

***HIKVISION***



# Network Video Recorder

## User Manual

UD04701B

## **User Manual**

COPYRIGHT ©2016 Hangzhou Hikvision Digital Technology Co., Ltd.

### **ALL RIGHTS RESERVED.**

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

### **About this Manual**

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

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

Please use this user manual under the guidance of professionals.

### **Trademarks Acknowledgement**

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

### **Legal Disclaimer**

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

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

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

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

## Regulatory Information

### FCC Information

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



This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, the LVD Directive 2014/35/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](http://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](http://www.recyclethis.info)

### Industry Canada ICES-003 Compliance

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

## **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 manufacturer.



## Applicable Models

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

Series	Models
DS-7600NI-E1/E2 series	DS-7604NI-E1, DS-7608NI-E1, DS-7616NI-E1
	DS-7604NI-E1/4P
	DS-7604NI-E1/4N
	DS-7608NI-E2, DS-7616NI-E2, DS-7632NI-E2
	DS-7608NI-E2/8P, DS-7616NI-E2/8P, DS-7616NI-E2/16P, DS-7632NI-E2/8P
	DS-7608NI-E2/8N, DS-7616NI-E2/8N, DS-7632NI-E2/8N
DS-7700NI-E4 series	DS-7708NI-E4, DS-7716NI-E4, DS-7732NI-E4
	DS-7708NI-E4/8P, DS-7716NI-E4/16P, DS-7732NI-E4/16P
DS-8600NI-E8 series	DS-8608NI-E8, DS-8616NI-E8, DS-8632NI-E8

## Symbol Conventions

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

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

# Product Key Features

## General

- Connectable to network cameras, network dome and encoders.
- Connectable to the third-party network cameras like ACTI, Arecont, AXIS, Bosch, Brickcom, Canon, PANASONIC, Pelco, SAMSUNG, SANYO, SONY, Vivotek and ZAVIO, and cameras that adopt ONVIF or PSIA protocol.
- Connectable to the smart IP cameras.
- PAL/NTSC adaptive video inputs.
- Supports H.264/H.264+ video streams.
- Each channel supports dual-stream.
- Up to 32 network cameras can be connected for DS-8600NI-E8, DS-7700NI-E4 and DS-7600NI-E2 series NVR; 16 network cameras for other DS-7600NI 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

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



The PTZ control is supported by the DS-8600NI-E8 and DS-7700NI-E4 series NVR only.

## HDD Management

- For DS-8600NI-E8 series, 8 SATA hard disks can be connected;  
For DS-7700NI-E4 series, 4 SATA hard disks can be connected;  
For DS-7600NI-E2 series, 2 SATA hard disks can be connected;  
For DS-7600NI-E1 series, 1 SATA hard disk can be connected;
- Each disk with a maximum of 6TB storage capacity for the DS-8600NI-E8, DS-7700NI-E4, DS-7600-E1 (E2) series NVR.
- 8 network disks (NAS /IP SAN disks) can be connected.
- Supports S.M.A.R.T. and bad sector detection.
- HDD group management.
- Supports HDD standby function.
- HDD property: redundancy, read-only, read/write (R/W).
- HDD quota management; different capacity can be assigned to different channel.

## Recording and Playback

- Holiday recording schedule configuration.
- Continuous and event video recording parameters.
- Multiple recording types: manual, continuous, alarm, motion, motion | alarm, motion & alarm, and VCA.
- 8 recording time periods with separated recording types each day.
- Pre-record and post-record for alarm, motion detection for recording, and pre-record time for schedule and manual recording.
- Searching record files by events (alarm input/motion detection/VCA).
- Playback by sub-periods.
- Tag adding for record files, searching and playing back by tags.
- Locking and unlocking record files.
- Local redundant recording.
- Provides new playback interface with easy and flexible operation.
- Searching and playing back record files by camera No., recording type, start time, end time, etc.
- Smart search for the selected area in the video.
- Zooming in when playback.
- Reverse playback of multi-channel.
- Supports pause, play reverse, speed up, speed down, skip forward, and skip backward when playback, and locating by dragging the mouse.
- Supports thumbnails view and fast view during playback.
- Supports playback by transcoded stream.
- Up to 4/8/16-ch synchronous playback.
- Supports enabling H.264+ to ensure high video quality with lowered bitrate.

### **Backup**

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

### **Alarm and Exception**

- Configurable arming time of alarm input/output.
- Alarm for video loss, motion detection, VCA, video tampering, HDD full, HDD error, network disconnected, IP conflict, illegal login, abnormal record, and PoE power overload (for the models supports PoE interfaces only), etc.
- Alarm triggers full screen monitoring, audio alarm, notifying surveillance center, sending email and alarm output.
- Automatic restore when system is abnormal.
- Supports VCA detection alarm and VCA search.
- VCA alarm message push via iVMS-4500 mobile client software.

### **Other Local Functions**

- Operable by front panel (depends on model), mouse, and remote control.
- Three-level user management; admin user is allowed to create many operating accounts and define their operating permission, which includes the limit to access any channel.
- 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**

- The dual-NIC network 10 /100/1000 Mbps self-adaptive Ethernet interfaces are provided for the DS-8600NI-E8 and DS-7700NI-E4 series NVR; one 10 /100 Mbps self-adaptive Ethernet interface for DS-7604/7608NI-E1(E2) series NVR; and one 10 /100/1000 Mbps self-adaptive Ethernet interface for other models.
- 1 self-adaptive 10M/100M/1000M network interfaces are provided for other models.
- 4 independent PoE network interfaces are provided for DS-7600NI-E1/P series.
- Up to 8 independent PoE network interfaces are provided for DS-7600NI-E2/P series.
- Up to 16 independent PoE network interfaces are provided for DS-7700NI-E4/P series.
- 4 independent built-in switch network interfaces are provided for DS-7600NI-E1/N series.
- Up to 8 independent built-in switch network interfaces are provided for DS-7600NI-E2/N series;
- IPv6 is supported.
- TCP/IP protocol, DHCP, DNS, DDNS, NTP, SADP, SMTP, NFS, and iSCSI are supported.
- TCP, UDP and RTP for unicast.
- Auto/Manual port mapping by UPnP™.
- Supports access by Hik-Connect.
- Remote reverse playback via RTSP.
- Supports accessing by the platform via ONVIF.
- Remote search, playback, download, locking and unlocking of the record files, and the breakpoint resume is supported for downloading files.
- Remote parameters setup; remote import/export of device parameters.
- Remote viewing of the device status, system logs and alarm status.
- Remote keyboard operation.
- Remote locking and unlocking of control panel and mouse.
- Remote HDD formatting and program upgrading.
- Remote system restart and shutdown.
- RS-232, RS-485 transparent channel transmission (depending on models).
- Alarm and exception information can be sent to the remote host
- Remotely start/stop recording.
- Remotely start/stop alarm output.
- Remote PTZ control (depending on models).
- Remote JPEG capture.
- Two-way audio and voice broadcasting.
- Embedded WEB server.
- Upgrade by FTP server.

**Development Scalability:**

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



# TABLE OF CONTENTS

<b>Product Key Features .....</b>	<b>5</b>
<b>Chapter 1 Introduction .....</b>	<b>13</b>
1.1 Front Panel .....	14
DS-8600NI-E8 Series.....	14
DS-7700NI-E4 Series.....	16
DS-7600NI-E1(E2) Series .....	18
1.2 IR Remote Control Operations .....	19
1.2 USB Mouse Operation .....	22
1.3 Input Method Description.....	23
1.4 Rear Panel .....	24
DS-8600NI-E8, DS-7700NI-E4 and DS-7700NI-E4/P Series .....	24
DS-7600NI-E1, DS-7600NI-E1/4N, DS-7600NI-E2 and DS-7600NI-E2/8N Series.....	25
DS-7600NI-E1/4P and DS-7600NI-E2/8P Series .....	25
<b>Chapter 2 Getting Started .....</b>	<b>27</b>
2.1 Device Startup and Activation.....	28
2.1.1 Starting Up and Shutting Down the NVR.....	28
2.1.2 Activating Your Device.....	30
2.1.3 Using the Unlock Pattern for Login.....	31
2.1.4 Login and Logout .....	34
2.1.5 Resetting Your Password .....	36
2.2 Using the Wizard for Basic Configuration.....	36
2.3 Adding and Connecting the IP Cameras .....	41
2.3.1 Activating the IP Camera.....	41
2.3.2 Adding the Online IP Cameras .....	42
2.3.3 Editing the Connected IP Cameras and Configuring Customized Protocols.....	46
2.3.4 Editing IP Cameras Connected to the PoE Interfaces .....	48
<b>Chapter 3 Live View.....</b>	<b>51</b>
3.1 Introduction of Live View .....	52
3.2 Operations in Live View Mode.....	53
3.2.1 Front Panel Operation on Live View.....	53
3.2.2 Using the Mouse in Live View .....	53
3.2.3 Quick Setting Toolbar in Live View Mode .....	54
3.3 Adjusting Live View Settings.....	56
3.4 Channel-zero Encoding.....	58
<b>Chapter 4 PTZ Controls .....</b>	<b>60</b>
4.1 Configuring PTZ Settings.....	61
4.2 Setting PTZ Presets, Patrols & Patterns.....	63
4.2.1 Customizing Presets.....	63
4.2.2 Calling Presets .....	63
4.2.3 Customizing Patrols.....	64
4.2.4 Calling Patrols .....	65
4.2.5 Customizing Patterns .....	66

4.2.6	Calling Patterns.....	66
4.2.7	Customizing Linear Scan Limit .....	67
4.2.8	Calling Linear Scan .....	68
4.2.9	One-touch Park.....	68
4.3	PTZ Control Panel.....	70
<b>Chapter 5</b>	<b>Recording Settings.....</b>	<b>71</b>
5.1	Configuring Parameters.....	72
5.2	Configuring Recording Schedule .....	75
5.3	Configuring Motion Detection Recording.....	78
5.4	Configuring Alarm Triggered Recording.....	80
5.5	Configuring VCA Event Recording.....	82
5.6	Manual Recording .....	83
5.7	Configuring Holiday Recording .....	84
5.8	Configuring Redundant Recording.....	85
5.9	Configuring HDD Group for Recording.....	87
5.10	Files Protection.....	88
5.10.1	Locking the Recording Files.....	88
5.10.2	Setting HDD Property to Read-only .....	90
<b>Chapter 6</b>	<b>Playback.....</b>	<b>92</b>
6.1	Playing Back Record Files .....	93
6.1.1	Instant Playback.....	93
6.1.2	Playing Back by Normal Search .....	93
6.1.3	Playing back by Smart Search .....	96
6.1.4	Playing Back by Event Search.....	98
6.1.5	Playing Back by Tag .....	99
6.1.6	Playing Back by System Logs .....	102
6.1.7	Playing Back External File .....	103
6.1.8	Playing Back by Sub-periods.....	104
6.2	Auxiliary Functions of Playback .....	105
6.2.1	Playing Back Frame by Frame.....	105
6.2.2	Thumbnails View .....	106
6.2.3	Fast View .....	106
6.2.4	Digital Zoom.....	107
6.2.5	File Management .....	108
<b>Chapter 7</b>	<b>Backup .....</b>	<b>109</b>
7.1	Backing up Record Files .....	110
7.1.1	Quick Export.....	110
7.1.2	Backing up by Normal Video Search.....	112
7.1.3	Backing up by Event Search .....	114
7.1.4	Backing up Video Clips .....	115
7.2	Managing Backup Devices.....	116
<b>Chapter 8</b>	<b>Alarm Settings.....</b>	<b>117</b>
8.1	Setting Motion Detection Alarm.....	118
8.2	Setting Sensor Alarms .....	120

8.3	Detecting Video Loss Alarm.....	123
8.4	Detecting Video Tampering Alarm .....	125
8.5	Handling Exceptions Alarm.....	127
8.6	Setting Alarm Response Actions .....	128
8.7	Triggering or Clearing Alarm Output Manually .....	131
<b>Chapter 9</b>	<b>VCA Alarm.....</b>	<b>132</b>
9.1	Face Detection .....	133
9.2	Vehicle Detection .....	135
9.3	Line Crossing Detection .....	137
9.4	Intrusion Detection .....	139
9.5	Region Entrance Detection.....	141
9.6	Region Exiting Detection .....	142
9.7	Unattended Baggage Detection .....	142
9.8	Object Removal Detection.....	142
9.9	Audio Exception Detection .....	143
9.10	Sudden Scene Change Detection .....	143
9.11	Defocus Detection .....	144
9.12	PIR Alarm .....	144
<b>Chapter 10</b>	<b>VCA Search .....</b>	<b>145</b>
10.1	Face Search .....	146
10.2	Behavior Search .....	148
10.3	Plate Search .....	149
10.4	People Counting .....	150
10.5	Heat Map .....	152
<b>Chapter 11</b>	<b>Network Settings .....</b>	<b>153</b>
11.1	Configuring General Settings .....	154
11.2	Configuring Advanced Settings.....	156
11.2.1	Configuring Hik-Connect .....	156
11.2.2	Configuring DDNS .....	158
11.2.3	Configuring NTP Server .....	159
11.2.4	Configuring SNMP .....	160
11.2.5	Configuring More Settings .....	161
11.2.6	Configuring HTTPS Port .....	162
11.2.7	Configuring Email .....	164
11.2.8	Configuring NAT .....	165
11.2.9	Configuring Virtual Host .....	168
11.3	Checking Network Traffic .....	170
11.4	Configuring Network Detection .....	171
11.4.1	Testing Network Delay and Packet Loss.....	171
11.4.2	Exporting Network Packet.....	171
11.4.3	Checking the Network Status.....	172
11.4.4	Checking Network Statistics.....	173
<b>Chapter 12</b>	<b>HDD Management.....</b>	<b>175</b>
12.1	Initializing HDDs .....	176

12.2	Managing Network HDD .....	178
12.3	Managing HDD Group .....	181
12.3.1	Setting HDD Groups.....	181
12.3.2	Setting HDD Property.....	182
12.4	Configuring Quota Mode.....	184
12.5	Checking HDD Status .....	185
12.6	HDD Detection.....	186
12.7	Configuring HDD Error Alarms .....	188
<b>Chapter 13</b>	<b>Camera Settings .....</b>	<b>189</b>
13.1	Configuring OSD Settings.....	190
13.2	Configuring Privacy Mask.....	191
13.3	Configuring Video Parameters .....	192
<b>Chapter 14</b>	<b>NVR Management and Maintenance .....</b>	<b>193</b>
14.1	Viewing System Information.....	194
14.2	Searching & Export Log Files .....	195
14.3	Importing/Exporting IP Camera Info .....	198
14.4	Importing/Exporting Configuration Files .....	199
14.5	Upgrading System .....	200
14.5.1	Upgrading by Local Backup Device .....	200
14.5.2	Upgrading by FTP .....	200
14.6	Restoring Default Settings.....	202
<b>Chapter 15</b>	<b>Others.....</b>	<b>203</b>
15.1	Configuring RS-232 Serial Port.....	204
15.2	Configuring General Settings .....	205
15.3	Configuring DST Settings .....	207
15.4	Configuring More Settings for Device Parameters .....	208
15.5	Managing User Accounts.....	209
15.5.1	Adding a User .....	209
15.5.2	Deleting a User .....	211
15.5.3	Editing a User .....	212
<b>Chapter 16</b>	<b>Appendix .....</b>	<b>215</b>
16.1	Specifications .....	216
	DS-7600NI-E1 .....	216
	DS-7600NI-E2 .....	217
	DS-7700NI-E4/P.....	218
	DS-7700NI-E4 .....	219
	DS-8600NI-E8 .....	220
	DS-7604NI-E1/4N and DS-7608NI-E2/8N.....	221
	DS-7600NI-E2/N .....	222
	DS-7604NI-E1/4P and DS-7608NI-E2/8P.....	223
	DS-7600NI-E2/P.....	224
16.2	Glossary.....	225
16.3	Troubleshooting.....	226
16.4	Summary of Changes .....	233

16.5	List of Compatible IP Cameras.....	236
16.5.1	List of Hikvision IP Cameras.....	236
16.5.2	List of Third-party IP Cameras .....	243

# **Chapter 1 Introduction**

# 1.1 Front Panel

## DS-8600NI-E8 Series

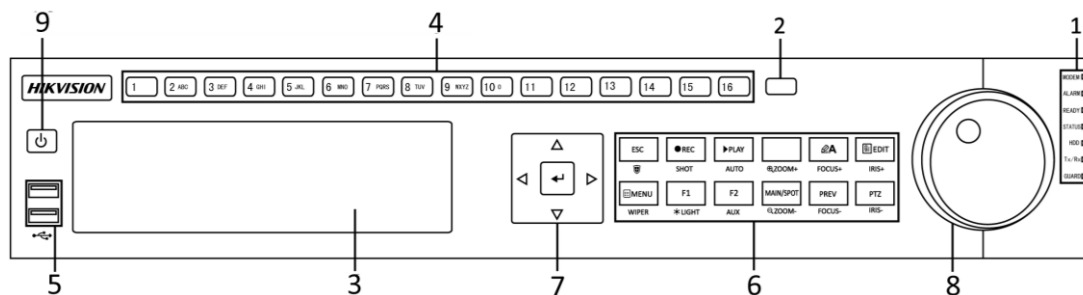


Figure 1. 1 DS-8600NI-E8 Series

Table 1. 1 Description of Control Panel Buttons

No.	Name	Function Description
1	Status Indicators	<b>ALARM</b> Turns red when a sensor alarm is detected.
		<b>READY</b> Turns blue when the device is functioning properly.
		<b>STATUS</b> Turns blue when device is controlled by an IR remote. Turns red when controlled by a keyboard and purple when IR remote and keyboard is used at the same time.
		<b>HDD</b> Flickers red when data is being read from or written to HDD.
		<b>MODEM</b> Reserved for future usage.
		<b>Tx/Rx</b> Flickers blue when network connection is functioning properly.
		<b>GUARD</b> Turns blue when the device is in armed status; at this time, an alarm is enabled when an event is detected. Turns off when the device is unarmed. The arm/disarm status can be changed by pressing and holding on the ESC button for more than 3 seconds in live view mode.
2	IR Receiver	Receiver for IR remote
3	DVD-R/W	Slot for DVD-R/W.
4	Alphanumeric Buttons	Switches to the corresponding channel in live view or PTZ control mode.
		Inputs numbers and characters in edit mode.
		Switches between different channels in playback mode.
		Turns blue when the corresponding channel is recording; turns red when the channel is in network transmission status; turns pink when the channel is recording and transmitting.
5	USB Interfaces	Universal Serial Bus (USB) ports for additional devices such as USB mouse and USB Hard Disk Drive (HDD).
6	Composite Keys	<b>ESC</b> Returns to the previous menu. Presses for arming/disarming the device in live view mode.
		<b>REC/SHOT</b> Enters the Manual Record settings menu. Presses this button followed by a numeric button to call a PTZ preset in PTZ control settings. Turns audio on/off in the playback mode.
		<b>PLAY/AUTO</b> Enters the playback mode.

No.	Name	Function Description
		Automatically scans in the PTZ control menu.
		<b>ZOOM+</b> Zooms in the PTZ camera in the PTZ control setting.
		<b>A/FOCUS+</b> Adjusts focus in the PTZ Control menu.
		Switches between input methods (upper and lower case alphabet, symbols and numeric input).
		<b>EDIT/IRIS+</b> Edits text fields. When editing text fields, it also deletes the character in front of the cursor.
		Checks the checkbox in the checkbox fields.
		Adjusts the iris of the camera in PTZ control mode.
		Generates video clips for backup in playback mode.
		Enters/exits the folder of USB device and eSATA HDD.
		<b>MAIN/SPOT/ZOOM-</b> Switches between main and spot output.
		Zooms out the image in PTZ control mode.
		<b>F1/ LIGHT</b> Selects all items on the list when used in a list field.
		Turns on/off PTZ light (if applicable) in PTZ control mode.
		Switches between play and reverse play in playback mode.
		<b>F2/ AUX</b> Cycles through tab pages.
		Switches between channels in synchronous playback mode.
		<b>MENU/WIPER</b> Returns to the Main menu (after successful login).
		Presses and holds the button for five seconds to turn off audible key beep.
		Starts wiper (if applicable) in PTZ control mode.
		Shows/hides the control interface in playback mode.
		<b>PREV/FOCUS-</b> Switches between single screen and multi-screen mode.
		Adjusts the focus in conjunction with the A/FOCUS+ button in PTZ control mode.
		<b>PTZ/IRIS-</b> Enters the PTZ Control mode.
		Adjusts the iris of the PTZ camera in PTZ control mode.
7	Control Buttons	<b>DIRECTION</b> Navigates between different fields and items in menus.
		In the playback mode, use the Up and Down buttons to speed up and slow down recorded video. Use the Left and Right buttons to select the next and previous video files.
		Cycles through channels in live view mode.
		Controls the movement of the PTZ camera in PTZ control mode.
		<b>ENTER</b> Confirms selection in any of the menu modes.
		Checks the checkbox fields.
		Plays or pauses the video playing in playback mode.
		Advances the video by a single frame in single-frame playback mode.
8	JOG SHUTTLE Control	Stops/starts auto switch in auto-switch mode.
		Moves the active selection up and down in a menu.
		Cycles through different channels in live view mode.
		Jumps 30s forward/backward in video files in the playback mode.
9	POWER ON/OFF	Controls the movement of the PTZ camera in PTZ control mode.
		Power on/off switch.



## DS-7700NI-E4 Series

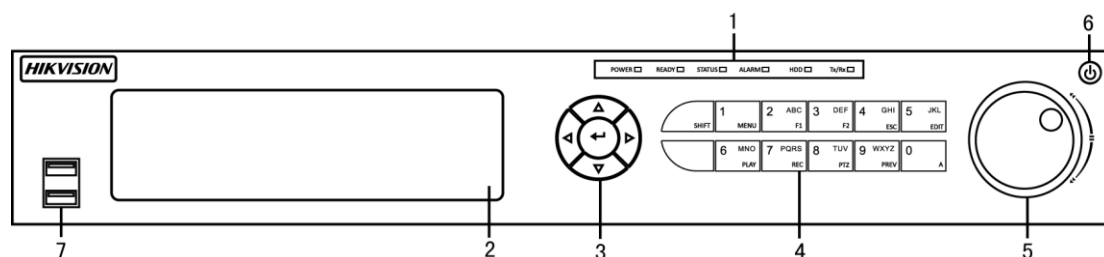


Figure 1.2 DS-7700NI-E4 Series

Table 1.2 Description of Control Panel Buttons

No.	Name	Function Description
1	Status Indicators	<b>POWER</b> Turns green when NVR is powered up.
		<b>READY</b> Turns green when the device is running normally.
		<b>STATUS</b> Turns green when the IR remote control is enabled; Turns red when the function of the composite keys (SHIFT) are used.
		<b>ALARM</b> Turns red when there is an alarm occurring.
		<b>HDD</b> Flickers red when HDD is reading/writing.
		<b>Tx/Rx</b> Flickers green when network connection is functioning normally.
2	DVD-R/W	Slot for DVD-R/W.
3	Control Buttons	<b>DIRECTION</b> Navigates between different fields and items in menus. In the playback mode, use the Up and Down buttons to speed up and slow down recorded video. Use the Left and Right buttons to select the next and previous video files. Cycles through channels in live view mode.
		<b>ENTER</b> Confirms selection in any of the menu modes. Checks the checkbox fields. Plays or pauses the video playing in playback mode. Advances the video by a single frame in single-frame playback mode.
4	Composite Keys	<b>SHIFT</b> Switches between the numeric or letter input and functions of the composite keys. (Input letter or numbers when the light is out; Realize functions when the light is red.)
		<b>1/MENU</b> Enters numeral “1”; Accesses the main menu interface.
		<b>2/ABC/F1</b> Enters numeral “2”; Enters letters “ABC”;
		Uses the F1 button in a list field to select all items.

No.	Name		Function Description
			In PTZ Control mode, turns on/off PTZ light and when the image is zoomed in, use it to zoom out.
		3/DEF/F2	Enters numeral “3”;
			Enters letters “DEF”;
			Uses the F2 button to change the tab pages.
			Zooms in the image in PTZ control mode.
		4/GHI/ESC	Enters numeral “4”;
			Enters letters “GHI”;
			Exits and back to the previous menu.
		5/JKL/EDIT	Enter numeral “5”;
			Enter letters “JKL”;
			Deletes characters before cursor;
			Checks the checkbox and selects the ON/OFF switch;
			Starts/stops record clipping in playback.
		6/MNO/PLAY	Enters numeral “6”;
			Enters letters “MNO”;
			Directly accesses to playback interface.
		7/PQRS/REC	Enters numeral “7”;
			Enters letters “PQRS”;
			Enters the manual record interface.
		8/TUV/PTZ	Enters numeral “8”;
			Enters letters “TUV”;
			Accesses PTZ control interface.
		9/WXYZ/PRE V	Enters numeral “9”;
			Enters letters “WXYZ”;
			Multi-channel display in live view.
		0/A	Enters numeral “0”;
			Shifts the input methods in the editing text field. (Upper and lowercase, alphabet, symbols or numeric input).
			Double presses the button to switch the main and auxiliary output.
		5	JOG SHUTTLE Control
Cycles through different channels in Live View mode.			
Jumps 30s forward/backward in video files in the Playback mode.			
Controls the movement of the PTZ camera in PTZ control mode.			
6	POWER ON/OFF		Power on/off switch.
7	USB Interfaces		Universal Serial Bus (USB) ports for additional devices such as USB mouse and USB Hard Disk Drive (HDD).

## DS-7600NI-E1(E2) Series

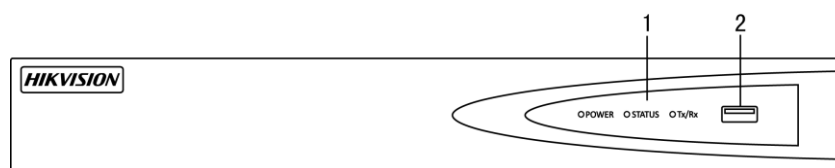


Figure 1. 3 DS-7600NI-E1(E2) Series

Table 1. 3 Description of Control Panel Buttons

No.	Name		Description
1	Status Indicator	Power	Turns green when system is running.
		Status	Flickers red when data is being read from or written to HDD.
		Tx/Rx	Flickers green when network connection is functioning properly.
2	USB Interface		Universal Serial Bus (USB) ports for additional devices such as USB mouse and USB Hard Disk Drive (HDD).

## 1.2 IR Remote Control Operations

The NVR may also be controlled with the included IR remote control, shown in Figure 1. 4.



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:

### Pairing (Enabling) the IR Remote to a Specific DVR (optional)

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

On the DVR:

1. Go to General > More Settings.
2. Type a number (255 digits maximum) into the Device No. field.
3. On the IR Remote:
4. Press the DEV button.
5. Use the Number buttons to enter the Device ID# that was entered into the DVR.
6. Press Enter button to accept the new Device ID#.

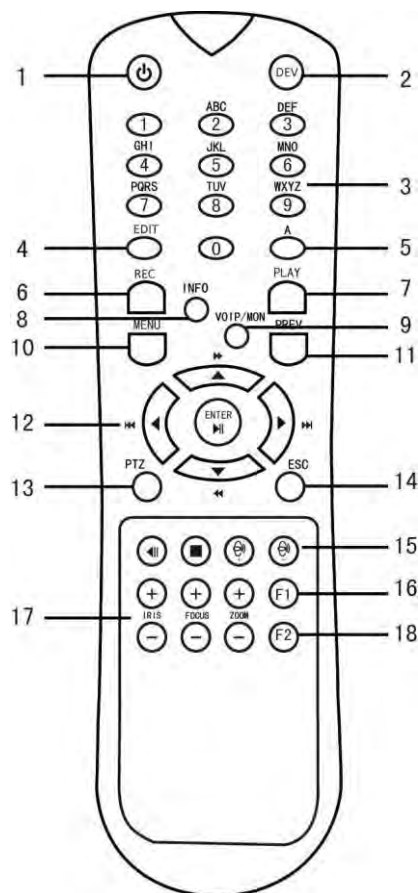


Figure 1. 4 Remote Control

## - Unpairing (Disabling) an IR Remote from a DVR

To unpair an IR Remote from a DVR so that the unit cannot control any DVR 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 DVR.



(Re)-enabling the IR Remote requires pairing to a DVR. See “Pairing the IR Remote to a Specific DVR (optional),” above.

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

Table 1. 4 IR Remote Functions

No.	Name	Function Description
1	POWER ON/OFF	<ul style="list-style-type: none"> <li>• <b>To Turn Power On:</b> <ul style="list-style-type: none"> <li>- <b>If User Has Not Changed the Default DVR Device ID# (255):</b> <ol style="list-style-type: none"> <li>1. Press <b>Power On/Off</b> button (1).</li> </ol> </li> <li>- <b>If User Has Changed the DVR Device ID#:</b> <ol style="list-style-type: none"> <li>1. Press <b>DEV</b> button.</li> <li>2. Press <b>Number</b> buttons to enter user-defined Device ID#.</li> <li>3. Press <b>Enter</b> button.</li> <li>4. Press <b>Power</b> button to start device.</li> </ol> </li> </ul> </li> <li>• <b>To Turn DVR Off:</b> <ul style="list-style-type: none"> <li>- <b>If User Is Logged On:</b> <ol style="list-style-type: none"> <li>1. Hold <b>Power On/Off</b> button (1) down for five seconds to display the “Yes/No” verification prompt.</li> <li>2. Use <b>Up/Down Arrow</b> buttons (12) to highlight desired selection.</li> <li>3. Press <b>Enter</b> button (12) to accept selection.</li> </ol> </li> <li>- <b>If User Is Not Logged On:</b> <ol style="list-style-type: none"> <li>1. Hold <b>Power On/Off</b> button (1) down for five seconds to display the user name/password prompt.</li> <li>2. Press the <b>Enter</b> button (12) to display the on-screen keyboard.</li> <li>3. Input the user name.</li> <li>4. Press the <b>Enter</b> button (12) to accept input and dismiss the on-screen keyboard.</li> <li>5. Use the <b>Down Arrow</b> button (12) to move to the “Password” field.</li> <li>6. Input password (use on-screen keyboard or numeric buttons (3) for numbers).</li> <li>7. Press the <b>Enter</b> button (12) to accept input and dismiss the on-screen keyboard.</li> <li>8. Press the <b>OK</b> button on the screen to accept input and display the Yes/No” verification prompt (use <b>Up/Down Arrow</b> buttons (12) to move between fields)</li> <li>9. Press <b>Enter</b> button (12) to accept selection.</li> </ol> </li> </ul> </li> </ul> <p> User name/password prompt depends on DVR is configuration. See “System Configuration” section.</p>
2	DEV	Enable IR Remote: Press DEV button, enter DVR Device ID# with number keys, press Enter to pair unit with the DVR Disable IR Remote: Press DEV button to clear Device ID#; unit will no longer be paired with the DVR
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 Confirm selection in any menu mode
	ENTER	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

**Troubleshooting Remote Control:**

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

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

**Steps:**

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

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

1. Batteries are installed correctly and the polarities of the batteries are not reversed.
2. Batteries are fresh and not out of charge.
3. IR receiver is not obstructed.
4. 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.

## 1.2 USB Mouse Operation

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

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

The operation of the mouse:

Table 1. 5 Description of the Mouse Control

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

## 1.3 Input Method Description

Refer to the following figures for the soft keyboard:



Figure 1.1 Soft Keyboard (1)



Figure 1.2 Soft Keyboard (2)



Figure 1.3 Soft Keyboard (3)

Description of the buttons on the soft keyboard:

Table 1.6 Description of the Soft Keyboard Icons

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



## 1.4 Rear Panel



The rear panel varies according to different models.

### DS-8600NI-E8, DS-7700NI-E4 and DS-7700NI-E4/P Series

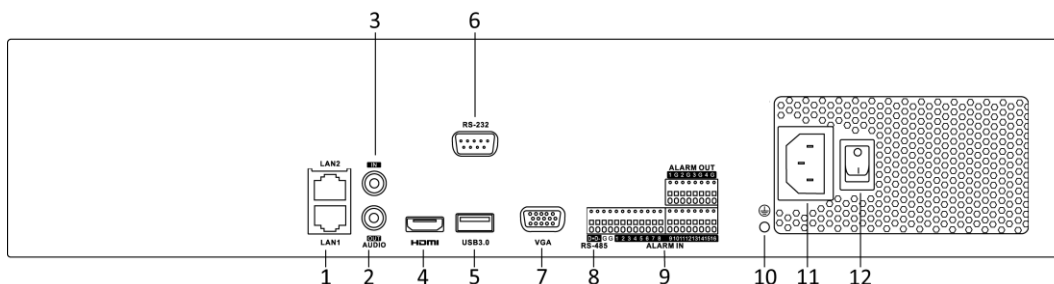


Figure 1.5 DS-8600NI-E8 and DS-7700NI-E4 Series

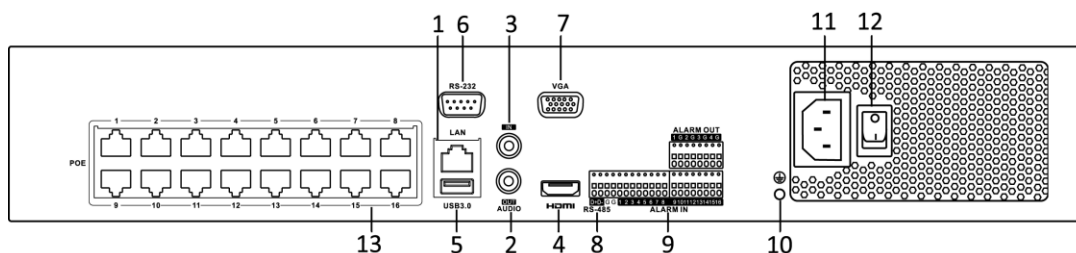


Figure 1.6 DS-7700NI-E4/P Series

Table 1.7 Description of Rear Panel Interfaces

No.	Item	Description
1	LAN Interface	1 network interface provided for DS-7700NI-E4/P and 2 network interfaces for DS-7700NI-E4 and DS-8600NI-E8.
2	AUDIO OUT	RCA connector for audio output.
3	LINE IN	RCA connector for audio input.
4	HDMI™	HDMI™ video output connector.
5	USB 3.0 interface	Universal Serial Bus (USB) ports for additional devices such as USB mouse and USB Hard Disk Drive (HDD).
6	RS-232 Interface	Connector for RS-232 devices.
7	VGA	DB9 connector for VGA output. Display local video output and menu.
8	RS-485 Interface	Half-duplex connector for RS-485 devices.
9	ALARM IN	Connector for alarm input.
	ALARM OUT	Connector for alarm output.
10	GROUND	Ground (needs to be connected when NVR starts up).
11	AC 100V ~ 240V	100 to 240 VAC power supply.
12	Power Switch	Switch for turning on/off the device.
13	Network Interfaces with PoE function (supported by DS-7700NI-E4/P)	Network interfaces for the cameras and to provide power over Ethernet.

## DS-7600NI-E1, DS-7600NI-E1/4N, DS-7600NI-E2 and DS-7600NI-E2/8N Series

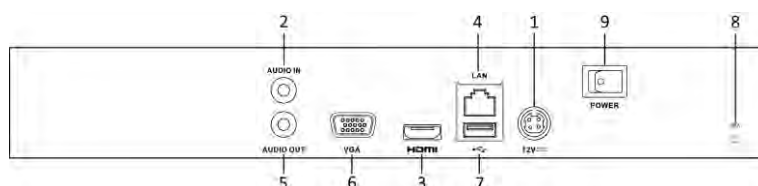


Figure 1. 7 DS-7600NI-E1/E2 Series

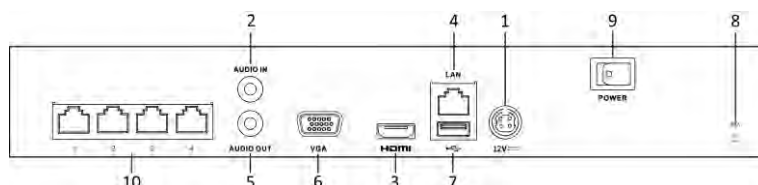


Figure 1. 8 DS-7600NI-E1/4N Series

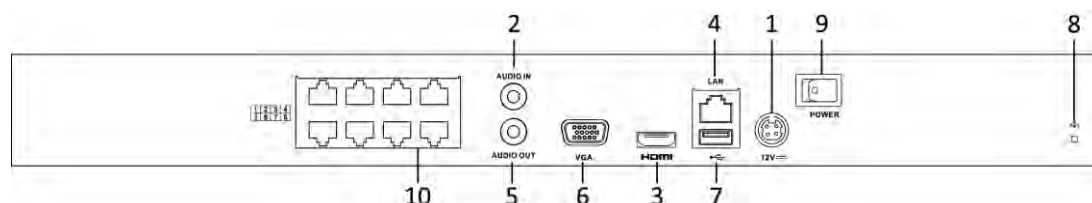


Figure 1. 9 DS-7600NI-E2/8N Series

Table 1. 8 Description of Rear Panel Interfaces

No.	Item	Description
1	Power Supply	DC 12V power supply.
2	Audio In	RCA connector for audio input.
3	HDMI™ Interface	HDMI™ video output connector.
4	LAN Network Interface	1 10 /100 /1000 Mbps self-adaptive Ethernet interface
5	Audio Out	RCA connector for audio output.
6	VGA Interface	DB9 connector for VGA output. Display local video output and menu.
7	USB Interface	Universal Serial Bus (USB) ports for additional devices such as USB mouse and USB Hard Disk Drive (HDD).
8	Ground	Ground (needs to be connected when NVR starts up).
9	Power Switch	Switch for turning on/off the device.
10	Network Interfaces with built-in switch function	Built-in switch network interfaces for the cameras. (Supported by DS-7600NI-E1/4N and DS-7600NI-E2/8N).

## DS-7600NI-E1/4P and DS-7600NI-E2/8P Series

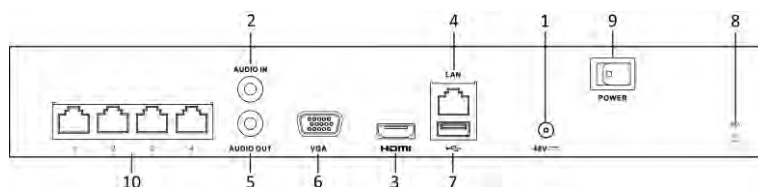


Figure 1. 10 DS-7600NI-E1/4P Series

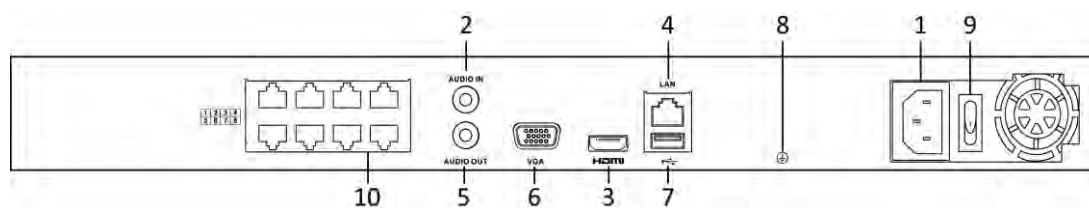


Figure 1. 11 DS-7600NI-E2/8P Series

Table 1. 9 Description of Rear Panel Interfaces

No.	Item	Description
1	<b>Power Supply</b>	48 VDC power supply for DS-7600NI-E1/4P and 100~240 VAC for DS-7600NI-E2/8P.
2	<b>Audio In</b>	RCA connector for audio input.
3	<b>HDMI™ Interface</b>	HDMI™ video output connector.
4	<b>LAN Network Interface</b>	One 10 /100 /1000 Mbps self-adaptive Ethernet interface
5	<b>Audio Out</b>	RCA connector for audio output.
6	<b>VGA Interface</b>	DB9 connector for VGA output. Display local video output and menu.
7	<b>USB Interface</b>	Universal Serial Bus (USB) ports for additional devices such as USB mouse and USB Hard Disk Drive (HDD).
8	<b>Ground</b>	Ground (needs to be connected when NVR starts up).
9	<b>Power Switch</b>	Switch for turning on/off the device.
10	<b>Network Interfaces with PoE function</b>	Network interfaces for the cameras and to provide power over Ethernet.

## **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 the NVR:**

**Steps:**

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

**Shutting down the NVR**

There are two proper ways to shut down the NVR.

● **OPTION 1: By Standard shutdown**

**Steps:**

1. Enter the Shutdown menu.  
Menu > Shutdown



Figure 2. 1 Shutdown Menu

2. Click the **Shutdown** button.
3. Click the **Yes** button.
4. For the DS-7600NI-E1 (E2) series, turn off the power switch on the rear panel when the attention pops up.

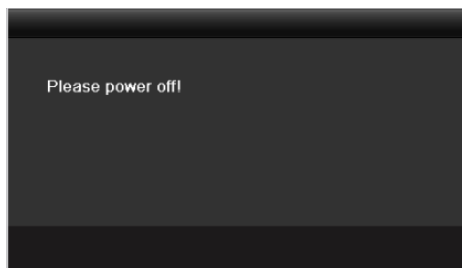



Figure 2. 2 Shutdown Attention


---

- **OPTION 2: By operating the front panel (supported by DS-8600NI-E8 and DS-7700NI-E4(/P) series)**

*Steps:*

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



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

### **Rebooting the NVR**

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

*Steps:*

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

## 2.1.2 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.

### **Steps:**

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

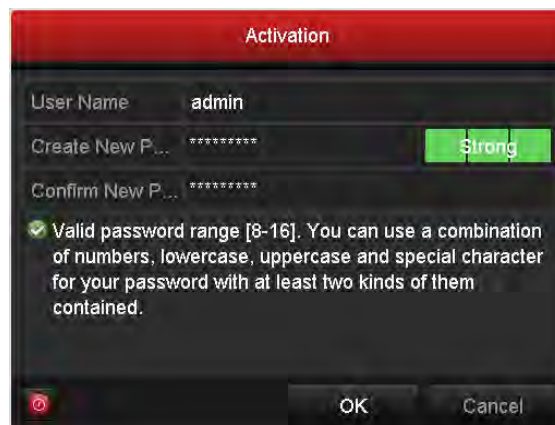


Figure 2. 3 Settings Admin Password

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

2. Click **OK** to save the password and activate the device.
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. 4 Export GUIDE File Remind

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 Chapter 2.1.5 Resetting Your Password for the instructions of password resetting.



Figure 2. 5 Export GUIDE File



Please keep your GUID file properly for future password resetting.

5. When the device is activated, the system pops up the message box to remind you to remember the password.



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

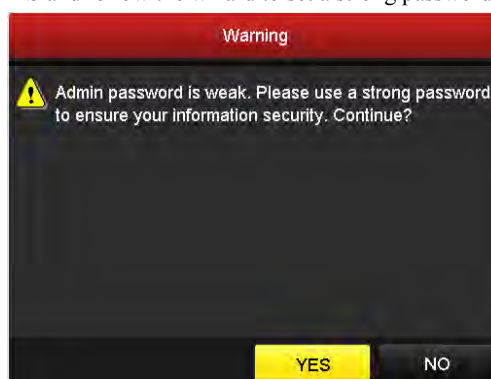


Figure 2. 6 Warning

## 2.1.3 Using the Unlock Pattern for Login

You can configure the unlock pattern for device login.

### Configuring the Unlock Pattern

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



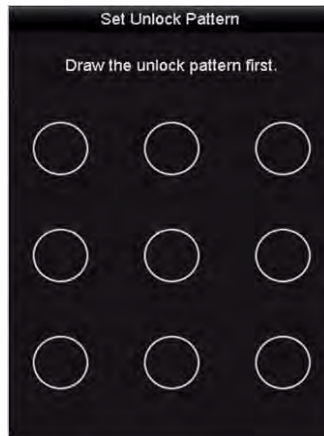


Figure 2. 7 Set Unlock Pattern

---

**Steps:**

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

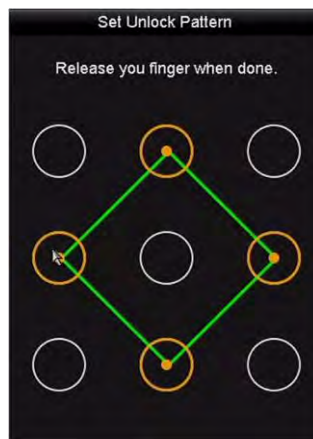


Figure 2. 8 Draw the Pattern



- Connect at least 4 dots to draw the pattern.
  - Each dot can be connected for once only.
2. Draw the same pattern again to confirm it. When the two patterns match, the pattern is configured successfully.

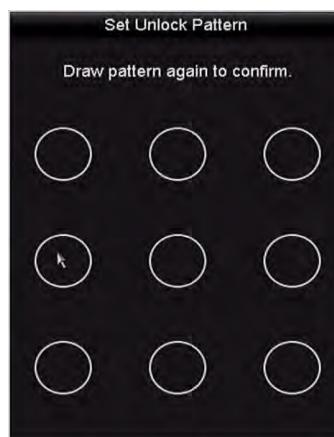


Figure 2. 9 Confirm the Pattern



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

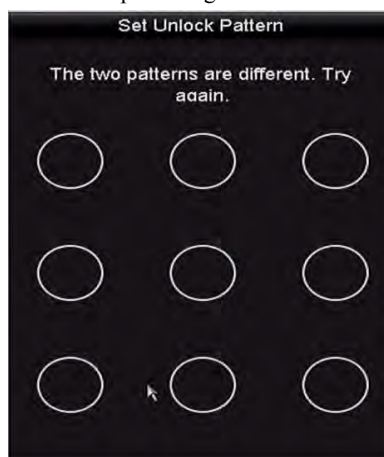


Figure 2. 10 Re-set the Pattern

## Logging in via Unlock Pattern



- 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

### Steps:

1. Right click the mouse on the screen and select the menu to enter the interface as shown in Figure 2.8.



Figure 2. 11 Draw the Unlock Pattern

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



- 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.

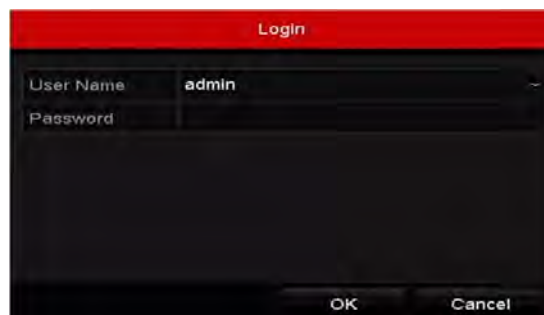


Figure 2. 12 Normal Login Dialog Box

---

## 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.

#### *Steps:*

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



Figure 2. 13 Login Interface

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



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.



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

## User Logout

### *Purpose:*

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

### *Steps:*

1. Enter the Shutdown menu.  
Menu>Shutdown



Figure 2. 14 Logout

2. Click **Logout**.



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

## 2.1.5 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).

### Steps:

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



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



Figure 2. 15 Reset Password

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



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

3. After the GUID file is successfully imported, enter the reset password interface to set the new admin password.
4. Click **OK** to set the new password. You can export the new GUID file to the U-flash disk for future password resetting.



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 the Wizard for Basic Configuration

### Purpose:

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

of the NVR.

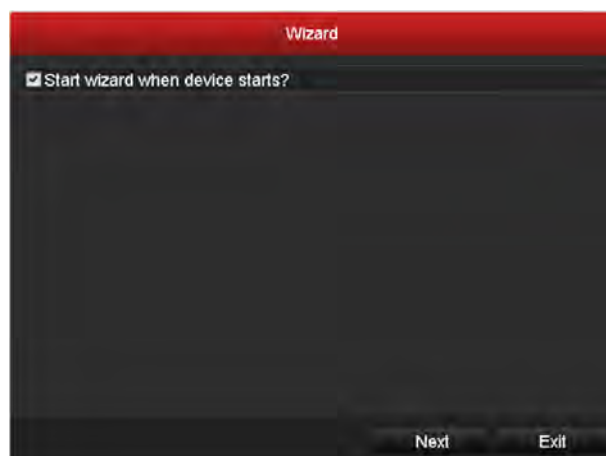


Figure 2. 16 Start Wizard Interface

---

**Steps:**

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



Figure 2. 17 Date and Time Settings

---

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

Figure 2.18 Network Settings



- The dual-NIC network 10 /100/1000 Mbps self-adaptive Ethernet interfaces are provided for the DS-8600NI-E8 and DS-7700NI-E4 series NVR; one 10 /100 Mbps self-adaptive Ethernet interface for DS-7604/7608NI-E1(E2) series NVR; and one 10 /100/1000 Mbps self-adaptive Ethernet interface for other models.
  - For the models have the PoE or built-in switch network interfaces, including DS-7600NI-E1(E2)/N, DS-7600NI-E1(E2)/P and DS-7700NI-E4/P series NVR, the internal NIC IPv4 address should be configured for the cameras connecting to the PoE or built-in switch network interface of the NVR.
4. Click **Next** button after you configured the basic network parameters. Enter the **Hik-Connect** interface to configure the parameters. Please refer to Chapter 11.2.1 Configuring Hik-Connect for detailed instructions.

Figure 2.19 Hik-Connect Parameters

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



Figure 2. 20 Advanced Network Parameters

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

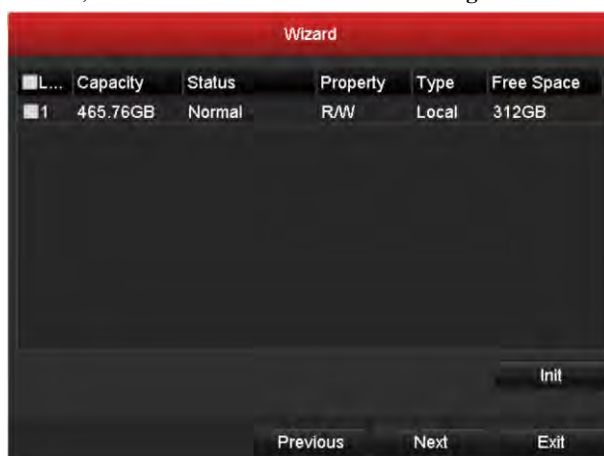


Figure 2. 21 HDD Management

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





Figure 2. 22 IP Camera Management

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



Figure 2. 23 Record Settings

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

## 2.3 Adding and Connecting the IP Cameras

### 2.3.1 Activating the IP Camera

**Purpose:**

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

**Steps:**

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

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

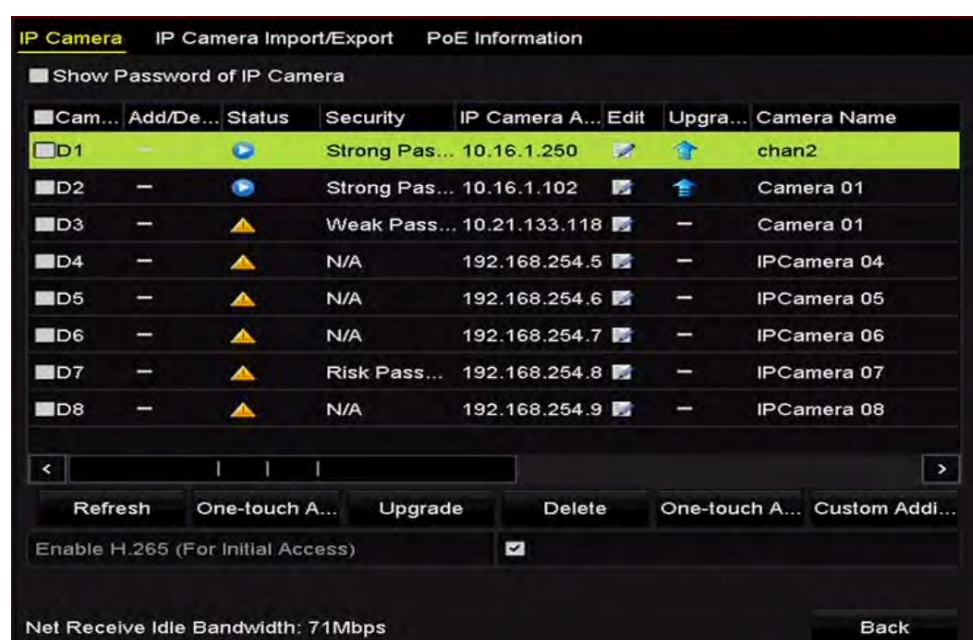


Figure 2. 24 IP Camera Management Interface

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

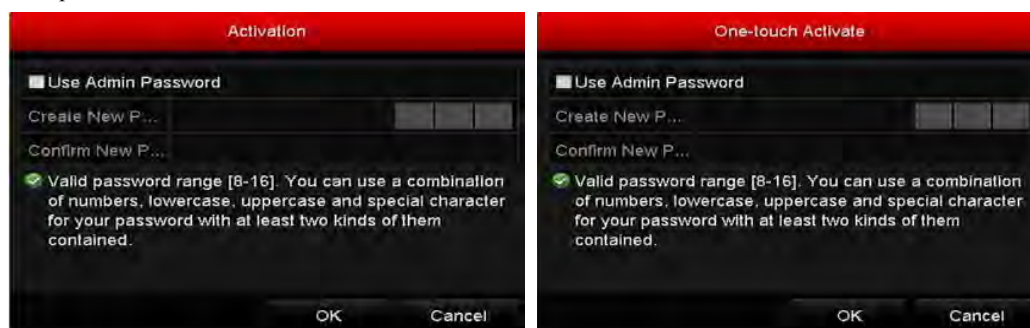


Figure 2. 25 Activate the Camera

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

**Use Admin Password:** when you check the checkbox, the camera (s) will be configured with the same

admin password of the operating NVR.



Figure 2. 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.

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

4. Click **OK** to finish the activation 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.

### **Before you start:**

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

### **Adding the IP Cameras**

#### • **OPTION 1:**

#### **Steps:**


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



Figure 2. 27 Icon of Adding IP Camera

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.

No.	IP Address	Amount of...	Device Ty...	Protocol	Managem
1	10.16.1.62	1	IPC	HIKVISION	8000
2	10.16.1.199	1	IP Dome	HIKVISION	8000

IP Camera Address	10.16.1.62
Protocol	HIKVISION
Management Port	8000
Channel Port	1
Transfer Protocol	Auto
User Name	admin
Admin Password	

Search Add Cancel

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:**

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.


Cam...	Add/De...	Status	Security	IP Camera A...	Edit	Upgra...	Camera Name
D1	—	●	Strong Pas...	10.16.1.250	✎	⬆	chan2
D2	—	●	Strong Pas...	10.16.1.102	✎	⬆	Camera 01
D3	—	▲	Weak Pass...	10.21.133.118	✎	—	Camera 01
D4	—	▲	N/A	192.168.254.5	✎	—	IPCamera 04
D5	—	▲	N/A	192.168.254.6	✎	—	IPCamera 05
D6	—	▲	N/A	192.168.254.7	✎	—	IPCamera 06
D7	—	▲	Risk Pass...	192.168.254.8	✎	—	IPCamera 07
D8	—	▲	N/A	192.168.254.9	✎	—	IPCamera 08

Refresh One-touch A... Upgrade Delete One-touch A... Custom Addi...

Enable H.265 (For Initial Access) ☒

Net Receive Idle Bandwidth: 71Mbps Back

Figure 2. 29 Adding IP Camera Interface

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



Make sure the camera to add has already been activated.

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:**

*Steps:*

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

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










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

3. (Optional) Check the checkbox of **Continue to Add** to add other IP cameras.
4. Click **Add** to add the camera. 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.	<b>Security</b>	Show the security status of the camera to be active/inactive or the password strength (strong/medium/weak/risk)



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

Cam...	Add/De...	Status	Security	IP Camera A...	Edit	Upgrade	Camera Name
D1	—		Weak Pass...	10.11.36.38			Camera 01
D2	—		Strong Pas...	10.16.1.250		—	IPdome
D3	—		N/A	192.168.254.4		—	IPCamera 03

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 Show Password of IP Camera



### 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.

**Steps:**

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



Edit IP Camera	
IP Camera No.	D1
IP Camera Address	10.16.1.2
Protocol	ONVIF
Management Port	80
Channel Port	1
Transfer Protocol	Auto
User Name	admin
Admin Password	


Protocol OK Cancel


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.

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

**To edit advanced parameters:**

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



Advance Set	
Network	Password
IP Camera No.	D3
IP Camera Address	172.6.23.124
Management Port	8000

Apply OK Cancel

Figure 2. 35 Network Configuration of the Camera

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



Figure 2.36 Password Configuration of the Camera

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

### Configuring the customized protocols

#### *Purpose:*

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

#### *Steps:*

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

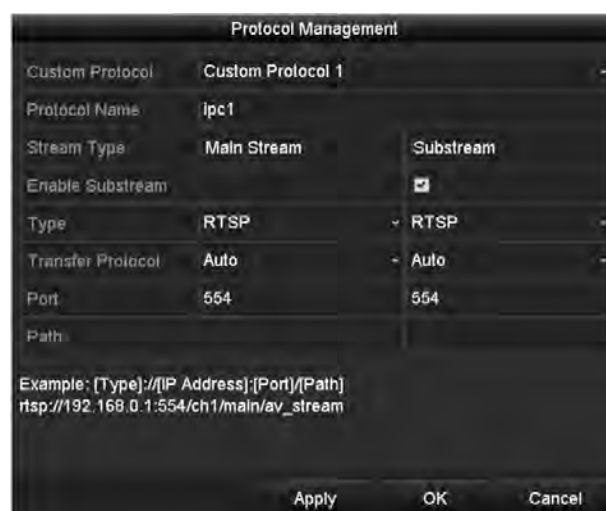


Figure 2.37 Protocol Management Interface

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

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



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

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



**Example:** rtsp://192.168.1.55:554/ch1/main/av\_stream.

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



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

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



Figure 2. 38 Protocol Setting

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

## 2.3.4 Editing IP Cameras Connected to the PoE Interfaces



This chapter is only applicable for the following models: DS-7604NI-E1/4P, DS-7600NI-E2/8P, DS-7600NI-E2/16P, DS-7700NI-E4/8P, DS-7700NI-E4/16P series NVR.

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

Up to 4 network cameras can be connected to /4P models, 8 network cameras to /8P models, and 16 network cameras to /16P models. If you disable the PoE interface, you can also connect to the online network cameras. And the PoE interface supports the Plug-and-Play function.

**To add Cameras for NVR supporting PoE function:**

**Before you start:**

Connect the network cameras via the PoE interfaces.

**Steps:**

1. Enter the Camera Management interface.

Menu&gt; Camera&gt; Camera

Cam...	Add/De...	Status	Security	IP Camera A...	Edit	Up...	Camera Name	Prot...
D1	—		Weak Pass...	10.11.36.38			Camera 01	HIK\
D2	—		Strong Pas...	10.16.1.250		—	IPdome	HIK\
D3	—		N/A	192.168.254.4		—	IPCamera 03	HIK\
D4	—		N/A	192.168.254.5		—	IPCamera 04	HIK\
D5	—		N/A	192.168.254.6		—	IPCamera 05	HIK\
D6	—		N/A	192.168.254.7		—	IPCamera 06	HIK\
D7	—		N/A	192.168.254.8		—	IPCamera 07	HIK\
D8	—		N/A	192.168.254.9		—	IPCamera 08	HIK\
...		—	Active	10.16.1.251		—	—	HIK\

Enable H.265 (For Initial Access) ☐

Figure 2. 39 List of Connected Cameras



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

- Click the button, and select the Adding Method in the drop-down list.
  - Plug-and-Play:** It means that the camera is connected to the PoE interface, so in this case, the parameters of the camera can't be edited. The IP address of the camera can only be edited in the Network Configuration interface, see *Chapter 11.1 Configuring General Settings* for detailed information.

Edit IP Camera	
IP Camera No.	D3
Adding Method	Plug-and-Play
IP Camera Address	192.168.254.4
Protocol	HIKVISION
Management Port	8000
Channel Port	1
Transfer Protocol	Auto
User Name	admin
Admin Password	
<input type="button" value="Protocol"/> <input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Figure 2. 40 Edit IP Camera Interface - Plug-and-Play

- Manual:** You can disable the PoE interface by selecting the manual while the current channel can be used as a normal channel and the parameters can also be edited.  
Input the IP address, the user name and password of administrator manually, and click **OK** to add the IP camera.



The screenshot displays a software window titled "Edit IP Camera". It contains a list of configuration fields for an IP camera. The fields and their values are as follows:

Field	Value
IP Camera No.	D1
Adding Method	Manual
IP Camera Address	172.6.23.123
Protocol	HIKVISION
Management Port	8000
Channel Port	1
Transfer Protocol	Auto
User Name	admin
Admin Password	*****

At the bottom right of the window, there are three buttons: "Protocol", "OK", and "Cancel".

Figure 2. 41 Edit IP Camera Interface - Manual

---

## **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.

### Live View Icons

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

Table 3. 1 Description of Live View Icons

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

## 3.2 Operations in Live View Mode

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

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

Menu > Configuration > Live View > Dwell Time.

- **Start Recording:** continuous record and motion detection record are supported.
- **Output Mode:** select the output mode to Standard, Bright, Gentle or Vivid.
- **Add IP Camera:** the shortcut to the IP camera management interface.
- **Playback:** playback the recorded videos for current day.
- **Aux Monitor:** the NVR checks the connection of the output interfaces to define the main and auxiliary output interfaces. The priority level for the main and aux output is HDMI > VGA  
When both the HDMI and VGA are connected, the HDMI is used as main output and the VGA is used as the aux output.

When the aux output is enabled, the main output cannot perform any operation, and you can do some basic operation on the live view mode for the Aux output.

### 3.2.1 Front Panel Operation on Live View



The front panel operation is supported by DS-8600NI-E8 and DS-7700NI-E4(P) models only.

Table 3. 2 Front Panel Operation in Live View

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

### 3.2.2 Using the Mouse in Live View

Table 3. 3 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.

Name	Description
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.
Output Mode	Four modes of output supported, including Standard, Bright, Gentle and Vivid.



- The *dwelt 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.

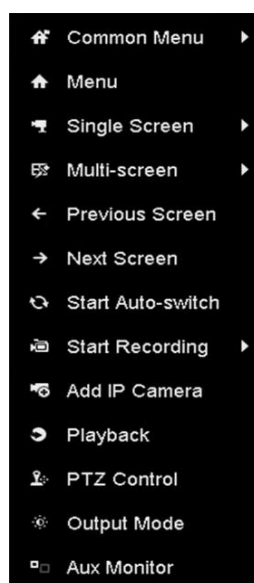


Figure 3. 1 Right-click Menu



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

### 3.2.3 Quick Setting Toolbar in Live View Mode

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



Figure 3.2 Quick Setting Toolbar

Table 3.4 Description of Quick Setting Toolbar Icons

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



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 to 16X)

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.





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.

**Steps:**

1. Enter the Live View Settings interface.

Menu > Configuration > Live View

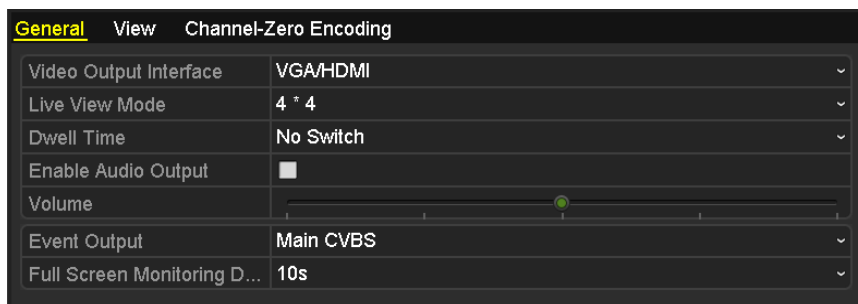


Figure 3. 7 Live View-General

The settings available in this menu include:

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


2. Setting Cameras Order





Figure 3. 8 Live View- Camera Order

- 1) Select a **View** mode in . Up to 36-screen display is supported for 32-ch NVR.

- 2) Select the small window, and double-click on the channel number to display the channel on the window.

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

You can also click  button to start live view for all the channels and click  to stop all the live view.

- 3) Click the **Apply** button to save the setting.
3. 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.

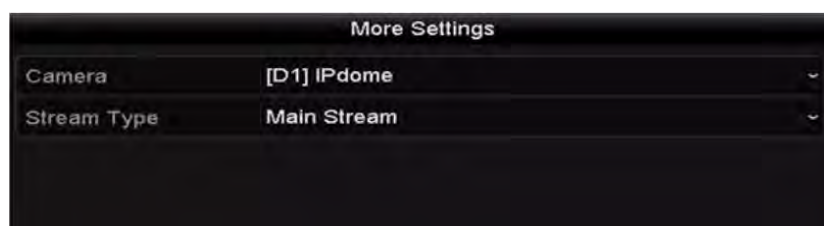


Figure 3. 9 Stream Type Settings

- 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.

### *Steps:*

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

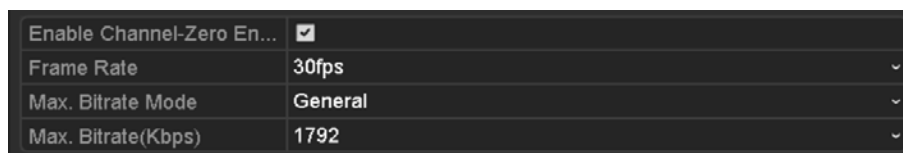


Figure 3. 10 Live View- Channel-Zero Encoding

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

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



## **Chapter 4 PTZ Controls**

## 4.1 Configuring PTZ Settings

### *Purpose:*

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

### *Steps:*

1. Enter the PTZ Settings interface.

Menu > Camera > PTZ



Figure 4. 1 PTZ Settings

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



Figure 4. 2 PTZ- General

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



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

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

## 4.2 Setting PTZ Presets, Patrols & Patterns

### *Before you start:*

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

### 4.2.1 Customizing Presets

#### *Purpose:*

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

#### *Steps:*

1. Enter the PTZ Control interface.

Menu > Camera > PTZ



Figure 4. 3 PTZ Settings

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

Repeat the steps2-3 to save more presets.

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

### 4.2.2 Calling Presets

#### *Purpose:*

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

#### *Steps:*





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



Figure 4. 4 PTZ Panel - General

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

## 4.2.3 Customizing Patrols

### *Purpose:*

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

### *Steps:*

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



Figure 4. 5 PTZ Settings

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

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



Figure 4. 6 Key point Configuration

- 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.
- Click the **Add** button to add the next key point to the patrol, and you can click the **OK** button to save the key point to the patrol.

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

## 4.2.4 Calling Patrols

### *Purpose:*

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

### *Steps:*



- 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.
- Click the  button to show the general settings of the PTZ control.



Figure 4. 7 PTZ Panel - General

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

## 4.2.5 Customizing Patterns

### *Purpose:*

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

### *Steps:*

1. Enter the PTZ Control interface.

Menu > Camera > PTZ



Figure 4. 8 PTZ Settings

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

The movement of the PTZ is recorded as the pattern.

## 4.2.6 Calling Patterns

### *Purpose:*

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

### *Steps:*



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



Figure 4. 9 PTZ Panel - General

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

## 4.2.7 Customizing Linear Scan Limit

### *Purpose:*

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



This function is supported by some certain models.

### *Steps:*

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



Figure 4. 10 PTZ Settings

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



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

## 4.2.8 Calling Linear Scan





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.

### **Steps:**

1. Click the button **PTZ** in the lower-right corner of the PTZ setting interface;  
Or press the PTZ button on the front panel or click the PTZ Control icon  in the quick setting bar to enter the PTZ setting menu in live view mode.
2. Click the  button to show the one-touch function of the PTZ control.

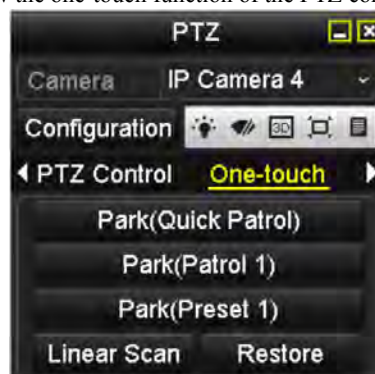


Figure 4. 11 PTZ Panel - One-touch

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

## 4.2.9 One-touch Park




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).

### **Steps:**

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

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


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



Figure 4. 12 PTZ Panel - One-touch

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

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

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

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



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

4. Click the button again to inactivate it.


## 4.3 PTZ Control Panel

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

### OPTION 1:

In the PTZ settings interface, click the **PTZ** button on the lower-right corner which is next to the Back button.

### OPTION 2:

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





















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

## **Chapter 5 Recording Settings**



## 5.1 Configuring Parameters

### Purpose:

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

### Before you start:

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



L...	Capacity	Status	Property	Type	Free Space	Gr...	Edit	D...
1	465.76GB	Normal	R/W	Local	305GB	1		-
2	931.51GB	Normal	R/W	Local	814GB	1		-

Figure 5. 1 HDD- General

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

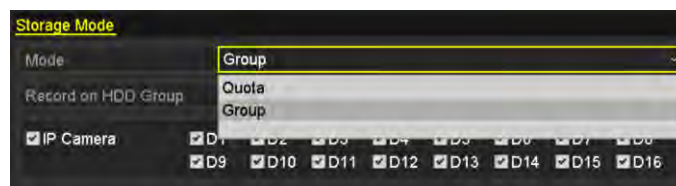


Figure 5. 2 HDD- Advanced

### Steps:

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

Menu > Record > Parameters



Figure 5. 3 Recording Parameters

## 2. Parameters Setting for Recording

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

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



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

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



Figure 5. 4 Recording Parameters-More Settings

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

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



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

### 3. Parameters Settings for Sub-stream

- 1) Enter the Sub-stream tab page.



Record	Substream
Camera	[D1] Camera 01
Stream Type	Video
Resolution (max.: 720P)	704*480(4CIF)
Bitrate Type	Variable
Video Quality	Medium
Frame Rate	Full Frame
Max. Bitrate Mode	General
Max. Bitrate (Kbps) (max,...)	1024
Max. Bitrate Range Reco...	1152~1920(Kbps)
Video Encode	H.265

Figure 5. 5 Sub-stream Parameters

---

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

## 5.2 Configuring Recording Schedule

### *Purpose:*

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

### *Steps:*

1. Enter the Record Schedule interface.

Menu > Record > Schedule

2. Configure Record Schedule

- 1) Select Record Schedule.

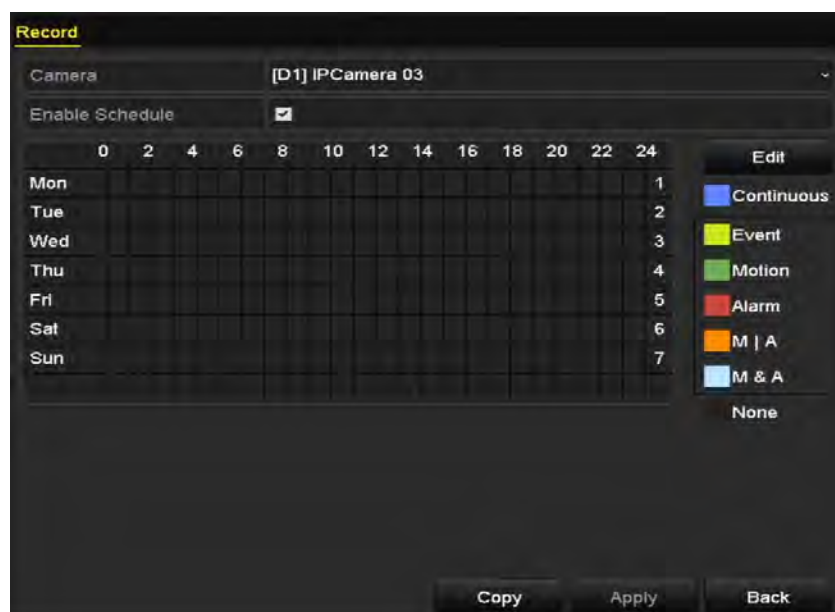


Figure 5. 6 Record Schedule

Different recording types are marked in different color icons.

**Continuous:** scheduled recording.

**Event:** recording triggered by all event triggered alarm.

**Motion:** recording triggered by motion detection.

**Alarm:** recording triggered by alarm.

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

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

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

### **Edit the schedule:**

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

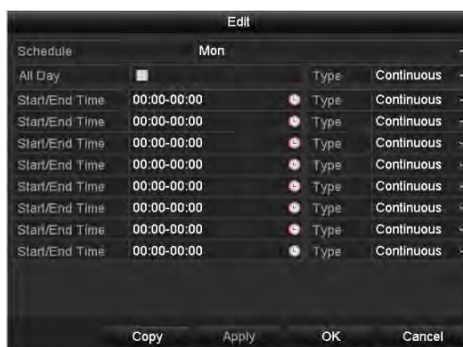



Figure 5.7 Recording Schedule Interface

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

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

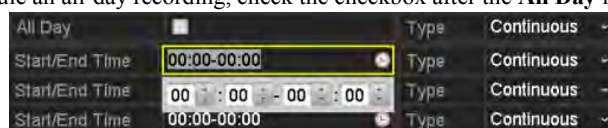


Figure 5.8 Edit Schedule

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



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

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



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

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

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

#### Draw the schedule:

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

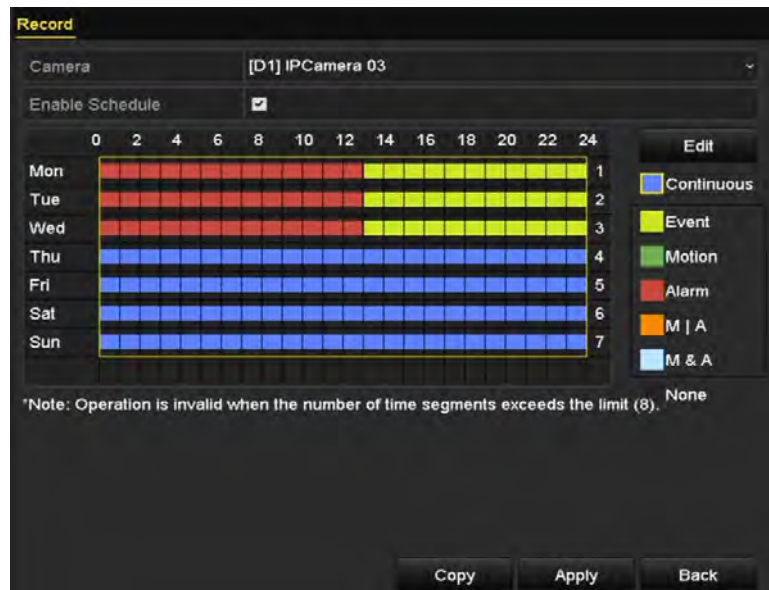


Figure 5. 9 Draw the Schedule

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

## 5.3 Configuring Motion Detection Recording

### Purpose:

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

### Steps:

1. Enter the Motion Detection interface.

Menu > Camera > Motion

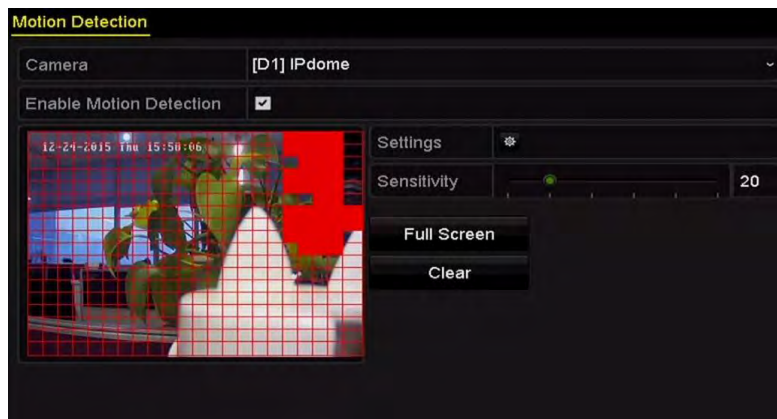


Figure 5. 10 Motion Detection

2. Configure Motion Detection

- 1) Choose camera you want to configure.
- 2) Check the checkbox after **Enable Motion Detection**.
- 3) Drag and draw the area for motion detection by mouse. If you want to set the motion detection for all the area shot by the camera, click **Full Screen**. To clear the motion detection area, click **Clear**.



By default, the feature of **Dynamic Analysis for Motion** is enabled. When the motion detection triggered frame (green) for the moving targets in the motion detection area will be displayed on the live video.

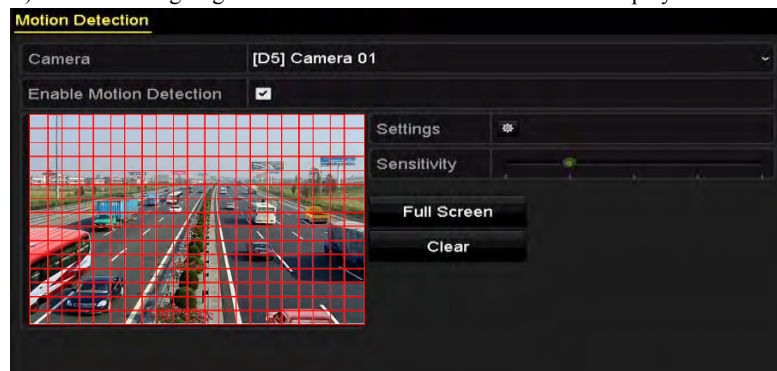


Figure 5. 11 Motion Detection- Mask

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



Figure 5. 12 Motion Detection Handling

- 
- 5) Select the channels which you want the motion detection event to trigger recording.
  - 6) Click **Apply** to save the settings.
  - 7) Click **OK** to back to the upper level menu.
  - 8) Exit the Motion Detection menu.
3. Edit the Motion Detection Record Schedule. For the detailed information of schedule configuration, see *Chapter 5.2 Configuring Recording Schedule*.



## 5.4 Configuring Alarm Triggered Recording

### Purpose:

Follow the procedure to configure alarm triggered recording.

### Steps:

1. Enter the Alarm setting interface.

Menu > Configuration > Alarm



Figure 5. 13 Alarm Settings

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

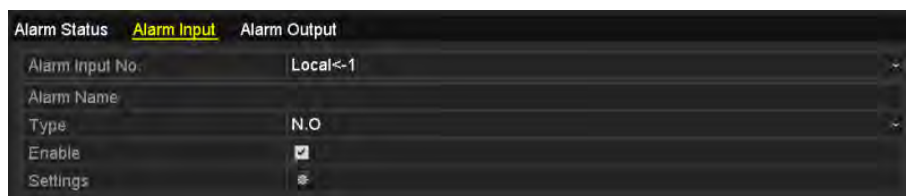


Figure 5. 14 Alarm Settings- Alarm Input

- 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 Enable.
- 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.

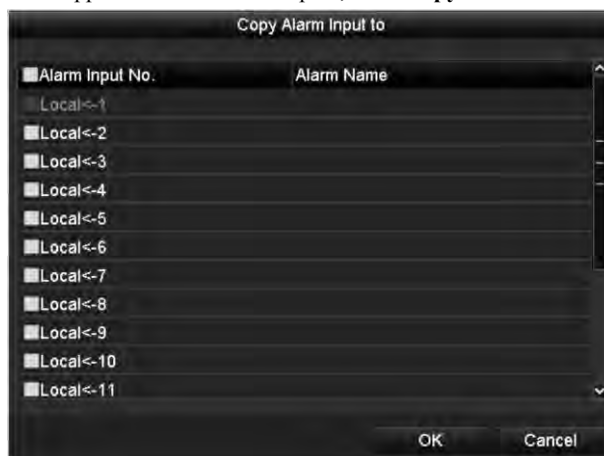


Figure 5.16 Copy Alarm Input

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

## 5.5 Configuring VCA Event Recording

### Purpose:

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

### Steps:

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

Menu > Camera > VCA

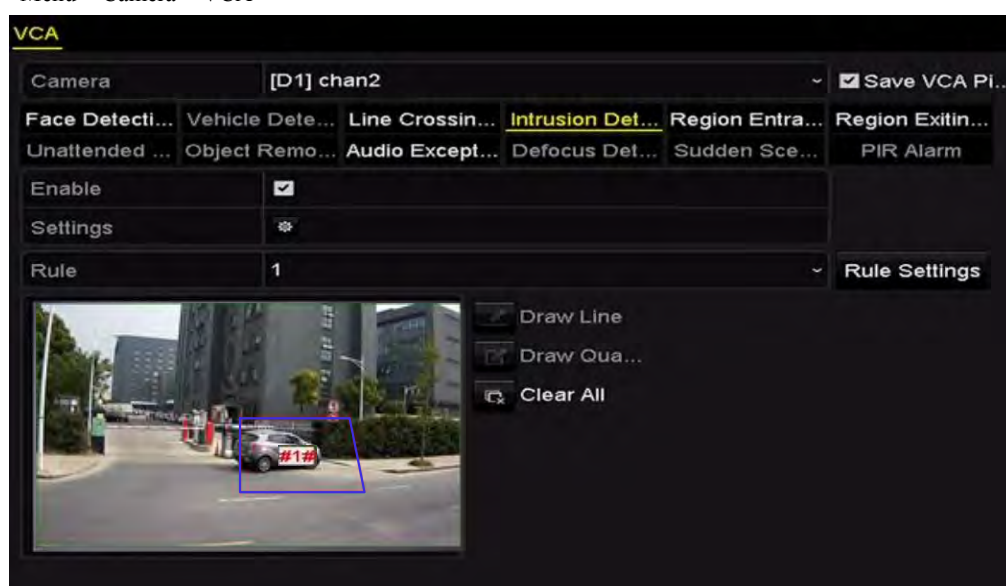


Figure 5. 17 VCA Settings


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



Figure 5. 18 Set Trigger Camera of VCA Alarm



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

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

## 5.6 Manual Recording

### *Purpose:*

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

### *Steps:*

1. Enter the Manual settings interface.

Menu > Manual

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

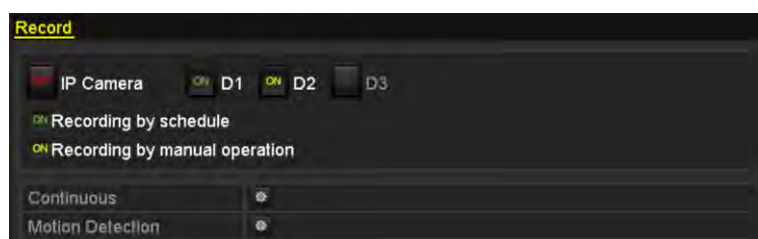


Figure 5. 19 Manual Record

2. Enable the Manual Record.
  - 1) Select **Record** on the left bar.
  - 2) Click the status button before camera number to change **OFF** to **ON**.
3. Disable manual record.
 

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



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.

### Steps:

1. Enter the Record setting interface.

Menu > Record > Holiday



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

Figure 5. 20 Holiday Settings

2. Enable Edit Holiday schedule.

- 1) Click to enter the Edit interface.



**Edit**

Holiday Name: Holiday1

Enable: ☒

Mode: By Week

Start Date: Jan 1st Sun

End Date: Jan 1st Sun

Apply OK Cancel

Figure 5. 21 Edit Holiday Settings

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

## 5.8 Configuring Redundant Recording

### Purpose:

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

### Steps:


1. Enter HDD Information interface.

Menu > HDD



	L...	Capacity	Status	Property	Type	Free Space	Gr...	Edit	D...
	1	465.76GB	Normal	R/W	Local	305GB	1		-
	2	931.51GB	Normal	R/W	Local	814GB	1		-

Figure 5.22 HDD General

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

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



Figure 5.23 HDD General-Editing

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



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

3. Enter the Record setting interface.

Menu > Record > Parameters

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



Figure 5. 24 Record Parameters

---

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

## 5.9 Configuring HDD Group for Recording

### Purpose:

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

### Steps:

1. Enter HDD setting interface.

Menu > HDD



HDD Information								
<input type="checkbox"/> L...	Capacity	Status	Property	Type	Free Space	Gr...	Edit	D...
<input checked="" type="checkbox"/> 1	465.76GB	Normal	R/W	Local	305GB	1		—
<input checked="" type="checkbox"/> 2	931.51GB	Normal	R/W	Local	814GB	1		—


Figure 5.25 HDD General

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



Figure 5.26 Storage Mode

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

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

Repeat the above steps to configure more HDD groups.

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



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



## 5.10 Files Protection

### *Purpose:*

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

### 5.10.1 Locking the Recording Files


#### Lock File when Playback

##### *Steps:*


1. Enter Playback interface.  
Menu> Playback
2. Check the checkbox of channel(s) in the channel list and then double-click to select a date on the calendar.




Figure 5. 27 Normal Playback

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



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

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

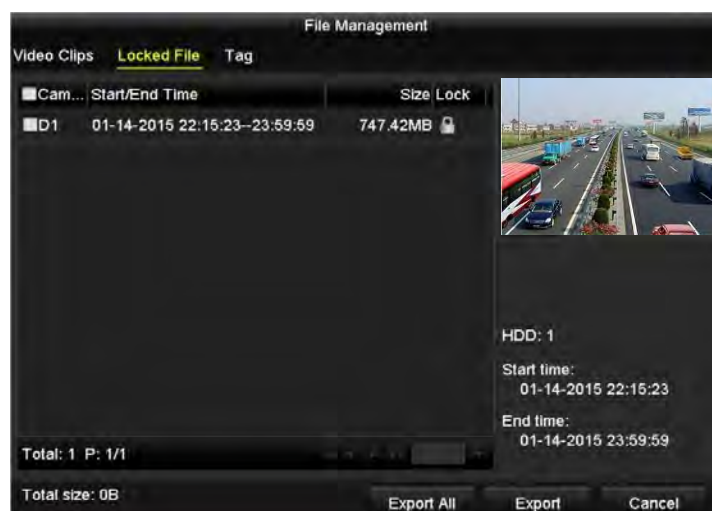




Figure 5. 28 Locked File Management

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

### ● Lock File when Export

#### Steps:

1. Enter Export setting interface.

Menu > Export

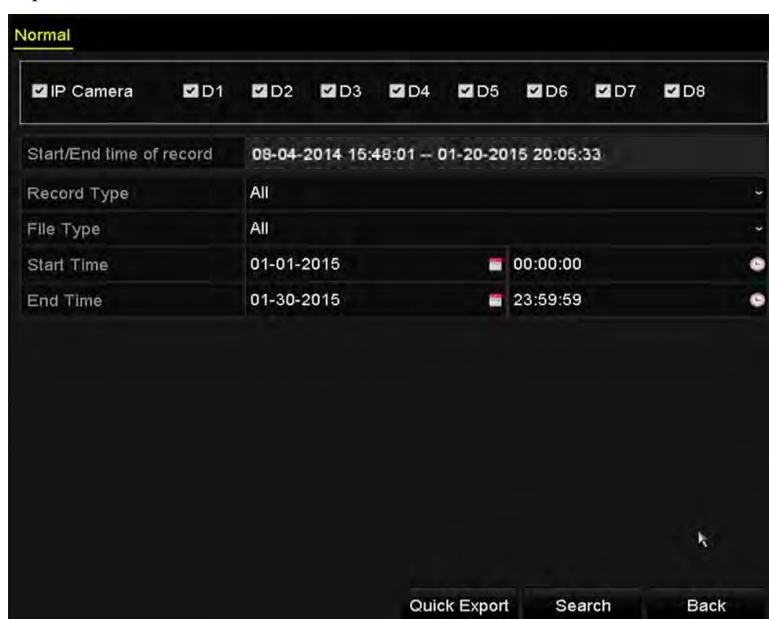


Figure 5. 29 Export


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



Figure 5.30 Export- Search Result

#### 5. Protect the record files.

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



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

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

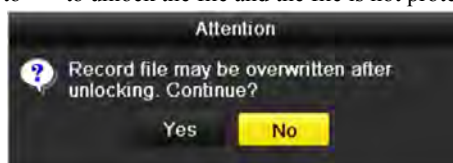


Figure 5.31 Unlocking Attention

## 5.10.2 Setting HDD Property to Read-only

#### Steps:

- Enter HDD setting interface.

Menu > HDD



Figure 5.32 HDD General

- Click to edit the HDD you want to protect.

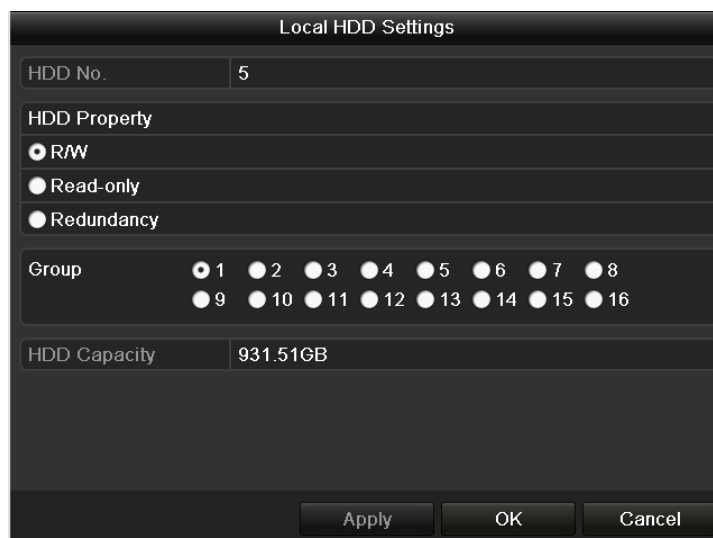


Figure 5. 33 HDD General- Editing



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

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



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

## **Chapter 6 Playback**

## 6.1 Playing Back Record Files


### 6.1.1 Instant Playback

**Purpose:**

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

**Instant playback by channel**

**Step:**

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



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



Figure 6. 1 Instant Playback Interface

---

### 6.1.2 Playing Back by Normal Search

**Playback by Channel**

Enter the Playback interface.

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

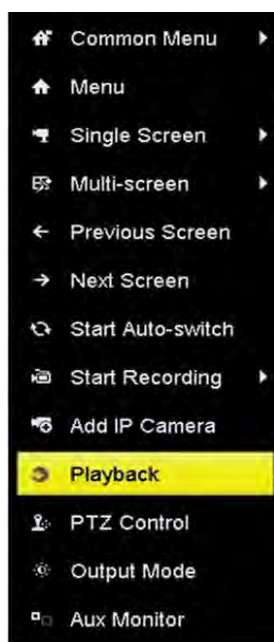


Figure 6. 2 Right-click Menu under Live View



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

## Playback by Time

### *Purpose:*

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

### *Steps:*



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



Figure 6. 3 Playback Calendar



If there are record files 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.

- 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.

























- The **01-01-2016 00:00:23 -- 04-07-2016 19:37:29** indicates the start/end time of the recorded video files.
- 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		Filter video files by setting



		intrusion detection		the target characters
<b>Operations</b>		Audio on/Mute		Start/Stop clipping
		Digital Zoom		Lock File
		Add default tag		Add customized tag
		File management for video clips, captured pictures, locked files and tags		
<b>Playing Control</b>		Pause/Play		Reverse play/ Pause
		Slow forward		Stop
		30s forward		30s reverse
		Next day		Fast forward
		Previous day		
<b>Time Bar Scaling</b>		Previous/Next period		Play the time bar in 30 minutes (default)
		Play the time bar in 1 hour		Play the time bar in 2 hours
		Play the time bar in 6 hours		Play the time bar in 24 hours



Please refer to the *Chapter 3.2.4 Fisheye Expansion* for the description and operation of the fisheye expansion.



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 or VCA information, mark it with green color and play it in the normal speed while the video without motion will be played in the 16-time speed. The smart playback rules and areas are configurable.

#### **Before you start:**

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

#### **Steps:**





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




Figure 6. 6 Playback by Smart Search

5. Click the  radio button to switch to the playback by smart search.
6. Set the rules and areas for smart search of line crossing detection, intrusion detection or motion detection event triggered recording.


- **Motion Detection**

Click the  button, and then hold the mouse on the image to draw the mouse to set the detection area manually. You can also click the  button to set the full screen as the detection area.

- **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.


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

## 6.1.4 Playing Back by Event Search

### *Purpose:*

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

### *Steps:*

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



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



Figure 6.8 Event Search Interface

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).



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

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



Pre-play and post-play can be configured.

8. Enter the Synch Playback interface to select the camera (s) for synchronous playback.

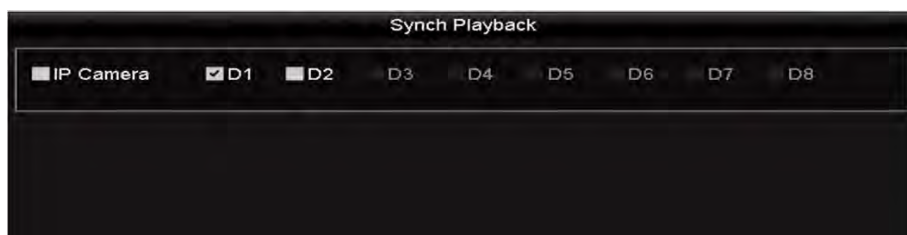


Figure 6.9 Synch Playback Interface

9. 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. Please refer to Table 6.1 for the description of buttons on the toolbar.

## 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:**

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



Figure 6.11 Interface of Playback by Time

- Click  button to add default tag.
- Click  button to add customized tag and input tag name.



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

**3. Tag management.**


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



Figure 6.12 Tag Management Interface



## Playing back by Tag

### Steps:

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



Figure 6. 13 Interface of Playback by Tag



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

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



Figure 6. 14 Interface of Playback by Tag



Pre-play and post-play can be configured.

You can click or button to select the previous or next tag. Please refer to Table 6.1 for the description of

buttons on the toolbar.

## 6.1.6 Playing Back by System Logs

### **Purpose:**

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

### **Steps:**

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

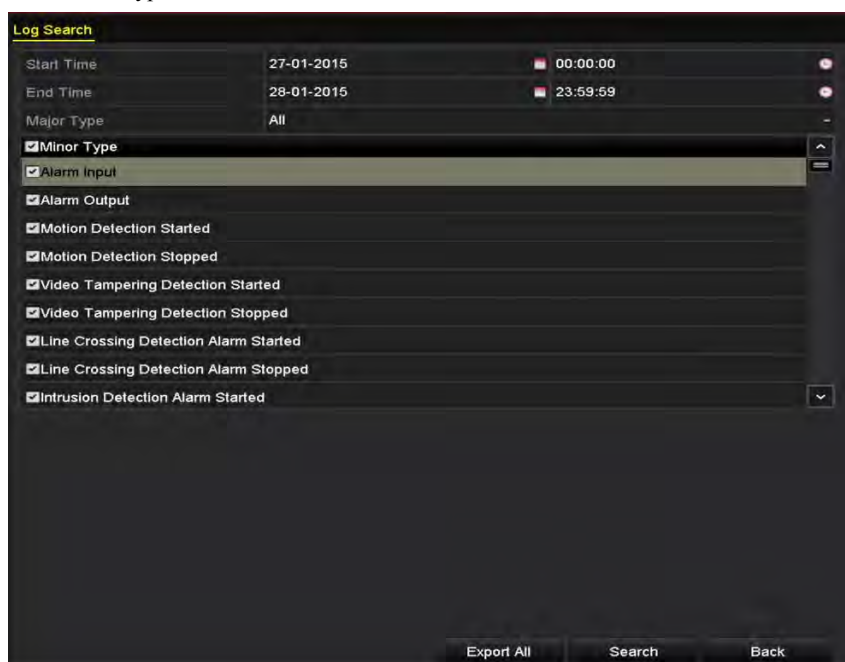



Figure 6. 15 System Log Search Interface

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



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

Search Result						
No.	Major Type	Time	Minor Type	Parameter	Play	Details
1	Exception	27-01-2015 10:02:58	HDD Error	N/A	—	✓
2	Exception	27-01-2015 10:02:58	HDD Error	N/A	—	✓
3	Exception	27-01-2015 10:02:58	HDD Error	N/A	—	✓
4	Operation	27-01-2015 10:03:00	Abnormal Shutd...	N/A	—	✓
5	Operation	27-01-2015 10:03:01	Power On	N/A	—	✓
6	Exception	27-01-2015 10:03:13	Record/Capture ...	N/A	⏮	✓
7	Exception	27-01-2015 10:03:13	Record/Capture ...	N/A	⏮	✓
8	Exception	27-01-2015 10:03:13	Record/Capture ...	N/A	⏮	✓
9	Operation	27-01-2015 11:06:34	Local Operation:...	N/A	—	✓
10	Exception	27-01-2015 11:07:36	HDD Error	N/A	—	✓
Total: 417 P: 1/5						
				Export	Back	

Figure 6. 16 Result of System Log Search

#### 4. Playback interface.

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



Figure 6. 17 Interface of Playback by Log

## 6.1.7 Playing Back External File

### Purpose:

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

### Steps:

1. Enter Tag Search interface.

Menu > Playback

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

The files are listed in the right-side list.

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




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





Figure 6. 18 Interface of External File Playback

## 6.1.8 Playing Back by Sub-periods



The DS-8600NI-E8, DS-7700/E4, DS-7600-E1(E2) series NVR supports playback by sub-periods.

### ***Purpose:***

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

### ***Steps:***

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



Figure 6. 19 Interface of Sub-periods Playback



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

## 6.2 Auxiliary Functions of Playback

### 6.2.1 Playing Back Frame by Frame

#### *Purpose:*

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

#### *Steps:*

- **Using a Mouse:**

Go to Playback interface.

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

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

- **Using the Front Panel:**

Click the button to set the speed to Single frame. One click on button, one click on the playback screen or Enter button on the front panel represents playback or reverse playback of one frame.

## 6.2.2 Thumbnails View

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

### Steps:

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



Figure 6. 20 Thumbnails View

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.



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.

### Steps:

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



Figure 6.21 Playback Interface

2. Use the mouse to hold and drag through the playing time bar to fast view the video files.
3. Release the mouse to the required time point to enter the full-screen playback.



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

## 6.2.4 Digital Zoom

### Steps:




1. Click the  button on the playback control bar to enter Digital Zoom interface.
2. You can zoom in the image to different proportions (1 to 16X) by moving the sliding bar from  to . You can also scroll the mouse wheel to control the zoom in/out.



Figure 6.22 Draw Area for Digital Zoom

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



## 6.2.5 File Management

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

*Steps:*


1. Enter the playback interface.
2. Click  on the toolbar to enter the file management interface.



Figure 6. 23 File Management

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

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 Quick Export

**Purpose:**

Export record files to backup device(s) quickly.

**Steps:**

1. Enter Video Export interface.

Menu > Export > Normal

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



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

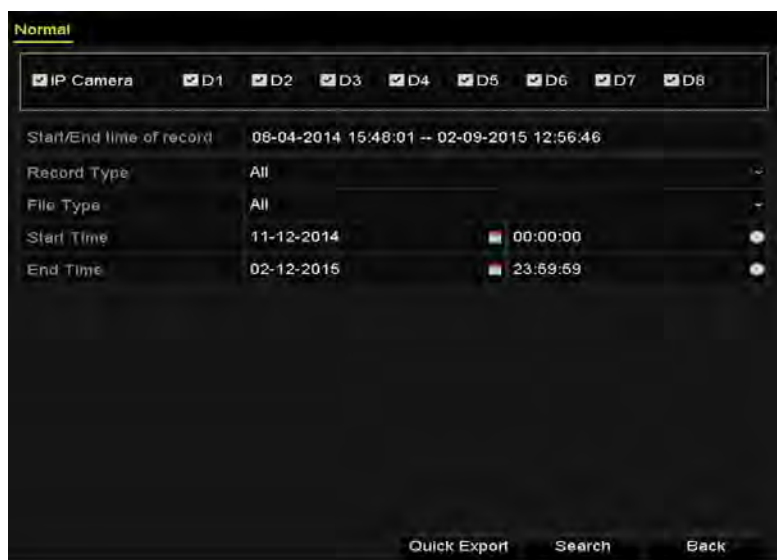


Figure 7. 1 Quick Export Interface

2. Select the format of the log files to be exported. Up to 9 formats are selectable.
3. Click the **Export** to start exporting.



Here we use USB Flash Drive and please refer to the next section Normal Backup for more backup devices supported by the NVR.

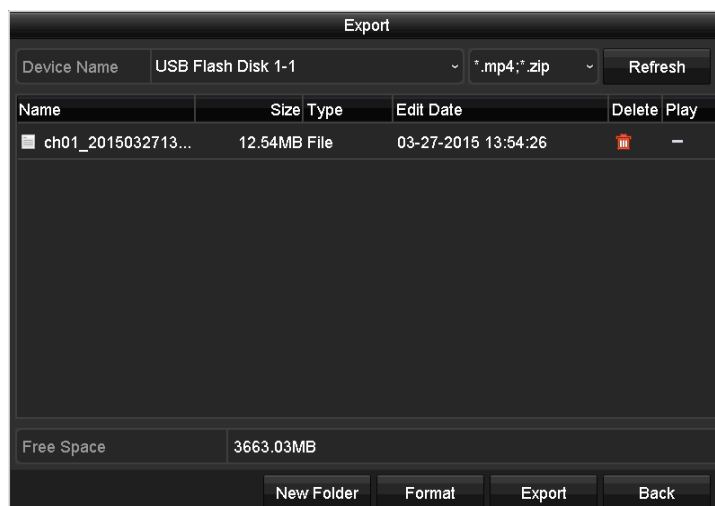


Figure 7. 2 Quick Export using USB1-1

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



Figure 7. 3 Export Finished

#### 4. Check backup result.



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

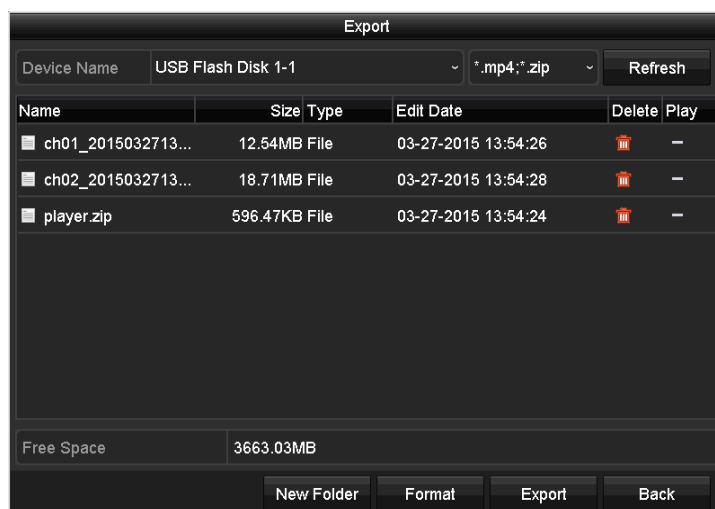


Figure 7. 4 Checkup of Quick Export Result Using USB1-1



## 7.1.2 Backing up by Normal Video Search

### *Purpose:*

The record files can be backup to various devices, such as USB devices (USB flash drives, USB HDDs, USB writer), SATA writer and e-SATA HDD.

### **Backup using USB flash drives and USB HDDs**

#### *Steps:*

1. Enter Export interface.  
Menu>Export>Normal
2. Select the cameras to search.
3. Set search condition and click **Search** button to enter the search result interface. The matched video files are displayed in Chart or List display mode.

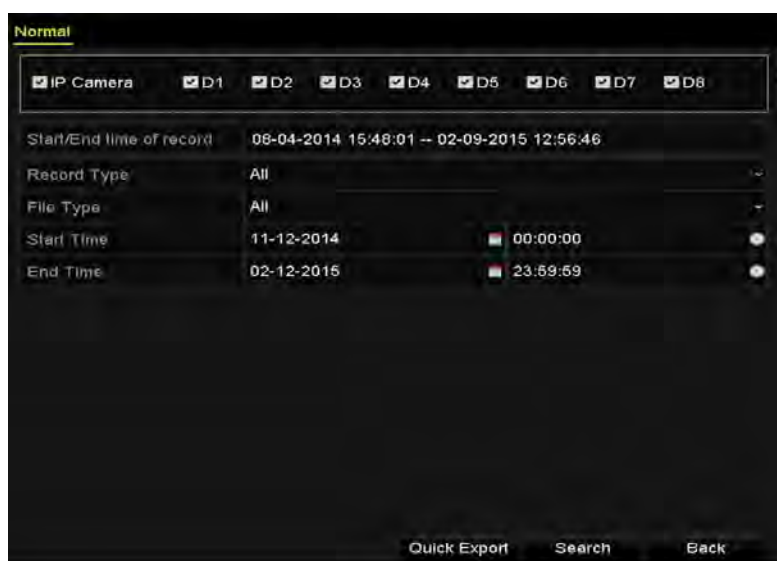



Figure 7. 5 Normal Video Search for Backup

4. Select video files or pictures from the Chart or List to export.

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

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



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



Figure 7. 6 Result of Normal Video Search for Backup

##### 5. Export the video files or picture files.

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

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



If the inserted USB device is not recognized:

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

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



Figure 7. 7 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. 8 Export Finished



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

### 7.1.3 Backing up by Event Search

#### *Purpose:*

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

#### *Steps:*

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

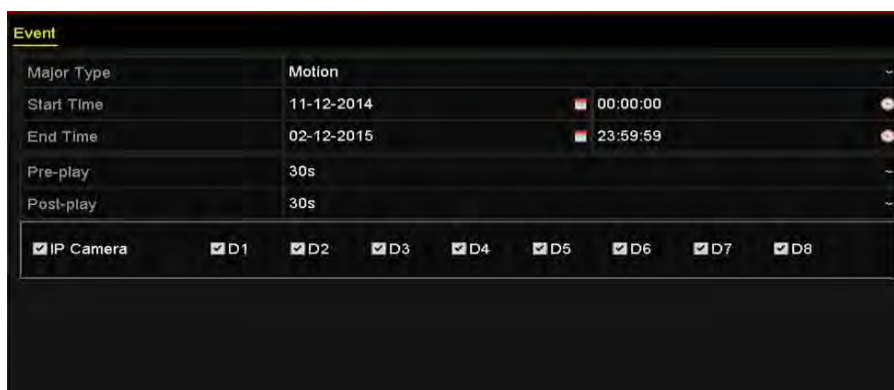


Figure 7. 9 Event Search for Backup

4. Set search condition and click **Search** button to enter the search result interface. The matched video files are displayed in Chart or List display mode.
5. Select video files from the Chart or List interface to export.



Figure 7.10 Result of Event Search

6. Export the video files. Please refer to step5 of *Chapter 7.1.2 Backing up by Normal Video Search* for details.

## 7.1.4 Backing up Video Clips

### **Purpose:**

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

### **Steps:**




1. Enter Playback interface.  
Please refer to *Chapter 6.1 Playing Back Record Files*.
2. During playback, use buttons  or  in the playback toolbar to start or stop clipping record file(s).
3. Click the  to enter the file management interface.



Figure 7.11 Video Clips Export Interface

7. Export the video clips in playback. Please refer to step5 of *Chapter 7.1.2 Backing up by Normal Video Search* for details.

## 7.2 Managing Backup Devices

### Management of USB flash drives, USB HDDs and eSATA HDDs

#### Steps:

1. Enter the Export interface.



Figure 7. 12 Storage Device Management

2. Backup device management.

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

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

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

Click **Format** button to format the backup device.



If the inserted storage device is not recognized:

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

## **Chapter 8 Alarm Settings**

## 8.1 Setting Motion Detection Alarm

### Steps:

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


Menu > Camera > Motion

2. Set up detection area and sensitivity.

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



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

Click  button and set alarm response actions.

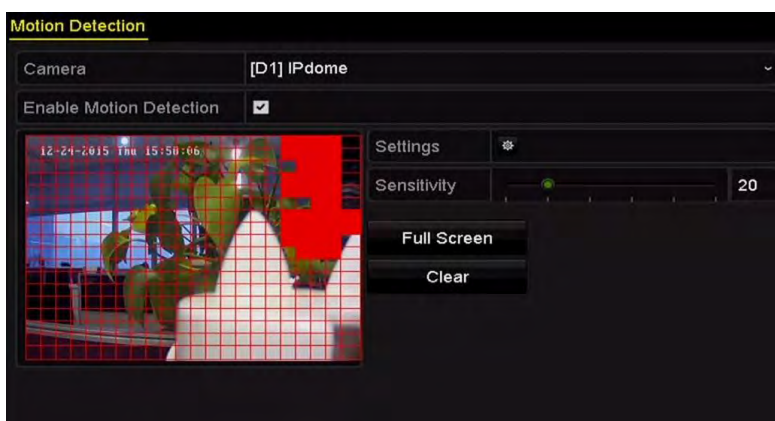


Figure 8. 1 Motion Detection Setup Interface



By default, the feature of **Dynamic Analysis for Motion** is enabled. When the motion detection triggered frame (green) for the moving targets in the motion detection area will be displayed on the live video.

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



Figure 8. 2 Set Trigger Camera of Motion Detection

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



Time periods shall not be repeated or overlapped.



Figure 8. 3 Set Arming Schedule of Motion Detection

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



## 8.2 Setting Sensor Alarms

### Purpose:

Set the handling action of an external sensor alarm.

### Steps:

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

Menu> Configuration> Alarm

Select Alarm Input tab to enter Alarm Input Settings interface.



Figure 8.4 Alarm Status Interface of System Configuration

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

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



Figure 8.5 Alarm Input Setup Interface

3. (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 local alarm input 1. The selected linkage actions include the Full Screen Monitoring, Audible Warning, Notify Surveillance Center, Send Email and Trigger Alarm Output.



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

4. 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.
5. Select **Arming Schedule** tab to set the arming schedule of handling actions.

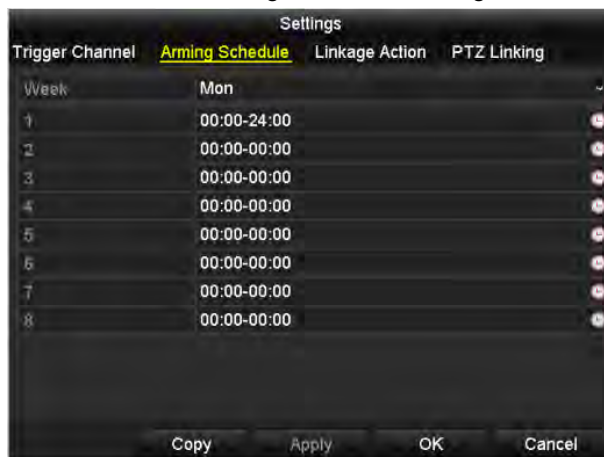


Figure 8. 6 Set Arming Schedule of Alarm Input

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



Time periods shall not be repeated or overlapped.

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

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



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

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



Figure 8. 7 Set PTZ Linking of Alarm Input

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

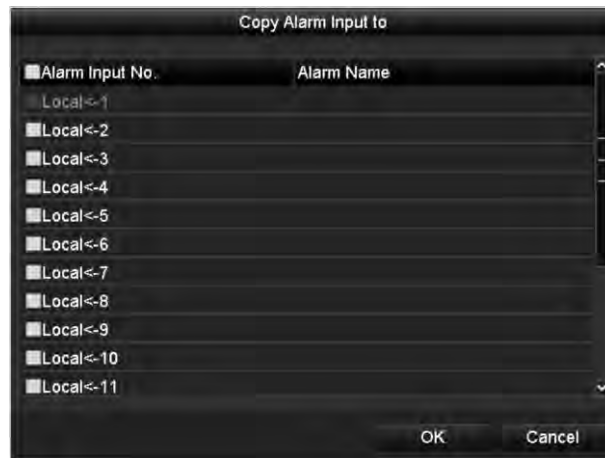


Figure 8. 8 Copy Settings of Alarm Input

---

## 8.3 Detecting Video Loss Alarm

### Purpose:

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

### Steps:

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

Menu > Camera > Video Loss

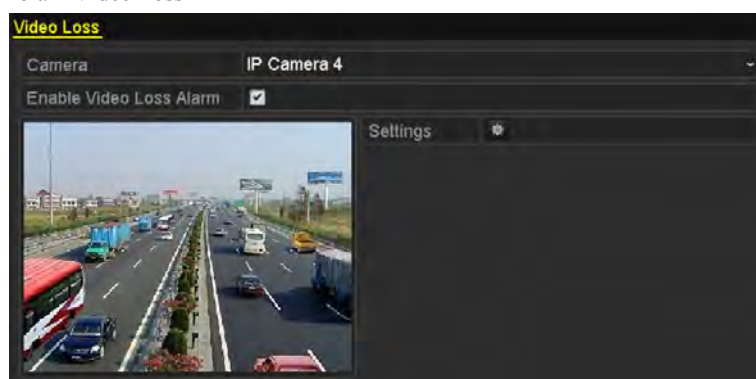



Figure 8.9 Video Loss Setup Interface

2. Set up handling action of video loss.

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

3. Set up arming schedule of the handling actions.

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



Time periods shall not be repeated or overlapped.

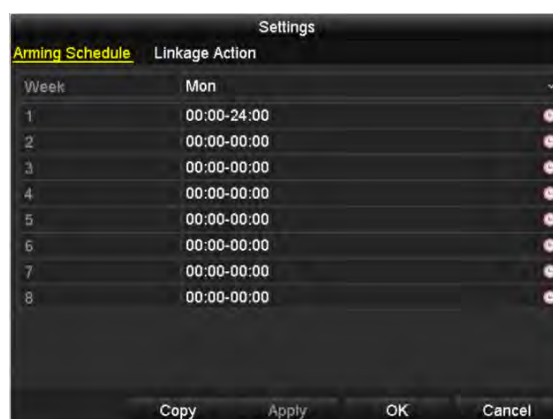


Figure 8.10 Set Arming Schedule of Video Loss

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

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

## 8.4 Detecting Video Tampering Alarm

### *Purpose:*

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

### *Steps:*

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

Menu> Camera> Video Tampering

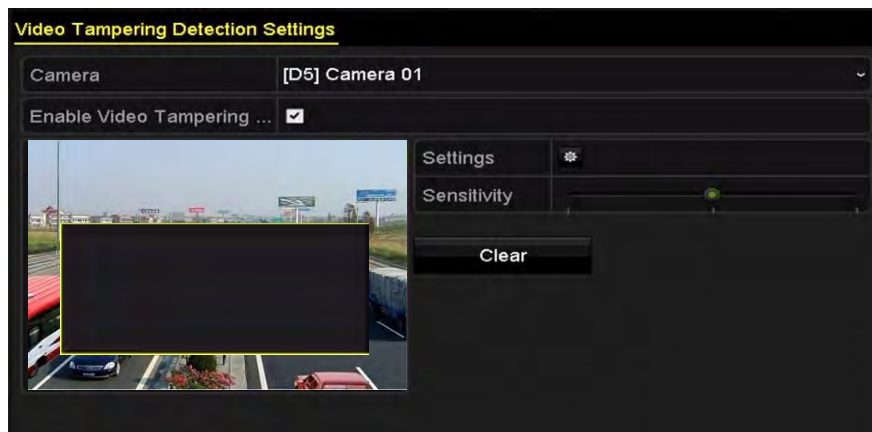


Figure 8. 11 Video Tampering Setup Interface

2. Set the video tampering handling action of the channel.  
Check the checkbox of **Enable Video Tampering Detection**.  
Drag the sensitivity bar to set a proper sensitivity level. Use the mouse to draw an area you want to detect video tampering.

Click  button to set up handling action of video tampering.

3. Set arming schedule and alarm response actions of the channel.
  - 1) Click Arming Schedule tab to set the arming schedule of handling actions.
  - 2) Choose one day of a week and max. eight time periods can be set within each day.
  - 3) Click **Apply** button to save the settings.



Time periods shall not be repeated or overlapped.



Figure 8. 12 Set Arming Schedule of Video Tampering

---

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

## 8.5 Handling Exceptions Alarm

### *Purpose:*

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

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



PoE Power Overload is only supported by DS-7600NI-E1/4P, DS-7600NI-E2/8P and DS-7700NI-E4/P series NVR.

### *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, Upload Picture to FTP, Trigger Alarm Output and Send Email.

### **Event Hint Display**

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

### *Steps:*

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

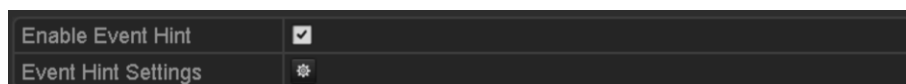


Figure 8. 14 Event Hint Settings Interface


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



Figure 8. 15 Event Hint Settings Interface

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

### **Full Screen Monitoring**

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

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

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



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

### Audible Warning

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

### Notify Surveillance Center

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



The alarm signal will be transmitted automatically at detection mode when remote alarm host is configured. Please refer to *Chapter 11.2.6* 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 11.2.7* for details of Email configuration.

### Trigger Alarm Output

Trigger an alarm output when an alarm is triggered.

1. Enter Alarm Output interface.

Menu> Configuration> Alarm> Alarm Output

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



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

Alarm Status	Alarm Input	Alarm Output
Alarm Output No.	Local->1	
Alarm Name		
Dwell Time	5s	
Settings		

Figure 8. 16 Alarm Output Setup Interface

2. Set up arming schedule of the alarm output.

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



Time periods shall not be repeated or overlapped.



Figure 8. 17 Set Arming Schedule of Alarm Output

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

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

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

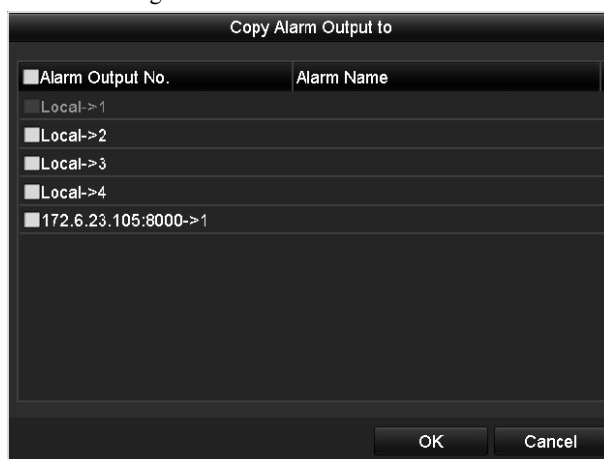


Figure 8. 18 Copy Settings of Alarm Output

## 8.7 Triggering or Clearing Alarm Output Manually

### *Purpose:*

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

### *Steps:*

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

Menu> Manual> Alarm

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

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

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



Alarm Output No.	Alarm Name	Trigger
Local->1		No
Local->2		No
Local->3		No
Local->4		No
172.6.23.105:8000->1		No

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.



- All VCA detection must be supported by the connected IP camera.
- Face detection and vehicle detection are supported by DS-8600NI-E8 and DS-7700NI-E4 series.

## 9.1 Face Detection

### *Purpose:*

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

### *Steps:*

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

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

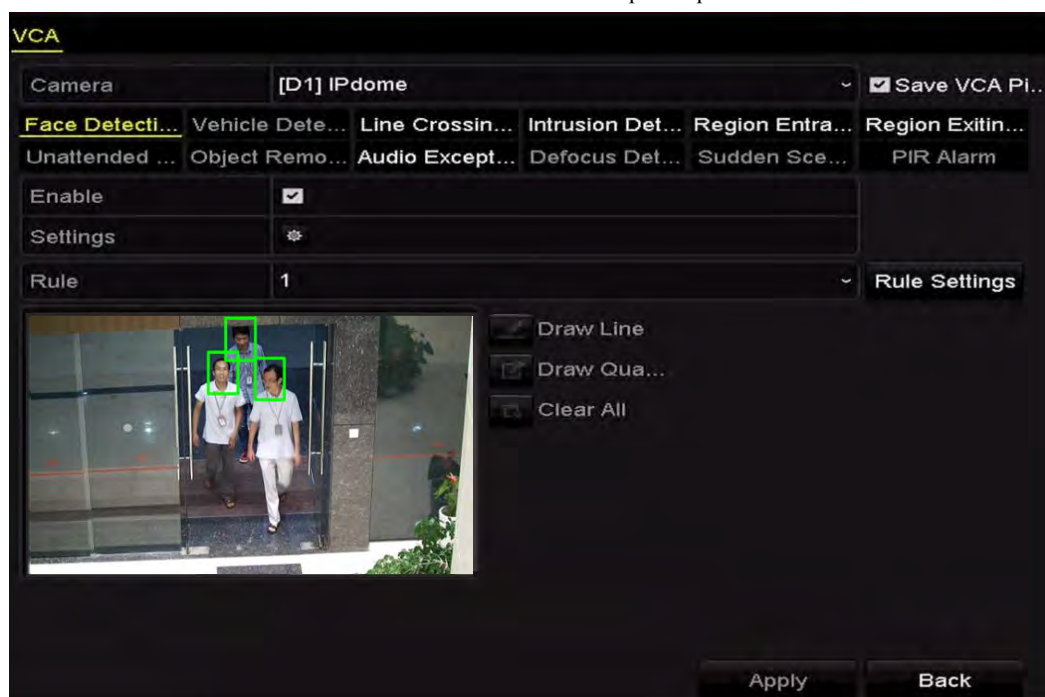



Figure 9. 1 Face Detection

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

detection sensitivity.

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



Figure 9. 2 Set Face Detection Sensitivity

---

6. Click Apply to activate the settings.

## 9.2 Vehicle Detection

### Purpose:

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

### Steps:

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

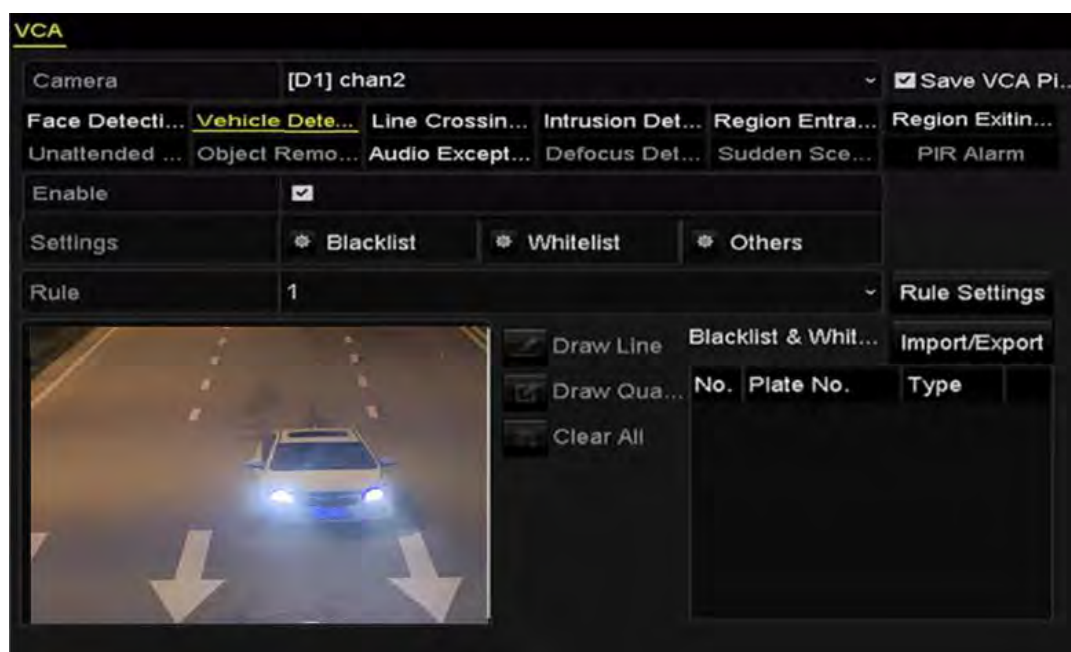



Figure 9. 3 Set Vehicle Detection

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



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

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

---

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




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

## 9.3 Line Crossing Detection

### Purpose:

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

### Steps:

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


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


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

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



Figure 9. 5 Set Line Crossing Detection Rules

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

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



Up to 4 rules can be configured.

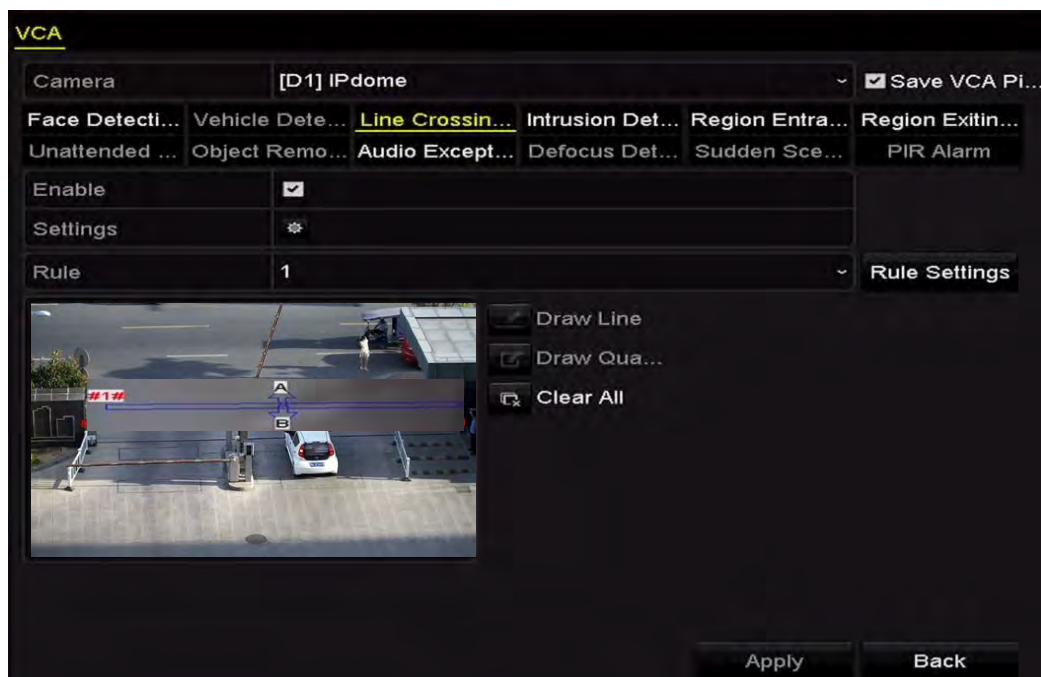


Figure 9. 6 Draw Line for Line Crossing Detection

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

## 9.4 Intrusion Detection

### Purpose:

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

### Steps:




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



Figure 9. 7 Set Intrusion Crossing Detection Rules

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

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



Up to 4 rules can be configured.

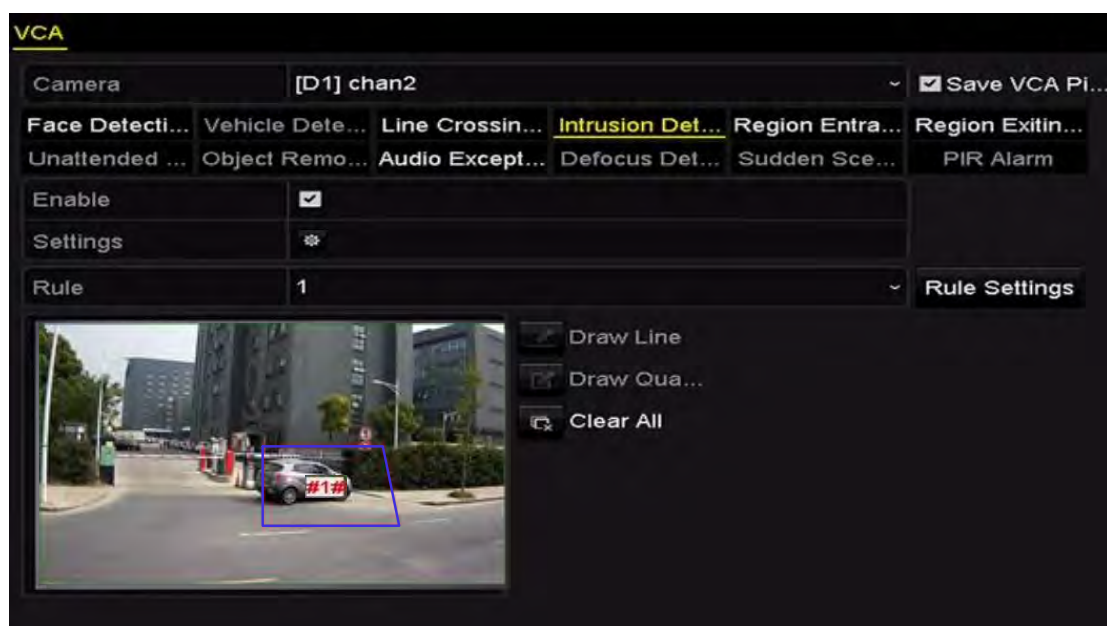


Figure 9. 8 Draw Area for Intrusion Detection



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


## 9.5 Region Entrance Detection

### Purpose:

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

### Steps:

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

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

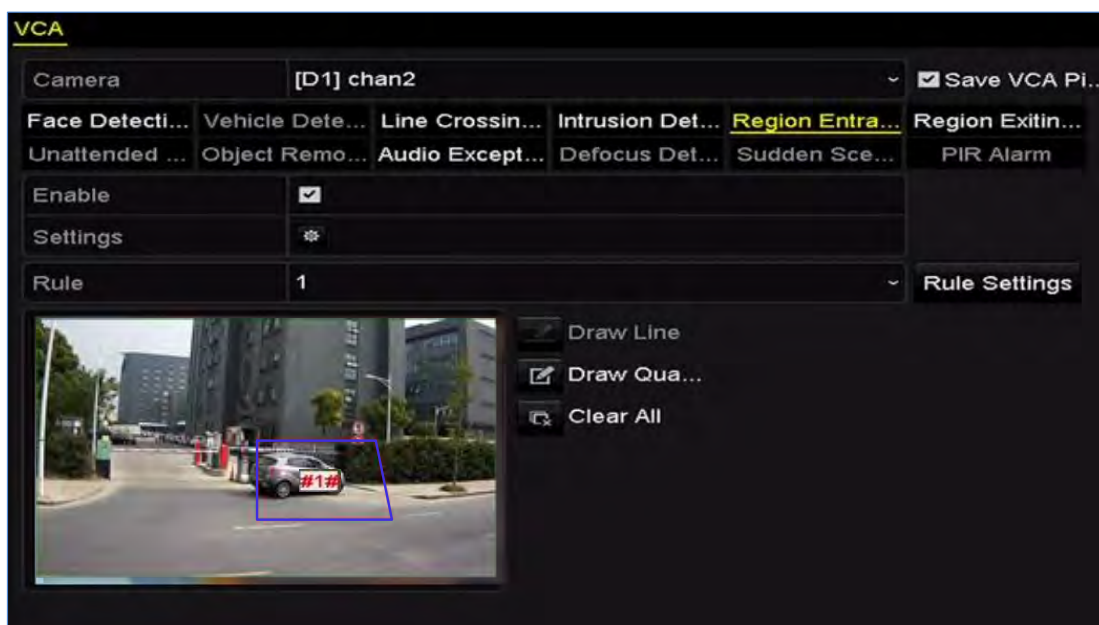


Figure 9. 9 Set Region Entrance Detection



Up to 4 rules can be configured.

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

## 9.6 Region Exiting Detection

### *Purpose:*

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



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

## 9.7 Unattended Baggage Detection

### *Purpose:*

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



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

## 9.8 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.



- 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.

### *Steps:*


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



Figure 9. 10 Set Audio Exception Detection Rules

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

## 9.10 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.



- 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.




- 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.

### **Steps:**

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

## **Chapter 10 VCA Search**

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



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

## 10.1 Face Search

### *Purpose:*

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

### *Before you start:*

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

### *Steps:*

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

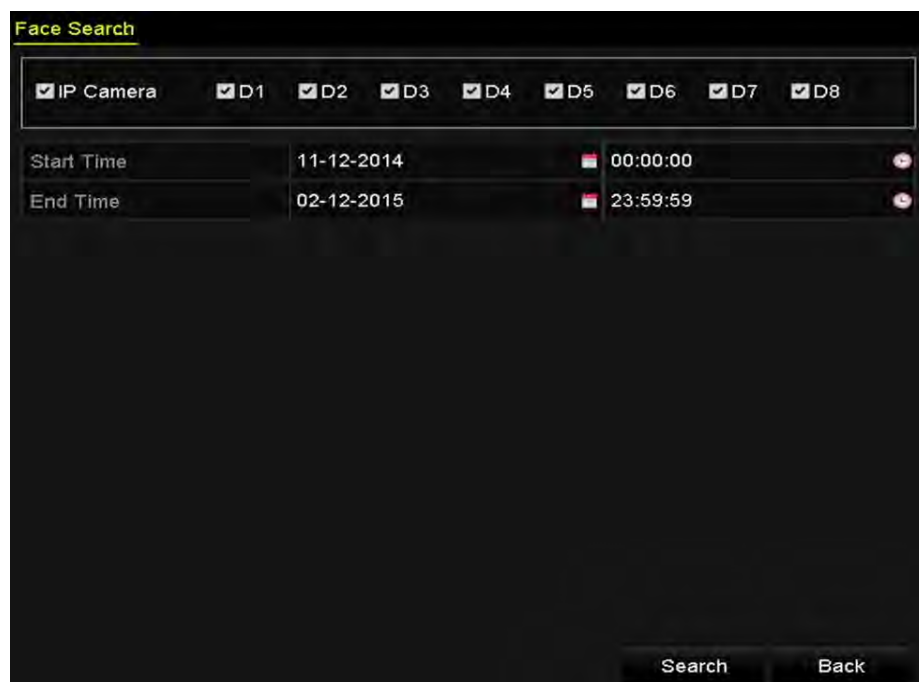



Figure 10. 1 Face Search




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



Figure 10. 2 Face Search Interface

5. Play the face picture related video file.

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

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

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

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

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



Figure 10. 3 Export Files

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.

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

Behavior Search

☒ IP Camera
 ☒ D1
 ☒ D2
 ☒ D3
 ☒ D4
 ☒ D5
 ☒ D6
 ☒ D7
 ☒ D8

Start Time	11-12-2014		00:00:00	
End Time	02-12-2015		23:59:59	
Type	All			

Search





Back

Figure 10. 4 Behavior Search Interface

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



Figure 10. 5 Behavior Search Results

6. Play the behavior analysis picture related video file.  
 You can double click on a picture from the list to play its related video file in the view window on the top right, or select a picture item and click  to play it.  
 You can also click  to stop the playing, or click   to play the previous/next file.
7. If you want to export the captured pictures to local storage device, connect the storage device to the device and click **Export All** to enter the Export interface.  
 Click **Export** to export all pictures to the storage device.

## 10.3 Plate Search

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

**Steps:**

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

Figure 10. 6 Plate Search

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



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

## 10.4 People Counting

### **Purpose:**

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

### **Steps:**

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

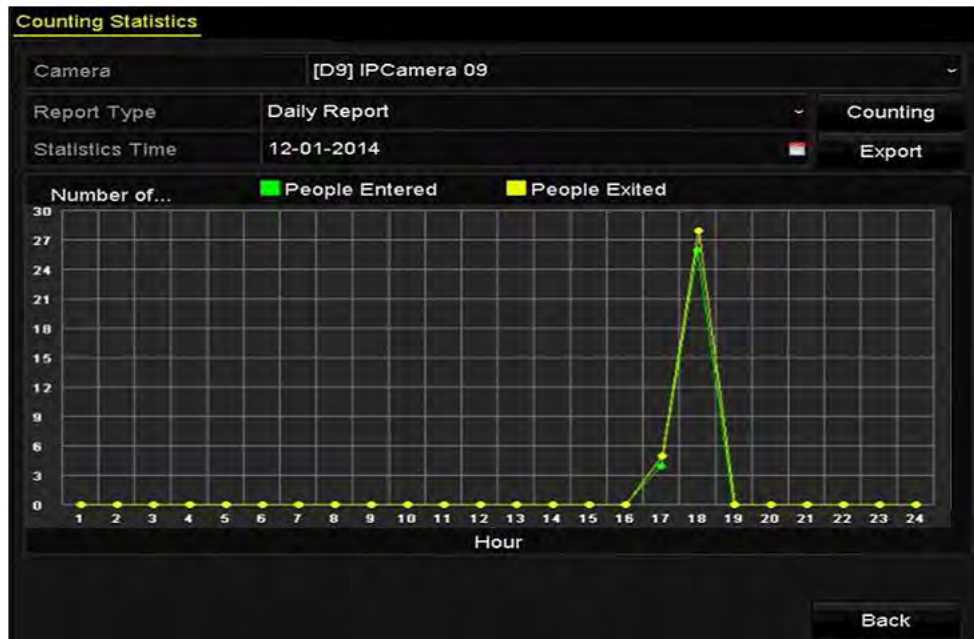


Figure 10. 7 People Counting Interface

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



## 10.5 Heat Map

### *Purpose:*

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



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

### *Steps:*

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

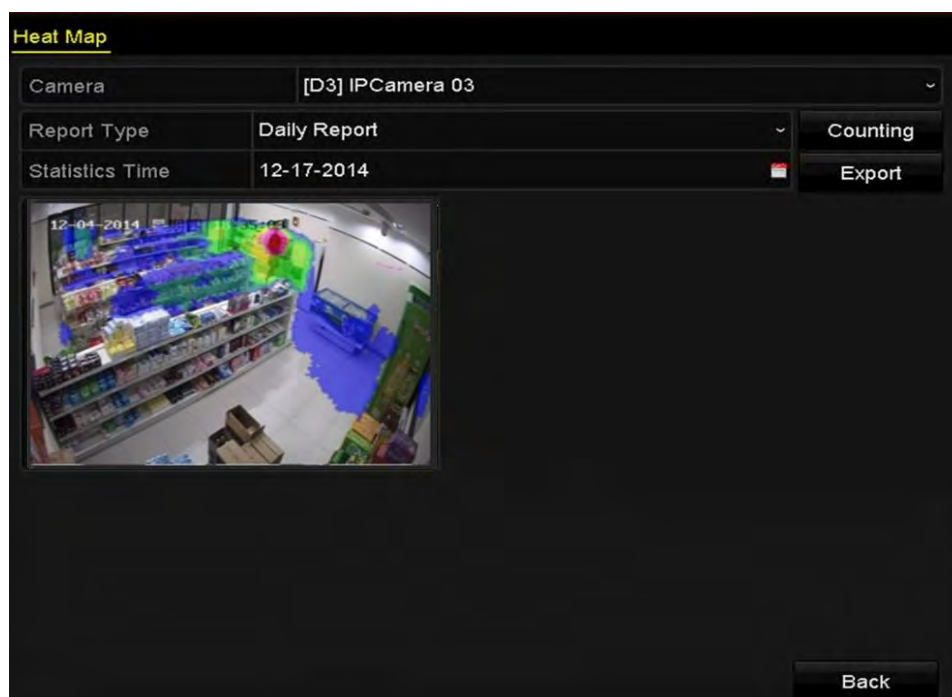


Figure 10. 8 Heat Map Interface

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



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

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.

### Steps:

1. Enter the Network Settings interface.

Menu > Configuration > Network

2. Select the **General** tab.



Figure 11. 1 Network Settings Interface of DS-8600NI-E8 and DS-7700NI-E4



- The dual-NIC network 10 /100/1000 Mbps self-adaptive Ethernet interfaces are provided for the DS-8600NI-E8 and DS-7700NI-E4 series NVR; one 10 /100 Mbps self-adaptive Ethernet interface for DS-7604/7608NI-E1(E2) series NVR; and one 10 /100/1000 Mbps self-adaptive Ethernet interface for other models.

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

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



- For the models which have the PoE or built-in switch network interfaces, including DS-7600NI-E1(E2)/N, DS-7600NI-E1(E2)/P and DS-7700NI-E4/P series NVR, the internal NIC IPv4 address should be configured for the cameras connecting to the PoE or built-in switch network interface of the NVR.
- The valid value range of MTU is 500 ~ 9676.

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

### Working Mode

Two 10M/100M/1000M NIC cards are provided by the DS-8600NI-E8 and DS-7700NI-E4 series device, which allows the device to work in the Multi-address and Net-fault Tolerance modes.

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

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

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

## 11.2 Configuring Advanced Settings

### 11.2.1 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.



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.

#### *Steps:*

1. Enter the **Network Settings** interface.  
Menu > Configuration > Network
2. Select the **Platform Access** tab to enter the Hik-Connect Settings interface.

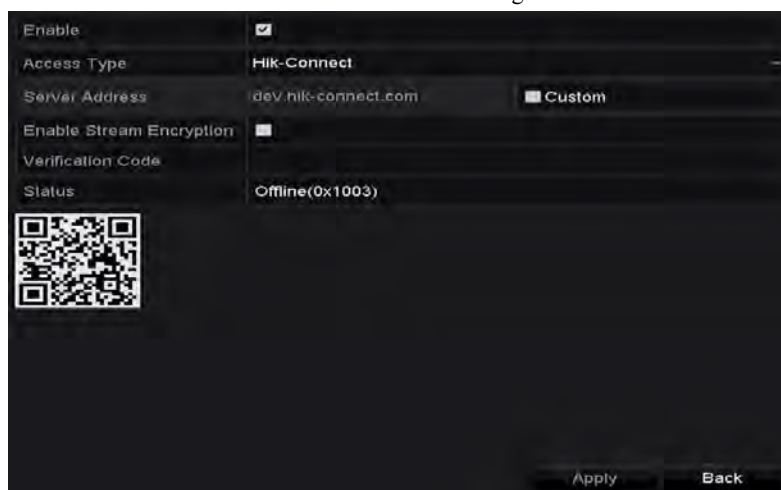


Figure 11. 2 Hik-Connect Settings

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

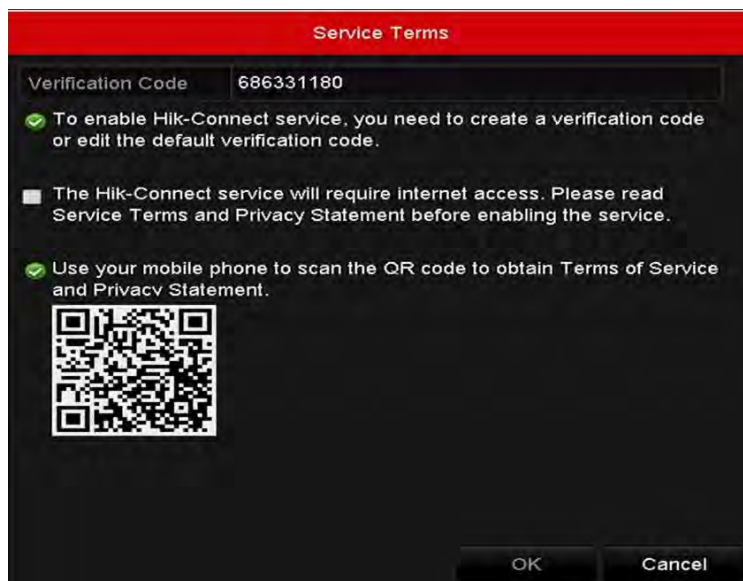


Figure 11.3 Service Terms

- 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.



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



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

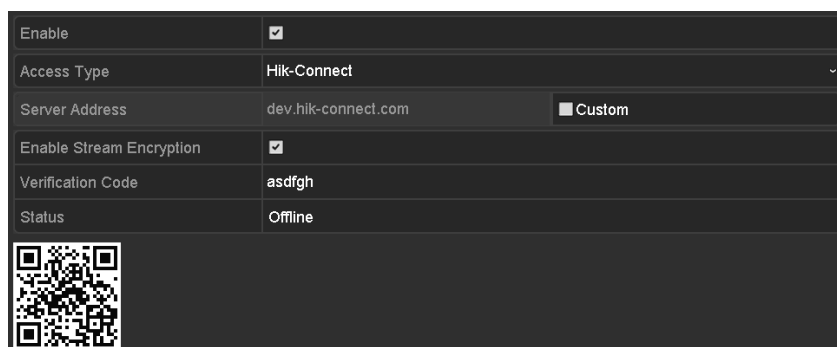


Figure 11.4 Hik-Connect Settings Interface

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](http://www.hik-connect.com)).



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

## 11.2.2 Configuring DDNS

### **Purpose:**

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

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

### **Steps:**

1. Enter the Network Settings interface.  
Menu > Configuration > Network
2. Select the **DDNS** tab to enter the DDNS Settings interface.
3. Check the **Enable DDNS** checkbox to enable this feature.
4. Select **DDNS Type**. Three different DDNS types are selectable: DynDNS, PeanutHull, and NO-IP.
  - **DynDNS:**
    - 1) Enter **Server Address** for DynDNS (i.e. [members.dyndns.org](http://members.dyndns.org)).
    - 2) In the NVR Domain Name text field, enter the domain obtained from the DynDNS website.
    - 3) Enter the **User Name** and **Password** registered in the DynDNS website.

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

Figure 11. 5 DynDNS Settings Interface

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

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

Figure 11. 6 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 NVR 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.

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

Figure 11. 7 NO-IP Settings Interface

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

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

## 11.2.3 Configuring NTP Server

**Purpose:**

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



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

**Steps:**



1. Enter the Network Settings interface.  
Menu > Configuration > Network
2. Select the **NTP** tab to enter the NTP Settings interface, as shown in Figure 11. 8.

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

Figure 11. 8 NTP Settings Interface

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



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

## 11.2.4 Configuring SNMP

### *Purpose:*

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

### *Steps:*

1. Enter the Network Settings interface.  
Menu > Configuration > Network
2. Select the **SNMP** tab to enter the SNMP Settings interface, as shown in Figure 11. 9.

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

Figure 11. 9 SNMP Settings Interface

3. Check the **SNMP** checkbox to enable this feature.
4. The enabling of SNMP may cause security problems. Click **Yes** to continue or **No** to cancel the operation.

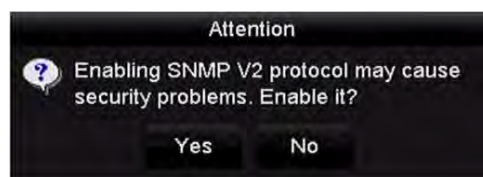


Figure 11.10 SNMP Settings Interface

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



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

## 11.2.5 Configuring More Settings

### Steps:

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

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

Figure 11.11 More Settings Interface

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.



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.

Alarm Host IP	192.0.0.10
Alarm Host Port	7200
Server Port	8000
HTTP Port	80
Multicast IP	239.252.2.50
RTSP Port	554

Figure 11. 12 Configure More Settings

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

## 11.2.6 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.



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

### *Steps:*

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

Figure 11. 13 HTTPS Settings

**OPTION 1: Create the self-signed certificate**

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

Figure 11. 14 Create Self-signed Certificate

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

**OPTION 2: Create the authorized certificate**

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

Figure 11. 15 Installed Certificate Property

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

## 11.2.7 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.

### *Steps:*

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

NIC Type	10M/100M/1000M Self-adaptive		
Enable DHCP	<input checked="" type="checkbox"/>		
IPv4 Address	10 .16 .1 .26	IPv6 Address	fe80::269:6cff:fe2a:fb88/64
IPv4 Subnet Mask	255 .255 .255 .0	IPv6 Address	
IPv4 Default Gateway	10 .16 .1 .254	IPv6 Default Gateway	
MAC Address	00:69:6c:2a:fb:88		
MTU(Bytes)	1500		
Enable DNS DHCP	<input checked="" type="checkbox"/>		
Preferred DNS Server	10.1.7.88		
Alternate DNS Server	10.1.7.77		

Figure 11. 16 Network Settings Interface

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

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

Figure 11. 17 Email Settings Interface

5. Configure the following Email settings:
  - Enable Server Authentication (optional):** Check the checkbox to enable the server authentication feature.
  - User Name:** The user account of sender's Email for SMTP server authentication.
  - Password:** The password of sender's Email for SMTP server authentication.
  - SMTP Server:** The SMTP Server IP address or host name (e.g., smtp.263xmail.com).
  - SMTP Port No.:** The SMTP port. The default TCP/IP port used for SMTP is 25.

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

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

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

6. Click **Apply** button to save the Email settings.
7. You can click **Test** button to test whether your Email settings work. The corresponding Attention message box will pop up. Refer to Figure 11. 18.

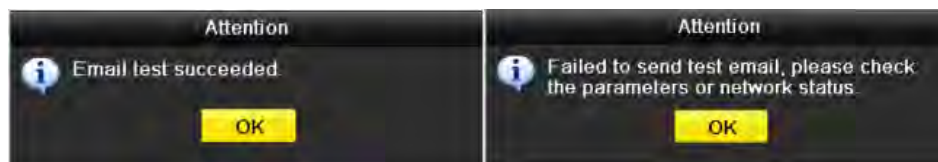


Figure 11. 18 Email Testing Attention

---

## 11.2.8 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.

### *Steps:*

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

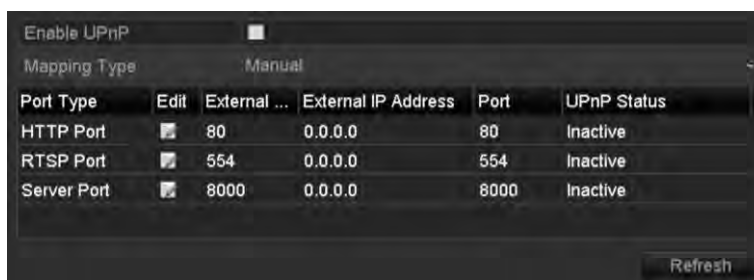


Figure 11. 19 UPnP™ Settings Interface

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

**OPTION 1: Auto**

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

**Steps:**

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

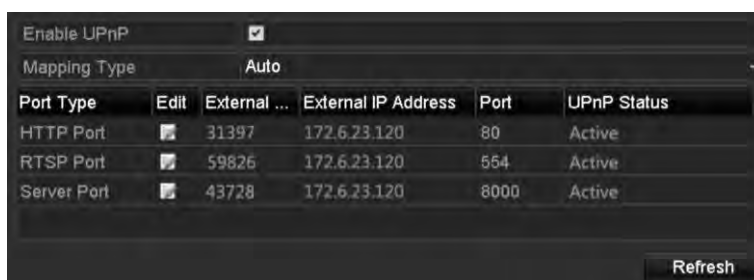


Figure 11. 20 UPnP™ Settings Finished-Auto

**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.



- 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.

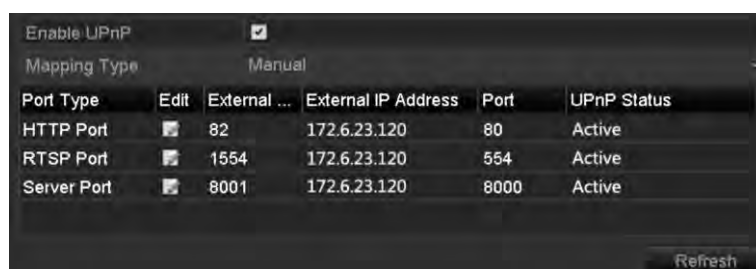


Figure 11. 22 UPnP™ Settings Finished-Manual

### ● Manual Mapping

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

#### **Before you start:**

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

#### **Steps:**

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



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



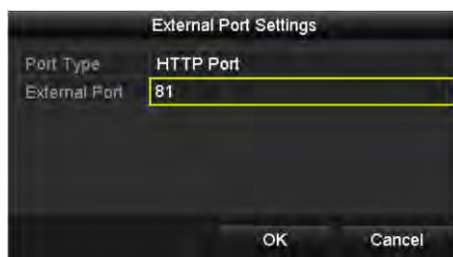


Figure 11. 23 External Port Settings Dialog Box

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



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

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

Figure 11. 24 Setting Virtual Server Item



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

## 11.2.9 Configuring Virtual Host

### *Purpose:*


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



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

### *Steps:*

1. Enter the Advanced settings interface, as shown in the Figure 11. 25.  
Configuration > Network > Advanced Settings > Other

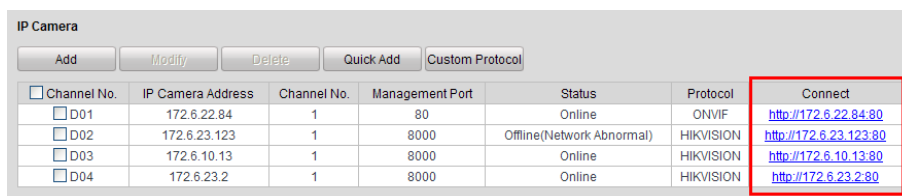


The Advanced Settings Interface is a web-based configuration window. It features a title bar 'Advanced' and four input fields: 'Alarm Host IP', 'Alarm Host Port' (containing '0'), and 'Multicast Address'. Below these is a checkbox labeled 'Enable Virtual Host' which is currently unchecked. A 'Save' button is located at the bottom left of the form.

Figure 11. 25 Advanced Settings Interface

2. Check the checkbox of the **Enable Virtual Host**.
3. Click the **Save** button to save the setting.
4. Enter the IP camera management interface of NVR. The Connect column appears on the right-most side of the camera list, as shown in the Figure 11. 26.

Configuration > Remote Configuration > Camera Management > IP Camera



The IP Camera Management Interface shows a table of configured cameras. Above the table are buttons for 'Add', 'Modify', 'Delete', 'Quick Add', and 'Custom Protocol'. The table has columns for 'Channel No.', 'IP Camera Address', 'Channel No.', 'Management Port', 'Status', 'Protocol', and 'Connect'. The 'Connect' column contains links to the camera's management interface. A red box highlights the 'Connect' column.

<input type="checkbox"/> Channel No.	IP Camera Address	Channel No.	Management Port	Status	Protocol	Connect
<input type="checkbox"/> D01	172.6.22.84	1	80	Online	ONVIF	<a href="http://172.6.22.84:80">http://172.6.22.84:80</a>
<input type="checkbox"/> D02	172.6.23.123	1	8000	Offline(Network Abnormal)	HIKVISION	<a href="http://172.6.23.123:80">http://172.6.23.123:80</a>
<input type="checkbox"/> D03	172.6.10.13	1	8000	Online	HIKVISION	<a href="http://172.6.10.13:80">http://172.6.10.13:80</a>
<input type="checkbox"/> D04	172.6.23.2	1	8000	Online	HIKVISION	<a href="http://172.6.23.2:80">http://172.6.23.2:80</a>

Figure 11. 26 Connect to IP Camera

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

## 11.3 Checking Network Traffic

### *Purpose:*

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

### *Steps:*

1. Enter the Network Traffic interface.

Menu > Maintenance > Net Detect

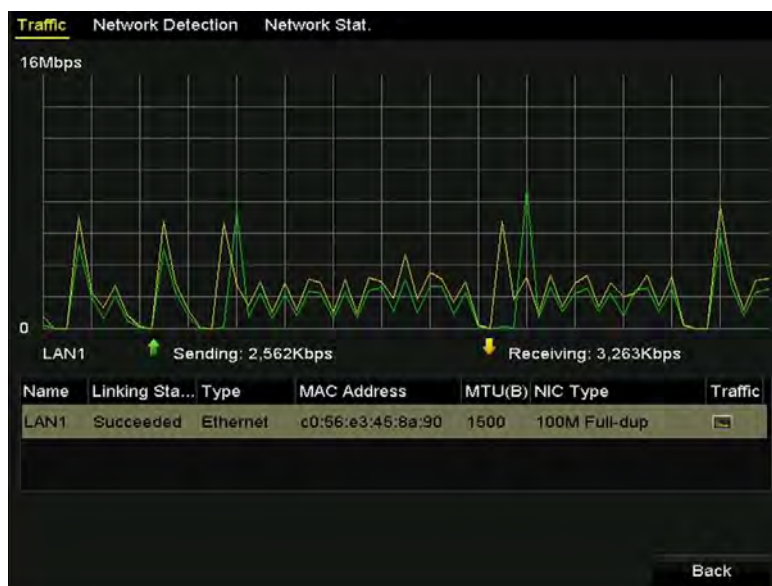


Figure 11. 27 Network Traffic Interface

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

## 11.4 Configuring Network Detection

### *Purpose:*

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

### 11.4.1 Testing Network Delay and Packet Loss

#### *Steps:*

1. Enter the Network Traffic interface.  
Menu > Maintenance > Net Detect
2. Click the **Network Detection** tab to enter the Network Detection menu, as shown in Figure 11. 28.

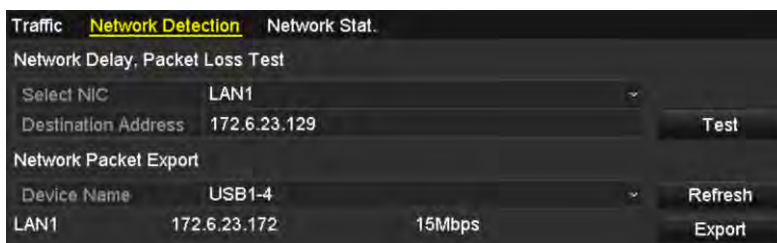


Figure 11. 28 Network Detection Interface

3. Enter the destination address in the text field of **Destination Address**.
4. Click **Test** button to start testing network delay and packet loss. The testing result pops up on the window. If the testing is failed, the error message box will pop up as well. Refer to Figure 11. 29.

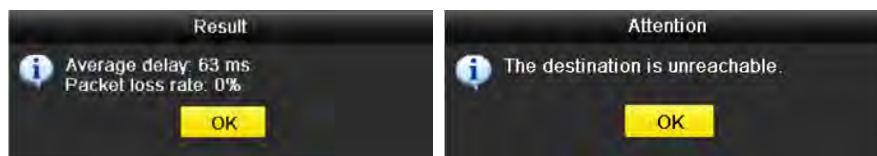


Figure 11. 29 Testing Result of Network Delay and Packet Loss

### 11.4.2 Exporting Network Packet

#### *Purpose:*

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

#### *Steps:*

1. Enter the Network Traffic interface.  
Menu > Maintenance > Net Detect
2. Click the **Network Detection** tab to enter the Network Detection interface.
3. Select the backup device from the dropdown list of Device Name, as shown in Figure 11. 30.



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.

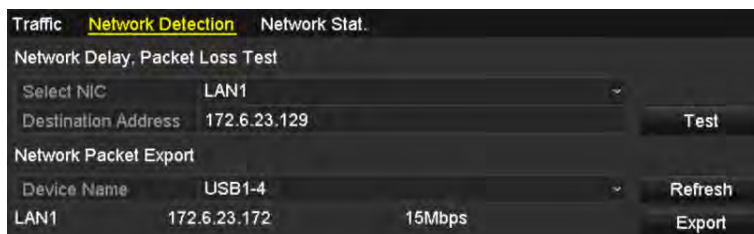


Figure 11. 30 Export Network Packet

4. Click **Export** button to start exporting.
5. After the exporting is complete, click **OK** to finish the packet export, as shown in Figure 11. 31.

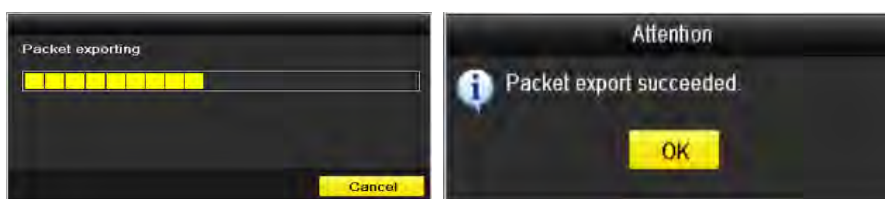


Figure 11. 31 Packet Export Attention



Up to 1M data can be exported each time.

### 11.4.3 Checking the Network Status

**Purpose:**

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

**Step:**

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

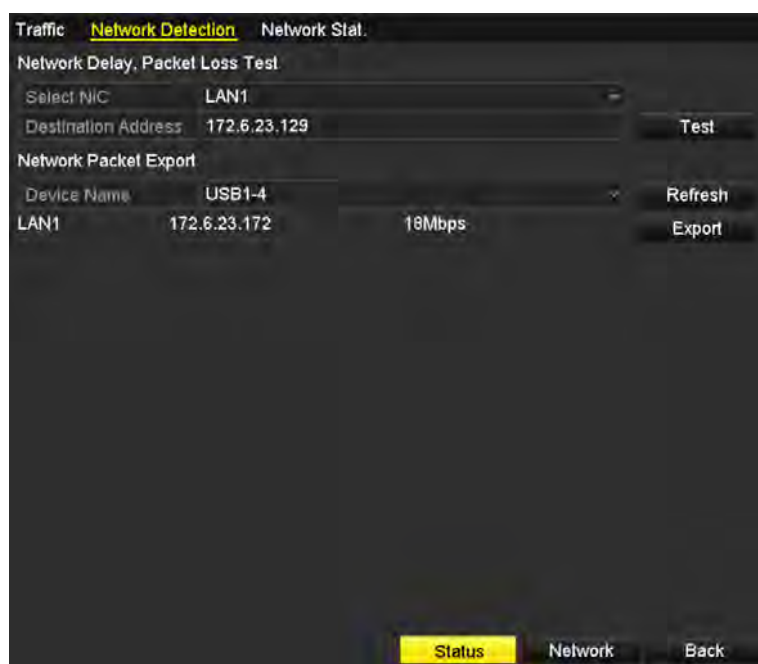


Figure 11. 32 Network Status Checking

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

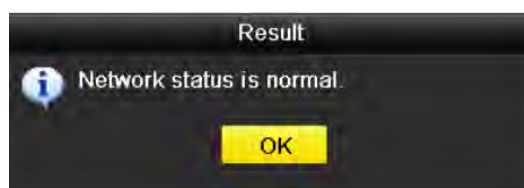


Figure 11. 33 Network status checking result

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

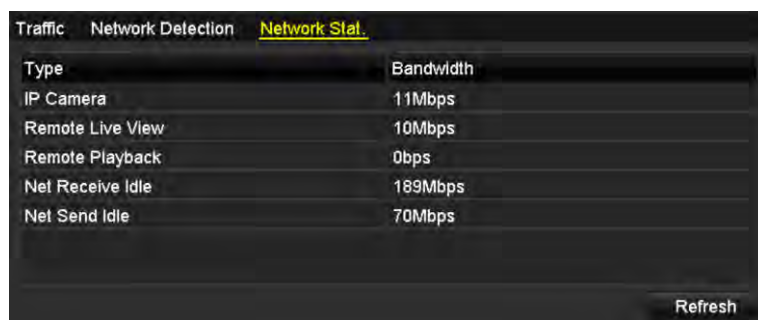
## 11.4.4 Checking Network Statistics

### *Purpose:*

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

### *Steps:*

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



The screenshot shows a web interface with three tabs: 'Traffic', 'Network Detection', and 'Network Stat.'. The 'Network Stat.' tab is selected and highlighted in yellow. Below the tabs is a table with two columns: 'Type' and 'Bandwidth'. The table contains five rows of data. At the bottom right of the table area is a 'Refresh' button.

Type	Bandwidth
IP Camera	11Mbps
Remote Live View	10Mbps
Remote Playback	0bps
Net Receive Idle	189Mbps
Net Send Idle	70Mbps

Refresh

Figure 11. 34 Network Stat. Interface

---

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

## **Chapter 12 HDD Management**



## 12.1 Initializing HDDs

### Purpose:

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



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



Figure 12.1 Message Box of Uninitialized HDD

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

### Steps:

1. Enter the HDD Information interface.

Menu > HDD > General

HDD Information							
<input type="checkbox"/> L...	Capacity	Status	Property	Type	Free Space	Gr...	Edit D...
<input checked="" type="checkbox"/> 1	465.76GB	Normal	R/W	Local	305GB	1	—

Figure 12.2 HDD Information Interface

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

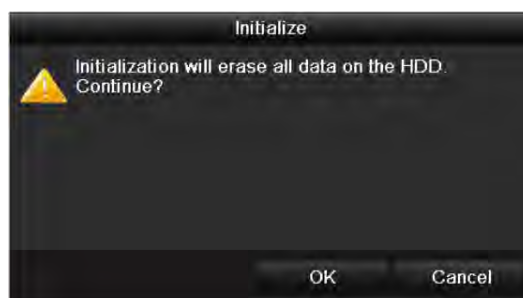


Figure 12.3 Confirm Initialization

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

HDD Information							
<input type="checkbox"/> L...	Capacity	Status	Property	Type	Free Space	Gr...	Edit D...
<input checked="" type="checkbox"/> 1	465.76GB	Initializing 20%	R/W	Local	0MB	1	—

Figure 12.4 Status changes to Initializing

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

**HDD Information**

<input type="checkbox"/> L...	Capacity	Status	Property	Type	Free Space	Gr...	Edit	D...
<input checked="" type="checkbox"/> 1	465.76GB	Normal	R/W	Local	465GB	1	—	—

Figure 12. 5 HDD Status Changes to Normal

---



Initializing the HDD will erase all data on it.

## 12.2 Managing Network HDD

### Purpose:

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

### Steps:

1. Enter the HDD Information interface.

Menu > HDD>General



<input type="checkbox"/> L...	Capacity	Status	Property	Type	Free Space	Gr...	Edit	D...
<input checked="" type="checkbox"/> 1	465.76GB	Normal	R/W	Local	305GB	1		—
<input checked="" type="checkbox"/> 2	931.51GB	Normal	R/W	Local	814GB	1		—

Figure 12. 6 HDD Information Interface

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



Add NetHDD

NetHDD: NetHDD 1

Type: NAS

NetHDD IP Address:

NetHDD Directory:

OK Cancel

Figure 12. 7 HDD Information Interface

3. Add the allocated NetHDD.
4. Select the type to NAS or IP SAN.
5. Configure the NAS or IP SAN settings.
  - **Add NAS disk:**
    - 1) Enter the NetHDD IP address in the text field.
    - 2) Click the **Search** button to search the available NAS disks.
    - 3) Select the NAS disk from the list shown below.  
Or you can just manually enter the directory in the text field of NetHDD Directory.
    - 4) Click the **OK** button to add the configured NAS disk.



Up to 8 NAS disks can be added.



Figure 12. 8 Add NAS Disk

- **Add IP SAN:**

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



Up to 1 IP SAN disk can be added.



Figure 12. 9 Add IP SAN Disk

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



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

**HDD Information**



<input type="checkbox"/> L...	Capacity	Status	Property	Type	Free Space	Gr...	Edit	D...
<input type="checkbox"/> 1	465.76GB	Normal	R/W	Local	465GB	1	—	—
<input type="checkbox"/> 6	931.51GB	Normal	R/W	Local	814GB	1	—	—
<input type="checkbox"/> 17	20.448MB	Normal	R/W	NAS	19,456MB	1		

Figure 12. 10 Initialize Added NetHDD

---

## 12.3 Managing HDD Group

### 12.3.1 Setting HDD Groups

**Purpose:**

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

**Steps:**

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

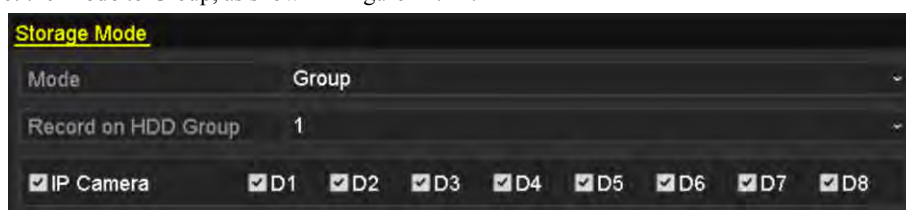


Figure 12. 11 Storage Mode Interface

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

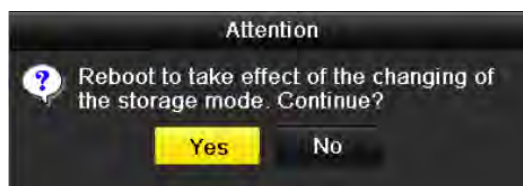


Figure 12. 12 Attention for Reboot


4. Click the **Yes** button to reboot the device to activate the changes.
5. After reboot of device, enter the HDD Information interface.  
Menu > HDD> General
6. Select HDD from the list and click  icon to enter the Local HDD Settings interface, as shown in Figure 12. 13.



Figure 12.13 Local HDD Settings Interface

7. Select the Group number for the current HDD.



The default group No. for each HDD is 1.

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

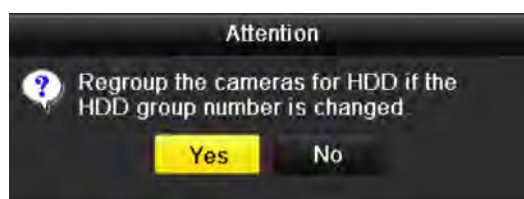


Figure 12.14 Confirm HDD Group Settings

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

## 12.3.2 Setting HDD Property

### **Purpose:**

The HDD property can be set to redundancy, read-only or read/write (R/W). Before setting the HDD property, please set the storage mode to Group (refer to step1-4 of *Chapter 12.3.1 Setting HDD Groups* ).

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

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

### **Steps:**


1. Enter the HDD Information interface.  
Menu > HDD> General
2. Select HDD from the list and click the  icon to enter the Local HDD Settings interface, as shown in Figure 12.15.



Figure 12. 15 Set HDD Property

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



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



## 12.4 Configuring Quota Mode

### Purpose:

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

### Steps:

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



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

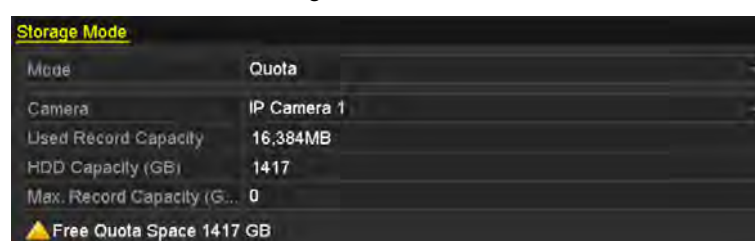


Figure 12. 16 Storage Mode Settings Interface

3. Select a camera for which you want to configure quota.
4. Enter the storage capacity in the text fields of **Max. Record Capacity (GB)**.
5. You can copy the quota settings of the current camera to other cameras if required. Click the **Copy** button to enter the Copy Camera menu, as shown in Figure 12. 17.



Figure 12. 17 Copy Settings to Other Camera(s)

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



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

## 12.5 Checking HDD Status

### Purpose:

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

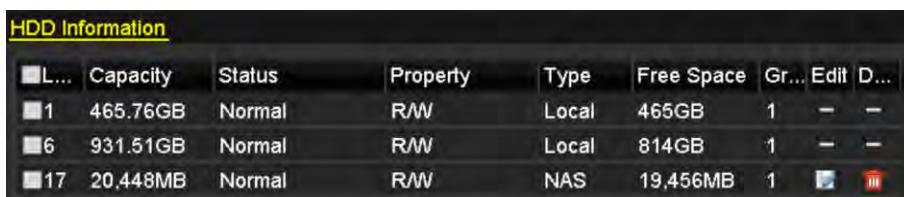
### Checking HDD Status in HDD Information Interface

#### Steps:

1. Enter the HDD Information interface.

Menu > HDD>General

2. Check the status of each HDD which is displayed on the list, as shown in Figure 12. 18.



L...	Capacity	Status	Property	Type	Free Space	Gr...	Edit	D...
1	465.76GB	Normal	R/W	Local	465GB	1	—	—
6	931.51GB	Normal	R/W	Local	814GB	1	—	—
17	20.448MB	Normal	R/W	NAS	19,456MB	1		

Figure 12. 18 View HDD Status (1)



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

### Checking HDD Status in HDD Information Interface

#### Steps:

1. Enter the System Information interface.

Menu > Maintenance > System Info

2. Click the **HDD** tab to view the status of each HDD displayed on the list, as shown in Figure 12. 19.



Label	Status	Capacity	Free Space	Property	Type	Group
1	Normal	465.76GB	465GB	R/W	Local	1
6	Normal	931.51GB	814GB	R/W	Local	1
17	Normal	20.448MB	19.456MB	R/W	NAS	1

Total Capacity	1.417GB
Free Space	1.298GB

Figure 12. 19 View HDD Status (2)

## 12.6 HDD Detection

### Purpose:

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

### S.M.A.R.T. Settings

#### Steps:

1. Enter the S.M.A.R.T. Settings interface.  
Menu > Maintenance > HDD Detect
2. Select the HDD to view its S.M.A.R.T. information list, as shown in Figure 12. 20.

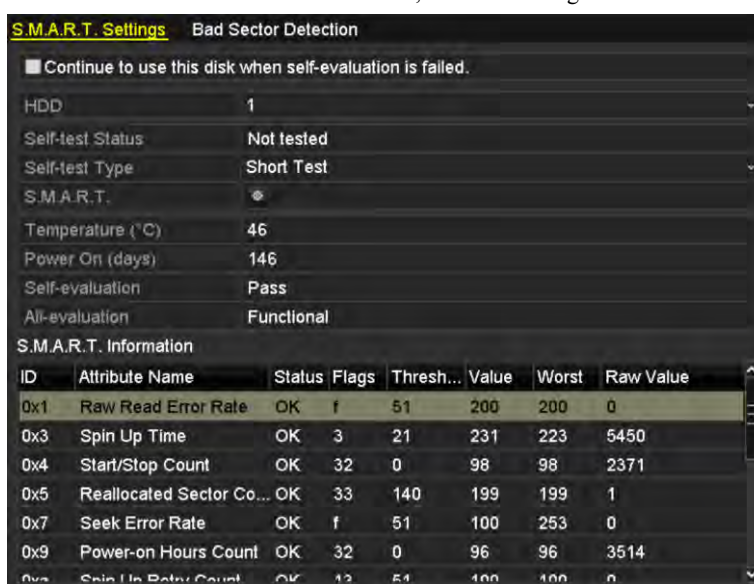


Figure 12. 20 S.M.A.R.T. Settings Interface

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

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

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



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

### Bad Sector Detection

#### Steps:

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

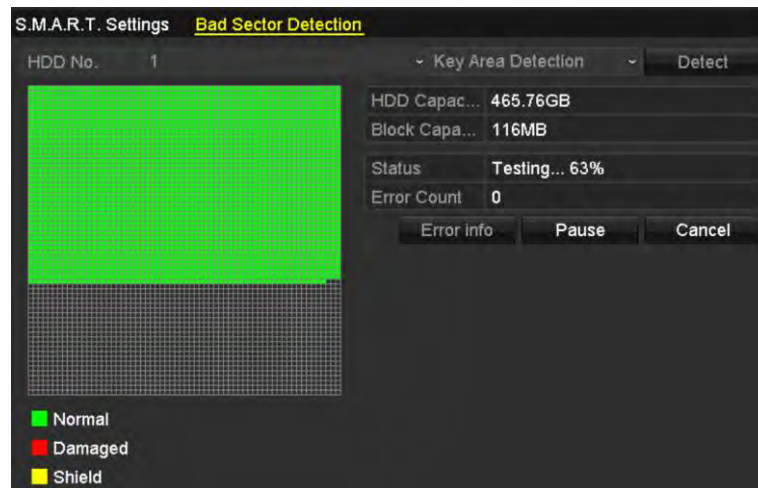


Figure 12. 21 Bad Sector Detection

---

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

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

## 12.7 Configuring HDD Error Alarms

### Purpose:

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

### Steps:

1. Enter the Exception interface.  
Menu > Configuration > Exceptions
2. Select the Exception Type to **HDD Error** from the dropdown list.
3. Click the checkbox(s) below to select the HDD error alarm type (s), as shown in Figure 12. 22.



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*.

Alarm Output No.	Alarm Name
<input type="checkbox"/> Local->1	
<input type="checkbox"/> Local->2	
<input type="checkbox"/> Local->3	
<input type="checkbox"/> Local->4	
<input checked="" type="checkbox"/> 172.6.23.105:8000->1	

Figure 12. 22 Configure HDD Error Alarm

4. When the Trigger Alarm Output is selected, you can also select the alarm output to be triggered from the list below.
5. Click the **Apply** button to save the settings

## **Chapter 13    Camera Settings**

## 13.1 Configuring OSD Settings

### *Purpose:*

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

### *Steps:*

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

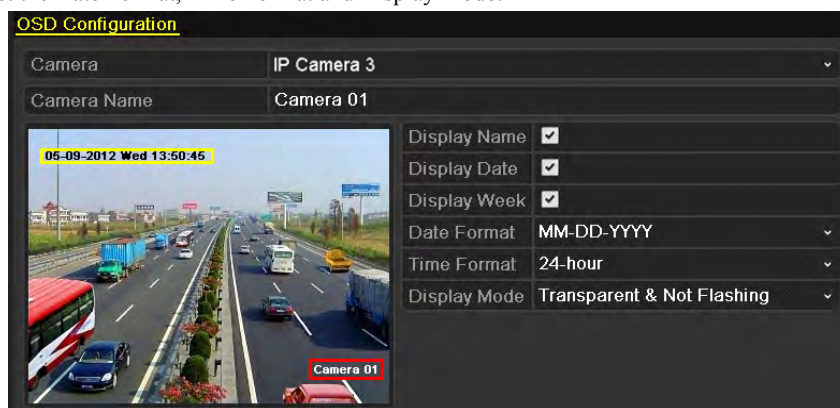


Figure 13. 1 OSD Configuration Interface

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

## 13.2 Configuring Privacy Mask

### *Purpose:*

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

### *Steps:*

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



Figure 13. 2 Privacy Mask Settings Interface

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



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

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



Figure 13. 3 Set Privacy Mask Area

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



## 13.3 Configuring Video Parameters

### *Purpose:*

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

### *Steps:*

1. Enter the Image Settings interface.

Menu > Camera > Image

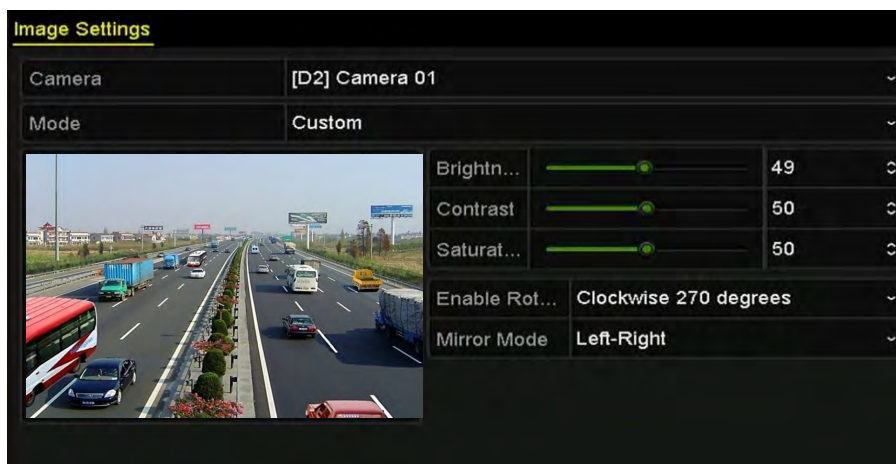


Figure 13. 4 Image Settings Interface

2. Select the camera to set image parameters.
3. Adjust the slider or click on the up/down arrow to set the value of the brightness, contrast or saturation.
4. Select the **Enable Rotate** function to Clockwise 270 degrees or OFF. When OFF is selected, the image is restored to original.
5. Select the **Mirror Mode** to Left-Right, Up-Down, Center or OFF. When OFF is selected, the image is restored to original.



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

# **Chapter 14 NVR Management and Maintenance**

## 14.1 Viewing System Information

*Steps:*

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



Figure 14. 1 Device Information Interface

---

## 14.2 Searching & Export Log Files

### *Purpose:*

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

### *Steps:*

1. Enter the Log Search interface.

Menu > Maintenance > Log Information

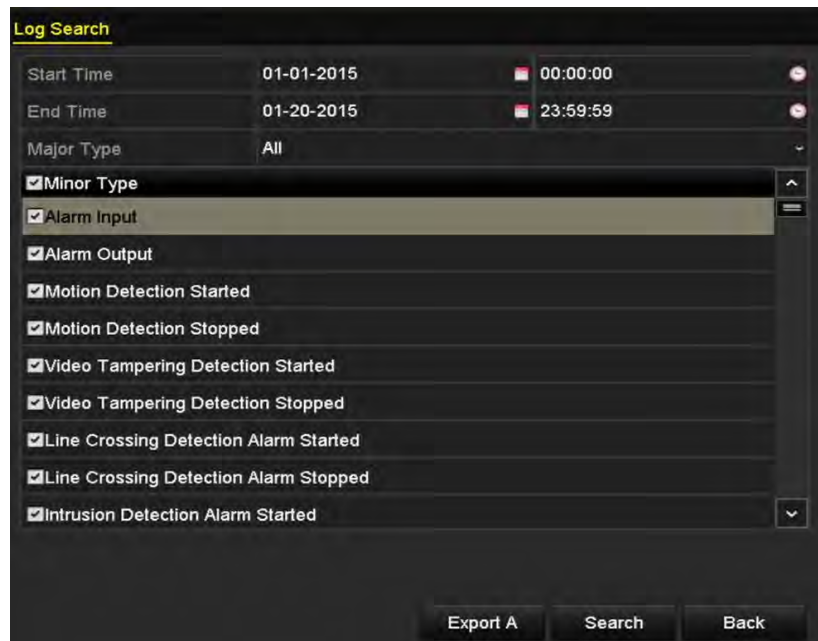


Figure 14. 2 Log Search Interface

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



No.	Major Type	Time	Minor Type	Parameter	Play	Details
1	Operation	01-14-2015 21:04:06	Abnormal Shutd...	N/A	—	✓
2	Operation	01-14-2015 21:04:08	Power On	N/A	—	✓
3	Exception	01-14-2015 21:04:08	Record Exception	N/A	⏮	✓
4	Operation	01-14-2015 21:11:44	Local Operation:...	N/A	—	✓
5	Operation	01-14-2015 21:39:45	Power On	N/A	—	✓
6	Exception	01-14-2015 21:39:47	Record Exception	N/A	⏮	✓
7	Operation	01-14-2015 21:44:05	Abnormal Shutd...	N/A	—	✓
8	Operation	01-14-2015 21:44:06	Power On	N/A	—	✓
9	Exception	01-14-2015 21:44:07	Record Exception	N/A	⏮	✓
10	Operation	01-14-2015 21:57:06	Abnormal Shutd...	N/A	—	✓



Total: 985 P: 1/10

Export Back

Figure 14. 3 Log Search Results



Up to 2000 log files can be displayed each time.

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



Time	01-14-2015 21:57:08
Type	Operation--Power On
Local User	N/A
Host IP Address	N/A
Parameter Type	N/A
Camera No.	N/A
Description:	
Model:	DS-96128N-H16
Serial No.:	DS-96128N-H161620141222CCRR201412224WCVU
Firmware version:	V3.2.0, Build 150109
Encoding version:	V1.0, Build 150108

Previous Next OK

Figure 14. 4 Log Details

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



Figure 14. 5 Export Log Files

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

You can click the **New Folder** button to create new folder in the backup device, or click the **Format** button to format the backup device before log export.



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

## 14.3 Importing/Exporting IP Camera Info

### *Purpose:*

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

### *Steps:*

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

## 14.4 Importing/Exporting Configuration Files

### *Purpose:*

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

### *Steps:*

1. Enter the Import/Export Configuration File interface.

Menu > Maintenance > Import/Export



Figure 14. 6 Import/Export Config File

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



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



## 14.5 Upgrading System

### *Purpose:*

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

### 14.5.1 Upgrading by Local Backup Device

#### *Steps:*

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

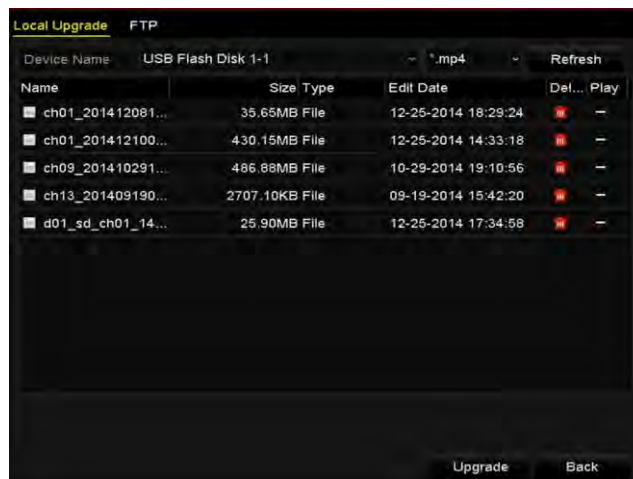


Figure 14. 7 Local Upgrade Interface

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

### 14.5.2 Upgrading by FTP

#### *Purpose:*

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



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

#### *Steps:*

1. Enter the Upgrade interface.

Menu > Maintenance > Upgrade

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

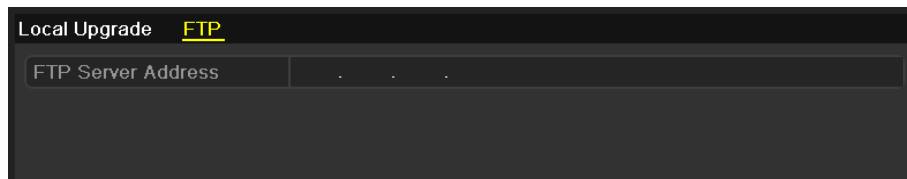


Figure 14. 8 FTP Upgrade Interface

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

## 14.6 Restoring Default Settings

### Steps:

1. Enter the Default interface.

Menu > Maintenance > Default

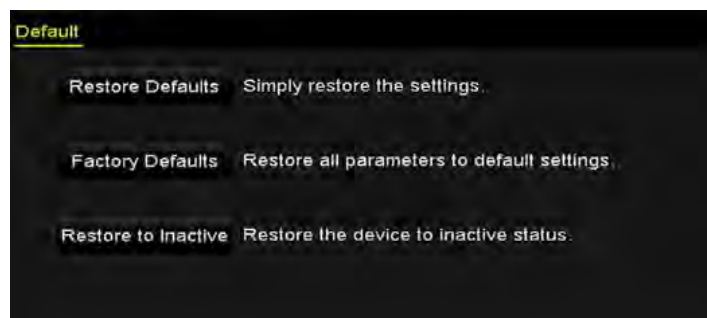


Figure 14. 9 Restore Defaults

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

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

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

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

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



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

## **Chapter 15   Others**

## 15.1 Configuring RS-232 Serial Port



The RS-232 is provided by the DS-8600NI-E8 and DS-7700NI-E4 series NVR only.

**Purpose:**

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

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

**Steps:**

1. Enter the RS-232 Settings interface.

Menu >Configuration> RS-232

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

Figure 15. 1 RS-232 Settings Interface

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

## 15.2 Configuring General Settings

### Purpose:

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

### Steps:

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

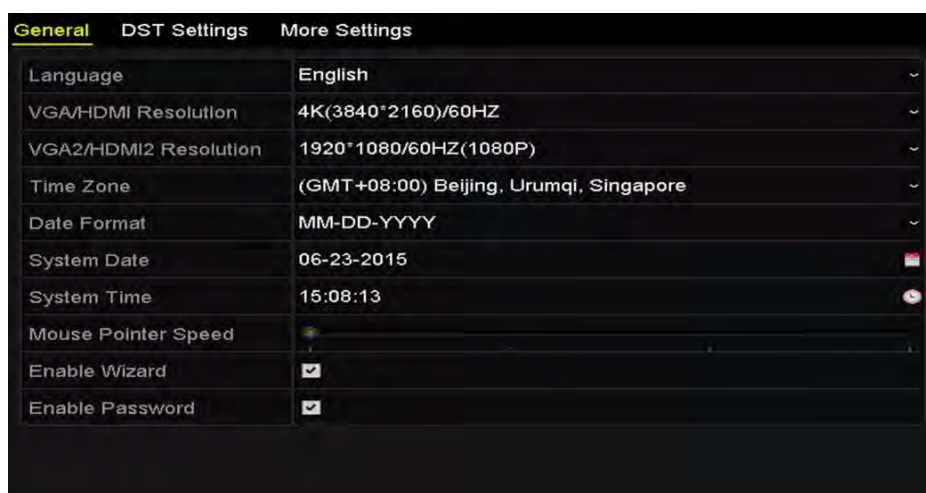


Figure 15. 2 General Settings Interface (DS-8600NI)



Figure 15. 3 General Settings Interface (DS-7600NI and DS-7700NI)

3. Configure the following settings:
  - **Language:** The default language used is *English*.

- **Resolution:** For DS-8600NI series NVR, you can configure the VGA/HDMI resolution and VGA2/HDMI 2 resolution. And up to 4K ( $3840 \times 2160$ ) resolution is selectable for the VGA/HDMI output.

For the DS-7600NI and DS-7700NI series NVR, you can configure the VGA resolution and HDMI resolution respectively. And up to 4K ( $3840 \times 2160$ ) resolution is selectable for the HDMI output.

- **Time Zone:** Select the time zone.
- **Date Format:** Select the date format.
- **System Date:** Select the system date.
- **System Time:** Select the system time.
- **Mouse Pointer Speed:** Set the speed of mouse pointer; 4 levels are configurable.
- **Enable Wizard:** Enable/disable the Wizard when the device starts up.
- **Enable Password:** Enable/disable the use of the login password.

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

## 15.3 Configuring DST Settings

### Steps:

1. Enter the General Settings interface.

Menu >Configuration>General

2. Choose **DST Settings** tab.

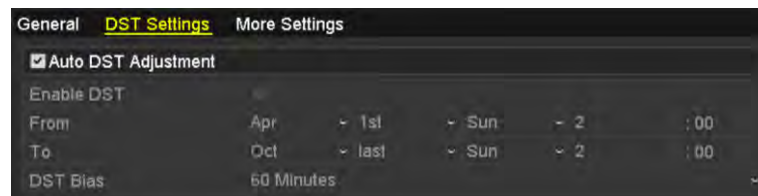


Figure 15. 4 DST Settings Interface

---

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

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



## 15.4 Configuring More Settings for Device Parameters

### Steps:

1. Enter the General Settings interface.

Menu > Configuration > General

2. Click the **More Settings** tab to enter the More Settings interface, as shown in Figure 15. 5.

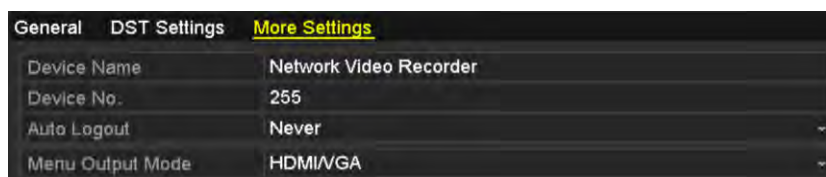


Figure 15. 5 More Settings Interface

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

## 15.5 Managing User Accounts

### *Purpose:*

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

### 15.5.1 Adding a User

#### *Steps:*

1. Enter the User Management interface.

Menu > Configuration > User

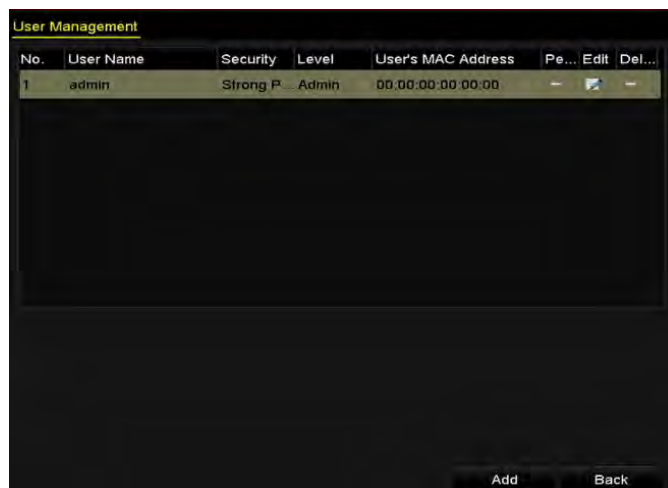


Figure 15. 6 User Management Interface

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

The screenshot shows the 'Add User' form. It has the following fields and values: 'User Name' is 1, 'Admin Password' is masked with asterisks, 'Password' is masked with asterisks and has a green 'Strong' indicator, 'Confirm' is masked with asterisks, 'Level' is set to 'Operator' with a dropdown arrow, and 'User's MAC Address' is 00 :00 :00 :00 :00 :00. At the bottom, there is a green checkmark icon and a message: 'Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.' Below the message are 'OK' and 'Cancel' buttons.

Figure 15. 7 Add User Menu

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.



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

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

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

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

4. Click the **OK** button to save the settings and go back to the User Management interface. The added new user will be displayed on the list, as shown in Figure 15. 8.

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

Figure 15. 8 Added User Listed in User Management Interface

5. Select the user from the list and then click the button to enter the Permission settings interface, as shown in Figure 15. 9.



Figure 15. 9 User Permission Settings Interface

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

**Local Configuration**

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

**Remote Configuration**

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

**Camera Configuration**

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

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

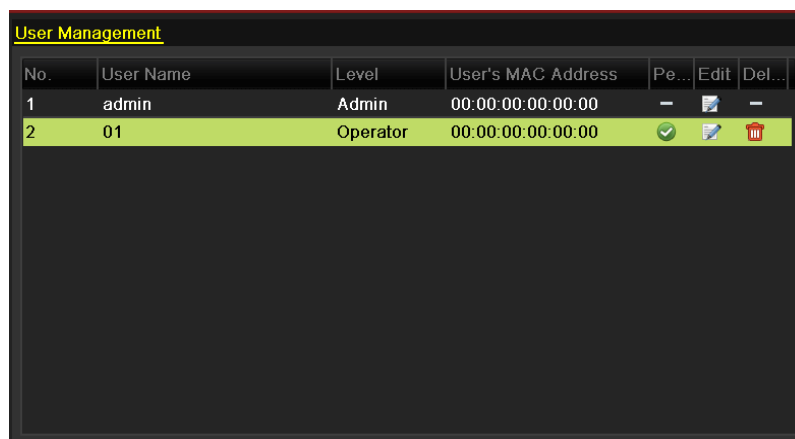


Only the *admin* user account has the permission of restoring factory default parameters.

## 15.5.2 Deleting a User


**Steps:**

1. Enter the User Management interface.  
Menu > Configuration > User
2. Select the user to be deleted from the list, as shown in Figure 15. 10.



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


Figure 15. 10 User List

- Click the  icon to delete the selected user account.

### 15.5.3 Editing a User

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

**Steps:**

- Enter the User Management interface.  
Menu > Configuration > User
- Select the user to be edited from the list, as shown in Figure 15. 10.
- Click the  icon to enter the Edit User interface, as shown in Figure 15.11.



Edit User	
User Name	example1
Change Password	<input checked="" type="checkbox"/>
Password	***** <span>Strong</span>
Confirm	*****
Level	Operator
User's MAC Address	00 : 00 : 00 : 00 : 00 : 00

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

OK Cancel

Figure 15. 11 Edit User (Operator/Guest)

Figure 15. 12 Edit User (admin)

4. Edit the corresponding parameters.


- **Operator and Guest**

You can edit the user information, including user name, password, permission level and MAC address.

Check the checkbox of **Change Password** if you want to change the password, and input the new password in the text field of **Password** and **Confirm**. A strong password is recommended.

- **Admin**

You are only allowed to edit the password and MAC address. Check the checkbox of **Change Password** if you want to change the password, and the input the correct old password, and the new password in the text field of **Password** and **Confirm**.

 **STRONG PASSWORD RECOMMENDED**—We highly recommend you create a strong password of your own choosing (Using a minimum of 8 characters, including 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.

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.



Please refer to *Chapter 2.3.1 Configuring the Unlock Pattern* for detailed instructions.

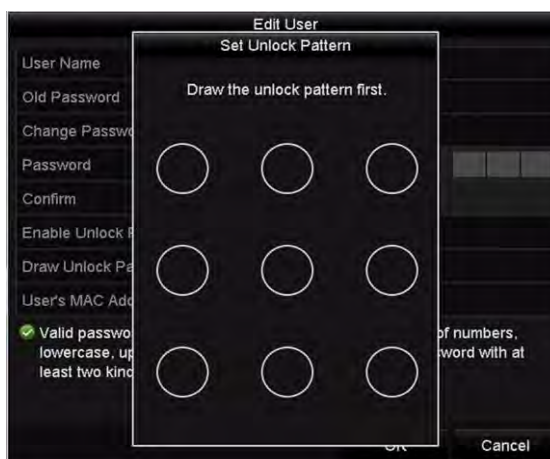




Figure 15. 13 Set Unlock Patter for Admin User

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 2.1.5Resetting Your Password for details.
7. Click the **OK** button to save the settings and exit the menu.
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

### DS-7600NI-E1

Model		DS-7604NI-E1	DS-7608NI-E1	DS-7616NI-E1
Video/Audio input	IP video input	4-ch	8-ch	16-ch
	Two-way audio input	1-ch, RCA (2.0 Vp-p, 1kΩ)		
Network	Incoming bandwidth	40 Mbps	80 Mbps	160 Mbps
	Outgoing bandwidth	80 Mbps		
	Remote connection	32	32	128
Video/Audio output	Recording resolution	6MP/5MP/4MP/3MP/1080p/UXGA/720p/VGA/4CIF/DCIF/2CIF/CIF/QCIF		
	Frame rate	Main stream: 50 fps (P)/60 fps (N)		
		Sub-stream: 50 fps (P)/60 fps (N)		
	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, 1kΩ)		
Decoding	Live view/Playback resolution	6MP/5MP/3MP/1080p/UXGA/720p/VGA/4CIF/DCIF/2CIF/CIF/QCIF		
	Capability	4-ch@1080p	8-ch@720p, 5-ch@1080p	16-ch@4CIF, 12-ch@720p, 6-ch@1080p
Network management	Network protocols	TCP/IP, DHCP, Hik-Connect, DNS, DDNS, NTP, SADP, SMTP, NFS, iSCSI, UPnP™, HTTPS		
Hard disk	SATA	1 SATA interface for 1 HDD		
	Capacity	Up to 4TB for each disk		
External interface	Network interface	1 RJ-45 10/100/1000 Mbps self-adaptive Ethernet interface		
	USB interface	1 × USB 2.0 and 1 × USB 3.0		
	Alarm in/out (Optional)	4/1		
General	Power supply	12 VDC		
	Consumption (without hard disk)	≤ 10 W		
	Working temperature	-10 °C to +55 °C (+14 °F to +131 °F)		
	Working humidity	10 % to 90 %		
	Chassis	Standalone 1U chassis		
	Dimensions (W × D × H)	315 × 240 × 48 mm (12.4" × 9.4" × 1.9")		
	Weight (without hard disk)	≤ 1 kg (2.2 lb)		

## DS-7600NI-E2

Model		DS-7608NI-E2	DS-7616NI-E2	DS-7632NI-E2
Video/Audio input	IP video input	8-ch	16-ch	32-ch
	Two-way audio	1-ch, RCA (2.0 Vp-p, 1kΩ)		
Network	Incoming bandwidth	80 Mbps	160 Mbps	160 Mbps
	Outgoing bandwidth	80 Mbps		
	Remote connection	32	128	
Video/Audio output	Recording resolution	6MP/5MP/4MP/3MP/1080p/UXGA/720p/VGA/4CIF/DCIF/2CIF/CIF/QCIF		
	Frame rate	Main stream: 50 fps (P)/60 fps (N)		
		Sub-stream: 50 fps (P)/60 fps (N)		
	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, 1kΩ)			
Decoding	Live view/Playback resolution	6MP/5MP/3MP/1080p/UXGA/720p/VGA/4CIF/DCIF/2CIF/CIF/QCIF		
	Capability	8-ch@720p, 5-ch@1080p	16-ch@4CIF, 12-ch@720p, 6-ch@1080p	
Network management	Network protocols	TCP/IP, DHCP, Hik-Connect, DNS, DDNS, NTP, SADP, SMTP, NFS, iSCSI, UPnP™, HTTPS		
Hard disk	SATA	2 SATA interfaces for 2 HDDs		
	Capacity	Up to 4TB for each disk		
External interface	Network interface	1 RJ-45 10/100/1000 Mbps self-adaptive Ethernet interface		
	USB interface	1 × USB 2.0 and 1 × USB 3.0		
	Alarm in/out (Optional)	4/1		
General	Power supply	12 VDC		
	Consumption (without hard disk)	≤ 10 W		
	Working temperature	-10 °C to +55 °C (+14 °F to +131 °F)		
	Working humidity	10 % to 90 %		
	Chassis	385 mm chassis		
	Dimensions (W × D × H)	385 × 315× 52 mm (15.2" × 12.4" × 2.0")		
	Weight (without hard disk)	≤ 1 kg (2.2 lb)		

**DS-7700NI-E4/P**

Model		DS-7708NI-E4/8P	DS-7716NI-E4/16P	DS-7732NI-E4/16P
Video/Audio input	IP video input	8-ch	16-ch	32-ch
	Two-way audio	1-ch, RCA (2.0 Vp-p, 1kΩ)		
Network	Incoming bandwidth	80 Mbps	160 Mbps	160 Mbps
	Outgoing bandwidth	80 Mbps		
	Remote connection	32	128	
Video/Audio output	Recording resolution	6MP/5MP/4MP/3MP/1080p/UXGA/720p/VGA/4CIF/DCIF/2CIF/CIF/QCIF		
	Frame rate	Main stream: 50 fps (P)/60 fps (N)		
		Sub-stream: 50 fps (P)/60 fps (N)		
	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, 1kΩ)			
Decoding	Live view/Playback resolution	6MP/5MP/3MP/1080p/UXGA/720p/VGA/4CIF/DCIF/2CIF/CIF/QCIF		
	Capability	8-ch@720p, 5-ch@1080p	16-ch@4CIF, 12-ch@720p, 6-ch@1080p	
Network management	Network protocols	TCP/IP, DHCP, Hik-Connect, DNS, DDNS, NTP, SADP, SMTP, NFS, iSCSI, UPnP™, HTTPS		
Hard disk	SATA	4 SATA interfaces for 2 HDDs + 1 DVD-R/W (default), or 4HDDs		
	eSATA (Optional)	1 eSATA interface		
	Capacity	Up to 6TB capacity for each HDD		
External interface	Network interface	1 RJ-45 10/100/1000 Mbps self-adaptive Ethernet interface		
	Serial interface	RS-232 and RS-485		
	USB interface	2 × USB 2.0 and 1 × USB 3.0		
	Alarm in/out	16/4 (optionally can be expanded to 16/8)		
PoE	Interface	8 independent 100 Mbps PoE network interfaces	16 independent 100 Mbps PoE network interfaces	
	Max. Power	200 W		
	Supported standard	AF and AT		
General	Power supply	100 to 240 VAC		
	Consumption (without hard disk, DVD-R/W or PoE)	≤ 20 W		
	Working temperature	-10℃ to +55℃ (14 °F to 131 F )		
	Working humidity	10 % to 90 %		
	Chassis	19-inch rack-mounted 1.5U chassis		
	Dimensions (W × D × H)	445 × 400 × 71 mm (17.5" × 15.7" × 2.8")		
	Weight (without hard disk or DVD-R/W)	≤ 4 kg (8.82 lb)		

## DS-7700NI-E4

Model		DS-7708NI-E4	DS-7716NI-E4	DS-7732NI-E4
Video/Audio input	IP video input	8-ch	16-ch	32-ch
	Two-way audio	1-ch, RCA (2.0 Vp-p, 1kΩ)		
Network	Incoming bandwidth	80 Mbps	160 Mbps	160 Mbps
	Outgoing bandwidth	80 Mbps		
	Remote connection	32	128	
Video/Audio output	Recording resolution	6MP/5MP/4MP/3MP/1080p/UXGA/720p/VGA/4CIF/DCIF/2CIF/CIF/QCIF		
	Frame rate	Main stream: 50 fps (P)/60 fps (N)		
		Sub-stream: 50 fps (P)/60 fps (N)		
	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, 1kΩ)			
Decoding	Live view/Playback resolution	6MP/5MP/3MP/1080p/UXGA/720p/VGA/4CIF/DCIF/2CIF/CIF/QCIF		
	Capability	8-ch@720p, 5-ch@1080p	16-ch@4CIF, 12-ch@720p, 6-ch@1080p	
Network management	Network protocols	TCP/IP, DHCP, Hik-Connect, DNS, DDNS, NTP, SADP, SMTP, NFS, iSCSI, UPnP™, HTTPS		
Hard disk	SATA	4 SATA interfaces for 2 HDDs + 1 DVD-R/W (default), or 4 HDDs		
	eSATA (Optional)	1 eSATA interface		
	Capacity	Up to 6TB capacity for each HDD		
External interface	Network interface	2 RJ-45 10/100/1000 Mbps self-adaptive Ethernet interfaces		
	Serial interface	RS-232 and RS-485		
	USB interface	2 × USB 2.0 and 1 × USB 3.0		
	Alarm in/out	16/4 (optionally can be expanded to 16/8)		
General	Power supply	100 to 240 VAC		
	Consumption (without hard disk or DVD-R/W)	≤ 20 W	≤ 20 W	≤ 20 W
	Working temperature	-10℃ to +55℃ (14 °F to 131°F )		
	Working humidity	10 % to 90 %		
	Chassis	19-inch rack-mounted 1.5U chassis		
	Dimensions (W × D × H)	445 × 400 × 71 mm (17.5" × 15.7" × 2.8")		
	Weight (without hard disk or DVD-R/W)	≤ 4 kg (8.82 lb)		

## DS-8600NI-E8

Model		DS-8608NI-E8	DS-8616NI-E8	DS-8632NI-E8
Video/Audio input	IP video input	8-ch	16-ch	32-ch
	Two-way audio	1-ch, RCA (2.0 Vp-p, 1kΩ)		
Network	Incoming bandwidth	80 Mbps	160 Mbps	160 Mbps
	Outgoing bandwidth	80 Mbps		
	Remote connection	32	128	
Video/Audio output	Recording resolution	6MP/5MP/4MP/3MP/1080p/UXGA/720p/VGA/4CIF/DCIF/2CIF/CIF/QCIF		
	Frame rate	Main stream: 50 fps (P)/60 fps (N)		
		Sub-stream: 50 fps (P)/60 fps (N)		
	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, 1kΩ)		
Decoding	Live view/Playback resolution	6MP/5MP/3MP/1080p/UXGA/720p/VGA/4CIF/DCIF/2CIF/CIF/QCIF		
	Capability	8-ch@720p, 5-ch@1080p	16-ch@4CIF, 12-ch@720p, 6-ch@1080p	
Network management	Network protocols	TCP/IP, DHCP, Hik-Connect, DNS, DDNS, NTP, SADP, SMTP, NFS, iSCSI, UPnP™, HTTPS		
Hard disk	SATA	8 SATA interfaces for 4 HDDs + 1 DVD-R/W (default), or 8 HDDs		
	eSATA (Optional)	1 eSATA interface		
	Capacity	Up to 6TB capacity for each HDD		
External interface	Network interface	2 RJ-45 10/100/1000 Mbps self-adaptive Ethernet interfaces		
	Serial interface	RS-232 and RS-485		
	USB interface	2 × USB 2.0 and 1 × USB 3.0		
	Alarm in/out	16/4 (optionally can be expanded to 16/8)		
General	Power supply	100 to 240 VAC		
	Consumption (without hard disk or DVD-R/W)	≤ 20 W	≤ 20 W	≤ 20 W
	Working temperature	-10℃ to +55℃ (14°F to 131°F )		
	Working humidity	10 % to 90 %		
	Chassis	19-inch rack-mounted 2U chassis		
	Dimensions (W × D × H)	445 × 470 × 90 mm (17.5" × 18.5" × 3.5")		
	Weight (without hard disk or DVD-R/W)	≤ 8 kg (17.6 lb)		

**DS-7604NI-E1/4N and DS-7608NI-E2/8N**

Model		DS-7604NI-E1/4N	DS-7608NI-E2/8N
Video/Audio input	IP video input	4-ch	8-ch
	Two-way audio input	1-ch, RCA (2.0 Vp-p, 1kΩ)	
Network	Incoming bandwidth	40 Mbps	80 Mbps
	Outgoing bandwidth	80 Mbps	
	Remote connection	32	
Video/Audio output	Recording resolution	6MP/5MP/4MP/3MP/1080p/UXGA/720p/VGA/4CIF/DCIF/2CIF/CIF/QCIF	
	Frame rate	Main stream: 50 fps (P)/60 fps (N)	
		Sub-stream: 50 fps (P)/60 fps (N)	
	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, 1kΩ)	
Decoding	Live view/Playback resolution	6MP/5MP/3MP/1080P/UXGA/720P/VGA/4CIF/DCIF/2CIF/CIF/QCIF	
	Capability	4-ch@1080p	8-ch@720p, 5-ch@1080p
Hard disk	SATA	1 SATA interface for 1 HDD	2 SATA interfaces for 2 HDDs
	Capacity	Up to 4TB for each disk	
Network management	Network protocols	TCP/IP, DHCP, Hik-Connect, DNS, DDNS, NTP, SADP, SMTP, NFS, iSCSI, UPnP™, HTTPS	
External interface	Network interface	1 RJ-45 10/100/1000 Mbps self-adaptive Ethernet interface	
		4 independent 100 Mbps built-in switch network interfaces	8 independent 100 Mbps built-in switch network interfaces
	USB interface	1 × USB 2.0 and 1 × USB 3.0	
	Alarm in/out (Optional)	4/1	
General	Power supply	12 VDC	
	Consumption (without hard disk)	≤ 10 W	
	Working temperature	-10℃ to +55℃ (14 °F to 131 °F )	
	Working humidity	10 % to 90 %	
	Chassis	Standalone 1U chassis	385 mm chassis
	Dimensions (W × D × H)	315 × 240 × 48 mm (12.4" × 9.4" × 1.9")	385 × 315 × 52 mm (15.2" × 12.4" × 2.0")
	Weight (without hard disk)	≤ 1 kg (2.2 lb)	

## DS-7600NI-E2/N

Model		DS-7616NI-E2/8N	DS-7632NI-E2/8N	DS-7616NI-E2/16N	DS-7632NI-E2/16N
Video/Audio input	IP video input	16-ch	32-ch	16-ch	32-ch
	Two-way audio input	1-ch, RCA (2.0 Vp-p, 1kΩ)			
Network	Incoming bandwidth	160 Mbps			
	Outgoing bandwidth	80 Mbps			
	Remote connection	128			
Video/Audio output	Recording resolution	6MP/5MP/4MP/3MP/1080p/UXGA/720p/VGA/4CIF/DCIF/2CIF/CIF/QCIF			
	Frame rate	Main stream: 50 fps (P)/60 fps (N)			
		Sub-stream: 50 fps (P)/60 fps (N)			
	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, 1kΩ)				
Decoding	Live view/Playback resolution	6MP/5MP/3MP/1080p/UXGA/720p/VGA/4CIF/DCIF/2CIF/CIF/QCIF			
	Capability	16-ch@4CIF, 12-ch@720p, 6-ch@1080p			
Network management	Network protocols	TCP/IP, DHCP, Hik-Connect, DNS, DDNS, NTP, SADP, SMTP, NFS, iSCSI, UPnP™, HTTPS			
Hard disk	SATA	2 SATA interfaces for 2 HDDs			
	Capacity	Up to 4TB for each disk			
External interface	Network interface	1 RJ-45 10/100/1000 Mbps self-adaptive Ethernet interface			
		8 independent 100 Mbps built-in switch network interfaces		16 independent 100 Mbps built-in switch network interfaces	
	USB interface	1 × USB 2.0 and 1 × USB 3.0			
	Alarm in/out (Optional)	4/1			
General	Power supply	12 VDC			
	Consumption (without hard disk)	≤ 10 W			
	Working temperature	-10℃ to +55℃ (14 °F to 131 F )			
	Working humidity	10 % to 90 %			
	Chassis	385 mm chassis			
	Dimensions (W × D × H)	385 × 315× 52 mm (15.2" × 12.4" × 2.0")			
	Weight (without hard disk)	≤ 1 kg (2.2 lb)			

## DS-7604NI-E1/4P and DS-7608NI-E2/8P

Model		DS-7604NI-E1/4P	DS-7608NI-E2/8P
Video/Audio input	IP video input	4-ch	8-ch
	Two-way audio input	1-ch, RCA (2.0 Vp-p, 1kΩ)	
Network	Incoming bandwidth	40 Mbps	80 Mbps
	Outgoing bandwidth	80 Mbps	
	Remote connection	32	
Video/Audio output	Recording resolution	6MP/5MP/4MP/3MP/1080p/UXGA/720p/VGA/4CIF/DCIF/2CIF/CIF/QCIF	
	Frame rate	Main stream: 50 fps (P)/60 fps (N)	
		Sub-stream: 50 fps (P)/60 fps (N)	
	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, 1kΩ)	
Decoding	Live view/Playback resolution	6MP/5MP/3MP/1080p/UXGA/720p/VGA/4CIF/DCIF/2CIF/CIF/QCIF	
	Capability	4-ch@1080p	8-ch@720p, 5-ch@1080p
Network management	Network protocols	TCP/IP, DHCP, Hik-Connect, DNS, DDNS, NTP, SADP, SMTP, NFS, iSCSI, UPnP™, HTTPS	
Hard disk	SATA	1 SATA interface for 1 HDD	2 SATA interfaces for 2 HDDs
	Capacity	Up to 4TB for each disk	
External interface	Network interface	1 RJ-45 10/100/1000 Mbps self-adaptive Ethernet interface	
	USB interface	1 × USB 2.0 and 1 × USB 3.0	
	Alarm in/out (Optional)	4/1	
PoE	Interface	4 independent 100 Mbps PoE network interfaces	8 independent 100 Mbps PoE network interfaces
	Max. Power	50 W	120 W
	Supported standard	AF and AT	
General	Power supply	48 VDC	100 to 240 VAC
	Consumption (without hard disk and PoE)	≤ 10 W	
	Working temperature	-10℃ to +55℃ (14 °F to 131 °F )	
	Working humidity	10 % to 90 %	
	Chassis	Standalone 1U chassis	385 mm chassis
	Dimensions (W × D × H)	315 × 240 × 48 mm (12.4" × 9.4" × 1.9")	385 × 315 × 52 mm (15.2" × 12.4" × 2.0")
	Weight (without hard disk)	≤ 1 kg (2.2 lb)	



## DS-7600NI-E2/P

Model		DS-7616NI-E2/8P	DS-7632NI-E2/8P	DS-7616NI-E2/16P	DS-7632NI-E2/16P
Video/Audio input	IP video input	16-ch	32-ch	16-ch	32-ch
	Two-way audio input	1-ch, RCA (2.0 Vp-p, 1kΩ)			
Network	Incoming bandwidth	160 Mbps			
	Outgoing bandwidth	80 Mbps			
	Remote connection	128			
Video/Audio output	Recording resolution	6MP/5MP/4MP/3MP/1080p/UXGA/720p/VGA/4CIF/DCIF/2CIF/CIF/QCIF			
	Frame rate	Main stream: 50 fps (P)/60 fps (N)			
		Sub-stream: 50 fps (P)/60 fps (N)			
	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, 1kΩ)			
Decoding	Live view/Playback resolution	6MP/5MP/3MP/1080p/UXGA/720p/VGA/4CIF/DCIF/2CIF/CIF/QCIF			
	Capability	16-ch@4CIF, 12-ch@720p, 6-ch@1080p			
Network management	Network protocols	TCP/IP, DHCP, Hik-Connect, DNS, DDNS, NTP, SADP, SMTP, NFS, iSCSI, UPnP™, HTTPS			
Hard disk	SATA	2 SATA interfaces for 2 HDDs			
	Capacity	Up to 4TB for each disk			
External interface	Network interface	1 RJ-45 10/100/1000 Mbps self-adaptive Ethernet interface			
	USB interface	1 × USB 2.0 and 1 × USB 3.0			
	Alarm in/out (Optional)	4/1			
PoE	Interface	8 independent 100 Mbps PoE network interfaces		16 independent 100 Mbps PoE network interfaces	
	Max. Power	120 W		200 W	
	Supported standard	AF and AT			
General	Power supply	100 to 240 VAC			
	Consumption (without hard disk and PoE)	≤ 10 W		≤ 15 W	
	Working temperature	-10℃ to +55℃ (14 °F to 131 °F )			
	Working humidity	10 % to 90 %			
	Chassis	385 mm chassis			
	Dimensions (W × D × H)	385 × 315× 52 mm (15.2" × 12.4" × 2.0")			
	Weight (without hard disk)	≤ 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 DVR, with the main stream having a maximum resolution of 4CIF and the sub-stream having a maximum resolution of CIF.
- **HDD:** Acronym for Hard Disk Drive. A storage medium which stores digitally encoded data on platters with magnetic surfaces.
- **DHCP:** Dynamic Host Configuration Protocol (DHCP) is a network application protocol used by devices (DHCP clients) to obtain configuration information for operation in an Internet Protocol network.
- **HTTP:** Acronym for Hypertext Transfer Protocol. A protocol to transfer hypertext request and information between servers and browsers over a network
- **DDNS:** Dynamic DNS is a method, protocol, or network service that provides the capability for a networked device, such as a router or computer system using the Internet Protocol Suite, to notify a domain name server to change, in real time (ad-hoc) the active DNS configuration of its configured hostnames, addresses or other information stored in DNS.
- **Hybrid DVR:** A hybrid DVR is a combination of a DVR and NVR.
- **NTP:** Acronym for Network Time Protocol. A protocol designed to synchronize the clocks of computers over a network.
- **NTSC:** Acronym for National Television System Committee. NTSC is an analog television standard used in such countries as the United States and Japan. Each frame of an NTSC signal contains 525 scan lines at 60Hz.
- **NVR:** Acronym for Network Video Recorder. An NVR can be a PC-based or embedded system used for centralized management and storage for IP cameras, IP Domes and other DVRs.
- **PAL:** Acronym for Phase Alternating Line. PAL is also another video standard used in broadcast televisions systems in large parts of the world. PAL signal contains 625 scan lines at 50Hz.
- **PTZ:** Acronym for Pan, Tilt, Zoom. PTZ cameras are motor driven systems that allow the camera to pan left and right, tilt up and down and zoom in and out.
- **USB:** Acronym for Universal Serial Bus. USB is a plug-and-play serial bus standard to interface devices to a host computer.

## 16.3 Troubleshooting

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

### *Possible Reasons*

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

### *Steps*

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

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

### *Possible Reasons*

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

### *Steps*

1. Verify at least one HDD is installed in the NVR.
  - 1) If not, please install the compatible HDD.

A small icon with the word "NOTE" inside a square border.

Please refer to the “Quick Operation Guide” for the HDD installation steps.
- 2) If you don't want to install a HDD, select “Menu>Configuration > Exceptions”, and uncheck the Audible Warning checkbox of “HDD Error”.
2. Verify the HDD is initialized.
  - 1) Select “Menu>HDD>General”.
  - 2) If the status of the HDD is “Uninitialized”, please check the checkbox of corresponding HDD and click the “Init” button.
3. Verify the HDD is detected or is in good condition.
  - 1) Select “Menu>HDD>General”.
  - 2) If the HDD is not detected or the status is “Abnormal”, please replace the dedicated HDD according to the requirement.
4. Check if the fault is solved by the step 1 to step 3.  
If it is solved, finish the process.  
If not, please contact the engineer from our company to do the further process.

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

**Possible Reasons**

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

**Steps**

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



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

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

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

If it is solved, finish the process.

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

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

**Possible Reasons**

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

**Steps**

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



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

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

4. Verify the switch is not flow control.

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

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

If it is solved, finish the process.

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

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

**Possible Reasons:**

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

**Steps:**

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



- The view settings can only be configured by the local operation of NVR.
  - Different camera orders and window-division modes can be set for different output interfaces separately, and digits like “D1” and “D2” stands for the channel number, and “X” means the selected window has no image output.
3. Check if the fault is solved by the above steps.
- If it is solved, finish the process.
- If not, please contact the engineer from our company to do the further process.

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

**Possible Reasons:**

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

**Steps:**

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



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

2. Verify the frame rate is real-time frame rate.
- Select “Menu > Record > Parameters > Record”, and set the Frame rate to Full Frame.
3. Check if the fault is solved by the above steps.
- If it is solved, finish the process.
- If not, please contact the engineer from our company to do the further process.

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

**Possible Reasons:**

- a) Poor network between NVR and IP camera, and there exists packet loss during the transmission.
- b) Poor network between NVR and PC, and there exists packet loss during the transmission.

- c) The performances of hardware are not good enough, including CPU, memory, etc..

**Steps:**

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



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

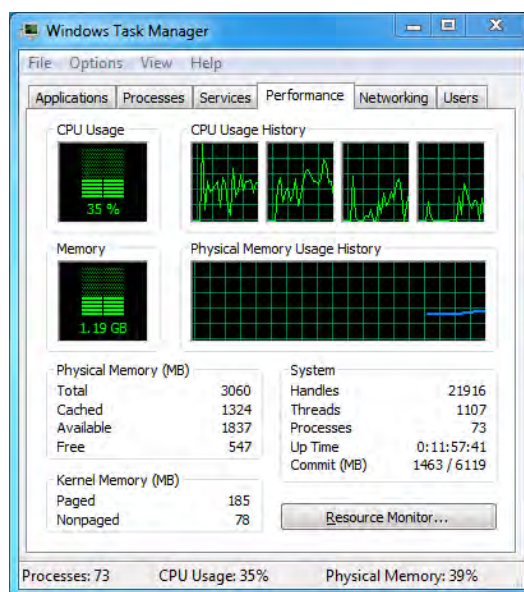
2. Verify the network between NVR and PC is connected.
  - 1) Open the cmd window in the Start menu, or you can press “windows+R” shortcut key to open it.
  - 2) Use the ping command to send large packet to the NVR, execute the command of “ping 192.168.0.0 -l 1472 -f” (the IP address may change according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



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

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

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



Windows task management interface

- Select the “Performance” tab; check the status of the CPU and Memory.
  - If the resource is not enough, please end some unnecessary processes.
4. Check if the fault is solved by the above steps.
 

If it is solved, finish the process.

If not, please contact the engineer from our company to do the further process.
- **When using the NVR to get the live view audio, there is no sound or there is too much noise, or the volume is too low.**
- Possible Reasons:**
- a) Cable between the pickup and IP camera is not connected well; impedance mismatches or incompatible.
  - b) The stream type is not set as “Video & Audio”.

- c) The encoding standard is not supported with NVR.

**Steps:**

1. Verify the cable between the pickup and IP camera is connected well; impedance matches and compatible.  
Log in the IP camera directly, and turn the audio on, check if the sound is normal. If not, please contact the manufacturer of the IP camera.
2. Verify the setting parameters are correct.  
Select “Menu > Record > Parameters > Record”, and set the Stream Type as “Audio & Video”.
3. Verify the audio encoding standard of the IP camera is supported by the NVR.  
NVR supports G722.1 and G711 standards, and if the encoding parameter of the input audio is not one of the previous two standards, you can log in the IP camera to configure it to the supported standard.
4. Check if the fault is solved by the above steps.  
If it is solved, finish the process.  
If not, please contact the engineer from our company to do the further process.

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

**Possible Reasons:**

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

**Steps:**

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



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

2. Verify the frame rate is real-time frame rate.  
Select “Menu > Record > Parameters > Record”, and set the Frame Rate to “Full Frame”.
3. Verify the hardware can afford the playback.  
Reduce the channel number of playback.  
Select “Menu > Record > Encoding > Record”, and set the resolution and bitrate to a lower level.
4. Reduce the number of local playback channel.  
Select “Menu > Playback”, and uncheck the checkbox of unnecessary channels.
5. Check if the fault is solved by the above steps.  
If it is solved, finish the process.  
If not, please contact the engineer from our company to do the further process.

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

**Possible Reasons:**

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

**Steps:**

1. Verify the system time setting is correct.  
Select “Menu > Configuration > General > General”, and verify the “Device Time” is correct.
2. Verify the search condition is correct.  
Select “Playback”, and verify the channel and time are correct.
3. Verify the HDD status is normal.  
Select “Menu > HDD > General” to view the HDD status, and verify the HDD is detected and can be read and written normally.
4. Check if the fault is solved by the above steps.  
If it is solved, finish the process.  
If not, please contact the engineer from our company to do the further process.





## 16.4 Summary of Changes

### Version 3.4.92

**Added:**

- Easy network access by Hik-Connect (Chapter 2.2 Using the Wizard for Basic Configuration, Chapter 11.2.1 Configuring Hik-Connect)

**Deleted:**

- Delete two DDNS types: IP sever and HiDDNS (Chapter 2.2 Using the Wizard for Basic Configuration, Chapter 11.2.2 Configuring DDNS)

### Version 3.4.90

**Added:**

- Reset the admin password by exporting/importing the GUID file. (Chapter 2.1.2, Chapter 2.1.4, Chapter 2.1.5, Chapter 15.5.3)
- Configurable main stream and sub-stream for the live view. (Chapter 3.1, Chapter 3.3)
- All-day continuous recording is configured by factory default. (Chapter 5.2)

**Updated:**

- Optimize the playback interface and add the configurable motion detection area for smart playback. (Chapter 6 Playback)
- Up to 2048 LRP lists supported in vehicle detection.

### Version 3.4.80

**Added:**

- Remind user to remember the password after the device is activated. (Chapter 2.2 Activating Your Device)
- One-key alarm disarming for the local alarm input 1. (Chapter 8.2 Setting Sensor Alarms)

**Updated:**

- Optimize the playback by normal/smart interface. (Chapter 6 Playback)
- Admin Password changed to Password when adding the IP camera. (Chapter 2.6 Adding and Connecting the IP Cameras)

**Deleted:**

- Delete four VCA detection types: people gathering, fast movement, parking and loitering (Chapter 10 VCA Alarm)
- Delete the PPPoE settings. (Delete Chapter 11.2.1 Configuring PPPoE Settings)

### Version 3.4.6

**Updated:**

- Update the description of IR remote control operation. (Chapter 1.2 IR Remote Control Operations)
- Change the EZVIZ Cloud P2P to HIK-CONNECT Cloud P2P. (Chapter 2.4 Using Wizard for Basic Configuration, Chapter 11.2.2 Configuring HIK-CONNECT Cloud P2P )

## Version 3.4.2

### Added:

- Support the display of IP camera's password on the IP camera management interface. (Chapter 2.6 Adding and Connecting the IP Cameras; Chapter 15.5.3 Editing a User)
- Add the configuration and use of unlock pattern for fast login. (Chapter 2.3 Using the Unlock Pattern for Login)
- Add the scaling display (30min/1h/2h/6h/24h) of time bar in the playback mode. (Chapter 6 Playback)
- Add the thumbnails view and fast view during playback. (Chapter Key Features, Chapter 6.2.2 Thumbnails View, Chapter 6.2.3 Fast View)

### Updated:

- Optimize the playback interface. (Chapter 6 Playback)
- Update the digital zoom operation in image. (Chapter 3.2.3 Quick Setting Toolbar in Live View Mode, Chapter 6.2.2 Digital Zoom)

## Version 3.4.0

### Added:

- Support up to 36-screen display mode for 32-ch NVR. (Chapter 3.3 Adjusting Live View Settings)
- Add the feature of **Dynamic Analysis for Motion** in the motion detection. (Chapter 5.3 Configuring Motion Detection Recording, Chapter 8.1 Setting Motion Detection Alarm)
- Support the admin password duplicated to the IP cameras that are connected with the default protocol. (Chapter 15.3 Editing a User)

### Updated:

- Optimize the input method of soft keypad. (Chapter 1.3 Input Method Description)

## Version 3.3.2

### Added:

Support H.264+. (Product Key Features, Chapter 5.1)

## Version 3.3.0

### Added:

- Support vehicle detection of VCA alarm. (Chapter 9.2)
- Support plate search. (Chapter 10.3)
- Set the strong password to activate the device is needed for the first-time startup (Chapter 2.2)

### Updated:

- Optimize the adding of IP camera. (Chapter 2.5)
- Optimize the DDNS configuration. (Chapter 11.2.3)
- Three methods are selectable for restoring to the default settings. (Chapter 14.6)
- Optimize the user account management. (Chapter 15.5)

## Version 3.2.0

### Added

- Support play back by sub-periods. (Chapter 6.1.6)
- Support VCA alarm for up to 15 VCA detections. (Chapter 9)

- Support VCA search function for behavior search, face search, people counting and heat map. (Chapter 10)
- Support up to 9 formats for selection when you export the files to storage device. (Chapter 7)
- The prompt will pop up when you input wrong user name or password in login interface.(Chapter 2.2)
- The continent/country is selectable for the HiDDNS settings. (Chapter 11.2.2)

**Update:**

- Optimize the interface of right-click menu. (Chapter 3.2.2)
- Optimize the interface of PTZ control panel. (Chapter 4)
- Optimize the interface of record parameters. (Chapter 5)
- Update the interface of recording schedule. (Chapter 5)
- Optimize the Device Info interface by adding QR Code. (Chapter 16.1)

## Version 3.0.6

**Updated**

- Optimize the PTZ control panels and operations. (Chapter 4)
- Change the ezviz Cloud to EZVIZ Cloud P2P. (Chapter 9.2.2)
- Add the models of DS-7100NI series, DS-7600NI-SE series and DS-7600NI-V(P) series NVR.

## Version 3.0.4

**Added**

- Connectable to smart IP cameras, and VCA alarm detection and recording are supported. (Chapter 5.2, Chapter 5.5 and Chapter 8.5)
- Support video searching, playing back and backing up by VCA events. (Chapter 6.1.3 and Chapter 7.1.3)
- Support smart playback by VCA rules. (Chapter 6.1.5)
- Support P2P protocol and access by ezviz. (Chapter 9.2.2)

**Deleted**

Combine the smart search function with the smart playback function, and the smart search section is deleted. (Chapter 6.2.2 Smart Search)

## 16.5 List of Compatible IP Cameras

### 16.5.1 List of Hikvision IP Cameras



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-2CD793NFW-D-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 build 150327	1280*960	√	×
	DS-2CD2132-I	V5.3.0 build 150327	2048*1536	√	×
	DS-2CD2410FD-I(W)	V5.3.0 build 150327	1920*1080	√	√
	DS-2CD2612F-I	V5.3.0 build 150327	1280*960	√	×
	DS-2CD2612F-IS	V5.3.0 build 150327	1280*960	√	√
	DS-2CD2632F-I	V5.3.0 build 150327	2048*1536	√	×
	DS-2CD2632F-IS	V5.3.0 build 150327	2048*1536	√	√
	DS-2CD2710F-I	V5.3.0 build 150327	1920*1080	√	×
	DS-2CD2720F-I	V5.3.0 build 150327	1920*1080	√	×
	DS-2CD4010F	V5.3.0 build 150327	1920*1080	√	√
	DS-2CD4012F	V5.3.0 build 150327	1280*1024	√	√
	DS-2CD4026FWD	V5.3.0 build 150327	1920*1080	√	√
	DS-2CD4026FWD-SDI	V5.3.0 build 150327	1920*1080	√	√
	DS-2CD4032FWD	V5.3.0 build 150327	2048*1536	√	√
	DS-2CD4065F	V5.3.0 build 150327	3072*2048	√	√
	DS-2CD4124F-I(2.8-12mm)	V5.3.0 build 150327	1920*1080	√	√
	DS-2CD4132FWD-I(2.8-12mm)	V5.3.0 build 150327	2048*1536	√	√
	DS-2CD4212F-I(2.8-12mm)	V5.3.0 build 150327	1280*1024	√	×
	DS-2CD4212F-IS(2.8-12mm)	V5.3.0 build 150327	1280*1024	√	√
	DS-2CD4212FWD-I	V5.3.0 build 150327	1280*960	√	×
	DS-2CD4212FWD-IS	V5.3.0 build 150327	1280*960	√	√
	DS-2CD4224F-I	V5.3.0 build 150327	1920*1080	√	×
	DS-2CD4232FWD-I	V5.3.0 build 150327	2048*1536	√	×
	DS-2CD4232FWD-IS(2.8-12mm)	V5.3.0 build 150327	2048*1536	√	√
	DS-2CD4312F-I	V5.3.0 build 150327	1280*1024	√	×

Type	Model	Version	Max. Resolution	Sub-stream	Audio
	DS-2CD4312FWD-I	V5.3.0 build150327	1280*960	√	×
	DS-2CD4324F-I	V5.3.0 build150327	1920*1080	√	×
	DS-2CD4332FHW-DS	V5.3.0 build150327	2048*1536	√	√
	DS-2CD4332FHW-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	√	√
	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	√	×

Type	Model	Version	Max. Resolution	Sub-stream	Audio
	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	√	×
	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	√	√

Type	Model	Version	Max. Resolution	Sub-stream	Audio
	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	√	√
	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	√	√
	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_2DF713015-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	√	√



Type	Model	Version	Max. Resolution	Sub-stream	Audio
	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	√	√
	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	√	√

Type	Model	Version	Max. Resolution	Sub-stream	Audio
	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	√	√
	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	√	√
	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	DS-2ZCN2006	V5.2.7 build141107	1280*960	√	√
Zoom	DS-2ZCN2006(B)	V5.2.7 build141107	1280*960	√	√
Camera	DS-2ZCN3006	V5.2.7 build141107	1280*960	√	√

Type	Model	Version	Max. Resolution	Sub-stream	Audio
Module	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	√	√

## 16.5.2 List of Third-party IP Cameras



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

IP Camera Manufacturer or Protocol	Model	Version	Max. Resolution	Sub-stream	Audio
ACTI	TCM4301-10D-X-00083	A1D-310-V4.12.09-AC	1280×1024	×	√
	TCM5311-11D-X-00023	A1D-310-V4.12.09-AC	1280×960	×	√
	TCM3401-09L-X-00227	A1D-220-V3.13.16-AC	1280×1024	×	×
ARECONT	AV8185DN	65172	1600×1200	×	×
	AV1305M	65175	1280×1024	√	×
	AV2155	65143	1600×1200	√	×
	AV2815	65220	1920×1080	√	×
	AV3105M	65175	1920×1080	√	×
	AV5105	65175	1920×1080	√	×
AXIS	M1114	5.09.1	1024×640	√	×
	M3011(ONVIF compatibility)	5.21	704×576	√(Only AXIS is supported)	×
	M3014(ONVIF compatibility)	5.21.1	1280×800	√	×
	P3301(ONVIF compatibility)	5.11.2	768×576	√	√(Only AXIS is supported)
	P3304(ONVIF compatibility)	5.20	1440×900	√	√(Only AXIS is supported)
	P3343(ONVIF compatibility)	5.20.1	800×600	√	√(Only AXIS is supported)
	P3344(ONVIF compatibility)	5.20.1	1440×900	√	√(Only AXIS is supported)
	P5532	5.15	720×576	√	×
	Q7404	5.02	720×576	√	√
Bosch (ONVIF compatibility)	AutoDome Jr 800HD	39500450	1920×1080	×	√
	NBC 265 P	07500453	1280×720	×	√
	Dinion NBN-921-P	10500453	1280×720	×	√
Brickcom	FB-130Np (ONVIF compatibility)	V3.1.0.8	1280×1024	×	√
	CB-500Ap (ONVIF compatibility)	V3.2.1.3	1920×1080	×	√

IP Camera Manufacturer or Protocol	Model	Version	Max. Resolution	Sub-stream	Audio
	compatibility)				
	WFB-100Ap	V3.1.0.9	1280×800	×	√
Canon	VB-M400	Ver.+1.0.0	1280×960	×	√
	VB-M6000D	Ver.+1.0.0	1280×960	×	×
	VB-M7000F	Ver.+1.0.0	1280×960	×	√
HUNT	HLC_79AD	V1.0.40	1600×1200	√	×
Panasonic	WV-SW152(ONVIF compatibility)	Application:1.66 Image data:1.05	800×600	√	×
	WV-SC386(ONVIF compatibility)	Application:1.66 Image data:1.05	1280×960	√	√
	WV-SW155(ONVIF compatibility)	Application:1.66 Image data:1.05	1280×960	√	×
	WV-SW316(ONVIF compatibility)	Application:1.66 Image data:2.03	1280×960	√	√
	WV-SP105(ONVIF compatibility)	Application:1.66 Image data:1.03	1280×960	√	×
	WV-SF132(ONVIF compatibility)	Application:1.66 Image data:1.03	640×360	√	×
	WV-SP102(ONVIF compatibility)	Application:1.66 Image data:1.03	640×480	√	×
	WV-SP509(ONVIF compatibility)	Application:1.30 Image data:2.21	1280×960	√	√
	WV-SW559(ONVIF compatibility)	Application:1.30 Image data:2.21	1920×1080	√	√
	WV-SW558(ONVIF compatibility)	Application:1.30 Image data:2.21	1920×1080	√	×
	WV-SW355(ONVIF compatibility)	Application:1.66 Image data:1.04	1280×960	√	√
	WV-SW352(ONVIF compatibility)	Application:1.66 Image data:1.04	800×600	√	√
	WV-SF342(ONVIF compatibility)	Application:1.66 Image data:1.06	800×600	√	√
	WV-SF332(ONVIF compatibility)	Application:1.66 Image data:1.06	800×600	√	√
	WV-SF346(ONVIF compatibility)	Application:1.66 Image data:1.06	1280×960	√	√
	WV-SP306H	Application:1.34 Image data:1.06	1280×960	√	√
	WV-SP336H	Application:1.06 Image data:1.06	1280×960	√	√
PELCO	D5118	1.8.2-20120327- 2.9310-A1.7852	1280×960	√	×
	IXE20DN-AAXVUU2	1.8.2-20120327- 2.9081-A1.7852	1920×1080	√	×

IP Camera Manufacturer or Protocol	Model	Version	Max. Resolution	Sub-stream	Audio
	IX30DN-ACFZHB3	1.8.2-20120327- 2.9080-A1.7852	2048×1536	√	×
SAMSUNG (ONVIF compatibility)	SNB-5080P	V3.10_130416	1280×1024	√(Only ONVIF is supported)	√
SANYO	VCC-HD2300P	2.03-02(110318-00)	1920×1080	×	×
	VCC-HD2500P	2.02-02(110208-00)	1920×1080	×	√
	VCC-HD4600P	2.03-02(110315-00)	1920×1080	×	√
SONY	SNC-CH220	1.50.00	1920×1080	×	×
	SNC-RH124(ONVIF compatibility)	1.73.00	1280×720	√	√
	SNC-EP580(ONVIF compatibility)	1.53.00	1920×1080	√	√
	SNC-DH220T(Only ONVIF is supported)	1.50.00	2048×1536	×	×
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	MG.1.6.03P8	1280×1024	√	×
	F3106	M2.1.6.03P8	1280×1024	√	√
	F3110	M2.1.6.01	1280×720	√	√
	F3206	MG.1.6.02c045	1920×1080	√	√
	F531E	LM.1.6.18P10	640×480	√	√



First Choice for Security Professionals