Digital Video Recorder

User Manual

User Manual

About this Manual

This Manual is applicable to HD-TVI Digital Video Recorder (DVR).

The Manual includes instructions for using and managing the product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version in the company website

Please use this user manual under the guidance of professionals.

Legal Disclaimer

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

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

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

Regulatory Information

FCC Information

FCC compliance: This equipment has been tested and found to comply with the limits for a Class 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 EMC Directive 2004/108/EC, the RoHS Directive 2011/65/EU.

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

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

Industry Canada ICES-003 Compliance

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

Safety Instruction

These instructions are intended to ensure that user can use the product correctly to avoid danger or property loss.

The precaution measure is divided into “Warnings” and “Cautions”

Warnings: Serious injury or death may occur if any of the warnings are neglected.

Cautions: Injury or equipment damage may occur if any of the cautions are neglected.

Warnings Follow these safeguards to prevent serious injury or death.	**Cautions** Follow these precautions to prevent potential injury or material damage.

Warnings

- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.
- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region. Please refer to technical specifications for detailed information.
- Input voltage should meet both the SELV (Safety Extra Low Voltage) and the Limited Power Source with 100 to 240 VAC or 12 VDC according to the IEC60950-1 standard. Please refer to technical specifications for detailed information.
- Do not connect several devices to one power adapter as adapter overload may cause over-heating or a fire hazard.
- Please make sure that the plug is firmly connected to the power socket.
- If smoke, odor or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.

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.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
NOTE	Provides additional information to emphasize or supplement important points of the main text.

Product Key Features

General

- Connectable to HD-TVI and analog cameras;
- Support UTC Function;
- Connectable to AHD cameras;
- Connectable to IP cameras;
- Each channel supports dual-stream. And sub-stream supports up to WD1 resolution;
- Support up to 5MP resolution;
- Independent configuration for each channel, including resolution, frame rate, bit rate, image quality, etc.
- Encoding for both video stream and video & audio stream; audio and video synchronization during composite stream encoding;
- Support enabling H.264+ to ensure high video quality with lowered bitrate;
- Watermark technology.

Local Monitoring

- 1/4/6/8/9/16-screen live view is supported, and the display sequence of screens is adjustable;
- Live view screen can be switched in group and manual switch and automatic cycle live view are also provided, the interval of automatic cycle can be adjusted;
- Quick setting menu is provided for live view;
- The selected live view channel can be shielded;
- Motion detection, video-tampering detection, video exception alarm, video loss alarm and VCA alarm functions;
- Privacy mask;
- Several PTZ protocols supported; PTZ preset, patrol and pattern;
- Zooming in/out by clicking the mouse and PTZ tracing by dragging mouse.

HDD Management

- 1 SATA or 2 SATA hard disk can be connected;
- Each disk with a maximum of 6TB storage capacity;
- 8 network disks (8 NAS disks, 8 IP SAN disks or n NAS disks + m IP SAN disks ($n+m \leq 8$)) can be connected.
- Support cloud storage.
- S.M.A.R.T. and bad sector detection;
- HDD sleeping function;
- HDD property: redundancy, read-only, read/write (R/W);
- HDD group management;
- HDD quota management; different capacity can be assigned to different channels.

Recording and Playback

- Holiday recording schedule configuration;
- Cycle and non-cycle recording modes;
- Normal and event video encoding parameters;
- Multiple recording types: manual, continuous, alarm, motion, motion | alarm, motion & alarm and Event;
- Support POS;
- 8 recording time periods with separated recording types;
- Support Channel-Zero encoding;
- Main stream and sub-stream configurable for simultaneous recording;

- Pre-record and post-record for motion detection triggered recording, and pre-record time for schedule and manual recording;
- Searching record files by events (alarm input/motion detection);
- Customization of tags, searching and playing back by tags;
- Locking and unlocking of record files;
- Local redundant recording;
- Searching and playing back record files by camera number, recording type, start time, end time, etc.;
- Smart playback to go through less effective information;
- Main stream and sub-stream selectable for local/remote playback;
- Zooming in for any area when playback;
- Multi-channel reverse playback;
- Supports pause, fast forward, slow forward, skip forward, and skip backward when playback, locating by dragging the mouse on the progress bar;
- 4/8/16-ch synchronous playback;

Backup

- Export data by a USB, and 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, video tampering, abnormal signal, video input/recording resolution mismatch, illegal login, network disconnected, IP confliction, record exception, HDD error, and HDD full, etc.;
- Alarm triggers full screen monitoring, audio alarm, notifying surveillance center, sending email and alarm output;
- VCA detection alarm (line crossing detection and intrusion detection) is supported;
- Support POS triggered alarm;
- Support coaxial alarm;
- Automatic restore when system is abnormal.

Other Local Functions

- Manual and automatic video quality diagnostics;
- Operable by mouse and remote control;
- Three-level user management; admin user can create many operating account and define their operating permission, which includes the permission to access any channel;
- Completeness of operation, alarm, exceptions and log writing and searching;
- Manually triggering and clearing alarms;
- Importing and exporting of configuration file of devices;
- Getting cameras type information automatically.

Network Functions

- 1 self-adaptive 10M/100M/1000M network interface or 1 self-adaptive 10M/100Mbps network interface;
- IPv6 is supported;
- TCP/IP protocol, PPPoE, DHCP, DNS, DDNS, NTP, SADP, SMTP, NFS, iSCSI, UPnP™ and HTTPS are supported;
- Extranet access by HiDDNS;
- Support access by PT Cloud;
- TCP, UDP and RTP for unicast;
- Auto/Manual port mapping by UPnP™;

- Remote search, playback, download, locking and unlocking the record files, and 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 HDD formatting and program upgrading;
- Remote system restart and shutdown;
- Support upgrading via remote FTP server;
- 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;
- Remote JPEG capture;
- 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 6
Chapter 1 Introduction 12
1.1 Front Panel 13
1.2 IR Remote Control Operations 15
1.3 USB Mouse Operation 17
1.4 Input Method Description 18
1.5 Rear Panel 19
Chapter 2 Getting Started 20
2.1 Starting Up and Shutting Down the DVR 21
2.2 Activating the Device 22
2.3 Basic Configuration in Startup Wizard 22
2.3.1 Configuring the Signal Input Channel 22
2.3.2 Using the Wizard for Basic Configuration 23
2.4 Login and Logout 26
2.4.3 User Login 26
2.4.4 User Logout 26
2.5 Adding and Connecting the IP Cameras 27
2.5.1 Activating the IP Camera 27
2.5.2 Adding the Online IP Cameras 27
2.5.3 Editing the Connected IP Cameras 29
2.6 Configuring the Signal Input Channel 30
Chapter 3 Live View 31
3.1 Introduction of Live View 32
3.2 Operations in Live View Mode 33
3.2.1 Using the Mouse in Live View 33
3.2.2 Main/Aux Output Switching 34
3.2.3 Quick Setting Toolbar in Live View Mode 34
3.3 Channel-Zero Encoding 36
3.4 Adjusting Live View Settings 37
3.5 Manual Video Quality Diagnostics 38
Chapter 4 PTZ Controls 39
4.1 Configuring PTZ Settings 40
4.2 Setting PTZ Presets, Patrols and Patterns 41
4.2.1 Customizing Presets 41
4.2.2 Calling Presets 41
4.2.3 Customizing Patrols 42
4.2.4 Calling Patrols 43
4.2.5 Customizing Patterns 43
4.2.6 Calling Patterns 44
4.2.7 Customizing Linear Scan Limit 44
4.2.8 Calling Linear Scan 45
4.2.9 One-touch Park 45
4.3 PTZ Control Panel 47
Chapter 5 Recording Settings 48
5.1 Configuring Encoding Parameters 49
5.2 Configuring Recording Schedule 52
5.3 Configuring Motion Detection Recording 54
5.4 Configuring Alarm Triggered Recording 55
5.5 Configuring Event Recording 56
5.6 Configuring Manual Recording 57
5.8 Configuring Holiday Recording 58
5.9 Configuring Redundant Recording 60
5.10 Configuring HDD Group 62
5.11 Files Protection 63
5.12 Configuring 1080P Efficient 65
Chapter 6 Playback 66
6.1 Playing Back Record Files 67
6.1.1 Instant Playback 67
6.1.2 Playing Back by Normal Search 67
6.1.3 Playing Back by Event Search 68
6.1.4 Playing Back by Tag 69
6.1.5 Playing Back by Smart Search 70

6.1.6 Playing Back by System Logs 72
6.1.7 Playing Back by Sub-periods 74
6.1.8 Playing Back External File 75
6.2 Auxiliary Functions of Playback 75
6.2.1 Playing Back Frame by Frame 75
6.2.2 Digital Zoom 75
6.2.3 Reverse Playback of Multi-channel 76
Chapter 7 Backup 77
7.1 Backing up Record Files 78
7.1.1 Backing up by Normal Video Search 78
7.1.2 Backing up by Event Search 79
7.1.3 Backing up Video Clips 80
7.2 Managing Backup Devices 80
Chapter 8 Alarm Settings 81
8.1 Setting Motion Detection 82
8.2 Setting Sensor Alarms 84
8.3 Detecting Video Loss 87
8.4 Detecting Video Tampering 89
8.5 Setting All-day Video Quality Diagnostics 91
8.6 Handling Exceptions 92
8.7 Setting Alarm Response Actions 93
Chapter 9 POS Configuration 95
9.1 Configuring POS Settings 96
9.2 Configuring Overlay Channel 99
9.3 Configuring POS Alarm 100
Chapter 10 VCA Alarm 101
10.1 Face Detection 102
10.2 Vehicle Detection 102
10.3 Line Crossing Detection 103
10.4 Intrusion Detection 104
10.5 Region Entrance Detection 105
10.6 Region Exiting Detection 105
10.7 Loitering Detection 105
10.8 People Gathering Detection 106
10.9 Fast Moving Detection 106
10.10 Parking Detection 106
10.11 Unattended Baggage Detection 106
10.12 Object Removal Detection 107
10.13 Audio Exception Detection 107
10.14 Defocus Detection 108
10.15 PIR Alarm 108
Chapter 11 VCA Search 109
11.1 Face Search 110
11.2 Behavior Search 111
11.3 Plate Search 112
11.4 People Counting 112
11.5 Heat Map 114
Chapter 12 Network Settings 115
12.1 Configuring General Settings 116
12.2 Configuring Advanced Settings 117
12.2.1 Configuring PPPoE Settings 117
12.2.2 Configuring PT Cloud 117
12.2.3 Configuring DDNS 118
12.2.4 Configuring NTP Server 120
12.2.5 Configuring NAT 120
12.2.6 Configuring More Settings 122
12.2.7 Configuring HTTPS Port 122
12.2.8 Configuring Email 123
12.3 Checking Network Traffic 124
12.4 Configuring Network Detection 126
12.4.1 Testing Network Delay and Packet Loss 126
12.4.2 Exporting Network Packet 126
12.4.3 Checking Network Status 127
12.4.4 Checking Network Statistics 127
Chapter 13 HDD Management 129
13.1 Initializing HDDs 130
13.2 Managing Network HDD 131

13.3 Managing HDD Group 133
13.3.1 Setting HDD Groups 133
13.3.2 Setting HDD Property 134
13.4 Configuring Quota Mode 135
13.5 Configuring Cloud Storage 136
13.6 Checking HDD Status 137
13.7 Checking S.M.A.R.T Information 138
13.8 Detecting Bad Sector 139
13.9 Configuring HDD Error Alarms 140
Chapter 14 Camera Settings 141
14.1 Configuring OSD Settings 142
14.2 Configuring Privacy Mask 143
14.3 Configuring Video Parameters 144
Chapter 15 DVR Management and Maintenance 145
15.1 Viewing System Information 146
15.2 Searching Log Files 146
15.3 Importing/Exporting IP Camera Info 148
15.4 Importing/Exporting Configuration Files 149
15.5 Upgrading System 150
15.5.1 Upgrading by Local Backup Device 150
15.5.2 Upgrading by FTP 150
15.6 Restoring Default Settings 151
Chapter 16 Others 152
16.1 Configuring General Settings 153
16.2 Configuring DST Settings 154
16.3 Configuring More Settings 155
16.4 Managing User Accounts 156
16.4.1 Adding a User 156
16.4.2 Deleting a User 158
16.4.3 Editing a User 158
Chapter 17 Appendix 160
17.1 Glossary 161
17.2 Troubleshooting 162

Chapter 1 Introduction

1.1 Front Panel

Front Panel:

Figure 1. 1 Front Panel

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 Interfaces		Universal Serial Bus (USB) ports for additional devices such as USB mouse and USB Hard Disk Drive (HDD).
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;

No.	Name		Function Description
			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**		Switch between the numeric or letter input and functions of the composite keys. (Input letter or numbers when the light is out; Realize functions when the light is red.)
5	**Control Buttons**		Directional buttons: In menu mode, the direction buttons are used to navigate between different fields and items and select setting parameters. 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. In the image setting interface, the up and down button can adjust the level bar of the image parameters. In live view mode, these buttons can be used to switch channels.
			Enter: The Enter button is used to confirm selection in menu mode; or used to check checkbox fields and ON/OFF switch. In playback mode, it can be used to play or pause the video. In single-frame play mode, pressing the Enter button will play the video by a single frame. And in auto sequence view mode, the buttons can be used to pause or resume auto sequence.
6	**IR Receiver**		Receiver for IR remote.

1.2 IR Remote Control Operations

The DVR may also be controlled with the included IR remote control, shown in Figure 1. 2.

NOTE

Batteries (2×AAA) must be installed before operation.

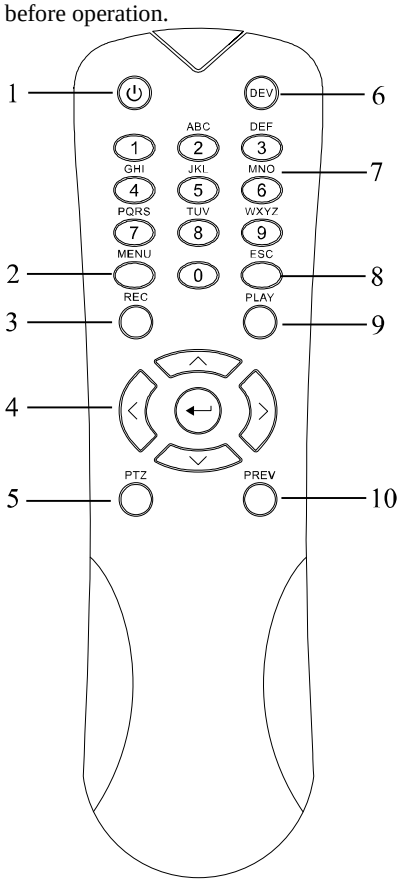


Figure 1. 2 Remote Control

The keys on the remote control closely resemble the ones found on the front panel. Refer to Table 1. 2, they include:

Table 1. 2 Description of the IR Remote Control Buttons

No.	Name	Description
1	POWER	Power on/off the device.
		Power on/off the device by pressing and holding the button for 5 seconds.
2	MENU Button	Press the button to 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 button will start wiper (if applicable).
		In Playback mode, it is used to show/hide the control interface.
3	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.
4	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

No.	Name	Description
		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 *tick* checkbox fields.
		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.
5	**PTZ Button**	In Auto-switch mode, it can be used to stop /start auto switch.
6	**DEV**	Enables/Disables Remote Control.
7	**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 the Playback mode.
8	**ESC Button**	Back to the previous menu.
		Press for Arming/disarming the device in Live View mode.
9	**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.
10	**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.

Troubleshooting Remote Control:

NOTE

Make sure you have install 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 into Menu > Configuration > General > More Settings by operating the front control panel or the mouse.
2. Check and remember the DVR No.. The default DVR No. is 255. This number valid for all IR remote controls.
3. Press the DEV button on the remote control.
4. Enter the DVR No. 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 cannot function properly, please change the 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 DVR. To use a USB mouse:

Steps:

1. Plug USB mouse into one of the USB interfaces on the front panel of the DVR.
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.
	Drag	PTZ control: Wheeling. 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

Description of the buttons on the soft keyboard:

Table 1. 4 Description of the Soft Keyboard Icons

Icon	Description	Icon	Description
0 … 9	Number	A … Z	English letter
	Lowercase/Uppercase		Backspace
123/., ABC	Switch the keyboard		Space
	Positioning the cursor		Exit
#+=	Symbols		Reserved

1.5 Rear Panel

NOTE

The rear panel vaires according to different models. Please refer to the actual product. The following figure is for reference only.

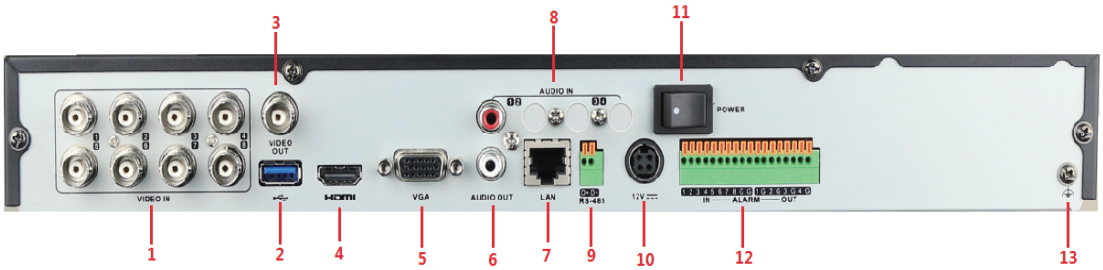


Figure 1. 4 Rear Panel

Table 1.5 Description of Rear Panel

No.	Item	Description
1	VIDEO IN	BNC interface for TVI and analog video input.
2	USB Port	Universal Serial Bus (USB) port for additional devices.
3	VIDEO	BNC connector for video output.
4	HDMI	HDMI video output connector.
5	VGA	DB15 connector for VGA output. Display local video output and
6	AUDIO	RCA connector.
7	Network Interface	Connector for network
8	AUDIO IN	RCA connector
9	RS-485	Connector for RS-485 devices. T+ and T- pins connect to R+ and R- pins of PTZ receiver respectively.
		D+, D- pin connects to Ta, Tb pin of controller. For cascading devices, the first NVR's D+, D- pin should be connected with the D+, D- pin of the next DVR.
10	Power Supply	12V DC power supply.
11	Power Switch	Switch for turning on/off the device.
12	Alarm	Connector for alarm input/output.
13	GND	Ground

Chapter 2 Getting Started

2.1 Starting Up and Shutting Down the DVR

Purpose:
Proper startup and shutdown procedures are crucial to expanding the life of the DVR.
Before you start:
Check that the voltage of the extra power supply is the same with the DVR's requirement, and the ground connection is working properly.
Starting up the DVR
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, and the Power indicator LED should turn on indicating that the unit begins to start up.
3. After startup, the Power indicator LED remains on.

Shutting down the DVR
Steps:
There are two proper ways to shut down the DVR. To shut down the DVR:

- **OPTION 1: Standard shutdown**
  1. Enter the Shutdown menu.
     Menu > Shutdown

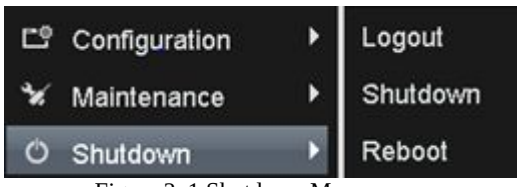


Figure 2. 1 Shutdown Menu

2. Select the **Shutdown** button.
3. Click the **Yes** button.
4. Turn off the power switch on the rear panel when the note appears.

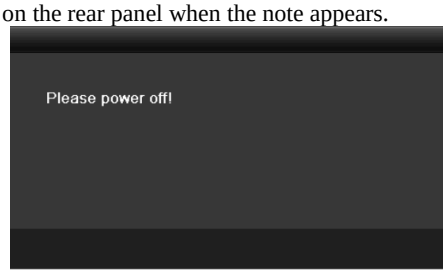


Figure 2. 2 Shutdown Tips

Rebooting the DVR
While in the Shutdown menu (Figure 2. 1), you can also reboot the DVR.
Steps:
1. Enter the **Shutdown** menu by clicking Menu > Shutdown.
2. Click the **Logout** button to log out or the **Reboot** button to reboot the DVR.

2.2 Activating the Device

Purpose:
For the first-time access, you need to activate the device by setting an admin password. No operation is allowed before activation. You can also activate the device via Web Browser, SADP or Client Software.
Steps:
1. Input the same password in the text field of **Create New Password** and **Confirm New Password**.

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 at least three of the following categories: 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.

NOTE

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.

2.3 Basic Configuration in Startup Wizard

2.3.1 Configuring the Signal Input Channel

After the startup and login, the device system enters the Wizard for configuring the signal input.

NOTE

You can also click **Menu** > **Camera** > **Signal Input Status** to configure the signal input.
Steps:
1. Check the checkbox to select different signal input types: TVI, AHD/CVBS or IP.
2. Click **Apply** to save the settings.

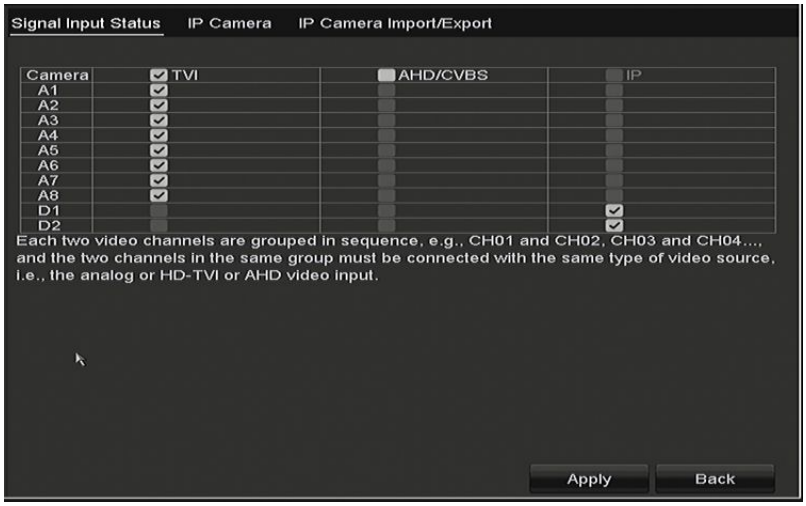


Figure 2. 4 Configure Signal Input Type

NOTE

- Each two video channels are grouped in sequence, e.g., CH01 and CH02, CH03 and CH04…, and the two channels in the same group must be connected with the same type of video source, i.e., the analog or HD-TVI or AHD video input.
- In the live view interface, when there is no video signal of the analog channel, the corresponding connectable video signal type message can be displayed on the screen.

2.3.2 Using the Wizard for Basic Configuration

By default, the **Setup Wizard** starts once the device has loaded.
Operating the Setup Wizard:

1. The **Start Wizard** can walk you through some important settings of the device. If you don't want to use the **Start Wizard** at that moment, click **Exit**. You can also choose to use the **Start Wizard** next time by leaving the "Start wizard when device starts?" checkbox checked.
2. Click **Next** to enter the **Password Configuration** interface. Enter the admin password. If you want to change the password, check the checkbox of **New Admin Password**, enter the new password and confirm it.

   NOTE

   For the admin, you have 7 times to enter the password.
3. After the password configuration, click **Next** button to enter the **Date and Time Settings** window.

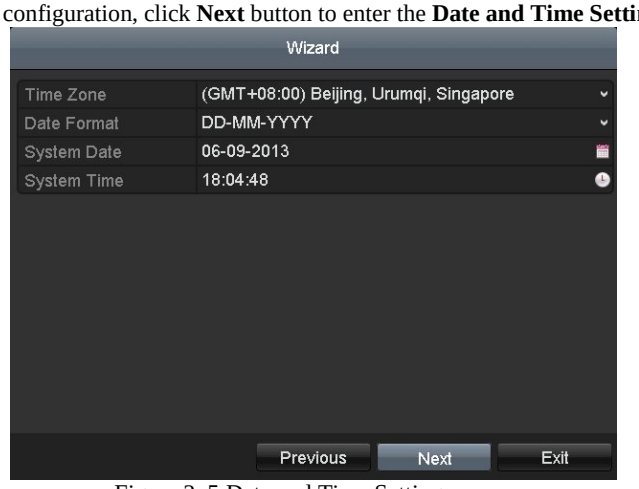


Figure 2. 5 Date and Time Settings

4. After the time settings, click **Next** button to enter the **General Network Setup Wizard** window, as shown in Figure 2.11.

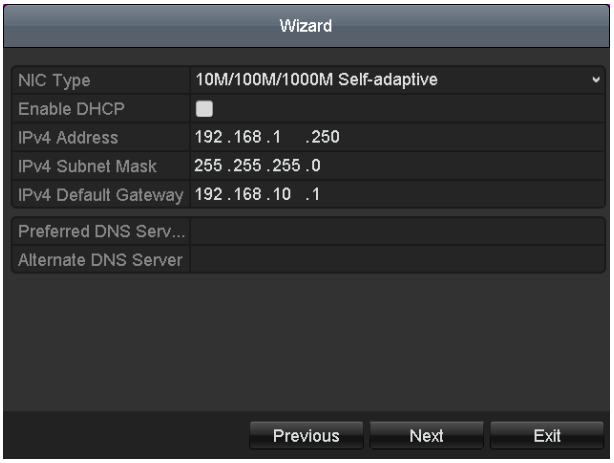


Figure 2. 6 General Network Configuration

5. Click **Next** button after you configured the basic network parameters. Then you will enter the **PT Cloud** interface. Configure the PT Cloud according to your need.
6. Click **Next** button to enter the **Advanced Network Parameter** interface. You can enable PPPoE, enable DDNS and set other ports according to your need.

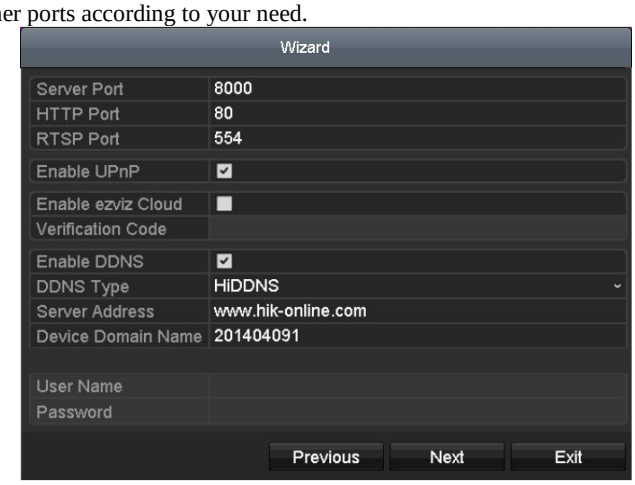


Figure 2. 7 Advanced Network Parameters

7. Click **Next** button after configuring the advanced network parameters, which will take you to the **HDD Management** window, shown in Figure 2.14.

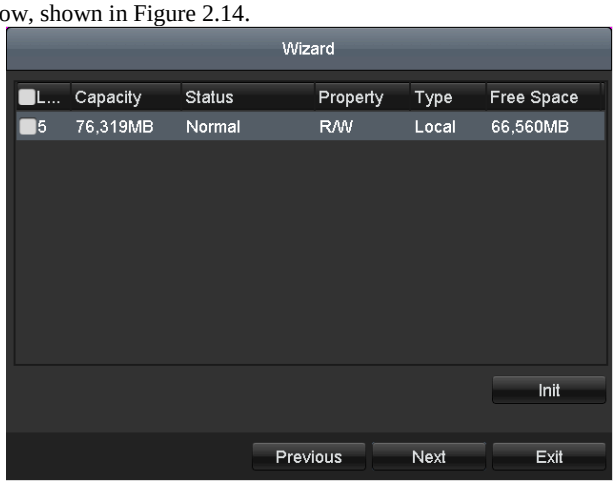


Figure 2. 8 HDD Management

8. To initialize the HDD, click the **Init** button. Initialization will remove all the data saved in the HDD.
9. Click **Next** to enter the **IP Camera Management** window.
10. Add the IP camera.
    1) Click **Search** to search the online IP Camera. 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.

2) Click the **Add** to add the camera.

11. After finishing IP Camera settings, click **Next** to enter the **Record Settings** window.

12. Click the icon , and you can enable the continuous recording or motion detection recording for all channels of the device.

13. Click **OK** to complete the wizard settings.

2.4 Login and Logout

2.4.3 User Login

Purpose:
You have to log in to the device before operating the menu and other functions
Steps:

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

Figure 2. 9 Login Interface

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

NOTE

In the Login interface, for the admin, if you have entered the wrong password for 7 times, the account will be locked for 60 seconds. For the operator, if you have entered the wrong password for 5 times, the account will be locked for 60 seconds.

2.4.4 User Logout

Purpose:
After logging out, the monitor turns to the live view mode and if you want to perform some operations, you need to enter the user name and password to log in again.
Steps:

1. Enter the **Shutdown** menu.
   Menu > Shutdown

Figure 2. 10 Logout

2. Click **Logout**.

NOTE

After you have logged out of 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> IP 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.

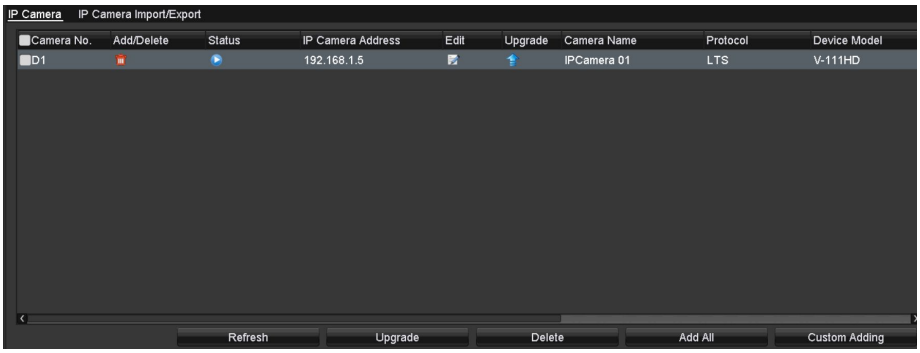


Figure 2. 11 IP Camera Management Interface

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.
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 DVR.
   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 at least three of the following categories: 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 acitavting of the IP camera. And the security status of camera will be changed to **Active**.

2.5.2 Adding the Online IP Cameras

Purpose:
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 11*.

- **OPTION 1:**

Steps:

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

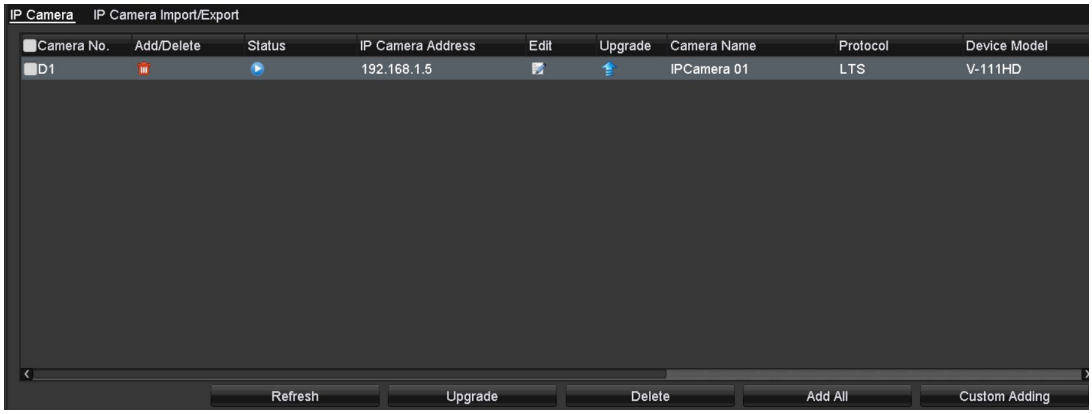


Figure 2. 12 Adding IP Camera Interface

2. The online cameras with same network segment will be detected and displayed in the camera list.
3. Select the IP camera from the list and click the button to add the camera (with the same admin password of the DVR's). Or you can click the **One-touch Adding** button to add all cameras (with the same admin password) from the list.

   NOTE

   Make sure the camera to add has already been actiavted by setting the admin password, and the admin password of the camera is the same with the DVR's.
4. (For the encoders with multiple channels only) check the checkbox of Channel Port in the pop-up window, as shown in the following figure, and click **OK** to add multiple channels.

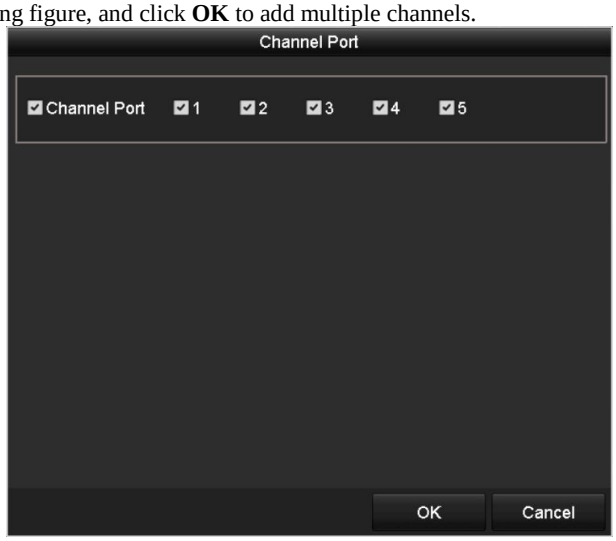


Figure 2. 13 Selecting Multiple Channels

- **OPTION 2:**

Steps:

1. On the IP Camera Management interface, click the **Custom Adding** button to pop up the **Add IP Camera (Custom)** interface.

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

   NOTE

   If the IP camera to add has not been actiavated, you can activate it from the IP camera list on the **IP Camera Management** interface.
3. Click **Add** to add the camera.

   For the successfully added IP cameras, the **Security** status shows the security level of the password of camera: strong password, weak password and risky password.

2.5.3 Editing the Connected IP Cameras

After the adding of the IP cameras, the basic information of the camera is listed on the page, you can configure the basic settings of the IP cameras.

Steps:

1. Click the icon to edit the parameters; You can edit the IP address, protocol and other parameters.
   Channel Port: If the connected device is an encoding device with multiple channels, you can choose the channel to connect by selecting the channel port No. in the dropdown list.
2. Click **OK** to save the settings and exit the editing interface.
3. Drag the horizontal scroll bar to the right side and click the icon to edit the advanced parameters.

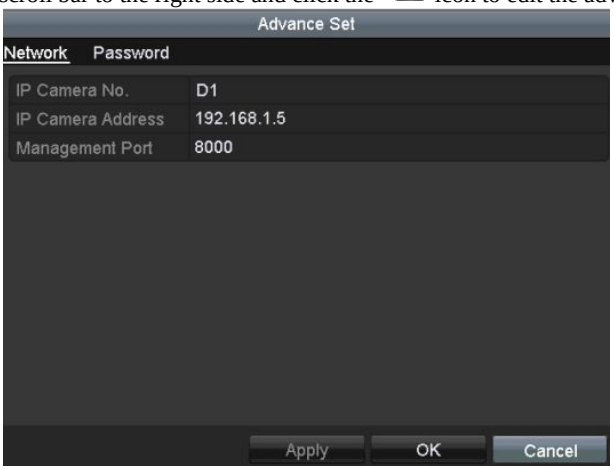


Figure 2. 14 Network Configuration of the Camera

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

Figure 2. 15 Password Configuration of the Camera

5. Click **OK** to save the settings and exit the interface.

2.6 Configuring the Signal Input Channel

Steps:

1. Enter the **Signal Input Status** interface.
Menu > Camera > Signal Input Status

2. Check the checkbox to select different signal input types: TVI, AHD/CVBS or IP. the 3MP and 5MP IP video input types are selectable.

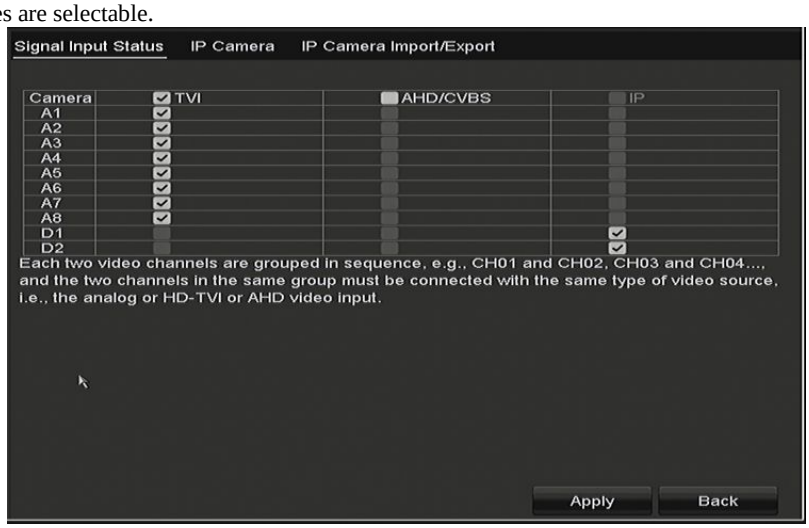


Figure 2. 16 Configure Signal Input Type

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

NOTE

- Each two video channels are grouped in sequence, e.g., CH01 and CH02, CH03 and CH04…, and the two channels in the same group must be connected with the same type of video source, i.e., the analog or HD-TVI or AHD video input.
- In the live view interface, when there is no video signal of the analog channel, the corresponding connectable video signal type message can be displayed on the screen.

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 DVR will automatically enter Live View mode when powered on. It is also at the very top of the menu hierarchy, thus hitting the ESC many times (depending on which menu you're on) will bring you to the Live View mode.

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
	Event/Exception (motion detection, sensor alarm or exception information. For details, see *Chapter 8.6 Handling Exceptions.*)

3.2 Operations in Live View Mode

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

- **Single Screen:** show only one screen on the monitor.
- **Multi-screen:** show multiple screens on the monitor simultaneously.
- **Auto-switch:** the screen is auto switched to the next one. And you must set the dwell time for each screen on the configuration menu before enabling the auto-switch. Menu>Configuration>Live View>Dwell Time.
- **Start Recording:** normal record and motion detection record are supported.
- **Quick Set:** select the output mode to Standard, Bright, Gentle or Vivid.
- **Playback:** play back the recorded videos for current day.
- **Aux/Main output switch:** the DVR checks the connection of the output interfaces to define the main and auxiliary output interfaces. When the aux output is enabled, the main output cannot do any operation, and you can do some basic operation on the live view mode for the Aux output.

The priority level for the main and aux output is HDMI/VGA>CVBS. See the table below.

Table 3. 2 Priorities of Interfaces

S.N	VGA/HDMI	CVBS	Main output	Auxiliary output
1	√	√	VGA/HDMI	CVBS
2	√	×	VGA/HDMI	
3	×	√	CVBS	

NOTE

√ means the interface is in use, × means the interface is out of use or the connection is invalid. And the HDMI, VGA and CVBS can be used at the same time.

3.2.1 Using the Mouse in Live View

You can refer to Table 3.3 for the description of mouse operation in live view mode.

Table 3. 3 Mouse Operation in Live View

Name	Description
Menu	Enter the main menu of the system by right clicking the mouse.
Single Screen	Switch to the single full screen by choosing channel number from the dropdown list.
Multi-screen	Adjust the screen layout by choosing from the dropdown list.
Previous Screen	Switch to the previous screen.
Next Screen	Switch to the next screen.
Start/Stop Auto-Switch	Enable/disable the auto-switch of the screens. NOTE The *dwell time* of the live view configuration must be set before using **Start Auto-Switch**.
Start Recording	Start recording of all channels, Continuous Record and Motion Detection Record are selectable from the dropdown list.
Add IP Camera	A shortcut to enter the IP camera management interface.(For HDVR series only)
Output Mode	Output Mode is configurable with Standard, Bright, Gentle and Vivid options.
Playback	Enter the playback interface and start playing back the video of the selected channel immediately.
PTZ Control	A shortcut to enter the PTZ control interface of the selected camera.
Aux Monitor	Switch to the auxiliary output mode and the operation for the main output is disabled. NOTE If you enter Aux monitor mode and the Aux monitor is not connected, the mouse operation is disabled. You need to switch back to the Main output with the F1 button on front panel or **VOIP/MON** button on IR remote control and then press the Enter button.

Figure 3. 1 Right-click Menu

3.2.2 Main/Aux Output Switching

NOTE

- When the HDMI/VGA output is configured as the main output, you can perform the following operation to switch to CVBS output as the main output.

Steps:

1. Use the mouse wheel to double-click on the HDMI/VGA output screen, and the following message box pops up:

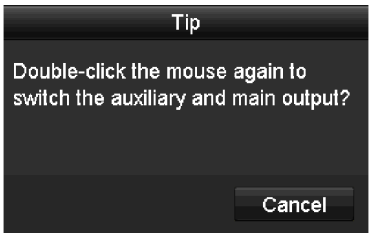


Figure 3. 2 Switch Main and Aux Output

2. Use the mouse wheel to double-click on the screen again to switch to the Aux output, or click **Cancel** to cancel the operation.
3. Select the **Menu Output Mode** to **Main CVBS** from the right-click menu on the monitor.
4. On the pop-up message box, click **Yes** to restart the device to enable the CVBS output as the main output.

NOTE

You can select the **Menu Output Mode** under Menu>Configuration>General>More Settings to **Auto**, or **HDMI/VGA** and then restart the device to switch the main output back to HDMI/VGA output.

3.2.3 Quick Setting Toolbar in Live View Mode

On the screen of each channel, there is a quick setting toolbar which shows when you click the screen.

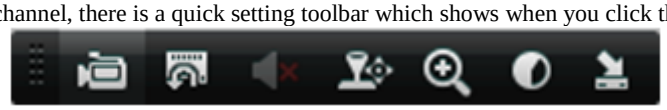


Figure 3. 3 Quick Setting Toolbar

You can refer to Table 3.4 for the description of Quick Setting Toolbar icons.

Table 3. 4 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
	Close Live View				

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. Click and draw to select the area to zoom in, as shown in Figure 3. 4.

Figure 3. 4 Digital Zoom

Image Settings icon can be selected to enter the Image Settings menu. You can drag the mouse or click to adjust the image parameters, including brightness, contrast, and saturation. Refer to the *Chapter 14.3 Configuring Video Parameters* for details.

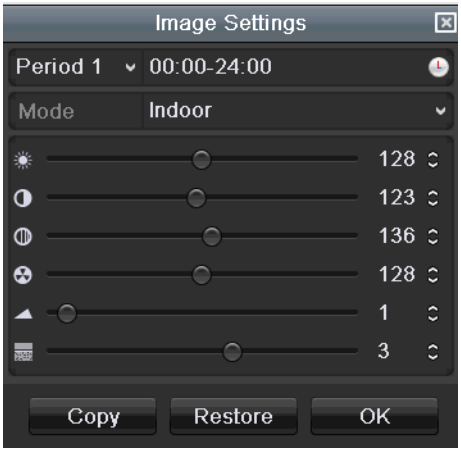


Figure 3. 5 Image Settings

Face Detection can be enabled if you click the icon. The dialog pops up. Click **Yes** and the full-screen live view of the channel is enabled. You can click to exit from the full-screen mode.

NOTE You can configure face detection only when it is supported by the connected camera.

Move the mouse onto the Information icon to show the real-time stream information, including the frame rate, bit rate, resolution and stream type.

3.3 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.

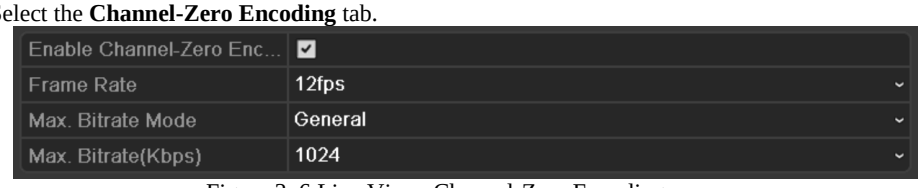


Figure 3. 6 Live View- Channel-Zero Encoding

3. Check the checkbox after **Enable Channel-Zero Encoding.**
4. Configure the Frame Rate, Max. Bitrate Mode and Max. Bitrate.
5. Click the **Apply** button to activate the settings.

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.

3.4 Adjusting Live View Settings

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

1. Enter the Live View Settings interface.
Menu> Configuration> Live View

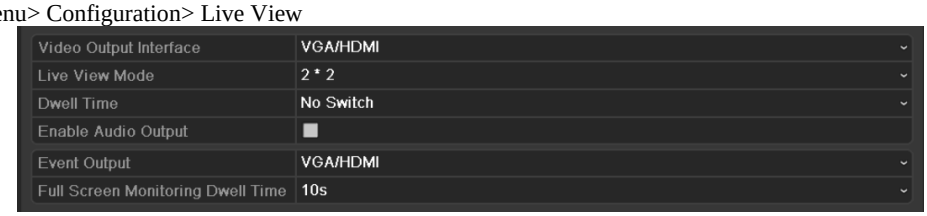


Figure 3. 7 Live View-General

The settings available in this menu include:

- **Video Output Interface:** Selects the output to configure the settings.
- **Live View Mode:** Selects 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 camera in the live view mode.
- **Volume:** Adjust the volume of the audio output.
- **Event Output:** Designates the output to show event video; If available, you can select a different video output interface from the Video Output Interface when an event occurs.
- **Full Screen Monitoring Dwell Time:** The time in seconds to show alarm event screen.

2. Set the camera order.

1) Select **View** tab.

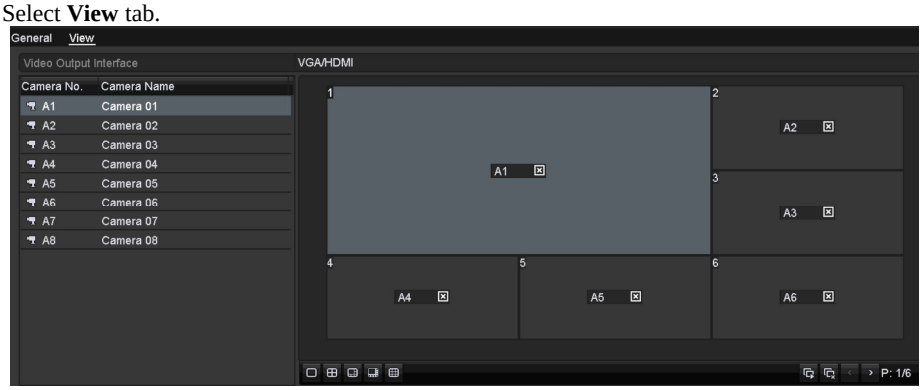


Figure 3. 8 Live View- Camera Order

2) Click a window to select it, and then double-click a camera name in the camera list you would like to display. Setting an 'X' means the window will not display any camera.
3) You can also click to start live view of all channels in order and click to stop live view of all channels. Click or to go to the previous or next page.
4) Click the **Apply** button.

3.5 Manual Video Quality Diagnostics

Purpose:
The video quality of the analog channels can be diagnosed manually and you can view the diagnostic results from a list.
Steps:

1. Enter the Manual **Video Quality Diagnostics** interface.
   Menu> Manual >Manual Video Quality Diagnostics

Figure 3. 9 Video Quality Diagnostics

2. Check the checkboxes to select the channels for diagnostics.
3. Click the button **Diagnose**, and the results will be displayed on a list. You can view the video status and diagnostics time of the selected channels.

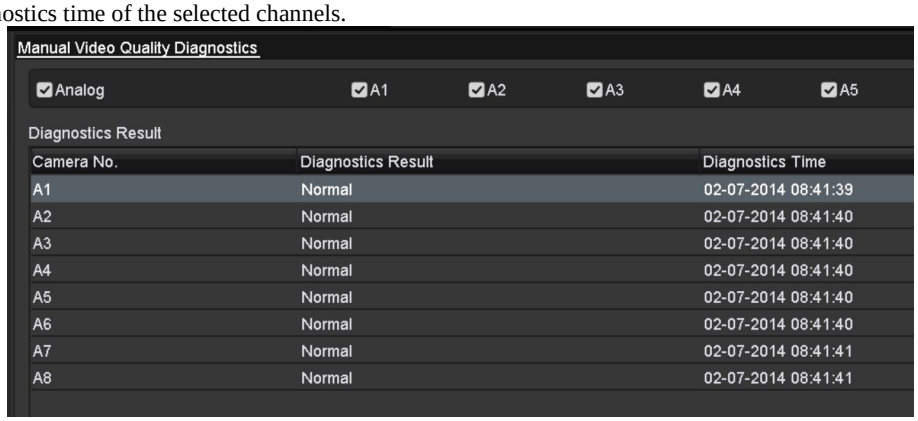


Figure 3. 10 Diagnostics Result

NOTE

- Connect the camera to the device for the video quality diagnostics.
- Three exception types can be diagnosed: Blurred Image, Abnormal Brightness and Color Cast.

Chapter 4 PTZ Controls

4.1 Configuring PTZ Settings

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

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

Figure 4. 1 PTZ Settings

2. Choose the camera for PTZ setting in the **Camera** dropdown list.
3. Click the **PTZ Parameters** button to set the PTZ parameters.

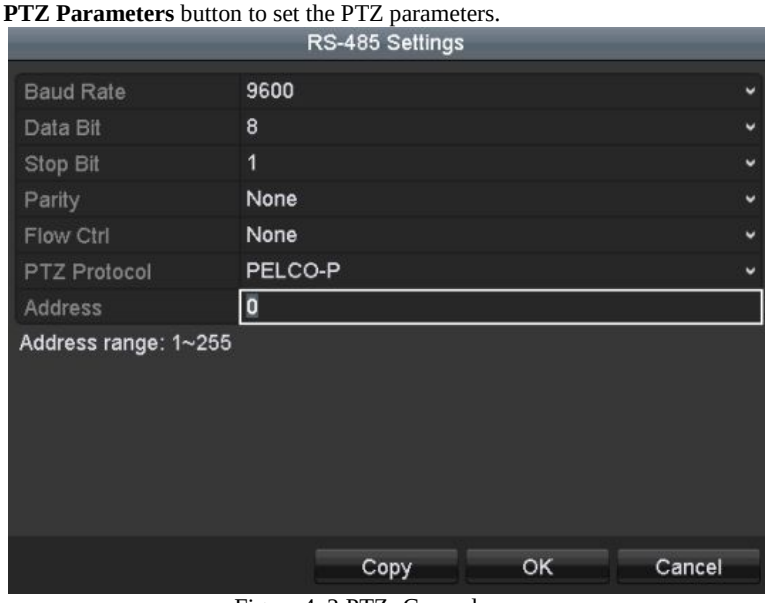


Figure 4. 2 PTZ- General

4. Select the parameters of the PTZ camera from the dropdown list.

NOTE

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

NOTE

When the Coaxitron protocol is selected, all the other parameters like the baud rate, data bit, stop bit, parity and flow control are not configurable.

5. (Optional) Click **Copy** button to copy the settings to the other channels. Select the channels you want to copy to and click **OK** to return to the **PTZ Parameters Settings** interface.
6. Click **OK** to save the settings.

4.2 Setting PTZ Presets, Patrols and 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

Figure 4. 3 PTZ Settings

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

4.2.2 Calling Presets

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

1. Click the button **PTZ** in the lower-right corner of the PTZ setting interface;
   Or press the PTZ button on the front panel or click the PTZ Control icon in the quick setting bar, or select the PTZ option in the right-click menu to show the PTZ control panel.
2. Choose C**amera** in the dropdown list.
3. Click the **General** tab to show the general settings of the PTZ control.

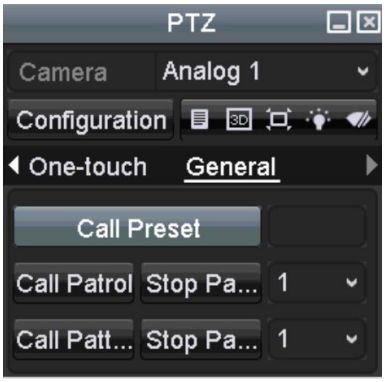


Figure 4. 4 PTZ Panel - General

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

Figure 4. 5 PTZ Settings

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

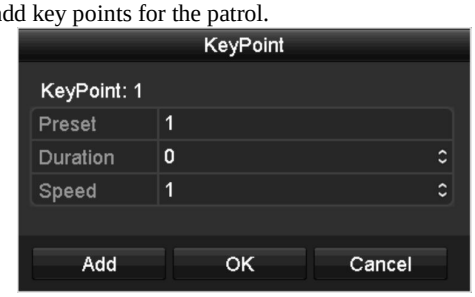


Figure 4. 6 Key point Configuration

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.

5. Click the **Add** button to add the next key point to the patrol, or you can click the **OK** button to save the key point to the patrol.
   You can delete all the key points by clicking the **Clear** button for the selected patrol, or click the **Clear All** button to delete all the key pints for all patrols.

4.2.4 Calling Patrols

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

1. Click the button **PTZ** in the lower-right corner of the PTZ setting interface;
   Or press the PTZ button on the front panel or click the PTZ Control icon in the quick setting bar, or select the PTZ option in the right-click menu to show the PTZ control panel.
2. Click the **General** tab to show the general settings of the PTZ control.

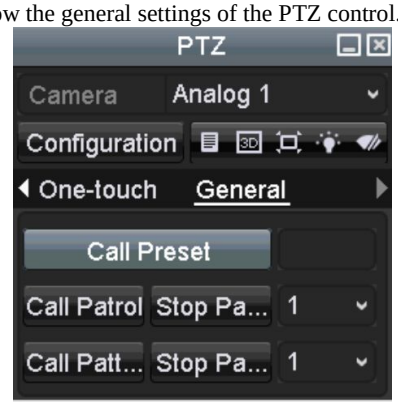


Figure 4. 7 PTZ Panel - General

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

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

Figure 4. 8 PTZ Settings

2. Choose pattern number in the dropdown list.
3. Click the **Start** button and click corresponding buttons in the control panel to move the PTZ camera, and click the **Stop** button to stop it.
   The movement of the PTZ is recorded as the pattern.

4.2.6 Calling Patterns

Purpose:
Follow the procedure to move the PTZ camera according to the predefined patterns.
Steps:
1. Click the button **PTZ** in the lower-right corner of the PTZ setting interface;
   Or press the PTZ button on the front panel or click the PTZ Control icon in the quick setting bar, or select the PTZ option in the right-click menu to show the PTZ control panel.
2. Click the **General** tab to show the general settings of the PTZ control.

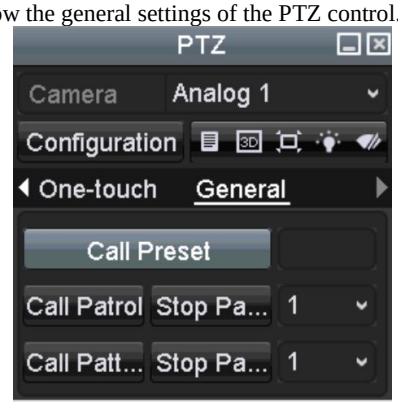


Figure 4. 9 PTZ Panel - General

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

4.2.7 Customizing Linear Scan Limit

Purpose:
The Linear Scan can be enabled to trigger the scan in the horizantal direction in the predefined range.

NOTE
This function is supported by some certain models.
Steps:
1. Enter the PTZ Control interface.
   Menu > Camera > PTZ

Figure 4. 10 PTZ Settings

2. Use the directional button to wheel the camera to the location where you want to set the limit, and click the **Left Limit** or **Right Limit** button to link the location to the corresponding limit.

NOTE

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

4.2.8 Calling Linear Scan

Purpose:

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

Steps:

1. Click the button **PTZ** in the lower-right corner of the PTZ setting interface;

   Or 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.

2. Click the **One-touch** tab to show the one-touch function of the PTZ control.

Figure 4. 11 PTZ Panel - One-touch

3. Click **Linear Scan** button to start the linear scan and click the **Linear Scan** button again to stop it.

   You can click the **Restore** button to clear the defined left limit and right limit data and the dome needs to reboot to make settings take effect.

4.2.9 One-touch Park

Purpose:

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

Steps:

1. Click the button **PTZ** in the lower-right corner of the PTZ setting interface;

   Or 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.
2. Click the **One-touch** tab to show the one-touch function of the PTZ control.

Figure 4. 12 PTZ Panel - One-touch

3. There are 3 one-touch park types selectable. Click the corresponding button to activate the park action.
   Park (Quick Patrol): The dome starts patrol from the predefined preset 1 to preset 32 in order after the park time. The undefined preset will be skipped.
   Park (Patrol 1): The dome starts moving according to the predefined patrol 1 path after the park time.
   Park (Preset 1): The dome moves to the predefined preset 1 location after the park time.

   NOTE

   The park time can only be set through the speed dome configuration interface. The default value is 5s.
4. Click the button again to inactivate it.

4.3 PTZ Control Panel

To enter the PTZ control panel, there are two ways supported.
OPTION 1:
In the **PTZ Settings** interface, click the **PTZ** button on the lower-right corner which is next to the **Back** button.
OPTION 2:
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 in the quick setting bar, or select the PTZ Control option in the right-click menu.
Click the **Configuration** button on the control panel, and you can enter the **PTZ Settings** interface.

NOTE

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

Figure 4. 13 PTZ Control Panel

You can refer to Table 4.1 for the description of the PTZ panel icons.

Table 4. 1 Description of the PTZ panel 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	3D-Zoom		Image Centralization		Menu
PTZ Control	Switch to the PTZ control interface	One-touch	Switch to the one-touch control interface	General	Switch to the general settings interface
	Exit		Minimize windows		

Chapter 5 Recording Settings

5.1 Configuring Encoding Parameters

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. Click **Advanced** tab to check the storage mode of the HDD. (Menu>HDD>Advanced)
   1) If the HDD mode is *Quota*, please set the maximum record capacity. For detailed information, see *Chapter 13.4 Configuring Quota Mode*.
   2) If the HDD mode is *Group*, you should set the HDD group. For detailed information, see *Chapter 5.10 Configuring HDD*.

Figure 5. 2 HDD- Advanced

Steps:

1. Enter the **Record Parameters** interface to configure the encoding parameters.
   Menu>Record>Parameters

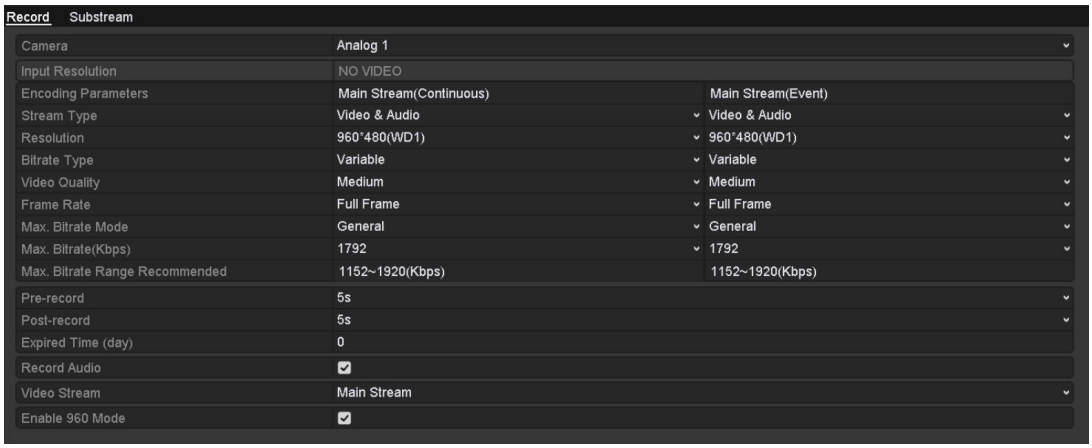


Figure 5. 3 Record Parameters

2. Set the parameters for recording.
   1) Select the **Record** tab to configure.
   2) Select a camera from the camera dropdown list.
   3) Configure the following parameters for the **Main Stream (Continuous)** and the **Main Stream (Event)**:
      Stream Type: Set the stream type to be Video or Video & Audio.
      Resolution: Set recording at resolution.
      Bitrate Type: Set the bitrate type to be Variable or Constant.
      Video Quality: Set the video quality of recording, with 6 levels configurable.

      NOTE The Stream Type, Resolution, Bitrate Type and Video Quality are not configurable for the Main Stream (Event) of the IP Camera.

      Frame Rate: Set the frame rate of recording.
      Max. Bitrate Mode: Set the mode to General or Custom (32-6144Kbps).
      Max Bitrate (Kbps): Select or customize the maximum bit rate for recording.
      Max. Bitrate Range Recommended: A recommended max. bit rate range is provided for reference.
      Max. Average Bitrate (Kbps): Set the max. average bit rate which refers to the average amount of data transferred per unit of time.
3. Check the checkbox of **Enable H.264+** to enable this function. Enabling it helps to ensure the high video

quality with a lowered bitrate.

NOTE

- After enabling the H.264+, the **Max. Bitrate Mode**, **Max. Bitrate(Kbps)** and **Max. Bitrate Range Recommend** are not configurable.
- The H.264+ can not be used with the SVC at the same time.
- For the connnected IP camera, the H.264+ should be supported by the camera and added to the DVR l.
- You should reboot the device to activate the new settings after enabling the H.264+.

4. Click **More Settings** to configure more parameters.

- **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 time for keeping the record files in the HDDs, once exceeded, the files will be deleted. The files will be saved permanently if the value is set as 0. The actual keeping time for the files should be determined by the capacity of the HDDs.
- **Redundant Record:** Enabling redundant record means you save the record in the redundant HDD. See *Chapter 5.8 Configuring Redundant Recording*.
- **Record Audio:** Enable this feature to record the sound and disable it to record the video without sound.
- **Video Stream:** Main stream and sub-stream are selectable for recording. When you select sub-stream, you can record for a longer time with the same storage space.
- **Enable 960 Mode:** The option is supported by analog cameras. Enabling the 960 mode to enable the WD1 resolution for the main stream, otherwise, the resolution supports up to 4CIF. And the option is not supported by TVI cameras, while the WD1 resolution is available all the time.

NOTE

- The **Redundant Record** option is only available when the HDD mode is *Group*.
- Redundant HDD is required for the redundant record function. For detailed information, see *Chapter 12.3.2 Setting HDD Property*.
- For network cameras, the parameters of Main Stream (Event) are not editable.

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

6. Optionally, you can click **Copy** to copy the settings to other analog channels if needed.

NOTE

You can copy the same settings to the cameras with the same signal, e.g., the channel No. 1-3 connect to the TVI cameras, and the channel No.4 connects to an analog camera, and then the settings of channel No. 1 can be only copied to channel 2 and 3.

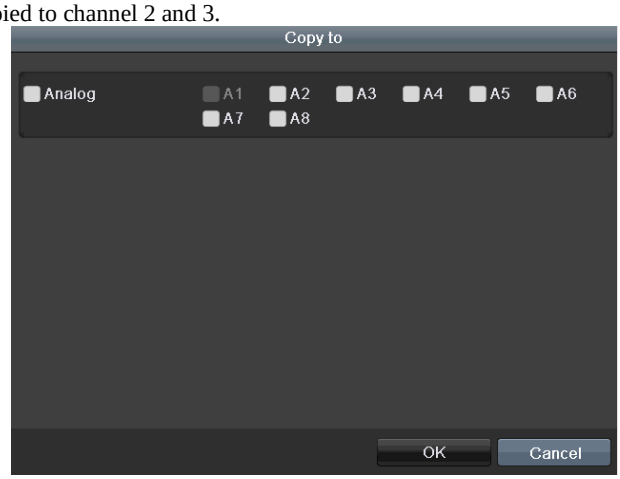


Figure 5. 4 Copy Camera Settings

7. Set encoding parameters for sub-stream.

1) Select the **Substream** tab.

Figure 5. 5 Sub-stream Encoding

2) Select a camera in the camera dropdown list.
3) Configure the parameters.
4) Click **Apply** to save the settings.
5) (Optional) If the parameters can also be used to other cameras, click **Copy** to copy the settings to other channels.

5.2 Configuring Recording Schedule

NOTE

- In this chapter, we take the record schedule procedure as an example, and the same procedure can be applied to configure schedule for both continuous recording.

Purpose:

Set the record schedule, and then the camera will automatically start/stop recording according to the configured schedule.

Steps:

1. Enter the **Record Schedule** interface.
   Menu> Record> Schedule

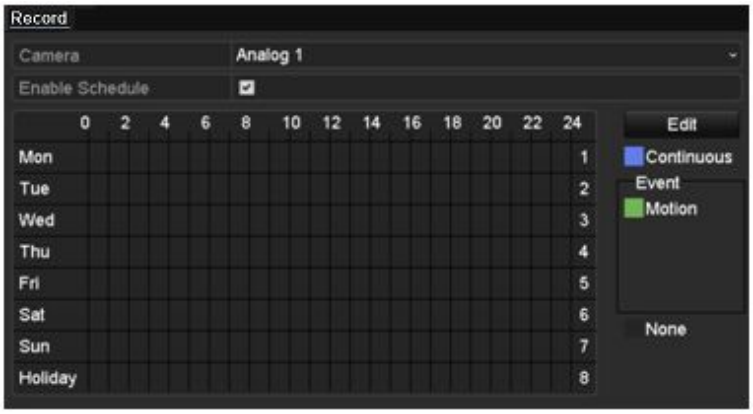


Figure 5. 6 Record Schedule

Different recording types are marked in different color icons.
Continous: scheduled recording.
Event: recording triggered by all event triggered alarm.
Motion: recording triggered by motion detection.
Alarm: recording triggered by alarm.
M/A: recording triggered by either motion detection or alarm.
M&A: recording triggered by motion detection and alarm.

2. Choose the camera you want to configure in the Camera dropdown list.
3. Check the checkbox of **Enable Schedule**.
4. Configure the record schedule.
   Edit the schedule
   1) Click **Edit**.
   2) In the message box, you can choose the day to which you want to set schedule.
   3) To schedule an all-day recording, check the checkbox after the **All Day** item.

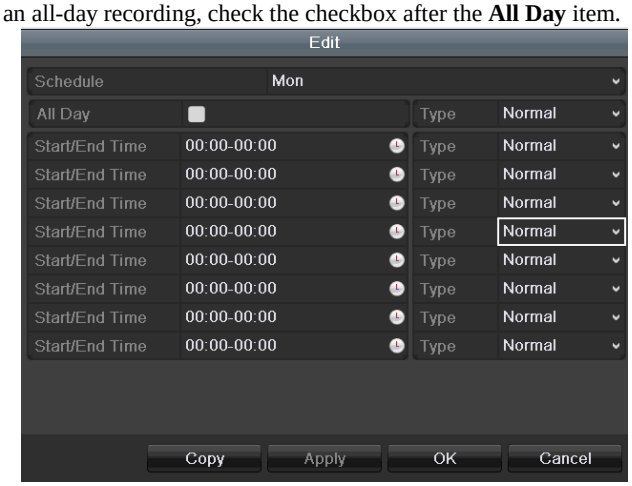


Figure 5. 7 Edit Schedule- All Day

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

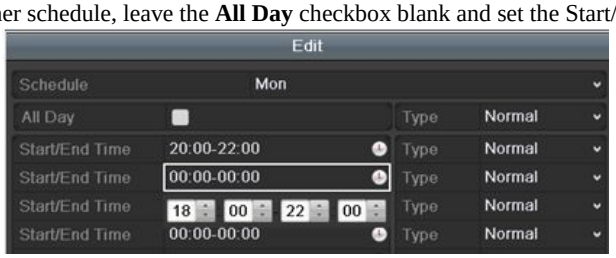


Figure 5. 8 Edit Schedule- Set Time Period

NOTE

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

NOTE

- To enable Event, Motion, Alarm, M | A (motion or alarm), M & A (motion and alarm) and POS triggered recording, you must configure the motion detection settings, alarm input settings or VCA settings as well. For detailed information, refer to *Chapter 8.1, Chapter 8.7 and Chapter 9.*
- The VCA settings are only available to the smart IP cameras.

Repeat the above steps 1)-4) to schedule recording for other days in the week. If the schedule can also be set to other days, click **Copy**.

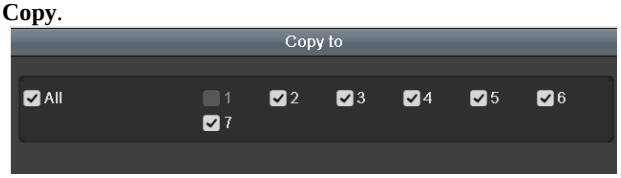


Figure 5. 9 Copy Schedule to Other Days

NOTE

The **Holiday** option is available when you enable holiday schedule in **Holiday settings**. See C*hapter 5.8 Configuring Holiday Record.*

5) Click **OK** to save setting and back to upper level menu.

Draw the schedule

1) Click on the color icon to select a record type in the event list on the right-side of the interface.

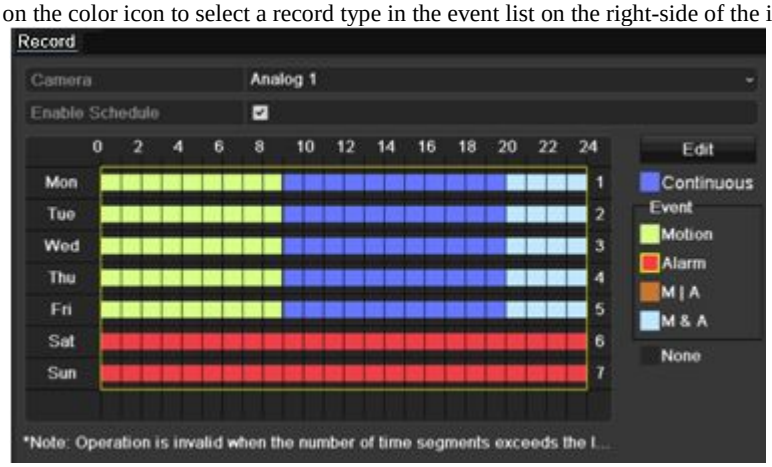


Figure 5. 10 Draw the Schedule

2) Click and drag the mouse on the schedule.

3) Click on the other area except for the schedule table to finish and exit from the drawing.

You can repeat step 4 to set schedule for other channels. If the settings can also be used to other channels, click **Copy**, and then choose the channel to which you want to copy to.

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

5.3 Configuring Motion Detection Recording

Purpose:
Follow the steps to set the motion detection parameters. In the live view mode, once a motion detection event takes place, the DVR 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, notifying the surveillance center, sending email and so on.
Steps:

1. Enter the **Motion Detection** interface.
Menu>Camera>Motion

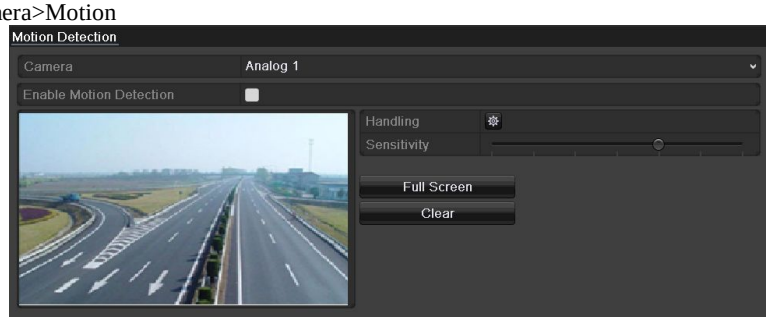


Figure 5. 11 Motion Detection

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**.

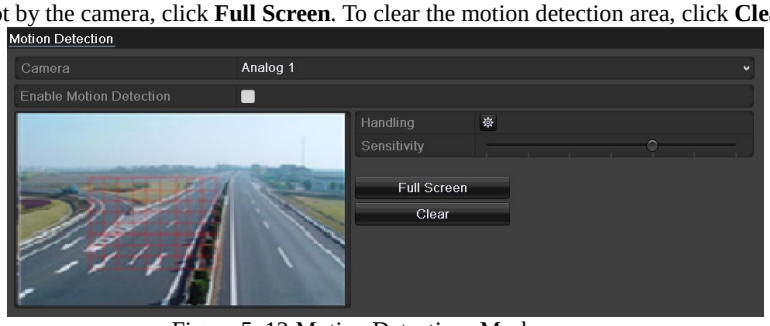


Figure 5. 12 Motion Detection- Mask

4) Click the , and the message box for channel information pops up.

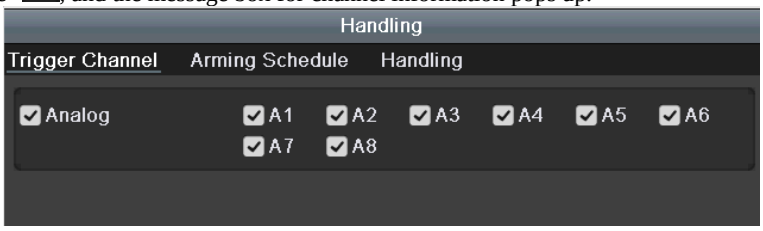


Figure 5. 13 Motion Detection Settings

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. Configure the schedule.
Please refer to the step 4 of *Chapter 5.2 Configuring Recording Schedule*, while you may choose Motion as the record type.

5.4 Configuring Alarm Triggered Recording

Purpose:
Follow the procedure to configure alarm triggered recording.
Steps:

1. Enter the **Alarm Setting** interface.
Menu> Configuration> Alarm

2. Click the **Alarm Input** tab.

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 of Setting.
4) Click the button.
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 steps from 1) to 8) to configure other alarm input parameters.
If the setting can also be applied to other alarm inputs, click **Copy** and choose the alarm input number.

3. Configure the schedule.
Please refer to the step 4 of *Chapter 5.2 Configuring Recording Schedule*, while you may choose Alarm as the record type.

5.5 Configuring 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. 14 VCA Settings

2. Configure the detection rules for VCA events. For details, see the step 6 in *Chapter 9.3 Line Crossing Detection*.

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.

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

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

5. Enter **Record Schedule Settings** interface (Menu> Record> Schedule>Record Schedule), and then set Event as the record type. For details, see step 2 in *Chapter 5.2 Configuring Record Schedule.*

5.6 Configuring Manual Recording

Purpose:
Follow the steps to set parameters for the manual record. Using manual record, you don't need to set a schedule for recording.
Steps:

1. Enter the **Manual Record** interface.
   Menu> Manual

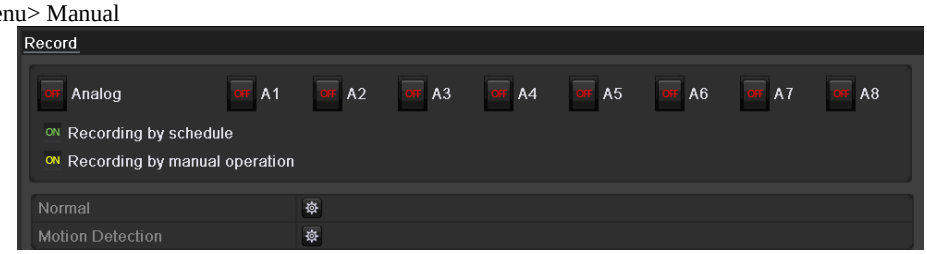


Figure 5. 15 Manual Record

2. Enable manual record.
   Click the status icon OFF before camera number to change it to ON.
   Or click the status icon OFF of **Analog** to enable manual record of all channels.
3. Disable manual record.
   Click the status icon ON to change it to OFF.
   Or click the status icon ON of **Analog** to disable manual record of all channels.

NOTE
After rebooting all the manual records enabled are canceled.

5.8 Configuring Holiday Recording

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

2. Choose **Holiday** on the left bar.

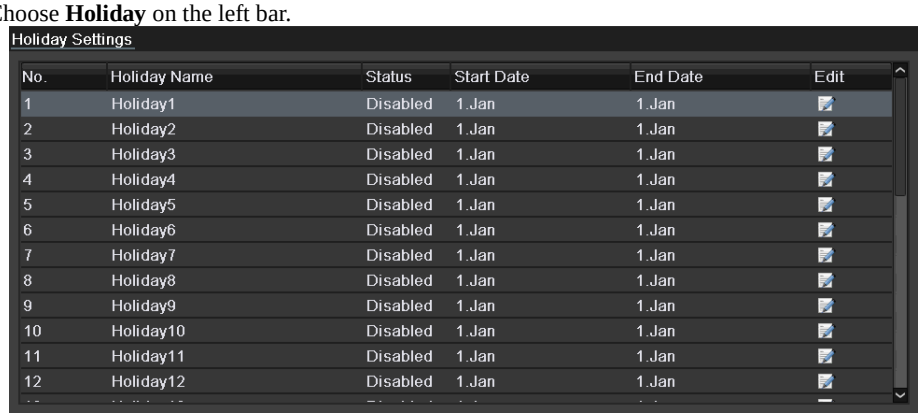


Figure 5. 16 Holiday Settings

3. Enable Edit Holiday schedule.

1) Click to enter the Edit interface.

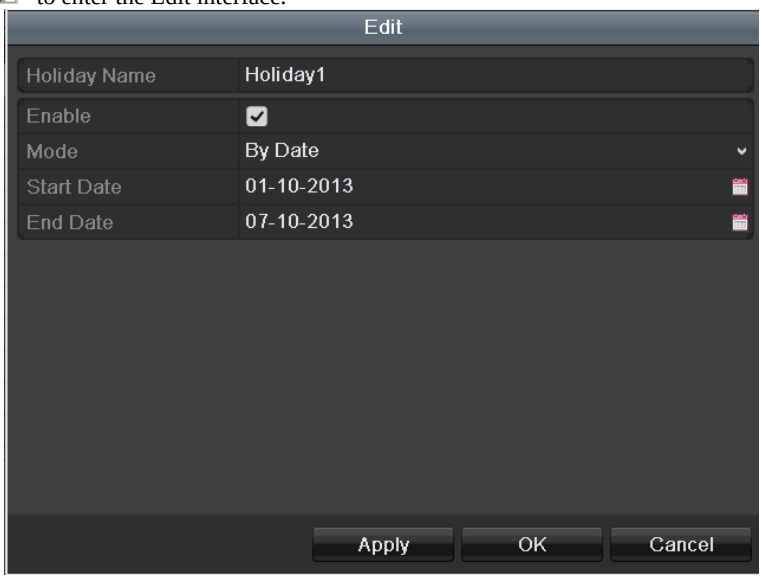


Figure 5. 17 Edit Holiday Settings

2) Check the checkbox of **Enable**.
3) Select Mode from the dropdown list.
There are three different modes for the date format to configure holiday schedule. By Month, By Week, and By Date are selectable.
4) Set the start and end date.
5) Click **Apply** to save settings.
6) Click **OK** to exit the Edit interface.

4. Configure the record schedule.
Please refer to the *Chapter 5.2 Configuring Record Schedule*, while you may choose Holiday in the Schedule dropdown list, or you can draw the schedule on the timeline of Holiday.

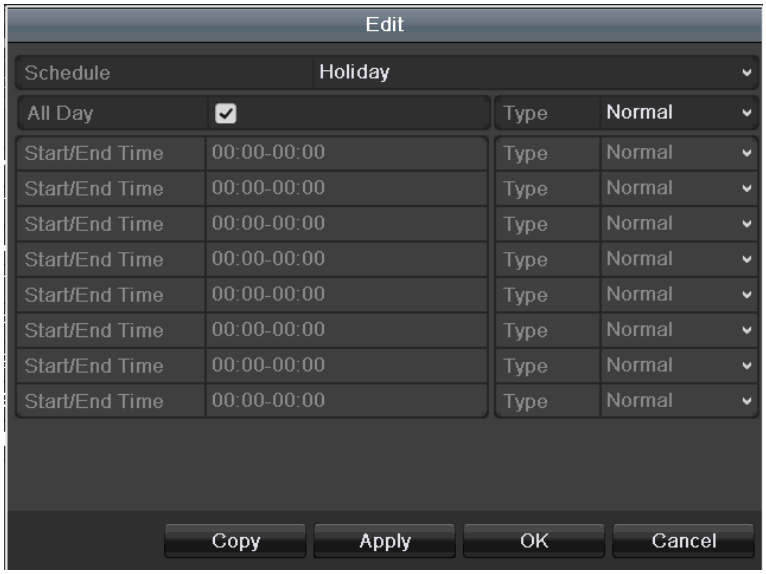


Figure 5. 18 Edit Schedule- Holiday

NOTE

- Up to 8 periods can be configured for each day. And the time periods cannot be overlapped each other.
- In the time table of the channel, both holiday schedule and normal day schedule are displayed.
- Repeat the above step 4 to set Holiday schedule for other channels. If the holiday schedule can also be used to other channels, click **Copy** and choose the channel you want to apply the settings.

5.9 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.
Before you start:
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 13.3 Managing HDD Group.* There should be at least another HDD which is in Read/Write status.
Steps:

1. Enter HDD Information interface.
Menu> HDD

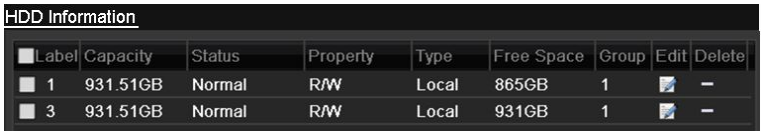


Figure 5. 19 HDD General

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

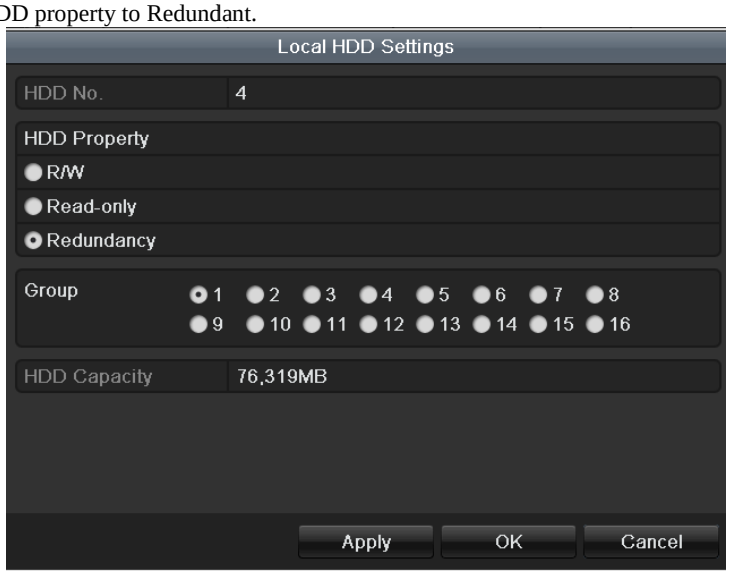


Figure 5. 20 HDD General-Editing

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

3. Enter the Record setting interface.
Menu> Record> Parameters
1) Select the **Record** tab.

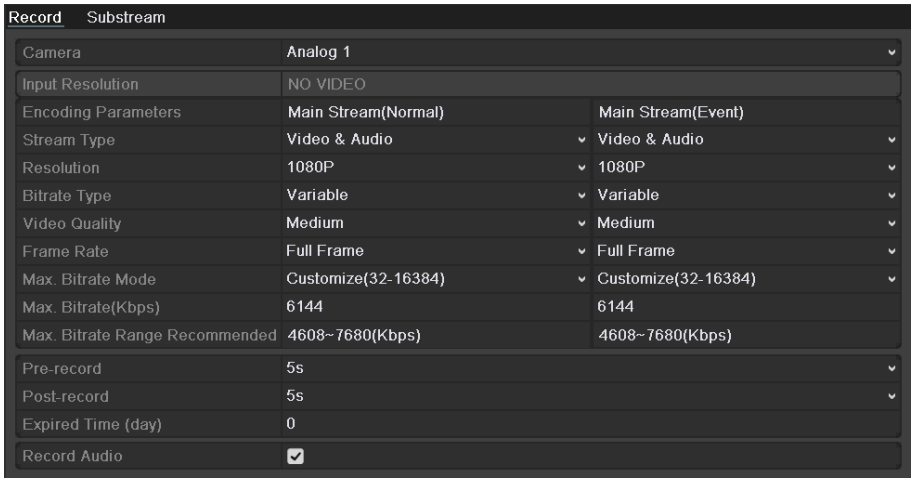


Figure 5. 21 Encoding Parameters

2) Select Camera you want to configure.
3) Check the checkbox of **Redundant Record**.
4) Click **Apply** to save settings.

If the encoding parameters can also be used to other channels, click **Copy** and choose the channel you want to apply the settings.

5.10 Configuring HDD Group

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

1. Enter HDD setting interface.
   Menu>HDD>Advanced
2. Select **Advanced** on the left bar.
   Check whether the storage mode of the HDD is Group. If not, set it to Group. For detailed information, please refer to *Chapter 13.3 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** 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.

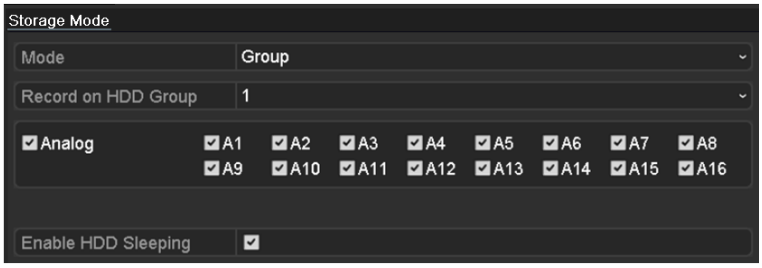


Figure 5. 22 HDD Advanced

   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 you have configured the HDD groups, you can configure the Recording settings following the procedure provided in *Chapter 5.2-5.7*.

5.11 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 **Export Settings** interface.
   Menu> Export

Figure 5. 23 Export

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

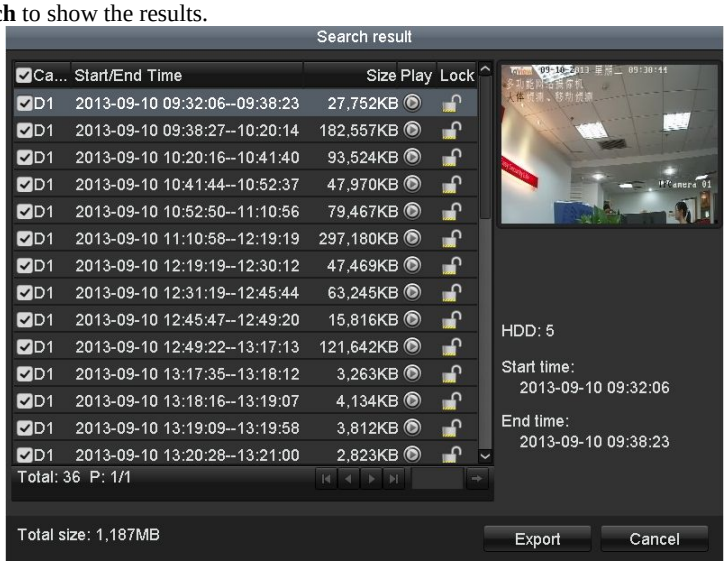


Figure 5. 24 Export-Search Result

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 cannot be locked.
   2) Click to change it to to unlock the file and the file is not protected.

Protect file by setting HDD property to Read-only

Before you start:
To edit HDD property, you need to set the storage mode of the HDD to Group. See *Chapter 13.3 Managing HDD Group*.

Steps:

1. Enter HDD setting interface.
   Menu> HDD

Figure 5. 25 HDD General

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

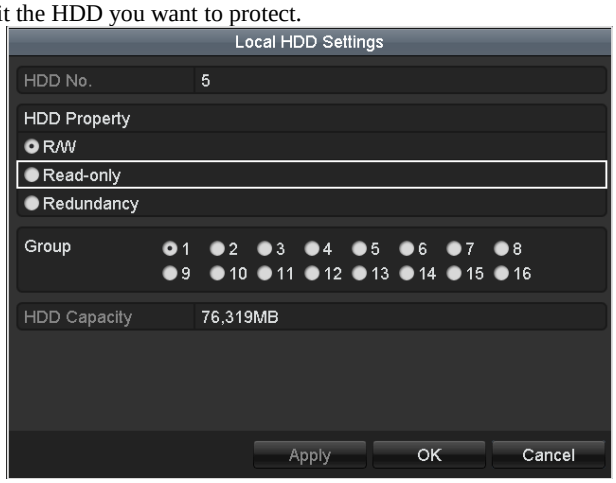


Figure 5. 26 HDD General- Editing

3. Set the HDD to Read-only.

4. Click **OK** to save settings and back to the upper level menu.

NOTE

- You cannot save any files in a Read-only HDD. If you want to save files in the HDD, change the property to R/W.
- If there is only one HDD and is set to Read-only, the DVR cannot record any files. Only live view mode is available.
- If you set the HDD to Read-only when the DVR 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.

5.12 Configuring 1080P Efficient

Purpose:

When the 1080P Efficient Mode is enabled, the encoding resolution at 1080P Efficient (real-time) is supported. If not, up to 1080P (non-real-time) is supported.

Task1: Enabling the 1080P Efficient Mode

Steps:

1. Enter the **Record** menu
   Menu > Record
2. Click **Advanced** to enter the advanced interface.

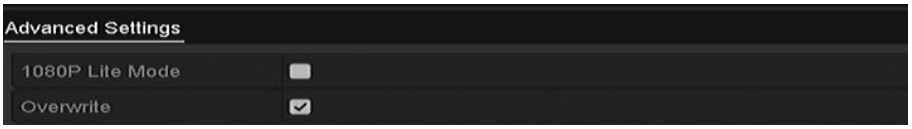


Figure 5. 27 Advanced Interface

3. Check the checkbox of **1080 Efficient Mode** and click **Apply** to pop up the attention box.
4. Click **Yes** to reboot the device to have new settings taken effect.

Task2: Disabling the 1080P Efficient Mode

Steps:

1. Enter the **Record** menu
   Menu > Record
2. Click **Advanced** to enter the advanced interface.
3. Uncheck the checkbox of **1080 Lite Mode** and click **Apply**. The following attention box pops up:

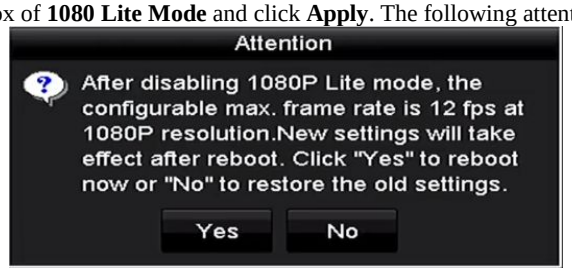


Figure 5. 28 Attention

4. Click **Yes** to reboot the device to activate the new settings or **No** to restore the old settings.

Chapter 6 Playback

6.1 Playing Back Record Files

6.1.1 Instant Playback

Purpose:

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

Instant playback by channel

Steps:

Choose a channel in live view mode 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

6.1.2 Playing Back by Normal Search

Playback by Channel

Enter the Playback interface.

Right click a channel in live view mode and select **Playback** from the menu, as shown in the following figure:

Figure 6. 2 Right-click Menu under Live View

Playback 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. 3 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 9. Otherwise it is displayed as 9.

Playback Interface

You can select the main stream or sub stream from the dropdown list for playback.
You can also use the toolbar in the bottom part of **Playback** interface to control playing progress, as shown in the following figure.
Select the channel(s) if you want to switch playback to another channel or execute simultaneous playback of multiple channels.

Figure 6. 4 Toolbar of Playback

Table 6. 1 Detailed Explanation of Playback Toolbar

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

NOTE

- The 01-01-2015 00:00:23 -- 14-07-2015 16:10:27 indicates the start time and end time of the record files.
- represents normal recording (manual or schedule); represents event recording (motion, alarm, motion | alarm, motion & alarm).
- Playback progress bar: use the mouse to click any point of 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 (motion detection, alarm input or VCA). Channel switch is supported.

Steps:

1. Enter the **Playback** interface.
   Menu>Playback
2. Click Normal and select Event to enter the **Event Playback** interface.
3. Select **Alarm Input**, **Motion**, **VCA** as the event type, and specify the start time and end time for search.
4. Click **Search**, and the record files matching the search conditions will be displayed on a list.
5. Select and click button to play back the record files.
   You can click **Back** button to return to the search interface.
   If there is only one channel triggered, clicking button takes you to **Full-screen Playback** interface of this channel.
   If several channels are triggered, clicking button takes you to the **Synchronous Playback** interface. Check checkbox to select one channel for playback or select multiple channels for synchronous playback.
   NOTE
   The maximum number of channels for synchronous playback supported varies to different models.
6. On the **Event Playback** interface, you can select the main stream or sub stream from the dropdown list for playback.
   The toolbar in the bottom part of **Playback** interface can be used to control playing process.
   Pre-play and post-play can be configured for the playback of event 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.
7. You can click or button to select the previous or next event. Please refer to Table 6.1 for the description of buttons on the toolbar.

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 6.1.2 Play Back by Channel* for the detailed information about searching and playback of the record files.
   Click button to add default tag.
   Click button to add customized tag and input tag name.

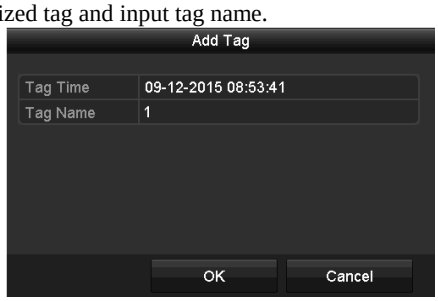


Figure 6. 5 Add Tag

NOTE

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

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

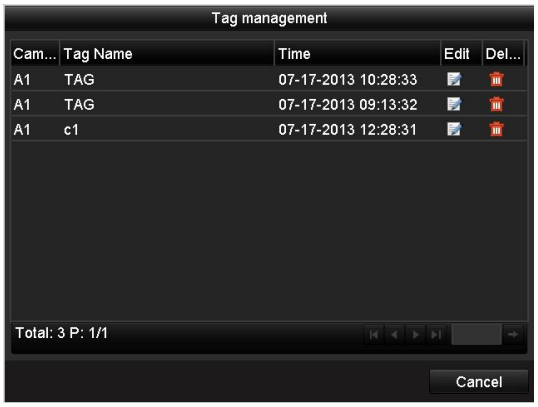


Figure 6. 6 Tag Management Interface

Steps:

1. Select **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 Keyword to search the tag on your command.

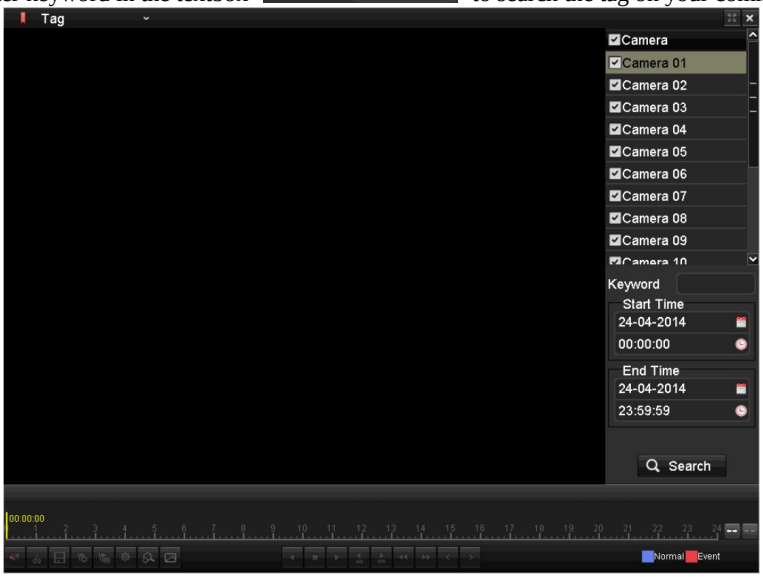


Figure 6. 7 Video Search by Tag

3. Click button to play back the file.

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

NOTE

- Pre-play and post-play can be configured.
- You can click or button to select the previous or next tag. Please refer to Table 6.1 for the description of buttons on the toolbar.

6.1.5 Playing Back by Smart Search

Purpose:

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

Before you start:

To get the smart search result, the corresponding event type must be enabled and configured on the IP camera. Here we take the intrusion detection as an example.

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

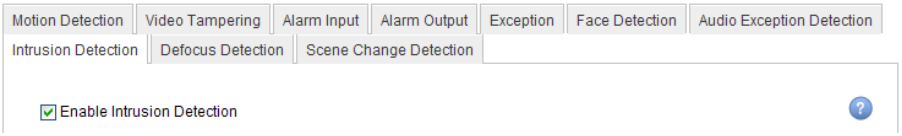


Figure 6. 8 Setting Intrusion Detection on IP Camera

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

Steps:

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

Figure 6. 9 Smart Playback Interface

4. Select a date in the calendar and click the button to play.
   Refer to Table 6.2 for the descriptions of the buttons on the Smart Playback Toolbar.

Table 6. 2 Detailed Explanation of Smart Playback Toolbar

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

5. Set the rules and areas for smart search of VCA event or motion event.
   - **Line Crossing Detection**

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

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

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

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

6. Click to configure the smart settings.

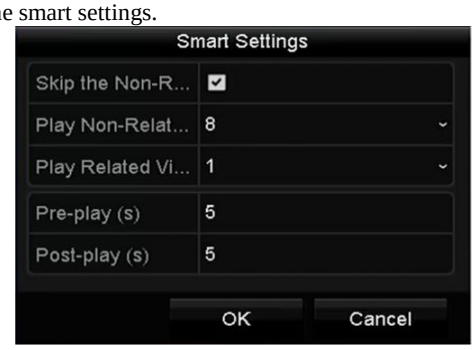


Figure 6. 10 Smart Settings

Skip the Non-Related Video: The non-related video will not be played if this function is enabled.
Play Non-Related Video at: Set the speed to play the non-related video. Max. 8/4/2/1 are selectable.
Play Related Video at: Set the speed to play the related video. Max. 8/4/2/1 are selectable.

NOTE

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

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

Figure 6. 11 Set Result Filter

NOTE

The Result Filter function is supported by the IP camera only.

6.1.6 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

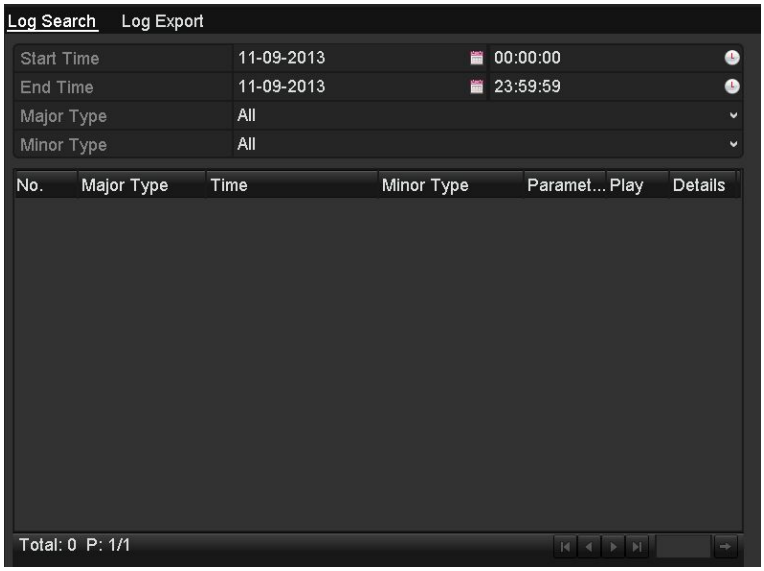


Figure 6. 12 System Log Search Interface

2. Click **Log Search** tab to enter **System Log Search** interface.
Set search time and type and click **Search** button.

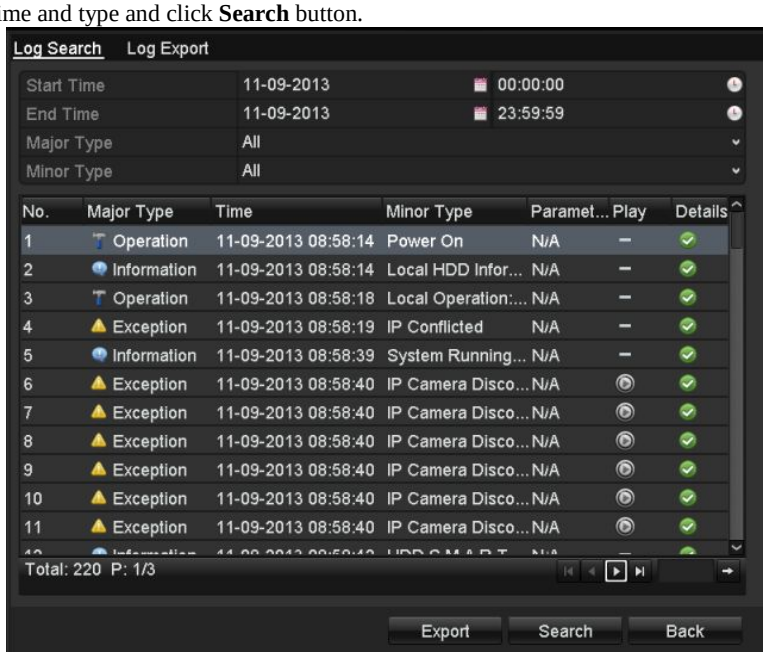


Figure 6. 13 Result of System Log Search

3. 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.

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

Figure 6. 14 Interface of Playback by Log

6.1.7 Playing Back by Sub-periods

Purpose:
The video files can be played in multiple sub-periods simultaneously on the screens.
Steps:

1. Enter **Playback** interface.
   Menu>Playback
2. Select **Sub-periods** from the drop-down list in the upper-left corner of the page to enter the **Sub-periods Playback** interface.
3. Select a date and start playing the video file.
4. Select the **Split-screen Number** from the dropdown list. Up to 16 screens are configurable.

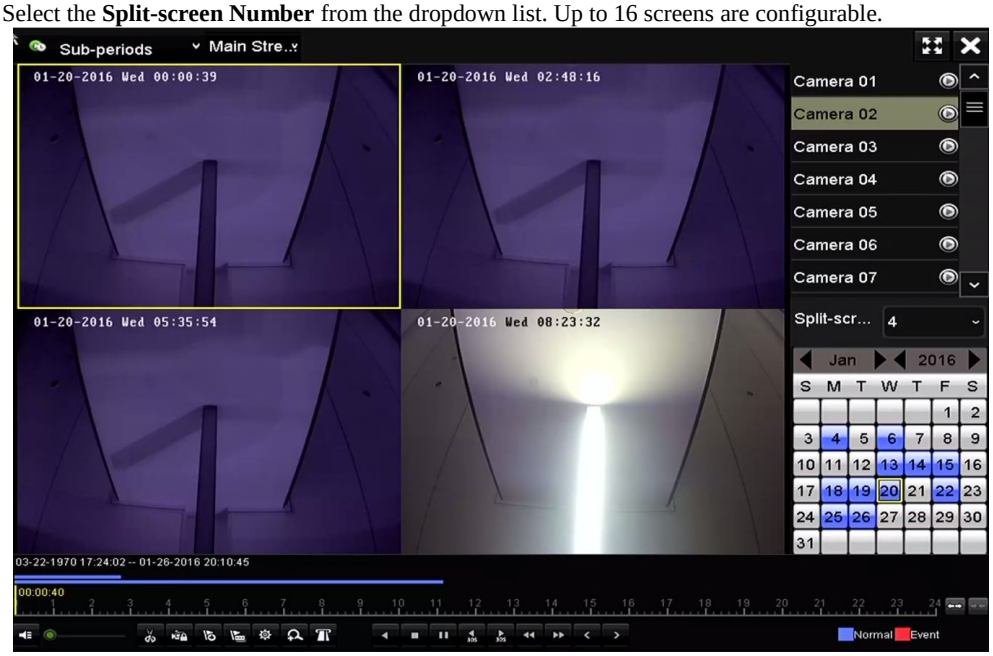


Figure 6. 15 Interface of Sub-periods Playback

According to the defined number of split-screens, the video files on the selected date can be divided into average segments for playback. E.g., if there are video files existing between 16:00 and 22:00, and the 6-screen display mode is selected, then it can play the video files for 1 hour on each screen simultaneously.

6.1.8 Playing Back External File

Purpose:
Perform the following steps to look up and play back files in the external devices.
Steps:
1. Enter the Playback 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. 16 Interface of External File Playback

6.2 Auxiliary Functions of Playback

6.2.1 Playing Back Frame by Frame

Purpose:
Play video files frame by frame, in order to check image details of the video when abnormal events happen.
Steps:
1. Go to Playback interface and click button until the speed changes to *Single* frame.
2. One click on the playback screen represents playback or adverse playback of one frame. You can use button in toolbar to stop the playing.

6.2.2 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. 17 Draw Area for Digital Zoom

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

6.2.3 Reverse Playback of Multi-channel

Purpose:
You can play back record files of multi-channel reversely. Up to 16-ch simultaneous 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. 18 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 Backing up by Normal Video Search

Purpose:
The record files can be backed up to various devices, such as USB devices (USB flash drives, USB HDDs, USB writer), SATA writer and e-SATA HDD.
Backup using USB flash drives and USB HDDs
Steps:

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

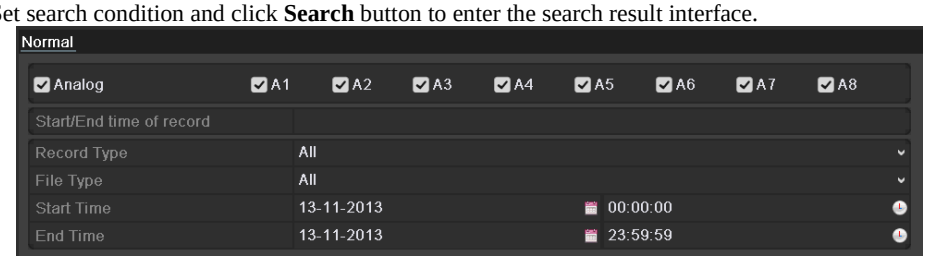


Figure 7. 1 Normal Video Search for Backup

4. The matched video files are displayed in **Chart** or **List** display mode.
   Click to play the record file if you want to check it.
   Check the checkbox before the video files you want to back up.

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

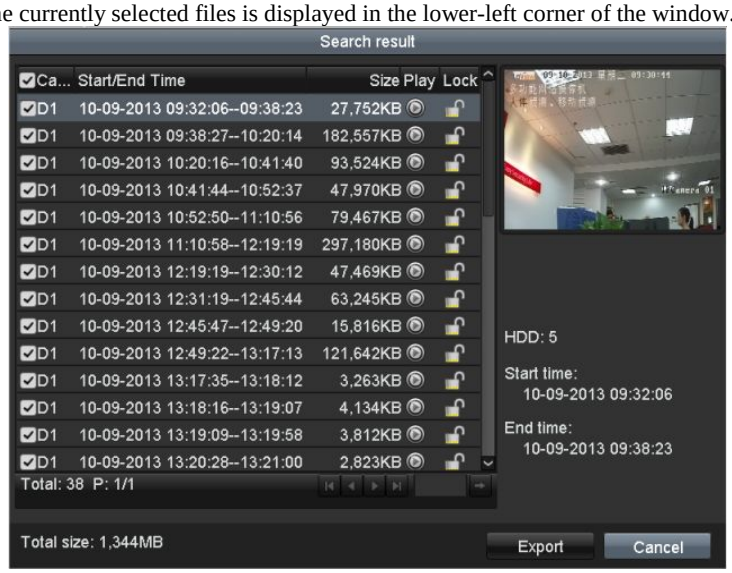


Figure 7. 2 Result of Normal Video Search for Backup

5. Select video files from the **Chart** or **List** to export, and click the button **Export** to enter the **Export** interface.
   You can also click **Export All** to select all the video files for backup and enter the **Export** interface.

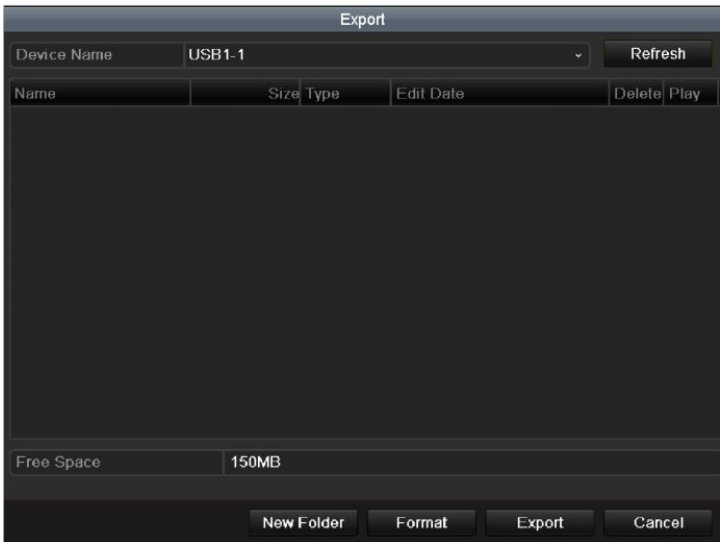


Figure 7. 3 Export by Normal Video Search using USB Flash Drive

6. Select the backup device from the drop-down list and you can also select the file format to filter the files existing in the backup device.
7. Select the save type to MP4 or AVI
8. Click the button **Export** on the Export interface to start the backup process. On the pop-up message box, select to export the video files or the player to the backup device. Click **OK** to confirm.

Figure 7. 4 Select File or Player for Backup

9. A prompt message will pop up after the backup process is complete. Click **OK** to confirm.

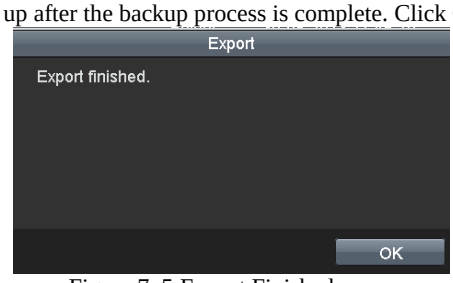


Figure 7. 5 Export Finished

NOTE

The backup of video files using USB writer or SATA writer has the same operating instructions. Please refer to steps described above.

7.1.2 Backing up by Event Search

Purpose:

Back up event-related record files using USB devices (USB flash drives, USB HDDs, USB writer), SATA writer or eSATA HDD. Quick Backup and Normal Backup are supported.

Steps:

1. Enter **Export** interface.
   Menu > Export > Event
2. Select the cameras to search.
3. Select the event type to alarm input, motion or VCA.

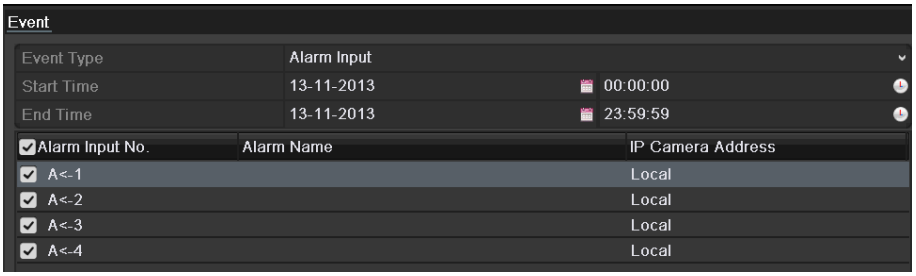


Figure 7. 6 Event Search for Backup

4. Set search condition and click **Search** button to enter the search result interface. The matched video files are displayed in **Chart** or **List** display mode.
5. Select video files from the **Chart** or **List** interface to export.
6. Export the video files. Please refer to step5 of Chapter 7.1.1 Backing up by Normal Video Search for details.

7.1.3 Backing up Video Clips

Purpose:
You may also select video clips in playback mode to export directly during Playback, using USB devices (USB flash drives, USB HDDs, USB writer), or SATA writer.
Steps:
1. Enter **Playback** interface.
2. During playback, use buttons or in the playback toolbar to start or stop clipping record file(s).
3. Click the to enter the file management interface.
4. Export the video clips in playback. Please refer to step5 of *Chapter 7.1.1 Backing up by Normal Video Search* for details.

7.2 Managing Backup Devices

Management of USB flash drives, USB HDDs and eSATA HDDs
Steps:
1. Enter the **Export** interface.
2. Backup device management.
   Click **New Folder** button if you want to create a new folder in the backup device.
   Select a record file or folder in the backup device and click button if you want to delete it.
   Click **Erase** button if you want to erase the files from a re-writable CD/DVD.
   Click **Format** button to format the backup device.

   NOTE
   If the inserted storage device is not recognized:
   - Click the **Refresh** button.
   - Reconnect device.
   - Check for compatibility from vendor.

Chapter 8 Alarm Settings

8.1 Setting Motion Detection

Steps:

1. Enter **Motion Detection** interface of Camera Management and choose a camera you want to set up motion detection.
   Menu> Camera> Motion

Figure 8. 1 Motion Detection Setup Interface

2. Set detection area and sensitivity.
   Check ☑ checkbox to enable motion detection. Use the mouse to draw detection area(s) or click **Full Screen** to set the detection area to be the full screen and drag the sensitivity bar to set sensitivity.
   Click ⚙ to set alarm response actions.

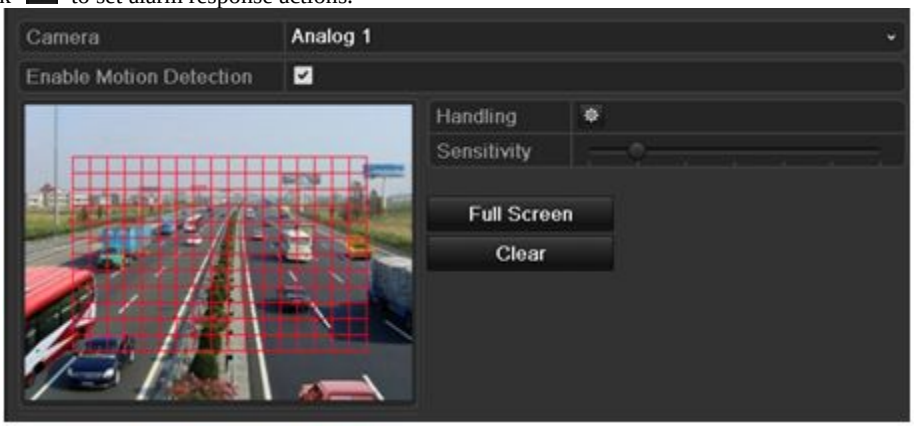


Figure 8. 2 Set Detection Area and Sensitivity

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.

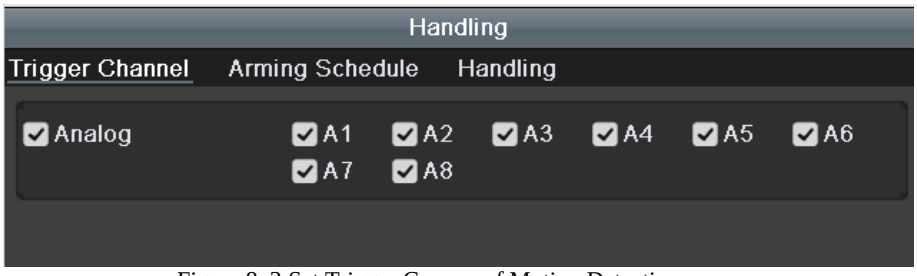


Figure 8. 3 Set Trigger Camera of Motion Detection

4. Set 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. Or you can click the **Copy** button to copy the time period settings to other day(s).

NOTE

Time periods shall not be repeated or overlapped.

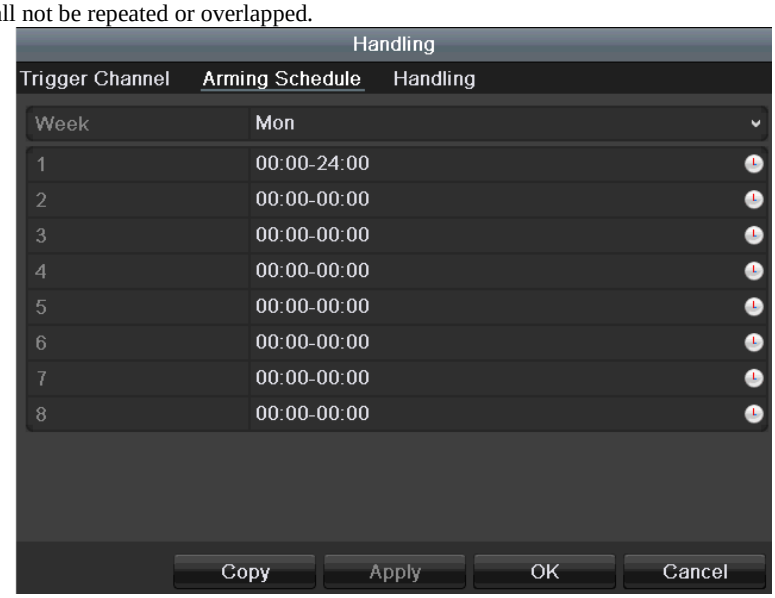


Figure 8. 4 Set Arming Schedule of Motion Detection

5. Click **Linkage Action** tab to set up alarm response actions of motion alarm (please refer to *Chapter 8.7 Setting Alarm Response Actions*).
   Repeat the above steps to set up arming schedule of other days of a week.
   Click the **OK** button to complete the motion detection settings of the channel.
6. If you want to set motion detection for another channel, repeat the above steps or just copy the above settings to it.

NOTE

You are not allowed to copy the “Trigger Channel” action.

8.2 Setting Sensor Alarms

Purpose:
Set up 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.

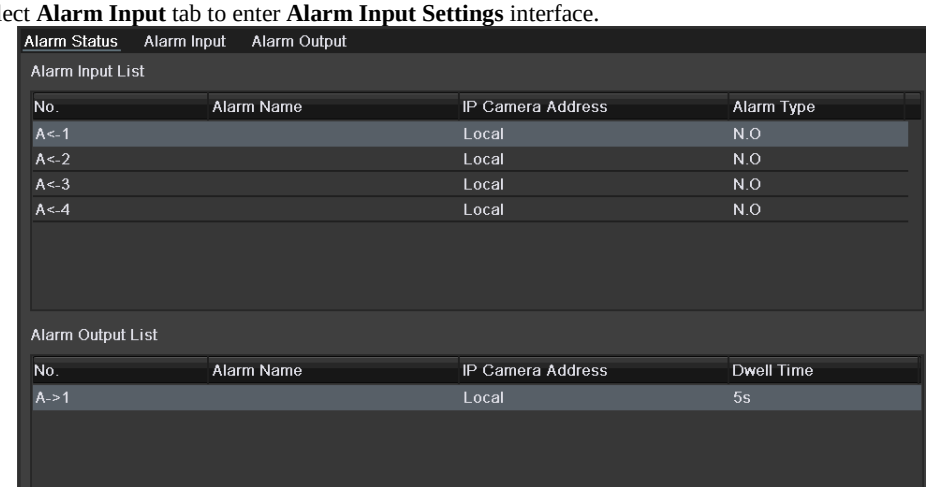


Figure 8. 5 Alarm Status Interface of System Configuration

2. Set the handling method of the selected alarm input.
Check the **Enable** checkbox and click button to set its alarm response actions.

Figure 8. 6 Alarm Input Settings 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 input is triggered.

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.

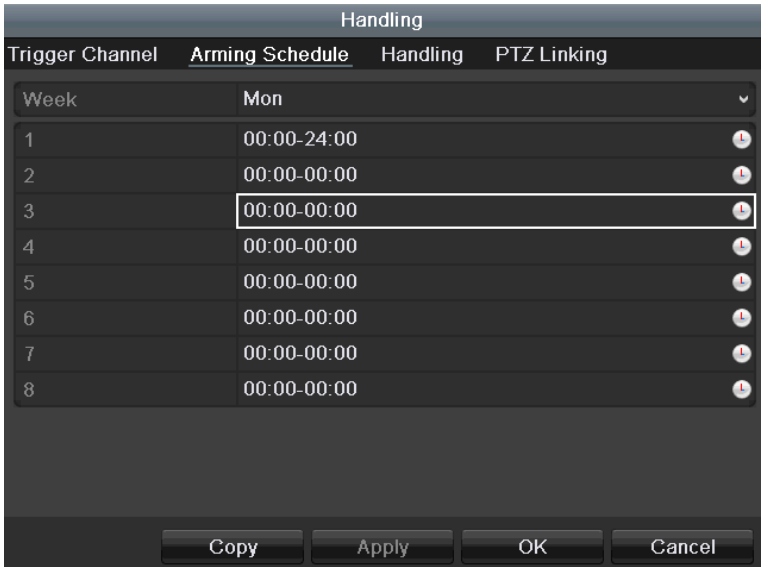


Figure 8. 7 Set Arming Schedule of Alarm Input

5. Select **Linkage Action** tab to set up alarm response actions of the alarm input (please refer to *Chapter 8.7 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.
6. If necessary, select **PTZ Linking** tab and set PTZ linkage of the alarm input.
   Set PTZ linking parameters and click the **OK** button 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.

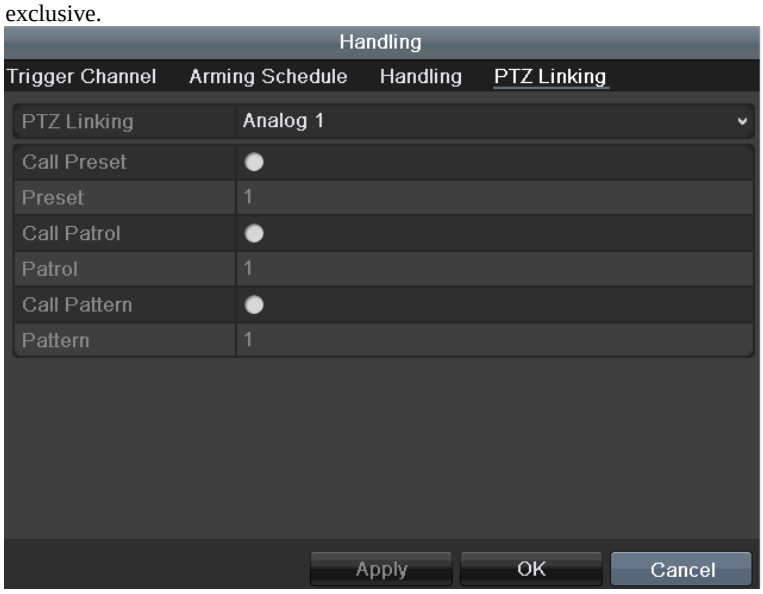


Figure 8. 8 Set PTZ Linking of Alarm Input

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

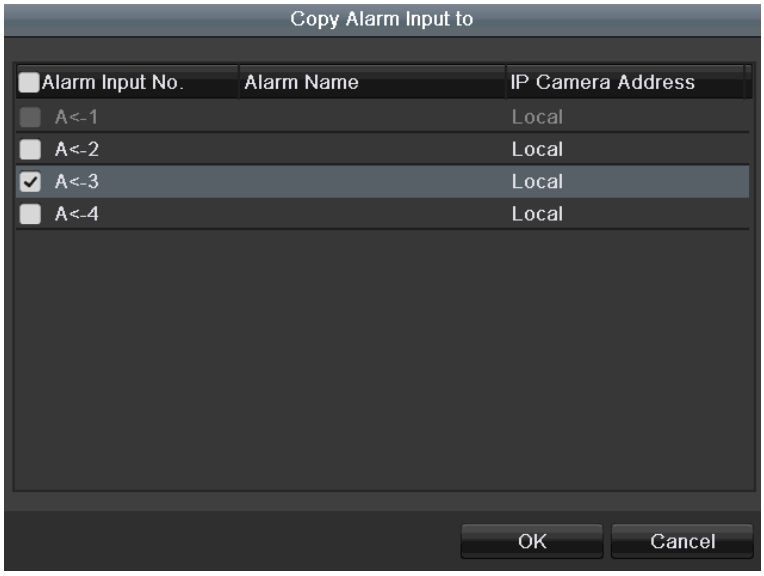


Figure 8. 9 Copy Settings of Alarm Input

8.3 Detecting Video Loss

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

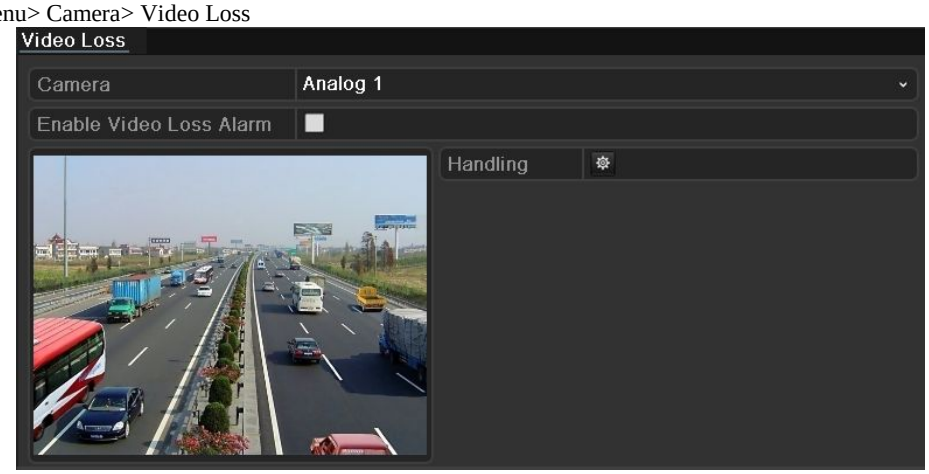


Figure 8. 10 Video Loss Setup Interface

2. Set up handling method of video loss.
   Check the checkbox of **Enable Video Loss Alarm**.
   Click button to set up handling method of video loss.
3. Set 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. Or you can click the **Copy** button to copy the time period settings to other day(s).

NOTE Time periods shall not be repeated or overlapped.

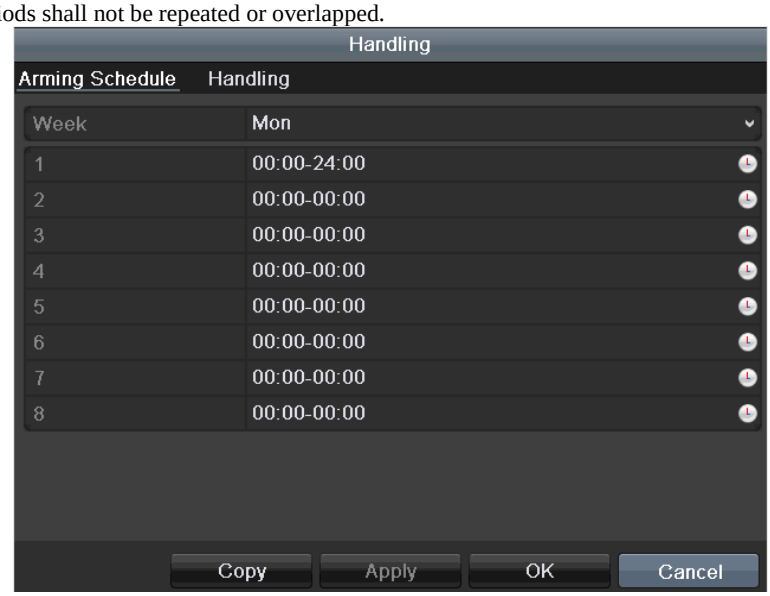


Figure 8. 11 Set Arming Schedule of Video Loss

   Repeat the above steps to set arming schedule of other days of a week. You can also use **Copy** button to copy an arming schedule to other days.
4. Select **Linkage Action** tab to set up alarm response action of video loss (please refer to *Chapter 8.7 Setting Alarm Response Actions*).
5. Click the **OK** button to complete the video loss settings of the channel.

Repeat the above steps to finish settings of other channels, or click the **Copy** button copy the above settings to them.

8.4 Detecting Video Tampering

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> Video Tampering Detection

Figure 8. 12 Video Tempering Interface

2. Check the checkbox of **Enable Video Tampering Detection**.
3. Drag the sensitivity bar and choose a proper sensitivity level.
4. Click to set handling method of video tampering. Set arming schedule and alarm response actions of the channel.
   1) Click **Arming Schedule** tab to set the arming schedule of response action.
   2) 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.

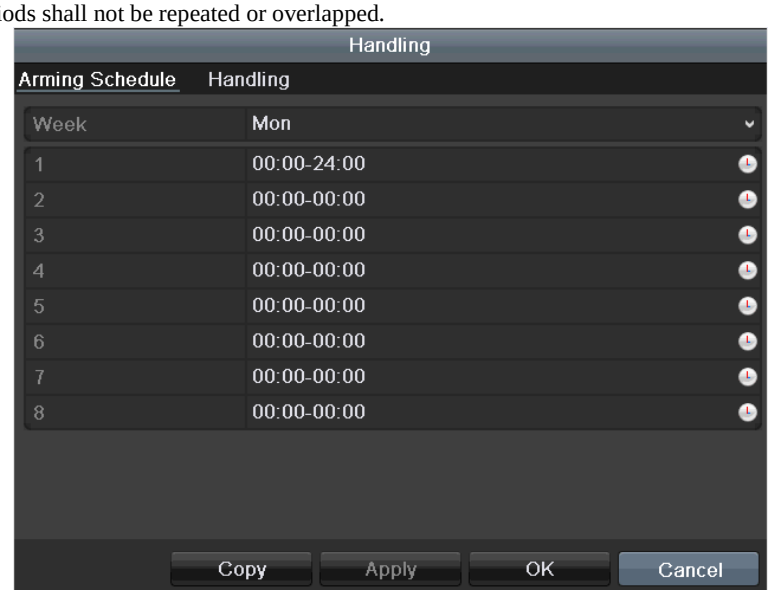


Figure 8. 13 Set Arming Schedule of Video Tampering

   3) Select **Linkage Action** tab to set alarm response actions of video tampering alarm (please refer to *Chapter 8.7 Setting Alarm Response Actions*).
      Repeat the above steps to set arming schedule of other days of a week. You can also use **Copy** button to copy an arming schedule to other days.
   4) Click the **OK** button to complete the video tampering settings of the channel.

Repeat the above steps to finish settings of other channels, or click the **Copy** button copy the above settings to them.

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

8.5 Setting All-day Video Quality Diagnostics

Purpose:
The device provides two ways to diagnose the video quality: manual and all-day. Perform the following steps to set the threshold of the diagnosing and the linkage actions.
Steps:

1. Enter **Video Quality Diagnostics Settings** interface of Camera Management and select a channel you want to detect video tampering.
   Menu> Camera> Video Quality Diagnostics
2. Check the checkbox of **Enable Video Quality Diagnostics**.
   NOTE
   To enable video quality diagnostics, the function should be supported by the selected camera.
3. Enable and set the threshold of the diagnostic types, there are **Blurred Image**, **Abnormal Brightness**, and **Color Cast**.
   Check the corresponding checkbox of the diagnostic type, and adjust the threshold of it by dragging the bar.
   NOTE
   The higher the threshold you set, the harder the exception will be detected.
4. Click to set handling method of video quality diagnostics. Set arming schedule and alarm response actions of the channel.
   1) Click **Arming Schedule** tab to set the arming schedule of response action.
   2) 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.

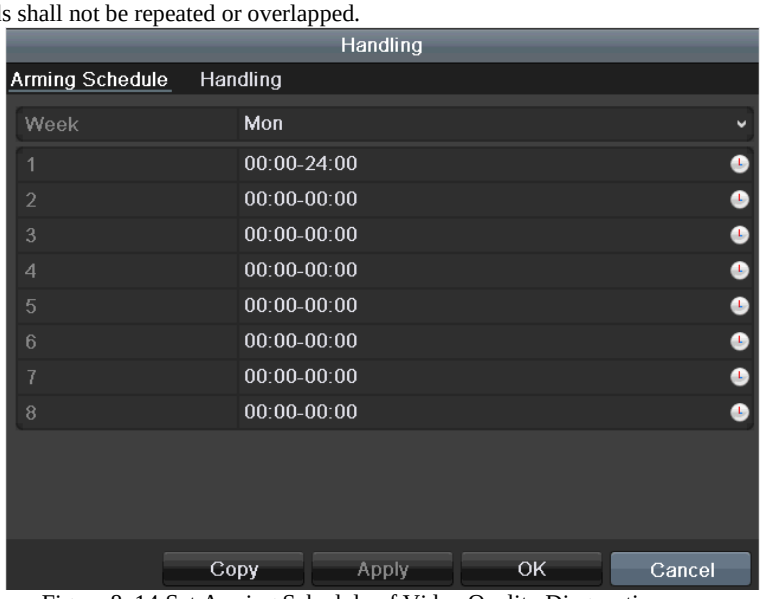


Figure 8. 14 Set Arming Schedule of Video Quality Diagnostics

   3) Select **Linkage Action** tab to set alarm response actions of video quality diagnostics alarm (please refer to *Chapter 8.7 Setting Alarm Response Actions*).
      Repeat the above steps to set arming schedule of other days of a week. You can also use **Copy** button to copy an arming schedule to other days.
   4) Click the **OK** button to complete the video quality diagnostics settings of the channel.
5. Click the **Apply** button to save and activate settings.
6. (Optional) you can copy the same settings to other cameras by clicking the **Copy** button.

8.6 Handling Exceptions

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

- **HDD Full:** The HDD is full.
- **HDD Error:** Writing HDD error, unformatted HDD, etc.
- **Network Disconnected:** Disconnected network cable.
- **IP Conflicted:** Duplicated IP address.
- **Illegal Login:** Incorrect user ID or password.
- **Input/Recording Resolution Mismatch:** The input resolution is smaller than the recording resolution.
- **Record Exception:** No space for saving recorded files.

Steps:

1. Enter **Exceptions** interface and handle various exceptions.
   Menu> Configuration> Exceptions

Figure 8. 15 Exception Settings Interface

2. Check the checkbox of **Enable Event Hint** to display the (Event/Exception icon) when an exceptional event occurs. And click the icon to select the detailed event hint for display.

   NOTE

   Click the icon appears in the live view interface, and you can view the detailed information of the exceptional event. Click the button **Set**, and then you can select the detailed event hint for display.

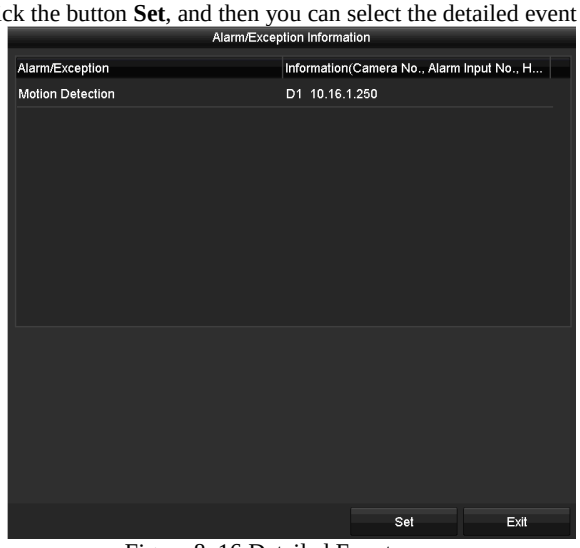


Figure 8. 16 Detailed Event

3. Set the alarm linkage actions. For details, see *Chapter 8.7 Setting Alarm Response Actions.*
4. Click **Apply** to save the settings.

8.7 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, Send Email and Trigger Alarm Output.

Full Screen Monitoring
When an alarm is triggered, the local monitor (HDMI, VGA or CVBS monitor) displays 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.
Auto-switch will terminate once the alarm stops and you will be taken back to the Live View interface.

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 11.2.6 Configuring More Settings* for details of alarm host configuration.

Send Email
Send an email with alarm information to a user or users when an alarm is detected.
Please refer to *Chapter 11.2.8 Configuring Email* for details of Email configuration.

Trigger Alarm Output
Trigger an alarm output when an alarm is triggered.
Steps:

1. Enter Alarm Output interface.
   Menu> Configuration> Alarm> Alarm Output
   Select an alarm output and set alarm name and dwell time.

   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. 17 Alarm Output Settings Interface

2. Click button to set the arming schedule of 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.

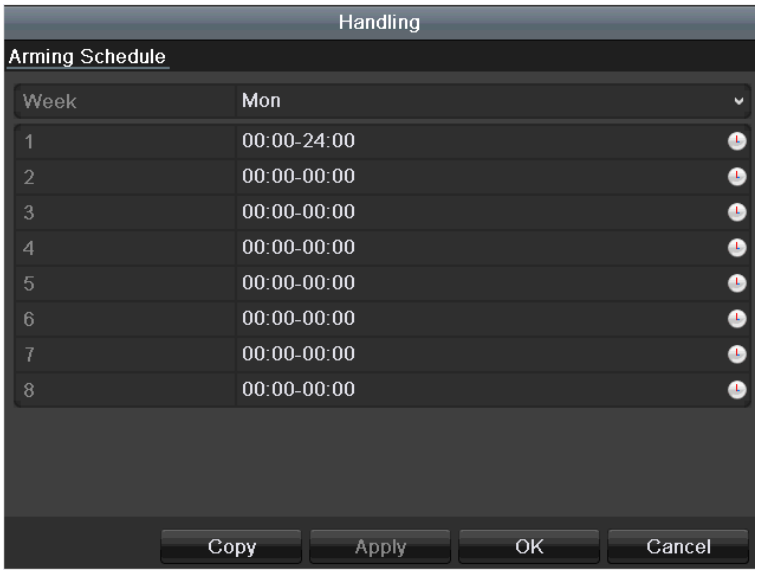


Figure 8. 18 Set Arming Schedule of Alarm Output

3. Repeat the above steps to set arming schedule of other days of a week. You can also click **Copy** button to copy an arming schedule to other days.
   Click the **OK** button to complete the arming schedule setting of alarm output.
4. Click the **Apply** button to save the settings.

Chapter 9 POS Configuration

This chapter is applicable to some series DVR only.

9.1 Configuring POS Settings

Steps:

1. Enter the POS settings interface.

   Menu > Configuration > POS> POS Settings

2. Select the POS from the drop-down list. Up to 8 POS units are selectable.
3. Check the checkbox to enable the POS feature.
4. Select the POS protocol to Universal Protocol, EPSON or AVE.

   - **Universal Protocol**

   Click the **Advanced** button to expand more settings when selecting the universal protocol. You can set the start line tag, line break tag and end line tag for the POS overlay characters, and the case-sensitive property of the characters.

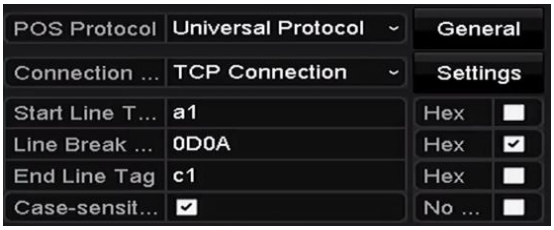


Figure 9. 1 Universal Protocol Settings

5. Select the connection mode to TPC, UDP, Multicast, RS-232, USB->RS-232 or Sniff, and click **Settings** to configure the parameters for each connection mode.

   - **TCP Connection**

   When using TCP connection, the port must be set from 0 to 65535, and the port for each POS machine must be unique.

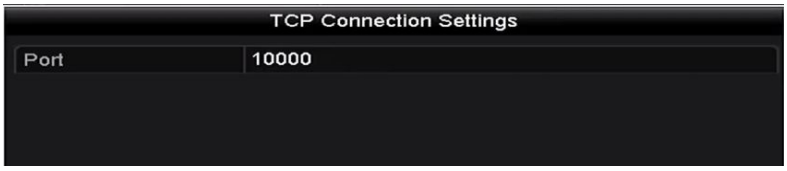


Figure 9. 2 TCP Connection Settings

   - **UDP Connection**

   When using UDP connection, the port must be set from 0 to 65535, and the port for each POS machine must be unique.

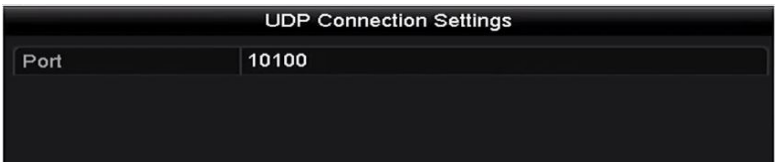


Figure 9. 3 UDP Connection Settings

   - **USB->RS-232 Connection**

   Configure the port parameters of USB-to-RS-232 convertor, including the serial number of port, baud

rate, data bit, stop bit, parity and flow ctrl.

NOTE

When using USB->RS-232 convertor mode, the port of USB-to-RS-232 convertor and the POS must be corresponding to each other, e.g., POS1 must be connected to port1 of the convertor.

Figure 9. 4 USB-to-RS-232 Settings

- **RS-232 Connection**

  Connect the DVR and the POS machine via RS-232. The RS-232 settings can be configured in Menu>Configuration>RS-232. The **Usage** must be set to Transparent Channel.

- **Multicast Connection**

  When connecting the DVR and the POS machine via Multicast protocol, set the multicast address and port.

Figure 9. 5 Multicast Settings

- **Sniff Connection**

  Connect the DVR and the POS machine via Sniff. Configure the source address and destination address settings.

Figure 9. 6 Sniff Settings

6. Set other parameters of characters overly.
   1) Select the character encoding format from the drop-down list.
   2) Select the overlay mode of the characters to display in scrolling or page mode. \
   3) Select the font size to small, medium or large.
   4) Set the overlay time of the characters. The value ranges 5 -3600 sec.
   5) (optional) Check the checkbox to enable the **POS Overlay in Live View**.
   6) Select the font color for the characters.

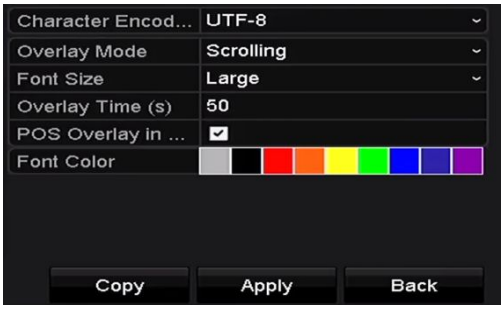


Figure 9. 7 Overlay Character Settings

NOTE

You can adjust the size and position of textbox on the preview screen of POS settings interface by dragging the frame.

7. Click **Apply** to activate the settings.
8. (Optional) You can click the **Copy** button to copy the current settings to other POS (s).

Figure 9. 8 Copy POS Settings

9.2 Configuring Overlay Channel

Purpose:
You can assign the POS machine to corresponding channel on which you want to overlay.

Steps:
1. Enter the POS settings interface.

   Menu > Configuration > POS> Overlay Channel
2. Click to select an analog or IP camera from the camera list on the right, and then click a POS item from the POS list you want to overlay on the selected camera.

   Click or to go to the previous or next page of cameras.
3. You can also click to overlay all POS items to the first 8 channels in order. And the is used to clear all POS overlay settings.
4. Click the **Apply** button to save the settings.

9.3 Configuring POS Alarm

Purpose:

Set the POS alarm parameters to trigger certain channels to start recording, or trigger full screen monitoring, audio warning, notifying the surveillance center, sending email and so on.

Steps:

1. Enter the POS settings interface.

   Menu > Configuration > POS> POS Settings

2. Follow the steps in Chapter 9.1-9.2 to configure the POS settings.

3. Click to enter the alarm settings interface.

4. Click **Trigger Channel** tab and select one or more channels to record or become full-screen monitoring when POS alarm is triggered.

5. Set 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. Or you can click the **Copy** button to copy the time period settings to other day(s).

NOTE

Time periods shall not be repeated or overlapped.

6. Click the **Handling** tab to set up alarm response actions of POS alarm (please refer to *Chapter 8.7 Setting Alarm Response Actions*).
   Repeat the above steps to set up arming schedule of other days of a week.
   Click the **OK** button to complete the POS settings of the channel.
   Select PTZ Linking tab and set PTZ linkage of the POS alarm.
   Set PTZ linking parameters and click the OK button to complete the settings of the alarm input.

NOTE

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

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

Chapter 10 VCA Alarm

Purpose:
The DVR can receive the VCA alarm (line crossing detection, intrusion detection, sudden scene change detection and audio exception detection) sent by analog camera, and the VCA detection must be enabled and configured on the camera settings interface first. All other VCA detection features must be supported by the connected IP camera.

10.1 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.
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 8.1 Setting Motion Detection* for detailed instructions.
5. Click the **Rule Settings** button to set the face detection rules. You can 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.

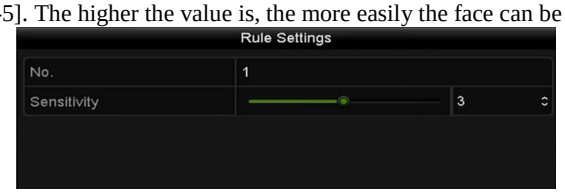


Figure 10. 1 Set Face Detection Sensitivity

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

10.2 Vehicle Detection

Purpose:

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

Steps:

1. Enter the VCA settings interface.
   Menu> Camera> VCA
2. Select the camera to configure the VCA.
   You can click the checkbox of **Save VCA Picture** to save the captured pictures of VCA detection.
3. Select the VCA detection type to **Vehicle Detection**.
4. Check the **Enable** checkbox to enable this function.
5. Click to configure the trigger channel, arming schedule and linkage actions for the Blacklist, Whitelist and Others.
6. Click the **Rule Settings** to enter the rule settings interface. Configure the lane, upload picture and overlay content settings. Up to 4 lanes are selectable.
7. Click **Save** to save the settings.

NOTE

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

10.3 Line Crossing Detection

Purpose:

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

Steps:

1. Enter the VCA settings interface.
   Menu> Camera> VCA
2. Select the camera to configure the VCA.
   You can click the checkbox of **Save VCA Picture** to save the captured pictures of VCA detection.
3. Select the VCA detection type to **Line Crossing Detection**.
4. Check the **Enable** checkbox to enable this function.
5. Click to configure the trigger channel, arming schedule and linkage actions for the line crossing detection alarm.
6. Click the **Rule Settings** button to set the line crossing detection rules.
   1) Select the direction to A<->B, A->B or B->A.
      A<->B: Only the arrow on the B side shows. When an object goes across the configured line, both directions can be detected and alarms are triggered.
      A->B: Only the object crossing the configured line from the A side to the B side can be detected.
      B->A: Only the object crossing the configured line from the B side to the A side can be detected.
   2) Drag the slider to set the detection sensitivity.
      Sensitivity: Range [1-100]. The higher the value is, the more easily the detection alarm can be triggered.
   3) Click **OK** to save the rule settings and return to the line crossing detection settings interface.

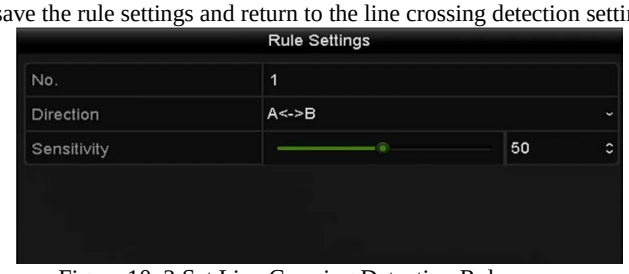


Figure 10. 2 Set Line Crossing Detection Rules

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

   NOTE

   Up to 4 rules can be configured.
8. Click **Apply** to activate the settings.

NOTE

The sudden scene change detection and the line crossing detection cannot be enabled at the same channel.

10.4 Intrusion Detection

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

Figure 10. 3 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.
   NOTE
   Up to 4 rules can be configured.
8. Click **Apply** to save the settings.

NOTE
The sudden scene change detection and the intrusion detection cannot be enabled at the same channel.

10.5 Region Entrance Detection

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

10.6 Region Exiting Detection

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

NOTE

- Please refer to the *Chapter 9.5 Region Entrance Detection* for operating steps to configure the region exiting detection.
- Up to 4 rules can be configured.

10.7 Loitering Detection

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

NOTE

- Please refer to the *Chapter 9.4 Intrusion Detection* for operating steps to configure the loitering detection.
- The **Threshold** [1s-10s] in the Rule Settings defines the time of the object loitering in the region. If you set the value as 5, alarm is triggered after the object loitering in the region for 5s; and if you set the value as 0, alarm is triggered immediately after the object entering the region.
- Up to 4 rules can be configured.

10.8 People Gathering Detection

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

NOTE

- Please refer to the *Chapter 9.4 Intrusion Detection* for operating steps to configure the people gathering detection.
- The **Percentage** in the Rule Settings defines the gathering density of the people in the region. Usually, when the percentage is small, the alarm can be triggered when small number of people gathered in the defined detection region.
- Up to 4 rules can be configured.

10.9 Fast Moving Detection

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

NOTE

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

10.10 Parking Detection

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

NOTE

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

10.11 Unattended Baggage Detection

Purpose:

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

NOTE

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

object left in the region can trigger the alarm.
- Up to 4 rules can be configured.

10.12 Object Removal Detection

Purpose:

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

NOTE

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

10.13 Audio Exception Detection

Purpose:

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

NOTE

The audio exception detection is supported by all analog channels.

Steps:

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

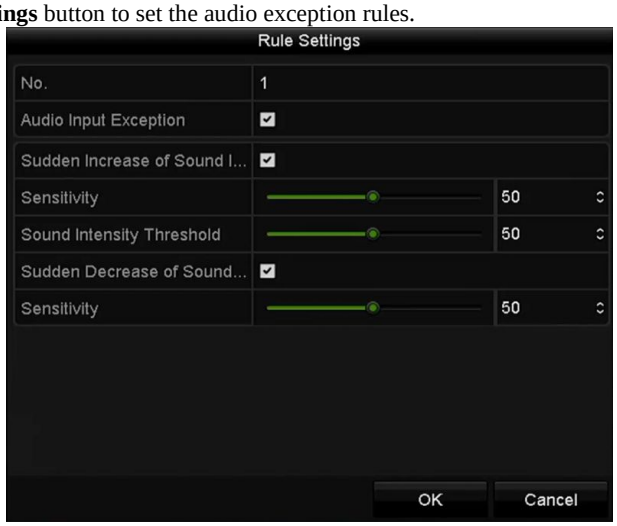


Figure 10. 4 Set Audio Exception Detection Rules

1) Check the checkbox of **Audio Loss Exception** to enable the audio loss detection function.
2) Check the checkbox of **Sudden Increase of Sound Intensity Detection** to detect the sound steep rise in the surveillance scene. You can set the detection sensitivity and threshold for sound steep rise.
   Sensitivity: Range [1-100], the smaller the value is, the more severe the change should be to trigger the detection.

Sound Intensity Threshold: Range [1-100], it can filter the sound in the environment, the louder the environment sound, the higher the value should be. You can adjust it according to the real environment.

3) Check the checkbox of **Sudden Decrease of Sound Intensity Detection** to detect the sound steep drop in the surveillance scene. You can set the detection sensitivity [1-100] for sound steep drop.

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

10.14 Defocus Detection

Purpose:

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

NOTE

- Please refer to the *Chapter 9.1 Face Detection* for operating steps to configure the defocus detection.
- The **Sensitivity** in the Rule Settings ranges from 1 to 100, and the higher the value is, the more easily the defocus image can trigger the alarm.

10.15 PIR Alarm

Purpose:

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

Steps:

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

Chapter 11 VCA Search

With the configured VCA detection, the device supports the VCA search for the behavior search, face search, plate search, people counting and heat map results.

11.1 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 files according to the specified conditions.
Before you start:
Please refer to *Section 9.2 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.

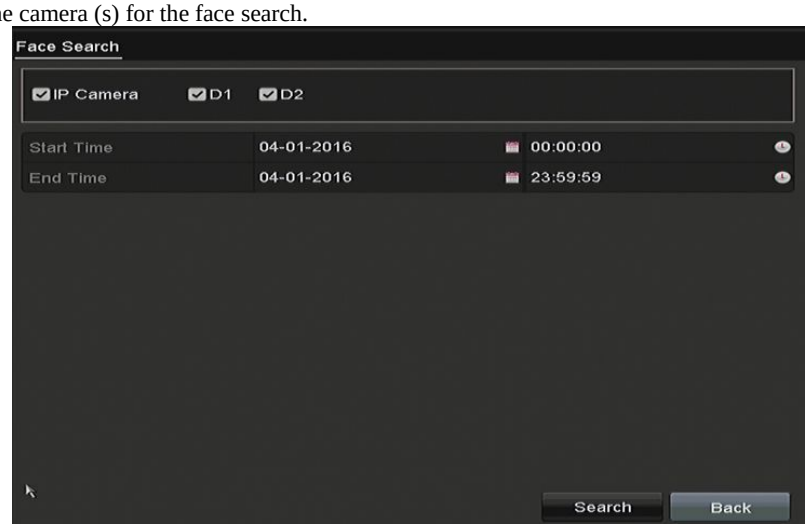


Figure 11. 1 Face Search

3. Specify the start time and end time for searching the captured face pictures or video files.
4. Upload the pictures from your local storage device for matching the detected face pictures.
5. Set the similarity level for the source pictures and the captured pictures.
6. Click **Search** to start searching. The search results of face detection pictures are displayed in list or in chart.
7. 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.
8. If you want to export the captured face pictures to local storage device, connect the storage device to the device and click **Export All** to enter the Export interface.
   Click **Export** to export all face pictures to the storage device.
   Please refer to *Chapter 7 Backup* for the operation of exporting files.

Figure 11. 2 Export Files

11.2 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.

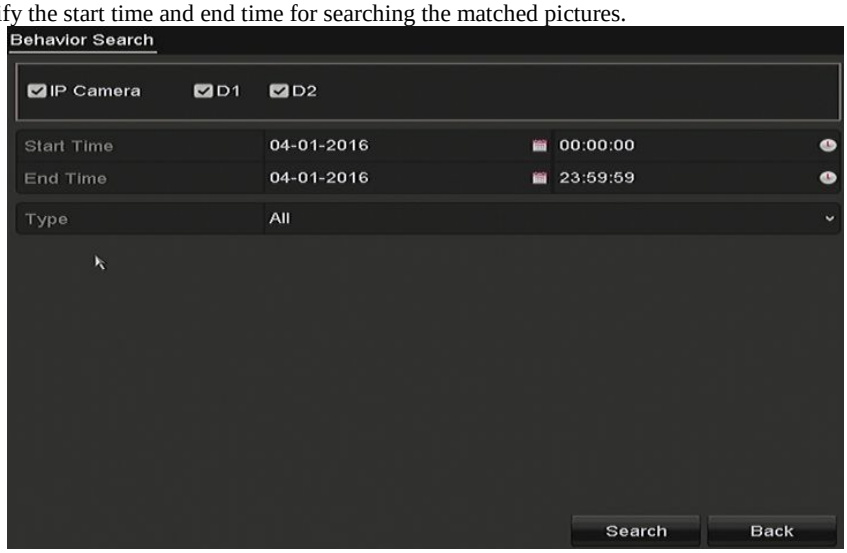


Figure 11. 3 Behavior Search Interface

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.
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.

11.3 Plate Search

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

Steps:

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

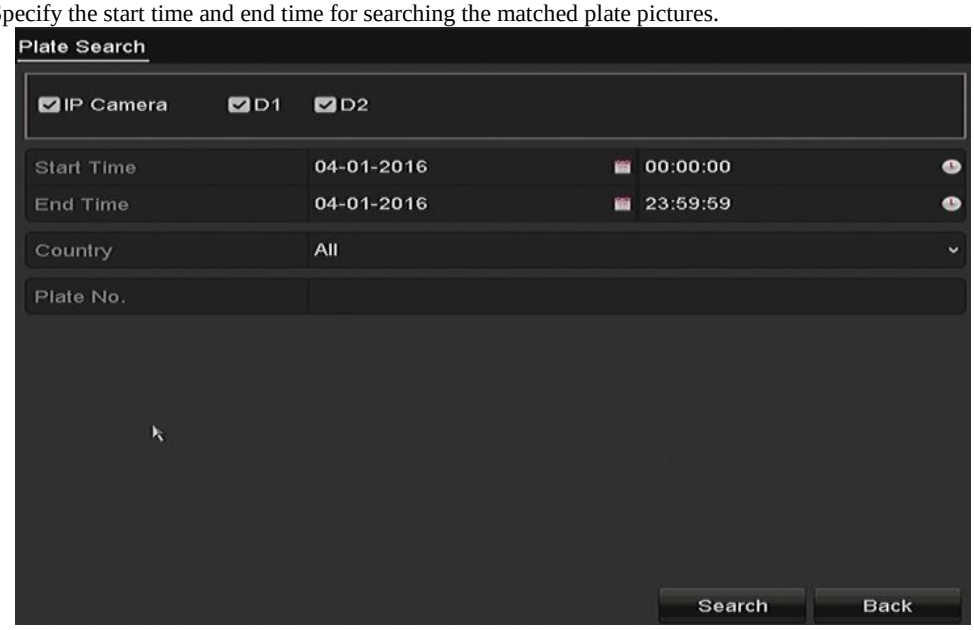


Figure 11. 4 Plate Search

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

NOTE

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

11.4 People Counting

Purpose:

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

Steps:

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

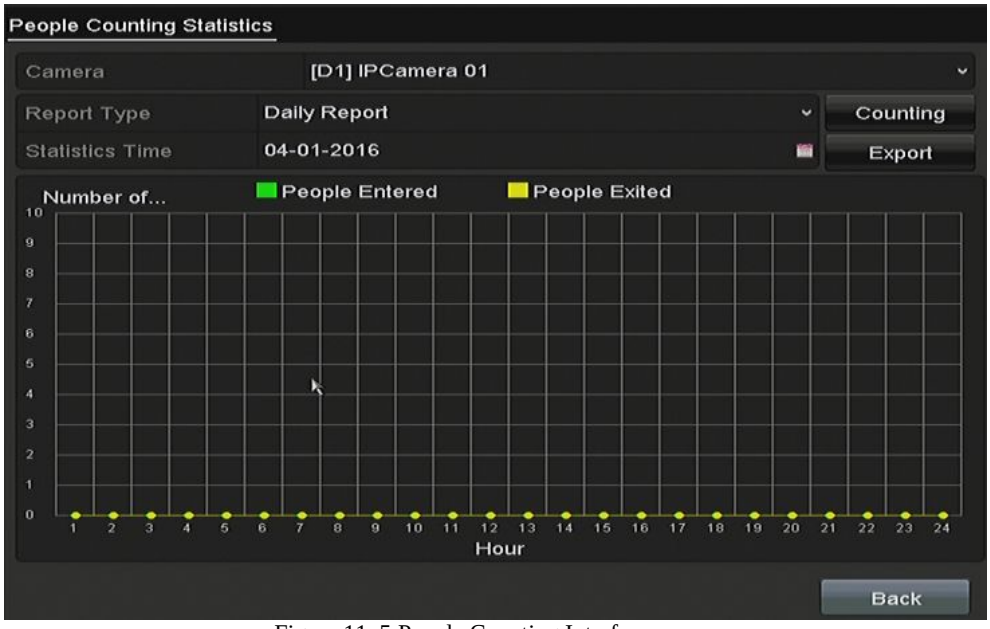


Figure 11. 5 People Counting Interface

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

11.5 Heat Map

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

NOTE

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.

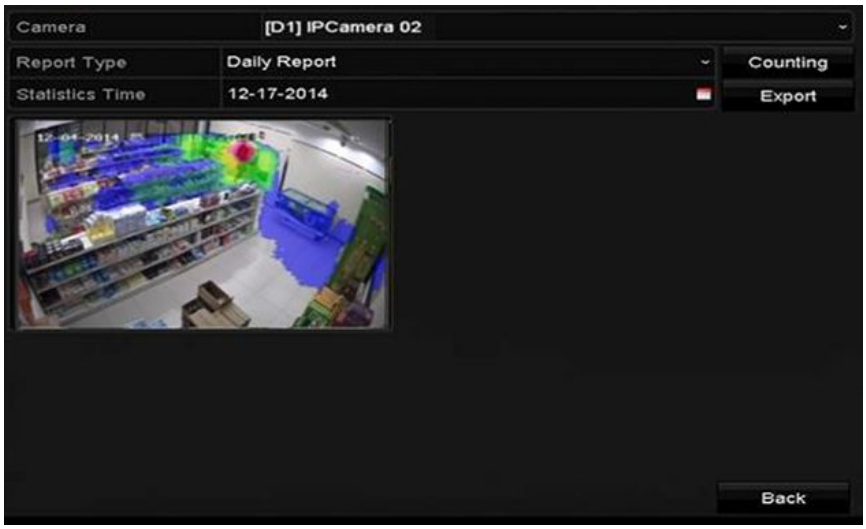


Figure 11. 6 Heat Map Interface

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.

NOTE

As shown in Figure 10.8, 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 12 Network Settings

12.1 Configuring General Settings

Purpose:
Network settings must be properly configured before you operate DVR over network.
Steps:

1. Enter the Network Settings interface.
   Menu > Configuration > Network

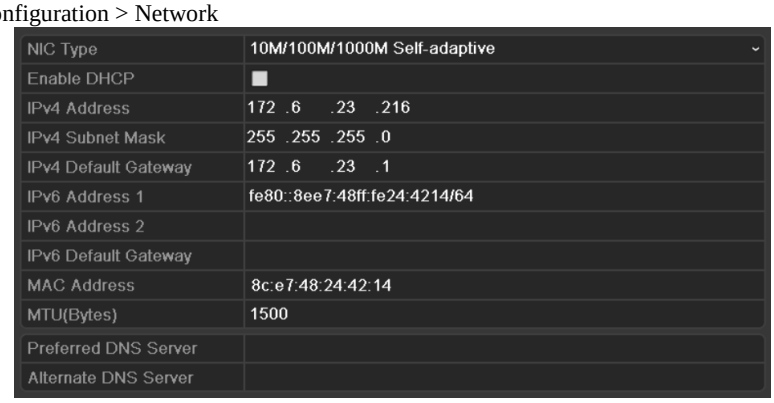


Figure 12. 1 Network Settings Interface

NOTE

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

NOTE

- The valid value of MTU is from 500 to 1500.
- If the DHCP server is available, you can check the checkbox of **DHCP** to automatically obtain an IP address and other network settings from that server.

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

12.2 Configuring Advanced Settings

12.2.1 Configuring PPPoE Settings

Purpose:
The DVR 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.

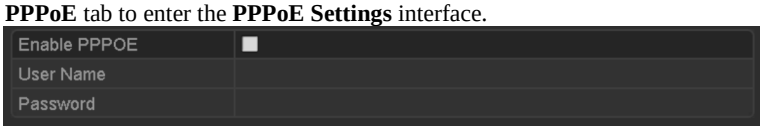


Figure 12. 2 PPPoE Settings Interface

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

   NOTE

   The User Name and Password should be assigned by your ISP.
5. Click the **Apply** button to save the settings.
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.

12.2.2 Configuring PT Cloud

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

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

   NOTE

   The verification code consists of 6 capital letters and is located at the bottom of the DVR. You can also use the scanning tool of your phone to quickly get the code by scanning the QR code below.

Figure 12. 3 PT Cloud Settings Interface

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

After configuration, you can access and manage the NVR by your mobile phone on which the PT Cloud application is installed or by the website (http://www. hicloudcam.com).

NOTE

For more operation instructions, please refer to the help file on the official website (http://www. hicloudcam.com).

12.2.3 Configuring DDNS

Purpose:

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

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

Steps:

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

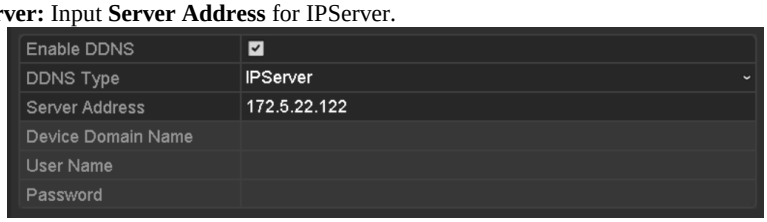


Figure 12. 4 IPServer Settings Interface

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

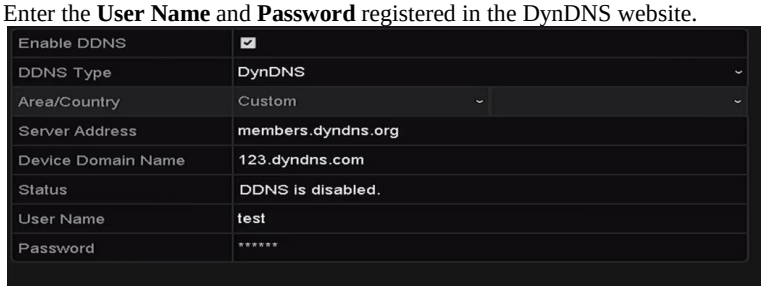


Figure 12. 5 DynDNS Settings Interface

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

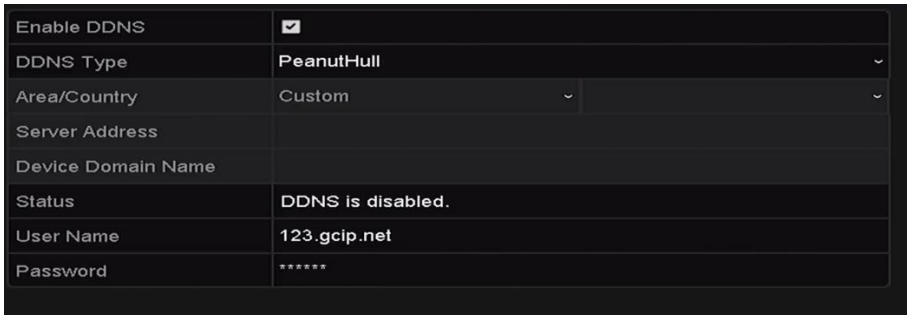


Figure 12. 6 PeanutHull Settings Interface

- **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 **Device 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.

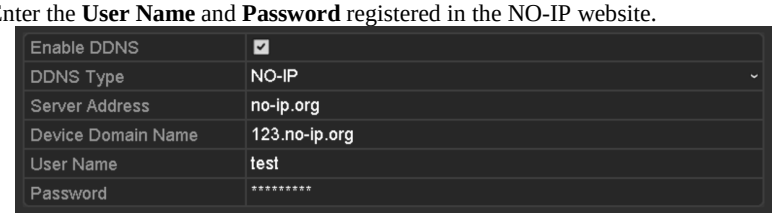


Figure 12. 7 NO-IP Settings Interface

- **HiDDNS:**

1) Select the continent/country of the server on which the device is registered.
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.

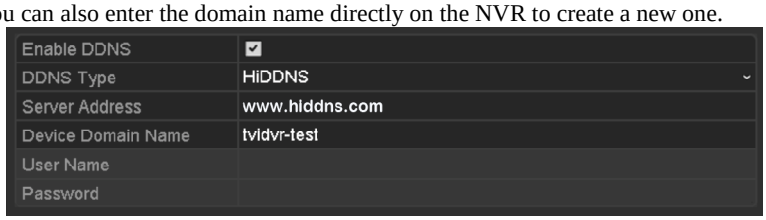


Figure 12. 8 HiDDNS Settings Interface

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

1) Go to the HiDDNS website: www.hiddns.com.
2) Click Register to register an account if you do not have one and use the account to log in.
3) In the Device Management interface, click Add to register the device.
4) Input **Device Serial No.**, **Device Domain (Device Name)** and **HTTP Port**. And click **OK** to add the device.

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

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

- **OPTION 1: Access the Device via Web Browser**

Open a web browser, and enter *http:// www.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*

NOTE

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** CMS

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.
Password: Enter the password of the device.

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

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

12.2.4 Configuring NTP Server

Purpose:
A Network Time Protocol (NTP) Server can be configured on your DVR 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.

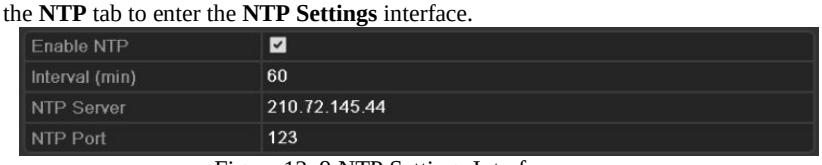


Figure 12. 9 NTP Settings Interface

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.

NOTE

The time synchronization interval can be set from 1 to 10080 minutes, and the default value is 60 minutes. If the DVR 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 DVR is set in a more customized network, NTP software can be used to establish a NTP server used for time synchronization.

12.2.5 Configuring NAT

Purpose:
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 **UPnP™ Settings** interface.

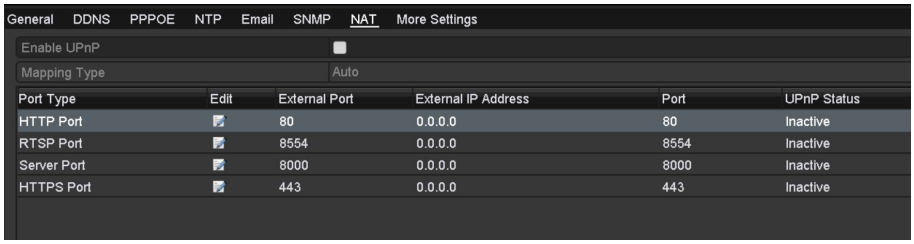


Figure 12. 10 UPnP™ Settings Interface

3. Check **Enable UPnP** 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.

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

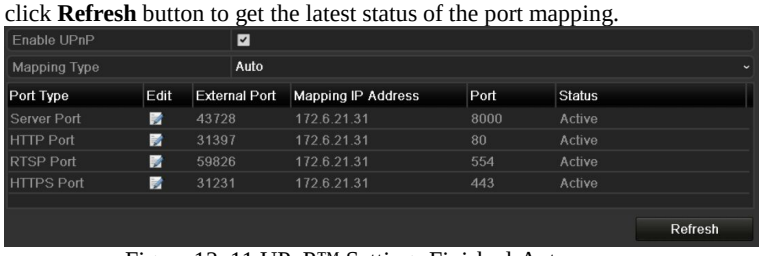


Figure 12. 11 UPnP™ Settings Finished-Auto

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) Click to activate the **External Port Settings** dialog box. Configure the external port No. for server port, http port and RTSP port respectively.

NOTE

- You can use the default port No., or change it according to actual requirements.
- External Port indicates the port No. for port mapping in the router.
- The value of the RTSP port No. should be 554 or between 1024 and 65535, while the value of the other ports should be between 1 and 65535 and the value must be different from each other. If multiple devices are configured for the UPnP™ settings under the same router, the value of the port No. for each device should be unique.

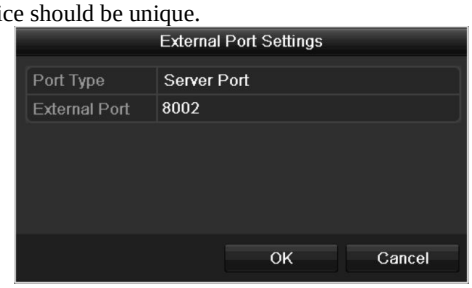


Figure 12. 12 External Port Settings Dialog Box

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

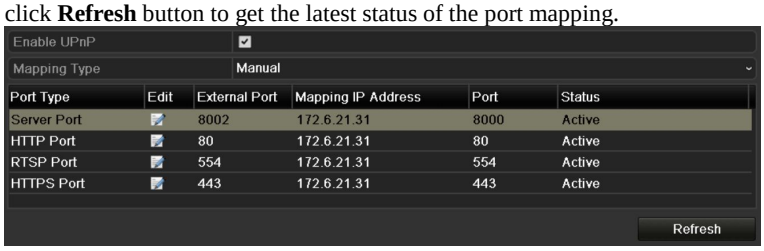


Figure 12. 13 UPnP™ Settings Finished-Manual

12.2.6 Configuring More Settings

Steps:

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

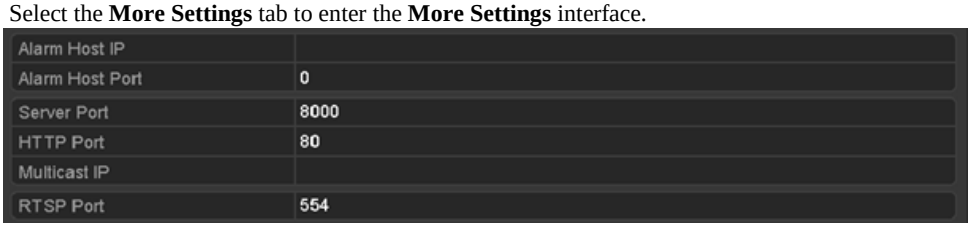


Figure 12. 14 More Settings Interface

3. Configure the remote alarm host, server port, HTTP port, multicast, and RTSP port.
   - **Alarm Host IP/Port**: With a remote alarm host configured, the device will send the alarm event or exception message to the host when an alarm is triggered. The remote alarm host must have the CMS (Client Management System) software installed.
     The **Alarm Host IP** refers to the IP address of the remote PC on which the CMS (Client Management System) software (e.g., NVMS7000) is installed, and the **Alarm Host Port** must be the same as the alarm monitoring port configured in the software (default port is 7200).
   - **Multicast IP**: The multicast can be configured to realize live view for more than the maximum number of cameras through network. 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.
     When adding a device to the CMS (Client Management System) software, the multicast address must be the same as the device's multicast IP.
   - **RTSP Port**: The RTSP (Real Time Streaming Protocol) is a network control protocol designed for use in entertainment and communications systems to control streaming media servers.
     Enter the RTSP port in the text field of **RTSP Port**. The default RTSP port is 554, and you can change it according to different requirements.
   - **Server Port** and **HTTP Port**: 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.

     NOTE
     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 IE access.

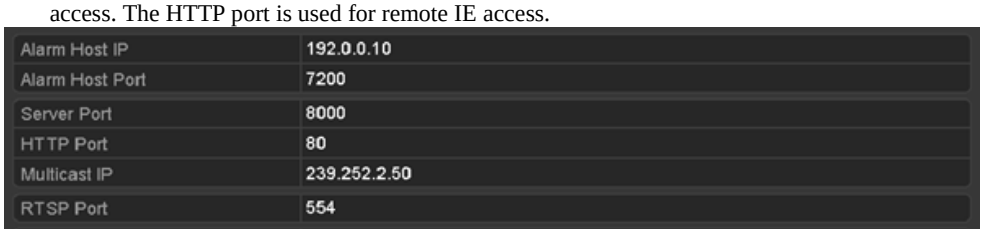


Figure 12. 15 Configure More Settings

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

12.2.7 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.

NOTE

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

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 12. 16 HTTPS Settings

OPTION 1: Create the self-signed certificate

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

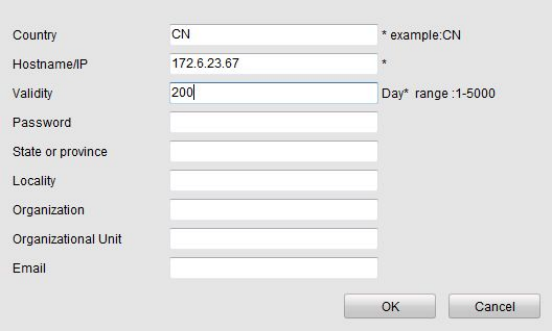


Figure 12. 17 Create Self-signed Certificate

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.

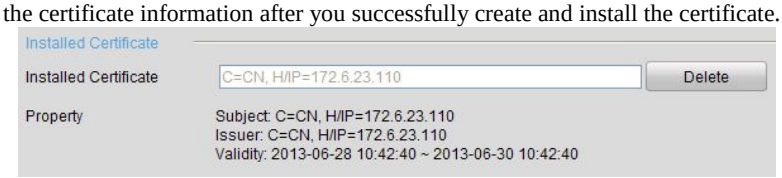


Figure 12. 18 Installed Certificate Property

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

12.2.8 Configuring Email

Purpose:

The system can be configured to send an Email notification to all designated users if an event is detected, e.g. an alarm or motion event is detected, etc.
Before configuring the Email settings, the DVR 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. Additional, the Preferred DNS server must be configured.
Before you start:
Make sure you have configured the IPv4 Address, IPv4 Subnet Mask, IPv4 Gateway and the Preferred DNS Server in the Network Settings menu. Please refer to *Chapter 12.1 Configuring General Settings* for detailed information.
Steps:

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

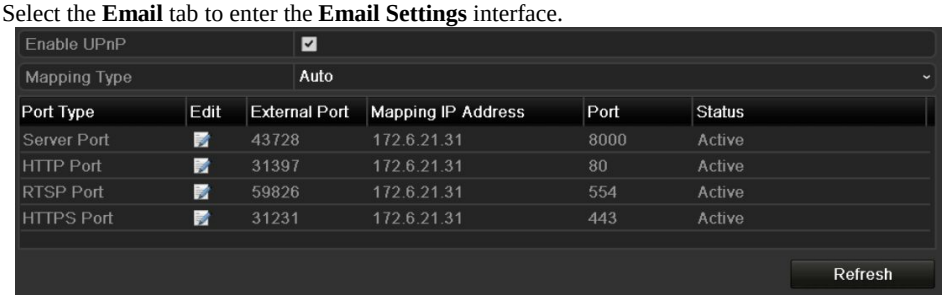


Figure 12. 19 Email Settings Interface

3. Configure the following Email settings:
   Enable Server Authentication (optional): Check the checkbox to enable the server authentication feature.
   User Name: The user account of sender's Email for SMTP server authentication.
   Password: The password of sender's Email for SMTP server authentication.
   SMTP Server: The SMTP Server IP address or host name (e.g., smtp.263xmail.com).
   SMTP Port: 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 the receiver of the Email.
   Receiver's Address: The Email address of the receiver.
   Enable Attached Pictures: Check the checkbox if you want to send email with attached alarm images. The interval is the time between two captures of the alarm images.

   NOTE

   - For the IP cameras, the alarm images are directly sent as the attached pictures by Email. Up to one picture can be sent for one IP camera. The attached pictures of the linked cameras cannot be sent.
   - For analog cameras, 3 attached pictures can be sent for one analog camera when the alarm is triggered.

   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.
4. Click the **Apply** button to save the Email settings.
5. You can click the **Test** button to test whether your Email settings work. The corresponding Attention message box pops up.

12.3 Checking Network Traffic

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

1. Enter the **Network Traffic** interface.
   Menu > Maintenance > Net Detect

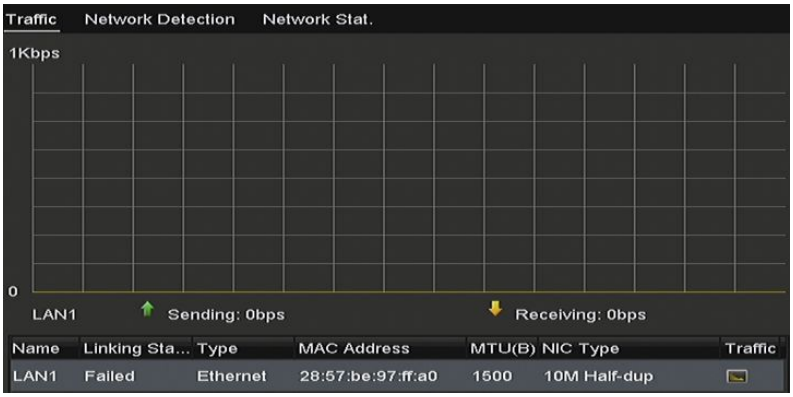


Figure 12. 20 Network Traffic Interface

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

12.4 Configuring Network Detection

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

12.4.1 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** interface.

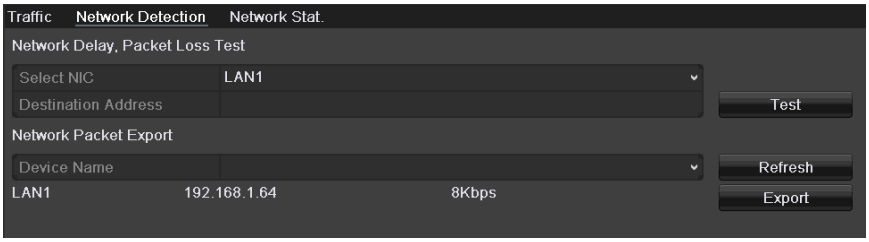


Figure 12. 21 Network Detection Interface

3. Select a NIC to test network delay and packet loss.
4. Enter the destination address in the text field of **Destination Address**.
5. Click the **Test** button to start testing network delay and packet loss.

12.4.2 Exporting Network Packet

Purpose:
By connecting the DVR to network, the captured network data packet can be exported to USB-flash disk, SATA 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**.

   NOTE
   Click the **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 DVR. You can format the backup device if the format is incorrect.

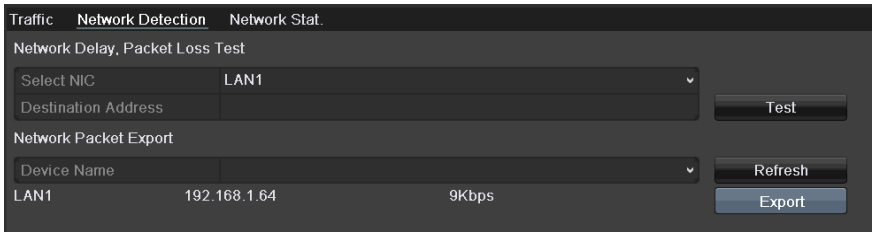


Figure 12. 22 Export Network Packet

4. Click the **Export** button to start exporting.
5. After the exporting is complete, click **OK** to finish the packet export.

NOTE
Up to 1M data can be exported each time.

12.4.3 Checking Network Status

Purpose:

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

Steps:

1. Enter the Network Traffic interface.
   Menu > Maintenance > Net Detect
2. Click the **Network Detection** tab to enter the **Network Detection** interface.
3. Click **Status** on the right bottom of the interface.

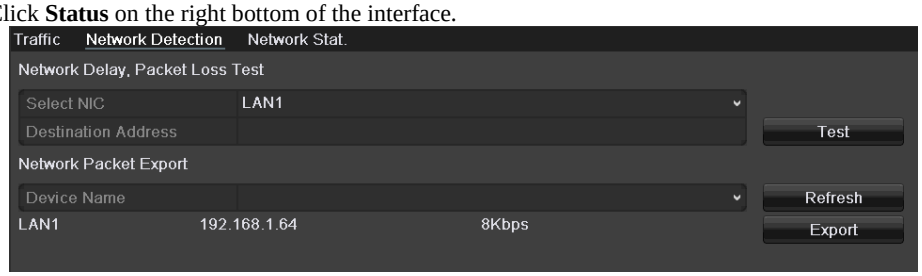


Figure 12. 23 Checking Network Status

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

Figure 12. 24 Network Status Checking Result

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

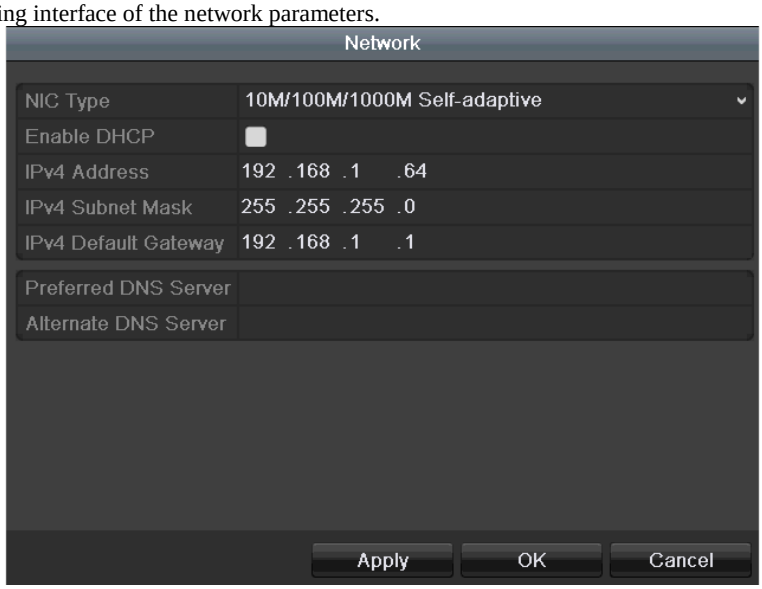


Figure 12. 25 Network Parameters Configuration

12.4.4 Checking Network Statistics

Purpose:

You can check the network statistics to obtain the real-time information of the device.

Steps:

1. Enter the **Network Statistics** interface.
   Menu > Maintenance> Net Detect

2. Click the **Network Stat.** tab to enter the **Network Statistics** interface.

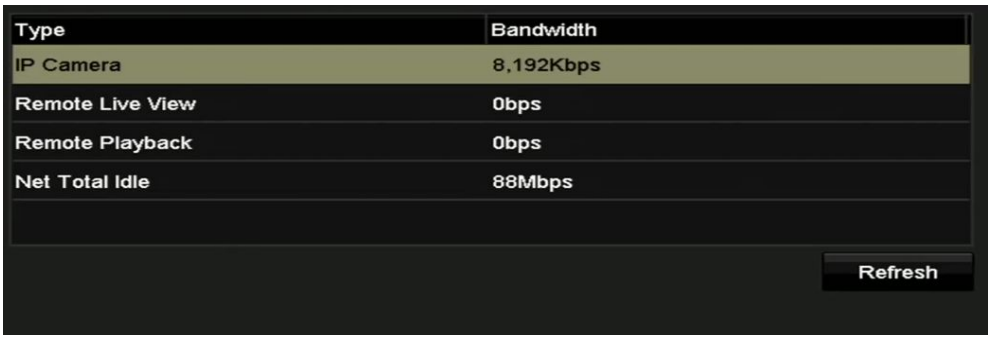


Figure 12. 26 Network Stat. Interface

3. View the bandwidth of Remote Live View, bandwidth of Remote Playback, and bandwidth of Net Total Idle.
4. Click **Refresh** button to get the latest bandwidth statistics.

Chapter 13 HDD Management

13.1 Initializing HDDs

Purpose:
A newly installed hard disk drive (HDD) must be initialized before it can be used with your DVR.
Steps:

1. Enter the **HDD Information** interface.
   Menu > HDD > General

Figure 13. 1 HDD Information Interface

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

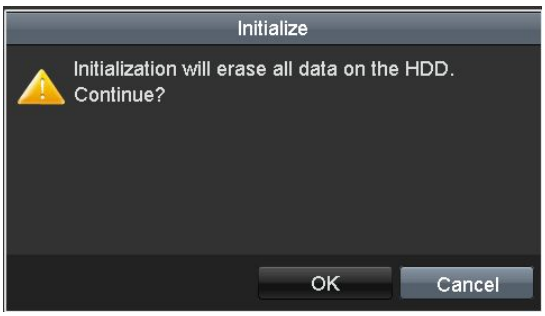


Figure 13. 2 Confirm Initialization

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

Figure 13. 3 Start Initialization

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

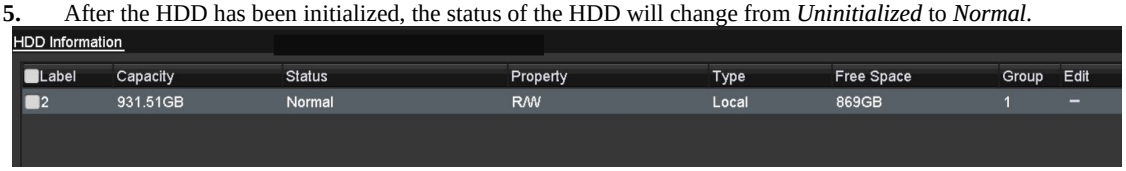


Figure 13. 4 HDD Status Changes to Normal

NOTE

Initializing the HDD will erase all data on it.

The HDDs which are free of working for a long time can be enabled to sleep, thus to decrease the power consumption of the device and extend the life of the HDDs.
Click Menu > HDD > Advanced.

Figure 13. 5 Enable HDD Sleeping

Check the checkbox of **Enable HDD Sleeping** (by default), and the HDDs which are free of working for a long time will be set to sleep.
Uncheck the checkbox of **Enable HDD Sleeping**, and the HDDs will be set to work for all time.

13.2 Managing Network HDD

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

1. Enter the HDD Information interface.
Menu > HDD>General

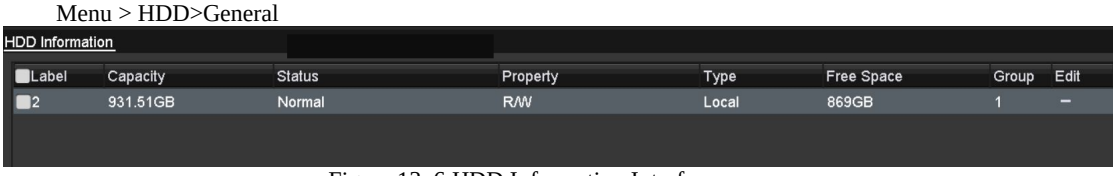


Figure 13. 6 HDD Information Interface

2. Click the **Add** button to enter the **Add NetHDD** interface, as shown in Figure 13. 7.

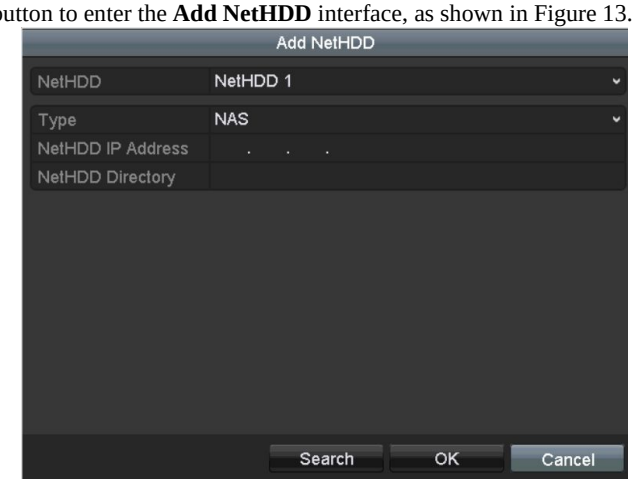


Figure 13. 7 HDD Information Interface

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) Click **Search** to search the available NAS disks.
  3) Select the NAS disk from the list shown below.
     Or you can just manually enter the directory in the text field of **NetHDD Directory**.
  4) Click **OK** to add the configured NAS disk.

  NOTE
  Up to 8 NAS disks can be added.

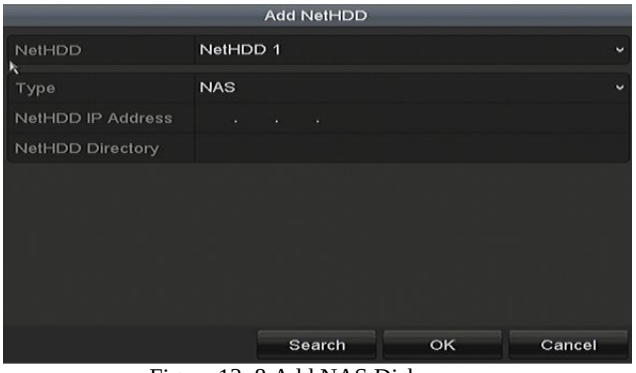


Figure 13. 8 Add NAS Disk

- **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 8 IP SAN disks can be added.

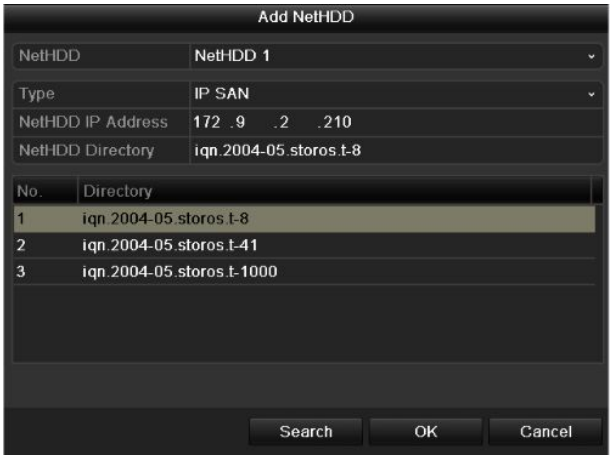


Figure 13. 9 Add IP SAN Disk

5) 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.

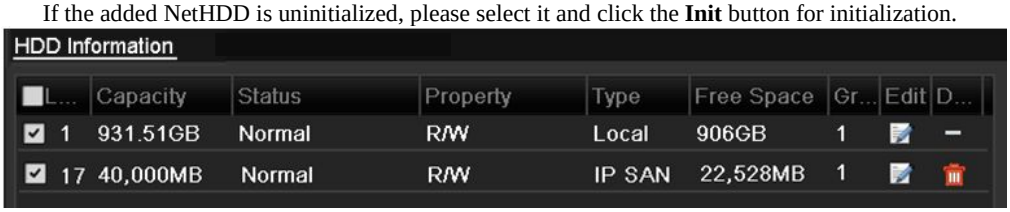


Figure 13. 10 Initialize Added NetHDD

13.3 Managing HDD Group

13.3.1 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 13. 11.

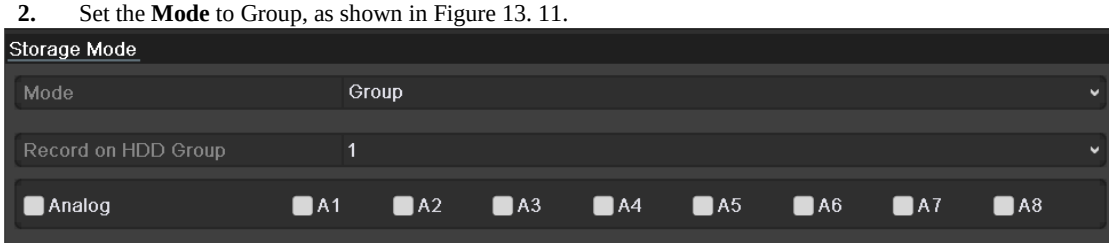


Figure 13. 11 Storage Mode Interface

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

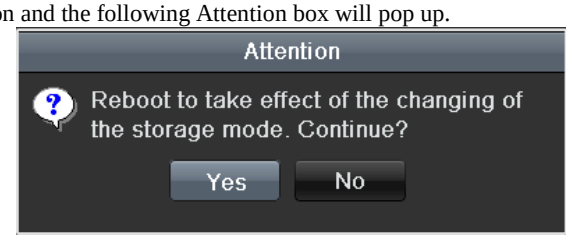


Figure 13. 12 Attention for Reboot

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 the icon to enter the **Local HDD Settings** interface, as shown in Figure 13. 13.

Figure 13. 13 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.

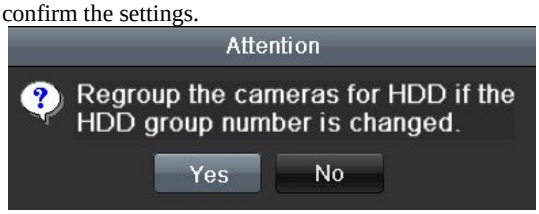


Figure 13. 14 Confirm HDD Group Settings

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

13.3.2 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 13.3.1 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 13. 15.

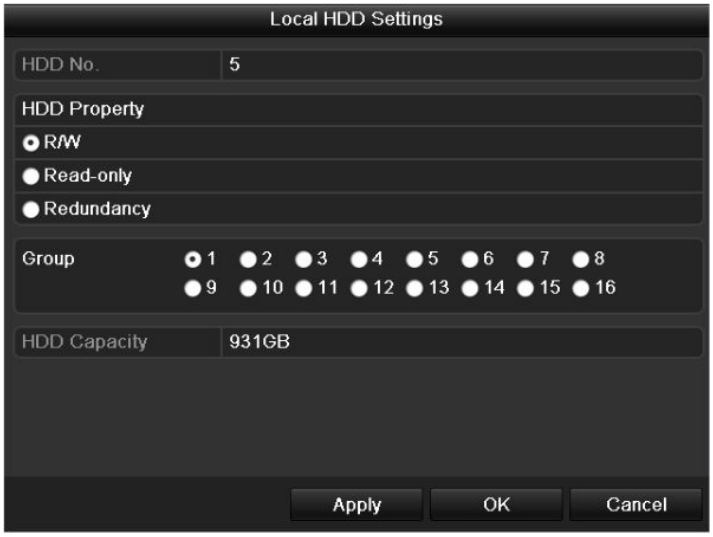


Figure 13. 15 Set HDD Property

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 added on your DVR when you want to set a HDD to Redundancy, and there is one HDD with R/W property.

13.4 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 13. 16.

NOTE

The DVR must be rebooted to enable the changes to take effect.

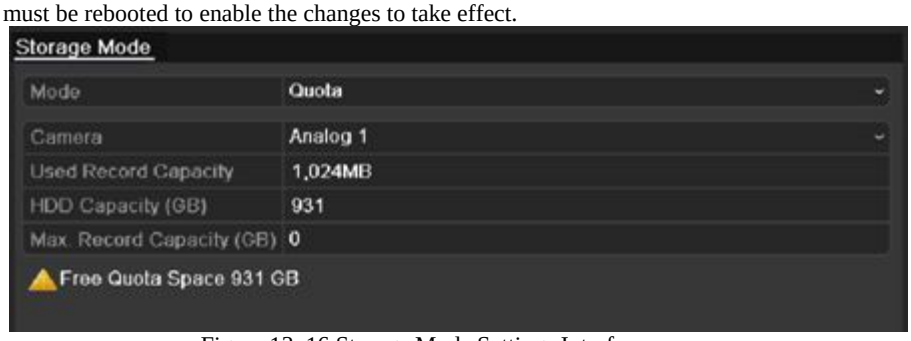


Figure 13. 16 Storage Mode Settings Interface

3. Select a camera for which you want to configure quota.
4. Enter the storage capacity in the text field of **Max. Record Capacity (GB)**.
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** interface, as shown in Figure 13. 17.

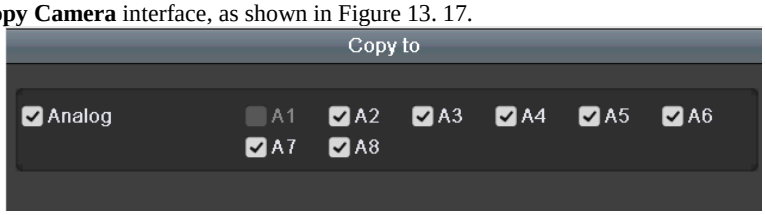


Figure 13. 17 Copy Settings to Other Camera(s)

6. Select the camera (s) to be configured with the same quota settings. You can also click the checkbox of Analog 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.

13.5 Configuring Cloud Storage

Purpose

The Cloud storage facilitates you to upload and download the recorded files at any time and any place, which can highly enhance the efficiency.

Steps

1. Enter the Cloud Storage interface
   Menu > HDD > General > Cloud Storage
2. Check the **Enable Cloud** checkbox to enable the feature.
3. Select the Cloud Type from the dropdown list to One Drive, Google Drive or Drop Box.
4. According to the prompts, you are required to use a mobile browser to scan the QR code to log in the selected cloud to get the authentication code. And then copy the authentication code to the **Authentication Code** text filed.
5. Click **Apply** and then back to the main menu.
6. Enter the cloud storage interface again about 20s later. When the **Status** shows online, it indicates the successful registration.
7. Configure the recording schedule.
   Back to enter the record interface, choose a certain camera from the **Camera** dropdown list and check the **Enable Schedule** checkbox to enable the schedule recording. For detailed recording schedule, refer to 5.2 Configuring Recording Schedule.

NOTE

This POS recording is supported by some DVRs only.

8. Upload the event triggered recording files to the cloud storage.
   1) Back to enter the cloud storage interface, and select the camera you have set in the recording schedule interface.
   2) Select the in the **Upload Type** text filed.
   3) Check the **Enable Event Upload** check box.
   4) Click **Apply** to finish the settings.

NOTE

- Only the sub-stream recorded files can be uploaded the Cloud Storage.
- Please configure the event triggered recording schedule and enable the corresponding event type.

9. (Optional) You can click the **Copy** button to copy the cloud storage settings to other cameras. You can also click the checkbox of Analog/IP Camera to select all cameras.
   Click **OK** button to back to the cloud storage interface and click **Apply** to finish the settings.

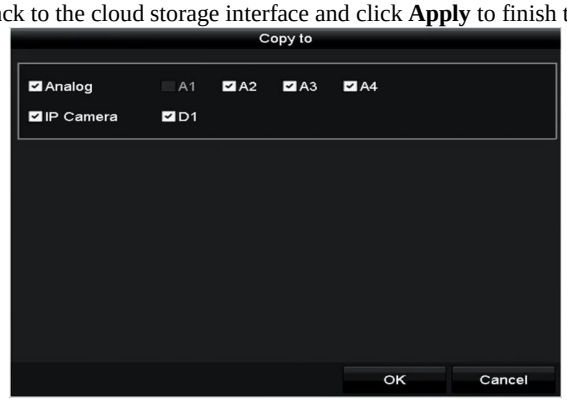


Figure 13. 18 Copy to Interface

13.6 Checking HDD Status

Purpose:
You may check the status of the installed HDDs on DVR 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 13. 19.

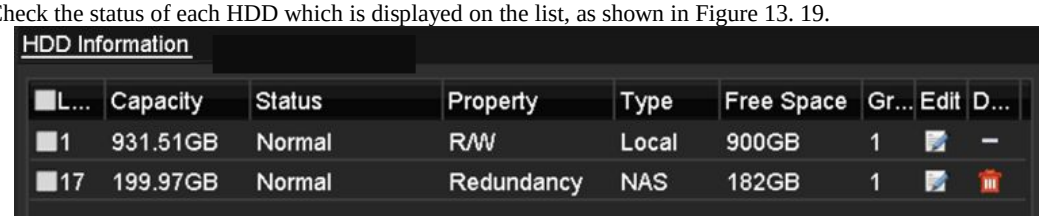


Figure 13. 19 View HDD Status (1)

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 System 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 13. 20.

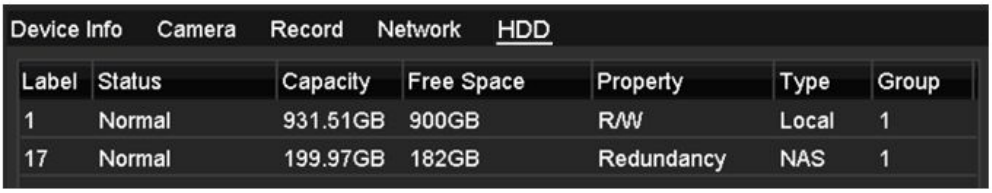


Figure 13. 20 View HDD Status (2)

13.7 Checking S.M.A.R.T Information

Purpose:
The S.M.A.R.T. *(*Self-Monitoring, Analysis and Reporting Technology*)* is a monitoring system for HDD to detect *a*nd report on various indicators of reliability in the hopes of anticipating failures.
Steps:

1. Enter the **HDD Detect** interface.
   Menu > Maintenance > HDD Detect
2. Click the **S.M.A.R.T. Settings** tab to enter the interface.
3. Select the HDD to view its S.M.A.R.T. information list, as shown in Figure 13. 21.

NOTE

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

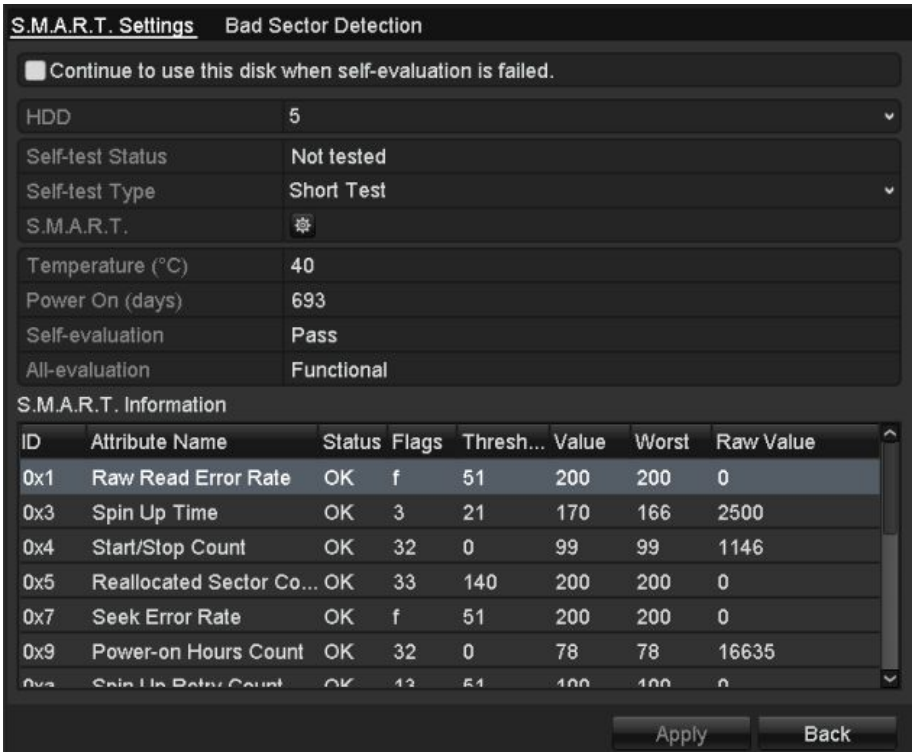


Figure 13. 21 S.M.A.R.T Settings Interface

13.8 Detecting Bad Sector

Purpose:
You can detect the bad sector of the HDD to check the status of the HDD.
Steps:

1. Enter the **HDD Detect** interface.
   Menu>HDD>HDD Detect
2. Click the **Bad Sector Detection** tab to enter the interface.
3. Select a HDD and click the **Detect** button to start detecting.

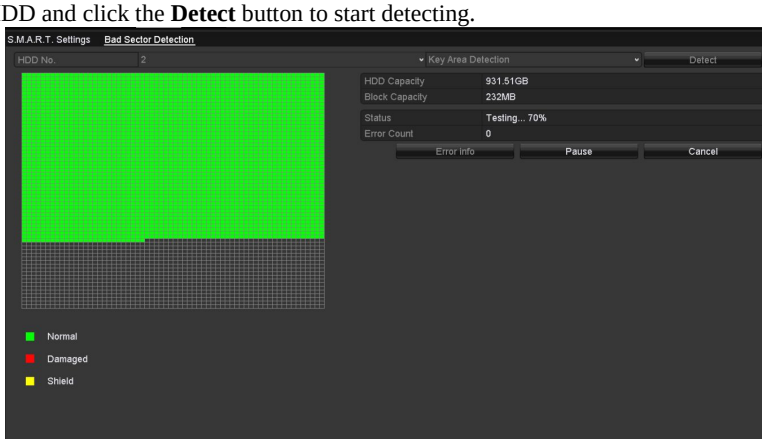


Figure 13. 22 Bad Sector Detecting

4. You can click the **Pause** button to pause the detection and click the **Resume** button to resume the detection.
5. If there is error information about the HDD, you can click the **Error Info** button to view the information.

13.9 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. Check the checkbox(s) below to select the linkage action(s) for HDD error, as shown in Figure 12.22. The linkage actions can be selected to: Audible Warning, Notify Surveillance Center, Send Email and Trigger Alarm Output.

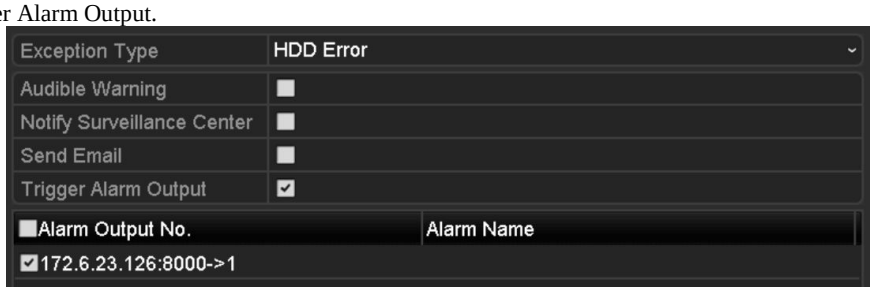


Figure 13. 23 Configure HDD Error Alarm

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 14 Camera Settings

14.1 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 checking the checkbox.
5. Select the Date Format, Time Format, Display Mode and the OSD font.

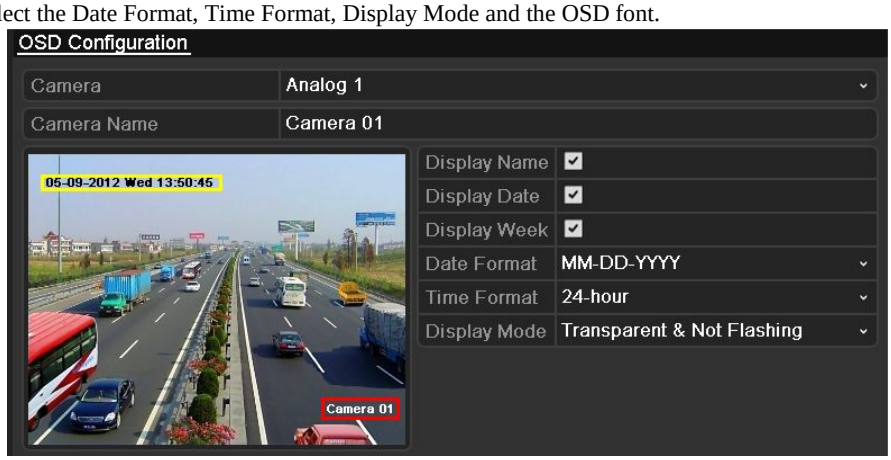


Figure 14. 1 OSD Configuration Interface

---

6. You can use the mouse to drag the text frame on the preview window to adjust the OSD position.
7. Copy Camera Settings
   1) If you want to copy the OSD settings of the current camera to other cameras, click the **Copy** button to enter the **Copy Camera** interface, as shown in Figure 14. 2.

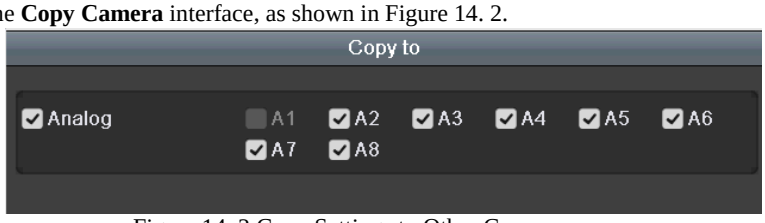


Figure 14. 2 Copy Settings to Other Cameras

---

   2) Select the camera (s) to be configured with the same OSD settings. You can also check the checkbox of **Analog** to select all cameras.
   3) Click the **OK** button to finish the **Copy** settings and back to the **OSD Configuration** interface.
8. Click the **Apply** button to apply the settings.

14.2 Configuring Privacy Mask

Purpose:
You are allowed to configure the four-sided privacy mask zones that cannot be viewed or recorded by the operator.
Steps:

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

Figure 14. 3 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 mask zones can be configured, and the size of each area can be adjusted.

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

Figure 14. 4 Set Privacy Mask Area

6. You can click the **Copy** button to copy the privacy mask settings of the current camera to other cameras. Please refer to step 7 of *Chapter 14.1 Configuring OSD Settings*.
7. Click the **Apply** button to save the settings.

14.3 Configuring Video Parameters

Steps:

1. Enter the Image Settings interface.
   Menu > Camera > Image

Figure 14. 5 Image Settings Interface (Analog Camera)

2. Select the camera to set image parameters.
3. Two periods for different image settings are provided, select the period name in the dropdown list.

NOTE

The time periods cannot be overlapped with each other.

4. Select the mode from the drop-down list of **Mode**, there are four modes selectable for the analog cameras: Standard, Indoor, Dim Light and Outdoor.
5. Adjust the image parameters according to actual needs. The parameters include Brightness, Contrast, Saturation, Hue, Sharpness and Denoising for the analog cameras. You can also click **Restore** to set the parameters to the default settings.
6. You can click **Copy** to copy the image settings of the current camera to other analog cameras.
7. Click **Apply** to save the settings.

Chapter 15 DVR Management and Maintenance

15.1 Viewing System Information

Steps:

1. Enter the **System Information** interface.
   Menu > Maintenance > System Info
2. You can click the **Device Info**, **Camera**, **Record**, **Alarm**, **Network** and **HDD** tabs to view the system information of the device.

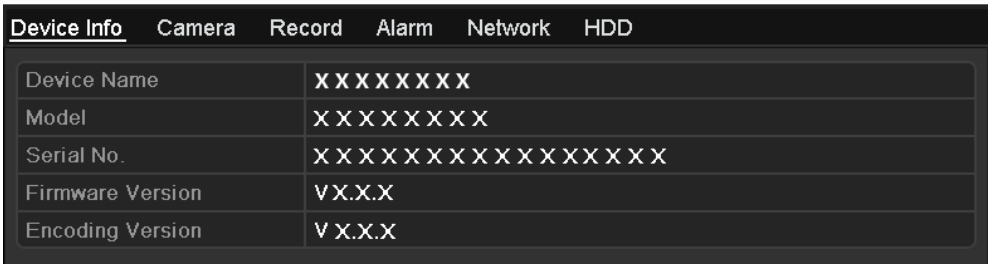


Figure 15. 1 System Information Interface

NOTE

- This alarm information is not available for the DVR without Alarm.
- You can view the hardware version in the **Device Information** interface.

15.2 Searching Log Files

Purpose:

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

Steps:

1. Enter the **Log Search** interface.
   Menu > Maintenance > Log Information

Figure 15. 2 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.

NOTE Up to 2000 log files can be displayed each time.

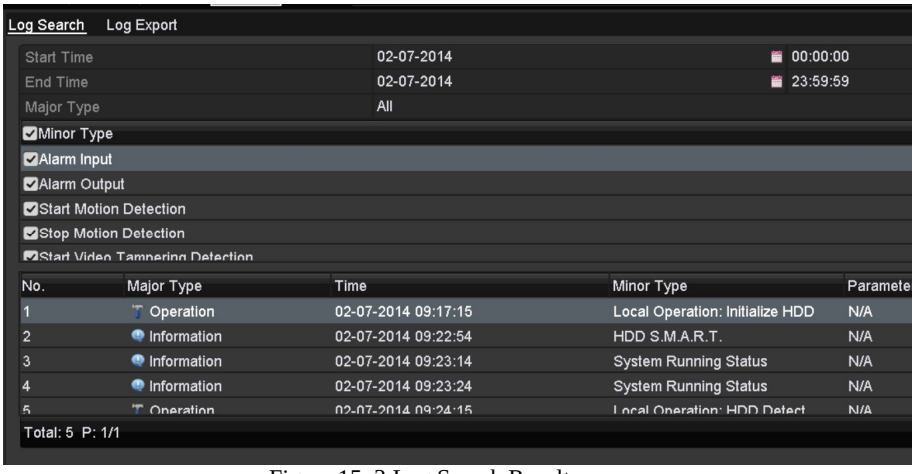


Figure 15. 3 Log Search Results

5. You can click the button of each log or double-click it to view its detailed information. And you can also click the button to view the related video files if available.
6. If you want to export the log files, click the **Export** button to enter the Export menu, as shown in Figure 14.5.

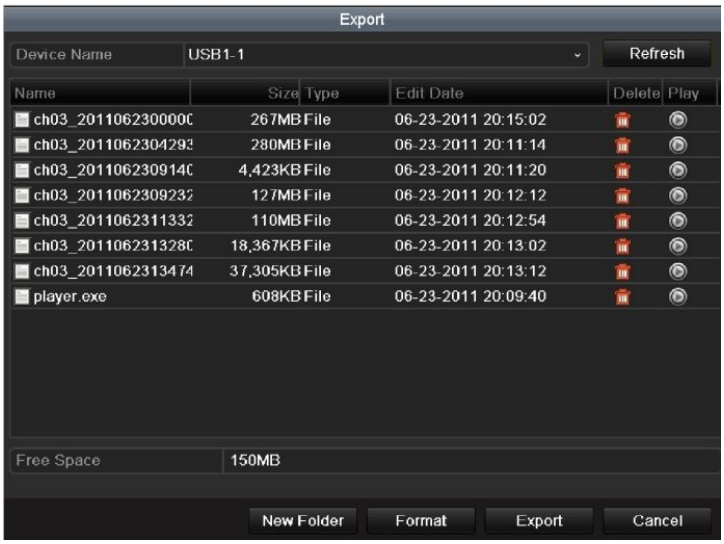


Figure 15. 4 Export Log Files

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.

NOTE

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

15.3 Importing/Exporting IP Camera Info

Purpose:
The information of added IP camera can be generated into an excel file and exported to the local device for backup, including the IP address, manage port, password of admin, etc. And the exported file can be edited on your PC, like adding or deleting the content, and copy the setting to other devices by importing the excel file to it.
Steps:

1. Enter the camera management interface.
   Menu > Camera > Camera
   Click the **IP Camera Import/Export** tab, the content of detected plugged external device appears.
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 importing process is completed, you must reboot the DVR.

15.4 Importing/Exporting Configuration Files

Purpose:
The configuration files of the DVR can be exported to local device for backup; and the configuration files of one DVR can be imported to multiple DVR devices if they are to be configured with the same parameters.
Steps:
1. Enter the **Import/Export Configuration File** interface.
   Menu > Maintenance > Import/Export
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 DVR.

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

15.5 Upgrading System

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

15.5.1 Upgrading by Local Backup Device

Steps:
1. Connect your DVR 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** interface, as shown in Figure 14.7.

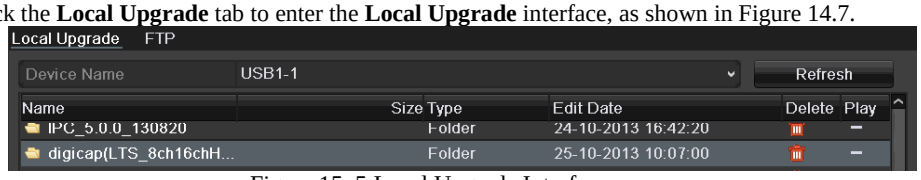


Figure 15. 5 Local Upgrade Interface

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 DVR to activate the new firmware.

15.5.2 Upgrading by FTP

Before you start:
Configure PC (running FTP server) and DVR 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 14.8.

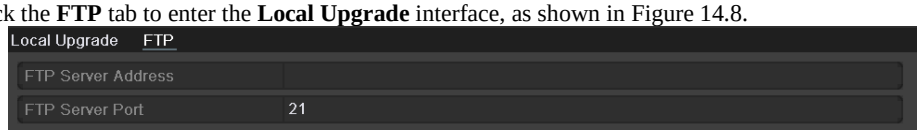


Figure 15. 6 FTP Upgrade Interface

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 DVR to activate the new firmware.

15.6 Restoring Default Settings

Steps:

1. Enter the **Default** interface.
   Menu > Maintenance > Default

Figure 15. 7 Restore Defaults

2. Select the restoring type from the following three options.
   Restore Defaults: Restore all parameters, except the network (including IP address, subnet mask, gateway, MTU, NIC working mode, default route, server port, etc.) and user account parameters, to the factory default settings.
   Factory Defaults: Restore all parameters to the factory default settings.
   Restore to Inactive: Restore the device to the inactive status.
3. Click the **OK** button to restore the default settings.

NOTE

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

Chapter 16 Others

16.1 Configuring General Settings

Purpose:
You can configure the output resolution, system time, mouse pointer speed, etc.
Steps:

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

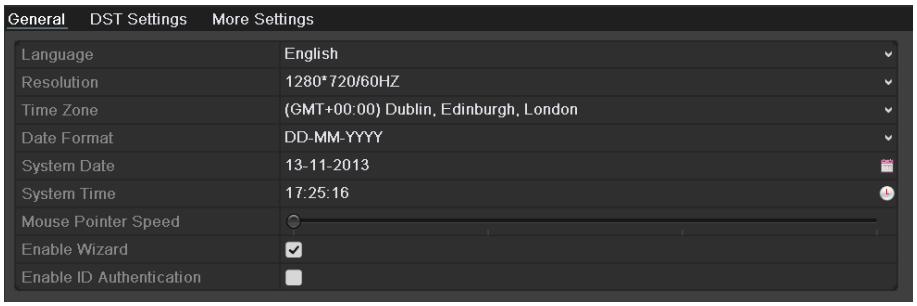


Figure 16. 1 General Settings Interface

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

16.2 Configuring DST Settings

Steps:

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

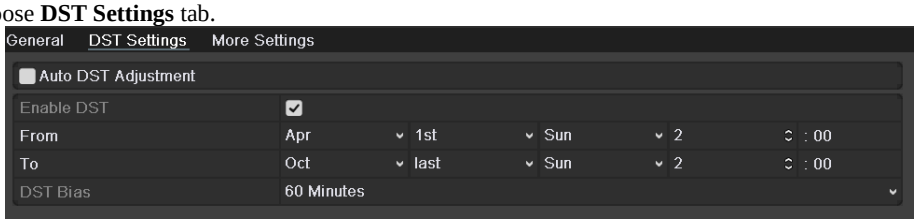


Figure 16. 2 DST Settings Interface

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.

16.3 Configuring More Settings

Steps:

1. Enter the General Settings interface.
   Menu > Configuration > General
2. Click the **More Settings** tab to enter the **More Settings** interface, as shown in Figure 15.3.

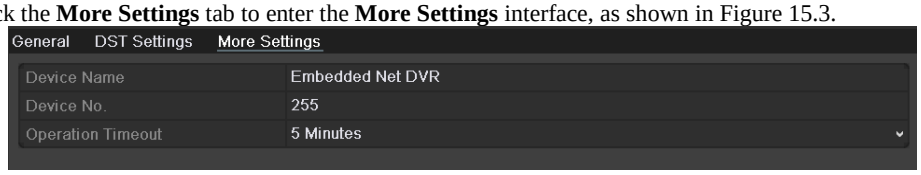


Figure 16. 3 More Settings Interface

3. Configure the following settings:
   - **Device Name:** Edit the name of DVR.
   - **Device No.:** Edit the serial number of DVR. The Device No. can be set in the range of 1~255, and the default No. is 255.
   - **CVBS Output Brightness:** Adjust the video output brightness via the CVBS interface.
   - **Auto Logout:** 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.
   - **Main CVBS Scaling:** You can check the checkbox to enable main CVBS scaling.
4. Click the **Apply** button to save the settings.

16.4 Managing User Accounts

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

16.4.1 Adding a User

Steps:

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

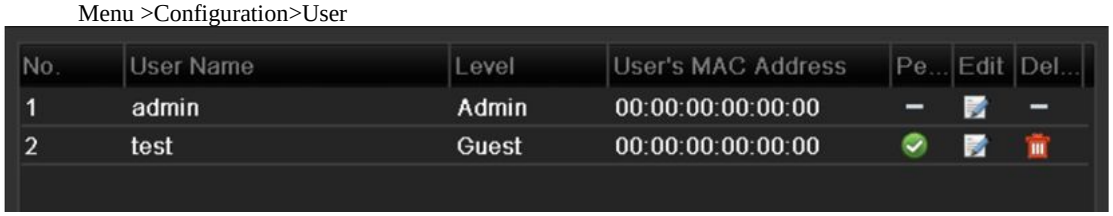


Figure 16. 4 User Management Interface

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

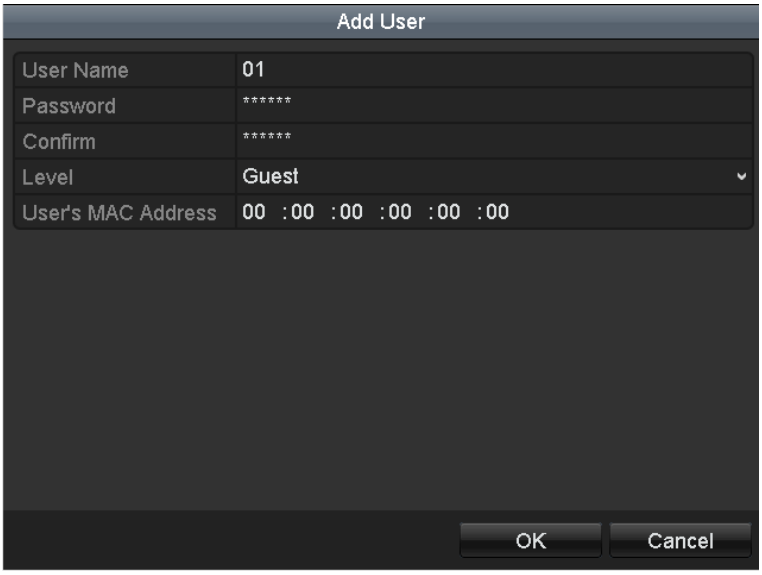


Figure 16. 5 Add User Menu

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

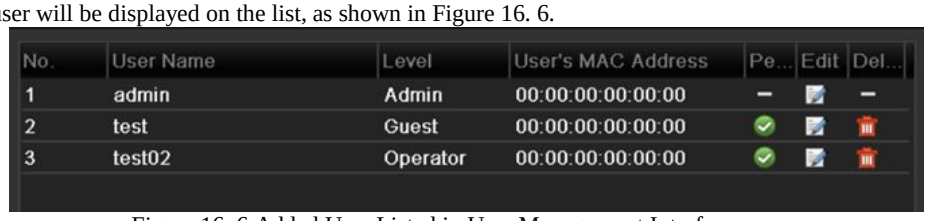
   STRONG PASSWORD RECOMMENDED– *We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password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

   Level: Set the user level to Operator or Guest. Different user levels have different operating permission.
   - **Operator:** The *Operator* user level has permission of Two-way Audio in Remote Configuration and all operating permission in Camera Configuration by default.
   - **Guest:** The *Guest* user has no permission of Two-way Audio in Remote Configuration and only has the local/remote playback in the Camera Configuration by default.

   User's MAC Address: The MAC address of the remote PC which logs onto the DVR. If it is configured and

enabled, it only allows the remote user with this MAC address to access the DVR.

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 16. 6.



No.	User Name	Level	User's MAC Address	Pe...	Edit	Del...
1	admin	Admin	00:00:00:00:00:00	–		–
2	test	Guest	00:00:00:00:00:00			
3	test02	Operator	00:00:00:00:00:00			

Figure 16. 6 Added User Listed in User Management Interface

5. You can assign permissions for the added user.
   1) Select the user from the list and then click to enter the **Permission Settings** interface, as shown in Figure 16. 7.

Figure 16. 7 User Permission Settings Interface

   2) 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 device.
- Local Parameters Settings: Configuring parameters, restoring factory default parameters and importing/exporting configuration files.
- Local Camera Management: Enabling and disabling analog camera (s). Adding, deleting and editing of network camera (s). This function is supported by HDVR series.
- Local Advanced Operation: Operating HDD management (initializing HDD, setting HDD property), upgrading system firmware.
- Local Shutdown /Reboot: Shutting down or rebooting the device.

Remote Configuration

- Remote Log Search: Remotely viewing logs that are saved on the device.
- Remote Parameters Settings: Remotely configuring parameters, restoring factory default parameters and importing/exporting configuration files.
- Remote Camera Management: Remotely enabling and disabling analog camera (s), and adding, deleting and editing of network camera (s). This function is supported by HDVR series.
- Remote Serial Port Control: Configuring settings for RS-485 port.
- Remote Video Output Control: Sending remote control panel signal.
- Two-way Audio: Realizing two-way radio between the remote client and the device.
- 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.

- Remote Shutdown/Reboot: Remotely shutting down or rebooting the device.

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).

NOTE

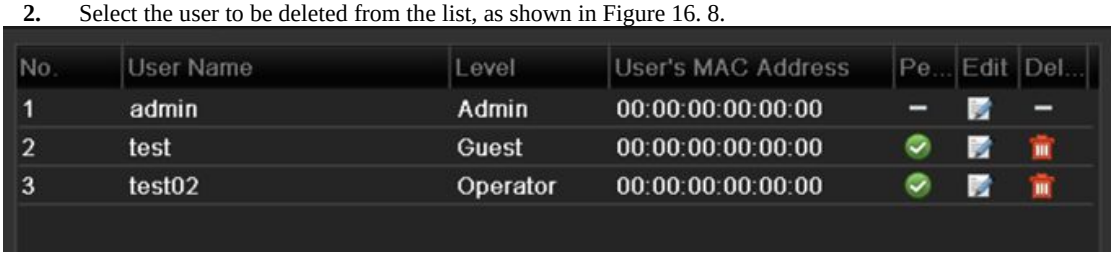
Local Camera Management is provided for the IP cameras only.

3) Click **OK** to save the settings and exit.

16.4.2 Deleting a User

Steps:

1. Enter the **User Management** interface.
   Menu >Configuration>User
2. Select the user to be deleted from the list, as shown in Figure 16. 8.



No.	User Name	Level	User's MAC Address	Pe...	Edit	Del...
1	admin	Admin	00:00:00:00:00:00	–		–
2	test	Guest	00:00:00:00:00:00			
3	test02	Operator	00:00:00:00:00:00			

Figure 16. 8 User List

3. Click to delete the selected user account.

16.4.3 Editing a User

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

Steps:

1. Enter the **User Management** interface.
   Menu >Configuration>User
2. Select the user to be edited from the list, as shown in Figure 16. 8.
3. Click the icon to enter the **Edit User** interface, as shown in Figure 16. 9.

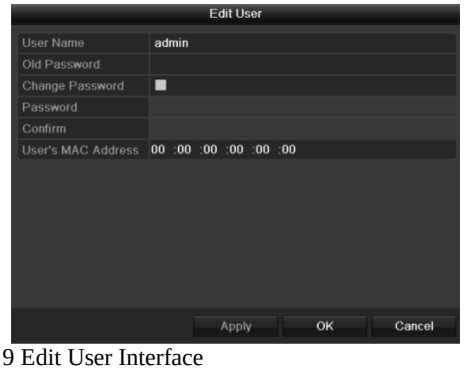


Figure 16. 9 Edit User Interface

4. Edit the corresponding parameters.

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

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

5. Click the **OK** button to save the settings and exit the menu.

6. For the **Operator** or **Guest** user account, you can also click the button on the **User Management** interface to edit the permission.

Chapter 17 Appendix

17.1 Glossary

- **Dual Stream:** Dual stream is a technology used to record high resolution video locally while transmitting a lower resolution stream over the network. The two streams are generated by the DVR, with the main stream having a maximum resolution of 1080P and the sub-stream having a maximum resolution of CIF.
- **DVR:** Acronym for Digital Video Recorder. A DVR is device that is able to accept video signals from analog cameras, compress the signal and store it on its hard drives.
- **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 televisions 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.

17.2 Troubleshooting

- **No image displayed on the monitor after the device is 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 DVR is HDMI output, then the input mode of monitor must be the HDMI input). And if not, please modify the input mode of monitor.

  4. Check if the fault is solved by the step 1 to step 3.

  If it is solved, finish the process.

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

- **There is a beep sound after a new bought device 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 device or is broken-down.

  Steps:

  1. Verify at least one HDD is installed in the device.

  1) If not, please install the compatible HDD.

  NOTE

  Please refer to the “Quick Operation Guide” for the HDD installation steps.

  2) If you do not 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 from our company to do the further process.

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

  Possible Reasons:

  a) The frame rate has not reached the real-time frame rate.

  Steps:

1. Check the parameters of Main Stream (Continuous) 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 (Continuous).
2. Verify the frame rate is real-time frame rate.

   Select “Menu > Record > Parameters > Record”, and set the Frame Rate to Full Frame.
3. Check if the fault is solved by the above steps.

   If it is solved, finish the process.

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

- **When using the device 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 camera is not connected well; impedance mismatches or incompatible.

  b) The stream type is not set as “Video & Audio”.

  Steps:

  1. Verify the cable between the pickup and camera is connected well; impedance matches and compatible.
  2. Verify the setting parameters are correct.

     Select “Menu > Record > Parameters > Record”, and set the Stream Type as “Audio & Video”.
  3. Check if the fault is solved by the above steps.

     If it is solved, finish the process.

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

- **The image gets stuck when DVR is playing back by single or multi-channel cameras.**

  Possible Reasons:

  a) The frame rate is not the real-time frame rate.

  b) The DVR 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 frame rate is real-time frame rate.

     Select “Menu > Record > Parameters > Record”, and set the Frame Rate to “Full Frame”.
  2. 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.
  3. Reduce the number of local playback channel.

     Select “Menu > Playback”, and uncheck the checkbox of unnecessary channels.
  4. Check if the fault is solved by the above steps.

     If it is solved, finish the process.

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

- **No record file found in the device local HDD, and the prompt “No record file found” pops up when you search the record files.**

  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 “System Time” is correct.
  2. Verify the search condition is correct.

     Select “Playback”, and verify the channel and time are correct.

3. Verify the HDD status is normal.

Select “Menu > HDD > General” to view the HDD status, and verify the HDD is detected and can be read and written normally.

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

If it is solved, finish the process.

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