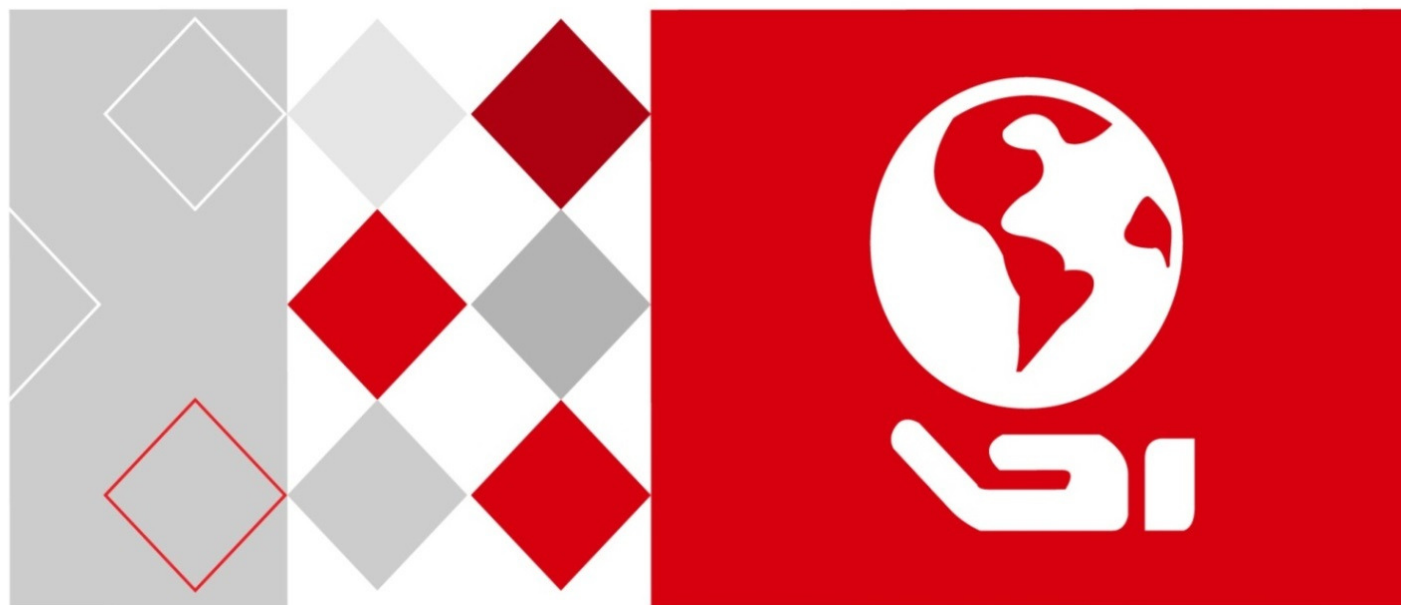


HIKVISION®



DS-72xxHUI-Kx, DS-72xxHQI-Kx
Digital Video Recorder (DVR)

User Manual

COPYRIGHT © 2017 Hangzhou Hikvision Digital Technology Co., Ltd.

ALL RIGHTS RESERVED.

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

About this Manual

This Manual is applicable to -K Series TurboHD Digital Video Recorders (DVRs).

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/>).

Images in this manual are for illustrative purposes only and may differ from the actual product.

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 LATER PREVAILS.

Regulatory Information

FCC Information

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

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

FCC Conditions

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

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

EU Conformity Statement



This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, the LVD Directive 2014/35/EU, the RoHS Directive 2011/65/EU.



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



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

Industry Canada ICES-003 Compliance

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




Applicable Models

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

Series	Model
DS-72xxHQI-Kx	DS-7204HQI-K1 DS-7208HQI-K2 DS-7216HQI-K2
DS-72xxHUI-Kx	DS-7204HUI-K1 DS-7208HUI-K2 DS-7216HUI-K2

Symbol Conventions

The symbols in this document are defined as follows.

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

Safety Instructions

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

Preventive and Cautionary Tips

Before connecting and operating your device, please be advised of the following tips:

- Ensure unit is installed in a well-ventilated, dust-free environment.
- Unit is designed for indoor use only.
- Keep all liquids away from the device.
- Ensure environmental conditions meet factory specifications.
- Ensure unit is properly secured to a rack or shelf. Major shocks or jolts to the unit as a result of dropping it may cause damage to the sensitive electronics within the unit.
- Use the device in conjunction with an UPS if possible.
- Power down the unit before connecting and disconnecting accessories and peripherals.
- A factory recommended HDD should be used for this device.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.
- Ensure to use the attached power adaptor only and not to change the adaptor randomly.

Product Key Features

General

- Connectable to Turbo HD and analog cameras
- Supports UTC protocol for connecting camera over coax
- Connectable to IP cameras
- The analog signal inputs including TurboHD and CVBS can be automatically recognized without configuration
- Each channel supports dual-stream, and sub-stream supports up to WD1 resolution
- The main stream of DS-72xxHQI-Kx Series supports up to 3 MP resolution for the first 4 channels
- The main stream of DS-72xxHUI-Kx Series supports up to 5 MP resolution of all the channels
- For DS-72xxHUI-Kx Series DVR, 5 MP long distance transmission can be enabled for the analog cameras
- Independent configuration for each channel, including resolution, frame rate, bit rate, image quality, etc.
- Encoding for both video stream and video & audio stream; audio and video synchronization during composite stream encoding
- Supports enabling H.265+/H.264+ to ensure high video quality with lowered bit rate
- H.265+/H.265/H.264+/H.264 encoding for the main stream, and H.265/H.264 encoding for the sub-stream of analog cameras
- Connectable to H.265 and H.264 IP cameras
- Defog level, night to day sensitivity, day to night sensitivity, and IR light brightness configurable for the connected analog cameras supporting these parameters
- 4 MP/5 MP signal switch for the supported analog cameras
- Watermark technology

Local Monitoring

- HDMI output at up to 4K (3840 × 2160) resolution
- 1/4/6/8/9/16/25 screen live view is supported, and the display sequence of screens is adjustable
- Live view screen can be switched in group and manual switch and automatic cycle live view are also provided, the interval of automatic cycle can be adjusted
- CVBS output only serves as the aux output or live view output
- Quick setting menu is provided for live view
- The selected live view channel can be shielded
- VCA information overlay in live view for the supported analog cameras and in smart playback for the supported analog and IP cameras
- Motion detection, video-tampering detection, video exception alarm, video loss alarm and VCA alarm functions
- DS-72xxHUI-Kx Series DVRs support VCA (line crossing detection and intrusion detection) of all channels. DS-7216HQI-Kx Series DVRs support 2-ch VCA (line crossing detection and intrusion detection). For the analog channels, the line crossing detection and intrusion detection conflict with other VCA detection such as sudden scene change detection, face detection and vehicle detection. You can enable only one function.

- For DS-72xxHUI-Kx Series DVRs, the enhanced VCA mode conflicts with the 2K/4K output and 4 MP/5 MP signal input
- Privacy mask
- Several PTZ protocols (including Omnicast VMS of Genetec) supported; PTZ preset, patrol and pattern
- Zooming in/out by clicking the mouse and PTZ tracing by dragging mouse

HDD Management

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

Recording and Playback

- Holiday recording schedule configuration
- Cycle and non-cycle recording modes
- Normal and event video encoding parameters
- Multiple recording types: manual, continuous, alarm, motion, motion | alarm, motion & alarm and event
- Eight recording time periods with separated recording types
- Supports Channel-Zero encoding
- Main stream and sub-stream configurable for simultaneous recording
- Pre-record and post-record for motion detection triggered recording, and pre-record time for schedule and manual recording
- Searching record files by events (alarm input/motion detection)
- Customization of tags, searching and playing back by tags
- Locking and unlocking of record files
- Local redundant recording
- When TurboHD input is connected, the information including the resolution and frame rate will be overlaid on the bottom right corner of the live view for 5 seconds. When CVBS input is connected, the information such as NTSC or PAL will be overlaid on the bottom right corner of the live view for 5 seconds.
- Searching and playing back record files by camera number, recording type, start time, end time, etc.
- Smart playback to go through less effective information
- Main stream and sub-stream selectable for local/remote playback
- Zooming in for any area when playback
- Multi-channel reverse playback

- Supports pause, fast forward, slow forward, skip forward, and skip backward when playback, locating by dragging the mouse on the progress bar
- 8/16-ch synchronous playback

Backup

- Exports data to a USB device
- Exports video clips for playback
- Video and Log, Video and Player, and Player are selectable to export for backup
- Management and maintenance of backup devices

Alarm and Exception

- Configurable arming time of alarm input/output
- Alarms for video loss, motion detection, video tampering, abnormal signal, video input/recording resolution mismatch, illegal login, network disconnected, IP confliction, record/capture exception, HDD error, HDD full, etc.
- Alarm triggers full screen monitoring, audio alarm, notifying surveillance center, sending e-mail, and alarm output
- One-key disarms the linkage actions of the alarm input
- PTZ linking for the VCA alarm
- VCA detection alarm is supported
- Supports coaxial alarm
- System will automatically reboot when a problem is detected in an attempt to restore normal functionality

Other Local Functions

- Manual and automatic video quality diagnostics
- Operable by mouse and remote control
- Three-level user management; admin user can create many operating account and define their operating permission, which includes the permission to access any channel
- Completeness of operation, alarm, exceptions and log writing and searching
- Manually triggering and clearing alarms
- Importing and exporting of configuration file of devices
- Getting cameras type information automatically
- Unlock pattern for device login for the *admin*
- Clear-text password available
- GUID file can be exported for password resetting
- Multiple connected TurboHD signal analog cameras can be upgraded simultaneously via DVR

Network Functions

- 1 self-adaptive 10M/100M/1000M network interface
- IPv6 is supported
- TCP/IP protocol, PPPoE, DHCP, DNS, DDNS, NTP, SADP, SMTP, NFS, iSCSI, UPnP™, and HTTPS are supported
- Supports access by Hik-Connect. If you enable Hik-Connect, the device will remind you of Internet access risk and ask you to confirm the “Terms of Service” and “Privacy Statement” before enabling the service. You should create a verification code to connect to Hik-Connect.
- TCP, UDP, and RTP for unicast
- Auto/Manual port mapping by UPnP™
- Remote search, playback, download, locking and unlocking record files, and downloading files broken transfer resume
- Remote parameters setup; remote import/export of device parameters
- Remote viewing of device status, system logs, and alarm status
- Remote keyboard operation
- Remote HDD formatting and program upgrading
- Remote system restart and shutdown
- Supports upgrading via remote FTP server
- RS-485 transparent channel transmission
- Alarm and exception information can be sent to the remote host
- Remotely start/stop recording
- Remotely start/stop alarm output
- Remote PTZ control
- Two-way audio and voice broadcasting
- Output bandwidth limit configurable
- Embedded WEB server
- If DHCP is enabled, ability to enable DNS DHCP or disable it and edit the Preferred DNS Server and Alternate DNS Server

Development Scalability

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

Table of Contents

Chapter 1 Introduction	14
1.1 Front Panel	14
1.2 IR Remote Control Operations.....	14
1.2.1 Using the Remote Control.....	15
1.2.2 Troubleshooting Remote Control.....	16
1.3 USB Mouse.....	16
1.3.1 Mouse Operation	17
1.3.2 Input Method.....	17
1.3.3 Description of the Soft Keyboard Buttons	17
1.4 Rear Panel.....	18
Chapter 2 Getting Started	20
2.1 Starting Up and Shutting Down the DVR	20
2.1.1 Before Starting.....	20
2.1.2 Starting the DVR.....	20
2.1.3 Shutting Down the DVR.....	20
2.1.4 Rebooting the DVR.....	21
2.2 Activating the Device	21
2.3 Using the Unlock Pattern for Login	22
2.3.1 Configuring the Unlock Pattern	23
2.3.2 Logging in via Unlock Pattern	24
2.4 Login and Logout	25
2.4.1 User Login	25
2.4.2 User Logout	26
2.5 Resetting Your Password	27
2.6 Adding and Connecting IP Cameras.....	28
2.6.1 Activating IP Cameras	28
2.6.2 Adding an Online IP Camera	32
2.6.3 Editing the Connected IP Camera	34
Chapter 3 Live View	36
3.1 Introduction	36
3.1.1 Live View Icons.....	36
3.2 Operations in Live View Mode	36
3.2.1 Using the Mouse in Live View.....	37
3.2.2 Switching Main/Aux Output.....	38
3.2.3 Quick Setting Toolbar in Live View Mode	38
3.3 Channel-Zero Encoding.....	42
3.4 Adjusting Live View Settings.....	42
3.5 Manual Video Quality Diagnostics	44
Chapter 4 PTZ Controls	46
4.1 Configuring PTZ Settings.....	46

4.2	Setting PTZ Presets, Patrols, and Patterns	48
4.2.1	Customizing Presets.....	48
4.2.2	Calling Presets.....	49
4.2.3	Customizing Patrols.....	50
4.2.4	Calling Patrols.....	52
4.2.5	Customizing Patterns.....	52
4.2.6	Calling Patterns	53
4.2.7	Customizing Linear Scan Limit	54
4.2.8	Calling Linear Scan.....	55
4.2.9	One-Touch Park	56
4.3	PTZ Control Panel	57
Chapter 5	Recording Settings	59
5.1	Configuring Encoding Parameters	59
5.1.1	Before Starting.....	59
5.1.2	Configure Record Parameters	59
5.2	Configuring Recording Schedule	64
5.2.1	Set the Record Schedule.....	64
5.2.2	Edit the Schedule.....	65
5.2.3	Draw the schedule	66
5.3	Configuring Motion Detection Recording	67
5.4	Configuring Alarm Triggered Recording and Capture	68
5.5	Configuring Event Recording.....	70
5.6	Configuring Manual Recording	72
5.7	Configuring Holiday Recording	73
5.8	Configuring Redundant Recording.....	74
5.9	Configuring HDD Group.....	76
5.10	Files Protection	77
5.10.1	Protect File by Locking the Record Files.....	77
5.10.2	Protect File by Setting HDD Property to Read-Only	78
5.11	One-Key Enabling and Disabling H.264+/H.265+ for Analog Cameras	79
5.11.1	One-Key Enabling H.264+/H.265+ All Analog Cameras	79
5.11.2	One-Key Disabling H.264+/H.265+ All Analog Cameras	80
5.12	Configuring 1080p Lite.....	80
5.12.1	Enabling 1080p Lite Mode	81
5.12.2	Disabling the 1080p Lite Mode	81
Chapter 6	Playback	82
6.1	Playing Back Record Files	82
6.1.1	Instant Playback	82
6.1.1.1	Instant Playback by Channel	82
6.1.1.2	Playing Back by Normal Search	82
6.2	Playback Auxiliary Functions	97
6.2.1	Playing Back Frame-by-Frame	97
6.2.2	Digital Zoom.....	98

6.2.3	Reverse Playback of Multi-Channel	98
Chapter 7	Backup	100
7.1	Backing up Record Files	100
7.1.1	Backing Up by Normal Video/Picture Search.....	100
7.1.2	Backing Up Video Clips	103
7.2	Managing Backup Devices	103
7.2.1	Management of USB Flash Drives, and USB HDDs.....	103
Chapter 8	Alarm Settings	105
8.1	Setting Motion Detection.....	105
8.2	Setting Sensor Alarms	107
8.3	Detecting Video Loss.....	109
8.4	Detecting Video Tampering	111
8.5	Setting All-day Video Quality Diagnostics	113
8.6	Handling Exceptions	115
8.7	Setting Alarm Response Actions	117
Chapter 9	VCA Alarm	120
9.1	Face Detection.....	120
9.2	Line Crossing Detection.....	122
9.3	Intrusion Detection.....	123
9.4	Region Entrance Detection	126
9.5	Region Exiting Detection.....	127
9.6	Loitering Detection.....	127
9.7	People Gathering Detection.....	128
9.8	Fast Moving Detection	128
9.9	Parking Detection	128
9.10	Unattended Baggage Detection.....	128
9.11	Object Removal Detection	129
9.12	Audio Exception Detection.....	129
9.13	Defocus Detection	130
9.14	Sudden Scene Change.....	130
9.15	PIR Alarm	131
Chapter 10	VCA Search	131
10.1	Face Search	132
10.2	Behavior Search	134
10.3	People Counting	135
10.4	Heat Map	136
Chapter 11	Network Settings	138
11.1	Configuring General Settings.....	138
11.2	Configuring Advanced Settings.....	139
11.2.1	Configuring PPPoE Settings	139
11.2.2	Configuring Hik-Connect.....	139
11.2.3	Configuring DDNS	141

11.2.4	Configuring NTP Server.....	143
11.2.5	Configuring NAT	144
11.2.6	Configuring More Settings	146
11.2.7	Configuring HTTPS Port	147
11.2.8	Configuring E-Mail	149
11.2.8.1	Before Starting	149
11.2.8.2	Procedure	149
11.2.9	Checking Network Traffic.....	151
11.3	Configuring Network Detection	151
11.3.1	Testing Network Delay and Packet Loss	151
11.3.2	Exporting Network Packet.....	152
11.3.3	Checking Network Status.....	153
11.3.4	Checking Network Statistics	154
Chapter 12	HDD Management	155
12.1	Initializing HDDs	155
12.2	Managing Network HDD	156
12.3	Managing HDD Groups.....	158
12.3.1	Setting HDD Groups	158
12.3.2	Setting HDD Property	160
12.4	Configuring Quota Mode.....	161
12.5	Configuring Cloud Storage.....	162
12.6	Checking HDD Status.....	165
12.7	Checking S.M.A.R.T. Information	166
12.8	Detecting Bad Sectors	166
12.9	Configuring HDD Error Alarms.....	167
Chapter 13	Camera Settings	169
13.1	Assigning 5 MP Long Distance Transmission.....	169
13.2	Configuring OSD Settings.....	170
13.3	Configuring Privacy Mask	171
13.4	Configuring Video Parameters.....	172
13.4.1	Configuring Image Settings.....	172
13.4.2	Configuring Camera Parameters Settings	174
Chapter 14	DVR Management and Maintenance	176
14.1	Viewing System Information	176
14.2	Searching Log Files	176
14.3	Importing/Exporting IP Camera Info.....	178
14.4	Importing/Exporting Configuration Files.....	178
14.5	Upgrading System	179
14.5.1	Upgrading by Local Backup Device	179
14.5.2	Upgrading by FTP.....	180
14.6	Upgrading Camera	181
14.7	Restoring Default Settings	182
Chapter 15	Others	184

15.1	Configuring General Settings.....	184
15.2	Configuring DST Settings	184
15.3	Configuring More Settings	186
15.4	Managing User Accounts.....	188
15.4.1	Adding a User.....	188
15.4.2	Deleting a User.....	192
15.4.3	Editing a User	192
Chapter 16	Appendix	195
16.1	Glossary.....	195
16.2	Troubleshooting.....	196

Chapter 1 Introduction

1.1 Front Panel

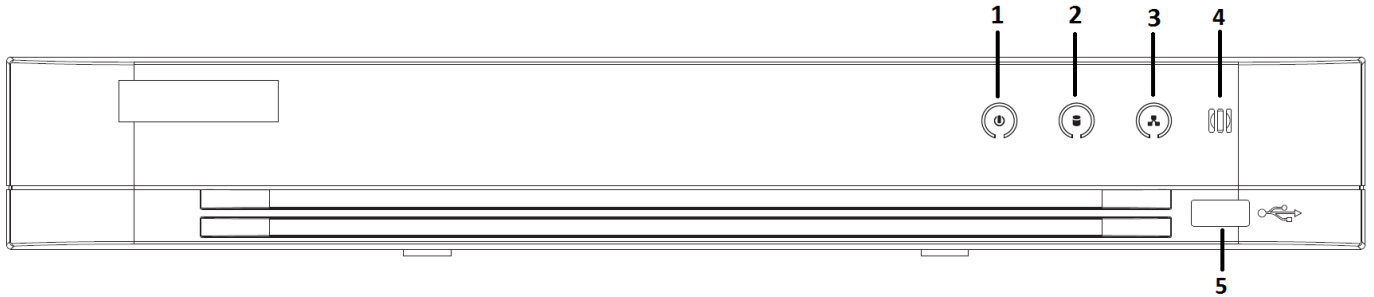


Figure 1, Front Panel of DS-7216HQI-Kx and DS-72xxHUI-Kx

Table 1-1 Front Panel Description

No.	Icon	Description
1		Lights when DVR is powered up
2		Lights when data is being read from or written to HDD
3		Flashes when the network is well connected
4		IR remote control receiver
5	USB Interface	Universal Serial Bus (USB) ports for additional devices such as USB mouse and USB Hard Disk Drive (HDD)

1.2 IR Remote Control Operations

The DVR may also be controlled with the included IR remote control, shown in Figure 1-9.



NOTE

2 × AAA batteries must be installed before operation.

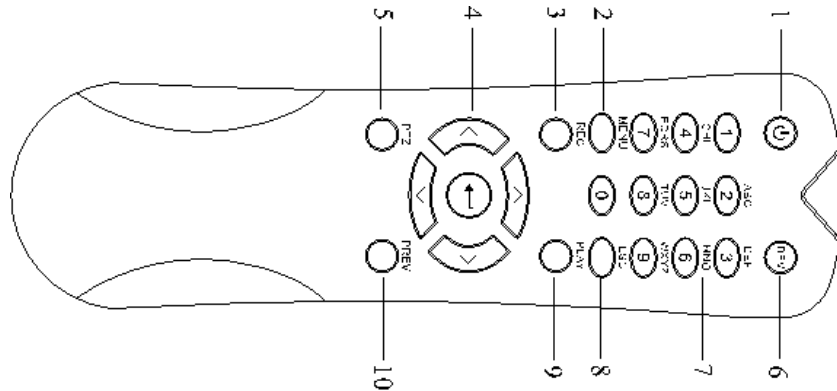


Figure 2, Remote Control

1.2.1 Using the Remote Control

The remote control keys resemble the ones on the front panel (see Table 1-2).

Table 1-2 Description of the IR Remote Control Buttons

No.	Name	Description
1	POWER	Power on/off the device by pressing and holding the button for 5 seconds
2	MENU Button	Press the button to return to the main menu (after successful login)
		Press and hold the button for 5 seconds will turn off audible key beep
		In PTZ Control mode, the MENU button will start wiper (if applicable)
		In Playback mode, it is used to show/hide the control interface
3	REC Button	Enter the Manual Record setting menu
		In PTZ control settings, press the button and then you can call a PTZ preset by pressing Numeric button
		It is also used to turn audio on/off in the Playback mode
4	DIRECTION Button	Navigate between different fields and items in menus
		In the Playback mode, the Up and Down button is used to speed up and slow down recorded video. The Left and Right button will select the next and previous record files.
		In Live View mode, these buttons can be used to cycle through channels
		In PTZ control mode, it can control the movement of the PTZ camera
	ENTER Button	Confirm selection in any of the menu modes
	It can also be used to tick checkbox fields	
	In Playback mode, it can be used to play or pause the video	
	In single-frame Playback mode, pressing the button will advance the video by a single frame	
5	PTZ Button	In Auto-switch mode, it can be used to stop /start auto switch
6	DEV	Enables/Disables Remote Control
7	Alphanumeric Buttons	Switch to the corresponding channel in Live view or PTZ Control mode
		Input numbers and characters in Edit mode
		Switch between different channels in the Playback mode
8	ESC Button	Back to the previous menu
		Press for Arming/disarming the device in Live View mode
9	PLAY Button	The button is used to enter the All-day Playback mode
		It is also used to auto scan in the PTZ Control menu
10	PREV Button	Switch between single screen and multi-screen mode
		In PTZ Control mode, it is used to adjust the focus in conjunction with the A/FOCUS+ button

1.2.2 Troubleshooting Remote Control



NOTE

Make sure you have installed batteries properly in the remote control. Also, the remote control must be aimed at the IR receiver on the front panel.

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

1. Go into Menu > Configuration > General > More Settings by operating the front control panel or the mouse.
2. Check and remember the DVR No. The default DVR No. is 255. This number is valid for all IR remote controls.
3. Press the DEV button on the remote control.
4. Enter the DVR No. in step 2.
5. Press the ENTER button on the remote.

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

If the remote still does not function properly, change the remote and try again, or contact the device provider.

1.3 USB Mouse

A regular 3-button (Left/Right/Scroll-wheel) USB mouse can also be used with this DVR.

1. Plug USB mouse into one of the USB interfaces on the front panel of the DVR.
2. The mouse should be detected automatically. 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.

1.3.1 Mouse Operation

Table 1-3 Description of the Mouse Control

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

1.3.2 Input Method



Figure 3, Soft Keyboard

1.3.3 Description of the Soft Keyboard Buttons

Table 1-4 Description of the Soft Keyboard Icons

Icon	Description	Icon	Description
	Numbers		Letters
	Lowercase/uppercase		Backspace
	Switch the keyboard		Space
	Position the cursor		Enter
	Symbols		Reserved

1.4 Rear Panel

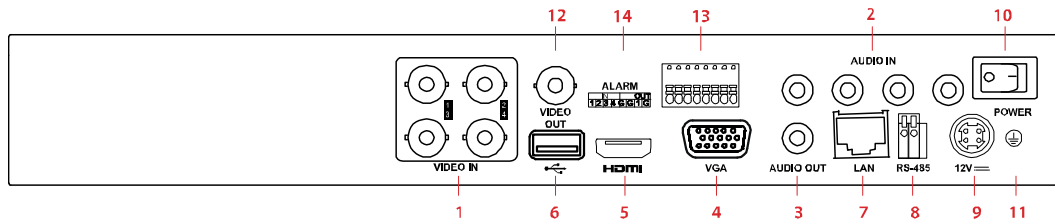


Figure 4, DS-7204HUI-K1 Rear Panel

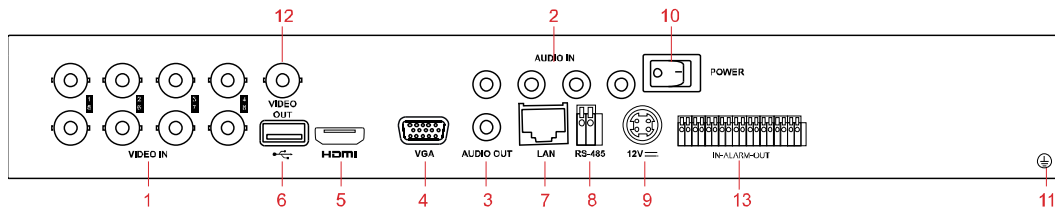


Figure 5, DS-7208HUI-K2 Rear Panel

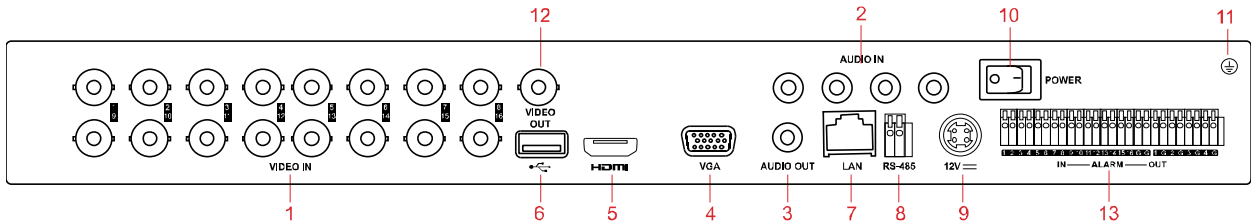


Figure 6, DS-7216HUI-K2 Rear Panel

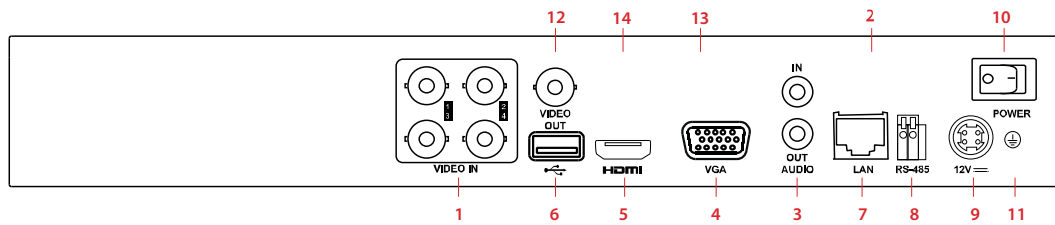


Figure 7, DS-7204HQI-K1

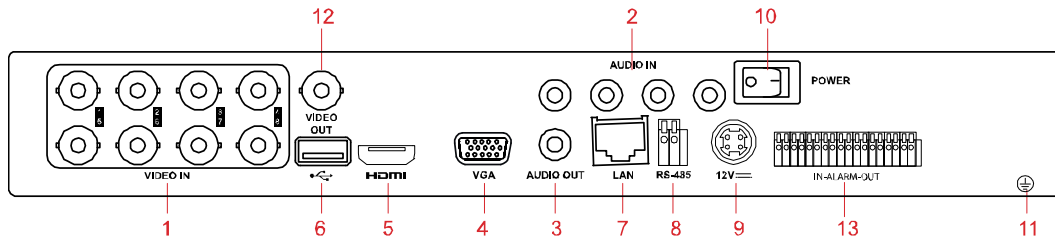


Figure 8, DS-7208HQI-K2

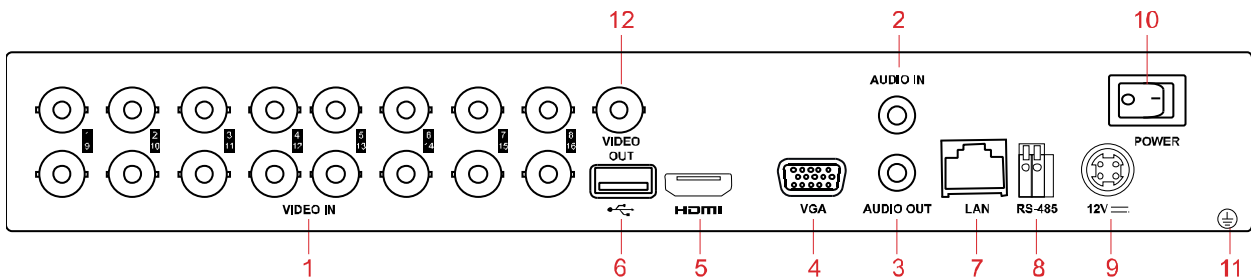


Figure 9, DS-7216HQI-K2 Rear Panel

Table 1-5 Description of Rear Panels

No.	Item	Description
1	VIDEO IN	BNC interface for TurboHD and analog video input
2	AUDIO IN	RCA connector
3	AUDIO OUT	RCA connector
4	VGA	DB-15 connector for VGA output. Display local video output and menu.
5	HDMI	HDMI video output connector
6	USB Port	USB port for additional devices
7	Network Interface	Connector for network
8	RS-485 Interface	Connector for RS-485 devices
9	Power Supply	12 VDC power supply
10	Power Switch	Switch for turning on/off the device
11	GND	Ground
12	VIDEO OUT	BNC connector for video output
13	Alarm In/Out	Connector for alarm input and output

Chapter 2 Getting Started

2.1 Starting Up and Shutting Down the DVR

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

2.1.1 Before Starting

Check that the power supply voltage matches the DVR's requirement, and ensure the ground connection is working properly.

2.1.2 Starting the DVR

1. Plug the power cord into an electrical outlet. It is HIGHLY recommended that an Uninterruptible Power Supply (UPS) be used in conjunction with the device.
2. Turn on the power switch on the rear panel, and the Power indicator LED should turn on indicating that the unit is starting.
3. After startup, the Power indicator LED remains on.

2.1.3 Shutting Down the DVR

1. Enter the Shutdown menu, Menu > Maintenance > Shutdown (icon in lower left corner).



Figure 10, Shutdown Menu

2. Click **Shutdown**.
3. Click **Yes**.
4. Turn off the rear panel power switch (16 channel only) when the "Please Power Off" prompt appears.

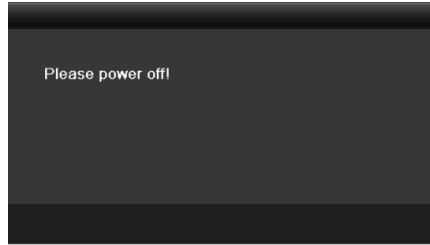


Figure 11, Shutdown Prompt

2.1.4 Rebooting the DVR

While in the Shutdown menu, you can also reboot the DVR.

1. Enter the Shutdown menu by clicking Menu > Shutdown.
2. Click **Logout** to log out or **Reboot** to reboot.

2.2 Activating the Device

For first-time access, you must activate the device by setting an admin password. No operation is allowed before activation. You can also activate the device via Web browser, SADP, or client software.

1. Input the same password in the Create New Password and Confirm New Password text fields.



NOTE

Click  to show/hide the password.



Figure 12, Settings Admin Password




WARNING

STRONG PASSWORD RECOMMENDED – We highly recommend 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. Resetting the password monthly or weekly can better protect your product.

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



Click  to show the password. Click again to hide the password.

3. After the device has been activated, the GUID Attention box pops up as below.



Figure 13, Attention Window

4. (Optional) Click **Yes** to export GUID. The Reset Password window pops up. Click **Export** to export GUID to the USB flash drive for password resetting.

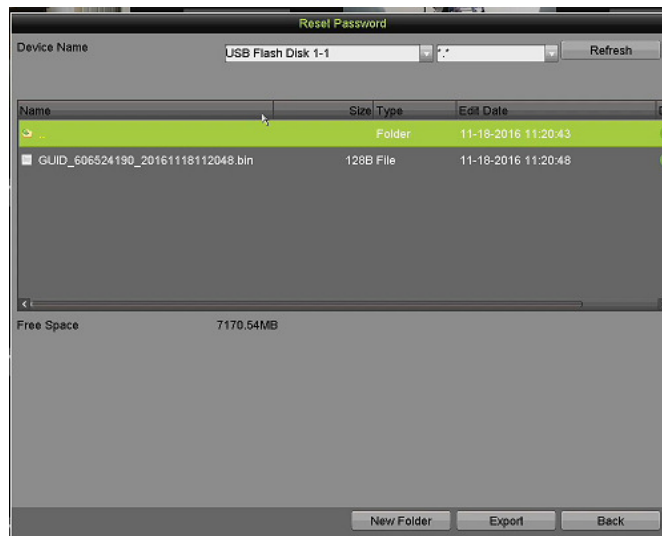


Figure 14, Export GUID

5. After exporting the GUID, the Attention box pops up as below. Click **Yes** to duplicate the password or **No** to cancel it.



Figure 15, Duplicate the Password

2.3 Using the Unlock Pattern for Login

For the *admin*, you can configure the unlock pattern for device login.

2.3.1 Configuring the Unlock Pattern

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

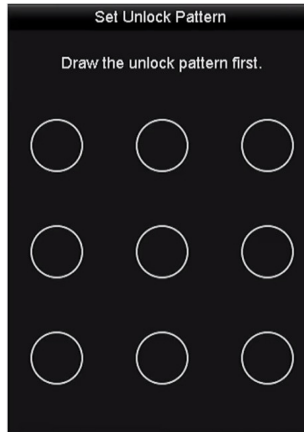


Figure 16, Set Unlock Pattern

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

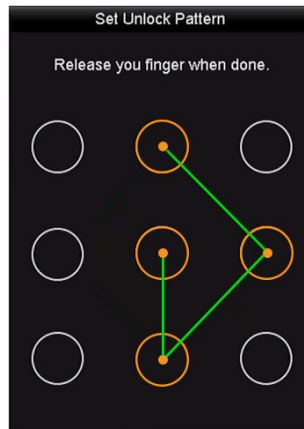


Figure 17, Draw the Pattern



NOTE

Connect at least four dots to draw the pattern.

Each dot can connect only once.

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

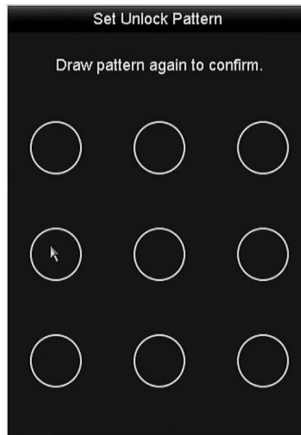


Figure 18, Confirm the Pattern



NOTE

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

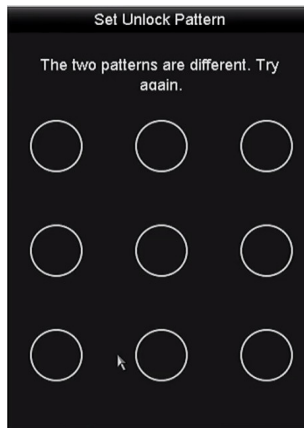


Figure 19, Reset the Pattern

2.3.2 Logging in via Unlock Pattern



NOTE

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

Configure the pattern before unlocking. Refer to section 2.3.1 Configuring the Unlock Pattern.

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

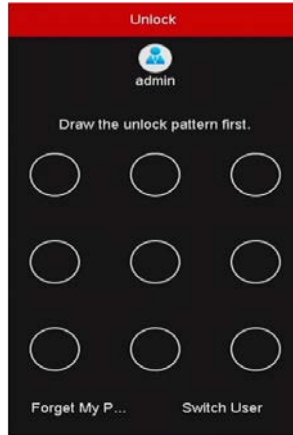


Figure 20, Draw the Unlock Pattern

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



NOTE

Right click the mouse to log in via the normal mode.

If you have forgotten your pattern, select **Forgot My Pattern** or **Switch User** to show the normal login dialog box.

If the pattern you draw is different from the pattern you configured, try again. If you draw the wrong pattern seven times, the account will lock for one minute.



Figure 21, Normal Login Dialog Box

2.4 Login and Logout

2.4.1 User Login

You must log in to the device before operating the menu and other functions

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



Figure 22, Login Interface

2. Enter the **Password**.
3. Click **OK** to log in.

 **NOTE**

If the admin enters the wrong logon password seven times, the account will lock for 60 seconds. If an operator enters the wrong password five times, the account will lock for 60 seconds.

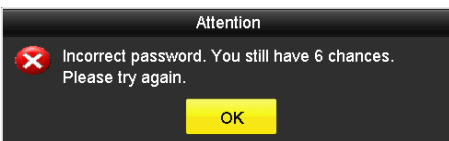


Figure 23, User Account Protection for the Admin

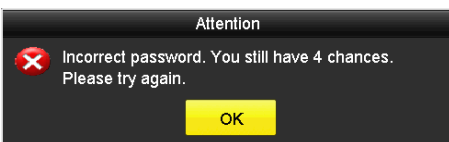


Figure 24, User Account Protection for the Operator

2.4.2 User Logout

After logging out, the monitor changes to Live View mode. To perform operations, enter the user name and password to log in again.

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



Figure 25, Logout

2. Click **Logout**.



If you log out of the system, menu operation is invalid. You must enter a valid user name and password to unlock the system.

2.5 Resetting Your Password

If you forget the *admin* password, you can reset it by importing the GUID file. The GUID file must be exported and saved in the local USB flash drive after activating the device.

1. On the user login interface, click **Forgot Password** to pop up the Import GUID interface.

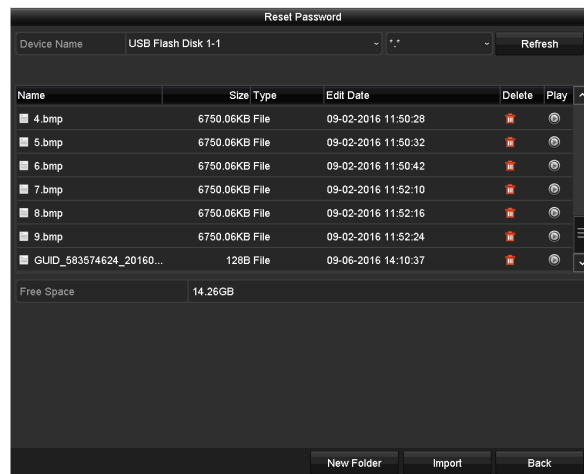


Figure 26, Import GUID

2. Select the GUID file from the USB flash drive.
3. Click **Import** to pop up the Reset Password interface.

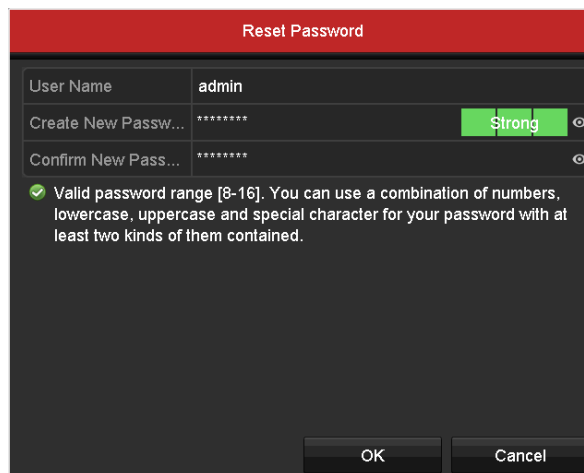


Figure 27, Reset Password

4. Enter and confirm the new password.

5. Click **OK** to save the new password. The Attention box will pop up as shown below.



Figure 28, GUID File Imported

6. Click **OK**, and the Attention box will pop up to remind you to duplicate the device password to IP cameras that are connected with default protocol. Click **Yes** to duplicate the password or **No** to cancel.



Figure 29, Duplicate the Password



NOTE

To retrieve a forgotten password, you must first export the GUID file.

Once the password is reset, the GUID file will be invalid. You can export a new GUID file.

2.6 Adding and Connecting IP Cameras

2.6.1 Activating IP Cameras

Before adding the cameras, make sure the IP cameras to be added are in active status.

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



NOTE

For IP cameras detected online in the same network segment, the **Security** status shows whether they are active or inactive.



Figure 30, IP Camera Management Interface

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

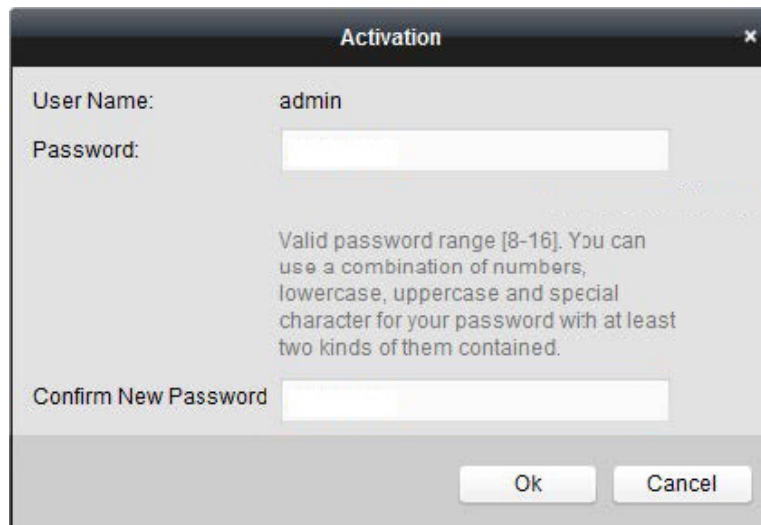


Figure 31, Activate the Camera

3. Set a camera password to activate it.
 - **Use Admin Password:** When you check the this checkbox, the camera(s) will be configured with the same admin password as the operating DVR.
 - **Create New Password:** If the admin password is not used, you must create and confirm a new password for the camera.

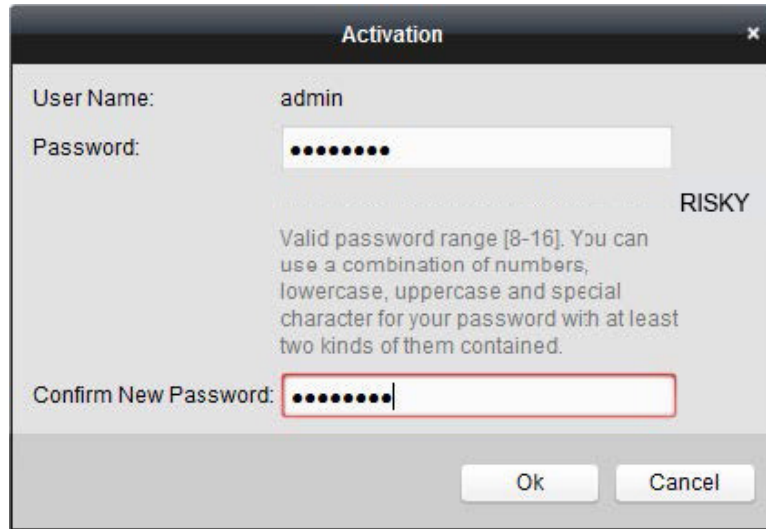


Figure 32, Level 0 (Inadequate) Strength Password

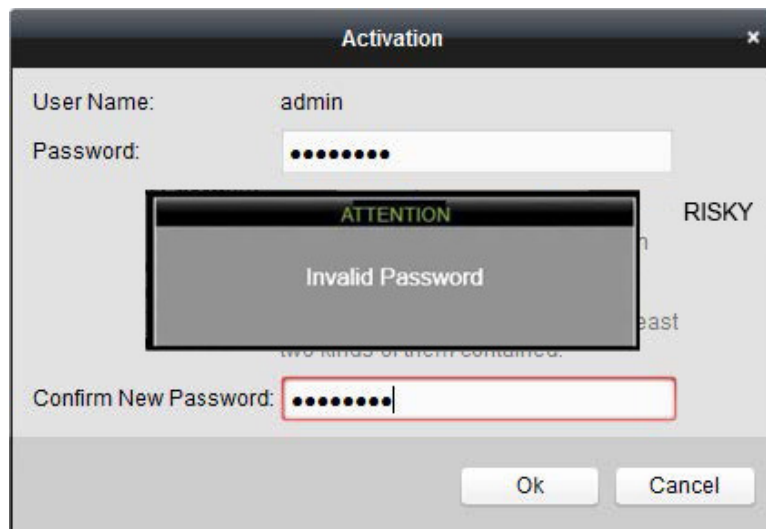


Figure 33, Invalid Password Message

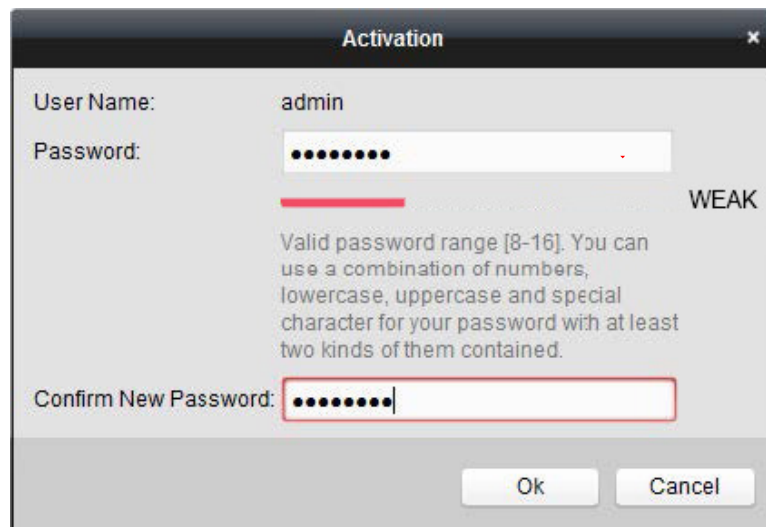


Figure 34, Level 1 Password Strength

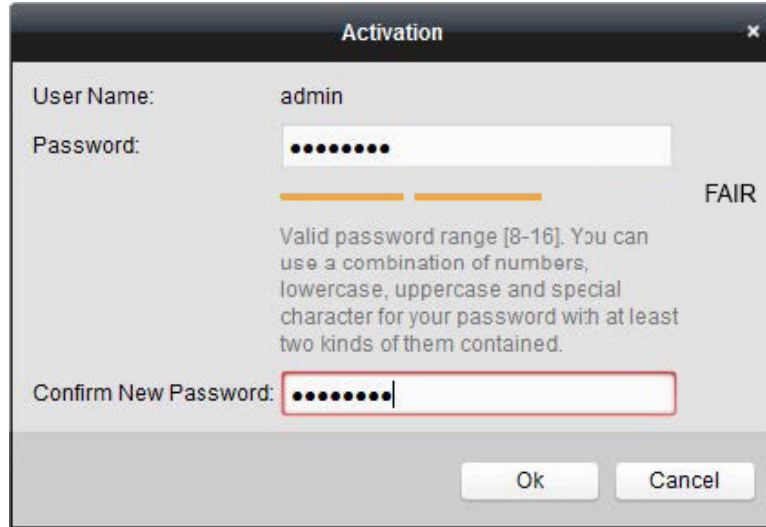


Figure 35, Level 2 Password Strength

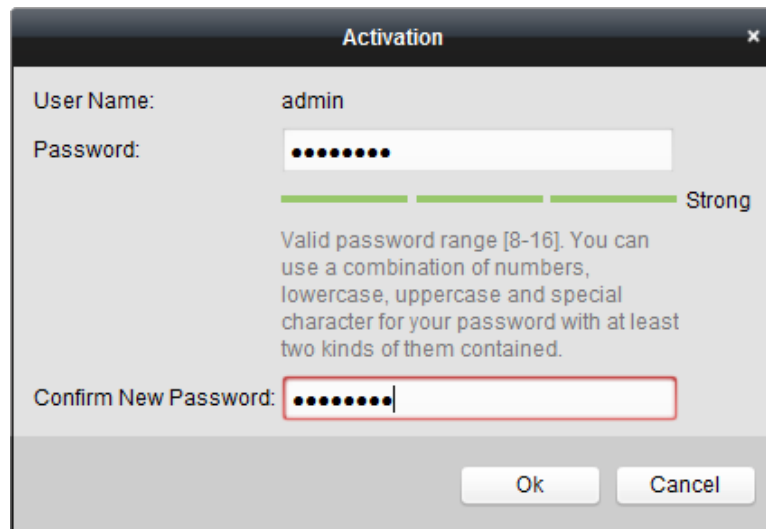


Figure 36, Level 3 and Level 4 Password Strength

 **WARNING**

STRONG PASSWORD RECOMMENDED – We highly recommend 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. Resetting the password monthly or weekly can better protect your product.

4. Click **OK** to finish activating the IP camera. The camera security status will change to **Active**.

2.6.2 Adding an Online IP Camera

Before using Live View or recording video, you must add the network cameras to the device connection list.

- **Before Starting**

Ensure the network connection is valid and correct.

- **OPTION 1**

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

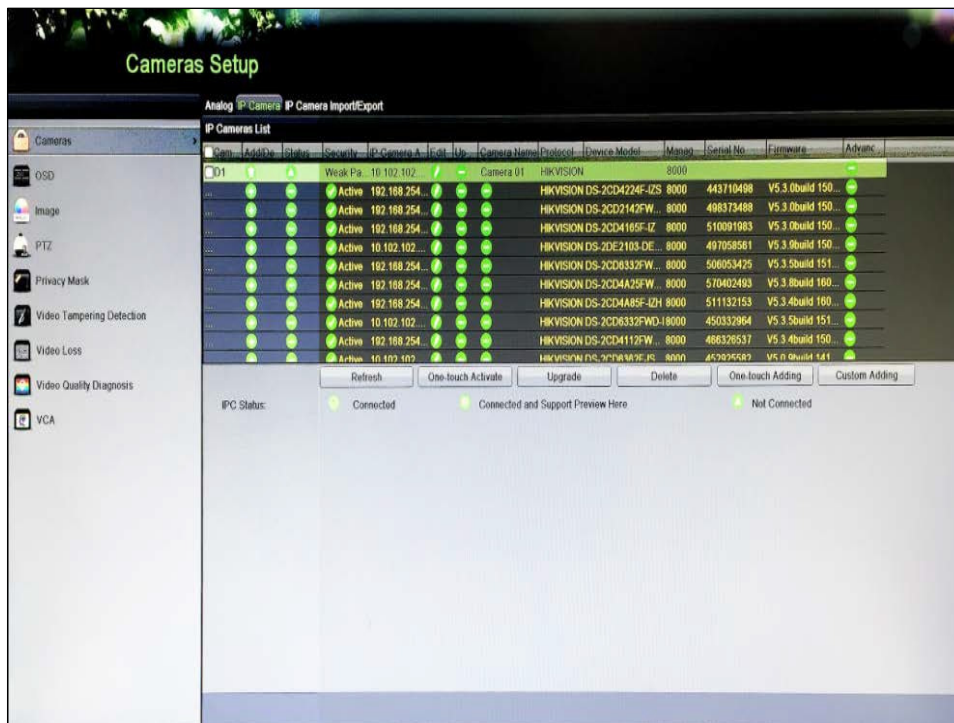



Figure 37, IP Camera Management Interface

2. Online cameras in the same network segment will be detected and displayed in the camera list.
3. Select the IP camera from the list and click  to add the camera (with the same admin password as the DVR), or click the **One-touch Adding** button to add all cameras (that have the same admin password) from the list.

Make sure the camera to add has already been activated by setting the admin password, and the admin password of the camera is the same as the DVR's.

4. (Optional) Check the **Enable H.265** checkbox (for initial access) for the connected IP camera supporting H.265. The IP camera will be encoded with H.265.

• **OPTION 2**

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

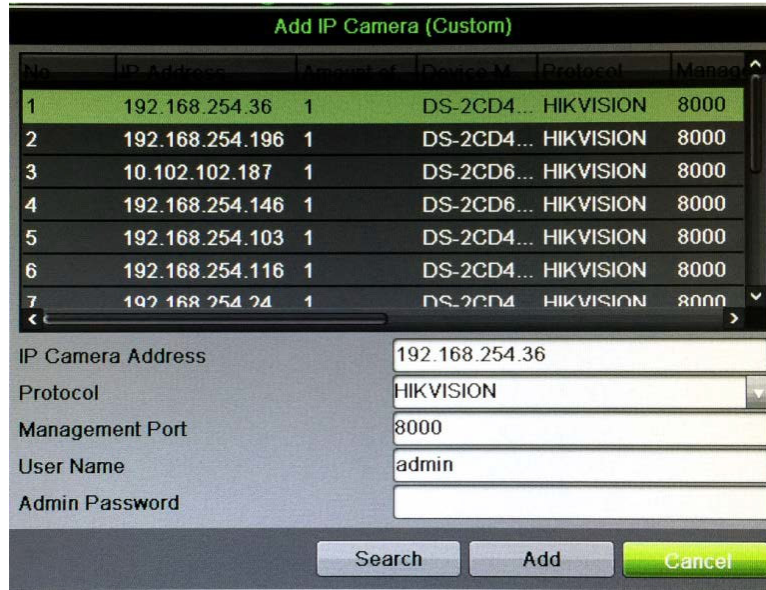


Figure 38, Custom Adding IP Camera Interface

2. You can edit the IP address, protocol, management port, and other information.

NOTE

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

3. Click **Add** to add the camera.










NOTE

For added IP cameras, the **Security** status shows the password security level.

Table 1-6 IP Cameras Supported

Camera Model	Number of IP Cameras Supported
DS-7204HQI-K1	1, up to 4 MP
DS-7208HQI-K2	2, up to 4 MP
DS-7216HQI-K2	
DS-7204HUI-K1	2, up to 6 MP
DS-7208HUI-K2	
DS-7216HUI-K2	

Table 1-7 Explanation of the Icons

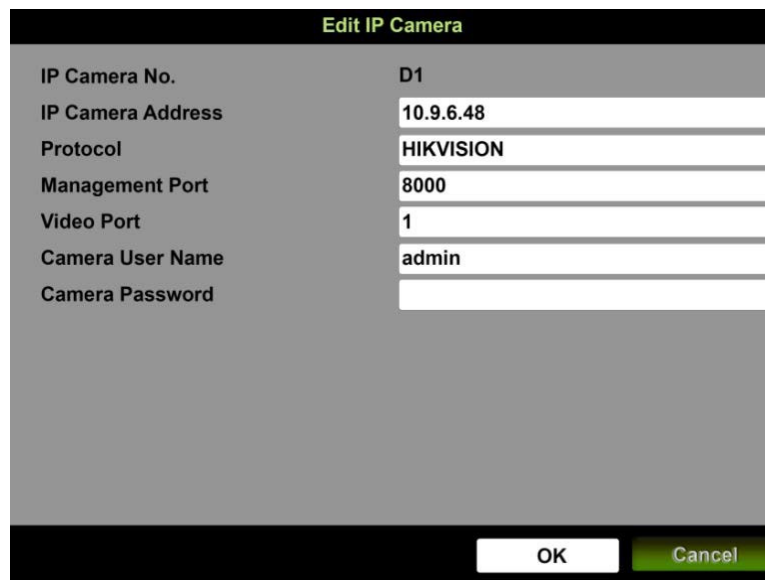
Icon	Explanation	Icon	Explanation
	EDIT (Pen): Press to edit basic IP camera parameters		ADD (+): Press to add the detected IP camera
	DISCONNECTED (!): Camera is disconnected; click the icon to get camera's exception information		DELETE (Trash Can): Press to delete the camera
	PLAY (Right Triangle): Play connected camera's live video		ADVANCED (Gear): Press to go to advanced settings window.
	UPGRADE (Up Arrow): Upgrade the connected camera's firmware		DASH: No advanced settings available for this camera
	REPAIR (?): Press to attempt to repair the connection	Security Column	SECURITY: Shows camera status (active/inactive) or password strength (strong/medium/weak/risky)

4. (Optional) Check the **Enable H.265** checkbox (for initial access) for a connected IP camera that supports H.265. The IP camera will be encoded with H.265.

2.6.3 Editing the Connected IP Camera

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

1. Click  to edit the parameters. You can edit the IP address, protocol, and other parameters.




The screenshot shows a dialog box titled "Edit IP Camera" with the following fields and values:

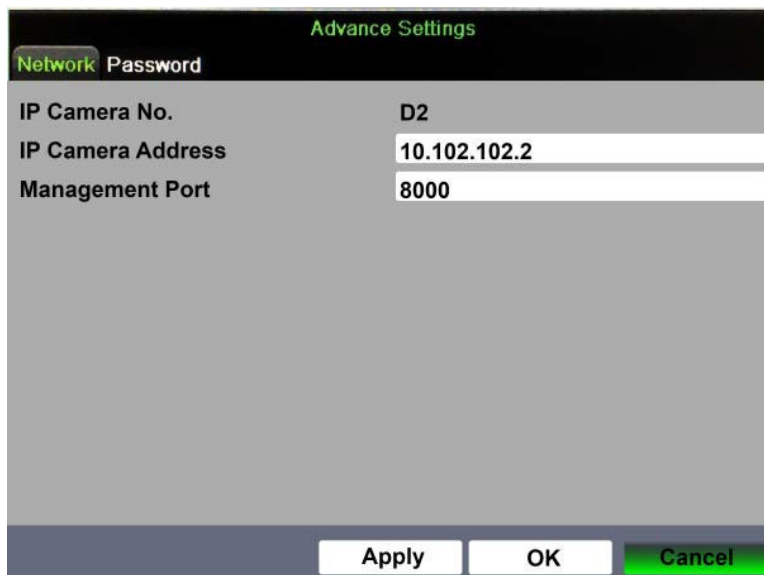
IP Camera No.	D1
IP Camera Address	10.9.6.48
Protocol	HIKVISION
Management Port	8000
Video Port	1
Camera User Name	admin
Camera Password	

At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

Figure 39, Edit IP Camera

- **Channel Port:** If the connected device is an encoding device with multiple channels, select the channel port No. in the drop-down list.
2. Click **OK** to save the settings and exit from the editing interface.

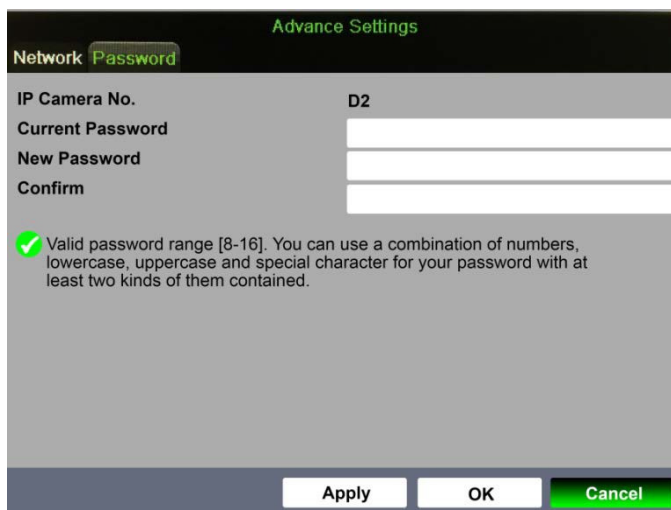
3. Drag the horizontal scroll bar to the right and click  to edit the advanced parameters.



The screenshot shows a dialog box titled "Advance Settings" with two tabs: "Network" (selected) and "Password". Under the "Network" tab, there are three input fields: "IP Camera No." with the value "D2", "IP Camera Address" with the value "10.102.102.2", and "Management Port" with the value "8000". At the bottom of the dialog, there are three buttons: "Apply", "OK", and "Cancel".

Figure 40, Network Configuration of the Camera

4. Edit the camera's network information and password.



The screenshot shows the same "Advance Settings" dialog box, but with the "Password" tab selected. The "IP Camera No." field still contains "D2". Below it are three empty input fields for "Current Password", "New Password", and "Confirm". A green checkmark is visible next to a text box that reads: "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, the "Apply", "OK", and "Cancel" buttons are present.

Figure 41, Password Configuration of the Camera

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

Chapter 3 Live View





3.1 Introduction

Live View shows real time video image from each camera. The DVR will automatically enter Live View mode when powered on. It is also at the very top of the menu hierarchy, thus hitting ESC many times (depending on which menu you're on) will bring you back to Live View mode.

3.1.1 Live View Icons

In Live View mode, icons at the right top of the screen for each channel show channel's record and alarm status, so that you can know if the channel is recorded or see alarms as soon as possible.

Table 1-1 Description of Live View Icons

Icons	Description
	Alarm (video loss, tampering, motion detection, VCA, or sensor alarm)
	Record (manual record, schedule record, motion detection, or alarm triggered record)
	Alarm & Record
	Event/Exception (motion detection, sensor alarm, or exception information. For details, see <i>Chapter 8.6 Handling Exceptions</i> .)

3.2 Operations in Live View Mode

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

- **Single Screen:** Show only one screen on the monitor.
- **Multi-screen:** Show multiple screens on the monitor simultaneously.
- **Start Auto-switch:** Screen is auto switched to next one; you must set dwell time for each screen on the configuration menu before enabling auto-switch (Menu > Configuration > Live View > Dwell Time).
- **Start Recording:** Normal record and motion detection record are supported.
- **Output Mode:** Set output mode to Standard, Bright, Gentle, or Vivid.
- **Playback:** Play back the recorded videos for current day.

- **For DS-72xxHUI-Kx Series DVRs with CVBS Output:** The VGA/HDMI output is the main output, and the CVBS output is the aux output. The priority relationship is shown as Table 3-2.

Table 1-2 Priorities of Outputs for DS-72xxHUI-Kx Series

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


 **NOTE**

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

When present the HDMI/VGA will provide the main monitor output with the CVBS serving only as a spot (Live View) monitor. If no HDMI or VGA monitor is connected at the time of bootup, the CVBS monitor can be used as the main monitor, allowing control of menu and playback. A reboot is required to return this function to the HDMI/VGA monitor(s).

3.2.1 Using the Mouse in Live View

Table 1-3 Mouse Operation in Live View

Name	Description
Menu	Enter the main menu of the system by right clicking the mouse.
Single Screen	Switch to the single full screen by choosing channel number from the drop-down list.
Multi-Screen	Adjust the screen layout by selecting 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.  NOTE Set the Live View configuration <i>dwel time</i> before using Start Auto-Switch .
Start Recording	Start recording of all channels, Continuous Record and Motion Detection Record are selectable from the drop-down list.
Add IP Camera	A shortcut to enter the IP camera management interface.(For HDVR series only)
Playback	Enter the playback interface and start playing back the video of the selected channel immediately.
PTZ Control	A shortcut to enter the PTZ control interface of the selected camera.
Output Mode	Output Mode is configurable with Standard, Bright, Gentle and Vivid options.

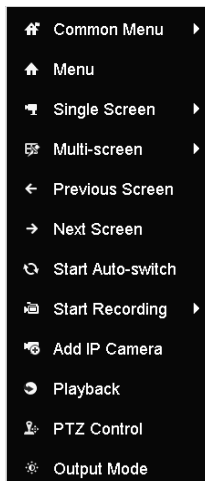


Figure 42, Right-click Menu

3.2.2 Switching Main/Aux Output



CVBS output serves only as aux output or Live View output.

1. Double click on the HDMI/VGA output screen, and the following message box pops up.

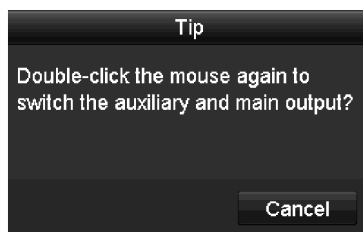


Figure 43, Switch Main and Aux Output

2. Double click on the screen again to switch to the aux output, or click **Cancel** to cancel the operation.
3. Select **Others** from the **Menu Output Mode** by right-clicking **Menu** on the monitor.
4. On the pop-up message box, click **Yes** to reboot the device to enable the selected menu output as the main output.



Select the **Menu Output Mode** under **Menu > Configuration > General > More Settings to Auto** and **HDMI/VGA** and then reboot the device to switch the main output.

3.2.3 Quick Setting Toolbar in Live View Mode

On each channel's screen, there is a quick setting toolbar that appears when you click the screen. See [Table 3-4](#) for the Quick Setting Toolbar icon descriptions.



Figure 44, Quick Setting Toolbar

Table 1-4 Description of Quick Setting Toolbar Icons

Icons	Description	Icons	Description	Icons	Description
	Start/Stop Manual Recording		Instant Playback		Audio On/Mute
	PTZ Control		Digital Zoom		Image Settings
	Close Live View		Face Detection		Information
	Capture		Live View Strategy		Information
	Fisheye				



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




Digital Zoom can zoom in the selected area to the full screen. Click and draw to select the area to zoom in.



Figure 45, Digital Zoom



Image Settings icon can be selected to enter the Image Settings menu. You can drag the mouse or click  to adjust the image parameters, including brightness, contrast, and saturation.

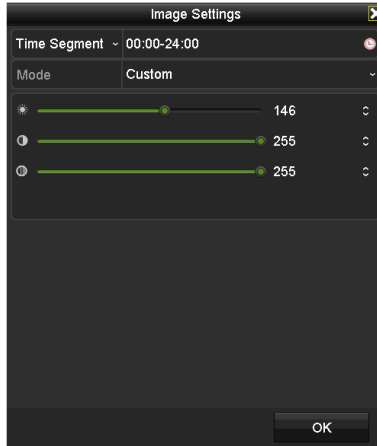


Figure 46, Image Settings




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



Figure 47, Enable Face Detection



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



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



When an H.264 IP camera is connected, the stream type is displayed as H.264. When an IP camera supporting H.264+ is connected, the stream type is displayed as H.264+. When an IP camera supporting H.265 is connected, the stream type is displayed as H.265. When an IP camera supporting H.265+ is connected, the stream type is displayed as H.265+.



For analog cameras supporting VCA, click the icon to show the VCA information. The configured line or quadrilateral in the VCA configuration and target frame(s) will be shown on Live View. Click the icon again to hide the VCA information.

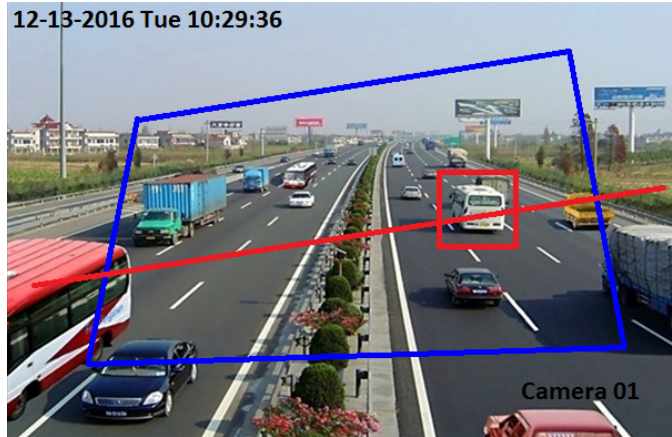


Figure 48, Enable VCA Information Overlay



NOTE

In Live View, only analog cameras support VCA information overlay.

Enable VCA function before showing the VCA information.

VCA information is hidden by default. If the connected analog camera does not support VCA, the icon displays grey and cannot be operated.

For analog cameras, the VCA information includes line crossing detection and intrusion detection.

The DVR supports VCA information overlay of only one channel. If you enable the function of one channel, the other channels will disable the function automatically.

Both single window and multi-window display modes support VCA information overlay.

Only the main output supports VCA information overlay. When switching to the aux output, the VCA information overlay of main output is disabled.

For the analog cameras, if the camera number does not exceed the limit for line crossing detection and intrusion detection, the VCA information overlay can be enabled for all the analog cameras with line crossing detection and intrusion detection. If the camera number exceeds the limit for line crossing detection, intrusion detection, and sudden scene change detection, only the cameras enabled line crossing detection and intrusion detection support VCA information overlay. Disabling line crossing detection and intrusion detection remotely will not affect the VCA information overlay in the local live view.

3.3 Channel-Zero Encoding

Channel-zero encoding provides a remote view of multiple channels in real time from a Web browser or CMS (Client Management System) software by decreasing the bandwidth requirement without affecting the image quality.

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

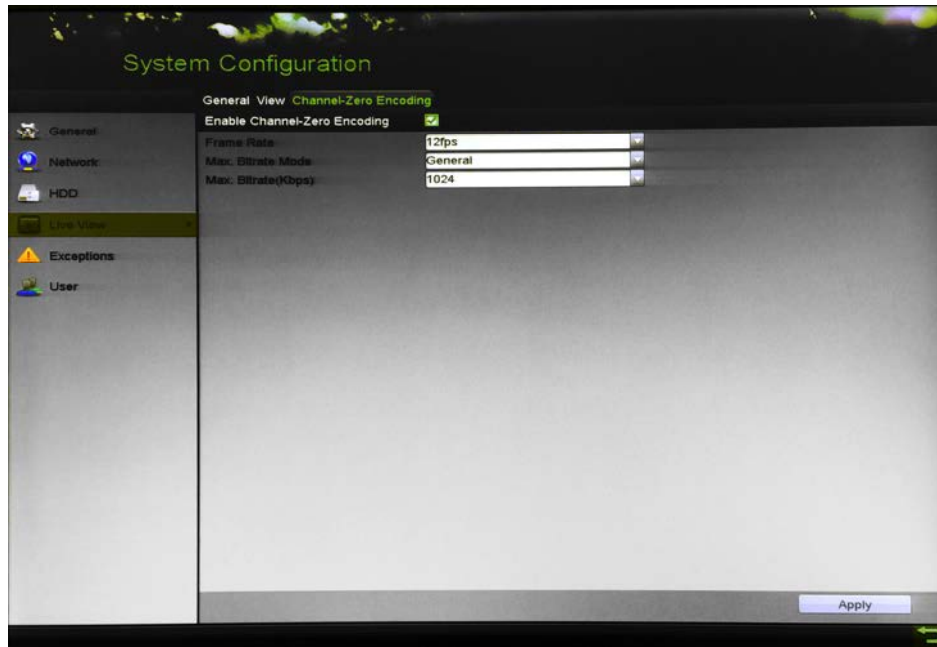


Figure 49, Live View Channel-Zero Encoding

3. Check the **Enable Channel-Zero Encoding** checkbox.
4. Configure the Frame Rate, Max. Bitrate Mode, and Max. Bitrate.
5. Click **Apply** to activate the settings.
6. After setting the Channel-Zero encoding, you can get a view in the remote client or Web browser of 16 channels on one screen.

3.4 Adjusting Live View Settings

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

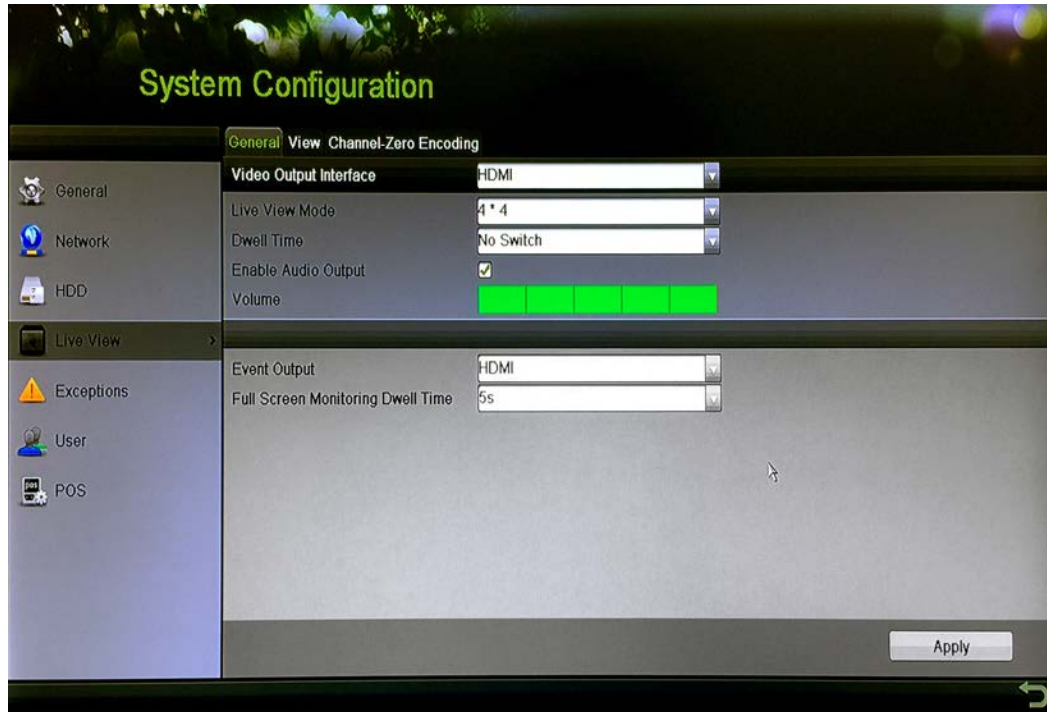






Figure 50, Live View – General

1. Enter the **Live View Settings** interface, Menu > Configuration > Live View > General. The settings available in this menu include:
 - **Video Output Interface:** Selects the output to configure the settings. You can select **Main CVBS** and **HDMI/VGA** for video output interface.
 - **Live View Mode:** Selects the display mode to be used for Live View.
 - **Dwell Time:** The time in seconds to *dwell* (pause) between switching of channels when enabling auto-switch in Live View.
 - **Enable Audio Output:** Enables/disables audio output for the selected camera in the live view mode.
 - **Volume:** Adjusts the volume of the audio output.
 - **Event Output:** Designates the output to show event video. If available, you can select a different video output interface from the Video Output Interface when an event occurs.
 - **Full Screen Monitoring Dwell Time:** Sets the time in seconds to show alarm event screen.



Figure 51, Live View > View Settings

2. Set the camera order.
 - a) Click the View tab and select the Video Output Interface from the drop-down list.
 - b) Click a window to select it, and then double click a camera name in the camera list you would like to display. Setting an “X” means the window will not display any camera.
 - c) You can also click  to start live view of all channels in order and click  to stop live view of all channels. Click  or  to go to the previous or next page.
 - d) Click **Apply**.

3.5 Manual Video Quality Diagnostics

The video quality of the analog channels can be diagnosed manually, and you can view the diagnostic results list.

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

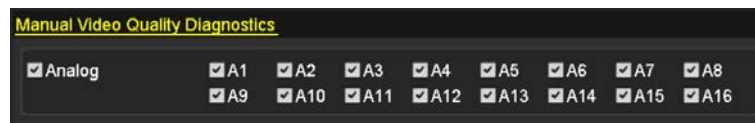


Figure 52, Manual Video Quality Diagnostics

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

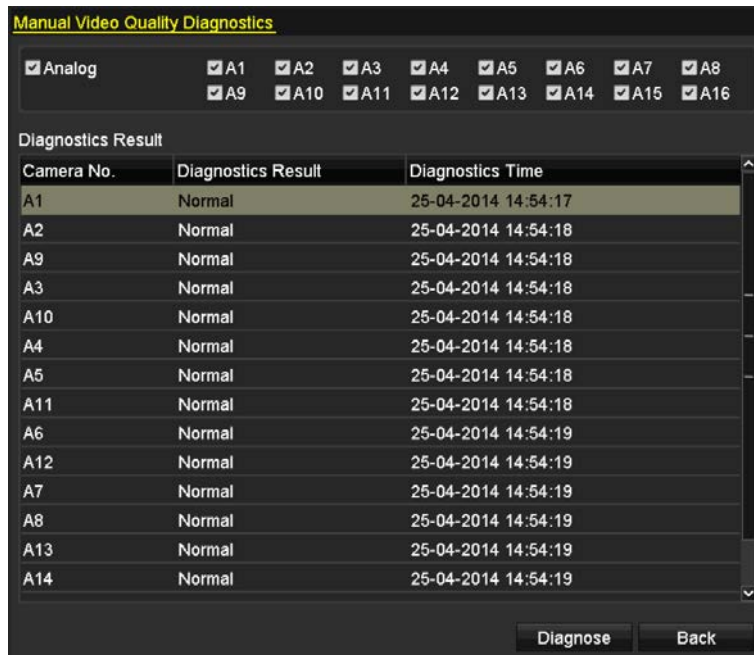


Figure 53, Diagnostics Result

 **NOTE**

Connect the camera to the device for the video quality diagnostics.

Three exception types can be diagnosed: Blurred Image, Abnormal Brightness, and Color Cast.

Chapter 4 PTZ Controls

4.1 Configuring PTZ Settings

Follow this procedure to set the PTZ parameters. Configure the PTZ parameters before controlling the PTZ camera.

1. Enter the **PTZ Settings** interface, Menu > Cameras Setup > PTZ.



Figure 54, PTZ Settings

2. Select the camera for PTZ setting in the Camera drop-down list.
3. Click **PTZ Parameters** to set the PTZ parameters.



Figure 55, PTZ – General

4. Select the PTZ camera parameters from the drop-down list.



NOTE

These parameters should be identical to the PTZ camera parameters.

For an Up-the-Coax camera/dome, select the UTC PTZ protocol. Make sure the protocol selected here is supported by the connected camera/dome.

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

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

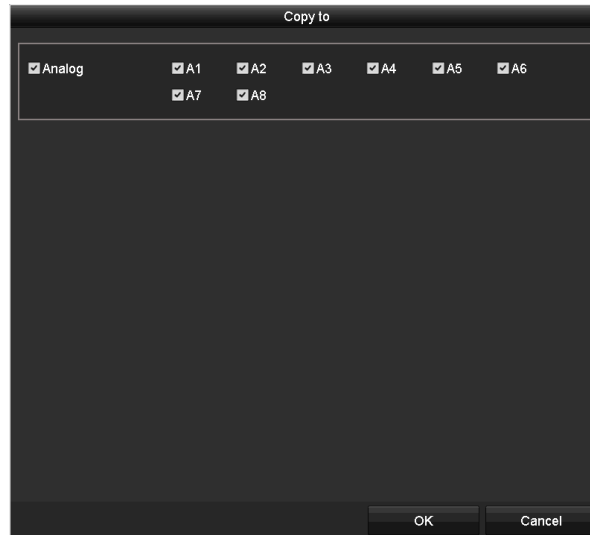


Figure 56, Copy to Other Channels

6. Click **OK** to save the settings.
7. (Optional) Check the **Enable Omnicast Control** checkbox to enable PTZ control of the selected camera via Omnicast VMS of Genetec.

4.2 Setting PTZ Presets, Patrols, and Patterns

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

4.2.1 Customizing Presets

Set the Preset location you want the PTZ camera to point to when an event takes place.

1. Enter the **PTZ Settings** interface, Menu > Cameras Setup > PTZ.



Figure 57, PTZ Settings


2. Use the directional button to move the camera to the location where you want to set the preset; the zoom and focus operations can be recorded in the preset as well.
3. Enter the preset No. (1 to 255) in the preset text field.
4. Click **Set** to link the location to the preset.
5. Repeat steps 2 and 3 to save more presets.



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

4.2.2 Calling Presets

This feature has the camera point to a specified location such as a window when an event occurs.

1. Perform **one** of the following actions to display the PTZ control panel:
 - Click **PTZ** in the lower-right corner of the PTZ setting interface.
 - Press **PTZ** on the front panel.
 - Click the PTZ Control icon  in the quick setting bar.
 - Select the PTZ option in the right-click menu.
2. Choose **Camera** in the drop-down list.
3. Click the **General** tab to show the PTZ control general settings.

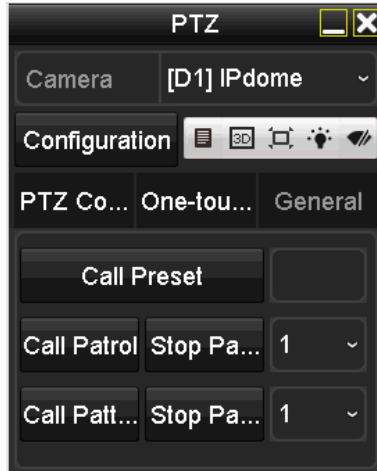


Figure 58, PTZ Panel – General

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



NOTE

When a UTC camera is connected and the PTZ protocol is set to UTC, you can call preset 95 to enter the UTC camera menu. Use the PTZ control panel directional buttons to operate the menu.

4.2.3 Customizing Patrols

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

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



Figure 59, PTZ Settings

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

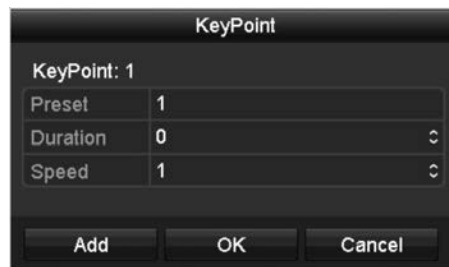


Figure 60, KeyPoint Configuration


4. Configure key point parameters.
 - **KeyPoint No.** determines the order the PTZ will follow while cycling through the patrol. KeyPoints correspond to the presets.
 - **Duration** is the time period to stay at the corresponding key point.
 - **Speed** defines the speed the PTZ will move from one key point to the next.
5. Click **Add** to add the next key point to the patrol, or click **OK** to save the key point to the patrol.



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

4.2.4 Calling Patrols

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

1. Perform **one** of the following actions to display the PTZ control panel:
 - Click **PTZ** in the lower-right corner of the **PTZ Settings** interface
 - Press **PTZ** on the front panel
 - Click the **PTZ** Control icon  in the quick setting bar
 - Select the **PTZ** option in the right-click menu to show the PTZ control panel
 1. Click the **General** tab to show the general settings of the PTZ control.

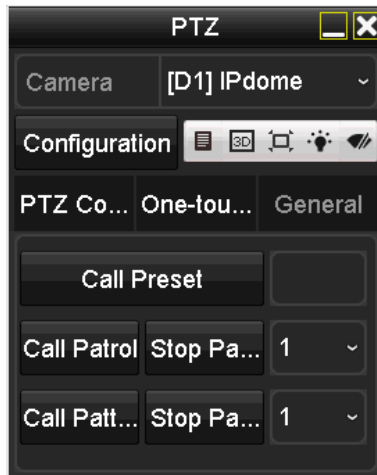


Figure 61, PTZ Panel – General

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

4.2.5 Customizing Patterns

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

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




Figure 62, PTZ Settings

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

4.2.6 Calling Patterns

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

1. Perform **one** of the following actions to display the PTZ control panel:
 - Click **PTZ** in the lower-right corner of the **PTZ Settings** interface.
 - Press **PTZ** on the front panel.
 - Click the PTZ Control icon  in the quick setting bar.
 - Select the PTZ option in the right-click menu.
2. Click the **General** tab to show the general settings of the PTZ control.

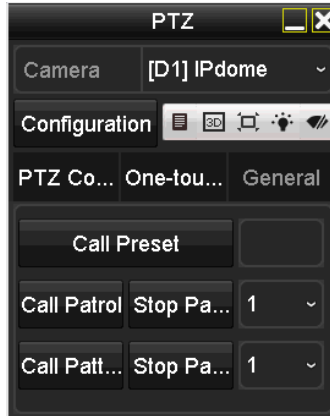


Figure 63, PTZ Panel – General

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

4.2.7 Customizing Linear Scan Limit

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



This function is supported by certain models.

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



Figure 64, PTZ Settings

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



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

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


1. Perform **one** of the following actions to display the PTZ control panel:
 - Click **PTZ** in the lower-right corner of the **PTZ Settings** interface.
 - Press **PTZ** on the front panel.
 - Click the PTZ Control icon  in the quick setting bar.
 - Select the PTZ option in the right-click menu.
2. Click the **One-touch** tab to show the one-touch function of the PTZ control.



Figure 65, PTZ Panel – One-Touch

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



Click **Restore** to clear the defined left right limit data. The dome needs to reboot for settings to take effect.

4.2.9 One-Touch Park

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


1. Perform **one** of the following actions to display the PTZ control panel:
 - Click **PTZ** in the lower-right corner of the **PTZ Settings** interface.
 - Press **PTZ** on the front panel.
 - Click the PTZ Control icon  in the quick setting bar.
 - Select the PTZ option in the right-click menu.
2. Click the **One-touch** tab to show the PTZ control one-touch function.



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 moving according to 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 be set only through the speed dome configuration interface. The default value is 5s.

4. Click the button again to de-activate 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 **PTZ** on the lower-right corner, next to the **Back** button.


- **OPTION 2**

In Live View mode:

- Press **PTZ Control** on the front panel.
- Press **PTZ Control** on the remote control.
- Choose the PTZ Control icon  in the quick setting bar.
- Select the PTZ Control option in the right-click menu.

1. Click **Configuration** on the control panel to enter the **PTZ Settings** interface.

 **NOTE**

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

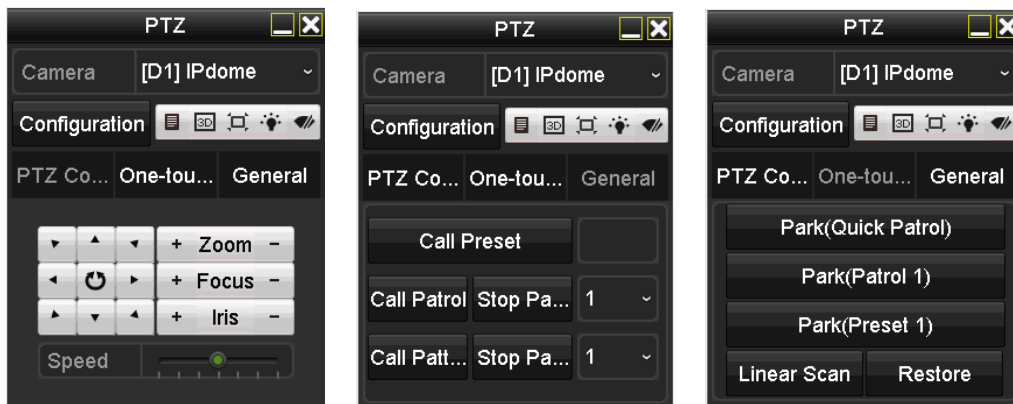
















Figure 67, PTZ Control Panel

Refer to Table 4-1 for the description of the PTZ panel icons.

Table 1-5 Description of the PTZ panel icons

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

Chapter 5 Recording Settings

5.1 Configuring Encoding Parameters

5.1.1 Before Starting

1. Make sure that the HDD has already been installed. If not, install and initialize an HDD (Menu > System Configuration > HDD).

Label	Capacity	Status	Property	Type	Free Space	Gro...	Edit	Delete
1	2794.52GB	Normal	R/W	Local	2613.00GB	1	-	-

Figure 68, HDD – General

2. Click **Advanced** tab to check the storage mode of the HDD (Menu > System Configuration > HDD > Storage Mode).
 - 1) If the HDD mode is Quota, set the maximum record capacity.
 - 2) If the HDD mode is Group, set the HDD group.

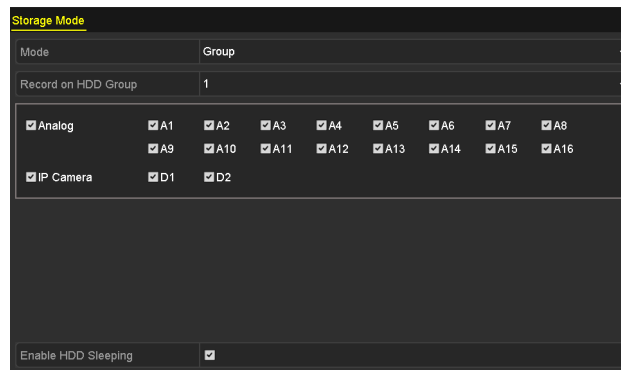


Figure 69, HDD – Advanced

5.1.2 Configure Record Parameters

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



Figure 70, Record Parameters

2. Set the parameters for recording.

- 1) Select the **Record** tab to configure.
- 2) Select a camera from the camera drop-down list.
- 3) View the Camera Resolution.

 **NOTE**

When TurboHD input is connected, you can view the information including the input signal type, resolution, and frame rate (e.g., 5 MP 20 Hz). When CVBS input is connected, you can view the information such as NTSC or PAL.

4) Configure the following parameters for the **Main Stream (Continuous)** and the **Main Stream (Event)**.

- **Stream Type:** Set the stream type to be Video or Video & Audio.
- **Resolution:** Set recording resolution.

 **NOTE**

DS-72xxHUI-Kx Series DVRs support 5 MP and 4 MP resolution on all channels.

DS-72xxHQI-Kx Series DVRs support up to 3 MP resolution for the first four channels.

Analog signal inputs (TurboHD, CVBS) and IP signal inputs can be recognized and connected automatically.

If the configured encoding resolution conflicts with the resolution of the front-end camera, the encoding parameters will adjust automatically to meet the front-end camera. E.g., if the resolution of the front-end camera is 720p, then the encoding resolution of the main stream will adjust to 720p automatically.

The 960 × 1080 (1080p Lite) resolution is available when 1080p Lite is enabled in the Record > Advanced Settings interface.

- **Bitrate Type:** Set the bitrate type to be Variable or Constant.
- **Video Quality:** Set the recording video quality, with six levels configurable.



NOTE

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

- **Frame Rate:** Set the frame rate of recording.



NOTE

For DS-72xxHQI-Kx Series DVRs, when a 3 MP signal input is connected, the main stream frame rate cannot exceed 15 fps.

For DS-72xxHUI-Kx Series DVRs, when a 5 MP signal input is connected, the frame rate of the main stream cannot exceed 12 fps. When 4 MP signal input is connected, the main stream frame rate cannot exceed 15 fps.

- **Max. Bitrate Mode:** Set the mode to General or Custom.
- **Max Bitrate (Kbps):** Select or customize the maximum bit rate for recording.
- **Max. Bitrate Range Recommended:** A recommended max. bit rate range is provided for reference.
- **Max. Average Bitrate (Kbps):** Set the max. average bit rate which refers to the average amount of data transferred per unit of time.
- **Video Encoding:** You can configure H.264 or H.265 for the main stream (continuous) of IP and analog cameras.



NOTE

When the connected IP camera does not support H.265, only H.264 can be selected for the main stream (continuous).

3. Check the **Enable H.264+** or **Enable H.265+** checkbox to enable this function. Enabling it helps to ensure high video quality with a lowered bitrate.



NOTE

For –K series DVRs, the analog and IP cameras support enabling H.264+/H.265+ if the video encoding is H.264/H.265 for the main stream.

After enabling H.264+ or H.265+, the Bitrate Type, Video Quality, Max. Bitrate Mode, Max. Bitrate(Kbps), and Max. Bitrate Range Recommend are not configurable.

If H.265+ is enabled, line crossing detection and region entrance detection are not supported.

For IP cameras, H.264+ or H.265+ should be supported by the camera and added to the DVR with HIKVISION protocol.

System will reboot to activate the new settings after enabling H.264+ or H.265+.

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



Figure 71, More Settings of Record Parameters

- **Pre-record:** The time to record before the scheduled time or event. For example, if an alarm triggers the recording at 10:00, if the pre-record time is 5 seconds, the camera starts recording at 9:59:55.
- **Post-record:** The time to record after the event or the scheduled time. For example, if an alarm triggers the recording to end at 11:00, if the post-record time is 5 seconds, it will record until 11:00:05.
- **Expired Time:** The time to keep the record files in the HDDs. Once exceeded, the files will be deleted. The files will be saved permanently if the value is set to 0. The actual keeping time for the files is determined by the capacity of the HDDs.
- **Redundant Record:** Enabling redundant record saves the record in the redundant HDD.
- **Record Audio:** Enable to record sound and disable it to record the video without sound.

- **Video Stream:** Main stream, Sub-stream, and Dual-stream are selectable for recording. If you select sub-stream, you can record for a longer time with the same storage space.



Redundant Record is available only when HDD mode is *Group*.

Redundant HDD is required for the redundant record function.

For network cameras, the Main Stream (Event) parameters are not editable.

5. Click **Apply** to save the settings.
6. (Optional) Click **Copy** to copy the settings to other analog channels if needed.

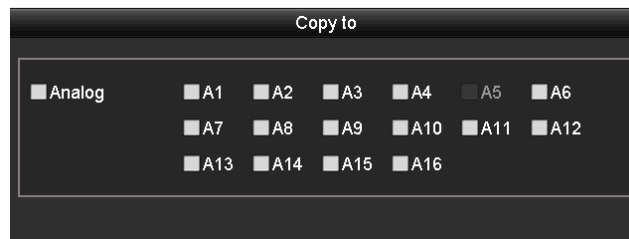


Figure 72, Copy Camera Settings

7. Set encoding parameters for sub-stream.

- 1) Select the **Sub-Stream** tab.

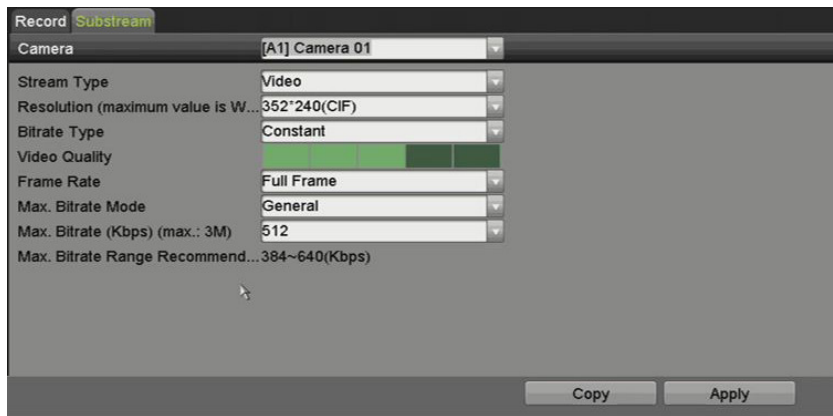


Figure 73, Sub-Stream Encoding

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

**NOTE**

You can select the **Video Encoding** for the IP sub-stream and analog cameras. For analog cameras, H.264 and H.265 are selectable. For IP cameras supporting H.265, you can select H.265 encoding mode.

5.2 Configuring Recording Schedule

**NOTE**

The –K series DVRs support continuous, alarm, motion, motion | alarm, motion & alarm, and event triggered recording types.

In this chapter, the record schedule procedure is used as an example; the same procedure can be applied to configure recording schedule.

5.2.1 Set the Record Schedule

Set the record schedule to have the camera automatically start/stop recording according to the configured schedule.

1. Enter the **Record Schedule** interface, Menu > Record > Schedule. Different recording types are marked in different color icons.

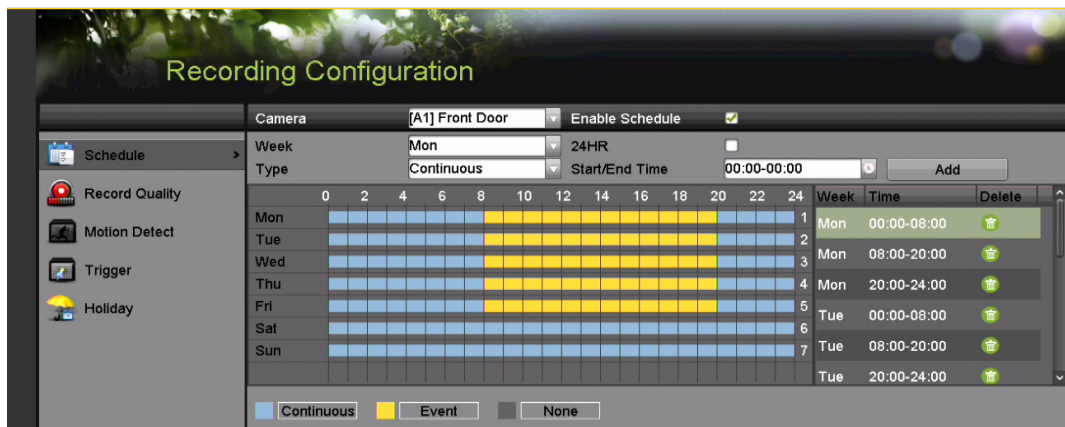


Figure 74, Record Schedule

- **Continuous:** Scheduled recording
 - **Event:** Recording triggered by event triggered alarm
2. Choose the camera you want to configure in the **Camera** drop-down list.
 3. Check the **Enable Schedule** checkbox.
 4. Configure the record schedule.

5.2.2 Edit the Schedule

1. Click **Edit**.
2. In the message box, choose the day to which you want to set the schedule.
3. To schedule an all-day recording, check the **All Day** checkbox.

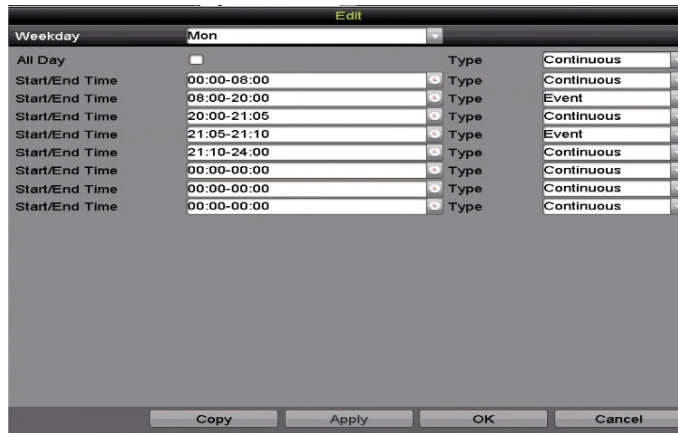


Figure 75, Edit Schedule – All Day

4. To set non-all day schedules, leave the **All Day** checkbox blank and set the Start/End times.

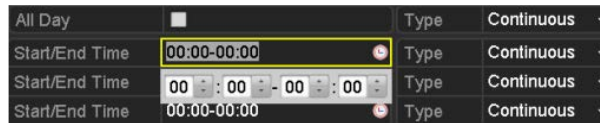


Figure 76, Edit Schedule – Set Time Period



NOTE

Up to eight periods can be configured for each day. Time periods cannot overlap.

To enable Event, Motion, Alarm, M | A (motion or alarm), and M & A (motion and alarm) triggered recording, you must configure the motion detection settings, alarm input settings, or VCA settings as well.

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

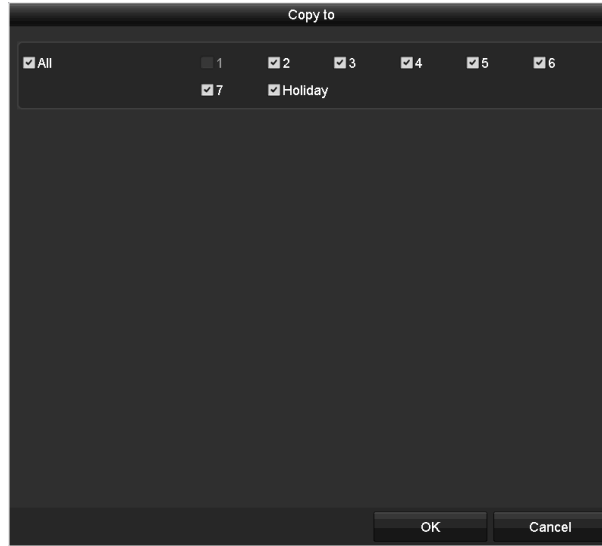


Figure 77, Copy Schedule to Other Days



NOTE

The **Holiday** option is available when you enable holiday schedule in **Holiday settings**.

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

5.2.3 Draw the schedule

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

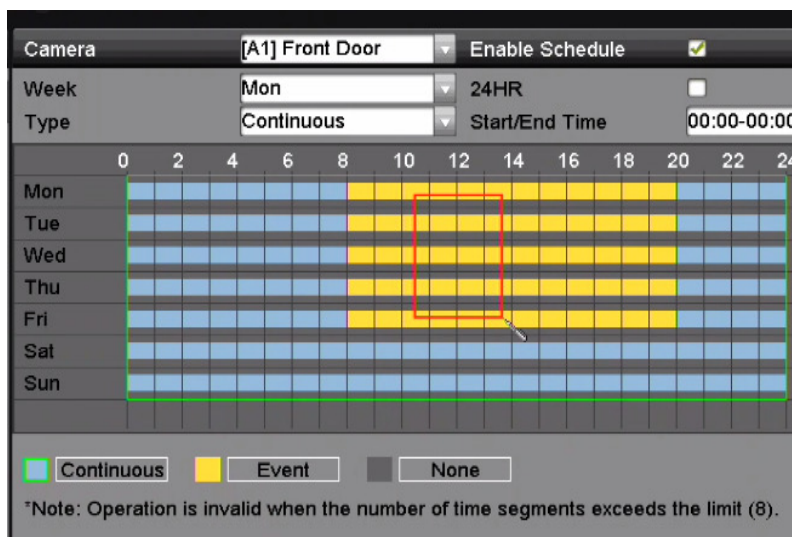


Figure 78, Draw the Recording Schedule

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

4. You can repeat step 3 to set schedule for other channels. If the settings can also be used for other channels, click **Copy**, and then choose the channel to which you want to copy to.
5. Click **Apply** in the **Record Schedule** interface to save the settings.

5.3 Configuring Motion Detection Recording

Follow the steps to set the motion detection parameters. In Live View mode, once a motion detection event takes place, the DVR can analyze it and perform many actions to handle it. Enabling the motion detection function can trigger specific channels to start recording or trigger full screen monitoring, activate an audio warning, notify the surveillance center, send e-mail, etc.

1. Enter the **Motion Detection** interface, Menu > Recording Configuration > Motion Detect.



Figure 79, Motion Detection

2. Configure Motion Detection.
 - a) Choose the camera you want to configure.
 - b) Check the **Enable Motion Detection** checkbox.
 - c) Use the mouse to drag and draw the area for motion detection. To set motion detection for the entire area shot by the camera, click **Full Screen**. To clear the motion detection area, click **Clear**.

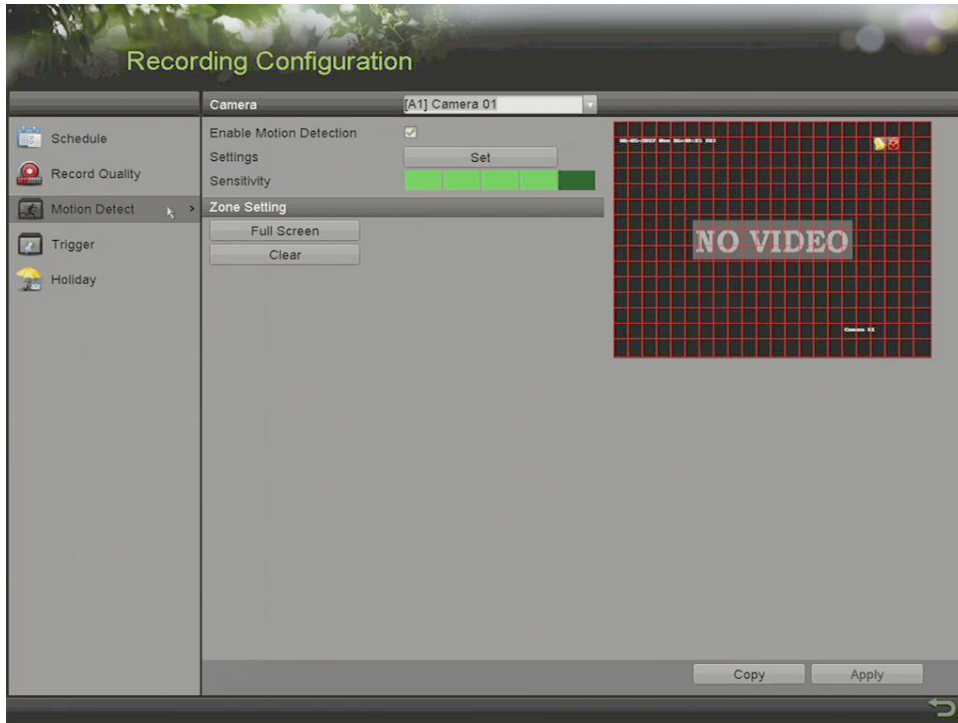


Figure 80, Motion Detection – Mask

- d) Click **Set** and the channel information message box pops up.

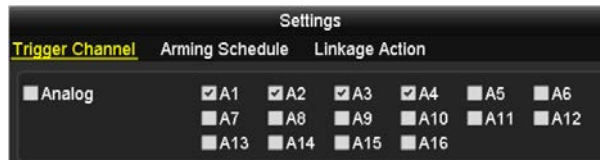


Figure 81, Motion Detection Settings

- e) Select the channels for which you want the motion detection event to trigger recording.
 - f) Click **Apply** to save the settings.
 - g) Click **OK** to go back to the upper level menu.
 - h) Exit the Motion Detection menu.
3. Configure the schedule (you may choose Motion as the record type).

5.4 Configuring Alarm Triggered Recording and Capture

Follow the procedure to configure alarm triggered recording or capture.

1. Enter the **Alarm Setting** interface, Menu > Recording Configuration > Trigger.



Figure 82, Alarm Settings

2. Click **Alarm Input** tab.
3. Select Alarm Input No.
4. Enter the Alarm Name.
5. Select **N.O.** (normally open) or **N.C.** (normally closed) for alarm type.
6. Check the **Enable** checkbox to enable alarm.
7. Click **Set** after **Settings** to set the triggered channels, arming schedule, linkage actions and PTZ linking.



Figure 83, Alarm Handling

8. Click **Apply** to save the settings.
9. Repeat steps 1 to 8 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

5.5 Configuring Event Recording

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).



NOTE

DS-72xxHUI-Kx Series DVRs support VCA (line crossing detection and intrusion detection) of all channels. Channels with audio support audio exception detection.

DS-7216HQI-Kx Series DVRs support 2-ch VCA (line crossing detection and intrusion detection). Channels with audio support audio exception detection.

For analog channels, line crossing detection and intrusion detection conflict with other VCA detection such as sudden scene change detection, face detection, and vehicle detection. Only one function can be enabled.

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. See step 6 in *Chapter 10.3 Line Crossing Detection*.
3. Click **Set** to configure the alarm linkage actions for the VCA events.
4. Click the **Trigger Channel** tab and select one or more channels to record when the VCA alarm is triggered.
5. Click **Apply** to save the settings.

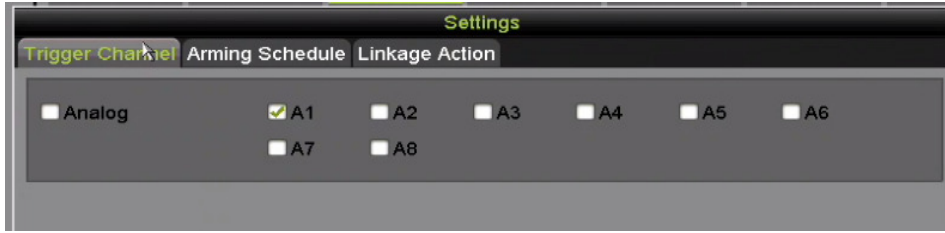


Figure 86, Set Triggered Camera of VCA Alarm

6. Enter **Record Schedule Settings** interface (Menu > Record > Schedule > Record Schedule), and then set Event as the record type.

5.6 Configuring Manual Recording

Follow these steps to set manual recording parameters. Manual recording is prior to scheduled recording.

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



Figure 87, Manual Record

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



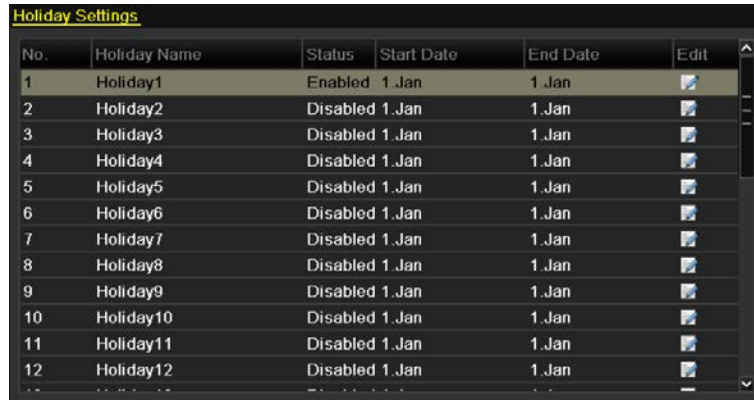
NOTE

After rebooting, all enabled manual records are canceled.

5.7 Configuring Holiday Recording

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

1. Enter the Record setting interface, Menu > Recording Configuration.
2. Choose **Holiday** on the left bar.



No.	Holiday Name	Status	Start Date	End Date	Edit
1	Holiday1	Enabled	1 .Jan	1 .Jan	
2	Holiday2	Disabled	1 .Jan	1 .Jan	
3	Holiday3	Disabled	1 .Jan	1 .Jan	
4	Holiday4	Disabled	1 .Jan	1 .Jan	
5	Holiday5	Disabled	1 .Jan	1 .Jan	
6	Holiday6	Disabled	1 .Jan	1 .Jan	
7	Holiday7	Disabled	1 .Jan	1 .Jan	
8	Holiday8	Disabled	1 .Jan	1 .Jan	
9	Holiday9	Disabled	1 .Jan	1 .Jan	
10	Holiday10	Disabled	1 .Jan	1 .Jan	
11	Holiday11	Disabled	1 .Jan	1 .Jan	
12	Holiday12	Disabled	1 .Jan	1 .Jan	

Figure 88, Holiday Settings

3. Enable Edit Holiday schedule.
4. Click to enter the Edit interface.



Edit

Holiday Name:

Enable:

Mode:

Start Date:

End Date:

Figure 89, Edit Holiday Settings

5. Check the **Enable** checkbox

6. Select **Mode** from the drop-down list.

There are three different modes for the date format to configure holiday schedule. By Month, By Week, and By Date are selectable.

7. Set the start and end dates.
8. Click **Apply** to save settings.
9. Click **OK** to exit the Edit interface.
10. Configure the record schedule.

Choose Holiday in the Schedule drop-down list or draw the schedule on the Holiday timeline.

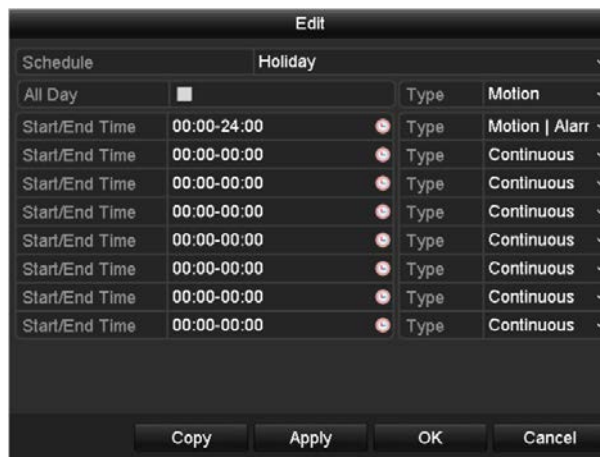


Figure 90, Edit Schedule – Holiday



NOTE

Up to eight periods can be configured for each day. Time periods cannot overlap each other.

In the channel time table, both holiday schedule and normal day schedule are displayed.

Repeat step 4 above to set Holiday schedule for other channels. If the holiday schedule can also be used for other channels, click **Copy** and choose the channel you want to apply the settings.

5.8 Configuring Redundant Recording

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

You must set the Storage mode in the HDD advanced settings to *Group* before you set the HDD property to Redundant. There should be at least another HDD that is in Read/Write status.

1. Enter the HDD Information interface, Menu > System Configuration > HDD.

<input type="checkbox"/>	Label	Capacity	Status	Property	Type	Free Space	Group	Edit	Delete
<input type="checkbox"/>	1	931.51GB	Normal	R/W	Local	865GB	1		-
<input type="checkbox"/>	3	931.51GB	Normal	R/W	Local	931GB	1		-

Figure 91, HDD General

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

Local HDD Settings

HDD No. 1

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

Figure 92, HDD General – Editing

4. Click **Apply** to save the settings.
5. Click **OK** to go back to the upper level menu.
6. Enter the Record setting interface, Menu > Record > Parameters.
7. Select the **Record** tab.
8. Select the Camera you want to configure.
9. Click the **More Settings** button.



Figure 93, More Settings

10. Check the **Redundant Record** checkbox.
11. Click **OK** to save the settings.
12. If the encoding parameters can also be used to other channels, click **Copy** and choose the channel to apply the settings to.

5.9 Configuring HDD Group

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

1. Enter HDD setting interface, Menu > System Configuration > HDD.
2. Select Storage Mode tab.


Check whether the storage mode of the HDD is Group. If not, set it to Group.
3. Select **General** in the left bar.
4. Click  to enter editing interface.
5. Configuring HDD group.
6. Choose a group number for the HDD group.
7. Click **Apply** to save your settings.
8. Click **OK** to go back to the upper level menu.
9. Repeat the above steps to configure more HDD groups.
10. Choose the Channels for which you want to save the record files in the HDD group.
11. Enter **Storage Mode** interface, Menu>HDD>Advanced> Storage Mode.



Figure 94, HDD Advanced

12. Choose Group number in the drop-down list of **Record on HDD Group**
13. Check the channels you want to save in this group.
14. Click **Apply** to save settings.



After configuring the HDD groups, configure the recording settings.

5.10 Files Protection

Lock the recorded files or set the HDD property to Read Only to protect the files from being overwritten.

5.10.1 Protect File by Locking the Record Files

1. Enter **Export Settings** interface, Menu > File Management.

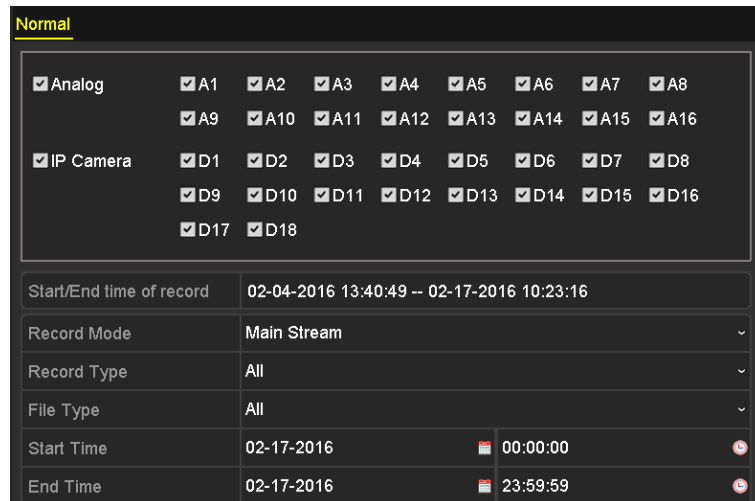




Figure 95, Export

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





Figure 96, Export – Search Result

5. Protect the record files.

- 1) Click the List tab to display the files in list view.
- 2) Find the record files you want to protect, and then click the  icon which will turn to , indicating that the file is locked.



Uncompleted record files cannot be locked.

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

5.10.2 Protect File by Setting HDD Property to Read-Only

To edit HDD property, you need to set the storage mode of the HDD to Group.

1. Enter HDD setting interface, Menu > System Configuration > HDD.

Label	Capacity	Status	Property	Type	Free Space	Group	Edit	Delete
1	931.51GB	Normal	R/W	Local	865GB	1		-
3	931.51GB	Normal	R/W	Local	931GB	1		-

Figure 97, HDD General


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



Figure 98, HDD General – Editing

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



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

If there is only one HDD and is set to Read-only, the DVR cannot record any files. Only live view mode is available.

If you set the HDD to Read-only when the DVR is saving files in it, then the file will be saved in next R/W HDD. If there is only one HDD, the recording will be stopped.

5.11 One-Key Enabling and Disabling H.264+/H.265+ for Analog Cameras

For –K series DVRs, you can one-key enable or disable H.264+/H.265+ for the analog cameras.

5.11.1 One-Key Enabling H.264+/H.265+ All Analog Cameras

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



Figure 99, Advanced Settings

3. Click **Enable** to enable H.264+/H.265+ for all the analog cameras and the following attention box pops up.

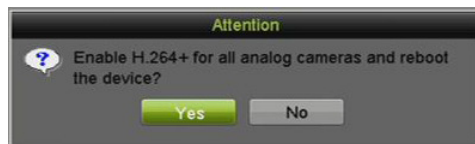


Figure 100, Attention Box

4. Click **Yes** to enable the function and reboot the device to have new settings taken effect.

5.11.2 One-Key Disabling H.264+/H.265+ All Analog Cameras

1. Enter the **Record** menu, Menu > Record.
2. Click **Advanced** to enter the advanced interface.
3. Click **Disable** to disable H.264+ for all the analog cameras and the following attention box pops up.



Figure 101, Attention Box

4. Click **Yes** to enable the function and reboot the device to have new settings taken effect.

5.12 Configuring 1080p Lite

When 1080p Lite Mode is enabled, 1080p Lite (real-time) encoding resolution is supported. If not, up to 1080p (non-real-time) is supported.



This chapter is applicable to DS-72xxHQI-Kx Series DVRs.

5.12.1 Enabling 1080p Lite Mode

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

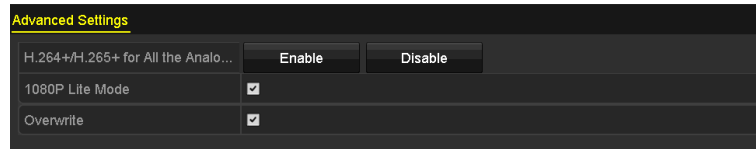


Figure 102, Advanced Interface

3. Check the **1080P Lite Mode** checkbox and click **Apply** to pop up the attention box. After enabling 1080p Lite Mode, the 3 MP signal is not accessible by analog channels.

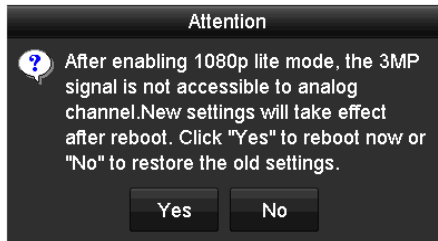


Figure 103, Attention

4. Click **Yes** to reboot the device to have new settings taken effect.

5.12.2 Disabling the 1080p Lite Mode

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



Figure 104, Attention

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


Chapter 6 Playback

6.1 Playing Back Record Files

6.1.1 Instant Playback

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

6.1.1.1 Instant Playback by Channel

Choose a channel in live view mode and click  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 105, Instant Playback Interface

6.1.1.2 Playing Back by Normal Search

- **Playback by Channel**

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

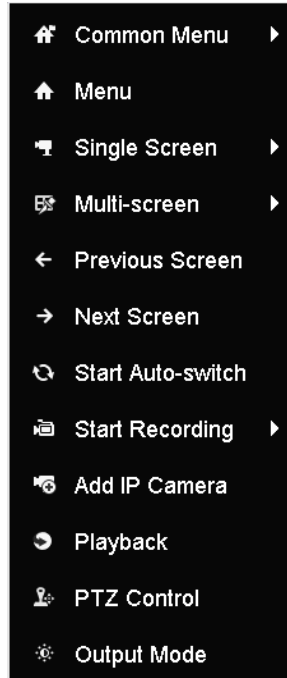


Figure 106, Right-click Menu Under Live View

- **Playback by Time**



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



Figure 107, Playback Calendar

 **NOTE**

If there are record files for that camera on that day, the calendar icon for that day is displayed as . Otherwise, it is displayed as .

- **Playback Interface**

Select the main stream or sub-stream from the drop-down playback list.

You can also use the toolbar in the bottom of the **Playback** interface to control playing progress, as shown in the following figure.



Figure 108, Playback Interface

Select the channel(s) if you want to switch playback to another channel or execute simultaneous playback of multiple channels.



Figure 109, Playback Toolbar

Table 1-8 Detailed Explanation of Playback Toolbar

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



NOTE

The **01-01-2015 00:00:23 – 14-07-2015 16:10:27** indicates the start time and end time of the record files.

- represents normal recording (manual or schedule).
- represents event recording (motion, alarm, motion | alarm, motion & alarm).

Playback progress bar: use the mouse to click any point of the progress bar to locate special frames.

• **Playing Back by Event Search**

Play back record files on one or several channels searched out by restricting event type (motion detection, alarm input or VCA). Channel switch is supported.

1. Enter the **Playback** interface, Menu > Playback.
2. Click **Normal** and select **Event** to enter the **Event Playback** interface.
3. Select **Alarm Input**, **Motion**, **VCA** as the event type, and specify the start time and end time for search.

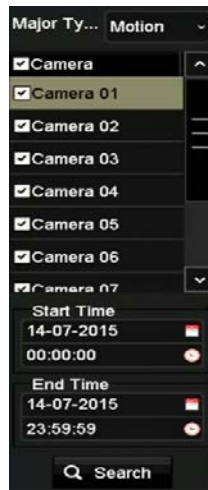



Figure 110, Video Search by Motion Detection


4. Click **Search**, and the record files matching the search conditions will be displayed on a list.
5. Select and click button to play back the record files.



NOTE

Click **Back** to return to the search interface.

If there is only one channel triggered, clicking  takes you to the **Full-screen Playback** interface of this channel.

If several channels are triggered, clicking  takes you to the **Synchronous Playback** interface. Check the checkbox to select one channel for playback or select multiple channels for synchronous playback.

The maximum number of channels for synchronous playback supported varies by model.



Figure 111, Select Channels for Synchronous Playback ????????

6. On the **Event Playback** interface, select main stream or sub-stream from the drop-down playback list.



Use the toolbar in the bottom of the **Playback** interface to control the playing process.





Figure 112, Playback by Event Interface

Pre-play and post-play can be configured for playing back event triggered record files.

Pre-play: The time to play back before the event. For example, if an alarm triggered the recording at 10:00, if the pre-play time is 5 seconds, the video will start play back at 9:59:55.

Post-play: The time to play back after the event. For example, if an alarm triggered recording ends at 11:00, if the post-play time is 5 seconds, the video plays until 11:00:05.

1. Click  or  to select the previous or next event. Refer to Table 6-1 for the description of buttons on the toolbar.



- **Playing Back by Tag**

Video tag allows you to record related information such as people and location of a certain time point during playback. You can also use video tag(s) to search for record files and position the time point.

1. Enter Playback interface, Menu > Playback.
2. Search and play back record file(s).



Figure 113, Playback by Time Interface

3. Click  to add default tag.
4. Click  to add customized tag and input tag name.

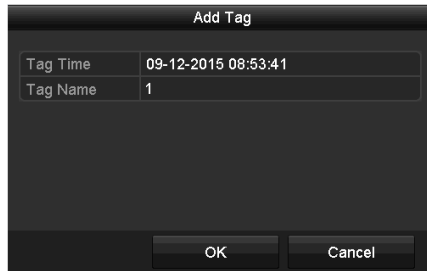


Figure 114, Add Tag

 **NOTE**

A maximum of 64 tags can be added to a single video file.

- **Tag Management**


1. Click the  button to check, edit, and delete tag(s).



Figure 115, Tag Management Interface

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



NOTE

Enter a keyword in the textbox to search the tag on your command.



Figure 116, Video Search by Tag



4. Click to play back the file.



NOTE

Can click **Back** to return to the search interface.

Pre-play and post-play can be configured.

Click  or  to select the previous or next tag. Refer to Table 6-1 for the description of toolbar buttons.

- **Playing Back by Smart Search**

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

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

1. Log in to the IP camera by the Web browser and enable intrusion detection by checking the checkbox. Enter the motion detection configuration interface by going to Configuration > Advanced Configuration > Events > Intrusion Detection.



Figure 117, Setting Intrusion Detection on IP Camera

2. Configure the required intrusion detection parameters, including area, arming schedule, and linkage methods. Refer to the smart IP camera user manual for detailed instructions.
3. Enter the Playback interface, Menu > Playback.
4. Select **Smart** in the drop-down list on the top-left side.
5. Select a camera in the camera list.



Figure 118, Smart Playback Interface

















6. Select a date on the calendar, and click the  button to play.

Table 1-9 Detailed Explanation of Smart Playback Toolbar

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

7. Set the rules and areas for VCA event or motion event smart search.

- **Line Crossing Detection** – Select , and click on the image to specify the start point and end point of the line.
- **Intrusion Detection** – Click , and specify four points to set a quadrilateral region for intrusion detection. Only one region can be set.




- **Motion Detection** – Click  and then click and draw the mouse to set the detection area manually. You can also click  to set the full screen as the detection area.
8. Click  to configure the smart settings.



Figure 119, Smart Settings

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

 **NOTE**

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



9. Click  to search and play the matched video files.
10. (Optional) 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 120, Set Result Filter

 **NOTE**

The Result Filter function is supported only by IP cameras.

11. (Optional) For cameras supporting VCA, click  to show the VCA information.

NOTE

The configured line or quadrilateral in VCA configuration and target frame(s) will be shown on the playback interface. Click  to hide the VCA information.

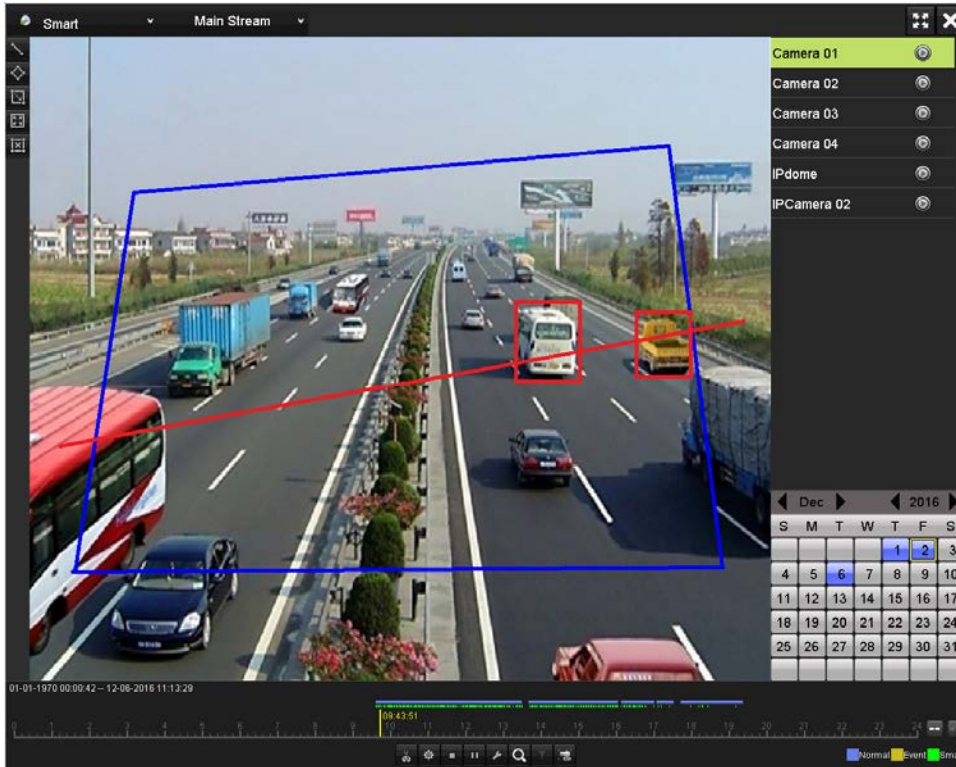


Figure 121, Show VCA Information

NOTE

This function is supported by DS-7200HUI-Kx Series DVRs.

In Smart Playback, both analog and IP cameras support VCA information overlay.

If the connected camera does not support VCA, the icon is grey and unavailable.

For analog cameras, the VCA information includes line crossing detection and intrusion detection. For IP cameras, the VCA information includes all the VCA detections of smart IP cameras.

- **Playing Back by System Logs**

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

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

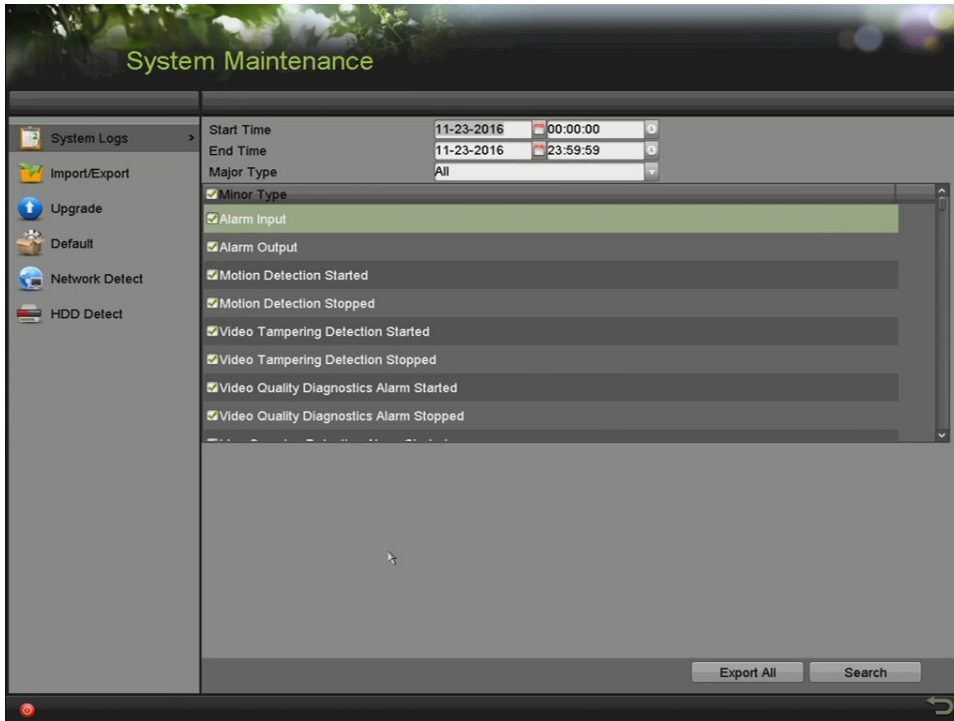



Figure 122, System Log Search Interface

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

No.	Major Type	Time	Minor Type	Parameter	Play	Details
1	Information	10-07-2015 09:53:59	Local HDD Infor...	N/A	—	✓
2	Operation	10-07-2015 09:53:59	Power On	N/A	—	✓
3	Information	10-07-2015 09:54:05	Start Recording	N/A	⏮	✓
4	Operation	10-07-2015 09:54:08	Local Operation:...	N/A	—	✓
5	Information	10-07-2015 09:54:25	HDD S.M.A.R.T.	N/A	—	✓
6	Information	10-07-2015 09:54:32	Start Recording	N/A	⏮	✓
7	Operation	10-07-2015 09:54:32	Local Operation:...	N/A	⏮	✓
8	Operation	10-07-2015 09:54:32	Local Operation:...	N/A	⏮	✓
9	Exception	10-07-2015 09:55:32	IP Camera Disco...	N/A	⏮	✓
10	Information	10-07-2015 10:04:09	System Running...	N/A	—	✓

Total: 1690 P: 1/17

Figure 123, Result of System Log Search

5. 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.

- **Playback Management**

Use the toolbar at the bottom of the Playback interface to control the playing process.



Figure 124, Interface of Playback by Log

- **Playing Back by Sub-Periods**

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

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



Figure 125, Interface of Sub-periods Playback

 **NOTE**

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


- **Playing Back External File**

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

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

 **NOTE**

The files are listed in the right-side list.

Click  Refresh to refresh the file list.

3. Select and click  to play it back.




Figure 126, Interface of External File Playback

6.2 Playback Auxiliary Functions

6.2.1 Playing Back Frame-by-Frame

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

1. Go to Playback interface and click  until the speed changes to *Single* frame.

2. One click on the playback screen represents playback or adverse playback of one frame. You can use  in the toolbar to stop the playing.

6.2.2 Digital Zoom


1. Click  on the playback control bar to enter Digital Zoom interface.
2. Use the mouse to draw a red rectangle, and the image within it will be enlarged up to 16 times.



Figure 127, Draw Area for Digital Zoom

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


6.2.3 Reverse Playback of Multi-Channel

You can play back record files of multi-channel reversely. Up to 16-ch simultaneous reverse playback is supported.

1. Enter Playback interface, Menu > Playback.
2. Check more than one checkbox to select multiple channels, and click to select a date on the calendar.



4-ch Synchronous Playback Interface

3. Click  to play back the record files reversely.

Chapter 7 Backup

7.1 Backing up Record Files

Insert the backup device(s) into the device.

7.1.1 Backing Up by Normal Video/Picture Search

The record files or pictures can be backed up to various devices such as USB devices (USB flash drives, USB HDDs, USB writer).

- **Backup Using USB Flash Drives and USB HDDs**
 1. Enter Export interface, Menu > File Management.
 2. Select the type of files to search.
 - Record
 - Event
 3. Select the cameras to search.
 4. Set search condition and click **Search** to enter the search result interface.

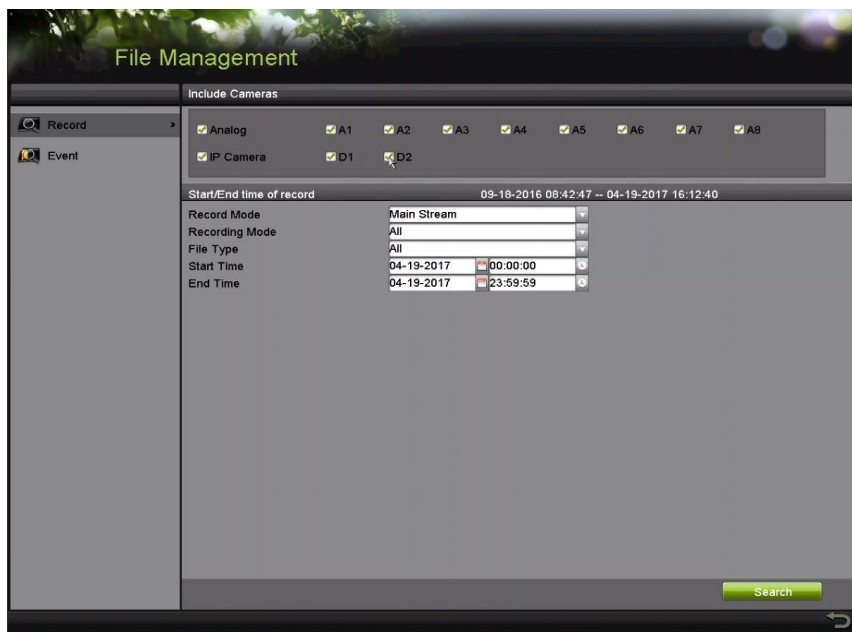



Figure 128, Normal Video Search for Backup

5. The matched video files are displayed in **Chart** or **List** display mode.
6. Click  to play the record file if you want to check it.

7. Check the checkbox next to the video files you want to back up.



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



Figure 129, Result of Normal Video Search for Backup

8. Select video files from the **Chart** or **List** to export
9. Click **Export** to enter the **Export** interface.



You can also click **Export All** to select all the video files for backup and enter the **Export** interface.



Figure 130, Export by Normal Video Search Using USB Flash Drive

10. Select the backup device from the drop-down list (you can also select the file format to filter the files existing in the backup device).
11. Select the saved file format type.
12. Click **Export** on the Export interface to start the backup process.
13. On the pop-up message box, click the radio button to export the video files, log, or the player to the backup device.
14. Click **OK** to confirm.



Figure 131, Select File or Player for Backup

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



Figure 132, Export Finished

NOTE

Backing up pictures using a USB writer has the same operating instructions. Refer to steps described above.

7.1.2 Backing Up Video Clips

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




1. Enter **Playback** interface.
2. During playback, use  or  in the playback toolbar to start or stop clipping record file(s).
3. Click  to enter the file management interface.



Figure 133, Video Clips Export Interface

4. Export the video clips in playback. See step 5 of Chapter 7.1.1 Backing Up by Normal Video/Picture Search for details.

7.2 Managing Backup Devices

7.2.1 Management of USB Flash Drives, and USB HDDs

1. Enter the **Export** interface.



Figure 134, Storage Device Management

2. Backup device management.

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

NOTE

If the inserted storage device is not recognized:

- Click **Refresh**.
- Reconnect device.
- Check vendor for compatibility.

Chapter 8 Alarm Settings

8.1 Setting Motion Detection

1. Enter **Motion Detection** interface of Camera Management, Menu > Recording Configuration > Motion Detect.
2. Choose a camera for which you want to set up motion detection,

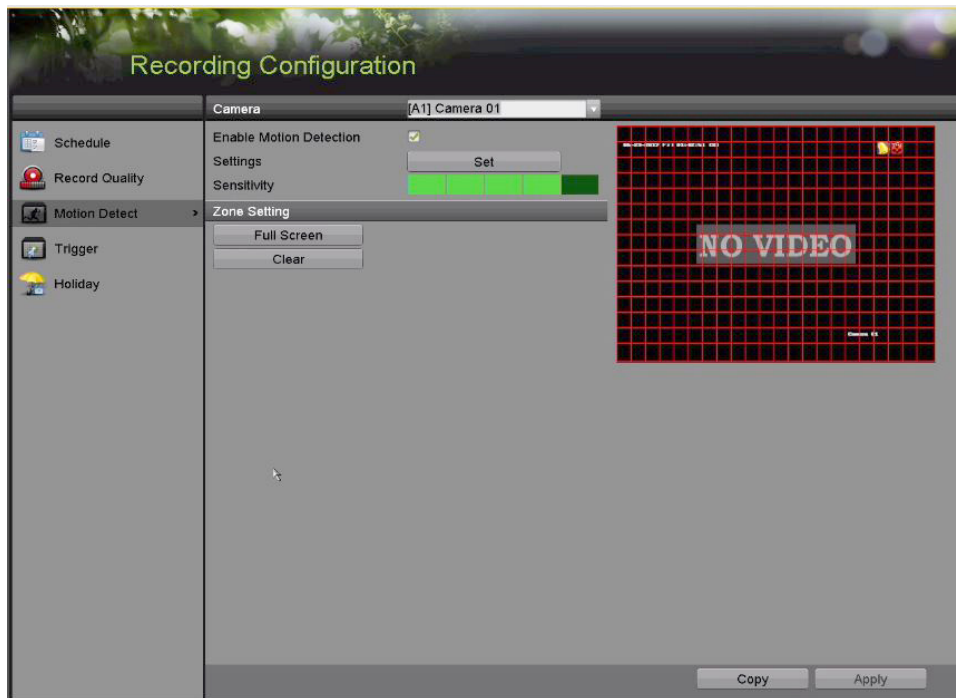



Figure 135, Motion Detection Setup Interface

3. Set detection area and sensitivity.
4. Check the motion detection checkbox to enable it.
5. Use the mouse to draw detection area(s) or click **Full Screen** to set the detection area to be the full screen.
6. Drag the sensitivity bar to set sensitivity.
7. Click  to set alarm response actions.

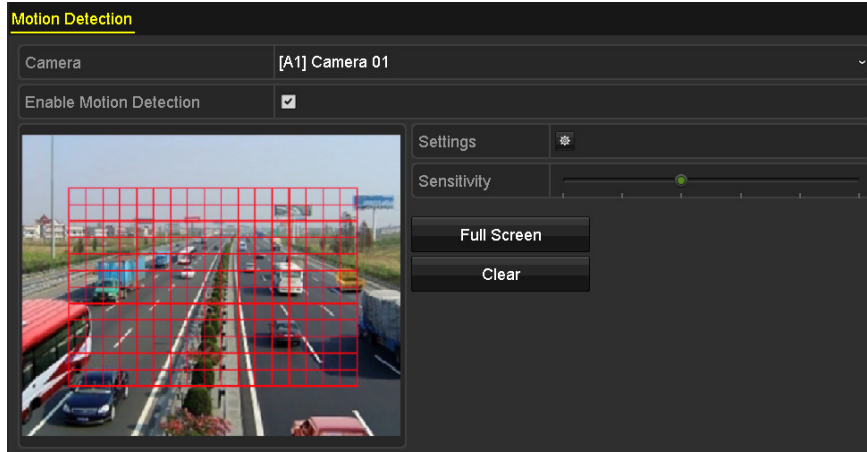


Figure 136, Set Detection Area and Sensitivity

8. Click the **Trigger Channel** tab and select one or more channels that are to start recording or be displayed full-screen on the monitor when a motion alarm is triggered.

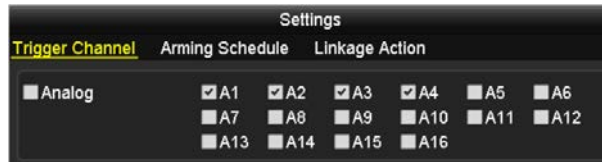


Figure 137, Set Trigger Camera of Motion Detection

9. Set channel arming schedule.
 - a) Select **Arming Schedule** tab to set the channel's arming schedule.
 - b) Choose one day of a week and up to eight time periods can be set within each day, or click **Copy** to copy the time period settings to other day(s).



NOTE

Time periods cannot repeat or overlap.



Figure 138, Set Arming Schedule of Motion Detection

10. Click **Linkage Action** tab to set up alarm response actions of motion alarm (see Chapter 8.7 Setting Alarm Response Actions).
11. Repeat the above steps to set up arming schedule for other days of the week.
12. Click **OK** to complete the channel's motion detection settings.
13. To set motion detection for another channel, repeat the above steps or copy the above settings to it.



You cannot copy the "Trigger Channel" action.

8.2 Setting Sensor Alarms

Set up handling method of an external sensor alarm.

1. Enter Alarm Input Settings interface, Menu > Recording Configuration > Trigger.

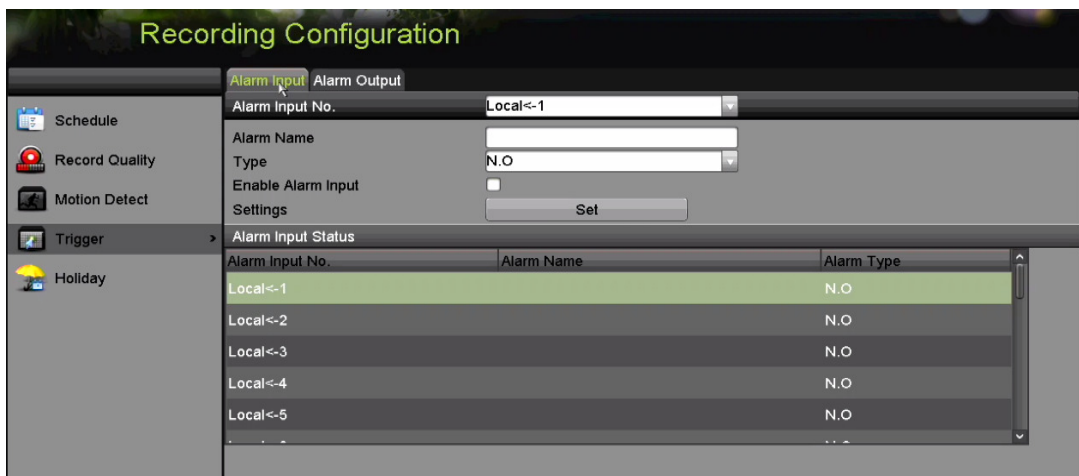


Figure 139, Alarm Input Settings Interface

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



Figure 140, Set Arming Schedule of Alarm Input

4. Select the **Trigger Channel** tab and select one or more channels to record or become full-screen monitoring when an external alarm input is triggered.
5. Select **Arming Schedule** tab to set the channel’s arming schedule. Select one day of a week. Eight time periods maximum can be set each day.



NOTE
Time periods cannot repeat or overlap.

6. Select **Linkage Action** tab to set up alarm response actions of the alarm input (Refer to Chapter 8.7 Setting Alarm Response Actions).
7. Repeat the above steps to set up arming schedule for other days of the week. You can also click on **Copy** to copy an arming schedule to other days.
8. To set another alarm input handling action, repeat the above steps or copy the above settings to it.



Figure 141, Copy Settings of Alarm Input

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



Figure 142, Disarm Linkage Actions



NOTE

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

8.3 Detecting Video Loss

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

1. Enter **Video Loss** interface of Camera Management, Menu> Camera> Video Loss.
2. Select a channel you want to detect.

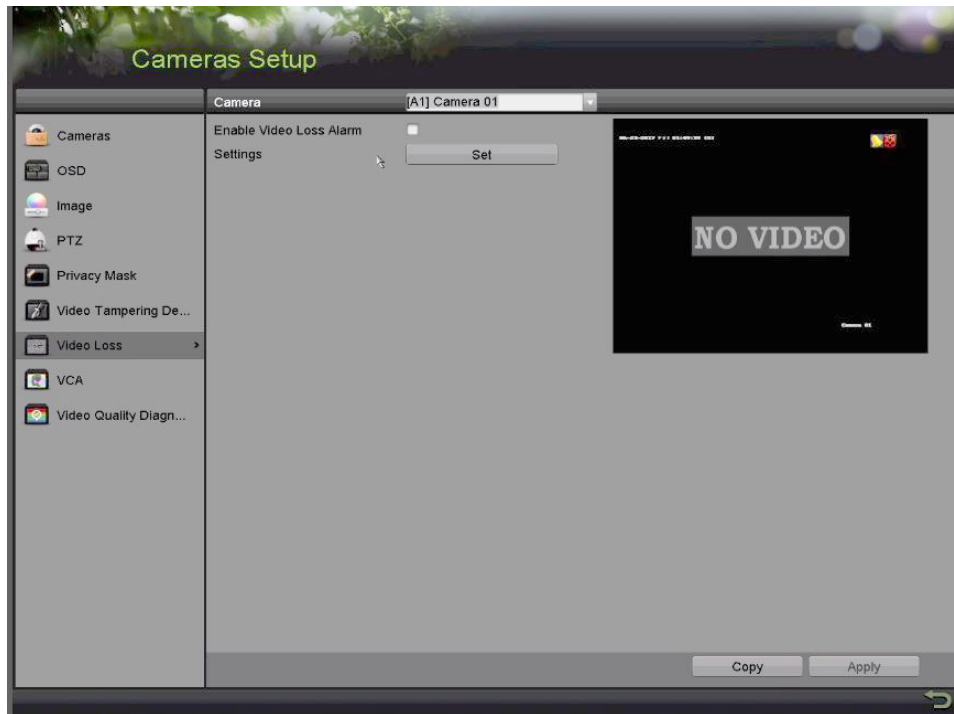


Figure 143, Video Loss Setup Interface

3. Set up video loss handling method.
4. Check the Enable Video Loss Alarm checkbox.
5. Click **Set** to set up video loss handling method.
6. Set the channel arming schedule.
 - a) Select Arming Schedule tab.
 - b) Choose one day of a week and up to eight time periods for each day, or click **Copy** to copy the time period settings to other day(s).



NOTE

Time periods cannot repeat or overlap.

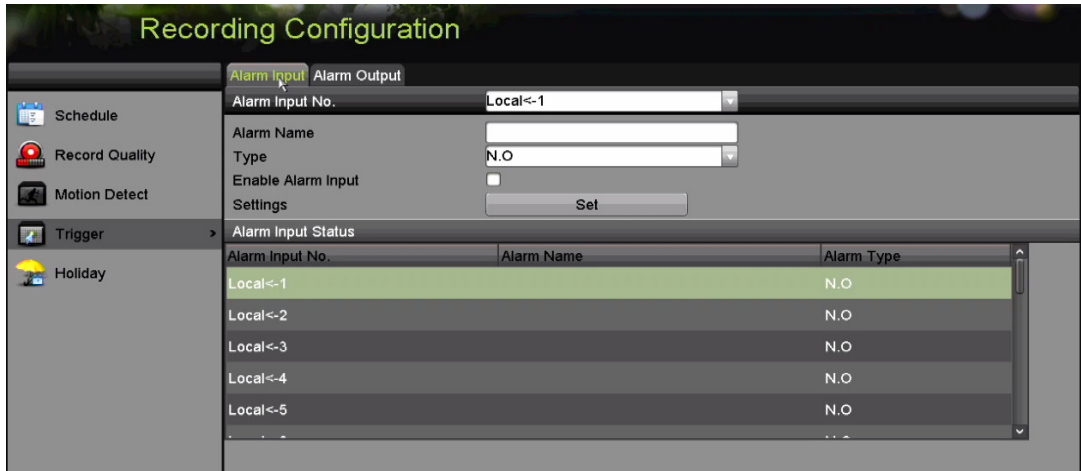


Figure 144, Set Video Loss Arming Schedule

- c) Repeat the above steps to set arming schedule for other days of the week, or click **Copy** to copy an arming schedule to other days.
7. Select the **Linkage Action** tab to set up video loss alarm response action (refer to Chapter 8.7 Setting Alarm Response Actions).
8. Click **OK** to complete the channel's video loss settings.
9. Repeat the above steps to finish setting other channels, or click **Copy** to copy the above settings to them.

8.4 Detecting Video Tampering

This feature triggers an alarm when the lens is covered and initiates alarm response action(s).

1. Enter the Camera Management **Video Tampering** interface, Menu > Camera > Video Tampering Detection.
2. Select a channel on which you want to detect video tampering.

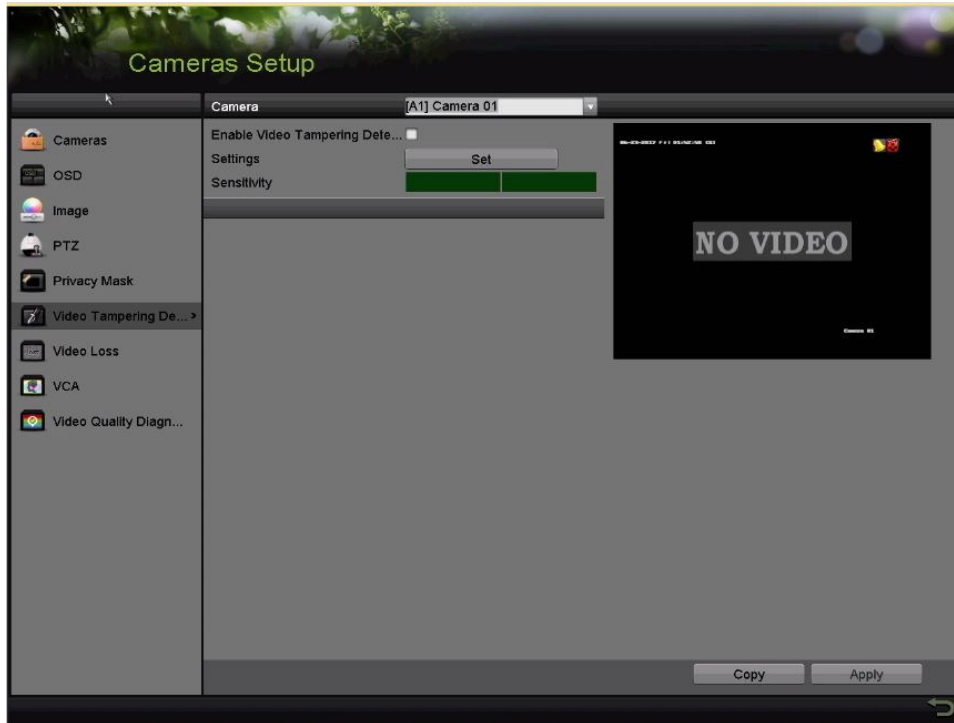


Figure 145, Video Tampering Interface

3. Check the Enable Video Tampering Detection checkbox.
4. Drag the **sensitivity** bar and choose a proper sensitivity level.
5. Click **Set** to set the video tampering handling method.
6. Set the channel's arming schedule and alarm response actions.
 - a) Click Arming Schedule tab to set the response action arming schedule.
 - b) Select a day of the week, with up to eight time periods each day.



NOTE

Time periods cannot repeat or overlap.

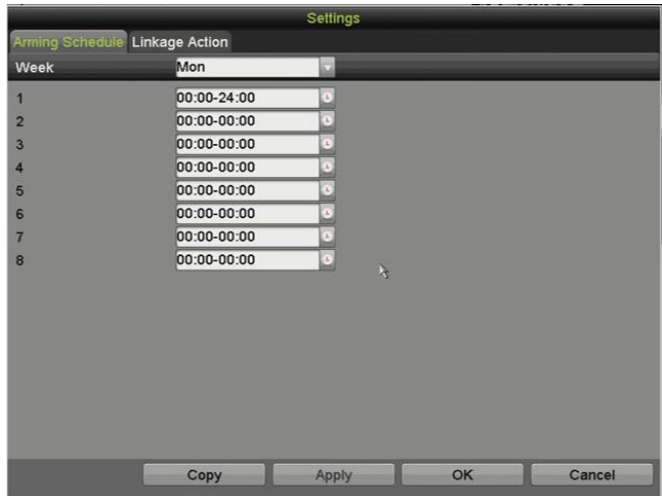


Figure 146, Set Video Tampering Arming Schedule

- c) Select **Linkage Action** tab to set alarm response actions of video tampering alarm (refer to Chapter 8.7 Setting Alarm Response Actions).
 - d) Repeat the above steps to set arming schedule for other days of the week, or use the **Copy** button to copy an arming schedule to other days.
 - e) Click **OK** to complete the video tampering settings of the channel.
7. Repeat the above steps to finish settings other channels, or click **Copy** to copy the above settings to them.
 8. Click **Apply** to save and activate the settings.

8.5 Setting All-day Video Quality Diagnostics

There are two ways to diagnose the video quality: manual and all-day. Perform the following steps to set the threshold of the diagnosing and the linkage actions.

1. Enter the Camera Management **Video Quality Diagnostics Settings** interface, Menu > Camera > Video Quality Diagnostics
2. Select a channel over which you want to detect video tampering.

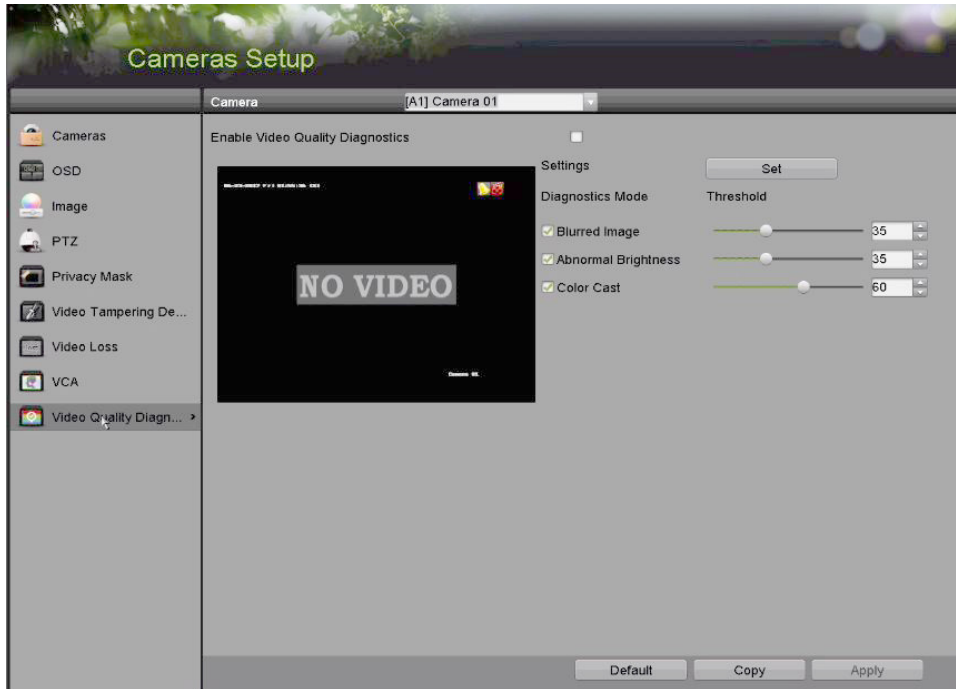


Figure 147, Video Quality Diagnostics Interface

3. Check the Enable Video Quality Diagnostics checkbox.



NOTE

To enable video quality diagnostics, the function must be supported by the selected camera.

4. Enable and set the threshold of the diagnostic types: **Blurred Image**, **Abnormal Brightness**, and **Color Cast**.
5. Check the corresponding checkbox of the diagnostic type, and adjust the threshold by dragging the bar.



NOTE

The higher the threshold, the harder it is to detect the exception.

6. Click **Set** to set the video quality diagnostics handling method. Set arming schedule and alarm response actions of the channel.
 - a) Click **Arming Schedule** tab to set the arming schedule of response action.
 - b) Choose a day of the week and up to eight time periods for each day.



NOTE

Time periods cannot repeat or overlap.

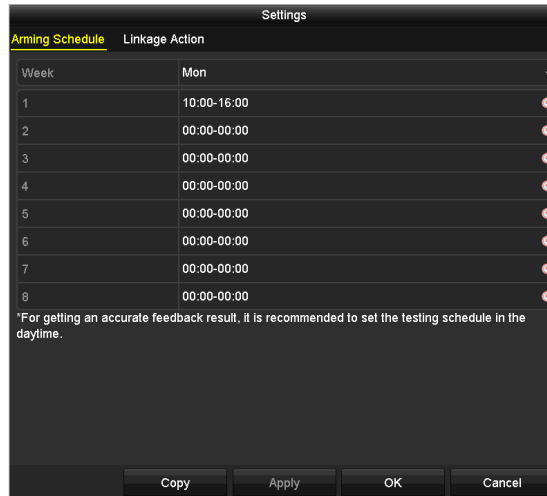


Figure 148, Set Arming Schedule of Video Quality Diagnostics

- c) Select **Linkage Action** tab to set alarm response actions of video quality diagnostics alarm (refer to Chapter 8.7 Setting Alarm Response Actions).
 - d) Repeat the above steps to set arming schedule for other days of the week, or click **Copy** to copy an arming schedule to other days.
 - e) Click **OK** to complete the video quality diagnostics settings of the channel.
7. Click **Apply** to save and activate the settings.
 8. (Optional) Copy the same settings to other cameras by clicking **Copy**.

8.6 Handling Exceptions

Exception settings refer to the handling method of various exceptions, as noted below:

- **HDD Full:** The HDD is full
 - **HDD Error:** Writing HDD error, unformatted HDD, etc.
 - **Network Disconnected:** Disconnected network cable
 - **IP Conflicted:** Duplicated IP address
 - **Illegal Login:** Incorrect user ID or password
 - **Input/Recording Resolution Mismatch:** The input resolution is smaller than the recording resolution
 - **Record/Capture Exception:** No space for saving recorded files or captured pictures
1. Enter **Exceptions** interface and handle various exceptions, Menu > Configuration > Exceptions.

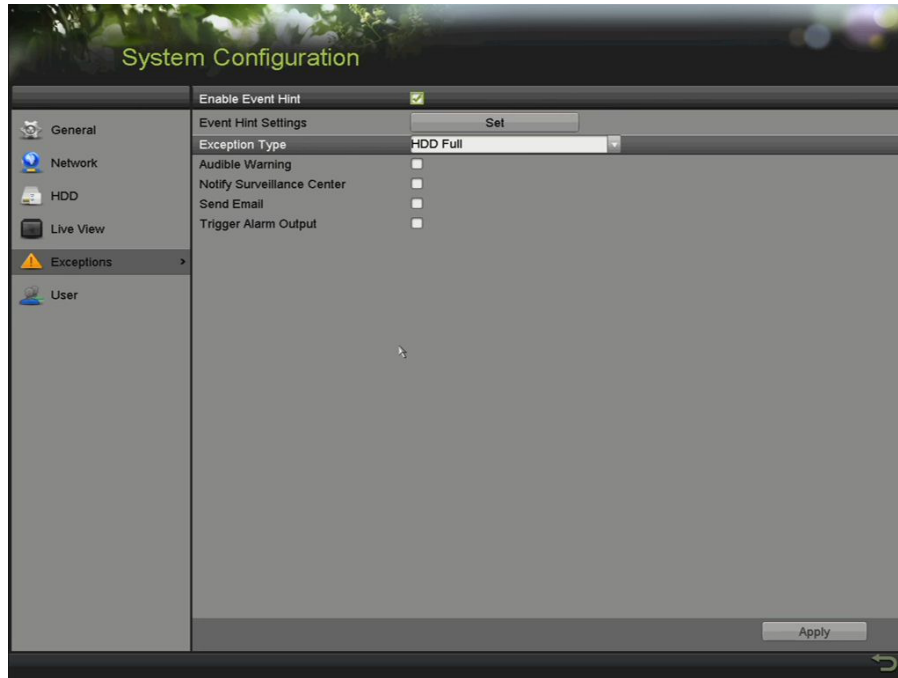



Figure 149, Exception Settings Interface

2. Check the **Enable Event Hint** checkbox to display the  (Event/Exception icon) when an exception event occurs. Click **Set** to display the event hint.

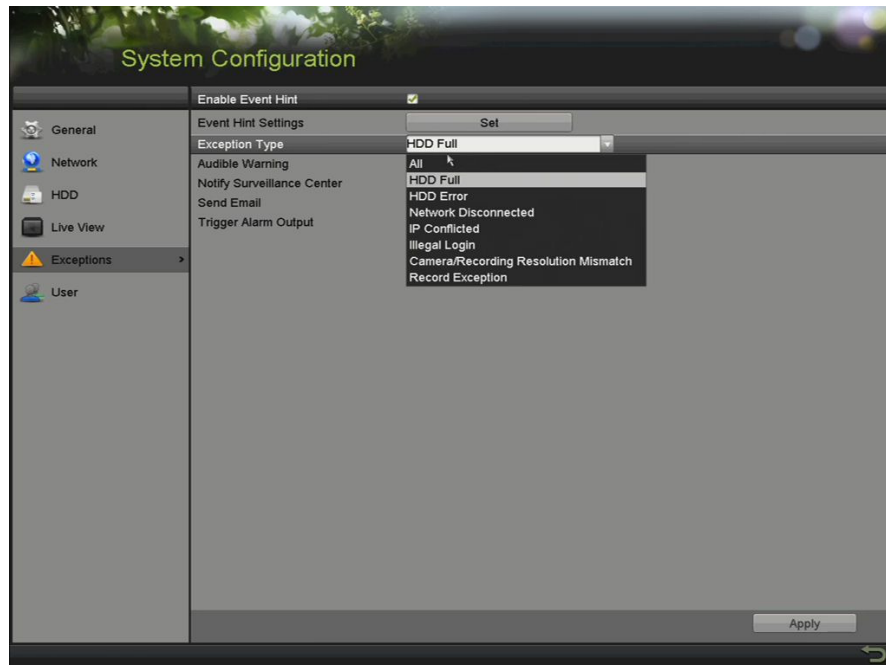


Figure 150, Event Hint Settings

 **NOTE**

Click  that appears in Live View to view detailed information about the exception event. Click **Set** to display the event hint.

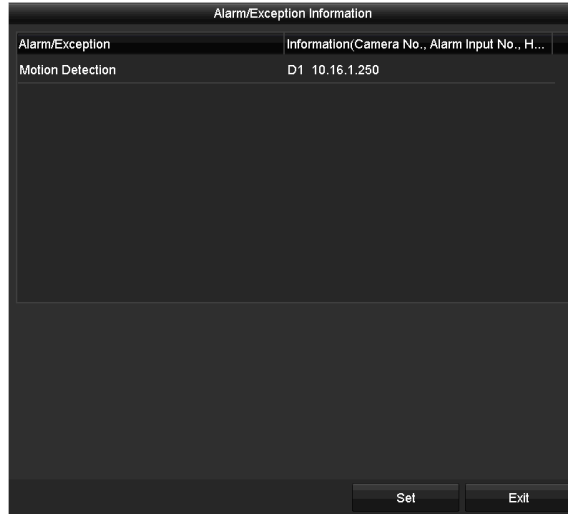


Figure 151, Detailed Event

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

8.7 Setting Alarm Response Actions

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

- **Full Screen Monitoring**

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

If alarms are triggered simultaneously in several channels, their full-screen images will be switched every 10 seconds (default dwell time). A different dwell time can be set in Menu > Configuration > Live View.

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

- **Audible Warning**

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

- **Notify Surveillance Center**

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



NOTE

The alarm signal will be transmitted automatically at detection mode when the remote alarm host is configured.

- **Send E-mail**

Send an e-mail with alarm information to a user or users when an alarm is detected.

- **Trigger Alarm Output**

Trigger an alarm output when an alarm is triggered.

1. Enter the Alarm Output interface, Menu > Record Configuration > Trigger > Alarm Output.
2. Select an alarm output and set the alarm name and dwell time.



Figure 152, Alarm Output Settings Interface



NOTE

If **Manually Clear** is selected in the **Dwell Time** drop-down list, it can be cleared only by going to Menu > Manual > Alarm.

3. Click the **Set** button to set the alarm output arming schedule.
 - 1) Choose a day of the week and set up to eight time periods each day.



NOTE

Time periods cannot repeat or overlap.



Figure 153, Set Arming Schedule of Alarm Output

- 2) Repeat the above steps to set arming schedule of other days of the week, or click **Copy** to copy an arming schedule to other days.
- 3) Click **OK** to complete the alarm output arming schedule setting.
- 4) Click **Apply** to save the settings.

Chapter 9 VCA Alarm

ATTENTION! Some of the features described below require special cameras. Not all features work with all cameras. Please contact your Hikvision Sales Expert for more information.

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



NOTE

DS-72xxHUI-Kx Series DVRs support VCA (line crossing detection and intrusion detection) of all channels. Channels with audio support audio exception detection.

DS-7216HQI-Kx Series support 2-ch VCA (line crossing detection and intrusion detection). Channels with audio support audio exception detection.

For the analog channels, line crossing detection and intrusion detection conflict with other VCA detection such as sudden scene change detection, face detection, and vehicle detection. You can enable only one function.

9.1 Face Detection

The Face Detection function detects faces that appear in the surveillance scene, and specific actions occur when the alarm is triggered.

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

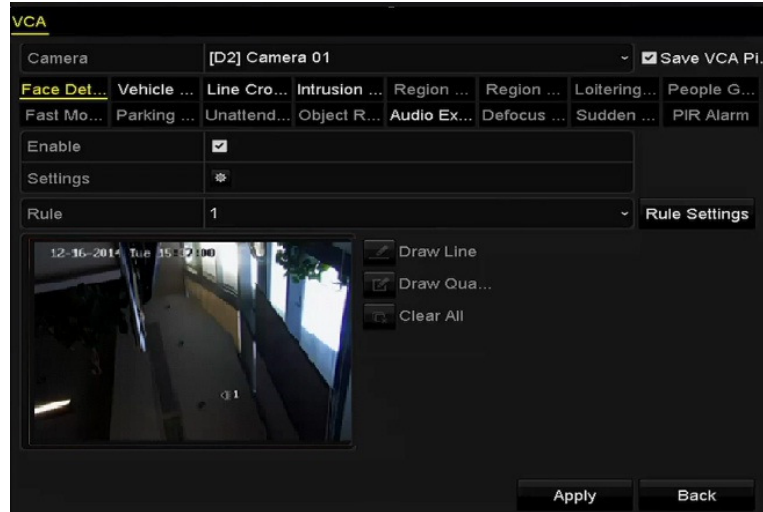


Figure 154, Face Detection

4. Set the VCA detection type to **Face Detection**.
5. Click **SET** to enter the face detection settings interface.
6. Configure the trigger channel, arming schedule, linkage action, and PTZ linking for the face detection alarm.



Figure 155, PTZ Linking

7. Click the **Rule Settings** button to set the face detection rules. Drag slider to set the detection sensitivity.

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

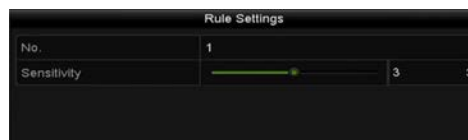


Figure 156, Set Face Detection Sensitivity

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

9.2 Line Crossing Detection

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.




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



Figure 157, Set Line Crossing Detection Rules

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



Click  to clear the existing virtual line.

Up to four rules can be configured.

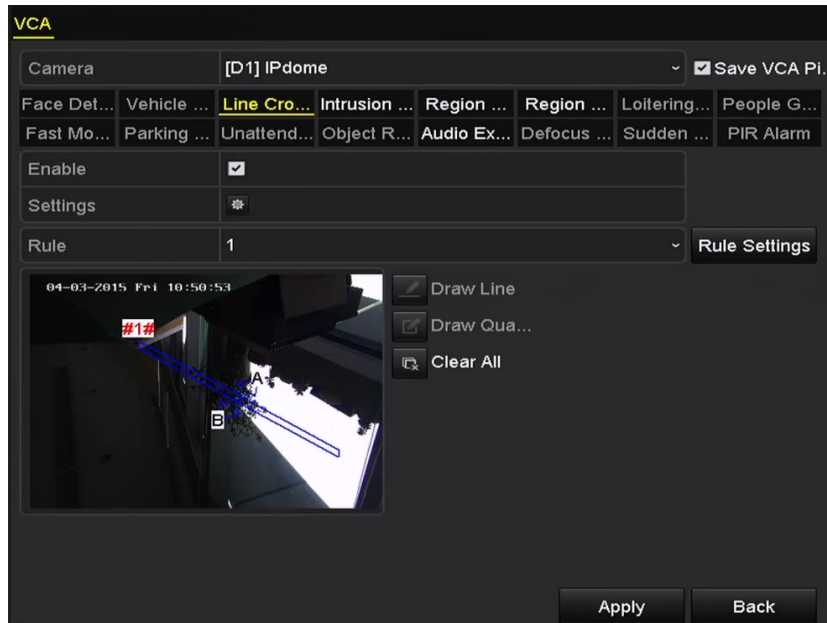


Figure 158, Draw Line for Line Crossing Detection


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



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

9.3 Intrusion Detection


The Intrusion Detection function detects people, vehicles, or other objects that enter and loiter in a pre-defined virtual region. Specific 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. Check 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, linkage action, and PTZ linking for the intrusion detection alarm.
7. Click **Rule Settings** to set the intrusion detection rules. Set the following parameters:


- **Threshold:** Range [1s-10s], the threshold for the time the object loiters in the region. When the object in the defined detection area loiters longer than the set time, the alarm will be triggered.
 - a) Drag the slider to set the detection sensitivity.
- **Sensitivity:** Range [1-100]. This value defines the size of the object that will trigger the alarm. The higher the value, the more easily the detection alarm will 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 to 50 percent, when the object enters the region and occupies half of the whole region, the alarm is triggered.



Figure 159, Set Intrusion Crossing Detection Rules

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

 **NOTE**

Click  to clear the existing virtual line.

Up to four rules can be configured.

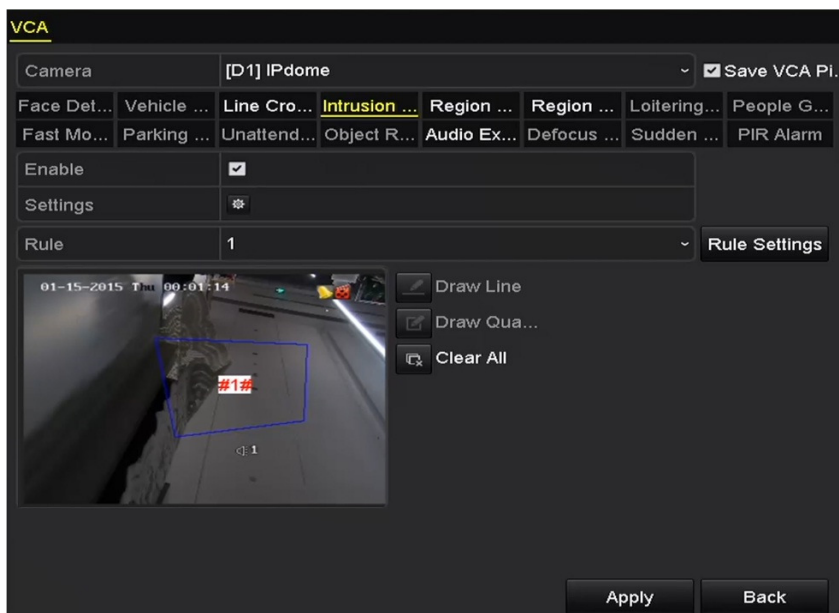


Figure 160, Draw Area for Intrusion Detection

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





NOTE

The sudden scene change detection and the intrusion detection features cannot be enabled on the same channel.

9.4 Region Entrance Detection

The Region Entrance Detection function detects people, vehicles, or other objects that enter a pre-defined virtual region. Specific 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. Check 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, linkage action, and PTZ linking for the region entrance detection alarm.
7. Click **Rule Settings** to set the sensitivity of the region entrance detection.
 - **Sensitivity: Range [0-100]**. The higher the value, the more easily the detection alarm will trigger.
8. Click  and draw a quadrilateral in the preview window by specifying four vertexes of the detection region, and right clicking to complete the drawing. Only one region can be configured.



NOTE

Click  to clear the existing virtual line.

Up to four rules can be configured.

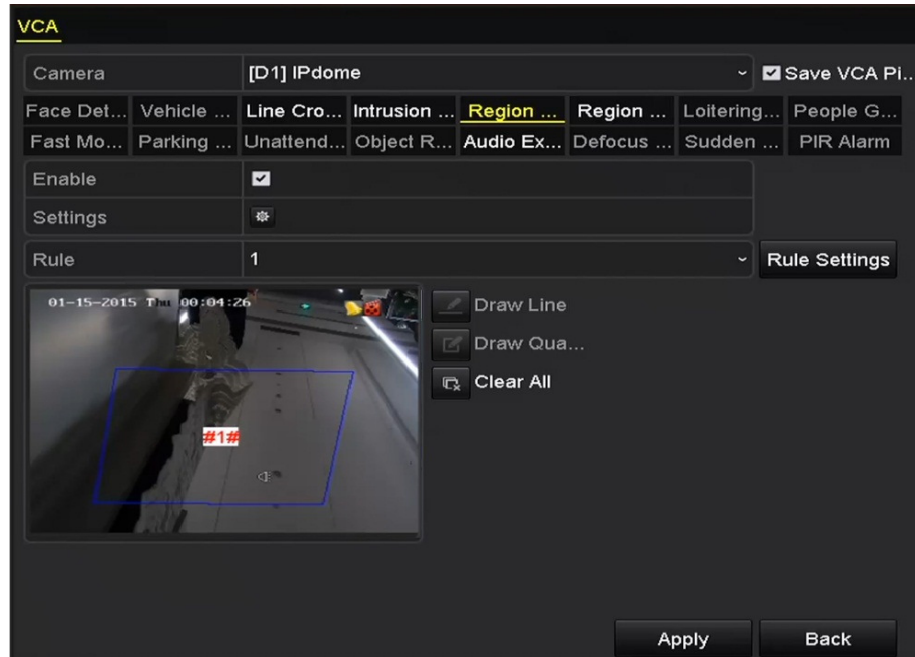


Figure 161, Set Region Entrance Detection

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

9.5 Region Exiting Detection

The Region Exiting Detection function detects people, vehicles, or other objects that exit from a pre-defined virtual region. Specific actions can be taken when the alarm is triggered.



See *Chapter 9.5 Region Entrance Detection* to configure region exiting detection. Up to four rules can be configured.

9.6 Loitering Detection

The Loitering Detection function detects people, vehicles, or other objects that loiter in a pre-defined virtual region for a pre-defined time. A series of actions can be taken when the alarm is triggered.



Threshold [1s-10s] in Rule Settings defines the time the object loiters in the region. If you set the value to 5, an alarm is triggered if the object loiters in the region for 5 seconds. If you set the value to 0, an alarm is triggered immediately once the object enters the region.

Up to four rules can be configured.

9.7 People Gathering Detection

The People Gathering Detection alarm is triggered when people gather in a pre-defined virtual region. A series of actions can be taken when the alarm is triggered.



NOTE

Percentage in Rule Settings defines the gathering density of the people in the region. If the percentage is small, the alarm is triggered when a small number of people gathers in the defined region.

Up to four rules can be configured.

9.8 Fast Moving Detection

The Fast Moving Detection alarm is triggered when people, vehicles, or other objects move fast in a pre-defined virtual region. A series of actions can be taken when the alarm is triggered.



NOTE

Sensitivity in Rule Settings defines the moving speed of the object that will trigger the alarm. The higher the value, the more easily a moving object will trigger the alarm.

Up to four rules can be configured.

9.9 Parking Detection

The Parking Detection function detects illegal parking in places such as highways, one-way streets, etc. A series of actions can be taken when the alarm is triggered.



NOTE

Threshold [5s-20s] in Rule Settings defines the time the vehicle parks in the region. If you set the value as 10, an alarm is triggered after the vehicle stays in the region for 10 seconds.

Up to four rules can be configured.

9.10 Unattended Baggage Detection

The Unattended Baggage Detection function detects objects left in a pre-defined region such as baggage, purses, dangerous materials, etc. A series of actions can be taken when the alarm is triggered.



NOTE

Threshold [5s-20s] in Rule Settings defines the time the objects are left in the region. If the value is set to 10, an alarm is triggered after the object stays in the region for 10 seconds. **Sensitivity** defines similarity of the object to the image's background. If the sensitivity is high, a small object left in the region will trigger the alarm.

Up to four rules can be configured.

9.11 Object Removal Detection

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



NOTE

Threshold [5s-20s] in Rule Settings defines the time the objects are removed from the region. If you set the value as 10, an alarm is triggered after the object disappears from the region for 10 seconds.

Sensitivity defines the similarity of the object to the image background. When the sensitivity is high, a very small object taken from the region will trigger the alarm.

Up to four rules can be configured.


9.12 Audio Exception Detection

The Audio Exception Detection function detects abnormal sounds in the surveillance scene such as the sudden increase/decrease of sound intensity. Specific actions can be taken when the alarm is triggered.



NOTE

Audio Exception Detection is supported on all analog channels.

1. Enter the VCA settings interface, Menu > Camera > VCA.
2. Select the camera for which to configure the VCA.
3. Check the **Save VCA Picture** checkbox to save the captured VCA detection pictures.
4. Set the VCA detection type to **Audio Exception Detection**.
5. Click the  icon to configure the trigger channel, arming schedule, linkage action, and PTZ linking for the audio exception alarm.
6. Click **Rule Settings** to set the audio exception rules.

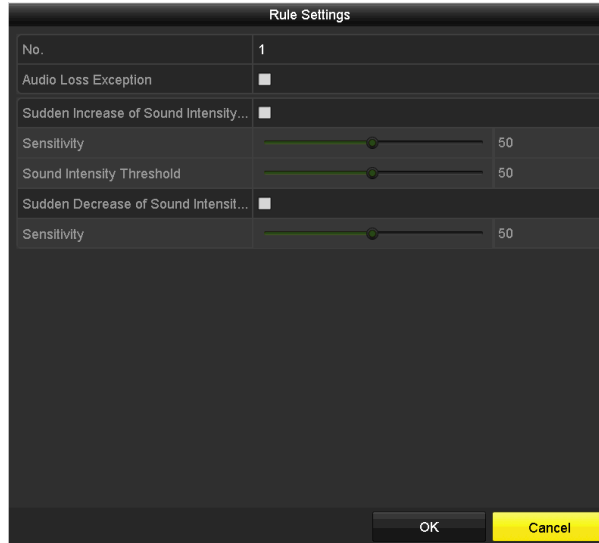


Figure 162, Set Audio Exception Detection Rules

- a) Check the **Audio Loss Exception** checkbox to enable the audio loss detection function.
- b) Check the **Sudden Increase of Sound Intensity Detection** checkbox to detect a steep rise in the surveillance scene sound. Set the sensitivity and threshold for the steep rise in sound.
- c) **Sensitivity:** Range [1-100], the smaller the value, the more severe the change must be to trigger the detection.
- d) **Sound Intensity Threshold:** Range [1-100], this filters the sound in the environment. The louder the environment sound, the higher the value should be. Adjust it according to the environment.
- e) Check the **Sudden Decrease of Sound Intensity Detection** checkbox to detect a steep drop in the surveillance scene sound. Set the detection sensitivity [1-100] for the steep drop in sound.

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

9.13 Defocus Detection

Image blur caused by defocusing of the lens can be detected. Specific actions can be taken when the alarm is triggered.



NOTE

Sensitivity in Rule Settings ranges from 1 to 100. The higher the value, the more easily the defocus image will trigger the alarm.

9.14 Sudden Scene Change

The Scene Change Detection function detects changes in the surveillance environment by external factors such as the intentional rotation of the camera. Specific actions can be taken when the alarm is triggered.

**NOTE**

Sensitivity in Rule Settings ranges from 1 to 100. The higher the value, the more easily the change of scene will trigger the alarm.

For analog cameras, line crossing detection and intrusion detection conflict with other VCA detections such as sudden scene change detection, face detection, and vehicle detection. Only one function can be enabled. If you enable line crossing detection or intrusion detection, if you enable sudden scene change detection and apply the settings, the following attention box pops up to remind you there is not enough resources and asks you to disable the enabled VCA type(s) of the selected channel(s).

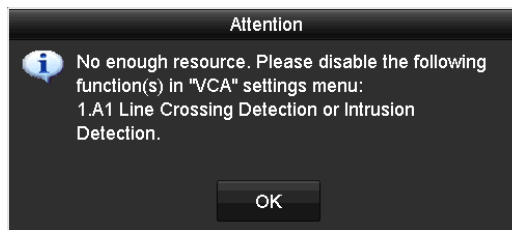



Figure 163, Disable Other VCA Type(s)

9.15 PIR Alarm

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 other warm blooded creatures 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. Check 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, linkage action, and PTZ linking for the PIR alarm.
6. Click **Rule Settings** to set the rules.
7. Click **Apply** to activate the settings.

Chapter 10 VCA Search

With the configured VCA detection, the device supports various VCA search functions: behavior search, face search, plate search, people counting, and heat map results of the IP cameras.

10.1 Face Search

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

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

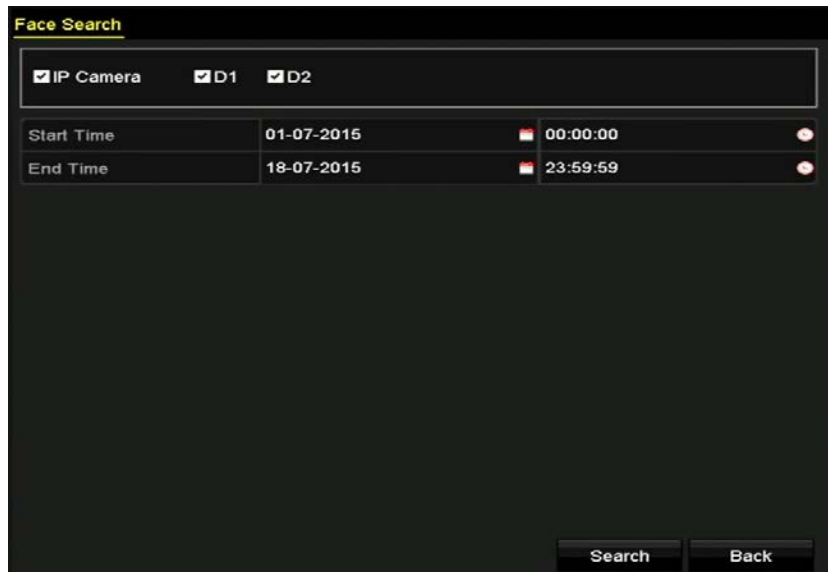






Figure 164, Face Search

3. Specify the start time and end time for searching the captured face pictures or video files.
4. Upload the pictures from your local storage device for matching the detected face pictures.
5. Set the similarity level for the source pictures and the captured pictures.
6. Click **Search** to start searching. The search results of face detection pictures are displayed in list or in chart.



Figure 165, Face Search Interface

7. Play the face picture related video file.
 - 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.
 - Click  to stop playing, or click  /  to play the previous/next file.
8. To export the captured face pictures to a local storage device, connect the storage device and click **Export All** to enter the Export interface.
 - a) Click **Export** to export all face pictures to the storage device.

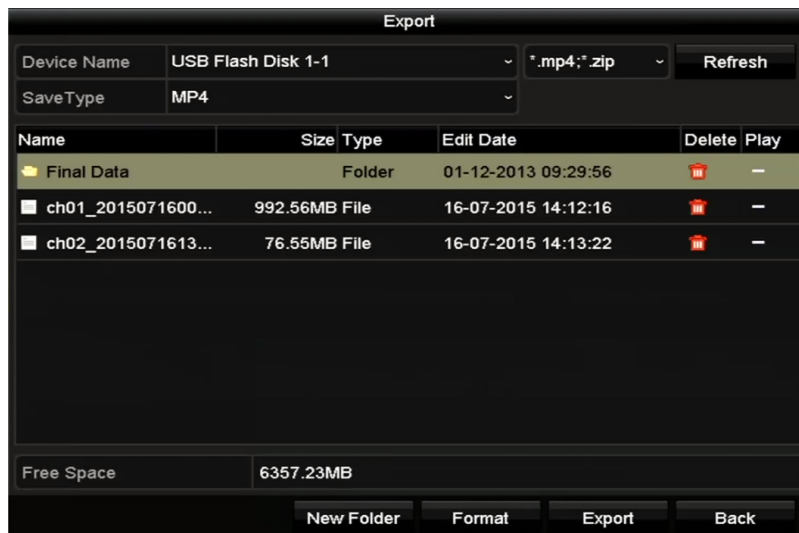


Figure 166, Export Files

10.2 Behavior Search

The Behavior Analysis function detects a series of suspicious behavior based on VCA detection. Specific 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 167, Behavior Search Interface

4. Select the VCA detection type from the drop-down list, including 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 result pictures are displayed in a list or chart.



Figure 168, Behavior Search Results

6. Play the behavior analysis picture related video file.
 - Double click 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.
 - Click  to stop 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 and click **Export All** to enter the Export interface.
8. Click **Export** to export all pictures to the storage device.

10.3 People Counting

People Counting is used to calculate the number of people who enter or left a pre-defined area and can provide daily/weekly/monthly/annual reports for analysis.

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

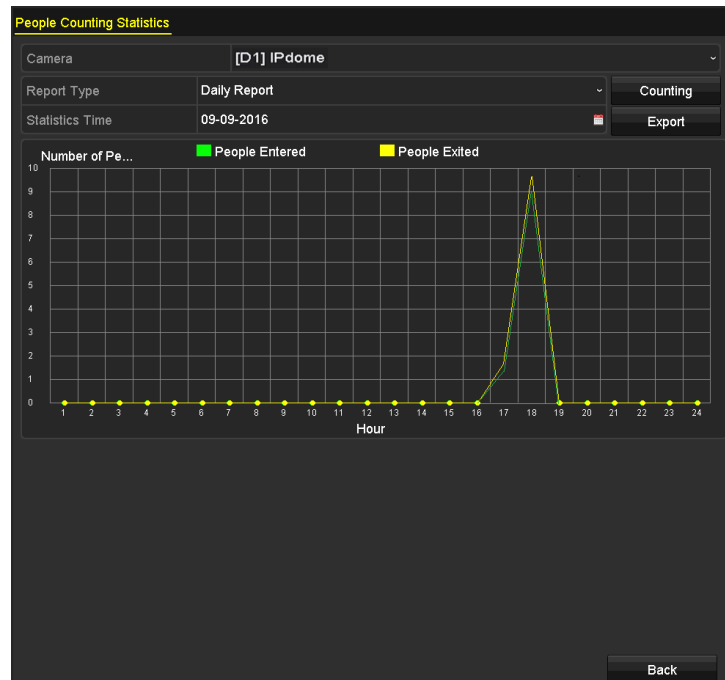


Figure 169, People Counting Interface

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

10.4 Heat Map

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

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

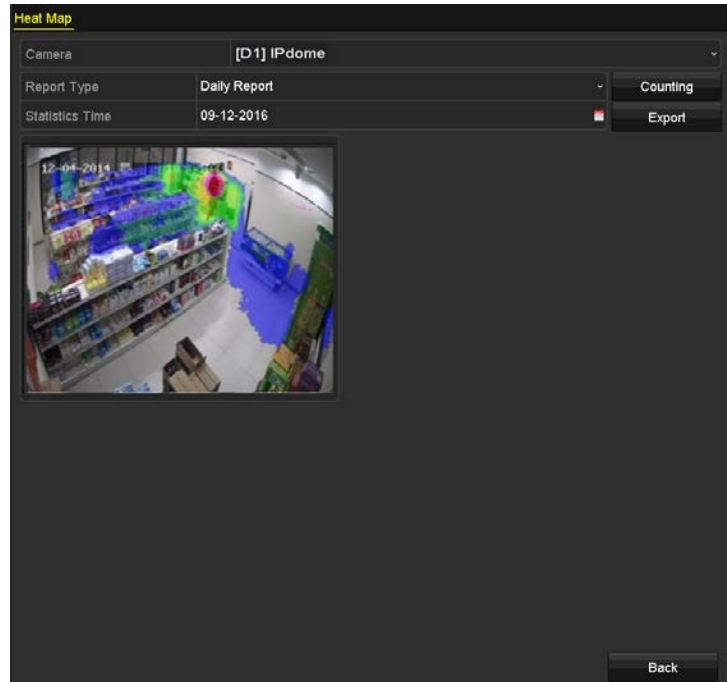


Figure 170, Heat Map Interface

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



NOTE

As shown in Figure 10-8, red color block (255, 0, 0) indicates the most popular area, and blue color block (0, 0, 255) indicates the less-popular area.

6. You can click **Export** to export the statistics report in Microsoft Excel format.

Chapter 11 Network Settings

11.1 Configuring General Settings

Network settings must be properly configured before you operate the DVR over a network.

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



Figure 171, Network Settings Interface

2. Select the **General** tab.
3. On the **General Settings** interface, configure the following parameters: NIC Type, IPv4 Address, IPv4 Gateway, MTU, DNS Server, and Main NIC.

NOTE

The valid value of MTU is from 500 to 1500.

If a DHCP server is available, check the **Enable DHCP** checkbox to obtain an IP address and other network settings from that server automatically.

If DHCP is enabled, you can check the **Enable DNS DHCP** checkbox or uncheck it and edit the **Preferred DNS Server** and **Alternate DNS Server**.

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

11.2 Configuring Advanced Settings

11.2.1 Configuring PPPoE Settings

The DVR 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.

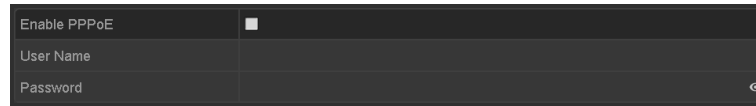



Figure 172, PPPoE Settings Interface

3. Check the **Enable PPPoE** checkbox to enable this feature.
 4. Enter **User Name** and **Password** for PPPoE access.
-  **NOTE**
The User Name and Password are assigned by your ISP.
5. Click **Apply** to save the settings.
 6. After successful settings, the system asks you to reboot the device to enable the new settings, and the PPPoE dial-up is automatically connected after reboot.
 7. You can go to Menu > Maintenance > System Info > Network interface to view the status of PPPoE connection.

11.2.2 Configuring Hik-Connect

Hik-Connect provides a mobile phone application and service platform page (www.hik-connect.com) to access and manage the DVR for convenient remote access to the surveillance system.



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

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

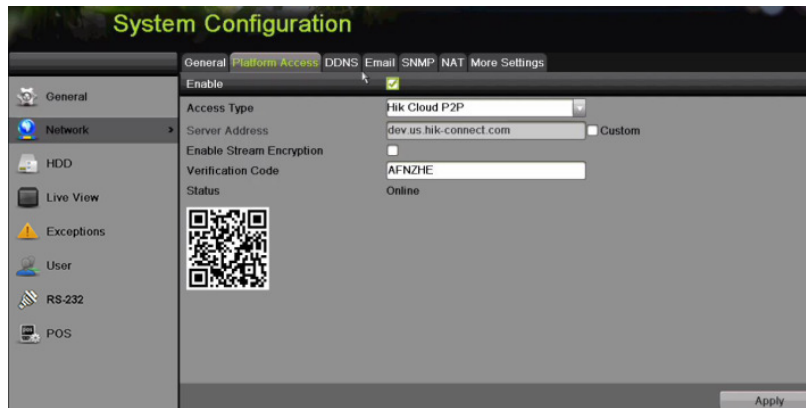


Figure 173, Hik-Connect Settings

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

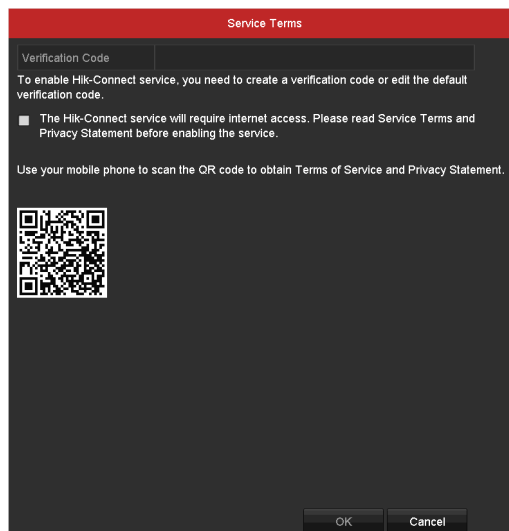


Figure 174, Service Terms

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



NOTE

Hik-Connect is disabled by default.

The verification code field is empty when the device leaves the factory.

The verification code must contain 6 to 12 letters or numbers and is case sensitive.

If you upgrade an older DVR version with Hik-Connect enabled, Hik-Connect is still enabled. If you disable it and then enable it for the first time, you need to change the verification code if the encrypted verification code is the same as that of the configuration file or the encrypted verification code is empty and the verification code of the configuration file is ABCDEF. In these two conditions, you must create a new verification code or you can delete the default and enter the same verification code as the default one.

Every time you enable Hik-Connect, the Service Terms interface pops up, and you should check the checkbox before enabling it.

8. (Optional) Check the **Custom** checkbox and enter the **Server Address**.
9. (Optional) Check the **Enable Stream Encryption** checkbox. If this feature is enabled, the verification code is required for remote access and live view.



NOTE

Use your phone's scanning tool to quickly get the device code by scanning the QR code.

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

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



NOTE

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

11.2.3 Configuring DDNS

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

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

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

- **DynDNS**

- Enter **Server Address** for DynDNS (i.e., members.dyndns.org).
- In the **Device Domain Name** text field, enter the domain obtained from the DynDNS website.
- Enter the **User Name** and **Password** registered on 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 175, DynDNS Settings Interface

- **PeanutHull**

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

Enable DDNS	<input checked="" type="checkbox"/>
DDNS Type	PeanutHull
Area/Country	Custom
Server Address	
Device Domain Name	
Status	DDNS is disabled.
User Name	123.gcjp.net
Password	*****

Figure 176, PeanutHull Settings Interface

- **NO-IP:**

- Enter the account information in the corresponding fields. Refer to the DynDNS settings.
- Enter **Server Address** for NO-IP.
- In the **Device Domain Name** text field, enter the domain obtained from the NO-IP website (www.no-ip.com).
- 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 177, NO-IP Settings Interface

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

11.2.4 Configuring NTP Server

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

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

Enable NTP	<input checked="" type="checkbox"/>
Interval (min)	60
NTP Server	210.72.145.44
NTP Port	123

Figure 178, 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 minutes.
 - **NTP Server:** IP address of NTP server
 - **NTP Port:** Port of NTP server
5. Click **Apply** to save and exit the interface.

 **NOTE**

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

11.2.5 Configuring NAT

Universal Plug and Play (UPnP™) lets the device seamlessly discover the presence of other network devices on the network and establish functional network services for data sharing, communications, etc. Use the UPnP™ function to quickly connect the device to the WAN via a router without port mapping.

- **Before Starting**

To enable the UPnP™ function, enable the device router's UPnP™ function. When the device network working mode is set to multi-address, the Default Route of the device must 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 **UPnP™ Settings** interface.

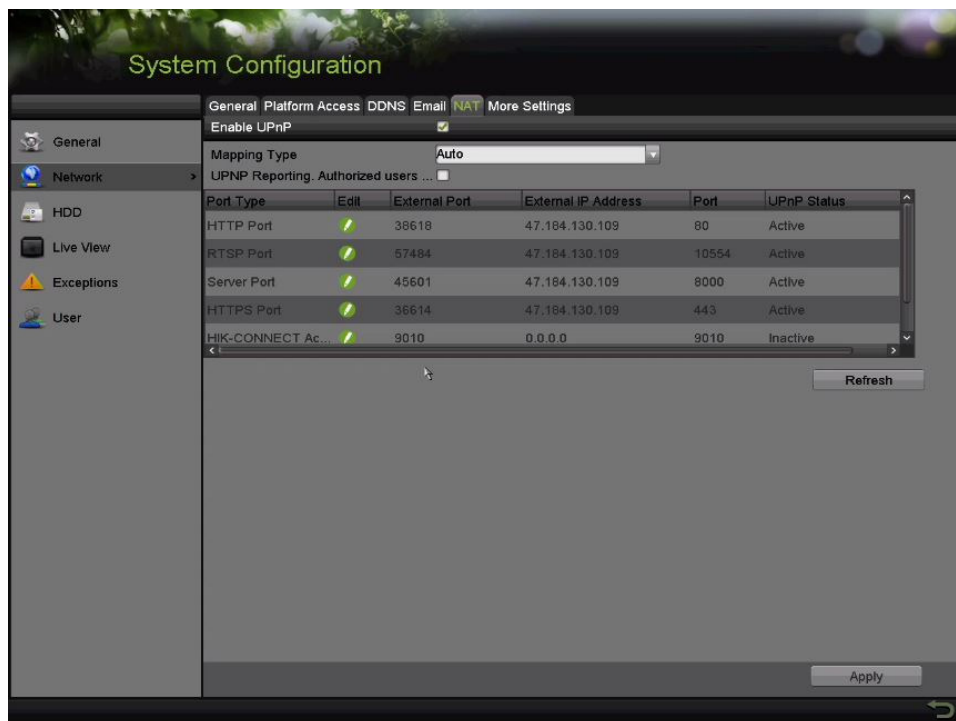


Figure 179, UPnP™ Settings Interface

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

- **OPTION 1: Auto**

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

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

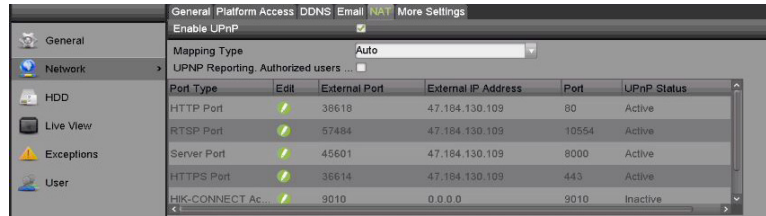


Figure 180, UPnP™ Settings Finished – Auto

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

NOTE

You can use the default port No. or change it according to actual requirements.

External Port indicates the port No. for the router’s port mapping.

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 each values must be different. 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 181, External Port Settings Dialog Box

- 2) Click **Apply** to save the settings.
- 3) Click **Refresh** to get the latest status of the port mapping.

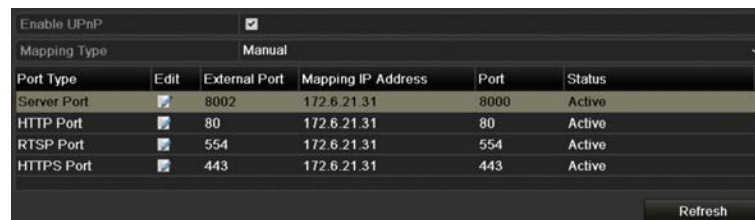


Figure 182, UPnP™ Settings Finished-Manual

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.

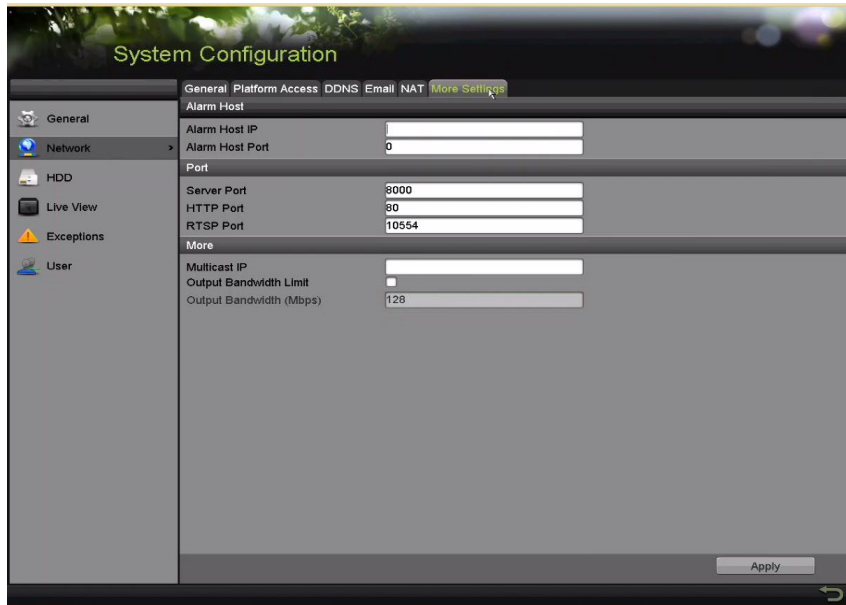


Figure 183, More Settings Interface

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 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:** 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 different requirements.

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



NOTE

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

- **Output Bandwidth Limit:** Check the checkbox to enable output bandwidth limit.
- **Output Bandwidth:** After enabling the output bandwidth limit, enter the output bandwidth into the text field.



NOTE

Output bandwidth limit is used for remote live view and playback.

The minimum output bandwidth is 2 Mbps.

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

11.2.7 Configuring HTTPS Port

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

If you set the port number to 443 and the IP address is 192.0.0.64, access the device by entering *https://192.0.0.64:443* in the Web browser.



NOTE

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

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

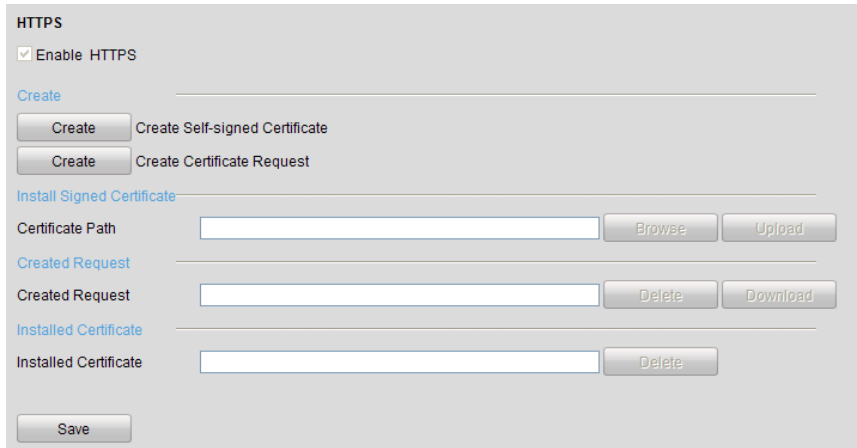


Figure 184, HTTPS Settings

- **OPTION 1: Create the Self-Signed Certificate**

a) Click **Create** to display the following dialog box:

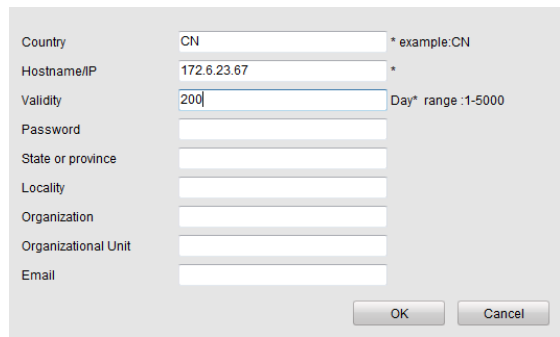


Figure 185, Create Self-signed Certificate

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

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

- **OPTION 2: Create the Authorized Certificate**

a) Click **Create** to create the certificate request.

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

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

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

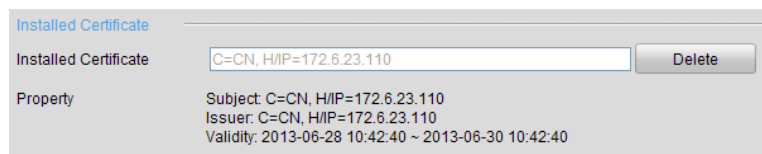


Figure 186, Installed Certificate Property

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

11.2.8 Configuring E-Mail

The system can be configured to send an e-mail notification to designated users if an event is detected, e.g., an alarm or motion event is detected, etc.

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

11.2.8.1 Before Starting

Configure the IPv4 Address, IPv4 Subnet Mask, IPv4 Gateway, and the Preferred DNS Server in the Network Settings menu. Refer to *Chapter •Configuring General Settings* for detailed information.

11.2.8.2 Procedure

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

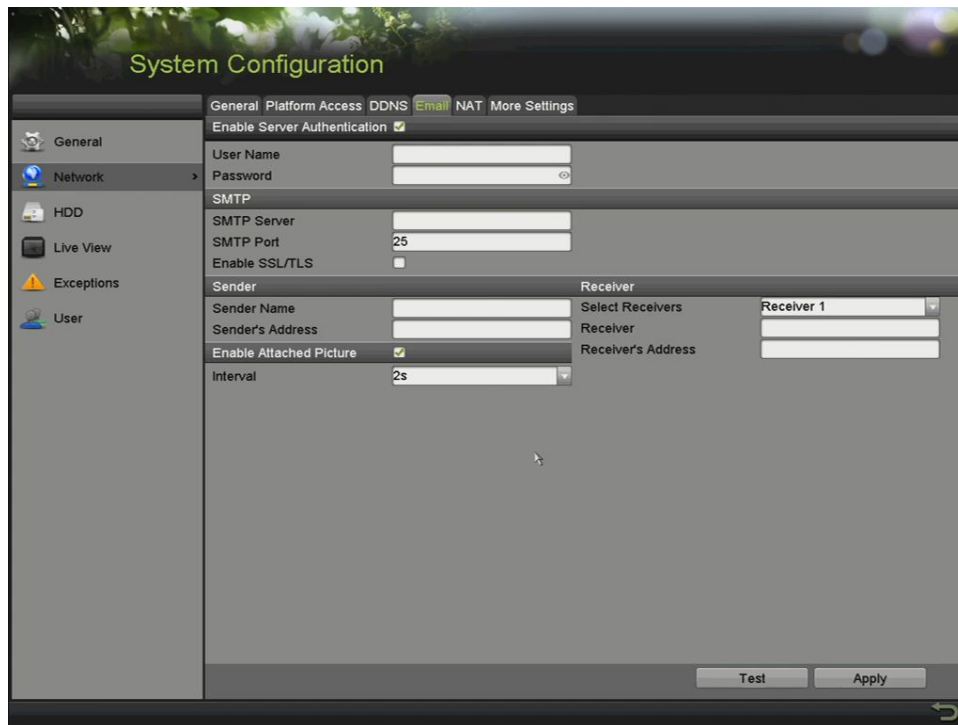



Figure 187, E-mail Settings Interface

3. Configure the following e-mail settings:
 - **Enable Server Authentication (optional):** Check the checkbox to enable the server authentication feature.
 - **User Name:** The sender's e-mail user account for SMTP server authentication
 - **Password:** The password of sender's e-mail for SMTP server authentication
 - **SMTP Server:** The SMTP Server IP address or host name (e.g., smtp.263xmail.com)
 - **SMTP Port:** The SMTP port. The default TCP/IP port used for SMTP is 25.
 - **Enable SSL (optional):** Click the checkbox to enable SSL if required by the SMTP server.
 - **Sender:** The name of sender
 - **Sender's Address:** The e-mail address of sender
 - **Select Receivers:** Select the receiver. Up to three receivers can be configured.
 - **Receiver:** The name of the receiver of the e-mail
 - **Receiver's Address:** The e-mail address of the receiver
 - **Enable Attached Picture:** Check the checkbox if you want to send e-mail with attached alarm images. The interval is the time between two captures of the alarm images.
-  **NOTE**

For IP cameras, the alarm images are directly sent as attached images by e-mail. One image can be sent for one IP camera. Attached images of the linked cameras cannot be sent.

For analog cameras, three attached images can be sent for one analog camera when the alarm is triggered.

 - **Interval:** Refers to the time between sending attached images.
 - **E-mail Test:** Sends a test message to verify that the SMTP server can be reached.
4. Click **Apply** to save the e-mail settings.
5. Click **Test** to test whether your e-mail settings work. The corresponding Attention message box pops up.

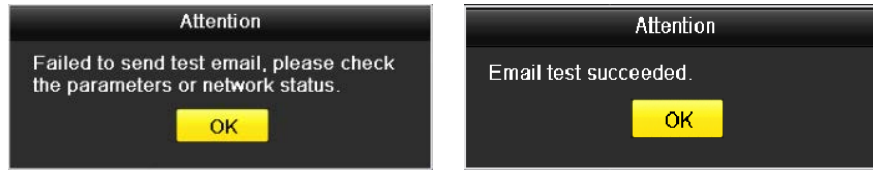


Figure 188, Email Testing Attention

11.2.9 Checking Network Traffic

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

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

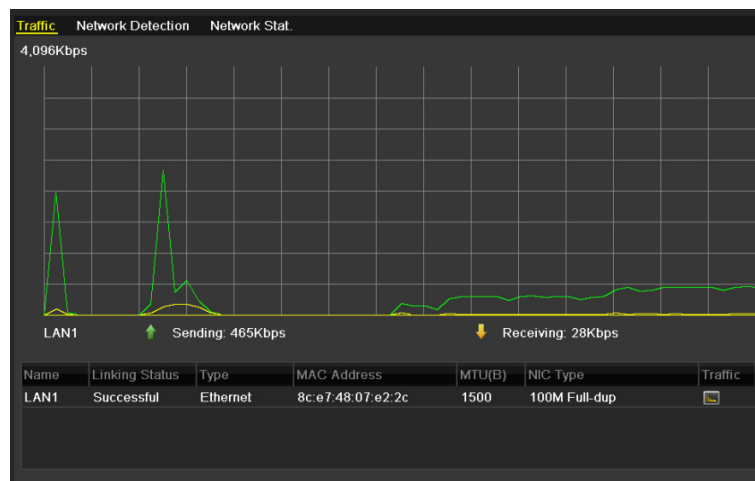


Figure 189, Network Traffic Interface

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

11.3 Configuring Network Detection

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

11.3.1 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** interface.

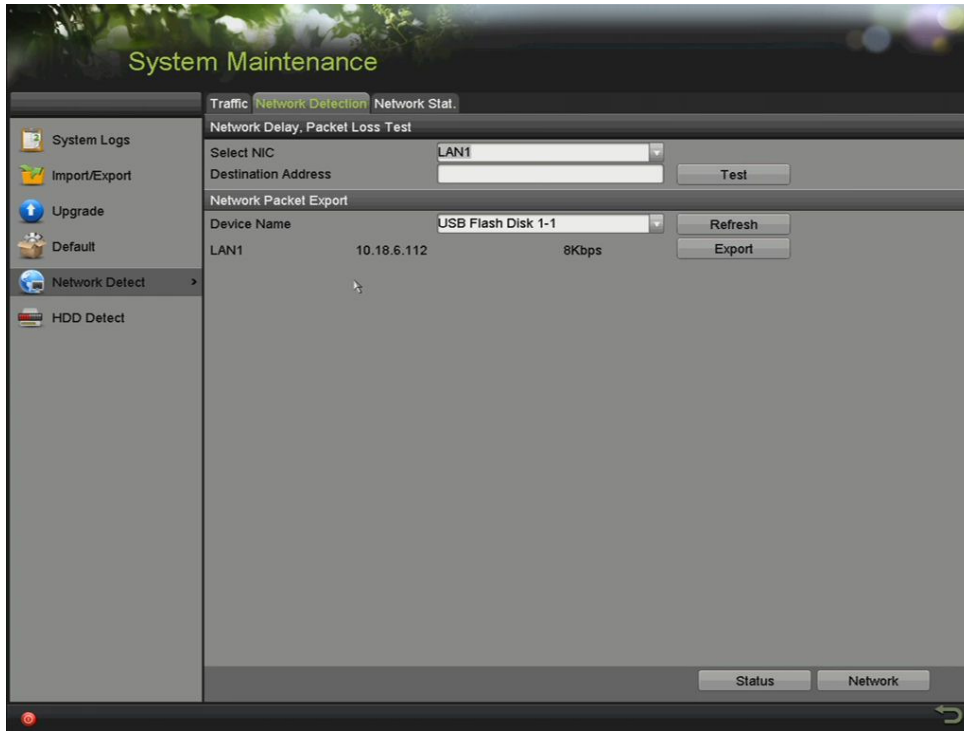


Figure 190, Network Detection Interface

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

11.3.2 Exporting Network Packet

By connecting the DVR to a network, the captured network data packet can be exported to a USB flash disk, 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 Name** drop-down list.



NOTE

Click the **Refresh** button if the connected local backup device is not displayed. If the system fails to detect the backup device, check whether it is compatible with the DVR. You can format the backup device if the format is incorrect.

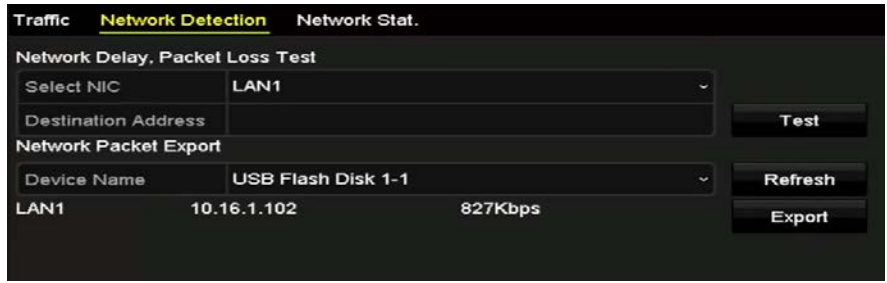


Figure 191, Export Network Packet

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

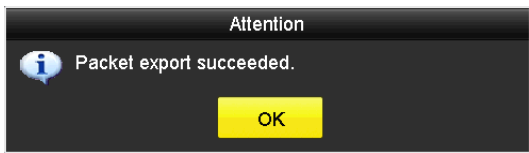


Figure 192, Packet Export Attention



NOTE
Up to 1 MB of data can be exported each time.

11.3.3 Checking Network Status

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

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

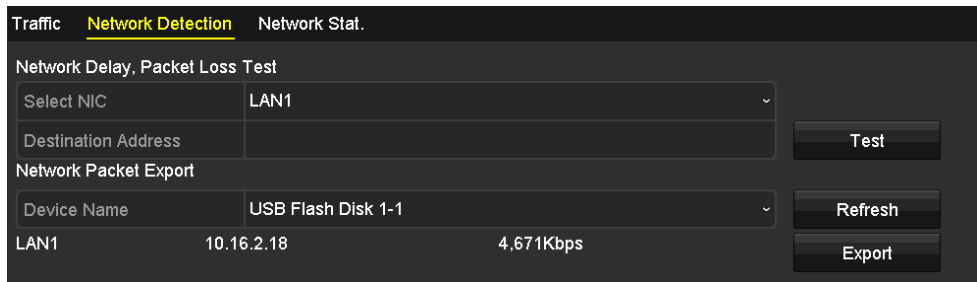


Figure 193, Checking Network Status

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



Figure 194, Network Status Checking Result

5. If the message box pops out with information other than this, click the **Network** button to show the network parameters quick setting interface.

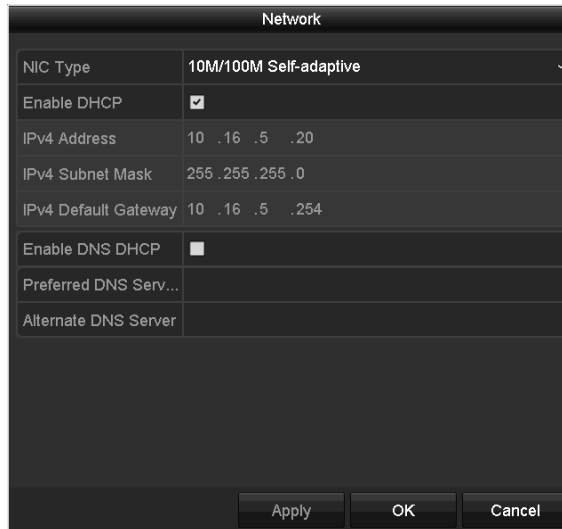


Figure 195, Network Parameters Configuration

11.3.4 Checking Network Statistics

Check the network statistics to obtain the real-time information of the device.

1. Enter the **Network Statistics** interface, Menu > Maintenance> Net Detect.
2. Click the **Network Stat.** tab to enter the **Network Statistics** interface.

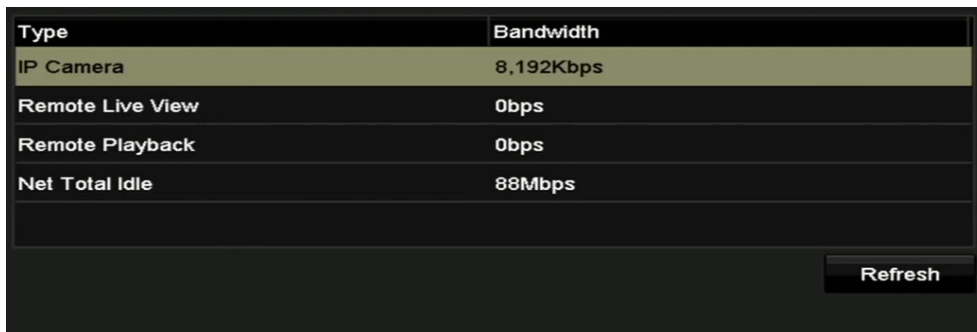


Figure 196, Network Stat. Interface

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

Chapter 12 HDD Management

12.1 Initializing HDDs

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

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

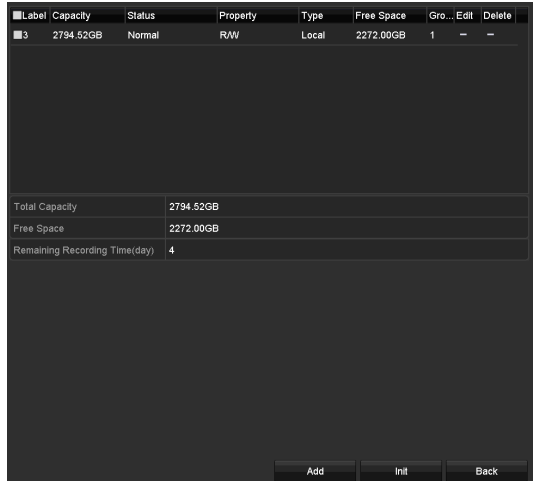


Figure 197, HDD Information Interface



NOTE

You can view the Total Capacity, Free Space, and Remaining Recording Time of the HDD. The algorithm of the Remaining Recording Time uses average bit rate for the channel enabling smart encoding to raise accuracy.

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

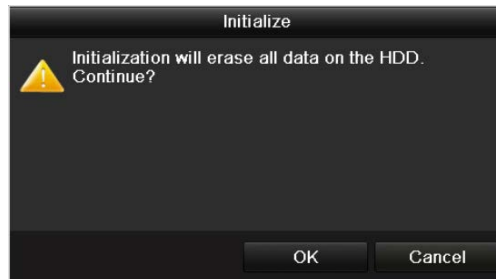


Figure 198, Confirm Initialization

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

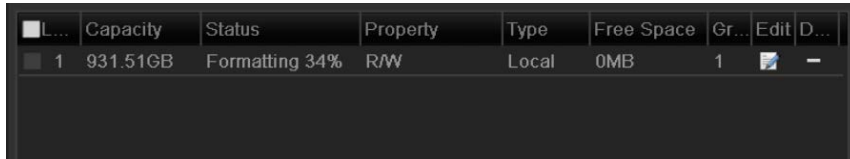


Figure 199, Start Initialization

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

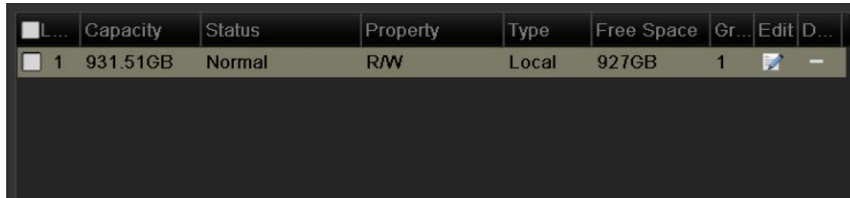


Figure 200, HDD Status Changes to Normal



NOTE

Initializing the HDD will erase all data on it.

HDDs that haven't been accessed for a long period of time can be configured to sleep, thus decreasing the device's power consumption and extending the life of the HDDs.

- Click Menu > HDD > Advanced

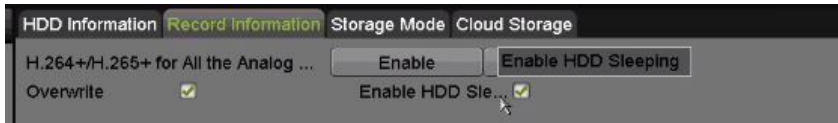


Figure 201, Enable HDD Sleeping

- Check the **Enable HDD Sleeping** checkbox (default), and the HDDs that haven't been accessed for a long period of time will be set to sleep.
- Uncheck the **Enable HDD Sleeping** checkbox, and the HDDs will be set to work at all times.

12.2 Managing Network HDD

You can add an allocated NAS or IP SAN disk to the DVR and use it as a network HDD.

- Enter the HDD Information interface, Menu > HDD > General.

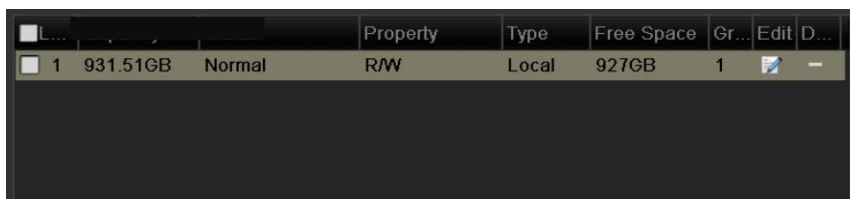


Figure 202, HDD Information Interface

- Click **Add** to enter the **Add NetHDD** interface, as shown in 0.



Figure 203, NetHDD Information Interface

3. Add the allocated NetHDD.
4. Set the type to NAS or IP SAN.
5. Configure the NAS or IP SAN settings.
 - **Adding a NAS Disk**
 - a) Enter the NetHDD IP address in the text field.
 - b) Click **Search** to search the available NAS disks.
 - c) Select the NAS disk from the list, or enter the directory in the **NetHDD Directory** text field.
 - d) Click **OK** to add the configured NAS disk.



NOTE

Up to eight NAS disks can be added.

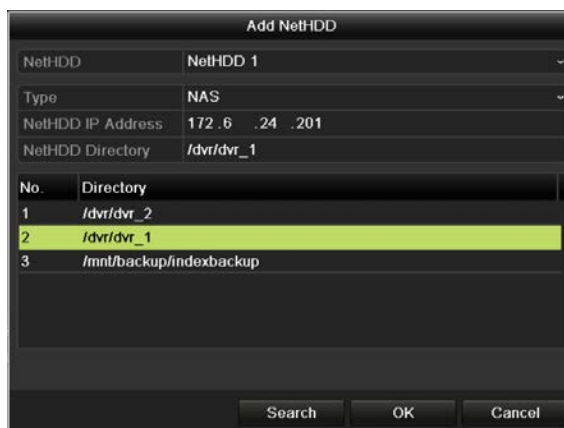


Figure 204, Add NAS Disk

- **Adding an IP SAN**
 - a) Enter the NetHDD IP address in the text field.
 - b) Click **Search** for the available IP SAN disks.

- c) Select the IP SAN disk from the list.
- d) Click **OK** to add the selected IP SAN disk.



NOTE

Up to eight IP SAN disks can be added.

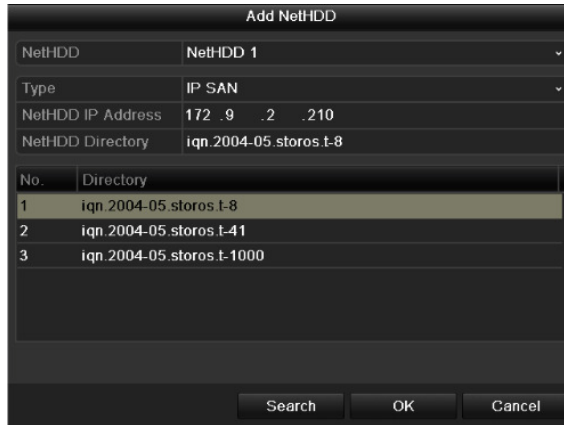


Figure 205, Add IP SAN Disk

- 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.

<input type="checkbox"/> L...	Capacity	Status	Property	Type	Free Space	Gr...	Edit	D...
<input checked="" type="checkbox"/> 1	931.51GB	Normal	R/W	Local	906GB	1		-
<input checked="" type="checkbox"/> 17	40,000MB	Normal	R/W	IP SAN	22,528MB	1		

Figure 206, Initialize Added NetHDD

12.3 Managing HDD Groups

12.3.1 Setting HDD Groups

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.
- 2. Set the **Mode** to Group, as shown in 0.

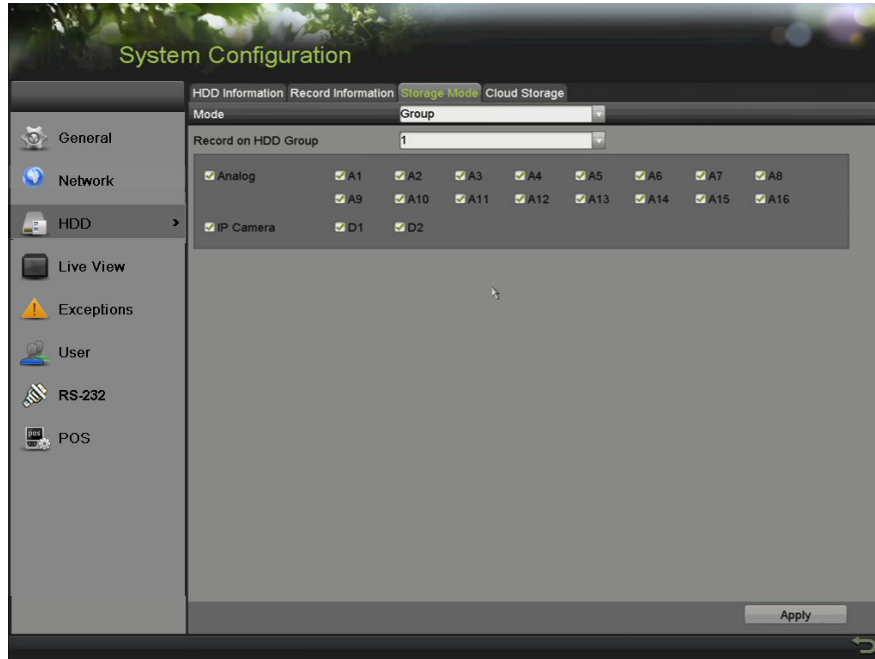


Figure 207, Storage Mode Interface

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

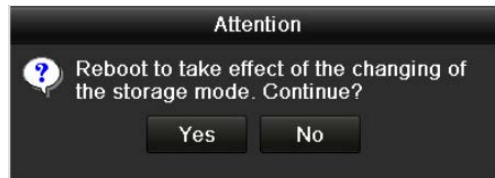



Figure 208, Attention for Reboot

4. Click **Yes** to reboot the device to activate the changes.
5. After device reboot, enter the HDD Information interface, Menu > HDD > General.
6. Select HDD from the list and click the  icon to enter the **Local HDD Settings** interface, as shown in 0.

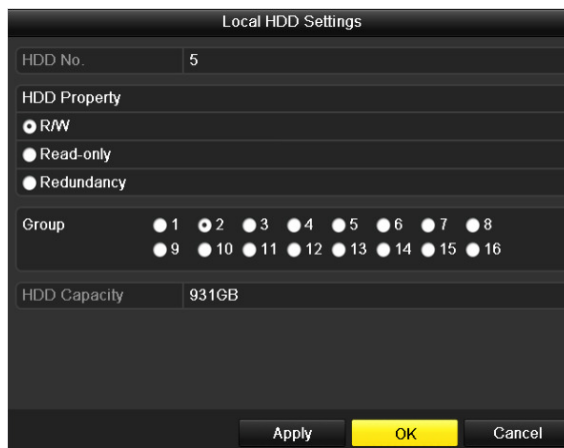


Figure 209, Local HDD Settings Interface

7. Select the Group number for the current HDD.



The default group no. for each HDD is 1.

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



Figure 210, Confirm HDD Group Settings

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

12.3.2 Setting HDD Property

The HDD can be set to redundancy, read-only, or read/write (R/W). Before setting the HDD property, set the storage mode to Group (see steps 1 – 4 of Chapter 12.3.1 Setting HDD Groups).

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

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

1. Enter the HDD Information interface, Menu > HDD > General.
2. Select HDD from the list and click to enter the **Local HDD Settings** interface.



Figure 211, Set HDD Property

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



At least two hard disks must be added to the DVR when to set an HDD to Redundancy, with one HDD set to R/W property.

12.4 Configuring Quota Mode

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

1. Enter the **Storage Mode** interface, Menu > HDD > Advanced.
2. Click the **Storage Mode** tab.
3. Set the **Mode** to Quota, as shown in 0.



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

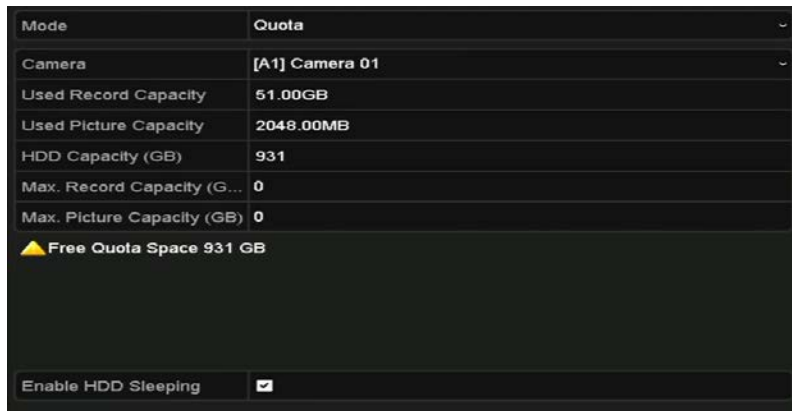


Figure 212, Storage Mode Settings Interface

4. Select a camera for which you want to configure quota.
5. Enter the storage capacity in the **Max. Record Capacity (GB)** text field.
6. Copy the current camera's quota settings to other cameras if desired. Click **Copy** to enter the **Copy Camera** interface, as shown in 0.

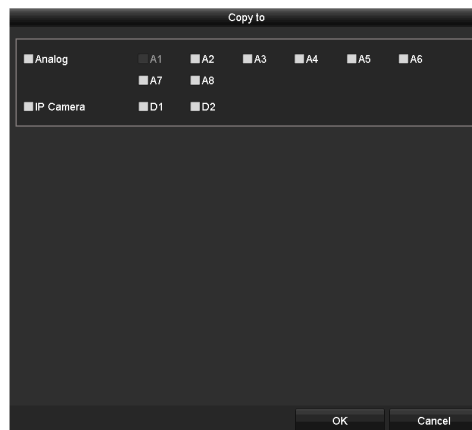


Figure 213, Copy Settings to Other Camera(s)

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



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

12.5 Configuring Cloud Storage

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

1. Enter the Cloud Storage interface, Menu > HDD > General > Cloud Storage.
2. Check the **Enable Cloud** checkbox to enable the feature.
3. Set the **Cloud Type** from the drop-down list to One Drive, Google Drive, or Drop Box.

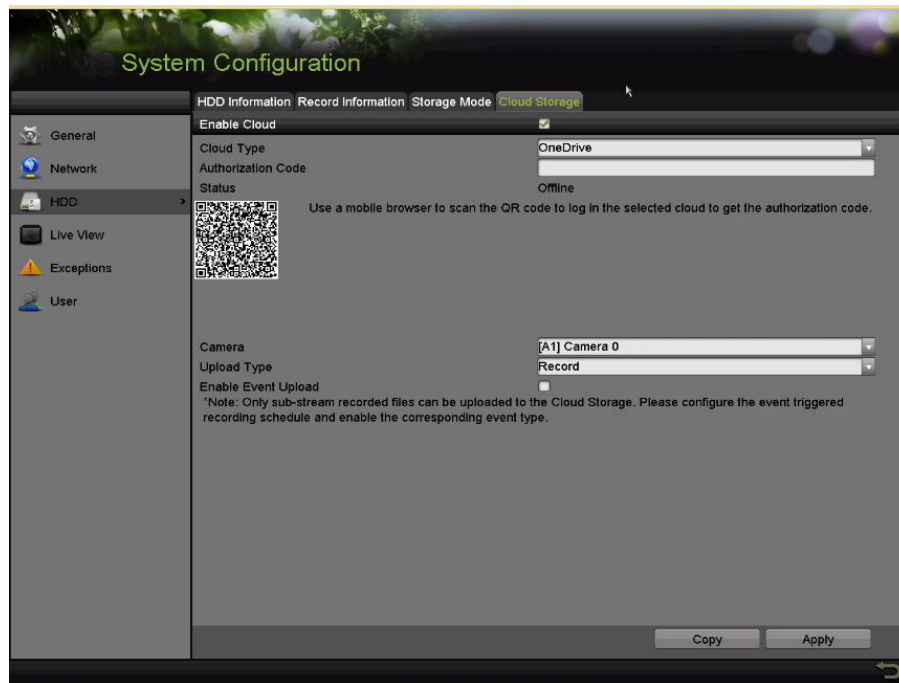


Figure 214, Cloud Storage Interface

4. Follow the prompts and use a mobile browser to scan the QR code to log in the selected cloud to get the authentication code. Then copy the authentication code to the **Authentication Code** text field.
5. Click **Apply**
6. Go back to the main menu.

7. Enter the cloud storage interface again about 20s later. When the **Status** shows online, it indicates successful registration.
8. Configure the recording schedule.
 - a) Go back to enter the record interface.
 - b) Choose a camera from the **Camera** drop-down list.
 - c) Check the **Enable Schedule** checkbox to enable the schedule recording. For detailed recording schedule information, refer to *5.2 Configuring Recording Schedule*.



Figure 215, Record Schedule

9. Upload the event triggered recording files to the cloud storage.
 - a) Go back to enter the cloud storage interface.
 - b) Select the camera you have set in the recording schedule interface.
 - c) Select the upload type in the **Upload Type** text filed.
 - d) Check the **Enable Event Upload** checkbox.
 - e) Click **Apply** to finish the settings.



Figure 216, Upload to Cloud Storage Interface



Only sub-stream record files can be uploaded to Cloud Storage.

Configure the event triggered recording schedule and enable the corresponding event type.

- f) (Optional) Click **Copy** to copy the cloud storage settings to other cameras. You can also click the Analog/IP Camera checkbox to select all cameras.

10. Click **OK** to go back to the cloud storage interface and click **Apply** to finish the settings.



Figure 217, Copy to Interface

12.6 Checking HDD Status

Check the status of installed HDDs so as to take immediate maintenance in case of HDD failure.

- **Checking HDD Status in HDD Information Interface**

1. Enter the HDD Information interface, Menu > System Configuration > HDD.
2. Check the status of each HDD that is displayed on the list, as shown in 0.

L...	Capacity	Status	Property	Type	Free Space	Gr...	Edit	D...
1	931.51GB	Normal	R/W	Local	900GB	1		-
17	199.97GB	Normal	Redundancy	NAS	182GB	1		

Figure 218, View HDD Status (1)



If the HDD status is *Normal* or *Sleeping*, it works 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 System Information Interface**

1. Enter the **System Information** interface, Menu > Maintenance > System Info.
2. Click the **HDD** tab to view the status of each HDD displayed on the list, as shown in 0.

Label	Status	Capacity	Free Space	Property	Type	Group
1	Normal	931.51GB	900GB	R/W	Local	1
17	Normal	199.97GB	182GB	Redundancy	NAS	1

Figure 219, View HDD Status (2)

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

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

1. Enter the **HDD Detect** interface, Menu > Maintenance > HDD Detect.
2. Click the **S.M.A.R.T. Settings** tab to enter the interface.
3. Select the HDD to analyze.
4. Click Test to start analyzing the selected HDD.
5. View the HDD's S.M.A.R.T. information list once the analysis is complete.



NOTE

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



Figure 220, S.M.A.R.T. Settings Interface

12.8 Detecting Bad Sectors

You can detect HDD bad sectors.

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



Figure 221, Bad Sector Detecting

4. Click **Pause** to pause the detection, and click **Resume** to resume the detection.
5. If the HDD returns error information, click **Error Info** to view the information.

12.9 Configuring HDD Error Alarms

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. Check the checkbox(s) below to select the linkage action(s) for HDD error, as shown in Figure 12-26.
 - **Audible Warning**
 - **Notify Surveillance Center**
 - **Send E-mail**
 - **Trigger Alarm Output**



Figure 222, Configure HDD Error Alarm

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

Chapter 13 Camera Settings

13.1 Assigning 5 MP Long Distance Transmission

Use this section to set 5 MP long distance transmission to extend the range of 5 MP cameras.

1. Enter the Signal Input Status interface, Menu > Cameras Setup > Signal Input Status.
2. Check the 5MP Long Distance Transmission checkbox to display the analog camera choices window.
3. Check the analog camera checkboxes that you wish to apply 5 MP Long Distance Transmission.
4. Click **Apply**.

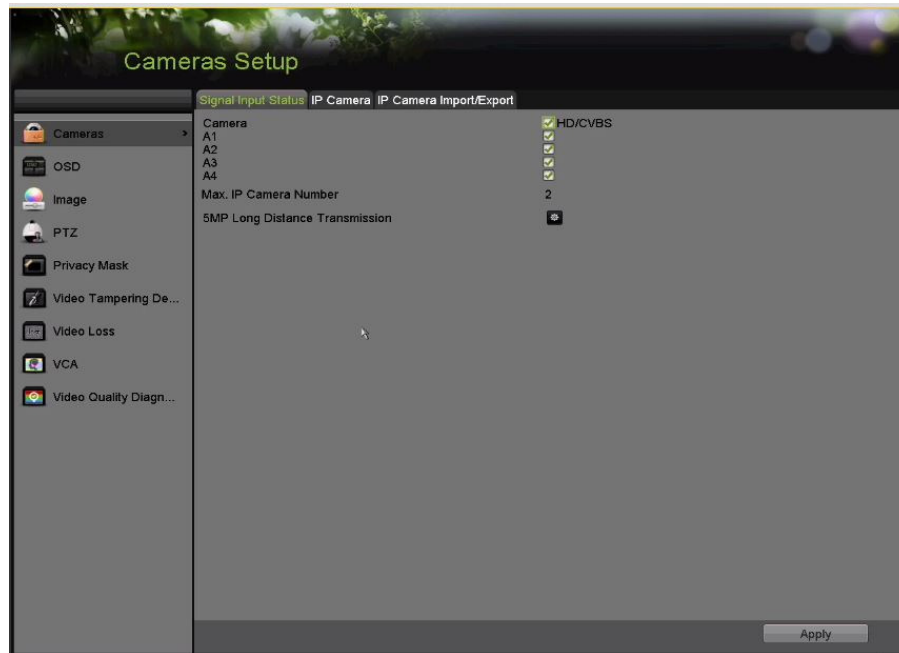


Figure 223, Menu > Cameras Setup > Cameras > Signal Input Status



NOTE

5MP Long Distance Transmission is the only setting functional on this page for this DVR series.



Figure 224, 5 MP Long Distance Transmission Analog Camera Choices

13.2 Configuring OSD Settings

Configure the OSD (On-Screen Display) settings for the camera, including date/time, camera name, etc.

1. Enter the OSD Configuration interface, Menu > Cameras Setup > OSD.
2. Select the camera to configure OSD settings.
3. Edit the **Camera Name** in the text field.
4. Configure the **Display Name**, **Display Date**, and **Display Week** by checking the checkbox.
5. Select the **Date Format**, **Time Format**, **Display Mode**, and the **OSD Font** (this setting is available in the Web interface only).

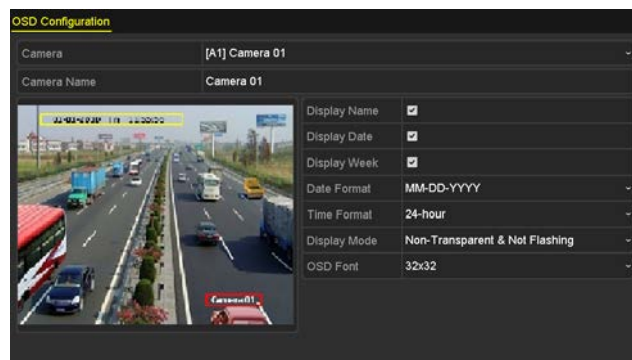


Figure 225, OSD Configuration Interface

6. Use the mouse to drag the text frame on the preview window to adjust the OSD position.
7. Copy Camera Settings
 - a) To copy the OSD settings of the current camera to other cameras, click **Copy** to enter the **Copy Camera** interface, as shown in 0.

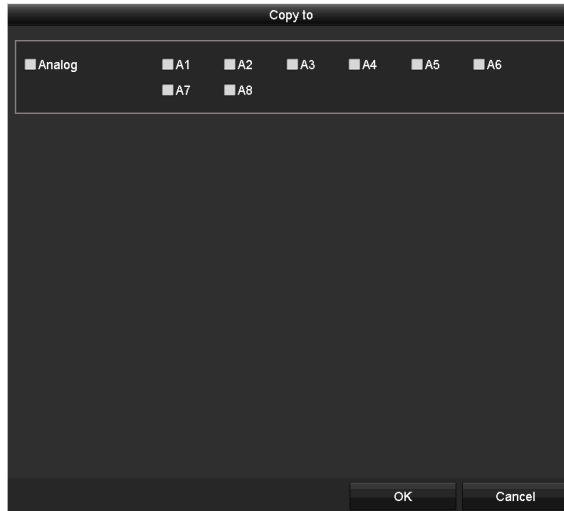


Figure 226, Copy Settings to Other Cameras

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

13.3 Configuring Privacy Mask

Configure the four-sided privacy mask zones that cannot be viewed or recorded by the operator.

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



Figure 227, 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 mask zones can be configured, and the size of each area can be adjusted.

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

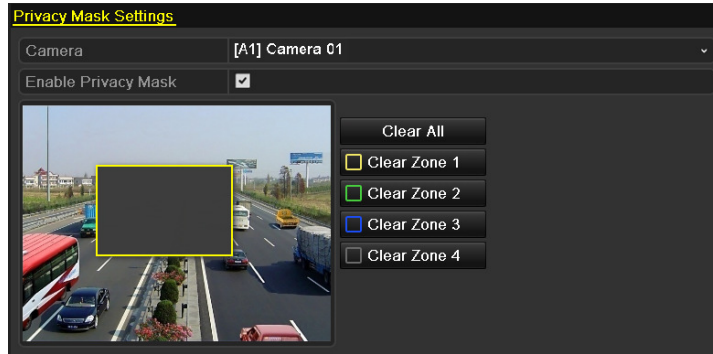


Figure 228, Set Privacy Mask Area

6. Click **Copy** to copy the privacy mask settings of the current camera to other cameras. Refer to step 7 of *Chapter •Configuring OSD Settings*.
7. Click **Apply** to save the settings.

13.4 Configuring Video Parameters

13.4.1 Configuring Image Settings

1. Enter the Image Settings interface, Menu > Cameras Setup > Image > Image Settings.
2. Select the **Image Settings** tab.

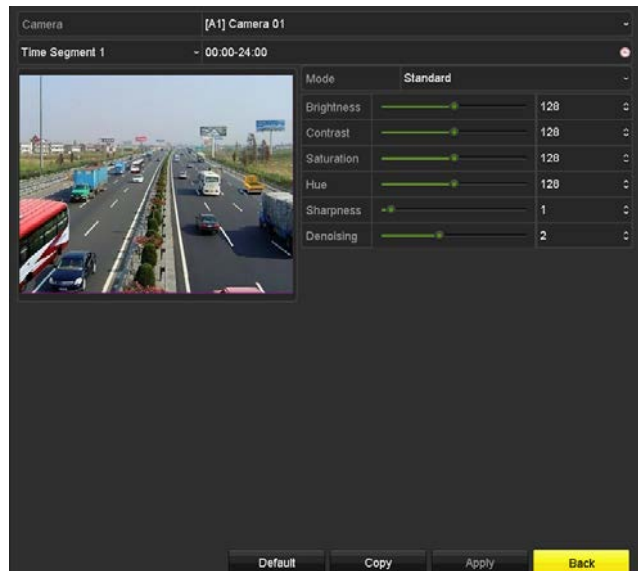


Figure 229, Image Settings Interface (Analog Camera)



Figure 230, Image Settings Interface (IP Camera)

3. Select the camera to set image parameters.
4. Select the period name in the drop-down list (two periods are provided).



NOTE

Time periods cannot overlap.

5. Select the for analog camera mode from the **Mode** drop-down list.

- **Standard**
- **Indoor**
- **Dim Light**
- **Outdoor**

6. Adjust the image parameters according to actual needs.

- **Analog Cameras**

- a) Brightness
- b) Contrast
- c) Saturation
- d) Hue
- e) Sharpness
- f) De-noising

- **IP Cameras**

- a) Brightness
- b) Contrast
- c) Saturation

**NOTE**

Click **Restore** to reset the parameters to the default settings.

7. Click **Copy** to copy the image settings of the current camera to other cameras.
8. Click **Apply** to save the settings.

13.4.2 Configuring Camera Parameters Settings

1. Enter the Image Settings interface, Menu > Cameras Setup > Image > Camera Parameters Settings.
2. Select the Camera Parameters Settings tab.

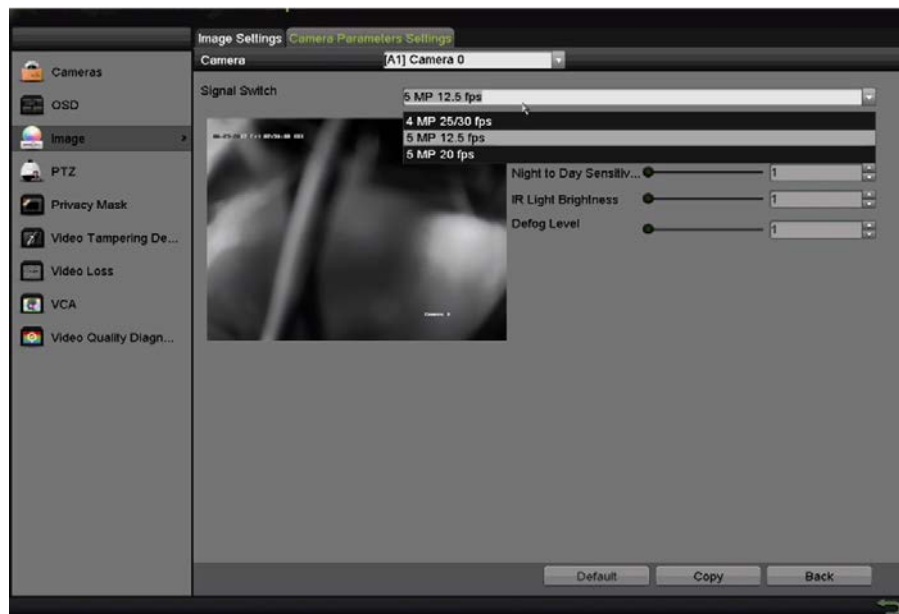


Figure 231, Camera Parameters Settings

3. Select the **Camera** from the drop-down list.
4. (Optional) Switch the 4 MP or 5 MP signal from the **Signal Switch** drop-down list. 4 MP 25/30 fps, 5 MP 12.5 fps, and 5 MP 20 fps are selectable. The 4 MP 25 fps and 4 MP 30 fps signals are self-adaptive for the camera.
5. (Optional) Check the **Enable Defog** checkbox to enable the defog function of the selected camera, and set the **Defog Level** from 1 to 4.
6. (Optional) Adjust the other camera parameters including **Day to Night Sensitivity**, **Night to Day Sensitivity**, and **IR Light Brightness** for the analog cameras. You can also click **Default** to set the parameters to the default settings.
7. (Optional) Click **Copy** to copy the parameters of the current camera to other analog cameras.
8. Click **Apply** to save the settings.

**NOTE**

The camera parameters settings are applicable only to analog cameras.

The 4 MP/5 MP Signal Switch, Defog, Day to Night Sensitivity, Night to Day Sensitivity, and IR Light Brightness functions must be supported by the connected analog camera. You cannot set the parameters if the connected analog camera does not support them or there is no video signal.

The parameters are saved to the connected analog camera and are not saved to the DVR.

The default value of Day to Night Sensitivity, Night to Day Sensitivity, and IR Light Brightness is 5. The effective value ranges from 1 to 9.

If you exit from the interface and enter it again, the parameters displayed are those you last set.

The DVR connects to analog cameras via Hikvision-C protocol and there is no response mechanism; even if the Hikvision-C is abnormal, the parameters are still displayed as having been successfully set.

Chapter 14 DVR Management and Maintenance

14.1 Viewing System Information

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

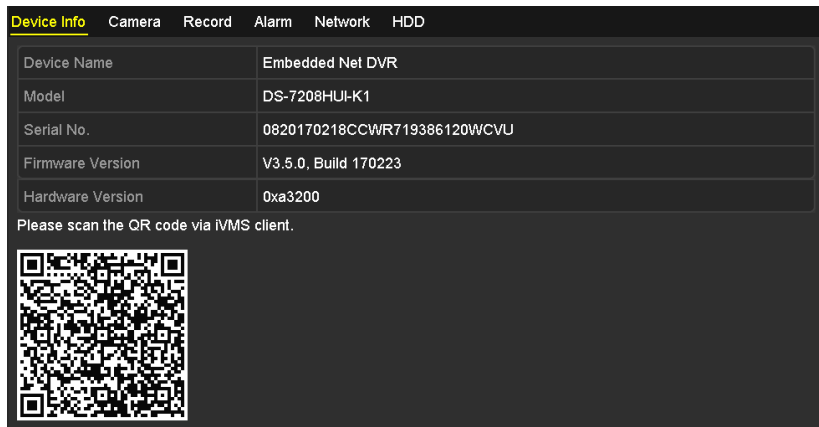


Figure 232, System Information Interface

14.2 Searching Log Files

The operation, alarm, exception, and DVR 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 Start Time, End Time, Major Type, and Minor Type.
3. Click **Search** to start searching log files.
4. The matched log files will be displayed on the list shown below.



NOTE

Up to 2,000 log files can be displayed each time.

No.	Major Type	Time	Minor Type	Parameter	Play	Details
1	Information	10-07-2015 09:53:59	Local HDD Infor...	N/A	—	✓
2	Operation	10-07-2015 09:53:59	Power On	N/A	—	✓
3	Information	10-07-2015 09:54:05	Start Recording	N/A	⏮	✓
4	Operation	10-07-2015 09:54:08	Local Operation:...	N/A	—	✓
5	Information	10-07-2015 09:54:25	HDD S.M.A.R.T.	N/A	—	✓
6	Information	10-07-2015 09:54:32	Start Recording	N/A	⏮	✓
7	Operation	10-07-2015 09:54:32	Local Operation:...	N/A	⏮	✓
8	Operation	10-07-2015 09:54:32	Local Operation:...	N/A	⏮	✓
9	Exception	10-07-2015 09:55:32	IP Camera Disco...	N/A	⏮	✓
10	Information	10-07-2015 10:04:09	System Running...	N/A	—	✓

Total: 2000 P: 1/20

Export Back

Figure 234, Log Search Results

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

Log Information	
Time	11-12-2015 08:52:15
Type	Information--Local HDD Information
Local User	N/A
Host IP Address	N/A
Parameter Type	N/A
HDD	1
Description:	
HDD: 1	
Serial: WD-WCAV58050978	
Firmware: 01.00A01	
Model: WDC WD10EVVS-63M5B0	

Previous Next OK

Figure 235, Log Information Interface

6. To export the log files, click **Export** to enter the Export menu, as shown in Figure 14-5.



Figure 236, Export Log Files

7. Select the backup device from the **Device Name** drop-down list.
8. Click **Export** to export the log files to the selected backup device.

**NOTE**

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

Connect the backup device to the DVR before operating log export.

The log files exported to the backup device are named by export time, e.g., *20110514124841logBack.txt*.

14.3 Importing/Exporting IP Camera Info

The added IP camera information can be generated into a Microsoft 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 to add or delete content, and the settings can be copied to other devices by importing the Excel file.

1. Enter the camera management interface, Menu > Camera > Camera.
2. Click **the IP Camera Import/Export** tab, and detected plugged external devices appears.
3. Click **Export** 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 **Import**. After the importing process is completed, you must reboot the DVR.

14.4 Importing/Exporting Configuration Files

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

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

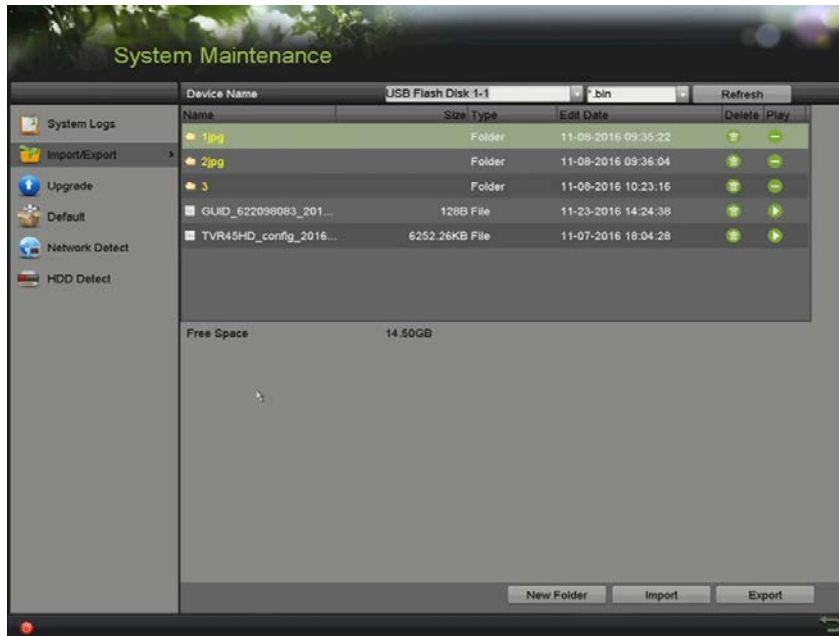


Figure 237, Import/Export Configuration File

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

**NOTE**

After finishing importing the configuration files, the device will reboot automatically.

14.5 Upgrading System

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

14.5.1 Upgrading by Local Backup Device

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

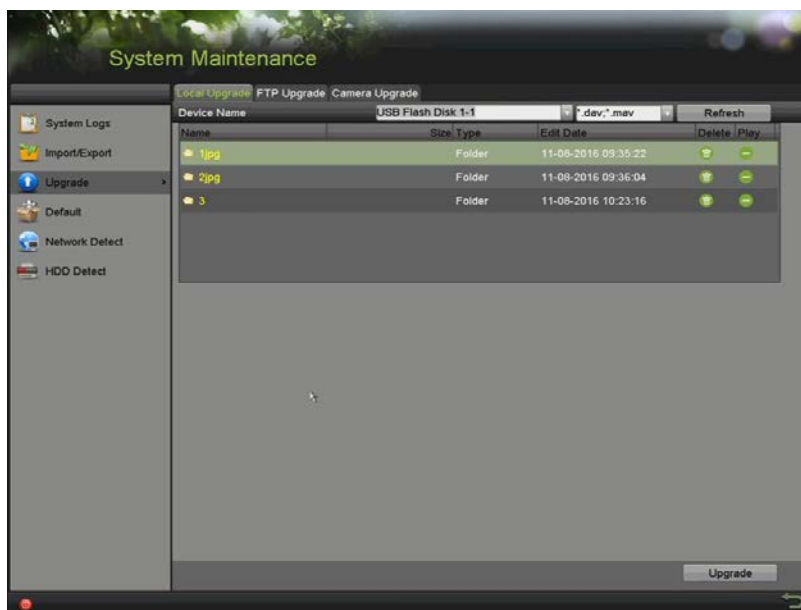


Figure 238, Local Upgrade Interface

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

14.5.2 Upgrading by FTP

Configure PC (running FTP server) and DVR to the same Local Area Network. Run the third-party TFTP software on the PC and copy the firmware into the root directory of TFTP.

1. Enter the **Upgrade** interface, Menu > Maintenance > Upgrade.
2. Click the **FTP** tab to enter the **Local Upgrade** interface, as shown in Figure 16-8.

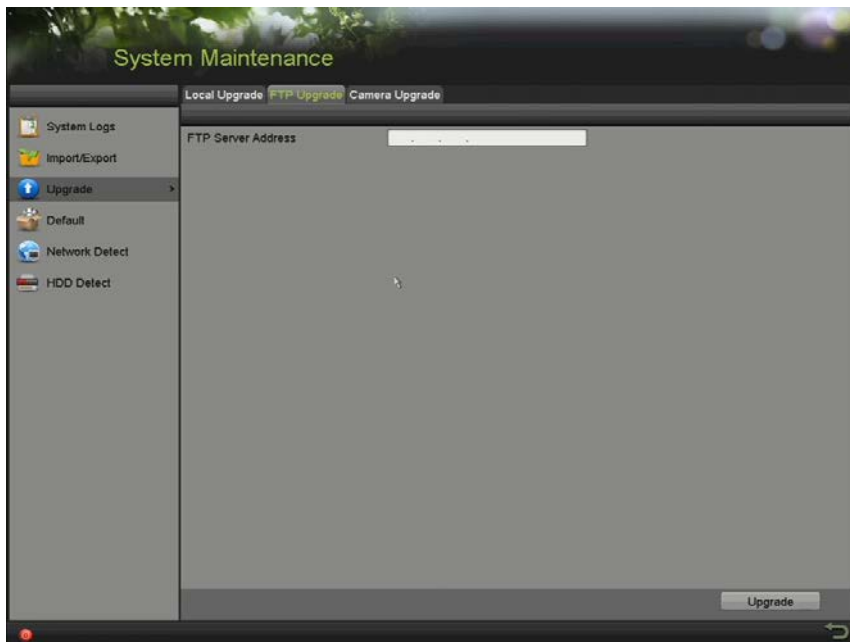


Figure 239, FTP Upgrade Interface

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

14.6 Upgrading Camera

1. You can upgrade multiple connected analog cameras supporting TurboHD signal simultaneously with the DVR.
2. Enter the **Camera Upgrade** interface, Menu > Maintenance > Upgrade > Camera Upgrade.

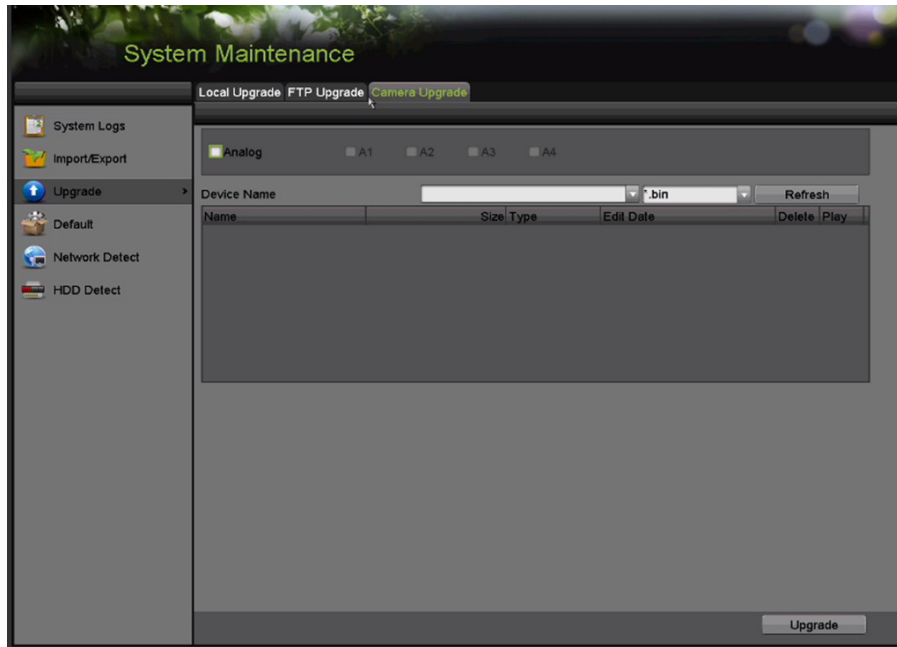


Figure 240, Camera Upgrade

3. Check the analog checkbox.
4. Check the camera checkbox(es) to select cameras to upgrade.



NOTE

The analog camera must support TurboHD signal.

5. Select the update file from the backup device.
6. Click **Upgrade** to start upgrading.

14.7 Restoring Default Settings

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

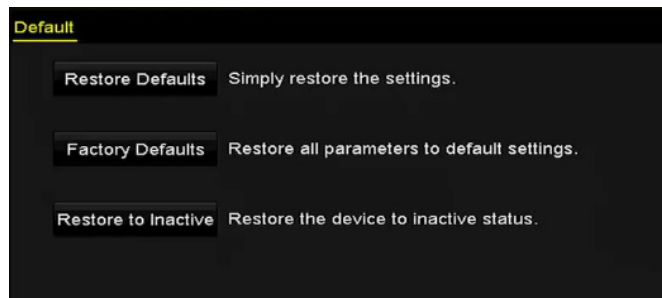


Figure 241, Restore Defaults

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 inactive status.
3. Click **OK** to restore the default settings.



NOTE

The device will reboot automatically after restoring the default settings.

Chapter 15 Others

15.1 Configuring General Settings

This section explains how to configure output resolution, system time, mouse pointer speed, etc.

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

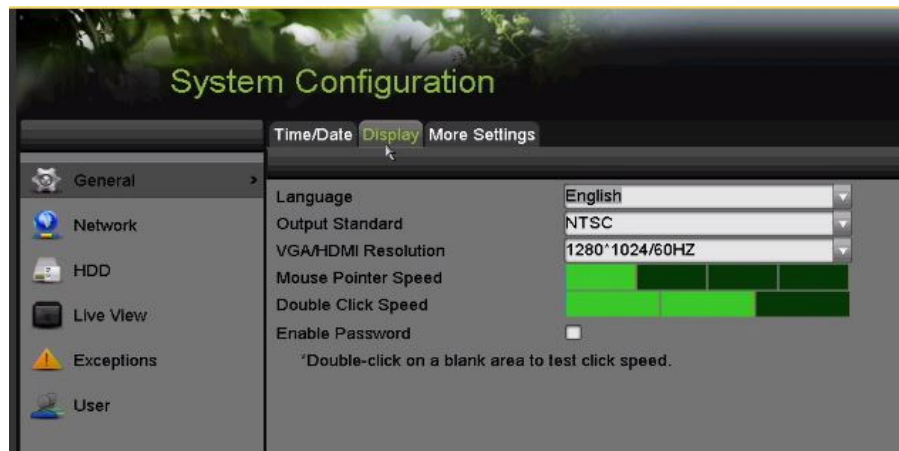


Figure 242, General Settings Interface

3. Configure the following settings:
 - **Language:** The default language used is *English*.
 - **Output Standard:** Select the output standard to be PAL or NTSC.
 - **VGA/HDMI Resolution:** Select the output resolution, which must be the same with the resolution of the VGA/HDMI display.
 - **Mouse Pointer Speed:** Set the speed of mouse pointer; four levels are configurable.
 - **Double Click Speed:** Set the speed of mouse double-click; three levels are configurable.
 - **Enable Password:** Enable/disable the use of the login password.

NOTE

If you check the **Enable Password** checkbox, every time you log in to the DVR, the Unlock Pattern interface will pop up. If you uncheck the **Enable Password** checkbox, when you log in to the DVR, the Unlock Pattern interface will not pop up.

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

15.2 Configuring DST Settings

1. Enter the **General Settings** interface, Menu > System Configuration > General > Time/Date.

2. Choose the **DST Settings** tab.



Figure 243, Time/Date Setting

3. Check the Enable DST checkbox.
4. Click **CUSTOMIZE**.



Figure 244, 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 choose the date of the DST period.

15.3 Configuring More Settings

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

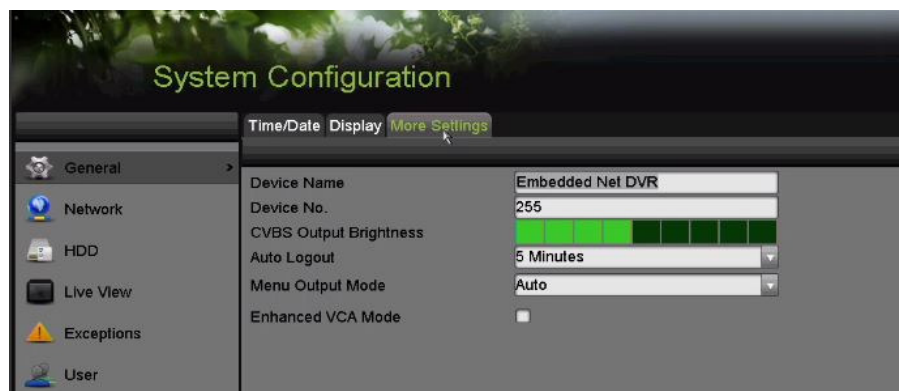


Figure 245, More Settings Interface

3. Configure the following settings:

- **Device Name:** Edit the DVR name.
- **Device No.:** Edit the DVR serial number. The Device No. can be set in the range of 1 to 255 (default No. is 255).
- **Auto Logout:** Set timeout time for menu inactivity. E.g., when the timeout time is set to *5 Minutes*, the system will exit from the current operation menu to the live view screen after 5 minutes of menu inactivity.
- **CVBS Output Brightness:** Adjust the video output brightness via the CVBS interface.
- **Menu Output Mode:** You can choose the menu display on different video output.
- **Auto and HDMI/VGA** are selectable.
- **Enhanced VCA Mode:** DS-72xxHUI-Kx Series DVRs support Enhanced VCA Mode, which allows line crossing detection and intrusion detection on all channels. Enhanced VCA Mode conflicts with 2K/4K output and 4 MP/5 MP signal input. Enable or disable VCA mode as needed.



NOTE

DS-72xxHQI-Kx Series DVRs don't support Enhanced VCR Mode.

The pop-up will only show mode(2),

- **Enable Enhanced VCA Mode**

- 1) Check the checkbox to enable enhanced VCA mode.
- 2) Click **Apply** and the attention box pops up as below.

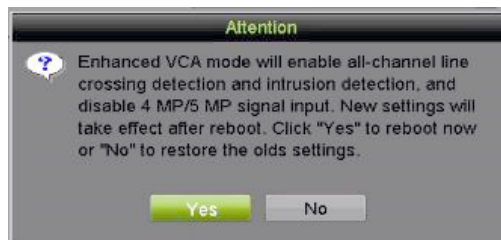


Figure 246, Enable Enhanced VCA Mode (1)

- 3) Click **Yes** to apply the function and reboot the device.



NOTE

Line crossing detection and intrusion detection will function on all channels.

If you have configured 2K/4K output, or connected 4 MP/5 MP signal input, when you enable Enhanced VCA Mode and the device reboots, the output resolution will decrease to 1080p and the 4 MP/5 MP signal input will display no video.

- **Disable Enhanced VCA Mode (Default)**

- 1) Uncheck the checkbox to disable enhanced VCA mode.
- 2) Click **Apply** and the attention box pops up as below.

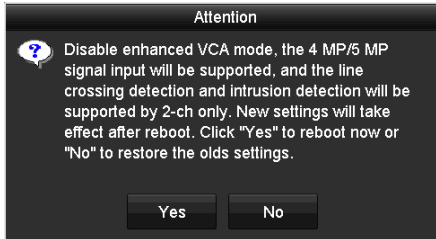


Figure 247, Disable Enhanced VCA Mode (2)

- 3) Click **Yes** to apply the function and reboot the device.
- 4) Click **Apply** to save the settings.

 **NOTE**

Line crossing detection and intrusion detection will be supported only on two channels. 2K/4K output and 4 MP/5 MP input signals will be supported.

15.4 Managing User Accounts

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

15.4.1 Adding a User

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

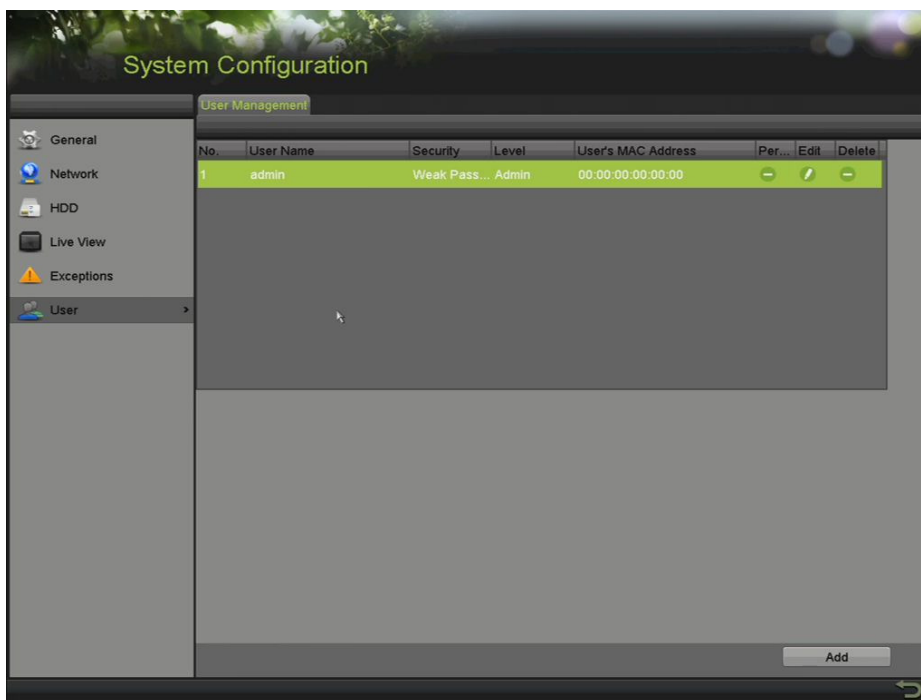


Figure 248, User Management Interface

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

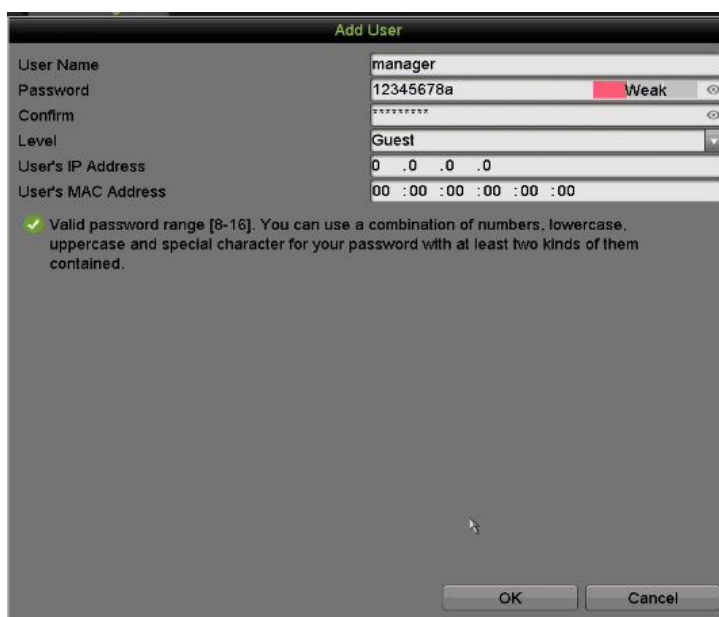


Figure 249, Add User Menu

3. Enter information for the new user:
 - **Password:** Set the password for the user account.

**WARNING**

STRONG PASSWORD RECOMMENDED – We highly recommend you create a strong password of your own choosing (using a minimum of 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 you reset your password regularly. Resetting the password monthly or weekly can better protect your product.

- **Level:** Set the user level to Operator or Guest. Different user levels have different operating permissions.
 - **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 has only the local/remote playback in the Camera Configuration by default.
 - **IP Address:** If this is enabled and configured only computers with this IP address can access the DVR. This can be a single computer or multiple computers if they share the same public facing IP address.
 - **User's MAC Address:** This is the MAC address of the remote PC that logs onto the DVR. If it is configured and enabled, it allows only the remote user with this MAC address to access the DVR.
4. Click **OK** to save the settings and go back to the **User Management** interface. The added new user will be displayed on the list, as shown in 0.

No.	User Name	Security	Level	User's MAC Address	Per...	Edit	Delete
1	admin	Strong Pas...	Admin	00:00:00:00:00:00	–		–
2	example 1	Strong Pas...	Guest	00:00:00:00:00:00			

Figure 250, Added User Listed in User Management Interface

5. Assign permissions for the added user.
- 1) Select the user from the list and then click to enter the **Permission Settings** interface, as shown in 0.



Figure 251, User Permission Settings Interface

- 2) Set the operating permissions for Local Configuration, Remote Configuration, and Camera Configuration for the user.
 - **Local Configuration**
 - Local Log Search: Searching and viewing logs and system information of device.
 - Local Parameters Settings: Configuring parameters, restoring factory default parameters, and importing/exporting configuration files.
 - Local Camera Management: Enable and disable analog camera(s). Add, delete, and edit network camera(s). Supported by the HDVR Series.
 - Local Advanced Operation: Operating HDD management (initializing HDD, setting HDD property), upgrading system firmware.
 - Local Shutdown /Reboot: Shutting down or rebooting the device.
 - **Remote Configuration**
 - Remote Log Search: Remotely view logs that are saved on the device.
 - Remote Parameters Settings: Remotely configure parameters, restore factory default parameters, and import/export configuration files.
 - Remote Camera Management: Remotely enable and disable analog camera(s), and add, delete, and edit network camera(s). Supported by the HDVR Series.
 - Remote Serial Port Control: Configure settings for RS-485 port.
 - Remote Video Output Control: Send remote control panel signal.
 - Two-way Audio: Realize two-way radio between the remote client and the device.
 - Remote Alarm Control: Remotely arm (notify alarm and exception message to the remote client) and control the alarm output.
 - Remote Advanced Operation: Remotely operate HDD management (initialize HDD, set HDD property), upgrade system firmware.
 - Remote Shutdown/Reboot: Remotely shut down or reboot the device.

- **Camera Configuration**

- Remote Live View: Remotely view live video of the selected camera(s).
- Local Manual Operation: Locally start/stop manual recording, picture capture, and alarm output of the selected camera(s).
- Remote Manual Operation: Remotely start/stop manual recording, picture capture, and alarm output of the selected camera(s).
- Local Playback: Locally play back recorded files of the selected camera(s).
- Remote Playback: Remotely play back recorded files of the selected camera(s).
- Local PTZ Control: Locally control PTZ movement of the selected camera(s).
- Remote PTZ Control: Remotely control PTZ movement of the selected camera(s).
- Local Video Export: Locally export recorded files of the selected camera(s).



NOTE

Local Camera Management is provided for IP cameras only.

6. Click **OK** to save the settings and exit.

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, as shown in 0.

No.	User Name	Security	Level	User's MAC Address	Per...	Edit	Delete
1	admin	Strong Pas...	Admin	00:00:00:00:00:00	-		-
2	example 1	Strong Pas...	Guest	00:00:00:00:00:00			

Figure 252, User List

3. Click to delete the selected user account.

15.4.3 Editing a User

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

1. Enter the **User Management** interface, Menu > Configuration > User.
2. Select the user to be edited from the list, as shown in 0.
3. Click to enter the **Edit User** interface, as shown in 0.

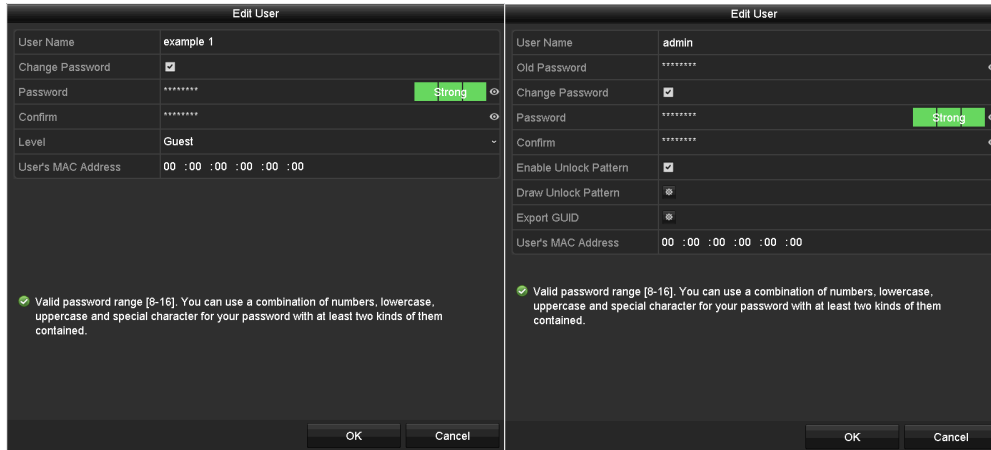


Figure 253, Edit User Interface

4. Edit the corresponding parameters.

- **Operator and Guest** – You can edit the user information, including user name, password, permission level, and MAC address. Check the **Change Password** checkbox 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 to change the password, and input the correct old password and the new password in the of Password and Confirm text fields.




WARNING

STRONG PASSWORD RECOMMENDED – We highly recommend 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 a high security system, resetting the password monthly or weekly can better protect your product.



NOTE

Hold down  and to see clear text of the password. Release the mouse and the password becomes hidden.

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.
- 3) Confirm the pattern again with the mouse.

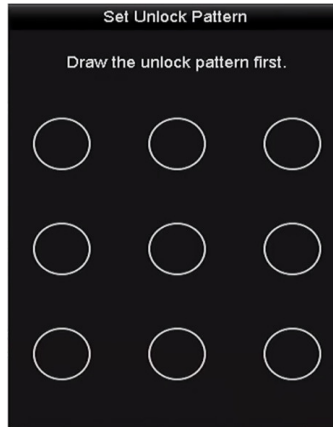


Figure 254, Set Unlock Patter for Admin User




6. (Optional) Click  after **Draw Unlock Pattern** to modify the pattern.
7. (Optional) Click  after **Export GUID** to pop up the Reset Password interface. Click **Export** to export GUID to the USB flash drive for retrieving the forgotten password.



Figure 255, Export GUID



NOTE
Enter the correct old *admin* password before exporting GUID.

8. Click **OK** to save the settings and exit from the menu.
9. (Optional) For an **Operator** or **Guest** user account, you can also click  on the **User Management** interface to edit the permissions.

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 DVR, with the main stream having a maximum resolution of 1080P and the sub-stream having a maximum resolution of CIF.
- **DVR:** Acronym for Digital Video Recorder. A DVR is device that is able to accept video signals from analog cameras, compress the signal and store it on its hard drives.
- **HDD:** Acronym for Hard Disk Drive. A storage medium which stores digitally encoded data on platters with magnetic surfaces.
- **DHCP:** Dynamic Host Configuration Protocol (DHCP) is a network application protocol used by devices (DHCP clients) to obtain configuration information for operation in an Internet Protocol network.
- **HTTP:** Acronym for Hypertext Transfer Protocol. A protocol to transfer hypertext request and information between servers and browsers over a network
- **PPPoE:** PPPoE, Point-to-Point Protocol over Ethernet, is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with ADSL services where individual users connect to the ADSL transceiver (modem) over Ethernet and in plain Metro Ethernet networks.
- **DDNS:** Dynamic DNS is a method, protocol, or network service that provides the capability for a networked device, such as a router or computer system using the Internet Protocol Suite, to notify a domain name server to change, in real time (ad-hoc) the active DNS configuration of its configured hostnames, addresses or other information stored in DNS.
- **Hybrid DVR:** A hybrid DVR is a combination of a DVR and NVR.
- **NTP:** Acronym for Network Time Protocol. A protocol designed to synchronize the clocks of computers over a network.
- **NTSC:** Acronym for National Television System Committee. NTSC is an analog television standard used in such countries as the United States and Japan. Each NTSC signal frame contains 525 scan lines at 60 Hz.
- **NVR:** Acronym for Network Video Recorder. An NVR can be a PC-based or embedded system used for centralized management and storage for IP cameras, IP Domes and other DVRs.
- **PAL:** Acronym for Phase Alternating Line. PAL is also another video standard used in broadcast televisions systems in large parts of the world. PAL signal contains 625 scan lines at 50Hz.
- **PTZ:** Acronym for Pan, Tilt, Zoom. PTZ cameras are motor driven systems that allow the camera to pan left and right, tilt up and down and zoom in and out.
- **USB:** Acronym for Universal Serial Bus. USB is a plug-and-play serial bus standard to interface devices to a host computer.

16.2 Troubleshooting

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

- **Possible Causes**

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

- **Possible Fixes**

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

- **There is a beeping sound after a new device 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 device or is defective

- **Possible Fixes**

1. Verify at least one HDD is installed in the device. If not, install a compatible HDD.



NOTE

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

2. If you do not want to install an HDD, select “Menu > Configuration > Exceptions,” and uncheck the “HDD Error” Audible Warning checkbox.
3. Verify the HDD is initialized by selecting “Menu > HDD > General.” If the HDD status is “Uninitialized,” check the corresponding HDD checkbox and click **Init**.
4. Verify the HDD is detected and is in good condition by selecting “Menu > HDD > General.” 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. If it is solved, finish the process. If not, contact our company.

- **Live View stuck when video outputs locally**

- **Possible Reasons**

- * The frame rate has not reached the real-time frame rate

- **Possible Fixes**

- 1. Check the parameters of Main Stream (Continuous) and Main Stream (Event). Select “Menu > Record > Parameters > Record,” and set the resolution of Main Stream (Event) the same as Main Stream (Continuous).
 2. Verify the frame rate is real-time frame rate. Select “Menu > Record > Parameters > Record,” and set the Frame Rate to Full Frame.
 3. Check if the fault is solved. If it is solved, finish the process. If not, contact our company.

- **When using the device to get Live View audio, there is no sound, there is too much noise, or the volume is too low**

- **Possible Reasons**

- * Cable between the pickup and camera is not connected well; impedance mismatches or incompatible
 - * The stream type is not set to “Video & Audio”

- **Possible Fixes**

- 1. Verify the cable between the pickup and camera is connected well; impedance matches is and compatible.
 2. Verify the setting parameters are correct. Select “Menu > Record > Parameters > Record,” and set the Stream Type as “Audio & Video.”
 3. Check if the fault is solved. If it is solved, finish the process. If not, contact our company.

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

- **Possible Reasons**

- * The frame rate is not the real-time frame rate
 - * The DVR supports up to 16-channel synchronized playback at 4CIF resolution. Frame extracting may occur during 16-channel synchronized playback at 720p resolution, which may cause image freezing.

- **Possible Fixes**

- 1. Verify the frame rate is real-time frame rate. Select “Menu > Record > Parameters > Record,” and set the Frame Rate to “Full Frame.”
 2. Verify the hardware can support the playback. Reduce the number of playback channels. Select “Menu > Record > Encoding > Record,” and set the resolution and bitrate to a lower level.
 3. Reduce the number of local playback channels. Select “Menu > Playback,” and uncheck unnecessary channels checkboxes.
 4. Check if the fault is solved. If it is solved, finish the process. If not, contact our company.

- **No record file found in the device's local HDD, and a "No record file found" prompt pops up when you search the record files**

- **Possible Reasons**

- * The time setting of system is incorrect
 - * The search condition is incorrect
 - * The HDD is error or not detected
1. Verify the system time setting is correct. Select "Menu > Configuration > General > General," and verify the "System Time" is correct.
 2. Verify the search condition is correct. Select "Playback," and verify the channel and time are correct.
 3. Verify the HDD status is normal. Select "Menu > HDD > General" to view the HDD status, and verify the HDD is detected and can be read and written normally.
 4. Check if the fault is solved. If it is solved, finish the process. If not, contact our company.