Click the checkbox to enable SSL if required by the SMTP server.
 - Sender:** The name of sender.
 - Sender's Address:** The Email address of sender.
 - Select Receivers:** Select the receiver. Up to 3 receivers can be configured.
 - Receiver:** The name of user to be notified.
 - Receiver's Address:** The Email address of user to be notified.
 - Enable Attached Pictures:** Check the checkbox of **Enable Attached Picture** if you want to send email with attached alarm images. The interval is the time of two adjacent alarm images. You can also set SMTP port and enable SSL here.

Interval: The interval refers to the time between two actions of sending attached pictures.

E-mail Test: Sends a test message to verify that the SMTP server can be reached.

6. Click **Apply** button to save the Email settings.
7. You can click **Test** button to test whether your Email settings work. The corresponding Attention message box will pop up. Refer to Figure 11. 22.

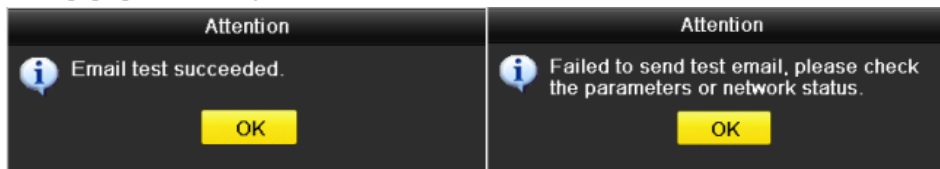


Figure 11. 22 Email Testing Attention

11.2.11 Configuring NAT

Purpose:

Two ways are provided for port mapping to realize the remote access via the cross-segment network, UPnP™ and manual mapping.

UPnP™

Universal Plug and Play (UPnP™) can permit the device seamlessly discover the presence of other network devices on the network and establish functional network services for data sharing, communications, etc. You can use the UPnP™ function to enable the fast connection of the device to the WAN via a router without port mapping.

Before you start:

If you want to enable the UPnP™ function of the device, you must enable the UPnP™ function of the router to which your device is connected. When the network working mode of the device is set as multi-address, the Default Route of the device should be in the same network segment as that of the LAN IP address of the router.

Steps:

1. Enter the Network Settings interface.
Menu > Configuration > Network
2. Select the **NAT** tab to enter the port mapping interface.

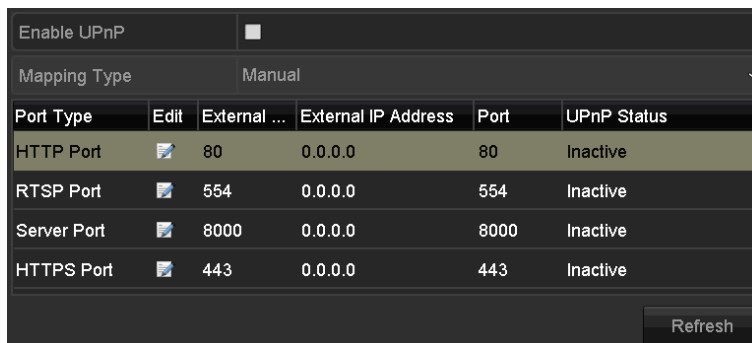


Figure 11. 23 UPnP™ Settings Interface

3. Check ☒ checkbox to enable UPnP™.
4. Select the Mapping Type as Manual or Auto in the drop-down list.

OPTION 1: Auto

If you select Auto, the Port Mapping items are read-only, and the external ports are set by the router

automatically.

Steps:

- 1) Select **Auto** in the drop-down list of Mapping Type.
- 2) Click **Apply** button to save the settings.
- 3) You can click **Refresh** button to get the latest status of the port mapping.

Port Type	Edit	External ...	External IP Address	Port	UPnP Status
HTTP Port		80	0.0.0.0	80	Active
RTSP Port		554	0.0.0.0	554	Active
Server Port		8000	0.0.0.0	8000	Active
HTTPS Port		443	0.0.0.0	443	Active

Figure 11. 24 UPnP™ Settings Finished-Auto

OPTION 2: Manual

If you select Manual as the mapping type, you can edit the external port on your demand by clicking to activate the External Port Settings dialog box.

Steps:

- 1) Select **Manual** in the drop-down list of Mapping Type.
- 2) Click to activate the External Port Settings dialog box. Configure the external port No. for server port, http port, RTSP port and https port respectively.



You can use the default port No., or change it according to actual requirements.

External Port indicates the port No. for port mapping in the router.

The value of the RTSP port No. should be 554 or between 1024 and 65535, while the value of the other ports should be between 1 and 65535 and the value must be different from each other. If multiple devices are configured for the UPnP™ settings under the same router, the value of the port No. for each device should be unique.

Figure 11. 25 External Port Settings Dialog Box

- 3) Click **Apply** button to save the settings.
- 4) You can click **Refresh** button to get the latest status of the port mapping.

Enable UPnP	<input checked="" type="checkbox"/>				
Mapping Type	Manual				
Port Type	Edit	External ...	External IP Address	Port	UPnP Status
HTTP Port		80	0.0.0.0	80	Active
RTSP Port		554	0.0.0.0	554	Active
Server Port		8000	0.0.0.0	8000	Active
HTTPS Port		443	0.0.0.0	443	Active
					Refresh

Figure 11. 26 UPnP™ Settings Finished-Manual

Manual Mapping

If your router does not support the UPnP™ function, perform the following steps to map the port manually in an easy way.

Before you start:

Make sure the router support the configuration of internal port and external port in the interface of Forwarding.

Steps:

1. Enter the Network Settings interface.
Menu > Configuration > Network
2. Select the **NAT** tab to enter the port mapping interface.
3. Leave the Enable UPnP checkbox unchecked.
4. Click to activate the External Port Settings dialog box. Configure the external port No. for server port, http port, RTSP port and https port respectively.



The value of the RTSP port No. should be 554 or between 1024 and 65535, while the value of the other ports should be between 1 and 65535 and the value must be different from each other. If multiple devices are configured for the UPnP™ settings under the same router, the value of the port No. for each device should be unique.

External Port Settings

Port Type	HTTP Port
External Port	81

OK
Cancel

Figure 11. 27 External Port Settings Dialog Box

5. Click **OK** to save the setting for the current port and return to the upper-level menu.
6. Click **Apply** button to save the settings.
7. Enter the virtual server setting page of router; fill in the blank of Internal Source Port with the internal port value, the blank of External Source Port with the external port value, and other required contents.



Each item should be corresponding with the device port, including Server Port, HTTP Port, RTSP Port and HTTPS

Port.

Delete	External Source Port	Protocol	Internal Source IP	Internal Source Port	Application
<input type="checkbox"/>	81	TCP	192.168.251.101	80	HTTP

Figure 11. 28 Setting Virtual Server Item



The above virtual server setting interface is for reference only, it may be different due to different router manufactures. Please contact the manufacture of router if you have any problems with setting virtual server.

11.3 Checking Network Traffic

Purpose:

You can check the network traffic to obtain real-time information of NVR such as linking status, MTU, sending/receiving rate, etc.

Steps:

1. Enter the Network Traffic interface.

Menu > Maintenance > Net Detect

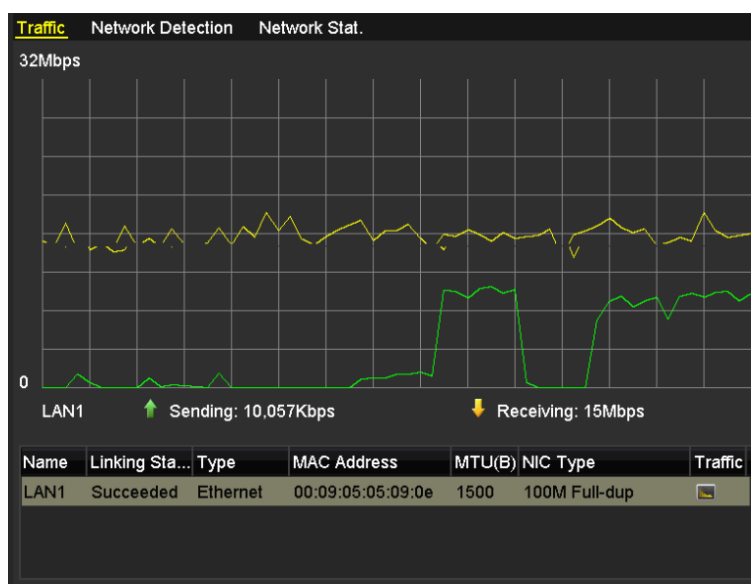


Figure 11. 29 Network Traffic Interface

2. You can view the sending rate and receiving rate information on the interface. The traffic data is refreshed every 1 second.

11.4 Configuring Network Detection

Purpose:

You can obtain network connecting status of NVR through the network detection function, including network delay, packet loss, etc.

11.4.1 Testing Network Delay and Packet Loss

Steps:

1. Enter the Network Traffic interface.
Menu >Maintenance>Net Detect
2. Click the **Network Detection** tab to enter the Network Detection menu, as shown in Figure 11. 30.

The screenshot shows the 'Network Detection' tab selected. It contains a 'Network Delay, Packet Loss Test' section with a 'Select NIC' dropdown set to 'LAN1' and a 'Destination Address' text field containing '10.16.1.19'. To the right is a 'Test' button. Below this is a 'Network Packet Export' section with a 'Device Name' dropdown set to 'USB Flash Disk 1-1' and a 'Refresh' button. At the bottom, there is a table showing 'LAN1' with '10.16.1.20' and '2.476Kbps', and an 'Export' button.

Figure 11. 30 Network Detection Interface

3. Enter the destination address in the text field of **Destination Address**.
4. Click **Test** button to start testing network delay and packet loss. The testing result pops up on the window. If the testing is failed, the error message box will pop up as well. Refer to Figure 11. 31.

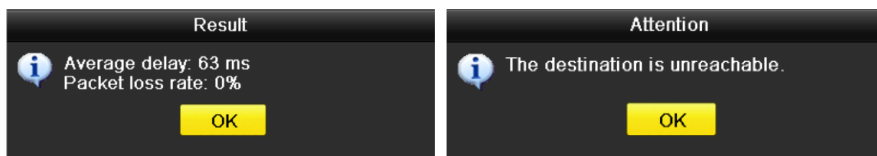


Figure 11. 31 Testing Result of Network Delay and Packet Loss

11.4.2 Exporting Network Packet

Purpose:

By connecting the NVR to network, the captured network data packet can be exported to USB-flash disk, SATA, DVD-R/W and other local backup devices.

Steps:

1. Enter the Network Traffic interface.
Menu >Maintenance>Net Detect
2. Click the **Network Detection** tab to enter the Network Detection interface.
3. Select the backup device from the drop-down list of Device Name, as shown in Figure 11. 32.



Click **Refresh** button if the connected local backup device cannot be displayed. When it fails to detect the backup device, please check whether it is compatible with the NVR. You can format the backup device if the format is incorrect.

Figure 11. 32 Export Network Packet

4. Click **Export** button to start exporting.
5. After the exporting is complete, click **OK** to finish the packet export, as shown in Figure 11. 33.

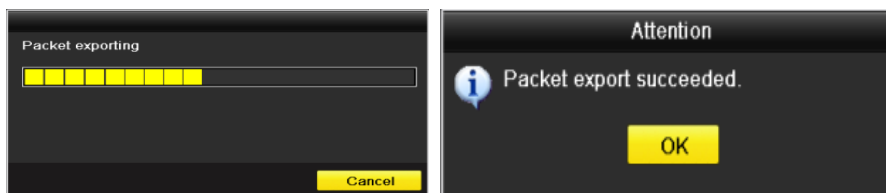


Figure 11. 33 Packet Export Attention



Up to 1M data can be exported each time.

11.4.3 Checking the Network Status

Purpose:

You can also check the network status and quick set the network parameters in this interface.

Step:

- Click the **Status** button on the lower- right corner of the page.

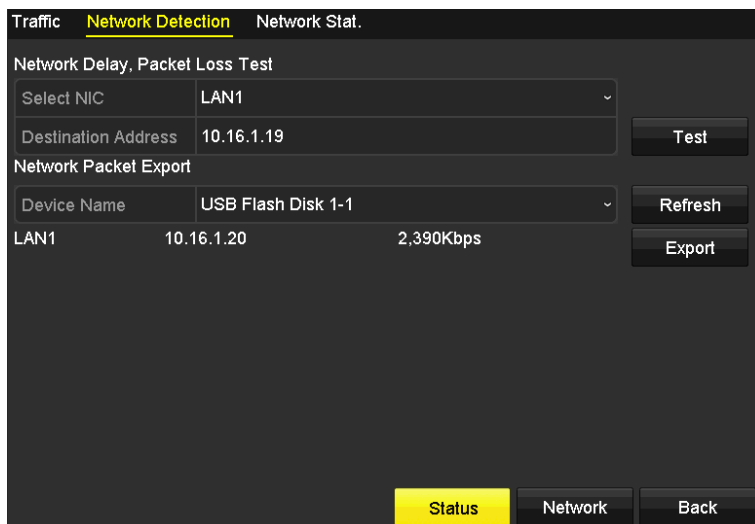


Figure 11. 34 Network Status Checking

If the network is normal the following message box pops out.

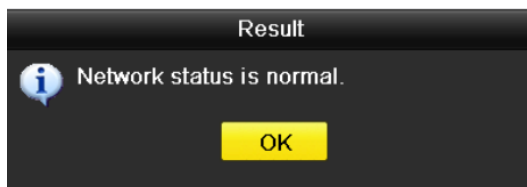


Figure 11. 35 Network status checking result

If the message box pops out with other information instead of this one, you can click **Network** button to show the quick setting interface of the network parameters.

11.4.4 Checking Network Statistics

Purpose:

You can check the network status to obtain the real-time information of NVR.

Steps:

1. Enter the Network Detection interface.
Menu > Maintenance > Net Detect
2. Choose the **Network Stat.** tab.

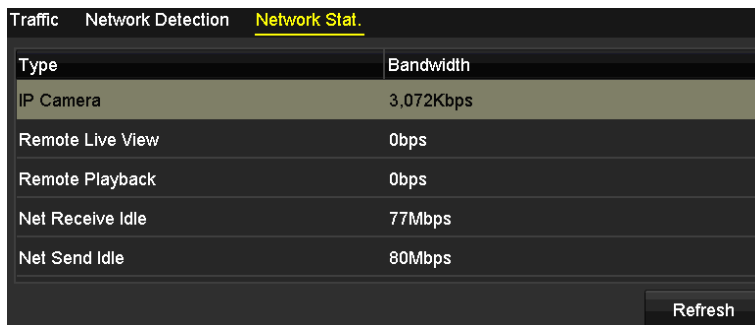


Figure 11. 36 Network Stat. Interface

3. Check the bandwidth of IP Camera, bandwidth of Remote Live View, bandwidth of Remote Playback, bandwidth of Net Receive Idle and bandwidth of Net Send Idle.
4. You can click **Refresh** to get the newest status.

Chapter 12 HDD Management

12.1 Initializing HDD

Purpose:

The hard disk drive (HDD) must be initialized before using it.



A message box pops up when the NVR starts up if there exists any uninitialized HDD.



Figure 12. 1 Message Box of Uninitialized HDD

Click **Yes** to initialize it immediately or you can perform the following steps to initialize the HDD.

Steps:

1. Enter the HDD Information interface.

Menu > HDD > General

HDD Information								
<input type="checkbox"/> L...	Capacity	Status	Property	Type	Free Space	Gr...	Edit	D...
<input checked="" type="checkbox"/> 1	931.51GB	Uninitialized	R/W	Local	0MB	1	-	-

Figure 12. 2 HDD Information Interface

2. Select HDD to be initialized.
3. Click the **Init** button.

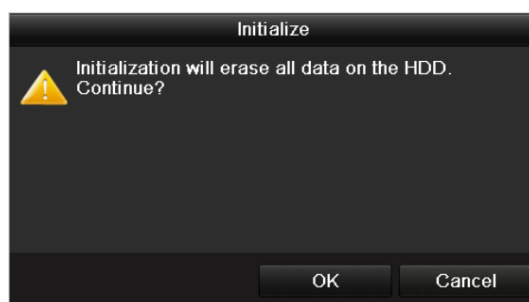


Figure 12. 3 Confirm Initialization

4. Select the **OK** button to start initialization.

HDD Information								
<input type="checkbox"/> L...	Capacity	Status	Property	Type	Free Space	Gr...	Edit	D...
<input checked="" type="checkbox"/> 1	931.51GB	Initializing 20%	R/W	Local	0MB	1	-	-

Figure 12. 4 Status changes to Initializing

5. After the HDD has been initialized, the status of the HDD will switch from *Uninitialized* to *Normal*.



L...	Capacity	Status	Property	Type	Free Space	Gr...	Edit	D...
1	931.51GB	Normal	R/W	Local	924GB	1	-	-

Figure 12. 5 HDD Status Changes to Normal



Initializing the HDD will erase all data on it.

12.2 Configuring Quota Mode

Purpose:

Each camera can be configured with allocated quota for the storage of recorded files.

Steps:

1. Enter the Storage Mode interface.

Menu > HDD > Advanced

Mode	Quota
Camera	[D1] Camera 01
Used Record Capacity	5120.00MB
Used Picture Capacity	0B
HDD Capacity (GB)	465
Max. Record Capacity (G...	0
Max. Picture Capacity (GB)	0
⚠ Free Quota Space 465 GB	

Figure 12. 6 Storage Mode Settings Interface

2. Select a **Camera** to configure quota parameters.
3. Input the capacity in the text fields of **Max. Record Capacity (GB)**.
4. Repeat the steps above to configure for other cameras.

Or copy the current camera settings to other cameras by clicking the **Copy** button to enter the Copy Camera menu, as shown in Figure 12. 7.



Figure 12. 7 Copy Settings to Other Camera(s)

5. Click the **OK** button to save the settings and back to the Storage Mode interface.
6. Click the **Apply** button to apply the settings.



If the quota capacity is set to 0, then all cameras will use the total capacity of HDD for record.

12.3 Checking HDD Status

Purpose:

You may check the status of the installed HDDs on NVR so as to take immediate check and maintenance in case of HDD failure.

Checking HDD Status in HDD Information Interface

Steps:

1. Enter the HDD Information interface.
Menu > HDD > General
2. Check the status of each HDD which is displayed on the list, as shown in Figure 12. 8.

HDD Information							
<input type="checkbox"/> L...	Capacity	Status	Property	Type	Free Space	Gr...	Edit D...
<input type="checkbox"/> 1	931.51GB	Normal	R/W	Local	924GB	1	- -

Figure 12. 8 View HDD Status (1)



If the status of HDD is *Normal*, it works normally. If the status is *Uninitialized* or *Abnormal*, please initialize the HDD before use. And if the HDD initialization is failed, please replace it with a new one.

Checking HDD Status in HDD Information Interface

Steps:

1. Enter the System Information interface.
Menu > Maintenance > System Info
2. Click the **HDD** tab to view the HDD status, as shown in Figure 12. 9.

Device Info						
Camera						
Record						
Alarm						
WAN						
WIFI						
LAN						
HDD						
Label	Status	Capacity	Free Space	Property	Type	Group
1	Normal	465.77GB	457.00GB	R/W	Local	1

Figure 12. 9 View HDD Status (2)


12.4 HDD Detection

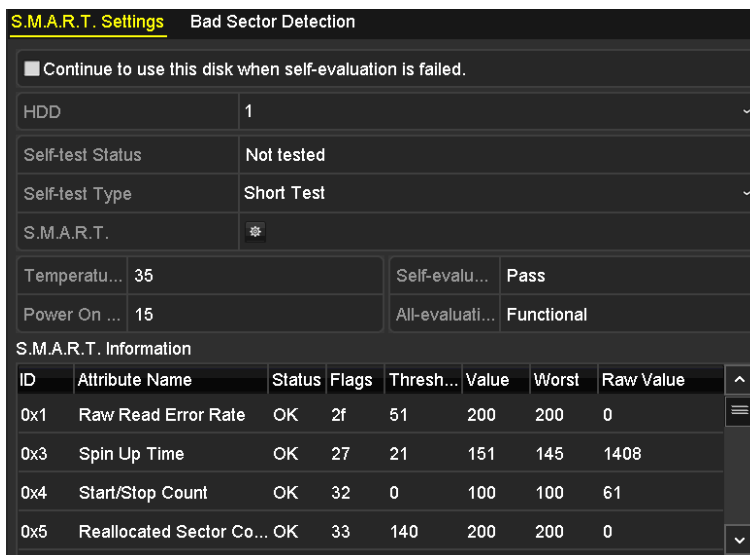
Purpose:

The device provides the HDD detection function such as the adopting of the S.M.A.R.T. and the Bad Sector Detection technique. The S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology) is a monitoring system for HDD to detect and report on various indicators of reliability in the hopes of anticipating failures.

S.M.A.R.T. Settings

Steps:

1. Enter the S.M.A.R.T Settings interface.
Menu > Maintenance > HDD Detect
2. Select the HDD to view its S.M.A.R.T information list, as shown in Figure 12. 10.
The related information of the S.M.A.R.T. is shown on the interface.
3. Test the HDD.
 - 1) Select the Self-test Type as Short Test, Expanded Test or the Conveyance Test.
 - 2) Click the  button to start the S.M.A.R.T. HDD self-evaluation.



ID	Attribute Name	Status	Flags	Thresh...	Value	Worst	Raw Value
0x1	Raw Read Error Rate	OK	2f	51	200	200	0
0x3	Spin Up Time	OK	27	21	151	145	1408
0x4	Start/Stop Count	OK	32	0	100	100	61
0x5	Reallocated Sector Co...	OK	33	140	200	200	0

Figure 12. 10 S.M.A.R.T Settings Interface



If you want to use the HDD even when the S.M.A.R.T. checking is failed, you can check the checkbox of the **Continue to use the disk when self-evaluation is failed** item.

Bad Sector Detection

Steps:

1. Click the **Bad Sector Detection** tab.
2. Select the **HDD No.** in the drop-down list.
3. Select the detection type as **Full Detection** or **Key Area Detection**.
4. Click **Detect** to start the detection.

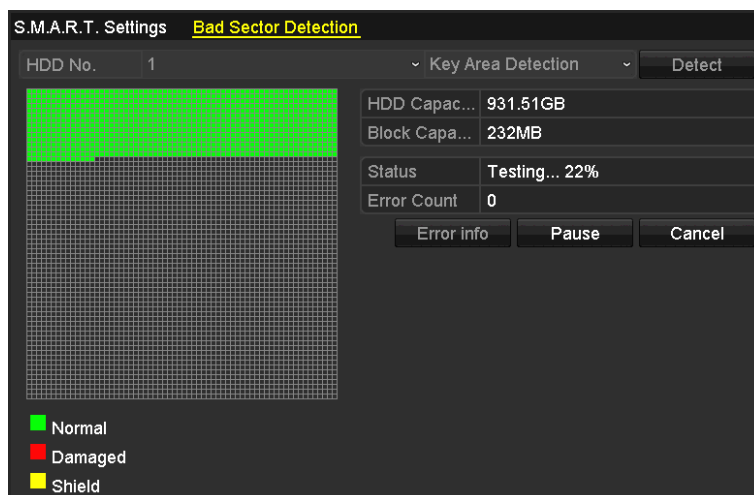


Figure 12. 11 Bad Sector Detection

5. Click **Pause** or **Cancel** to pause or cancel the detection.
6. Click **Error info** button to see the detailed damage information.

12.5 Configuring HDD Error Alarms

Purpose:

You can configure the HDD error alarms when the HDD status is uninitialized or abnormal.

Steps:

1. Enter the Exception interface.
Menu > Configuration > Exceptions
2. Select the Exception Type as **HDD Error**.
3. Click the checkbox(s) linkage action to set the HDD error alarm type (s), as shown in Figure 12. 12.



The alarm type can be selected as **Audible Warning**, **Notify Surveillance Center**, **Send Email** and **Trigger Alarm Output**. For details, please refer to section 8.5 *Handling Exceptions Alarm*.

Exception	
Enable Event Hint	<input checked="" type="checkbox"/>
Event Hint Settings	
Exception Type	HDD Error
Audible Warning	<input type="checkbox"/>
Notify Surveillance Center	<input type="checkbox"/>
Send Email	<input type="checkbox"/>
Trigger Alarm Output	<input checked="" type="checkbox"/>
<input type="checkbox"/> Alarm Output No.	Alarm Name
<input type="checkbox"/> 10.16.1.2:8000->1	
<input type="checkbox"/> 10.16.1.2:8000->2	

Figure 12. 12 Configure HDD Error Alarm

4. Click the **Apply** button to save the settings

Chapter 13 Camera Settings

13.1 Configuring OSD Settings

Purpose:

You can configure the OSD (On-screen Display) settings for the camera, including date /time, camera name, etc.

Steps:

1. Enter the OSD Configuration interface.
Menu > Camera > OSD
2. Select the **Camera** to configure.
3. Edit the **Camera Name** in the text field.
4. Enable the **Display Name**, **Display Date** and **Display Week** by checking the checkboxes.
5. Select the **Date Format**, **Time Format** and **Display Mode**.

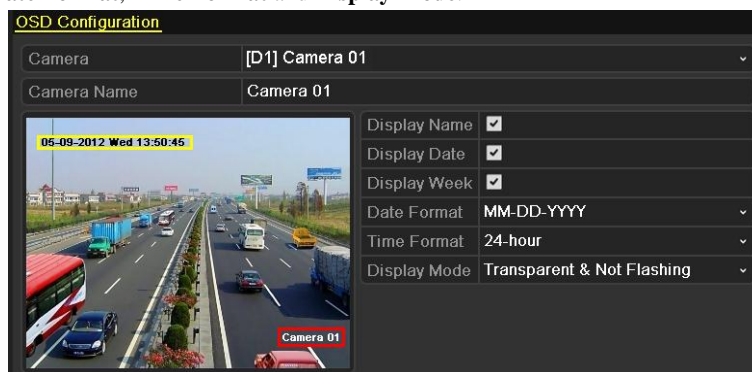


Figure 13. 1 OSD Configuration Interface

6. Adjust OSD position by using the mouse to drag the text frame on the preview window.
7. Click the **Apply** button to save the settings.

13.2 Configuring Privacy Mask

Purpose:

You are allowed to configure the four-sided privacy mask zones that cannot be viewed by the operator. The privacy mask can prevent certain surveillance areas to be viewed or recorded.

Steps:

1. Enter the Privacy Mask Settings interface.
Menu > Camera > Privacy Mask
2. Select the **Camera** to set privacy mask.
3. Check the checkbox of **Enable Privacy Mask** to enable this feature.



Figure 13. 2 Privacy Mask Settings Interface

4. Use the mouse to draw a zone on the window. The zones will be marked with different frame colors.



Up to 4 privacy mask zones can be configured and the size of each area can be adjusted.

5. The configured privacy mask zones on the window can be cleared by clicking the corresponding Clear Zone1-4 icons on the right side of the window, or click **Clear All** to clear all zones.

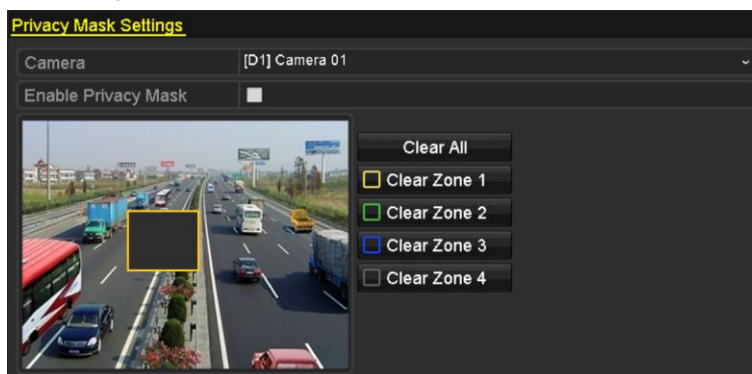


Figure 13. 3 Set Privacy Mask Area

6. Click the **Apply** button to save the settings.

13.3 Configuring Video Parameters


Steps:

1. Enter the Image Settings interface.

Menu > Camera > Image



Figure 13. 4 Image Settings Interface

2. Select the **Camera** to set image parameters.
3. Click the  icon or drag the scroll bar to change the value of each parameter.
4. Click the **Apply** button to save the settings.

Chapter 14 NVR Management and Maintenance

14.1 Viewing System Information

14.1.1 Viewing Device Information

Steps:

1. Enter the System Information interface.
Menu > Maintenance > System Info
2. Click the **Device Info**, **Camera**, **Record**, **Alarm**, **WAN**, **WIFI**, **LAN** or **HDD** tabs to view the system information of the device.



Figure 14. 1 Device Information Interface

14.2 Searching & Export Log Files

Purpose:

The operation, alarm, exception and information of the NVR can be stored in log files, which can be viewed and exported at any time.

Steps:

1. Enter the Log Search interface.

Menu > Maintenance > Log Information

The screenshot shows the 'Log Search' interface. At the top, there are fields for 'Start Time' (04-21-2015 00:00:00) and 'End Time' (04-21-2015 23:59:59). Below these is a 'Major Type' dropdown set to 'All'. A section titled 'Minor Type' contains a list of checkboxes, all of which are checked: Alarm Input, Alarm Output, Motion Detection Started, Motion Detection Stopped, Video Tampering Detection Started, Video Tampering Detection Stopped, Line Crossing Detection Alarm Started, Line Crossing Detection Alarm Stopped, and Intrusion Detection Alarm Started. At the bottom right, there are three buttons: 'Export All', 'Search', and 'Back'.

Figure 14. 2 Log Search Interface

2. Set the search conditions to refine your search, including the **Start Time**, **End Time**, **Major Type** and **Minor Type**.
3. Click **Search** to start search log files.
4. The matched log files will be displayed on the list shown below.

Search Result						
No.	Major Type	Time	Minor Type	Parameter	Play	Details
1	Information	04-21-2015 00:00:02	System Running...	N/A	—	✓
2	Information	04-21-2015 00:00:12	System Running...	N/A	—	✓
3	Information	04-21-2015 00:10:12	System Running...	N/A	—	✓
4	Information	04-21-2015 00:10:22	System Running...	N/A	—	✓
5	Information	04-21-2015 00:20:22	System Running...	N/A	—	✓
6	Information	04-21-2015 00:20:32	System Running...	N/A	—	✓
7	Information	04-21-2015 00:30:32	System Running...	N/A	—	✓
8	Information	04-21-2015 00:30:43	System Running...	N/A	—	✓
9	Information	04-21-2015 00:40:42	System Running...	N/A	—	✓
10	Information	04-21-2015 00:40:52	System Running...	N/A	—	✓
Total: 434 P: 1/5						
					Export	Back

Figure 14. 3 Log Search Results



Up to 2000 log files can be displayed each time.

- Click the button or double click a log to view its detailed information, as shown in Figure 14. 4. And you can also click the button to view the related video files if available.

Log Information	
Time	11-21-2014 16:29:31
Type	Operation--Local Operation: Initialize HDD
Local User	admin
Host IP Address	N/A
Parameter Type	N/A
HDD	1
Description:	
User admin Initialized the No.1 HDD Initialization status: Succeeded	
<div>Previous</div> <div>Next</div> <div>OK</div>	

Figure 14. 4 Log Details

- If you want to export the log files, click **Export** to enter the Export menu, as shown in Figure 14. 5.



Figure 14. 5 Export Log Files

7. Select the backup device from the drop-down list of **Device Name**.
8. Click the **Export** to export the log files to the selected backup device.
You can click the **New Folder** button to create new folder in the backup device, or click the **Format** button to format the backup device before log export.



Please connect the backup device to NVR before operating log export.

The log files exported to the backup device are named by exporting time, e.g.,
20110514124841logBack.txt.

To export all the log files:

Steps:

1. Enter the Log Information interface.
Menu > Maintenance > Log Information
2. Click the **Export All** to export all the log files stored in the HDD.

14.3 Importing/Exporting IP Camera Info

Purpose:

The information of added IP camera, including the IP address, manage port, password of admin, etc., can be generated into an excel file and the file can be exported to the backup device. And the exported file can be edited on your PC, like adding or deleting the content.

Steps:

1. Enter the camera management interface.

Menu > Camera > IP Camera Import/Export

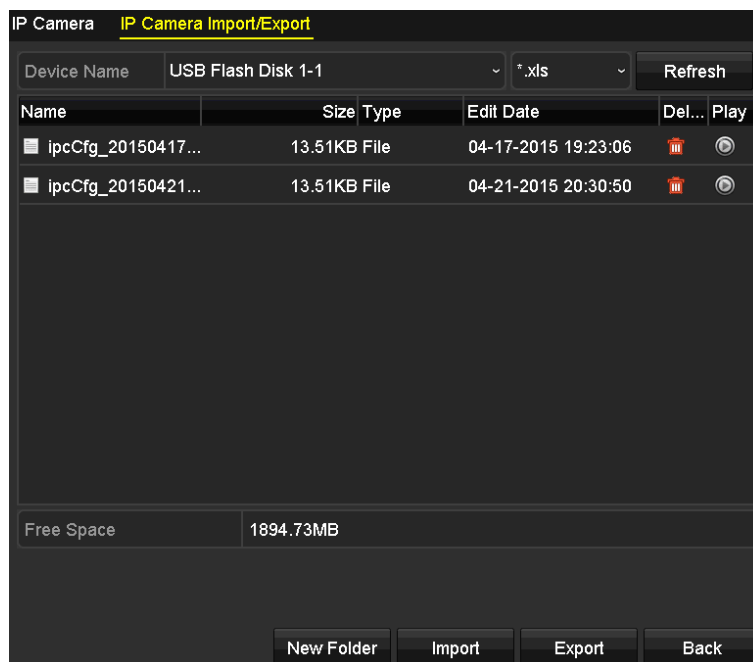


Figure 14. 6 IP Camera Import/Export Interface

2. Click the **IP Camera Import/Export** tab, the content of detected plugged external device appears.
3. Select **Device Name** and **File Type** you want to show in respective dropdown lists.



The default File Type is ***.xls**.

4. Click **Export** to export configuration files to the selected local backup device.
5. To import a configuration file, select the file from the selected backup device and click **Import**.

14.4 Importing/Exporting Configuration Files

Purpose:

The configuration files of the NVR can be exported to local backup device; and the configuration files of one NVR can be imported to multiple NVR devices if they are to be configured with the same parameters.

Steps:

1. Enter the Import/Export Configuration File interface.

Menu > Maintenance > Import/Export



Figure 14. 7 Import/Export Config File

2. Select **Device Name** and **File Type** you want to show in respective dropdown lists.



The default File Type is ***.bin**.

3. Click **Export** to export configuration files to the selected local backup device.
4. To import a configuration file, select the file from the selected backup device and click the **Import** button.

After the import process is completed, you must reboot the NVR.



After having finished the import of configuration files, the device will reboot automatically.

14.5 Upgrading System

Purpose:

The firmware on your NVR can be upgraded by local backup device or remote FTP server.

14.5.1 Upgrading by Local Backup Device

Before you start:

Connect your NVR with a local backup device where the update firmware file is located.

Steps:

1. Enter the Upgrade interface.
Menu > Maintenance > Upgrade
2. Click the **Local Upgrade** tab to enter the local upgrade menu, as shown in Figure 14. 8.

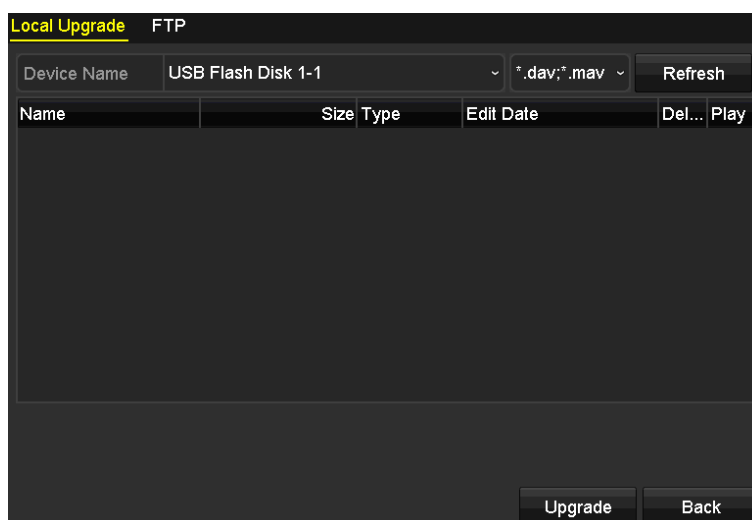


Figure 14. 8 Local Upgrade Interface

3. Select **Device Name** and **File Type** you want to show in respective dropdown lists.



The default File Type is ***.dav** and ***.mav**.

4. Click to select the update file in the backup device.
5. Click **Upgrade** to start upgrading.
6. After the upgrading is complete, reboot the NVR to activate the new firmware.

14.5.2 Upgrading by FTP

Purpose:

Ensure the network connection of the PC (running FTP server) and the device is valid and correct. Run the FTP server on the PC and copy the firmware into the corresponding directory of your PC.



Refer to the user manual of the FTP server to set the FTP server on your PC and put the firmware file into the directory as required.

Steps:

1. Enter the Upgrade interface.
Menu > Maintenance > Upgrade
2. Click the **FTP** tab to enter the local upgrade interface, as shown in Figure 14. 9.



Figure 14. 9 FTP Upgrade Interface

3. Input the **FTP Server Address** in the text field.
4. Click **Upgrade** to start upgrading.
5. After the upgrading is complete, reboot the NVR to activate the new firmware.

14.6 Restoring Default Settings

Steps:

1. Enter the Default interface.

Menu > Maintenance > Default

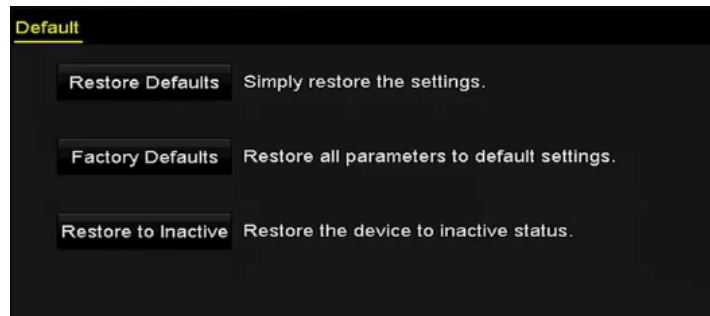


Figure 14. 10 Restore Defaults

2. Select the restoring type from the following three options.

Restore Defaults: Restore all parameters, except the network (including IP address, subnet mask, gateway, MTU, NIC working mode, default route, server port, etc.) and user account parameters, to the factory default settings.

Factory Defaults: Restore all parameters to the factory default settings.

Restore to Inactive: Restore the device to the inactive status.

3. Click the **OK** button to restore the default settings.



The device will reboot automatically after restoring to the default settings.

Chapter 15 Others

15.1 Configuring General Settings

Purpose:

You can configure the output resolution, mouse pointer speed, etc..

Steps:

1. Enter the General Settings interface.
Menu > Configuration > General
2. Select the **General** tab.

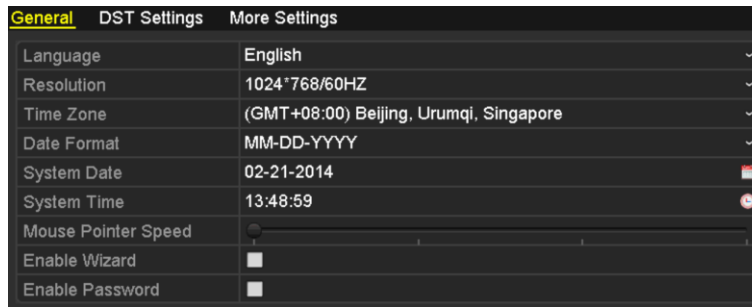


Figure 15. 1 General Settings Interface

3. Configure the following settings:
 - **Language:** The default language used is *English*.
 - **Resolution:** Select the resolution for the video output, which must be the same with the resolution of the monitor screen.
 - **Time Zone:** Select the time zone.
 - **Date Format:** Select the date format.
 - **System Date:** Select the system date.
 - **System Time:** Select the system time.
 - **Mouse Pointer Speed:** Set the speed of mouse pointer; 4 levels are configurable.
 - **Enable Wizard:** Enable/disable the Wizard when the device starts up.
 - **Enable Password:** Enable/disable the use of the login password.
4. Click the **Apply** button to save the settings.

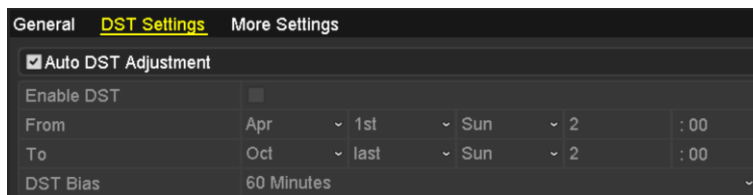
15.2 Configuring DST Settings

Steps:

1. Enter the General Settings interface.

Menu > Configuration > General

2. Choose **DST Settings** tab.



General		DST Settings		More Settings	
<input checked="" type="checkbox"/> Auto DST Adjustment					
Enable DST <input type="checkbox"/>					
From	Apr	1st	Sun	2	:00
To	Oct	last	Sun	2	:00
DST Bias	60 Minutes				

Figure 15. 2 DST Settings Interface

3. Check the checkbox of **Auto DST Adjustment** item.

Or you can manually check the **Enable DST** checkbox, and then you choose the date of the DST period.

15.3 Configuring More Settings for NVR

Steps:

1. Enter the General Settings interface.
Menu > Configuration > General
2. Click the **More Settings** tab to enter the More Settings interface, as shown in Figure 15. 3.

General	DST Settings	<u>More Settings</u>
Device Name	Network Video Recorder	
Device No.	255	
Auto Logout	Never	

Figure 15. 3 More Settings Interface

3. Configure the following settings:
 - **Device Name:** Edit the name of NVR.
 - **Device No.:** The No. is used for the remote and keyboard control. The Device No. can be set in the range of 1~255, and the default No. is 255.
 - **Auto Logout:** Specify timeout for menu inactivity. E.g., when it is set to *5 Minutes*, then the system will exit from the current operation menu to live view after 5 minutes of menu inactivity.
4. Click the **Apply** button to save the settings.

15.4 Managing User Accounts

Purpose:

There is a default account in the NVR: *Administrator*. The *Administrator* user name is *admin* and the password is set when you start the device for the first time. The *Administrator* has the permission to add and delete user and configure user parameters.

15.4.1 Adding a User

Steps:

1. Enter the User Management interface.

Menu >Configuration>User

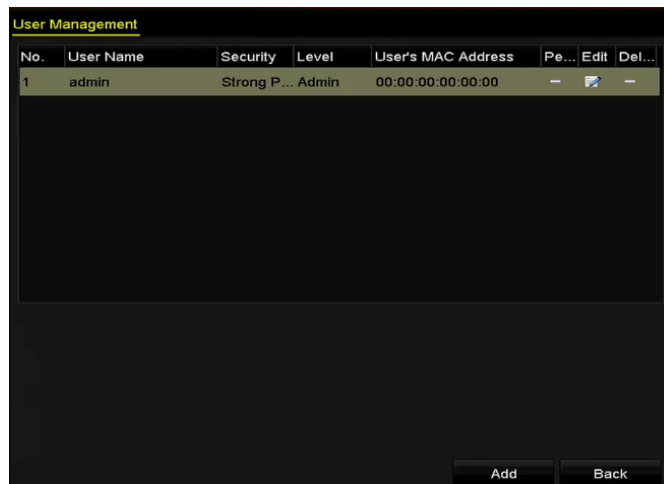


Figure 15. 4 User Management Interface

2. Click the **Add** button to enter the Add User interface.

Add User

User Name	example1
Password	***** Strong
Confirm	*****
Level	Operator
User's MAC Address	00 :00 :00 :00 :00 :00

✓ Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.

OK Cancel

Figure 15. 5 Add User Menu

3. Enter the information for new user, including **User Name**, **Password**, **Confirm**, **Level** and **User's MAC**

Address.

Password: Set the password for the user account.



STRONG PASSWORD RECOMMENDED– We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Level: Set the user level to Operator or Guest. Different user levels have different operating permission.

- **Operator:** The *Operator* user level has permission of Two-way Audio in Remote Configuration and all operating permission in Camera Configuration by default.
- **Guest:** The *Guest* user has no permission of Two-way Audio in Remote Configuration and only has the local/remote playback in the Camera Configuration by default.

User's MAC Address: The MAC address of the remote PC which logs onto the NVR. If it is configured and enabled, it only allows the remote user with this MAC address to access the NVR.

4. Click the **OK** button to save the settings and go back to the User Management interface. The added new user will be displayed on the list, as shown in Figure 15. 6.

No.	User Name	Level	User's MAC Address	Pe...	Edit	Del...
1	admin	Admin	00:00:00:00:00:00	—		—
2	01	Operator	00:00:00:00:00:00			

Figure 15. 6 Added User Listed in User Management Interface

5. Select the user from the list and then click the button to enter the Permission settings interface, as shown in Figure 15. 7.

Permission

Local Configuration Remote Configuration Camera Configuration

☒ Local Log Search
☐ Local Parameters Settings
☐ Local Camera Management
☐ Local Advanced Operation
☐ Local Shutdown / Reboot

Figure 15. 7 User Permission Settings Interface

6. Set the operating permission of Local Configuration, Remote Configuration and Camera Configuration for the user.

Local Configuration

- Local Log Search: Searching and viewing logs and system information of NVR.
- Local Parameters Settings: Configuring parameters, restoring factory default parameters and importing/exporting configuration files.
- Local Camera Management: The adding, deleting and editing of IP cameras.
- Local Advanced Operation: Operating HDD management (initializing HDD, setting HDD property), upgrading system firmware, clearing I/O alarm output.
- Local Shutdown Reboot: Shutting down or rebooting the NVR.

Remote Configuration

- Remote Log Search: Remotely viewing logs that are saved on the NVR.
- Remote Parameters Settings: Remotely configuring parameters, restoring factory default parameters and importing/exporting configuration files.
- Remote Camera Management: Remote adding, deleting and editing of the IP cameras.
- Remote Serial Port Control: Configuring settings for RS-232 and RS-485 ports.
- Remote Video Output Control: Sending remote button control signal.
- Two-Way Audio: Realizing two-way radio between the remote client and the NVR.
- Remote Alarm Control: Remotely arming (notify alarm and exception message to the remote client) and controlling the alarm output.
- Remote Advanced Operation: Remotely operating HDD management (initializing HDD, setting HDD property), upgrading system firmware, clearing I/O alarm output.
- Remote Shutdown/Reboot: Remotely shutting down or rebooting the NVR.

Camera Configuration

- Remote Live View: Remotely viewing live video of the selected camera (s).
- Local Manual Operation: Locally starting/stopping manual recording and alarm output of the selected camera (s).
- Remote Manual Operation: Remotely starting/stopping manual recording and alarm output of the selected camera (s).
- Local Playback: Locally playing back recorded files of the selected camera (s).
- Remote Playback: Remotely playing back recorded files of the selected camera (s).
- Local PTZ Control: Locally controlling PTZ movement of the selected camera (s).
- Remote PTZ Control: Remotely controlling PTZ movement of the selected camera (s).
- Local Video Export: Locally exporting recorded files of the selected camera (s).

7. Click the **OK** button to save the settings and exit interface.



Only the *admin* user account has the permission of restoring factory default parameters.

15.4.2 Deleting a User

Steps:

1. Enter the User Management interface.
Menu > Configuration > User
2. Select the user to be deleted from the list, as shown in Figure 15. 8.

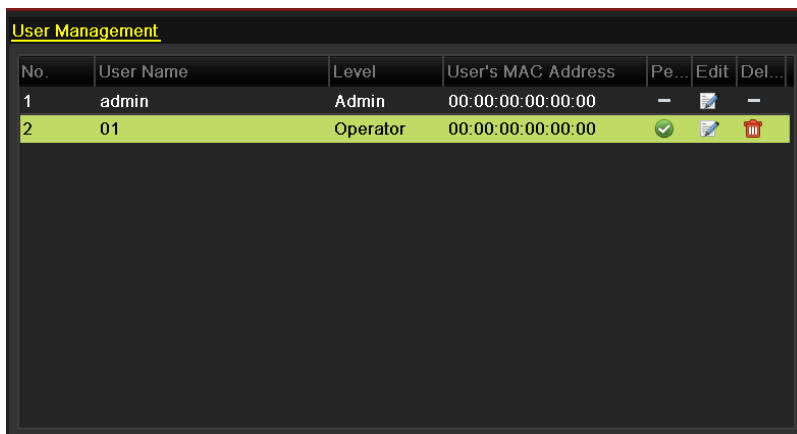


Figure 15. 8 User List

3. Click the icon to delete the selected user account.

15.4.3 Editing a User

For the added user accounts, you can edit the parameters.

Steps:

1. Enter the User Management interface.
Menu > Configuration > User
2. Select the user to be edited from the list, as shown in Figure 15. 8.
3. Click the icon to enter the Edit User interface, as shown in Figure 15. 9.

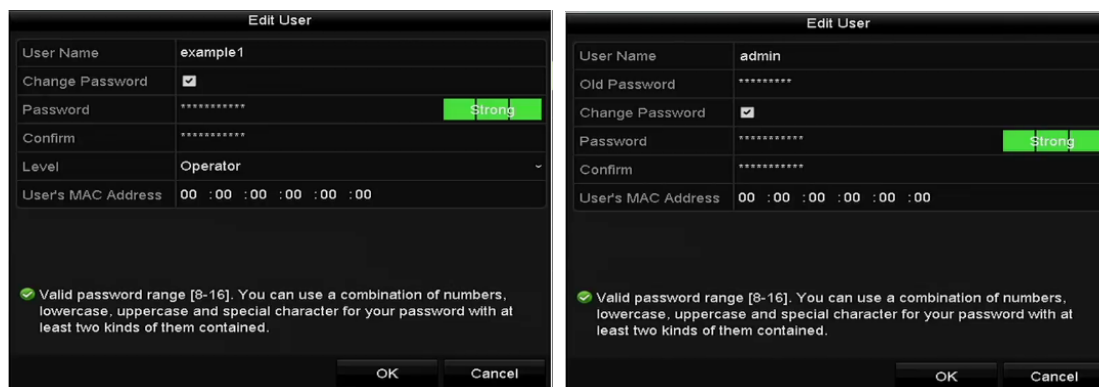



Figure 15. 9 Edit User Interface

4. Edit the corresponding parameters.
 - **Operator and Guest**
You can edit the user information, including user name, password, permission level and MAC address. Check the checkbox of **Change Password** if you want to change the password, and input the new password in the text field of **Password** and **Confirm**. A strong password is recommended.
 - **Admin**
You are only allowed to edit the password and MAC address. Check the checkbox of **Change Password** if you want to change the password, and the input the correct old password, and the new password in the text field of **Password** and **Confirm**.



STRONG PASSWORD RECOMMENDED– We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

5. Click the **OK** button to save the settings and exit the menu.
6. For the **Operator** or **Guest** user account, you can also click the  button on the user management interface to edit the permission.

Chapter 16 Appendix

16.1 Glossary

- **Dual Stream:** Dual stream is a technology used to record high resolution video locally while transmitting a lower resolution stream over the network. The two streams are generated by the DVR, with the main stream having a maximum resolution of 4CIF and the sub-stream having a maximum resolution of CIF.
- **HDD:** Acronym for Hard Disk Drive. A storage medium which stores digitally encoded data on platters with magnetic surfaces.
- **DHCP:** Dynamic Host Configuration Protocol (DHCP) is a network application protocol used by devices (DHCP clients) to obtain configuration information for operation in an Internet Protocol network.
- **HTTP:** Acronym for Hypertext Transfer Protocol. A protocol to transfer hypertext request and information between servers and browsers over a network
- **PPPoE:** PPPoE, Point-to-Point Protocol over Ethernet, is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with ADSL services where individual users connect to the ADSL transceiver (modem) over Ethernet and in plain Metro Ethernet networks.
- **DDNS:** Dynamic DNS is a method, protocol, or network service that provides the capability for a networked device, such as a router or computer system using the Internet Protocol Suite, to notify a domain name server to change, in real time (ad-hoc) the active DNS configuration of its configured hostnames, addresses or other information stored in DNS.
- **NTP:** Acronym for Network Time Protocol. A protocol designed to synchronize the clocks of computers over a network.
- **NVR:** Acronym for Network Video Recorder. An NVR can be a PC-based or embedded system used for centralized management and storage for IP cameras, IP Domes and other DVRs.
- **PTZ:** Acronym for Pan, Tilt, Zoom. PTZ cameras are motor driven systems that allow the camera to pan left and right, tilt up and down and zoom in and out.
- **USB:** Acronym for Universal Serial Bus. USB is a plug-and-play serial bus standard to interface devices to a host computer.

16.2 Troubleshooting

No image displayed on the monitor after starting up normally.

Possible Reasons

- a) No HDMI™ connections.
- b) Connection cable is damaged.
- c) Input mode of the monitor is incorrect.

Steps

1. Verify the device is connected with the monitor via HDMI™ cable.
If not, please connect the device with the monitor and reboot.
2. Verify the connection cable is good.
If there is still no image display on the monitor after rebooting, please check if the connection cable is good, and change a cable to connect again.
3. Verify Input mode of the monitor is correct.
Please check the input mode of the monitor matches with the output mode of the device (e.g. if the output mode of NVR is HDMI™ output, then the input mode of monitor must be the HDMI™ input). And if not, please modify the input mode of monitor.
4. Check if the fault is solved by the step 1 to step 3.
If it is solved, finish the process.
If not, please contact the engineer from our company to do the further process.

- **There is an audible warning sound “Di-Di-Di-Di” after a new bought NVR starts up.**

Possible Reasons

- a) The installed HDD has not been initialized.
- b) The installed HDD is not compatible with the NVR or is broken-down.

Steps

1. Verify the HDD is initialized.
 - 1) Select “Menu > HDD > General”.
 - 2) If the status of the HDD is “Uninitialized”, please check the checkbox of corresponding HDD and click the “Init” button.
2. Verify the HDD is detected or is in good condition.
 - 1) Select “Menu > HDD > General”.
 - 2) If the HDD is not detected or the status is “Abnormal”, please replace the dedicated HDD according to the requirement.
3. Check if the fault is solved by the step 1 to step 2.
If it is solved, finish the process.
If not, please contact the engineer from our company to do the further process.

- **The status of the added IP camera displays as “Disconnected” when it is connected through Private Protocol. Select “Menu > Camera > Camera” to get the camera status.**

Possible Reasons

- a) Network failure, and the NVR and IP camera lost connections.
- b) The configured parameters are incorrect when adding the IP camera.
- c) Insufficient bandwidth.

Steps

1. Verify the network is connected.
 - 1) Connect the NVR and PC with the RS-232 cable.

- 2) Open the Super Terminal software, and execute the ping command. Input “ping IP” (e.g. ping 172.6.22.131).



Simultaneously press **Ctrl** and **C** to exit the ping command.

If there exists return information and the time value is little, the network is normal.

2. Verify the configuration parameters are correct.
 - 1) Select “Menu > Camera > Camera”.
 - 2) Verify the following parameters are the same with those of the connected IP devices, including IP address, protocol, management port, user name and password.
3. Verify the whether the bandwidth is enough.
 - 1) Select “Menu > Maintenance > Net Detect > Network Stat.”.
 - 2) Check the usage of the access bandwidth, and see if the total bandwidth has reached its limit.
4. Check if the fault is solved by the step 1 to step 3.

If it is solved, finish the process.

If not, please contact the engineer from our company to do the further process.

- **The IP camera frequently goes online and offline and the status of it displays as “Disconnected”.**

Possible Reasons

- a) The IP camera and the NVR versions are not compatible.
- b) Unstable power supply of IP camera.
- c) Unstable network between IP camera and NVR.
- d) Limited flow by the switch connected with IP camera and NVR.

Steps

1. Verify the IP camera and the NVR versions are compatible.
 - 1) Enter the IP camera Management interface “Menu > Camera > Camera>IP Camera”, and view the firmware version of connected IP camera.
 - 2) Enter the System Info interface “Menu>Maintenance>System Info>Device Info”, and view the firmware version of NVR.
2. Verify power supply of IP camera is stable.
 - 1) Verify the power indicator is normal.
 - 2) When the IP camera is offline, please try the ping command on PC to check if the PC connects with the IP camera.
3. Verify the network between IP camera and NVR is stable.
 - 1) When the IP camera is offline, connect PC and NVR with the RS-232 cable.
 - 2) Open the Super Terminal, use the ping command and keep sending large data packages to the connected IP camera, and check if there exists packet loss.



Simultaneously press **Ctrl** and **C** to exit the ping command.

Example: Input **ping 172.6.22.131 -l 1472 -f**.

4. Verify the switch is not flow control.

Check the brand, model of the switch connecting IP camera and NVR, and contact with the manufacturer of the switch to check if it has the function of flow control. If so, please turn it down.
5. Check if the fault is solved by the step 1 to step 4.

If it is solved, finish the process.

If not, please contact the engineer from our company to do the further process.

No monitor connected with the NVR locally and when you manage the IP camera to connect with the device by web browser remotely, of which the status displays as Connected. And then you connect the

device with the monitor via HDMI™ interface and reboot the device, there is black screen with the mouse cursor.

Connect the NVR with the monitor before startup via HDMI™ interface, and manage the IP camera to connect with the device locally or remotely, the status of IP camera displays as Connect.

Possible Reasons:

After connecting the IP camera to the NVR, the image is output via the main spot interface by default.

Steps:

1. Enable the output channel.
2. Select “Menu > Configuration > Live View > View”, and select video output interface in the drop-down list and configure the window you want to view.



The view settings can only be configured by the local operation of NVR.

Different camera orders and window-division modes can be set for different output interfaces separately, and digits like “D1” and “D2” stands for the channel number, and “X” means the selected window has no image output.

3. Check if the fault is solved by the above steps.

If it is solved, finish the process.

If not, please contact the engineer from our company to do the further process.

Live view stuck when video output locally.

Possible Reasons:

- a) Poor network between NVR and IP camera, and there exists packet loss during the transmission.
- b) The frame rate has not reached the real-time frame rate.

Steps:

1. Verify the network between NVR and IP camera is connected.
 - 1) When image is stuck, connect the RS-232 ports on PC and the rear panel of NVR with the RS-232 cable.
 - 2) Open the Super Terminal, and execute the command of “**ping 192.168.0.0 -l 1472 -f**” (the IP address may change according to the real condition), and check if there exists packet loss.



Simultaneously press **Ctrl** and **C** to exit the ping command.

2. Verify the frame rate is real-time frame rate.

Select “Menu > Record > Parameters > Record”, and set the Frame rate to Full Frame.

3. Check if the fault is solved by the above steps.

If it is solved, finish the process.

If not, please contact the engineer from our company to do the further process.

Live view stuck when video output remotely via the Internet Explorer or platform software.

Possible Reasons:

- a) Poor network between NVR and IP camera, and there exists packet loss during the transmission.
- b) Poor network between NVR and PC, and there exists packet loss during the transmission.
- c) The performances of hardware are not good enough, including CPU, memory, etc..

Steps:

1. Verify the network between NVR and IP camera is connected.
 - 1) When image is stuck, connect the RS-232 ports on PC and the rear panel of NVR with the RS-232 cable.
 - 2) Open the Super Terminal, and execute the command of “**ping 192.168.0.0 -l 1472 -f**” (the IP address may change according to the real condition), and check if there exists packet loss.



Simultaneously press **Ctrl** and **C** to exit the ping command.

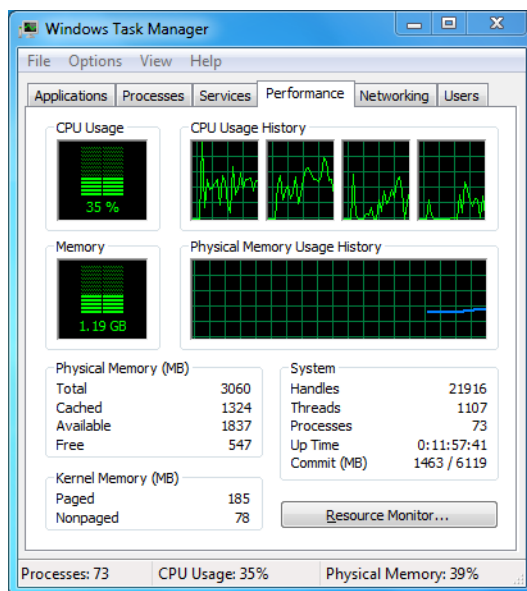
2. Verify the network between NVR and PC is connected.
 - 1) Open the cmd window in the Start menu, or you can press “windows+R” shortcut key to open it.
 - 2) Use the ping command to send large packet to the NVR, execute the command of “ping 192.168.0.0 -l 1472 -f” (the IP address may change according to the real condition), and check if there exists packet loss.



Simultaneously press **Ctrl** and **C** to exit the ping command.

3. Verify the hardware of the PC is good enough.

Simultaneously press **Ctrl**, **Alt** and **Delete** to enter the windows task management interface, as shown in the following figure.



Windows task management interface

Select the “Performance” tab; check the status of the CPU and Memory.

If the resource is not enough, please end some unnecessary processes.

4. Check if the fault is solved by the above steps.

If it is solved, finish the process.

If not, please contact the engineer from our company to do the further process.

When using the NVR to get the live view audio, there is no sound or there is too much noise, or the volume is too low.

Possible Reasons:

- a) Cable between the pickup and IP camera is not connected well; impedance mismatches or incompatible.
- b) The stream type is not set as “Video & Audio”.
- c) The encoding standard is not supported with NVR.

Steps:

1. Verify the cable between the pickup and IP camera is connected well; impedance matches and compatible.

Log in the IP camera directly, and turn the audio on, check if the sound is normal. If not, please contact the manufacturer of the IP camera.

2. Verify the setting parameters are correct.

Select “Menu > Record > Parameters > Record”, and set the Stream Type as “Audio & Video”.

3. Verify the audio encoding standard of the IP camera is supported by the NVR.

NVR supports G722.1 and G711 standards, and if the encoding parameter of the input audio is not one of the previous two standards, you can log in the IP camera to configure it to the supported standard.

4. Check if the fault is solved by the above steps.

If it is solved, finish the process.

If not, please contact the engineer from our company to do the further process.

The image gets stuck when NVR is playing back by single or multi-channel.

Possible Reasons:

- a) Poor network between NVR and IP camera, and there exists packet loss during the transmission.
- b) The frame rate is not the real-time frame rate.
- c) The NVR supports up to 16-channel synchronize playback at the resolution of 4CIF, if you want a 16-channel synchronize playback at the resolution of 720p, the frame extracting may occur, which leads to a slight stuck.

Steps:

1. Verify the network between NVR and IP camera is connected.
 - 1) When image is stuck, connect the RS-232 ports on PC and the rear panel of NVR with the RS-232 cable.
 - 2) Open the Super Terminal, and execute the command of “**ping 192.168.0.0 -l 1472 -f**” (the IP address may change according to the real condition), and check if there exists packet loss.



Simultaneously press the **Ctrl** and **C** to exit the ping command.

2. Verify the frame rate is real-time frame rate.

Select “Menu > Record > Parameters > Record”, and set the Frame Rate to “Full Frame”.
3. Verify the hardware can afford the playback.

Reduce the channel number of playback.
Select “Menu > Record > Encoding > Record”, and set the resolution and bitrate to a lower level.
4. Reduce the number of local playback channel.

Select “Menu > Playback”, and uncheck the checkbox of unnecessary channels.
5. Check if the fault is solved by the above steps.

If it is solved, finish the process.
If not, please contact the engineer from our company to do the further process.

No record file found in the NVR local HDD, and prompt “No record file found”.

Possible Reasons:

- a) The time setting of system is incorrect.
- b) The search condition is incorrect.
- c) The HDD is error or not detected.

Steps:

1. Verify the system time setting is correct.

Select “Menu > Configuration > General > General”, and verify the “Device Time” is correct.
2. Verify the search condition is correct.

Select “Playback”, and verify the channel and time are correct.
3. Verify the HDD status is normal.

Select “Menu > HDD > General” to view the HDD status, and verify the HDD is detected and can be read and written normally.

4. Check if the fault is solved by the above steps.

If it is solved, finish the process.

If not, please contact the engineer from our company to do the further process.

16.3 Summary of Changes

Version 3.3.0

Add

1. Add the new features. (Product Key Features)
2. Support VCA alarm for up to 15 VCA detections. (Chapter 9)
3. Support VCA search function for behavior search, face search, people counting and heat map. (Chapter 10)

Update

1. Update the interface of input method. (Chapter 1.3 Input Method Description)
2. Set the strong password to activate the device is needed for the first-time startup (Chapter 2.2)
3. Optimize the steps of the start wizard. (Chapter 2.3 2.3 Using the Wizard for Basic Configuration)
4. Optimize the adding of IP camera. (Chapter 2.4)
5. Optimize the interface of quick start toolbar. (Chapter 3.2.2 Quick Setting Toolbar in Live View Mode)
6. Optimize the interface of PTZ control panel. (Chapter 4 PTZ Controls)
7. Optimize recording associated interface. (Chapter 5 Recording Settings)
8. Update the allowed quantity of IP SAN disk. (Chapter 12.2 Managing Network HDD)
9. Update the interfaces of system maintenance. (Chapter 14 NVR Management and Maintenance)
10. Optimize the DDNS configuration. (Chapter 11.2.3)
11. Three methods are selectable for restoring to the default settings. (Chapter 14.6)
12. Optimize the user account management. (Chapter 15.5)

Version 3.0.12

Updated

1. Update the figures of wireless network interface. (Chapter 9.2.1 Configuring Wireless Network)
2. Update the figures of wizard interface. (Chapter 2.2 Using the Wizard for Basic Configuration)
3. Optimize the steps of adding IP cameras (Chapter 2.3 Adding and Connecting the IP cameras)

Version 3.0.7

Updated

1. Optimize the PTZ control panels and operations. (Chapter 9.2.1 Configuring Wireless Network)

Version 3.0.6

Updated

1. Optimize the PTZ control panels and operations. (Chapter 4)
2. Change the ezviz Cloud to EZVIZ Cloud P2P. (Chapter 9.2.2)
3. Add the models of DS-7100NI series, DS-7600NI-SE series and DS-7600NI-V(P) series NVR.

Version 3.0.4

Added

1. Connectable to smart IP cameras, and VCA alarm detection and recording are supported. (Chapter 5.2, Chapter

5.5 and Chapter 8.5)

2. Support video searching, playing back and backing up by VCA events. (Chapter 6.1.3 and Chapter 7.1.3)
3. Support smart playback by VCA rules. (Chapter 6.1.5)
4. Support P2P protocol and access by ezviz. (Chapter 9.2.2)

Deleted

- Combine the smart search function with the smart playback function, and the smart search section is deleted. (Chapter 6.2.2 Smart Search)

16.4 List of Compatible IP Cameras

List of Hikvision IP Cameras



For the list, our company holds right to interpret.

Type	Model	Version	Max. Resolution	Sub-stream	Audio
Hikvision Network Camera	DS-2CD2010F-I(W)	5.2.3 build 141024	1280×960	√	√
	DS-2CD2012F-I(W)	5.2.1 build 140820	1280×960	√	√
	DS-2CD2020F-I(W)	5.2.3 build 141024	1920×1080	√	√
	DS-2CD2032F-I(W)	5.2.1 build 140820	2048×1536	√	√
	DS-2CD2110F(D)-I(W)(S)	5.2.3 build 141024	1280×960	√	√
	DS-2CD2112F(D)-I(W)(S)	5.2.1 build 140820	1280×960	√	√
	DS-2CD2120F(D)-I(W)(S)	5.2.3 build 141024	1920×1080	√	√
	DS-2CD2132F(D)-I(W)(S)	5.2.1 build 140820	2048×1536	√	√
	DS-2CD2E10F-W	5.2.3 build 141024	1280×960	√	√
	DS-2CD2E20F-W	5.2.3 build 141024	1920×1080	√	√
	DS-2CD2410FD-I(W)	5.2.3 build 141024	1280×720	√	√
	DS-2CD2412FD-I(W)	5.2.1 build 140820	1280×960	√	√
	DS-2CD2420FD-I(W)	5.2.3 build 141024	1920×1080	√	√
	DS-2CD2432FD-I(W)	5.2.1 build 140820	2048×1536	√	√
	DS-2CD2512F-I(W)(S)	5.2.1 build 140820	1280×960	√	√
	DS-2CD2532F-I(W)(S)	5.2.1 build 140820	2048×1536	√	√
	DS-2CD2C10F-IW	5.2.3 build 141024	1280×720	√	×
	DS-2CD2942F-I(W)(S)	5.2.1 build 140925	2560×1440	√	√
	DS-2CD2Q10FD-IW	5.2.3 build 141024	1280×720	√	√

List of Third-party IP Cameras



ONVIF compatibility refers to the camera can be supported both when it uses the ONVIF protocol and its private protocols. **Only ONVIF is supported** refers to the camera can only be supported when it uses the ONVIF protocol. **Only AXIS is supported** refers to the function can only be supported when it uses the AXIS protocol.

IP Camera Manufacturer or Protocol	Model	Version	Max. Resolution	Sub-stream	Audio
ACTI	TCM4301-10D-X-00083	A1D-310-V4.12.09-AC	1280×1024	×	√
	TCM5311-11D-X-00023	A1D-310-V4.12.09-AC	1280×960	×	√
	TCM3401-09L-X-00227	A1D-220-V3.13.16-AC	1280×1024	×	×
ARECONT	AV1305M	65175	1600×1200	√	×
	AV2155	65143	1280×1024	√	×
	AV2815	65220	1600×1200	√	×
	AV3105M	65175	1920×1080	√	×
	AV5105	65175	1920×1080	√	×
	AV8185DN	65172	1920×1080	×	×
AXIS	M1114	5.09.1	1024×640	√	×
	M3011(ONVIF compatibility)	5.21	704×576	√ (Only AXIS is supported)	×
	M3014(ONVIF compatibility)	5.21.1	1280×800	√	×
	P3301(ONVIF compatibility)	5.11.2	768×576	√	√ (Only AXIS is supported)
	P3304(ONVIF compatibility)	5.20	1440×900	√	√ (Only AXIS is supported)
	P3343(ONVIF compatibility)	5.20.1	800×600	√	√ (Only AXIS is supported)
	P3344(ONVIF compatibility)	5.20.1	1440×900	√	√ (Only AXIS is supported)
	P5532	5.15	720×576	√	×
	P1346E	5.06.1	1920×1080	√	×
	Q7404	5.02	720×576	√	√

IP Camera Manufacturer or Protocol	Model	Version	Max. Resolution	Sub-stream	Audio
Bosch (ONVIF compatibility)	AutoDome Jr 800HD	39500450	1920×1080	×	√
	Dimion NBN-921-P	10500453	1280×720	×	√
	NBC 265 P	07500452	1280×720	×	√
Brickcom	CB-500Ap (ONVIF compatibility)	V3.2.1.3	1920×1080	×	√
	FB-130Np (ONVIF compatibility)	V3.1.0.8	1280×1024	×	√
	WFB-100Ap	V3.1.0.9	1280×800	×	√
Canon	VB-H410 (ONVIF compatibility)	Ver.+1.0.0	1280×960	×	√
	VB-H6100D	Ver. 1.0.0	1920×1080	×	×
	VB-H7100F	Ver. 1.0.0	1920×1080	×	×
	VB-M400 (ONVIF compatibility)	Ver.+1.0.0	1280×960	×	√
	VB-M6000D (ONVIF compatibility)	Ver.+1.0.0	1280×960	×	×
	VB-M7000F (ONVIF compatibility)	Ver.+1.0.0	1280×960	×	√
	VB-S300D	Ver. 1.0.0	1920×1080	×	×
	VB-S8000	Ver. 1.0.0	1920×1080	×	×
	VB-S9000F	Ver. 1.0.0	1920×1080	×	×
HUNT	HLC_79AD	V1.0.40	1600×1200	×	√
Panasonic (ONVIF compatibility)	WV-NP502	1.41	1920×1080	×	√
	WV—SC385	Application: 1.0 Image data: 1.09	1280×960	×	×
	WV—SC386	Application: 1.66 Image data: 1.05	1280×960	√	√
	WV-SF132	Application: 1.66 Image data: 1.03	640×360	√	×
	WV-SF336H	Application: 1.06 Image data: 1.06	1280×960	√	√
	WV-SF332	Application: 1.66 Image data: 1.06	800×600	√	√
	WV-SF342	Application: 1.66 Image data: 1.06	800×600	√	√
	WV-SF346	Application: 1.66 Image data: 1.06	1280×960	√	√
	WV-SP102	Application: 1.66 Image data: 1.03	640×480	√	×
	WV-SP105	Application: 1.66 Image data: 1.03	1280×960	√	×

IP Camera Manufacturer or Protocol	Model	Version	Max. Resolution	Sub-stream	Audio
	WV-SP302	Application: 1.66 Image data: 1.06	800×600	√	√
	WV-SP306H	Application: 1.34 Image data: 1.06	1280×960	√	√
	WV-SP509	Application: 30 Image data: 2.21	1280×960	√	√
	WV-SW152	Application: 1.66 Image data: 1.05	800×600	√	×
	WV-SW155	Application: 1.66 Image data: 1.05	1280×960	√	×
	WV-SW316	Application: 1.66 Image data: 2.0.3	1280×960	√	√
	WV-SW352	Application: 1.66 Image data: 1.04	800×600	√	√
PELCO	D5118	1.8.2-20120327- 2.9310-A1.7852	1280×960	√	×
	IXE20DN-AAXVUU2	1.8.2-20120327- 2.9081-A1.7852	1920×1080	√	×
	IXE10DN-ACDJV44	1.8.2-20120327- 2.9081-A1.7852	1280×1024	√	×
	IX30DN-ACFZHB3	1.8.2-20120327- 2.9080-A1.7852	2048×1536	√	×
SAMSUNG (ONVIF compatibility)	5000P	3.10_130416	1280×1024	√	√
	SNB-3000P	V1.41_110709	704×576	×	√
	SNB-5000P	V2.00_110727	1280×1024	√	√
	SNB-7000P	V1.10_110819	2048×1536	×	√
	SND-5080	3.10_130416	1280×1024	√	√
	SNP-5200H	V1.04_110825	1280×1024	√	√
	SNZ-5200	V1.04_110825	1280×1024	√	√
SANYO	VCC-HD2300P	2.03-02 (110318-00)	1920×1080	×	×
	VCC-HD2500P	2.02-02 (110208-00)	1920×1080	×	√
	VCC-HD4600P	2.03-02 (110315-00)	1920×1080	×	√
	VCC-HD5400	2.03-06 (110315-00)	1920×1080	×	√
SONY	SNC-CH220	1.50.00	1920×1080	×	×
	SNC DH220T (ONVIF compatibility)	1.50.00	2048×1536	×	×
	SNC-DH260	1.23.00	1920×1080	×	×
	SNC-EP580	1.53.00	1920×1080	√	√
	SNC-ER580	1.42.00	1280×720	×	√
	SNC-RH124	1.73.00	1280×720	√	√
Vivotek	IP7121	0202a	720×576	×	√
	IP7133	0203a	640×480	×	×
	FD8134 (ONVIF	0107a	1280×800	×	×

IP Camera Manufacturer or Protocol	Model	Version	Max. Resolution	Sub-stream	Audio
	compatibility)				
	IP8161 (ONVIF compatibility)	0104a	1600×1200	×	√ (Vivotek Protocol)
	IP8331 (ONVIF compatibility)	0102a	640×480	×	×
	IP8332 (ONVIF compatibility)	0105b	1280×800	×	×
	VS8102	0200S	704×576	×	√
ZAVIO	D5110	MG.1.6.03P8	1280×1024	√	×
	F3106	M2.1.6.03P8	1280×1024	√	√
	F3110	M2.1.6.01	1280×720	√	√
	F3206	MG.1.6.02c045	1920×1080	√	√
	F531E	LM.1.6.18P10	640×480	√	√

0300031050420

