

Network Video Recorder

User Manual

Regulatory information

FCC information

FCC compliance: This equipment has been tested and found to comply with the limits for a digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

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 EMC Directive 2004/108/EC.



2002/96/EC (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.

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.
- 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 battery manufacturer.

Thank you for purchasing our product. If there is any question or request, please do not hesitate to contact dealer.
This manual is applicable to the models listed in the following table.

Series	Model	Type
87XX-P series	4CH(4 POE) 8CH(4 POE) 8CH(8 POE) 16CH(8 POE) 16CH(16 POE)	Network Video Recorder

Product Key Features

General

- Connectable to network cameras, network dome and encoders.
- Connectable to the third-party network cameras like AXIS, ONVIF, PANASONIC, PSIA, SAMSUNG and SANYO.
- PAL/NTSC adaptive video inputs.
- Each channel supports dual-stream.
- Up to 16 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

- Simultaneous HDMI and VGA outputs.
- HDMI output and VGA 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 cycle live view are also provided, and the interval of automatic cycle can be adjusted.
- Quick setting menu is provided for live view.
- Motion detection, tamper-proof, 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

- Up to 2 SATA hard disks can be connected. (Each disk with a maximum of 4TB storage capacity.)
- 8 network disks (8 NAS disks, or 7 NAS disks+1 IP SAN disk) can be connected.
- HDD group management.
- Support HDD standby function.
- HDD property: redundancy, read-only, read/write (R/W).
- HDD quota management; different capacity can be assigned to different channel.

Recording and Playback

- Holiday recording schedule configuration.
- Normal and event video encoding parameters.
- Multiple recording types: manual, normal, alarm, motion, motion | alarm, motion & alarm.
- 8 recording time periods with separated recording types.
- 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).
- Tag adding for record files, searching and playing back by tags.
- Locking and unlocking record files.
- Local redundant recording.
- Searching and playing back record files by channel number, recording type, start time, end time, etc.
- Motion analysis for the selected area in the video.
- Zooming in when playback.

- Playing reversely.
- Adverse 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 at 4CIF real time.

Backup

- Export video data by USB or SATA 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, tampering, abnormal signal, video input/output standard mismatch, illegal login, network disconnected, IP confliction, abnormal record, HDD error, and HDD full, etc.
- Alarm triggers full screen monitoring, audio alarm, notifying surveillance center, sending email and alarm output.
- Automatic restore when system is abnormal.

Other Local Functions

- Operable by mouse and remote control.
- 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/1000M network interface.
- 4 independent PoE network interfaces for B Series4 series.
- Up to 8 independent network interfaces with built-in switch function are provided for B Series8 series.
- 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.
- Remote search, playback, download, locking and unlocking of the record files, and support downloading files broken transfer resume.
- Remote parameters setup; remote import/export of device parameters.
- Remote viewing of the device status, system logs and alarm status.
- Remote keyboard operation.
- Remote locking and unlocking of mouse.
- Remote HDD formatting and program upgrading.
- Remote system restart and shutdown.
- RS-485 transparent channel transmission.
- Alarm and exception information can be sent to the remote host
- Remotely start/stop recording.
- Remotely start/stop alarm output.
- Remote PTZ control.

- Two-way audio and 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	12
1.1 Front Panel	13
1.2 IR Remote Control Operations.....	15
1.3 USB Mouse Operation	18
1.4 Input Method Description	19
1.5 Rear Panel.....	20
Chapter 2 Getting Started	21
2.1 Starting Up and Shutting Down the NVR	22
2.2 Setting Admin Password	23
2.3 Using the Wizard for basic configuration.....	24
2.4 Login and Logout	27
2.4.1 User Login	27
2.4.2 User Logout	28
2.5 Adding and Connecting the IP Cameras.....	29
2.5.1 Activating the IP Camera	29
2.5.2 Adding the Online IP Cameras.....	30
2.5.3 Editing the Connected IP cameras and Configuring Customized Protocols	32
2.5.4 Editing IP cameras connected to the PoE interfaces	34
2.5.5 Editing IP cameras connected to the built-in switch network interfaces.....	35
Chapter 3 Live View	37
3.1 Introduction of Live View	38
3.2 Operations in Live View Mode	39
3.2.1 Using the Mouse in Live View	39
3.2.2 Quick Setting Toolbar in Live View Mode.....	40
3.3 Adjusting Live View Settings.....	41
3.4 Channel-zero Encoding	42
Chapter 4 PTZ Controls	44
4.1 Configuring PTZ Settings.....	45
4.2 Setting PTZ Presets, Patrols & Patterns.....	46
4.2.1 Customizing Presets	46
4.2.2 Calling Presets	47
4.2.3 Customizing Patrols	48
4.2.4 Calling Patrols.....	49
4.2.5 Customizing Patterns.....	50
4.2.6 Calling Patterns	51
4.3 PTZ Control Toolbar	52
Chapter 5 Record Settings	53
5.1 Configuring Encoding Parameters	54
5.2 Configuring Record Schedule.....	56
5.3 Configuring Motion Detection Record.....	60

5.4	Configuring Alarm Triggered Record.....	62
5.5	Configuring VCA Event Recording.....	64
5.6	Manual Record.....	65
5.7	Configuring Holiday Record.....	67
5.7	Configuring POS Record.....	69
5.8	Configuring Redundant Recording.....	71
5.9	Configuring HDD Group for Recording.....	73
5.10	Files Protection.....	74
Chapter 6 Playback.....		76
6.1	Playing Back Record Files.....	77
6.1.1	Playing Back by Channel.....	77
6.1.2	Playing Back by Time.....	79
6.1.3	Playing Back by Event Search.....	80
6.1.4	Playing Back by Tag.....	83
6.1.5	Playing Back by System Logs.....	86
6.1.6	Playing Back External File.....	88
6.1.7	Playing Back POS.....	89
6.2	Auxiliary Functions of Playback.....	91
6.2.1	Playing Back Frame by Frame.....	91
6.2.2	Smart Search.....	91
6.2.3	Digital Zoom.....	94
6.2.4	Reverse Playback of Multi-channel.....	94
Chapter 7 Backup.....		96
7.1	Backing up Record Files.....	97
7.1.1	Quick Export.....	97
7.1.2	Backing up by Normal Video Search.....	99
7.1.3	Backing up by Event Search.....	102
7.1.4	Backing up Video Clips.....	104
7.1.5	Backing up POS.....	106
7.2	Managing Backup Devices.....	109
Chapter 8 Alarm Settings.....		112
8.1	Setting Motion Detection Alarm.....	113
8.2	Setting Sensor Alarms.....	115
8.3	Detecting Video Loss Alarm.....	118
8.4	Detecting Video Tampering Alarm.....	119
8.5	Handling Exceptions Alarm.....	121
8.6	Setting Alarm Response Actions.....	122
8.7	Triggering or Clearing Alarm Output Manually.....	126
Chapter 9 VCA Alarm.....		127
9.1	Face Detection.....	128
9.2	Line Crossing Detection.....	129
9.3	Intrusion Detection.....	131
9.4	People Gathering Detection.....	133
Chapter 10 VCA Search.....		134

10.1	Face Search	135
10.2	Behavior Search	136
10.3	People Counting	138
10.4	Heat Map	139
Chapter 11 Network Settings		140
11.1	Configuring General Settings	141
11.2	Configuring Advanced Settings	143
11.2.1	Configuring PPPoE Settings	143
11.2.2	Configuring DDNS	143
11.2.3	Configuring NTP Server	147
11.2.4	Configuring SNMP	148
11.2.5	Configuring Remote Alarm Host	148
11.2.6	Configuring Multicast	149
11.2.7	Configuring RTSP	150
11.2.8	Configuring Server and HTTP Ports	150
11.2.9	Configuring HTTPS Port	151
11.2.10	Configuring Email	152
11.2.11	Configuring NAT	153
11.2.12	Configuring High-speed Download	156
11.2.13	Configuring Virtual Host	157
11.2.14	Configuring Telnet	158
11.3	Checking Network Traffic	159
11.4	Configuring Network Detection	160
11.4.1	Testing Network Delay and Packet Loss	160
11.4.2	Exporting Network Packet	160
11.4.3	Checking the Network Status	161
11.4.4	Checking Network Statistics	162
Chapter 12 HDD Management		163
12.1	Initializing HDDs	164
12.2	Managing Network HDD	166
12.3	Managing HDD Group	168
12.3.1	Setting HDD Groups	168
12.3.2	Setting HDD Property	169
12.4	Configuring Quota Mode	171
12.5	Checking HDD Status	173
12.6	HDD Detection	175
12.7	Configuring HDD Error Alarms	177
Chapter 13 Camera Settings		178
13.1	Configuring OSD Settings	179
13.2	Configuring Privacy Mask	180
13.3	Configuring Video Parameters	181
Chapter 14 NVR Management and Maintenance		182
14.1	Viewing System Information	183
14.1.1	Viewing Device Information	183

14.1.2	Viewing Camera Information	183
14.1.3	Viewing Record Information	184
14.1.4	Viewing Alarm Information	184
14.1.5	Viewing Network Information.....	184
14.1.6	Viewing HDD Information	185
14.2	Searching & Export Log Files	186
14.3	Importing/Exporting Configuration Files	189
14.4	Upgrading System	190
14.4.1	Upgrading by Local Backup Device	190
14.4.2	Upgrading by FTP	190
14.5	Restoring Default Settings	192
Chapter 15	Others.....	193
15.1	Configuring General Settings	194
15.2	Configuring DST Settings	195
15.3	Configuring More Settings for Device Parameters.....	196
13.4	Configuring POS.....	197
15.5	Managing User Accounts	201
15.5.1	Adding a User	201
15.5.2	Deleting a User	203
15.5.3	Editing a User	204
15.6	Logging out/Shutting down/Rebooting Device.....	205
Appendix	206
	Glossary.....	207
	FAQ	208
	List of Compatible IP Cameras.....	214

Chapter 1 Introduction

1.1 Front Panel



Figure 1. 1 87XX-P Series

Table 1. 1 Description of Front Panel

No.	Name	Function Description
1	Status Indicators	POWER: the POWER indicator turns green when NVR is powered up.
		READY: The indicator light is green when the device is running normally.
		STATUS: 1.The light is green when the IR remote control is enabled; 2.The light is red when the function of the composite keys (SHIFT) are used; 3. The light is out when none of the above condition is met/
		ALARM: the light is red when there is an alarm occurring.
		HDD: the indicator flickers red when HDD is reading/writing.
		Tx/Rx: TX/RX indicator flickers green when network connection is functioning normally.
2	USB Interface	Connects USB mouse or USE flash memory devices.
3	Composite Keys	1/MENU: Enter numeral "1"; Access the main menu interface.
		2/ABC/F1: Enter numeral "2"; Enter letters "ABC"; The F1 button when used in a list field will select all items in the list. In PTZ Control mode, it will turn on/off PTZ light and when the image is zoomed in, the key is used to zoom out.
		3/DEF/F2: Enter numeral "3"; Enter letters "DEF"; The F2 button is used to change the tab pages. In PTZ control mode, it zooms in the image.
		4/GHI/ESC: Enter numeral "4"; Enter letters "GHI"; Exit and back to the previous menu.
		5/JKL/EDIT: Enter numeral "5"; Enter letters "JKL"; Delete characters before cursor; Check the checkbox and select the ON/OFF switch; Start/stop record clipping in playback.
		6/MNO/PLAY: Enter numeral "6";

			Enter letters "MNO";
			Playback, for direct access to playback interface.
		7/PQRS/REC:	Enter numeral "7";
			Enter letters "PQRS";
			Open the manual record interface.
		8/TUV/PTZ:	Enter numeral "8";
			Enter letters "TUV";
			Access PTZ control interface.
		9/WXYZ/PREV:	Enter numeral "9";
			Enter letters "WXYZ";
			Multi-channel display in live view.
		0/A:	Enter numeral "0";
			Shift the input methods in the editing text field. (Upper and lowercase, alphabet, symbols or numeric input).
			Double press the button to switch the main and auxiliary output.
		4	SHIFT
5	Control Buttons	<p>Directional buttons:</p> <p>In menu mode, the direction buttons are used to navigate between different fields and items and select setting parameters.</p> <p>In playback mode, the Up and Down buttons are used to speed up and slow down record playing, and the Left and Right buttons are used to move the recording 30s forwards or backwards.</p> <p>In the image setting interface, the up and down button can adjust the level bar of the image parameters.</p> <p>In live view mode, these buttons can be used to switch channels.</p> <p>Enter:</p> <p>The Enter button is used to confirm selection in menu mode; or used to check checkbox fields and ON/OFF switch.</p> <p>In playback mode, it can be used to play or pause the video.</p> <p>In single-frame play mode, pressing the Enter button will play the video by a single frame.</p> <p>And in auto sequence view mode, the buttons can be used to pause or resume auto sequence.</p>	
6	IR Receiver	Receiver for IR remote.	

1.2 IR Remote Control Operations

The NVR may also be controlled with the IR remote control (Remote option may vary based on model), shown in Figure 1. 2.

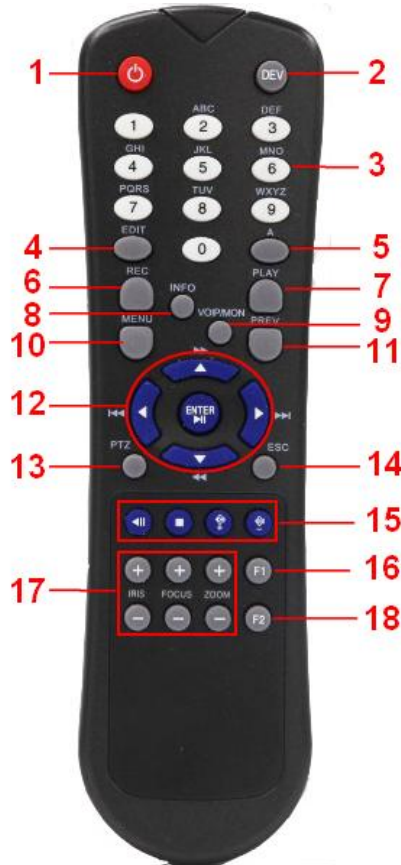


Figure 1. 2 Remote Control

The keys on the remote control closely resemble the ones on the front panel. See Figure 1. 2.

Table 1. 2 Description of the Soft Keyboard Icons

No.	Name	Description
1	POWER	Power on/off the device.
2	DEV	Enables/Disables Remote Control.
3	Alphanumeric Buttons	Switch to the corresponding channel in Live view or PTZ Control mode. Input numbers and characters in Edit mode. Switch between different channels in All-day Playback mode.
4	EDIT Button	Edit text fields. When editing text fields, it will also function as a Backspace button to delete the character in front of the cursor. On checkbox fields, pressing the button will <i>tick</i> the checkbox. In PTZ Control mode, the button adjusts the iris of the camera. In Playback mode, it can be used to generate video clips for backup. Enter/exit the folder of USB device.
5	A Button	Adjust focus in the PTZ Control menu. It is also used to switch between input methods (upper and lowercase

		alphabet, symbols and numeric input).
6	REC Button	Enter the Manual Record setting menu.
		In PTZ control settings, press the button and then you can call a PTZ preset by pressing Numeric button.
		It is also used to turn audio on/off in the Playback mode.
7	PLAY Button	The button is used to enter the All-day Playback mode.
		It is also used to auto scan in the PTZ Control menu.
8	INFO Button	Reserved.
9	VOIP Button	Switch between main and spot output.
		In PTZ Control mode, it can be used to zoom out the image.
10	MENU Button	Press the button will help you return to the Main menu (after successful login).
		Press and hold the button for 5 seconds will turn off audible key beep.
		In PTZ Control mode, the MENU/WIPER button will start wiper (if applicable).
		In Playback mode, it is used to show/hide the control interface.
11	PREV Button	Switch between single screen and multi-screen mode.
		In PTZ Control mode, it is used to adjust the focus in conjunction with the A/FOCUS+ button.
12	DIRECTION Button	Navigate between different fields and items in menus.
		In the Playback mode, the Up and Down button is used to speed up and slow down recorded video. The Left and Right button will select the next and previous record files .
		In Live View mode, these buttons can be used to cycle through channels.
		In PTZ control mode, it can control the movement of the PTZ camera.
	ENTER Button	Confirm selection in any of the menu modes.
		It can also be used to <i>tick</i> checkbox fields.
13	PTZ Button	In Playback mode, it can be used to play or pause the video.
		In single-frame Playback mode, pressing the button will advance the video by a single frame.
14	ESC Button	In Auto-switch mode, it can be used to stop /start auto switch.
		Back to the previous menu.
15	RESERVED	Press for Arming/disarming the device in Live View mode.
		Reserved for future usage.
16	F1 Button	Select all items on the list when used in a list field.
		In PTZ Control mode, it will turn on/off PTZ light (if applicable).
		In Playback mode, it is used to switch between play and reverse play.
17	PTZ Control Buttons	Buttons to adjust the iris, focus and zoom of a PTZ camera.
18	F2 Button	Cycle through tab pages.
		In synchronous playback mode, it is used to switch between channels.

Troubleshooting Remote Control:

Note: Make sure you have installed batteries properly in the remote control. And you have to aim the remote control at the IR receiver in the front panel.

If there is no response after you press any button on the remote, follow the procedure below to troubleshoot.

Steps:

1. Go to Menu > Settings > General > More Settings by operating the front control panel or the mouse.
2. Check and remember NVR ID#. The default ID# is 255. This ID# is valid for all the IR remote controls.
3. Press the DEV button on the remote control.
4. Enter the NVR ID# you set in step 2.
5. Press the ENTER button on the remote.

If the Status indicator on the front panel turns blue, the remote control is operating properly. If the Status indicator does not turn blue and there is still no response from the remote, please check the following:

1. Batteries are installed correctly and the polarities of the batteries are not reversed.
2. Batteries are fresh and not out of charge.
3. IR receiver is not obstructed.

If the remote still can't function properly, please change a remote and try again, or contact the device provider.

1.3 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 one of the USB interfaces on the front 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. 3 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. Tamper-proof, 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.

1.4 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. 4 Description of the Soft Keyboard Icons

Icons	Description	Icons	Description
	Numbers		Capital English
	Lowercase/Uppercase		Backspace
	Switch the keyboard		Space
	Positioning the cursor		Exit
	Symbols		Reserved

1.5 Rear Panel

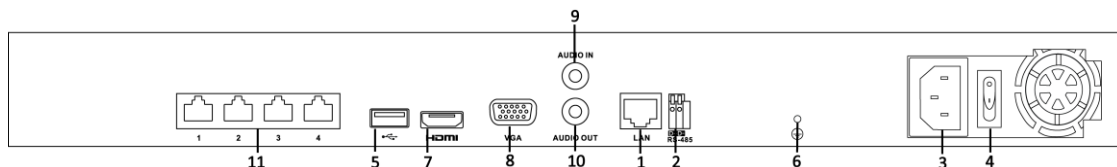


Figure 1. 5 87XX-P Series

Note: The rear panels of others provide 8 POE interfaces

No.	Item	Description
1	LAN Network Interface	Connector for LAN (Local Area Network).
2	RS-485 Interface	Connects to RS-485 devices.
3	Power Supply	100~240VAC power supply
4	Power Switch	Switch for turning on/off the device.
5	USB Interface	Universal Serial Bus (USB) ports for additional devices such as USB mouse and USB Hard Disk Drive (HDD).
6	GND	Ground (needs to be connected when NVR starts up).
7	HDMI Interface	HDMI video output connector.
8	VGA Output	DB9 connector for VGA output. Display local video output and menu.
9	Audio In	RCA connector for voice talk input
10	Audio Out	RCA connector for audio output
11	Network interfaces with PoE function (for B Series)	Network interface for the cameras and to provide power over Ethernet.

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:

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:

Steps:

1. 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.
2. Turn on the power switch on the rear panel.
3. After startup, the Power LED indicator turns on (supported by A Series series NVR only). A splash screen with the status of the HDD appears on the monitor. The row of icons at the bottom of the screen shows the HDD status. 'X' means that the HDD is not installed or cannot be detected.

Shutting down the NVR

Steps:

1. Enter the Shutdown menu.

Menu > Shutdown

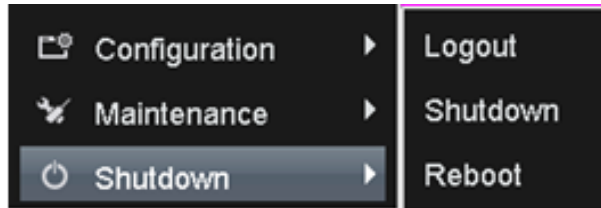


Figure 2. 1 Shutdown Menu

2. Click the **Shutdown** button.
3. Click the **Yes** button.
4. Turn off the power switch on the rear panel when the attention pops up.

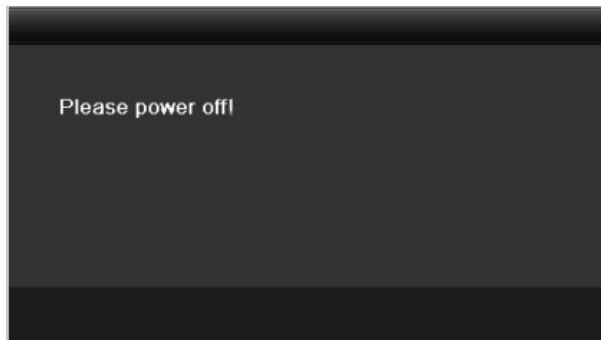


Figure 2. 2 Shutdown Attention

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**.

Activation	
User Name	admin
Create New P...	***** Strong
Confirm New P...	*****
<p>✓ 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.</p>	
<p>⏻ OK Cancel</p>	

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.

Warning	
<p>⚠ Admin password is weak. Please use a strong password to ensure your information security. Continue?</p>	
<p>YES NO</p>	

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.

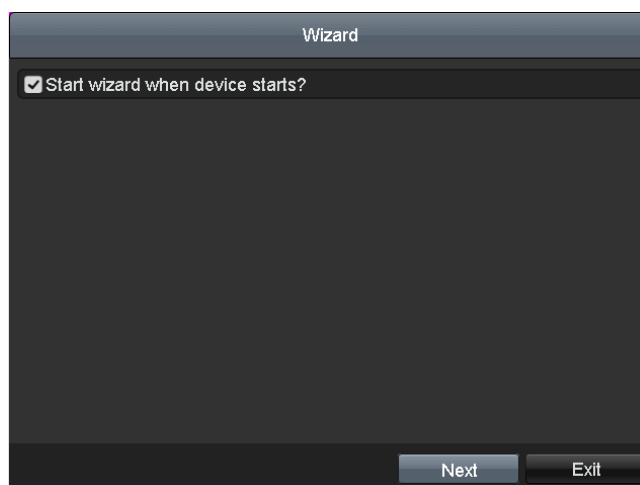


Figure 2. 5 Start Wizard Interface

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.

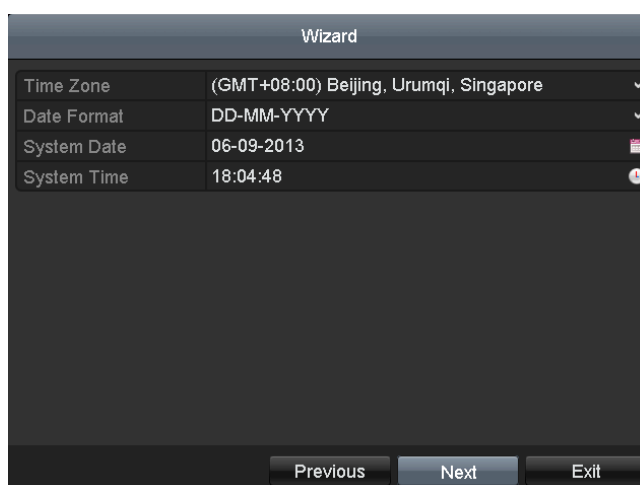


Figure 2. 6 Date and Time Settings

3. After the time settings, click **Next** button which takes you back to the **Basic Network Setup Wizard** interface.

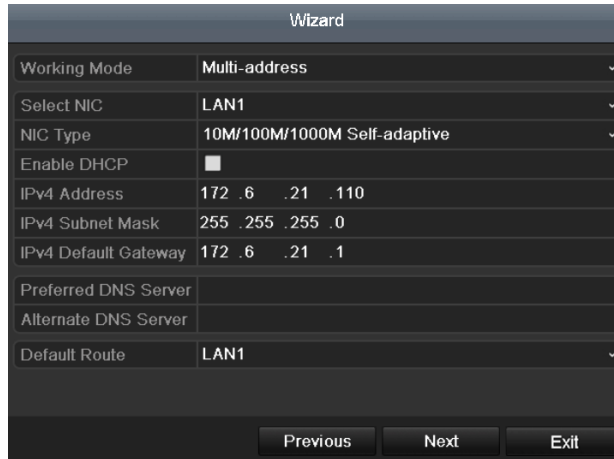


Figure 2. 7 Network Configuration



- The dual-NIC network 10 /100/1000 Mbps self-adaptive Ethernet interfaces are provided for the DS-8600NI-E8 and DS-7700NI-E4 series NVR; one 10 /100 Mbps self-adaptive Ethernet interface for DS-7604/7608NI-E1(E2) series NVR; and one 10 /100/1000 Mbps self-adaptive Ethernet interface for other models.
 - For the models have the PoE or built-in switch network interfaces, including DS-7600NI-E1(E2)/N, DS-7600NI-E1(E2)/P and DS-7700NI-E4/P series NVR, the internal NIC IPv4 address should be configured for the cameras connecting to the PoE or built-in switch network interface of the NVR.
4. Click **Next** button after you configured the basic network parameters. Then you will enter the **Cloud P2P** interface. Configure the Cloud P2P according to your need.



Figure 2. 8 Advanced Network Parameters

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

The screenshot shows a 'Wizard' window with the following fields and values:

Server Port	8000
HTTP Port	80
RTSP Port	554
Enable UPnP	<input type="checkbox"/>
Enable DDNS	<input checked="" type="checkbox"/>
DDNS Type	HIDDNS
Area/Country	Custom
Server Address	www.hiddns.com
Device Domain Name	
Status	DDNS status is normal.
User Name	
Password	

At the bottom of the window are three buttons: 'Previous', 'Next', and 'Exit'.

Figure 2. 9 Advanced Network Parameters

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

The screenshot shows a 'Wizard' window displaying a table of HDD information:

<input type="checkbox"/>	L...	Capacity	Status	Property	Type	Free Space
<input checked="" type="checkbox"/>	5	76,319MB	Normal	R/W	Local	66,560MB

At the bottom of the window are three buttons: 'Previous', 'Next', and 'Exit'. An 'Init' button is located above the 'Next' button.

Figure 2. 10 HDD Management

7. To initialize the HDD, click the **Init** button. Initialization removes all the data saved in the HDD.
8. Click **Next** button to enter the **IP Camera Management** interface.
9. 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.

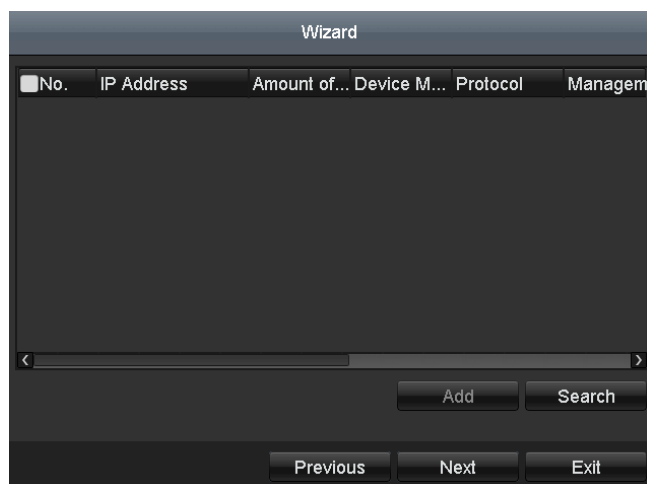


Figure 2. 11 IP Camera Management

-
10. Click **Next** button. Configure the recording for the searched IP Cameras.

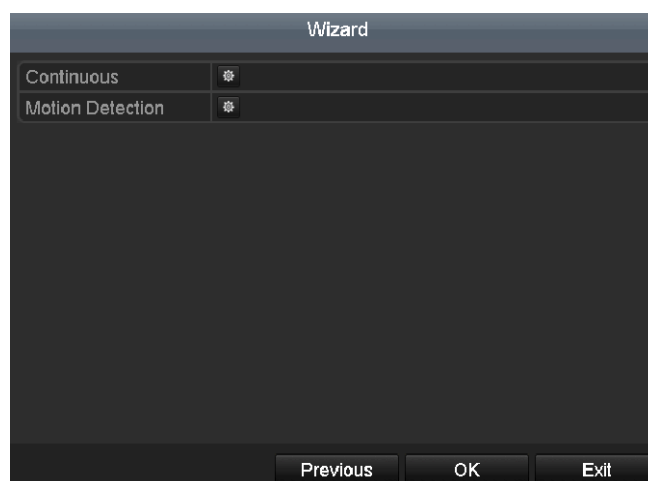


Figure 2. 12 Record Settings

-
11. Click **OK** to complete the startup Setup Wizard.

2.4 Login and Logout

2.4.1 User Login

Purpose:

If NVR has logged out, you must login the device before operating the menu and other functions.

Steps:

1. Select the **User Name** in the dropdown list.

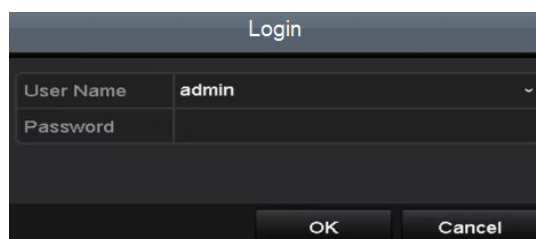


Figure 2. 13 Login Interface

2. Input **Password**.
3. Click **OK** to log in.



The device gets locked for 60 seconds if the admin user performs 7 failed password attempts (5 attempts for the guest/operator).

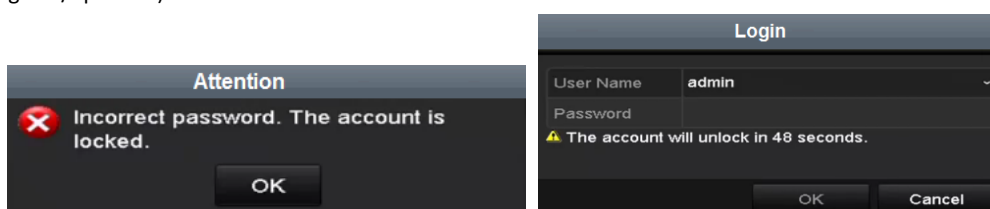


Figure 2. 14 User Account Protection

2.4.2 User Logout

Purpose:

After logging out, the monitor turns to the live view mode and if you want to do some operation, you need to enter user name and password to log in again.

Steps:

1. Enter the Shutdown menu.
Menu>Shutdown

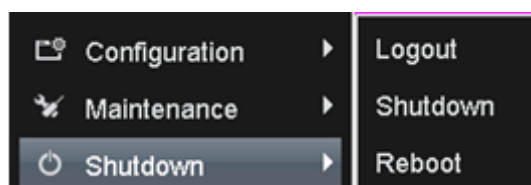


Figure 2. 15 Logout

2. Click **Logout**.



After you have logged out the system, menu operation on the screen is invalid. It is required to input a user name and password to unlock the system.

2.5 Adding and Connecting the IP Cameras

2.5.1 Activating the IP Camera

Purpose:

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

Steps:

1. Select the **Add IP Camera** option from the right-click menu in live view mode or click Menu> Camera> Camera to enter the IP camera management interface.

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



Figure 2. 16 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.

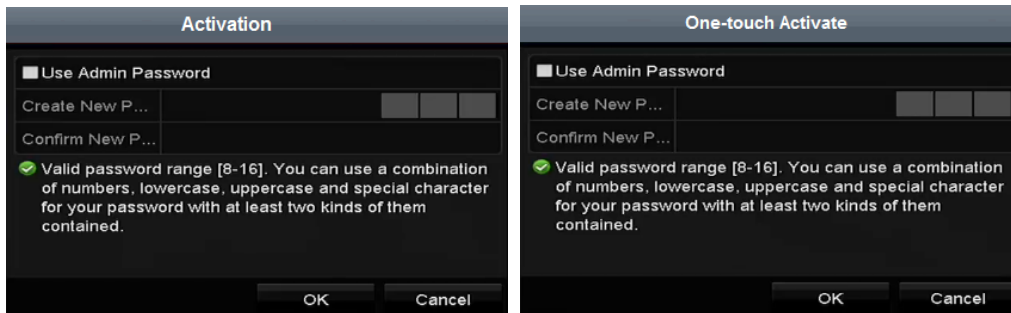


Figure 2. 17 Activate the Camera

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.

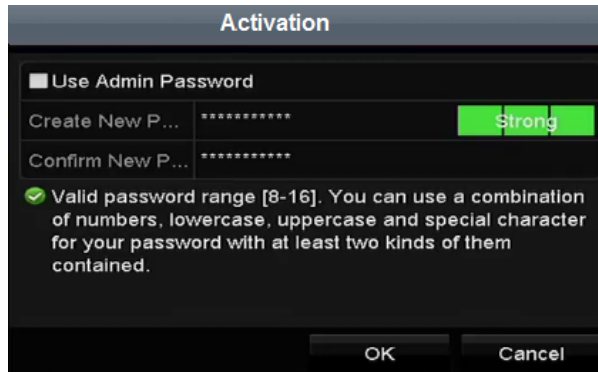



Figure 2. 18 Set New Password

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 activation of the IP camera. And the security status of camera will be changed to **Active**.

2.5.2 Adding the Online IP Cameras

Purpose:

The main function of the NVR is to connect the network cameras and record 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:

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

Option 1:

Steps:

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



2. Select  on your demand.

Steps:







1. To add the online cameras with same network segment:
 - 1) The detected online camera will be listed in the camera list, as shown in the figure below.



Figure 2. 19 Manual Adding IP Camera Interface

- 2) Click the  button to add the camera.

Table 2. 1 Explanation of the icons:

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

2. To add other IP cameras:
 - 1) Click the **Custom Adding** button to pop up the Add IP Camera (Custom) interface.

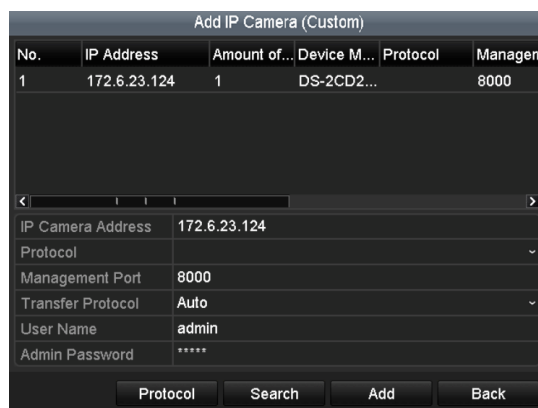


Figure 2. 20 Custom Adding IP Camera Interface

- 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

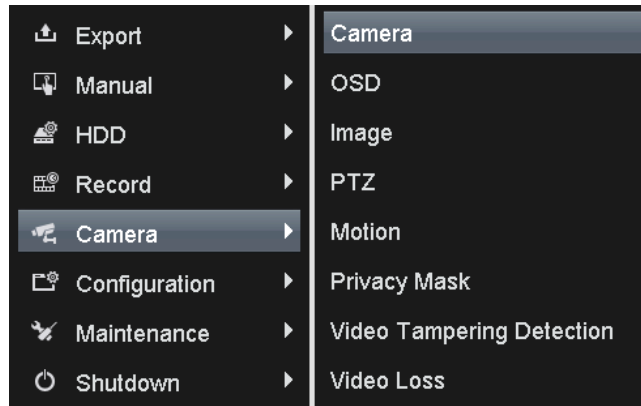


Figure 2. 21 Menu

2. To add the online cameras with same network segment:

- 1) Click **Search** to search the online cameras.

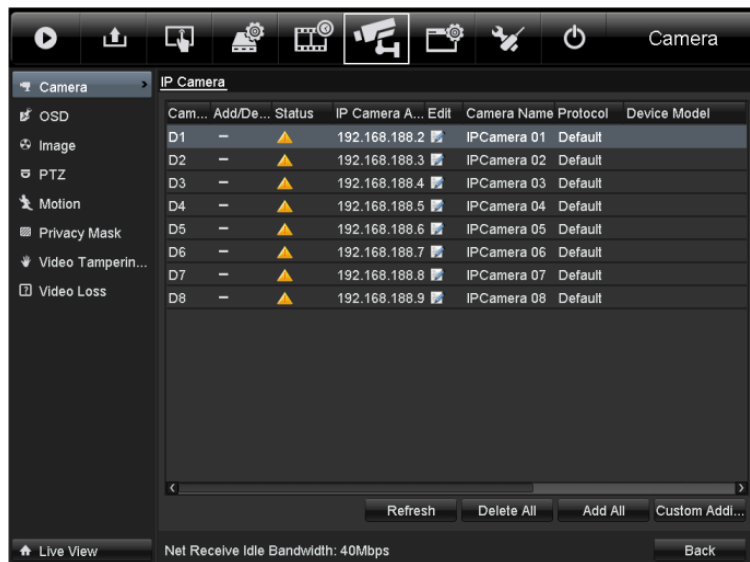


Figure 2. 22 Camera Settings Interface

- 2) Check the checkbox of certain cameras to be added.
 - 3) Click **Quick Add** to add the camera.
3. To add other IP cameras:
- 1) On the left side of the interface, you can enter the IP address, protocol, management port, user name, password and other information of the IP camera to be added.
 - 2) Click **Add** to add the camera.


Note: If you check the Synchronize IP Camera checkbox, the default settings of the NVR for the IP camera is applied to the added camera.

2.5.3 Editing the Connected IP cameras and Configuring 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.

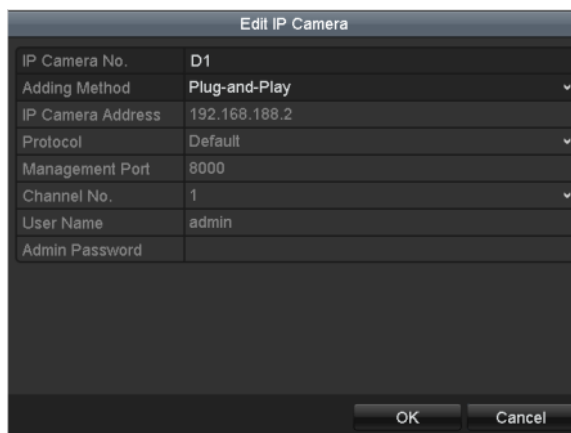


Figure 2. 23 Edit the Parameters

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

To edit more parameters:

1. Click the **Advance Set** icon.

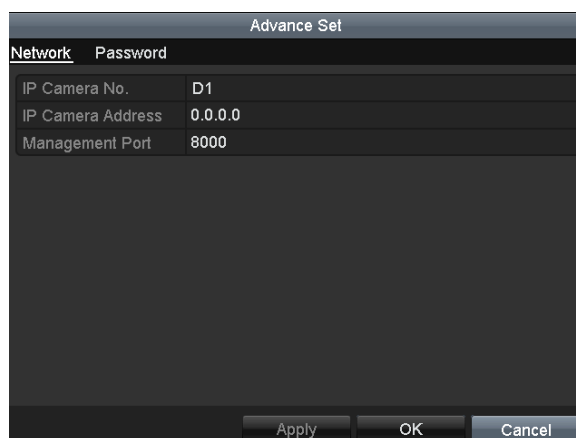


Figure 2. 24 Network Configuration of the Camera

2. You can edit the network information and the password of the camera.

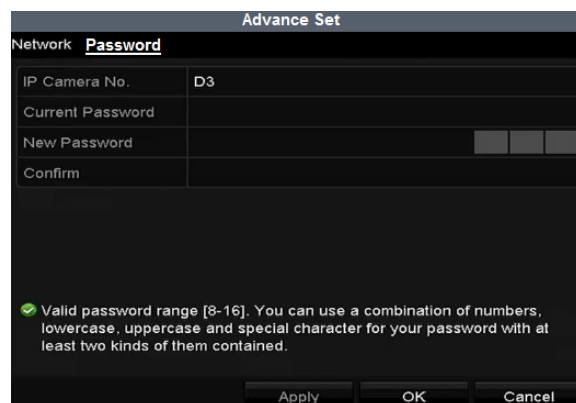



Figure 2. 25 Password Configuration of the Camera

3. Click **Apply** to save the settings and click **OK** to exit the interface.

Explanation of the icons

	
Edit basic parameters of the camera	Get the live view of the camera

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

Note: 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 dropdown list, please refer to Figure 2. 26.

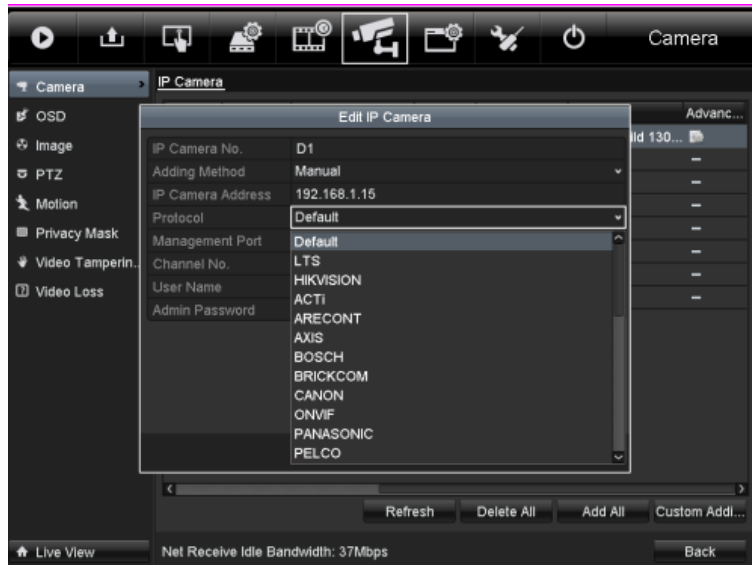


Figure 2. 26 Protocol Setting

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

2.5.4 Editing IP cameras connected to the PoE interfaces

The PoE interfaces enables the NVR system to pass electrical power safely, along with data, on Ethernet cabling to the connected network cameras.

The B Series and C Series NVR provides 4 PoE interfaces which can connect to 4 network cameras directly; and if you disable the PoE interface, you can also connect to the online network cameras. And the PoE interface supports the Plug-and-Play function.

Example:

As for 4CH NVR, when you want to connect 1 online camera and connect 3 network cameras via PoE interfaces, you must disable 1 PoE interface in the **Edit IP camera** panel.

To add Cameras for NVR supporting PoE function:

Before you start:

Connect the network cameras via the PoE interfaces.

Steps:

1. Enter the Camera Management interface.

Main menu> Camera> Camera

You can see the connected cameras are listed.

Cam...	Add/De...	Status	Security	IP Camera A...	Edit	Up...	Camera Name
D1	-	▲	N/A	192.168.254.2	✎	-	IPCamera 01
D2	-	▲	N/A	192.168.254.3	✎	-	IPCamera 02
D3	-	▲	N/A	192.168.254.4	✎	-	IPCamera 03
D4	-	▲	N/A	192.168.254.5	✎	-	IPCamera 04
D5	-	▲	N/A	192.168.254.6	✎	-	IPCamera 05
D6	-	▲	N/A	192.168.254.7	✎	-	IPCamera 06
D7	-	▲	N/A	192.168.254.8	✎	-	IPCamera 07
D8	-	▲	N/A	192.168.254.9	✎	-	IPCamera 08

Figure 2. 27 List of Connected Cameras

Note: The cameras connecting to the PoE interface cannot be deleted in this menu.

Click the **Edit** button.

Edit IP Camera	
IP Camera No.	D1
Adding Method	Plug-and-Play
IP Camera Address	192.168.1.15
Protocol	Default
Management Port	8000
Channel No.	1
User Name	admin
Admin Password	

Figure 2. 28 Edit IP Camera Interface

Note: Plug-and-Play means that the camera is connected to the PoE interface, so in this case, the parameters of the camera can't be edited. The IP address of the camera can only be edited in the Network Configuration interface, see *Chapter 9.1 Configuring General Settings* for detailed information.

2.5.5 Editing IP cameras connected to the built-in switch network interfaces

For A SeriesN-Pseries NVR, the extra network interfaces provide a built-in switch with plug-and-play function.

Example:

As for 8CH NVR, when you want to connect 2 online cameras and connect 6 network cameras via built-in switch interfaces, you must disable 2 built-in switch interfaces in the **Edit IP camera** panel.

To add Cameras for NVR via built-in switch interfaces:

Before you start:

Connect the network cameras via the built-in switch interfaces.

Steps:

1. Enter the Camera Management interface.

Main menu> Camera> Camera

You can see the connected cameras are listed.

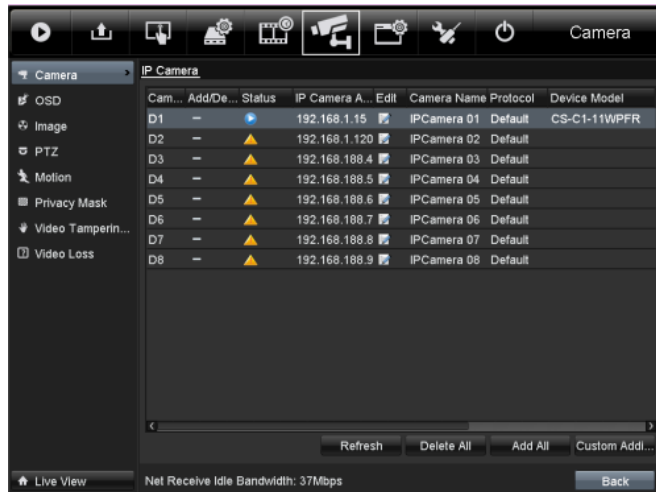


Figure 2. 29 List of Connected Cameras

Note: The cameras connecting to the built-in switch interface cannot be deleted in this menu.

2. Click the **Edit** button.

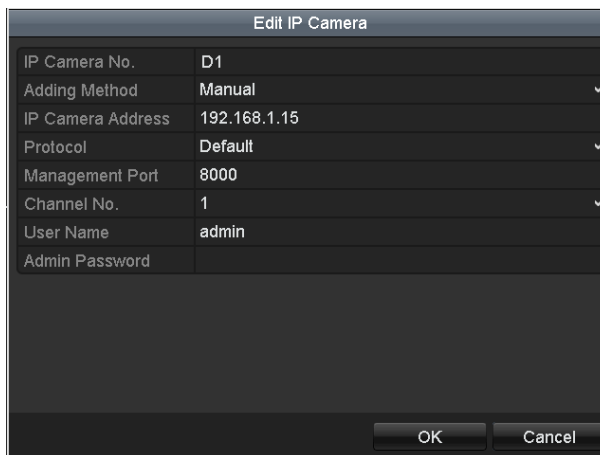


Figure 2. 30 Edit IP Camera Interface

Note: Plug-and-Play means that the camera is connected to the switch interface, so in this case, the parameters of the camera can't be edited. The IP address of the camera can only be edited in the Network Configuration interface, see *Chapter 9.1 Configuring General Settings* for detailed information.

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.

Live View Icons

In the live view mode, there are icons at the right top 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, tampering, motion detection or sensor alarm)
	Record (manual record, schedule record, motion detection or alarm triggered record)
	Alarm & Record

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>General.
- **Start Recording:** normal record and motion detection record are supported.
- **Output Mode:** select the output mode to Standard, Bright, Gentle or Vivid.
- **All-day Playback:** playback the recorded videos for current day.

3.2.1 Using the Mouse in Live View

Table 3. 2 Mouse Operation in Live View

Name	Description
Menu	Enter the menu of the system by clicking the icon.
	Switch to the single full screen.
	Adjust the screen layout by clicking the specific icon.
	Switch to the previous/next screen.
	Enable/disable the auto-switch of the screens.
	Start continuous recording or motion detection recording of all channels.
	Enter the playback interface and start playing back the video of the selected channel immediately.
	Four modes of output supported, including Standard, Bright, Gentle and Vivid.
	Fix the menu

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

Note: If the corresponding camera supports intelligent function, the Reboot Intelligence option is included when right-clicking mouse on this camera.



Figure 3. 1 Right-click Menu

Note:

- Two ways are provided to show the Right-click Menu Bar: right-clicking or moving the mouse to the bottom of the screen.
- You can click on the right side of the menu bar to fix the 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.


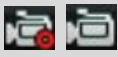

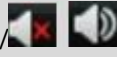






Note:  Live View Strategy icon is only available for network cameras.



Figure 3. 2 Quick Setting Toolbar

Table 3. 3 Description of Quick Setting Toolbar Icons

Icons	Description	Icons	Description	Icons	Description
	Enable/Disable Manual Record		Instant Playback		Mute/Audio on
	PTZ Control		Digital Zoom		Image Settings
	Live View Strategy		Text show		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.

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

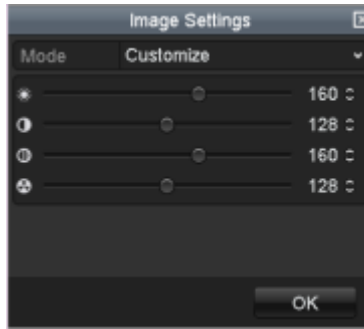


Figure 3. 4 Image Settings- Customize



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

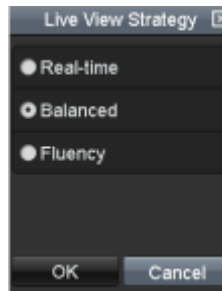


Figure 3. 5 Live View Strategy

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. 6 Live View-General

The settings available in this menu include:

- **Video Output Interface:** Designates the output to configure the settings for. Outputs include VGA/HDMI.
- **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:** Enables/disables audio output for the selected video output.
- **Event Output:** Designates the output to show event video.
- **Full Screen Monitoring Dwell Time:** The time in seconds to show alarm event screen.

2. Setting Cameras Order

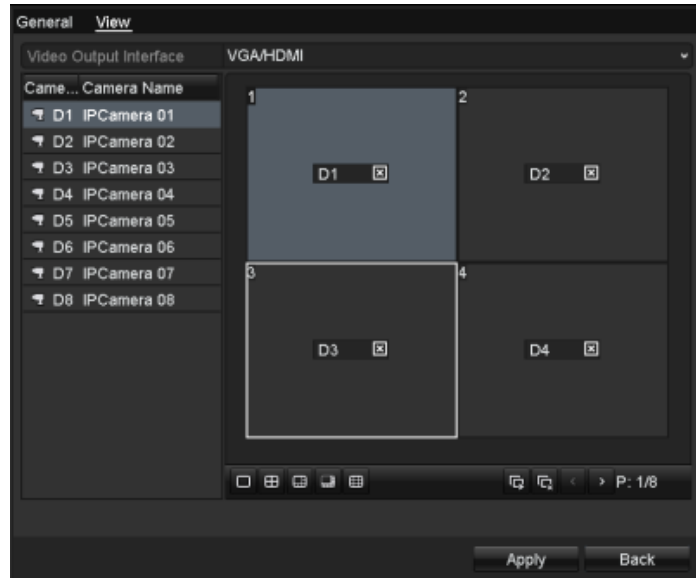





Figure 3. 7 Live View- Camera Order

To set the 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.

You can 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.

3.4 Channel-zero Encoding

Purpose:

Sometimes you need to get a remote view of many channels in real time from web browser or CMS (Client Management System) software, in order to decrease the bandwidth requirement without affecting the image quality, channel-zero encoding is supported as an option for you.

Steps:

1. Enter the **Live View** Settings interface.
Menu > Configuration > Live View
2. Select the **Channel-Zero Encoding** tab.

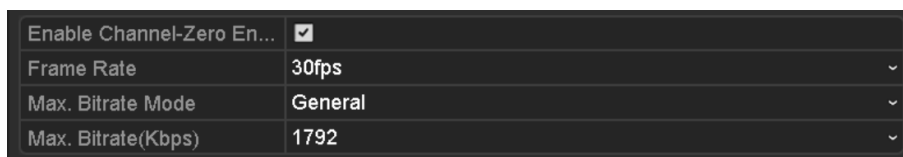


Figure 3. 8 Live View- Channel-Zero Encoding

3. Check the checkbox after **Enable Channel Zero Encoding**.
4. Configure the Frame Rate, Max. Bitrate Mode and Max. Bitrate.

After you set the Channel-Zero encoding, you can get a view in the remote client or web browser of 16 channels in one screen.

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

General	More Settings
Camera	IP Camera 1
Baud Rate	9600
Data Bit	8
Stop Bit	1
Parity	None
Flow Ctrl	None
PTZ Protocol	Default
Address	0

Address range: 0~255

Figure 4. 1 PTZ- General

2. Choose the camera for PTZ setting in the **Camera** dropdown list.
3. Enter the parameters of the PTZ camera.

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

Example: If the PTZ camera uses the protocol of DRAGON, you should select DRAGON in the PTZ Protocol field.

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

4.2 Setting PTZ Presets, Patrols & Patterns

Before you start:

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

4.2.1 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>More Settings



Figure 4. 2 PTZ- More Settings

2. Use the directional button to wheel the camera to the location where you want to set preset.
3. Click the round icon before **Save Preset**.
4. Click the preset number to save the preset.

Repeat the steps2-4 to save more presets. If the number of the presets you want to save is more than 17, you can click [...] and choose the available numbers.

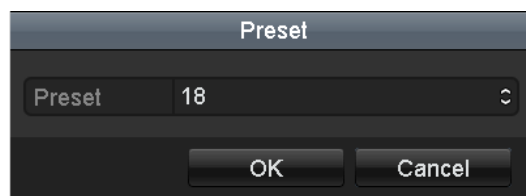


Figure 4. 3 More Presets

4.2.2 Calling Presets

Purpose:

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

Call preset in the PTZ setting interface:

Steps:

1. Enter the PTZ Control interface.
Menu>Camera>PTZ>More Settings
2. Check the round icon of **Call Preset**.



Figure 4. 4 PTZ- Call Preset

3. Choose the preset number.

Call preset in live view mode:

Steps:


1. Press the PTZ button on the front panel or click the PTZ Control icon  in the quick setting bar to enter the PTZ setting menu in live view mode.



Figure 4. 5 PTZ Toolbar

2. Choose **Camera** in the list on the menu.
3. Double click the preset in the **Preset** list to call it.

4.2.3 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>More Settings
2. Select patrol number in the drop-down list of patrol.
3. Select the  under Patrol option box to add key points for the patrol.



Figure 4. 6 PTZ- Add Key Point

4. Configure key point parameters, such as the key point No., duration of staying for one key point and speed of patrol. The key point is corresponding to the preset. The **Key Point No.** determines the order at which the PTZ will follow while cycling through the patrol. The **Duration** refers to the time span to stay at the corresponding key point. The **Speed** defines the speed at which the PTZ will move from one key point to the next.

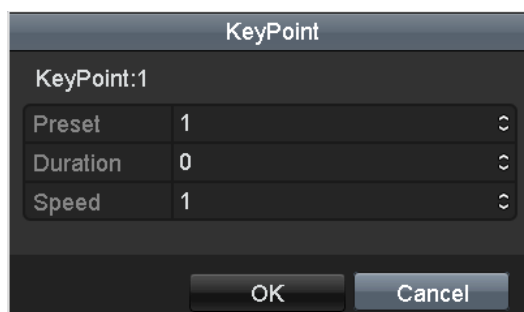






Figure 4. 7 Key Point Configuration

5. Click **OK** to save the key point to the patrol.

Repeat the above steps to add more key points.

Click the  icon to delete the corresponding key point, and click the trash icon  to delete all the key points.

Select a key point, then click  or  button to adjust the order of the key points.

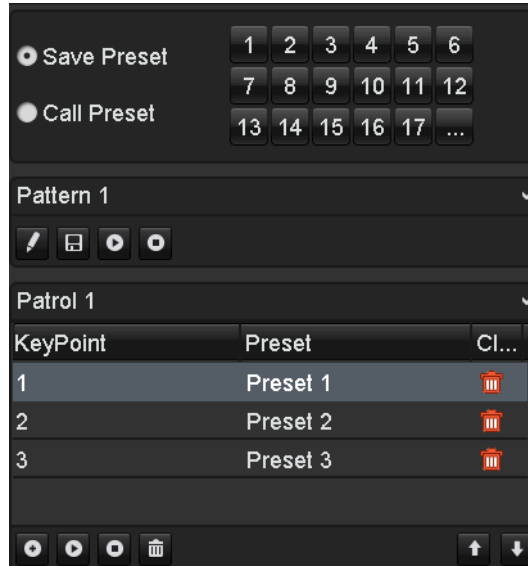


Figure 4. 8 Key Points Deletion



4.2.4 Calling Patrols

Purpose:

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

Calling patrol in the PTZ setting interface:

Steps:

1. In the PTZ setting interface.
Menu> Camera> PTZ> More Settings
2. Select the patrol number, and then click  to call the patrol.
3. Click  to stop it.

Calling patrol in live view mode:

Steps:



1. Press PTZ control on the front panel or on the remote, or click PTZ Control icon  on the quick setting toolbar, to show the PTZ control toolbar.
2. Choose **Patrol** on the control bar.
3. Double click the patrol or select the patrol and click  to call it.



Figure 4. 9 PTZ Toolbar- Patrol

4.2.5 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>More Settings
2. Choose pattern number in the option box.



Figure 4. 10 PTZ- Pattern

3. Click  and use your mouse to drag the image or click the eight directional buttons in the control box under the image to move the PTZ camera.
The movement of the PTZ is recorded as the pattern.
4. Click  to save the pattern.



4.2.6 Calling Patterns

Purpose:

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

Calling pattern in the PTZ setting interface

Steps:

1. Enter the PTZ Control interface.
Menu>Camera>PTZ>More Settings
2. Select the pattern number.
3. Click , then the PTZ moves according to the pattern. Click  to stop it.

Call pattern in live view mode

Steps:




1. In the live view mode, press PTZ control on the front panel or on the remote control, or click PTZ Control icon  on the quick setting toolbar.
2. And then choose **Pattern** on the control bar.
3. Double click the pattern or select the pattern and click  to call it.



Figure 4. 11 PTZ Toolbar- Pattern

4.3 PTZ Control Toolbar

In the Live View mode, you can press the PTZ Control button on the front panel or on the remote control, or

choose the PTZ Control icon  to enter the PTZ toolbar.

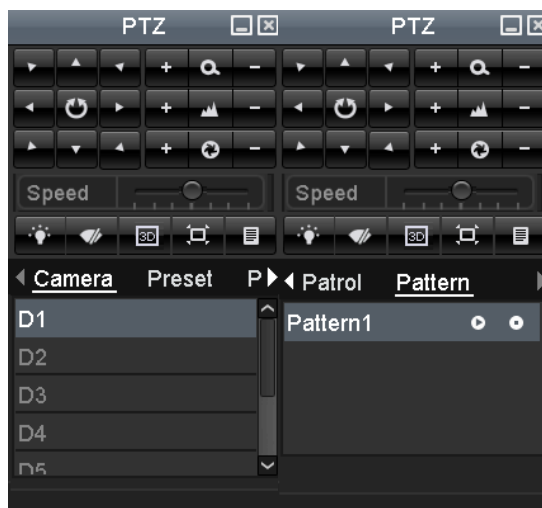




















Figure 4. 12 PTZ Toolbar

Table 4. 1 Description of the PTZ toolbar icons

Icon	Description	Icon	Description	Icon	Description
	Direction button and the 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		Preset
	Patrol		Pattern		Menu
	Previous item		Next item		Start pattern/patrol
	Stop the patrol or pattern movement		Minimize windows		Exit

Chapter 5 Record Settings

5.1 Configuring Encoding Parameters

Purpose:

By configuring the encoding 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)

L...	Capacity	Status	Property	Type	Free Space	Gr...	Edit	D...
5	76,319MB	Normal	R/W	Local	33,792MB	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) If the HDD mode is *Quota*, please set the maximum record capacity and maximum picture capacity. For detailed information, see *Chapter Configuring Quota Mode*.
- 3) If the HDD mode is **Group**, you should set the HDD group. For detailed information, see *Chapter Configuring HDD Group for Recording*.

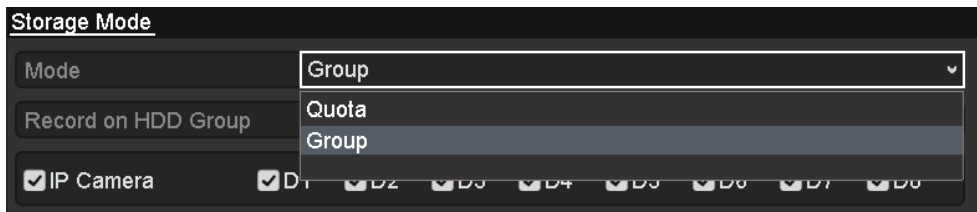


Figure 5. 2 HDD- Advanced

Steps:

1. Enter the Record settings interface to configure the encoding parameters:

Menu>Record>Encoding

Camera	IP Camera 1	
Encoding Parameters	Main Stream(Normal)	Main Stream(Event)
Stream Type	Video & Audio	Video & Audio
Resolution	1280*720(HD720P)	1280*720(HD720P)
Bitrate Type	Constant	Constant
Video Quality	Higher	Higher
Frame Rate	10fps	10fps
Max. Bitrate Mode	General	General
Max. Bitrate(Kbps)	512	512
Max. Bitrate Range Reco...	1023~1706(Kbps)	1023~1706(Kbps)
Pre-record	5s	
Post-record	5s	
Expired Time (day)	0	
Record Audio	<input checked="" type="checkbox"/>	

Figure 5. 3 Record Parameters

2. Encoding 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.

- **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.
- **Redundant Record:** Enabling redundant record means you save the record in the redundant HDD. See *Chapter Configuring Redundant Recording*.
- **Record Audio:** Check the checkbox to enable or disable audio recording.

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

Note: The redundant record is to decide whether you want the camera to save the record files in the redundant HDD. You must configure the redundant HDD in HDD settings. For detailed information, see *Chapter 12.4.2 Setting HDD Property*.

3. Encoding Parameters Settings for Sub-stream

1) Enter the Sub-stream tab page.

Camera	IP Camera 1
Encoding Parameters	Main Stream(Normal)
Stream Type	Video & Audio
Resolution	1280*720(HD720P)
Bitrate Type	Constant
Video Quality	Higher
Frame Rate	10fps
Max. Bitrate Mode	General
Max. Bitrate(Kbps)	512
Max. Bitrate Range Reco...	1023~1706(Kbps)

Figure 5. 4 Sub-stream Encoding

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

5.2 Configuring Record Schedule

Purpose:

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

Steps:

1. Enter the Record Schedule interface.
Menu>Record>Schedule
2. Configure Record Schedule
 - 1) Select Record Schedule.

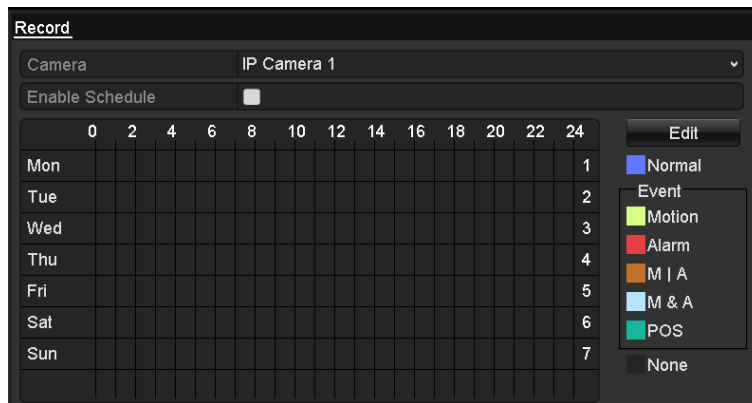


Figure 5. 5 Record Schedule

- 2) Choose the camera you want to configure.
- 3) Select the check box after the **Enable Schedule** item.
- 4) Click **Edit** button or click on the color icon under the edit button and draw the schedule line on the panel.

Edit the schedule:

- I. In the message box, you can choose the day to which you want to set schedule.

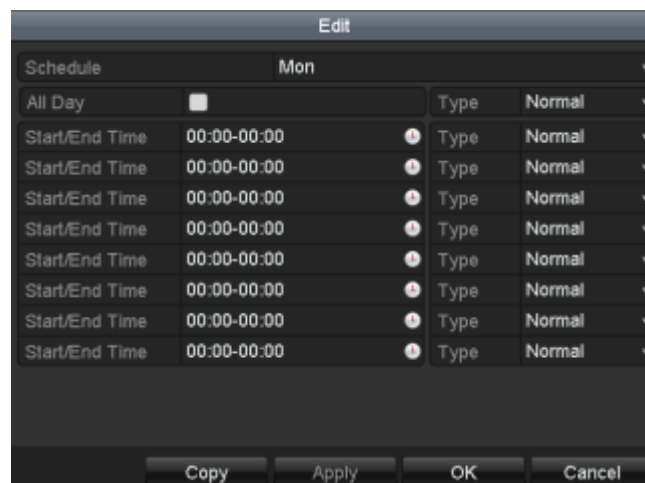



Figure 5. 6 Recording Schedule Interface

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.

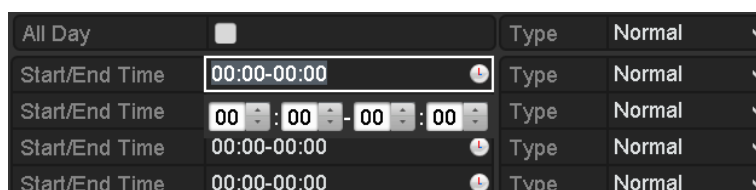


Figure 5. 7 Edit Schedule

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

Note: Up to 8 periods can be configured for each day. And the time periods can't be overlapped each other.

Repeat the above edit schedule steps to schedule recording for other days in the week. If the schedule can also be applied to other days, click **Copy**.

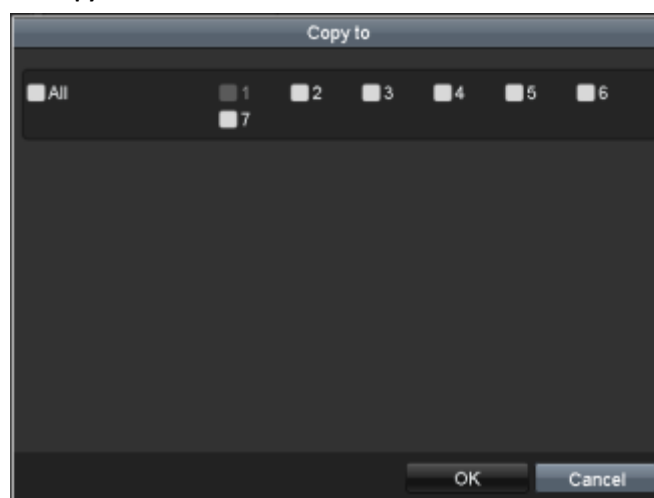


Figure 5. 8 Copy Schedule to Other Days

- IV. Click **OK** to save setting and back to upper level menu.
 V. Click **Apply** in the Record Schedule interface to save the settings.

Draw the schedule:

Click on the color icons, you can choose the schedule type as normal or event.

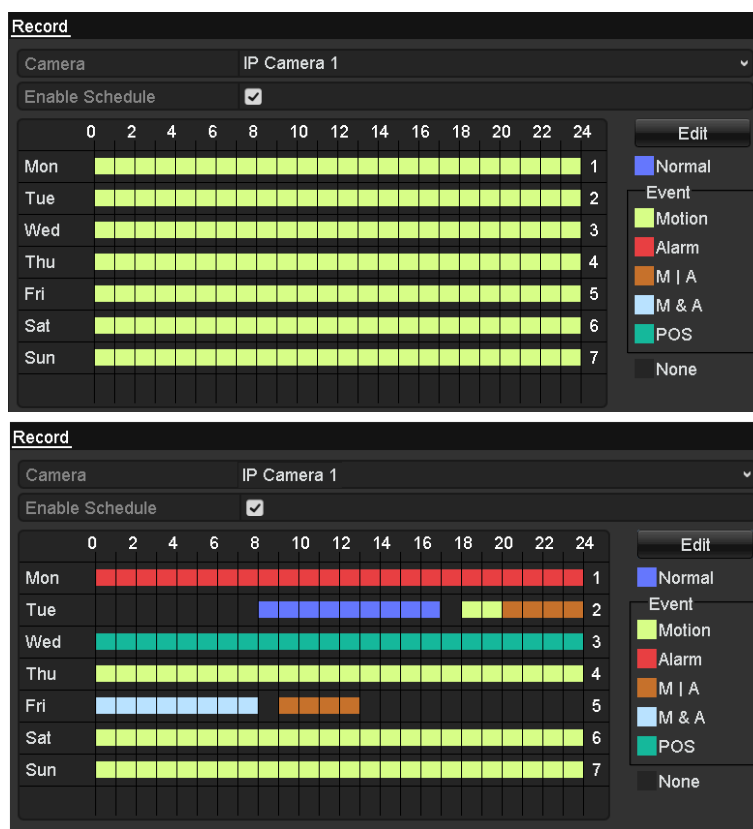


Figure 5. 9 Draw the Schedule

Descriptions of the color icons are shown in the figure below.

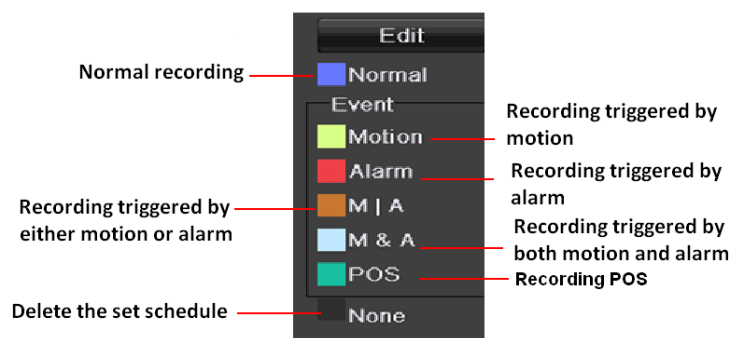


Figure 5. 10 Descriptions of the color icons

Click the **Apply** button to validate the settings.

If the settings can also be used to other channels, click **Copy**, and then choose the channel to which you want to copy.

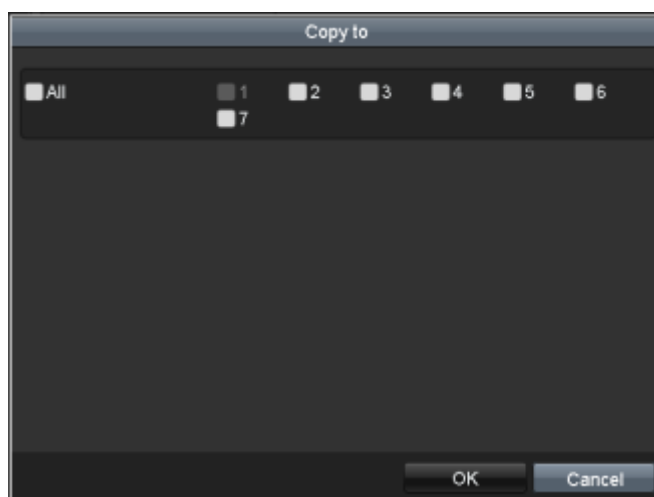


Figure 5. 11 Copy Schedule to Other Channels

5.3 Configuring Motion Detection Record

Purpose:

Follow the steps to set the motion detection parameters. 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, audio 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



Figure 5. 12 Motion Detection

2. Configure Motion Detection:

- 1) Choose camera you want to configure.
- 2) Check the checkbox after **Enable Motion Detection**.
- 3) Drag and draw the area for motion detection by mouse. 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. 13 Motion Detection- Mask

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

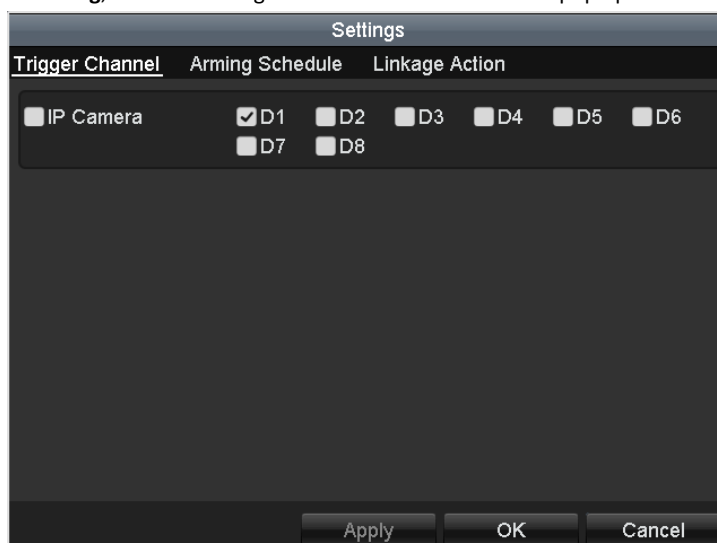


Figure 5. 14 Motion Detection Settings

- 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 *Chapter Configuring Record Schedule*.

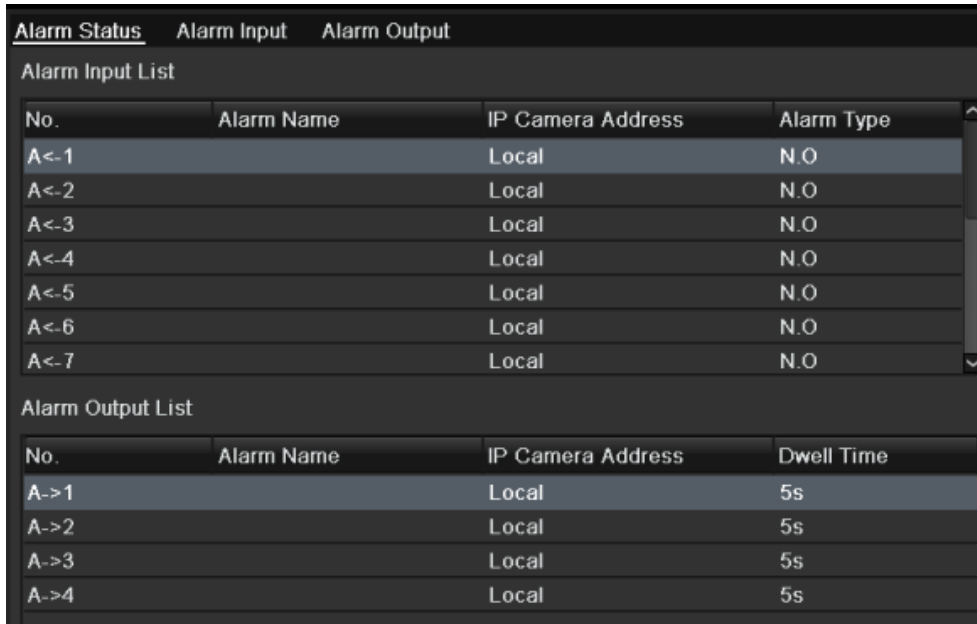
5.4 Configuring Alarm Triggered Record

Purpose:

Follow the procedure to configure alarm triggered recording.

Steps:

1. Enter the Alarm setting interface.
Menu> Configuration> Alarm



The screenshot shows the 'Alarm Settings' interface with three tabs: 'Alarm Status', 'Alarm Input', and 'Alarm Output'. The 'Alarm Input List' table is as follows:

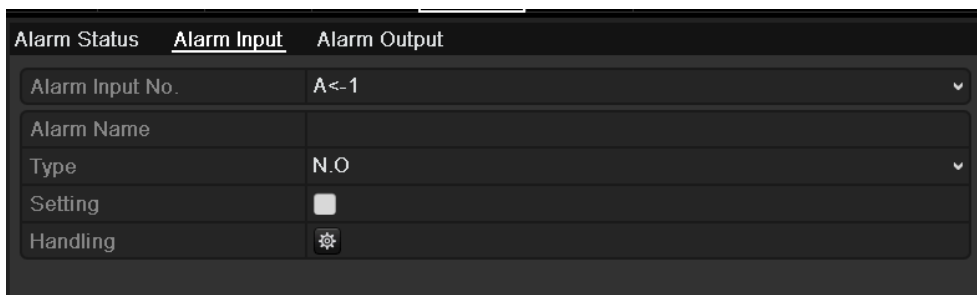
No.	Alarm Name	IP Camera Address	Alarm Type
A<-1		Local	N.O
A<-2		Local	N.O
A<-3		Local	N.O
A<-4		Local	N.O
A<-5		Local	N.O
A<-6		Local	N.O
A<-7		Local	N.O

The 'Alarm Output List' table is as follows:

No.	Alarm Name	IP Camera Address	Dwell Time
A->1		Local	5s
A->2		Local	5s
A->3		Local	5s
A->4		Local	5s

Figure 5. 15 Alarm Settings

2. Click **Alarm Input**.



The screenshot shows the 'Alarm Settings- Alarm Input' configuration form with the following fields:

Alarm Status	Alarm Input	Alarm Output
Alarm Input No.	A<-1	
Alarm Name		
Type	N.O	
Setting	<input type="checkbox"/>	
Handling		

Figure 5. 16 Alarm Settings- Alarm Input

- 1) Select Alarm Input number and configure alarm parameters.
- 2) Choose N.O (normally open) or N.C (normally closed) for alarm type.
- 3) Check the checkbox for Setting .
- 4) Click **Handling**.

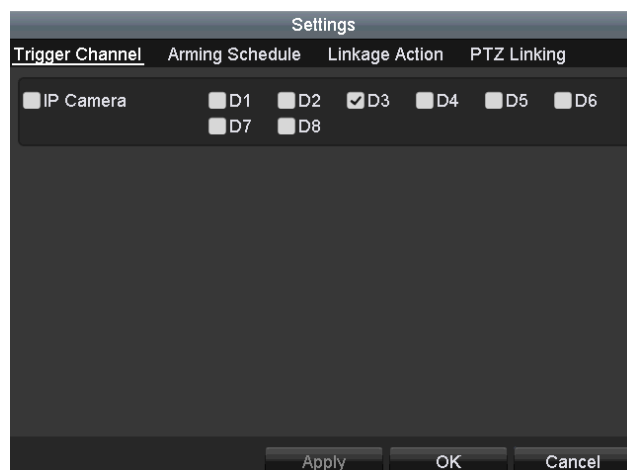


Figure 5. 17 Alarm Setting

- 5) Choose the alarm triggered recording channel.
- 6) Check the checkbox to select channel.
- 7) Click **Apply** to save settings.
- 8) Click **OK** to back to the upper level menu.

Repeat the above steps to configure other alarm input parameters.

If the settings can also be applied to other alarm inputs, click **Copy** and choose the alarm input number.

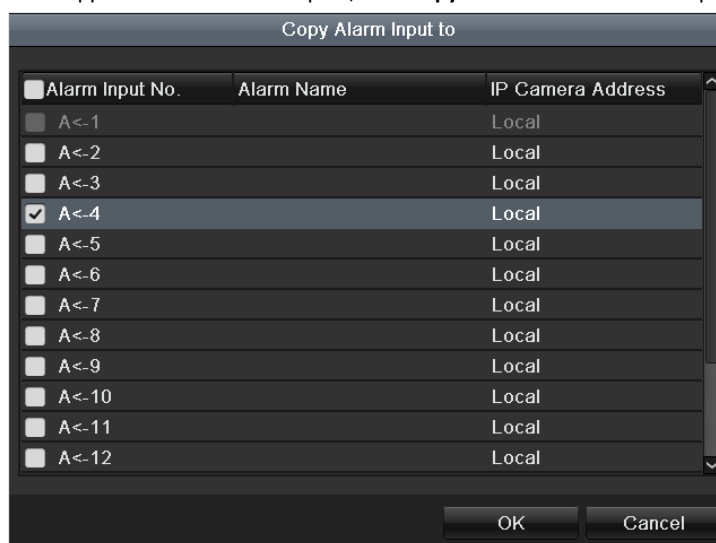


Figure 5. 18 Copy Alarm Input

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

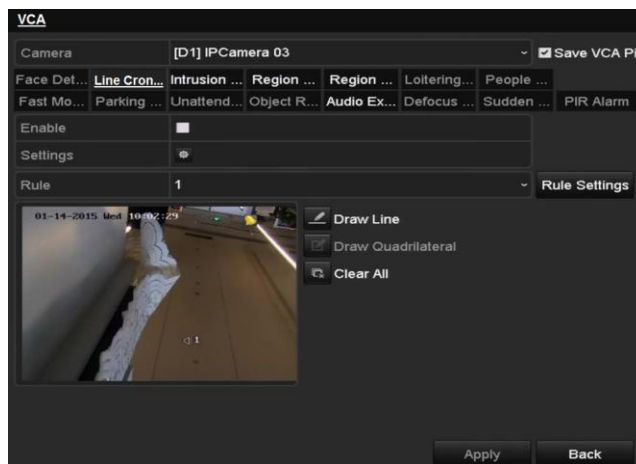



Figure 5. 19 VCA Settings

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

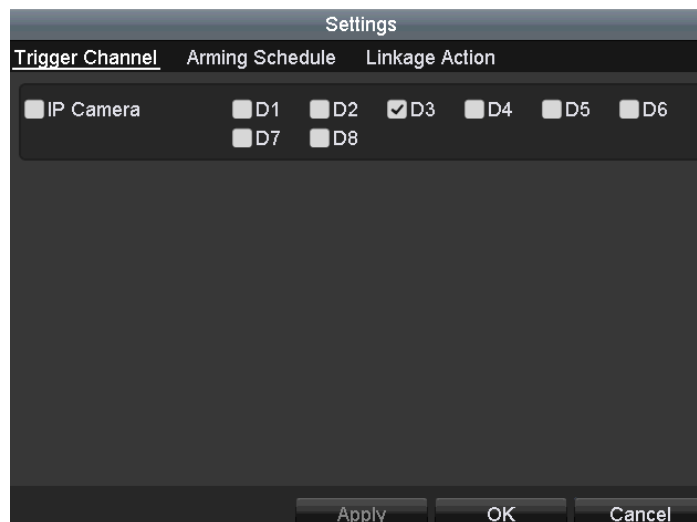


Figure 5. 20 Set Trigger Camera of VCA Alarm



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 *Chapter 5.2 Configuring Record Schedule*.

5.6 Manual Record

Purpose:

Follow the steps to set parameters for the manual record. The manual recording is prior to the scheduled recording.

Steps:

1. Enter the Manual settings interface.
Menu> Manual
Or press the **REC** button on the remote control.

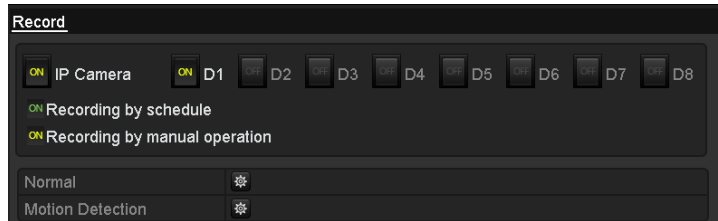


Figure 5. 21 Manual Record

2. Enabling Manual Record
 - 1) Select **Record** on the left bar.
 - 2) Click the status button before camera number to change **OFF** to **ON**.
3. Disable manual record.
Click the status button to change **ON** to **OFF**.
4. Start all-day normal recording or all-day motion detection recording of all channels.
 - 1) Click for **Continuous** or **Motion Detection**.

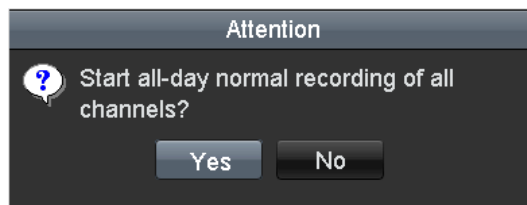


Figure 5. 22 Continuous Recording

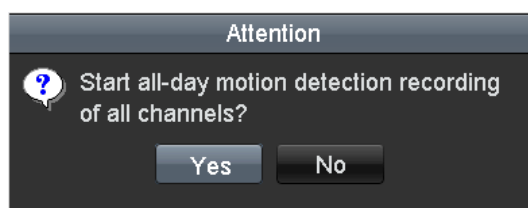


Figure 5. 23 Motion Detection Recording

- 2) Click **Yes** to enable all-day continuous recording or all-day motion detection recording of all channels.

5.7 Configuring Holiday Record

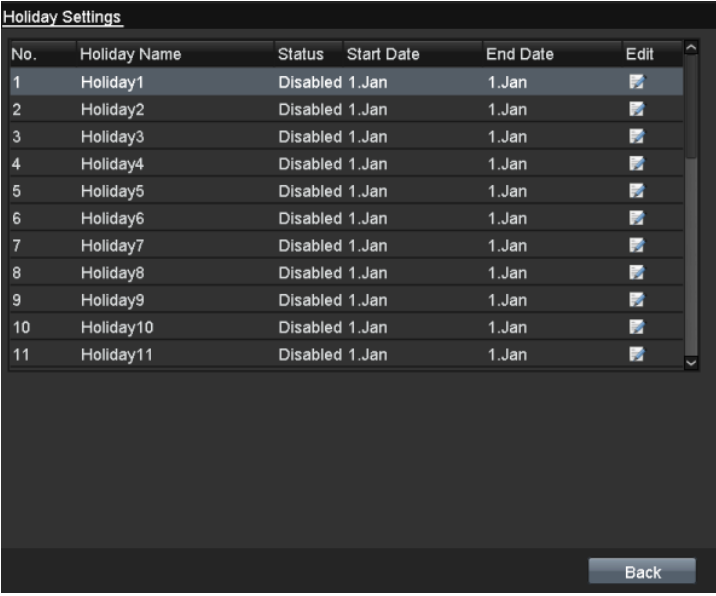
Purpose:

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

Steps:

1. Enter the Record setting interface.

Menu>Record> Holiday



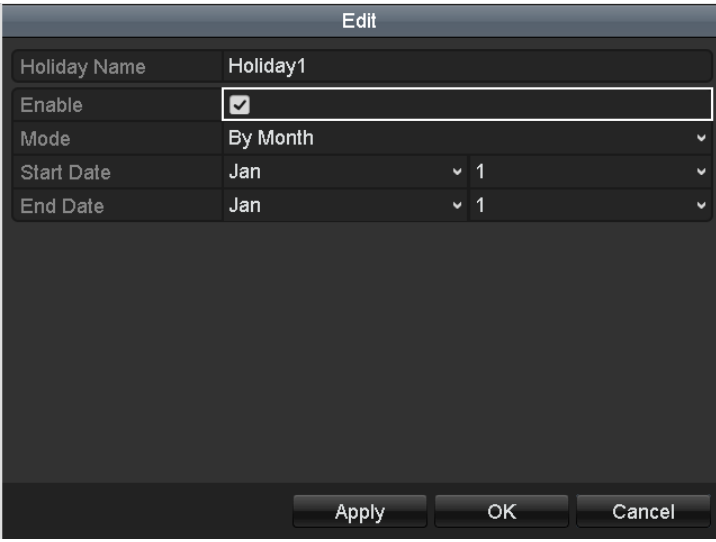
The screenshot shows the 'Holiday Settings' window with a table of holiday records. The table has columns for No., Holiday Name, Status, Start Date, End Date, and Edit. There are 11 rows, all with 'Disabled' status and '1.Jan' for both start and end dates. Each row has an 'Edit' icon in the last column. A 'Back' button is located at the bottom right of the window.

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. 24 Holiday Settings

2. Enable Edit Holiday schedule.

- 1) Click  to enter the Edit interface.



The screenshot shows the 'Edit' window for 'Holiday1'. It has fields for 'Holiday Name' (Holiday1), 'Enable' (checked checkbox), 'Mode' (By Month), 'Start Date' (Jan 1), and 'End Date' (Jan 1). There are 'Apply', 'OK', and 'Cancel' buttons at the bottom.

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

Figure 5. 25 Edit Holiday Settings

- 2) Check the checkbox after **Enable Holiday**.

- 3) Select Mode from the dropdown list.
There are three different modes for the date format to configure holiday schedule.
 - 4) Set the start and end date.
 - 5) Click **Apply** to save settings.
 - 6) Click **OK** to exit the Edit interface.
3. Enter Record Schedule settings interface (Menu> Record> Schedule>Record). For detailed information about record schedule settings, refer to step 2 in *Chapter 5.2 Configuring Record Schedule*.

Note: You need to select schedule type as Holiday or draw the schedule for the Holiday.

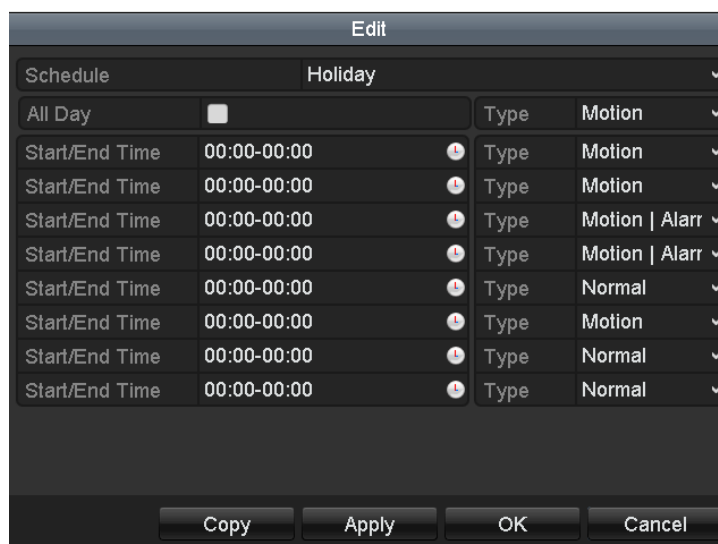


Figure 5. 26 Edit Schedule- Holiday

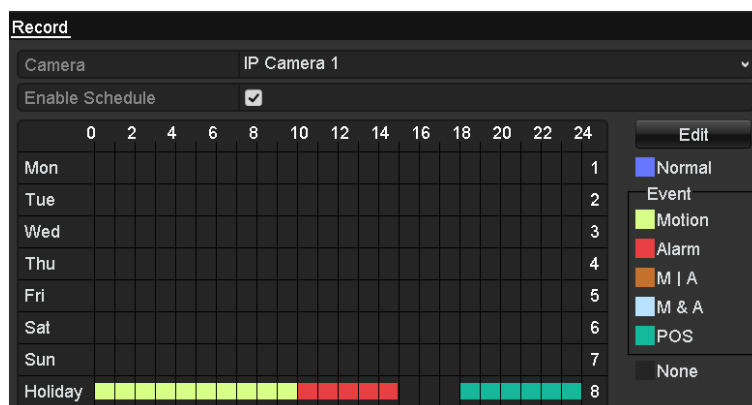


Figure 5. 27 Draw Schedule- Holiday

5.7 Configuring POS Record

Purpose:

Follow the steps to set parameters for the POS record..

Steps:

1. Enter Schedule settings interface.
Menu> Record> Schedule>Record Schedule

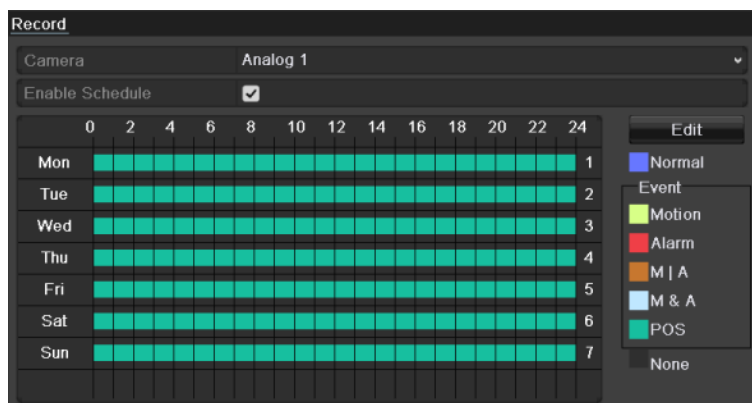


Figure 5. 28 Draw Schedule- Holiday

- 1) Check the checkbox after the **Enable Schedule** item.
- 2) Click **Edit**.

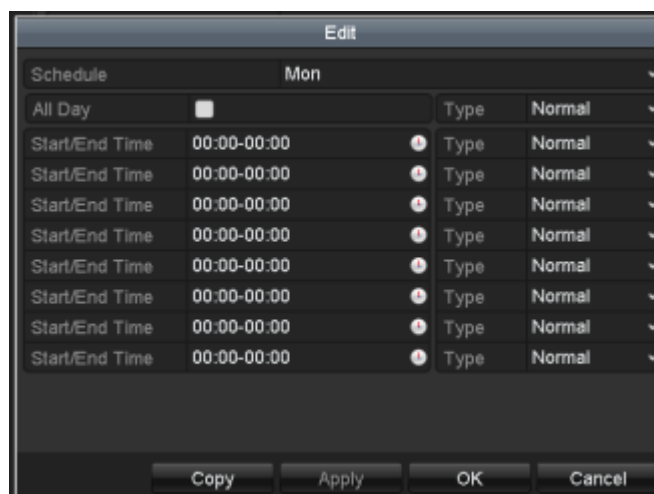


Figure 5. 29 Edit Schedule-POS

- 3) In the message box, you can choose the day to which you want to set schedule.
- 4) Set the **Type** as **POS**.
- 5) To schedule an all-day recording, check the checkbox after the **All Day** item.

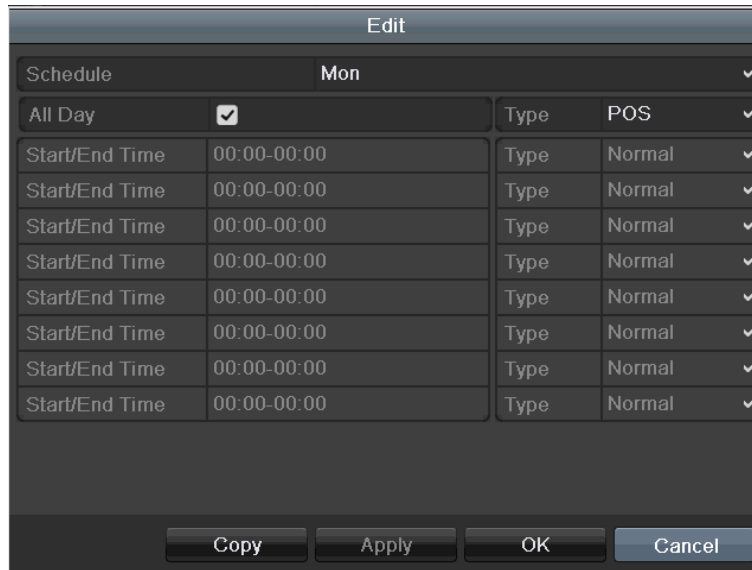


Figure 5. 30 Edit Schedule- All Day

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

Note: Up to 8 periods can be configured for each day. And the time periods can't be overlapped each other.

Repeat the above steps3)-6) to schedule motion detection triggered recording for all the week. If the schedule can also be set to other days, click **Copy**.

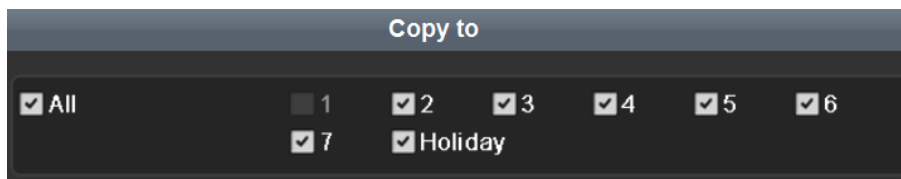


Figure 5. 31 Copy Schedule to Other Days

7) Click **OK** to back to upper level menu.

If you can to copy the same schedule settings to other camera (s), click **Copy** to enter the Copy Camera interface, and then select the camera (s) you want to copy.

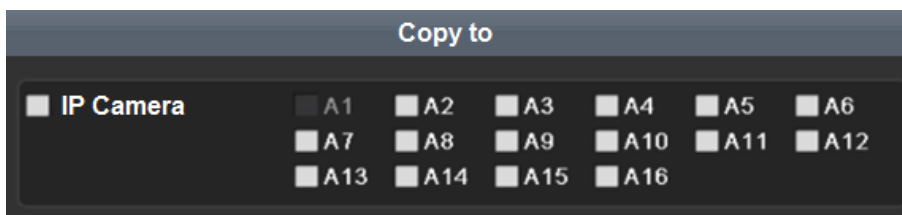


Figure 5. 32 Copy Schedule to Other Channels

5.8 Configuring Redundant Recording

Purpose:

Enabling redundant recording, which means saving the record files not only in the R/W HDD but also in the redundant HDD, will effectively enhance the data safety and reliability. .


Steps:

1. Enter HDD Information interface.

Menu> HDD

HDD Information							
<input type="checkbox"/> L...	Capacity	Status	Property	Type	Free Space	Gr...	Edit D...
<input type="checkbox"/> 4	76,319MB	Normal	R/W	Local	74,752MB	1	[-]

Figure 5. 33 HDD General

2. Select the **HDD** and click  to enter the Local HDD Settings interface.
 - 1) Set the HDD property to Redundancy.

Local HDD Settings	
HDD No.	4
HDD Property	<input type="radio"/> R/W <input type="radio"/> Read-only <input checked="" type="radio"/> Redundancy
Group	<input checked="" type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4 <input type="radio"/> 5 <input type="radio"/> 6 <input type="radio"/> 7 <input type="radio"/> 8 <input type="radio"/> 9 <input type="radio"/> 10 <input type="radio"/> 11 <input type="radio"/> 12 <input type="radio"/> 13 <input type="radio"/> 14 <input type="radio"/> 15 <input type="radio"/> 16
HDD Capacity	76,319MB
<input type="button" value="Apply"/> <input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Figure 5. 34 HDD General-Editing

- 2) Click **Apply** to save the settings.
- 3) Click **OK** to back to the upper level menu.

Note: You must set the Storage mode in the HDD advanced settings to Group before you set the HDD property to Redundant. For detailed information, please refer to *Chapter 12.4 Managing HDD Group*. There should be at least another HDD which is in Read/Write status.

3. Enter the Record setting interface.

Menu> Record> Parameters

- 1) Select **Parameters** tab.

Camera	IP Camera 1	
Encoding Parameters	Main Stream(Normal)	Main Stream(Event)
Stream Type	Video & Audio	Video & Audio
Resolution	1280*720(HD720P)	704*576(4CIF)
Bitrate Type	Constant	Variable
Video Quality	Medium	Medium
Frame Rate	10fps	25fps
Max. Bitrate Mode	General	General
Max. Bitrate(Kbps)	512	2048
Max. Bitrate Range Reco...	1197~1996(Kbps)	1344~2240(Kbps)
Pre-record	5s	
Post-record	5s	
Expired Time (day)	0	
Redundant Record	<input type="checkbox"/>	
Record Audio	<input checked="" type="checkbox"/>	

Figure 5. 35 Encoding Record

- 2) Select Camera you want to configure in the drop-down list.
- 3) Check the checkbox of **Redundant Record**.
- 4) Click **Apply** to save settings and back to the upper level menu.

Repeat the above steps for configuring other channels.

5.9 Configuring HDD Group for Recording

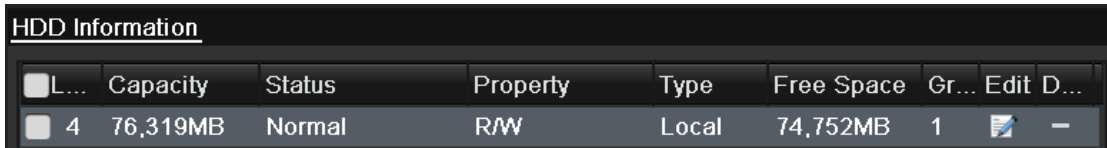
Purpose:

You can group the HDDs and save the record files in certain HDD group.

Steps:

1. Enter HDD setting interface.

Menu>HDD



L...	Capacity	Status	Property	Type	Free Space	Gr...	Edit D...
4	76,319MB	Normal	R/W	Local	74,752MB	1	


Figure 5. 36 HDD General

2. Select **Advanced** on the left bar.



Figure 5. 37 Storage Mode

Check whether the storage mode of the HDD is Group. If not, set it to Group. For detailed information, please refer to *Chapter 12.4 Managing HDD Group*.

3. Select **General** in the left bar.
Click  to enter editing interface.
4. Configuring HDD group.
 - 1) Choose a group number for the HDD group.
 - 2) Click **Apply** and then in the pop-up message box, click **Yes** to save your settings.
 - 3) Click **OK** to back to the upper level menu.

Repeat the above steps to configure more HDD groups.

5. Choose the Channels which you want to save the record files in the HDD group.
 - 1) Select **Advanced** on the left bar.
 - 2) Choose Group number in the dropdown list of **Record on HDD Group**
 - 3) Check the channels you want to save in this group.
 - 4) Click **Apply** to save settings.

Note: After having configured the HDD groups, you can configure the recording settings following the procedure provided in *Chapter 5.2-5.7*.

5.10 Files Protection

Purpose:

You can lock the recorded files or set the HDD property to Read-only to protect the record files from being overwritten.

Protect file by locking the record files:

Steps:

1. Enter Playback setting interface.

Menu> Export>Normal

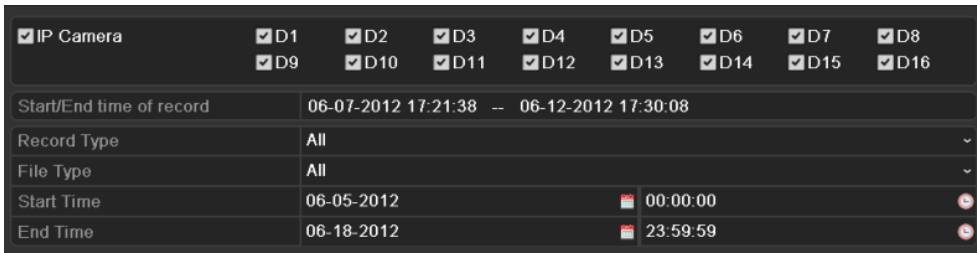


Figure 5. 38 Playback

2. Select the channels you want to investigate by checking the checkbox to .
3. Configure the record type, file type start/end time.
4. Click **Search** to show the results.

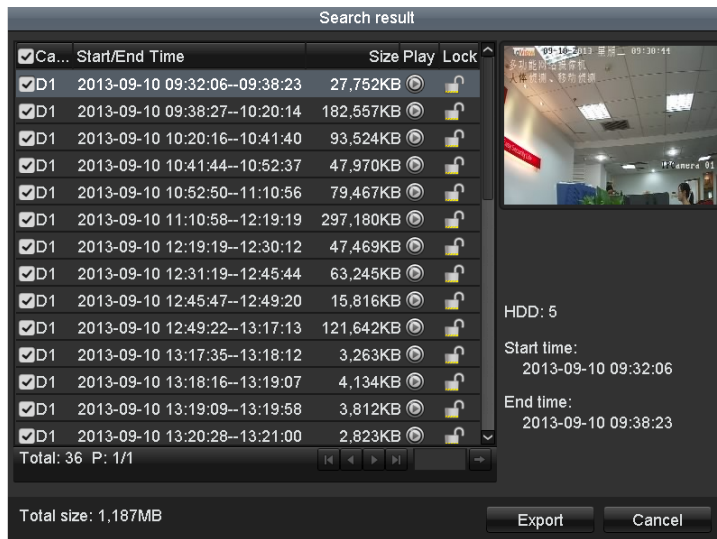


Figure 5. 39 Playback- Search Result

5. Protect the record files.
 - 1) Find the record files you want to protect, and then click the icon which will turn to , indicating that the file is locked.

Note: The record files of which the recording is still not completed can't be locked.
 - 2) Click to change it to to unlock the file and the file is not protected.

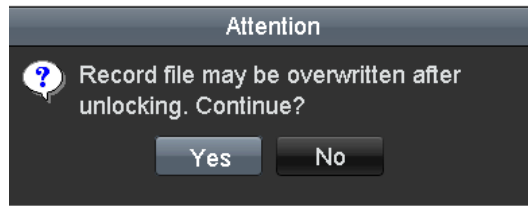


Figure 5. 40 Unlocking Attention

Protect file by setting HDD property to Read-only

Steps:

1. Enter HDD setting interface.
Menu> HDD

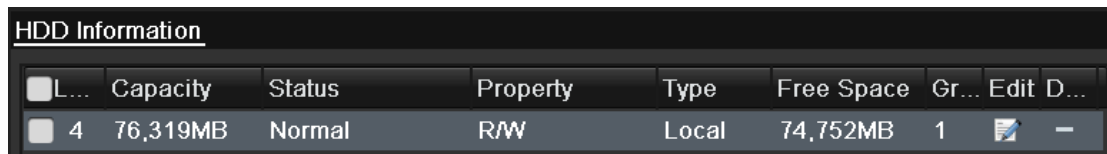


Figure 5. 41 HDD General

2. Click to edit the HDD you want to protect.

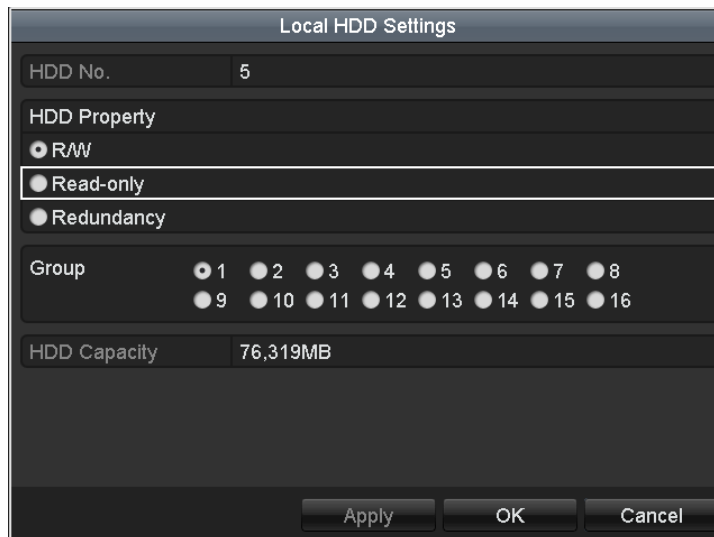


Figure 5. 42 HDD General- Editing

Note: To edit HDD property, you need to set the storage mode of the HDD to Group. See *Chapter Managing HDD Group*.

3. Set the HDD property to Read-only.
4. Click **OK** to save settings and back to the upper level menu.

Notes:

1. You can't save any files in a Read-only HDD. If you want to save files in the HDD, change the property to R/W.
2. If there is only one HDD and is set to Read-only, the NVR can't record any files. Only live view mode is available.
3. If you set the HDD to Read-only when the NVR is saving files in it, then the file will be saved in next R/W HDD. If there is only one HDD, the recording will be stopped.

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.

● **OPTION 1:**

Choose a channel in live view mode using the mouse and click the  button in the quick setting toolbar.

Note: In the instant playback mode, only record files recorded during the last five minutes on this channel will be played back.



Figure 6. 1 Instant Playback Interface

● **OPTION 2:**

1. Enter the Playback interface.


Mouse: right click a channel in live view mode and select  from the menu.



Figure 6. 2 Right-click Menu under Live View

Front Panel: press **PLAY** button to play back record files of the channel under single-screen live view mode.

Under multi-screen live view mode, the recorded files of the top-left channel will be played back.

Note: Pressing numerical buttons will switch playback to the corresponding channels during playback process.

2. Playback management.

The toolbar in the bottom part of Playback interface can be used to control playing progress, as shown in Figure 6. 3.



Figure 6. 3 Playback Interface

Click the channel(s) to execute simultaneous playback of multiple channels.



Figure 6. 4 Toolbar of Playback

Note: The 2013-09-10 16:18:14 -- 2013-09-10 18:44:22 indicates the start/end time of the record.

Table 6. 1 Detailed Explanation of Playback Toolbar

Button	Operation	Button	Operation	Button	Operation	Button	Operation
	Audio on /Mute		Start/Stop clipping		Add default tag		Add customized tag
	Tag management		Digital Zoom		Smart Search		Text Show
	Pause play/ Play/ Single-frame play		Pause reverse play/ Reverse play/ Single-frame reverse play		Stop		30s forward
	30s reverse		Slow forward		Fast forward		Previous day
	Next day		Scaling up/down time bar		Process bar		Full Screen
	Exit		Video type				

Note: Playback progress bar: use the mouse to click any point of the progress bar or drag the progress bar to locate special frames.

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

Note:

If there are record files for that camera in that day, in the calendar, the icon for that day is displayed as **10**.

Otherwise it is displayed as **11**. And the selected date is surrounded by a white rectangle, which is displayed as **10**.

In the Playback interface:

The toolbar in the bottom part of Playback interface can be used to control playing process, as shown in Figure 6.

6.



Figure 6. 6 Interface of Playback by Time



Figure 6. 7 Toolbar of Playback by Time

Note: The **2013-09-10 16:18:14 -- 2013-09-10 18:44:22** indicates the start/end time of the record.

Table 6. 2 Detailed Explanation of Playback-by-time Interface

Button	Operation	Button	Operation	Button	Operation	Button	Operation
	Audio on /Mute		Start/Stop clipping		Add default tag		Add customized tag
	Tag management		Digital Zoom		Smart Search		Text Show
	Pause play/ Play/ Single-frame play		Pause reverse play/ Reverse play/ Single-frame reverse play		Stop		30s forward
	30s reverse		Slow forward		Fast forward		Previous day
	Next day		Scaling up/down time bar		Process bar		Full Screen
	Exit		Video type				

Note:

Playback progress bar: use the mouse to click any point of the progress bar or drag the progress bar to locate special frames.

6.1.3 Playing Back by Event Search

Purpose:

Play back record files on 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.
3. Select **Alarm Input** or **Motion** as the event type, edit the Start time and End time.

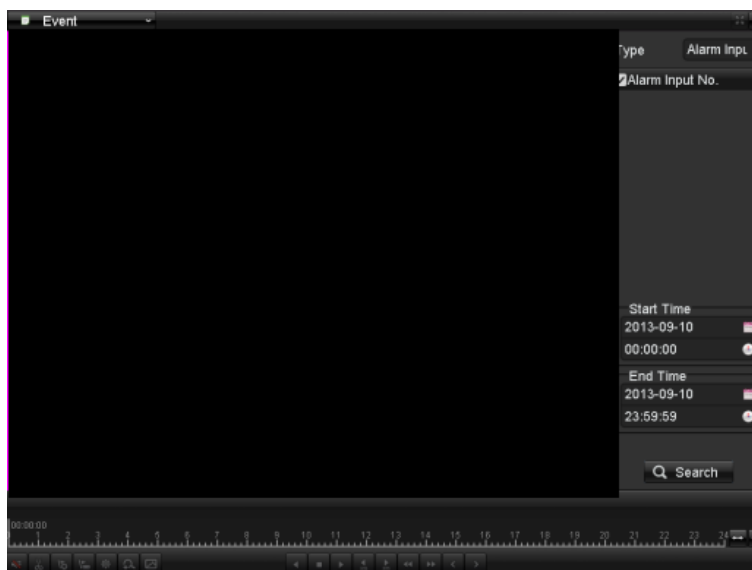


Figure 6. 8 Alarm Input Search Interface

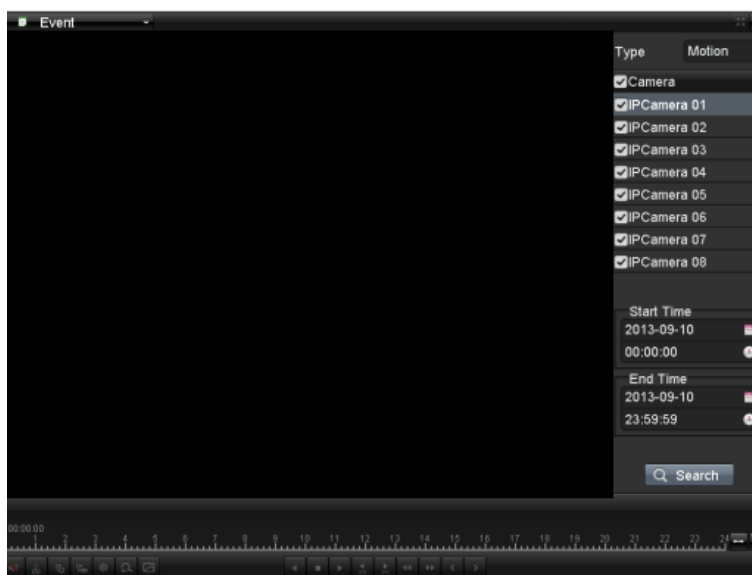


Figure 6. 9 Motion Search Interface

-
4. Click **Search** button to get the search result information. You may refer to the right-side bar for the result.

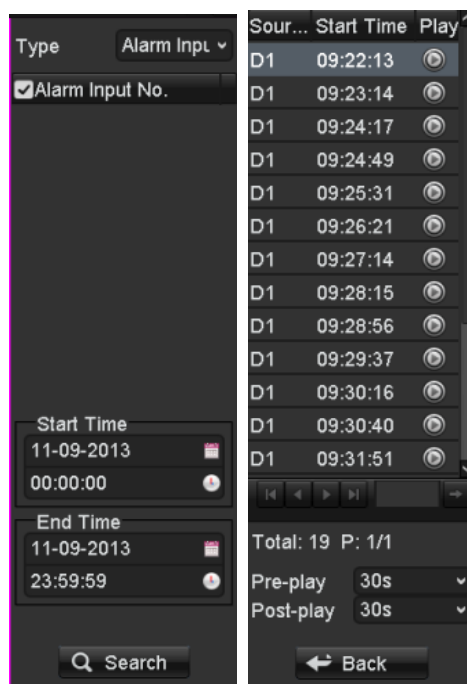




Figure 6. 10 Search Result Bar(Alarm In and Motion)

5. Click  button to play back the file.

Note:

1. Pre-play and post-play can be configured.
2. If the event is set to trigger the recording of multiple channels, clicking the  will pop up the Synch Playback interface. You can select the channels to play back synchronously.

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

6. Playback interface.

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



Figure 6. 11 Interface of Playback by Event



Figure 6. 12 Toolbar of Playback by Event

Table 6. 3 Detailed Explanation of Playback-by-event Toolbar

Button	Operation	Button	Operation	Button	Operation	Button	Operation
	Audio on /Mute		Start/Stop clipping		Add default tag		Add customized tag
	Tag management		Digital Zoom		Smart Search		Pause reverse play/ Reverse play/ Single-frame reverse play
	Pause play/ Play/ Single-frame play		Stop		30s forward		30s reverse
	Slow forward		Fast forward		Previous day		Next day
	Scaling up/down time bar		Process bar		Full Screen		Exit
	Video type						

Note:

Playback progress bar: use the mouse to click any point of the progress bar or drag the progress bar to locate special frames.

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.


Before playing back by tag:

1. Enter Playback interface.
Menu>Playback
2. Search and play back the record file(s). Refer to *Chapter 6.1.1* for the detailed information about searching and playback of the record files.




Figure 6. 13 Interface of Playback by Time

Click  button to add default tag.

Click  button to add customized tag and input tag name.

Note: Max. 64 tags can be added to a single video file.

3. Tag management.

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

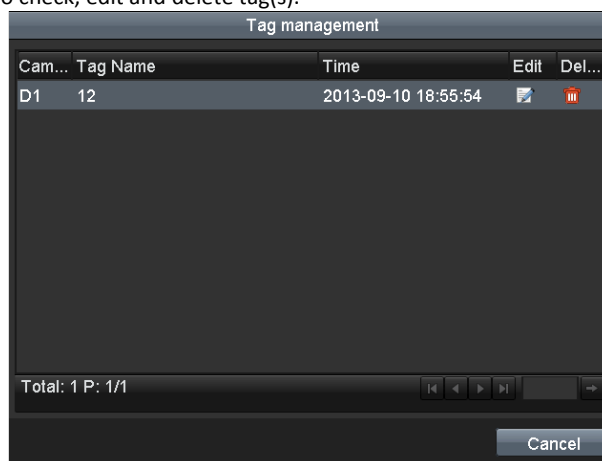


Figure 6. 14 Tag Management Interface

Steps:

1. Select the **Tag** from the drop-down list in the Playback interface.
2. Choose channels, edit start time and end time, and then click Search to enter Search Result interface.

Note:

You can enter keyword in the textbox to search the tag on your command.

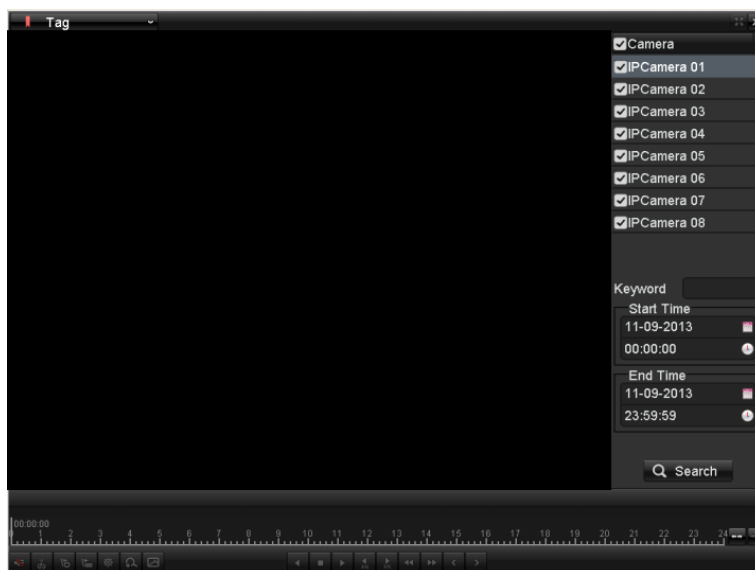



Figure 6. 15 Video Search by Tag

3. Click  button to play back the file.
You can click the **Back** button to back to the search interface.

Note:

Pre-play and post-play can be configured.



Figure 6. 16 Interface of Playback by Tag



Figure 6. 17 Toolbar of Playback by Tag

Table 6. 4 Detailed Explanation of Playback-by-tag Toolbar

Button	Operation	Button	Operation	Button	Operation	Button	Operation
	Audio on /Mute		Start/Stop clipping		Add default tag		Add customized tag
	Tag management		Digital Zoom		Smart Search		Pause reverse play/ Reverse play/ Single-frame reverse play
	Pause play/ Play/ Single-frame play		Stop		30s forward		30s reverse
	Slow forward		Fast forward		Previous day		Next day
	Scaling up/down time bar		Process bar		Full Screen		Exit
	Video type						

Note: Playback progress bar: use the mouse to click any point of the progress bar or drag the progress bar to locate special frames.

6.1.5 Playing Back by System Logs

Purpose:

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

Steps:

1. Enter Log Information interface.
Menu>Maintenance>Log Information
2. Click **Log Search** tab to enter Playback by System Logs.
Set search time and type and click **Search** button.



Figure 6. 18 System Log Search Interface

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

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

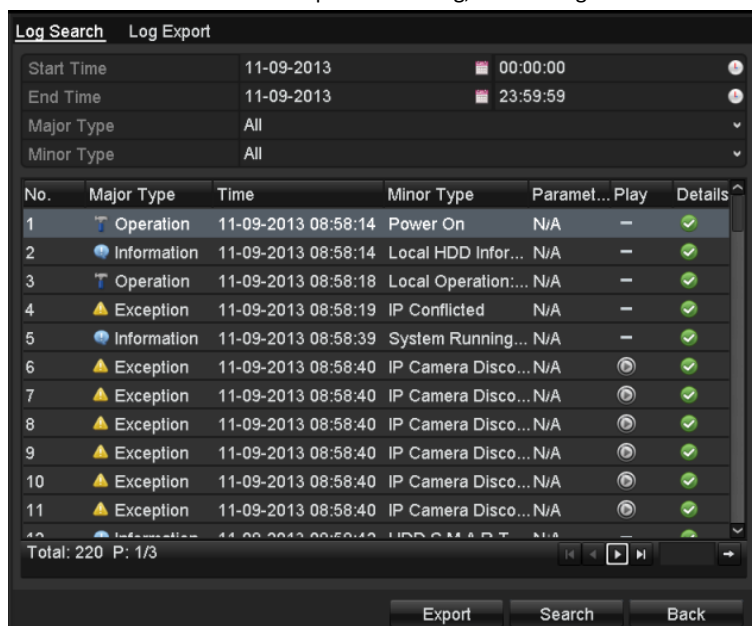


Figure 6. 19 Result of System Log Search

- Playback interface.

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



Figure 6. 20 Interface of Playback by Log

6.1.6 Playing Back External File

Purpose:

Perform the following steps to look up 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.
3. Select and click the  button to play back it.







Figure 6. 21 Interface of External File Playback

6.1.7 Playing Back POS

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 pos to search for record files and position time point.

Steps:

1. Enter the playback interface.
Menu>Playback
2. Click  and select  to enter the Event Playback interface.
3. Choose channels, edit the Start and End time, you can enter keyword in the textbox   to search the text on your command.

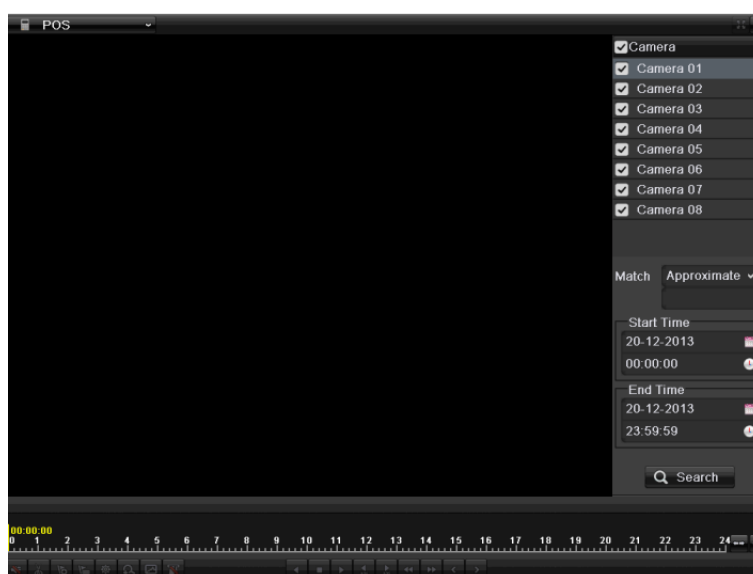


Figure 6. 22 Event Playback Interface-Alarm Input



Figure 6. 23 Exact match set

Note:“Match” condition can choose “Exact match” or “Approximate match”

“Approximate match”: you can enter specific keyword in the textbox, then it can search all the videos which include the keyword

“Exact match”: you can add logical and conditional statement to search the video you want.

4. Click Search to get the search result information listed in the right-side panel.

5. Click button to play back the record files.

You can click Back to return to the search interface.

Note: Pre-play and post-play can be configured for the alarm input triggered record files.

Pre-play: The time you set to play back before the event. For example, when an alarm triggered the recording at 10:00, if you set the pre-play time as 5 seconds, the video plays back from 9:59:55.

Post-play: The time you set to play back after the event. For example, when an alarm triggered the recording ends at 11:00, if you set the post-play time as 5 seconds, the video plays back till 11:00:05.

If there is only one channel is triggered by an alarm input, clicking button takes you to Full-screen Playback interface of this channel.

If several channels are triggered, clicking button takes you to the interface for checking checkbox to select one channel for playback or select multiple channels for synchronous playback.

Note: 4-ch, 8-ch, 16-ch devices support 8-ch, 16-ch and 16-ch synchronous playback respectively.

6. Playback interface.

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

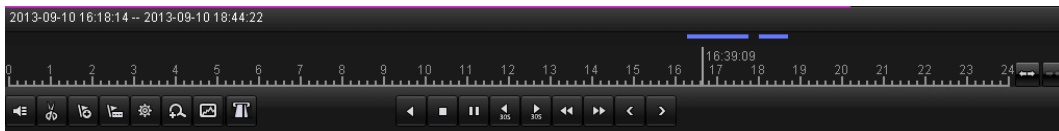


Figure 6. 24 Toolbar of Playback by POS

Table 6. 5 Detailed Explanation of Playback-by-event Interface

Button	Operation	Button	Operation	Button	Operation	Button	Operation
	Audio on /Mute		Start/Stop clipping		Add default tag		Add customized tag
	Tag management		Digital Zoom		Smart Search		Text Show
	Pause play/ Play/ Single-frame play		Pause reverse play/ Reverse play/ Single-frame reverse play		Stop		30s forward
	30s reverse		Slow forward		Fast forward		Previous day
	Next day		Scaling up/down time bar		Process bar		Full Screen
	Exit		Video type				

Notes: Playback progress bar: use the mouse to click any point of the progress bar or drag the progress bar to locate specific frames.

6.2 Auxiliary Functions of Playback

6.2.1 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:



- **Using a Mouse:**

Go to Playback interface.

If you choose playback of the record file: click button  until the speed changes to Single frame and one click on the playback screen represents playback of one frame.

If you choose reverse playback of the record file: click button  until the speed changes to Single frame and one click on the playback screen represents reverse playback of one frame. It is also feasible to use button  in toolbar.

- **Using the Front Panel:**

Rotate and hold the outer ring on Jog Shuttle counter clockwise (for 7700/8600 only) or click the  button to set the speed to Single frame. One click on  button, one click on the playback screen or Enter button on the front panel represents playback or reverse playback of one frame.

6.2.2 Smart Search

Purpose:

In order to locate motion detection event easily and accurately in the playback progress bar, you are allowed to analyze a certain area (scene) dynamically, and to get all of the related motion detection events that occurred in this area.

Note: The smart search function varies according to the camera connected to the NVR.

Before you start:

1. Log in the network camera by the web browser, and enable the Dynamic Analysis for Motion by checking the checkbox of it. You may enter the motion detection configuration interface by Configuration> Advanced Configuration> Events> Motion Detection.

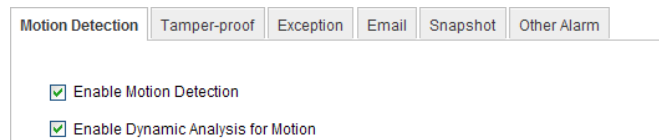


Figure 6. 25 Motion Detection Settings




2. Enable the motion detection function and set the arming area to the full screen in the NVR local menu. Please refer to *chapter 8.1* for details.

Steps:

1. Enter the Playback interface and play a record file. Refer to *Chapter 6.1.1* for the detailed information about searching and playback of the record files.



Figure 6. 26 Interface of Playback by Time

2. Click the  on the playback control toolbar to enter Smart Search mode.
3. Click and drag the mouse to draw area(s). You can click button  to set the full screen as target searching area. After drawing area(s), click button  to execute smart search in this area.

Note: Multi-area and full-screen searching modes are supported.

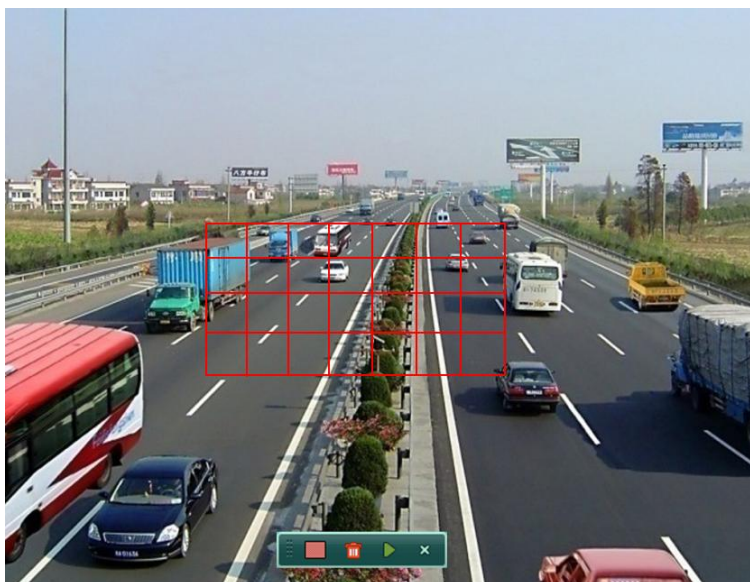



Figure 6. 27 Draw Area of Smart Search

The results of smart search will be marked as  in the progress bar.

The hidden list of record files display when moving the mouse to the right of the playback interface.



Figure 6. 28 Smart Search Result



Figure 6. 29 Toolbar of Smart Search Playback

Note: The **2013-09-10 16:18:14 -- 2013-09-10 18:44:22** indicates the start/end time of the record.

Table 6. 6 Detailed Explanation of Smart-search-playback Toolbar

Button	Operation	Button	Operation	Button	Operation	Button	Operation
	Audio on /Mute		Start/Stop clipping		Add default tag		Add customized tag
	Tag management		Digital Zoom		Smart Search		Pause reverse play/ Reverse play/ Single-frame reverse play
	Pause play/ Play/ Single-frame play		Stop		30s forward		30s reverse
	Slow forward		Fast forward		Previous day		Next day
	Scaling up/down time bar		Process bar		Full Screen		Exit
	Video type		Smart search result				

Note:

Playback progress bar: use the mouse to click any point of the progress bar or drag the progress bar to locate special frames.

6.2.3 Digital Zoom

Steps:


1. Click the  button on the playback control bar 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 6.30 Draw Area for Digital Zoom

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

6.2.4 Reverse Playback of Multi-channel

Purpose:


You can play back record files of multi-channel reversely. Up to 16-ch (with 1280*720 resolution) simultaneous reverse playback is supported; up to 4-ch (with 1920*1080P resolution) simultaneous reverse playback is supported and up to 1-ch (with 2560*1920 resolution) reverse playback is supported.

Steps:

1. Enter Playback interface.
Menu>Playback
2. Check more than one checkboxes to select multiple channels and click to select a date on the calendar.



Figure 6. 31 4-ch Synchronous Playback Interface

3. Click  to play back the record files reversely.

Chapter 7 Backup

7.1 Backing up Record Files

Before you start:

Please insert the backup device(s) into the device.

7.1.1 Quick Export

Purpose:

Export record files to backup device(s) quickly.

Steps:

1. Enter Video Export interface.

Menu>Export>Normal

Choose the channel(s) you want to back up and click **Quick Export**.

Note: 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.

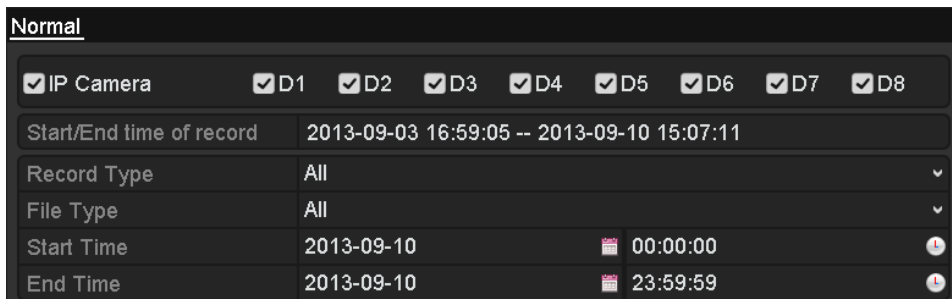


Figure 7. 1 Quick Export Interface

2. Export.

Go to Export interface, choose backup device and click **Export** to start exporting.

Note: Here we use USB Flash Drive and please refer to *Chapter 7.1.2 Backing up by Normal Video Search* for more backup devices supported by the device.

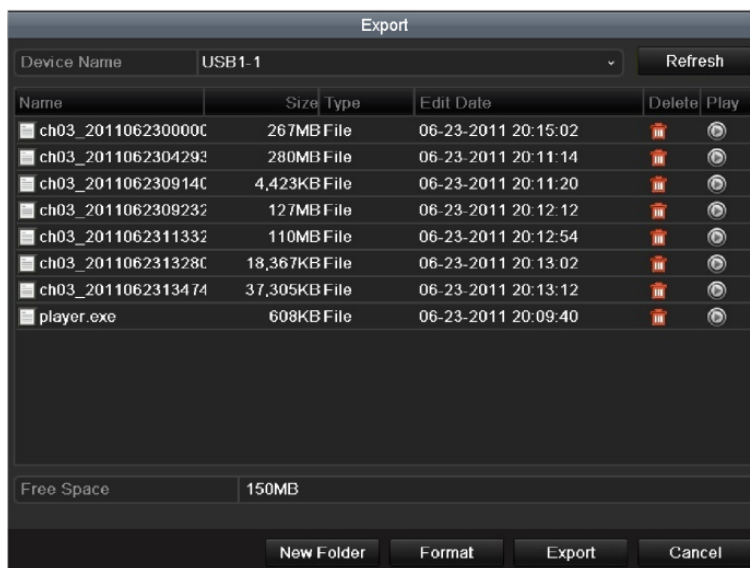


Figure 7. 2 Quick Export using USB1-1

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

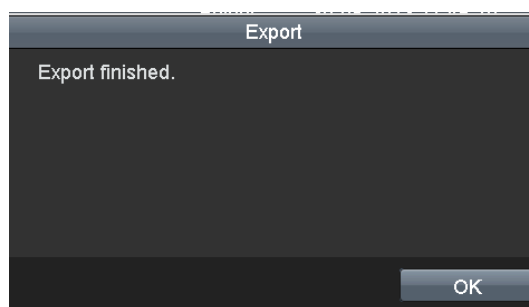


Figure 7. 3 Export Finished

3. Check backup result.

Choose the record file in Export interface and click button  to check it.

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

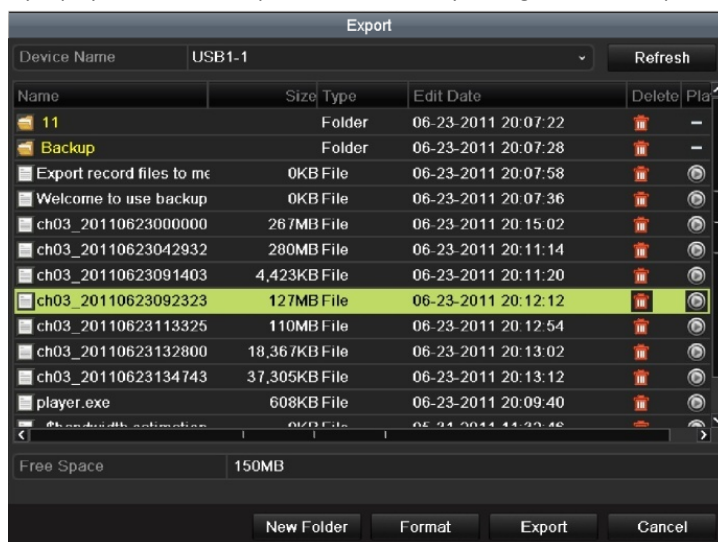


Figure 7. 4 Checkup of Quick Export Result Using USB1-1

7.1.2 Backing up by Normal Video Search

Purpose:

The record files can be backup to various devices, such as USB devices (USB flash drives, USB HDDs, USB writer) and DVD-R/W.

Backup using USB flash drives, USB HDDs, USB writer and DVD-R/W

Steps:

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

Notes:

- 1) Six different Record types are selectable: Continuous, Motion, Alarm, Motion | Alarm, Motion & Alarm, Command Triggered and Manual. The command triggered record is configured by the platform when the device accessed via the platform.
- 2) Two different File types are selectable: Unlocked and Locked.



Figure 7. 5 Normal Video Search for Backup

3. Select record files you want to back up.

Click button  to play the record file if you want to check it.

Check the checkbox before the record files you want to back up.

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

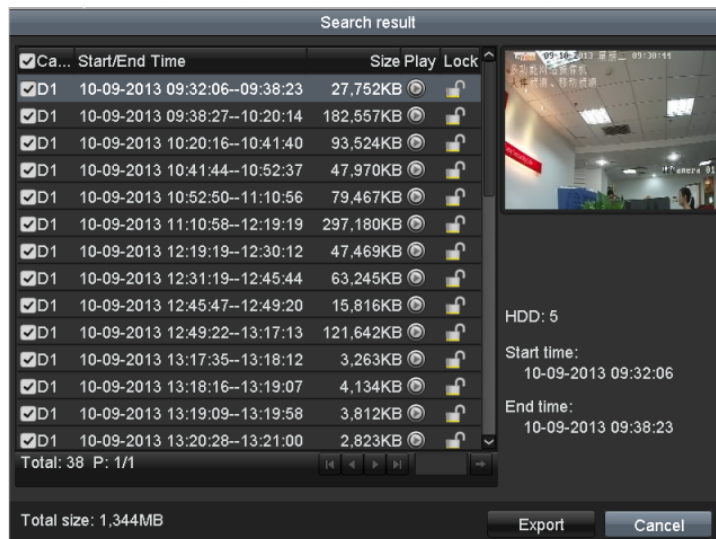


Figure 7. 6 Result of Normal Video Search for Backup

4. Export.

Click **Export** and start backup.

Note: If the inserted device is not recognized:

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

You can also format USB flash drives or USB HDDs via the device. USB writer and DVD-R/W cannot be formatted.

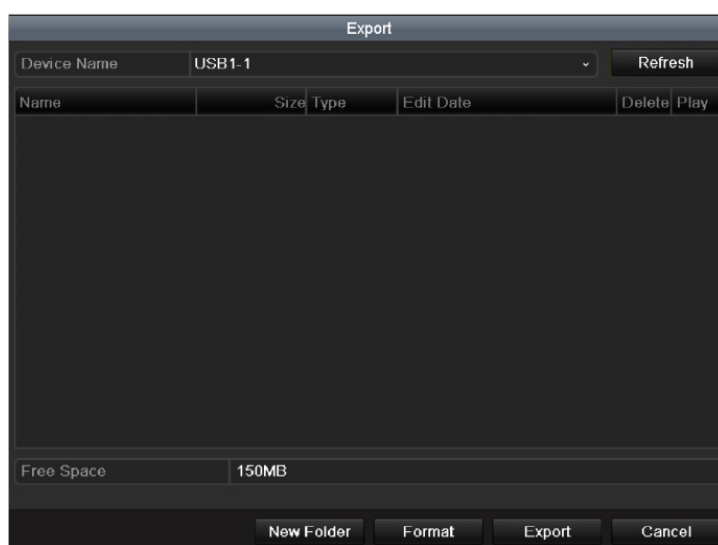


Figure 7. 7 Export by Normal Video Search using USB Flash Drive

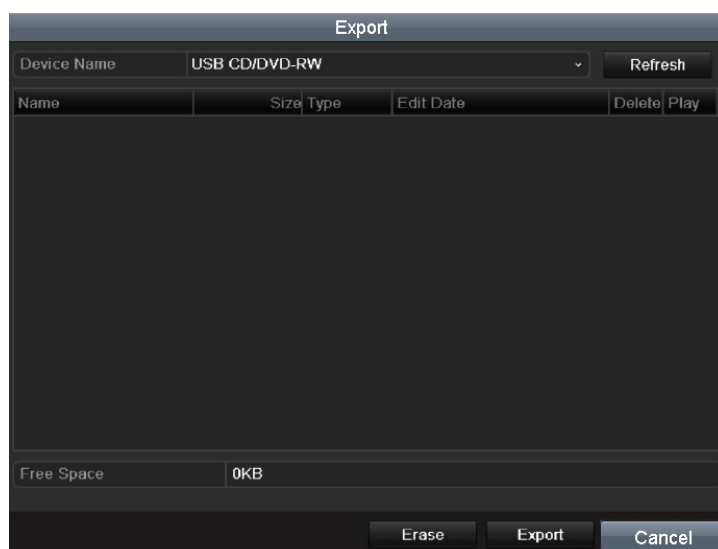


Figure 7. 8 Export by Normal Video Search using USB Writer

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

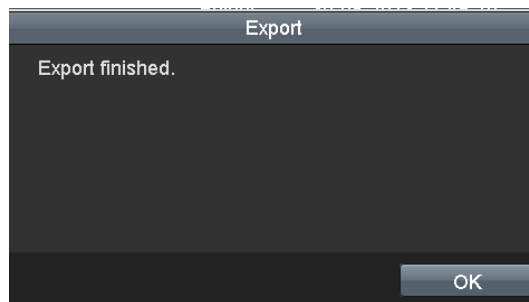


Figure 7. 9 Export Finished

5. Check backup result.

Choose the record file in Export interface and click button  to check it.

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

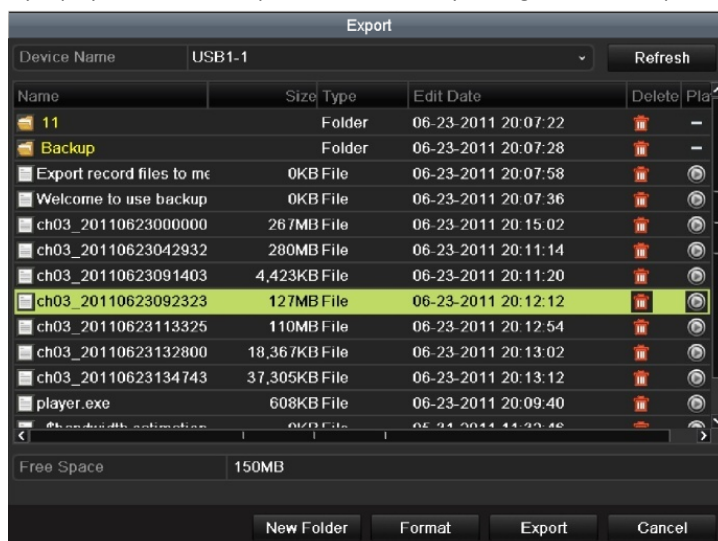


Figure 7. 10 Checkup of Export Result using USB Flash Drive

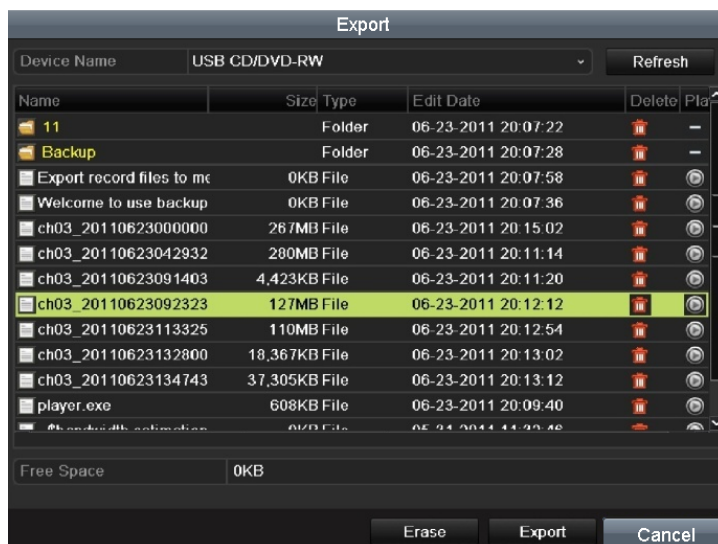


Figure 7. 11 Checkup of Export Result using USB Writer

7.1.3 Backing up by Event Search

Purpose:

Back up event-related record files using USB devices (USB flash drives, USB HDDs, USB writer), or DVD-R/W. Quick Backup and Normal Backup are supported.

Steps:

1. Enter Export interface.

Menu>Export>Event

- 1) Select Alarm Input/Motion from the dropdown list of Event Type.

Note: Here we take Alarm Input as an example.

- 2) Select the alarm input No. and time.
- 3) Click **Search** to enter the Search Result interface.

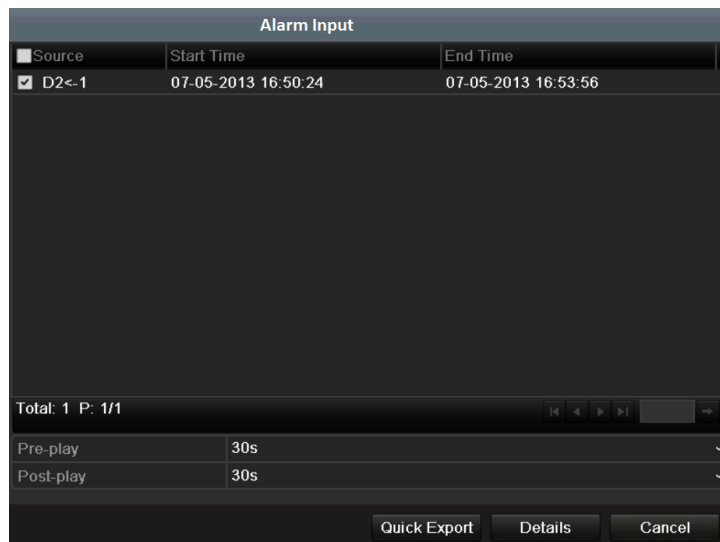


Figure 7. 12 Event Search for Backup

2. Select record files to export.

- 1) Select an alarm input in the list and click **Quick Export** to enter Export interface.
- 2) Clicking **Details** will take you to the interface with detailed information of all channels triggered by the selected alarm input. You can view detailed information of the record file, e.g. start time, end time and file size.

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

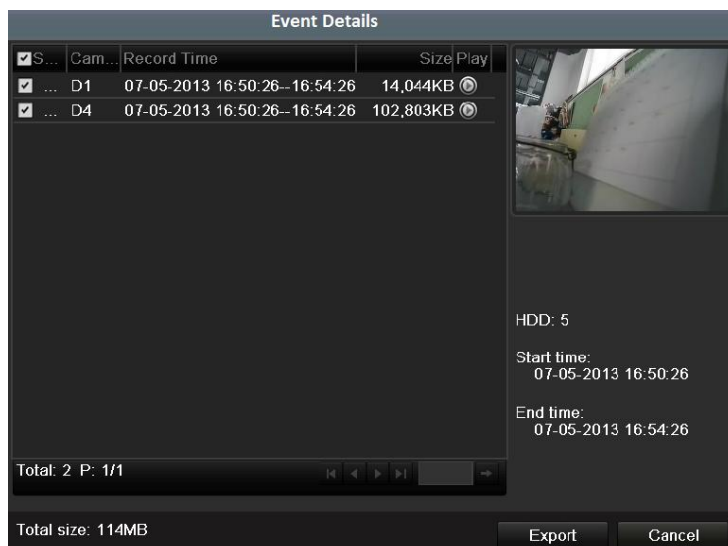


Figure 7. 13 Event Details Interface

3. Export.

Click **Export** and start backup.

Note: If the inserted USB device is not recognized:

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

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

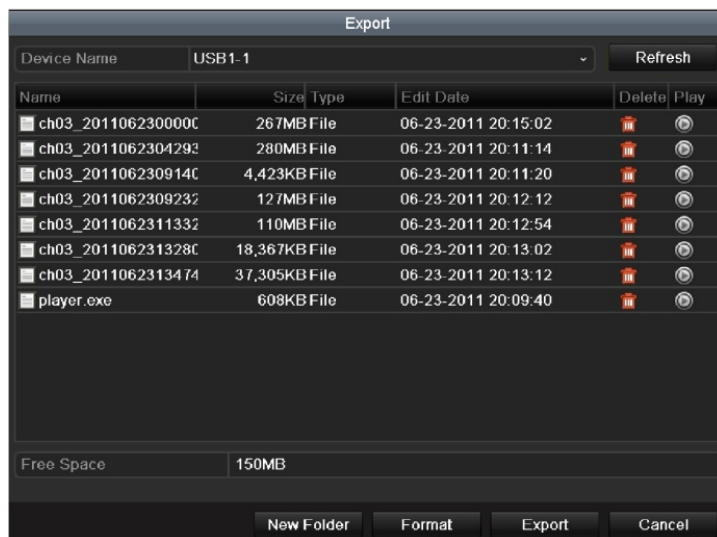


Figure 7. 14 Export by Event Using USB Flash Drive

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

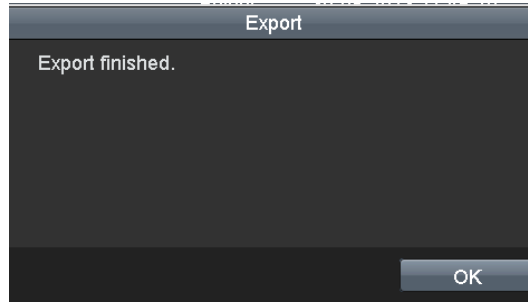


Figure 7. 15 Export Finished

4. Check backup result.

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

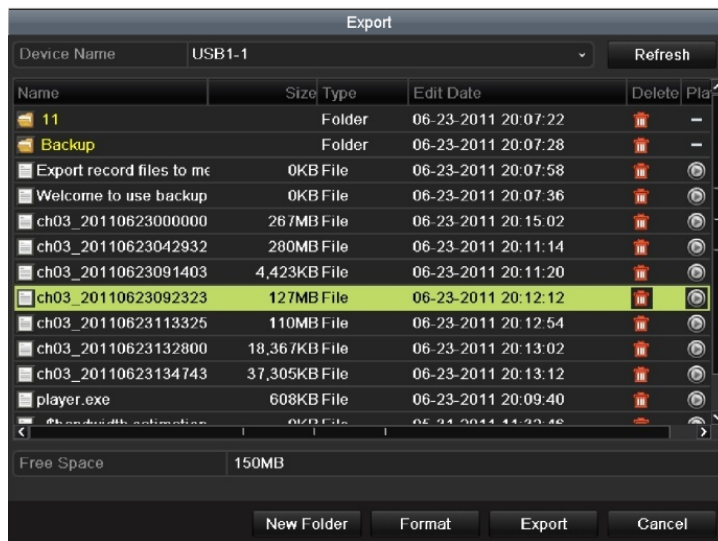




Figure 7. 16 Checkup of Event Export Result Using USB Flash Drive

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), or DVD-R/W.

Steps:

1. Enter Playback interface and play back the record file you want to set video clips.
Please refer to *Chapter 6.1 Playing Back Record Files*.
2. During playback, use buttons  and  in the playback toolbar to start or stop clipping record file(s).
3. Quit Playback interface after finishing clipping and you will then be prompted to save the clips.

Note: A maximum of 30 clips can be selected for each channel.



Figure 7. 17 Interface of Playback by Time

4. Click **Yes** to save video clips and enter Export interface, or click **No** to quit and do not save video clips.

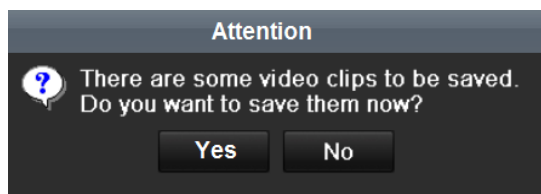


Figure 7. 18 Attention to Video Clip Saving

5. Export.

Click **Export** and start backup.

Note: If the inserted USB device is not recognized:

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

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

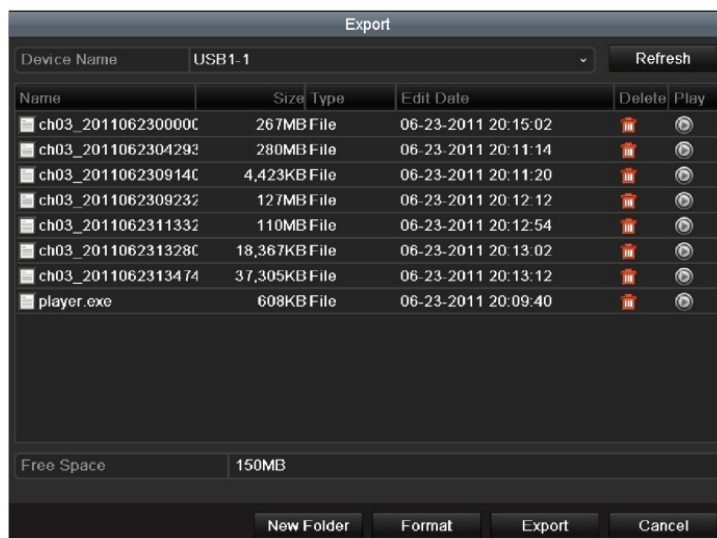


Figure 7. 19 Export Video Clips Using USB Flash Drive

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

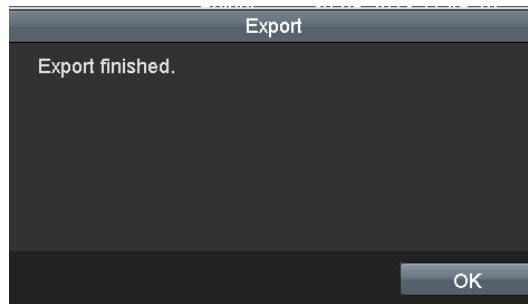


Figure 7. 20 Export Finished

6. Check backup result.

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

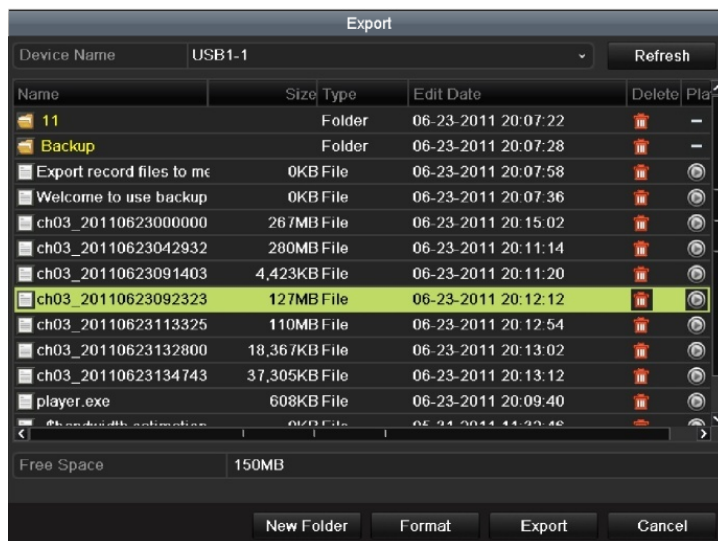


Figure 7. 21 Checkup of Video Clips Export Result Using USB Flash Drive

7.1.5 Backing up POS

Purpose:

Back up event-related record files using USB devices (USB flash drives, USB HDDs, USB writer), or DVD-R/W. Quick Backup and Normal Backup are supported.

Steps:

5. Enter Export interface.

Menu>Export>POS

- 1) Select Alarm Input/Motion from the dropdown list of Event Type.

Note: Here we take Alarm Input as an example.

- 2) Select the channels input No. and time. You can also enter keyword or condition in the textbox

Match Approximate to search the text on your command.

- 3) Click **Search** to enter the Search Result interface.

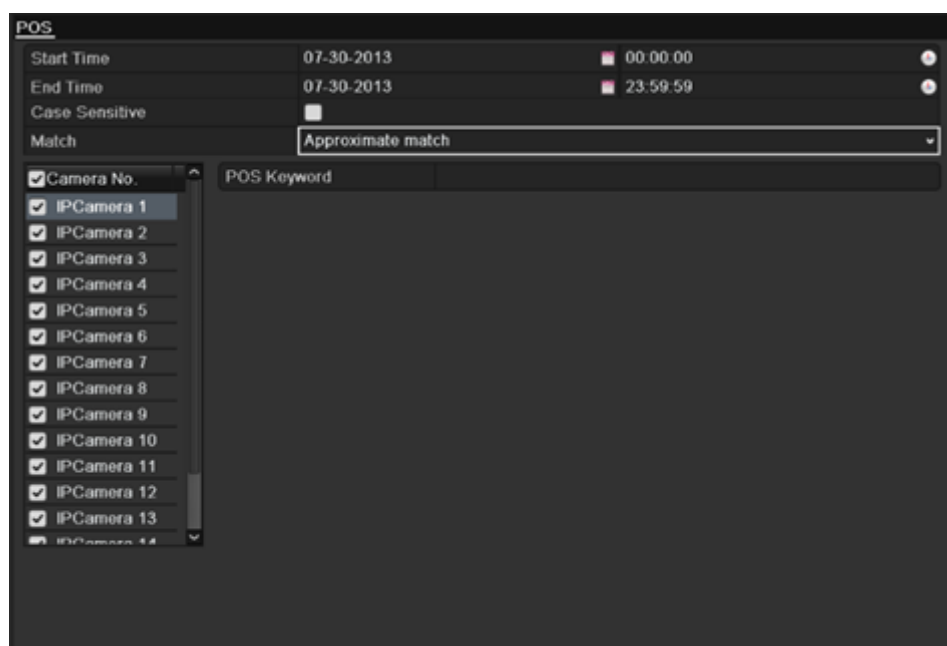


Figure 7. 22 POS Search for Backup

6. Select record files to export.

- 3) Select an alarm input in the list and click **Quick Export** to enter Export interface.
- 4) Clicking **Details** will take you to the interface with detailed information of all channels triggered by the selected alarm input. You can view detailed information of the record file, e.g. start time, end time and file size.

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



Figure 7. 23 POS Details Interface

7. Export.

Click **Export** and start backup.

Note: If the inserted USB device is not recognized:

- Click **Refresh**.

- Reconnect device.
- Check for compatibility from vendor.

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

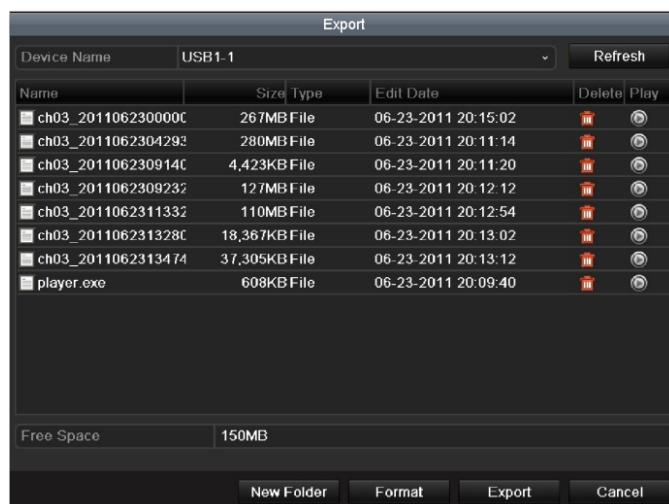


Figure 7. 24 Export by POS Using USB Flash Drive

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

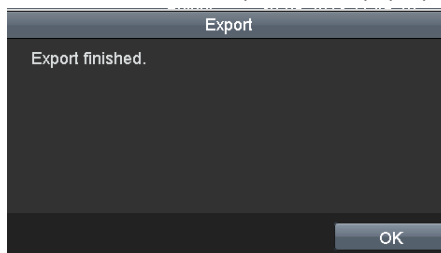


Figure 7. 25 Export Finished

8. Check backup result.

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

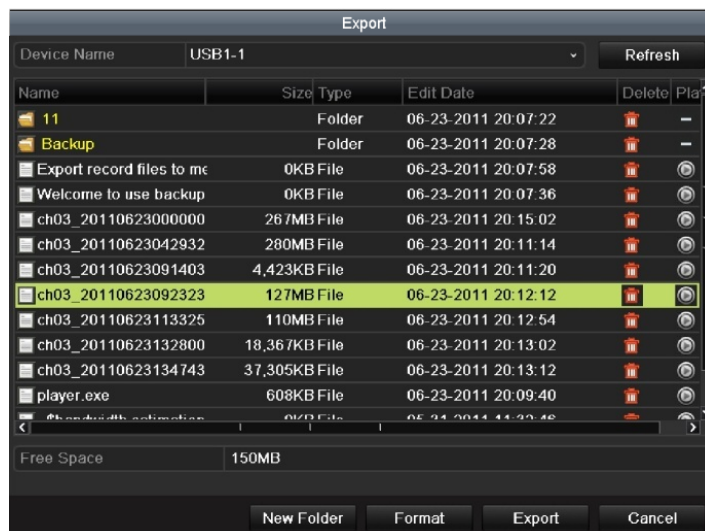


Figure 7. 26 Checkup of POSExport Result Using USB Flash Drive

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

Set search condition and click **Search** to enter Search Result interface.

Note: At least one channel shall be selected.

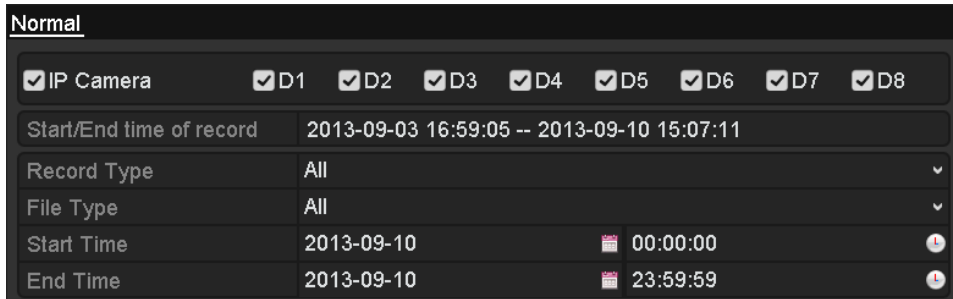


Figure 7. 27 Normal Video Search for Backup

2. Select record files you want to back up.

Click **Export** to enter Export interface.

Note: At least one record file shall be selected.

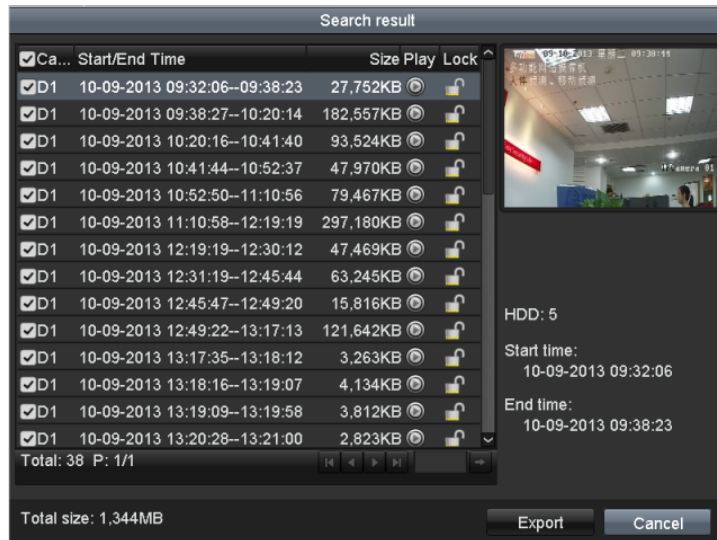


Figure 7. 28 Result of Normal Video Search for Backup

3. Backup device management.

Click **New Folder** if you want to create a new folder in the backup device.

Select a record file or folder in the backup device and click **Delete** if you want to delete it.

Select a record file in the backup device and click **Play** to play it.

Click **Format** to format the backup device. Two kinds of file system can be configurable, including FAT32 and NTFS.

Note: If the inserted USB device is not recognized:

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

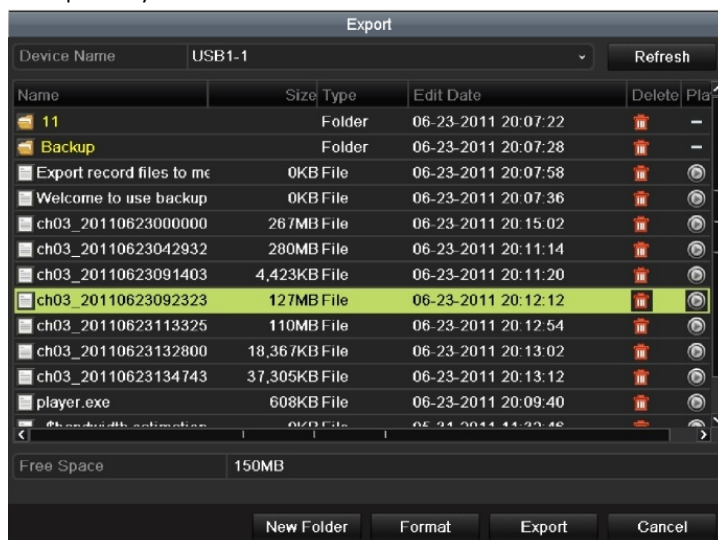


Figure 7. 29 USB Flash Drive Management

Management of USB writers and DVD-R/W

1. Enter Search Result interface of record files.

Menu>Export>Normal

Set search condition and click **Search** to enter Search Result interface.

Note: At least one channel shall be selected.

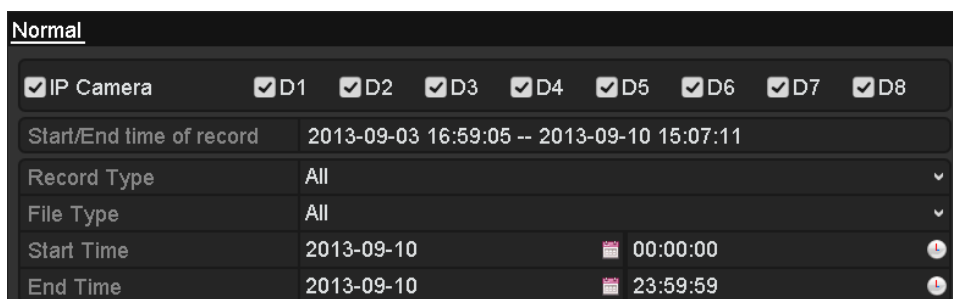


Figure 7. 30 Normal Video Search for Backup

2. Select record files you want to back up.

Click **Export** to enter Export interface.

Note: At least one record file shall be selected.

Chapter 8 Alarm Settings

8.1 Setting Motion Detection Alarm

Steps:

1. Enter Motion Detection interface and choose a camera you want to set motion detection.

Menu> Camera> Motion

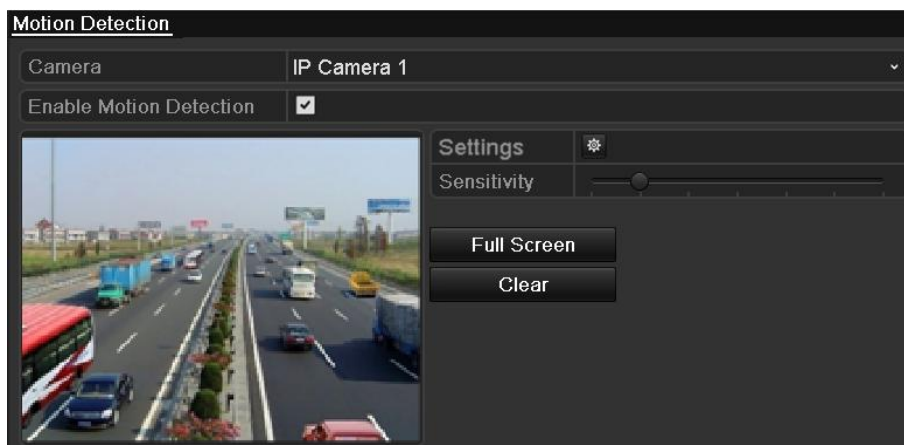


Figure 8. 1 Motion Detection Setup Interface

2. Set up detection area and sensitivity.

Tick “Enable Motion Detection”, use the mouse to draw detection area(s) and drag the sensitivity bar to set sensitivity.

Click **Handling** button and set alarm response actions.



Figure 8. 2 Set Detection Area and Sensitivity

3. 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.

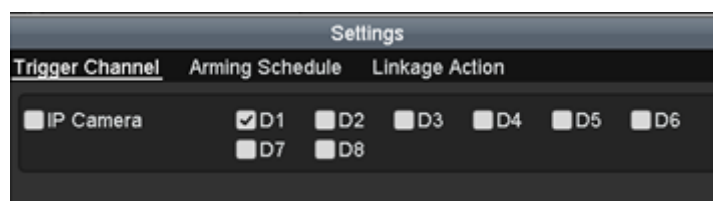


Figure 8. 3 Set Trigger Camera of Motion Detection

4. Set up arming schedule of the channel.

Select Arming Schedule tab to set the channel's arming schedule for the motion detection.

Choose one day of a week and up to eight time periods can be set within each day.

Note: Time periods shall not be repeated or overlapped.

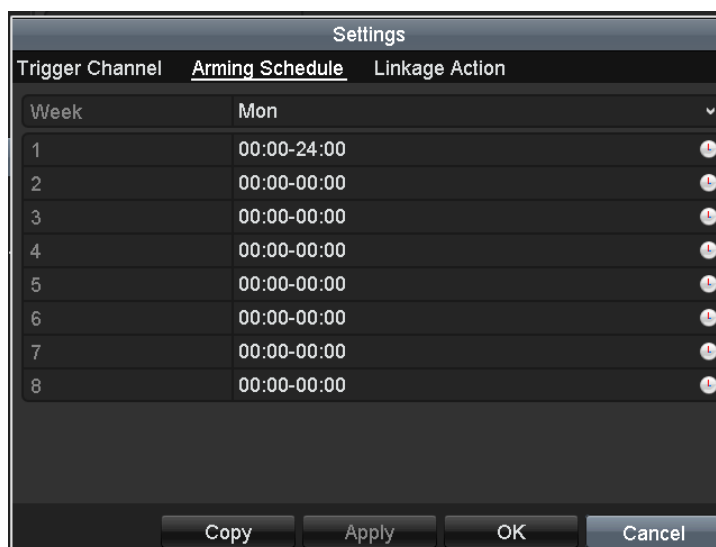


Figure 8. 4 Set Arming Schedule of Motion Detection

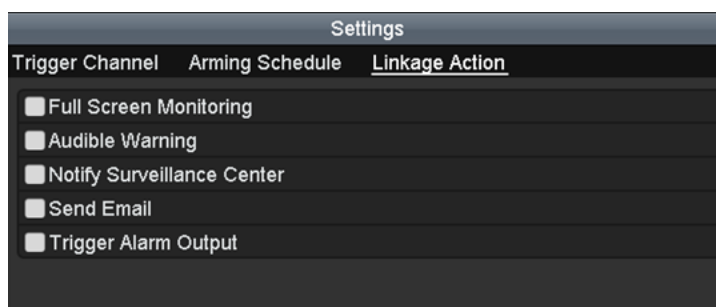
5. Click Linkage Action tab to set up alarm response actions of motion alarm (please refer to *Chapter Setting Alarm Response Actions*).

Figure 8. 5 Set Alarm Response Actions of Motion Detection

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.

6. Click the OK button to complete the motion detection settings of the channel.

8.2 Setting Sensor Alarms

Purpose:

Set handling method of an external sensor alarm.

Steps:

1. Enter Alarm Settings of System Configuration and select an alarm input.

Menu> Configuration> Alarm

Select Alarm Input tab to enter Alarm Input Settings interface.

No.	Alarm Name	IP Camera Address	Alarm Type
A<-1		Local	N.O
A<-2		Local	N.O
A<-3		Local	N.O
A<-4		Local	N.O
A<-5		Local	N.O
A<-6		Local	N.O
A<-7		Local	N.O

No.	Alarm Name	IP Camera Address	Dwell Time
A->1		Local	5s
A->2		Local	5s
A->3		Local	5s
A->4		Local	5s

Figure 8. 6 Alarm Status Interface of System Configuration

2. Set up the handling method of the selected alarm input.

Check the **Setting** checkbox and click **Handling** button to set up its alarm response actions.

Alarm Input No.	A<-1
Alarm Name	
Type	N.O
Setting	<input type="checkbox"/>
Handling	

Figure 8. 7 Alarm Input Setup Interface

3. 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.
4. Select **Arming Schedule** tab to set the channel's arming schedule.
Choose one day of a week and Max. eight time periods can be set within each day.
Note: Time periods shall not be repeated or overlapped.
5. Select **Handling** tab to set up alarm response actions of the alarm input (please refer to *Chapter Setting Alarm Response Actions*).
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.

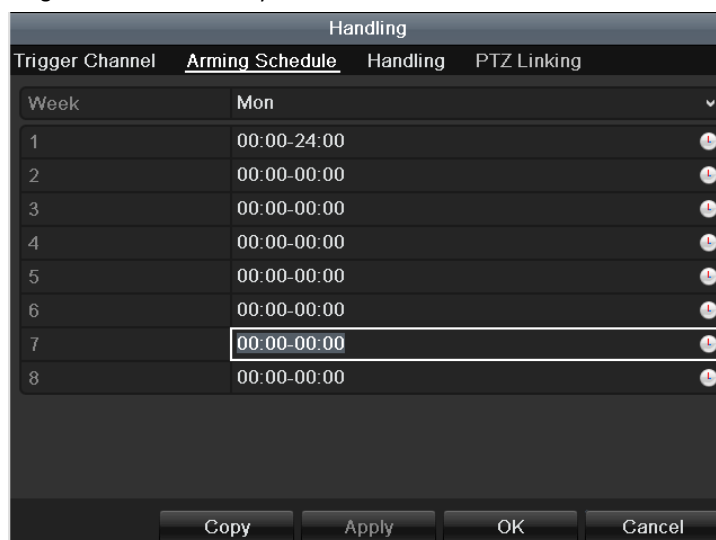


Figure 8. 8 Set Arming Schedule of Alarm Input

6. If necessary, select PTZ Linking tab and set PTZ linkage of the alarm input.

Set PTZ linking parameters and click **OK** to complete the settings of the alarm input.

Note: Please check whether the PTZ or speed dome supports PTZ linkage.

One alarm input can trigger presets, patrol or pattern of more than one channel. But presets, patrols and patterns are exclusive.

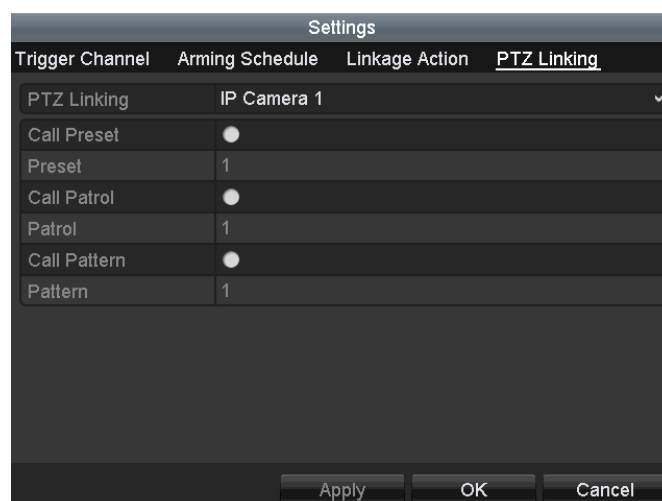


Figure 8. 9 Set PTZ Linking of Alarm Input

7. If you want to set handling method of another alarm input, repeat the above steps or just copy the above settings to it.

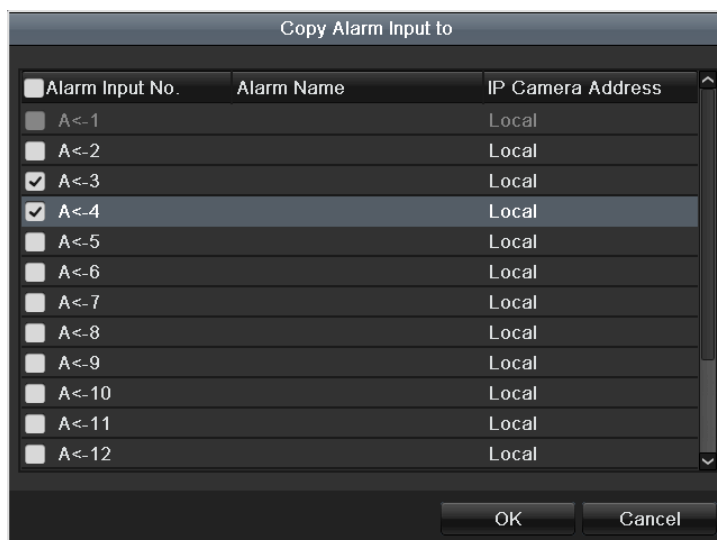


Figure 8. 10 Copy Settings of Alarm Input

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 and select a channel you want to detect.

Menu> Camera> Video Loss

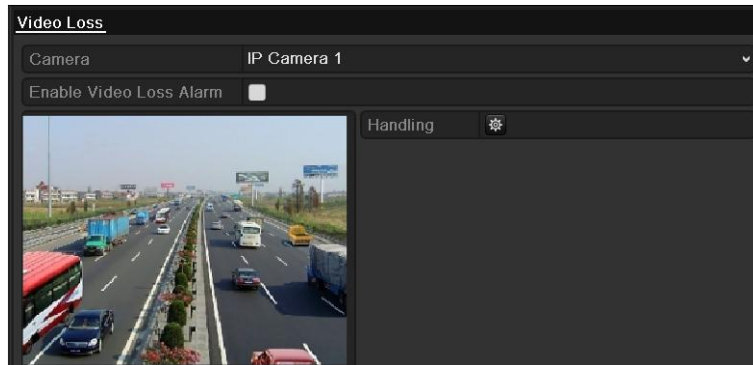


Figure 8. 11 Video Loss Setup Interface

2. Set up handling method of video loss.

Check the checkbox of “Enable Video Loss Alarm”, and click **Handling** button to set up handling method of video loss.

3. Set up arming schedule of the channel.

Select Arming Schedule tab to set the channel’s arming schedule.

Choose one day of a week and up to eight time periods can be set within each day.

Note: Time periods shall not be repeated or overlapped.

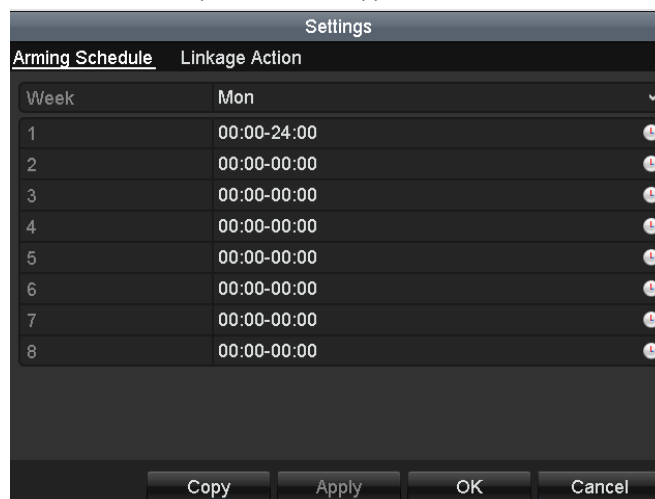


Figure 8. 12 Set Arming Schedule of Video Loss

4. Select **Handling** tab to set up alarm response action of video loss (please refer to *Chapter Setting Alarm Response Actions*).

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.

5. Click the **OK** button to complete the video loss settings of the channel.

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 of Camera Management and select a channel you want to detect video tampering.

Menu> Camera> Tamper-proof



Figure 8. 13 Tamper-proof Setup Interface

2. Set the video tampering handling method of the channel.

Check the checkbox of “Enable Tamper-proof”.

Drag the sensitivity bar and choose a proper sensitivity level. Use the mouse to draw an area you want to detect video tampering.

Click **Handling** button to set up handling method of video tampering.

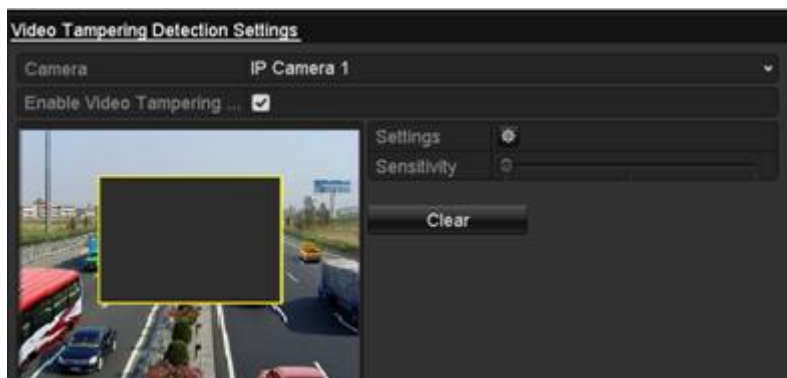


Figure 8. 14 Set Detection Area and Sensitivity of Video Tampering

3. Set arming schedule and alarm response actions of the channel.

- 1) Click Arming Schedule tab to set the channel’s arming schedule.

- 2) Choose one day of a week and Max. eight time periods can be set within each day.

Note: Time periods shall not be repeated or overlapped.

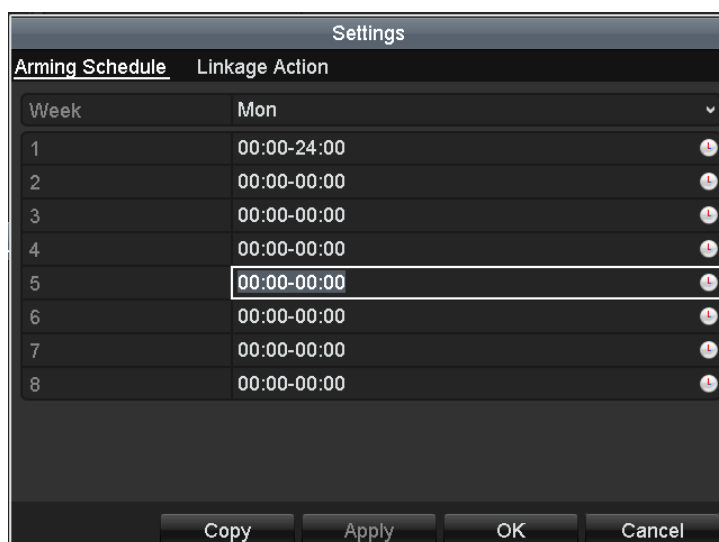


Figure 8. 15 Set Arming Schedule of Video Tampering

4. Select **Handling** tab to set up alarm response actions of video tampering alarm (please refer to *Chapter Setting Alarm Response Actions*).

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.

5. Click the **OK** button to complete the video tampering settings of the channel.

8.5 Handling Exceptions Alarm

Purpose:

Exception settings refer to the handling method of various exceptions, e.g.

- **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.

Steps:

Enter Exception interface of System Configuration and handle various exceptions.

Menu> Configuration> Exceptions

Please refer to *Chapter Setting Alarm Response Actions* for detailed alarm response actions.

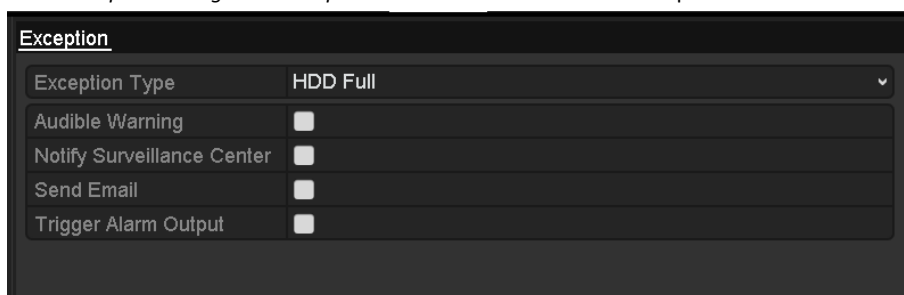


Figure 8.16 Exceptions Setup Interface

8.6 Setting Alarm Response Actions

Purpose:

Alarm response actions will be activated when an alarm or exception occurs, including Full Screen Monitoring, Audible Warning (buzzer), Notify Surveillance Center, Trigger Alarm Output and Send Email.

Full Screen Monitoring

When an alarm is triggered, the local monitor (VGA or HDMI monitor) display in full screen the video image from the alarming channel configured for full screen monitoring.

If alarms are triggered simultaneously in several channels, their full-screen images will be switched at an interval of 10 seconds (default dwell time). A different dwell time can be set by going to Menu >Configuration>Live View>Alarm Picture Dwell Time.

Auto-switch will terminate once the alarm stops and you will be taken back to the Live View interface.

Note: You must select during “Trigger Channel” settings the channel(s) you want to make full screen monitoring.

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.

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

Email Linkage

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

Please refer to *Chapter Steps*:

1. Open web browser, input the IP address of device, and the web server will select the language automatically according to the system language and maximize the web browser.
2. Input the correct user name and password, and click **Login** button to log in the device.
3. Enter the HTTPS settings interface.
Configuration > Remote Configuration > Network Settings > HTTPS
4. Create the self-signed certificate or authorized certificate.

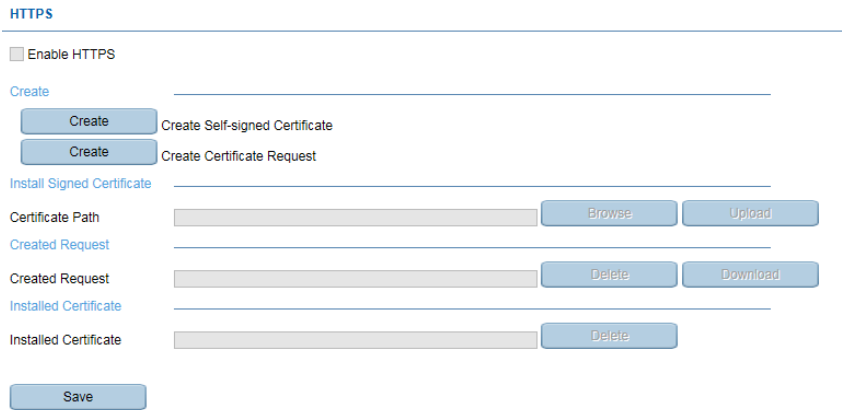


Figure 8. 1 HTTPS Settings

OPTION 1: Create the self-signed certificate

- 1) Click the **Create** button to create the following dialog box.

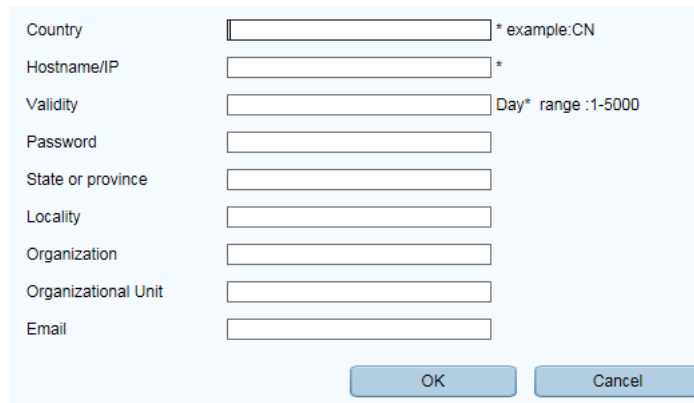


Figure 8. 2 Create Self-signed Certificate

- 2) Enter the country, host name/IP, validity and other information.
- 3) Click **OK** to save the settings.

OPTION 2: Create the authorized certificate

- 1) Click the **Create** button to create the certificate request.
 - 2) Download the certificate request and submit it to the trusted certificate authority for signature.
 - 3) After receiving the signed valid certificate, import the certificate to the device.
5. There will be the certificate information after you successfully create and install the certificate.

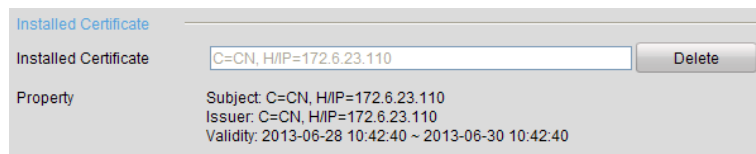


Figure 8. 3 Installed Certificate Property

6. Check the checkbox to enable the HTTPS function.
7. Click the **Save** button to save the settings.

Configuring Email for details of Email configuration.

Trigger Alarm Output

Trigger an alarm output when an alarm is triggered.

1. Enter Alarm Output interface.

Menu> Configuration> Alarm> Alarm Output

Select an alarm output and set alarm name and dwell time. Click **Schedule** button to set the arming schedule of alarm output.

Note: If “Manually Clear” is selected in the dropdown list of Dwell Time, you can clear it only by going to Menu> Manual> Alarm.

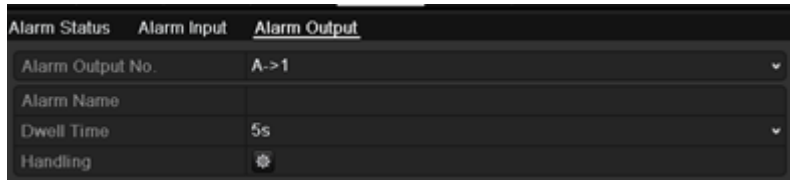


Figure 8. 4 Alarm Output Setup Interface

2. Set up arming schedule of the alarm output.

Choose one day of a week and up to 8 time periods can be set within each day.

Note: Time periods shall not be repeated or overlapped.

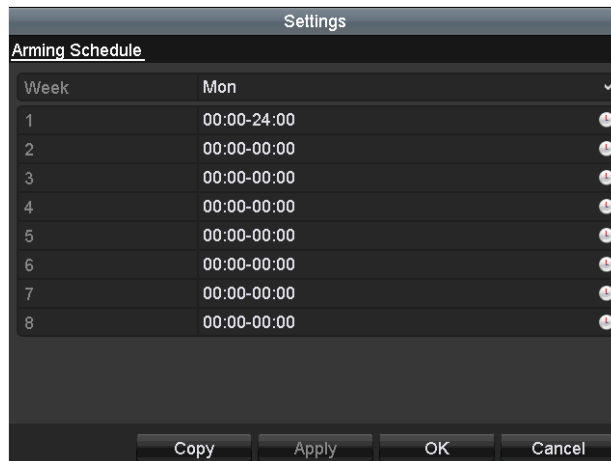


Figure 8. 5 Set Arming Schedule of Alarm Output

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.

Click the **OK** button to complete the video tampering settings of the alarm output No.

4. You can also copy the above settings to another channel.

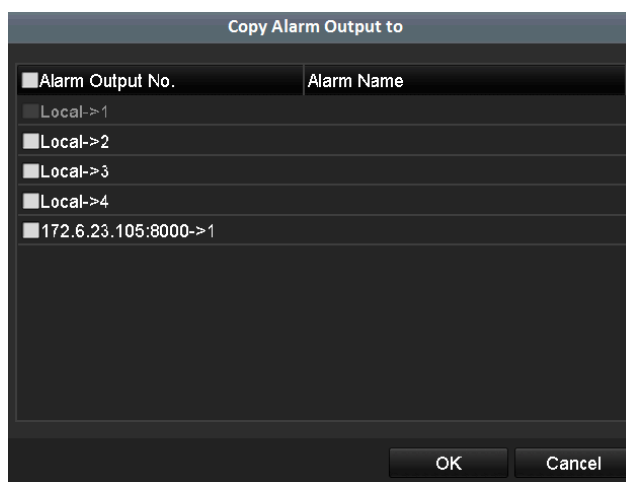


Figure 8. 6 Copy Settings of Alarm Output

8.7 Triggering or Clearing Alarm Output Manually

Purpose:

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

Steps:

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

Menu> Manual> Alarm

Click **Trigger/Clear** button if you want to trigger or clear an alarm output.

Click **Trigger All** button if you want to trigger all alarm outputs.

Click **Clear All** button if you want to clear all alarm output.

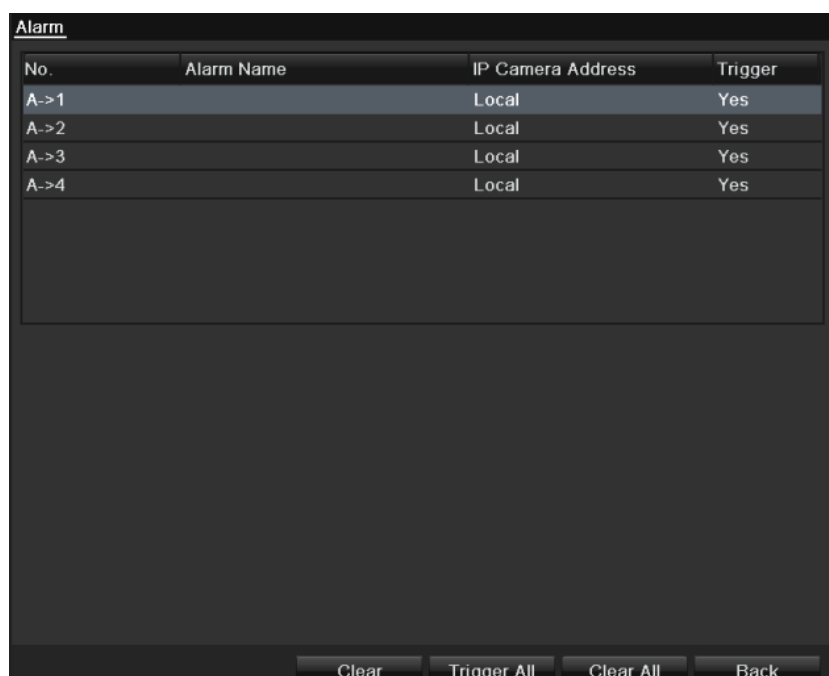


Figure 8. 7 Clear or Trigger Alarm Output Manually

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.

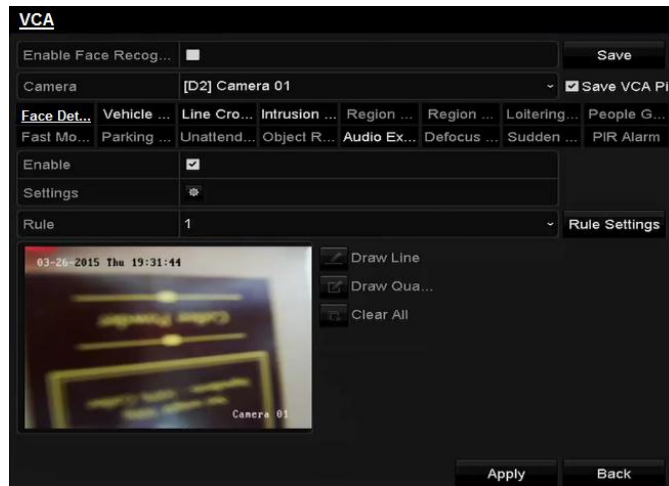



Figure 9. 1 Face Detection

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 *Chapter 错误! 未找到引用源。 错误! 未找到引用源。* 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.

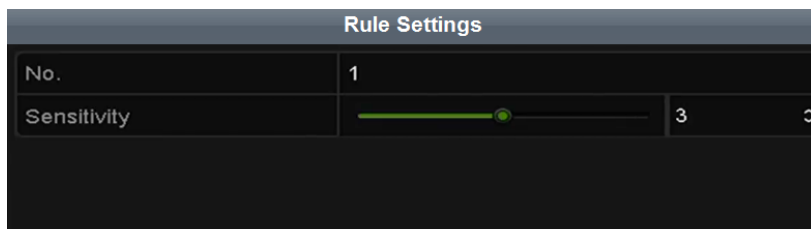


Figure 9. 2 Set Face Detection Sensitivity


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

9.2 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:

- Enter the VCA settings interface.
Menu> Camera> VCA
- Select the camera to configure the VCA.
You can click the checkbox of **Save VCA Picture** to save the captured pictures of VCA detection.
- Select the VCA detection type to **Line Crossing Detection**.
- Check the **Enable** checkbox to enable this function.
- Click  to configure the trigger channel, arming schedule and linkage actions for the line crossing detection alarm.
- Click the **Rule Settings** button to set the line crossing detection rules.
 - 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.
 - 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.
 - Click-**OK** to save the rule settings and back to the line crossing detection settings interface.



Figure 9. 3 Set Line Crossing Detection Rules

- 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.

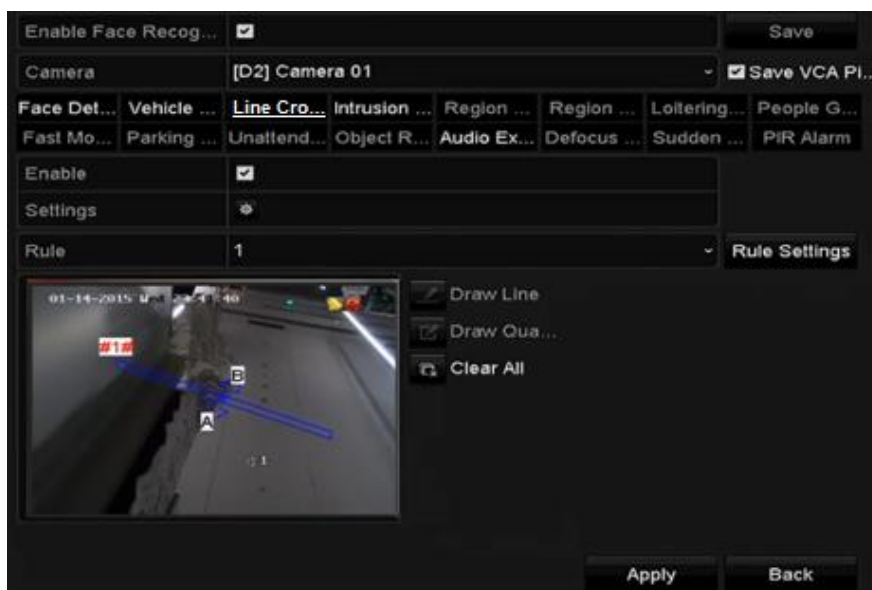


Figure 9. 4 Draw Line for Line Crossing Detection


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

9.3 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.




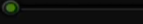



Rule Settings			
No.	1		
Time Threshold (s)		5	
Sensitivity		50	
Percentage		0	

Figure 9. 5 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.

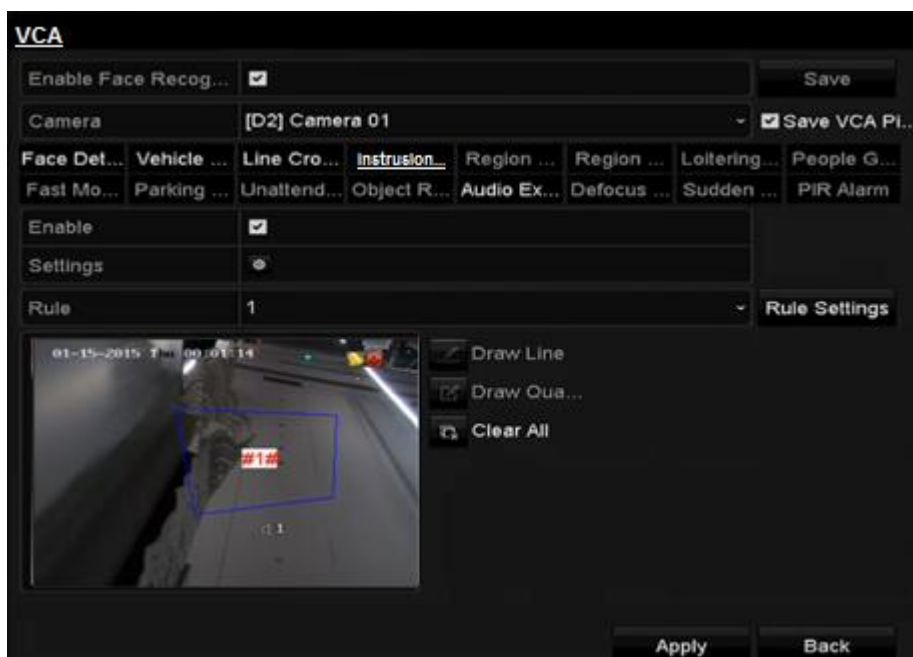


Figure 9. 6 Draw Area for Intrusion Detection

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

9.4 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 9.3 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.

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.

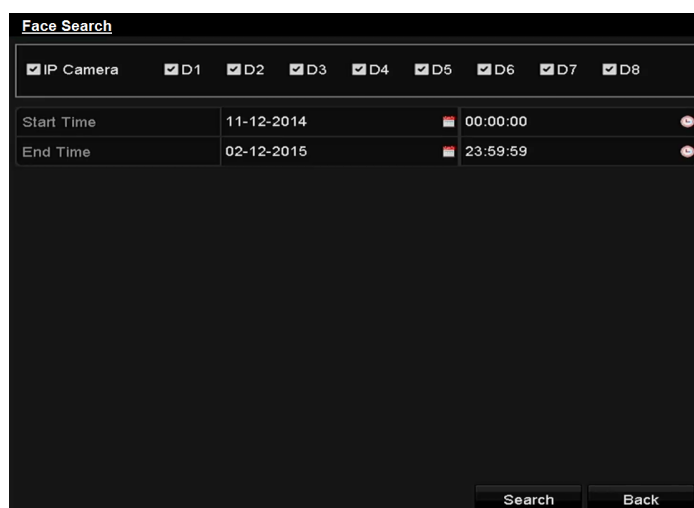


Figure 10. 1 Face Search

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.

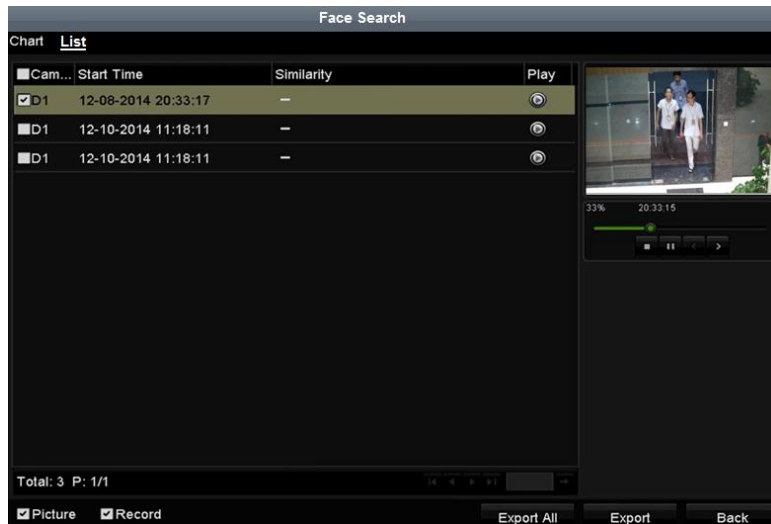






Figure 10. 2 Face Search Interface

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 *错误! 未找到引用源。错误! 未找到引用源。* for the operation of exporting files.

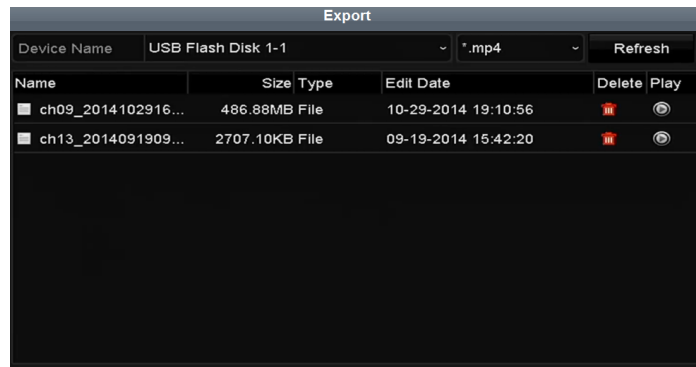


Figure 10. 3 Export Files

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.

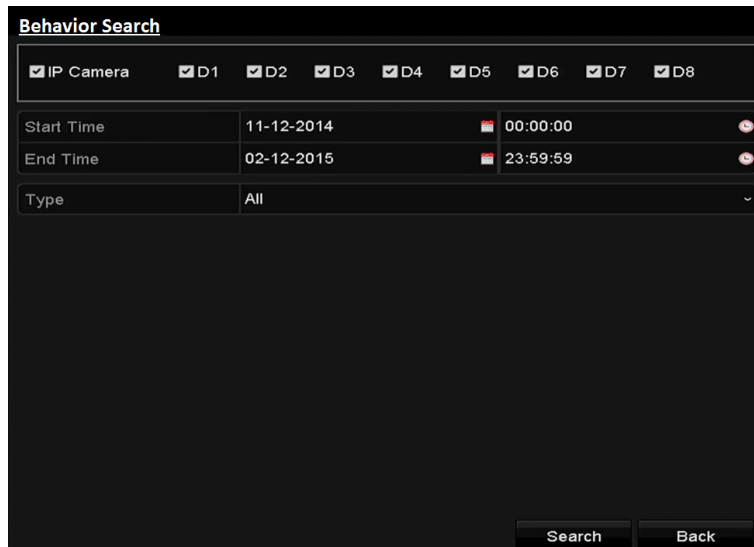


Figure 10. 4 Behavior Search Interface

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.

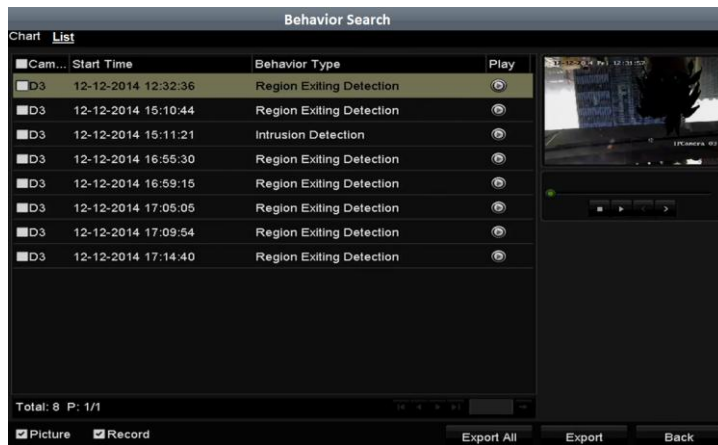






Figure 10. 5 Behavior Search Results

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  to play it.
 You can also click  to stop the playing, or click  /  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 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.

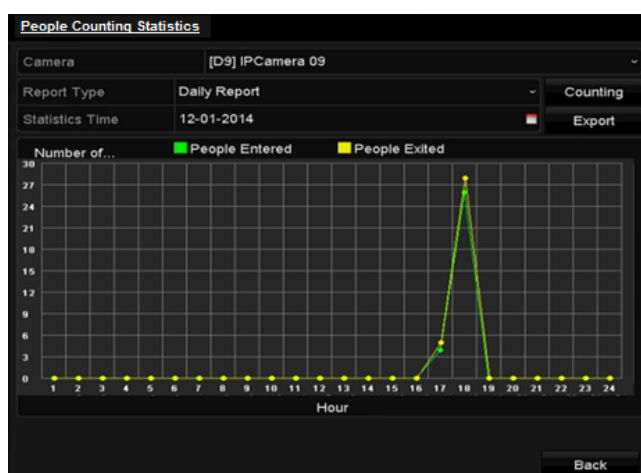


Figure 10. 6 People Counting Interface

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

10.4 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.

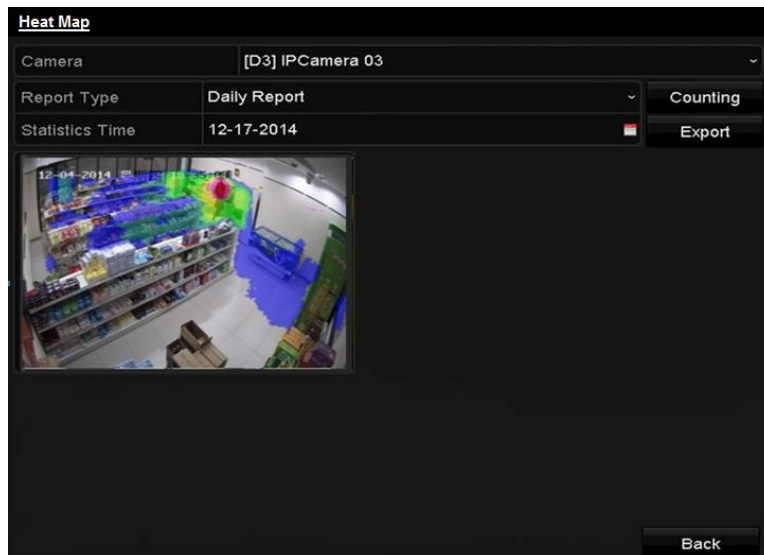


Figure 10. 7 Heat Map Interface

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.

Working Mode	Net Fault-tolerance
Select NIC	bond0
NIC Type	10M/100M/1000M Self-adaptive
Enable DHCP	<input type="checkbox"/>
IPv4 Address	172 .6 .21 .159
IPv4 Subnet Mask	255 .255 .255 .0
IPv4 Default Gateway	172 .6 .21 .1
IPv6 Address 1	fec0::a:240:48ff:fe62:dcd/64
IPv6 Address 2	2002:ac06:1578:a:240:48ff:fe62:dcd/64
IPv6 Default Gateway	
MAC Address	00:40:48:62:0d:cd
MTU(Bytes)	1500
Preferred DNS Server	
Alternate DNS Server	
Main NIC	LAN1

Figure 11. 9 Network Settings Interface

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

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



The valid value range of MTU is 500 ~ 9676.

4. After having configured the general settings, click **Apply** button to save the settings.

Working Mode

There are two 10M/100M/1000M NIC cards provided by the 9600NI-H8 series device, and it allows the device to work in the Multi-address, Load Balance and Net-fault Tolerance modes.

Multi-address Mode: The parameters of the two NIC cards can be configured independently. You can select LAN1 or LAN2 in the NIC type field for parameter settings.

You can select one NIC card as default route. And then the system is connecting with the extranet the data will be forwarded through the default route.

Net-fault Tolerance Mode: The two NIC cards use the same IP address, and you can select the Main NIC to LAN1 or LAN2. By this way, in case of one NIC card failure, the device will automatically enable the other standby NIC card so as to ensure the normal running of the whole system.

Load Balance Mode: By using the same IP address and two NIC cards share the load of the total bandwidth, which enables the system to provide two Gigabit network capacity.

Working Mode	Net Fault-tolerance
Select NIC	bond0
NIC Type	10M/100M/1000M Self-adaptive
Enable DHCP	<input type="checkbox"/>
IPv4 Address	172 .6 .21 .159
IPv4 Subnet Mask	255 .255 .255 .0
IPv4 Default Gateway	172 .6 .21 .1
IPv6 Address 1	fec0::a:240:48ff:fe62:dcd/64
IPv6 Address 2	2002:ac06:1578:a:240:48ff:fe62:dcd/64
IPv6 Default Gateway	
MAC Address	00:40:48:62:0d:cd
MTU(Bytes)	1500
Preferred DNS Server	
Alternate DNS Server	
Main NIC	LAN1

Figure 11. 10 Net Fault-tolerance Working Mode

11.2 Configuring Advanced Settings

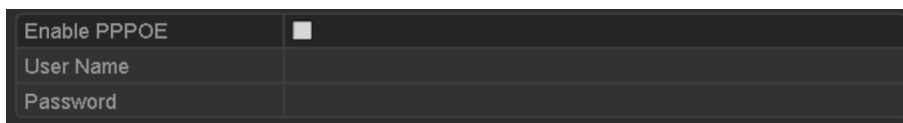
11.2.1 Configuring PPPoE Settings

Purpose:

Your NVR also allows access by Point-to-Point Protocol over Ethernet (PPPoE).

Steps:

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



Enable PPPOE	<input checked="" type="checkbox"/>
User Name	
Password	

Figure 11. 11 PPPoE Settings Interface

3. Check the **PPPoE** checkbox to enable this feature.
4. Enter **User Name**, and **Password** for PPPoE access.



The User Name and Password should be assigned by your ISP.

5. Click the **Apply** button to save and exit the interface.
6. After successful settings, the system asks you to reboot the device to enable the new settings, and the PPPoE dial-up is automatically connected after reboot.

You can go to Menu >Maintenance>System Info >Network interface to view the status of PPPoE connection.

Please refer to *Chapter Viewing System Information* for PPPoE status.

11.2.2 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:

2. Enter the Network Settings interface.
Menu >Configuration> Network
3. Select the **DDNS** tab to enter the DDNS Settings interface, as shown in Figure 11. 12.

Enable DDNS	<input type="checkbox"/>
DDNS Type	IPServer
Server Address	
Device Domain Name	
User Name	
Password	
Confirm	

Figure 11. 12 DDNS Settings Interface

4. Check the **DDNS** checkbox to enable this feature.
5. Select **DDNS Type**. Five different DDNS types are selectable: IPSEver, DynDNS, PeanutHull, NO-IP and HiDDNS.

- **LTS:**

Enter the **Server Address** and **Device Domain Name** for LTS.

- 1) Enter the **Server Address** of the LTS server, which is ns1.dvrlist.com by default.
- 2) Enter the **Device Domain Name**. You can use the alias you registered in the LTS 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 LTS 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	LTS
Server Address	ns1.dvrlists.com
Device Domain Name	
User Name	
Password	
Confirm	

Figure 11. 13 LTS Settings Interface

- **IPSEver:** Enter **Server Address** for IPSEver.

Enable DDNS	<input checked="" type="checkbox"/>
DDNS Type	IPSEver
Server Address	172.5.22.122
Device Domain Name	
User Name	
Password	
Confirm	

Figure 11. 14 IPSEver 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
Server Address	members.dyndns.org
Device Domain Name	123.dyndns.com
User Name	test
Password	*****
Confirm	*****

Figure 11. 15 DynDNS Settings Interface

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

Enable DDNS	<input checked="" type="checkbox"/>
DDNS Type	PeanutHull
Server Address	
Device Domain Name	
User Name	123.gicp.net
Password	*****
Confirm	*****

Figure 11. 16 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
Server Address	no-ip.org
Device Domain Name	123.no-ip.org
User Name	test
Password	*****
Confirm	*****

Figure 11. 17 NO-IP Settings Interface

- **HiDDNS:**
 - 1) The **Server Address** of the HiDDNS server appears by default: www.hiddns.com.
 - 2) 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
Server Address	www.hiddns.com
Device Domain Name	intelligent
User Name	
Password	
Confirm	

Figure 11. 18 HiDDNS Settings Interface

Register the device on the HiDDNS server.

- 1) Go to the HiDDNS website: www.hiddns.com.
- 2) Click [Register new user](#) to register an account if you do not have one and use the account to log in.

Figure 11. 19 Register an Account

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

Figure 11. 20 Register the Device



The device name can only contain the lower-case English letter, numeric and '-'; and it must start with the lower-case English letter and cannot end with '-'.

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.hiddns.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.hiddns.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.hiddns.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 NVMS7000**

For NVMS7000, in the Add Device window, select **HIDDNS** and then edit the device information.

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

Server Address: www.hiddns.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. By default it is admin.

Password: Enter the password of the device. By default it is 12345.

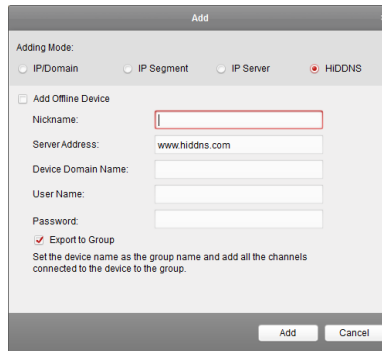


Figure 11. 21 Access Device via NVMS7000

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

11.2.3 Configuring NTP Server

Purpose:

A Network Time Protocol (NTP) Server can be configured on your NVR to ensure the accuracy of system date/time.

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. 22.

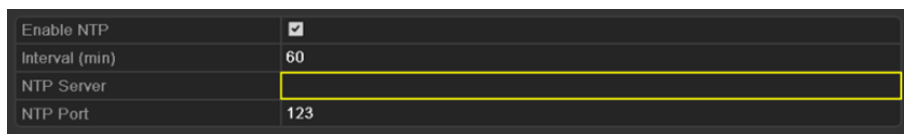


Figure 11. 22 NTP Settings Interface

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.

11.2.4 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. 23.

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. 23 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.

11.2.5 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. 24.

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. 24 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., NVMS7000) 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.

11.2.6 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. 24.
3. Set **Multicast IP**, as shown in Figure 11. 25. 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. 25 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.

11.2.7 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. 24.

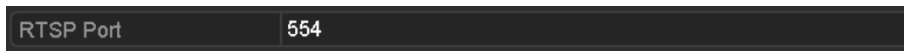


Figure 11. 26 RTSP Settings Interface

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.

11.2.8 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. 24.
3. Enter new **Server Port** and **HTTP Port**.

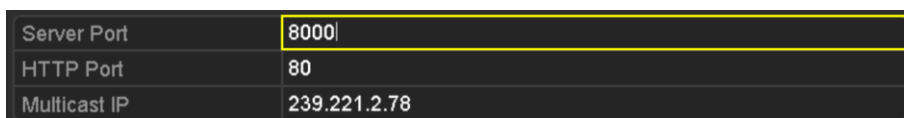


Figure 11. 27 Host/Others Settings Menu

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.

11.2.9 Configuring HTTPS Port

Purpose:

HTTPS provides authentication of the web site and associated web server that one is communicating with, which protects against Man-in-the-middle attacks. Perform the following steps to set the port number of https.

Example:

If you set the port number as 443 and the IP address is 192.0.0.64, you may access the device by inputting `https://192.0.0.64:443` via the web browser.



The HTTPS port can be only configured through the web browser.

Steps:

8. Open web browser, input the IP address of device, and the web server will select the language automatically according to the system language and maximize the web browser.
9. Input the correct user name and password, and click **Login** button to log in the device.
10. Enter the HTTPS settings interface.
Configuration > Remote Configuration > Network Settings > HTTPS
11. Create the self-signed certificate or authorized certificate.

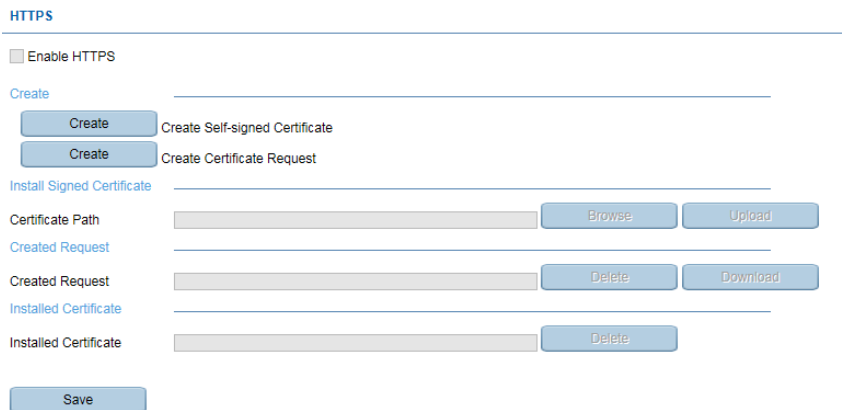


Figure 11. 28 HTTPS Settings

OPTION 1: Create the self-signed certificate

- 1) Click the **Create** button to create the following dialog box.

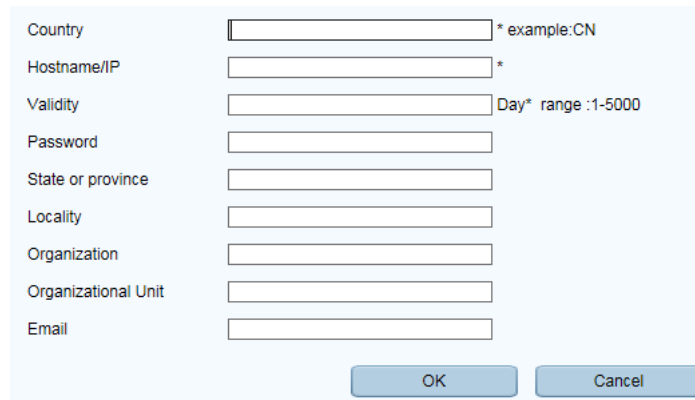


Figure 11. 29 Create Self-signed Certificate

- 2) Enter the country, host name/IP, validity and other information.
- 3) Click **OK** to save the settings.

OPTION 2: Create the authorized certificate

- 4) Click the **Create** button to create the certificate request.
- 5) Download the certificate request and submit it to the trusted certificate authority for signature.
- 6) After receiving the signed valid certificate, import the certificate to the device.

12. There will be the certificate information after you successfully create and install the certificate.

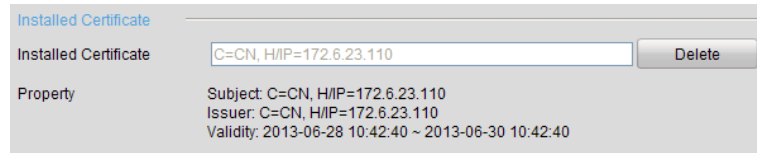


Figure 11. 30 Installed Certificate Property

13. Check the checkbox to enable the HTTPS function.

14. Click the **Save** button to save the settings.

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. 31.

Working Mode	Net Fault-tolerance
Select NIC	bond0
NIC Type	10M/100M/1000M Self-adaptive
Enable DHCP	<input type="checkbox"/>
IPv4 Address	172 .6 .21 .159
IPv4 Subnet Mask	255 .255 .255 .0
IPv4 Default Gateway	172 .6 .21 .1
IPv6 Address 1	fec0::a:240:48ff:fe62:dcd/64
IPv6 Address 2	2002:ac06:1578:a:240:48ff:fe62:dcd/64
IPv6 Default Gateway	
MAC Address	00:40:48:62:0d:cd
MTU(Bytes)	1500
Preferred DNS Server	
Alternate DNS Server	
Main NIC	LAN1

Figure 11. 31 Network Settings Interface

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

Enable Server Authentication	<input type="checkbox"/>
User Name	
Password	
SMTP Server	xxx.smtp.com
SMTP Port	25
Enable SSL	<input type="checkbox"/>
Sender	name1
Sender's Address	name1@xxx.com
Select Receivers	Receiver 1
Receiver	name2
Receiver's Address	name2@xxx.com
Enable Attached Picture	<input checked="" type="checkbox"/>
Interval	2s

Figure 11. 32 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 name of sender's account registered on the SMTP server.

Password: The password of sender's account registered on the SMTP server.

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.

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.

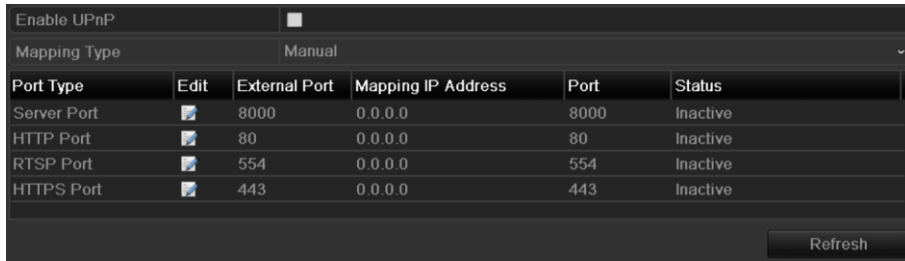


Figure 11. 33 UPnP™ Settings Interface

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.

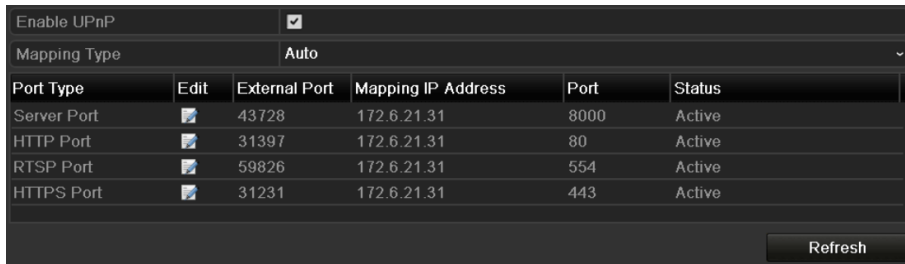


Figure 11. 34 UPnP™ Settings Finished-Auto

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.



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

- 2) External Port indicates the port No. for port mapping in the router.
- 3) 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.

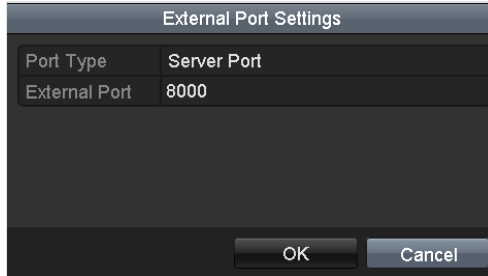


Figure 11. 35 External Port Settings Dialog Box

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

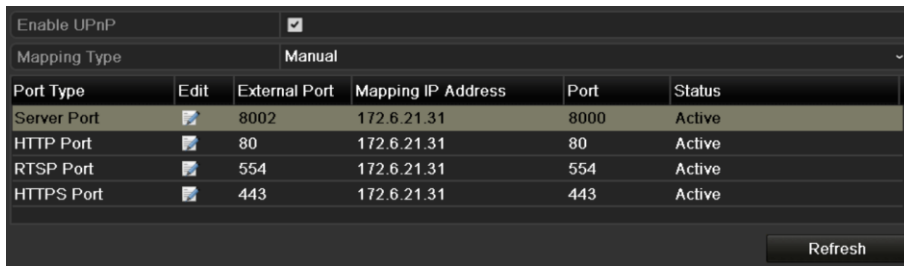


Figure 11. 36 UPnP™ Settings Finished-Manual

● **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.

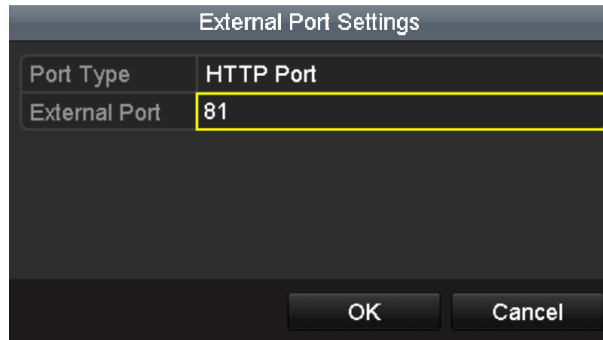


Figure 11. 37 External Port Settings Dialog Box

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. 38 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.

11.2.12 Configuring High-speed Download

Purpose:

You can enable the High-speed Download function to widen the outgoing bandwidth of the device. In this way you can speed up the download of record files through web browser or CMS software.



If you enable the high-speed download function, the outgoing bandwidth of the device will be increased by 40Mbps and the local menu operation will be affected. It is recommended to disable this function after finishing the remote downloading of record files.

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. 24.

3. Check the checkbox of **Enable High-speed Download**. And click the **OK** button in the pop-up message box to confirm the settings.



Figure 11. 39 High-speed Download Settings Menu

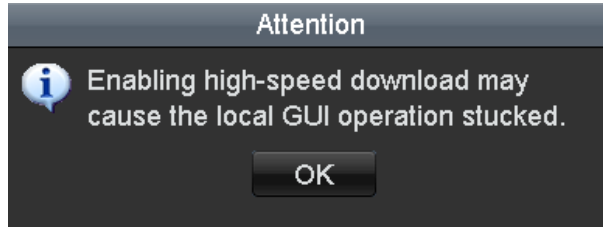


Figure 11. 40 Message Box of High-speed Download

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

11.2.13 Configuring Virtual Host

Purpose:

You can directly get access to the IP camera management interface after enabling this function.



The Virtual host function can be only configured through the web browser.

Steps:

1. Enter the Advanced settings interface, as shown in the Figure 11. 41.
Configuration > Remote Configuration > Network Settings > Advanced

Advanced

Alarm Host IP

Alarm Host Port

Multicast Address

Enable Virtual Host

Enable Telnet

Figure 11. 41 Advanced Settings Interface

2. Check the checkbox of the **Enable Virtual Host**.
3. Click the **Save** button to save the setting.
4. Enter the IP camera management interface of NVR. The Connect column appears on the right-most side of the camera list, as shown in the Figure 11. 42.
Configuration > Remote Configuration > Camera Management > IP Camera

IP Camera

<input type="checkbox"/> Channel No.	IP Camera Address	Channel No.	Management Port	Status	Protocol	Connect
<input type="checkbox"/> D01	192.168.1.2	1	8000	Online	Default	http://192.168.1.2:80
<input type="checkbox"/> D02	192.168.1.3	1	8000	Online	Default	http://192.168.1.3:80

Figure 11. 42 Connect to IP Camera

5. Click the link and the page of IP camera management appears.

11.2.14 Configuring Telnet

Purpose:

Telnet function provides an easy way to get access to the NVR. You can see the advanced information about the device by inputting command; as well the configuration can also be realized through telnet connection.

Steps:

1. Enter the Advanced settings interface, as shown in the Figure 11. 41.
Configuration > Remote Configuration > Network Settings > Advanced
2. Check the checkbox of the **Enable Telnet**.
3. Click the **Save** button to save the setting.
4. You can open the Command Prompt window in your PC, and input "telnet *IP Address*" to connect with the NVR, as shown in the figure below.

Example:

If the IP address of the NVR is 192.0.0.64, you can input "telnet 192.0.0.64" and then press Enter to connect to the NVR.

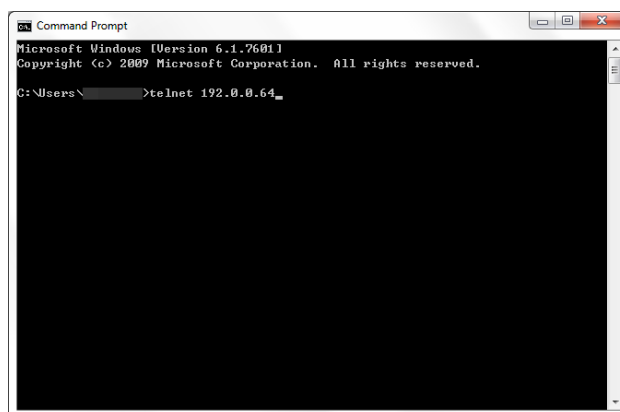


Figure 11. 43 Connect to NVR



The telnet function turns invalid after the device shutting down or rebooting, you have to enable it again if required.

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. 44 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. 45.

Figure 11. 45 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.

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/eSATA, 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 dropdown list of Device Name, as shown in Figure 11. 46.



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.

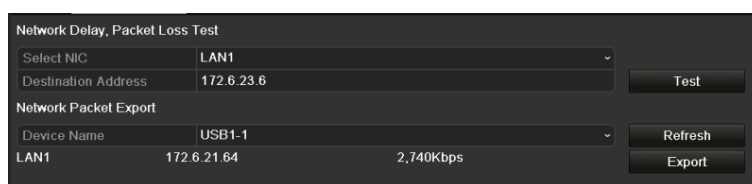


Figure 11. 46 Export Network Packet

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. 47.



Figure 11. 47 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.

Steps:

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

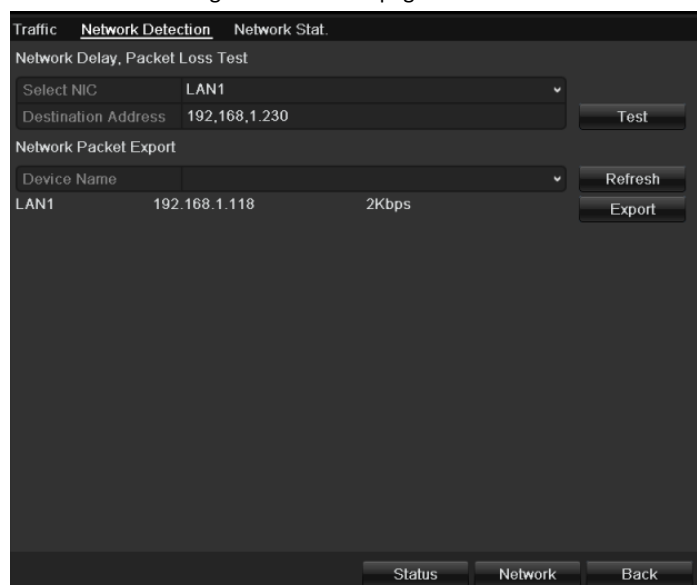


Figure 11. 48 Network Status Checking

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

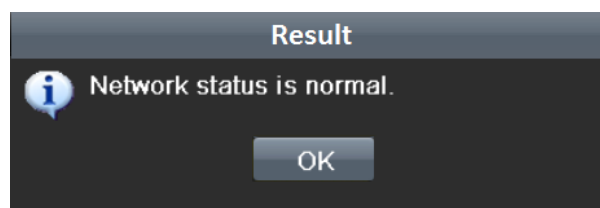


Figure 11. 49 Network Status Checking Result

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

11.4.4 Checking Network Statistics

Purpose:

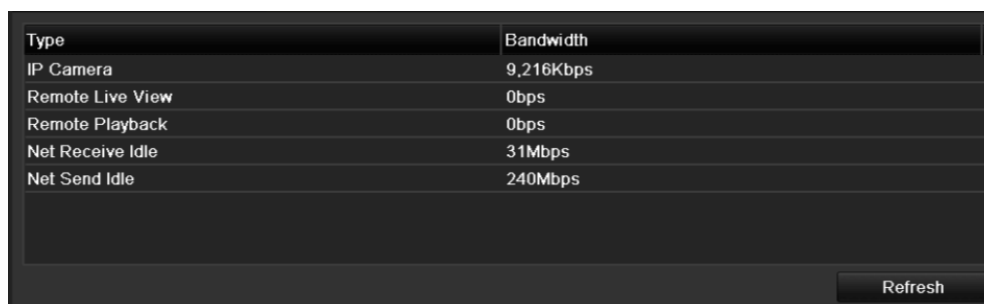
You can check the network status to obtain the real-time information of NVR.

Steps:

1. Enter the Network Detection interface.

Menu>Maintenance>Net Detect

2. Choose the **Network Stat.** tab.



Type	Bandwidth
IP Camera	9,216Kbps
Remote Live View	0bps
Remote Playback	0bps
Net Receive Idle	31Mbps
Net Send Idle	240Mbps

Figure 11. 50 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 HDDs

Purpose:

A newly installed hard disk drive (HDD) must be initialized before it can be used with your NVR.

Steps:

1. Enter the HDD Information interface.

Menu > HDD > General



Figure 12. 9 HDD Information Interface

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

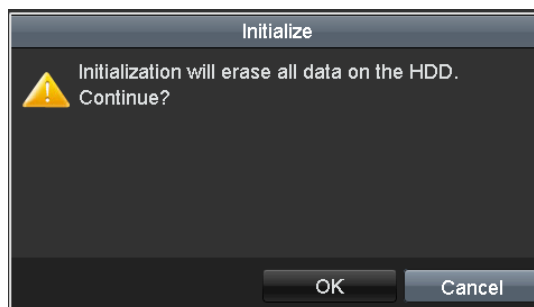


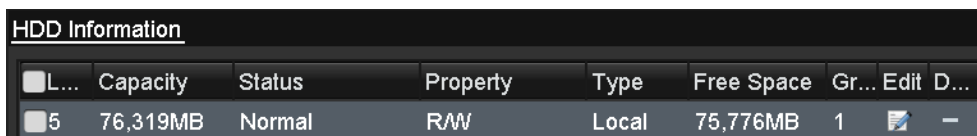
Figure 12. 10 Confirm Initialization

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

L...	Capacity	Status	Property	Type	Free Space	Gr...	Edit	D...
5	76,319MB	Initializing 20%	R/W	Local	0MB	1	-	-

Figure 12. 11 Status changes to Formatting

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



The screenshot shows a table titled "HDD Information" with the following data:

<input type="checkbox"/> L...	Capacity	Status	Property	Type	Free Space	Gr...	Edit	D...
<input type="checkbox"/> 5	76,319MB	Normal	RAW	Local	75,776MB	1		-

Figure 12. 12 HDD Status Changes to Normal

Note: Initializing the HDD will erase all data on it.

12.2 Managing Network HDD

Purpose:

You can add the allocated NAS or disk of IP SAN to NVR, and use it as network HDD.

Steps:

1. Enter the HDD Information interface.
Menu > HDD>General
2. Click the **Add** button to enter the Add NetHDD interface, as shown in Figure 12. 13.

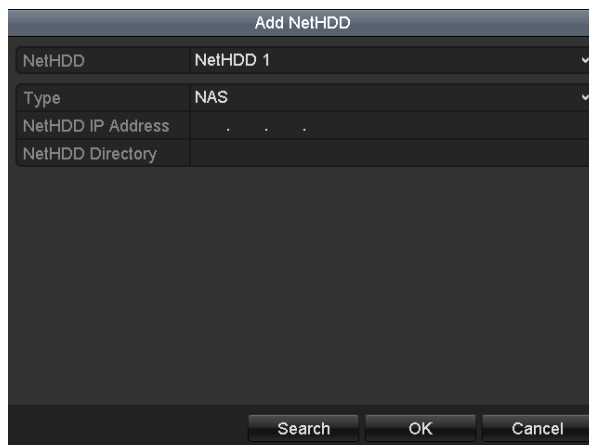


Figure 12. 13 HDD Information Interface

3. Add the allocated NetHDD.
4. Select the type to NAS or IP SAN.
5. Configure the NAS or IP SAN settings.
 - **Add NAS disk:**
 - 1) Enter the NetHDD IP address in the text field.
 - 2) Enter the NetHDD Directory in the text field.
 - 3) Click the **OK** button to add the configured NAS disk.

Note: Up to 8 NAS disks can be added.

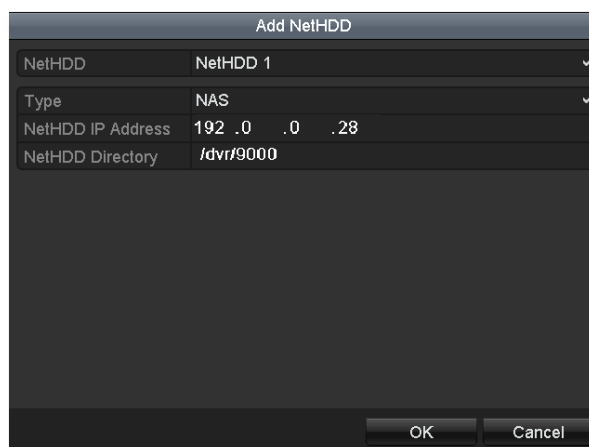


Figure 12. 14 Add NAS Disk

- **Add IP SAN:**

- 1) Enter the NetHDD IP address in the text field.
- 2) Click the **Search** button to the available IP SAN disks.
- 3) Select the IP SAN disk from the list shown below.
- 4) Click the **OK** button to add the selected IP SAN disk.

Note: Up to 1 IP SAN disk can be added.

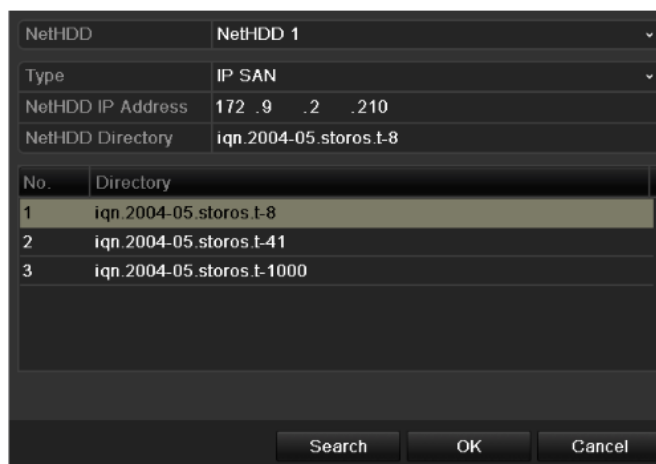


Figure 12. 15 AddIP SAN Disk

6. After having successfully added the NAS or IP SAN disk, return to the HDD Information menu. The added NetHDD will be displayed in the list.

Note: If the added NetHDD is uninitialized, please select it and click the **Init** button for initialization.

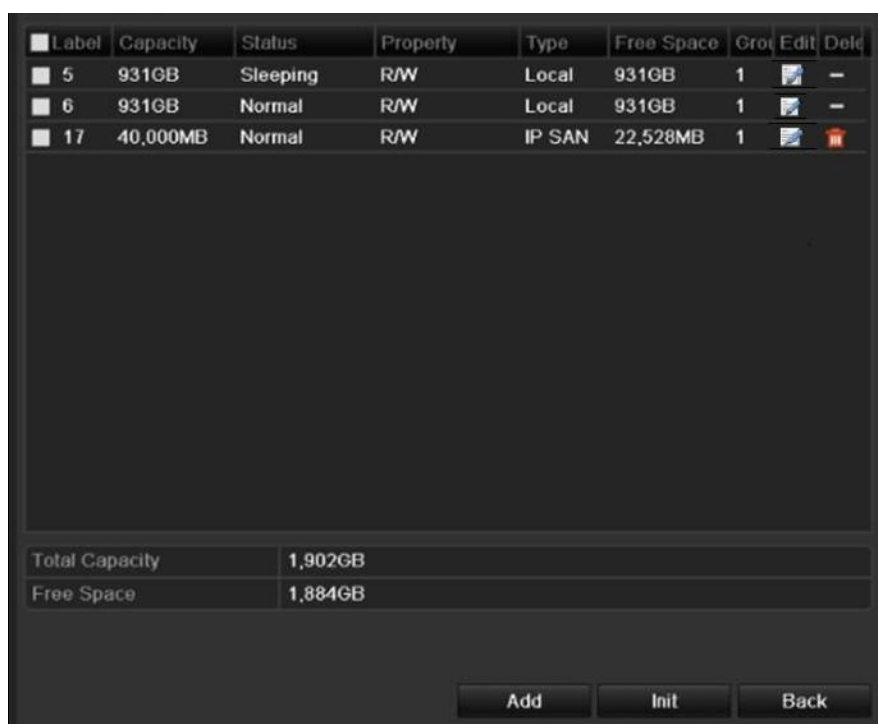


Figure 12. 16 Initialize Added NetHDD

12.3 Managing HDD Group

12.3.1 Setting HDD Groups

Purpose:

Multiple HDDs can be managed in groups. Video from specified channels can be recorded onto a particular HDD group through HDD settings.

Steps:

1. Enter the Storage Mode interface.
Menu > HDD > Advanced
2. Set the **Mode** to Group, as shown in Figure 12. 17.



Figure 12. 17 Storage Mode Interface

3. Click the **Apply** button and the following Attention box will pop up.

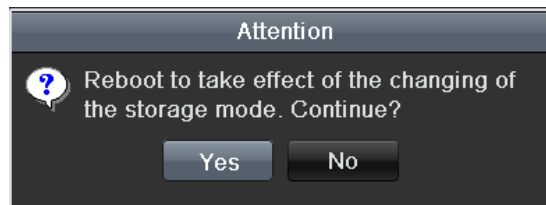


Figure 12. 18 Attention for Reboot


4. Click the **Yes** button to reboot the device to activate the changes.
5. After reboot of device, enter the HDD Information interface.
Menu > HDD> General
6. Select HDD from the list and click  icon to enter the Local HDD Settings interface, as shown in Figure 12. 19.



Figure 12. 19 Local HDD Settings Interface

7. Select the Group number for the current HDD.

Note: The default group No. for each HDD is 1.

8. Click the **OK** button to confirm the settings.

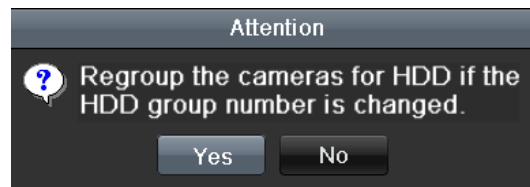


Figure 12. 20 Confirm HDD Group Settings

9. In the pop-up Attention box, click the **Yes** button to finish the settings.

12.3.2 Setting HDD Property

Purpose:

The HDD property can be set to redundancy, read-only or read/write (R/W). Before setting the HDD property, please set the storage mode to Group (refer to step1-4 of Chapter Setting HDD Groups).

A HDD can be set to read-only to prevent important recorded files from being overwritten when the HDD becomes full in overwrite recording mode.

When the HDD property is set to redundancy, the video can be recorded both onto the redundancy HDD and the R/W HDD simultaneously so as to ensure high security and reliability of video data.

Steps:


1. Enter the HDD Information interface.
Menu > HDD > General
2. Select HDD from the list and click the  icon to enter the Local HDD Settings interface, as shown in Figure 12. 21.



Figure 12. 21 Set HDD Property

3. Set the HDD property to R/W, Read-only or Redundancy.
4. Click the **OK** button to save the settings and exit the interface.
5. In the HDD Information menu, the HDD property will be displayed in the list.

Note: At least 2 hard disks must be installed on your NVR when you want to set a HDD to Redundancy, and there is one HDD with R/W property.

12.4 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
2. Set the **Mode** to Quota, as shown in Figure 12. 22.

Note: The NVR must be rebooted to enable the changes to take effect.

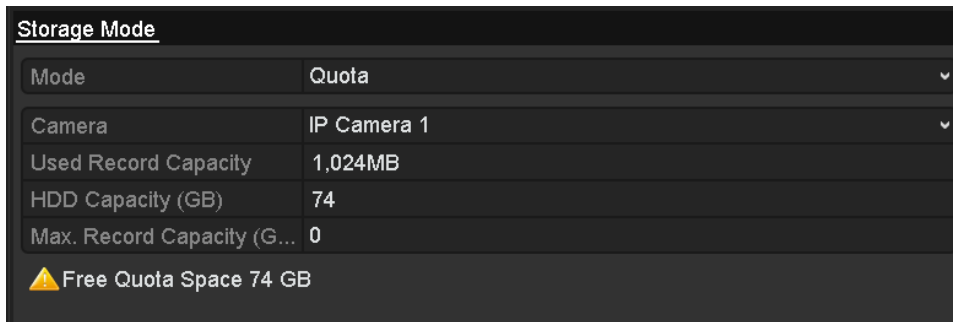


Figure 12. 22 Storage Mode Settings Interface

3. Select a camera for which you want to configure quota.
4. Enter the storage capacity in the text fields of **Max. Record Capacity (GB)**, as shown in Figure 12. 23.

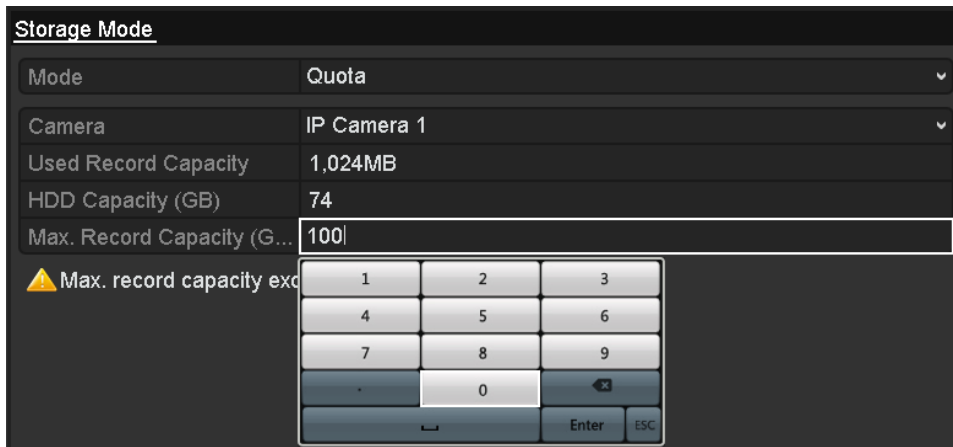


Figure 12. 23 Configure Record/Picture Quota

5. You can copy the quota settings of the current camera to other cameras if required. Click the **Copy** button to enter the Copy Camera menu, as shown in Figure 12. 24.

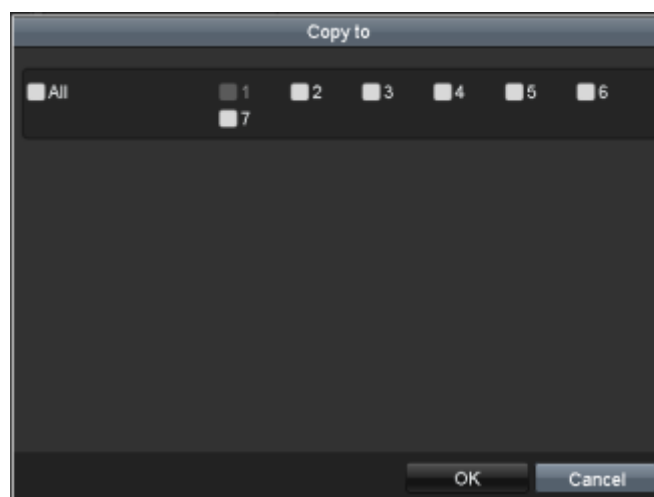


Figure 12. 24 Copy Settings to Other Camera(s)

-
6. Select the camera (s) to be configured with the same quota settings. You can also click the checkbox of IP Camera to select all cameras.
 7. Click the **OK** button to finish the Copy settings and back to the Storage Mode interface.
 8. Click the **Apply** button to apply the settings.

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

12.5 Checking HDD Status

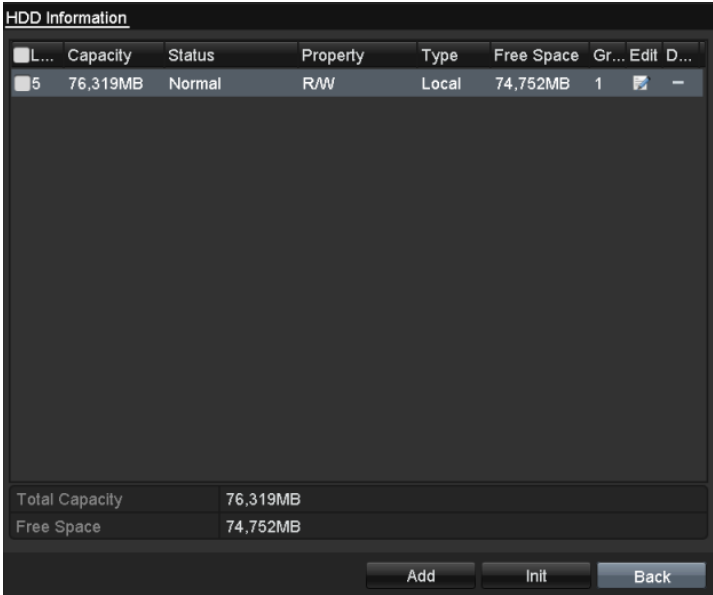
Purpose:

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. 25.



L...	Capacity	Status	Property	Type	Free Space	Gr...	Edit D...
5	76,319MB	Normal	R/W	Local	74,752MB	1	[-]

Total Capacity: 76,319MB
Free Space: 74,752MB

Add Init Back

Figure 12. 25 View HDD Status (1)

Note: If the status of HDD is *Normal* or *Sleeping*, 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 status of each HDD displayed on the list, as shown in Figure 12. 26.

Label	Status	Capacity	Free Space	Property	Type	Group
5	Normal	76,319MB	74,752MB	R/W	Local	1

Total Capacity	76,319MB
Free Space	74,752MB

Back

Figure 12. 26 View HDD Status (2)

12.6 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 Detec >S.M.A.R.T.
2. Select the HDD to view its S.M.A.R.T. information list, as shown in Figure 12. 27.

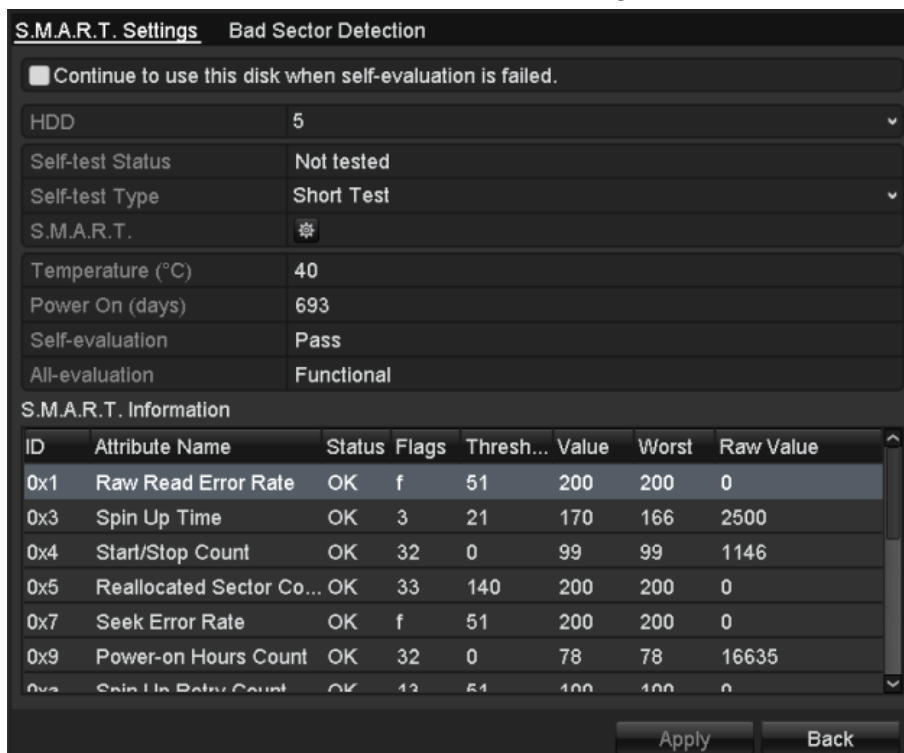


Figure 12. 27 S.M.A.R.T. Settings Interface

The related information of the S.M.A.R.T. is shown on the interface.

You can choose the self-test types as Short Test, Expanded Test or the Conveyance Test.

Click the start button to start the S.M.A.R.T. HDD self-evaluation.



Note: 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. Enter the Bad Sector Detection tab page.
2. Select in the dropdown list of the HDD you want to configure

3. Click the **Detect** button to start the detection

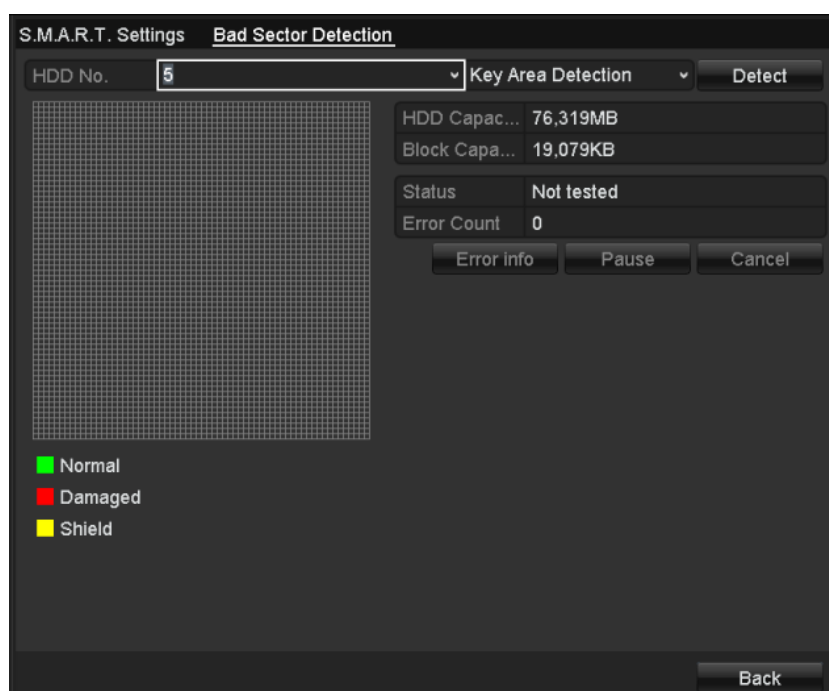


Figure 12. 28 Bad Sector Detection

4. If the HDD is normal you can see the green color icon on the screen, otherwise the red icon is shown. And you can click Error info button to see the detailed damage information And you can also pause or cancel the detection.

12.7 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 to **HDD Error** from the dropdown list.
3. Click the checkbox(s) below to select the HDD error alarm type (s), as shown in Figure 12. 29.

Note: The alarm type can be selected to: Audio Warning, Notify Surveillance Center, Send Email and Trigger Alarm Output. Please refer to *Chapter Setting Alarm Response Actions*.

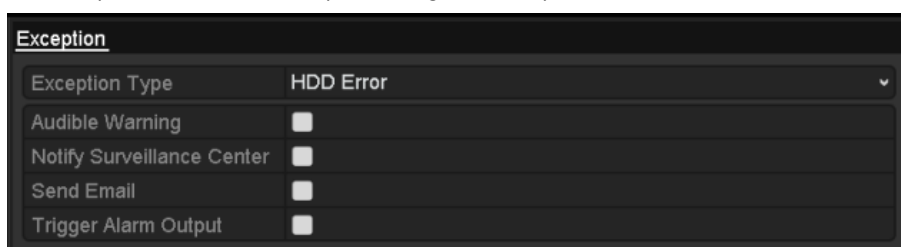


Figure 12. 29 Configure HDD Error Alarm

4. When the Trigger Alarm Output is selected, you can also select the alarm output to be triggered from the list below.
5. 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 OSD settings.
3. Edit the Camera Name in the text field.
4. Configure the Display Name, Display Date and Display Week by clicking the checkbox.
5. Select the Date Format, Time Format and Display Mode.

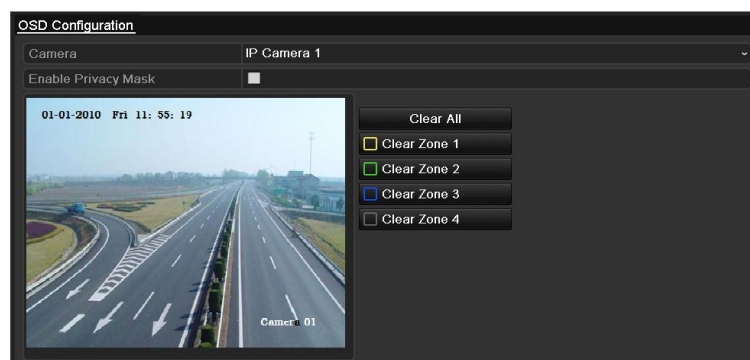


Figure 13. 9 OSD Configuration Interface

6. You can use the mouse to click and drag the text frame on the preview window to adjust the OSD position.
7. Click the **Apply** button to apply 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. Click the checkbox of **Enable Privacy Mask** to enable this feature.

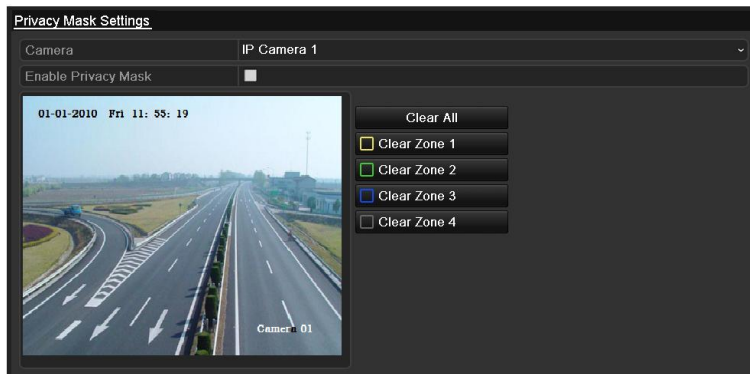


Figure 13. 10 Privacy Mask Settings Interface

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

Note: Up to 4 privacy masks 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.

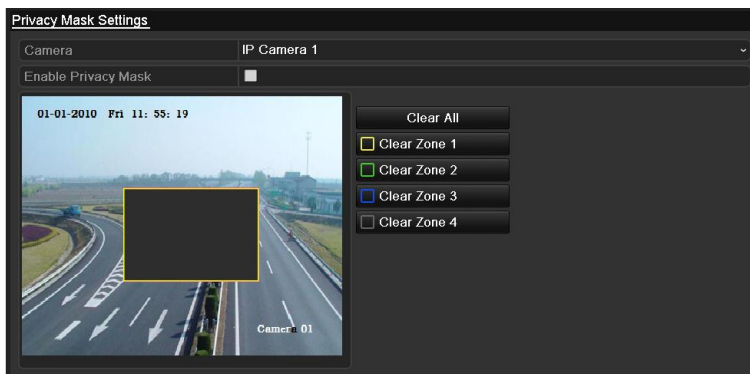


Figure 13. 11 Set Privacy Mask Area

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. 12 Image Settings Interface

2. Select the camera to set image parameters.
3. You can click on the arrow 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** tab to enter the Device Information menu to view the device name, model, serial No. , firmware version and encode version, as shown in Figure 14. 9.

<u>Device Info</u>	Camera	Record	Alarm	Network	HDD
Device Name	XXXXXXXXXX				
Model	XXXXXXXXXX				
Serial No.	XXXXXXXXXXXXXXXXXXXX				
Firmware Version	V X.X.X				
Encoding Version	V X.X.X				

Figure 14. 9 Device Information Interface

14.1.2 Viewing Camera Information

Steps:

1. Enter the System Information interface.
Menu >Maintenance>Camera
2. Click the **Camera** tab to enter the Camera Information menu to view the status of each camera, as shown in Figure 14. 10.

<u>Device Info</u>	<u>Camera</u>	Record	Alarm	Network	HDD
Camer...	Camera Name	Status	Motion Det...	Video Tamp...	Video Loss
D1	IPCamera 01	Connected	Occur	Not used	Used
D2	IPCamera 02	Disconnected	Not support...	Not supported	Not support...
D3	IPCamera 03	Disconnected	Not support...	Not supported	Not support...
D4	IPCamera 04	Disconnected	Not support...	Not supported	Not support...
D5	IPCamera 05	Disconnected	Not support...	Not supported	Not support...
D6	IPCamera 06	Disconnected	Not support...	Not supported	Not support...
D7	IPCamera 07	Disconnected	Not support...	Not supported	Not support...
D8	IPCamera 08	Disconnected	Not support...	Not supported	Not support...

Figure 14. 10 Camera Information Interface

14.1.3 Viewing Record Information

Steps:

1. Enter the System Information interface.
Menu >Maintenance>System Info
2. Click the **Record** tab to enter the Record Information menu to view the recording status encoding parameters of each camera, as shown in Figure 14. 11.

Device Info	Camera	Record	Alarm	Network	HDD			
Camer...	Recor...	Stream...	Frame ...	Bitrate(Kbps)	Resolution	Recor...	Encodi...	Redun...
D1	Used	Video ...	30fps	2048	704*576(4...	Normal	Event	No
D2	Not used	Video ...	30fps	2048	Unknown ...		Normal	No
D3	Not used	Video ...	30fps	2048	Unknown ...		Normal	No
D4	Not used	Video ...	30fps	2048	Unknown ...		Normal	No
D5	Not used	Video ...	30fps	2048	Unknown ...		Normal	No
D6	Not used	Video ...	30fps	2048	Unknown ...		Normal	No
D7	Not used	Video ...	30fps	2048	Unknown ...		Normal	No
D8	Not used	Video ...	30fps	2048	Unknown ...		Normal	No

Figure 14. 11 Record Information Interface

14.1.4 Viewing Alarm Information

Steps:

1. Enter the System Information interface.
Menu >Maintenance>System Info
2. Click the **Alarm** tab to enter the Alarm Information menu to view the alarm information, as shown in Figure 14. 12.

Device Info	Camera	Record	Alarm	Network	HDD
No.	Alarm Name	Alarm Type	Alarm Status	Triggered Camera	
D2<-1		N.O	Used	D1~D4	
D2->1		Not supported	Used		

Figure 14. 12 Alarm Information Interface

14.1.5 Viewing Network Information

Steps:

1. Enter the System Information interface.
Menu >Maintenance>System Info
2. Click the **Network** tab to enter the Network Information menu to view the network information, as shown in Figure 14. 13.

Device Info		Camera	Record	Alarm	<u>Network</u>	HDD
NIC		LAN1				
IPv4 Address		192.168.1.250				
IPv4 Subnet Mask		255.255.255.0				
IPv4 Default Gateway		192.168.10.1				
IPv6 Address 1		fe80::8ee7:48ff:fe12:79af/64				
IPv6 Address 2						
IPv6 Default Gateway						
Preferred DNS Server		0.0.0.0				
Alternate DNS Server		0.0.0.0				
Enable DHCP		Disabled				
Enable PPPOE		Disabled				
PPPOE Address						
PPPOE Subnet Mask						
PPPOE Default Gateway						

Figure 14. 13 Network Information Interface

14.1.6 Viewing HDD Information

Steps:

1. Enter the System Information interface.
Menu >Maintenance>System Info
2. Click the **HDD** tab to enter the HDD Information menu to view the HDD status, free space, property, etc., as shown in Figure 14. 14.

Device Info		Camera	Record	Alarm	Network	<u>HDD</u>
Label	Status	Capacity	Free Space	Property	Type	Group
5	Normal	76,319MB	74,752MB	R/W	Local	1
Total Capacity		76,319MB				
Free Space		74,752MB				
Back						

Figure 14. 14 HDD 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 Search

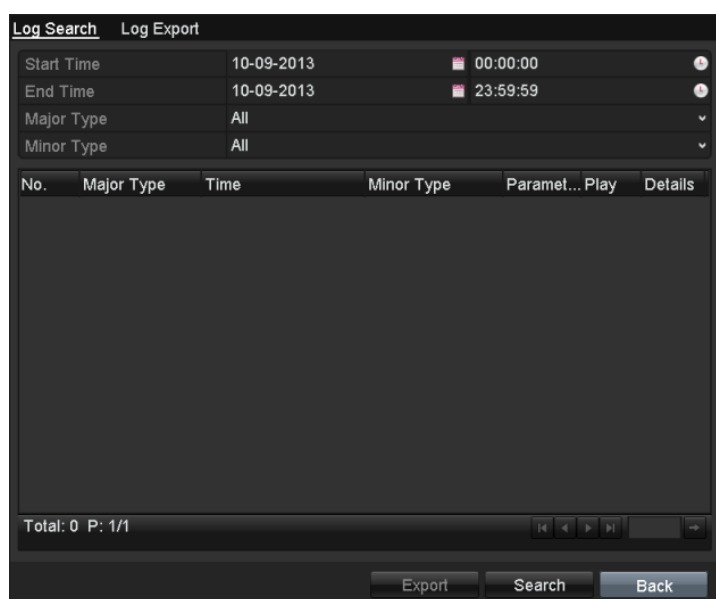


Figure 14. 15 Log Search Interface

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

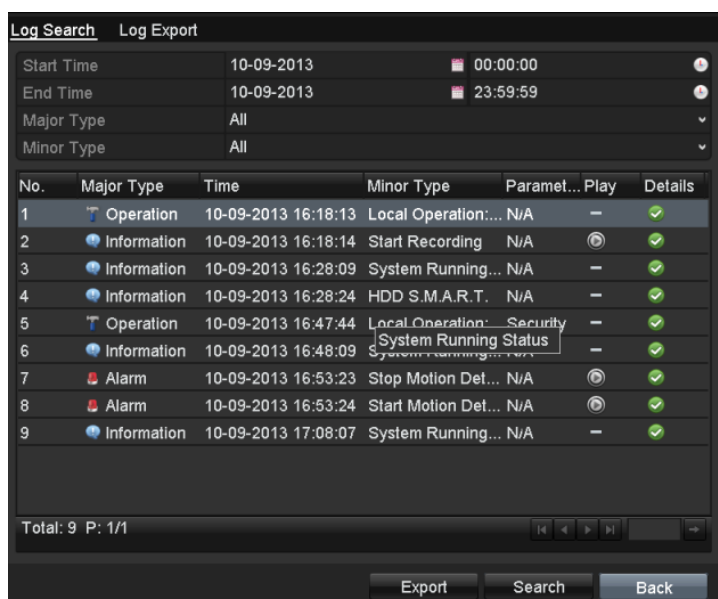


Figure 14. 16 Log Search Results

Note: Up to 2000 log files can be displayed each time.


5. You can click the  button of each log or double click it to view its detailed information, as shown in

Figure 14. 17. And you can also click the  button to view the related video files if available.

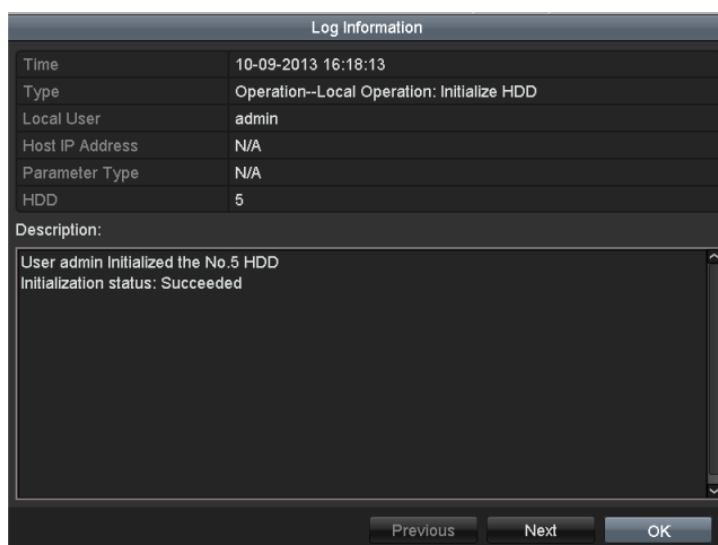


Figure 14. 17 Log Details

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

18.

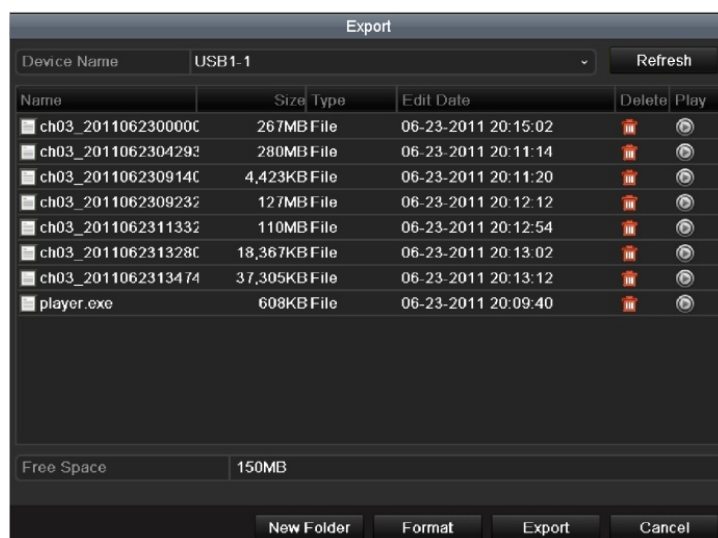


Figure 14. 18 Export Log Files

7. Select the backup device from the dropdown 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.

Notes:

- 1) Please connect the backup device to NVR before operating log export.
- 2) The log files exported to the backup device are named by exporting time, e.g., *20110514124841logBack.txt*.

To export all the log files:

You can enter the Log Export interface.

Menu> Maintenance> Log Information> Log Export

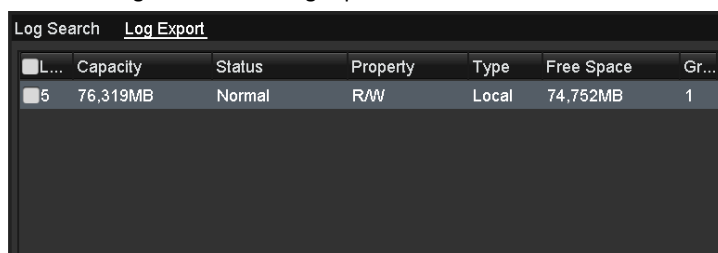


Figure 14. 19 Log Export Interface

You can check the checkbox of the HDD.

Click the Export button to export all the log files stored in the HDD.

14.3 Importing/Exporting Configuration Files

Purpose:

The configuration files of the NVR can be exported to local device for backup; 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

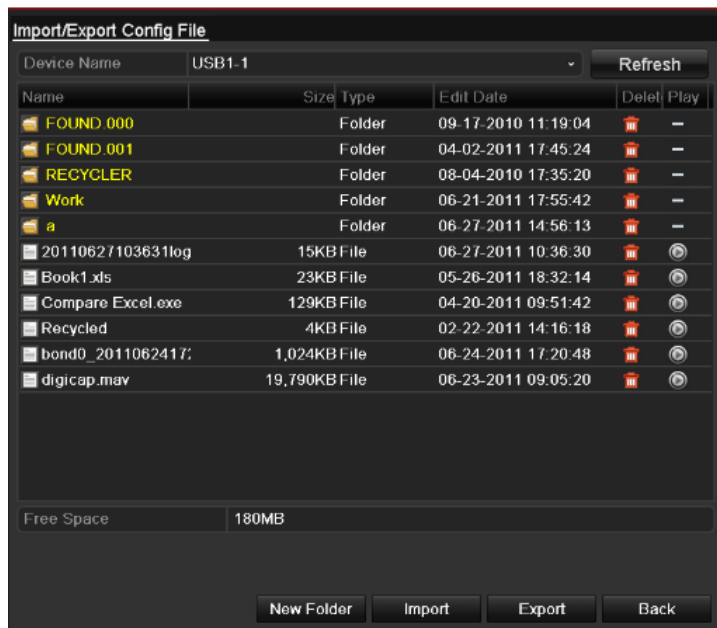


Figure 14. 20 Import/Export Config File

2. Click the **Export** button to export configuration files to the selected local backup device.
3. 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.

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

14.4 Upgrading System

Purpose:

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

14.4.1 Upgrading by Local Backup Device

Steps:

1. Connect your NVR with a local backup device where the update firmware file is located.
2. Enter the Upgrade interface.
Menu >Maintenance>Upgrade
3. Click the **Local Upgrade** tab to enter the local upgrade menu, as shown in Figure 14. 21.

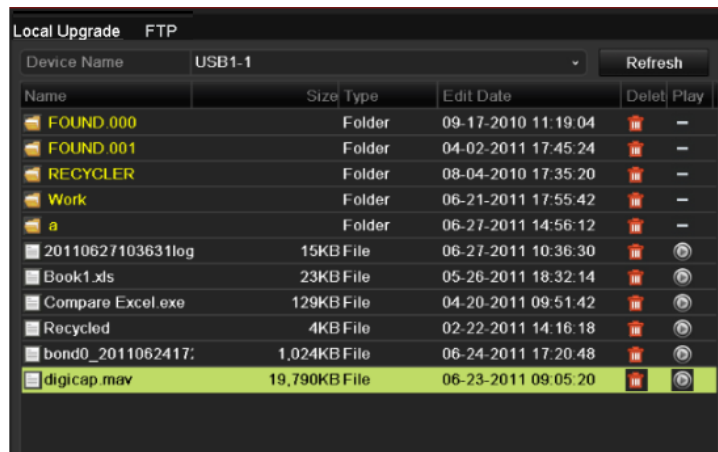


Figure 14. 21 Local Upgrade Interface

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

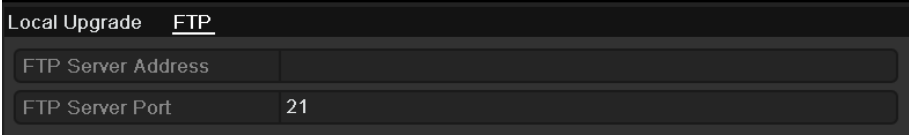
14.4.2 Upgrading by FTP

Before you start:

Configure PC (running FTP server) and NVR to the same Local Area Network. Run the 3rd-party TFTP software on the PC and copy the firmware into the root directory of TFTP.

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. 22.



The screenshot shows a dark-themed interface for a local upgrade. At the top, there are two tabs: 'Local Upgrade' and 'FTP'. Below the tabs, there are two input fields. The first field is labeled 'FTP Server Address' and is currently empty. The second field is labeled 'FTP Server Port' and contains the number '21'.

Figure 14. 22 FTP Upgrade Interface

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

14.5 Restoring Default Settings

Steps:

1. Enter the Default interface.

Menu > Maintenance > Default

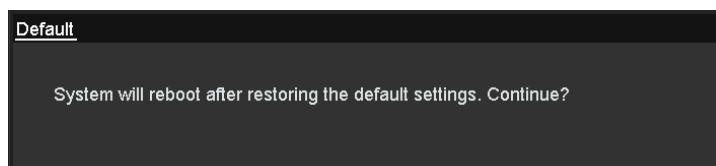


Figure 14. 23 Restore Factory Default

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

Note: Except the network parameters (including IP address, subnet mask, gateway, MTU, default route and server port), all other parameters of the device will be restored to factory default settings.

Chapter 15 Others

15.1 Configuring General Settings

Purpose:

You can configure the output resolution, system time, mouse pointer speed through the Menu > Configuration > General interface.

Steps:

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

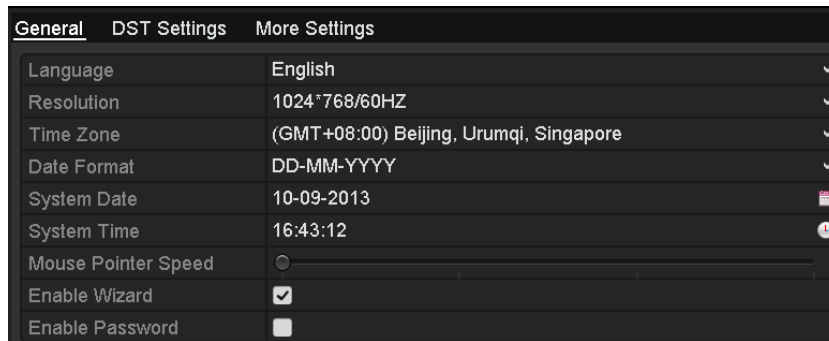


Figure 15.9 General Settings Interface

3. Configure the following settings:
 - **Language:** The default language used is *English*.
 - **Resolution:** Select the output resolution, 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 ID Authentication:** 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.

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

Figure 15. 10 DST Settings Interface

You can check the checkbox before the 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 Device Parameters

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. 11.

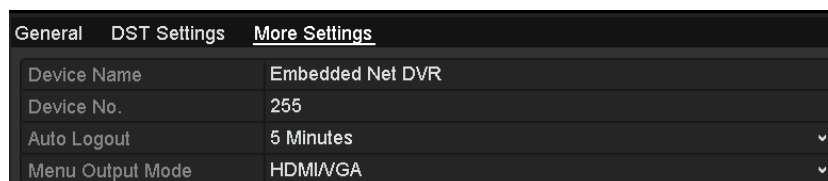


Figure 15. 11 More Settings Interface

3. Configure the following settings:
 - **Device Name:** Edit the name of NVR.
 - **Device No.:** Edit the serial number of NVR. The Device No. can be set in the range of 1~255, and the default No. is 255. The number is used for the remote and keyboard control.
 - **Operation Timeout:** Set timeout time for menu inactivity. E.g.,when the timeout time is set to 5 *Minutes*, then the system will exit from the current operation menu to live view screen after 5 minutes of menu inactivity.
 - **Menu Output Mode:** You can choose the menu display on different video output.
4. Click the **Apply** button to save the settings.

15.4 Configuring POS


Steps:

1. Enter the **POS Settings** interface.
Menu > Configuration > POS
2. Select the **POS Setting** tab to enter the POS Settings interface.



Figure 15.4 POS Settings Interface

3. Check the **POS** checkbox to enable this feature. Enter **POS Name** and **Select connection type**.
"TCP Receive" or "RS232" optional
4. Connection can be used in two ways
 - **TCP Receive Setting**

Click the  icon of **TCP Receive port** to set receive port of **POS**. Through the port settings, Data- directed transmission can be successfully between POS server and DVR/NVR

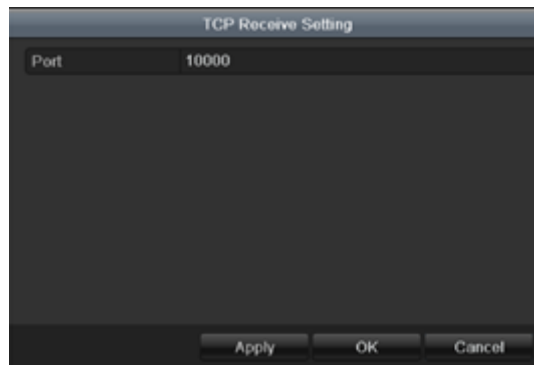


Figure 15.5 TCP Receive port Settings Interface

- **RS232 Setting**

Purpose: The RS-232 port can be used in two ways:

- Parameters Configuration: Connect a PC to the device through the PC serial port. Device parameters can be configured by using software such as HyperTerminal. The serial port parameters must be the same as the device's when connecting with the PC serial port.
- Transparent Channel: Connect a serial device directly to the device. The serial device will be controlled remotely by the PC through the network.

Steps:


Click the  icon of **RS232-setting port** to set receive port of **POS**.



Figure 15.6 RS232-Receive port Settings Interface

Configure RS-232 parameters, including baud rate, data bit, stop bit, parity, flow control and usage. The parameters in DVR should be the same as POS device.

Click Apply to save the settings.

Note: the default usage setting is **“Console”**. When you use RS232-Setting you should changed it as **“Transparent channel”** and restart your device.

5. POS Protocol setting

Note: choose connection type as “RS2323”, protocol items **Generic** and **AVE** are available
 Choose connection type as “TCP Receive”, protocol item only **Generic** is available

● **General POS Setting**

Click the  icon of **POS Protocol** to set **POS settings**.

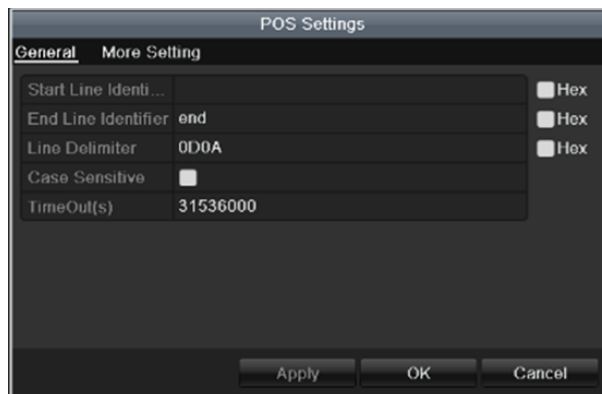


Figure 15.7 General POS Settings Interface

Note: click **“Hex”** enable **“Hex”** character conversion

Note: **“Start Line Identifier”** if the time value is null, that means POS recording is starting all the time, no beginning command. **“End Line Identifier”** if the item value is null, that means POS recording is running all the time, no ending command.

Note: **“Timeout”**: POS network timeout. The POS device is in the connected state over the time period

- **Morel POS Setting**

Click more setting tab of **POS setting** to extra items

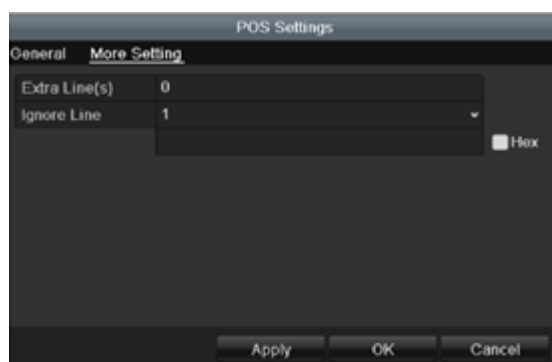


Figure 15.8 More POS Settings Interface

Note: "Extra Line(s)" means you can get extra character after the "End Line Identifier", the value between 0~ 10.

Note: "Ignore Line": max support is 4 lines. If you ignore specific characters, the POS information within the corresponding characters will not display.

- **AVE POS Setting**

Click the  icon of **AVE POS Protocol** to set **POS settings**.

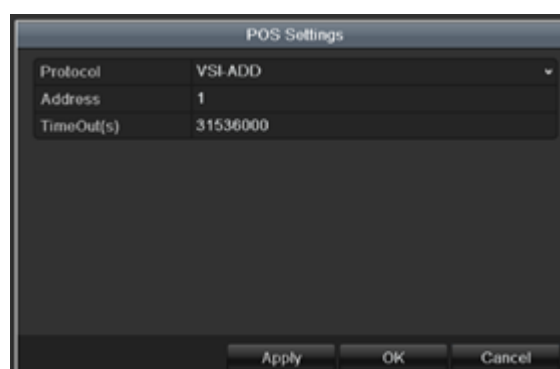



Figure 15.9 AVE POS Settings Interface

Note: "Protocol": VSI-ADD" and "Vnet" available

Note: "Address": POS device's AVE master address.

6. Handle setting

Click the  icon to make **handle settings** about Trigger channel, Handling and PTZ linking (preset, patrol and pattern)

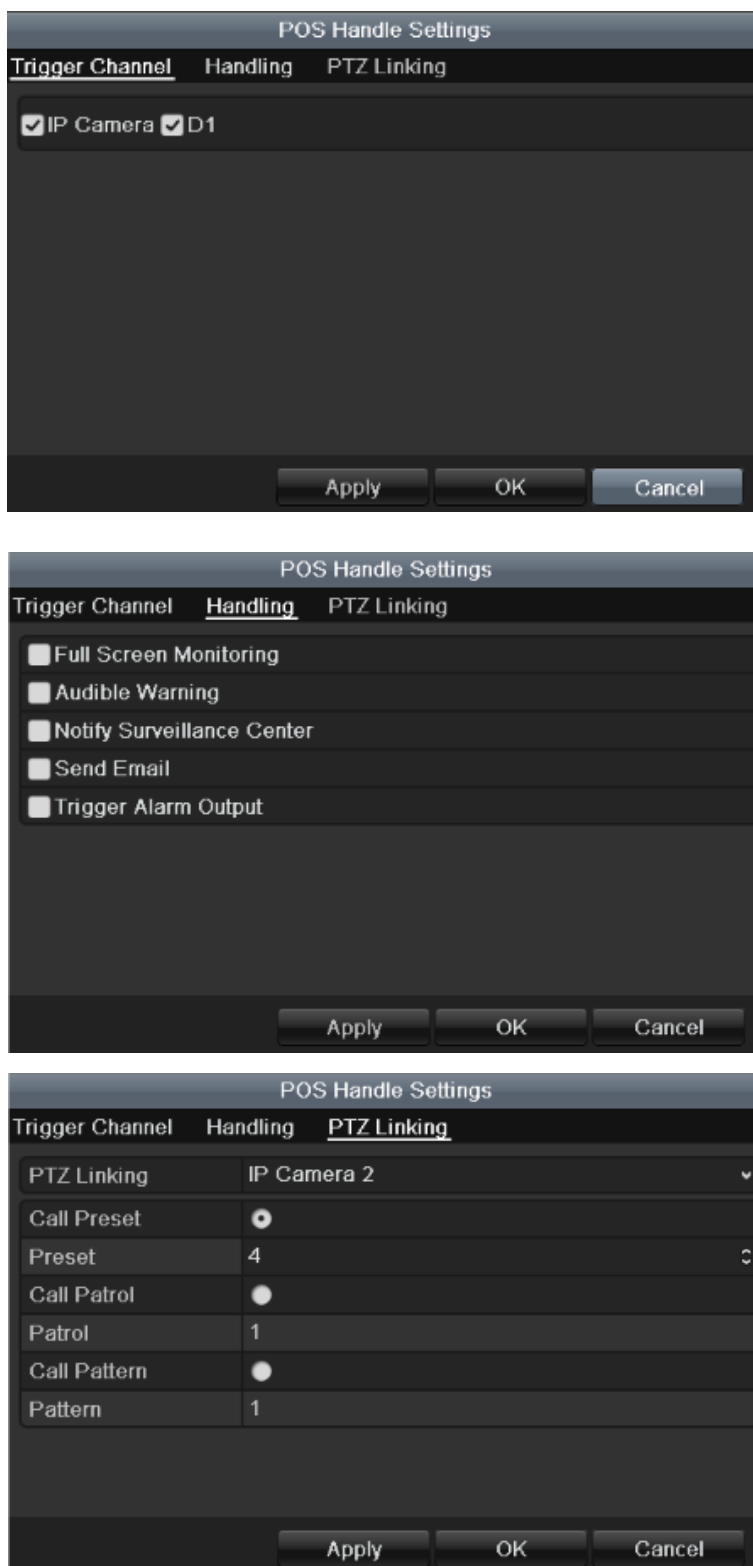


Figure 15.10 POS Handle Settings Interface

Note: "PTZ Linking" is not available until PTZ device has already connected

15.5 Managing User Accounts

Purpose:

There is a default account in the NVR: *Administrator*. The *Administrator* user name is *admin* and the password is *12345*. The *Administrator* has the permission to add and delete user and configure user parameters.

15.5.1 Adding a User

Steps:

1. Enter the User Management interface.
Menu >Configuration>User

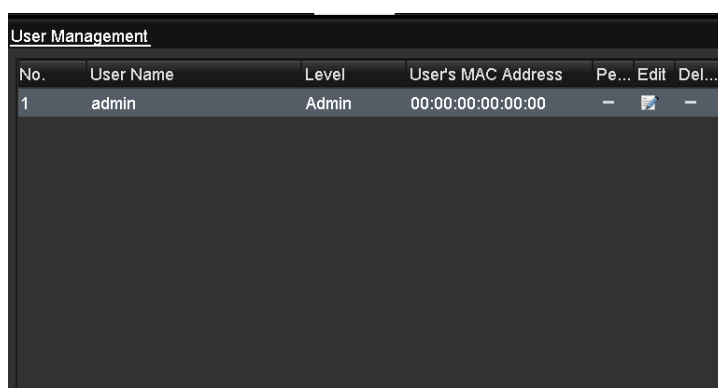
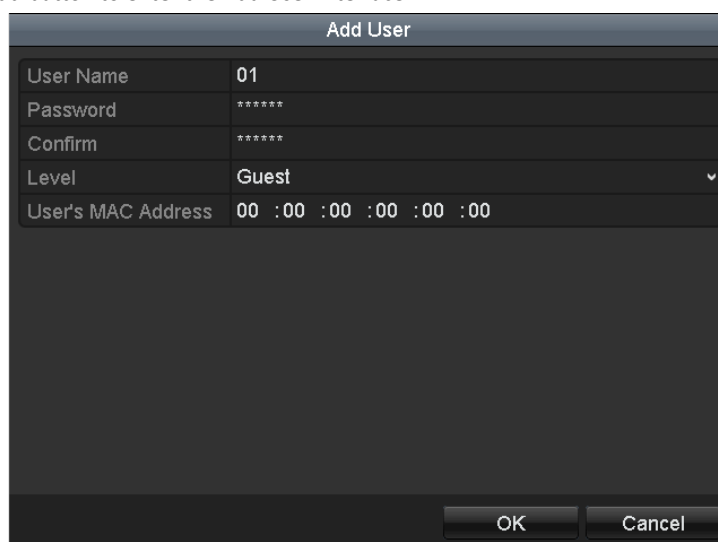


Figure 15. 11 User Management Interface

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



User Name	01
Password	*****
Confirm	*****
Level	Guest
User's MAC Address	00 : 00 : 00 : 00 : 00 : 00

OK Cancel

Figure 15. 12 Add User Menu

3. Enter the information for new user, including **User Name**, **Password**, **Level** and **User's MAC Address**.
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.
 - **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.
 - **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. 13.

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

Figure 15. 13 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. 14.

Figure 15. 14 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, picture capturing and alarm output of the selected camera (s).
- Remote Manual Operation: Remotely starting/stopping manual recording, picture capturing 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.

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

15.5.2 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. 15.


User Management						
No.	User Name	Level	User's MAC Address	Pe...	Edit	Del...
1	admin	Admin	00:00:00:00:00:00	-		-
2	01	Guest	00:00:00:00:00:00			

Figure 15. 15 User List

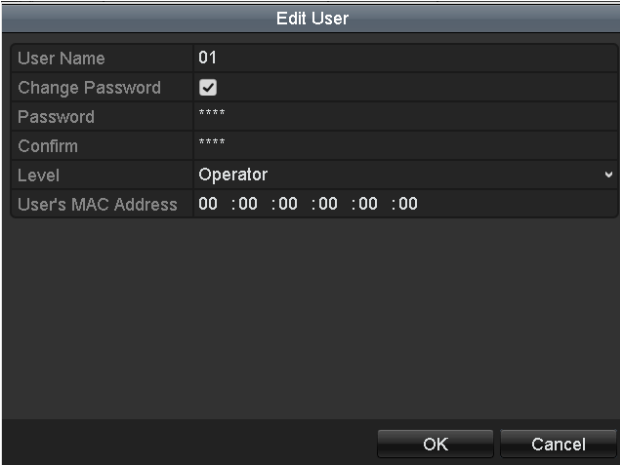
3. Click the icon to delete the selected user.

15.5.3 Editing a User

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. 15.
3. Click the  icon to enter the Edit User interface, as shown in Figure 15. 16.

Note: The admin user can also be edited.



Edit User	
User Name	01
Change Password	<input checked="" type="checkbox"/>
Password	****
Confirm	****
Level	Operator
User's MAC Address	00 :00 :00 :00 :00 :00

Figure 15. 16 Edit User Interface

4. Edit the user information, including user name, password, level and MAC address.
Check the checkbox of **Change Password** if you want to change the password of the current user.
5. Click the **OK** button to save the settings and exit the menu.

15.6 Logging out/Shutting down/Rebooting Device

Steps:

1. Enter the Shutdown interface.

Menu > Shutdown

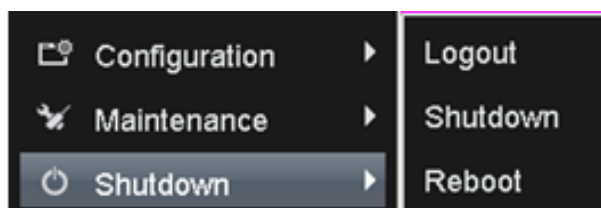


Figure 15. 17 Shutdown Menu

2. Click **Logout** to log out, or

Click **Shutdown** to shut down the device, or

Click **Reboot** to reboot the device.

Note: After you have logged out the system, menu operation on the screen is invalid. It is required a user name and password to log in to the system.

Appendix

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.
- **Hybrid DVR:** A hybrid DVR is a combination of a DVR and NVR.
- **NTP:** Acronym for Network Time Protocol. A protocol designed to synchronize the clocks of computers over a network.
- **NTSC:** Acronym for National Television System Committee. NTSC is an analog television standard used in such countries as the United States and Japan. Each frame of an NTSC signal contains 525 scan lines at 60Hz.
- **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.
- **PAL:** Acronym for Phase Alternating Line. PAL is also another video standard used in broadcast television systems in large parts of the world. PAL signal contains 625 scan lines at 50Hz.
- **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.

FAQ

- **No image displayed on the monitor after starting up normally.**

Possible Reasons

- a) No VGA or 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 or VGA 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 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) No HDD is installed in the device.
- b) The installed HDD has not been initialized.
- c) The installed HDD is not compatible with the NVR or is broken-down.

Steps

1. Verify at least one HDD is installed in the NVR.
 - 4) If not, please install the compatible HDD.
Note: Please refer to the “Quick Operation Guide” for the HDD installation steps.
 - 5) If you don’t want to install a HDD, select “Menu>Configuration > Exceptions”, and uncheck the Audible Warning checkbox of “HDD Error”.
2. 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.
3. 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.
4. Check if the fault is solved by the step 1 to step 3.
 - 1) If it is solved, finish the process.
 - 2) If not, please contact the engineer to do the further process.

- **The status of the added IPC displays as “Disconnected” when it is connected through Private Protocol.**

Select “Menu>Camera>Camera>IP Camera” to get the camera status.

Possible Reasons

- a) Network failure, and the NVR and IPC lost connections.
- b) The configured parameters are incorrect when adding the IPC.
- 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).

Note: 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>IP 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 to do the further process.

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

Possible Reasons

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

Steps

1. Verify the IPC and the NVR versions are compatible.
 - 1) Enter the IPC Management interface “Menu > Camera > Camera>IP Camera”, and view the firmware version of connected IPC.
 - 2) Enter the System Info interface “Menu>Maintenance>System Info>Device Info”, and view the firmware version of NVR.
2. Verify power supply of IPC is stable.
 - 1) Verify the power indicator is normal.
 - 2) When the IPC is offline, please try the ping command on PC to check if the PC connects with the IPC.
3. Verify the network between IPC and NVR is stable.
 - 1) When the IPC 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 IPC, and check if there exists packet loss.

Note: 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 IPC 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 to do the further process.

- **No monitor connected with the NVR locally and when you manage the IPC 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 VGA or HDMI interface and reboot the device, there is black screen with the mouse cursor. Connect the NVR with the monitor before startup via VGA or HDMI interface, and manage the IPC to connect with the device locally or remotely, the status of IPC displays as Connect. And then connect the device with the CVBS, and there is black screen either.**

Possible Reasons:

After connecting the IPC 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.

Notes:

- 1) The view settings can only be configured by the local operation of NVR.
 - 2) 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 to do the further process.

- **Live view stuck when video output locally.**

Possible Reasons:

- a) Poor network between NVR and IPC, and there exists packet loss during the transmission.
- b) The motion detection and alarm functions are enabled, and the parameters of Main Stream (Normal) and Main Stream (Event) are different. So the image looks stuck due to the image changes between different resolutions.
- c) The frame rate has not reached the real-time frame rate.

Steps:

1. Verify the network between NVR and IPC 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.

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

2. Check the parameters of Main Stream (Normal) and Main Stream (Event).

Select "Menu > Record > Parameters > Record", and set the resolution of Main Stream (Event) the same as the one of Main Stream (Normal).

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

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

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

If it is solved, finish the process.

If not, please contact the engineer 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 IPC, 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 IPC 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.

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

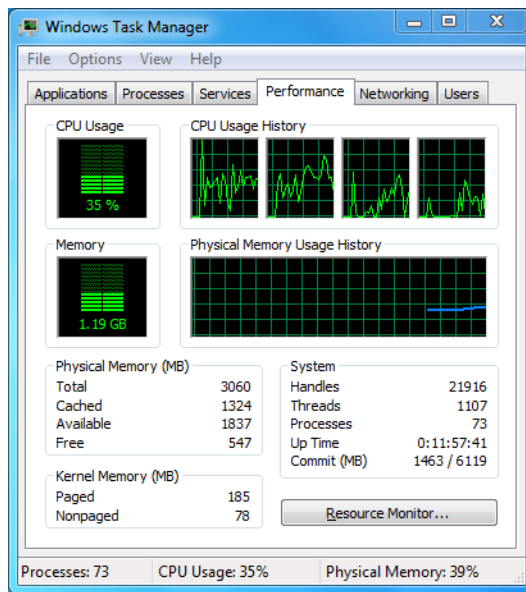
2. Verify the network between NVR and PC is connected.

- 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.

Note: 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 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 IPC 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 IPC is connected well; impedance matches and compatible.
Log in the IPC directly, and turn the audio on, check if the sound is normal. If not, please contact the manufacturer of the IPC.
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 IPC 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 IPC 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 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 IPC, and there exists packet loss during the transmission.
- b) The motion detection and alarm functions are enabled, and the parameters of Main Stream (Normal) and Main Stream (Event) are different. So the image looks stuck due to the image changes between different resolutions.
- c) The frame rate is not the real-time frame rate.
- d) 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 IPC 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.

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

2. Check the parameters of Main Stream (Normal) and Main Stream (Event).
Select "Menu > Record > Parameters > Record", and set the resolution of Main Stream (Event) the same as the one of Main Stream (Normal).
3. Verify the frame rate is real-time frame rate.
Select "Menu > Record > Parameters > Record", and set the Frame Rate to "Full Frame".
4. 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.
5. Reduce the number of local playback channel.
Select "Menu > Playback", and uncheck the checkbox of unnecessary channels.
6. Check if the fault is solved by the above steps.
If it is solved, finish the process.
If not, please contact the engineer 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 to do the further process.

List of Compatible IP Cameras

Note: 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.

IPC Manufacturer or Protocol	Model	Version	Max. Resolution	Audio	Sub stream
Arecont	AV1305M	65175	1280×1024	√	×
	AV2155	65143	1600×1200	√	×
	AV2815	65220	1920×1080	√	×
	AV3105M	65175	1920×1080	√	×
	AV5105	65175	1920×1080	√	×
Axis	M1114	5.09.1	1024×640	√	×
	M3011(ONVIF compatibility)	5.21	704×576	√	×
	M3014(ONVIF compatibility)	5.21.1	1280×800	√	×
	P3301(ONVIF compatibility)	5.11.2	768×576	√	√
	P3304(ONVIF compatibility)	5.20	1440×900	√	√
	P3343(ONVIF compatibility)	5.20.1	800×600	√	√
	P3344(ONVIF compatibility)	5.20.1	1440×900	√	√
	P5532	5.15	720×576	√	×
	Q7404	5.02	720×576	√	√
Hikvision	DS-2CD883F-E	V4.0.1 build 120508	2560×1920	√	√
	DS-2CD886BF-E	V2.0 build 110715	2560×1920	√	√
	DS-2CD886MF-E	V2.0 build 110715	2560×1920	√	√
	DS-2CD854F-E	V4.0.1 build 120508	2048×1536	√	√
	DS-2CD754F-E(I)	V4.0.1 build 120508	2048×1536	√	√
	DS-2CD8254F-E	V4.0.1 build 120508	2048×1536	√	√
	DS-2CD754FWD-E	V4.0.1 build 120508	1920×1080	√	√
	DS-2CD753F-E(I)	V4.0.1 build 120508	1600×1200	√	√
DS-2CD853F-E	V4.0.1 build 120508	1600×1200	√	√	

DS-2CD8153F-E	V4.0.1 build 120508	1600×1200	√	√
DS-2CD8253F-E	V4.0.1 build 120508	1600×1200	√	√
DS-2CD7153-E	V4.0.1 build 120508	1600×1200	√	×
DS-2CD876BF-E	V2.0 build 110715	1600×1200	√	√
DS-2CD876MF-E	V2.0 build 110715	1600×1200	√	√
DS-2CD877BF	V2.0 build 110715	1920×1080	√	√
DS-2CD752MF-E	V2.0 build 110614	1600×1200	√	√
DS-2CD852MF-E DS-2CD852F-E	V2.0 build 110426			
DS-2CD862MF-E	V2.0 build 110614	1280×960	√	√
	V2.0 build 110426			
DS-2CD8464F-EI	V4.0.1 build 120508	1280×960	√	√
DS-2CD863PF/NF-E	V4.0.1 build 120508	1280×960	√	√
DS-2CD864FWD-E	V4.0.1 build 120508	1280×720	√	√
DS-2CD763PF/NF-E	V4.0.1 build 120508	1280×960	√	√
DS-2CD763NF-EI	V4.0.1 build 120508	1280×960	√	√
DS-2CD7133-E	V4.0.1 build 120508	640×480	√	×
DS-2CD733F-E(I)	V4.0.1 build 120508	640×480	√	√
DS-2CD833F-E	V4.0.1 build 120508	640×480	√	√
DS-2CD8133F-E	V4.0.1 build 120508	640×480	√	√
DS-2CD802NF DS-2CD812PF DS-2CD832F DS-2CD892PF/NF	V2.0 build 090522	704×576	√	√
DS-2CD893PF(WD)-E	V4.0.1 build 120508	704×576	√	√
DS-2CD793PF(WD)-E(I)	V4.0.1 build 120508	704×576	√	√
DS-2CD793NF(WD)-E(I)	V4.0.1 build 120508	704×576	√	√
DS-2CD8313PF-E40	V3.0 build 110812	352×288	√	√
DS-2CD966(B) DS-2CD966-V(B)	V3.1.0 build120423	1360×1024	×	×
DS-2CD976(B) DS-2CD976-V(B)	V3.1.0 build120423	1600×1200	×	×
DS-2CD976(C)	V3.1.0 build120423	1600×1200	×	×
DS-2CD976-V(C)	V3.1.0 build120423	1600×1200	×	×
DS-2CD977(B) DS-2CD977(C)	V3.1.3 build120710	1920×1080	×	×
DS-2CD986A(B)	V3.1.0 build120423	2448×2048	×	×
DS-2CD986A(C)	V3.1.0 build120423	2448×2048	×	×
DS-2CD986C(B)	V2.1 build 110521	2560×1920	×	×

	DS-2DF1-572	V4.0.2 build 120813	1280×720	√	√
	DS-2DF1-772	V4.0.2 build 120813	1280×720	√	√
	DS-2DF1-618H	V3.1.0 build 110811	704×576	√	√
	DS-2DF1-718	V3.1.0 build 110811	704×576	√	√
	DS-2DF1-518	V3.1.0 build 110811	704×576	√	√
	DS-6601HFHI	V1.0.1 build 120409	1920×1080	√	√
	DS-6601HFHI/L	V1.0.1 build 120409	1920×1080	√	√
	DS-6501HCI-SATA DS-6504HCI-SATA DS-6516HCI-SATA	V1.0.1 build 110104	704×576	×	√
	DS-6508HFI-SATA	V1.0.1 build 110104	704×576	×	√
	DS-6601HCI DS-6602HCI DS-6604HCI	V1.2.0 build 120215	704×576	×	√
	DS-6601HFI DS-6602HFI DS-6604HFI	V1.2.0 build 120215	704×576	×	√
Panasonic	WV-SF336H	Application:1.06 Image data:1.06	1280×960	√	√
	WV-SP306H	Application:1.34 Image data:1.06	1280×960	√	√
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)	SNB-3000P	V1.41_110709	704×576	×	√
	SNB-5000P	V2.00_110727	1280×1024	×	√
	SNB-7000P	V1.10_110819	2048×1536	×	√
	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 (Only ONVIF is supported)	SNC-DH220T	1.50.00	2048×1536	×	×
ZAVIO	D5110	MG.1.6.03P1	1280×1024	√	×
	F3106	MG.1.6.03P1	1280×1024	√	√
	F3206	M2.1.6.01C2	1920×1080	√	√
	F531E	LM.1.6.18	640×480	√	√