Network Video Recorder

User Manual

User Manual

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.

Please use this user manual under the guidance of professionals.

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 OUR COMPANY 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 OUR COMPANY, 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 OUR COMPANY 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. OUR COMPANY 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, OUR COMPANY 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. OUR COMPANY 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 LVD Directive 2006/95/EC and 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.

This manual is applicable to LTN07256-R.

Product Key Features

General

- Connectable to network cameras, network dome 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 the smart IP cameras.
- PAL/NTSC adaptive video inputs.
- Each channel supports dual-stream.
- Up to 256 network cameras can be connected.
- Independent configuration for each channel, including resolution, frame rate, bit rate, image quality, etc..
- The quality of the input and output record is configurable.
- A redundant power supply is provided to improve the system stability.

Local Monitoring

- Simultaneous HDMI1/VGA output as the main output and the HDMI2 works as the auxiliary output.
- All video outputs at up to 1920×1080 resolution.
- Live view screen can be switched in group, and manual switch and auto-switch live view are also provided, and the interval of automatic cycle can be adjusted.
- Quick setting menu is provided for live view.
- Motion detection, video tampering, video exception alert and video loss alert functions.
- Privacy mask.
- Multiple PTZ protocols supported; PTZ preset, patrol and pattern.
- Zooming in by clicking the mouse and 3D positioning by dragging mouse.

HDD Management

- Up to 16 SATA hard disks can be connected. (Each disk with a maximum of 6TB storage capacity.)
- 8 network disks (8 NAS disks, or 7 NAS disks+1 IP SAN disk) can be connected.
- Support S.M.A.R.T. and bad sector detection. (Not supported when the RAID function is enabled.)
- HDD group management.
- Support HDD standby function.
- HDD property: redundancy, read-only, read/write (R/W).
- HDD quota management; different capacity can be assigned to different channel.
- Support RAID0, RAID1, RAID5 and RAID10 storage scheme, and can be enabled and disabled on your demand.

Recording and Playback

- Holiday recording schedule configuration.
- Continuous and event video recording parameters.
- Multiple recording types: manual, continuous, alarm, motion, motion | alarm, motion & alarm.
- 8 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.
- Locking and unlocking record files.
- Local redundant recording.
- Playing back record files by events (alarm input/motion detection/VCA).
- Playing back record files by smart search (intrusion/motion detection).
- Tag adding for record files, searching and playing back by tags.

- 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.
- Up to 16-ch synchronous playback.

Backup
- Export video data by USB or SATA device.
- 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.

Alarm and Exception
- Configurable arming time of alarm input/output.
- Alarm for video loss, motion detection, video tampering, abnormal signal, video input/output standard mismatch, illegal login, network disconnected, IP confliction, record exception, HDD error, and HDD full, hot spare exception, etc.
- VCA detection alarm is supported.
- VCA search for face detection, 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.

Other Local Functions
- Operable by front panel, mouse and 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.

Network Functions
- 4 self-adaptive 10M/100M/1000M network interfaces, and various working modes are configurable: multi-address, network fault tolerance, etc.
- 4 1000M optical fiber interfaces.
- IPv6 is supported.
- TCP/IP protocol, PPPoE, DHCP, DNS, DDNS, NTP, SADP, SMTP, SNMP, NFS, and iSCSI are supported.
- TCP, UDP and RTP for unicast.
- Auto/Manual port mapping by UPnP^{TM}.
- Remote web browser access by HTTPS ensures high security.
- Remote reverse playback via RTSP.
- Support accessing by the platform via ONVIF.
- Remote search, playback, download, locking and unlocking of the record files, and support downloading files breakpoint 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.
- Two-way audio and voice broadcasting.
- Embedded WEB server.

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

TABLE OF CONTENTS

Chapter 1   Introduction

1.1   Front Panel
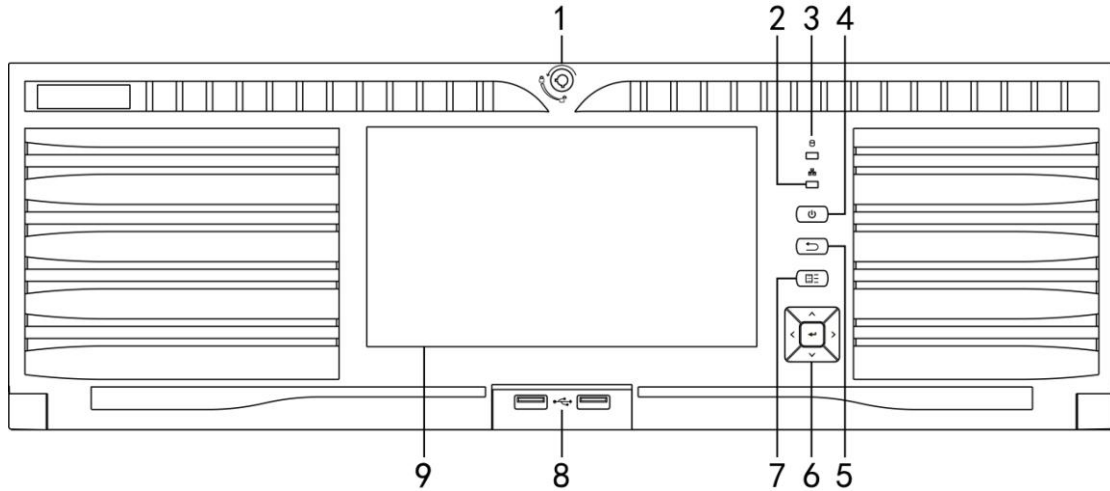
Figure 1. 1 Front Panel

Table 1. 1 Description of Front Panel Buttons

No.	Name		Function Description
1	Front Panel Lock		You can lock or unlock the panel by the key.
2	Tx/Rx Status Indicator		Flashes blue when network connection is functioning properly.
3	HDD Status Indicator		Flashes red when data is being read from or written to HDD.
	POWER ON/OFF		Power on/off switch.
5	ESC		Back to the previous menu.
			Press to enter the PTZ control mode of the first camera.
			Double-press for switching between main and auxiliary output.
6	Control Buttons	DIRECTION	The DIRECTION buttons are used to navigate between different fields and items in menus.
			In the Playback mode, the Up and Down button is used to speed up and slow down recorded video. The Left and Right button is used to reverse 30s and forward 30s the playback progress.
			In Live View mode, the Up button is to switch the live view mode between single- and multi-window divisions. The Down button is used to enter the normal playback mode. The Left button is to show the quick setting toolbar. And the Right button can be used to switch the live view image of the next camera.
			In PTZ control mode, it can control the movement of the PTZ camera.
		ENTER	The ENTER button is used to confirm selection in any of the menu modes.
			It can also be used to *tick* checkbox fields.
			In Playback mode, it can be used to play or pause the video.
			In single-frame Playback mode, pressing the button will advance the video by a single frame.
			In Auto-switch mode, it can be used to stop /start auto switch.

No.	Name	Function Description
7	MENU	Pressing the button will help you return to the Main menu (after successful login).
		Press and hold the button for 5 seconds will turn off audible key beep.
8	USB Interfaces	Universal Serial Bus (USB) ports for additional devices such as USB mouse and USB Hard Disk Drive (HDD). ![NOTE]The USB ports are provided for the use of intel board when it is connected.
9	Touch LCD Screen	The touch LCD is supported by /H and /H/I models by default, and is optional for other models. It outputs the simultaneous image with the VGA/HDMI1 and the local menu can be controlled by the touch operation.

1.2   USB Mouse Operation

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

1. Plug USB mouse into one of the USB interfaces on the front panel of the NVR.

2. The mouse should automatically be detected. If in a rare case that the mouse is not detected, the possible reason may be that the two devices are not compatible, please refer to the recommended the device list from your provider.

The operation of the mouse:

Table 1. 2 Description of the Mouse Control

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

1.3   Input Method Description

Figure 1. 2 Soft Keyboard (1)

Figure 1. 3 Soft Keyboard (2)

Description of the buttons on the soft keyboard:

Table 1. 3 Description of the Soft Keyboard Icons

Icon	Description	Icon	Description
0 ... 9	Numbers	A ... Z	Capital English
⬆	Lowercase/Uppercase	⌫	Backspace
123/., ABC	Switch the keyboard	␣	Space
◀ ▶	Positioning the cursor	↵	Exit
#+=	Symbols	🌐	Reserved

1.4   Rear Panel
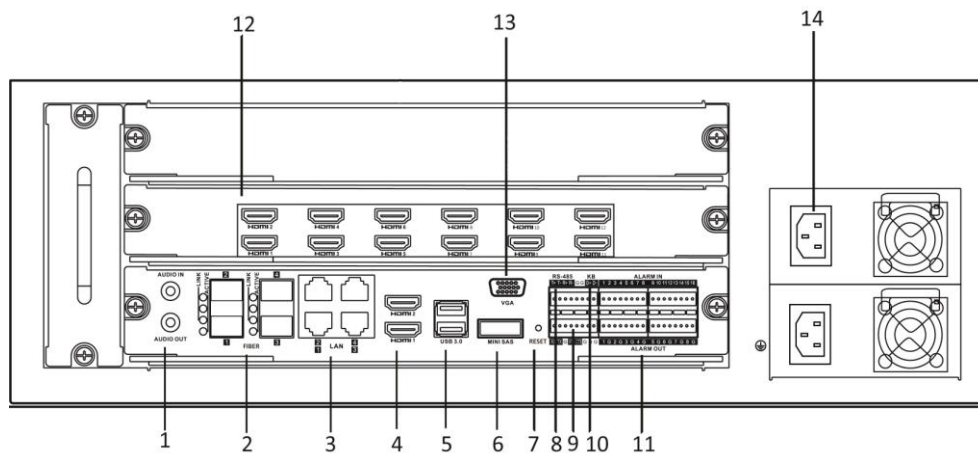
Figure 1. 4 Rear Panel

Table 1. 4 Description of the Rear Panel

No.	Item	Description
1	**AUDIO OUT**	RCA connector for audio output. This connector is synchronized with VGA video output.
	AUDIO IN	RCA connector for audio input.
2	**FIBER Interface**	4 FIBER network interfaces.
3	**LAN Interface**	4 LAN network interfaces.
4	**HDMI™**	2 HDMI™ video output connectors.
5	**USB 3.0 interface**	Universal Serial Bus (USB) ports for additional devices such as USB mouse and USB Hard Disk Drive (HDD).
6	**MINI SAS (Optional)**	Connects to SAS expansion enclosure.
7	**Reset**	Reset the device.
8	**RS-485 Interface**	Connector for RS-485 devices. T+ and T- pins connect to R+ and R- pins of PTZ receiver respectively.
9	**RS-232 Interface**	Connector for RS-232 devices.
10	**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.
11	**ALARM IN**	Connector for alarm input.
	ALARM OUT	Connector for alarm output.
12	**HDMI™ Output Extension Board**	16 HDMI™ video output connectors. (provided for /H and /H/I models only)
13	**VGA**	DB9 connector for VGA output. Display local video output and menu.
14	**AC 100V ~ 240V**	100 ~ 240VAC power supply.

Chapter 2   Getting Started

2.1 Starting Up and Shutting Down the NVR

Purpose:

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

Before you start:

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

Starting up the NVR:

Steps:

1. Plug the power supply into an electrical outlet. It is HIGHLY recommended t plug that an Uninterruptible Power Supply (UPS) be used in conjunction with the device. The Power indicator LED should turn blue indicating that the unit begins to start up.

2. After startup, the Power indicator LED remains blue.

Shutting down the NVR

There are two proper ways to shut down the NVR.

*   **OPTION 1: Standard shutdown**

    Steps:
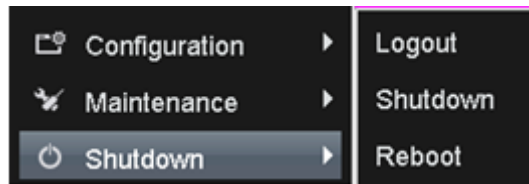
    1. Enter the Shutdown menu.

        Menu > Shutdown

Figure 2. 1 Shutdown Menu

---

    2. Click the **Shutdown** button.

    3. Click the **Yes** button.

*   **OPTION 2: By operating the front panel**

    Steps:

    1. Press and hold the POWER button on the front panel for 3 seconds.

    2. Enter the administrator's username and password in the dialog box for authentication if needed.

    3. Click the **Yes** button.

Do not press the POWER button again when the system is shutting down.

Rebooting the NVR

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

Steps:

1. Enter the **Shutdown** menu by clicking Menu > Shutdown.

2. Click the **Logout** button to lock the NVR or the **Reboot** button to reboot the NVR.

2.2   Setting the Admin Password

Purpose:

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

Steps:

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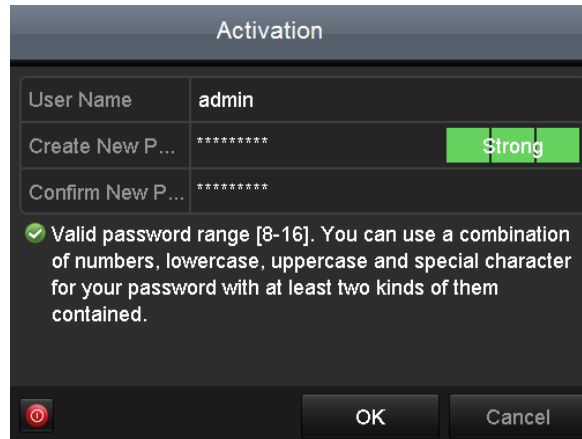

Figure 2. 2 Settings Admin Password

> ⚠ **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. 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.*

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

For the old version device, if you update it to the new version, the following dialog box will pop up once the device starts up. You can click **YES** and follow the wizard to set a strong password.
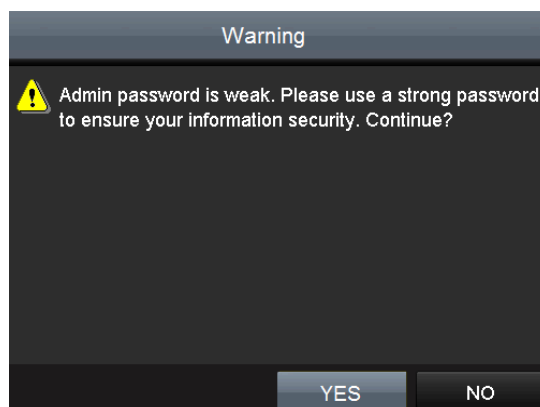

Figure 2. 3 Warning

2.3 Using the Wizard for Basic Configuration

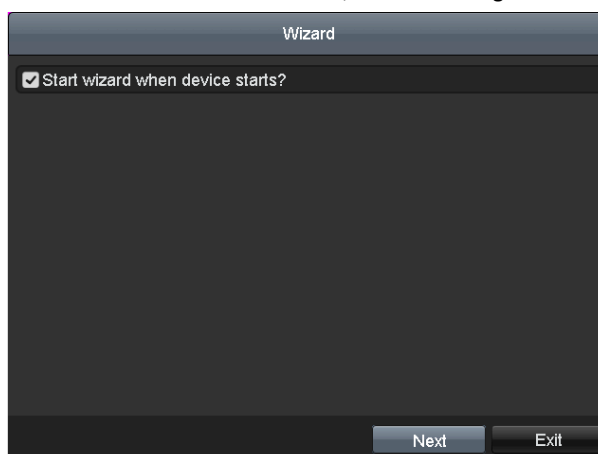By default, the Setup Wizard starts once the NVR has loaded, as shown in Figure 2. 4.

Figure 2. 4 Start Wizard Interface

Operating the Setup Wizard:

1. The Setup Wizard can walk you through some important settings of the NVR. If you don't want to use the Setup Wizard at that moment, click the **Cancel** button. You can also choose to use the Setup Wizard next time by leaving the "Start wizard when the device starts?" checkbox checked.

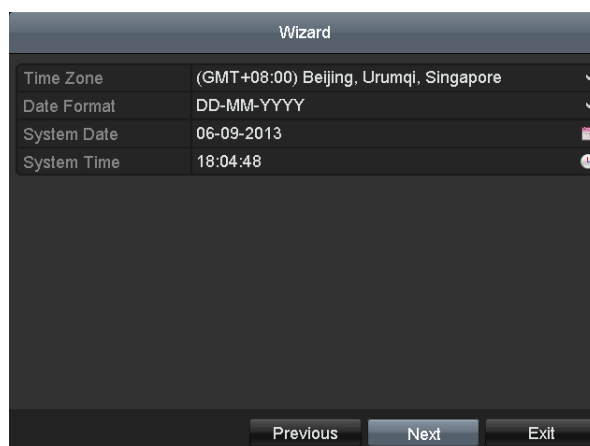2. Click **Next** button to enter the date and time settings window, as shown in Figure 2. 5.

Figure 2. 5 Date and Time Settings

3. After the time settings, click **Next** button which takes you back to the Network Setup Wizard window, as shown in the following figure.
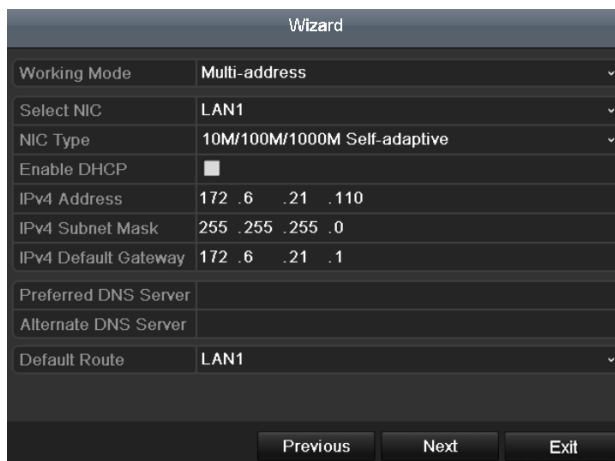
Figure 2. 6 Network Configuration

4. Click **Next** button after you configured the network parameters, which takes you to the RAID configuration window.
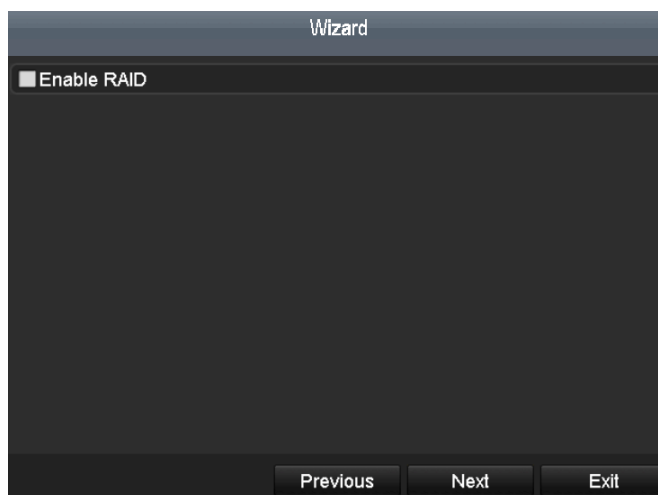

Figure 2. 7 Array Management

5. Click **Next** button to enter the Array Management window (Supported if you check the checkbox to enable the RAID function in the previous window).
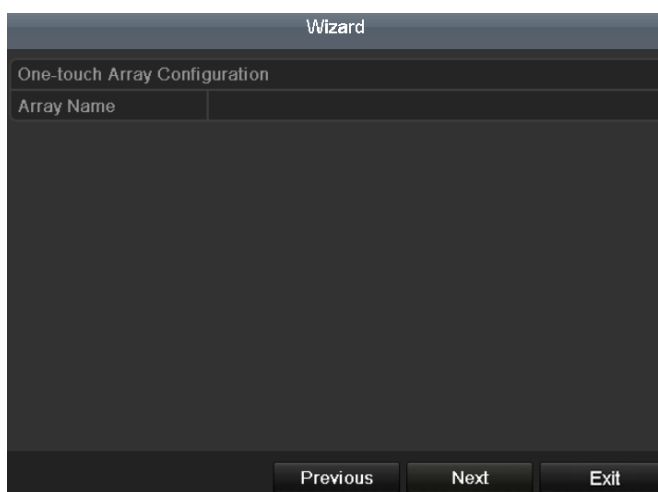

Figure 2. 8 Array Management

6. Click **Next** button after you configured the network parameters, which takes you to the **HDD Management** window, shown in Figure 2. 9.
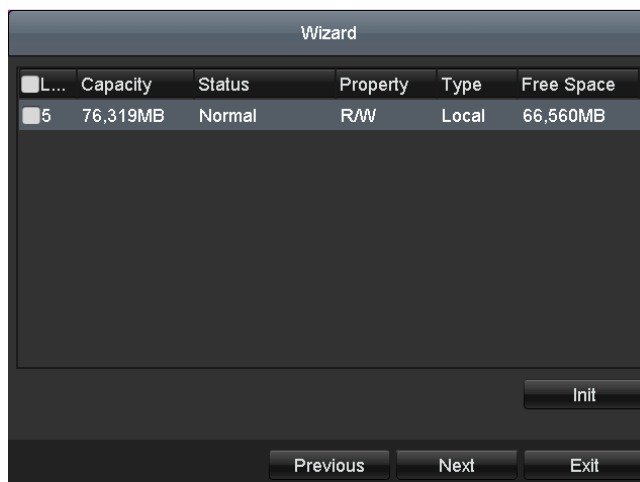

Figure 2. 9 HDD Management

7. To initialize the HDD, click the **Init** button. Initialization removes all the data saved in the HDD.

8. Click **Next** button. You enter the **Adding IP Camera** interface.

9. Click **Search** to search the online IP Camera and the **Security** status shows whether it is active or inactive. Before adding the camera, make sure the IP camera to be added is in active status.
If the camera is in inactive status, you can click the inactive icon of the camera to set the password to activate it. You can also select multiple cameras from the list and click the **One-touch Activate** to activate the cameras in batch.
Click the **Add** to add the camera.

Figure 2. 10 Add IP Cameras

10. Click **Next** button. Configure the recording for the searched IP Cameras.
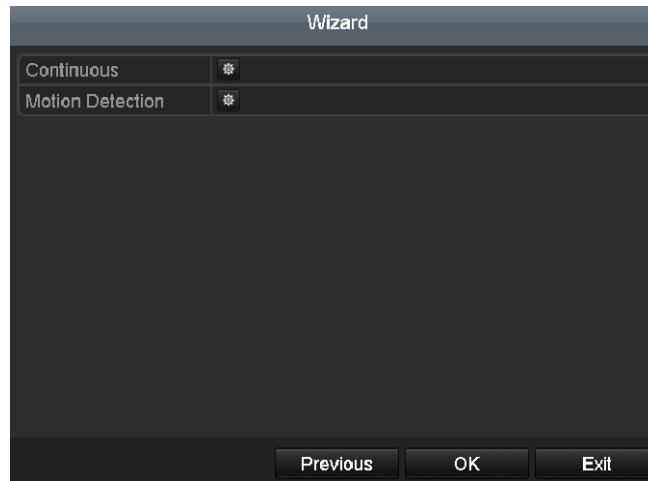
Figure 2. 11 Record Settings

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

2.4   Adding and Connecting the IP Cameras

2.4.1 Setting the Admin Password for IP Camera

Purpose:

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

Steps:

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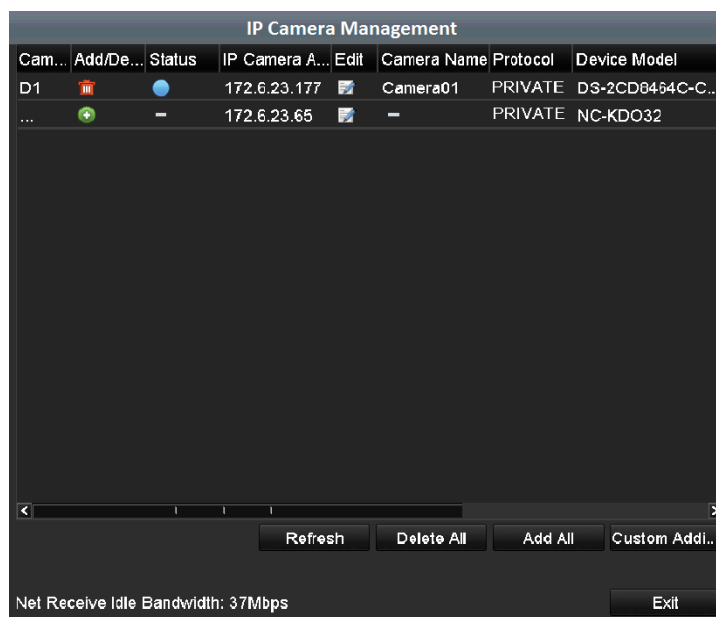

Figure 2. 12 IP Camera Management Interface

2. Click the inactive icon of the camera to enter the following interface to activate it. You can also select multiple cameras from the list and click the **One-touch Activate** to activate the cameras in batch.
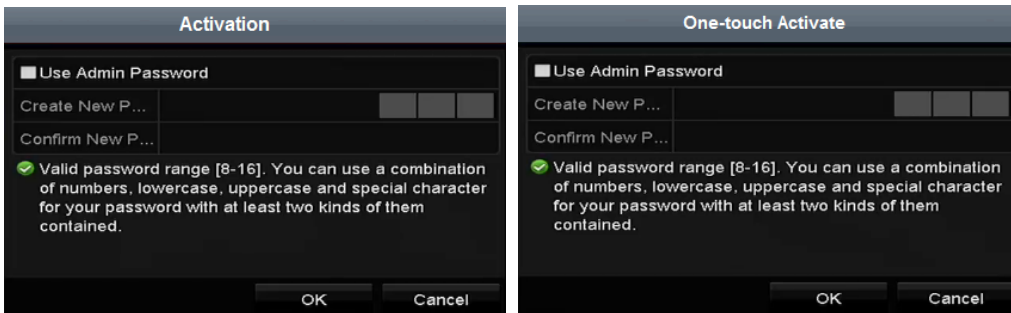
Figure 2. 13 Activate the Camera

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

   Use Admin Password: when you check the checkbox, the camera (s) will be configured with the same admin password of the operating NVR.
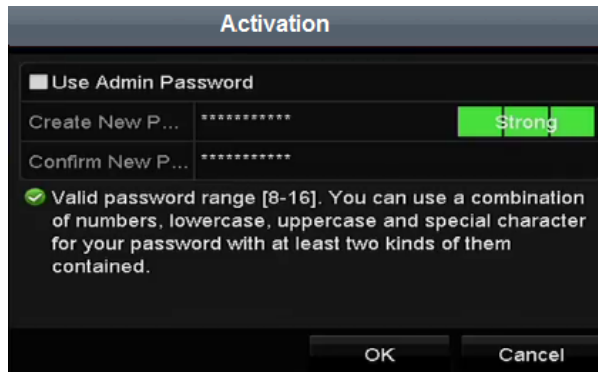
Figure 2. 14 Set New Password

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

> ⚠️ **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.*

4. Click **OK** to finish the acitavting of the IP camera. And the security status of camera will be changed to **Active**.

2.4.2 Adding the Online IP Cameras

Purpose:

The main function of the NVR is to connect the network cameras and record the video got from it. So before you can get a live view or record of the video, you should add the network cameras to the connection list of the device.

Before you start:

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

- **OPTION 1:**

Steps:

1. Click to select an idle window in the live view mode.
2. Click the [icon] icon in the center of the windw to pop up the adding IP camera interface.

Figure 2. 15 Quick Adding IP Camera Interface

3. Select the detected IP camera and click the **Add** button to add it directly, and you can click the **Search** button to refresh the online IP camera manually.

   Or you can choose to custom add the IP camera by editing the parameters in the corresponding textfiled and then click the **Add** button to add it.

- **OPTION 2:**

Steps:

1. Select the **Add IP Camera** option from the right-click menu in live view mode or click Menu> Camera> Camera to enter the IP camera management interface.
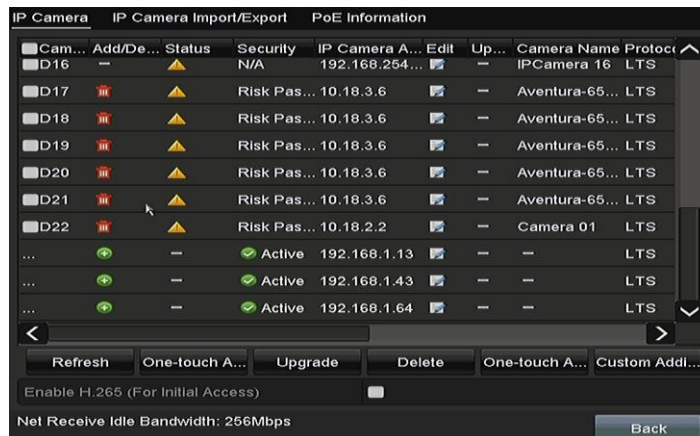
Figure 2. 16 Adding IP Camera Interface

2. The online cameras with same network segment will be detected and displayed in the camera list.
3. Select the IP camera from the list and click the [icon] button to add the camera. Or you can click the

One-touch Adding button to add all cameras (with the same login password) from the list.

NOTE

Make sure the camera to add has already been actiavted.

4. (For the encoders with multiple channels only) check the checkbox of Channel Port in the pop-up window, as shown in the following figure, and click **OK** to add multiple channels.
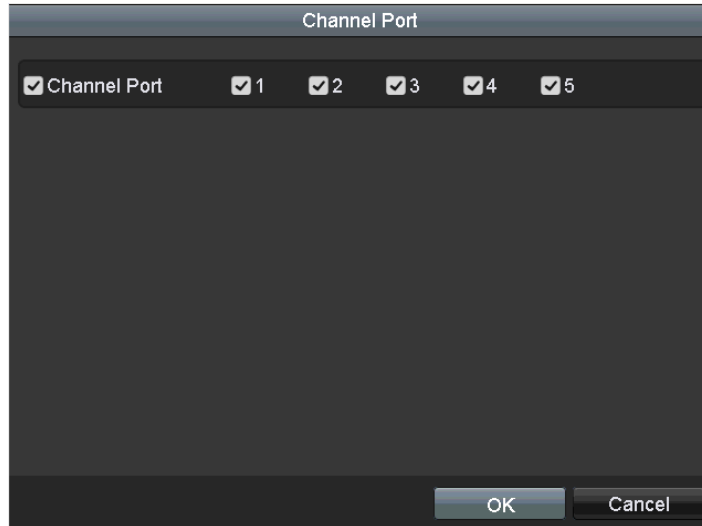
Figure 2. 17 Selecting Multiple Channels

- **OPTION 3:**

    Steps:

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

Figure 2. 18 Custom Adding IP Camera Interface

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

NOTE

If the IP camera to add has not been actiavated, 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.

For the successful**y** added IP cameras, the Security status shows the security level of the password of camera: strong password, weak password and risk password.
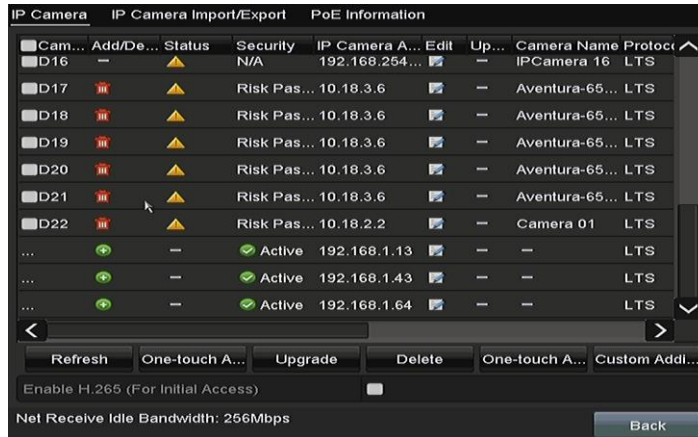

Figure 2. 19 Successfully Added IP Cameras

Table 2. 1 Explanation of the icons

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

2.4.3 Editing the Connected IP cameras and Configuring Customized Protocols

After the adding of the IP cameras, the basic information of the camera lists in the page, you can configure the basic setting of the IP cameras.

Steps:

1. Click the   icon to edit the parameters; you can edit the IP address, protocol and other parameters.
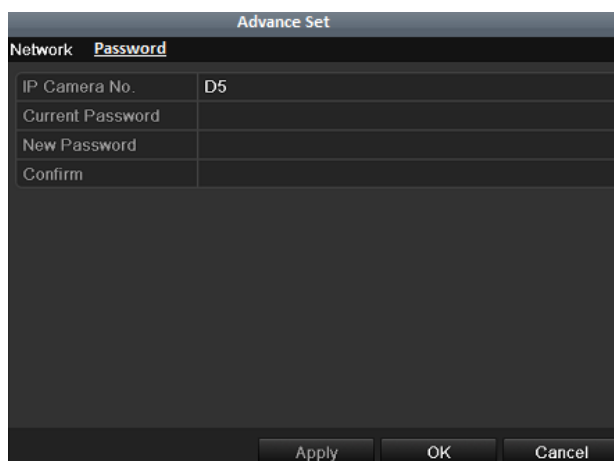
Figure 2. 20 Edit the Parameters

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

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

To edit advanced parameters:

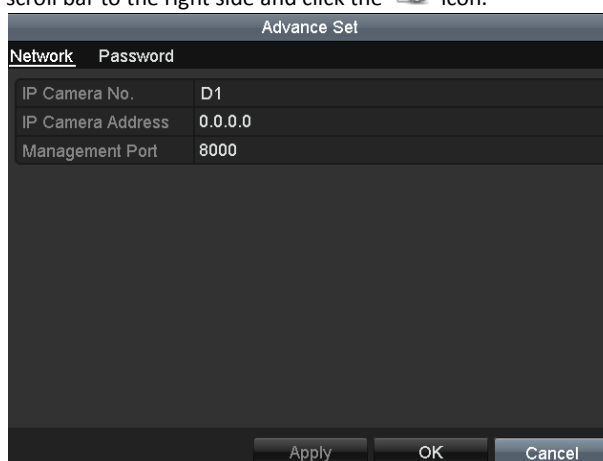1. Drag the horizontal scroll bar to the right side and click the icon.

Figure 2. 21 Network Configuration of the Camera

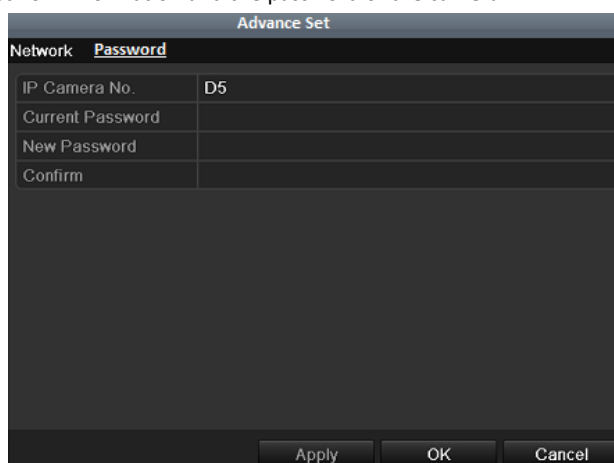2. You can edit the network information and the password of the camera.

Figure 2. 22 Password Configuration of the Camera

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

Configuring the customized protocols

Purpose:

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

Steps:

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

Figure 2. 23 Protocol Management Interface

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

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

NOTE

Before customizing the protocol for the network camera, you have to contact the manufacturer of the network camera to consult the URL (uniform resource locator) for getting main stream and sub-stream.

The format of the URL is: [Type]://[IP Address of the network camera]:[Port]/[Path].

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

- **Protocol Name:** Edit the name for the custom protocol.
- **Enable Substream:** If the network camera does not support sub-stream or the sub-stream is not needed leave the checkbox empty.
- **Type:** The network camera adopting custom protocol must support getting 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 is listed in the dropdown list, please refer to Figure 2. 24.
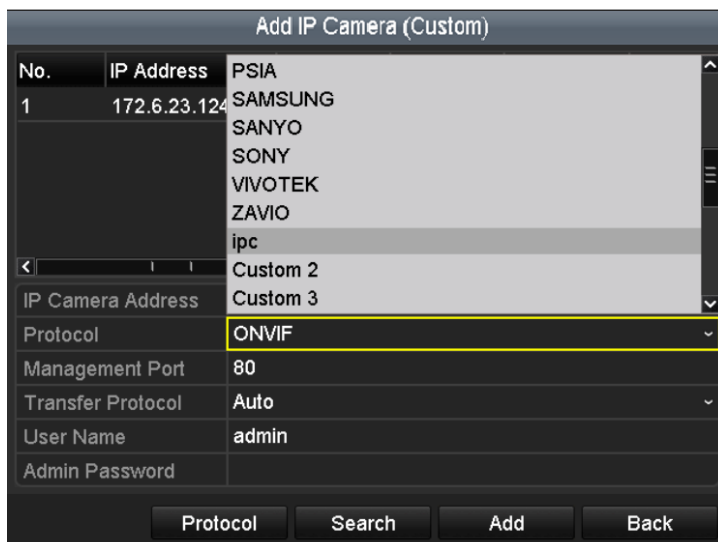
Figure 2. 24 Protocol Setting

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

Chapter 3   Live View

3.1   Introduction of Live View

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

Live View Icons

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

Table 3. 1 Description of Live View Icons

Icons	Description
	Alarm (video loss, video tampering, motion detection, sensor alarm, or VCA alarm)
	Record (manual record, schedule record, motion detection, alarm or VCA triggered record)
	Alarm & Record
	Event/Exception (motion detection, sensor alarm, VCA or exception information, appears at the lower-left corner of the screen. Please refer to *Chapter 8.6 Setting Alarm Response Actions* for details.)

3.2   Operations in Live View Mode

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

- **Single Screen**: showing only one screen on the monitor.
- **Multi-screen:** showing multiple screens on the monitor simultaneously.
- **Auto-switch:** the screen is auto switched to the next one. And 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 to Standard, Bright, Gentle or Vivid.
- **Add IP Camera:** the shortcut to the IP camera management interface.
- **Playback:** playback the recorded videos for current day.
- **Aux/Main output switch:** the NVR checks the connection of the output interfaces to define the main and auxiliary output interfaces. By default the HDMI1/VGA/LCD is the main output, and the HDMI2 is the auxiliary one.
  You can click the Aux Monitor button in the right-click menu to switch the video output to the auxiliary one, and when the aux output is enabled, the main output cannot do any operation, and you can do some basic operation on the live view mode for the Aux output.

3.2.1 Front Panel Operation on Live View

Table 3. 2 Front Panel Operation in Live View

Functions	Front Panel Operation
Manually switch screens	Next screen: right/down direction button. Previous screen: left/up direction button.
Auto-switch	Press **Enter** button.
Activate right-click menu	On the LCD screen, tap the icon on the lower-left corner of the screen to pop up the right-click menu.

3.2.2 Using the Mouse in Live View

Table 3. 3 Mouse Operation in Live View

Name	Description
Common Menu	Quick access to the sub-menus which you frequently visit.
Menu	Enter the main menu of the system by right clicking the mouse.
Single Screen	Switch to the single full screen by choosing channel number from the dropdown list.
Multi-screen	Adjust the screen layout by choosing from the dropdown 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 Control	
Output Mode	Four modes of output supported, including Standard, Bright, Gentle and Vivid.
Aux Monitor	Switch to the auxiliary output mode and the operation for the main output is disabled.

NOTE

- The *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 3. 1 Right-click Menu

3.2.3 Using an Auxiliary Monitor

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

- **Single Screen:** Switch to a full screen display of the selected camera. Camera can be selected from a dropdown list.

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

NOTE

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

3.2.4 Quick Setting Toolbar in Live View Mode

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

Figure 3. 2 Quick Setting Toolbar

Table 3. 4 Description of Quick Setting Toolbar Icons

Icon	Description	Icon	Description	Icon	Description
	Enable/Disable Manual Record		Instant Playback		Mute/Audio on
	Capture		PTZ Control		Digital Zoom
	Image Settings		Live View Strategy		Stream Information
	Close				

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

Digital Zoom can zoom in the selected area to the full screen. You can left-click and draw to select the area to zoom in, as shown in Figure 3. 3.

Figure 3. 3 Digital Zoom

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

You can set the image parameters like brightness, contrast, saturation and hue.
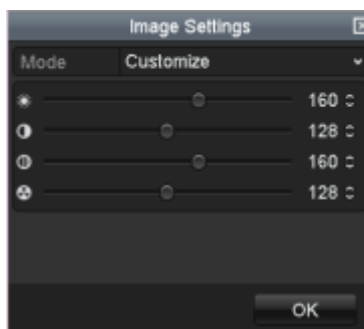

Figure 3. 4 Image Settings- Customize

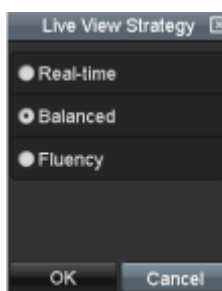 Live View Strategy can be selected to set strategy, including Real-time, Balanced, Fluency.

Figure 3. 5 Live View Strategy

3.3   Adjusting Live View Settings

Purpose:

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

Steps:

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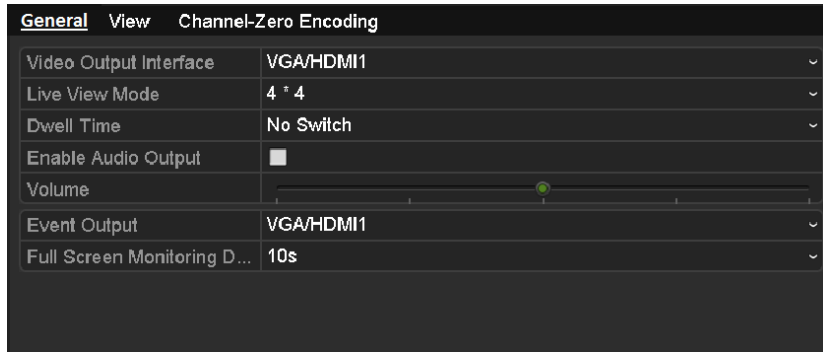
    Menu> Configuration> Live View

Figure 3. 6 Live View-General

The settings available in this menu include:

*   **Video Output Interface:** Designates the output to configure the settings. Outputs include VGA/HDMI, and HDMI2.

*   **Live View Mode:** Designates the display mode to be used for Live View.

*   **Dwell Time:** The time in seconds to *dwell* between switching of channels when enabling auto-switch in Live View.

*   **Enable Audio Output:** Enables/disables audio output for the selected video output.

*   **Event Output:** Designates the output to show event video.

*   **Full Screen Monitoring Dwell Time:** The time in seconds to show alarm event screen.

2. Setting Cameras Order

Figure 3. 7 Live View- Camera Order

1) Select a **View** mode in .

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

   You can click button to start live view for all the channels and click to stop all the live view.

3) Click the **Apply** button to save the setting.

Chapter 4   PTZ Controls

4.1 Configuring PTZ Settings

Purpose:

Follow the procedure to set the parameters for PTZ. The configuring of the PTZ parameters should be done before you control the PTZ camera.

Steps:

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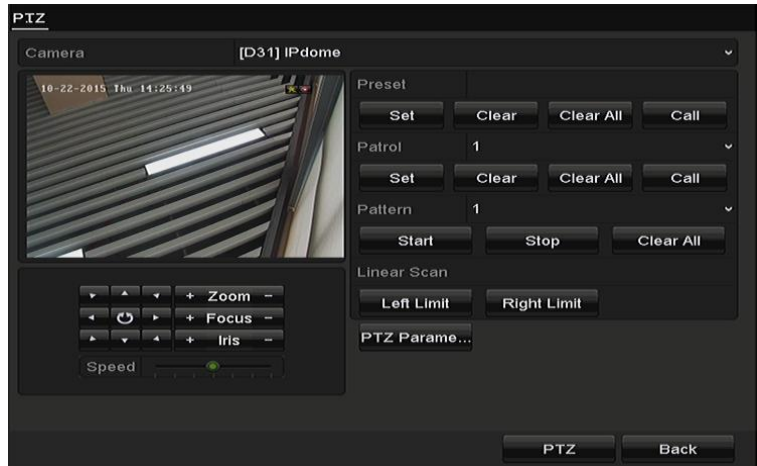
   Menu >Camera> PTZ

Figure 4. 1 PTZ Settings

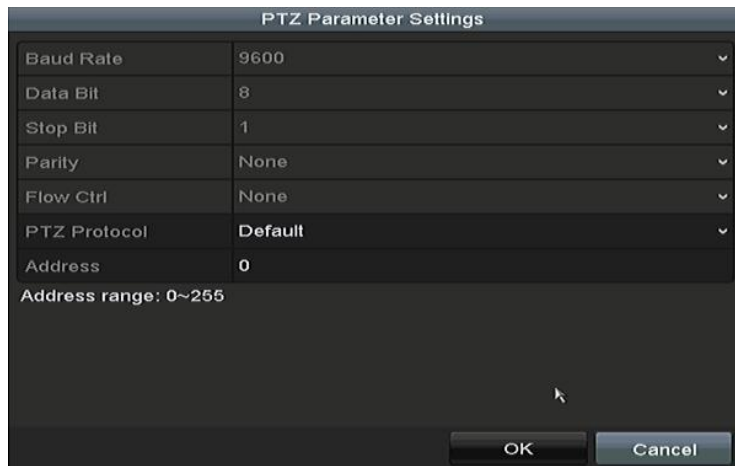2. Click the **PTZ Parameter Settings** button to set the RS-485 parameters.

Figure 4. 2 PTZ- General

3. Enter the parameters of the PTZ camera.

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

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

4.2 Setting PTZ Presets, Patrols & Patterns

Before you start:

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

4.2.1 Customizing Presets

Purpose:

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

Steps:

1. Enter the PTZ Control interface.

   Menu>Camera>PTZ

Figure 4. 3 PTZ Settings

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

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

   Repeat the steps2-3 to save more presets.

   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.

4.2.2 Calling Presets

Purpose:

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

Steps:

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 [image] 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 dropdown list.

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

Figure 4. 4 PTZ Panel - General

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

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

4.2.3 Customizing Patrols

Purpose:

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

Steps:

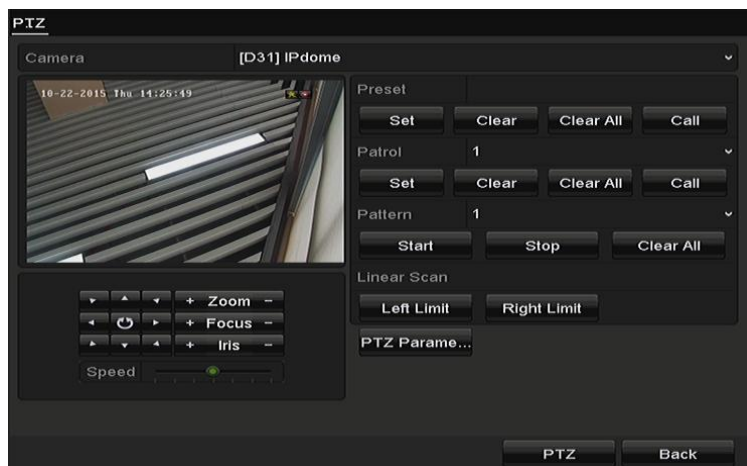1. Enter the PTZ Control interface.

   Menu>Camera>PTZ

Figure 4. 5 PTZ Settings

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

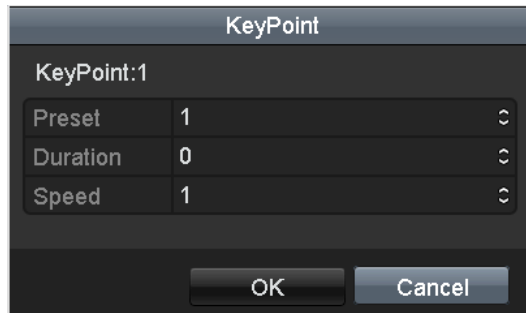3. Click the **Set** button to add key points for the patrol.

Figure 4. 6 Key point Configuration

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

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

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

4.2.4 Calling Patrols

Purpose:

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

Steps:

1. Click the button **PTZ** in the lower-right corner of the PTZ setting interface;

   Or press the PTZ button on the front panel or click the PTZ Control icon in the quick setting bar, or

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

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

Figure 4. 7 PTZ Panel - General

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

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

4.2.5 Customizing Patterns

Purpose:

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

Steps:

1. Enter the PTZ Control interface.

    Menu > Camera > PTZ

Figure 4. 8 PTZ Settings

2. Choose pattern number in the dropdown list.

3. Click the **Start** button and click corresponding buttons in the control panel to move the PTZ camera, and click the **Stop** button to stop it.

    The movement of the PTZ is recorded as the pattern.

4.2.6 Calling Patterns

Purpose:

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

Steps:

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 ![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 ![icon] button to show the general settings of the PTZ control.

Figure 4. 9 PTZ Panel - General

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

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

4.2.7 Customizing Linear Scan Limit

Purpose:

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

This function is supported by some certain models.

Steps:

1. Enter the PTZ Control interface.

   Menu > Camera > PTZ

Figure 4. 10 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.

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 should be no more than 180º.

4.2.8 Calling Linear Scan

Purpose:

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

Steps:

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 4. 11 PTZ Panel - One-touch

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

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

4.2.9 One-touch Park

Purpose:

For some certain model of the speed dome, it can be configured to start a predefined park action (scan, preset, patrol and etc.) automatically after a period of inactivity (park time).

Steps:

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 4. 12 PTZ Panel - One-touch

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

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

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

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

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

4. Click the button again to inactivate it.

4.3 PTZ Control Panel

To enter the PTZ control panel, there are two ways supported.

OPTION 1:

In the PTZ settings interface, click the **PTZ** button on the lower-right corner which is 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.

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

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

Figure 4. 13 PTZ Panel

Table 4. 1 Description of the PTZ panel icons

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

Chapter 5   Recording Settings

5.1 Configuring Parameters

Purpose:

By configuring the parameters you can define the parameters which affect the image quality, such as the transmission stream type, the resolution and so on.

Before you start:

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

Figure 5. 1 HDD- General

2. Check the storage mode of the HDD

   1) Click **Advanced** to check the storage mode of the HDD.

   2) If the HDD mode is *Quota*, please set the maximum record capacity and maximum picture capacity. For detailed information, see *Chapter Configuring Quota Mode.*

   3) If the HDD mode is **Group**, you should set the HDD group. For detailed information, see *Chapter 13 HDD Management.*
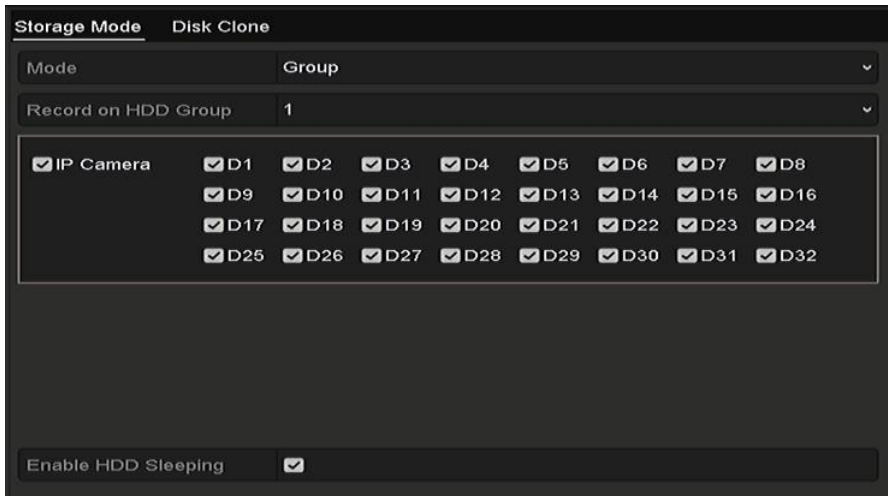

Figure 5. 2 HDD- Advanced

Steps:

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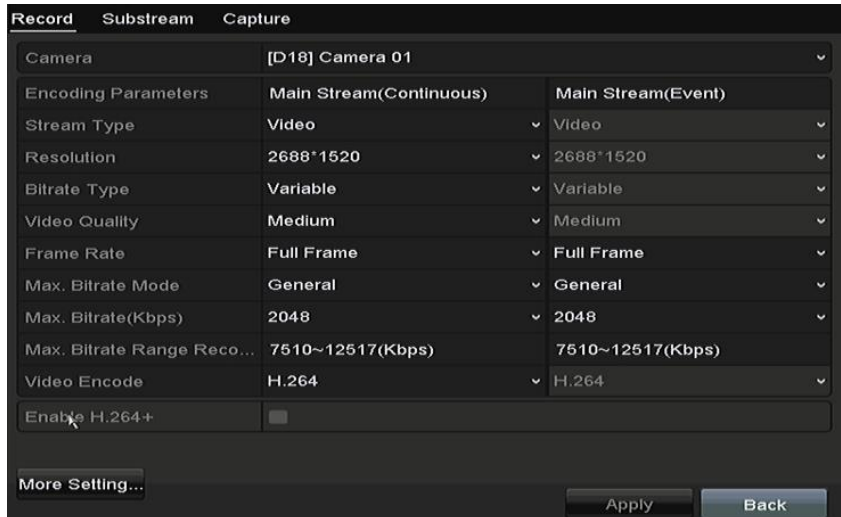
   Menu>Record>Parameters

Figure 5. 3 Recording Parameters

2. Parameters Setting for Recording

1) Select **Record** tab page to configure. You can configure the stream type, the resolution, and other parameters on your demand.

2) Click the **More Settings** button to set the advanced parameters for recording and then click **OK** button to finish editing.
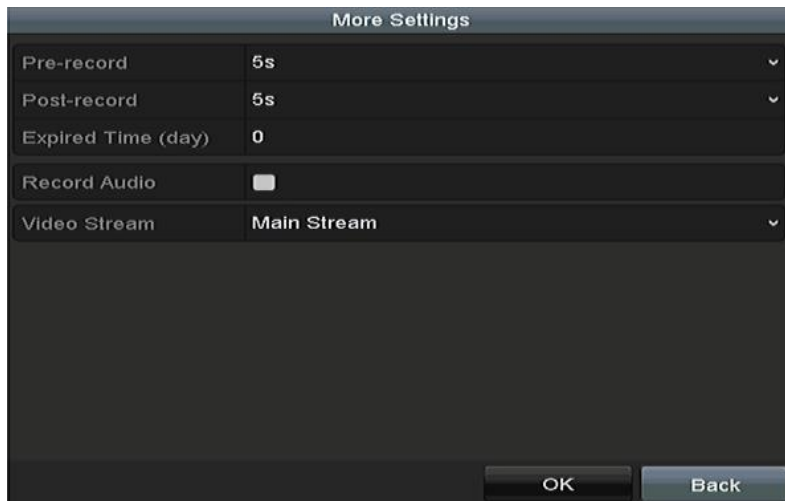

Figure 5. 4 Recording Parameters-More Settings

- **Pre-record:** The time you set to record before the scheduled time or event. For example, when an alarm triggered the recording at 10:00, if you set the pre-record time as 5 seconds, the camera records it at 9:59:55.

- **Post-record:** The time you set to record after the event or the scheduled time. For example, when an alarm triggered the recording ends at 11:00, if you set the post-record time as 5 seconds, it records till 11:00:05.

- **Expired Time:** The expired time is the longest time for a record file to be kept in the HDD, if the deadline is reached, the file will be deleted. You can set the expired time to 0, and then the file will not be deleted. The actual keeping time for the file should be determined by the capacity of the HDD.

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

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

- The redundant record is to decide whether you want the camera to save the record files in the redundant HDD. You must configure the redundant HDD in HDD settings. For detailed information, see *Chapter 13.3.2*.
- The parameters of Main Stream (Event) are read-only.

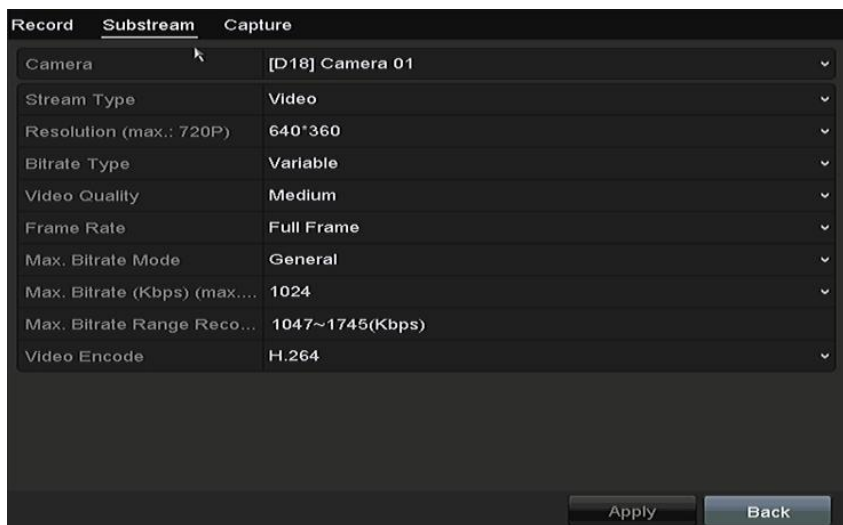3. Parameters Settings for Sub-stream

1) Enter the Sub-stream tab page.

Figure 5. 5 Sub-stream Parameters

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

5.2 Configuring Recording Schedule

Purpose:

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

In this chapter, we take the record schedule procedure as an example, and the same procedure can be applied to configure schedule for both recording.

Steps:

1. Enter the Record Schedule interface.

    Menu>Record >Schedule

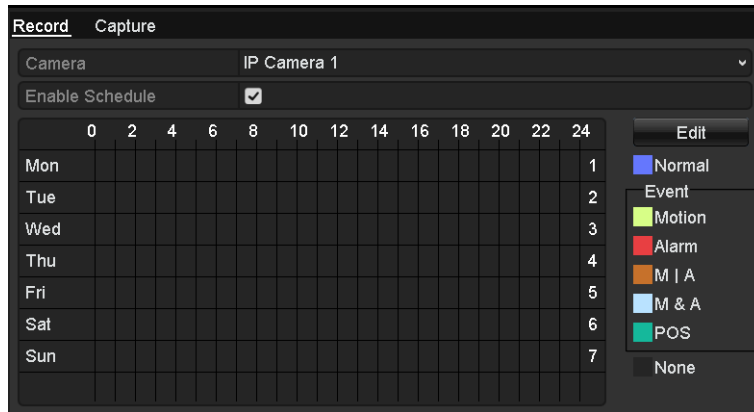2. Configure Record Schedule

1) Select Record Schedule.

Figure 5. 6 Record Schedule

Different recording types are marked in different color icons.

Continous: scheduled recording.

Event: recording triggered by all event triggered alarm.

Motion: recording triggered by motion detection.

Alarm: recording triggered by alarm.

M/A: recording triggered by either motion detection or alarm.

M&A: recording triggered by motion detection and alarm.

You can delete the set schedule by clicking the **None** icon.

2) Choose the camera you want to configure.

3) Select the check box after the **Enable Schedule** item.

4) Click **Edit** button or click on the color icon under the edit button and draw the schedule line on the panel.

Edit the schedule:

I. In the message box, you can choose the day to which you want to set schedule.
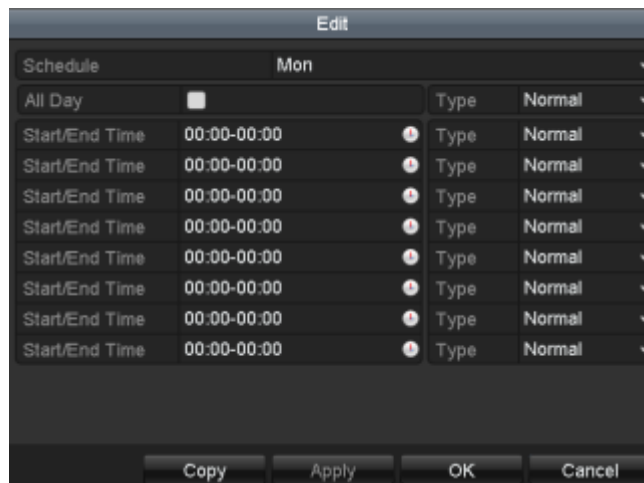

Figure 5. 7 Recording Schedule Interface

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

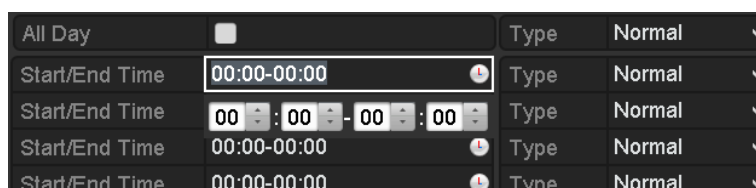II. To schedule an all-day recording, check the checkbox after the **All Day** item.

Figure 5. 8 Edit Schedule

III. To arrange other schedule, leave the **All Day** checkbox blank and set the Start/End time.

NOTE

Up to 8 periods can be configured for each day. And the time periods can't be overlapped each other.

IV. Select the record type in the dropdown list.

NOTE

● To enable Motion, Alarm, M | A (motion or alarm), M & A (motion and alarm) and VCA (Video Content Analysis) triggered recording, you must configure the motion detection settings, alarm input settings or VCA settings as well. For detailed information, refer to *Chapter 8.1*, *Chapter 8.2 and Chapter 8.5*.

● The VCA settings are only available to the smart IP cameras.

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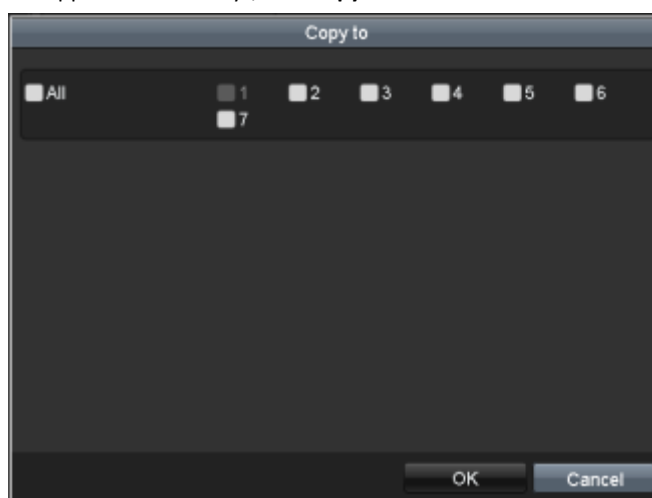

Figure 5. 9 Copy Schedule to Other Days

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

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

Draw the schedule:

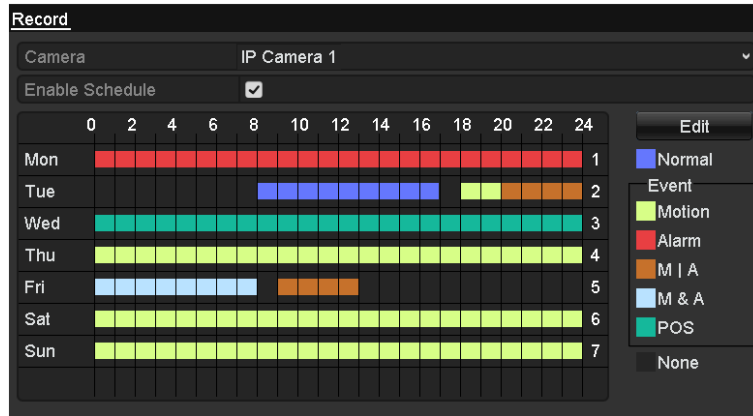I. Click on the color icons, you can choose the schedule type as continuous or event.

Figure 5. 10 Draw the Schedule

II. Click the **Apply** button to validate the settings.

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

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

5.3 Configuring Motion Detection Recording

Purpose:

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 which triggered by the detected motion.

Steps:

1. Enter the Motion Detection interface.

   Menu>Camera>Motion

Figure 5. 11 Motion Detection

2. Configure Motion Detection:

   1) Choose camera you want to configure.

   2) Check the checkbox after **Enable Motion Detection**.

   3) Drag and draw the area for motion detection by mouse. If you want to set the motion detection for all

the area shot by the camera, click **Full Screen**. To clear the motion detection area, click **Clear**.

NOTE The full-screen motion detection is configured by default.
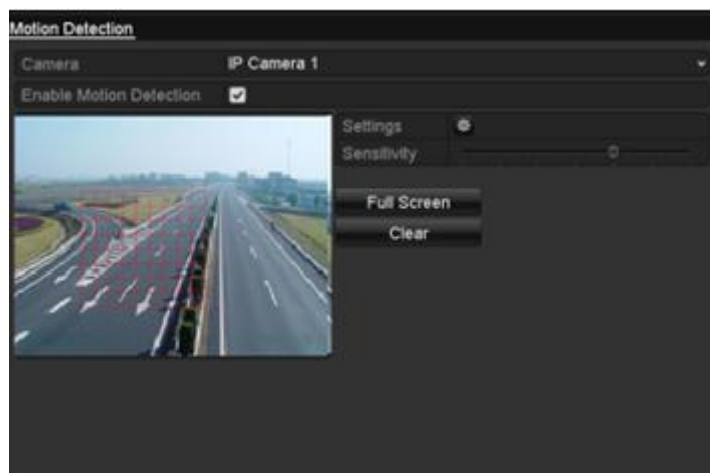

Figure 5. 12 Motion Detection- Mask

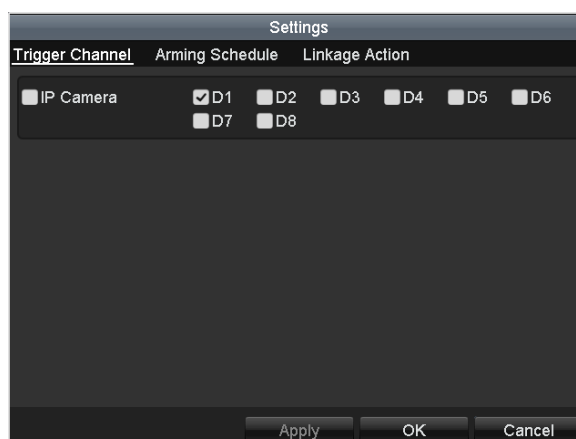4) Click **Settings**, and the message box for channel information pop up.

Figure 5. 13 Motion Detection Handling

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

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

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

8) Exit the Motion Detection menu.

3. Edit the Motion Detection Record Schedule. For the detailed information of schedule configuration, see *Chapter Configuring Recording Schedule.*

5.4   Configuring VCA Event Recording

Purpose:

The event triggered recording can be configured through the menu. Then events include the motion detection, alarm and VCA events (face detection/face capture, line crossing detection, intrusion detection, region entrance detection, region exiting detection, loitering detection, people gathering detection, fast moving detection, parking detection, unattended baggage detection, object removal detection, audio loss exception detection, sudden change of sound intensity detection, and defocus detection).

Steps:

1. Enter the VCA settings interface and select a camera for the VCA settings.

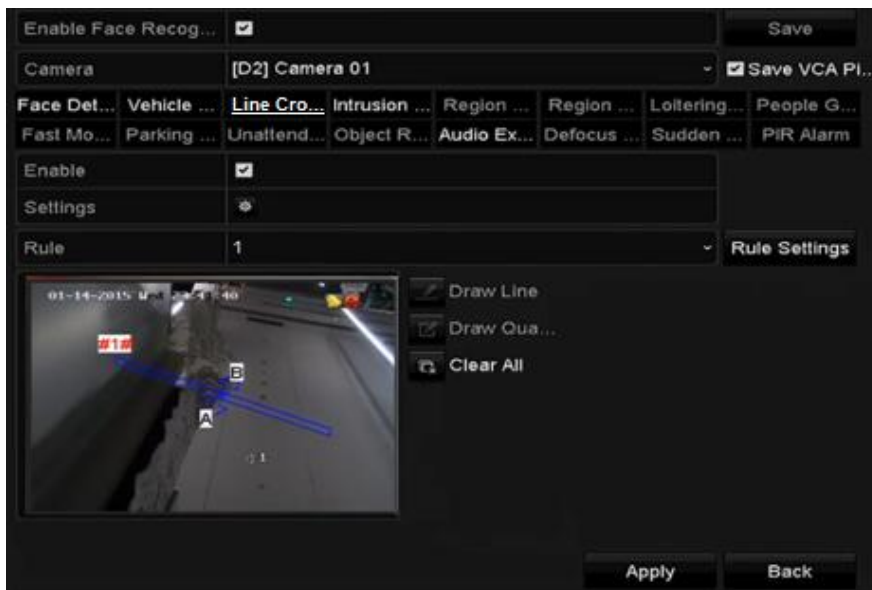   Menu> Camera> VCA

Figure 5. 14 VCA Settings

2. Configure the detection rules for VCA events. For details, see the step 2 in *Chapter 9 VCA Alarm*.

3. Click the icon   to configure the alarm linkage actions for the VCA events.

    Select **Trigger Channel** tab and select one or more channels which will start to record when VCA alarm is triggered.
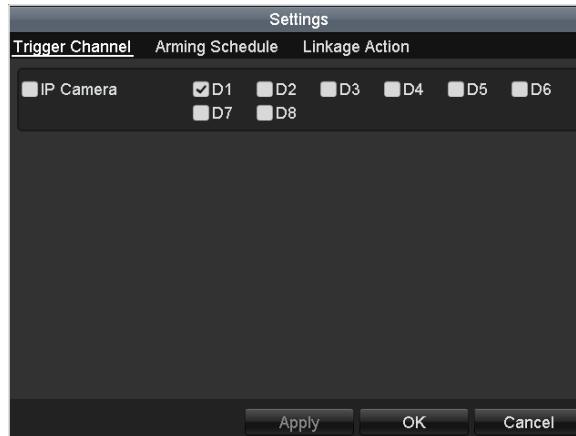
    Click **Apply** to save the settings

Figure 5. 15 Set Trigger Camera of VCA Alarm

NOTE

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

4. Enter Record Schedule settings interface (Menu> Record> Schedule>Record Schedule), and then set VCA as the record type. For details, see step 2 in *Chapter 5.2 Configuring Record Schedule.*

5.5   Configuring Alarm Triggered Recording

Follow the procedure to configure alarm triggered recording.

Steps:

1. Enter the Alarm setting interface.

    Menu> Configuration> Alarm

Figure 5. 16 Alarm Settings

2. Click **Alarm Input**.

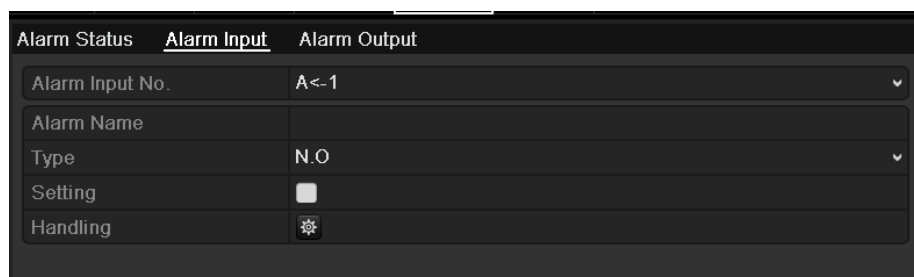| Alarm Status	Alarm Input	Alarm Output	
Alarm Input No.		A<-1	⌄
Alarm Name			
Type		N.O	⌄
Setting		☐	
Handling		⚙	

Figure 5. 17 Alarm Settings- Alarm Input

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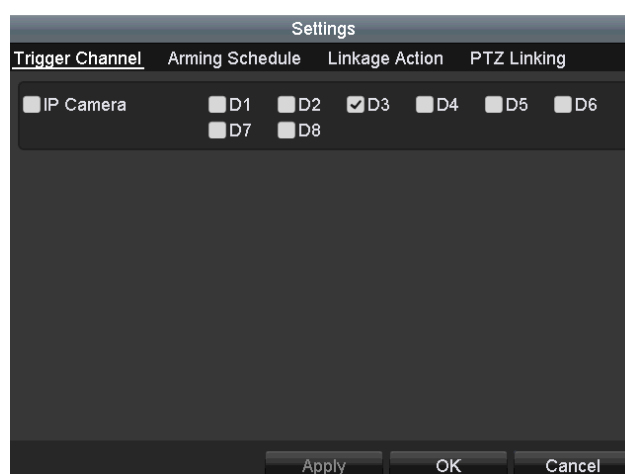3) Check the checkbox for Setting ☑.
4) Click **Settings**.

Settings						
Trigger Channel	Arming Schedule		Linkage Action		PTZ Linking	
☐IP Camera	☐D1	☐D2	☑D3	☐D4	☐D5	☐D6
	☐D7	☐D8				
			Apply	OK	Cancel	

Figure 5. 18 Alarm Settings

5) Choose the alarm triggered recording channel.

6) Check the checkbox ☑ to select channel.

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

8) Click **OK** to back to the upper level menu.

Repeat the above steps to configure other alarm input parameters.

If the settings can also be applied to other alarm inputs, click **Copy** and choose the alarm input number.
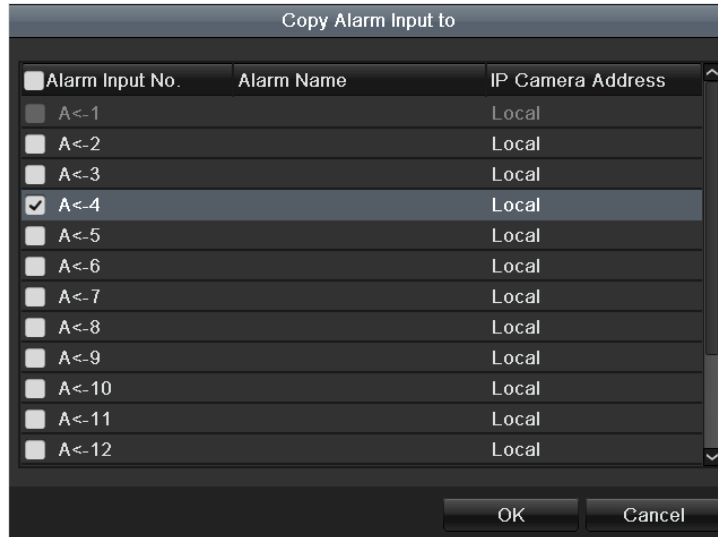
Figure 5. 19 Copy Alarm Input

3. Edit the Alarm triggered record in the Record/Capture Schedule setting interface. For the detailed information of schedule configuration, see *Chapter5.2 Configuring Recording Schedule.*

5.6 Manual Recording

Purpose:

Follow the steps to set the manual recording. When the manual recording is enabled, you don't need to set a schedule for recording..

Steps:

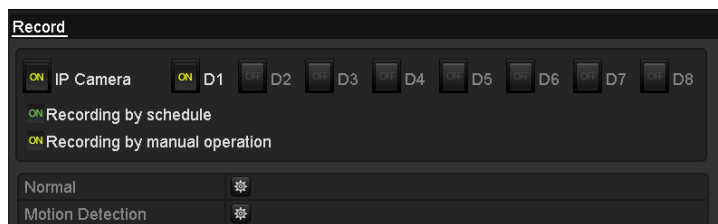1. Enter the Manual settings interface.

   Menu> Manual

Figure 5. 20 Manual Record

2. Enable recording for camera (s).

   Click the status button beside each camera number to change ![OFF] to ![ON], or you can enable recording for all cameras by clicking the status bar before **Analog** to change it to ![ON].

3. Set recording mode to manual.

   By default, the camera is enabled with recording by schedule (![ON]). Click the ![ON] status bar to change it to ![OFF] and click again to enable the recording to manual (![ON]).

   ![ON]: recording by schedule.

   ![ON]: recording by manual operation.

   ![NOTE]After rebooting, all the manual records enabled are canceled.

4. Start all-day continuous recording or all-day motion detection recording of all channels.

     1)   Click   for Continuous or Motion Detection recording.

Figure 5. 21 Start Normal or Motion Detection Recording

     2)   Click **Yes** to enable all-day continuous or motion detection recording of all channels.

5.7 Configuring Holiday Recording

Purpose:

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

Steps:

1. Enter the Record setting interface.

    Menu > Record > Holiday
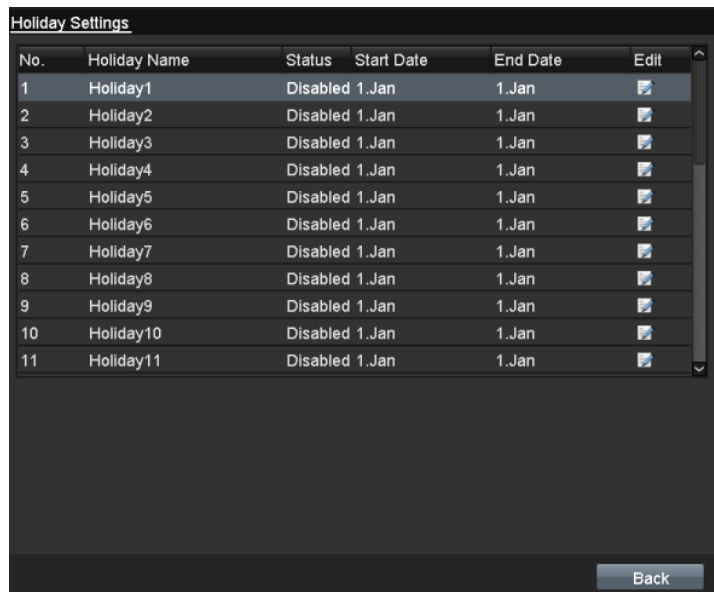

Figure 5. 22 Holiday Settings

2. Enable Edit Holiday schedule.
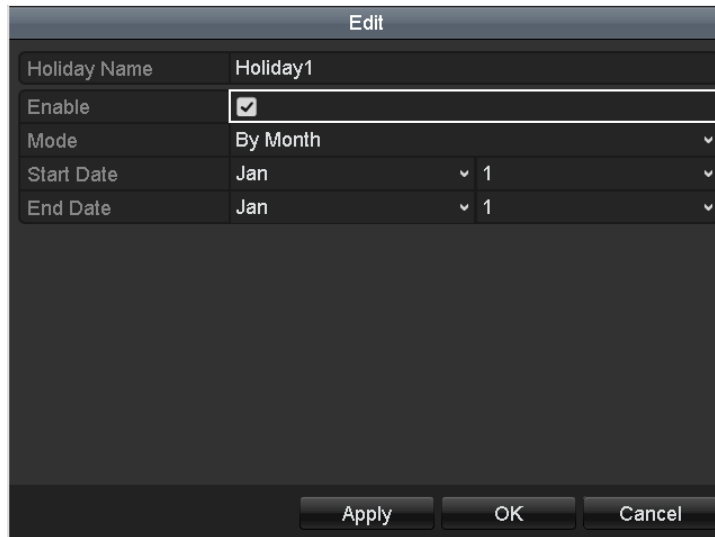
     1)   Click   to enter the Edit interface.

Figure 5. 23 Edit Holiday Settings

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

3) Select **Mode** from the dropdown list.

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

4) Set the start and end date.

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

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

3. Enter Record/Capture Schedule settings interface to edit the holiday recording schedule. See *Chapter 5.2 Configuring Recording Schedule.*

5.8   Configuring Redundant Recording

Purpose:

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

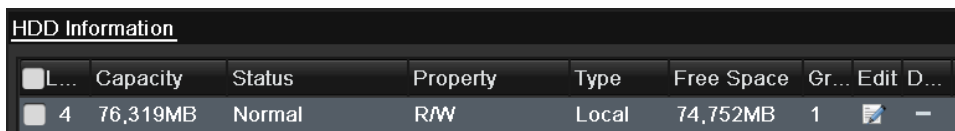*Steps:*

1. Enter HDD Information interface.

Menu> HDD

Figure 5. 24 HDD General

2. Select the **HDD** and click to enter the Local HDD Settings interface.
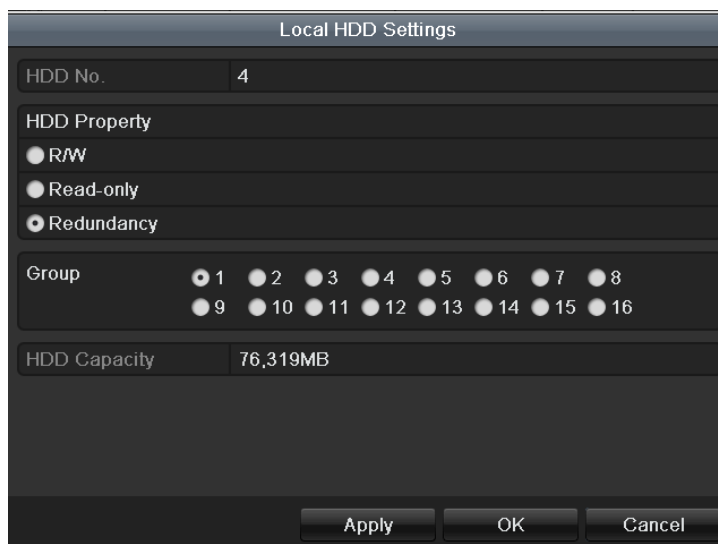
1) Set the HDD property to Redundancy.

Figure 5. 25 HDD General-Editing

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

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

You must set the Storage mode in the HDD advanced settings to Group before you set the HDD property to Redundant. For detailed information, please refer to *Chapter 11.4.1 Setting HDD Property*. There should be at least another HDD which is in Read/Write status.

3. Enter the Record setting interface.

Menu> Record> Parameters

1)   Select **Record** tab.
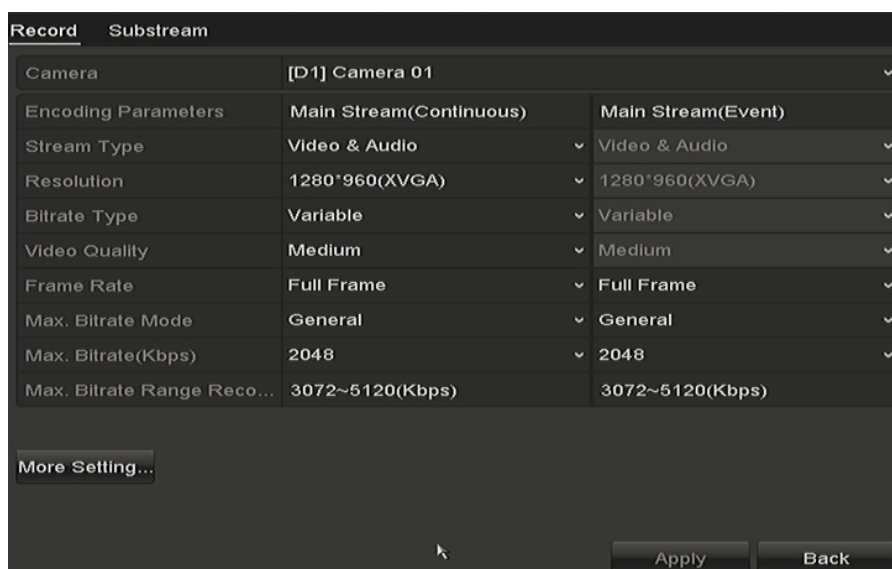

Figure 5. 26 Record Parameters

2)   Select Camera you want to configure in the drop-down list.

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

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

Repeat the above steps for configuring other channels.

5.9   Configuring HDD Group for Recording

Purpose:

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

Steps:

1. Enter HDD setting interface.

   Menu>HDD

Figure 5. 27 HDD General

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

Figure 5. 28 Storage Mode

Check whether the storage mode of the HDD is Group. If not, set it to Group. For detailed information, please refer to *Chapter 11.4 Managing HDD Group.*

3. Select **General** in the left side menu

4. Click [icon] to enter editing interface.

5. Configuring 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 back to the upper level menu.

      Repeat the above steps to configure more HDD groups.

6. Choose the Channels 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 dropdown list of Record **on HDD Group**

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

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

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

5.10 Files Protection

Purpose:

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

5.10.1 Locking the Recording Files

Lock File when Playback

Steps:

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 5. 29 Normal Playback

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

   In the 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.
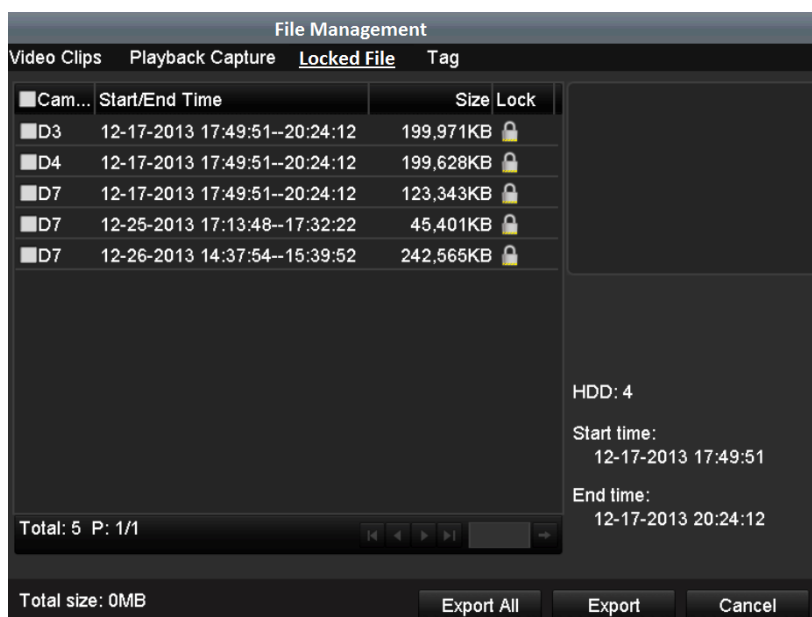
Figure 5. 30 Locked File Management

In the File Management interface, you can also click [icon] to change it to [icon] to unlock the file and the file is not protected.

● **Lock File when Export**

Steps:

1. Enter Export setting interface.

   Menu> Export

Figure 5. 31 Export

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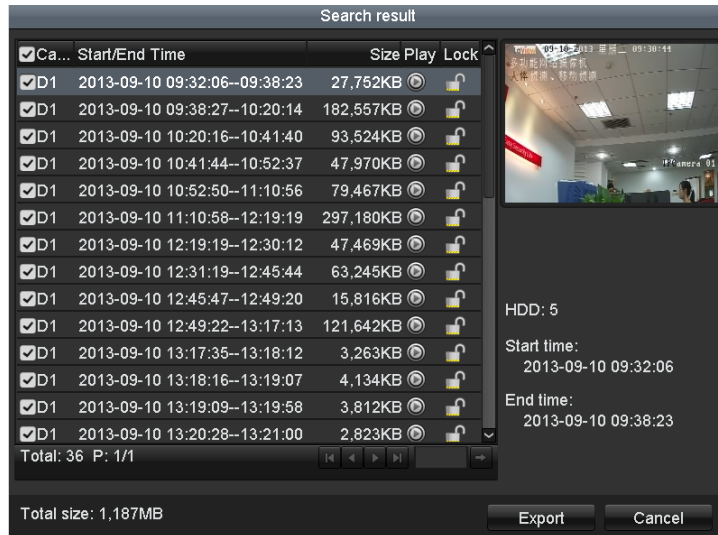4. Click **Search** to show the results.

Figure 5. 32 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.

The record files of which the recording is still not completed cannot be locked.

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

Figure 5. 33 Unlocking Attention

5.10.2 Setting HDD Property to Read-only

Steps:

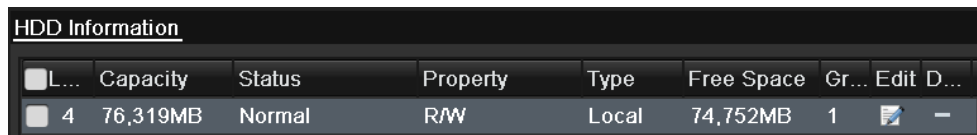**1.** Enter HDD setting interface.

Menu> HDD

Figure 5. 34 HDD General

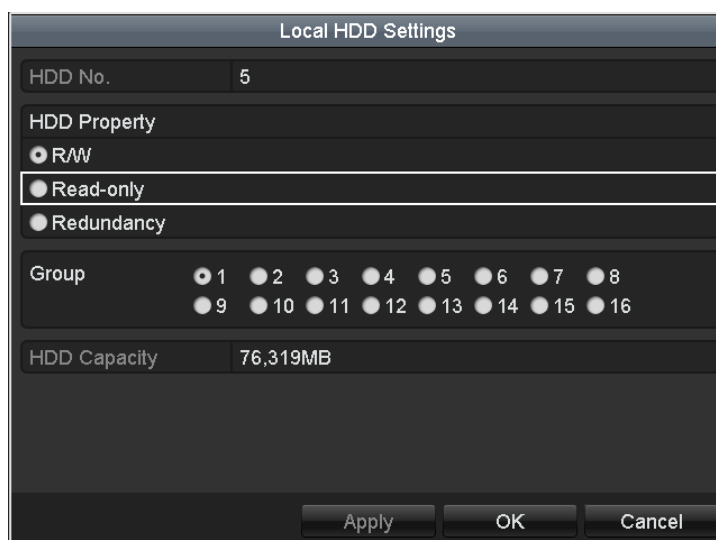**2.** Click 📝 to edit the HDD you want to protect.

Figure 5. 35 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 back to the upper level menu.

NOTE

- You cannot save any files in a Read-only HDD. If you want to save files in the HDD, change the property to R/W.
- If there is only one HDD and is set to Read-only, the NVR can't record any files. Only live view mode is available.
- If you set the HDD to Read-only when the NVR is saving files in it, then the file will be saved in next R/W HDD. If there is only one HDD, the recording will be stopped.

Chapter 6   Playback

6.1   Playing Back Record Files

6.1.1   Instant Playback

Purpose:

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

Instant playback by channel

Steps:

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

![NOTE]

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

Figure 6. 1 Instant Playback Interface

6.1.2   Playing Back by Normal Search

Playback by Channel

1. Enter the Playback interface.

   Mouse: right click a channel in live view mode and select Playback from the menu, as shown in Figure 6. 2.

Figure 6. 2 Right-click Menu under Live View

![NOTE]

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

Playback by Time

Purpose:

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

Steps:

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 6. 3 Playback Calendar

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

Otherwise it is displayed as

Playback Interface

You can use the toolbar in the bottom part of Playback interface to control playing progress, as shown in Figure 6. 4.
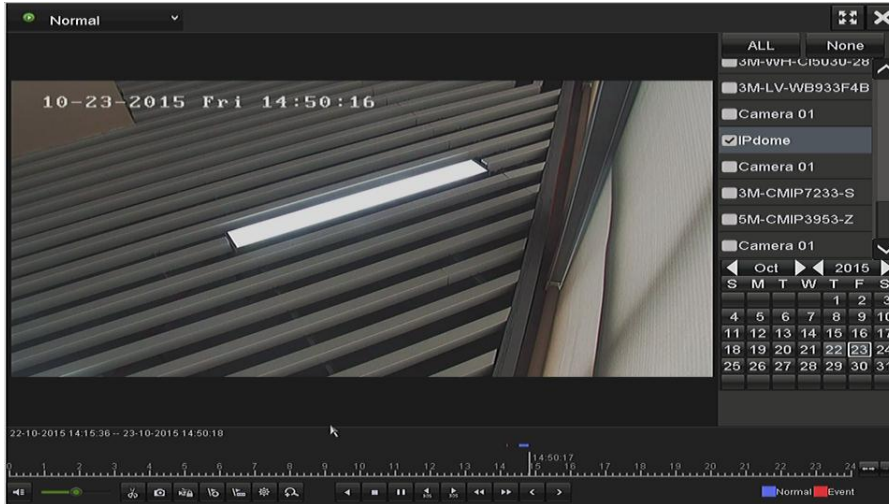
Figure 6. 4 Playback Interface

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

Figure 6. 5 Toolbar of Playback

● The ![09-15-2014 12:54:41 -- 12-09-2014 14:11:21] indicates the start/end time of the record.

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

Table 6. 1 Detailed Explanation of Playback Toolbar

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

6.1.3 Playing Back by Event Search

Purpose:

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

Steps:

1. Enter the Playback interface.

    Menu>Playback

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

3. Select **Alarm Input**, **Motion** or **VCA** as the event type.

    NOTE Here we take playback by VCA as the example.
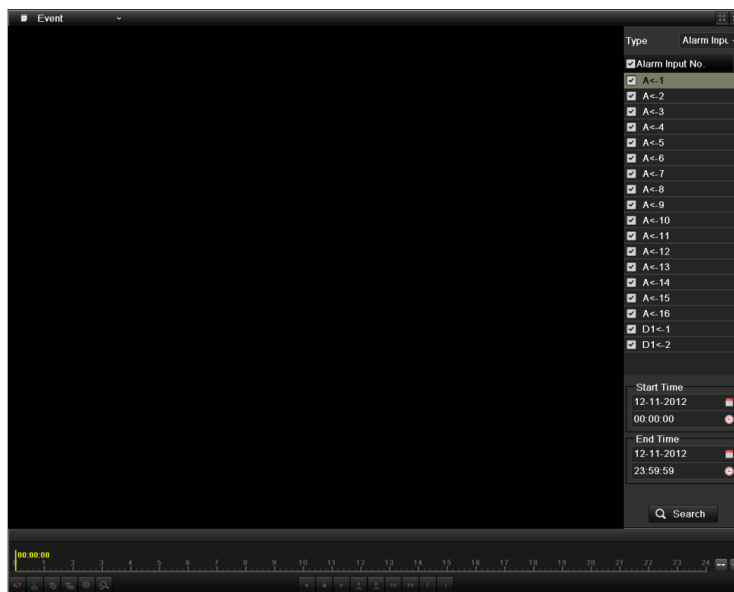

Figure 6. 6 Motion Search Interface

4. Select the minor type of VCA from the drop-down list.

    NOTE For configuring the VCA recording, please refer to *Chapter 5.4 Configuring VCA Event Recording*.

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. You may refer to the right-side bar for the result.

7. Click button to play back the file.

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

8. Playback interface.

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

Figure 6. 7 Interface of Playback by Event

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

6.1.4 Playing Back by Tag

Purpose:

Video tag allows you to record related information like 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.

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.
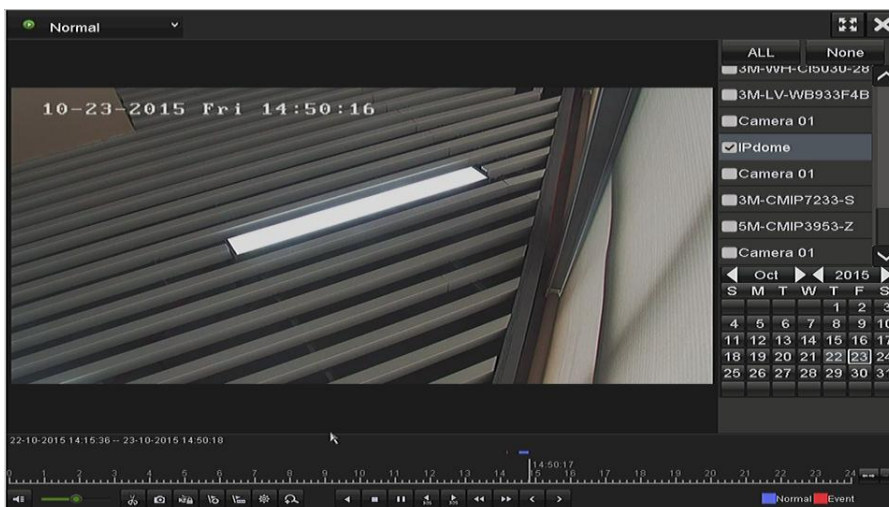

Figure 6. 8 Interface of Playback by Time

Click ![icon] button to add default tag.

Click ![icon] button to add customized tag and input tag name.

![NOTE]

Max. 64 tags can be added to a single video file.

3. Tag management.

Click ![icon] button to enter the File Management interface and click **Tag** to manage the tags. You can check, edit and delete tag(s).
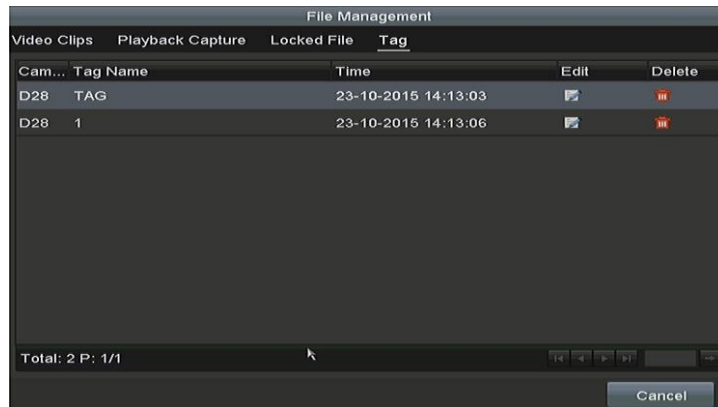
Figure 6. 9 Tag Management Interface

Playing back by Tag

Steps:

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 Search Result interface.

![NOTE] You can enter keyword in the textbox ![Keyword] to search the tag on your command.

3. Click ![icon] button to play back the selected tag file.

You can click the **Back** button to back to the search interface.

Figure 6. 10 Interface of Playback by Tag

Pre-play and post-play can be configured.

You can click or button to select the previous or next tag. Please refer to Table 6.1 for the description of buttons on the toolbar.

6.1.5 Playing back by Smart Playback

Purpose:

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

Before you start:

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

1. Log in the IP camera by the web browser, and enable the intrusion detection by checking the checkbox of it. You may enter the motion detection configuration interface by Configuration> Advanced Configuration> Events> Intrusion Detection.

Figure 6. 11 Setting Intrusion Detection on IP Camera

2. Configure the required parameters of intrusion detection, including area, arming schedule and linkage methods. Refer to the user manual of smart IP camera for detailed instructions.

Steps:

1. Enter Playback interface.

   Menu>Playback

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

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 6. 12 Smart Playback Interface

Table 6. 2 Detailed Explanation of Smart Playback Toolbar

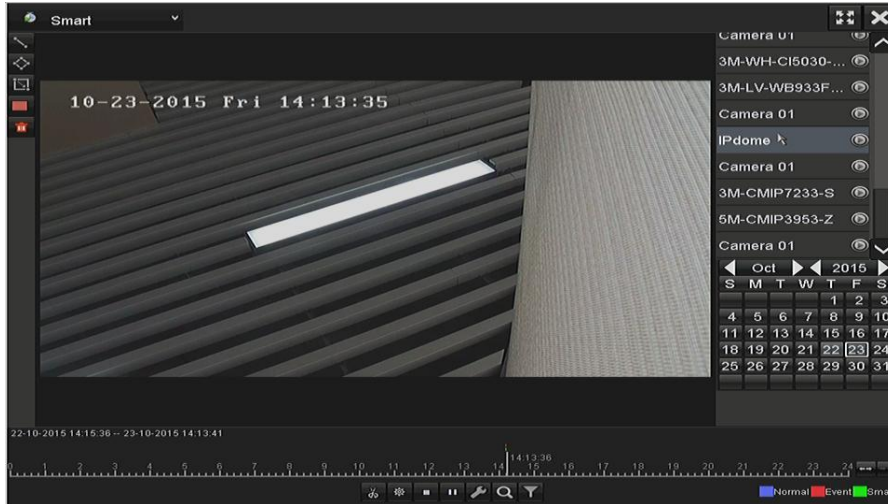| Button	Operation	Button	Operation	Button	Operation
	Draw line for the line crossing detection		Draw quadrilateral for the intrusion detection		Draw rectangle for the intrusion detection
	Set full screen for motion detection		Clear all		Start/Stop clipping
	File management for video clips		Stop playing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

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

 ● **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 4 points to set a quadrilateral region for intrusion detection. Only one region can be set.

 ● **Motion Detection**

Click the [ ] button and then click and draw the mouse to set the detection area manually. You can also click the [ ] button to set the full screen as the detection area.

6. You can click [ ] to configure the smart settings.
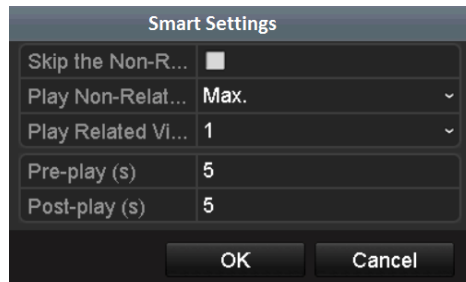
Figure 6. 13 Smart Settings

Skip the Non-Related Video: The non-related video will not be played if this function is enabled.

Play Non-Related Video at: Set the speed to play the non-related video. Max./8/4/1 are selectable.

Play Related Video at: Set the speed to play the related video. Max./8/4/1 are selectable.

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

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

8. (Optional) You can click to filter the searched video files by setting the target characters, including the gender and age of the human and whether he/she wears glasses.

Figure 6. 14 Set Result Filter

6.1.6 Playing Back by System Logs

Purpose:

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

Steps:

1. Enter Log Information interface.

   Menu>Maintenance>Log Information

2. Click **Log Search** tab to enter Playback by System Logs.

   Set search time and type and click **Search** button.
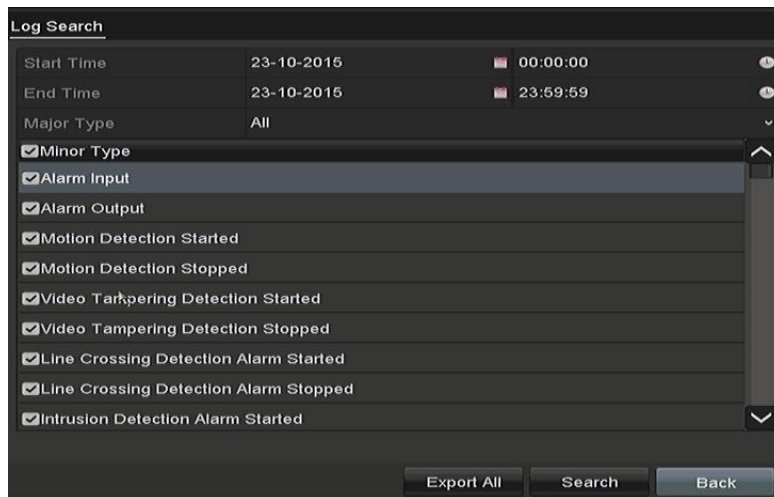
Figure 6. 15 System Log Search Interface

3. Choose a log with record file and click button to enter Playback interface.
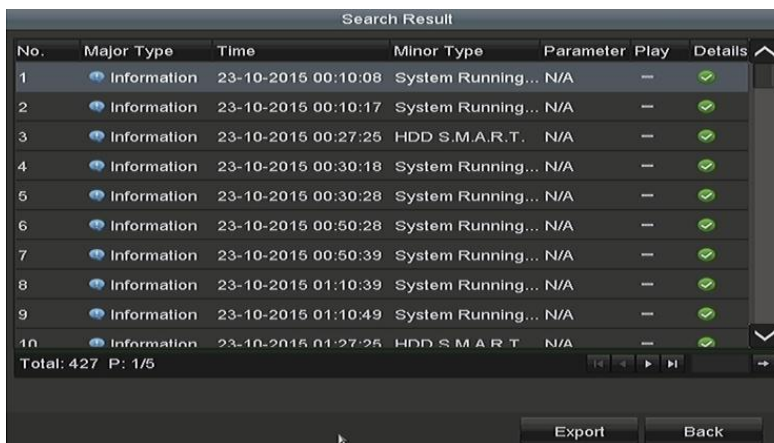
Figure 6. 16 Result of System Log Search

4. Playback interface.

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

Figure 6. 17 Interface of Playback by Log

6.1.7 Playing Back External File

Purpose:

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

Steps:

1. Enter Tag Search interface.

   Menu>Playback

2. Select the **External File** in the drop-down list on the top-left side.

   The files are listed in the right-side list.

   You can click the [⟳ Refresh] button to refresh the file list.

3. Select and click the [▶] button to play back it. And you can adjust the playback speed by clicking [▶▶] and
   [◀◀].

Figure 6. 18 Interface of External File Playback

6.1.8 Playing Back by Sub-periods

Purpose:

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

Steps:

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 dropdown list. Up to 16 screens are configurable.

User Manual of Network Video Recorder
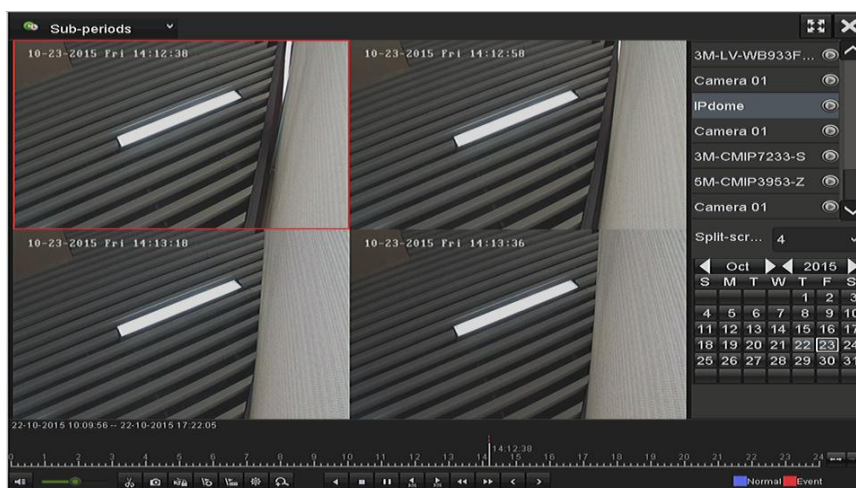
Figure 6. 19 Interface of Sub-periods Playback

NOTE

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

Chapter 7   Backup

7.1 Backing up Record Files

7.1.1 Quick Export

Purpose:

Export record files to backup device(s) quickly.

Steps:

1. Enter Video Export interface.

   Menu>Export>Normal

   Choose the channel(s) you want to back up and click **Quick Export** button.

   ![NOTE]The time duration of record files on a specified channel cannot exceed one day. Otherwise, the

   message box "Max. 24 hours are allowed for quick export." will pop up.

Normal								
☑ IP Camera	☑ D1	☑ D2	☑ D3	☑ D4	☑ D5	☑ D6	☑ D7	☑ D8
Start/End time of record	2013-09-03 16:59:05 -- 2013-09-10 15:07:11							
Record Type	All							˅
File Type	All							˅
Start Time	2013-09-10		🗓	00:00:00				🕒
End Time	2013-09-10		🗓	23:59:59				🕒
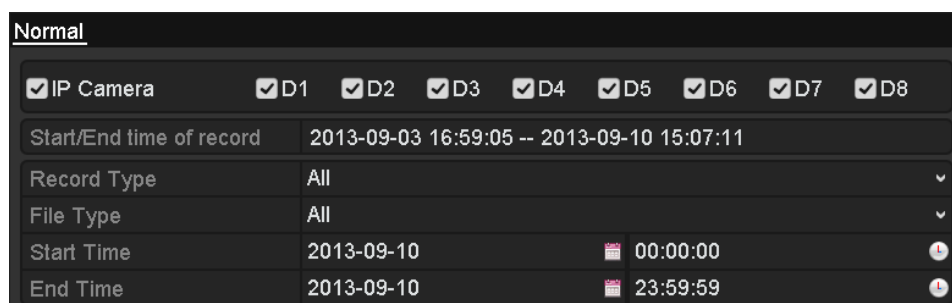
Figure 7. 1 Quick Export Interface

2. Select the format of the log files to be exported. Up to 9 formats are selectable.

3. Click the **Export** to start exporting.

![NOTE]

Here we use USB Flash Drive and please refer to the next section Normal Backup for more backup devices

supported by the NVR.
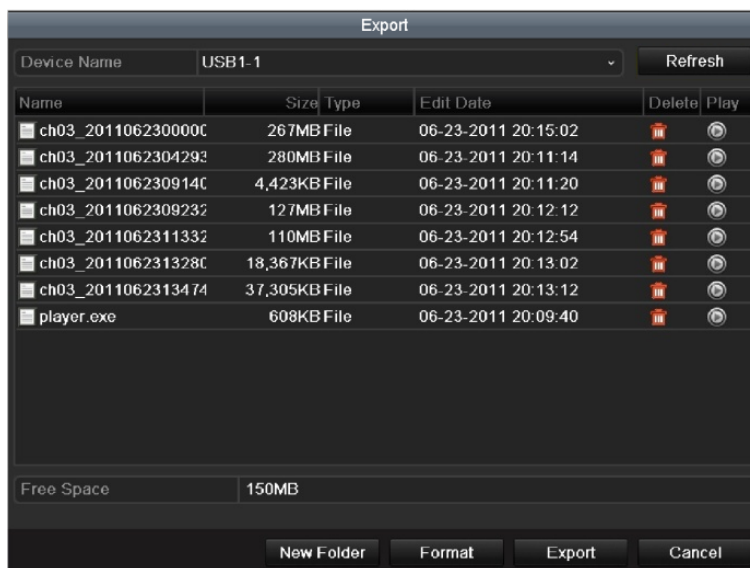
Figure 7. 2 Quick Export using USB1-1

Stay in the Exporting interface until all record files are exported.
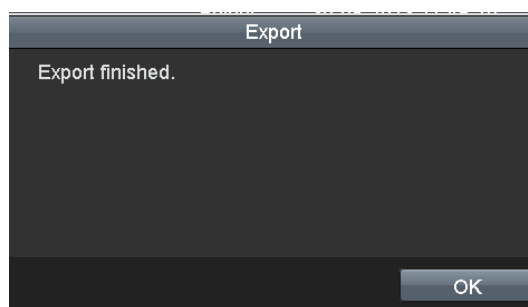
Figure 7. 3 Export Finished

4. Check backup result.

Choose the record file in Export interface and click button ![play] to check it.

![NOTE]

The Player player.exe will be exported automatically during record file export.
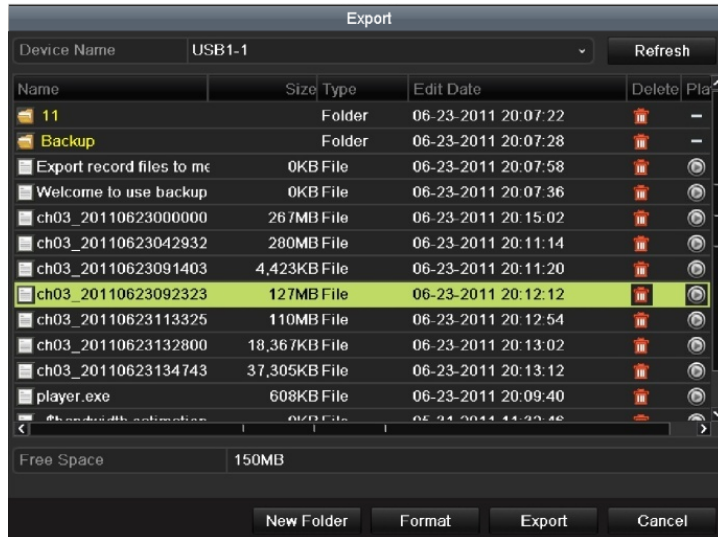
Figure 7. 4 Checkup of Quick Export Result Using USB1-1

7.1.2   Backing up by Normal Video Search

Purpose:

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

Backup using USB flash drives and USB HDDs

Steps:

1. Enter Export interface.

    Menu>Export>Normal

2. Select the cameras to search.

3. Set search condition and click **Search** button to enter the search result interface. The matched video files are displayed in Chart or List display mode.
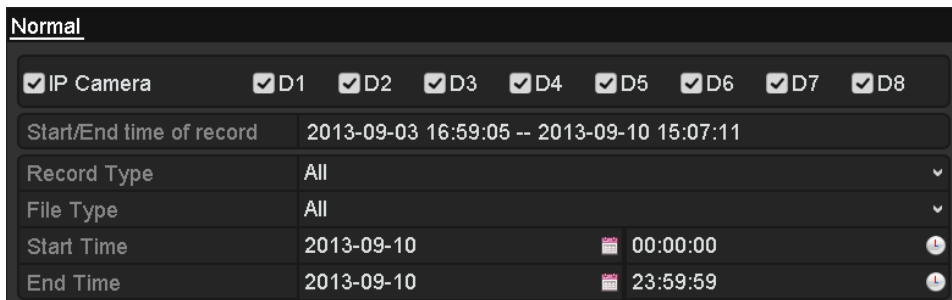
Figure 7. 5 Normal Video Search for Backup

4. Select video files or pictures from the Chart or List to export.

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

    Check the checkbox before the record files you want to back up.

    The size of the currently selected files is displayed in the lower-left corner of the window.
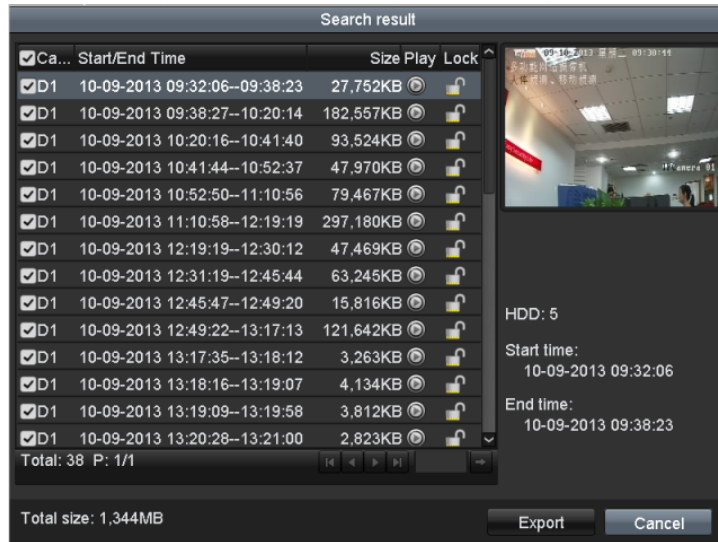
Figure 7. 6 Result of Normal Video Search for Backup

5. Export the video files or picture files.

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 Export interface.

NOTE

> If the inserted USB device is not recognized:

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

You can also format USB flash drives or USB HDDs via the device.
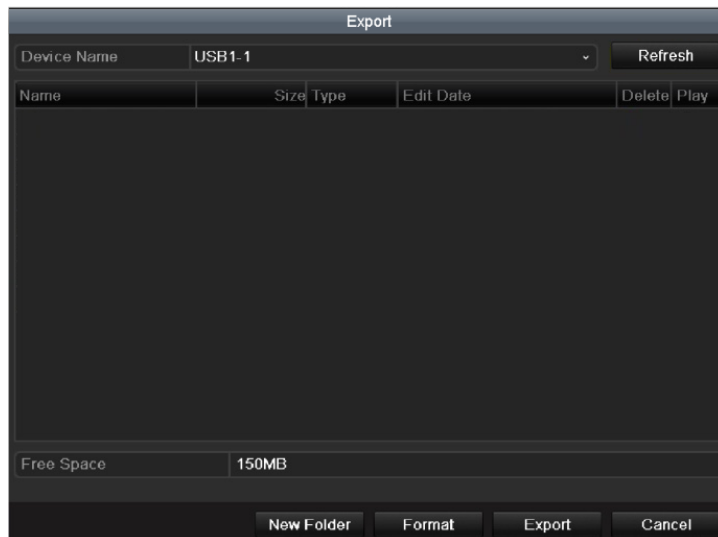
Figure 7. 7 Export by Normal Video Search using USB Flash Drive

Stay in the Exporting interface until all record files are exported with pop-up message box "Export finished".
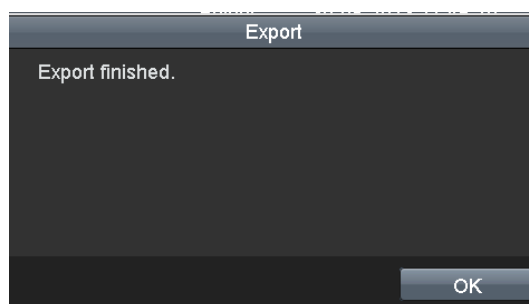
Figure 7. 8 Export Finished

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

7.1.3 Backing up by Event Search

Purpose:

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

Steps:

1. Enter Export interface.

   Menu>Export>Event

2. Select the cameras to search.

3. Select the event type to alarm input, motion or VCA.
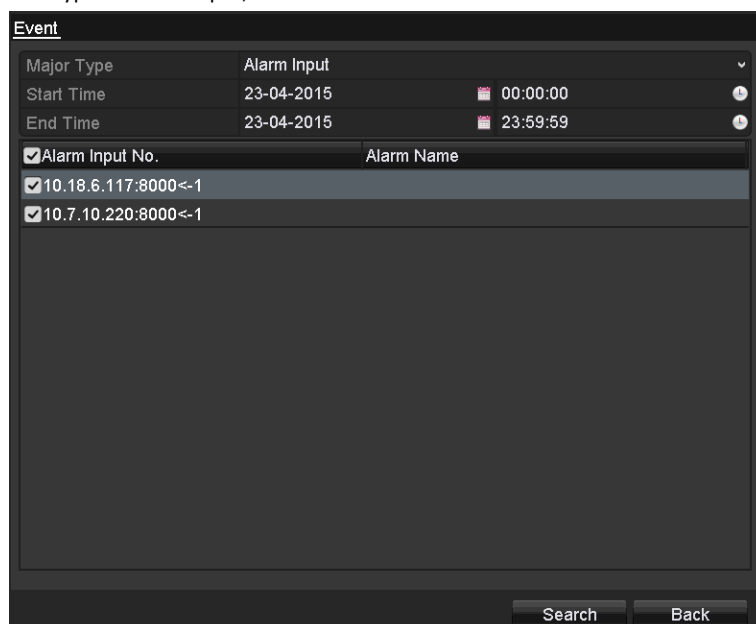
Figure 7. 9 Event Search for Backup

4. Set search condition and click **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.
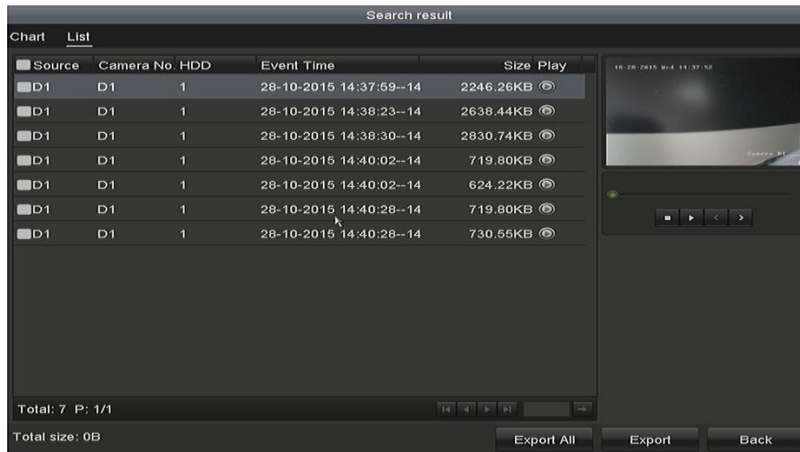
Figure 7. 10 Result of Event Search

6. Export the video files. Please refer to step5 of *Chapter 7.1.2 Backing up by Normal Video Search* for details.

7.1.4 Backing up Video Clips

Purpose:

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

Steps:

1. Enter Playback interface.

   Please refer to *Chapter 6.1 Playing Back Record Files.*

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

3. Click the ⬛ to enter the file management interface.
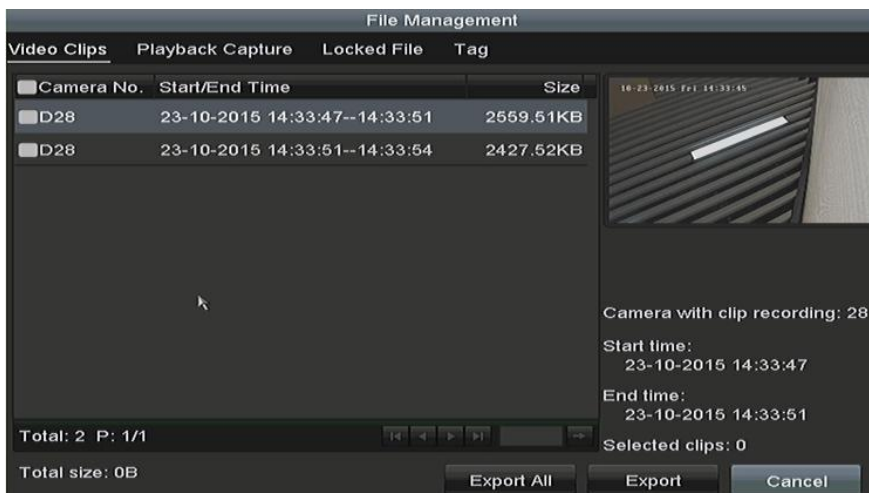
Figure 7. 11 Video Clips Export Interface

7. Export the video clips in playback. Please refer to step5 of *Chapter 7.1.2 Backing up by Normal Video Search* for details.

7.2 Managing Backup Devices

Management of USB flash drives and USB HDDs

Steps:

1. Enter the Export interface.
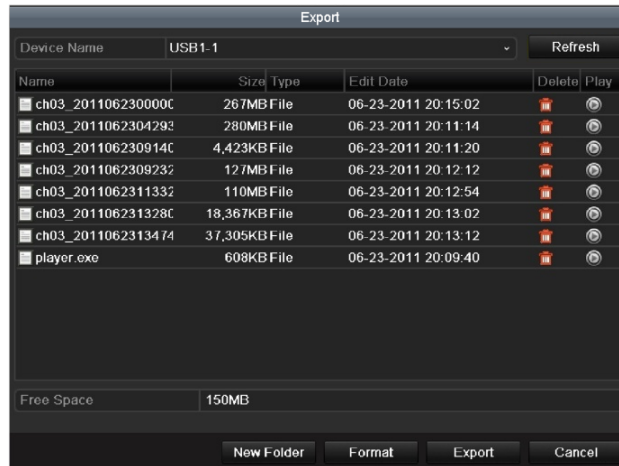
Figure 7. 12 Storage Device Management

2. Backup device management.

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

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

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

   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.

7.3 Hot Spare Device Backup

Purpose:

Several devices, including NVR and HDVR, can form an N+1 hot spare system. The system consists of several working devices and a hot spare device; when the working device fails, the hot spare device switches into operation, thus increasing the reliability of the system.

![NOTE]

Please contact dealer for details of models which support the hot spare function.

Before you start:

At least 2 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.
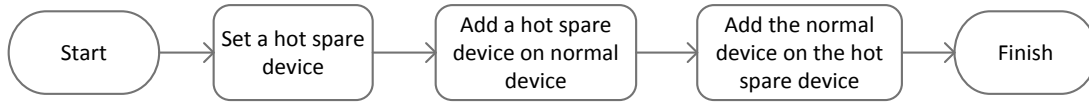
Figure 7. 13 Building Hot Spare System

7.3.1 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 defaults of the device after switching the working mode of the hot spare device to normal mode to ensure the normal operation afterwards.

Steps:
1. Enter the Hot Spare settings interface.
   Menu > Configuration > Hot Spare
2. Set the Work Mode as Hot Spare Mode, click the **Apply** button to confirm the settings.
3. Reboot the device to make the change take effect.
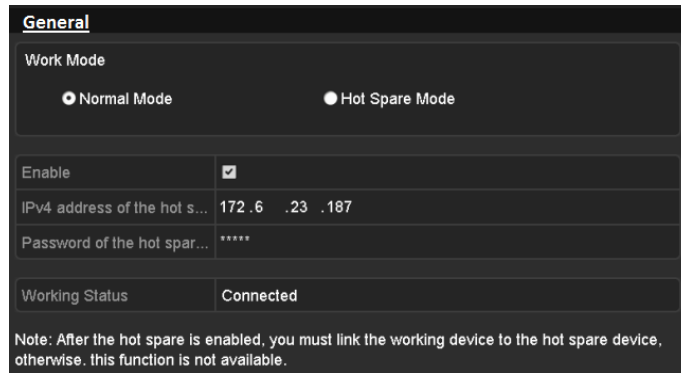
Figure 7. 14 Reboot Attention

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

7.3.1 Setting Working Device

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

Figure 7. 15 Setting Working Mode for Working device

5. Click the **Apply** button to save the settings.
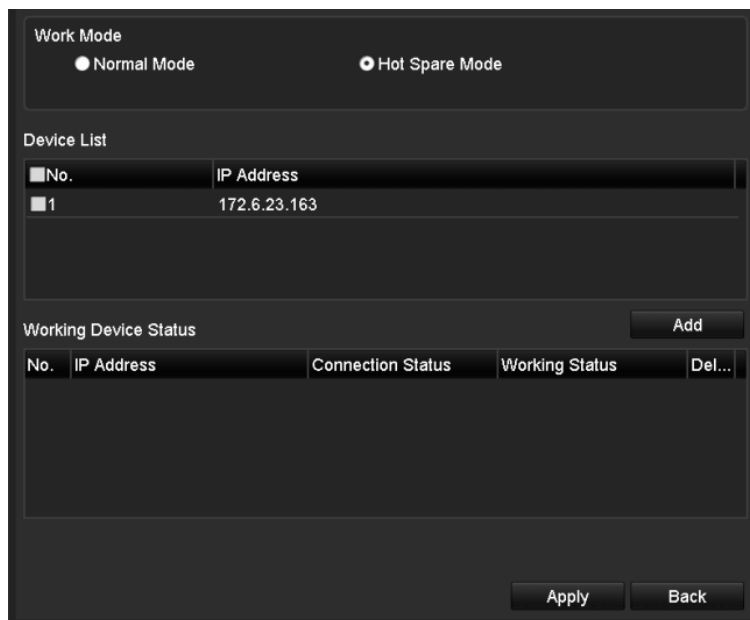
7.3.2 Managing Hot Spare System

Steps:

1. Enter the Hot Spare Settings interface of the hot spare device.

   The connected working device is displayed on the device list. Check the checkbox to select the working device from the list, and click the **Add** button to link the working device to the hot spare device.

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

Figure 7. 16 Add Working Device

2. You can view the working status of the hot spare device on the Working Device Status list.

   When the working device works properly, the working status of the hot spare device is displayed as *No record*.

Figure 7. 17 No Recording

When the working device gets offline, the hot spare device will record the video of the IP Camera connected to the working device for backup, and the working status of the hot spare device is displayed as *Backing up*.

NOTE

The record backing up can be functioned for 1 working device at a time.

Figure 7. 18 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 is displayed as *Synchronizing*.

NOTE

The record synchronization function can be enabled for 1 working device at a time.

Figure 7. 19 Synchronizing

Chapter 8   Alarm Settings

8.1   Setting Motion Detection Alarm

Steps:

1. Enter Motion Detection interface of Camera Management and choose a camera you want to set up motion detection.

    Menu> Camera> Motion

Figure 8. 1 Motion Detection Setup Interface

2. Set up detection area and sensitivity.

    Check the checkbox of **Enable Motion Detection**, use the mouse to draw detection area(s) and drag the sensitivity bar to set sensitivity.

      The full-screen motion detection is configured by default.

    Click button and set alarm response actions.

3. Click **Trigger Channel** tab and select one or more channels which will start to record or become full-screen monitoring when motion alarm is triggered, and click **Apply** to save the settings.
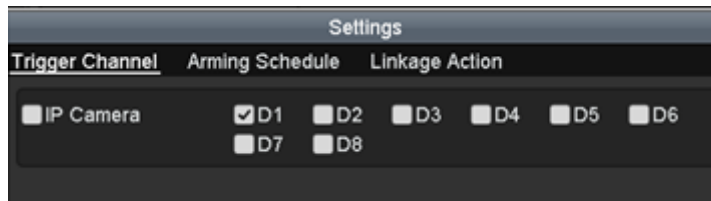
Figure 8. 2 Set Trigger Camera of Motion Detection

4. Set up arming schedule of the channel.

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

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

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

    Time periods shall not be repeated or overlapped.
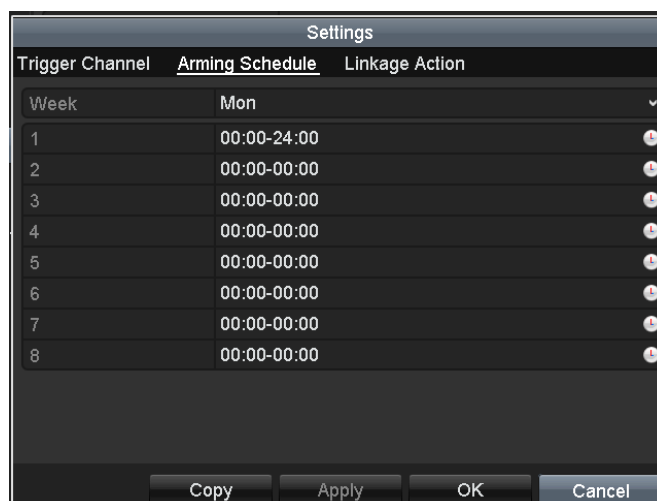
Figure 8. 3 Set Arming Schedule of Motion Detection

5. Click **Linkage Action** tab to set up alarm response actions of motion alarm (please refer to *Chapter Setting Alarm Response Actions*).

6. If you want to set motion detection for another channel, repeat the above steps or just click **Copy** in the Motion Detection interface to copy the above settings to it.

8.2   Setting Sensor Alarms

Purpose:

Set the handling action of an external sensor alarm.

Steps:

1. Enter Alarm Settings of System Configuration and select an alarm input.

   Menu> Configuration> Alarm

   Select Alarm Input tab to enter Alarm Input Settings interface.
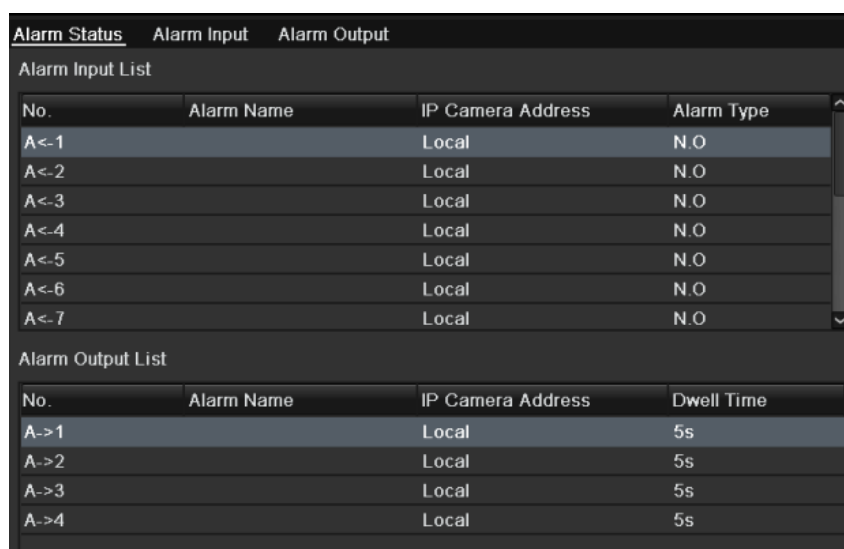
Figure 8. 4 Alarm Status Interface of System Configuration

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

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

Alarm Status	Alarm Input	Alarm Output
Alarm Input No.	A<-1	
Alarm Name		
Type	N.O	
Setting	☐	
Handling	⚙	
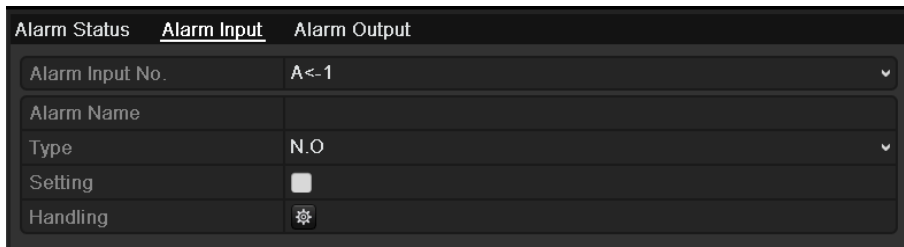
Figure 8. 5 Alarm Input Setup Interface

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

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

Settings			
Trigger Channel	Arming Schedule	Linkage Action	PTZ Linking
Week	Mon		
1	00:00-24:00		🕐
2	00:00-00:00		🕐
3	00:00-00:00		🕐
4	00:00-00:00		🕐
5	00:00-00:00		🕐
6	00:00-00:00		🕐
7	00:00-00:00		🕐
8	00:00-00:00		🕐
	Copy	Apply	OK	Cancel
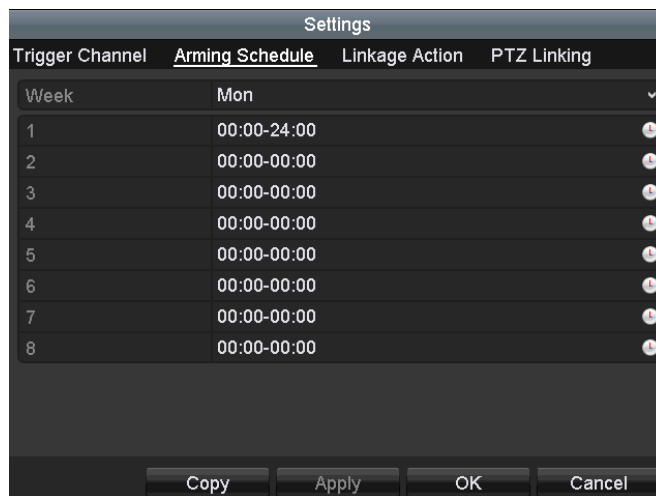
Figure 8. 6 Set Arming Schedule of Alarm Input

Choose one day of a week and Max. eight time periods can be set within each day, and click **Apply** to save the settings.

![NOTE]

Time periods shall not be repeated or overlapped.

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

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

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

![NOTE]

Please check whether the PTZ or speed dome supports PTZ linkage.

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

Figure 8. 7 Set PTZ Linking of Alarm Input

7. If you want to set handling action of another alarm input, repeat the above steps.

Or you can click the **Copy** button on the Alarm Input Setup interface and check the checkbox of alarm inputs to copy the settings to them.
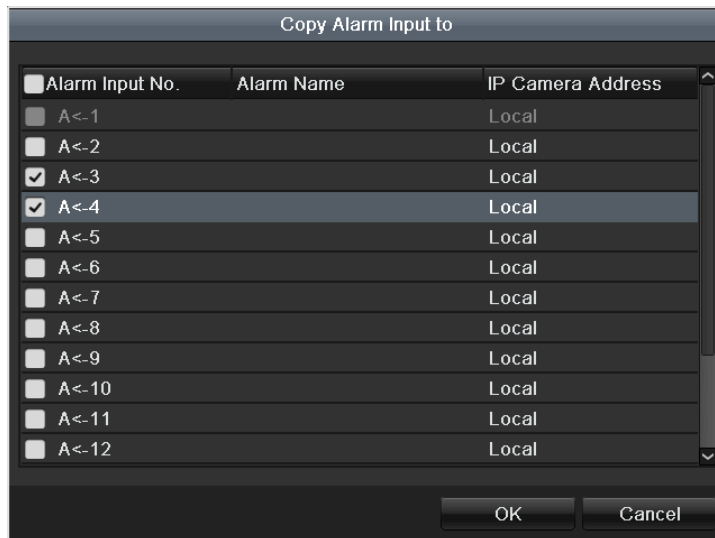
Figure 8. 8 Copy Settings of Alarm Input

8.3 Detecting Video Loss Alarm

Purpose:

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

Steps:

1. Enter Video Loss interface of Camera Management and select a channel you want to detect.

Menu> Camera> Video Loss
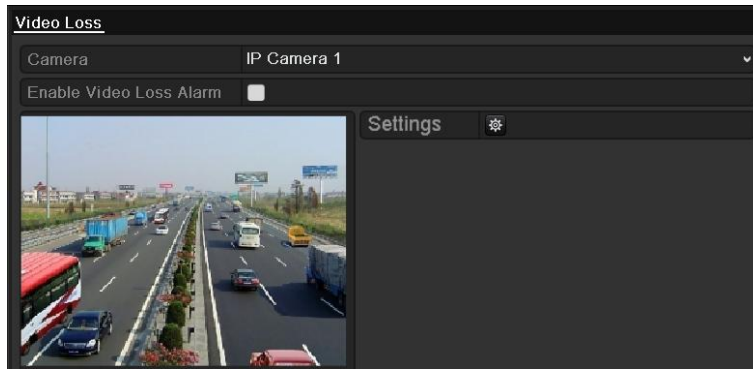
Figure 8. 9 Video Loss Setup Interface

2. Set up handling action of video loss.

Check the checkbox of "Enable Video Loss Alarm", and click ⚙ button to set up handling action of video loss.

3. Set up arming schedule of the handling actions.

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

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

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

NOTE Time periods shall not be repeated or overlapped.
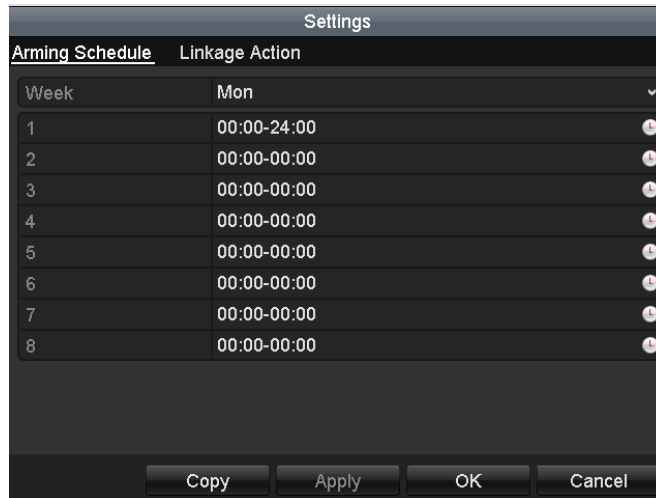
Figure 8. 10 Set Arming Schedule of Video Loss

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

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

8.4 Detecting Video Tampering Alarm

Purpose:

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

Steps:

1. Enter Video Tampering interface of Camera Management and select a channel you want to detect video tampering.

   Menu> Camera> Video Tampering

Figure 8. 11 Video Tampering Setup Interface

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

   Check the checkbox of **Enable Video Tampering Detection**.

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

   Click ⚙ button to set up handling action of video tampering.

3. Set arming schedule and alarm response actions of the channel.

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

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

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

   NOTE Time periods shall not be repeated or overlapped.
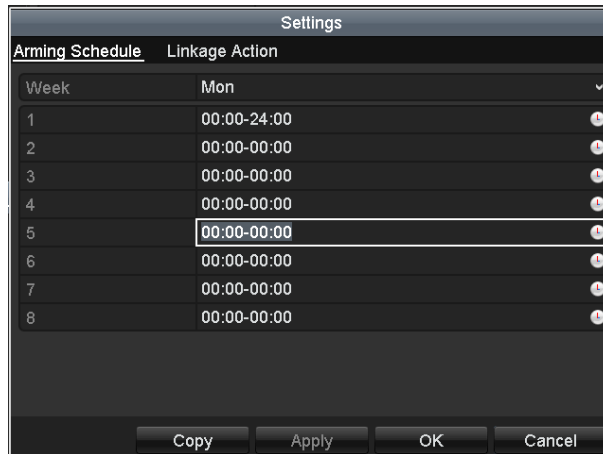
Figure 8. 12 Set Arming Schedule of Video Tampering

4. Select **Linkage Action** tab to set up alarm response actions of video tampering alarm (please refer to
    Chapter Setting Alarm Response Actions).

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

8.5   Handling Exceptions Alarm

Purpose:

Exception settings refer to the handling action of various exceptions, e.g.

*   **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 Exception:** No space for saving recorded files.

*   **Hot Spare Exception:** Disconnected with the working device.

*   **Array Exception:** Abnormal virtual disks exist under array.

Array Exception is only supported after the RAID is enabled, refer to chapter 10.1.1 for details.

Steps:

Enter Exception interface of System Configuration and handle various exceptions.

Menu> Configuration> Exceptions

Please refer to *Chapter Setting Alarm Response Actions* for detailed alarm response actions.

Figure 8. 13 Exceptions Setup Interface

8.6   Setting Alarm Response Actions

Purpose:

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

Event Hint Display

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

Steps:

1. Enter the Exception settings interface.

    Menu > Configuration > Exceptions

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

Figure 8. 14 Event Hint Settings Interface

3. Click the ⚙ to set the type of event to be displayed on the image.
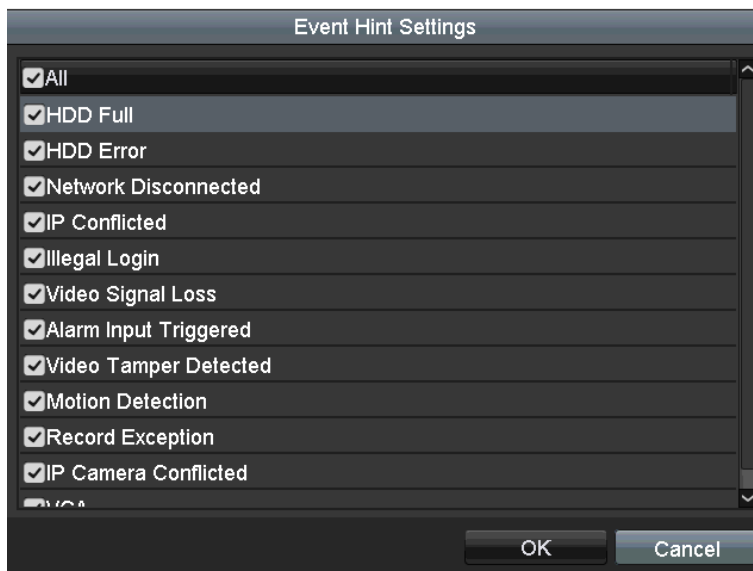
Figure 8. 15 Event Hint Settings Interface

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

Full Screen Monitoring

When an alarm is triggered, the local monitor (VGA, HDMI™ or LCD output) 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 at an interval

of 10 seconds (default dwell time). A different dwell time can be set by going to Menu >Configuration>Live View > Full Screen Monitoring Dwell Time.

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

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

Audible Warning

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

Notify Surveillance Center

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

NOTE The alarm signal will be transmitted automatically at detection mode when remote alarm host is configured. Please refer to *Chapter Configuring* for details of alarm host configuration.

Email Linkage

Send an email with alarm information to a user or users when an alarm is detected.

Please refer to *Chapter* 11.2.7 for details of Email configuration.

Trigger Alarm Output

Trigger an alarm output when an alarm is triggered.

1. Enter Alarm Output interface.

    Menu> Configuration> Alarm> Alarm Output

    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 dropdown list of Dwell Time, you can clear it only by going to Menu> Manual> Alarm.

Alarm Status	Alarm Input	Alarm Output	
Alarm Output No.		A->1	˅
Alarm Name			
Dwell Time		5s	˅
Handling		⚙	
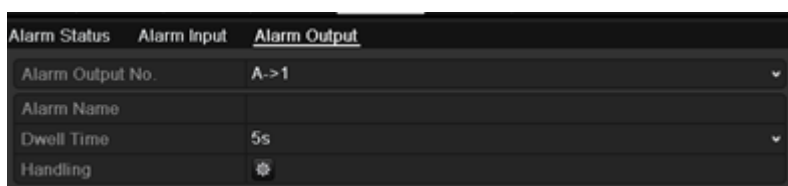
Figure 8. 16 Alarm Output Setup Interface

2. Set up arming schedule of the alarm output.

    Choose one day of a week and up to 8 time periods can be set within each day.

    NOTE Time periods shall not be repeated or overlapped.
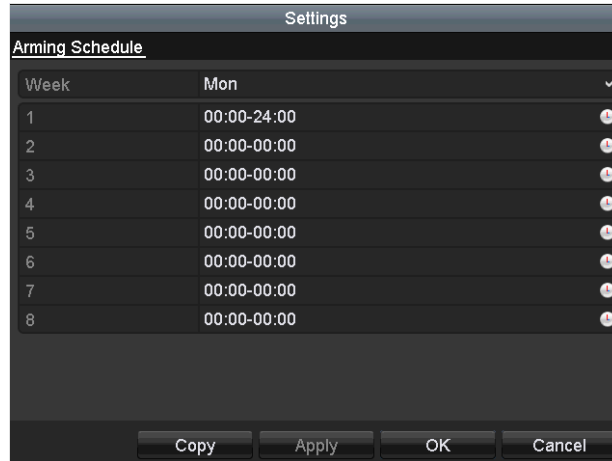
Figure 8. 17 Set Arming Schedule of Alarm Output

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

    Click the **OK** button to complete the video tampering settings of the alarm output No.
4. You can also copy the above settings to another channel.
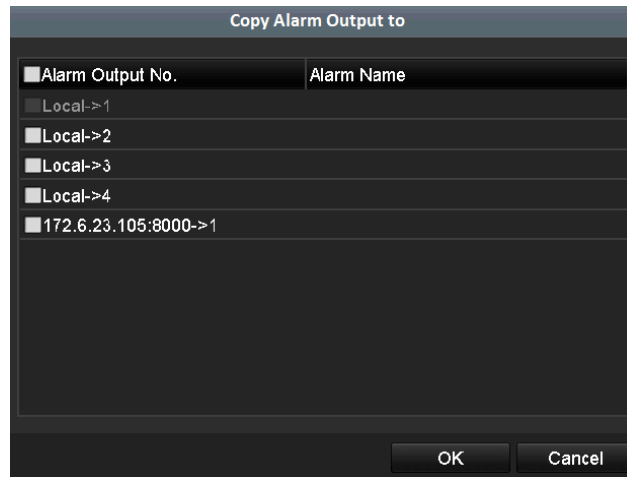
Figure 8. 18 Copy Settings of Alarm Output

8.7 Triggering or Clearing Alarm Output Manually

Purpose:

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

Steps:
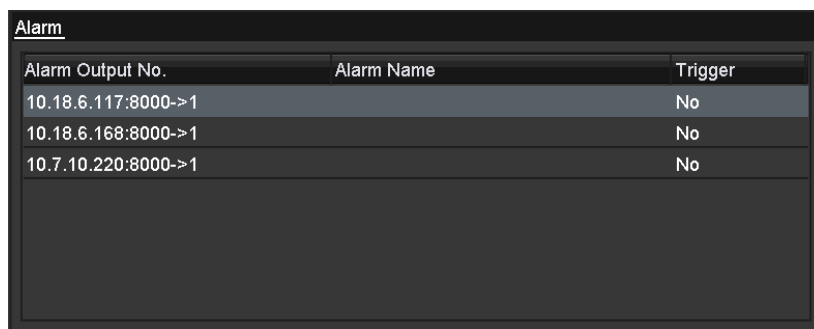
Select the alarm output you want to trigger or clear and make related operations.

Menu> Manual> Alarm

Click **Trigger/Clear** button if you want to trigger or clear an alarm output.

Click **Trigger All** button if you want to trigger all alarm outputs.

Click **Clear All** button if you want to clear all alarm output.

Figure 8. 19 Clear or Trigger Alarm Output Manually

Chapter 9   VCA Alarm

- For the /I models, the device supports the face detection and contiguration. For other models, the face detection must be supported by the connected IP camera.
- For all models, all other VCA detection functions must be supported by the connected IP camera

9.1 Line Crossing Detection

Purpose:

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

Steps:

1. Enter the VCA settings interface.
   Menu> Camera> VCA
2. Select the camera to configure the VCA.
   You can click the checkbox of **Save VCA Picture** to save the captured pictures of VCA detection.
3. Select the VCA detection type to **Line Crossing Detection**.
4. Check the **Enable** checkbox to enable this function.
5. Click to configure the trigger channel, arming schedule and linkage actions for the line crossing detection alarm.
6. 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: Only the arrow on the B side shows; when an object going across the configured line with both

      direction can be detected and alarms are triggered.

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

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

   2) Click-and-drag the slider to set the detection sensitivity.

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

   triggered.

   3) Click-**OK** to save the rule settings and back to the line crossing detection settings interface.
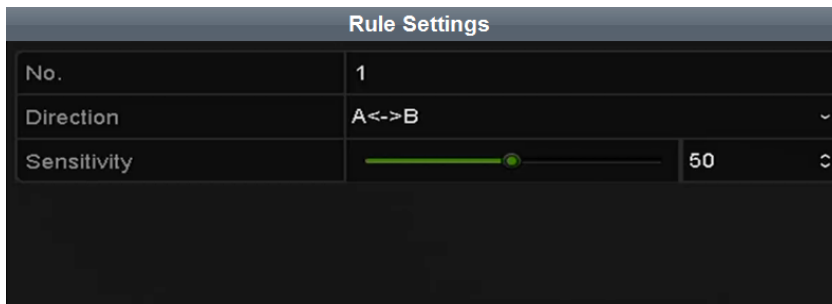
Figure 9. 1 Set Line Crossing Detection Rules

7. Click ![pencil icon] and set two points in the preview window to draw a virtual line.

    You can use the ![clear icon] to clear the existing virtual line and re-draw it.

    ![NOTE icon]

    Up to 4 rules can be configured.

Figure 9. 2 Draw Line for Line Crossing Detection

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

9.2 Intrusion Detection

Purpose:

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

Steps:

1. Enter the VCA settings interface.

    Menu> Camera> VCA

2. Select the camera to configure the VCA.

    You can click the checkbox of **Save VCA Picture** to save the captured pictures of VCA detection.

3. Select the VCA detection type to **Intrusion Detection**.

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

5. Click ![gear icon] to configure the trigger channel, arming schedule and linkage actions for the line crossing detection alarm.

6. Click the **Rule Settings** button to set the intrusion detection rules. Set the following parameters.

1) **Threshold:** Range [1s-10s], the threshold for the time of the object loitering in the region. When the duration of the object in the defined detection area is longer than the set time, the alarm will be triggered.

2) Click-and-drag the slider to set the detection sensitivity.

   Sensitivity: Range [1-100]. The value of the sensitivity defines the size of the object which can trigger the alarm. The higher the value is, the more easily the detection alarm can be triggered.

3) **Percentage:** Range [1-100]. Percentage defines the ratio of the in-region part of the object which can trigger the alarm. For example, if the percentage is set as 50%, when the object enters the region and occupies half of the whole region, the alarm is triggered.

Rule Settings		
No.	1	
Time Threshold (s)	●━━━	5 ⌄
Sensitivity	●━━	50 ⌄
Percentage	●━	0 ⌄
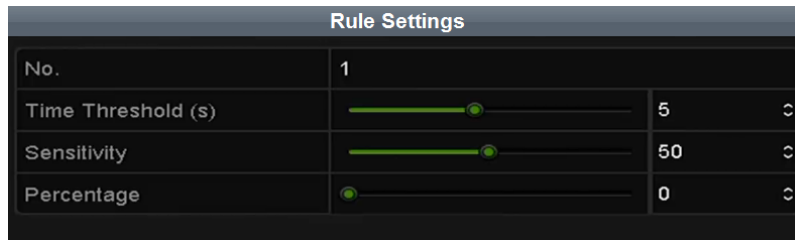
Figure 9. 3 Set Intrusion Crossing Detection Rules

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

7. 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.

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

NOTE

Up to 4 rules can be configured.
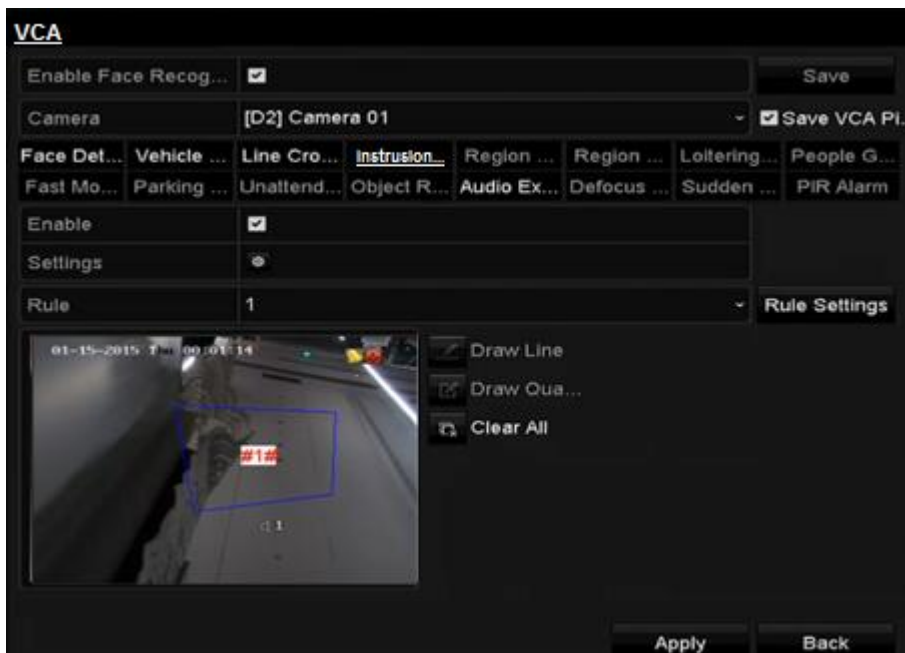
Figure 9. 4 Draw Area for Intrusion Detection

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

9.3 People Gathering Detection

Purpose:

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

NOTE

● The **Percentag**e in the Rule Settings defines the gathering density of the people in the region. Usually, when the percentage is small, the alarm can be triggered when small number of people gathered in the defined detection region.
● Up to 4 rules can be configured.

Chapter 10   VCA Search

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

10.1 People Counting

Purpose:

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

Steps:

1. Enter the **People Counting** interface.

   Menu>VCA Search> People Counting

2. Select the camera for the people counting.

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

4. Set the statistics time.

5. Click the **Counting** button to start people counting statistics.
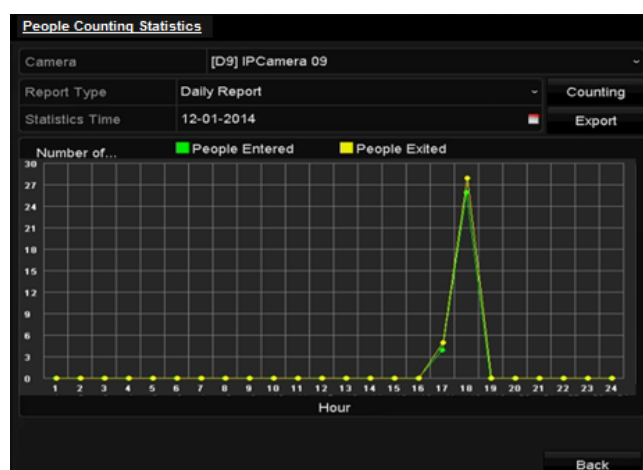
Figure 10. 1 People Counting Interface

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

Chapter 11 Network Settings

11.1 Configuring General Settings

Purpose:

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

Steps:

1. Enter the Network Settings interface.

    Menu >Configuration>Network

2. Select the **General** tab.

Figure 11. 1 Network Settings Interface

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

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

    The valid value range of MTU is 500 ~ 9676.

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

Working Mode

There are two 10M/100M/1000M NIC cards provided by the 9600NI-E series device, and it allows the device to work in the Multi-address, Load Balance and Net-fault Tolerance modes.

Multi-address Mode: The parameters of the two NIC cards can be configured independently. You can select LAN1~LAN4 in the NIC type field for parameter settings.

You can select one NIC card as default route. And then the system is connecting with the extranet the data will be forwarded through the default route.

Net-fault Tolerance Mode: The two NIC cards use the same IP address, and you can select the Main NIC to LAN1~LAN4. By this way, in case of one NIC card failure, the device will automatically enable another standby NIC card so as to ensure the normal running of the whole system.

11.2 Configuring Advanced Settings

11.2.1 Configuring PPPoE Settings

Purpose:

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

Steps:

1. Enter the **Network Settings** interface.

    Menu >Configuration> Network

2. Select the **PPPoE** tab to enter the PPPoE Settings interface, as shown in Figure 11. 2.

Enable PPPOE	☐
User Name	
Password	
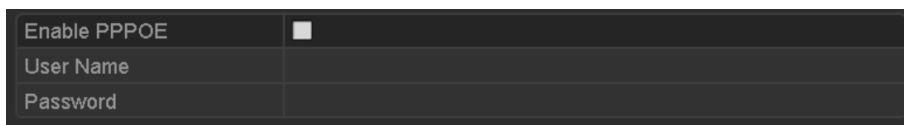
Figure 11. 2 PPPoE Settings Interface

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

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

NOTE

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

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

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

You can go to Menu >Maintenance>System Info >Network interface to view the status of PPPoE connection. Please refer to *Chapter Viewing System Information* for PPPoE status.

11.2.2 Configuring DDNS

Purpose:

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

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

Steps:

1. Enter the Network Settings interface.

    Menu >Configuration> Network

2. Select the **DDNS** tab to enter the DDNS Settings interface, as shown in Figure 11. 3.

Figure 11. 3 DDNS Settings Interface

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

4. Select **DDNS Type**. Five different DDNS types are selectable: LTS,IPServer, DynDNS, PeanutHull, NO-IP and HiDDNS.

- **LTS:**

     Enter the **Server Address** and **Device Domain Name** for LTS.

     1) Enter the **Server Address** of the LTS server, which is ns1.dvrlist.com by default.

     2) Enter the **Device Domain Name.** You can use the alias you registered in the LTS server or define a new device domain name. If a new alias of the device domain name is defined in the NVR, it will replace the old one registered on the server. You can register the alias of the device domain name in the LTS server first and then enter the alias to the **Device Domain Name** in the NVR; you can also enter the domain name directly on the NVR to create a new one.

Figure 11. 4 LTS Settings Interface

- **IPServer:** Enter **Server Address** for IPServer.

Figure 11. 5 IPServer Settings Interface

- **DynDNS:**
     1) Enter **Server Address** for DynDNS (i.e. members.dyndns.org).
     2) In the NVR Domain Name text field, enter the domain obtained from the DynDNS website.
     3) Enter the **User Name** and **Password** registered in the DynDNS website.

Figure 11. 6 DynDNS Settings Interface

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

Figure 11. 7 PeanutHull Settings Interface

- **NO-IP:**

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

  1) Enter **Server Address** for NO-IP.

  2) In the NVR Domain Name text field, enter the domain obtained from the NO-IP website (www.no-ip.com).

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

Figure 11. 8 NO-IP Settings Interface

- **HiDDNS:**

  1) The **Server Address** of the HiDDNS server appears by default: www.hiddns.com.

  2) Enter the **Device Domain Name.** You can use the alias you registered in the HiDDNS server or define a new device domain name. If a new alias of the device domain name is defined in the NVR, it will replace the old one registered on the server. You can register the alias of the device domain name in the HiDDNS server first and then enter the alias to the **Device Domain Name** in the NVR; you can also enter the domain name directly on the NVR to create a new one.

Figure 11. 9 HiDDNS Settings Interface

Register the device on the HiDDNS server.

1) Go to the HiDDNS website: www.hiddns.com.

2) Click <u>Register new user</u> to register an account if you do not have one and use the account to log in.
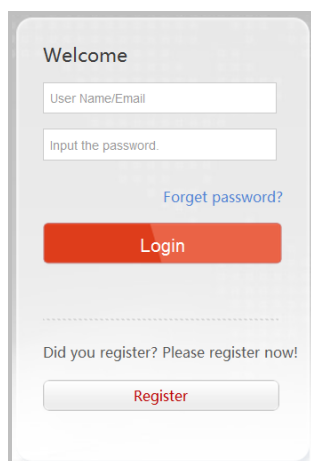
Figure 11. 10 Register an Account

3) In the Device Management interface, click `Register` to register the device.

Figure 11. 11 Register the Device

The device name can only contain the lower-case English letter, numeric and '-'; and it must start with the lower-case English letter and cannot end with '-'.

Access the Device via Web Browser or Client Software

After having successfully registered the device on the HiDDNS server, you can access your device via web browser or Client Software with the **Device Domain Name** (**Device Name**).

● **OPTION 1: Access the Device via Web Browser**

Open a web browser, and enter *http://www.hiddns.com/alias* in the address bar. Alias refers to the **Device Domain Name** on the device or the **Device Name** on the HiDDNS server**.**

Example: http://www.hiddns.com/nvr

If you mapped the HTTP port on your router and changed it to port No. except 80, you have to enter *http://www.hiddns.com/alias:HTTP port* in the address bar to access the device. You can refer to *Chapter 9.2.11* for the mapped HTTP port No.

● **OPTION 2: Access the devices via NVMS7000**

For NVMS7000, in the Add Device window, select ⊙ HiDDNS and then edit the device information.

Nickname: Edit a name for the device as you want.

Server Address: www.hiddns.com

Device Domain Name: It refers to the **Device Domain Name** on the device or the **Device Name** on the HiDDNS server you created**.**

User Name: Enter the user name of the device. By default it is admin.

Password: Enter the password of the device. By default it is 12345.

Figure 11. 12 Access Device via NVMS7000

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

11.2.3 Configuring NTP Server

Purpose:

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

Steps:

1. Enter the Network Settings interface.

   Menu >Configuration> Network

2. Select the **NTP** tab to enter the NTP Settings interface, as shown in Figure 11. 13.

Figure 11. 13 NTP Settings Interface

3. Check the **Enable NTP** checkbox to enable this feature.

4. Configure the following NTP settings:

   - **Interval:** Time interval between the two synchronizing actions with NTP server. The unit is minute.

   - **NTP Server:** IP address of NTP server.

   - **NTP Port:** Port of NTP server.

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

The time synchronization interval can be set from1 to 10080min, and the default value is 60min. 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 setup in a more customized network, NTP software can be used to establish a NTP server used for time synchronization.

11.2.4 Configuring SNMP

Purpose:

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

Steps:

1. Enter the Network Settings interface.

    Menu >Configuration> Network

2. Select the **SNMP** tab to enter the SNMP Settings interface, as shown in Figure 11. 14.

Enable SNMP	☑
SNMP Version	V2
SNMP Port	161
Read Community	public
Write Community	private
Trap Address	
Trap Port	162

Figure 11. 14 SNMP Settings Interface

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

4. Configure the following SNMP settings:

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

    - **Trap Port:** Port of SNMP host.

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

NOTE

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

11.2.5 Configuring More Settings

Purpose:

With a remote alarm host configured, the NVR will send the alarm event or exception message to the host when an alarm is triggered. The remote alarm host must have the Network Video Surveillance software installed.

Steps:

1. Enter the Network Settings interface.

    Menu >Configuration> Network

2. Select the **More Settings** tab to enter the More Settings interface, as shown in Figure 11. 15.

Alarm Host IP	
Alarm Host Port	0
Server Port	8000
HTTP Port	80
Multicast IP	
RTSP Port	554

Figure 11. 15 More Settings Interface

3. Configure the remote alarm host, server port, HTTP port, multicast or 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., NVMS7000) is installed, and the **Alarm Host Port** must be the same as the alarm monitoring port configured in the software (default port is 7200).
- **Multicast IP**: The multicast can be configured to realize live view for more than the maximum number of cameras through network. A multicast address spans the Class-D IP range of 224.0.0.0 to 239.255.255.255. It is recommended to use the IP address ranging from 239.252.0.0 to 239.255.255.255.
  When adding a device to the CMS (Client Management System) software, the multicast address must be the same as the device's multicast IP.
- **RTSP Port**: The RTSP (Real Time Streaming Protocol) is a network control protocol designed for use in entertainment and communications systems to control streaming media servers.
  Enter the RTSP port in the text field of **RTSP Port**. The default RTSP port is 554, and you can change it according to different requirements.
- **Server Port** and **HTTP Port**: Enter the **Server Port** and **HTTP Port** in the text fields. The default Server Port is 8000 and the HTTP Port is 80, and you can change them according to different requirements.

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

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

11.2.6 Configuring HTTPS Port

Purpose:

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

Example:

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

NOTE The HTTPS port can be only configured through the web browser.

Steps:

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 the device.
3. Enter the HTTPS settings interface.
   Configuration > Remote Configuration > Network Settings > HTTPS
4. Create the self-signed certificate or authorized certificate.
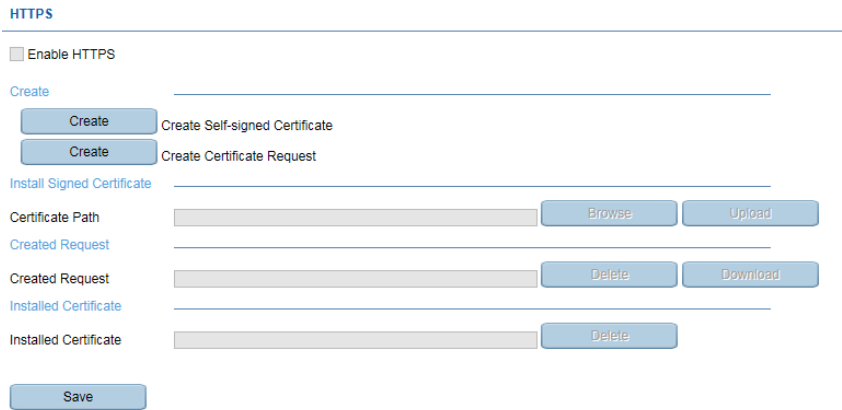
Figure 11. 16 HTTPS Settings

OPTION 1: Create the self-signed certificate

1) Click the **Create** button to create the following dialog box.
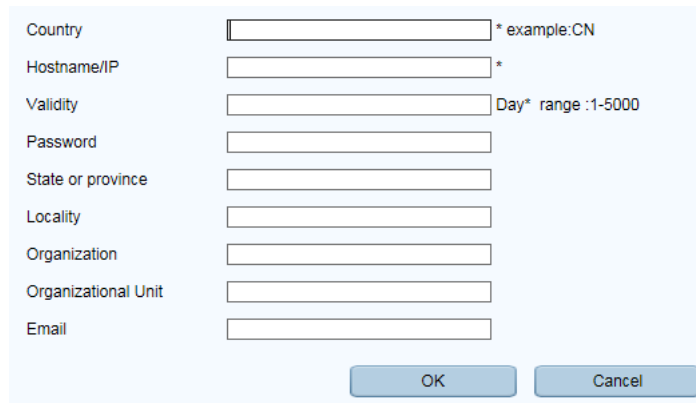
Figure 11. 17 Create Self-signed Certificate

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.
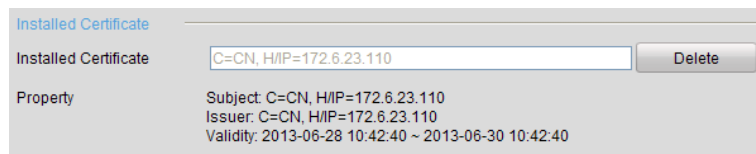
Figure 11. 18 Installed Certificate Property

6. Check the checkbox to enable the HTTPS function.

7. Click the **Save** button to save the settings.

11.2.7 Configuring Email

Purpose:

The system can be configured to send an Email 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 Email 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.

Steps:

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 11. 19.
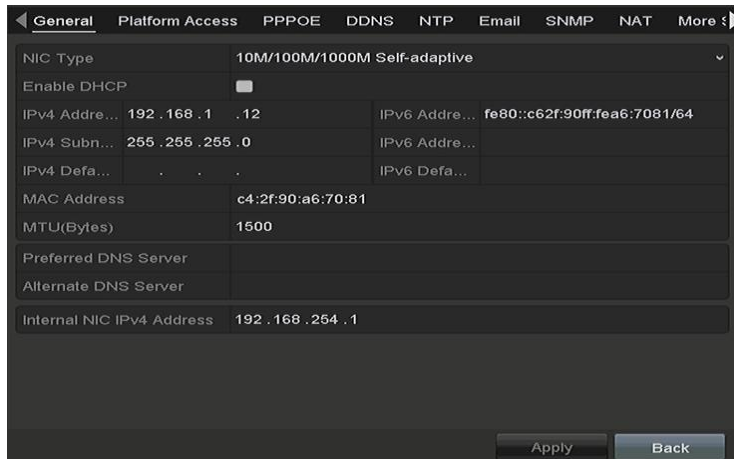
Figure 11. 19 Network Settings Interface

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

4. Select the Email tab to enter the Email Settings interface.
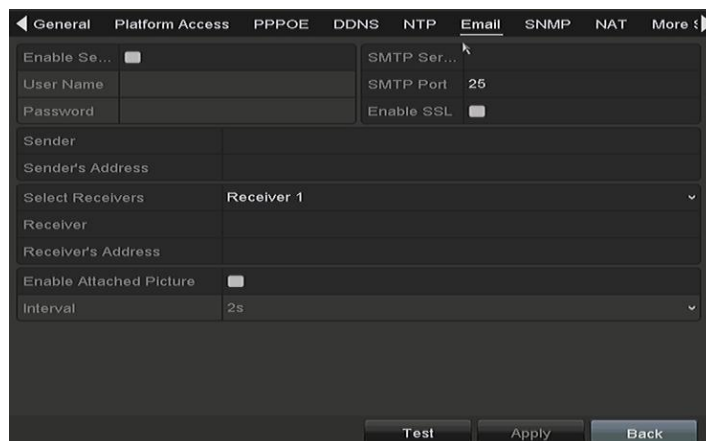
Figure 11. 20 Email Settings Interface

5. Configure the following Email settings:

   Enable Server Authentication (optional): Check the checkbox to enable the server authentication feature.

   User Name: The user account of sender's Email for SMTP server authentication.

Password: The password of sender's Email for SMTP server authentication.

SMTP Server: The SMTP Server IP address or host name (e.g., smtp.263xmail.com).

SMTP Port No.: The SMTP port. The default TCP/IP port used for SMTP is 25.

Enable SSL (optional): Click the checkbox to enable SSL if required by the SMTP server.

Sender: The name of sender.

Sender's Address: The Email address of sender.

Select Receivers: Select the receiver. Up to 3 receivers can be configured.

Receiver: The name of user to be notified.

Receiver's Address: The Email address of user to be notified.

Enable Attached Pictures: Check the checkbox of **Enable Attached Picture** 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.

E-mail Test: Sends a test message to verify that the SMTP server can be reached.

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

7. You can click **Test** button to test whether your Email settings work.

11.2.8 Configuring NAT

Purpose:

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

● **UPnP**^{TM}

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

Before you start:

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

Steps:

1. Enter the Network Settings interface.

   Menu > Configuration > Network

2. Select the **NAT** tab to enter the port mapping interface.
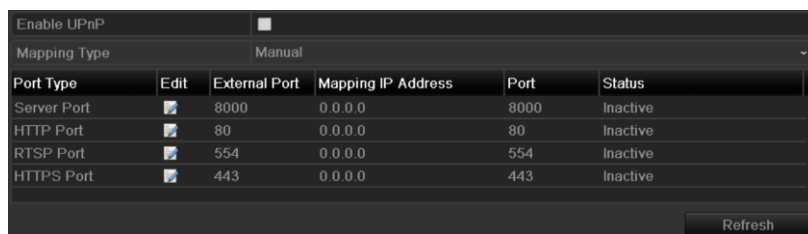
Figure 11. 21 UPnP™ Settings Interface

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.

Steps:

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

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

3) You can click **Refresh** button to get the latest status of the port mapping.

Enable UPnP		☑			
Mapping Type		Auto			
Port Type	Edit	External Port	Mapping IP Address	Port	Status
Server Port	📝	43728	172.6.21.31	8000	Active
HTTP Port	📝	31397	172.6.21.31	80	Active
RTSP Port	📝	59826	172.6.21.31	554	Active
HTTPS Port	📝	31231	172.6.21.31	443	Active
					Refresh

Figure 11. 22 UPnP™ Settings Finished-Auto

OPTION 2: Manual

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

Steps:

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

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

External Port Settings	
Port Type	Server Port
External Port	8000
	OK Cancel
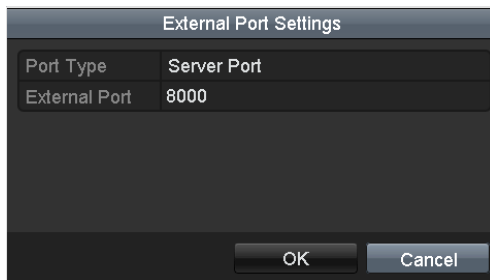
Figure 11. 23 External Port Settings Dialog Box

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

4) You can click **Refresh** button to get the latest status of the port mapping.
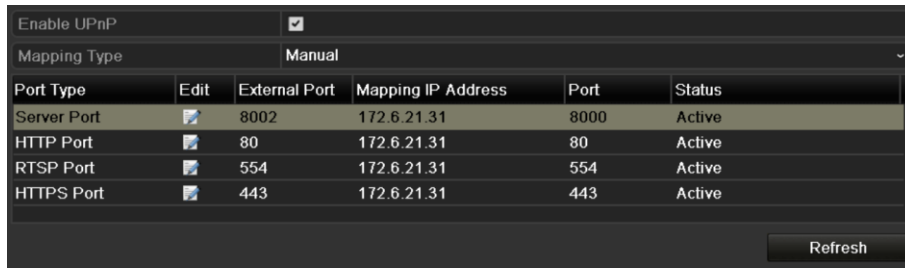
Figure 11. 24 UPnP™ Settings Finished-Manual

● **Manual Mapping**

If your router does not support the UPnP^TM function, perform the following steps to map the port manually in an easy way.

Before you start:

Make sure the router support the configuration of internal port and external port in the interface of Forwarding.

Steps:

1. Enter the Network Settings interface.

   Menu > Configuration > Network

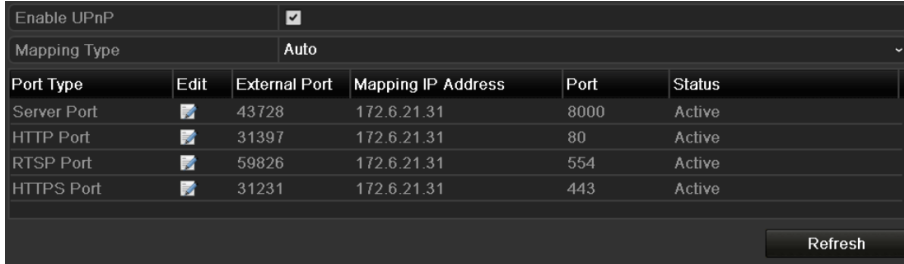2. Select the **NAT** tab to enter the port mapping interface.

3. Leave the Enable UPnP checkbox unchecked.

4. Click [icon] 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 value must be different from each other. If multiple devices are configured for the UPnP™ settings under the same router, the value of the port No. for each device should be unique.
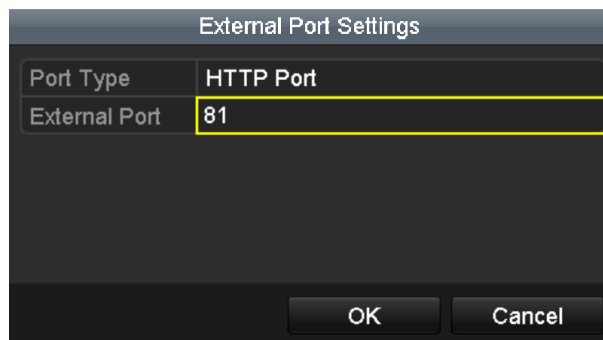
Figure 11. 25 External Port Settings Dialog Box

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 be corresponding with the device port, including server port, http port, RTSP port and https port.

Figure 11. 26 Setting Virtual Server Item

The above virtual server setting interface is for reference only, it may be different due to different router manufactures. Please contact the manufacture of router if you have any problems with setting virtual server.

11.3 Checking Network Traffic

Purpose:

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

Steps:

1. Enter the Network Traffic interface.

   Menu > Maintenance > Net Detect
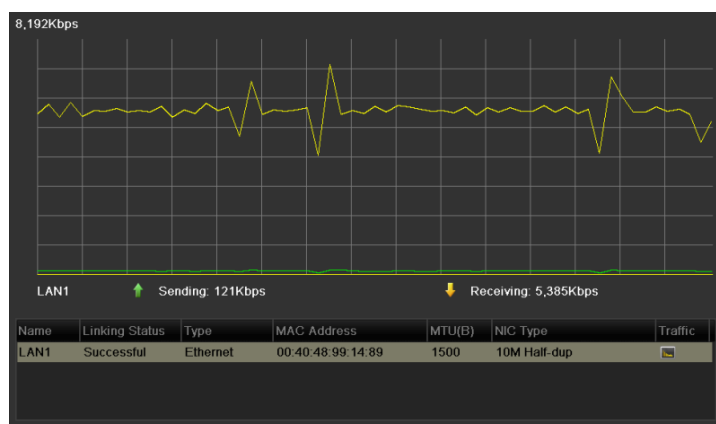
Figure 11. 27 Network Traffic Interface

2. You can view the sending rate and receiving rate information on the interface. The traffic data is refreshed every 1 second.

11.4 Checking Network Statistics

Purpose:

You can check the network status to obtain the real-time information of NVR.

Steps:

1. Enter the Network Detection interface.

   Menu>Maintenance>Net Detect

2. Click the **Network Stat.** tab.
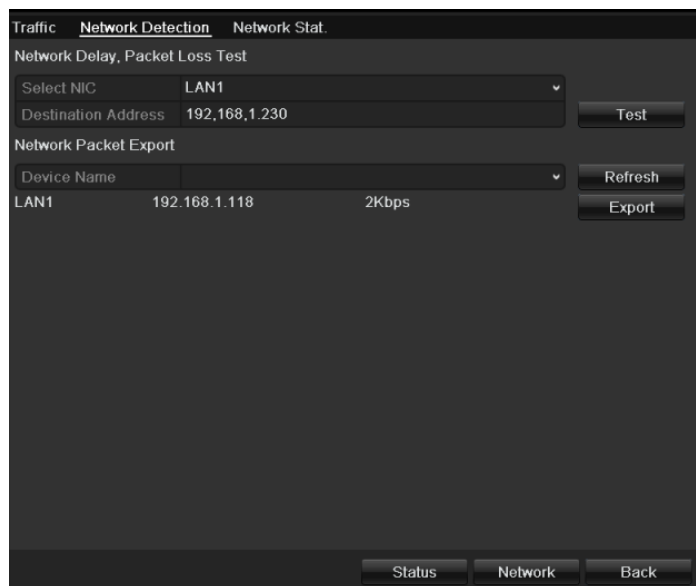
Figure 11. 28 Network Stat. Interface

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

4. You can click **Refresh** to get the newest status.

Chapter 12   RAID

12.1 Configuring Array

Purpose:

RAID (redundant array of independent disks) is a storage technology that combines multiple disk drive components into a logical unit. A RAID setup stores data over multiple hard disk drives to provide enough redundancy so that data can be recovered if one disk fails. Data is distributed across the drives in one of several ways called "RAID levels", depending on what level of redundancy and performance is required.

The NVR supports the disk array which is realized by the software, and RAID0, RAID1, RAID5 and RAID 10 are supported. You can enable the RAID function on your demand.

Before you start:

Please 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.

Introduction:

If the RAID is enabled, the NVR can store the data (such as record, picture, log information) in the HDD only after you have created the virtual disk or you have configured network HDD (refer to *Chapter 11.2 Managing Network HDD*). Our device provides two ways for creating the virtual disk, including one-touch configuration and manual configuration. The following flow chart shows the process of creating virtual disk.
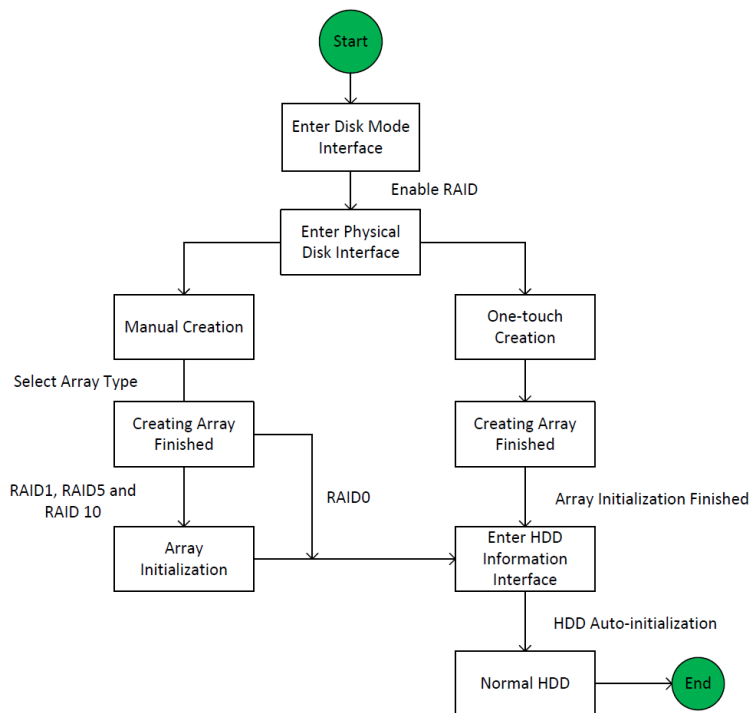
Figure 12. 1 RAID Working Flow

12.1.1 Enable RAID

Purpose:

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 startup, please refer to step 7 of Chapter 2.2.

- **OPTION 2:**

Enable the RAID function in the HDD Management Interface.

Steps:

1. Enter the disk mode configuration interface.

   Menu > HDD > Advanced
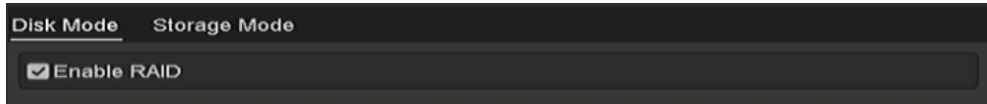
Figure 12. 2 Enable RAID Interface

2. Check the checkbox of **Enable RAID**.

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

12.1.2 One-touch Configuration

Purpose:

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

Before you start:

1. The RAID function should be enabled, please refer to the Chapter 10.1.1 for details.

2. As the default array type is RAID 5, please install at least 3 HDDs in you device.

Steps:

1. Enter the RAID configuration interface.

   Menu > HDD > RAID
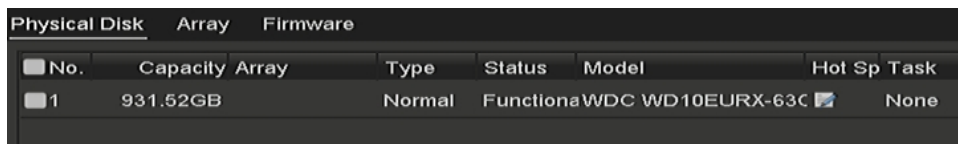
Figure 12. 3 Physical Disk Interface

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

3. Click the **One-touch Create** button to enter the One-touch Array Configuration interface.
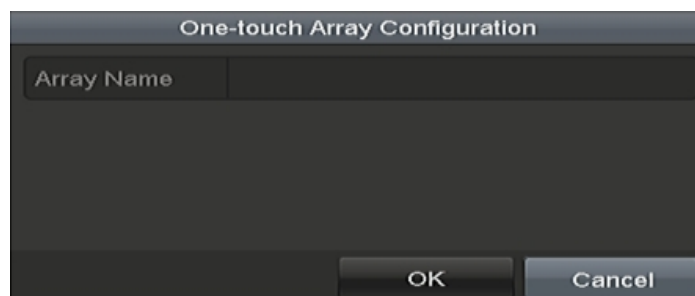
Figure 12. 4 One-touch Array Configuration

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

![NOTE]

If you install 4 HDDs or above for one-touch configuration, a hot spare disk will be set by default. It is recommended to set hot spare disk for automatically rebuilding the array when the array is abnormal.

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

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.
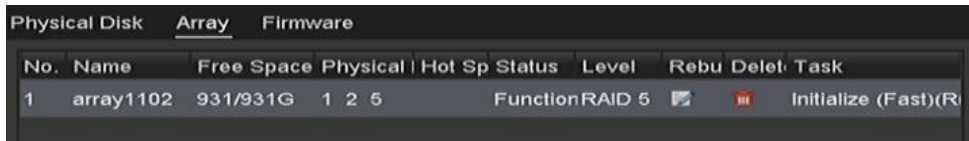
Figure 12. 5 Array Settings Interface

7. A created array displays as an HDD in the HDD information interface.
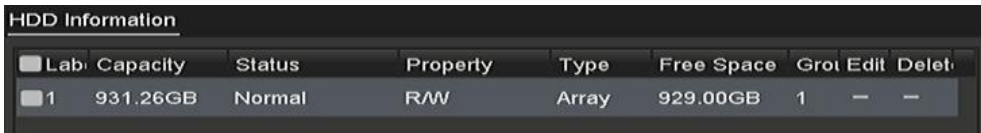
Figure 12. 6 HDD Information Interface

12.1.3 Manually Creating Array

Purpose:

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

![NOTE]

In this section, we take RAID 5 as an example to describe the manual configuration of array and virtual disk.

Steps:

1. Enter the Physical Disk Settings interface.

   Menu > HDD > RAID > Physical Disk
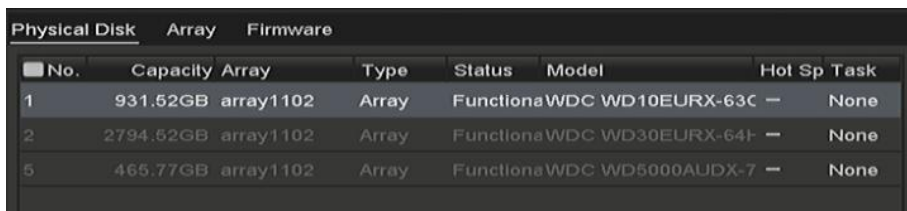
Figure 12. 7 Physical Disk Settings Interface

2. Click **Creat** button to enter the Create Array interface.
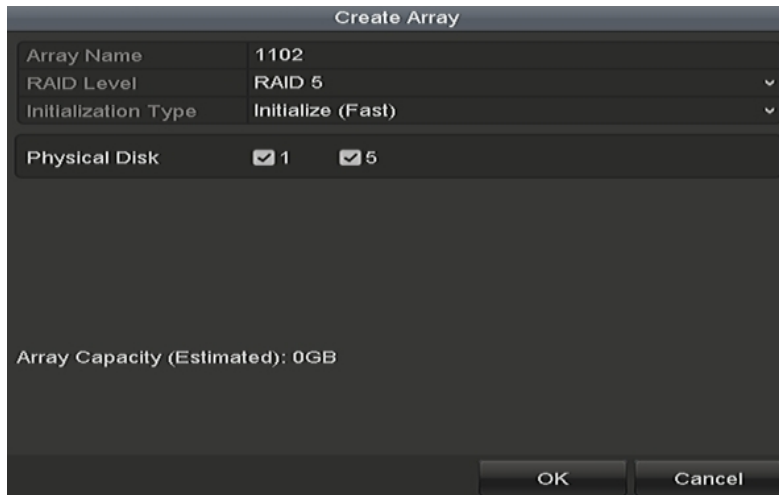
Figure 12. 8 Create Array Interface

3. Edit the **Array Name**; set the **RAID Level** to RAID 0, RAID 1, RAID 5 or RAID 10; select the **Physical Disk** that you want to configure array.

NOTE

- If you choose RAID 0, at least 2 HDDs must be installed.
- If you choose RAID 1, 2 HDDs need to be configured for RAID 1.
- If you choose RAID 5, at least 3 HDDs must be installed.
- If you choose RAID 10, the number of HDDs installed should be even in the range of 4~16.

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.
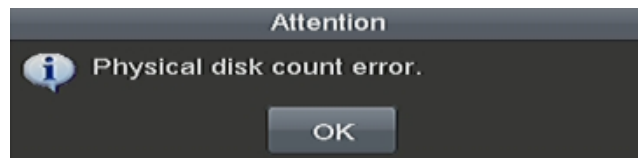
Figure 12. 9 Error Message Box

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

Figure 12. 10 Array Settings Interface

12.2 Rebuilding Array

Purpose:

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

When there is no disk loss in the array, the working status of array will change to Functional; when the number of lost disks has exceeded the limit, the working status of array will change to Offline; in other conditions, the working status is Degraded.

When the virtual disk is in Degraded status, you can restore it to Functional by array rebuilding.

Before you start:

Please make sure the hot spare disk is configured.

1. Enter the Physical Disk Settings interface to configure the hot spare disk.
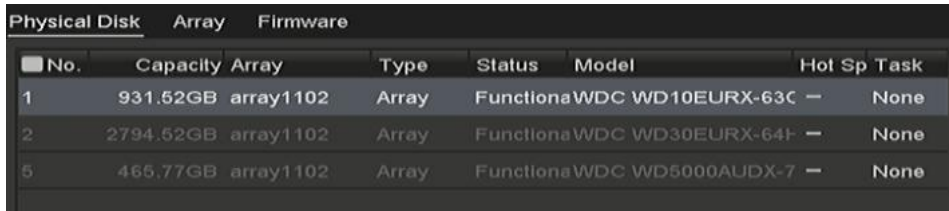
Figure 12. 11 Physical Disk Settings Interface

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

[NOTE icon]

Only global hot spare mode is supported.

12.2.1 Automatically Rebuilding Array

Purpose:

When the virtual disk is in Degraded status, the device can start rebuilding the array automatically with the hot spare disk to ensure the high security and reliability of the data.

Steps:

Enter the Array Settings interface. The status of the array is Degraded. Since the hot spare disk is configured, the system will automatically start rebuilding using it.

Menu > HDD > RAID > Array
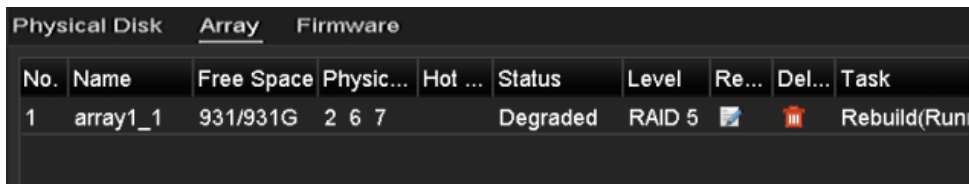
Figure 12. 12 Array Settings Interface

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

12.2.1 Manually Rebuilding Array
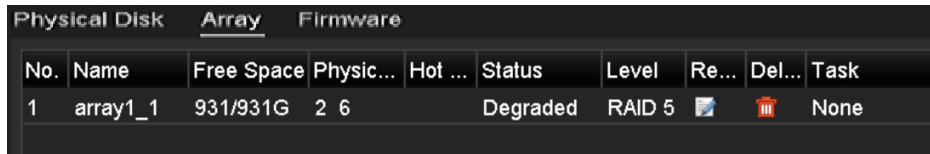
Purpose:

If you do not enable the Auto-rebuild in Firmware Settings interface (Menu>HDD>RAID>Firmware) or the hot spare disk has not been configured, then you can rebuild the array manually to restore the array when the virtual disk is in Degraded status.

Steps:

1. Enter the Array Settings interface. The disk 3 is lost.

   Menu > HDD > RAID > Array

Physical Disk	Array	Firmware							
No.	Name	Free Space	Physic...	Hot ...	Status	Level	Re...	Del...	Task
1	array1_1	931/931G	2 6		Degraded	RAID 5	📝	🗑	None

Figure 12. 13 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 should exist for rebuilding the array.

Rebuild Array

Array Name	array1102
RAID Level	RAID 5
Array Disk	1 2 5

OK   Cancel

Figure 12. 14 Rebuild Array Interface

3. Select the available physical disk and click **OK** button to confirm to rebuild the array.
4. The "Do not unplug the physical disk when it is under rebuilding" message box pops up. Click **OK** button to start rebuilding.
5. You can enter the Array Settings interface to view the rebuilding status.
6. After rebuilding successfully, the array and virtual disk will restore to Functional.

12.3 Deleting Array

NOTE

Deleting array will cause to delete all the data saved in the disk.

Steps:

1. Enter the Array Settings interface.

    Menu>HDD>RAID>Array
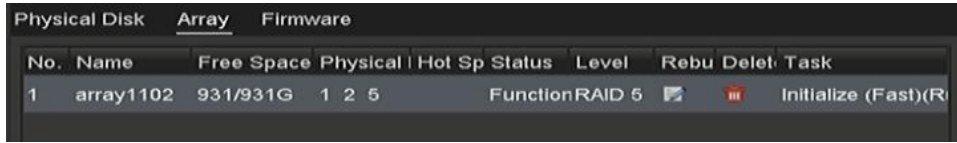
Figure 12. 15 Array Settings Interface

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

Figure 12. 16 Confirm Array Deletion

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

NOTE

Deleting array will cause to delete all the data in the array.

12.4 Checking the Firmware Information

Purpose:

You can view and check the information of the firmware on the Firmware interface.

Steps:

1. Enter the Firmware interface to check the information of the firmware, including the version, maximum physical disk quantity, maximum array quantity, auto-rebuild status, etc.
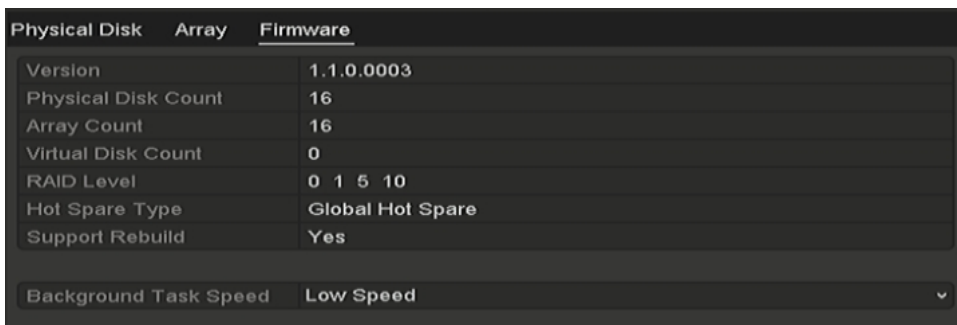
Figure 12. 17 Firmware Interface

2. You can set the Background Task Speed in the drop-down list.

Chapter 13   HDD Management

13.1 Initializing HDDs

Purpose:

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

A message box pops up when the NVR starts up if there exits any uninitialized HDD.
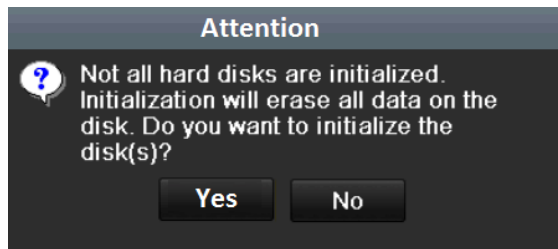
Figure 13. 1 Message Box of Uninitialized HDD

Click **Yes** button to initialize it immediately or you can perform the following steps to initialize the HDD.

Steps:

1. Enter the HDD Information interface.

    Menu > HDD> General

L...	Capacity	Status	Property	Type	Free Space	Gr...	Edit	D...
5	76,319MB	Initializing 20%	R/W	Local	0MB	1	–	–

Figure 13. 2 HDD Information Interface

---

2. Select HDD to be initialized.

3. Click the **Init** button.
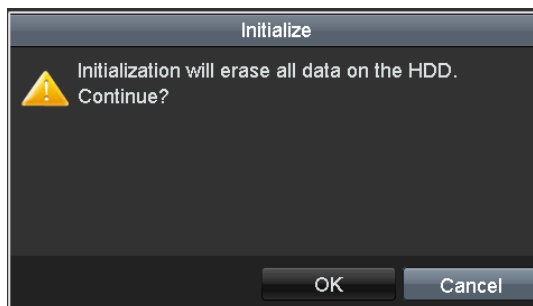
Figure 13. 3 Confirm Initialization

---

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

L...	Capacity	Status	Property	Type	Free Space	Gr...	Edit	D...
5	76,319MB	Initializing 20%	R/W	Local	0MB	1	–	–

Figure 13. 4 Status changes to Initializing

---

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

Figure 13. 5 HDD Status Changes to Normal

NOTEInitializing the HDD will erase all data on it.

13.2 Managing Network HDD

Purpose:

You can add the allocated NAS or disk of IP SAN to NVR, and use it as network HDD.

Steps:

1. Enter the HDD Information interface.

   Menu > HDD>General

Figure 13. 6 HDD Information Interface

2. Click the **Add** button to enter the Add NetHDD interface, as shown in Figure 13. 7.

Figure 13. 7 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 you can just manually enter the directory in the text field of NetHDD Directory.

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

NOTE Up to 8 NAS disks can be added.
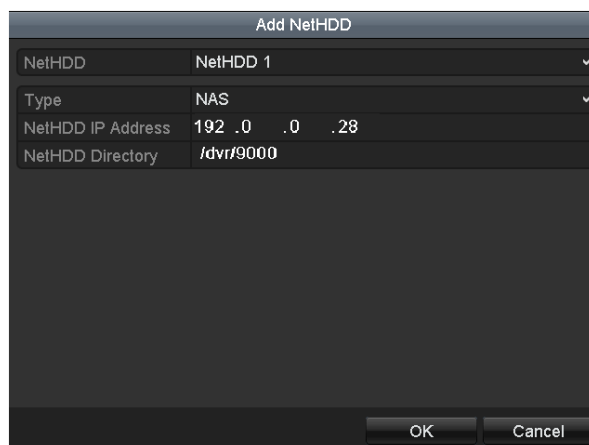
Figure 13. 8 Add NAS Disk

- **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 13. 9 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, please select it and click the **Init** button for initialization.

Figure 13. 10 Initialize Added NetHDD

13.3 Managing HDD Group

13.3.1 Setting HDD Groups

Purpose:

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

Steps:

1. Enter the Storage Mode interface.

    Menu > HDD > Advanced

2. Set the Mode to Group, as shown in Figure 13. 11.
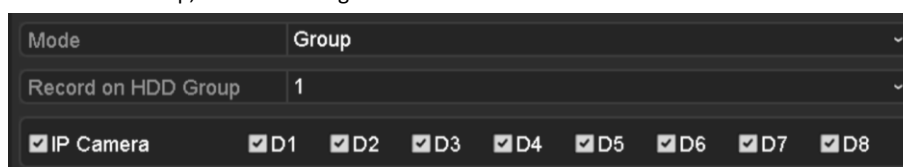
Figure 13. 11 Storage Mode Interface

3. Click the **Apply** button and the following Attention box will pop up.
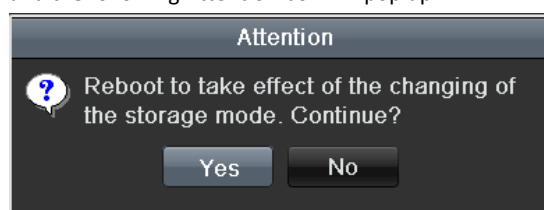
Figure 13. 12 Attention for Reboot

4. Click the **Yes** button to reboot the device to activate the changes.

5. After reboot of device, enter the HDD Information interface.

   Menu > HDD> General

6. Select HDD from the list and click [icon] icon to enter the Local HDD Settings interface, as shown in Figure 13. 13.

Figure 13. 13 Local HDD Settings Interface

7. Select the Group number for the current HDD.

The default group No. for each HDD is 1.

8. Click the **OK** button to confirm the settings.
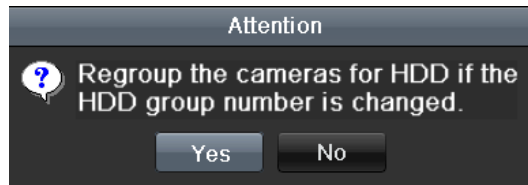
Figure 13. 14 Confirm HDD Group Settings

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

13.3.2 Setting HDD Property

Purpose:

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

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

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

Steps:

1. Enter the HDD Information interface.

   Menu > HDD> General

2. Select HDD from the list and click the [image] icon to enter the Local HDD Settings interface, as shown in Figure 13. 15.
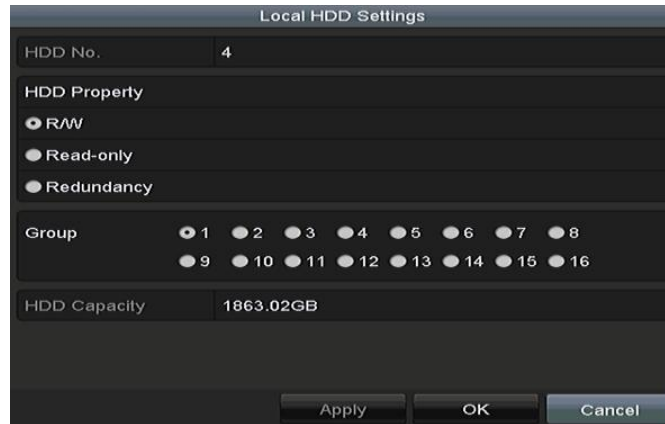
Figure 13. 15 Set HDD Property

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 2 hard disks must be installed on your NVR when you want to set a HDD to Redundancy, and there is one HDD with R/W property.

13.4 Configuring Quota Mode

Purpose:

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

Steps:

1. Enter the Storage Mode interface.

   Menu > HDD > Advanced

2. Set the **Mode** to Quota, as shown in Figure 13. 16.

   [NOTE]

   The NVR must be rebooted to enable the changes to take effect.
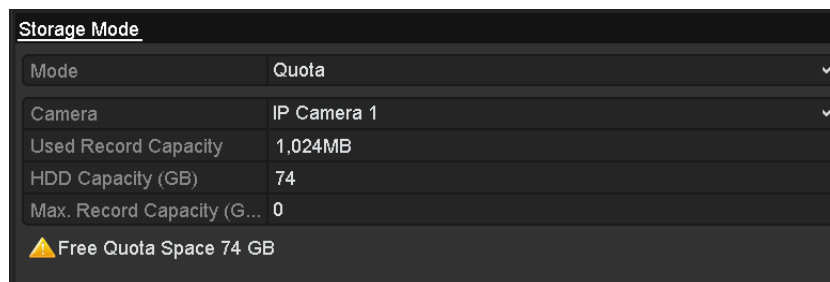
Figure 13. 16 Storage Mode Settings Interface

3. Select a camera for which you want to configure quota.

143

4. Enter the storage capacity in the text field of **Max. Record Capacity (GB)**, as shown in Figure 13. 17.
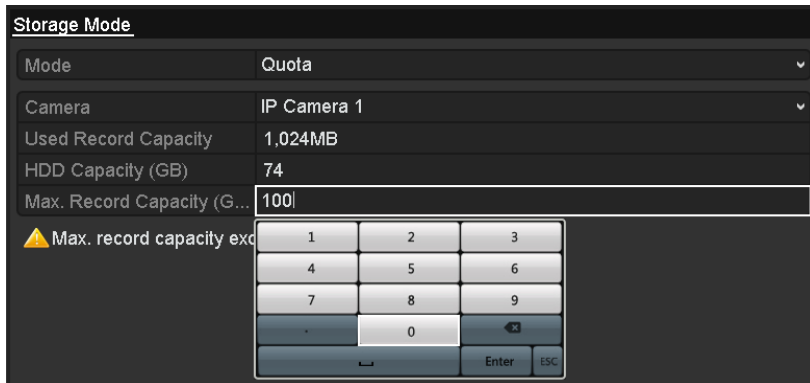
Figure 13. 17 Configure Record/Picture Quota

5. You can copy the quota settings of the current camera to other cameras if required. Click the **Copy** button to enter the Copy Camera menu, as shown in Figure 13. 18.

Figure 13. 18 Copy Settings to Other Camera(s)

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

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

13.5 Checking HDD Status

Purpose:

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

Checking HDD Status in HDD Information Interface

Steps:

1. Enter the HDD Information interface.

   Menu > HDD>General

2. Check the status of each HDD which is displayed on the list, as shown in Figure 13. 19.
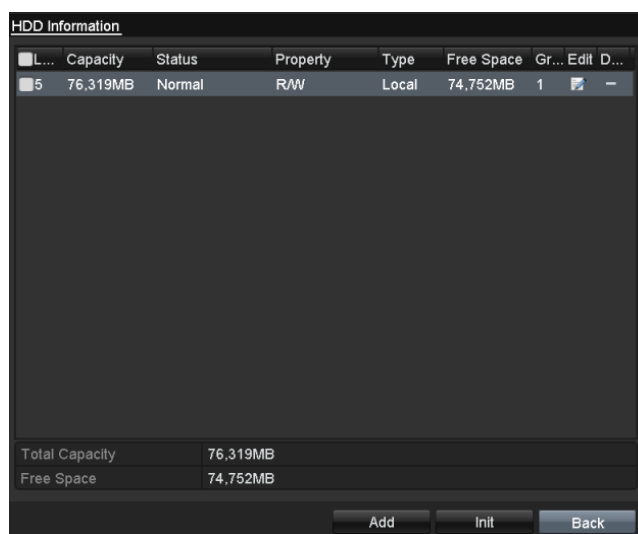
Figure 13. 19 View HDD Status (1)

If the status of HDD is *Normal* or *Sleeping*, it works normally. If the status is *Uninitialized* or *Abnormal*, please initialize the HDD before use. And if the HDD initialization is failed, please replace it with a new one.

Checking HDD Status in HDD Information Interface

Steps:

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 13. 20.
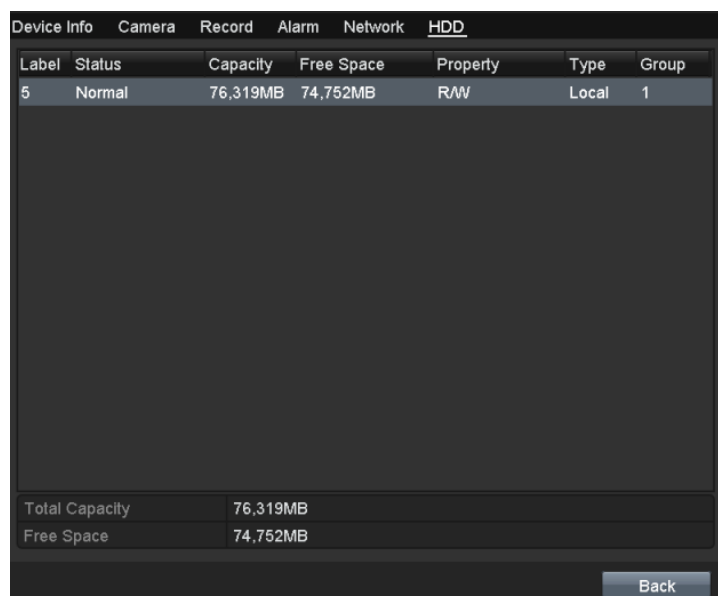
Figure 13. 20 View HDD Status (2)

13.6 HDD Detection

This function is not supported if the RAID function is enabled.

Purpose:

The device provides the HDD detection function such as the adopting of the 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 indicators of reliability in the hopes of anticipating failures.

S.M.A.R.T. Settings

Steps:

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 13. 21.
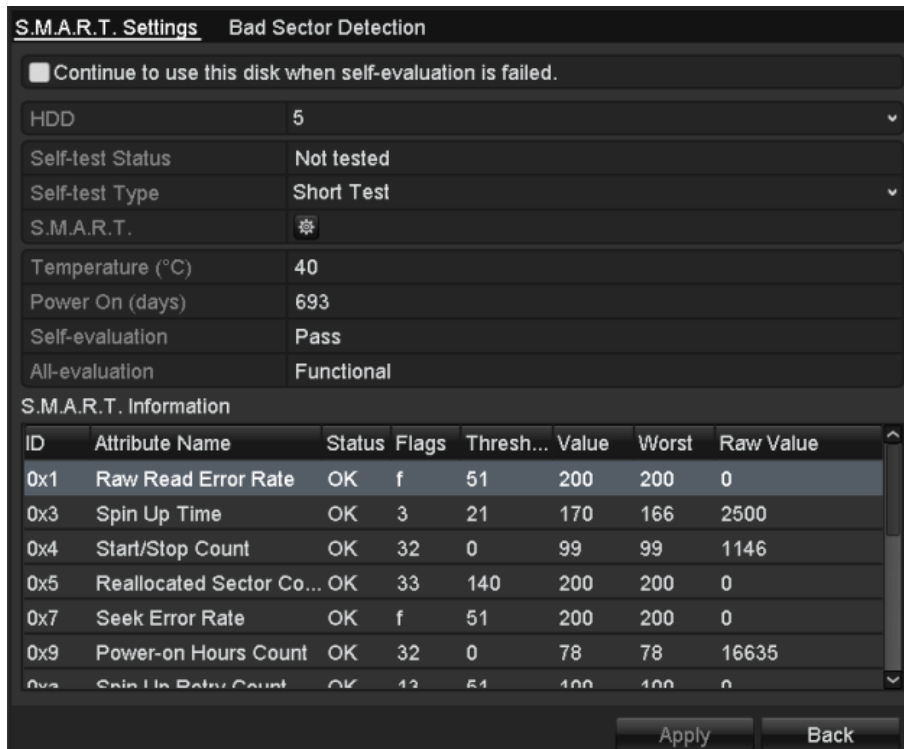
Figure 13. 21 S.M.A.R.T Settings Interface

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

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

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

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

Bad Sector Detection

Steps:

1. Click the Bad Sector Detection tab.

2. Select the HDD No. in the dropdown 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.
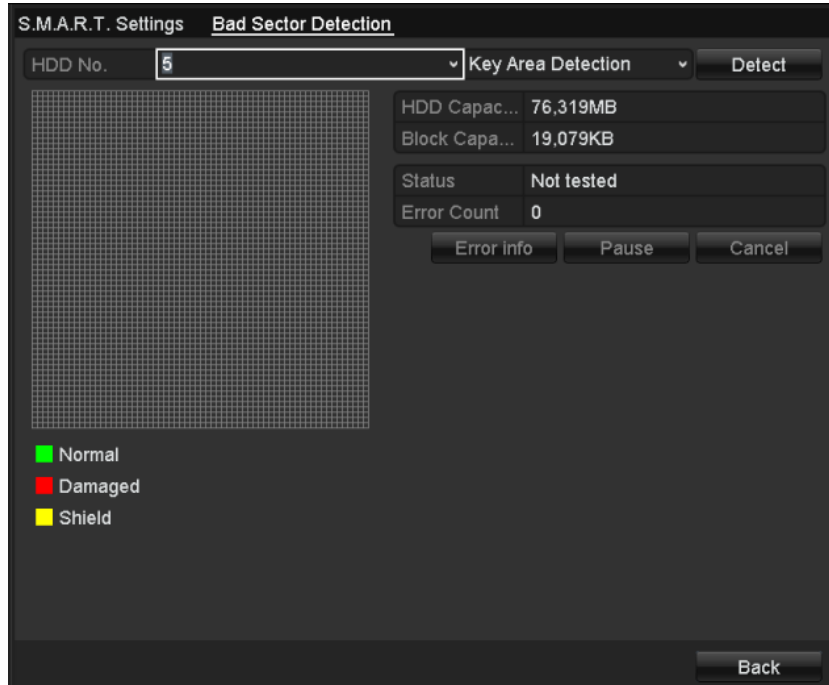
Figure 13. 22 Bad Sector Detection

And you can click **Error info** button to see the detailed damage information.

And you can also pause/resume or cancel the detection.

13.7 Configuring HDD Error Alarms

Purpose:

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

Steps:

1. Enter the Exception interface.

   Menu > Configuration > Exceptions

2. Select the Exception Type to **HDD Error** from the dropdown list.

3. Click the checkbox(s) below to select the HDD error alarm type (s), as shown in Figure 13. 23.

   ![NOTE]

   The alarm type can be selected to: Audible Warning, Notify Surveillance Center, Send Email and Trigger Alarm Output. Please refer to *Chapter Setting Alarm Response Actions*.

Figure 13. 23 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 14   Camera Settings

14.1 Configuring OSD Settings

Purpose:

You can configure the OSD (On-screen Display) settings for the camera, including date /time, camera name, etc.

Steps:

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.
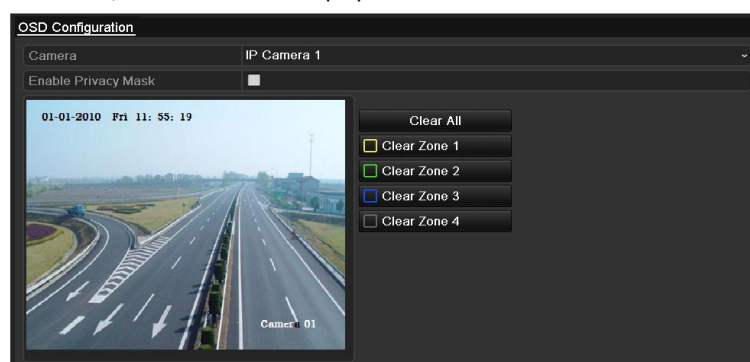
Figure 14. 1 OSD Configuration Interface

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.

14.2 Configuring Privacy Mask

Purpose:

You are allowed to configure the four-sided privacy mask zones that cannot be viewed by the operator. The privacy mask can prevent certain surveillance areas to be viewed or recorded.

Steps:

1. Enter the Privacy Mask Settings interface.

   Menu > Camera >Privacy Mask

2. Select the camera to set privacy mask.

3. Click the checkbox of **Enable Privacy Mask** to enable this feature.
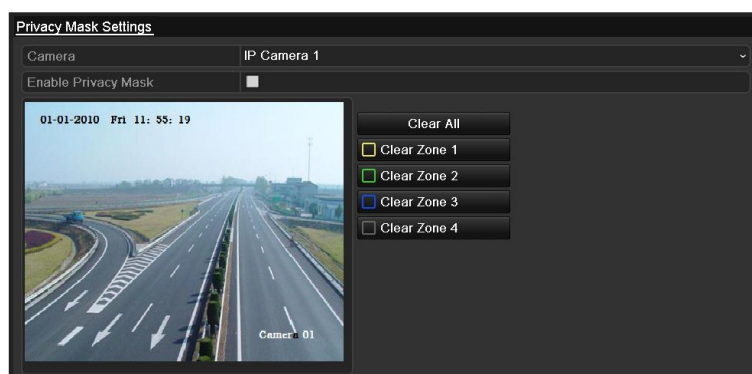
Figure 14. 2 Privacy Mask Settings Interface

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

NOTE

Up to 4 privacy masks zones can be configured and the size of each area can be adjusted.

5. The configured privacy mask zones on the window can be cleared by clicking the corresponding Clear Zone1-4 icons on the right side of the window, or click **Clear All** to clear all zones.
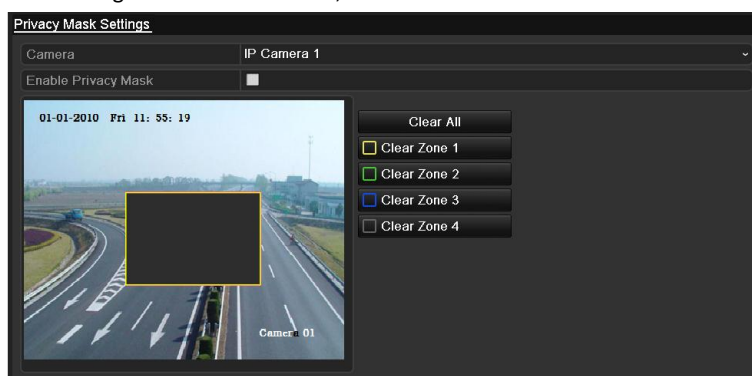
Figure 14. 3 Set Privacy Mask Area

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

14.3 Configuring Video Parameters

Steps:

1. Enter the Image Settings interface.

   Menu > Camera >Image

Figure 14. 4 Image Settings Interface

---

2. Select the camera to set image parameters.

3. You can click on the arrow to change the value of each parameter.

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

Chapter 15   NVR   Management   and Maintenance

15.1 Viewing System Information

Steps:

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.

Device Info	Camera	Record	Alarm	Network	HDD
Device Name	X X X X X X X X				
Model	X X X X X X X X				
Serial No.	X X X X X X X X X X X X X X X X				
Firmware Version	V X.X.X				
Encoding Version	V X.X.X				
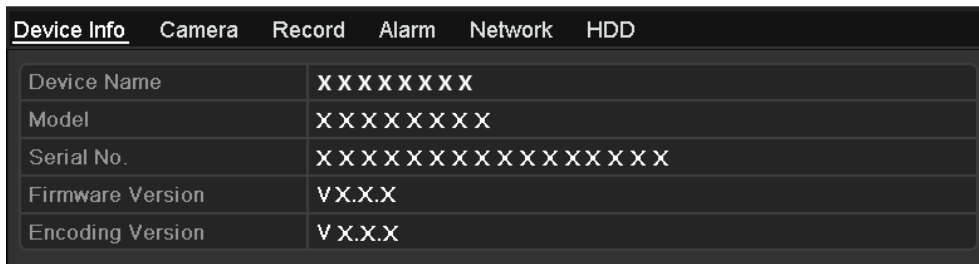
Figure 15. 1 Device Information Interface

15.2 Searching & Export Log Files

Purpose:

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

Steps:

1. Enter the Log Search interface.
   Menu > Maintenance > Log Information
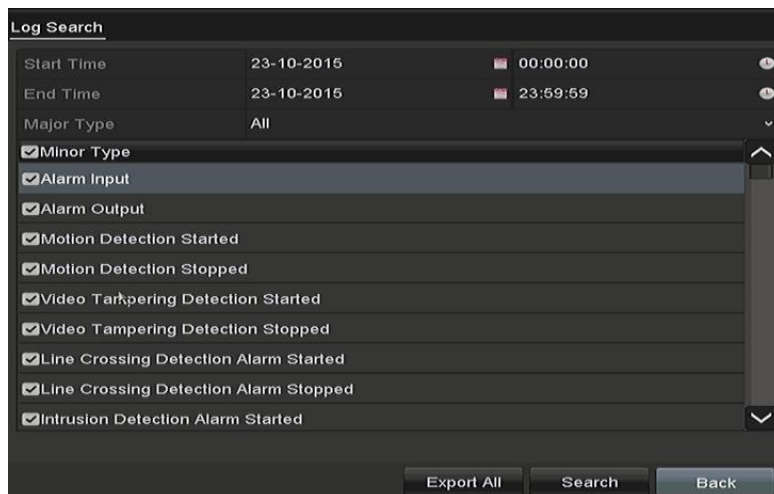
Figure 15. 2 Log Search Interface

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

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

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

Figure 15. 3 Log Search Results

Up to 2000 log files can be displayed each time.

5. You can click the ✅ button of each log or double click it to view its detailed information, as shown in Figure 15. 4. And you can also click the ⏺ button to view the related video files if available.

Figure 15. 4 Log Details

6. If you want to export the log files, click the **Export** button to enter the Export menu, as shown in Figure 15. 5.
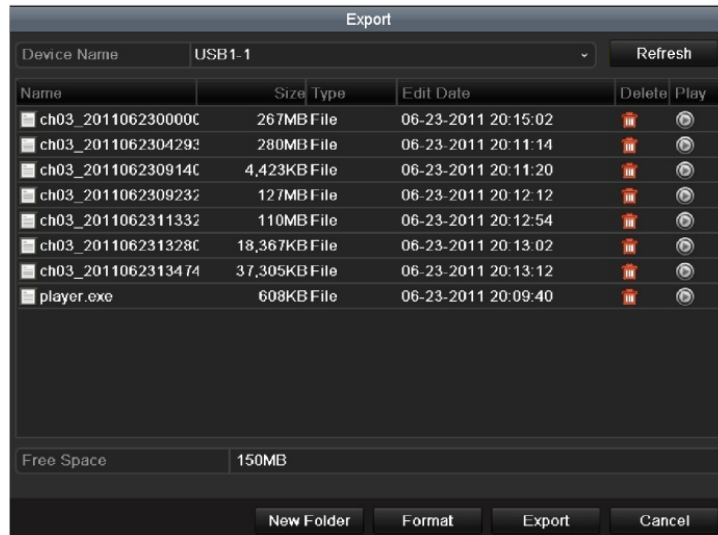
Figure 15. 5 Export Log Files

---

7. Select the backup device from the dropdown list of **Device Name**.

8. Select the format of the log files to be exported. Up to 9 formats are selectable.

9. Click the **Export** to export the log files to the selected backup device.

    You can click the **New Folder** button to create new folder in the backup device, or click the **Format** button

    to format the backup device before log export.

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

15.3 Importing/Exporting IP Camera Info

Purpose:

The information of added IP camera can be generated into an excel file and exported to the local device for

backup, including the IP address, manage port, password of admin, etc.. And the exported file can be edited on

your PC, like adding or deleting the content, and copy the setting to other devices by importing the excel file to it.

Steps:

1. Enter the camera management interface.

    Menu > Camera > IP Camera Import/Export

2. Click the IP Camera Import/Export tab, the content of detected plugged external device appears.

3. Click the **Export** button to export configuration files to the selected local backup device.

4. To import a configuration file, select the file from the selected backup device and click the **Import** button.

    After the importing process is completed, you must reboot the NVR.

15.4 Importing/Exporting Configuration Files

Purpose:

The configuration files of the NVR can be exported to 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.

Steps:

1. Enter the Import/Export Configuration File interface.

   Menu > Maintenance >Import/Export

Figure 15. 6 Import/Export Config File

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

NOTE

After having finished the import of configuration files, the device will reboot automatically.

15.5 Upgrading System

Purpose:

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

15.5.1 Upgrading by Local Backup Device

Steps:

1. Connect your NVR with a local backup device where the update firmware file is located.

2. Enter the Upgrade interface.

    Menu >Maintenance>Upgrade

3. Click the **Local Upgrade** tab to enter the local upgrade menu, as shown in Figure 15. 7.
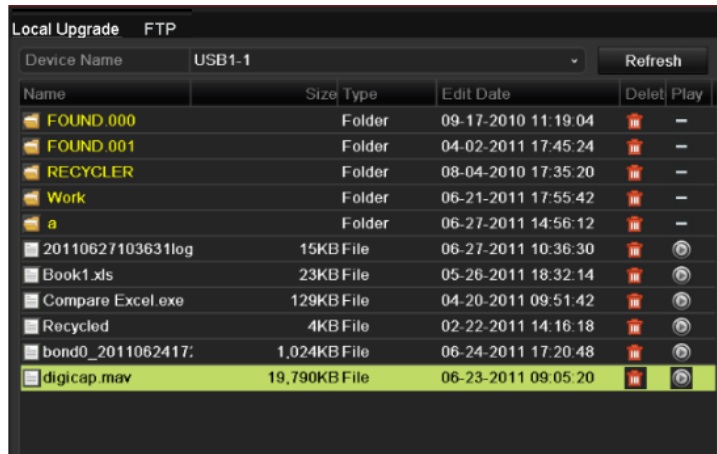
Figure 15. 7 Local Upgrade Interface

4. Select the update file from the backup device.

5. Click the **Upgrade** button to start upgrading.

6. After the upgrading is complete, reboot the NVR to activate the new firmware.

15.5.2 Upgrading by FTP

Purpose:

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

Refer to the user manual of the FTP server to set the FTP server on your PC and put the firmware file into the directory as required.

Steps:

1. Enter the Upgrade interface.

    Menu >Maintenance>Upgrade

2. Click the **FTP** tab to enter the local upgrade interface, as shown in Figure 15. 8.
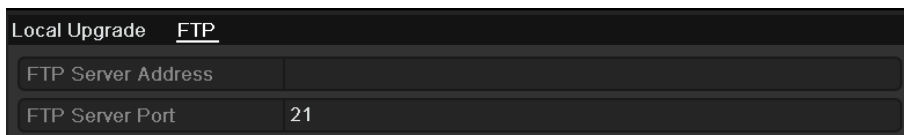
Figure 15. 8 FTP Upgrade Interface

3. Enter the FTP Server Address in the text field.

4. Click the **Upgrade** button to start upgrading.

5. After the upgrading is complete, reboot the NVR to activate the new firmware.

15.6 Restoring Default Settings

Steps:

1. Enter the Default interface.

    Menu > Maintenance > Default
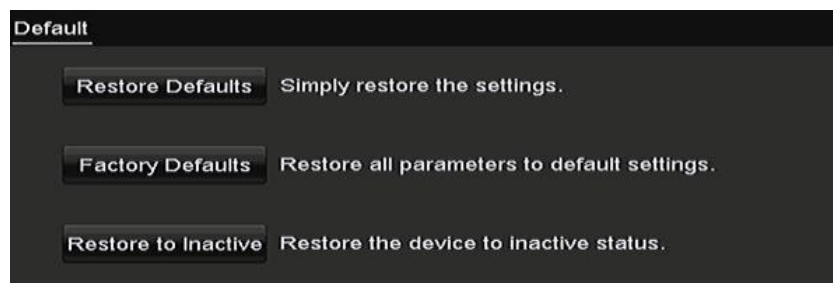
Figure 15. 9 Restore Defaults

2. Select the restoring type from the following three options.

Restore Defaults: Restore all parameters, except the network (including IP address, subnet mask, gateway, MTU, NIC working mode, default route, server port, etc.) and user account parameters, to the factory default settings.

Factory Defaults: Restore all parameters to the factory default settings.

Restore to Inactive: Restore the device to the inactive status.

3. Click the **OK** button to restore the default settings.

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

Chapter 16   Others

16.1 Configuring RS-232 Serial Port

Purpose:

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.

Steps:

1. Enter the RS-232 Settings interface.

   Menu >Configuration> RS-232
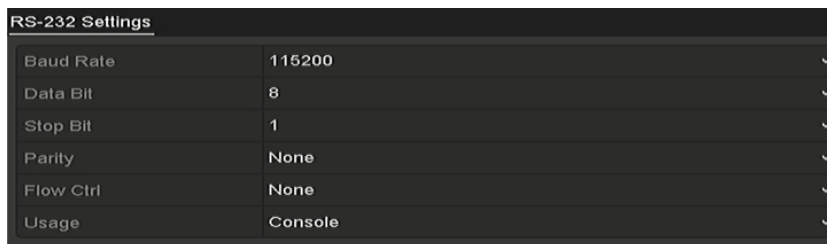
Figure 16. 1 RS-232 Settings Interface

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.

16.2 Configuring General Settings

Purpose:

You can configure the output standard and resolution for the monitors, system time and date, and mouse pointer speed through the Menu > Configuration > General interface.

Steps:

1. Enter the General Settings interface.

   Menu >Configuration> General

2. Select the **General** tab.
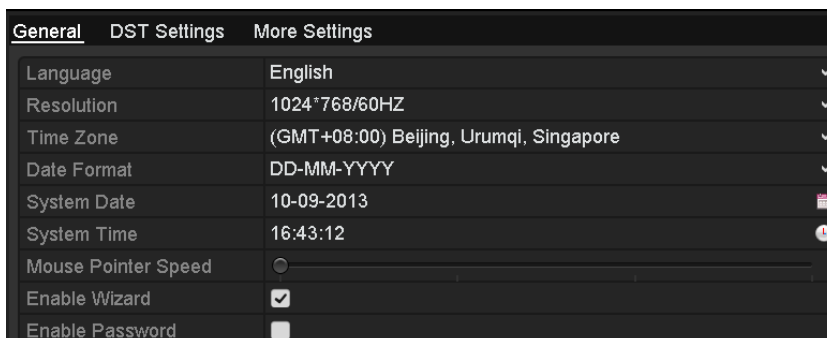
Figure 16. 2 General Settings Interface

3. Configure the following settings:

    - **Language:** The default language used is *English*.
    - **VGA/HDMI Resolution:** Select the output resolution for the main output (HDMI1/VGA), which must be the same with the resolution of the monitor screen.
    - **HDMI2 Resolution:** Select the HDMI2 resolution, which must be the same with the resolution of the monitor screen.
    - **Time Zone:** Select the time zone.
    - **Date Format:** Select the date format.
    - **System Date:** Select the system date.
    - **System Time:** Select the system time.
    - **Mouse Pointer Speed:** Set the speed of mouse pointer; 4 levels are configurable.
    - **Enable Wizard:** Enable/disable the Wizard when the device starts up.
    - **Enable Password:** Enable/disable the use of the login password.

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

16.3 Configuring DST Settings

Steps:

1. Enter the General Settings interface.

    Menu >Configuration>General

2. Choose **DST Settings** tab.

Figure 16. 3 DST Settings Interface

You can check the checkbox before the Auto DST Adjustment item.

Or you can manually check the Enable DST checkbox, and then you choose the date of the DST period.

16.4 Configuring More Settings for Device Parameters

Steps:

1. Enter the General Settings interface.

    Menu >Configuration>General

2. Click the **More Settings** tab to enter the More Settings interface, as shown in Figure 16. 4.
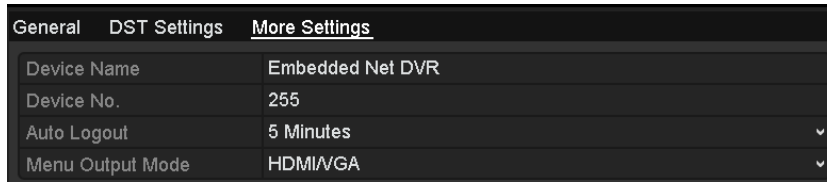
Figure 16. 4 More Settings Interface

3. Configure the following settings:

- **Device Name:** Edit the name of NVR.
- **Device No.:** Edit the serial number of NVR. The Device No. can be set in the range of 1~255, and the default No. is 255. The number is used for the remote and keyboard control.
- **Auto Logout:** Set timeout time for menu inactivity. E.g., when the timeout time is set to *5 Minutes*, then the system will exit from the current operation menu to live view screen after 5 minutes of menu inactivity.

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

16.5 Managing User Accounts

Purpose:

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

16.5.1 Adding a User

Steps:

1. Enter the User Management interface.

    Menu >Configuration>User

Figure 16. 5 User Management Interface

2. Click the **Add** button to enter the Add User interface.
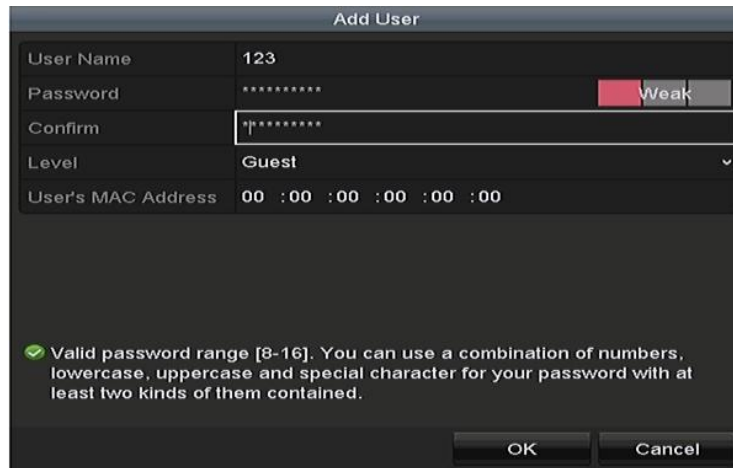
Figure 16. 6 Add User Menu

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

    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 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.*

    Level: Set the user level to Operator or Guest. Different user levels have different operating permission.

    - **Operator:** The *Operator* user level has permission of Two-way Audio in Remote Configuration and all operating permission in Camera Configuration by default.

    - **Guest:** The Guest user has no permission of Two-way Audio in Remote Configuration and only has the local/remote playback in the Camera Configuration by default.

    User's MAC Address: The MAC address of the remote PC which logs onto the NVR. If it is configured and enabled, it only allows 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, as shown in Figure 16. 7.

Figure 16. 7 Added User Listed in User Management Interface

5. Select the user from the list and then click the ✅ button to enter the Permission settings interface, as shown in Figure 16. 8.

Figure 16. 8 User Permission Settings Interface

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

Local Configuration
- Local Log Search: Searching and viewing logs and system information of NVR.
- Local Parameters Settings: Configuring parameters, restoring factory default parameters and importing/exporting configuration files.
- Local Camera Management: The adding, deleting and editing of IP cameras.
- Local Advanced Operation: Operating HDD management (initializing HDD, setting HDD property), upgrading system firmware, clearing I/O alarm output.
- Local Shutdown Reboot: Shutting down or rebooting the NVR.

Remote Configuration
- Remote Log Search: Remotely viewing logs that are saved on the NVR.
- Remote Parameters Settings: Remotely configuring parameters, restoring factory default parameters and importing/exporting configuration files.
- Remote Camera Management: Remote adding, deleting and editing of the IP cameras.
- Remote Serial Port Control: Configuring settings for RS-232 and RS-485 ports.
- Remote Video Output Control: Sending remote button control signal.
- Two-Way Audio: Realizing two-way radio between the remote client and the NVR.
- Remote Alarm Control: Remotely arming (notify alarm and exception message to the remote client) and controlling the alarm output.
- Remote Advanced Operation: Remotely operating HDD management (initializing HDD, setting HDD property), upgrading system firmware, clearing I/O alarm output.
- Remote Shutdown/Reboot: Remotely shutting down or rebooting the NVR.

Camera Configuration
- Remote Live View: Remotely viewing live video of the selected camera (s).
- Local Manual Operation: Locally starting/stopping manual recording and alarm output of the selected camera (s).
- Remote Manual Operation: Remotely starting/stopping manual recording and alarm output of the selected camera (s).
- Local Playback: Locally playing back recorded files of the selected camera (s).
- Remote Playback: Remotely playing back recorded files of the selected camera (s).
- Local PTZ Control: Locally controlling PTZ movement of the selected camera (s).

- Remote PTZ Control: Remotely controlling PTZ movement of the selected camera (s).
- Local Video Export: Locally exporting recorded files of the selected camera (s).

7. Click the **OK** button to save the settings and exit interface.

![NOTE icon]

Only the *admin* user account has the permission of restoring factory default parameters.

16.5.2 Deleting a User

Steps:

1. Enter the User Management interface.

   Menu >Configuration>User

2. Select the user to be deleted from the list, as shown in Figure 16. 9.

Figure 16. 9 User List

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

16.5.3 Editing a User

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

Steps:

1. Enter the User Management interface.

   Menu >Configuration>User

2. Select the user to be edited from the list, as shown in Figure 16. 9.

3. Click the 📝 icon to enter the Edit User interface, as shown in Figure 16. 10.

Figure 16. 10 Edit User Interface

4. Edit the corresponding parameters.

- **Operator and Guest**

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

- **Admin**

  You are only allowed to edit te password and MAC address. Check the checkbox of **Change Password** if you want to change the password, and the input the correct old password, and the new password in the text field of **Password** and **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. 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 te user management interface to edit the permission.

Chapter 17   Video Wall Configuration and Operation

Purpose:

With the extension HDMI output board, the model can realize the video wall display, windowing and roaming of images directly via the HDMI outputs.

The NVMS7000 is a versatile video management software for the DVRs, NVRs, IP cameras, encoders, decoders, VCA device, alarm host, etc. It provides multiple functionalities, including real-time live view, video recording, remote search and playback, file backup, alarm receiving, etc., for the connected devices to meet the needs of monitoring task.

Run the supplied disk and double-click icon to install the NVMS7000 client software in your PC.

NOTE

Please refer to the user manual of NVMS7000 for more detailed information.

17.1 User Registration and Login

Registering a Super User

For the first time to use NVMS7000 client software, you need to register a super user for login.

Steps:

1. Input the super user name and password.

2. Confirm the password.

3. Optionally, check the checkbox **Enable Auto-login** to log into the software automatically.

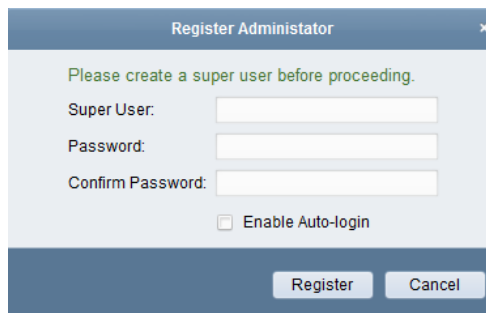4. Click **Register**. Then, you can log into the software as the super user.

Figure 17. 1 Register a Super User

Logging into the Software

When starting the NVMS7000 after registration, you can log into the client software with the registered user name and password.

Steps:

1. Input the user name and password you registered.

NOTE

If you forget your password, please click **Forgot Password** and remember the encrypted string in the pop-up window. Contact your dealer and send the encrypted string to him to reset your password.

2. Optionally, check the checkbox **Enable Auto-login** to log into the software automatically.
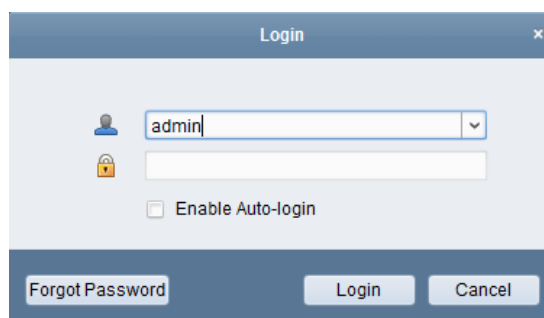
3. Click **Login**.

Figure 17. 2 User Login

After running the client software, a wizard will pop up to guide you to add the device and operate some basic settings. For detailed configuration about the wizard, please refer to the *Quick Start Guide of NVMS7000*.

The following figure shows the main interface after accessing to the software:
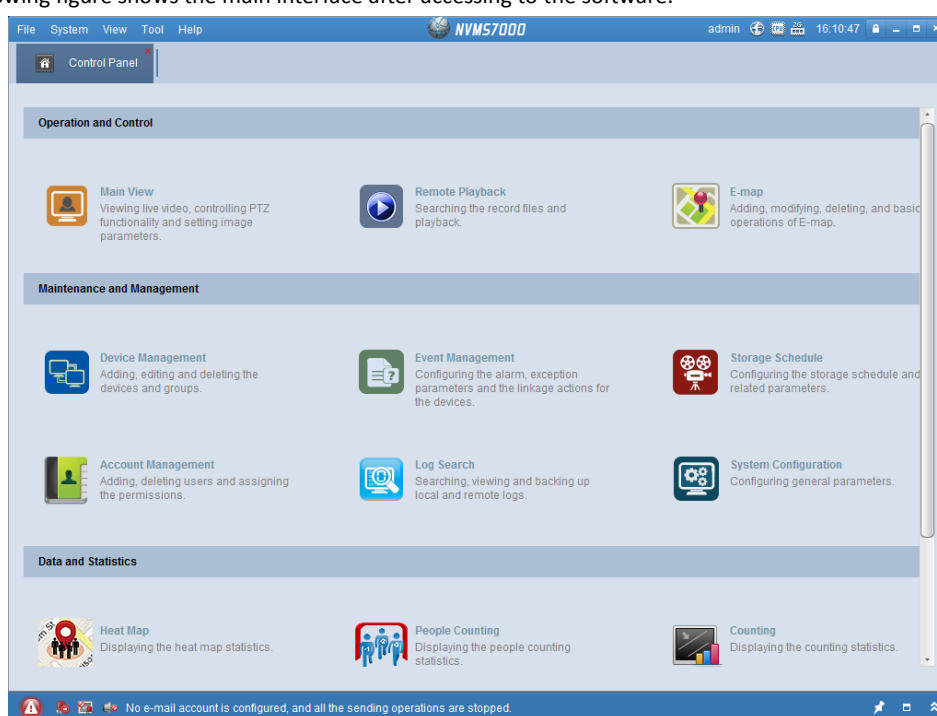

Figure 17. 3 Control Panel

17.2 Adding the NVR to the Client Software

Perform the following steps to enter the Device Adding interface:

1. Click the icon on the control panel,

   or click **Tools**->**Device Management** to open the Device Management page.

2. Click the **Server** tab.

3. Click **Encoding Device** to enter Encoding Device Adding interface.
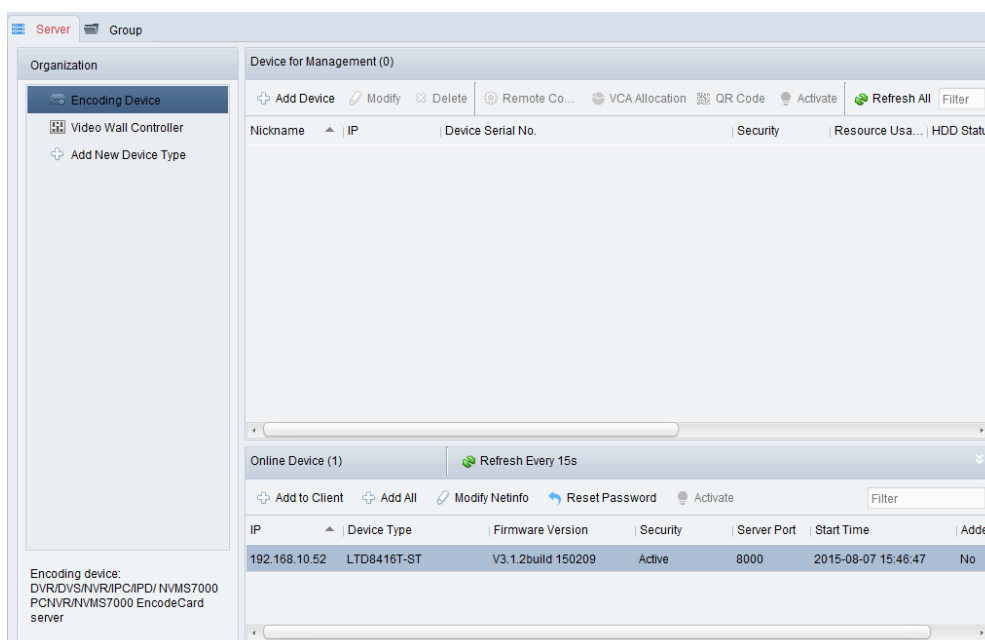
Figure 17. 4 Add Encoding Device

4. Click **Add Device** to open the device adding dialog box.
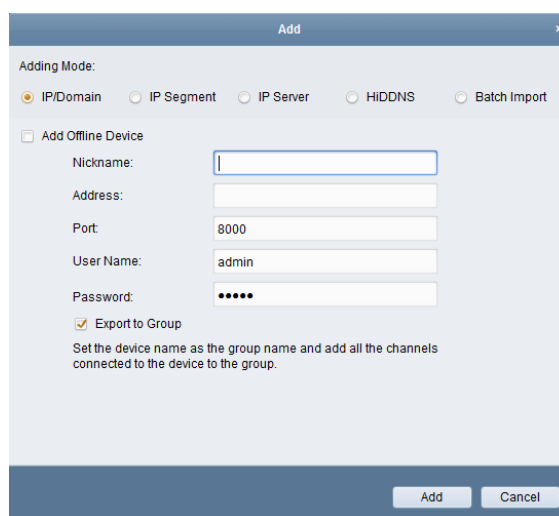
Figure 17. 5 Add Device

You can add the NVR by IP/Domain, IP Segment, IP Server or HiDDNS. You can also add the NVR by searching the online device. Please refer to the User Manual of NVMS7000 for detailed instructions. The following section introduces the adding device by IP/Domain as the example.

5. Select **IP/Domain** as the adding mode.
6. Input the required information.

    Nickname: Edit a name for the device as you want.

    Address: Input the device's IP address or domain name.

Port: Input the device port No.. The default value is *8000*.

User Name: Input the device user name. By default, the user name is *admin*.

Password: Input the device 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. 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.*

7. Optionally, you can check the checkbox **Export to Group** to create a group by the device name. All the channels of the device will be imported to the corresponding group by default.

NOTE

NVMS7000 also provides a method to add the offline devices. Check the checkbox **Add Offline Device**, input the required information and the device channel number and alarm input number, and then click **Add**. When the offline device comes online, the software will connect it automatically.

8. Click **Add** to add the device.

Nickname ▲	IP	Device Serial No.	Security	Resource Usa...	HDD Status	Recording Statu
LTN07256-R	192.168.1.95	1620151022CCRR531014776WCVU	Weak	🌐	⌂	🗄
CMIP8912	192.168.1.96	CMIP891220141028CCWR486204908	Weak	🌐	⌂	🗄

Figure 17. 6 List of Successfully Added Device

17.3 Configuring the Video Wall

Steps:

1. Click the [icon] icon on the control panel to enter the video wall configuration and operation interface.
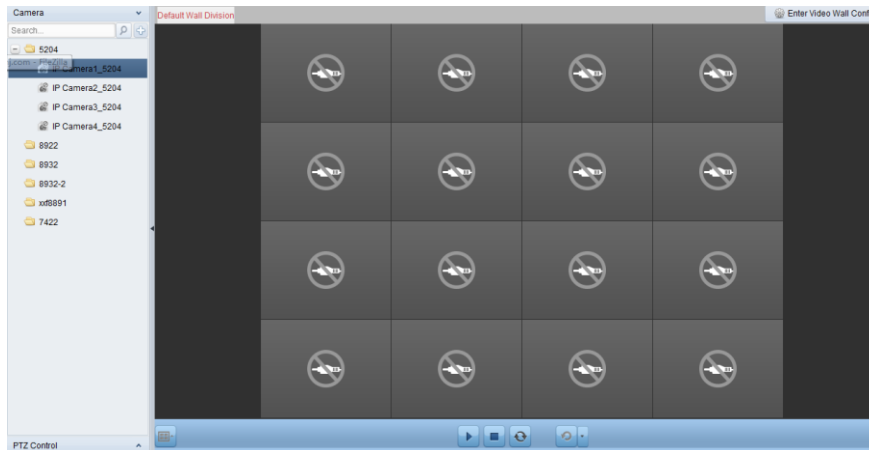
Figure 17. 7 List of Successfully Added Device

2. Click **Enter Video Wall Config** to enter the decoding device and video wall configuration interface.

3. A default video wall view with the window division of 4*4 is provided. You can edit the default video wall or add a new video wall as desired.

4. Click-and-drag the decoding output on the left-side list to the display window of video wall, to configure the one-to-one correspondence. You can also click and hold the *Ctrl* or *Shift* key to select multiple outputs and then drag them to the video wall for configuring linkage in batch. You can click ▣ in the upper-right corner of the display window to release the linkage.

NOTE

● Up to 4 video walls can be added to the client software.

● The total number of the display windows of the video wall should be no more than 100.

● The ranges of the row number and column number are both between 1 and 10.
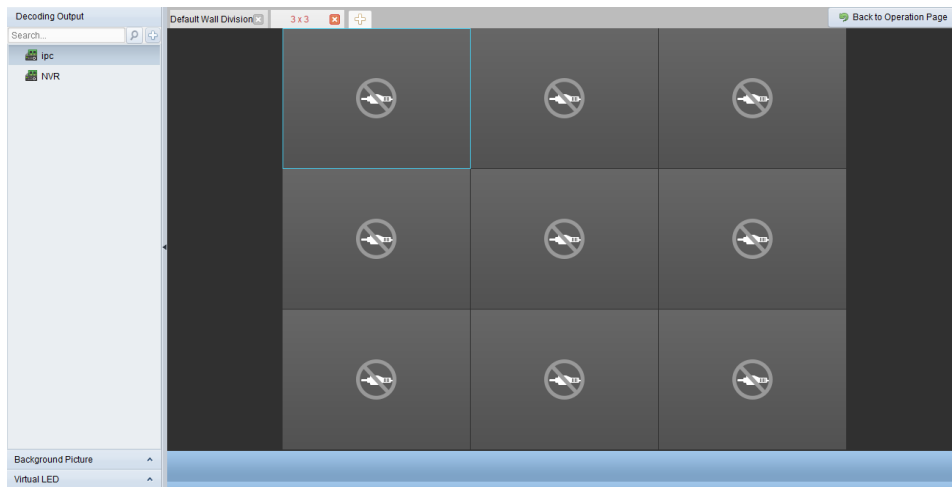
Figure 17. 8 Video Wall Configuration

17.4 Decoding and Displaying Video on Video Wall

Steps:

1. Click **Back to Operation Page** to go back to the Video Wall Operation interface.

2. Click-and-drag the camera under the NVR on the left-side list to the display window of video wall. The video stream from the camera will be decoded and displayed on the video wall. You can also select a window and then double-click a camera to decode and display the video.
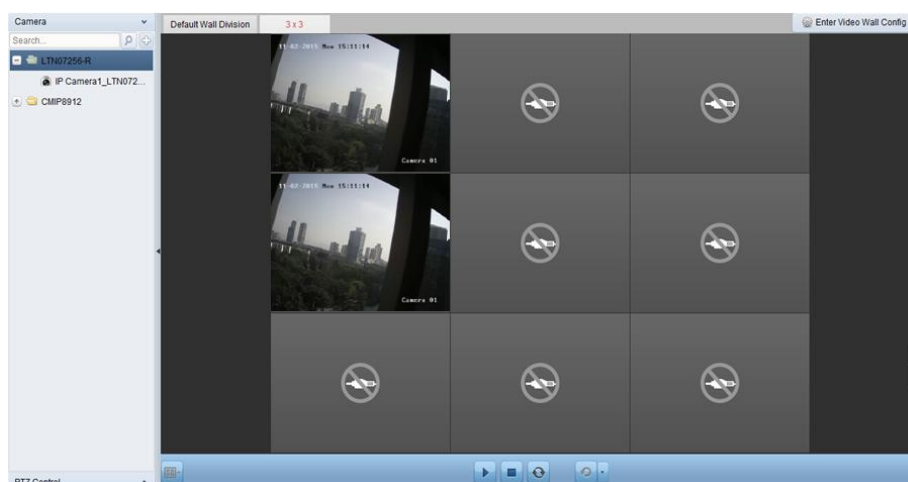
Figure 17. 9 Video Wall Configuration

3. You can use the toolbar at the bottom of the window and the right-click menu to the stop/stop decoding, switch window-division mode, set window display layer, etc.
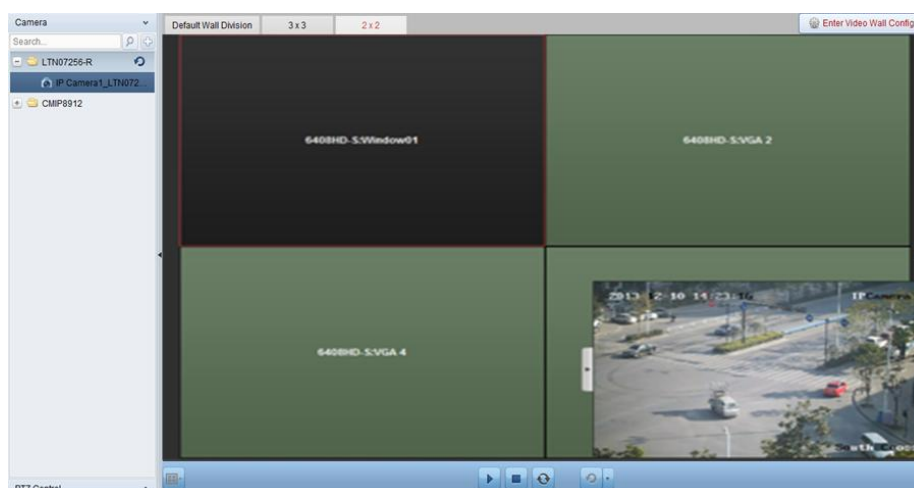
Figure 17. 10 Displaying Video on Video Wall

17.5 Operating Windowing and Roaming on Video Wall

Purpose:

Windowing is to open a new window on the screen(s). The window can be within a screen or span multiple screens. You can move the playing window within the video wall as desired and this function is called roaming.

Steps:

1. Click-and-drag on a screen which links to a decoding output to open a window. The window can be within a screen or span multiple screens. If you want to open a window on the opened window, click-and-drag and hold the *Ctrl* key to create one.

Figure 17. 11 Windowing on Video Wall

2. You can move the window when the cursor becomes ![icon] and adjust its size when the cursor becomes directional arrow. You can also hold the *Shift* key to scale the window in proportion.
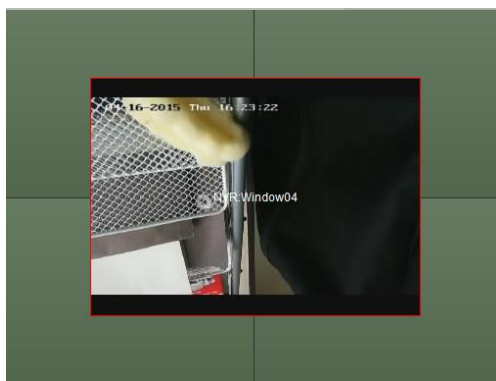
3. During moving the window, the dotted borders will display. The window will be adjusted to align with the borders if it is moved to the location near the dotted borders.

Figure 17. 12 Roaming on Video Wall

4. Double-click the window and it will enlarge to fill the spanning screens and display on the top layer. You can double-click again to restore.

Figure 17. 13 Window Enlarging

![NOTE icon]
NOTE

Please refer to the User Manual of NVMS7000 for more detailed instructions of video wall operation.

Chapter 18   Access by Web Browser

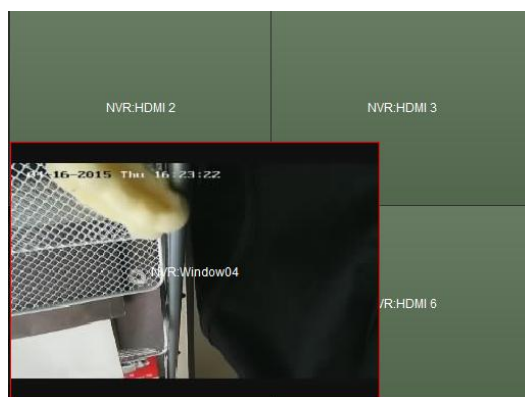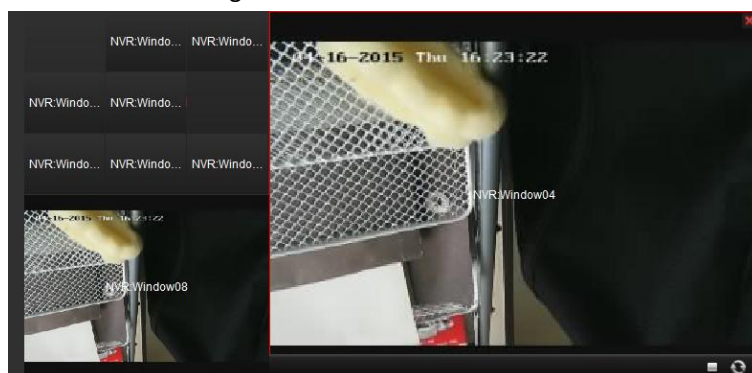You shall acknowledge that the use of the product with Internet access might be under network security risks. For avoidance of any network attacks and information leakage, please strengthen your own protection. If the product does not work properly, please contact with your dealer or the nearest service center.

18.1 Logging In

You can get access to the device via web browser. You may use one of the following listed web browsers: Internet Explorer 6.0, Internet Explorer 7.0, Internet Explorer 8.0, Internet Explorer 9.0, Internet Explorer 10.0, Apple Safari, Mozilla Firefox, and Google Chrome. The supported resolutions include 1024*768 and above.

Steps:

1.   Open web browser, input the IP address of the device and then press Enter.

2.   Login to the device.

●   If the device has not been activated, you need to activate the device first before login.

Figure 18. 1 Setting Admin Password

1)   Set the password for the admin user account.

2)   Click **OK** to login to the device.

⚠ **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.*

●   If the device is already activated, enter the user name and password in the login interface, and click
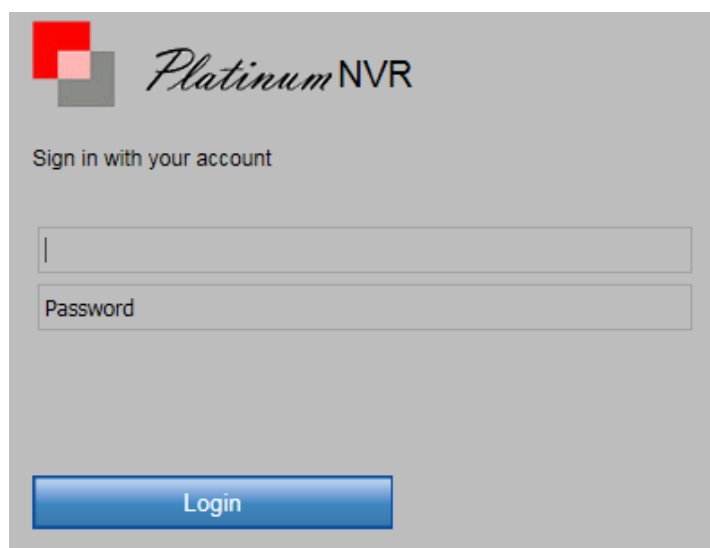
the **Login** button.

Figure 18. 2 Logging In

3. Install the plug-in before viewing the live video and managing the camera. Please follow the installation prompts to install the plug-in.

You may have to close the web browser to finish the installation of the plug-in.

18.2 Live View

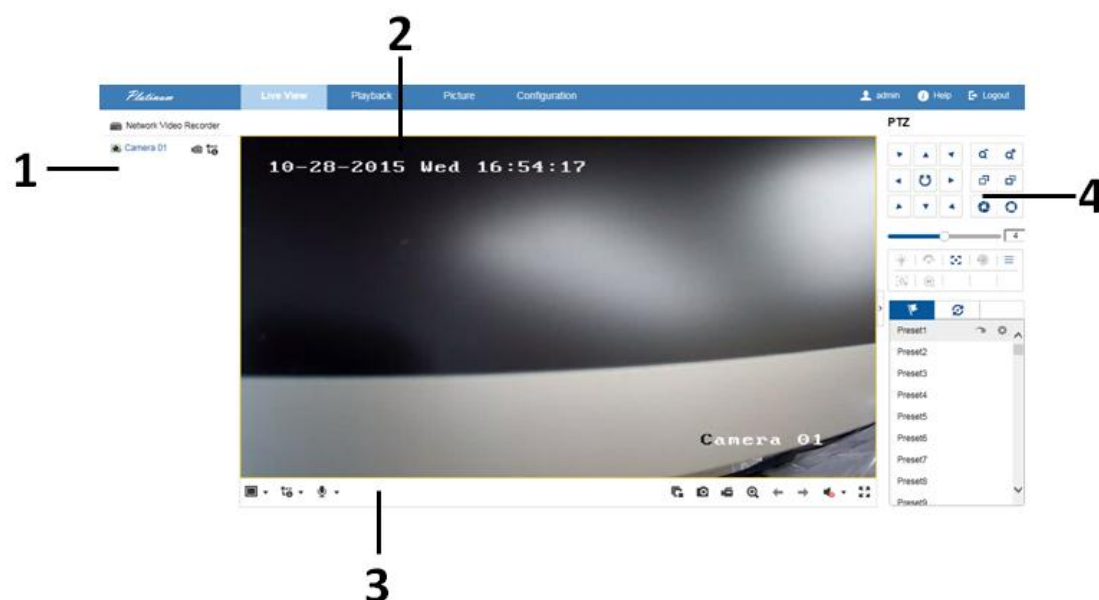The live view interface appears by default when you log in the device.

Figure 18. 3 Live View

The live view interface may differ according to different models.

Table 18. 1 Description of Live View Interface

No.	Name	Description
1	Channel List	Displays the list of channels and the playing and recording status of each channel.
2	Live View Window	Displays the image of channel, and multi-window division is supported.
3	Play Control Bar	Play control operations are supported.
4	PTZ Control	Pan, tilt, zoom operations are supported, as well as preset editing and calling. NOTE PTZ function can only be realized if the connected camera supports PTZ control.

Start Live View

Steps:

1. In the live view window, select a playing window by clicking the mouse.

2. Double click a camera from the device list to start the live view.

3. You can click the [icon] button on the toolbar to start the live view of all cameras on the device list.

    Refer to the following table for the description of buttons on the live view window:

Table 18. 2 Description of Live View Toolbar

Icon	Description	Icon	Description
[icon]	Select the window-division mode	[icon]	Open/Close audio
[icon]	Start/Stop all live view	[icon]	Start/Stop two-way Audio
[icon]	Capture pictures in the live view mode	[icon]	Adjust volume
[icon]	Start/Stop all recording	[icon]	Enable/Disable digital zoom
[icon]	Previous/Next page	[icon]	Full screen
[icon]	Select different stream type for live view by clicking the icon [icon] : live view in main stream; [icon] : live view in sub stream; [icon] :live view in transcoded stream.		

18.3 Recording

Before you start

Make sure the device is connected with HDD or network disk, and the HDD or network disk has been initialized

for the first time to use.

Two recording types can be configured: Manual and Scheduled. The following section introduces the configuration of scheduled recording.

Steps:

1. Click **Configuration> Storage> Schedule Settings** to enter Record Schedule settings interface.

2. Select the camera to configure the record schedule.

3. Check the checkbox of **Enable** to enable recording schedule.
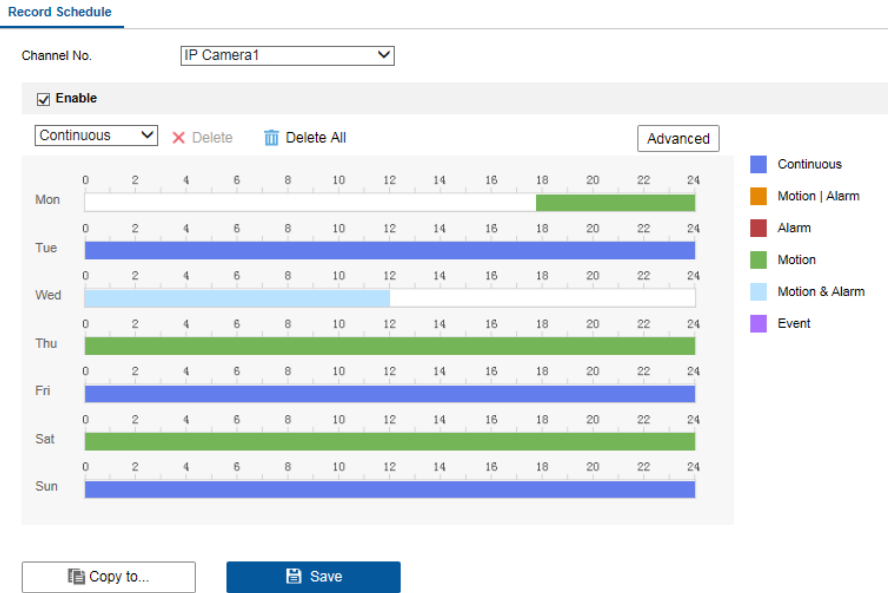
Figure 18. 4 Record Schedule Settings

4. Choose the day in a week configure the recording schedule.

    1) Click a day to set the start time and end time for recording.
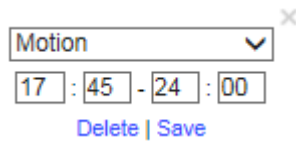
Figure 18. 5 Set Start/Stop Time

    2) Select the **Record Type** for the period. The record type can be Schedule, Motion, Alarm, Motion & Alarm, Motion | Alarm and Event.

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

    4) Click the icon of the day to copy the settings of current day to other days of the week if required.
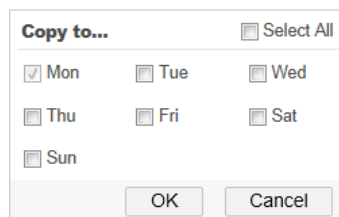
Figure 18. 6 Copy Settings

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

5. Click **Advanced** to configure advanced record parameters**.**
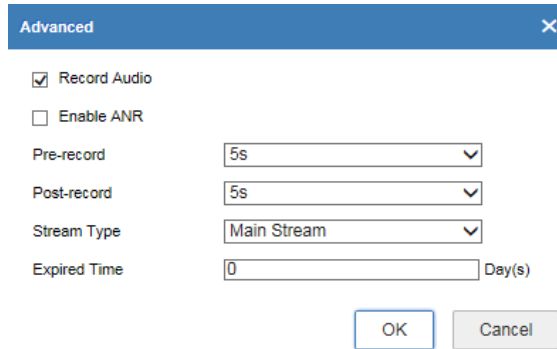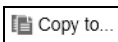
Figure 18. 7 Advanced Settings

6. You can click [Copy to...] to configure advanced record parameters to copy the schedule of current

camera to other cameras.

7. Click **Save** to activate the above settings.

18.4 Playback
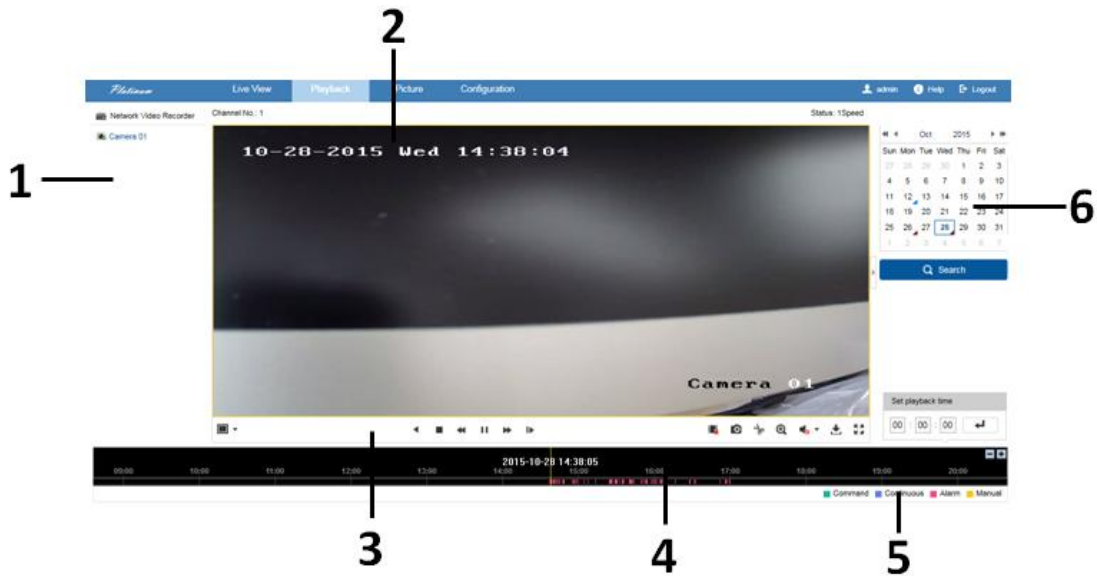
Figure 18. 8 Playback

The playback interface may differ according to different models.

Table 18. 3 Description of Playback Interface

No.	Name	Description
1	Channel List	Displays the list of channels and the playing status of each channel.

2	Playback Window	Displays the image of channel.
3	Play Control Bar	Play control operations are supported.
4	Time Line	Displays the time bar and the records marked with different colors.
5	Recording Type	Show the icons of different recording types.
6	Calendar	You can select the date to play the video files.

Start Playback

Steps:

1. Click **Playback** on the menu bar to enter playback interface.
2. Click the camera from the device list for playback.
3. Select the date from the calendar and click **Search**.
4. Click the **Play** button to play the video file searched on the current date.
5. Use the buttons on the toolbar to operate in playback mode.

Table 18. 4 Description of Playback Toolbar

Button	Description	Button	Description
▶ / ‖	Play/Pause	■	Stop
◀◀	Speed down	▶▶	Speed up
‖▶	Play by single frame	◎	Capture
🎞	Stop all playback	⬇	Download
✂ / ✂	Start/Stop video clipping	🔇 / 🔊	Open/Close audio
⤢	Full screen	◀	Reverse playback
⟲ ▾	Transcoded Playback		

6. You can drag the progress bar with the mouse to locate the exact playback point. You can also input the time in the textbox [00 : 00 : 00] and click [↵] button to locate the playback point.

The color of the video on the progress bar stands for the different video types.

■ Command ■ Schedule ■ Alarm ■ Manual
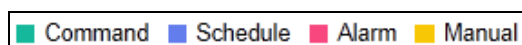
Appendix

Specifications

Model		LTN07256-R
Video/Audio input	IP video input	256-ch
		Up to 8MP resolution
	Two-way audio	2-ch, RCA (2.0 Vp-p, 1kΩ)
Network	Incoming bandwidth	640Mbps, or 400Mbps (when RAID is enabled)
	Outgoing bandwidth	400Mbps
	Remote connection	256
Video/Audio output	Recording resolution	8MP/6MP/5MP/3MP/1080P/UXGA/720P/VGA/4CIF/DCIF/2CIF/CIF/ QCIF
	HDMI1/VGA output resolution	1-ch, 1920 × 1080P /60Hz, 1600 × 1200 /60Hz, 1280 × 1024 /60Hz, 1280 × 720 /60Hz, 1024 × 768 /60Hz
	HDMI2 output	1-ch, 1920 × 1080P /60Hz, 1600 × 1200 /60Hz, 1280 × 1024 /60Hz, 1280 × 720 /60Hz, 1024 × 768 /60Hz
	HDMI output (on HDMI output extension board)	12-ch(for /H and /H/I models only), 1920 × 1080P /60Hz, 1600 × 1200 /60Hz, 1280 × 1024 /60Hz, 1280 × 720 /60Hz, 1024 × 768 /60Hz
	HDMI output (on x86 board)	4-ch, 4096 × 2304@24Hz, 2560 × 1600@60Hz, 1920 × 1080P /60Hz, 1600 × 1200 /60Hz, 1280 × 1024 /60Hz, 1280 × 720 /60Hz, 1024 × 768 /60Hz
	VGA output (on x86 board)	1-ch, 1920 × 2000@60Hz, 1920 × 1080P /60Hz, 1600 × 1200 /60Hz, 1280 × 1024 /60Hz, 1280 × 720 /60Hz, 1024 × 768 /60Hz
	LCD Screen	Available for /H and /H/I models only
	Audio output	2-ch, RCA (2.0Vp-p, 1KΩ)
Decoding	Live view / Playback resolution	8MP/6MP/5MP/3MP/1080P/UXGA/720P/VGA/4CIF/DCIF/2CIF/CIF/ QCIF
	Synchronous playback	16-ch
	HDMI outputs (HDMI Output Extension Board)	12 HDMI outputs for /H and /H/I models, 1920 × 1080P /60Hz, 1600 × 1200 /60Hz, 1280 × 1024 /60Hz, 1280 × 720 /60Hz, 1024 × 768 /60Hz
	Capability	44-ch@1080P
Hard disk	SATA	16 SATA interfaces for 16 HDDs
	miniSAS (Optional)	1 miniSAS interface
	Capacity	Up to 6TB capacity for each HDD
Disk array	Array type	RAID0, RAID1, RAID5, RAID10
	Number of arrays	16
External interface	Network interface	8, RJ-45 10 /100 /1000 Mbps self-adaptive Ethernet interface
	Optic fiber interface	4, 1000 Mbps optic fiber interface
	Serial interface	1×RS-232; 5× RS-485; 1× Keyboard
	USB interface	Front panel: 2 × USB 2.0; Rear panel: 4 × USB 3.0
	Alarm in/out	16 / 8
General	Power supply	100 ~ 240 VAC, 50 ~ 60 Hz
	Max. Power	600 W
	Consumption (without hard disk)	≤ 120 W
	Working temperature	-10ºC ~ +55ºC (14ºF ~ 131ºF)
	Working humidity	10 % ~ 90 %
	Chassis	19-inch rack-mounted 3U chassis
	Dimensions(W × D × H)	442 × 494 ×146 mm (17.4" ×19.4"× 5.7")
	Weight(without hard disk)	≤ 17.3Kg (38.1 lb)

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:** Acronym for Hard Disk Drive. A storage medium which stores digitally encoded data on platters with magnetic surfaces.

- **DHCP:** Dynamic Host Configuration Protocol (DHCP) is a network application protocol used by devices (DHCP clients) to obtain configuration information for operation in an Internet Protocol network.

- **HTTP:** Acronym for Hypertext Transfer Protocol. A protocol to transfer hypertext request and information between servers and browsers over a network

- **PPPoE:** PPPoE, Point-to-Point Protocol over Ethernet, is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with ADSL services where individual users connect to the ADSL transceiver (modem) over Ethernet and in plain Metro Ethernet networks.

- **DDNS:** Dynamic DNS is a method, protocol, or network service that provides the capability for a networked device, such as a router or computer system using the Internet Protocol Suite, to notify a domain name server to change, in real time (ad-hoc) the active DNS configuration of its configured hostnames, addresses or other information stored in DNS.

- **Hybrid DVR:** A hybrid DVR is a combination of a DVR and NVR.

- **NTP:** Acronym for Network Time Protocol. A protocol designed to synchronize the clocks of computers over a network.

- **NTSC:** Acronym for National Television System Committee. NTSC is an analog television standard used in such countries as the United States and Japan. Each frame of anNTSC signal contains 525 scan lines at 60Hz.

- **NVR:** Acronym for Network Video Recorder. An NVR can be a PC-based or embedded system used for centralized management and storage for IP cameras, IP Domes and other DVRs.

- **PAL:** Acronym for Phase Alternating Line. PAL is also another video standard used in broadcast televisions systems in large parts of the world. PAL signal contains 625 scan lines at 50Hz.

- **PTZ:** Acronym for Pan, Tilt, Zoom. PTZ cameras are motor driven systems that allow the camera to pan left and right, tilt up and down and zoom in and out.

- **USB:** Acronym for Universal Serial Bus. USB is a plug-and-play serial bus standard to interface devices to a host computer.

Troubleshooting

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

  Possible Reasons

  a)   No VGA or HDMI^{TM} connections.

  b)   Connection cable is damaged.

  c)Input mode of the monitor is incorrect.

  Steps

    1. Verify the device is connected with the monitor via HDMI^{TM} or VGA cable.

       If not, please connect the device with the monitor and reboot.

    2. Verify the connection cable is good.

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

    3. Verify Input mode of the monitor is correct.

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

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

       If it is solved, finish the process.

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

- **There is an audible warning sound "Di-Di-Di-DiDi" after a new bought NVR starts up.**

  Possible Reasons

  a)   No HDD is installed in the device.

  b)   The installed HDD has not been initialized.

  c)The installed HDD is not compatible with the NVR or is broken-down.

  Steps

    1. Verify at least one HDD is installed in the NVR.

       1) If not, please install the compatible HDD.

       NOTE

          Please refer to the "Quick Operation Guide" for the HDD installation steps.

       2) If you don't want to install a HDD, select "Menu>Configuration > Exceptions", and uncheck the Audible Warning checkbox of "HDD Error".

    2. Verify the HDD is initialized.

       1) Select "Menu>HDD>General".

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

    3. 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", please replace the dedicated HDD according to the requirement.

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

       If it is solved, finish the process.

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

- **The status of the added IP camera displays as "Disconnected" when it is connected through Private Protocol. Select "Menu>Camera>Camera>IP Camera" to get the camera status.**

  Possible Reasons

  a) Network failure, and the NVR and IP camera lost connections.

  b) The configured parameters are incorrect when adding the IP camera.

  c)Insufficient bandwidth.

  Steps

  1. Verify the network is connected.

     1) Connect the NVR and PC with the RS-232 cable.

     2) Open the Super Terminal software, and execute the ping command. Input "ping IP" (e.g. ping 172.6.22.131).

        NOTE

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

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

  2. Verify the configuration parameters are correct.

     1) Select "Menu>Camera>Camera>IP Camera".

     2) Verify the following parameters are the same with those of the connected IP devices, including IP address, protocol, management port, user name and password.

  3. Verify the whether the bandwidth is enough.

     1) Select "Menu >Maintenance > Net Detect > Network Stat.".

     2) Check the usage of the access bandwidth, and see if the total bandwidth has reached its limit.

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

     If it is solved, finish the process.

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

- **The IP camera frequently goes online and offline and the status of it displays as "Disconnected".**

  Possible Reasons

  a) The IP camera and the NVR versions are not compatible.

  b) Unstable power supply of IP camera.

  c)Unstable network between IP camera and NVR.

  d) 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 firmware version of connected IP camera.

     2) Enter the System Info interface "Menu>Maintenance>System Info>Device Info", and view the firmware version of NVR.

  2. Verify power supply of IP camera is stable.

     1) Verify the power indicator is normal.

     2) When the IP camera is offline, please try the ping command on PC to check if the PC connects with the IP camera.

  3. Verify the network between IP camera and NVR is stable.

     1) When the IP camera is offline, connect PC and NVR with the RS-232 cable.

     2) Open the Super Terminal, use the ping command and keep sending large data packages to the connected IP camera, and check if there exists packet loss.

NOTE

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

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

4. Verify the switch is not flow control.

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

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

    If it is solved, finish the process.

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

- **No monitor connected with the NVR locally and when you manage the IP camera to connect with the device by web browser remotely, of which the status displays as Connected. And then you connect the device with the monitor via VGA or HDMI^TM interface and reboot the device, there is black screen with the mouse cursor.**
Connect the NVR with the monitor before startup via VGA or HDMI^TM interface, and manage the IP camera to connect with the device locally or remotely, the status of IP camera displays as Connect.
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.

NOTE

- The view settings can only be configured by the local operation of NVR.
- Different camera orders and window-division modes can be set for different output interfaces separately, and digits like "D1"and "D2" stands for the channel number, and "X" means the selected window has no image output.

3. Check if the fault is solved by the above steps.

    If it is solved, finish the process.

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

- **Live view stuck when video output locally.**
Possible Reasons:
a) Poor network between NVR and IP camera, and there exists packet loss during the transmission.
b) 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 is stuck, connect the RS-232 ports on PC and the rear panel of NVR with the RS-232 cable.
   2) Open the Super Terminal, and execute the command of "**ping** *192.168.0.0* **–l 1472 –f**" (the IP address may change according to the real condition), and check if there exists packet loss.

NOTE

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

2. Verify the 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.

If it is solved, finish the process.

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

- **Live view stuck when video output remotely via the Internet Explorer or platform software.**
  Possible Reasons:

  a) Poor network between NVR and IP camera, and there exists packet loss during the transmission.

  b) Poor network between NVR and PC, and there exists packet loss during the transmission.

  c) The performances of hardware are not good enough, including CPU, memory, etc..

  Steps:

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

     1) When image is stuck, connect the RS-232 ports on PC and the rear panel of NVR with the RS-232 cable.

     2) Open the Super Terminal, and execute the command of "**ping** *192.168.0.0* **–l 1472 –f**" (the IP address may change according to the real condition), and check if there exists packet loss.

     ![NOTE]

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

  2. Verify the network between NVR and PC is connected.

     1) Open the cmd window in the Start menu, or you can press "windows+R" shortcut key to open it.

     2) Use the ping command to send large 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 good enough.

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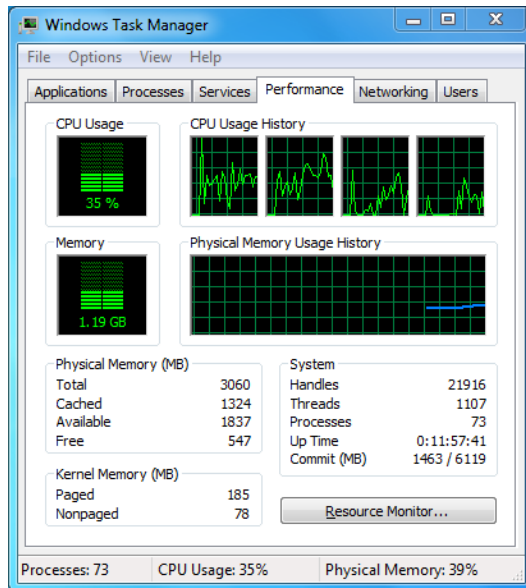
Windows task management interface

  - Select the "Performance" tab; check the status of the CPU and Memory.

- If the resource is not enough, please end some unnecessary processes.

4. Check if the fault is solved by the above steps.

   If it is solved, finish the process.

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

- **When using the NVR to get the live view audio, there is no sound or there is too much noise, or the volume is too low.**
  Possible Reasons:
  a) Cable between the pickup and IP camera is not connected well; impedance mismatches or incompatible.
  b) The stream type is not set as "Video & Audio".
  c) The encoding standard is not supported with NVR.
  Steps:
  1. Verify the cable between the pickup and IP camera is connected well; impedance matches and compatible.

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

  2. Verify the setting parameters are correct.

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

  3. Verify the audio encoding standard of the IP camera is supported by the NVR.

     NVR supports G722.1 and G711 standards, and if the encoding parameter of the input audio is not one of the previous two standards, you can log in the IP camera to configure it to the supported standard.

  4. Check if the fault is solved by the above steps.

     If it is solved, finish the process.

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

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

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

     NOTE

   Simultaneously press the **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. Verify the hardware can afford the playback.

     Reduce the channel number of playback.

     Select "Menu > Record > Encoding > Record", and set the resolution and bitrate to a lower level.
  4. Reduce the number of local playback channel.

     Select "Menu > Playback", and uncheck the checkbox of unnecessary channels.

5. Check if the fault is solved by the above steps.

   If it is solved, finish the process.

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

- **No record file found in the NVR local HDD, and prompt "No record file found".**

   Possible Reasons:

   a) The time setting of system is incorrect.

   b) The search condition is incorrect.

   c)The HDD is error or not detected.

   Steps:

   1. Verify the system time setting is correct.

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

   2. Verify the search condition is correct.

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

   3. Verify the HDD status is normal.

      Select "Menu > HDD > General" to view the HDD status, and verify the HDD is detected and can be read and written normally.

   4. Check if the fault is solved by the above steps.

      If it is solved, finish the process.

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