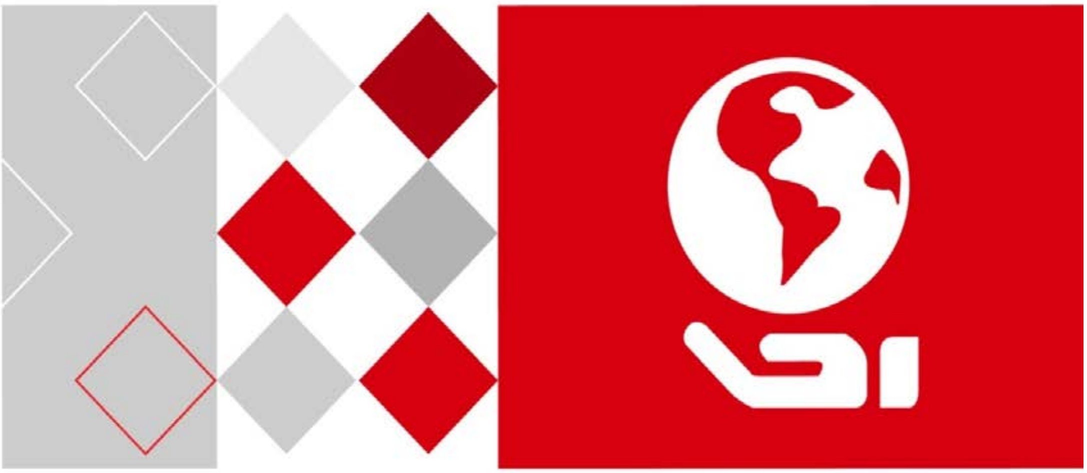


User Manual

Digital Video Recorder (DVR)

DS-73xxHUI-K4, DS-73xxHQI-K4, DS-90xxHUI-K8

User Manual

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

About this Manual

This Manual is applicable to Turbo HD Digital Video Recorder (DVR).

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

Please use this user manual under the guidance of professionals.

Trademarks Acknowledgement

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

Legal Disclaimer

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

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

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

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

Regulatory Information

FCC Information

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

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

FCC Conditions

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

1. This device may not cause harmful interference.

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

EU Conformity Statement

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

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

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

Industry Canada ICES-003 Compliance

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

Applicable Models

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

Series	Model
DS-73xxHUI-K4	DS-7304HUI-K4 DS-7308HUI-K4 DS-7316HUI-K4
DS-73xxHQI-K4	DS-7308HQI-K4 DS-7316HQI-K4 DS-7332HQI-K4
DS-90xxHUI-K8	DS-9008HUI-K8 DS-9016HUI-K8

Symbol Conventions

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

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

Safety Instructions

- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.
- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region. Please refer to technical specifications for detailed information.
- Input voltage should meet both the SELV (Safety Extra Low Voltage) and the Limited Power Source with 100 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.
- Please make sure that the plug is firmly connected to the power socket.
- If smoke, odor or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.

Preventive and Cautionary Tips

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

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

Product Key Features

General

- Connectable to TurboHD and analog cameras
- Supports UTC protocol for connecting camera over coax
- Connectable to IP cameras
- The analog signal inputs including TurboHD and CVBS can be automatically recognized without configuration
- Each channel supports dual-stream. And sub-stream supports up to WD1 resolution
- The main stream of HUI Series supports up to 5 MP resolution of all the channels (HUI Series)
- 5 MP long distance transmission can be enabled for the analog cameras (HUI Series)
- 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
- There are two HDMI interfaces of which the HDMI1 and VGA interfaces share simultaneous output. For HDMI1/VGA output, up to 1920 × 1080 resolution is supported. For HDMI2 output, up to 4K (3840 × 2160) resolution is supported
- 1/4/6/8/9/16/25/36 screen live view is supported, and the display sequence of screens is adjustable

  NOTE

  If the sum of the analog and IP channels exceeds 25, up to 32-window division mode is supported for the VGA/HDMI1 output

- Live view screen can be switched in group and manual switch and automatic cycle live view are also provided, the interval of automatic cycle can be adjusted
- CVBS output only serves as the aux output or live view output
- Quick setting menu is provided for live view
- The selected live view channel can be shielded
- VCA information overlay in live view for the supported analog cameras and in smart playback for the supported analog and IP cameras
- Motion detection, video-tampering detection, video exception alarm, video loss alarm, and VCA alarm functions
- 1-ch analog camera supports people counting and heat map functions
- HUI Series supports line crossing detection and intrusion detection of all channels, and 2-ch sudden scene change detection.
- The enhanced VCA mode conflicts with the 2K/4K output and 4 MP/5 MP signal input (HUI Series)
- Privacy mask
- Several PTZ protocols (including Omnicast VMS of Genetec) supported; PTZ preset, patrol and pattern
- Zooming in/out by clicking the mouse and PTZ tracing by dragging mouse.

HDD Management

- Each disk can have a maximum of 8 TB storage capacity
- 8 network disks (8 NAS disks, 8 IP SAN disks, or n NAS disks + m IP SAN disks (n+m ≤ 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
- Hot-swappable HDD supports RAID 0, RAID 1, RAID 5, RAID 6, and RAID 10 storage schemes, and can be enabled and disabled on your demand. 16 arrays can be configured (DS-90xxHUI-K8 only)

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
- Supports POS triggered recording
- Eight recording time periods with separated recording types
- Supports Channel-Zero encoding
- Main stream and sub-stream configurable for simultaneous recording
- Pre-record and post-record for motion detection triggered recording, and pre-record time for schedule and manual recording
- Searching record files 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
- When TurboHD input is connected, the information including the resolution and frame rate will be overlaid on the bottom right corner of the live view for five seconds. When CVBS input is connected, the information such as NTSC or PAL will be overlaid on the bottom right corner of the live view for five seconds.
- Search and play back record files by camera number, recording type, start time, end time, etc.
- Smart playback to go through less effective information
- Main stream and sub-stream selectable for local/remote playback
- Zooming in for any area when playback
- Multi-channel reverse playback
- Supports pause, fast forward, slow forward, skip forward, and skip backward when playback, locating by dragging the mouse on the progress bar
- 4/8/16-ch synchronous playback
- Manual capture, continuous capture of video images, and playback of captured pictures

Backup

- Exports data to a USB or eSATA 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

Alarms and Exceptions

- 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, and HDD full, etc.
- Alarm triggers full screen monitoring, audio alarm, notifying surveillance center, sending email 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 (requires camera with alarm I/O)
- System will automatically reboot when a problem is detected in an attempt to restore normal functionality

Other Local Functions

- Manual and automatic video quality diagnostics
- Operable by mouse and remote control
- Three-level user management; admin user can create many operating account and define their operating permission, which includes the permission to access any channel
- Completeness of operation, alarm, exceptions and log writing and searching
- Manually triggering and clearing alarms
- Importing and exporting of configuration file of devices
- Getting cameras type information automatically
- Unlock pattern for device login for the *admin*
- Clear-text password available
- GUID file can be exported for use in resetting the password
- Multiple connected analog cameras supporting TurboHD can be upgraded simultaneously via the 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 the Internet access risk and ask you to confirm the “Terms of Service” and “Privacy Statement” before enabling the service. You should create a verification code to connect to Hik-Connect.
- TCP, UDP, and RTP for unicast
- Auto/Manual port mapping by UPnP™
- Remote search, playback, download, locking and unlocking 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

NOTE: Figures in this manual are for illustration only; your screens may differ.

1 Introduction

1.1 Front Panel

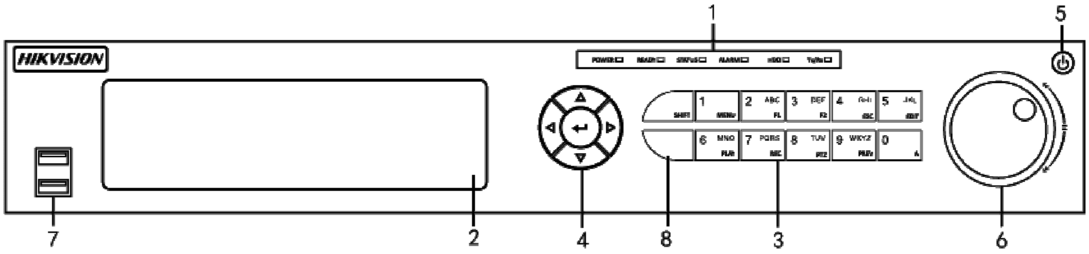


Figure 1, DS-73xxHUI-K4, DS-73xxHQI-K4 Front Panel

Table 1-1 DS-73xxHUI-K4, DS-73xxHQI-K4 Front Panel Description

No.	Name		Function Description
1	POWER		Turns green when DVR is powered up
	READY		Turns green, indicating that the DVR is functioning properly
	STATUS		Turns green when device is controlled by an IR remote
			Turns red when controlled by a keyboard and purple when IR remote and keyboard is used at the same time
	ALARM		Turns red when a sensor alarm is detected
	HDD		Flickers red when data is being read from or written to HDD
	Tx/Rx		Flickers green when network connection is functioning properly
2	DVD-R/W		Slot for DVD-R/W
3	Composite Keys	SHIFT	Switches between the numeric or letter input and functions of the composite keys. (Input letter or numbers when the light is out; Realize functions when the light is red.)
		1/MENU	Enters numeral “1” Accesses the main menu interface
		2/ABC/F1	Enters numeral “2”
			Enters letters “ABC”
			The F1 button when used in a list field will select all items in the list
			Turns on/off PTZ light in PTZ Control mode, and use it to zoom out the image
			Switches between main and spot video output in live view or playback mode.
		3/DEF/F2	Enters numeral “3”
			Enters letters “DEF”
			Uses the F2 button is used to change the tab pages
			Zooms in the image in PTZ control mode
		4/GHI/ESC	Enters numeral “4”
			Enters letters “GHI”
			Exits and back to the previous menu
		5/JKL/EDIT	Enters numeral “5”
			Enters letters “JKL”
			Deletes characters before cursor
			Check the checkbox and select the ON/OFF switch
			Starts/stops record clipping in playback
		6/MNO/PLAY	Enters numeral “6”
			Enters letters “MNO”
			Accesses to playback interface in Playback mode
		7/PQRS/REC	Enters numeral “7”
			Enters letters “PQRS”
			Accesses to manual record interface Manually enables/disables record
		8/TUV/PTZ	Enters numeral “8”
			Enters letters “TUV”
			Accesses PTZ control interface
		9/WXYZ/PREV	Enters numeral “9”
			Enters letters “WXYZ”
			Multi-channel display in live view
		0/A	Enters numeral “0”

No.	Name	Function Description
		Shifts the input methods in the editing text field. (Upper and lowercase, alphabet, symbols or numeric input).
4	DIRECTION	Navigates between different fields and items in menus
		Uses the Up and Down buttons to speed up and slow down the playing of video files in Playback mode. The Left and Right button will select the next and previous record files.
		Cycles through channels in Live View mode.
		Controls the movement of the PTZ camera in PTZ control mode
	ENTER	Confirms selection in any of the menu modes
		Checks the checkbox
		Plays or pauses the playing of video files in Playback mode
		Advances the video by a single frame in single-frame Playback mode
		Stops/starts auto switch in Auto-switch mode
5	POWER	Power on/off switch
6	JOG SHUTTLE Control	Moves the active selection up and down in a menu
		Cycles through different channels in live view mode
		Jumps 30s forward/backward in video files in the playback mode
		Controls the movement of the PTZ camera in PTZ control mode
		Moves the active selection up and down in a menu
7	USB Interface	Universal Serial Bus (USB) ports for additional devices such as USB mouse and USB Hard Disk Drive (HDD)
8	IR Receiver	Receiver for IR remote control

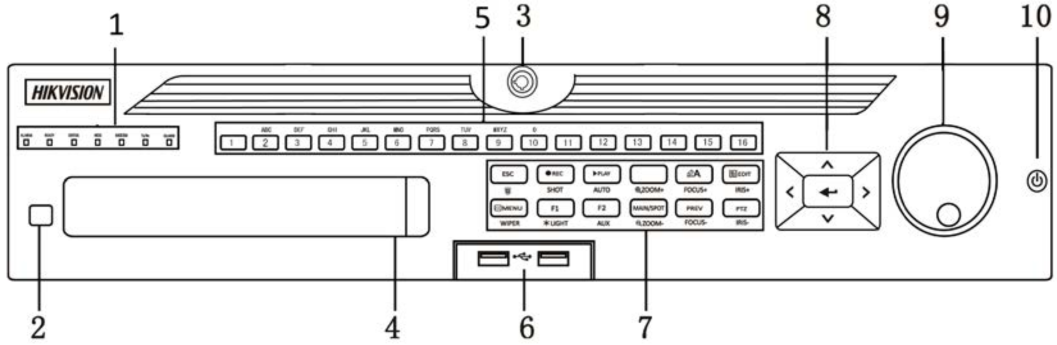


Figure 2, DS-90xxHUI-K8 Front Panel

Table 1-2 DS-90xxHUI-K8 Front Panel Description

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

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

1.2 IR Remote Control Operations

The DVR may also be controlled with the included IR remote control.

NOTE

If your system is secured with a password pattern, press ESC on the remote to display the password input window and input the password by using a keyboard.

NOTE

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

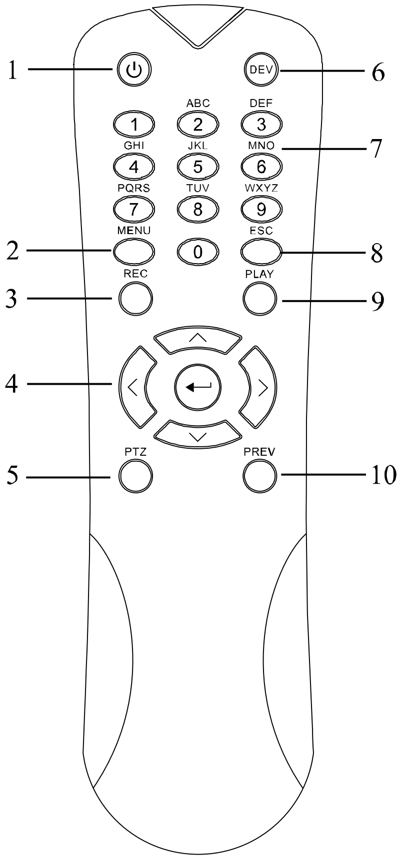


Figure 3, Remote Control

The keys on the remote control resemble the ones found on the front panel. See Table 1-3.

Table 1-3 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 5 seconds.
2	MENU Button	Press the button to return to the main menu (after successful login).
		Press and hold the button for 5 seconds will turn off audible key beep.
		In PTZ Control mode, the MENU button will start wiper (if applicable).
		In Playback mode, it is used to show/hide the control interface.
3	REC Button	Enter the Manual Record setting menu.
		In PTZ control settings, press the button and then you can call a PTZ preset by pressing Numeric button.
		It is also used to turn audio on/off in the Playback mode.
4	DIRECTION Button	Navigate between different fields and items in menus.
		In the Playback mode, the Up and Down button is used to speed up and slow down recorded video. The Left and Right button will select the next and previous record files.
		In Live View mode, these buttons can be used to cycle through channels.
		In PTZ control mode, it can control the movement of the PTZ camera.
	ENTER Button	Confirm selection in any of the menu modes.
		It can also be used to *tick* checkbox fields.
		In Playback mode, it can be used to play or pause the video.
		In single-frame Playback mode, pressing the button will advance the video by a single frame.
5	PTZ Button	In Auto-switch mode, it can be used to stop /start auto switch.
6	DEV	Enables/Disables Remote Control.
7	Alphanumeric Buttons	Switch to the corresponding channel in Live view or PTZ Control mode.
		Input numbers and characters in Edit mode.
		Switch between different channels in the Playback mode.
8	ESC Button	Back to the previous menu.
		Press for Arming/disarming the device in Live View mode.
9	PLAY Button	The button is used to enter the All-day Playback mode.
		It is also used to auto scan in the PTZ Control menu.
10	PREV Button	Switch between single screen and multi-screen mode.
		In PTZ Control mode, it is used to adjust the focus in conjunction with the A/FOCUS+ button.

1.2.1 Troubleshooting Remote Control

NOTE

Make sure batteries have been installed properly. Also, note that the remote control must be aimed at the IR receiver on the NVR 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 front panel Status indicator turns blue, the remote control is operating properly. If the Status indicator does not turn blue and there is no response, check the following:

- Batteries are installed correctly and the polarities are not reversed.
- Batteries are fresh and not out of charge.
- IR receiver is not obstructed.

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

1.3 USB Mouse Operation

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

1. Plug mouse into a USB interface on the DVR. The mouse should automatically be detected. If not, the mouse might not be compatible. Refer to your mouse provider.

Table 1-4 Description of the Mouse Control

Name	Action	Description
Left-Click	Single-Click	Live view: Select channel and show the quick set menu. Menu: Select and enter.
	Double-Click	Live view: Switch between single-screen and multi-screen.
	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

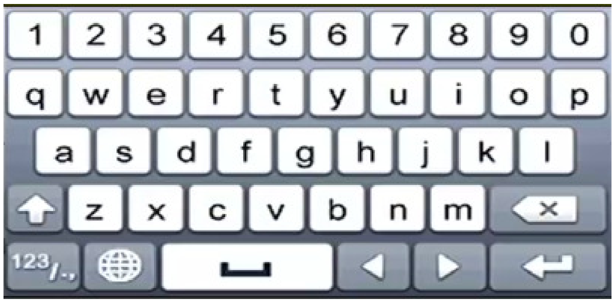


Figure 4, Soft Keyboard

Description of the buttons on the soft keyboard:

Table 1-5 Description of the Soft Keyboard Icons

Icon	Description	Icon	Description
0 … 9	Number	A … Z	English letter
⇧	Lowercase/Uppercase	⌫	Backspace
123/., ABC	Switch the keyboard	␣	Space
◀ ▶	Positioning the cursor	↵	Enter
#+=	Symbols	🌐	Reserved

1.5 Rear Panel

NOTE

The rear panel varies by model. Refer to the actual product. The following figures are for reference only.

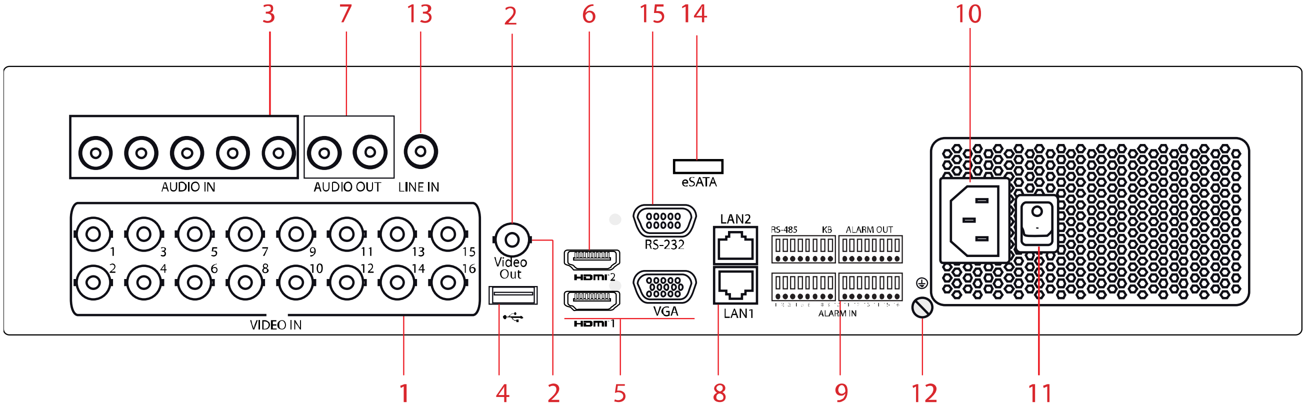


Figure 5, DS-73xxHUI-K4 Rear Panel

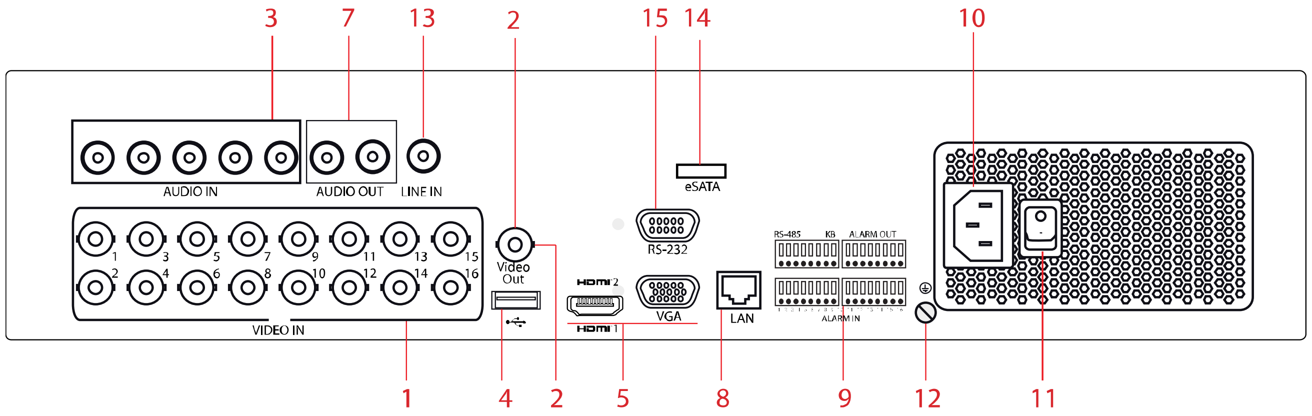


Figure 6, DS-73xxHQI-K4 Rear Panel

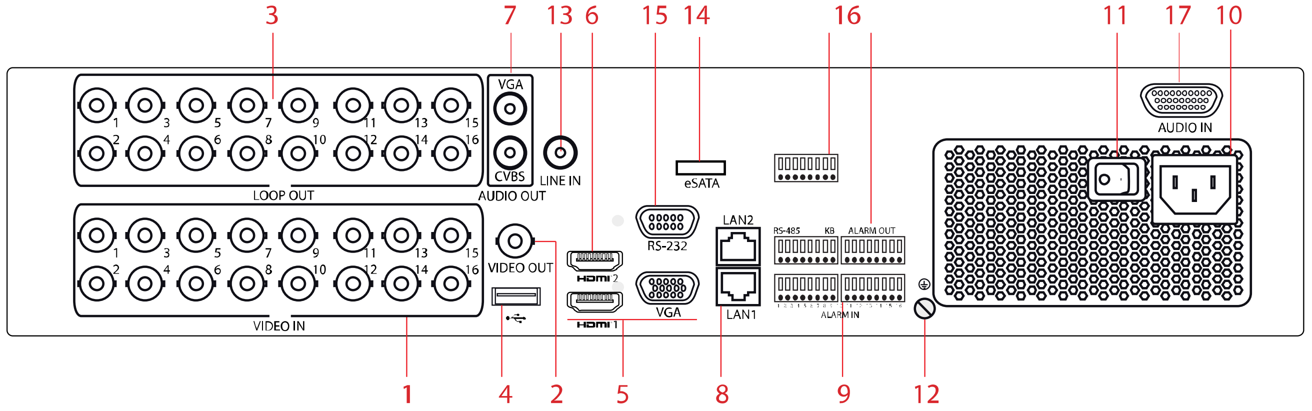


Figure 7, DS-90xxHUI-K8 Rear Panel

Table 1-6 Description of DS-73xxHUI-K4, DS-73xxHQI-K4, and DS-90xxHUI-K8 Rear Panel

No.	Item	Description
1	VIDEO IN	BNC interface for TurboHD and analog video input.
2	VIDEO OUT	BNC connector for video output.
3	AUDIO IN/LOOP OUT (for DS-90xxHUI-K8)	RCA connector
4	USB Port	Universal Serial Bus (USB) port for additional devices.
5	HDMI1/VGA	Simultaneous HDMI1/VGA output. Display local video output and menu.
6	HDMI2	HDMI2 video output connector (DS-73xxHUI-K4 and DS-90xxHUI-K8)
7	AUDIO OUT	RCA connector
8	Network Interface	Connector for network (DS-73xxHUI-K4 and DS-90xxHUI-K8 = x2, DS-73xxHUI-K4 = x1)
9	RS-485 and Alarm Interface	Connector for RS-485 devices. T+ and T- pins connect to R+ and R- pins of PTZ receiver respectively.
		D+, D- pin connects to Ta, Tb pin of controller. For cascading devices, the first DVR's D+, D- pin should be connected with the D+, D- pin of the next DVR.
		Connector for alarm input
		Connector for alarm output
10	Power Supply	100 to 240 VAC power supply
11	Power Switch	Switch for turning on/off the device
12	GND	Ground
13	LINE IN	BNC connector for audio input
14	eSATA	Connects external SATA HDD, CD/DVD-RW
15	RS-232 Interface	Connector for RS-232 devices
16	ALARM OUT	Connector for alarm output
17	AUDIO IN (for DS-90xxHUI-K8)	RCA connector

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 power supply is the same with the DVR's requirement, and the ground connection is working properly.

2.1.1 Starting the DVR

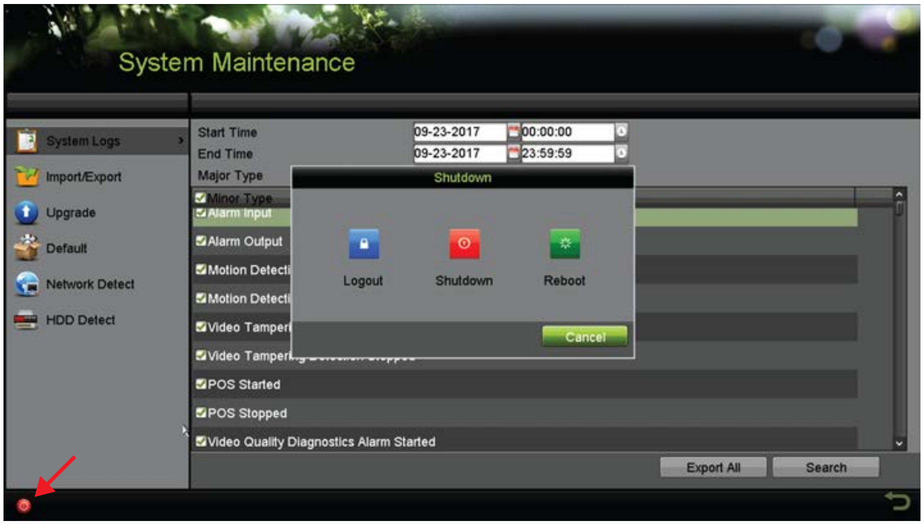
Check that the power supply is plugged into an electrical outlet. It is HIGHLY recommended that an Uninterruptible Power Supply (UPS) be used in conjunction with the device.

Turn on the power switch on the rear panel, and the Power indicator LED should turn on indicating that the unit begins to start up.

After startup, the Power indicator LED remains on.

2.1.2 Shutting Down/Logging Out/Rebooting the DVR

1. Go to Menu > Maintenance.



Start Time 09-23-2017 00:00:00
End Time 09-23-2017 23:59:59

Figure 8, Shutdown Menu

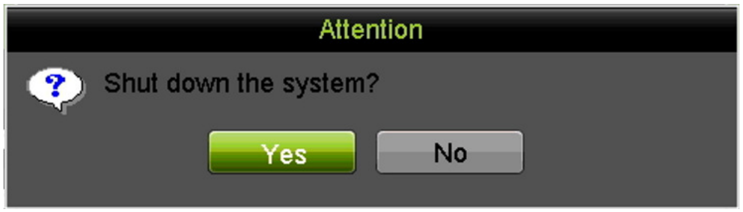
2. Click ⏻ (lower left corner of screen) to display the Shutdown window.

3. Click one of the following:

- **Logout** – Logs the current user out of the system.

- **Shutdown** – Shuts system down.
- **Reboot** – Shuts system down and reboots.
- **Cancel** – Cancels shutdown.

4. Click **Yes**.
5. Turn off the power switch on the rear panel.



Shut down the system?

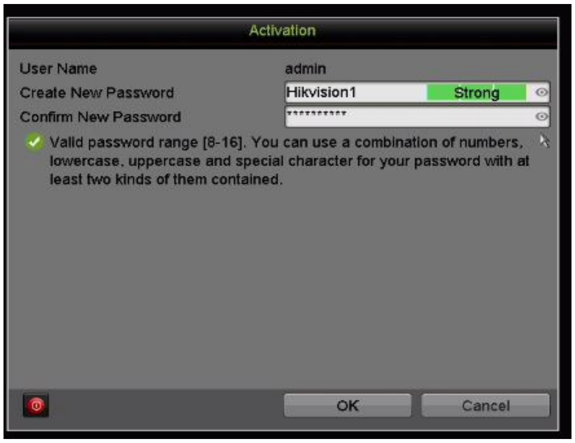
Figure 9, Shutdown Prompt

2.2 Activating the Device

Purpose

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

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



User Name admin

Create New Password Hikvision1 Strong

Confirm New Password **********

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

Figure 10, Settings Admin Password

WARNING

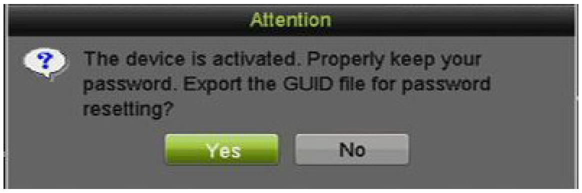
STRONG PASSWORD RECOMMENDED – We highly recommend you create a strong password of your own choosing (using a minimum of eight characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of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

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

NOTE

Clear text password is supported. Click ◉ to see the clear text of the password. Click the icon again and the password again becomes invisible.

3. After the device is activated, the Attention box pops up as below.

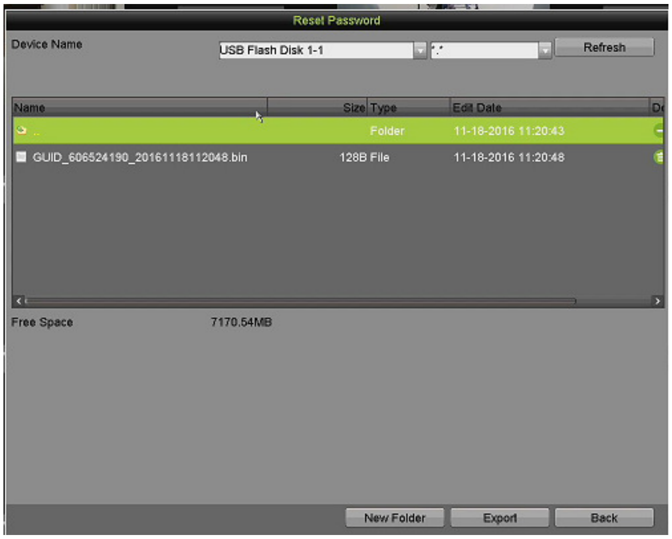


Attention

The device is activated. Properly keep your password. Export the GUID file for password resetting?

Figure 11, Attention Window

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



Reset Password

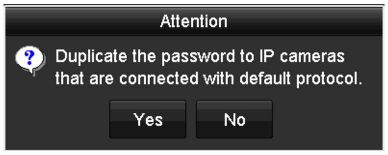
Device Name: USB Flash Disk 1-1 | *.*

Name	Size	Type	Edit Date	De
..		Folder	11-18-2016 11:20:43	
GUID_606524190_20161118112048.bin	128B	File	11-18-2016 11:20:48	

Free Space: 7170.54MB

Figure 12, Export GUID

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



Attention

Duplicate the password to IP cameras that are connected with default protocol.

Figure 13, Duplicate the Password

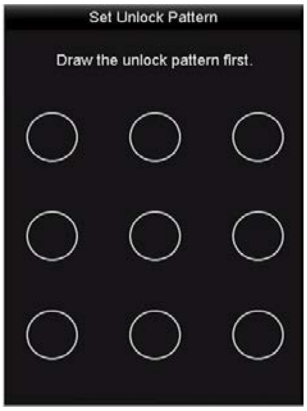
2.3 Using the Unlock Pattern for Login

Purpose

An *admin* can configure an unlock pattern for device login.

2.3.1 Configuring the Unlock Pattern

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

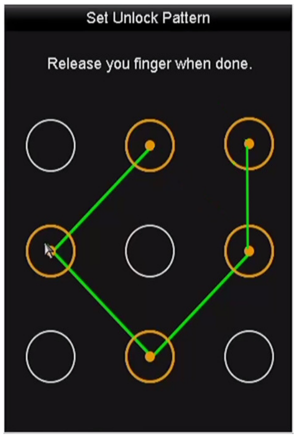


Set Unlock Pattern

Draw the unlock pattern first.

Figure 14, 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.



Set Unlock Pattern

Release you finger when done.

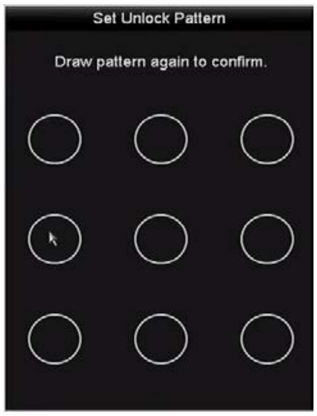
Figure 15, Draw the Pattern

NOTE

Connect at least four dots to draw the pattern.

Each dot can be connected only once.

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

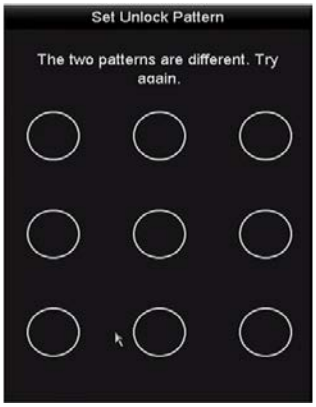


Set Unlock Pattern

Draw pattern again to confirm.

Figure 16, Confirm the Pattern

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



Set Unlock Pattern

The two patterns are different. Try again.

Figure 17, Reset the Pattern

2.3.2 Logging in via Unlock Pattern

NOTE

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

Configure the pattern first before unlocking.

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

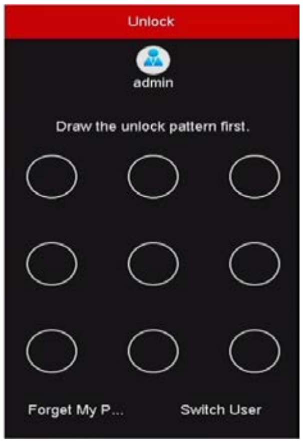


Figure 18, Draw the Unlock Pattern

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

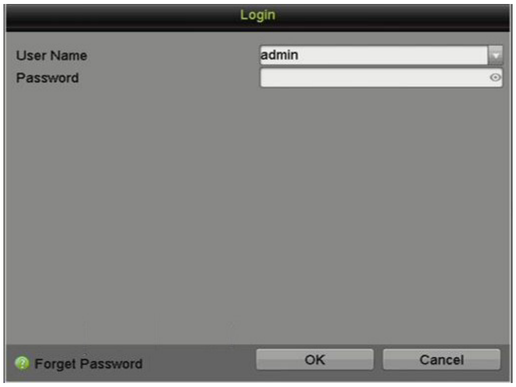
NOTE

You can right click the mouse to log in via the normal mode.

If you have forgotten your pattern, you can select the **Forget My Pattern** or **Switch User** option to enter the normal login dialog box.

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

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



User Name: admin

Password:

Figure 19, Normal Login Dialog Box

2.3.3 Login and Logout

2.3.3.1 User Login

Purpose

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

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

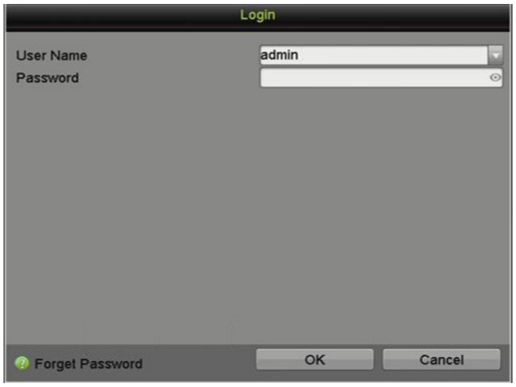


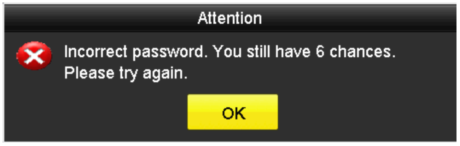
Figure 20, Login Interface

2. Input the **Password**.

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

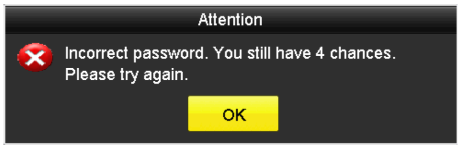
NOTE

In the Login interface, for the admin user, if you have entered the wrong password seven times, the account will be locked for 60 seconds. For operators, if you have entered the wrong password for five times, the account will be locked for 60 seconds.



Incorrect password. You still have 6 chances. Please try again.

Figure 21, User Account Protection for the Admin



Incorrect password. You still have 4 chances. Please try again.

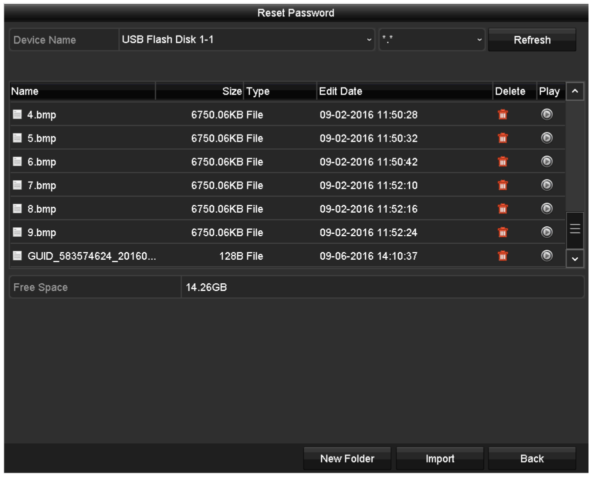
Figure 22, User Account Protection for the Operator

2.3.4 Resetting Your Password

Purpose

If you forget the *admin* password, you can reset the password by importing the GUID file, which was exported and saved in the local USB flash drive after you activated the device.

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



Reset Password

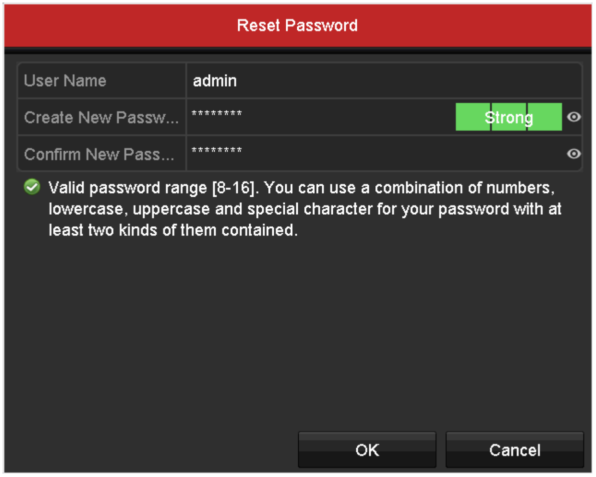
Device Name: USB Flash Disk 1-1 | *.*

Name	Size	Type	Edit Date	Delete	Play
4.bmp	6750.06KB	File	09-02-2016 11:50:28	🗑	▶
5.bmp	6750.06KB	File	09-02-2016 11:50:32	🗑	▶
6.bmp	6750.06KB	File	09-02-2016 11:50:42	🗑	▶
7.bmp	6750.06KB	File	09-02-2016 11:52:10	🗑	▶
8.bmp	6750.06KB	File	09-02-2016 11:52:16	🗑	▶
9.bmp	6750.06KB	File	09-02-2016 11:52:24	🗑	▶
GUID_583574624_20160...	128B	File	09-06-2016 14:10:37	🗑	▶

Free Space: 14.26GB

Figure 23, Import GUID

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



Reset Password

User Name: admin

Create New Passw...: ******** Strong

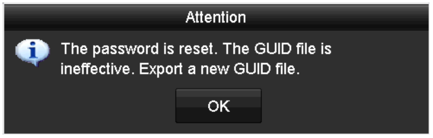
Confirm New Pass...: ********

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

Figure 24, Reset Password

3. Input the new password and confirm the password.

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

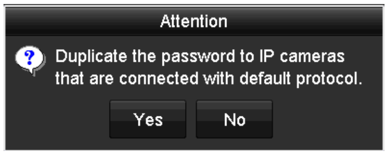


Attention

The password is reset. The GUID file is ineffective. Export a new GUID file.

Figure 25, GUID File Imported

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



Duplicate the password to IP cameras that are connected with default protocol.

Figure 26, Duplicate the Password

NOTE

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

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

2.3.5 Adding and Connecting IP Cameras

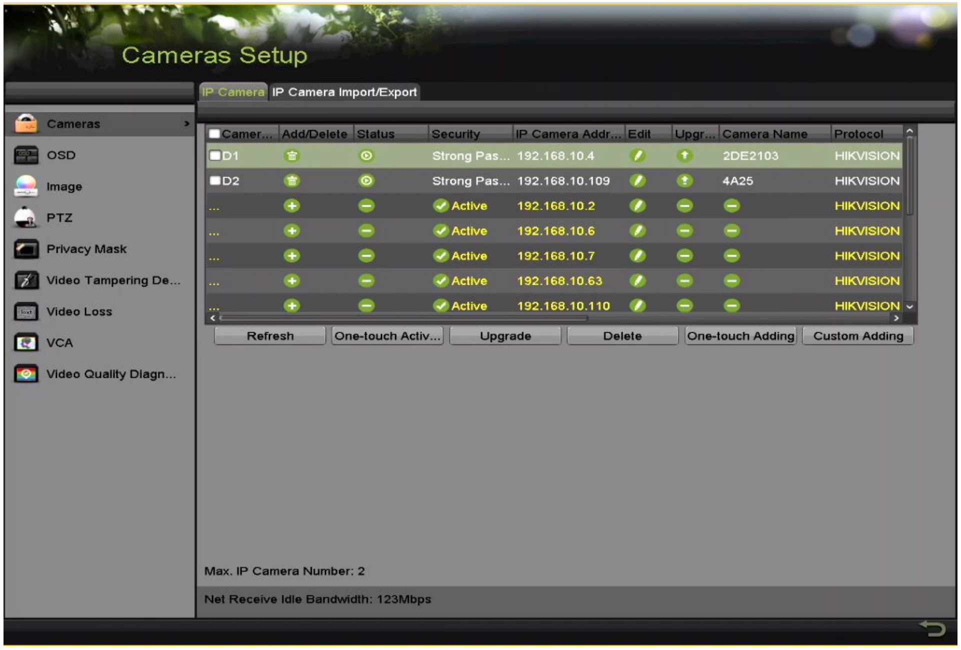
2.3.5.1 Activating an IP Camera

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



□ Camer...	Add/Delete	Status	Security	IP Camera Addr...	Edit	Upgr...	Camera Name	Protocol
□ D1	🗑	⊙	Strong Pas...	192.168.10.4	✎	↑	2DE2103	HIKVISION
□ D2	🗑	⊙	Strong Pas...	192.168.10.109	✎	↑	4A25	HIKVISION
...	+	−	✓ Active	192.168.10.2	✎	−	−	HIKVISION
...	+	−	✓ Active	192.168.10.6	✎	−	−	HIKVISION
...	+	−	✓ Active	192.168.10.7	✎	−	−	HIKVISION
...	+	−	✓ Active	192.168.10.63	✎	−	−	HIKVISION
...	+	−	✓ Active	192.168.10.110	✎	−	−	HIKVISION

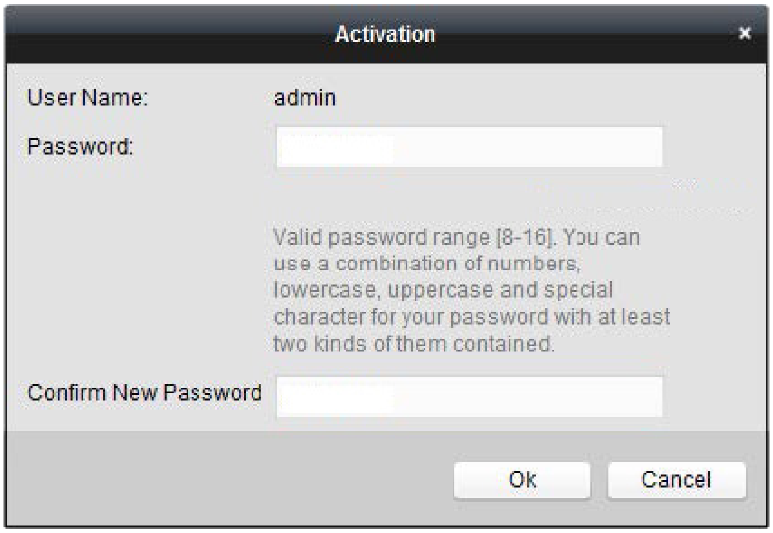
Max. IP Camera Number: 2

Net Receive Idle Bandwidth: 123Mbps

Figure 27, IP Camera Management Interface

2. Click the inactive icon of the camera to enter the following interface to activate it. You can also select multiple cameras

from the list and click the **One-touch Activate** to activate the cameras in batch.



User Name: admin

Password:

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

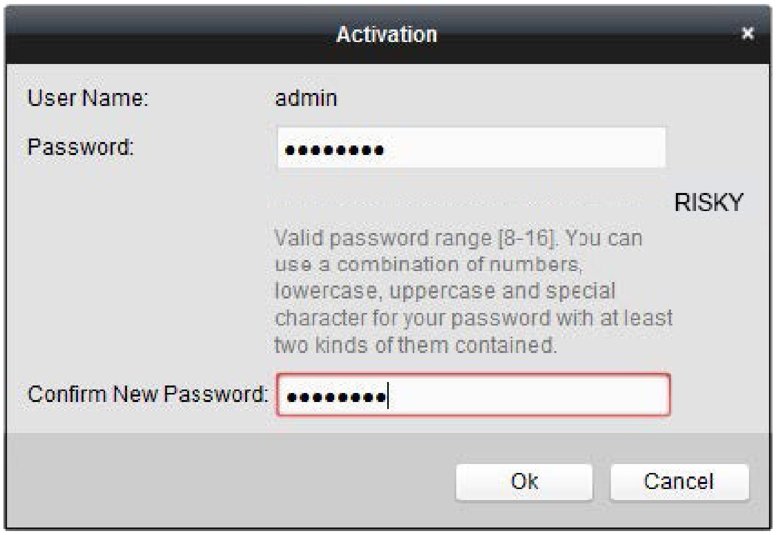
Confirm New Password

Figure 28, Activate the Camera

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

   Use Admin Password: If you check this checkbox, the camera(s) will be configured with the admin password of the operating DVR.

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



User Name: admin

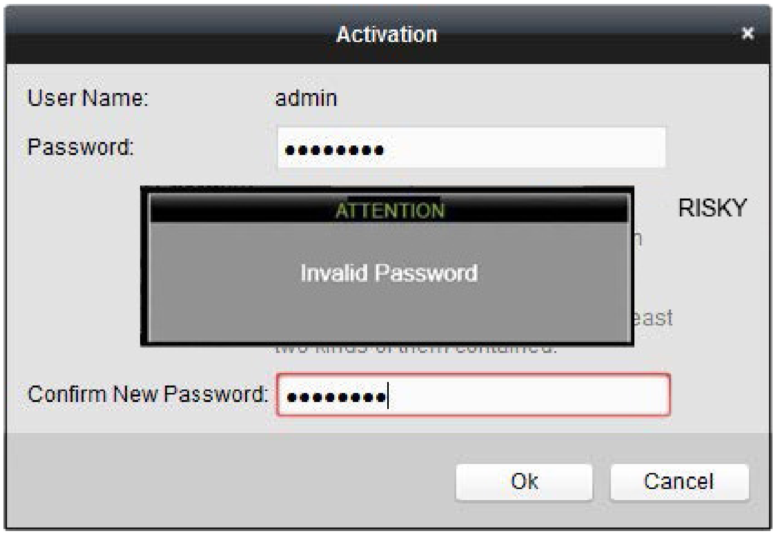
Password: ••••••••

RISKY

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

Confirm New Password: ••••••••

Figure 29, Level 0 (Inadequate) Strength Password



User Name: admin

Password: •••••••••

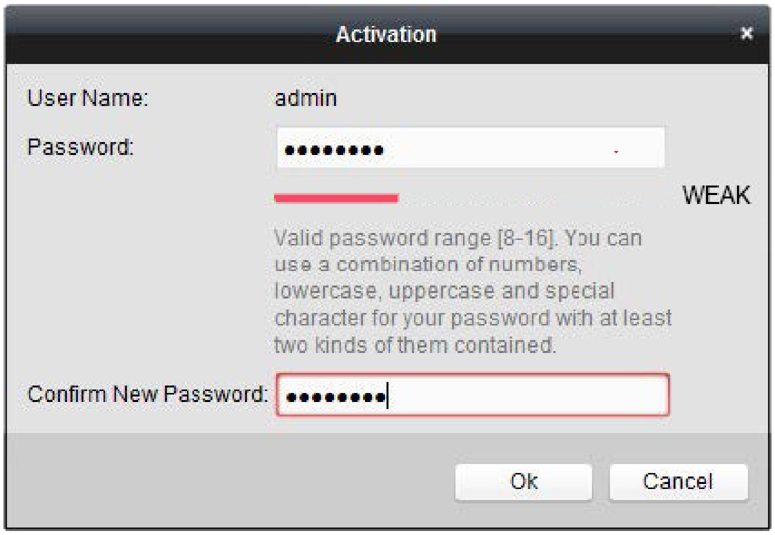
ATTENTION

Invalid Password

RISKY

Confirm New Password: ••••••••

Figure 30, Invalid Password Message



User Name: admin

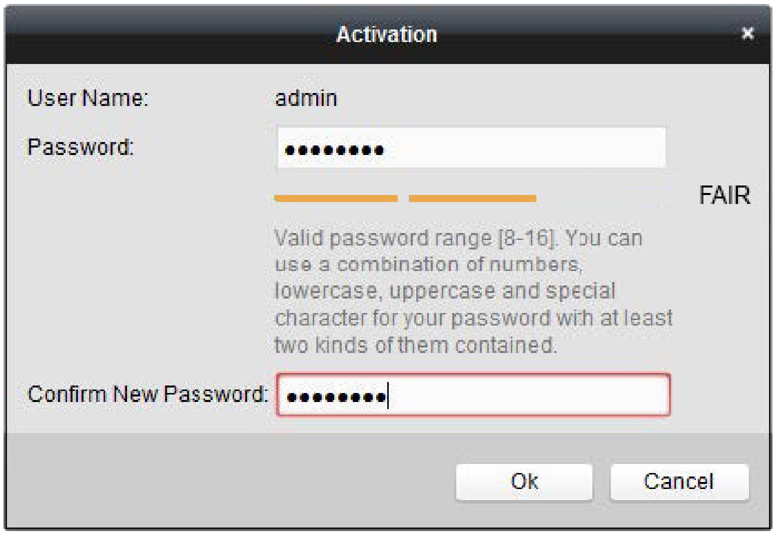
Password: •••••••••

WEAK

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

Confirm New Password: ••••••••

Figure 31, Level 1 Password Strength



User Name: admin

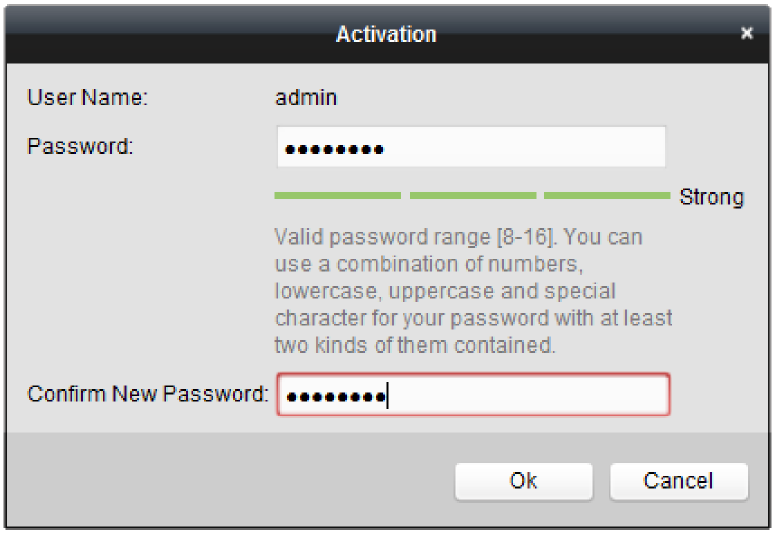
Password: •••••••••

FAIR

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

Confirm New Password: ••••••••

Figure 32, Level 2 Password Strength



User Name: admin

Password: ●●●●●●●● Strong

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

Confirm New Password: ●●●●●●●●

Figure 33, Level 3 and Level 4 Password Strength

WARNING

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

2.3.6 Adding an Online IP Camera

Purpose

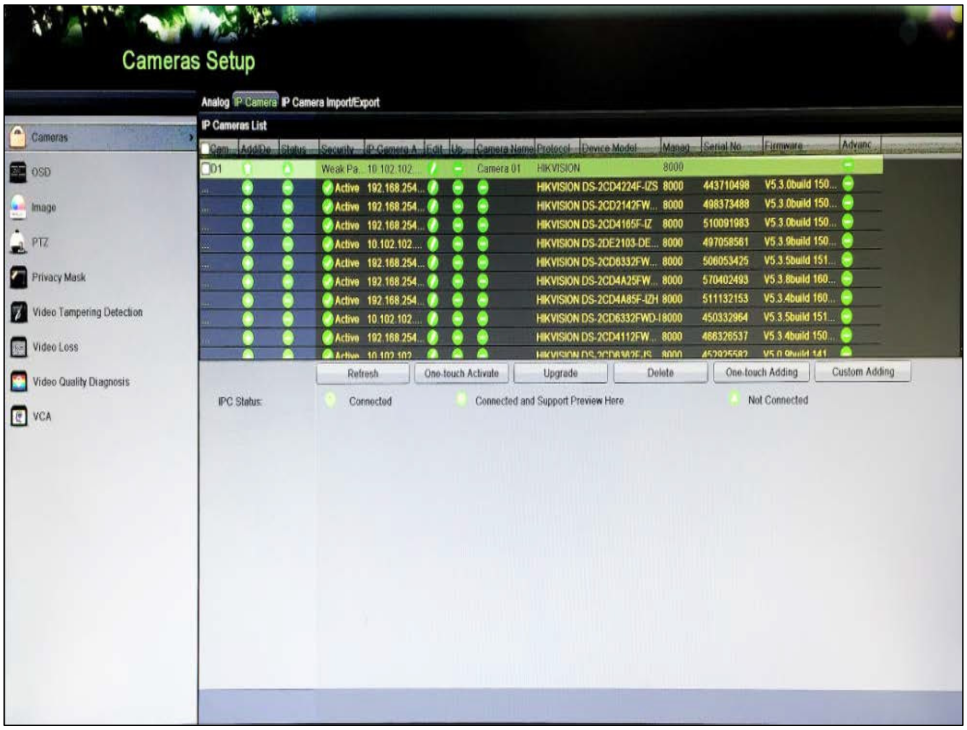
Before you can get a live view or record of the video, add the network cameras to the device's connection list.

Before You Start

Ensure the network connection is valid and correct.

- **OPTION 1**

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



□ Cam...	Add/De...	Status	Security	IP Camera A...	Edit	Up...	Camera Name	Protocol	Device Model	Manag...	Serial No.	Firmware	Advanc...
□D1	●	▲	Weak Pa...	10.102.102....	✎	●	Camera 01	HIKVISION		8000			●
...	●	●	✓ Active	192.168.254...	✎	●	●	HIKVISION	DS-2CD4224F-IZS	8000	443710498	V5.3.0build 150...	●
...	●	●	✓ Active	192.168.254...	✎	●	●	HIKVISION	DS-2CD2142FW...	8000	498373488	V5.3.0build 150...	●
...	●	●	✓ Active	192.168.254...	✎	●	●	HIKVISION	DS-2CD4165F-IZ	8000	510091983	V5.3.0build 150...	●
...	●	●	✓ Active	10.102.102....	✎	●	●	HIKVISION	DS-2DE2103-DE...	8000	497058561	V5.3.9build 150...	●
...	●	●	✓ Active	192.168.254...	✎	●	●	HIKVISION	DS-2CD6332FW...	8000	506053425	V5.3.5build 151...	●
...	●	●	✓ Active	192.168.254...	✎	●	●	HIKVISION	DS-2CD4A25FW...	8000	570402493	V5.3.8build 160...	●
...	●	●	✓ Active	192.168.254...	✎	●	●	HIKVISION	DS-2CD4A85F-IZH	8000	511132153	V5.3.4build 160...	●
...	●	●	✓ Active	10.102.102....	✎	●	●	HIKVISION	DS-2CD6332FWD-I	8000	450332964	V5.3.5build 151...	●
...	●	●	✓ Active	192.168.254...	✎	●	●	HIKVISION	DS-2CD4112FW...	8000	466326537	V5.3.4build 150...	●
...	●	●	✓ Active	10.102.102	✎	●	●	HIKVISION	DS-2CD8382F-IS	8000	452925582	V5.0.9build 141	●

Figure 34, IP Camera Management Interface

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

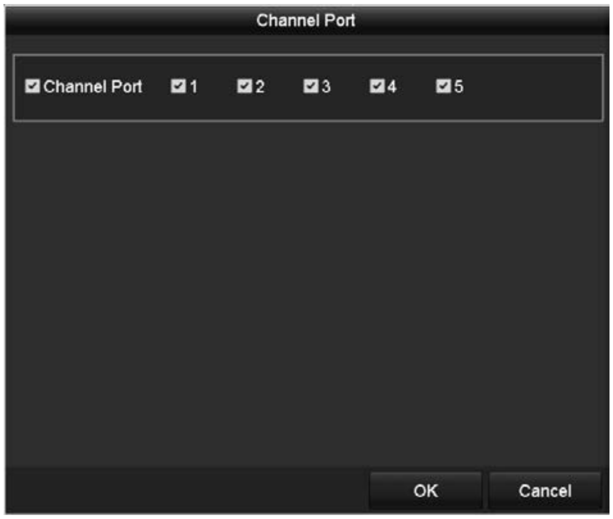
3. Select the IP camera from the list and click ⊕ to add the camera (with the same admin password of the DVR). Or you can click **One-touch Adding** to add all cameras (with the same admin password) from the list.

NOTE

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

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

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



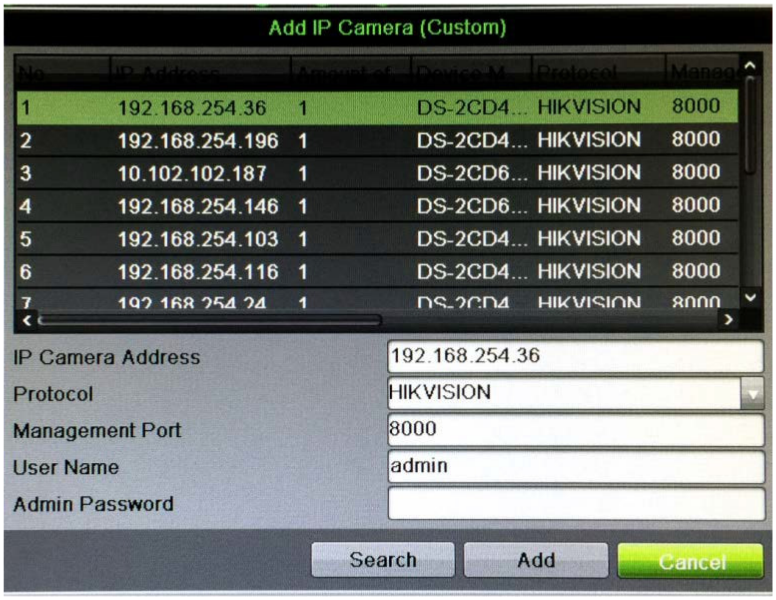
Channel Port

☑ Channel Port ☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5

Figure 35, Select Multiple Channels

- **OPTION 2**

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



Add IP Camera (Custom)

No.	IP Address	Amount of	Device M...	Protocol	Manage
1	192.168.254.36	1	DS-2CD4...	HIKVISION	8000
2	192.168.254.196	1	DS-2CD4...	HIKVISION	8000
3	10.102.102.187	1	DS-2CD6...	HIKVISION	8000
4	192.168.254.146	1	DS-2CD6...	HIKVISION	8000
5	192.168.254.103	1	DS-2CD4...	HIKVISION	8000
6	192.168.254.116	1	DS-2CD4...	HIKVISION	8000
7	192.168.254.24	1	DS-2CD4	HIKVISION	8000

IP Camera Address: 192.168.254.36
Protocol: HIKVISION
Management Port: 8000
User Name: admin
Admin Password:

Figure 36, Custom Adding IP Camera Interface

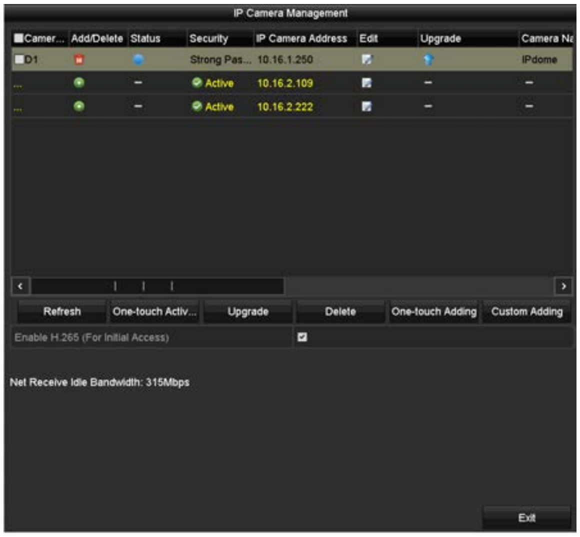
2. You can edit the IP address, protocol, management port, and other information of the IP camera to be added.

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


IP Camera Management

□Camer...	Add/Delete	Status	Security	IP Camera Address	Edit	Upgrade	Camera Na
□D1		●	Strong Pas...	10.16.1.250			IPdome
...	●	–	✓ Active	10.16.2.109		–	–
...	●	–	✓ Active	10.16.2.222		–	–

Enable H.265 (For Initial Access) ☑

Net Receive Idle Bandwidth: 315Mbps

Figure 37, Successfully Added IP Cameras

Table 1-7 Explanation of the Icons

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

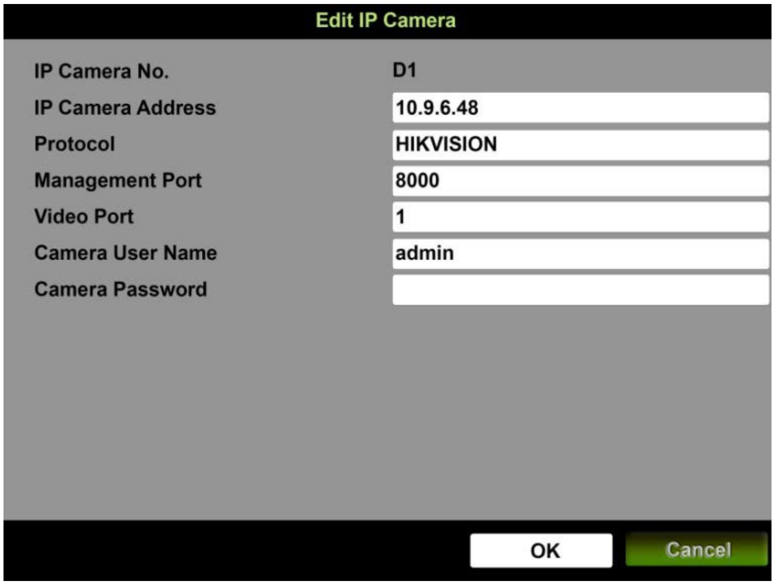
4. (Optional) Check the **Enable H.265** checkbox (For Initial Access) for the connected IP camera supporting H.265. Then the IP camera will be encoded with H.265.

2.3.7 Editing the Connected IP Camera

Purpose

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

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



Edit IP Camera

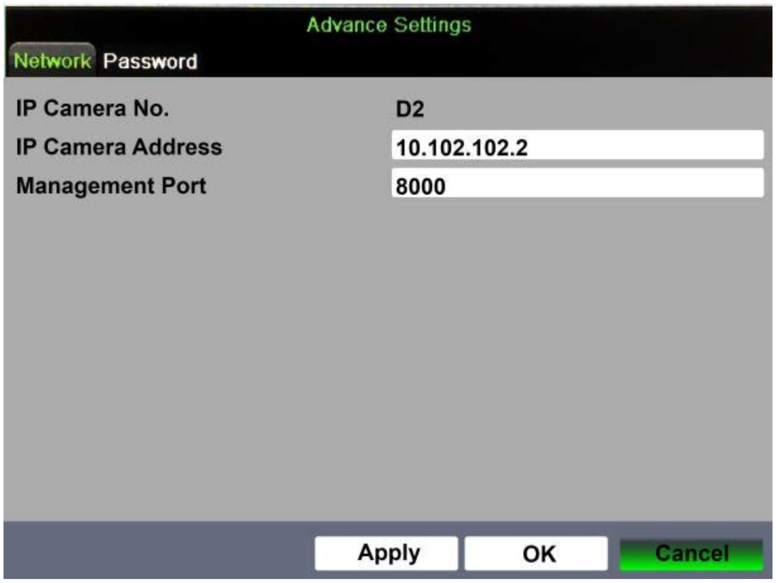
IP Camera No.	D1
IP Camera Address	10.9.6.48
Protocol	HIKVISION
Management Port	8000
Video Port	1
Camera User Name	admin
Camera Password	

Figure 38, Edit IP Camera

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

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

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



Advance Settings

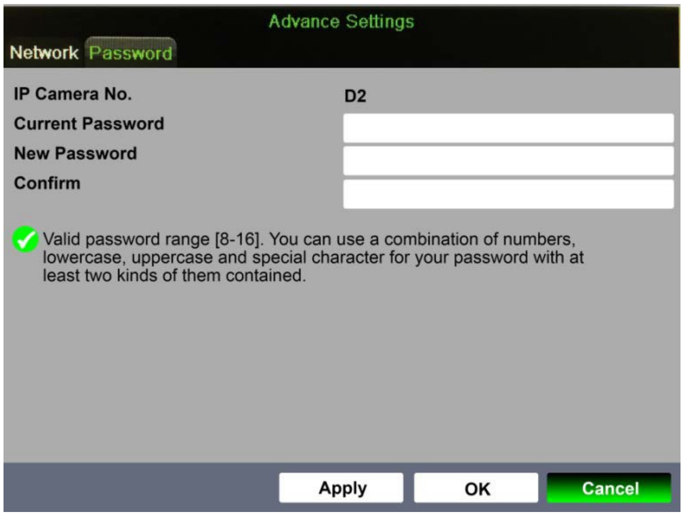
IP Camera No. D2

IP Camera Address 10.102.102.2

Management Port 8000

Figure 39, Network Configuration of the Camera

4. You can edit the camera network information and the password.



Advance Settings

IP Camera No. D2

Current Password

New Password

Confirm

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

Figure 40, Password Configuration of the Camera

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

2.3.8 Configuring Signal Input Channel

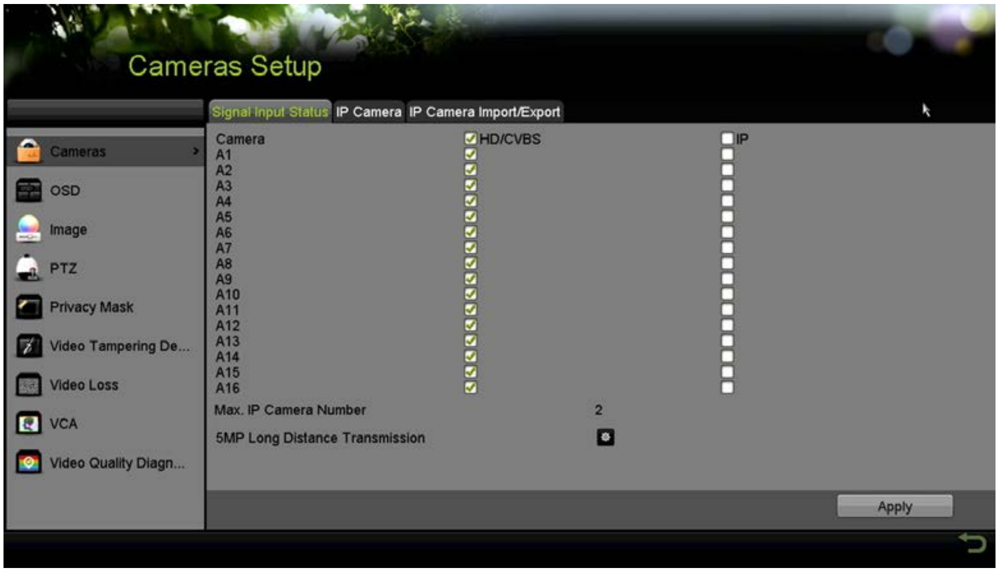
NOTE

This chapter is applicable only to DS-73xx/90xxHUI-K Series DVRs.

Purpose

You can configure the analog and IP signal input types and enable 5 MP long distance transmission.

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



Camera	☑ HD/CVBS	□ IP
A1	☑	□
A2	☑	□
A3	☑	□
A4	☑	□
A5	☑	□
A6	☑	□
A7	☑	□
A8	☑	□
A9	☑	□
A10	☑	□
A11	☑	□
A12	☑	□
A13	☑	□
A14	☑	□
A15	☑	□
A16	☑	□

Max. IP Camera Number: 2

5MP Long Distance Transmission

Figure 41, Signal Input Status

2. Check this checkbox to select different signal input types: HD/CVBS and IP. If you select HD/CVBS, four types of analog signal inputs including TurboHD and CVBS can be connected randomly for the selected channel. If you select IP, an IP camera can be connected to the selected channel.

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

   You can view the maximum number IP cameras in the **Max. IP Camera Number** text field. Disabling one analog channel will add one IP channel. For DS-73xxHUI-K4 Series and DS-73xxHQI-K4 Series DVRs, the accessible IP channels are X+2 (X refers to the disabled analog channel(s) of the DVR; maximum is 10 IP cameras). For DS-9008HUI-K8, the accessible IP channels are X+8 (X refers to the disabled analog channel(s) of the DVR; maximum is 16 IP cameras). For DS-9016HUI-K8, the accessible IP channels are X+16 (X refers to the disabled analog channel(s) of the DVR; maximum is 36 IP cameras).

2.3.9 Configuring 5 MP Long Distance Transmission

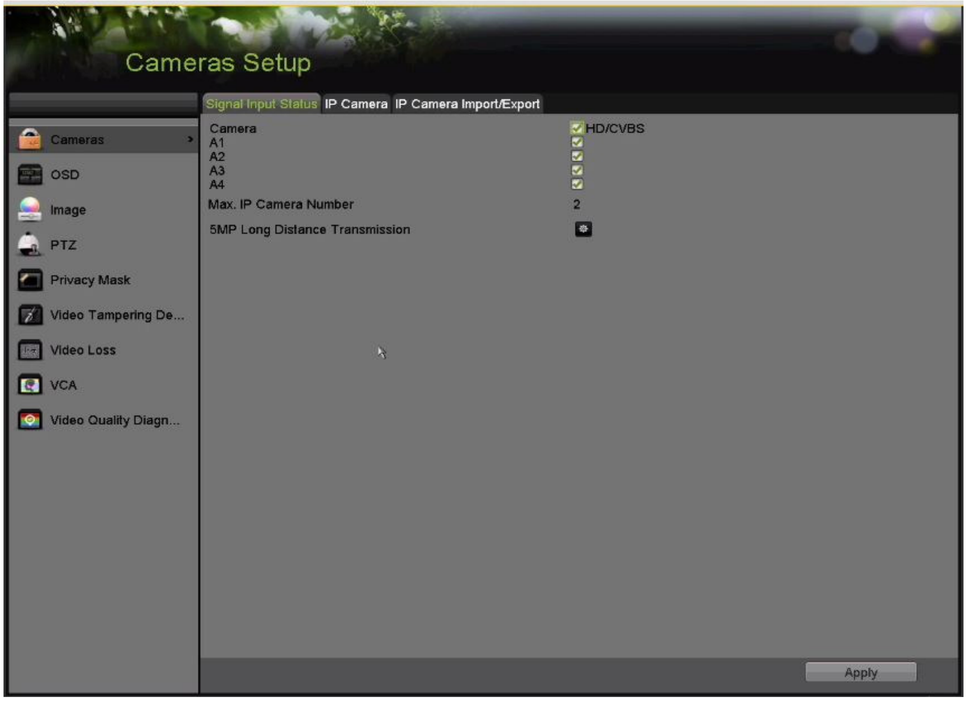
NOTE

This chapter is applicable only to HUI Series DVRs.

Purpose

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

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



Camera	☑ HD/CVBS
A1	☑
A2	☑
A3	☑
A4	☑
Max. IP Camera Number	2
5MP Long Distance Transmission	⚙

Figure 42, Signal Input Status (for DS-73xx/90xxHUI Series)

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

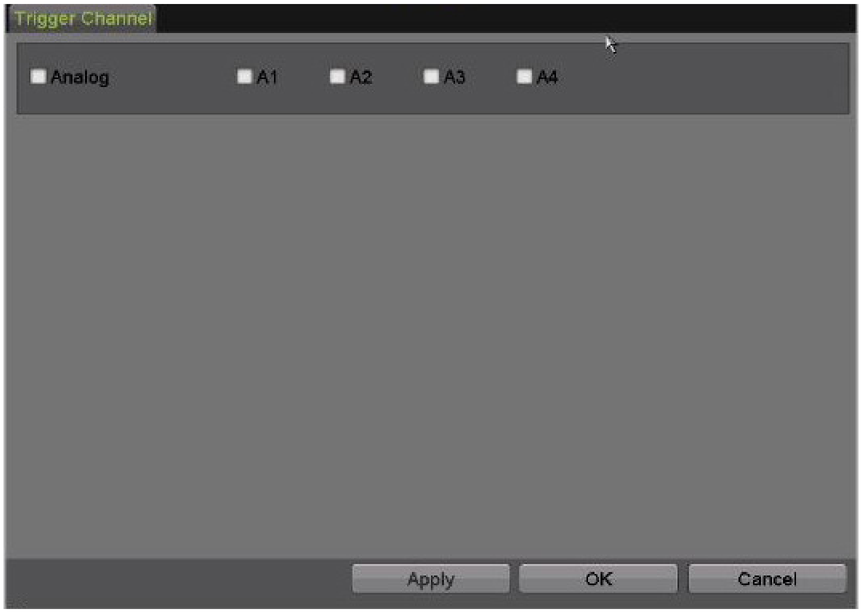


Figure 43, 5 MP Long Distance Transmission Settings

3. Check this checkbox to enable 5 MP Long Distance Transmission of the selected channel.

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

3 Live View

3.1 Introduction

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 multiple times (depending on which menu you're on) will bring you back to Live View mode.

3.2 Live View Icons

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

Table 1-8 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.

3.3 Live View Mode Operations

There are many functions provided in Live View mode. 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. You must set the dwell time for each screen on the configuration menu before enabling the auto-switch. Menu > Configuration > Live View > Dwell Time.
- **Start Recording:** normal record and motion detection record are supported.
- **Output Mode:** set the output mode to Standard, Bright, Gentle, or Vivid.
- **Playback:** play back the recorded videos for the current day.
- **Aux/Main Monitor:** the DVR checks the output interface connections to define the main and auxiliary output interfaces. When the aux output is enabled, the main output cannot perform any operations; you can perform some basic operations on the Live View mode for the Aux output.

There are two HDMI interfaces. HDMI1 and VGA interfaces share simultaneous output. The priority level for the main and aux output is HDMI2 > VGA/HDMI1. The CVBS output only serves as the aux output or Live View output.

Table 1-9 Priorities of Outputs

S.N.	HDMI2	VGA/HDMI1	CVBS	Main output	Auxiliary output	For Live View Output Only
1	√	√	√ or ×	HDMI2	VGA/HDMI1	CVBS
2	√ or ×	×	√ or ×	HDMI2	CVBS	VGA/HDMI1
3	×	√	√ or ×	VGA/HDMI1	CVBS	HDMI2

For other DVRs with CVBS output, the VGA/HDMI output is the main output, and the CVBS output is the aux output.

Table 1-10 Priorities of Outputs

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

NOTE

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

3.3.1 Using the Mouse in Live View

Refer to Table 1-11 for the description of mouse operation in live view mode.

Table 1-11 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 the Enter button.

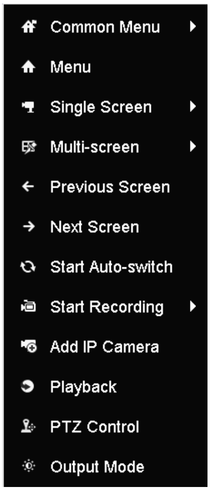


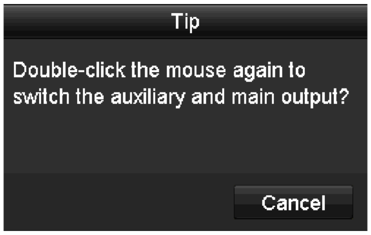
Figure 44, Right-click Menu

3.3.2 Switching Main/Aux Output

NOTE

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

1. Use the mouse wheel to double-click on the HDMI1/VGA, or HDMI2, or HDMI/VGA output screen, and the following message box pops up.



Tip

Double-click the mouse again to switch the auxiliary and main output?

Figure 45, Switch Main and Aux Output

2. Use the mouse wheel to double-click on the screen again to switch to the aux output, or click **Cancel** to cancel the operation.

3. Select the **Menu Output Mode** to others from the right-click menu on the monitor.

4. On the pop-up message box, click **Yes** to reboot the device to enable the selected menu output as the main output.

NOTE

You can select the **Menu Output Mode** under Menu > Configuration > General > More Settings to **Auto**, **HDMI1/VGA** and **HDMI2** and then reboot the device to switch the main output.

3.3.3 Quick Setting Toolbar in Live View Mode

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

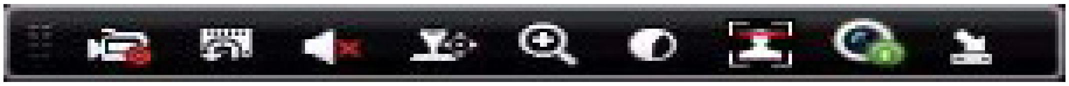


Figure 46, Quick Setting Toolbar

Refer to Table below for description of the Quick Setting Toolbar icons.

Table 1-12 Description of Quick Setting Toolbar Icons

Icons	Description	Icons	Description	Icons	Description
🎥	**Start/Stop Manual Recording**	↺	**Instant Playback**	🔇	**Audio On/Mute**
✥	**PTZ Control**	🔍	**Digital Zoom**	◐	**Image Settings**
⇲	**Close Live View**	⛶	**Face Detection**	ⓘ	**Information**
📷	**Capture**	⚙	**Live View Strategy**	◉	**Fisheye**

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

🔍 Digital Zoom zooms in the live image. You can zoom in the image to different proportions (1 to 16x) by moving the sliding bar. You can also scroll the mouse wheel to control the zoom in/out.

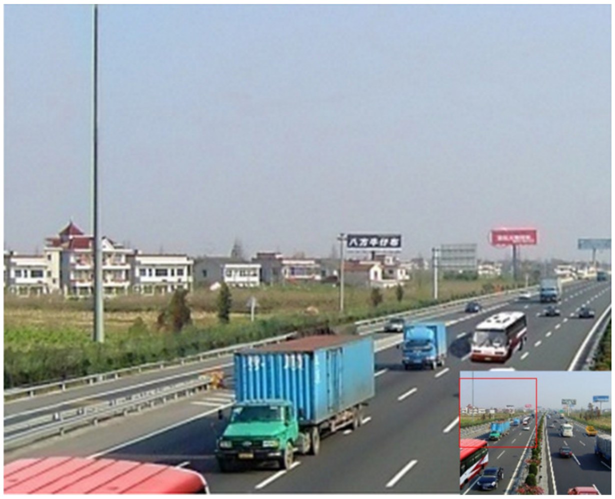


Figure 47, Digital Zoom

Image Settings icon enters the Image Settings menu. Drag the mouse or click to adjust the image parameters, including brightness, contrast, and saturation.

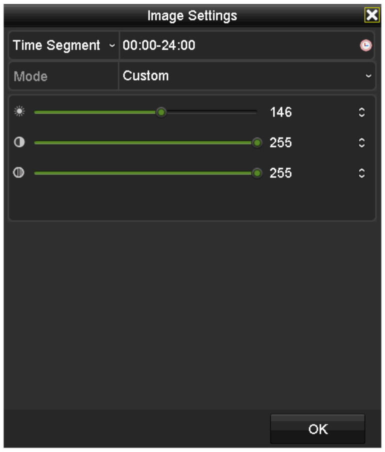


Image Settings

Time Segment: 00:00-24:00

Mode: Custom

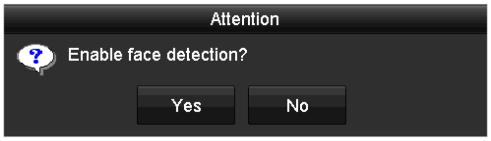
146

255

255

Figure 48, Image Settings

Enable Face Detection by clicking 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 full-screen mode. You can configure face detection only when it is supported by the connected camera.

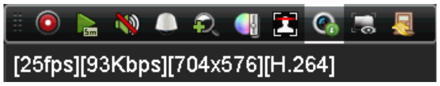


Attention

Enable face detection?

Figure 49, Enable Face Detection

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



[25fps][93Kbps][704x576][H.264]

Figure 50, 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 IP camera supporting H.265 is connected, the stream type is displayed as H.265. When IP camera supporting H.265+ is connected, the stream type is displayed as H.265+.

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

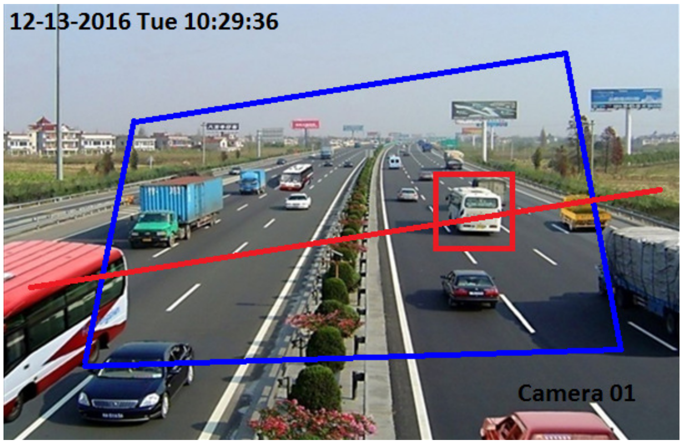


Figure 51, Enable VCA Information Overlay

NOTE

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

Enable VCA function first before showing the VCA information.

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

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

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

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

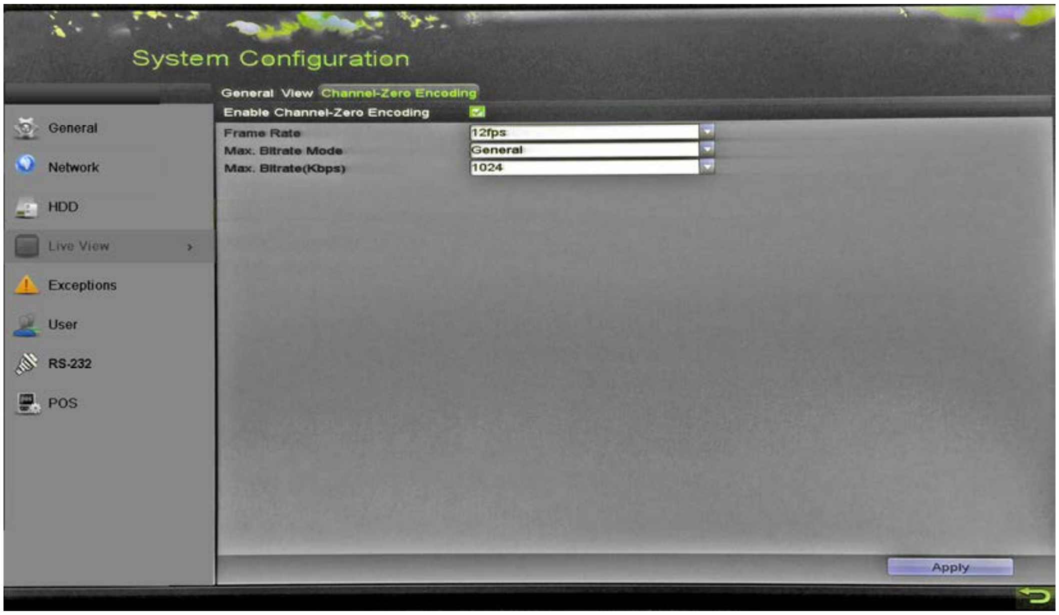
For analog cameras, if the camera number does not exceed the limit for line crossing detection and intrusion detection, the VCA information overlay can be enabled for all the analog cameras' enabled line crossing detection and intrusion detection. If the camera number exceeds the limit for line crossing 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.

3.4 Channel-Zero Encoding

Purpose

Channel-Zero Encoding provides a way to view many channels in real time from a Web browser or CMS (Client Management System) software by decreasing the bandwidth requirement without affecting the image quality.

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



System Configuration

Enable Channel-Zero Encoding ☑

Frame Rate: 12fps

Max. Bitrate Mode: General

Max. Bitrate(Kbps): 1024

Figure 52, Live View Channel-Zero Encoding

2. Check the Enable Channel-Zero Encoding checkbox.

3. Configure the Frame Rate, Max. Bitrate Mode, and Max. Bitrate.

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

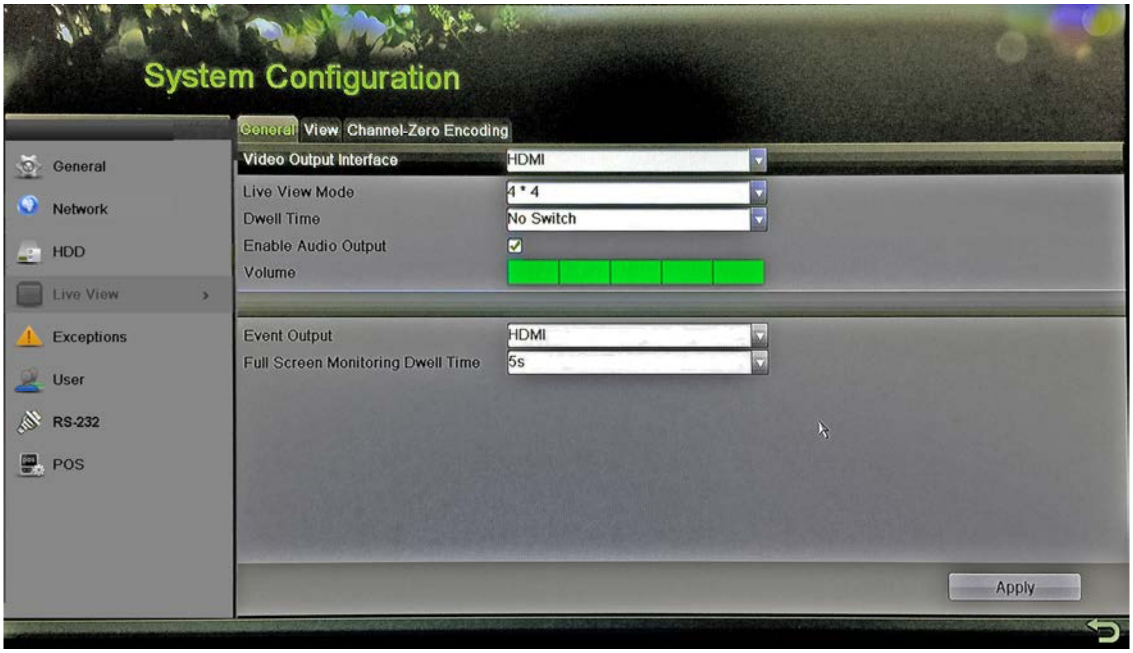
5. After you set the Channel-Zero encoding, you can view 16 channels in one screen in the remote client or Web browser.

3.5 Adjusting Live View Settings

Purpose

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

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



Video Output Interface: HDMI
Live View Mode: 4 * 4
Dwell Time: No Switch
Enable Audio Output: ☑
Volume: 🟩🟩🟩🟩🟩
Event Output: HDMI
Full Screen Monitoring Dwell Time: 5s

Figure 53, Live View General

2. The settings available in this menu include:

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

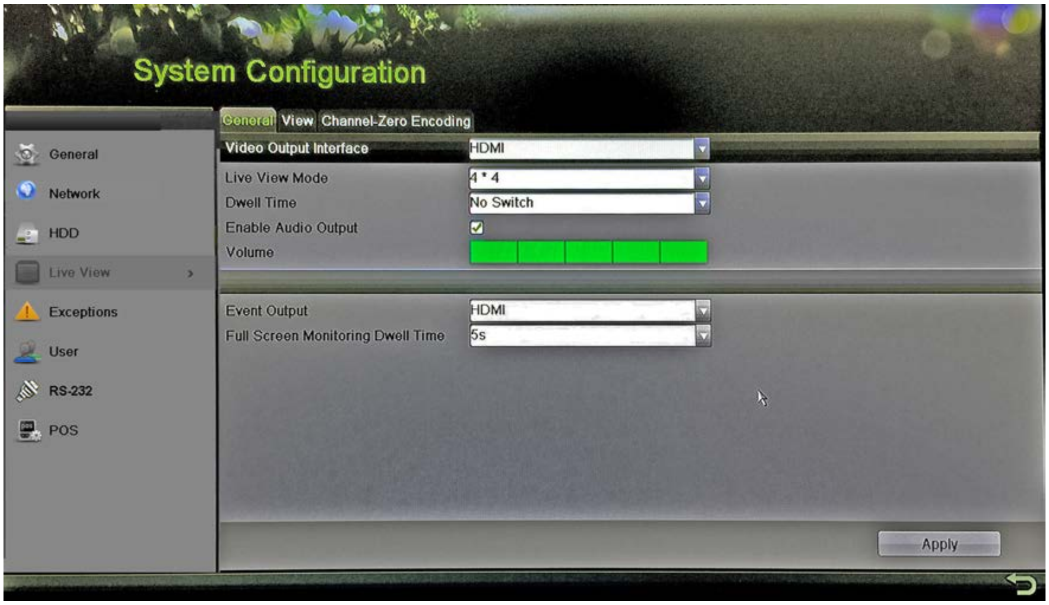
3. You can select **VGA/HDMI1**, **HDMI2**, **Main CVBS** for video output interface.

- **Live View Mode:** Selects the display mode to be used for Live View.
- **Dwell Time:** The time in seconds to *dwell* between switching of channels when enabling auto-switch in Live View.
- **Enable Audio Output:** Enables/disables audio output for the selected camera in Live View mode.
- **Volume:** Adjusts the audio output volume.
- **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 the alarm event screen.

4. Set the camera order.

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



System Configuration

General | View | Channel-Zero Encoding

Video Output Interface	HDMI
Live View Mode	4 * 4
Dwell Time	No Switch
Enable Audio Output	☑
Volume	🟩🟩🟩🟩🟩
Event Output	HDMI
Full Screen Monitoring Dwell Time	5s

Apply

Figure 54, Live View Camera Order

   2) Click a window to select **it**, then double-click a camera to display in the camera list. 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**.

NOTE

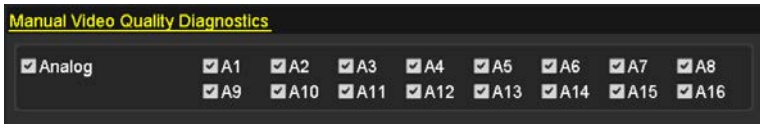
If the sum of the analog and IP channels exceeds 25, up to 32-window division mode is supported for the VGA/HDMI1 output.

3.6 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.



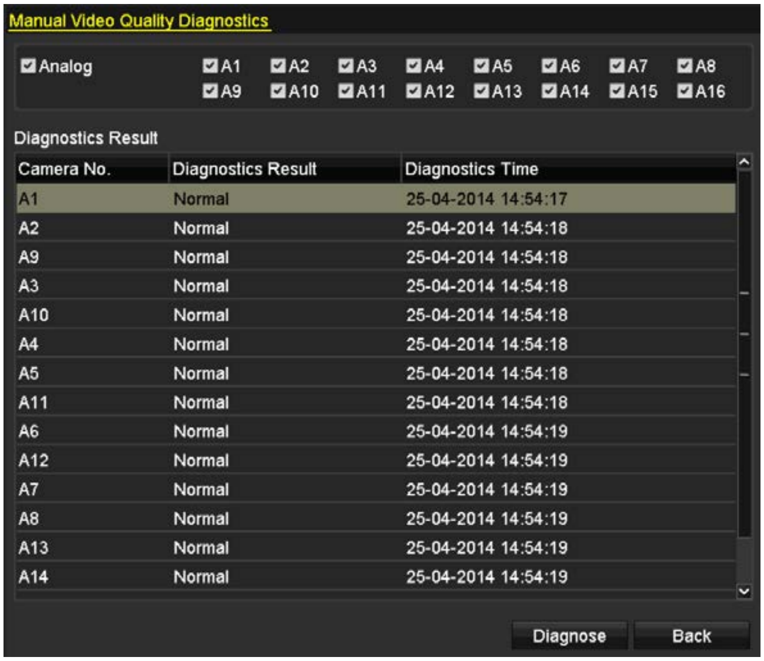
Manual Video Quality Diagnostics

☑ Analog ☑ A1 ☑ A2 ☑ A3 ☑ A4 ☑ A5 ☑ A6 ☑ A7 ☑ A8
☑ A9 ☑ A10 ☑ A11 ☑ A12 ☑ A13 ☑ A14 ☑ A15 ☑ A16

Figure 55, Video Quality Diagnostics

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

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



Manual Video Quality Diagnostics

☑ Analog ☑ A1 ☑ A2 ☑ A3 ☑ A4 ☑ A5 ☑ A6 ☑ A7 ☑ A8
☑ A9 ☑ A10 ☑ A11 ☑ A12 ☑ A13 ☑ A14 ☑ A15 ☑ A16

Diagnostics Result

Camera No.	Diagnostics Result	Diagnostics Time
A1	Normal	25-04-2014 14:54:17
A2	Normal	25-04-2014 14:54:18
A9	Normal	25-04-2014 14:54:18
A3	Normal	25-04-2014 14:54:18
A10	Normal	25-04-2014 14:54:18
A4	Normal	25-04-2014 14:54:18
A5	Normal	25-04-2014 14:54:18
A11	Normal	25-04-2014 14:54:18
A6	Normal	25-04-2014 14:54:19
A12	Normal	25-04-2014 14:54:19
A7	Normal	25-04-2014 14:54:19
A8	Normal	25-04-2014 14:54:19
A13	Normal	25-04-2014 14:54:19
A14	Normal	25-04-2014 14:54:19

Figure 56, 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.

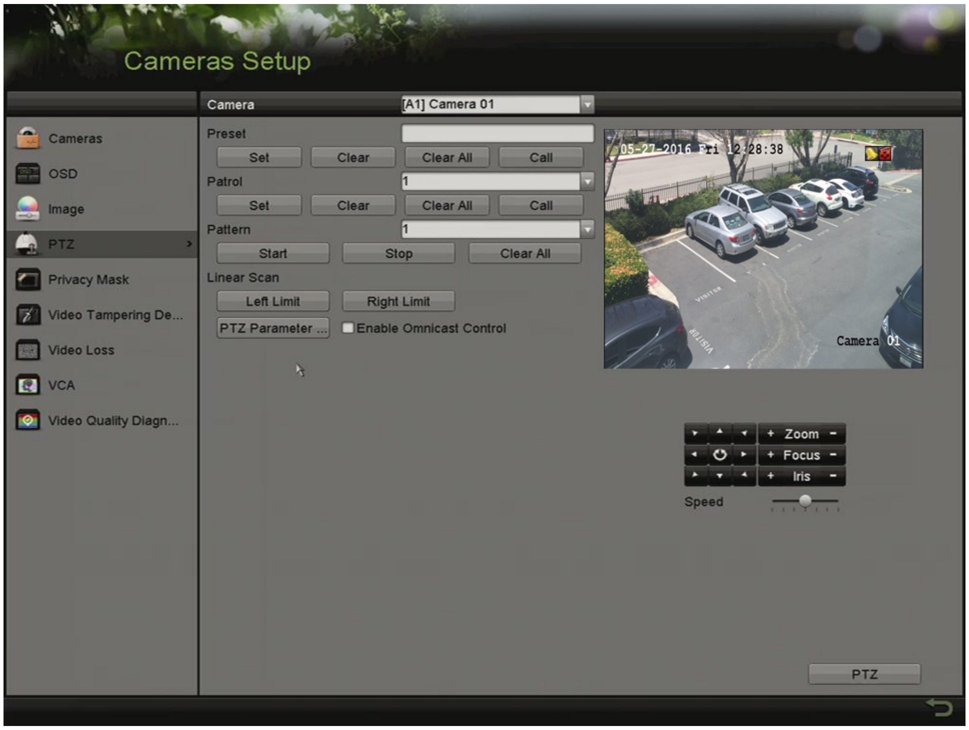
4 PTZ Controls

4.1 Configuring PTZ Settings

Purpose

Follow the following procedure to set PTZ parameters. Configure PTZ parameters before you control the PTZ camera.

1. Go to Menu > Camera > PTZ.



Camera: [A1] Camera 01

Preset

Patrol: 1

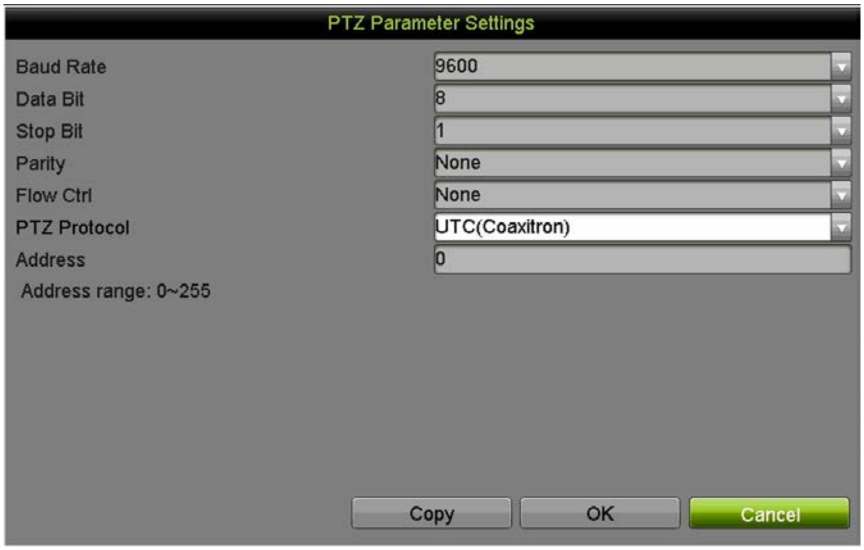
Pattern: 1

Linear Scan

Figure 57, PTZ Settings

2. Select the camera for PTZ setting in the **Camera** drop-down list.

3. Click **PTZ Parameters** to set the PTZ parameters.



PTZ Parameter Settings

Baud Rate: 9600

Data Bit: 8

Stop Bit: 1

Parity: None

Flow Ctrl: None

PTZ Protocol: UTC(Coaxitron)

Address: 0

Address range: 0~255

Figure 58, PTZ General

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

NOTE

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

For UTC cameras/domes connected, you can select the PTZ protocol to UTC. Make sure the protocol selected here is supported by the connected camera/dome.

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

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

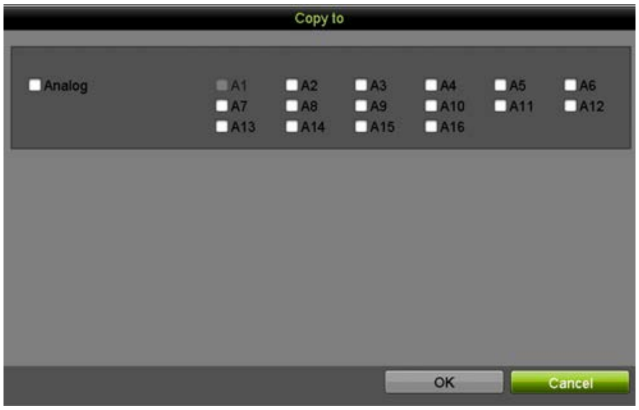


Figure 59, Copy to Other Channels

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

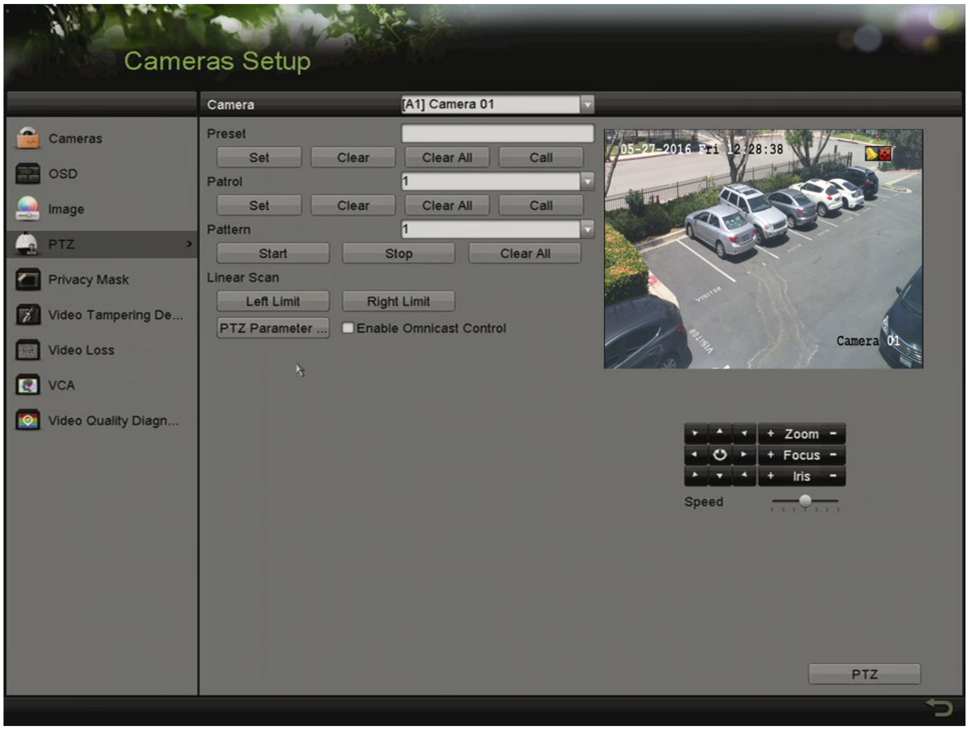
Ensure that the presets, patrols, and patterns are supported by PTZ protocols.

4.2.1 Customizing Presets

Purpose

Follow the steps below to set the preset location you want the PTZ camera to point to when an event occurs.

1. Go to Menu > Camera > PTZ.



Camera [A1] Camera 01

Preset

Patrol 1

Pattern 1

Linear Scan

□Enable Omnicast Control

Figure 60, PTZ Settings

2. Use the directional button to position the camera to the location you want to set the preset. The zoom and focus operations can be recorded in the preset as well.

3. Enter the preset No. (1 to 255) in the preset text field, and click Set to link the location to the preset.

4. Repeat steps 2 and 3 to save more presets.

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

4.2.2 Calling Presets

Purpose

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

1. Click **PTZ** in the lower-right corner of the PTZ setting 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. Choose C**amera** in the drop-down list.

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

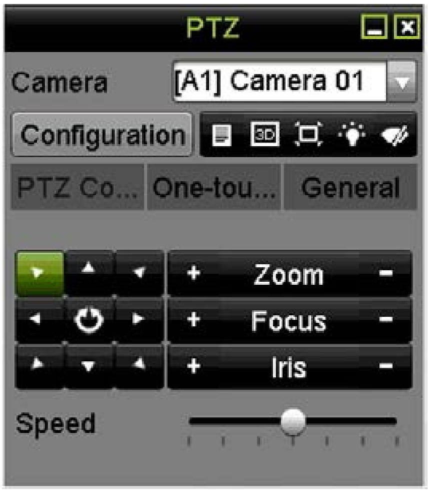


Figure 61, PTZ Panel General

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

5. Click **Call Preset** to call it.

NOTE

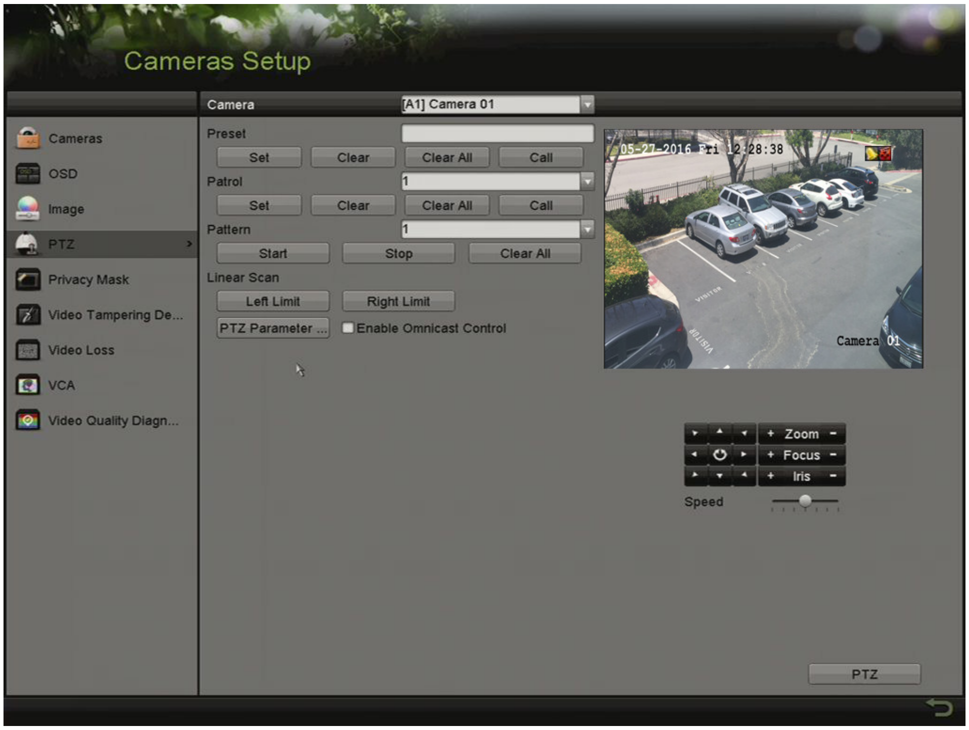
When the camera/dome connected and the PTZ protocol is set to UTC, you can call preset 95 to enter the menu of the connected camera/dome. Use the directional buttons on the PTZ control panel to operate the menu.

4.2.3 Customizing Patrols

Purpose

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

1. Go to Menu > Camera > PTZ.



Camera: [A1] Camera 01

Preset:

Patrol: 1

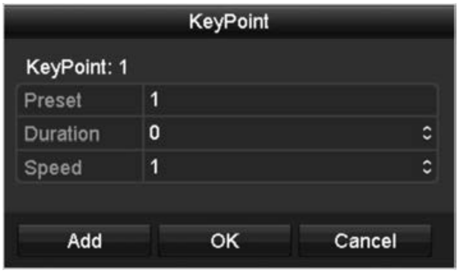
Pattern: 1

□ Enable Omnicast Control

Figure 62, PTZ Settings

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

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



KeyPoint: 1

Preset	1
Duration	0
Speed	1

Figure 63, Key point Configuration

4. Configure key point parameters such as the key point No., duration to stay at one key point, and patrol speed. The key point corresponds to the preset. The **Key Point No.** determines the order the PTZ will follow while cycling through the patrol. **Duration** refers to the time span to stay at the corresponding key point. **Speed** defines the speed 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.

6. 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 Patrols

Purpose

Calling a patrol moves the PTZ 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 PTZ controls general settings.

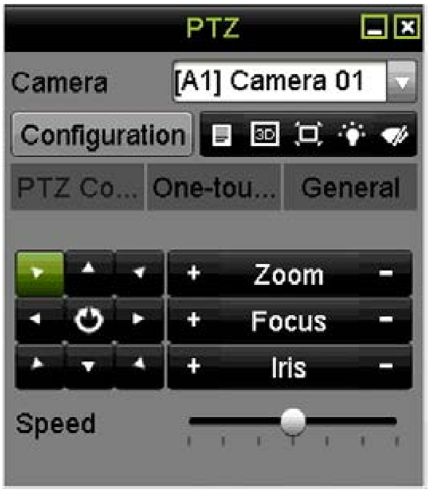


Figure 64, PTZ Panel General

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

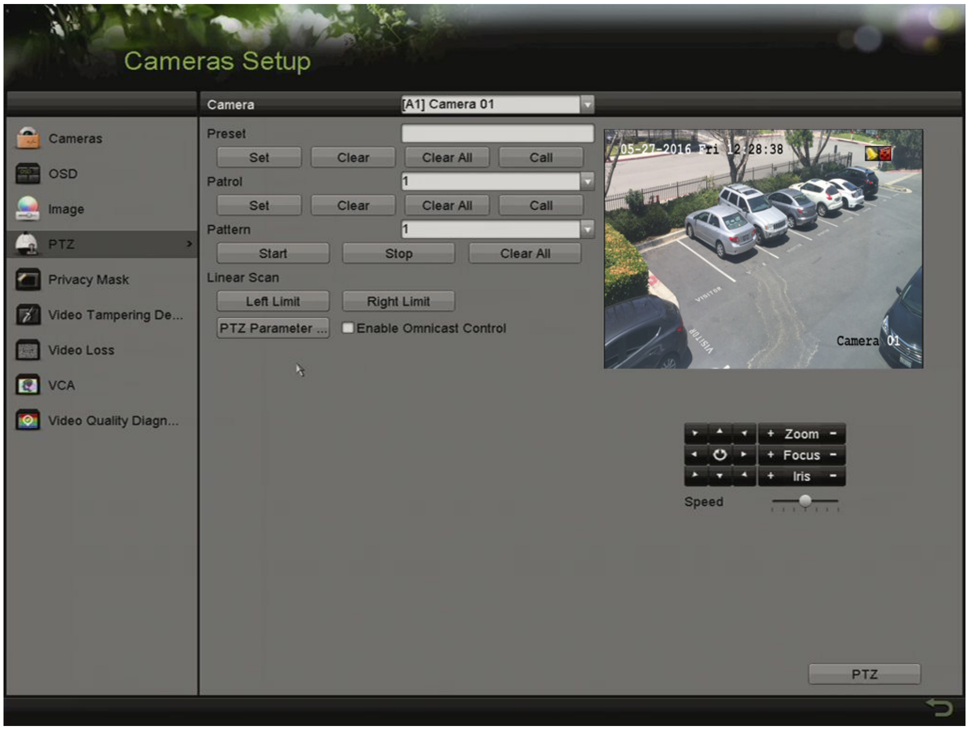
4. You can click **Stop Patrol** to stop calling it.

4.2.5 Customizing Patterns

Purpose

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

1. Go to Menu > Camera > PTZ.



Camera: [A1] Camera 01

Patrol: 1

Pattern: 1

Figure 65, 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. Click **Stop** to stop movement.

4. The movement of the PTZ is recorded as the pattern.

4.2.6 Calling Patterns

Purpose

Follow the procedure below 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.

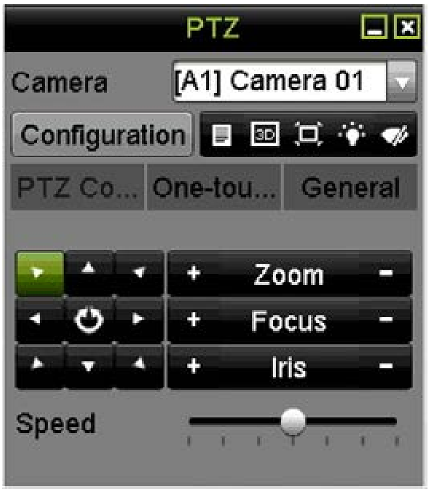


Figure 66, PTZ Panel General

3. Click **Call Pattern** to call it.

4. Click **Stop Pattern** to stop calling it.

4.2.7 Customizing Linear Scan Limit

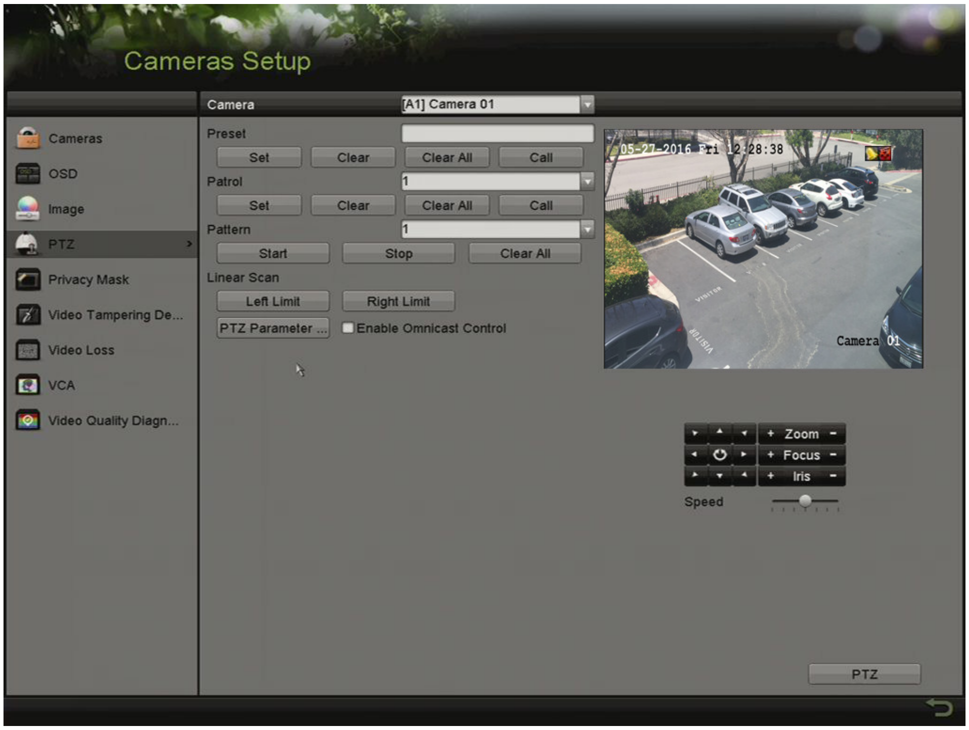
Purpose

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

NOTE

This function is supported only by certain models.

1. Go to Menu > Camera > PTZ.



Camera [A1] Camera 01

Patrol 1

Pattern 1

Figure 67, PTZ Settings

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

NOTE

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

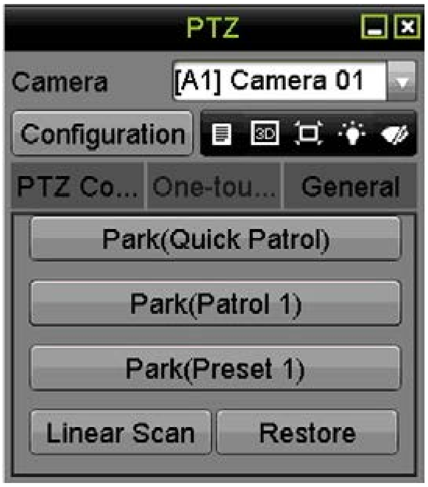
4.2.8 Calling Linear Scan

Purpose

Follow the following 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.



Camera [A1] Camera 01

Figure 68, 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 for settings to take effect.

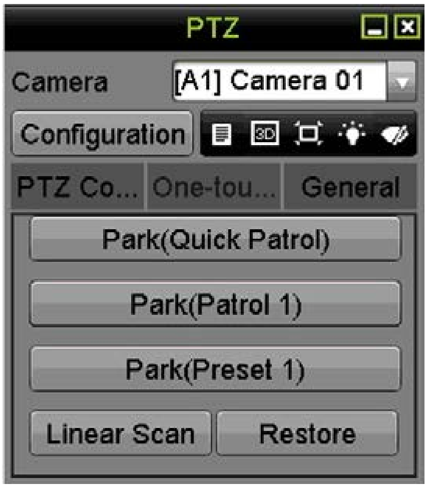
4.2.9 One-Touch Park

Purpose

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

1. 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 PTZ control's one-touch function.



Camera [A1] Camera 01

Figure 69, PTZ Panel One-touch

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

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

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

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

NOTE

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

7. 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 **PTZ Control** on the front panel or on 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.

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.

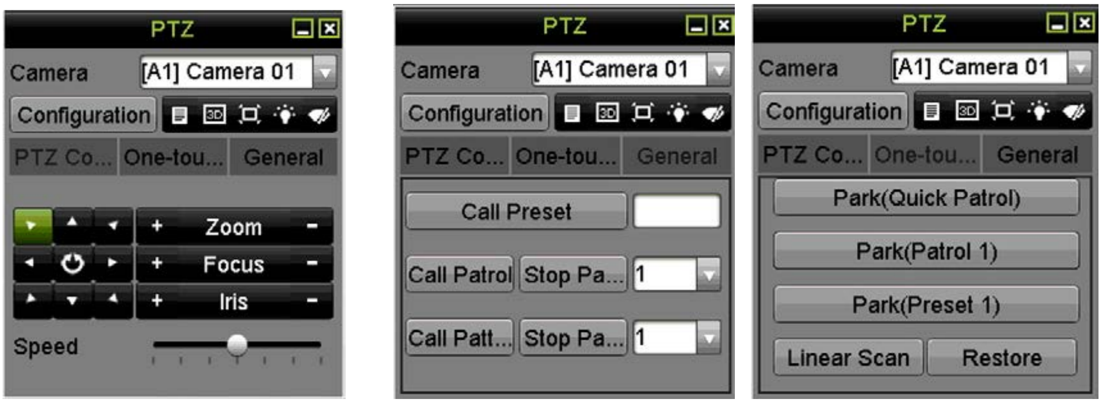


Figure 70, PTZ Control Panel

Refer to Table 1-13 for description of the PTZ panel icons.

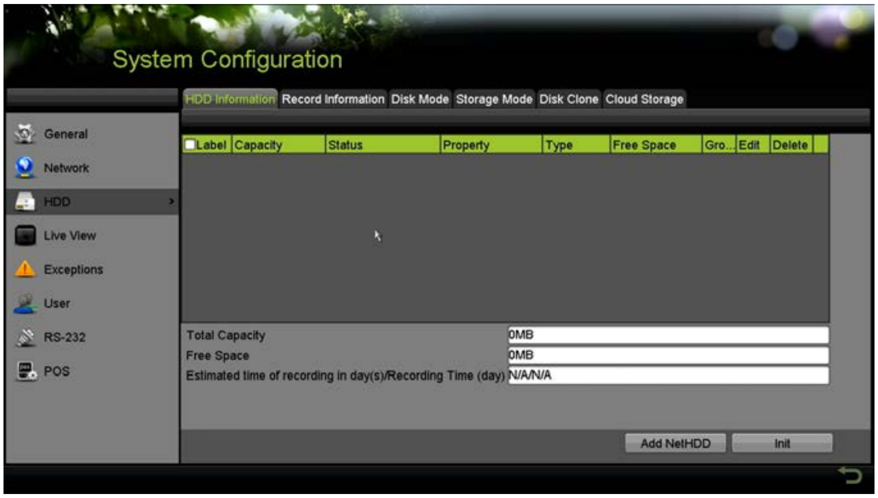
Table 1-13 Description of the PTZ Panel Icons

Icon	Description	Icon	Description	Icon	Description
▲▼◀▶ ↻	Direction button and the auto-cycle button	+	Zoom+, Focus+, Iris+	−	Zoom-, Focus-, Iris-
—●—	The PTZ movement speed	💡	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		

5 Recording and Capture Settings

5.1 Configuring Encoding Parameters

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



□Label	Capacity	Status	Property	Type	Free Space	Gro...	Edit	Delete

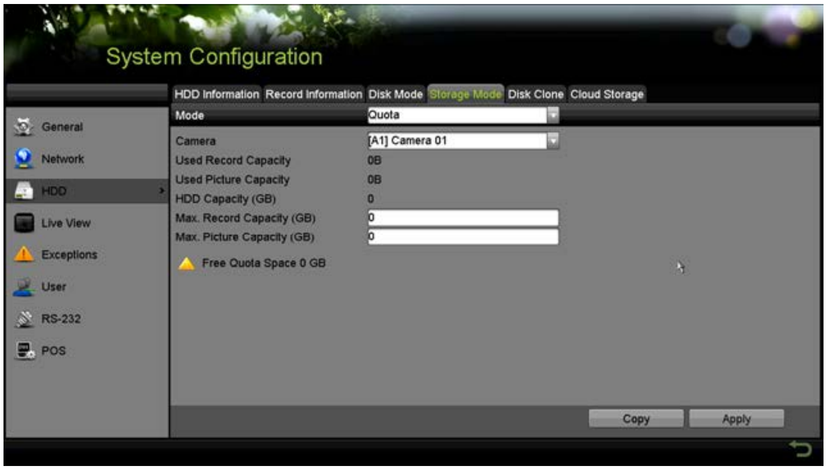
Total Capacity: 0MB
Free Space: 0MB
Estimated time of recording in day(s)/Recording Time (day): N/A/N/A

Figure 71, HDD

2. Click **Advanced** tab to check the HDD storage mode (Menu > HDD > Storage Mode).

    1) If the HDD mode is Quota, set the maximum record capacity.

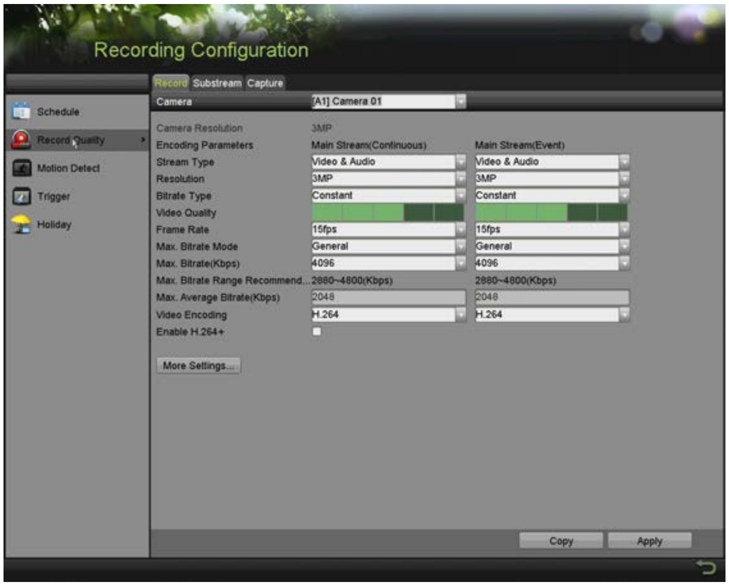
    2) If the HDD mode is Group, set the HDD group.



Mode: Quota
Camera: [A1] Camera 01
Used Record Capacity: 0B
Used Picture Capacity: 0B
HDD Capacity (GB): 0
Max. Record Capacity (GB): 0
Max. Picture Capacity (GB): 0
Free Quota Space 0 GB

Figure 72, HDD – Storage Mode

3. Go to Menu > Record Information > Parameters.



Camera	[A1] Camera 01	
Camera Resolution	3MP	
Encoding Parameters	Main Stream(Continuous)	Main Stream(Event)
Stream Type	Video & Audio	Video & Audio
Resolution	3MP	3MP
Bitrate Type	Constant	Constant
Video Quality		
Frame Rate	15fps	15fps
Max. Bitrate Mode	General	General
Max. Bitrate(Kbps)	4096	4096
Max. Bitrate Range Recommend...	2880~4800(Kbps)	2880~4800(Kbps)
Max. Average Bitrate(Kbps)	2048	2048
Video Encoding	H.264	H.264
Enable H.264+	□	

Figure 73, Record Parameters

4. 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.

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

HUI Series DVRs support 5 MP and 4 MP resolution on all channels.

The analog signal inputs (TurboHD CVBS) and IP signal input is recognized and connect automatically.

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

Refer to the *Appendix-Specifications* for the supported resolutions by model.

- **Bitrate Type:** Set the bitrate type to be Variable or Constant.

- **Video Quality**: Set the video quality of recording, with six levels configurable.

NOTE

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

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

NOTE

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

The minimum frame rate for main stream is 1 fps.

- **Max. Bitrate Mode:** Set the mode to General or Custom.

- **Max Bitrate (Kbps):** Select or customize the maximum bit rate for recording.

- **Max. Bitrate Range Recommended:** A recommended max. bit rate range is provided for reference.

- **Max. Average Bitrate (Kbps):** Set the max. average bit rate, which refers to the average amount of data transferred per unit of time.

- **Video Encoding:** You can configure H.264 or H.265 for the main stream (continuous) of IP and analog cameras. Check the **Enable H.264+** or **Enable H.265+** checkbox to enable this function. Enabling it helps to ensure high video quality with a lowered bitrate.

NOTE

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

The analog and IP cameras support enabling H.264+/H.265+ if the video encoding is H.264/H.265 for the main stream.

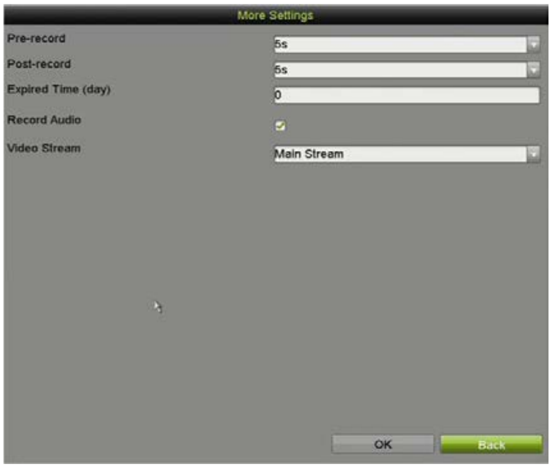
After enabling H.264+ or H.265+, the **Bitrate Type**, **Video Quality**, **Max. Bitrate Mode**, **Max. Bitrate (Kbps),** and **Max. Bitrate Range Recommend** are not configurable.

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

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

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

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


More Settings

Pre-record: 5s

Post-record: 5s

Expired Time (day): 0

Record Audio: ☑

Video Stream: Main Stream

Figure 74, More Settings of Record Parameters (Quota Mode Shown)

- **Pre-record:** The amount of time to record before the scheduled time or event. For example, if an alarm triggers recording at 10:00, if the pre-record time is 5 seconds, the camera starts recording at 9:59:55.

- **Post-record:** The time to record after the event or scheduled time. For example, if an alarm recording ends at 11:00, if the post-record time is 5 seconds, it records until 11:00:05.

- **Expired Time:** The time to keep the record files in the HDDs. Once this time is exceeded, the files will be deleted. The files will be saved permanently if the value is set to “0.” The actual retention time for the files should be determined by the HDDs capacity.

- **Redundant Record:** Enabling redundant record means records will be saved in the redundant HDD.

- **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. Sub-stream records for a longer time in the same storage space.

NOTE

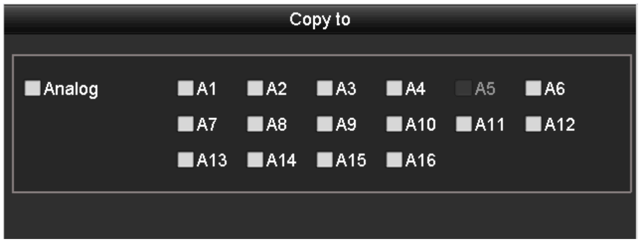
Redundant Record is available only when the HDD mode is *Group.*

A redundant HDD is required for the redundant record function.

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

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

8. Optionally, click **Copy** to copy the settings to other analog channels if needed.



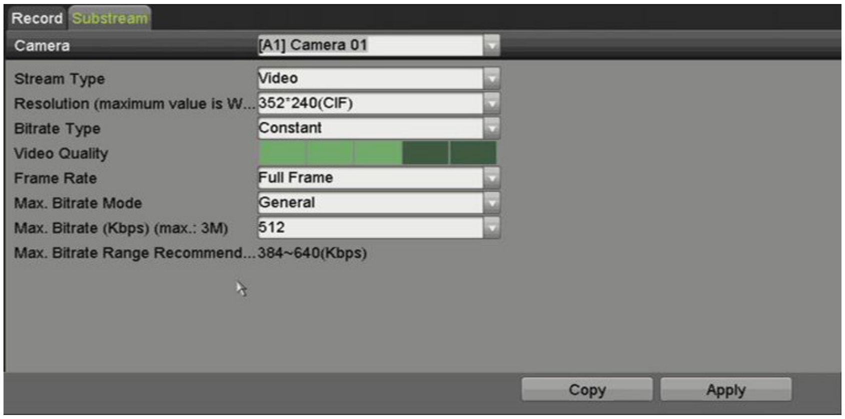
Copy to

☐ Analog ☐ A1 ☐ A2 ☐ A3 ☐ A4 A5 ☐ A6
☐ A7 ☐ A8 ☐ A9 ☐ A10 ☐ A11 ☐ A12
☐ A13 ☐ A14 ☐ A15 ☐ A16

Figure 75, Copy Camera Settings

9. Set encoding parameters for sub-stream.

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



Camera	[A1] Camera 01
Stream Type	Video
Resolution (maximum value is W...	352*240(CIF)
Bitrate Type	Constant
Video Quality	
Frame Rate	Full Frame
Max. Bitrate Mode	General
Max. Bitrate (Kbps) (max.: 3M)	512
Max. Bitrate Range Recommend...	384~640(Kbps)

Figure 76, 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

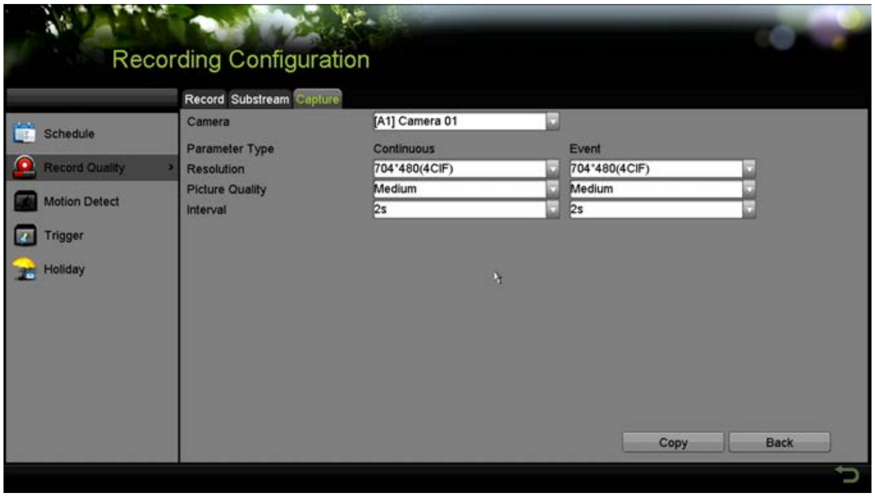
The sub-stream resolution can be selected among WD1, 4CIF, and CIF.

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

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

10. Set parameters for capture.

   1) Select the **Capture** tab.



Camera	[A1] Camera 01	
Parameter Type	Continuous	Event
Resolution	704*480(4CIF)	704*480(4CIF)
Picture Quality	Medium	Medium
Interval	2s	2s

Figure 77, Capture Settings

2) Select a camera from the 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 interval is the time period between two capturing actions. You can configure all the parameters on this menu upon demand.

5.2 Configuring Recording and Capture Schedule

NOTE

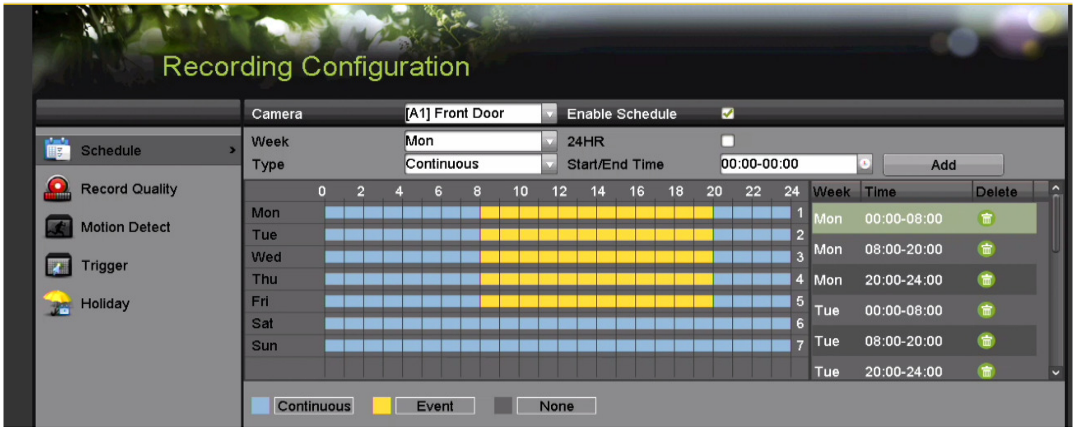
The DVR supports continuous, alarm, motion, motion | alarm, motion & alarm, event, and POS triggered recording types.

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

Purpose

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

1. Go to Menu > Record/Capture > Schedule.



Camera: [A1] Front Door
Enable Schedule: ☑
Week: Mon
24HR: □
Type: Continuous
Start/End Time: 00:00-00:00

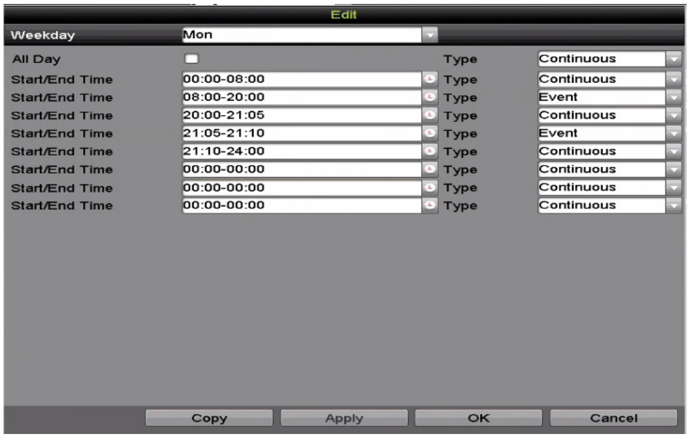
Week	Time	Delete
Mon	00:00-08:00	🗑
Mon	08:00-20:00	🗑
Mon	20:00-24:00	🗑
Tue	00:00-08:00	🗑
Tue	08:00-20:00	🗑
Tue	20:00-24:00	🗑

Figure 78, Record Schedule

Different recording types are marked in different color icons.

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

2. Choose the camera you want to configure in the **Camera** drop-down list.
3. Check the **Enable Schedule** checkbox.
4. Configure the record schedule.
5. Edit the schedule
    1) Click **Edit**.
    2) Choose the day you want to set the schedule in the message box.
    3) To schedule all-day recording, check the **All Day** item checkbox.

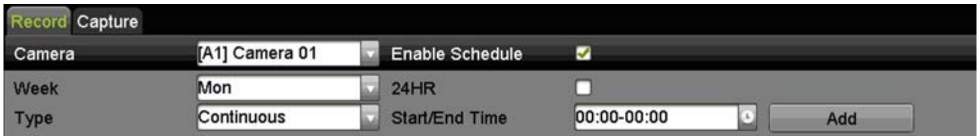


Weekday: Mon

All Day	□	Type	Continuous
Start/End Time	00:00-08:00	Type	Continuous
Start/End Time	08:00-20:00	Type	Event
Start/End Time	20:00-21:05	Type	Continuous
Start/End Time	21:05-21:10	Type	Event
Start/End Time	21:10-24:00	Type	Continuous
Start/End Time	00:00-00:00	Type	Continuous
Start/End Time	00:00-00:00	Type	Continuous
Start/End Time	00:00-00:00	Type	Continuous

Figure 79, Edit Schedule – All Day

4) To arrange other schedules, leave the **24HR** checkbox blank and set the Start/End time.



Camera: [A1] Camera 01
Enable Schedule: ☑
Week: Mon
24HR: □
Type: Continuous
Start/End Time: 00:00-00:00

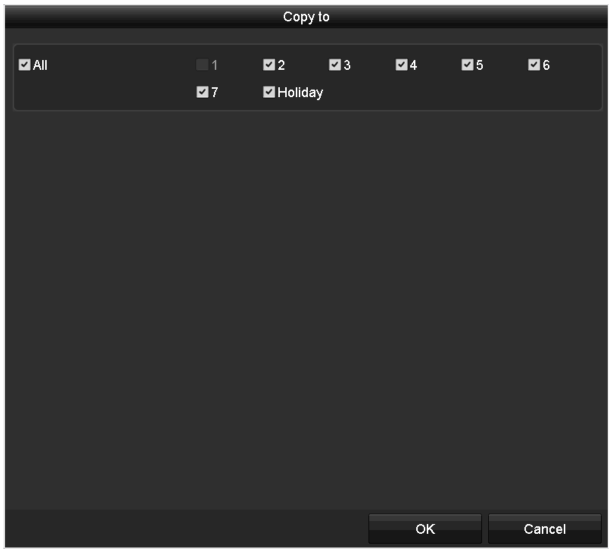
Figure 80, Edit Schedule – Set Time Period

NOTE

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

To enable Event, Motion, Alarm, M | A (motion or alarm), M & A (motion and alarm), and POS 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 recordings for other days in the week. If the schedule can also be set for other days, click **Copy**.



☑ All
□ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6
☑ 7 ☑ Holiday

Figure 81, Copy Schedule to Other Days

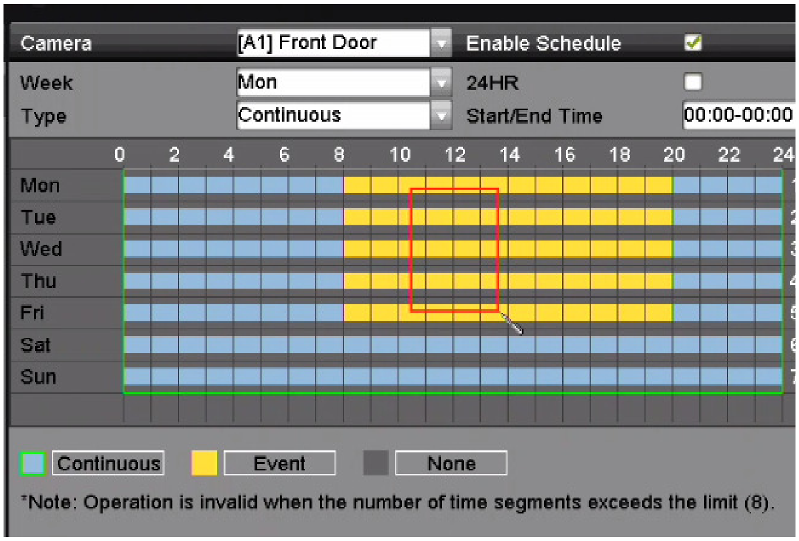
NOTE

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

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

6. Draw the schedule

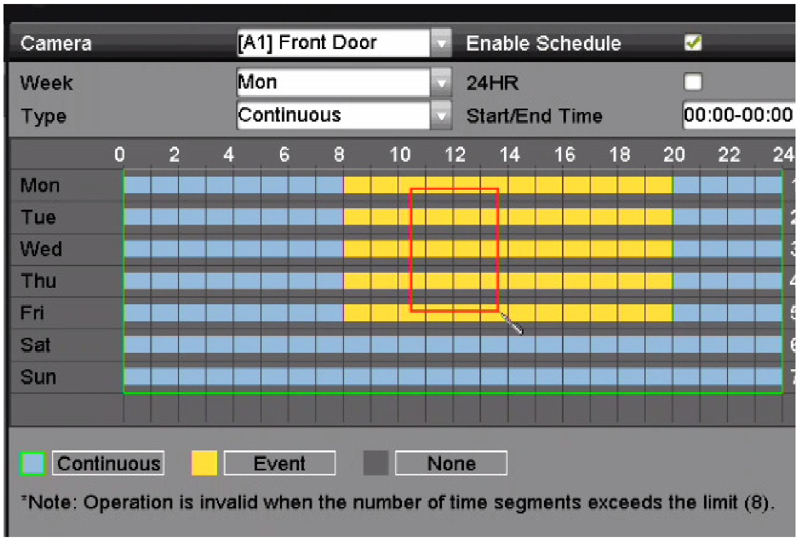
1) Click the color icon to select a record type in the event list on the right side of the interface.



Camera: [A1] Front Door
Enable Schedule: ☑
Week: Mon
24HR: □
Type: Continuous
Start/End Time: 00:00-00:00

*Note: Operation is invalid when the number of time segments exceeds the limit (8).

Figure 82, Draw the Recording Schedule



Camera: [A1] Front Door
Enable Schedule: ☑
Week: Mon
24HR: □
Type: Continuous
Start/End Time: 00:00-00:00

*Note: Operation is invalid when the number of time segments exceeds the limit (8).

Figure 83, Draw the Capture Schedule

2) Drag the mouse on the schedule.

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

NOTE

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

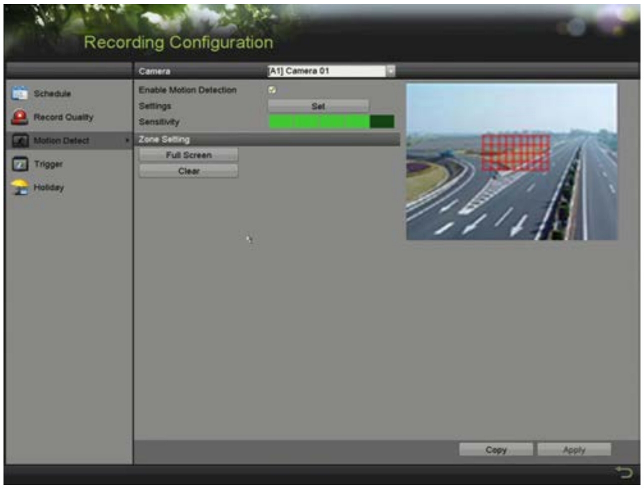
7. Click **Apply** in the **Record Schedule** interface to save the settings.

5.3 Configuring Motion Detection Recording and Capture

Purpose

Follow these steps to set the motion detection parameters. In Live View mode, once a motion detection event takes place, the DVR can analyze it and perform many actions to handle it. Enabling the motion detection function can trigger certain channels to start recording, or trigger full screen monitoring, audio warning, notifying the surveillance center, sending e-mail, and so on.

1. Go to Menu > Camera > Motion.



Recording Configuration

Camera: [A1] Camera 01

Enable Motion Detection: ☑

Settings: Set

Sensitivity

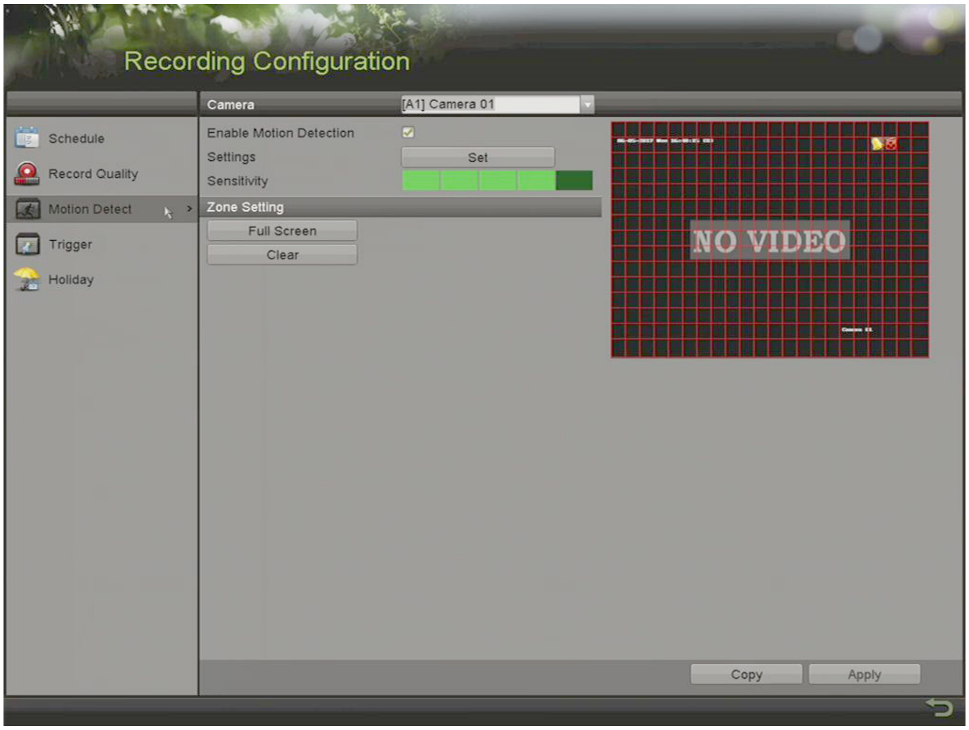
Figure 84, Motion Detection

2. Configure Motion Detection:

   1) Choose camera you want to configure.

   2) Check the Enable Motion Detection checkbox.

   3) 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**.

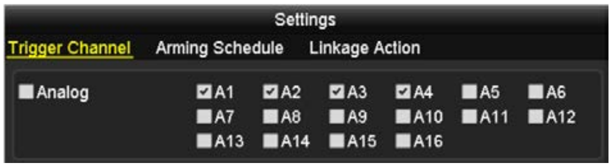


Camera: [A1] Camera 01

Enable Motion Detection ☑

Figure 85, Motion Detection – Mask

4) Click **Set**, and the channel information message box pops up.



□ Analog ☑A1 ☑A2 ☑A3 ☑A4 □A5 □A6
□A7 □A8 □A9 □A10 □A11 □A12
□A13 □A14 □A15 □A16

Figure 86, Motion Detection Settings

5) Select the channels that you want the motion detection event to trigger recording.

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

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

8) Exit the Motion Detection menu.

3. Configure the schedule.

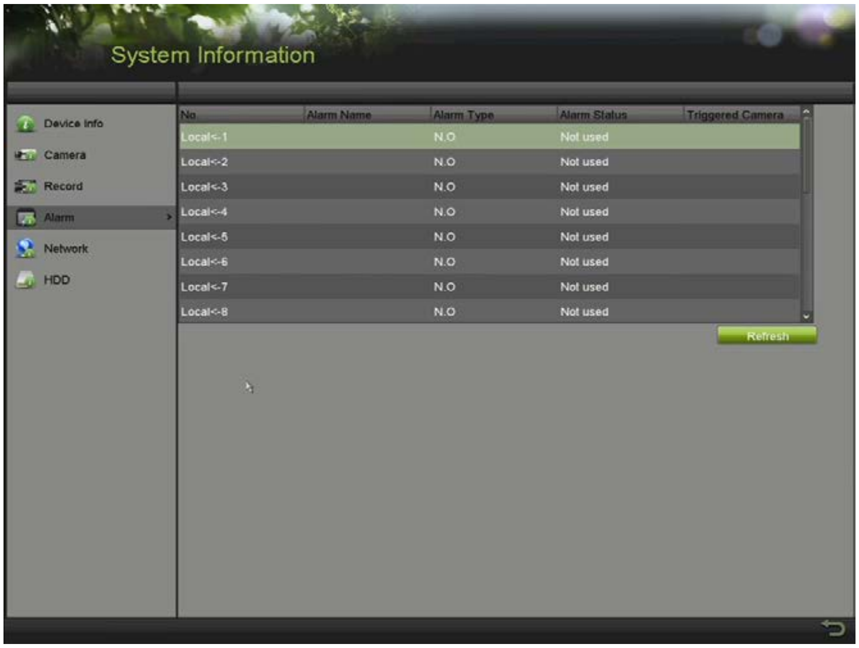
4. Choose Motion as the record type.

5.4 Configuring Alarm Triggered Recording and Capture

Purpose

Follow the procedure to configure alarm triggered recording or capture.

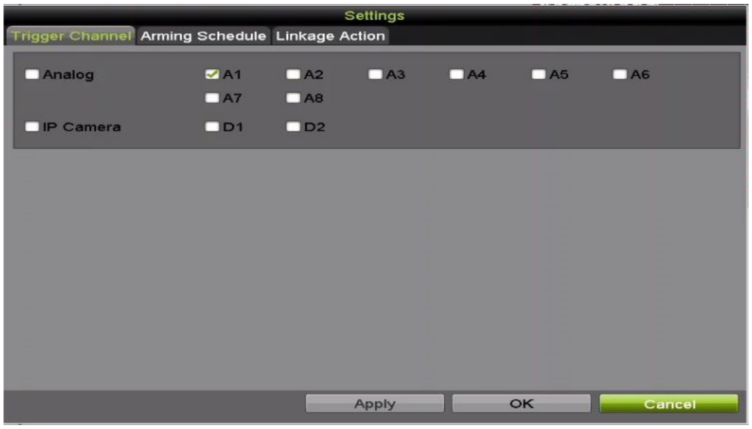
1. Go to Menu > Recording Configuration > Trigger > Alarm Input.



No	Alarm Name	Alarm Type	Alarm Status	Triggered Camera
Local<-1		N.O	Not used	
Local<-2		N.O	Not used	
Local<-3		N.O	Not used	
Local<-4		N.O	Not used	
Local<-5		N.O	Not used	
Local<-6		N.O	Not used	
Local<-7		N.O	Not used	
Local<-8		N.O	Not used	

Figure 87, 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 **Set** to set the triggered channels, arming schedule, linkage actions, and PTZ linking.

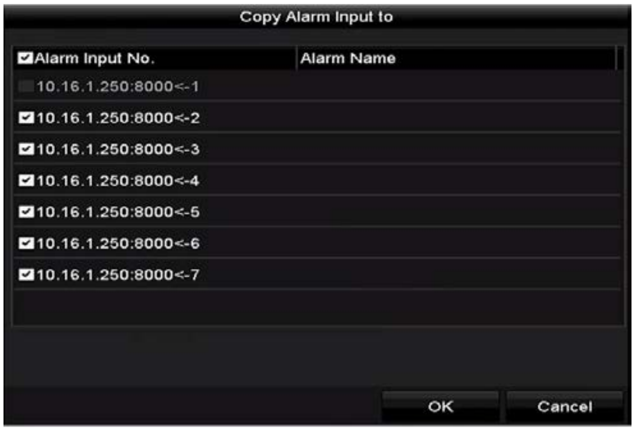


□ Analog ☑ A1 □ A2 □ A3 □ A4 □ A5 □ A6 □ A7 □ A8

□ IP Camera □ D1 □ D2

Figure 88, Alarm Handling

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



Copy Alarm Input to

☑Alarm Input No.	Alarm Name
□10.16.1.250:8000<-1	
☑10.16.1.250:8000<-2	
☑10.16.1.250:8000<-3	
☑10.16.1.250:8000<-4	
☑10.16.1.250:8000<-5	
☑10.16.1.250:8000<-6	
☑10.16.1.250:8000<-7	

Figure 89, Copy Alarm Input

5.5 Configuring Event Recording and Capture

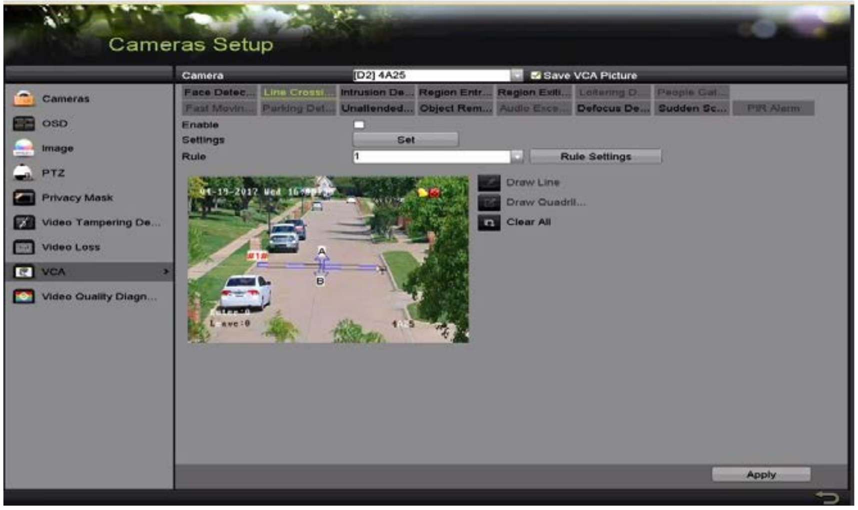
Purpose

Event triggered recording can be configured through the menu. The 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 HUI Series supports line crossing detection and intrusion detection of all channels, and 2-ch sudden scene change detection. Channels with audio support audio exception detection.
>
> For 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 > Camera > VCA.



Cameras Setup

Camera: [D2] 4A25 ☑ Save VCA Picture

Enable: □

Settings: Set

Rule: 1

Figure 90, VCA Settings

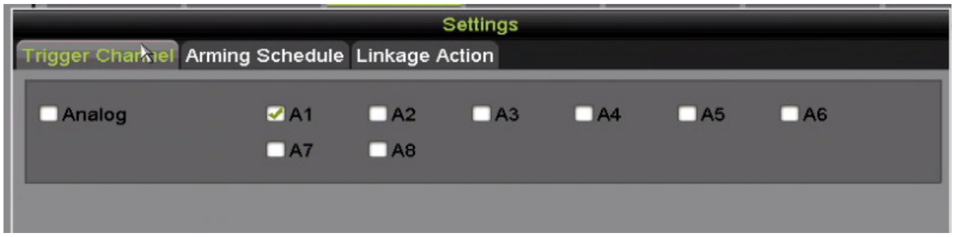
2. Select a **Camera**.

3. Configure the detection rules for VCA events.

4. Click **Set** to configure the alarm linkage actions for the VCA events.

5. Select **Trigger Channel** tab and select one or more channels that will start to record when a VCA alarm is triggered.

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



□ Analog ☑ A1 □ A2 □ A3 □ A4 □ A5 □ A6
□ A7 □ A8

Figure 91, Set Triggered Camera of VCA Alarm

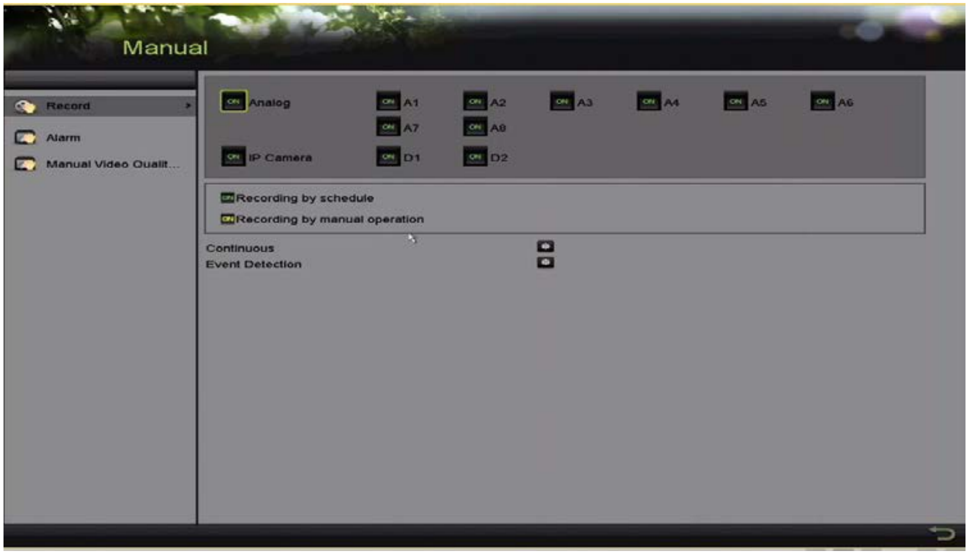
7. Enter **Record Schedule Settings** interface (Menu > Record > Schedule > Record Schedule) and set Event as the record type.

5.6 Configuring Manual Recording and Continous Capture

Purpose

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

1. Go to Menu > Manual > Record.



ON Analog ON A1 ON A2 ON A3 ON A4 ON A5 ON A6
ON A7 ON A8
ON IP Camera ON D1 ON D2

ON Recording by schedule
ON Recording by manual operation

Continuous
Event Detection

Figure 92, Manual Record

2. Enable manual record.

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

4. Disable manual record.

5. Click ON to change it to OFF, or click **Analog** ON to disable manual record of all channels.

NOTE

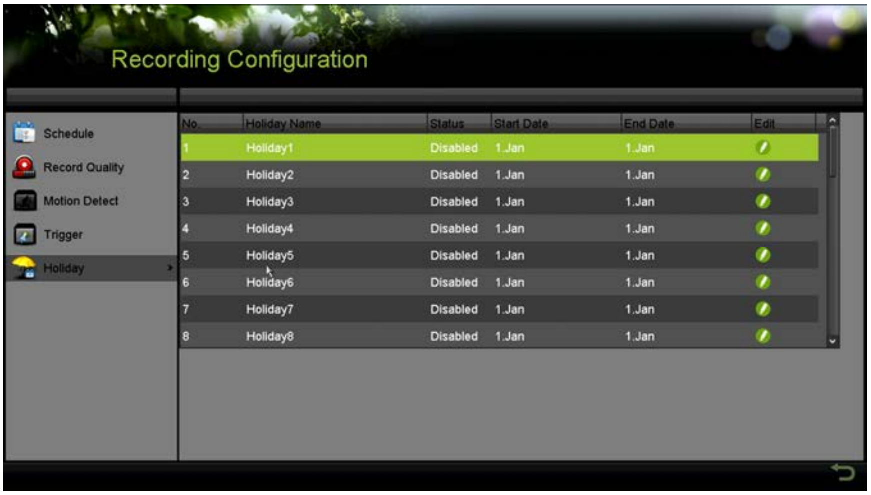
After rebooting all the manual records enabled are canceled.

5.7 Configuring Holiday Recording and Capture

Purpose

Follow these steps to configure the record or capture holiday schedules for the year to have different recording plans on holidays.

1. Go to Menu > Recording Configuration > Holiday.

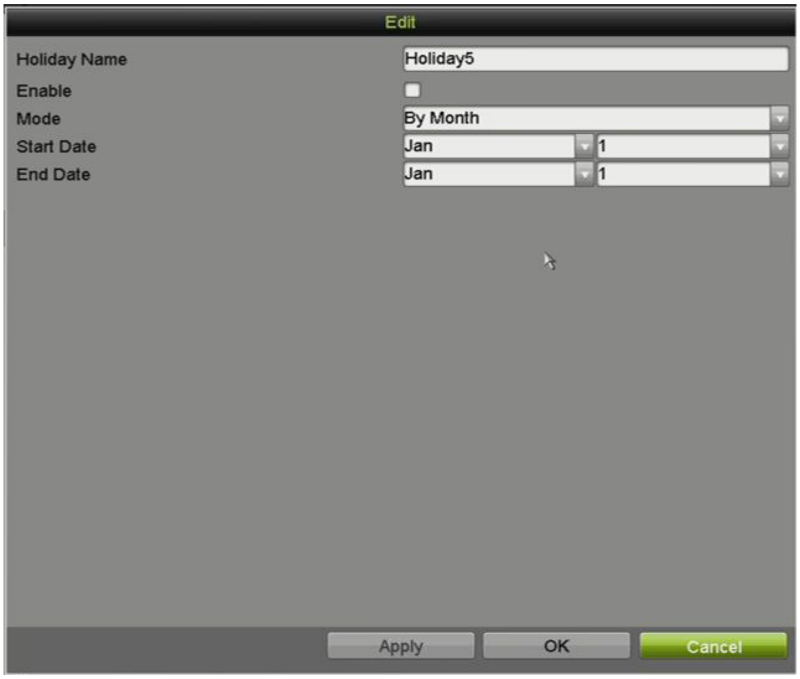


No.	Holiday Name	Status	Start Date	End Date	Edit
1	Holiday1	Disabled	1.Jan	1.Jan	✎
2	Holiday2	Disabled	1.Jan	1.Jan	✎
3	Holiday3	Disabled	1.Jan	1.Jan	✎
4	Holiday4	Disabled	1.Jan	1.Jan	✎
5	Holiday5	Disabled	1.Jan	1.Jan	✎
6	Holiday6	Disabled	1.Jan	1.Jan	✎
7	Holiday7	Disabled	1.Jan	1.Jan	✎
8	Holiday8	Disabled	1.Jan	1.Jan	✎

Figure 93, Holiday Settings

2. Enable Edit Holiday schedule.

   1) Click ✎ to enter the Edit interface.



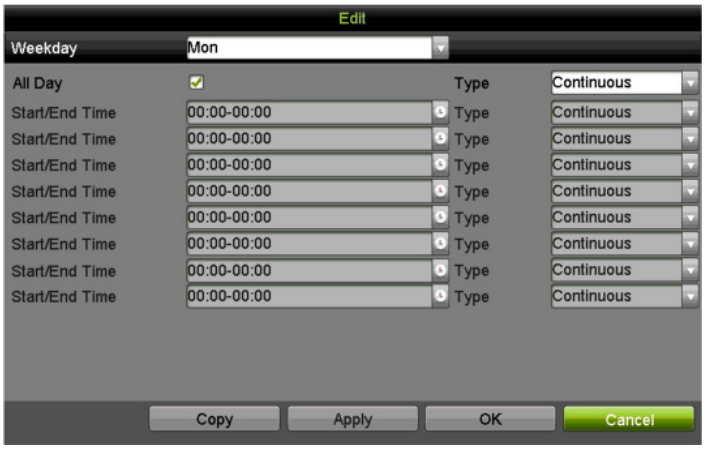
Holiday Name	Holiday5
Enable	□
Mode	By Month
Start Date	Jan 1
End Date	Jan 1

Figure 94, Edit Holiday Settings

2) Check the **Enable** checkbox.

3) Select Mode from the drop-down list (by Month, By Week, and By Date are selectable).

3. Set the start and end date.
4. Click **Apply** to save settings.
5. Click **OK** to exit the Edit interface.
6. Go to Menu > Recording Configuration > Schedule.
7. Click on **Edit**.
8. Choose Holiday in the Schedule drop-down list or draw the schedule on the Holiday timeline.



Edit

Weekday	Mon		
All Day	☑	Type	Continuous
Start/End Time	00:00-00:00	Type	Continuous
Start/End Time	00:00-00:00	Type	Continuous
Start/End Time	00:00-00:00	Type	Continuous
Start/End Time	00:00-00:00	Type	Continuous
Start/End Time	00:00-00:00	Type	Continuous
Start/End Time	00:00-00:00	Type	Continuous
Start/End Time	00:00-00:00	Type	Continuous
Start/End Time	00:00-00:00	Type	Continuous

Figure 95, Edit Schedule – Holiday

NOTE

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

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

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

5.8 Configuring Redundant Recording and Capture

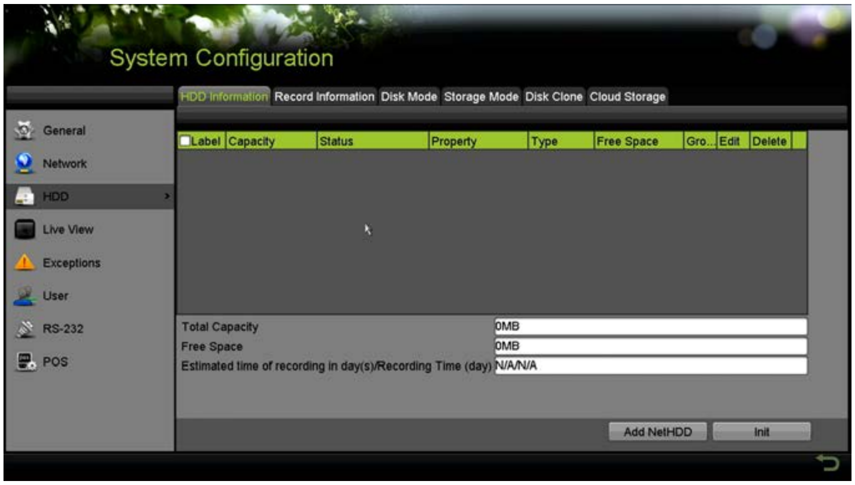
Purpose

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

Before You Start

Set the Storage mode in the HDD advanced settings to *Group* before setting the HDD property to Redundant. There must be at least one other HDD in Read/Write status.

1. Go to Menu > System Configuration > HDD.



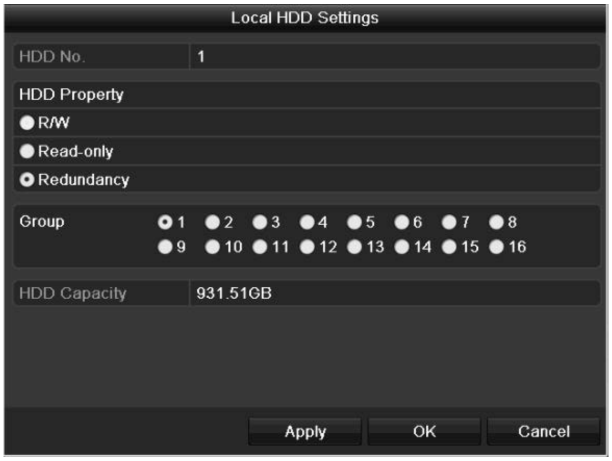
□Label	Capacity	Status	Property	Type	Free Space	Gro...	Edit	Delete

Total Capacity	0MB
Free Space	0MB
Estimated time of recording in day(s)/Recording Time (day)	N/A/N/A

Figure 96, HDD Information

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

   1) Set the HDD property to Redundant.



HDD No. 1

HDD Property

○ R/W

○ Read-only

● Redundancy

Group ● 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7 ○ 8 ○ 9 ○ 10 ○ 11 ○ 12 ○ 13 ○ 14 ○ 15 ○ 16

HDD Capacity 931.51GB

Figure 97, HDD General – Editing

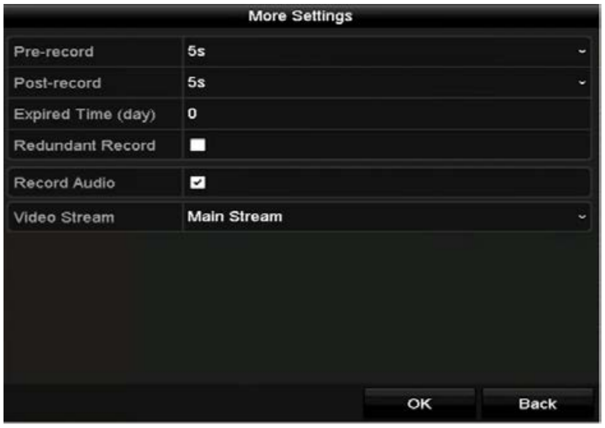
   2) Click **Apply** to save the settings.

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

3. Go to Menu > Record > Parameters > Record.

   1) Select the Camera you want to configure.

   2) Click **More Settings**.



More Settings

Pre-record	5s
Post-record	5s
Expired Time (day)	0
Redundant Record	□
Record Audio	☑
Video Stream	Main Stream

Figure 98, More Settings

3) Check the **Redundant Record** checkbox.

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 you want to apply the settings.

5.9 Configuring HDD Group

Purpose

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

1. Go to Menu > HDD > Advanced > Storage Mode.
2. Check whether the storage mode of the HDD is Group. If not, set it to Group.
3. Select **General** in the left bar.
4. Click ✎ to enter editing interface.
5. Configuring HDD group.

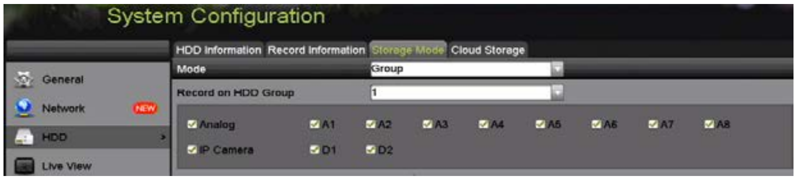
   1) Choose a group number for the HDD group.

   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 that you want to save the record files in the HDD group.

   1) Go to Menu > HDD > Advanced > Storage Mode.



Mode: Group

Record on HDD Group: 1

☑ Analog ☑ A1 ☑ A2 ☑ A3 ☑ A4 ☑ A5 ☑ A6 ☑ A7 ☑ A8

☑ IP Camera ☑ D1 ☑ D2

Figure 99, HDD Advanced

2) Choose Group number in the drop-down list of **Record on HDD Group**

3) Check the channels you want to save in this group.

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

NOTE

After you have configured the HDD groups, configure the recording settings.

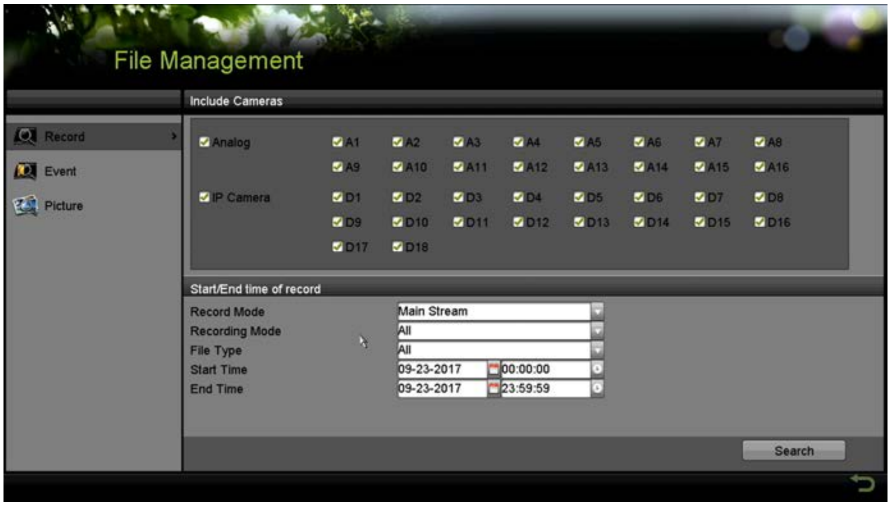
5.10 Files Protection

Purpose

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

5.10.1 Protect Record Files by Locking Them

- Go to Menu > File Management.



☑ Analog ☑ A1 ☑ A2 ☑ A3 ☑ A4 ☑ A5 ☑ A6 ☑ A7 ☑ A8 ☑ A9 ☑ A10 ☑ A11 ☑ A12 ☑ A13 ☑ A14 ☑ A15 ☑ A16

☑ IP Camera ☑ D1 ☑ D2 ☑ D3 ☑ D4 ☑ D5 ☑ D6 ☑ D7 ☑ D8 ☑ D9 ☑ D10 ☑ D11 ☑ D12 ☑ D13 ☑ D14 ☑ D15 ☑ D16 ☑ D17 ☑ D18

Record Mode: Main Stream

Recording Mode: All

File Type: All

Start Time: 09-23-2017 00:00:00

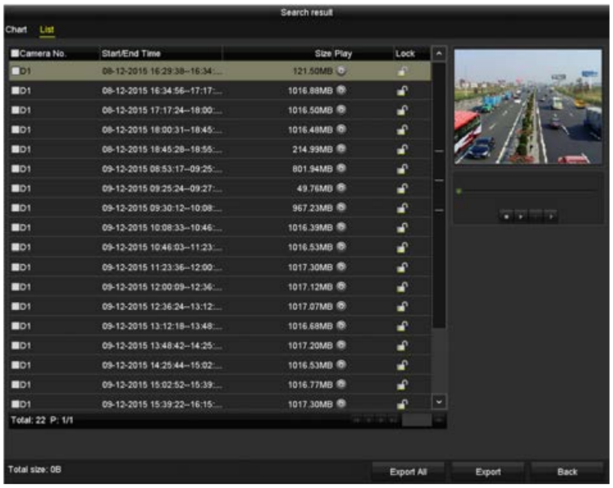
End Time: 09-23-2017 23:59:59

Figure 100, Export

- Select the channels you want to investigate by checking the ☑ checkbox.

- Configure the record mode, record type, file type, start time, and end time.

- Click **Search** to show the results.



☐Camera No.	Start/End Time	Size	Play	Lock
☐D1	08-12-2015 16:29:38--16:34:...	121.50MB	●	🔓
☐D1	08-12-2015 16:34:56--17:17:...	1016.88MB	●	🔓
☐D1	08-12-2015 17:17:24--18:00:...	1016.50MB	●	🔓
☐D1	08-12-2015 18:00:31--18:45:...	1016.48MB	●	🔓
☐D1	08-12-2015 18:45:28--18:55:...	214.99MB	●	🔓
☐D1	09-12-2015 08:53:17--09:25:...	801.94MB	●	🔓
☐D1	09-12-2015 09:25:24--09:27:...	49.76MB	●	🔓
☐D1	09-12-2015 09:30:12--10:08:...	967.23MB	●	🔓
☐D1	09-12-2015 10:08:33--10:46:...	1016.39MB	●	🔓
☐D1	09-12-2015 10:46:03--11:23:...	1016.53MB	●	🔓
☐D1	09-12-2015 11:23:36--12:00:...	1017.30MB	●	🔓
☐D1	09-12-2015 12:00:09--12:36:...	1017.12MB	●	🔓
☐D1	09-12-2015 12:36:24--13:12:...	1017.07MB	●	🔓
☐D1	09-12-2015 13:12:18--13:48:...	1016.68MB	●	🔓
☐D1	09-12-2015 13:48:42--14:25:...	1017.20MB	●	🔓
☐D1	09-12-2015 14:25:44--15:02:...	1016.53MB	●	🔓
☐D1	09-12-2015 15:02:52--15:39:...	1016.77MB	●	🔓
☐D1	09-12-2015 15:39:22--16:15:...	1017.30MB	●	🔓

Total: 22 P: 1/1

Total size: 0B

Figure 101, Export – Search Result

- Protect the record files.

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

Record file recordings not completed cannot be locked.

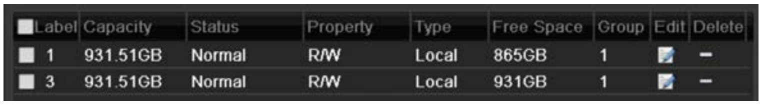
2) Click 🔒 to change it to 🔓 to unlock and unprotect the file.

5.10.2 Protect File by Setting HDD to Read-Only

Before You Start

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

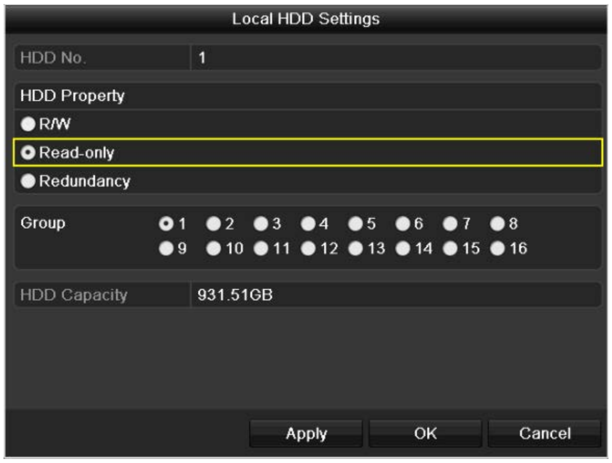
1. Go to Menu > HDD > General.



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

Figure 102, HDD General

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



Local HDD Settings

HDD No. 1

HDD Property

● R/W

◉ Read-only

● Redundancy

Group ◉ 1 ● 2 ● 3 ● 4 ● 5 ● 6 ● 7 ● 8 ● 9 ● 10 ● 11 ● 12 ● 13 ● 14 ● 15 ● 16

HDD Capacity 931.51GB

Figure 103, HDD General – Editing

3. Set the HDD to Read-only.

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

NOTE

You cannot save files to a read-only HDD. If you want 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 in it, the file will be saved to the next R/W HDD. If there is only one HDD, the recording will be stopped.

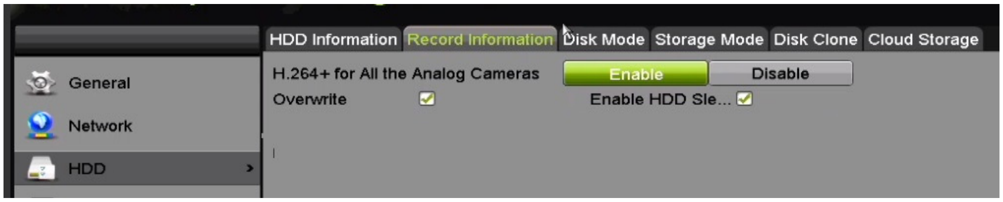
5.11 One-Key Enable/Disable H.264+/H.265+, Analog Cameras

Purpose

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

5.11.1 Enabling

1. Go to Menu > Record > Advanced.



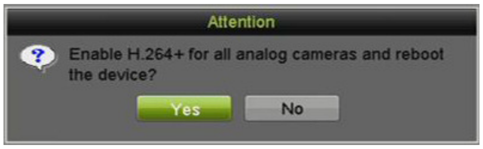
H.264+ for All the Analog Cameras Enable Disable

Overwrite ☑

Enable HDD Sle... ☑

Figure 104, Advanced Settings

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


Attention

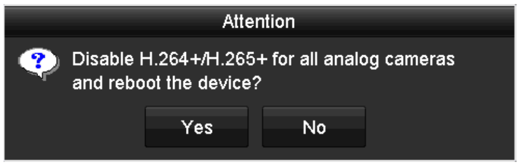
Enable H.264+ for all analog cameras and reboot the device?

Figure 105, Attention Box

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

5.11.2 Disabling

1. Go to Menu > Record > Advanced.
2. Click **Disable** to disable H.264+ for all the analog cameras and the following attention box pops up.


Attention

Disable H.264+/H.265+ for all analog cameras and reboot the device?

Figure 106, Attention Box

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

5.12 Playback

5.12.1 Instant Playback by Channel

Purpose

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

1. Choose a channel in Live View mode and click ▶ in the quick setting toolbar.

NOTE

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

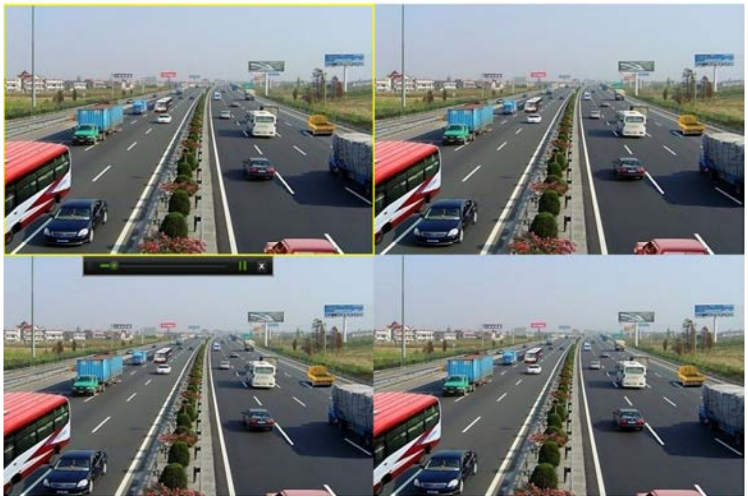


Figure 107, Instant Playback Interface

5.12.2 Playback by Normal Search

5.12.2.1 Playback by Channel

1. Enter the **Playback** interface.
2. Right click a channel in Live View mode and select **Playback** from the menu, as shown below:

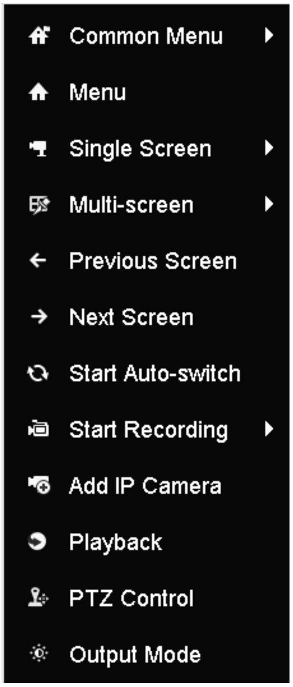


Figure 108, Right-click Menu under Live View

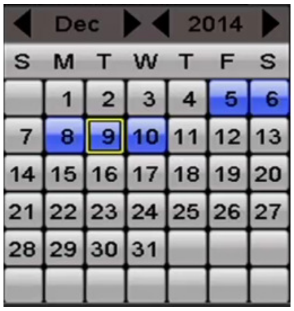
5.12.2.2 Playback by Time

Purpose

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

1. Go to Menu > Playback.

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



◀ Dec ▶ ◀ 2014 ▶

S	M	T	W	T	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

Figure 109, Playback Calendar

NOTE

If there are record files for that camera on that day, the icon for that day is displayed on the calendar as 9. Otherwise it is displayed as 9.

5.12.3 Playback Interface

1. You can select main stream or sub-stream from the playback drop-down list. You can also use the toolbar in the bottom part of **Playback** interface to control playing progress, as shown in the following figure.

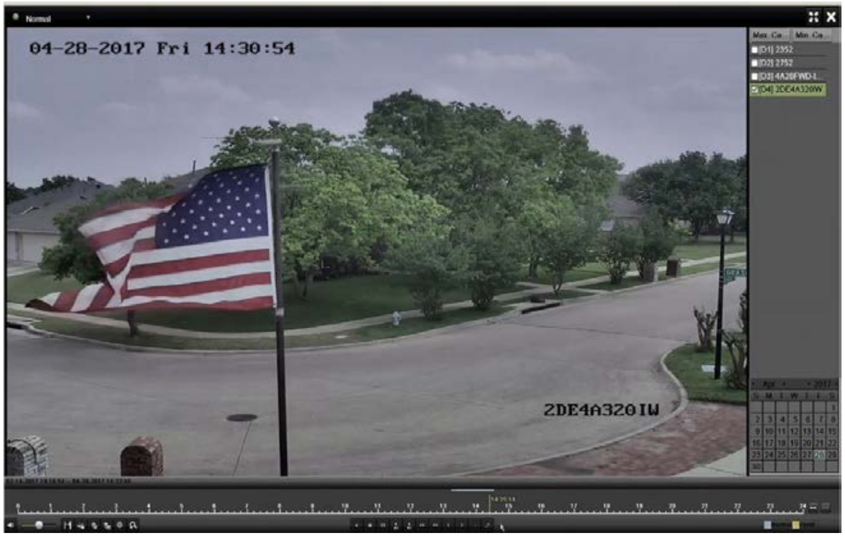


Figure 110, Playback Interface

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

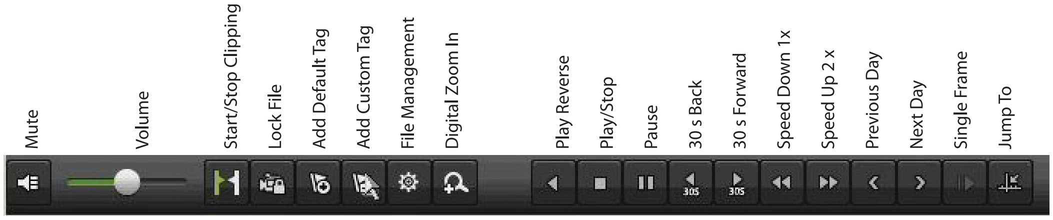


Figure 111, Playback Toolbar

Table 1-14 Detailed Explanation of Playback Toolbar

Button	Operation	Button	Operation	Button	Operation
🔈/🔇	Audio on/Mute	✂/✂	Start/Stop clipping	🔒	Lock File
🏷	Add default tag	🏷	Add customized tag	⚙	File management for video clips, captured pictures, locked files and tags
◀/❚❚	Reverse play/Pause	■	Stop	🔍	Digital Zoom
▶ 30S	30s forward	◀ 30S	30s reverse	❚❚/▶	Pause/Play
▶▶	Fast forward	<	Previous day	◀◀	Slow forward
⛶	Full Screen	✖	Exit	>	Next day
💾	Save the clips	10 11 12	Process bar	↔/→←	Scaling up/down the time line
📷	Capture Picture	T	Enable/Disable POS information overlay		

NOTE

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

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

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

When POS is enabled when playing back, the POS information will be overlaid on the video. Keyword searching is supported.

5.12.4 Playback by Event Search

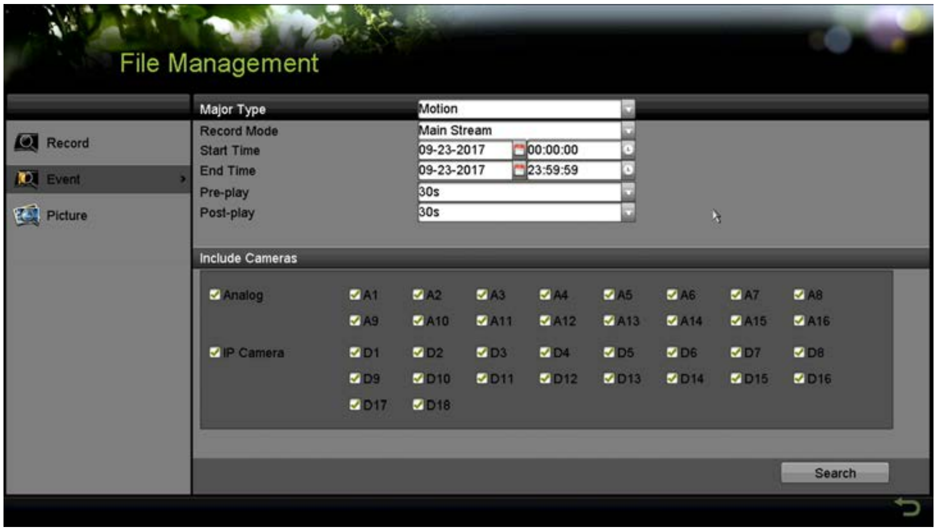
Purpose

Play back record files on one or several channels searched 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.



Major Type: Motion
Record Mode: Main Stream
Start Time: 09-23-2017 00:00:00
End Time: 09-23-2017 23:59:59
Pre-play: 30s
Post-play: 30s

Include Cameras

☑ Analog: ☑ A1 ☑ A2 ☑ A3 ☑ A4 ☑ A5 ☑ A6 ☑ A7 ☑ A8 ☑ A9 ☑ A10 ☑ A11 ☑ A12 ☑ A13 ☑ A14 ☑ A15 ☑ A16

☑ IP Camera: ☑ D1 ☑ D2 ☑ D3 ☑ D4 ☑ D5 ☑ D6 ☑ D7 ☑ D8 ☑ D9 ☑ D10 ☑ D11 ☑ D12 ☑ D13 ☑ D14 ☑ D15 ☑ D16 ☑ D17 ☑ D18

Figure 112, Video Search by Motion Detection

4. Click **Search**, and the record files matching the search conditions will be listed.

5. Select and click ▶ to play back the record files.

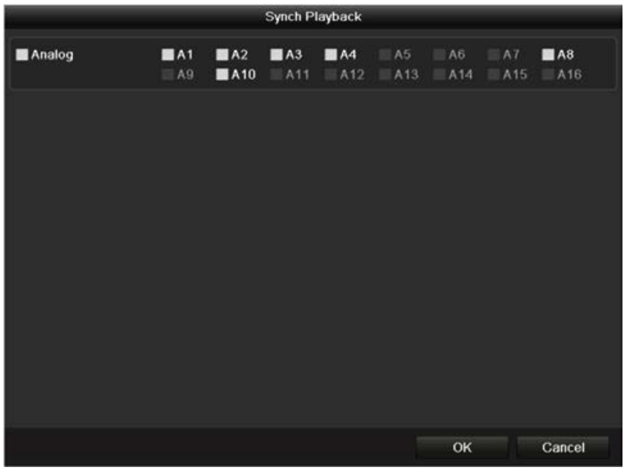
6. You can click **Back** to return to the search interface.

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

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

NOTE

The maximum synchronous playback channels varies by model.



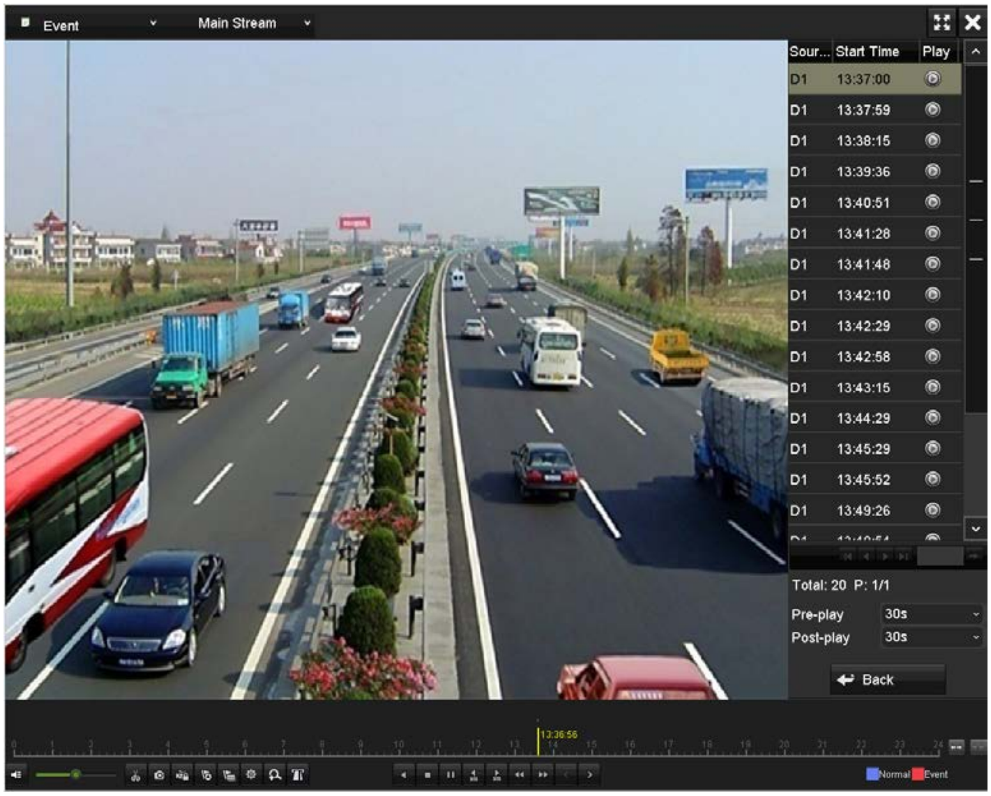
Synch Playback

□ Analog

□ A1 □ A2 □ A3 □ A4 □ A5 □ A6 □ A7 □ A8
□ A9 □ A10 □ A11 □ A12 □ A13 □ A14 □ A15 □ A16

Figure 113, Select Channels for Synchronous Playback

9. On the **Event Playback** interface, select the main stream or sub-stream from the drop-down list for playback. The toolbar in the bottom part of the **Playback** interface can be used to control the playing process.



Event
Main Stream

Sour...	Start Time	Play
D1	13:37:00	●
D1	13:37:59	●
D1	13:38:15	●
D1	13:39:36	●
D1	13:40:51	●
D1	13:41:28	●
D1	13:41:48	●
D1	13:42:10	●
D1	13:42:29	●
D1	13:42:58	●
D1	13:43:15	●
D1	13:44:29	●
D1	13:45:29	●
D1	13:45:52	●
D1	13:49:26	●

Total: 20 P: 1/1

Pre-play 30s

Post-play 30s

Figure 114, Interface of Playback by Event

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

- **Pre-play**: The time to play back before the event. For example, if an alarm triggered the recording at 10:00, if the pre-play time is five seconds, the video starts playback from 9:59:55.

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

11. Click ‹ or › to select the previous or next event.

5.12.5 Playback by Tag

Purpose

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

Before Playing Back by Tag

1. Go to Menu > Playback.
2. Search and play back the record file(s).

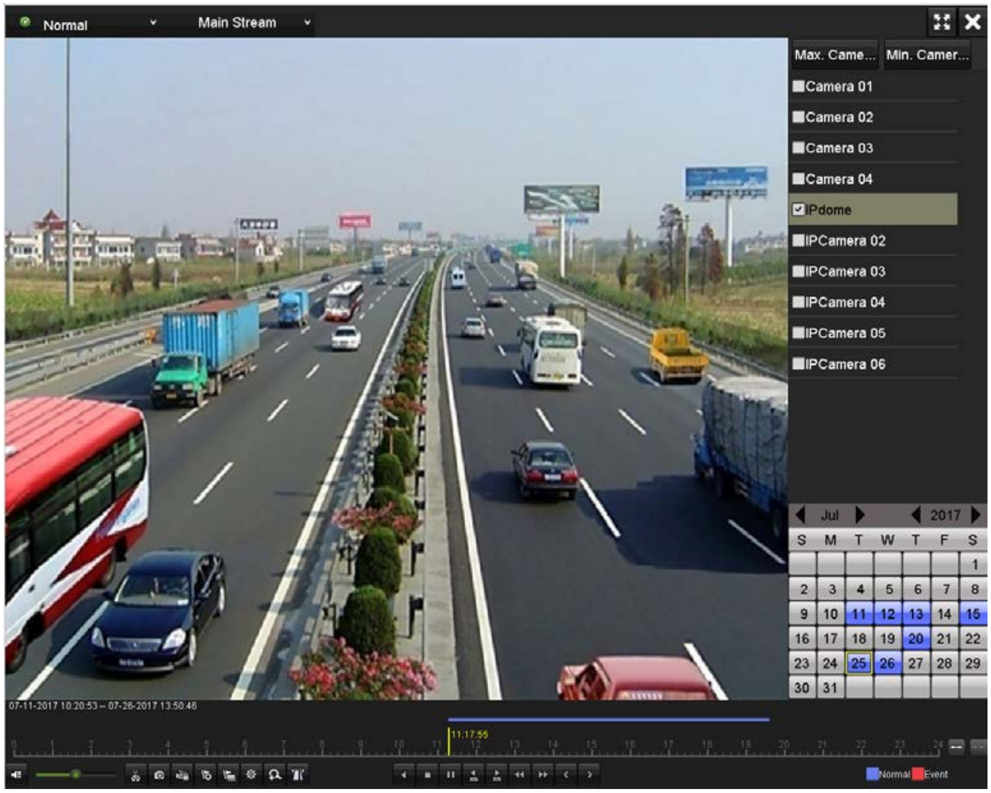
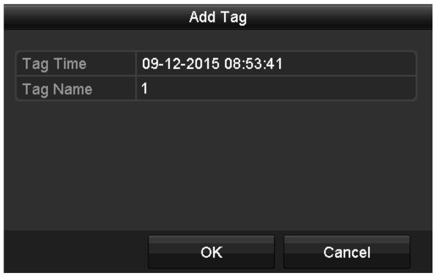


Figure 115, Interface of Playback by Time

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



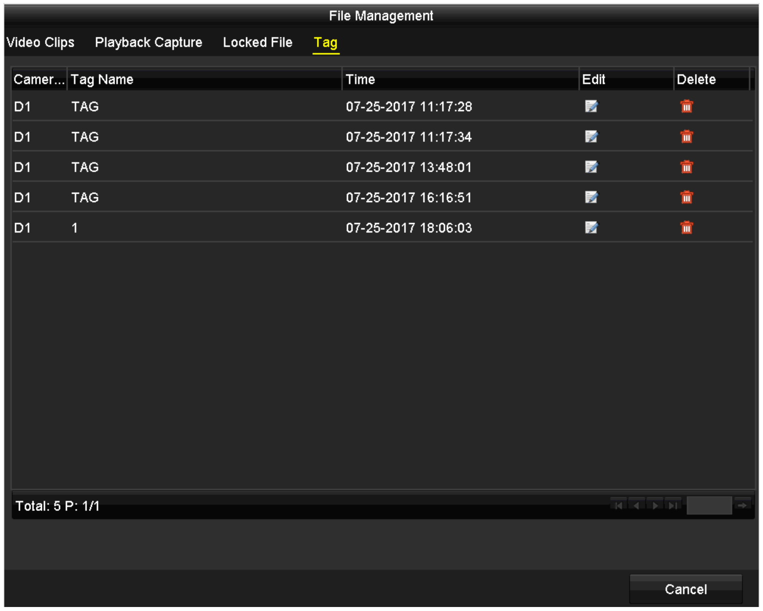
Tag Time	09-12-2015 08:53:41
Tag Name	1

Figure 116, Add Tag

NOTE

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

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



Camer...	Tag Name	Time	Edit	Delete
D1	TAG	07-25-2017 11:17:28	✎	🗑
D1	TAG	07-25-2017 11:17:34	✎	🗑
D1	TAG	07-25-2017 13:48:01	✎	🗑
D1	TAG	07-25-2017 16:16:51	✎	🗑
D1	1	07-25-2017 18:06:03	✎	🗑

Total: 5 P: 1/1

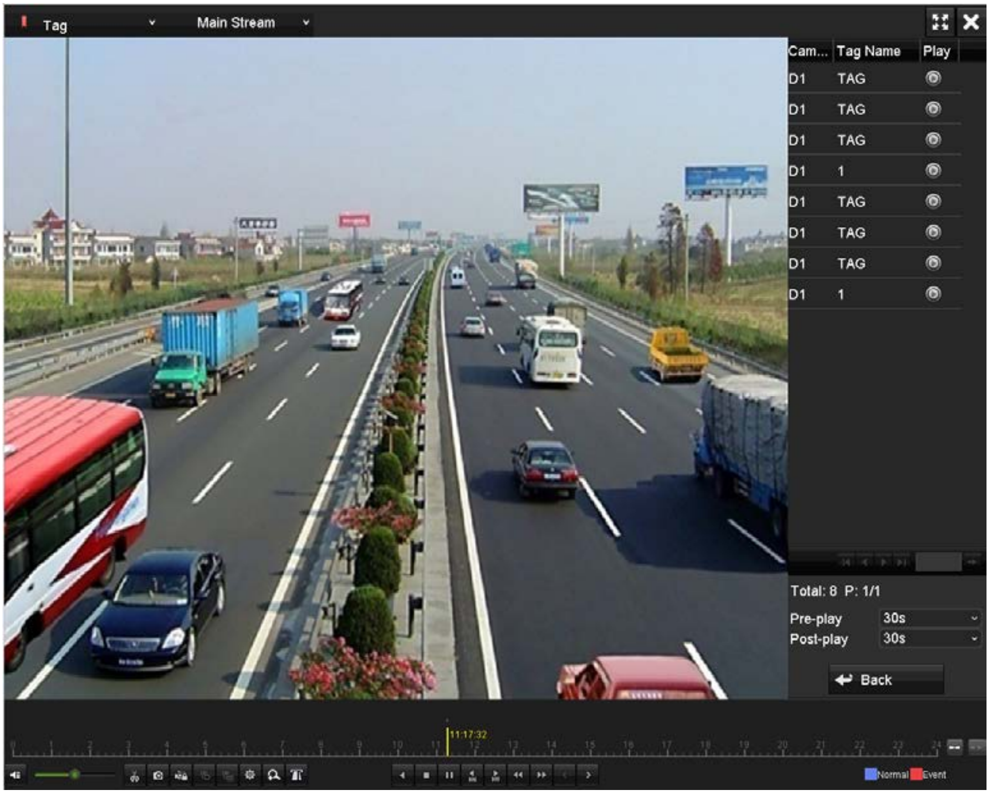
Figure 117, Tag Management Interface

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 the **Search Result** interface.

NOTE

Enter a keyword into the Keyword textbox to search a tag on command.



Tag ▾ Main Stream ▾

Cam...	Tag Name	Play
D1	TAG	◎
D1	TAG	◎
D1	TAG	◎
D1	1	◎
D1	TAG	◎
D1	TAG	◎
D1	TAG	◎
D1	1	◎

Total: 8 P: 1/1

Pre-play 30s

Post-play 30s

Figure 118, Video Search by Tag

6. Click ◎ to play back the file.

7. 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.

5.12.6 Playback by Smart Search

Purpose

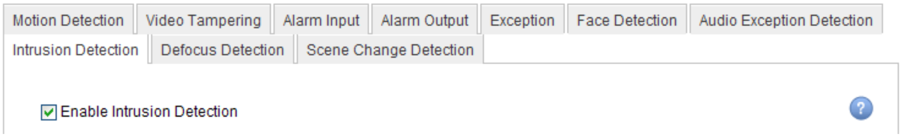
The Smart Playback provides an easy way to speed through less relevant information. In Smart Playback mode, the system will analyze the video containing the motion or VCA information, mark it in green, and play it at normal speed while video without motion will be played at 16 times speed. The Smart 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 via a Web browser, and enable intrusion detection by checking the checkbox. You may enter the motion detection

configuration interface at Configuration > Advanced Configuration > Events > Intrusion Detection.



☑ Enable Intrusion Detection

Figure 119, 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 side.

   3) Select a camera in the camera list.

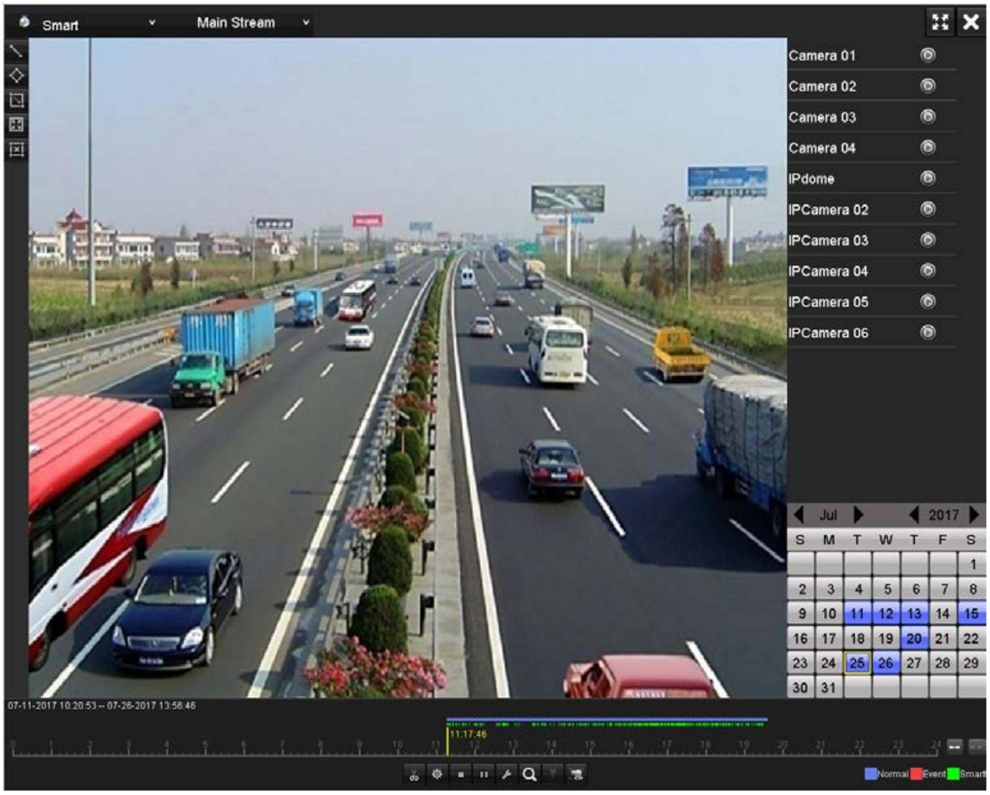


Figure 120, Smart Playback Interface

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

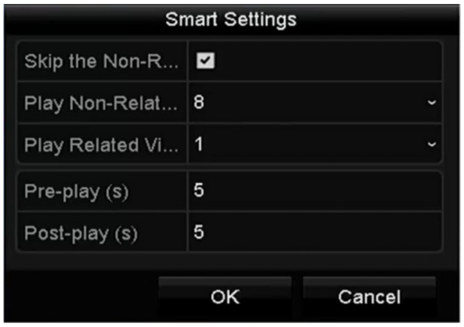
Table 1-15 Detailed Explanation of Smart Playback Toolbar

Button	Operation	Button	Operation	Button	Operation
╲	Draw line for the line crossing detection	◇	Draw quadrilateral for the intrusion detection	⧄	Draw rectangle for the intrusion detection
⛶	Set full screen for motion detection	☒	Clear all	✂/✂	Start/Stop clipping
⚙	File management for video clips	■	Stop playing	⏸/▶	Pause playing /Play
🔧	Smart settings	🔍	Search matched video files	▼	Filter video files by setting the target characters
/	Show/Hide VCA information				

5) Set the Smart Search rules and areas for 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.

6) Click 🔧 to configure the Smart settings.



Smart Settings

Skip the Non-R...	☑
Play Non-Relat...	8
Play Related Vi...	1
Pre-play (s)	5
Post-play (s)	5

Figure 121, Smart Settings

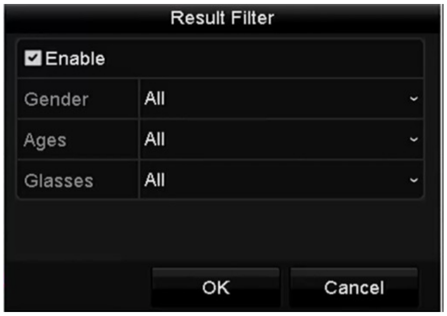
- **Skip the Non-Related Video:** Non-related video will not be played if this function is enabled.
- **Play Non-Related Video at:** Set the speed to play the non-related video. Maximum 8/4/2/1 are selectable.
- **Play Related Video at:** Set the speed to play the related video. Maximum 8/4/2/1 are selectable.

NOTE

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

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

4. (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.



Result Filter

☑ Enable

Gender	All
Ages	All
Glasses	All

OK Cancel

Figure 122, Set Result Filter

NOTE

The Result Filter function is supported by IP cameras only.

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

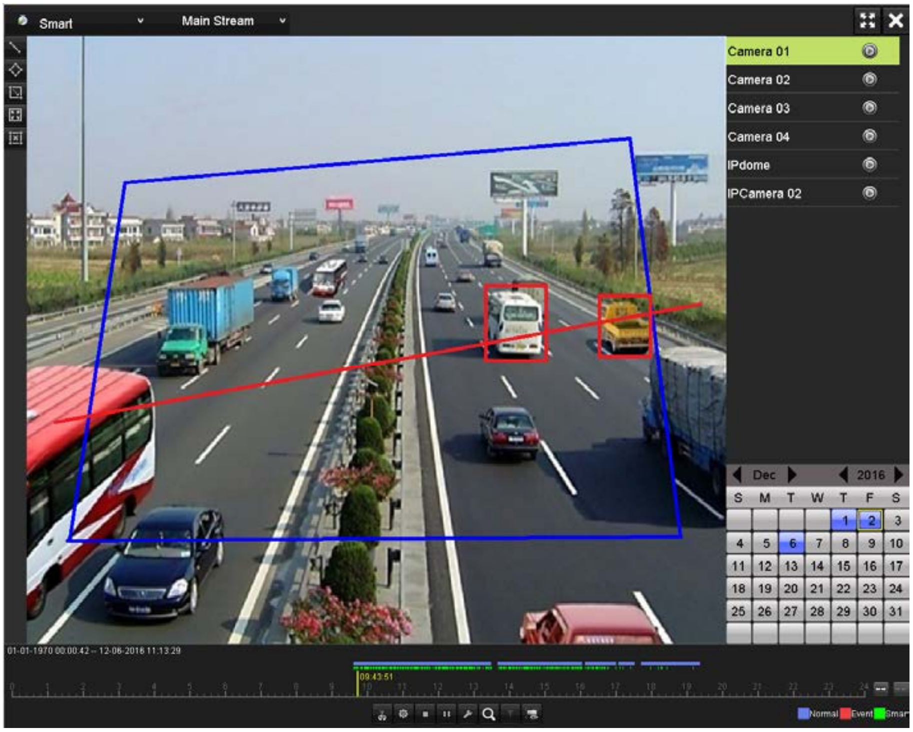


Figure 123, Show VCA Information

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.

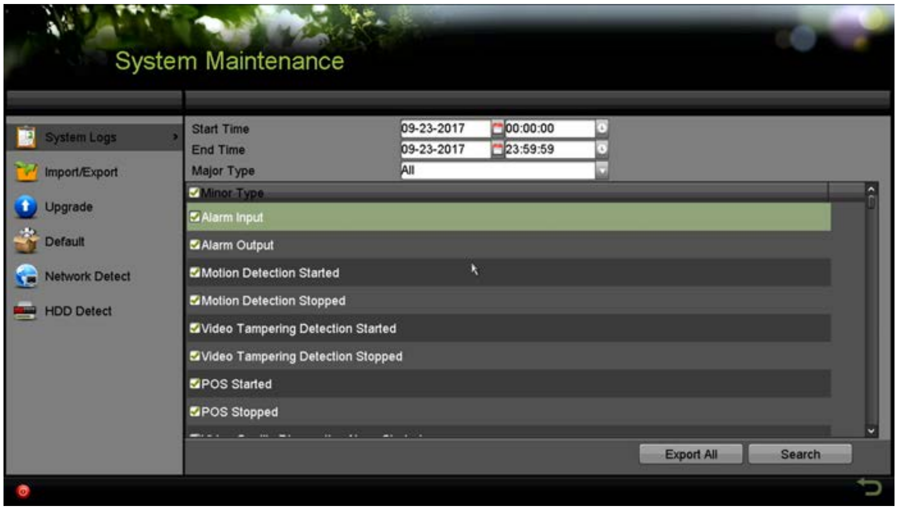
For analog cameras, the VCA information includes line crossing detection and intrusion detection. For IP cameras, the VCA information includes all the VCA detections of smart IP camera.

5.12.7 Playback by System Logs

Purpose

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

1. Go to Menu > Maintenance > System Logs.

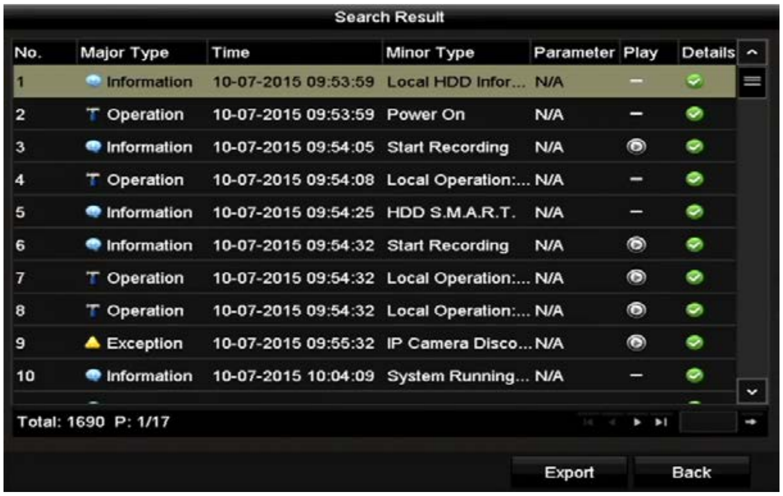


Start Time 09-23-2017 00:00:00
End Time 09-23-2017 23:59:59
Major Type All

☑ Minor Type
☑ Alarm Input
☑ Alarm Output
☑ Motion Detection Started
☑ Motion Detection Stopped
☑ Video Tampering Detection Started
☑ Video Tampering Detection Stopped
☑ POS Started
☑ POS Stopped

Figure 124, System Log Search Interface

2. Set search time and type and **Search**.



Search Result

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

Total: 1690 P: 1/17

Figure 125, Result of System Log Search

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

NOTE

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

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

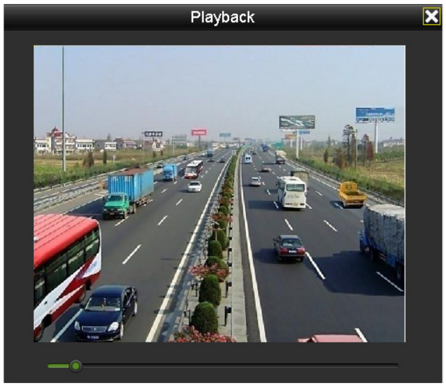


Figure 126, Interface of Playback by Log

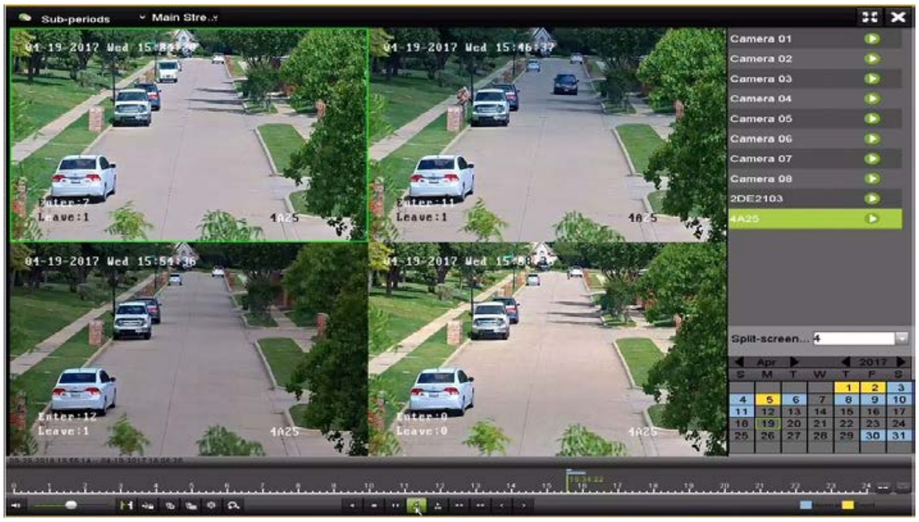
5.12.8 Playback by Sub-Periods

Purpose

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

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.



Split-screen... 4

Figure 127, Interface of Sub-periods Playback

NOTE

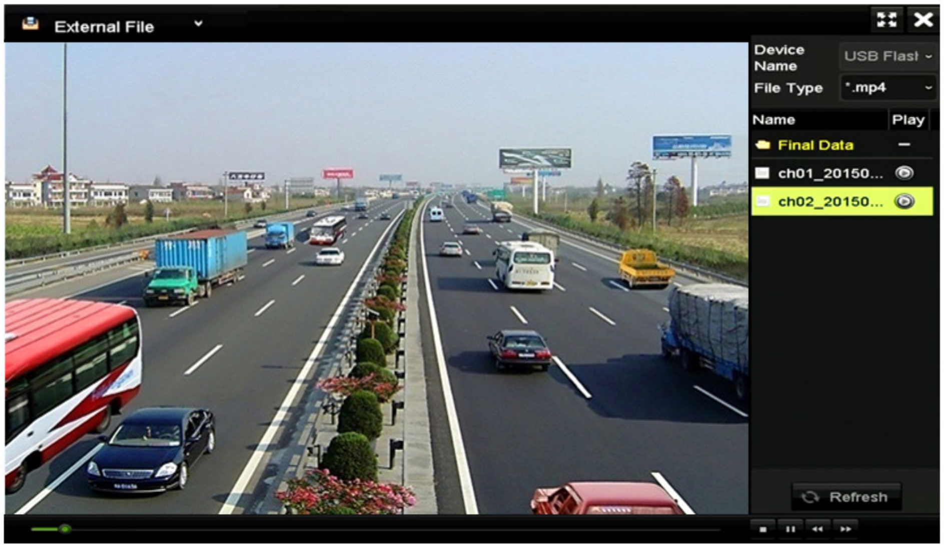
According to the defined number of split-screens, the video files on the selected date can be divided into average segments for playback. E.g., if there are video files existing between 16:00 and 22:00, and the 6-screen display mode is selected, then it can play the video files for 1 hour on each screen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

5.12.9 Play Back External Files

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 side.
3. The files are listed in the right-side list.
4. You can click the Refresh button to refresh the file list.
5. Select and click the ◉ button to play back it.



Device Name: USB Flash

File Type: *.mp4

Figure 128, Interface of External File Playback

5.13 Auxiliary Functions of Playback

5.13.1 Playing Back Frame-by-Frame

Purpose

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

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

5.13.2 Digital Zoom

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

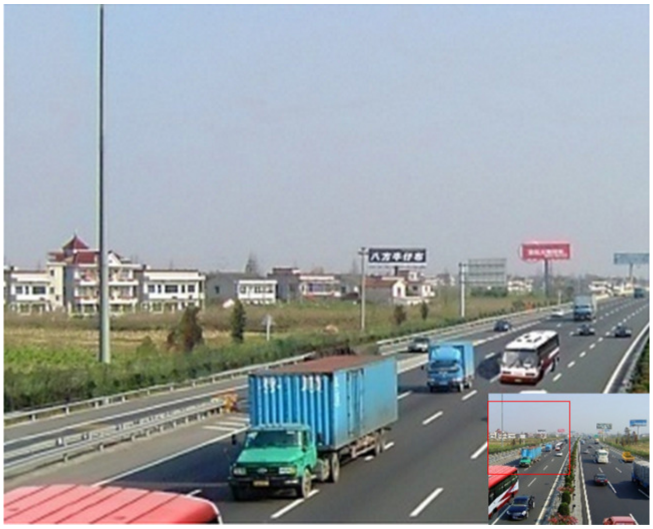


Figure 129, Draw Area for Digital Zoom

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

5.13.3 Multi-Channel Reverse Playback

Purpose

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

1. Go to Menu > Playback.

2. Check more than one checkboxes to select multiple channels and click to select a date on the calendar.

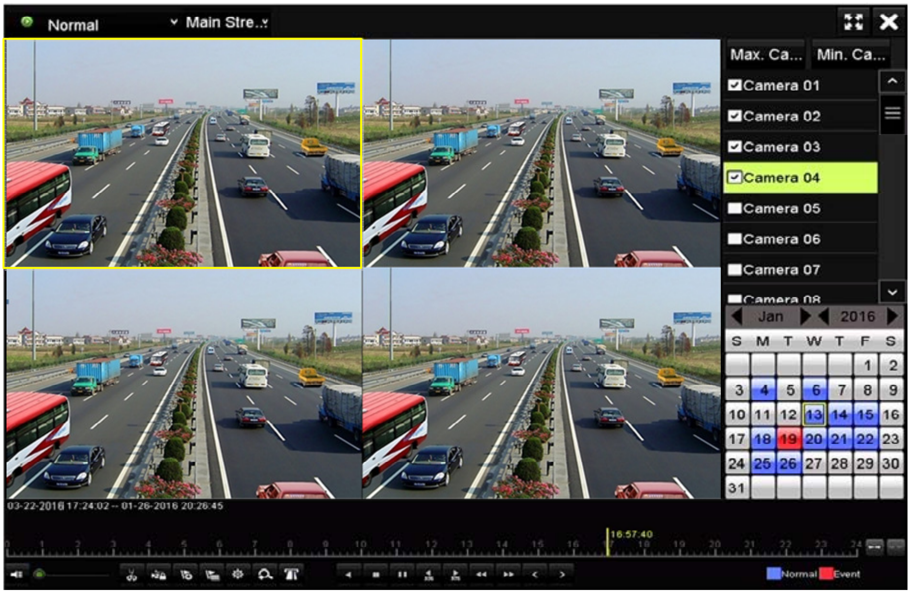


Figure 130, 4-ch Synchronous Playback Interface

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

5.13.4 File Management

Purpose

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

1. Enter the playback interface.

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

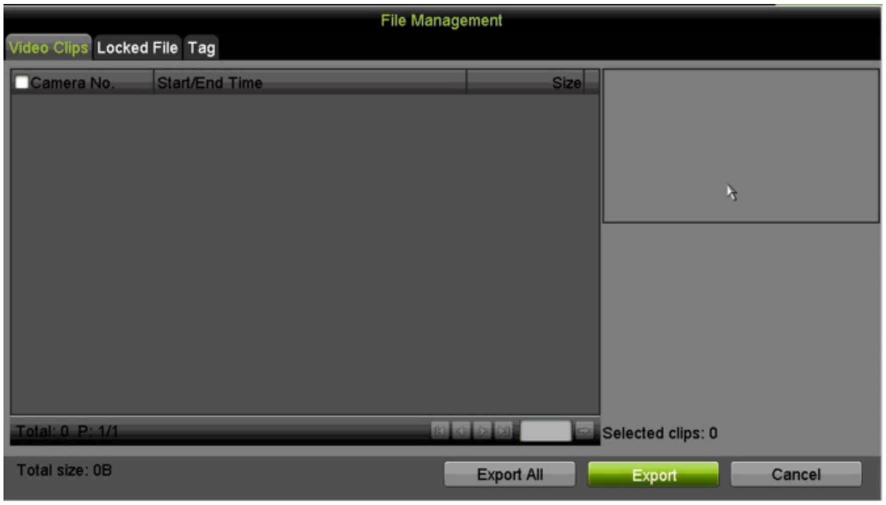


Figure 131, File Management

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

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

5.14 Backup

Before You Start

Attach the backup device(s) to the device.

5.14.1 Backup by Normal Video/Picture Search

Purpose

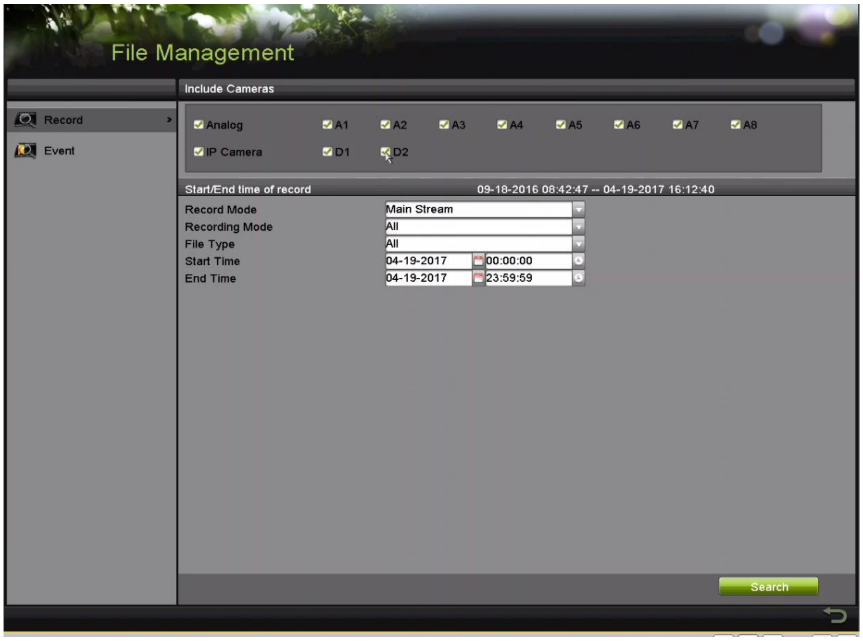
The record files or pictures can be backed up to various devices such as USB devices (USB flash drives, USB HDDs, USB writer), SATA writer, and e-SATA HDD.

5.14.1.1 Using USB Flash Drives, USB HDDs

1. Go to Menu > Export > Normal/Picture.

2. Select the cameras to search.

3. Set the search condition and click **Search** to enter the search result interface.



Include Cameras

☑ Analog ☑ A1 ☑ A2 ☑ A3 ☑ A4 ☑ A5 ☑ A6 ☑ A7 ☑ A8

☑ IP Camera ☑ D1 ☑ D2

Start/End time of record 09-18-2016 08:42:47 -- 04-19-2017 16:12:40

Record Mode	Main Stream
Recording Mode	All
File Type	All
Start Time	04-19-2017 00:00:00
End Time	04-19-2017 23:59:59

Figure 132, Normal Video Search for Backup

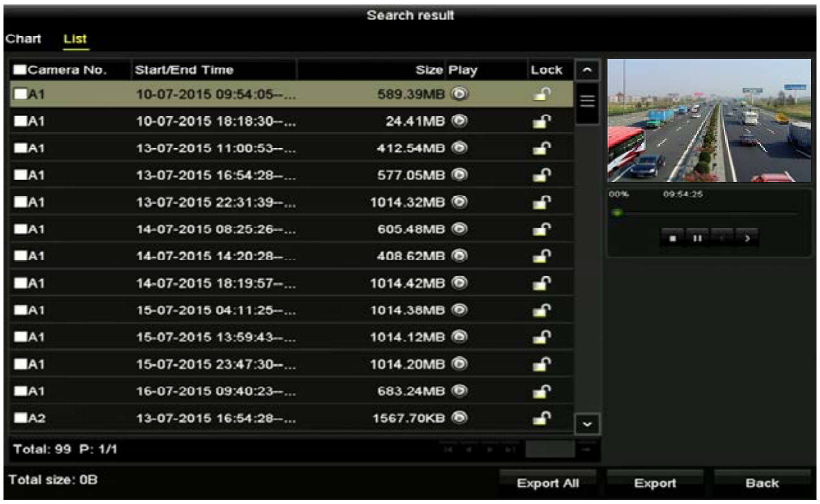
4. The matched video files are displayed in **Chart** or **List** display mode.

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

6. Check the checkbox before 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.



Search result

Chart List

Camera No.	Start/End Time	Size	Play	Lock
□A1	10-07-2015 09:54:05--...	589.39MB	◉	🔓
■A1	10-07-2015 18:18:30--...	24.41MB	◉	🔓
■A1	13-07-2015 11:00:53--...	412.54MB	◉	🔓
■A1	13-07-2015 16:54:28--...	577.05MB	◉	🔓
■A1	13-07-2015 22:31:39--...	1014.32MB	◉	🔓
■A1	14-07-2015 08:25:26--...	605.48MB	◉	🔓
■A1	14-07-2015 14:20:28--...	408.62MB	◉	🔓
■A1	14-07-2015 18:19:57--...	1014.42MB	◉	🔓
■A1	15-07-2015 04:11:25--...	1014.38MB	◉	🔓
■A1	15-07-2015 13:59:43--...	1014.12MB	◉	🔓
■A1	15-07-2015 23:47:30--...	1014.20MB	◉	🔓
■A1	16-07-2015 09:40:23--...	683.24MB	◉	🔓
■A2	13-07-2015 16:54:28--...	1567.70KB	◉	🔓

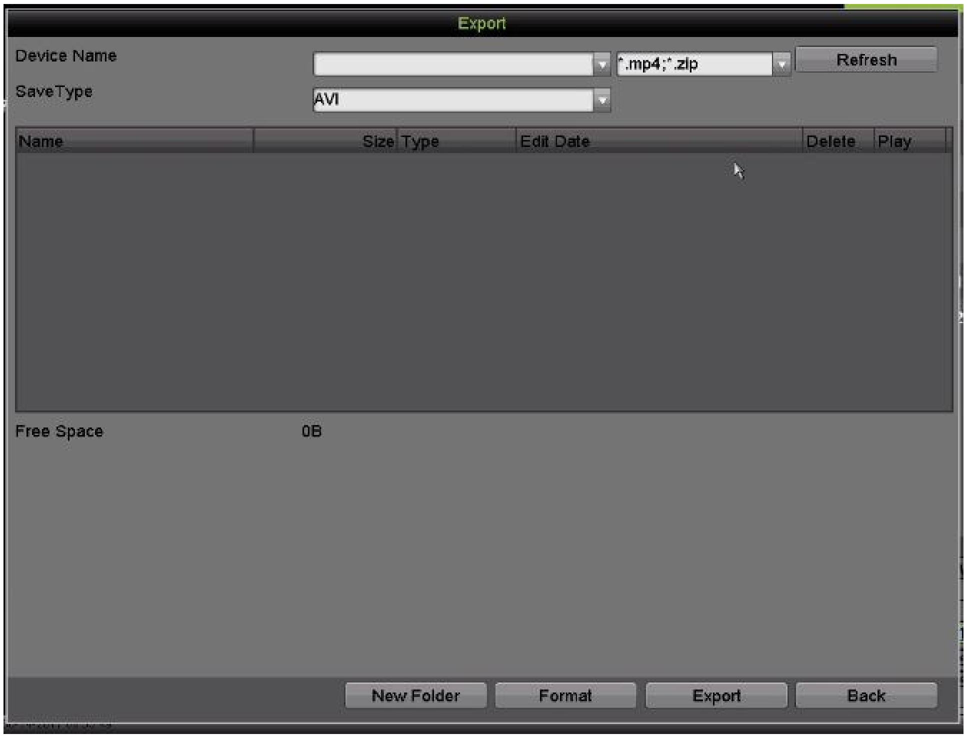
Total: 99 P: 1/1

Total size: 0B

Figure 133, Result of Normal Video Search for Backup

7. Select video files from the **Chart** or **List** to export, and click the button **Export** to enter the **Export** interface.

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



Export

Device Name: *.mp4;*.zip

SaveType: AVI

Name	Size	Type	Edit Date	Delete	Play

Free Space: 0B

Figure 134, Export by Normal Video Search using USB Flash Drive

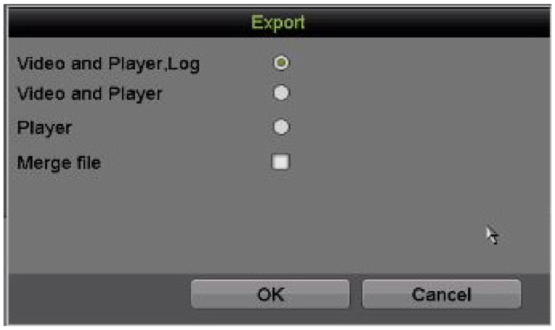
9. Select the backup device from the drop-down list and you can also select the file format to filter the files existing in the backup device.

10. Select the saving type.

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

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

13. Click **OK** to confirm.

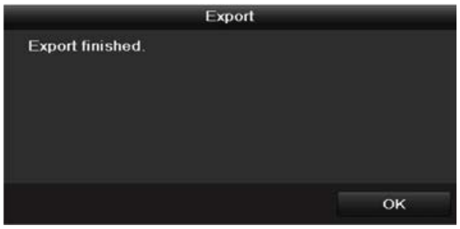


Export

Video and Player,Log ●
Video and Player ○
Player ○
Merge file □

Figure 135, Select File or Player for Backup

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



Export

Export finished.

Figure 136, Export Finished

NOTE

The backup of pictures using USB writer or SATA writer has the same operating instructions. Refer to steps described above.

5.14.2 Backup by Event Search

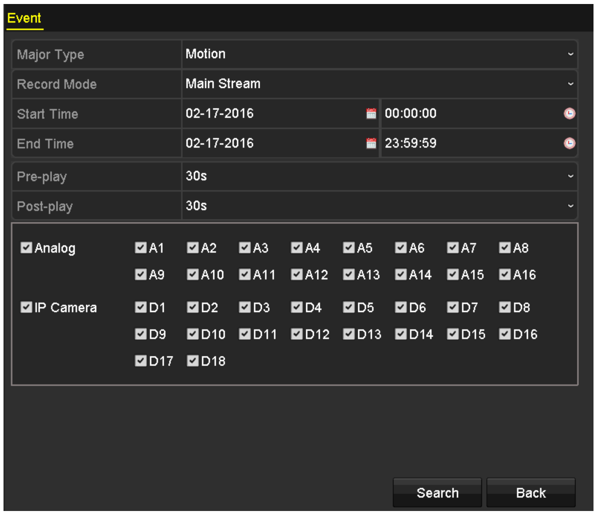
Purpose

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

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

2. Select the cameras to search.

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



Event

Major Type	Motion	
Record Mode	Main Stream	
Start Time	02-17-2016	00:00:00
End Time	02-17-2016	23:59:59
Pre-play	30s	
Post-play	30s	

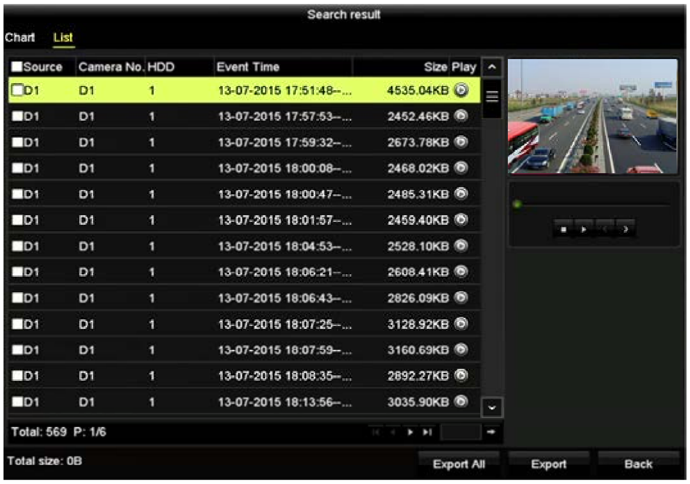
☑ Analog ☑ A1 ☑ A2 ☑ A3 ☑ A4 ☑ A5 ☑ A6 ☑ A7 ☑ A8
☑ A9 ☑ A10 ☑ A11 ☑ A12 ☑ A13 ☑ A14 ☑ A15 ☑ A16

☑ IP Camera ☑ D1 ☑ D2 ☑ D3 ☑ D4 ☑ D5 ☑ D6 ☑ D7 ☑ D8
☑ D9 ☑ D10 ☑ D11 ☑ D12 ☑ D13 ☑ D14 ☑ D15 ☑ D16
☑ D17 ☑ D18

Figure 137, Event Search for Backup

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

5. Select video files from the **Chart** or **List** interface to export.



Search result

□ Source	Camera No.	HDD	Event Time	Size	Play
□ D1	D1	1	13-07-2015 17:51:48--...	4535.04KB	
□ D1	D1	1	13-07-2015 17:57:53--...	2452.46KB	
□ D1	D1	1	13-07-2015 17:59:32--...	2673.78KB	
□ D1	D1	1	13-07-2015 18:00:08--...	2468.02KB	
□ D1	D1	1	13-07-2015 18:00:47--...	2485.31KB	
□ D1	D1	1	13-07-2015 18:01:57--...	2459.40KB	
□ D1	D1	1	13-07-2015 18:04:53--...	2528.10KB	
□ D1	D1	1	13-07-2015 18:06:21--...	2608.41KB	
□ D1	D1	1	13-07-2015 18:06:43--...	2826.09KB	
□ D1	D1	1	13-07-2015 18:07:25--...	3128.92KB	
□ D1	D1	1	13-07-2015 18:07:59--...	3160.69KB	
□ D1	D1	1	13-07-2015 18:08:35--...	2892.27KB	
□ D1	D1	1	13-07-2015 18:13:56--...	3035.90KB	

Total: 569 P: 1/6

Total size: 0B

Figure 138, Result of Event Search

6. Export the video files.

5.14.3 Back Up Video Clips

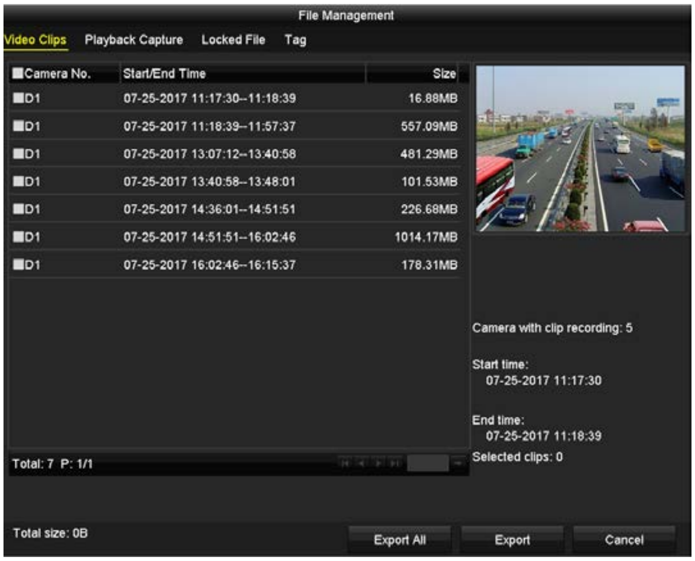
Purpose

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

1. Go to Menu > Playback.

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

3. Click ⚙ to enter the file management interface.



File Management

■Camera No.	Start/End Time	Size
■D1	07-25-2017 11:17:30--11:18:39	16.88MB
■D1	07-25-2017 11:18:39--11:57:37	557.09MB
■D1	07-25-2017 13:07:12--13:40:58	481.29MB
■D1	07-25-2017 13:40:58--13:48:01	101.53MB
■D1	07-25-2017 14:36:01--14:51:51	226.68MB
■D1	07-25-2017 14:51:51--16:02:46	1014.17MB
■D1	07-25-2017 16:02:46--16:15:37	178.31MB

Camera with clip recording: 5

Start time:
07-25-2017 11:17:30

End time:
07-25-2017 11:18:39

Selected clips: 0

Total: 7 P: 1/1

Total size: 0B

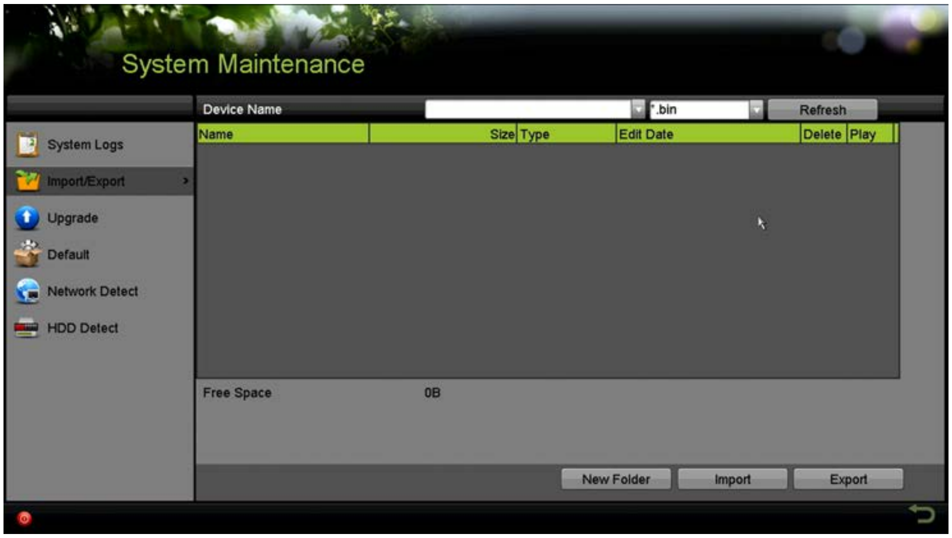
Figure 139, Video Clips Export Interface

4. Export the video clips in playback.

5.15 Managing Backup Devices

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

1. Enter the **Export** interface.



System Maintenance

Device Name *.bin

Name	Size	Type	Edit Date	Delete	Play

Free Space 0B

Figure 140, Storage Device Management

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

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

NOTE

If the inserted storage device is not recognized:

Click **Refresh**.

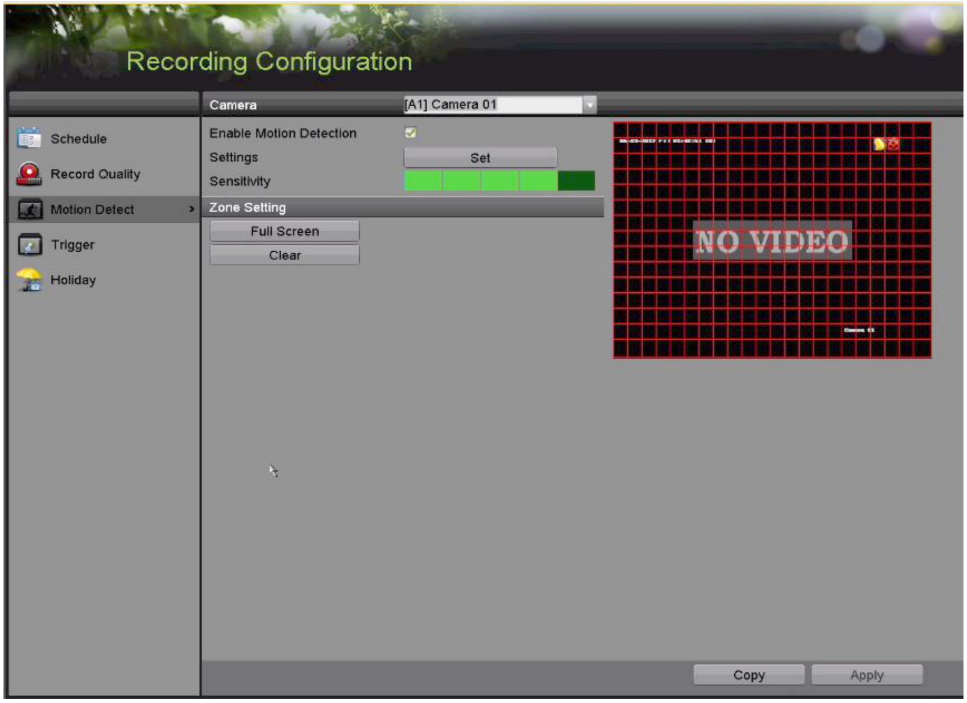
Reconnect device.

Check for compatibility from vendor.

6 Alarm Settings

6.1 Setting Motion Detection

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



Camera [A1] Camera 01

Enable Motion Detection ☑

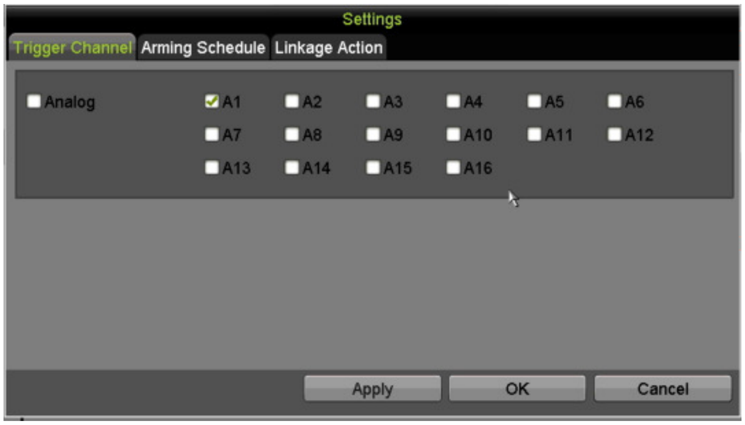
Figure 141, Motion Detection Setup Interface

2. Select a camera you want to set up motion detection.

3. Set detection area and sensitivity.

4. 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.

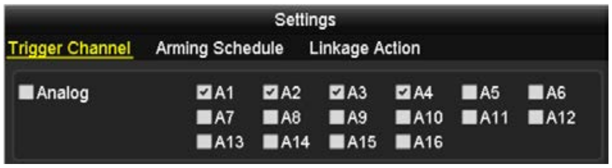
5. Click **Set** to set alarm response actions.



□ Analog ☑ A1 □ A2 □ A3 □ A4 □ A5 □ A6
□ A7 □ A8 □ A9 □ A10 □ A11 □ A12
□ A13 □ A14 □ A15 □ A16

Figure 142, Motion Detection Settings

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



□ Analog ☑ A1 ☑ A2 ☑ A3 ☑ A4 □ A5 □ A6
□ A7 □ A8 □ A9 □ A10 □ A11 □ A12
□ A13 □ A14 □ A15 □ A16

Figure 143, Set Trigger Camera of Motion Detection

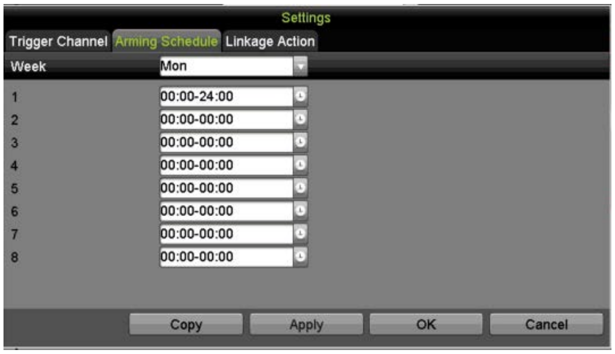
7. Set arming schedule of the channel.

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

9. Choose a day of the week, with up to eight time periods within each day. Click **Copy** to copy the time period settings to other day(s).

NOTE

Time periods must not repeat or overlap.



Week Mon

1 00:00-24:00
2 00:00-00:00
3 00:00-00:00
4 00:00-00:00
5 00:00-00:00
6 00:00-00:00
7 00:00-00:00
8 00:00-00:00

Figure 144, Set Motion Detection Arming Schedule

10. Click **Linkage Action** tab to set up alarm response actions of motion alarm.

11. Repeat the above steps to set up arming schedule for other days of the week.

12. Click **OK** to complete the motion detection settings of the channel.

13. To set motion detection for another channel, repeat the above steps or copy the above settings to it.

NOTE

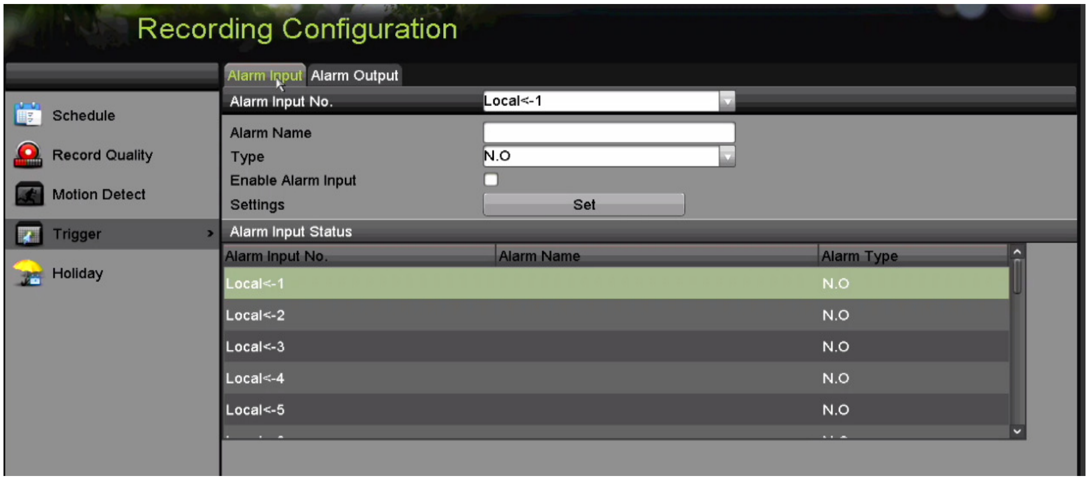
You cannot copy the “Trigger Channel” action.

6.2 Setting Sensor Alarms

Purpose

Set up handling method of an external sensor alarm.

1. Go to Menu > Recording Configuration > Trigger.



Alarm Input No.: Local<-1
Alarm Name:
Type: N.O
Enable Alarm Input: ☐
Settings: Set

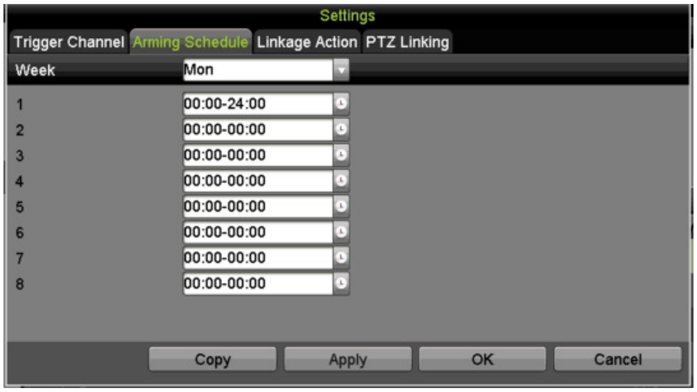
Alarm Input Status

Alarm Input No.	Alarm Name	Alarm Type
Local<-1		N.O
Local<-2		N.O
Local<-3		N.O
Local<-4		N.O
Local<-5		N.O

Figure 145, Alarm Input Settings Interface

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

3. Check the **Enable** checkbox and click **Set** to set its alarm response actions.



Week: Mon

1	00:00-24:00
2	00:00-00:00
3	00:00-00:00
4	00:00-00:00
5	00:00-00:00
6	00:00-00:00
7	00:00-00:00
8	00:00-00:00

Figure 146, Set Arming Schedule of Alarm Input

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

5. Select **Arming Schedule** tab to set the channel’s arming schedule.

6. Select a day of the week, with a maximum of eight time periods within each day.

NOTE

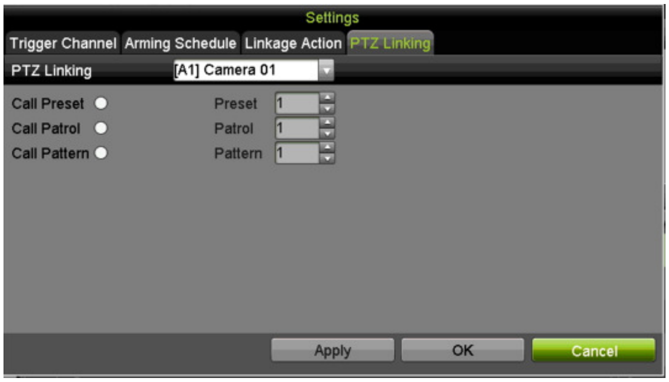
Time periods must not repeat or overlap.

7. Select **Linkage Action** tab to set up alarm response actions of the alarm input.
8. Repeat the above steps to set up arming schedule for other days of the week. Use **Copy** to copy an arming schedule to other days.
9. (Optional) Select **PTZ Linking** tab and set PTZ linkage of the alarm input.
10. 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.



PTZ Linking [A1] Camera 01

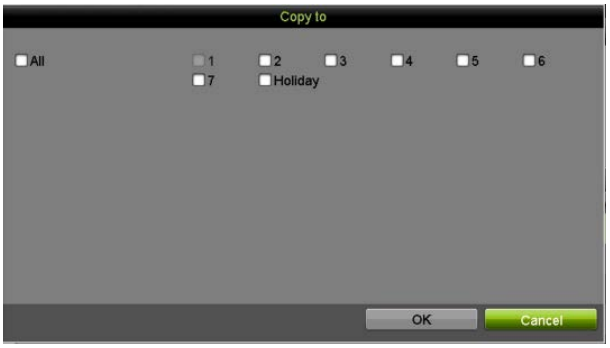
Call Preset ○ Preset 1

Call Patrol ○ Patrol 1

Call Pattern ○ Pattern 1

Figure 147, Set PTZ Linking of Alarm Input

11. To set the handling action of another alarm input, repeat the above steps or copy the above settings to it.



□All □1 □2 □3 □4 □5 □6 □7 □Holiday

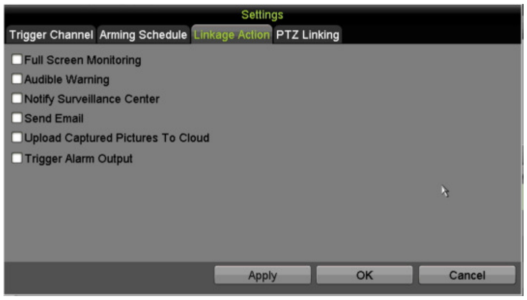
Figure 148, Copy Settings of Alarm Input

12. (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. The selected linkage actions include Full Screen Monitoring, Audible Warning, Notify Surveillance Center, Send E-mail, Upload Captured Pictures to Cloud, and Trigger Alarm Output.



☐ Full Screen Monitoring
☐ Audible Warning
☐ Notify Surveillance Center
☐ Send Email
☐ Upload Captured Pictures To Cloud
☐ Trigger Alarm Output

Figure 149, Disarm Linkage Actions

NOTE

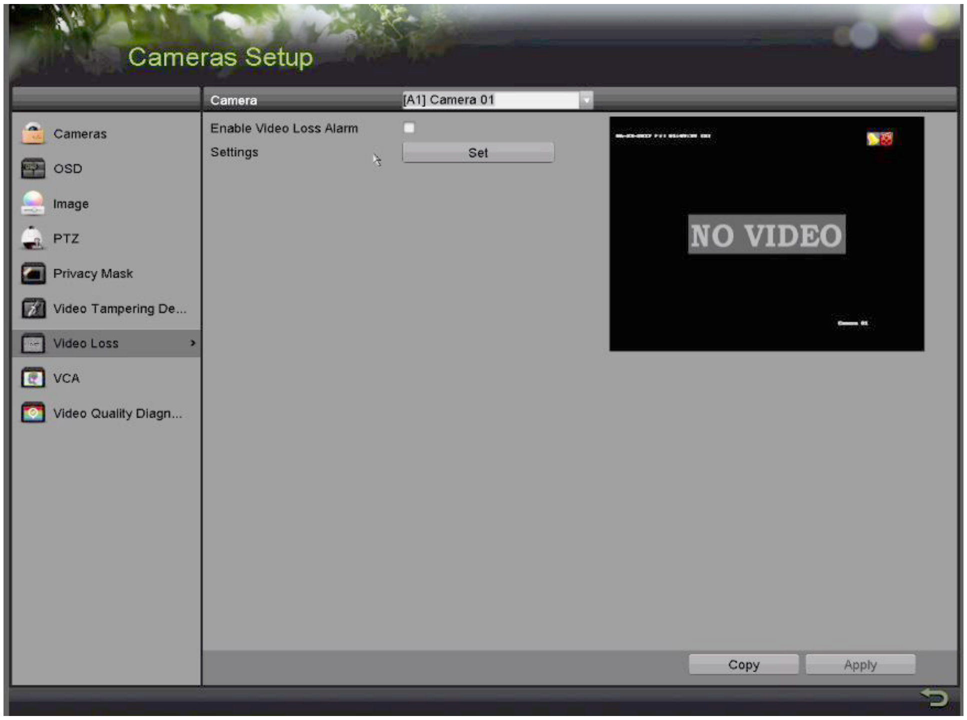
When alarm input 1 (Local <- 1) is enabled with one-key disarming, the other alarm input settings are not configurable.

6.2.1 Detecting Video Loss

Purpose

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

1. Go to Menu > Camera > Video Loss.



Camera [A1] Camera 01
Enable Video Loss Alarm ☐
Settings Set

Figure 150, Video Loss Setup Interface

2. Select a **Camera** you want to detect.

3. Set up handling method of video loss.

4. Check the Enable Video Loss Alarm checkbox.

5. Click **Set** to set up handling method of video loss.

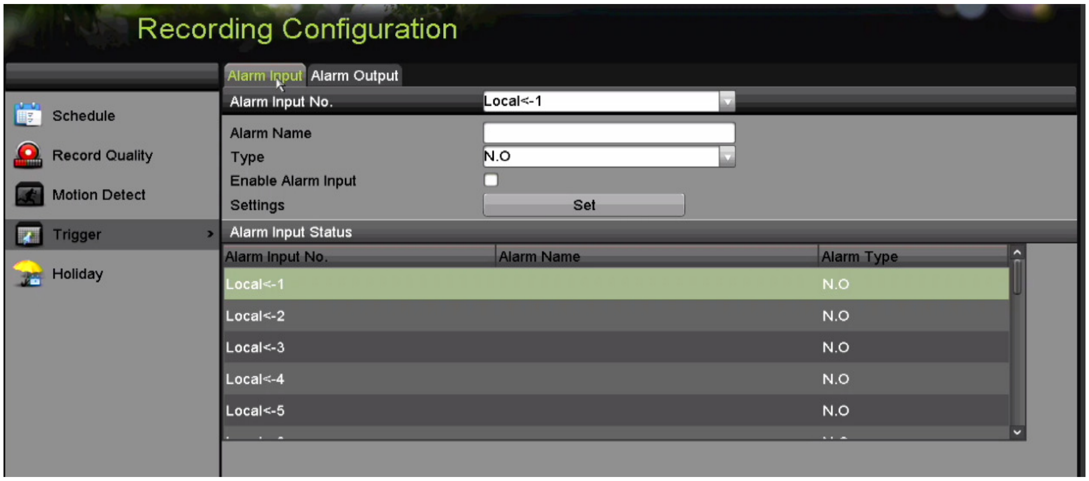
6. Set arming schedule of the channel.

7. Select **Arming Schedule** tab to set the channel’s arming schedule.

8. Choose a day of the week, with up to eight time periods within each day. Click **Copy** to copy the time period settings to other day(s).

NOTE

Time periods cannot repeat or overlap.



Alarm Input No.	Local<-1
Alarm Name	
Type	N.O
Enable Alarm Input	☐
Settings	Set

Alarm Input Status

Alarm Input No.	Alarm Name	Alarm Type
Local<-1		N.O
Local<-2		N.O
Local<-3		N.O
Local<-4		N.O
Local<-5		N.O

Figure 151, Set Arming Schedule of Video Loss

9. Repeat the above steps to set arming schedule of other days of the week. Use **Copy** to copy an arming schedule to other days.

10. Select **Linkage Action** tab to set up alarm response action of video loss.

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

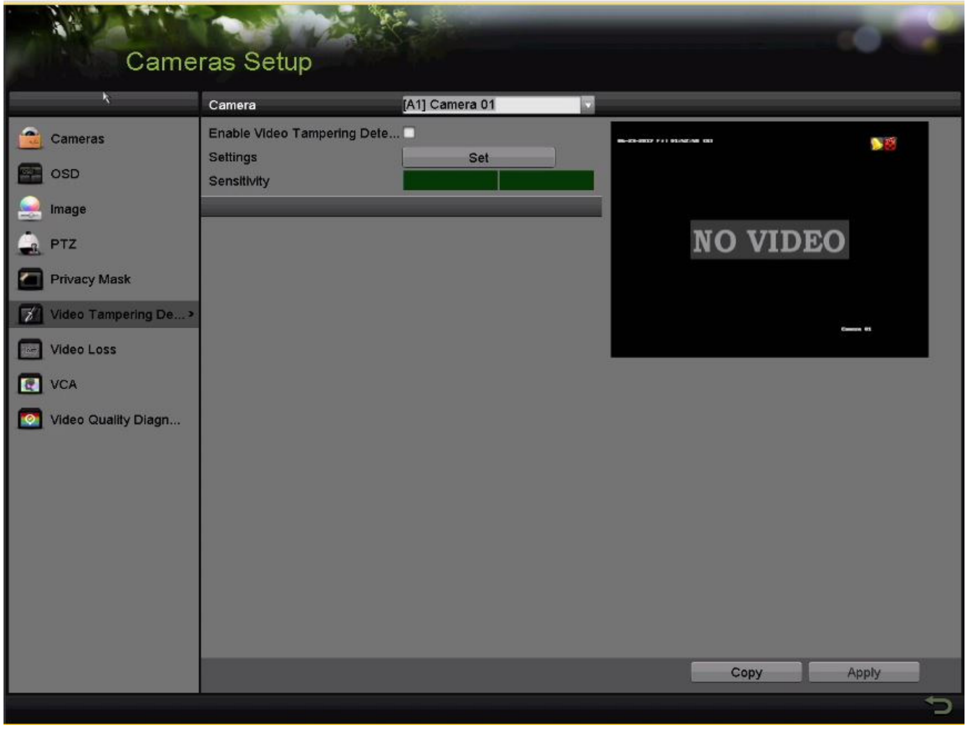
12. Repeat the above steps to finish settings of other channels, or click **Copy** to copy the above settings to them.

6.2.2 Detecting Video Tampering

Purpose

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

1. Go to Menu > Camera > Video Tampering Detection.



Camera [A1] Camera 01

Enable Video Tampering Dete... □

Settings Set

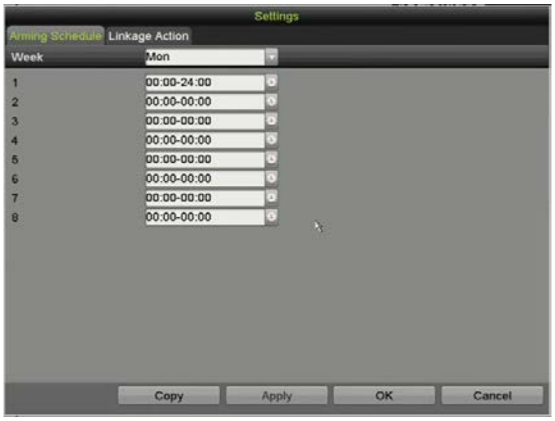
Sensitivity

Figure 152, Video Tampering Interface

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

NOTE

Time periods cannot repeat or overlap.



Week	Mon
1	00:00-24:00
2	00:00-00:00
3	00:00-00:00
4	00:00-00:00
5	00:00-00:00
6	00:00-00:00
7	00:00-00:00
8	00:00-00:00

Figure 153, Set Arming Schedule of Video Tampering

8. Select **Linkage Action** tab to set alarm response actions of video tampering alarm.

9. Repeat the above steps to set arming schedule of other days of a week. Use **Copy** to copy an arming schedule to other days.

10. Click **OK** to complete the video tampering settings of the channel.

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

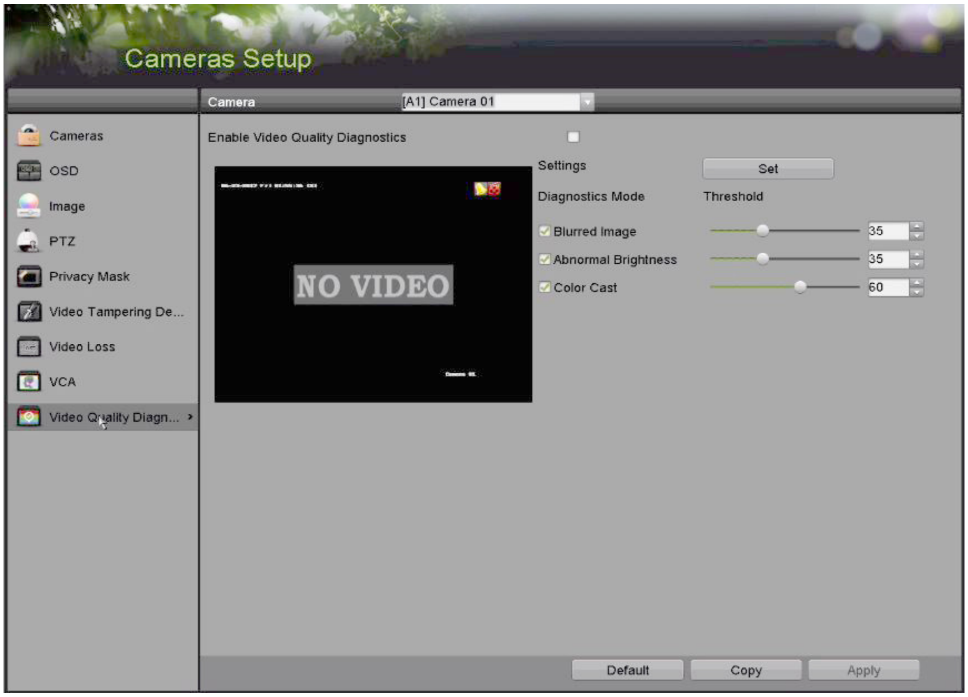
12. Click **Apply** to save and activate the settings.

6.3 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 threshold of the diagnosing and the linkage actions.

1. Go to Menu > Camera > Video Quality Diagnostics.



Camera: [A1] Camera 01

Enable Video Quality Diagnostics □

Settings: Set

Diagnostics Mode	Threshold
☑ Blurred Image	35
☑ Abnormal Brightness	35
☑ Color Cast	60

Figure 154, Video Quality Diagnostics Interface

2. Select a **Camera** you want to detect video tampering.

3. Check the checkbox of Enable Video Quality Diagnostics.

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**.

5. Check the corresponding checkbox of the diagnostic type, and adjust the threshold of it by dragging the bar.

NOTE

The higher the threshold set, the harder the exception will be to detect.

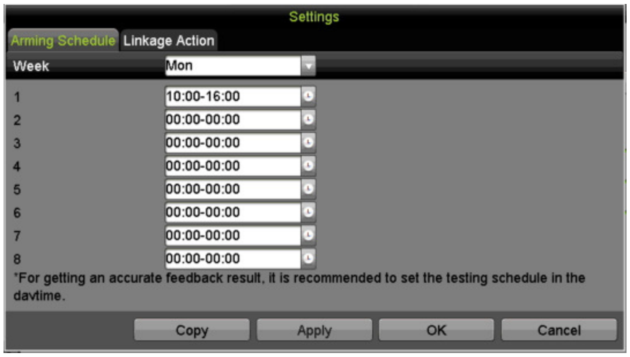
6. Click **Set** to set handling method of video quality diagnostics. Set arming schedule and alarm response actions of the channel.

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

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

NOTE

Time periods cannot repeat or overlap.



Week	Mon
1	10:00-16:00
2	00:00-00:00
3	00:00-00:00
4	00:00-00:00
5	00:00-00:00
6	00:00-00:00
7	00:00-00:00
8	00:00-00:00

*For getting an accurate feedback result, it is recommended to set the testing schedule in the davtime.

Figure 155, Set Arming Schedule of Video Quality Diagnostics

   3) Select **Linkage Action** tab to set alarm response actions of video quality diagnostics alarm.

7. Repeat the above steps to set arming schedule of other days of the week. Use **Copy** to copy an arming schedule to other days.

   1) Click **OK** to complete the video quality diagnostics settings of the channel.

8. Click **Apply** to save and activate settings.

9. (Optional) you can copy the same settings to other cameras by clicking **Copy**.

6.4 Handling Exceptions

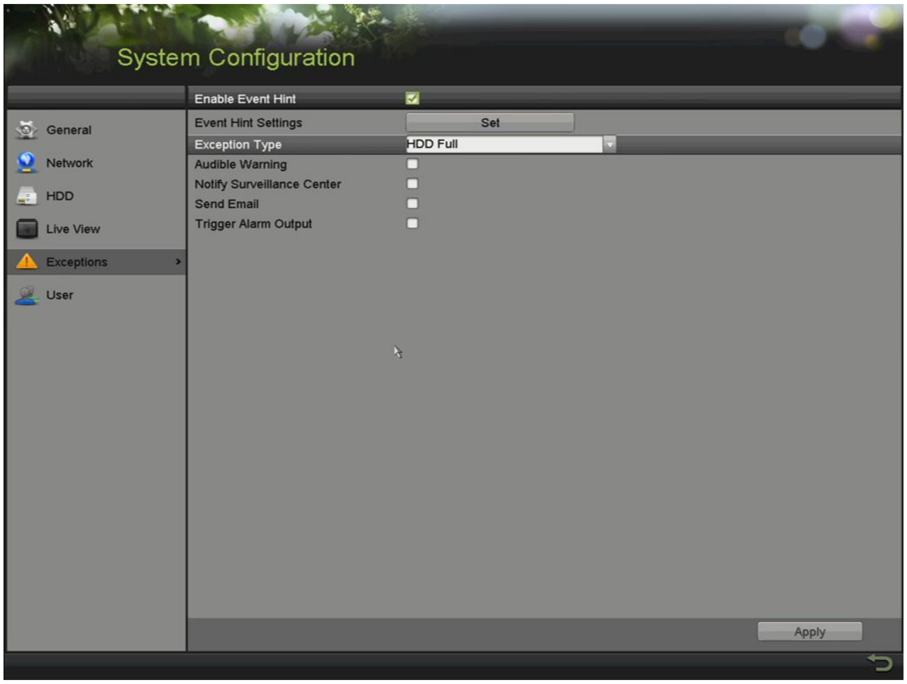
Purpose

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 smaller than the recording resolution
- **Record/Capture Exception:** No space for saving recorded files or captured pictures

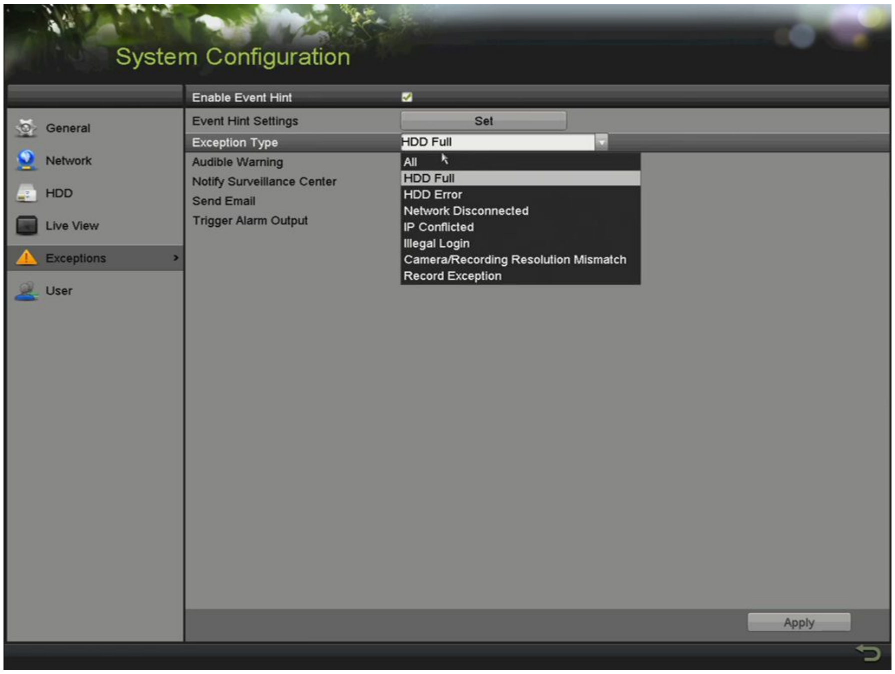
1. Go to Menu > Configuration > Exceptions.



Enable Event Hint ☑
Event Hint Settings
Exception Type: HDD Full
Audible Warning □
Notify Surveillance Center □
Send Email □
Trigger Alarm Output □

Figure 156, Exception Settings Interface

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



Enable Event Hint ☑

Event Hint Settings: Set

Exception Type: HDD Full

Audible Warning

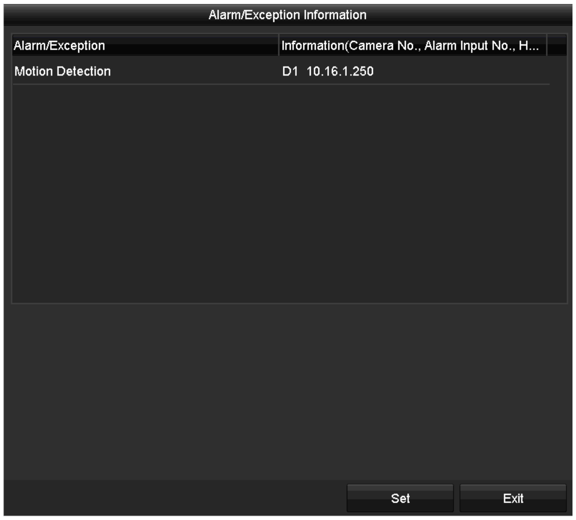
Notify Surveillance Center

Send Email

Trigger Alarm Output

Figure 157, Event Hint Settings

The ⚠ appears in the live view interface, and you can view the detailed information of the exceptional event. Click **Set**, then you can select the detailed event hint for display.



Alarm/Exception Information

Alarm/Exception	Information(Camera No., Alarm Input No., H...
Motion Detection	D1 10.16.1.250

Figure 158, Detailed Event

3. Set the alarm linkage actions.

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

7 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 > Configuration > Live View.

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

- **Audible Warning**

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

- **Notify Surveillance Center**

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

  NOTE

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

- **Send E-Mail**

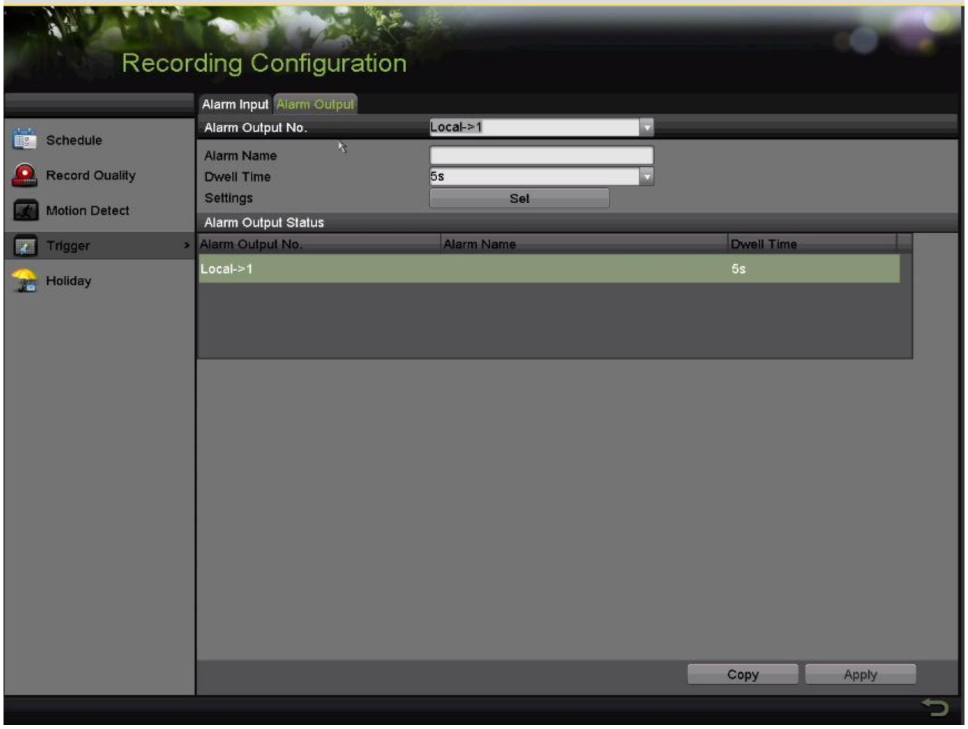
  Send an e-mail with alarm information to a user or users when an alarm is detected.

- **Trigger Alarm Output**

  Trigger an alarm output when an alarm is triggered.

1. Go to Menu > Recording Configuration > Trigger.

2. Select an alarm output and set the alarm name and dwell time.



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

Alarm Output Status

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

Figure 159, Alarm Output Settings Interface

NOTE

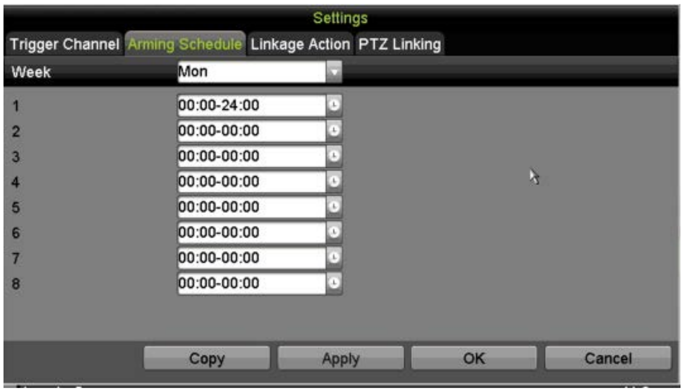
If **Manually Clear** is selected in the **Dwell Time** drop-down list, clear it by going to **Menu > Manual > Alarm**.

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

4. Choose a day of the week, with up to eight time periods each day.

NOTE

Time periods cannot repeat or overlap.



Week Mon

1	00:00-24:00
2	00:00-00:00
3	00:00-00:00
4	00:00-00:00
5	00:00-00:00
6	00:00-00:00
7	00:00-00:00
8	00:00-00:00

Figure 160, Set Arming Schedule of Alarm Output

5. Repeat the above steps to set the arming schedule for other days of the week. Click **Copy** to copy an arming schedule to other days.

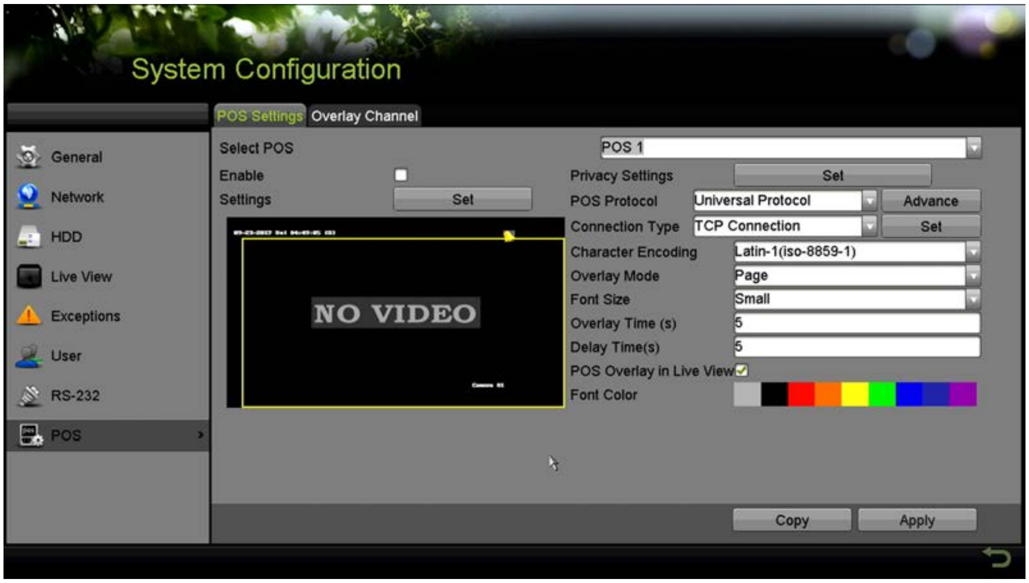
6. Click **OK** to complete the arming schedule setting of alarm output.

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

8 POS Configuration

8.1 Configuring POS Settings

1. Go to Menu > System Configuration > POS > POS Settings.
2. Select POS from the drop-down list. Up to eight POS units are selectable.
3. Check the checkbox to enable the POS function.



Select POS: POS 1

Enable: □

Settings: Set

Privacy Settings: Set

POS Protocol: Universal Protocol

Connection Type: TCP Connection

Character Encoding: Latin-1(iso-8859-1)

Overlay Mode: Page

Font Size: Small

Overlay Time (s): 5

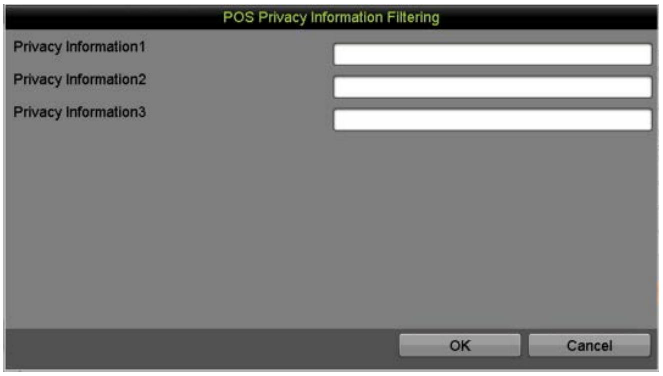
Delay Time(s): 5

POS Overlay in Live View: ☑

Font Color

Figure 161, POS Settings

4. Filter the POS privacy information if needed.
   1) Click **Set** after **Privacy Settings** to enter POS Privacy Information Filtering interface.



Privacy Information1:

Privacy Information2:

Privacy Information3:

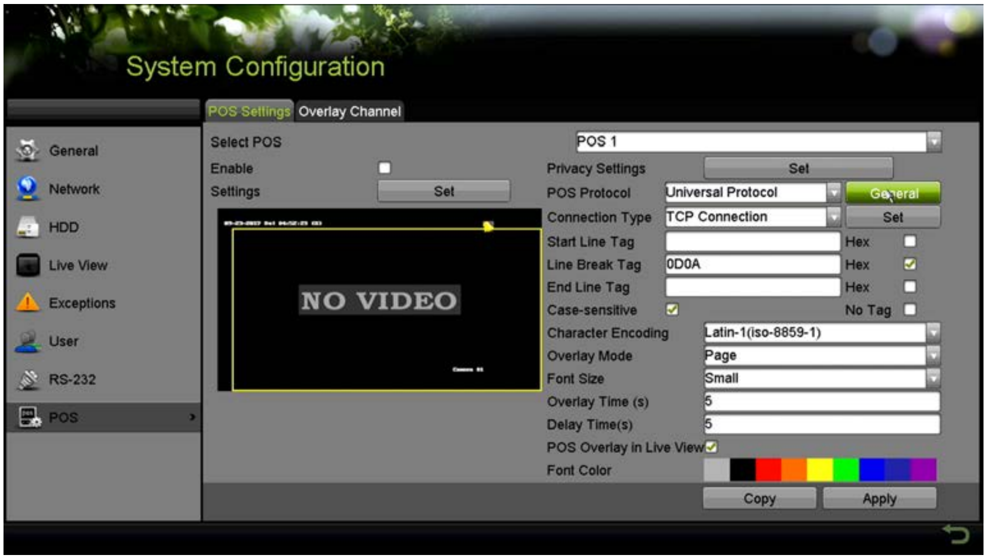
Figure 162, POS Privacy Information Filtering

   2) Edit the **Privacy Information** in the text field to hide the input information overlay. Up to three pieces of privacy information can be edited, with no more than 32 characters input for each piece of information.

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

5. Set the POS protocol to Universal Protocol, EPSON, AVE, or NUCLEUS.

- **Universal Protocol**
  Click **Advanced** to expand more settings when selecting the universal protocol. You can set the start line tag, line break tag, and end line tag for the POS overlay characters, and the case-sensitive property of the characters.



Select POS: POS 1
Enable ☐
Privacy Settings
Settings
POS Protocol: Universal Protocol
Connection Type: TCP Connection
Start Line Tag: Hex ☐
Line Break Tag: 0D0A Hex ☑
End Line Tag: Hex ☐
Case-sensitive ☑ No Tag ☐
Character Encoding: Latin-1(iso-8859-1)
Overlay Mode: Page
Font Size: Small
Overlay Time (s): 5
Delay Time(s): 5
POS Overlay in Live View ☑
Font Color

Figure 163, Universal Protocol Settings

- **NUCLEUS**
  If you select NUCLEUS protocol, reboot the device to have the new settings take effect.

  1) Click **Set** to enter the NUCLEUS Settings interface.

  2) Edit the Employee, Shift, and Terminal information. No more than 32 characters can be input.

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

NOTE

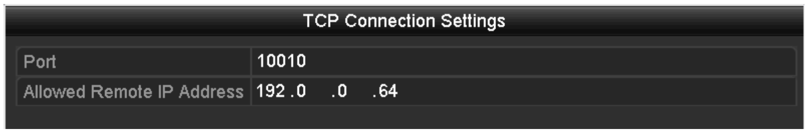
If you select NUCLEUS protocol, the connection type defaults to be RS-232, and all the other POS protocol will change to be NUCLEUS.

Set **Usage** to be Transparent Channel for RS-232 settings in **Menu > Configuration > RS-232** first.

1. Set the Connection Type to TCP, UDP, Multicast, RS-232, USB->RS-232, or Sniff, and click **Set** to configure the parameters for each connection type.

- **TCP Connection**

When using TCP connection, the port must be set from 0 to 65535, and the port for each POS machine must be unique. Input the Allowed Remote IP Address for connecting the DVR and the POS machine via TCP.



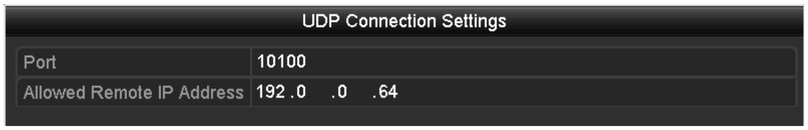
TCP Connection Settings

Port	10010
Allowed Remote IP Address	192 .0 .0 .64

Figure 164, TCP Connection Settings

- **UDP Connection**

  When using UDP connection, the port must be set from 0 to 65535, and the port for each POS machine must be unique. Input the Allowed Remote IP Address for connecting the DVR and the POS machine via UDP.



UDP Connection Settings

Port	10100
Allowed Remote IP Address	192 .0 .0 .64

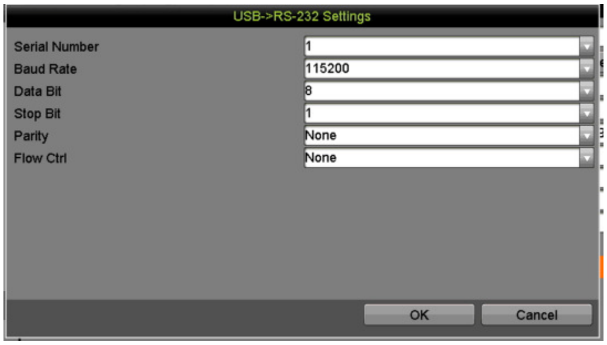
Figure 165, UDP Connection Settings

- **USB -> RS-232 Connection**

  Configure the port parameters of USB-to-RS-232 convertor, including the serial number of port, baud rate, data bit, stop bit, parity, and flow ctrl.

NOTE

When using USB -> RS-232 convertor mode, the port of USB-to-RS-232 convertor and the POS must correspond to each other, e.g., POS1 must be connected to port1 of the convertor.



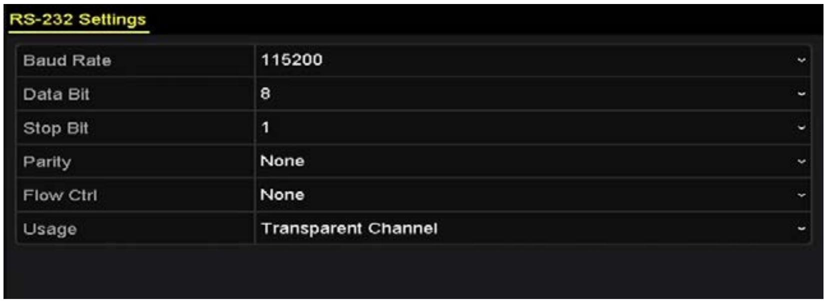
USB->RS-232 Settings

Serial Number	1
Baud Rate	115200
Data Bit	8
Stop Bit	1
Parity	None
Flow Ctrl	None

Figure 166, USB-to-RS-232 Settings

- **RS-232 Connection**

  Connect the DVR and the POS machine via RS-232. The RS-232 settings can be configured in **Menu > Configuration > RS-232**. The **Usage** must be set to Transparent Channel.



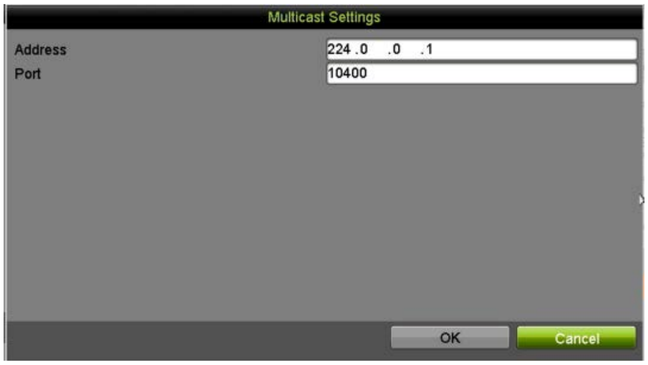
RS-232 Settings

Baud Rate	115200
Data Bit	8
Stop Bit	1
Parity	None
Flow Ctrl	None
Usage	Transparent Channel

Figure 167, RS-232 Settings

- **Multicast Connection**

  When connecting the DVR and the POS machine via Multicast protocol, set the multicast address and port.



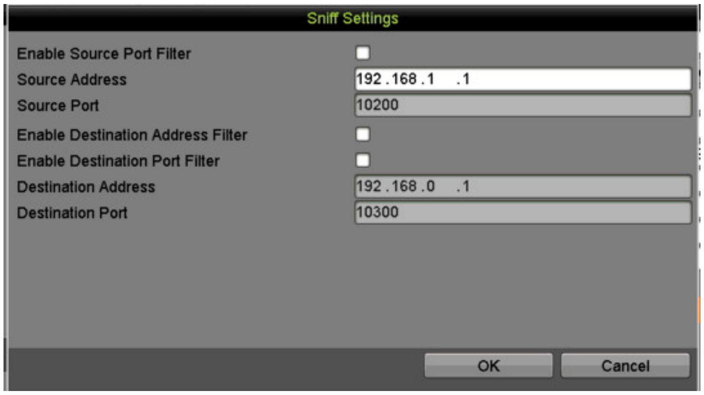
Multicast Settings

Address	224 .0 .0 .1
Port	10400

Figure 168, Multicast Settings

- **Sniff Connection**

  Connect the DVR and the POS machine via Sniff. Configure the source address and destination address settings.



Sniff Settings

Enable Source Port Filter	☐
Source Address	192 .168 .1 .1
Source Port	10200
Enable Destination Address Filter	☐
Enable Destination Port Filter	☐
Destination Address	192 .168 .0 .1
Destination Port	10300

Figure 169, Sniff Settings

2. Set other parameters of characters overlay.

   1) Select the character encoding format from the drop-down list.

   2) Select the overlay mode of the characters to display in scrolling or page mode.

3) Set the font size to small, medium, or large.

4) Set the overlay time of the characters. The value ranges from 5 to 3600 sec.

5) Set the delay time of the characters. The value ranges from 5 to 3600 sec.

6) (Optional) Check the checkbox to enable the **POS Overlay in Live View**.

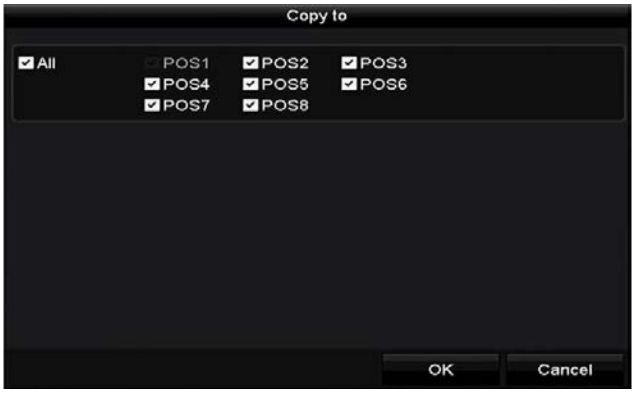
7) Select the font color for the characters.

NOTE

You can adjust the size and position of the textbox on the POS settings interface live view screen by dragging the frame.

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

4. (Optional) Click **Copy** to copy the current settings to other POS(s).



☑ All □ POS1 ☑ POS2 ☑ POS3 ☑ POS4 ☑ POS5 ☑ POS6 ☑ POS7 ☑ POS8

Figure 170, Copy POS Settings

8.2 Configuring Overlay Channel

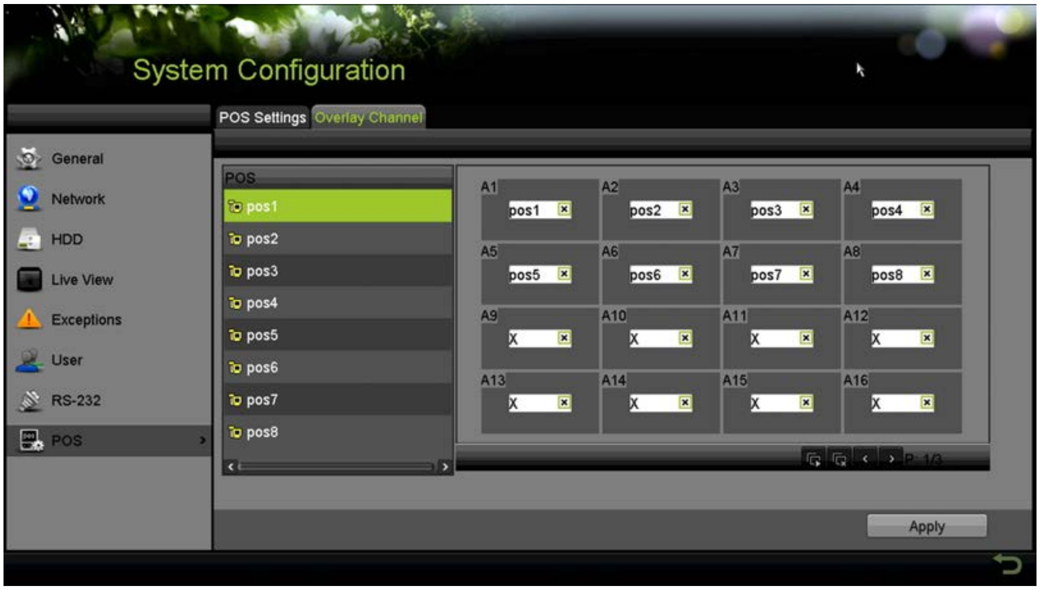
Purpose

You can assign the POS machine to the corresponding channel on which you want to overlay.

1. Go to Menu > Configuration > POS > Overlay Channel.

2. Click to select an analog or IP camera from the camera list on the right, and then click a POS item from the POS list you want to overlay on the selected camera.

3. Click ‹ or › to go to the previous or next page of cameras.



A1: pos1
A2: pos2
A3: pos3
A4: pos4
A5: pos5
A6: pos6
A7: pos7
A8: pos8
A9: X
A10: X
A11: X
A12: X
A13: X
A14: X
A15: X
A16: X

Figure 171, Overlay Channel Settings

4. You can also click to overlay all POS items to the first eight channels in order. Click to clear all POS overlay settings.

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

8.3 Configuring POS Alarm

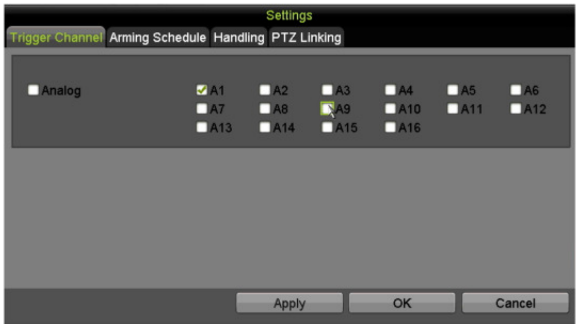
Purpose

Set the POS alarm parameters to trigger certain channels to start recording, or trigger full screen monitoring, audio warning, notifying the surveillance center, sending e-mail, and so on.

1. Go to Menu > Configuration > POS > POS Settings.

2. Follow the steps in Chapter 10.1 and 10.2 to configure the POS settings.

3. Click **Set** to enter the alarm settings interface.



□ Analog
☑ A1 □ A2 □ A3 □ A4 □ A5 □ A6
□ A7 □ A8 □ A9 □ A10 □ A11 □ A12
□ A13 □ A14 □ A15 □ A16

Figure 172, Set Trigger Cameras of POS

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

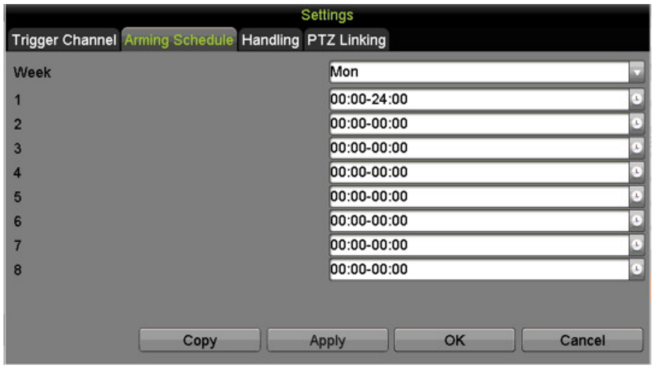
5. Set arming schedule of the channel.

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

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

NOTE

Time periods cannot repeat or overlap.



Week	Mon
1	00:00-24:00
2	00:00-00:00
3	00:00-00:00
4	00:00-00:00
5	00:00-00:00
6	00:00-00:00
7	00:00-00:00
8	00:00-00:00

Figure 173, Set Arming Schedule

6. Click the **Handling** tab to set up alarm response actions of POS alarm.

7. Repeat the above steps to set up arming schedule of other days of the week.

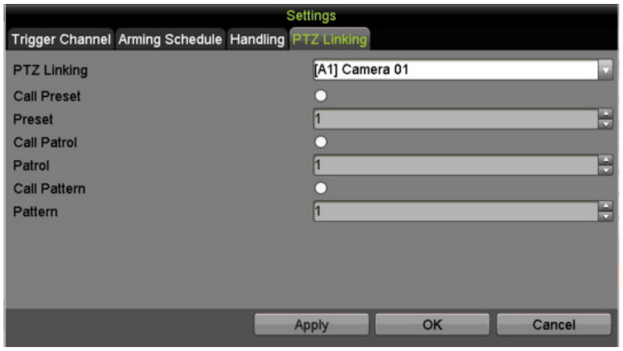
8. Click **OK** to complete the POS settings of the channel.

9. Select **PTZ Linking** tab and set PTZ linkage of the POS alarm.

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

NOTE

Ensure the PTZ or speed dome supports PTZ linkage.



PTZ Linking: [A1] Camera 01
Call Preset: ○
Preset: 1
Call Patrol: ○
Patrol: 1
Call Pattern: ○
Pattern: 1

Figure 174, Set PTZ Linking

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

9 VCA Alarm

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

Purpose

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

NOTE

HUI series supports line crossing detection and intrusion detection of all channels, and 2-ch sudden scene change detection. Channels with audio support 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 only enable one function.

9.1 Face Detection

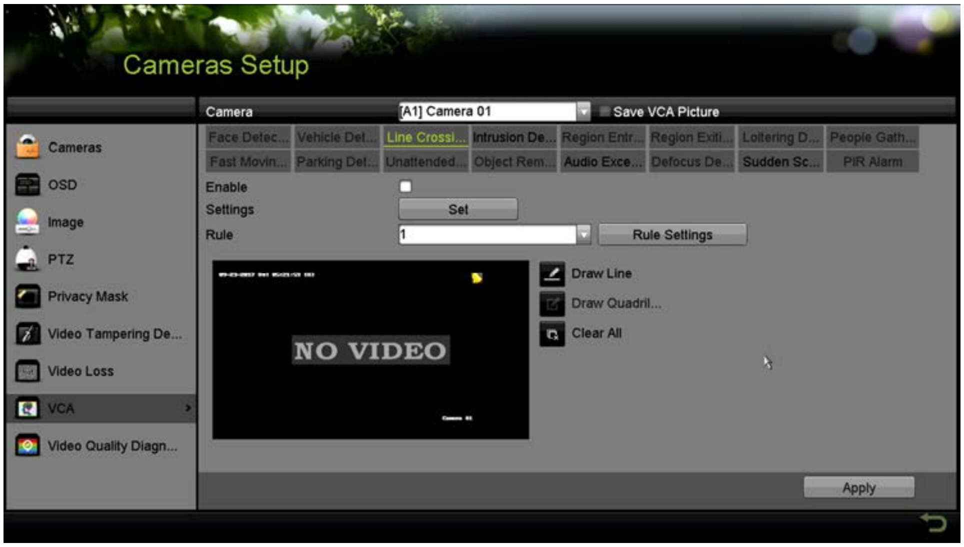
Purpose

The face detection function 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 to configure the VCA.

3. You can check the **Save VCA Picture** checkbox to save the captured VCA detection pictures.

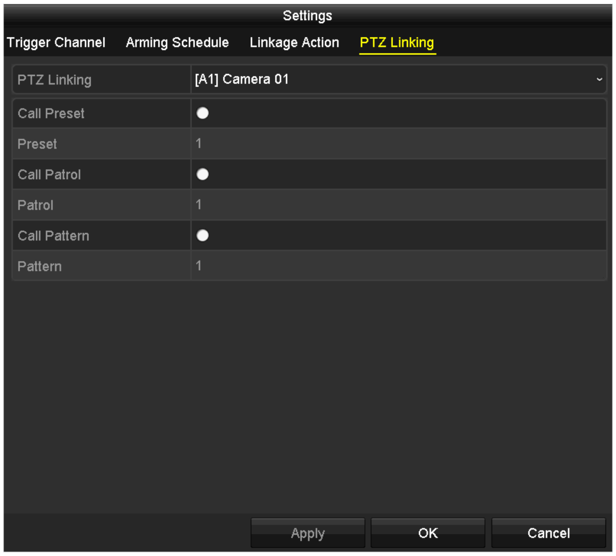


Camera	[A1] Camera 01
Enable	□
Settings	Set
Rule	1

Figure 175, Cameras Setup > VCA Window

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.

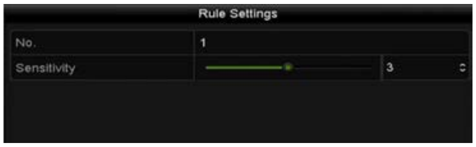


PTZ Linking	[A1] Camera 01
Call Preset	●
Preset	1
Call Patrol	●
Patrol	1
Call Pattern	●
Pattern	1

Figure 176, 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 can be detected.



No.	1
Sensitivity	3

Figure 177, 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.

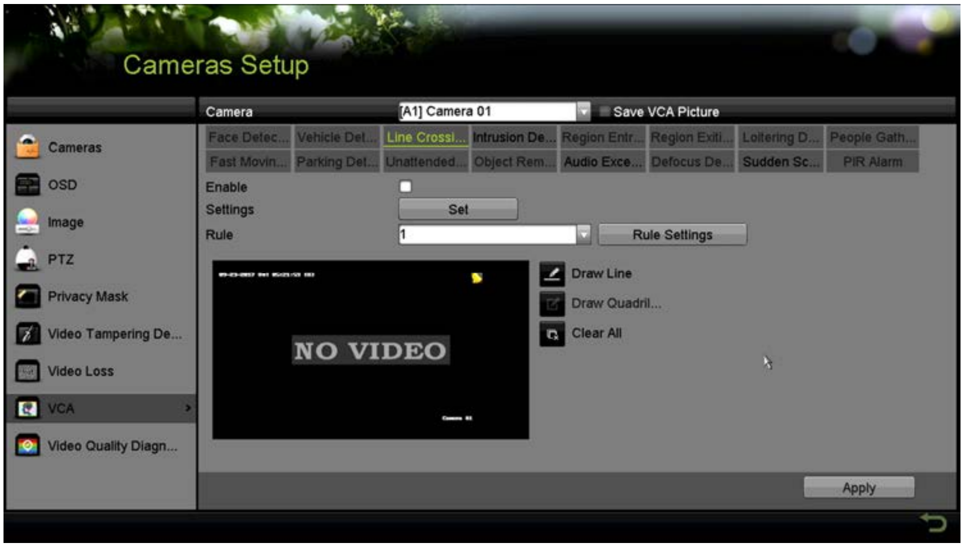
1. Go to Menu > Camera > VCA.

2. Select the camera to configure the VCA.

3. You can check the **Save VCA Picture** checkbox to save the captured VCA detection pictures.

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

5. Check the Enable checkbox to enable this function.



Camera [A1] Camera 01

Enable □

Settings

Rule 1

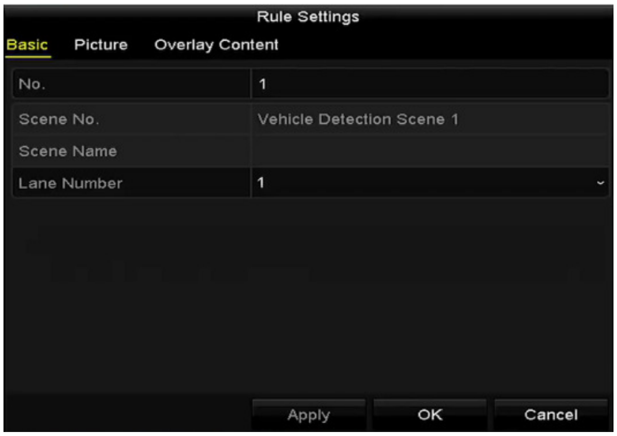
Figure 178, Set Vehicle Detection

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

NOTE

PTZ linking is applicable only to other list, not to whitelist and 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.



No.	1
Scene No.	Vehicle Detection Scene 1
Scene Name	
Lane Number	1

Figure 179, Rule Settings

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

NOTE

Refer to the network camera’s user manual for detailed vehicle detection instructions.

9.3 Line Crossing Detection

Purpose

This function detects people, vehicles, and objects crossing 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 > 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 **Line Crossing 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 line crossing detection alarm.
7. 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 goes across the configured line, both directions can be detected and alarms are triggered.

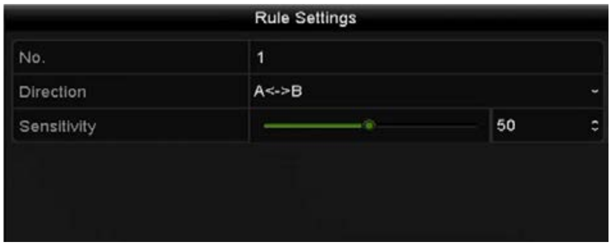
A->B: Only an object crosses the configured line from the A side to the B side can be detected.

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

2) Drag the slider to set the detection sensitivity.

Sensitivity: Range [1-100]. The higher the value, the more easily the detection alarm will be triggered.

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



Rule Settings

No.	1
Direction	A<->B
Sensitivity	50

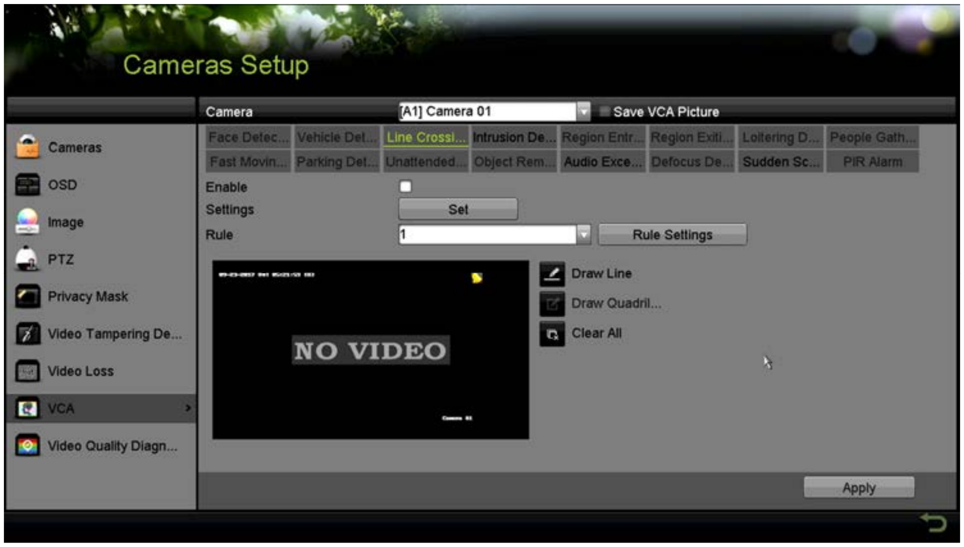
Figure 180, Set Line Crossing Detection Rules

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

9. Use ⧉ to clear the existing virtual line and re-draw it.

NOTE

Up to four rules can be configured.



Camera: [A1] Camera 01
□ Save VCA Picture
Enable: □
Rule: 1

Figure 181, Draw Line for Line Crossing Detection

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

NOTE

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

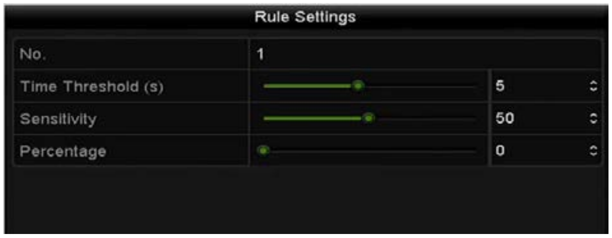
9.4 Intrusion Detection

Purpose

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

1. Go to Menu > Camera > 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 **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.

    - **Threshold:** Range [1s-10s], the threshold for the time the object loiters in the region. When the duration of the object in the defined detection area is longer than the set time, the alarm will be triggered.
    - **Sensitivity:** Range [1-100]. The value of the sensitivity defines the size of the object that will trigger the alarm. The higher the value, the more easily the detection alarm is triggered.
    - **Percentage:** Range [1-100]. Percentage defines the ratio of the in-region part of the object that will trigger the alarm. For example, if the percentage is set to 50%, when the object enters the region and occupies half of the whole region, the alarm is triggered.



Rule Settings

No.	1
Time Threshold (s)	5
Sensitivity	50
Percentage	0

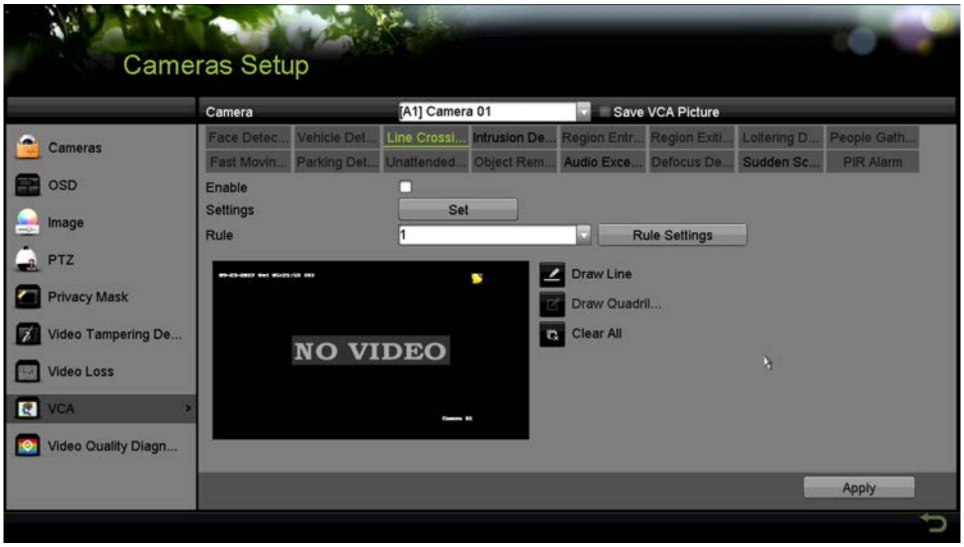
Figure 182, Set Intrusion Crossing Detection Rules

8. Click **OK** to save the rule settings and back to the line crossing detection settings interface.

9. Click and draw a quadrilateral in the preview window by specifying four vertexes of the detection region, and right click to complete 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.



Camera: [A1] Camera 01
□ Save VCA Picture
Enable: □
Rule: 1

Figure 183, Draw Area for Intrusion Detection

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

NOTE

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

9.5 Region Entrance Detection

Purpose

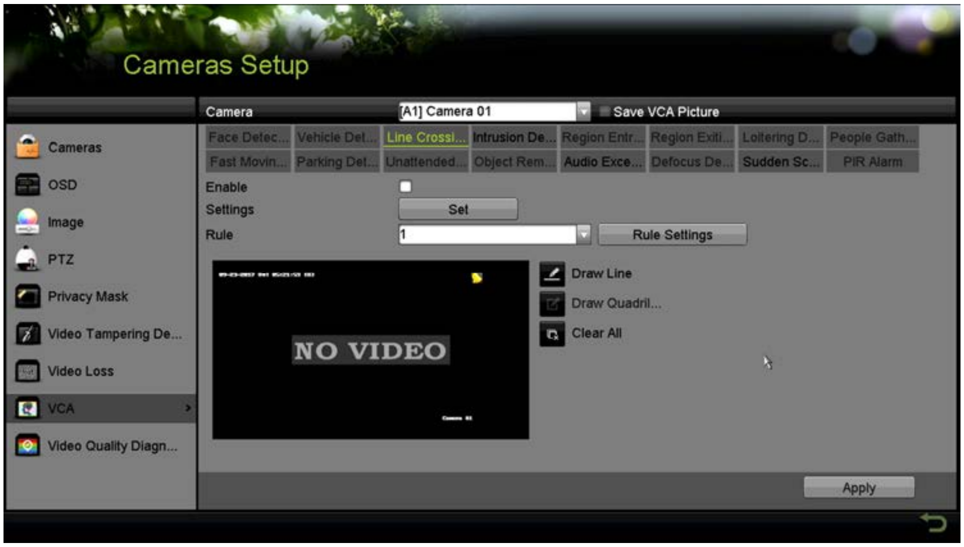
The region entrance detection function detects people, vehicles, or other objects that enter a pre-defined virtual region, and certain actions can be taken when the alarm is triggered.

1. Go to Menu > Camera > 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 **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 sensitivity of the region entrance detection.

   Sensitivity: Range [0-100]. The higher the value, the more easily the detection alarm will be triggered.

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



Camera: [A1] Camera 01

□ Save VCA Picture

Enable: □

Settings: Set

Rule: 1

Figure 184, 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

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

NOTE

Up to four rules can be configured.

9.7 Loitering Detection

Purpose

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

- **Threshold** [1s-10s] in the Rule Settings defines the time the object can loiter in the region. If you set the value to 5, an alarm is triggered after the object loiters in the region for 5s; and if you set the value to 0, an alarm is triggered immediately if the object enters the region.
- Up to four rules can be configured.

9.8 People Gathering Detection

Purpose

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

The **Percentag**e in the Rule Settings defines the gathering density of the people in the region. If the percentage is small, the alarm will be triggered when a small number of people gathered in the defined detection region.

Up to four rules can be configured.

9.9 Fast Moving Detection

Purpose

The 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.

- **Sensitivity** in the Rule Settings defines the moving speed of the object that can 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 a highway, one-way street, etc., and a series of actions can be taken when the alarm is triggered.

- **Threshold** [5s-20s] in the Rule Settings defines the time of the vehicle parking in the region. If you set the value as 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.

- **Threshold** [5s-20s] in the Rule Settings defines the time of the objects left in the region. If you set the value to 10, an alarm is triggered after the object is left and stays in the region for 10s.
- **Sensitivity** defines the similarity degree of the background image. When the sensitivity is high, a very small object left in the region can trigger the alarm.
- Up to four rules can be configured.

9.12 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.

- **Threshold** [5s-20s] in the Rule Settings defines the time of the objects removed from the region. If you set the value to 10, an alarm is triggered after the object disappears from the region for 10s.
- **Sensitivity** defines the similar degree of the background image. If the sensitivity is high, a very small object taken from the region can trigger the alarm.
- Up to four rules can be configured.

9.13 Audio Exception Detection

Purpose

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

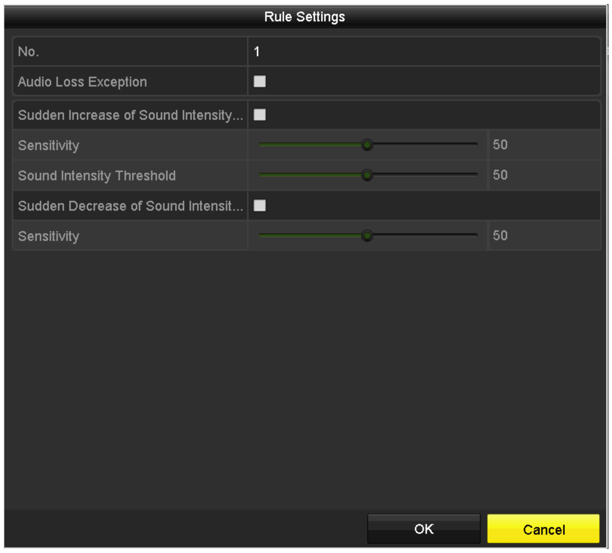
NOTE

Audio exception detection is supported by all analog channels.

1. Go to Menu > Camera > 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.



Rule Settings

No. 1

Audio Loss Exception □

Sudden Increase of Sound Intensity... □

Sensitivity 50

Sound Intensity Threshold 50

Sudden Decrease of Sound Intensit... □

Sensitivity 50

Figure 185, Set Audio Exception Detection Rules

7. Check the **Audio Loss Exception** checkbox to enable the audio loss detection function.

8. Check the **Sudden Increase of Sound Intensity Detection** checkbox to detect a steep sound rise in the surveillance scene. Set the detection sensitivity and threshold for a steep sound rise.

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

   - **Sound Intensity Threshold**: Range [1-100], filters the sound in the environment, the louder the environment sound, the higher the value should be. Adjust it according to the environment.

9. Check the **Sudden Decrease of Sound Intensity Detection** checkbox to detect a steep sound drop in the surveillance scene. Set the detection sensitivity [1-100] for a steep sound drop.

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

9.14 Defocus Detection

Purpose

Image blur caused by lens defocus can be detected, and specific actions can be taken when the alarm is triggered.

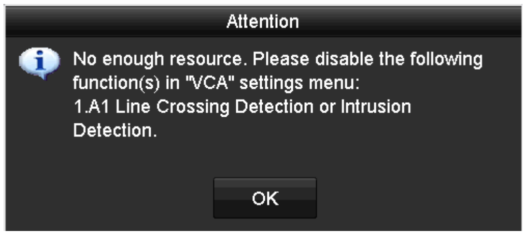
- **Sensitivity** in the Rule Settings ranges from 1 to 100. The higher the value, the more easily the defocused image will trigger the alarm.

9.15 Sudden Scene Change

Purpose

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

- **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, line crossing detection and intrusion detection conflict with other VCA detections 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).


Attention

No enough resource. Please disable the following function(s) in "VCA" settings menu:
1.A1 Line Crossing Detection or Intrusion Detection.

Figure 186, 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 creatures such as dogs, cats, etc., can be detected.

1. Go to Menu > Camera > VCA.
2. Select the camera to configure the VCA.
3. Check the **Save VCA Picture** checkbox to save the captured VCA detection pictures.
4. Select 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.
7. Click **Apply** to activate the settings.

10 VCA Search

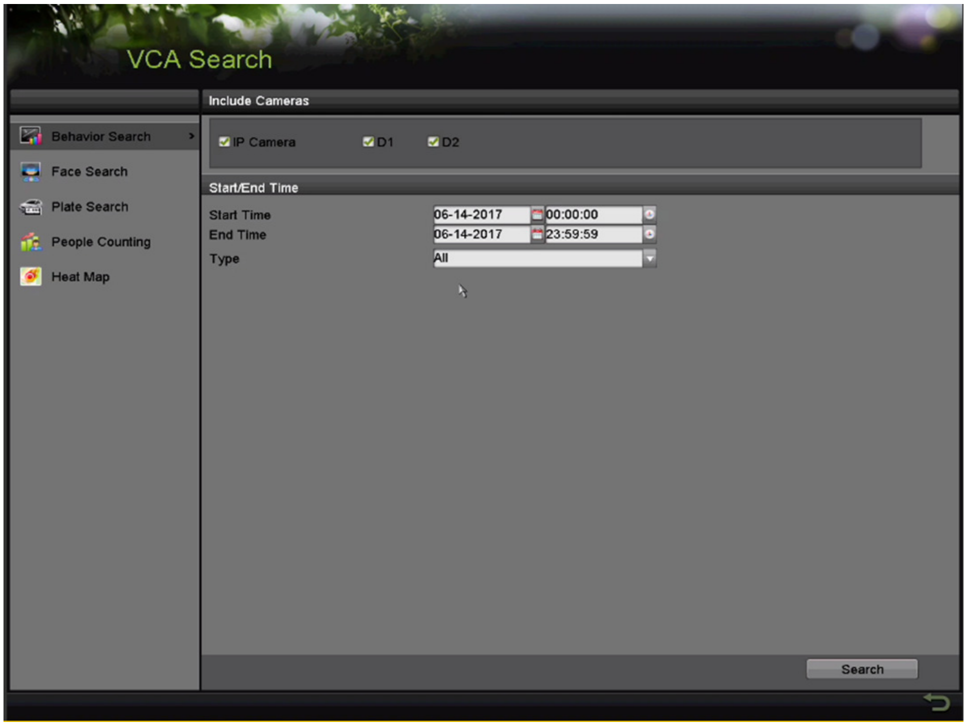
With the configured VCA detection, the device supports VCA search for the behavior search, face search, plate search, people counting, and heat map results of the IP cameras.

10.1 Behavior Search

Purpose

The behavior analysis detects a series of suspicious behavior based on VCA detection, and specific 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.



Include Cameras

☑IP Camera ☑D1 ☑D2

Start/End Time

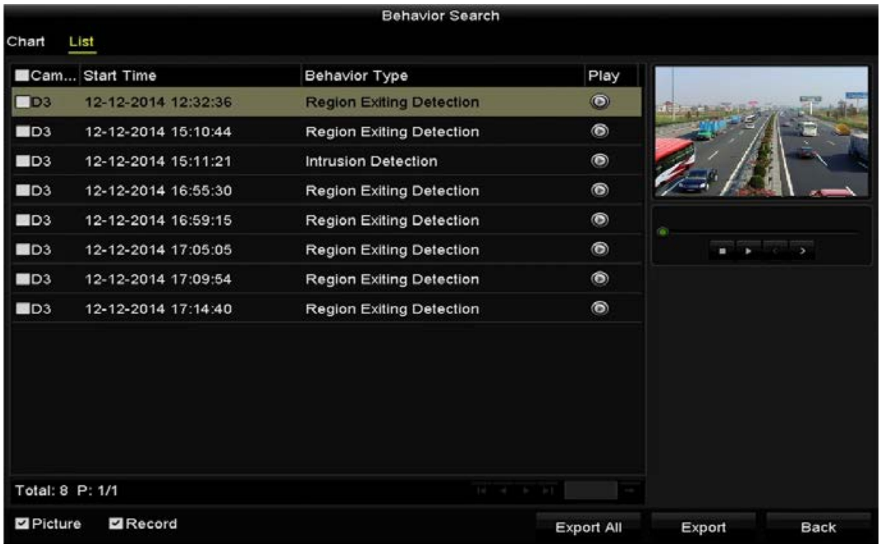
Start Time 06-14-2017 00:00:00

End Time 06-14-2017 23:59:59

Type All

Figure 187, Behavior Search Interface

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



■Cam...	Start Time	Behavior Type	Play
□D3	12-12-2014 12:32:36	Region Exiting Detection	◉
■D3	12-12-2014 15:10:44	Region Exiting Detection	◉
■D3	12-12-2014 15:11:21	Intrusion Detection	◉
■D3	12-12-2014 16:55:30	Region Exiting Detection	◉
■D3	12-12-2014 16:59:15	Region Exiting Detection	◉
■D3	12-12-2014 17:05:05	Region Exiting Detection	◉
■D3	12-12-2014 17:09:54	Region Exiting Detection	◉
■D3	12-12-2014 17:14:40	Region Exiting Detection	◉

Total: 8 P: 1/1

☑Picture ☑Record

Figure 188, Behavior Search Results

6. Play the behavior analysis picture related video file.

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

8. You can click ■ to stop playing, or click ‹/› to play the previous/next file.

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

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

10.2 Plate Search

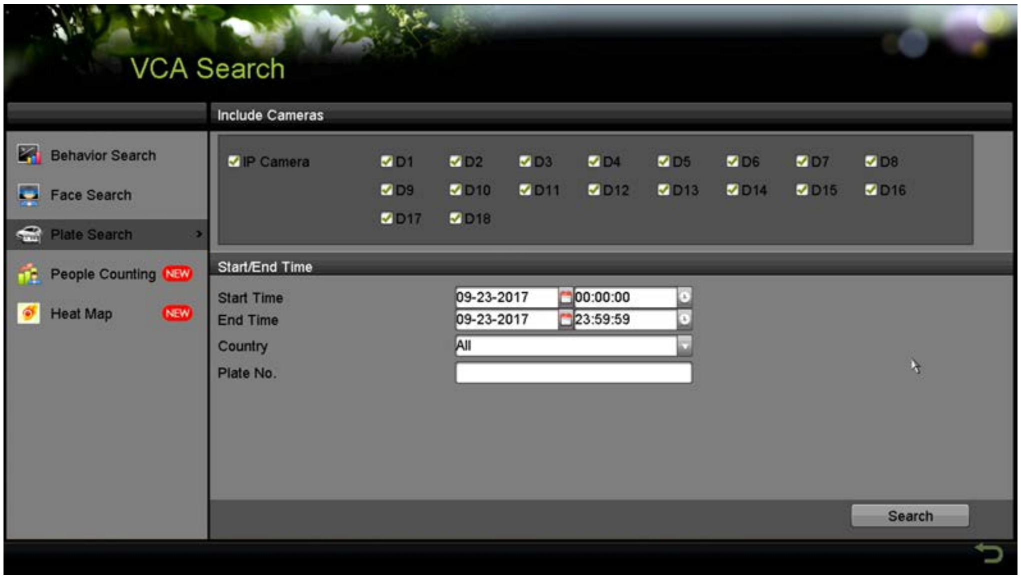
Purpose

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.



Include Cameras

☑ IP Camera ☑ D1 ☑ D2 ☑ D3 ☑ D4 ☑ D5 ☑ D6 ☑ D7 ☑ D8 ☑ D9 ☑ D10 ☑ D11 ☑ D12 ☑ D13 ☑ D14 ☑ D15 ☑ D16 ☑ D17 ☑ D18

Start/End Time

Start Time 09-23-2017 00:00:00

End Time 09-23-2017 23:59:59

Country All

Plate No.

Figure 189, Plate Search

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

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 list or in chart.

10.3 People Counting

NOTE

Requires camera(s) that support the counting feature.

Purpose

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

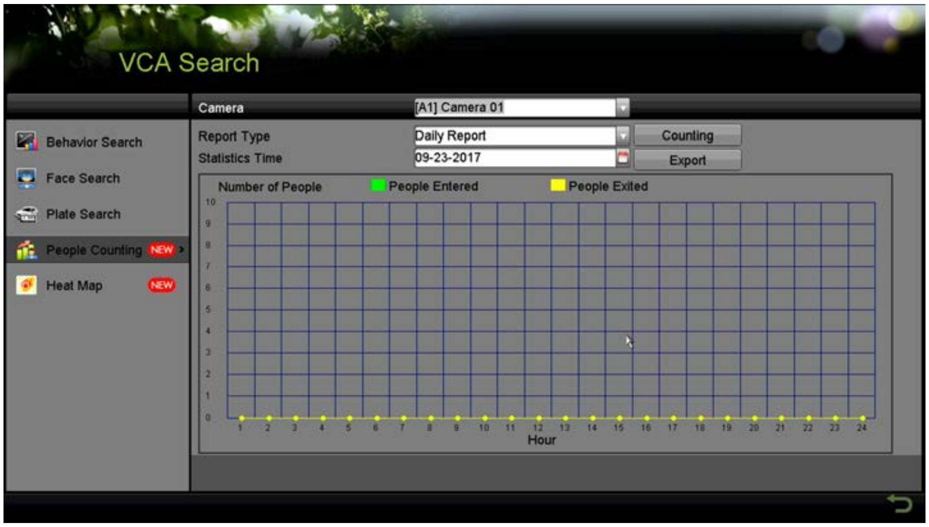
1. Go to Menu > VCA Search > People Counting.

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.



Camera: [A1] Camera 01

Report Type: Daily Report

Statistics Time: 09-23-2017

Figure 190, People Counting Interface

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

10.4 Heat Map

Purpose

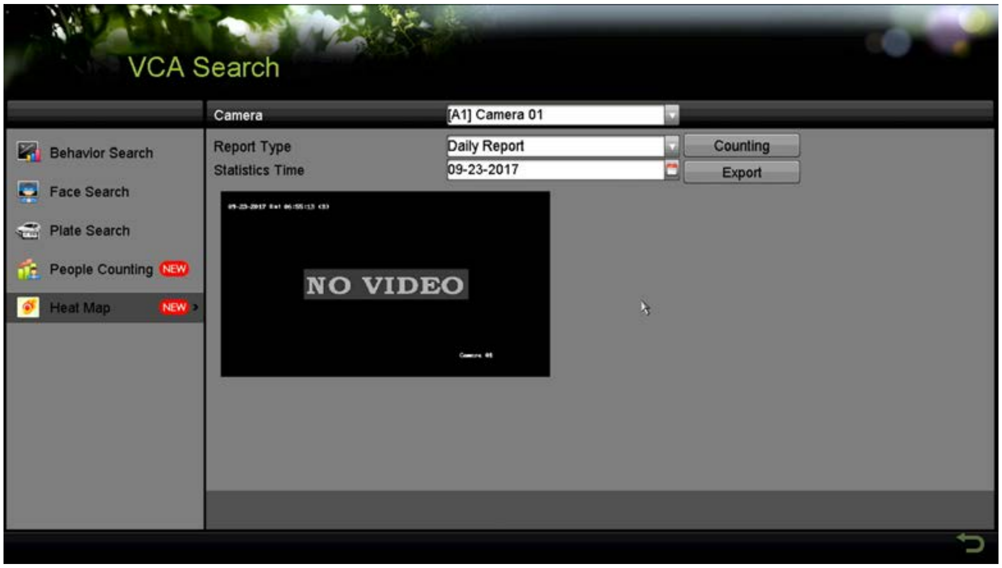
Heat map is a graphical representation of data represented by colors. The heat map function is usually used to analyze the visit times and dwell time of customers in a configured area.

1. Go to Menu > VCA Search > Heat Map.

2. Select the camera for the heat map processing.

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

4. Set the statistics time.



Camera: [A1] Camera 01
Report Type: Daily Report
Statistics Time: 09-23-2017

Figure 191, Heat Map Interface

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

NOTE

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

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

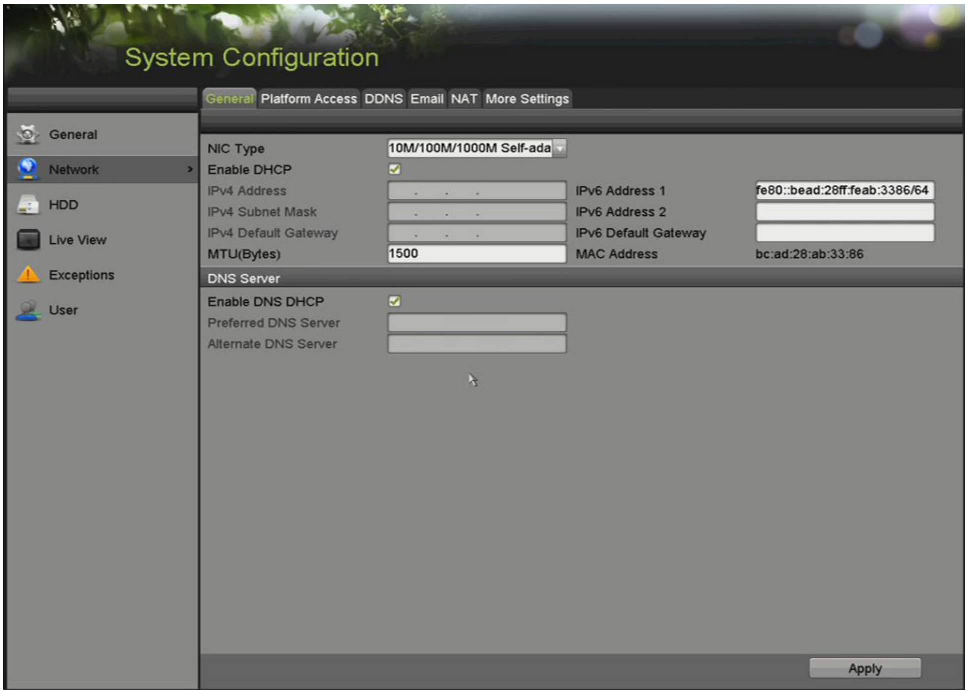
11 Network Settings

11.1 Configuring General Settings

Purpose

Network settings must be properly configured before operating the DVR over a network. On the **General Settings** interface, you can configure Working Mode (DS-73xxHUI-K4 and DS-90xxHUI-K8 only), NIC Type, IPv4 Address, IPv4 Gateway, MTU, DNS Server, and Main NIC.

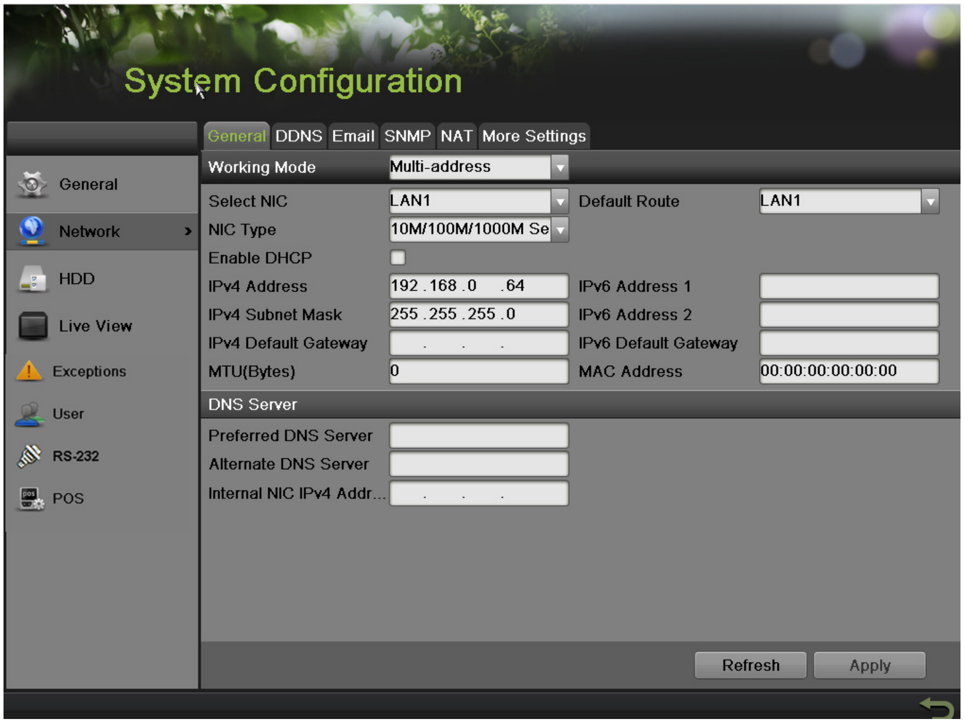
1. Go to Menu > System Configuration > Network > General.



NIC Type: 10M/100M/1000M Self-ada
Enable DHCP: ☑
IPv4 Address: . . .
IPv4 Subnet Mask: . . .
IPv4 Default Gateway: . . .
MTU(Bytes): 1500
IPv6 Address 1: fe80::bead:28ff:feab:3386/64
IPv6 Address 2:
IPv6 Default Gateway:
MAC Address: bc:ad:28:ab:33:86

DNS Server
Enable DNS DHCP: ☑
Preferred DNS Server:
Alternate DNS Server:

Figure 192, Network Settings Interface (DS-73xxHQI-K4)



Working Mode: Multi-address
Select NIC: LAN1
Default Route: LAN1
NIC Type: 10M/100M/1000M Se
Enable DHCP: □
IPv4 Address: 192 .168 .0 .64
IPv4 Subnet Mask: 255 .255 .255 .0
IPv4 Default Gateway: . . .
MTU(Bytes): 0
IPv6 Address 1:
IPv6 Address 2:
IPv6 Default Gateway:
MAC Address: 00:00:00:00:00:00

DNS Server
Preferred DNS Server:
Alternate DNS Server:
Internal NIC IPv4 Addr...: . . .

Figure 193, Network Settings Interface (DS-73xxHQI-K4)

2. (DS-73xxHUI-K4 and DS-90xxHUI-K8 only) Select one NIC card as default route, and the system will connect with the extranet and the data will be forwarded through the default route.

   Working Mode – There are two 10M/100M/1000M NIC cards provided, and they allow the device to work in Multi-address and Net-fault Tolerance.

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

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

NOTE

The valid value of MTU is from 500 to 1500.

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

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

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

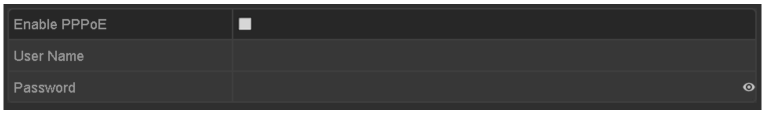
11.2 Configuring Advanced Settings

11.2.1 Configuring PPPoE Settings

Purpose

The DVR allows access by Point-to-Point Protocol over Ethernet (PPPoE).

1. Go to Menu > System Configuration > Network > PPPoE.



Enable PPPoE □
User Name
Password

Figure 194, PPPoE Settings Interface

2. Check the **Enable PPPoE** checkbox to enable this feature.

3. Enter **User Name** and **Password** for PPPoE access.

NOTE

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

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

5. After successful settings, the system asks you to reboot the device to enable the new settings, and the PPPoE dial-up is automatically connected after reboot.

6. You can go to Menu > Maintenance > System Info > Network interface to view the status of PPPoE connection.

11.2.2 Configuring Hik-Connect

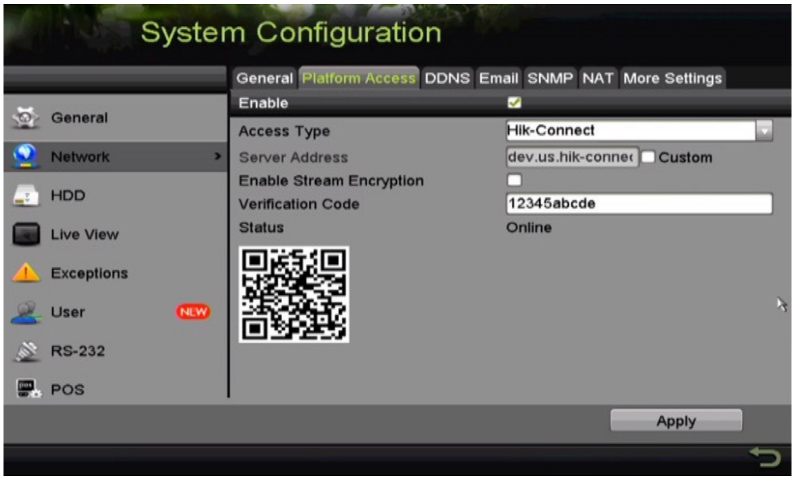
Purpose

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



Enable ☑

Access Type: Hik-Connect

Server Address: dev.us.hik-conne □ Custom

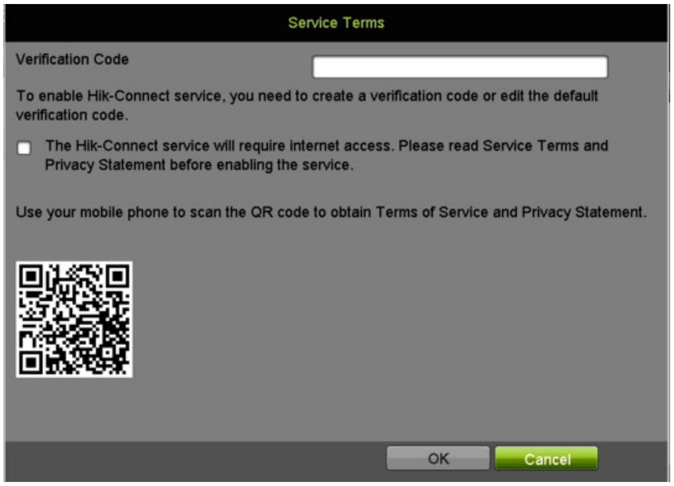
Enable Stream Encryption □

Verification Code: 12345abcde

Status: Online

Figure 195, Hik-Connect Settings

2. Check the **Enable** checkbox to activate the function. Then the **Service Terms** interface pops up, as below.



Verification Code

To enable Hik-Connect service, you need to create a verification code or edit the default verification code.

□ The Hik-Connect service will require internet access. Please read Service Terms and Privacy Statement before enabling the service.

Use your mobile phone to scan the QR code to obtain Terms of Service and Privacy Statement.

Figure 196, Service Terms

3. Create the verification code and enter the code in the **Verification Code** text field.

4. Check the “The Hik-Connect service will require internet access. Checkbox. Please read Service Terms and Privacy Statement.”

5. Scan the QR code on the interface to read the Service Terms and the Privacy Statement.

6. Click **OK** to save the settings and return to the Hik-Connect interface.

NOTE

Hik-Connect is disabled by default.

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

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

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

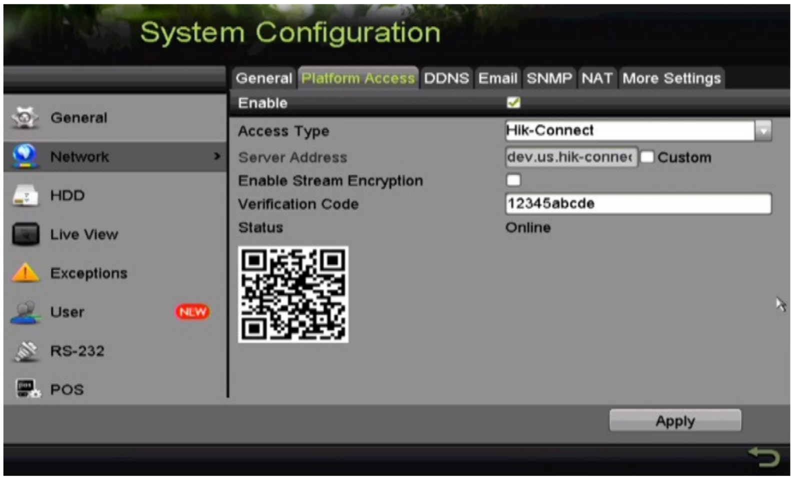
7. (Optional) Check the **Custom** checkbox and input the **Server Address**.

8. (Optional) Check the **Enable Stream Encryption** checkbox.

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

NOTE

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



Enable ☑
Access Type Hik-Connect
Server Address dev.us.hik-connec ☐ Custom
Enable Stream Encryption ☐
Verification Code 12345abcde
Status Online

Figure 197, Hik-Connect Settings Interface

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

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

NOTE

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

11.2.3 Configuring DDNS

Purpose

If the 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.

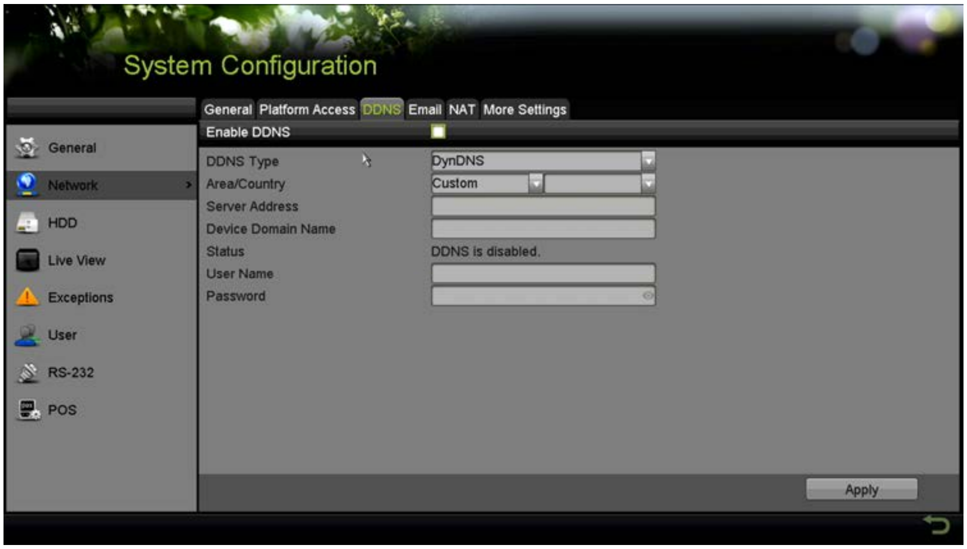
1. Go to Menu > System Configuration > Network > DDNS.
2. Check the **Enable DDNS** checkbox to enable this feature.
3. Select **DDNS Type**. Three different DDNS types are selectable: DynDNS, PeanutHull, and NO-IP.

   - **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 Website.

     3) Enter the **User Name** and **Password** registered in the DynDNS Website.



Enable DDNS ☐

DDNS Type: DynDNS

Area/Country: Custom

Server Address

Device Domain Name

Status: DDNS is disabled.

User Name

Password

Figure 198, DynDNS Settings Interface

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

- **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 Website (www.no-ip.com).

  3) Enter the **User Name** and **Password** registered in the NO-IP Website.

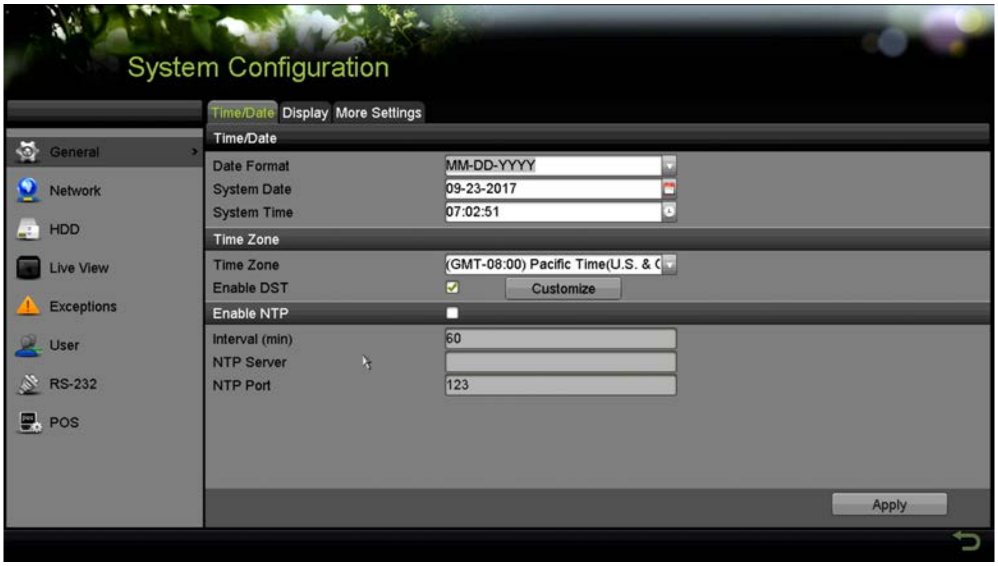
- Click **Apply** to save and exit the interface.

11.2.4 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 > Date/Time.



Time/Date

Date Format: MM-DD-YYYY

System Date: 09-23-2017

System Time: 07:02:51

Time Zone

Time Zone: (GMT-08:00) Pacific Time(U.S. & C

Enable DST: ☑

Enable NTP: □

Interval (min): 60

NTP Server:

NTP Port: 123

Figure 199, 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 10080 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 customized network, NTP software can be used to establish a NTP server used for time synchronization.

11.2.5 Configuring NAT

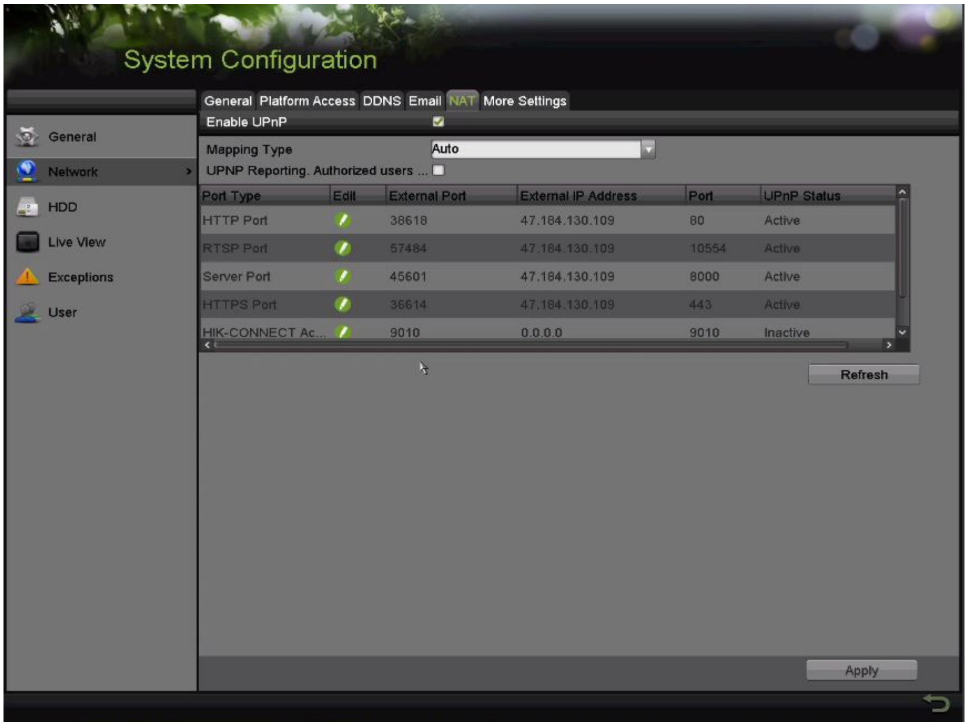
Purpose

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

Before You Start

If you want to enable the UPnP™ function of the device, you must enable the UPnP™ function of the router to which your device is connected. When the network working mode of the device is set as multi-address, the Default Route of the device should be in the same network segment as that of the LAN IP address of the router.

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



Enable UPnP ☑

Mapping Type: Auto

UPNP Reporting. Authorized users ... ☐

Port Type	Edit	External Port	External IP Address	Port	UPnP Status
HTTP Port	✎	38618	47.184.130.109	80	Active
RTSP Port	✎	57484	47.184.130.109	10554	Active
Server Port	✎	45601	47.184.130.109	8000	Active
HTTPS Port	✎	36614	47.184.130.109	443	Active
HIK-CONNECT Ac...	✎	9010	0.0.0.0	9010	Inactive

Figure 200, UPnP™ Settings Interface

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

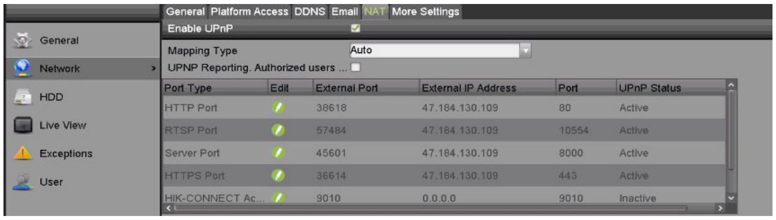
3. Select the **Mapping Type** as Manual or Auto in the drop-down list.

OPTION 1: Auto

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

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

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



Enable UPnP ☑

Mapping Type: Auto

UPNP Reporting. Authorized users ... ☐

Port Type	Edit	External Port	External IP Address	Port	UPnP Status
HTTP Port	✎	38618	47.184.130.109	80	Active
RTSP Port	✎	57484	47.184.130.109	10554	Active
Server Port	✎	45601	47.184.130.109	8000	Active
HTTPS Port	✎	36614	47.184.130.109	443	Active
HIK-CONNECT Ac...	✎	9010	0.0.0.0	9010	Inactive

Figure 201, UPnP™ Settings Finished – Auto

OPTION 2: Manual

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

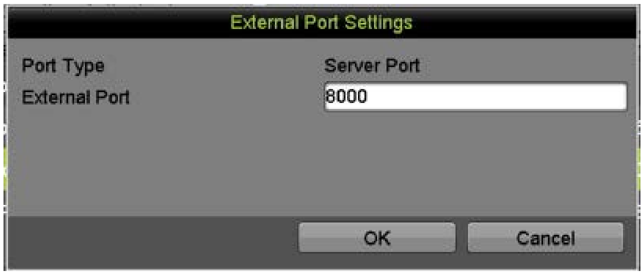
1) Click ✎ to activate the **External Port Settings** dialog box. Configure the external port No. for server port, http port and RTSP port respectively.

NOTE

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

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

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



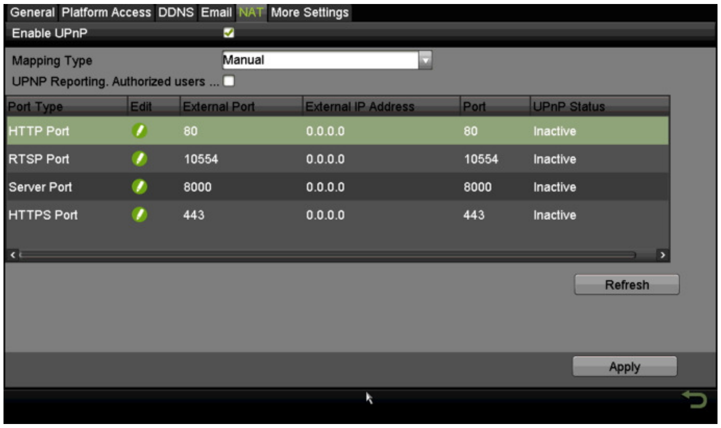
Port Type: Server Port

External Port: 8000

Figure 202, External Port Settings Dialog Box

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

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



Enable UPnP ☑

Mapping Type: Manual

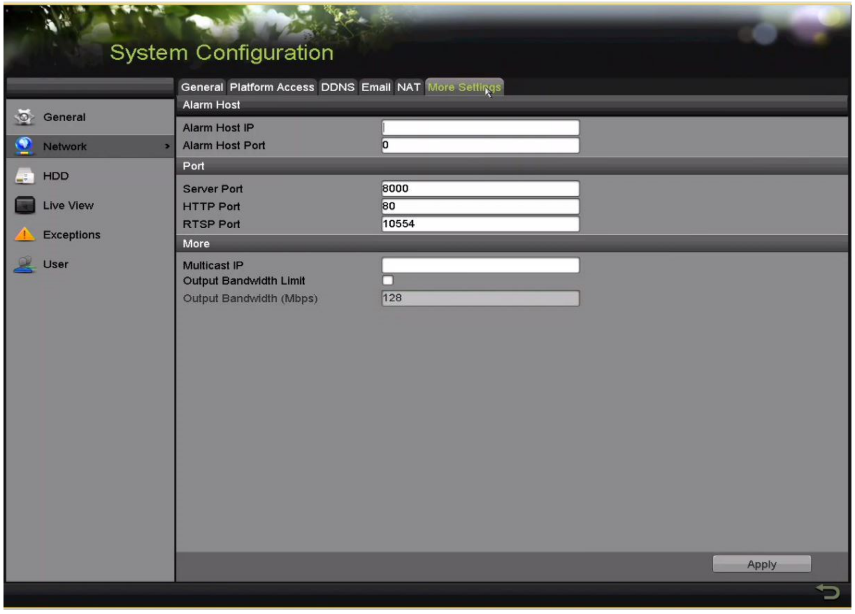
UPNP Reporting. Authorized users ... □

Port Type	Edit	External Port	External IP Address	Port	UPnP Status
HTTP Port	✎	80	0.0.0.0	80	Inactive
RTSP Port	✎	10554	0.0.0.0	10554	Inactive
Server Port	✎	8000	0.0.0.0	8000	Inactive
HTTPS Port	✎	443	0.0.0.0	443	Inactive

Figure 203, UPnP™ Settings Finished – Manual

11.2.6 Configuring More Settings

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



Alarm Host

Alarm Host IP:

Alarm Host Port: 0

Port

Server Port: 8000

HTTP Port: 80

RTSP Port: 10554

More

Multicast IP:

Output Bandwidth Limit □

Output Bandwidth (Mbps): 128

Figure 204, 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 text field of **RTSP Port**. The default RTSP port is 554, and you can change it according to different requirements.

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

NOTE

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

- **Output Bandwidth Limit**: Check this 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 the remote live view and playback.

The default output bandwidth is the maximum limit.

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

11.2.7 Configuring HTTPS Port

Purpose

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

Example: If you set the port number 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 the Web browser.

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

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

3. Go to Menu > System Configuration > Remote Configuration > Network Settings > HTTPS.

4. Create the self-signed certificate or authorized certificate.

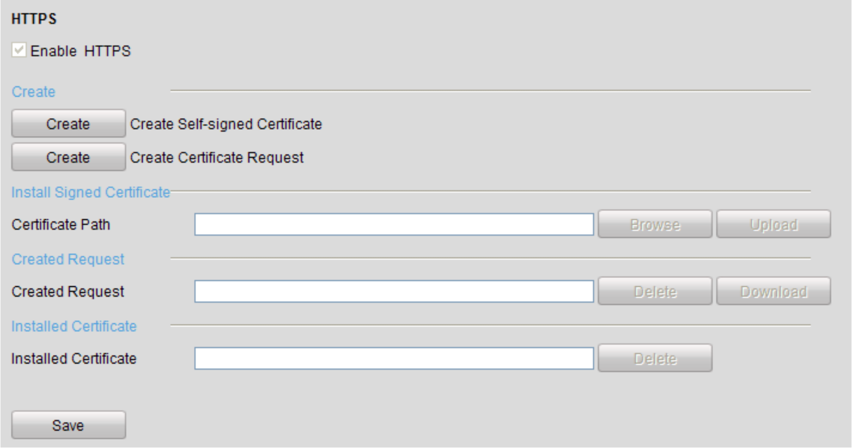
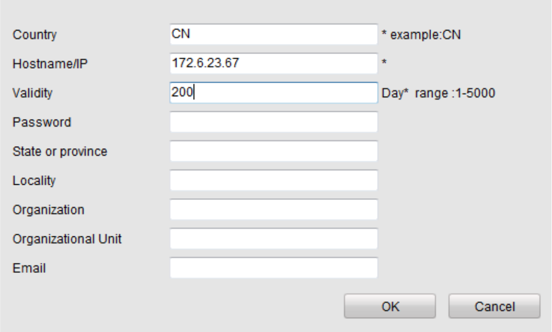


Figure 205, HTTPS Settings

OPTION 1: Create the self-signed certificate

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



Country: CN * example:CN
Hostname/IP: 172.6.23.67 *
Validity: 200 Day* range :1-5000

Figure 206, Create Self-signed Certificate

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

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

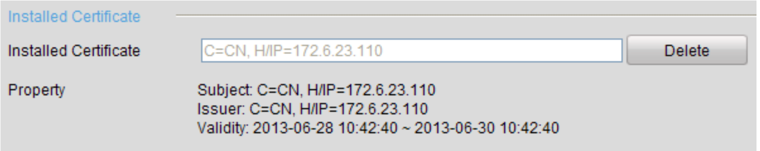
OPTION 2: Create the authorized certificate

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.

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



Installed Certificate

Installed Certificate: C=CN, H/IP=172.6.23.110

Property:
Subject: C=CN, H/IP=172.6.23.110
Issuer: C=CN, H/IP=172.6.23.110
Validity: 2013-06-28 10:42:40 ~ 2013-06-30 10:42:40

Figure 207, Installed Certificate Property

6. Check the checkbox to enable the HTTPS function.

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

11.2.8 Configuring E-Mail

Purpose

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

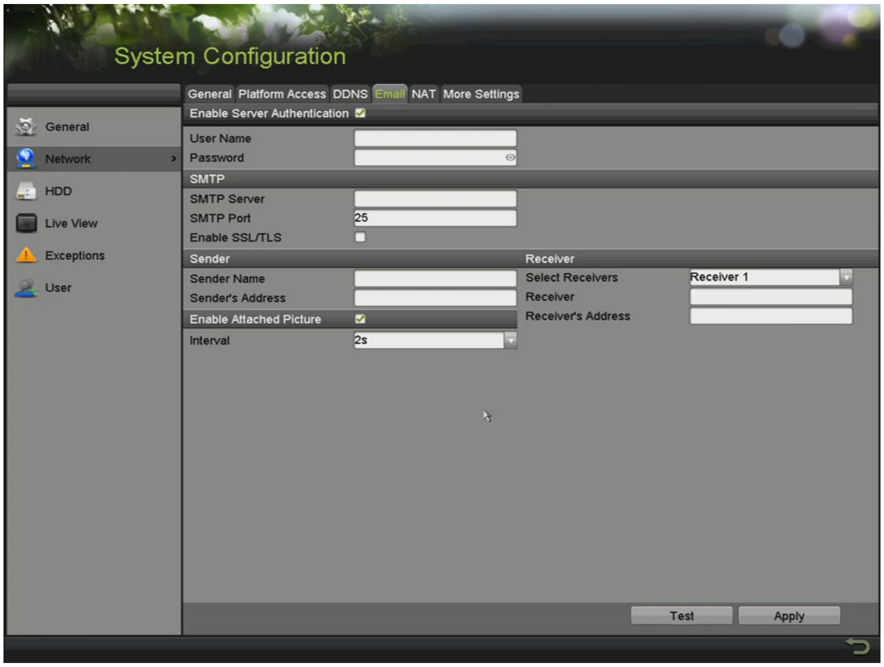
Before configuring the e-mail settings, the DVR must be connected to a local area network (LAN) that maintains an SMTP mail server. The network must also be connected to either an intranet or the Internet depending on the location of the e-mail accounts to which you want to send notification. Additionally,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

Before You Start

Make sure you have configured the IPv4 Address, IPv4 Subnet Mask, IPv4 Gateway, and the Preferred DNS Server in the Network Settings menu.

1. Go to Menu > System Configuration > Network > Email.

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



Enable Server Authentication ☑

User Name

Password

SMTP Server

SMTP Port 25

Enable SSL/TLS □

Sender Name

Sender's Address

Enable Attached Picture ☑

Interval 2s

Select Receivers Receiver 1

Receiver

Receiver's Address

Figure 208, 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 default TCP/IP port used for SMTP is 25.

   Enable SSL (optional): Click the checkbox to enable SSL if required by the SMTP server.

   Sender: The name of sender.

   Sender’s Address: The e-mail address of sender.

   Select Receivers: Select the receiver. Up to three receivers can be configured.

   Receiver: The name of the receiver of the e-mail.

   Receiver’s Address: The e-mail address of the receiver.

   Enable Attached Picture: Check the checkbox if you want to send email with attached alarm images. The interval is the time between two captures of the alarm images.

NOTE

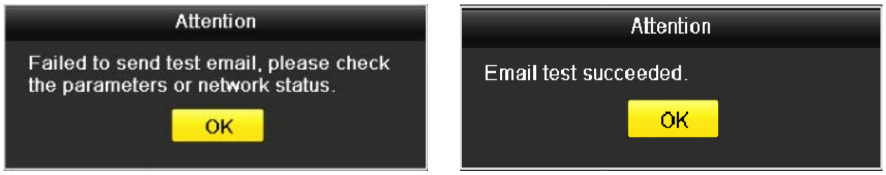
For IP cameras, the alarm images are directly sent as attached pictures by e-mail. Up to one picture can be sent for one IP camera. The attached pictures of the linked cameras cannot be sent.

For analog cameras, three attached pictures can be sent for one analog camera when the 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.

1. Click **Apply** to save the e-mail settings.
2. You can click **Test** to test whether your e-mail settings work. The corresponding Attention message box pops up.



Attention

Failed to send test email, please check the parameters or network status.

Attention

Email test succeeded.

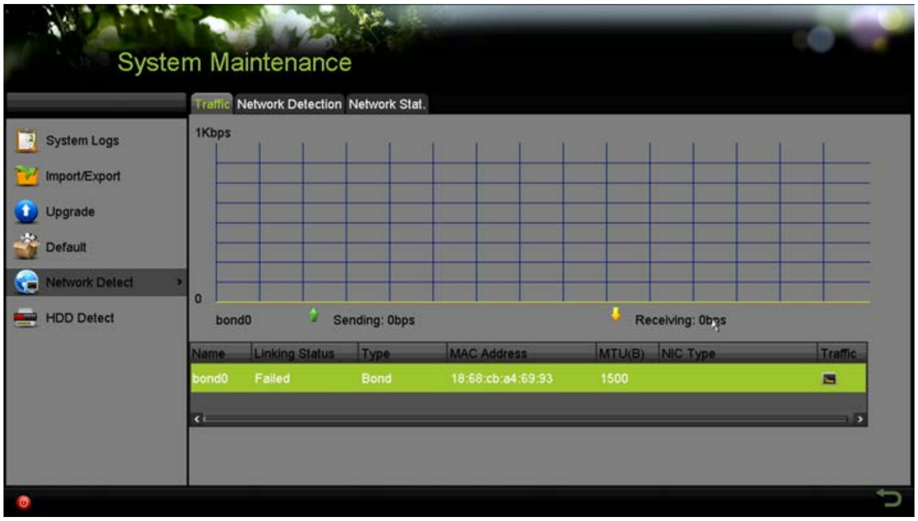
Figure 209, Email Testing Attention

11.2.9 Checking Network Traffic

Purpose

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

1. Go to Menu > Maintenance > Net Detect > Traffic.



bond0 Sending: 0bps Receiving: 0bps

Name	Linking Status	Type	MAC Address	MTU(B)	NIC Type	Traffic
bond0	Failed	Bond	18:68:cb:a4:69:93	1500		▨

Figure 210, Network Traffic Interface

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

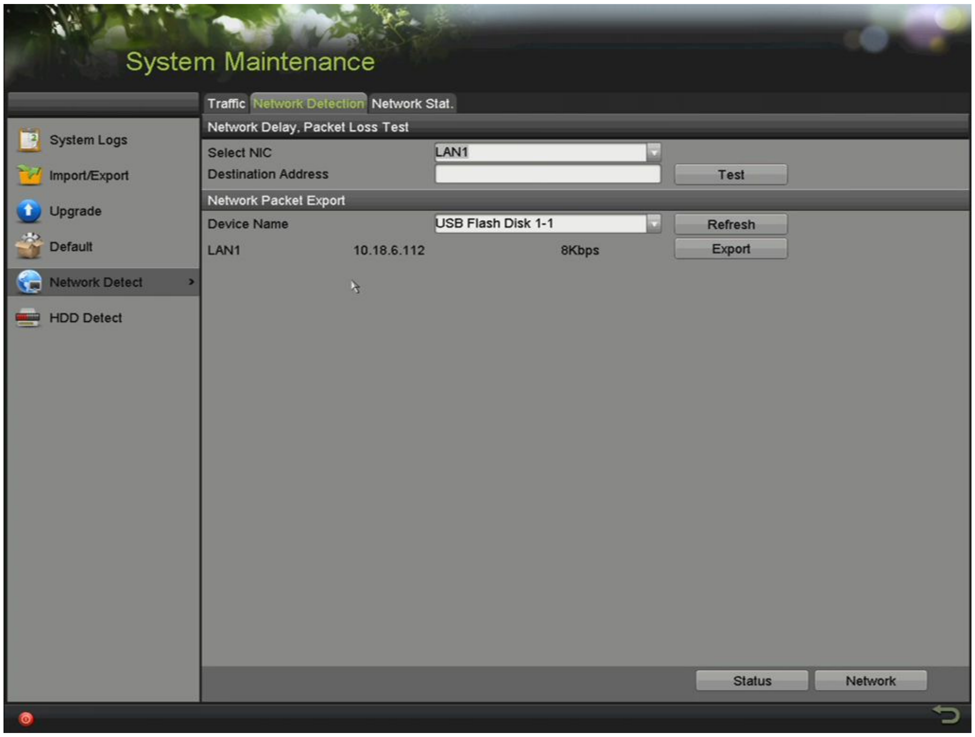
11.3 Configuring Network Detection

Purpose

You can obtain network connecting status of 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 > Net Detect > Network Detection.



Network Delay, Packet Loss Test

Select NIC: LAN1

Destination Address:

Network Packet Export

Device Name: USB Flash Disk 1-1

LAN1 10.18.6.112 8Kbps

Figure 211, Network Detection Interface

2. Select a NIC to test network delay and packet loss.

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

4. Click **Test** to start testing network delay and packet loss.

11.3.2 Exporting Network Packet

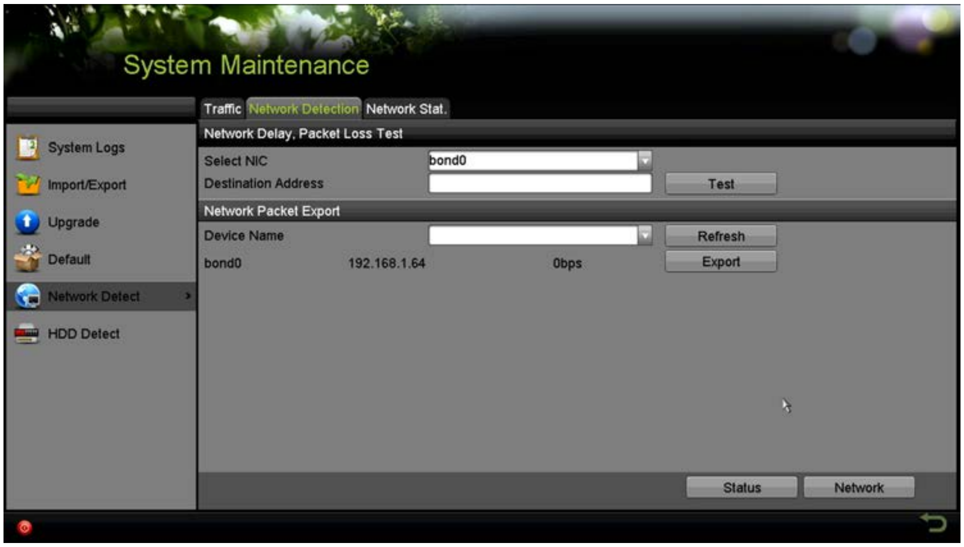
Purpose

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 > Net Detect > Network Detection.

2. Select the backup device from the **Device Name** drop-down list.

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



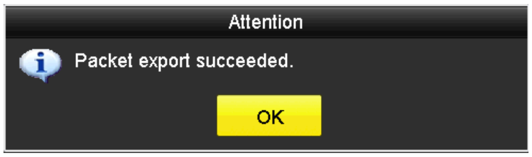
Select NIC: bond0

bond0 192.168.1.64 0bps

Figure 212, Export Network Packet

3. Click **Export** to start exporting.

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



Packet export succeeded.

Figure 213, Packet Export Attention

NOTE

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

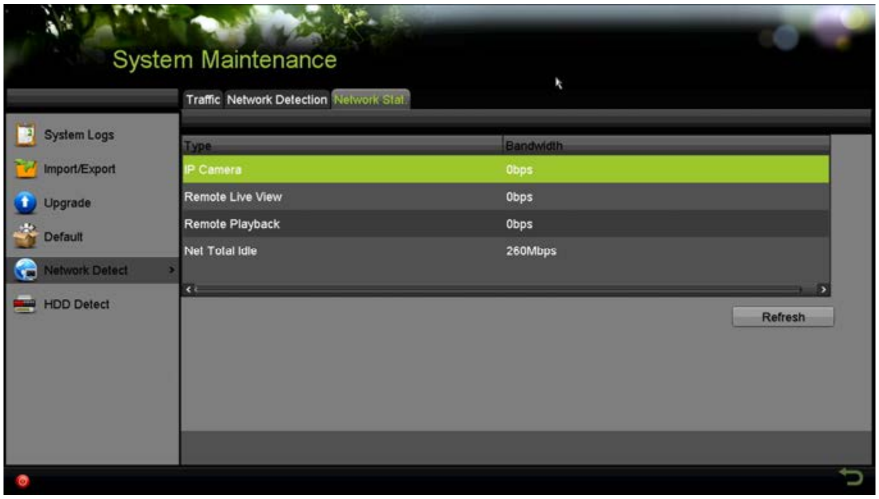
11.3.3 Checking Network Status

Purpose

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

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

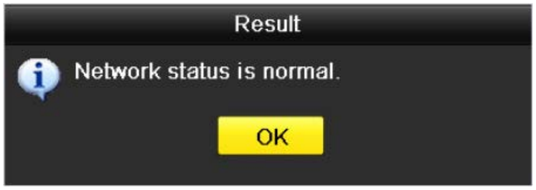
2. Click **Status** on the right bottom of the interface.



Type	Bandwidth
IP Camera	0bps
Remote Live View	0bps
Remote Playback	0bps
Net Total Idle	260Mbps

Figure 214, Checking Network Status

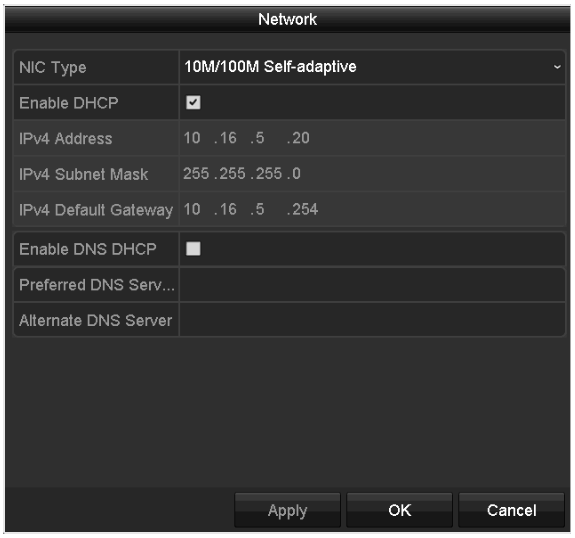
3. If the network is normal the following message box pops out.



Network status is normal.

Figure 215, Network Status Checking Result

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



NIC Type	10M/100M Self-adaptive
Enable DHCP	☑
IPv4 Address	10 .16 .5 .20
IPv4 Subnet Mask	255 .255 .255 .0
IPv4 Default Gateway	10 .16 .5 .254
Enable DNS DHCP	□
Preferred DNS Serv...	
Alternate DNS Server	

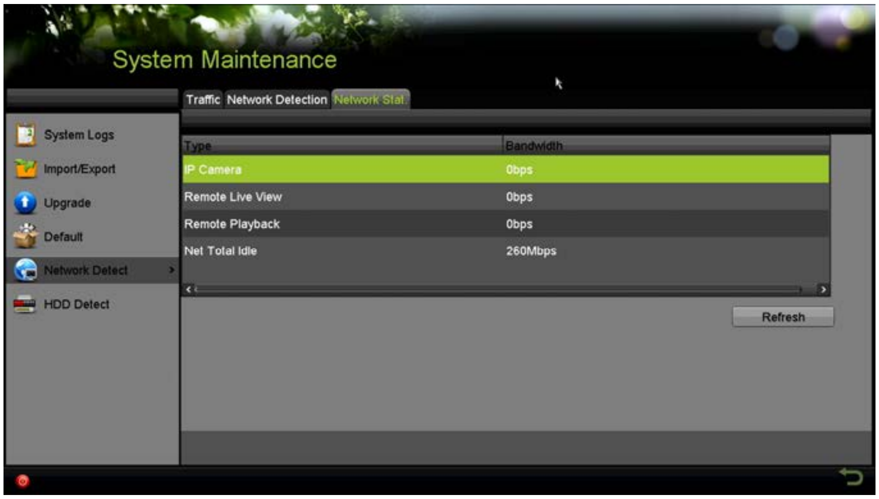
Figure 216, Network Parameters Configuration

11.3.4 Checking Network Statistics

Purpose

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

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



Type	Bandwidth
IP Camera	0bps
Remote Live View	0bps
Remote Playback	0bps
Net Total Idle	260Mbps

Figure 217, Network Stat. Interface

2. View the bandwidth of Remote Live View, bandwidth of Remote Playback, and bandwidth of Net Total Idle.

3. Click **Refresh** to get the latest bandwidth statistics.

12 RAID

12.1 Configuring Array

Purpose

RAID (redundant array of independent disks) is a storage technology that combines multiple disk drive components into a logical unit. A RAID setup stores data over multiple hard disk drives to provide enough redundancy so that data can be recovered if one disk fails. Data is distributed across the drives in one of several ways called "RAID levels," depending on what level of redundancy and performance is required.

The DVR supports software disk arrays. You can enable the RAID function on demand.

NOTE

The DVR supports RAID 0, RAID 1, RAID 5, RAID 6, and RAID 10 array types.

Before You Start

Install the HDD(s) properly (it is recommended to use the same enterprise-level HDDs, including model and capacity, for array creation and configuration so as to maintain reliable and stable running of the disks).

Introduction

The DVR can store the data (e.g., record, picture, log information) in the HDD only after you have created the array or you have configured network HDD. There are two ways to create an array, including one-touch configuration and manual configuration. The following flow chart shows the process of creating an array.

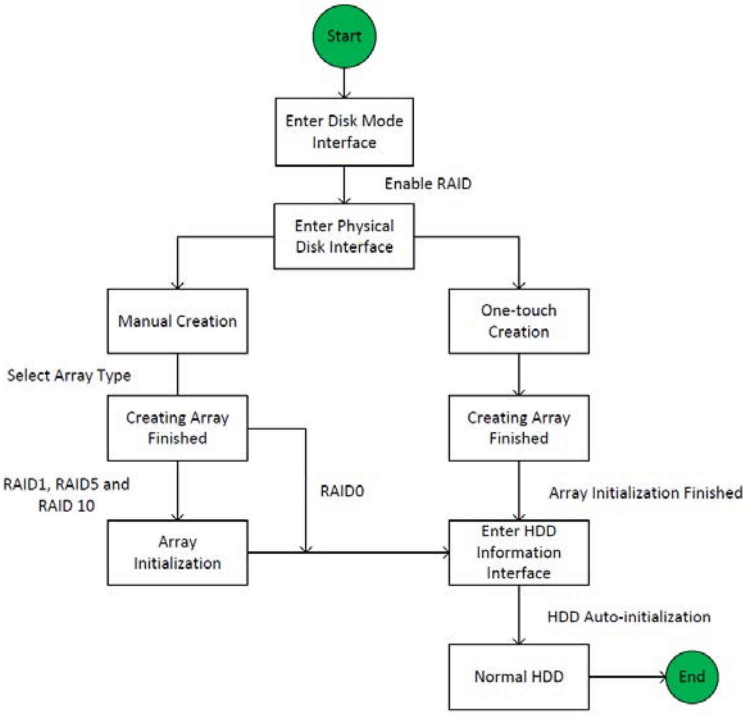


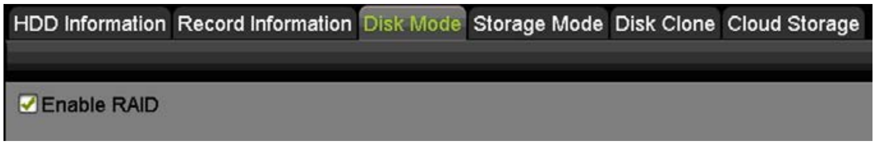
Figure 218, RAID Workflow

12.1.1 Enable RAID

Purpose

You must enable the RAID function before you can create the disk array.

1. Enter the Disk Mode configuration interface, Menu > System Configuration > HDD



☑ Enable RAID

Figure 219, Enable RAID Interface

2. Check the **Enable RAID** checkbox.

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

4. Reboot the device to have the RAID take effect.

12.1.2 One-Touch Configuration

Purpose

Through one-touch configuration, you can quickly create the disk array. By default, the array type to be created is RAID 5.

Before You Start

The RAID function should be enabled.

As the default array type is RAID 5, install at least three HDDs in you device. If more than 10 HDDs are installed, two arrays can be configured.

1. Enter the RAID configuration interface, Menu > System Configuration > RAID.

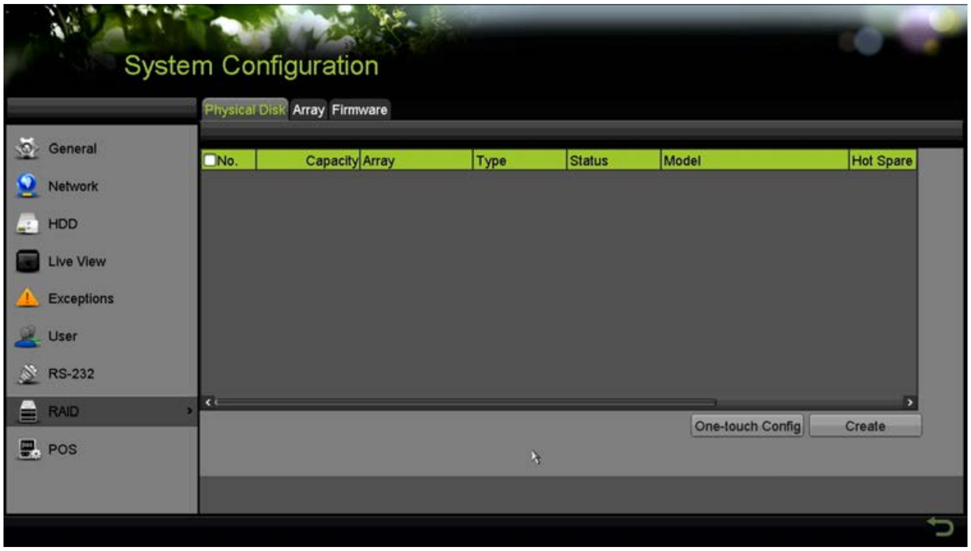


Figure 220, Physical Disk Interface

2. Check the corresponding HDD No. checkbox to select it.

3. Click **One-touch Config** to enter the One-touch Array Configuration interface.

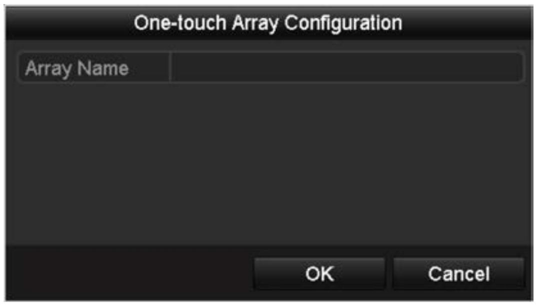


Figure 221, One-touch Array Configuration

4. Edit the array name in the **Array Name** text filed and click **OK** to start configuring the array.

NOTE

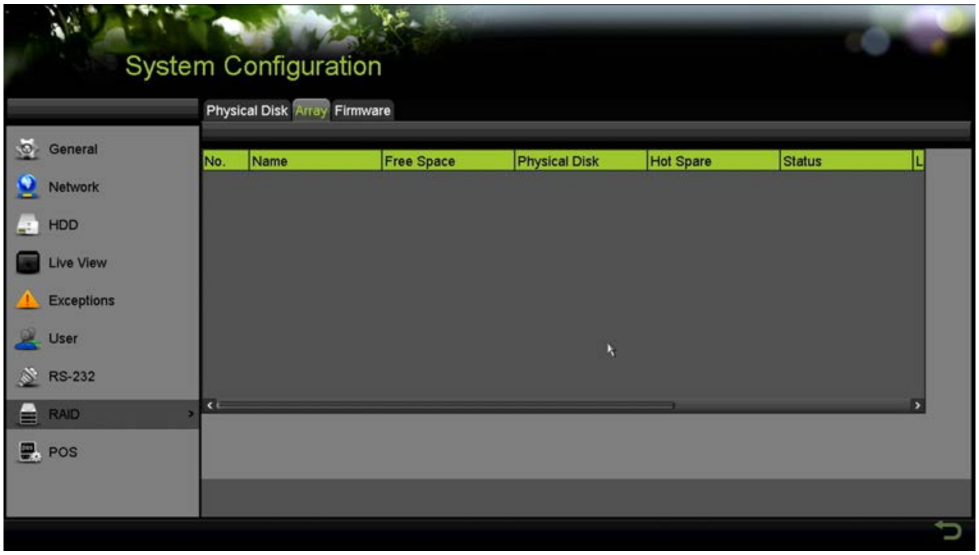
If you install four HDDs or more for one-touch configuration, a hot spare disk will be set by default. It is recommended to set a hot spare disk to automatically rebuild the array if the array becomes abnormal.

5. When the array configuration is completed, click **OK** in the pop-up message box to finish the settings.

6. Click **Array** tab to view the information of the successfully created array.

NOTE

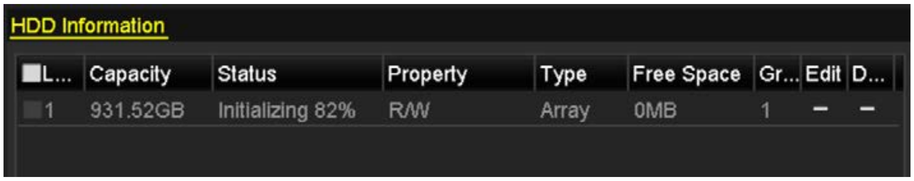
By default, one-touch configuration creates an array and a virtual disk.



No.	Name	Free Space	Physical Disk	Hot Spare	Status	L

Figure 222, Array Settings Interface

7. A created array displays as an HDD in the HDD information interface.



L...	Capacity	Status	Property	Type	Free Space	Gr...	Edit	D...
1	931.52GB	Initializing 82%	R/W	Array	0MB	1	–	–

Figure 223, HDD Information Interface

12.1.3 Manually Creating Array

Purpose

You can manually create a RAID 0, RAID 1, RAID 5, RAID6, or RAID 10 array.

NOTE

In this chapter, we take RAID 5 as an example to describe the manual configuration of array and virtual disk.

1. Enter the Physical Disk Settings interface, Menu > HDD > RAID > Physical Disk

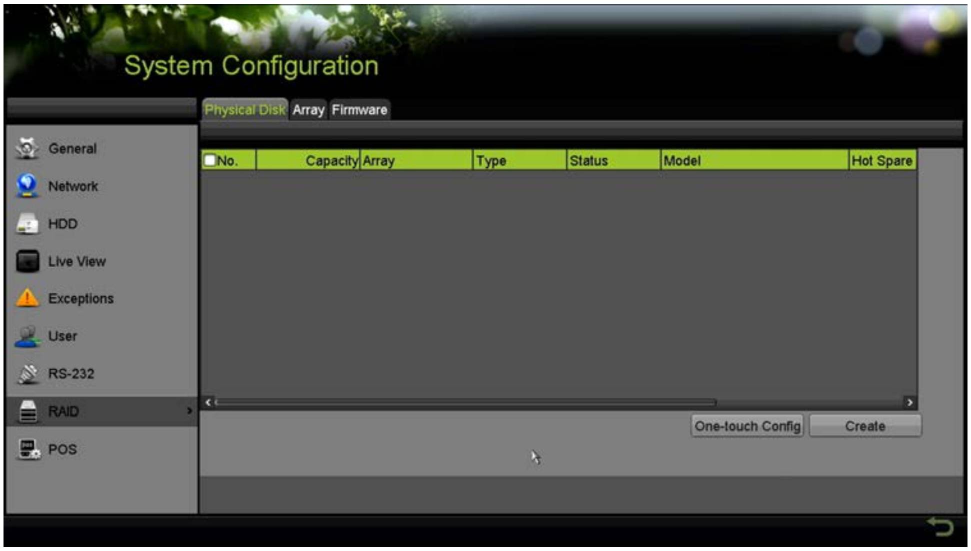
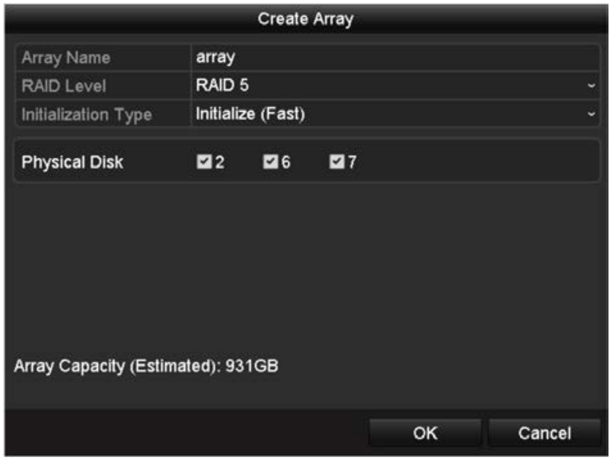


Figure 224, Physical Disk Settings Interface

2. Click Create to enter the Create Array interface.



Create Array

Array Name	array
RAID Level	RAID 5
Initialization Type	Initialize (Fast)

Physical Disk ☑2 ☑6 ☑7

Array Capacity (Estimated): 931GB

Figure 225, Create Array Interface

3. Edit the Array Name, set the RAID Level to RAID 0, RAID 1, RAID 5, RAID 6 or RAID 10, select the Physical Disk on which to configure the array.

   If you choose RAID 0, at least two HDDs must be installed.

   If you choose RAID 1, two HDDs need to be configured for RAID 1.

   If you choose RAID 5, at least three HDDs must be installed.

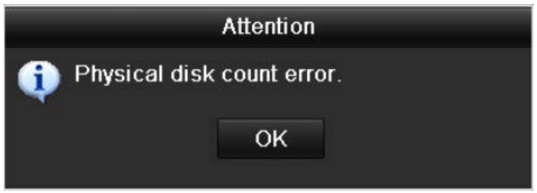
   If you choose RAID 6, at least four HDDs must be installed.

   If you choose RAID 10, the number of HDDs installed should be even in the range of four to 16.

4. Click **OK** to create the array.

NOTE

If the number of HDDs you select is not compatible with the requirement of the RAID level, the error message box will pop up.

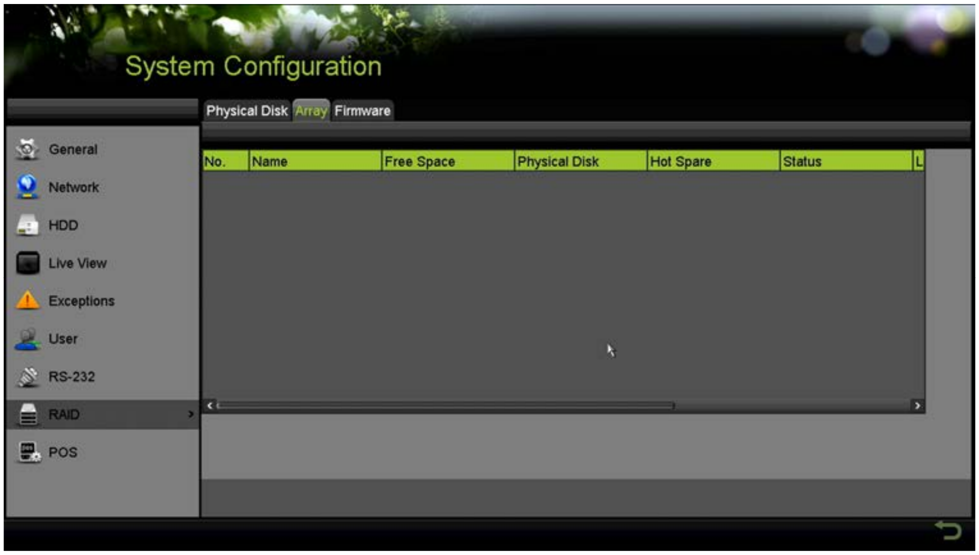


Attention

Physical disk count error.

Figure 226, Error Message Box

5. Click Array tab to view the successfully created array.



System Configuration

No.	Name	Free Space	Physical Disk	Hot Spare	Status	L

Figure 227, Array Settings Interface

12.1.4 Rebuilding Array

Purpose

The working status of an array includes Functional, Degraded, and Offline. By viewing the array status, you can take immediate and proper maintenance for the disks so as to ensure the high security and reliability of the data stored in the disk array.

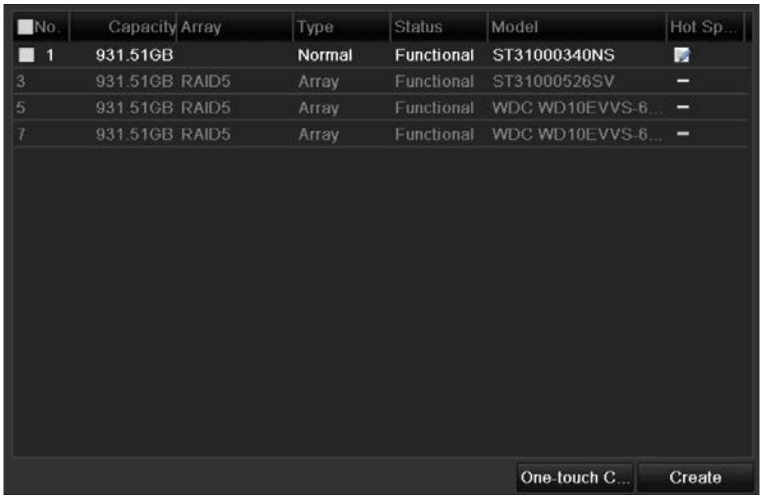
When there is no disk loss in the array, the working status of array will change to Functional; if the number of lost disks has exceeded the limit, the working status of array will change to Offline; in other conditions, the working status is Degraded.

When the virtual disk is in Degraded status, you can restore it to Functional by array rebuilding.

Before You Start

Make sure the hot spare disk is configured.

1. Enter the Physical Disk Settings interface to configure the hot spare disk.



□No.	Capacity	Array	Type	Status	Model	Hot Sp...
□ 1	931.51GB		Normal	Functional	ST31000340NS	✎
3	931.51GB	RAID5	Array	Functional	ST31000526SV	–
5	931.51GB	RAID5	Array	Functional	WDC WD10EVVS-6...	–
7	931.51GB	RAID5	Array	Functional	WDC WD10EVVS-6...	–

Figure 228, Physical Disk Settings Interface

2. Select a disk and click ✎ to set it as the hot spare disk.

NOTE

Only global hot spare mode is supported.

12.1.5 Automatically Rebuilding Array

Purpose

When the virtual disk is in Degraded status, the device can start rebuilding the array automatically with the hot spare disk to ensure the high security and reliability of the data.

1. Enter the Array Settings interface, Menu > System Configuration > HDD > RAID > Array. The status of the array is Degraded. Since the hot spare disk is configured, the system will automatically start rebuilding using it.

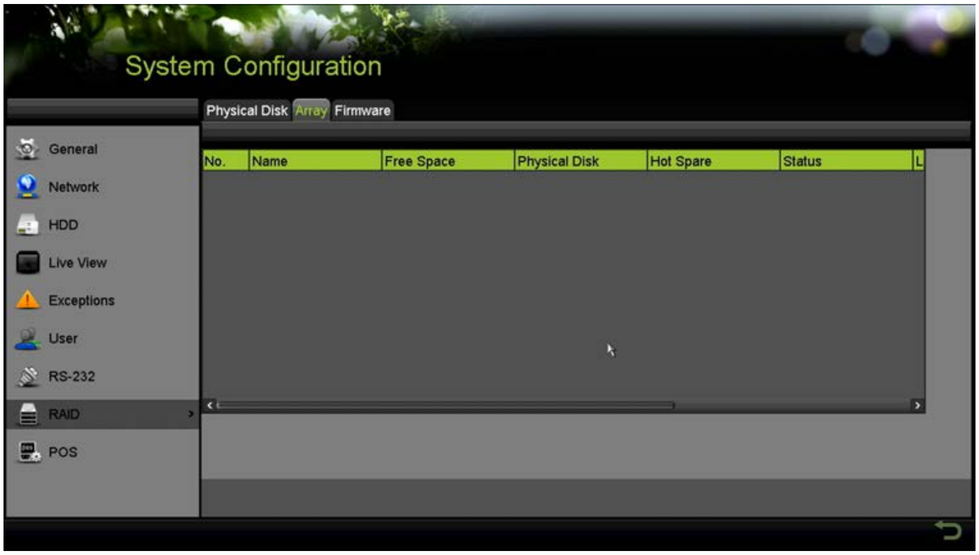


Figure 229, Array Settings Interface

2. If there is no hot spare disk after rebuilding, it is recommended to install an HDD into the device and set is as a hot spare disk to ensure the high security and reliability of the array.

12.1.6 Manually Rebuilding Array

Purpose

If the hot spare disk has not been configured, you can rebuild the array manually to restore the array when the virtual disk is in Degraded status.

1. Enter the Array Settings interface, Menu > System Configuration > HDD > RAID > Array.

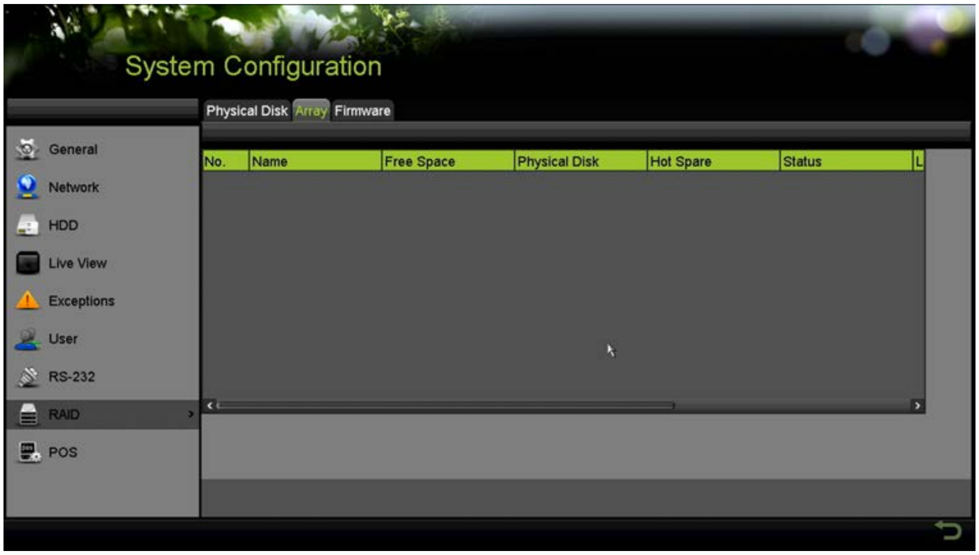
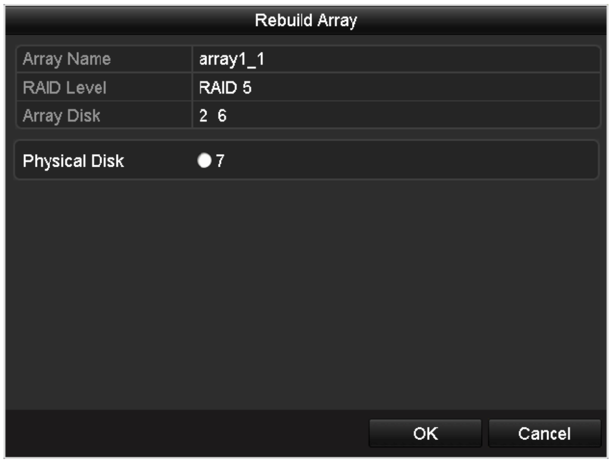


Figure 230, Array Settings Interface

2. Click the Array tab to return to the Array Settings interface and click 📝 to configure the array rebuild.

NOTE

At least one available physical disk must exist for rebuilding the array.



Rebuild Array

Array Name	array1_1
RAID Level	RAID 5
Array Disk	2 6

Physical Disk ○ 7

Figure 231, Rebuild Array Interface

3. Select the available physical disk and click OK to confirm rebuilding the array.

4. The “Do not unplug the physical disk when it is under rebuilding” message box pops up. Click **OK** to start rebuilding.

5. Enter the Array Settings interface to view the rebuilding status.

6. After rebuilding successfully, the array and virtual disk will restore to Functional.

12.1.7 Deleting Array

NOTE

Deleting an array will cause deletion of all data saved on the disk.

1. Enter the Array Settings interface, Menu > System Configuration > HDD > RAID > Array.

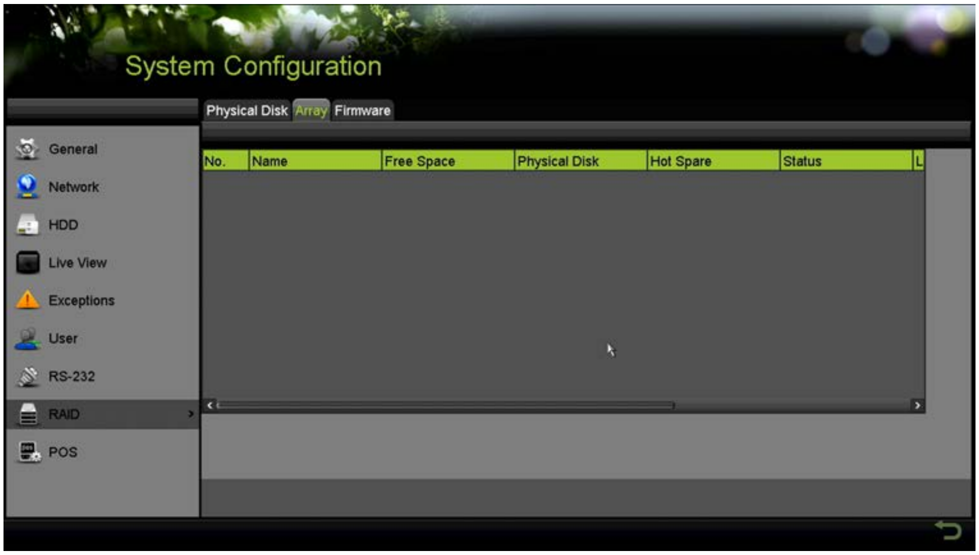
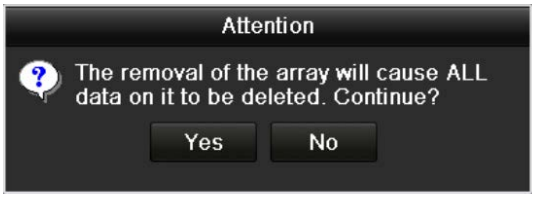


Figure 232, Array Settings Interface

2. Select an array and click 🗑 to delete the array.



Attention

The removal of the array will cause ALL data on it to be deleted. Continue?

Figure 233, Confirm Array Deletion

3. In the pop-up message box, click **Yes** to confirm the array deletion.

NOTE

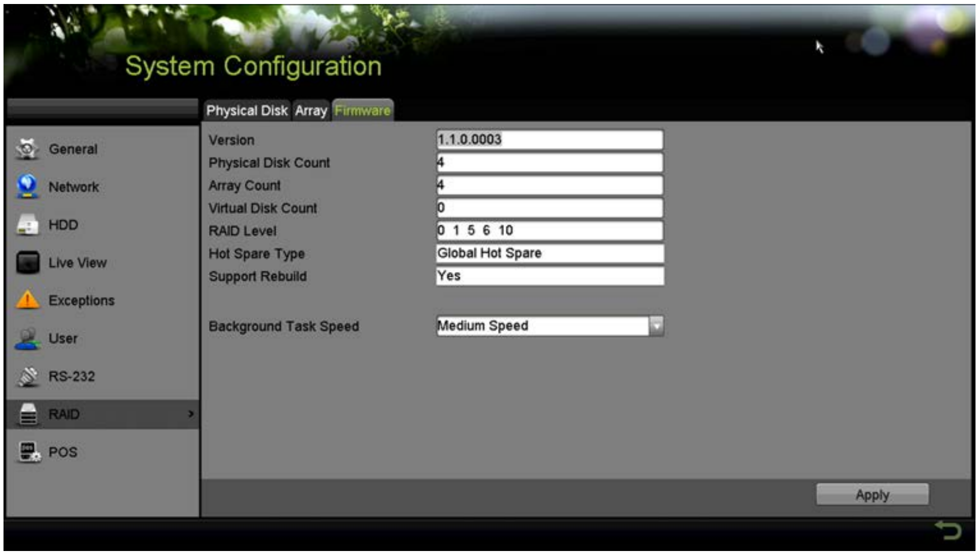
Deleting an array will delete all data in the array.

13 Checking and Editing Firmware

Purpose

You can view the firmware information and set the background task speed on the Firmware interface.

1. Enter the Firmware interface to check the firmware information, including the version, maximum physical disk quantity, maximum array quantity, auto-rebuild status, etc.



Version: 1.1.0.0003
Physical Disk Count: 4
Array Count: 4
Virtual Disk Count: 0
RAID Level: 0 1 5 6 10
Hot Spare Type: Global Hot Spare
Support Rebuild: Yes

Background Task Speed: Medium Speed

Figure 234, Firmware Interface

2. You can set the Background Task Speed in the drop-down list.

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

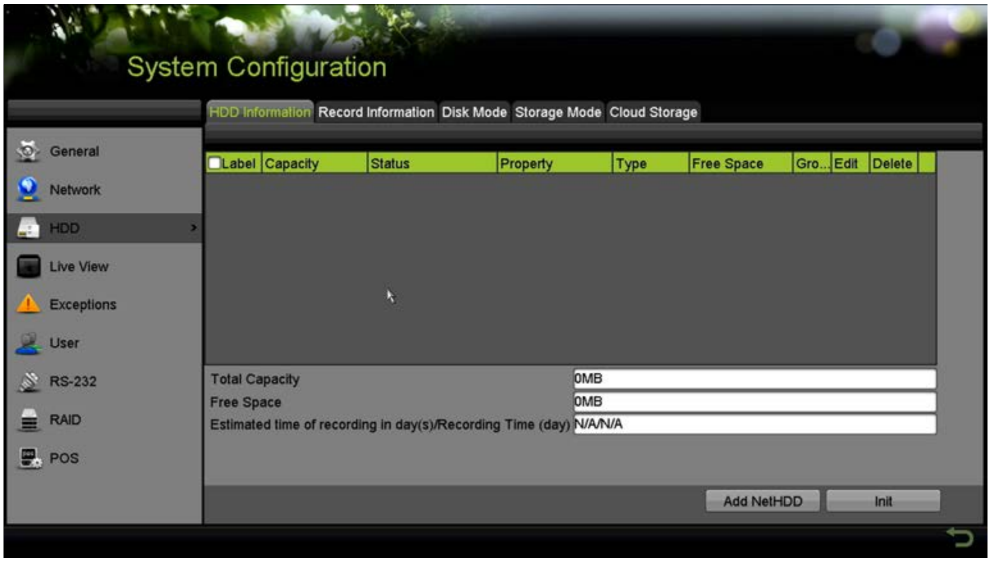
14 HDD Management

14.1 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.



□Label	Capacity	Status	Property	Type	Free Space	Gro...	Edit	Delete

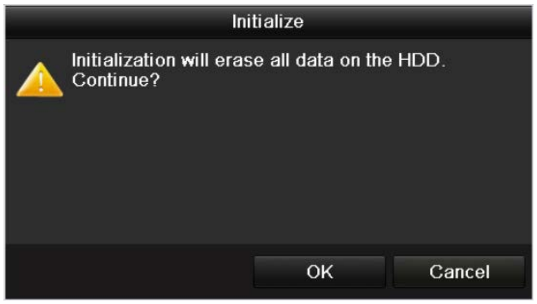
Total Capacity: 0MB
Free Space: 0MB
Estimated time of recording in day(s)/Recording Time (day): N/A/N/A

Figure 235, HDD Information Interface

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

3. Select HDD to be initialized.

4. Click **Init**.

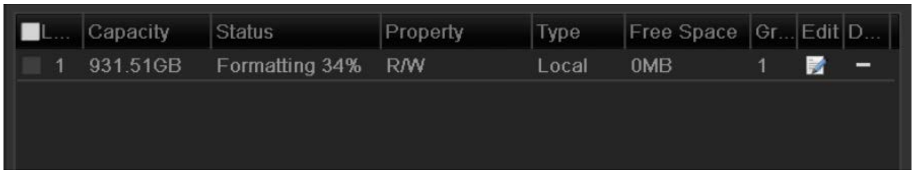


Initialize

Initialization will erase all data on the HDD. Continue?

Figure 236, Confirm Initialization

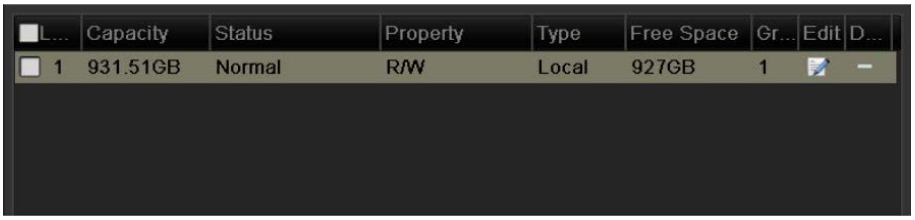
5. Select **OK** to start initialization.



□L...	Capacity	Status	Property	Type	Free Space	Gr...	Edit	D...
□ 1	931.51GB	Formatting 34%	R/W	Local	0MB	1	✎	−

Figure 237, Start Initialization

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



□L...	Capacity	Status	Property	Type	Free Space	Gr...	Edit	D...
□ 1	931.51GB	Normal	R/W	Local	927GB	1	✎	−

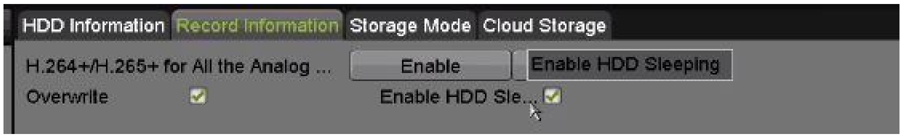
Figure 238, HDD Status Changes to Normal

NOTE

Initializing the HDD will erase all data on it.

HDDs that are free of working for a long time can be enabled to sleep, thus to decrease the power consumption of the device and extend the life of the HDDs.

7. Go to Menu > System Configuration > HDD > Advanced.



H.264+/H.265+ for All the Analog ... Enable

Enable HDD Sleeping

Overwrite ☑

Enable HDD Sle... ☑

Figure 239, Enable HDD Sleeping

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

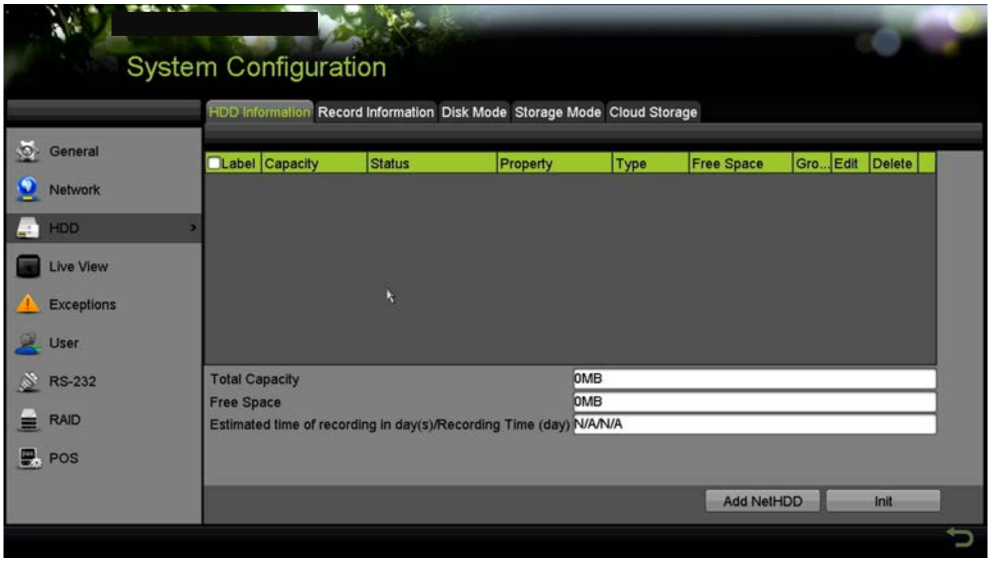
Uncheck the **Enable HDD Sleeping** checkbox, and the HDDs will never sleep.

14.2 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.


[redacted]

□ Label	Capacity	Status	Property	Type	Free Space	Gro...	Edit	Delete

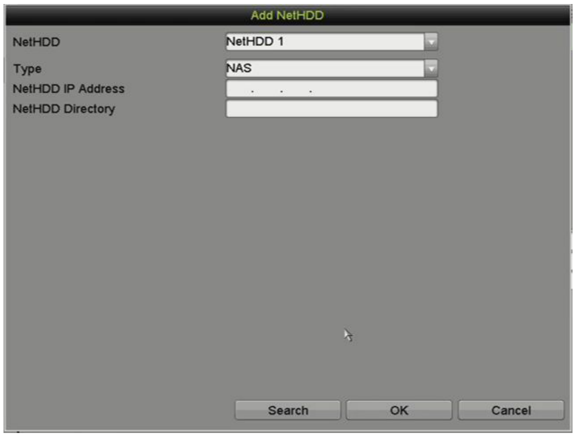
Total Capacity: 0MB

Free Space: 0MB

Estimated time of recording in day(s)/Recording Time (day): N/A/N/A

Figure 240, HDD Information Interface

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



NetHDD: NetHDD 1

Type: NAS

NetHDD IP Address: . . .

NetHDD Directory:

Figure 241, NetHDD Information Interface

3. Add the allocated NetHDD.

4. Set the type to NAS or IP SAN.

5. Configure the NAS or IP SAN settings.

- **Add NAS disk**

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

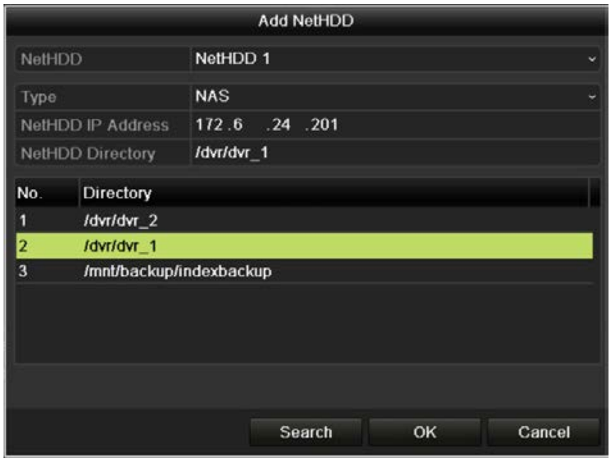
2) Click **Search** to search the available NAS disks.

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.



NetHDD: NetHDD 1

Type: NAS

NetHDD IP Address: 172 .6 .24 .201

NetHDD Directory: /dvr/dvr_1

No.	Directory
1	/dvr/dvr_2
2	/dvr/dvr_1
3	/mnt/backup/indexbackup

Figure 242, Add NAS Disk

- **Add IP SAN**

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

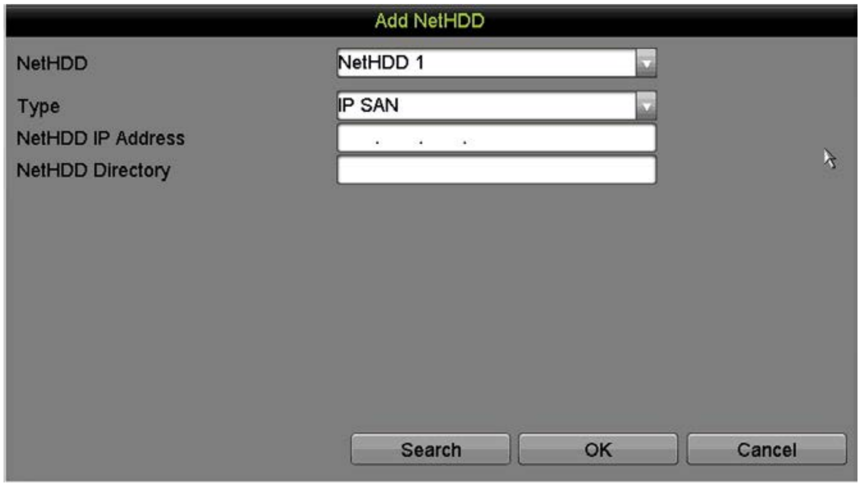
2) Click **Search** to the available IP SAN disks.

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.



Add NetHDD

NetHDD: NetHDD 1

Type: IP SAN

NetHDD IP Address: . . .

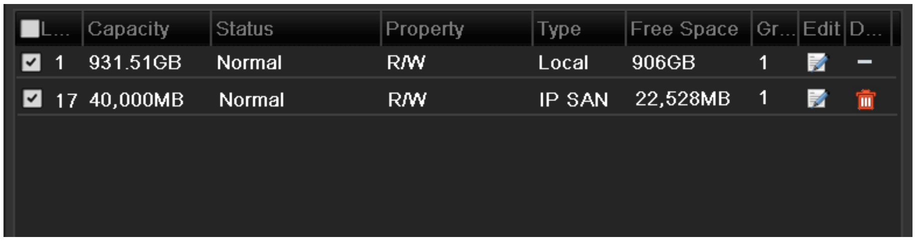
NetHDD Directory:

Figure 243, Add IP SAN Disk

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

NOTE

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



□ L...	Capacity	Status	Property	Type	Free Space	Gr...	Edit	D...
☑ 1	931.51GB	Normal	R/W	Local	906GB	1	📝	−
☑ 17	40,000MB	Normal	R/W	IP SAN	22,528MB	1	📝	🗑

Figure 244, Initialize Added NetHDD

14.3 Managing HDD Group

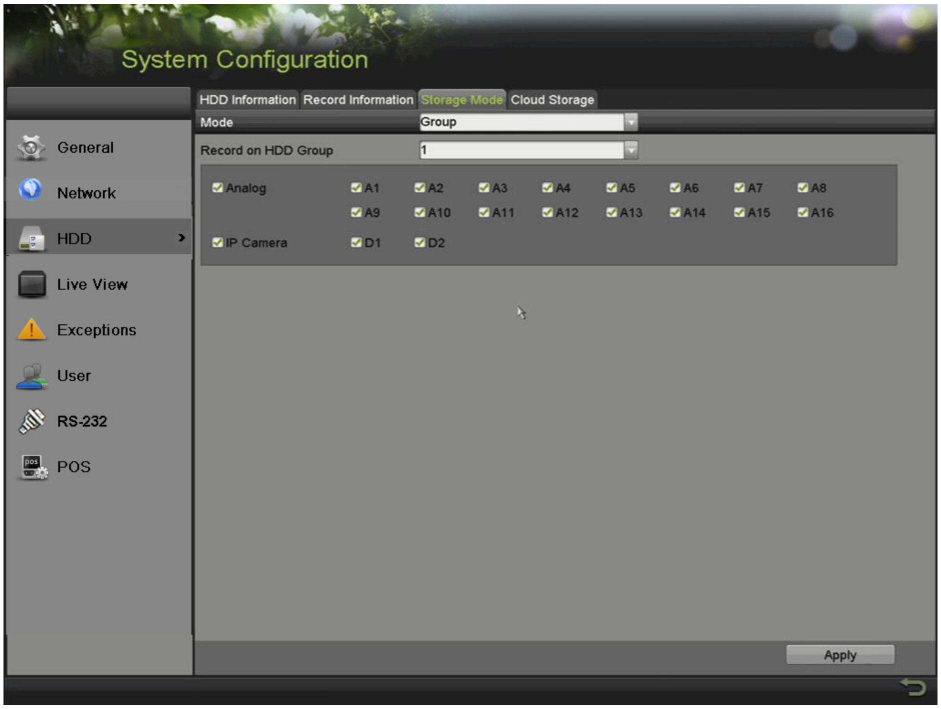
14.3.1 Setting HDD Groups

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.

2. Set the **Mode** to Group, as shown below.



Mode: Group

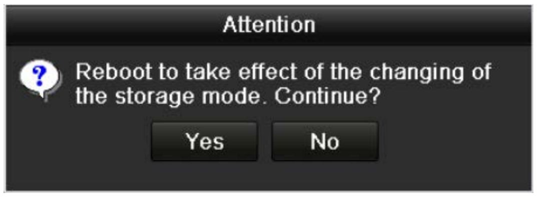
Record on HDD Group: 1

☑ Analog: ☑ A1 ☑ A2 ☑ A3 ☑ A4 ☑ A5 ☑ A6 ☑ A7 ☑ A8 ☑ A9 ☑ A10 ☑ A11 ☑ A12 ☑ A13 ☑ A14 ☑ A15 ☑ A16

☑ IP Camera: ☑ D1 ☑ D2

Figure 245, Storage Mode Interface

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



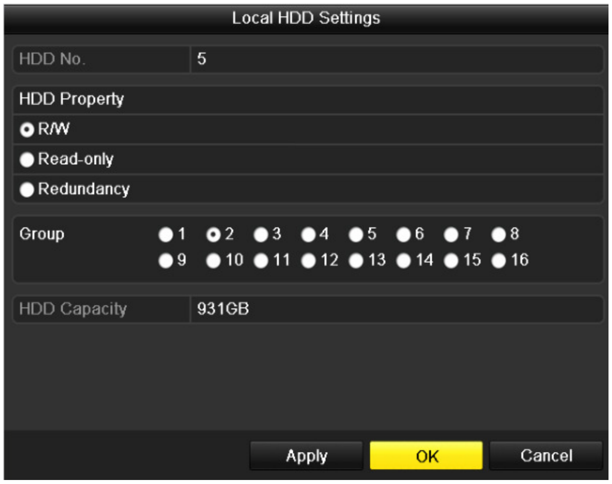
Reboot to take effect of the changing of the storage mode. Continue?

Figure 246, Attention for Reboot

4. Click **Yes** to reboot the device to activate the changes.

5. After rebooting the device, go to Menu > System Configuration > HDD > General.

6. Select HDD from the list and click 📝 to enter the **Local HDD Settings** interface, as shown below.



Local HDD Settings

HDD No.: 5

HDD Property

- ● R/W
- ○ Read-only
- ○ Redundancy

Group: ○ 1 ● 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7 ○ 8 ○ 9 ○ 10 ○ 11 ○ 12 ○ 13 ○ 14 ○ 15 ○ 16

HDD Capacity: 931GB

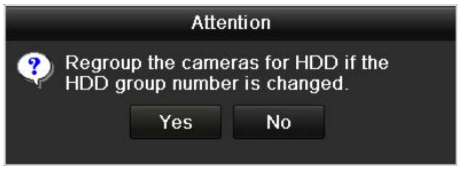
Figure 247, Local HDD Settings Interface

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.



Attention

Regroup the cameras for HDD if the HDD group number is changed.

Figure 248, Confirm HDD Group Settings

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

14.4 Setting HDD Property

Purpose

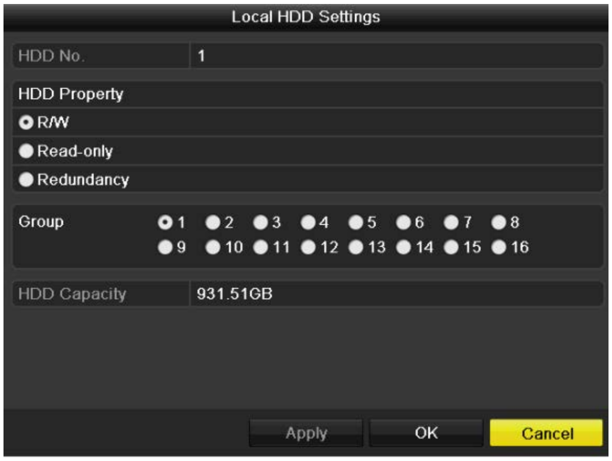
The HDD property can be set to redundancy, read-only, or read/write (R/W). Before setting the HDD property, set the storage mode to Group.

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 > HDD > General.

2. Select HDD from the list and click ✎ to enter the **Local HDD Settings** interface, as shown below.



Local HDD Settings

HDD No. 1

HDD Property

◉ R/W

● Read-only

● Redundancy

Group ◉ 1 ● 2 ● 3 ● 4 ● 5 ● 6 ● 7 ● 8 ● 9 ● 10 ● 11 ● 12 ● 13 ● 14 ● 15 ● 16

HDD Capacity 931.51GB

Figure 249, 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.

In the HDD Information menu, the HDD property will be displayed in the list.

NOTE

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

14.5 Configuring Quota Mode

Purpose

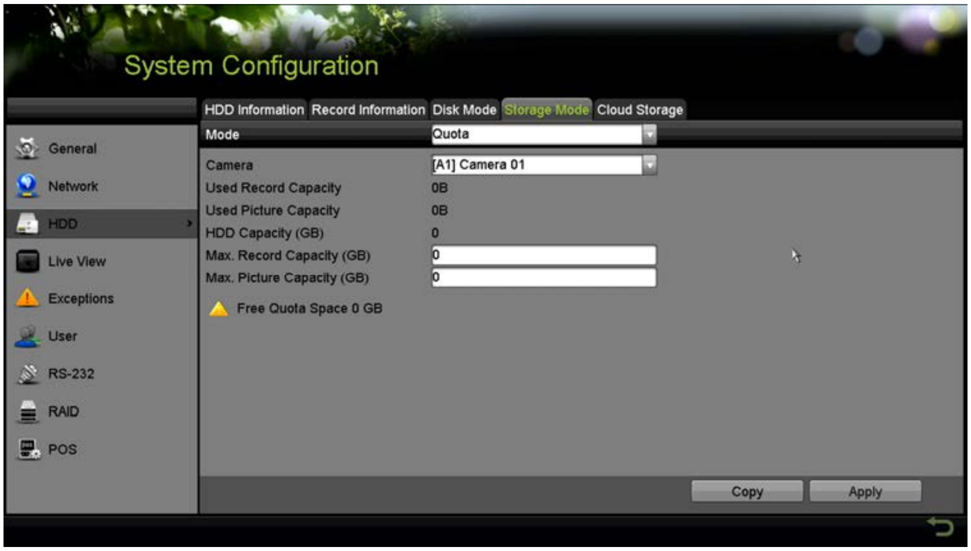
Each camera can be configured with allocated quota for the storage of recorded files.

1. Go to Menu > System Configuration > HDD > Advanced > Storage Mode.

2. Set the **Mode** to Quota, as shown below.

NOTE

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



Mode: Quota

Camera: [A1] Camera 01

Used Record Capacity: 0B

Used Picture Capacity: 0B

HDD Capacity (GB): 0

Max. Record Capacity (GB): 0

Max. Picture Capacity (GB): 0

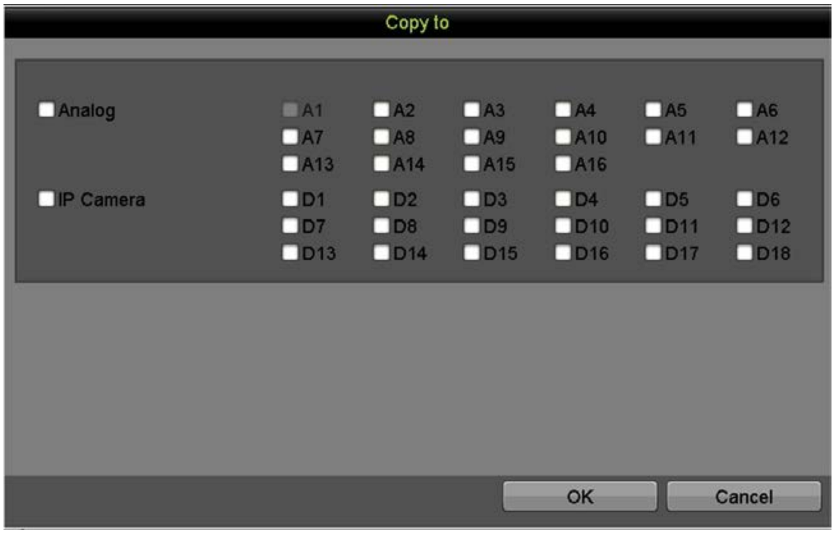
Free Quota Space 0 GB

Figure 250, Storage Mode Settings Interface

3. Select a camera for which you want to configure quota.

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

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



□ Analog — □ A1 □ A2 □ A3 □ A4 □ A5 □ A6 □ A7 □ A8 □ A9 □ A10 □ A11 □ A12 □ A13 □ A14 □ A15 □ A16

□ IP Camera — □ D1 □ D2 □ D3 □ D4 □ D5 □ D6 □ D7 □ D8 □ D9 □ D10 □ D11 □ D12 □ D13 □ D14 □ D15 □ D16 □ D17 □ D18

Figure 251, Copy Settings to Other Camera(s)

6. Select the camera(s) to be configured with the same quota settings. You can also click the checkbox of Analog 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 capacity of the HDD for record.

14.6 Configuring Cloud Storage

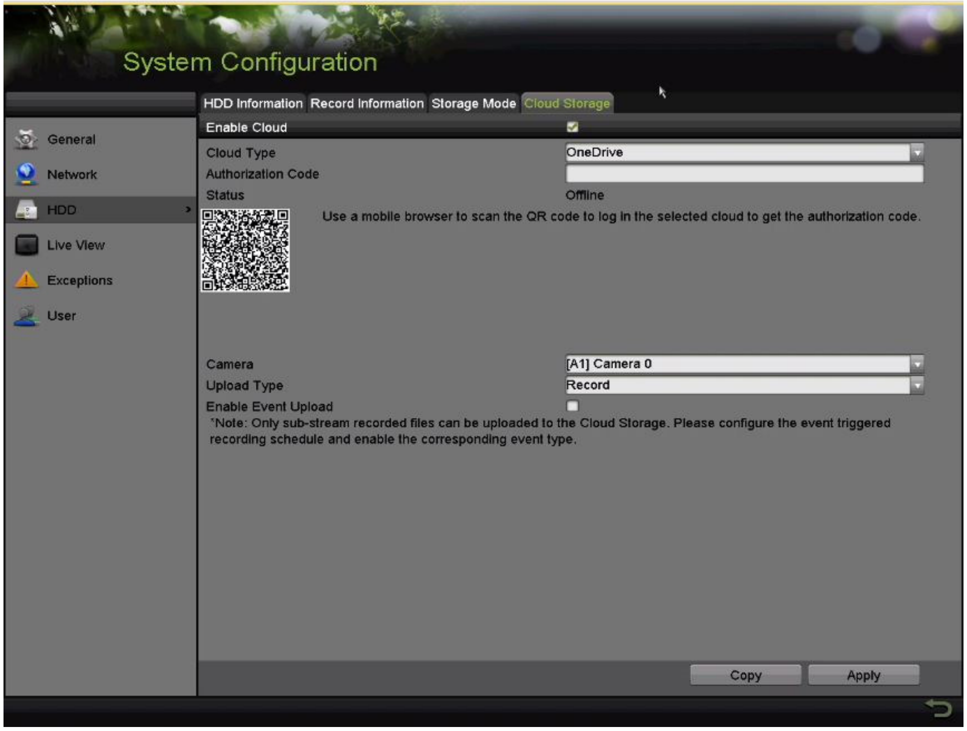
Purpose

Cloud storage facilitates uploading and downloading the recorded files at any time and any place, which can highly enhance the efficiency.

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

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

3. Select the **Cloud Type** from the drop-down list to One Drive, Google Drive, or Drop Box.



Enable Cloud ☑
Cloud Type OneDrive
Authorization Code
Status Offline
Use a mobile browser to scan the QR code to log in the selected cloud to get the authorization code.
Camera [A1] Camera 0
Upload Type Record
Enable Event Upload ☐
*Note: Only sub-stream recorded files can be uploaded to the Cloud Storage. Please configure the event triggered recording schedule and enable the corresponding event type.

Figure 252, Cloud Storage Interface

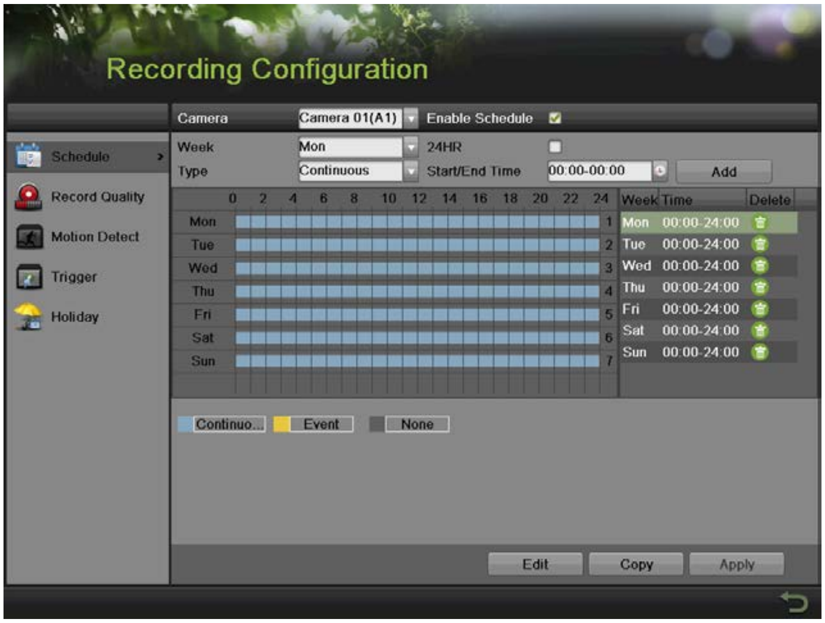
4. According to the prompts, you are required to use a mobile browser to scan the QR code to log in the selected cloud to get the authentication code, and then copy the authentication code to the **Authentication Code** text filed.

5. Click **Apply** and then go back to the main menu.

6. Enter the cloud storage interface again about 20s later. When the **Status** shows online, it indicates the successful registration.

7. Configure the recording schedule.

8. Go back to enter the record interface, choose a camera from the **Camera** drop-down list and check the **Enable Schedule** checkbox to enable the schedule recording.



Recording Configuration

Camera: Camera 01(A1) Enable Schedule ☑

Week: Mon 24HR □

Type: Continuous Start/End Time: 00:00-00:00

Week	Time	Delete
Mon	00:00-24:00	
Tue	00:00-24:00	
Wed	00:00-24:00	
Thu	00:00-24:00	
Fri	00:00-24:00	
Sat	00:00-24:00	
Sun	00:00-24:00	

Figure 253, Record Schedule

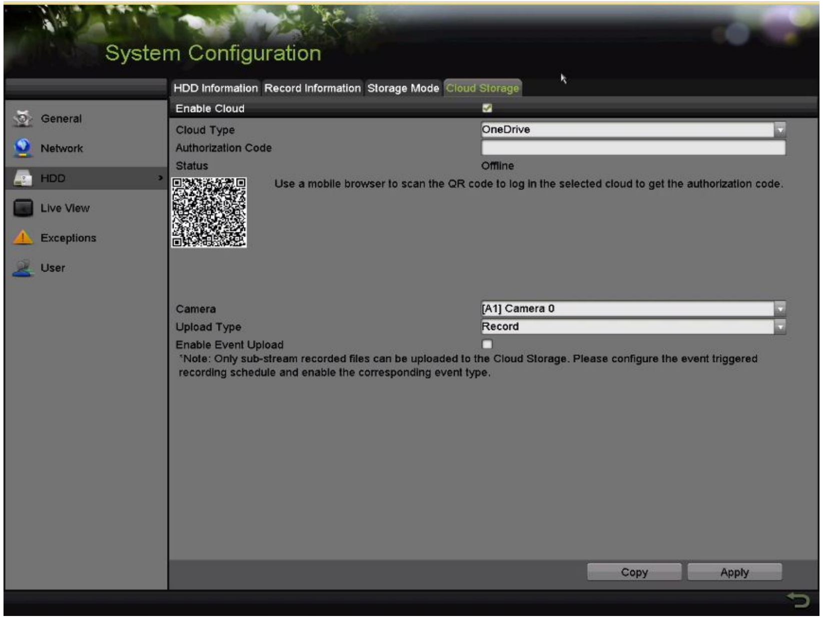
9. Upload the event triggered recording files to the cloud storage.

    1) Return to the cloud storage interface and select the camera you have set in the recording schedule interface.

    2) Select the upload type in the **Upload Type** text filed.

    3) Check the **Enable Event Upload** checkbox.

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



System Configuration

Enable Cloud ☑

Cloud Type: OneDrive

Authorization Code:

Status: Offline

Use a mobile browser to scan the QR code to log in the selected cloud to get the authorization code.

Camera: [A1] Camera 0

Upload Type: Record

Enable Event Upload □

*Note: Only sub-stream recorded files can be uploaded to the Cloud Storage. Please configure the event triggered recording schedule and enable the corresponding event type.

Figure 254, Upload to Cloud Storage Interface

NOTE

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

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

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

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

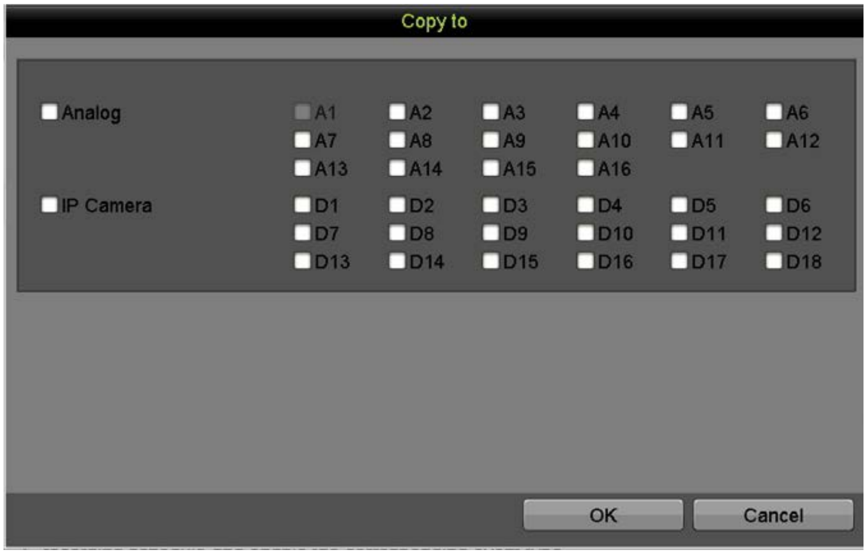

Copy to
□ Analog
□ A1 □ A2 □ A3 □ A4 □ A5 □ A6
□ A7 □ A8 □ A9 □ A10 □ A11 □ A12
□ A13 □ A14 □ A15 □ A16
□ IP Camera
□ D1 □ D2 □ D3 □ D4 □ D5 □ D6
□ D7 □ D8 □ D9 □ D10 □ D11 □ D12
□ D13 □ D14 □ D15 □ D16 □ D17 □ D18
OK
Cancel

Figure 255, Copy to Interface

14.7 Configuring Disk Clone

NOTE

This chapter is applicable to only DVRs with eSATA.

Purpose

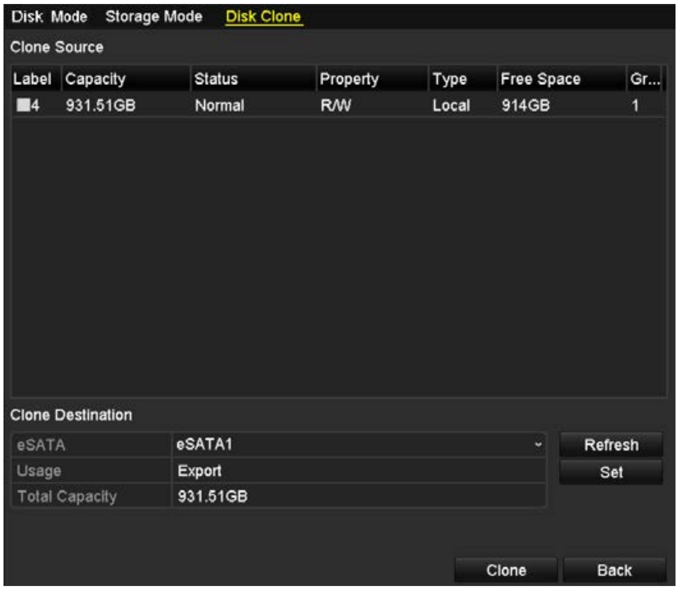
If the S.M.A.R.T. detection result declares the HDD is abnormal, you can choose to clone all the data on the HDD to an inserted eSATA disk manually.

Before You Start

An eSATA disk should be connected to the device.

1. Enter the HDD Advanced Setting interface, Menu > System Configuration > HDD > Advanced.

2. Click the **Disk Clone** tab to enter the disk clone configuring interface.



Clone Source

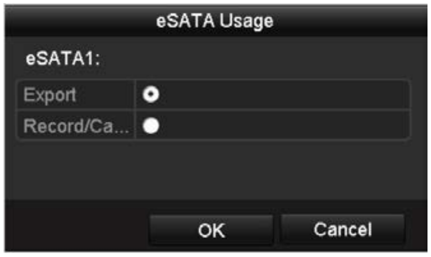
Label	Capacity	Status	Property	Type	Free Space	Gr...
□4	931.51GB	Normal	R/W	Local	914GB	1

Clone Destination

eSATA	eSATA1
Usage	Export
Total Capacity	931.51GB

Figure 256, Disk Clone Configuration Interface

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



eSATA1:

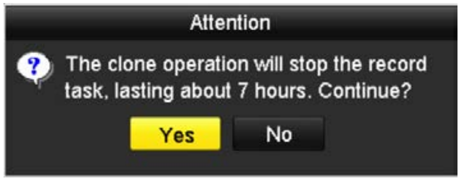
Export	◉
Record/Ca...	○

Figure 257, Setting eSATA Usage

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

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

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

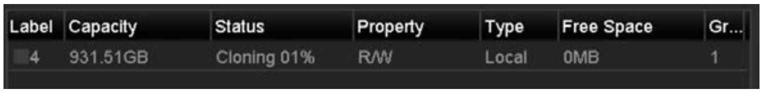


The clone operation will stop the record task, lasting about 7 hours. Continue?

Figure 258, Message Box for Disk Clone

6. Click **Yes** to continue.

7. You can check the clone progress in the HDD status.



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

Figure 259, Check Disk Clone Progress

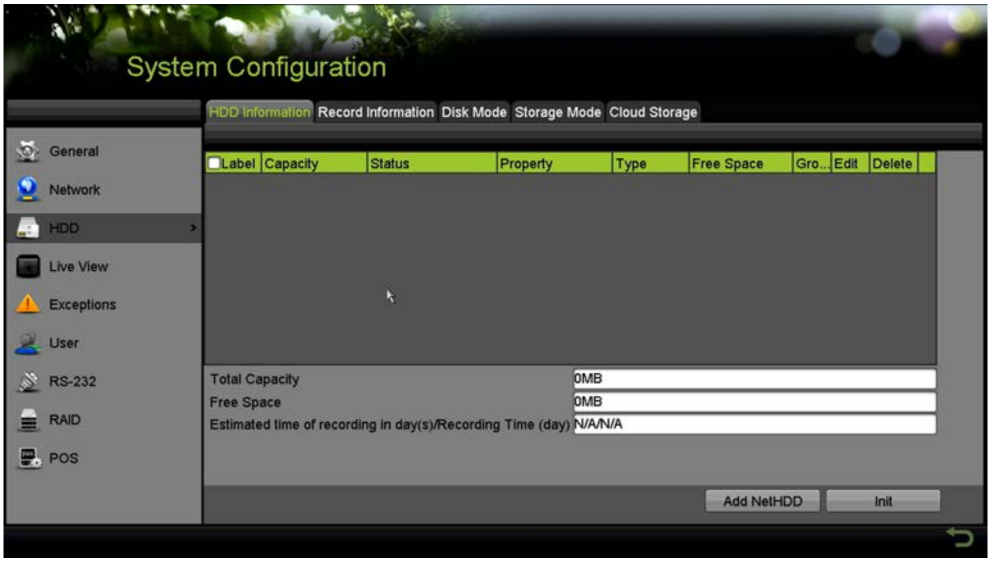
14.8 Checking HDD Status

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.

1. Go to Menu > System Configuration > HDD.

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



Total Capacity 0MB
Free Space 0MB
Estimated time of recording in day(s)/Recording Time (day) N/A/N/A

Figure 260, View HDD Status (1)

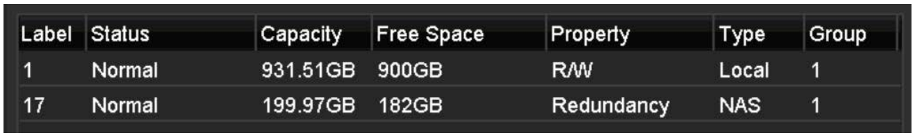
NOTE

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

Checking HDD Status in System Information Interface

3. Go to Menu > Maintenance > System Info > HDD.

4. View the status of each HDD displayed on the list, as shown below.



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

Figure 261, View HDD Status (2)

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

Purpose

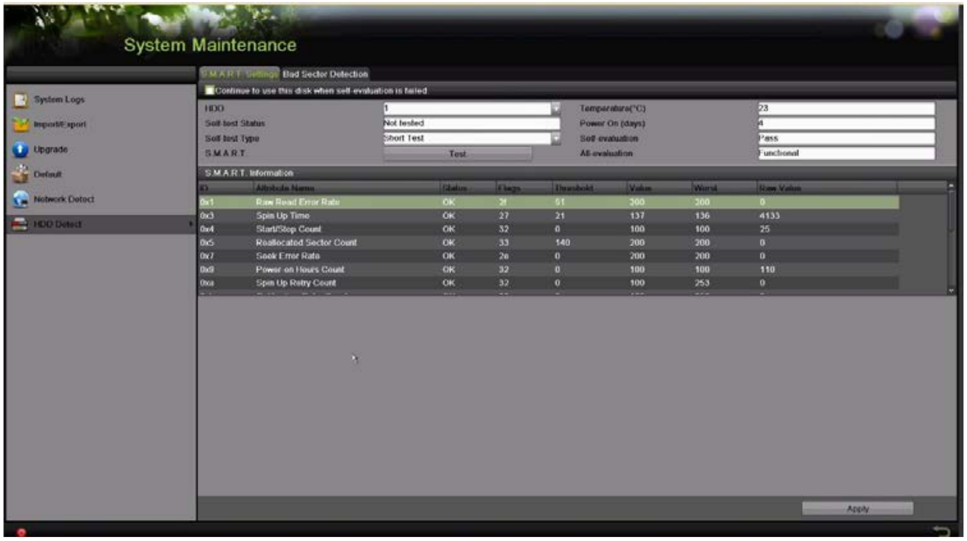
The S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology) is a monitoring system for HDD to detect *a*nd report on various indicators of reliability in the hopes of anticipating failures.

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 checkbox before the **Continue to use this disk when self-evaluation is failed** item.



□ Continue to use this disk when self-evaluation is failed.

HDD	1	Temperature(°C)	23
Self-test Status	Not tested	Power On (days)	4
Self-test Type	Short Test	Self-evaluation	Pass
S.M.A.R.T.	Test	All-evaluation	Functional

S.M.A.R.T. Information

ID	Attribute Name	Status	Flags	Threshold	Value	Worst	Raw Value
0x1	Raw Read Error Rate	OK	2f	51	200	200	0
0x3	Spin Up Time	OK	27	21	137	136	4133
0x4	Start/Stop Count	OK	32	0	100	100	25
0x5	Reallocated Sector Count	OK	33	140	200	200	0
0x7	Seek Error Rate	OK	2e	0	200	200	0
0x9	Power on Hours Count	OK	32	0	100	100	110
0xa	Spin Up Retry Count	OK	32	0	100	253	0

Figure 262, S.M.A.R.T. Settings Interface

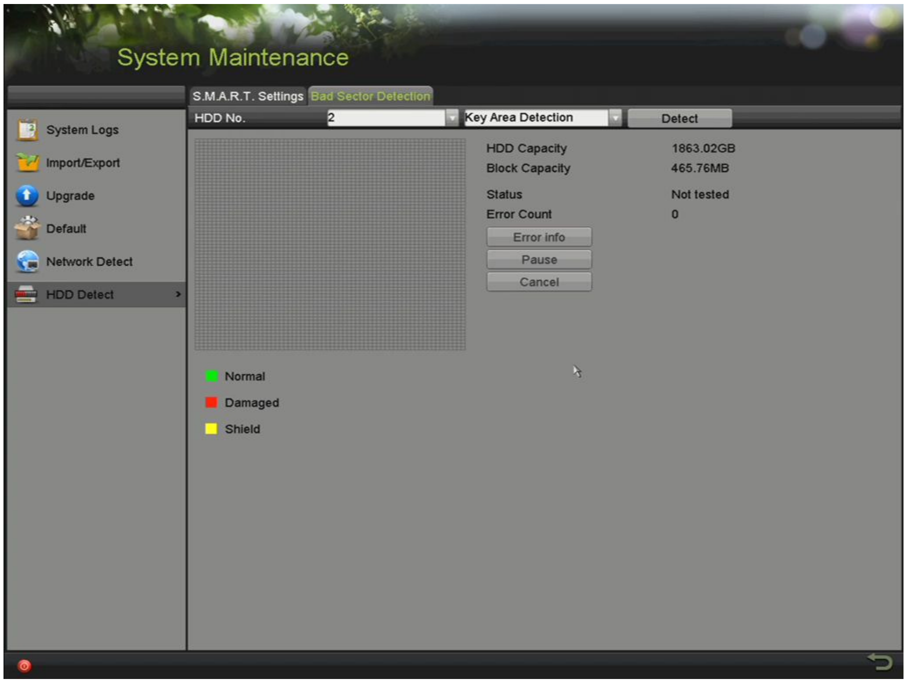
14.10 Detecting Bad Sectors

Purpose

You can detect the bad sector(s) of the HDD to check the status of the HDD.

1. Go to Menu > Maintenance > HDD Detect > Bad Sector Detection.

2. Select an HDD and click **Detect** to start detecting.



HDD No. 2

Key Area Detection

HDD Capacity 1863.02GB

Block Capacity 465.76MB

Status Not tested

Error Count 0

🟩 Normal

🟥 Damaged

🟨 Shield

Figure 263, 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.

14.11 Configuring HDD Error Alarms

Purpose

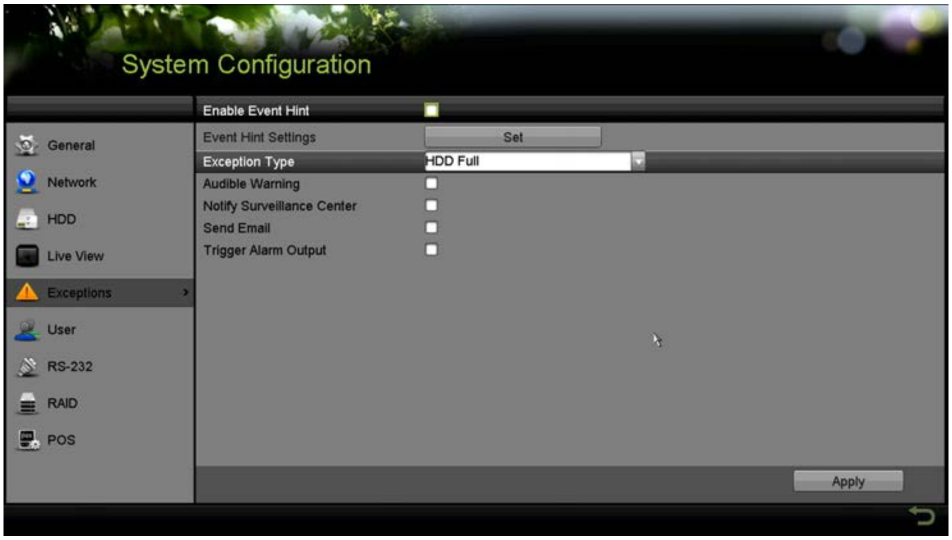
You can configure the HDD error alarms when the HDD status is *Uninitialized* or *Abnormal*.

1. Go to Menu > System Configuration > Exceptions.

2. Select the Exception Type to **HDD Error** from the drop-down list.

3. Check the checkbox(s) below to select the linkage action(s) for an HDD error, as shown in Figure 12-26.

4. The linkage actions can be selected to: Audible Warning, Notify Surveillance Center, Send Email, and Trigger Alarm Output.



Enable Event Hint ☑
Event Hint Settings
Exception Type: HDD Full
Audible Warning ☐
Notify Surveillance Center ☐
Send Email ☐
Trigger Alarm Output ☐

Figure 264, Configure HDD Error Alarm

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

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

15 Camera Settings

15.1 Configuring OSD Settings

Purpose

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

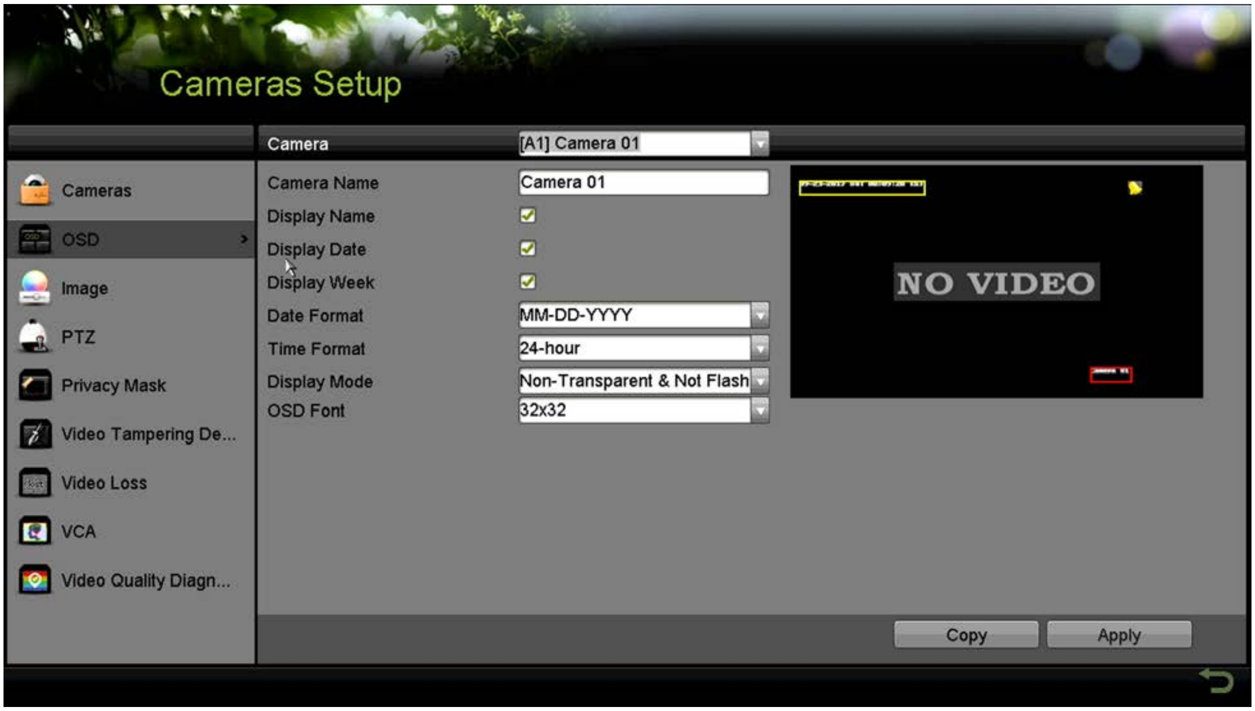
1. Go to Menu > Cameras Setup > OSD.

2. Select the camera for which to configure OSD settings.

3. Edit the **Camera Name** in the text field.

4. Configure the **Display Name**, **Display Date,** and **Display Week** by checking the checkbox.

5. Select the Date Format, Time Format, Display Mode, and the OSD Font.



Camera: [A1] Camera 01

Camera Name: Camera 01

Display Name ☑

Display Date ☑

Display Week ☑

Date Format: MM-DD-YYYY

Time Format: 24-hour

Display Mode: Non-Transparent & Not Flash

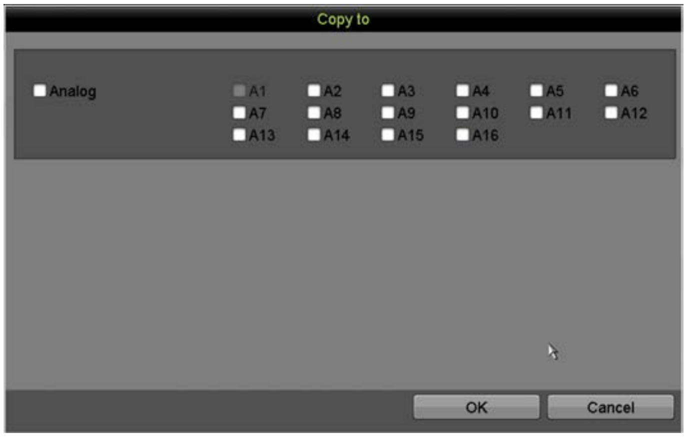
OSD Font: 32x32

Figure 265, 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.



□ Analog

□ A1 □ A2 □ A3 □ A4 □ A5 □ A6
□ A7 □ A8 □ A9 □ A10 □ A11 □ A12
□ A13 □ A14 □ A15 □ A16

Figure 266, Copy Settings to Other Cameras

    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.

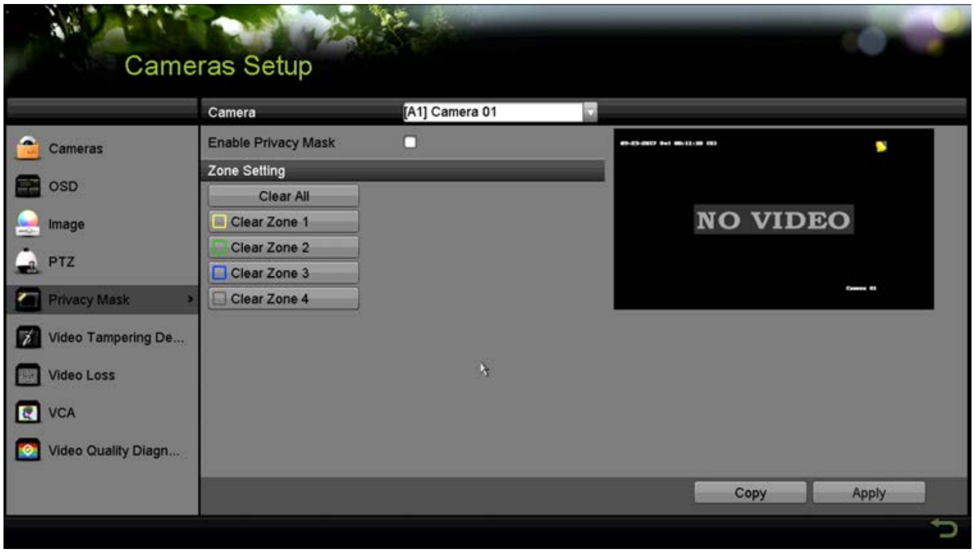
8. Click **Apply** to apply the settings.

15.2 Configuring Privacy Mask

Purpose

To configure the four-sided privacy mask zones that cannot be viewed or recorded by the operator as follows.

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



Camera: [A1] Camera 01

Enable Privacy Mask □

Figure 267, Privacy Mask Settings Interface

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

NOTE

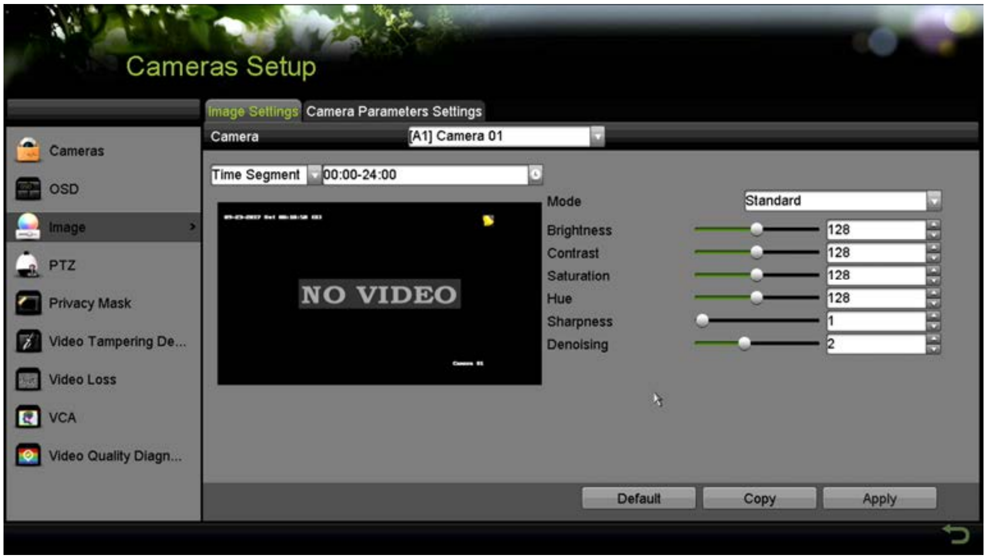
Up to four privacy mask zones can be defined, and the size of each area can be adjusted.

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.
6. You can click **Copy** to copy the privacy mask settings of the current camera to other cameras.
7. Click **Apply** to save the settings.

15.3 Configuring Video Parameters

15.3.1 Configuring Image Settings

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



Camera: [A1] Camera 01

Time Segment: 00:00-24:00

Mode	Standard
Brightness	128
Contrast	128
Saturation	128
Hue	128
Sharpness	1
Denoising	2

Figure 268, Image Settings Interface

2. Select the camera for which to set 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 drop-down list of **Mode**, there are four modes selectable for analog cameras: Standard, Indoor, Dim Light, and Outdoor.

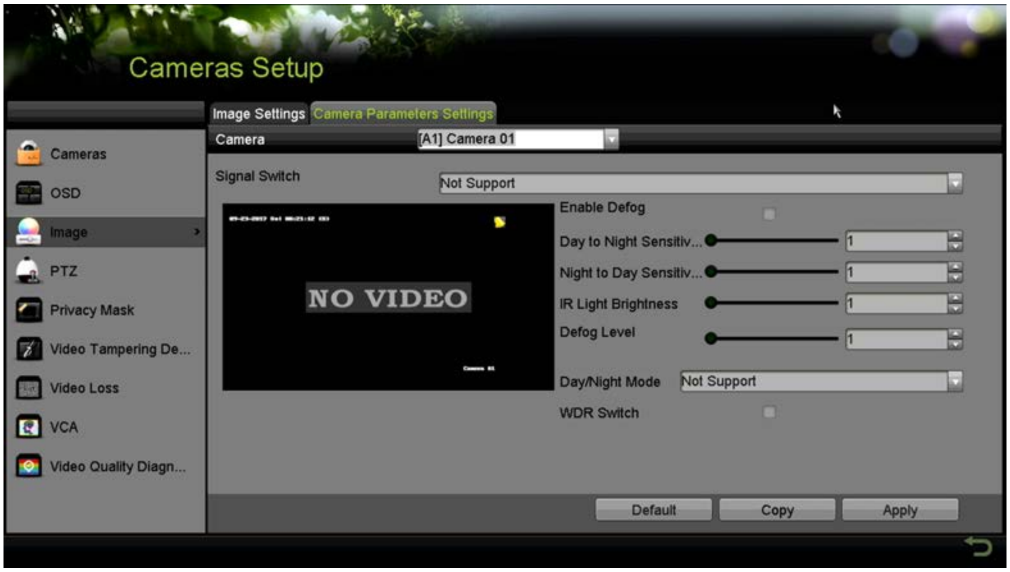
5. Adjust the image parameters according to actual needs. The parameters include Brightness, Contrast, Saturation, Hue, Sharpness, and Denoising for analog cameras and Brightness, Contrast, and Saturation for IP cameras. You can click **Restore** to set the parameters to the default settings.

6. Click **Copy** to copy the image settings of the current camera to other cameras.

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

15.3.2 Configuring Camera Parameters Settings

1. Go to Menu > Camera > Image > Camera Parameters Settings.



Camera: [A1] Camera 01

Signal Switch: Not Support

Enable Defog □

Day to Night Sensitiv... 1

Night to Day Sensitiv... 1

IR Light Brightness 1

Defog Level 1

Day/Night Mode: Not Support

WDR Switch □

Figure 269, Camera Parameters Settings

2. Select the **Camera** from the drop-down list.

3. Configure the parameters.

   1) Switch the 4 MP or 5 MP signal from 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.

   2) Check **Enable Defog** to enable the defog function of the selected camera, and set the **Defog Level** from 1 to 4.

   3) Adjust the parameters including Day to Night Sensitivity, Night to Day Sensitivity, and IR Light Brightness for the analog cameras.

   4) Select the **Day/Night Mode** of the camera from the drop-down list.

   5) Check the **WDR Switch** checkbox to enable the function of the camera.

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 values range from 1 to 9.

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

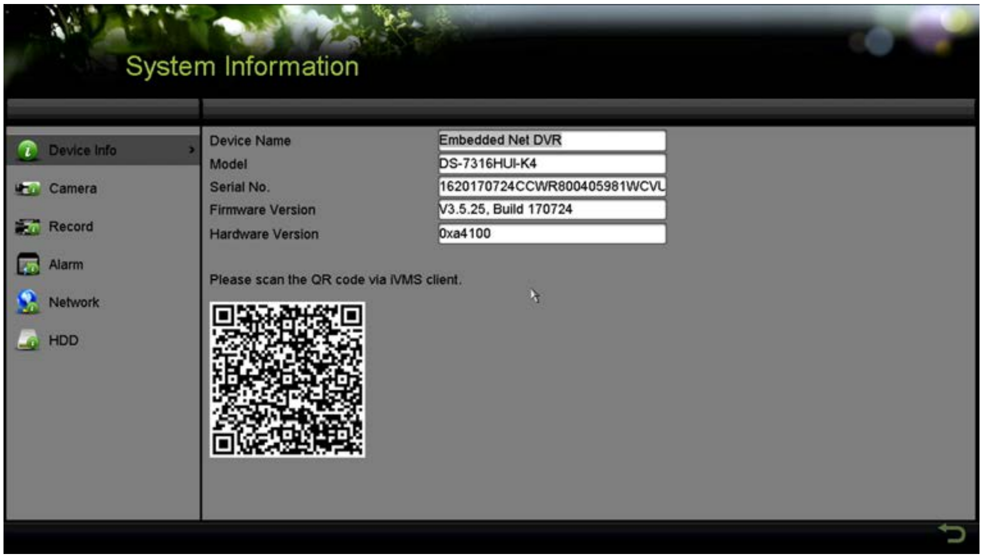
The DVR connects to the analog camera via Hikvision-C protocol and there is no response mechanism. Even if the Hikvision-C protocol is abnormal, the parameters are still displayed to be set successfully.

16 DVR Management and Maintenance

16.1 Viewing System Information

1. Go to Menu > Maintenance > System Info.

2. Click the **Device Info**, **Camera**, **Record**, **Alarm**, **Network,** and **HDD** tabs to view the system information of the device.



Device Name: Embedded Net DVR
Model: DS-7316HUI-K4
Serial No.: 1620170724CCWR800405981WCVU
Firmware Version: V3.5.25, Build 170724
Hardware Version: 0xa4100

Please scan the QR code via iVMS client.

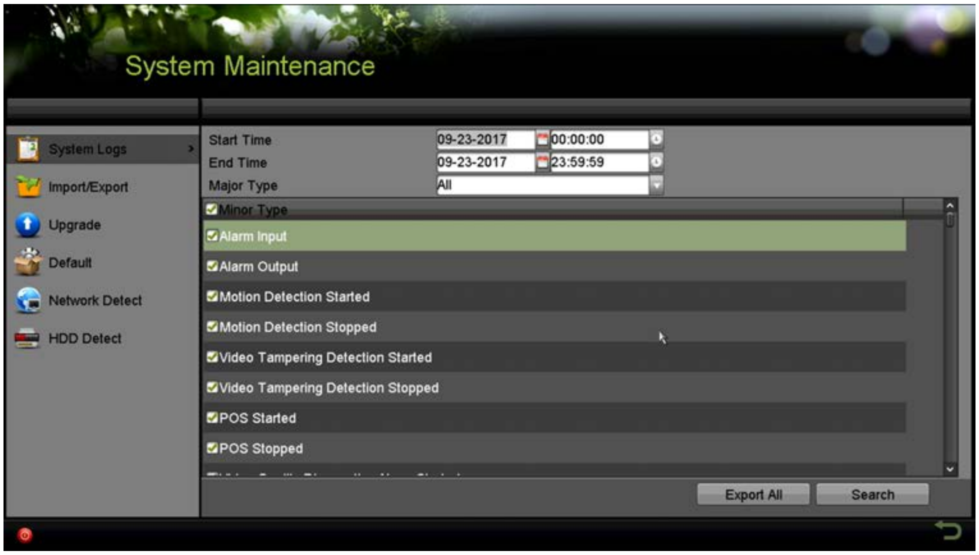
Figure 270, System Information Interface

16.2 Searching Log Files

Purpose

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

1. Go to Menu > Maintenance > Log Information.



Start Time 09-23-2017 00:00:00
End Time 09-23-2017 23:59:59
Major Type All

☑ Minor Type
☑ Alarm Input
☑ Alarm Output
☑ Motion Detection Started
☑ Motion Detection Stopped
☑ Video Tampering Detection Started
☑ Video Tampering Detection Stopped
☑ POS Started
☑ POS Stopped

Figure 271, Log Search Interface

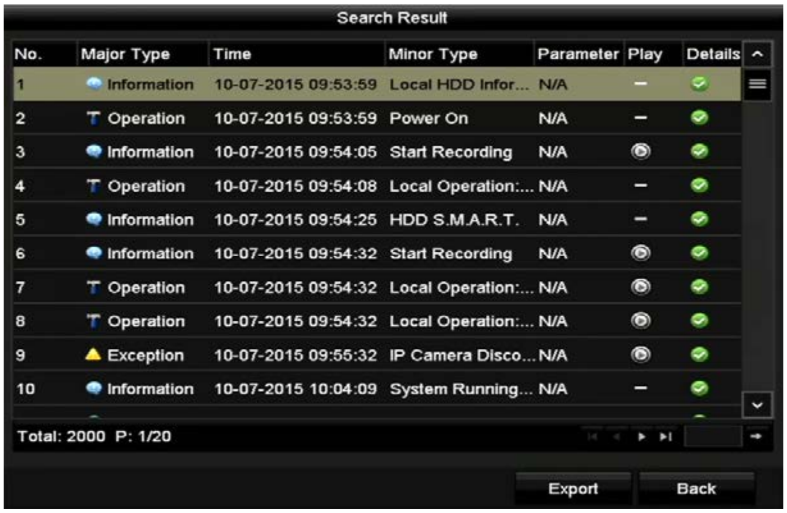
2. Set the log search conditions to refine your search, including the Start Time, End Time, Major Type, and Minor Type.

3. Click **Search** to start searching the log files.

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

NOTE

Up to 2000 log files can be displayed each time.



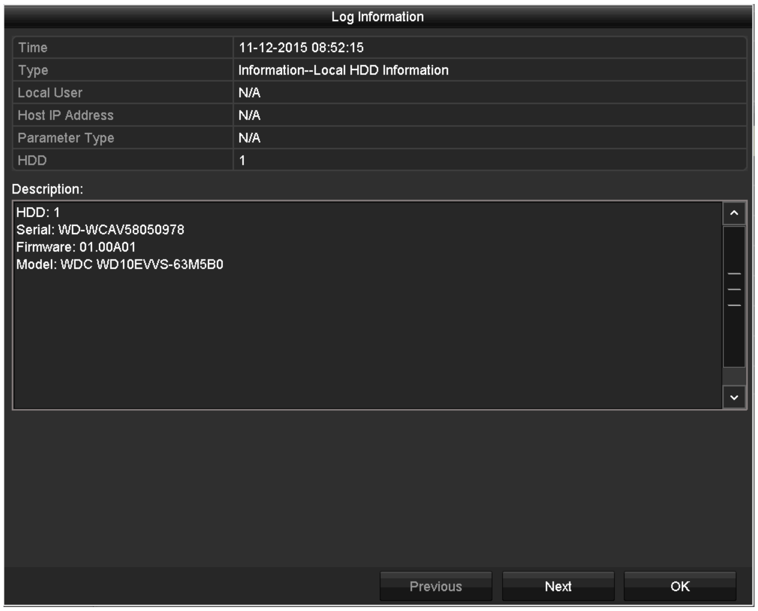
Search Result

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

Total: 2000 P: 1/20

Figure 272, Log Search Results

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



Log Information

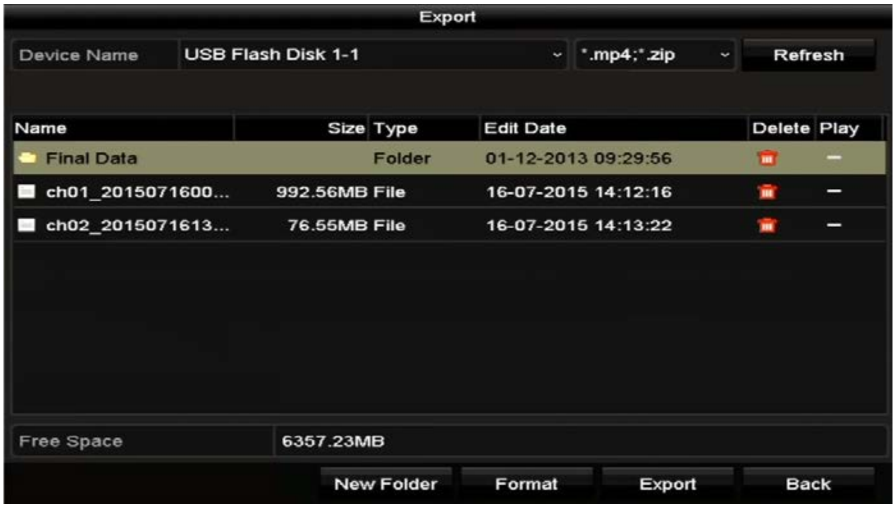
Time	11-12-2015 08:52:15
Type	Information--Local HDD Information
Local User	N/A
Host IP Address	N/A
Parameter Type	N/A
HDD	1

Description:

HDD: 1
Serial: WD-WCAV58050978
Firmware: 01.00A01
Model: WDC WD10EVVS-63M5B0

Figure 273, Log Information Interface

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



Export

Device Name: USB Flash Disk 1-1 | *.mp4;*.zip

Name	Size	Type	Edit Date	Delete	Play
Final Data		Folder	01-12-2013 09:29:56		–
ch01_2015071600...	992.56MB	File	16-07-2015 14:12:16		–
ch02_2015071613...	76.55MB	File	16-07-2015 14:13:22		–

Free Space: 6357.23MB

Figure 274, 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. You can 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 export time, e.g., *20110514124841logBack.txt*.

16.3 Importing/Exporting IP Camera Info

Purpose

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

1. Go to Menu > Camera > Camera > IP Camera Import/Export.

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

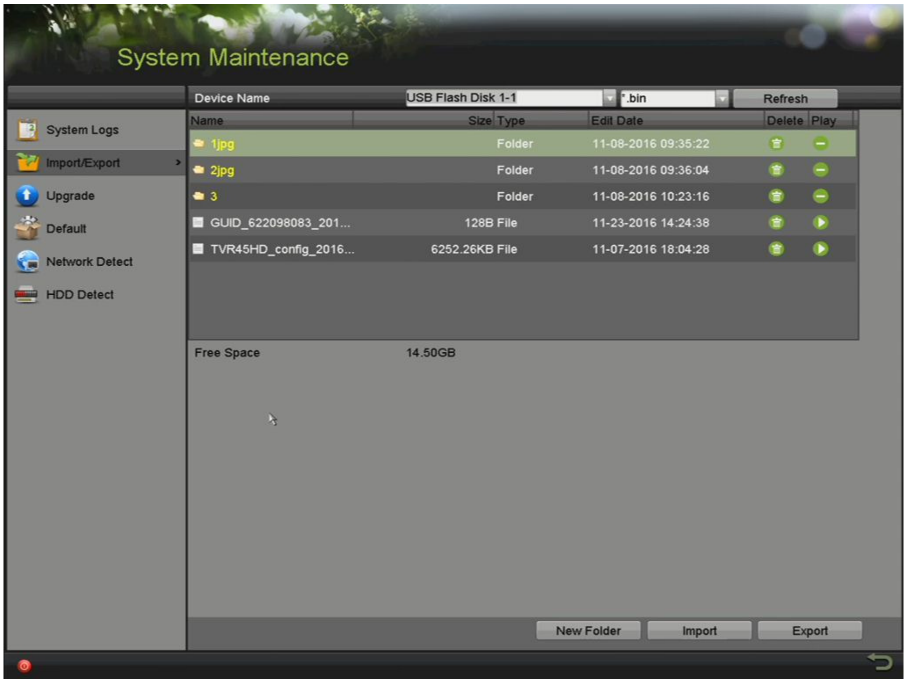
3. To import a configuration file, select the file from the selected backup device and click **Import**. After the importing process is completed, you must reboot the DVR.

16.4 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 DVR devices if they are to be configured with the same parameters.

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



System Maintenance

Device Name: USB Flash Disk 1-1 | *.bin

Name	Size	Type	Edit Date	Delete	Play
1jpg		Folder	11-08-2016 09:35:22		
2jpg		Folder	11-08-2016 09:36:04		
3		Folder	11-08-2016 10:23:16		
GUID_622098083_201...	128B	File	11-23-2016 14:24:38		
TVR45HD_config_2016...	6252.26KB	File	11-07-2016 18:04:28		

Free Space: 14.50GB

Figure 275, 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 completed, you must reboot the DVR.

NOTE

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

16.5 Upgrading System

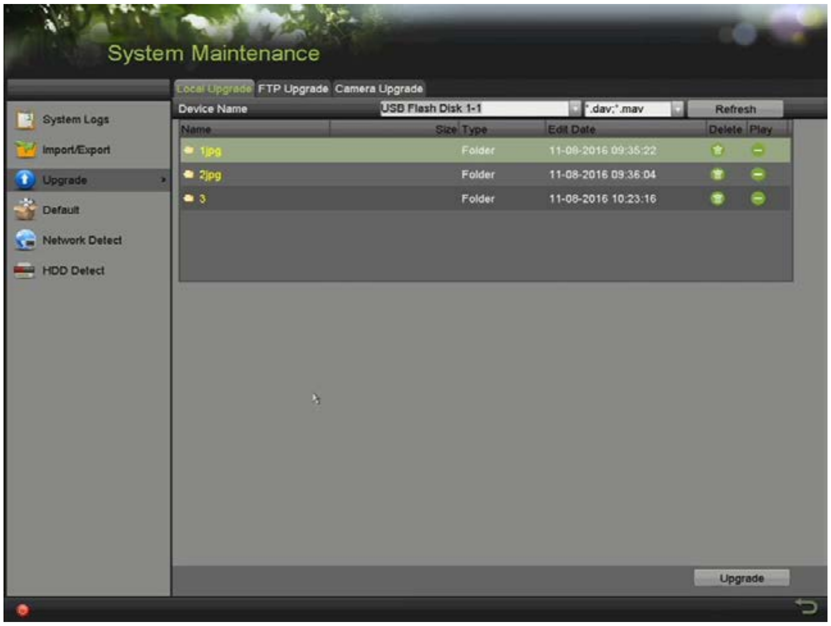
Purpose

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

16.5.1 Upgrading by Local Backup Device

1. Connect your DVR to a local backup device with the updated firmware file.

2. Go to Menu > Maintenance > Upgrade > Local Upgrade.



Device Name: USB Flash Disk 1-1 | *.dav;*.mav

Name	Size	Type	Edit Date	Delete	Play
1jpg		Folder	11-08-2016 09:35:22		
2jpg		Folder	11-08-2016 09:36:04		
3		Folder	11-08-2016 10:23:16		

Figure 276, Local Upgrade Interface

3. Select the update file from the backup device.

4. Click **Upgrade** to start upgrading.

5. After upgrading is done, reboot the DVR to activate the new firmware.

16.5.2 Upgrading by FTP

Before You Start

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

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

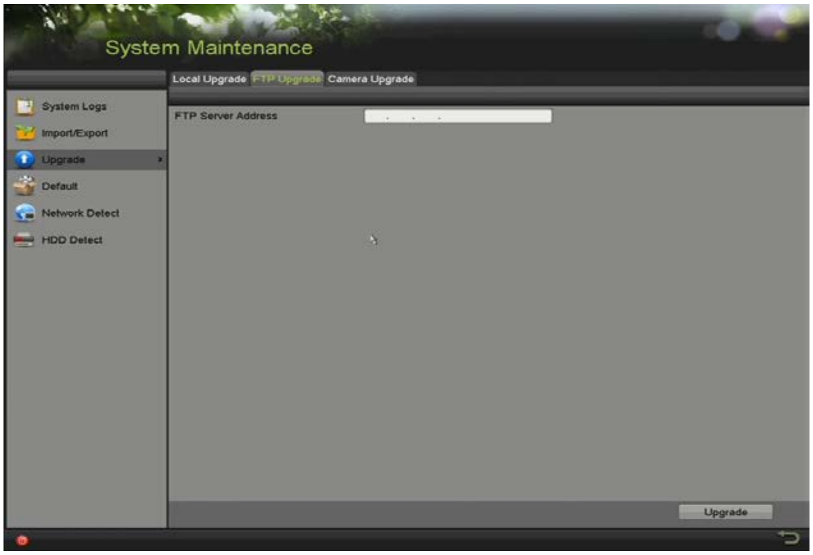


Figure 277, FTP Upgrade Interface

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.

16.6 Upgrading Camera

Purpose

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

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

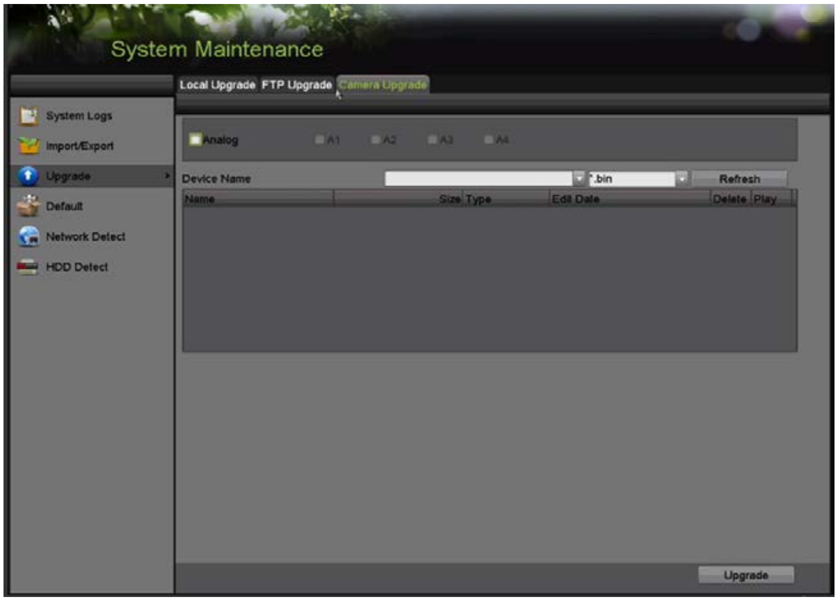


Figure 278, Camera Upgrade

2. Check the checkbox(es) of the analog camera(s) for upgrading.

NOTE

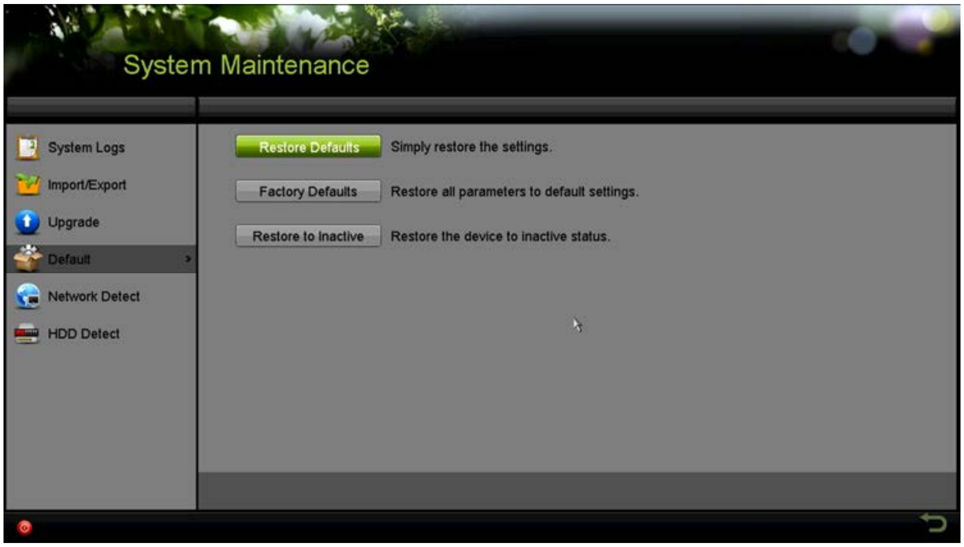
The analog camera must support TurboHD signal.

3. Select the update file from the backup device.

4. Click **Upgrade** to start upgrading.

16.7 Restoring Default Settings

1. Go to Menu > Maintenance > Default.



Restore Defaults Simply restore the settings.

Factory Defaults Restore all parameters to default settings.

Restore to Inactive Restore the device to inactive status.

Figure 279, Restore Defaults

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

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

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

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

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

NOTE

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

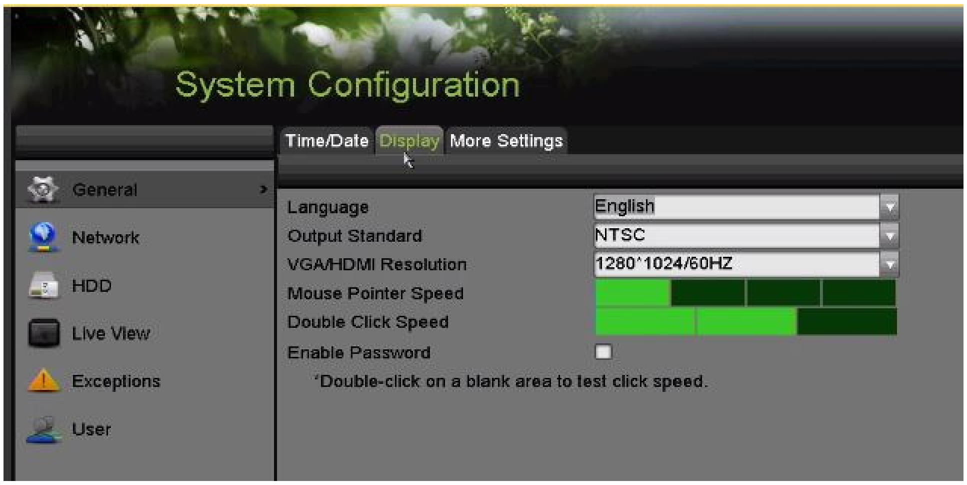
17 Other

17.1 Configuring General Settings

Purpose

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

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



Language: English

Output Standard: NTSC

VGA/HDMI Resolution: 1280*1024/60HZ

Mouse Pointer Speed: 🟩■■■

Double Click Speed: 🟩🟩■

Enable Password: □

*Double-click on a blank area to test click speed.

Figure 280, General Settings Interface

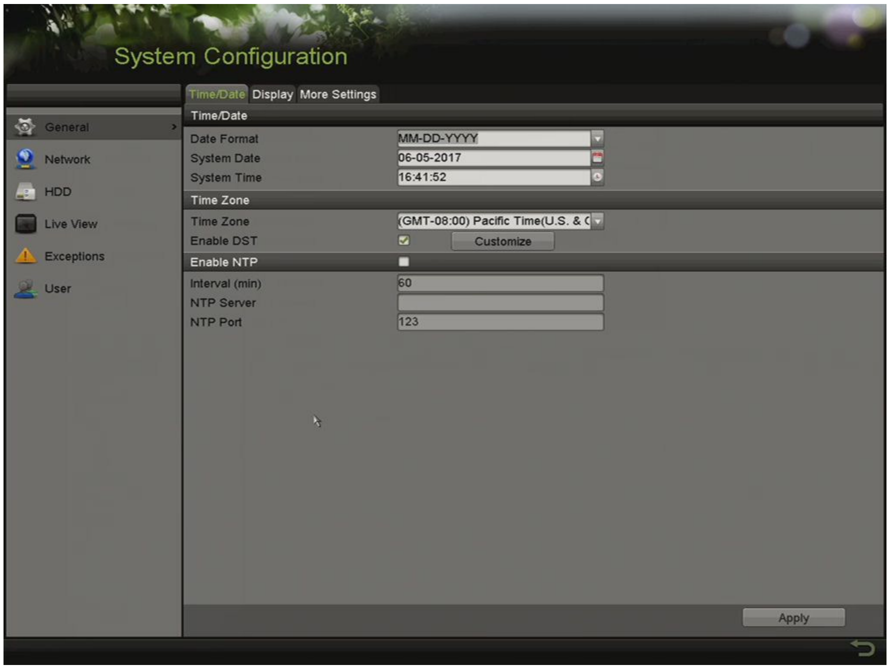
2. Configure the following settings:

- **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.

NOTE

VGA/HDMI1 Resolution and **HDMI2 Resolution** can be configured separately. Up to 1920 × 1080/60 Hz resolution is supported for VGA/HDMI1 output and up to 4K (3840 × 2160)/30 Hz resolution is supported for HDMI2 output.

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



Time/Date

Date Format: MM-DD-YYYY

System Date: 06-05-2017

System Time: 16:41:52

Time Zone

Time Zone: (GMT-08:00) Pacific Time(U.S. & C

Enable DST: ☑

Enable NTP: □

Interval (min): 60

NTP Server:

NTP Port: 123

Figure 281, Time/Date Setting

NOTE

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

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

17.2 Configuring RS-232 Serial Port

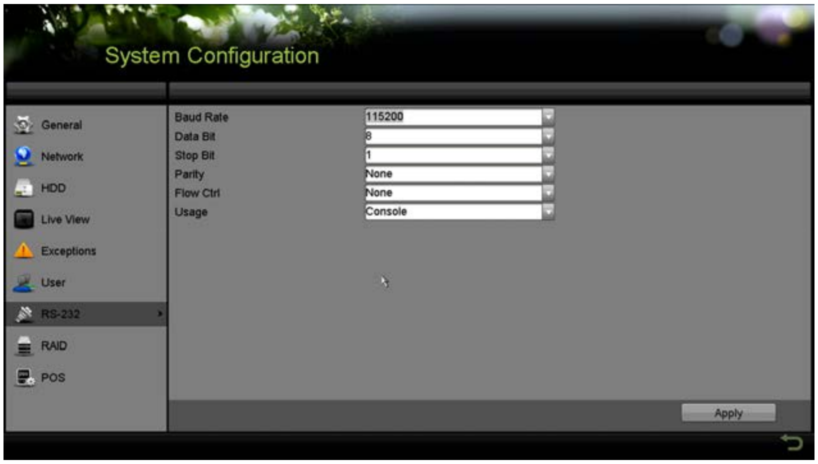
Purpose

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

- **Parameters Configuration:** Connect a PC to the DVR through the PC serial port. Device parameters can be configured by using software such as HyperTerminal. The serial port parameters must be the same as the DVR's when connecting with the PC serial port.

- **Transparent Channel:** Connect a serial device directly to the DVR. It will be controlled remotely by the PC through the network and the protocol of the serial device.

1. Go to Menu > System Configuration > RS-232.



Baud Rate: 115200
Data Bit: 8
Stop Bit: 1
Parity: None
Flow Ctrl: None
Usage: Console

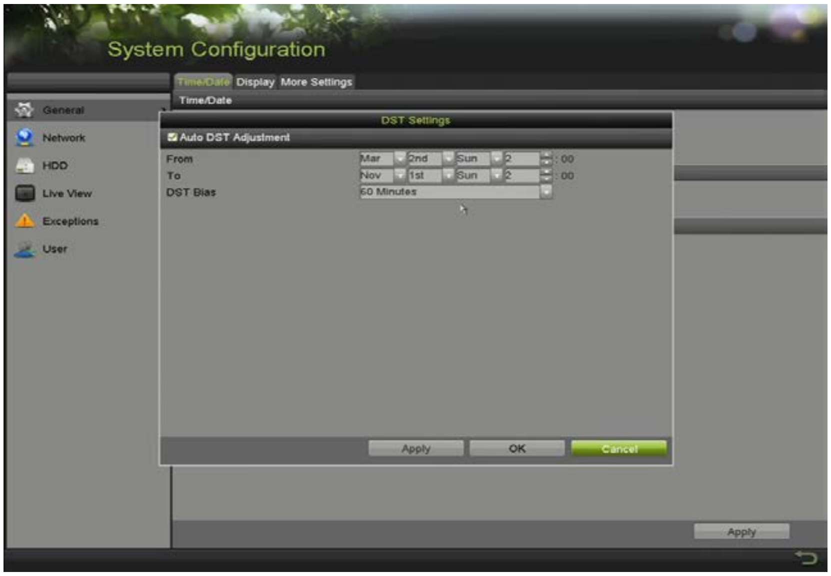
Figure 282, RS-232 Settings Interface

2. Configure RS-232 parameters (baud rate, data bit, stop bit, parity, flow control, usage).

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

17.3 Configuring DST Settings

1. Go to Menu > System Configuration > General > DST Settings.



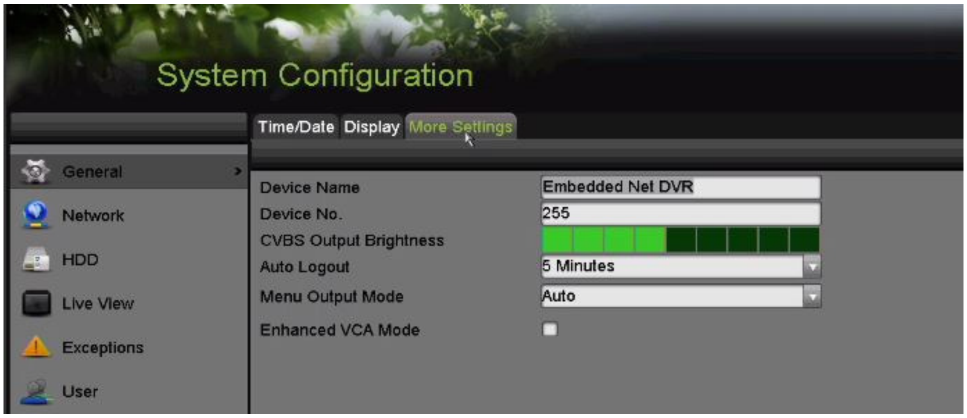
☑ Auto DST Adjustment
From: Mar 2nd Sun 2 : 00
To: Nov 1st Sun 2 : 00
DST Bias: 60 Minutes

Figure 283, DST Settings Interface

2. Check the checkbox before the **Auto DST Adjustment** item, or manually check the **Enable DST** checkbox and choose the date of the DST period.

17.4 Configuring More Settings

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



Device Name: Embedded Net DVR
Device No.: 255
CVBS Output Brightness
Auto Logout: 5 Minutes
Menu Output Mode: Auto
Enhanced VCA Mode: □

Figure 284, More Settings Interface

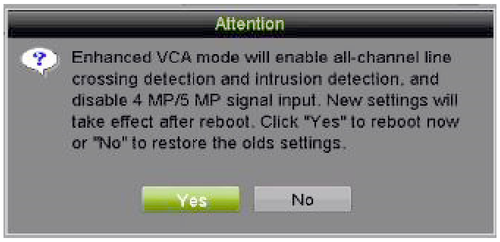
2. Configure the following settings:

   - **Device Name:** Edit the name of the DVR.
   - **Device No.:** Edit the DVR serial number. The Device No. can be set in the range of 1 to 255, and the default No. is 255.
   - **Auto Logout:** Set timeout time for menu inactivity. E.g., when the timeout time is set to *5 Minutes*, the system will exit from the current operation menu to live view screen after 5 minutes of menu inactivity.
   - **CVBS Output Brightness:** Adjust the video output brightness via the CVBS interface.
   - **Menu Output Mode:** You can choose the menu display on different video output. **Auto**, **HDMI1/VGA**, and **HDMI2** are selectable.
   - **Enhanced VCA Mode:** The enhanced VCA mode conflicts with the 2K/4K output and 4 MP/5 MP signal input. You can enable or disable VCA mode.

     Enable Enhanced VCA Mode

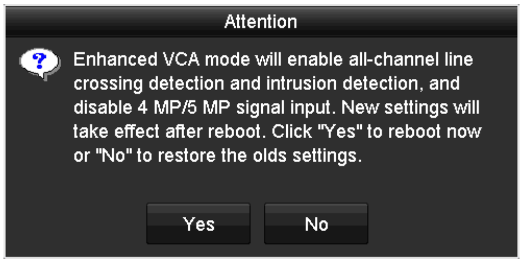
     1) Check the checkbox to enable enhanced VCA mode.

     2) Click **Apply** and the attention box pops up as below.



Enhanced VCA mode will enable all-channel line crossing detection and intrusion detection, and disable 4 MP/5 MP signal input. New settings will take effect after reboot. Click "Yes" to reboot now or "No" to restore the olds settings.

Figure 285, Enable Enhanced VCA Mode (1)



Attention

Enhanced VCA mode will enable all-channel line crossing detection and intrusion detection, and disable 4 MP/5 MP signal input. New settings will take effect after reboot. Click "Yes" to reboot now or "No" to restore the olds settings.

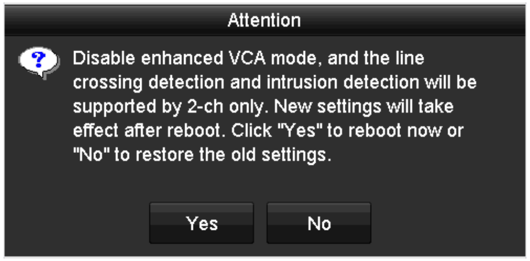
Figure 286, Enable Enhanced VCA Mode (2)

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

Disable Enhanced VCA Mode

1) Uncheck the checkbox to disable enhanced VCA mode.

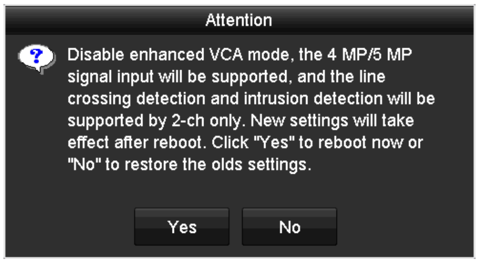
2) Click **Apply** and the attention box pops up as below.



Attention

Disable enhanced VCA mode, and the line crossing detection and intrusion detection will be supported by 2-ch only. New settings will take effect after reboot. Click "Yes" to reboot now or "No" to restore the old settings.

Figure 287, Disable Enhanced VCA Mode (1)



Attention

Disable enhanced VCA mode, the 4 MP/5 MP signal input will be supported, and the line crossing detection and intrusion detection will be supported by 2-ch only. New settings will take effect after reboot. Click "Yes" to reboot now or "No" to restore the olds settings.

Figure 288, Disable Enhanced VCA Mode (2)

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

NOTE

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

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

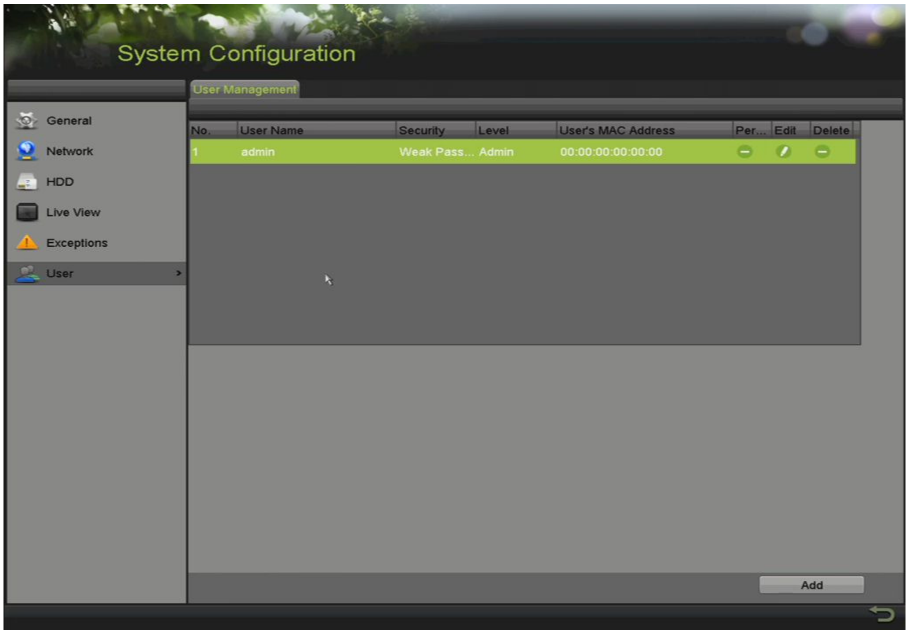
17.5 Managing User Accounts

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.

17.5.1 Adding a User

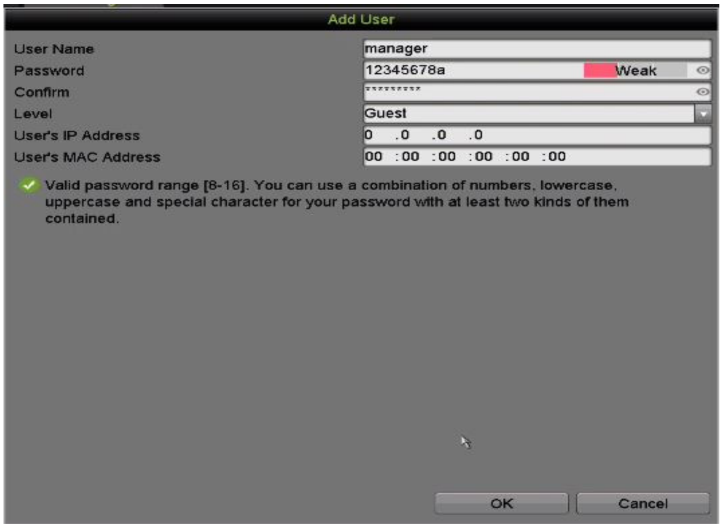
1. Go to Menu > System Configuration > User.



No.	User Name	Security	Level	User's MAC Address	Per...	Edit	Delete
1	admin	Weak Pass...	Admin	00:00:00:00:00:00	⊖	✎	⊖

Figure 289, User Management Interface

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



User Name	manager
Password	12345678a Weak
Confirm	*********
Level	Guest
User's IP Address	0 .0 .0 .0
User's MAC Address	00 :00 :00 :00 :00 :00

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

Figure 290, Add User Menu

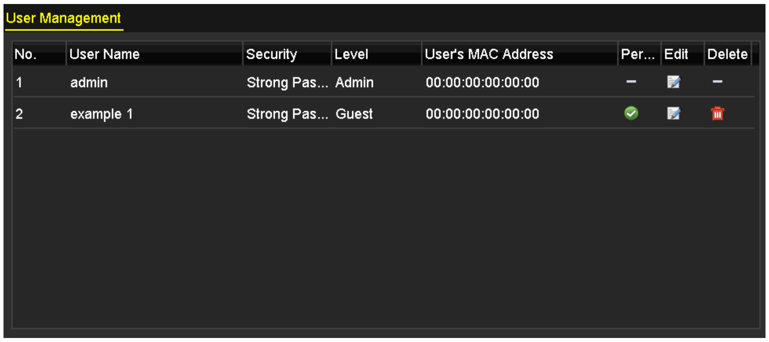
3. Enter information for the new user, including **User Name**, **Password**, **Confirm**, **Level,** and **User's MAC Address**.

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

WARNING

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

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



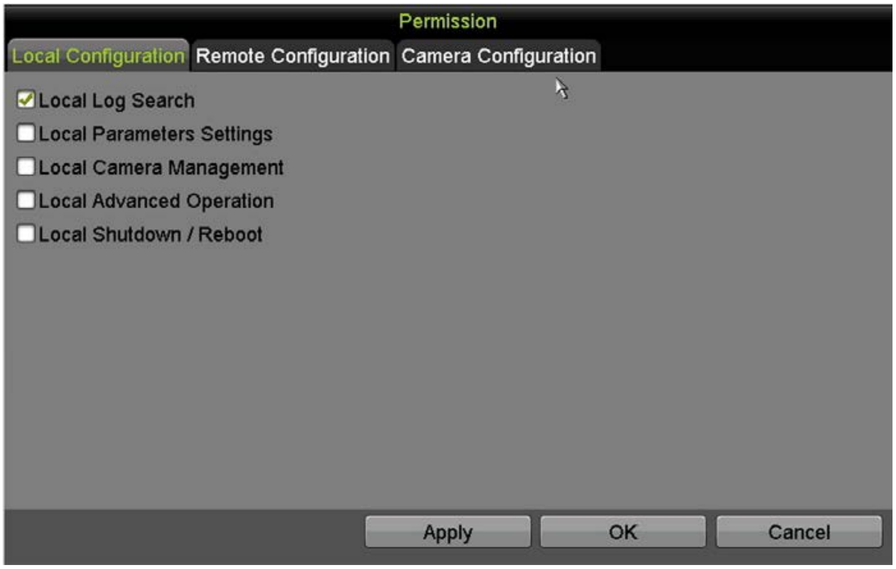
User Management

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

Figure 291, Added User Listed in User Management Interface

- 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.



☑ Local Log Search
□ Local Parameters Settings
□ Local Camera Management
□ Local Advanced Operation
□ Local Shutdown / Reboot

Figure 292, 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 system information of device
- **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 of 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)

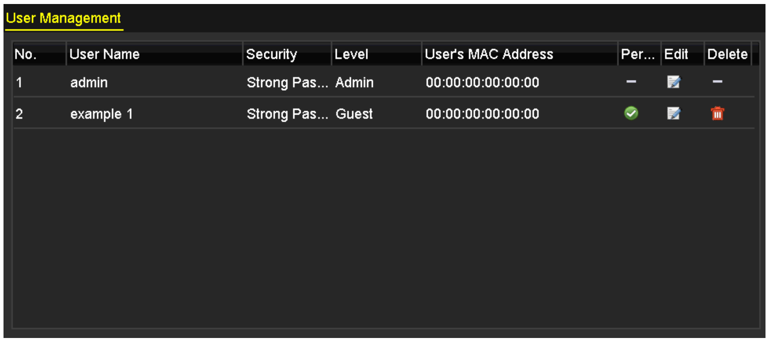
NOTE

Local Camera Management is provided for IP cameras only.

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

17.5.2 Deleting a User

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



User Management

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

Figure 293, User List

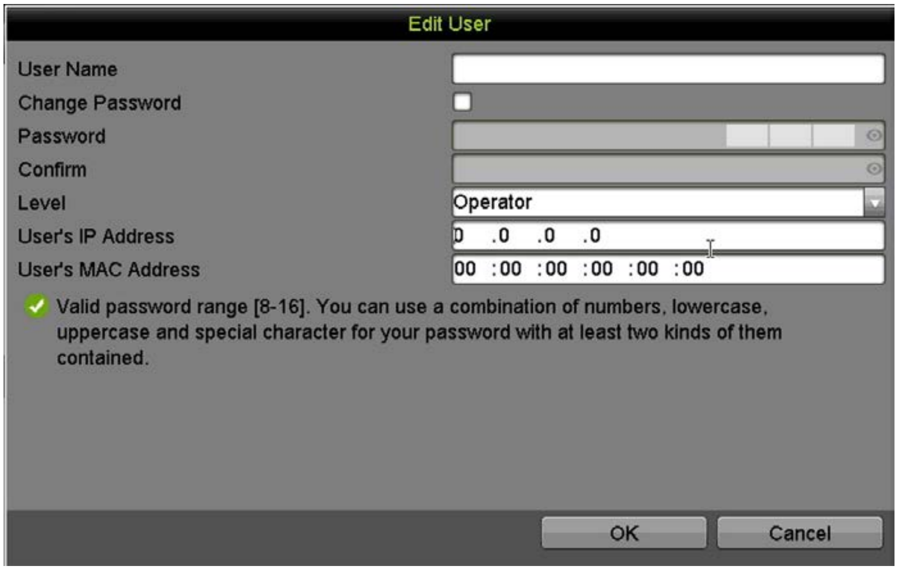
3. Click 🗑 to delete the selected user account.

17.5.3 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 ✎ to enter the **Edit User** interface, as shown below.



Edit User

User Name

Change Password □

Password

Confirm

Level: Operator

User's IP Address: 0 .0 .0 .0

User's MAC Address: 00 :00 :00 :00 :00 :00

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

Figure 294, Edit User Interface

4. Edit the corresponding parameters.

- **Operator and Guest**

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

- **Admin**

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

WARNING

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

NOTE

Hold down the ◉ icon to see the clear text of the password. Release the mouse and the content of the password again becomes invisible.

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

   1) Check the **Enable Unlock Pattern** checkbox to enable the use of the unlock pattern when logging in to the device.

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

   3) Confirm the pattern again with the mouse.

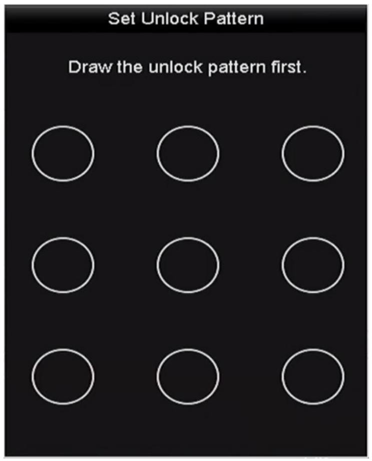
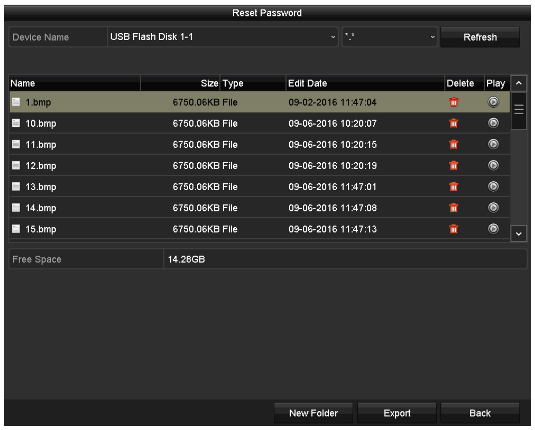


Figure 295, Set Unlock Patter for Admin User

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

7. (Optional) Click ⚙ after **Export GUID** to display the Reset Password interface. Click **Export** to export the GUID to the USB flash drive to retrieve a forgotten password. A GUID file will be saved.



Reset Password

Device Name: USB Flash Disk 1-1 · *.*

Name	Size	Type	Edit Date	Delete	Play
1.bmp	6750.06KB	File	09-02-2016 11:47:04	🗑	▶
10.bmp	6750.06KB	File	09-06-2016 10:20:07	🗑	▶
11.bmp	6750.06KB	File	09-06-2016 10:20:15	🗑	▶
12.bmp	6750.06KB	File	09-06-2016 10:20:19	🗑	▶
13.bmp	6750.06KB	File	09-06-2016 11:47:01	🗑	▶
14.bmp	6750.06KB	File	09-06-2016 11:47:08	🗑	▶
15.bmp	6750.06KB	File	09-06-2016 11:47:13	🗑	▶

Free Space: 14.28GB

Figure 296, Export GUID

NOTE

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, you can also click ✓ on the **User Management** interface to edit the permission.

18 Appendix

18.1 Specifications

18.1.1 DS-73xxHUI-K4

Model		DS-7304HUI-K4	DS-7308HUI-K4	DS-7316HUI-K4
Video/Audio Input	Video Compression	H.265+/H.265/H.264+/H.264		
	Analog Video Input	4-ch	8-ch	16-ch
		BNC interface (1.0 Vp-p, 75 Ω), supporting Hikvision-C connection		
	HDTVI Input	5 MP, 4 MP, 3 MP, 1080p25, 1080p30, 720p25, 720p30, 720p50, 720p60		
	CVBS Input	Supported		
	IP Video Input	2-ch (up to 6-ch)	2-ch (up to 10-ch)	2-ch (up to 18-ch)
		Up to 8 MP resolution		
		Supports H.265+/H.265/H.264+/H.264 IP cameras		
	Network Bandwidth	200 Mbps		260 Mbps
	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		
	HDMI1/VGA Output	1-ch, 1920 × 1080/60 Hz, 1280 × 1024/60 Hz, 1280 × 720/60 Hz, 1024 × 768/60 Hz		
	HDMI2 Output	1-ch, 4K (3840 × 2160)/30 Hz, 2K (2560 × 1440)/60 Hz, 1920 × 1080/60 Hz, 1280 × 1024/60 Hz, 1280 × 720/60 Hz, 1024 × 768/60 Hz		
	Encoding Resolution	5 MP/4 MP/3 MP/1080p/720p/WD1/4CIF/VGA/CIF		
	Frame Rate	Main stream: 5 MP @ 12 fps; 4 MP @ 15 fps; 3 MP @ 18 fps; 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 10 Mbps		
	Audio Output	2-ch, RCA (Linear, 1 KΩ)		
	Audio Bit Rate	64 Kbps		
	Dual Stream	Supported		
	Stream Type	Video, Video & Audio		
	Synchronous Playback	4-ch	8-ch	16-ch
Network Management	Remote Connections	128		
	Network Protocols	TCP/IP, PPPoE, DHCP, Hik-Connect, DNS, DDNS, NTP, SADP, NFS, iSCSI, UPnP™, HTTPS, ONVIF, SNMP		
Hard Disk	SATA	4 SATA interfaces		
	eSATA	Supported		
	Capacity	Up to 8 TB capacity for each disk		
Disk Array	Array type	RAID 0, RAID 1, RAID 5, RAID 6, RAID 10		
External Interface	Two-way Audio Input	1-ch, RCA (2.0 Vp-p, 1 KΩ) (independent)		
	Network Interface	2, RJ-45 10M/100M/1000M self-adaptive Ethernet interface		
	USB Interface	Front panel: 2 × USB 2.0 Rear panel: 1 × USB 3.0		
	Serial Interface	RS-232, RS-485 (full-duplex), keyboard		
	Alarm In/Out	16/4		
General	Power Supply	100 to 240 VAC		
	Consumption (w/o HDD)	≤35 W	≤45 W	≤65 W
	Working Temperature	-10° to +55° C (+14° to +131° F)		
	Working Humidity	10% to 90%		
	Dimensions (W × D × H)	445 × 390 × 70 mm (17.5 × 15.4 × 2.8 inch)		
	Weight (w/o HDD)	≤ 5 kg (11.0 lb)		

18.1.2 DS-90xxHUI-K8

Model		DS-9008HUI-K8	DS-9016HUI-K8
Video/Audio Input	Video Compression	H.265+/H.265/H.264+/H.264	
	Analog Video Input	8-ch	16-ch
		BNC interface (1.0 Vp-p, 75 Ω), supporting Hikvision-C connection	
	HDTVI Input	5 MP, 4 MP, 3 MP, 1080p25, 1080p30, 720p25, 720p30, 720p50, 720p60	
	CVBS Input	Supported	
	IP Video Input	10-ch (up to 18-ch)	18-ch (up to 32-ch)
		Up to 12 MP resolution	
		Supports H.265+/H.265/H.264+/H.264 IP cameras	
	Network Bandwidth	260 Mbps	320 Mbps
	Audio Compression	G.711u	
	Audio Input	8-ch	16-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	
	HDMI1/VGA Output	1-ch, 1920 × 1080/60 Hz, 1280 × 1024/60 Hz, 1280 × 720/60 Hz, 1024 × 768/60 Hz	
	HDMI2 Output	1-ch, 4K (3840 × 2160)/30 Hz, 2K (2560 × 1440)/60 Hz, 1920 × 1080/60 Hz, 1280 × 1024/60 Hz, 1280 × 720/60 Hz, 1024 × 768/60 Hz	
	Video Loop	Supported	
	Encoding Resolution	5 MP/4 MP/3 MP/1080p/720p/WD1/4CIF/VGA/CIF	
	Frame Rate	Main stream: 5 MP @ 12 fps; 4 MP @ 15 fps; 3 MP @ 18 fps; 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 10 Mbps	
	Audio Output	2-ch, RCA (Linear, 1 KΩ)	
	Audio Bit Rate	64 Kbps	
	Dual Stream	Support	
	Stream Type	Video, Video & Audio	
	Synchronous Playback	8-ch	16-ch
Network Management	Remote Connections	128	
	Network Protocols	TCP/IP, PPPoE, DHCP, Hik-Connect, DNS, DDNS, NTP, SADP, NFS, iSCSI, UPnP™, HTTPS, ONVIF, SNMP	
Hard Disk	SATA	8 SATA interfaces	
	eSATA	Supported	
	Capacity	Up to 8 TB capacity for each disk.	
Disk Array	Array Type	RAID 0, RAID 1, RAID 5, RAID 6, RAID 10	
External Interface	Two-Way Audio Input	1-ch, RCA (2.0 Vp-p, 1 KΩ) (independent)	
	Network Interface	2, RJ-45 10M/100M/1000M self-adaptive Ethernet interface	
	USB Interface	Front panel: 2 × USB 2.0 Rear panel: 1 × USB 3.0	
	Serial Interface	RS-232, RS-485 (full-duplex), keyboard	
	Alarm In/Out	16/8	
General	Power Supply	100 to 240 VAC	
	Consumption (w/o HDD)	≤45 W	≤65 W
	Working Temperature	-10° to +55° C (+14° to +131° F)	
	Working Humidity	10% to 90%	
	Dimensions (W × D × H)	445 × 470 × 90 mm (17.5 × 18.5 × 3.5 inch)	
	Weight (w/o HDD)	≤ 8 kg (17.6 lb)	

18.1.3 DS-73xxHQI-K4

Model		DS-7304HQI-K4	DS-7308HQI-K4	DS-7316HQI-K4
Video/Audio Input	Video Compression	H.265+/H.265/H.264+/H.264		
	Analog Video Input	4-ch	8-ch	16-ch
		BNC interface (1.0 Vp-p, 75 Ω), supporting Hikvision-C connection		
	HDTVI Input	3 MP, 1080p25, 1080p30, 720p25, 720p30, 720p50, 720p60 Note: The 3 MP signal input is available only for channel 1 of DS-7304HQI-K4, channel 1/2 of DS-7308HQI-K4, and channel 1/2/3/4 of DS-7316HQI-K4.		
	CVBS Input	PAL/NTSC		
	IP Video Input	2-ch (up to 6-ch)	2-ch (up to 10-ch)	2-ch (up to 18-ch)
		Up to 4 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	HDMI: 1-ch, 4K (3840 × 2160)/30 Hz, 2K (2560 × 1440)/60 Hz, 1920 × 1080/60 Hz, 1280 × 1024/60 Hz, 1280 × 720/60 Hz, 1024 × 768/60 Hz		
		VGA: 1-ch, 1920 × 1080/60 Hz, 1280 × 1024/60 Hz, 1280 × 720/60 Hz, 1024 × 768/60 Hz		
	Encoding Resolution	When 1080p Lite mode not enabled: 3 MP/1080p/720p/VGA/WD1/4CIF/CIF When 1080p Lite mode enabled: 3 MP/1080p lite/720p lite/VGA/WD1/4CIF/CIF		
	Frame Rate	Main stream: When 1080p Lite mode not enabled: For 3 MP stream access: 3 MP/1080p/720p/VGA/WD1/4CIF/CIF @ 15 fps For 1080p stream access: 1080p/720p @ 15 fps; VGA/WD1/4CIF/CIF @ 25 fps (P)/30 fps (N) For 720p stream access: 720p/VGA/WD1/4CIF/CIF @ 25 fps (P)/30 fps (N) When 1080p Lite mode enabled: 3 MP @ 15 fps 1080p lite/720p lite/VGA/WD1/4CIF/CIF @ 25fps (P)/30 fps (N)		
		Sub-stream: WD1/4CIF @ 12 fps; CIF @ 25 fps (P)/30 fps (N)		
	Video Bit Rate	32 Kbps to 6 Mbps		
	Audio Output	2-ch, RCA (linear, 1 KΩ)		
	Audio Bit Rate	64 Kbps		
	Dual Stream	Supported		
	Stream Type	Video, Video & Audio		
	Synchronous Playback	4-ch	8-ch	16-ch
Network Management	Remote Connections	128		
	Network Protocols	TCP/IP, PPPoE, DHCP, Hik-Connect, DNS, DDNS, NTP, SADP, NFS, iSCSI, UPnP™, HTTPS, ONVIF		
Hard Disk	SATA	4 SATA interfaces		
	eSATA	Supported		
	Capacity	Up to 8 TB capacity for each disk		
External Interface	Two-Way Audio Input	1-ch, RCA (2.0 Vp-p, 1 KΩ) (independent)		
	Network Interface	1, RJ-45 10M/100M/1000M self-adaptive Ethernet interface		
	USB Interface	Front panel: 2 × USB 2.0 Rear panel: 1 × USB 3.0		
	Serial Interface	RS-232, RS-485 (full-duplex), keyboard		
	Alarm In/Out	16/4		
General	Power Supply	100 to 240 VAC		
	Consumption (w/o HDD)	≤30 W	≤40 W	≤55 W
	Working Temperature	-10 to +55° C (+14 to +131° F)		
	Working Humidity	10% to 90%		
	Dimensions (W × D × H)	445 mm × 390 mm × 70 mm (17.5" × 15.4" × 2.8")		
	Weight (w/o HDD)	≤5 kg (11.0 lb)		

18.2 Glossary

- **Dual-Stream:** 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:** 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:** Hard Disk Drive. A storage medium which stores digitally encoded data on platters with magnetic surfaces.

- **DHCP:** Dynamic Host Configuration Protocol is a network application protocol used by devices (DHCP clients) to obtain configuration information for operation in an Internet Protocol network.

- **HTTP:** Hypertext Transfer Protocol. A protocol to transfer hypertext request and information between servers and browsers over a network

- **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 combination of a DVR and NVR.

- **NTP:** Network Time Protocol. A protocol designed to synchronize the clocks of computers over a network.

- **NTSC:** 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:** 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:** 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:** 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:** Universal Serial Bus. USB is a plug-and-play serial bus standard to interface devices to a host computer.

18.3 Troubleshooting

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

  Possible Reasons:

  — No VGA or HDMI connection

  — 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, connect the device with the monitor and reboot.

  Step 2 Verify the connection cable is good.

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

  Step 3 Verify the monitor input mode is correct.

  Check that the monitor input mode matches the output mode of the device (e.g., if the output mode of the DVR is HDMI, then the monitor input mode must be HDMI). If not, modify the monitor input mode.

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

  If it is solved, finish the process.

  If not, contact an engineer from our company to do further analysis.

- **There is a beep after a new device starts up.**

  Possible Reasons:

  — No HDD is installed in the device.

  — The installed HDD has not been initialized.

  — The installed HDD is not compatible with the device or is broken.

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

  1) If not, install a 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 > Configuration > Exceptions,” and uncheck the “HDD Error” Audible Warning checkbox.

  Step 2 Verify the HDD is initialized.

  1) Select “Menu > System Configuration > HDD > General.”

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

Step 3 Verify the HDD is detected and 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 step 1 to step 3.

1) If it is solved, finish the process.

2) If not, contact an engineer from our company for further analysis.

- **Live view becomes 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).

Step 2 Select "Menu > Record > Parameters > Record," and set the resolution of Main Stream (Event) the same as the one of Main Stream (Continuous).

Step 3 Verify the frame rate is real-time frame rate.

Step 4 Select "Menu > Record > Parameters > Record," and set the Frame Rate to Full Frame.

Step 5 Check if the fault is solved by the above steps.

Step 6 If it is solved, finish the process.

Step 7 If not, contact an engineer from our company for further analysis.

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

Possible Reasons:

— Cable between the pickup and camera is not connected well; impedance mismatches or is incompatible.

— The stream type is not set to "Video & Audio."

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

Step 2 Verify the setting parameters are correct.

Step 3 Select "Menu > Record > Parameters > Record," and set the Stream Type to "Audio & Video."

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

Step 5 If it is solved, finish the process.

Step 6 If not, contact an engineer from our company for further analysis.

- **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 delay.

  Step 1 Verify the frame rate is real-time frame rate.

  Step 2 Select “Menu > Record > Parameters > Record,” and set the Frame Rate to “Full Frame.”

  Step 3 Verify the hardware can support the playback.

  Step 4 Reduce the channel number of playback.

  Step 5 Select “Menu > Record > Encoding > Record”, and set the resolution and bitrate to a lower level.

  Step 6 Reduce the number of local playback channel.

  Step 7 Select “Menu > Playback,” and uncheck the checkbox of unnecessary channels.

  Step 8 Check if the fault is solved by the above steps.

  Step 9 If it is solved, finish the process.

  Step 10 If not, contact an engineer from our company for further analysis.

- **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 time setting of system is incorrect.

  — The search condition is incorrect.

  — The HDD is error or not detected.

  Step 1 Verify the system time setting is correct.

  Step 2 Select “Menu > Configuration > General > General,” and verify the “System Time” is correct.

  Step 3 Verify the search condition is correct.

  Step 4 Select “Playback,” and verify the channel and time are correct.

  Step 5 Verify the HDD status is normal.

Step 6 Select “Menu > System Configuration > HDD > General” to view the HDD status, and verify the HDD is detected and can be read and written normally.

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

Step 8 If it is solved, finish the process.

Step 9 If not, contact an engineer from our company for further analysis.

18.4 List of Compatible Hikvision IP Cameras

Type	Model	Version	Max. 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	V5.1.0build 131202	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 build 131012	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	V5.0.2Build 130926	1280×960	√	√

NOTE

Hikvision holds the right to interpret this list.

18.5 List of Compatible Third-Party IP Cameras

Manufacturer	Model	Version	Max. 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	√	×