



**Network Video Recorder  
User Manual**

## **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 specific Network Video Recorders (NVRs).

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 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 LATTER 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:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

**EU Conformity Statement**

**CE** This product and, if applicable, the supplied accessories too are marked with “CE” and comply therefore with the applicable harmonized European standards listed under the 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.

**Symbol Conventions**

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

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

**Safety Instructions**

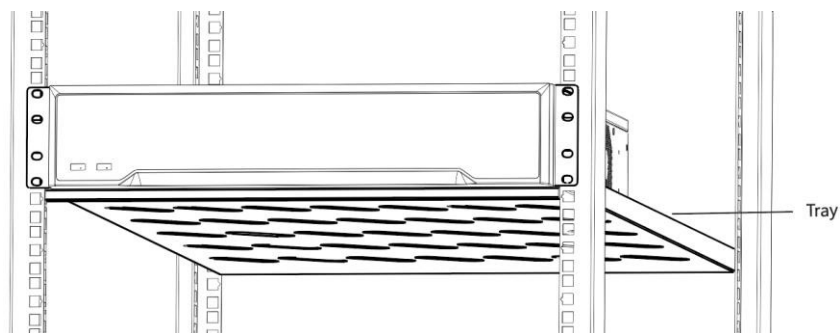
- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region. Please refer to technical specifications for detailed information.
- Input voltage should meet both the SELV (Safety Extra Low Voltage) and the Limited Power Source with 100 to 240 VAC or 12 VDC according to the IEC60950-1 standard. Please refer to technical specifications for detailed information.
- Do not connect several devices to one power adapter as adapter overload may cause overheating 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 a 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 explosion hazard. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.
- When installing the device into a cabinet over 2U height, it is suggested to use a rack shelf to bear the weight. If the cabinet height is over 4U, it is suggested to use slide rails or a rack shelf to bear the weight.





## Product Key Features

### General

- Connectable to network cameras, network dome, and encoders.
- Connectable to third-party network cameras such as ACTI, Arecont, AXIS, Bosch, Brickcom, Canon, PANASONIC, Pelco, SAMSUNG, SANYO, SONY, Vivotek, and ZAVIO, and cameras that adopt ONVIF or PSIA protocol.
- Connectable to smart IP cameras.
- H.265+/H.265/ H.264+/H.264/MPEG4 video formats.
- PAL/NTSC adaptive video inputs.
- Each channel supports dual-stream.
- Up to 8/16/32 network cameras can be added according to different models.
- Independent configuration for each channel, including resolution, frame rate, bit rate, image quality, etc.
- The quality of the input and output record is configurable.

### Local Monitoring

- HDMI and VGA outputs provided.
- HDMI video output at up to 4K 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. Manual switch and auto-switch are provided and the auto-switch interval is configurable.
- Configurable main stream and sub-stream for the live view.
- Quick setting menu is provided for live view.
- [Motion detection](#), [video tampering](#), video exception alert, and video loss alert functions.
- Privacy mask.
- Multiple [PTZ](#) protocols supported; [PTZ](#) preset, patrol, and pattern.
- Zooming in by clicking the mouse and [PTZ](#) tracing by dragging mouse.

### HDD Management

- Up to 6 TB storage capacity for each disk supported.
- Supports eight network disks (NAS/IP SAN disk).

- 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, and motion & alarm [VCA](#).
- Eight recording time periods with separated recording types.
- Pre-record and post-record for alarm, [motion detection](#) for recording, and pre-record time for schedule and manual recording.
- Searching record files and captured pictures by events (alarm input/[motion detection](#)).
- Tag adding for record files, searching and playing back by tags.
- Locking and unlocking record files.
- Local [redundant recording](#).
- Provide new playback interface with easy and flexible operation.
- Searching and playing back record files by channel number, recording type, start time, end time, etc.
- [Smart search](#) for the selected area in the video.
- Zooming in when playback.
- Reverse playback of multi-channel.
- Supports pause, play reverse, speed up, speed down, skip forward, and skip backward when playback, and locating by dragging the mouse.
- Supports thumbnails view and fast view during playback.
- Up to 16-ch synchronous playback at 1080p real time.
- Supports playback by transcoded stream.
- 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.

### Alarms and Exceptions

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

### Other Local Functions

- Operable by front panel, mouse, remote control, or control keyboard.
- Three-level user management; admin user is allowed to create many operating accounts and define their operating permission, which includes the limit to access any channel.
- Admin password resetting by exporting/importing the GUID file.
- Operation, alarm, exceptions and log recording and searching.
- Manually triggering and clearing alarms.
- Import and export of device configuration information.

### Network Functions

- Self-adaptive 10M/100M/1000Mbps network interface.
- Four independent PoE network interfaces are provided for /4P models, eight independent PoE network interfaces for /8P models, and sixteen independent PoE network interfaces for /16P models.
- Long distance (100–300 m) network transmission via PoE (for /P models).
- IPv6 is supported.
- TCP/IP protocol, DHCP, DNS, DDNS, NTP, SADP, SMTP, [SNMP](#), NFS, and iSCSI are supported.
- TCP, UDP and RTP for unicast.

- Auto/Manual port mapping by UPnP™.
- Support access by Hik-Connect.
- Remote Web browser access by HTTPS ensures high security.
- The ANR (Automatic Network Replenishment) function is supported, it enables the IP camera save the recording files in the local storage when the network is disconnected and synchronizes the files to the NVR when the network is resumed.
- Remote reverse playback via RTSP.
- Supports accessing by the platform via ONVIF.
- Remote search, playback, download, locking, and unlocking of the record files, and supports downloading files broken transfer resume.
- Remote parameters setup; remote import/export of device parameters.
- Remote viewing of the device status, system logs and alarm status.
- Remote keyboard operation.
- Remote HDD formatting and program upgrading.
- Remote system restart and shutdown.
- RS-485 transparent channel transmission.
- Alarm and exception information can be sent to the remote host.
- Remotely start/stop recording.
- Remotely start/stop alarm output.
- Remote [PTZ](#) control.
- Remote JPEG capture.
- Virtual host function is provided to get access and manage the IP camera directly.
- Two-way audio and voice broadcasting.
- Embedded Web server.

### **Development Scalability**

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

# TABLE OF CONTENTS

<b>Chapter 1 Introduction</b> .....	<b>14</b>
1.1 Front Panel (Typical) .....	14
1.2 <b>IR Remote</b> Control Operations .....	14
1.2.1 Pairing (Enabling) the <b>IR Remote</b> to a Specific NVR (optional).....	14
1.2.2 Unpairing (Disabling) an <b>IR Remote</b> from an NVR .....	15
1.3 USB Mouse Operation .....	17
1.4 Input Method Description .....	18
1.5 Rear Panel (Typical).....	18
<b>Chapter 2 Getting Started</b> .....	<b>19</b>
2.1 Device Startup and Activation.....	19
2.1.1 Starting Up and Shutting Down the NVR .....	19
2.1.2 Activating Your Device .....	20
2.1.3 Using the Unlock Pattern for Login .....	21
2.1.4 Login and Logout .....	24
2.1.5 Resetting Your Password .....	25
2.2 Using Wizard for Basic Configuration .....	26
2.3 Adding and Connecting IP Cameras .....	30
2.3.1 Activating the IP Camera.....	30
2.3.2 Adding the Online IP Cameras.....	31
2.3.3 Editing the Connected IP Cameras and Configuring Customized Protocols .....	35
2.3.4 Editing IP Cameras Connected to the PoE Interfaces .....	38
2.3.5 Configuring PoE Interface.....	40
<b>Chapter 3 Live View</b> .....	<b>42</b>
3.1 Live View Introduction .....	42
3.2 Operations in Live View Mode.....	42
3.2.1 Front Panel Operation on Live View .....	43
3.2.2 Using the Mouse in Live View .....	43
3.2.3 Using an Auxiliary Monitor.....	44
3.2.4 Quick Setting Toolbar in Live View Mode .....	44
3.3 Adjusting Live View Settings.....	46
3.4 Channel-Zero Encoding .....	48
<b>Chapter 4 PTZ Controls</b> .....	<b>48</b>
4.1 Configuring <b>PTZ</b> Settings .....	48
4.2 Setting <b>PTZ</b> Presets, Patrols, and Patterns .....	49
4.2.1 Customizing Presets .....	49
4.2.2 Calling Presets.....	50

4.2.3	Customizing Patrols .....	51
4.2.4	Calling Patrols.....	52
4.2.5	Customizing Patterns .....	53
4.2.6	Calling Patterns.....	53
4.2.7	Customizing <a href="#">Linear Scan</a> Limit .....	54
4.2.8	Calling <a href="#">Linear Scan</a> .....	55
4.2.9	<a href="#">One-Touch Park</a> .....	55
4.3	<a href="#">PTZ</a> Control Panel .....	56
<b>Chapter 5 Recording Settings.....</b>		<b>57</b>
5.1	Configuring Parameters.....	57
5.2	Configuring Recording Schedule .....	60
5.3	Configuring <a href="#">Motion Detection</a> Recording .....	63
5.4	Configuring Alarm Triggered Recording.....	64
5.5	Configuring <a href="#">VCA</a> Event Recording .....	66
5.6	Manual Recording .....	67
5.7	Configuring Holiday Recording.....	68
5.8	Configuring <a href="#">Redundant Recording</a> .....	70
5.9	Configuring HDD Group for Recording .....	71
5.10	Files Protection.....	72
5.10.1	Locking the Recording Files.....	72
5.10.2	Setting HDD Property to Read-only .....	74
<b>Chapter 6 Playback.....</b>		<b>75</b>
6.1	Playing Back Record Files.....	75
6.1.1	Instant Playback .....	75
6.1.2	Playing Back by Normal Search .....	76
6.1.3	Playing back by <a href="#">Smart Search</a> .....	78
6.1.4	Playing Back by <a href="#">Event Search</a> .....	80
6.1.5	Playing Back by Tag .....	82
6.1.6	Playing Back by System Logs.....	84
6.1.7	Playing Back External File.....	85
6.2	Auxiliary Playback Functions .....	86
6.2.1	Playing Back Frame-by-Frame.....	86
6.2.2	Thumbnails View .....	86
6.2.3	Fast View .....	87
6.2.4	Digital Zoom .....	87
6.2.5	File Management.....	88
<b>Chapter 7 Backup.....</b>		<b>89</b>
7.1	Backing up Record Files .....	89

7.1.1	Quick Export.....	89
7.1.2	Backing up by Normal Video Search.....	90
7.1.3	Backing up by <a href="#">Event Search</a> .....	93
7.1.4	Backing up Video Clips.....	94
7.2	Managing Backup Devices.....	95
<b>Chapter 8 Alarm Settings .....</b>		<b>95</b>
8.1	Setting <a href="#">Motion Detection Alarm</a> .....	95
8.2	Setting Sensor Alarms .....	97
8.3	Detecting Video Loss Alarm .....	99
8.4	Detecting <a href="#">Video Tampering Alarm</a> .....	100
8.5	Handling Exceptions Alarm.....	102
8.6	Setting Alarm Response Actions.....	103
8.7	Triggering or Clearing Alarm Output Manually .....	105
<b>Chapter 9 VCA Alarm .....</b>		<b>106</b>
9.1	<a href="#">Face Detection</a> .....	106
9.2	<a href="#">Line Crossing Detection</a> .....	107
9.3	<a href="#">Intrusion Detection</a> .....	109
9.4	<a href="#">Region Entrance Detection</a> .....	110
9.5	<a href="#">Region Exiting Detection</a> .....	111
9.6	<a href="#">Unattended Baggage Detection</a> .....	112
9.7	<a href="#">Object Removal Detection</a> .....	112
9.8	<a href="#">Audio Exception Detection</a> .....	112
9.9	<a href="#">Sudden Scene Change Detection</a> .....	113
9.10	<a href="#">Defocus Detection</a> .....	113
9.11	<a href="#">PIR Alarm</a> .....	114
<b>Chapter 10 VCA Search .....</b>		<b>114</b>
10.1	<a href="#">Face Search</a> .....	114
10.2	<a href="#">Behavior Search</a> .....	116
<b>Chapter 11 Network Settings.....</b>		<b>117</b>
11.1	Configuring General Settings .....	117
11.2	Configuring Advanced Settings .....	118
11.2.1	Configuring Hik-Connect .....	118
11.2.2	Configuring DDNS.....	121
11.2.3	Configuring PPPoE.....	122
11.2.4	Configuring NTP Server.....	123
11.2.5	Configuring <a href="#">SNMP</a> .....	123
11.2.6	Configuring More Settings .....	124
11.2.7	Configuring HTTPS Port .....	125

11.2.8	Configuring E-Mail.....	127
11.2.9	Configuring NAT.....	129
11.2.10	Configuring Virtual Host.....	131
11.3	Checking Network Traffic.....	132
11.4	Configuring Network Detection.....	132
11.4.1	Testing Network Delay and Packet Loss.....	132
11.4.2	Exporting Network Packet.....	133
11.4.3	Checking the Network Status.....	133
11.4.4	Checking Network Statistics.....	134
<b>Chapter 12 HDD Management.....</b>		<b>135</b>
12.1	Initializing HDDs.....	135
12.2	Managing Network HDD.....	136
12.3	Managing HDD Groups.....	138
12.3.1	Setting HDD Groups.....	138
12.3.2	Setting HDD Property.....	140
12.4	Configuring Quota Mode.....	140
12.5	Configuring Disk Clone.....	142
12.6	Checking HDD Status.....	143
12.7	HDD Detection.....	144
12.8	Configuring HDD Error Alarms.....	146
<b>Chapter 13 Camera Settings.....</b>		<b>147</b>
13.1	Configuring OSD Settings.....	147
13.2	Configuring Privacy Mask.....	147
13.3	Configuring Video Parameters.....	148
<b>Chapter 14 NVR Management and Maintenance.....</b>		<b>149</b>
14.1	Viewing System Information.....	149
14.2	Searching and Exporting Log Files.....	150
14.3	Importing/Exporting IP Camera Info.....	152
14.4	Importing/Exporting Configuration File.....	152
14.4.1	Exporting Configuration File.....	152
14.4.2	Importing Configuration File.....	153
14.5	Upgrading System.....	154
14.5.1	Upgrading by Local Backup Device.....	154
14.5.2	Upgrading by FTP.....	154
14.6	Restoring Default Settings.....	155
<b>Chapter 15 Others.....</b>		<b>155</b>
15.1	Configuring General Settings.....	155
15.2	Configuring DST Settings.....	157



- 15.3 Configuring More Settings ..... 157
- 15.4 Managing User Accounts ..... 158
  - 15.4.1 Adding a User..... 158
  - 15.4.2 Deleting a User ..... 161
  - 15.4.3 Editing a User..... 162
- Chapter 16 Appendix..... 164**
- 16.1 Glossary ..... 164
- 16.2 Troubleshooting..... 164

# Chapter 1 Introduction



**IMPORTANT!**

Not all NVRs support all features in this manual.

Some features (noted in blue type) require camera support.

Please check your hardware specifications for usage.

## 1.1 Front Panel (Typical)

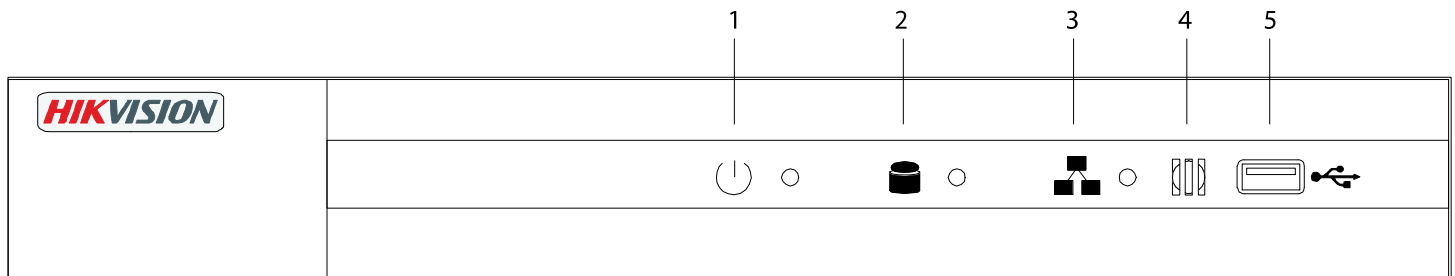


Figure 1, Typical Front Panel

Table 1-4 Panel Description

No.	Name	Connections
1	POWER	Turns white when device is powered up
2	HDD	Flickers white when data is being read from or written to HDD
3	Tx/Rx	Flickers white when network connection is functioning properly
4	Infrared Receiver	Receiver for <a href="#">IR Remote</a> control
5	USB Interface	Universal Serial Bus (USB) port 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.

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

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

### 1.2.1 Pairing (Enabling) the [IR Remote](#) to a Specific NVR (optional)

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

On the NVR:

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

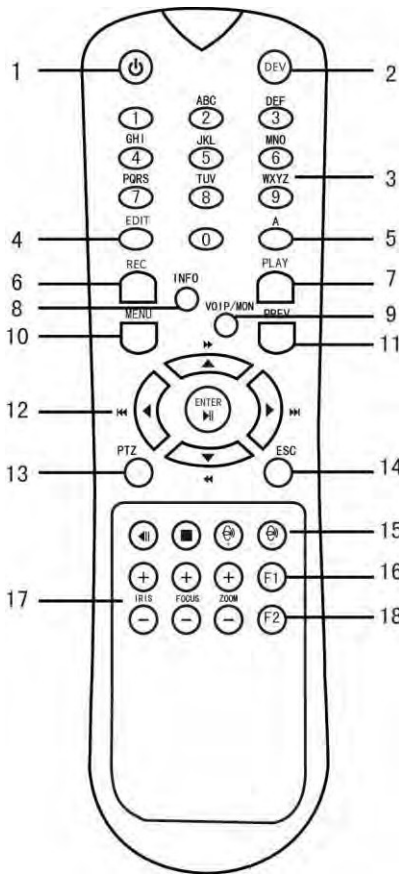


Figure 2, Remote Control

## 1.2.2 Unpairing (Disabling) an **IR Remote** from an NVR

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

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

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

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

Table 1-4 IR Remote Functions

No.	Name	Function Description
1	POWER ON/OFF	<ul style="list-style-type: none"> <li>• To Turn Power On:                             <ul style="list-style-type: none"> <li>- If User Has Not Changed the Default NVR Device ID# (255):                                     <ol style="list-style-type: none"> <li>1. Press Power On/Off button (1).</li> </ol> </li> <li>- If User Has Changed the NVR Device ID#:                                     <ol style="list-style-type: none"> <li>1. Press DEV button.</li> <li>2. Press Number buttons to enter user-defined Device ID#.</li> <li>3. Press Enter button.</li> <li>4. Press Power button to start device.</li> </ol> </li> </ul> </li> <li>• To Turn NVR Off:                             <ul style="list-style-type: none"> <li>- If User Is Logged On:                                     <ol style="list-style-type: none"> <li>1. Hold Power On/Off button (1) down for five seconds to display the "Yes/No" verification prompt.</li> <li>2. Use Up/Down Arrow buttons (12) to highlight desired selection.</li> <li>3. Press Enter button (12) to accept selection.</li> </ol> </li> <li>- If User Is <i>Not</i> Logged On:                                     <ol style="list-style-type: none"> <li>1. Hold Power On/Off button (1) down for five seconds to display the user name/password prompt.</li> <li>2. Press the Enter button (12) to display the on-screen keyboard.</li> <li>3. Input the user name.</li> <li>4. Press the Enter button (12) to accept input and dismiss the on-screen keyboard.</li> <li>5. Use the Down Arrow 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 Enter button (12) to accept input and dismiss the on-screen keyboard.</li> <li>8. Press the OK button on the screen to accept input and display the Yes/No" verification prompt (use Up/Down Arrow buttons (12) to move between fields)</li> <li>9. Press Enter button (12) to accept selection.</li> </ol> </li> </ul> </li> </ul> <p>User name/password prompt depends on NVR is configuration. See "System Configuration" section.</p>
2	DEV	Enable IR Remote: Press DEV button, enter NVR Device ID# with number keys, press Enter to pair unit with the NVR Disable IR Remote: Press DEV button to clear Device ID#; unit will no longer be paired with the NVR
3	Numerals	Switch to the corresponding channel in Live View or PTZ Control mode Input numbers in Edit mode
4	EDIT	Delete characters before cursor Check the checkbox and select the ON/OFF switch
5	A	Adjust focus in the PTZ Control menu Switch on-screen keyboards (upper and lower case alphabet, symbols, and numerals)
6	REC	Enter Manual Record setting menu Call a PTZ preset by using the numeric buttons in PTZ control settings Turn audio on/off in Playback mode
7	PLAY	Go to Playback mode Auto scan in the PTZ Control menu
8	INFO	Reserved
9	VOIP	Switches between main and spot output Zooms out the image in PTZ control mode Return to Main menu (after successful login)
10	MENU	N/A Show/hide full screen in Playback mode
12	DIRECTION	Navigate between fields and menu items
		Use Up/Down buttons to speed up/slow down recorded video, and Left/Right buttons to advance/rewind 30 secs in Playback mode
		Cycle through channels in Live View mode
		Control PTZ camera movement in PTZ control mode
	ENTER	Confirm selection in any menu mode
		Checks checkbox
13	PTZ	Enter PTZ Control mode
		Go back to previous screen
		N/A
14	ESC	Reserved
		Select all items on a list
15	RESERVED	N/A
		Switch between play and reverse play in Playback mode
16	F1	Adjust PTZ camera iris, focus, and zoom
		Cycle through tab pages
17	PTZ Control	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.

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.

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

- Batteries are installed correctly and the polarities of the batteries are not reversed.
- Batteries are fresh and not out of charge.
- IR receiver is not obstructed.
- No fluorescent lamp is used nearby
- If the remote still can't function properly, change the remote and try again, or contact the device provider.

## 1.3 USB Mouse Operation

A regular 3-button (Left/Right/Scroll-wheel) USB mouse can also be used with this 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 the mouse is not detected, the possible reason may be that the two devices are not compatible, refer to the recommended device list from your provider.

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: multi-screen Switch between single-screen and multi-screen
	Click and Drag	PTZ Control: pan, tilt, and zoom <a href="#">Video tampering</a> , privacy mask, and <a href="#">motion detection</a> : Select target area Digital Zoom-in: Drag and select target area Live View: Drag channel/time bar
Right-Click	Single-Click	Live View: Show menu Menu: Exit current menu to upper level menu
Scroll-Wheel	Scrolling Up	Live View: Previous screen Menu: Previous item
	Scrolling Down	Live View: Next screen Menu: Next item

## 1.4 Input Method Description



Figure 3, Soft Keyboard (1)



Figure 4, Soft Keyboard (2)

Table 1-6 Description of the Soft Keyboard Icons

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

## 1.5 Rear Panel (Typical)

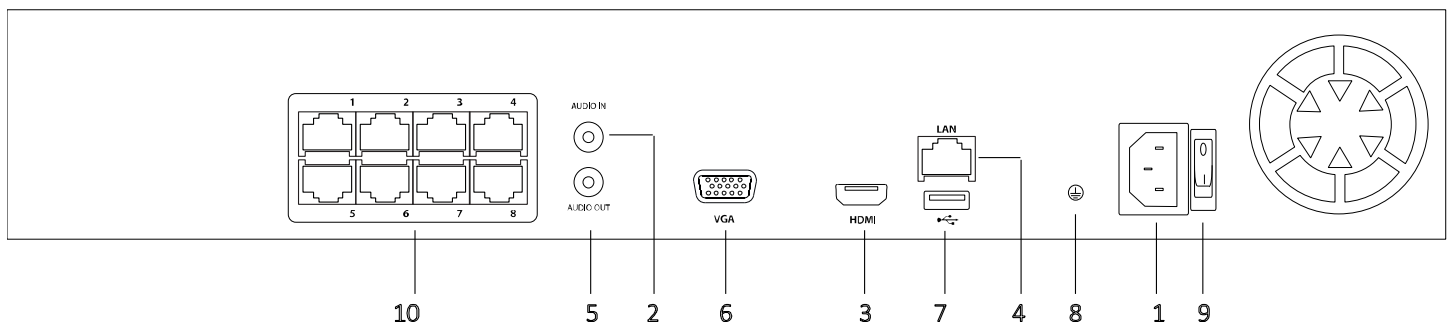


Figure 5, Rear Panel (Typical)

Index	Description	Index	Description
1	100 to 240 VAC	6	VGA
2	Audio In	7	USB 2.0 Interface
3	HDMI Interface	8	Ground
4	LAN Interface	9	Power Switch
5	Audio Out	10	LAN Network Interfaces with PoE Function

# 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 external power supply is the same with the NVR's requirement and the ground connection is working properly.

#### Starting up the NVR

1. Check that 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. Press the **Power** button on the front panel. The Power indicator LED should turn blue, indicating that the unit is starting.
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: Standard Shutdown**

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



Figure 6, Shutdown Menu

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

- **OPTION 2: By Operating the Front Panel**

1. Press and hold the **Power** button on the front panel for three seconds.

2. Enter the administrator's username and password in the dialog box for authentication.
3. Click the **Yes** button.

**NOTE:** Do not press the **Power** button again when the system is shutting down.

## Rebooting the NVR

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

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. You can also activate the device via Web Browser, SADP software, or Client software.

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

Figure 7, Set Admin Password



**STRONG PASSWORD RECOMMENDED** – We highly recommend that you create a strong password of your own choosing (using a minimum of eight 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. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.



2. In the **IP Camera Activation** text field, enter the password to activate the IP camera(s) connected to the device.
3. Click **OK** to save the password and activate the device.
4. When the device is activated, the system pops up the message box to remind you to remember the password. Click **Yes** to continue to export the GUID file for the future password resetting.



Figure 8, Export GUID File Remind

5. Insert the USB flash disk into your device, and export the GUID file to the USB flash disk in the Reset Password interface. Please see *Resetting Your Password* for password resetting instructions.



Figure 9, Export GUID File

**NOTE:** Please keep your GUID file properly for future password resetting.

If the Admin's password is modified, the following menu pops up. Optionally, click the **Yes** button to duplicate the password to IP cameras that are connected with the default protocol.



Figure 10, Attention Interface

### 2.1.3 Using the Unlock Pattern for Login

The Admin user can configure the unlock pattern for device login.

## Configuring the Unlock Pattern

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

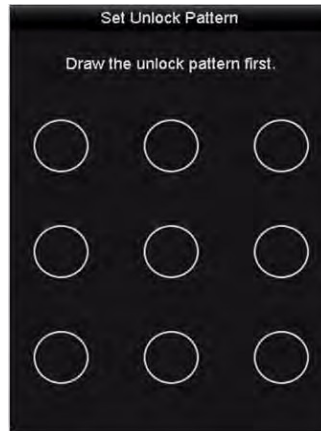


Figure 11, Set Unlock Pattern

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



Figure 12, Draw the Pattern

**NOTE:** Connect at least four dots to draw the pattern. Each dot can connect only once.

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

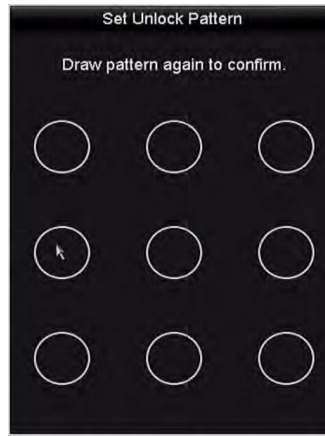


Figure 13, Confirm the Pattern

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

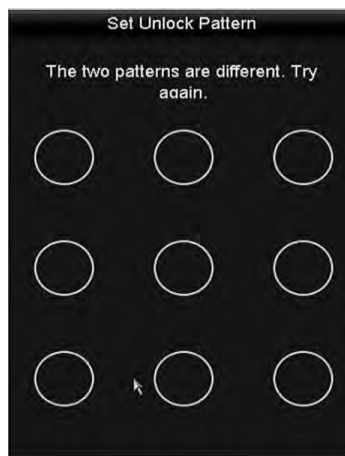


Figure 14, Re-set the Pattern

### Logging in via Unlock Pattern

**NOTE:** Only the *admin* user has the permission to unlock the device.

Please configure the pattern first before unlocking. See *Configuring the Unlock Pattern*.

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

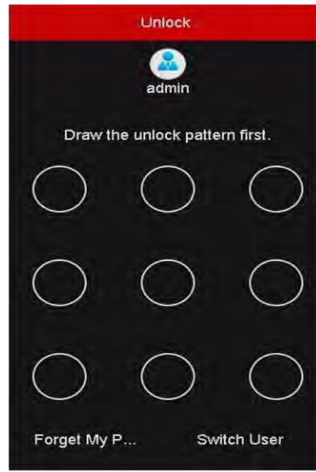


Figure 15, Draw the Unlock Pattern

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

**NOTE:** If you forget your pattern, select **Forget My Pattern** or **Switch User** to enter the normal login dialog box.

If the pattern you draw is different from the pattern you have configured, try again.

If you draw the wrong pattern more than five times, the system will switch to the normal login mode automatically.



Figure 16, Normal Login Dialog Box

## 2.1.4 Login and Logout

### User Login

#### Purpose

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

1. Select the **User Name** in the drop-down list.

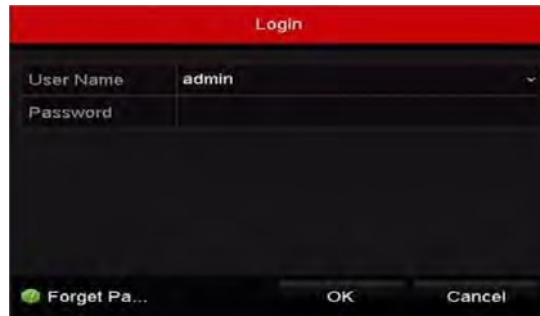


Figure 17, Login Interface

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

**NOTE:** If you forget the admin password, click **Forget Password** to reset the password. See *Resetting Your Password* for details.

In the Login dialog box, if you enter the wrong password seven times, the current user account will be locked for 60 seconds.

## User Logout

### Purpose

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

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



Figure 18, Logout

2. Click **Logout**.

**NOTE:** After you log out of the system, menu operation on the screen is invalid. You must input a user name and password to unlock the system.

## 2.1.5 Resetting Your Password

If you forget the admin password, you can reset the password by importing the GUID file. The GUID file must be exported and saved in the local USB flash disk after you have activated the device (see *Activating Your Device*).

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

**NOTE:** Insert the USB flash disk with the GUID file into the NVR before resetting the password.



Figure 19, Reset Password

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

**NOTE:** If you import the wrong GUID file seven times, you will be not allowed to reset the password for 30 minutes.

3. Once the GUID file is successfully imported, enter the reset password interface to set the new admin password. See *Activating Your Device* for details.
4. Click **OK** to set the new password. You can export the new GUID file to the USB flash disk for future password resetting.

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

## 2.2 Using Wizard for Basic Configuration

By default, the Setup Wizard starts once the NVR has loaded, as shown below.



Figure 20, Start Wizard Interface

### Operating the Setup Wizard

1. The Setup Wizard can walk you through some important NVR settings. If you don't want to use the

Setup Wizard at that moment, click the **Cancel** button. You can also choose to use the Setup Wizard next time by leaving the “Start wizard when the device starts?” checkbox checked.

2. Click the **Next** button to enter the date and time settings window, as shown below.



Figure 21, Date and Time Settings

3. After the time settings, click the **Next** button, which takes you back to the Network Setup Wizard window, as shown below.



Figure 22, Network Settings

4. Click the **Next** button after you configure the basic network parameters. Enter the **Hik-Connect** interface to configure the parameters. See *Configuring Hik-Connect* for detailed instructions.

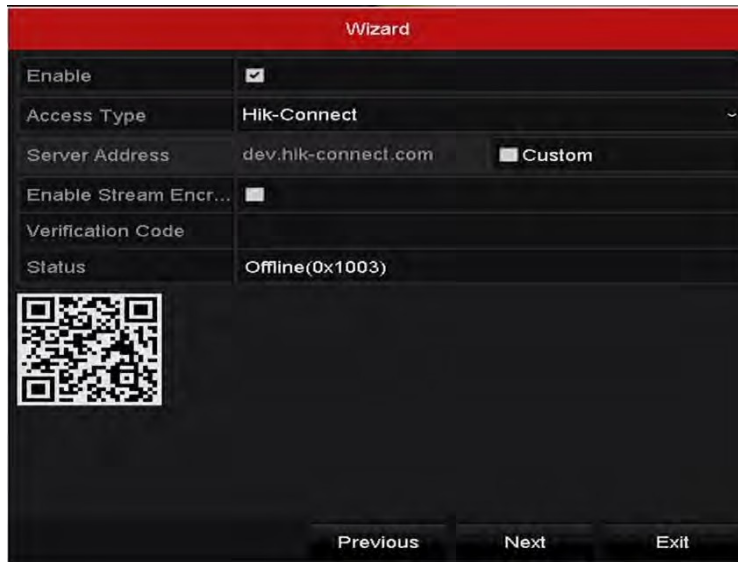


Figure 23, Hik-Connect Settings

5. Click the **Next** button after you configure 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 needs.



Figure 24, Advanced Network Parameters

6. Click the **Next** button after you configure the network parameters.
7. Click the **Next** button to enter the **HDD Management** window, shown in below.



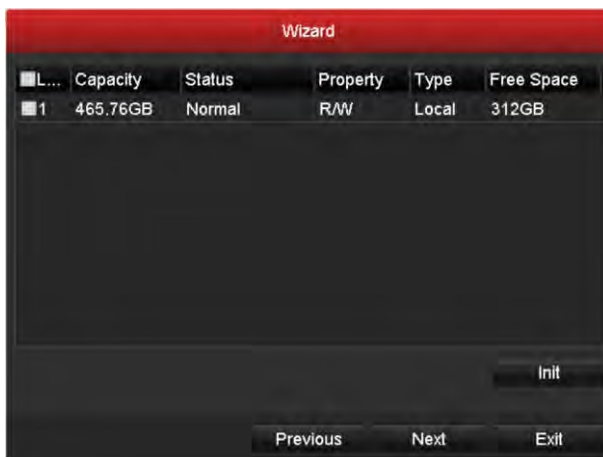


Figure 25, HDD Management

8. To initialize the HDD, click the **Init** button. Initialization removes all data saved on the HDD.
9. Click the **Next** button to enter the **Adding IP Camera** interface.
10. Click **Search** to search for online IP cameras, 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.
11. 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.
12. Click **Add** to add the camera.

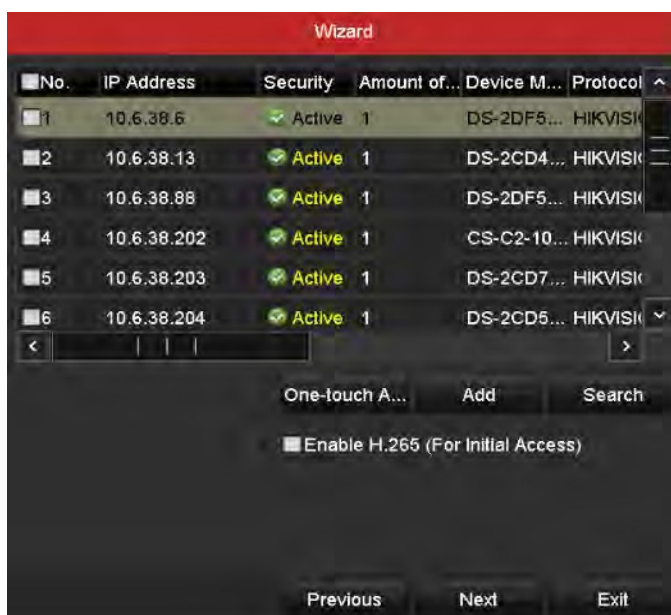


Figure 26, Search for IP Cameras

If you check the **Enable H.265** checkbox, the NVR can automatically switch to the H.265 stream of IP cameras that support the H.265 video format for the initial access.

13. Click the **Next** button. Configure the recording for the added IP cameras.



Figure 27, Record Settings

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

## 2.3 Adding and Connecting IP Cameras

### 2.3.1 Activating the IP Camera

#### Purpose

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

You can activate the IP camera when activating the device. See *Activating Your Device*.

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

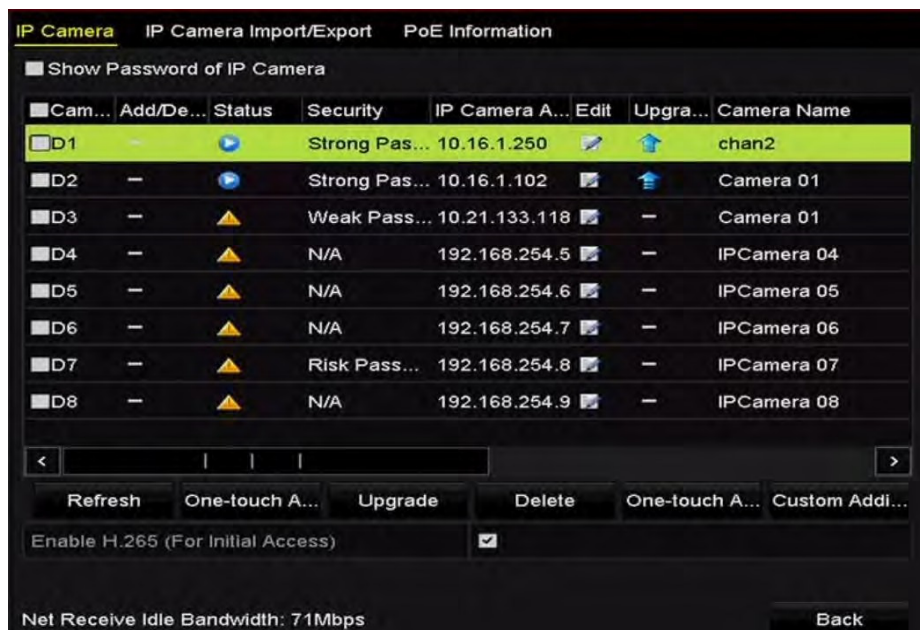


Figure 28, IP Camera Management Interface

2. Click the camera's inactive icon to enter the interface to activate it. You can also select multiple cameras from the list and click **One-touch Activate** to activate the cameras in batch.
3. Set the camera password to activate it.
  - **Use IP Camera Activation Password:** If you check this checkbox, the camera(s) will be configured with the same password that you set in the device activation interface. See *Activating Your Device*.



Figure 29, Set New Password

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



**STRONG PASSWORD RECOMMENDED** – We highly recommend that you create a strong password of your own choosing (using a minimum of eight 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. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

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 from it. So before you can get a live view or record of the video, add the network cameras to the device's connection list.

### Before You Start

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

## Adding the IP Cameras

### • OPTION 1


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 30, Adding IP Camera Icon

3. Select the detected IP camera and click the **Add** button to add it directly, you can click the **Search** button to refresh the online IP camera manually, or you can choose to custom add the IP camera by editing the parameters in the corresponding text field, and then click the **Add** button to add it.

Add IP Camera					
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				
Password					


**Search**      **Add**      **Cancel**

### • 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.



Figure 31, Adding IP Camera Interface

- Online cameras in the same network segment will be detected and displayed on the camera list.
- Select the IP camera from the list and click the  button to add the camera or click the **One-touch Adding** button to add all cameras (with the same login password) from the list.

**NOTE:** Make sure the camera to add has already been activated.

- (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 32, Selecting Multiple Channels

• **OPTION 3**

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



Figure 33, Custom Adding IP Camera Interface

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

**NOTE:** 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 **Continue to Add** checkbox to add additional IP cameras.
4. Click **Add** to add the camera. The successfully added cameras are listed in the interface.

Table 2-1 Description of Icons

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

**NOTE:** For the added IP cameras, the Security status shows the security level of the camera password: strong password, weak password, or risky 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 34, Security Level of IP Camera's Password

### Displaying the IP Camera Password

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

You must enter the admin password to confirm permission.



Figure 35, List of Added IP Cameras

### Enabling the H.265 Stream Access

Check the **Enable H.265** checkbox to have the NVR automatically switch to the H.265 stream of IP cameras that support the H.265 video format for the initial access.

## 2.3.3 Editing the Connected IP Cameras and Configuring Customized Protocols

After adding the IP cameras, the cameras' basic information lists in the page and you can configure the basic IP camera settings.

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



Figure 36, 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 drop-down list.

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

### To Edit Advanced Parameters


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



Figure 37, Camera Network Configuration

2. You can edit the camera's network information and password.



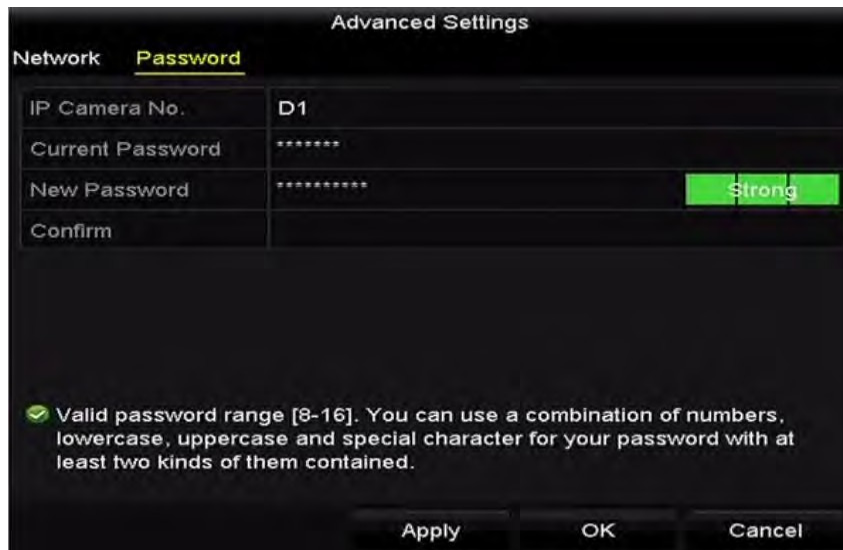


Figure 38, Camera Password Configuration

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

### Configuring Customized Protocols

#### Purpose

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

1. Click the **Protocol** button in the **Custom Adding IP Camera** interface to enter the protocol management interface.

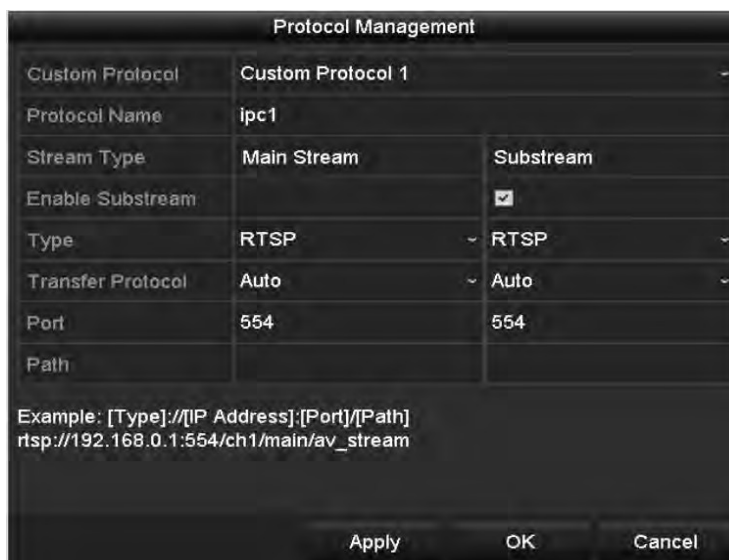


Figure 39, Protocol Management Interface

**NOTE:** 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 transmission type and choose the transfer protocols.

**NOTE:** Before customizing the protocol for the network camera, you have to contact the

network camera manufacturer to identify the URL (uniform resource locator) for getting the 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 cameras adopting custom protocols must support getting a stream through standard RTSP.
- **Transfer Protocol:** Select the transfer protocol for the custom protocol.
- **Port:** Set the custom protocol port no.
- **Path:** Set the resource path for the custom protocol (e.g., ch1/main/av\_stream).

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

After adding the customized protocols, you will see the protocol name is listed in the drop-down list, see below.



Figure 40, Protocol Setting

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

### 2.3.4 Editing IP Cameras Connected to the PoE Interfaces

**NOTE:** This chapter is applicable only to /P Series NVRs.

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

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

**Example:** For DS-7608NI-I2/8P, if you want to connect six network cameras via PoE interfaces and two online cameras, you must disable two PoE interfaces in the **Edit IP Camera** menu.

## To Add Cameras for NVR Supporting PoE Function

### Before You Start

Connect the network cameras via the PoE interfaces.

1. Enter the Camera Management interface, **Menu > Camera > IP 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
...		—		10.16.1.251		—	—	HIK

Refresh One-touch A... Upgrade Delete One-touch A... Custom Addi...  
Enable H.265 (For Initial Access)

Figure 41, List of Connected Cameras

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

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



Figure 42, Edit IP Camera Interface – Plug-and-Play

- **Manual:** You can disable the PoE interface by selecting **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.



Figure 43, Edit IP Camera Interface - Manual

### 2.3.5 Configuring PoE Interface

**NOTE:** This chapter is applicable only for /P Series NVRs.

When it requires long-distance PoE transmission (100 to 300 m), you can configure the PoE channel to the long network cable mode.

1. Enter the PoE Configuration interface, **Menu > Camera > Camera > PoE Configuration**.

2. Click the radio button of each PoE channel to switch **OFF** and **ON**. You can click the **PoE Channel** radio button to enable or disable the long network cable mode.
  - **ON**: Long-distance (100–300 meters) network transmissions via PoE interface.
  - **OFF**: Short-distance (<100 meters) network transmission via PoE interface.

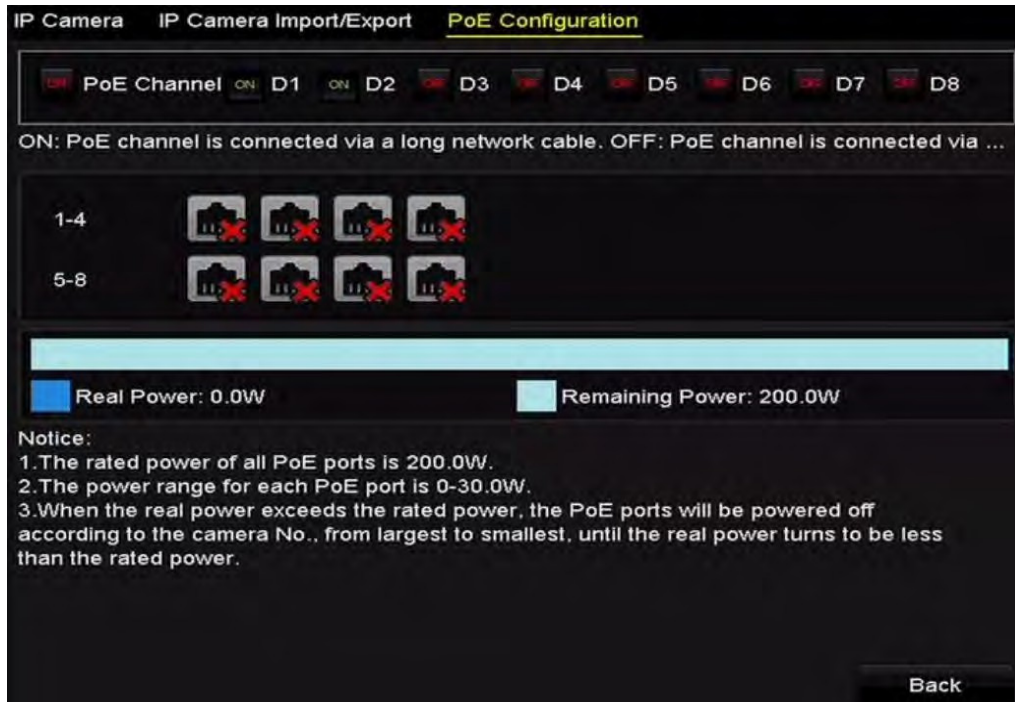


Figure 44, Configure PoE Interface

**NOTE:** The PoE is enabled with the short network cable mode (OFF) by default.

The bandwidth of IP camera connected to the PoE via long network cable (100–300 meters) cannot exceed 6 MP.

The allowed maximum long network cable may be less than 300 meters depending on IP camera model and cable materials.

When the transmission distance reaches 100 to 250 meters, you must use CAT5E or CAT6 network cable to connect with the PoE interface.

When the transmission distance reaches 250 to 300 meters, you must use CAT6 network cable to connect with the PoE interface.

Refer to the Appendix 16.3 List of IP Cameras Connected to PoE by Long Network Cable (100–300 m) for the list of IP cameras.

You can check the connecting status and power information of PoE channel on the interface.

3. Click **Back** to finish the settings.

# Chapter 3 Live View





## 3.1 Live View Introduction

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, <a href="#">video tampering</a> , <a href="#">motion detection</a> , <a href="#">VCA</a> , and sensor alarm)
	Record (manual record, schedule record, <a href="#">motion detection</a> , <a href="#">VCA</a> , and alarm triggered record)
	Alarm and Record
	Event/Exception ( <a href="#">motion detection</a> , <a href="#">VCA</a> , sensor alarm, or exception information appears at the lower-left corner of the screen; refer to <i>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:** Shows only one screen on the monitor
- **Multi-Screen:** Shows multiple screens on the monitor simultaneously
- **Auto-Switch:** Screen auto switches to the next one. You must set the dwell time for each screen on the configuration menu before enabling the auto-switch at **Menu > Configuration > Live View > Dwell Time**.
- **Start Recording:** Continuous record and [motion detection](#) record
- **Output Mode:** Set the output mode to Standard, Bright, Gentle, or Vivid.
- **Add IP Camera:** Shortcut to the IP camera management interface
- **Playback:** Play back the recorded videos for current day
- **Aux Monitor:** 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 HDMI and VGA are connected, HDMI is used as main output and VGA is used as the aux output.

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

### 3.2.1 Front Panel Operation on Live View

Table 3-2 Front Panel Operation in Live View

Functions	Front Panel Operation
Show Single Screen	Press the corresponding alphanumeric button. E.g. Press 2 to display only the screen for channel 2
Show Multi-Screen	Press the PREV/FOCUS button
Manually Switch Screens	Next screen: right/down direction button. Previous screen: left/up direction button
Auto-Switch	Press Enter button
Playback	Press Play button
Switch Between Main and Aux Output	Press Main/Aux 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
Single Screen	Switch to the single full screen by choosing channel number from the drop-down list
Multi-screen	Adjust the screen layout by choosing from the drop-down 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 <a href="#">motion detection</a> recording of all channels
Add IP Camera	Enter the IP Camera Management interface, and manage the cameras
Playback	Enter the playback interface and start playing back the video of the selected channel immediately
PTZ	Enter the <a href="#">PTZ</a> control interface
Output Mode	Four modes of output supported, including Standard, Bright, Gentle, and Vivid
Aux Monitor	Switch to the auxiliary output mode and the operation for the main output is disabled

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

If you enter Aux monitor mode and the Aux monitor is not connected, the mouse operation is disabled; you need to switch back to the Main output with the MAIN/AUX button on the front panel or remote.

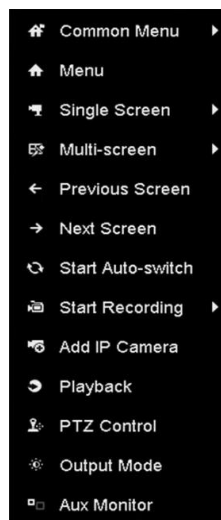


Figure 45, Right-Click Menu

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



### 3.2.3 Using an Auxiliary Monitor

Certain features of the Live View are also available while in an Aux monitor. These features include:

- **Single Screen:** Switch to a full screen display of the selected camera. Camera can be selected from a drop-down list.
- **Multi-Screen:** Switch between different display layout options. Layout options can be selected from a drop-down list.
- **Next Screen:** When displaying less than the maximum number of cameras in Live View, clicking this feature will switch to the next set of displays.
- **Playback:** Enter into Playback mode.
- **PTZ Control:** Enter PTZ Control mode.
- **Main Monitor:** Enter Main operation mode.

**NOTE:** In the live view mode of the main output monitor, the menu operation is not available while Aux output mode is enabled.

### 3.2.4 Quick Setting Toolbar in Live View Mode

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



Figure 46, 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
	Capture		PTZ Control		Digital Zoom
	Image Settings		Live View Strategy		Information
	Main/Sub-Stream		Close		

Instant Playback shows the record only in the 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 to the live image. You can zoom in the image to different magnifications (1x to 16x) by moving the sliding bar from to . You can also scroll the mouse wheel to zoom in/out.






Figure 47, Digital Zoom

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

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



Figure 48, Image Settings–Customize

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

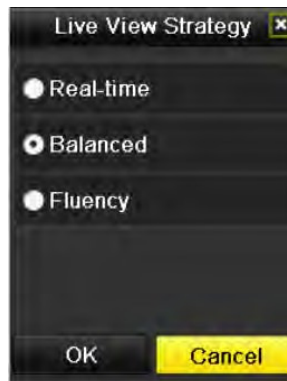


Figure 49, Live View Strategy

 Face detection function can be used to detect the human faces in live view mode and save in HDD.

When there are human faces with the specified size detected in the front of the camera, the device will capture the human face and save in HDD.


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



Figure 50, 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.

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

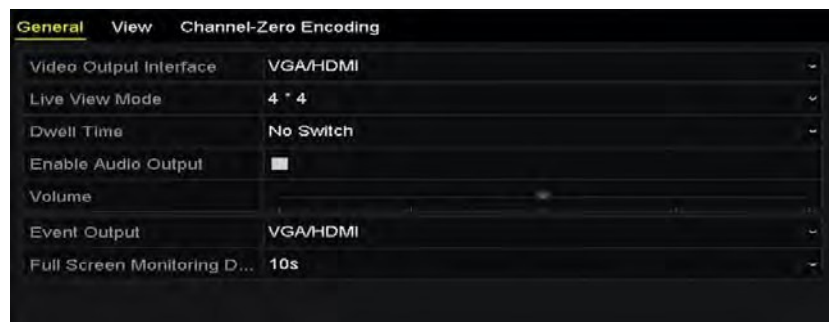


Figure 51, Live View-General

The settings available in this menu include:

- **Video Output Interface:** Select the video output to configure the live view parameters.
- **Live View Mode:** Select 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 eventscreen.

2. Set cameras' order.

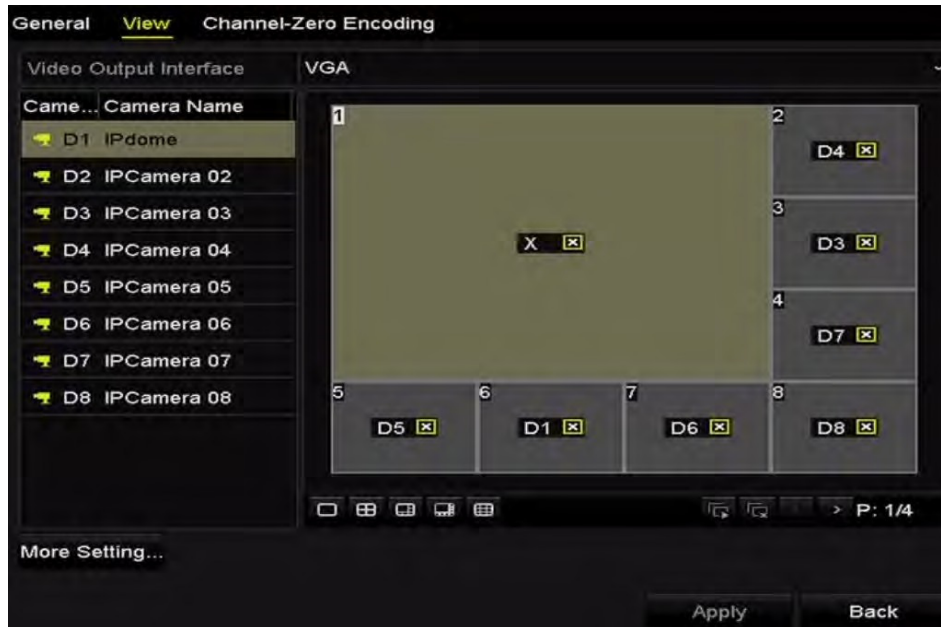


Figure 52, Live View–Camera Order

- 1) Select a **View** mode in , 1/4/6/8/16-window division modes are supported depending on model.
- 2) Select the small window, and double-click the channel number to display the channel on the window.
- 3) You can click the button to start live view for all channels and click to stop all live views.
- 4) Click the **Apply** button to save the setting.

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

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 53, Stream Type Settings

- 4) Click **Apply** to save the settings.
- 5) (Optional) 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 a Web browser or CMS (Client Management System) software. To decrease the bandwidth requirement without affecting the image quality, channel-zero encoding is supported as an option.

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

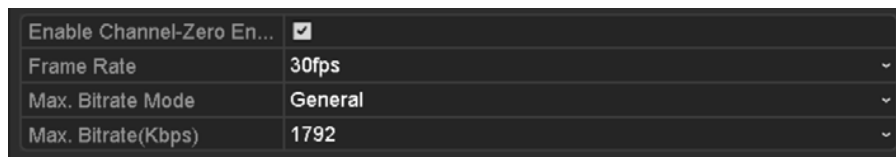


Figure 54, Live View-Channel-Zero Encoding

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

After you set the Channel-Zero encoding, you can view in the remote client or Web browser 16 channels on one screen.

## Chapter 4 PTZ Controls

### 4.1 Configuring PTZ Settings

#### Purpose

Follow these procedures to set the **PTZ** parameters. The configuring of the **PTZ** parameters should be done before you control the **PTZ** camera.

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



Figure 55, PTZ Settings

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



Figure 56, PTZ-General

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

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

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

## 4.2 Setting PTZ Presets, Patrols, and Patterns

### Before You Start

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

### 4.2.1 Customizing Presets

#### Purpose

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

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




Figure 57, PTZ Settings

2. Use the directional button to wheel the camera to the location where you want to set the 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.
4. Repeat steps 2–3 to save more presets.
5. You can click the **Clear** button to clear the preset location information, 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.

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 the **Camera** in the drop-down list.



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



Figure 58, 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. Key points correspond to the presets. The presets can be set following the steps above in Customizing Presets.

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



Figure 59, PTZ Settings

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



Figure 60, Key Point Configuration

4. Configure key point parameters such as the key point no., duration of staying at one key point, and patrol speed. The key point corresponds to the preset. The **Key Point No.** determines the order in which the PTZ will follow while cycling through the patrol. **Duration** refers to the time span to stay at the corresponding key point. **Speed** defines the speed at which the PTZ will move from one key point to the next.
5. Click the **Add** button to add the next key point to the patrol, or you can click the **OK** button to save the key point to the patrol.

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

## 4.2.4 Calling Patrols

### Purpose

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



1. Click the PTZ button 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 61, PTZ Panel–General

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



## 4.2.5 Customizing Patterns

### Purpose

Patterns can be set by recording the [PTZ](#) movement. You can call the pattern to have the [PTZ](#) move according to the predefined path.

1. Enter the [PTZ](#) Control interface, **Menu > Camera > PTZ**.



Figure 62, [PTZ](#) Settings

2. Choose pattern number in the drop-down 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.



1. Click the [PTZ](#) button 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 63, 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.

**NOTE:** This function is supported by certain models.

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



Figure 64, PTZ Settings

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

**NOTE:** The speed dome starts linear scan from the left limit to the right limit, and you must set the left limit to 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

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

### Purpose

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



1. Click the **PTZ** button 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 65, **PTZ** Panel–One-Touch

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

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

## 4.2.9 One-Touch Park

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

### Purpose

Certain models of speed dome can be configured to start a predefined park action (scan, preset, patrol, etc.) automatically after a period of inactivity (park time).



1. Click the **PTZ** button 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 66, PTZ Panel–One-Touch

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


- **Park (Quick Patrol):** The dome starts patrol from predefined preset 1 to preset 32 in order after the park time. Undefined presets will be skipped.
- **Park (Patrol 1):** The dome starts to move according to the predefined patrol 1 path after the park time.
- **Park (Preset 1):** The dome moves to the predefined preset 1 location after the park time.

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

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 (next to the Back button).
- **OPTION 2:** In Live View mode, press the PTZ Control button on the front panel or on the remote control, or choose the PTZ Control icon , or select the PTZ option in the right-click menu.

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


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



Figure 67, PTZ Panel

Table 4-1 Description of the PTZ panel icons

Icon	Description	Icon	Description	Icon	Description
	Direction button and the auto-cycle button		Zoom+, Focus+, Iris+		Zoom-, Focus-, Iris-
	The speed of the PTZ movement		Light on/off		Wiper on/off
	3D Positioning		Image Centralization		Menu
	Switch to the PTZ control interface		Switch to the one-touch control interface		Switch to the general settings interface
	Previous item		Next item		Start pattern/ patrol
	Stop the patrol/pattern movement		Exit		Minimize windows

## Chapter 5 Recording Settings

### 5.1 Configuring Parameters

#### Purpose

By configuring the parameters you can define the parameters that affect the image quality such as the transmission stream type, the resolution, etc.

#### Before You Start

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

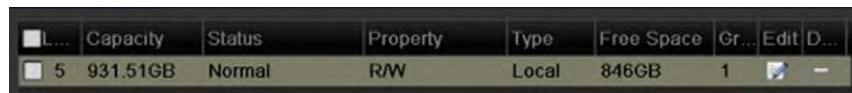


Figure 68, HDD-General

2. Click **Advanced** to check the storage mode of the HDD.
  - If the HDD mode is *Quota*, set the maximum record capacity and maximum picture capacity. For detailed information, see *Configuring Quota Mode*.

- If the HDD mode is **Group**, set the HDD group. For detailed information, see *Configuring HDD Group for Recording*.

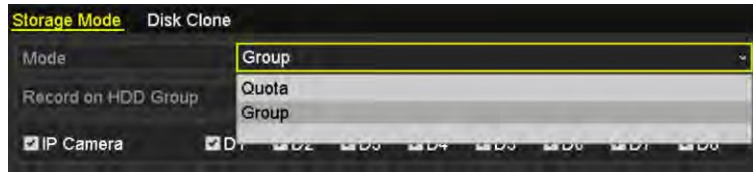


Figure 69, HDD–Advanced

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



Figure 70, Recording Parameters

4. Set recording parameters
  - 1) Select **Record** tab page to configure. You can configure the stream type, the resolution, and other parameters on demand.
    - **Video Encode:** Set the video encoding to H.265 or H.264.
    - **Enable H.264+ Mode:** Check the checkbox to enable. Once enabled, the **Max. Bitrate Mode**, **Max. Bitrate (Kbps)** and **Max. Bitrate Range Recommend** are not configurable. Enabling it helps to ensure high video quality with a lowered bitrate.

**NOTE:** The H.265 and H.264+ should be supported by the connected IP camera.
  - 2) Click the **More Settings** button to set the advanced parameters for recording, and then click the **OK** button to finish editing.



Figure 71, More Settings

- **Pre-Record:** The time you set to record before the scheduled time or event. For example, when an alarm triggers the recording at 10:00, and if you set the pre-record time as 5 seconds, the camera starts recording at 9:59:55.
- **Post-Record:** The time you set to record after the event or the scheduled time. For example, when an alarm triggered recording ends at 11:00, and if you set the post-record time as 5 seconds, it will record until 11:00:05.
- **Expired Time:** The expired time is the time period for a recorded file to be kept in the HDD. When the deadline is reached, the file will be deleted. If you set the expired time to 0, the file will not be deleted. The actual keeping time for the file should be determined by the HDD capacity.
- **Redundant Record/Capture:** By enabling redundant record or capture, you save the record and captured picture in the redundant HDD. See *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.

**NOTE:** You can enable the ANR (Automatic Network Replenishment) function via the Web browser (**Configuration > Storage > Schedule Settings > Advanced**) to save the video files in the IP camera when the network is disconnected, and synchronize the files to the NVR when the network resumes.

**NOTE:** The redundant record/capture is used when you want to save the record files or captured pictures in the redundant HDD. You must configure the redundant HDD in HDD settings.

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

5. Set sub-stream parameter settings

1) Enter the Sub-stream tab page.



Record	Substream	Capture
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 72, Sub-Stream Parameters

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

## 5.2 Configuring Recording Schedule

### Purpose

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

**NOTE:** In this chapter, we take the record schedule procedure as an example. The same procedure can be applied to configure the schedule for both recording and capture. To schedule automatic capture, choose the Capture tab in the **Schedule** interface.

1. Enter the Record Schedule interface, **Menu > Record > Schedule**.
2. Configure Record Schedule.
  - 1) Select Record Schedule. Different recording types are marked in different color icons.
    - **Continuous:** Scheduled recording
    - **Event:** Recording triggered by all **event** triggered alarm
    - **Motion:** Recording triggered by **motion detection**
    - **Alarm:** Recording triggered by alarm
    - **M/A:** Recording triggered by either **motion detection** or alarm
    - **M&A:** Recording triggered by **motion detection** and alarm

**NOTE:** You can delete the set schedule by clicking the **None** icon

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



## Edit the Schedule



Figure 73, Recording Schedule Interface

**NOTE:** All-day continuous recording is configured for the device by factory default.

1. In the message box, choose the day for which you want to set a schedule.

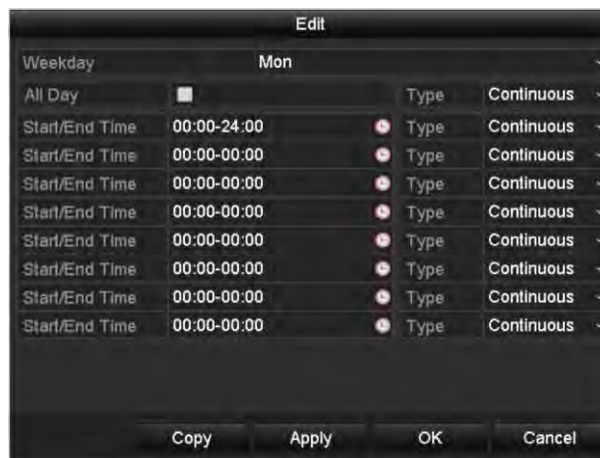



Figure 74, Recording Schedule Interface

2. You can click the  button to set the accurate time of the schedule.
3. To schedule an all-day recording, check the checkbox after the **All Day** item.

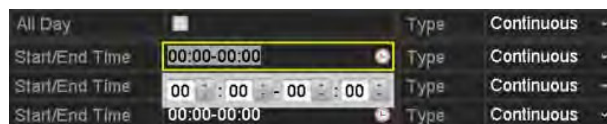


Figure 75, Edit Schedule

4. To arrange other schedules, set the Start/End time for each period.

**NOTE:** Up to eight periods can be configured for each day. Time periods can't overlap.

5. Select the record type in the drop-down list.

**NOTE:** 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.

The **VCA** settings are available only for smart IP cameras.

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



Figure 76, Copy Schedule to Other Days

7. Click **OK** to save setting and go back to the upper level menu.

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

### Draw the Schedule

1. Click on the color icons to choose the schedule type as continuous or event.

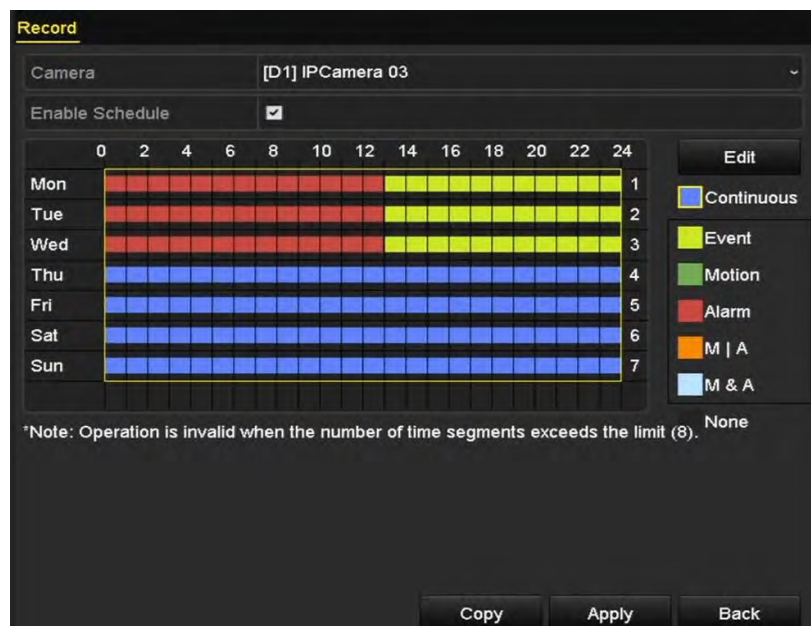


Figure 77, Draw the Schedule

2. 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.



Figure 78, Copy Schedule to Other Channels

## 5.3 Configuring Motion Detection Recording

### Purpose

Follow the steps to set the [motion detection](#). In the live view mode, once a [motion detection](#) event takes place, the NVR can analyze it and take alarm response actions. 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 triggered by detected motion.

1. Enter the [Motion Detection](#) interface, **Menu > Camera > Motion**.

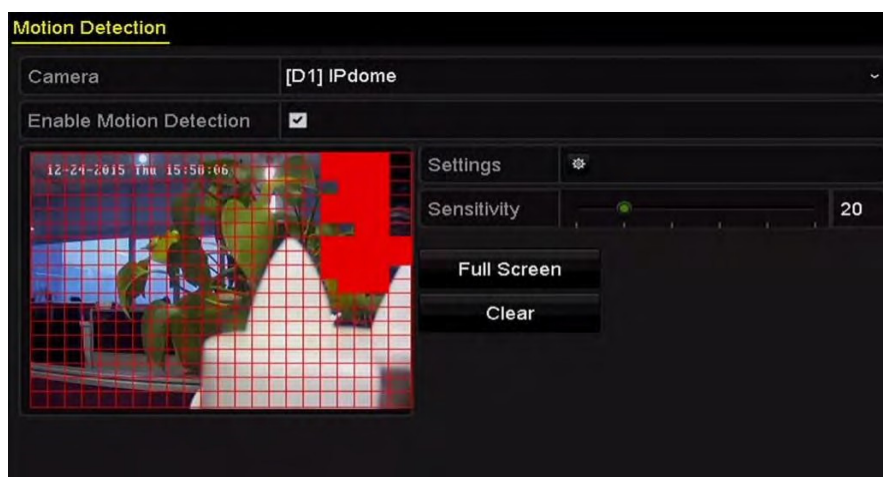


Figure 79, Motion Detection

2. Configure [Motion Detection](#).
  - 1) Choose camera you want to configure.

- 2) Check the **Enable Motion Detection** checkbox.
- 3) Drag and draw the [motion detection](#) area with the mouse. If you want to set the [motion detection](#) for all the area shot by the camera, click **Full Screen**. To clear the [motion detection](#) area, click **Clear**.
- 4) Click **Settings**, and the message box for channel information pops up.



Figure 80, [Motion Detection](#) Handling

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

## 5.4 Configuring Alarm Triggered Recording

### Purpose

Follow the procedure to configure alarm triggered recording.

1. Enter the Alarm settings interface, **Menu > Configuration > Alarm**.

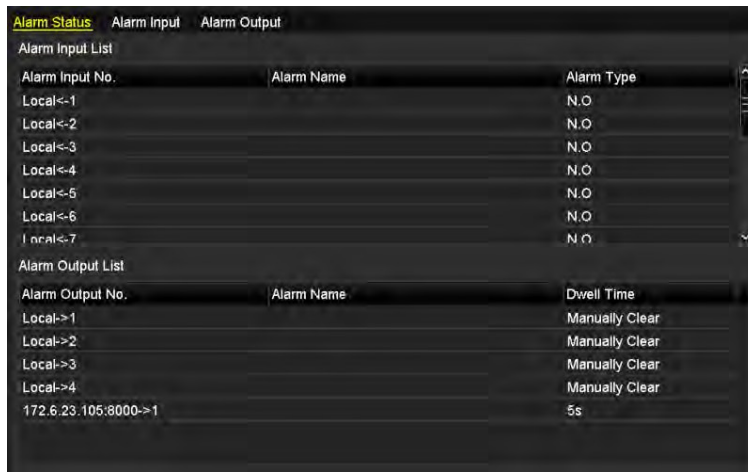


Figure 81, Alarm Settings

2. Click **Alarm Input**.



Figure 82, Alarm Settings–Alarm Input

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



Figure 83, 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 go back to the upper level menu.
- 9) Repeat the above steps to configure other alarm input parameters.
- 10) If the settings can also be applied to other alarm inputs, click **Copy** and choose the alarm input number.



Figure 84, Copy Alarm Input

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

## 5.5 Configuring VCA Event Recording

### Purpose

The event triggered recording can be configured through the menu. Events include [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](#)).

1. Enter the [VCA](#) settings interface and select a camera for the [VCA](#) settings, **Menu > Camera > VCA**.

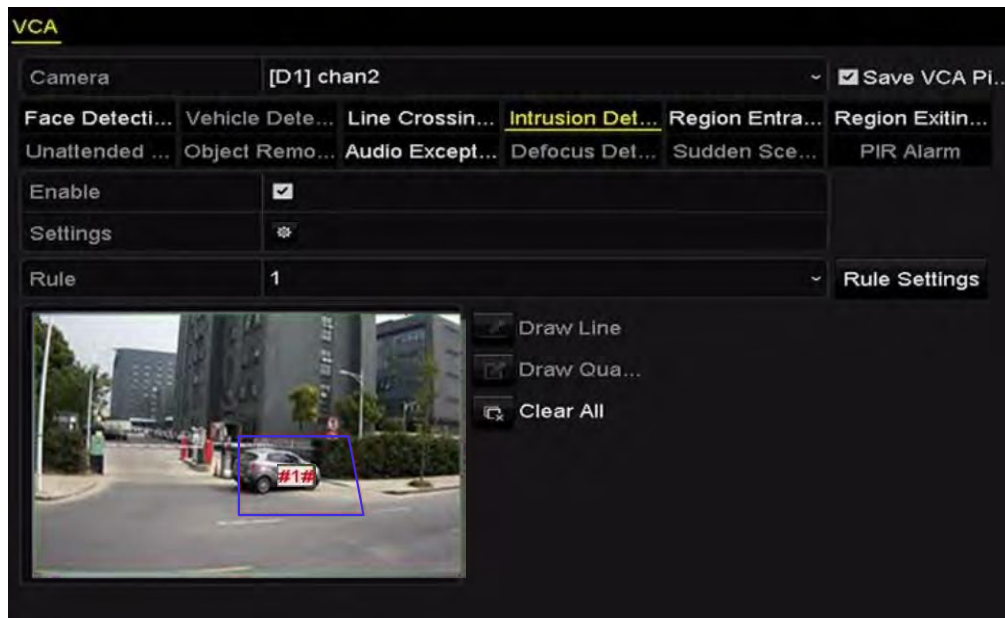


Figure 85, VCA Settings


2. Configure the detection rules for VCA events. For details, refer to [VCA Alarm](#).
3. Click the  icon to configure the alarm linkage actions for the VCA events.
4. Select **Trigger Channel** tab, and select one or more channels which will start to record when VCA alarm is triggered.
5. Click **Apply** to save the settings



Figure 86, Set Trigger Camera of VCA Alarm

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

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

## 5.6 Manual Recording

### Purpose

Follow the steps to set parameters for the manual recording and continuous capture. Using manual

recording and continuous capture, you need to manually cancel the record and capture. The manual recording and manual continuous capture is prior to the scheduled recording and capture.

1. Enter the Manual settings interface, **Menu > Manual**, or press the **REC/SHOT** button on the front panel.



Figure 87, Manual Record

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

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

## 5.7 Configuring Holiday Recording

### Purpose

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

1. Enter the Record setting interface, **Menu > Record > Holiday**.



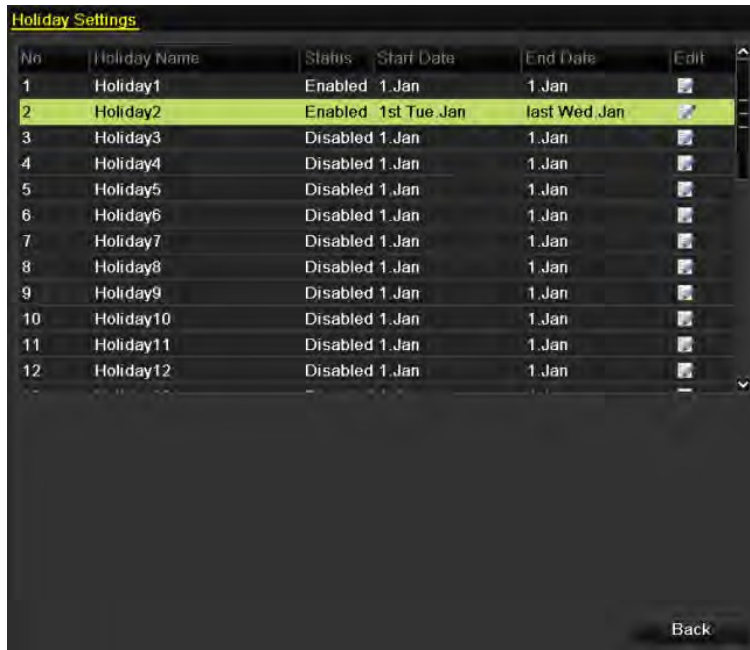


Figure 88, Holiday Settings

2. Enable **Edit Holiday** schedule.

1) Click to enter the **Edit** interface.



Figure 89, Edit Holiday Settings

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

3) Select Mode from the drop-down list.

4) There are three different modes for the date format to configure holiday schedule.

5) Set the start and end date.

6) Click **Apply** to save settings.

7) Click **OK** to exit the Edit interface.

3. Enter Record/Capture Schedule settings interface to edit the holiday recording schedule.

## 5.8 Configuring Redundant Recording

### Purpose

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

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

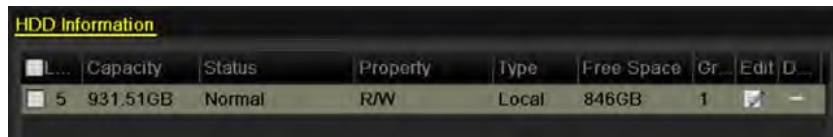


Figure 90, HDD General

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

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



Figure 91, HDD General—Editing

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

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

3. Enter the Record setting interface, **Menu > Record > Parameters**.

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



Figure 92, Record Parameters

- 3) Select Camera you want to configure in the drop-down list.
- 4) Check the checkbox of **Redundant Record/Capture**.
- 5) Click **OK** to save settings and back to the upper level menu. Repeat the above steps to configure other channels.

## 5.9 Configuring HDD Group for Recording

### Purpose

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

1. Enter HDD setting interface, **Menu > HDD**.




Figure 93, HDD General

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



Figure 94, Storage Mode

3. Check if the storage mode of the HDD is Group. If not, set it to Group. For detailed information, refer to *Managing HDD Group*.
4. Select **General** in the left side menu S
5. Click  to enter editing interface.
6. Configuring HDD group.
  - 1) Choose a group number for the HDD group.

- 2) Click **Apply**, and in the pop-up message box, click **Yes** to save your settings.
  - 3) Click **OK** to go back to the upper level menu.
  - 4) Repeat the above steps to configure more HDD groups.
7. Choose the Channels that you want to save the record files in the HDD group.
- 1) Select **Advanced** on the left bar.
  - 2) Choose Group number in the drop-down list of Record on HDD Group
  - 3) Check the channels you want to save in this group.
  - 4) Click **Apply** to save settings.

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

## 5.10 Files Protection

### Purpose

You can lock the 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**
  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 95, Normal/Smart Playback

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

**NOTE:** 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 96, 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**

1. Enter Export setting interface, **Menu > Export**.



Figure 97, Export

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



Figure 98, Export–Search Result

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

**NOTE:** The record files for which recording is still not completed cannot be locked.

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




Figure 99, Unlocking Attention

## 5.10.2 Setting HDD Property to Read-only

1. Enter HDD setting interface, **Menu > HDD**.

HDD Information							
L...	Capacity	Status	Property	Type	Free Space	Gr...	Edit D...
5	931.51GB	Normal	R/W	Local	846GB	1	✎

Figure 100,, HDD General

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



The dialog box titled "Local HDD Settings" contains the following fields and options:

- HDD No.: 5
- HDD Property:
  - R/W
  - Read-only
  - Redundancy
- Group:
  - 1  2  3  4  5  6  7  8
  - 9  10  11  12  13  14  15  16
- HDD Capacity: 931.51GB

Buttons at the bottom: Apply, OK, Cancel

Figure 101, HDD General- Editing

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

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

**NOTE:** You cannot save any files in a Read-only HDD. If you want to save files in the HDD, change the property to R/W.

If there is only one HDD and is set to Read-only, the 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



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

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



Figure 102, 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.

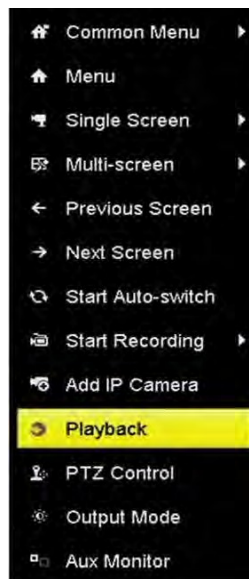


Figure 103, Right-Click Menu under Live View

**NOTE:** 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.

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.

**NOTE:** The main stream or sub stream for recording is configurable in **Menu > Record > Parameters**.

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



Figure 104, 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.

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

### Playback Interface

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



Figure 105, Playback Interface



Figure 106, Playback Toolbar

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

**NOTE:** The **05-06-2016 16:33:42 -- 06-07-2016 10:53:24** indicates 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 <a href="#">motion detection</a>		Search the matched video
		Set full screen for <a href="#">motion detection</a>		Draw line for the <a href="#">line crossing detection</a>
		Draw quadrilateral for the <a href="#">intrusion detection</a>		Filter video files by setting the target characters
Operations		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		
Playing Control		Pause/Play		Reverse play/Pause
		Slow forward		Stop
		30s forward		30s reverse
		Next day		Fast forward
		Previous day		
Time Bar Scaling		Previous/Next period		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

**NOTE:** 256x playing speed is supported.

### 6.1.3 Playing back by Smart Search

#### Purpose

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

1. Enter Playback interface, **Menu > Playback**.
2. Select **Normal/Smart** in the drop-down list on the top-left side.

**NOTE:** The main stream or sub stream for recording is configurable in **Menu > Record > Parameters**.

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 107, 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.
- **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 four points to set a quadrilateral region for intrusion detection. Only one region can be set.
  - **Motion Detection:** Click the  button, and then hold the mouse on the image to draw the detection area manually. You can also click the  button to set the full screen as the detection area.
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 108, 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](#)).

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.


**NOTE:** We take playback by [VCA](#) as an example in the following instructions.



Figure 109, [Event Search](#) Interface

4. Select the minor type of [VCA](#) from the drop-down list. (Refer to [VCA Alarm](#) for [VCA](#) detection types).

**NOTE:** For configuring the [VCA](#) recording, refer to *Configuring VCA Event Recording and Capture*. For [VCA](#) detection type details, refer to [VCA Alarm](#).

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

**NOTE:** Pre-play and post-play can be configured.

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



Figure 110, Synch Playback Interface

9. Enter the playback interface.

The toolbar in the bottom of the playback interface can control the playing process.



Figure 111, Interface of Playback by Event

You can click the or button to select the previous or next event. Refer to Table 6.1 for the description of buttons on the toolbar.



## 6.1.5 Playing Back by Tag

### Purpose



Video tags allow you to record related information such as people and locations 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).



Figure 112, Interface of Playback by Time

3. Set tags, as desired.
  - Click the  button to add a default tag.
  - Click the  button to add a customized tag and input tag name.


**NOTE:** 64 tags maximum can be added to a single video file.
4. Tag management.
  - Click the  button to enter the File Management interface, and click **Tag** to manage the tags. You can check, edit, and delete tag(s).



Figure 113, Tag Management Interface

### Playing Back by Tag

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

**NOTE:** You can enter a keyword in the textbox  to search for the tag on your command.




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



Figure 114, Interface of Playback by Tag

**NOTE:** Pre-play and post-play can be configured.

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

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

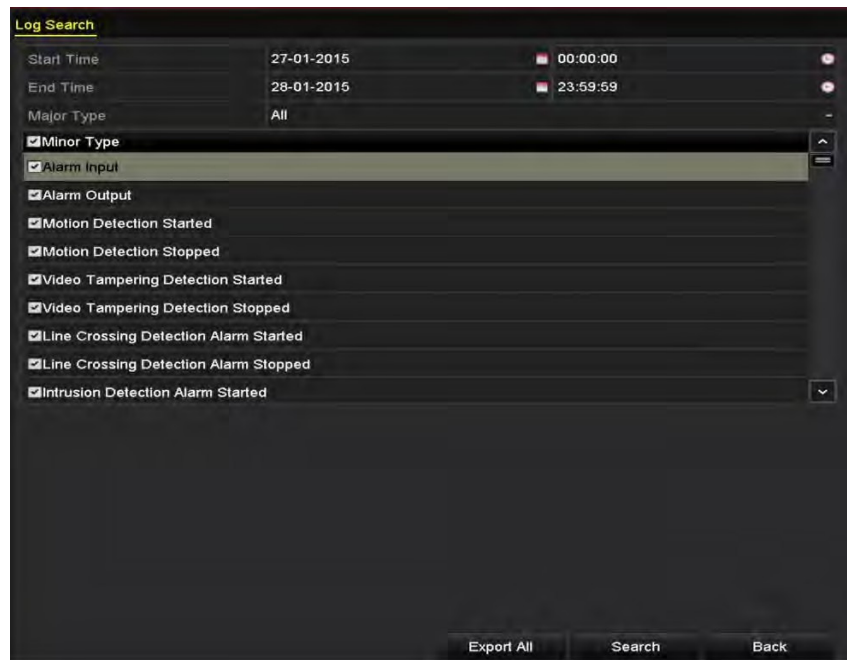



Figure 115, System Log Search Interface

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

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



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 116, Result of System Log Search

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



Figure 117, 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.

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 it back. Adjust the playback speed by clicking  and .



Figure 118, Interface of External File Playback

## 6.2 Auxiliary Playback Functions

### 6.2.1 Playing Back Frame-by-Frame

#### Purpose

Play video files frame-by-frame, to check video image details when abnormal events happen.

Go to Playback interface.

If you choose playback of the record file: click the **⏮** button until the speed changes to Single frame, where one click on the playback screen will play back one frame.

If you choose reverse playback of the record file, click the **⏮** button until the speed changes to Single frame, and one click on the playback screen will reverse playback one frame. It is also possible to use the **⏮** button in the toolbar.

### 6.2.2 Thumbnails View

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

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



Figure 119, Thumbnails View

**NOTE:** The thumbnail view is supported only in the 1x single-camera playback mode.

### 6.2.3 Fast View

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

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

**NOTE:** The fast view is supported only in the 1x single-camera playback mode.

### 6.2.4 Digital Zoom




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



Figure 120, 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, captured pictures in playback, locked files, and tags you have added in the playback mode.


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



Figure 121, File Management

3. You can view the saved video clips, lock/unlock the files, and edit the tags that you added in playback mode.
4. If required, select the items and click **Export All** or **Export** to export the clips/pictures/files/tags to a 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.

1. Enter Video Export interface, **Menu > Export > Normal**.
2. Choose the channel(s) you want to back up, and click **Quick Export** button.

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

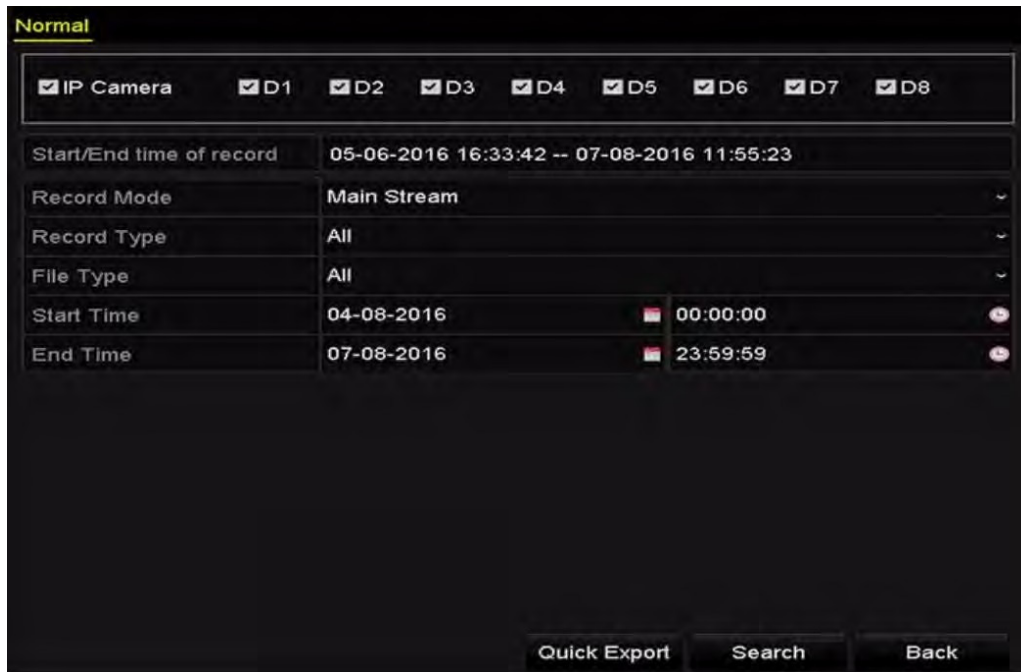


Figure 122, Quick Export Interface

3. Select the format of the log files to be exported. Up to 15 formats are selectable.
4. Click the **Export** to start exporting.

**NOTE:** Here we use a USB Flash Drive. Refer to the next section, *Normal Backup*, for more backup devices supported by the NVR.

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






Figure 123, Quick Export using USB1-1



Figure 124, Export Finished

5. Check backup result.
6. Choose the record file in the Export interface, and click the  button to check it.

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



Figure 125, 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 NVR User Manual 061220NA


writer), or a SATA writer.

## Backup Using USB Flash Drives and USB HDDs

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



Figure 126, 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.

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



Figure 127, Result of Normal Video Search for Backup

5. Export the video files or picture files.

- Click the **Export All** button to export all the files, or you can select recording files you want to back up, and click the **Export** button to enter the Export interface.

**NOTE:** If the inserted USB device is not recognized:

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

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



Figure 128, Export by Normal Video Search using USB Flash Drive

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





Figure 129, Export Finished

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

### 7.1.3 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.

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



Figure 130, Event Search for Backup

4. Set the search conditions, and click the **Search** button to enter the search result interface. For the POS event type, you can also set the Keyword and enable the Case Sensitivity (upper case and lower case) to search the video files with the key word containing the POS information.
5. The matched video files are displayed in Chart or List display mode. Select video files from the Chart or List interface to export.



Figure 131, Result of [Event Search](#)

- Export the video files. Refer to step 5 of *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.

- Enter the Playback interface.

**NOTE:** Refer to *Playing Back Record Files*.

- During playback, use or in the playback toolbar to start or stop clipping record file (s); or use the button to capture pictures.
- Click the to enter the file management interface.



Figure 132, Video Clips or Captured Pictures Export Interface

- Export the video clips or captured pictures in playback. Refer to step 5 of *Backing up by Normal Video Search* for details.

## 7.2 Managing Backup Devices

### Management of USB Flash Drives, USB HDDs, and eSATA HDDs

1. Enter the Export interface.



Figure 133, 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 the button if you want to delete it.
3. Click the **Erase** button if you want to erase the files from a re-writable CD/DVD. Click the **Format** button to format the backup device.

**NOTE:** If the inserted storage device is not recognized:

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

## Chapter 8 Alarm Settings

### 8.1 Setting Motion Detection Alarm

1. Enter the Camera Management [Motion Detection](#) interface, and choose a camera for which you want to set up [motion detection](#), **Menu > Camera > Motion**.

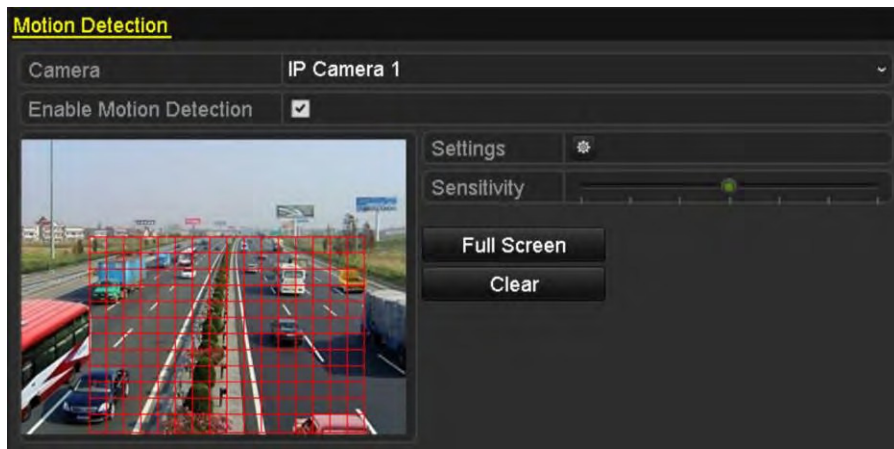


Figure 134, Motion Detection Setup Interface


2. Set up detection area and sensitivity.
3. Tick "Enable Motion Detection," use the mouse to draw detection area(s), and drag the sensitivity bar to set sensitivity.
4. Click the  button, and set alarm response actions.
5. Click the **Trigger Channel** tab, and select one or more channels that will start to record/capture or become full-screen monitoring when motion alarm is triggered, and click **Apply** to save the settings.



Figure 135, Set Trigger Camera of Motion Detection

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

**NOTE:** Time periods shall not repeat or overlap.



Figure 136, Set Arming Schedule of Motion Detection

7. Click **Handling** tab to set up alarm response actions of motion alarm (refer to *Setting Alarm Response Actions*).
8. 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.

1. Enter Alarm Settings of System Configuration and select an alarm input, **Menu > Configuration > Alarm**.
2. Select Alarm Input tab to enter Alarm Input Settings interface.



Figure 137, Alarm Status Interface of System Configuration

3. Set up the handling action of the selected alarm input.
4. Check the **Enable** checkbox and click the **Settings** button to set up its alarm response actions.



Figure 138, Alarm Input Setup Interface

5. (Optional) Enable the one-key disarming for local alarm input 1 (Local<-1).
  - 1) Check the **Enable One-Key Disarming** checkbox.
  - 2) Click the **Settings** button to enter the linkage action settings interface.
  - 3) Select the alarm linkage action(s) you want to disarm for the local alarm input. The selected linkage actions include Full Screen Monitoring, Audible Warning, Notify Surveillance Center, Send E-mail, and Trigger Alarm Output.

**NOTE:** When alarm input 1 (Local<-1) is enabled with one-key disarming, the other alarm input settings are not configurable.
6. Select the Trigger Channel tab and select one or more channels that will start to record/capture or become full-screen monitoring when an external alarm is input, and click **Apply** to save the settings.
7. Select the **Arming Schedule** tab to set the arming schedule of handling actions.



Figure 139, Set Arming Schedule of Alarm Input

- Choose one day of a week. A maximum of eight time periods can be set within each day. Click **Apply** to save the settings.

**NOTE:** Time periods cannot repeat or overlap.

8. Repeat the above steps to set up arming schedule of other days of a week. You can also use the **Copy** button to copy an arming schedule to other days.
9. Select **Linkage Action** tab to set up alarm response actions of the alarm input (refer to *Chapter Setting Alarm Response Actions*).

- If necessary, select **PTZ** Linking tab and set **PTZ** linkage of the alarm input.
- Set **PTZ** linking parameters and click **OK** to complete the settings of the alarm input.

**NOTE:** Make sure the connected **PTZ** or speed dome supports **PTZ** linkage.



Figure 140, Set **PTZ** Linking of Alarm Input

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

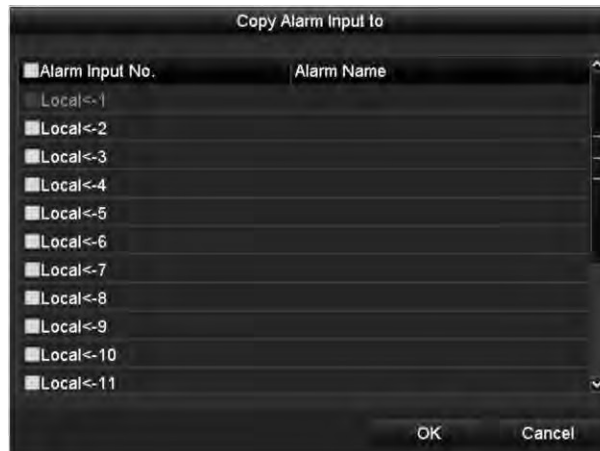


Figure 141, Copy Settings of Alarm Input

## 8.3 Detecting Video Loss Alarm

### Purpose


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

- Enter Video Loss interface of Camera Management, and select a channel you want to detect, **Menu > Camera > Video Loss**.





Figure 142, Video Loss Setup Interface

2. Set up handling action of video loss.
  - Check the "Enable Video Loss Alarm" checkbox, and click the  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 the week. Up to eight time periods can be set within each day.
  - 3) Click the **Apply** button to save the settings.

**NOTE:** Time periods cannot repeat or overlap.



Figure 143, Set Arming Schedule of Video Loss

4. Select **Linkage Action** tab to set up alarm response action of video loss (refer to *Chapter 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).

1. Enter [Video Tampering](#) interface of Camera Management, and select a channel for which you want to detect [video tampering](#), **Menu > Camera > Video Tampering**.

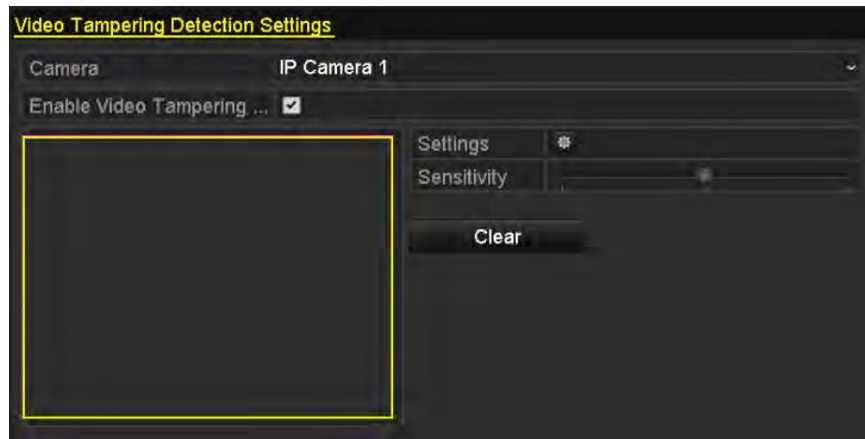



Figure 144, [Video Tampering](#) Setting Interface

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

**NOTE:** Time periods cannot repeat or overlap.

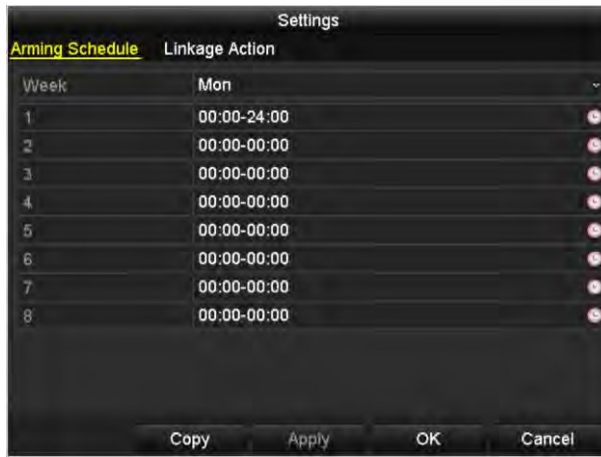


Figure 145, Set Arming Schedule of [Video Tampering](#)

4. Select **Linkage Action** tab to set up alarm response actions of [video tampering alarm](#) (refer to *Chapter 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.

- **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/Capture Exception:** No space for saving recorded files or captured images
- **Hot Spare Exception:** Disconnected with the working device

1. Enter the System Configuration Exception interface. and handle various exceptions, **Menu > Configuration > Exceptions**.

**NOTE:** Refer to *Setting Alarm Response Actions* for detailed alarm response actions.



Figure 146, Exceptions Setup Interface

## 8.6 Setting Alarm Response Actions

### Purpose

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

### Event Hint Display

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

1. Enter the Exception settings interface, **Menu > Configuration > Exceptions**.



Figure 147, Event Hint Settings Interface

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

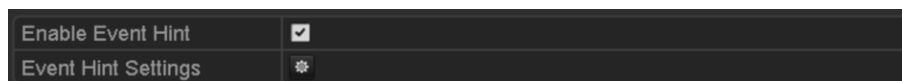



Figure 148, Event Hint Settings Interface

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

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

### Full Screen Monitoring

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

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

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

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

### Audible Warning

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

### Notify Surveillance Center

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

**NOTE:** The alarm signal will be transmitted automatically at detection mode when a remote alarm host is configured. Refer to *Configuring More Settings* for details of alarm host configuration.

### E-Mail Linkage

Send an e-mail with alarm information to a user or users when an alarm is detected. Refer to *Configuring Email* for details of e-mail configuration.

### Trigger Alarm Output

Trigger an alarm output when an alarm is triggered.

1. Enter Alarm Output interface, **Menu > Configuration > Alarm > Alarm Output**.
2. Select an alarm output, and set alarm name and dwell time.
3. Click **Schedule** button to set the arming schedule of alarm output.

**NOTE:** If “Manually Clear” is selected in the Dwell Time drop-down list, you can clear it only by going to **Menu > Manual > Alarm**.



Figure 149, Alarm Output Setup Interface

4. Set up arming schedule of the alarm output. Choose one day of the week. Up to eight time periods can be set within each day.

**NOTE:** Time periods cannot repeat or overlap.



Figure 150, Set Arming Schedule of Alarm Output

5. Repeat the above steps to set up arming schedule of other days of a week. You can also use the **Copy** button to copy an arming schedule to other days.
6. Click the **OK** button to complete the [video tampering](#) settings of the alarm output no.
7. You can also copy the above settings to another channel.

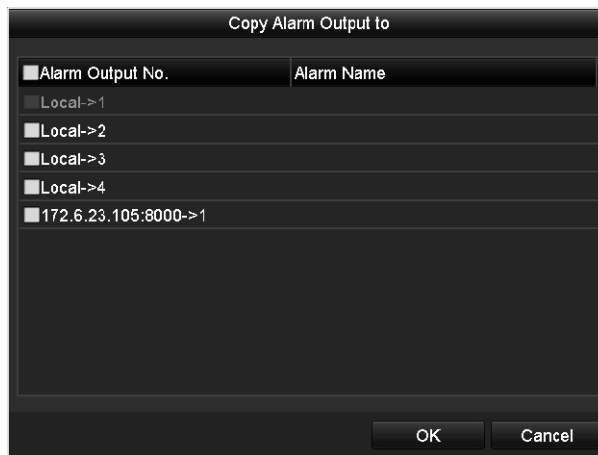


Figure 151, Copy Settings of Alarm Output

## 8.7 Triggering or Clearing Alarm Output Manually

### Purpose

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

1. Select the alarm output you want to trigger or clear, and make related operations, **Menu > Manual > Alarm**.
2. Click the **Trigger/Clear** button if you want to trigger or clear an alarm output.
3. Click the **Trigger All** button if you want to trigger all alarm outputs. Click **Clear All** button if you want to

clear all alarm outputs.



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 152, Clear or Trigger Alarm Output Manually

## Chapter 9 VCA Alarm

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

**NOTE:** VCA detections must be supported by the connected IP camera.

Refer to the User Manual of Network Camera for the detailed instructions for the all VCA detection types.

### 9.1 Face Detection

#### Purpose

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

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

**NOTE:** Click the **Save VCA Picture** checkbox to save the captured VCA detection pictures.

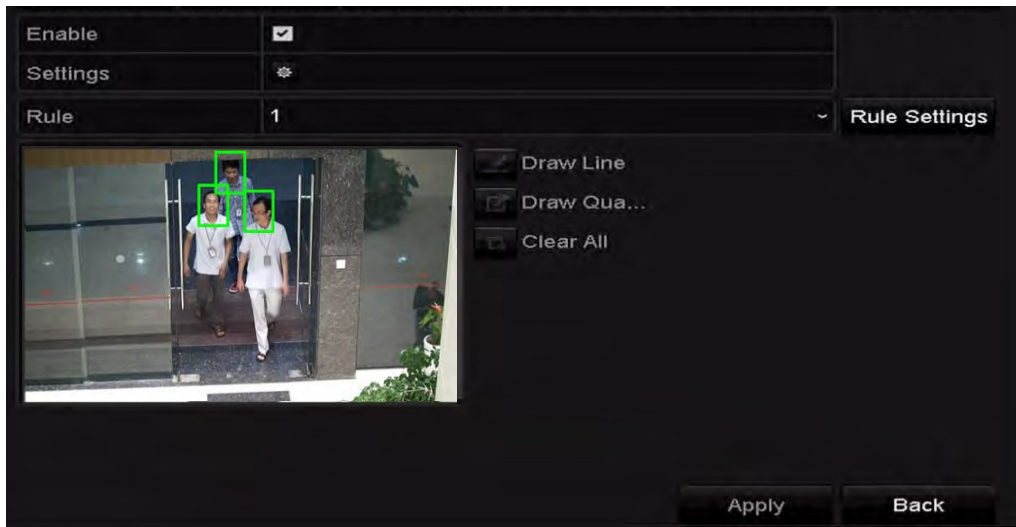


Figure 153, Face Detection


3. Set the **VCA** detection type to **Face Detection**.
4. Check the **Enable** checkbox to enable this function.
5. Click  to enter the **face detection** settings interface. Configure the trigger channel, arming schedule, and linkage action for the **face detection** alarm. Refer to steps 3–5 of *Setting Motion Detection Alarm* for detailed instructions.
6. Click the **Rule Settings** button to set the **face detection** rules. You can click-and-drag the slider to set the detection sensitivity.
  - **Sensitivity:** Range [1–5]. The higher the value, the more easily the face can be detected.



Figure 154, Set Face Detection Sensitivity

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

## 9.2 Line Crossing Detection

### Purpose

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

1. Enter the **VCA** settings interface, **Menu > Camera > VCA**.
2. Select the camera for which to configure the **VCA**.
3. (Optional) Click the **Save VCA Picture** checkbox to save the captured **VCA** detection pictures.




4. Set the **VCA** detection type to **Line Crossing Detection**.
5. Check the **Enable** checkbox to enable this function.
6. Click  to configure the trigger channel, arming schedule, and linkage actions for the **line crossing detection** alarm.
7. Click the **Rule Settings** button to set the **line crossing detection** rules.
  - 1) Set the direction to **A<->B**, **A->B**, or **A<-B**.
    - **A<->B**: Only the arrow on the B side shows; an object going across the configured line in either direction will be detected and trigger an alarm.
    - **A->B**: Only an object crossing the configured line from the A side to the B side will be detected.
    - **B->A**: Only an object crossing the configured line from the B side to the A side will be detected.
  - 2) Click-and-drag the slider to set the detection sensitivity.
    - **Sensitivity**: Range [1–100]. The higher the value, the more easily the detection alarm can be triggered.
  - 3) Click **OK** to save the rule settings and go back to the **line crossing detection** settings interface.



Figure 155, Set **Line Crossing Detection** Rules

8. Click  and set two points in the preview window to draw a virtual line.
9. (Optional) Use the  to clear the existing virtual line and re-draw it.

**NOTE:** Up to four rules can be configured.



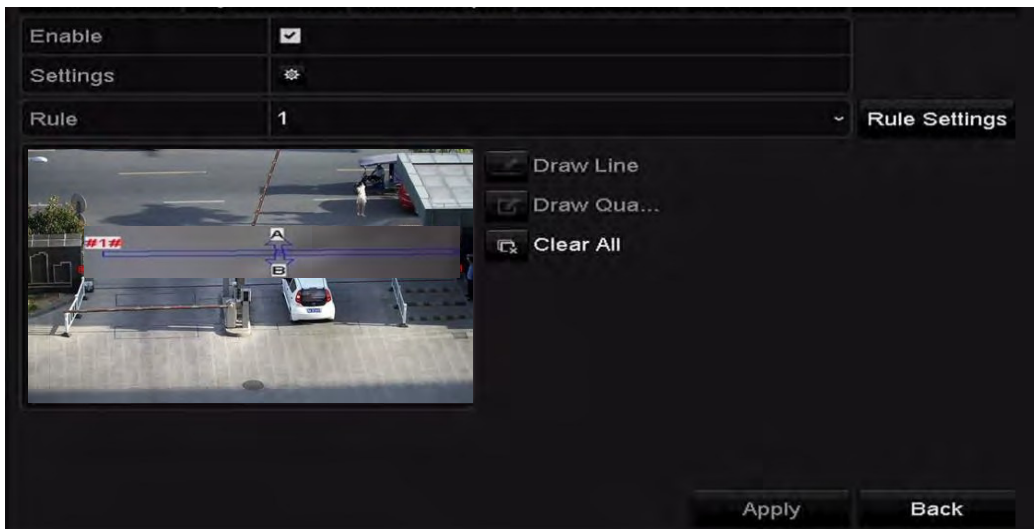



Figure 156, Draw Line for [Line Crossing Detection](#)

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

## 9.3 Intrusion Detection

### Purpose

[Intrusion detection](#) detects people, vehicles, or other objects that enter and loiter in a pre-defined virtual region, and certain actions can be taken when the alarm is triggered.


1. Enter the [VCA](#) settings interface, **Menu > Camera > VCA**.
2. Select the camera for which to configure the [VCA](#).
3. (Optional) Click the **Save VCA Picture** checkbox to save the captured [VCA](#) detection pictures.
4. Set the [VCA](#) detection type to [Intrusion Detection](#).
5. Check the **Enable** checkbox to enable this function.
6. Click  to configure the trigger channel, arming schedule and linkage actions for the [line crossing detection](#) alarm.
7. 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 that will trigger the alarm. The higher the value, the more easily the detection alarm can be triggered.
    - **Percentage:** Range [1–100]. Percentage defines the ratio of the in-region part of the object that will 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 157, Set Intrusion Crossing Detection Rules

3) Click **OK** to save the rule settings and go back to the [line crossing detection](#) settings interface.

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

9. (Optional) You can use  to clear the existing virtual line and re-draw it.

**NOTE:** Up to four rules can be configured.

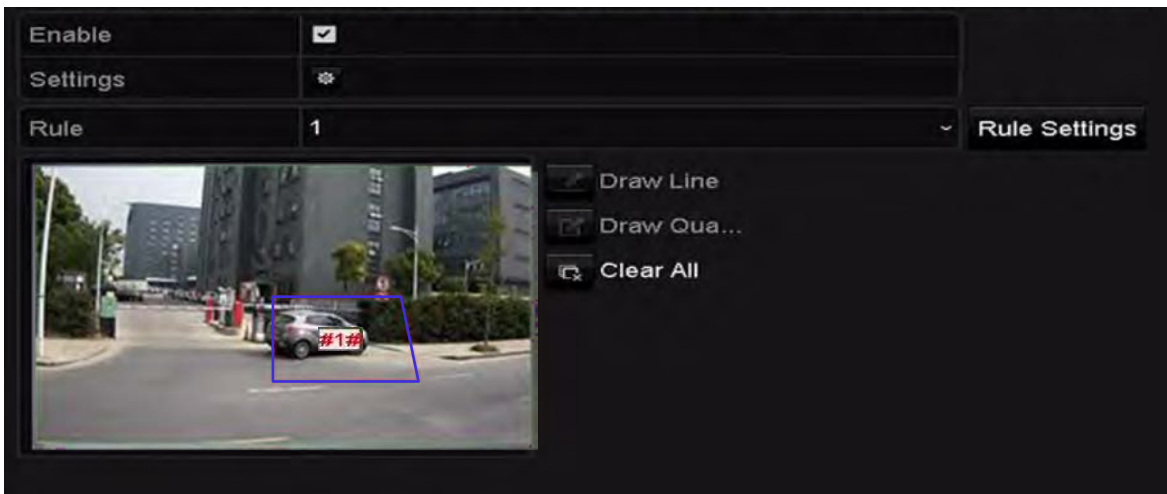


Figure 158, Draw Area for [Intrusion Detection](#)




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

## 9.4 Region Entrance Detection

### Purpose

[Region entrance detection](#) function detects people, vehicles, or other objects that enter a pre-defined virtual region from an outside area, and certain actions can be taken when the alarm is triggered.

1. Enter the [VCA](#) settings interface, **Menu > Camera > VCA**.
2. Select the camera for which to configure the [VCA](#).

3. (Optional) Click the **Save VCA Picture** checkbox to save the captured **VCA** detection pictures.
4. Set the **VCA** detection type to **Region Entrance Detection**.
5. Check the **Enable** checkbox to enable this function.
6. Click  to configure the trigger channel, arming schedule, and linkage actions for the **line crossing detection** alarm.
7. Click the **Rule Settings** button to set the sensitivity of the **region entrance detection**.
  - **Sensitivity:** Range [0–100]. The higher the value, the more easily the detection alarm can be triggered.
8. 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.
9. (Optional) Use  to clear the existing virtual line and re-draw it.

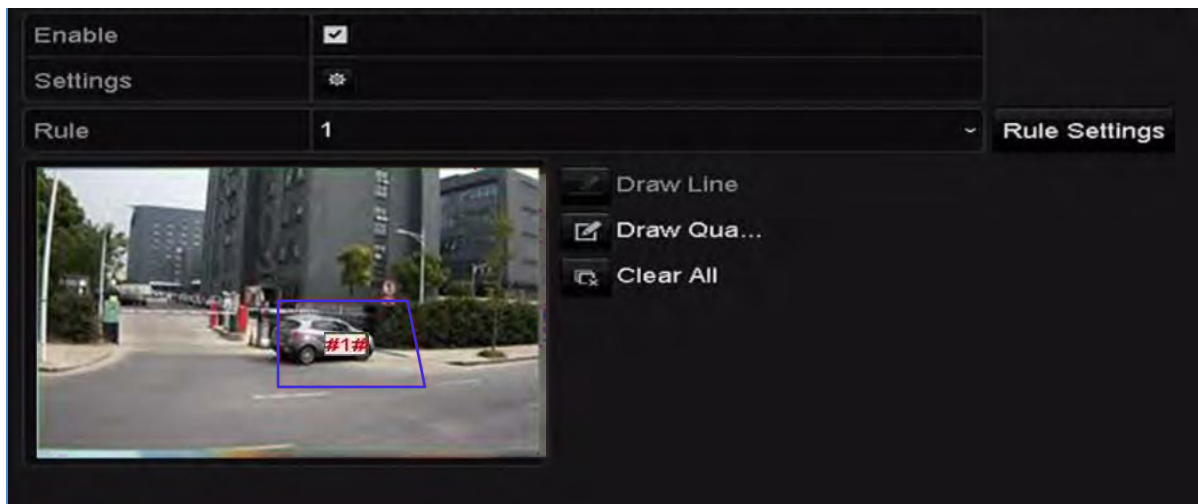


Figure 159, Set **Region Entrance Detection**

**NOTE:** Up to four rules can be configured.

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

## 9.5 Region Exiting Detection

### Purpose

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

**NOTE:** Refer to **Region Entrance Detection** for operating steps to configure **region exiting detection**.

Up to four rules can be configured.

## 9.6 Unattended Baggage Detection

### Purpose

[Unattended Baggage Detection](#) detects objects such as baggage, purses, dangerous materials, etc. left in a pre-defined region, and a series of actions can be taken when an alarm is triggered.

**NOTE:** Refer to [Intrusion Detection](#) for operating steps to configure [unattended baggage detection](#).

The **Threshold** [5s–20s] in the Rule Settings defines the time the objects are left in the region. If you set the value as 10, an alarm is triggered after the object is left and stays in the region for 10s. **Sensitivity** defines the similarity of the object with the background. When the sensitivity is high, a very small object left in the region can trigger the alarm.

Up to four rules can be configured.

## 9.7 Object Removal Detection

### Purpose

[Object Removal Detection](#) detects objects removed from a pre-defined region such as exhibits on display, and a series of actions can be taken when the alarm is triggered.

**NOTE:** Refer to [Intrusion Detection](#) for operating steps to configure [object removal detection](#).

The **Threshold** [5s–20s] in Rule Settings defines the time of the objects removed from the region. If you set the value as 10, an alarm is triggered after the object disappears from the region for 10s. **Sensitivity** defines the similarity of the object with the background. When the sensitivity is high, a very small object taken from the region can trigger the alarm.

Up to four rules can be configured.

## 9.8 Audio Exception Detection

### Purpose

[Audio Exception Detection](#) detects abnormal sounds in the surveillance scene such as a sudden increase/decrease in sound intensity, and certain actions can be taken when the alarm is triggered.


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



Figure 160, Set [Audio Exception Detection](#) Rules

- 1) Check the **Audio Input Exception** checkbox to enable the audio loss detection function.
  - 2) Check the **Sudden Increase of Sound Intensity Detection** checkbox to detect a steep rise in sound in the surveillance scene. You can set the detection sensitivity and threshold.
    - **Sensitivity:** Range [1–100], the smaller the value, the more severe the change must 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. Adjust it according to the real environment.
  - 3) Check the **Sudden Decrease of Sound Intensity Detection** checkbox to detect a steep drop in sound in the surveillance scene. You can set the detection sensitivity [1–100].
7. Click **Apply** to activate the settings.

## 9.9 Sudden Scene Change Detection

### Purpose

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

**NOTE:** Refer to [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, the more easily the change of scene can trigger the alarm.

## 9.10 Defocus Detection

### Purpose

Image blur caused by lens [defocus](#) can be detected, and certain actions can be taken when the alarm is triggered.


**NOTE:** Refer to the [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, the more easily the [defocus](#) image can trigger the alarm.

## 9.11 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.

1. Enter the [VCA](#) settings interface, **Menu > Camera > VCA**.
2. Select the camera for which to configure the [VCA](#).
3. (Optional) Click the **Save VCA Picture** checkbox to save the captured [VCA](#) detection pictures.
4. Set the [VCA](#) detection type to **PIR Alarm**.
5. Click  to configure the trigger channel, arming schedule, and linkage action for the [PIR alarm](#).
6. Click the **Rule Settings** button to set the rules. Refer to [Face Detection](#) for instructions.
7. Click **Apply** to activate the settings.

## Chapter 10 VCA Search

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

### 10.1 Face Search

#### Purpose

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

#### Before You Start

Refer to [Face Detection](#) for configuring [face detection](#).

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



Figure 161, Face Search

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



Figure 162, 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.



7. (Optional) Click **Export** to export all face pictures to the storage device.

**NOTE:** Refer to *Backup* for operation of exporting files.



Figure 163, Export Files

## 10.2 Behavior Search

### Purpose

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

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

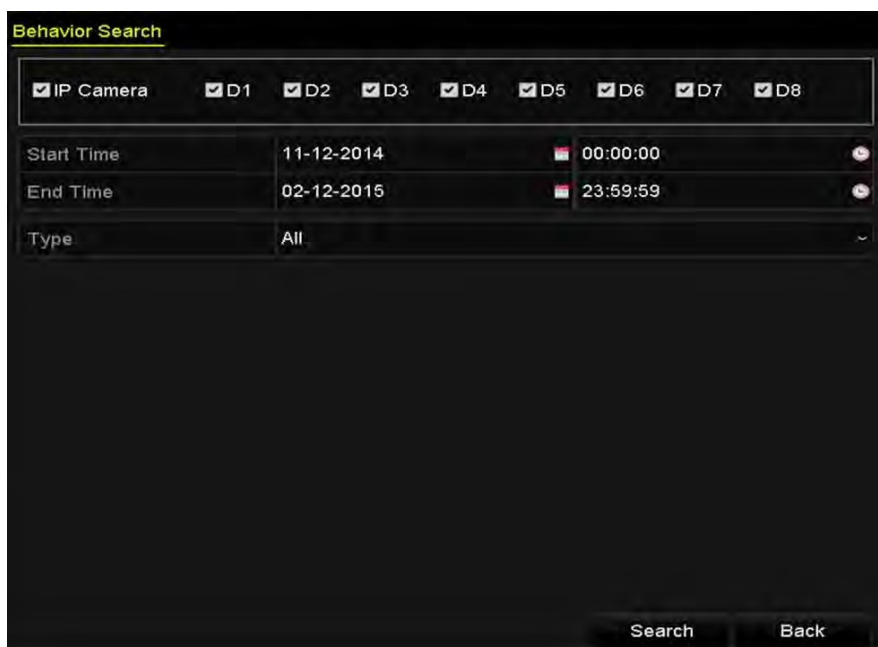






Figure 164, Behavior Search Interface

4. Select the **VCA** detection type from the drop-down 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 are displayed in list or in chart form.



Figure 165, [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 a local storage device, connect the storage device to the device, and click **Export All** to enter the Export interface.
8. (Optional) Click **Export** to export all pictures to the storage device.

## Chapter 11 Network Settings

### 11.1 Configuring General Settings

#### Purpose

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

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

NIC Type	10M/100M/1000M Self-adaptive		
Enable DHCP	<input type="checkbox"/>		
IPv4 Address...	10 .15 .1 .76	IPv6 Address...	fe80::240:5eff:fef6:3c92/64
IPv4 Subn...	255 .255 .255 .0	IPv6 Address...	
IPv4 Defa...	10 .15 .1 .254	IPv6 Defa...	
MAC Address	00:40:5e:f6:3c:92		
MTU(Bytes)	1500		
Enable Obtain DNS Serv...	<input type="checkbox"/>		
Preferred DNS Server	10.1.7.88		
Alternate DNS Server	10.1.7.77		
Internal NIC IPv4 Address	192 .168 .254 .1		
<input type="button" value="Apply"/> <input type="button" value="Back"/>			

Figure 166, Network Settings Interface

- In the **General Settings** interface, you can configure Working Mode, NIC Type, IPv4 Address, IPv4 Gateway, MTU, DNS, DHCP, and DNS Server.

**NOTE:** The valid value range of MTU is 500–9676.

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

**NOTE:** For DS-7600NI-Q1/P and DS-7600NI-Q2/P Series NVRs, you need to configure the internal NIC address, so that IP addresses are assigned to the cameras connected to the PoE interfaces.

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

### Working Mode

Two 10M/100M/1000M NIC cards are provided, and they allow the device to work in 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 for the system 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 set the Main NIC to LAN1 or LAN2. In this way, in case of one NIC card failure, the device will automatically enable the other standby NIC card so as to ensure normal running of the system.

## 11.2 Configuring Advanced Settings

### 11.2.1 Configuring Hik-Connect

## Purpose

Hik-Connect is a mobile phone application and service platform page ([www.hik-connect.com](http://www.hik-connect.com)) to access and manage your connected DVR. It offers convenient remote access to the surveillance system.

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

1. Go to **Menu > Configuration > Network > Platform Access.**

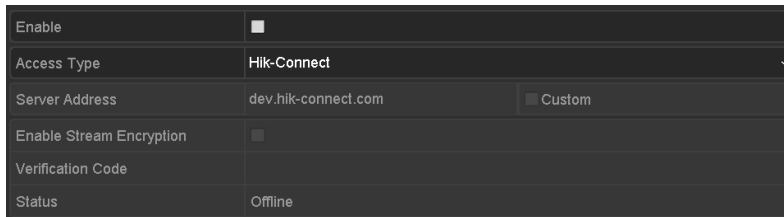


Figure 167, Hik-Connect Settings

2. Check the **Enable** checkbox to activate the function. The **Service Terms** interface pops up.



Figure 168, Service Terms

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

**NOTE:** Hik-Connect is disabled by default.

The verification code is empty when the device leaves the 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.

3. (Optional) Check the **Custom** checkbox and input the **Server Address**.
4. (Optional) Check the **Enable Stream Encryption** checkbox.

After this feature is enabled, the verification code is required for remote access and live view.

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

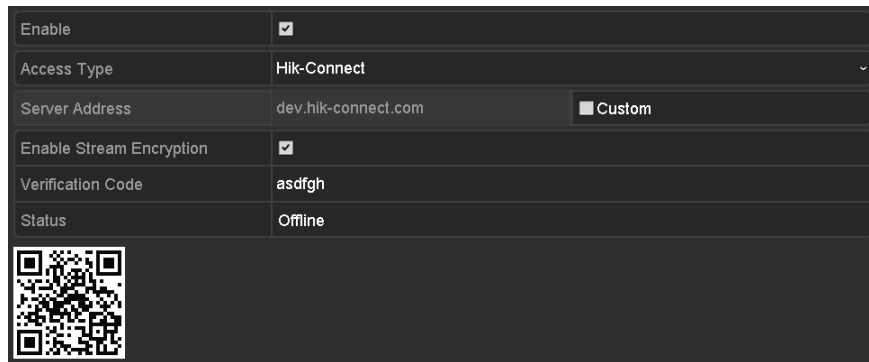


Figure 169, Hik-Connect Settings Interface

5. Click **Apply** to save the settings.
  6. After configuration, you can access and manage the DVR by your mobile phone or by the Website ([www.hik-connect.com](http://www.hik-connect.com)).
- For iOS users, scan the QR code below to download the Hik-Connect application for subsequent operations.



Figure 170, QR Code for iOS Users

- For Android users, scan the QR code below to download the Hik-Connect application for subsequent operations. You must install *googleplay* on your Android mobile phone to skip to the address successfully.



Figure 171, QR Code for Android Users

**NOTE:** 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) for network access.

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

1. Enter the Network Settings interface, **Menu > Configuration > Network**.
2. Select the **DDNS** tab to enter the DDNS Settings interface.
3. Check the **DDNS** checkbox to enable this feature.
4. Select **DDNS Type**. Three 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 **Device Domain Name** text field, enter the domain obtained from the DynDNS Website.
    - 3) Enter the **User Name** and **Password** registered in the DynDNS Website.

Enable DDNS	<input checked="" type="checkbox"/>
DDNS Type	DynDNS
Area/Country	Custom
Server Address	members.dyndns.org
Device Domain Name	123.dyndns.com
Status	DDNS is disabled.
User Name	test
Password	*****

Figure 172, DynDNS Settings Interface

- **PeanutHull**

- 1) 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	123_gcip.net
Password	*****

Figure 173, PeanutHull Settings Interface

- **NO-IP**

- 1) Enter the account information in the corresponding fields. Refer to the DynDNS settings.
- 2) Enter **Server Address** for NO-IP.
- 3) In the **Device Domain Name** text field, enter the domain obtained from the NO-IP Website (www.no-ip.com).
- 4) 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	no-ip.org
Device Domain Name	123.no-ip.org
Status	DDNS is disabled.
User Name	test
Password	*****

Figure 174, NO-IP Settings Interface

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

### 11.2.3 Configuring PPPoE

#### Purpose

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

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

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

Figure 175, PPPoE Settings Interface

3. Check the **PPPoE** checkbox to enable this feature.



4. Enter **User Name**, and **Password** for PPPoE access.

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

5. Click the **Apply** button to save and exit the interface.
6. After successful settings, the system asks you to reboot the device to enable the new settings, and the PPPoE dial-up is automatically connected after reboot.
7. (Optional) Go to **Menu > Maintenance > System Info > Network** interface to view the status of PPPoE connection.

## 11.2.4 Configuring NTP Server

### Purpose

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

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

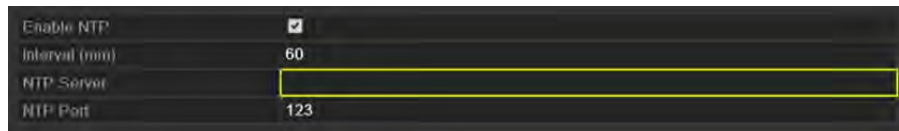


Figure 176, NTP Settings Interface

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

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

## 11.2.5 Configuring SNMP

### Purpose

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

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

2. Select the **SNMP** tab to enter the **SNMP** Settings interface.

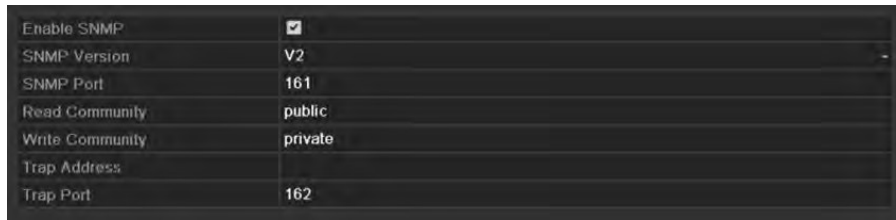


Figure 177, **SNMP** Settings Interface

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 operation.

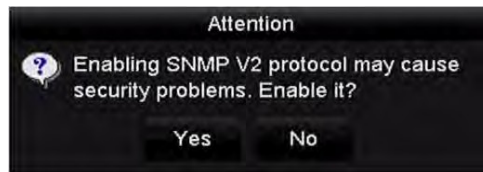


Figure 178, **SNMP** Settings Interface

5. If you choose the **Yes** option in step 4, 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.

**NOTE:** Before setting the **SNMP**, 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.

## 11.2.6 Configuring More Settings

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



Figure 179, More Settings Interface

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

The **Alarm Host IP** refers to the IP address of the remote PC on which the **CMS (Client Management System)** software (e.g., 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 the 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 **RTSP Port** text field. The default RTSP port is 554, and you can change it according to 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 requirements.

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



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 180, Configure More Settings

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

## 11.2.7 Configuring HTTPS Port

### Purpose

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

### Example:

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

**NOTE:** The HTTPS port can be configured only through the Web browser.

1. Open the 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 the **Login** button to log in to the device.

3. Enter the HTTPS settings interface, **Configuration > Network > Advanced Settings > HTTPS**.
4. Create the self-signed certificate or authorized certificate.

Figure 181, HTTPS Settings

- **OPTION 1:** Create the self-signed certificate
  - 1) Click the **Create** button to create the following dialog box.

Figure 182, 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.

- **OPTION 3:** Install the available certificate
  - 1) Click **Browse** to locate the certificate file from your local directory.
  - 2) Click **Install** to install the certificate.

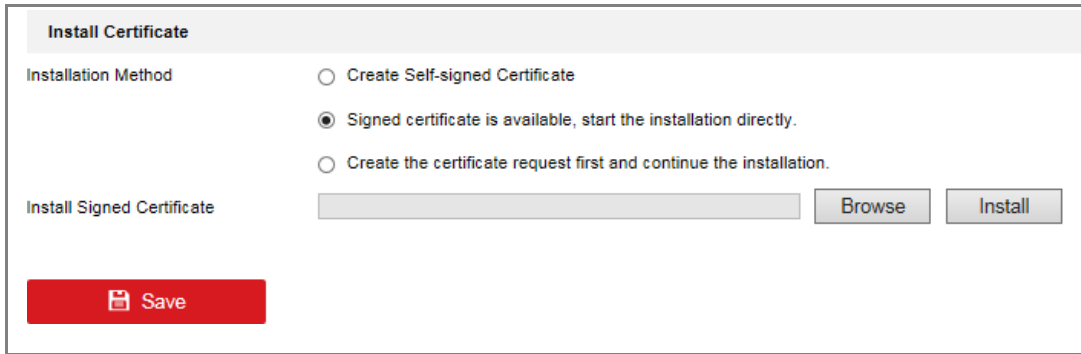


Figure 183, Install Available Certificate

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

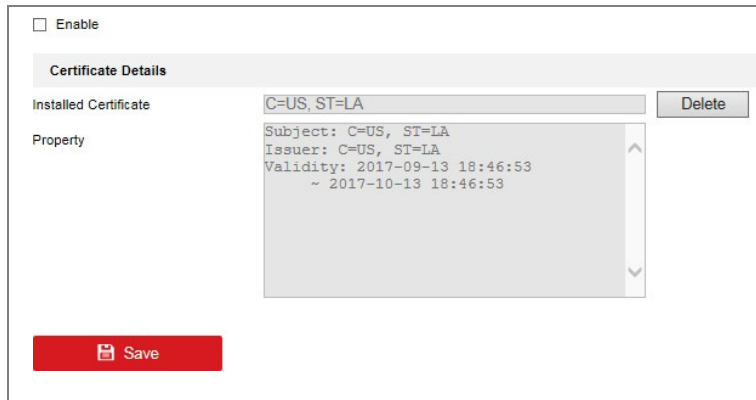


Figure 184, Installed Certificate Property

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

## 11.2.8 Configuring E-Mail

### Purpose

The system can be configured to send an e-mail 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 e-mail 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.

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

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 Subn...	255 .255 .255 .0	IPv6 Address...	
IPv4 Defa...	10 .16 .1 .254	IPv6 Defa...	
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 185, Network Settings Interface

3. Click **Apply** to save the settings.
4. Select the **E-mail** tab to enter the **E-mail Settings** interface.

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

Figure 186, E-Mail Settings Interface

5. Configure the following e-mail settings:
  - **Enable Server Authentication** (optional): Check the checkbox to enable the server authentication feature
  - **User Name:** The user name of sender's account registered on the SMTP server
  - **Password:** The password of sender's account registered on the SMTP server
  - **SMTP Server:** The SMTP Server IP address or host name (e.g., smtp.263xmail.com)
  - **SMTP Port:** The SMTP port, the default TCP/IP port used for SMTP is 25
  - **Enable SSL/TLS** (optional): Click the checkbox to enable SSL/TLS if required by the SMTP server.
  - **Sender:** The name of sender
  - **Sender's Address:** The e-mail address of sender
  - **Select Receivers:** Select the receiver; up to three receivers can be configured

- **Receiver:** The name of user to be notified
  - **Receiver's Address:** The e-mail address of user to be notified
  - **Enable Attached Picture:** Check the **Enable Attached Picture** checkbox if you want to send e-mail 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.
6. Click the **Apply** button to save the e-mail settings.
  7. You can click the **Test** button to test whether your e-mail settings work.

## 11.2.9 Configuring NAT

### Purpose

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

- **UPnP™**

Universal Plug and Play (UPnP™) can permit the device seamlessly to 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 fast connection of the device to the WAN via a router without port mapping.

### Before You Start

If you want to enable the device's UPnP™ function, 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.

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



Figure 187, UPnP™ Settings Interface

3. Check the  checkbox to enable UPnP™.
4. Set the Mapping Type as **Manual** or **Auto** in the drop-down list.
  - **OPTION 1: Auto**


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


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



Figure 188, UPnP™ Settings Finished-Auto

- **OPTION 2: Manual**

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

- 1) Select **Manual** in the drop-down Mapping Type list.
- 2) Click  to activate the External Port Settings dialog box. Configure the external port no. for server port, http port, RTSP port, and https port respectively.

**NOTE:** You can use the default port no., or change it according to actual requirements.

External Port indicates the port no. for port mapping in the router.

The value of the RTSP port no. should be 554 or between 1024 and 65535, while the value of the other ports should be between 1 and 65535 and the values 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 189, External Port Settings Dialog Box

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



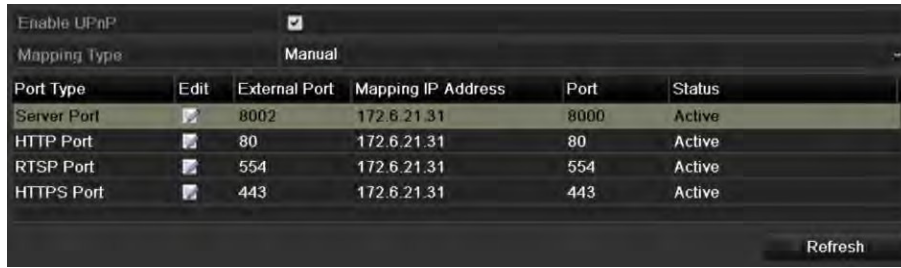


Figure 190, UPNP™ Settings Finished-Manual

- Enter the virtual server setting page of router; fill in the blank of Internal Source Port with the internal port value, the blank of External Source Port with the external port value, and other required contents.

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

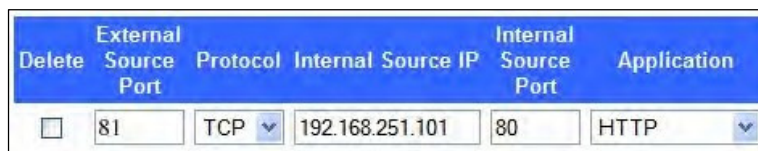


Figure 191, Setting Virtual Server Item

**NOTE:** The above virtual server setting interface is for reference only, it may be different due to different router manufacturers. Contact your router manufacturer if you have any problems with setting the virtual server.

## 11.2.10 Configuring Virtual Host

### Purpose

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

**NOTE:** The Virtual host function can be configured only through the Web browser.

- Enter the Advanced settings interface, **Configuration > Network > Advanced Settings > Other**.

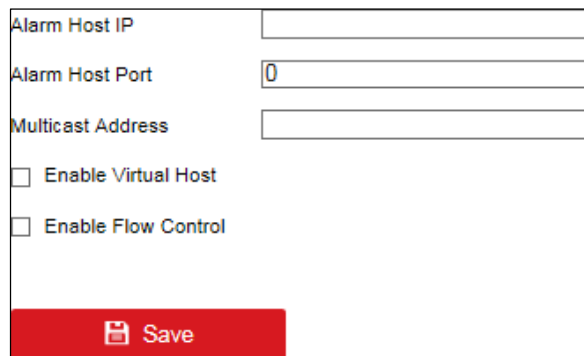


Figure 192, Advanced Settings Interface

- Check the of **Enable Virtual Host** checkbox.
- Click the **Save** button to save the setting.

3. Enter the NVR's IP camera management interface. The Connect column appears on the right-most side of the camera list.

## 11.3 Checking Network Traffic

### Purpose

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

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



Figure 193, Network Traffic Interface

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

1. Enter the Network Traffic interface, **Menu > Maintenance > Net Detect**.
2. Click the **Network Detection** tab to enter the Network Detection menu.

The screenshot shows the 'Network Delay, Packet Loss Test' configuration window. It includes the following fields and buttons:

- Select NIC:** A dropdown menu currently set to 'LAN1'.
- Destination Address:** A text field containing '172.6.23.6'.
- Test:** A button to initiate the network delay and packet loss test.
- Network Packet Export:** A section with a dropdown menu for 'Device Name' set to 'LAN1'.
- Device Name:** A text field showing '172.6.21.64'.
- 2,789Kbps:** A value displayed next to the device name.
- Refresh:** A button to refresh the data.
- Export:** A button to export the data.

Figure 194, Network Detection Interface

3. Enter the destination address in the **Destination Address** text field.
4. Click the **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.

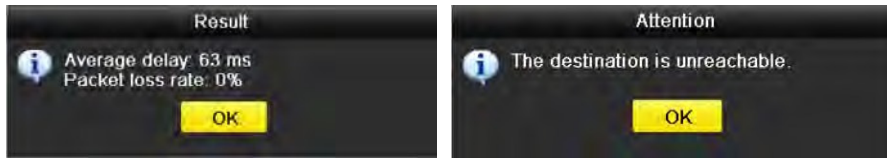


Figure 195, Testing Result of Network Delay and Packet Loss

## 11.4.2 Exporting Network Packet

### Purpose

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

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 Device Names drop-down list.

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

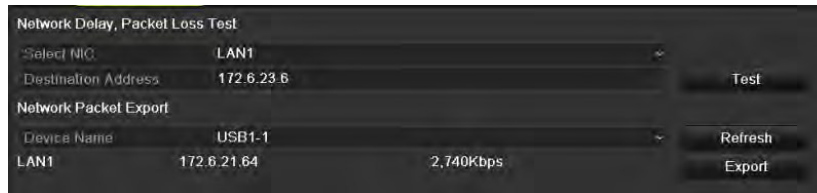


Figure 196, Export Network Packet

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

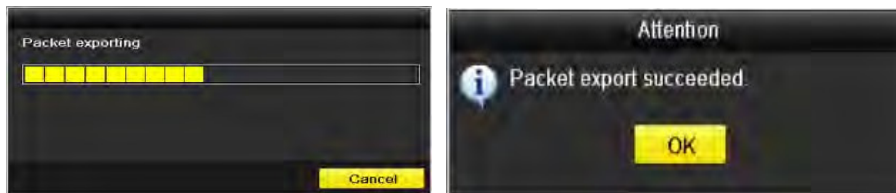


Figure 197, Packet Export Attention

**NOTE:** Up to 1 MB of 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.

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

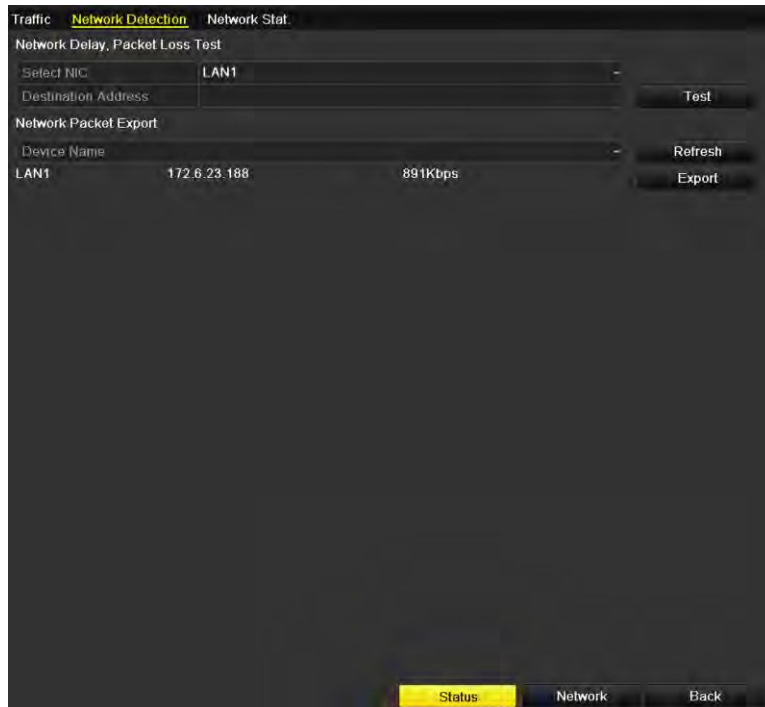


Figure 198, Network Status Checking

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

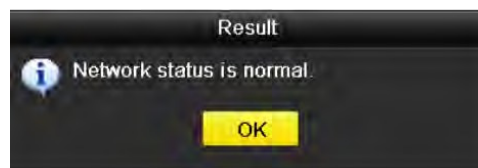


Figure 199, Network Status Checking Result

If the message box pops out with other information instead of this one, you can click the **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 real-time information of the NVR.

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

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

Refresh

Figure 200, 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.

**NOTE:** A message box pops up when the NVR starts up if there exists any uninitialized HDDs.



Figure 201, Message Box of Uninitialized HDD

1. Click **Yes** button to initialize it immediately or perform the following steps to initialize the HDD.
2. Enter the HDD Information interface, **Menu > HDD > General**.

HDD Information									
<input type="checkbox"/>	L...	Capacity	Status	Property	Type	Free Space	Gr.	Edit	D..
<input type="checkbox"/>	5	931.51GB	Normal	R/W	Local	846GB	1		-

Figure 202, HDD Information Interface

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



Figure 203, Confirm Initialization

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

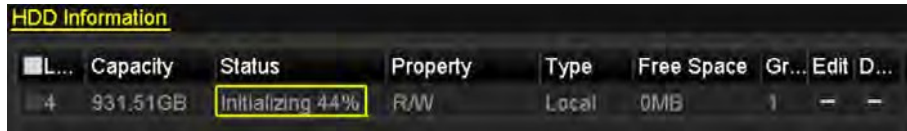


Figure 204, Status changes to Initializing

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

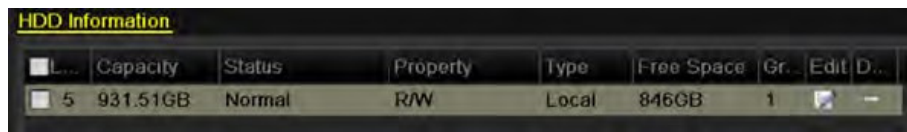


Figure 205, HDD Status Changes to Normal

**NOTE:** Initializing the HDD will erase all data on it.

## 12.2 Managing Network HDD

### Purpose

You can add an allocated NAS or IP SAN disk to the NVR and use it as a network HDD. Up to eight network disks can be added.

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

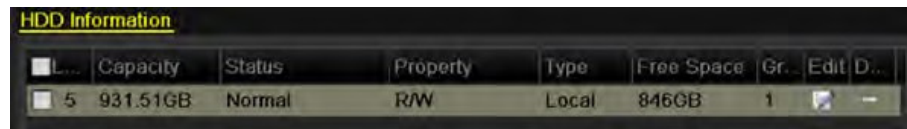


Figure 206, HDD Information Interface

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



Figure 207, HDD Information Interface

3. Add the allocated NetHDD.
4. Set 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 for available NAS disks.
- 3) Select the NAS disk from the list shown, or manually enter the directory in the NetHDD Directory text field.
- 4) Click the **OK** button to add the configured NAS disk.



Figure 208, Add NAS Disk

- **Add IP SAN**

- 1) Enter the NetHDD IP address in the text field.

- 2) Click the **Search** button to search for available IP SAN disks.
- 3) Select the IP SAN disk from the list shown.
- 4) Click the **OK** button to add the selected IP SAN disk.

**NOTE:** Up to 1 IP SAN disk can be added.



Figure 209, 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.

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

Label	Capacity	Status	Property	Type	Free Space	Gro...	Edit	Del.
3	931.51GB	Normal	R/W	Local	890GB	1	[Edit]	[-]
4	931.51GB	Normal	R/W	Local	867GB	1	[Edit]	[-]
17	79,968MB	Normal	R/W	NAS	79,872MB	1	[Edit]	[Init]

Figure 210, Initialize Added NetHDD

## 12.3 Managing HDD Groups

### 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.

1. Enter the Storage Mode interface, **Menu > HDD > Advanced > Storage Mode**.
2. Set the **Mode** to Group.



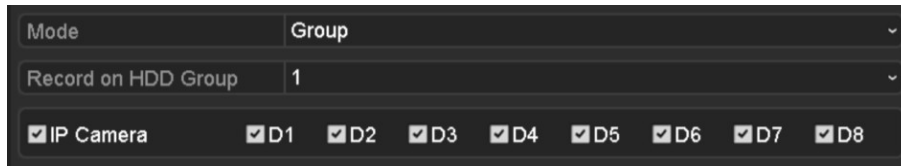


Figure 211, Storage Mode Interface

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



Figure 212, Attention for Reboot


4. Click the **Yes** button to reboot the device to activate the changes.
5. After rebooting device, enter the HDD Information interface, **Menu > HDD > General**.
6. Select HDD from the list and click the  icon to enter the Local HDD Settings interface.



Figure 213, Local HDD Settings Interface

7. Select the Group number for the current HDD.

**NOTE:** The default group no. for each HDD is 1.

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

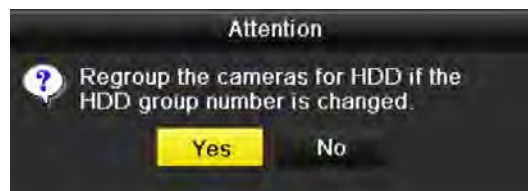


Figure 214, Confirm HDD Group Settings

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, set the storage mode to Group (refer to steps 1–4 of Chapter Setting HDD Groups ).

An 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.


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.



Figure 215, Set HDD Property

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

**NOTE:** At least two hard disks must be installed on your NVR when you want to set an HDD to Redundancy, with 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 or captured pictures.

1. Enter the Storage Mode interface, **Menu > HDD > Advanced**.
2. Set the **Mode** to Quota.

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



Figure 216, Storage Mode Settings Interface

3. Select a camera for which you want to configure quota.
4. Enter the storage capacity in the **Max. Record Capacity (GB)** and **Max. Picture Capacity (GB)** text fields.



Figure 217, Configure Record/Picture Quota

5. You can copy the quota settings of the current camera to other cameras if required. Click the **Copy** button to enter the Copy Camera menu.



Figure 218, Copy Settings to Other Camera(s)

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

**NOTE:** If the quota capacity is set to 0, then all cameras will use the total capacity of the HDD for record and picture capture.

## 12.5 Configuring Disk Clone

### Purpose

If the S.M.A.R.T. detection result declares the HDD is abnormal, you can choose to clone all the data on the HDD to an inserted eSATA disk manually. Refer to *HDD Detection* for details of S.M.A.R.T. detection.

### Before You Start

An eSATA disk should be connected to the device.

1. Enter the HDD Advanced Setting interface, **Menu > HDD > Advanced**.
2. Click the **Disk Clone** tab to enter the disk clone configuring interface.

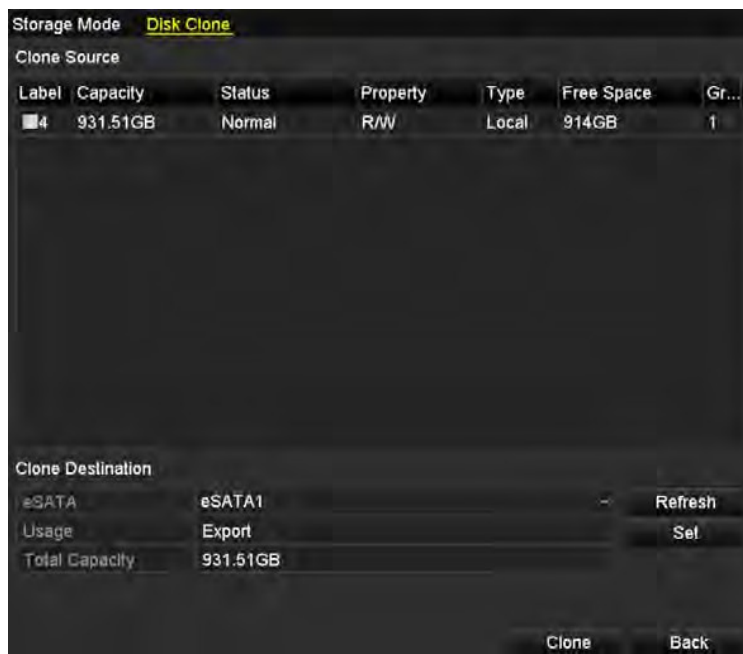


Figure 219, Disk Clone Configuration Interface

3. Make sure the usage of the eSATA disk is set to Export. If not, click the **Set** button to set it. Choose Export and click the **OK** button.



Figure 220, Setting eSATA Usage

**NOTE:** The capacity of destination disk must be the same as that of the clone source disk.

4. Check the HDD checkbox to be cloned in the Clone Source list.

5. Click the **Clone** button and a message box pops up.

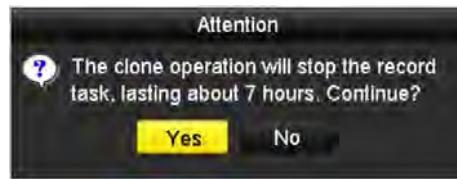


Figure 221, Message Box for Disk Clone

6. Click the **Yes** button to continue.

You can check the clone progress in the HDD status.

Label	Capacity	Status	Property	Type	Free Space	Gr...
4	931.51GB	Cloning 01%	R/W	Local	0MB	1

Figure 222, Check Disk Clone Progress

## 12.6 Checking HDD Status

### Purpose

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

### Checking HDD Status in HDD Information Interface

1. Enter the HDD Information interface, **Menu > HDD > General**.
2. Check the status of each HDD, which are displayed on the list.

Label	Capacity	Status	Property	Type	Free Space	Gr...	Edit	Def...
4	931.51GB	Normal	R/W	Local	921GB	1		
18	10,048MB	Uninitialized	R/W	NAS	0MB	1		
25	931.51GB	Normal	R/W	eSATA	894GB	1		

Total Capacity: 1,872GB  
Free Space: 1,815GB

Figure 223, View HDD Status (1)

**NOTE:** If the status of HDD is *Normal* or *Sleeping*, it is working normally. If the status is *Uninitialized* or *Abnormal*, initialize the HDD before use. If the HDD initialization fails, replace it with a new one.

## Checking HDD Status in HDD Information Interface

3. Enter the System Information interface, **Menu > Maintenance > System Info**.
4. Click the **HDD** tab to view the status of each HDD displayed on the list.



The screenshot shows a web interface with a dark theme. At the top, there are navigation tabs: Device Info, Camera, Record, Alarm, Network, and HDD (which is highlighted). Below the tabs is a table with the following data:

Label	Status	Capacity	Free Space	Property	Type	Group
5	Normal	931GB	931GB	R/W	Local	1
6	Sleeping	931GB	931GB	Redundancy	Local	1
17	Normal	40,000MB	22,528MB	R/W	IP SAN	1

Below the table, there are summary statistics:

Total Capacity	1,902GB
Free Space	1,884GB

A yellow 'Back' button is located at the bottom right of the interface.

Figure 224, View HDD Status (2)

## 12.7 HDD Detection

### Purpose

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

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

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.

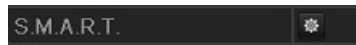


Figure 225, S.M.A.R.T. Settings Interface

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

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

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



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

### Bad Sector Detection

1. Click the **Bad Sector Detection** tab.
2. Select the HDD no. in the drop-down list you want to configure, and choose All Detection or Key Area Detection as the detection type.

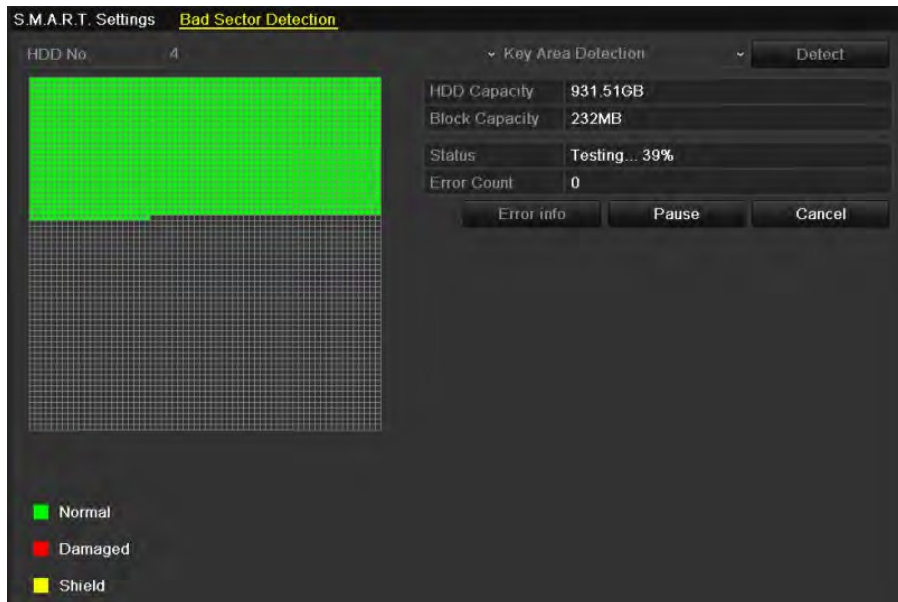


Figure 226, Click the Detect Button To Start the Detection.

You can click **Error info** button to see the detailed damage information. You can also pause/resume or cancel the detection.

## 12.8 Configuring HDD Error Alarms

### Purpose

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

1. Enter the Exception interface, **Menu > Configuration > Exceptions**.
2. Set the Exception Type to **HDD Error** from the drop-down list.
3. Click the checkbox(es) below to select the HDD error alarm type(s).

**NOTE:** The alarm type can be selected as: Audible Warning, Notify Surveillance Center, Send E-mail and Trigger Alarm Output. Refer to *Setting Alarm Response Actions*.



Figure 227, 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.

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 228, OSD Configuration Interface

6. 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.

1. Enter the Privacy Mask Settings interface, **Menu > Camera > Privacy Mask**.
2. Select the camera for which to set privacy mask.

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



Figure 229, Privacy Mask Settings Interface

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

**NOTE:** Up to four 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 230, 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.

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

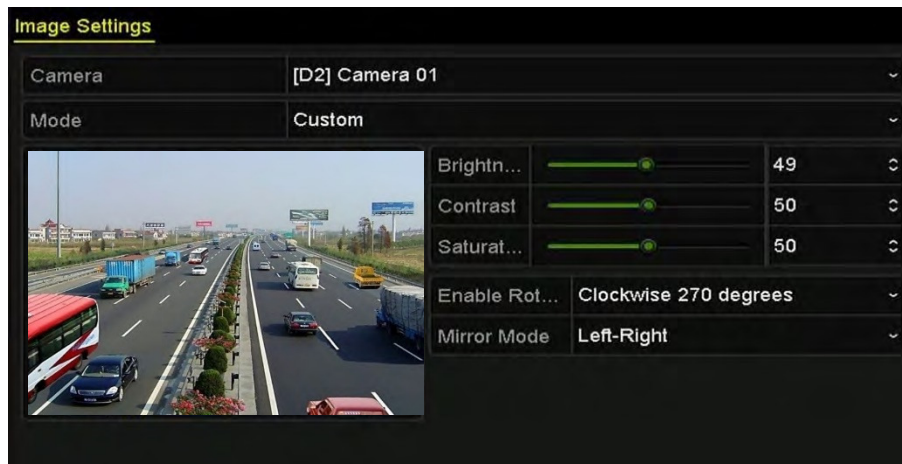


Figure 231, Image Settings Interface

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.

**NOTE:** The Rotate and Mirror functions must be supported by the connected IP camera.

The image parameters adjustment can affect both the live view and the recording quality.

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

## Chapter 14 NVR Management and Maintenance

### 14.1 Viewing System Information

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 232, Device Information Interface

**NOTE:** You can add the device to your mobile client software (iVMS-4500) by scanning the QR Code.

## 14.2 Searching and Exporting Log Files

### Purpose

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

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

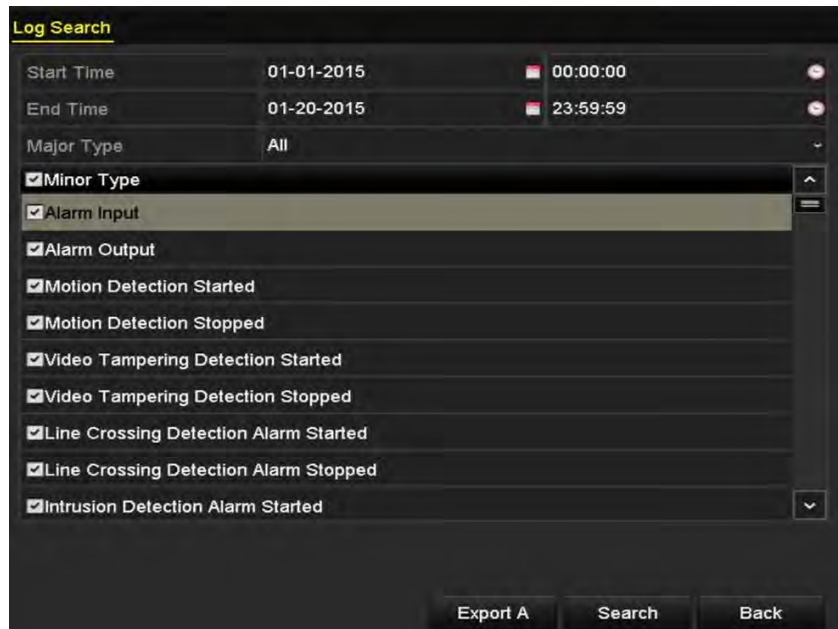


Figure 233, Log Search Interface

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.

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 234, Log Search Results

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

- You can click the button of each log or double click it to view its detailed information. You can also click the button to view the related video files if available.

Log Information	
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 235, Log Details

- If you want to export the log files, click the **Export** button to enter the Export menu. You can also click **Export All** on the Log Search interface to enter the Export interface, and all system logs will be exported to the backup device.



Figure 236, Export Log Files

7. Select the backup device from the **Device Name** drop-down list.
8. Select the format of the log files to be exported. Up to 15 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 a new folder in the backup device, or click the **Format** button to format the backup device before log export.

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

## 14.3 Importing/Exporting IP Camera Info

### Purpose

The added IP camera information can be generated into an Excel file and exported to the local device for backup, including the IP address, manage port, admin password, etc. 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.

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 File

### Purpose

The NVR configuration files can be exported to a 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.

### 14.4.1 Exporting Configuration File

## Before You Start

Insert a USB flash disk into the device. For importing the configuration file, the configuration file must be available on the USB flash disk.

1. Enter the Export Configuration File interface, **Menu > Maintenance > Export**.



Figure 237, Import/Export Config File

2. Select a USB flash disk.
3. Click **Export**.
4. Input the admin password.
5. Export configuration file to the selected local backup device.

## 14.4.2 Importing Configuration File

### Before You Start

Insert a USB flash disk with the configuration file into the device.

1. Enter the Export Configuration File interface, **Menu > Maintenance > Import**.
2. Select a USB flash disk.
3. Select the configuration file from the USB flash disk.
4. Click **Import**.
5. Input the admin password.
6. Import the configuration file to device.

**NOTE:** After finished importing the configuration files, the device will reboot automatically.



## 14.5 Upgrading System

### Purpose

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

### 14.5.1 Upgrading by Local Backup Device

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.

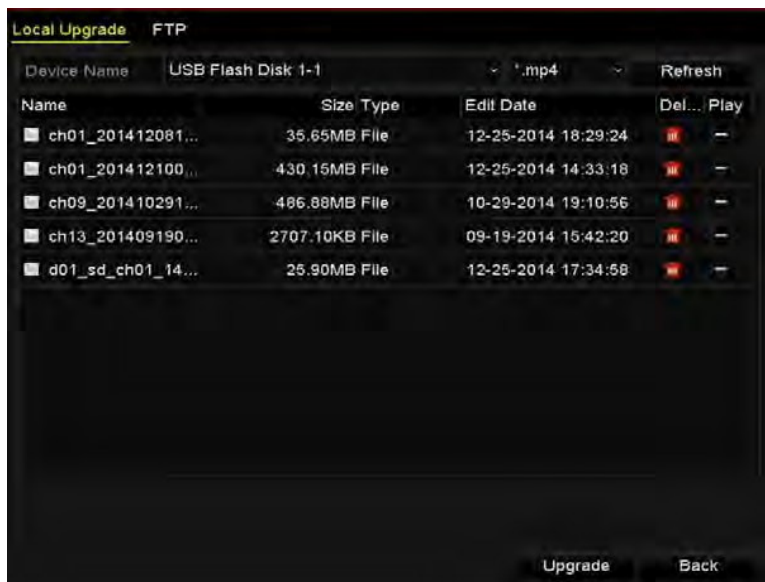


Figure 238, Local Upgrade Interface

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

#### Before You Start

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

1. Enter the Upgrade interface, **Menu > Maintenance > Upgrade**.
2. Click the **FTP** tab to enter the local upgrade interface.



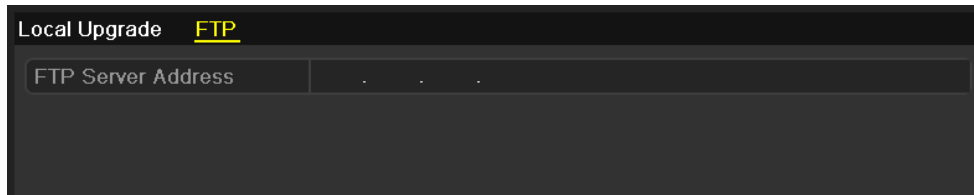


Figure 239, FTP Upgrade Interface

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

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

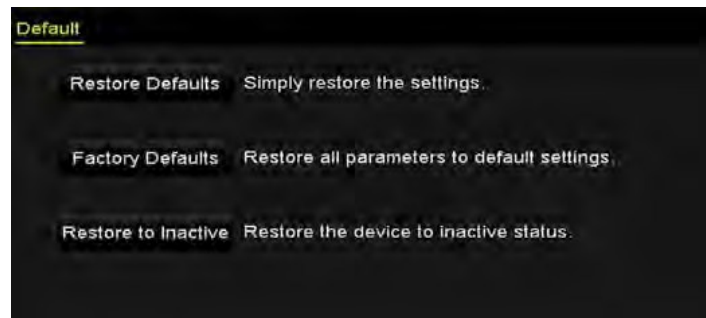


Figure 240, Restore Defaults

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

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

# Chapter 15 Others

## 15.1 Configuring General Settings

### Purpose

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

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



Figure 241, General Settings Interface

3. Configure the following settings:
  - **Language:** The default language used is *English*.
  - **Output Standard:** Select the output standard to NTSC or PAL, which must be the same as the video input standard.
  - **Resolution:** You can configure the VGA resolution and HDMI resolution respectively. Up to 4K (3840 × 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; four 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.

## 15.2 Configuring DST Settings

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



Figure 242, DST Settings Interface

You can check the checkbox before the Auto DST Adjustment item, or you can manually check the Enable DST checkbox, and then you choose the date of the DST period.

## 15.3 Configuring More Settings

1. Enter the General Settings interface, **Menu > Configuration > General**.
2. Click the **More Settings** tab to enter the More Settings interface.



Figure 243, More Settings Interface

3. Configure the following settings:
  - **Device Name:** Edit the NVR name.
  - **Device No.:** Edit the NVR serial number. 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.
  - **Enable HDMI/VGA Simultaneous Output** (for DS-9600NI and DS-8600NI only): By default, the video outputs from HDMI and VGA interfaces can be operated separately. You can set the simultaneous output for the HDMI and VGA by checking the checkbox of the option.
  - **Menu Output Mode:** You can choose the menu display on different video output.

You can set the menu output mode to **VGA**, **HDMI**, or **Auto**. When **Auto** is selected and both HDMI and VGA outputs are connected, the device will detect and set the HDMI as the menu output.

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

## 15.4 Managing User Accounts

### Purpose

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

### 15.4.1 Adding a User

- Enter the User Management interface, **Menu > Configuration > User**.

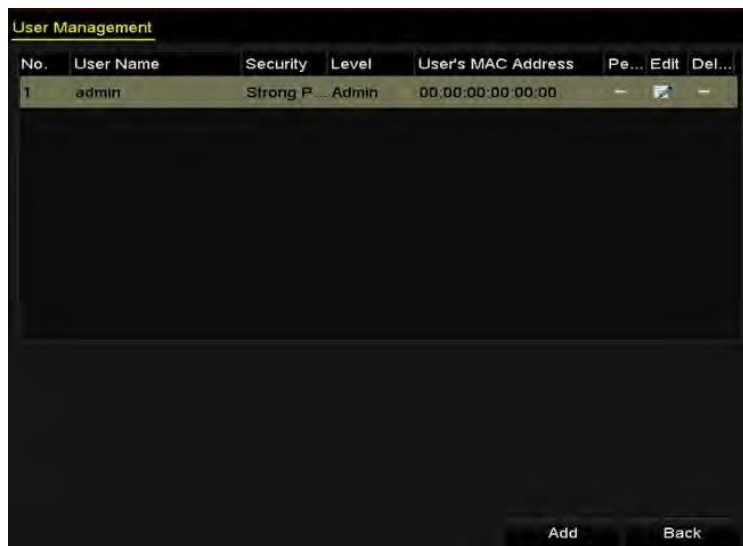
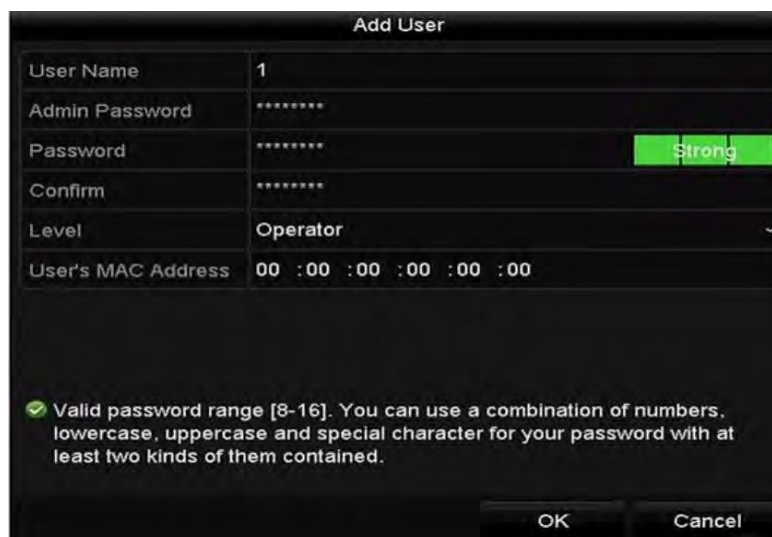


Figure 244, User Management Interface

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



User Name	1
Admin Password	*****
Password	***** <span style="background-color: green; color: white; padding: 2px;">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.

Figure 245, Add User Menu

- 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 that you create a strong password of your own choosing (using a minimum of eight 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. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

- **Level:** Set the user level to **Operator** or **Guest**. Different user levels have different operating permission.
    - **Operator:** The Operator user level has permission for Two-way Audio in Remote Configuration and all operating permissions in Camera Configuration by default.
    - **Guest:** The Guest user has no permission for 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 that logs onto the NVR. If it is configured and enabled, it allows only 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.

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 246, 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.



Figure 247, 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 NVR logs and system information
- **Local Parameters Settings:** Configuring parameters, restoring factory default parameters, and importing/exporting configuration files
- **Local Camera Management:** Add, delete, and edit IP cameras
- **Local Advanced Operation:** Operating HDD management (initializing HDD, setting HDD property), upgrading system firmware, clearing I/O alarm output.
- **Local Shutdown Reboot:** Shut down or reboot the NVR

- **Remote Configuration**

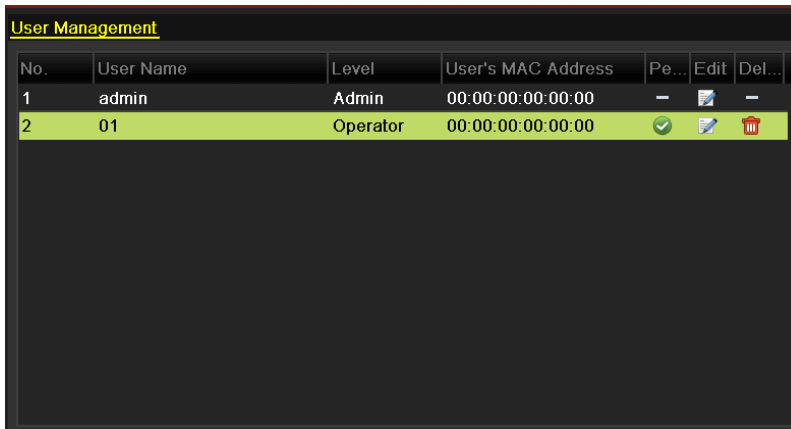
- **Remote Log Search:** Remotely view logs that are saved on the NVR
- **Remote Parameters Settings:** Remotely configure parameters, restore factory default parameters, and import/export configuration files
- **Remote Camera Management:** Remote add, delete, and edit IP cameras
- **Remote Serial Port Control:** Configure RS-232 and RS-485 port settings
- **Remote Video Output Control:** Sending remote button control signal
- **Two-Way Audio:** Realize two-way radio between remote client and NVR
- **Remote Alarm Control:** Remotely arm (notify alarm and exception message to remote client) and control the alarm output
- **Remote Advanced Operation:** Remotely operate HDD management (initialize HDD, set HDD property), upgrade system firmware, clear I/O alarm output

- **Remote Shutdown/Reboot:** Remotely shut down or reboot the NVR
  - **Camera Configuration**
    - **Remote Live View:** Remotely view live video of selected camera(s)
    - **Local Manual Operation:** Locally start/stop manual recording and alarm output of selected camera(s)
    - **Remote Manual Operation:** Remotely start/stop manual recording and alarm output of selected camera(s)
    - **Local Playback:** Locally play back recorded files of selected camera(s).
    - **Remote Playback:** Remotely play back recorded files of selected camera(s)
    - **Local PTZ Control:** Locally control **PTZ** movement of selected camera(s)
    - **Remote PTZ Control:** Remotely control **PTZ** movement of selected camera(s)
    - **Local Video Export:** Locally export recorded files of selected camera(s)
7. Click the **OK** button to save the settings and exit interface.

**NOTE:** Only the admin user account has permission to restore factory default parameters.

## 15.4.2 Deleting a User

1. Enter the User Management interface, **Menu > Configuration > User**.
2. Select the user to be deleted from the list.




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 248, User List

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

### 15.4.3 Editing a User

For added user accounts, you can edit the parameters.

1. Enter the User Management interface, **Menu > Configuration > User**.
2. Select the user to be edited from the list.
3. Click the  icon to enter the Edit User interface.



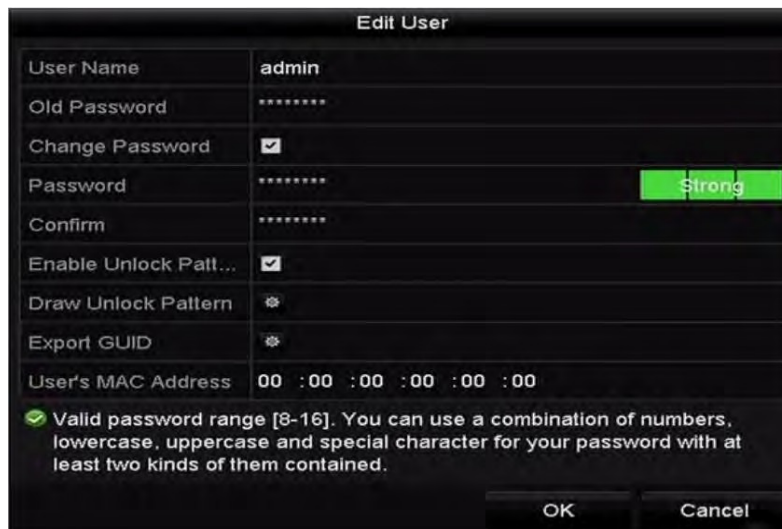
The screenshot shows the 'Edit User' dialog box with the following fields and values:

User Name	example1
Change Password	<input checked="" type="checkbox"/>
Password	***** <span style="background-color: green; color: white; padding: 2px;">Strong</span>
Confirm	*****
Level	Operator
User's MAC Address	00 :00 :00 :00 :00 :00

Below the fields, there is a green checkmark icon and the text: "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."

At the bottom right, there are 'OK' and 'Cancel' buttons.

Figure 249, Edit User (Operator/Guest)



The screenshot shows the 'Edit User' dialog box with the following fields and values:

User Name	admin
Old Password	*****
Change Password	<input checked="" type="checkbox"/>
Password	***** <span style="background-color: green; color: white; padding: 2px;">Strong</span>
Confirm	*****
Enable Unlock Patt...	<input checked="" type="checkbox"/>
Draw Unlock Pattern	
Export GUID	
User's MAC Address	00 :00 :00 :00 :00 :00

Below the fields, there is a green checkmark icon and the text: "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."

At the bottom right, there are 'OK' and 'Cancel' buttons.

Figure 250, Edit User (admin)

4. Edit the user password.
  - **Operator and Guest:** You can edit the user information, including user name, password, permission level, and MAC address. Check the **Change Password** checkbox if you want to change the password, and input the new password in the Password and Confirm text fields. A strong password is recommended.



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



**STRONG PASSWORD RECOMMENDED** – We highly recommend that you create a strong password of your own choosing (using a minimum of eight 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. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

5. Edit the unlock pattern for the admin user account.
  - 1) Check the **Enable Unlock Pattern** checkbox to enable the use of an unlock pattern when logging in to the device.
  - 2) Use the mouse to draw a pattern among the nine dots on the screen. Release the mouse when the pattern is done.

**NOTE:** Refer to *Configuring the Unlock Pattern* for detailed instructions.

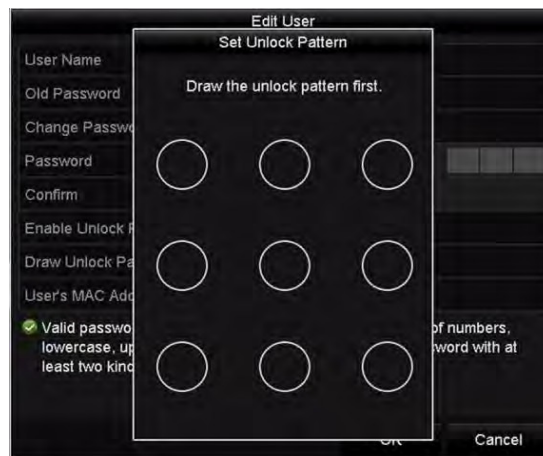




Figure 251, Set Unlock Patter for Admin User

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 USB flash disk for future password resetting. Refer to *Resetting 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 Glossary

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

## 16.2 Troubleshooting

- No image displayed on the monitor after starting up normally. Possible Reasons:
  - No VGA or HDMI connections.
  - Connection cable is damaged.

- Input mode of the monitor is incorrect.
1. Verify the device is connected with the monitor via HDMI or VGA cable.
  2. If not, please connect the device with the monitor and reboot.
  3. Verify the connection cable is good.
  4. If there is still no image display on the monitor after rebooting, please check if the connection cable is good, and change a cable to connect again.
  5. Verify Input mode of the monitor is correct.
  6. 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). If not, modify the monitor's input mode.
  7. Check if the fault is solved by steps 1 to 3.
  8. If it is solved, finish the process. If not, contact an engineer from Hikvision for further processing.
- There is an audible warning sound "Di-Di-Di-DiDi" after a new bought NVR starts up.

#### **Possible Reasons:**

- No HDD is installed in the device.
  - The installed HDD has not been initialized.
  - The installed HDD is not compatible with the NVR or is defective.
1. Verify at least one HDD is installed in the NVR, if not, install a compatible HDD.
    - NOTE:** 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 "HDD Error" Audible Warning checkbox.
  3. Verify the HDD is initialized.
    - 1) Select "**Menu > HDD > General.**"
    - 2) If the status of the HDD is "Uninitialized," check the checkbox of corresponding HDD and click the "Init" button.
  4. Verify the HDD is detected and is in good condition.
    - 1) Select "**Menu > HDD > General.**"
    - 2) If the HDD is not detected or the status is "Abnormal," replace the dedicated HDD according to the requirement.
  5. Check if the fault is solved by steps 1 to 3.

6. If it is solved, finish the process, if not, contact an engineer from Hikvision for further processing.
- The status of the added IP camera displays as “Disconnected” when it is connected through Private Protocol. Select “**Menu > Camera > Camera > IP Camera**” to get the camera status.

**Possible Reasons:**

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

1. Verify the network is connected.

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

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

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

2. Verify the configuration parameters are correct.

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

3. Verify the bandwidth is adequate.

- 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 steps 1 to 3. If it is solved, finish the process. If not, contact an engineer from Hikvision for further processing.

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

**Possible Reasons:**

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

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 > DeviceInfo,**" 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, 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.

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

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

4. Verify the switch is not flow control.

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

5. Check if the fault is solved by the steps 1 to 4. If it is solved, finish the process. If not, contact an engineer from Hikvision for further processing.
- No monitor connected to the NVR locally, and when you manage the IP camera to connect with the device by Web browser remotely, the status displays as Connected. And when you connect the device with the monitor via VGA or HDMI interface and reboot the device, there is black screen with the mouse cursor.
  - Connect the NVR with the monitor before startup via VGA or HDMI interface, and manage the IP camera to connect with the device locally or remotely, the status of IP camera displays as Connect. And then connect the device with the CVBS, and there is a black screen.

#### **Possible Reasons:**

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

**NOTE:** The view settings can be configured only by local NVR operation.

Different camera orders and window-division modes can be set for different output

interfaces separately, and digits such as "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, contact an engineer from Hikvision for further processing.
  - Live view is stuck when video output locally. Possible Reasons:
    - Poor network between NVR and IP camera, and there exists packet loss during the transmission.
    - The frame rate has not reached the real-time frame rate.
4. Verify the network between NVR and IP camera is connected.
  - When image is stuck, connect the RS-232 ports on PC and the rear panel of NVR with the RS-232 cable.
  - Open the Super Terminal, and execute the command of "**ping 192.168.0.0 -l 1472 -f**" (the IP address may change according to the real condition), and check if there exists packet loss.

**NOTE:** Simultaneously press **Ctrl** and **C** to exit the ping command.
5. Verify the frame rate is real-time frame rate.
  - Select "**Menu > Record > Parameters > Record,**" and set the Frame rate to Full Frame.
6. Check if the fault is solved by the above steps. If it is solved, finish the process. If not, contact an engineer from Hikvision for further processing.
  - Live view is stuck when video output remotely via Internet Explorer or platform software. Possible Reasons:
    - Poor network between NVR and IP camera, and there exists packet loss during the transmission.
    - Poor network between NVR and PC, and there exists packet loss during the transmission.
    - The hardware performance is not good enough, including CPU, memory, etc.
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.

**NOTE:** Simultaneously press **Ctrl** and **C** to exit the ping command.
2. Verify the network between NVR and PC is connected.
  - 1) Open the cmd window in the Start menu, or you can press "windows+R" shortcut key to open it.
  - 2) Use the ping command to send large packets to the NVR, execute the command "ping 192.168.0.0 -l

1472 -f" (the IP address may change according to the real condition), and check if there exists packet loss.

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

3. Verify the hardware of the PC is good enough.

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

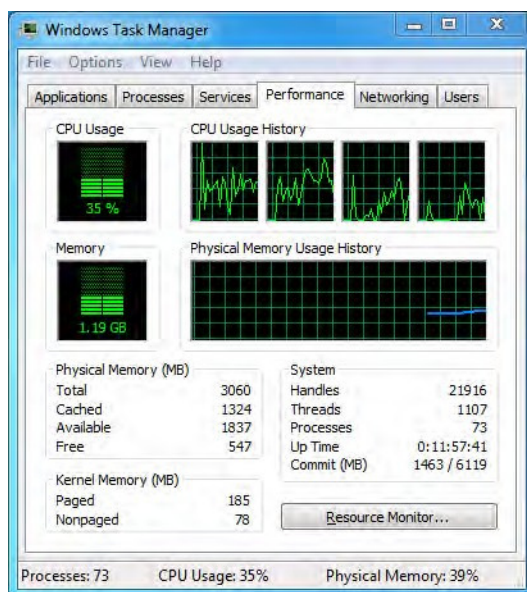


Figure 252, Windows Task Management Interface

- Select the "Performance" tab; check the status of the CPU and Memory.
  - If the resource is not enough, end some unnecessary processes.
4. Check if the fault is solved by the above steps. If it is solved, finish the process. If not, contact an engineer from Hikvision for further processing.
- When using the NVR to get the live view audio, there is no sound or there is too much noise, or the volume is too low.

#### Possible Reasons:

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

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

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

2. Verify the setting parameters are correct.

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

3. Verify the IP camera's audio encoding standard 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, contact an engineer from Hikvision for further processing.

- The image gets stuck when the NVR is playing back by single or multi-channel. Possible Reasons:
  - Poor network between NVR and IP camera, and there exists packet loss during the transmission.
  - The frame rate is not the real-time frame rate.
  - The NVR supports up to 16-channel synchronize playback at the resolution of 4CIF, if you want a 16-channel synchronize playback at the resolution of 720p, the frame extracting may occur, which leads to the image getting slightly stuck.

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

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

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

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

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

7. Verify the hardware can afford the playback.

Reduce the channel number of playback.

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

8. Reduce the number of local playback channel.

Select "**Menu > Playback**," and uncheck the checkbox(es) of unnecessary channels.

9. Check if the fault is solved by the above steps. If it is solved, finish the process. If not, contact an engineer from Hikvision for further processing.

- No record file found in the NVR's local HDD, and prompt "No record file found." Possible Reasons:
  - The time setting of system is incorrect.



- The search condition is incorrect.
- The HDD is error or not detected.

10. Verify the system time setting is correct.

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

11. Verify the search condition is correct.

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

12. 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.

13. Check if the fault is solved by the above steps. If it is solved, finish the process. If not, contact an engineer from Hikvision for further processing.