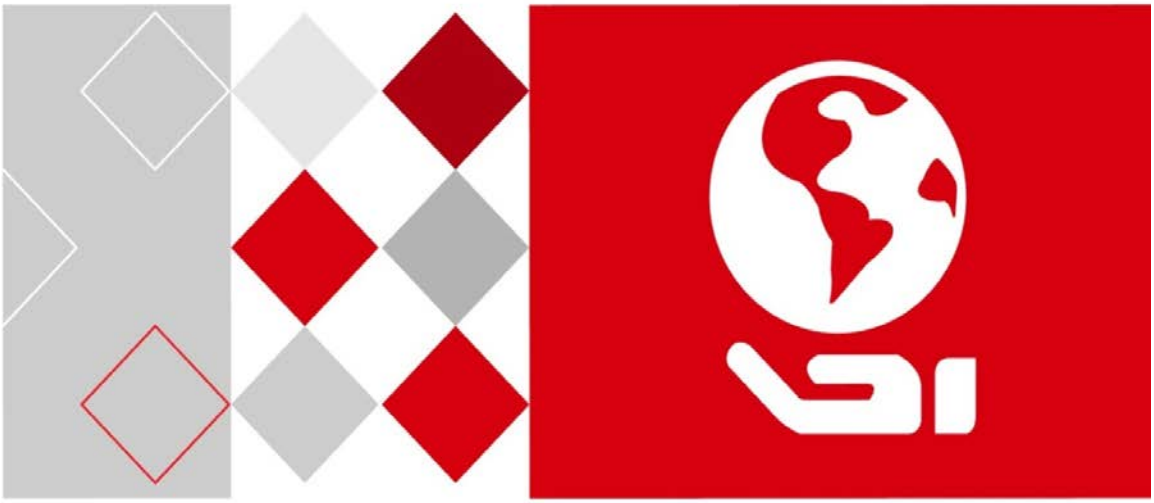
HIKVISION



Digital Video Recorder

DS-7204HTI-K1
DS-7208HTI-K2

User Manual

Hikvision USA Inc., 18639 Railroad St., City of Industry, CA 91748, USA • **Hikvision Canada**, 4848 rue Levy, Saint Laurent, Quebec, Canada, H4R 2P1

Telephone: +1-909-895-0400 • Toll Free in USA: +1-866-200-6690 • E-Mail: sales.usa@hikvision.com • www.hikvision.com.

About this Manual

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. Find the latest version in the company Web site at (http://overseas.hikvision.com/en/).

Please use this user manual under the guidance of professionals.

Illustrations in this manual are for illustration purposes only; your device's screens and/or hardware may differ.

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 RESPONSIBILITES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

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

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

Regulatory Information

FCC Information

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

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

FCC Conditions

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

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

EU Conformity Statement

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

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.

Symbol Conventions: The symbols that may be found in this document are defined as follows:

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. 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, 12 VDC, or 48 VDC according to the IEC60950-1 standard. 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.
- 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 contact the service center.

Preventive and Cautionary Tips

Before connecting and operating your device, 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.
- Use only a factory recommended HDD 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.

Mandatory Electrical Requirements

Hikvision requires the following conditions and equipment for all of its electronic equipment:

- **Grounding**

  Ensure good conductivity for all ground paths; examine ground path contact surfaces for defects, dirt, corrosion, or non-conductive coatings that may impede conductivity. Repair or clean contact surfaces as necessary to assure good metal-to-metal contact. Ensure fasteners are properly installed and tightened.

- **Electrical Wiring**

  Ensure your outlets are properly wired. They can be checked with an electrical outlet tester.

- **Surge Suppressor (Required)**

  Hikvision is not responsible for any damage to equipment caused by power spikes in the electrical power grid. Use of a surge suppressor meeting the following specifications is mandatory for all Hikvision electronic equipment:

- **Specifications**
  - Listed by Underwriter's Laboratories, meeting the UL 1449 Voltage Protection Rating (VPR)
  - Minimum protection of 1,000 joules or higher
  - Clamping voltage of 400 V or less
  - Response time of 1 nanosecond or less
- **Usage**
  - Surge suppressors must not be daisy chained with power strips or other surge suppressors

- **Maintenance**
  - Replace after a serious electrical event (e.g., lighting blew out a transformer down the street)
  - Replace yearly in storm-prone areas
  - Replace every two years as routine maintenance

Product Key Features

General

- Connectable to TurboHD and analog cameras
- Supports UTC protocol for connecting camera over coax
- Connectable to AHD cameras
- Connectable to HD-CVI cameras
- Connectable to IP cameras
- The analog signal inputs including TurboHD, AHD, HD-CVI, and CVBS can be automatically recognized without configuration
- Each channel supports dual-stream, and sub-stream supports up to WD1 resolution
- Supports up to 8 MP resolution of all the channels
- 5 MP long distance transmission can be enabled for analog cameras
- Independent configuration for each channel, including resolution, frame rate, bit rate, image quality, etc.
- The minimum frame rate for main stream and sub-stream is 1 fps
- 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, IR light brightness, day/night mode, and WDR switch 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
- 1/4/6/8/9/16/25/36 screen live view is supported, and the display sequence of screens is adjustable

NOTE

If video output resolution is set to 1024*768, if more than 16 windows set, the device will recommend switching to higher output resolution. If video output resolution is set to 1280*720 or 1280*1024, if more than 25 windows set, the same note will pop up.

- Live view screen can be switched in groups, manually, or automatic cycle. The automatic interval 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
- HTHI series DVR support full-channel line crossing detection and intrusion detection, and 2-ch sudden scene change detection.
- Privacy mask
- Several PTZ protocols (including Genetec Omnicast VMS) supported; PTZ preset, patrol and pattern
- Zoom in/out by clicking the mouse and PTZ tracing by dragging mouse
- If Hikvision CVBS camera is connected, you can control PTZ via coax and call the OSD of the camera

HDD Management

- Each disk with a maximum of 8 TB storage capacity
- Eight network disks (eight NAS disks, eight IP SAN disks or n NAS disks + m IP SAN disks (n+m ≤8)) can be connected
- Remaining recording time of the HDD can be viewed

- Supports cloud storage
- 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, Capture 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
- The device will note that the exported AVI video may have problems if the frame rates of the continuous and event recording are different
- 8 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 and captured pictures by events (alarm input/motion detection)
- Customization of tags, searching and playing back by tags
- Locking and unlocking of record files
- Local redundant recording and capture
- With TurboHD, AHD, or HD-CVI input, information including resolution and frame rate will be overlaid on the bottom right corner of live view for five seconds. With CVBS input, information such as NTSC or PAL will be overlaid on bottom right corner of live view for five 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
- Pause, fast forward, slow forward, skip forward, and skip backward when playback, locating by dragging the mouse on the progress bar
- 4/8/16-ch synchronous playback
- Manual capture, continuous capture of video images and playback of captured pictures

Backup

- Exports data by a USB, and SATA device
- Exports video clips when 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, 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 POS triggered alarm
- Supports coaxial alarm
- System will automatically reboot when a problem is detected in an attempt to restore normal functionality

- You can enable false alarm filer for the motion detection of the PIR cameras. Then only when the motion detection events and PIR events are both triggered, the motion detection alarm will be triggered.

Other Local Functions

- Manual and automatic video quality diagnostics
- Operable by mouse and remote control
- Three-level user management: admin user can create operating accounts and define their permissions, which includes channel access
- 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 analog cameras supporting TurboHD or AHD signal can be upgraded simultaneously via DVR.

Network Functions

- Self-adaptive 100M or 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 the Internet access risk and ask you to confirm the "Terms of Service" and "Privacy Statement" before enabling the service. You must 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 the record files, and downloading files broken transfer resume
- Remote parameters setup; remote import/export of device parameters
- Remote viewing of the device status, system logs and alarm status
- Remote keyboard operation
- Remote HDD formatting and program upgrading
- Remote system restart and shutdown
- 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, you can 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

1.1 Front Panel

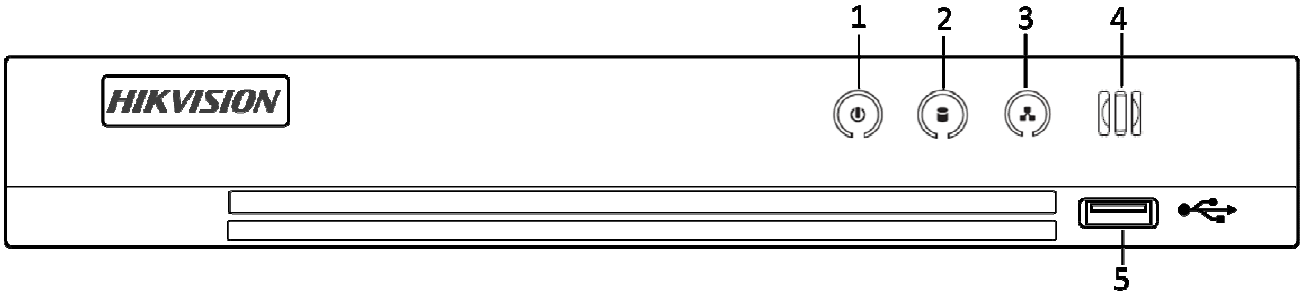


Figure 1-1 Front Panel

Table 1-1Front Panel Description

No.	Icon	Description
1		Turns white when DVR is powered up
2		Turns red when data is being read from or written to HDD
3		Flashes white when the network is well-connected
4		Receiver for IR remote control
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 1-2.

NOTE

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

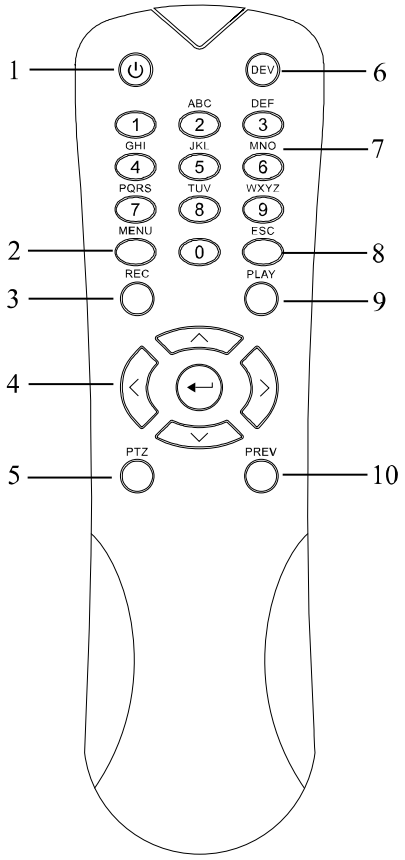


Figure 1-2 Remote Control

The keys on the remote control closely resemble the ones found on the front panel. Refer to Table 1-2.

Table 1-2 Description of the IR Remote Control Buttons

No.	Name	Description
1	POWER	Power on/off the device.
		Power on/off the device by pressing and holding the button for five seconds.
2	MENU Button	Press to return to the main menu (after successful login).
		Press and hold for 5 seconds to turn off audible key beep.
		In PTZ Control mode, the MENU button will start wiper (if applicable).
		In Playback mode, shows/hides the control interface.
3	REC Button	Enters the Manual Record setting menu.
		In PTZ control settings, press to call a PTZ preset by pressing Numeric button.
		Also turns audio on/off in Playback mode.
4	DIRECTION Button	Navigate between menu fields and items.
		In Playback mode, the Up and Down button speeds up and slows down recorded video. The Left and Right button selects the next and previous record files.
		In Live View mode, these buttons cycle through channels.

No.	Name	Description
		In PTZ control mode, controls PTZ camera movement.
	ENTER Button	Confirm selection in any menu mode.
		Can *tick* checkbox fields.
		In Playback mode, plays or pauses the video.
		In single-frame Playback mode, advances video a single frame.
5	PTZ Button	In Auto-switch mode, stops/starts auto switch.
6	DEV	Enables/Disables Remote Control.
7	Alphanumeric Buttons	Switches to corresponding channel in Live view or PTZ Control mode.
		Inputs numbers and characters in Edit mode.
		Switches between channels in Playback mode.
8	ESC Button	Goes back to previous menu.
		Arms/disarmsthe device in Live View mode.
9	PLAY Button	Enters the All-day Playback mode.
		Auto scans in the PTZ Control menu.
10	PREV Button	Switches between single screen and multi-screen mode.
		In PTZ Control mode, adjusts focus in conjunction with the A/FOCUS+ button.

Troubleshooting Remote Control

NOTE

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

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

1. Go to **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 valid for all IR remote controls.
3. Press **DEV** on the remote control.
4. Enter the **DVR No.** in step 2.
5. Press **ENTER** 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 Operation

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

1. Plug USB mouse into one of the USB interfaces on the DVR front panel.
2. The mouse should automatically be detected. If the mouse is not detected, it may be that the two devices are not compatible. Refer to the recommended device list from your provider.

Table 1-3 Description of the Mouse Controls

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

1.4 Input Method Description

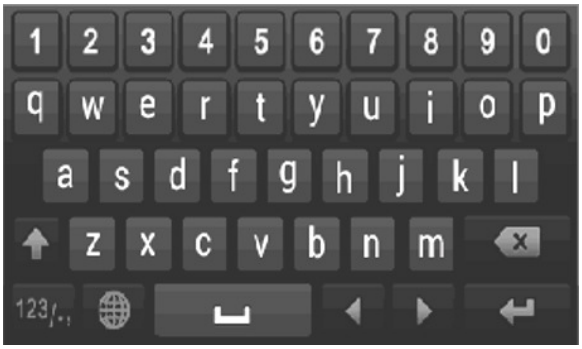


Figure 1-3 Soft Keyboard

Table 1-4 Description of the Soft Keyboard Buttons

Icon	Description	Icon	Description
0 ... 9	Numbers	A ... Z	English letters
	Lowercase/Uppercase		Backspace
123 ABC	Switch the keyboard		Space
	Positioning the cursor		Enter
#+=	Symbols		Reserved

1.5 Rear Panels

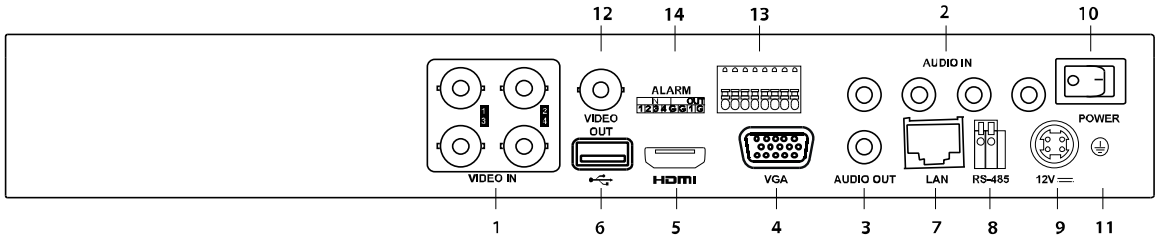


Figure 1-4 DS-7204HTI-K1 Rear Panel

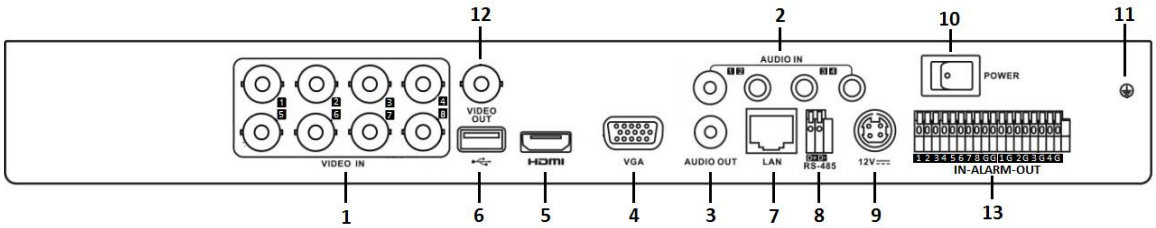
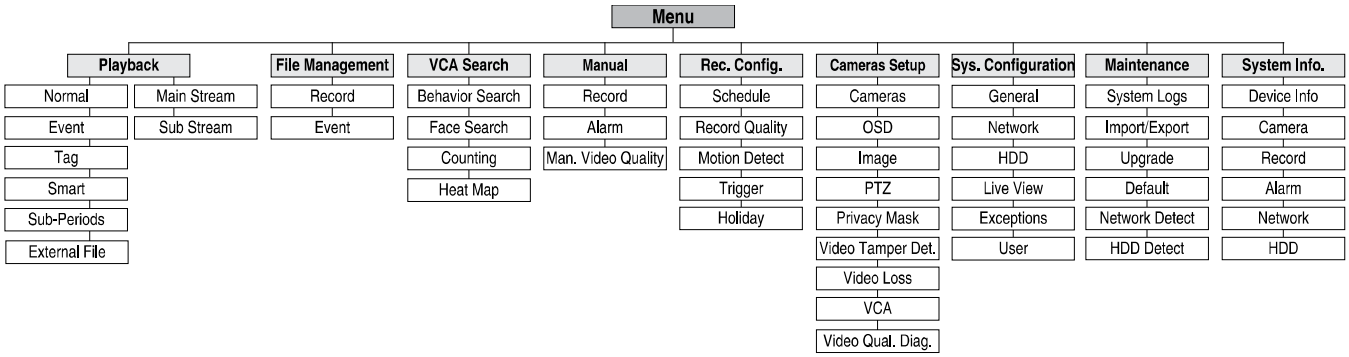


Figure 1-5 DS-7208HTI-K2 Rear Panel

Table 1-5 Description of Rear Panel

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 Interface	Universal Serial Bus (USB) port for additional devices
7	Network Interface	Connector for network
8	RS-485 Interface	Connector for RS-485 devices
9	Power Supply	48 VDC or 12 VDC
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

1.6 Menu Tree



Chapter 2 Getting Started

2.1 Starting Up and Shutting Down the DVR

Purpose

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

Before You Start

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

Starting up the DVR

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

User Logout, Shutdown, and Reboot

You can log out of the system, shut down, or reboot the device upon demand.

1. Go to **Menu > System Maintenance**.
2. Click the  icon in the bottom left corner of the screen.
3. Click **Logout**, **Shutdown**, or **Reboot**.

NOTE

If logged out, menu operation is invalid; enter a user name and password to unlock system.

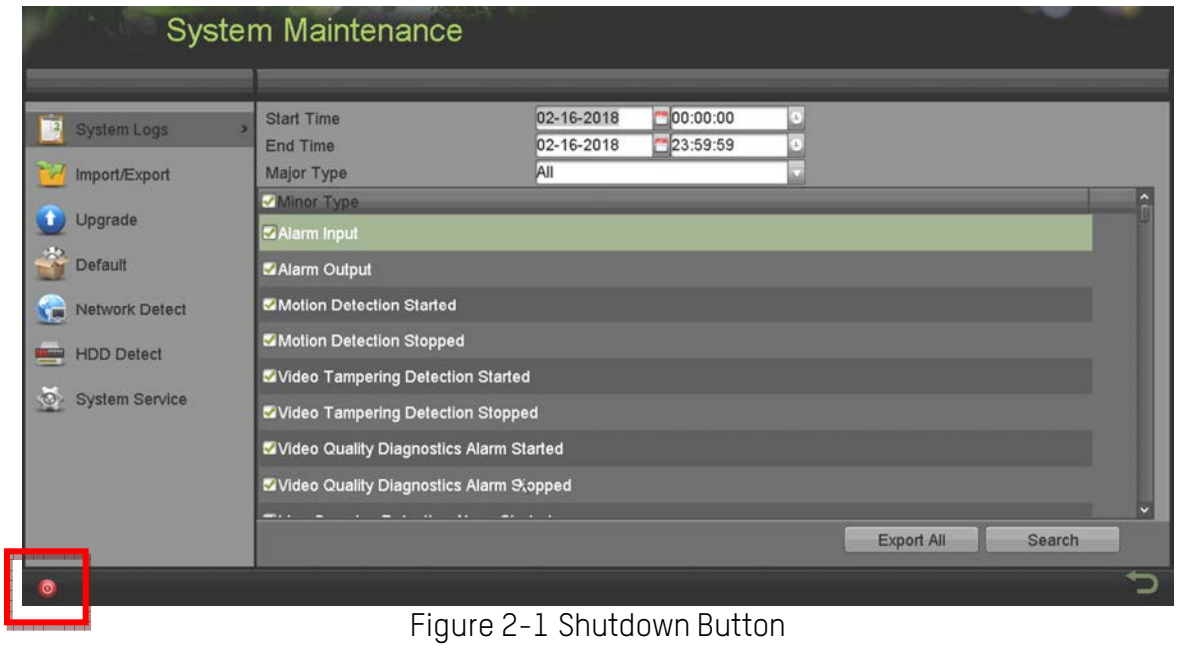


Figure 2-1 Shutdown Button

Figure 2-2 Shutdown Menu

4. Click **Yes**.
5. Turn off the power switch on the rear panel when the following note appears.

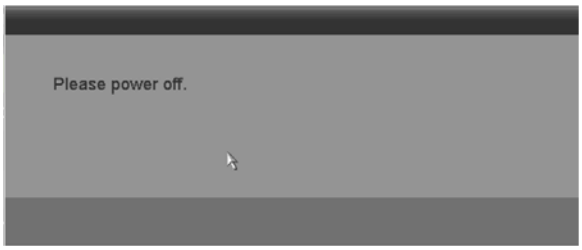


Figure 2-3 Shutdown Tips

2.2 Activating the Device

Purpose

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

1. Input the same password into the **Create New Password** and **Confirm New Password** text fields.
2. In the **IP Camera Activation** text field, enter a password to activate the connected IP camera(s).

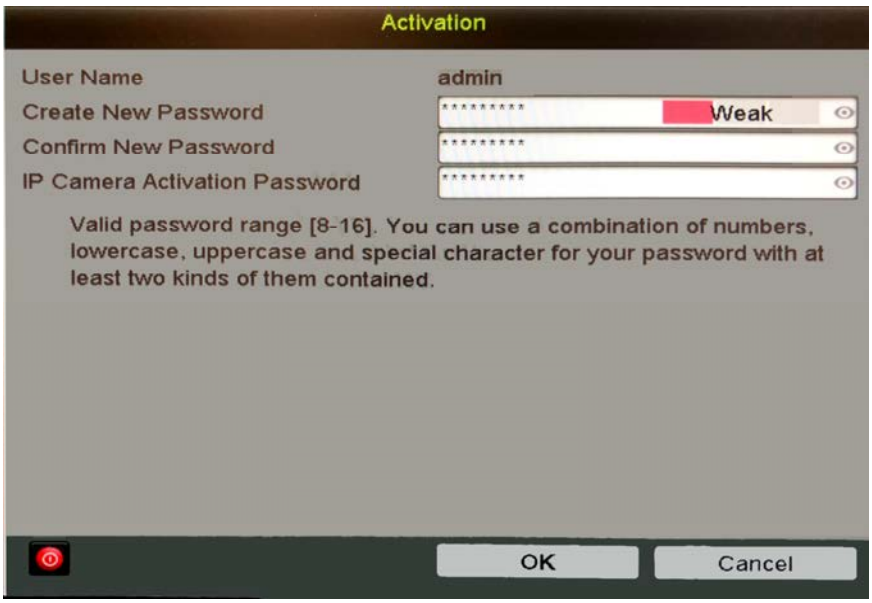


Figure 2-4 Settings Admin Password

WARNING

STRONG PASSWORD RECOMMENDED – We highly recommend that you create a strong password of your own choosing (using a minimum of eight characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

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

NOTE

Clear text password is supported. Click  to see the password. Click the icon again to hide the password.

If you update an older version device that has the old password scheme, the following dialog box will pop up once the device starts. Click **YES** and follow the prompts to set a strong password.

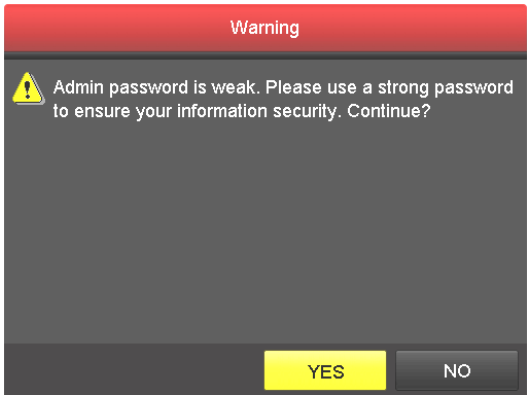


Figure 2-5 Warning

4. After the device has been activated, the Attention box pops up.

Figure 2-6 Attention

5. (Optional) Click **Yes** to export the GUID (Globally Unique Identifier). The Reset Password interface pops up. Click **Export** to export the GUID to the USB flash drive for password resetting.

NOTE

The GUID is a file that is generated, exported, and saved that is used to reset the user's password.

Figure 2-7 Export GUID

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

Figure 2-8 Duplicate the Password

2.3 Using the Unlock Pattern for Login

Purpose

You can configure an unlock pattern for the *admin's* device login.

2.3.1 Configuring the Unlock Pattern

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

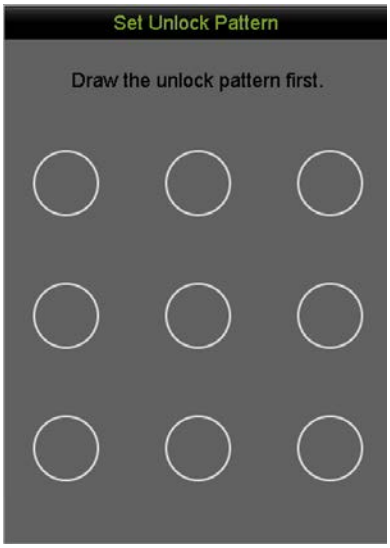


Figure 2-9 Set Unlock Pattern

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

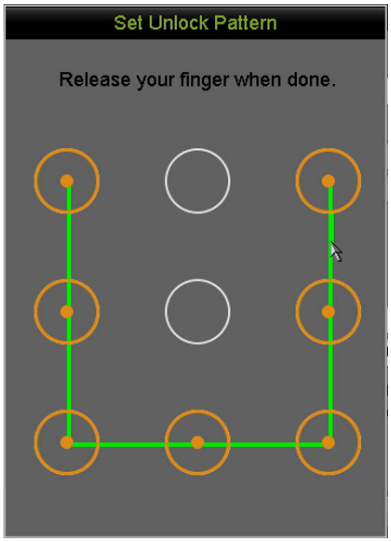


Figure 2-10 Draw the Pattern

NOTE

Connect at least four dots to draw the pattern.

Each dot can be connected once only.

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

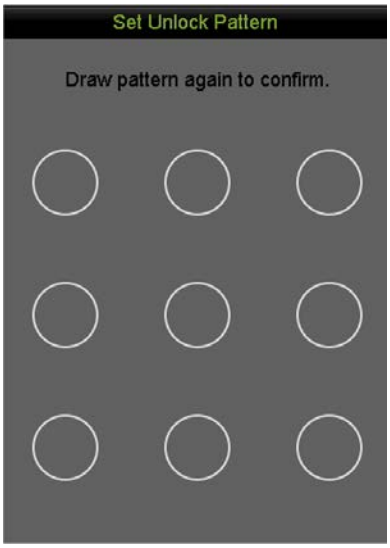


Figure 2-11 Confirm the Pattern

NOTE

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

2.3.2 Logging in via the Unlock Pattern

NOTE

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

Configure the pattern before unlocking. See *2.3.1 Configuring the Unlock Pattern*.

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

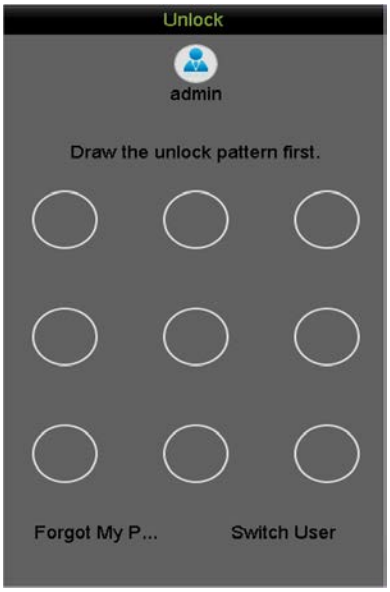


Figure 2-12 Draw the Unlock Pattern

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

NOTE

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

If you forgot your pattern, click **Forgot My Pattern** or **Switch User** to display the normal login dialog box.

If the pattern you draw differs from the pattern you configured, try again.

If you draw the wrong pattern seven times, the account will lock for one minute.

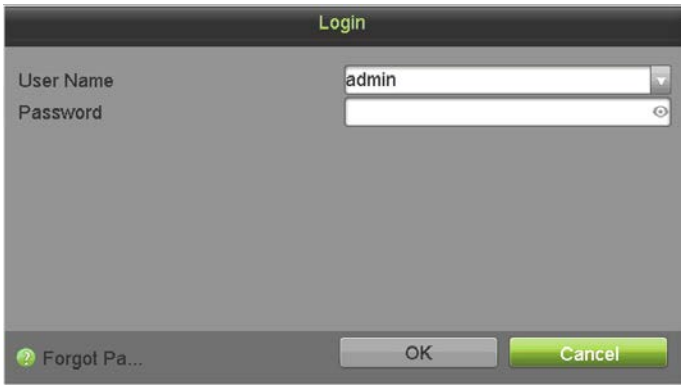


Figure 2-13 Normal Login Dialog Box

2.4 Login and Logout

2.4.1 User Login

Purpose

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

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

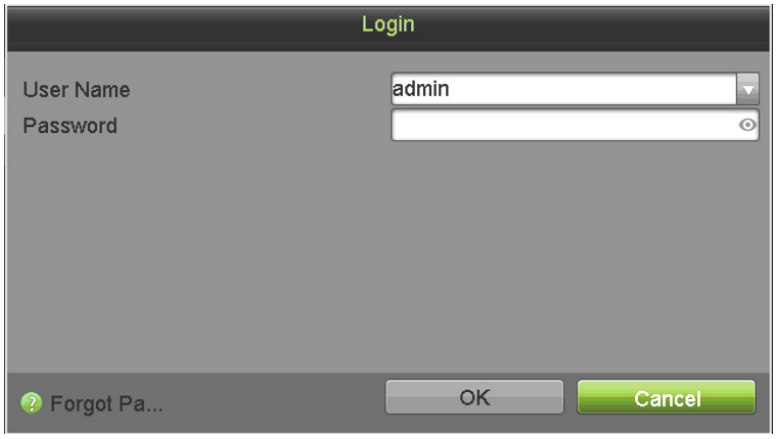


Figure 2-14 Login Interface

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

NOTE

In the Login interface, for the admin, if you enter the wrong password seven times, the account will lock for 60 seconds. For an operator, if you enter the wrong password five times, the account will lock for 60 seconds.

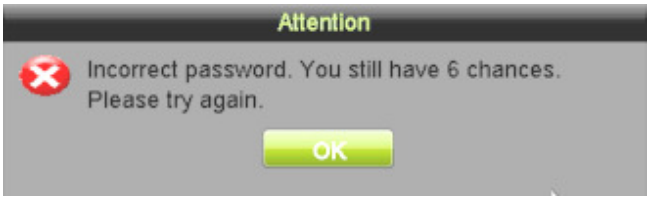


Figure 2-15 User Account Protection for the Admin

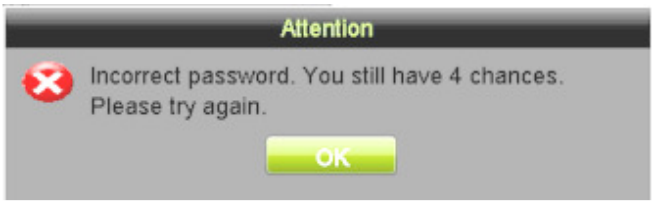


Figure 2-16 User Account Protection for the Operator

2.4.2 User Logout

Purpose

You can log out of the system, shut down, or reboot the device upon demand.

1. Go to **Menu > System Maintenance**.
2. Click the icon in the bottom left corner of the screen.
3. Click **Logout**, **Shutdown**, or **Reboot**.

Figure 2-17 Logout, Shutdown, Reboot

NOTE

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

2.5 Resetting Your Password

Purpose

When you forget the password of the *admin*, you can reset the password by importing the GUID file. The GUID file must be exported and saved in the local USB flash drive after you have activated the device (refer to *Activating the Device 2.2*).

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

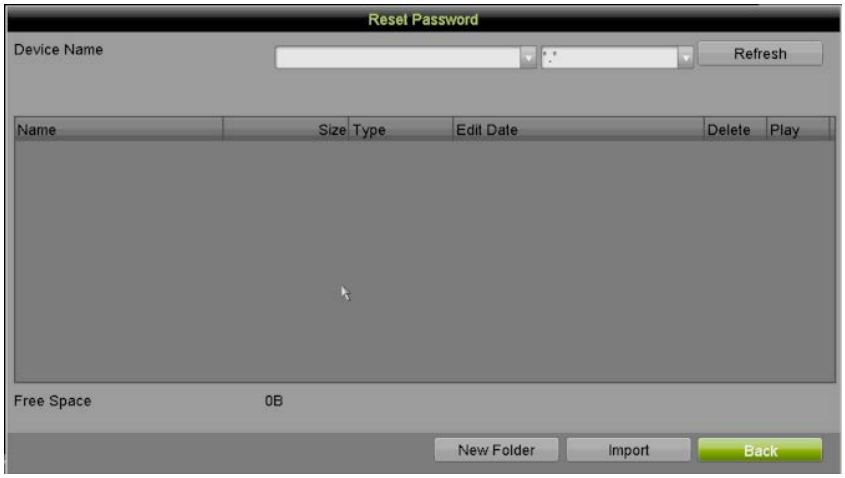


Figure 2-18 Import GUID

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

Figure 2-19 Reset Password

3. Input the new password and confirm the password.

4. Click **OK** to save the new password. The Attention box pops up as shown below.

Figure 2-20 GUID File Imported

5. Click **OK** and the Attention box below pops up to remind you to duplicate the device password to connected IP cameras with default protocol. Click **Yes** to duplicate the password or **No** to cancel it.

Figure 2-21 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. Refer to *Editing a User* 15.4.3 .

2.6 Adding Analog Cameras

2.6.1 Adding Analog Cameras

Connect analog camera(s) to the "Video In" BNC connectors.

2.6.2 Enabling Analog Cameras

Analog cameras are enabled by default; no further action is required.

2.7 Adding and Connecting IP Cameras

2.7.1 Activating IP Cameras

Purpose

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

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

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

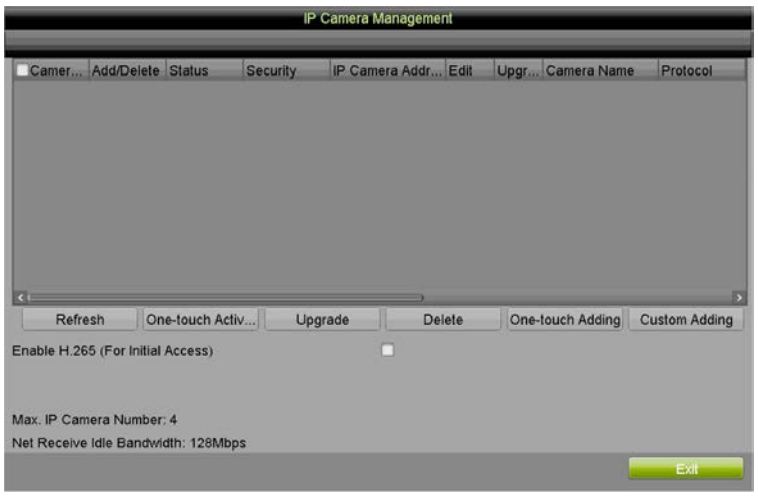


Figure 2-22 IP Camera Management Interface

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

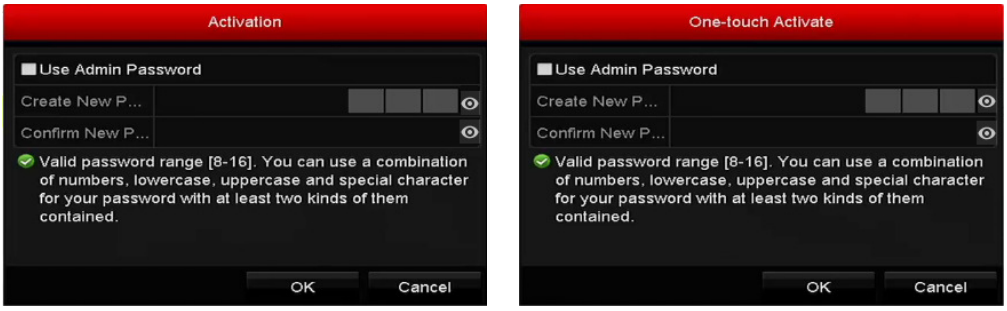


Figure 2-23 Activate the Camera

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

   - **Use Admin Password:** When checked, the camera(s) will use the DVR's admin password.
   - **Create New Password:** If admin password is not used, create and confirm a new camera password.

Figure 2-24 Set New Password

WARNING

STRONG PASSWORD RECOMMENDED – We highly recommend that you create a strong password of your own choosing (using a minimum of eight characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

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

2.7.2 Adding an Online IP Camera

Purpose

Before you can get a live view or record the video, add the IP cameras to the connection list of the device.

Before You Start

Ensure the network connection is valid. See *Chapter 11 Network Settings.*

- **OPTION 1:**

1. Select **Add IP Camera** from the right-click menu in live view or go to **Menu> Camera> IP Camera**.

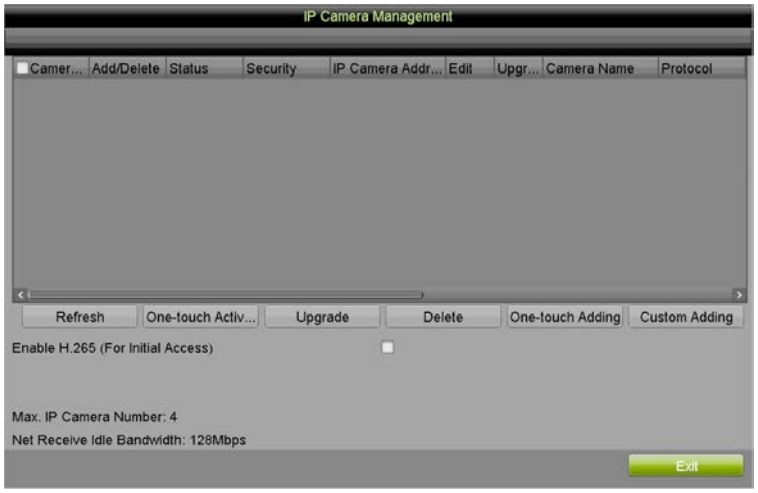


Figure 2-25 IP Camera Management Interface

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

NOTE

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

4. (Optional) Check the **Enable H.265** checkbox (For Initial Access) for the connected IP camera supporting H.265. Then, the IP camera will be encoded with H.265.
5. (For encoders with multiple channels only) check the checkbox of Channel Port in the pop-up window, as shown in the following figure, and click **OK** to add multiple channels.

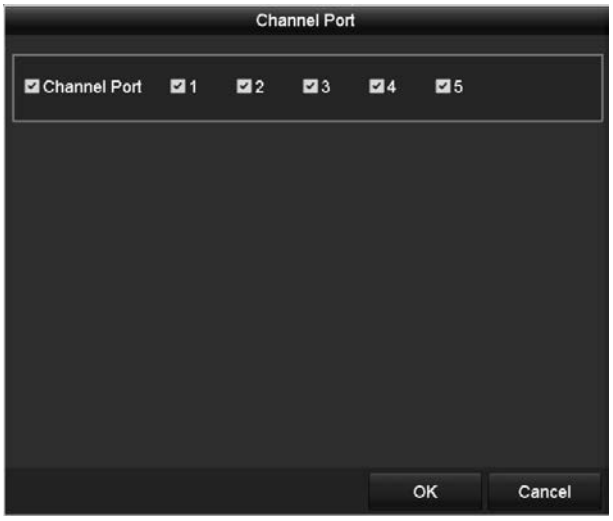


Figure 2-26 Select Multiple Channels

- **OPTION 2:**
  1. On the **IP Camera Management** interface, click **Custom Adding** to show **Add IP Camera (Custom)**.

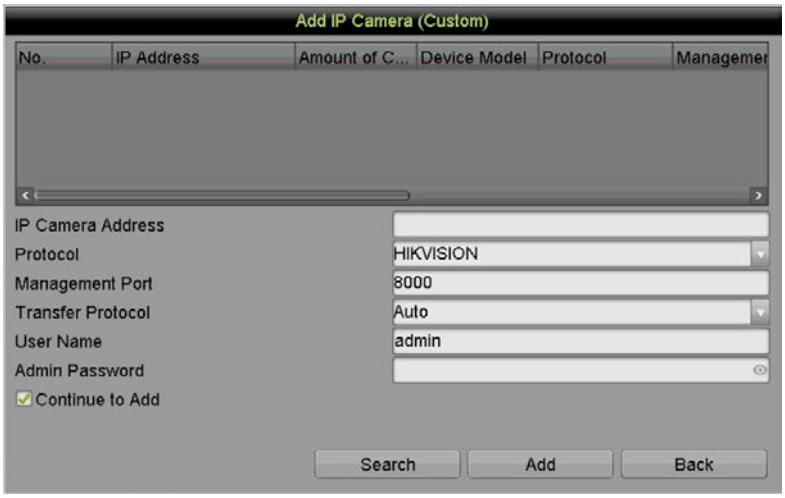


Figure 2-27 Custom Adding IP Camera Interface

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

NOTE

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

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

For the successfully added IP cameras, the **Security** status shows the security level of the password of camera: strong password, weak password, or risky password.

Table 1-6 Explanation of the Icons

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

4. (Optional) Check the **Enable H.265** checkbox (For Initial Access) for the connected IP camera supporting H.265. Then, the IP camera will be encoded with H.265.

2.7.3 Editing the Connected IP Camera

Purpose

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

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

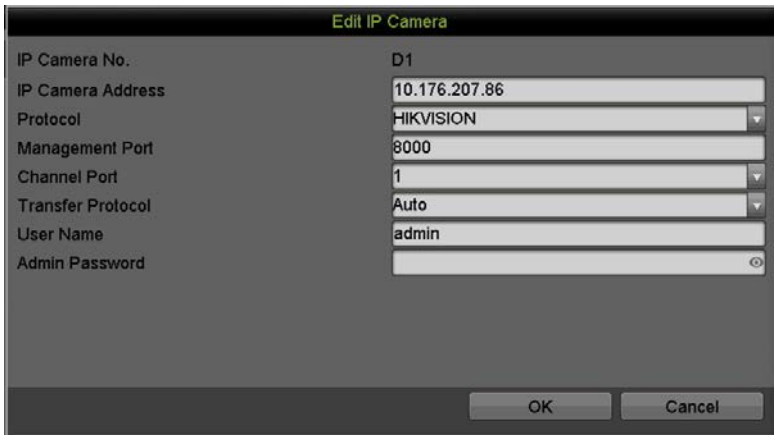


Figure 2-28 Edit IP Camera

- **Channel Port:** If the connected device is an encoding device with multiple channels, choose the channel to connect by selecting the channel port no. in the drop-down list.

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

2. Drag the horizontal scroll bar to the far right and click the icon to edit the advanced parameters.

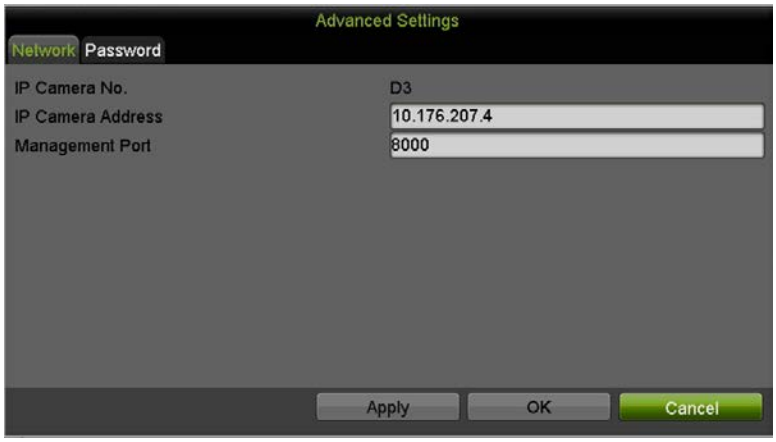


Figure 2-29 Camera Network Configuration

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

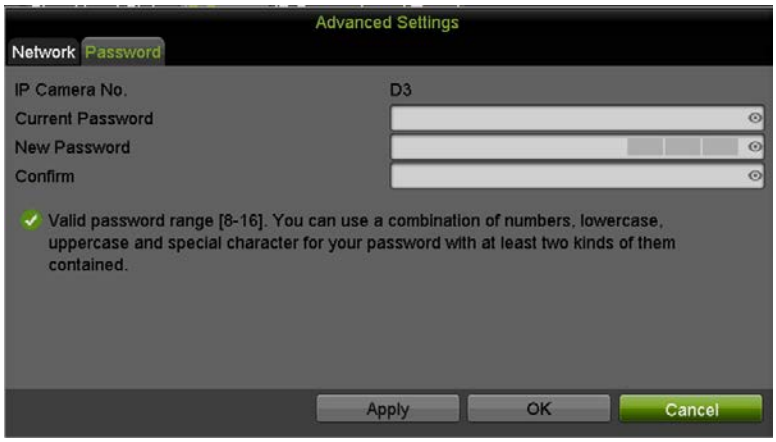


Figure 2-30 Camera Password Configuration

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

2.8 Configuring 5 MP Long Distance Transmission

Purpose

You can configure 5 MP long distance transmission on the Signal Input Status interface.

1. Go to **Menu > Camera Setup > Signal Input Status**.

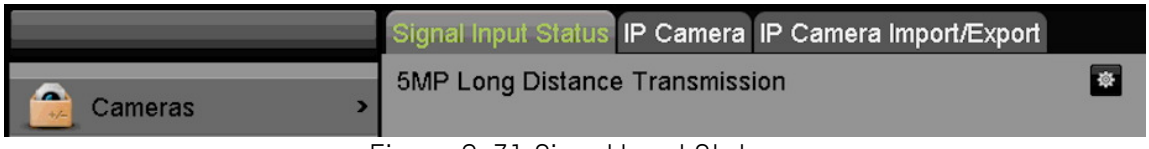


Figure 2-31 Signal Input Status

2. Click  to enter the 5 MP Long Distance Transmission Settings interface.

Figure 2-32 5 MP Long Distance Transmission Settings

3. Check the checkbox to enable 5 MP Long Distance Transmission of the selected channel.
4. Click **Apply** to save the settings.

Chapter 3 Live View

3.1 Introduction of Live View

Live view shows the video image from each camera in real time. 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 to the Live View mode.

Live View Icons

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

Table 1-7 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 8.7 *8.7 Handling Exceptions*.)

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:** the screen is auto switched to the next one. Set the dwell time for each screen on the configuration menu before enabling the auto-switch in **Menu > System Configuration > Live View > Dwell Time**.
- **Start Recording:** normal record and motion detection record are supported.
- **Output Mode:** select the output mode to Standard, Bright, Gentle or Vivid.
- **Playback:** play back the recorded videos for current day.
- **Aux/Main Monitor:** the DVR checks the connection of the output interfaces to define the main and auxiliary output interfaces. When the aux output is enabled, the main output cannot do any operation, and you can do some basic operation on the live view mode for the Aux output.

The DVR supports independent VGA and HDMI output, and simultaneous VGA/HDMI output. In the independent output mode, the priority level for the main and aux output is HDMI > VGA. The CVBS output serves only as the aux output or live view output. The priority relationship is shown in Table 3-3. In the simultaneous output mode, VGA/HDMI output is the main output, and CVBS output is the aux output.

Table 1-8 Priorities of Outputs in Independent Output Mode

S.N	HDMI	VGA	CVBS	Main Output	Auxiliary Output	For Live View Output Only
1	√	√	√ or ×	HDMI	VGA	CVBS
2	√ or ×	×	√ or ×	HDMI	CVBS	VGA
3	×	√	√ or ×	VGA	CVBS	HDMI

NOTE

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

3.2.1 Using the Mouse in Live View

Table 1-9 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** The *dwell time* of the live view configuration must be set 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.
Aux Monitor	Switch to the auxiliary output mode and the operation for the main output is disabled. **NOTE** If you enter Aux monitor mode and the Aux monitor is not connected, the mouse operation is disabled. You need to switch back to the Main output with the F1 button on front panel or **VOIP/MON** button on IR remote control and then press **Enter**.

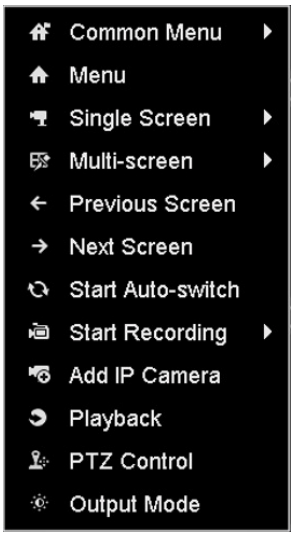


Figure 3-1 Right-Click Menu

3.2.2 Quick Setting Toolbar in Live View Mode

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

Figure 3-2 Quick Setting Toolbar

Table 1-10 Description of Quick Setting Toolbar Icons

Icons	Description	Icons	Description	Icons	Description
/	Start/Stop Manual Record		Instant Playback		Image Settings
	PTZ Control		Digital Zoom		Information
	Close Live View		Face Detection		
/	Show/Hide VCA Information	/	Mute/Audio on		

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

Digital Zoom is for zooming in the live image. You can zoom in the image to different proportions (1 to16X) by moving the sliding bar. You can also scroll the mouse wheel to control the zoom in/out.

Figure 3-3 Digital Zoom

Image Settings icon can be selected to enter the Image Settings menu. You can drag the mouse or click to adjust the image parameters, including brightness, contrast, and saturation. Refer to *13.3 Configuring Video Parameters* for details.

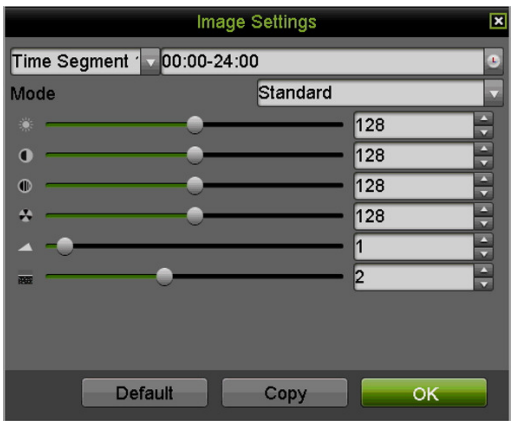


Figure 3-4 Image Settings

Face Detection can be enabled if you click the icon. The dialog pops up as shown in Figure 3-6. Click **Yes** and the full-screen live view of the channel is enabled. Click to exit from the full-screen mode.

Figure 3-5 Enable Face Detection

NOTE

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

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

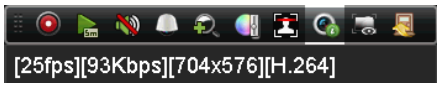


Figure 3-6 Information

NOTE

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. Then the configured line or quadrilateral in the VCA configuration and target frame(s) will be shown on the live view. Click the icon again to hide the VCA information.

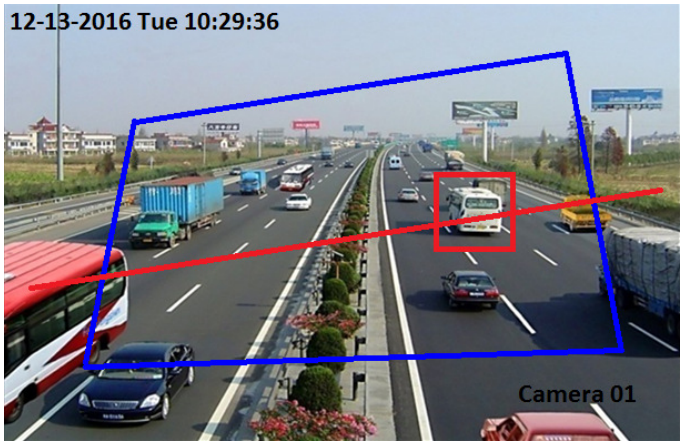


Figure 3-7 Enable VCA Information Overlay

NOTE

In the live view, only the analog cameras support VCA information overlay.

Enable VCA function first before showing the VCA information. Refer to *Chapter 9 VCA Alarm* for detailed operation.

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

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

The DVR only supports VCA information overlay of 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 enabled 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

Purpose

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

1. Go to **Menu > System Configuration > Live View > Channel-Zero Encoding**.

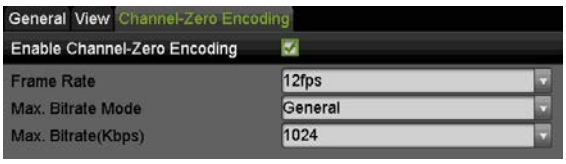


Figure 3-8 Live View Channel-Zero Encoding

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

3.4 Adjusting Live View Settings

Purpose

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

1. Go to **Menu > System Configuration > Live View > General**.

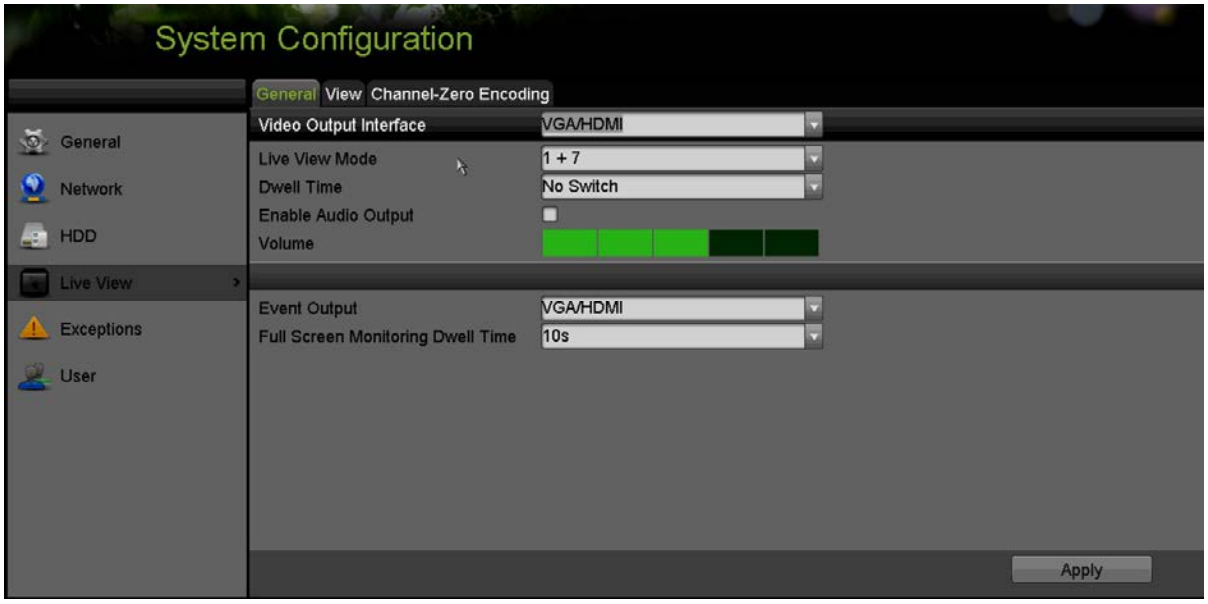


Figure 3-9 Live View-General

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.

NOTE

If you set the video output resolution as 1024*768 in **Menu > Configuration > General**, when you set more than 16 windows, the following message box will pop up as below. If you set the video output resolution as 1280*720 or 1280*1024 in **Menu > Configuration > General**, if you set more than 25 windows, the following message box will pop up as below.

Figure 3-10 Note for Live View Mode

If you set the video output resolution larger than 1280*1024, and then switch to low resolution, the former live view mode will not be changed.

- **Dwell Time:** The time in seconds to *dwell* between switching of channels when enabling auto-switch in Live View.
- **Enable Audio Output:** Enables/disables audio output for the selected 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.

2. Set the camera order.

   1) Click the **View** tab and select **Video Output Interface** from the drop-down list.

Figure 3-11 Live View-Camera Order

   2) Select a window, 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.

3) 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.

4) Click **Apply**.

3.5 Manual Video Quality Diagnostics

Purpose

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

1. Go to **Menu > Manual > Manual Video Quality Diagnostics**.

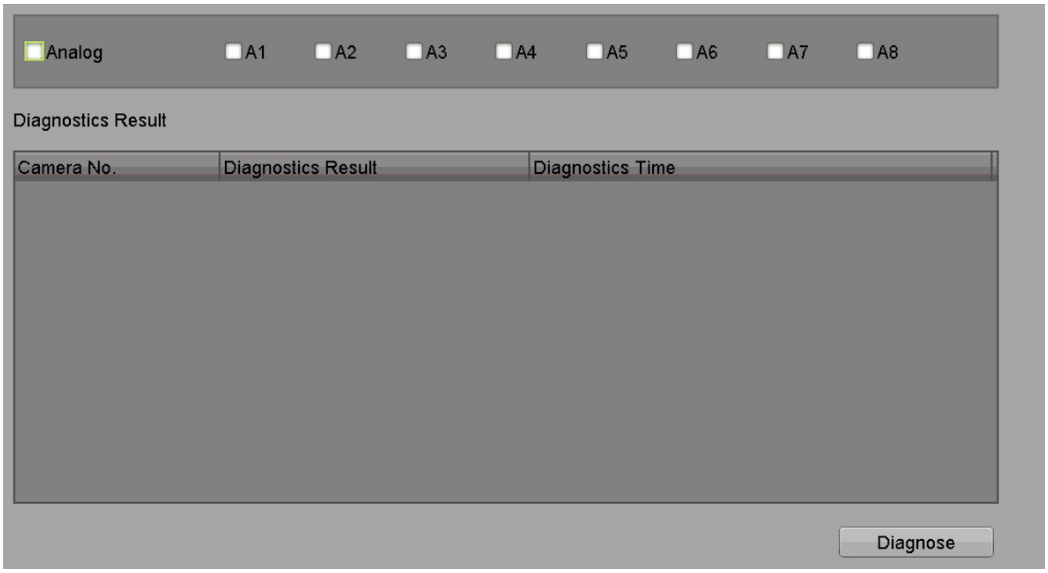


Figure 3-12 Video Quality Diagnostics

2. Check the checkboxes to select the channels for diagnostics.

3. Click **Diagnose** and the results will display on a list. You can view the video status and diagnostics time of the selected channels.

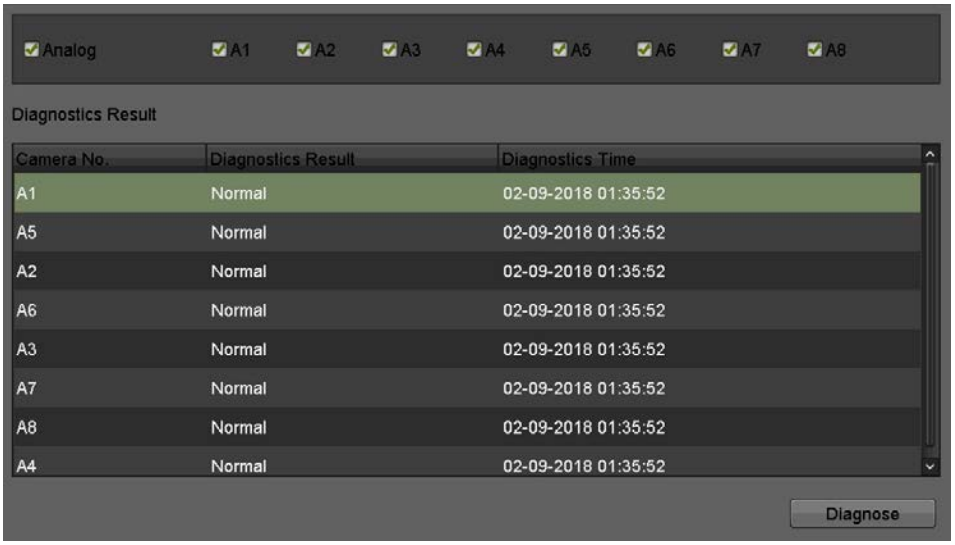


Figure 3-13 Diagnostics Result

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

Purpose

Configure the PTZ parameters before you attempt to control the PTZ camera.

1. Go to **Menu > Cameras Setup > PTZ**.

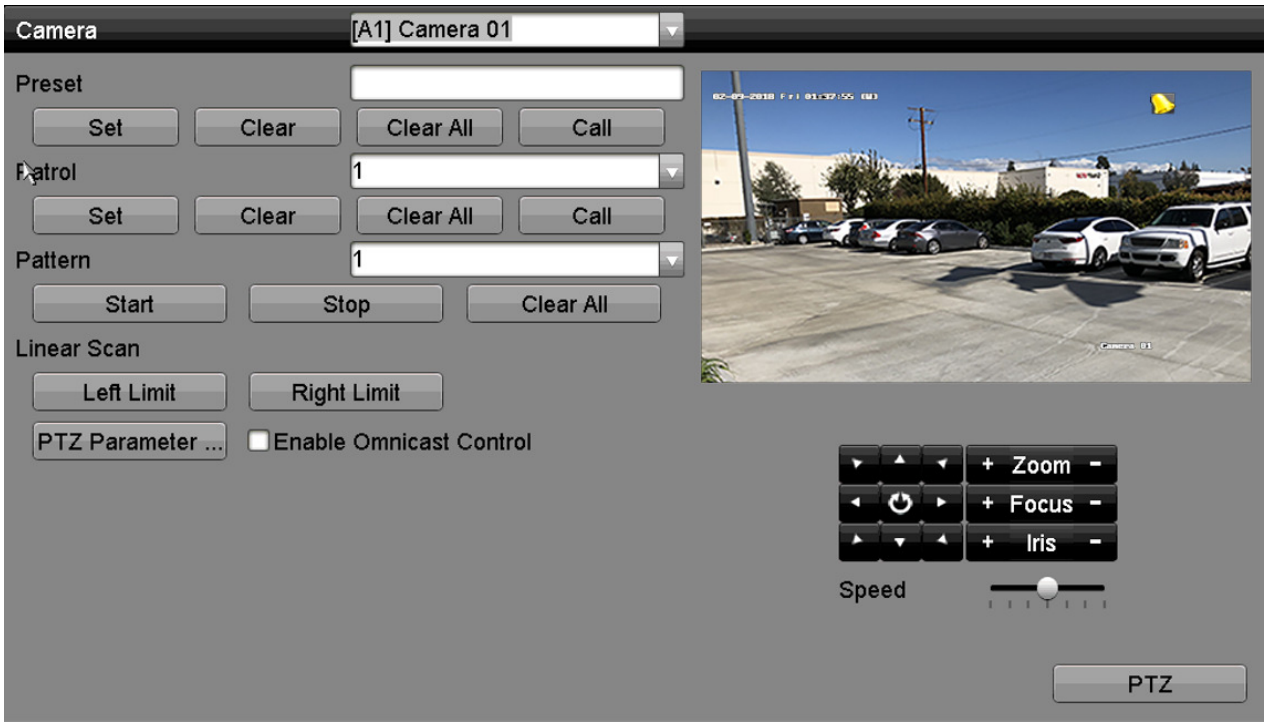


Figure 4-1 PTZ Settings

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

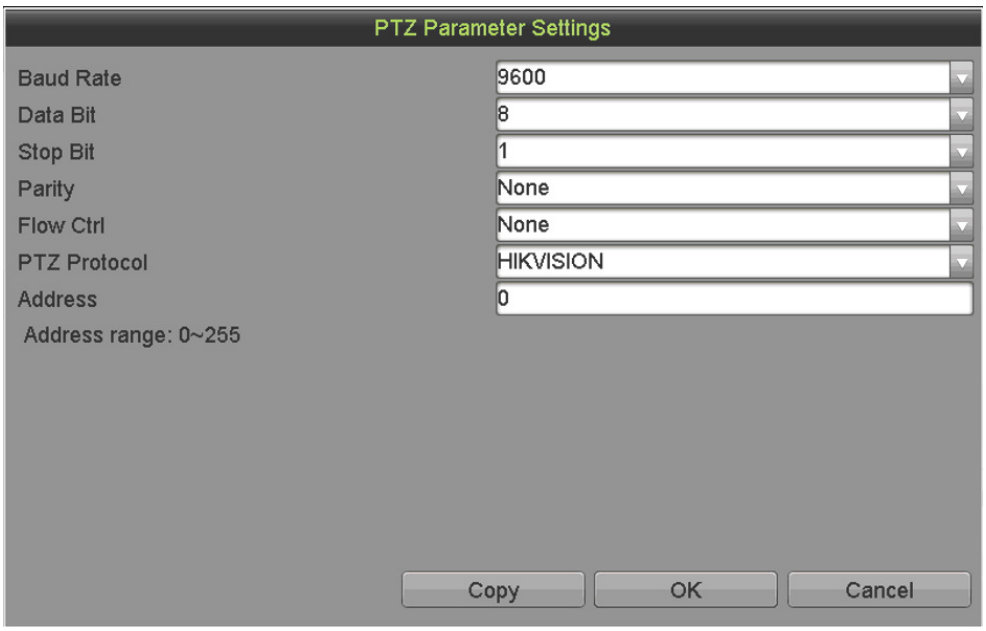


Figure 4-2 PTZ-Parameter Settings

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

NOTE

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

For a connected Hikvision-C camera/dome, you can set the PTZ protocol to UTC. Make sure the protocol selected here is supported by the connected camera/dome.

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

When a Hikvision CVBS camera is connected, you can control PTZ via UTC.

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.

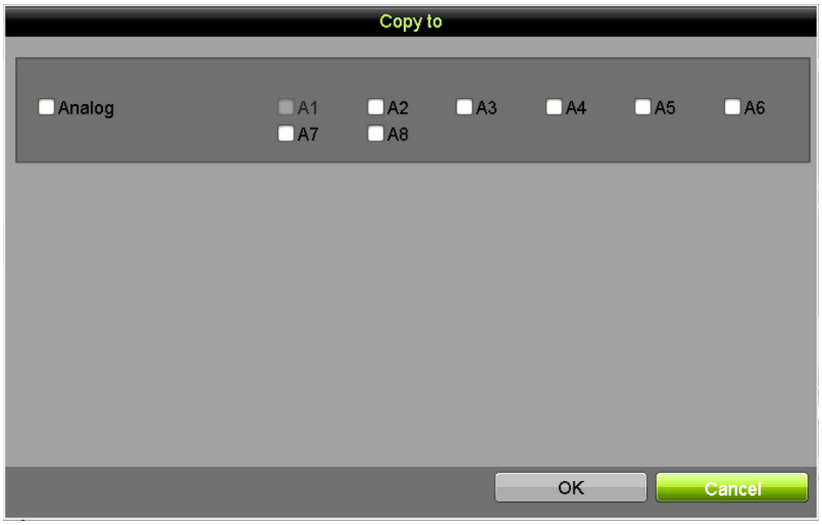


Figure 4-3 Copy to Other Channels

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

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

4.2 Setting PTZ Presets, Patrols, and Patterns

Before You Start

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

4.2.1 Customizing Presets

Purpose

To set the preset location you want the PTZ camera to point to when an event occurs.

1. Go to **Menu > Cameras Setup > PTZ**.

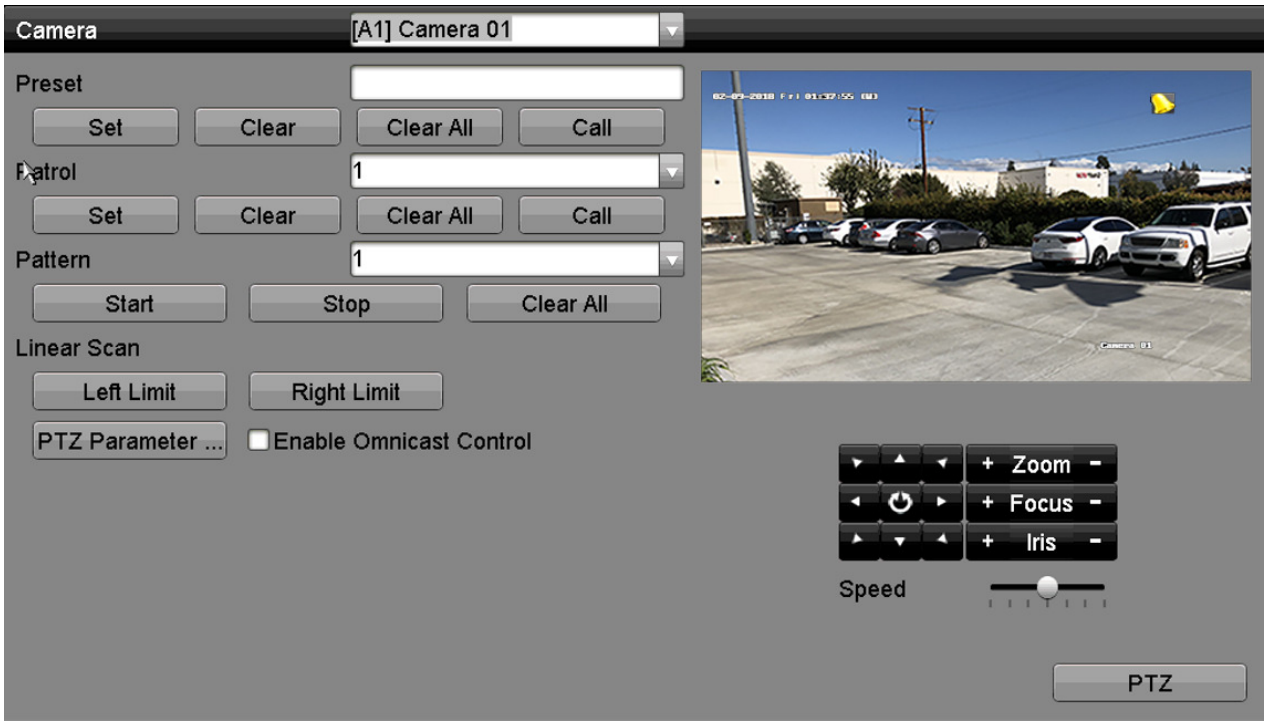


Figure 4-4 PTZ Settings

2. Use the directional button to wheel the camera to the location where you want to set preset; and the zoom and focus operations can be recorded in the preset as well.
3. Enter the preset No. (1~255) in the preset text field, and click **Set** to link the location to the preset.
4. Repeat steps from 2 to 3 to save more presets.
5. You can click **Clear** to clear the location information of the preset, or click **Clear All** to clear the location information of all the presets.

4.2.2 Calling Presets

Purpose

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

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

Figure 4-5 PTZ Panel-General

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

NOTE

When the connected Hikvision-C camera/dome's PTZ protocol is set to UTC (Hikvision-C), call the preset 95 to enter the connected Hikvision-C camera/dome menu. Use the directional buttons on the PTZ control panel to operate the menu.

4.2.3 Customizing Patrols

Purpose

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

1. Go to **Menu > Cameras Setup > PTZ**.

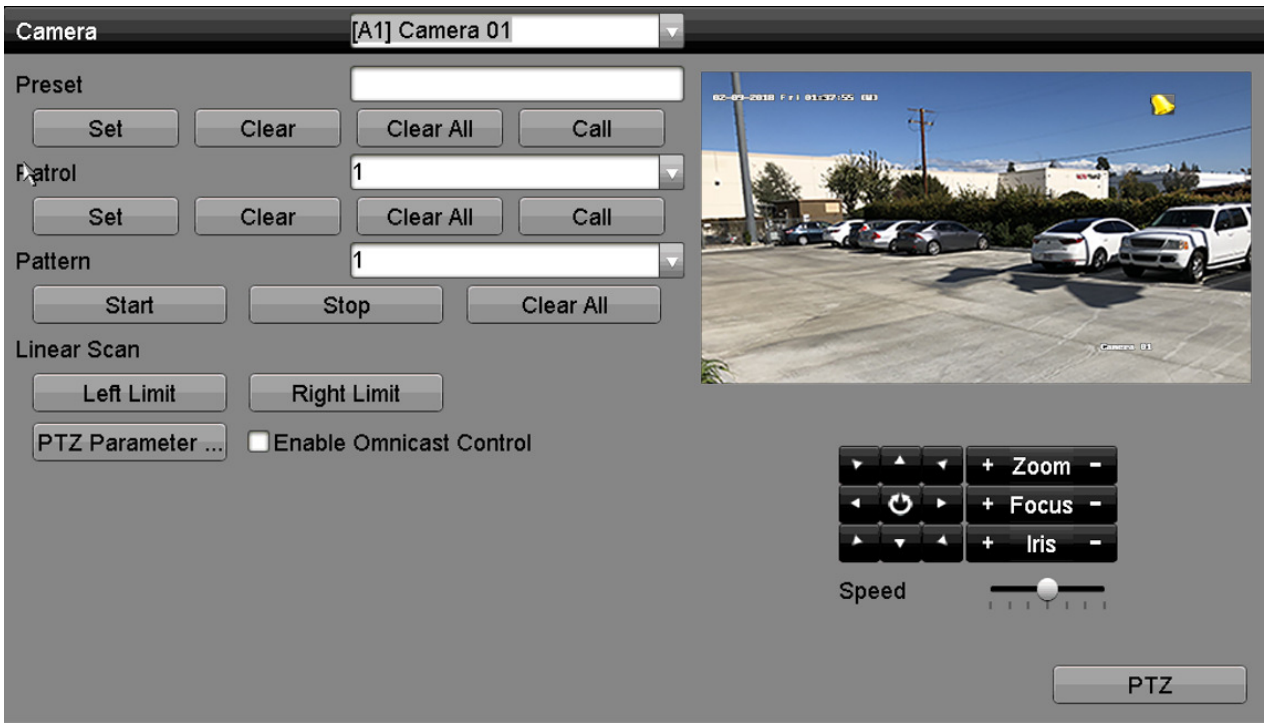


Figure 4-6 PTZ Settings

2. Select patrol no. in the drop-down patrols list.

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

Figure 4-7 KeyPoint Configuration

4. Configure key point parameters such as key point no., key point stay duration, and patrol speed. The key point corresponds to the preset. **KeyPoint No.** determines the order in which the PTZ will follow while cycling through the patrol. **Duration** refers to the time interval to stay at the corresponding key point. **Speed** defines the speed at which the PTZ will move from one key point to the next.

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

NOTE

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

4.2.4 Calling Patrol

Purpose

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

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

2. Click the **General** tab to show the general settings of the PTZ control.

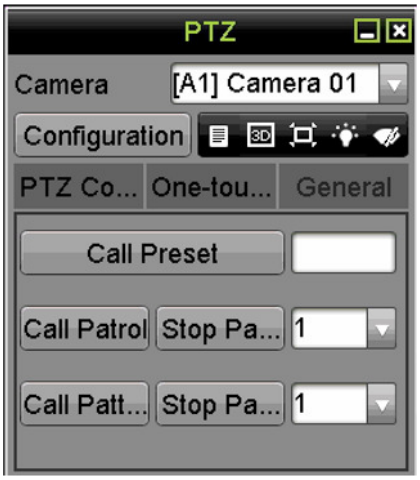


Figure 4-8 PTZ Panel - General

3. Select a patrol in the drop-down list and click **Call Patrol** to call it.

4. You can click **Stop Patrol** to stop calling it.

4.2.5 Customizing Patterns

Purpose

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

1. Go to **Menu > Cameras Setup > PTZ**.

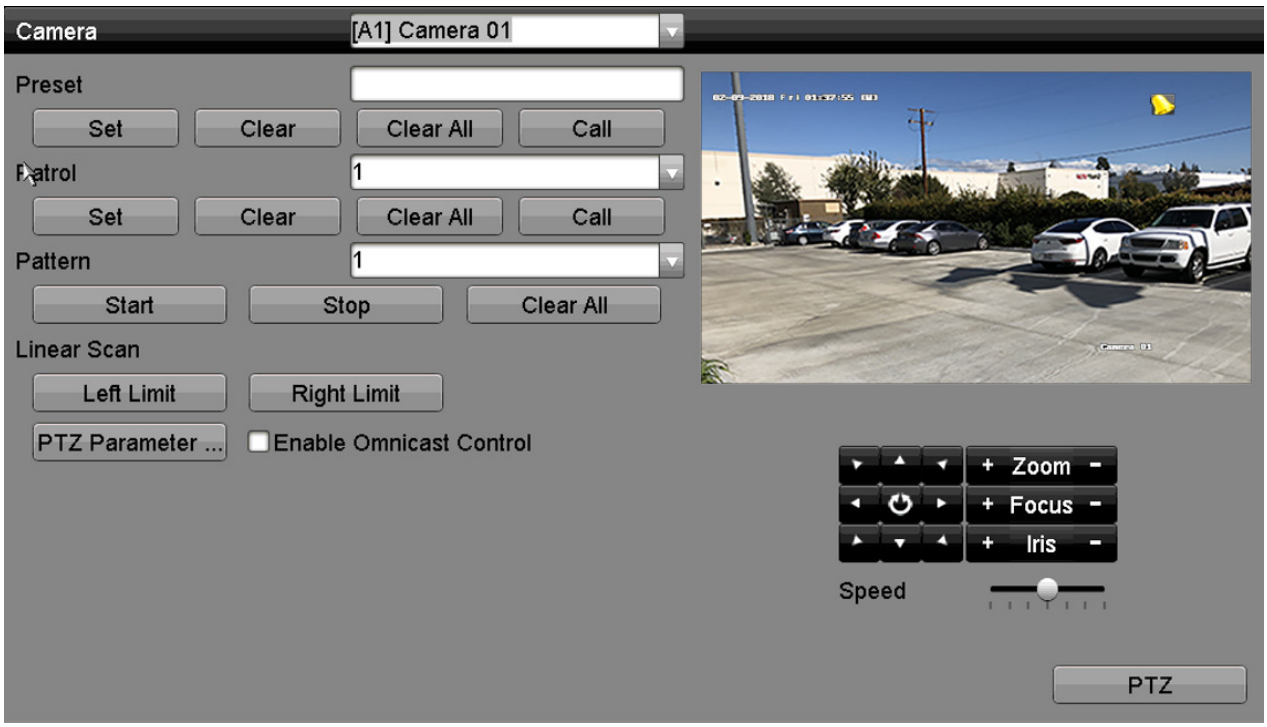


Figure 4-9 PTZ Settings

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 the **Stop** button to stop it. The PTZ movement is recorded as the pattern.

4.2.6 Calling Patterns

Purpose

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

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

2. Click the **General** tab to show the general settings of the PTZ control.

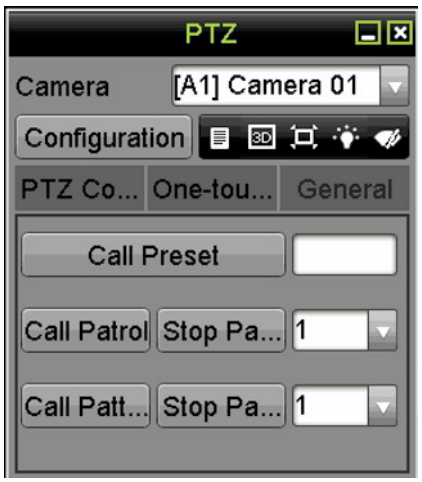


Figure 4-10 PTZ Panel - General

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

4.2.7 Customizing Linear Scan Limit

Purpose

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

1. Go to **Menu > Cameras Setup > PTZ**.

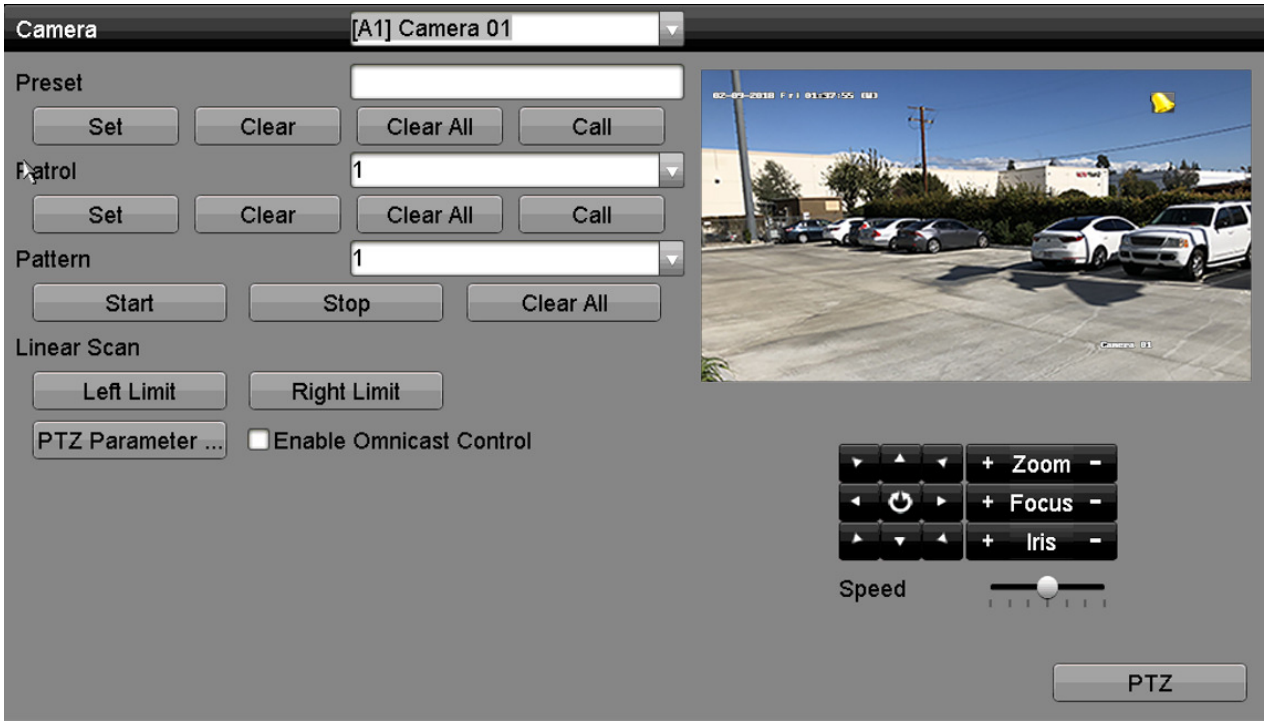


Figure 4-11 PTZ Settings

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

NOTE

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

4.2.8 Calling Linear Scan

Purpose

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

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

Figure 4-12 PTZ Panel – One-touch

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

4.2.9 One-Touch Park

Purpose

Configure settings to start a predefined park action (scan, preset, patrol, etc.) automatically after a period of inactivity (park time).

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

Figure 4-13 PTZ Panel - One-touch

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

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

NOTE

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

4. Click the button again to deactivate it.

4.3 PTZ Control Panel

There are two ways to enter the PTZ control panel:

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 the **PTZ Control** button on the front panel or the remote control, or choose the PTZ Control icon in the quick setting bar, or select the PTZ Control option in the right-click menu.

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 to the device. If no mouse is connected, the PTZ icon appears in the lower-left corner of the window, indicating that this camera is in PTZ control mode.

Figure 4-14 PTZ Control Panels

Table 1-11 Descriptions of the PTZ Panel Icons

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

NOTE

When a Hikvision CVBS camera is connected, click to call the camera OSD.

Chapter 5 Recording and Capture Settings

5.1 Configuring Encoding Parameters

Before You Start

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

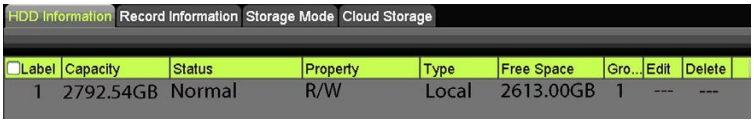


Figure 5-1 HDD Information

2. Click the **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. See *12.4 Configuring Quota Mode*.

   2) If the HDD mode is Group, you must set the HDD group. See *5.9 Configuring HDD Group*.

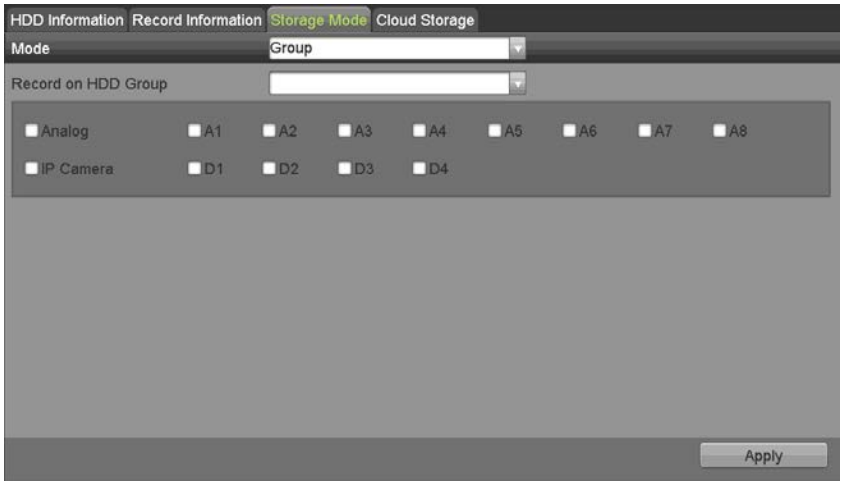


Figure 5-2 HDD - Storage Mode

Setting Parameters

1. Go to **Menu > Recording Configuration > Record Quality > Record**.

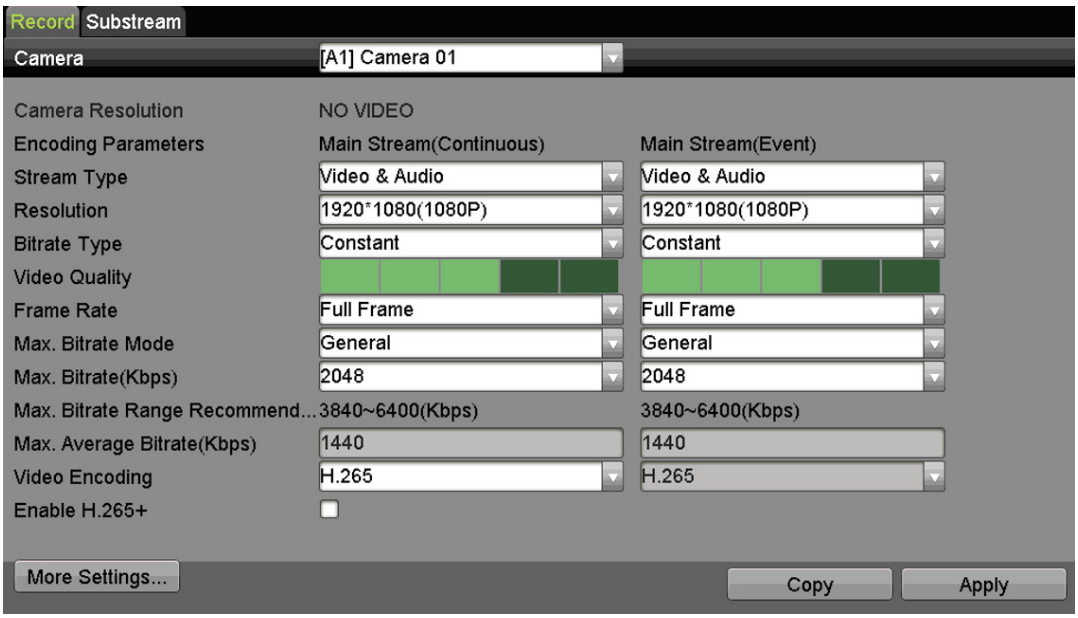


Figure 5-3 Record Parameters

2. Set the recording parameters.

   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, AHD, or HD-CVI input is connected, you can view information including input signal type, resolution, and frame rate (e.g., 1080P30). When CVBS input is connected, you can view 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

Analog signal inputs (TurboHD, AHD, HD-CVI, CVBS) and IP signal input can be recognized and connected automatically.

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

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

NOTE

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

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

NOTE

When an 8 MP signal input is connected, the main stream frame rate cannot exceed 12 fps.

The minimum frame rate for the main stream is 1 fps.

If you set different frame rates for continuous and event recording, when you click **Apply** to save the settings, the following note pops up:

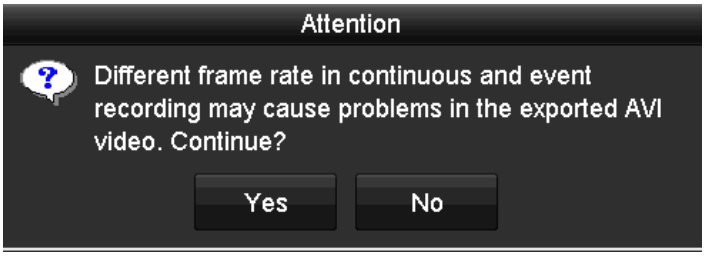


Figure 5-4 Note for Different Frame Rates

- **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 maximum average bit rate which refers to the average amount of data transferred per unit of time.
- **Video Encoding:** Configure H.264 or H.265 for IP and analog camera main stream (continuous).

NOTE

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

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

NOTE

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

Reboot the device to activate the new settings after enabling H.264+ or H.265+.

6) Click **More Settings** to configure additional parameters.

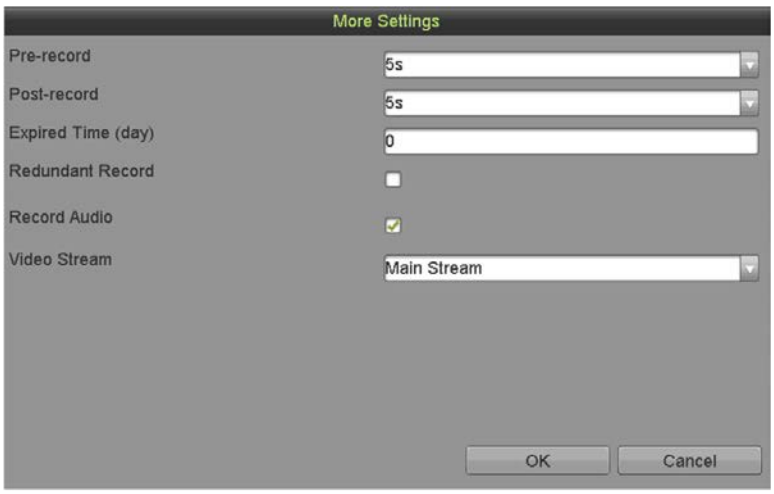


Figure 5-5 More Settings of Record Parameters

- **Pre-record:** The time you set to record before the scheduled time or event. For example, when an alarm triggered the recording at 10:00, if you set the pre-record time as 5 seconds, the camera records it at 9:59:55.
- **Post-record:** The time you set to record after the event or the scheduled time. For example, when an alarm triggered the recording ends at 11:00, if you set the post-record time as 5 seconds, it records till 11:00:05.
- **Expired Time:** The time for keeping the record files in the HDDs, once exceeded, the files will be deleted. The files will be saved permanently if the value is set as 0. The actual keeping time for the files should be determined by the capacity of the HDDs.
- **Redundant Record:** Enabling redundant record means you save the record in the redundant HDD. See *5.8 Configuring Redundant Recording and Capture*.
- **Record Audio:** Enable this feature to record the video with sound, and disable it to record the video without sound.
- **Video Stream:** Main Stream, Sub-Stream, and Dual-Stream are selectable for recording. When you select sub-stream, you can record longer with the same storage space.

NOTE

The **Redundant Record** option is available only when the HDD mode is *Group.*

Redundant HDD is required for the redundant record function. For detailed information, see *12.3.2 Setting HDD Property*.

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

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

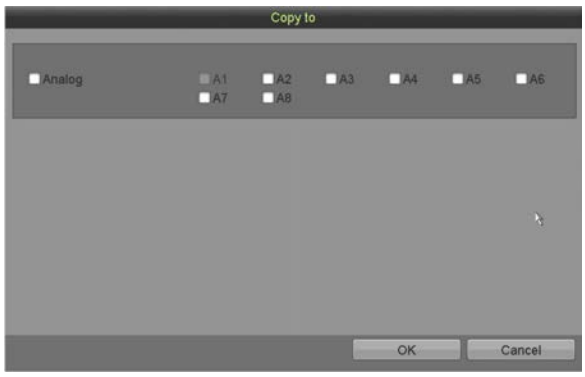


Figure 5-6 Copy Camera Settings

5. Set encoding parameters for sub-stream.

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

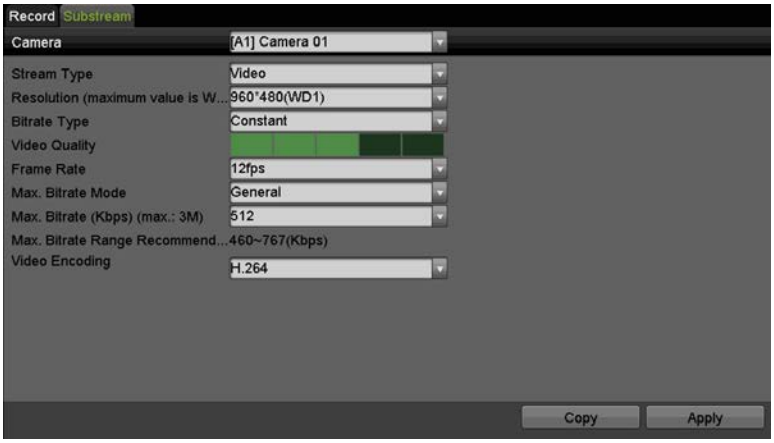


Figure 5-7 Sub-Stream Encoding

   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 for other cameras, click **Copy** to copy the settings to other channels.

NOTE

The sub-stream resolution can be selected as WD1, 4CIF, or CIF.

The minimum frame rate for the sub-stream is 1 fps.

You can select the **Video Encoding** for the IP and analog camera sub-streams. 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

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

Purpose

Set the recording schedule, and the camera will automatically start/stop recording according to the configured schedule.

1. Go to **Menu > Recording Configuration > Schedule**.

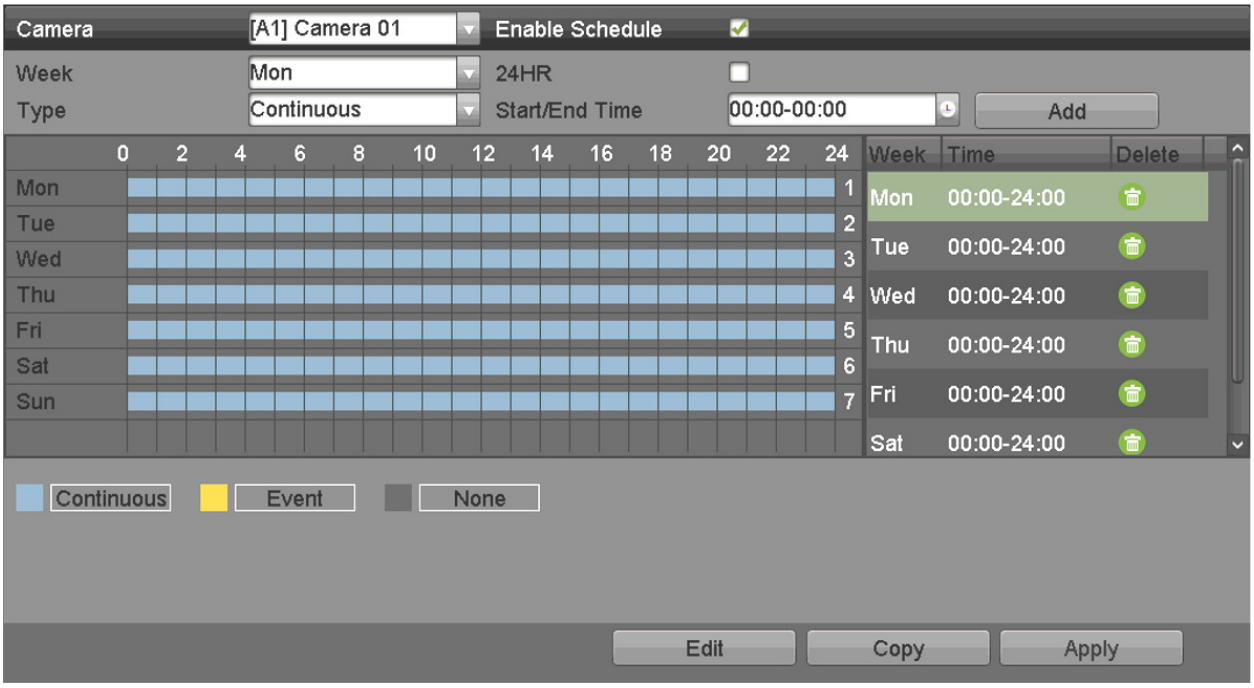


Figure 5-8 Record Schedule

Different Recording Types Are Marked in Different Colors

- **Continuous**: Scheduled recording
- **Event**: Recording triggered by any event triggered alarm
- **None**: No recording

2. Choose the camera to configure in the **Camera** drop-down list.
3. Check the **Enable Schedule** checkbox.
4. Configure the record schedule.

Edit the Schedule

1) Click **Edit**.

2) In the message box, choose the day for which you want to set the schedule.

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

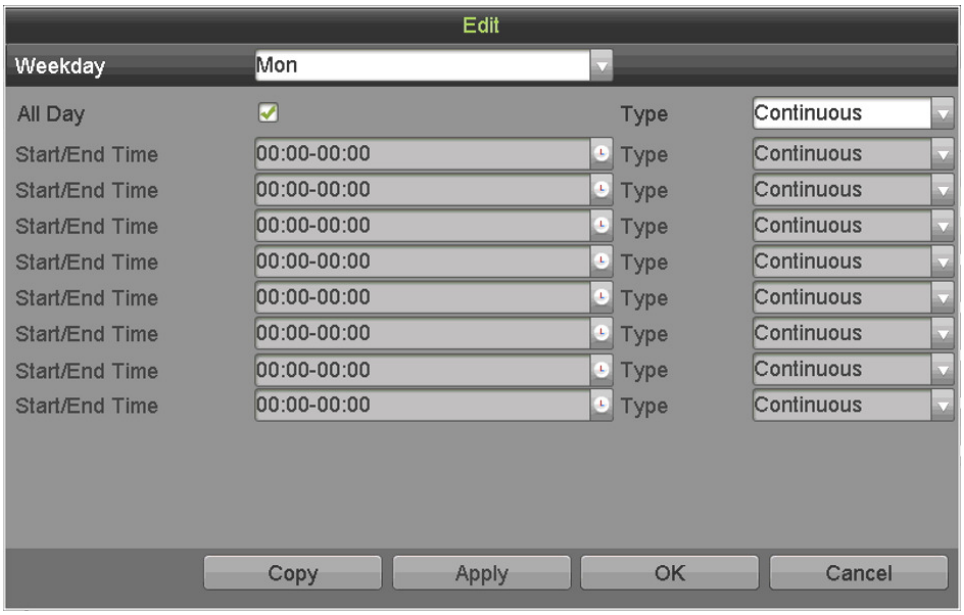


Figure 5-9 Edit Schedule

4) To arrange another schedule, leave the **24HR** checkbox blank and set the Start/End times.

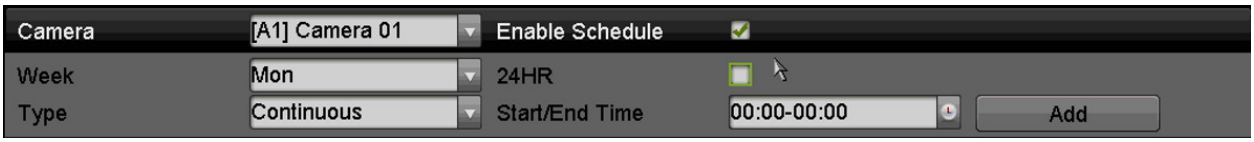


Figure 5-10 Edit Schedule - Set Time Period

NOTE

Up to eight periods can be configured for each day, and the 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**.

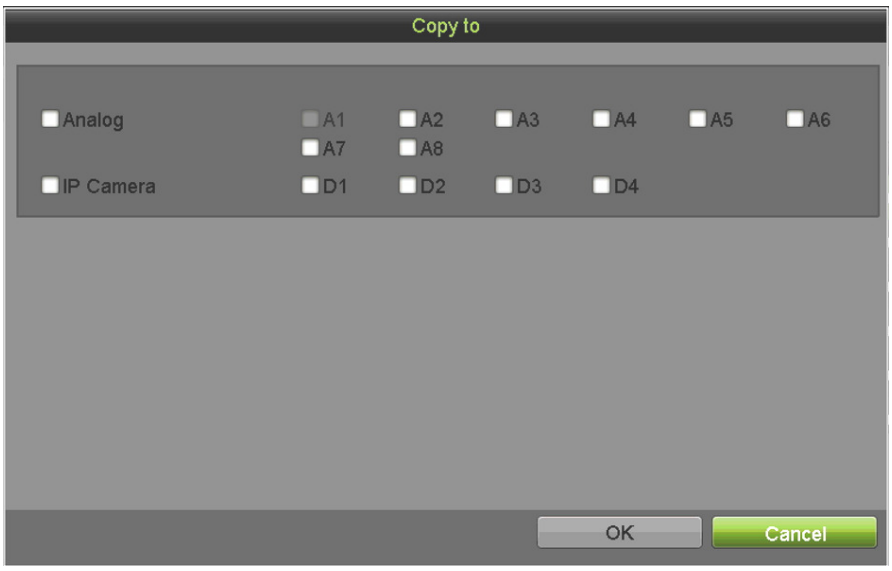


Figure 5-11 Copy Schedule to Other Days

NOTE

The **Holiday** option is available when you enable holiday schedule in **Holiday Settings**. See *5.7 Configuring Holiday Recording and Capture.*

6) Click **OK** to save the settings and return to upper level menu.

Draw the Schedule

1) Click the color icon to select a record type in the event list on the bottom of the interface.

Figure 5-12 Draw the Recording Schedule

2) Drag the mouse on the schedule.

3) Click an area outside of the schedule table to finish and exit from the drawing.

Repeat **Step 4** to set schedules for other channels. If the settings can also be used for other channels, click **Copy**, and then choose the channel you want to copy to.

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

5.3 Configuring Motion Detection Recording

Purpose

Follow the steps to set the motion detection parameters. In live view mode, once a motion detection event occurs, the DVR analyzes it and performs action(s) to handle it. Enabling the motion detection function can trigger certain channels to start recording, trigger full screen monitoring, broadcast an audio warning, notify the surveillance center, send e-mail, etc.

1. Go to **Menu > Recording Configuration > Motion Detect**.
2. Configure Motion Detection.
   1) Choose the camera you want to configure.
   2) Check Enable Motion Detection.
   3) Check **False Alarm Filter**. Refer to *8.2 Setting PIR Camera Alarm* for details.
   4) Use the mouse to drag and draw the area for motion detection. To set the motion detection for the entire area shot by the camera, click **Full Screen**. To clear the motion detection area, click **Clear**.

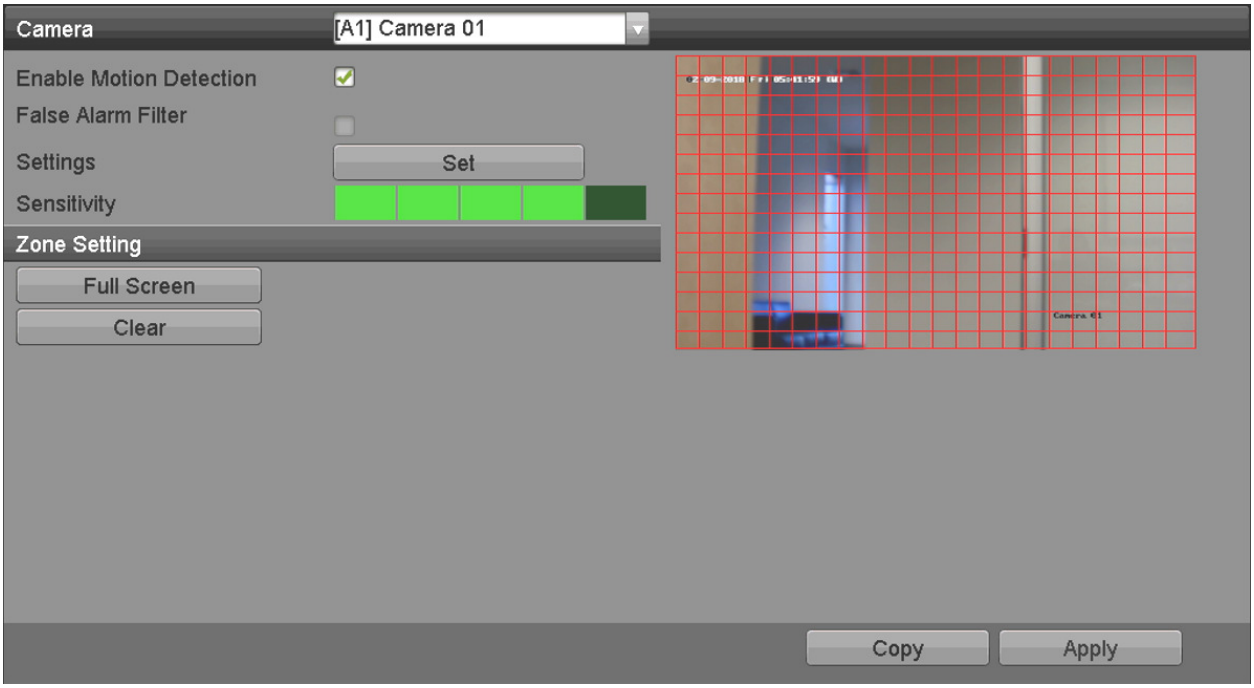


Figure 5-13 Motion Detection - Mask

   5) Click , and the message box for channel information pops up.

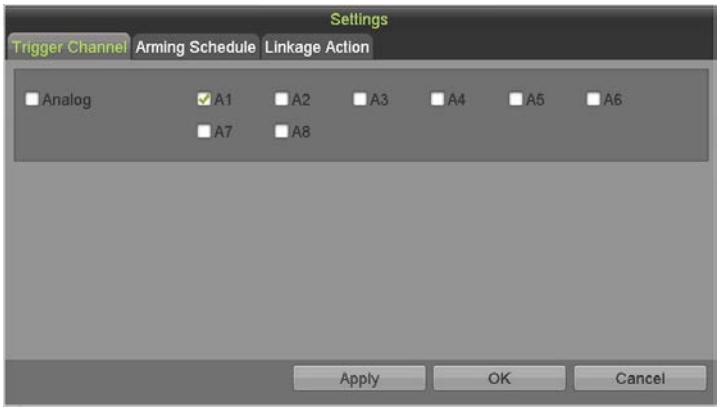


Figure 5-14 Motion Detection Settings

6) Select the channels for which the motion detection event should trigger recording.
7) Click **Apply** to save the settings.
8) Click **OK** to return to the upper level menu.
9) Exit the Motion Detection menu.

3. Configure the schedule (see *5.2*

Configuring *Recording* Schedule*,* and choose Motion as the record type).

5.4 Configuring Alarm Triggered Recording

Purpose

Follow the procedure to configure alarm triggered recording.

1. Go to **Menu > Recording Configuration > Trigger > Alarm Input**.

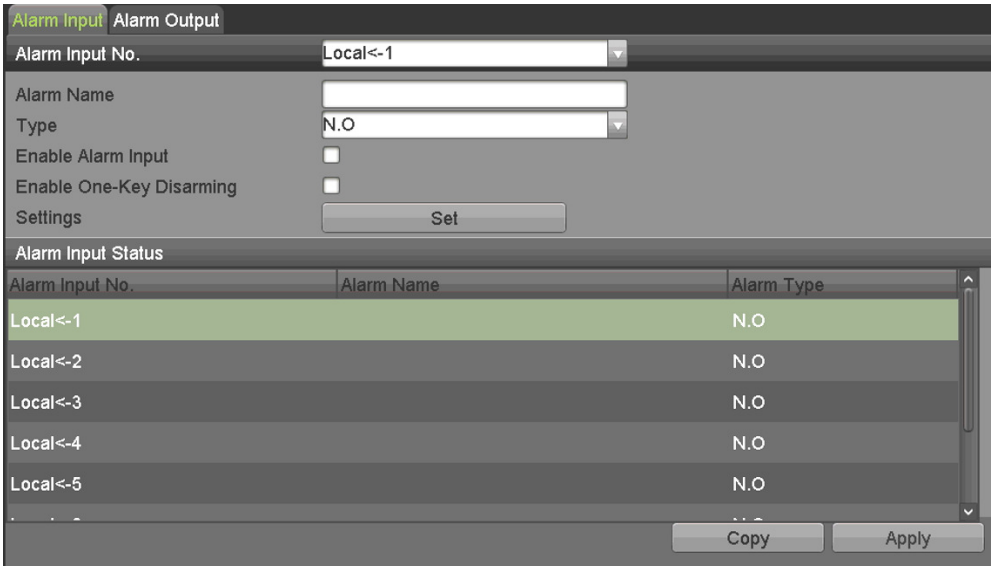


Figure 5-15 Alarm Settings - Alarm Input

2. Select Alarm Input No.
3. Input **Alarm Name**.
4. Select **N.O.** (normally open) or **N.C.** (normally closed) for alarm type.
5. Check the **Enable** checkbox to enable alarm.
6. Click the  after **Settings** to set the triggered channels, arming schedule, linkage actions, and PTZ linking. See *5.2*

Configuring Recording Schedule for detailed operations.

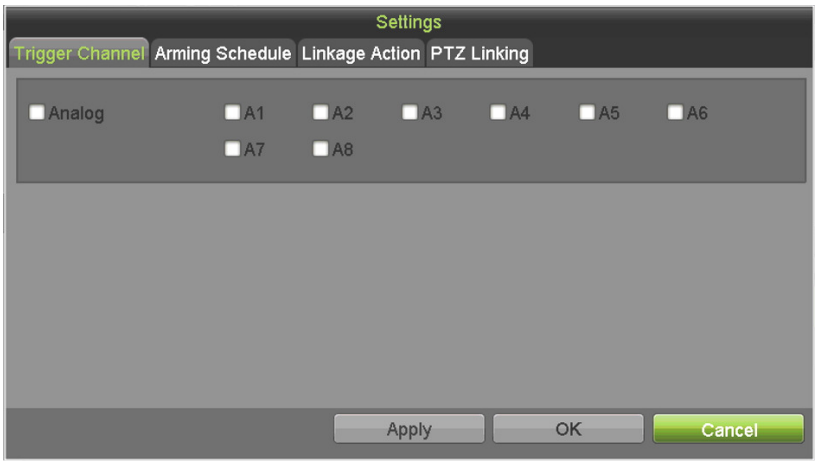


Figure 5-16 Trigger Channel

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

8. Repeat steps 1 to 8 to configure other alarm input parameters. If the settings can also be applied to other alarm inputs, click **Copy** and choose the alarm input number.

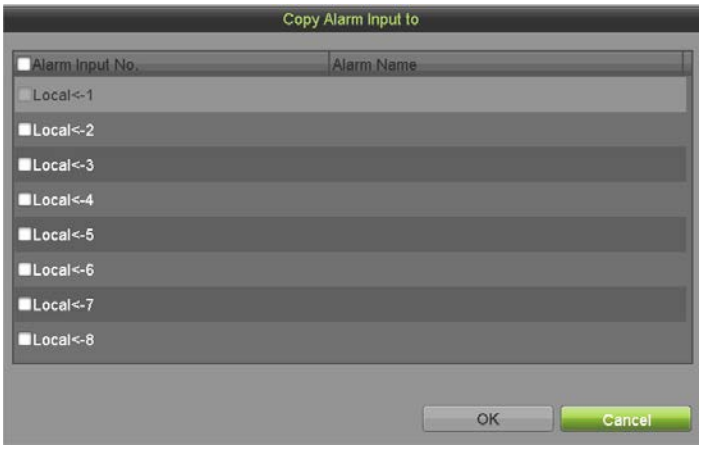


Figure 5-17 Copy Alarm Input

5.5 Configuring Event Recording

Purpose

Event triggered recording can be configured through the menu. These events include motion detection, alarms, 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

The DVR supports full-channel line crossing detection and intrusion detection, 2-ch sudden scene change detection, and audio exception 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.

1. Go to **Menu > Cameras Setup > VCA**.

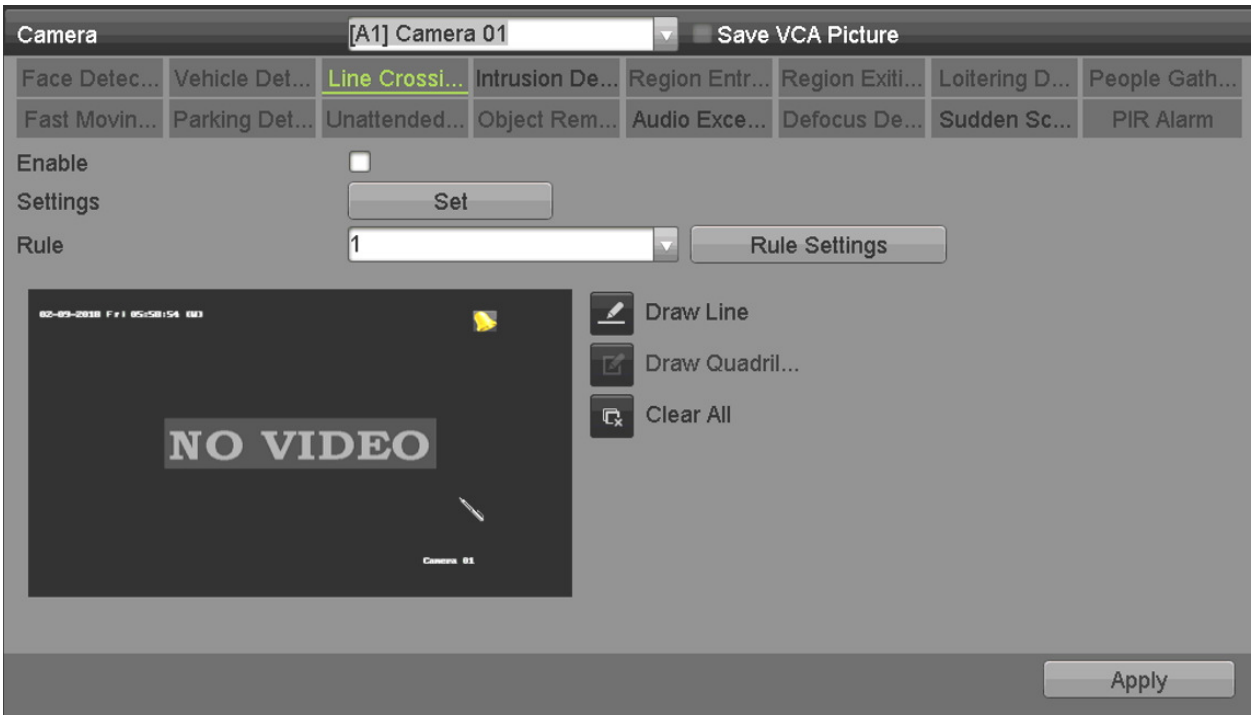


Figure 5-18 VCA Settings

2. Select a **Camera**.
3. Configure the detection rules for VCA events. See *9.3 Line Crossing Detection*.
4. Click **Set** to configure the alarm linkage actions for the VCA events.
5. Select **Trigger Channel** tab and select one or more channels to record when the VCA alarm is triggered.
6. Click **Apply** to save the settings.

Figure 5-19 Set Triggered Camera of VCA Alarm

7. Enter **Record Schedule Settings** interface (**Menu > Recording Configuration > Schedule**), and set **Event** as the record type. See *5.2 Configuring Recording Schedule.*

5.6 Configuring Manual Recording

Purpose

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

1. Go to **Menu > Manual > Record**.

Figure 5-20 Manual Record

2. Enable manual record.

   1) Click the OFF status icon before the camera number to change it to ON, or click the **Analog** OFF status icon to enable manual record of all channels.

3. Disable manual record.

   1) Click the ON status icon to change it to OFF, 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

Purpose

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

1. Go to **Menu > Recording Configuration > Holiday**.

Figure 5-21 Holiday Settings

2. Enable Edit Holiday schedule.

   1) Click  to enter the Edit interface.

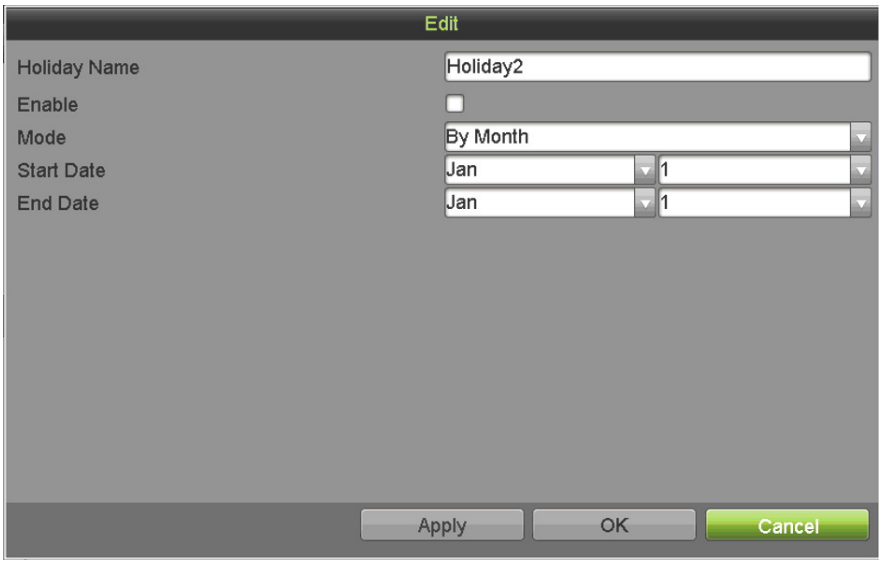


Figure 5-22 Edit Holiday Settings

   2) Check the **Enable** checkbox.

   3) 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.

      1) Set the start and end date.

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

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

3. Configure the record schedule. Refer to *5.2 Configuring Recording Schedule* and choose Holiday in the Schedule drop-down list, or you can draw the schedule on the Holiday timeline.

NOTE

Up to eight periods can be configured for each day, and the time periods cannot overlap.

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

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

5.8 Configuring Redundant Recording

Purpose

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

Before You Start

Set the HDD Advanced Settings **Storage Mode** to *Group* before setting the HDD property to Redundant. See *12.3 Managing HDD Group.* There must be at least one other HDD in Read/Write status.

1. Go to **Menu > System Configuration > HDD**.

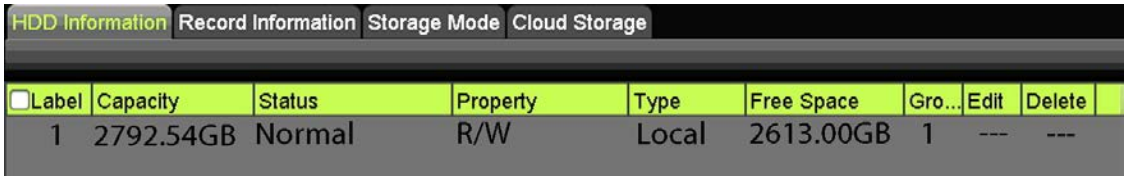


Figure 5-23 HDD Information

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

   1) Set the HDD property to **Redundant**.

Figure 5-24 HDD General-Editing

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

   3) Click **OK** to return to the upper level menu.

3. Go to **Menu > Recording Configuration > Record Quality > Record**.

1) Select the camera you want to configure.
2) Click **More Settings**.

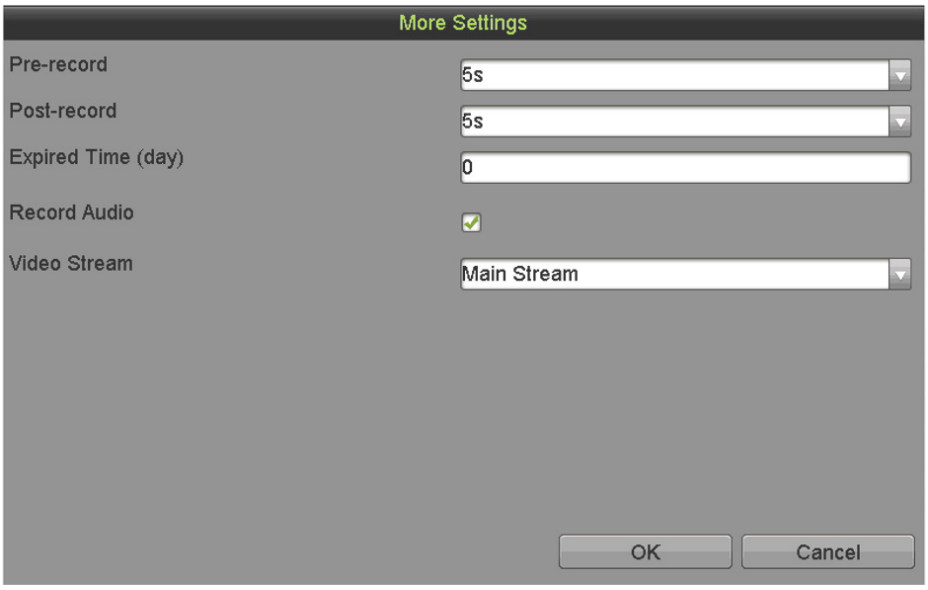


Figure 5-25 More Settings

3) Set the following parameters:
   a) **Pre-Record** – Enter the number of seconds to record before the triggered event.
   b) **Post-Record** – Enter the number of seconds to record after the triggered event.
   c) **Expired Time (day)** – Enter the number days to keep the recording.
   d) **Record Audio (checkbox)** – Check to enable audio recording.
   e) **Video Stream** – Use the pull-down menu to select the video stream to record.
4) Click **OK** to save the settings.
5) If the encoding parameters can also be used for other channels, click **Copy** and choose the channel for which you want to apply the settings.

5.9 Configuring HDD Group

Purpose

You can group the HDDs and save the record files by HDD group.

1. Go to **Menu > System Configuration > HDD > Storage Mode**, and check whether the storage mode of the HDD is **Group**. If not, use the pull-down menu to set the storage mode to **Group**. See *12.3 Managing HDD Group*.
2. Select the **HDD Information** tab.
3. Highlight an HDD.

4. Click to enter the editing interface.
5. Assign the HDD group.
   1) Use the radio selection button to choose a group number for the HDD group.
   2) Click **Apply** to save your settings.
   3) Click **OK** to return to the upper level menu.
6. Repeat the above steps to configure more HDD groups.
7. Choose the Channels for which you want to save the record files in the HDD group.
   1) Go to **Menu > System Configuration > HDD > Storage Mode**.

Figure 5-26 HDD Storage Mode

   2) Choose Group number in the **Record on HDD Group** drop-down list.
   3) Check the channels you want to save in this group.
   4) Click **Apply** to save settings.

NOTE

After configuring the HDD groups, configure the recording settings following the procedure in *Chapter 5.2-5.7*.

5.10 Files Protection

Purpose

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

Protect File by Locking the Record Files

1. Go to **Menu > File Management > Record**.

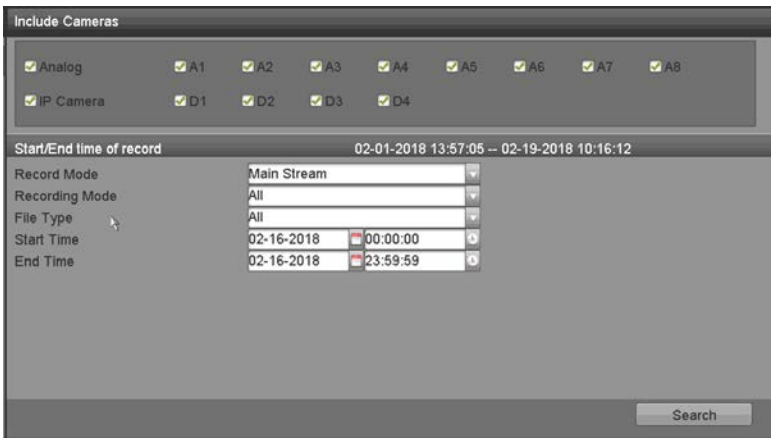


Figure 5-27 Export

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

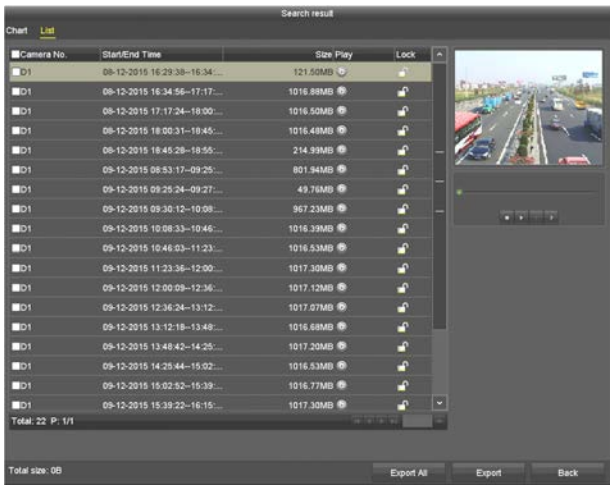


Figure 5-28 Export-Search Result

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

NOTE

Record files with recording not completed cannot be locked.

   2) Click to change it to to unlock the file; the file will not be protected.
   3) Protect files by setting the HDD property to Read-only

Before You Start

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

1. Go to **Menu > System Configuration > HDD > HDD Information**.

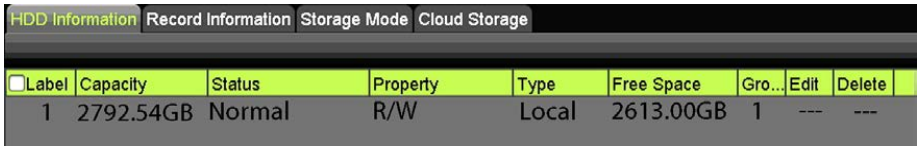


Figure 5-29 HDD Information

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

Figure 5-30 HDD Information - Editing

3. Set the HDD to Read-only.

4. Click **OK** to save the settings and return to the upper level menu.

NOTE

You cannot save any files to a Read-only HDD. To save files to the HDD, change the property to R/W.

If there is only one HDD and it 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 to it, the file will be saved in the next R/W HDD. If there is only one HDD, the recording will be stopped.

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

Purpose

You can one-key enable or disable H.264+/H.265+ for analog cameras.

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

1. Go to **Menu > System Configuration > HDD > Record Information**.

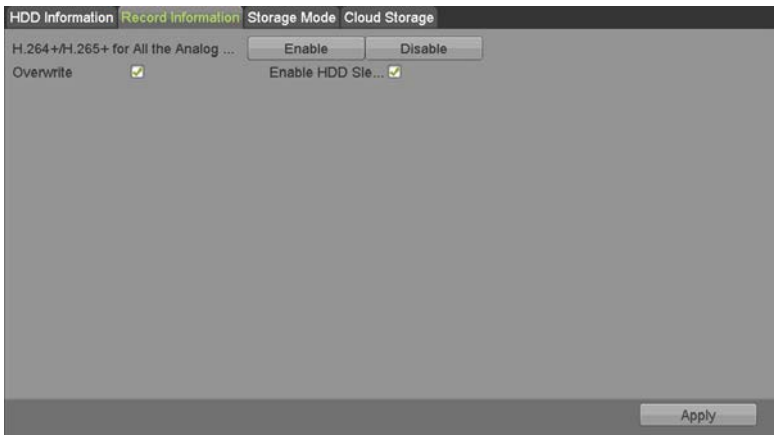


Figure 5-31 Advanced Settings

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

Figure 5-32 Attention Box

3. Click **Yes** to enable the function and reboot the device to have the new settings take effect.

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

1. Go to **Menu > System Configuration > HDD > Record Information**.
2. Click **Disable** to disable H.264+/H.265+ for all the analog cameras and the following box pops up.

Figure 5-33 Attention Box

3. Click **Yes** to enable the function and reboot the device to have new settings take effect.

Chapter 6 Playback

6.1 Playing Back Record Files

6.1.1 Instant Playback

Purpose

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

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 6-1 Instant Playback Interface

6.1.2 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.

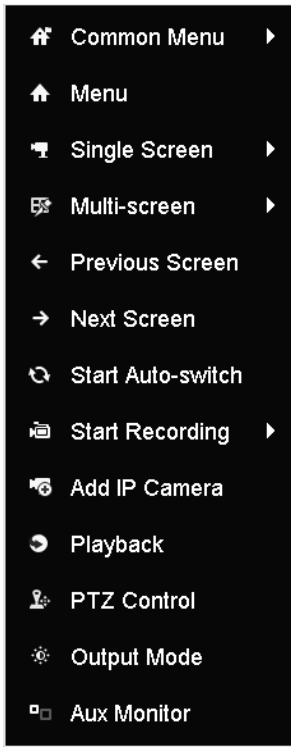


Figure 6-2 Right-click Menu under Live View

Playback by Time

Purpose

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

1. Go to **Menu > Playback**.
2. Check the checkbox of channel(s) in the channel list, then double-click to select a calendar date.

Figure 6-3 Playback Calendar

NOTE

If there are record files for that camera on a day, the color for that day shows Normal Record or Event Record.

Playback Interface

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

You can also use the toolbar at the bottom of the **Playback** interface to control the playing progress.

Figure 6-4 Playback Interface

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

Figure 6-5 Playback Toolbar

Table 1-12 Detailed Explanation of the Playback Toolbar

Icon	Operation	Icon	Operation	Icon	Operation
/	Audio on/mute	/	Start/stop clipping		Lock file
	Add default tag		Add customized tag		File management for video clips, captured pictures, locked files and tags
/	Reverse play/pause		Stop		Digital zoom
	30s forward		30s reverse	/	Pause/play
	Fast forward		Previous day		Slow forward
	Full screen		Exit		Next day
	Save the clips		Process bar	/	Scaling up/down the time line
	Capture picture		Enable/disable POS information overlay		

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 on the progress bar to locate special frames.

6.1.3 Playing Back by Event Search

Purpose

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. Go to **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.

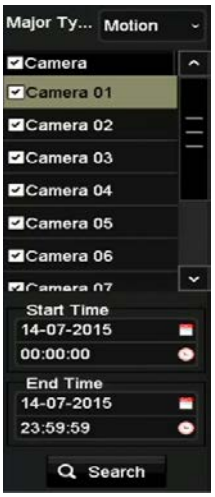


Figure 6-6 Video Search by Motion Detection

4. Click **Search**, and the record files matching the search conditions will be displayed on a list.
5. Select and click to play back the record files.
   - Click **Back** to return to the search interface.
   - If there is only one channel triggered, clicking takes you to **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.

Figure 6-7 Select Channels for Synchronous Playback

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

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

Figure 6-8 Playback by Event Interface

Pre-play and post-play can be configured for playback of event triggered record files.

- **Pre-play:** The time you set to play back before the event. For example, when an alarm triggered the recording at 10:00, if you set the pre-play time as 5 seconds, the video plays back from 9:59:55.
- **Post-play:** The time to play back after the event. Example: When an alarm triggered recording ends at 11:00, if you set the post-play time as 5 seconds, the video plays back until 11:00:05.

7. Click ◀ or ▶ to select the previous or next event.

6.1.4 Playing Back by Tag

Purpose

Video tags allow 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 time points.

Before Playing Back by Tag

1. Go to **Menu > Playback**.
2. Search and play back the record file(s). Refer to *6.1.2 Playing Back by Normal Search* for detailed information about searching and playback of the record files.

Figure 6-9 Playback by Time Interface

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

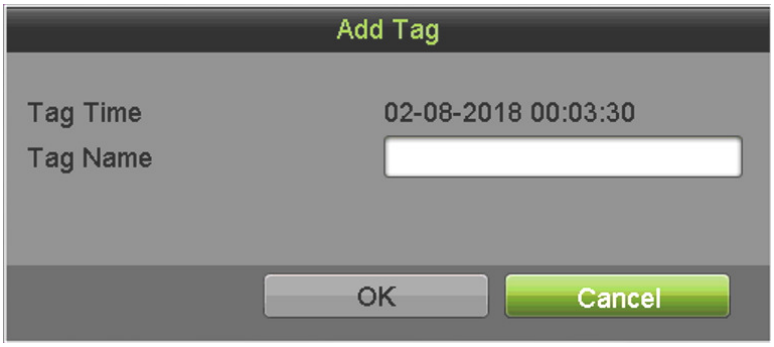


Figure 6-10 Add Tag

NOTE

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

Tag Management

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

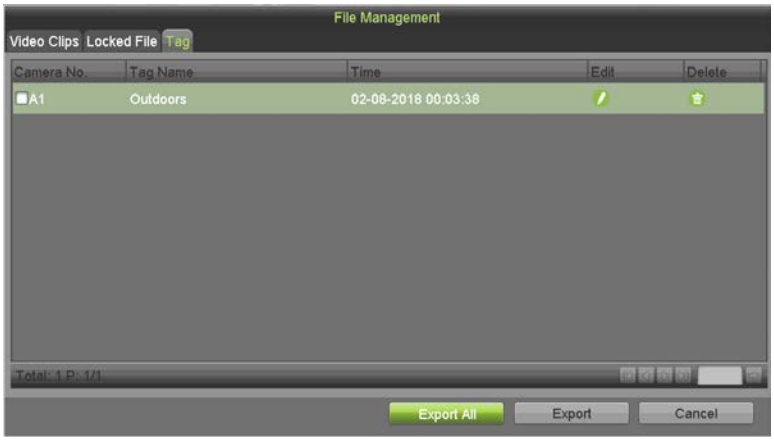


Figure 6-11 Tag Management Interface

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

NOTE

You can enter keyword in the textbox Keyword to search for the tag.

Figure 6-12 Video Search by Tag

2. Click to play back the file.

3. You can click **Back** to return to the search interface.

NOTE

Pre-play and post-play can be configured.

Click or to select the previous or next tag.

6.1.5 Playing Back by Smart Search

Purpose

The **Smart Playback** function provides an easy way to get through the less relevant information. When you select **Smart Playback** mode, the system will analyze the video containing the motion or VCA information, mark it in green, and play it at normal speed, while the video without motion will be played at 16x speed. The **Smart Playback** rules and areas are configurable.

Before You Start

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

1. Log into the IP camera through a Web browser, and enable intrusion detection by checking the checkbox. You may enter the motion detection configuration interface by going to **Configuration > Advanced Configuration > Events > Intrusion Detection**.

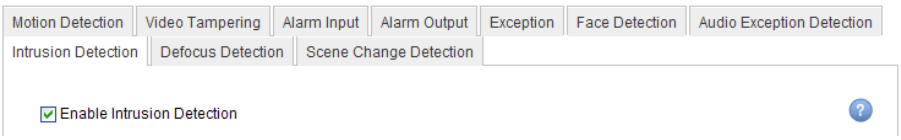


Figure 6-13 Setting Intrusion Detection on IP Camera

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.

   1) Go to **Menu > Playback**.

   2) Select **Smart** in the drop-down list on the top-left.

   3) Select a camera in the camera list.

Figure 6-14 Smart Playback Interface

   4) Select a date in the calendar and **click** to play.

Table 1-13 Explanation of the Smart Playback Toolbar

Icon	Operation	Icon	Operation	Icon	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				

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

   - **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.

4. Click to configure the smart settings.

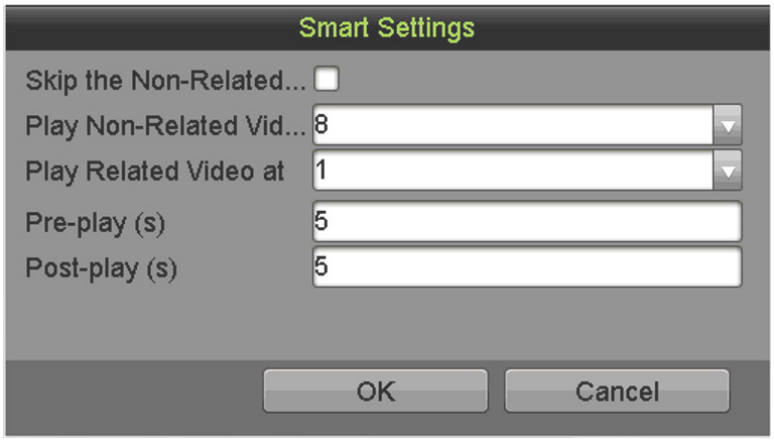


Figure 6-15 Smart Settings

- **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. Maximum 8/4/2/1 are selectable.
- **Play Related Video at:** Set the speed to play the related video. Maximum 8/4/2/1 are selectable.

NOTE

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

5. Click to search and play the matched video files.

6. (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 6-16 Set Result Filter

NOTE

The **Result Filter** function is supported by IP cameras only.

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

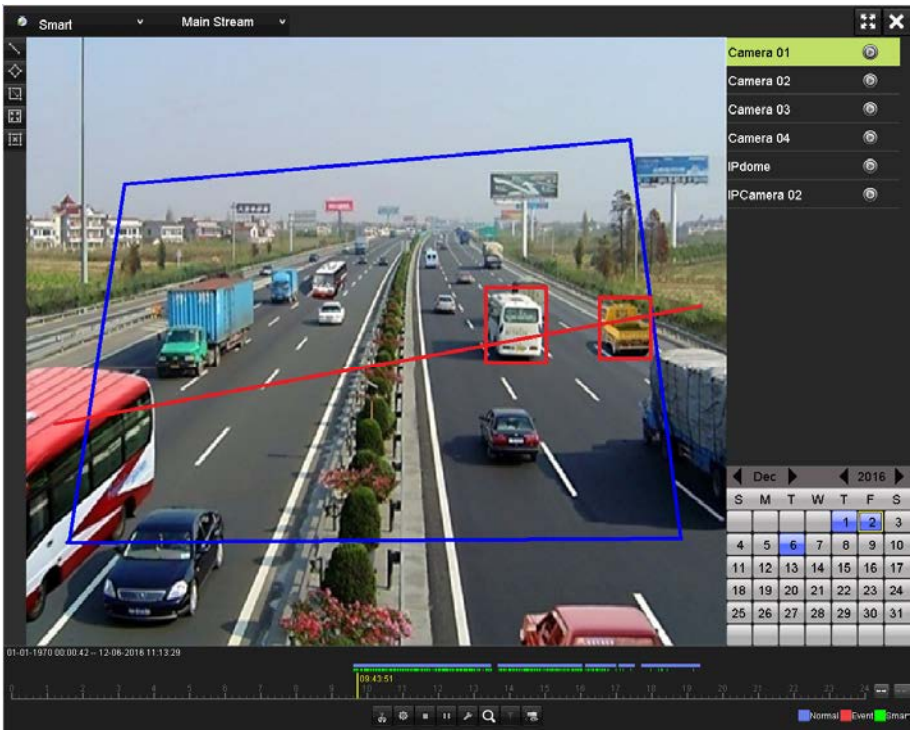


Figure 6-17 Show VCA Information

NOTE

In smart playback, both the 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 smart IP camera VCA detections.

6.1.6 Playing Back by System Logs

Purpose

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

1. Go to **Menu > Maintenance > System Logs**.

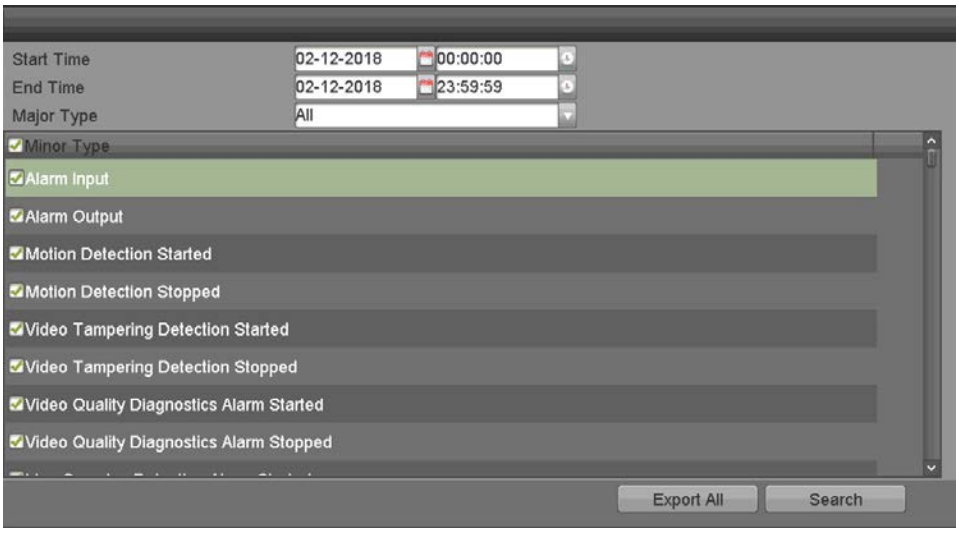


Figure 6-18 System Log Search Interface

2. Set search time and type and click **Search**.
3. Choose a log with a record file and click to enter the **Playback** interface.

NOTE

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

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

Figure 6-19 Playback by Log Interface

6.1.7 Playing Back by Sub-Periods

Purpose

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

1. Go to **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 6-20 Sub-periods Playback Interface

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.

6.1.8 Playing Back an External File

Purpose

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

1. Go to **Menu > Playback**.
2. Select the **External File** in the drop-down list on the top-left.
   - The files are listed in the right-side list.

- Click Refresh to refresh the file list.

3. Select and click to play it.

Figure 6-21 External File Playback Interface

6.2 Auxiliary Playback Functions

6.2.1 Playing Back Frame-by-Frame

Purpose

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

1. Go to the Playback interface and click until the speed changes to *Single* frame.
2. One click on the playback screen represents playback or reverse playback of one frame. Use in the toolbar to stop playing.

6.2.2 Digital Zoom

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

Figure 6-22 Digital Zoom Draw Area

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

6.2.3 Reverse Playback of Multi Channels

Purpose

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

1. Go to **Menu > Playback**.
2. Check checkbox(es) to select multiple channels and click to select a date on the calendar.

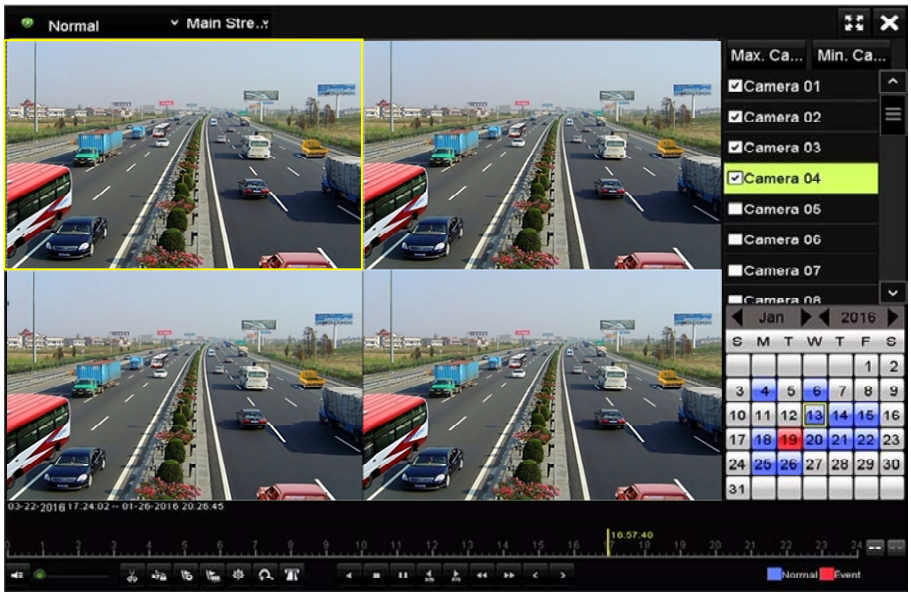


Figure 6-23 4-ch Synchronous Playback Interface

3. Click ◀ to play back the record files in reverse.

6.2.4 File Management

Purpose

Manage video clips, pictures captured in playback, locked files, and tags added in playback mode.

1. Go to **Menu > File Management > Record**.

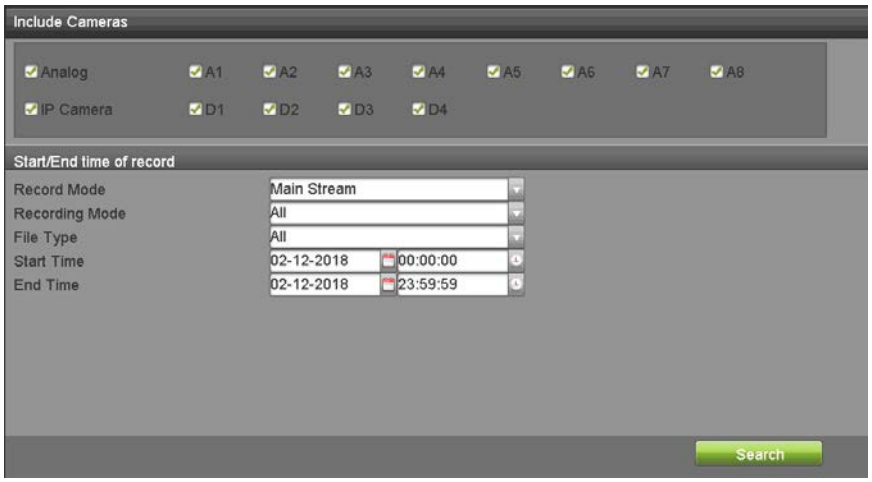


Figure 6-24 File Management > Record

2. Check the cameras you wish to search.
3. Set the search filters:
   a. Record Mode
      - Main Stream
      - Sub Stream
   b. Recording Mode
      - Continuous
      - Event
      - Manual
      - All
   c. File Type
      - Unlocked
      - Locked
      - All
   d. Start Time
   e. End Time

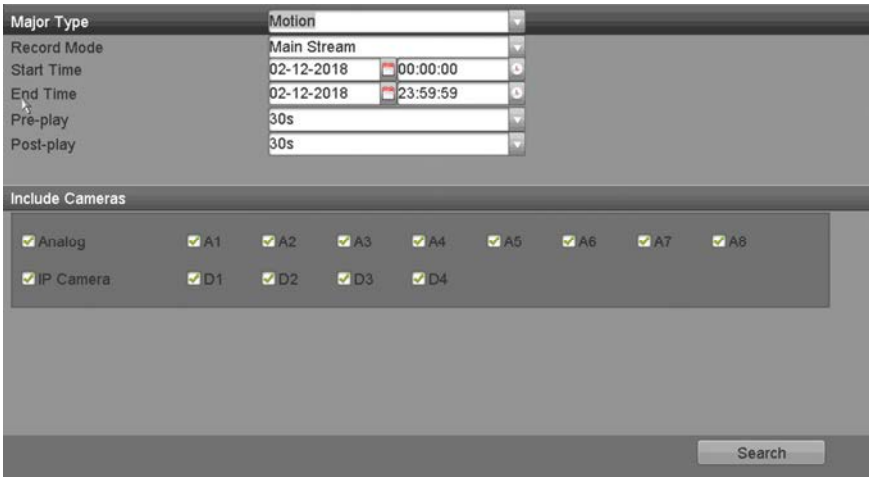


Figure 6-25 File Management > Event

4. You can view the saved video clips, captured playback pictures, lock/unlock the files, and edit the tags that you added in the playback mode.

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

Chapter 7 Backup

7.1 Backing up Record Files

Before You Start

Attach the backup device(s) to the DVR.

7.1.1 Backing up by Normal Video/Picture Search

Purpose

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

Back up Using USB Flash Drives and USB HDDs.

1. Go to **Menu > File Management**.

- **To Choose Record Files To Back Up**

    1. Select **Record** on the left panel.
    2. Use the checkboxes to select which cameras to search.
    3. Set the search conditions.
        a. Record Mode
        b. Recording Mode
        c. File Type
        d. Start Time
        e. End Time
    4. Click **Search** to display the found files.

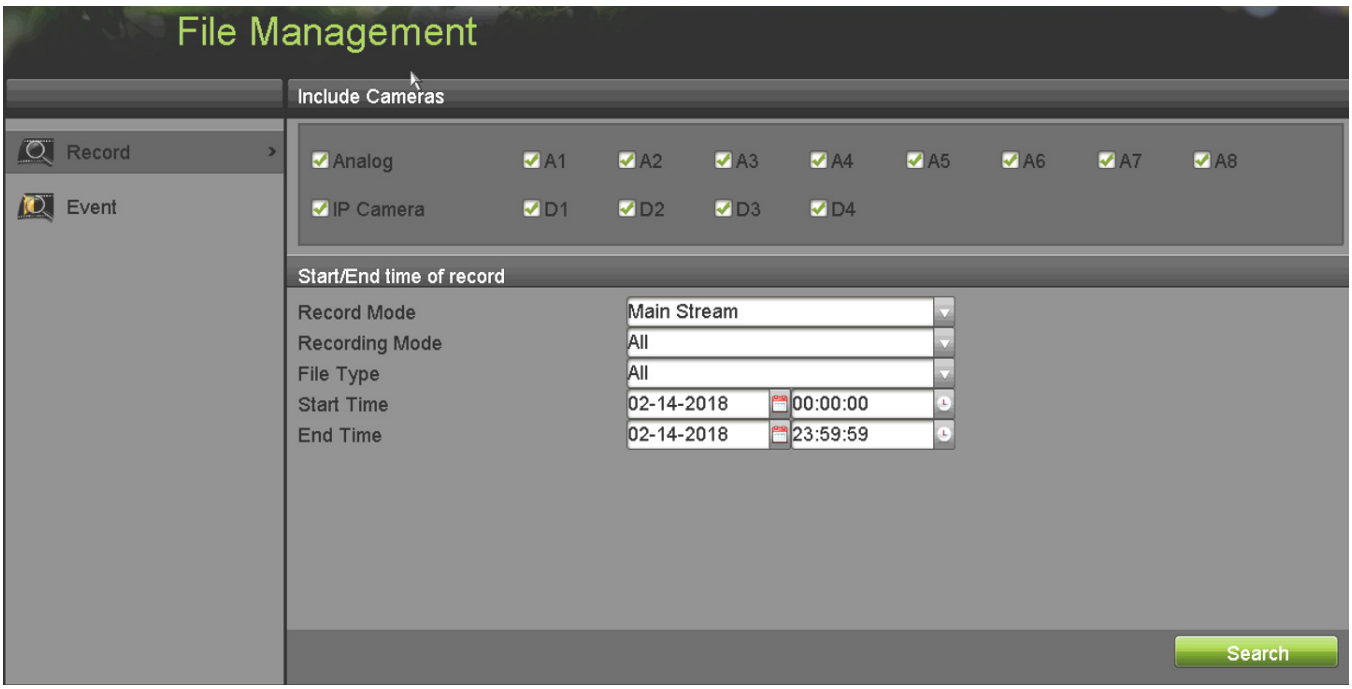


Figure 7-1 Menu > File Management > Record

- **To Choose the Event Files To Back Up:** Select **Event** on the left panel.

1. Select **Event** on the left panel.
2. Set the search conditions.
    a. Major Type
    b. Recording Mode
    c. Start Time
    d. End Time
    e. Pre-Play
    f. Post-Play
3. Use the checkboxes to select which cameras to search.
4. Click **Search** to display the found files.

Figure 7-2 Menu > File Management > Event

2. The matched video files are displayed in **Chart** or **List** display mode.

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

   2) Check the checkbox adjacent to the video files you want to back up.

NOTE

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

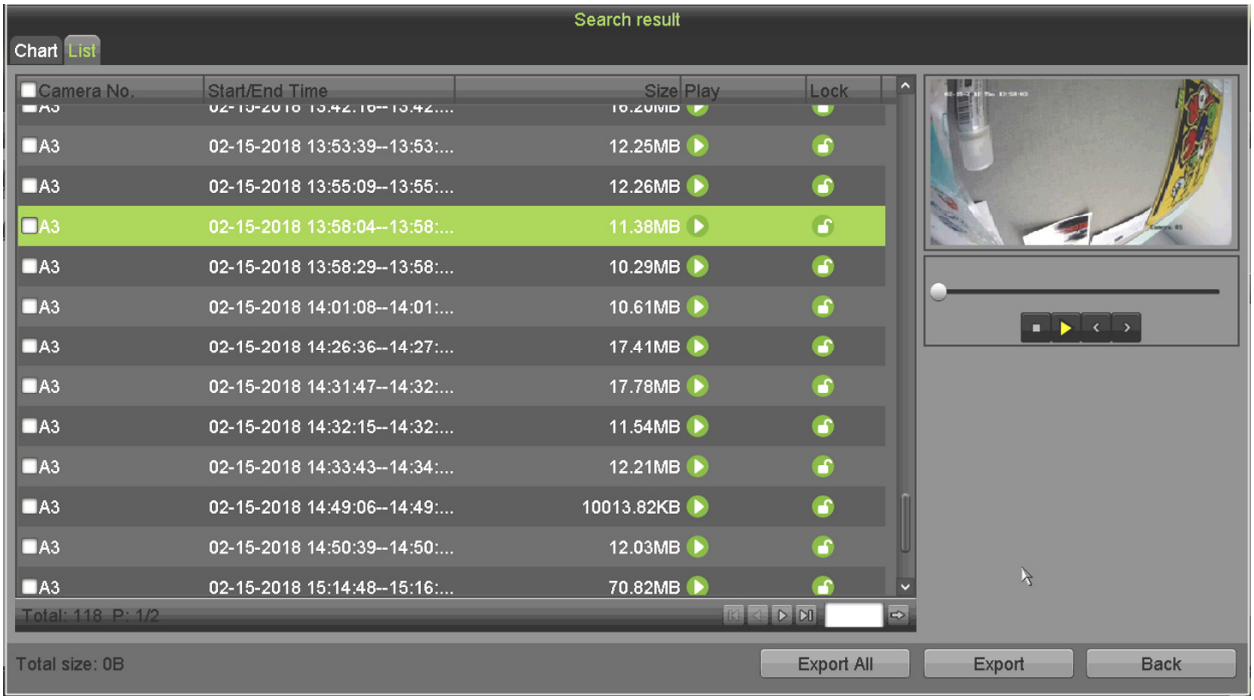


Figure 7-3 Search Result

3. Select video files from the **Chart** or **List** to export, and 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.

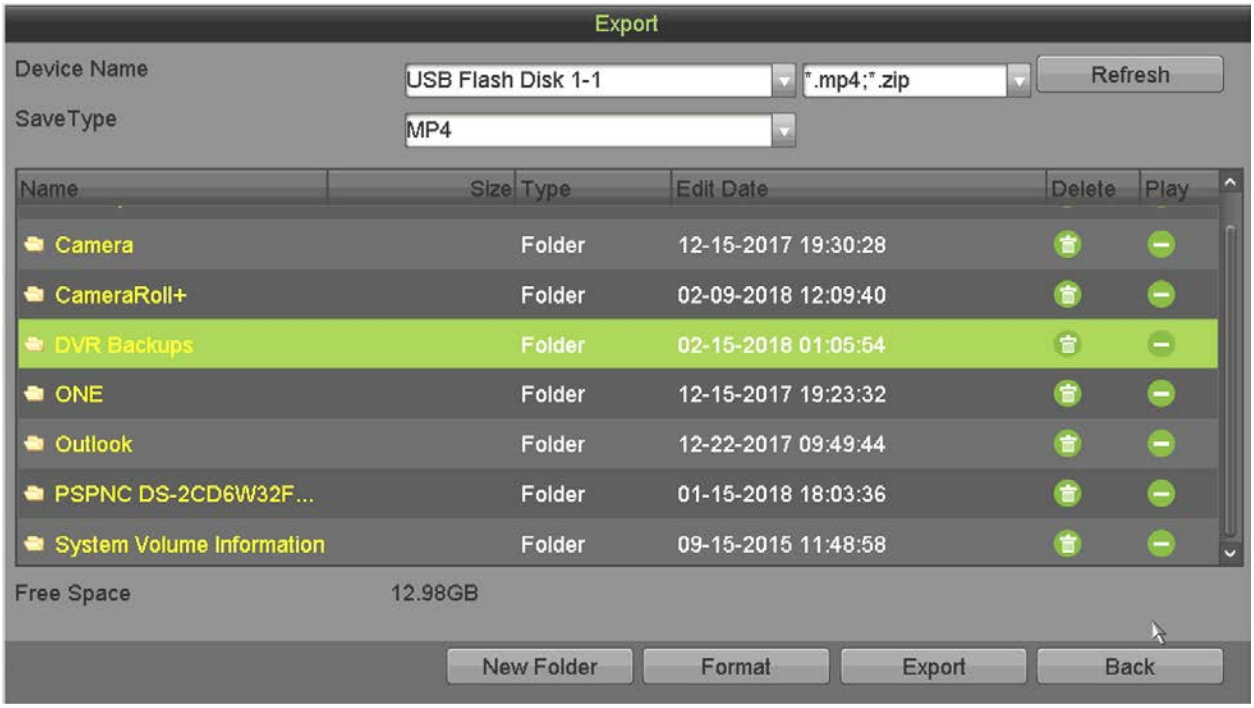


Figure 7-4 Export using USB Flash Drive

4. Select the backup device from the drop-down list and you can also select the file format to filter the files existing in the backup device.

5. Select the saving format type.

6. Click **Export** on the Export interface to start the backup process.

   1) On the pop-up message box, click the radio button to export the video files, log, or the player to the backup device.

   2) Click **OK** to confirm.

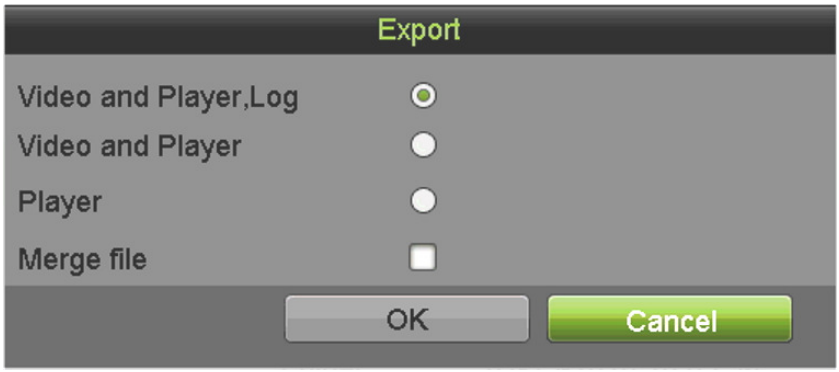


Figure 7-5 Select File or Player for Backup

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

Figure 7-6 Export Finished

NOTE

Backing up pictures using a USB writer or SATA writer uses the same procedures as above.

7.1.2 Backing up Video Clips

Purpose

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

1. Go to **Menu > Playback**.
2. During playback, use or in the playback toolbar to start or stop clipping record file(s).

Figure 7-7 Menu > Playback

3. Click  to enter the file management interface.

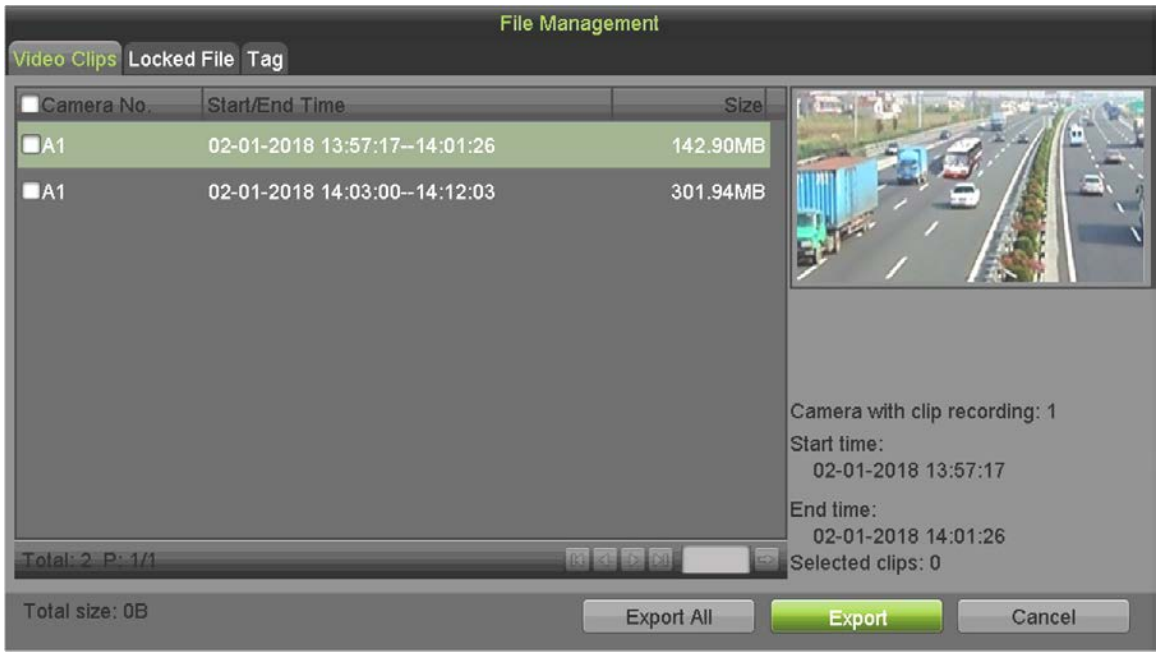


Figure 7-8 Video Clips Export Interface

4. Check the checkboxes of video clips you want to export.
5. Click **Export**.

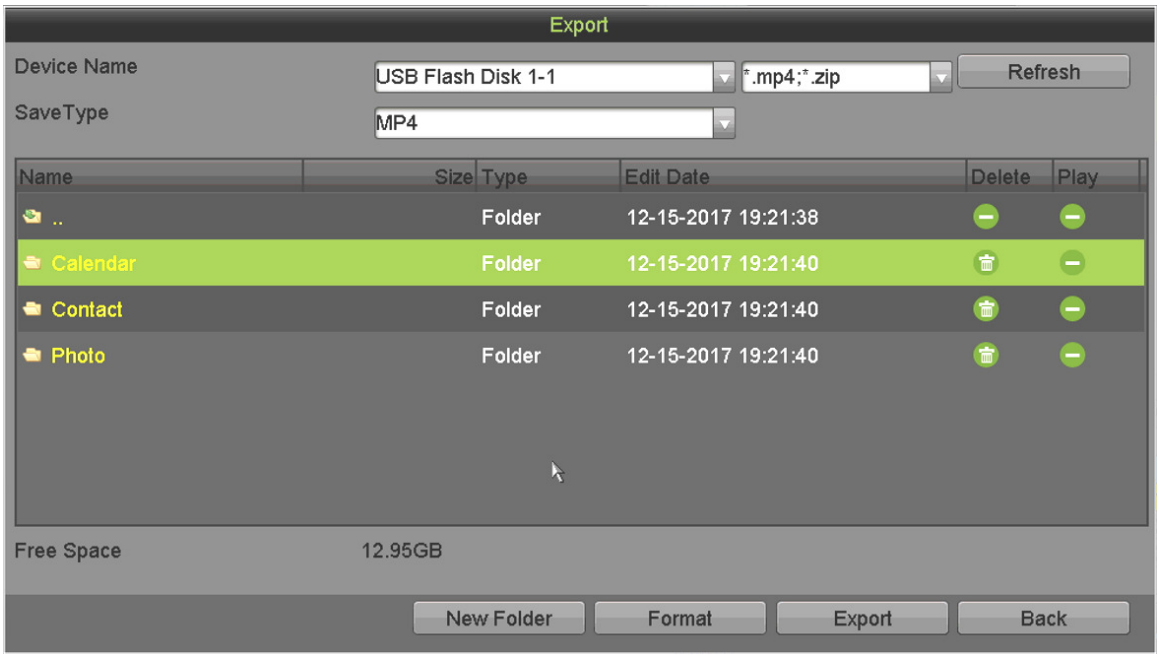


Figure 7-9 Export

6. Double-click a folder to save the chosen video clips to (click **New Folder** to create a new folder).
7. Click **Export** to save the video clips.

8. To format the disk, click **Format**.

9. To delete a file, highlight the file and click  .

NOTE

If the inserted storage device is not recognized, click **Refresh**. If it is still not recognized, disconnect then reconnect the device. If it is still not recognized, check for compatibility from vendor.

Chapter 8 Alarm Settings

8.1 Setting Motion Detection

1. Go to **Menu > Recording Configuration > Motion Detect**.

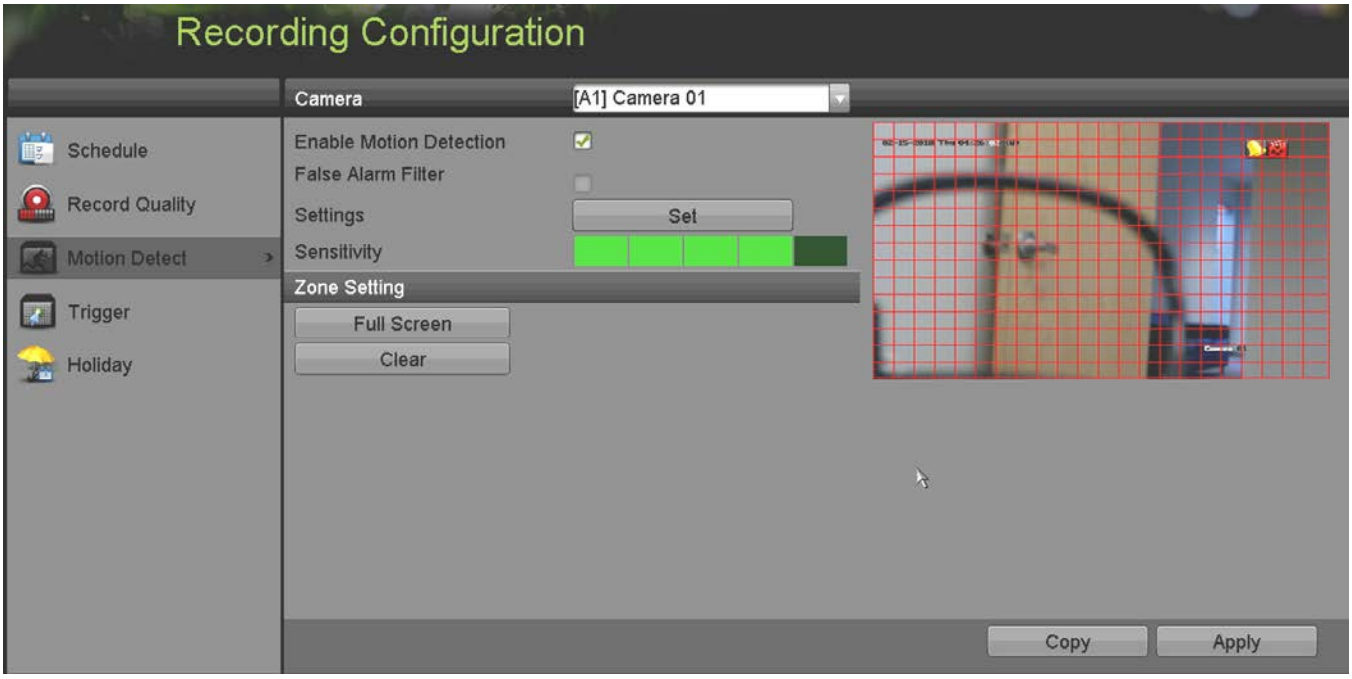


Figure 8-1 Motion Detection Setup Interface

2. Select a camera for which you want to set up motion detection.
3. Set detection area and sensitivity.
   1) Check ☑ checkbox to enable motion detection. Use the mouse to draw detection area(s) or click **Full Screen** to set the detection area to be the full screen, and drag the sensitivity bar to set sensitivity.
   2) Click **Set** to set alarm response actions.

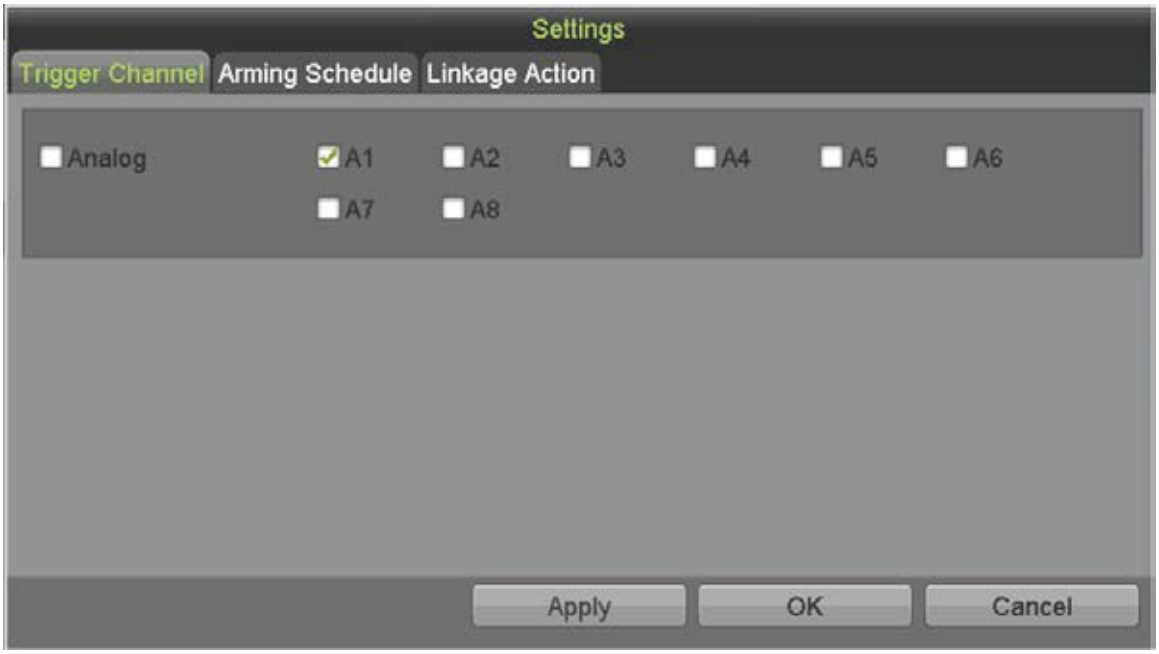


Figure 8-2 Set Motion Detection Trigger Camera

4. Click **Trigger Channel** tab and select one or more channels which will start to record or become full-screen monitoring when motion alarm is triggered.

5. Set the channel's arming schedule.

   1) Select **Arming Schedule** tab.

   2) Choose one day of a week, with up to eight time periods set within each day, or click **Copy** to copy the time period settings to other day(s).

NOTE

Time periods cannot repeat or overlap.

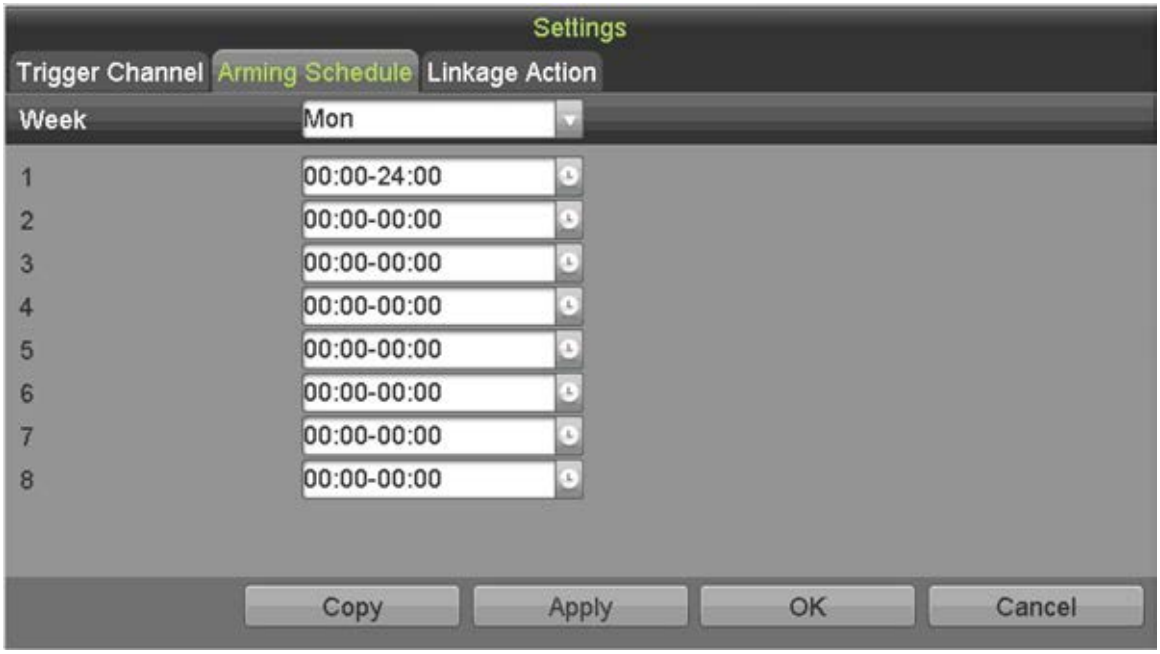


Figure 8-3 Set Motion Detection Arming Schedule

6. Click **Linkage Action** tab to set up motion alarm response actions (refer to *8.8* Setting Alarm Response Actions).

Figure 8-4 Set Motion Detection Linkage Action

7. Repeat the above steps to set up arming schedule for other days of the week.
8. Click **OK** to complete the channel motion detection settings.
9. To set motion detection for another channel, repeat the above steps or copy the above settings to it.

NOTE

You are not allowed to copy the "Trigger Channel" action.

8.2 Setting PIR Camera Alarm

Purpose

DVR can receive the PIR (Passive Infrared) alarm of the analog cameras supporting the function via coaxial communication. You can enable the false alarm filter for the motion detection of the PIR cameras. Then, the motion detection alarm will be triggered only when the motion detection event and PIR event are both triggered, and the alarm indicator will light on for the PIR cameras supporting enabling alarm indicator.

Before You Start

Connect the PIR camera to the DVR. Configure **White Light** as **Alarm** and **Trigger Mode** as **DVR** for the camera OSD.

1. Go to **Menu > Recording Configuration > Motion Detect**.

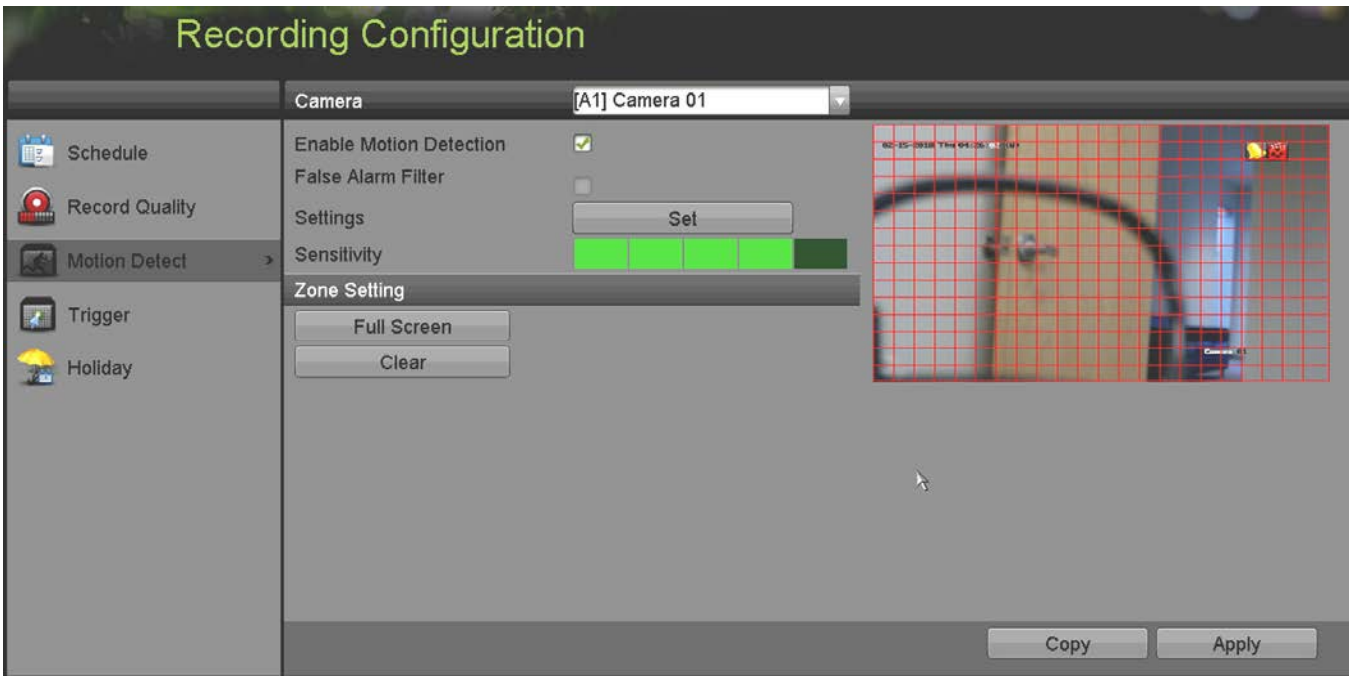


Figure 8-5 Motion Detection

2. Select the connected PIR camera.
3. Check Enable Motion Detection.
4. Check **False Alarm Filter** to enable PIR motion detection. The message box pops up as below.

Figure 8-6 Note

5. Click **OK** to enable PIR motion detection. Then, only when the motion detection events and PIR events are both triggered, the motion detection alarm will be triggered.
6. Set detection area and sensitivity. Refer to *8.1 Setting Motion Detection*.
7. Click **Set** to set motion detection alarm response actions. See *8.1 Setting Motion Detection*.
8. Click **Apply** to save the settings.

NOTE

This function is applicable only to Hikvision PIR analog cameras.

The PIR alarm does not support detection area configuration. It is full screen by default.

The PIR alarm does not support sensitivity configuration.

If you disable the false alarm filter, only when the motion detection events are triggered will the motion detection alarm be triggered. The PIR alarm will not be considered.

8.3 Setting Sensor Alarms

Purpose

Set up external sensor alarm handling method.

1. Go to **Menu > Recording Configuration > Trigger > Alarm Input**.

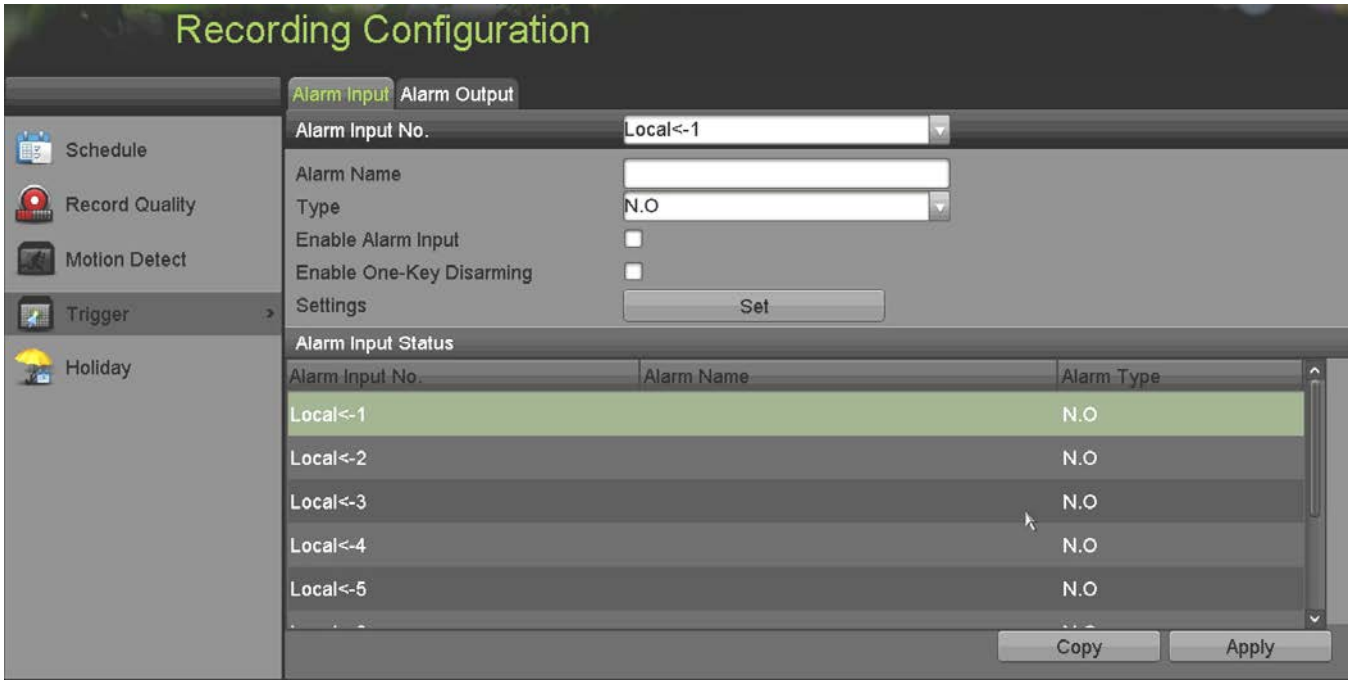


Figure 8-7 Alarm Input Settings Interface

2. Set the handling method of the selected alarm input.

   1) Check the **Enable Alarm Input** checkbox and click **Set** to set its alarm response actions.

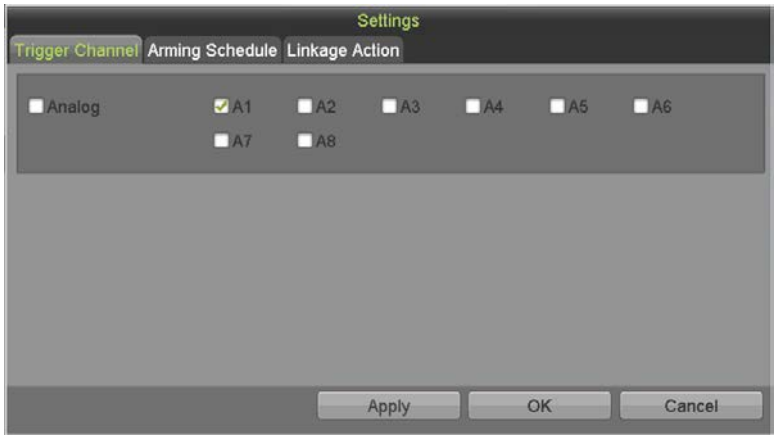


Figure 8-8 Set Trigger Channel of Alarm Input

3. Select **Trigger Channel** tab and select one or more channels which will start to record or become full-screen monitoring when an external alarm input is triggered.

4. Select **Arming Schedule** tab to set the channel's arming schedule.

1) Select one day of a week, and a maximum of eight time periods can be set within each day.

NOTE

Time periods shall not repeat or overlap.

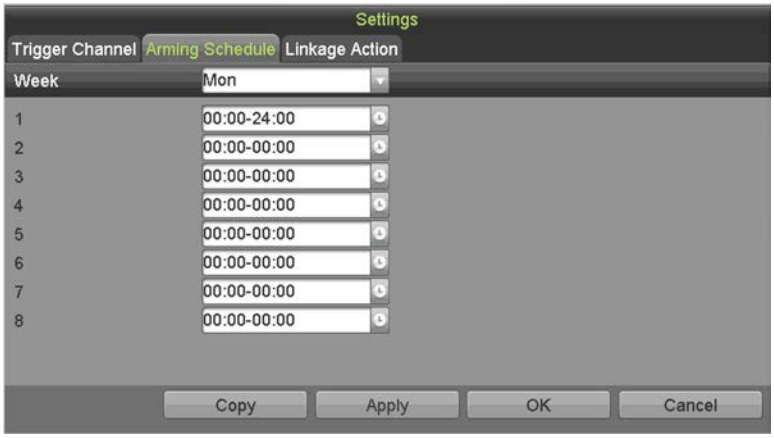


Figure 8-9 Alarm Arming Schedule

5. Select **Linkage Action** tab to set up alarm response actions of the alarm input (refer to *8.8 Setting Alarm Response Actions*).

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

Figure 8-10 Alarm Linkage Actions

6. (Optional) Select **PTZ Linking** tab and set PTZ linkage of the alarm input.

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

NOTE

Check whether the PTZ or speed dome supports PTZ linkage.

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

Figure 8-11 Set PTZ Linking of Alarm Input

7. If you want to set handling action of another alarm input, repeat the above steps or just copy the above settings to it.

Figure 8-12 Copy Alarm Input Settings

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

   1) Check the **Enable One-Key Disarming** checkbox.

   2) Click **Settings** to enter the linkage action settings interface.

   3) Select the alarm linkage action(s) you want to disarm for the local alarm input 1. Linkage actions include Full Screen Monitoring, Audible Warning, Notify Surveillance Center, Send E-mail, Upload Captured Pictures to Cloud, and Trigger Alarm Output.

Figure 8-13 Disarm Linkage Actions

NOTE

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

8.4 Detecting Video Loss

Purpose

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

1. Go to **Menu > Cameras Setup > Video Loss**.

Figure 8-14 Video Loss Setup Interface

2. Select a **Camera** you want to detect.
3. Set up the video loss handling method.
   1) Check the **Enable Video Loss Alarm** checkbox.
   2) Click **Set** to set up the video loss handling method.

4. Set the channel's arming schedule.

   1) Select the **Arming Schedule** tab to set the channel's arming schedule.

   2) Choose one day of a week, and up to eight time periods can be set within each day.

NOTE

Time periods must not repeat or overlap.

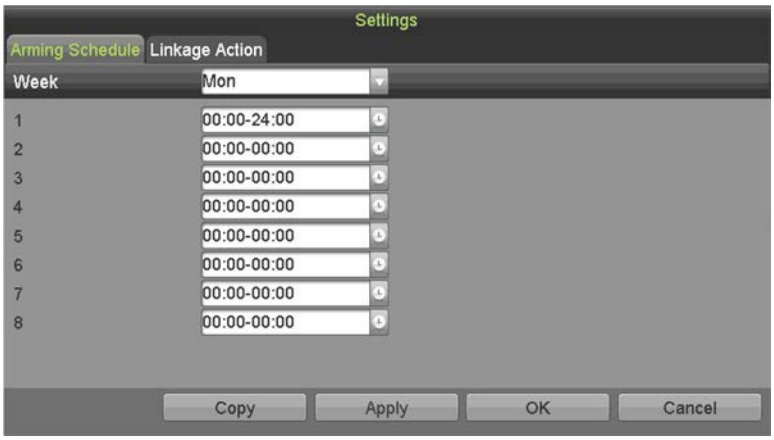


Figure 8-15 Set Video Loss Arming Schedule

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

5. Select the **Linkage Action** tab to set up the alarm response action of video loss (refer to *8.8 Setting Alarm Response Actions*).

Figure 8-16 Video Loss Linkage Action

6. Click **OK** to complete the channel's video loss settings.

7. Repeat the above steps to finish setting other channels, or click **Copy** to copy the settings to them.

8.5 Detecting Video Tampering

Purpose

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

1. Go to **Menu > Cameras Setup > Video Tampering Detection**.

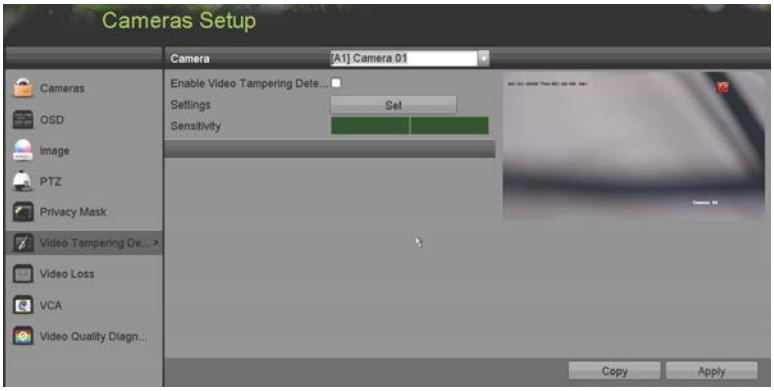


Figure 8-17 Video Tampering Interface

2. Select a **Camera** for which you want to detect video tampering.
3. Check the **Enable Video Tampering Detection** checkbox.
4. Drag the sensitivity bar and choose a sensitivity level.
5. Click **Set** to set the video tampering handling method. Set the channel's arming schedule and alarm response actions.
   1) Click the **Arming Schedule** tab to set the response action arming schedule.
   2) Select one day of a week, with up to eight time periods set within each day.

NOTE

Time periods must not repeat or overlap.

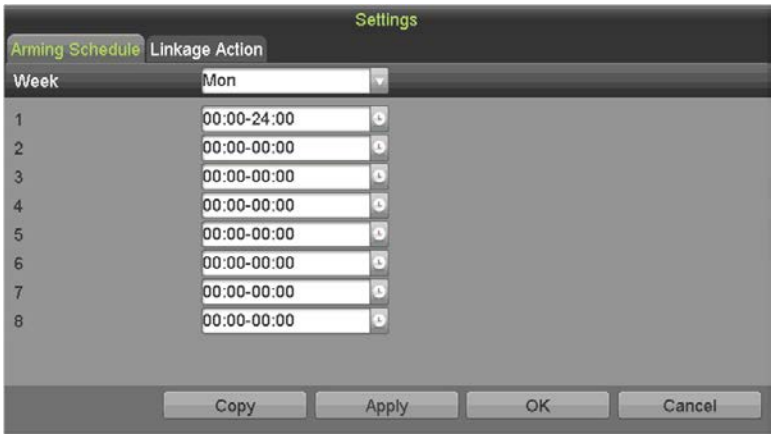


Figure 8-18 Set Video Tampering Arming Schedule

3) Select **Linkage Action** tab to set the video tampering alarm response actions of (refer to *8.8 Setting Alarm Response Actions*).

4) Repeat the above steps to set arming schedule for other days of the week. You can use **Copy** to copy an arming schedule to other days.

5) Click **OK** to complete the channel's video tampering settings.

6) Repeat the above steps to finish setting other channels, or click **Copy** to copy the above settings to them.

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

Figure 8-19 Video Tampering Linkage Action

8.6 Setting All-Day Video Quality Diagnostics

Purpose

The device provides two ways to diagnose the video quality: manual and all-day. Perform the following steps to set the diagnosing threshold and the linkage actions.

1. Go to **Menu > Cameras Setup > Video Quality Diagnostics**.

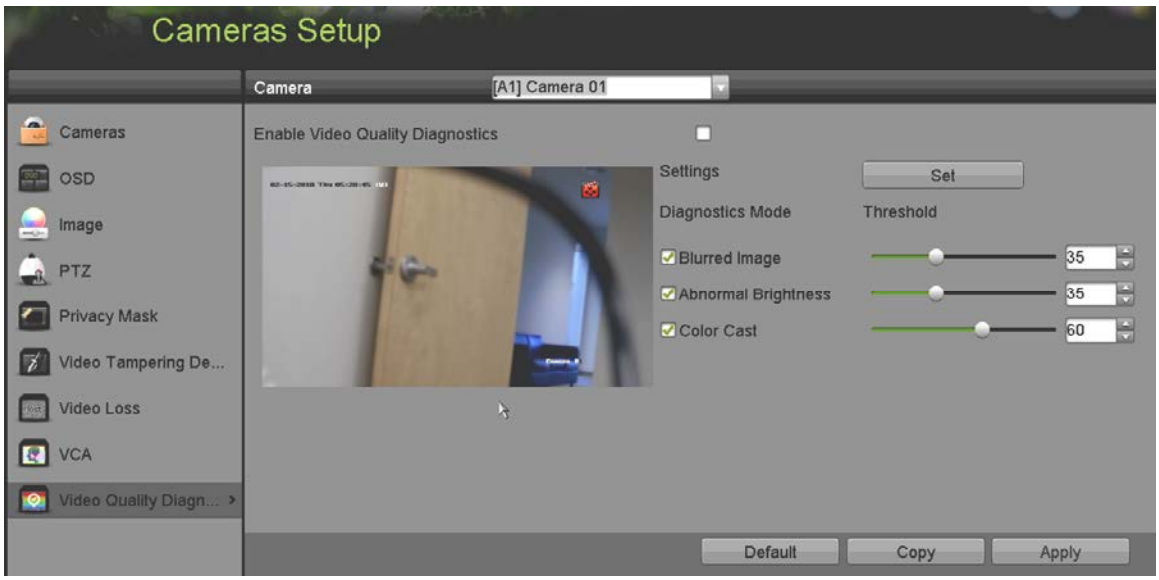


Figure 8-20 Video Quality Diagnostics Interface

2. Select a **Camera** for which you want to detect video tampering.
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, there are **Blurred Image**, **Abnormal Brightness**, and **Color Cast**.

   1) Check the corresponding checkbox of the diagnostic type, and adjust its threshold by dragging the bar.

NOTE

The higher the threshold set, the harder it will be to have the exception detected.

5. Click **Set** to configure the video quality diagnostics handling method. Set the channel's arming schedule and alarm response actions.

   1) Click **Arming Schedule** tab to set the response action arming schedule.

   2) Choose one day of a week, and up to eight time periods can be set within each day.

NOTE

Time periods must not repeat or overlap.

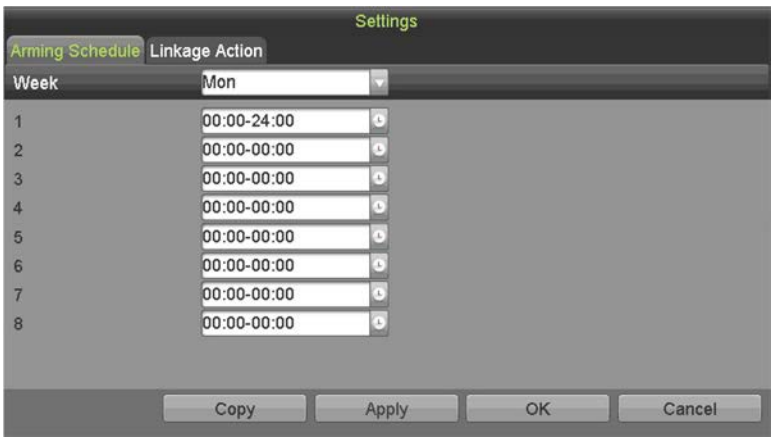


Figure 8-21 Set Video Quality Diagnostics Arming Schedule

3) Select the **Linkage Action** tab to set the alarm's video quality diagnostics alarm response actions (refer to *8.8 Setting Alarm Response Actions*).

4) Repeat the above steps to set the arming schedules for other days of the week. You can also use **Copy** to copy an arming schedule to other days.

5) Click **OK** to complete the channel's video quality diagnostics settings.

Figure 8-22 Video Quality Diagnostics Linkage Action

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

7. (Optional) Copy the same settings to other cameras by clicking **Copy**.

8.7 Handling Exceptions

Purpose

Exception settings refer to the handling method of various exceptions.

- **HDD Full:** The HDD is full
- **HDD Error:** Writing HDD error, unformatted HDD, etc.
- **Network Disconnected:** Disconnected network cable
- **IP Conflicted:** Duplicate IP address

- **Illegal Login:** Incorrect user ID or password
- **Input/Recording Resolution Mismatch:** The input resolution is lower than the recording resolution
- **Record/Capture Exception:** No space for saving recorded files or captured pictures
- **PoC Module Exception:** DVR cannot detect PoC module or PoC module powered off abnormally

1. Go to **Menu > System Configuration > Exceptions**.

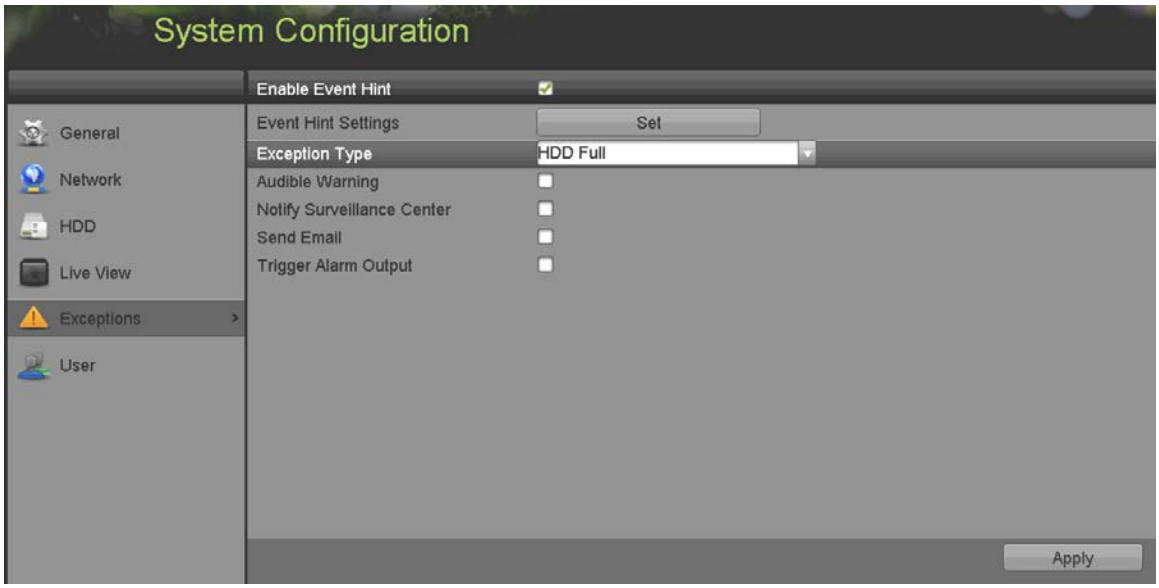


Figure 8-23 Exception Settings Interface

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

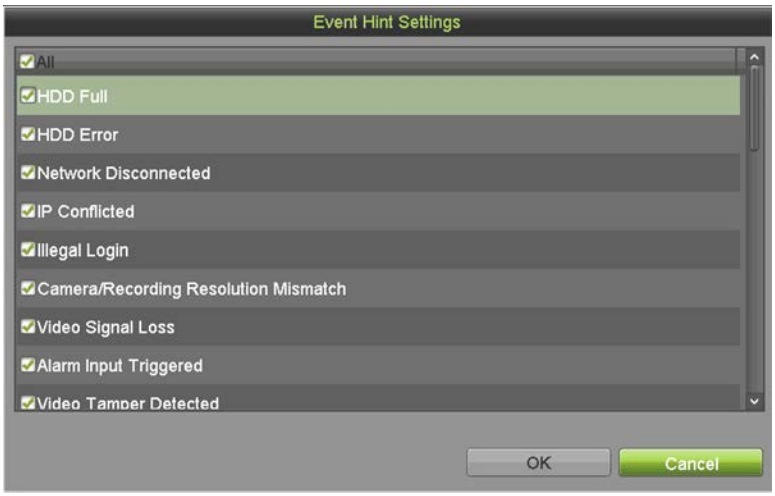


Figure 8-24 Event Hint Settings

NOTE

Click in the live view interface to view detailed information of the exceptional event. Click **Set**, and then select the detailed event hint for display.

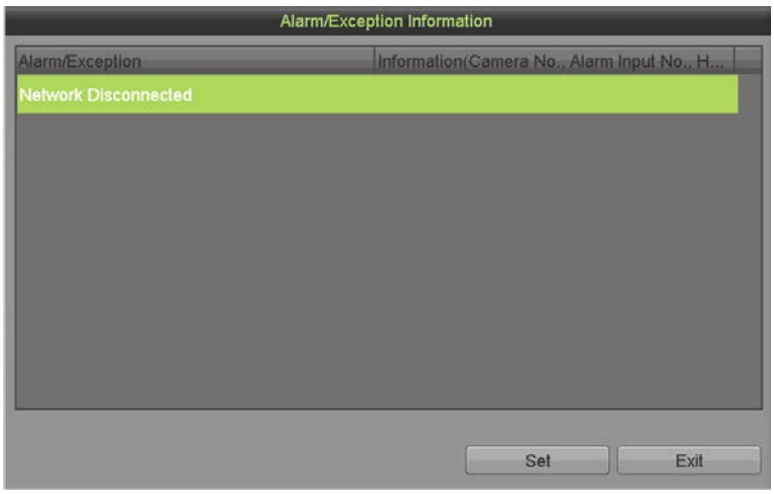


Figure 8-25 Detailed Event

3. Set the alarm linkage actions. For details, *8.8 Setting Alarm Response Actions*.
4. Click **Apply** to save the settings.

8.8 Setting Alarm Response Actions

Purpose

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 at an interval of 10 seconds (default dwell time). A different dwell time can be set by going to **Menu > System Configuration > Live View**.

Auto switching 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 the PC installed with Remote Client.

NOTE

The alarm signal will be transmitted automatically at detection mode when the remote alarm host is configured. See *11.2.5 Configuring More Settings* for details of alarm host configuration.

Send E-Mail

Send an e-mail with alarm information to a user or users when an alarm is detected (see *11.2.7 Configuring Email* for details of e-mail configuration).

Trigger Alarm Output

Trigger an alarm output when an alarm is triggered.

1. Go to **Menu > Recording Configuration > Trigger > Alarm Output**.
2. Select an alarm output, and set the alarm name and dwell time.

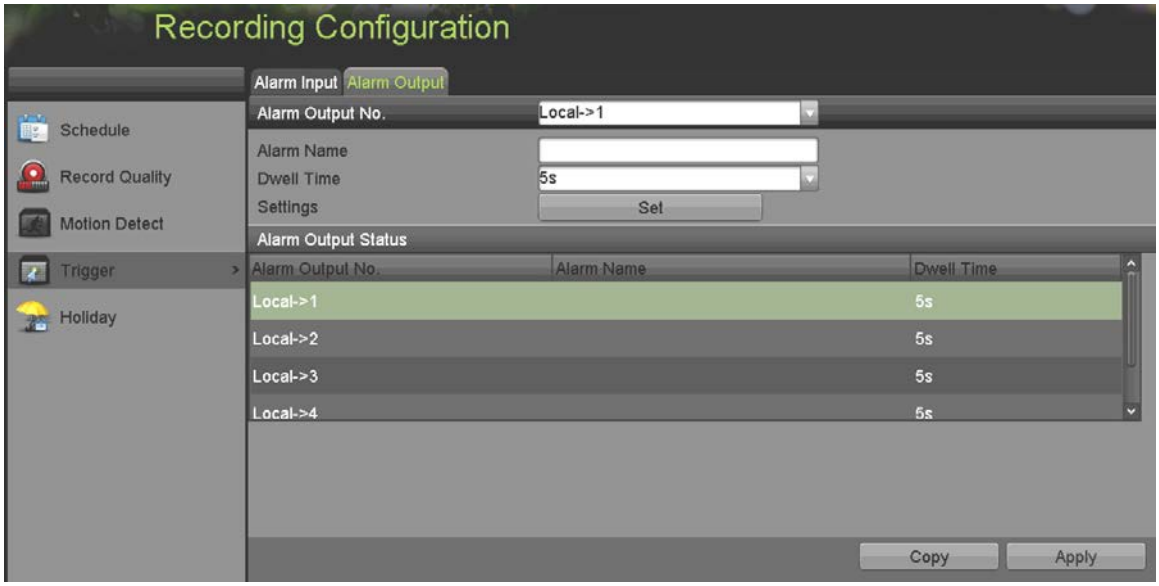


Figure 8-26 Alarm Output Settings Interface

NOTE

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

3. Click **Set** to set the alarm output arming schedule.

   1) Choose a day of the week, with up to eight time periods within each day.

NOTE

Time periods must not repeat or overlap.

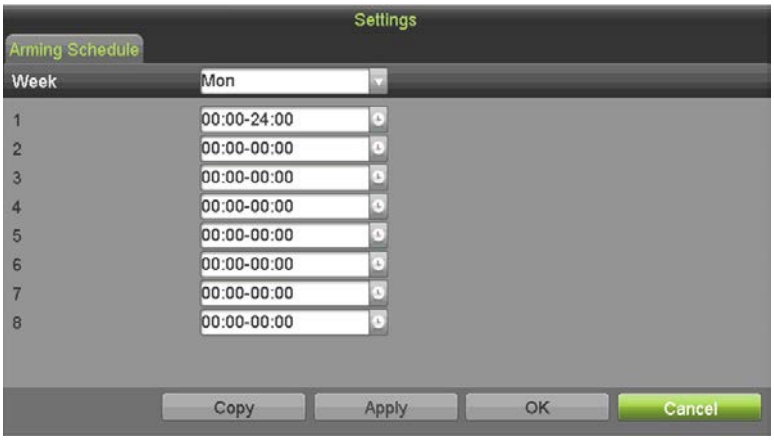


Figure 8-27 Set Alarm Output Arming Schedule

4. Repeat the above steps to set arming schedules for other days of the week. You can also click **Copy** to copy an arming schedule to other days.

5. Click **OK** to complete the alarm output arming schedule setting.

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

Chapter 9 VCA Alarm

Purpose

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

NOTE

The DVR supports full-channel line crossing detection, intrusion detection, 2-ch sudden scene change detection, and audio exception 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.

9.1 Face Detection

Purpose

Face detection detects faces appearing in the surveillance scene, and certain actions can be taken when the alarm is triggered.

1. Go to **Menu > Cameras Setup > 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.

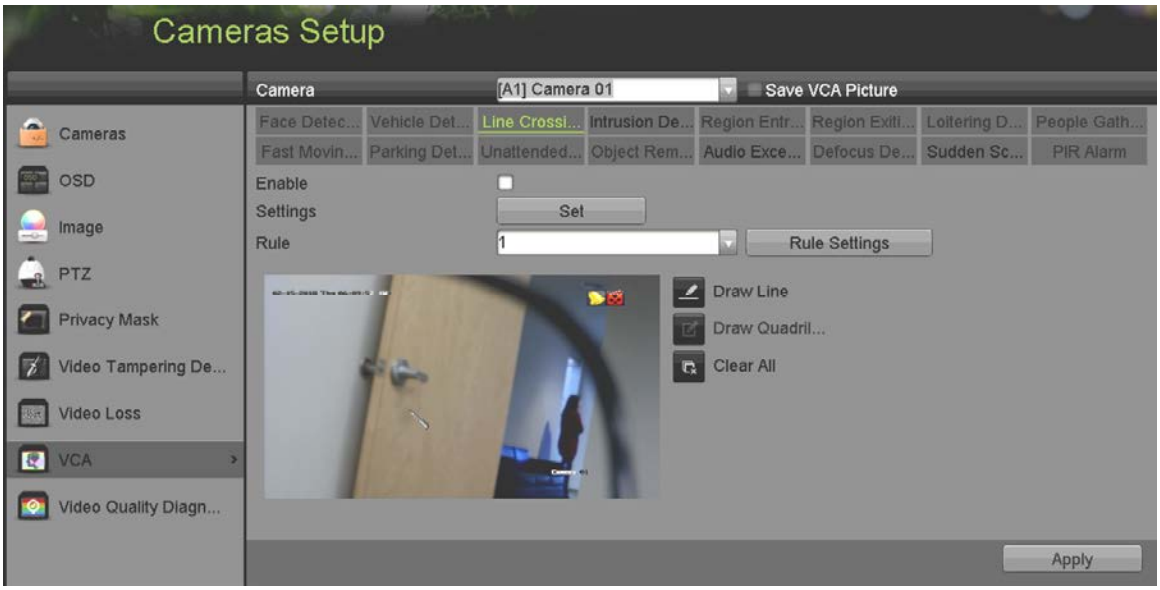


Figure 9-1 Face Detection

4. Set the VCA detection type to **Face Detection**.

5. Click **Set** to enter the Face Detection Settings interface. Configure the trigger channel, arming schedule, linkage action, and PTZ linking for the face detection alarm. Refer to *8.3 Setting Sensor Alarms* for detailed instructions.

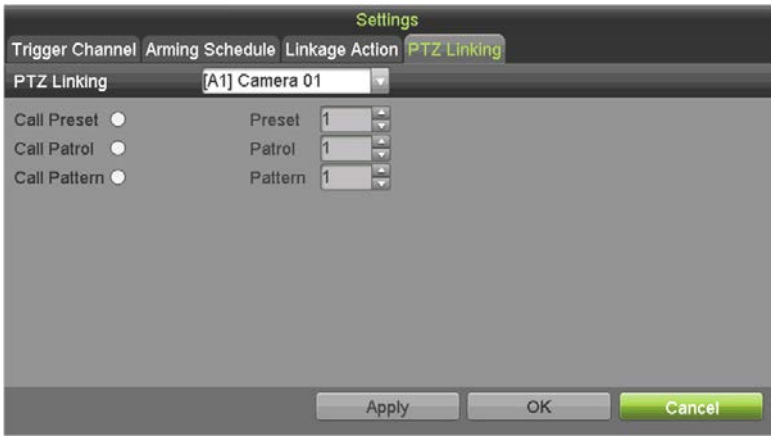


Figure 9-2 PTZ Linking

6. Click **Rule Settings** to set the face detection rules. You can drag the slider to set the detection sensitivity.

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

Figure 9-3 Set Face Detection Sensitivity

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

9.2 Vehicle Detection

Purpose

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

1. Go to **Menu > Camera Setup > 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 **Vehicle Detection**.

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

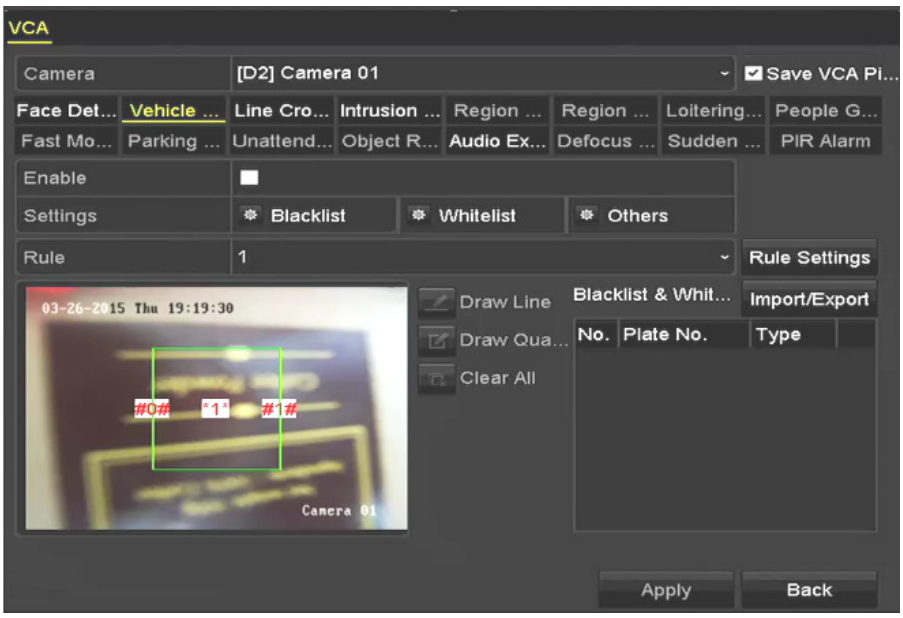


Figure 9-4 Set Vehicle Detection

6. Click **Set** to configure the trigger channel, arming schedule, linkage action, and PTZ linking.

NOTE

PTZ linking is applicable only to other lists, not to whitelist or blacklist.

7. Click **Rule Settings** to enter the rule settings interface. Configure the lane, upload picture, and overlay content settings. Up to four lanes are selectable.

Figure 9-5 Rule Settings

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

NOTE

See the network camera user manual for detailed instructions for the vehicle detection.

9.3 Line Crossing Detection

Purpose

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

1. Go to **Menu > Camera Setup > VCA**.
2. Select the camera for which to configure the VCA. Check the **Save VCA Picture** checkbox to save the captured VCA detection pictures.
3. Set the VCA detection type to **Line Crossing Detection**.
4. Check the **Enable** checkbox to enable this function.
5. Click **Set** to configure the trigger channel, arming schedule, linkage action, and PTZ linking for the line crossing detection alarm.
6. Click **Rule Settings** to set the line crossing detection rules.
   1) Set the direction to **A<->B**, **A->B**, or **B->A**.

      A<->B: Only the arrow on the B side shows. When an object crosses the configured line, both directions can be detected and alarms are triggered.

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

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

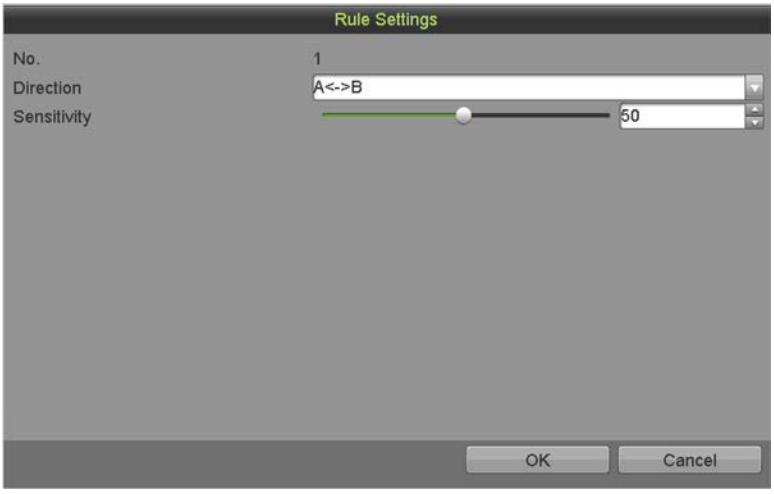


Figure 9-6 Set Line Crossing Detection Rules

7. Click and set two points in the preview window to draw a virtual line. Use to clear the existing virtual line and re-draw it.

NOTE

Up to four rules can be configured.

Figure 9-7 Draw Line for Line Crossing Detection

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

NOTE

Sudden scene change detection and line crossing detection cannot be enabled on the same channel.

9.4 Intrusion Detection

Purpose

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

1. Go to **Menu > Camera Setup > 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 **Set** 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.
   1) **Threshold:** Range [1s-10s], the threshold for the time the object loiters in the region. If the object stays in the defined detection area longer than the set time, the alarm will be triggered.

2) Drag the slider to set the detection sensitivity.

Sensitivity: Range [1-100]. Defines the size of the object that will trigger the alarm. The higher the value, the more easily the detection alarm is triggered.

Percentage: Range [1-100]. Defines the ratio of the in-region part of the object that will trigger the alarm. For example, if the percentage is set as 50%, if the object enters the region and occupies half of the whole region, the alarm is triggered.

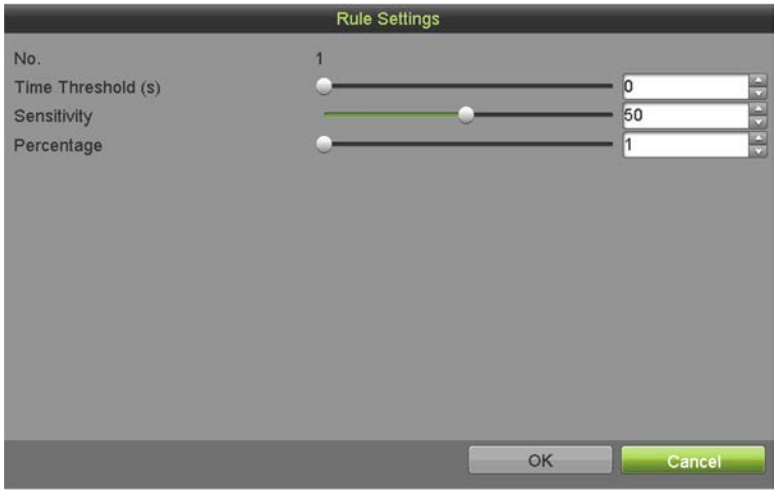


Figure 9-8 Set Intrusion Crossing Detection Rules

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

8. Click and draw a quadrilateral in the preview window by specifying the four vertices of the detection region, and right click to complete drawing. Only one region can be configured. Use to clear the existing virtual line and re-draw it.

NOTE

Up to four rules can be configured.

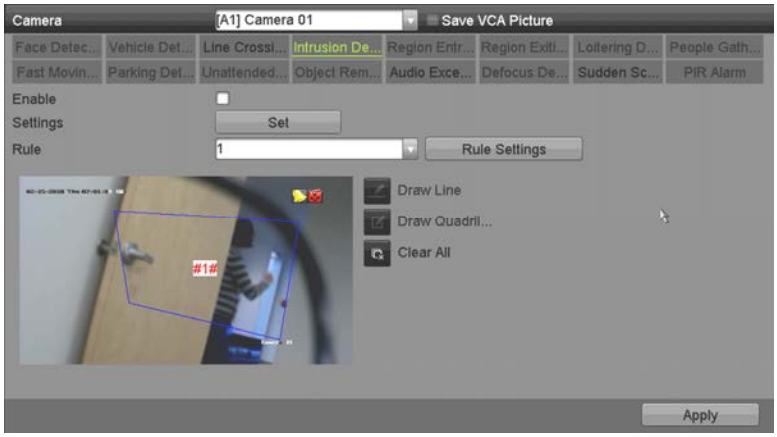


Figure 9-9 Intrusion Detection Draw Area

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

NOTE

Sudden scene change detection and intrusion detection cannot be enabled on the same channel.

9.5 Region Entrance Detection

Purpose

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

1. Go to **Menu > Cameras Setup > 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 **Set** 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 region entrance detection sensitivity.
   - **Sensitivity:** Range [0-100]. The higher the value, the more easily the detection alarm is triggered.
8. Click and draw a quadrilateral in the preview window by specifying the four vertexes of the detection region, and right click to complete drawing. Only one region can be configured. Use to clear the existing virtual line and re-draw it.

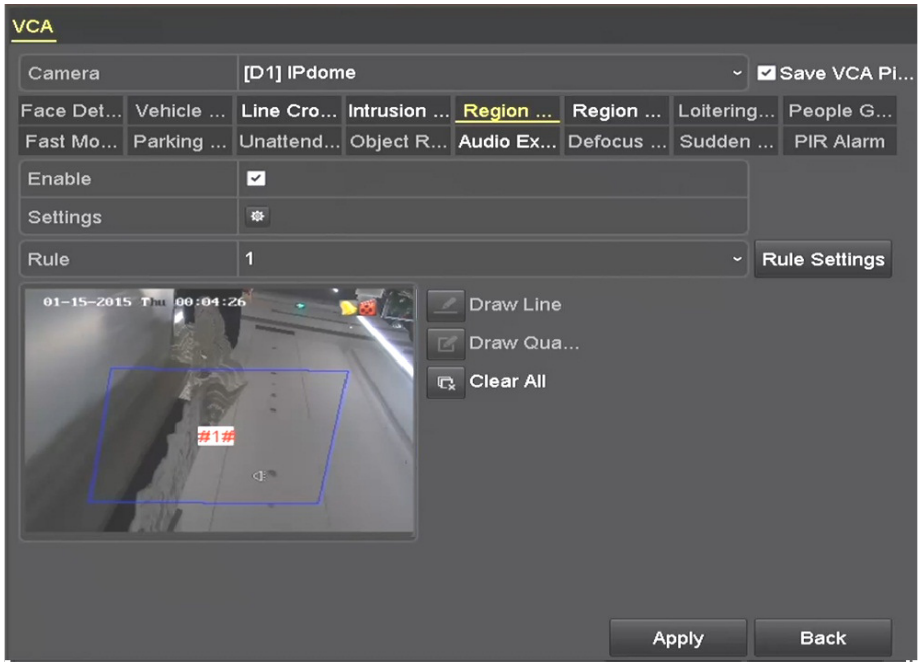


Figure 9-10 Set Region Entrance Detection

NOTE

Up to four rules can be configured.

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

9.6 Region Exiting Detection

Purpose

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

NOTE

Refer to *9.5 Region Entrance Detection* for steps to configure region exiting detection.

Up to four rules can be configured.

9.7 Loitering Detection

Purpose

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

NOTE

See *9.4 Intrusion Detection* for configuring loitering detection.

Threshold [1s-10s] in the Rule Settings defines the time the object loiters in the region. If the value is 5, an alarm is triggered after the object loiters in the region for 5s. If the value is 0, an alarm is triggered immediately when the object enters the region.

Up to four rules can be configured.

9.8 People Gathering Detection

Purpose

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

NOTE

See *9.4 Intrusion Detection* for operating steps to configure the people gathering detection.

The **Percentage** in the Rule Settings defines the gathering density of the people in the region. When the percentage is small, the alarm is triggered when a small number of people gather in the defined detection region.

Up to four rules can be configured.

9.9 Fast Moving Detection

Purpose

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

NOTE

Refer to *9.4 Intrusion Detection* for steps to configure fast moving detection.

Sensitivity in the 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.

9.10 Parking Detection

Purpose

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

NOTE

Refer to *9.4 Intrusion Detection* for steps to configure parking detection.

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

Up to four rules can be configured.

9.11 Unattended Baggage Detection

Purpose

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

NOTE

Refer to *9.4 Intrusion Detection* for steps to configure unattended baggage detection.

Threshold [5s-20s] in the Rule Settings defines the time of the objects can be left in the region. If the value is 10, an alarm is triggered after the object is left in the region for 10s.

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

Up to four rules can be configured.

9.12 Object Removal Detection

Purpose

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

NOTE

Refer to *9.4 Intrusion Detection* for steps to configure object removal detection.

Threshold [5s-20s] in the Rule Settings defines the time the objects have been removed from the region. If value is 10, an alarm is triggered if the object disappears from the region for 10s. **Sensitivity** defines the similarity of the background image to the object. When the sensitivity is high, a very small object taken from the region will trigger the alarm.

Up to four rules can be configured.

9.13 Audio Exception Detection

Purpose

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

NOTE

The audio exception detection is supported by all analog channels.

1. Go to **Menu > Cameras Setup > VCA**.
2. Select the camera 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 **Set** 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.

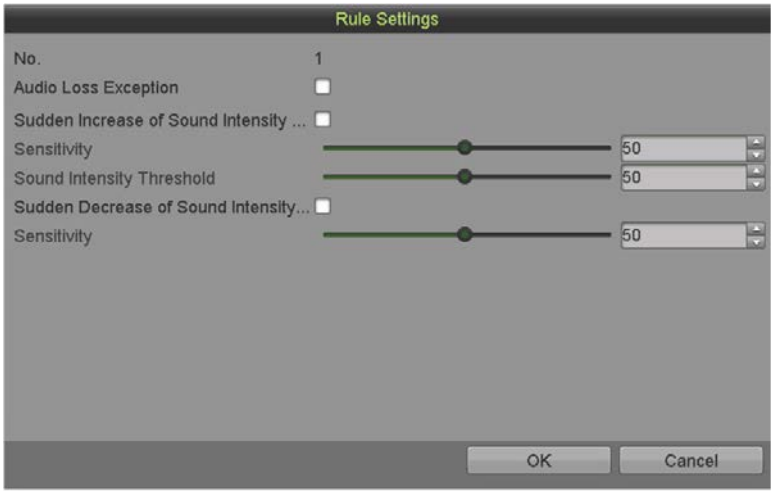


Figure 9-11 Set Audio Exception Detection Rules

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

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

   Sound Intensity Threshold: Range [1-100]. Filters the environment sounds. The louder the environment sound, the higher the value should be. Adjust it according to the real environment.
3) Check the **Sudden Decrease of Sound Intensity Detection** checkbox to detect a steep drop in the surveillance scene sound. Set the detection sensitivity [1-100].

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

9.14 Defocus Detection

Purpose

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

NOTE

Refer to *9.1 Face Detection* for operating steps to configure the defocus detection.

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

9.15 Sudden Scene Change

Purpose

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

NOTE

Refer to *9.1 Face Detection* for steps to configure scene change detection.

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

For analog cameras, 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. If you have enabled line crossing detection or intrusion detection, when you enable sudden scene change detection and apply the settings, the following attention box pops up to remind you there are not enough resources and asks you to disable the enabled VCA type(s) of the selected channel(s).

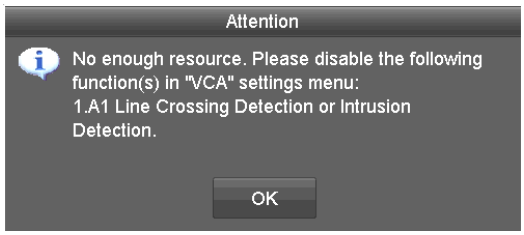


Figure 9-12 Disable Other VCA Type(s)

9.16 PIR Alarm

Purpose

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

1. Go to **Menu > Cameras Setup > 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 **Set** to configure the trigger channel, arming schedule, linkage action, and PTZ linking for the PIR alarm.
6. Click **Rule Settings** to set the rules. Refer to *9.1 Face Detection* for instructions.
7. Click **Apply** to activate the settings.

Chapter 10 VCA Search

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

10.1 Face Search

Purpose

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

Before You Start

Refer to *9.1 Face Detection* for configuring face detection.

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

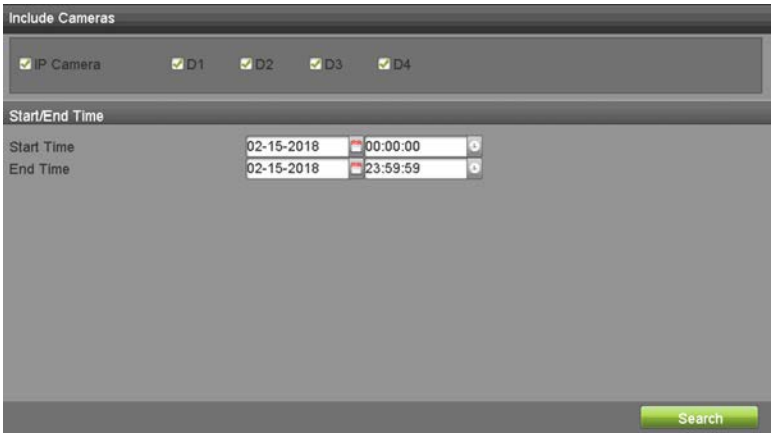


Figure 10-1 Face Search

3. Specify the start time and end time for 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 are displayed in a list or chart.

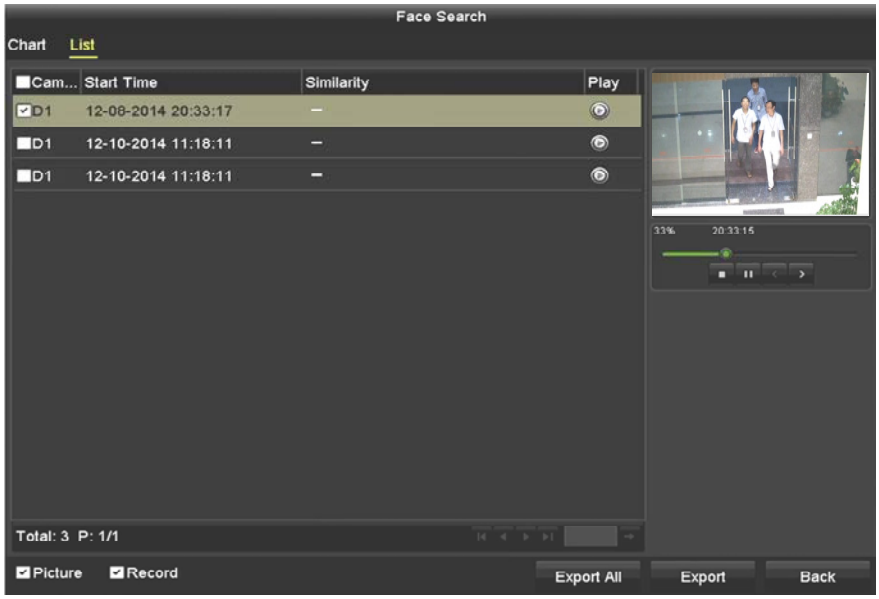


Figure 10-2 Face Search Interface

7. Play the face picture related video file.

   - You can double click on a face picture to play its related video file in the view window on the top right, or select a picture item and click to play it.
   - You can click to stop the 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 to the device and click **Export All** to enter the Export interface.

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

NOTE

Refer to *Chapter 7 Backup* for the steps to export files.

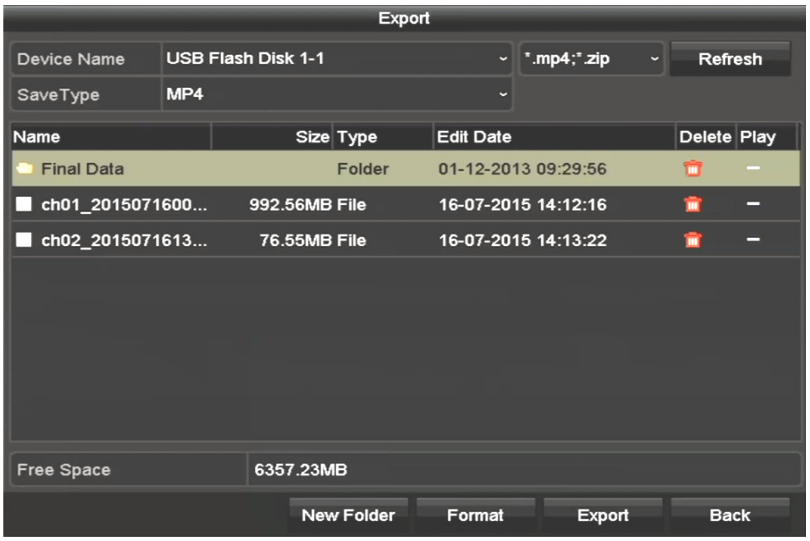


Figure 10-3 Export Files

10.2 Behavior Search

Purpose

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

1. Go to **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.

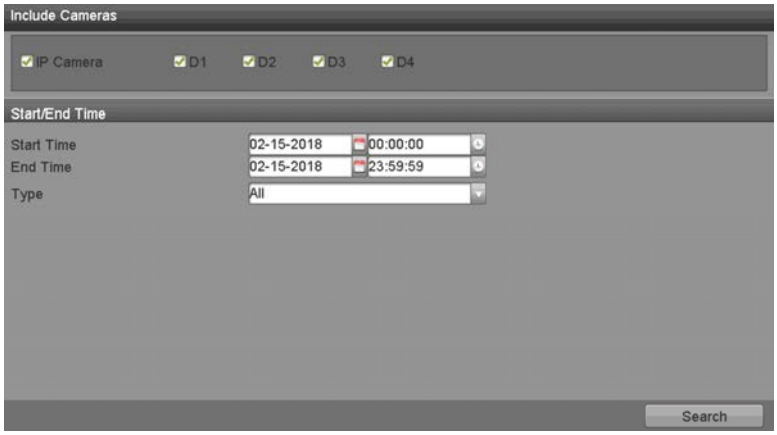


Figure 10-4 Behavior Search Interface

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 results are displayed in a list or chart.

Figure 10-5 Behavior Search Results

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

10.3 Plate Search

Purpose

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

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

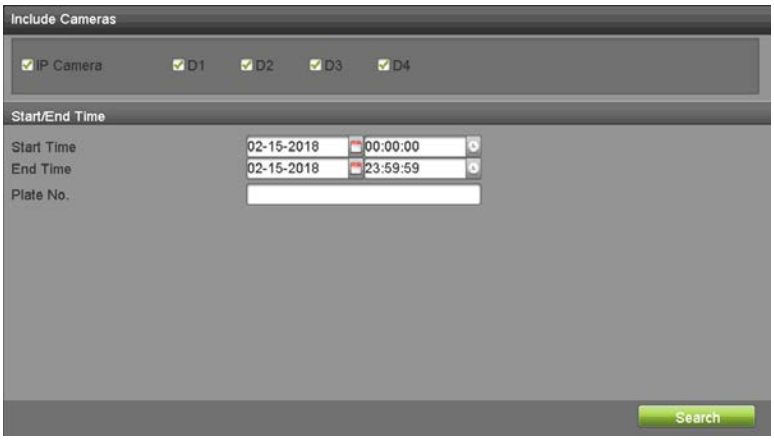


Figure 10-6 Plate Search

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

NOTE

Refer to *10.1 Face Search* for operation of the search results.

10.4 People Counting

Purpose

People Counting calculates the number of people entering or leaving a configured area and creates daily/weekly/monthly/annual reports for analysis.

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

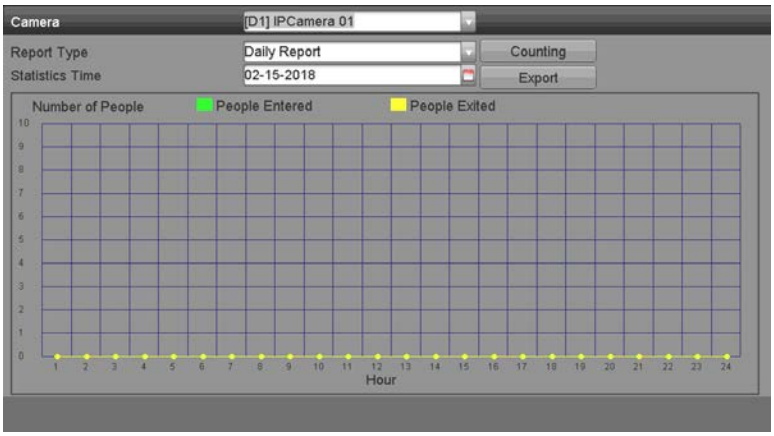


Figure 10-7 People Counting Interface

6. Click **Export** to export the statistics report in Microsoft Excel format.

10.5 Heat Map

Purpose

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

1. Go to **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.

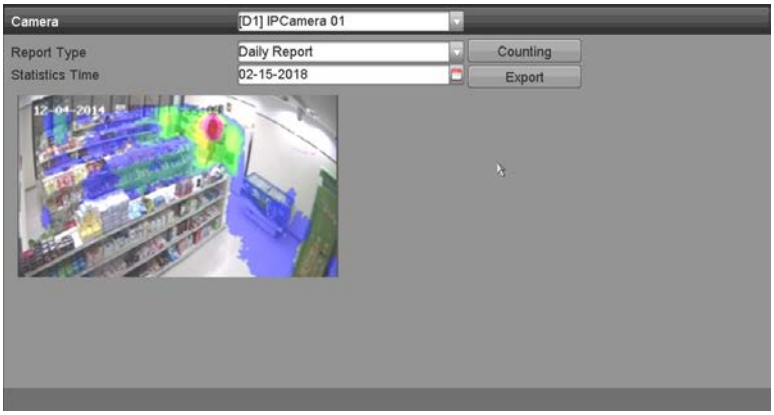


Figure 10-8 Heat Map Interface

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

NOTE

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

6. Click **Export** to export the statistics report in Microsoft Excel format.

Chapter 11 Network Settings

11.1 Configuring General Settings

Purpose

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

1. Go to **Menu > System Configuration > Network > General**.

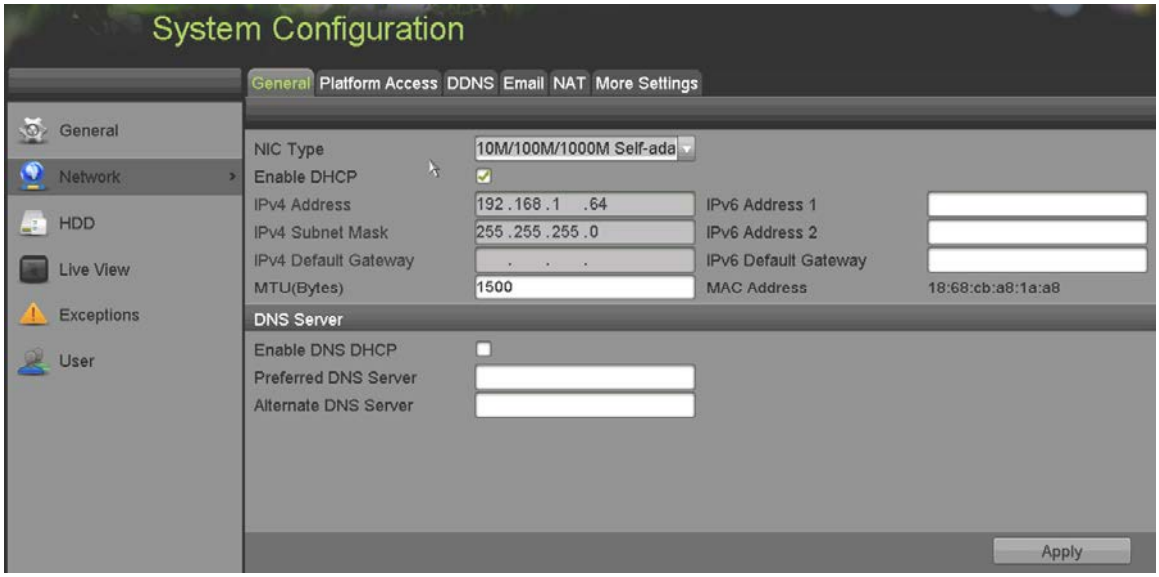


Figure 11-1 Network Settings Interface

2. On the **General Settings** interface, you can 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 the DHCP server is available, you can check the **Enable DHCP** checkbox to automatically obtain an IP address and other network settings from that server.

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**.

3. After configuring the general settings, click **Apply** to save the settings.

11.2 Configuring Advanced Settings

11.2.1 Configuring Hik-Connect

Purpose

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

NOTE

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

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

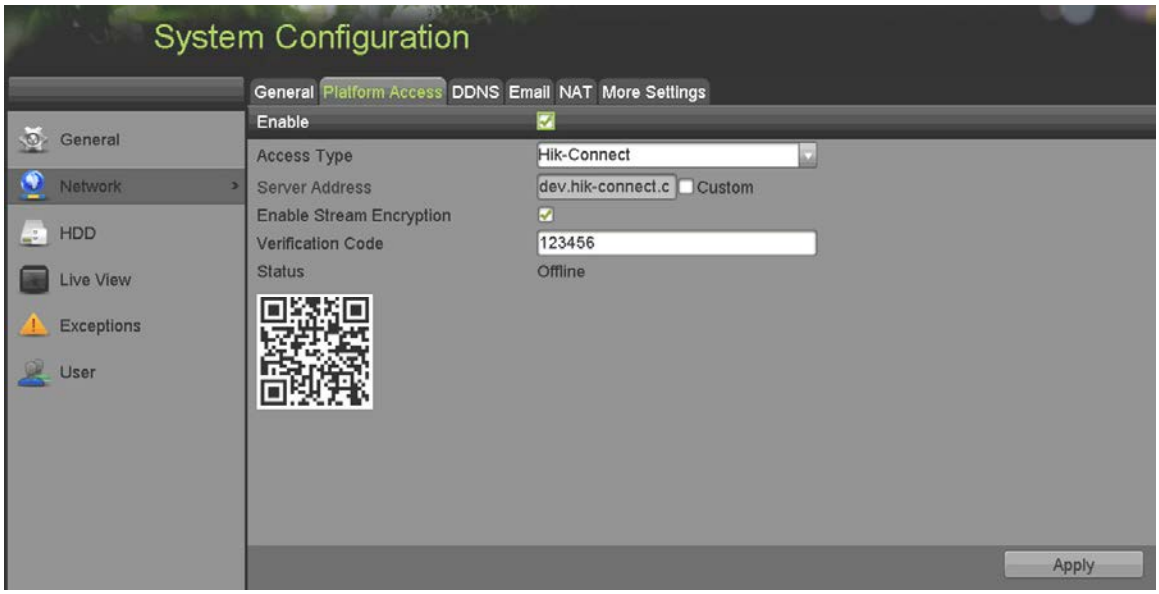


Figure 11-2 Hik-Connect Settings

2. Check the **Enable** checkbox to activate the function and display the following **Service Terms**.

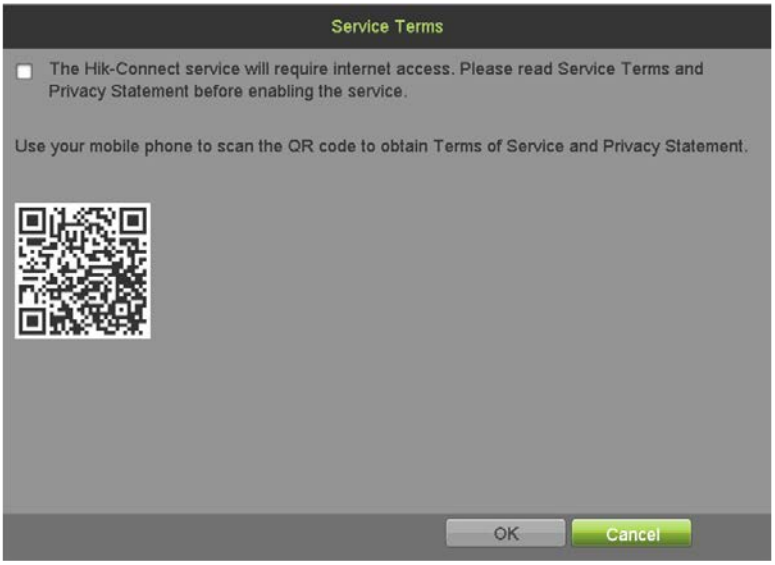


Figure 11-3 Service Terms

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

NOTE

Hik-Connect is disabled by default.

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

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

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

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

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

NOTE

Use your phone's scanning tool to scan the QR code below to get the device code.

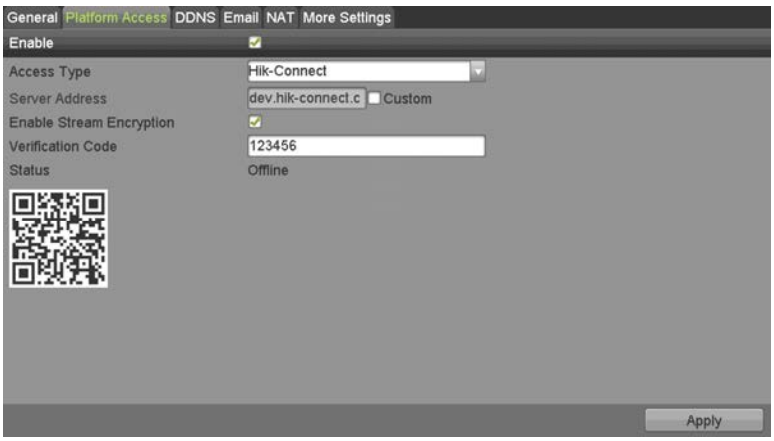


Figure 11-4 Hik-Connect Settings Interface

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

6. After configuration, you can access and manage the DVR with your mobile phone or the Web site (*www.hik-connect.com*).

   - **iOS Users:** Scan the QR code below to download the Hik-Connect app for subsequent operations.

Figure 11-5 QR Code for iOS Users

   - **Android Users**: Scan the QR code below to download the Hik-Connect app for subsequent operations.

NOTE

You must install *googleplay* on your Android mobile phone to skip to the address successfully.

Figure 11-6 QR Code for Android Users

NOTE

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

11.2.2 Configuring DDNS

Purpose

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. Go to **Menu > System Configuration > Network > DDNS**.
2. Check the **Enable DDNS** checkbox to enable this feature.
3. Select **DDNS Type**. Three different DDNS types are selectable: DynDNS, PeanutHull, and NO-IP.
   - **DynDNS**
     1) Enter **Server Address** for DynDNS (i.e., members.dyndns.org).
     2) In the **Device Domain Name** text field, enter the domain obtained from the DynDNS Web site.
     3) Enter the **User Name** and **Password** registered in the DynDNS Web site.

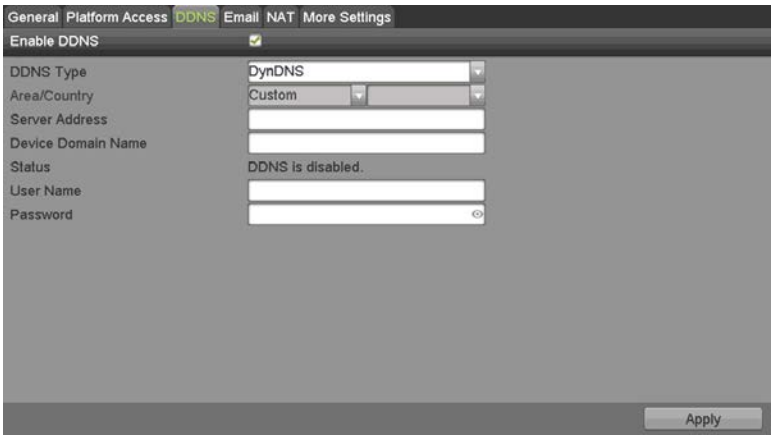


Figure 11-7 DynDNS Settings Interface

- **PeanutHull**

  1) Enter the **User Name** and **Password** obtained from the PeanutHull Web site.

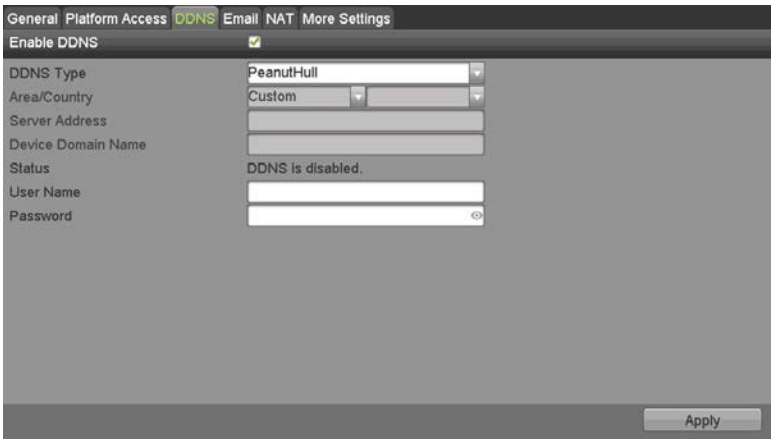


Figure 11-8 PeanutHull Settings Interface

- **NO-IP**

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

  1) Enter **Server Address** for NO-IP.
  2) In the **Device Domain Name** text field, enter the domain obtained from the NO-IP Web site (www.no-ip.com).
  3) Enter the **User Name** and **Password** registered in the NO-IP Web site.

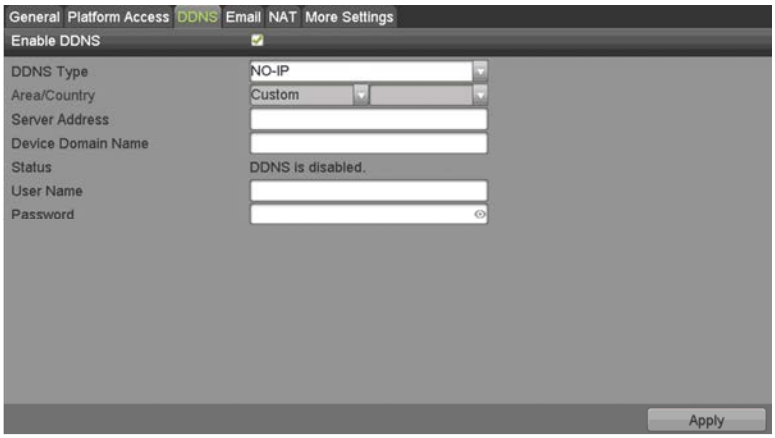


Figure 11-9 NO-IP Settings Interface

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

11.2.3 Configuring NTP Server

Purpose

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

1. Go to **Menu > System Configuration > General > Time/Date**.

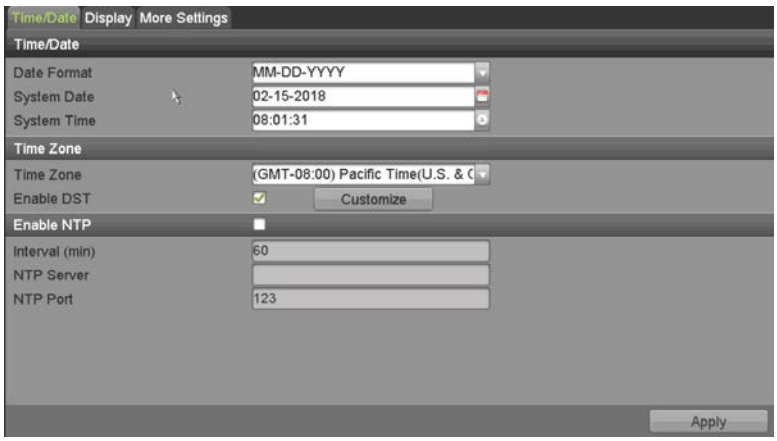


Figure 11-10 NTP Settings Interface

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

NOTE

The time synchronization interval can be set from 1 to 10,080 minutes, and the default value is 60 minutes. If the DVR is connected to a public network, use an NTP server that has a time synchronization function such as the server at the National Time Center (IP address: 210.72.145.44). If the DVR is set in a more customized network, NTP software can be used to establish an NTP server used for time synchronization.

11.2.4 Configuring NAT

Purpose

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

Before You Start

To enable the device's UPnP™ function, you must enable the UPnP™ function of the router the device is connected to. When the network working mode of the device is set as multi-address, the default route of the device should be in the same network segment as that of the router's LAN IP address.

1. Go to **Menu > System Configuration > Network > NAT**.

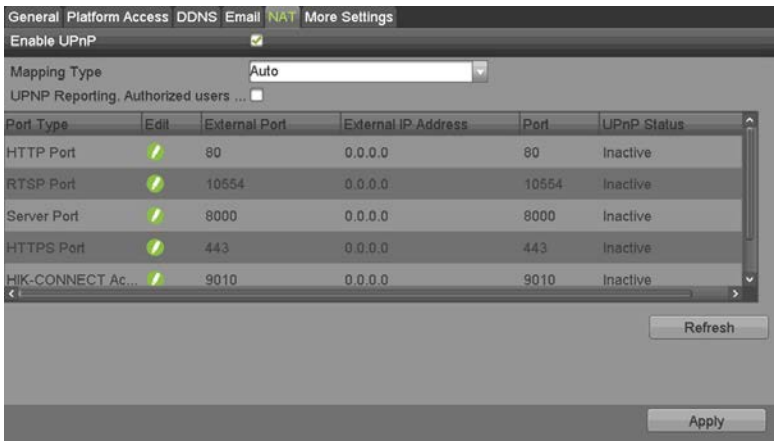


Figure 11-11 UPnP™ Settings Interface

2. Check **Enable UPnP** checkbox to enable UPnP™.

3. Set the **Mapping Type** as Manual or Auto in the drop-down list.

   OPTION 1: Auto

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

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

   2) Click **Refresh** to get the latest status of the port mapping.

   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 port mapping in the router.

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

Figure 11-12 External Port Settings Dialog Box

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

3) Click **Refresh** to get the latest status of the port mapping.

11.2.5 Configuring More Settings

1. Go to **Menu > System Configuration > Network > More Settings**.

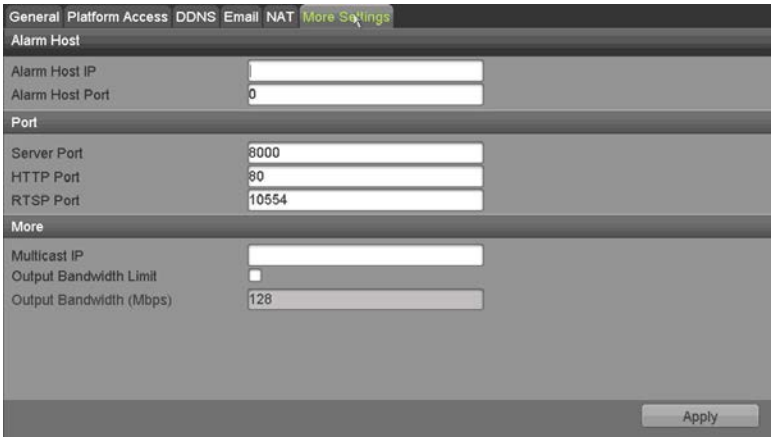


Figure 11-13 More Settings Interface

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

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

NOTE

Set the Server Port in the range of 2000-65535. 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, input the output bandwidth in the text field.

NOTE

The output bandwidth limit is used for remote live view and playback.

The default output bandwidth is the maximum limit.

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

11.2.6 Configuring HTTPS Port

Purpose

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

Example

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

NOTE

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

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

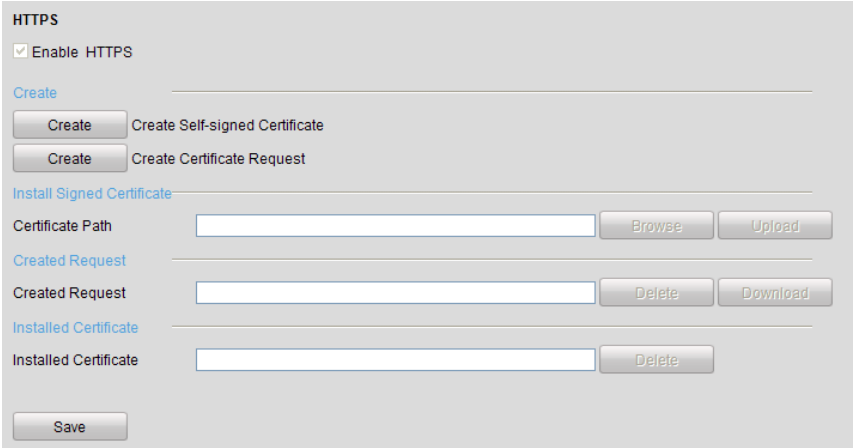


Figure 11-14 HTTPS Settings

OPTION 1: Create the self-signed certificate

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

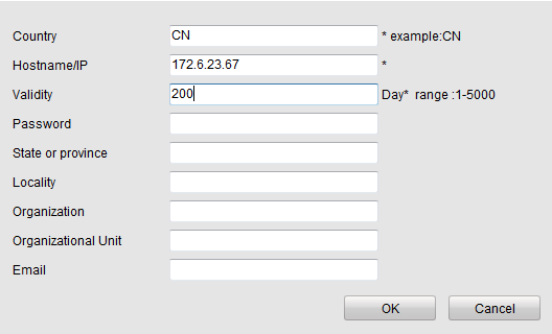


Figure 11-15 Create Self-Signed Certificate

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

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

OPTION 2: Create the authorized certificate

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

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

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

6. The certificate information will appear after you successfully create and install the certificate.

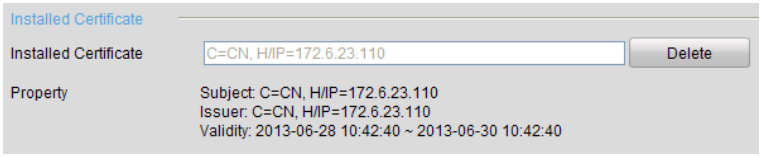


Figure 11-16 Installed Certificate Property

7. Check the checkbox to enable the HTTPS function.

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

11.2.7 Configuring E-Mail

Purpose

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

Before You Start

Make sure you configured the IPv4 Address, IPv4 Subnet Mask, IPv4 Gateway, and the Preferred DNS Server in the Network Settings menu. Refer to *11.1 Configuring General Settings* for detailed information.

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

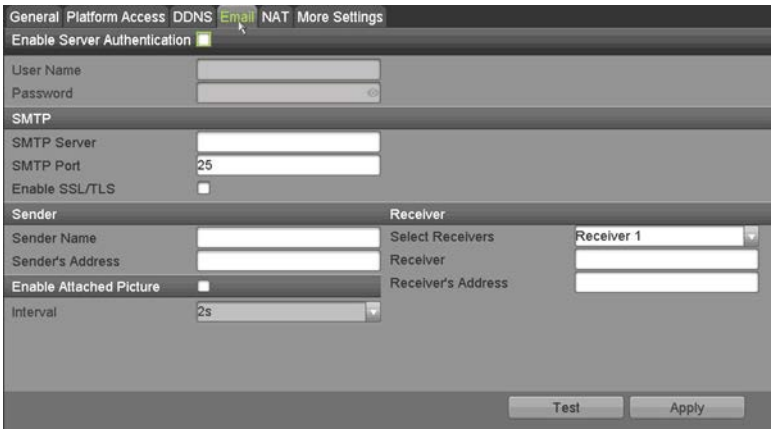


Figure 11-17 Email Settings Interface

3. Configure the following e-mail settings:
   - **Enable Server Authentication (optional):** Check the checkbox to enable the server authentication feature.
   - **User Name**: The user account of sender's e-mail 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 the sender
   - **Sender's Address:** The e-mail address of the 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, alarm images are sent directly as attached pictures by e-mail. Up to one picture can be sent for one IP camera. The attached pictures of linked cameras cannot be sent.

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

- **Interval:** The interval refers to the time between two actions of sending attached pictures.
- **E-mail Test:** Sends a test message to verify that the SMTP server can be reached.

4. Click **Apply** to save the e-mail settings.
5. Click **Test** to test your e-mail settings. The corresponding Attention message box pops up.

Figure 11-18 Email Testing Attention

11.2.8 Checking Network Traffic

Purpose

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

1. Go to **Menu > Maintenance > Network Detect > Traffic**.

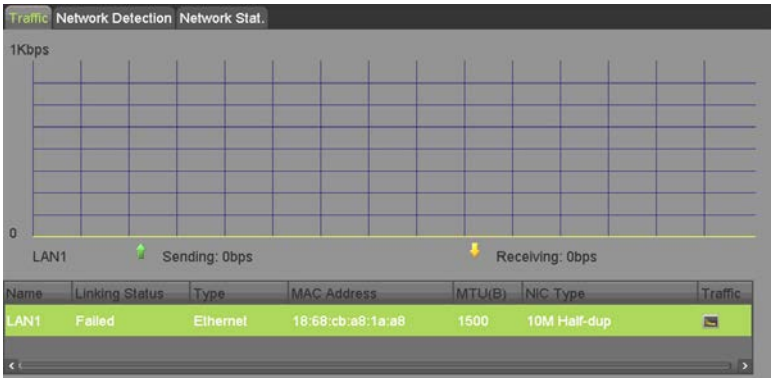


Figure 11-19 Network Traffic Interface

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

11.3 Configuring Network Detection

Purpose

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

11.3.1 Testing Network Delay and Packet Loss

1. Go to **Menu > Maintenance > Network Detect > Network Detection**.

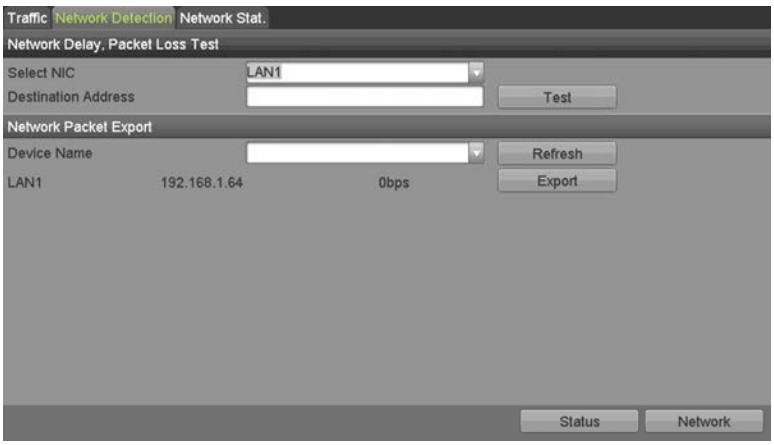


Figure 11-20 Network Detection Interface

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

11.3.2 Exporting Network Packet

Purpose

By connecting the DVR to a network, the captured network data packet can be exported to a USB flash disk, SATA, or other local backup device.

1. Go to **Menu > Maintenance > Network Detect > Network Detection**.
2. Select the backup device from the **Device Name** drop-down list.

NOTE

Click **Refresh** if the connected local backup device cannot be displayed. If it fails to detect the backup device, check if it is compatible with the DVR. Format the backup device if the format is incorrect.

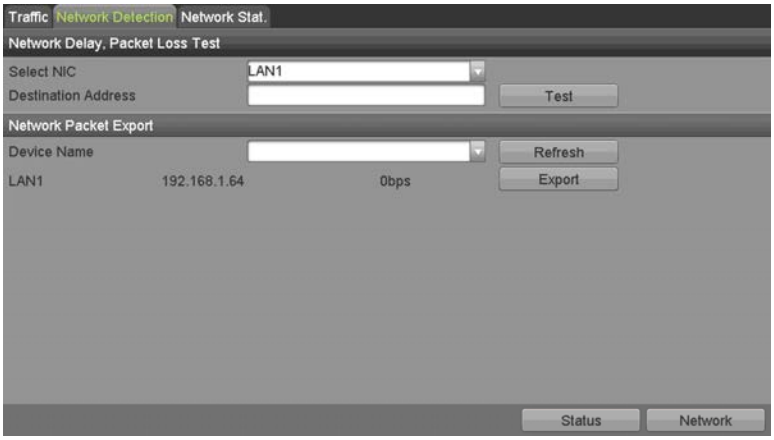


Figure 11-21 Export Network Packet

1. Click **Export** to start exporting.

2. After exporting is complete, click **OK** to finish the packet export.

Figure 11-22 Packet Export Attention

NOTE

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

11.3.3 Checking Network Status

Purpose

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

1. Go to **Menu > Maintenance > Network Detect > Network Detection**.
2. Click **Status** on the right bottom of the interface.

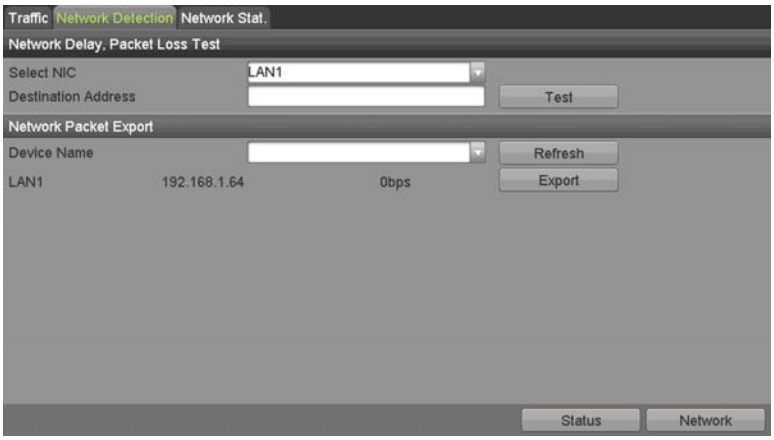


Figure 11-23 Checking Network Status

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

Figure 11-24 Network Status Checking Result

4. If the message box appears with other information, click **Network** to show the network parameters quick setting interface.

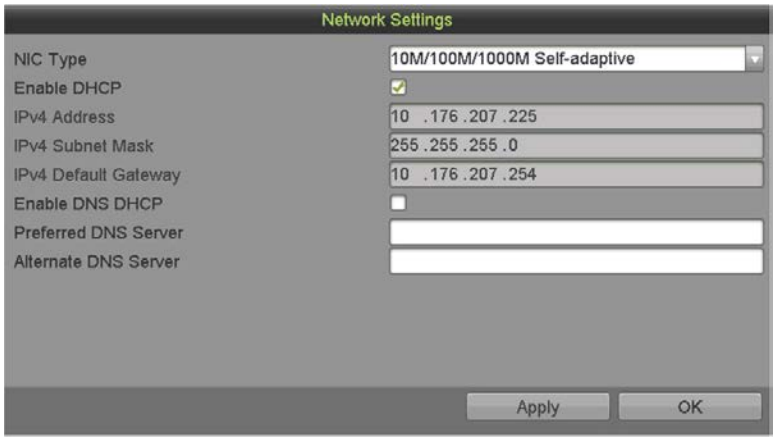


Figure 11-25 Network Parameters Configuration

11.3.4 Checking Network Statistics

Purpose

You can check the network statistics to obtain the real-time information of the device.

1. Go to **Menu > Maintenance> Network Detect > Network Stat**.

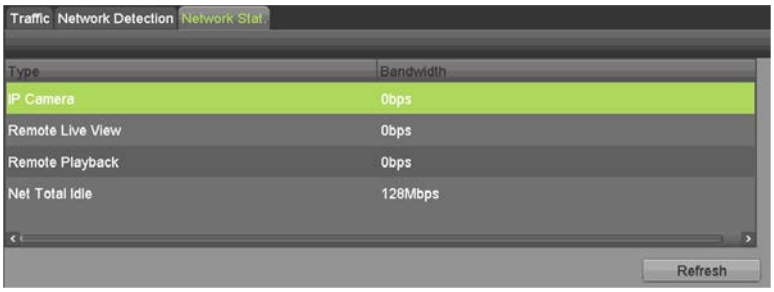


Figure 11-26 Network Stat. Interface

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

Chapter 12 HDD Management

12.1 Initializing HDDs

Purpose

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

1. Go to **Menu > System Configuration > HDD > HDD Information**.

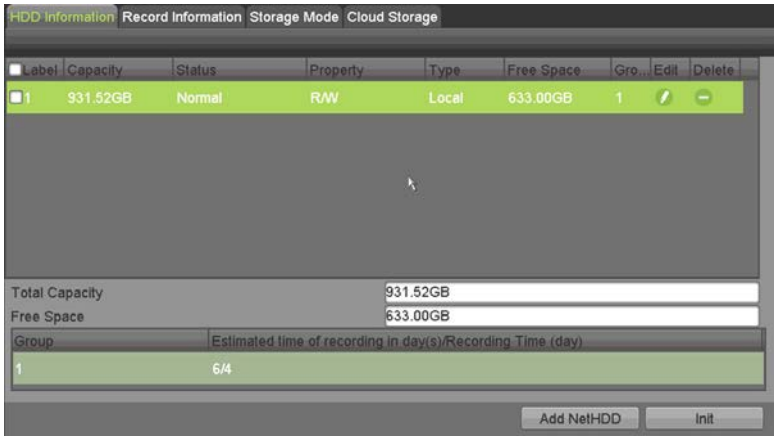


Figure 12-1 HDD Information Interface

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 12-2 Confirm Initialization

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

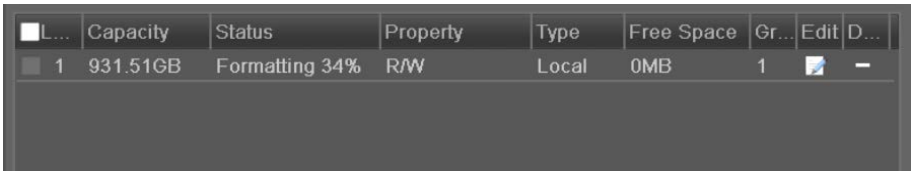


Figure 12-3 Start Initialization

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

NOTE

Initializing the HDD will erase all data on it.

HDDs that are idle for a long period of time can be put to sleep to decrease the power consumption and extend the life of the HDDs.

1. Go to **Menu > System Configuration > HDD > Record Information**.

Figure 12-4 Enable HDD Sleeping

2. Check the **Enable HDD Sleeping** checkbox (by default), and the HDDs that are idle for a long period of time will be set to sleep.

3. (Optional) Uncheck the **Enable HDD Sleeping** checkbox, and the HDDs will be set to work at all times.

12.2 Managing Network HDD

Purpose

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

1. Go to **Menu > System Configuration > HDD > HDD Information**.

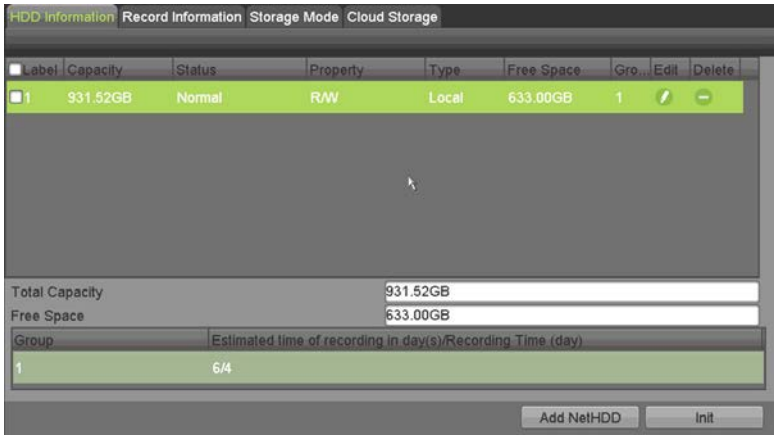


Figure 12-5 HDD Information Interface

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

Figure 12-6 Add NetHDD

3. Add the allocated NetHDD.
4. Set the type to **NAS** or **IP SAN**.
5. Configure the NAS or IP SAN settings.

- **Add a NAS Disk**

  1) Enter the NetHDD IP address in the text field.
  2) Click **Search** to search for available NAS disks.
  3) Select the NAS disk from the list shown below, or manually enter the directory in the **NetHDD Directory** text field.

4) Click **OK** to add the configured NAS disk.

NOTE

Up to eight NAS disks can be added.

- **Add an IP SAN**

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

NOTE

Up to eight IP SAN disks can be added.

5) After successfully adding 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.

12.3 Managing HDD Group

12.3.1 Setting HDD Groups

Purpose

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

1. Go to **Menu > System Configuration > HDD > Storage Mode**.
2. Set the **Mode** to Group, as shown below.

Figure 12-7 Storage Mode Interface

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

Figure 12-8 Attention for Reboot

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

Figure 12-9 Local HDD Settings Interface

7. Select the Group number for the current HDD.

NOTE

The default group no. for each HDD is 1.

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

Figure 12-10 Confirm HDD Group Settings

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

12.3.2 Setting HDD Property

Purpose

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

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

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

1. Go to **Menu > System Configuration > HDD > HDD Information**.

2. Highlight an HDD on the list and click the icon to enter the **Local HDD Settings** interface.

Figure 12-11 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.

NOTE

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

12.4 Configuring Quota Mode

Purpose

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

1. Go to **Menu > System Configuration > HDD > Storage Mode**.
2. Set the **Mode** to Quota, as shown below.

NOTE

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

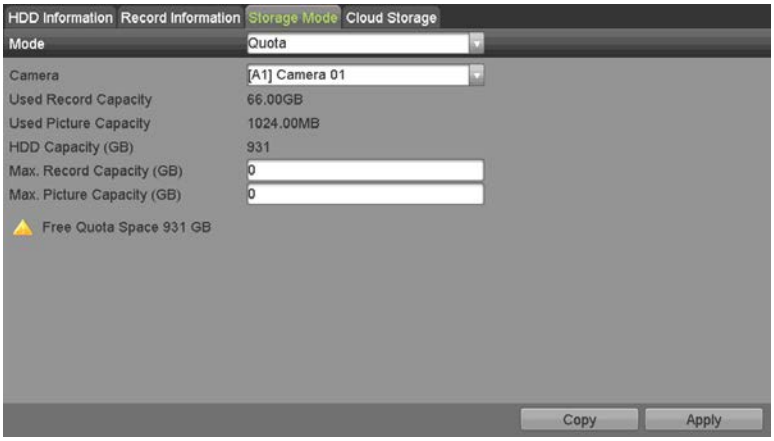


Figure 12-12 Storage Mode Settings Interface

3. Select a camera for which to configure quota.

4. Enter the storage capacity in the **Max. Record Capacity (GB)** text field.

5. Copy the quota settings of the current camera to other cameras if required. Click **Copy** to enter the **Copy Camera** interface, as shown below.

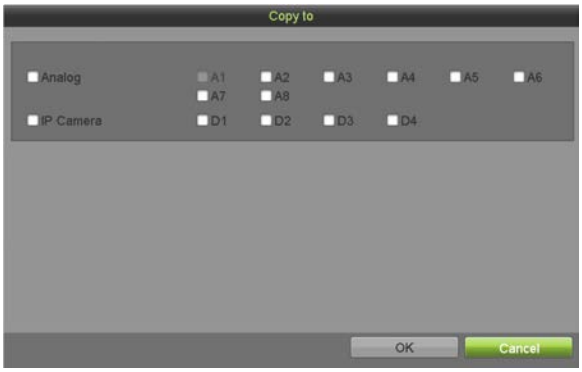


Figure 12-13 Copy Settings to Other Camera(s)

6. Select the camera(s) to be configured with the same quota settings. You can also click the Analog checkbox to select all cameras.

7. Click **OK** to finish the Copy settings and return to the Storage Mode interface.

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

NOTE

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

12.5 Configuring Cloud Storage

Purpose

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

1. Go to **Menu > System Configuration > HDD > Cloud Storage**.

2. Check the **Enable Cloud** checkbox to enable the feature.

3. Select **Cloud Type** from the drop-down list (e.g., One Drive, Google Drive, or Drop Box).

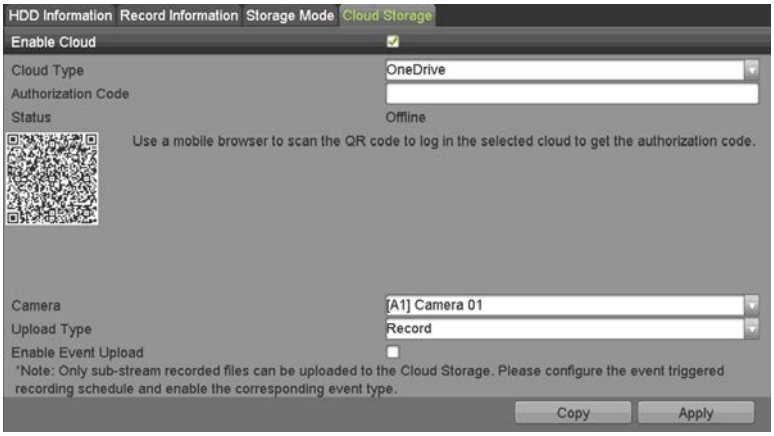


Figure 12-14 Cloud Storage Interface

4. Follow the prompts and use a mobile QR Code scanner app to scan the QR code to log in to the selected cloud to get the authentication code, then copy the authentication code to the **Authentication Code** text filed.

5. Click **Apply** to save the settings and return to the main menu.

6. Enter the cloud storage interface again in approximately 20 seconds. The **Status** should indicate successful registration.

7. Configure the recording schedule (see 5.2

Configuring Recording Schedule*)*.

8. Upload the event triggered recording files to the cloud storage.

   1) Go to **Menu > System Configuration > HDD > Cloud Storage**.
   2) Select the camera you set in the recording schedule interface.
   3) Select the upload type in the **Upload Type** text filed.
   4) Check the **Enable Event Upload** checkbox.
   5) Click **Apply** to finish the settings.

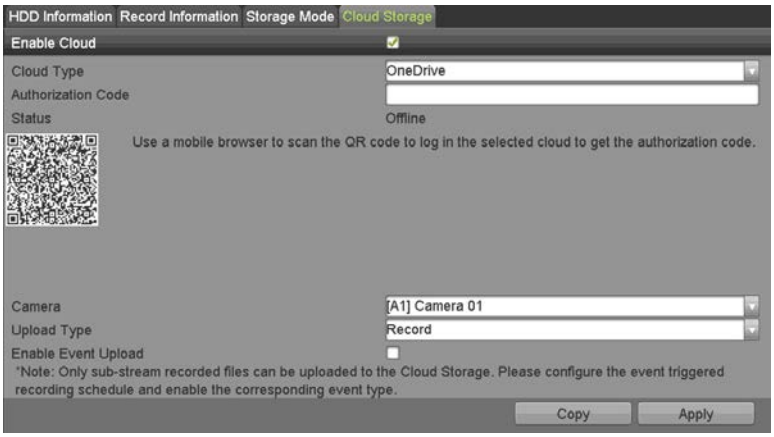


Figure 12-15 Upload to Cloud Storage Interface

NOTE

Only the sub-stream recorded files can be uploaded to the cloud storage.

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

9. (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 return to the cloud storage interface, and click **Apply** to finish the settings.

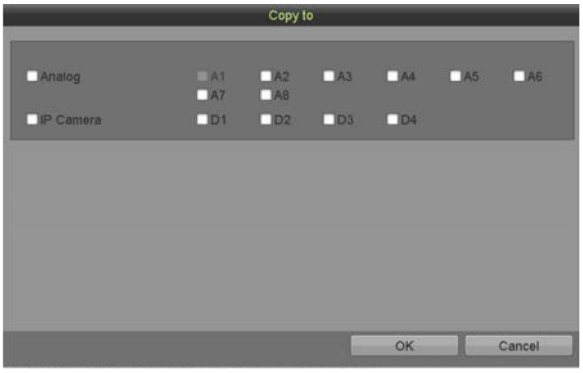


Figure 12-16 Copy to Interface

12.6 Checking HDD Status

Purpose

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

Checking HDD Status in HDD Information Interface

1. Go to **Menu > System Configuration > HDD > HDD Information**.

2. Check the status of each HDD displayed on the list, as shown below.

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 12-17 View HDD Status (1)

NOTE

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

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

Purpose

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

1. Go to **Menu > Maintenance > HDD Detect > S.M.A.R.T. Settings**.
2. Select the HDD to view its S.M.A.R.T. information list, as shown below.

NOTE

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

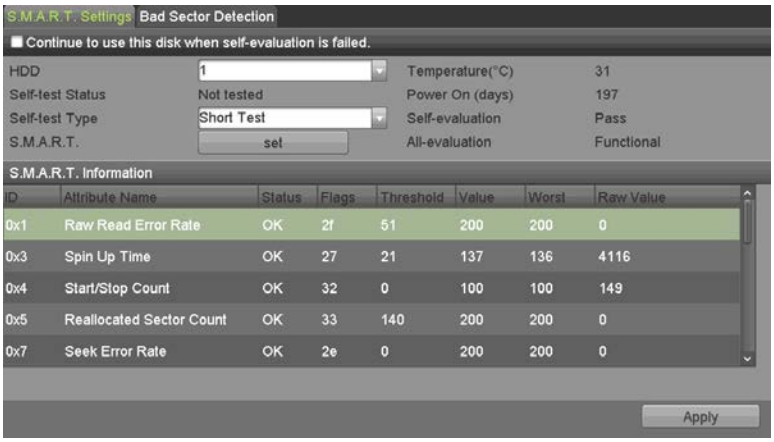


Figure 12-18 S.M.A.R.T. Settings Interface

12.8 Detecting Bad Sectors

Purpose

You can detect the bad HDD sectors to determine the HDD status.

1. Go to **Menu > Maintenance > HDD Detect > Bad Sector Detection**.
2. Select an HDD, and click **Detect** to start detecting.

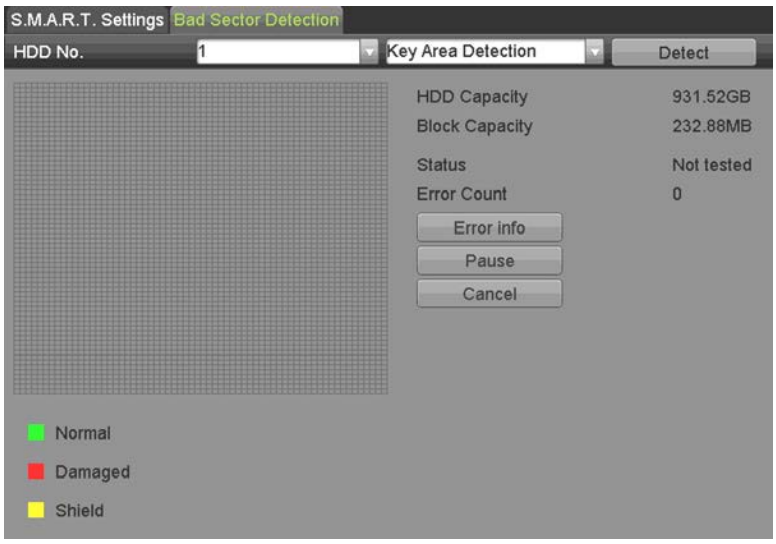


Figure 12-19 Bad Sector Detecting

3. Click **Pause** to pause the detection, and click **Resume** to resume the detection.
4. If there is error information about the HDD, click **Error Info** to view the information.

12.9 Configuring HDD Error Alarms

Purpose

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

1. Go to **Menu > System 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 errors. The linkage actions can be set to: Audible Warning, Notify Surveillance Center, Send Email, and Trigger Alarm Output.

Figure 12-20 Configure HDD Error Alarm

4. If **Trigger Alarm Output** is selected, you can trigger the alarm output from the list that appears.
5. Click **Apply** to save the settings.

Chapter 13 Camera Settings

13.1 Configuring OSD Settings

Purpose

You can configure the camera's OSD (On-Screen Display) settings (e.g., date/time, camera name, etc.)

1. Go to **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(es).
5. Select the Date Format, Time Format, Display Mode, and the OSD Font.

Figure 13-1 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.
   1) To copy the OSD settings of the current camera to other cameras, click **Copy** to enter the **Copy Camera** interface.
   2) Select the camera(s) to be configured with the same OSD settings. You can also check the **Analog** checkbox to select all cameras.
   3) Click **OK** to finish the **Copy** settings and go back to the **OSD Configuration** interface.
8. Click **Apply** to apply the settings.

13.2 Configuring Privacy Mask

Purpose

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

1. Go to **Menu > Cameras Setup > Privacy Mask**.
2. Select the camera for which to set the privacy mask.
3. Check the **Enable Privacy Mask** checkbox to enable this feature.

Figure 13-2 Privacy Mask Settings Interface

4. Use the mouse to draw a zone on the window. The zones will be marked in 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.

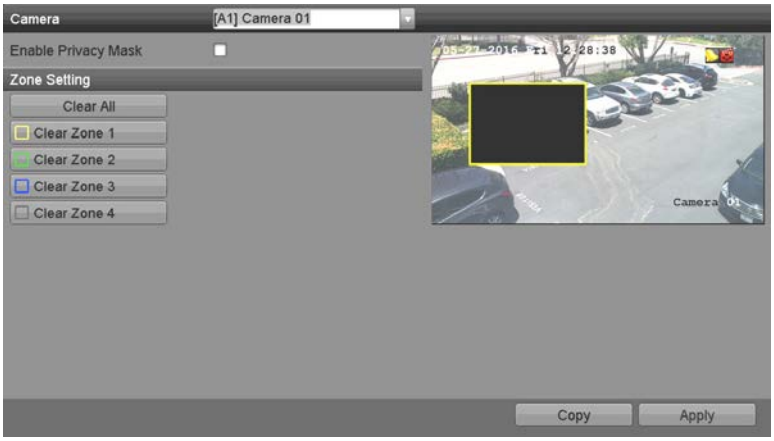


Figure 13-3 Set Privacy Mask Area

6. Click **Copy** to copy the privacy mask settings to other cameras.
7. Click **Apply** to save the settings.

13.3 Configuring Video Parameters

13.3.1 Configuring Image Settings

1. Go to **Menu > Cameras Setup > Image > Image Settings**.

Figure 13-4 Image Settings Interface (Choices Will Vary by Camera)

2. Select the camera for which to set the image parameters.
3. Two periods for different image settings are provided, select the period name in the drop-down list.

NOTE

The time periods cannot overlap.

4. Select the mode from the **Mode** drop-down list. There are four modes selectable for analog cameras: Standard, Indoor, Dim Light, and Outdoor.
5. Adjust the image parameters according to actual needs. The parameters include Brightness, Contrast, Saturation, Hue, Sharpness, and Denoising for the analog cameras and Brightness, Contrast, and Saturation for the IP cameras. Click **Restore** to set the parameters to the default settings.
6. Click **Copy** to copy the image settings of the current camera to other cameras.
7. Click **Apply** to save the settings.

13.3.2 Configuring Camera Parameters Settings

1. Go to **Menu > Cameras Setup > Image > Camera Parameters Settings**.

Figure 13-5 Camera Parameters Settings

2. Select the **Camera** from the drop-down list.
3. Configure the parameters.
   - Switch the 4 MP or 5 MP signal with the **Signal Switch** drop-down list. 4 MP 25/30 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.
   - Check **Enable Defog** to enable the selected camera's defog function. Set **Defog Level** from 1 to 4.
   - Adjust the parameters including Day to Night Sensitivity, Night to Day Sensitivity, and IR Light Brightness for the analog cameras.
   - Select the **Day/Night Mode** of the camera from the drop-down list.
   - Check the **WDR Switch** checkbox to enable the function.
4. (Optional) Click **Default** to set the parameters to the default settings.
5. (Optional) Click **Copy** to copy the parameters of the current camera to other analog cameras.
6. Click **Apply** to save the settings.

NOTE

The camera parameters settings is applicable only for analog cameras.

The 4 MP/5 MP Signal Switch, Defog, Day to Night Sensitivity, Night to Day Sensitivity, IR Light Brightness, Day/Night Mode, and WDR Switch 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 the last ones set.

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

Chapter 14 DVR Management and Maintenance

14.1 Viewing System Information

1. Go to **Menu > System Information**
2. Select the type of information you wish to view.
   - **Device Info**
   - **Camera**
   - **Record**
   - **Alarm**
   - **Network**
   - **HDD**

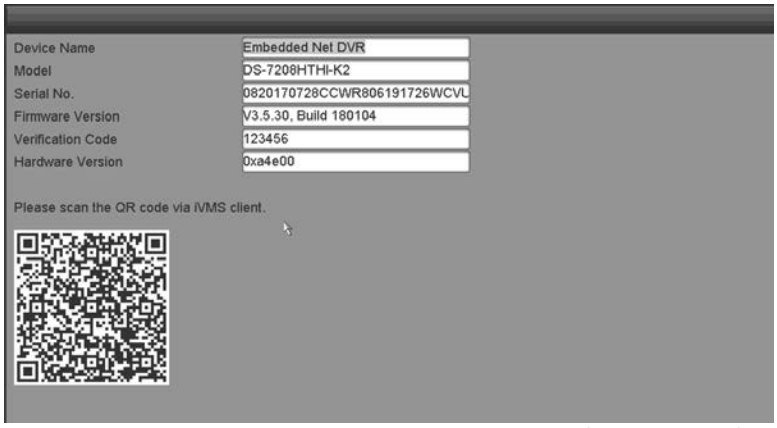


Figure 14-1 System Information Interface (Device Info)

14.2 Searching Log Files

Purpose

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

1. Go to **Menu > Maintenance > System Logs**.

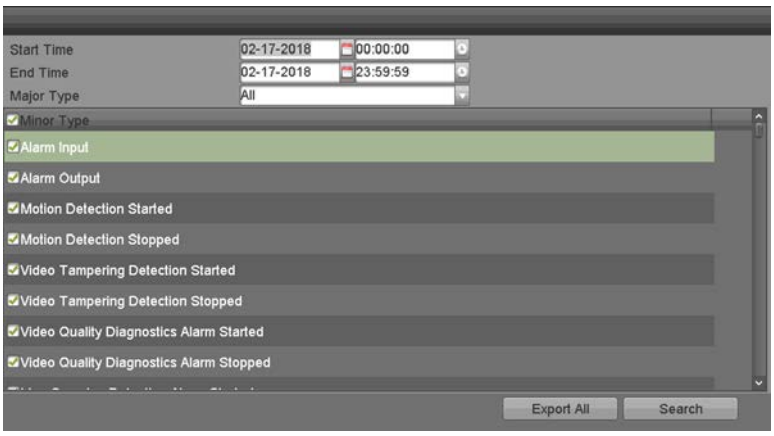


Figure 14-2 Log Search Interface

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

3. Click **Search** to start search log files.

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

NOTE

Up to 2000 log files can be displayed each time.

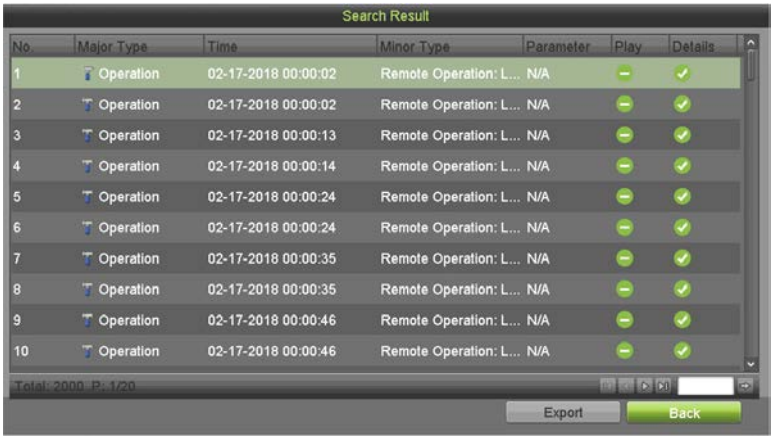


Figure 14-3 Log Search Results

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.

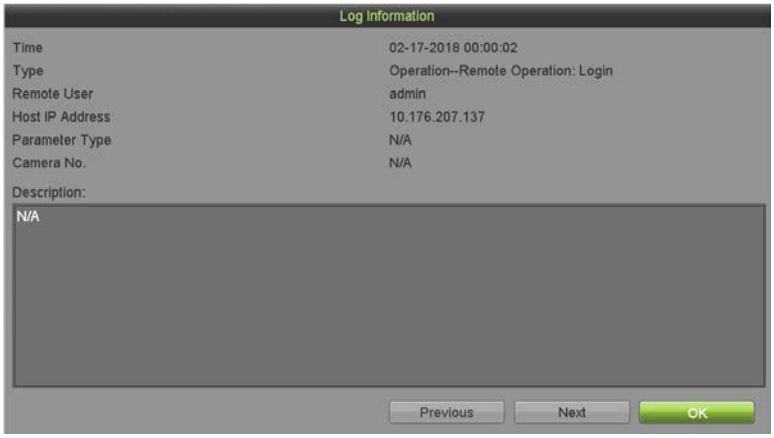


Figure 14-4 Log Information Interface

6. To export the log files, click **Export** to enter the Export menu, as shown below.

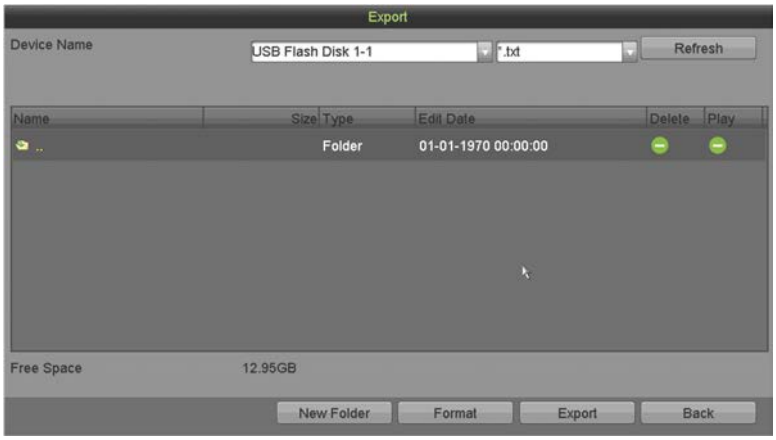


Figure 14-5 Export Log Files

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

NOTE

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

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

14.3 Importing/Exporting IP Camera Info

Purpose

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, password of admin, etc. The exported file can

be edited on your PC (e.g., adding or deleting content, copying the setting to other devices by importing the Excel file to it, etc.).

1. Go to **Menu > Cameras Setup > Cameras > IP Camera Import/Export**.
2. Click **Export** to export configuration files to the selected local backup device.
3. To import a configuration file, select the file from the selected backup device and click **Import**. After the importing process is completed, you must reboot the DVR.

14.4 Importing/Exporting Configuration Files

Purpose

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 DVRs if they are to be configured with the same parameters.

1. Go to **Menu > Maintenance > Import/Export**.

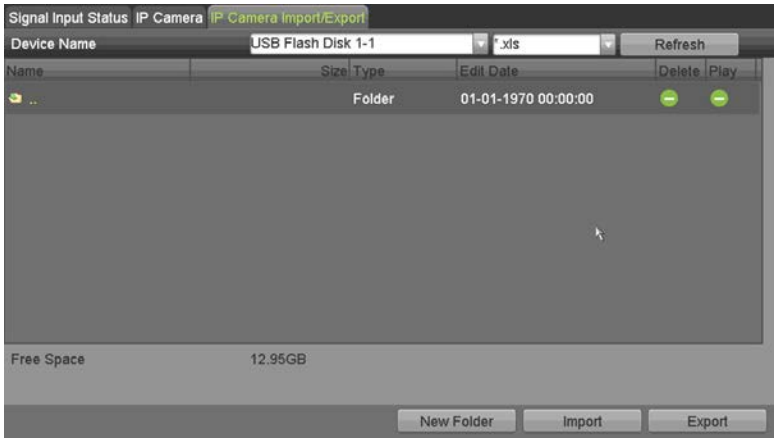


Figure 14-6 Import/Export Configuration File

2. Click **Export** to export configuration files to the selected local backup device.
3. To import a configuration file, select the file from the selected backup device, and click **Import**. After the import process is complete, the device will reboot automatically.

14.5 Upgrading System

Purpose

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

14.5.1 Upgrading by Local Backup Device

1. Connect your DVR to a local backup device that contains the update firmware file.
2. Go to **Menu > Maintenance > Upgrade > Local Upgrade**.

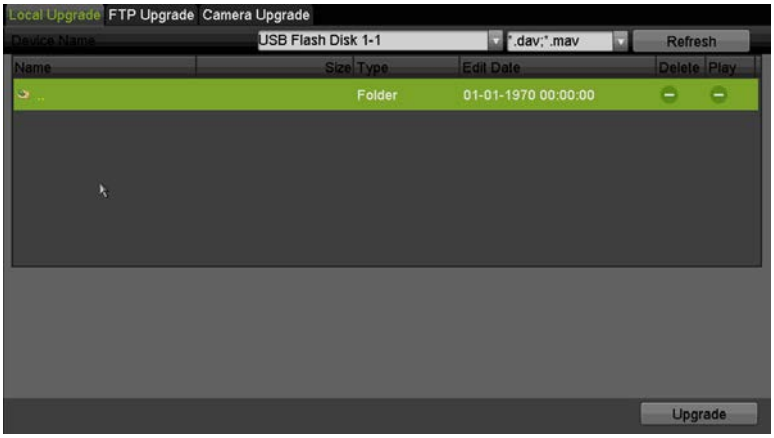


Figure 14-7 Local Upgrade Interface

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

14.5.2 Upgrading by FTP

Before You Start

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

1. Go to **Menu > Maintenance > Upgrade > FTP Upgrade**.

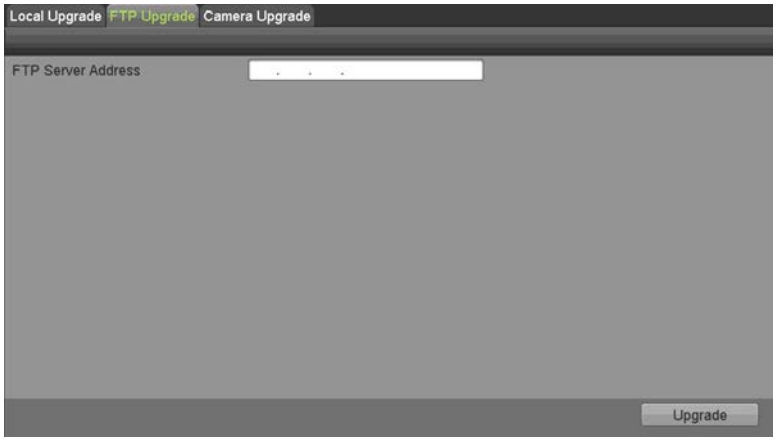


Figure 14-8 FTP Upgrade Interface

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

14.6 Upgrading Camera

Purpose

You can upgrade multiple connected analog cameras supporting TurboHD or AHD signal simultaneously with the DVR.

1. Go to **Menu > Maintenance > Upgrade > Camera Upgrade**.

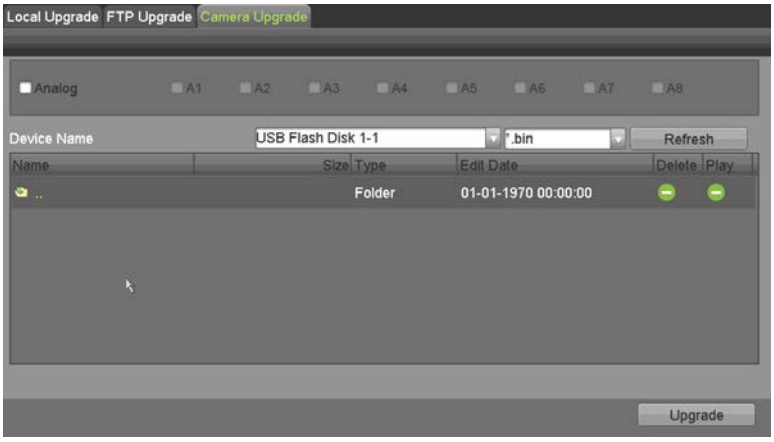


Figure 14-9 Camera Upgrade

2. Check the checkbox(es) of the analog camera(s) to upgrade.

NOTE

The analog camera(s) must support TurboHD or AHD signal.

3. Select the update file from the backup device.
4. Click **Upgrade** to start upgrading.

14.7 Restoring Default Settings

1. Go to **Menu > Maintenance > Default**.

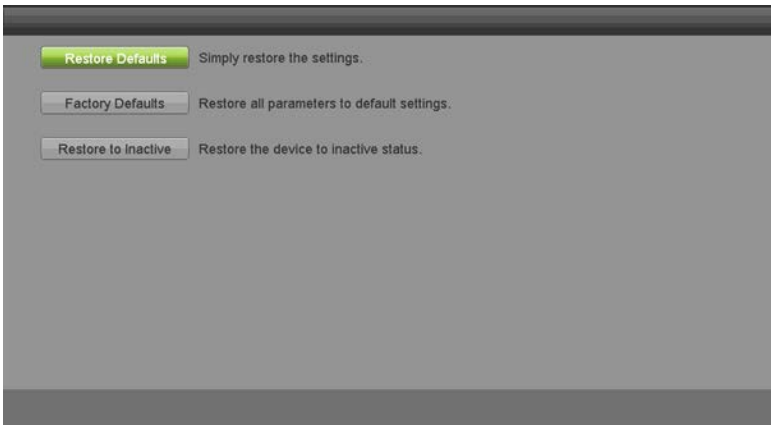


Figure 14-10 Restore Defaults

2. Select the restore 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.

The device will reboot automatically after restoring the default settings.

Chapter 15 Others

15.1 Configuring General Settings

Purpose

You can configure the output resolution, system time, mouse pointer speed, etc.

1. Go to **Menu > System Configuration > General > Display**.

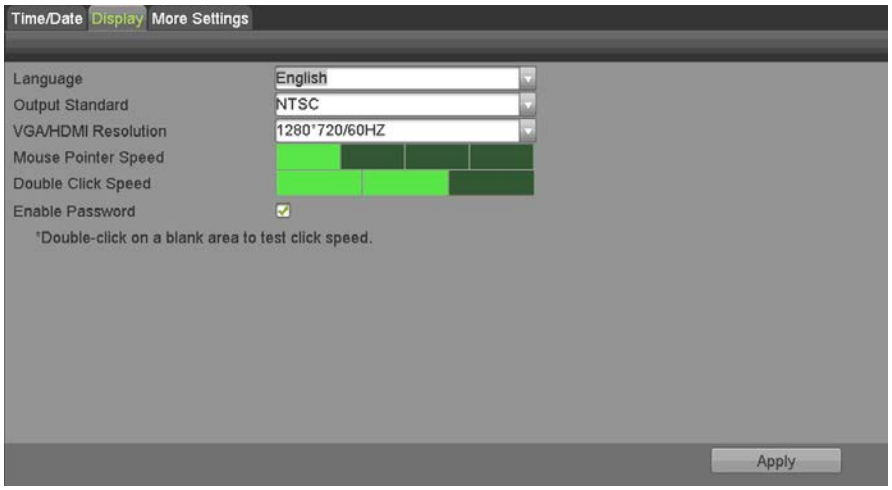


Figure 15-1 General Settings Interface (for Other Models))

2. 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 as 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 for double-clicks to register; 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.

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

15.2 Configuring DST Settings

1. Go to **Menu > System Configuration > General > Time/Date**.
2. Check the **Enable DST** checkbox.
3. Click **Customize**.

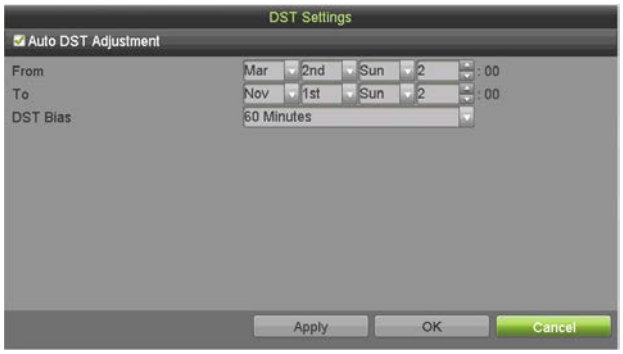


Figure 15-2 DST Settings Interface

4. Check the **Auto DST Adjustment** checkbox, or manually set the date of the DST period.

15.3 Configuring More Settings

1. Go to **Menu > System Configuration > General > More Settings**.

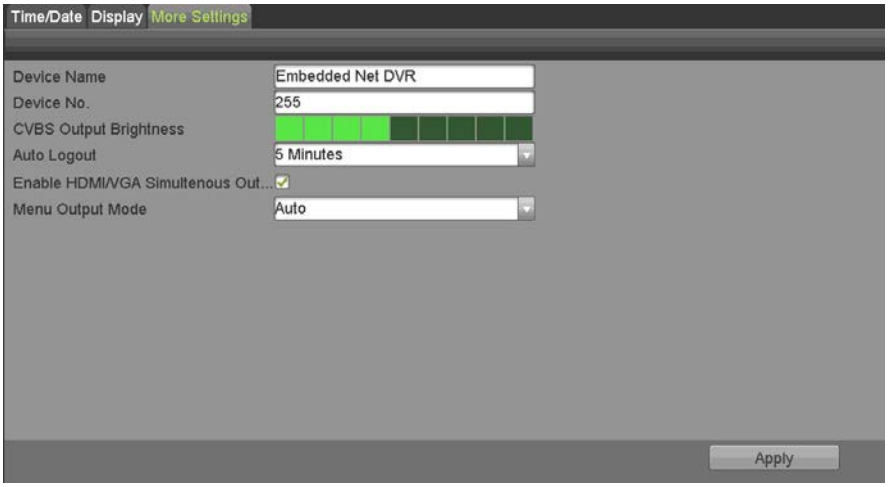


Figure 15-3 More Settings Interface

2. Configure the following settings:
   - **Device Name:** Edit the name of DVR.
   - **Device No.:** Used by PTZ joystick to identify the device to control. The Device No. can be set in the range of 1 to 255, and the default No. is 255.
   - **CVBS Output Brightness:** Adjust the video output brightness via the CVBS interface.

- **Auto Logout:** Set timeout time for menu inactivity. E.g., when the timeout time is set to *5 Minutes*, then the system will exit from the current operation menu to live view screen after five minutes of menu inactivity.
- **Enable HDMI/VGA Simultaneous Output:** Causes the HDMI monitor and the VGA monitor to display the same (main) image.
- **Menu Output Mode:** You can choose the menu display on different video output. **Auto** and **HDMI/VGA** are selectable.

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

15.4 Managing User Accounts

Purpose

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 permission to add and delete users and configure user parameters.

15.4.1 Adding a User

1. Go to **Menu > System Configuration > User > User Management**.

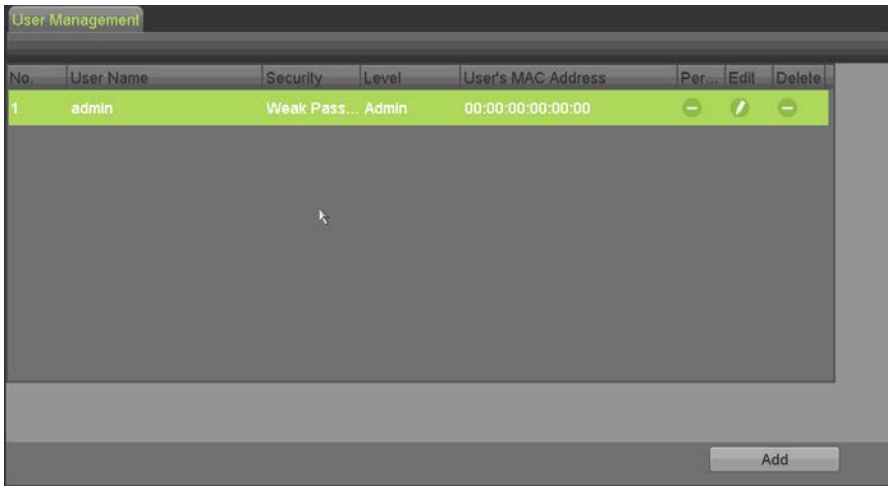


Figure 15-4 User Management Interface

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

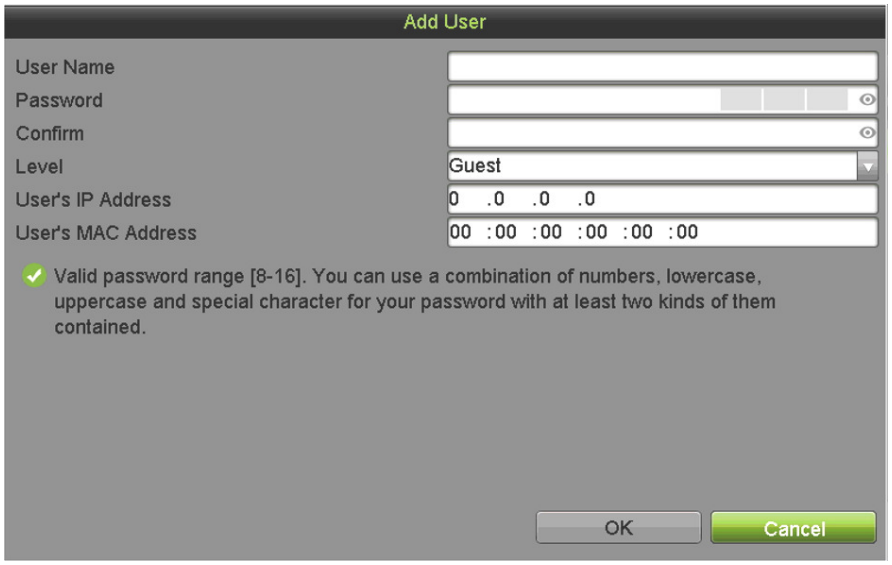


Figure 15-5 Add User Menu

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

   - **Password**: Set the password for the user account.

   WARNING

   STRONG PASSWORD RECOMMENDED – We highly recommend you create a strong password of your own choosing (using a minimum of eight characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters). in order to increase the security of your product. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

   - **Level:** Set the user level to **Operator** or **Guest**. Different user levels have different operating permissions.
     - **Operator:** The *Operator* user level has permission of Two-way Audio in Remote Configuration and all operating permissions in Camera Configuration by default.
     - **Guest:** The *Guest* user has no permission of Two-way Audio in Remote Configuration and has only the local/remote playback in the Camera Configuration by default.
   - **User's IP Address:** Enter the IP address of the user's computer on the network.
   - **User's MAC Address:** 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 below.

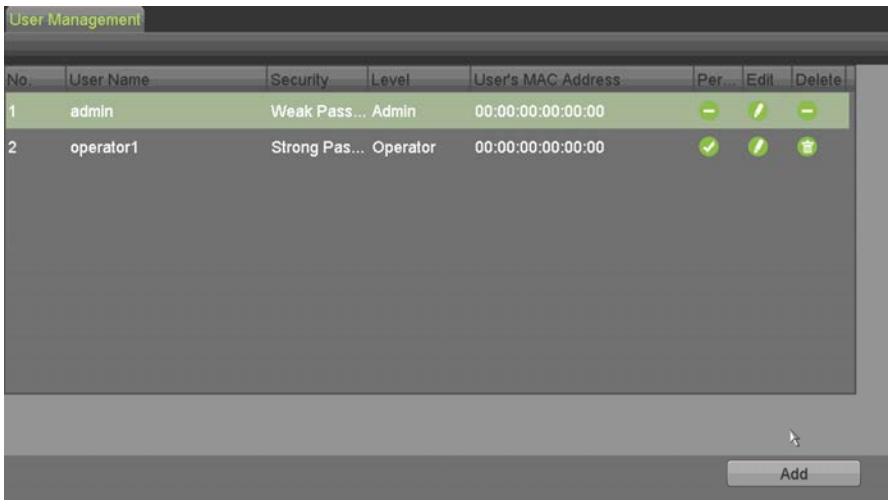


Figure 15-6 Added User Listed in User Management Interface

5. You can assign permissions for the added user.

   1) Select the user from the list and then click to enter the **Permission Settings** interface, as shown below.

Figure 15-7 User Permission Settings Interface

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

      - **Local Configuration**
        - **Local Log Search:** Searching and viewing logs and device system information.
        - **Local Parameters Settings:** Configuring parameters, restoring factory default parameters, and importing/exporting configuration files.
        - **Local Camera Management:** Enabling and disabling analog camera(s). Adding, deleting, and editing network camera(s). This function is supported by 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 viewing logs that are saved on the device.
  - **Remote Parameters Settings:** Remotely configuring parameters, restoring factory default parameters, and importing/exporting configuration files.
  - **Remote Camera Management:** Remotely enabling and disabling analog camera(s), and adding, deleting, and editing network camera(s). This function is supported by HDVR series.
  - **Remote Serial Port Control:** Configuring settings for RS-485 port.
  - **Remote Video Output Control:** Sending remote control panel signal.
  - **Two-way Audio:** Realizing two-way radio between the remote client and the device.
  - **Remote Alarm Control:** Remotely arming (notify alarm and exception message to the remote client) and controlling the alarm output.
  - **Remote Advanced Operation:** Remotely operating HDD management (initializing HDD, setting HDD property), upgrading system firmware.
  - **Remote Shutdown/Reboot:** Remotely shutting down or rebooting the device.
- **Camera Configuration**
  - **Remote Live View:** Remotely viewing live video of the selected camera(s).
  - **Local Manual Operation:** Locally starting/stopping manual recording, picture capturing, and alarm output of the selected camera(s).
  - **Remote Manual Operation:** Remotely starting/stopping manual recording, picture capturing, and alarm output of the selected camera(s).
  - **Local Playback:** Locally playing back recorded files of the selected camera(s).
  - **Remote Playback:** Remotely playing back recorded files of the selected camera(s).
  - **Local PTZ Control:** Locally controlling PTZ movement of the selected camera(s).
  - **Remote PTZ Control:** Remotely controlling PTZ movement of the selected camera(s).
  - **Local Video Export:** Locally exporting recorded files of the selected camera(s).

Local Camera Management is provided only for IP cameras.

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

15.4.2 Deleting a User

1. Go to **Menu > System Configuration > User**.
2. Select the user to be deleted from the list, as shown below.

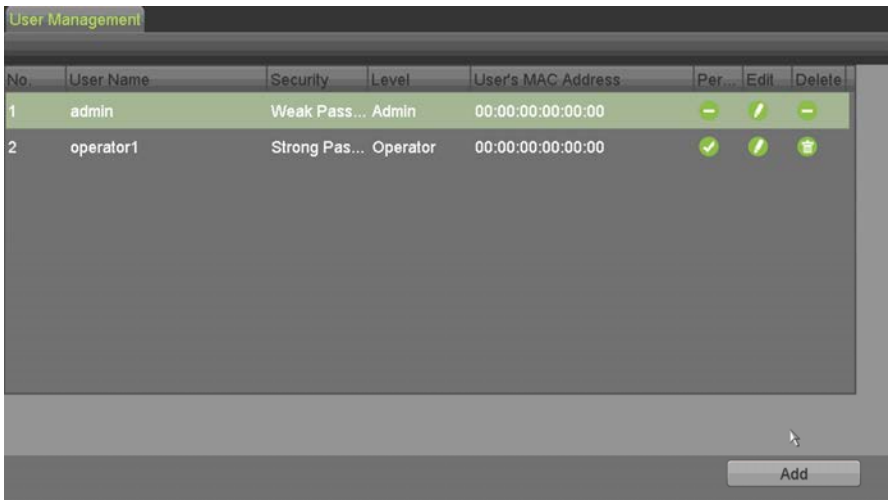


Figure 15-8 User List

3. Click to delete the selected user account.

15.4.3 Editing a User

Purpose

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

1. Go to **Menu > System Configuration > User**.
2. Select the user to be edited from the list.
3. Click the icon to enter the **Edit User** interface, as shown below.

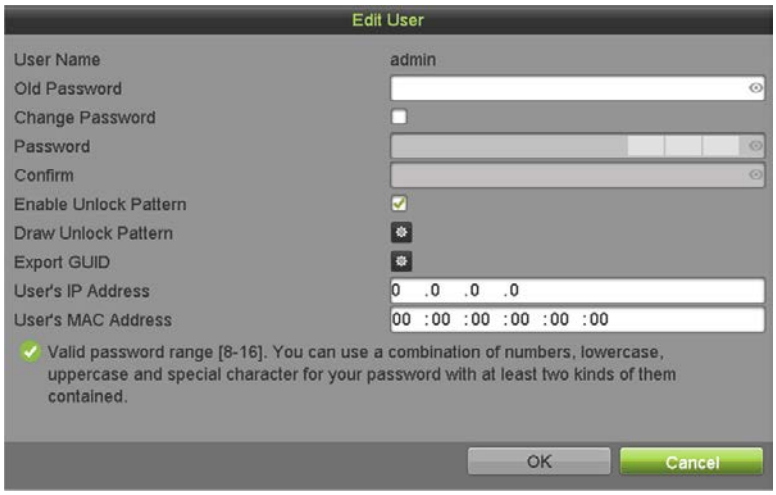


Figure 15-9 Edit User Interface (admin)

4. Edit the corresponding parameters.

   - **Operator and Guest**

     You can edit the user information, including user name, password, permission level, and MAC address. Check the **Change Password** checkbox to change the password, and input the new password in the **Password** and **Confirm** text field. A strong password is recommended.

   - **Admin**

     You are allowed only to edit the password and MAC address. Check the **Change Password** checkbox if you want to change the password, and input the correct old password and the new password in the **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 high security systems, resetting the password monthly or weekly can better protect your product.

NOTE

Hold down the icon and you will see clear text of the password. Release the mouse and the content of the password will again be 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.

NOTE

Refer to *2.3.1 Configuring the Unlock Pattern* for detailed instructions.

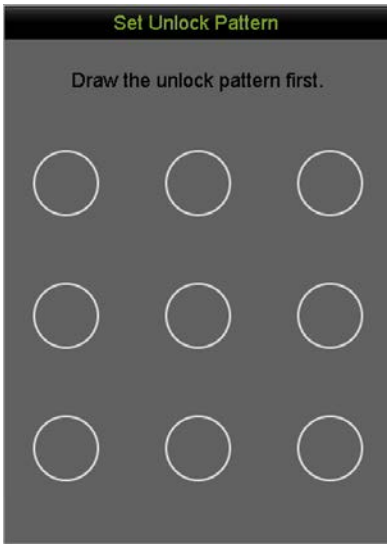


Figure 15-10 Set Unlock Pattern for Admin User

6. (Optional) Click the icon after **Draw Unlock Pattern** to modify the pattern.

7. (Optional) Click the icon after **Export GUID** to pop up the Reset Password interface. Click **Export** to export the GUID (Globally Unique Identifier; a file generated, exported, and saved to reset the user's password) to the USB flash drive for retrieving the forgotten password. Then a GUID file will be saved in the USB flash drive.

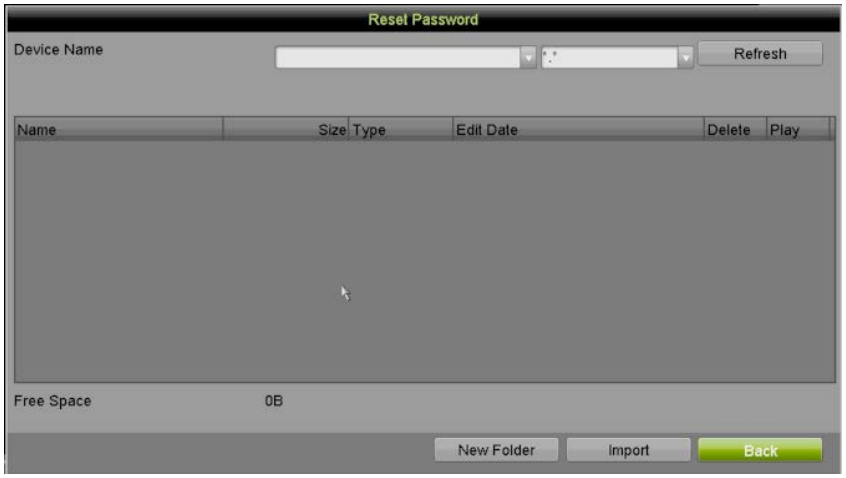


Figure 15-11 Export GUID

NOTE

You must input the correct old password of the *admin* before exporting the GUID.

8. Click **OK** to save the settings and exit from the menu.

9. (Optional) For the **Operator** or **Guest** user account, click the on the **User Management** interface to edit the permission.

Chapter 16 Appendix

16.1 Specifications

Model		DS-7204HTI-K1	DS-7208HTI-K2
Video/Audio Input	Video Compression	H.265+/H.265/H.264+/H.264	
	Analog Video Input	4-ch	8-ch
		BNC interface (1.0 Vp-p, 75 Ω), supporting Hikvision-C connection	
	HD-TVI Input	8 MP, 5 MP, 4 MP, 3 MP, 1080p30, 1080p25, 720p60, 720p50, 720p30, 720p25	
	AHD Input	5 MP, 4 MP, 3 MP, 1080p25, 1080p30, 720p25, 720p30	
	HDCVI Input	4 MP, 1080p25, 1080p30, 720p25, 720p30	
	CVBS Input	PAL/NTSC	
	IP Video Input	2-ch	4-ch
		Up to 8 MP resolution	
		Supports H.265+/H.265/H.264+/H.264 IP cameras	
	Audio Compression	G.711u	
	Audio Input	4-ch, RCA (2.0 Vp-p, 1 KΩ)	
Video/Audio Output	CVBS Output	1-ch, BNC (1.0 Vp-p, 75 Ω), resolution: PAL: 704 × 576, NTSC: 704 × 480	
	HDMI/VGA Output	VGA: 1-ch, 1920 × 1080/60 Hz, 1280 × 1024/60 Hz, 1280 × 720/60 Hz, 1024 × 768/60 Hz	
		HDMI: 1-ch, 4K (3840 × 2160)/30Hz, 2K (2560 × 1440)/60Hz, 1920 × 1080/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz	
	Encoding Resolution	8 MP/5 MP/4 MP/3 MP/1080p/720p/WD1/4CIF/VGA/CIF	
	Frame Rate	Main stream: 8 MP @ 12fps, 5 MP @ 20 fps, 3 MP @ 18 fps 4 MP/1080p/720p/WD1/4CIF/VGA/CIF @ 25 fps (P)/30 fps (N)	
		Sub-stream: WD1/4CIF/CIF @ 25 fps (P)/30 fps (N)	
	Video Bit Rate	32 Kbps to 16 Mbps	
	Audio Output	1-ch, RCA (linear, 1K Ω)	
	Audio Bit Rate	64 Kbps	
	Dual Stream	Supported	
	Stream Type	Video, Video & Audio	
	Synchronous Playback	4-ch	8-ch
Network Management	Remote Connections	32	64
	Network Protocols	TCP/IP, PPPoE, DHCP, Hik-Connect, DNS, DDNS, NTP, SADP, NFS, iSCSI, UPnP™, HTTPS, ONVIF	
Hard Disk	SATA	2 SATA interfaces	
	Capacity	Up to 8 TB capacity for each disk	
External Interface	Two-Way Audio Input	1-ch, RCA (2.0 Vp-p, 1 KΩ) (using the first audio input)	
	Network Interface	1, RJ45 10M/100M/1000M self-adaptive Ethernet interface	
	USB Interface	Front panel: 1 × USB 2.0 Rear panel: 1 × USB 3.0	
	Serial Interface	RS-485 (half-duplex)	
	Alarm In/Out	4/1	8/4
General	Power Supply	12 VDC	
	Consumption (w/o HDD)	≤15 W	≤20 W
	Working Temperature	-10° to +55° C (+14° to +131° F)	
	Working Humidity	10% to 90%	
	Dimensions (W × D × H)	380 × 320 × 48 mm (15.0 × 12.6 × 1.9 inch)	
	Weight (w/o HDD)	≤1.5 kg (3.3 lb)	≤2 kg (4.4 lb)

16.2 Glossary

- **Dual-Stream:** Dual-stream is a technology used to record high resolution video locally while transmitting a lower resolution stream over the network. The two streams are generated by the DVR, with the main stream having a maximum resolution of 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 frame of an NTSC signal contains 525 scan lines at 60Hz.
- **NVR:** Acronym for Network Video Recorder. An NVR can be a PC-based or embedded system used for centralized management and storage for IP cameras, IP Domes and other DVRs.
- **PAL:** Acronym for Phase Alternating Line. PAL is also another video standard used in broadcast televisions systems in large parts of the world. PAL signal contains 625 scan lines at 50Hz.
- **PTZ:** Acronym for Pan, Tilt, Zoom. PTZ cameras are motor driven systems that allow the camera to pan left and right, tilt up and down and zoom in and out.
- **USB:** Acronym for Universal Serial Bus. USB is a plug-and-play serial bus standard to interface devices to a host computer.

16.3 Troubleshooting

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

  Possible Reasons:

  — No VGA or HDMI connections.

  — Connection cable is damaged.

  — Input mode of the monitor is incorrect.

  Step 1 Verify the device is connected with the monitor via HDMI or VGA cable. If not, please connect the device with the monitor and reboot.

  Step 2 Verify the connection cable is good.

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

  Step 3 Verify Input mode of the monitor is correct.

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

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

  If it is solved, finish the process.

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

- **There is a beep sound after a new bought 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 broken-down.

  Step 1 Verify at least one HDD is installed in the device.

  1) If not, please install the compatible HDD.

  NOTE
  Refer to the "Quick Operation Guide" for the HDD installation steps.

  2) If you do not want to install an HDD, select **Menu > System Configuration > Exception** and uncheck the Audible Warning checkbox of "HDD Error."

  Step 2 Verify the HDD is initialized.

  1) Select **Menu > System Configuration > HDD > General**.

2) If the status of the HDD is "Uninitialized," check the checkbox of the corresponding HDD and click **Init**.

Step 3 Verify the HDD is detected or is in good condition.

1) Select **Menu > System Configuration > HDD > General**.

2) If the HDD is not detected or the status is "Abnormal," replace the dedicated HDD according to the requirement.

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

1) If it is solved, finish the process.

2) If not, please contact an engineer from our company to further process.

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

  Possible Reasons:

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

  Step 1 Check the parameters of Main Stream (Continuous) and Main Stream (Event).

  Select **Menu > Record Configuration > Record**, and set the resolution of Main Stream (Event) the same as the Main Stream (Continuous).

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

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

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

  If it is solved, finish the process.

  If not, please contact an engineer from our company for further process.

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

  Possible Reasons:

  — Pickup/camera cable is not connected well, impedance mismatches or is incompatible.

  — The stream type is not set as "Video & Audio."

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

  Step 2 Verify the setting parameters are correct.

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

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

  If it is solved, finish the process.

If not, contact an engineer from our company further process.

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

  Possible Reasons:

  — The frame rate is not the real-time frame rate.

  — The DVR supports up to 16-channel synchronize playback at the resolution of 4CIF, if you want a 16-channel synchronize playback at the resolution of 720p, the frame extracting may occur, which leads to a slight stuck.

  Step 1 Verify the frame rate is real-time frame rate.

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

  Step 2 Verify the hardware can support the playback.

  Reduce the playback channel numbers.

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

  Step 3 Reduce the number of local playback channels.

  Select **Menu > Playback**, and uncheck the checkboxes of unnecessary channels.

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

  If it is solved, finish the process.

  If not, contact an engineer from our company for further process.

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

  Possible Reasons:

  — The system time setting is incorrect.

  — The search condition is incorrect.

  — The HDD is in error or not detected.

  Step 1 Verify the system time setting is correct.

  Select **Menu > System Configuration > General > Time/Date**, and verify the "System Time" is correct.

  Step 2 Verify the search condition is correct.

  Select **Menu > Playback**, and verify the channel and time are correct.

  Step 3 Verify the HDD status is normal.

  Select **Menu > System Configuration > HDD > HDD Information** to view the HDD status and verify the HDD is detected and can be read and written normally.

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

If it is solved, finish the process.

If not, contact an engineer from our company for further process.

16.4 Compatible Hikvision IP Cameras

Type	Model	Version	Maximum Resolution	Sub-Stream	Audio
HD Network Camera	DS-2CD7153-E	V5.1.0 build 131202	1600×1200	√	×
	DS-2CD754F-EI	V5.1.0 build 131202	2048×1536	√	√
	DS-2CD783F-EI	V5.1.0 build 131202	2560×1920	√	√
	DS-2CD7164-E	V5.1.0 build 131202	1280×720	√	×
	DS-2CD864FWD-E	V5.1.0 build 131202	1600×1200	√	√
	DS-2CD4026FWD 14.33	V5.1.0 build5 131202	1920×1080	√	√
	DS-2CD6233F 14.24	V5.1.0 build5 131202	2048×1536	√	×
	DS-2CD2012-I	V5.1.0build131202	1280×960	√	×
	DS-2CD4012F	V5.1.0 build 131202	1280×1024	√	√
	DS-2CD4232FWD-I	V5.1.0 build 131202	2048×1536	√	√
SD Network Camera	DS-2CD793PFWD-EI	V5.1.0 build 131202	704×576	√	√
Intelligence Traffic Camera	iDS-2CD9122	V3.5.0 build131012	1920×1080	×	×
	iDS-2CD9121	V3.4.2 build 130718	1600×1200	×	×
Network Speed Dome	DS-2DF7274	V5.1.0 build 130923	1280×960	√	√
	DS-2DE7174	V5.0.2Build130926	1280×960	√	√

NOTE

For the list, our company holds the right to interpret.

16.5 Compatible Third-Party IP Cameras

Manufacturer	Model	Version	Maximum Resolution	Sub-Stream	Audio
Axis	P3304	5.2	1440×900	√	×
Sony	SNC-RH124	1.7.00	1280×720	√	√
Samsung	SND-5080P	3.10_130416	1280×1024	√	√
Vivotek	FD8134	0107a	1280×800	√	×
Bosch	Dinion NBN-921-P	V10500453	1280×720	×	×
Panasonic	SP306H	Application: 1.34 Image Data: 1.06	1280×960	×	√
Cannon	VB-H410	Ver.+1.0.0	1280×960	×	√
Zavio	F3206	MG.1.6.02c045	1920×1080	√	×
Pelco	IX30DN-ACFZHB3	1.8.2-20120327-2.9080-A1.7852	2048×1536	√	×

16.6 Applicable Power Adapters

NOTE

Use only power supplies listed in the user instructions.

Power Adapter Model	Specifications	Manufacturer
MSA-C1500IC12.0-18P-DE	12 V, 1.5 A	0000201935 MOSO Technology Co., Ltd.
ADS-25FSG-12 12018GPG	CE, 100 to 240 VAC, 12 V, 1.5 A, 18 W, Φ5.5 × 2.1 × 10	0000200174 Shenzhen Honor Electronic Co., Ltd.
MSA-C1500IC12.0-18P-US	12 V, 1.5 A	0000201935 MOSO Technology Co., Ltd.
TS-A018-120015AD	100 to 240 VAC, 12 V, 1.5 A, 18 W, Φ5.5 × 2.1 × 10	0000200878 Shenzhen Transin Technologies Co., Ltd.
MSA-C2000IC12.0-24P-DE	12 V, 2 A	0000201935 MOSO Technology Co., Ltd.
ADS-24S-12 1224GPG	CE, 100 to 240 VAC, 12 V, 2 A, 24 W, Φ2.1	0000200174 Shenzhen Honor Electronic Co., Ltd.
MSA-C2000IC12.0-24P-US	US, 12 V, 2 A	0000201935 MOSO Technology Co., Ltd.
ADS-26FSG-12 12024EPCU	US, 12 V, 2 A	0000200174 Shenzhen Honor Electronic Co., Ltd.
KPL-040F-VI	12 V, 3.33 A, 40 W	0000203078 Channel Well Technology Co., Ltd.
MSA-Z3330IC12.0-48W-Q	12 V, 3.33 A	0000201935 MOSO Technology Co., Ltd.
MSP-Z1360IC48.0-65W	48 V, 1.36 A	0000201935 MOSO Technology Co., Ltd.
KPL-050S-II	48 V, 1.04 A	0000203078 Channel Well Technology Co., Ltd.


First Choice for Security Professionals