Network Video Recorder

I Series NVR User Manual

03/01/17

DS-7608NI-I2/8P • DS-7616NI-I2/16P • DS-7716NI-I4/16P • DS-9616NI-I8 • DS-9632NI-I8 • DS-9664NI-I8

I Series Network Video Recorder User Manual, 030117NA

About this Manual

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

Please use this user manual under the guidance of professionals.

Trademarks Acknowledgement

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

Legal Disclaimer

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

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. HIKVISION SHALL NOT TAKE ANY 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

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 2004/108/EC, 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.

Safety Instruction

These instructions are intended to ensure that user can use the product correctly to avoid danger or property loss.

The precaution measure is divided into “Warnings” and “Cautions”

Warnings: Serious injury or death may occur if any of the warnings are neglected.

Cautions: Injury or equipment damage may occur if any of the cautions are neglected.

	
Warnings Follow these safeguards to prevent serious injury or death.	**Cautions** Follow these precautions to prevent potential injury or material damage.

 Warnings

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

In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region. Please refer to technical specifications for detailed information.

Input voltage should meet both the SELV (Safety Extra Low Voltage) and the Limited Power Source with 100~240 VAC or 12 VDC according to the IEC60950-1 standard. Please refer to technical specifications for detailed information.

Do not connect several devices to one power adapter as adapter overload may cause over-heating or a fire hazard.

Please make sure that the plug is firmly connected to the power socket.

If smoke, odor or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.

Preventive and Cautionary Tips

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

- Ensure unit is installed in a well-ventilated, dust-free environment.
- Unit is designed for indoor use only.
- Keep all liquids away from the device.
- Ensure environmental conditions meet factory specifications.
- Ensure unit is properly secured to a rack or shelf. Major shocks or jolts to the unit as a result of dropping it may cause

damage to the sensitive electronics within the unit.

- Use the device in conjunction with an UPS if possible.
- Power down the unit before connecting and disconnecting accessories and peripherals.
- A factory recommended HDD should be used for this device.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.

Thank you for purchasing our product. If there is any question or request, please do not hesitate to contact dealer.

The figures in the manual are for reference only.

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

Series	Model
DS-96xxNI-I8	DS-9616NI-I8
	DS-9632NI-I8
	DS-9664NI-I8
DS-77xxNI-I4/P	DS-7716NI-I4/16P
DS-76xxNI-Ix/xP	DS-7608NI-I2/8P
	DS-7616NI-I2/16P

Table of Contents

Chapter 1 Product Key Features

1.1 General

- Compatible with network cameras, network domes, and encoders
- Connectable to the third-party network cameras like ACTI, Arecont, AXIS, Bosch, Brickcom, Canon, PANASONIC, Pelco, SAMSUNG, SANYO, SONY, Vivotek, and ZAVIO, and cameras that adopt ONVIF or PSIA protocol
- Connectable to smart IP cameras
- H.265/H.264/MPEG4 video formats
- PAL/NTSC adaptive video inputs
- Each channel supports dual-stream
- Up to 8/16/32/64 network cameras can be added according to different models
- Independent configuration for each channel (e.g., resolution, frame rate, bit rate, image quality, etc.)
- The quality of the input and output record is configurable

1.2 Local Monitoring

- HDMI/VGA1 and HDMI2/VGA2 outputs provided for DS-9600NI series NVR
- HDMI and VGA outputs provided for DS-7716NI-I4/16P NVR.
- HDMI Video output at up to 4K resolution and VGA video output at up to 2K resolution
- Multiple screen display in live view is supported, and the display sequence of channels is adjustable
- Live view screen can be switched in group. Manual switch and auto-switch are provided and the auto-switch interval is configurable.
- Quick setup menu is provided for live view
- Motion detection, video tampering, video exception alert and video loss alert functions
- Privacy mask
- Multiple PTZ protocols supported; PTZ preset, patrol and pattern
- Zooming in by clicking the mouse and PTZ tracing by dragging mouse
- Supports fisheye expansions: PTZ, 180° expansion, and 360° expansion

1.3 HDD Management

- Up to eight SATA hard disks and one eSATA disk can be connected to DS-9600NI-I8, four SATA hard disks for DS-7716NI-I4/16P
- Up to 6 TB storage capacity for each disk supported

- Supports eight network disks (NAS/IP SAN disk)
- Supports S.M.A.R.T. and bad sector detection
- HDD group management
- Supports HDD standby function
- HDD property: redundancy, read-only, read/write (R/W)
- HDD quota management; different capacity can be assigned to different channel
- For DS-9600NI-I8 series, RAID0, RAID1, RAID5, RAID6, and RAID 10 are supported
- Hot-swappable RAID storage scheme, and can be enabled and disabled on your demand. 16 arrays can be configured
- DS-9600NI-I8 series NVR supports disk clone to the eSATA disk
- Supports encrypted WD HDDs: WD2000FYYZ-31, WD3000FYYZ-31, WD4000FYYZ-31

1.4 Recording, Capture, and Playback

NOTE: Capture is supported by DS-96xxNI-I8 only.

- Holiday recording schedule configuration
- Continuous and event video recording parameters
- Multiple recording types: manual, continuous, alarm, motion, motion & alarm, and VCA
- Eight recording time periods with separated recording types
- Pre-record and post-record for alarm, motion detection for recording, and pre-record time for schedule and manual recording
- Searching record files and captured pictures by events (alarm input/motion detection)
- Tag adding for record files, searching and playing back by tags
- Locking and unlocking record files
- Local redundant recording and capture
- Provide new playback interface with easy and flexible operation
- Searching and playing back record files by channel number, recording type, start time, end time, etc.
- Smart search for the selected area in the video
- Zooming in when playback
- Reverse playback of multi-channel
- Supports pause, play reverse, speed up, speed down, skip forward, and skip backward when playback, and locating by dragging the mouse

- Supports thumbnails view and fast view during playback
- Up to 16-ch synchronous playback at 1080p real time
- Manual capture, continuous capture of video images and playback of captured pictures
- Supports enabling H.264+ to ensure high video quality with lowered bitrate

1.5 Backup

- Export video data by USB, SATA, or eSATA device (for DS-96xxNI-I8)
- Export video clips when playback
- Management and maintenance of backup devices
- Either Normal or Hot Spare working mode is configurable to constitute an N+1 hot spare system

1.6 Alarm and Exception

- Configurable arming time of alarm input/output
- Alarm for video loss, motion detection, tampering, abnormal signal, video input/output standard mismatch, illegal login, network disconnected, IP confliction, abnormal record/capture, HDD error, and HDD full, etc.
- VCA detection alarm is supported
- VCA search for face detection, vehicle plate, behavior analysis, people counting and heat map
- Alarm triggers full screen monitoring, audio alarm, notifying surveillance center, sending email and alarm output
- Automatic restore when system is abnormal

1.7 Other Local Functions

- Operable by front panel, mouse, remote control, or control keyboard
- Three-level user management; admin user is allowed to create many operating accounts and define their operating permission, which includes the limit to access any channel
- Operation, alarm, exceptions and log recording and searching
- Manually triggering and clearing alarms
- Import and export of device configuration information
- User can control 3D PTZ function through a network keyboard

1.8 Network Functions

- Two self-adaptive 10M/100M/1000M network interfaces for DS-96xxNI-I8, with multi-address mode for separate camera subnet or fault tolerance mode for the highest network reliability
- One self-adaptive 10M/100M/1000M network interface for DS-7716NI-I4/16P
- Sixteen independent PoE network interfaces for the /16P models

- IPv6 is supported
- TCP/IP protocol, DHCP, DNS, DDNS, NTP, SADP, SMTP, SNMP, NFS, and iSCSI are supported
- TCP, UDP and RTP for unicast
- Auto/Manual port mapping by UPnPTM
- Supports access by HIK-Connect Cloud P2P
- Remote Web browser access by HTTPS ensures high security
- ANR (Automatic Network Replenishment) function is supported, it enables the IP camera to save the recording files in the local storage when the network is disconnected, and synchronizes the files to the NVR when the network is resumed.
- Remote reverse playback via RTSP
- Supports accessing by the platform via ONVIF
- Remote search, playback, download, locking and unlocking of the record files, and support 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 locking and unlocking of control panel and mouse
- Remote HDD formatting and program upgrading
- Remote system restart and shutdown
- RS-232, RS-485 transparent channel transmission
- Alarm and exception information can be sent to the remote host
- Remotely start/stop recording
- Remotely start/stop alarm output
- Remote PTZ control
- Remote JPEG capture
- Virtual host function is provided to get access and manage the IP camera directly
- Two-way audio and voice broadcasting
- Embedded Web server

1.9 Development Scalability

- SDK for Windows system
- Source code of application software for demo

- Development support and training for application system

1.10 Security

- Supports quick unlocking of the device by using an optional user-defined pattern
- Users can view the password of connected IPCs by enabling IP Channel Password Is Visible (requires admin password if Enable Password option is disabled in Configuration Settings)

Chapter 2 Introduction

NOTE: Screenshots in this manual are for reference only; your NVR's screenshots may look different.

2.1 DS-96xxNI-I8 Series Front Panel

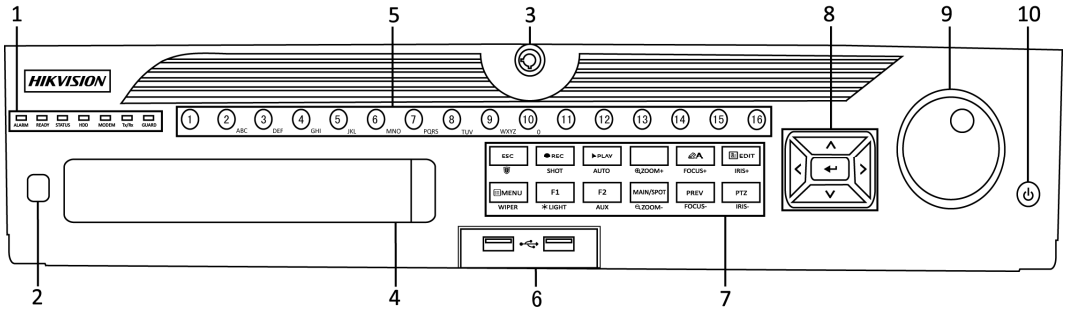


Figure 1 DS-96xxNI-I8 Series

Table 1 – Panel Description

No.	Name		Function Description
1	Status Indicators	ALARM	Turns red when a sensor alarm is detected
		READY	Turns blue when the device is functioning properly
		STATUS	Turns blue when device is controlled by an IR remote
			Turns red when controlled by a keyboard and purple when IR remote and keyboard are used at same time
		HDD	Flickers red when data is being read from or written to HDD
		MODEM	Reserved for future usage
		Tx/Rx	Flickers blue when network connection is functioning properly
		GUARD	Turns blue when the device is in armed status; at this time, an alarm is enabled when an event is detected
			Turns off when the device is unarmed (the arm/disarm status can be changed by pressing and holding on the ESC button for more than 3 seconds in live view mode)
2	IR Receiver		Receiver for IR remote control
3	Front Panel Lock		Locks or unlocks the panel by the key
4	DVD-R/W		Slot for DVD-R/W disk
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
			Turns blue when the corresponding channel is recording; turns red when the channel is in network transmission status; turns pink when the channel is recording and transmitting
6	USB Interfaces		USB ports for additional devices such as USB mouse and USB Hard Disk Drive
7	Composite Keys	ESC	Returns to the previous menu
			Press to arm/disarm the device in live view mode
		REC/SHOT	Enters the Manual Record settings menu
			Press 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 the PTZ control menu
		ZOOM+	Zooms in the PTZ camera in the PTZ control setting
		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 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

No.	Name		Function Description
		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	Control Buttons	DIRECTION	Navigates between different fields and items in menus
			In playback mode, use the Up and Down buttons to speed up and slow down recorded video; use the Left and Right buttons to select the next and previous video files
			Cycles through channels in live view mode
			Controls the movement of the PTZ camera in PTZ control mode
		ENTER	Confirms selection in any of the menu modes
			Checks the checkbox fields
			Plays or pauses the video playing in playback mode
			Advances the video by a single frame in single-frame playback mode
			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		Long press the button for more than 3 seconds to turn on/off the NVR

2.2 DS-7716NI-I4/16P Front Panel

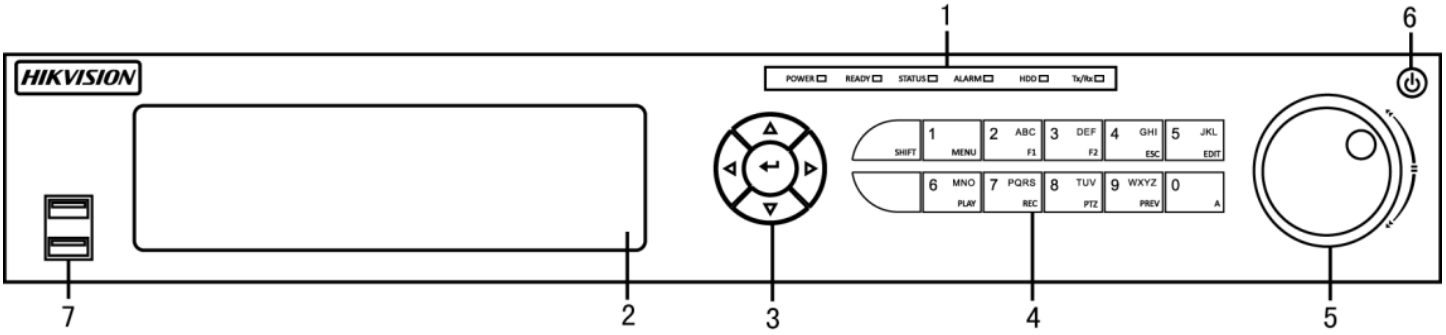


Figure 2 DS-7716NI-I4/16P

Table 2 – Panel Description

No.	Name		Function Description
1	Status Indicators	Alarm	Red when a sensor alarm is detected
		Ready	Blue when DVR is functioning properly
		Status	Blue when DVR is controlled by IR remote, red when controlled by a keyboard, and purple when IR remote and keyboard is used at the same time
		HDD	Blinks red when data is being read from/written to HDD
		Modem	Reserved
		TX/RX	Blinks blue when network connection is functioning properly
2	DVD-ROM		Slot for DVR-ROM
3	Direction/ Enter Buttons	Direction Buttons	Navigates between fields and menu items. In playback mode, Up and Down buttons fast-forward and rewind recorded video. Left and Right buttons select next and previous day or pauses video.
		ENTER	Confirms menu selection. Ticks checkbox fields. In Playback mode, plays or pauses video. In Single Play mode, advances video a single frame.
4	Control Buttons	1/MENU	Types “1.” Also accesses main menu.
		2ABC/F1	Types “2, A, B, and C.” Selects all items on a list; In PTZ Control mode, zooms out (zoom-) the PTZ camera; In live view or playback mode, switches between main and spot video output.
		3DEF/F2	Types “3, D, E, and F.” In PTZ Control mode, zooms in (zoom+) the PTZ camera; cycles through tab pages.
		4GHI/ESC	Types “4, G, H, and I.” Exits to previous menu.
		5JKL/EDIT	Types “5, J, K, and L.” Deletes character before cursor; Selects checkbox and ON/OFF switch; Start/stops record clipping in playback.
		SHIFT	Switches compound keys between numeric/letter input and functional control
		6MNO/PLAY	Types “6, M, N, and O.” In Playback mode, accesses playback interface.
		7PQRS/REC	Enters “7, P, Q, R, and S.” Manual record, for direct access to manual record interface; manually enables/disables record.
		8TUV/PTZ	Types “8, T, U, and V.” Accesses PTZ control interface.
		9WXYZ/PREV	Types “9, W, X, Y, and Z.” Multi-camera display in live view. In Playback mode or Menu>Playback>Tag playback interface, deletes selected tag.
		0/A	Types “0.” Switches between input methods (upper and lower case alphabet, symbols, and numeric input). In Playback mode, adds default tag.
5	Jog Shuttle Control		Moves active selection in a menu. In playback mode, outer ring speeds up/slows down video. Inner ring jumps 30 seconds forward/backward in video. In Preview mode, cycles through channels.
6	Power Button		Powers DVR on/off
7	USB Ports		Connects USB mouse or USB flash memory devices

2.3 DS-76xxNI-I2/xP Series Front Panel

Figure 3 DS-76xxNI-I2/xP Series

Table 3 – Panel Description

No.	Item	Description
1.	On/Off Power	Turns green when device is on
2.	Hard Drive	Flickers red when data is being read from or written to HDD
3.	Network Tx/Rx	Flickers blue when network connection is functioning properly
4.	USB Port	Connects USB mouse or USB flash memory devices

2.4 DS-96xxNI-I8 Series Rear Panel

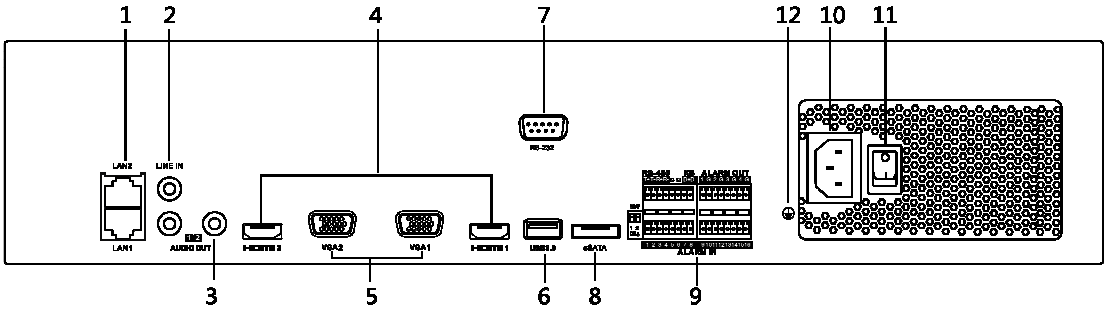


Figure 4 DS-96xxNI-I8 Series

Table 3 – Panel Description

No.	Name	Description
1	LAN1/LAN2 Interface	2 RJ-45 10/100/1000 Mbps self-adaptive Ethernet interfaces provided.
2	LINE IN	RCA connector for audio input.
3	AUDIO OUT	2 RCA connectors for audio output.
4	HDMI1/HDMI2	HDMI video output connector.
5	VGA1/VGA2	DB-15 connector for VGA output. Display local video output and menu.
6	USB 3.0 interface	USB ports for additional devices such as USB mouse and USB Hard Disk Drive (HDD).
7	RS-232 Interface	Connector for RS-232 devices.
8	eSATA	Connects external SATA HDD, CD/DVD-RM.
9	Controller Port	D+, D- pin connects to Ta, Tb pin of controller. For cascading devices, the first NVR's D+, D- pin should be connected with the D+, D- pin of the next NVR.
	ALARM IN	Connector for alarm input.
	ALARM OUT	Connector for alarm output.
10	100 to 240 VAC	100 to 240 VAC power supply.
11	Power Switch	Switch for turning on/off the device.
12	GROUND	Ground (needs to be connected when NVR starts up).

2.5 DS-77xxNI-I4/16P Rear Panel

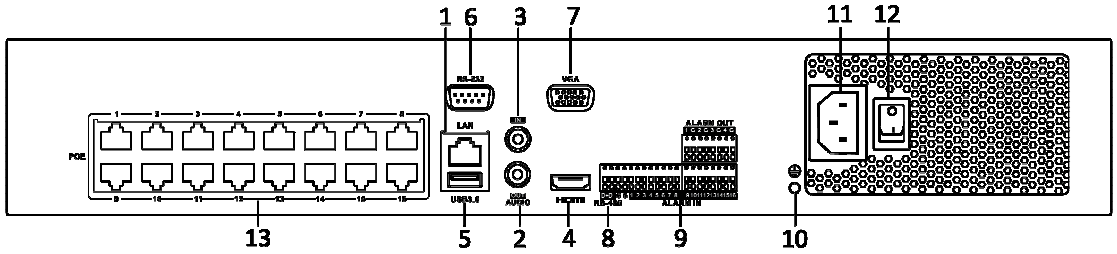


Figure 5 DS-77xxNI-I4/16P

Table 4 – Panel Description

No.	Name	Description
1	LAN Interface	1 network interface provided for DS-7700NI-I4/P.
2	AUDIO OUT	RCA connector for audio output
3	LINE IN	RCA connector for audio input
4	HDMI	HDMI video output connector
5	USB 3.0 interface	USB ports for additional devices such as USB mouse and USB Hard Disk Drive (HDD)
6	RS-232 Interface	Connector for RS-232 devices
7	VGA	DB-15 connector for VGA output. Display local video output and menu.
8	RS-485 Interface	Half-duplex connector for RS-485 devices
9	ALARM IN	Connector for alarm input
	ALARM OUT	Connector for alarm output
10	GROUND	Ground (needs to be connected when NVR starts up)
11	100 VAC to 240 VAC	100 to 240 VAC power supply
12	Power Switch	Switch for turning on/off the device
13	Network Interfaces with PoE function (supported by DS-7700NI-I4/P)	Network interfaces for the cameras and to provide power over Ethernet

2.6 DS-76xxNI-I2/xP Series Rear Panels

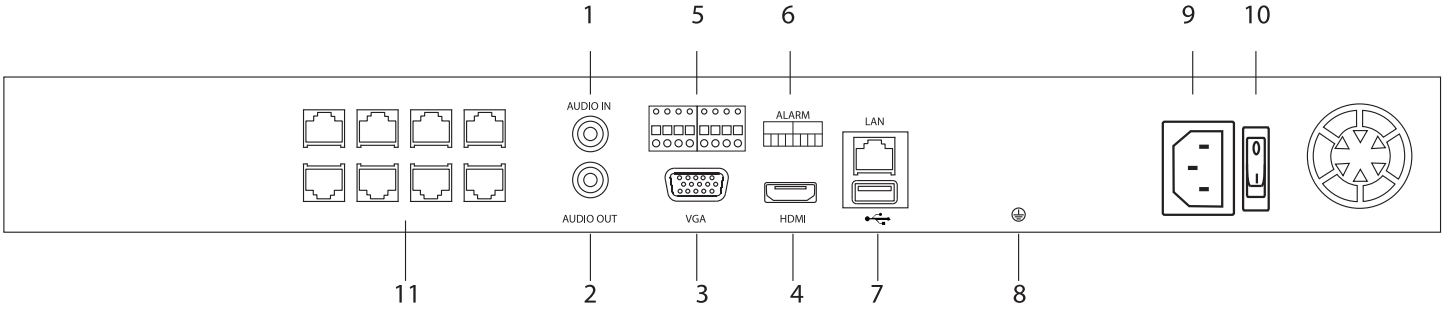


Figure 6 DS-76xxNI-I2/8P

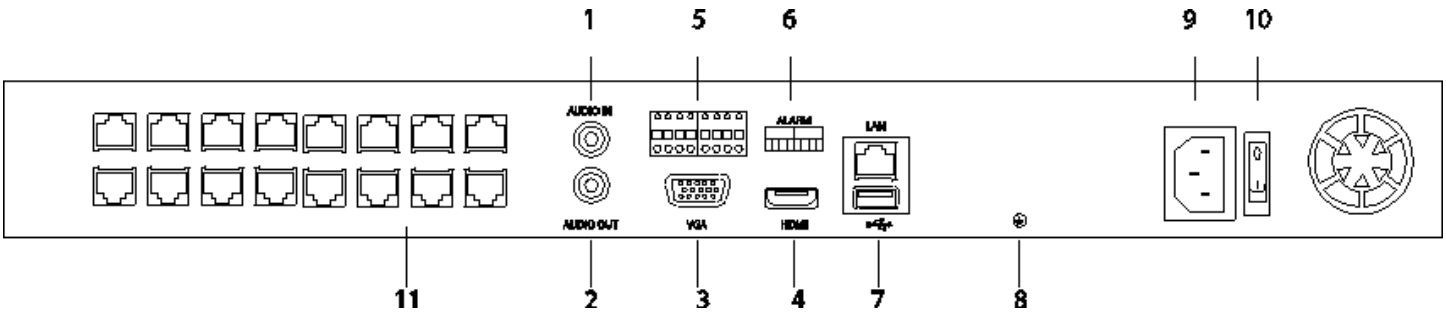


Figure 7 DS-7608NI-I2/16P

Table 5 – Panel Description

No.	Name	Description							
1	AUDIO IN	RCA connector for audio input							
2	AUDIO OUT	RCA connector for audio output							
3	VGA	DB-15 connector for VGA output. Display local video output and menu.							
4	HDMI	HDMI video output connector							
5	ALARM I/O	1	2	3	4	5	6	7	8
		In	In	In	In	Gnd	Gnd	Out	Gnd
6	Alarm Legend	Printed legend for alarm connections							
7	USB 3.0 interface	USB ports for additional devices such as USB mouse and USB Hard Disk Drive (HDD)							
8	GROUND	Ground (needs to be connected when NVR starts up)							
9	100 VAC to 240 VAC	100 to 240 VAC power supply							
10	Power Switch	Switch for turning on/off the device							
11	Network Interfaces with PoE function	Network interfaces for the cameras and to provide power over Ethernet							

2.7 IR Remote Control Operations

The NVR may also be controlled with the included IR remote control, shown in Figure 8. The keys on the remote control closely resemble the ones on the front panel.

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

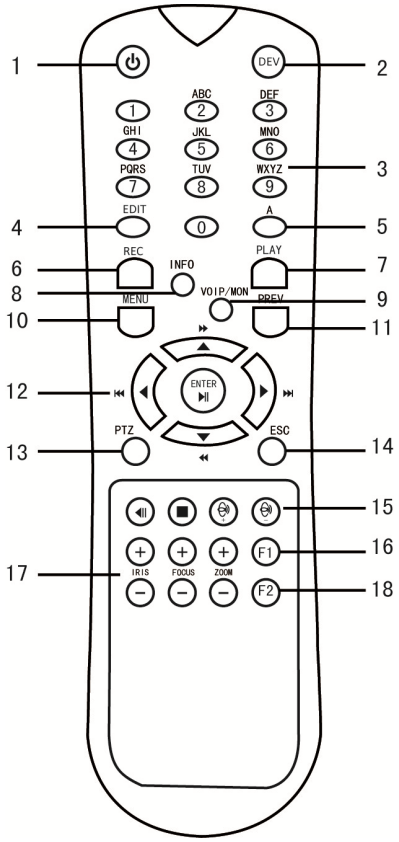


Figure 8 Remote Control

Table 6 – Description of the Soft Keyboard Icons

No.	Name	Description
1	POWER	Power on/off the device
2	DEV	Enables/Disables Remote Control
3	Alphanumeric Buttons	Same as Alphanumeric buttons on front panel
4	EDIT Button	Same as EDIT/IRIS+ button on front panel
5	A Button	Same as A/FOCUS+ button on front panel
6	REC Button	Same as REC/SHOT button on front panel
7	PLAY Button	Same as the PLAY/AUTO button on front panel
8	INFO Button	Reserved
9	VOIP/MON Button	Same as the MAIN/SPOT/ZOOM- button on front panel
10	MENU Button	Same as the MENU/WIPER button on front panel
11	PREV Button	Same as the PREV/FOCUS- button on front panel
12	DIRECTION/ENTER Buttons	Same as the DIRECTION/ENTER buttons on front panel
13	PTZ Button	Same as the PTZ/IRIS- button on front panel
14	ESC Button	Same as the ESC button on front panel
15	RESERVED	Reserved for future usage
16	F1 Button	Same as the F1/LIGHT button on front panel
17	PTZ Control Buttons	Buttons to adjust the iris, focus and zoom of a PTZ camera
18	F2 Button	Same as the F2/AUX button on front panel

2.8 Troubleshooting Remote Control

NOTE: Make sure you have installed batteries properly in the remote control. Note that you have to aim the remote control at the IR receiver in the front panel.

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

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

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

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

If the remote still doesn't function properly, change the remote and try again, or contact the device provider.

2.9 USB Mouse Operation

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

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

Table 7 – Mouse Control

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

2.10 Input Method Description

Figure 9 Soft Keyboard (1) Figure 10 Soft Keyboard (2)

Table 8 – 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		Exit
#+=	Symbols		Reserved

Chapter 3 Getting Started

3.1 Starting Up and Shutting Down the NVR

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

3.1.1. Before You Start

Check that the voltage of the extra power supply is the same as the NVR's requirement and the ground connection is working properly.

3.1.2. Starting the NVR

Check to ensure the power supply cable is firmly inserted into the NVR and is properly plugged into the electrical outlet. It is HIGHLY recommended that an Uninterruptible Power Supply (UPS), preferably a UPS capable of providing a constant level of power, be used in conjunction with the device. The Power indicator LED on the front panel should be red, indicating the device gets the power supply.

1. Press the **POWER** button on the front panel. The Power indicator LED should turn blue indicating that the unit begins to start up.

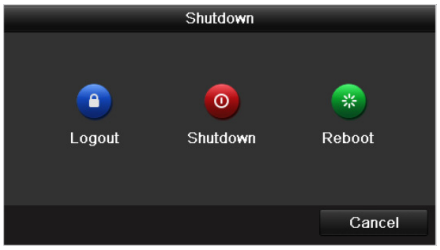
2. After startup, the Power indicator LED remains blue. A splash screen with the status of the HDD appears on the monitor. The row of icons at the bottom of the screen shows the HDD status. 'X' means that the HDD is not installed or cannot be detected.

3.1.3. Shutting Down the NVR

There are two proper ways to shut down the NVR.

- **OPTION 1: Standard Shutdown**

  1. Enter the Shutdown menu by going to Menu > Maintenance > Shutdown



Shutdown Menu

  2. Click the **Shutdown** button.

  3. Click the **Yes** button.

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

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

     NOTE: Do not press POWER button again while system is shutting down.

3.1.4. Rebooting the NVR

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

3.2 Activating Your Device

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

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

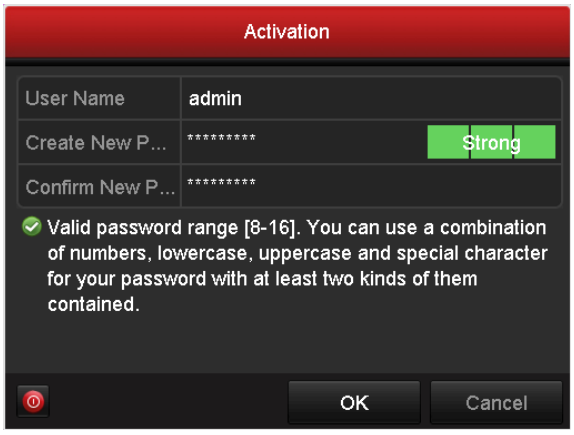


Figure 11 Settings Admin Password

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.

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

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

Figure 12 Attention Interface

3.3 Using the Unlock Pattern for Login

For the Admin user, you can configure the unlock pattern for device login.

3.3.1. Configuring the Unlock Pattern

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

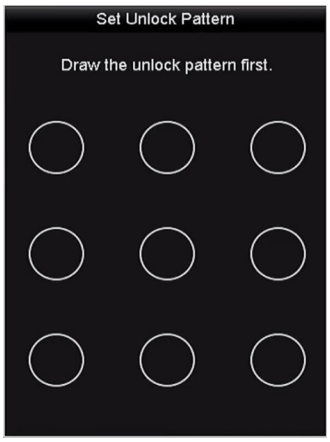


Figure 13 Set Unlock Pattern

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

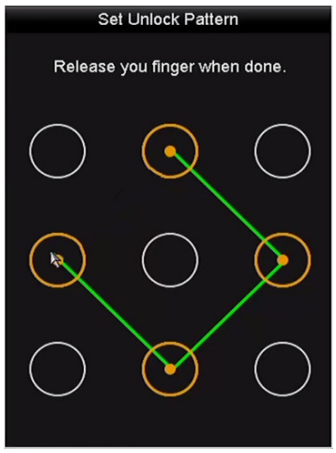


Figure 14 Draw the Pattern

- Connect at least four dots to draw the pattern.
- Each dot can be connected once only.

2. Draw the same pattern again to confirm it. If the two patterns match, the pattern is successful.

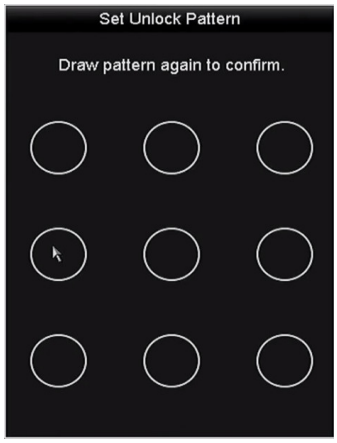


Figure 15 Confirm the Pattern

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

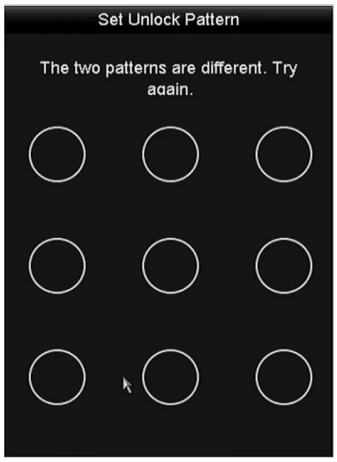


Figure 16 Reset the Pattern

3.3.2. Logging in via Unlock Pattern

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

Configure the pattern before unlocking. See “

Configuring the **Unlock Pattern**.”

1. Right click the mouse and select the menu to enter the interface as shown in Figure 17.

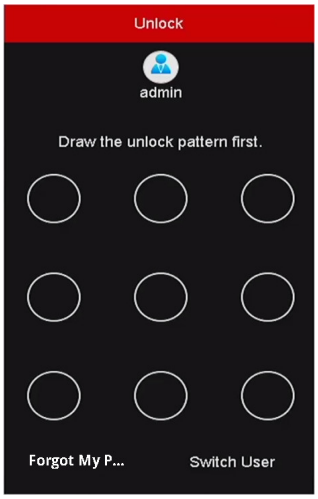


Figure 17 Draw the Unlock Pattern

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

NOTES: If you have forgotten your pattern, you can select the “Forgot My Pattern” or “Switch

User" option to enter the normal login dialog box.

When the pattern you draw differs from the configured pattern, you must try again.

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

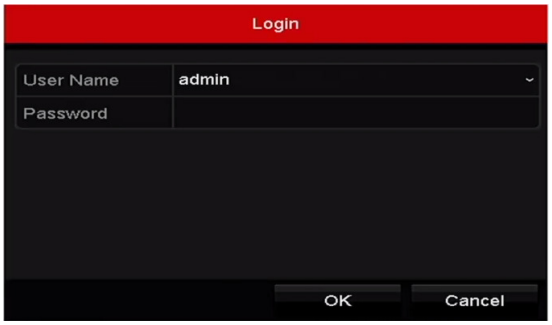


Figure 18 Normal Login Dialog Box

3.4 Login and Logout

3.4.1. User Login

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

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

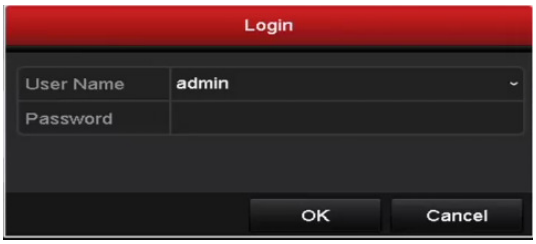


Figure 19 Login Interface

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

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

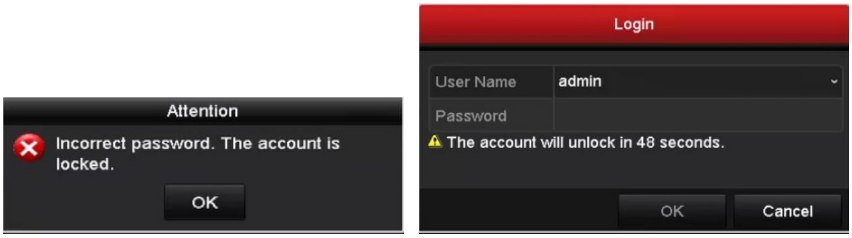


Figure 20 User Account Protection

3.4.2. User Logout

After logging out, the monitor turns to the live view mode. To perform any operations, log in again.

1. Enter the Shutdown menu, Menu > Shutdown.

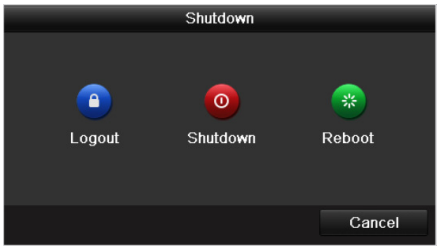


Figure 21 Logout

2. Click **Logout**.

NOTE: After logging out, menu operations are invalid. Input user name and password to unlock system.

3.5 Adding and Connecting the IP Cameras

3.5.1. Activating the IP Camera

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

1. Select the **Add IP Camera** option from the right-click menu in live view mode or click Menu > Camera > Camera to enter the IP camera management interface. For IP cameras detected online in the same network segment, **Password** status shows whether it is active or inactive.

Figure 22 IP Camera Interface

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

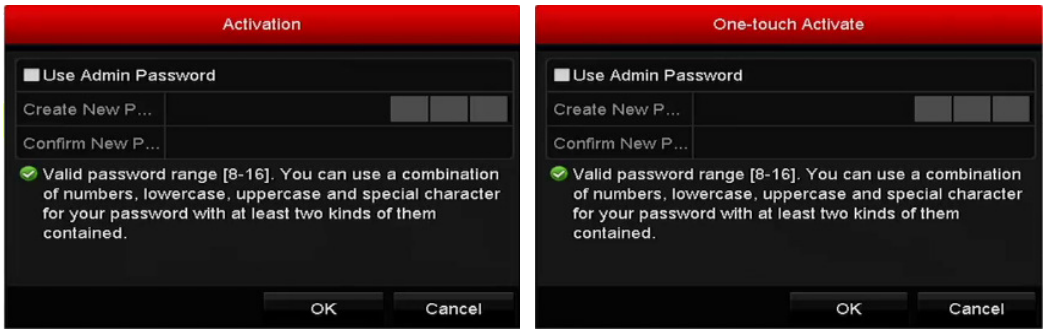


Figure 23 Activate the Camera

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

   - **Use Admin Password:** Check the checkbox to have camera(s) will be configured with the same admin password as the operating NVR.

Figure 24 Set New Password

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

> **Strong Password Recommended**
>
> We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. 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.

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

3.5.2. Adding the Online IP Cameras

The NVR's primary function is to connect to, and record video from, the network cameras. Before you can get a live view or record the video, you must add the network cameras to the connection list of the device.

3.5.2.1 Before You Start

Ensure the network connection is valid and correct. See Chapter *Checking Network Traffic* and Chapter *Configuring Network Detection*.

3.5.2.2 Add the IP Cameras

- **OPTION 1**

1. Click to select an idle window in the live view mode.
2. Click the icon in the window center to show the Adding IP Camera interface.
3. Select the IP camera and click the **Add** button to add it directly, or custom add it by editing the corresponding text field parameters, then clicking the **Add** button. Click the **Search** button to refresh online IP cameras manually.

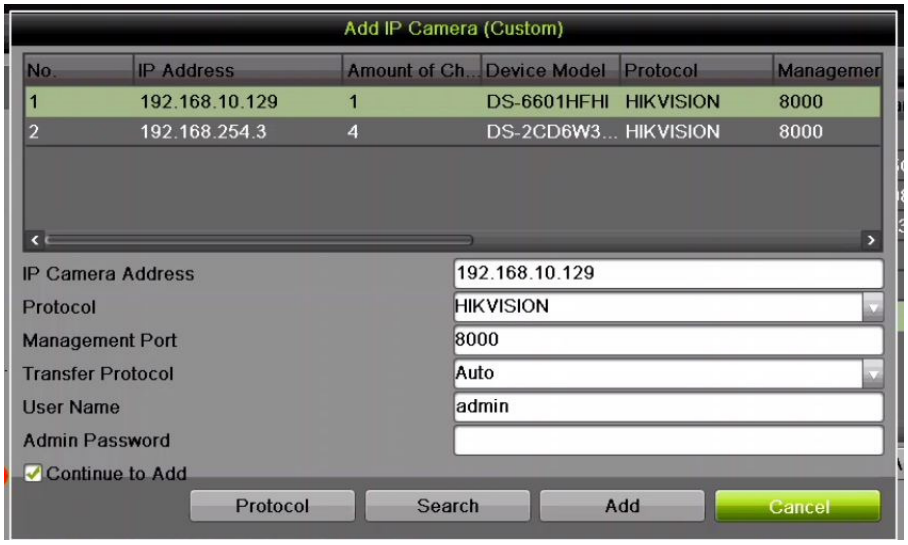


Figure 25 Add IP Camera Interface

- **OPTION 2**

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

Figure 26 Adding IP Camera Interface

2. Online cameras in the same network segment will be displayed.

3. Select the IP camera from the list and click the button to add the camera, or click the **One-touch Adding** button to add all cameras (with the same login password) from the list.

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

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

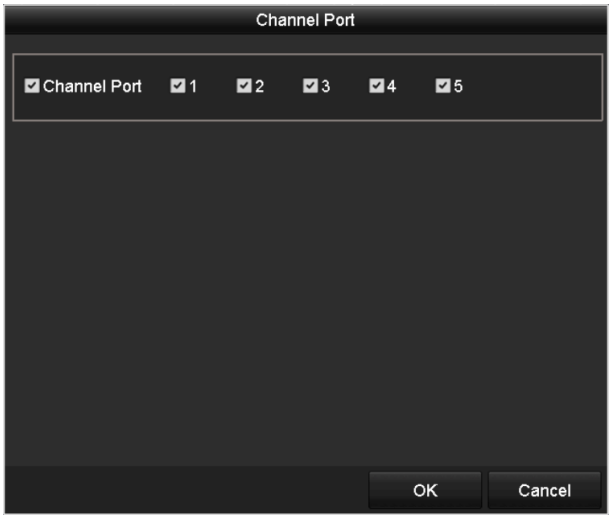


Figure 27 Selecting Multiple Channels

- **OPTION 3**

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

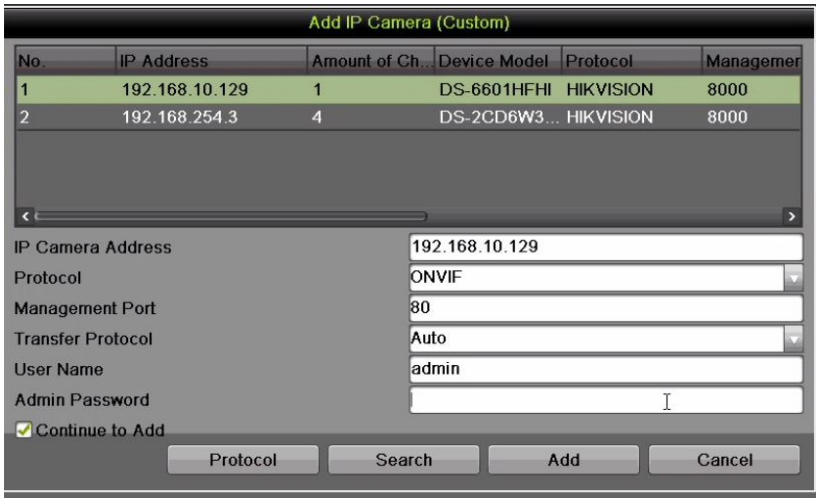


Figure 28 Add IP Camera (Custom) Interface

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, you can activate it from the IP camera list on the camera management interface.

3. (Optional) Check the checkbox of **Continue to Add** to add other IP cameras.

4. Click **Add** to add the camera. The successfully added cameras are listed in the interface.

Table 9 – Icon Descriptions

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

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

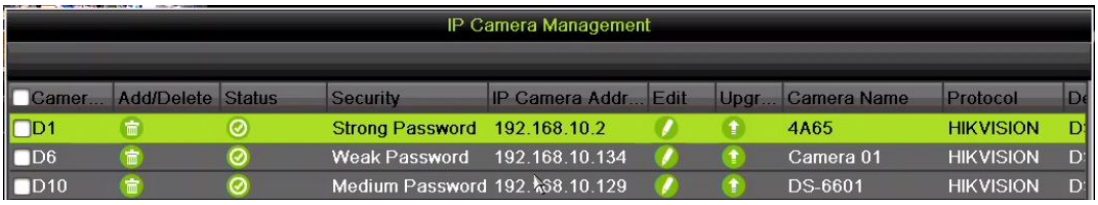


Figure 29 Security Level of IP Camera's Password

3.5.2.3 Enabling the IP Camera Show Password Setting

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

Figure 30 List of Added IP Cameras

3.5.3. Enabling the H.265 Stream Access

Check the **Enable H.265** checkbox to have the NVR automatically switch to the IP camera's (that support H.265 video format) H.265 stream for the initial access.

3.5.4. Editing Connected IP Cameras and Custom Configuring Protocols

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

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

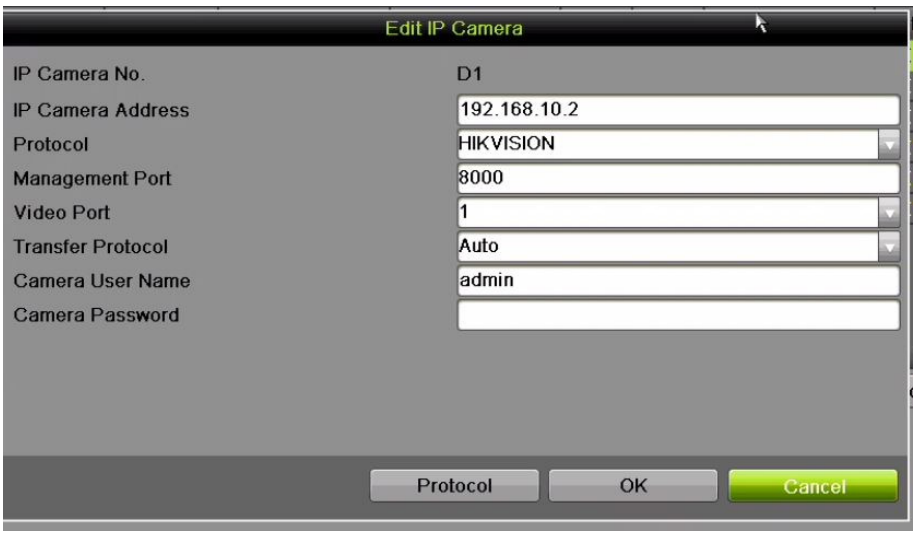


Figure 31 Edit IP Camera

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

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

3.5.4.1 Editing Advanced Parameters

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

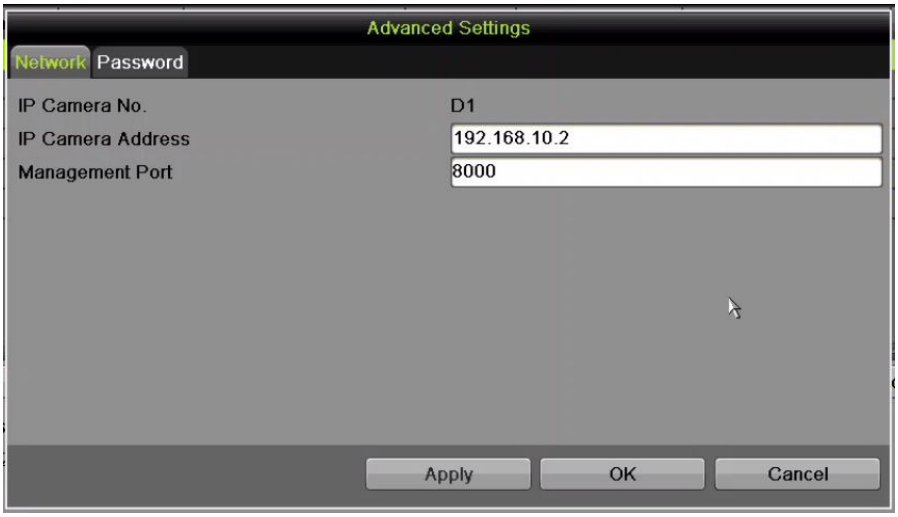


Figure 32 Network Configuration of the Camera

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

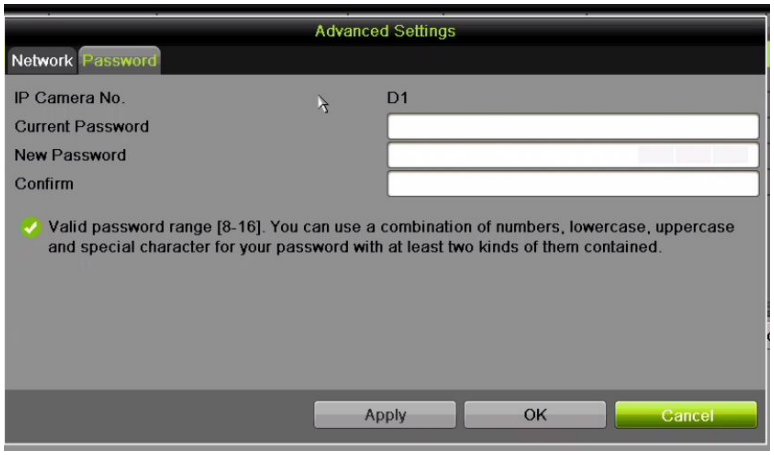


Figure 33 Password Configuration of the Camera

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

3.5.4.2 Configuring Custom Protocols

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

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

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

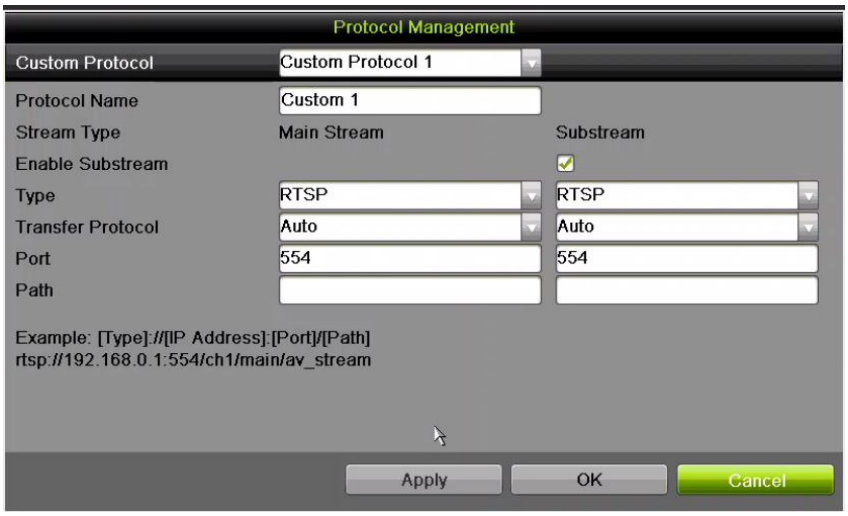


Figure 34 Protocol Management Interface

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

NOTE: Before customizing the protocol for the network camera, contact the manufacturer of

the network camera to consult the URL (uniform resource locator) for getting the main stream and sub-stream. The URL format is: [Type]://[IP Address of the network camera]:[Port]/[Path].

Example: rtsp://192.168.1.55:554/ch1/main/av_stream.

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

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

After adding the customized protocols, you can see the protocol name listed in the drop-down list (Figure 35).

Figure 35 Protocol Setting

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

3.5.5. Editing IP Cameras Connected to PoE Interfaces

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

NOTE: The DS-7700NI-I4/16P NVR PoE interface supports the Plug-and-Play function.

3.5.6. To Add Cameras for NVR Supporting PoE Function

3.5.6.1 Before You Start

Connect the network cameras via the PoE interfaces.

1. Enter the camera management interface, Menu > Camera Setup.

Figure 36 List of Connected Cameras

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

2. Click the button, and select the Adding Method in the drop-down list.

- **Plug-and-Play:** It means that the camera is connected to the PoE interface, so in this case, the parameters of the camera can't be edited. The IP address of the camera can only be edited in the Network Configuration interface, see *Chapter 11.1*

- *Configuring General* Settings for detailed information.

Figure 37 Edit IP Camera Interface, Plug-and-Play

- **Manual:** You can disable the PoE interface by selecting manual while the current channel can be used as a normal channel and the parameters can also be edited.

3. Input the IP address, user name, and administrator password manually, and click **OK** to add the IP camera.

Figure 38 Edit IP Camera Interface, Manual

Chapter 4 Live View

4.1 Introduction of Live View

Live view shows the video image from each camera in real time. The NVR automatically enters Live View mode when powered on. It is also at the very top of the menu hierarchy, thus pressing the ESC many times (depending on which menu you're on) brings you to the Live View mode.

NOTE: "Unsupported Stream Type" will appear if the stream doesn't match the NVR's decoding standard (compression or resolution).

4.2 Live View Icons

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

Table 10 – Description of Live View Icons

Icons	Description
	Alarm (video loss, video tampering, motion detection, VCA and sensor alarm)
	Record (manual record, schedule record, motion detection, VCA and alarm triggered record)
	Alarm and Record
	Event/Exception (motion detection, VCA, sensor alarm, or exception information, appears at the lower-left corner of the screen. Refer to *Chapter 0 Setting Alarm Response Actions* for details.)

4.3 Operations in Live View Mode

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

- Single Screen: Show only one screen on the monitor
- Multi-screen: Show multiple screens on the monitor simultaneously
- Auto-switch: 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: Continuous record and motion detection record are supported
- Output Mode: Select the output mode: Standard, Bright, Gentle, or Vivid
- Add IP Camera: Shortcut to the IP camera management interface
- Playback: Play back recorded videos for the current day

- Aux Monitor: NVR checks the connection of the output interfaces to define the main and auxiliary output. The priority level for the main and aux output is HDMI1/VGA1> HDMI2/VGA2 (for DS-9600NI-I8) and HDMI > VGA (for DS-7716NI-I4/16P).

DS-96xxNI-I8: When the HDMI1, HDMI2, VGA1, and VGA2 are all connected, the HDMI1/VGA1 is used as main output and the HDMI2/VGA2 is used as the aux output.

DS-7716NI-I4/16P: When both the HDMI and VGA are connected, the HDMI is used as main output and the VGA is used as the aux output.

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

4.4 Live View Operations

4.4.1. Front Panel Operation

Table 11 – Front Panel Operation in Live View

Functions	Front Panel Operation
Common Menu	Quick access to the sub-menus you frequently visit. Up to five sub-menu options are supported.
Menu	Enter the main menu of the system by right clicking the mouse.
Show single screen	Press the corresponding Alphanumeric button (e.g. Press 2 to display only the screen for channel 2).
Show multi-screen	Press the **PREV/FOCUS-** button.
Manually switch screens	Next screen: right/down direction button. Previous screen: left/up direction button.
Auto-switch	Press **Enter** button.
Playback	Press **Play** button.
Switch between main and aux output	Press **Main/Aux** button.

4.4.2. Using the Mouse in Live View

Table 12 – Mouse Operation in Live View

Name	Description
Common Menu	Quick access to the sub-menus that you frequently visit.
Menu	Enter the main menu of the system by right clicking the mouse.
Single Screen	Switch to the single full screen by choosing channel number from the drop-down list.
Multi-screen	Adjust the screen layout by choosing from the drop-down list.
Previous Screen	Switch to the previous screen.
Next Screen	Switch to the next screen.
Start/Stop Auto-switch	Enable/disable the auto-switch of the screens.
Start Recording	Start continuous recording or motion detection recording of all channels.
Add IP Camera	Enter the IP Camera Management interface, and manage the cameras.
Playback	Enter the playback interface and start playing back the video of the selected channel immediately.
PTZ	Enter the PTZ control interface.
Output Mode	Four modes of output supported, including Standard, Bright, Gentle, and Vivid.
Aux Monitor	Switch to the auxiliary output mode and the operation for the main output is disabled.

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

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

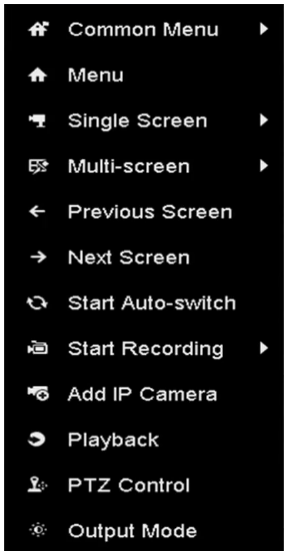


Figure 39 Right-click Menu

4.4.3. Quick Setting Toolbar in Live View Mode

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

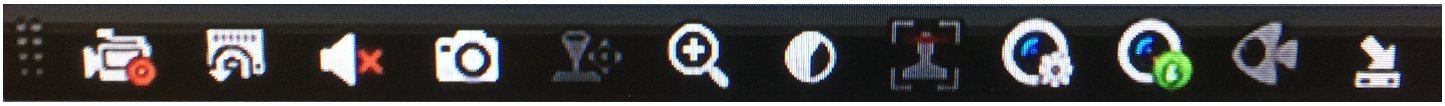


Figure 40 Quick Setting Toolbar

The fisheye expansion view feature is supported by the DS-7700/9600-I(/P) series NVRs only.

Table 13 – Description of Quick Setting Toolbar Icons

Icon	Description	Icon	Description	Icon	Description
/	**Enable/Disable Manual Record**		**Instant Playback**. Shows the record only in the last five minutes. If no record is found, there is no record during the last five minutes.	/	**Mute/Audio On**
	Capture		**PTZ Control**		**Digital Zoom**. Zoom in on live image in different magnifications (1 to 16x) by moving sliding bar from to . You can also scroll mouse wheel to control the zoom.
	Image Settings. Select to enter the Image Settings menu to set image parameters such as brightness, contrast, saturation, and hue		**Face Detection**. In live view mode, when human faces of a specified size are detected, the device will capture the human face and save to the HDD.		**Live View Strategy**. Sets strategy, including Real-time, Balanced, Fluency
	Information. Move mouse onto the icon to show real-time stream information, including frame rate, bitrate, resolution, and stream type		**Fisheye Expansion**		**Close**
	Fisheye Settings		**Information**	/	**Start Record/Stop Record**

Figure 41 Digital Zoom

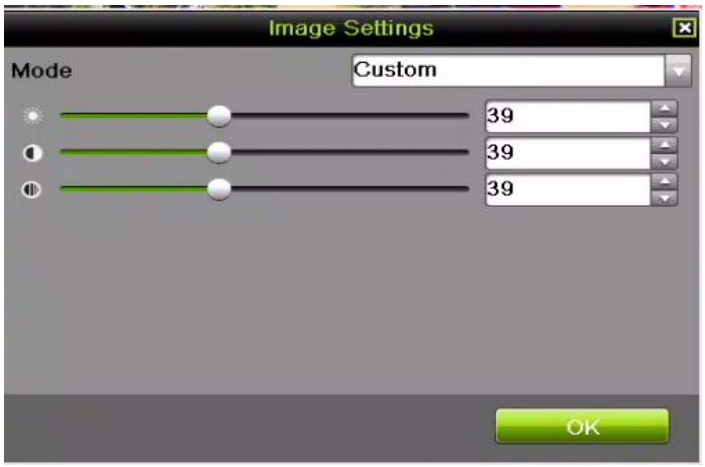


Figure 42 Image Settings, Customize

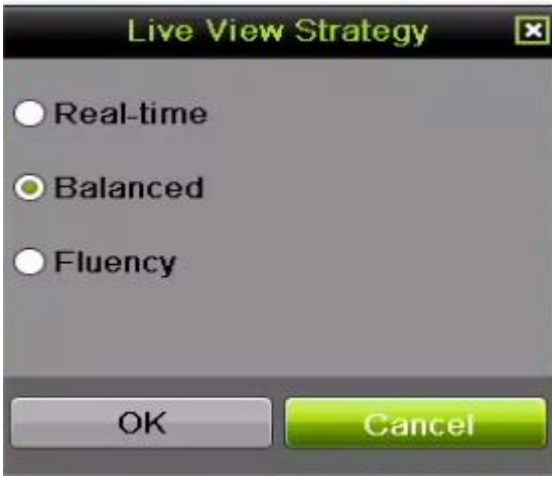


Figure 43 Live View Strategy

Figure 44 Information

4.4.4. Fisheye Expansion View

The device supports fisheye expansion of the connected fisheye camera in live view or playback mode.

1. Click  to enter fisheye expansion mode.

Table 14 – Fisheye Display Mode

	Button	Operation
Fisheye Expansion		180° panorama
		360° panorama
		PTZ expansion
		Fisheye

2. Four different display modes are available. Select a display mode as needed.
   - **180° Panorama**: Switch the live view image to the 180° panorama view.
   - **360° Panorama**: Switch the live view image to the 360° panorama view.
   - **PTZ Expansion**: The PTZ Expansion is the close-up view of a defined area in the fisheye view or panorama expansion, and it supports the electronic PTZ function, which is also called e-PTZ.
   - **Fisheye**: The whole wide-angle view of the fisheye camera is displayed. This mode is called Fisheye View because it approximates the vision of a fish's convex eye. The lens produces curvilinear images of a large area, while distorting the perspective and angles of objects.

4.5 Adjusting Live View Settings

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

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

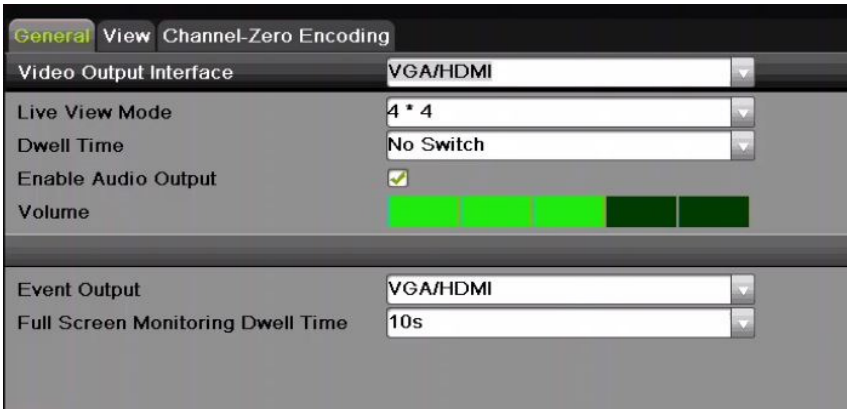


Figure 45 Live View, General

2. Configure the following settings, as appropriate:

   - Video Output Interface: Designates the output for which to configure the settings. DS-9600NI provides VGA/HDMI and VGA2/HDMI2, and DS-7700NI provides HDMI and VGA video outputs.
   - Live View Mode: Designate the display mode to be used for Live View
   - Dwell Time: The time in seconds to dwell between channels with auto-switch enabled in Live View
   - Enable Audio Output: Enable/disable audio output for the selected video output
   - Volume: Adjust the volume of live view, playback, and two-way audio for the selected output interface
   - Event Output: Designate the output to show event video
   - Full Screen Monitoring Dwell Time: The time in seconds to show alarm event screen

3. Set Camera Order.

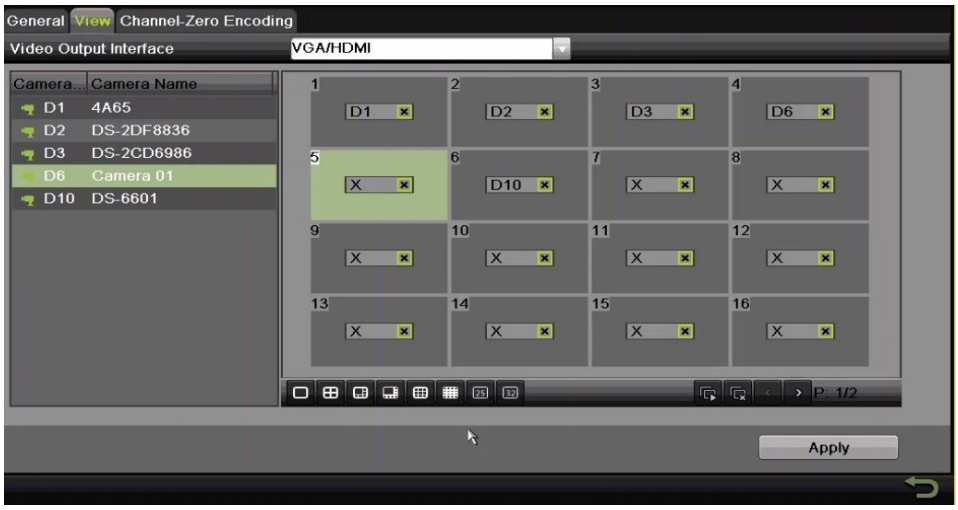


Figure 46 Live View, Camera Order

1) Select a View mode in  , including 1/4/6/8/16/25/32/36/64-window division modes, which are supported depending on model.

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

3) Click  button to start live view for all the channels and click  to stop all live views.

4) Click the Apply button to save the setting.

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

4.6 Channel-Zero Encoding

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

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

Figure 47 Live View, Channel-Zero Encoding

3. Check the Enable Channel Zero Encoding checkbox.
4. Configure the Frame Rate, Max. Bitrate Mode, and Max. Bitrate.
5. After setting Channel-Zero encoding, use the remote client or Web browser to view 16 channels on one screen.

Chapter 5 PTZ Controls

5.1 Configuring PTZ Settings

Follow these procedures to set PTZ parameters. Configure PTZ parameters before you control the PTZ camera.

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

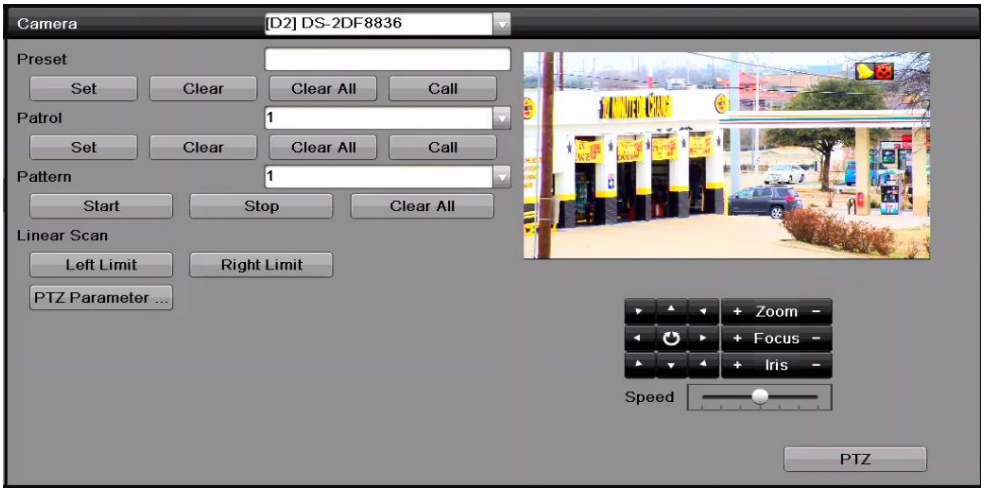


Figure 48 PTZ Settings

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

Figure 49 PTZ, General

3. Choose the camera for PTZ setting in the **Camera** drop-down list.

4. Enter the parameters of the PTZ camera.

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

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

5.2 Setting PTZ Presets, Patrols, and Patterns

5.2.1. Before You Start

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

5.2.2. Customizing Presets

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

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

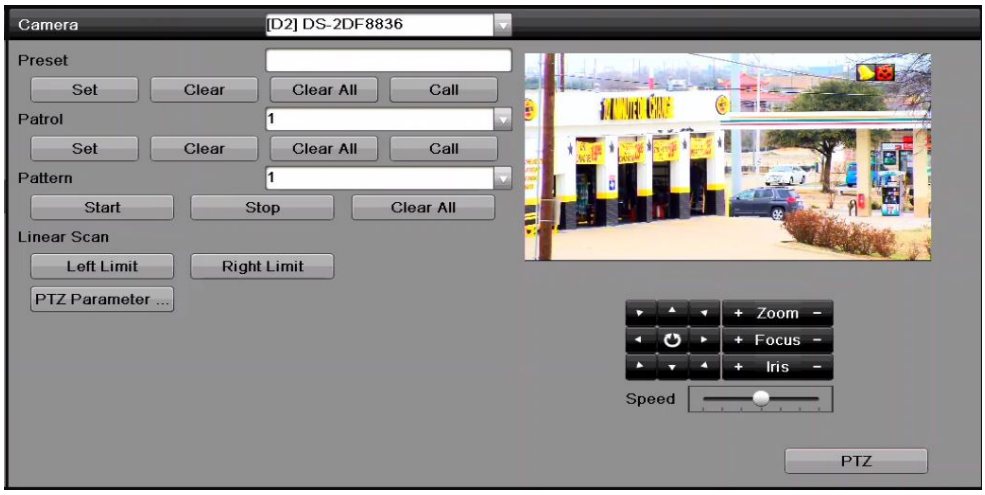


Figure 50 PTZ Settings

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

5.2.3. Calling Presets

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

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

in the right-click menu to show the PTZ control panel.

2. Choose Camera in the drop-down list.

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

Figure 51 PTZ Panel, General

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

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

5.2.4. Customizing Patrols

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

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

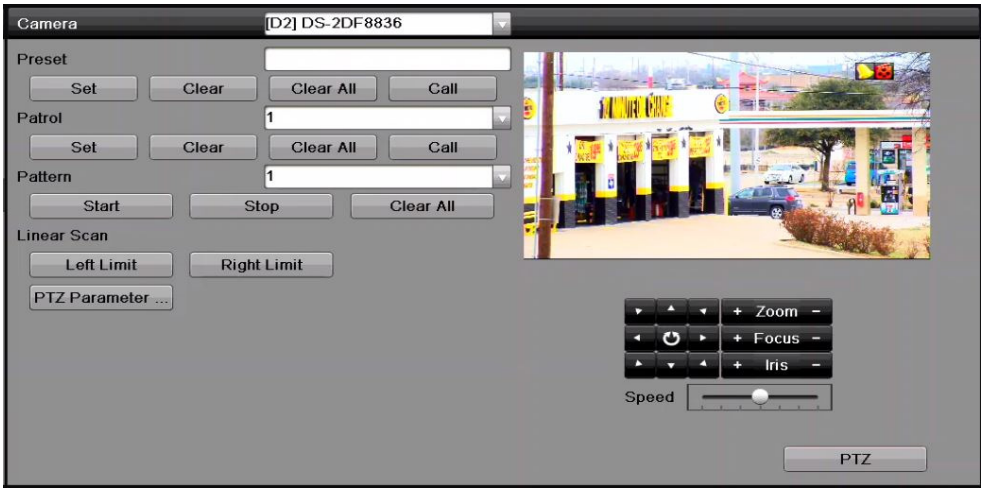


Figure 52 PTZ Settings

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

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

Figure 53 Key Point Configuration

4. Configure key point parameters such as the key point No., key point interval duration, and patrol speed. The key point is corresponding to the preset. **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 the **Add** button to add the next key point to the patrol, or click the **OK** button to save the key point to the patrol.

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

5.2.5. Calling Patrols

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

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

2. Click the ▶ button to show the general settings of the PTZ control.

Figure 54 PTZ Panel, General

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

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

5.2.6. Customizing Patterns

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

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

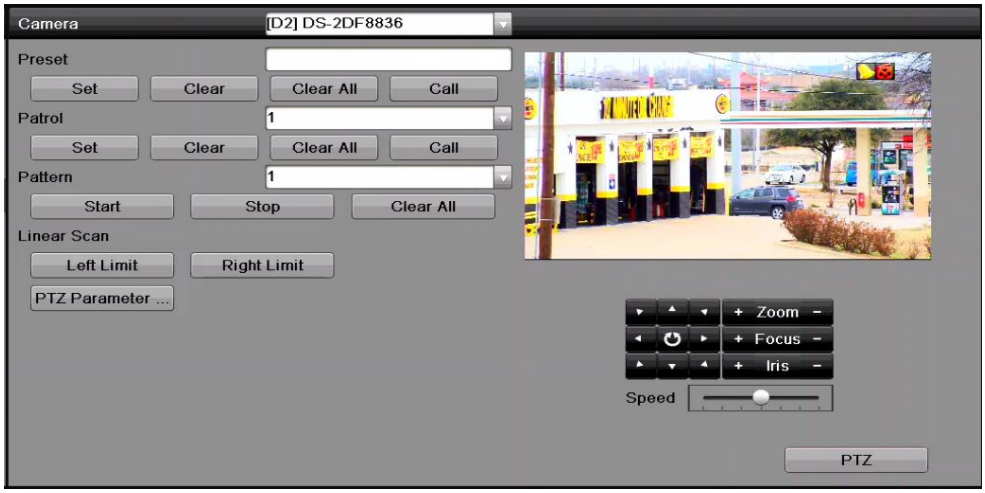


Figure 55 PTZ Settings

2. Choose pattern number in the drop-down list.

3. Click the **Start** button and click corresponding buttons in the control panel to move the PTZ camera, and click the **Stop** button to stop it. The movement of the PTZ is recorded as the pattern.

5.2.7. Calling Patterns

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

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

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

Figure 56 PTZ Panel, General

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

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

5.2.8. Customizing Linear Scan Limit

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

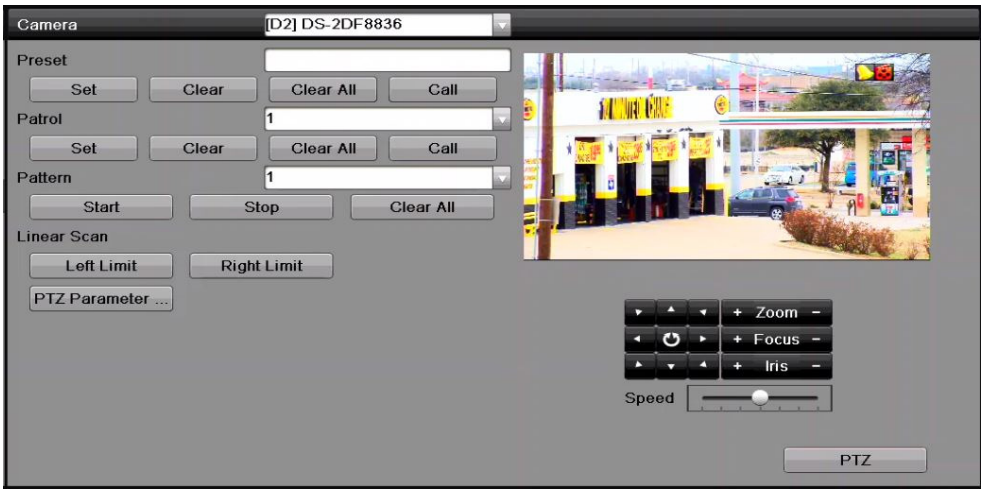


Figure 57 PTZ Settings

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

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

5.2.9. Calling Linear Scan

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

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

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

Figure 58 PTZ Panel, One-Touch

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

5.2.10. One-Touch Park

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

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

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

Figure 59 PTZ Panel, One-Touch

3. Click the corresponding button to activate the park action type.

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

   NOTE: Set park time through the speed dome configuration interface, default is 5s.

4. Click the button again to deactivate it.

5.3 PTZ Control Panel

There are two ways to enter the PTZ control panel.

- **OPTION 1:** In the PTZ settings interface, click the **PTZ** button next to the Back button.
- **OPTION 2:** In the Live View mode, you can press the PTZ Control button on the front panel or on the remote control, or choose the PTZ Control icon  , or select the PTZ option in the right-click menu.

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

   NOTE: In PTZ control mode, the PTZ panel will be displayed when a mouse is connected to the device. If no mouse is connected, the 

icon appears in the lower-left corner of the window, indicating that this camera is in PTZ control mode.

Figure 60 PTZ Panel

Table 15 – Description of the PTZ Panel Icons

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

Chapter 6 Recording and Capture Settings

6.1 Configuring Parameters

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

NOTE: Picture capture is supported by DS-9600/7700NI Series NVRs only.

6.1.1. Before You Start

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

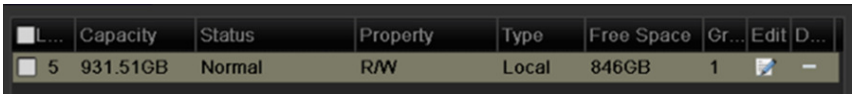


Figure 61 HDD, General

2. Click **Storage Mode** to check the storage mode of the HDD.

   - If the HDD mode is *Quota*, set the maximum record capacity and maximum picture capacity. For detailed information, see *Chapter Configuring Quota Mode.*
   - If the HDD mode is **Group**, set the HDD group. For detailed information, see *Chapter Configuring HDD Group for Recording and Capture.*

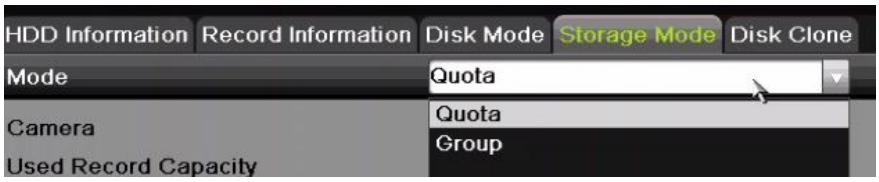


Figure 62 HDD, Advanced

3. Enter the Record settings interface to configure the recording parameters, Menu > Record Configuration > Parameters.

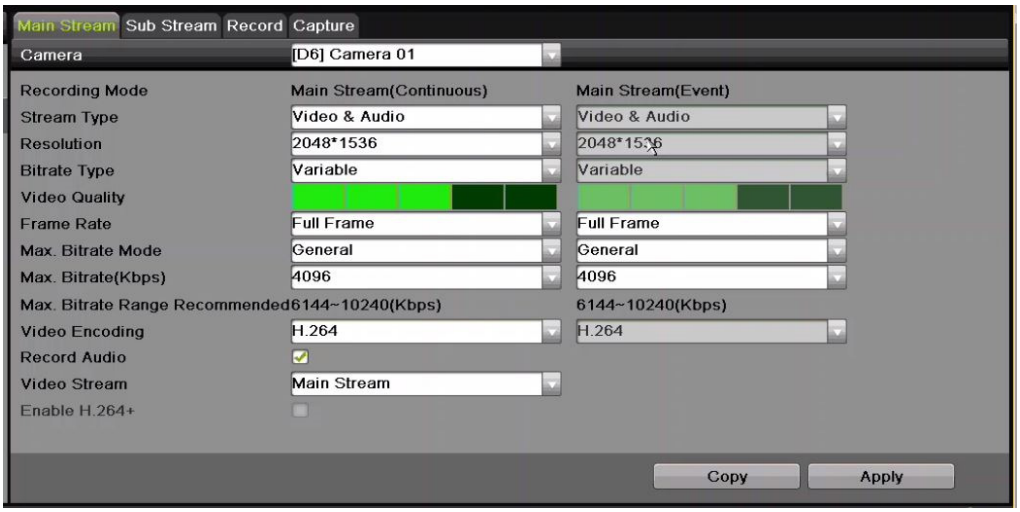


Figure 63 Recording Parameters

4. Select **Main Stream** tab page to configure parameters for recording. You can configure the stream type, the resolution, and other parameters on your demand.

   - **Video Encode**: Select the video encoding, H.265 or H.264.
   - **Enable H.264+ Mode**: Check the checkbox to enable. Once enabled, the **Max. Bitrate Mode**, **Max. Bitrate (Kbps),** and **Max. Bitrate Range Recommend** are not configurable. Enabling it helps to ensure the high video quality with a lowered bitrate.

     NOTE: H.265 and H.264+ should be supported by the connected IP camera.

   - **Record Audio:** Check the checkbox to enable or disable audio recording.
   - **Video Stream:** Main stream and sub-stream are selectable for recording. When you select sub-stream, you can record for a longer time with the same storage space.

5. Click the **Main Stream** button to set the advanced parameters for recording, then click **OK** button.

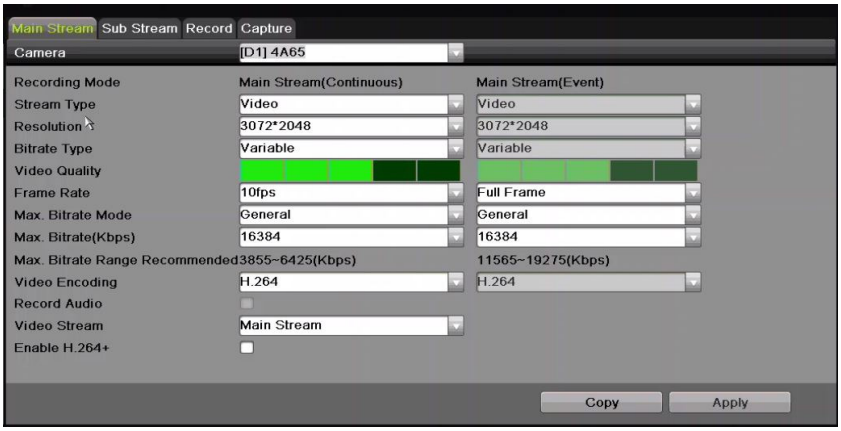


Figure 64 Record Quality

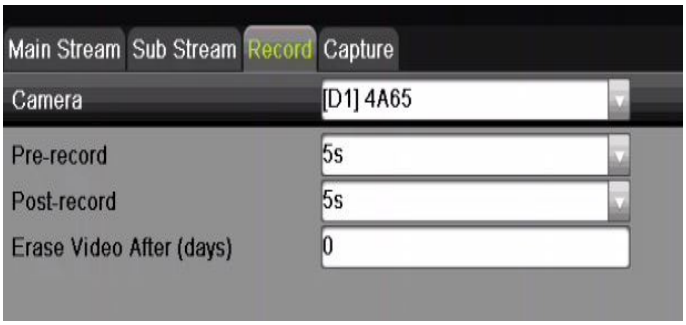


Figure 65 Record Settings

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

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

NOTE: You can enable the ANR (Automatic Network Replenishment) function via the Web browser (Configuration > Storage > Schedule Settings > Advanced) to save the video files

in the IP camera when the network is disconnected, and synchronize the files to the NVR when the network connection has resumed.

Redundant record/capture is used to save the record files or captured pictures in the redundant HDD. You must configure the redundant HDD in HDD settings. For detailed information, see page 75.

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

7. Set sub-stream parameters settings.

   1). Enter the Sub-stream tab page.

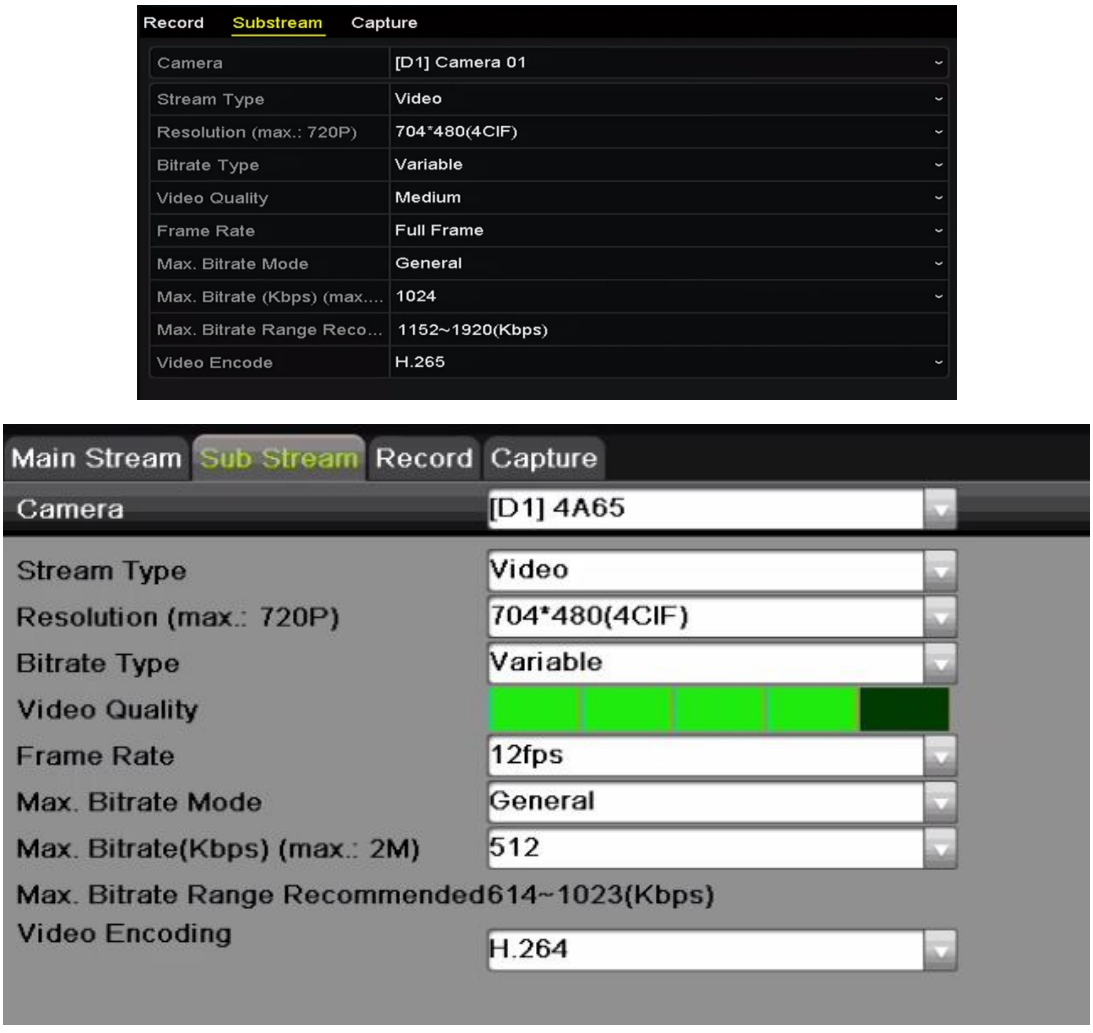


Figure 66 Sub-stream Parameters

   2). Configure the camera parameters.

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

8. Set capture parameters settings.

1). Select the **Capture** tab.

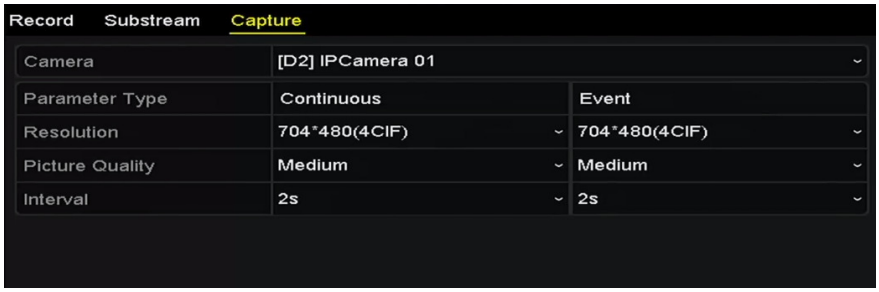


Figure 67 Capture Parameters

2). Configure the parameters.

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

NOTE: Interval is the time period between two capturing actions. You can configure all the parameters on this menu on your demand.

6.2 Configuring Recording and Capture Schedule

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

NOTE: In this section, the record schedule procedure is used as an example, and the same procedure can be applied to configure both recording and capture schedules. To schedule automatic capture, choose the Capture tab in the **Schedule** interface.

1. Enter the Record Schedule interface, Menu > Record Configuration > Schedule.

2. Select Record/Capture Schedule.

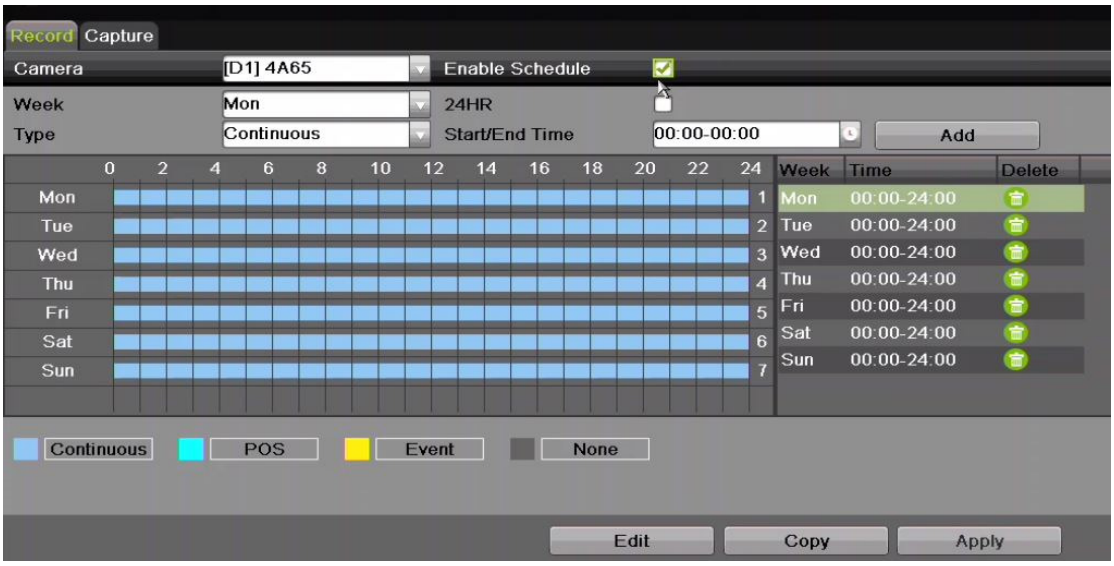


Figure 68 Record Schedule

3. View the different recording types that are marked with different color icons.
   - Continuous: Scheduled recording
   - Event: Recording triggered by all event triggered alarm
   - POS: Recording of POS transactions
4. You can delete the set schedule by clicking the **None** icon.
5. Choose the camera you want to configure.
6. Select the check box after the **Enable Schedule** item.
7. Click **Edit** button or click on the color icon under the edit button and draw the schedule line on the panel.
8. Edit the schedule:
   1). In the message box, choose the day for which you want to set a schedule.

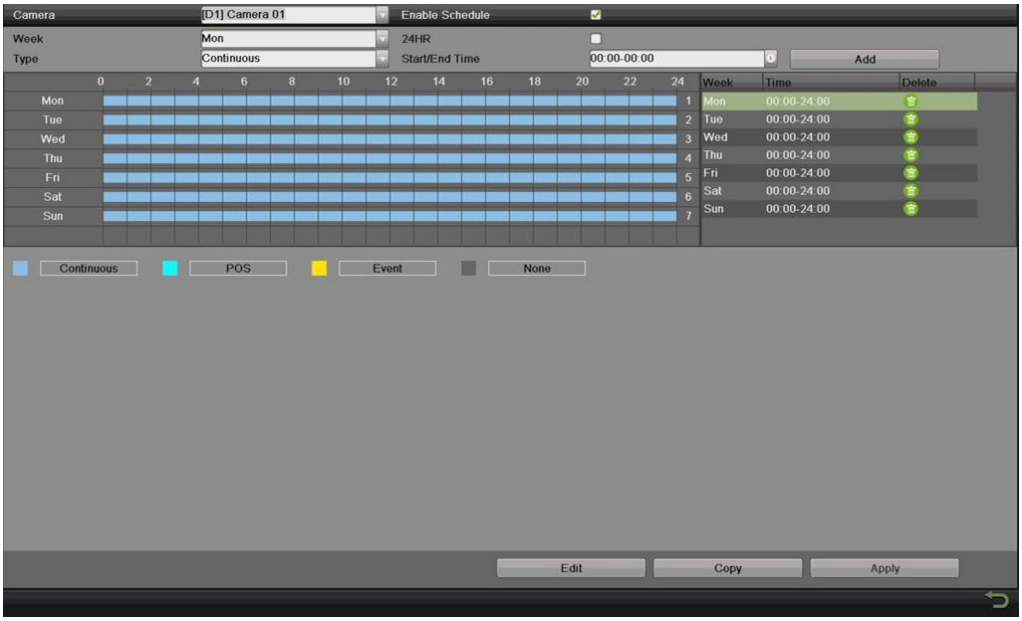


Figure 69 Recording Schedule Interface

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

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

Figure 70 Edit Schedule

4). To arrange another schedule, set the Start/End time for each period.

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

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

NOTE: To enable Event recording (Motion, Alarm, VCA (Video Content Analysis)), you must configure motion, alarm, and VCA to trigger recording. See *Chapter 8.1* and *Chapter 9*. VCA settings are available only to Smart IP cameras

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

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

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

12. Draw the schedule:

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

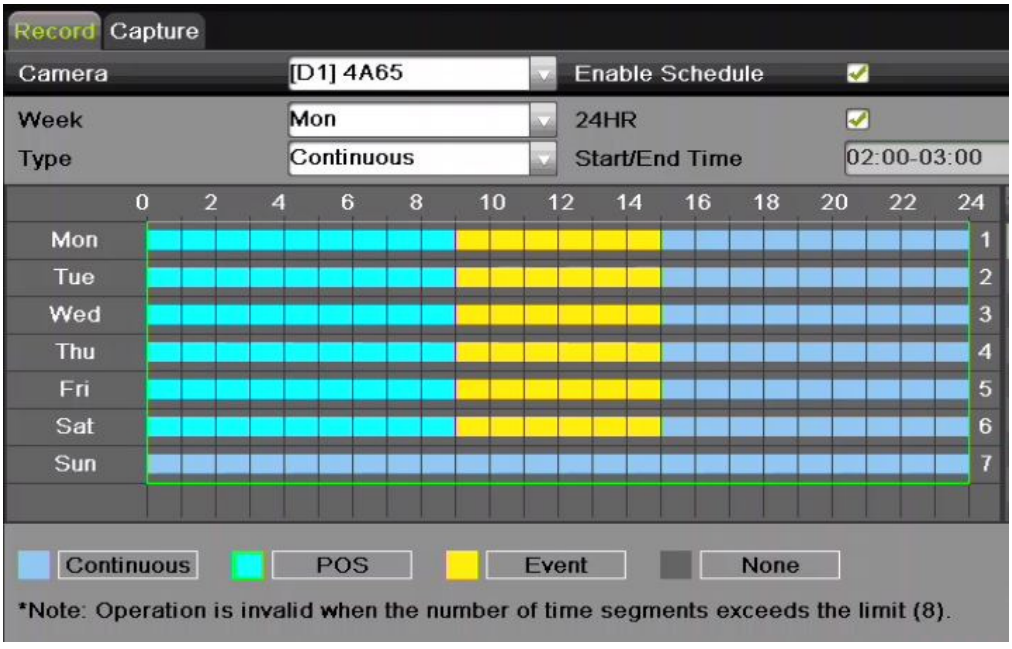


Figure 71 Draw the Schedule

2). Click the Apply button to validate the settings.

13. (Optional) If the settings can also be used for other channels, click **Copy**, then choose the channel to which you want to copy.

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

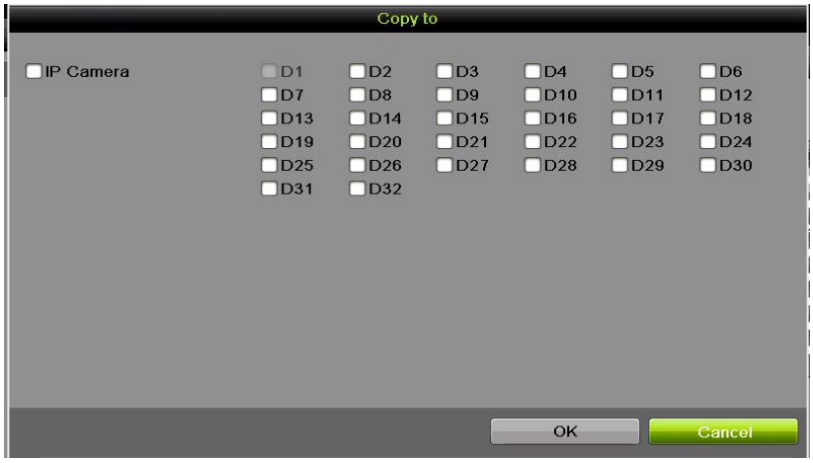


Figure 72 Copy Schedule to Other Channels

6.3 Configuring Motion Detection Recording and Capture

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

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

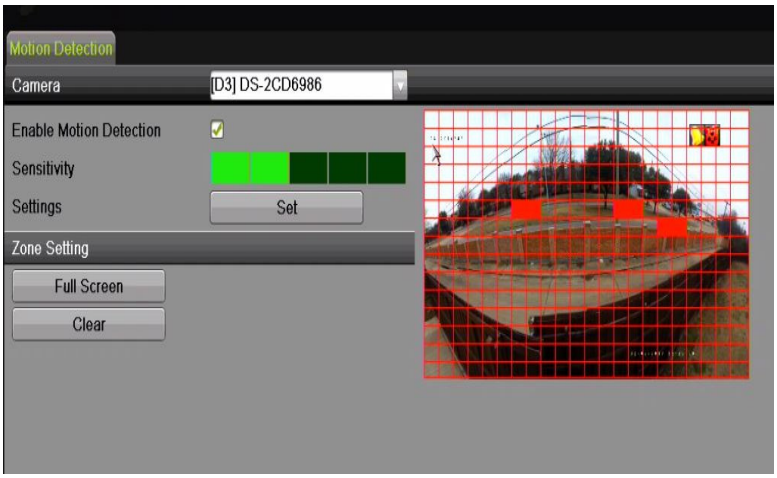


Figure 73 Motion Detection

2. Choose camera you want to configure.
3. Check the Enable Motion Detection checkbox.
4. Drag and draw the area for motion detection with the mouse. If you want to set motion detection for the entire area shot by the camera, click **Full Screen**. To clear the motion detection area, click **Clear**.
5. Click **Settings**, and the message box for channel information pops up.

Figure 74 Motion Detection Handling

6. Select the channels that you want the motion detection event to trigger recording.
7. Click **Apply** to save the settings.
8. Click **OK** to go back to the upper level menu.
9. Exit the Motion Detection menu.
10. Edit the Motion Detection Record Schedule. For the detailed information of schedule configuration, see *Configuring Recording and Capture Schedule.*

6.4 Configuring Alarm Triggered Recording and Capture

Follow the procedure below to configure alarm triggered recording or capture.

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

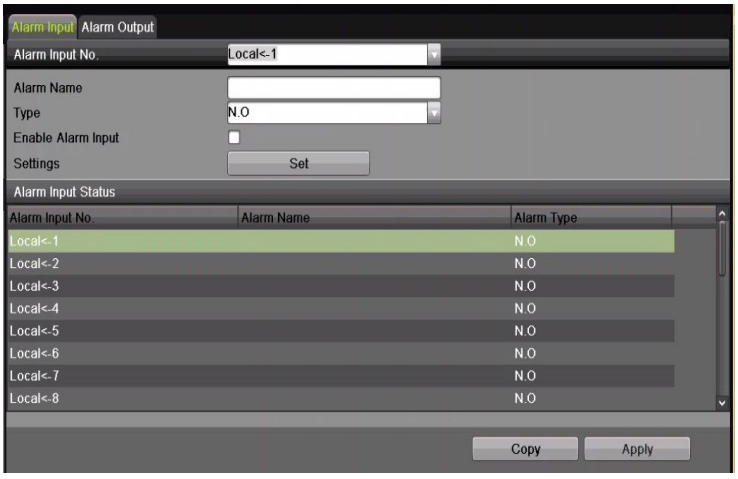


Figure 75 Alarm Settings

2. Click Alarm Input.

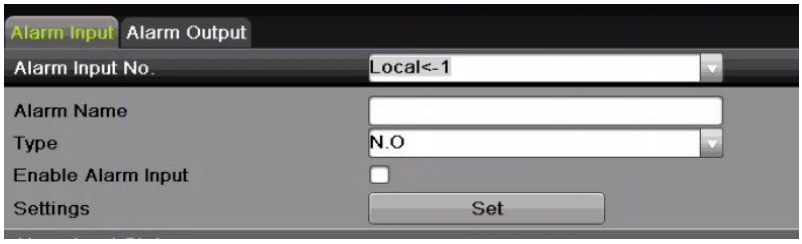


Figure 76 Alarm Settings, Alarm Input

3. Select Alarm Input number and configure alarm parameters.
4. Choose N.O. (normally open) or N.C. (normally closed) alarm type.
5. Check the Setting ☑ checkbox.

Figure 77 Alarm Settings

6. Click **Set**.
7. Choose the alarm triggered recording channel.
8. Check the checkbox ☑ to select channel.
9. Click **Apply** to save settings.
10. Click **OK** to go back to the upper level menu.
11. Repeat the above steps to configure other alarm input parameters.
12. If the settings can also be applied to other alarm inputs, click **Copy** and choose the alarm input number.

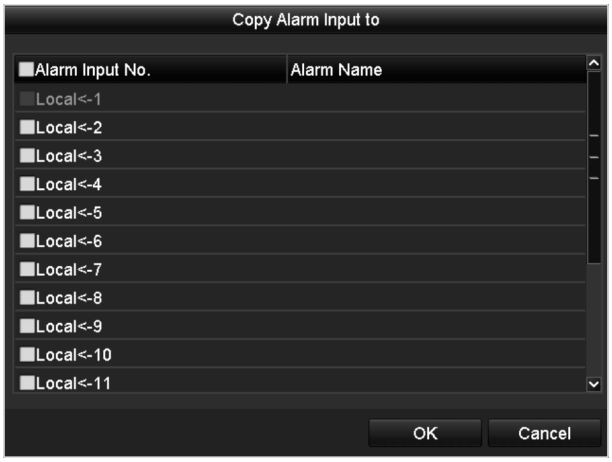


Figure 78 Copy Alarm Input

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

6.5 Configuring Holiday Recording and Capture

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

1. Enter the Record setting interface, Menu > Recording Configuration > Holiday.

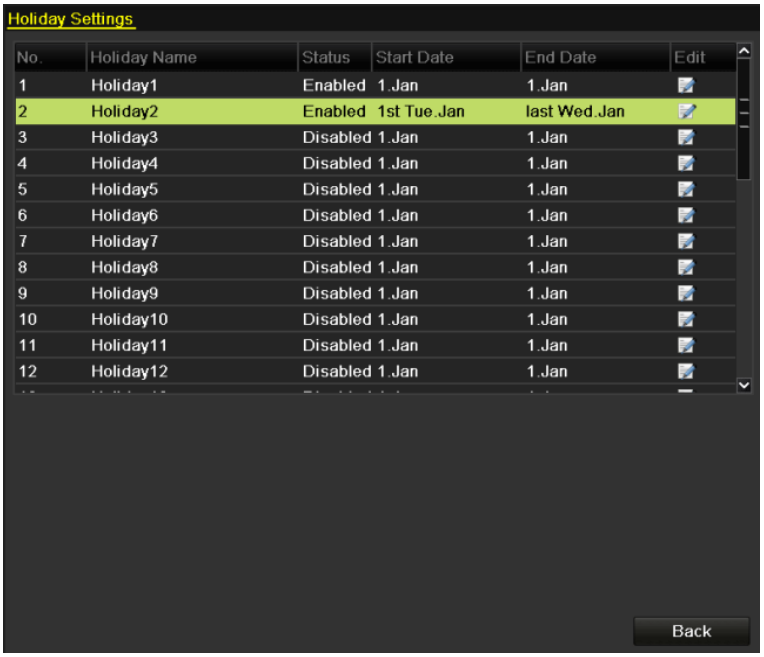


Figure 79 Holiday Settings

2. Click  to enter the Edit interface.

Figure 80 Edit Holiday Settings

3. Check the Enable Holiday checkbox.
4. Select Mode from the drop-down list.
5. Set the start and end dates.
6. Click Apply to save settings.
7. Click OK to exit the Edit interface.
8. Enter the Record/Capture Schedule settings interface to edit the holiday recording schedule. See Chapter 6.2 *Configuring Recording and Capture Schedule*.

6.6 Configuring Redundant Recording and Capture

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

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

   NOTE: You must set the Storage mode in the HDD advanced settings to Group before you set the HDD property to Redundant. See *Chapter 11.4.1*

Setting HDD Property. There should be at least another HDD that is in Read/Write status.

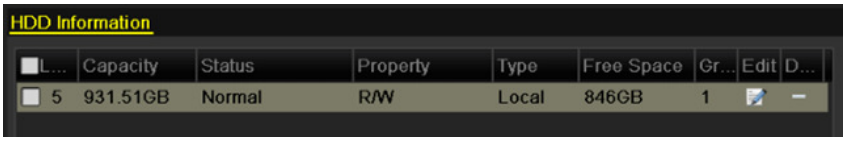


Figure 81 HDD General

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

3. Set the HDD property to Redundancy.

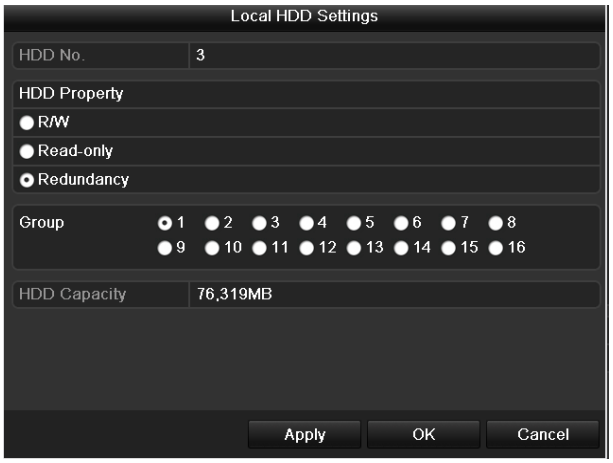


Figure 82 HDD General-Editing

4. Click Apply to save the settings.

5. Click OK to go back to the upper level menu.

NOTE: You must set the Storage mode in the HDD advanced settings to Group before you set the HDD property to Redundant. See *Chapter 11.4.1*

Setting HDD Property. There should be at least another HDD that is in Read/Write status.

6. Enter the Record setting interface, Menu > Recording Configuration > Parameters

7. Select Record tab.

8. Click More Settings to enter the following interface.

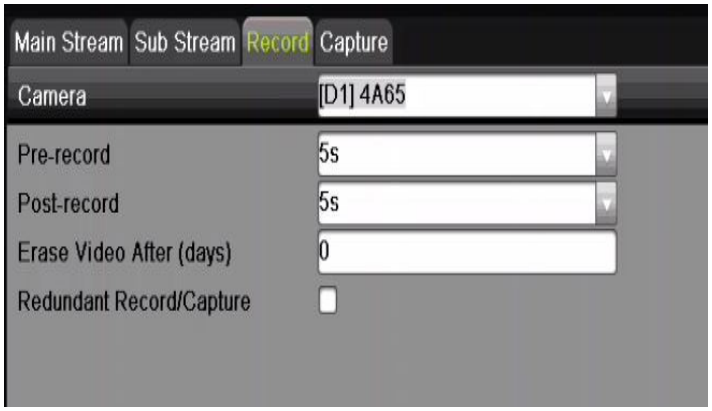


Figure 83 Record Parameters

9. Select the camera you want to configure in the drop-down list.
10. Check the Redundant Record/Capture checkbox.
11. Click OK to save settings and to back to the upper level menu.
12. Repeat the above steps to configure other channels.

6.7 Configuring HDD Group for Recording and Capture

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

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

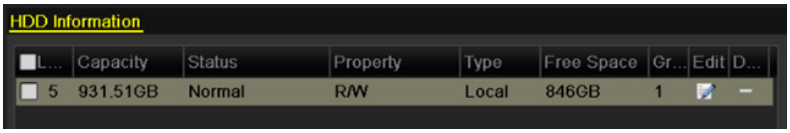


Figure 84 HDD General

2. Select Advanced on the left side menu.

Figure 85 Storage Mode

3. Check whether the HDD storage mode is Group. If not, set it to Group. See Chapter *Managing HDD Group*.
4. Select General in the left side menu.
5. Click  to enter the editing interface.
6. Configure HDD group.
    1). Choose a group number for the HDD group.
    2). Click Apply and then, in the pop-up message box, click Yes to save your settings.
    3). Click OK to go back to the upper level menu.
    4). Repeat the above steps to configure more HDD groups.
7. Choose the Channels of which you want to save the record files and captured pictures in the HDD group.
    1). Select Advanced on the left bar.

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

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

4). Click Apply to save settings.

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

6.8 Files Protection

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

6.8.1. Locking the Recording Files

6.8.1.1 Lock File During Playback

1. Enter Playback interface, Menu > Playback

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

Figure 86 Normal Playback

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

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

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

Figure 87 Locked File Management

5. In the File Management interface, you can also click to change it to to unlock the file; the file will not be protected.

6.8.1.2 Lock File When Exporting

1. Enter Export setting interface, Menu > File Management.

Figure 88 Export

2. Select the channels you want to search by checking their checkboxes.

3. Configure the record type, file type, and start/end times.

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

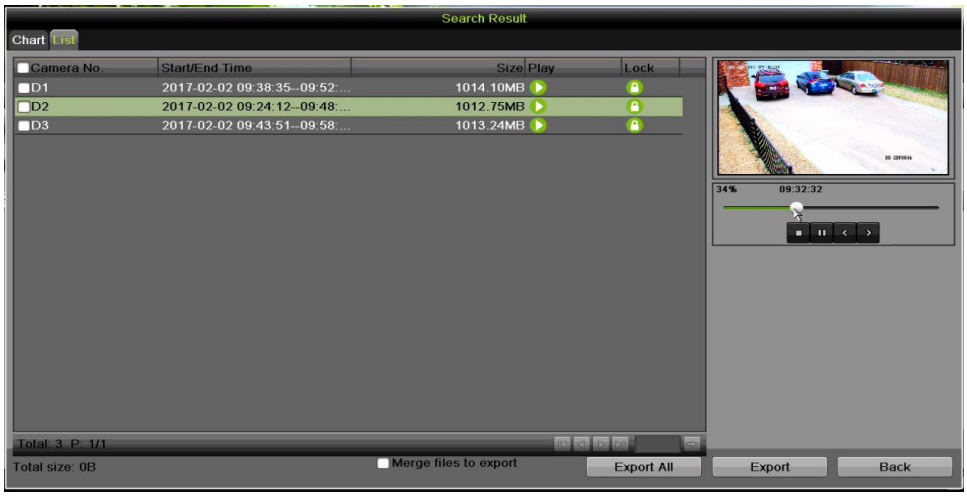


Figure 89 Export, Search Result

5. Protect the record files.

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

NOTE: The record files still recording cannot be locked.

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

Figure 90 Unlocking Attention

6.8.2. Setting HDD Property to Read-Only

1. Enter HDD setting interface, Menu > HDD.

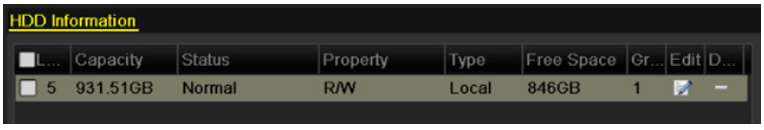


Figure 91 HDD General

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

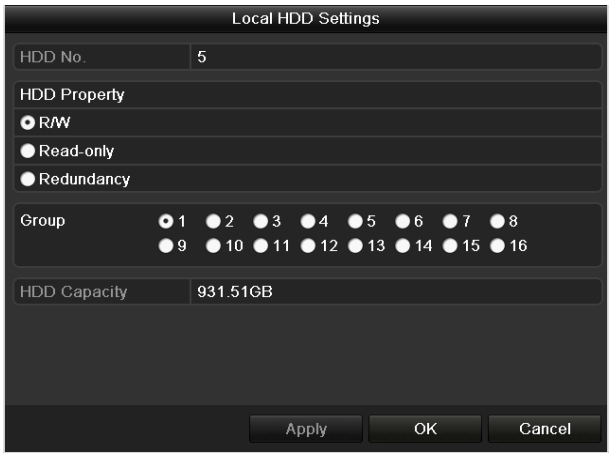


Figure 92 HDD General, Editing

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

3. Set the HDD property to Read-only.

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

NOTES: You cannot save any 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 NVR can't record any files. Only live view mode is available.

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

Chapter 7 Playback

7.1 Playing Back Record Files

7.1.1. Instant Playback

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

7.1.1.1 Instant Playback by Channel

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

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

Figure 93 Instant Playback Interface

7.1.2. Playing Back by Normal Search

7.1.2.1 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 in Figure 94.

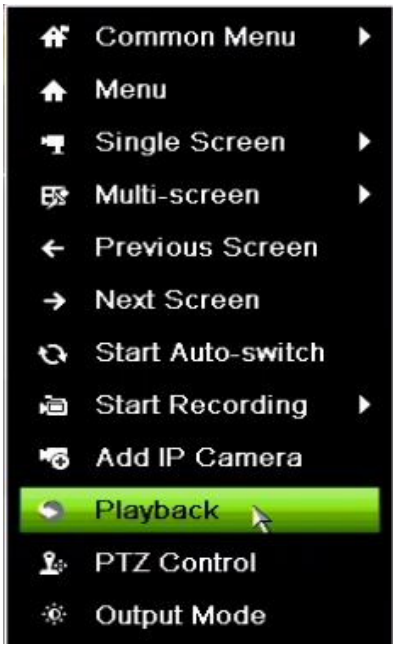


Figure 94 Right-Click Menu Under Live View

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

7.1.2.2 Playback by Time

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

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

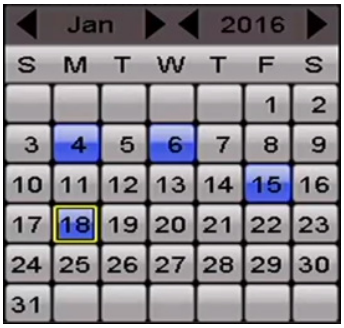


Figure 95 Playback Calendar

3. If there are record files for that camera on that day in the calendar, the icon for that day is displayed as 18. Otherwise it is displayed as 18.

7.1.2.3 Playback Interface

You can use the toolbar in the bottom part of the Playback interface to control playing progress, as shown in Figure 96.

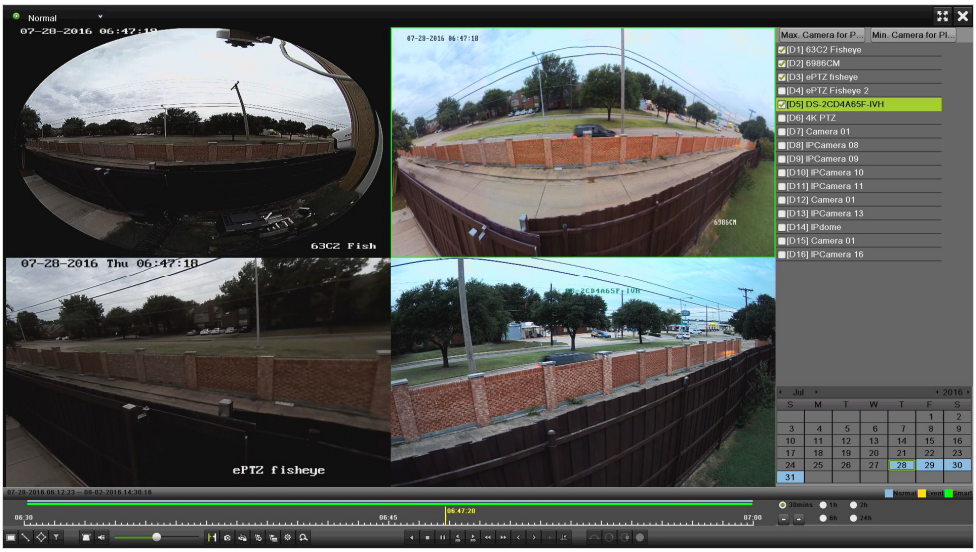


Figure 96 Playback Interface

1. Click the channel(s) to execute simultaneous playback of multiple channels.

Figure 97 Playback Toolbar

NOTE: The 03-22-2016 17:24:02 -- 01-18-2016 11:36:12 indicates the start/end time of the recorded video files.

The ▬ indicates the smart playback time bar and the ▬ indicates the normal playback time bar.

Playback progress bar: use the mouse to click any point of the progress bar to display a thumbnail. Click on the thumbnail to jump to that period. You can also drag the progress bar to locate specific frames.

Table 16 – Detailed Explanation of Playback Toolbar

Item	Button	Operation	Button	Operation
Smart Search		Set full screen for motion detection		Draw line for the line crossing detection
		Draw quadrilateral for the intrusion detection		Filter video files by setting the target characters
Operations		Audio on/Mute		Start/Stop clipping
		Capture Picture		Lock File
		Add default tag		Add customized tag
		File management for video clips, captured pictures, locked files and tags		Digital Zoom
Playing Control		Pause/Play		Reverse play/Pause
		Slow forward		Stop
		30s forward		30s reverse
		Next day		Fast forward
		Previous day		
Time Bar Scaling		Previous/Next period	30mins	Play the time bar in 30 minute periods (default)
	1h	Play the time bar in 1 hour periods	2h	Play the time bar in 2 hour periods
	6h	Play the time bar in 6 hour periods	24h	Play the time bar in 24 hour periods
Fisheye Expansion		180° panorama		360° panorama
		PTZ expansion		Fisheye

NOTES: Refer to *Chapter 3.2.5 Fisheye Expansion* for the description and operation of the fisheye expansion.

256x playing speed is supported.

7.1.3. Playing Back Using Smart Playback

An easy way to bypass less relevant information, Smart Playback mode analyzes the video containing motion or VCA information, marks it in green, and plays it at normal speed while video without motion plays at 16x speed. Smart Playback rules and areas are configurable.

NOTE: Volume control, capture, setting tag, digital zoom, reverse playback, fast forward, and fast reverse are not supported during smart playback.

7.1.3.1 Before You Start

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

1. Log into the IP camera through a Web browser.

2. Enable intrusion detection by checking the checkbox.

3. Enter the motion detection configuration interface, Configuration > Advanced Configuration > Events > Intrusion Detection.

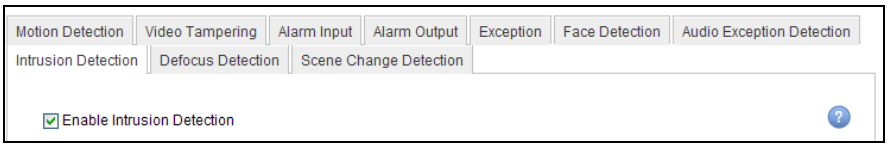


Figure 98 Setting Intrusion Detection on IP Camera

7.1.3.2 Configure Intrusion Detection

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. Enter Playback interface, Menu > Playback.

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

3. Select a camera in the camera list.

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

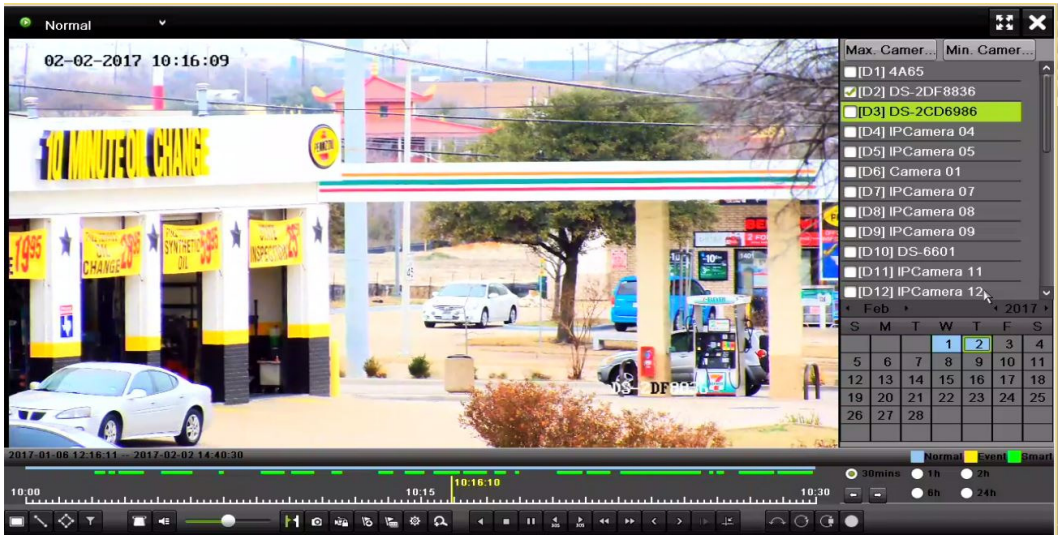


Figure 99 Playback by Smart Search

5. Click the status bar to switch to the playback by Smart Search interface.

6. Set the Smart Search rules and areas for line crossing detection, intrusion detection, or motion detection event triggered recording.

- **Full Screen Motion/Intrusion Detection —** Click to set the full screen as the detection area.
- **Line Crossing Detection —** Select the button, and click on the image to specify the start point and end point of the line.
- **Intrusion Detection —** Click the button, and specify four points to set a quadrilateral region for intrusion detection. Only one region can be set.
- **Motion Detection —** Click the button and then click and drag the mouse to set the detection area manually. You can also click the button to set the full screen as the detection area.

7. Click to search and play the matched video files.
8. (Optional) Click to filter the searched video files by setting the target characters, including the gender and age of the human and whether he/she wears glasses.

Figure 100 Set Result Filter

7.1.4. Playing Back by Event Search

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

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

NOTE: Playback by VCA is used as the example in the following instructions.

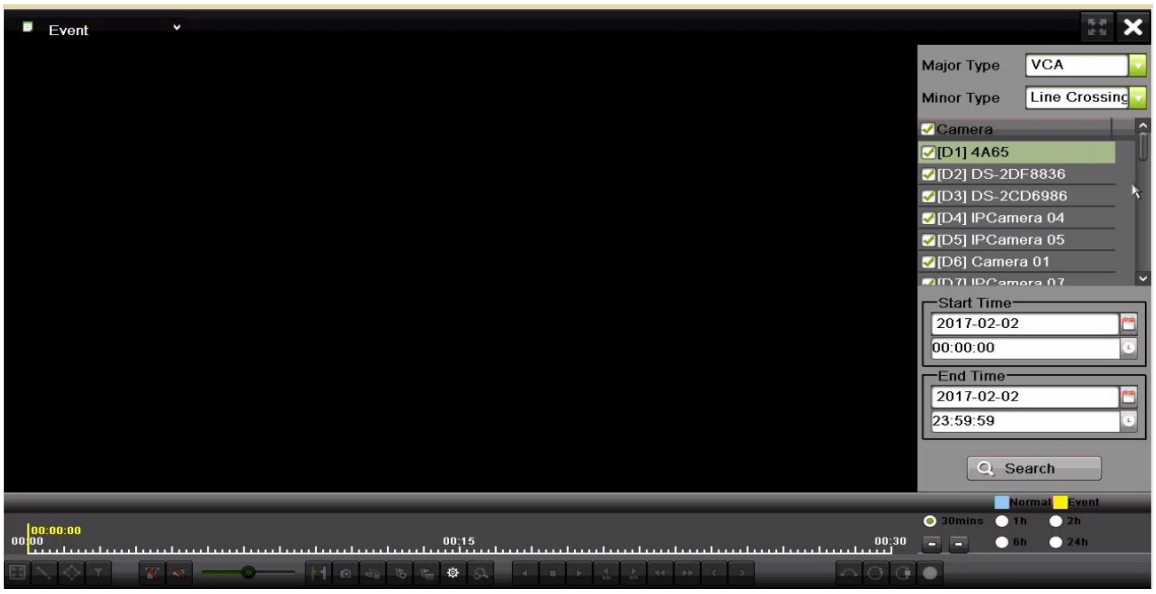


Figure 101 Event Search Interface

4. Select the minor type of VCA from the drop-down list. (Please refer to *Chapter 9 VCA Alarm* for the details of VCA detection types).

   NOTE: For configuring the VCA recording, refer to *Chapter 5.4 Configuring VCA Event Recording and Capture*; and for details of VCA detection types, refer to *Chapter 9 VCA Alarm*.

5. Select the camera(s) for searching, and set the Start time and End time.

6. Click **Search** button to get the search result information. Refer to the right-side bar for the results.

7. Select a result item and click the button to play back the file.

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

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

Figure 102 Synch Playback Interface

9. Enter the playback interface.

10. Use the toolbar in the bottom section of the playback interface to control the playing process.

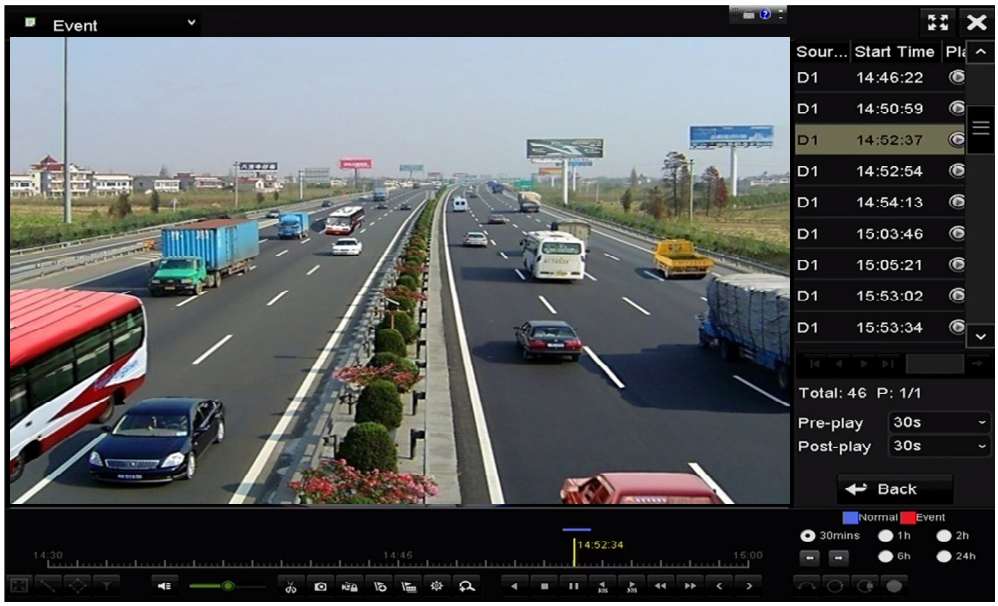


Figure 103 Interface of Playback by Event

11. Click ‹ or › button to select the previous or next event. Refer to Table 6.1 for description of toolbar buttons.

7.1.5. Video Tags

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

7.1.5.1 Before Playing Back by Tag

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

Figure 104 Interface of Playback by Time

3. Click button to add default tag.

4. Click button to add customized tag and input tag name.

NOTE: Maximum of 64 tags can be added to a single video file.

7.1.5.2 Tag Management

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

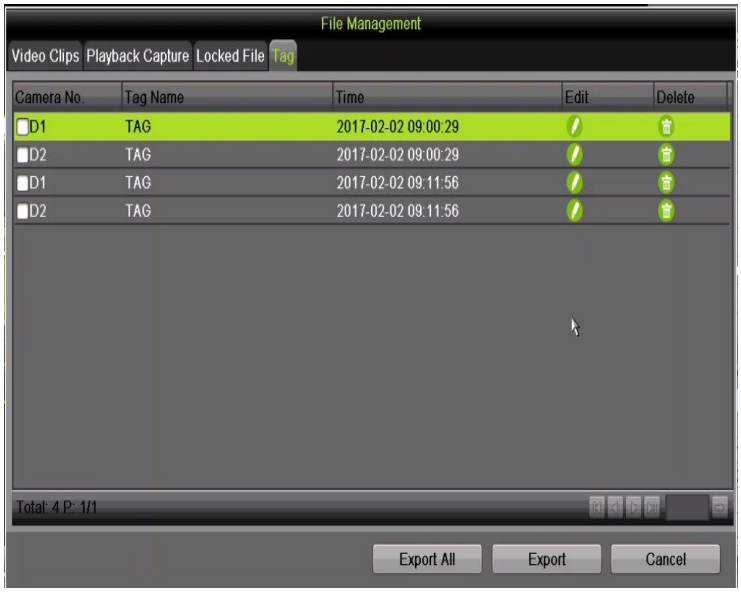


Figure 105 Tag Management Interface

7.1.6. Playing Back by Tag

1. Select the **Tag** from the drop-down list in the Playback interface.

2. Choose channels, edit start time and end time, and then click **Search** to enter the Search Result interface.

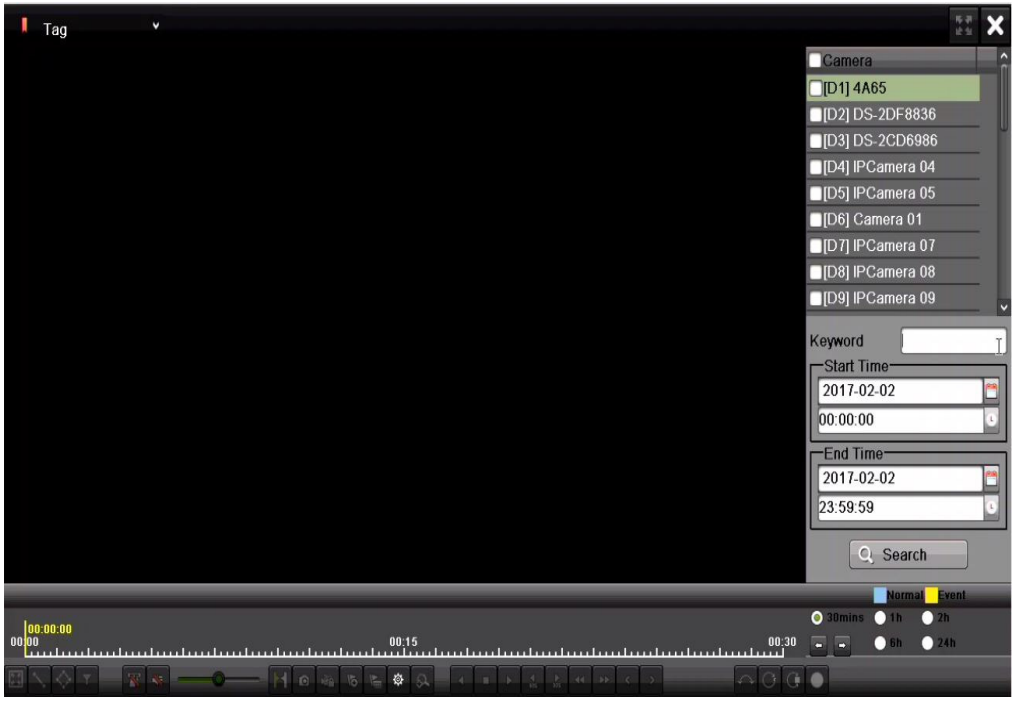


Figure 106 Playback by Tag Interface

NOTE: Enter keyword in the text box 

to search for tags on your command.

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

4. Click the **Back** button to back to the search interface.

Figure 107 Playback by Tag Interface

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

5. Click ◀ or ▶ button to select the previous or next tag. Refer to Table 6.1 for description of toolbar buttons.

7.1.7. Playing Back by Sub-Periods

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

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

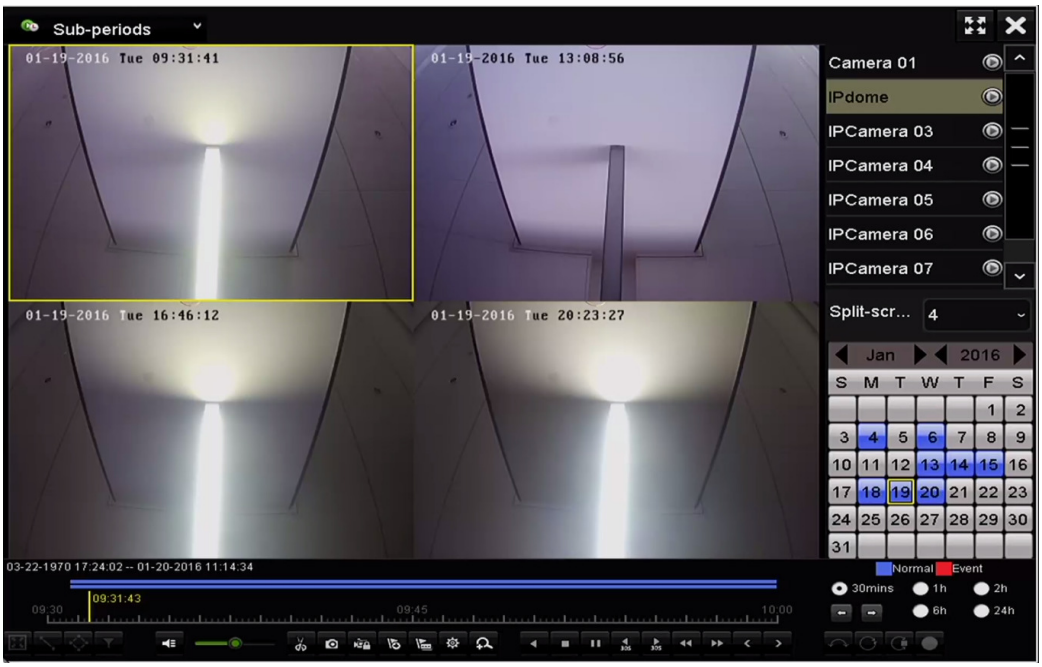


Figure 108 Sub-Periods Playback Interface

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

7.1.8. Playing Back by System Logs

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

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

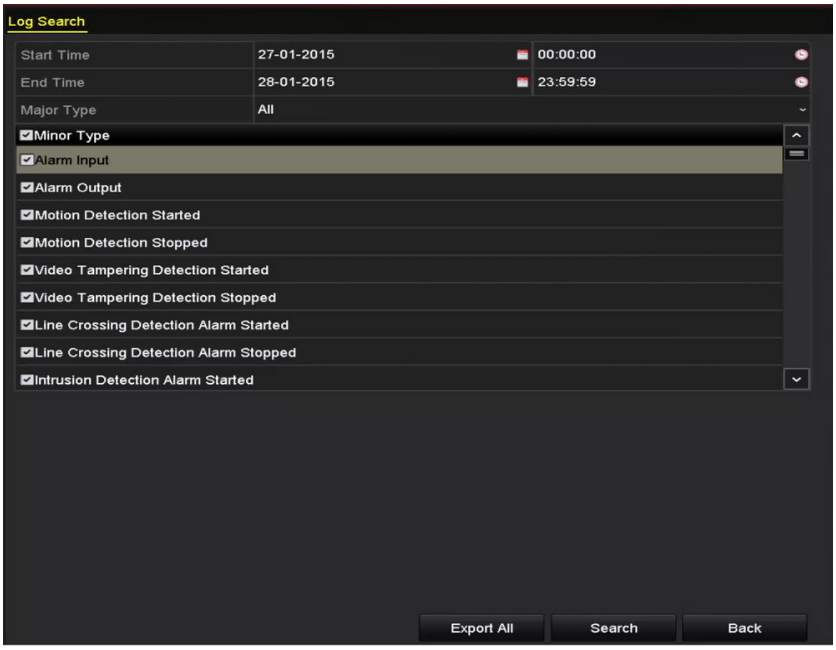


Figure 109 System Log Search Interface

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

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

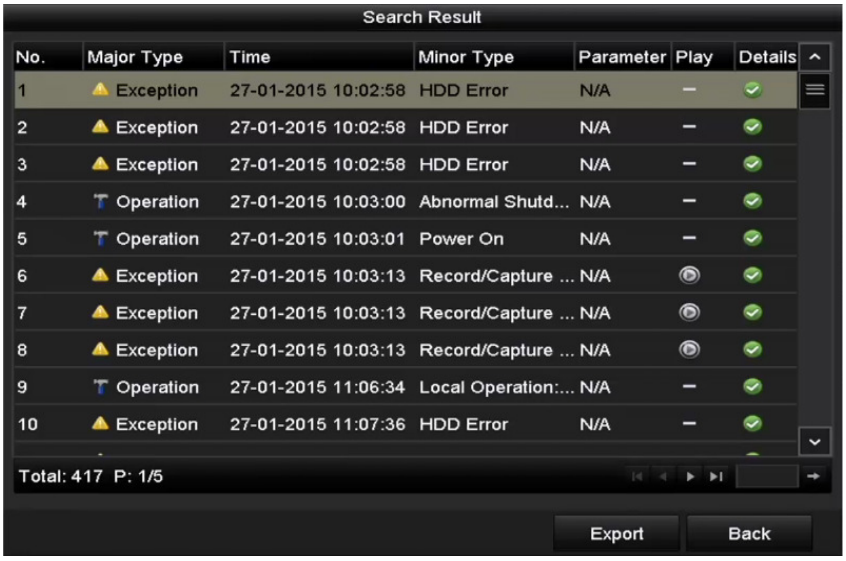


Figure 110 Result of System Log Search

7.1.9. Playback Interface

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

Figure 111 Playback by Log Interface

7.1.9.1 Playing Back External Files

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

1. Enter Tag Search interface, Menu > Playback.
2. Select the **External File** in the drop-down list on the top-left side. The files are listed on the right-side list.
3. Click the Refresh button to refresh the file list.
4. Select a file and click the button to play it. Adjust playback speed by clicking and .

Figure 112 External File Playback Interface

7.1.9.2 Playing Back Pictures

Captured pictures stored in the device's HDDs can be searched and viewed.

1. Enter Playback interface, Menu > Playback.
2. Select **Picture** from the drop-down list in the upper-left corner of the page to enter the Picture Playback interface.
3. Check ☑ checkbox to select channel(s) and specify search start time and end time.
4. Click **Search** to enter Search Result interface.

   NOTE: Up to 4,000 pictures can be displayed each time.
5. Choose a picture you want to view and click the ⏵ button.
6. Click **Back** to return to the search interface.

Figure 113 Picture Playback Result

7. Use the toolbar in the bottom section of the Playback interface to control playback.

Figure 114 Picture Playback Toolbar

Table 17 – Detailed Explanation of Picture-Playback Toolbar

Button	Function	Button	Function	Button	Function	Button	Function
	Play reverse		Play		Previous picture		Next picture

7.2 Playback Auxiliary Functions

7.2.1. Playing Back Frame-by-Frame

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

7.2.1.1 Using a Mouse

1. Go to Playback interface.
2. If you choose playback of the record file: click  button until the speed changes to single frame. One click on the playback screen will play back one frame.
3. If you choose reverse playback of the record file: click  button until the speed changes to single frame. One click on the playback screen will reverse play back one frame. It is also possible to use the  button in the toolbar.

NOTE: You can also advance/reverse single frames by using the mouse wheel.

7.2.1.2 Using the Front Panel

1. Click the  button to set the speed to single frame. One click on the  button, or one click on the playback screen or Enter button on the front panel, will play back or reverse play back one frame.

7.2.2. Thumbnails View

Use the playback interface thumbnail views to locate the required video files on the time bar.

NOTE: This feature is supported by cameras of 6 MP or less.

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

Figure 115 Thumbnails View

2. Move the mouse to the time bar to show the video file preview thumbnails. Select and double click on a thumbnail to enter full-screen playback.

NOTE: Thumbnail view is supported only in 1x single-camera playback mode.

7.2.3. Fast View

Use the mouse to drag on the time bar for a fast view of the video files.

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

Figure 116 Playback Interface

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

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

7.2.4. Digital Zoom

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

Figure 117 Digital Zoom Draw Area

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

7.2.5. File Management

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

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

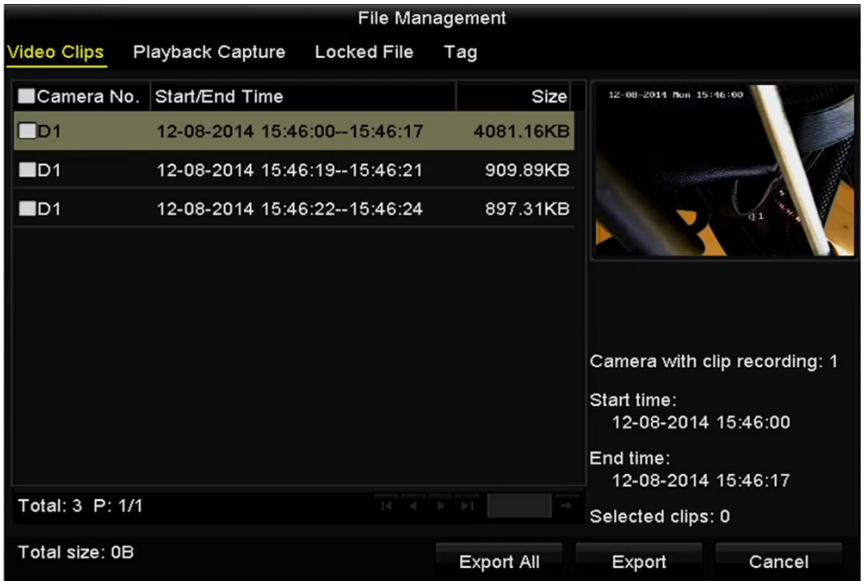


Figure 118 File Management

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

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

Chapter 8 Backup

8.1 Backing Up Record Files

8.1.1. Quick Export

Export record files to backup device(s) quickly.

1. Enter Video Export interface, Menu > File Management.
2. Choose the channel(s) you want to back up.

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

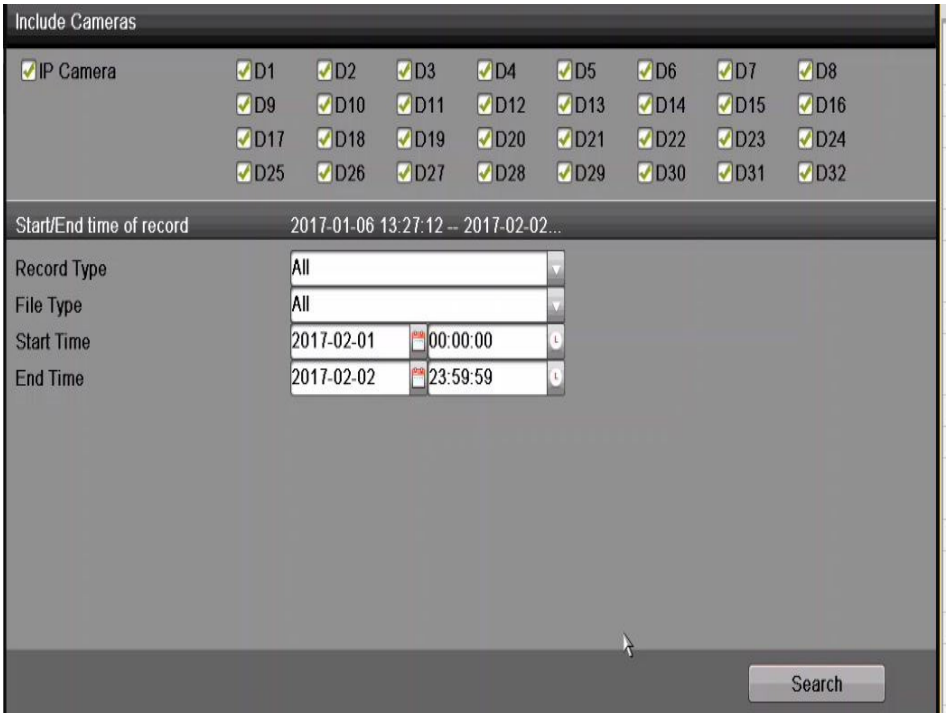


Figure 119 Export Interface

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

NOTE: This example uses a USB flash drive. Refer to the next section, *Normal Backup*, for more backup devices supported by the NVR.

Figure 120 Quick Export Using USB

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

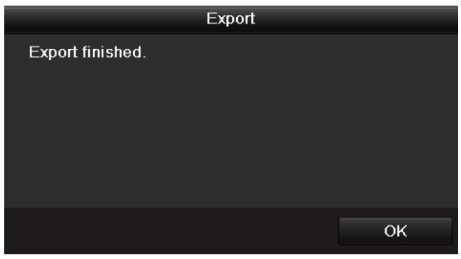


Figure 121 Export Finished

6. Check backup result.

7. Choose the record file in Export interface and click the button to check it.

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

Figure 122 Checkup of Quick Export Result Using USB

8.1.2. Backing Up by Normal Video/Picture Search

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

NOTE: eSATA HDD is supported by DS-9600NI-I8 Series NVRs only.

8.1.2.1 Backup Using USB Flash Drives and USB HDDs

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

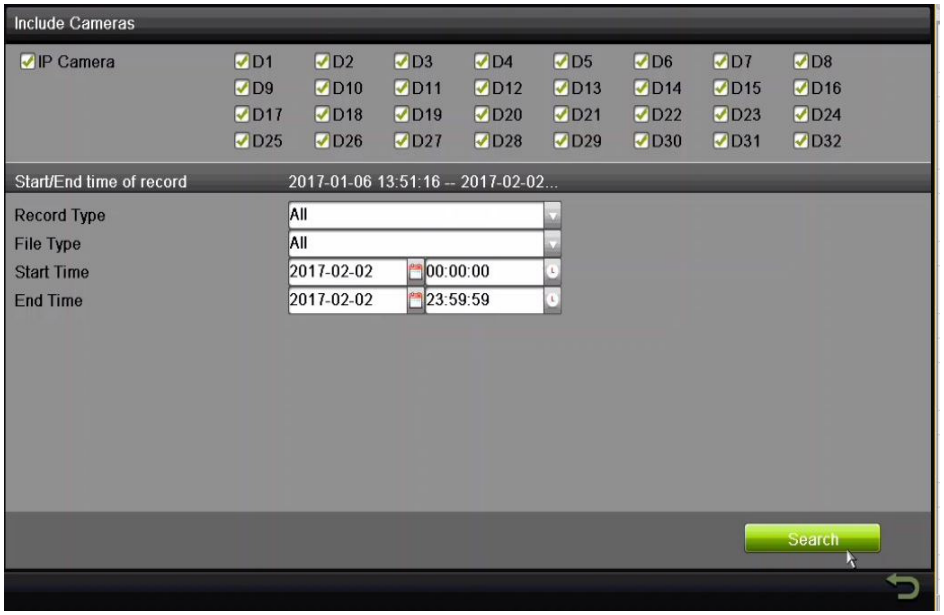


Figure 123 Normal Video Search for Backup

4. Select video files or pictures from the Chart or List to export.
5. Click to play the record file if you want to check it.
6. Check the checkbox next to the record files you want to back up.

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

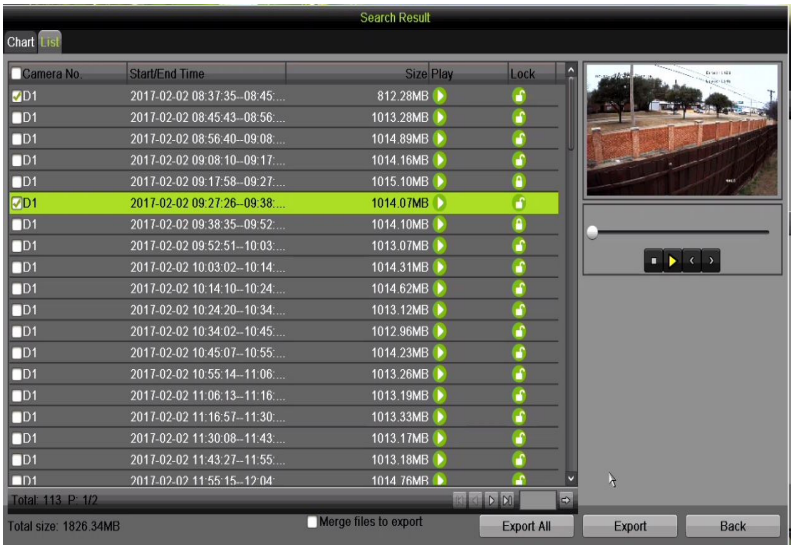


Figure 124 Result of Normal Video Search for Backup

7. Export the video files or picture files.

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

9. If the inserted USB device is not recognized:

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

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

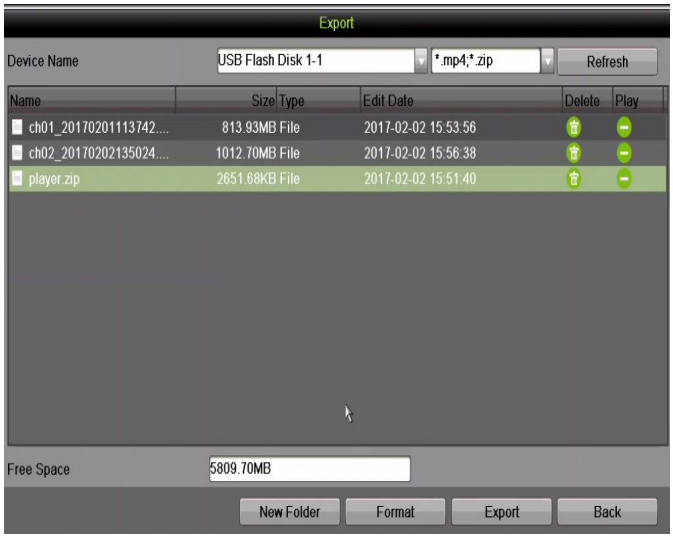


Figure 125 Export by Normal Video Search Using USB Flash Drive

10. Stay in the Exporting interface until all record files are exported and the “Export finished” pop-up message box appears.

Figure 126 Export Finished

NOTE: Backing up video files using a USB writer or SATA writer has the same operating instructions. Please refer to steps described above.

8.1.3. Backing Up by Event Search

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

1. Enter Export interface, Menu > File Management > Event.
2. Select the cameras to search.
3. Select the event type from the drop-down menu: alarm input, motion, POS, or VCA.

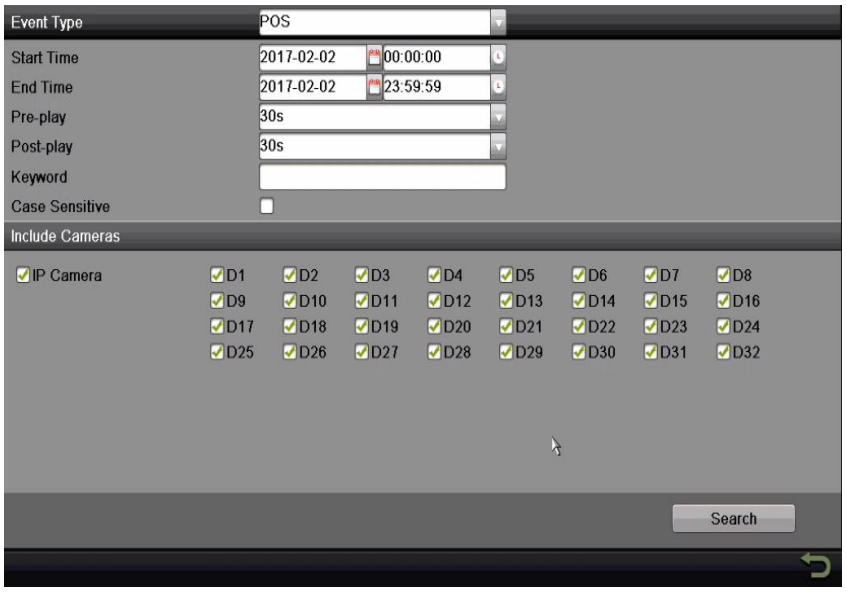


Figure 127 Event Search for Backup

4. Set search condition and click the **Search** button to enter the search result interface. The matched

video files are displayed in Chart or List display mode.

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

   NOTE: Check **Merge Files to Export** checkbox to combine the selected files when exporting.

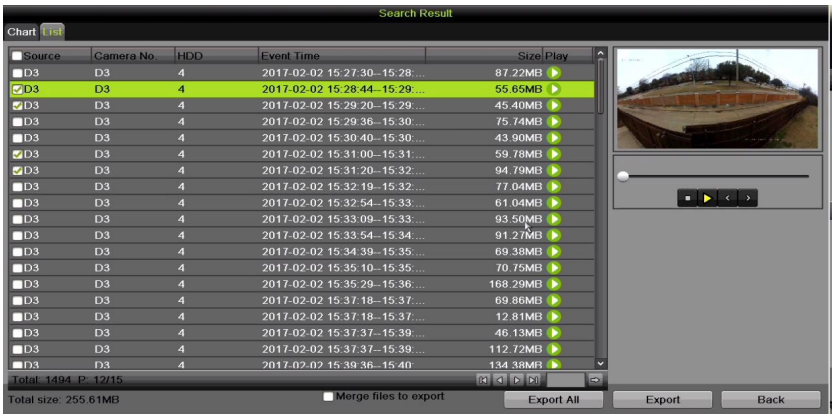


Figure 128 Result of Event Search

6. Export the video files. See step 5 of *Chapter 7.1.2 Backing up by Normal Video Search* for details.

8.1.4. Backing Up Video Clips or Captured Playback Pictures

Select video clips or captured pictures in playback mode to export directly during Playback, using USB devices (USB flash drives, USB HDDs, USB writer), SATA writer, or eSATA HDD.

1. Enter Playback interface (see

2.

3. Playing Back Record Files).

4. During playback, use or buttons in the playback toolbar to start or stop clipping record file(s); or use the button to capture pictures.

5. Click to enter the file management interface.

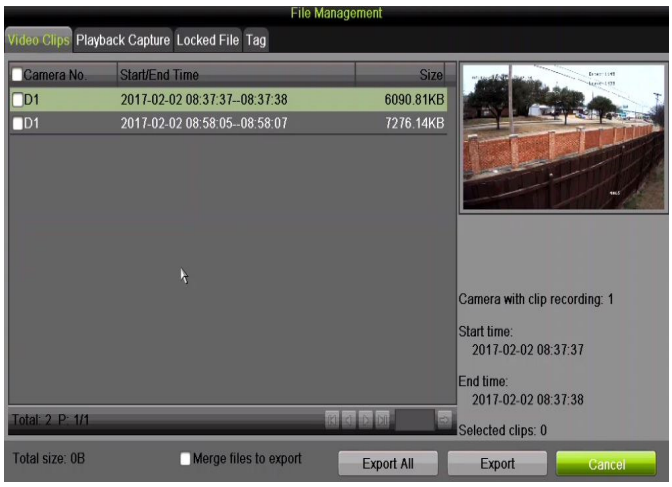


Figure 129 Video Clips or Captured Pictures Export Interface

6. Export the video clips or captured pictures in playback. Please refer to step 5 of *Chapter 7.1.2 Backing up by Normal Video Search* for details.

8.2 Managing Backup Devices

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

1. Enter the Export interface.

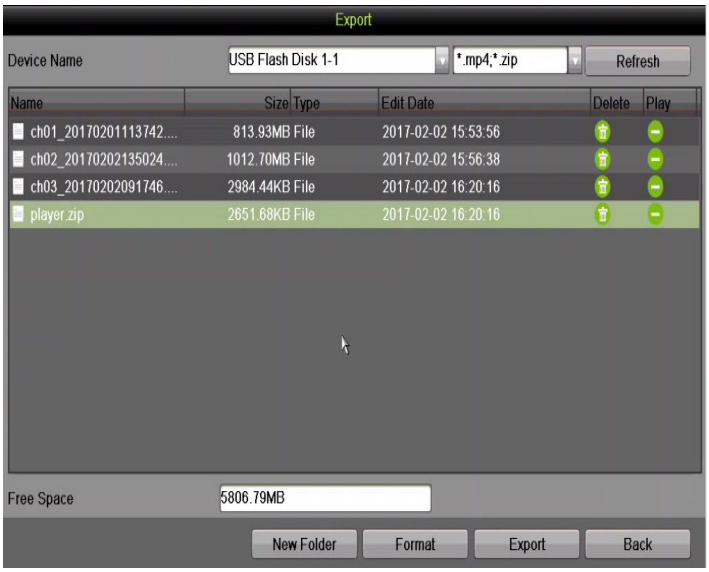


Figure 130 Storage Device Management

2. Backup device management.

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

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

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

6. Click Format button to format the backup device.

NOTE: If the inserted storage device is not recognized:

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

8.3 Hot Spare Device Backup

The device supports an N +1 hot spare system. The system consists of several working devices and a hot spare device. If the working device fails, the hot spare device switches into operation, increasing the system reliability.

NOTE: Contact dealer for details of models that support the hot spare function.

8.3.1. Before You Start

Ensure at least two devices are online.

A bidirectional connection shown in the figure below is required to be built between the hot spare device and each working device.

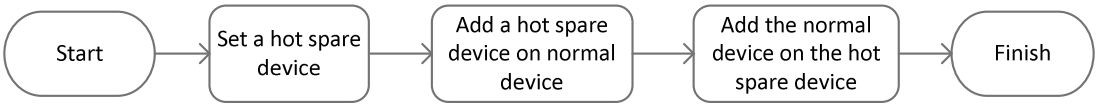


Figure 131 Building Hot Spare System

8.3.2. Setting Hot Spare Device

NOTE: The camera connection will be disabled when the device works in the hot spare mode.

It's highly recommended to restore the device defaults after switching the working mode of the hot spare device to normal mode to ensure normal operation afterwards.

1. Enter the Hot Spare settings interface, Menu > Configuration > Hot Spare.
2. Set the **Work Mode** as **Hot Spare Mode** and click the **Apply** button to confirm the settings.
3. Reboot the device to have the change take effect.

Figure 132 Reboot Attention

4. Click the **Yes** button in the pop-up attention box.

8.3.3. Setting Working Device

1. Enter the Hot Spare settings interface, Menu > Configuration > Hot Spare.
2. Set the Work Mode to Normal Mode (default).
3. Check the Enable checkbox to enable the hot spare function.
4. Enter the IP address and admin password of the hot spare device.

Figure 133 Setting Working Mode for Working Device

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

8.3.4. Managing the Hot Spare System

1. Enter the Hot Spare Settings interface of the hot spare device, Menu > Configuration > Hot Spare. The connected working device will be displayed on the device list.

2. Check the checkbox to select the working device from the device list, and click the **Add** button to link the working device to the hot spare device.

   NOTE: A hot spare device can connect up to 32 working devices.

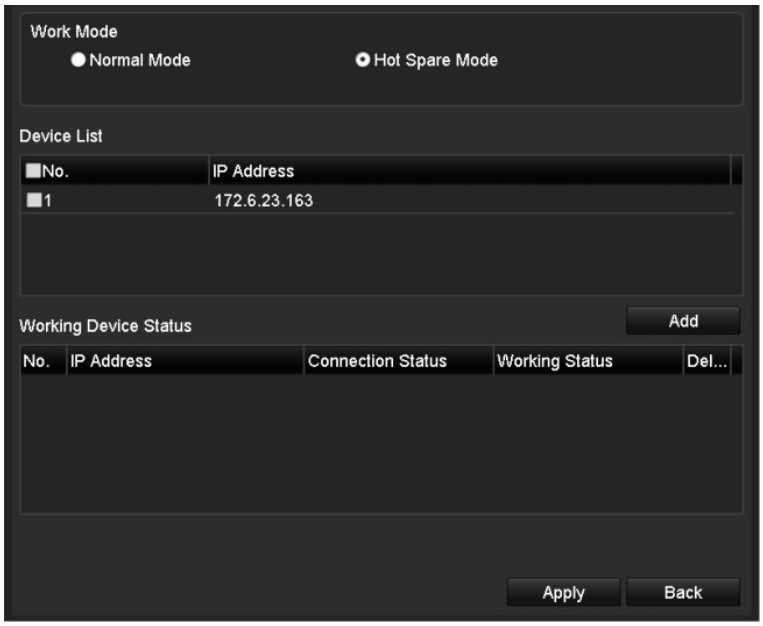


Figure 134 Add Working Device

3. View the working status of the hot spare device on the Working Status list. When the device is working properly, the working status of the hot spare device is displayed as *No record*.

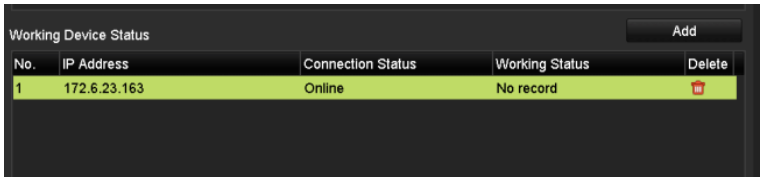


Figure 135 No Recording

NOTE: If the working device goes offline, the hot spare device will record the video of the IP Camera connected to the working device for backup, and the hot spare device working status will be displayed as *Backing up*. The record backup function supports one device at a time.

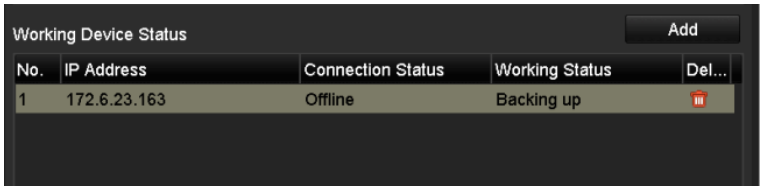


Figure 136 Backing Up

When the working device comes online, the lost video files will be restored by the record synchronization function, and the working status of the hot spare device will be displayed as *Synchronizing*.

The record synchronization function can be enabled for one working device at a **time.**

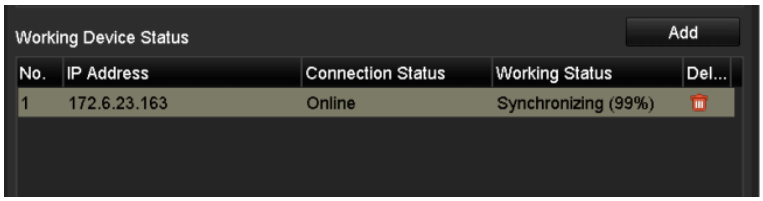


Figure 137 Synchronizing

Chapter 9 Alarm Settings

9.1 Setting Motion Detection Alarm

1. Enter the Camera Management Motion Detection interface and choose a camera for which you want to set up motion detection, Menu > Recording Configuration > Motion Detect.

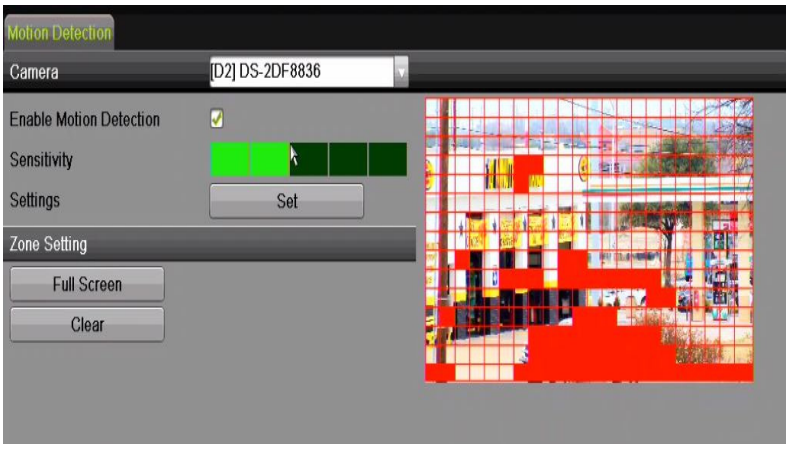


Figure 138 Motion Detection Setup Interface

2. Set up detection area and sensitivity.

3. Tick “Enable Motion Detection.” Use the mouse to draw detection area(s) and drag the sensitivity bar to set sensitivity.

4. Click **Set** button and set alarm response actions.

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

Figure 139 Set Trigger Camera of Motion Detection

6. Set up arming schedule of the channel.

   1). Select Arming Schedule tab to set the arming schedule of handling actions for motion detection.

   2). Choose a day of the week (up to eight time periods can be set within each day).

   3). Click Apply to save the settings.

   NOTE: Time periods cannot be repeated or overlapped.

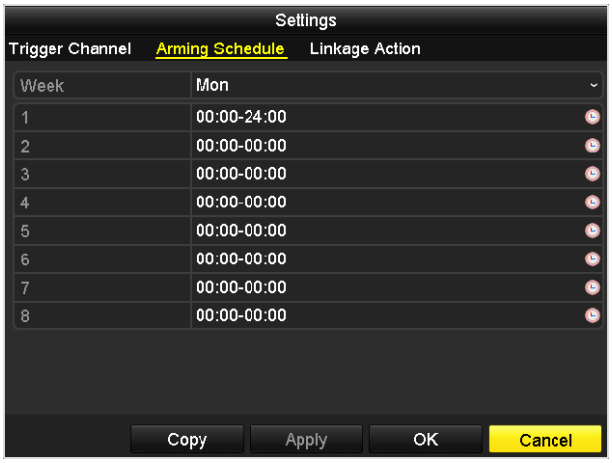


Figure 140 Set Arming Schedule of Motion Detection

7. Click Handling tab to set up motion alarm's response actions.

8. To set motion detection for another channel, repeat the above steps or just click Copy in the Motion Detection interface to copy the above settings to it.

9.2 Setting Sensor Alarms

Set the handling action of an external sensor alarm.

1. Enter System Configuration Alarm Settings and select an alarm input, Menu > Configuration > Alarm.

2. Select Alarm Input tab.

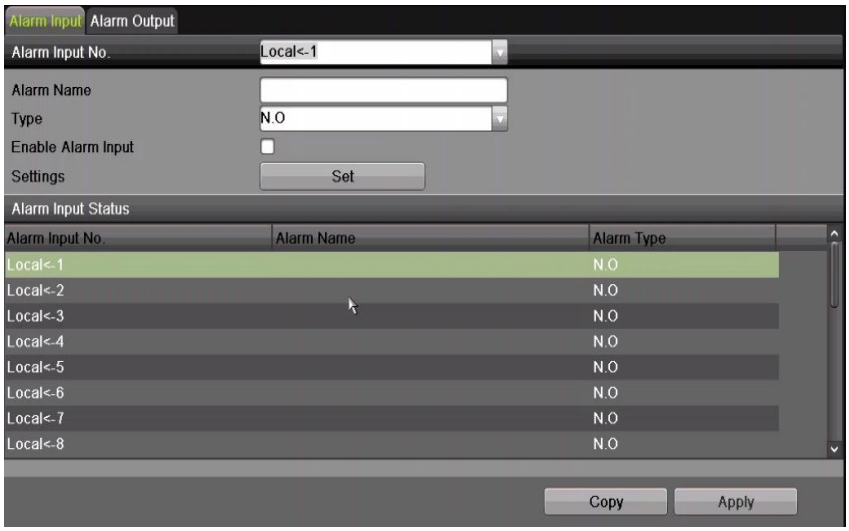


Figure 141 System Configuration Alarm Status Page

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

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

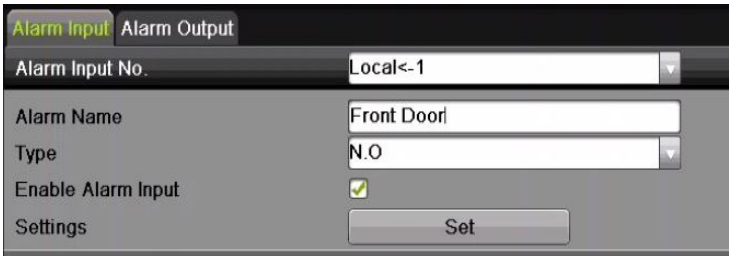


Figure 142 Alarm Input Setup Interface

5. Select Trigger Channel tab and select one or more channels that will start to record/capture or become full-screen monitoring when an external alarm is input, and click Apply to save the settings.

6. Select Arming Schedule tab to set the arming schedule of handling actions.

Figure 143 Set Arming Schedule of Alarm Input

7. Choose a day of the week (maximum of eight time periods can be set within each day).
8. Click Apply to save the settings.

   NOTE: Time periods cannot repeat or overlap.

9. Repeat the above steps to set up arming schedule of other days of the week. You can also use Copy button to copy an arming schedule to other days.
10. Select Linkage Action tab to set up alarm response actions of the alarm input.
11. If necessary, select PTZ Linking tab and set PTZ linkage of the alarm input.
12. Set PTZ linking parameters and click OK to complete the alarm input settings.

    NOTE: Check whether the PTZ or speed dome supports PTZ linkage.

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

Figure 144 Set PTZ Linking of Alarm Input

13. To set the handling action of another alarm input, repeat the above steps, or click the Copy button in the Alarm Input Setup interface and check the alarm inputs checkbox to copy the settings.

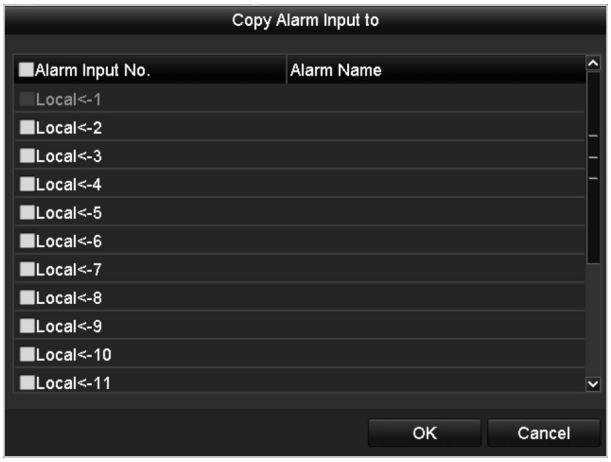


Figure 145 Alarm Input Copy Settings

9.3 Detecting Video Loss Alarm

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

1. Go to Menu > Camera > Video Loss and select a channel to detect.

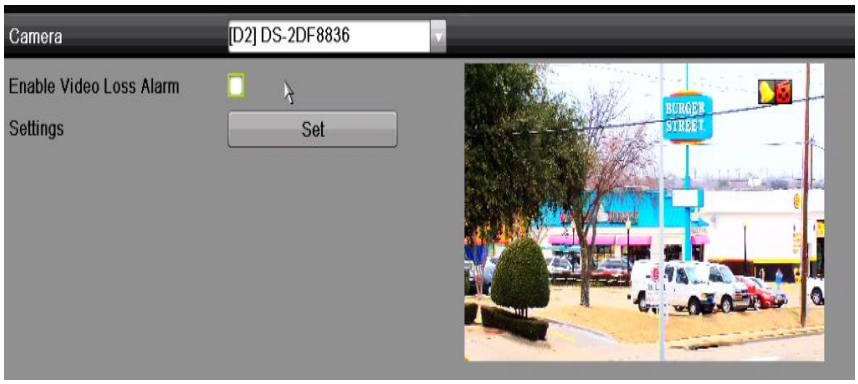


Figure 146 Video Loss Setup Interface

2. Set up handling action of video loss.
3. Check the “Enable Video Loss Alarm” checkbox.
4. Click the **Set** button to set up the video loss handling action.
5. Set up the handling actions arming schedule.
   - Select Arming Schedule tab to set the channel’s arming schedule.
   - Choose a day of the week (up to eight time periods can be set within each day).
   - Click Apply button to save the settings.

     NOTE: Time periods cannot repeat or overlap.

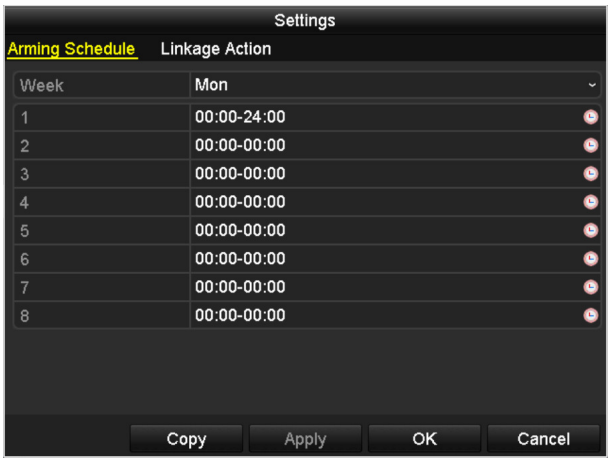


Figure 147 Set Arming Schedule of Video Loss

6. Select Linkage Action tab to set up video loss alarm response action.

7. Click the OK button to complete the channel's video loss settings.

9.4 Detecting Video Tampering Alarm

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

1. Go to Menu > Camera Setup > Video Tampering and select a channel to detect video tampering,.

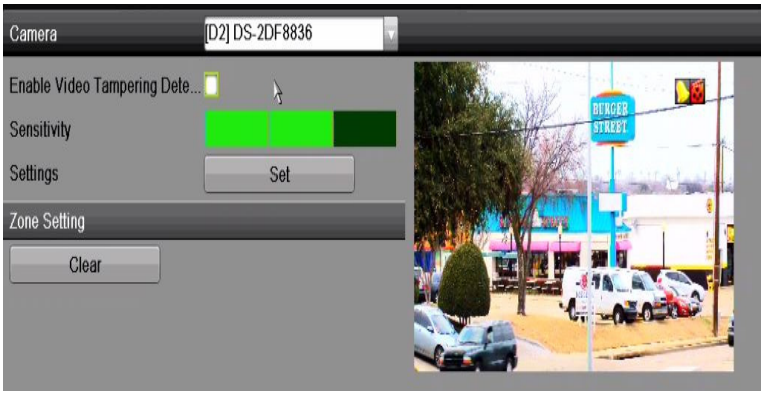


Figure 148 Video Tampering Setting Interface

2. Set the video tampering handling action of the channel.

3. Check the "Enable Video Tampering Detection" checkbox.

4. Drag the sensitivity bar to set a proper sensitivity level. Use the mouse to draw an area you want to detect video tampering.

5. Click **Set** button to set up video tampering handling action.

6. Set channel's arming schedule and alarm response actions.

1) Click Arming Schedule tab to set the handling actions arming schedule.

2) Choose a day of the week (maximum of eight time periods can be set within each day).

3) Click Apply button to save the settings.

NOTE: Time periods cannot repeat or overlap.

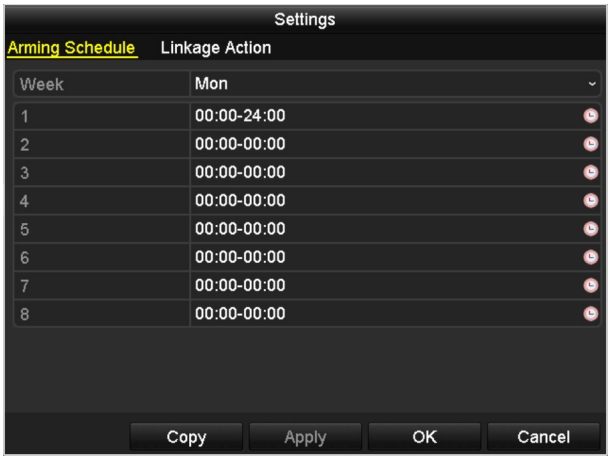


Figure 149 Set Arming Schedule of Video Tampering

7. Select Linkage Action tab to set up video tampering alarm response actions.

8. Click the OK button to complete the channel's video tampering settings.

9.5 Handling Exceptions Alarm

Exception settings refer to the handling action of various exceptions.

- HDD Full: The HDD is full
- HDD Error: Writing HDD error or unformatted HDD
- Network Disconnected: Disconnected network cable
- IP Conflicted: Duplicated IP address
- Illegal Login: Incorrect user ID or password
- Record/Capture Exception: No space for saving recorded files or captured images
- Hot Spare Exception: Disconnected from the working device

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

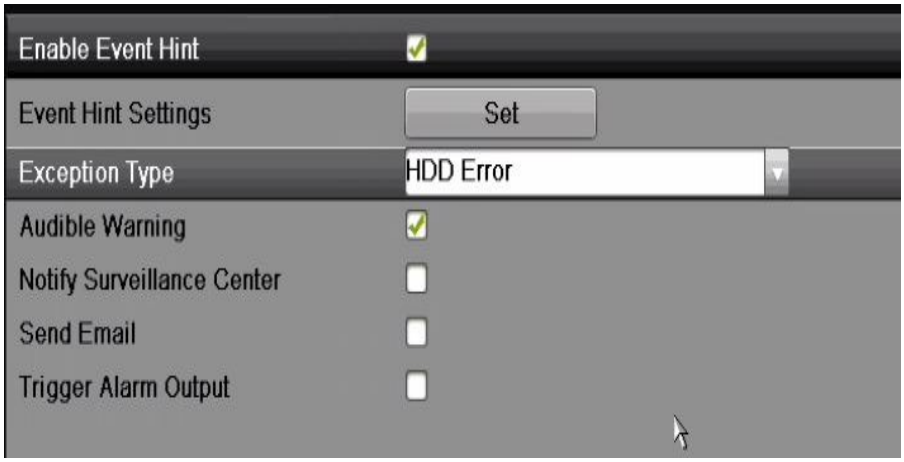


Figure 150 Exceptions Setup Interface

9.5.1. Setting Alarm Response Actions

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

9.5.2. Event Hint Display

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

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

Figure 151 Event Hint Settings Interface

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

Figure 152 Event Hint Settings Interface

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

9.5.3. Full Screen Monitoring

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

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

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

NOTE: Select the channel(s) you want to make full screen monitoring in “Trigger Channel” settings.

9.5.4. Audible Warning

An audible *beep* will sound when an alarm is detected.

9.5.5. Notify Surveillance Center

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

NOTE: The alarm signal will be transmitted automatically in detection mode when a remote alarm host is configured. Refer to *Chapter 11.2.6 Configuring More Settings* for details of alarm host configuration.

9.5.6. E-Mail Linkage

Send an e-mail with alarm information to a user or users when an alarm is detected. Refer to *Chapter 11.2.8 Configuring E-Mail* for details of e-mail configuration.

9.5.7. Trigger Alarm Output

Trigger an alarm output when an alarm is triggered.

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

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

Figure 153 Alarm Output Setup Interface

3. Set up arming schedule of the alarm output.
4. Choose a day of the week (up to eight time periods can be set within each day).

   NOTE: Time periods cannot repeat or overlap.

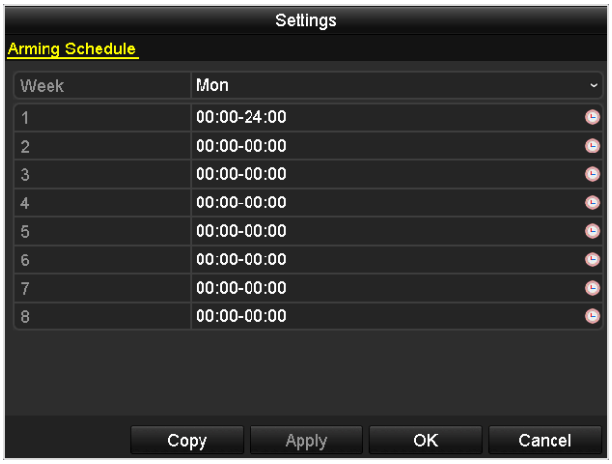


Figure 154 Set Arming Schedule of Alarm Output

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

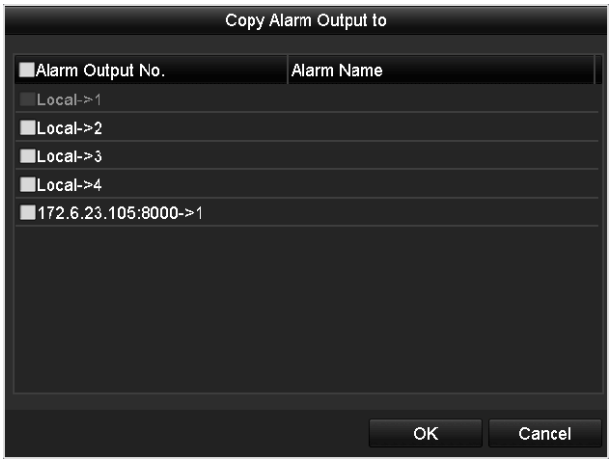


Figure 155 Alarm Output Copy Settings

9.6 Triggering or Clearing Alarm Output Manually

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

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

4. Click Clear All button to clear all alarm output.

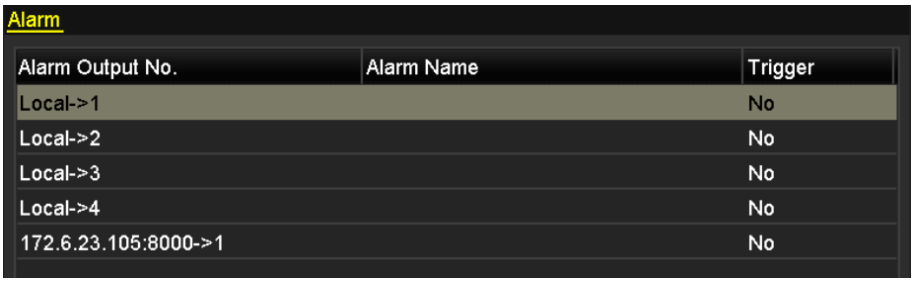


Figure 156 Clear or Trigger Alarm Output Manually

Chapter 10 VCA Alarm

The NVR supports VCA detection alarms (face detection, vehicle detection, line crossing detection and 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) sent by IP cameras. VCA detection must first be enabled and configured in the IP camera settings interface.

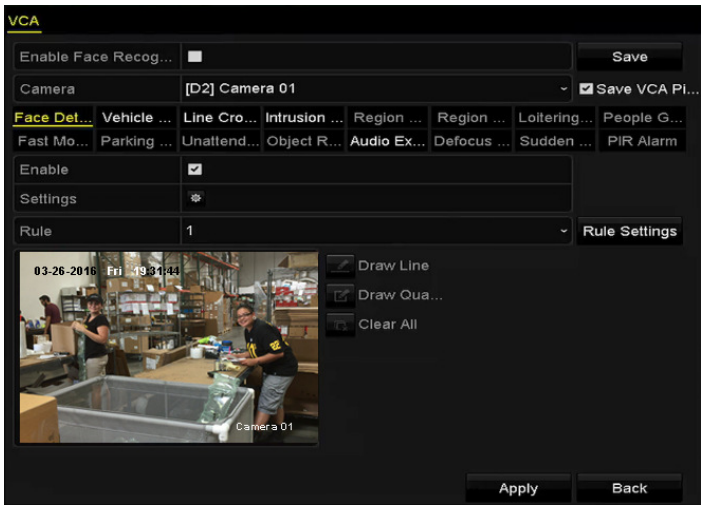
NOTE: The VCA detection alarm must be supported by the connected IP camera to function.

See network camera's user manual for detailed instructions of all VCA detection types.

10.1 Face Detection

The Face Detection function detects faces that appear in the surveillance scene, and certain actions can be taken when the alarm is triggered.

1. Enter the VCA settings interface, Menu > Camera > VCA.
2. Select the camera to configure the VCA.
3. You can click the Save VCA Picture checkbox to save the captured VCA detection pictures.



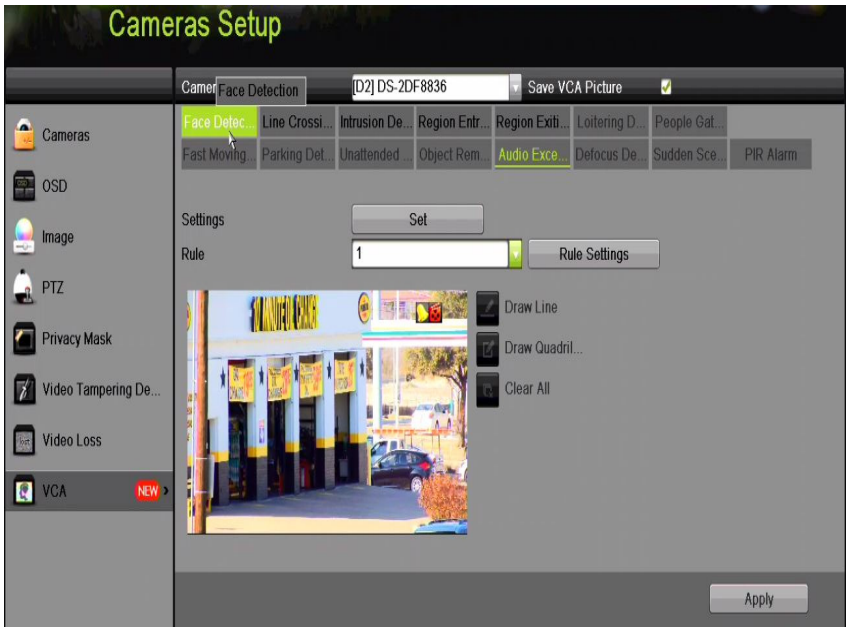


Figure 157 Face Detection

4. Select Face Detection as the VCA detection type.

5. Check the Enable checkbox to enable this function.

6. Click **Set** button to enter the face detection settings interface. Configure the trigger channel, arming schedule, and linkage action for the face detection alarm. Refer to Step 3 through Step 5 of Chapter 8.1 Setting Motion Detection Alarm for detailed instructions.

7. Click the Rule Settings button to set the face detection rules. You can click-and-drag the slider to set the detection sensitivity.

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

Figure 158 Set Face Detection Sensitivity

8. Click Apply to activate the settings.

10.2 Line Crossing Detection

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

1. Enter the VCA settings interface, Menu > Camera > VCA.
2. Select the camera for which to configure the VCA.
3. Click the Save VCA Picture checkbox to save the captured VCA detection pictures.
4. Select Line Crossing Detection as the VCA detection type.
5. Check the Enable checkbox to enable this function.
6. Click Set button to configure the trigger channel, arming schedule, and linkage actions for the line crossing detection alarm.
7. Click the Rule Settings button to set the line crossing detection rules.
   1). Select the direction to A<->B, A->B or A<-B.
   - A<->B: An object crossing the configured line in either direction will be detected and trigger an alarm.
   - A->B: Only an object crossing the configured line from the A side to the B side will be detected.
   - B->A: Only an object crossing the configured line from the B side to the A side will be detected.

   2). Click-and-drag the slider to set the detection sensitivity.
   - Sensitivity: Range [1-100]. The higher the value, the more easily the detection alarm will be triggered.

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

Figure 159 Set Line Crossing Detection Rules

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

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

Up to four rules can be configured.

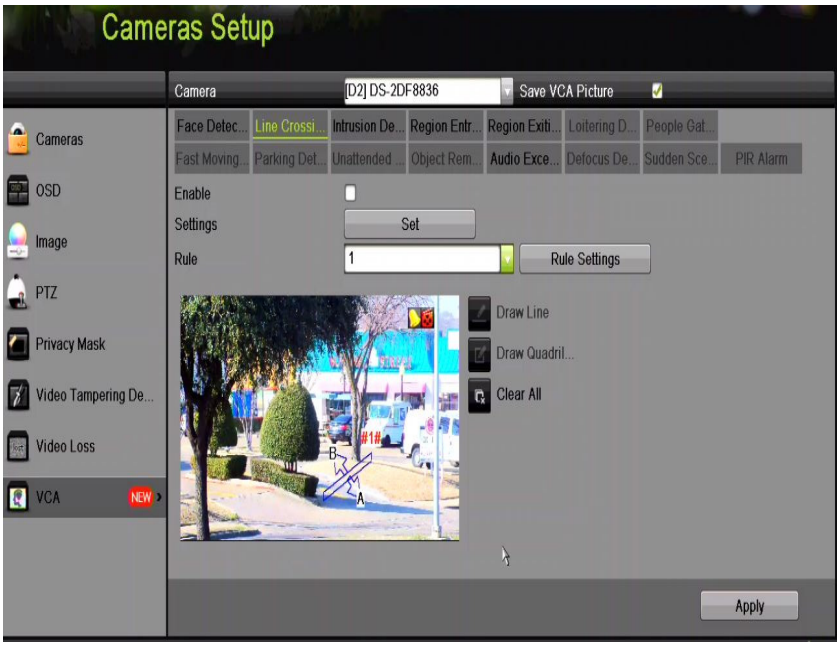


Figure 160 Draw Line for Line Crossing Detection

9. Click Apply to activate the settings.

10.3 Intrusion Detection

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

1. Enter the VCA settings interface, Menu > Camera > VCA
2. Select the camera for which to configure the VCA.
3. Click the Save VCA Picture checkbox to save the captured VCA detection pictures.
4. Select Intrusion Detection as the VCA detection type.
5. Check the Enable checkbox to enable this function.
6. Click **Set** button to configure the trigger channel, arming schedule, and linkage actions for the line crossing detection alarm.
7. Click the Rule Settings button to set the intrusion detection rules. Set the following parameters.
   - Threshold: Range [1s-10s], the threshold for the time the object loiters in the region. When the duration the

object is 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 can trigger the alarm. The higher the value, the more easily the detection alarm will be triggered. Click-and-drag the slider to set the detection sensitivity.
- Percentage: Range [1-100]. Percentage defines the ratio of the in-region part of the object that will trigger the alarm. For example, if the percentage is set as 50%, when the object enters the region and occupies half of the whole region, the alarm will be triggered.

Figure 161 Set Intrusion Crossing Detection Rules

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

NOTES: You can use the  to clear the existing virtual region and re-draw it.

Up to four rules can be configured.

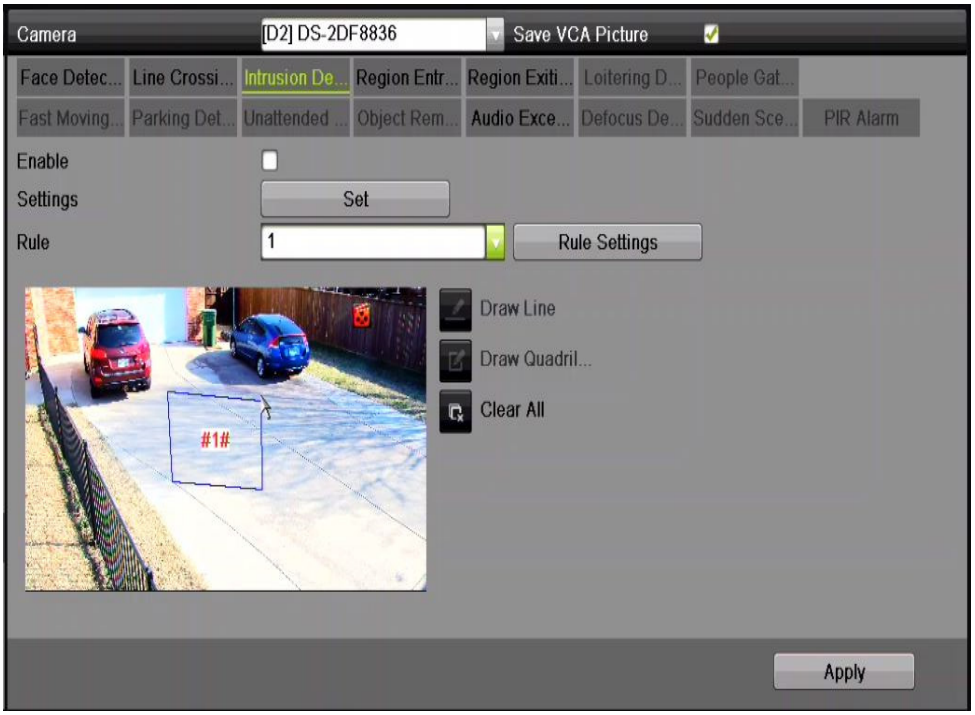


Figure 162 Draw Area for Intrusion Detection

10. Click Apply to save the settings.

10.4 Region Entrance Detection

The Region Entrance Detection function detects people, vehicles, or other objects that enter a pre-defined virtual region from an outside area, and certain actions can be taken when the alarm is triggered.

1. Enter the VCA settings interface, Menu > Camera > VCA.
2. Select the camera for which to configure the VCA.
3. Click the Save VCA Picture checkbox to save the captured VCA detection pictures.
4. Select Region Entrance Detection as the VCA detection type.
5. Check the Enable checkbox to enable this function.
6. Click **Set** button to configure the trigger channel, arming schedule, and linkage actions for the line crossing detection alarm.
7. Click the Rule Settings button to set the region entrance detection sensitivity.
    - 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.

   NOTES: You can use the  button to clear an existing virtual region and re-draw it.

   Up to four rules can be configured.

9. Click Apply to save the settings.

Figure 163 Set Region Entrance Detection

10.5 Region Exiting Detection

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.

NOTES: Up to four rules can be configured.

10.6 Unattended Baggage Detection

The Unattended Baggage Detection function detects objects (e.g., baggage, purse, dangerous materials, etc.) left in a pre-defined region, and a series of actions can be taken when the alarm is triggered.

NOTES: Refer to *Chapter 9.4 Intrusion Detection* for steps to configure Unattended Baggage Detection.

Threshold [5s-20s] in Rule Settings defines the time the objects must be left in the region to generate an alarm. If the value is 10, an alarm is triggered if the object is left and stays in the region for 10 seconds. **Sensitivity** defines similarity of the object to the background. When the sensitivity is high, a very small object left in the region can trigger the alarm.

Up to four rules can be configured.

10.7 Object Removal Detection

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 an alarm is triggered.

NOTES: Refer to *Chapter 9.4 Intrusion Detection* for steps to configure Object Removal Detection.

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

Up to four rules can be configured.

10.8 Audio Exception Detection

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

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

Figure 164 Set Audio Exception Detection Rules

7. Check the Audio Input Exception checkbox to enable the Audio Loss Detection function.
8. Check the Sudden Increase of Sound Intensity Detection checkbox to detect a steep rise in sound in the surveillance scene. Set the sound detection sensitivity and threshold (see below).
   - Sensitivity: Range [1-100], the smaller the value, the more severe the change must be to trigger the detection.
   - Sound Intensity Threshold: Range [1-100] filters the environment sound. The louder the environment sound, the higher the value should be. Adjust it according to the real environment.
9. Check the Sudden Decrease of Sound Intensity Detection checkbox to detect a steep drop in sound in the surveillance scene. Set the detection sensitivity [1-100] as required.
10. Click Apply to activate the settings.

10.9 Sudden Scene Change Detection

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

NOTES: Refer to *Chapter 9.2 Face Detection* for steps to configure Scene Change Detection.

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

10.10 Defocus Detection

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

NOTES: Refer to *Chapter 9.2 Face Detection* for steps to configure Defocus Detection.

Sensitivity in Rule Settings ranges from 1 to 100, and the higher the value, the more easily a defocused image will trigger an alarm.

10.11 PIR Alarm

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

1. Enter the VCA settings interface, Menu > Camera > VCA.
2. Select the camera to configure the VCA.
3. Click the Save VCA Picture checkbox to save the captured VCA detection pictures.
4. Select PIR Alarm as the VCA detection type.
5. Click Set button to configure the trigger channel, arming schedule, and linkage action for the PIR alarm.
6. Click the Rule Settings button to set the rules. Refer to Chapter 9.2 Face Detection for instructions.
7. Click Apply to activate the settings.

Chapter 11 VCA Search

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

11.1 Face Search

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

NOTE: Refer to Chapter 0 Face Detection for configuring Face Detection.

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

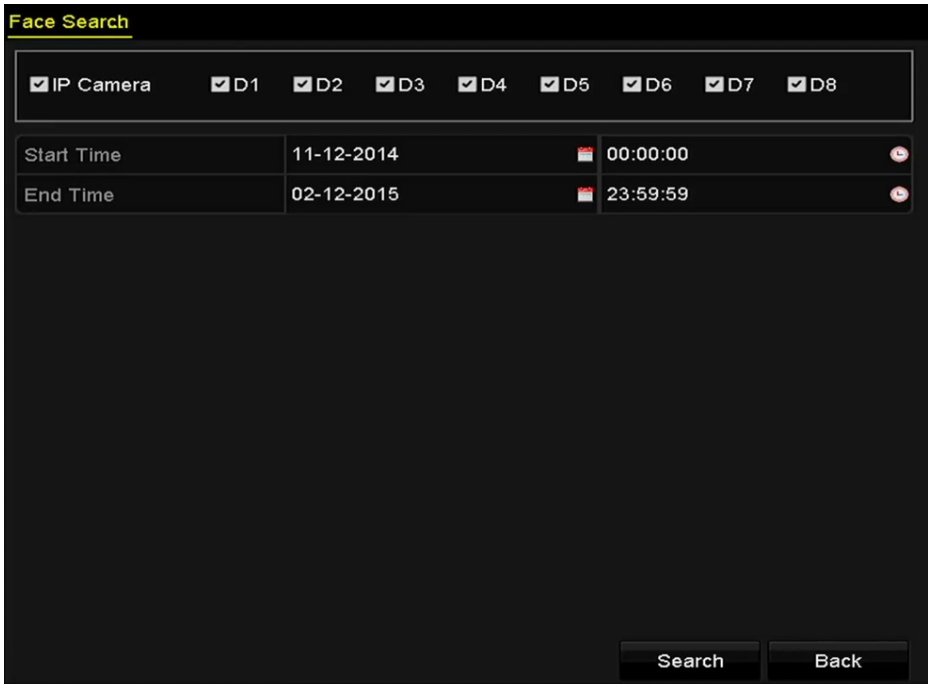


Figure 165 Face Search

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

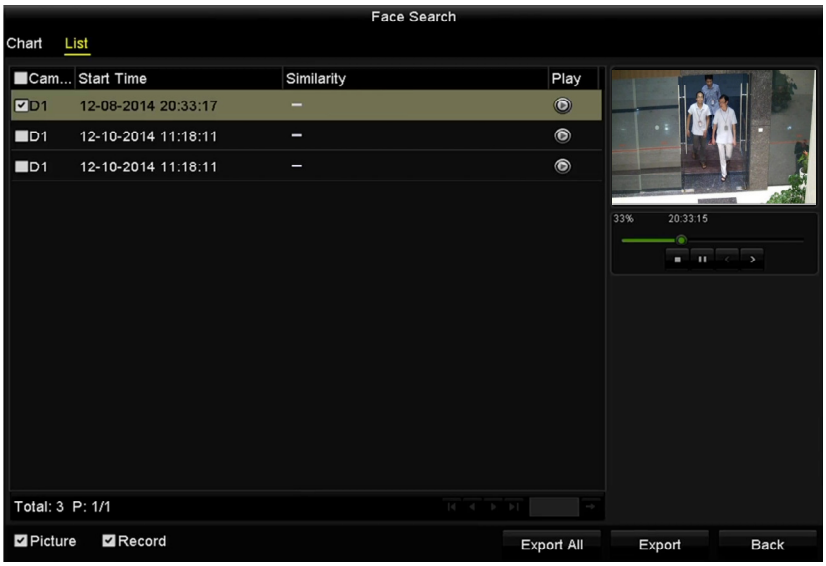


Figure 166 Face Search Interface

5. Play the face picture related video file.

6. Double click a face picture to play its related video file in the view window on the top right, or select a picture item and click to play it. You can also click to stop the playing, or click / to play the previous/next file.

7. To export the captured face pictures to a local storage device, connect the storage device and click Export All to enter the Export interface.

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

NOTES: Refer to *Chapter7 Backup* for operation of exporting files.

Figure 167 Export Files

11.2 Behavior Search

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

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

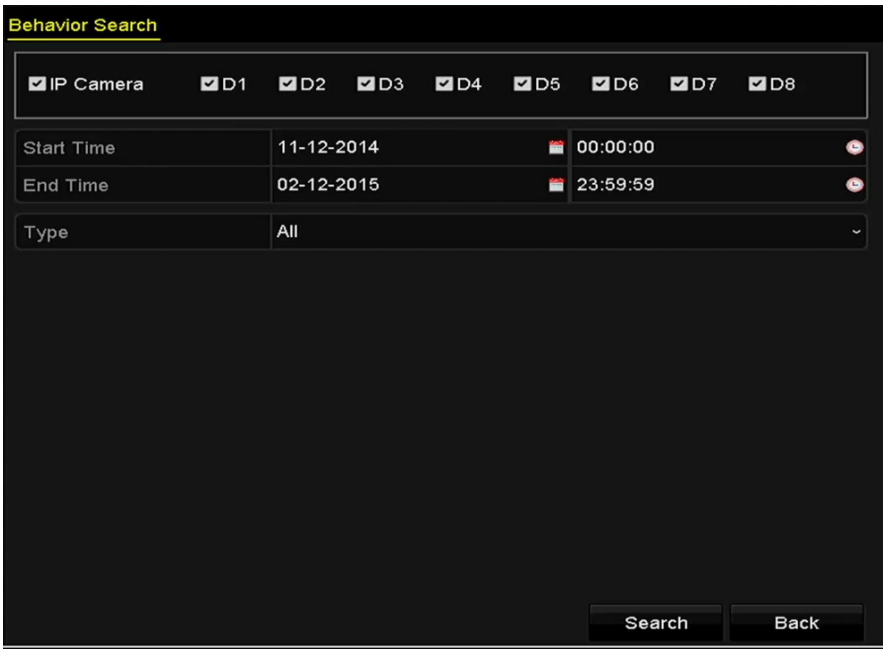


Figure 168 Behavior Search Interface

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

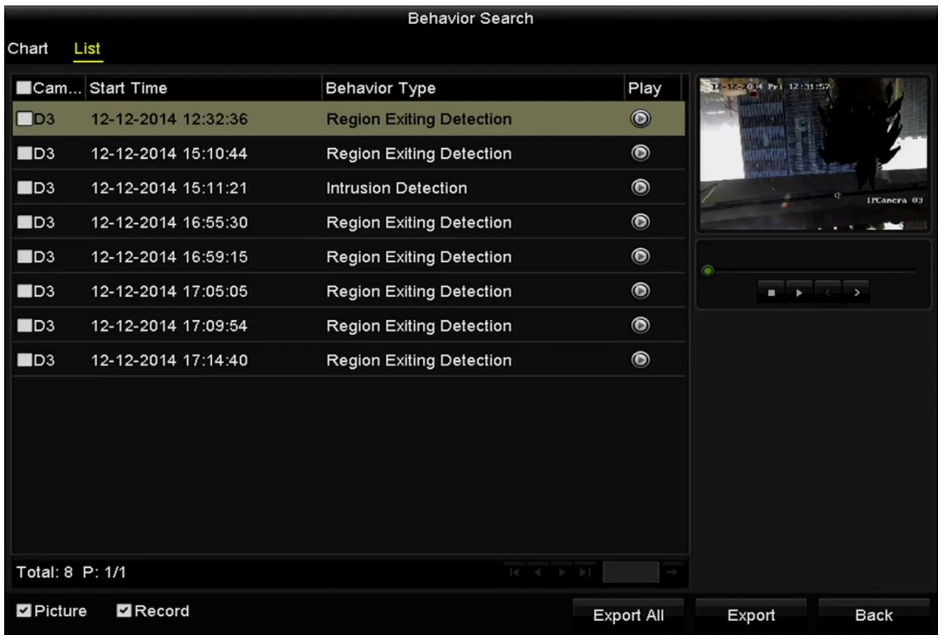


Figure 169 Behavior Search Results

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

11.3 Plate Search

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

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

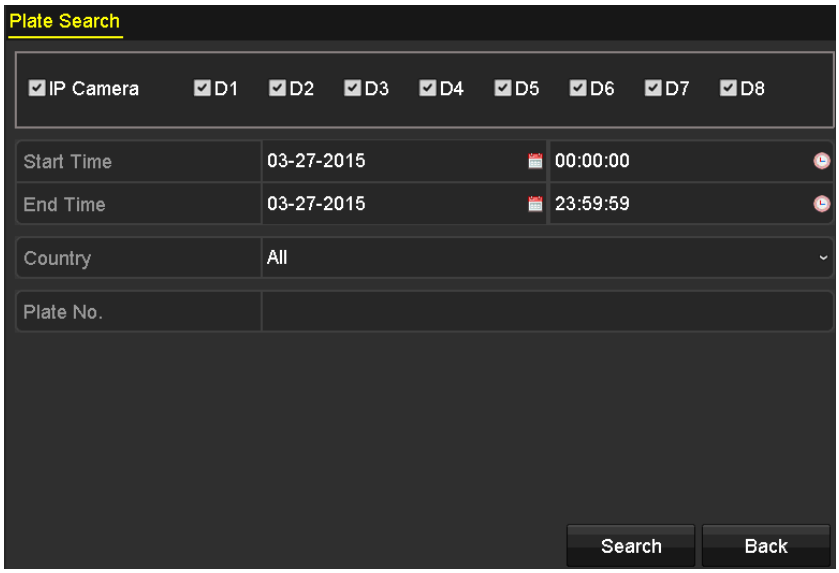


Figure 170 Plate Search

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

NOTE: Refer to Step 7 and Step 8 of *Section 10.1 Face Search* for operation of the search results.

11.4 People Counting

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

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

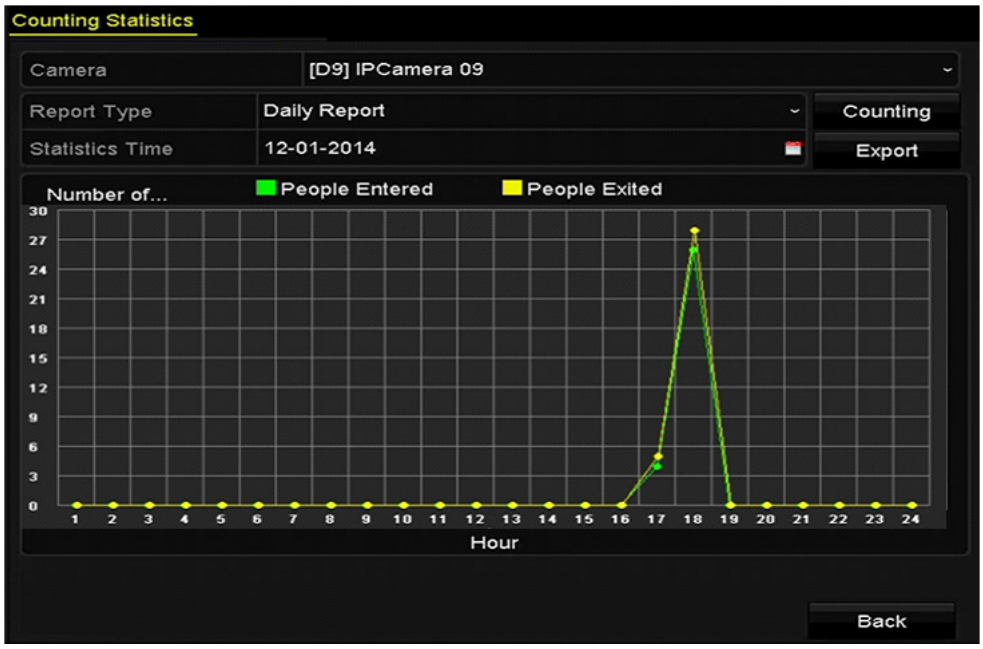


Figure 171 People Counting Interface

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

11.5 Heat Map

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

NOTE: The Heat Map function must be supported by the connected IP camera and the corresponding configuration must be set.

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

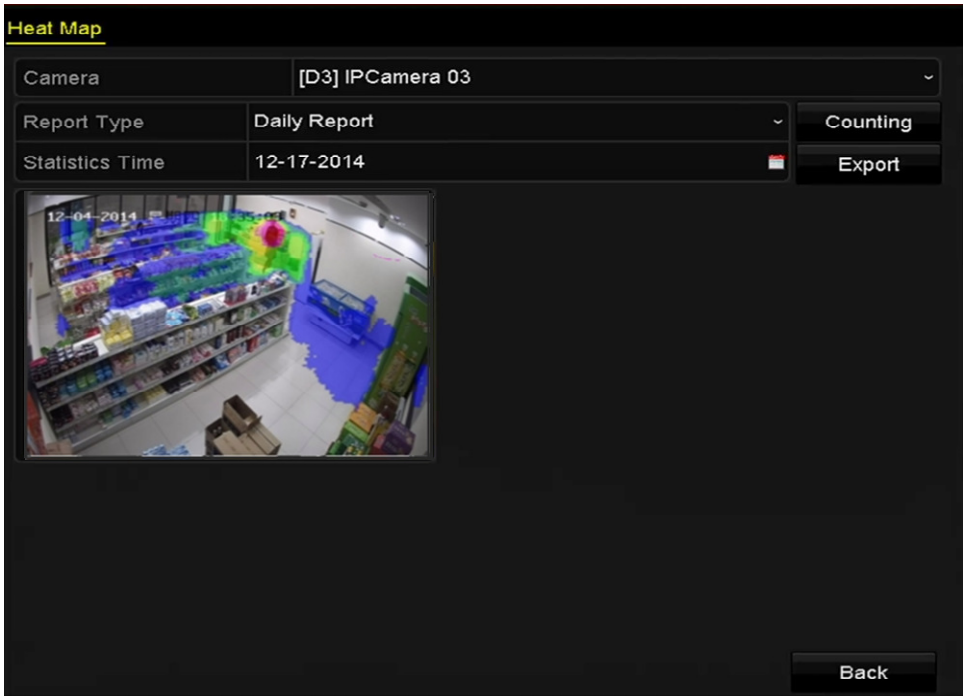


Figure 172 Heat Map Interface

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

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

Chapter 12 Network Settings

12.1 Configuring General Settings

Network settings must be properly configured before operating the NVR over a network.

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

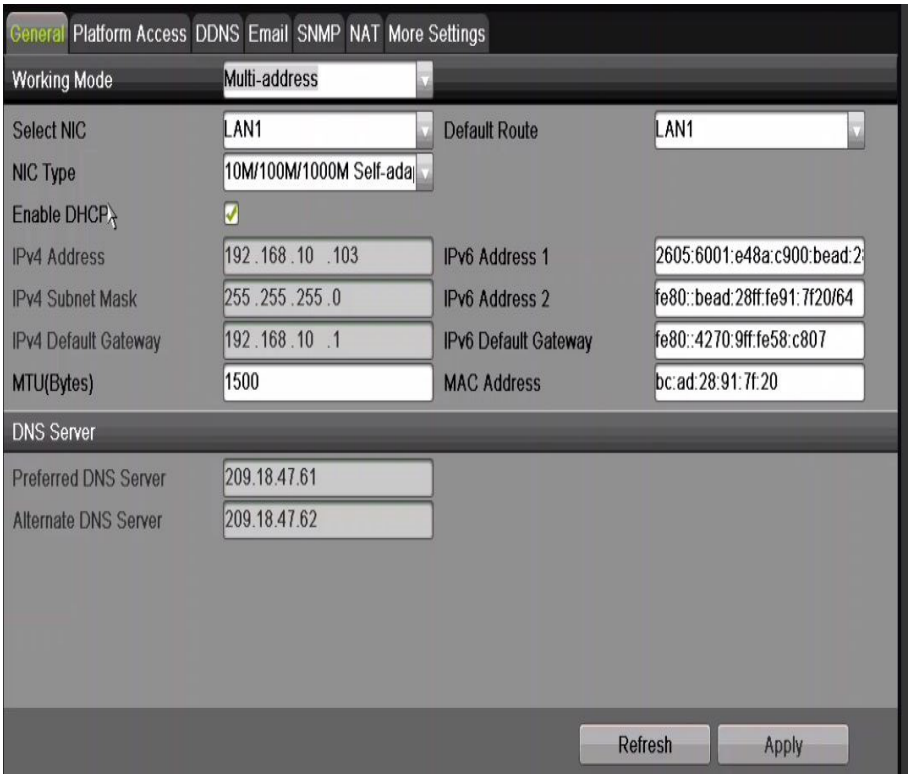


Figure 173 Network Settings Interface

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

NOTES: The valid value MTU range is 500 – 9676.

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

Two self-adaptive 10M/100M/1000M network interfaces for DS-9600NI-I8, DS-7700NI-I4, and the multi-address and network fault tolerance working modes are configurable.

One self-adaptive 10M/100M/1000M network interface for DS-7700NI-I4/P.

For DS-7700NI-I(I)/P Series NVRs, you need to configure the internal NIC address so that IP addresses are assigned to the cameras connected to the PoE interfaces.

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

12.1.1. Working Mode (DS-96xxNI-I8 Models)

Two 10M/100M/1000M NIC cards are provided and it allows the device to work in the Multi-address and Net-fault Tolerance modes.

- **Multi-address Mode:** The parameters of the two NIC cards can be configured independently. Select LAN1 or LAN2 in the NIC type field for parameter settings. Select one NIC card as the default route, and the data connecting to the extranet will be forwarded through the default route.
- **Net-Fault Tolerance Mode:** The two NIC cards use the same IP address. Select the Main NIC as LAN1 or LAN2. This way, in case one NIC card fails, the device will automatically enable the other standby NIC card so as to ensure normal running of the system.

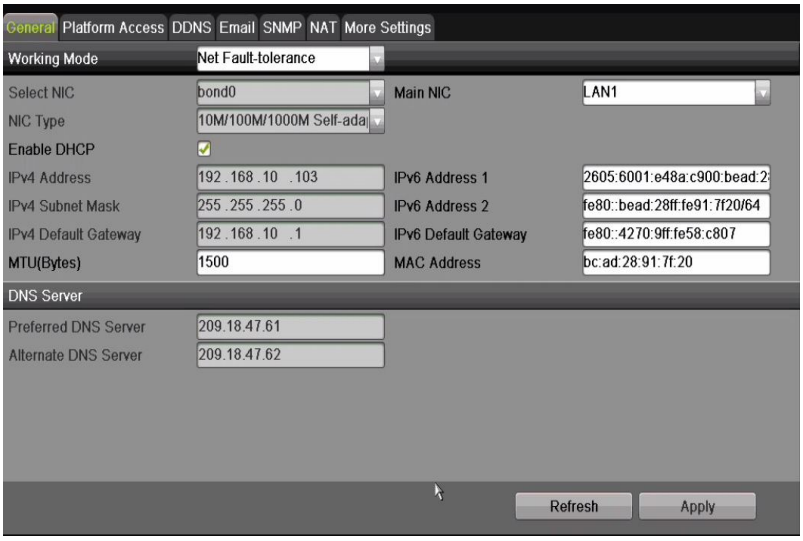


Figure 174 Net Fault-tolerance Working Mode (/I8 NVRs only)

12.2 Configuring Advanced Settings

12.2.1. Register a HIK-Connect P2P Cloud Service Account

1. Use the Hik-Connect mobile app (from iOS App Store or Google Play) to create a Hik-Connect P2P Cloud account to connect Hikvision devices over the Internet.
2. Click on “Register an Account.”
3. Check the **Read and Agree** checkbox.

4. Register the Account.

   - Using Mobile Phone Number:

     1） Click Register by Mobile Phone Number.

     2） Click on your country to display checkmark, then click **Finish**.

     3） Enter your mobile phone number, then press **Get Verification Code** button.

     4） Check your phone for the verification code that was texted, and enter it into the “Input the received verification code” field, then click the **Next** button.

     5） Create user name and password, re-type confirmation password, then click **Finish** button.

   - Using E-Mail Address:

     1） Click Register by E-Mail Address.

     2） Click on your country to display checkmark, then click the **Finish** button.

     3） Enter your e-mail address, then click the **Next** button.

     4） Check your e-mail for the verification code that was texted, and enter it into the “Input the received verification code” field, then click the **Next** button.

     5） Create user name and password, re-type confirmation password, then click **Finish** button.

12.2.2. Enable Hik-Connect P2P on the NVR.

1. Go to Main Menu > System Configuration > Network > Platform Access.
2. Check the **Enable** checkbox.
3. Server Address must be “dev.hik-connect.com.” If not, check the **Custom** checkbox, and type “dev.hik-connect.com.”
4. To turn **Enable Stream Encryption** on, select its checkbox.
5. Click the **Apply** button. Status will change to “Online” (if all settings are correct).
6. Note the Serial Number and Verification Code shown here (for use when registering the NVR in your Hik-Connect account) or use the QR code displayed.

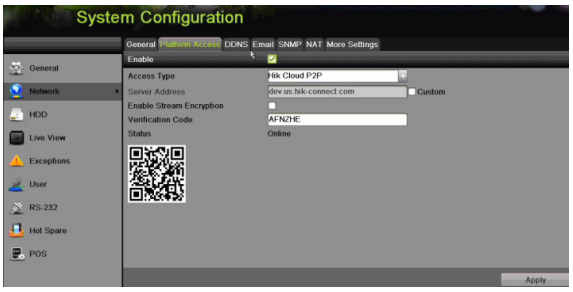


Figure 175, HIK-Connect Cloud P2P Settings Interface

12.2.3. Add the NVR to the Hik-Connect Service

To see a video stream on the Hik-Connect or iVMS-4500 mobile app, you must add the NVR.

1. Login to Hik-Connect mobile app with your user name, e-mail, or mobile number and password.
2. On the Home screen, click the "**+**" button (upper right corner).
3. Enter the device's information.
   - If you have device's **QR Code**: Use QR Code Scanner to scan **QR Code**.
   - If you do not have device's **QR Code**: Enter device information manually:

     1） Click the Edit (pencil) icon on top right.

     2） Enter device serial number (device must be online), then click the **OK** button.

     3） When the device appears on the "Results" screen, click the **Add** button.

     4） Enter the device's 6-character Verification Code (all upper case), then click the **OK** button.

     5） Click the **Finish** button.

NOTES: For existing DVRs with Hik-Connect enabled, Hik-Connect will still be enabled if upgraded. If Hik-Connect is disabled then enabled for the first time, you must change the verification code if the encrypted verification code is the same as that of the configuration file, or if the encrypted verification code is empty and the configuration file's verification code is "ABCDEF." Under either of these conditions, create a new verification code or delete the default code and input the same same default verification code.

12.2.4. Accessing the NVR

After configuration, you can access and manage the NVR on your mobile phone with the HIK-Connect Cloud P2P app (iOS or Android) or through the HIK-Connect website (www.hik-connect.com).

NOTE: For more help, see the help file on the Hik-Connect website at www.hik-connect.com.

12.2.5. Configuring NTP Server

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

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

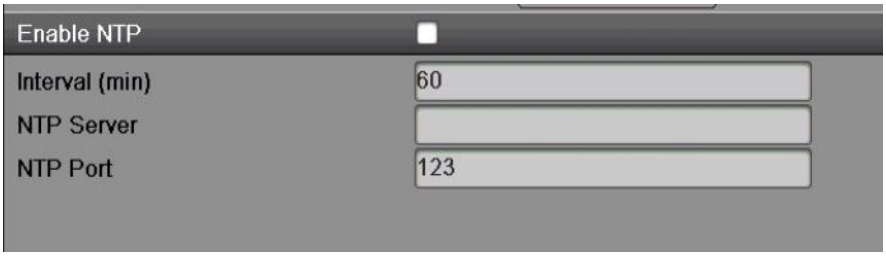


Figure 176 NTP Settings Interface

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

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

12.2.6. Configuring SNMP

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

1. Enter the Network Settings interface, Menu > Configuration > Network.
2. Select the **SNMP** tab to enter the SNMP Settings interface, as shown in Figure 177.

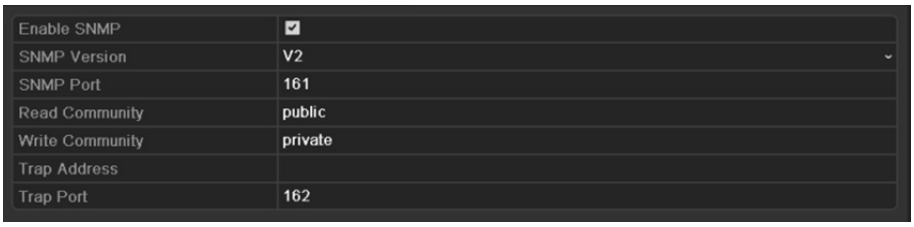


Figure 177 SNMP Settings Interface

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

4. Enabling SNMP may cause security problems. Click **Yes** to continue or **No** to cancel the operation.

Figure 178 SNMP Settings Interface

5. When you choose the Yes option in Step 4, configure the following SNMP settings:

   - **Trap Address:** IP Address of SNMP host
   - **Trap Port:** Port of SNMP host

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

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

12.2.7. Configuring More Settings

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

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

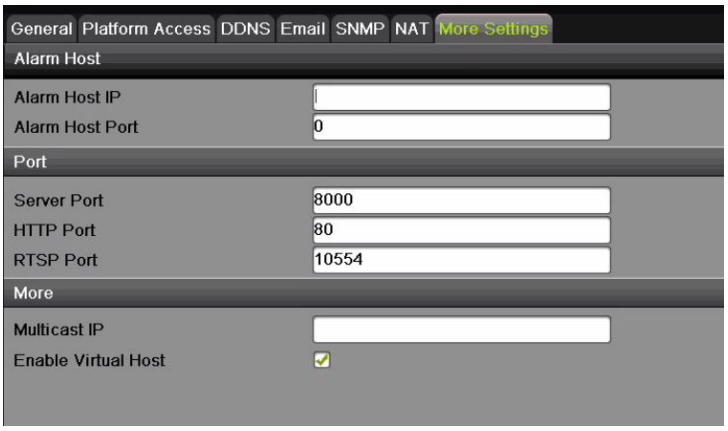


Figure 179 More Settings Interface

3. Configure the remote alarm host, server port, HTTP port, multicast, RTSP port.

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

     The **Alarm Host IP** refers to the IP address of the remote PC on which the CMS (Client Management System) software (e.g., iVMS-4200) is installed, and the **Alarm Host Port** must be the same as the alarm monitoring port configured in the software (default port is 7200).

   - **Multicast IP**: The multicast can be configured to realize live view for more than the maximum number of cameras through the network. A multicast address spans the Class-D IP range of 224.0.0.0 to 239.255.255.255. It is recommended to use the IP address ranging from 239.252.0.0 to 239.255.255.255.

     When adding a device to the CMS (Client Management System) software, the multicast address must be the same as the device's multicast IP.

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

     Enter the RTSP port in the **RTSP Port** text field. The default RTSP port is 554, and you can change it according to 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 in the range of 2000-65535 and it is used for remote client software access. The HTTP port is used for remote IE access.

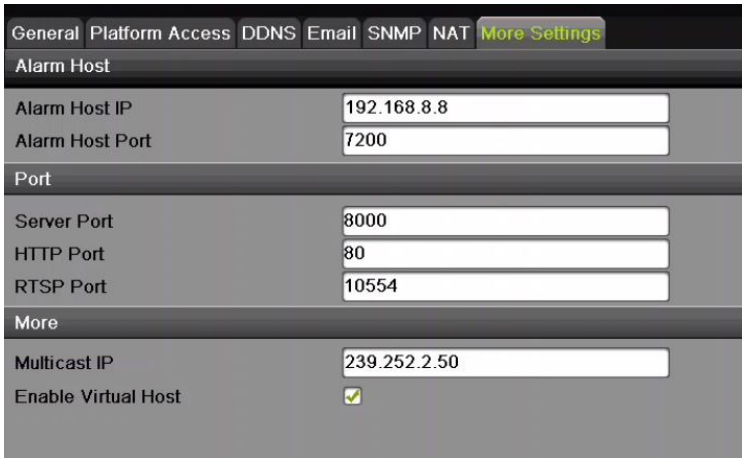


Figure 180 Configure More Settings

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

12.2.8. Configuring HTTPS Port

HTTPS authenticates 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 the port number is set to 443 and the IP address is set to 192.0.0.64, 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 button to log in to the device.
3. Enter the HTTPS settings interface, Configuration > Remote Configuration > Network Settings > HTTPS.
4. Create the self-signed certificate or authorized certificate.

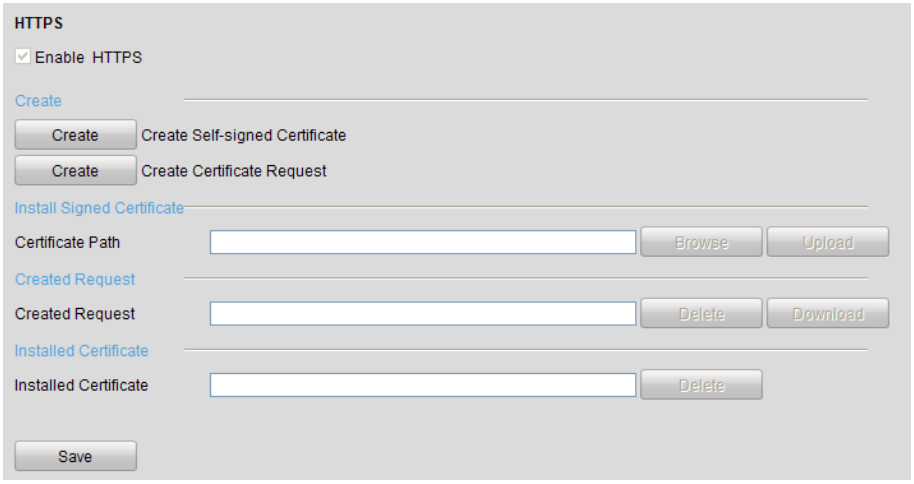


Figure 181 HTTPS Settings

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

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

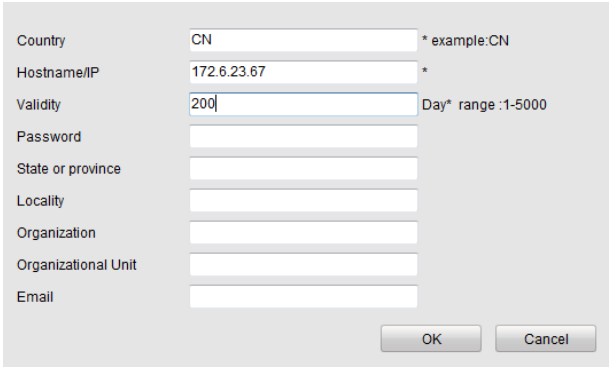


Figure 182 Create Self-signed Certificate

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

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

- **OPTION 2**: Create the authorized certificate

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

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

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

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

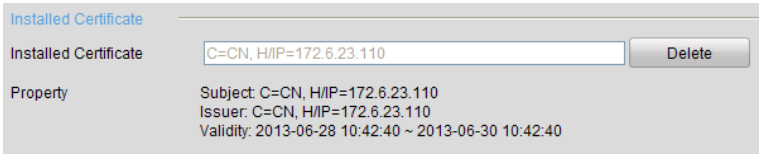


Figure 183 Installed Certificate Property

6. Check the checkbox to enable the HTTPS function.

7. Click the Save button to save the settings.

12.2.9. Configuring E-Mail

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

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

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

2. Set the IPv4 Address, IPv4 Subnet Mask, IPv4 Gateway, and the Preferred DNS Server in the Network Settings menu, as shown in Figure 184.

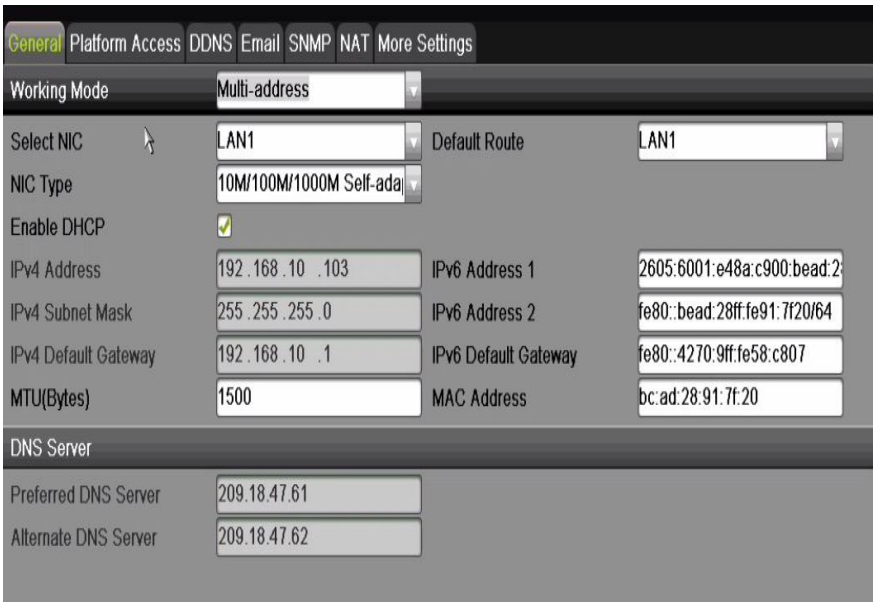


Figure 184 Network Settings Interface

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

4. Select the e-mail tab to enter the Email Settings interface.

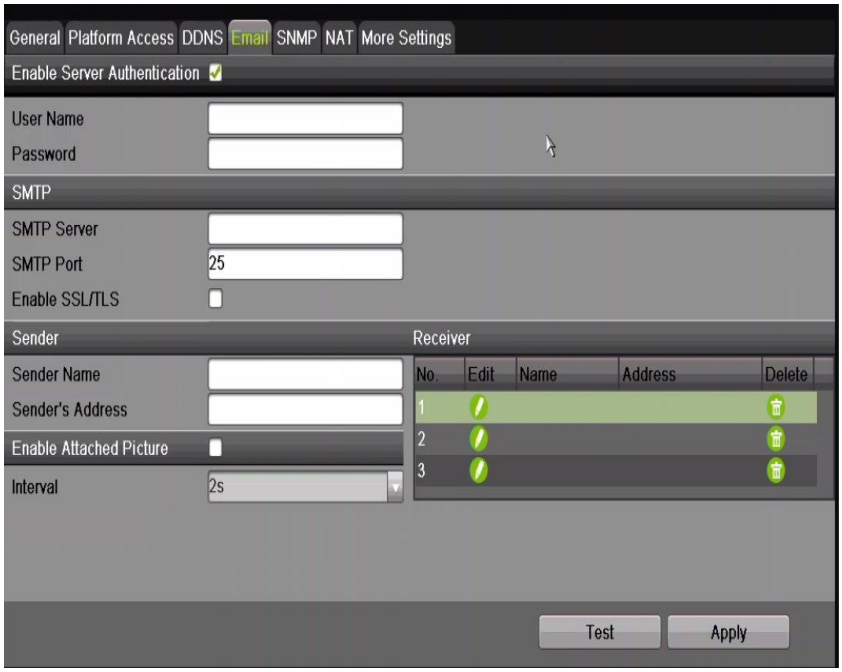


Figure 185 Email Settings Interface

5. Configure the following e-mail settings:

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

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

6. Click **Apply** button to save the e-mail settings.
7. Click **Test** button to test whether your e-mail settings work.

12.2.10. Configuring NAT

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

12.2.10.1 UPnP™

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

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

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

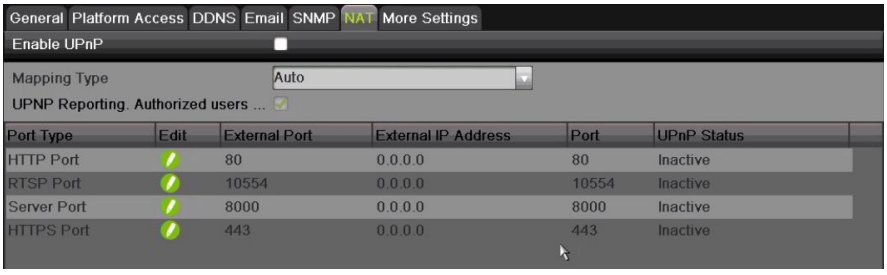


Figure 186 UPnP™ Settings Interface

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

- **OPTION 1:** Auto

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

  1) Select **Auto** in the Mapping Type drop-down list.

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

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

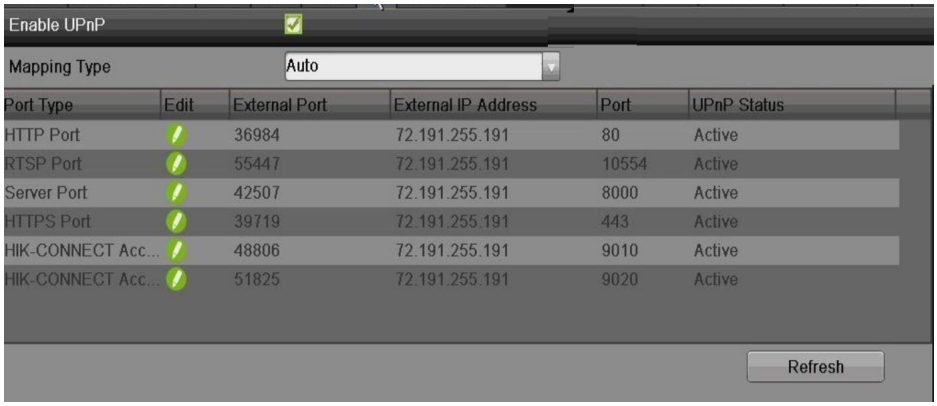


Figure 187 UPnP™ Settings Finished-Auto

- **OPTION 2:** Manual

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

  1) Select **Manual** in the Mapping Type drop-down list.

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

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

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

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

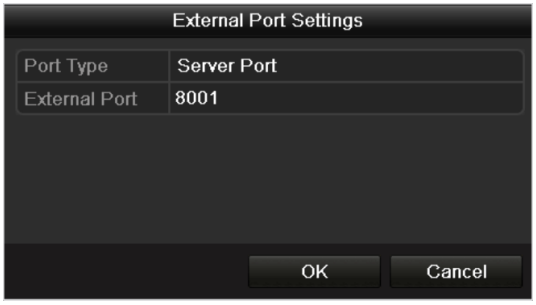


Figure 188 External Port Settings Dialog Box

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

6. Click **Refresh** button to get the latest status of the port mapping.

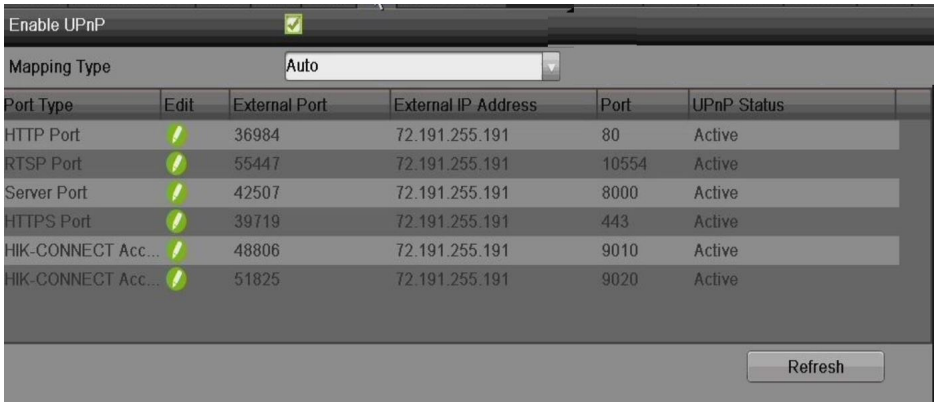


Figure 189 UPnP™ Settings Finished-Manual

12.2.10.2 Manual Mapping

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

NOTE: Make sure the router supports the configuration of internal port and external port in the Forwarding interface.

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

2. Select the **NAT** tab to enter the port mapping interface.

3. Leave the Enable UPnP checkbox unchecked.

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

NOTE: The value of the RTSP port No. should be 554 or between 1024 and 65535, while the value of the other ports should be between 1 and 65535, and the values must

be different from each other. If multiple devices are configured for the UPnP™ settings under the same router, the value of the port No. for each device should be unique.

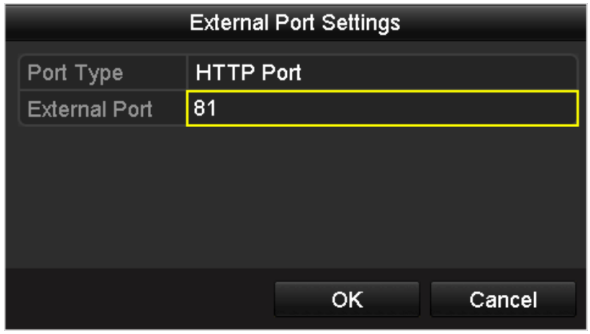


Figure 190 External Port Settings Dialog Box

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

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

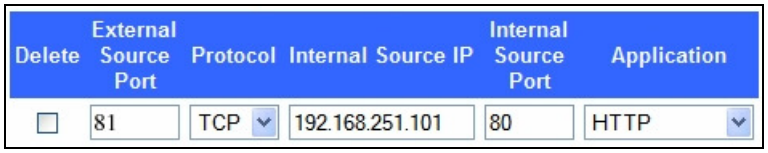


Figure 191 Setting Virtual Server Item

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

12.2.11. Configuring Virtual Host

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

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

1. Enter the Advanced settings interface, as shown in Figure 192, Configuration > Network > Advanced Settings > Other.

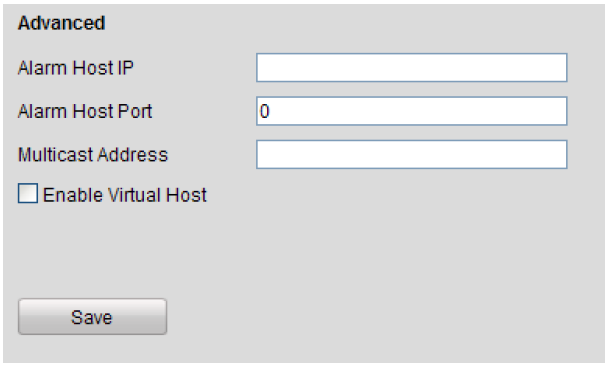


Figure 192 Advanced Settings Interface

2. Check the **Enable Virtual Host** checkbox.

3. Click the **Save** button to save the setting.

4. Enter the NVR's IP camera management interface. The Connect column appears on the right-most side of the camera list, as shown in **Error! Reference source not found.**, Configuration > Remote Configuration > Camera Management > IP Camera.

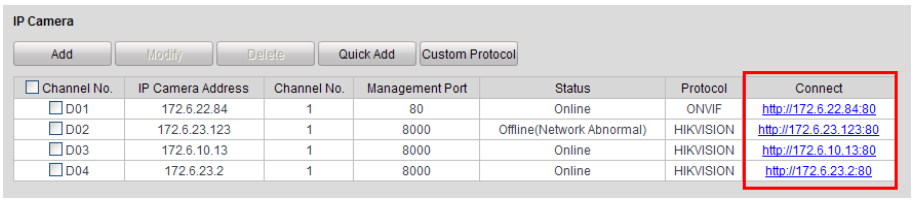


Figure 193 Connect to IP Camera

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

12.3 Checking Network Traffic

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

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

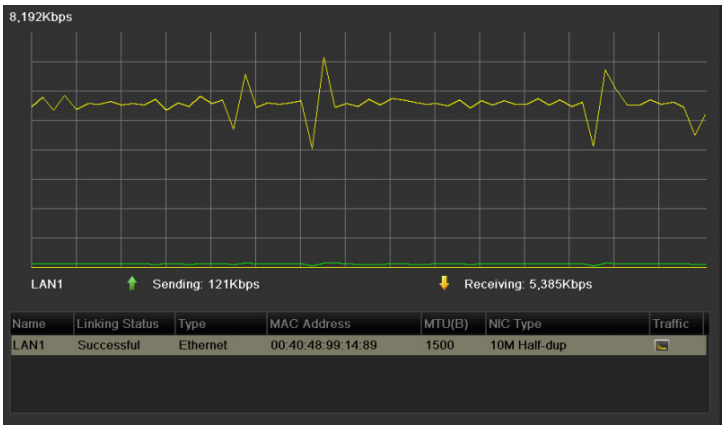


Figure 194 Network Traffic Interface

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

12.4 Configuring Network Detection

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

12.4.1. Testing Network Delay and Packet Loss

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

2. Click the **Network Detection** tab to enter the Network Detection menu, as shown in Figure 195.

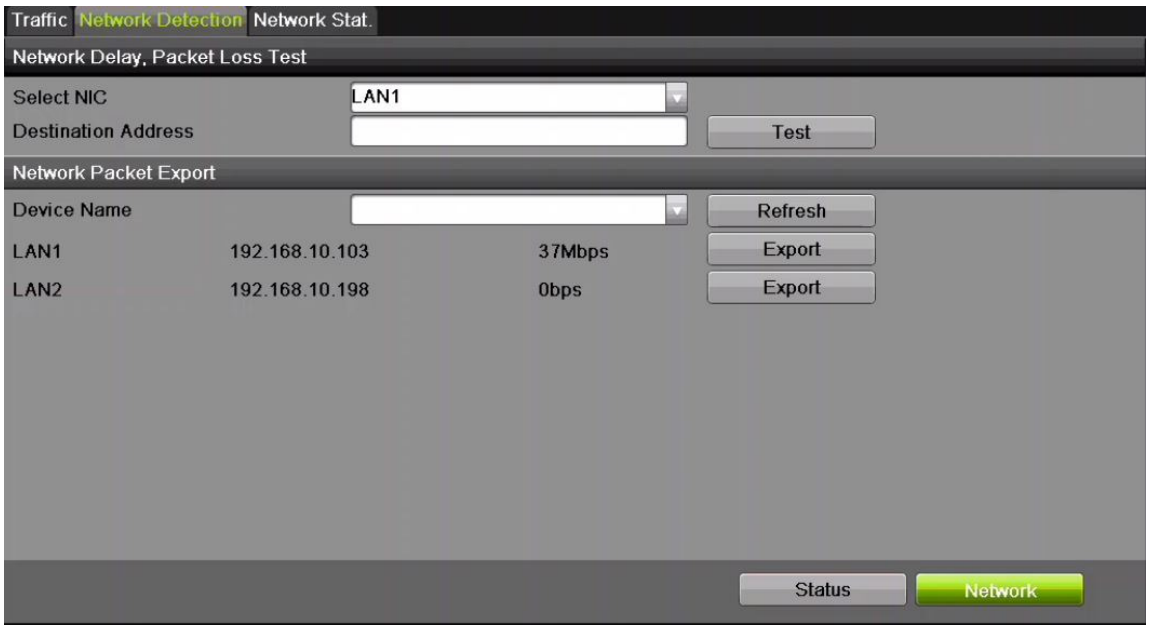


Figure 195 Network Detection Interface

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

4. Click **Test** button to start testing network delay and packet loss. The testing result pops up in the window. If the testing fails, the error message box will pop up as well. Refer to Figure 196.

Figure 196 Testing Result of Network Delay and Packet Loss

12.4.2. Exporting Network Packet

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

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

2. Click the **Network Detection** tab to enter the Network Detection interface.

3. Select the backup device from the Device Name drop-down list, as shown in Figure 197.

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

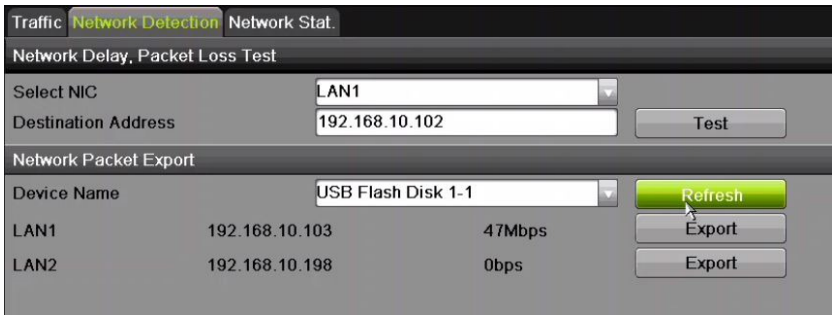


Figure 197 Export Network Packet

4. Click **Export** button to start exporting.

5. After exporting is complete, click **OK** to finish the packet export, as shown in Figure 198.

Figure 198 Packet Export Attention

NOTE: Up to 1 MB of data can be exported at a time.

12.4.3. Checking the Network Status

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

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

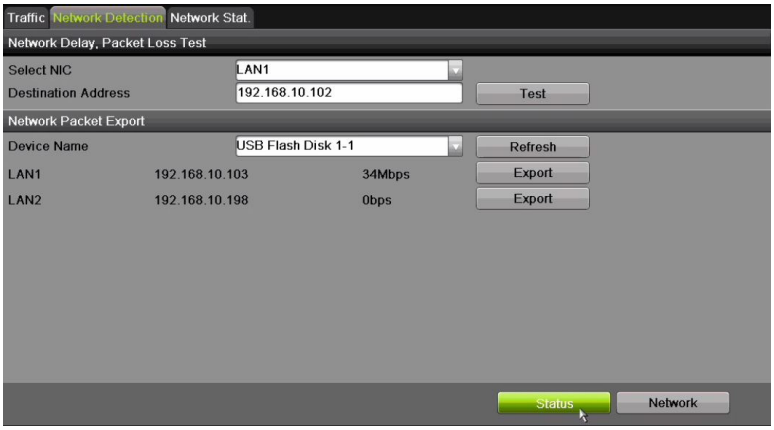


Figure 199 Network Status Checking

2. If the network is normal, the following message box appears. If the message box appears with information other than this, click the **Network** button to show the network parameters quick setting interface.

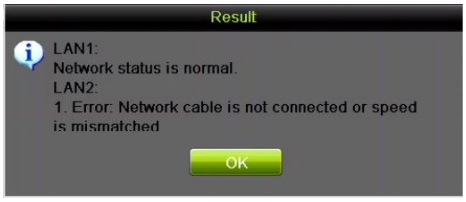


Figure 200 Network Status Checking Result

12.4.4. Checking Network Statistics

Check the network status to obtain NVR's real-time information.

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

2. Choose the **Network Stat.** tab.

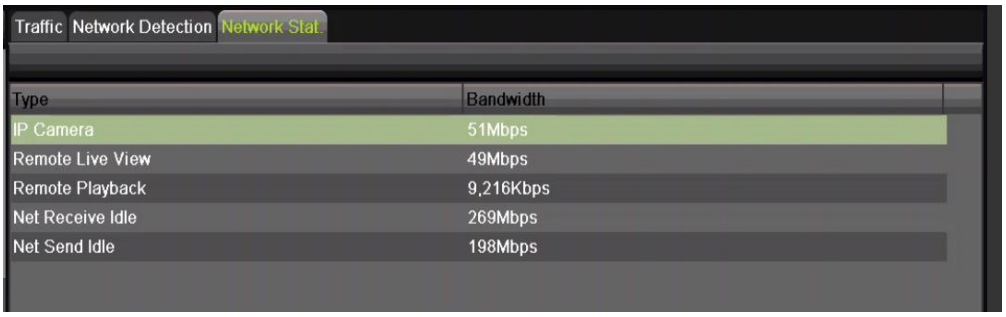


Figure 201 Network Stat. Interface

3. Check the bandwidth of IP Camera, bandwidth of Remote Live View, bandwidth of Remote Playback, bandwidth of Net Receive Idle, and bandwidth of Net Send Idle.

4. Click **Refresh** to get the newest status.

Chapter 13 RAID

This chapter applies to DS-9600NI-I8 NVRs.

13.1 Configuring Array

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 NVR supports software-based disk array. You can enable the RAID function at your demand.

NOTE: DS-9600NI-I8 Series NVRs support RAID0, RAID1, RAID5, RAID6, and RAID 10 array types.

13.1.1. Before You Start

Install the HDD(s) properly and 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.

13.1.2. Introduction

The NVR can store the data (such as record, picture, log information) in the HDD only after you have created the array or you have configured a network HDD (refer to Chapter14.2 Managing Network HDD). Our device provides two ways for creating an array, including one-touch configuration and manual configuration. The following flow chart shows the process of creating an array.

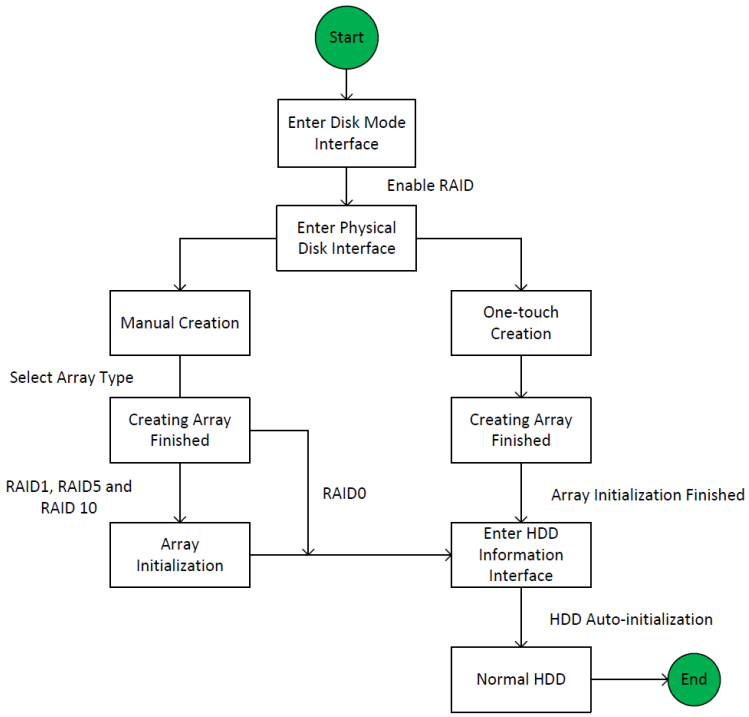


Figure 202 RAID Working Flow

13.1.3. Enable RAID

Perform the following steps to enable the RAID function, or the disk array cannot be created.

- **OPTION 1:** Enable the RAID function in the Wizard when the device starts up, refer to step 7 of Chapter 2.2.
- **OPTION 2:** Enable the RAID function in the HDD Management Interface.

1. Enter the disk mode configuration interface, Menu > HDD > Advanced.

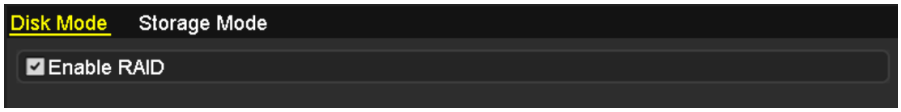


Figure 203 Enable RAID Interface

2. Check the checkbox of **Enable RAID**.
3. Click the **Apply** button to save the settings.

13.1.4. One-Touch Configuration

Through one-touch configuration, you can quickly create the disk array. By default, the array type to be created is RAID 5.

NOTE: Before You Start. The RAID function should be enabled, refer to Section 13.1.3.

As the default array type is RAID 5, please install at least three HDDs in your device.

If more than 10 HDDs are installed, two arrays can be configured.

1. Enter the RAID configuration interface, Menu > HDD > RAID.

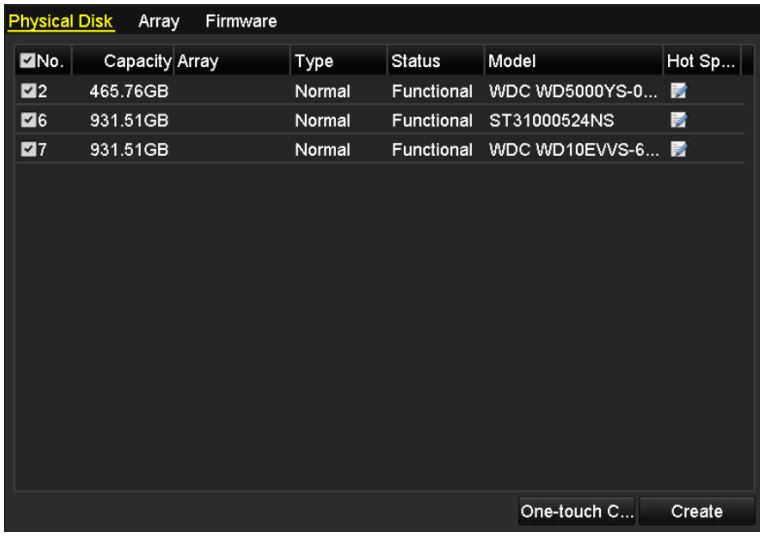


Figure 204 Physical Disk Interface

2. Check the corresponding HDD No. checkbox to select it.

3. Click the **One-touch Create** button to enter the One-touch Array Configuration interface.

Figure 205 One-Touch Array Configuration

4. Edit the array name in the **Array Name** text filed and click **OK** button to start configuring array.

NOTE: If you install four HDDs or above 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 when the array is abnormal.

5. When the array configuration is done, click the **OK** button in the pop-up message box to finish.

6. You can 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.

Figure 206 Array Settings Interface

7. A created array displays as an HDD in the HDD information interface.

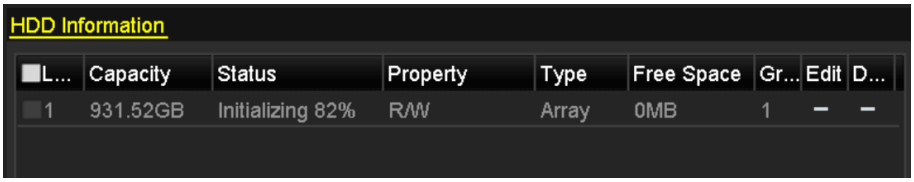


Figure 207 HDD Information Interface

13.1.5. Manually Creating Array

You can manually create the array of RAID 0, RAID 1, RAID 5, RAID6 and RAID 10.

NOTE: In this section, we take RAID 5 as an example to describe manually configuring arrays and virtual disks.

1. Enter the Physical Disk Settings interface, Menu > HDD > RAID > Physical Disk.

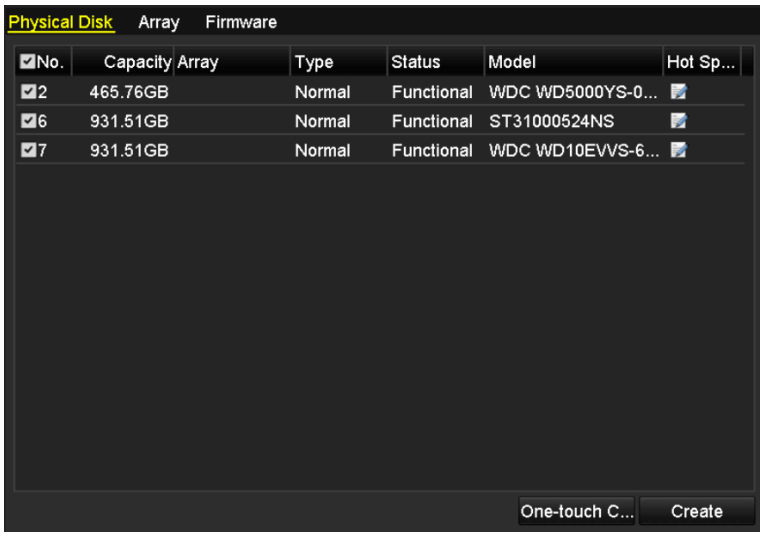


Figure 208 Physical Disk Settings Interface

2. Click Create button to enter the Create Array interface.

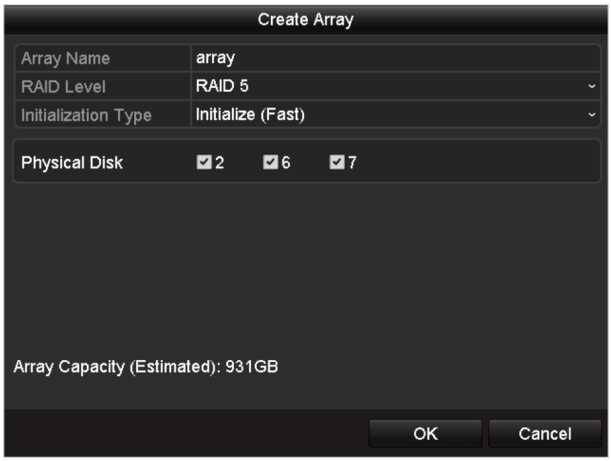


Figure 209 Create Array Interface

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 that you want to configure array.

   NOTES: 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 4 to 16.

4. Click OK button to create 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.

Figure 210 Error Message Box

5. You can click Array tab to view the successfully created array.

Figure 211 Array Settings Interface

13.2 Rebuilding Array

The array working status includes Functional, Degraded, and Offline. By viewing the array status, you can take immediate and proper maintenance of the disks to ensure high data security and reliability.

If there is no disk loss in the array, the working status will be Functional; if the number of lost disks has exceeded the limit, the working status 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.

13.2.1. Before You Start

Make sure the hot spare disk is configured.

1. Enter the Physical Disk Settings interface to configure the hot spare disk.

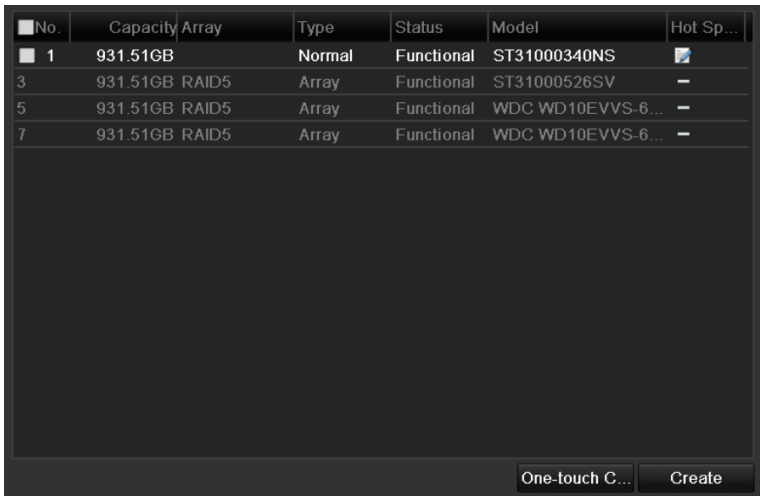


Figure 212 Physical Disk Settings Interface

2. Select a disk and click to set it as the hot spare disk.

NOTE: Only global hot spare mode is supported.

13.2.2. Automatically Rebuilding Array

When the virtual disk is in Degraded status, the device can rebuild 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 > HDD > RAID > Array. The array status is Degraded. Since the hot spare disk is configured, the system will automatically use it to start rebuilding,

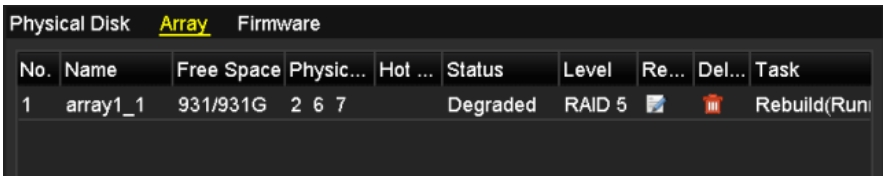


Figure 213 Array Settings Interface

NOTE: If there is no hot spare disk after rebuilding, it is recommended to install a HDD into the device and set it as a hot spare disk to ensure high security and reliability of the array.

13.2.3. Manually Rebuilding Array

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 > HDD > RAID > Array. In this example, disk 3 is lost.

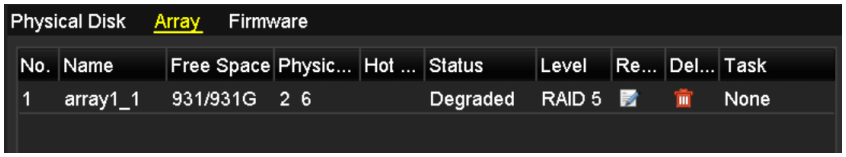


Figure 214 Array Settings Interface

2. Click Array tab to back 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.

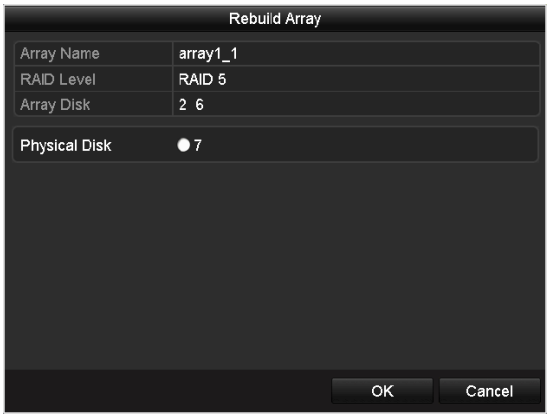


Figure 215 Rebuild Array Interface

3. Select the available physical disk and click OK button to confirm rebuilding the array.
4. When “Do not unplug the physical disk when it is under rebuilding” message appears, click OK.
5. Enter the Array Settings interface to view the rebuilding status.
6. After rebuilding is successfully, the array and virtual disk will restore to Functional.

13.3 Deleting Array

NOTE: Deleting the array will delete all data in the array.

1. Enter the Array Settings interface, Menu > HDD > RAID > Array.

Figure 216 Array Settings Interface

2. Select an array and click to delete the array.

Figure 217 Confirm Array Deletion

3. In the pop-up message box, click Yes button to confirm the array deletion.

13.4 Checking and Editing Firmware

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 version, maximum physical disk quantity, maximum array quantity, auto-rebuild status, etc.

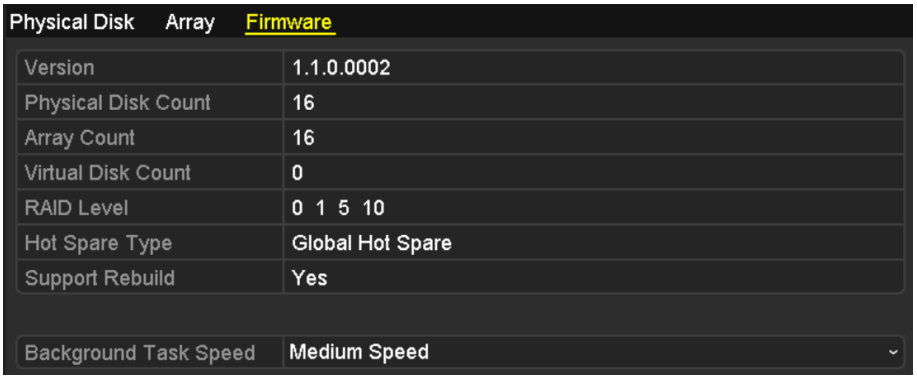


Figure 218 Firmware Interface

2. Set the Background Task Speed in the drop-down list.

3. Click the Apply button to save the settings.

Chapter 14 HDD Management

14.1 Initializing HDDs

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

NOTE: A message box appears when the NVR starts up if there are any uninitialized HDDs. Click Yes button to initialize it immediately, or perform the following steps.

Figure 219 Message Box of Uninitialized HDD

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

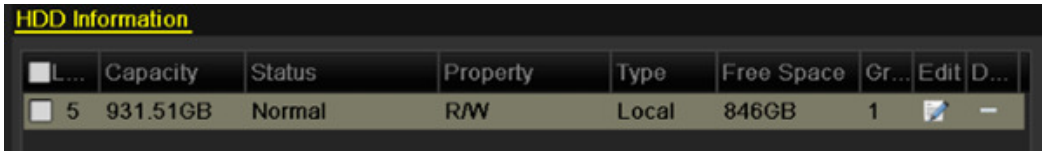


Figure 220 HDD Information Interface

2. Select HDD to be initialized.

3. Click the Init button.

Figure 221 Confirm Initialization

4. Select the OK button to start initialization.

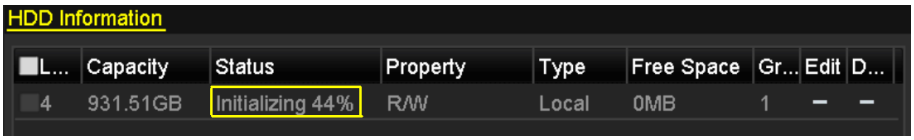


Figure 222 Status changes to Initializing

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

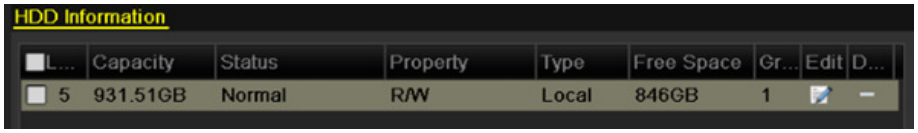


Figure 223 HDD Status Changes to Normal

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

14.2 Managing Network HDD

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

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

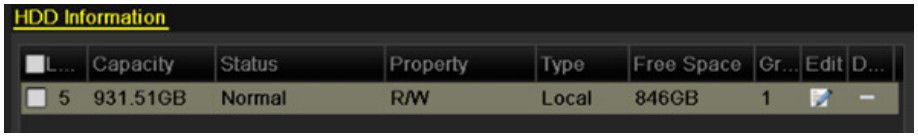


Figure 224 HDD Information Interface

2. Click the Add button to enter the Add NetHDD interface, as shown in Figure 225.

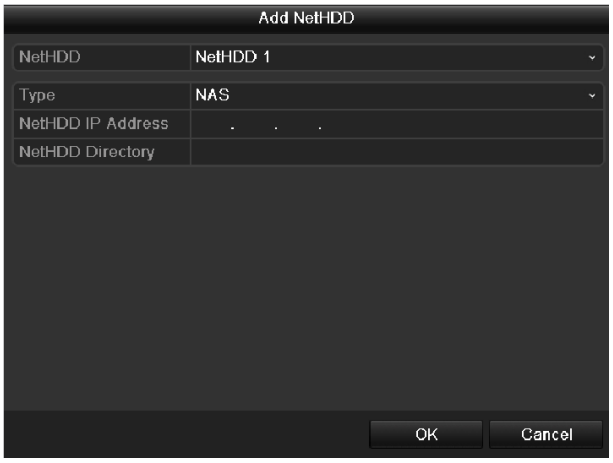


Figure 225 HDD Information Interface

3. Add the allocated NetHDD.

4. Select the type to NAS or IP SAN.

5. Configure the NAS or IP SAN settings.

- **Add NAS Disk**

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

  2) Click the **Search** button to search the available NAS disks.

  3) Select the NAS disk from the list shown below (or, manually enter the directory in the NetHDD Directory text field).

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

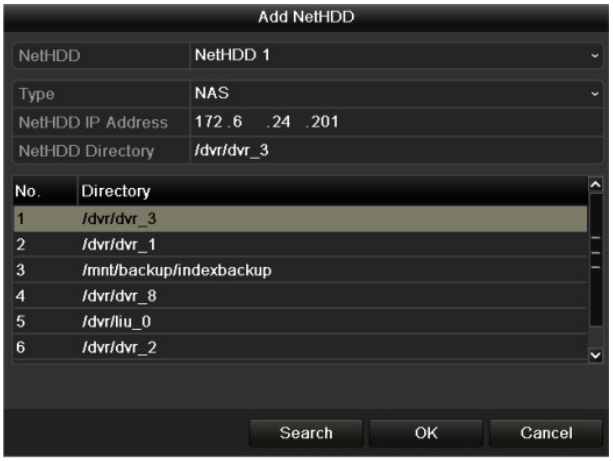


Figure 226 Add NAS Disk

- **Add IP SAN:**

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

  2) Click the **Search** button to search the available IP SAN disks.

  3) Select the IP SAN disk from the list shown below.

  4) Click the **OK** button to add the selected IP SAN disk.

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

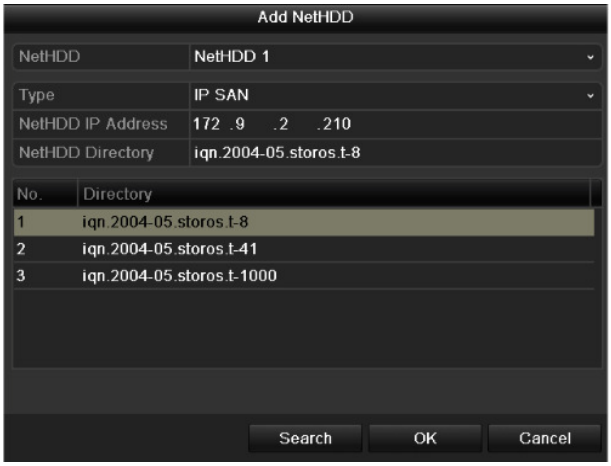


Figure 227 Add IP SAN Disk

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

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

Figure 228 Initialize Added NetHDD

14.3 Managing eSATA

When there is an external eSATA device connected to the NVR, you can configure the eSATA for the use of Record/Capture or Export, and you can manage the eSATA in the NVR.

1. Enter the Advanced Record Settings interface, Menu > Record > Advanced.
2. Select the eSATA type to Export or Record/Capture from the drop-down list of eSATA.

   - **Export:** Use the eSATA for backup. Refer to Backup using eSATA HDDs in Chapter *Backing Up by Normal Video/Picture* Search for operating instructions.
   - **Record/Capture:** Use the eSATA for record/capture. Refer to the following steps for operating instructions.

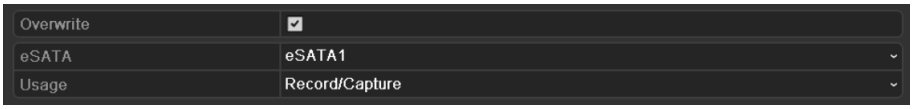


Figure 229 Set eSATA Mode

3. When the eSATA type is selected as Record/Capture, enter the HDD Information interface, Menu > HDD > General.

4. Edit the selected eSATA property, or initialize it as required.

NOTE: Two storage modes can be configured for the eSATA when it is used for Record/Capture. Refer to *Chapter Managing HDD Group* and *Chapter Configuring Quota Mode* for details.

Figure 230 Initialize Added eSATA

14.4 Managing HDD Group

14.4.1. Setting HDD Groups

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

1. Enter the Storage Mode interface, Menu > HDD > Advanced > Storage Mode.
2. Set the **Mode** to Group, as shown in Figure 231.

Figure 231 Storage Mode Interface

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

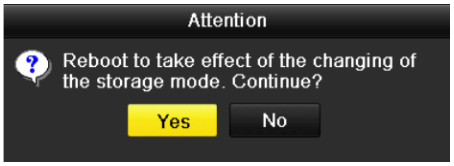


Figure 232 Attention for Reboot

4. Click the **Yes** button to reboot the device to activate the changes.
5. After rebooting the device, enter the HDD Information interface, Menu > HDD > General.
6. Select HDD from the list and click the icon to enter the Local HDD Settings interface, as shown in Figure 233.

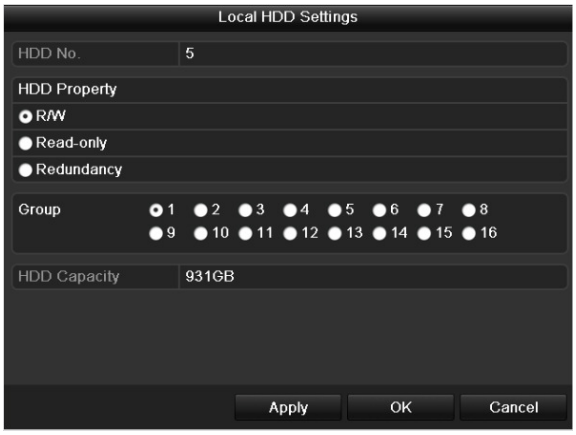


Figure 233 Local HDD Settings Interface

7. Select the Group number for the current HDD.

   NOTE: The default group No. for each HDD is 1.

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

Figure 234 Confirm HDD Group Settings

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

14.4.2. Setting HDD Property

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

2. Select HDD from the list and click the icon to enter the Local HDD Settings interface, as shown in Figure 235.

Figure 235 Set HDD Property

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

NOTE: At least two hard disks must be installed in the NVR to set an HDD to Redundancy, with one HDD with R/W property.

14.5 Configuring Quota Mode

Each camera can be configured with allocated quota for storing recorded files or captured pictures.

1. Enter the Storage Mode interface, Menu > HDD > Advanced.
2. Set the Mode to Quota, as shown in Figure 236.

NOTE: Reboot the NVR to enable the changes.

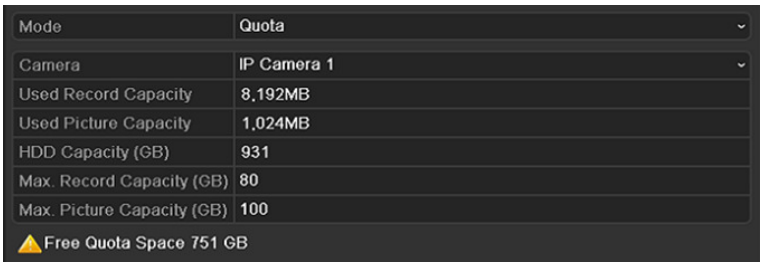


Figure 236 Storage Mode Settings Interface

3. Select a camera for which you want to configure quota.
4. Enter the storage capacity in the Max. Record Capacity (GB) and Max. Picture Capacity (GB) text fields, as shown in Figure 237.

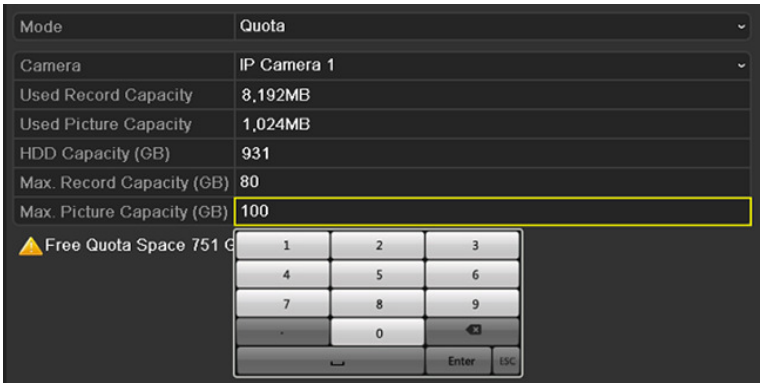


Figure 237 Configure Record/Picture Quota

5. Copy the quota settings of the current camera to other cameras if required. Click the Copy button to enter the Copy Camera menu, as shown in Figure 238.

Figure 238 Copy Settings to Other Camera(s)

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

7. Click the OK button to finish the Copy settings and go back to the Storage Mode interface.

8. Click the Apply button to apply the settings.

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

14.6 Configuring Disk Clone

If the S.M.A.R.T. detection result declares the HDD is abnormal, you can choose to clone all the data on the HDD to an inserted eSATA disk manually. Refer to *Chapter 12.8 HDD Detection* for details of S.M.A.R.T. detection.

NOTE: Before starting, connect an eSATA disk to the device.

1. Enter the HDD Advanced Setting interface, Menu > HDD > Advanced.

2. Click the Disk Clone tab to enter the disk clone configuring interface.

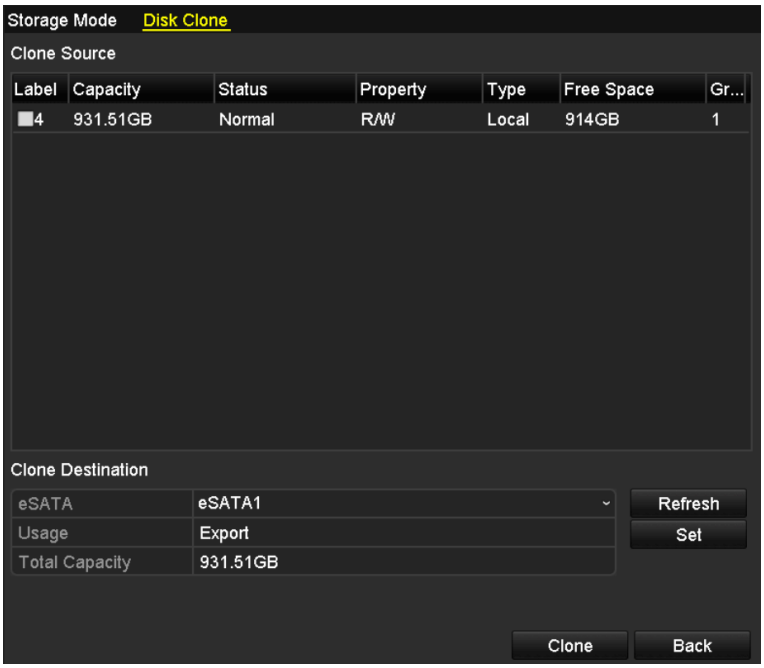


Figure 239 Disk Clone Configuration Interface

3. eSATA Usage must be set to Export. If not, click **Set** button to set it. Choose Export and click the **OK** button.

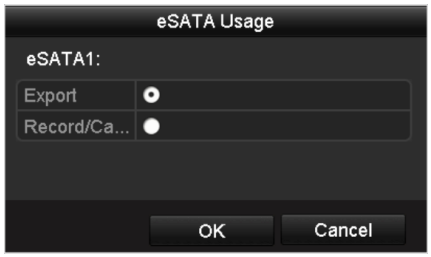


Figure 240 Setting eSATA Usage

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

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

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

Figure 241 Message Box for Disk Clone

6. Click the Yes button to continue.
7. You can check the clone progress in the HDD status.

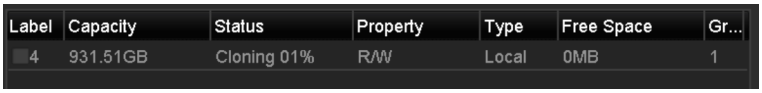


Figure 242 Check Disk Clone Progress

14.7 Checking HDD Status

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

- Checking HDD Status in HDD Information Interface
  1. Enter the HDD Information interface, Menu > HDD > General.
  2. Check the status of each HDD displayed on the list.

Figure 243 View HDD Status (1)

NOTE: If the HDD status is *Normal* or *Sleeping*, it works normally. If the status is *Uninitialized* or *Abnormal*, initialize the HDD before use. If the HDD initialization fails, replace HDD.

- Checking HDD Status in System Info Interface
  1. Enter the System Information interface, Menu > Maintenance > System Info.
  2. Click the HDD tab to view the status of each HDD displayed on the list, as shown in Figure 244.

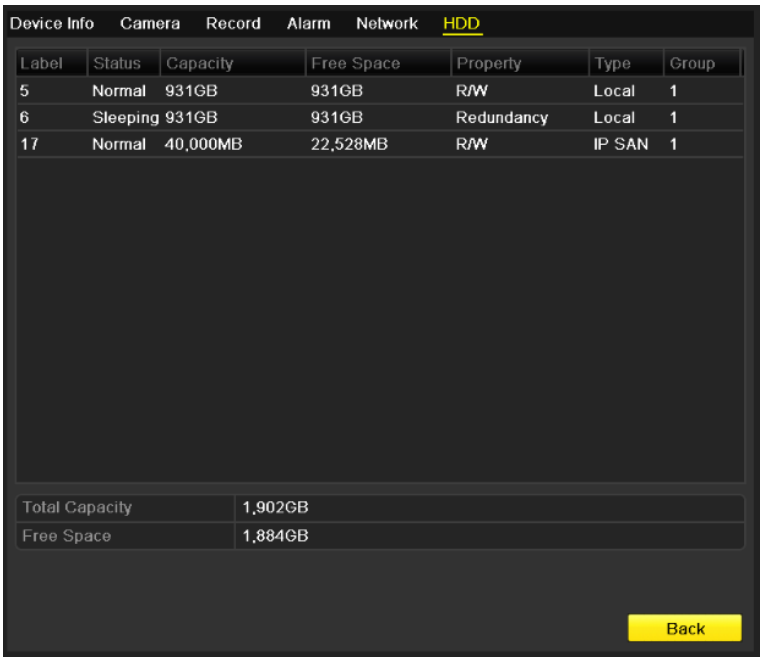


Figure 244 View HDD Status (2)

14.8 HDD Detection

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

14.8.1. S.M.A.R.T. Settings

1. Enter the S.M.A.R.T Settings interface, Menu > Maintenance > HDD Detect.
2. Select the HDD to view its S.M.A.R.T. information list, as shown in Figure 245. The related S.M.A.R.T. information is shown on the interface.

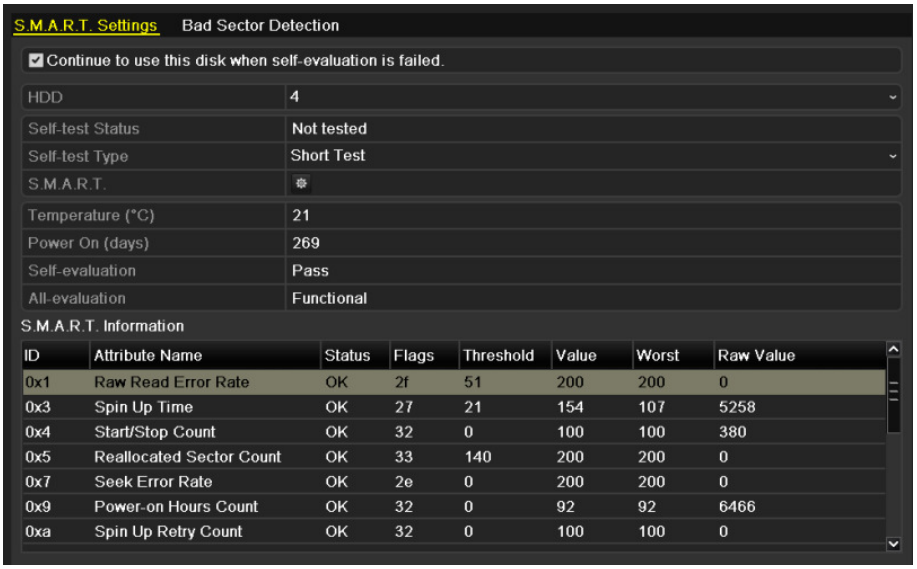


Figure 245 S.M.A.R.T. Settings Interface

3. Choose the self-test types as Short Test, Expanded Test, or Conveyance Test.

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

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

14.8.2. Bad Sector Detection

1. Click the Bad Sector Detection tab.

2. Select the HDD No. in the drop-down list you want to configure, and choose All Detection or Key Area Detection as the detection type.

3. Click the **Detect** button to start the detection.

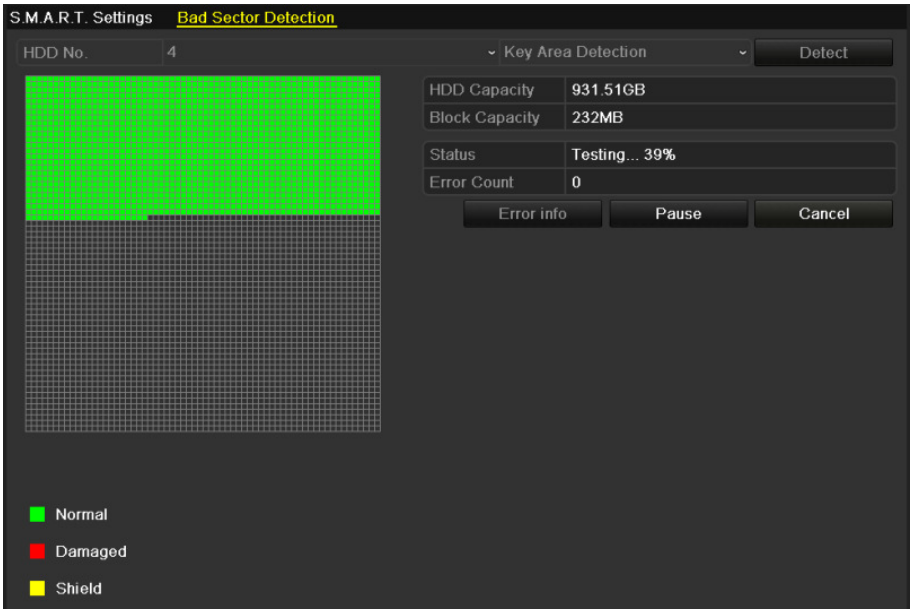


Figure 246 Bad Sector Detection

4. Click **Error info** button to see the detailed damage information.

NOTE: You can also pause/resume, or cancel the detection.

14.9 Configuring HDD Error Alarms

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

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

2. Select the Exception Type to HDD Error from the drop-down list.

3. Click the checkbox(s) below to select the HDD error alarm type(s), as shown in Figure 247.

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

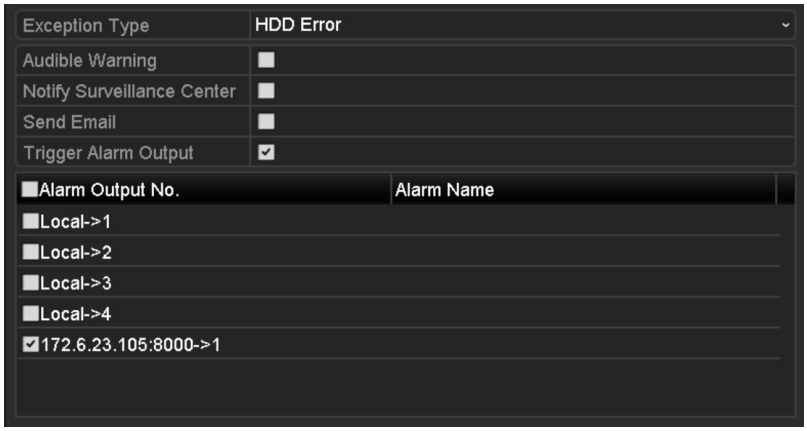


Figure 247 Configure HDD Error Alarm

4. When the Trigger Alarm Output is selected, you can also select the alarm output to be triggered from the list below.

5. Click the Apply button to save the settings.

Chapter 15 Camera Settings

15.1 Configuring OSD Settings

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

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

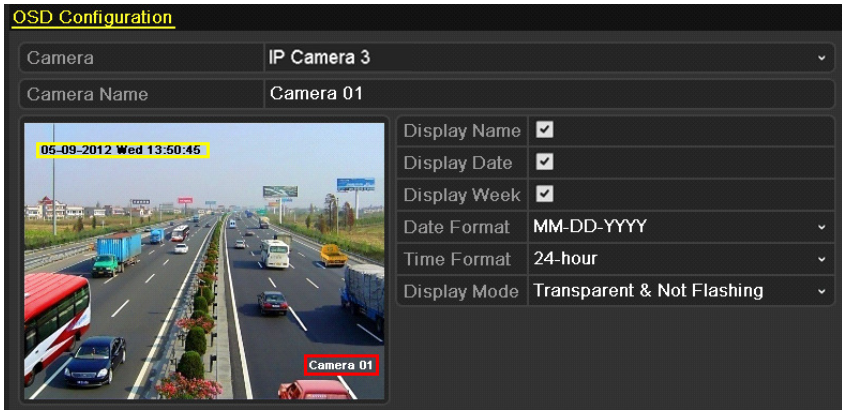


Figure 248 OSD Configuration Interface

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

15.2 Configuring Privacy Mask

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

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

Figure 249 Privacy Mask Settings Interface

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

   NOTE: Up to four privacy mask zones can be configured, and the size of each area can be adjusted.

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

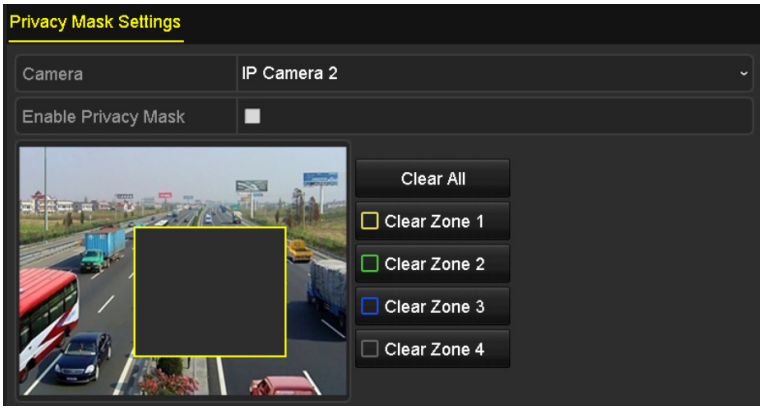


Figure 250 Set Privacy Mask Area

6. Click the Apply button to save the settings.

15.3 Configuring Video Parameters

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

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

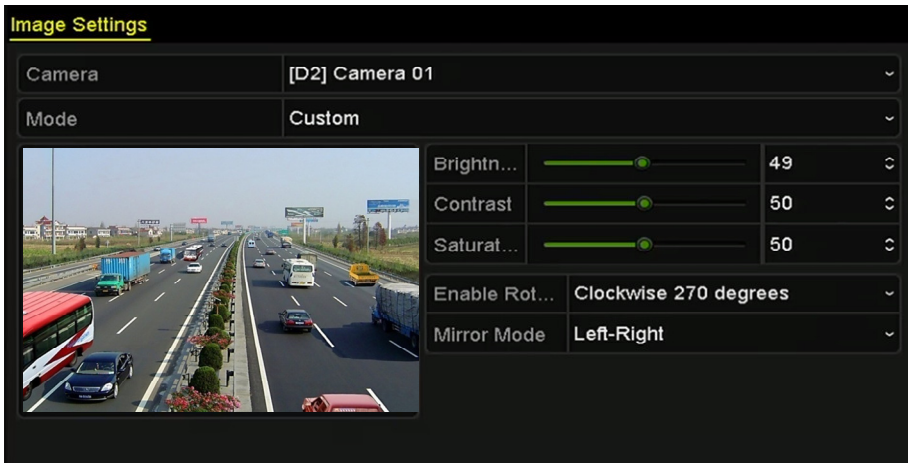


Figure 251 Image Settings Interface

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

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

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

6. Click the Apply button to save the settings.

Chapter 16 NVR Management and Maintenance

16.1 Viewing System Information

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

Figure 252 Device Information Interface

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

16.2 Searching and Exporting Log Files

The NVR operation, alarm, exception, and information can be stored in log files, which can be viewed and exported.

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

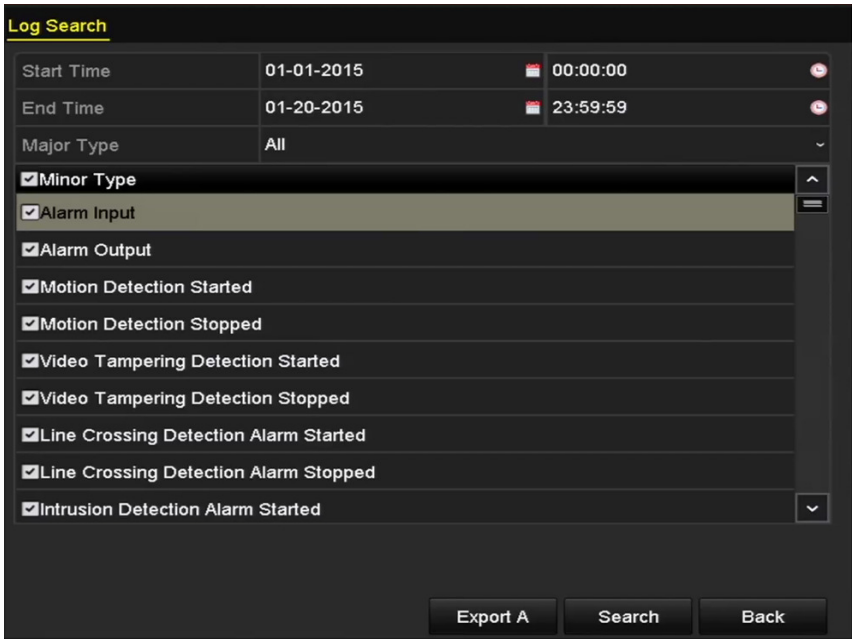


Figure 253 Log Search Interface

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

3. Click the Search button to start searching log files.

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

Figure 254 Log Search Results

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

5. Click the button of each log or double click it to view its detailed information, as shown in Figure 255. You can also click the button to view the related video files if available.

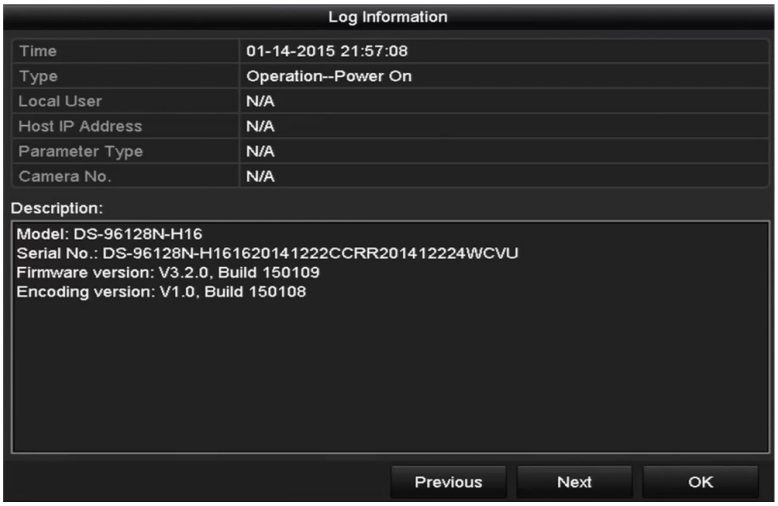


Figure 255 Log Details

6. To export the log files, click the Export button to enter the Export menu, as shown in Figure 256.

7. Click Export All on the Log Search interface to enter the Export interface, and all the system logs will be exported to the backup device.

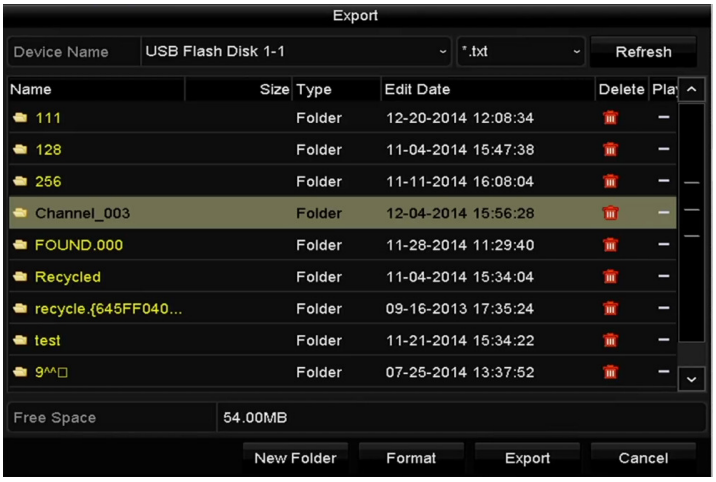


Figure 256 Export Log Files

8. Select the backup device from the Device Name drop-down list.

9. Select the format of the log files to be exported. Up to nine formats are selectable.

10. Click **Export** to export the log files to the selected backup device.

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

    NOTE: Connect the backup device to the NVR before running log export.

16.3 Importing/Exporting IP Camera Info

The added IP cameras' information can be exported to an Excel file and moved to a 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 copying the settings to other devices by importing the Excel file.

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

16.4 Importing/Exporting Configuration Files

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

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

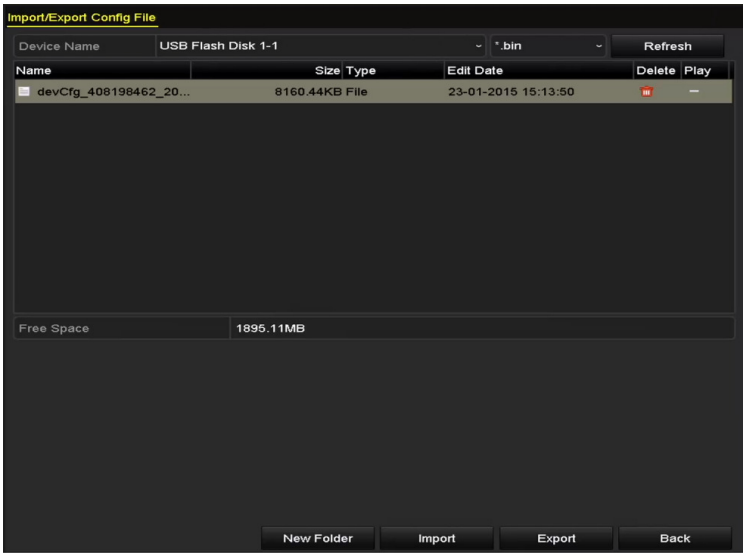


Figure 257 Import/Export Config File

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

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

16.5 Upgrading System

The NVR firmware can be upgraded through a local backup device or remote FTP server.

16.5.1. Upgrading by Local Backup Device

1. Connect your NVR to a local backup device containing the update firmware.
2. Enter the Upgrade interface, Menu > Maintenance > Upgrade.
3. Click the **Local Upgrade** tab to enter the local upgrade menu, as shown in Figure 258.

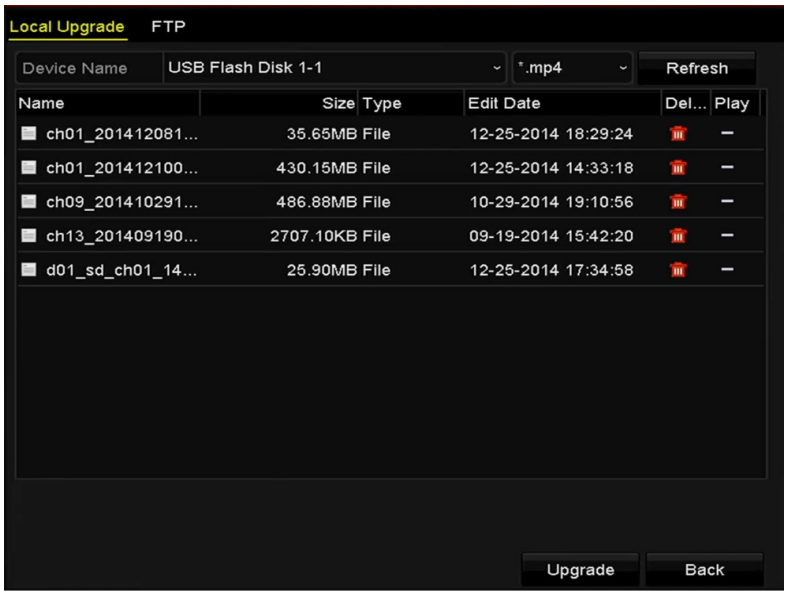


Figure 258 Local Upgrade Interface

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

16.5.2. Upgrading by FTP

NOTE: Before you start, ensure the network connection of the PC (running the FTP server) and the device is valid and correct. Run the FTP server on the PC and copy the firmware into the corresponding directory of your PC.

1. Enter the Upgrade interface, Menu > Maintenance > Upgrade.
2. Click the **FTP** tab to enter the local upgrade interface, as shown in Figure 259.

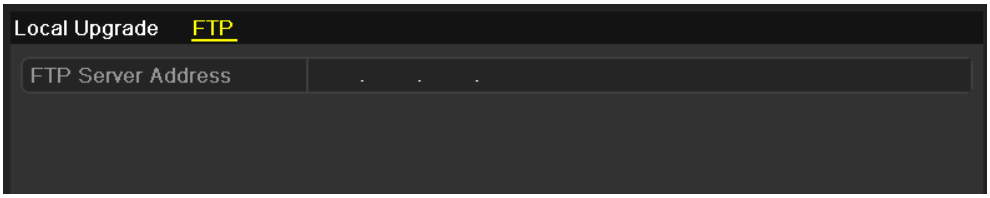


Figure 259 FTP Upgrade Interface

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

16.5.3. Restoring Default Settings

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

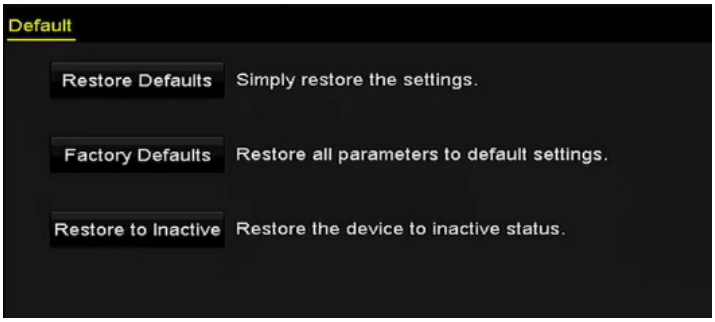


Figure 260 Restore Defaults

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

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

Chapter 17 Others

17.1 Configuring RS-232 Serial Port

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

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

1. Enter the RS-232 Settings interface, Menu > Configuration > RS-232.

Figure 261 RS-232 Settings Interface

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

17.2 Configuring General Settings

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

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

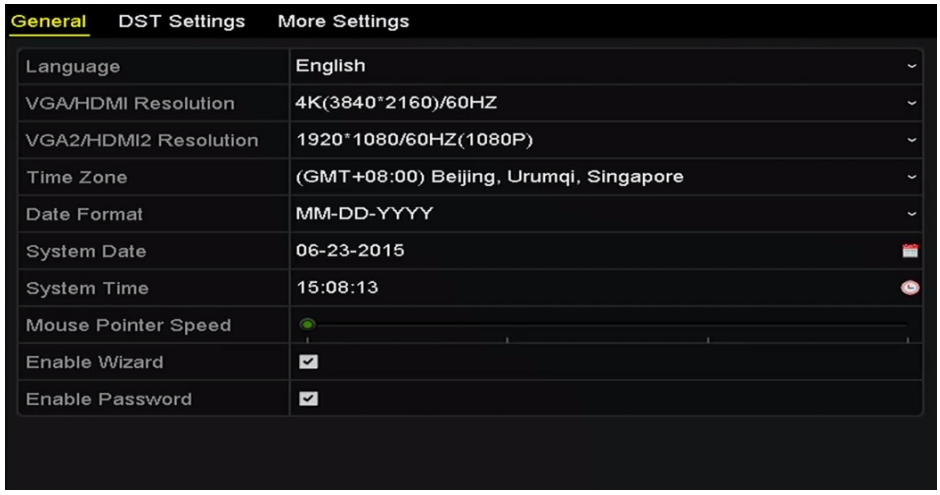


Figure 262 General Settings Interface (DS-9600NI)

Figure 263 General Settings Interface (DS-7700NI)

3. Configure the following settings:

   - **Language:** The default language used is English.
   - **Output Standard:** Set to NTSC or PAL, which must be the same as the video input standard.
   - **Resolution:** For DS-9600NI Series NVRs, you can configure the VGA/HDMI resolution and VGA2/HDMI 2 resolution. Up to 4K (3840 × 2160) resolution is selectable for VGA/HDMI output.

     For DS-7700NI Series NVRs, you can configure the VGA resolution and HDMI resolution respectively. Up to 4K (3840 × 2160) resolution is selectable for the HDMI output.

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

4. Click the Apply button to save the settings.

17.3 Configuring DST Settings

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

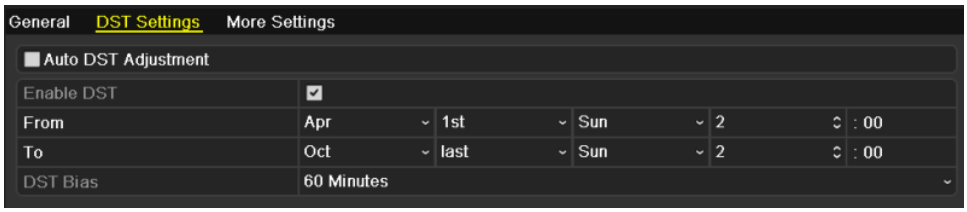


Figure 264 DST Settings Interface

3. Check the Auto DST Adjustment checkbox (or you can manually check the Enable DST checkbox, and then choose the date of the DST period).

17.4 Configuring More Settings

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

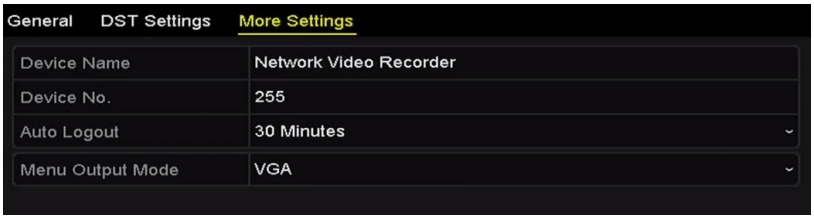


Figure 265 More Settings Interface

3. Configure the following settings:

   - **Device Name:** Edit the NVR name.
   - **Device No.:** Edit the NVR serial number. The Device No. can be set in the range of 1 to 255. The default No. is 255. This number is used for remote and keyboard control.
   - **Auto Logout:** Set timeout time for menu inactivity (e.g., when the timeout time is set to 5 Minutes, then the system will exit from the current operation menu to live view screen after 5 minutes of menu inactivity).
   - **Enable HDMI/VGA Simultaneous Output (DS-9600NI-I8 only):** By default, the HDMI and VGA interface video outputs can be operated separately. Set simultaneous output for HDMI and VGA by checking the option checkbox.
   - **Menu Output Mode:** Choose the menu display on different video outputs.

     For DS-9600NI-I8 Series NVRs, set the menu output mode to VGA/HDMI, VGA2/HDMI2.

     For DS-7700NI-I4 (/P) series NVRs, set the menu output mode to VGA, HDMI, or Auto. When the Auto option is selected and both HDMI and VGA outputs are connected, the device will detect and set HDMI as the menu output.

4. Click the Apply button to save the settings.

17.5 Managing User Accounts

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

17.5.1. Adding a User

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

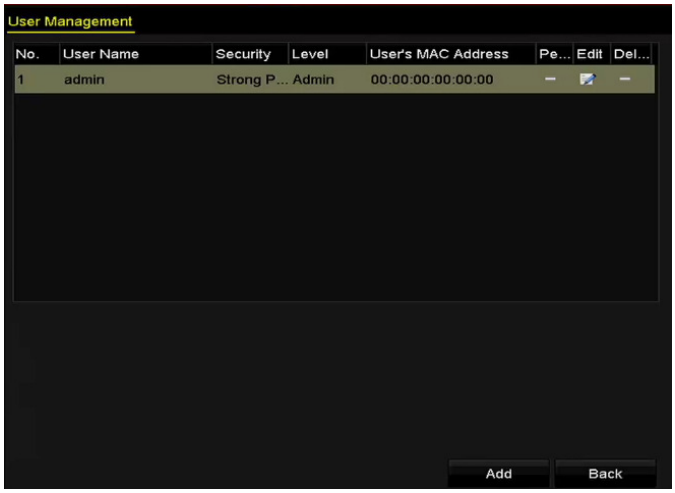


Figure 266 User Management Interface

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

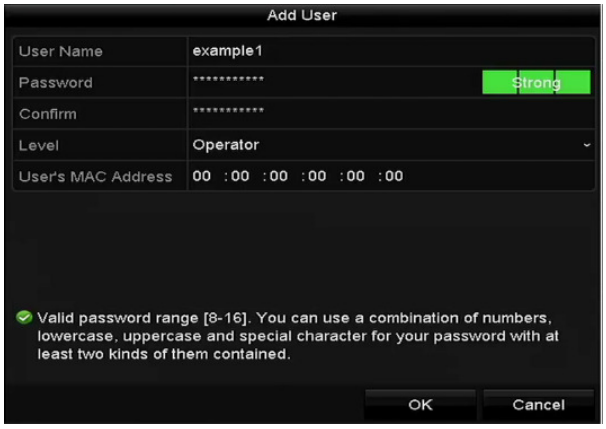


Figure 267 Add User Menu

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

   NOTE: New user name cannot be "admin" or "root."

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

     STRONG PASSWORD RECOMMENDED – We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including at least three in 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 high security systems, resetting the password monthly or weekly can better protect your product.

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

permissions.

- **Operator:** The *Operator* user level permissions include Two-way Audio in Remote Configuration and all operating permissions in Camera Configuration by default.
- **Guest:** A Guest user has no permission for Two-way Audio in Remote Configuration and has only local/remote playback in the Camera Configuration by default.
- **User's MAC Address:** The MAC address of the remote PC that logs onto the NVR. If it is configured and enabled, it allows only the remote user with this MAC address to access the NVR.

4. Click the **OK** button to save the settings and go back to the User Management interface. The added new user will be displayed on the list.

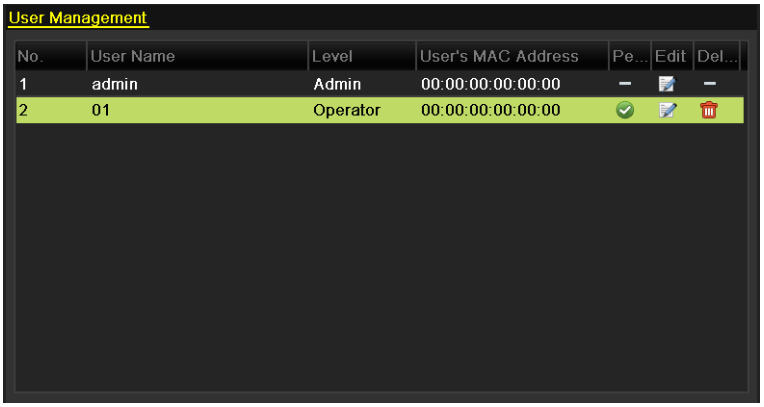


Figure 268 Added User Listed in User Management Interface

5. Select user from the list, then click the button to enter the Permission settings interface.

Figure 269 User Permission Settings Interface

6. Set the user permissions for Local Configuration, Remote Configuration, and Camera Configuration.

- Local Configuration
  - **Local Log Search:** Search and view NVR logs and system information.
  - **Local Parameters Settings:** Configure parameters, restore factory default parameters, and import/export configuration files.
  - **Local Camera Management:** Add, delete, and edit IP cameras.
  - **Local Advanced Operation:** Operate HDD management (initialize HDD, set HDD property), upgrade system firmware, clear I/O alarm output.
  - **Local Shutdown Reboot:** Shut down or reboot the NVR.
- Remote Configuration
  - **Remote Log Search:** Remotely view logs saved on the NVR.
  - **Remote Parameters Settings:** Remotely configure parameters, restore factory default parameters, and import/export configuration files.
  - **Remote Camera Management:** Remote add, delete, and edit IP cameras.
  - **Remote Serial Port Control:** Configure RS-232 and RS-485 port settings.
  - **Remote Video Output Control:** Send remote button control signal.
  - **Two-Way Audio:** Realize two-way radio between the remote client and the NVR.
  - **Remote Alarm Control:** Remotely arm (notify alarm and exception message to the remote client) and control the alarm output.
  - **Remote Advanced Operation:** Remotely operate HDD management (initialize HDD, set HDD property), upgrade system firmware, clear I/O alarm output.
  - **Remote Shutdown/Reboot:** Remotely shut down or reboot the NVR.
- Camera Configuration
  - **Remote Live View:** Remotely view live video of the selected camera(s).
  - **Local Manual Operation:** Locally start/stop manual recording and alarm output of selected camera(s).
  - **Remote Manual Operation:** Remotely start/stop manual recording and alarm output of selected camera(s).
  - **Local Playback:** Locally play back recorded files of selected camera(s).
  - **Remote Playback:** Remotely play back recorded files of selected camera(s).
  - **Local PTZ Control:** Locally control PTZ movement of selected camera(s).
  - **Remote PTZ Control:** Remotely control PTZ movement of selected camera(s).

- **Local Video Export:** Locally export recorded files of selected camera(s).

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

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

17.5.2. Deleting a User

1. Enter the User Management interface, Menu > Configuration > User.
2. Select the user to be deleted from the list, as shown in Figure 270.

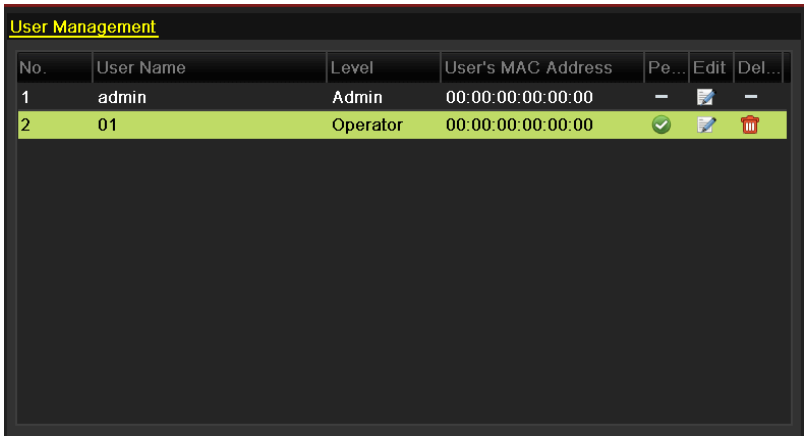


Figure 270 User List

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

17.5.3. Editing a User

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

1. Enter the User Management interface, Menu > Configuration > User.
2. Select the user to be edited from the list, as shown in Figure 271.
3. Click the icon to enter the Edit User interface, as shown in.

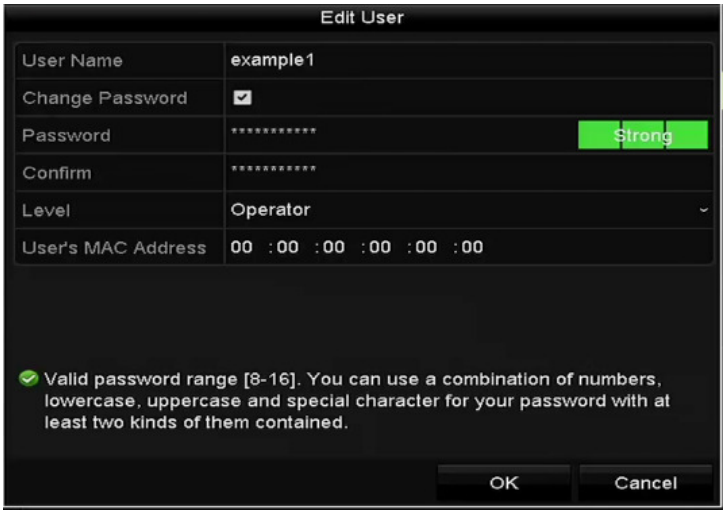


Figure 271 Edit User (Operator/Guest)

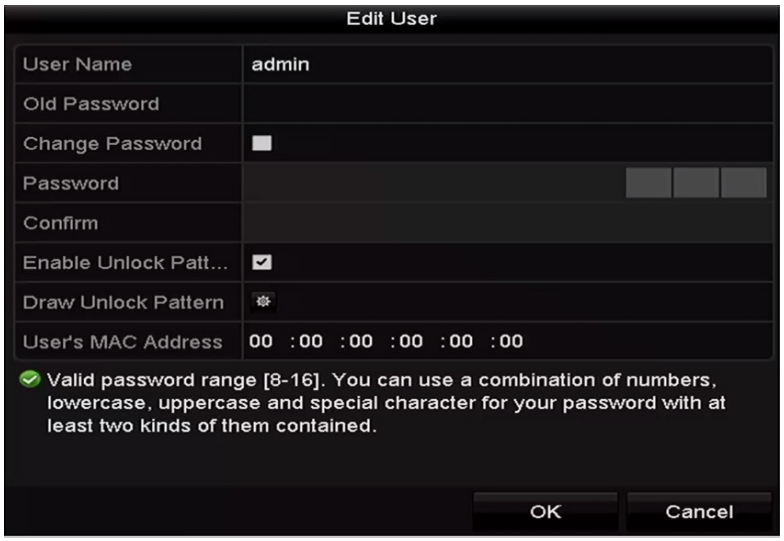


Figure 272 Edit User (admin)

4. Edit the password for the user.

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

   - **Admin** – You are allowed only to edit the password and MAC address. Check the **Change Password** checkbox if you want to change the password. Input the correct old password, then the new password in the **Password** text field, the press **Confirm**.

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

5. Edit the unlock pattern for the admin user account.

   1) Check the **Enable Unlock Pattern** checkbox to enable use of an unlock pattern when logging in to the device.

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

   NOTE: Refer to Chapter 2.3.1 Configuring the Unlock Pattern for detailed instructions.

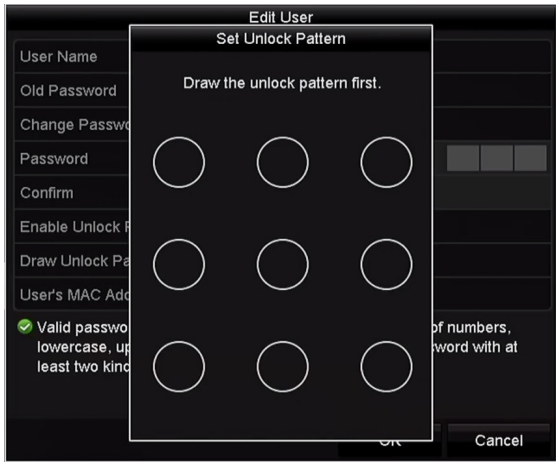


Figure 273 Set Unlock Patter for Admin User

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

6. For the **Operator** or **Guest** user account, you can also click the button on the user management interface to edit the permission.

Chapter 18 Appendix

18.1 Specifications

18.1.1. DS-96xxNI-I8

Model		DS-9632NI-I8	DS-9664NI-I8
Video/Audio Input	IP Video Input	32-ch	64-ch
		Up to 12 MP resolution	
	Two-Way Audio	1-ch, RCA (2.0 Vp-p, 1 k Ω)	
Network	Incoming Bandwidth	320 Mbps, or 200 Mbps (when RAID is enabled)	
	Outgoing Bandwidth	256 Mbps, or 200 Mbps (when RAID is enabled)	
	Remote Connection	128	
Video/Audio Output	Recording Resolution	12 MP/8 MP/6 MP/5 MP/4 MP/3 MP/1080p/UXGA/720p/VGA/4CIF/ DCIF/2CIF/CIF/QCIF	
	VGA1/HDMI1 Output Resolution	HDMI1: 4K (3840 × 2160)/60Hz, 4K (3840 × 2160)/30Hz, 2K (2560 × 1440)/60Hz, 1920 × 1080p/60Hz, 1600 × 1200/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz	
		VGA1: 2K (2560 × 1440)/60Hz, 1920 × 1080p/60Hz, 1600 × 1200/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz	
	VGA2 /HDMI2 Output Resolution	1920 × 1080p/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz	
	Audio Output	2-ch, RCA (2.0Vp-p, 1 KΩ)	
Decoding	Decoding Format	H.265/H.264/H.264+/MPEG4	
	Live View/Playback Resolution	12 MP/8 MP/6 MP/5 MP/4 MP/3 MP/1080p/UXGA/720p/VGA/4CIF/DCIF/2CIF/CIF/QCIF	
	Synchronous Playback	16-ch	
	Capability	4-ch @ 8 MP, or 16-ch @ 1080p	
Network Management	Network Protocols	TCP/IP, DHCP, EZVIZ Cloud P2P, DNS, DDNS, NTP, SADP, SMTP, NFS, iSCSI, UPnP™, HTTPS	
Hard Disk	Sata	8 SATA interfaces for 8HDDs	
	eSata	1 eSATA interface	
	Capacity	Up to 6 TB capacity for each HDD	
Disk Array	Array Type	RAID0, RAID1, RAID5, RAID6, RAID10	
	Number Of Arrays	4	
External Interface	Network Interface	2, RJ-45 10/100/1000 Mbps self-adaptive Ethernet interface	
	Serial Interface	RS-232; RS-485; Keyboard	
	USB Interface	Front panel: 2 × USB 2.0; Rear panel: 1 × USB 3.0	
	Alarm In/Out	16/4	
General	Power Supply	100 to 240 VAC, 50 to 60 Hz	
	Maximum Power	200 W	
	Consumption (w/o Hard Disk)	≤ 30 W	
	Working Temperature	-10 to +55º C (+14 to +131º F)	
	Working Humidity	10 to 90 %	
	Chassis	19-inch rack-mounted 2U chassis	
	Dimensions(W×D×H)	445 × 470 ×90 mm (17.5"× 18.5" × 3.5")	
	Weight (w/o Hard Disk)	≤ 10 kg (22 lb)	

18.1.2. DS-7716NI-I4/P

Model		DS-7716NI-I4/16P
Video/Audio Input	IP Video Input	16-ch
		Up to 12 MP resolution
	Two-Way Audio	1-ch, RCA (2.0 Vp-p, 1 k Ω)
Network	Incoming Bandwidth	160 Mbps
	Outgoing Bandwidth	256 Mbps
	Remote Connection	128
Video/Audio Output	Recording Resolution	12 MP/8 MP/6 MP/5 MP/4 MP/3 MP/1080p/UXGA/720p/VGA/4CIF/DCIF/ 2CIF/CIF/QCIF
	HDMI Output Resolution	4K (3840 × 2160)/60Hz, 4K (3840 × 2160)/30Hz, 1920 × 1080p/60Hz, 1600 × 1200/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz
	VGA Output Resolution	1920 × 1080p/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz
	Audio Output	1-ch, RCA (Linear, 1 KΩ)
Decoding	Decoding Format	H.265/H.264/MPEG4
	Live View/Playback Resolution	12 MP/8 MP/6 MP/5 MP/4 MP/3 MP/1080p/UXGA/720p/VGA/4CIF/DCIF/ 2CIF/CIF/QCIF
	Synchronous Playback	16-ch
	Capability	4-ch @ 4K, or 16-ch @ 1080p
Network Management	Network Protocols	TCP/IP, DHCP, EZVIZ Cloud P2P, DNS, DDNS, NTP, SADP, SMTP, NFS, iSCSI, UPnP™, HTTPS
Hard Disk	SATA	4 SATA interfaces for 4HDDs
	Capacity	Up to 6TB capacity for each HDD
External Interface	Network Interface	1 RJ-45 10/100/1000 Mbps self-adaptive Ethernet interface
	Serial Interface	1 RS-485 (half-duplex), 1 RS-232
	USB Interface	Front panel: 2 × USB 2.0; Rear panel: 1 × USB 3.0
	Alarm In/Out	16/4
Poe Interface	Interface	16 RJ-45 10/100 Mbps self-adaptive Ethernet interfaces
	Power	≤200 W
	Supported Standard	IEEE 802.3 af/at
General	Power Supply	100 to 240 VAC
	Power	≤300 W
	Consumption (without Hard Disk)	≤20 W (without enabling PoE)
	Working Temperature	-10 to +55º C (+14 to +131º F)
	Working Humidity	10 to 90 %
	Chassis	19-inch rack-mounted 1.5U chassis
	Dimensions(W×D×H)	445 × 390 ×70 mm (17.5"× 15.3" × 2.8")
	Weight (w/o Hard Disk)	≤ 5 kg (11 lb)

18.1.3. DS-76xxNI-I2/xP

	DS-7608NI-I2/8P	DS-7616NI-I2/16P
Max. Recording Resolution	12 MP	12 MP
Video Compression	H.264, H.264+, H.265	H.264, H.264+, H.265
HDMI/VGA Output	3840x2160/1920x1080, 1920x1080/ 1920x1080, independent output	3840x2160/1920x1080, 1920x1080/1920x1080, independent Output
IP Video Input	8-ch IPC w/integrated 8-port 802.3af/at PoE switch	16-ch IPC w/integrated 16-port 802.3af/at PoE switch
Audio Input/Output	1 line in/1 line out	1 line in/1 line out
Alarm Input/Output	4 ch/1 ch	4 ch/1 ch
USB	1 USB 2.0; 1 USB 3.0	1 USB 2.0; 1 USB 3.0
Internal SATA	2 SATA interfaces (up to 6 TB each)	2 SATA interfaces (up to 6 TB each)
eSATA Interface	---	---
Max. Internal Storage	12 TB	12 TB
Support DVD-RW	---	---
Max. Incoming Bandwidth (Mbps)	80	160
Max. Outgoing Bandwidth (Mbps)	256	256
Max. Remote Connections	128	128
Rack Units	1	1
Ratings	UL/cUL Listed	UL/cUL Listed
PoE Budget	180 W	280 W
Power Requirements	100 to 240 VAC, ≤15W without HDD	100 to 240 VAC, ≤15 W w/o HDD

18.2 Glossary

- Dual Stream: Dual stream is a technology used to record high resolution video locally while transmitting a lower resolution stream over the network. The two streams are generated by the DVR, with the main stream having a maximum resolution of 4CIF and the sub-stream having a maximum resolution of CIF.
- HDD: Hard Disk Drive. A storage medium that stores digitally encoded data on platters with magnetic surfaces.
- DHCP: Dynamic Host Configuration Protocol (DHCP) is a network application protocol used by devices (DHCP clients) to obtain configuration information for operation in an Internet Protocol network.
- HTTP: Hypertext Transfer Protocol. A protocol to transfer hypertext request and information between servers and browsers over a network
- DDNS: Dynamic DNS is a method, protocol, or network service that provides the capability for a networked device, such as a router or computer system using the Internet Protocol Suite, to notify a domain name server to change, in real time (ad-hoc) the active DNS configuration of its configured hostnames, addresses or other information stored in DNS.
- Hybrid DVR: A hybrid DVR is a combination of a DVR and NVR.
- NTP: 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 60 Hz.
- NVR: Acronym for Network Video Recorder. An NVR can be a PC-based or embedded system used for centralized management and storage for IP cameras, IP Domes, and other DVRs.
- PAL: Phase Alternating Line. PAL is also another video standard used in broadcast television systems in large parts of the world. PAL signal contains 625 scan lines at 50 Hz.
- 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 displayed on the monitor after starting up normally.

  Possible Reasons

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

  Steps

  1. Verify the device is connected to the monitor via HDMI or VGA cable.
  2. If not, connect the device to the monitor and reboot.
  3. Verify the connection cable is good.
  4. If there is still no image display on the monitor after rebooting, check if the connection cable is good, and replace the cable and try connecting again.
  5. Verify the monitor input mode is correct.
  6. Check that the monitor input mode matches the output mode of the device (e.g., if the output mode of the NVR is HDMI, then the input mode of the monitor must be HDMI). If not, modify the monitor input mode.
  7. Check if the fault is solved by Step 1 to Step 3.
  8. If it is solved, finish the process.
  9. If not, contact Hikvision tech support for further help.

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

  Possible Reasons

  - No HDD is installed in the device.
  - The installed HDD has not been initialized.
  - The installed HDD is not compatible with the NVR or is broken.

  Steps

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

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

  2. If you don’t want to install an HDD, select “Menu > Configuration > Exceptions,” and uncheck the “HDD Error” Audible Warning checkbox.

3. Verify that the HDD is initialized.
    1) Select “Menu > HDD > General.”
    2) If the HDD status is “Uninitialized,” check the corresponding HDD checkbox and click the “Init” button.
4. Verify the HDD is detected or is in good condition.
    1) Select “Menu > HDD > General.”
    2) If the HDD is not detected or the status is “Abnormal,” replace the dedicated HDD according to the requirement.
5. Check if the fault is solved by the Step 1 to Step 3.
    1) If it is solved, finish the process.
    2) If not, please contact Hikvision tech support for further help.

- The added IP camera status displays as “Disconnected” when it is connected through Private Protocol.

    NOTE: Select “Menu > Camera > Camera > IP Camera” to get the camera status.

Possible Reasons

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

Steps

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

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

        If there exists return information and the time value is short, the network is normal.
2. Verify the configuration parameters are correct.
    1) Select “Menu > Camera > Camera > IP Camera.”
    2) Verify the following parameters are the same with those of the connected IP devices, including IP address, protocol, management port, user name, and password.

3. Verify that the bandwidth is adequate.

    1) Select “Menu > Maintenance > Net Detect > Network Stat.”

    2) Check usage of the access bandwidth, and see if the total bandwidth has reached its limit.

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

    1) If it is solved, finish the process.

    2) If not, contact Hikvision tech support for further help.

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

Possible Reasons

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

Steps

1. Verify the IP camera and the NVR versions are compatible.

    1) Enter the IP camera Management interface “Menu > Camera > Camera > IP Camera,” and view the connected IP camera’s firmware version.

    2) Enter the System Info interface “Menu > Maintenance > System Info > Device Info,” and view the NVR’s firmware version.

2. Verify that the IP camera power supply is stable.

    1) Verify the power indicator is normal.

    2) When the IP camera is offline, try the ping command on a PC to check if the PC connects to the IP camera.

3. Verify the network between the IP camera and NVR is stable.

    1) When the IP camera is offline, connect PC and NVR with a RS-232 cable.

    2) Open the Super Terminal, use the ping command and keep sending large data packages to the connected IP camera, and check if there exists packet loss.

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

Example: Input ping 172.6.22.131 –l 1472 –f.

4. Verify the switch is not in flow control.

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

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

   1) If it is solved, finish the process.

   2) If not, contact Hikvision tech support for further help.

- No monitor connects to the NVR locally. When you manage the IP camera to connect with the device remotely through a Web browser, the status displays as Connected. Then, when you connect the device to the monitor via the VGA or HDMI interface and reboot the device, there is a black screen with the mouse cursor.

  When connecting the NVR to the monitor before startup via the VGA or HDMI interface and managing the IP camera to connect with the device locally or remotely, the status of the IP camera displays as Connect. Then, connecting the device with CVBS, there is a black screen.

  Possible Reasons

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

  Steps

  1. Enable the output channel.

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

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

     Different camera orders and window-division modes can be set for different output interfaces separately, and digits like “D1”and “D2” stand for the channel number, and “X” means the selected window has no image output.

  3. Check if the fault is solved by the above steps.

     1) If it is solved, finish the process.

     2) If not, contact Hikvision tech support for further help.

- Live view freezes outputting video locally.

Possible Reasons

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

Steps

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

        NOTE: Simultaneously press Ctrl and C to exit the ping command.
2. Verify the frame rate is real-time frame rate (select "Menu > Record > Parameters > Record" and set the Frame rate to Full Frame).
3. Check if the fault is solved by the above steps.
    1) If it is solved, finish the process.
    2) If not, contact Hikvision tech support for further help.

- Live view freezes when video is output remotely via Internet Explorer or platform software.

Possible Reasons

- Poor network between NVR and IP camera, and there exists packet loss during the transmission.
- Poor network between NVR and PC, and there exists packet loss during the transmission.
- The hardware performance is not good enough, including CPU, memory, etc.

Steps

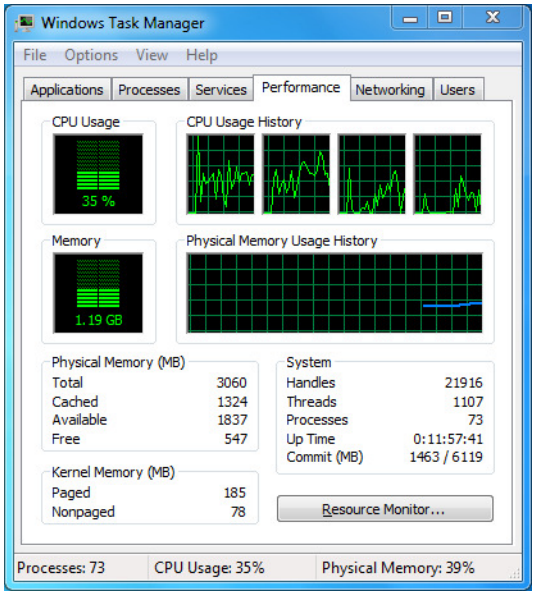
1. Verify the network between NVR and IP camera is connected.
    1) When image is frozen, connect the RS-232 ports on a PC and the rear panel of the NVR with an RS-232 cable.
    2) Open the Super Terminal, and execute the command of "**ping** *192.168.0.0* **–l 1472 –f**" (the IP address may change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

        NOTE: Simultaneously press Ctrl and C to exit the ping command.
2. Verify the network between NVR and PC is connected.

1. Open the cmd window in the Start menu, or press “windows+R” shortcut key to open it.
2. Use the ping command to send large packet to the NVR, execute the command of “ping 192.168.0.0 –l 1472 –f” (the IP address may change according to the real condition), and check if there exists packet loss.

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

3. Verify the hardware of the PC is adequate (simultaneously press **Ctrl**, **Alt,** and **Delete** to enter the windows task management interface, as shown in the following figure).



4. In Windows task management interface:

   1) Select the “Performance” tab; check the status of the CPU and Memory.

   2) If the resource is not enough, end unnecessary processes.

5. Check if the fault is solved by the above steps.

   1) If it is solved, finish the process.

   2) If not, contact Hikvision tech support for further help.

- When using the NVR 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 IP camera is not connected well; impedance mismatches or is incompatible.
- The stream type is not set to “Video & Audio.”
- The encoding standard is not supported by the NVR.

Steps

1. Verify the cable between the pickup and IP camera is connected well; impedance matches and is compatible.
2. Log into the IP camera directly, and turn the audio on. Check if the sound is normal. If not, contact the IP camera manufacturer.
3. Verify the setting parameters are correct.
4. Select "Menu > Record > Parameters > Record", and set the Stream Type to "Audio & Video."
5. Verify the NVR supports the IP camera audio encoding standard.
6. NVR supports G722.1 and G711 standards, and if the encoding parameter of the input audio is not one of these standards, log in the IP camera to configure it to the supported standard.
7. Check if the fault is solved by the above steps.
    1) If it is solved, finish the process.
    2) If not, contact Hikvision tech support for further help.

- The image freezes when the NVR plays back single or multi-channel.

Possible Reasons

- Poor network between NVR and IP camera, and there exists packet loss during the transmission.
- The frame rate is not the real-time frame rate.
- The NVR supports up to 16-channel synchronize playback at 4CIF resolution. For 16-channel synchronized playback at 720p resolution, frame extracting may occur, which leads to image freezing.

Steps

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

        NOTE: Simultaneously press the Ctrl and C to exit the ping command.
2. Verify the frame rate is real-time frame rate.
3. Select "Menu > Record > Parameters > Record", and set the Frame Rate to "Full Frame."

4. Verify the hardware can support the playback.
5. Reduce the number of playback channels.
6. Select “Menu > Record > Encoding > Record,” and set the resolution and bitrate to a lower level.
7. Reduce the number of local playback channels.
8. Select “Menu > Playback,” and uncheck the checkbox of unnecessary channels.
9. Check if the fault is solved by the above steps.
    1) If it is solved, finish the process.
    2) If not, contact Hikvision tech support for further help.

- No record file found in the NVR local HDD, and “No record file found” prompt appears.

Possible Reasons

- The system time setting is incorrect.
- The search condition is incorrect.
- The HDD is in error or not detected.

Steps

1. Verify the system time setting is correct.
2. Select “Menu > Configuration > General > General,” and verify the “Device Time” is correct.
3. Verify the search condition is correct.
4. Select “Playback,” and verify the channel and time are correct.
5. Verify the HDD status is normal.
6. Select “Menu > HDD > General” to view the HDD status, and verify the HDD is detected and can be read and written normally.
7. Check if the fault is solved by the above steps.
    1) If it is solved, finish the process.
    2) If not, contact Hikvision tech support for further help.

18.4 Summary of Changes

18.4.1. Version 3.4.2

- **Added**
  - Support display of IP camera's password on the IP camera management interface (Chapter 2.4 Adding and Connecting the IP Cameras; Chapter 16.5.2 Editing a User)
  - Add configuration and use of unlock pattern for fast login (Chapter 2.3 Using the Unlock Pattern for Login)
  - Add fisheye expansion view for connected fisheye camera in live view and playback (Chapter 3.2.5 Fisheye Expansion View)
  - Add scaling display (30min/1h/2h/6h/24h) of time bar in playback mode (Chapter 6 Playback)
  - Add thumbnails view and fast view during playback (Chapter Key Features, Chapter 6.2.2 Thumbnails View, Chapter 6.2.3 Fast View)
- **Updated**
  - Optimize playback interface (Chapter 6 Playback)
  - Update digital zoom operation in image (Chapter 3.2.3 Quick Setting Toolbar in Live View Mode, Chapter 6.2.2 Digital Zoom)

18.5 List of Compatible IP Cameras

List of Hikvision IP Cameras

NOTE: Hikvision holds the right to interpret this list.

Type	Model	Version	Max. Resolution	Sub-stream	Audio
SD Network Camera	DS-2CD7133F-E	V5.2.0 build 140721	640*480	√	×
	DS-2CD793NFWD-EI	V5.2.0 build 140721	704*576	√	√
	DS-2CD802NF	V2.0 build 090522 V2.0 build 090715 V2.0 build 110301	704*576	√	√
	DS-2CD833F-E	V5.2.0 build 140721	640*480	√	√
	DS-2CD893PF-E	V5.2.0 build 140721	704*576	√	√
HD Network Camera	DS-2CD2012-I	V5.3.0 build150327	1280*960	√	×
	DS-2CD2132-I	V5.3.0 build150327	2048*1536	√	×
	DS-2CD2410FD-I(W)	V5.3.0 build150327	1920*1080	√	√
	DS-2CD2612F-I	V5.3.0 build150327	1280*960	√	×
	DS-2CD2612F-IS	V5.3.0 build150327	1280*960	√	√
	DS-2CD2632F-I	V5.3.0 build150327	2048*1536	√	×
	DS-2CD2632F-IS	V5.3.0 build150327	2048*1536	√	√
	DS-2CD2710F-I	V5.3.0 build150327	1920*1080	√	×
	DS-2CD2720F-I	V5.3.0 build150327	1920*1080	√	×
	DS-2CD4010F	V5.3.0 build150327	1920*1080	√	√
	DS-2CD4012F	V5.3.0 build150327	1280*1024	√	√
	DS-2CD4026FWD	V5.3.0 build150327	1920*1080	√	√
	DS-2CD4026FWD-SDI	V5.3.0 build150327	1920*1080	√	√
	DS-2CD4032FWD	V5.3.0 build150327	2048*1536	√	√
	DS-2CD4065F	V5.3.0 build150327	3072*2048	√	√
	DS-2CD4124F-I(2.8-12mm)	V5.3.0 build150327	1920*1080	√	√
	DS-2CD4132FWD-I(2.8-12mm)	V5.3.0 build150327	2048*1536	√	√
	DS-2CD4212F-I(2.8-12mm)	V5.3.0 build150327	1280*1024	√	×
	DS-2CD4212F-IS(2.8-12mm)	V5.3.0 build150327	1280*1024	√	√
	DS-2CD4212FWD-I	V5.3.0 build150327	1280*960	√	×
	DS-2CD4212FWD-IS	V5.3.0 build150327	1280*960	√	√
	DS-2CD4224F-I	V5.3.0 build150327	1920*1080	√	×
	DS-2CD4232FWD-I	V5.3.0 build150327	2048*1536	√	×
	DS-2CD4232FWD-IS(2.8-12mm)	V5.3.0 build150327	2048*1536	√	√
	DS-2CD4312F-I	V5.3.0 build150327	1280*1024	√	×
	DS-2CD4312FWD-I	V5.3.0 build150327	1280*960	√	×
	DS-2CD4324F-I	V5.3.0 build150327	1920*1080	√	×
	DS-2CD4332FHWD-IS	V5.3.0 build150327	2048*1536	√	√
	DS-2CD4332FHWD-I	V5.3.0 build150327	2048*1536	√	×
	DS-2CD4332FWD-I	V5.3.0 build150327	2048*1536	√	×
	DS-2CD6213F	V5.2.6 build 141218	1280*960	√	×
	DS-2CD6223F	V5.2.6 build 141218	1920*1080	√	×
	DS-2CD6233F	V5.2.6 build 141218	2048*1536	√	×
	DS-2CD7153-E	V5.2.0 build 140721	1600*1200	√	×
	DS-2CD7164-E	V5.2.0 build 140721	1280*720	√	×
	DS_2CD754F-EI	V5.2.0 build 140721	2048*1536	√	√
	DS-2CD754FWD-E	V5.2.0 build 140721	1920*1080	√	√
	DS-2CD754FWD-EIZ	V5.2.0 build 140721	2048*1536	√	√
	DS_2CD783F-EI	V5.2.0 build 140721	2560*1920	√	√
	DS-2CD8153F-E	V5.2.0 build 140721	1600*1200	√	√
	DS-2CD8464F-EI	V5.2.0 build 140721	1280*960	√	√
	DS-2CD852MF-E	V2.0 build 110614 V2.0 build 110426 V2.0 build 100521	1600*1200	√	√
	DS-2CD855F-E	V5.2.0 build 140721	1920*1080	√	√
	DS-2CD862MF-E	V2.0 build 110614 V2.0 build 110426 V2.0 build 100521	1280*960	√	√

Type	Model	Version	Max. Resolution	Sub-stream	Audio
	DS-2CD863PF/NF-E	V5.2.0 build 140721	1280*960	√	√
	DS-2CD864FWD-E	V5.2.0 build 140721	1280*720	√	√
	DS-2CD876MF/BF-E	V4.0.3 build120913	1600*1200	√	√
	DS-2CD877BF	V4.0.3 build120913	1920*1080	√	√
	DS-2CD886MF-E	V4.0.3 build 120913	2560*1920	√	√
	DS-2CD966(B)	V3.1 build 120423	1360*1024	×	×
	DS-2CD966-V(B)	V3.1 build 120423	1360*1024	×	×
	DS-2CD976(C)	V3.1 build 120423	1600*1200	×	×
	DS-2CD976-V(C)	V3.1 build 120423	1600*1200	×	×
	DS-2CD977(C)	V3.1 build 120423	1920*1080	×	×
	DS-2CD986A(C)	V3.1 build 120423	2448*2048	×	×
	DS-2CD986C（B）	V2.3.6 build 120401	2560*1920	×	×
HD Network Camera	DS-2CD9122	V3.7.1 build140417	1920*1080	√	×
	DS-2CD9152	V3.7.1 build140417	2560*1920	√	×
	iDS-2CD9152	V3.7.1 build140417	2560*1920	√	×
	DS-2CD9122-H	V3.7.1 build140417	1920*1080	√	×
	DS-2CD9182-H	V3.8.1 build140815	3296*2472	√	×
	DS-2CD9121	V3.7.1 build140417	1600*1200	√	×
	iDS-2CD9121	V3.7.1 build140417	1600*1200	√	×
	DS-2CD9131	V4.0.0 build150213	2048*1536	√	×
	iDS-2CD9131	V4.0.0 build150213	2048*1536	√	×
	DS-2CD9121A	V3.8.2 build141121	1600*1200	√	×
	iDS-2CD9121A	V3.8.2 build141121	1600*1200	√	×
	DS-2CD9111(B)	V3.7.1 build140417	1360*1024	√	×
	DS-2CD9151A	V3.8.2 build141121	2448*2048	√	×
	DS-2CD9152-H	V3.8.2 build141121	2592*2048	√	×
	iDS-2CD9282	V3.8.2 build141121	3296*2472	√	×
	DS-2CD9131-K	V4.0.0 build150213	2048*1536	√	√
	DS-2CD9152-HK	V3.8.2 build141121	2592*2048	√	√
	iDS-2CD9131-E	V3.8.2 build141121	2048*1536	√	×
	iDS-2CD9151A-E	V3.8.2 build141121	2448*2048	√	×
	iDS-2CD9151A	V3.8.2 build141121	2448*2048	√	×
	iDS-2CD9152-EH	V3.8.2 build141121	2592*2048	√	×
	iDS-2CD9152-H	V3.8.2 build141121	2592*2048	√	×
	DS-2CD9120-H	V3.7.1 build140417	1600*1200	√	×
	iDS-2CD9361	V4.0.0 build150213	2752*2208	√	×
	iDS-2CD9022	V4.0.0 build150213	1920*1080	√	√
	iDS-2CD9025	V3.8.2 build141114	1920*1080	√	×
	iDS-2CD9022-SZ	V4.0.0 build150213	1920*1080	√	×
	DS-2CD9125-KS	V3.8.1 build150113	1920*1080	√	×
SD Encoder	DS-6501HCI	V1.0.1 build130607	352*288	√	√
	DS-6501HCI-SATA	V1.0.1 build130607	352*288	√	√
	DS-6501HFI	V1.0.1 build130607	704*576	√	√
	DS-6501HFI- SATA	V1.0.1 build130607	704*576	√	√
	DS-6502HCI	V1.0.1 build130607	352*288	√	√
	DS-6502HCI- SATA	V1.0.1 build130607	352*288	√	√
	DS-6502HFI	V1.0.1 build130607	704*576	√	√
	DS-6502HFI- SATA	V1.0.1 build130607	704*576	√	√
	DS-6504HCI	V1.0.1 build130607	352*288	√	√
	DS-6504HCI- SATA	V1.0.1 build130607	352*288	√	√
	DS-6504HFI	V1.0.1 build130607	704*576	√	√
	DS-6504HFI- SATA	V1.0.1 build130607	704*576	√	√
	DS-6508HCI	V1.0.1 build130607	352*288	√	√
	DS-6508HCI- SATA	V1.0.1 build130607	352*288	√	√
	DS-6508HFI	V1.0.1 build130607	704*576	√	√
	DS-6508HFI- SATA	V1.0.1 build130607	704*576	√	√
	DS-6516HCI	V1.0.1 build130607	352*288	√	√
	DS-6516HCI- SATA	V1.0.1 build130607	352*288	√	√
	DS-6516HFI	V1.0.1 build130607	704*576	√	√
	DS-6516HFI- SATA	V1.0.1 build130607	704*576	√	√
	DS-6601HCI	V1.2.1 build131202	352*288	√	√
	DS-6602HCI	V1.2.1 build131202	352*288	√	√

Type	Model	Version	Max. Resolution	Sub-stream	Audio
	DS-6604HCI	V1.2.1 build131202	352*288	√	√
	DS-6601HFI(-SATA)	V1.2.1 build131202	704*576	√	√
	DS-6602HFI(SATA)	V1.2.1 build131202	704*576	√	√
	DS-6604HFI(-SATA)	V1.2.1 build131202	704*576	√	√
	DS-6701HWI	V1.2.3 build141202	960*576	√	√
	DS-6701HWI-SATA	V1.2.3 build141202	960*576	√	√
	DS-6704HWI	V1.2.3 build141202	960*576	√	√
	DS-6704HWI-SATA	V1.2.3 build141202	960*576	√	√
	DS-6708HWI	V1.2.3 build141202	960*576	√	√
	DS-6708HWI-SATA	V1.2.3 build141202	960*576	√	√
	DS-6716HWI	V1.2.3 build141202	960*576	√	√
	DS-6716HWI-SATA	V1.2.3 build141202	960*576	√	√
HD Encoder	DS-6601HFHI	V1.1.0 build150123	1920*1080	√	√
	DS-6601HFHI/L	V1.1.0 build150123	1920*1080	√	√
Network Speed Dome	DS-2DF7274-A/D/AF	V5.2.8 build150124	1280*960	√	√
	iDS-2DF7274-A/D/AF	V5.2.8 build150124	1280*960	√	√
	DS-2DM7274-A	V5.2.8 build150124	1280*960	√	√
	DS-2DF5274-A/D/A3/D3/AF/A3F	V5.2.8 build150124	1280*960	√	√
	iDS-2DF5274-A/D/A3/D3/AF/A3F	V5.2.8 build150124	1280*960	√	√
	DS-2DM5274-A/A3	V5.2.8 build150124	1280*960	√	√
	DS-2DF7276-A/D/AF	V5.2.8 build150124	1280*960	√	√
	iDS-2DF7276-A/D/AF	V5.2.8 build150124	1280*960	√	√
	DS-2DF5276-A/D/A3/D3/AF/A3F	V5.2.8 build150124	1280*960	√	√
	iDS-2DF5276-A/D/A3/D3/AF/A3F	V5.2.8 build150124	1280*960	√	√
	DS-2DF7274-AH/DH/AFH	V5.2.8 build150124	1280*960	√	√
	iDS-2DF7274-AH/DH/AFH	V5.2.8 build150124	1280*960	√	√
	DS-2DF5274-AH/DH/A3H/D3H/AFH/A3FH	V5.2.8 build150124	1280*960	√	√
	iDS-2DF5274-AH/DH/A3H/D3H/AFH/A3FH	V5.2.8 build150124	1280*960	√	√
	DS-2DF7276-AH/DH/AFH	V5.2.8 build150124	1280*960	√	√
	iDS-2DF7276-AH/DH/AFH	V5.2.8 build150124	1280*960	√	√
	DS-2DF5276-AH/DH/A3H/D3H/AFH/A3FH	V5.2.8 build150124	1280*960	√	√
	iDS-2DF5276-AH/DH/A3H/D3H/AFH/A3FH	V5.2.8 build150124	1280*960	√	√
	DS_2DF7130I5-AW	V5.2.8 build150124	1280*960	√	√
	DS-2DF7285-AH	V5.2.8 build150124	1920*1080	√	√
	DS-2DF5285-AH	V5.2.8 build150124	1920*1080	√	√
	DS-2DF7294-A/D/AF	V5.2.8 build150124	2048*1536	√	√
	iDS-2DF7294-A/D/AF	V5.2.8 build150124	2048*1536	√	√
	DS-2DF5294-A/D/A3/D3/AF/A3F	V5.2.8 build150124	2048*1536	√	√
	iDS-2DF5294-A/D/A3/D3/AF/A3F	V5.2.8 build150124	2048*1536	√	√
	DS-2DF7296-A/D/AF	V5.2.8 build150124	2048*1536	√	√
	iDS-2DF7296-A/D/AF	V5.2.8 build150124	2048*1536	√	√
	DS-2DF5296-A/D/A3/D3/AF/A3F	V5.2.8 build150124	2048*1536	√	√
	iDS-2DF5296-A/D/A3/D3/AF/A3F	V5.2.8 build150124	2048*1536	√	√
	DS-2DF6223-A	V5.2.8 build150124	1920*1080	√	√
	iDS-2DF6223-A	V5.2.8 build150124	1920*1080	√	√
	DS-2DF8223i-A	V5.2.8 build150124	1920*1080	√	√
	iDS-2DF8223i-A	V5.2.8 build150124	1920*1080	√	√
	DS-2DF7284-A/D/AF	V5.2.8 build150124	1920*1080	√	√
	iDS-2DF7284-A/D/AF	V5.2.8 build150124	1920*1080	√	√
	DS-2DF7286-A/D/AF	V5.2.8 build150124	1920*1080	√	√
	iDS-2DF7286-A/D/AF	V5.2.8 build150124	1920*1080	√	√
	DS-2DF5284-A/D/A3/D3/AF/A3F	V5.2.8 build150124	1920*1080	√	√
	iDS-2DF5284-A/D/A3/D3/AF/A3F	V5.2.8 build150124	1920*1080	√	√
	DS-2DF5286-A/D/A3/D3/AF/A3F	V5.2.8 build150124	1920*1080	√	√
	iDS-2DF5286-A/D/A3/D3/AF/A3F	V5.2.8 build150124	1920*1080	√	√
	DS_2DF7230I5-AW	V5.2.8 build150124	1920*1080	√	√
	DS-2AF7220-A/D	V5.2.8 build150124	1920*1080	√	√
	DS-2AF7230-A/D	V5.2.8 build150124	1920*1080	√	√
	DS-2AF5220-A/D	V5.2.8 build150124	1920*1080	√	√
	DS-2AF5230-A/D	V5.2.8 build150124	1920*1080	√	√
	iDS-2DF5220S-D4/JY	V5.2.8 build150124	1920*1080	√	√
	DS-2DF7268-A	V5.2.8 build150124	704*576	√	√

Type	Model	Version	Max. Resolution	Sub-stream	Audio
	DS-2DF5268-A	V5.2.8 build150124	704*576	√	√
	DS-2DF7264-A	V5.2.8 build150124	704*576	√	√
	DS-2DF5264-A	V5.2.8 build150124	704*576	√	√
	DS-2DE5172-A/A3	V5.2.10 build150128	1280*960	√	√
	DS-2DE5174-A/AE/AE3/A3/D/D3	V5.2.10 build150128	1280*960	√	√
	DS-2DE5176-A/AE	V5.2.10 build150128	1280*960	√	√
	DS-2DE7172-A	V5.2.10 build150128	1280*960	√	√
	DS-2DE7174-A/AE/D	V5.2.10 build150128	1280*960	√	√
	DS-2DE7176-A/AE	V5.2.10 build150128	1280*960	√	√
	DS-2DE7120i-A/AE	V5.2.10 build150128	1280*960	√	√
	DS-2DM7130i-A	V5.2.10 build150128	1280*960	√	√
	DS-2DM4120-A	V5.2.10 build150128	1280*960	√	√
	DS-2DE5120I-A	V5.2.10 build150128	1280*960	√	√
	DS-2DM5120-A	V5.2.10 build150128	1280*960	√	√
	DS-2DM5130-A	V5.2.10 build150128	1280*960	√	√
	DS-2DE2103-DE3/W	V5.2.10 build150128	1280*960	√	√
	DS-2DE2103I-DE3/W	V5.2.10 build150128	1280*960	√	√
	DS-2DE7184-A/AE/D	V5.2.10 build150128	1920*1080	√	√
	DS-2DE5182-A/A3	V5.2.10 build150128	1920*1080	√	√
	DS-2DE5184-A/AE/AE3/A3/D/D3	V5.2.10 build150128	1920*1080	√	√
	DS-2DE5186-A/AE	V5.2.10 build150128	1920*1080	√	√
	DS-2DE7182-A	V5.2.10 build150128	1920*1080	√	√
	DS-2DE4582-A	V5.2.10 build150128	1920*1080	√	√
	DS-2DE4220-A	V5.2.10 build150128	1920*1080	√	√
	DS-2DE4182-A	V5.2.10 build150128	1920*1080	√	√
	DS-2DM7230i-A	V5.2.10 build150128	1920*1080	√	√
	DS-2DM7220i-A	V5.2.10 build150128	1920*1080	√	√
	DS-2DE7186-A/AE	V5.2.10 build150128	1920*1080	√	√
	DS-2DE5220I-A	V5.2.10 build150128	1920*1080	√	√
	DS-2DM5220-A	V5.2.10 build150128	1920*1080	√	√
	DS-2DM5230-A	V5.2.10 build150128	1920*1080	√	√
	DS-2DE2202-DE3/W	V5.2.10 build150128	1920*1080	√	√
	DS-2DE2202I-DE3/W	V5.2.10 build150128	1920*1080	√	√
	DS-2DE4572-A	V5.2.10 build150128	1280*720	√	√
	DS-2DE4172-A	V5.2.10 build150128	1280*720	√	√
	DS-2DE7194-A/A3	V5.2.10 build150128	2048*1536	√	√
	DS-2DE5194-A/A3	V5.2.10 build150128	2048*1536	√	√
	DS-2DF1-518	V3.2.0 build131223	704*576	√	√
	DS-2DM1-718	V3.2.0 build131223	704*576	√	√
	DS-2DM1-518	V3.2.0 build131223	704*576	√	√
	DS-2DF1-718	V3.2.0 build131223	704*576	√	√
	DS-2DF1-514	V3.2.0 build131223	704*576	√	√
	DS-2DF1-714	V3.2.0 build131223	704*576	√	√
	DS-2DY9174-A	V5.2.8 build150124	1280*960	√	√
	DS-2DY9176-A	V5.2.8 build150124	1280*960	√	√
	DS-2DY9194-A	V5.2.8 build150124	2048*1536	√	√
	DS-2DY9196-A	V5.2.8 build150124	2048*1536	√	√
	DS-2DY9184-A	V5.2.8 build150124	1920*1080	√	√
	DS-2DY9186-A	V5.2.8 build150124	1920*1080	√	√
	DS-2DY9185-A	V5.2.8 build150124	1920*1080	√	√
	DS-2DY9187-A	V5.2.8 build150124	1920*1080	√	√
	DS-2DF8223IV-A	V5.3.0 build150304	1920*1080	√	√
	DS-2DF8623IV-A	V5.3.0 build150304	3072*1728	√	√
	DS-2DF6623V-A	V5.3.0 build150304	3072*1728	√	√
	DS-2DF8823IV-A	V5.3.0 build150304	4096*2160	√	√
Network Zoom Camera Module	DS-2ZCN2006	V5.2.7 build141107	1280*960	√	√
	DS-2ZCN2006(B)	V5.2.7 build141107	1280*960	√	√
	DS-2ZCN3006	V5.2.7 build141107	1280*960	√	√
	DS-2ZCN3006(B)	V5.2.7 build141107	1280*960	√	√
	DS-2ZMN2006	V5.2.7 build141107	1280*960	√	√
	DS-2ZMN2006(B)	V5.2.7 build141107	1280*960	√	√
	DS-2ZMN3006	V5.2.7 build141107	1280*960	√	√

Type	Model	Version	Max. Resolution	Sub-stream	Audio
	DS-2ZMN3006(B)	V5.2.7 build141107	1280*960	√	√
	DS-2ZCN2007	V5.2.7 build141107	1920*1080	√	√
	DS-2ZCN3007	V5.2.7 build141107	1920*1080	√	√
	DS-2ZCN3007(B)	V5.2.7 build141107	1920*1080	√	√
	DS-2ZMN2007	V5.2.7 build141107	1920*1080	√	√
	DS-2ZMN3007	V5.2.7 build141107	1920*1080	√	√
	DS-2ZMN3007(B)	V5.2.7 build141107	1920*1080	√	√
	DS-2ZMN0407	V5.2.7 build141107	1920*1080	√	√
	DS-2ZMN3207	V5.2.7 build141107	1920*1080	√	√
	DS-2ZMN2008	V5.2.7 build141107	2048*1536	√	√
	DS-2ZCN2008	V5.2.7 build141107	2048*1536	√	√
	DS-2ZMN3007(S)	V5.2.2 build141113	1920*1080	√	√
	DS-2ZCN3007(S)	V5.2.2 build141113	1920*1080	√	√
	DS-2ZMN2307	V5.2.2 build141113	1920*1080	√	√
	DS-2CN2307	V5.2.2 build141113	1920*1080	√	√
	DS-2ZMN2309	V5.2.2 build141113	3072*2048	√	√
	DS-2ZCN2309	V5.2.2 build141113	3072*2048	√	√

18.6 List of Third-Party IP Cameras

NOTES: ONVIF compatibility refers to cameras that can be supported by both ONVIF protocol and its private protocols. Only ONVIF is supported refers to cameras that can be supported only when it uses the ONVIF protocol. Only AXIS is supported refers to a function that can be supported only when it uses the AXIS protocol.

IP Camera Manufacturer or Protocol	Model	Version	Max. Resolution	Sub-Stream	Audio
ACTi	ACM3401-09L-X-00227	A1D-220-V3.13.16-AC	1208*1024	×	×
	TCM4301-10D-X-00083	A1D-310-V4.12.09-AC	1208*1024	×	√
	TCM5311-11D-X-00023	A1D-310-V4.12.09-AC	1208*960	×	√
Arecont	AV1305 M	65175	1208*1024	√	×
	AV2815	65220	1920*1080	√	×
	AV3105M	65175	1920*1080	√	×
	AV8185DN	65172	1600*1200	×	×
Axis	M1114	5.09.1	1024*640	√	×
	M3011(ONVIF compatibility)	5.21	640*480 (704*576)	√ (×)	×
	M3014 (ONVIF compatibility)	5.21.1	1280*800	√	×
	P1346	5.40.9.2	2048*1536	√	√
	P3301 (ONVIF compatibility)	5.11.2	640*480 (768*576)	√	√ (×)
	P3304 (ONVIF compatibility)	5.20	1280*800 (1440*900)	√	√ (×)
	P3343 (ONVIF compatibility)	5.20.1	800*600	√	√ (×)
	P3344 (ONVIF compatibility)	5.20.1	1280*800 (1440*900)	√	√ (×)
	P5532	5.15	720*576	√	×
	Q7404	5.02	720*576	√	√
Bosch	AutoDome Jr 800 HD (ONVIF compatibility)	39500450	1920*1080	×	√ (×)
	Dinion NBN-921-P (ONVIF compatibility)	10500453	1280*720	×	√ (×)
	NBC 265 P (ONVIF compatibility)	07500452	1280*720	×	√ (×)
Brickcom	CB-500Ap (Brickcom-50xA) (ONVIF compatibility)	v3.2.1.3	1920*1080	×	√ (×)
Canon	VB-H410 (ONVIF compatibility)	Ver.+1.0.0	1920*1080 (1280*960)	×	√
	VB-S9000F	Ver. 1.0.0	1920*1080	×	×
	VB-S300D	Ver. 1.0.0	1920*1080	×	×
	VB-H6100D	Ver. 1.0.0	1920*1080	×	×
	VB-H7100F	Ver. 1.0.0	1920*1080	×	√
	VB-S8000	Ver. 1.0.0	1920*1080	×	×
Panasonic	SP306H (ONVIF compatibility)	Application:1.34/Image data:1.06	1280*960	√ (×)	√
	SF336H	Application:1.06/Image data: 1.06	1280*960	√	√
Pelco	D5118 (ONVIF compatibility)	1.8.2-20120327-2.9310-A1.7852	1280*960	√	×
	IX30DN-ACFZHB3 (ONVIF compatibility)	1.8.2-20120327-2.9080-A1.7852	2048*1536	√	×
	IXE20DN-AAXVUU2 (ONVIF compatibility)	1.8.2-20120327-2.9081-A1.7852	1920*1080	√	×
Sanyo	2300P (with lens)	2.03-02 (110318-00)	1920*1080	×	×
	2500P (with lens)	2.02-02 (110208-00)	1920*1080	×	√
	4600P	2.03-02 (110315-00)	1920*1080	×	√
SONY	SNC-CH220	1.50.00	1920*1080	×	×
	SNCDH220T (ONVIF only)	1.50.00	2048*1536	×	×
	SNC-EP580 (ONVIF compatibility)	1.53.00	1920*1080	√	√
	SNC-RH124 (ONVIF compatibility)	1.79.00	1280*720	√	√
SAMSUNG	SND-5080 (ONVIF compatibility)	3.10_130416	1280*1024	√	√
Vivotek	IP7133	0203a	640*480	×	×
	FD8134 (ONVIF compatibility)	0107a	1280*800	×	×
	IP8161 (ONVIF compatibility)	0104a	1600*1200	×	√ (×)
	IP8331 (ONVIF compatibility)	0102a	640*480	×	×
	IP8332 (ONVIF compatibility)	0105b	1280*800	×	×
Zavio	D5110 (ONVIF compatibility)	MG.1.6.03P8	1280*1024	√ (×)	×
	F3106 (ONVIF compatibility)	M2.1.6.03P8	1280*1024	√ (×)	√
	F3110 (ONVIF compatibility)	M2.1.6.01	1280*720	√ (×)	√
	F3206 (ONVIF compatibility)	MG.1.6.02c045	1920*1080	√ (×)	√
	F531E (ONVIF compatibility)	LM.1.6.18P10	640*480	√ (×)	√