HIKVISION

Network Video Recorder

User Manual

UD06041B

User Manual

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

About this Manual

This Manual is applicable to Wi-Fi Network Video Recorder.

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

Please use this user manual under the guidance of professionals.

Trademarks Acknowledgement

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

Legal Disclaimer

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

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

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

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

Regulatory Information

FCC Information

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

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

FCC Conditions

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

1. This device may not cause harmful interference.

2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement

CE 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 RE Directive 2014/53/EU, the EMC Directive 2014/30/EU, the RoHS Directive 2011/65/EU.

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

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

Industry Canada ICES-003 Compliance

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

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

(1) this device may not cause interference, and

(2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radioexempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

(1) l'appareil ne doit pas produire de brouillage, et

(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

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

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut

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

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

Cet équipement doit être installé et utilisé à une distance minimale de 20 cm entre le radiateur et votre corps.

Applicable Models

This manual is applicable to the models listed in the following table.

Series	Model
DS-7600NI-KI/W	DS-7604NI-KI/W
	DS-7608NI-KI/W

Symbol Conventions

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

Symbol	Description
NOTE	Provides additional information to emphasize or supplement important points of the main text.
WARNING	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
DANGER	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.

Safety Instructions

- 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 battery manufacturer.

Product Key Features

General

- Connectable to network cameras, network dome and encoders.
- Connectable to the third-party network cameras like ACTI, Arecont, AXIS, Bosch, Brickcom, Canon, PANASONIC, Pelco, SAMSUNG, SANYO, SONY, Vivotek and ZAVIO, and cameras that adopt ONVIF or PSIA protocol.
- Connectable to the smart IP cameras.
- H.265+/H.265/ H.264+/H.264/MPEG4 video formats
- Each channel supports dual-stream.
- Up to 4 network cameras can be added according to different models.
- 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

- HDMI/VGA output is provided.
- Multiple screen display in live view is supported, and the display sequence of channels is adjustable.
- Live view screen can be switched in group. Manual switch and auto-switch are provided and the auto-switch interval is configurable.
- Configurable main stream and sub-stream for the live view.
- Quick setting menu is provided for live view.
- Motion detection, video tampering, 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

- One SATA interface for one hard disk.
- Up to 6TB storage capacity for each disk.
- Supports S.M.A.R.T. and bad sector detection.
- Supports HDD standby function.
- 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.
- Pre-record and post-record for alarm, motion detection for recording, and pre-record time for schedule and manual recording.
- Searching record files by events (alarm input/motion detection).
- Tag adding for record files, searching and playing back by tags.
- Locking and unlocking record files.
- Local redundant recording.
- Provide new playback interface with easy and flexible operation.
- Searching and playing back record files by channel number, 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.
- Supports thumbnails view and fast view during playback.
- Up to 4/8-ch synchronous playback at 1080p.
- Supports enabling H.264+ to ensure high video quality with lowered bitrate.

Backup

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

Alarm and Exception

- Configurable arming time of alarm input/output.
- Alarm for video loss, motion detection, tampering, abnormal signal, video input/output standard mismatch, illegal login, network disconnected, IP confliction, abnormal record, HDD error, and HDD full, etc.
- VCA detection alarm is supported.
- VCA search for face detection, vehicle plate, and behavior analysis.
- Alarm triggers full screen monitoring, audio alarm, notifying surveillance center, sending email and alarm output.
- Automatic restore when system is abnormal.

Other Local Functions

- Operable by mouse, remote control, or control keyboard.

- 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.
- Admin password resetting by exporting/importing the GUID file.
- Operation, alarm, exceptions and log recording and searching.
- Manually triggering and clearing alarms.
- Import and export of device configuration information.

Network Functions

- One self-adaptive 100Mbps network interface.
- IPv6 is supported.
- TCP/IP protocol, DHCP, DNS, DDNS, NTP, SADP, SMTP, SNMP, NFS, and iSCSI are supported.
- TCP, UDP and RTP for unicast.
- Auto/Manual port mapping by UPnP™.
- Support access by Hik-Connect.
- Remote web browser access by HTTPS ensures high security.
- The ANR (Automatic Network Replenishment) function is supported, it enables the IP camera save the recording files in the local storage when the network is disconnected, and synchronizes the files to the NVR when the network is resumed.
- Remote reverse playback via RTSP.
- Supports accessing by the platform via ONVIF.
- Remote search, playback, download, locking and unlocking of the record files, and support downloading files broken transfer resume.
- Remote parameters setup; remote import/export of device parameters.
- Remote viewing of the device status, system logs and alarm status.
- Remote keyboard operation.
- Remote HDD formatting and program upgrading.
- Remote system restart and shutdown.
- RS-232, RS-485 transparent channel transmission.
- Alarm and exception information can be sent to the remote host
- Remotely start/stop recording.
- Remotely start/stop alarm output.
- Remote PTZ control.
- Virtual host function is provided to get access and manage the IP camera directly.
- Two-way audio and voice broadcasting.
- Embedded WEB server.

Development Scalability:

- SDK for Windows system.

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

TABLE OF CONTENTS

Chapter 1 Introduction 15
1.1 Front Panel 15
1.2 Rear Panel 15
1.3 IR Remote Control Operations 16
1.3.1 Pairing (Enabling) the IR Remote to a Specific NVR (optional) 16
1.3.2 Unpairing (Disabling) an IR Remote from a NVR 17
1.3.3 Troubleshooting Remote Control: 20
1.4 USB Mouse Operation 22
1.5 Input Method Description 23
Chapter 2 Getting Started 24
2.1 Device Startup and Activation 24
2.1.1 Starting Up and Shutting Down the NVR 24
2.1.2 Activating Your Device 25
2.1.3 Using the Unlock Pattern for Login 26
2.1.4 Login and Logout 29
2.1.5 Resetting Your Password 31
2.2 Using Wizard for Basic Configuration 32
2.3 Adding and Connecting the IP Cameras 37
2.3.1 Activating the IP Camera 37
2.3.2 Adding the Online IP Cameras 38
2.3.3 Editing the Connected IP Cameras and Configuring Customized Protocols 43
2.3.4 Binding IP Camera 47
Chapter 3 Live View 49
3.1 Introduction of Live View 49
3.2 Operations in Live View Mode 50
3.2.1 Using the Mouse in Live View 50
3.2.2 Quick Setting Toolbar in Live View Mode 51
3.3 Adjusting Live View Settings 54
3.4 Channel-Zero Encoding 57
Chapter 4 PTZ Controls 58
4.1 Configuring PTZ Settings 58
4.2 Setting PTZ Presets, Patrols & Patterns 60

4.2.1 Customizing Presets 60
4.2.2 Calling Presets 60
4.2.3 Customizing Patrols 61
4.2.4 Calling Patrols 62
4.2.5 Customizing Patterns 63
4.2.6 Calling Patterns 64
4.2.7 Customizing Linear Scan Limit 64
4.2.8 Calling Linear Scan 65
4.2.9 One-touch Park 66
4.3 PTZ Control Panel 68
Chapter 5 Recording Settings 70
5.1 Configuring Parameters 70
5.2 Configuring Recording Schedule 73
5.3 Configuring Motion Detection Recording 77
5.4 Configuring Alarm Triggered Recording 79
5.5 Configuring VCA Event Recording 81
5.6 Manual Recording 83
5.7 Configuring Holiday Recording 84
5.8 Files Protection 86
5.8.1 Locking the Recording Files 86
Chapter 6 Playback 89
6.1 Playing Videos 89
6.1.1 Instant Playback 89
6.1.2 Playing Back by Normal Search 89
6.1.3 Playing back by Smart Search 93
6.1.4 Playing Back by Event Search 96
6.1.5 Playing Back by Tag 97
6.1.6 Playing Back by System Logs 100
6.1.7 Playing Back External File 102
6.2 Auxiliary Functions of Playback 103
6.2.1 Playing Back Frame by Frame 103
6.2.2 Thumbnails View 103
6.2.3 Fast View 104
6.2.4 Digital Zoom 104
6.2.5 File Management 105

Chapter 7 Backup 107
7.1 Backing up Record Files 107
7.1.1 Backing up by Normal Video Search 107
7.1.2 Backing up by Event Search 109
7.1.3 Backing up Video Clips 111
7.2 Managing Backup Devices 111
Chapter 8 Alarm Settings 113
8.1 Setting Motion Detection Alarm 113
8.2 Setting Sensor Alarms 115
8.3 Detecting Video Loss Alarm 118
8.4 Detecting Video Tampering Alarm 120
8.5 Handling Exceptions Alarm 122
8.6 Setting Alarm Response Actions 123
8.7 Triggering or Clearing Alarm Output Manually 127
Chapter 9 VCA Alarm 128
9.1 Face Detection 128
9.2 Vehicle Detection 130
9.3 Line Crossing Detection 131
9.4 Intrusion Detection 134
9.5 Region Entrance Detection 136
9.6 Region Exiting Detection 137
9.7 Unattended Baggage Detection 137
9.8 Object Removal Detection 138
9.9 Audio Exception Detection 138
9.10 Sudden Scene Change Detection 139
9.11 Defocus Detection 140
9.12 PIR Alarm 140
Chapter 10 VCA Search 141
10.1 Face Search 141
10.2 Behavior Search 143
10.3 Plate Search 144
10.4 People Counting 145
10.5 Heat Map 146
Chapter 11 Network Settings 148
11.1 Configuring General Settings 148

11.2 Configuring Wi-Fi Settings 150
11.3 Configuring Advanced Settings 151
11.3.1 Configuring Hik-Connect 151
11.3.2 Configuring DDNS 153
11.3.3 Configuring NTP Server 154
11.3.4 Configuring SNMP 155
11.3.5 Configuring More Settings 156
11.3.6 Configuring HTTPS Port 157
11.3.7 Configuring Email 159
11.3.8 Configuring NAT 161
11.3.9 Configuring Virtual Host 163
11.4 Checking Network Traffic 164
11.5 Configuring Network Detection 166
11.5.1 Testing Network Delay and Packet Loss 166
11.5.2 Exporting Network Packet 166
11.5.3 Checking the Network Status 167
11.5.4 Checking Network Statistics 168
Chapter 12 HDD Management 170
12.1 Initializing HDDs 170
12.2 Configuring Quota Mode 172
12.3 Checking HDD Status 174
12.3.1 Checking HDD Status in HDD Information Interface 174
12.3.2 Checking HDD Status in HDD Information Interface 174
12.4 HDD Detection 176
12.4.1 S.M.A.R.T. Settings 176
12.4.2 Bad Sector Detection 177
12.5 Configuring HDD Error Alarms 178
Chapter 13 Camera Settings 179
13.1 Configuring OSD Settings 179
13.2 Configuring Privacy Mask 180
13.3 Configuring Video Parameters 182
Chapter 14 NVR Management and Maintenance 183
14.1 Viewing System Information 183
14.2 Searching & Exporting Log Files 184
14.3 Importing/Exporting IP Camera Info 186

14.4 Importing/Exporting Configuration Files 187
14.5 Upgrading System 188
14.5.1 Upgrading by Local Backup Device 188
14.5.2 Upgrading by FTP 188
14.6 Restoring Default Settings 190
Chapter 15 Others 191
15.1 Configuring General Settings 191
15.2 Configuring DST Settings 193
15.3 Configuring More Settings 194
15.4 Managing User Accounts 195
15.4.1 Adding a User 195
15.4.2 Deleting a User 198
15.4.3 Editing a User 198
Chapter 16 Appendix 201
16.1 Specifications 201
16.2 Glossary 202
16.3 Troubleshooting 203
16.4 List of Compatible IP Cameras 211
16.4.1 List of Hikvision IP Cameras 211
16.4.2 List of Third-party IP Cameras 221

Chapter 1 Introduction

1.1 Front Panel

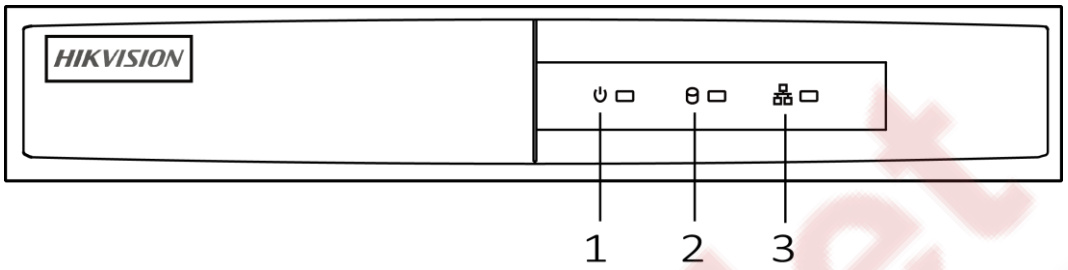


Figure 1-1 Front Panel

Table 1-1 Panel Description

No.	Name	Description
1	Power indicator	Turns green when NVR is powered up.
2	HDD indicator	Blinks red when HDD is reading/writing.
3	Network indicator	Blinks green when network connection is functioning normally.

1.2 Rear Panel

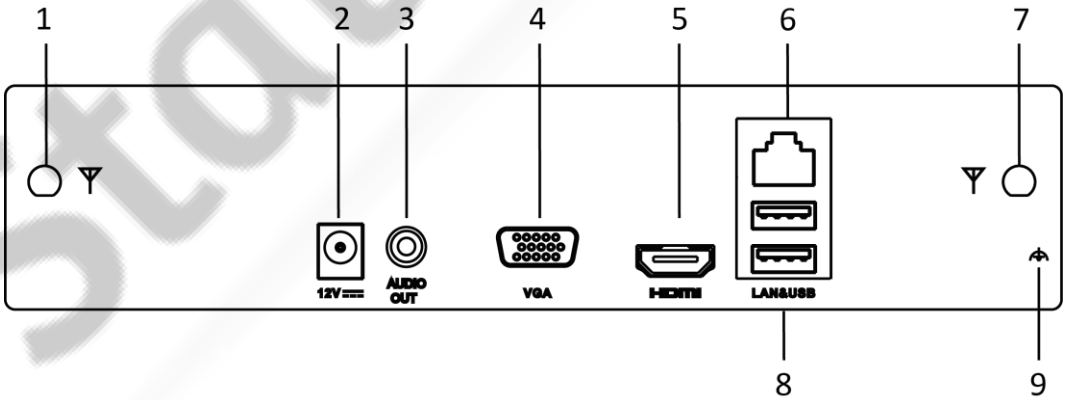


Figure 1-2 Rear Panel

Table 1-2 Panel Description

No.	Name	Description
1	Wi-Fi Antenna	Wi-Fi antenna interface.
2	Power supply	12 VDC power supply.
3	Audio out	2 RCA connectors for audio output.
4	VGA	VGA video output connector.
5	LAN	One RJ-45 10M/100M self-adaptive Ethernet interfaces provided.
6	Wi-Fi Antenna	Wi-Fi antenna interface.
7	HDMI	HDMI video output connector.
8	USB	Two USB 2.0 interface.
9	Ground	Ground (needs to be connected when device starts up).

1.3 IR Remote Control Operations

The NVR may also be controlled with the included IR remote control, shown in Figure 1-3.

NOTE

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

The IR Remote is set at the factory to control the NVR (using default Device ID# 255) without any additional steps. Device ID# 255 is the default universal device identification number shared by the NVRs. You may also pair an IR Remote to a specific NVR by changing the Device ID#, as follows:

1.3.1 Pairing (Enabling) the IR Remote to a Specific NVR (optional)

You can pair an IR Remote to a specific Hikvision NVR by creating a user-defined Device ID#. This feature is useful when using multiple IR Remotes and NVRs.

On the NVR:

Step 1 Go to General > More Settings.

Step 2 Type a number (255 digits maximum) into the Device No. field.

Step 3 :

Step 4 Press the DEV button.

Step 5 Use the Number buttons to enter the Device ID# that was entered into the NVR.

Step 6 Press Enter button to accept the new Device ID#.

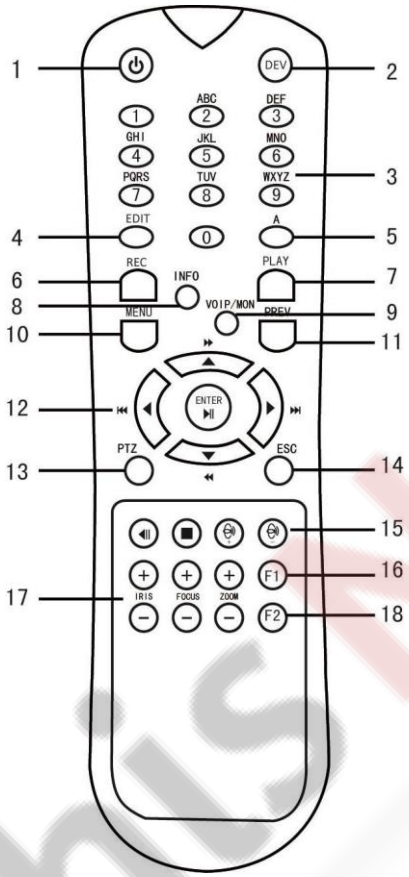


Figure 1-3 Remote Control

1.3.2 Unpairing (Disabling) an IR Remote from a NVR

To unpair an IR Remote from a NVR so that the unit cannot control any NVR functions, proceed as follows:

Press the DEV key on the IR Remote. Any existing Device ID# will be erased from the unit's memory and it will no longer function with the NVR.

NOTE

(Re)-enabling the IR Remote requires pairing to a NVR. See "Pairing the IR Remote to a Specific NVR (optional)," above.

The keys on the remote control closely resemble the ones on the front panel. See the table 1.4.

Table 1-3 IR Remote Functions

No.	Name	Function Description
1	**POWER ON/OFF**	• To Turn Power On: - If User Has Not Changed the Default NVR Device ID# (255): 1. Press Power On/Off button (1). - If User Has Changed the NVR Device ID#: 1. Press DEV button. 2. Press Number buttons to enter user-defined Device ID#. 3. Press Enter button. 4. Press Power button to start device. • To Turn NVR Off: - If User Is Logged On: 1. Hold Power On/Off button (1) down for five seconds to display the "Yes/No" verification prompt. 2. Use Up/Down Arrow buttons (12) to highlight desired selection. 3. Press Enter button (12) to accept selection. - If User Is *Not* Logged On: 1. Hold Power On/Off button (1) down for five seconds to display the user name/password prompt. 2. Press the Enter button (12) to display the on-screen keyboard. 3. Input the user name. 4. Press the Enter button (12) to accept input and dismiss the on-screen keyboard. 5. Use the Down Arrow button (12) to move to the "Password" field. 6. Input password (use on-screen keyboard or numeric buttons (3) for numbers). 7. Press the Enter button (12) to accept input and dismiss the on-screen keyboard. 8. Press the OK button on the screen to accept input and display the Yes/No" verification prompt (use Up/Down Arrow buttons (12) to move between fields) 9. Press Enter button (12) to accept selection.

		User name/password prompt depends on NVR is configuration. See “System Configuration” section.
2	**DEV**	Enable IR Remote: Press DEV button, enter NVR Device ID# with number keys, press Enter to pair unit with the NVR
		Disable IR Remote: Press DEV button to clear Device ID#; unit will no longer be paired with the NVR
3	**Numerals**	Switch to the corresponding channel in Live View or PTZ Control mode
		Input numbers in Edit mode
4	**EDIT**	Delete characters before cursor
		Check the checkbox and select the ON/OFF switch
5	**A**	Adjust focus in the PTZ Control menu
		Switch on-screen keyboards (upper and lower case alphabet, symbols, and numerals)
6	**REC**	Enter Manual Record setting menu
		Call a PTZ preset by using the numeric buttons in PTZ control settings
		Turn audio on/off in Playback mode
7	**PLAY**	Go to Playback mode
		Auto scan in the PTZ Control menu
8	**INFO**	Reserved
9	**VOIP**	Switches between main and spot output Zooms out the image in PTZ control mode
10	**MENU**	Return to Main menu (after successful login)
		N/A
		Show/hide full screen in Playback mode
12	**DIRECTION**	Navigate between fields and menu items
		Use Up/Down buttons to speed up/slow down recorded video, and Left/Right buttons to advance/rewind 30 secs in Playback mode
		Cycle through channels in Live View mode

		Control PTZ camera movement in PTZ control mode
	ENTER	Confirm selection in any menu mode
		Checks checkbox
		Play or pause video in Playback mode
		Advance video a single frame in single-frame Playback mode
		Stop/start auto switch in auto-switch mode
13	**PTZ**	Enter PTZ Control mode
14	**ESC**	Go back to previous screen
		N/A
15	**RESERVED**	Reserved
16	**F1**	Select all items on a list
		N/A
		Switch between play and reverse play in Playback mode
17	**PTZ Control**	Adjust PTZ camera iris, focus, and zoom
18	**F2**	Cycle through tab pages
		Switch between channels in Synchronous Playback mode

1.3.3 Troubleshooting Remote Control:

NOTE

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

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

Step 1 Go to Menu > Settings > General > More Settings by operating the front control panel or the mouse.

Step 2 Check and remember NVR ID#. The default ID# is 255. This ID# is valid for all the IR remote controls.

Step 3 Press the DEV button on the remote control.

Step 4 Enter the NVR ID# you set in step 2.

Step 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:

- Batteries are installed correctly and the polarities of the batteries are not reversed.
- Batteries are fresh and not out of charge.
- IR receiver is not obstructed.
- No fluorescent lamp is used nearby

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

1.4 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:

Step 1 Plug USB mouse into one of the USB interfaces on the front panel of the NVR.

Step 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 1-4 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.

1.5 Input Method Description

Figure 1-4 Soft Keyboard (1)

Figure 1-5 Soft Keyboard (2)

Description of the buttons on the soft keyboard:

Table 1-5 Description of the Soft Keyboard Icons

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

Chapter 2 Getting Started

2.1 Device Startup and Activation

2.1.1 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

Step 1 Plug the power supply into an electrical outlet. It is HIGHLY recommended that an Uninterruptible Power Supply (UPS) be used in conjunction with the device.

Shutting down

Step 1 Go to **Menu > Shutdown.**

Figure 2-1 Shutdown Menu

Step 2 Click the **Shutdown** button.

Step 3 Click the **Yes** button.

Step 4 When the dialog box "Please power off" shows, unplug the power supply.

Rebooting

Step 1 Go to **Menu > Shutdown**.

Step 2 Click the **Logout** button to lock the NVR or the Reboot button to reboot the NVR.

2.1.2 Activating Your Device

Purpose:

For the first-time access, you need to activate the device by setting an admin password. No operation is allowed before activation. You can also activate the device via Web Browser, SADP or Client Software.

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

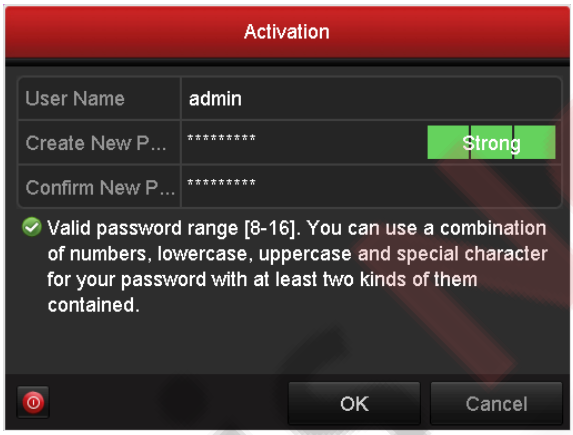


Figure 2-2 Settings Admin Password

WARNING

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

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

Step 3 When the device is activated, the system pops up the message box to remind you to remember the password. And you can click **Yes** to continue to export the GUID file for the future password resetting.

Figure 2-3 Export GUID File Remind

Step 4 Insert the U flash disk to your device, and export the GUID file to the U flash disk in the Reset Password interface. Please refer to Chapter2.1.5 Resetting Your Password for the instructions of password resetting.

Figure 2-4 Export GUID File

NOTE

- Please keep your GUID file properly for future password resetting.
- If Admin's password is modified, the following menu pops up. Optionally, click the Yes button to duplicate the password to IP cameras that are connected with default protocol.

Figure 2-5 Attention Interface

2.1.3 Using the Unlock Pattern for Login

For the Admin user, you can configure the unlock pattern for device login.

Configuring the Unlock Pattern

Step 1 After the device is activated, you can enter the following interface to configure the device unlock pattern.

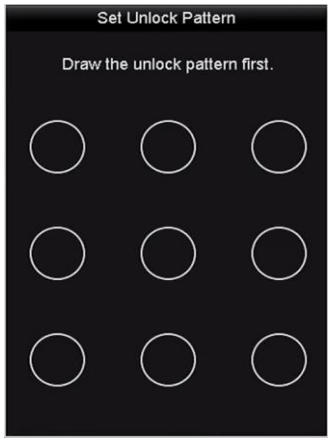


Figure 2-6 Set Unlock Pattern

Step 2 Use the mouse to draw a pattern among the 9 dots on the screen. Release the mouse when the pattern is done.

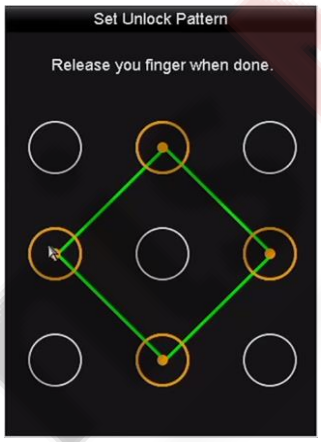


Figure 2-7 Draw the Pattern

NOTE

- Connect at least 4 dots to draw the pattern.
- Each dot can be connected for once only.

Step 3 Draw the same pattern again to confirm it. When the two patterns match, the pattern is configured successfully.

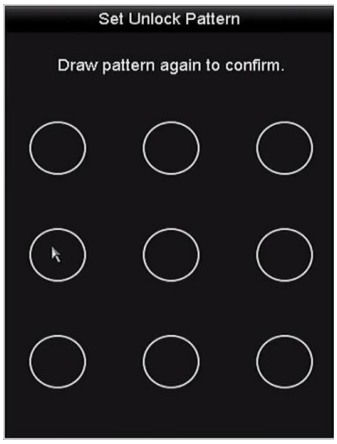


Figure 2-8 Confirm the Pattern

NOTE

If the two patterns are different, you must set the pattern again.

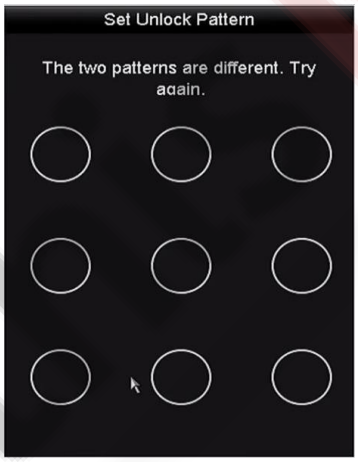


Figure 2-9 Reset the Pattern

Logging in via Unlock Pattern

NOTE

- Only the *admin* user has the permission to unlock the device.
- Please configure the pattern first before unlocking. Please refer to *Configuring the Unlock Pattern.*

Step 1 Right click the mouse on the screen and select the menu to enter the interface.

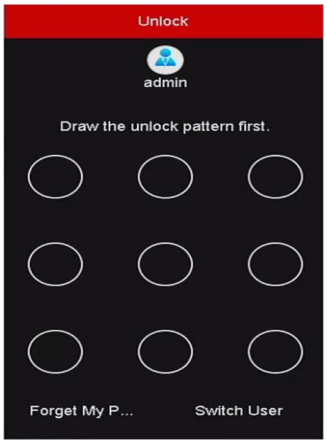


Figure 2-10 Draw the Unlock Pattern

Step 2 Draw the pre-defined pattern to unlock to enter the menu operation.

NOTE

- If you have forgotten your pattern, you can select the **Forget My Pattern** or **Switch User** option to enter the normal login dialog box.
- When the pattern you draw is different from the pattern you have configured, you should try again.
- If you have drawn the wrong pattern for more than 5 times, the system will switch to the normal login mode automatically.

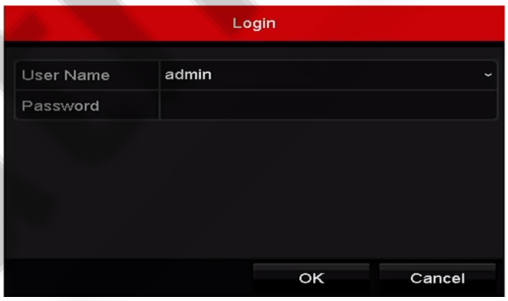


Figure 2-11 Normal Login Dialog Box

2.1.4 Login and Logout

User Login

Purpose:

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

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

Figure 2-12 Login Interface

Step 2 Input password.

Step 3 Click **OK** to log in.

NOTE

- When you forget the password of the admin, you can click **Forget Password** to reset the password. Please refer to Chapter *2.1.5 Resetting Your Password* for details.
- In the Login dialog box, if you enter the wrong password 7 times, the current user account will be locked for 60 seconds.

User Logout

Purpose:

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

Step 1 Enter the Shutdown menu.

Menu > Shutdown

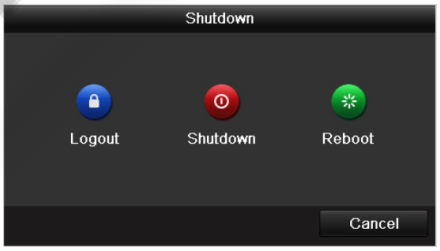


Figure 2-13 Logout

Step 2 Click **Logout**.

NOTE

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.

2.1.5 Resetting Your Password

When you forget the password of the admin, you can reset the password by importing the GUID file. The GUID file must be exported and saved in the local U flash disk after you have activated the device (refer to Chapter *2.1.2 Activating Your Device*).

Step 1 On the user login interface, click **Forget Password** to enter the Reset Password interface.

NOTE

Please insert the U flash disk stored with the GUID file to the NVR before resetting password.

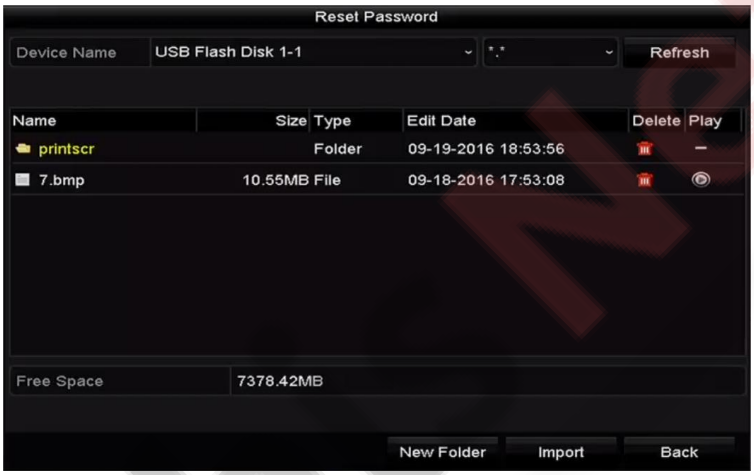


Figure 2-14 Reset Password

Step 2 Select the GUID file from the U flash disk and click **Import** to import the file to the device.

NOTE

If you have imported the wrong GUIE file for 7 times, you will be not allowed to reset the password for 30 minutes.

Step 3 After the GUID file is successfully imported, enter the reset password interface to set the new admin password. Refer to Chapter 2.1.2 Activating Your Device for details.

Step 4 Click OK to set the new password. You can export the new GUID file to the U flash disk for future password resetting.

NOTE

When the new password is set, the original GUID file will be invalid. The new GUID file should be exported for future password resetting. You can also enter the User>User Management interface to edit the admin user and export the GUID file.

2.2 Using Wizard for Basic Configuration

By default, the Setup Wizard starts once the NVR has loaded, as shown in Figure 2-15.

Figure 2-15 Start Wizard Interface

Operating the Setup Wizard:

The Setup Wizard can walk you through some important settings of the NVR. If you don't want to use the Setup Wizard at that moment, click the **Cancel** button. You can also choose to use the Setup Wizard next time by leaving the "Start wizard when the device starts?" checkbox checked.

Step 1 Click **Next** button to enter the date and time settings page.

Figure 2-16 Date and Time Settings

Step 2 Click **Next** to enter wireless network settings page.

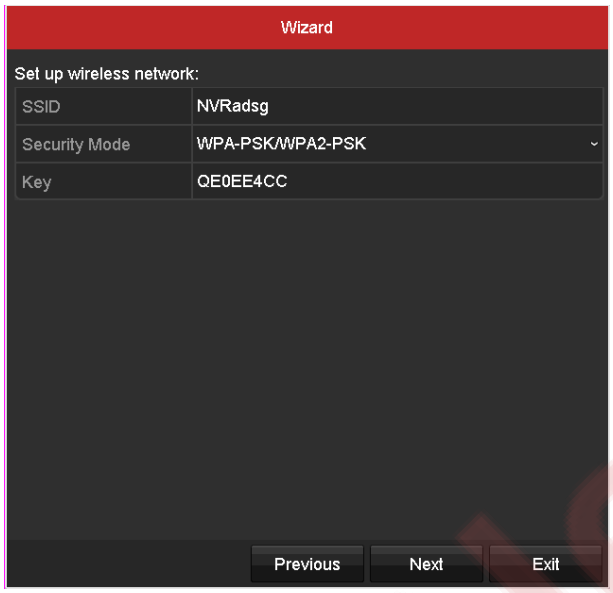


Figure 2-17 Wireless Network Settings

Step 3 Configure wireless network parameters, including **SSID, Security Mode,** and **Key**.

- **SSID**: It is the short for Service Set Identifier. SSID is the WiFi name that the device provides.
- **Security Mode**: The security protocol you choose to secure wireless networks.
- **Key**: Enter the encryption key.

Step 4 Click **Next** button to enter network setup page.

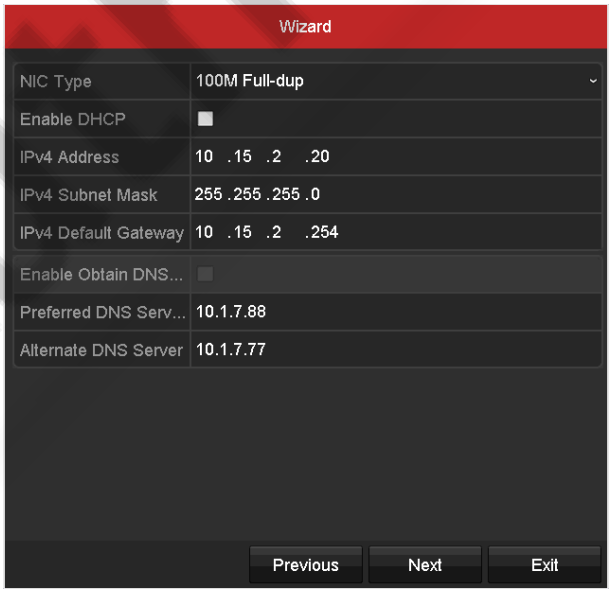


Figure 2-18 Network Settings

Step 5 Click **Next** button to enter the Hik-Connect settings page. Refer to Chapter 11.3.1 Configuring Hik-Connect for detailed instructions.

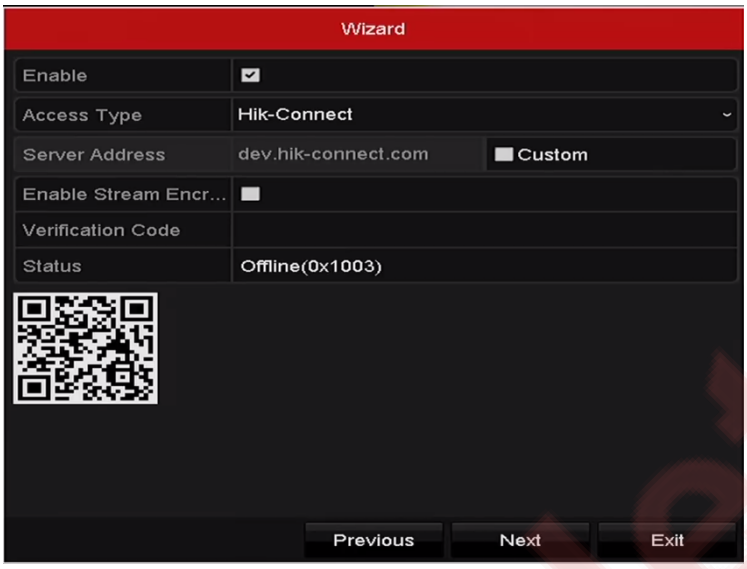


Figure 2-19 Hik-Connect Settings

Step 6 Click **Next** button to enter the advanced network parameter page. You can enable UPnP, DDNS and set other ports according to your needs.

Figure 2-20 Advanced Network Parameters

Step 7 Click **Next** button to enter the HDD management page.

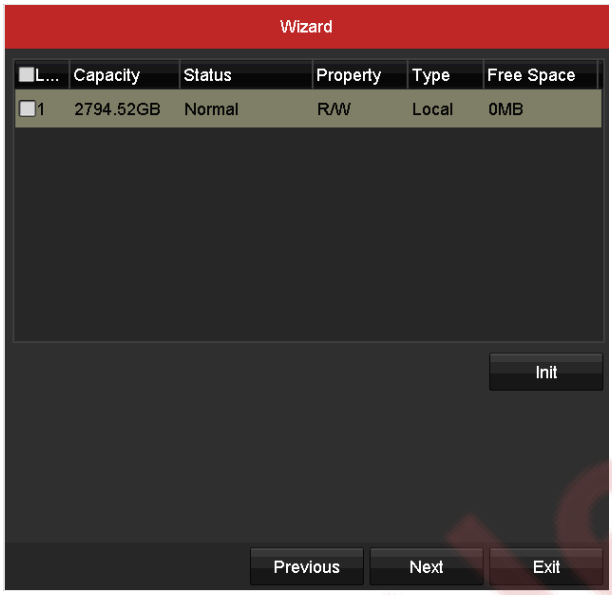


Figure 2-21 HDD Management

Step 8 To initialize the HDD, select an HDD and click the **Init** button. Initialization removes all the data saved in the HDD.

Step 9 Click **Next** button to enter the adding IP camera page.

- **Search**: Click **Search** to search the online IP Camera.
- **Security**: It shows whether it is active or inactive. Before adding the camera, make sure the IP camera to be added is in active status.
- **One-touch Activate**: If the camera is inactive, 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.
- **Add**: Select cameras and click **Add** to add them.
- **Enable H.265**: When you check the checkbox of **Enable H.265**, the NVR can automatically switch to the H.265 stream of IP camera (which supports H.265 video format) for the initial access.

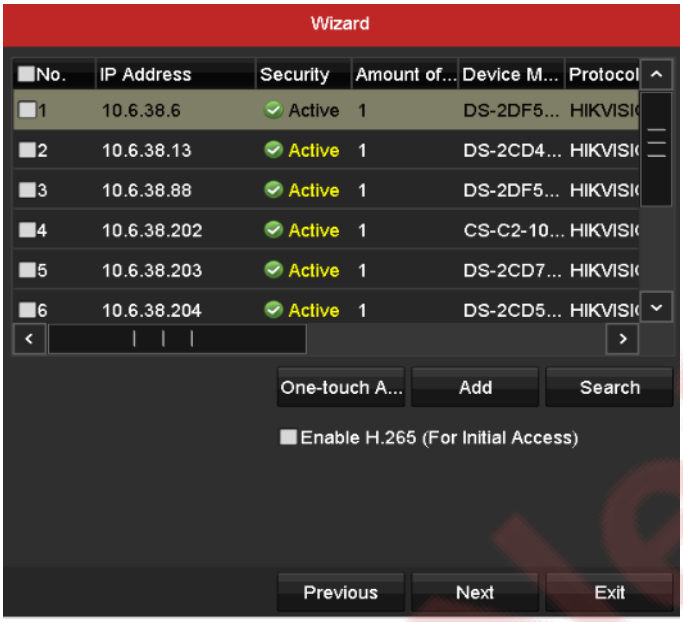


Figure 2-22 IP Cameras

Step 10 Click **Next** button.

Step 11 Configure the recording schedule for the added IP Cameras.

Figure 2-23 Record Settings

Step 12 Click **OK** to complete the startup Setup Wizard.

2.3 Adding and Connecting the IP Cameras

Before you start:

- Ensure the network connection between IP camera and NVR is valid and correct.

NOTE

Cameras in the product bundle and bound IP cameras will automatically connect the NVR Wi-Fi.

- Activate the IP cameras to add. Please refer to the User Manual for activating the inactive IP camera.

2.3.1 Activating the IP Camera

Purpose:

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

Step 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 **Password** status shows whether it is active or inactive.

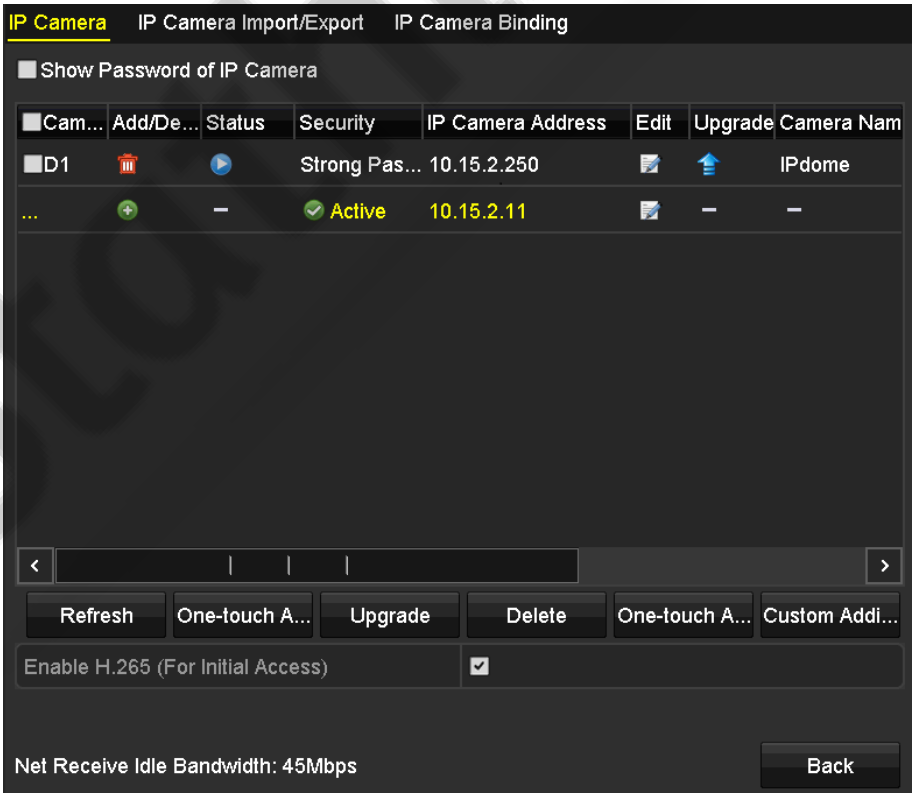


Figure 2-24 IP Camera Management Interface

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

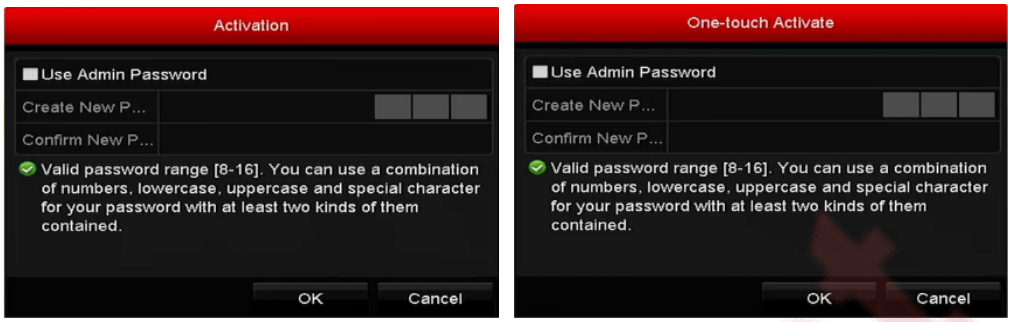


Figure 2-25 Activate the Camera

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

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

Figure 2-26 Set New Password

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

WARNING

Strong Password recommended–We highly recommend you create a strong password of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

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

2.3.2 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.

Adding the IP Cameras

- **OPTION 1:**

Step 1 Click to select an idle window in the live view mode.

Step 2 Click the icon in the center of the windw to pop up the adding IP camera interface.

Figure 2-27 Icon of Adding IP Camera

Step 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.

Figure 2-28 Quick Adding IP Camera Interface

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:**

Step 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 2-29 Adding IP Camera Interface

Step 2 The online cameras with same network segment will be detected and displayed in the camera list.

Step 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 (with the same login password) from the list.

NOTE

Make sure the camera to add has already been activated.

Step 4 (For the encoders with multiple channels only) check the **Channel Port** checkbox in the pop-up window, as shown in the following figure, and click **OK** to add multiple channels.

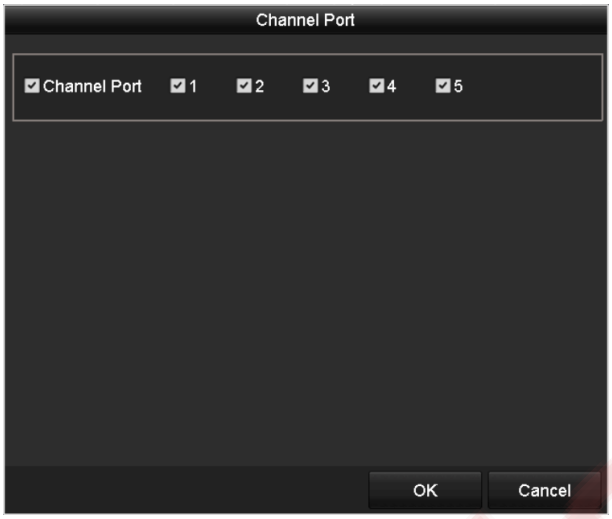


Figure 2-30 Selecting Multiple Channels

- **OPTION 3:**

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

Figure 2-31 Custom Adding IP Camera Interface

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

NOTE

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

Step 3 (Optional) Check the checkbox of **Continue to Add** to add other IP cameras.

Step 4 Click **Add** to add the camera. The successfully added cameras are listed in the interface.

Refer to the following table for the description of the icons

Table 2-1 Description of 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/medium/weak/risk)

NOTE

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

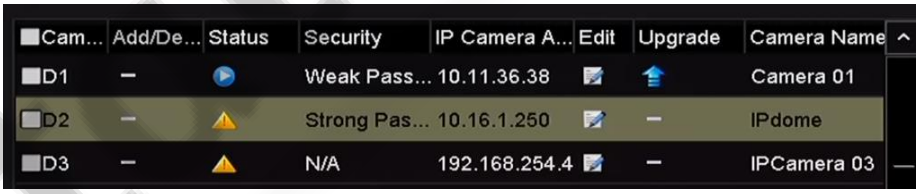


Figure 2-32 Security Level of IP Camera's Password

Enabling the Password of IP Camera Visible

For the admin login user account, you can check the checkbox of **Show Password of IP Camera** to enable the show the passwords of the successfully added IP cameras in the list.

You must enter the admin password to confirm permission.

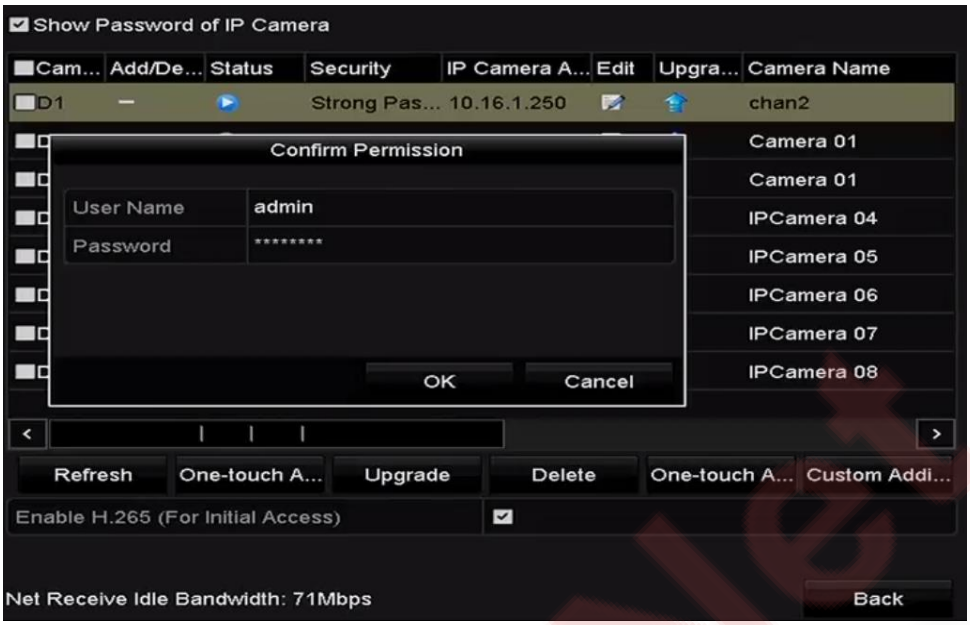


Figure 2-33 List of Added IP Cameras

Enabling the H.265 Stream Access

You can check the checkbox of **Enable H.265**, the NVR can automatically switch to the H.265 stream of IP camera (which supports H.265 video format) for the initial access.

2.3.3 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.

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

Figure 2-34 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.

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

- To edit advanced parameters:

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

Figure 2-35 Network Configuration of the Camera

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

Figure 2-36 Password Configuration of the Camera

Step 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.

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

Figure 2-37 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.

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

NOTE

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.

NOTE

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

After adding the customized protocols, you can see the protocol name is listed in the dropdown list, please refer to Figure 2-38.

Figure 2-38 Protocol Setting

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

2.3.4 Binding IP Camera

Purpose:

Bind the IP camera by adding its serial number in Wi-Fi NVR. The bound IP cameras will automatically connect NVR Wi-Fi signal. Up to 4/8 IP cameras can be bound.

NOTE

- Only camera of specified models can be added. Ask the manufacturer for models.
- Cameras in bundle are bound by default.

Step 1 Go to **Menu > Camera > Camera**.

Step 2 Select the **IP Camera Binding** tab.

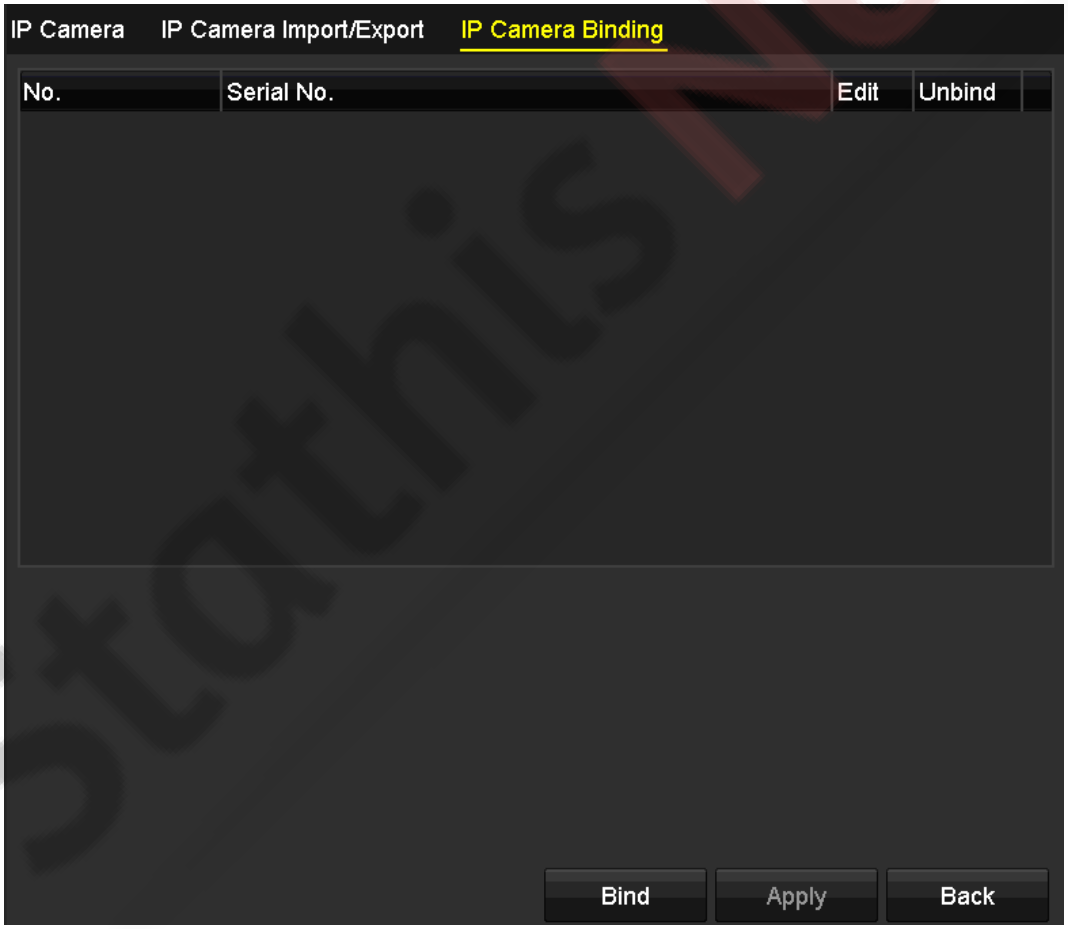


Figure 2-39 IP Camera Binding

Step 3 Click **Bind**.

Step 4 Enter the IP camera **Serial No.**

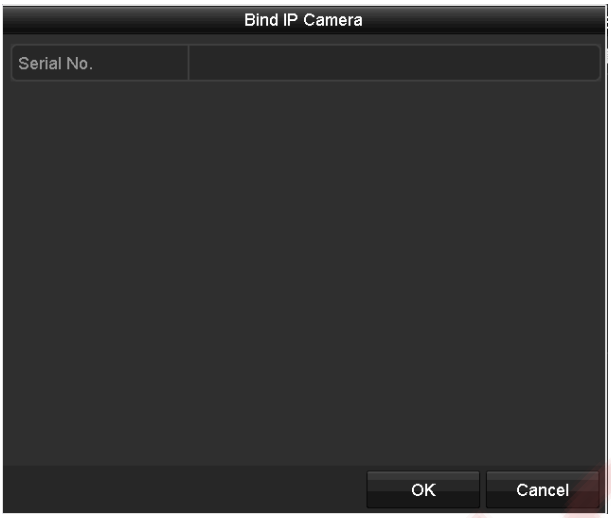


Figure 2-40 Bind IP Camera

Step 5 Click **OK**.

Chapter 3 Live View

3.1 Introduction of Live View

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

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, VCA and sensor alarm)
	Record (manual record, schedule record, motion detection, VCA and alarm triggered record)
	Alarm and Record
	Event/Exception (motion detection, VCA, sensor alarm or exception information, appears at the lower-left corner of the screen. Please refer to *Chapter 8.6 Setting Alarm Response Actions* for details.)

3.2 Operations in Live View Mode

3.2.1 Using the Mouse in Live View

Table 3-2 Mouse Operation in Live View

Name	Description
Common Menu	Quick access to the sub-menus which you frequently visit.
Menu	Enter the main menu of the system by right clicking the mouse.
Single Screen	Switch to the single full screen by choosing channel number from the dropdown list.
Multi-screen	Adjust the screen layout by choosing from the dropdown list.
Previous Screen	Switch to the previous screen.
Next Screen	Switch to the next screen.
Start/Stop Auto-switch	Enable/disable the auto-switch of the screens.
Start Recording	Start continuous recording or motion detection recording of all channels.
Add IP Camera	Enter the IP Camera Management interface, and manage the cameras.
Playback	Enter the playback interface and start playing back the video of the selected channel immediately.
PTZ Control	Enter the PTZ control interface.
.Network Quick Settings	Configure the Hik-Connect, DDNS, UPnP, DHCP, PPPoE settings.
Output Mode	Four modes of output supported, including Standard, Bright, Gentle and Vivid.

NOTE

- The *dwell time* of the live view configuration must be set before using **Start Auto-switch**.
- If the corresponding camera supports intelligent function, the Reboot Intelligence option is included when right-clicking mouse on this camera.

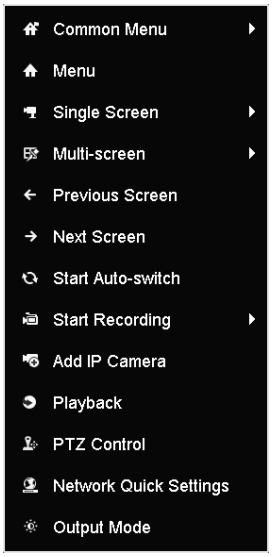


Figure 3-1 Right-click Menu

3.2.2 Quick Setting Toolbar in Live View Mode

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

Figure 3-2 Quick Setting Toolbar

Table 3-3 Description of Quick Setting Toolbar Icons

Icon	Description	Icon	Description	Icon	Description
/	Enable/Disable Manual Record		Instant Playback	/	Mute/Audio on
	PTZ Control		Digital Zoom		Image Settings
	Live View Strategy		Information		Main/Sub-Stream
	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 is for zooming in the live image. You can zoom in the image to different proportions (1 to16X) by moving the sliding bar from to . You can also scroll the mouse wheel to control the zoom in/out.

Figure 3-3 Digital Zoom

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

  You can set the image parameters like brightness, contrast, saturation and hue according to the actual demand.

Figure 3-4 Image Settings- Customize

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

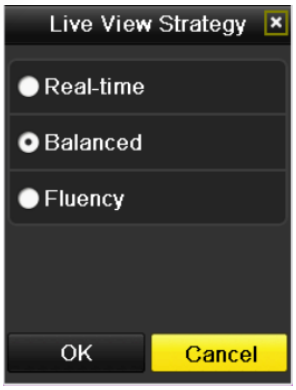


Figure 3-5 Live View Strategy

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

Figure 3-6 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.

Step 1 Enter the Live View Settings interface.

Menu> Configuration> Live View

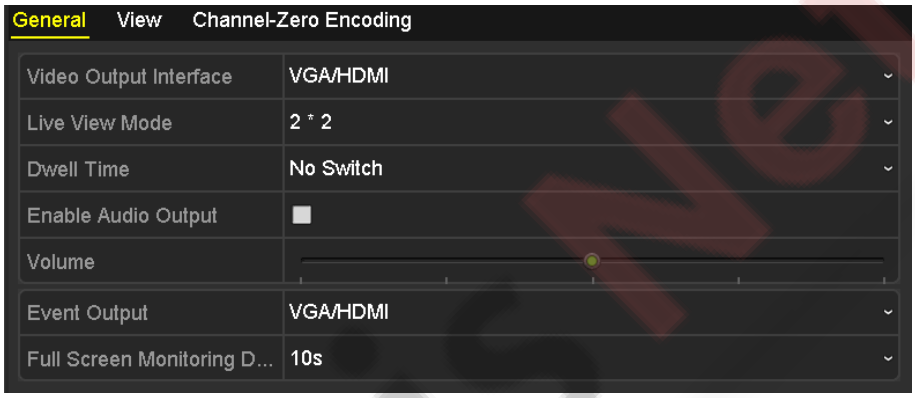


Figure 3-7 Live View-General

The settings available in this menu include:

- **Video Output Interface:** Designates the output to configure the settings for.
- **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.

Step 2 Set cameras order.

Figure 3-8 Live View- Camera Order

1) Select a **View** mode in  。
2) Select the small window, and double-click on the channel number to display the channel on the window.
3) You can click  button to start live view for all the channels and click  to stop all the live view.
4) Click the **Apply** button to save the setting.

You can also click-and-drag the camera to the desired window on the live view interface to set the camera order.

Step 3 Set the stream type for live view of camera.

1) Click the **More Settings** to enter the more settings interface.
2) Select the camera to configure from the list.
3) Select the stream type to main stream, sub-stream or Auto.

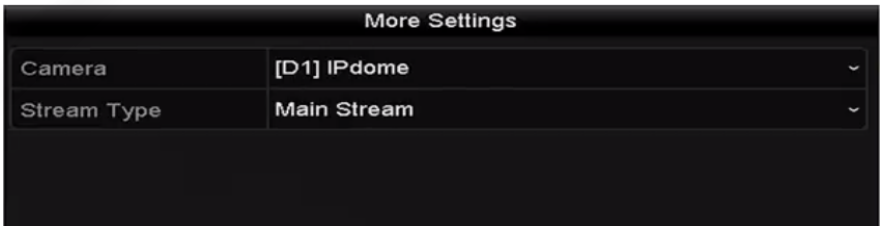


Figure 3-9 Stream Type Settings

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

5) (Optional) You can click the **Copy** button to copy the stream type settings of the current camera to other camera(s).

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.

Step 1 Enter the Live View Settings interface.

Menu > Configuration> Live View

Step 2 Select the Channel-Zero Encoding tab.

Figure 3-10 Live View- Channel-Zero Encoding

Step 3 Check the checkbox of **Enable Channel Zero Encoding**.

Step 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 all the 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.

Step 1 Enter the PTZ Settings interface.

Menu > Camera > PTZ

Figure 4-1 PTZ Settings

Step 2 Click the **PTZ Parameters** button to set the PTZ parameters.

Figure 4-2 PTZ- General

Step 3 Choose the camera for PTZ setting in the **Camera** dropdown list.

Step 4 Enter the parameters of the PTZ camera.

NOTE

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

Step 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.

Step 1 Enter the PTZ Control interface.

Menu > Camera > PTZ

Figure 4-3 PTZ Settings

Step 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.

Step 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.

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

Or press the PTZ button on the front panel or click the PTZ Control icon in the quick setting bar, or select the PTZ option in the right-click menu to show the PTZ control panel.

Step 2 Choose C**amera** in the dropdown list.

Step 3 Click the button to show the general settings of the PTZ control.

Figure 4-4 PTZ Panel - General

Step 4 Click to enter the preset No. in the corresponding text field.

Step 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.

Step 1 Enter the PTZ Control interface.

Menu>Camera>PTZ

Figure 4-5 PTZ Settings

Step 2 Select patrol No. in the drop-down list of patrol.

Step 3 Click the **Set** button to add key points for the patrol.

Figure 4-6 Key point Configuration

Step 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.

Step 5 Click the **Add** button to add the next key point to the patrol, or you can click the **OK** button to save the key point to the patrol.

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

4.2.4 Calling Patrols

Purpose:

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

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

Or press the PTZ button on the front panel or click the PTZ Control icon in the quick setting bar, or select the PTZ option in the right-click menu to show the PTZ control panel.

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

Figure 4-7 PTZ Panel - General

Step 3 Select a patrol in the dropdown list and click the **Call Patrol** button to call it.

Step 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.

Step 1 Enter the PTZ Control interface.

Menu > Camera > PTZ

Figure 4-8 PTZ Settings

Step 2 Choose pattern number in the dropdown list.

Step 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.

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

Or press the PTZ button on the front panel or click the PTZ Control icon in the quick setting bar, or select the PTZ option in the right-click menu to show the PTZ control panel.

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

Figure 4-9 PTZ Panel - General

Step 3 Click the **Call Pattern** button to call it.

Step 4 Click the **Stop Pattern** button to stop calling it.

4.2.7 Customizing Linear Scan Limit

Purpose:

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

NOTE

This function is supported by some certain models.

Step 1 Enter the PTZ Control interface.

Menu > Camera > PTZ

Figure 4-10 PTZ Settings

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

NOTE

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

4.2.8 Calling Linear Scan

NOTE

Before operating this function, make sure the connected camera supports the linear scan and is in HIKVISION protocol.

Purpose:

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

Step 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.

Step 2 Click the button to show the one-touch function of the PTZ control.

Figure 4-11 PTZ Panel - One-touch

Step 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

NOTE

Before operating this function, make sure the connected camera supports the linear scan and is in HIKVISION protocol.

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).

Step 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.

Step 2 Click the button to show the one-touch function of the PTZ control.

Figure 4-12 PTZ Panel - One-touch

Step 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.

NOTE

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

Step 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 , or select the PTZ option in the right-click menu.

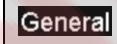
Click the **Configuration** button on the control panel, and you can enter the PTZ Settings interface.

NOTE

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

Figure 4-13 PTZ 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 Positioning		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)

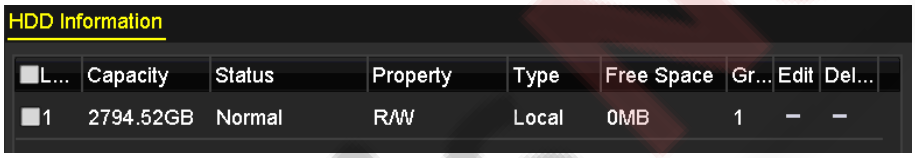


Figure 5-1 HDD

Step 1 Enter the Record settings interface to configure the recording parameters:

Menu > Record > Parameters

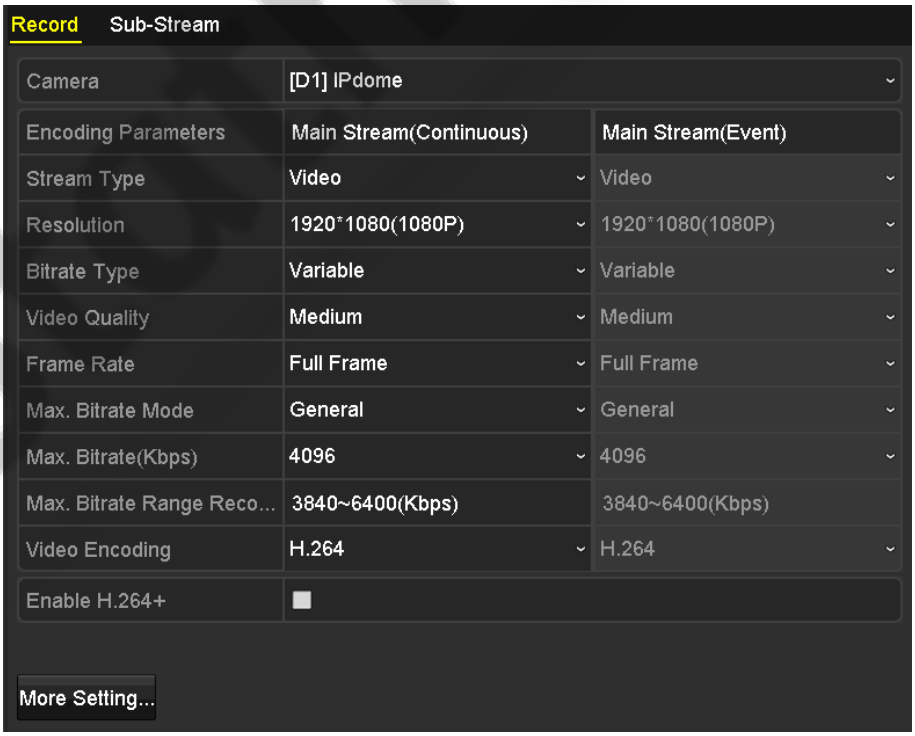


Figure 5-2 Recording Parameters

Step 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.

Video Encode: select the video encoding to H.265 or H.264.

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.

NOTE

The H.265 and H.264+ should be supported by the connected IP camera.

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

Figure 5-3 More Settings

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

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

NOTE

- You can enable the ANR (Automatic Network Replenishment) function via the web browser (Configuration > Storage > Schedule Settings > Advanced) to save the video files in the IP

camera when the network is disconnected, and synchronize the files to the NVR when the network is resumed.

- The parameters of Main Stream (Event) are read-only.

Step 3 Parameters Settings for Sub-stream

1) Enter the Sub-stream tab page.

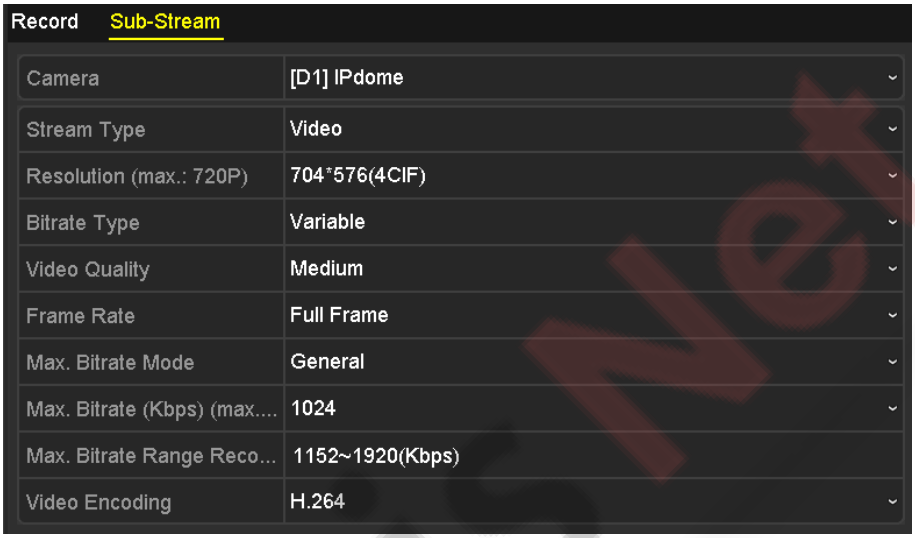


Figure 5-4 Sub-stream Parameters

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

5.2 Configuring Recording Schedule

Purpose:

Set the record schedule, and then the camera automatically starts/stops recording according to the configured schedule. In this chapter, we take the record schedule procedure as an example.

Step 1 Enter the Record Schedule interface.

Menu > Record > Schedule

Step 2 Configure Record Schedule

1) Select Record Schedule.

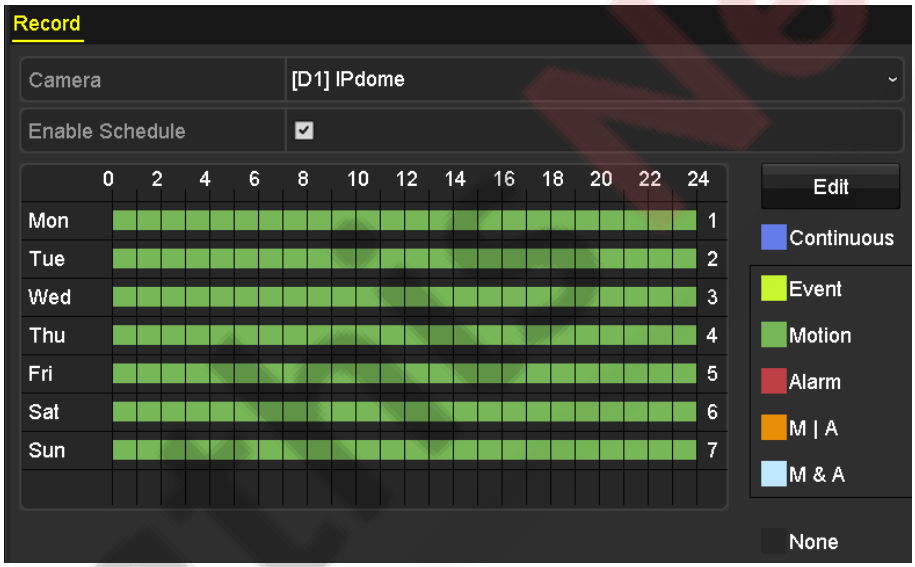


Figure 5-5 Record Schedule

Different recording types are marked in different color icons.

- **Continuous:** scheduled recording.
- **Event**: recording triggered by all event triggered alarm.
- **Motion**: recording triggered by motion detection.
- **Alarm:** recording triggered by alarm.
- **M/A:** recording triggered by either motion detection or alarm.
- **M&A:** recording triggered by motion detection and alarm.

NOTE

You can delete the set schedule by clicking the **None** icon.

2) Choose the camera you want to configure.
3) Check the checkbox of **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**

NOTE

The all-day continuous recording is configured for the device by factory default.

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

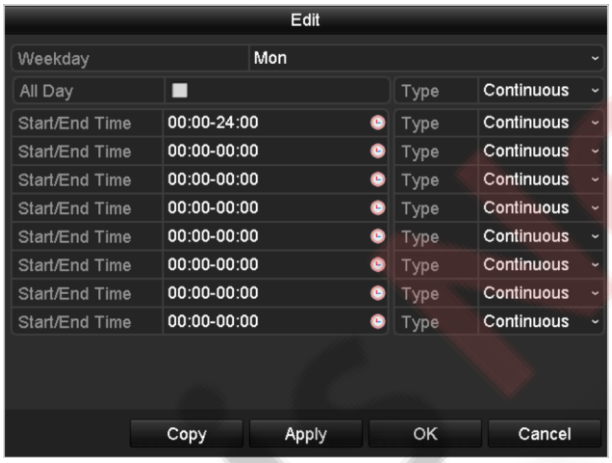


Figure 5-6 Recording Schedule Interface

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

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

Figure 5-7 Edit Schedule

III. To arrange other schedule, set the Start/End time for each period.

NOTE

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

IV. Select the record type in the dropdown list.

NOTE

- To enable Motion, Alarm, M | A (motion or alarm), M & A (motion and alarm) and VCA (Video Content Analysis) triggered recording, you must configure the motion detection settings, alarm input settings or VCA settings as well. For detailed information, refer to *Chapter 9* VCA Alarm and *Chapter 10 VCA Search*.
- 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. If the schedule can also be applied to other days, click **Copy**.

Figure 5-8 Copy Schedule to Other Days

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

VI. 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.

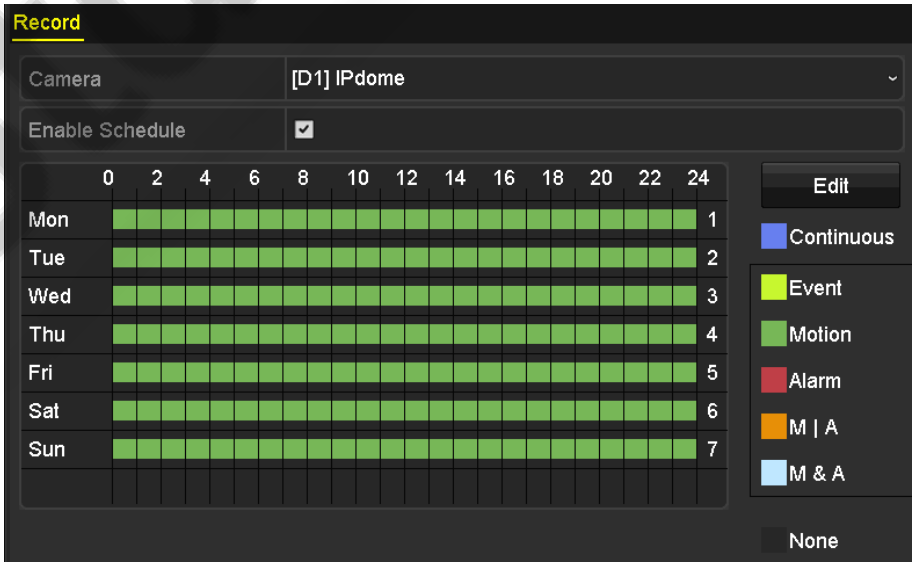


Figure 5-9 Draw the Schedule

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

Step 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.

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

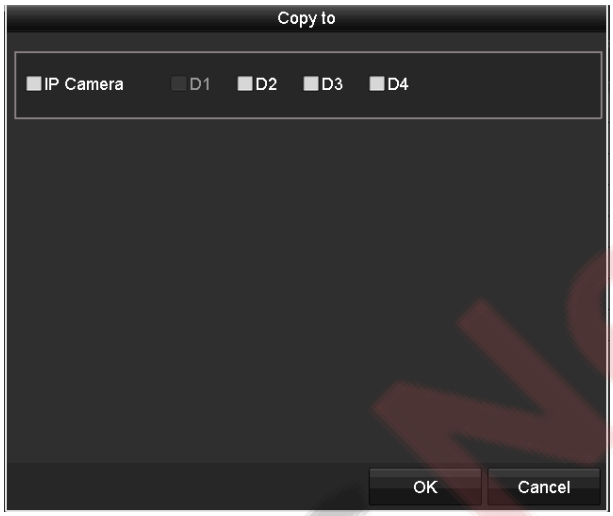


Figure 5-10 Copy Schedule to Other Channels

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.

Step 1 Enter the Motion Detection interface.

Menu > Camera > Motion

Figure 5-11 Motion Detection

Step 2 Configure Motion Detection:

1) Choose camera you want to configure.
2) Check the checkbox of **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**.
4) Click **Settings**, and the message box for channel information pops up.

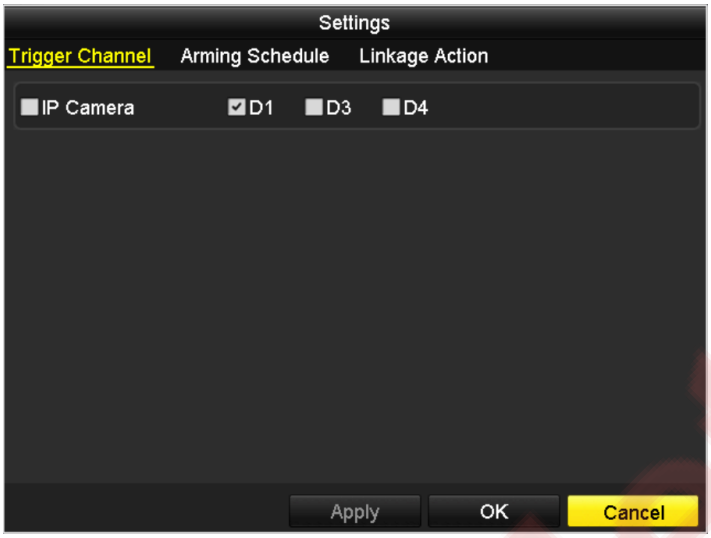


Figure 5-12 Motion Detection Handling

1) Select the channels which you want the motion detection event to trigger recording.
2) Click **Apply** to save the settings.
3) Click **OK** to back to the upper level menu.
4) Exit the Motion Detection menu.

Step 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.

Step 1 Enter the Alarm settings interface.

Menu > Configuration > Alarm

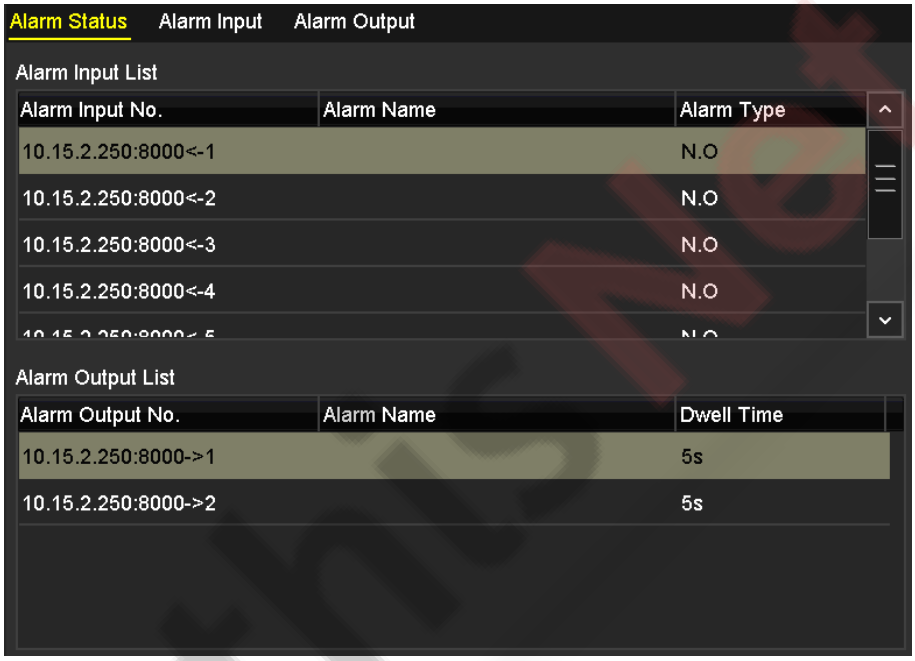


Figure 5-13 Alarm Settings

Step 2 Click Alarm Input.

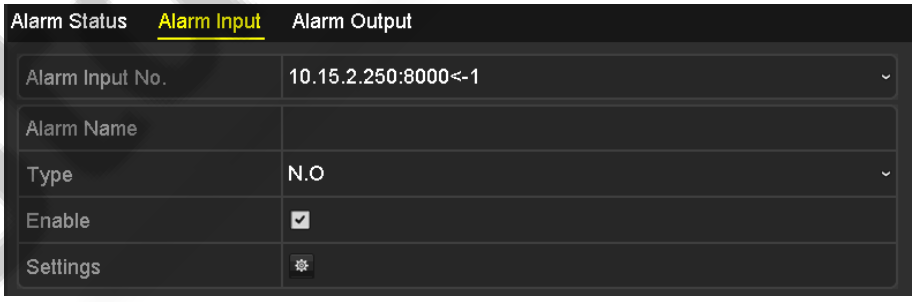


Figure 5-14 Alarm Settings- Alarm Input

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

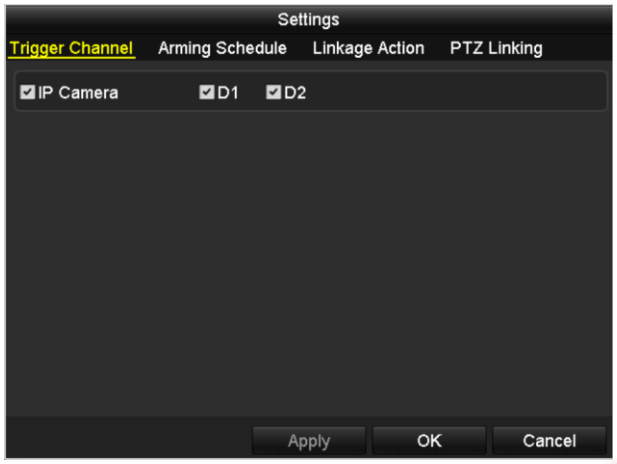


Figure 5-15 Alarm Settings

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.

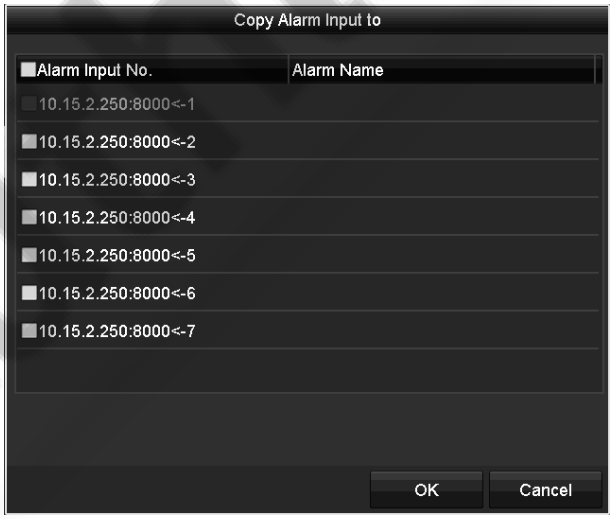


Figure 5-16 Copy Alarm Input

Step 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, 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).

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

Menu > Camera > VCA

Figure 5-17 VCA Settings

Step 2 Configure the detection rules for VCA events. For details, please refer to *Chapter 9 VCA Alarm.*

Step 3 Click the icon to configure the alarm linkage actions for the VCA events.

Step 4 Select **Trigger Channel** tab and select one or more channels which will start to record when VCA alarm is triggered.

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

Figure 5-18 Set Trigger Camera of VCA Alarm

Step 6 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 recording. Using manual recording, you need to manually cancel the record. The manual recording is prior to the scheduled recording.

Step 1 Enter the Manual settings interface.

Menu> Manual

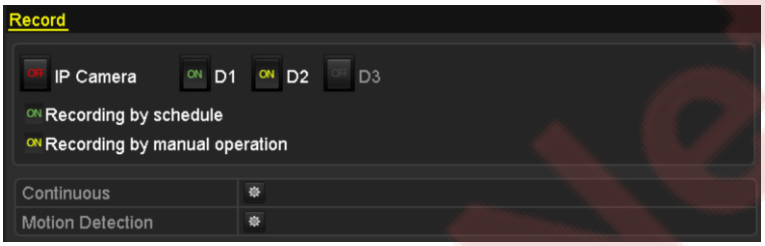


Figure 5-19 Manual Record

Step 2 Enable the Manual Recording.

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

Step 3 Disable manual record.

Click the status button to change ON to OFF.

NOTE

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

5.7 Configuring Holiday Recording

Purpose:

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

Step 1 Enter the Record setting interface.

Menu > Record > Holiday

Figure 5-20 Holiday Settings

Step 2 Enable Edit Holiday schedule.

1) Click  to enter the Edit interface.

Figure 5-21 Edit Holiday Settings

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

Step 3 Enter record schedule settings interface to edit the holiday recording schedule. See *Chapter 5.2 Configuring Recording Schedule.*

5.8 Files Protection

Purpose:

You can lock the videos or set the HDD property to read-only to protect the videos from being overwritten.

5.8.1 Locking the Recording Files

Lock File when Playback

Step 1 Enter Playback interface.

Menu > Playback

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

Figure 5-22 Normal/Smart Playback

Step 3 During playback, click the button to lock the current video.

NOTE

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

Step 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 5-23 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

Step 1 Enter Export setting interface.

Menu > Export

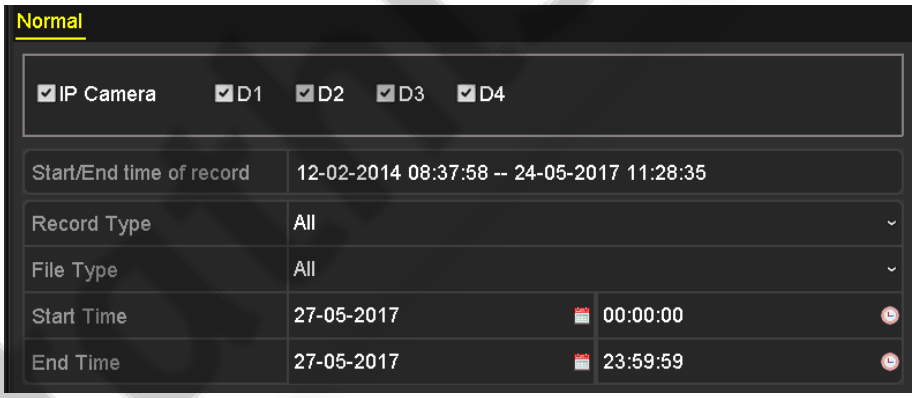


Figure 5-24 Export

Step 2 Select the channels you want to search by checking the checkbox to .

Step 3 Configure the record type, file type start/end time.

Step 4 Click **Search** to show the results.

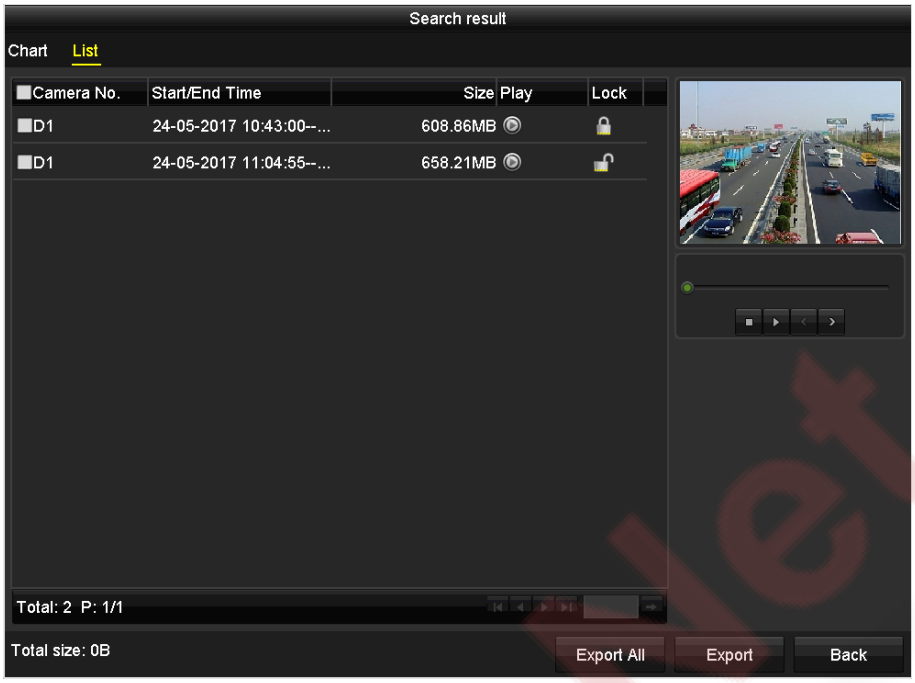


Figure 5-25 Export- Search Result

Step 5 Protect the record files.

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

NOTE

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

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

Figure 5-26 Unlocking Attention

Chapter 6 Playback

6.1 Playing Videos

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.

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

NOTE

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

Figure 6-1 Instant Playback Interface

6.1.2 Playing Back by Normal Search

Playback by Channel

Enter the Playback interface.

Right click a channel in live view mode and select Playback from the menu, as shown in Figure 6-2.

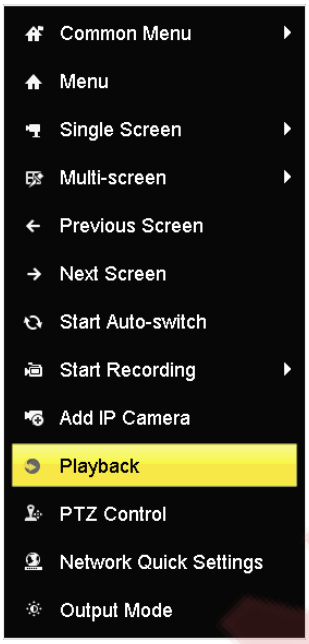


Figure 6-2 Right-Click Menu

Playback by Time

Purpose

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

Step 1 Enter playback interface.

Menu > Playback

Step 2 Select the **Normal/Smart** in the drop-down list on the top-left side.

Step 3 Select a camera in the camera list.

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

Figure 6-3 Playback Calendar

If there are videos for that camera in that day, in the calendar, the icon for that day is displayed in different colors for different recording types: blue for continuous recording and red for event recording.

Step 5 Click the Normal radio button to start playing the continuous recorded files.

Playback Interface

You can use the toolbar in the bottom part of Playback interface to control playing progress, as shown in Figure 6-4.

Figure 6-4 Playback Interface

Figure 6-5 Toolbar of Playback

You can click the channel(s) to execute simultaneous playback of multiple channels.

NOTE

- The 05-06-2016 16:33:42 -- 06-07-2016 10:53:24 indicates the start/end time of the videos.
- 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

Item	Button	Operation	Button	Operation
Smart Search		Draw quadrilateral for the motion detection		Search the matched video
		Set full screen for motion detection		Draw line for the line crossing detection
		Draw quadrilateral for the intrusion detection		Filter video files by setting the target characters
Operations	/	Audio on/Mute	/	Start/Stop clipping
		Lock File		Add default tag
		Add customized tag		File management for video clips, locked files, and tags
		Digital Zoom		
Playing Control	/	Pause/Play	/	Reverse play/ Pause
		Slow forward		Stop
		30s forward		30s reverse
		Next day		Fast forward
		Previous day		
Time Bar Scaling		Previous/Next period	30mins	Play the time bar in 30 minutes (default)
	1h	Play the time bar in 1 hour	2h	Play the time bar in 2 hours
	6h	Play the time bar in 6 hours	24h	Play the time bar in 24 hours

NOTE

The playing speed of 256X is supported.

6.1.3 Playing back by Smart Search

Purpose

The smart playback function provides an easy way to get through the less effective information. When you select the smart playback mode, the system will analyze the video containing the motion, line or intrusion detection 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.

Step 1 Enter Playback interface.

Menu > Playback

Step 2 Select the **Normal/Smart** in the drop-down list on the top-left side.

Step 3 Select a camera in the camera list.

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

Figure 6-6 Playback by Smart Search

Step 5 Click the Smart radio button to switch to the playback by smart search.

Step 6 Set the rules and areas for smart search of line crossing detection, intrusion detection or motion detection event triggered recording.

- **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 hold the mouse on the image to draw the detection area manually. You can also click the button to set the full screen as the detection area.

Step 7 (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 6-7 Set Result Filter

Step 8 (Optional) Click to enter the Smart Settings to configure the related parameters.

- **Skip the Non-Related Video**: check the checkbox to enable the device to skip non-related video files.
- **Play Non-Related Video**: set the playing speed to 8X/4X/2X/1X when playing the non-related video files.
- **Play Related Video**: set the playing speed to 4X/2X/1X when playing the non-related video files.

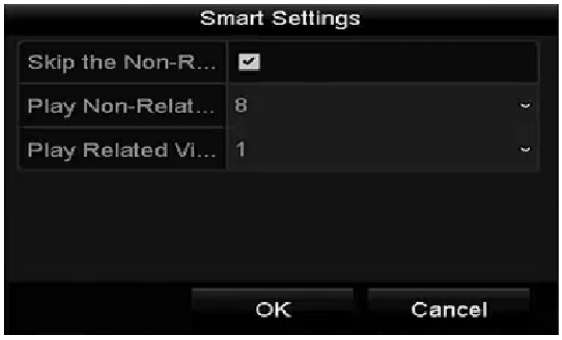


Figure 6-8 Smart Settings

6.1.4 Playing Back by Event Search

Purpose

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

Step 1 Enter the Playback interface.

Menu > Playback

Step 2 Select the **Event** in the drop-down list on the top-left side.

Step 3 Select the major type to **Alarm Input**, **Motion,** or **VCA** as the event type.

NOTE

We take playback by VCA as the example in the following instructions.

Figure 6-9 Event Search Interface

Step 4 Select the minor type of VCA from the drop-down list. (Please refer to *Chapter 9 VCA Alarm* for the details of VCA detection types).

NOTE

For configuring the VCA recording, please refer to *Chapter 5.5 Configuring VCA Event Recording*; and for details of VCA detection types, please refer to *Chapter 9 VCA Alarm*.

Step 5 Select the camera(s) for searching, and set the **Start Time** and **End Time**.

Step 6 Click **Search** button to get the search result information. You may refer to the right-side bar for the result.

Step 7 Select a result item and click button to play back the file.

NOTE

Pre-play and post-play can be configured.

Step 8 Enter the playback interface.

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

Figure 6-10 Interface of Playback by Event

You can click or button to select the previous or next event..

6.1.5 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

Step 1 Enter Playback interface.

Menu > Playback

Step 2 Search and play back the record file(s). Refer to *Chapter 6.1.1* for the detailed information about searching and playback of the record files.

Figure 6-11 Interface of Playback by Time

Click button to add default tag.

Click button to add customized tag and input tag name.

NOTE

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

Step 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).

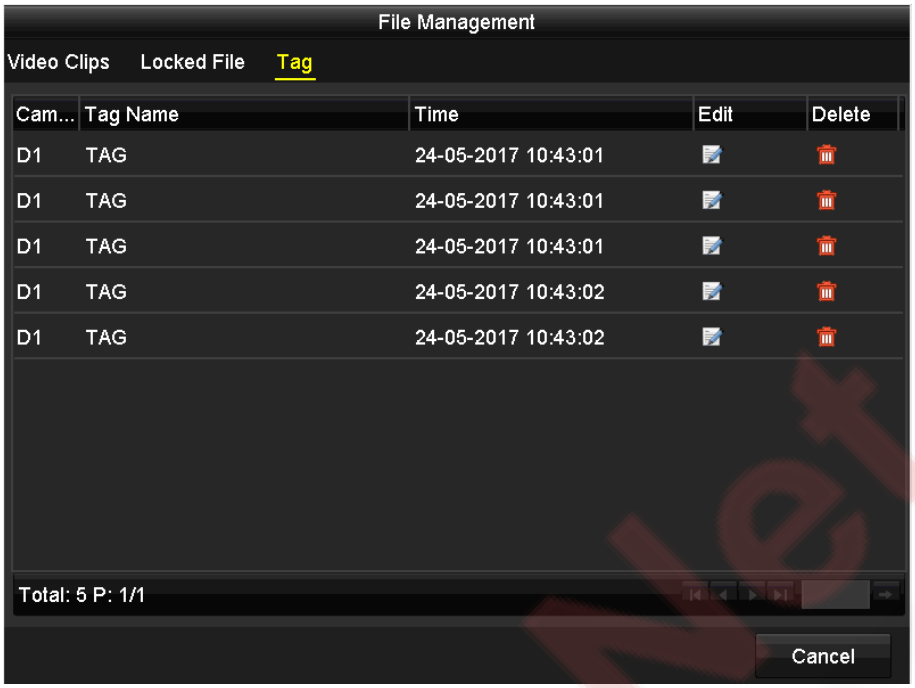


Figure 6-12 Tag Management Interface

Playing Back by Tag

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

Step 2 Select the stream to Main Stream or Sub Stream.

Step 3 Choose channels, edit start time and end time, and then click **Search** to enter Search Result interface.

NOTE

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

Step 4 Click button to play back the selected tag file.

Figure 6-13 Interface of Playback by Tag

NOTE

Pre-play and post-play can be configured.

You can click or button to select the previous or next tag.

6.1.6 Playing Back by System Logs

Purpose:

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

Step 1 Enter Log Information interface.

Menu>Maintenance>Log Information

Step 2 Click **Log Search** tab to enter Playback by System Logs.

Step 3 Set search time and type and click **Search** button.

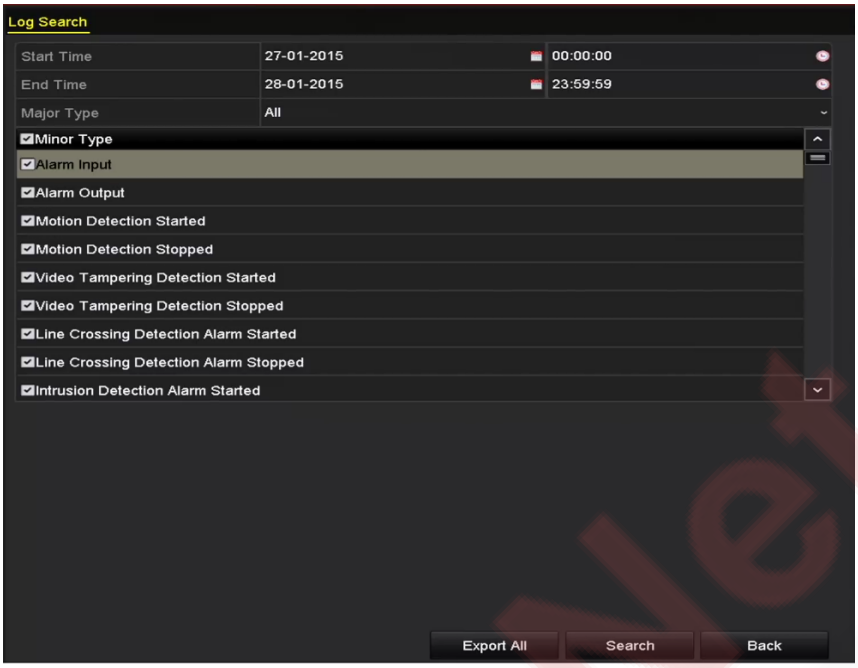


Figure 6-14 System Log Search Interface

Step 4 Choose a log with record file and click button to enter Playback interface.

NOTE

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

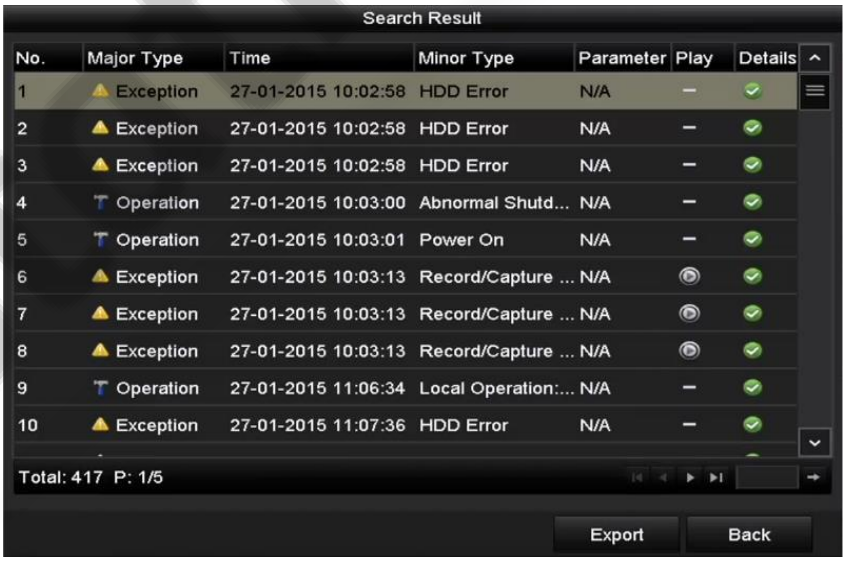


Figure 6-15 Result of System Log Search

Step 5 Playback interface.

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

Figure 6-16 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.

Step 1 Enter Tag Search interface.

Menu > Playback

Step 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.

Step 3 Select and click the button to play back it. And you can adjust the playback speed by clicking and .

Figure 6-17 Interface of External File Playback

6.2 Auxiliary Functions of Playback

6.2.1 Playing Back Frame by Frame

Purpose:

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

Go to Playback interface.

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

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

6.2.2 Thumbnails View

With the thumbnails view on the playback interface, you can conveniently locate the required video files on the time bar.

Step 1 Enter the playback interface and start to play the video files.

Step 2 Move the mouse to the time bar to get the preview thumbnails of the video files. Select and double click on a required thumbnail to enter the full-screen playback.

Figure 6-18 Thumbnails View

NOTE

The thumbnail view is supported only in the 1X single-camera playback mode.

6.2.3 Fast View

You can hold the mouse to drag on the time bar to get the fast view of the video files.

Step 1 Enter the playback interface and start to play the video files.

Step 2 Use the mouse to hold and drag through the playing time bar to fast view the video files.

Step 3 Release the mouse to the required time point to enter the full-screen playback.

NOTE

The fast view is supported only in the 1X single-camera playback mode.

6.2.4 Digital Zoom

Step 1 Click the button on the playback control bar to enter Digital Zoom interface.

Step 2 You can zoom in the image to different proportions (1 to16X) by moving the sliding bar from to . You can also scroll the mouse wheel to control the zoom in/out.

Figure 6-19 Draw Area for Digital Zoom

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

6.2.5 File Management

You can manage the video clips in playback, locked files and tags you have added in the playback mode.

Step 1 Enter the playback interface.

Step 2 Click on the toolbar to enter the file management interface.

Figure 6-20 File Management

Step 3 You can view the saved video clips, lock/unlock the files, and edit the tags which you added in the playback mode.

Step 4 If required, select the items and click **Export All** or **Export** to export the clips/ files/tags to local storage device.

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.

Step 1 Enter Export interface.

Menu > Export > Normal

Step 2 Select the cameras to search.

Step 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.

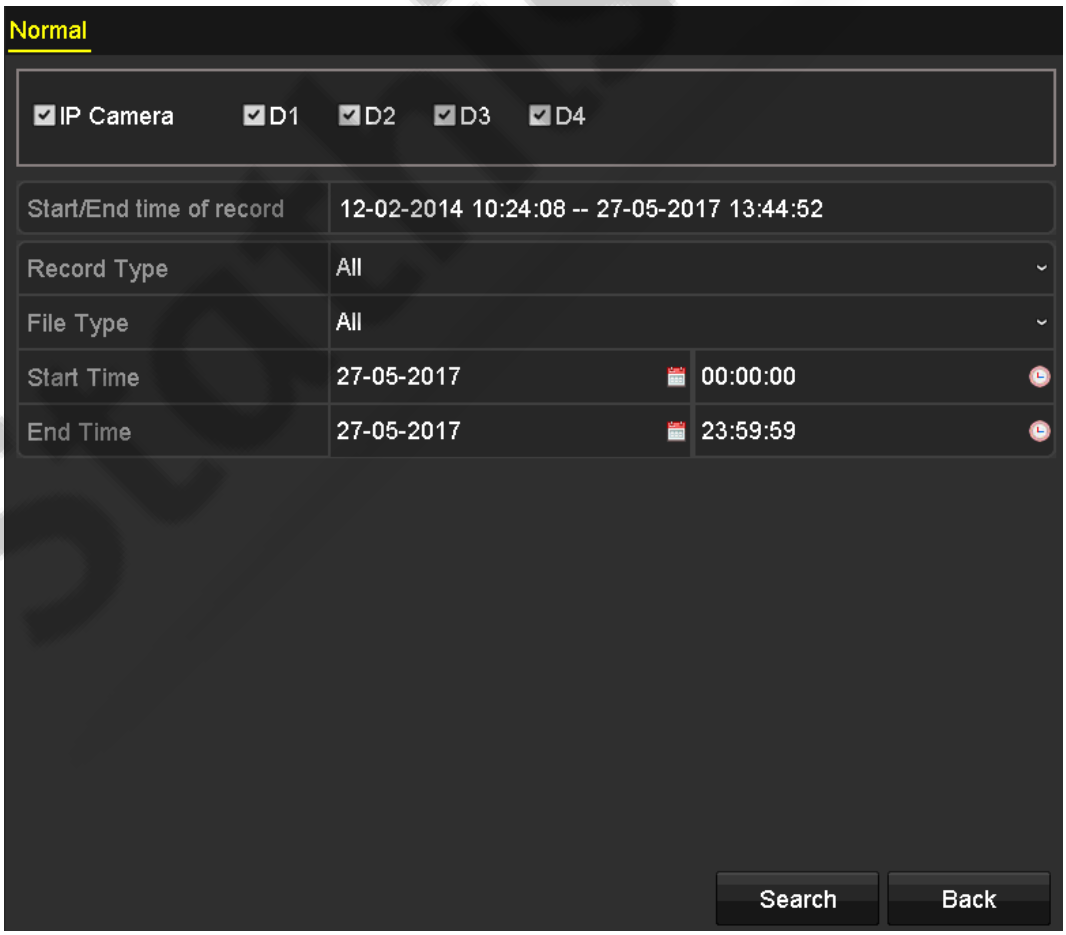


Figure 7-1 Normal Video Search for Backup

Step 4 Select video files 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.

NOTE

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

Figure 7-2 Result of Normal Video Search for Backup

Step 5 Export the videos.

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.

NOTE

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".

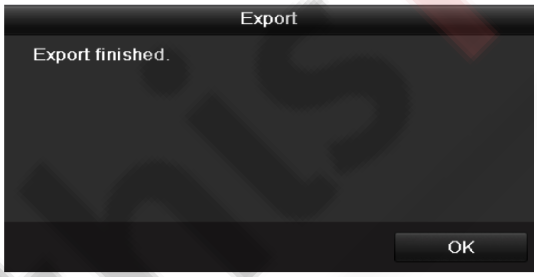


Figure 7-4 Export Finished

NOTE

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

7.1.2 Backing up by Event Search

Purpose:

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

Step 1 Enter Export interface.

Menu > Export > Event

Step 2 Select the cameras to search.

Step 3 Select the event type to alarm input, motion, or VCA.

Figure 7-5 Event Search for Backup

Step 4 Set the search conditions and click **Search** button to enter the search result interface.

Step 5 The matched video files are displayed in Chart or List display mode. Select video files from the Chart or List interface to export.

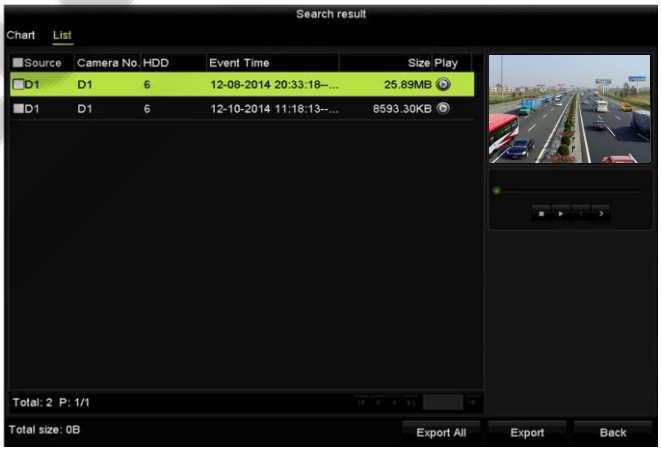


Figure 7-6 Result of Event Search

Step 6 Export the video files. Please refer to step 5 of *Chapter 7.1.1* Backing up by Normal Video Search for details.

7.1.3 Backing up Video Clips

Purpose:

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

Step 1 Enter Playback interface. Please refer to *Chapter 6.1 Playing Videos.*

Step 2 During playback, use buttons  or  in the playback toolbar to start or stop clipping record file(s).

Step 3 Click  to enter the file management interface.

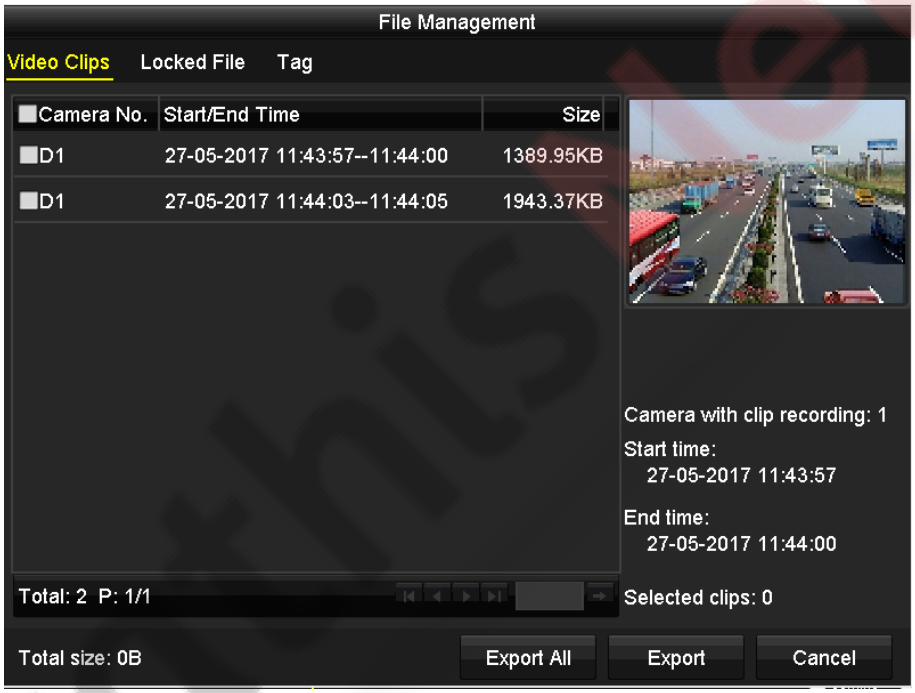


Figure 7-7 Video Clips Export Interface

Step 4 Export the video clips in playback. Please refer to step 5 of *Chapter 7.1.1 Backing up by Normal Video Search* for details.

7.2 Managing Backup Devices

Step 1 Enter the Export interface.

Figure 7-8 Storage Device Management

Step 2 Backup device management.

- Click **New Folder** button if you want to create a new folder in the backup device.
- Select a record file or folder in the backup device and click button if you want to delete it.
- Click **Erase** button if you want to erase the files from a re-writable CD/DVD.
- Click **Format** button to format the backup device.

NOTE

If the inserted storage device is not recognized:

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

Chapter 8 Alarm Settings

8.1 Setting Motion Detection Alarm

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

Menu> Camera> Motion

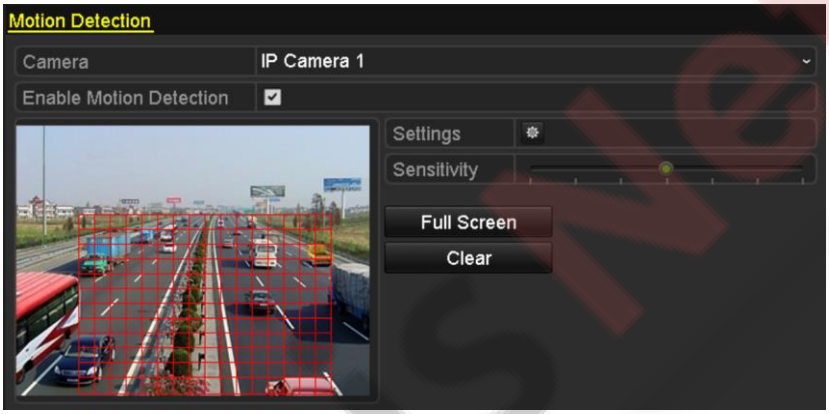


Figure 8-1 Motion Detection Setup Interface

Step 2 Set up detection area and sensitivity.

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

Click button and set alarm response actions.

Step 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.

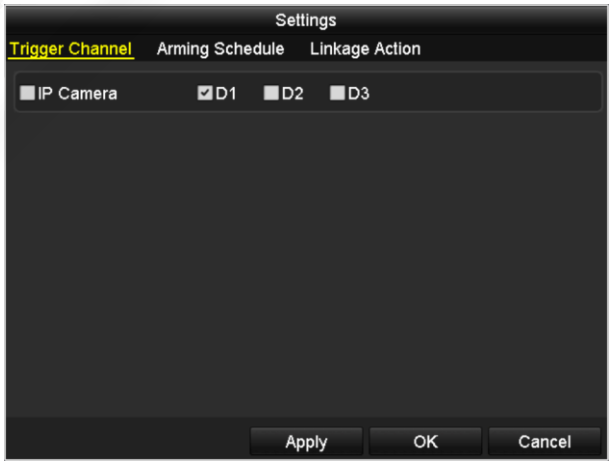


Figure 8-2 Set Trigger Camera of Motion Detection

Step 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

NOTE

Time periods shall not be repeated or overlapped.

Figure 8-3 Set Arming Schedule of Motion Detection

Step 5 Click **Handling** tab to set up alarm response actions of motion alarm (please refer to *Chapter 8.6 Setting Alarm Response Actions*).

Step 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.

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

Menu > Configuration > Alarm

Step 2 Select Alarm Input tab.

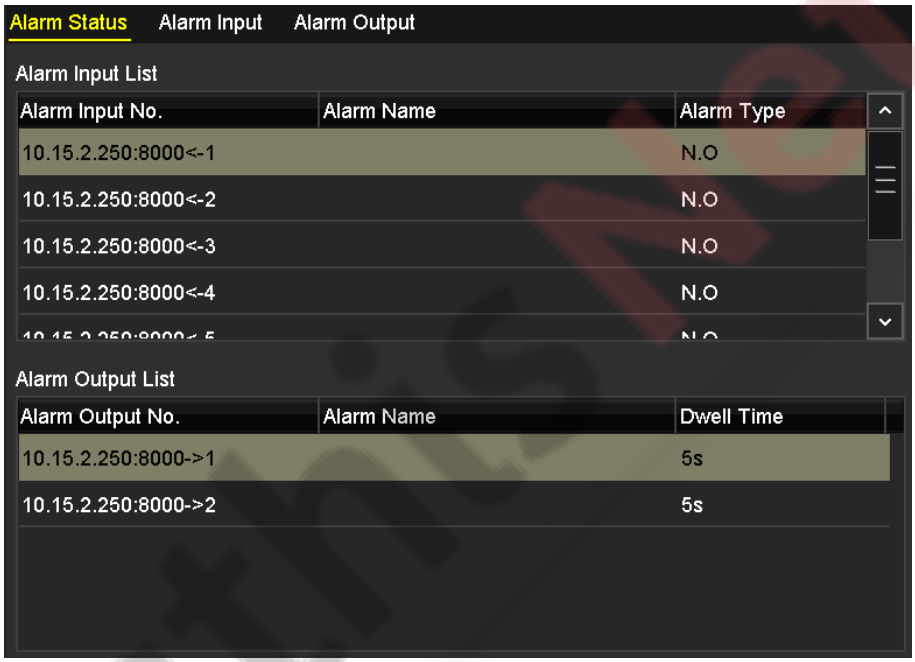


Figure 8-4 Alarm Status Interface of System Configuration

Step 3 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.

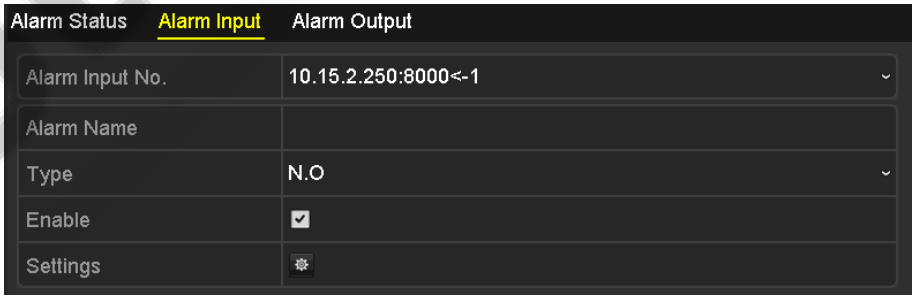


Figure 8-5 Alarm Input Setup Interface

Step 4 (Optional) Enable the one-key disarming for local alarm input 1 (Local<-1).

1) Check the checkbox of Enable One-Key Disarming.
2) Click the **Settings** button to enter the linkage action settings interface.

3) Select the alarm linkage action (s) you want to disarm for the local alarm input1. The selected linkage actions include the Full Screen Monitoring, Audible Warning, Notify Surveillance Center, Send Email and Trigger Alarm Output.

NOTE

When the alarm input 1 (Local<-1) is enabled with one-key disarming, the other alarm input settings are not configurable.

Step 5 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.

Step 6 Select **Arming Schedule** tab to set the arming schedule of handling actions.

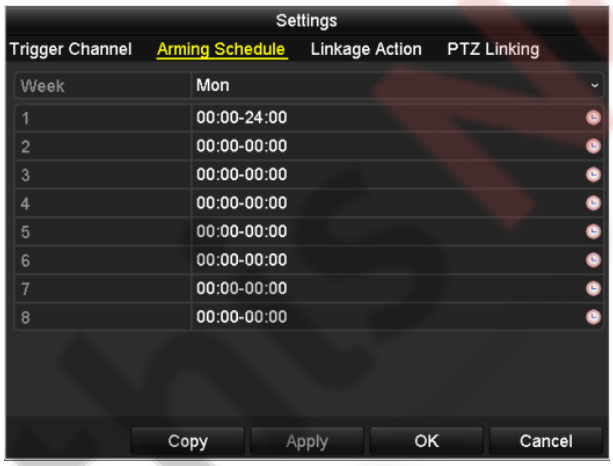


Figure 8-6 Set Arming Schedule of Alarm Input

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

NOTE

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.

Step 7 Select **Linkage Action** tab to set up alarm response actions of the alarm input (please refer to *Chapter 8.6 Setting Alarm Response Actions*).

Step 8 If necessary, select PTZ Linking tab and set PTZ linkage of the alarm input.

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

NOTE

Make sure the PTZ or speed dome connected supports PTZ linkage.

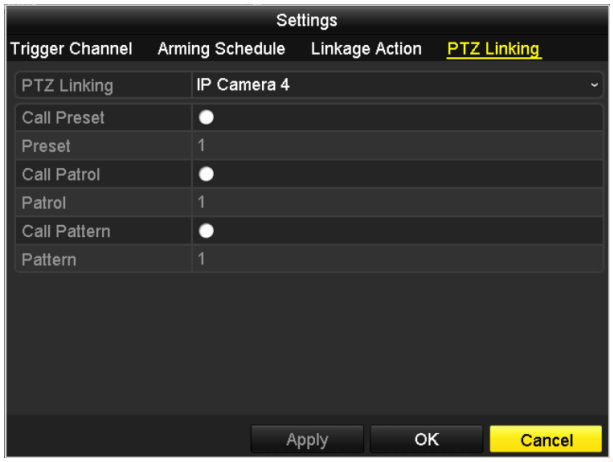


Figure 8-7 Set PTZ Linking of Alarm Input

Step 9 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.

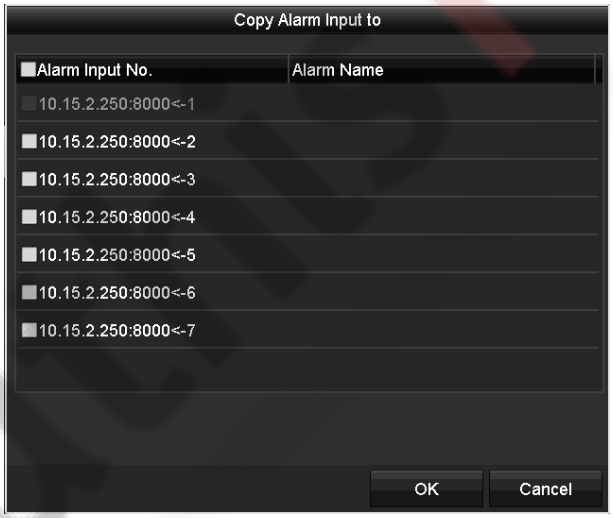


Figure 8-8 Copy Settings of Alarm Input

8.3 Detecting Video Loss Alarm

Purpose:

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

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

Menu > Camera > Video Loss

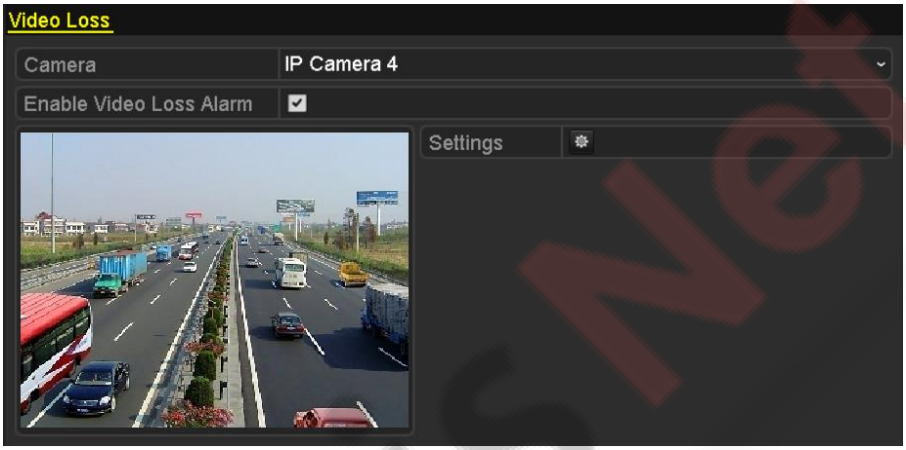


Figure 8-9 Video Loss Setup Interface

Step 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.

Step 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.

NOTE

Time periods shall not be repeated or overlapped.

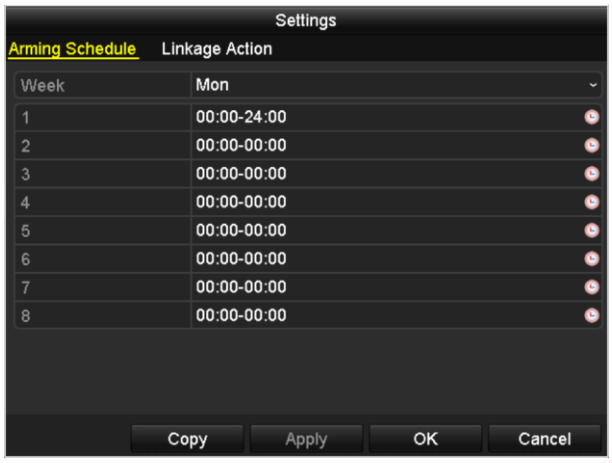


Figure 8-10 Set Arming Schedule of Video Loss

Step 4 Select **Linkage Action** tab to set up alarm response action of video loss (please refer to *Chapter 8.6 Setting Alarm Response Actions*).

Step 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).

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

Menu > Camera> Video Tampering

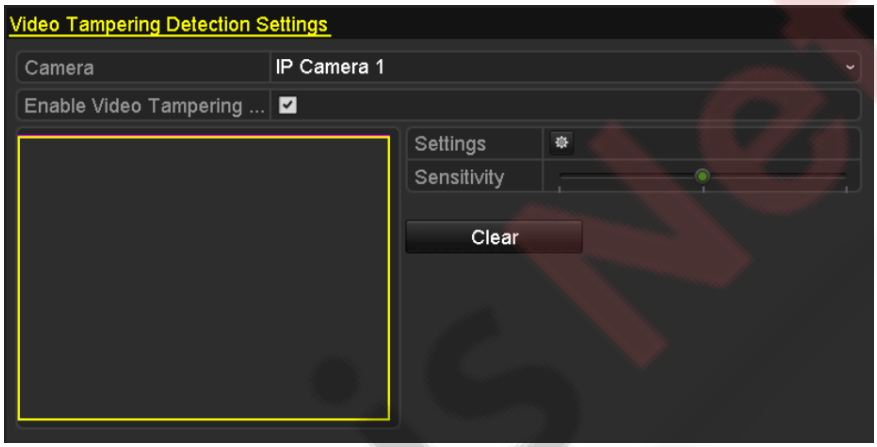


Figure 8-11 Video Tampering Setting Interface

Step 2 Set the video tampering handling action of the channel.

1) Check the checkbox of “Enable Video Tampering Detection”.
2) Drag the sensitivity bar to set a proper sensitivity level. Use the mouse to draw an area you want to detect video tampering.
3) Click button to set up handling action of video tampering.

Step 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.

NOTE

Time periods shall not be repeated or overlapped.

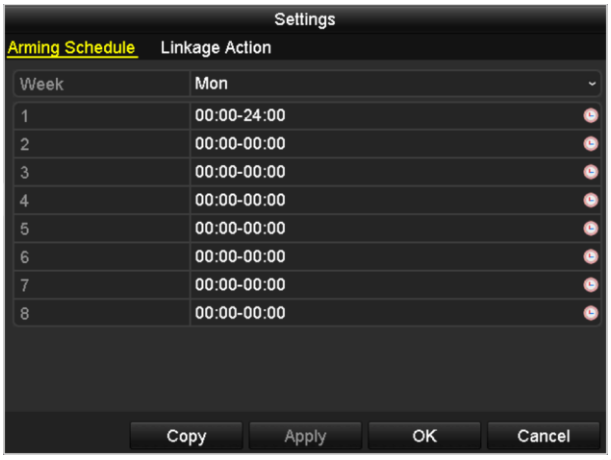


Figure 8-12 Set Arming Schedule of Video Tampering

Step 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*).

Step 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.

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.

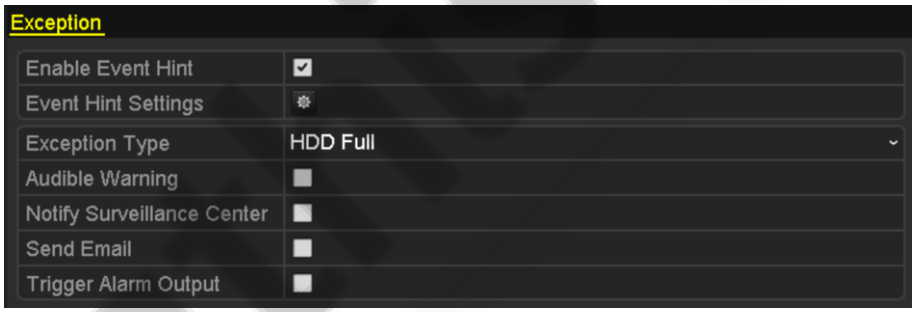


Figure 8-13 Exceptions Setup Interface

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, 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.

Step 1 Enter the Exception settings interface.

Menu > Configuration > Exceptions

Step 2 Check the checkbox of **Enable Event Hint**.

Figure 8-14 Event Hint Settings Interface

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

Figure 8-15 Event Hint Settings Interface

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

- Full Screen Monitoring

When an alarm is triggered, the local monitor (VGA or HDMI) 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.

NOTE

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

- Audible Warning

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

- Notify Surveillance Center

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

NOTE

The alarm signal will be transmitted automatically at detection mode when remote alarm host is configured. Please refer to *Chapter 11.3.5 Configuring More Settings* 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 11.3.7 Configuring Email* for details of Email configuration.

- Trigger Alarm Output

Trigger an alarm output when an alarm is triggered.

Step 1 Enter Alarm Output interface.

Menu > Configuration > Alarm > Alarm Output

Step 2 Select an alarm output and set alarm name and dwell time. Click **Schedule** button to set the arming schedule of alarm output.

NOTE

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

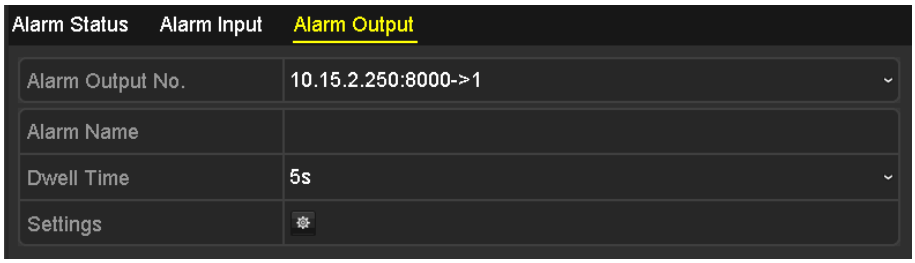


Figure 8-16 Alarm Output Setup Interface

Step 3 Set up arming schedule of the alarm output.

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

NOTE

Time periods shall not be repeated or overlapped.

Figure 8-17 Set Arming Schedule of Alarm Output

Step 4 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..

Step 5 You can also copy the above settings to another channel.

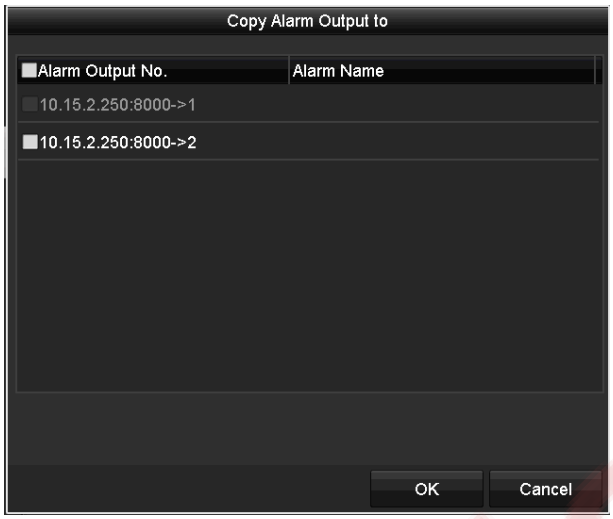


Figure 8-18 Copy Settings of Alarm Output

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.

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

Menu > Manual> Alarm

Step 2 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.

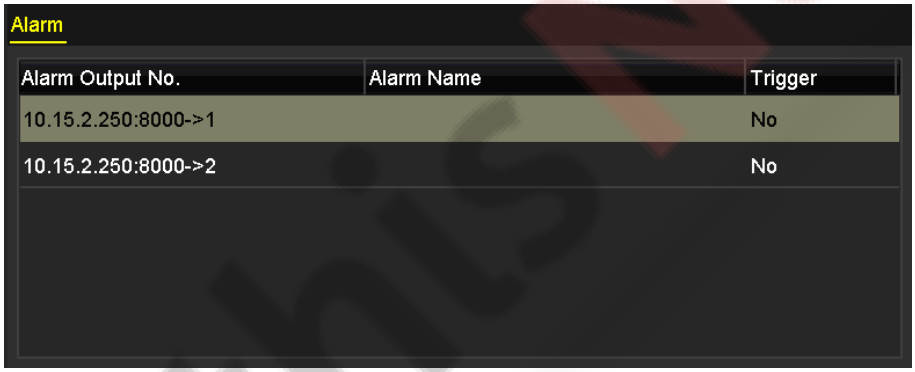


Figure 8-19 Clear or Trigger Alarm Output Manually

Chapter 9 VCA Alarm

The NVR supports the VCA detection alarm (face detection, vehicle detection, line crossing detection and intrusion detection, region entrance detection, region exiting detection, unattended baggage detection, object removal detection, audio loss exception detection, sudden change of sound intensity detection, and defocus detection) sent by IP camera. The VCA detection must be enabled and configured on the IP camera settings interface first.

NOTE

- All VCA detection must be supported by the connected IP camera.
- Please refer to the User Manual of Network Camera for the detailed instructions for the all VCA detection types.

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.

Step 1 Enter the VCA settings interface.

Menu > Camera > VCA

Step 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.

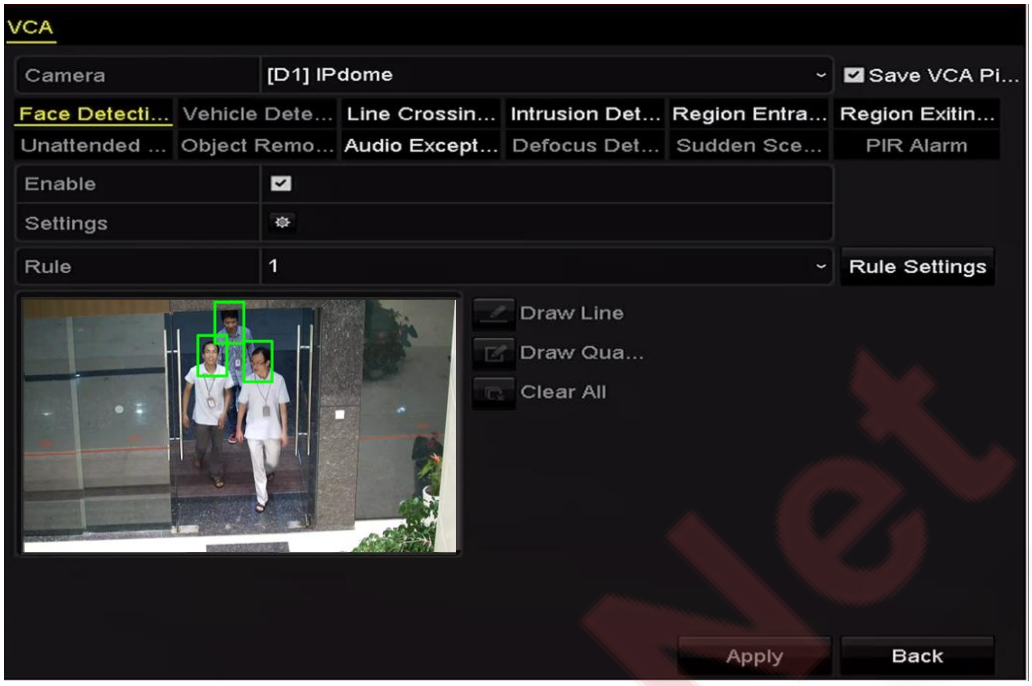


Figure 9-1 Face Detection

Step 3 Select the VCA detection type to **Face Detection**.

Step 4 Check the **Enable** checkbox to enable this function.

Step 5 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 step 3 to step 5 of *Chapter8.1 Setting Motion Detection Alarm* for detailed instructions.

Step 6 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

Step 7 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.

Step 1 Enter the VCA settings interface.

Menu> Camera> VCA

Step 2 Select the camera to configure the VCA.

Step 3 You can click the checkbox of **Save VCA Picture** to save the captured pictures of VCA detection.

Step 4 Select the VCA detection type to **Vehicle Detection**.

Step 5 Check the **Enable** checkbox to enable this function.

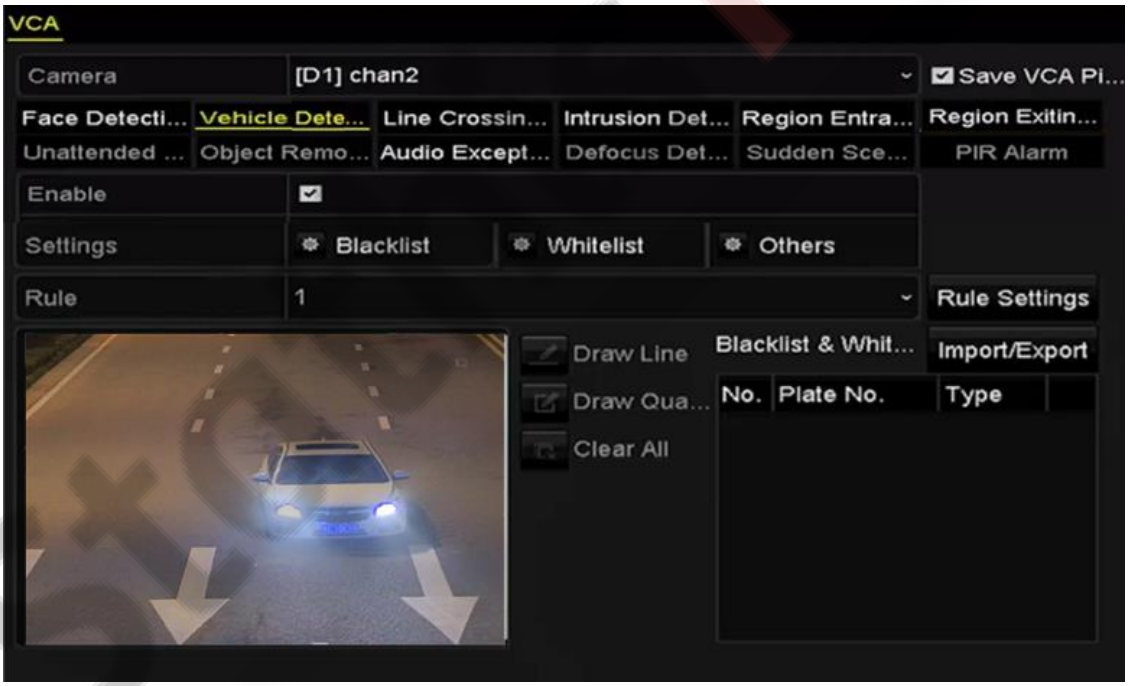


Figure 9-3 Set Vehicle Detection

Step 6 Click  to configure the trigger channel, arming schedule and linkage actions for the Blacklist, Whitelist and Others.

NOTE

Up to 2, 048 backlists or whitelists are supported for import and export.

Step 7 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.

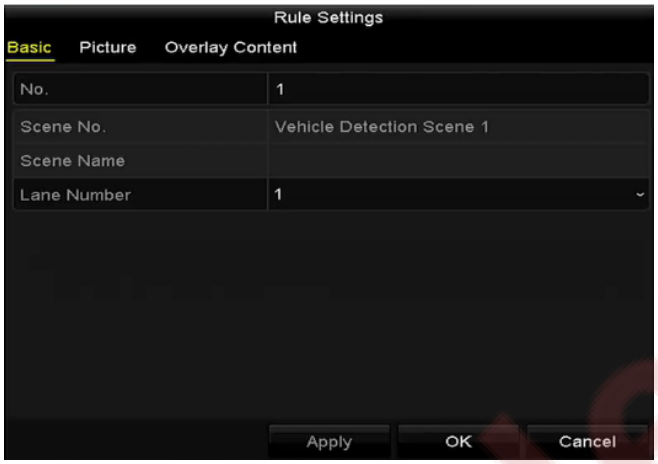


Figure 9-4 Rule Settings

Step 8 Click **Save** to save the settings.

NOTE

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.

Step 1 Enter the VCA settings interface.

Menu> Camera> VCA

Step 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.

Step 3 Select the VCA detection type to **Line Crossing Detection**.

Step 4 Check the **Enable** checkbox to enable this function.

Step 5 Click  to configure the trigger channel, arming schedule and linkage actions for the line crossing detection alarm.

Step 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

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

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

NOTE

Up to 4 rules can be configured.

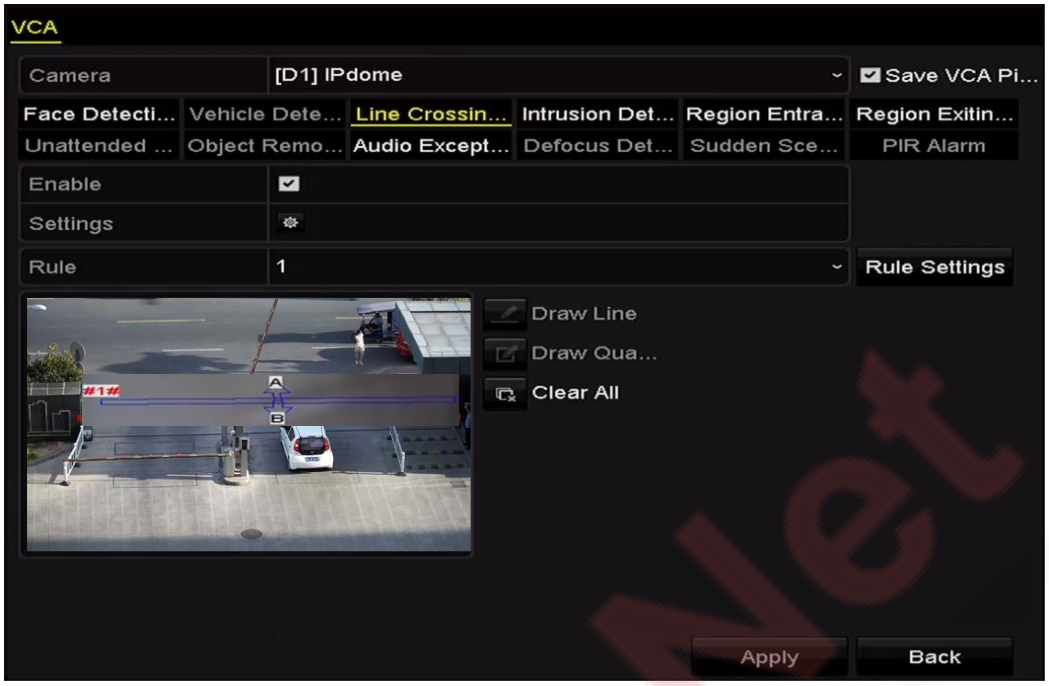


Figure 9-6 Draw Line for Line Crossing Detection

Step 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.

Step 1 Enter the VCA settings interface.

Menu> Camera> VCA

Step 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.

Step 3 Select the VCA detection type to **Intrusion Detection**.

Step 4 Check the **Enable** checkbox to enable this function.

Step 5 Click  to configure the trigger channel, arming schedule and linkage actions for the line crossing detection alarm.

Step 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.
3) **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.
4) **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

5) Click-**OK** to save the rule settings and back to the line crossing detection settings interface.

Step 7 Click  and draw a quadrilateral in the preview window by specifying four vertexes of the detection region, and right click to complete drawing. Only one region can be configured.

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

NOTE

Up to 4 rules can be configured.

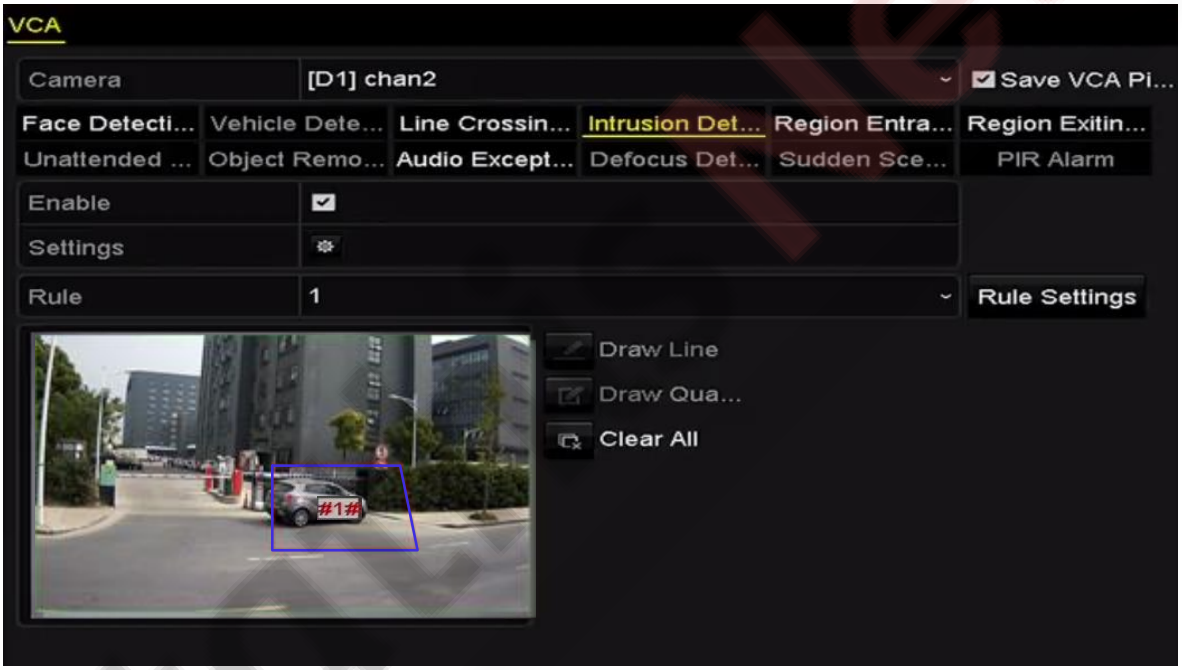


Figure 9-8 Draw Area for Intrusion Detection

Step 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.

Step 1 Enter the VCA settings interface.

Menu> Camera> VCA

Step 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.

Step 3 Select the VCA detection type to **Region Entrance Detection**.

Step 4 Check the **Enable** checkbox to enable this function.

Step 5 Click  to configure the trigger channel, arming schedule and linkage actions for the line crossing detection alarm.

Step 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.

Step 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.

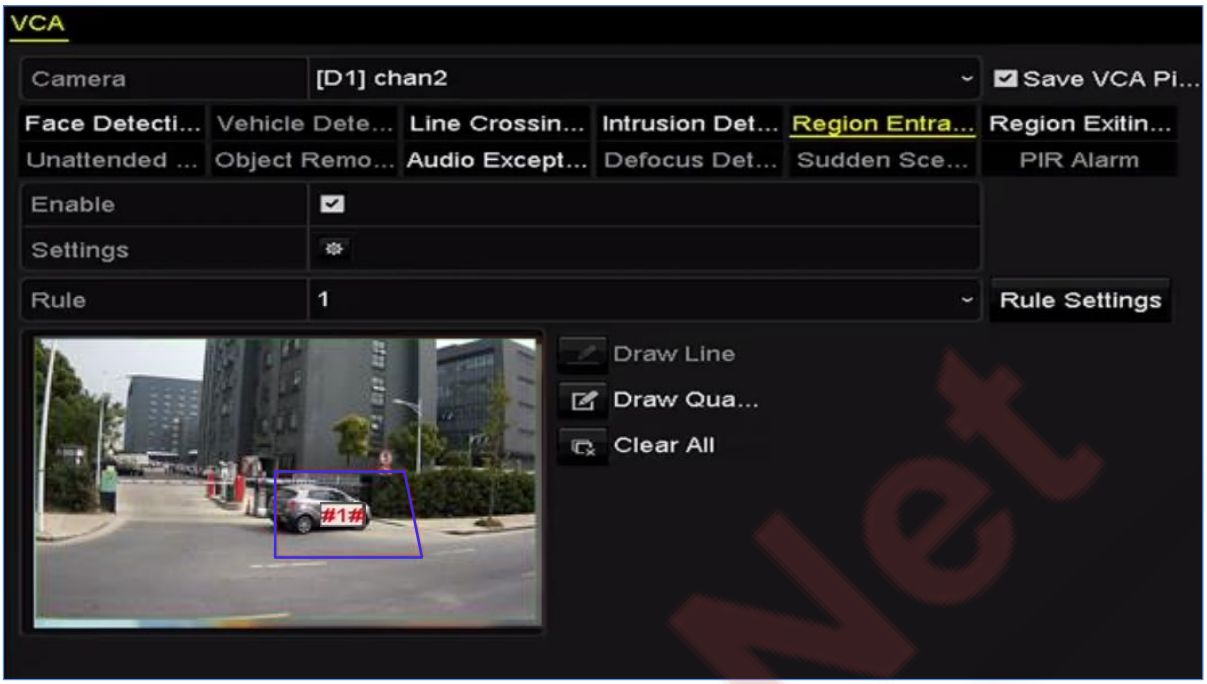


Figure 9-9 Set Region Entrance Detection

NOTE

Up to 4 rules can be configured.

Step 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.

NOTE

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

9.7 Unattended Baggage Detection

Purpose:

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

NOTE

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

9.8 Object Removal Detection

Purpose:

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

NOTE

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

9.9 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.

Step 1 Enter the VCA settings interface.

Menu> Camera> VCA

Step 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.

Step 3 Select the VCA detection type to **Audio Exception Detection**.

Step 4 Click  to configure the trigger channel, arming schedule and linkage action for the face detection alarm.

Step 5 Click the **Rule Settings** button to set the audio exception rules.

Figure 9-10 Set Audio Exception Detection Rules

1) Check the checkbox of **Audio Input Exception** to enable the audio loss detection function.
2) Check the checkbox of **Sudden Increase of Sound Intensity Detection** to detect the sound steep rise in the surveillance scene. You can set the detection sensitivity and threshold for sound steep rise.

   Sensitivity: Range [1-100], the smaller the value is, the more severe the change should be to trigger the detection.

   Sound Intensity Threshold: Range [1-100], it can filter the sound in the environment, the louder the environment sound, the higher the value should be. You can adjust it according to the real environment.
3) Check the checkbox of **Sudden Decrease of Sound Intensity Detection** to detect the sound steep drop in the surveillance scene. You can set the detection sensitivity[1-100] for sound steep drop.

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

9.10 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.

NOTE

- 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.

9.11 Defocus Detection

Purpose:

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

NOTE

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

9.12 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.

Step 1 Enter the VCA settings interface.

Menu> Camera> VCA

Step 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.

Step 3 Select the VCA detection type to **PIR Alarm**.

Step 4 Click  to configure the trigger channel, arming schedule and linkage action for the PIR alarm.

Step 5 Click the **Rule Settings** button to set the rules. Please refer to the *Chapter 9.1 Face Detection* for instructions.

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

Chapter 10 VCA Search

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

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 *Chapter 9.1 Face Detection* for configuring the face detection.

Step 1 Enter the **Face Search** interface.

Menu >VCA Search > Face Search

Step 2 Select the camera (s) for the face search.

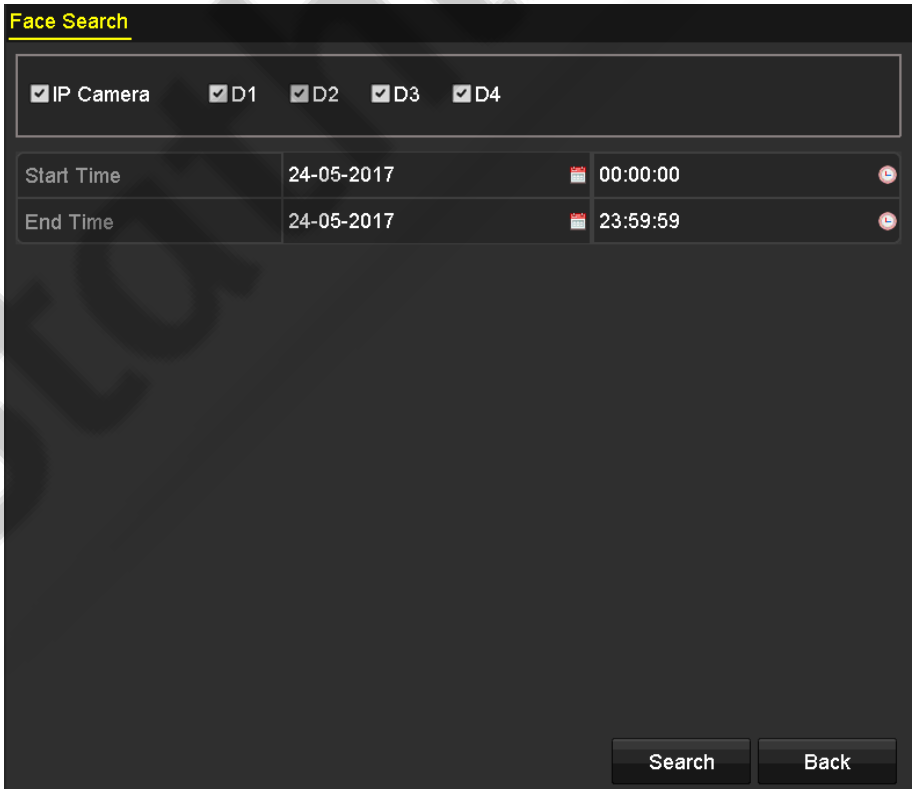


Figure 10-1 Face Search

Step 3 Specify the start time and end time for search the captured face pictures or video files.

Step 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

Step 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.

Step 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.

Step 1 Enter the **Behavior Search** interface.

Menu > VCA Search > Behavior Search

Step 2 Select the camera(s) for the behavior search.

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

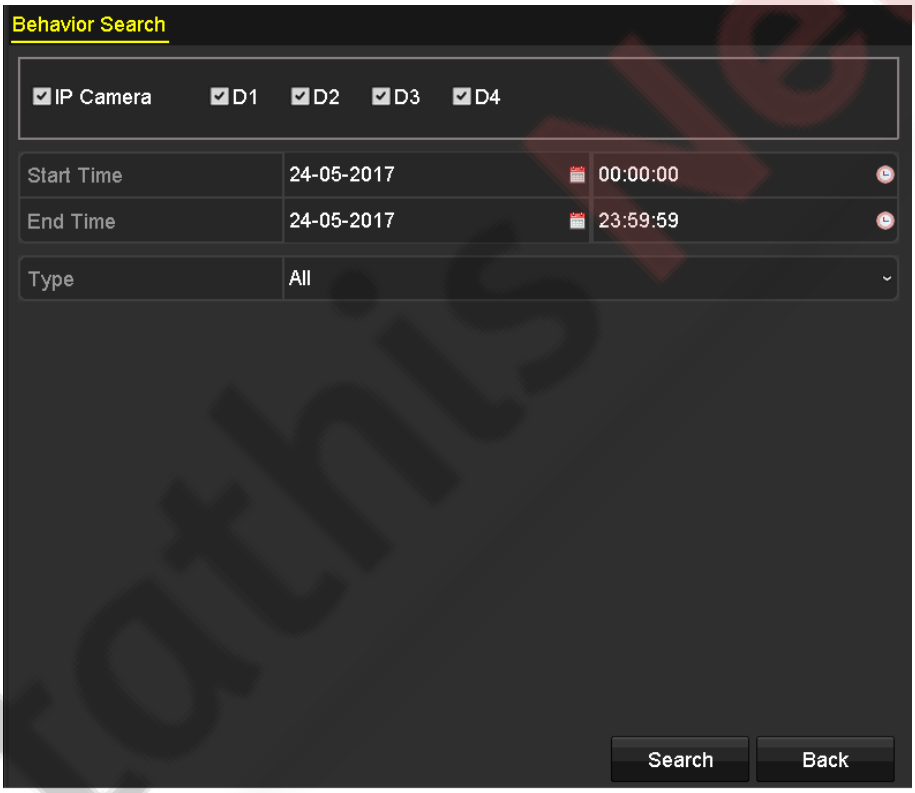


Figure 10-4 Behavior Search Interface

Step 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.

Step 5 Click **Search** to start searching. The search results of pictures are displayed in list or in chart.

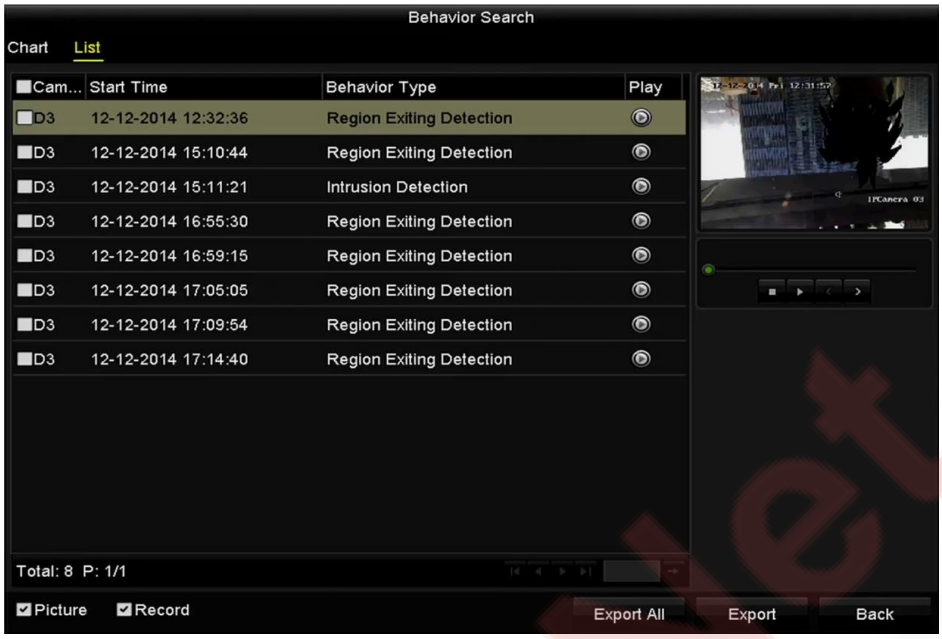


Figure 10-5 Behavior Search Results

Step 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.

Step 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.

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

Menu > VCA Search > Plate Search

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

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

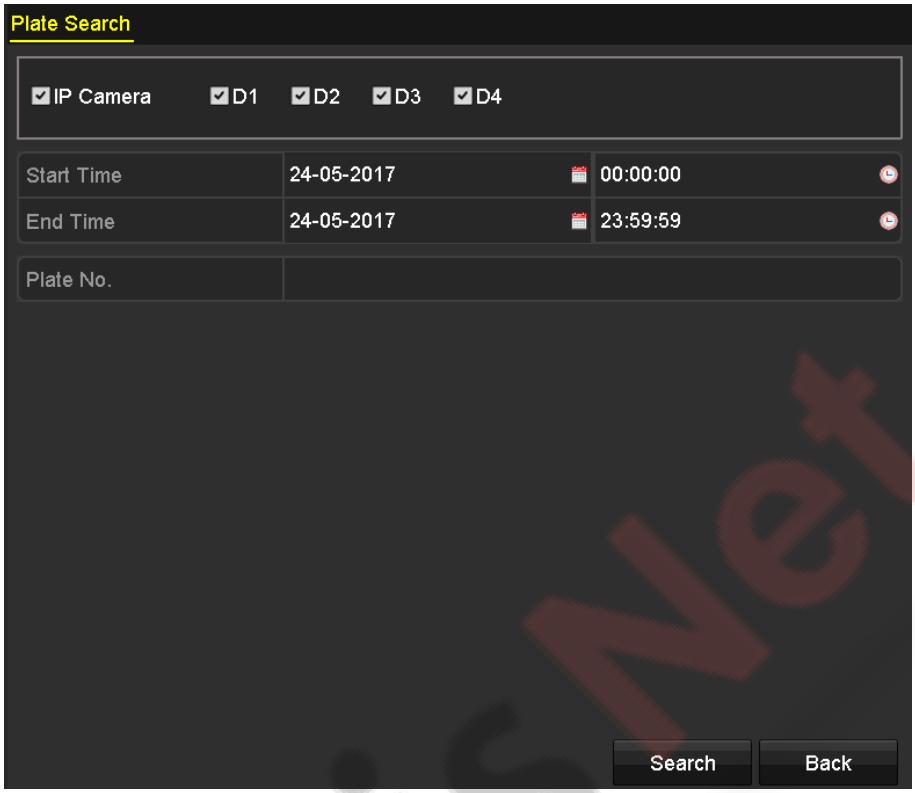


Figure 10-6 Plate Search

Step 4 Select the country from the drop-down list for searching the location of the vehicle plate.

Step 5 Input the plate No. in the field for search.

Step 6 Click **Search** to start searching. The search results of detected vehicle plate pictures are displayed in list or in chart.

NOTE

Please refer to the Step 7 to Step 8 of *Chapter 10.1 Face Search* for the operation of the search results.

10.4 People Counting

Purpose:

The 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.

Step 1 Enter the Counting interface.

Menu > VCA Search > Counting

Step 2 Select the camera for the people counting.

Step 3 Select the report type to Daily Report, Weekly Report, Monthly Report or Annual Report.

Step 4 Set the statistics time.

Step 5 Click the **Counting** button to start people counting statistics.

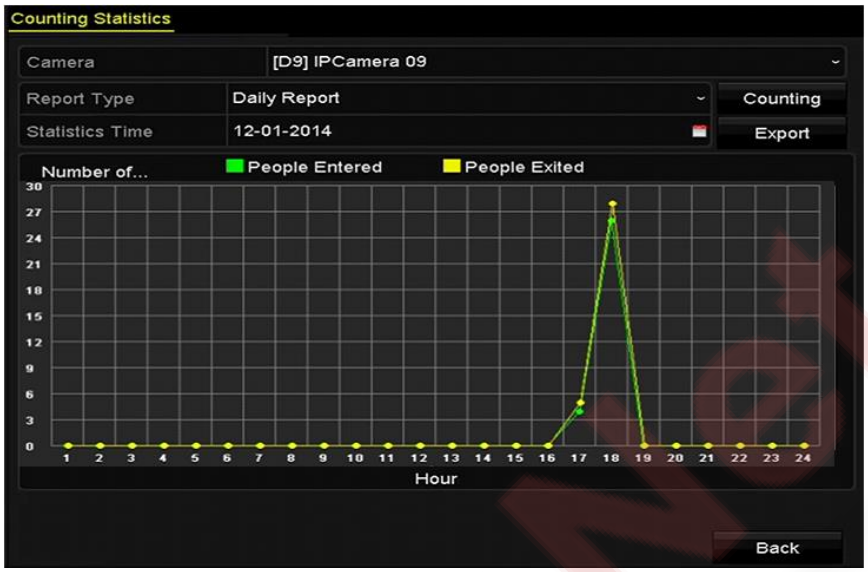


Figure 10-7 People Counting Interface

Step 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.

NOTE

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

Step 1 Enter the **Heat Map** interface.

Menu > VCA Search > Heat Map

Step 2 Select the camera for the heat map processing.

Step 3 Select the report type to Daily Report, Weekly Report, Monthly Report or Annual Report.

Step 4 Set the statistics time.

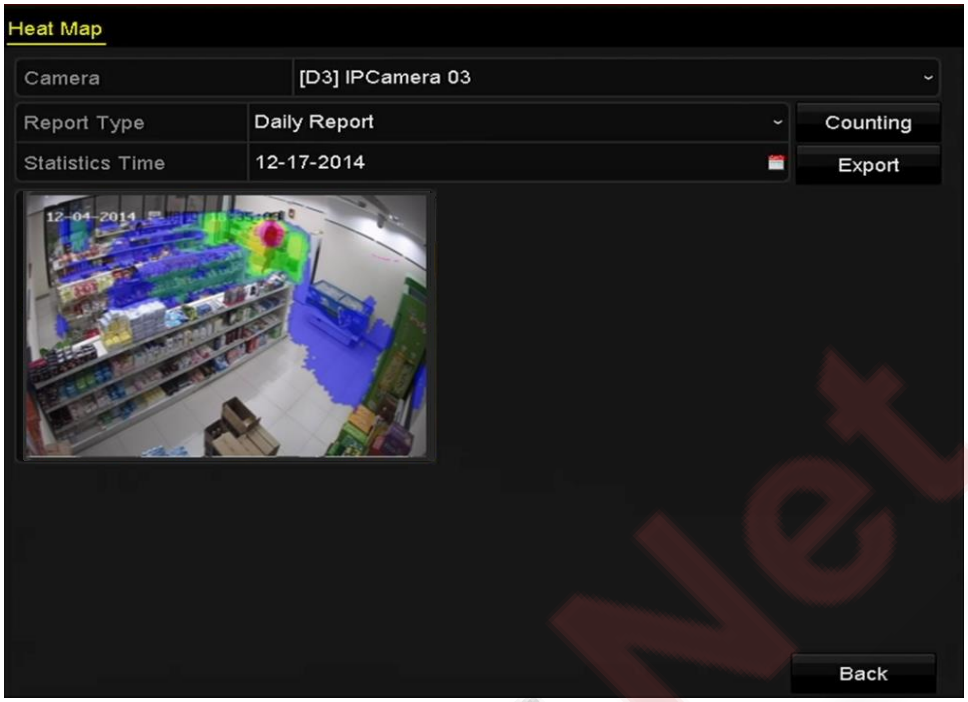


Figure 10-8 Heat Map Interface

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

NOTE

As shown in 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.

Step 6 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.

Step 1 Enter the Network Settings interface.

Menu > Configuration > Network

Step 2 Select the **General** tab.

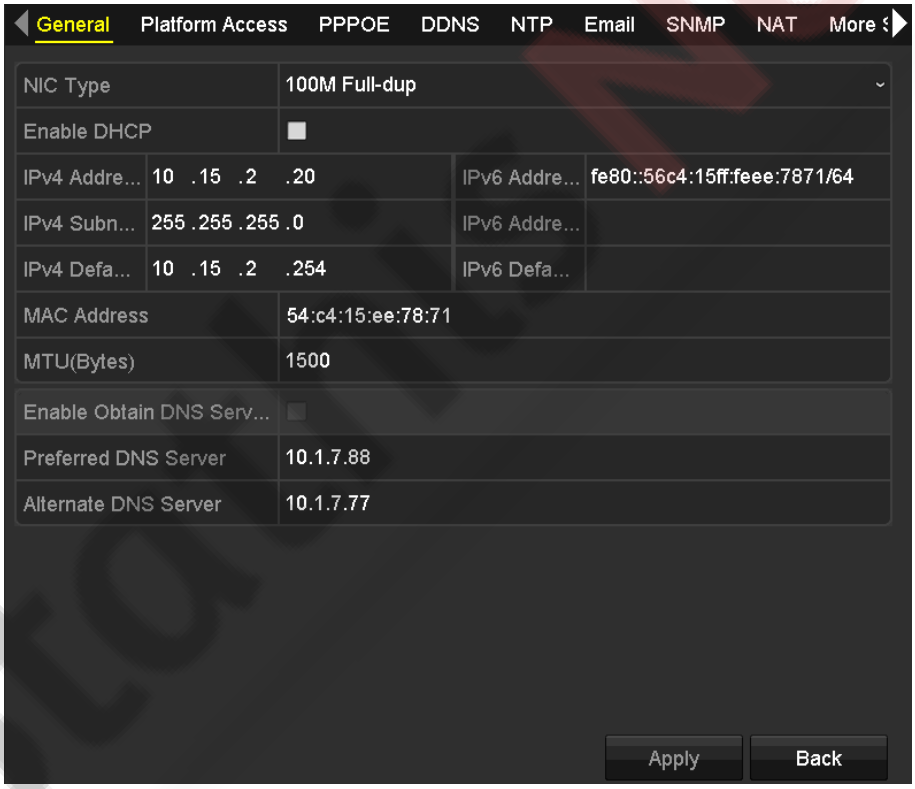


Figure 11-1 Network Settings Interface

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

NOTE

The valid value range of MTU is 500 to 9676.

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.

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

11.2 Configuring Wi-Fi Settings

Purpose:

The device can work as a wireless network router. Follow the steps to setup a network router.

Step 1 Enter WiFi interface

Menu > Configuration > WiFi

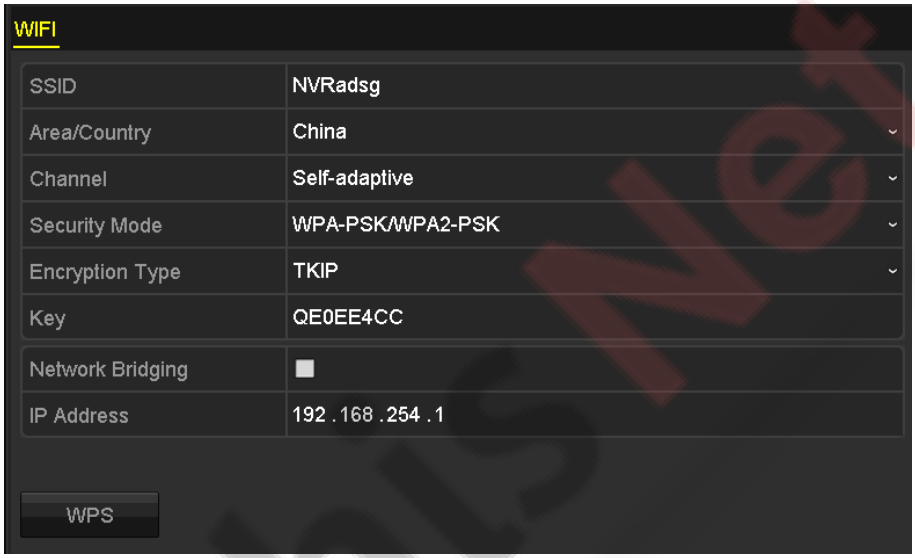


Figure 11-2 Wi-Fi Settings

Step 2 Configure wireless network parameters, including **Network Bridging, SSID, Security Mode,** and **Key**.

- **Network Bridging**: Enable device to create a single aggregate network from multiple communication networks or network segments
- **SSID**: It is the short for Service Set Identifier. SSID is the WiFi name that the device provides.
- **Area/Country:** Select where the router is used.
- **Channel**: Select the best channel according to your situation.
- **Security Mode**: Select the security protocol for the wireless network.
- **Encryption Type**: It is used to protect information. **TKIP** and **AES** are selectable.
- **Key**: Enter the encryption key.
- **WPS:** It is the short of Wi-Fi Protected Setup. Click the button and then you can connect the wireless network without password for once.

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

11.3 Configuring Advanced Settings

11.3.1 Configuring Hik-Connect

Purpose

Hik-Connect enables the mobile phone application and the service platform page (www.hik-connect.com) to access and manage your connected NVR, providing a convenient remote access to the surveillance system.

NOTE

The Hik-Connect can be enabled via operation on SADP software, GUI and Web browser. We introduce the operation steps on GUI in this section.

Step 1 Enter the **Network Settings** interface.

Menu > Configuration > Network

Step 2 Select the **Platform Access** tab to enter the Hik-Connect Settings interface.

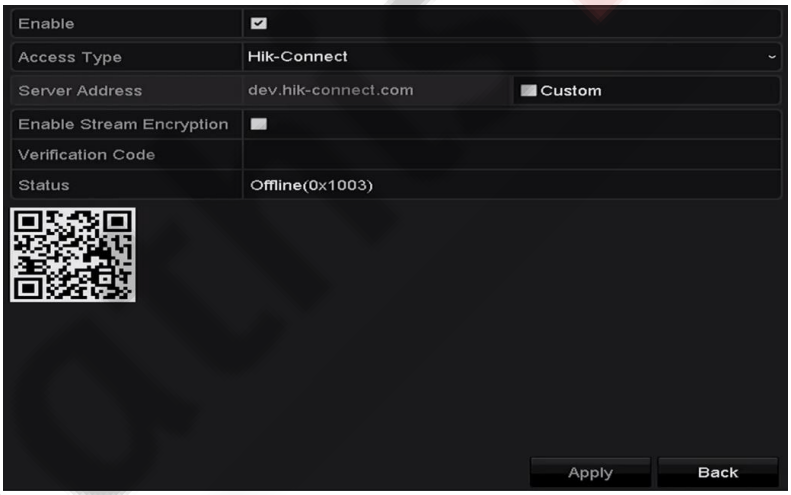


Figure 11-3 Hik-Connect Settings

Step 3 Check the **Enable** checkbox to activate the function. The **Service Terms** interface pops up as below.

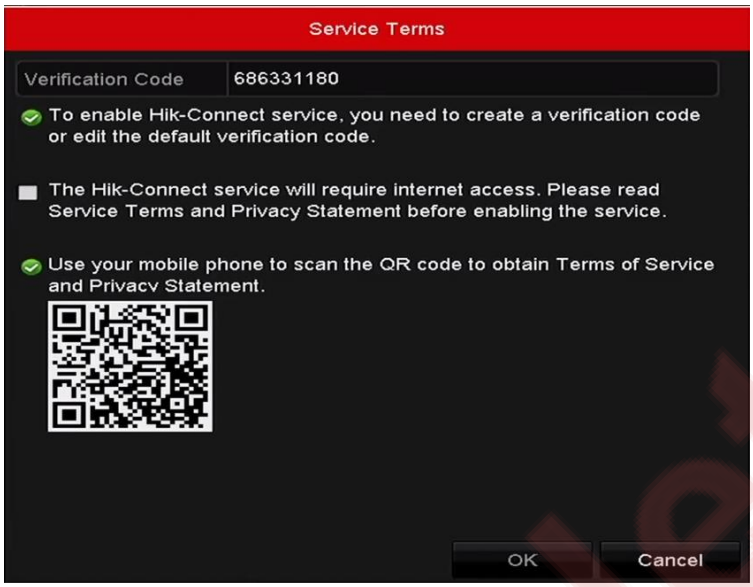


Figure 11-4 Service Terms

1) Create the verification code and enter the code in the **Verification Code** text field.
2) Check the checkbox of **The Hik-Connect service will require internet access. Please read Service Terms and Privacy Statement before enabling the service.**
3) Scan the QR code on the interface to read the Service Terms and the Privacy Statement.
4) Click **OK** to save the settings and return to the Hik-Connect interface.

NOTE

- Hik-Connect is disabled by default.
- The verification code is empty when the device leaves factory.
- The verification code must contain 6 to 12 letters or numbers and is case sensitive.
- Every time you enable Hik-Connect, the Service Terms interface pops up and you should check the checkbox before enabling it.

Step 4 (Optional) Check the checkbox of **Custom** and input the **Server Address**.

Step 5 (Optional) Check the checkbox of **Enable Stream Encryption**. After this feature is enabled, the verification code is required for remote access and live view.

NOTE

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

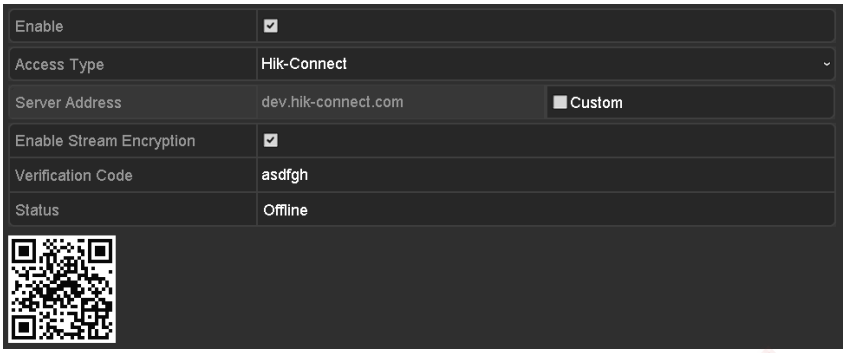


Figure 11-5 Hik-Connect Settings Interface

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

After configuration, you can access and manage the NVR by your mobile phone on which the Hik-Connect application is installed or by the website (www.hik-connect.com).

NOTE

Please refer to the help file on the official website (www.hik-connect.com) and the *Hik-Connect Mobile Client User Manual* for adding the device to Hik-Connect and more operation instructions.

11.3.2 Configuring DDNS

Purpose:

You can set the Dynamic DNS (DDNS) for network access.

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

Step 1 Enter the Network Settings interface.

Menu > Configuration > Network

Step 2 Select the **DDNS** tab to enter the DDNS Settings interface.

Step 3 Check the **DDNS** checkbox to enable this feature.

Step 4 Select **DDNS Type**. Three DDNS types are selectable: DynDNS, PeanutHull, and NO-IP.

- **DynDNS:**

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

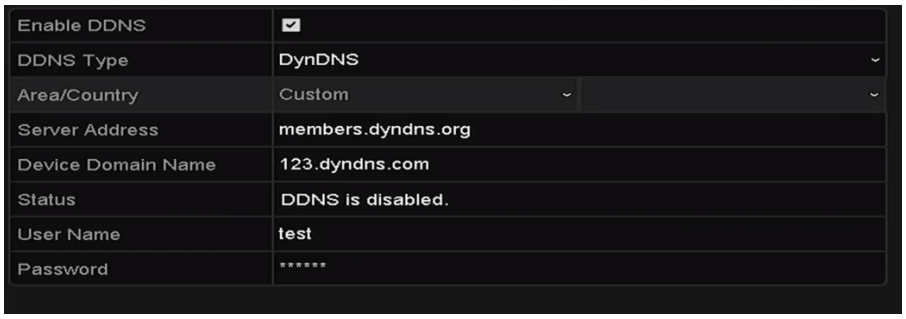


Figure 11-6 DynDNS Settings Interface

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

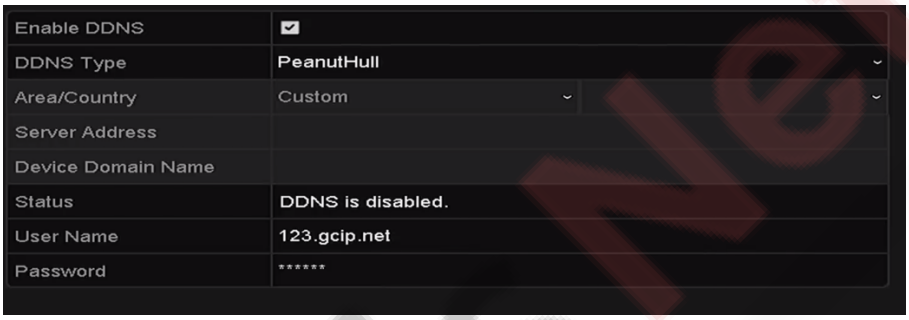


Figure 11-7 PeanutHull Settings Interface

•**NO-IP:**

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

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

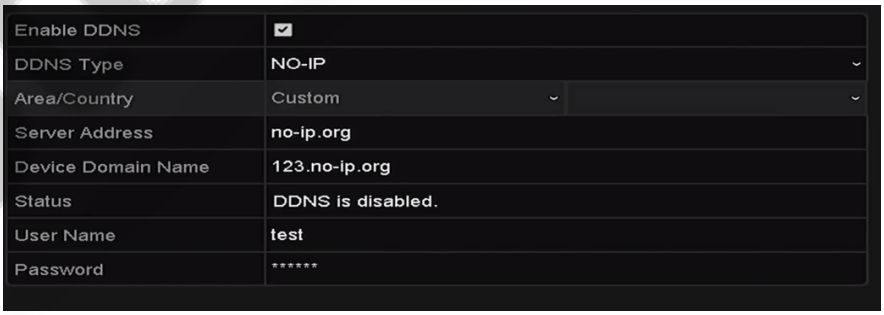


Figure 11-8 NO-IP Settings Interface

Step 5 Click the **Apply** button to save and exit the interface.

11.3.3 Configuring NTP Server

Purpose:

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

Step 1 Enter the Network Settings interface.

Menu >Configuration> Network

Step 2 Select the **NTP** tab to enter the NTP Settings interface, as shown in Figure 11-9.

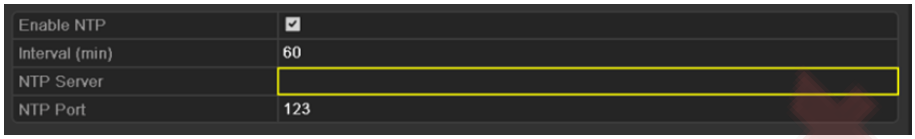


Figure 11-9 NTP Settings Interface

Step 3 Check the **Enable NTP** checkbox to enable this feature.

Step 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.

Step 5 Click the **Apply** button to save and exit the interface.

NOTE

The time synchronization interval can be set from1 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.

11.3.4 Configuring SNMP

Purpose:

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

Step 1 Enter the Network Settings interface.

Menu >Configuration> Network

Step 2 Select the **SNMP** tab to enter the SNMP Settings interface, as shown in Figure 11-10.

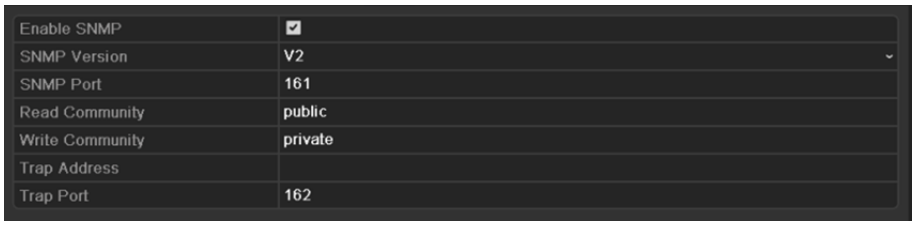


Figure 11-10 SNMP Settings Interface

Step 3 Check the **SNMP** checkbox to enable this feature.

Step 4 The enabling of SNMP may cause security problems. Click **Yes** to continue or **No** to cancel the operation.

Figure 11-11 SNMP Settings Interface

Step 5 When you choose the Yes option in step4, configure the following SNMP settings:

Trap Address: IP Address of SNMP host.

Trap Port: Port of SNMP host.

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

NOTE

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

11.3.5 Configuring More Settings

Step 1 Enter the Network Settings interface.

Menu > Configuration > Network

Step 2 Select the **More Settings** tab to enter the More Settings interface.

Figure 11-12 More Settings Interface

Step 3 Configure the remote alarm host, server port, HTTP port, multicast, RTSP port.

- **Alarm Host IP/Port**: With a remote alarm host configured, the device will send the alarm event or exception message to the host when an alarm is triggered. The remote alarm host must have the CMS (Client Management System) software installed.

  The **Alarm Host IP** refers to the IP address of the remote PC on which the CMS (Client Management System) software (e.g., iVMS-4200) is installed, and the **Alarm Host Port** must be the same as the alarm monitoring port configured in the software (default port is 7200).

- **Multicast IP**: The multicast can be configured to realize live view for more than the maximum number of cameras through network. A multicast address spans the Class-D IP range of 224.0.0.0 to 239.255.255.255. It is recommended to use the IP address ranging from 239.252.0.0 to 239.255.255.255.

  When adding a device to the CMS (Client Management System) software, the multicast address must be the same as the device's multicast IP.

- **RTSP Port**: The RTSP (Real Time Streaming Protocol) is a network control protocol designed for use in entertainment and communications systems to control streaming media servers.

  Enter the RTSP port in the text field of **RTSP Port**. The default RTSP port is 554, and you can change it according to different requirements.

- **Server Port** and **HTTP Port**: Enter the **Server Port** and **HTTP Port** in the text fields. The default Server Port is 8000 and the HTTP Port is 80, and you can change them according to different requirements.

NOTE

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

Figure 11-13 Configure More Settings

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

11.3.6 Configuring HTTPS Port

Purpose:

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

Example:

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

NOTE

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

Step 1 Open web browser, input the IP address of device, and the web server will select the language automatically according to the system language and maximize the web browser.

Step 2 Input the correct user name and password, and click **Login** button to log in the device.

Step 3 Enter the HTTPS settings interface.

Step 4 Configuration > Remote Configuration > Network Settings > HTTPS

Step 5 Create the self-signed certificate or authorized certificate.

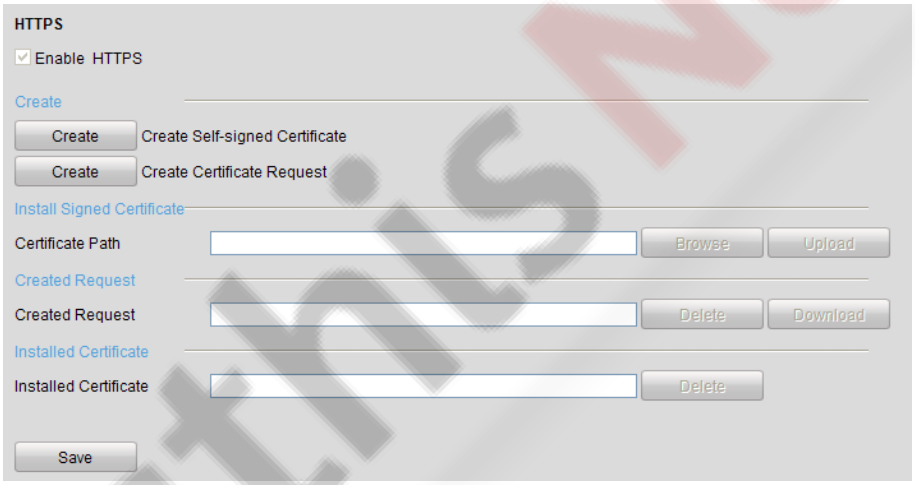


Figure 11-14 HTTPS Settings

OPTION 1: Create the self-signed certificate

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

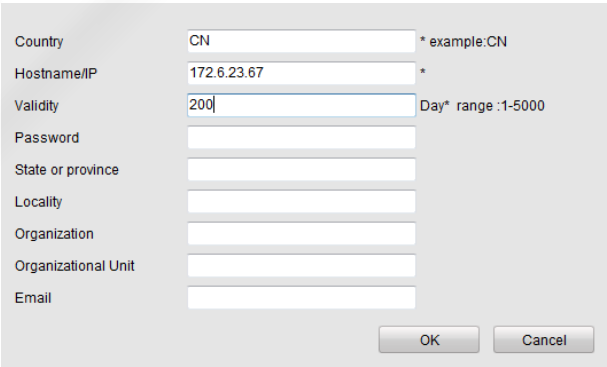


Figure 11-15 Create Self-signed Certificate

2) Enter the country, host name/IP, validity and other information.

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

OPTION 2: Create the authorized certificate

1) Click the **Create** button to create the certificate request.

2) Download the certificate request and submit it to the trusted certificate authority for signature.

3) After receiving the signed valid certificate, import the certificate to the device.

Step 6 There will be the certificate information after you successfully create and install the certificate.

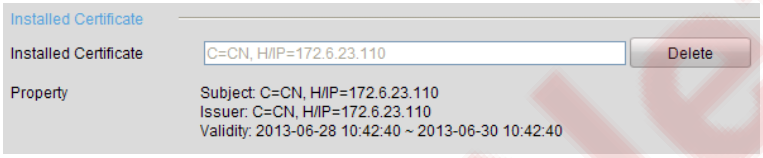


Figure 11-16 Installed Certificate Property

Step 7 Check the checkbox to enable the HTTPS function.

Step 8 Click the **Save** button to save the settings.

11.3.7 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.

Step 1 Enter the Network Settings interface.

Menu >Configuration> Network

Step 2 Set the IPv4 Address, IPv4 Subnet Mask, IPv4 Gateway and the Preferred DNS Server in the Network Settings menu, as shown in Figure 11-17.

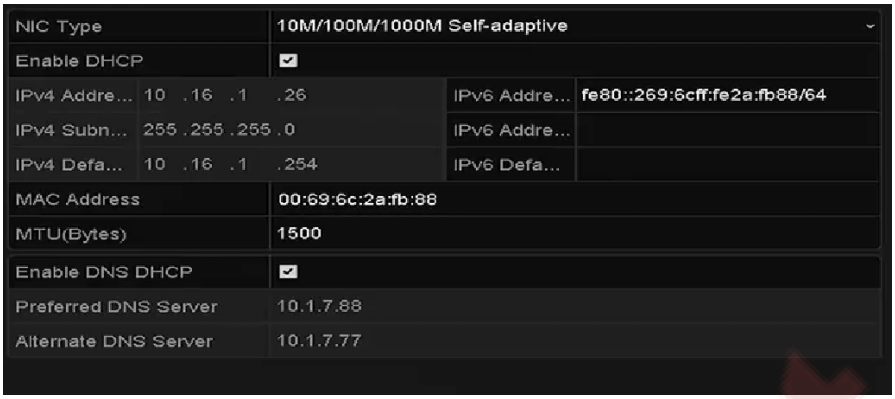


Figure 11-17 Network Settings Interface

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

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

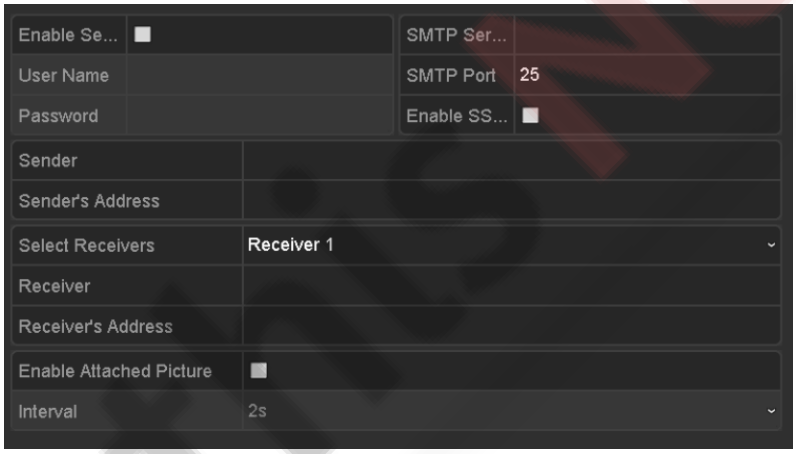


Figure 11-18 Email Settings Interface

Step 5 Configure the following Email settings:

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

User Name: The user name of sender's account registered on the SMTP server.

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

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

SMTP Port: The SMTP port. The default TCP/IP port used for SMTP is 25.

Enable SSL/TLS (optional)**:** Click the checkbox to enable SSL/TLS 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 Picture: 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.

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

Step 7 You can click **Test** button to test whether your Email settings work.

11.3.8 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.

Step 1 Enter the Network Settings interface.

Menu > Configuration > Network

Step 2 Select the **NAT** tab to enter the port mapping interface.

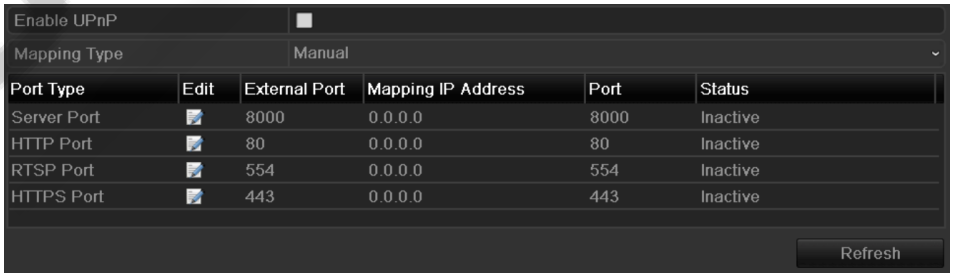


Figure 11-19 UPnP™ Settings Interface

Step 3 Check ☑ checkbox to enable UPnP™.

Step 4 Select the Mapping Type as Manual or Auto in the drop-down list.

OPTION 1: Auto

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

1) 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.

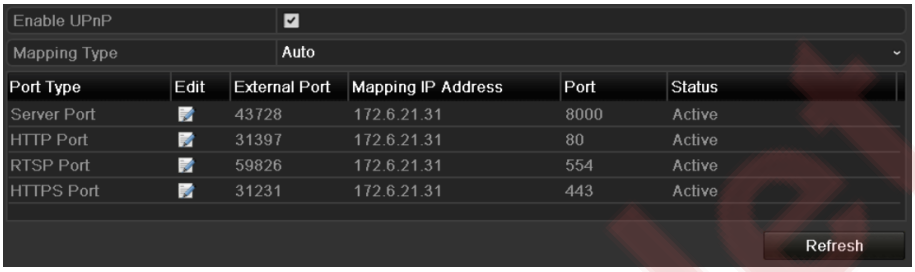


Figure 11-20 UPnP™ Settings Finished-Auto

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.

NOTE

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

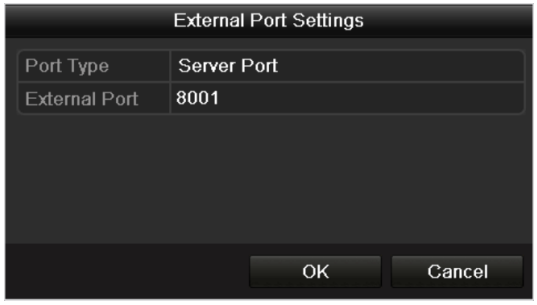


Figure 11-21 External Port Settings Dialog Box

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

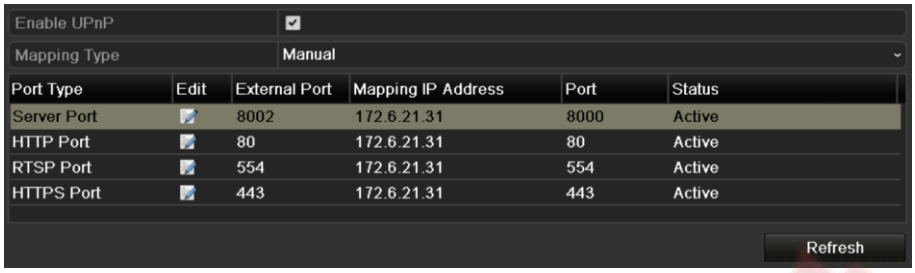


Figure 11-22 UPnP™ Settings Finished-Manual

Step 5 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.

NOTE

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

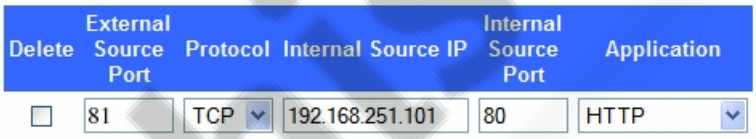


Figure 11-23 Setting Virtual Server Item

NOTE

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.

11.3.9 Configuring Virtual Host

Purpose:

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

NOTE

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

Step 1 Enter the Advanced settings interface, as shown in the Figure 11-24.

Configuration > Network > Advanced Settings > Other

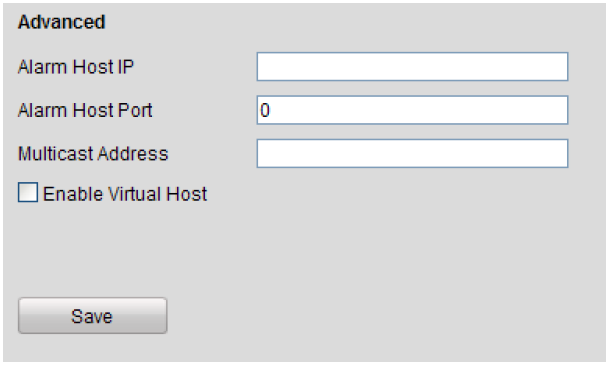


Figure 11-24 Advanced Settings Interface

Step 2 Check the checkbox of the **Enable Virtual Host**.

Step 3 Click the **Save** button to save the setting.

Step 4 Enter the IP camera management interface of NVR. The Connect column appears on the right-most side of the camera list, as shown in the Figure 11-25.

Configuration > Remote Configuration > Camera Management > IP Camera

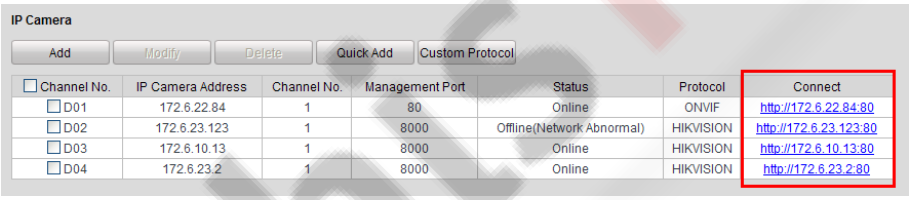


Figure 11-25 Connect to IP Camera

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

11.4 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.

Step 1 Enter the Network Traffic interface.

Menu > Maintenance > Net Detect

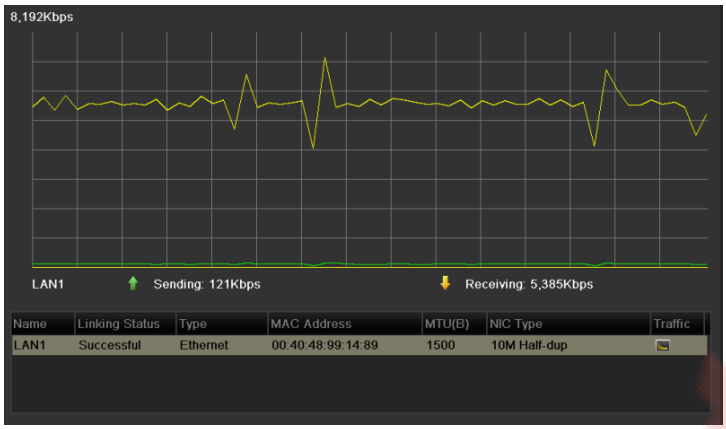


Figure 11-26 Network Traffic Interface

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

11.5 Configuring Network Detection

Purpose:

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

11.5.1 Testing Network Delay and Packet Loss

Step 1 Enter the Network Traffic interface.

Menu > Maintenance > Net Detect

Step 2 Click the **Network Detection** tab to enter the Network Detection menu, as shown in Figure 11-27.

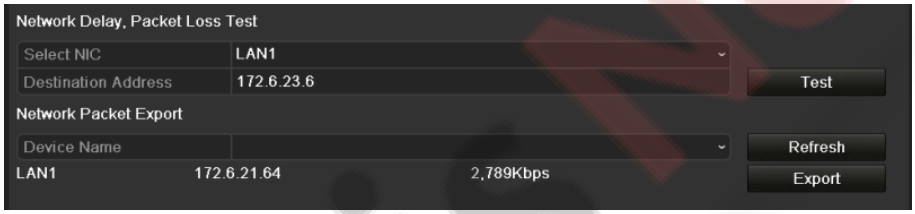


Figure 11-27 Network Detection Interface

Step 3 Enter the destination address in the text field of **Destination Address**.

Step 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 11-28.

Figure 11-28 Testing Result of Network Delay and Packet Loss

11.5.2 Exporting Network Packet

Purpose:

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

Step 1 Enter the Network Traffic interface.

Menu > Maintenance > Net Detect

Step 2 Click the **Network Detection** tab to enter the Network Detection interface.

Step 3 Select the backup device from the dropdown list of Device Name, as shown in Figure 11-29.

NOTE

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.

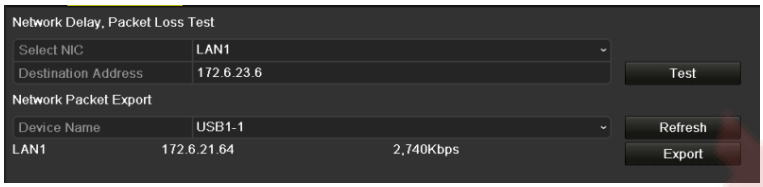


Figure 11-29 Export Network Packet

Step 4 Click **Export** button to start exporting.

Step 5 After the exporting is complete, click **OK** to finish the packet export, as shown in Figure 11-30.

Figure 11-30 Packet Export Attention

NOTE

Up to 1M data can be exported each time.

11.5.3 Checking the Network Status

Purpose:

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

Steps:

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

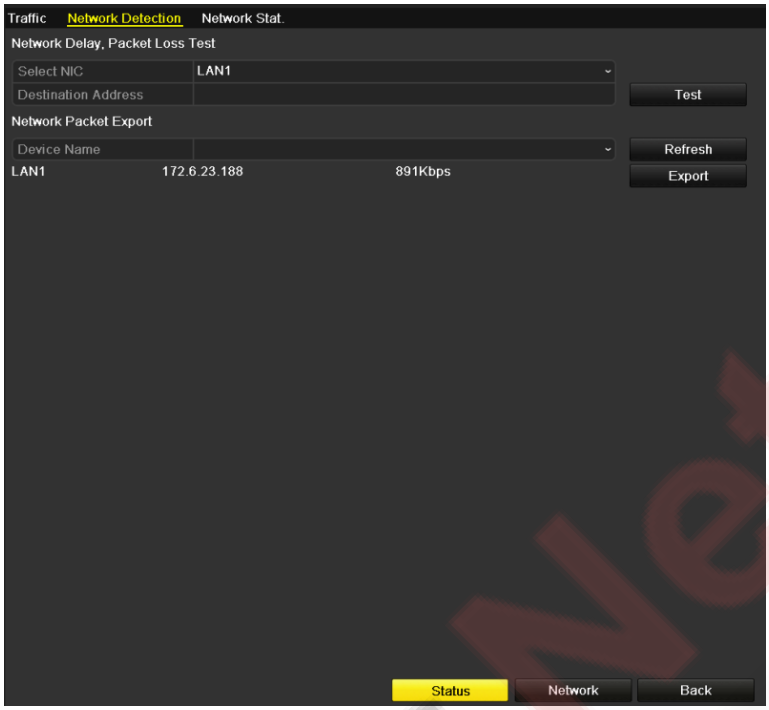


Figure 11-31 Network Status Checking

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

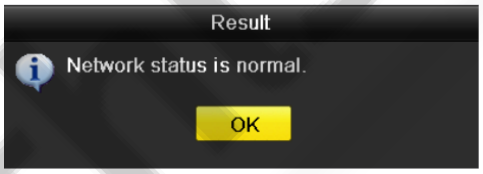


Figure 11-32 Network Status Checking Result

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.

11.5.4 Checking Network Statistics

Purpose:

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

Step 1 Enter the Network Detection interface.

Menu>Maintenance>Net Detect

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

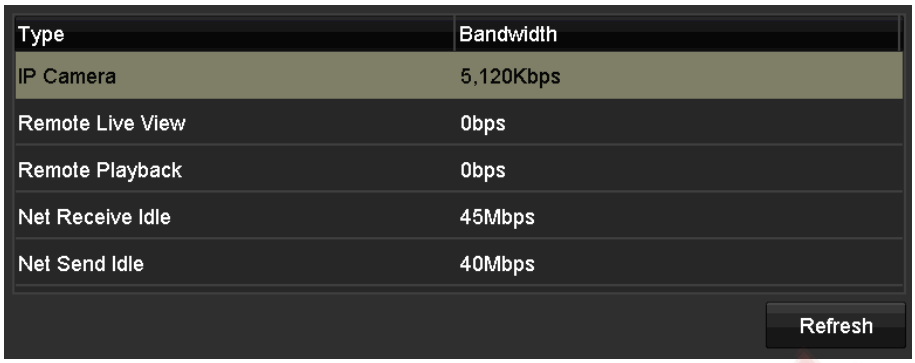


Figure 11-33 Network Stat. Interface

Step 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.

Step 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.

NOTE

A message box pops up when the NVR starts up if there exits 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.

Step 2 Enter the HDD Information interface.

Menu > HDD > General

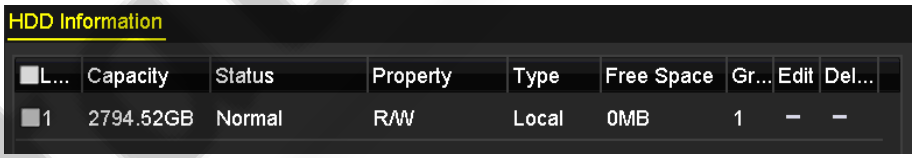


Figure 12-2 HDD Information Interface

Step 3 Select HDD to be initialized.

Step 4 Click the **Init** button.

Figure 12-3 Confirm Initialization

Step 5 Select the **OK** button to start initialization.

Step 6 After the HDD has been initialized, the status of the HDD will change from *Uninitialized* to *Normal*.

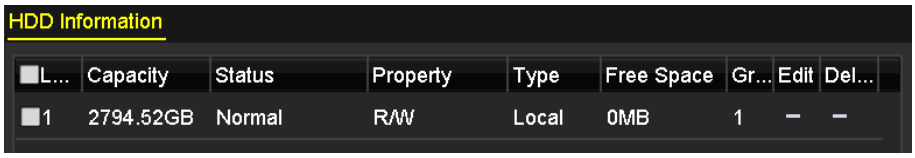


Figure 12-4 HDD Status Changes to Normal

NOTE

Initializing the HDD will erase all data on it.

12.2 Configuring Quota Mode

Purpose:

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

Step 1 Enter the Storage Mode interface.

Menu > HDD > Advanced

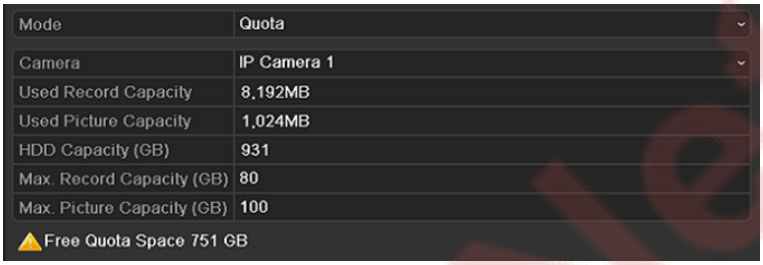


Figure 12-5 Storage Mode Settings Interface

Step 2 Select a camera for which you want to configure quota.

Step 3 Enter the storage capacity in the text fields of **Max. Record Capacity (GB)** and **Max. Picture Capacity (GB)**, as shown in Figure 12-6.

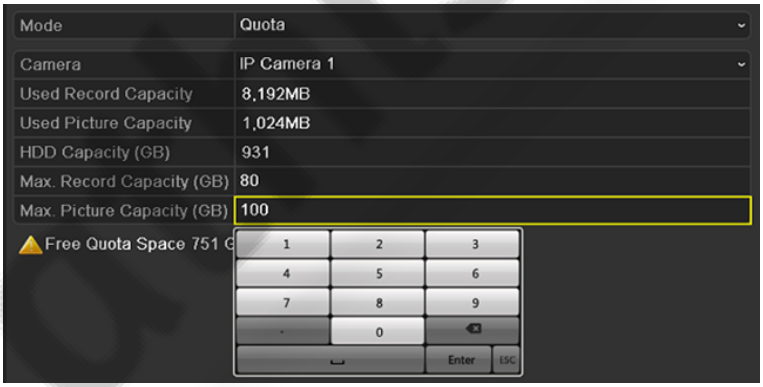


Figure 12-6 Configure Record/Picture Quota

Step 4 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 12-7.

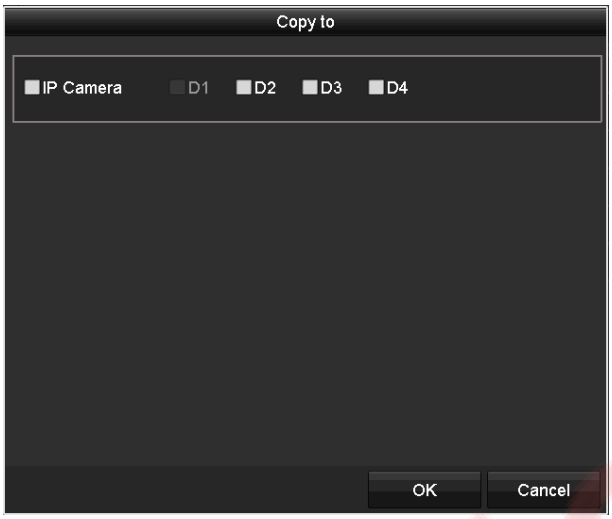


Figure 12-7 Copy Settings to Other Camera(s)

Step 5 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.

Step 6 Click the **OK** button to finish the Copy settings and back to the Storage Mode interface.

Step 7 Click the **Apply** button to apply the settings.

NOTE

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

12.3 Checking HDD Status

Purpose:

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

12.3.1 Checking HDD Status in HDD Information Interface

Step 1 Enter the HDD Information interface.

Menu > HDD > General

Step 2 Check the status of each HDD which is displayed on the list, as shown in Figure 12-8.

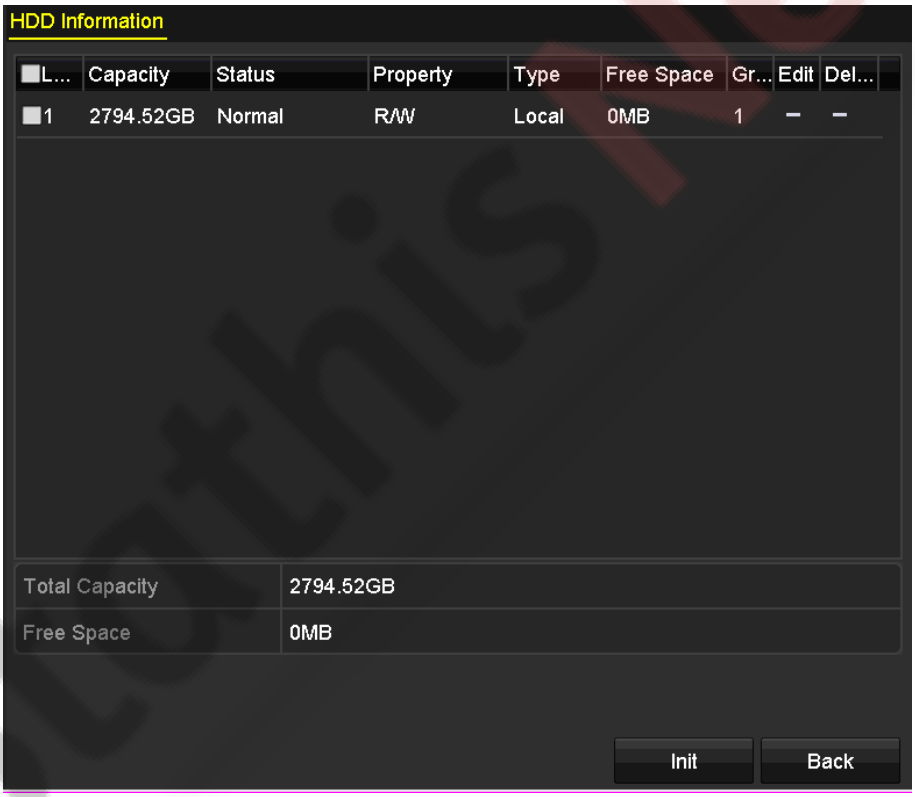


Figure 12-8 View HDD Status (1)

NOTE

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

12.3.2 Checking HDD Status in HDD Information Interface

Step 1 Enter the System Information interface.

Menu >Maintenance > System Info

Step 2 Click the **HDD** tab to view the status of each HDD displayed on the list, as shown in Figure 12-9.

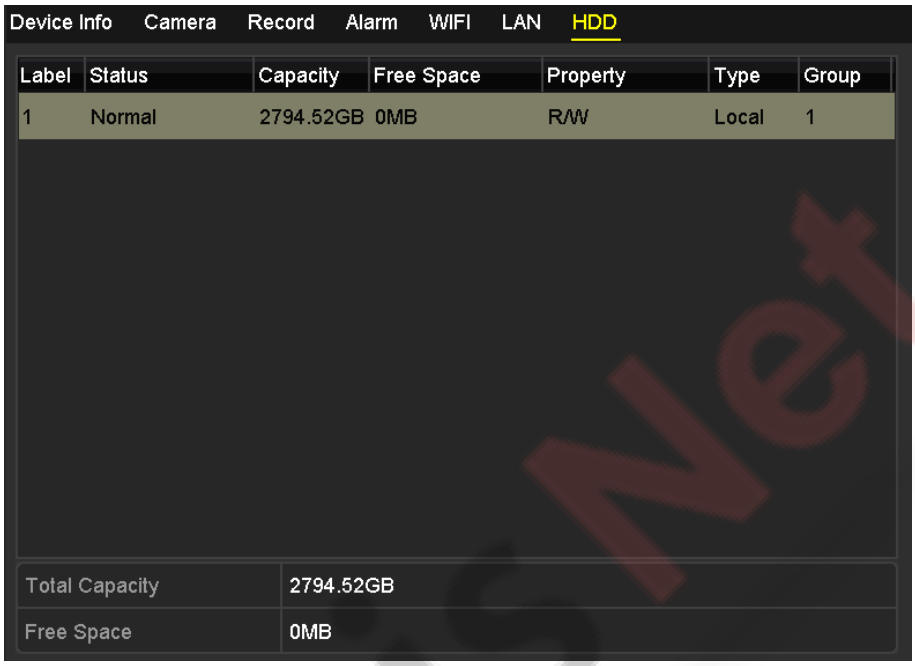


Figure 12-9 View HDD Status (2)

12.4 HDD Detection

Purpose:

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

12.4.1 S.M.A.R.T. Settings

Step 1 Enter the S.M.A.R.T Settings interface.

Menu > Maintenance >HDD Detect

Step 2 Select the HDD to view its S.M.A.R.T information list, as shown in Figure 12-10.

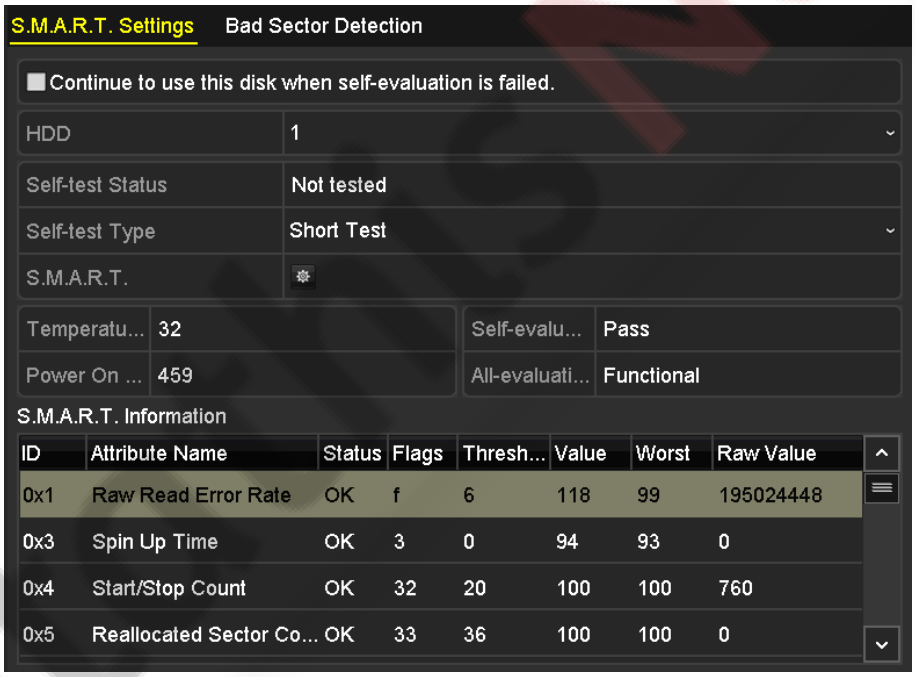


Figure 12-10 S.M.A.R.T Settings Interface

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

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

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

NOTE

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

12.4.2 Bad Sector Detection

Step 1 Click the Bad Sector Detection tab.

Step 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.

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

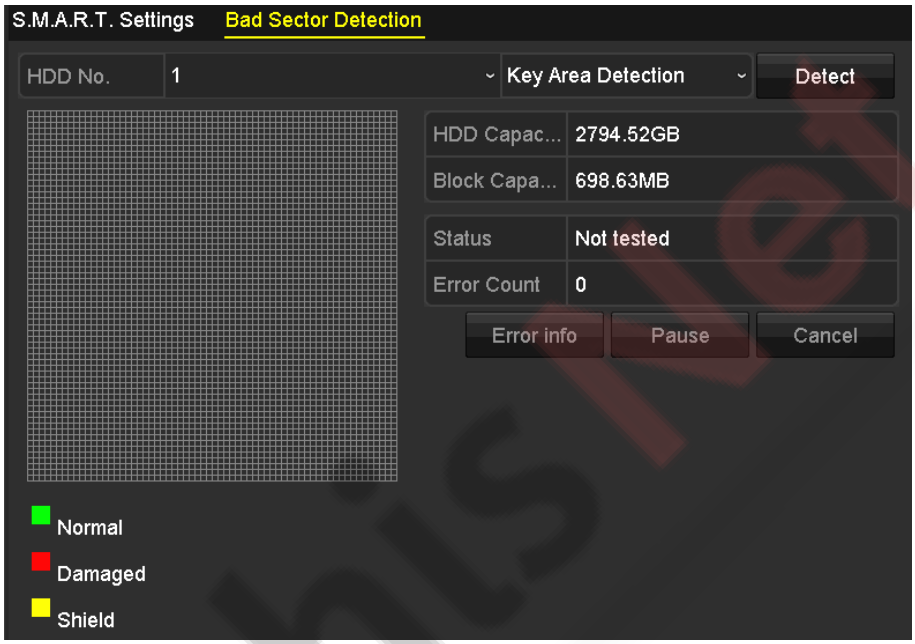


Figure 12-11 Bad Sector Detection

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

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

12.5 Configuring HDD Error Alarms

Purpose:

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

Step 1 Enter the Exception interface.

Menu > Configuration > Exceptions

Step 2 Select the Exception Type to **HDD Error** from the dropdown list.

Step 3 Click the checkbox(s) below to select the HDD error alarm type (s), as shown in Figure 12-12.

NOTE

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*.

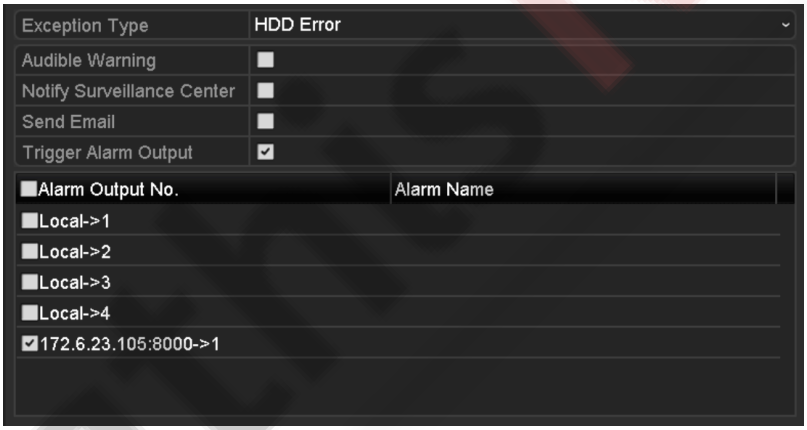


Figure 12-12 Configure HDD Error Alarm

Step 4 When the Trigger Alarm Output is selected, you can also select the alarm output to be triggered from the list below.

Step 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.

Step 1 Enter the OSD Configuration interface.

Menu > Camera > OSD

Step 2 Select the camera to configure OSD settings.

Step 3 Edit the **Camera Name**.

Step 4 Configure the **Display Name, Display Date,** and **Display Week** by clicking the checkboxes.

Step 5 Select the **Date Format, Time Format,** and **Display Mode**.

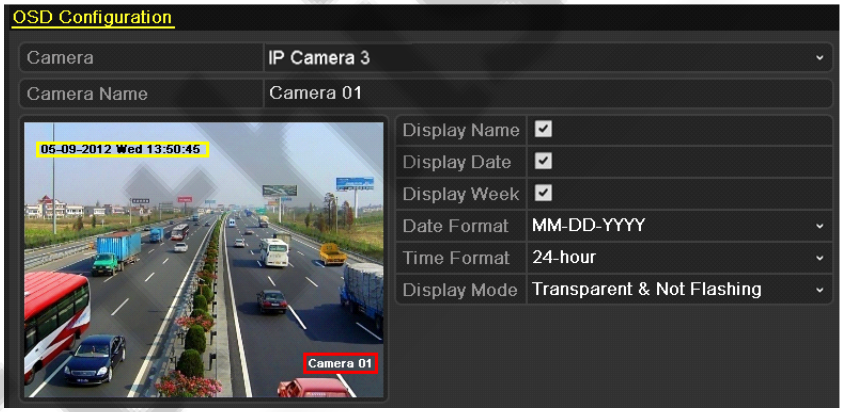


Figure 13-1 OSD Configuration Interface

Step 6 You can use the mouse to click and drag the text frame on the preview window to adjust the OSD position.

Step 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.

Step 1 Enter the Privacy Mask Settings interface.

Menu > Camera > Privacy Mask

Step 2 Select the camera to set privacy mask.

Step 3 Click the checkbox of **Enable Privacy Mask** to enable this feature.

Figure 13-2 Privacy Mask Settings Interface

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

NOTE

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

Step 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.

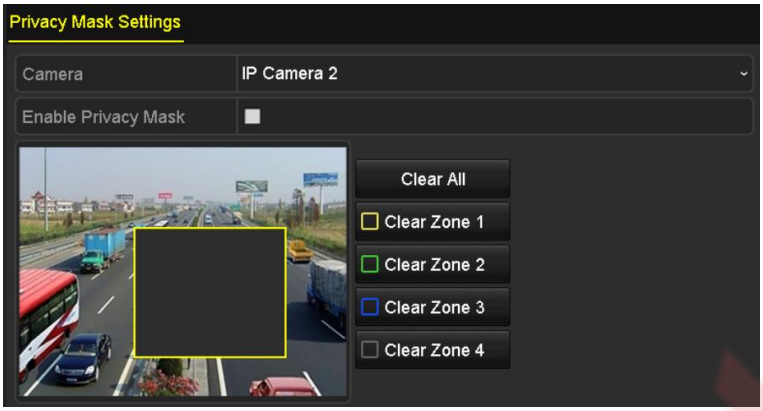


Figure 13-3 Set Privacy Mask Area

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

13.3 Configuring Video Parameters

Purpose:

You can customize the image parameters including the brightness, contrast, saturation, image rotate and mirror for the live view and recording effect.

Step 1 Enter the Image Settings interface.

Menu > Camera > Image

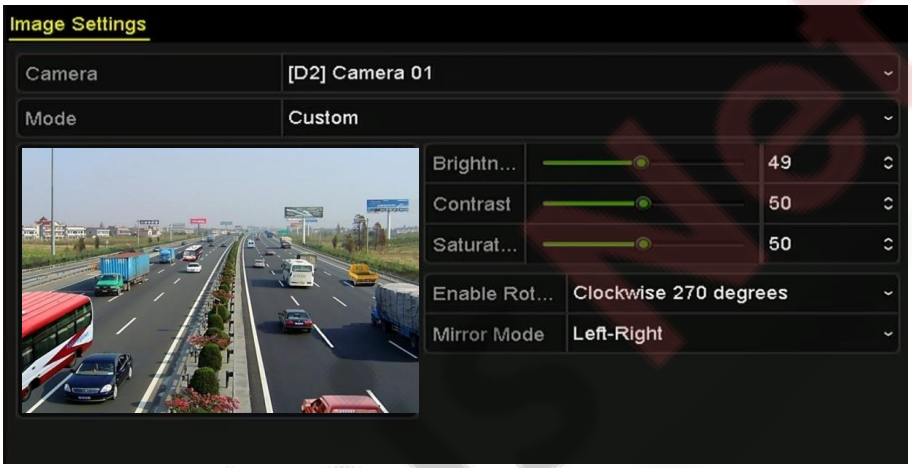


Figure 13-4 Image Settings Interface

Step 2 Select the camera to set image parameters.

Step 3 Adjust the slider or click on the up/down arrow to set the value of the brightness, contrast or saturation.

Step 4 Select the **Enable Rotate** function to Clockwise 270 degrees or OFF. When OFF is selected, the image is restored to original.

Step 5 Select the **Mirror Mode** to Left-Right, Up-Down, Center or OFF. When OFF is selected, the image is restored to original.

NOTE

- The Rotate and Mirror functions must be supported by the connected IP camera.
- The image parameters adjustment can affect both the live view and the recording quality.

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

Chapter 14 NVR Management and Maintenance

14.1 Viewing System Information

Step 1 Enter the System Information interface.

Menu > Maintenance > System Info

Step 2 You can click the **Device Info**, **Camera**, **Record**, **Alarm**, **WiFi**, **Network** and **HDD** tabs to view the system information of the device.

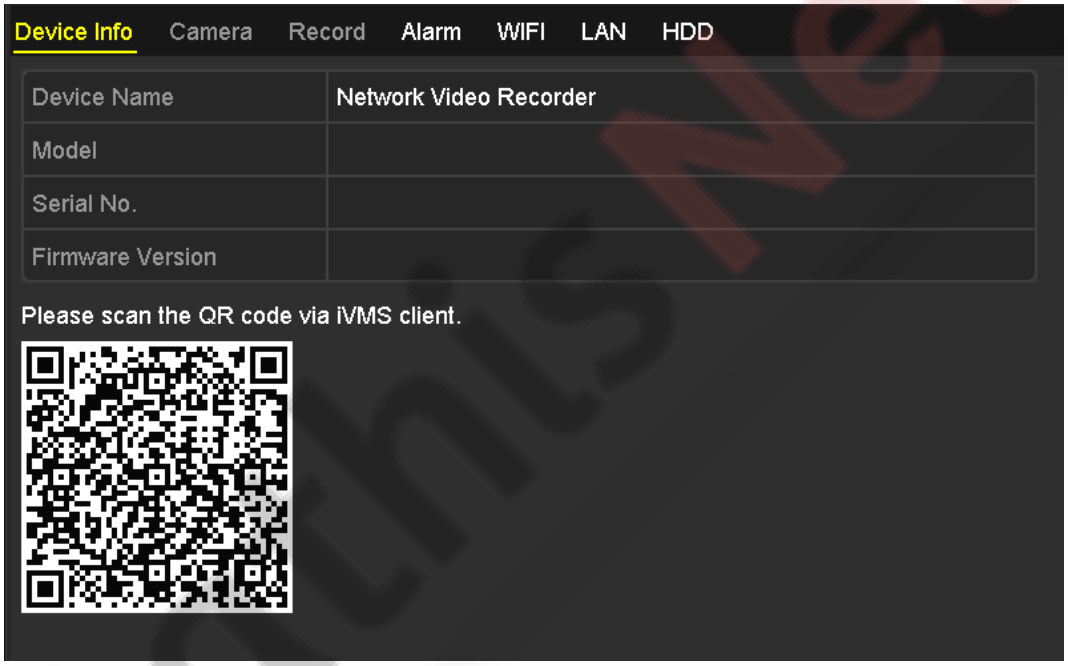


Figure 14-1 Device Information Interface

NOTE

You can add the device to your mobile client software (iVMS-4500) via scanning the QR Code.

14.2 Searching & Exporting 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.

Step 1 Enter the Log Search interface.

Menu > Maintenance > Log Information

Figure 14-2 Log Search Interface

Step 2 Set the log search conditions to refine your search, including the Start Time, End Time, Major Type and Minor Type.

Step 3 Click the **Search** button to start search log files.

Step 4 The matched log files will be displayed on the list shown below.

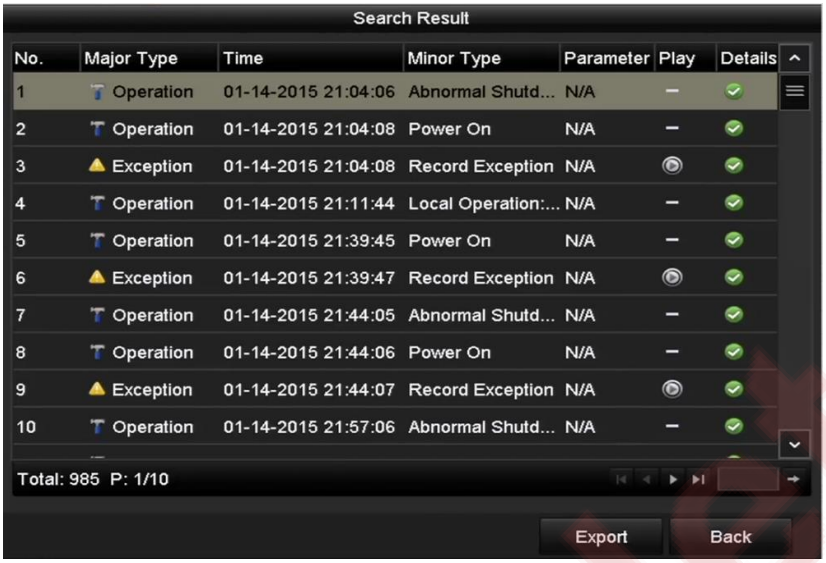


Figure 14-3 Log Search Results

NOTE

Up to 2000 log files can be displayed each time.

Step 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.

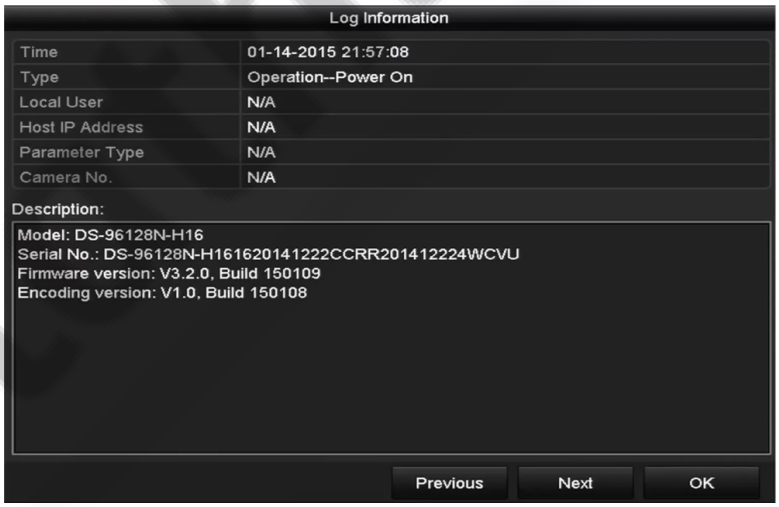


Figure 14-4 Log Details

Step 6 If you want to export the log files, click the **Export** button to enter the Export menu, as shown in Figure 14-4 Log Details.

You can also click **Export All** on the Log Search interface (Figure 15.2) to enter the Export interface (Figure 15.5), and all the system logs will be exported to the backup device.

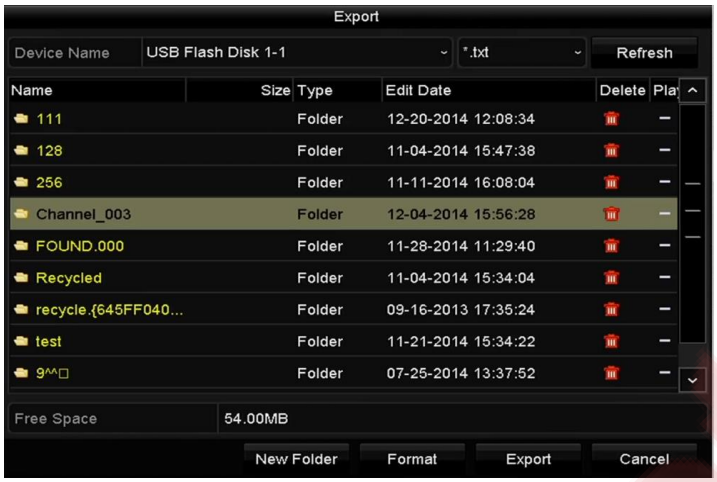


Figure 14-5 Export Log Files

Step 7 Select the backup device from the dropdown list of **Device Name**.

Step 8 Select the format of the log files to be exported. Up to 15 formats are selectable.

Step 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.

Step 1 Enter the camera management interface.

Menu > Camera > IP Camera Import/Export

Step 2 Click the IP Camera Import/Export tab, the content of detected plugged external device appears.

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

Step 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.

Step 1 Enter the Import/Export Configuration File interface.

Menu > Maintenance >Import/Export

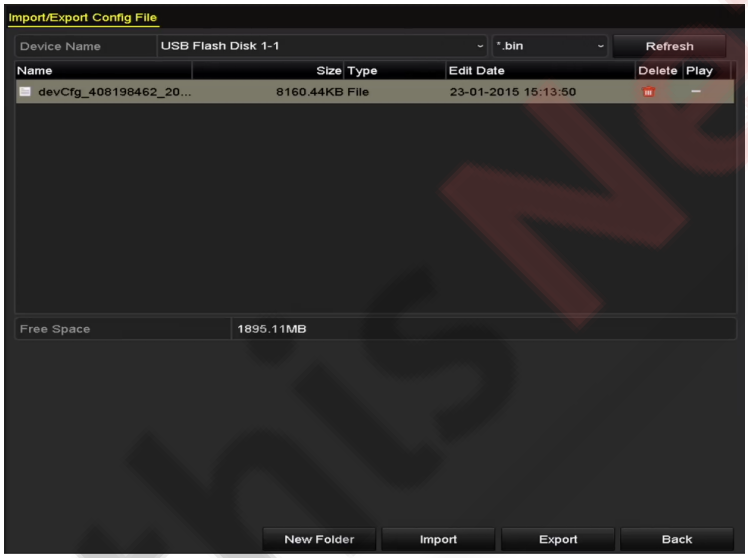


Figure 14-6 Import/Export Config File

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

Step 3 To import a configuration file, select the file from the selected backup device and click the **Import** button. After the import process is completed, you must reboot the NVR.

NOTE

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

14.5 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

Step 1 Connect your NVR with a local backup device where the update firmware file is located.

Step 2 Enter the Upgrade interface.

Menu > Maintenance > Upgrade

Step 3 Click the **Local Upgrade** tab to enter the local upgrade menu, as shown in Figure 14-7.

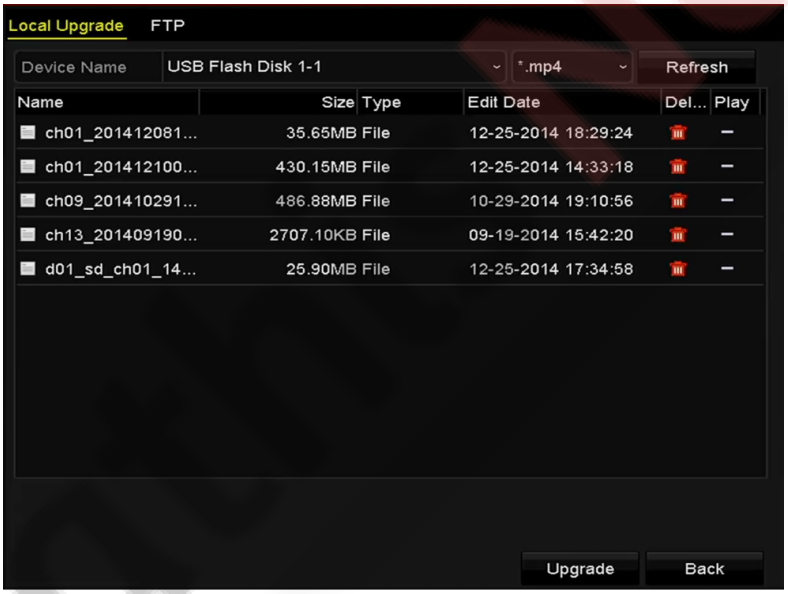


Figure 14-7 Local Upgrade Interface

Step 4 Select the update file from the backup device.

Step 5 Click the **Upgrade** button to start upgrading.

Step 6 After the upgrading is complete, reboot the NVR to activate the new firmware.

14.5.2 Upgrading by FTP

Before you start:

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.

Step 1 Enter the Upgrade interface.

Menu > Maintenance > Upgrade

Step 2 Click the **FTP** tab to enter the local upgrade interface, as shown in Figure 14-8.

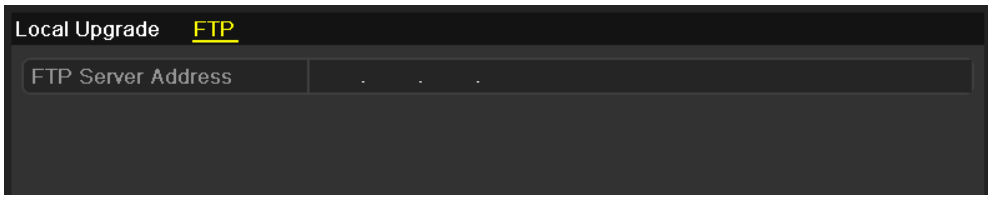


Figure 14-8 FTP Upgrade Interface

Step 3 Enter the FTP Server Address in the text field.

Step 4 Click the **Upgrade** button to start upgrading.

Step 5 After the upgrading is complete, reboot the NVR to activate the new firmware.

14.6 Restoring Default Settings

Step 1 Enter the Default interface.

Menu > Maintenance > Default

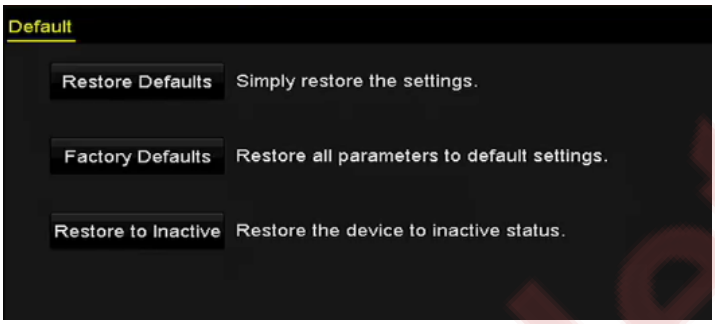


Figure 14-9 Restore Defaults

Step 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.

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

NOTE

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

Chapter 15 Others

15.1 Configuring General Settings

Purpose:

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

Step 1 Enter the General Settings interface.

Menu > Configuration > General

Step 2 Select the **General** tab.

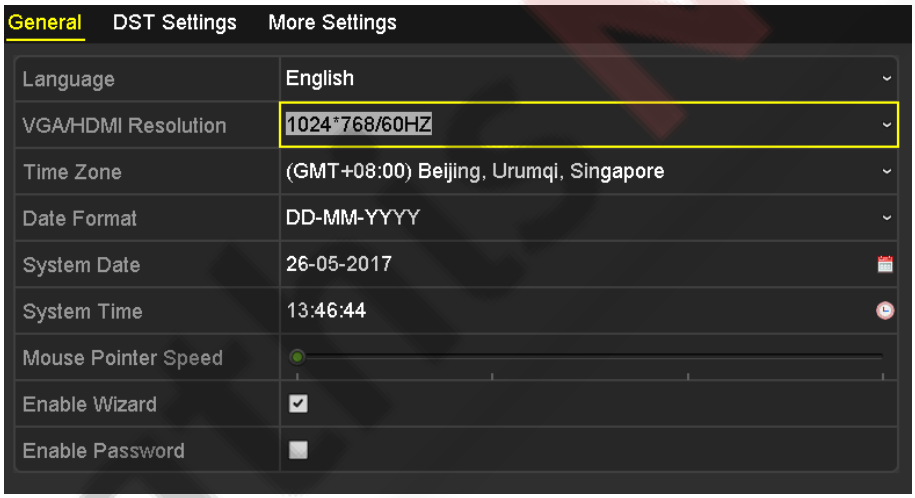


Figure 15-1 General Settings Interface

Step 3 Configure the following settings:

- **Language:** The default language used is *English*.
- **Output Standard:** Select the output standard to NTSC or PAL, which must be the same with the video input standard.
- **Resolution:** Configure the VGA/HDMI resolution.
- **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.

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

15.2 Configuring DST Settings

Step 1 Enter the General Settings interface.

Menu > Configuration > General

Step 2 Choose **DST Settings** tab.

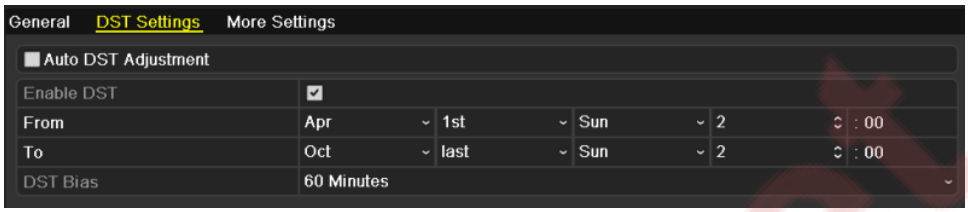


Figure 15-2 DST Settings Interface

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

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

15.3 Configuring More Settings

Step 1 Enter the General Settings interface.

Menu > Configuration > General

Step 2 Click the **More Settings** tab to enter the More Settings interface.

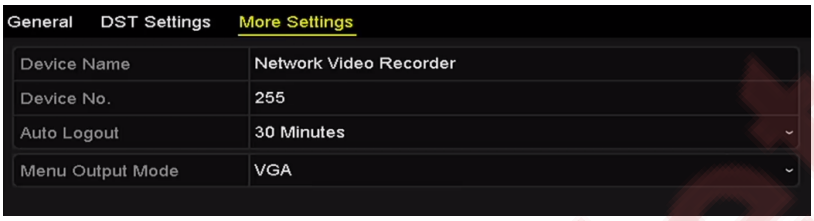


Figure 15-3 More Settings Interface

Step 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 Log out:** 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.

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

15.4 Managing User Accounts

Purpose:

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

15.4.1 Adding a User

Step 1 Enter the User Management interface.

Menu > Configuration > User

Figure 15-4 User Management Interface

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

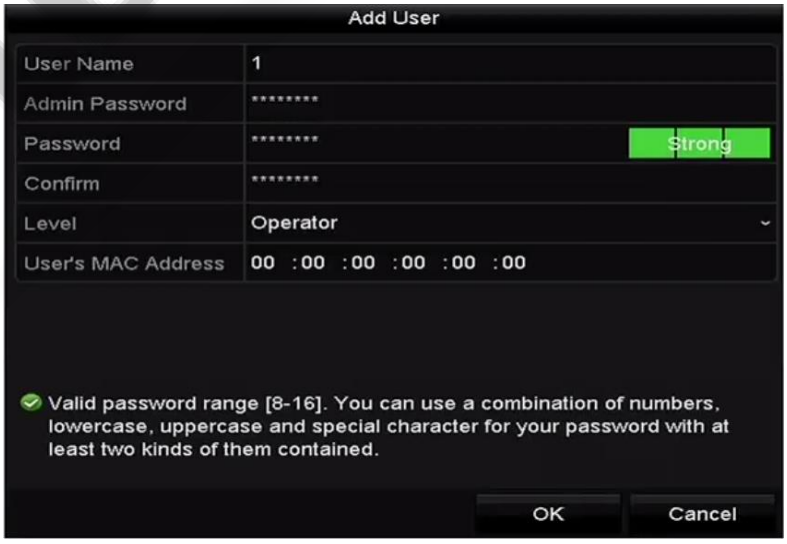


Figure 15-5 Add User Menu

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

Password: Set the password for the user account.

WARNING

Strong Password recommended–We highly recommend you create a strong password of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

- **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.

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

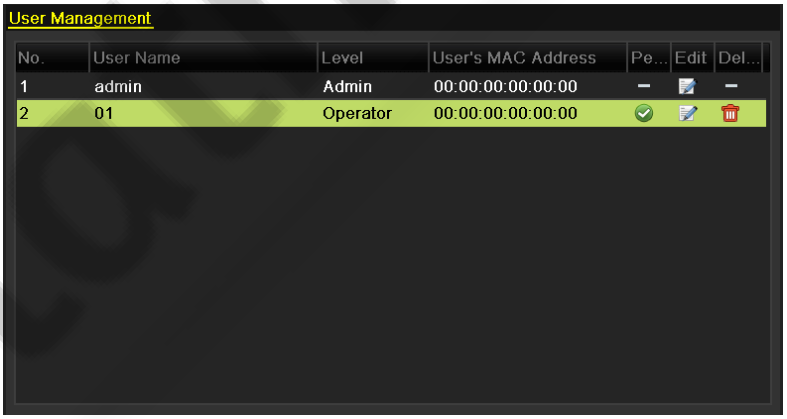


Figure 15-6 Added User Listed in User Management Interface

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

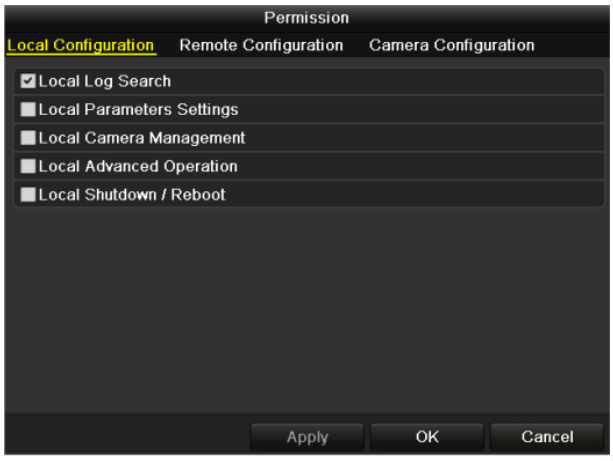


Figure 15-7 User Permission Settings Interface

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

- Local Configuration

  Local Log Search: Searching and viewing logs and system information of NVR.

  Local Parameters Settings: Configuring parameters, restoring factory default parameters and importing/exporting configuration files.

  Local Camera Management: The adding, deleting and editing of IP cameras.

  Local Advanced Operation: Operating HDD management (initializing HDD, setting HDD property), upgrading system firmware, clearing I/O alarm output.

  Local Shutdown Reboot: Shutting down or rebooting the NVR.

- Remote Configuration

  Remote Log Search: Remotely viewing logs that are saved on the NVR.

  Remote Parameters Settings: Remotely configuring parameters, restoring factory default parameters and importing/exporting configuration files.

  Remote Camera Management: Remote adding, deleting and editing of the IP cameras.

  Remote Serial Port Control: Configuring settings for RS-232 and RS-485 ports.

  Remote Video Output Control: Sending remote button control signal.

  Two-Way Audio: Realizing two-way radio between the remote client and the NVR.

  - **Remote Alarm Control**: Remotely arming (notify alarm and exception message to the remote client) and controlling the alarm output.
  - **Remote Advanced Operation**: Remotely operating HDD management (initializing HDD, setting HDD property), upgrading system firmware, clearing I/O alarm output.
  - **Remote Shutdown/Reboot**: Remotely shutting down or rebooting the NVR.

- Camera Configuration

  Remote Live View: Remotely viewing live video of the selected camera (s).

Local Manual Operation: Locally starting/stopping manual recording and alarm output of the selected camera (s).

Remote Manual Operation: Remotely starting/stopping manual recording and alarm output of the selected camera (s).

Local Playback: Locally playing back recorded files of the selected camera (s).

Remote Playback: Remotely playing back recorded files of the selected camera (s).

Local PTZ Control: Locally controlling PTZ movement of the selected camera (s).

Remote PTZ Control: Remotely controlling PTZ movement of the selected camera (s).

Local Video Export: Locally exporting recorded files of the selected camera (s).

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

NOTE

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

15.4.2 Deleting a User

Step 1 Enter the User Management interface.

Menu >Configuration>User

Step 2 Select the user to be deleted from the list, as shown in Figure 15-8.

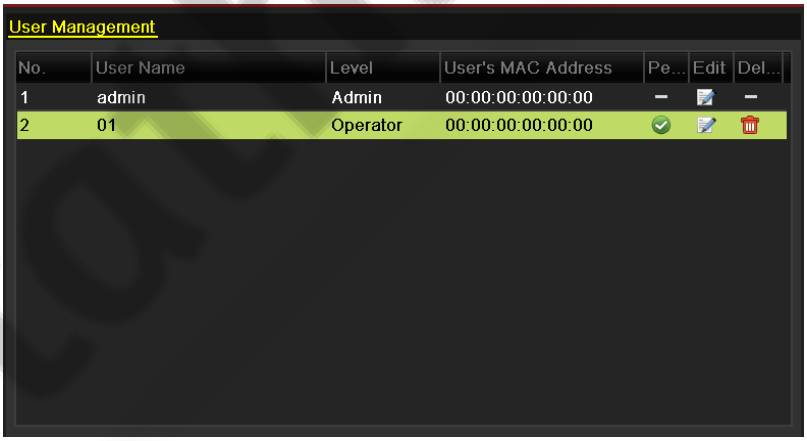


Figure 15-8 User List

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

15.4.3 Editing a User

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

Step 1 Enter the User Management interface.

Menu >Configuration>User

Step 2 Select the user to be edited from the list, as shown in Figure 15-8.

Step 3 Click the icon to enter the Edit User interface, as shown in Figure 15-10.

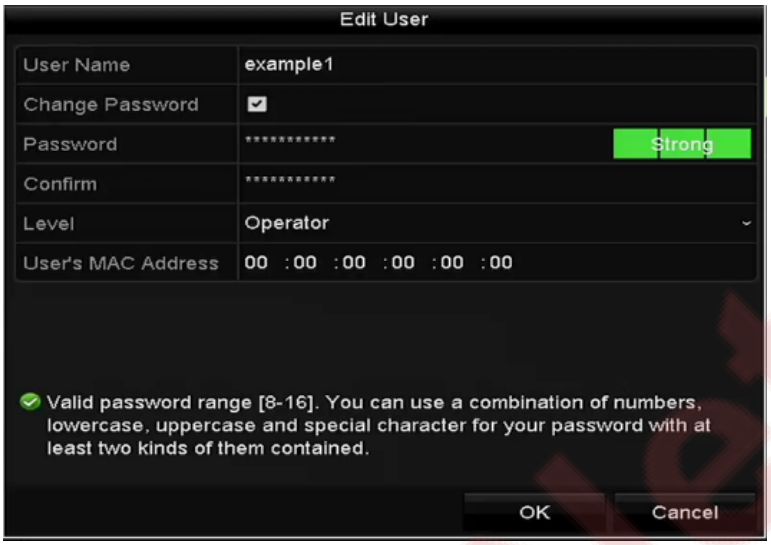


Figure 15-9 Edit User (Operator/Guest)

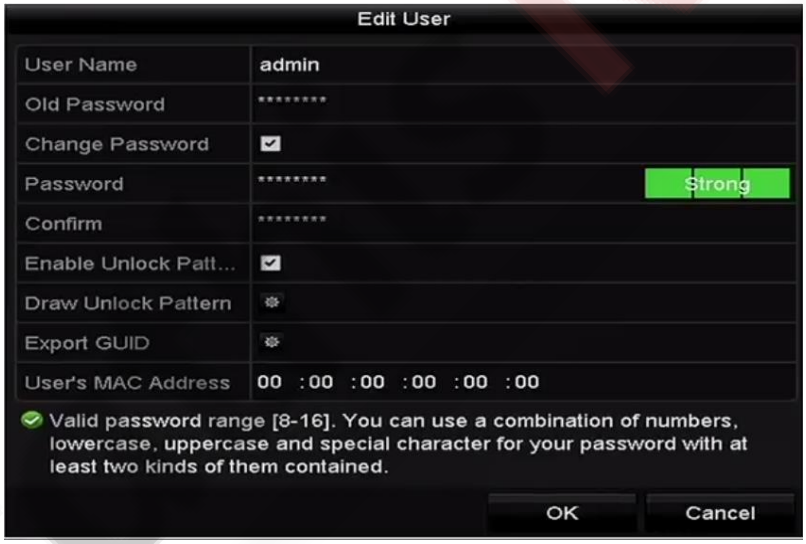


Figure 15-10 Edit User (admin)

Step 4 Edit the password for the user

- **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**.

WARNING

Strong Password recommended–We highly recommend you create a strong password of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Step 5 Edit the unlock pattern for the admin user account.

1) Check the checkbox of **Enable Unlock Pattern** to enable the use of unlock pattern when logging in to the device.
2) Use the mouse to draw a pattern among the 9 dots on the screen. Release the mouse when the pattern is done.

NOTE

Please refer to *Chapter 2.1.3 Using the Unlock Pattern for Login* for detailed instructions.

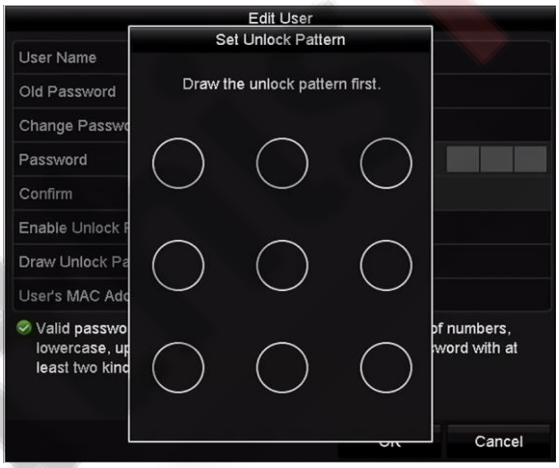


Figure 15-11 Set Unlock Patter for Admin User

Step 6 Click the of **Export GUID** to enter the reset password interface to export the GUID file for the admin user account.

When the admin password is changed, you can re-export the GUID file to the connected U flash disk for the future password resetting. Please refer to *Chapter 2.1.5 Resetting Your Password* for details.

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

Step 8 For the **Operator** or **Guest** user account, you can also click the button on the user management interface to edit the permission.

Chapter 16 Appendix

16.1 Specifications

Model		DS-7804N-K1/W	DS-7808N-K1/W
Video/Audio input	IP video input	4-ch	8-ch
	Incoming bandwidth	50 Mbps	
Video/Audio output	HDMI/VGA output	1-ch, resolution: 1920 × 1080/60Hz, 1600 × 1200/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz	
	Audio output	1-ch, RCA (linear, 1 KΩ)	
Decoding	Recording resolution	5M/4M/3M/1080p/1.3M/720p	
	Synchronous playback	4-ch	8-ch
Hard disk	SATA	1 SATA interface	
	Capacity	Up to 6 TB capacity for each disk	
Wireless parameters	Frequency band	2.4 GHz	
	Antenna structure	2*2MIMO. External antennas. PA and LNA modules are supported.	
	Transmission speed	300 Mbps	
	Transmission standard	IEEE 802.11b/g/n	
External interface	Network interface	1, RJ45 100M Ethernet interface	
	USB interface	Rear panel: 2 × USB 2.0	
General	Power supply	12 VDC	
	Consumption (without HDDs)	≤ 18 W	
	Working temperature	-10 °C to +55 °C (14 °F to 131 °F)	
	Working humidity	10% to 90%	
	Dimensions (W × D × H)	205 × 205 × 45 mm (8.1 × 8.1 × 1.8 in)	
	Weight (without HDDs)	≤ 1 kg (2.2 lb)	

16.2 Glossary

- **Dual Stream:** Dual stream is a technology used to record high resolution video locally while transmitting a lower resolution stream over the network. The two streams are generated by the NVR, with the main stream having a maximum resolution of 4CIF and the sub-stream having a maximum resolution of CIF.
- **HDD:** Acronym for Hard Disk Drive. A storage medium which stores digitally encoded data on platters with magnetic surfaces.
- **DHCP:** Dynamic Host Configuration Protocol (DHCP) is a network application protocol used by devices (DHCP clients) to obtain configuration information for operation in an Internet Protocol network.
- **HTTP:** Acronym for Hypertext Transfer Protocol. A protocol to transfer hypertext request and information between servers and browsers over a network
- **DDNS:** Dynamic DNS is a method, protocol, or network service that provides the capability for a networked device, such as a router or computer system using the Internet Protocol Suite, to notify a domain name server to change, in real time (ad-hoc) the active DNS configuration of its configured hostnames, addresses or other information stored in DNS.
- **Hybrid NVR:** A hybrid NVR is a combination of a NVR and NVR.
- **NTP:** Acronym for Network Time Protocol. A protocol designed to synchronize the clocks of computers over a network.
- **NTSC:** Acronym for National Television System Committee. NTSC is an analog television standard used in such countries as the United States and Japan. Each frame of an NTSC signal contains 525 scan lines at 60Hz.
- **NVR:** Acronym for Network Video Recorder. An NVR can be a PC-based or embedded system used for centralized management and storage for IP cameras, IP Domes and other NVRs.
- **PAL:** Acronym for Phase Alternating Line. PAL is also another video standard used in broadcast televisions systems in large parts of the world. PAL signal contains 625 scan lines at 50Hz.
- **PTZ:** Acronym for Pan, Tilt, Zoom. PTZ cameras are motor driven systems that allow the camera to pan left and right, tilt up and down and zoom in and out.
- **USB:** Acronym for Universal Serial Bus. USB is a plug-and-play serial bus standard to interface devices to a host computer.

16.3 Troubleshooting

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

  Possible Reasons:

  - No VGA or HDMI connections.
  - Connection cable is damaged.
  - Input mode of the monitor is incorrect.

Step 1 Verify the device is connected with the monitor via HDMI or VGA cable.

Step 2 If not, please connect the device with the monitor and reboot.

Step 3 Verify the connection cable is good.

Step 4 If there is still no image display on the monitor after rebooting, please check if the connection cable is good, and change a cable to connect again.

Step 5 Verify Input mode of the monitor is correct.

Step 6 Please check the input mode of the monitor matches with the output mode of the device (e.g. if the output mode of NVR is HDMI output, then the input mode of monitor must be the HDMI input). And if not, please modify the input mode of monitor.

Step 7 Check if the fault is solved by the step 1 to step 3.

Step 8 If it is solved, finish the process.

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

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

  Possible Reasons:

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

Step 9 Verify at least one HDD is installed in the NVR.

- If not, please install the compatible HDD.

NOTE

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

- If you don’t want to install a HDD, select “Menu>Configuration > Exceptions”, and uncheck the Audible Warning checkbox of “HDD Error”.

Step 10 Verify the HDD is initialized.

1) Select “Menu>HDD>General”.
2) If the status of the HDD is “Uninitialized”, please check the checkbox of corresponding HDD and click the “Init” button.

Step 11 Verify the HDD is detected or is in good condition.

3) Select “Menu>HDD>General”.
4) If the HDD is not detected or the status is “Abnormal”, please replace the dedicated HDD according to the requirement.

Step 12 Check if the fault is solved by the step 1 to step 3.

If it is solved, finish the process.

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

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

Possible Reasons:

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

Step 1 Verify the network is connected.

1) Connect the NVR and PC with the RS-232 cable.
2) Open the Super Terminal software, and execute the ping command. Input “ping IP” (e.g. ping 172.6.22.131).

NOTE

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

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

Step 2 Verify the configuration parameters are correct.

1) Select “Menu>Camera>Camera>IP Camera”.
2) Verify the following parameters are the same with those of the connected IP devices, including IP address, protocol, management port, user name and password.

Step 3 Verify the whether the bandwidth is enough.

1) Select “Menu >Maintenance > Net Detect > Network Stat.”.
2) Check the usage of the access bandwidth, and see if the total bandwidth has reached its limit.

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

If it is solved, finish the process.

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

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

  Possible Reasons:

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

Step 1 Verify the IP camera and the NVR versions are compatible.

1) Enter the IP camera Management interface "Menu > Camera > Camera>IP Camera", and view the firmware version of connected IP camera.
2) Enter the System Info interface "Menu>Maintenance>System Info>Device Info", and view the firmware version of NVR.

Step 2 Verify power supply of IP camera is stable.

1) Verify the power indicator is normal.
2) When the IP camera is offline, please try the ping command on PC to check if the PC connects with the IP camera.

Step 3 Verify the network between IP camera and NVR is stable.

3) When the IP camera is offline, connect PC and NVR with the RS-232 cable.
4) Open the Super Terminal, use the ping command and keep sending large data packages to the connected IP camera, and check if there exists packet loss.

NOTE

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

Example: Input ping 172.6.22.131 –l 1472 –f.

Step 1 Verify the switch is not flow control.

Check the brand, model of the switch connecting IP camera and NVR, and contact with the manufacturer of the switch to check if it has the function of flow control. If so, please turn it down.

Step 2 Check if the fault is solved by the step 1 to step 4.

If it is solved, finish the process.

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

- **No monitor connected with the NVR locally and when you manage the IP camera to connect with the device by web browser remotely, of which the status displays as Connected. And then you connect the device with the monitor via VGA or HDMI interface and reboot the device, there is black screen with the mouse cursor.**

  Connect the NVR with the monitor before startup via VGA or HDMI interface, and manage the IP camera to connect with the device locally or remotely, the status of IP camera displays as Connect. And then connect the device with the CVBS, and there is black screen either.

  Possible Reasons:

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

Step 1 Enable the output channel.

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

NOTE

- The view settings can only be configured by the local operation of NVR.
- Different camera orders and window-division modes can be set for different output interfaces separately, and digits like “D1”and “D2” stands for the channel number, and “X” means the selected window has no image output.

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

If it is solved, finish the process.

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

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

  Possible Reasons:

  – Poor network between NVR and IP camera, and there exists packet loss during the transmission.

  – The frame rate has not reached the real-time frame rate.

Step 1 Verify the network between NVR and IP camera is connected.

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

NOTE

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

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

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

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

If it is solved, finish the process.

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

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

Possible Reasons:

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

Step 4 Verify the network between NVR and IP camera is connected.

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

NOTE

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

Step 5 Verify the network between NVR and PC is connected.

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

NOTE

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

Step 6 Verify the hardware of the PC is good enough.

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

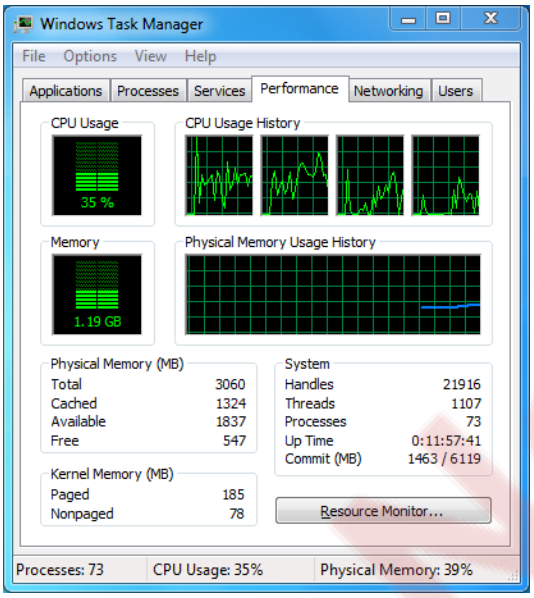


Figure 16-1 Windows task management interface

- Select the “Performance” tab; check the status of the CPU and Memory.
- If the resource is not enough, please end some unnecessary processes.

Step 7 Check if the fault is solved by the above steps.

If it is solved, finish the process.

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

- **When using the NVR to get the live view audio, there is no sound or there is too much noise, or the volume is too low.**

Possible Reasons:

- Cable between the pickup and IP camera is not connected well; impedance mismatches or incompatible.
- The stream type is not set as “Video & Audio”.
- The encoding standard is not supported with NVR.

Step 1 Verify the cable between the pickup and IP camera is connected well; impedance matches and compatible.

Log in the IP camera directly, and turn the audio on, check if the sound is normal. If not, please contact the manufacturer of the IP camera.

Step 2 Verify the setting parameters are correct.

Select “Menu > Record > Parameters > Record”, and set the Stream Type as “Audio & Video”.

Step 3 Verify the audio encoding standard of the IP camera is supported by the NVR.

NVR supports G722.1 and G711 standards, and if the encoding parameter of the input audio is not one of the previous two standards, you can log in the IP camera to configure it to the supported standard.

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

If it is solved, finish the process.

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

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

Possible Reasons:

- Poor network between NVR and IP camera, and there exists packet loss during the transmission.
- The frame rate is not the real-time frame rate.
- The NVR supports up to 16-channel synchronize playback at the resolution of 4CIF, if you want a 16-channel synchronize playback at the resolution of 720p, the frame extracting may occur, which leads to a slight stuck.

Step 5 Verify the network between NVR and IP camera is connected.

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

NOTE

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

Step 6 Verify the frame rate is real-time frame rate.

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

Step 7 Verify the hardware can afford the playback.

Reduce the channel number of playback.

Select "Menu > Record > Encoding > Record", and set the resolution and bitrate to a lower level.

Step 8 Reduce the number of local playback channel.

Select "Menu > Playback", and uncheck the checkbox of unnecessary channels.

Step 9 Check if the fault is solved by the above steps.

If it is solved, finish the process.

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

- **No record file found in the NVR local HDD, and prompt "No record file found".**

Possible Reasons:

- The time setting of system is incorrect.
- The search condition is incorrect.
- The HDD is error or not detected.

Step 1 Verify the system time setting is correct.

Select "Menu > Configuration > General > General", and verify the "Device Time" is correct.

Step 2 Verify the search condition is correct.

Select "Playback", and verify the channel and time are correct.

Step 3 Verify the HDD status is normal.

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

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

If it is solved, finish the process.

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

16.4 List of Compatible IP Cameras

16.4.1 List of Hikvision IP Cameras

NOTE

For the list, our company holds right to interpret.

Type	Model	Version	Max. Resolution	Sub-stream	Audio
SD Network Camera	DS-2CD7133F-E	V5.2.0 build 140721	640*480	√	×
	DS-2CD793NFWD-EI	V5.2.0 build 140721	704*576	√	√
	DS-2CD802NF	V2.0 build 090522	704*576	√	√
		V2.0 build 090715			
		V2.0 build 110301			
	DS-2CD833F-E	V5.2.0 build 140721	640*480	√	√
	DS-2CD893PF-E	V5.2.0 build 140721	704*576	√	√
HD Network Camera	DS-2CD2012-I	V5.3.0 build150327	1280*960	√	×
	DS-2CD2132-I	V5.3.0 build150327	2048*1536	√	×
	DS-2CD2410FD-I(W)	V5.3.0 build150327	1920*1080	√	√
	DS-2CD2612F-I	V5.3.0 build150327	1280*960	√	×
	DS-2CD2612F-IS	V5.3.0 build150327	1280*960	√	√
	DS-2CD2632F-I	V5.3.0 build150327	2048*1536	√	×
	DS-2CD2632F-IS	V5.3.0 build150327	2048*1536	√	√
	DS-2CD2710F-I	V5.3.0 build150327	1920*1080	√	×
	DS-2CD2720F-I	V5.3.0 build150327	1920*1080	√	×
	DS-2CD4010F	V5.3.0 build150327	1920*1080	√	√
	DS-2CD4012F	V5.3.0 build150327	1280*1024	√	√
	DS-2CD4026FWD	V5.3.0 build150327	1920*1080	√	√
	DS-2CD4026FWD-SDI	V5.3.0 build150327	1920*1080	√	√
	DS-2CD4032FWD	V5.3.0 build150327	2048*1536	√	√
	DS-2CD4065F	V5.3.0 build150327	3072*2048	√	√
	DS-2CD4124F-I(2.8-12mm)	V5.3.0 build150327	1920*1080	√	√
	DS-2CD4132FWD-I(2.8-12mm)	V5.3.0 build150327	2048*1536	√	√
	DS-2CD4212F-I(2.8-12mm)	V5.3.0 build150327	1280*1024	√	×
	DS-2CD4212F-IS(2.8-12mm)	V5.3.0 build150327	1280*1024	√	√
	DS-2CD4212FWD-I	V5.3.0 build150327	1280*960	√	×
	DS-2CD4212FWD-IS	V5.3.0 build150327	1280*960	√	√
	DS-2CD4224F-I	V5.3.0 build150327	1920*1080	√	×
	DS-2CD4232FWD-I	V5.3.0 build150327	2048*1536	√	×

Type	Model	Version	Max. Resolution	Sub-stream	Audio
	DS-2CD4232FWD-IS(2.8-12mm)	V5.3.0 build150327	2048*1536	√	√
	DS-2CD4312F-I	V5.3.0 build150327	1280*1024	√	×
	DS-2CD4312FWD-I	V5.3.0 build150327	1280*960	√	×
	DS-2CD4324F-I	V5.3.0 build150327	1920*1080	√	×
	DS-2CD4332FHWD-IS	V5.3.0 build150327	2048*1536	√	√
	DS-2CD4332FHWD-I	V5.3.0 build150327	2048*1536	√	×
	DS-2CD4332FWD-I	V5.3.0 build150327	2048*1536	√	×
	DS-2CD6213F	V5.2.6 build 141218	1280*960	√	×
	DS-2CD6223F	V5.2.6 build 141218	1920*1080	√	×
	DS-2CD6233F	V5.2.6 build 141218	2048*1536	√	×
	DS-2CD7153-E	V5.2.0 build 140721	1600*1200	√	×
	DS-2CD7164-E	V5.2.0 build 140721	1280*720	√	×
	DS_2CD754F-EI	V5.2.0 build 140721	2048*1536	√	√
	DS-2CD754FWD-E	V5.2.0 build 140721	1920*1080	√	√
	DS-2CD754FWD-EIZ	V5.2.0 build 140721	2048*1536	√	√
	DS_2CD783F-EI	V5.2.0 build 140721	2560*1920	√	√
	DS-2CD8153F-E	V5.2.0 build 140721	1600*1200	√	√
	DS-2CD8464F-EI	V5.2.0 build 140721	1280*960	√	√
	DS-2CD852MF-E	V2.0 build 110614	1600*1200	√	√
		V2.0 build 110426			
		V2.0 build 100521			
	DS-2CD855F-E	V5.2.0 build 140721	1920*1080	√	√
	DS-2CD862MF-E	V2.0 build 110614	1280*960	√	√
		V2.0 build 110426			
		V2.0 build 100521			
	DS-2CD863PF/NF-E	V5.2.0 build 140721	1280*960	√	√
	DS-2CD864FWD-E	V5.2.0 build 140721	1280*720	√	√
	DS-2CD876MF/BF-E	V4.0.3 build120913	1600*1200	√	√
	DS-2CD877BF	V4.0.3 build120913	1920*1080	√	√
	DS-2CD886MF-E	V4.0.3 build 120913	2560*1920	√	√

Type	Model	Version	Max. Resolution	Sub-stream	Audio
	DS-2CD966(B)	V3.1 build 120423	1360*1024	×	×
	DS-2CD966-V(B)	V3.1 build 120423	1360*1024	×	×
	DS-2CD976(C)	V3.1 build 120423	1600*1200	×	×
	DS-2CD976-V(C)	V3.1 build 120423	1600*1200	×	×
	DS-2CD977(C)	V3.1 build 120423	1920*1080	×	×
	DS-2CD986A(C)	V3.1 build 120423	2448*2048	×	×
	DS-2CD986C（B）	V2.3.6 build 120401	2560*1920	×	×
HD Network Camera	DS-2CD9122	V3.7.1 build140417	1920*1080	√	×
	DS-2CD9152	V3.7.1 build140417	2560*1920	√	×
	iDS-2CD9152	V3.7.1 build140417	2560*1920	√	×
	DS-2CD9122-H	V3.7.1 build140417	1920*1080	√	×
	DS-2CD9182-H	V3.8.1 build140815	3296*2472	√	×
	DS-2CD9121	V3.7.1 build140417	1600*1200	√	×
	iDS-2CD9121	V3.7.1 build140417	1600*1200	√	×
	DS-2CD9131	V4.0.0 build150213	2048*1536	√	×
	iDS-2CD9131	V4.0.0 build150213	2048*1536	√	×
	DS-2CD9121A	V3.8.2 build141121	1600*1200	√	×
	iDS-2CD9121A	V3.8.2 build141121	1600*1200	√	×
	DS-2CD9111(B)	V3.7.1 build140417	1360*1024	√	×
	DS-2CD9151A	V3.8.2 build141121	2448*2048	√	×
	DS-2CD9152-H	V3.8.2 build141121	2592*2048	√	×
	iDS-2CD9282	V3.8.2 build141121	3296*2472	√	×
	DS-2CD9131-K	V4.0.0 build150213	2048*1536	√	√
	DS-2CD9152-HK	V3.8.2 build141121	2592*2048	√	√
	iDS-2CD9131-E	V3.8.2 build141121	2048*1536	√	×
	iDS-2CD9151A-E	V3.8.2 build141121	2448*2048	√	×
	iDS-2CD9151A	V3.8.2 build141121	2448*2048	√	×
	iDS-2CD9152-EH	V3.8.2 build141121	2592*2048	√	×
	iDS-2CD9152-H	V3.8.2 build141121	2592*2048	√	×
	DS-2CD9120-H	V3.7.1 build140417	1600*1200	√	×

Type	Model	Version	Max. Resolution	Sub-stream	Audio
	iDS-2CD9361	V4.0.0 build150213	2752*2208	√	×
	iDS-2CD9022	V4.0.0 build150213	1920*1080	√	√
	iDS-2CD9025	V3.8.2 build141114	1920*1080	√	×
	iDS-2CD9022-SZ	V4.0.0 build150213	1920*1080	√	×
	DS-2CD9125-KS	V3.8.1 build150113	1920*1080	√	×
SD Encoder	DS-6501HCI	V1.0.1 build130607	352*288	√	√
	DS-6501HCI-SATA	V1.0.1 build130607	352*288	√	√
	DS-6501HFI	V1.0.1 build130607	704*576	√	√
	DS-6501HFI- SATA	V1.0.1 build130607	704*576	√	√
	DS-6502HCI	V1.0.1 build130607	352*288	√	√
	DS-6502HCI- SATA	V1.0.1 build130607	352*288	√	√
	DS-6502HFI	V1.0.1 build130607	704*576	√	√
	DS-6502HFI- SATA	V1.0.1 build130607	704*576	√	√
	DS-6504HCI	V1.0.1 build130607	352*288	√	√
	DS-6504HCI- SATA	V1.0.1 build130607	352*288	√	√
	DS-6504HFI	V1.0.1 build130607	704*576	√	√
	DS-6504HFI- SATA	V1.0.1 build130607	704*576	√	√
	DS-6508HCI	V1.0.1 build130607	352*288	√	√
	DS-6508HCI- SATA	V1.0.1 build130607	352*288	√	√
	DS-6508HFI	V1.0.1 build130607	704*576	√	√
	DS-6508HFI- SATA	V1.0.1 build130607	704*576	√	√
	DS-6516HCI	V1.0.1 build130607	352*288	√	√
	DS-6516HCI- SATA	V1.0.1 build130607	352*288	√	√
	DS-6516HFI	V1.0.1 build130607	704*576	√	√
	DS-6516HFI- SATA	V1.0.1 build130607	704*576	√	√
	DS-6601HCI	V1.2.1 build131202	352*288	√	√
	DS-6602HCI	V1.2.1 build131202	352*288	√	√
	DS-6604HCI	V1.2.1 build131202	352*288	√	√
	DS-6601HFI(-SATA)	V1.2.1 build131202	704*576	√	√
	DS-6602HFI(SATA)	V1.2.1 build131202	704*576	√	√

Type	Model	Version	Max. Resolution	Sub-stream	Audio
	DS-6604HFI(-SATA)	V1.2.1 build131202	704*576	√	√
	DS-6701HWI	V1.2.3 build141202	960*576	√	√
	DS-6701HWI-SATA	V1.2.3 build141202	960*576	√	√
	DS-6704HWI	V1.2.3 build141202	960*576	√	√
	DS-6704HWI-SATA	V1.2.3 build141202	960*576	√	√
	DS-6708HWI	V1.2.3 build141202	960*576	√	√
	DS-6708HWI-SATA	V1.2.3 build141202	960*576	√	√
	DS-6716HWI	V1.2.3 build141202	960*576	√	√
	DS-6716HWI-SATA	V1.2.3 build141202	960*576	√	√
HD Encoder	DS-6601HFHI	V1.1.0 build150123	1920*1080	√	√
	DS-6601HFHI/L	V1.1.0 build150123	1920*1080	√	√
Network Speed Dome	DS-2DF7274-A/D/AF	V5.2.8 build150124	1280*960	√	√
	iDS-2DF7274-A/D/AF	V5.2.8 build150124	1280*960	√	√
	DS-2DM7274-A	V5.2.8 build150124	1280*960	√	√
	DS-2DF5274-A/D/A3/D3/AF/A3F	V5.2.8 build150124	1280*960	√	√
	iDS-2DF5274-A/D/A3/D3/AF/A3F	V5.2.8 build150124	1280*960	√	√
	DS-2DM5274-A/A3	V5.2.8 build150124	1280*960	√	√
	DS-2DF7276-A/D/AF	V5.2.8 build150124	1280*960	√	√
	iDS-2DF7276-A/D/AF	V5.2.8 build150124	1280*960	√	√
	DS-2DF5276-A/D/A3/D3/AF/A3F	V5.2.8 build150124	1280*960	√	√
	iDS-2DF5276-A/D/A3/D3/AF/A3F	V5.2.8 build150124	1280*960	√	√
	DS-2DF7274-AH/DH/AFH	V5.2.8 build150124	1280*960	√	√
	iDS-2DF7274-AH/DH/AFH	V5.2.8 build150124	1280*960	√	√
	DS-2DF5274-AH/DH/A3H/D3H/AFH/A3FH	V5.2.8 build150124	1280*960	√	√
	iDS-2DF5274-AH/DH/A3H/D3H/AFH/A3FH	V5.2.8 build150124	1280*960	√	√
	DS-2DF7276-AH/DH/AFH	V5.2.8 build150124	1280*960	√	√
	iDS-2DF7276-AH/DH/AFH	V5.2.8 build150124	1280*960	√	√

Type	Model	Version	Max. Resolution	Sub-stream	Audio
	DS-2DF5276-AH/DH/A3H/D3H/AFH/A3FH	V5.2.8 build150124	1280*960	√	√
	iDS-2DF5276-AH/DH/A3H/D3H/AFH/A3FH	V5.2.8 build150124	1280*960	√	√
	DS_2DF7130I5-AW	V5.2.8 build150124	1280*960	√	√
	DS-2DF7285-AH	V5.2.8 build150124	1920*1080	√	√
	DS-2DF5285-AH	V5.2.8 build150124	1920*1080	√	√
	DS-2DF7294-A/D/AF	V5.2.8 build150124	2048*1536	√	√
	iDS-2DF7294-A/D/AF	V5.2.8 build150124	2048*1536	√	√
	DS-2DF5294-A/D/A3/D3/AF/A3F	V5.2.8 build150124	2048*1536	√	√
	iDS-2DF5294-A/D/A3/D3/AF/A3F	V5.2.8 build150124	2048*1536	√	√
	DS-2DF7296-A/D/AF	V5.2.8 build150124	2048*1536	√	√
	iDS-2DF7296-A/D/AF	V5.2.8 build150124	2048*1536	√	√
	DS-2DF5296-A/D/A3/D3/AF/A3F	V5.2.8 build150124	2048*1536	√	√
	iDS-2DF5296-A/D/A3/D3/AF/A3F	V5.2.8 build150124	2048*1536	√	√
	DS-2DF6223-A	V5.2.8 build150124	1920*1080	√	√
	iDS-2DF6223-A	V5.2.8 build150124	1920*1080	√	√
	DS-2DF8223i-A	V5.2.8 build150124	1920*1080	√	√
	iDS-2DF8223i-A	V5.2.8 build150124	1920*1080	√	√
	DS-2DF7284-A/D/AF	V5.2.8 build150124	1920*1080	√	√
	iDS-2DF7284-A/D/AF	V5.2.8 build150124	1920*1080	√	√
	DS-2DF7286-A/D/AF	V5.2.8 build150124	1920*1080	√	√
	iDS-2DF7286-A/D/AF	V5.2.8 build150124	1920*1080	√	√
	DS-2DF5284-A/D/A3/D3/AF/A3F	V5.2.8 build150124	1920*1080	√	√
	iDS-2DF5284-A/D/A3/D3/AF/A3F	V5.2.8 build150124	1920*1080	√	√
	DS-2DF5286-A/D/A3/D3/AF/A3F	V5.2.8 build150124	1920*1080	√	√

Type	Model	Version	Max. Resolution	Sub-stream	Audio
	iDS-2DF5286-A/D/A3/D3/AF/A3F	V5.2.8 build150124	1920*1080	√	√
	DS_2DF7230I5-AW	V5.2.8 build150124	1920*1080	√	√
	DS-2AF7220-A/D	V5.2.8 build150124	1920*1080	√	√
	DS-2AF7230-A/D	V5.2.8 build150124	1920*1080	√	√
	DS-2AF5220-A/D	V5.2.8 build150124	1920*1080	√	√
	DS-2AF5230-A/D	V5.2.8 build150124	1920*1080	√	√
	iDS-2DF5220S-D4/JY	V5.2.8 build150124	1920*1080	√	√
	DS-2DF7268-A	V5.2.8 build150124	704*576	√	√
	DS-2DF5268-A	V5.2.8 build150124	704*576	√	√
	DS-2DF7264-A	V5.2.8 build150124	704*576	√	√
	DS-2DF5264-A	V5.2.8 build150124	704*576	√	√
	DS-2DE5172-A/A3	V5.2.10 build150128	1280*960	√	√
	DS-2DE5174-A/AE/AE3/A3/D/D3	V5.2.10 build150128	1280*960	√	√
	DS-2DE5176-A/AE	V5.2.10 build150128	1280*960	√	√
	DS-2DE7172-A	V5.2.10 build150128	1280*960	√	√
	DS-2DE7174-A/AE/D	V5.2.10 build150128	1280*960	√	√
	DS-2DE7176-A/AE	V5.2.10 build150128	1280*960	√	√
	DS-2DE7120i-A/AE	V5.2.10 build150128	1280*960	√	√
	DS-2DM7130i-A	V5.2.10 build150128	1280*960	√	√
	DS-2DM4120-A	V5.2.10 build150128	1280*960	√	√
	DS-2DE5120I-A	V5.2.10 build150128	1280*960	√	√
	DS-2DM5120-A	V5.2.10 build150128	1280*960	√	√
	DS-2DM5130-A	V5.2.10 build150128	1280*960	√	√
	DS-2DE2103-DE3/W	V5.2.10 build150128	1280*960	√	√
	DS-2DE2103I-DE3/W	V5.2.10 build150128	1280*960	√	√
	DS-2DE7184-A/AE/D	V5.2.10 build150128	1920*1080	√	√
	DS-2DE5182-A/A3	V5.2.10 build150128	1920*1080	√	√
	DS-2DE5184-A/AE/AE3/A3/D/D3	V5.2.10 build150128	1920*1080	√	√

Type	Model	Version	Max. Resolution	Sub-stream	Audio
	DS-2DE5186-A/AE	V5.2.10 build150128	1920*1080	√	√
	DS-2DE7182-A	V5.2.10 build150128	1920*1080	√	√
	DS-2DE4582-A	V5.2.10 build150128	1920*1080	√	√
	DS-2DE4220-A	V5.2.10 build150128	1920*1080	√	√
	DS-2DE4182-A	V5.2.10 build150128	1920*1080	√	√
	DS-2DM7230i-A	V5.2.10 build150128	1920*1080	√	√
	DS-2DM7220i-A	V5.2.10 build150128	1920*1080	√	√
	DS-2DE7186-A/AE	V5.2.10 build150128	1920*1080	√	√
	DS-2DE5220I-A	V5.2.10 build150128	1920*1080	√	√
	DS-2DM5220-A	V5.2.10 build150128	1920*1080	√	√
	DS-2DM5230-A	V5.2.10 build150128	1920*1080	√	√
	DS-2DE2202-DE3/W	V5.2.10 build150128	1920*1080	√	√
	DS-2DE2202I-DE3/W	V5.2.10 build150128	1920*1080	√	√
	DS-2DE4572-A	V5.2.10 build150128	1280*720	√	√
	DS-2DE4172-A	V5.2.10 build150128	1280*720	√	√
	DS-2DE7194-A/A3	V5.2.10 build150128	2048*1536	√	√
	DS-2DE5194-A/A3	V5.2.10 build150128	2048*1536	√	√
	DS-2DF1-518	V3.2.0 build131223	704*576	√	√
	DS-2DM1-718	V3.2.0 build131223	704*576	√	√
	DS-2DM1-518	V3.2.0 build131223	704*576	√	√
	DS-2DF1-718	V3.2.0 build131223	704*576	√	√
	DS-2DF1-514	V3.2.0 build131223	704*576	√	√
	DS-2DF1-714	V3.2.0 build131223	704*576	√	√
	DS-2DY9174-A	V5.2.8 build150124	1280*960	√	√
	DS-2DY9176-A	V5.2.8 build150124	1280*960	√	√
	DS-2DY9194-A	V5.2.8 build150124	2048*1536	√	√
	DS-2DY9196-A	V5.2.8 build150124	2048*1536	√	√
	DS-2DY9184-A	V5.2.8 build150124	1920*1080	√	√
	DS-2DY9186-A	V5.2.8 build150124	1920*1080	√	√
	DS-2DY9185-A	V5.2.8 build150124	1920*1080	√	√

Type	Model	Version	Max. Resolution	Sub-stream	Audio
	DS-2DY9187-A	V5.2.8 build150124	1920*1080	√	√
	DS-2DF8223IV-A	V5.3.0 build150304	1920*1080	√	√
	DS-2DF8623IV-A	V5.3.0 build150304	3072*1728	√	√
	DS-2DF6623V-A	V5.3.0 build150304	3072*1728	√	√
	DS-2DF8823IV-A	V5.3.0 build150304	4096*2160	√	√
Network Zoom Camera Module	DS-2ZCN2006	V5.2.7 build141107	1280*960	√	√
	DS-2ZCN2006(B)	V5.2.7 build141107	1280*960	√	√
	DS-2ZCN3006	V5.2.7 build141107	1280*960	√	√
	DS-2ZCN3006(B)	V5.2.7 build141107	1280*960	√	√
	DS-2ZMN2006	V5.2.7 build141107	1280*960	√	√
	DS-2ZMN2006(B)	V5.2.7 build141107	1280*960	√	√
	DS-2ZMN3006	V5.2.7 build141107	1280*960	√	√
	DS-2ZMN3006(B)	V5.2.7 build141107	1280*960	√	√
	DS-2ZCN2007	V5.2.7 build141107	1920*1080	√	√
	DS-2ZCN3007	V5.2.7 build141107	1920*1080	√	√
	DS-2ZCN3007(B)	V5.2.7 build141107	1920*1080	√	√
	DS-2ZMN2007	V5.2.7 build141107	1920*1080	√	√
	DS-2ZMN3007	V5.2.7 build141107	1920*1080	√	√
	DS-2ZMN3007(B)	V5.2.7 build141107	1920*1080	√	√
	DS-2ZMN0407	V5.2.7 build141107	1920*1080	√	√
	DS-2ZMN3207	V5.2.7 build141107	1920*1080	√	√
	DS-2ZMN2008	V5.2.7 build141107	2048*1536	√	√
	DS-2ZCN2008	V5.2.7 build141107	2048*1536	√	√
	DS-2ZMN3007(S)	V5.2.2 build141113	1920*1080	√	√
	DS-2ZCN3007(S)	V5.2.2 build141113	1920*1080	√	√
	DS-2ZMN2307	V5.2.2 build141113	1920*1080	√	√
	DS-2CN2307	V5.2.2 build141113	1920*1080	√	√
	DS-2ZMN2309	V5.2.2 build141113	3072*2048	√	√
	DS-2ZCN2309	V5.2.2 build141113	3072*2048	√	√

16.4.2 List of Third-party IP Cameras

NOTE

ONVIF compatibility refers to the camera can be supported both when it uses the ONVIF protocol and its private protocols. **Only ONVIF is supported** refers to the camera can only be supported when it uses the ONVIF protocol. **Only AXIS is supported** refers to the function can only be supported when it uses the AXIS protocol.

IP Camera Manufacturer or Protocol	Model	Version	Max. Resolution	Sub-stream	Audio
ACTi	ACM3401-09L-X-00227	A1D-220-V3.13.16-AC	1208*1024	×	×
	TCM4301-10D-X-00083	A1D-310-V4.12.09-AC	1208*1024	×	√
	TCM5311-11D-X-00023	A1D-310-V4.12.09-AC	1208*960	×	√
Arecont	AV1305 M	65175	1208*1024	√	×
	AV2815	65220	1920*1080	√	×
	AV3105M	65175	1920*1080	√	×
	AV8185DN	65172	1600*1200	×	×
Axis	M1114	5.09.1	1024*640	√	×
	M3011(ONVIF compatibility)	5.21	640*480 (704*576)	√ (×)	×
	M3014(ONVIF compatibility)	5.21.1	1280*800	√	×
	P1346	5.40.9.2	2048*1536	√	√
	P3301(ONVIF compatibility)	5.11.2	640*480 (768*576)	√	√ (×)
	P3304(ONVIF compatibility)	5.20	1280*800 (1440*900)	√	√ (×)
	P3343(ONVIF compatibility)	5.20.1	800*600	√	√ (×)
	P3344(ONVIF compatibility)	5.20.1	1280*800 (1440*900)	√	√ (×)
	P5532	5.15	720*576	√	×
	Q7404	5.02	720*576	√	√
Bosch	AutoDome Jr 800 HD (ONVIF compatibility)	39500450	1920*1080	×	√ (×)
	Dinion NBN-921-P (ONVIF compatibility)	10500453	1280*720	×	√ (×)

	NBC 265 P (ONVIF compatibility)	07500452	1280*720	×	√ (×)
Brickcom	CB-500Ap(Brickcom-50xA) (ONVIF compatibility)	v3.2.1.3	1920*1080	×	√ (×)
Canon	VB-H410(ONVIF compatibility)	Ver.+1.0.0	1920*1080 (1280*960)	×	√
	VB-S9000F	Ver. 1.0.0	1920*1080	×	×
	VB-S300D	Ver. 1.0.0	1920*1080	×	×
	VB-H6100D	Ver. 1.0.0	1920*1080	×	×
	VB-H7100F	Ver. 1.0.0	1920*1080	×	√
	VB-S8000	Ver. 1.0.0	1920*1080	×	×
Panasonic	SP306H (ONVIF compatibility)	Application:1.34 Image data:1.06	1280*960	√ (×)	√
	SF336H	Application:1.06 Image data: 1.06	1280*960	√	√
Pelco	D5118 (ONVIF compatibility)	1.8.2-20120327-2.9310-A1.7852	1280*960	√	×
	IX30DN-ACFZHB3 (ONVIF compatibility)	1.8.2-20120327-2.9080-A1.7852	2048*1536	√	×
	IXE20DN-AAXVUU2 (ONVIF compatibility)	1.8.2-20120327-2.9081-A1.7852	1920*1080	√	×
Sanyo	2300P(with lens)	2.03-02 (110318-00)	1920*1080	×	×
	2500P(with lens)	2.02-02 (110208-00)	1920*1080	×	√
	4600P	2.03-02 (110315-00)	1920*1080	×	√
SONY	SNC-CH220	1.50.00	1920*1080	×	×
	SNCDH220T (ONVIF only)	1.50.00	2048*1536	×	×
	SNC-EP580 (ONVIF compatibility)	1.53.00	1920*1080	√	√

	SNC-RH124 (ONVIF compatibility)	1.79.00	1280*720	√	√
SUMSUNG	SND-5080 (ONVIF compatibility)	3.10_130416	1280*1024	√	√
Vivotek	IP7133	0203a	640*480	×	×
	FD8134 (ONVIF compatibility)	0107a	1280*800	×	×
	IP8161 (ONVIF compatibility)	0104a	1600*1200	×	√ (×)
	IP8331 (ONVIF compatibility)	0102a	640*480	×	×
	IP8332 (ONVIF compatibility)	0105b	1280*800	×	×
Zavio	D5110 (ONVIF compatibility)	MG.1.6.03P8	1280*1024	√ (×)	×
	F3106 (ONVIF compatibility)	M2.1.6.03P8	1280*1024	√ (×)	√
	F3110 (ONVIF compatibility)	M2.1.6.01	1280*720	√ (×)	√
	F3206 (ONVIF compatibility)	MG.1.6.02c045	1920*1080	√ (×)	√
	F531E (ONVIF compatibility)	LM.1.6.18P10	640*480	√ (×)	√

0304931070518

First Choice for Security Professionals

www.hikvision.com