

Network Video Recorder

User Manual

About this Manual

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

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 RESPONSIBILITIES 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 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 (B)/NMB-3(B) 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 100~240 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 manufacturer.

Thank you for purchasing our product. If there is any question or request, please do not hesitate to contact dealer.
The figures in the manual are for reference only.

Product Key Features

General

- Connectable to network cameras, network dome and encoders.
- Connectable to the third-party network cameras like ACTI, Arecont, AXIS, Bosch, Brickcom, Canon, PANASONIC, Pelco, SAMSUNG, SANYO, SONY, Vivotek and ZAVIO, and cameras that adopt ONVIF or PSIA protocol.
- Connectable to the smart IP cameras.
- PAL/NTSC adaptive video inputs.
- Each channel supports dual-stream.
- Up to 32 network cameras can be connected for VN4016 series NVR;
- Independent configuration for each channel, including resolution, frame rate, bit rate, image quality, etc.
- The quality of the input and output record is configurable.

Local Monitoring

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

HDD Management

- For VN4016 series, 4 SATA hard disks can be connected;
- Each disk with a maximum of 6TB storage capacity
- 8 network disks (NAS /IP SAN disks) can be connected.
- Support S.M.A.R.T. and bad sector detection.
- HDD group management.
- Support HDD standby function.
- HDD property: redundancy, read-only, read/write (R/W).
- HDD quota management; different capacity can be assigned to different channel.

Recording and Playback

- Holiday recording schedule configuration.
- Continuous and event video recording parameters.
- Multiple recording types: manual, continuous, alarm, motion, motion | alarm, motion & alarm, and VCA.
- 8 recording time periods with separated recording types each day.
- Pre-record and post-record for alarm, motion detection for recording, and pre-record time for schedule and manual recording.
- Searching record files by events (alarm input/motion detection/VCA).
- Playback by sub-periods.
- Tag adding for record files, searching and playing back by tags.
- Locking and unlocking record files.

- Local redundant recording.
- Provide new playback interface with easy and flexible operation.
- Searching and playing back record files by camera No., recording type, start time, end time, etc.
- Smart search for the selected area in the video.
- Zooming in when playback.
- Reverse playback of multi-channel.
- Supports pause, play reverse, speed up, speed down, skip forward, and skip backward when playback, and locating by dragging the mouse.
- Up to 4/8/16-ch synchronous playback.
- Support enabling H.264+ to ensure high video quality with lowered bitrate.

Backup

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

Alarm and Exception

- Configurable arming time of alarm input/output.
- Alarm for video loss, motion detection, VCA, video tampering, HDD full, HDD error, network disconnected, IP conflict, illegal login, abnormal record, and PoE power overload (for the models support PoE interfaces only), etc.
- Alarm triggers full screen monitoring, audio alarm, notifying surveillance center, sending email and alarm output.
- Automatic restore when system is abnormal.
- Support VCA detection alarm and VCA search.

Other Local Functions

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

Network Functions

- The dual-NIC network 10 /100/1000 Mbps self-adaptive Ethernet interfaces are provided
- 1 self-adaptive 10M/100M/1000M network interfaces are provided for other models.
- And up to 16 independent PoE network interfaces are provided for VN4016/P series.
- IPv6 is supported.
- TCP/IP protocol, PPPoE, DHCP, DNS, DDNS, NTP, SADP, SMTP, SNMP, NFS, and iSCSI are supported.
- TCP, UDP and RTP for unicast.
- Auto/Manual port mapping by UPnP™.
- Extranet access by HiDDNS.
- Support access by Cloud P2P.
- Remote reverse playback via RTSP.
- Support accessing by the platform via ONVIF.
- Remote search, playback, download, locking and unlocking of the record files, and the breakpoint resume is supported for downloading files.
- Remote parameters setup; remote import/export of device parameters.

- Remote viewing of the device status, system logs and alarm status.
- Remote keyboard operation.
- Remote locking and unlocking of control panel and mouse.
- Remote HDD formatting and program upgrading.
- Remote system restart and shutdown.
- RS-232, RS-485 transparent channel transmission (depending on models).
- Alarm and exception information can be sent to the remote host
- Remotely start/stop recording.
- Remotely start/stop alarm output.
- Remote PTZ control (depending on models).
- 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	13
1.1 Front Panel	14
VN4016 Series	14
1.2 IR Remote Control Operations	16
1.2 USB Mouse Operation	19
1.3 Input Method Description	20
1.4 Rear Panel	21
VN4016 Series	21
Chapter 2 Getting Started	22
2.1 Starting Up and Shutting Down the NVR	23
2.2 Setting Admin Password	25
2.3 Using the Wizard for Basic Configuration	26
2.4 Login and Logout	30
2.4.1 User Login	30
2.4.2 User Logout	31
2.5 Adding and Connecting the IP Cameras	32
2.5.1 Activating the IP Camera	32
2.5.2 Adding the Online IP Cameras	32
2.5.3 Editing the Connected IP cameras and Configuring Customized Protocols	35
Chapter 3 Live View	38
Introduction of Live View	39
3.2 Operations in Live View Mode	40
3.2.2 Front Panel Operation on Live View	40
3.2.3 Using the Mouse in Live View	40
3.2.4 Quick Setting Toolbar in Live View Mode	41
3.3 Adjusting Live View Settings	44
3.4 Channel-zero Encoding	45
Chapter 4 PTZ Controls	46
4.1 Configuring PTZ Settings	47
4.2 Setting PTZ Presets, Patrols & Patterns	48
4.2.1 Customizing Presets	48
4.2.2 Calling Presets	48
4.2.3 Customizing Patrols	49
4.2.4 Calling Patrols	50
4.2.5 Customizing Patterns	51
4.2.6 Calling Patterns	51
4.2.7 Customizing Linear Scan Limit	52
4.2.8 Calling Linear Scan	53
4.2.9 One-touch Park	53
4.3 PTZ Control Panel	55
Chapter 5 Recording Settings	56

5.1	Configuring Parameters	57
5.2	Configuring Recording Schedule	60
5.3	Configuring Motion Detection Recording	63
5.4	Configuring Alarm Triggered Recording	65
5.5	Configuring VCA Event Recording	67
5.6	Manual Recording	68
5.7	Configuring Holiday Recording	69
5.8	Configuring Redundant Recording	70
5.9	Configuring HDD Group for Recording	72
5.10	Files Protection	73
5.10.1	Locking the Recording Files	73
5.10.2	Setting HDD Property to Read-only	75
Chapter 6	Playback	77
6.1	Playing Back Record Files	78
6.1.1	Instant Playback	78
6.1.2	Playing Back by Normal Search	78
6.1.3	Playing Back by Event Search	80
6.1.4	Playing Back by Tag	82
6.1.5	Playing back by Smart Playback	84
6.1.6	Playing Back by System Logs	86
6.1.7	Playing Back External File	87
6.1.8	Playing Back by Sub-periods	88
Chapter 7	Backup	90
7.1	Backing up Record Files	91
7.1.1	Backing up by Normal Video Search	91
7.1.2	Backing up by Event Search	92
7.1.3	Backing up Video Clips	94
7.2	Managing Backup Devices	95
Chapter 8	Alarm Settings	96
8.1	Setting Motion Detection Alarm	97
8.2	Setting Sensor Alarms	99
8.3	Detecting Video Loss Alarm	102
8.4	Detecting Video Tampering Alarm	103
8.5	Handling Exceptions Alarm	105
8.6	Setting Alarm Response Actions	106
8.7	Triggering or Clearing Alarm Output Manually	109
Chapter 9	VCA Alarm	110
9.1	Face Detection	111
9.2	Vehicle Detection	112
9.3	Line Crossing Detection	114
9.4	Intrusion Detection	116
9.5	Region Entrance Detection	118
9.6	Region Exiting Detection	119
9.7	Loitering Detection	119

9.8	People Gathering Detection	119
9.9	Fast Moving Detection	119
9.10	Parking Detection	120
9.11	Unattended Baggage Detection	120
9.12	Object Removal Detection.....	120
9.13	Audio Exception Detection	121
9.14	Sudden Scene Change Detection.....	122
9.15	Defocus Detection	122
9.16	PIR Alarm	122
Chapter 10	VCA Search	123
10.1	Face Search	124
10.2	Behavior Search	126
10.3	Plate Search.....	127
10.4	People Counting	128
10.5	Heat Map.....	130
Chapter 11	Network Settings	131
11.1	Configuring General Settings	132
11.2	Configuring Advanced Settings.....	134
11.2.1	PPPoE Settings	134
11.2.2	Configuring Cloud P2P.....	134
11.2.3	Configuring DDNS.....	135
11.2.4	Configuring NTP Server.....	139
11.2.5	Configuring Remote Alarm Host.....	140
11.2.6	Configuring Multicast.....	141
11.2.7	Configuring RTSP	141
11.2.8	Configuring Server and HTTP Ports.....	141
11.2.9	Configuring Email	142
11.2.10	Configuring NAT.....	143
11.3	Checking Network Traffic	146
11.4	Configuring Network Detection	148
11.4.1	Testing Network Delay and Packet Loss.....	148
11.4.2	Exporting Network Packet.....	148
11.4.3	Checking the Network Status.....	149
11.4.4	Checking Network Statistics.....	150
Chapter 12	HDD Management.....	152
12.1	Initializing HDDs	153
12.2	Managing Network HDD	155
12.3	Managing HDD Group	158
12.3.1	Setting HDD Groups.....	158
12.3.2	Setting HDD Property.....	159
12.4	Configuring Quota Mode.....	161
12.5	Checking HDD Status	163
12.6	HDD Detection.....	164
12.7	Configuring HDD Error Alarms	166

Chapter 13	Camera Settings	167
13.1	Configuring OSD Settings	168
13.2	Configuring Privacy Mask	169
13.3	Configuring Video Parameters	170
Chapter 14	NVR Management and Maintenance	171
14.1	Viewing System Information	172
14.2	Searching & Export Log Files	173
14.3	Importing/Exporting IP Camera Info	176
14.4	Importing/Exporting Configuration Files	177
14.5	Upgrading System	178
14.5.1	Upgrading by Local Backup Device	178
14.5.2	Upgrading by FTP	178
14.6	Restoring Default Settings	180
Chapter 15	Others	181
15.1	Configuring RS-232 Serial Port	182
15.2	Configuring General Settings	183
15.3	Configuring DST Settings	184
15.4	Configuring More Settings for Device Parameters	185
15.5	Managing User Accounts	186
15.5.1	Adding a User	186
15.5.2	Deleting a User	188
15.5.3	Editing a User	189

Chapter 1 Introduction

1.1 Front Panel

VN4016 Series

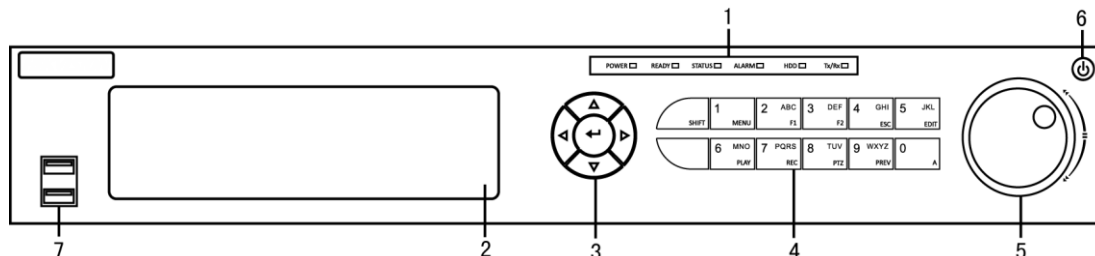


Figure 1. 1 VN4016 Series

Table 1. 1 Description of Control Panel Buttons

No.	Name	Function Description	
1	Status Indicators	POWER	Turns green when NVR is powered up.
		READY	The indicator is green when the device is running normally.
		STATUS	The light is green when the IR remote control is enabled; The light is red when the function of the composite keys (SHIFT) are used; The light is out when none of the above condition is met.
		ALARM	The light is red when there is an alarm occurring.
		HDD	Blinks red when HDD is reading/writing.
		Tx/Rx	Blinks green when network connection is functioning normally.
2	DVD-R/W	Slot for DVD-R/W.	
3	DIRECTION	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.	
		In auto sequence view mode, the buttons can be used to pause or resume auto sequence.	
4	Composite Keys	SHIFT	Switch between the numeric or letter input and functions of the composite keys. (Input letter or numbers when the light is out;

No.	Name	Function Description	
		Realize functions when the light is red.)	
		1/MENU	
		Enter numeral "1";	
		Access the main menu interface.	
		2/ABC/F1	Enter numeral "2";
			Enter letters "ABC";
			The F1 button when used in a list field will select all items in the list.
			In PTZ Control mode, it will turn on/off PTZ light and when the image is zoomed in, the key is used to zoom out.
		3/DEF/F2	Enter numeral "3";
			Enter letters "DEF";
			The F2 button is used to change the tab pages.
			In PTZ control mode, it zooms in the image.
		4/GHI/ESC	Enter numeral "4";
			Enter letters "GHI";
			Exit and back to the previous menu.
		5/JKL/EDIT	Enter numeral "5";
			Enter letters "JKL";
			Delete characters before cursor;
			Check the checkbox and select the ON/OFF switch;
			Start/stop record clipping in playback.
		6/MNO/PLAY	Enter numeral "6";
			Enter letters "MNO";
			Playback, for direct access to playback interface.
		7/PQRS/REC	Enter numeral "7";
			Enter letters "PQRS";
			Open the manual record interface.
		8/TUV/PTZ	Enter numeral "8";
			Enter letters "TUV";
Access PTZ control interface.			
9/WXYZ/PRE V	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.		
5	JOG SHUTTLE Control	Move the active selection in a menu. It will move the selection up and down.	
		In Live View mode, it can be used to cycle through different channels.	
		In the Playback mode, it can be used to jump 30s forward/backward in video files.	
		In PTZ control mode, it can control the movement of the PTZ camera.	

No.	Name	Function Description
6	POWER ON/OFF	Power on/off switch.
7	USB Interfaces	Universal Serial Bus (USB) ports for additional devices such as USB mouse and USB Hard Disk Drive (HDD).

1.2 IR Remote Control Operations

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



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

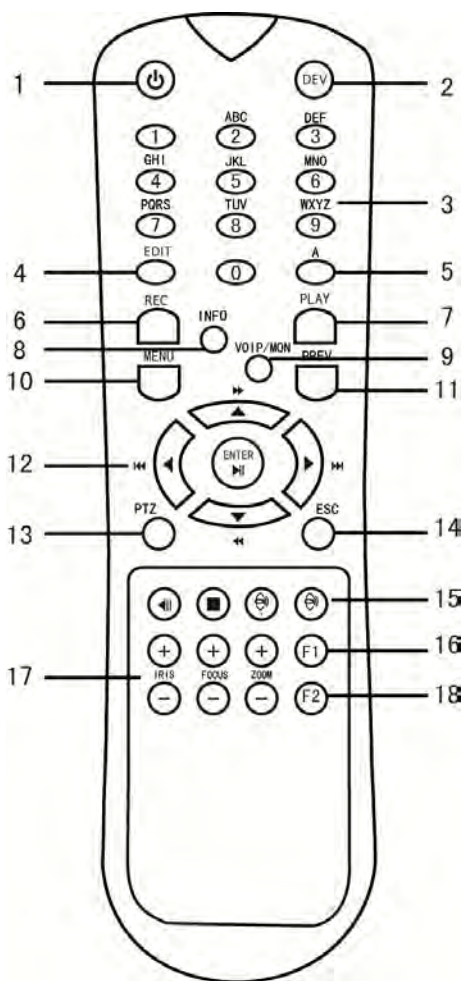


Figure 1. 2 Remote Control

The keys on the remote control closely resemble the ones on the front panel.

Table 1. 2 Description of the Soft Keyboard Icons

No.	Name	Description
1	POWER	Power on/off the device.
2	DEV	Enables/Disables Remote Control.

No.	Name	Description
3	Alphanumeric Buttons	Switch to the corresponding channel in Live view or PTZ Control mode.
		Input numbers and characters in Edit mode.
		Switch between different channels in the Playback mode.
4	EDIT Button	Edit text fields. When editing text fields, it will also function as a Backspace button to delete the character in front of the cursor.
		On checkbox fields, pressing the button will <i>check</i> the checkbox.
		In PTZ Control mode, the button adjusts the iris of the camera.
		In Playback mode, it can be used to generate video clips for backup.
		Enter/exit the folder of USB device.
5	A Button	Adjust focus in the PTZ Control menu.
		It is also used to switch between input methods (upper and lowercase alphabet, symbols and numeric input).
6	REC Button	Enter the Manual Record setting menu.
		In PTZ control settings, press the button and then you can call a PTZ preset by pressing Numeric button.
		It is also used to turn audio on/off in the Playback mode.
7	PLAY Button	The button is used to enter the All-day Playback mode.
		It is also used to auto scan in the PTZ Control menu.
8	INFO Button	Reserved.
9	VOIP Button	Switch between main and spot output.
		In PTZ Control mode, it can be used to zoom out the image.
10	MENU Button	Press the button will help you return to the Main menu (after successful login).
		Press and hold the button for 5 seconds will turn off audible key beep.
		In PTZ Control mode, the MENU button will start wiper (if applicable).
		In Playback mode, it is used to show/hide the control interface.
11	PREV Button	Switch between single screen and multi-screen mode.
		In PTZ Control mode, it is used to adjust the focus in conjunction with the A/FOCUS+ button.
12	DIRECTION Button	Navigate between different fields and items in menus.
		In the Playback mode, the Up and Down button is used to speed up and slow down recorded video. The Left and Right button will select the next and previous record files.
		In Live View mode, these buttons can be used to cycle through channels.
		In PTZ control mode, it can control the movement of the PTZ camera.
	ENTER Button	Confirm selection in any of the menu modes.
	It can also be used to <i>tick</i> checkbox fields.	
	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.	
13	PTZ Button	In Auto-switch mode, it can be used to stop /start auto switch.

No.	Name	Description
14	ESC Button	Back to the previous menu.
		Press for Arming/disarming the device in Live View mode.
15	RESERVED	Reserved for future usage.
16	F1 Button	Select all items on the list when used in a list field.
		In PTZ Control mode, it will turn on/off PTZ light (if applicable).
		In Playback mode, it is used to switch between play and reverse play.
17	PTZ Control Buttons	Buttons to adjust the iris, focus and zoom of a PTZ camera.
18	F2 Button	Cycle through tab pages.
		In synchronous playback mode, it is used to switch between channels.

Troubleshooting Remote Control:



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

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

Steps:

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

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

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

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

1.2 USB Mouse Operation

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

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

The operation of the mouse:

Table 1. 3 Description of the Mouse Control

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

1.3 Input Method Description



Figure 1. 1 Soft Keyboard (1)



Figure 1. 2 Soft Keyboard (2)

Description of the buttons on the soft keyboard:

Table 1. 1 Description of the Soft Keyboard Icons

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

1.4 Rear Panel



The rear panel varies according to different models.

VN4016 Series

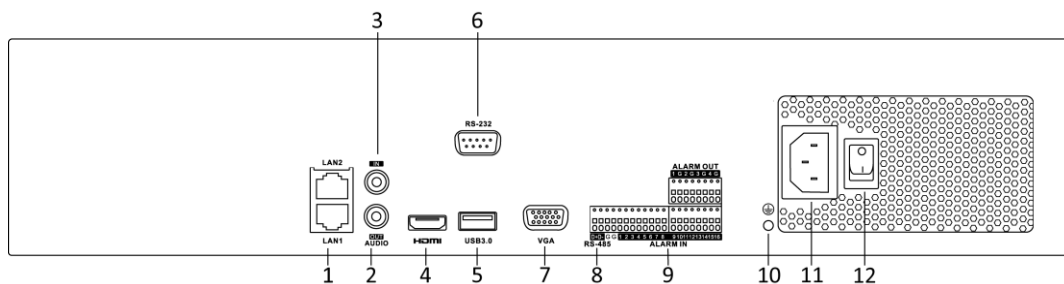


Figure 1.3 VN4016 Series

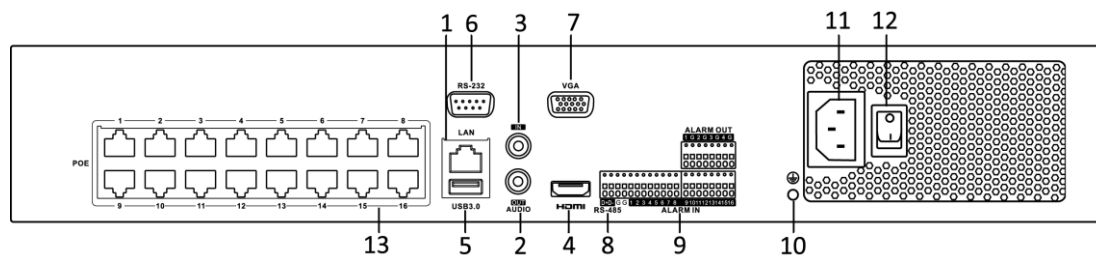


Figure 1.4 VN4016/P Series

Table 1.4 Description of Rear Panel Interfaces

No.	Item	Description
1	LAN Interface	1 network interface provided for VN4016/P and 2 network interfaces for VN4016
2	AUDIO OUT	RCA connector for audio output.
3	LINE IN	RCA connector for audio input.
4	HDMI™	HDMI™ video output connector.
5	USB 3.0 interface	Universal Serial Bus (USB) ports for additional devices such as USB mouse and USB Hard Disk Drive (HDD).
6	RS-232 Interface	Connector for RS-232 devices.
7	VGA	DB9 connector for VGA output. Display local video output and menu.
8	RS-485 Interface	Half-duplex connector for RS-485 devices.
9	ALARM IN	Connector for alarm input.
	ALARM OUT	Connector for alarm output.
10	GROUND	Ground (needs to be connected when NVR starts up).
11	AC 100V ~ 240V	AC 100V ~ 240V power supply.
12	Power Switch	Switch for turning on/off the device.
13	Network Interfaces with	Network interfaces for the cameras and to provide power over Ethernet.

No.	Item	Description
	PoE function (supported by VN4016/P)	

Chapter 2 Getting Started

2.1 Starting Up and Shutting Down the NVR

Purpose:


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

Before you start:

Check that the voltage of the extra power supply is the same with the NVR's requirement, and the ground connection is working properly.

Starting up the NVR:

Steps:

1. Check the power supply is plugged into an electrical outlet. It is **HIGHLY** recommended that an Uninterruptible Power Supply (UPS) be used in conjunction with the device. The Power indicator LED on the front panel should be red, indicating the device gets the power supply.
2. Turn on the power switch on the rear panel if the device starts up for the first time, or press the  button on the front panel. The Power indicator LED should turn blue indicating that the unit begins to start up.
3. After startup, the Power indicator LED remains blue. A splash screen with the status of the HDD appears on the monitor. The row of icons at the bottom of the screen shows the HDD status. 'X' means that the HDD is not installed or cannot be detected.

Shutting down the NVR

There are two proper ways to shut down the NVR.

● **OPTION 1: By Standard shutdown**

Steps:

1. Enter the Shutdown menu.
Menu > Shutdown



Figure 2. 1 Shutdown Menu

2. Click the **Shutdown** button.
3. Click the **Yes** button.

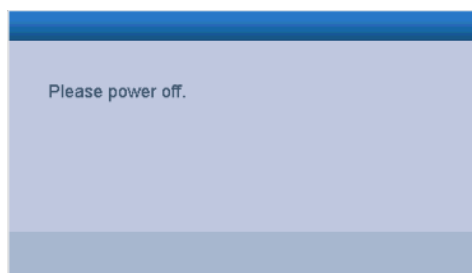




Figure 2. 2 Shutdown Attention

● **OPTION 2: By operating the front panel**

Steps:

1. Press and hold the  button on the front panel for 3 seconds.
2. Enter the administrator's username and password in the dialog box for authentication if required.
3. Click the **Yes** button.



Do not press the  button again when the system is shutting down.

Rebooting the NVR

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

Steps:

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

2.2 Setting Admin Password

Purpose:

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

Steps:

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

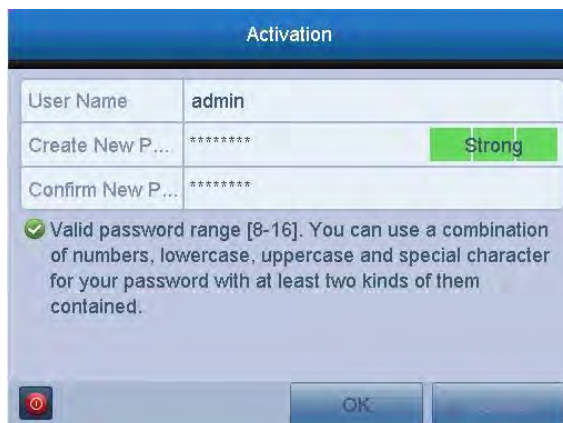


Figure 2. 3 Settings Admin Password

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

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



For the old version device, if you update it to the new version, a warning box will pop up once the device starts up to remind you to use a strong admin password to ensure your information security. You can click **YES** and follow the wizard to set a strong password.

2.3 Using the Wizard for Basic Configuration

Purpose:

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

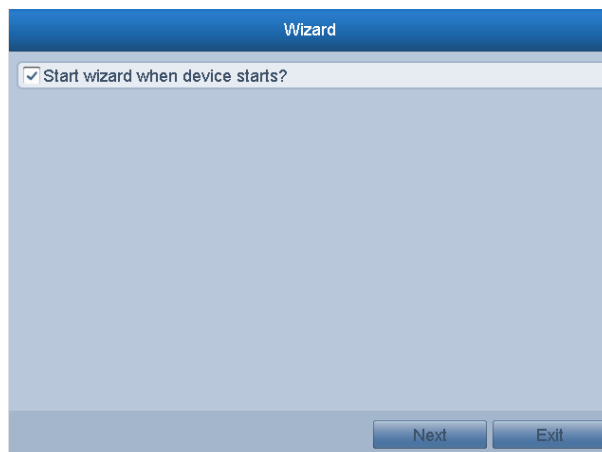


Figure 2. 4 Start Wizard Interface

Steps:

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



Figure 2. 5 Date and Time Settings

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

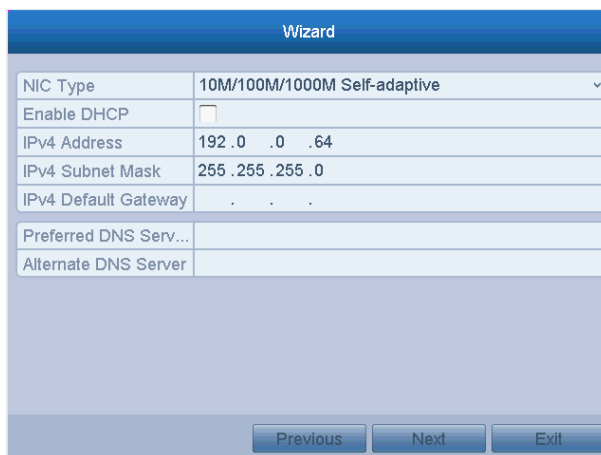


Figure 2. 6 Network Configuration



- The dual-NIC network 10/100/1000 Mbps self-adaptive Ethernet interfaces are provided for the VN4016 series NVR;
 - For the models have the PoE or built-in switch network interfaces, including VN4016/P series NVR, the internal NIC IPv4 address should be configured for the cameras connecting to the PoE or built-in switch network interface of the NVR.
4. Click **Next** button after you configured the basic network parameters. Then you will enter the **Cloud P2P** interface. Configure the Cloud P2P according to your need.

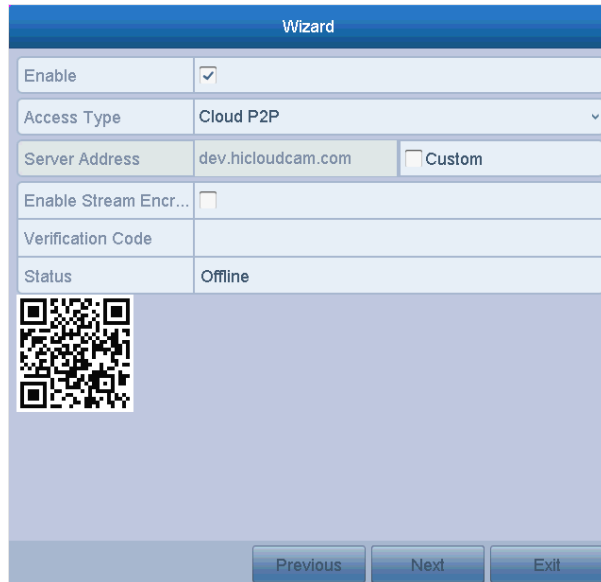


Figure 2. 7 Advanced Network Parameters

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



Figure 2. 8 Advanced Network Parameters

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

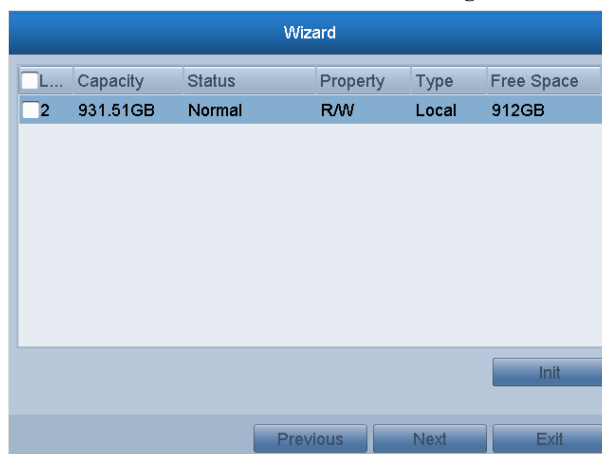


Figure 2. 9 HDD Management

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

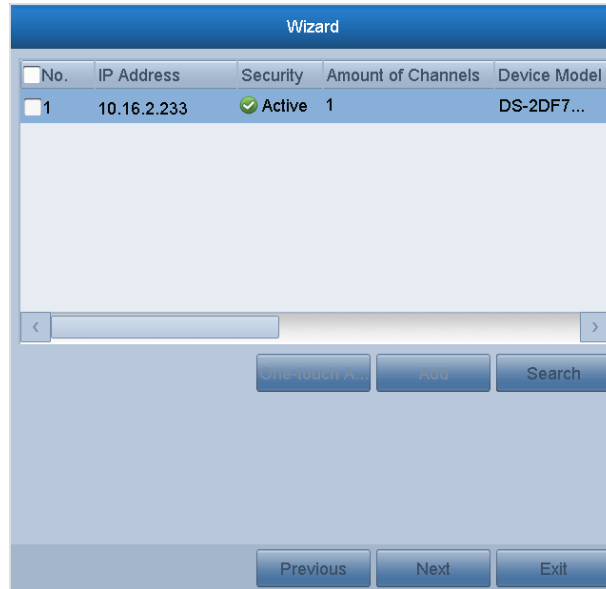


Figure 2. 10 IP Camera Management

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

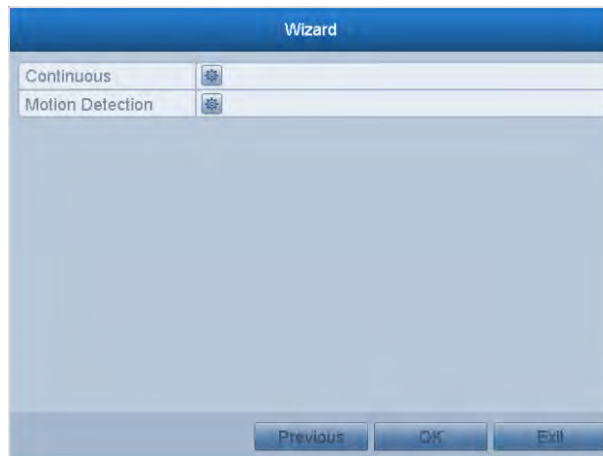


Figure 2. 11 Record Settings

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

2.4 Login and Logout

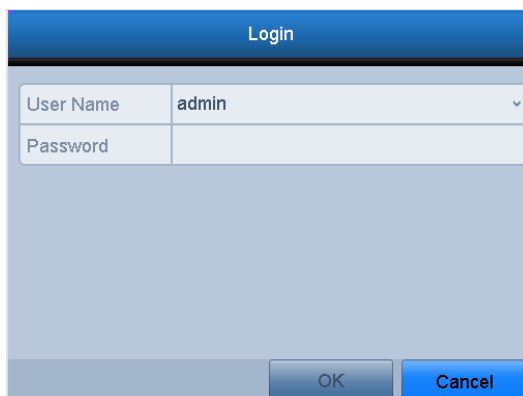
2.4.1 User Login

Purpose:

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

Steps:

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



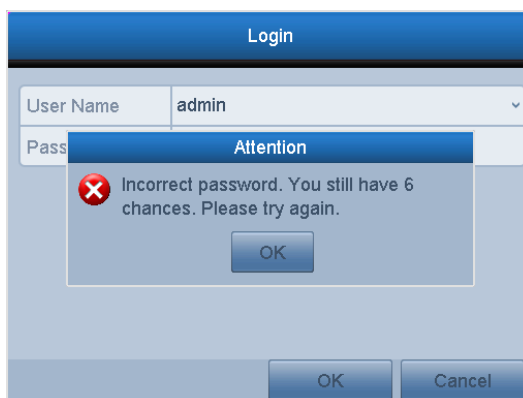
The screenshot shows a 'Login' dialog box with a blue header. Below the header, there are two input fields: 'User Name' with a dropdown menu showing 'admin' and a downward arrow, and 'Password' which is currently empty. At the bottom of the dialog, there are two buttons: 'OK' and 'Cancel'.

Figure 2. 12 Login Interface

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



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



The screenshot shows the same 'Login' dialog box as in Figure 2.12, but with an 'Attention' dialog box overlaid on top. The 'Attention' dialog has a blue header and a red 'X' icon. The text inside reads: 'Incorrect password. You still have 6 chances. Please try again.' Below the text is an 'OK' button. The 'User Name' dropdown in the background is still set to 'admin' and the 'Pass' field is empty. The 'OK' and 'Cancel' buttons from the background dialog are also visible at the bottom.

Figure 2. 13 User Account Protection

2.4.2 User Logout

Purpose:

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

Steps:

1. Enter the Shutdown menu.
Menu>Shutdown

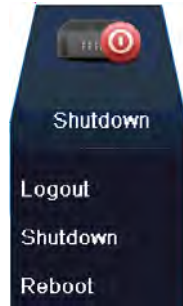


Figure 2. 14 Logout

2. Click **Logout**.



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

2.5 Adding and Connecting the IP Cameras

2.5.1 Activating the IP Camera

Purpose:

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

Steps:

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

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

2. Click the inactive icon of the camera to enter the activation 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 NVR.

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



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

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

2.5.2 Adding the Online IP Cameras

Purpose:


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

Before you start:

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

- **OPTION 1:**

Steps:

1. Click to select an idle window in the live view mode.
2. Click the  icon in the center of the window to pop up the adding IP camera interface.

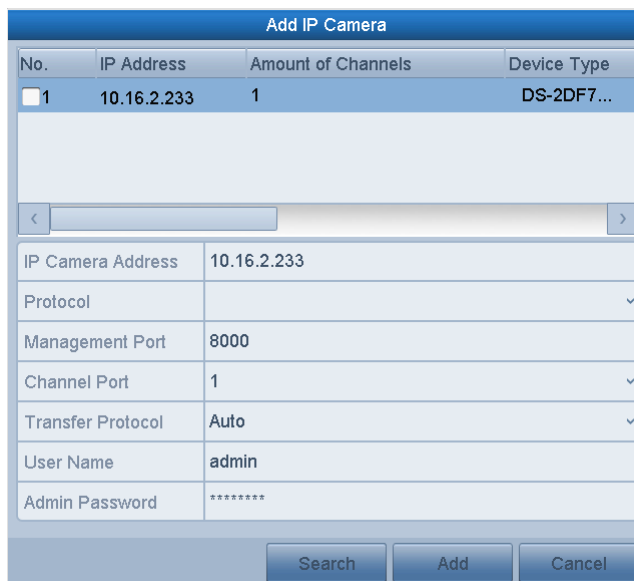


Figure 2. 15 Quick Adding IP Camera Interface

3. Select the detected IP camera and click the **Add** button to add it directly, and you can click the **Search** button to refresh the online IP camera manually.

Or you can choose to custom add the IP camera by editing the parameters in the corresponding textfiled and then click the **Add** button to add it.

- **OPTION 2:**

Steps:

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



Figure 2. 16 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. Or you can click the **One-touch Adding** button to add all cameras from the list.
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.

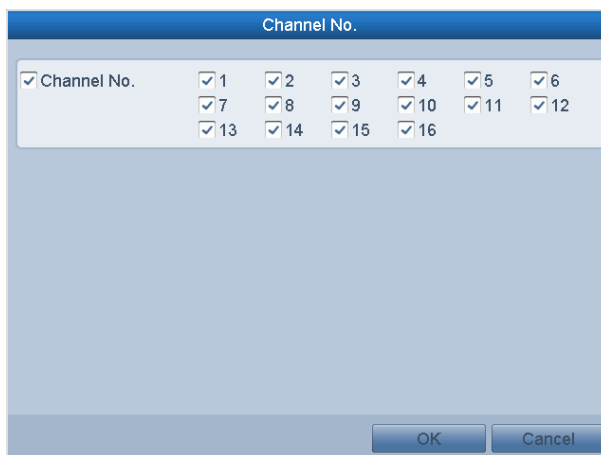


Figure 2. 17 Selecting Multiple Channels

• **OPTION 3:**

Steps:

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



Figure 2. 18 Custom Adding IP Camera Interface

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



If the IP camera to add has not been activated, you can activate it from the IP camera list on the camera management interface.

- 3) (Optional) Check the checkbox of **Continue to Add** to add other IP cameras.
- 4) 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 risk password.



Figure 2. 19 Successfully Added IP Cameras

Table 2. 1 Explanation of the icons

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



You can click on the interface or select the Camera No. and click **Delete** to delete the IP cameras.

2.5.3 Editing the Connected IP cameras and Configuring Customized Protocols

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

Steps:

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




Figure 2. 20 Edit the 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.

To edit advanced parameters:

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

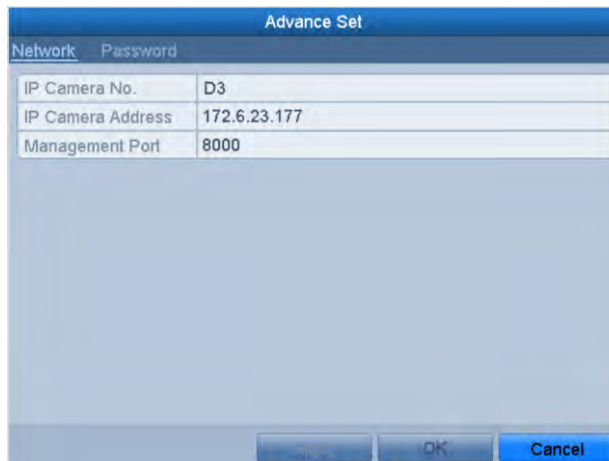


Figure 2. 21 Network Configuration of the Camera

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

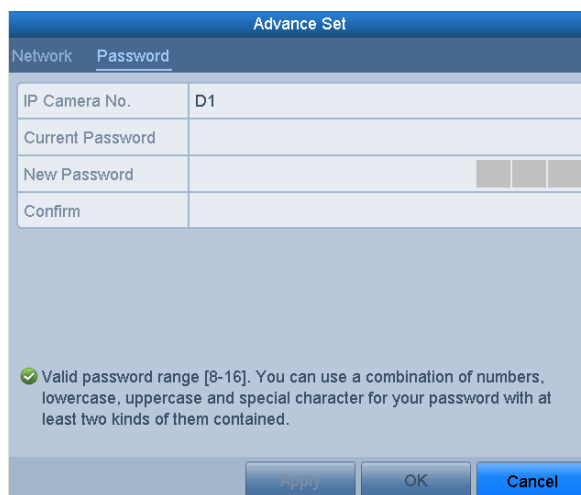


Figure 2. 22 Password Configuration of the Camera

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

Configuring the customized protocols

Purpose:

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

Steps:

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

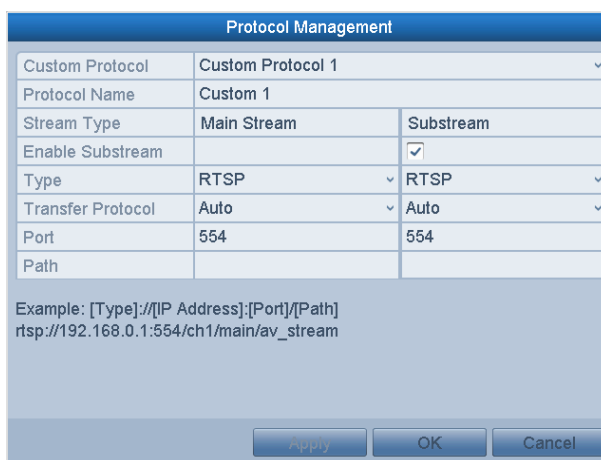


Figure 2. 23 Protocol Management Interface

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

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



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

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

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

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



The protocol type and the transfer protocols must be supported by the connected network camera. After adding the customized protocols, you can see the protocol name is listed in the dropdown list, please refer to Figure 2. 24.



Figure 2. 24 Protocol Setting

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

Chapter 3 Live View





Introduction of Live View

Live view shows you the video image getting from each camera in real time. The NVR automatically enters Live View mode when powered on. It is also at the very top of the menu hierarchy, thus pressing the ESC many times (depending on which menu you're on) brings you to the Live View mode.

Live View Icons

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

Table 3. 1 Description of Live View Icons

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

3.2 Operations in Live View Mode

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

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

Menu > Configuration > Live View > Dwell Time.

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

3.2.2 Front Panel Operation on Live View

Table 3. 2 Front Panel Operation in Live View

Functions	Front Panel Operation
Show single screen	Press the corresponding Alphanumeric button. E.g. Press 2 to display only the screen for channel 2.
Show multi-screen	Press the PREV/FOCUS- button.
Manually switch screens	Next screen: right/down direction button. Previous screen: left/up direction button.
Auto-switch	Press Enter button.
Playback	Press Play button.








3.2.3 Using the Mouse in Live View

In live view mode, right click on the screen to enter the menu bar:



Figure 3. 2 Right-click Menu Bar

Table 3. 3 Mouse Operation in Live View

Icon	Name	Description
 Comm...	Common Menu	Quick access to the sub-menus which you frequently visit.
 Menu	Menu	Enter the main menu of the system\
	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.

Icon	Name	Description
	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.
	Continuous Record	Start continuous recording of all channels, Normal Record and Motion Detection Recording are selectable from the dropdown list.
	Motion Detection Record	Start motion detection recording of all channels.
	Add IP Camera	Enter the IP Camera Management interface, and manage the cameras.
	Playback	Enter the playback interface and start playing back the video of the selected channel immediately.
	Output Mode	Four modes of output supported, including Standard, Bright, Gentle and Vivid.



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



The right-click menu varies according to different models. Please refer to the actual GUI menu of the device.

3.2.4 Quick Setting Toolbar in Live View Mode

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



Figure 3.3 Quick Setting Toolbar

Table 3.4 Description of Quick Setting Toolbar Icons

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



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

during the last five minutes.


 Digital Zoom can zoom in the selected area to the full screen. You can left-click and draw to select the area to zoom in, as shown in Figure 3. 4.



Figure 3. 4 Digital Zoom


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



Figure 3. 5 Image Settings- Preset

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

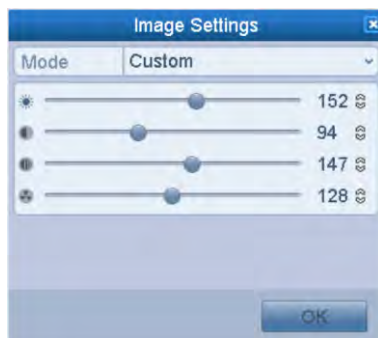


Figure 3. 6 Image Settings- Customize



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

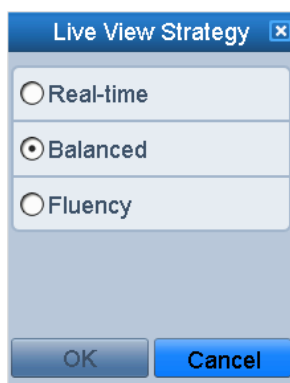


Figure 3. 7 Live View Strategy



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



Figure 3. 8 Information

3.3 Adjusting Live View Settings

Purpose:

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

Steps:

1. Enter the Live View Settings interface.

Menu > Configuration > Live View

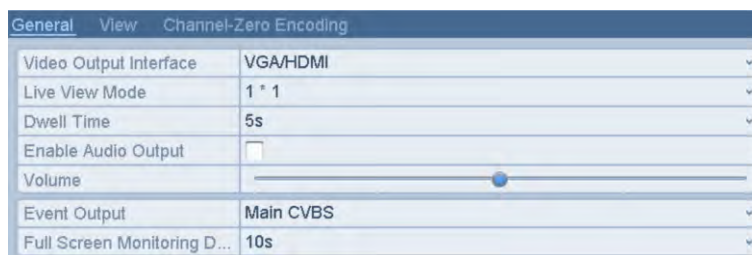


Figure 3.9 Live View-General

The settings available in this menu include:

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

2. Setting Cameras Order

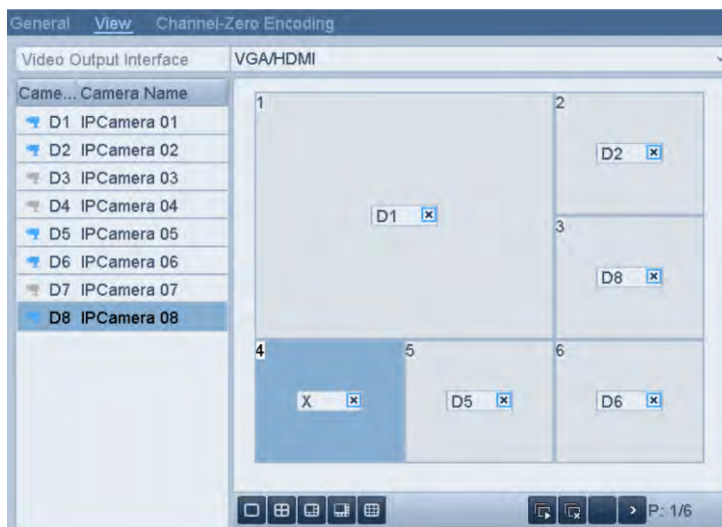






Figure 3.10 Live View- Camera Order

- 1) Select a **View** mode in .
- 2) Select the small window, and double-click on the channel number to display the channel on the window.
 If you do not want the camera to be displayed on the live view interface, click the corresponding  to stop it.
 You can also click  button to start live view for all the channels and click  to stop all the live view.
- 3) Click the **Apply** button to save the setting.

3.4 Channel-zero Encoding

Purpose:

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

Steps:

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

Enable Channel-Zero En...	<input checked="" type="checkbox"/>
Frame Rate	Full Frame ▾
Max. Bitrate Mode	General ▾
Max. Bitrate(Kbps)	1792 ▾

Figure 3. 11 Live View- Channel-Zero Encoding

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

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

Chapter 4 PTZ Controls

4.1 Configuring PTZ Settings

Purpose:

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

Steps:

1. Enter the PTZ Settings interface.

Menu > Camera > PTZ

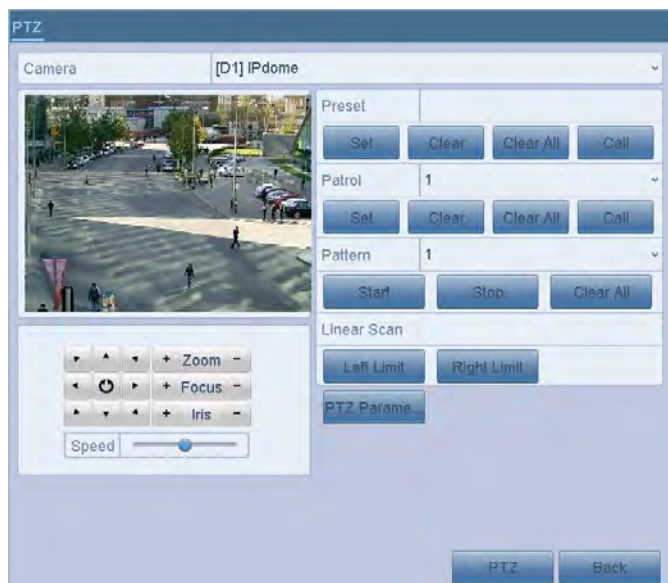


Figure 4. 1 PTZ Settings

2. Click the PTZ Setting button to set the PTZ parameters.

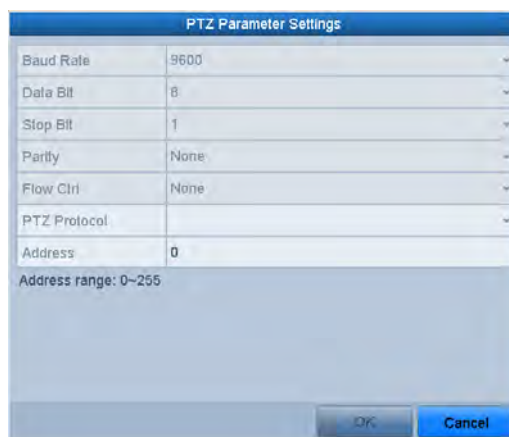


Figure 4. 2 PTZ- General

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



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

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

4.2 Setting PTZ Presets, Patrols & Patterns

Before you start:

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

4.2.1 Customizing Presets

Purpose:

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

Steps:

1. Enter the PTZ Control interface.

Menu > Camera > PTZ

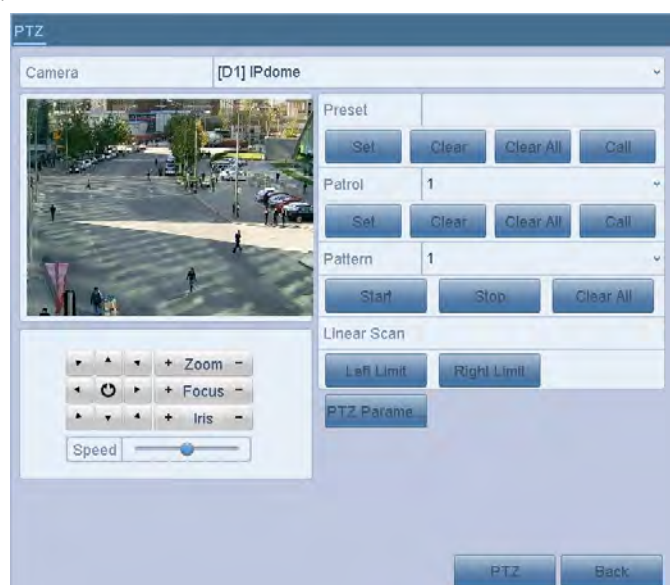


Figure 4. 3 PTZ Settings

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 steps2-3 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 to show the PTZ control panel.

2. Choose **Camera** in the dropdown list.
3. Click the  button to show the general settings of the PTZ control.

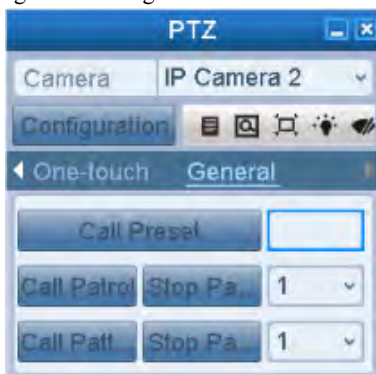


Figure 4. 4 PTZ Panel - General

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

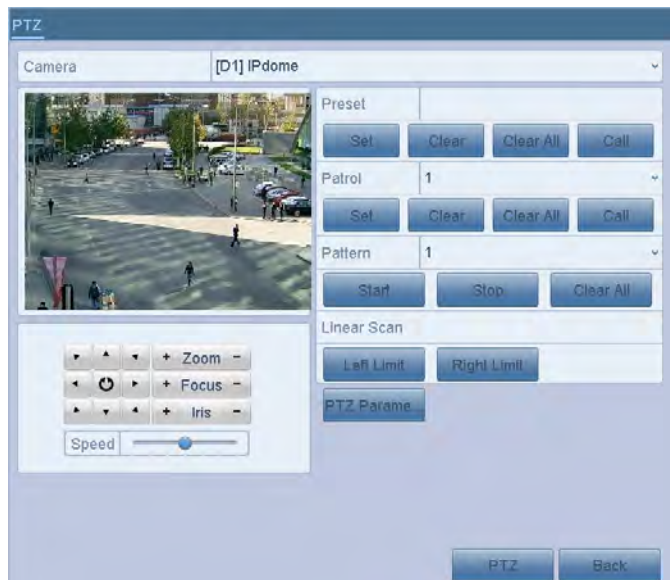


Figure 4. 5 PTZ Settings

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

4.2.4 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 to show the PTZ control panel.
2. Click the  button to show the general settings of the PTZ control.

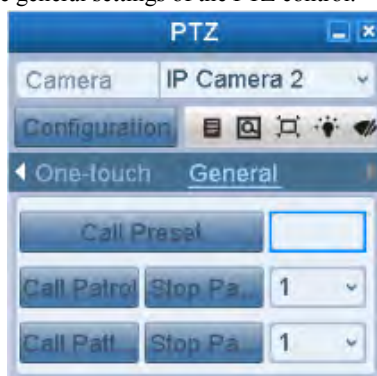


Figure 4. 7 PTZ Panel - General

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

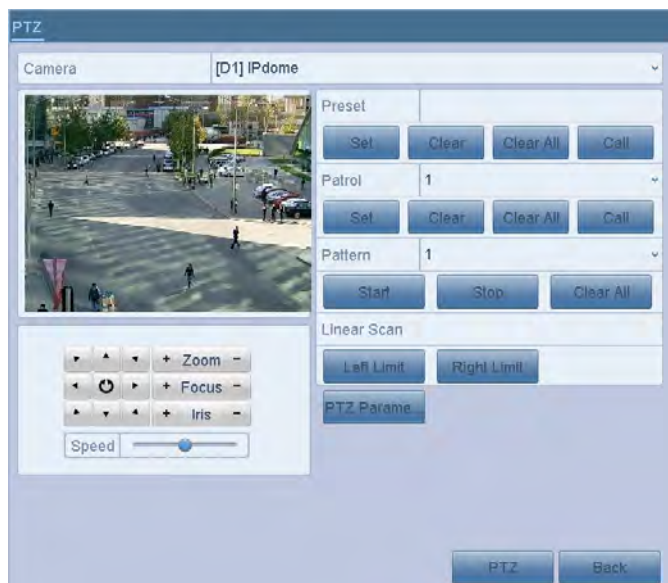


Figure 4. 8 PTZ Settings

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 to show the PTZ control panel.
2. Click the  button 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 horizontal direction in the predefined range.



This function is supported by some certain models.

Steps:

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

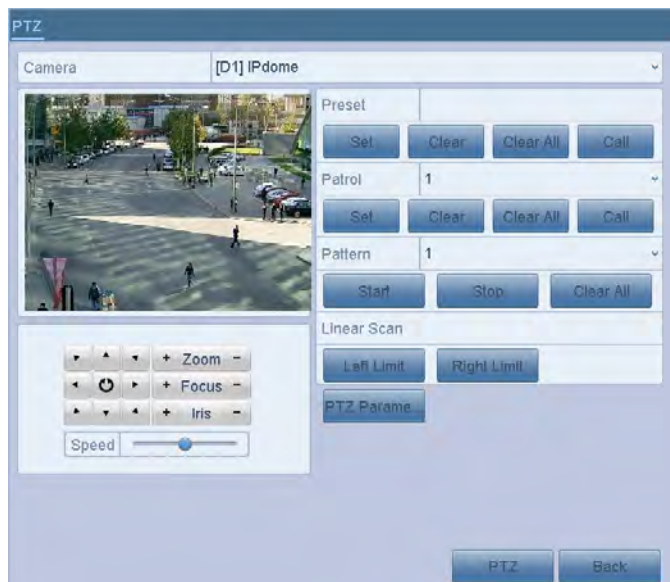


Figure 4. 10 PTZ Settings

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.



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

4.2.8 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  button 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  button 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 move 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.



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

4. Click the button again to inactivate it.


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.

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













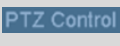

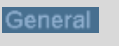






In PTZ control mode, the PTZ panel will be displayed when a mouse is connected with the device. If no mouse is connected, the  icon appears in the lower-left corner of the window, indicating that this camera is in PTZ control mode.



Figure 4. 13 PTZ Panel

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-Zoom		Image Centralization		Menu
	Switch to the PTZ control interface		Switch to the one-touch control interface		Switch to the general settings interface
	Previous item		Next item		Start pattern / patrol
	Stop the patrol / pattern movement		Exit		Minimize windows

Chapter 5 Recording Settings

5.1 Configuring Parameters

Purpose:

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

Before you start:

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

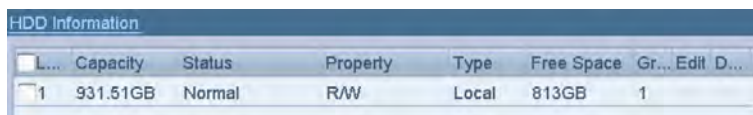


Figure 5. 1 HDD- General

2. Check the storage mode of the HDD.
 - 1) Click **Advanced** to check the storage mode of the HDD.
 - 2) If the HDD mode is *Quota*, please set the maximum record capacity For detailed information, see *Chapter 12.4 Configuring Quota Mode*.
 - 3) If the HDD mode is **Group**, you should set the HDD group. For detailed information, see *Chapter Configuring HDD Group for Recording*.

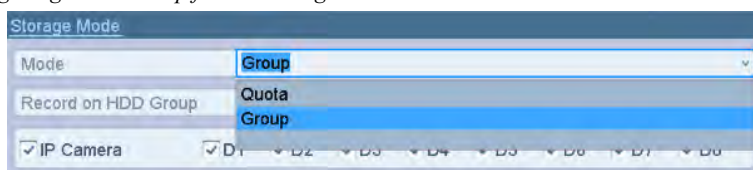


Figure 5. 2 HDD- Advanced

Steps:

1. Enter the Record settings interface to configure the recording parameters:
Menu > Record > Parameters

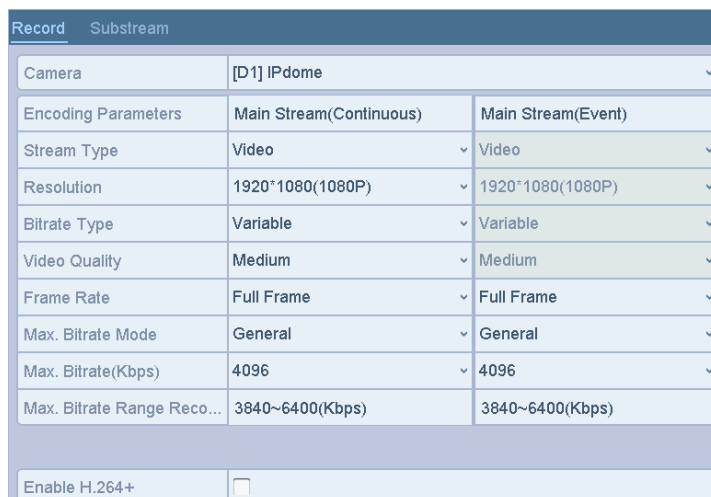


Figure 5. 3 Recording Parameters

2. Parameters Setting for Recording
 - 1) Select **Record** tab page to configure. You can configure the stream type, the resolution, and other parameters on your demand.

- **Enable H.264+ Mode:** check the checkbox to enable. Once enabled, the **Max. Bitrate Mode**, **Max. Bitrate(Kbps)** and **Max. Bitrate Range Recommend** are not configurable. Enabling it helps to ensure the high video quality with a lowered bitrate.



The function is only available for IP cameras which support H.264+ stream.

- 2) Click the **More Settings** button to set the advanced parameters for recording and then click **OK** button to finish editing.



Figure 5. 4 Recording Parameters-More Settings

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



- The redundant record is to decide whether you want the camera to save the recording files in the redundant HDD. You must configure the redundant HDD in HDD settings. For detailed information, see *Chapter12.3.2 Setting HDD Property*.
- The parameters of Main Stream (Event) are read-only.

3. Parameters Settings for Sub-stream

- 1) Enter the Sub-stream tab page.

Record	Substream
Camera	IP Camera 3
Stream Type	Video & Audio
Resolution	352*288(CIF)
Bitrate Type	Variable
Video Quality	Medium
Frame Rate	12fps
Max. Bitrate Mode	General
Max. Bitrate(Kbps)	512
Max. Bitrate Range Reco...	153~255(Kbps)

Figure 5. 5 Sub-stream Parameters

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

5.2 Configuring Recording Schedule

Purpose:

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

Steps:

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

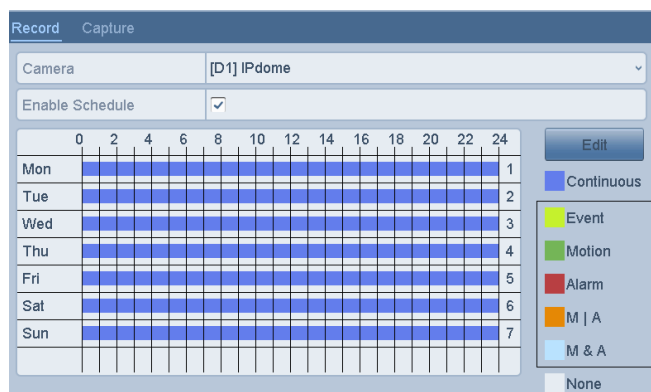


Figure 5. 6 Record Schedule

Different recording types are marked in different color icons.

Continuous: scheduled recording.

Event: recording triggered by all event triggered alarm.

Motion: recording triggered by motion detection.

Alarm: recording triggered by alarm.

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

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

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

Edit the schedule:

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

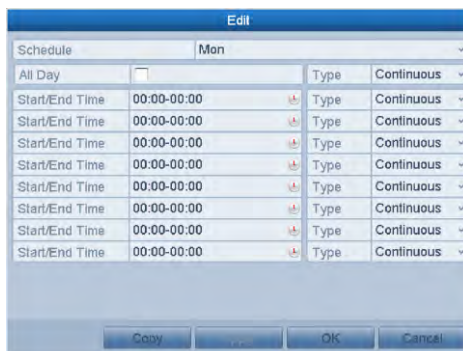



Figure 5. 7 Recording Schedule Interface

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

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

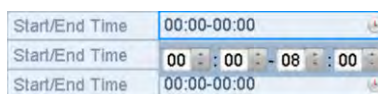


Figure 5. 8 Edit Schedule

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



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

- IV. Select the record type in the dropdown list.



- To enable Motion, Alarm, M | A (motion or alarm), M & A (motion and alarm) and VCA (Video Content Analysis) triggered recording and capture, you must configure the motion detection settings, alarm input settings or VCA settings as well. For detailed information, refer to *Chapter 8.1, Chapter 8.2 and Chapter 5.5*.
- The VCA settings are only available to the smart IP cameras.

Repeat the above edit schedule steps to schedule recording for other days in the week. You can click **Copy** to enter the Copy to interface to copy the schedule settings to other days

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

Draw the schedule:

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

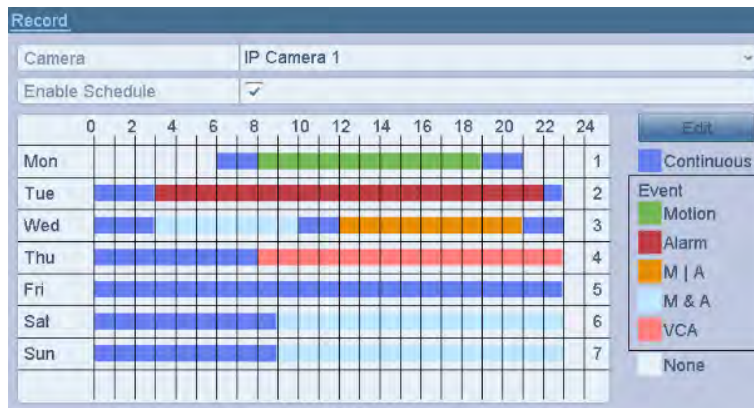


Figure 5. 9 Draw the Schedule

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

5.3 Configuring Motion Detection Recording

Purpose:

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

Steps:

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

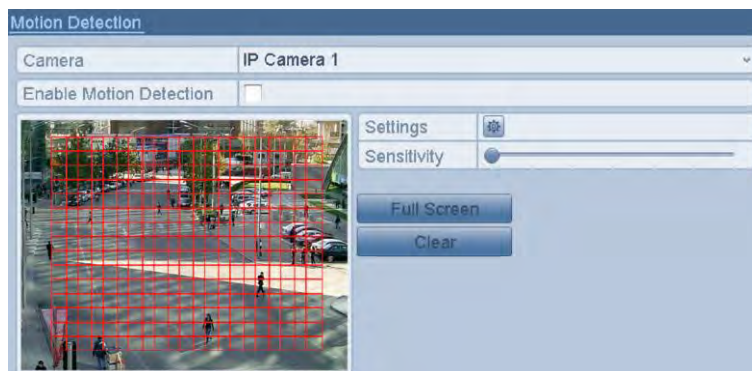


Figure 5. 10 Motion Detection- Mask

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

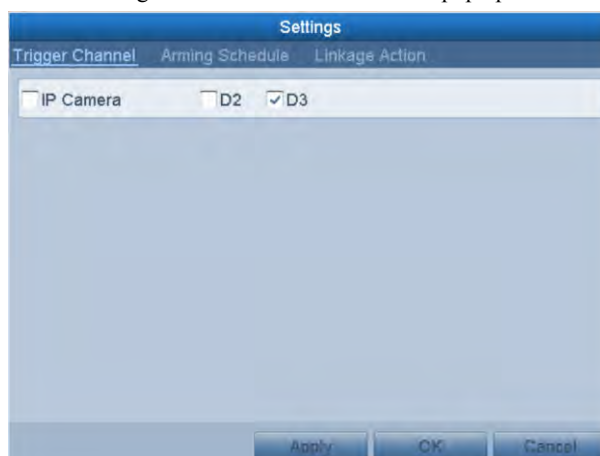


Figure 5. 11 Motion Detection Handling

- 5) Select the channels which you want the motion detection event to trigger recording.
- 6) Click **Apply** to save the settings.
- 7) Click **OK** to back to the upper level menu.

- 8) Exit the Motion Detection menu.
3. Edit the Motion Detection Record Schedule. For the detailed information of schedule configuration, see *Chapter 5.2 Configuring Recording Schedule*.

5.4 Configuring Alarm Triggered Recording

Purpose:

Follow the procedure to configure alarm triggered recording.

Steps:

1. Enter the Alarm setting interface.

Menu > Configuration > Alarm



Figure 5. 12 Alarm Settings

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

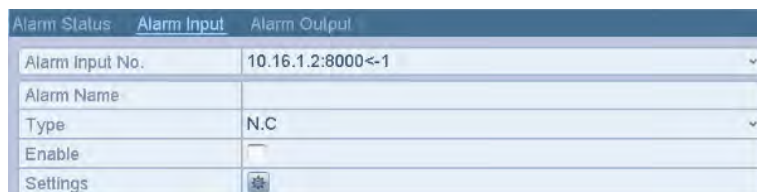


Figure 5. 13 Alarm Settings- Alarm Input

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



Figure 5. 14 Alarm Settings

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

Repeat the above steps to configure other alarm input parameters.

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



Figure 5. 15 Copy Alarm Input

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

5.5 Configuring VCA Event Recording

Purpose:

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

Steps:

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

Menu > Camera > VCA

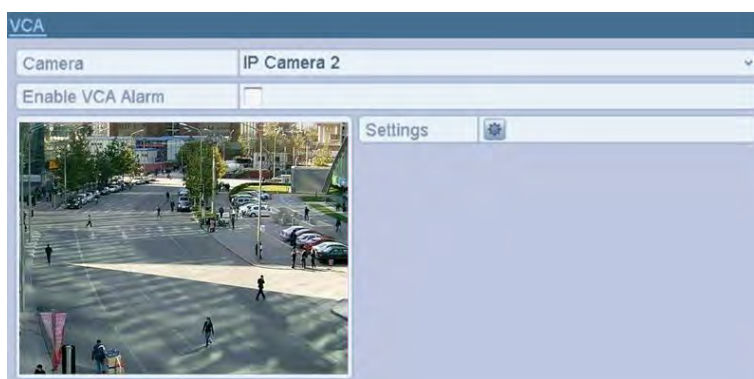



Figure 5. 16 VCA Settings

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

Click **Apply** to save the settings

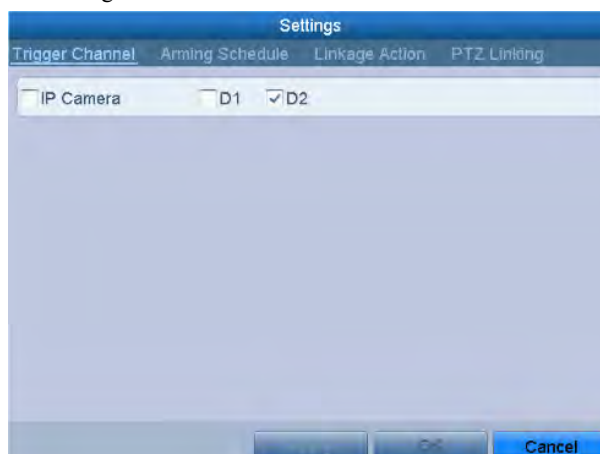


Figure 5. 17 Set Trigger Camera of VCA Alarm



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

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

5.6 Manual Recording

Purpose:

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

Steps:

1. Enter the Manual settings interface.

Menu > Manual

Or press the **REC/SHOT** button on the front panel.

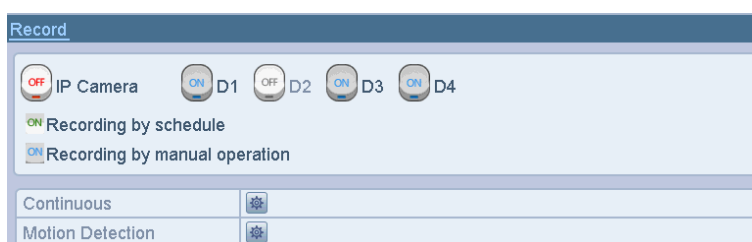






Figure 5. 18 Manual Record

2. Enable the Manual Record.


1) Select **Record** on the left bar.

2) Click the status button before camera number to change  to .

3. Disable manual record.

Click the status button to change  to .



Green icon  means that the channel is configured the record schedule. After rebooting, all the manual records enabled will be canceled.

5.7 Configuring Holiday Recording

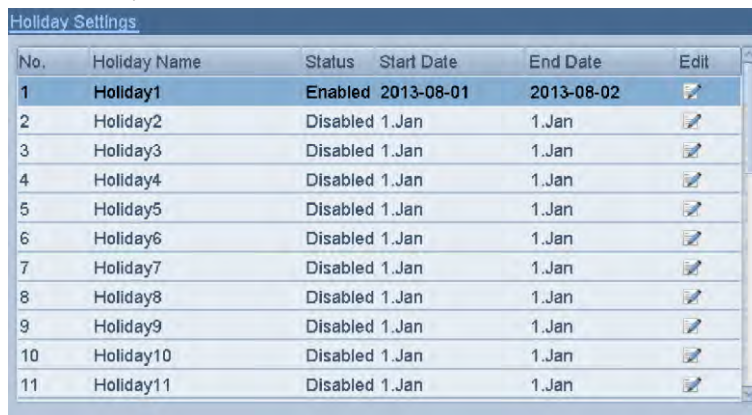
Purpose:

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

Steps:

1. Enter the Record setting interface.


Menu > Record > Holiday

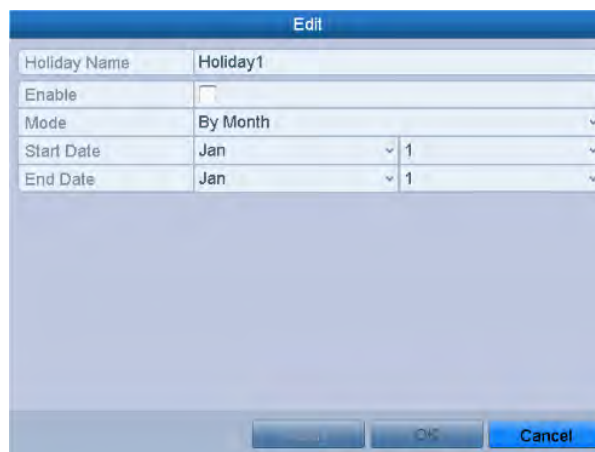


No.	Holiday Name	Status	Start Date	End Date	Edit
1	Holiday1	Enabled	2013-08-01	2013-08-02	
2	Holiday2	Disabled	1.Jan	1.Jan	
3	Holiday3	Disabled	1.Jan	1.Jan	
4	Holiday4	Disabled	1.Jan	1.Jan	
5	Holiday5	Disabled	1.Jan	1.Jan	
6	Holiday6	Disabled	1.Jan	1.Jan	
7	Holiday7	Disabled	1.Jan	1.Jan	
8	Holiday8	Disabled	1.Jan	1.Jan	
9	Holiday9	Disabled	1.Jan	1.Jan	
10	Holiday10	Disabled	1.Jan	1.Jan	
11	Holiday11	Disabled	1.Jan	1.Jan	

Figure 5. 19 Holiday Settings

2. Enable Edit Holiday schedule.

- 1) Click  to enter the Edit interface.



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

Figure 5. 20 Edit Holiday Settings

- 2) Check the checkbox after **Enable Holiday**.
 - 3) Select Mode from the dropdown list.
There are three different modes for the date format to configure holiday schedule.
 - 4) Set the start and end date.
 - 5) Click **Apply** to save settings.
 - 6) Click **OK** to exit the Edit interface.
3. Enter Record Schedule settings interface to edit the holiday recording schedule. See *Chapter 5.2 Configuring Recording Schedule*.

5.8 Configuring Redundant Recording

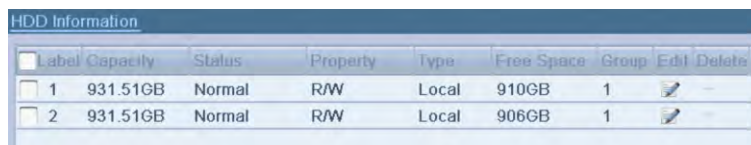
Purpose:

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

Steps:

1. Enter HDD Information interface.

Menu > HDD



Label	Capacity	Status	Property	Type	Free Space	Group	Edit	Delete
1	931.51GB	Normal	R/W	Local	910GB	1		
2	931.51GB	Normal	R/W	Local	906GB	1		

Figure 5. 21 HDD General

2. Select the **HDD** and click to enter the Local HDD Settings interface.

- 1) Set the HDD property to **Redundancy**.



Local HDD Settings

HDD No. 2

HDD Property

R/W

Read-only

Redundancy

Group 1 2 3 4 5 6 7 8
 9 10 11 12 13 14 15 16

HDD Capacity 931.51GB

Apply OK Cancel

Figure 5. 22 HDD General-Editing

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



You must set the Storage mode in the HDD advanced settings to Group before you set the HDD property to Redundant. For detailed information, please refer to *Chapter 12.3.2 Setting HDD Property*. There should be at least another HDD which is in Read/Write status.

3. Enter the Record setting interface.

Menu > Record > Parameters

- 1) Select **Record** tab.
- 1) Click **More Settings** to enter the following interface.



Figure 5. 23 Record Parameters

- 2) Check the **checkbox** of **Redundant Record**.
 - 3) Click **OK** to save settings and back to the upper level menu.
- Repeat the above steps for configuring other channels.

5.9 Configuring HDD Group for Recording

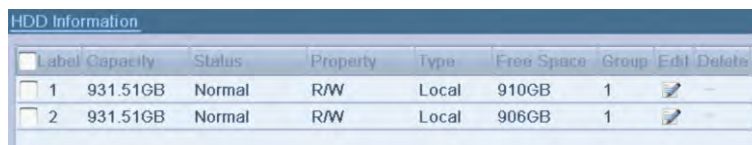
Purpose:

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

Steps:

1. Enter HDD setting interface.

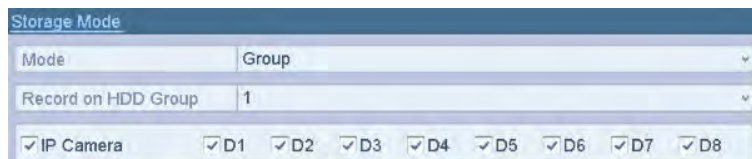
Menu > HDD



Label	Capacity	Status	Property	Type	Free Space	Group	Edit	Delete
1	931.51GB	Normal	R/W	Local	910GB	1		
2	931.51GB	Normal	R/W	Local	906GB	1		

Figure 5. 24 HDD General

2. Select **Advanced** on the left side menu.



Storage Mode

Mode: Group

Record on HDD Group: 1

IP Camera D1 D2 D3 D4 D5 D6 D7 D8

Figure 5. 25 Storage Mode

Check whether the storage mode of the HDD is Group. If not, set it to Group. For detailed information, please refer to *Chapter 12.3 Managing HDD Group*.

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

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



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

5.10 Files Protection

Purpose:

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

5.10.1 Locking the Recording Files

Lock File when Playback

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.

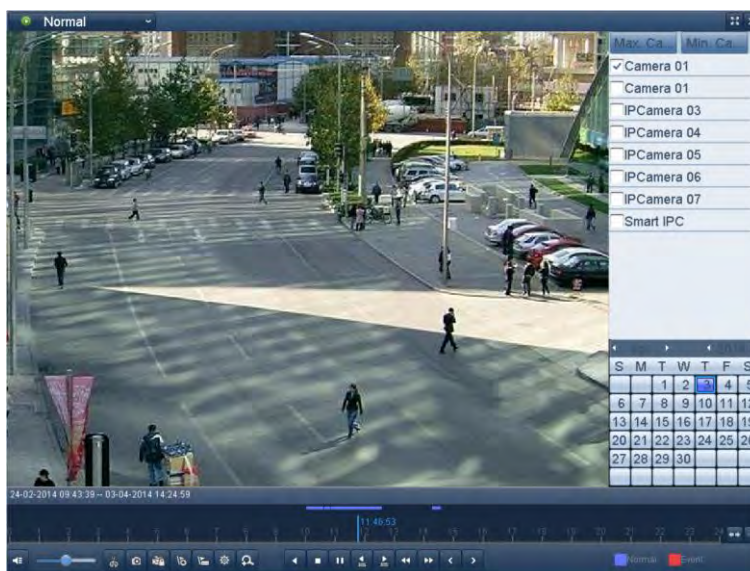





Figure 5. 26 Normal Playback

3. During playback, click the  button to lock the current recording file.



In the multi-channel playback mode, clicking the  button will lock all the record files related to the playback channels.

4. You can click the  button to pop up the file management interface. Click the **Locked File** tab to check and export the locked files.

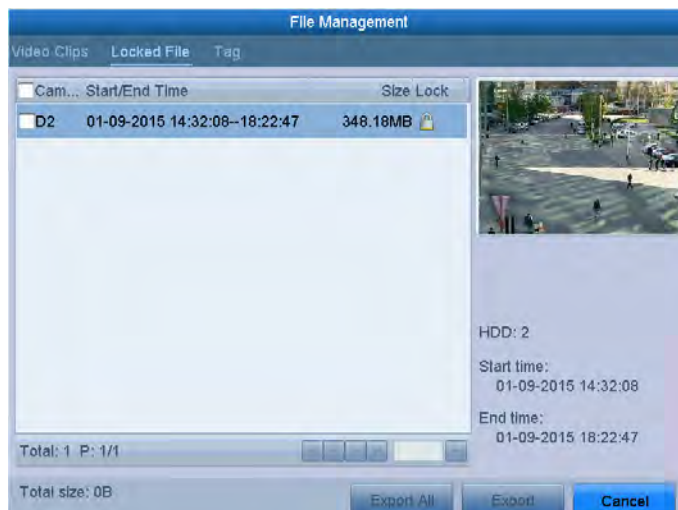


Figure 5. 27 Locked File Management

In the File Management interface, you can also click to change it to to unlock the file and the file is not protected.

● **Lock File when Export**

Steps:

1. Enter Export setting interface.
Menu > Export

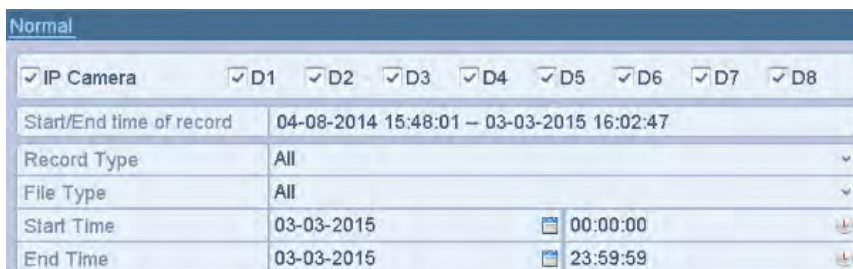


Figure 5. 28 Export

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

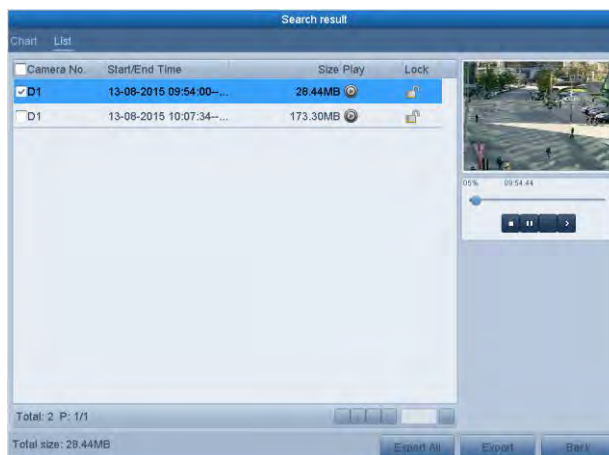






Figure 5. 29 Export- Search Result

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.



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

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

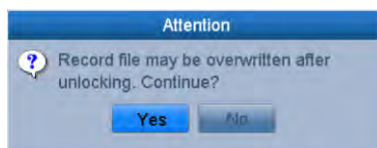


Figure 5. 30 Unlocking Attention

5.10.2 Setting HDD Property to Read-only

Steps:

1. Enter HDD setting interface.
Menu > HDD






HDD Information									
<input type="checkbox"/>	Label	Capacity	Status	Property	Type	Free Space	Group	Edit	Delete
<input type="checkbox"/>	1	931.51GB	Normal	R/W	Local	910GB	1		
<input type="checkbox"/>	2	931.51GB	Normal	R/W	Local	906GB	1		

Figure 5. 31 HDD General

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

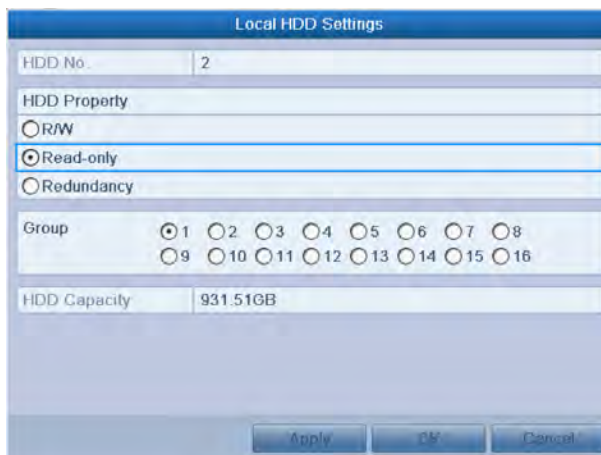


Figure 5. 32 HDD General- Editing



To edit HDD property, you need to set the storage mode of the HDD to Group. See *Chapter 12.3 Managing HDD Group*.

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



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

Chapter 6 Playback

6.1 Playing Back Record Files


6.1.1 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

Step:

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



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

1. Enter the Playback interface.


Mouse: right click a channel in live view mode and select Playback button  from the menu, as shown in Figure 6. 2.



Figure 6. 2 Right-click Menu under Live View



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

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



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 use the toolbar in the bottom part of Playback interface to control playing progress.

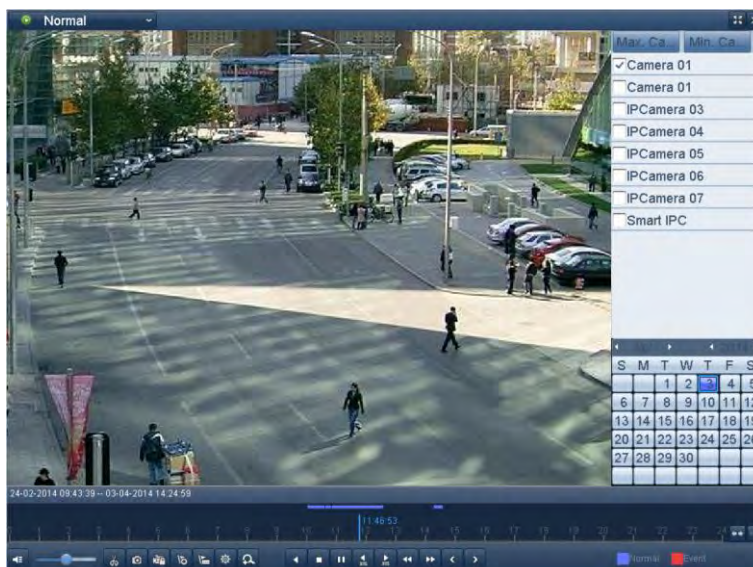


Figure 6. 4 Playback Interface

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



Figure 6. 5 Toolbar of Playback



- The **14-01-2015 22:15:23 -- 03-03-2015 09:49:37** indicates the start/end time of the record.
- Playback progress bar: use the mouse to click any point of the progress bar or drag the progress bar to locate specific frames.

Table 6. 1 Detailed Explanation of Playback Toolbar

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

6.1.3 Playing Back by Event Search

Purpose:

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

Steps:

1. Enter the Playback interface.
Menu > Playback
2. Select the **Event** in the drop-down list on the top-left side.
3. Select **Alarm Input**, **Motion** or **VCA** as the event type.



Here we take playback by VCA as the example.

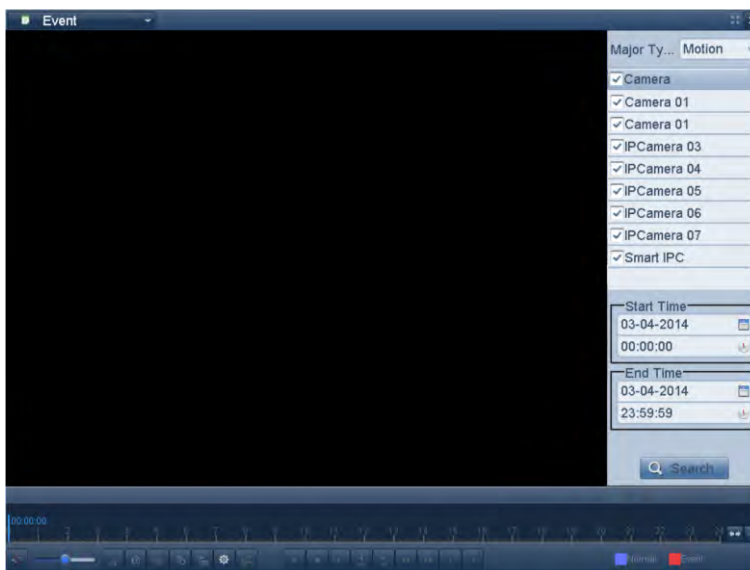



Figure 6. 6 Motion Search Interface

4. Select the minor type of VCA from the drop-down list.



For configuring the VCA recording, please refer to *Chapter 5.5 Configuring VCA Event Recording*.

5. Select the camera (s) for searching, and set the Start time and End time.
6. Click **Search** button to get the search result information. You may refer to the right-side bar for the result.
7. Click  button to play back the file.



Pre-play and post-play can be configured.

8. Playback interface.

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

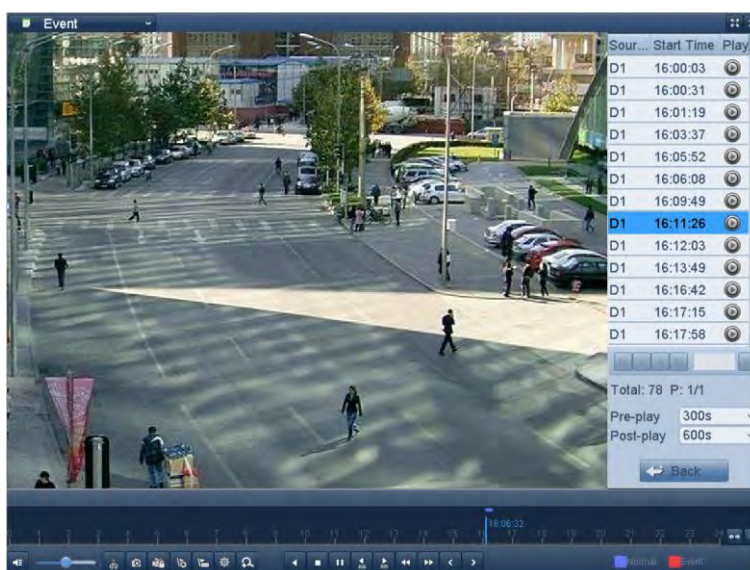




Figure 6. 7 Interface of Playback by Event

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 can 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* for the detailed information about searching and playback of the record files.

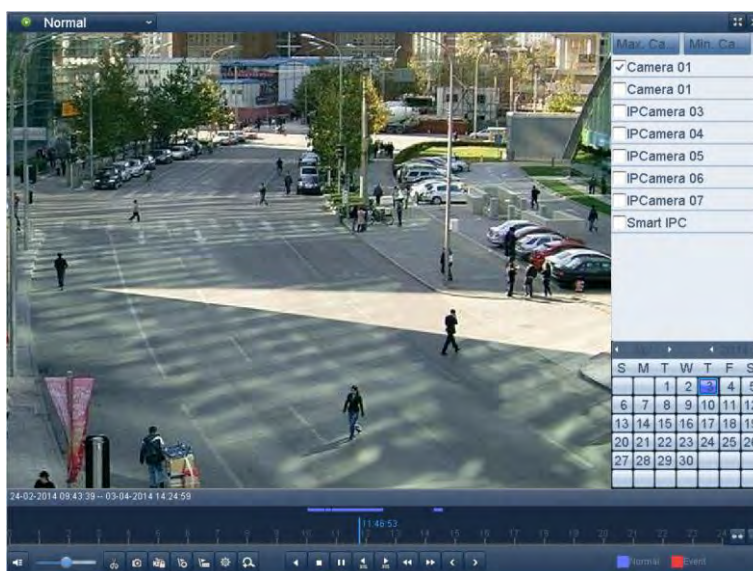



Figure 6. 8 Interface of Playback by Time

Click  button to add default tag.

Click  button to add customized tag and input tag name.



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

3. Tag management.


Click  button to enter the File Management interface and click **Tag** to manage the tags. You can check, edit and delete tag(s).



Figure 6. 9 Tag Management Interface

Playing back by Tag

Steps:

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



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

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

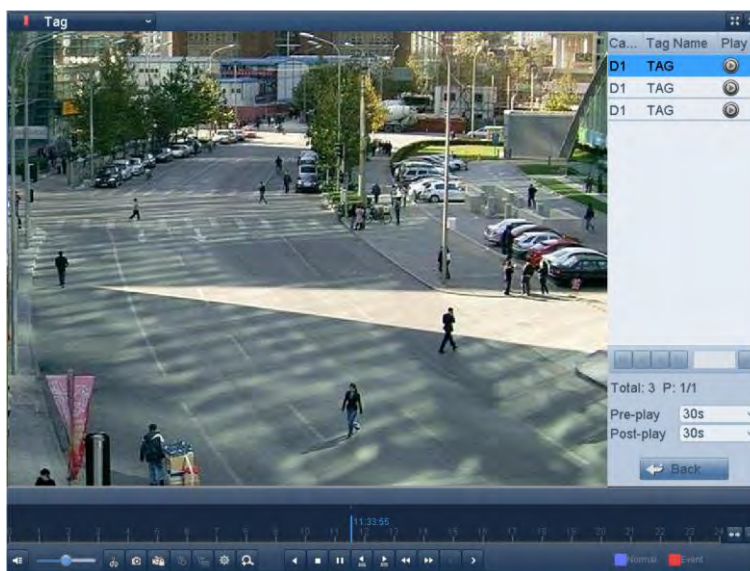


Figure 6. 10 Interface of Playback by Tag



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 Playback

Purpose:

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

Before you start:

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

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

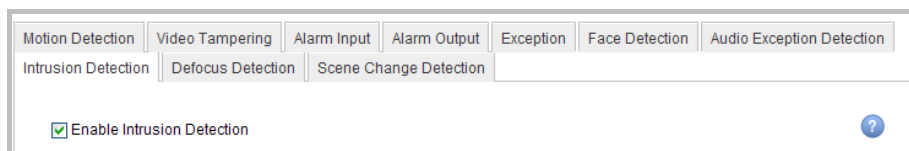



Figure 6. 11 Setting Intrusion Detection on IP Camera

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

Steps:

1. Enter Playback interface.
Menu > Playback
2. Select the **Smart** in the drop-down list on the top-left side.
3. Select a camera in the camera list.
4. Select a date in the calendar and click the  button on the left toolbar to play the video file.

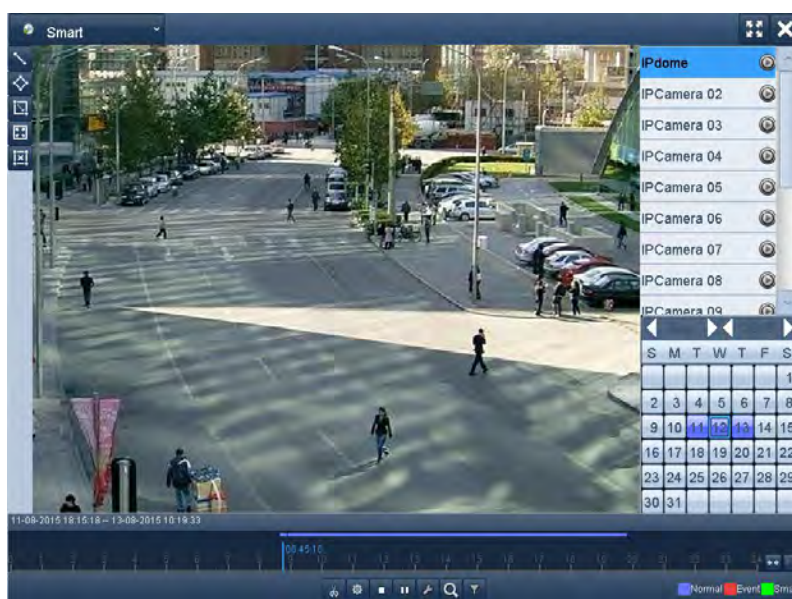















Figure 6. 12 Smart Playback Interface

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. You can click  to configure the smart settings.



Figure 6. 13 Smart Settings


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


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

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



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

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.

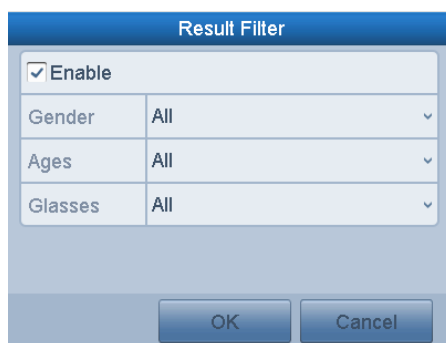


Figure 6. 14 Set Result Filter

6.1.6 Playing Back by System Logs

Purpose:


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

Steps:

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



Figure 6. 15 System Log Search Interface

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

No.	Major Type	Time	Minor Type	Parameter	Play	Details
1	Operation	03-03-2015 08:33:35	Power On	N/A	—	✓
2	Information	03-03-2015 08:33:35	Local HDD Infor...	N/A	—	✓
3	Operation	03-03-2015 08:33:38	Local Operation:...	N/A	—	✓
4	Information	03-03-2015 08:34:03	HDD S.M.A.R.T.	N/A	—	✓
5	Operation	03-03-2015 08:56:02	Local Operation:...	N/A	⏸	✓
6	Operation	03-03-2015 08:56:02	Local Operation:...	Preview	—	✓
7	Information	03-03-2015 08:56:05	Start Recording	N/A	⏸	✓
8	Operation	03-03-2015 08:56:33	Local Operation:...	N/A	⏸	✓
9	Operation	03-03-2015 08:56:33	Local Operation:...	Preview	—	✓
10	Information	03-03-2015 08:56:36	Start Recording	N/A	⏸	✓
11	Alarm	03-03-2015 08:56:38	Alarm Input	N/A	—	✓
12	Operation	03-03-2015 08:58:55	Remote Operati...	Alarm	—	✓
13	Operation	03-03-2015 08:59:10	Remote Operati...	Network	—	✓
14	Operation	03-03-2015 08:59:10	Remote Operati...	Network	—	✓

Total: 253 P: 1/3

Figure 6. 16 Result of System Log Search

4. Playback interface.

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



Figure 6. 17 Interface of Playback by Log

6.1.7 Playing Back External File

Purpose:

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

Steps:

1. Enter Tag Search interface.
Menu > Playback
2. Select the **External File** in the drop-down list on the top-left side.
The files are listed in the right-side list.
You can click the **Refresh** button to refresh the file list.
3. Select and click the button to play back it. And you can adjust the playback speed by clicking and .

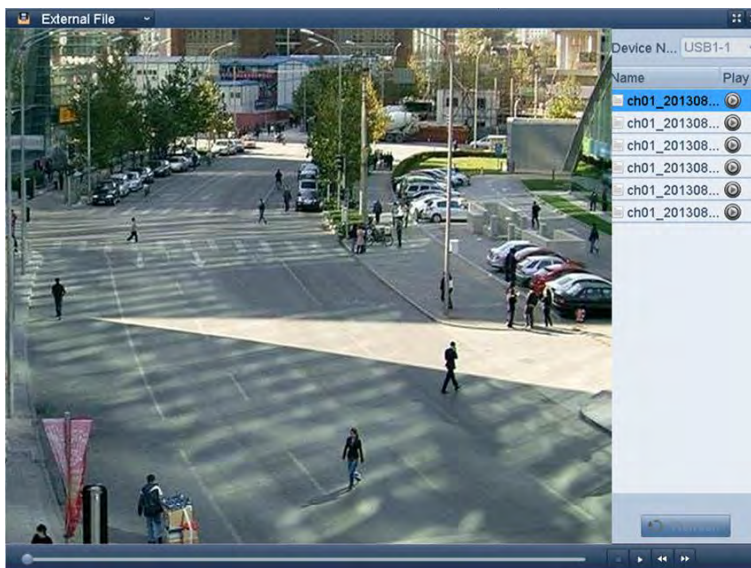


Figure 6. 18 Interface of External File Playback

6.1.8 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.

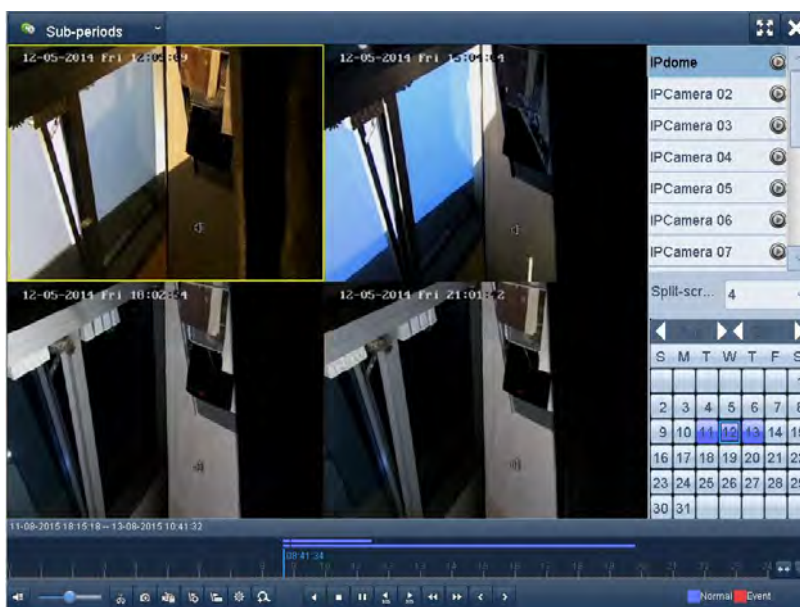


Figure 6. 19 Interface of Sub-periods Playback



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.

Chapter 7 Backup

7.1 Backing up Record Files

7.1.1 Backing up by Normal Video Search

Purpose:

The record files can be backup to various devices, such as USB devices (USB flash drives, USB HDDs, USB writer), 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. The matched video files are displayed in Chart or List display mode.

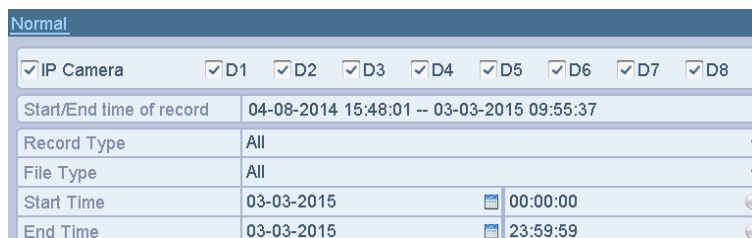



Figure 7. 1 Normal Video Search for Backup

4. Select video files or pictures from the Chart or List to export.
Click  to play the record file if you want to check it.
Check the checkbox before the record files you want to back up.



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

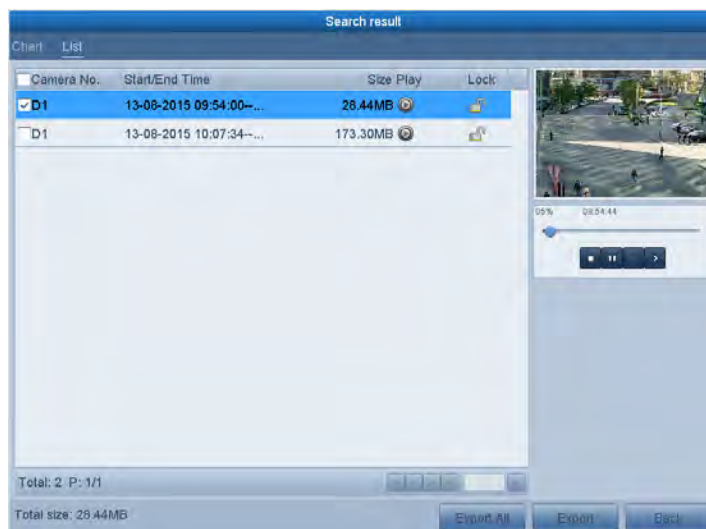


Figure 7. 2 Result of Normal Video Search for Backup

5. Export the video files or picture files.

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

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



If the inserted USB device is not recognized:

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

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



Figure 7.3 Export by Normal Video Search using USB Flash Drive

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

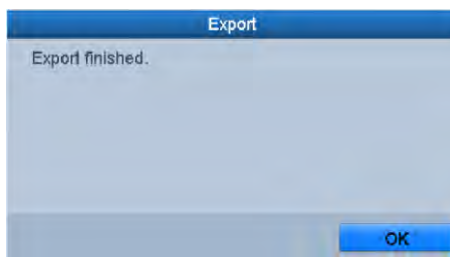


Figure 7.4 Export Finished



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. 5 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.

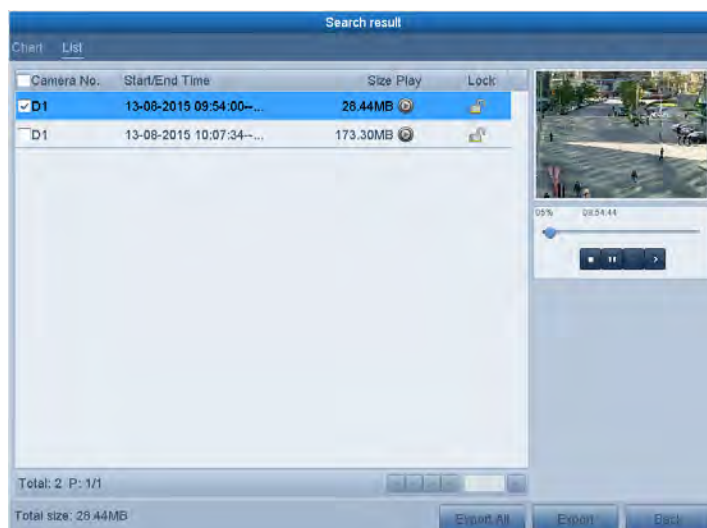


Figure 7. 6 Result of Event Search


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), SATA writer or eSATA HDD.

Steps:

1. Enter Playback interface.
Please refer to *Chapter 6.1 Playing Back Record Files*.
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.

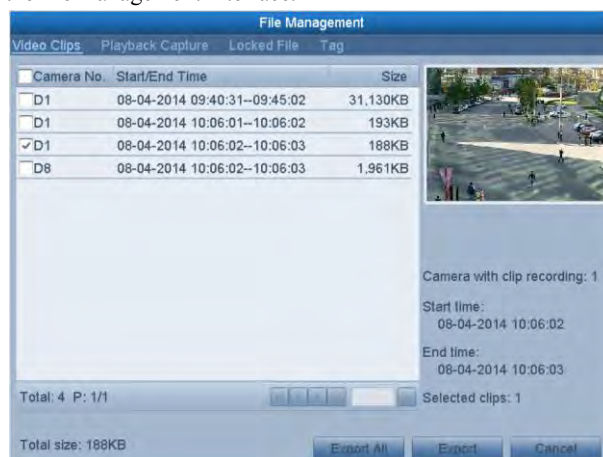


Figure 7.7 Video Clips Export Interface

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.

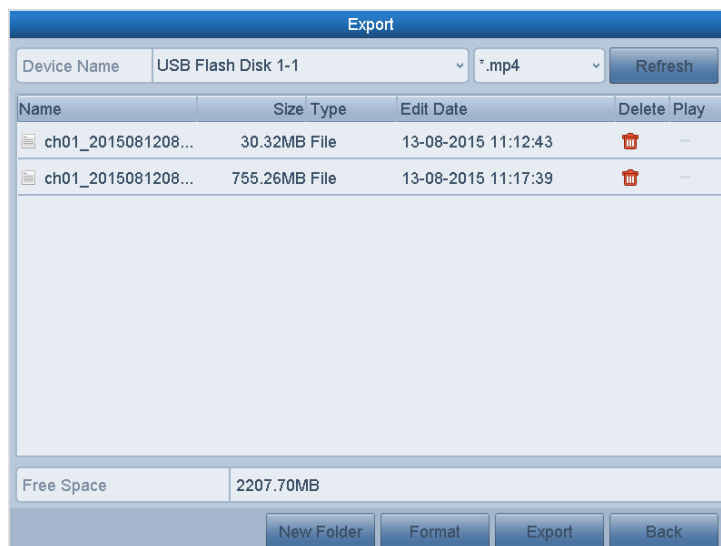


Figure 7. 8 Storage Device Management

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.



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 Alarm

Steps:

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


Menu > Camera > Motion

2. Set up detection area and sensitivity.

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



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

Click  button and set alarm response actions.

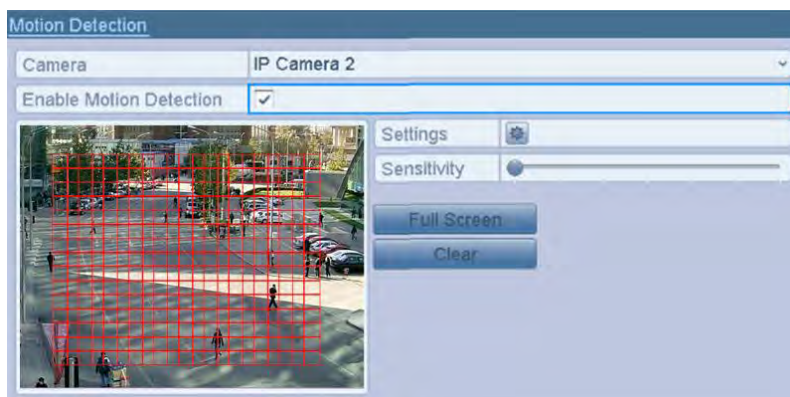


Figure 8. 1 Motion Detection Setup Interface

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, and click **Apply** to save the settings.

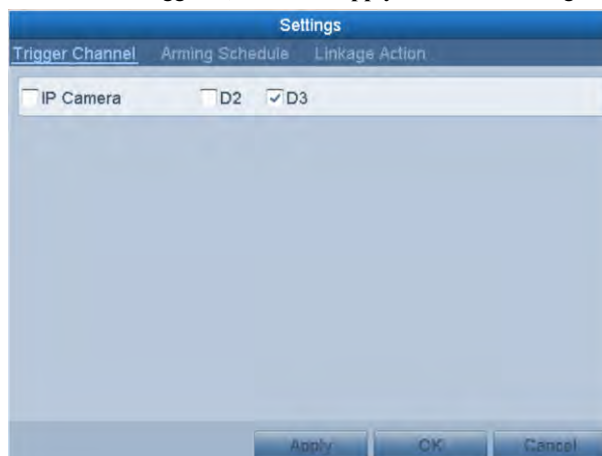


Figure 8. 2 Set Trigger Camera of Motion Detection

4. Set up arming schedule of the channel.
 - 1) Select Arming Schedule tab to set the arming schedule of handling actions for the motion detection.
 - 2) Choose one day of a week and up to eight time periods can be set within each day.
 - 3) Click **Apply** to save the settings



Time periods shall not be repeated or overlapped.

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

Figure 8. 3 Set Arming Schedule of Motion Detection

5. Click **Handling** tab to set up alarm response actions of motion alarm (please refer to *Chapter 8.6 Setting Alarm Response Actions*).
6. If you want to set motion detection for another channel, repeat the above steps or just click **Copy** in the Motion Detection interface to copy the above settings to it.

8.2 Setting Sensor Alarms

Purpose:

Set the handling action of an external sensor alarm.

Steps:

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

Menu> Configuration> Alarm

Select Alarm Input tab to enter Alarm Input Settings interface.



Figure 8. 4 Alarm Status Interface of System Configuration

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

Check the **Enable** checkbox and click **Settings** button to set up its alarm response actions.

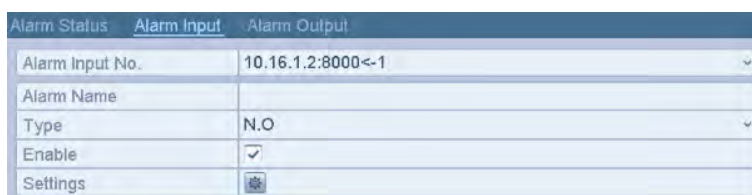


Figure 8. 5 Alarm Input Setup Interface

3. Select Trigger Channel tab and select one or more channels which will start to record or become full-screen monitoring when an external alarm is input, and click **Apply** to save the settings.
4. Select **Arming Schedule** tab to set the arming schedule of handling actions.



Figure 8. 6 Set Arming Schedule of Alarm Input

Choose one day of a week and Max. eight time periods can be set within each day, and click **Apply** to save the settings.



Time periods shall not be repeated or overlapped.

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

5. Select **Linkage Action** tab to set up alarm response actions of the alarm input (please refer to *Chapter 8.6 Setting Alarm Response Actions*).
6. If necessary, select **PTZ Linking** tab and set PTZ linkage of the alarm input.
Set PTZ linking parameters and click **OK** to complete the settings of the alarm input.



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. 7 Set PTZ Linking of Alarm Input

7. If you want to set handling action of another alarm input, repeat the above steps.
Or you can click the **Copy** button on the Alarm Input Setup interface and check the checkbox of alarm

inputs to copy the settings to them.



Figure 8. 8 Copy Settings of Alarm Input

8.3 Detecting Video Loss Alarm

Purpose:

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

Steps:

1. Enter Video Loss interface of Camera Management and select a channel you want to detect.

Menu > Camera > Video Loss

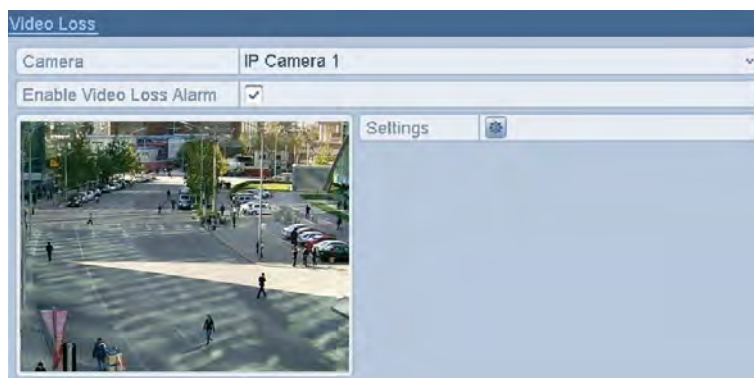



Figure 8. 9 Video Loss Setup Interface

2. Set up handling action of video loss.

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

3. Set up arming schedule of the handling actions.

- 1) Select Arming Schedule tab to set the channel’s arming schedule.
- 2) Choose one day of a week and up to eight time periods can be set within each day.
- 3) Click **Apply** button to save the settings.



Time periods shall not be repeated or overlapped.

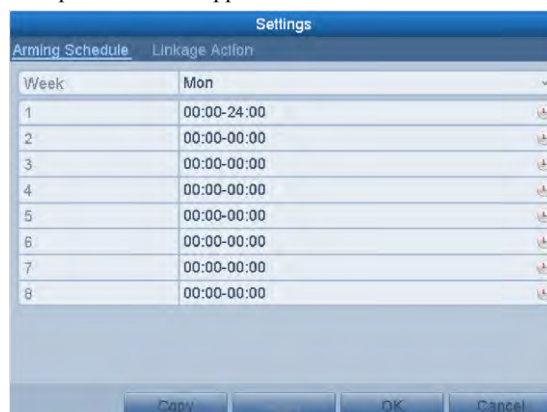


Figure 8. 10 Set Arming Schedule of Video Loss

4. Select **Linkage Action** tab to set up alarm response action of video loss (please refer to *Chapter 8.6 Setting Alarm Response Actions*).
5. Click the **OK** button to complete the video loss settings of the channel.

8.4 Detecting Video Tampering Alarm

Purpose:

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


Steps:

1. Enter Video Tampering interface of Camera Management and select a channel you want to detect video tampering.

Menu> Camera> Video Tampering



Figure 8. 11 Video Tampering Setup Interface

2. Set the video tampering handling action of the channel.
 - Check the checkbox of **Enable Video Tampering Detection**.
 - Drag the sensitivity bar to set a proper sensitivity level. Use the mouse to draw an area you want to detect video tampering.
 - Click  button to set up handling action of video tampering.
3. Set arming schedule and alarm response actions of the channel.
 - 1) Click Arming Schedule tab to set the arming schedule of handling actions.
 - 2) Choose one day of a week and max. eight time periods can be set within each day.
 - 3) Click **Apply** button to save the settings.



Time periods shall not be repeated or overlapped.

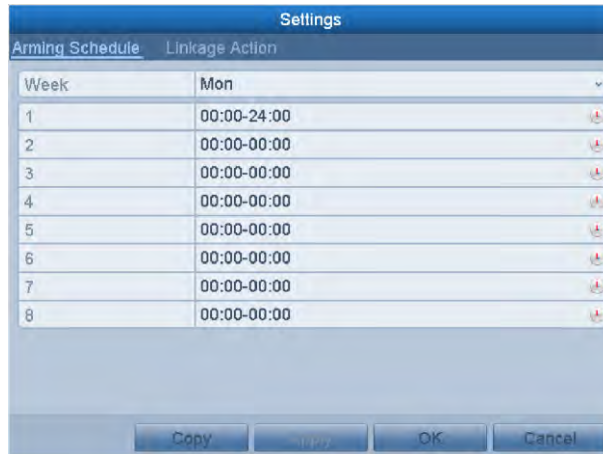


Figure 8. 12 Set Arming Schedule of Video Tampering

4. Select **Linkage Action** tab to set up alarm response actions of video tampering alarm (please refer to *Chapter 8.6 Setting Alarm Response Actions*).
5. Click the **OK** button to complete the video tampering settings of the channel.

8.5 Handling Exceptions Alarm

Purpose:

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

- **HDD Full:** The HDD is full.
- **HDD Error:** Writing HDD error or unformatted HDD.
- **Network Disconnected:** Disconnected network cable.
- **IP Conflicted:** Duplicated IP address.
- **Illegal Login:** Incorrect user ID or password.
- **Record Exception:** No space for saving recorded files.
- **PoE Power Overload:** The power consumption of the connected cameras via the PoE interface exceeds the maximum PoE power.

Steps:

Enter Exception interface of System Configuration and handle various exceptions.

Menu> Configuration> Exceptions

Please refer to *Chapter 8.6 Setting Alarm Response Actions* for detailed alarm response actions.

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

Figure 8. 13 Exceptions Setup Interface

8.6 Setting Alarm Response Actions

Purpose:

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

Event Hint Display

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

Steps:

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

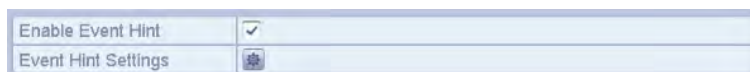


Figure 8. 14 Event Hint Settings Interface


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



Figure 8. 15 Event Hint Settings Interface

4. Click the **OK** button to finish settings.

Full Screen Monitoring

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

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

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



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

Audible Warning

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

Notify Surveillance Center

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



The alarm signal will be transmitted automatically at detection mode when remote alarm host is configured. Please refer to *Chapter 11.2.5 Configuring Remote Alarm Host* for details of alarm host configuration.

Email Linkage

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

Please refer to *Chapter 11.2.9* for details of Email configuration.

Trigger Alarm Output

Trigger an alarm output when an alarm is triggered.

1. Enter Alarm Output interface.

Menu> Configuration> Alarm> Alarm Output

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



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

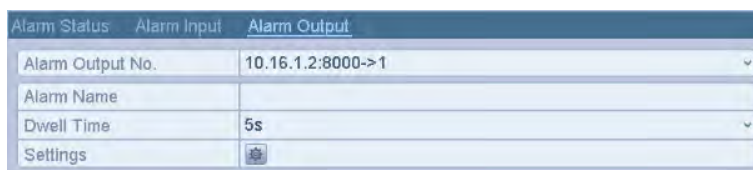


Figure 8. 16 Alarm Output Setup Interface

2. Set up arming schedule of the alarm output.

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



Time periods shall not be repeated or overlapped.

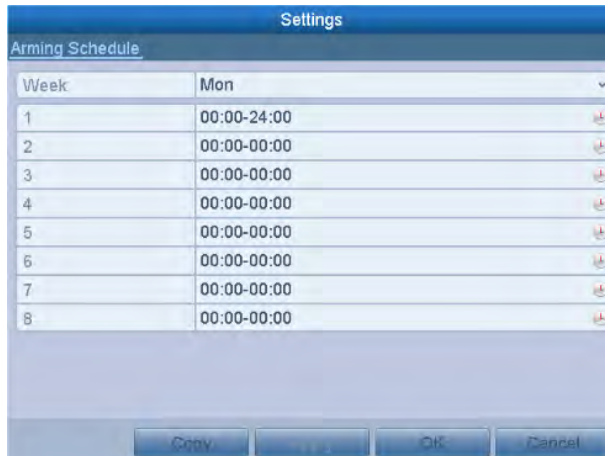


Figure 8. 17 Set Arming Schedule of Alarm Output

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

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

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



Figure 8. 18 Copy Settings of Alarm Output

8.7 Triggering or Clearing Alarm Output Manually

Purpose:

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

Steps:

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

Menu> Manual> Alarm

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

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

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

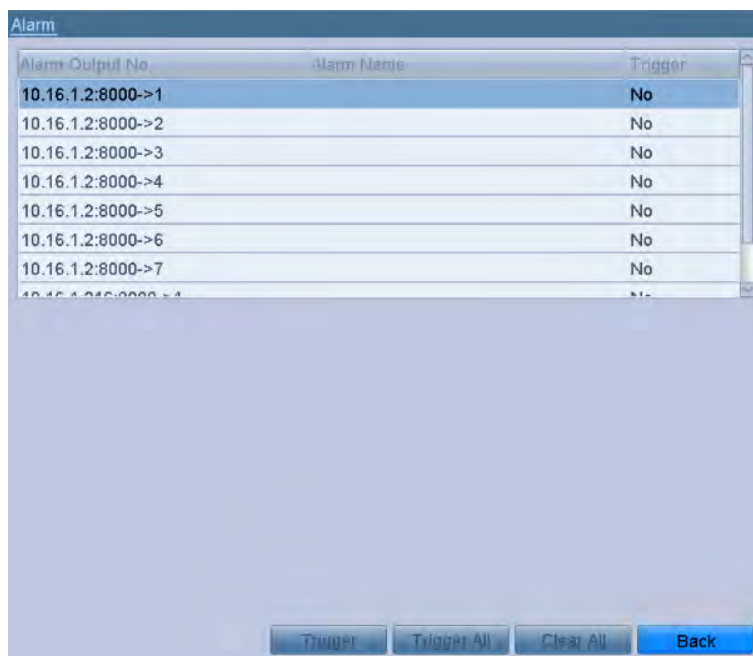


Figure 8. 19 Clear or Trigger Alarm Output Manually

Chapter 9 VCA Alarm



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

9.1 Face Detection

Purpose:

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

Steps:

1. Enter the VCA settings interface.
Menu> Camera> VCA
2. Select the camera to configure the VCA.
You can click the checkbox of **Save VCA Picture** to save the captured pictures of VCA detection.

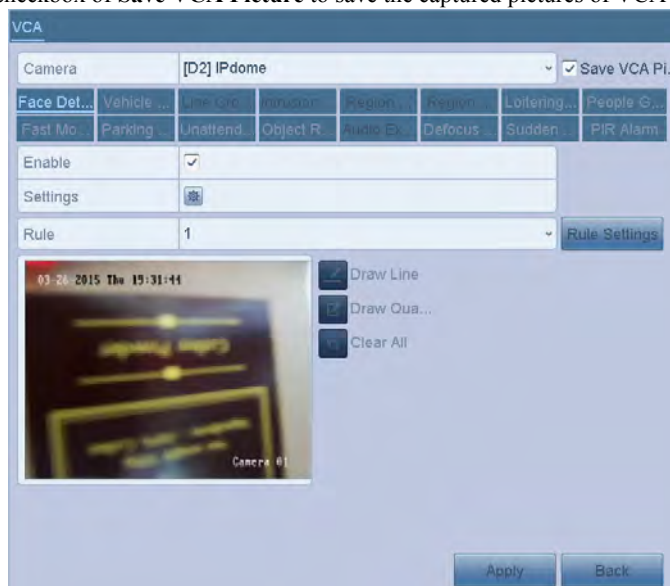



Figure 9. 1 Face Detection

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

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



Figure 9. 2 Set Face Detection Sensitivity

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

9.2 Vehicle Detection

Purpose:

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

Steps:

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

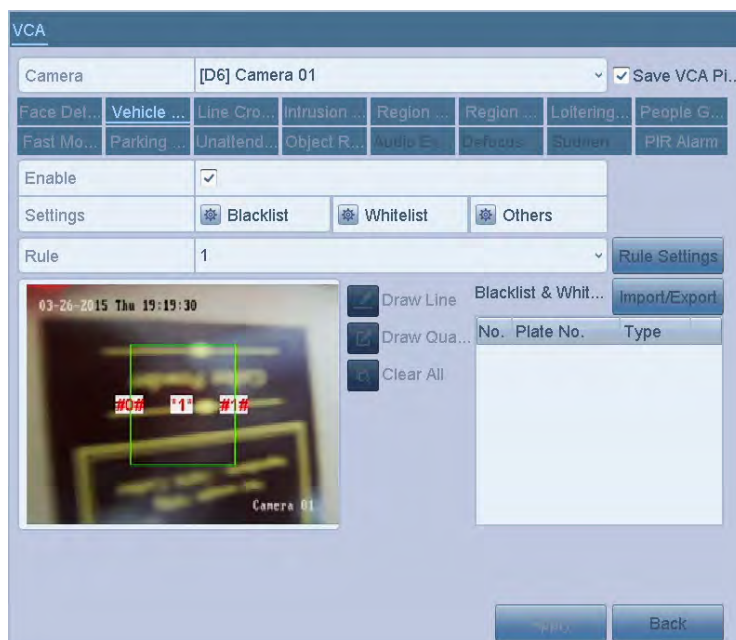



Figure 9. 3 Set Vehicle Detection

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

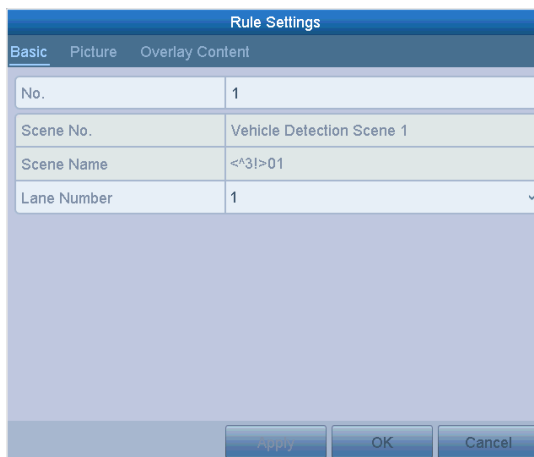


Figure 9. 4 Rule Settings

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




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

9.3 Line Crossing Detection

Purpose:

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

Steps:

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


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


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

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



Figure 9. 5 Set Line Crossing Detection Rules

7. Click  and set two points in the preview window to draw a virtual line.

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



Up to 4 rules can be configured.



Figure 9. 6 Draw Line for Line Crossing Detection

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

9.4 Intrusion Detection

Purpose:

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

Steps:




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



Figure 9.7 Set Intrusion Crossing Detection Rules

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

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



Up to 4 rules can be configured.



Figure 9. 8 Draw Area for Intrusion Detection



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

9.5 Region Entrance Detection

Purpose:

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

Steps:

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


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



Figure 9.9 Set Region Entrance Detection



Up to 4 rules can be configured.

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

9.6 Region Exiting Detection

Purpose:

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



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

9.7 Loitering Detection

Purpose:

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



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

9.8 People Gathering Detection

Purpose:

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



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

9.9 Fast Moving Detection

Purpose:

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



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

9.10 Parking Detection

Purpose:

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



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

9.11 Unattended Baggage Detection

Purpose:

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



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

9.12 Object Removal Detection

Purpose:

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




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

9.13 Audio Exception Detection

Purpose:

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

Steps:

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





Rule Settings	
No.	1
Audio Loss Exception	<input checked="" type="checkbox"/>
Sudden Increase of Sound I...	<input checked="" type="checkbox"/>
Sensitivity	<input type="range" value="50"/> 50 
Sound Intensity Threshold	<input type="range" value="50"/> 50 
Sudden Decrease of Sound...	<input checked="" type="checkbox"/>
Sensitivity	<input type="range" value="50"/> 50 
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Figure 9. 10 Set Audio Exception Detection Rules

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

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

9.14 Sudden Scene Change Detection

Purpose:

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



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

9.15 Defocus Detection

Purpose:

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




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

9.16 PIR Alarm

Purpose:

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

Steps:

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

Chapter 10 VCA Search

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

10.1 Face Search

Purpose:

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

Before you start:

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

Steps:

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

Start Time	13-08-2015	00:00:00
End Time	13-08-2015	23:59:59

Figure 10. 1 Face Search

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

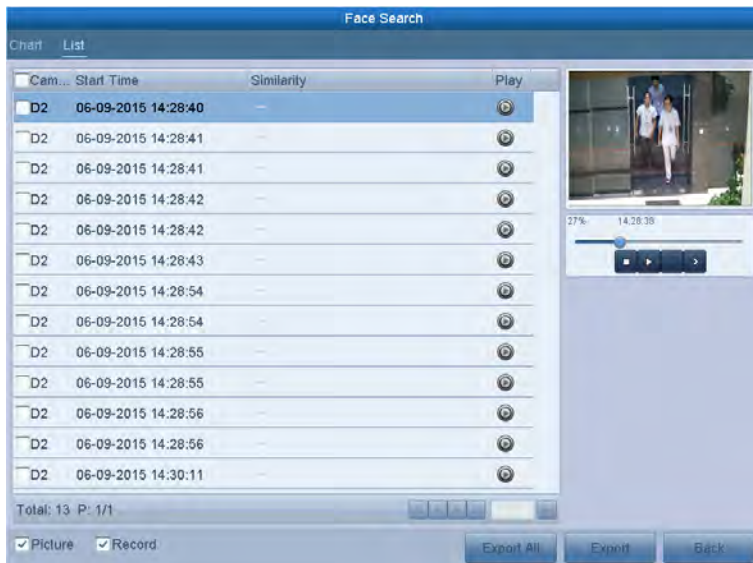






Figure 10. 2 Face Search Interface

5. Play the face picture related video file.

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

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

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

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

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

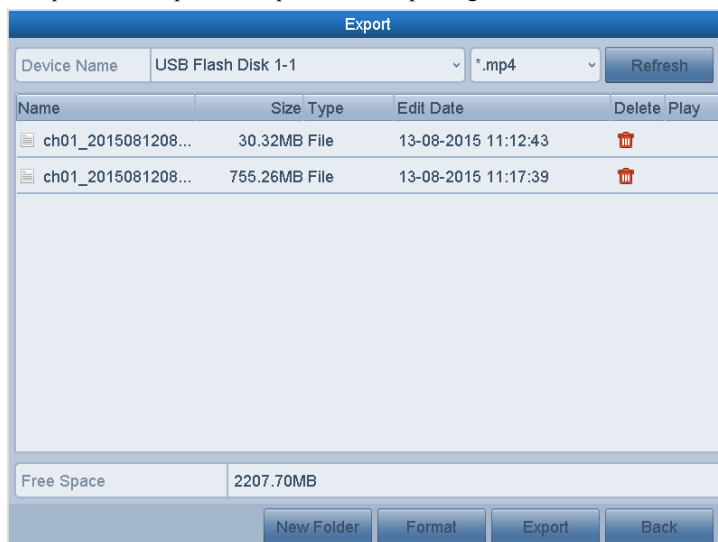


Figure 10. 3 Export Files

10.2 Behavior Search

Purpose:

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

Steps:

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

Behavior Search			
<input checked="" type="checkbox"/> IP Camera	<input checked="" type="checkbox"/> D1	<input checked="" type="checkbox"/> D2	<input checked="" type="checkbox"/> D3
	<input checked="" type="checkbox"/> D4	<input checked="" type="checkbox"/> D5	<input checked="" type="checkbox"/> D6
	<input checked="" type="checkbox"/> D7	<input checked="" type="checkbox"/> D8	<input checked="" type="checkbox"/> D9
	<input checked="" type="checkbox"/> D10	<input checked="" type="checkbox"/> D11	<input checked="" type="checkbox"/> D12
	<input checked="" type="checkbox"/> D13	<input checked="" type="checkbox"/> D14	<input checked="" type="checkbox"/> D15
	<input checked="" type="checkbox"/> D16		
Start Time	13-08-2015	00:00:00	
End Time	13-08-2015	23:59:59	
Type	All		
<input type="button" value="Search"/> <input type="button" value="Back"/>			

Figure 10. 4 Behavior Search Interface

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

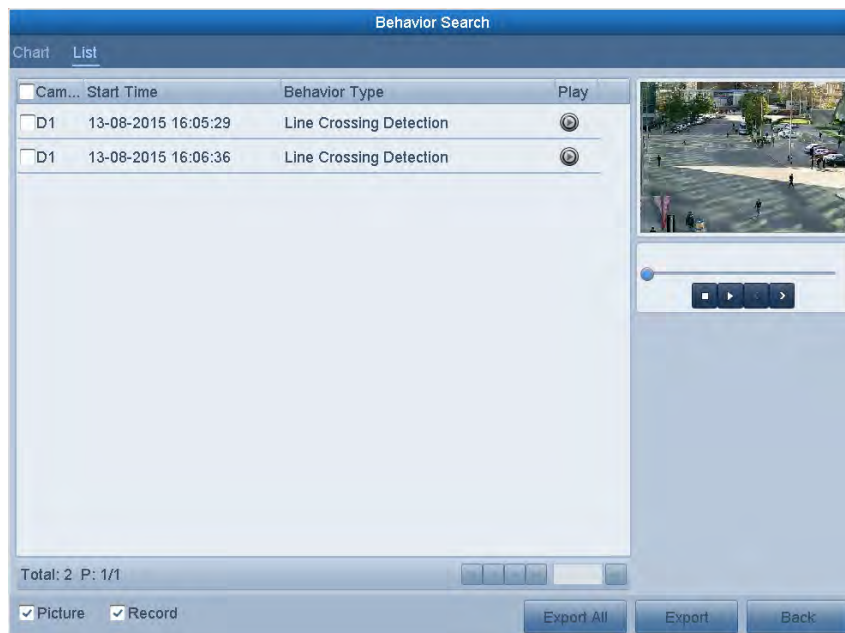


Figure 10. 5 Behavior Search Results

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

You can also click to stop the playing, or click to play the previous/next file.
7. If you want to export the captured pictures to local storage device, connect the storage device to the device and click **Export All** to enter the Export interface.
Click **Export** to export all pictures to the storage device.

10.3 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.

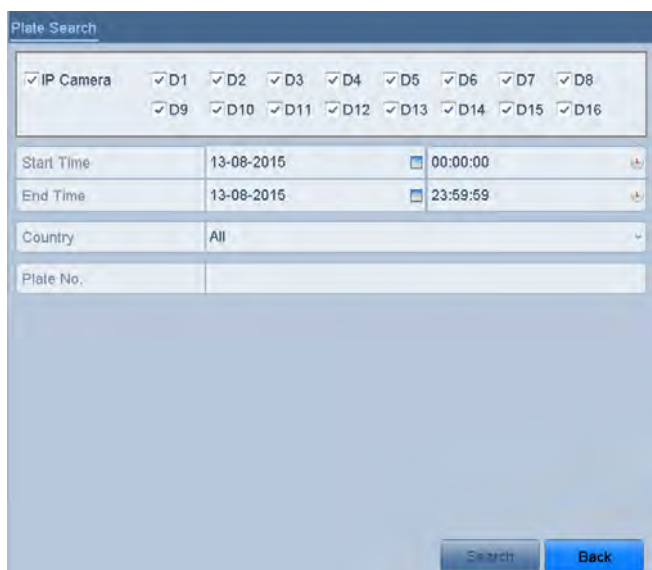


Plate Search	
<input checked="" type="checkbox"/> IP Camera	<input checked="" type="checkbox"/> D1 <input checked="" type="checkbox"/> D2 <input checked="" type="checkbox"/> D3 <input checked="" type="checkbox"/> D4 <input checked="" type="checkbox"/> D5 <input checked="" type="checkbox"/> D6 <input checked="" type="checkbox"/> D7 <input checked="" type="checkbox"/> D8
	<input checked="" type="checkbox"/> D9 <input checked="" type="checkbox"/> D10 <input checked="" type="checkbox"/> D11 <input checked="" type="checkbox"/> D12 <input checked="" type="checkbox"/> D13 <input checked="" type="checkbox"/> D14 <input checked="" type="checkbox"/> D15 <input checked="" type="checkbox"/> D16
Start Time	13-08-2015 00:00:00
End Time	13-08-2015 23:59:59
Country	All
Plate No.	
<input type="button" value="Search"/> <input type="button" value="Back"/>	

Figure 10. 6 Plate Search

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



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

10.4 People Counting

Purpose:

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

Steps:

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

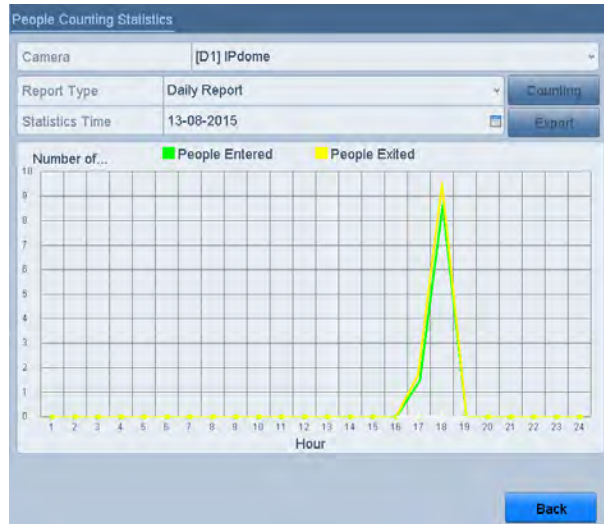


Figure 10. 7 People Counting Interface

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

10.5 Heat Map

Purpose:

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



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

Steps:

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

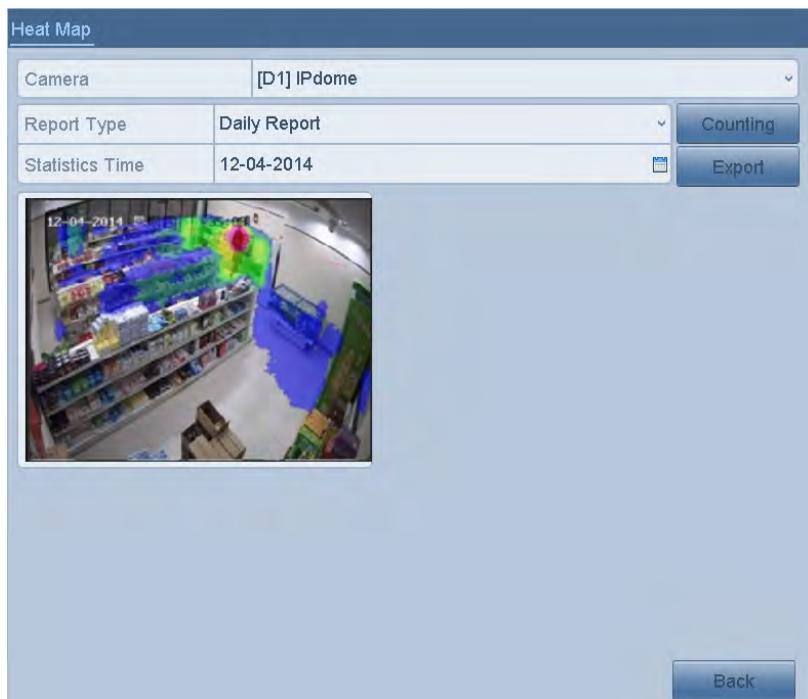


Figure 10. 8 Heat Map Interface

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



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

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

Chapter 11 Network Settings

11.1 Configuring General Settings

Purpose:

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

Steps:

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

General				Platform Access	PPPOE	DDNS	NTP	Email	NAT	More Settings	
NIC Type		10M/100M/1000M Self-adaptive									
Enable DHCP		<input checked="" type="checkbox"/>									
IPv4 Address	10	.16	.2	.109	IPv6 Address	fe80::269:6cff:fe2a:fb88/64					
IPv4 Subnet	255	.255	.255	.0	IPv6 Address						
IPv4 Default	10	.16	.2	.254	IPv6 Default						
MAC Address		00:69:6c:2a:fb:88									
MTU(Bytes)		1500									
Preferred DNS Server		10.1.7.88									
Alternate DNS Server		10.1.7.77									

Figure 11. 1 Network Settings Interface

3. In the **General Settings** interface, you can configure the following settings: Working Mode, NIC Type, IPv4 Address, IPv4 Gateway, MTU and DNS Server.
If the DHCP server is available, you can click the checkbox of **DHCP** to automatically obtain an IP address and other network settings from that server.
4. After having configured the general settings, click **Apply** button to save the settings.

Working Mode

Two 10M/100M/1000M NIC cards are provided by the VN4016 series device, which allows the device to work in the Multi-address and Net-fault Tolerance modes.

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

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

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

Working Mode	Net Fault-tolerance
Select NIC	bond0
NIC Type	10M/100M/1000M Self-adaptive
Enable DHCP	<input type="checkbox"/>
IPv4 Address	172.16.23.186
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	172.16.23.1
IPv6 Address 1	fe80::8ee7:48ff:fe1b:c18a/64
IPv6 Address 2	
IPv6 Default Gateway	
MAC Address	8c:e7:48:1b:c1:8a
MTU(Bytes)	1500
Preferred DNS Server	192.168.1.1
Alternate DNS Server	
Main NIC	LAN1

Figure 11. 2 Net Fault-tolerance Working Mode

11.2 Configuring Advanced Settings

11.2.1 PPPoE Settings

Purpose:

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

Steps:

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

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

Figure 11. 3 PPPoE Settings Interface

3. Check the **PPPoE** checkbox to enable this feature.
 4. Enter **User Name** and **Password** for PPPoE access.
-
- The User Name and Password should be assigned by your ISP.
5. Click the **Apply** button to save and exit the interface.
 6. After successful settings, the system asks you to reboot the device to enable the new settings, and the PPPoE dial-up is automatically connected after reboot.

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

Please refer to *Chapter 14.1 Viewing System Information* for PPPoE status.

11.2.2 Configuring Cloud P2P

Purpose:

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

Steps:

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



The verification code consists of 6 capital letters and is located at the bottom of the DVR. You can also use the

scanning tool of your phone to quickly get the code by scanning the QR code below.

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



Figure 11. 4 Cloud P2P 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 Cloud P2P application is installed or by the website (<http://www.hicloudcam.com>).



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

11.2.3 Configuring DDNS

Purpose:

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

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

Steps:

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

Enable DDNS	<input checked="" type="checkbox"/>
DDNS Type	IPServer
Area/Country	Custom
Server Address	
Device Domain Name	
Status	DDNS is disabled.
User Name	
Password	

Figure 11. 5 IPServer Settings Interface

- **DynDNS:**

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

Enable DDNS	<input checked="" type="checkbox"/>
DDNS Type	DynDNS
Area/Country	Custom
Server Address	
Device Domain Name	
Status	DDNS is disabled.
User Name	
Password	

Figure 11. 6 DynDNS Settings Interface

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

Enable DDNS	<input checked="" type="checkbox"/>
DDNS Type	PeanutHull
Area/Country	Custom
Server Address	
Device Domain Name	
Status	DDNS is disabled.
User Name	
Password	

Figure 11. 7 PeanutHull Settings Interface

- **NO-IP:**

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

- 1) Enter **Server Address** for NO-IP.

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

Enable DDNS	<input checked="" type="checkbox"/>
DDNS Type	NO-IP
Area/Country	Custom
Server Address	
Device Domain Name	
Status	DDNS is disabled.
User Name	
Password	

Figure 11. 8 NO-IP Settings Interface

- **HiDDNS:**

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

Enable DDNS	<input checked="" type="checkbox"/>
DDNS Type	HiDDNS
Area/Country	Custom
Server Address	www.hiddns.com
Device Domain Name	
Status	DDNS is disabled.
User Name	
Password	

Figure 11. 9 HiDDNS Settings Interface

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

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

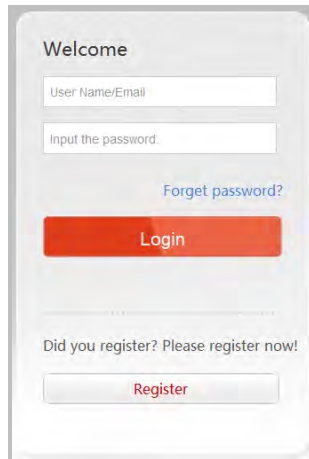


Figure 11. 10 Register an Account

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

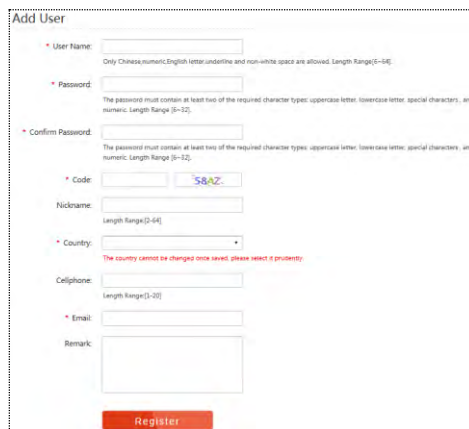


Figure 11. 11 Register an Account

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

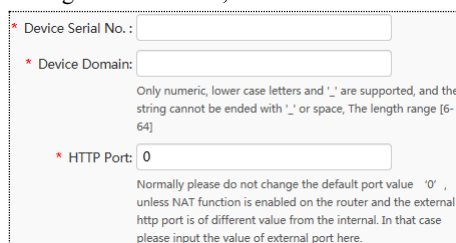


Figure 11. 12 Register the Device

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

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

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

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

Open a web browser, and enter *http://_www.hiddns.com/alias* in the address bar. Alias refers to the

Device Domain Name on the device or the **Device Name** on the HiDDNS server.

Example: `http://www.hiddns.com/nvr`



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

● **OPTION 2: Access the devices via iVMS-4200**

For iVMS-4200, 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.

Figure 11. 13 Access Device via iVMS-4200

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

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

11.2.4 Configuring NTP Server

Purpose:

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



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

Steps:

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

2. Select the **NTP** tab to enter the NTP Settings interface, as shown in Figure 11. 14.

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

Figure 11. 14 NTP Settings Interface

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



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

11.2.5 Configuring Remote Alarm Host

Purpose:

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

Steps:

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

Alarm Host IP	
Alarm Host Port	0
Server Port	8000
HTTP Port	80
Multicast IP	
RTSP Port	554

Figure 11. 15 More Settings Interface

3. Enter **Alarm Host IP** and **Alarm Host Port** in the text fields.
The **Alarm Host IP** refers to the IP address of the remote PC on which the Network Video Surveillance Software (e.g., iVMS-4200) is installed, and the **Alarm Host Port** must be the same as the alarm monitoring port configured in the software.
4. Click the **Apply** button to save and exit the interface.

11.2.6 Configuring Multicast

Purpose:

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

Steps:

1. Enter the Network Settings interface.
Menu > Configuration > Network
2. Select the **More Settings** tab to enter the More Settings interface, as shown in Figure 11. 15.
3. Set **Multicast IP**, as shown in Figure 11. 16. When adding a device to the Network Video Surveillance Software, the multicast address must be the same as the NVR's multicast IP.

Server Port	8000
HTTP Port	80
Multicast IP	239.221.2.78

Figure 11. 16 Configure Multicast

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



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

11.2.7 Configuring RTSP

Purpose:

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

Steps:

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

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

Figure 11. 17 RTSP Settings Interface

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

11.2.8 Configuring Server and HTTP Ports

Purpose:

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

default HTTP port is 80.

Steps:

1. Enter the Network Settings interface.
Menu >Configuration> Network
2. Select the **More Settings** tab to enter the More Settings interface, as shown in Figure 11. 15.
3. Enter new **Server Port** and **HTTP Port**.

Server Port	8000
HTTP Port	80
Multicast IP	239.221.2.78

Figure 11. 18 Host/Others Settings Menu

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



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

11.2.9 Configuring Email

Purpose:

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

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

Steps:

1. Enter the Network Settings interface.
Menu >Configuration> Network
2. Set the IPv4 Address, IPv4 Subnet Mask, IPv4 Gateway and the Preferred DNS Server in the Network Settings men.

NIC Type	10M/100M/1000M Self-adaptive		
Enable DHCP	<input checked="" type="checkbox"/>		
IPv4 Address...	10 .16 .2 .109	IPv6 Address...	fe80::269:6cff.fe2a:fb88/64
IPv4 Subn...	255 .255 .255 .0	IPv6 Address...	
IPv4 Defa...	10 .16 .2 .254	IPv6 Defa...	
MAC Address	00:69:6c:2a:fb:88		
MTU(Bytes)	1500		
Preferred DNS Server	10.1.7.88		
Alternate DNS Server	10.1.7.77		

Figure 11. 19 Network Settings Interface

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

4. Select the Email tab to enter the Email Settings interface.

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

Figure 11. 20 Email Settings Interface

5. Configure the following Email settings:

Enable Server Authentication (optional): Check the checkbox to enable the server authentication feature.

User Name: The user account of sender's Email for SMTP server authentication.

Password: The password of sender's Email for SMTP server authentication.

SMTP Server: The SMTP Server IP address or host name (e.g., smtp.263xmail.com).

SMTP Port No.: The SMTP port. The default TCP/IP port used for SMTP is 25.

Enable SSL (optional): Click the checkbox to enable SSL if required by the SMTP server.

Sender: The name of sender.

Sender's Address: The Email address of sender.

Select Receivers: Select the receiver. Up to 3 receivers can be configured.

Receiver: The name of user to be notified.

Receiver's Address: The Email address of user to be notified.

Enable Attached Pictures: Check the checkbox of **Enable Attached Picture** if you want to send email with attached alarm images. The interval is the time of two adjacent alarm images. You can also set SMTP port and enable SSL here.

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

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

6. Click **Apply** button to save the Email settings.
7. You can click **Test** button to test whether your Email settings work. The corresponding Attention message box will pop up. Refer to Figure 11. 21.

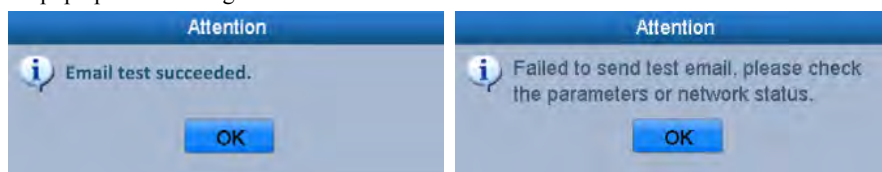


Figure 11. 21 Email Testing Attention

11.2.10 Configuring NAT

Purpose:

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

● **UPnP™**

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

Before you start:

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

Steps:

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

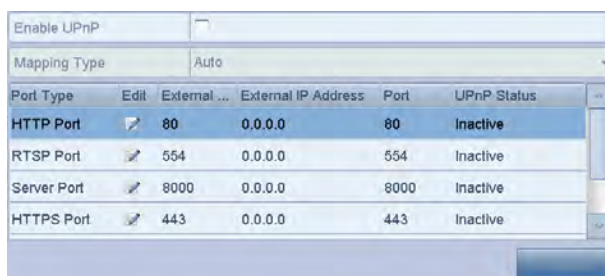


Figure 11. 22 UPnP™ Settings Interface

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

OPTION 1: Auto

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

Steps:

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

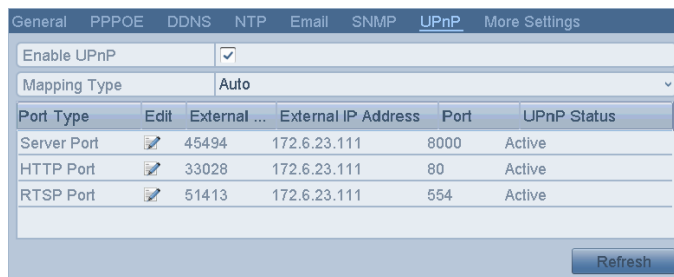



Figure 11. 23 UPnP™ Settings Finished-Auto

OPTION 2: Manual

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

Steps:

- 1) Select **Manual** in the drop-down list of Mapping Type.

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



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



Figure 11. 24 External Port Settings Dialog Box

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

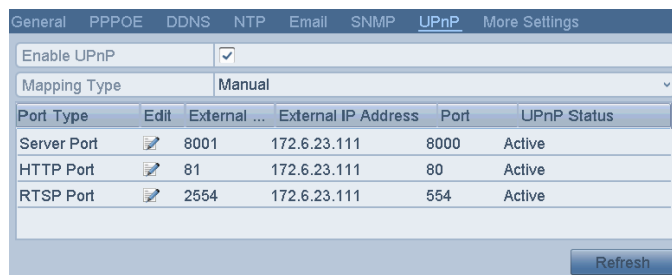


Figure 11. 25 UPnP™ Settings Finished-Manual


● **Manual Mapping**

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

Before you start:

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

Steps:

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



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

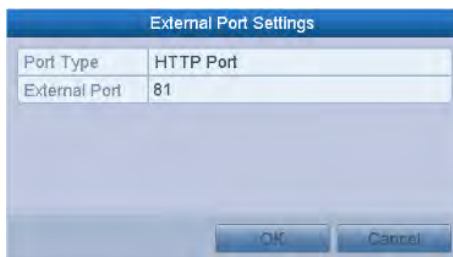


Figure 11. 26 External Port Settings Dialog Box

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



Each item should be corresponding with the device port, including server port, http port, RTSP port and https port.

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

Figure 11. 27 Setting Virtual Server Item



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

11.3 Checking Network Traffic

Purpose:

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

Steps:

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

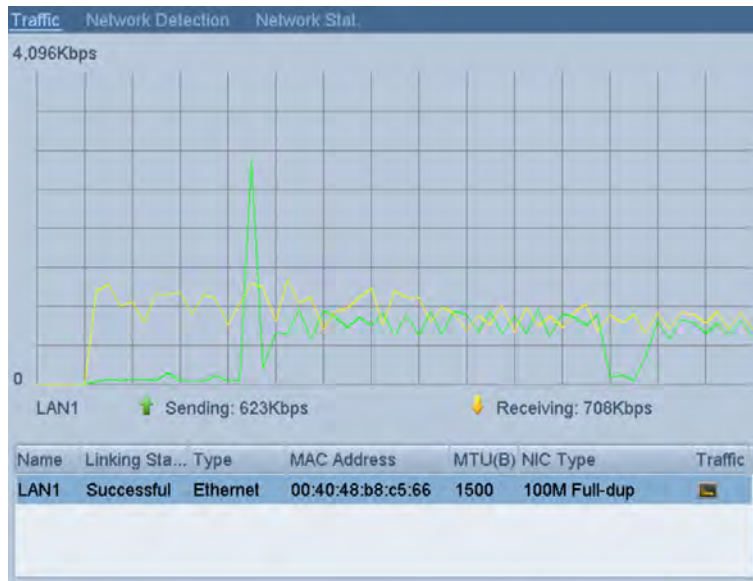


Figure 11. 28 Network Traffic Interface

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

11.4 Configuring Network Detection

Purpose:

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

11.4.1 Testing Network Delay and Packet Loss

Steps:

1. Enter the Network Traffic interface.
Menu >Maintenance>Net Detect
2. Click the **Network Detection** tab to enter the Network Detection menu, as shown in Figure 11. 29.

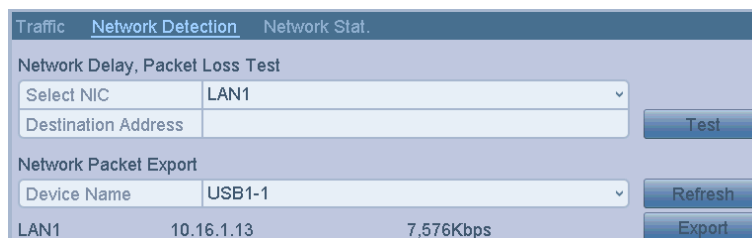


Figure 11. 29 Network Detection Interface

3. Enter the destination address in the text field of **Destination Address**.
4. Click **Test** button to start testing network delay and packet loss. The testing result pops up on the window. If the testing is failed, the error message box will pop up as well. Refer to Figure 11. 30.

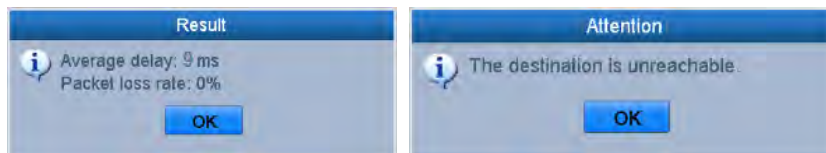


Figure 11. 30 Testing Result of Network Delay and Packet Loss

11.4.2 Exporting Network Packet

Purpose:

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

Steps:

1. Enter the Network Traffic interface.
Menu >Maintenance>Net Detect
2. Click the **Network Detection** tab to enter the Network Detection interface.
3. Select the backup device from the dropdown list of Device Name, as shown in Figure 11. 31.



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

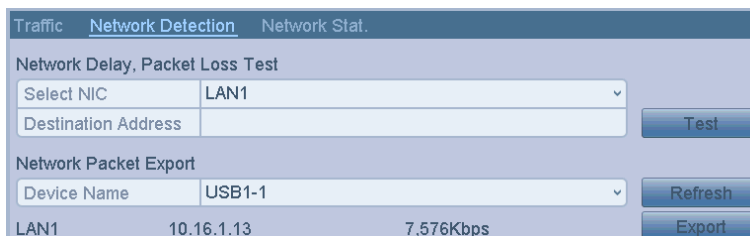


Figure 11. 31 Export Network Packet

4. Click **Export** button to start exporting.
5. After the exporting is complete, click **OK** to finish the packet export, as shown in Figure 11. 32.

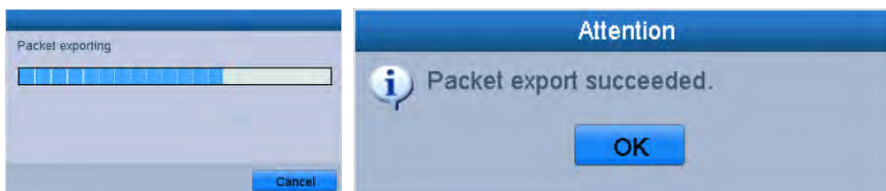


Figure 11. 32 Packet Export Attention



Up to 1M data can be exported each time.

11.4.3 Checking the Network Status

Purpose:

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

Step:

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

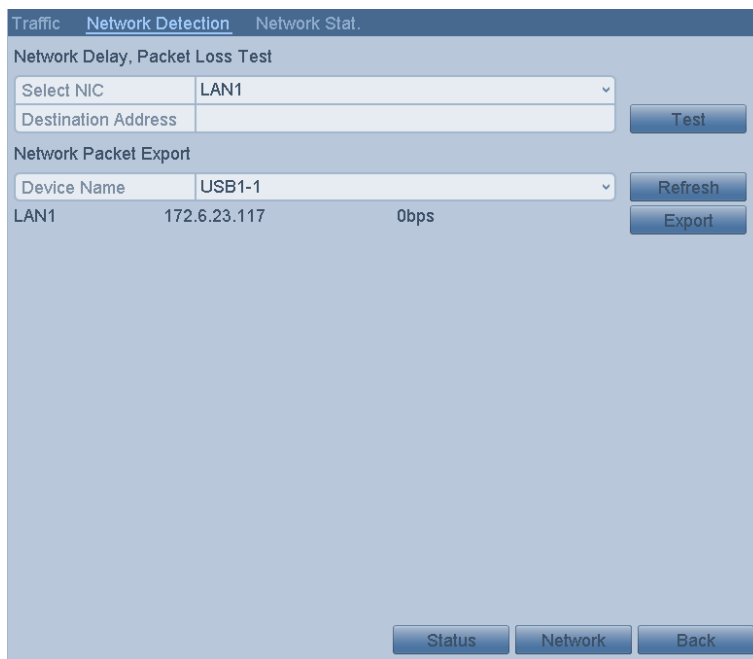


Figure 11. 33 Network Status Checking

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

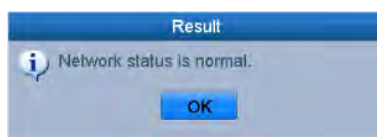


Figure 11. 34 Network status checking result

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

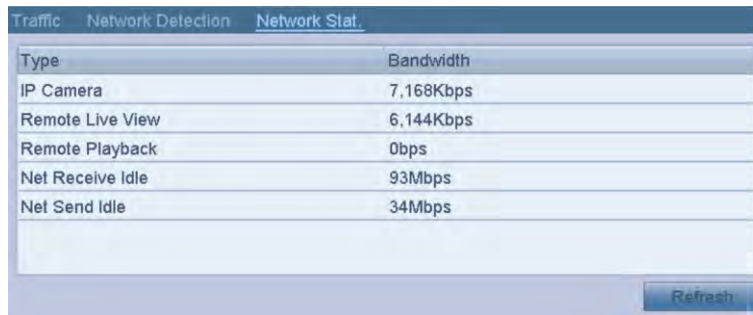
11.4.4 Checking Network Statistics

Purpose:

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

Steps:

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



Type	Bandwidth
IP Camera	7,168Kbps
Remote Live View	6,144Kbps
Remote Playback	0bps
Net Receive Idle	93Mbps
Net Send Idle	34Mbps

Figure 11. 35 Network Stat. Interface

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

Chapter 12 HDD Management

12.1 Initializing HDDs

Purpose:

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



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

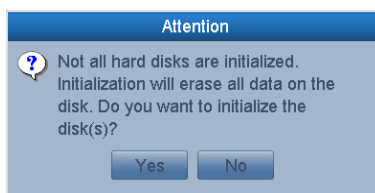


Figure 12. 1 Message Box of Uninitialized HDD

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

Steps:

1. Enter the HDD Information interface.

Menu > HDD> General



Figure 12. 2 HDD Information Interface

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

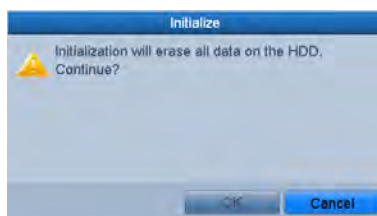


Figure 12. 3 Confirm Initialization

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



Figure 12. 4 Status changes to Initializing

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



Figure 12. 5 HDD Status Changes to Normal



Initializing the HDD will erase all data on it.

12.2 Managing Network HDD

Purpose:

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

Steps:

1. Enter the HDD Information interface.

Menu > HDD>General



L...	Capacity	Status	Property	Type	Free Space	Gr...	Edit	D...
1	931.51GB	Normal	RAW	Local	802GB	1		

Figure 12. 6 HDD Information Interface

2. Click the **Add** button to enter the Add NetHDD interface, as shown in Figure 12. 7.

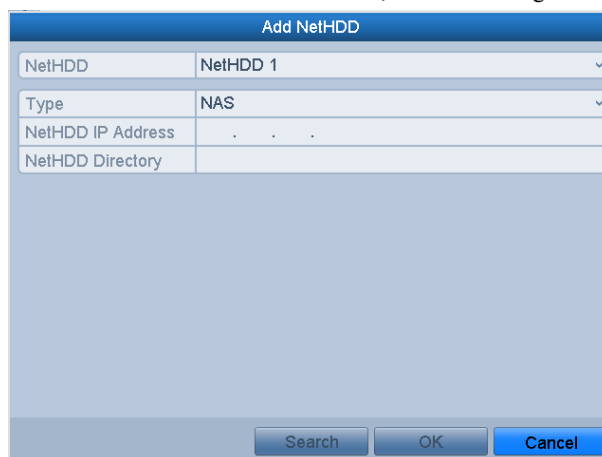


Figure 12. 7 HDD Information Interface

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 the **Search** button 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 the **OK** button to add the configured NAS disk.



Up to 8 NAS disks can be added.

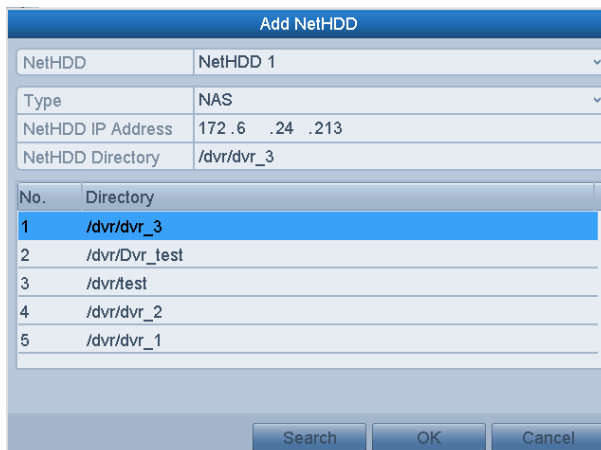


Figure 12. 8 Add NAS Disk

• **Add IP SAN:**

- 1) Enter the NetHDD IP address in the text field.
- 2) Click the **Search** button to search 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.



Up to 1 IP SAN disk can be added.

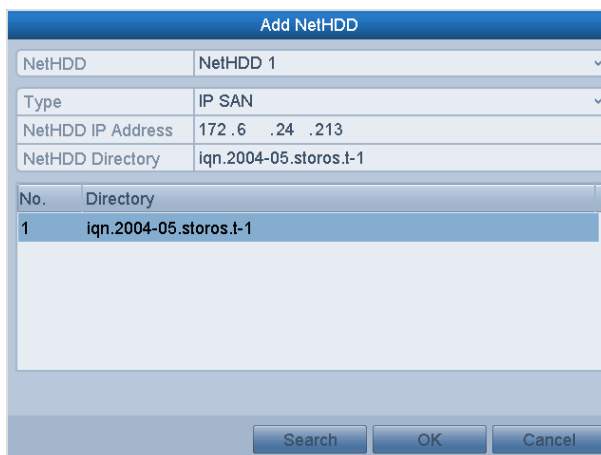
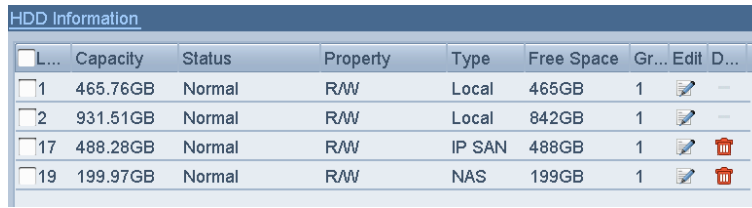


Figure 12. 9 Add IP SAN Disk

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



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



The screenshot shows a table titled "HDD Information" with the following columns: L..., Capacity, Status, Property, Type, Free Space, Gr..., Edit, and D... The table contains four rows of data:

L...	Capacity	Status	Property	Type	Free Space	Gr...	Edit	D...
1	465.76GB	Normal	R/W	Local	465GB	1		--
2	931.51GB	Normal	R/W	Local	842GB	1		--
17	488.28GB	Normal	R/W	IP SAN	488GB	1		
19	199.97GB	Normal	R/W	NAS	199GB	1		

Figure 12. 10 Initialize Added NetHDD

12.3 Managing HDD Group

12.3.1 Setting HDD Groups

Purpose:

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

Steps:

1. Enter the Storage Mode interface.
Menu > HDD > Advanced
2. Set the **Mode** to Group, as shown in Figure 12. 11.

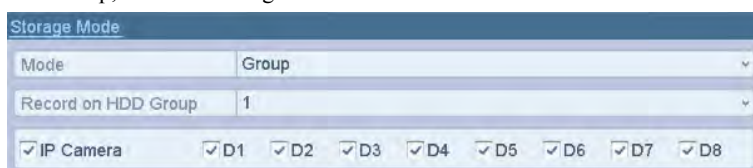


Figure 12. 11 Storage Mode Interface

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

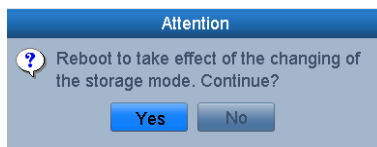



Figure 12. 12 Attention for Reboot

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  icon to enter the Local HDD Settings interface, as shown in Figure 12. 13.

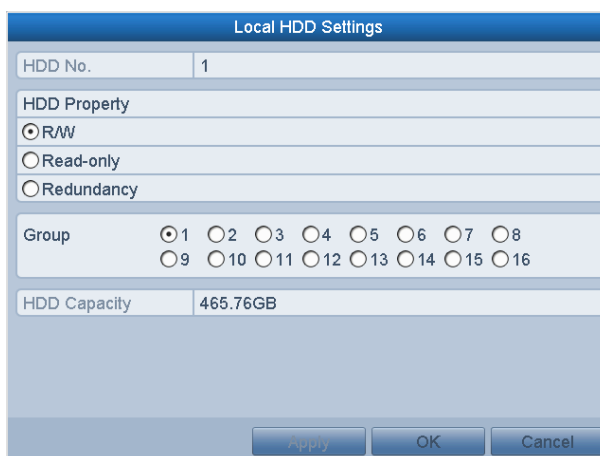


Figure 12. 13 Local HDD Settings Interface

7. Select the Group number for the current HDD.



The default group No. for each HDD is 1.

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

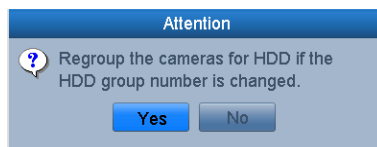


Figure 12. 14 Confirm HDD Group Settings

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

12.3.2 Setting HDD Property

Purpose:

The HDD property can be set to redundancy, read-only or read/write (R/W). Before setting the HDD property, please set the storage mode to Group (refer to step 1-4 of *Chapter 12.3.1 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 12. 15.

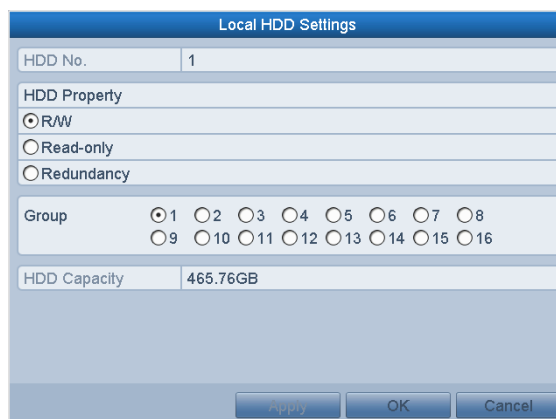


Figure 12. 15 Set HDD Property

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.



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

12.4 Configuring Quota Mode

Purpose:

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

Steps:

1. Enter the Storage Mode interface.
Menu > HDD > Advanced
2. Set the **Mode** to Quota, as shown in Figure 12. 16.



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

Mode	Quota
Camera	[D1] IPdome
Used Record Capacity	3072.00MB
Used Picture Capacity	1024.00MB
HDD Capacity (GB)	931
Max. Record Capacity (G...)	0
Max. Picture Capacity (GB)	0
Free Quota Space 931 GB	

Figure 12. 16 Storage Mode Settings Interface

3. Select a camera for which you want to configure quota.
4. Enter the storage capacity in the text fields of **Max. Record Capacity (GB)**, as shown in Figure 12. 17.



Figure 12. 17 Configure Record Quota

5. You can copy the quota settings of the current camera to other cameras if required. Click the **Copy** button to enter the Copy Camera menu, as shown in Figure 12. 18.

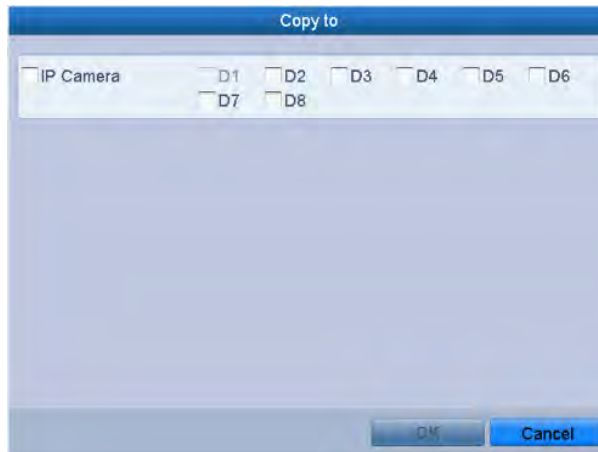


Figure 12. 18 Copy Settings to Other Camera(s)

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



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

12.5 Checking HDD Status

Purpose:

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

Checking HDD Status in HDD Information Interface

Steps:

1. Enter the HDD Information interface.
Menu > HDD>General
2. Check the status of each HDD which is displayed on the list, as shown in Figure 12. 19.

L...	Capacity	Status	Property	Type	Free Space	Gr...	Edit	D...
1	931.51GB	Normal	R/W	Local	927GB	1	-	-

Figure 12. 19 View HDD Status (1)



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

Checking HDD Status in HDD Information Interface

Steps:

1. Enter the System Information interface.
Menu >Maintenance > System Info
2. Click the **HDD** tab to view the status of each HDD displayed on the list, as shown in Figure 12. 20.

Label	Status	Capacity	Free Space	Property	Type	Group
1	Normal	1,397GB	1,336GB	R/W	Local	1
Total Capacity		1,397GB				
Free Space		1,336GB				

Figure 12. 20 View HDD Status (2)

12.6 HDD Detection

Purpose:

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

S.M.A.R.T. Settings

Steps:

1. Enter the S.M.A.R.T Settings interface.
Menu > Maintenance > HDD Detect
2. Select the HDD to view its S.M.A.R.T information list, as shown in Figure 12. 21.

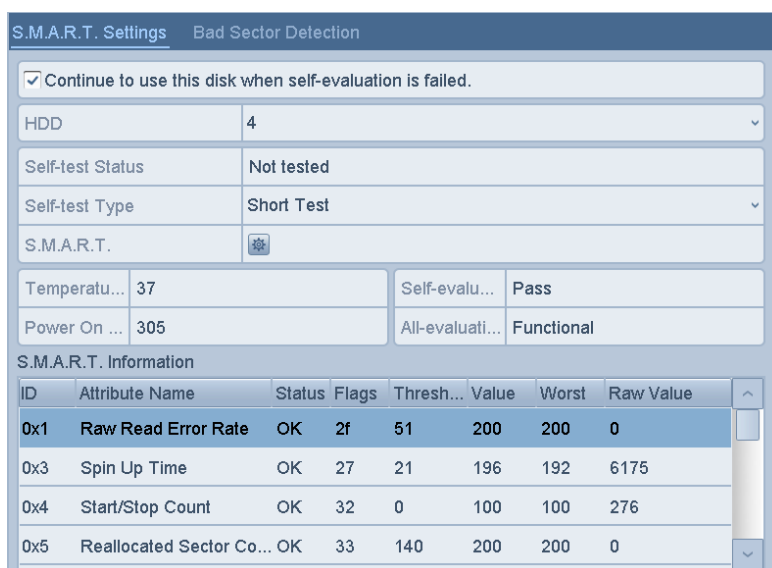
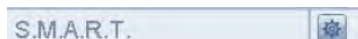


Figure 12. 21 S.M.A.R.T Settings Interface

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

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

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



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

Bad Sector Detection

Steps:

1. Click the Bad Sector Detection tab.
2. Select the HDD No. in the dropdown list you want to configure, and choose All Detection or Key Area Detection as the detection type.
3. Click the **Detect** button to start the detection.

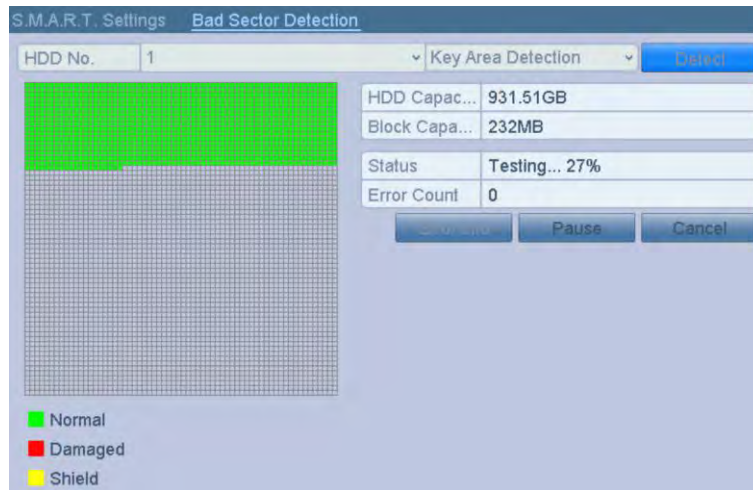


Figure 12. 22 Bad Sector Detection

And you can click **Error info** button to see the detailed damage information.

And you can also pause/resume or cancel the detection.

12.7 Configuring HDD Error Alarms

Purpose:

You can configure the HDD error alarms when the HDD status is *Uninitialized* or *Abnormal*.

Steps:

1. Enter the Exception interface.
Menu > Configuration > Exceptions
2. Select the Exception Type to **HDD Error** from the dropdown list.
3. Click the checkbox(s) below to select the HDD error alarm type (s), as shown in Figure 12. 23.



The alarm type can be selected to: Audible Warning, Notify Surveillance Center, Send Email and Trigger Alarm Output. Please refer to *Chapter 8.6 Setting Alarm Response Actions*.

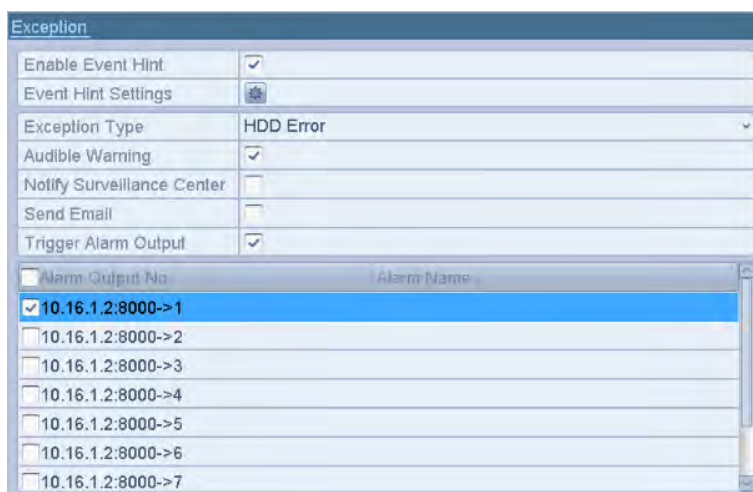


Figure 12. 23 Configure HDD Error Alarm

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 13 Camera Settings

13.1 Configuring OSD Settings

Purpose:

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

Steps:

1. Enter the OSD Configuration interface.
Menu > Camera > OSD
2. Select the camera to configure OSD settings.
3. Edit the Camera Name in the text field.
4. Configure the Display Name, Display Date and Display Week by clicking the checkbox.
5. Select the Date Format, Time Format and Display Mode.

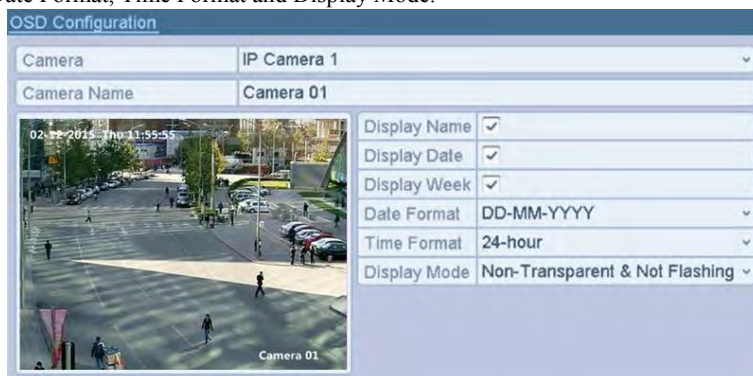


Figure 13. 1 OSD Configuration Interface

6. You can use the mouse to click and drag the text frame on the preview window to adjust the OSD position.
7. Click the **Apply** button to apply the settings.

13.2 Configuring Privacy Mask

Purpose:

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

Steps:

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



Figure 13. 2 Privacy Mask Settings Interface

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



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

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

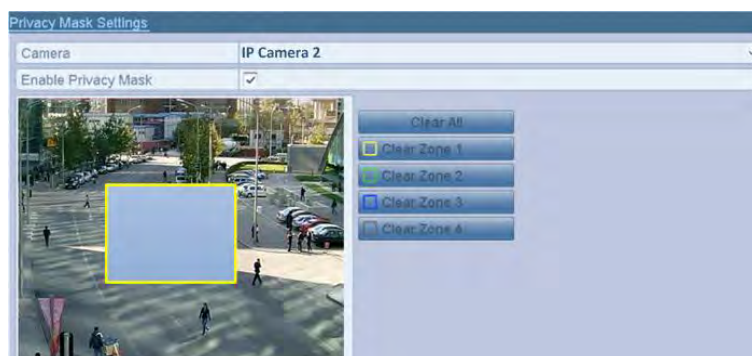


Figure 13. 3 Set Privacy Mask Area

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

13.3 Configuring Video Parameters

Steps:

1. Enter the Image Settings interface.

Menu > Camera > Image



Figure 13. 4 Image Settings Interface

2. Select the camera to set image parameters.
3. You can click on the arrow to change the value of each parameter.
4. Click the **Apply** button to save the settings.

Chapter 14 NVR Management and Maintenance

14.1 Viewing System Information

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 14. 1 Device Information Interface

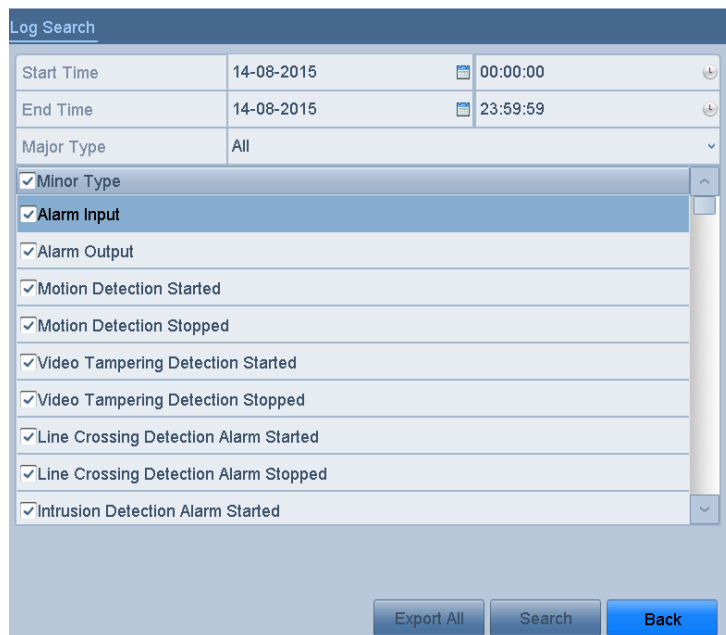
14.2 Searching & Export Log Files

Purpose:

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

Steps:

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



The screenshot shows the 'Log Search' interface. It features a table for search criteria and a list of minor types. The search criteria table is as follows:

Field	Value	Icon	Reset Icon
Start Time	14-08-2015	Calendar	Reset
End Time	14-08-2015	Calendar	Reset
Major Type	All	Dropdown	

Below the table is a list of minor types, each with a checked checkbox:

- Minor Type
- Alarm Input
- Alarm Output
- Motion Detection Started
- Motion Detection Stopped
- Video Tampering Detection Started
- Video Tampering Detection Stopped
- Line Crossing Detection Alarm Started
- Line Crossing Detection Alarm Stopped
- Intrusion Detection Alarm Started

At the bottom of the interface are three buttons: 'Export All', 'Search', and 'Back'.

Figure 14. 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.

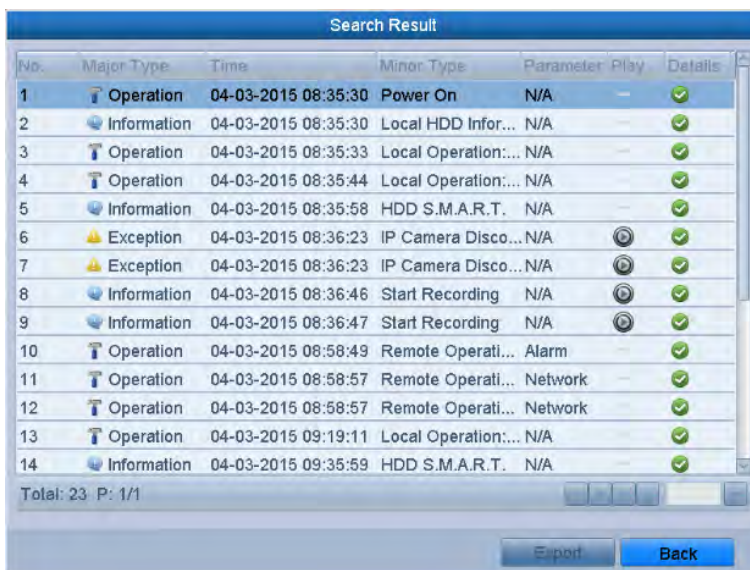


Figure 14. 3 Log Search Results



Up to 2000 log files can be displayed each time.

5. You can click the button of each log or double click it to view its detailed information, as shown in Figure 14. 4. And you can also click the button to view the related video files if available.



Figure 14. 4 Log Details

6. If you want to export the log files, click the **Export** button on the Search Result interface to enter the Export menu, as shown in Figure 14. 5.

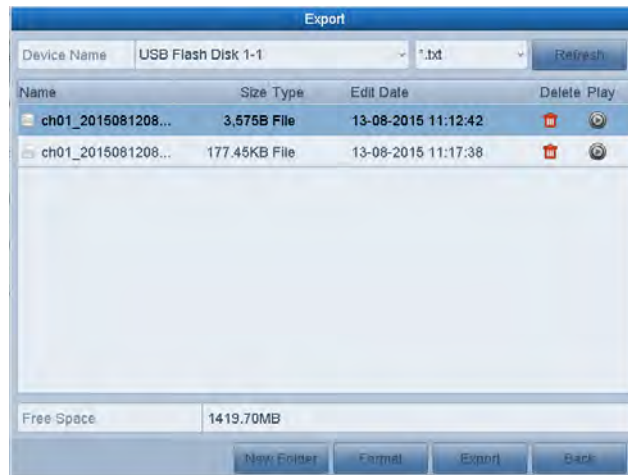


Figure 14. 5 Export Log Files

7. Select the backup device from the dropdown list of **Device Name**.
8. Select the format of the log files to be exported. Up to 9 formats are selectable.
9. 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 NVR before operating log export.

14.3 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 > IP Camera Import/Export
2. Click the IP Camera Import/Export tab, the content of detected plugged external device appears.
3. Click the **Export** button to export configuration files to the selected local backup device.
4. To import a configuration file, select the file from the selected backup device and click the **Import** button.
After the importing process is completed, you must reboot the NVR.

14.4 Importing/Exporting Configuration Files

Purpose:

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

Steps:

1. Enter the Import/Export Configuration File interface.

Menu > Maintenance > Import/Export

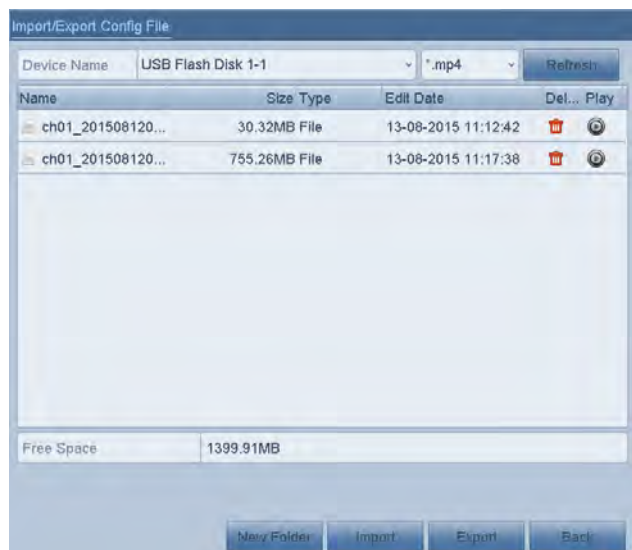


Figure 14. 6 Import/Export Config File

2. Click the **Export** button to export configuration files to the selected local backup device.
3. To import a configuration file, select the file from the selected backup device and click the **Import** button.
After the import process is completed, you must reboot the NVR.



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

14.5 Upgrading System

Purpose:

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

14.5.1 Upgrading by Local Backup Device

Steps:

1. Connect your NVR with a local backup device where the update firmware file is located.
2. Enter the Upgrade interface.
Menu >Maintenance>Upgrade
3. Click the **Local Upgrade** tab to enter the local upgrade menu, as shown in Figure 14. 7.

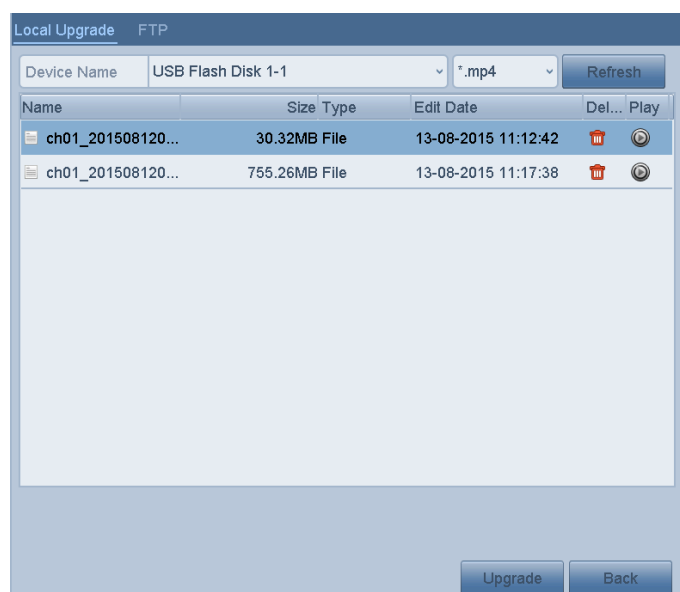


Figure 14. 7 Local Upgrade Interface

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

14.5.2 Upgrading by FTP

Purpose:

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



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

directory as required.

Steps:

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



Figure 14. 8 FTP Upgrade Interface

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

14.6 Restoring Default Settings

Steps:

1. Enter the Default interface.

Menu > Maintenance > Default

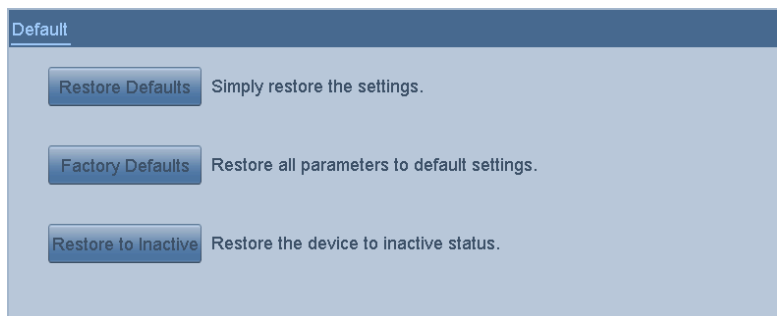


Figure 14. 9 Restore Defaults

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

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

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

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

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



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

Chapter 15 Others

15.1 Configuring RS-232 Serial Port

Purpose:

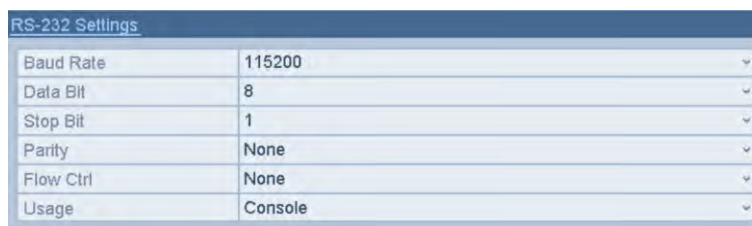
The RS-232 port can be used in two ways:

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

Steps:

1. Enter the RS-232 Settings interface.

Menu >Configuration> RS-232



RS-232 Settings	
Baud Rate	115200
Data Bit	8
Stop Bit	1
Parity	None
Flow Ctrl	None
Usage	Console

Figure 15. 1 RS-232 Settings Interface

2. Configure RS-232 parameters, including baud rate, data bit, stop bit, parity, flow control and usage.
3. Click the **Apply** button to save the settings.

15.2 Configuring General Settings

Purpose:

You can configure the BNC output standard, VGA output resolution, mouse pointer speed through the Menu > Configuration > General interface.

Steps:

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



Figure 15. 2 General Settings Interface

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

15.3 Configuring DST Settings

Steps:

1. Enter the General Settings interface.

Menu >Configuration>General

2. Choose **DST Settings** tab.

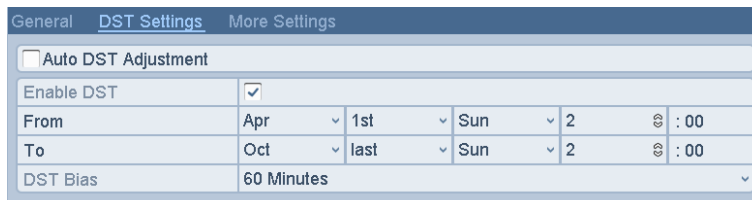


Figure 15. 3 DST Settings Interface

You can check the checkbox before the Auto DST Adjustment item.

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

15.4 Configuring More Settings for Device Parameters

Steps:

1. Enter the General Settings interface.
Menu >Configuration>General
2. Click the **More Settings** tab to enter the More Settings interface, as shown in Figure 15. 4.

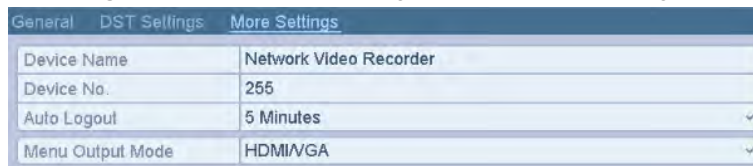


Figure 15. 4 More Settings Interface

3. Configure the following settings:
 - **Device Name:** Edit the name of NVR.
 - **Device No.:** Edit the serial number of NVR. The Device No. can be set in the range of 1~255, and the default No. is 255. The number is used for the remote and keyboard control.
 - **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. By default, only HDMI™ /VGA is selectable.
4. Click the **Apply** button to save the settings.

15.5 Managing User Accounts

Purpose:

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

15.5.1 Adding a User

Steps:

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

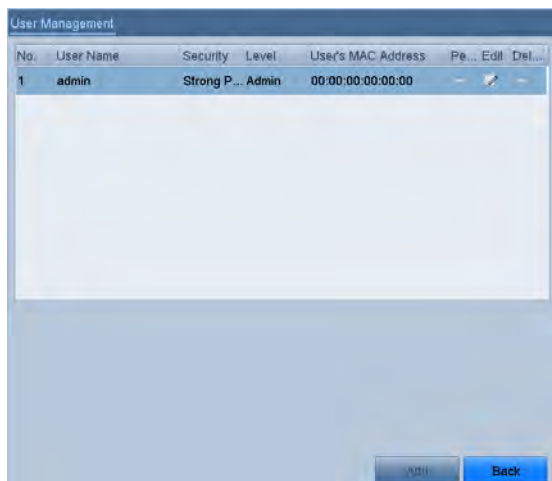


Figure 15. 5 User Management Interface

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

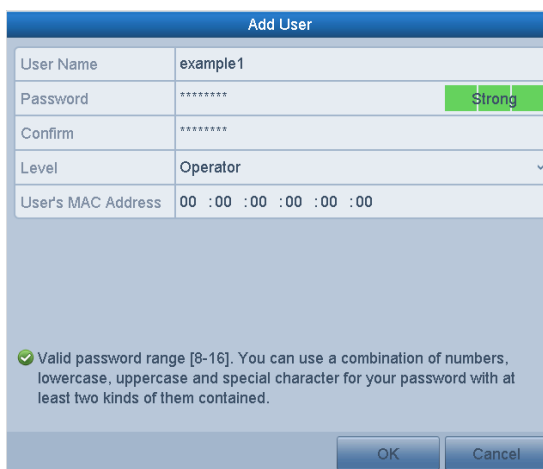



Figure 15. 6 Add User Menu

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

Address.

Password: Set the password for the user account.

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

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


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

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

4. Click the **OK** button to save the settings and go back to the User Management interface. The added new user will be displayed on the list, as shown in Figure 15. 7.



Figure 15. 7 Added User Listed in User Management Interface

5. Select the user from the list and then click the  button to enter the Permission settings interface, as shown in Figure 15. 8.

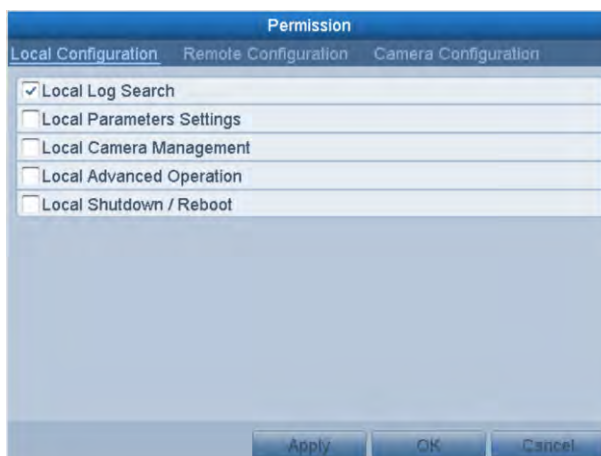


Figure 15. 8 User Permission Settings Interface

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

Local Configuration

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

Remote Configuration

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

Camera Configuration

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

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



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

15.5.2 Deleting a User

Steps:

- Enter the User Management interface.
Menu >Configuration>User
- Select the user to be deleted from the list, as shown in Figure 15. 9.

No.	User Name	Security	Level	User's MAC Address	Pe...	Edit	Del...
1	admin	Strong P...	Admin	00:00:00:00:00	-		
2	example1	Strong P...	Operator	00:00:00:00:00			

Figure 15. 9 User List

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

15.5.3 Editing a User

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

Steps:

1. Enter the User Management interface.
Menu > Configuration > User
2. Select the user to be edited from the list, as shown in Figure 15. 9.
3. Click the icon to enter the Edit User interface, as shown in Figure 15. 10.


Figure 15. 10 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.