NETWORK VIDEO RECORDER

USER MANUAL – VERSION 1.04

About this Manual
This Manual is applicable to Network Video Recorder (NVR)

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

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 SCOPE PROTECTIVE & DATA SOLUTIONS 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 SCOPE PROTECTIVE & DATA SOLUTIONS, 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 SCOPE PROTECTIVE & DATA SOLUTIONS 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. SCOPE PROTECTIVE & DATA SOLUTIONS 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, SCOPE PROTECTIVE & DATA SOLUTIONS 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. SCOPE PROTECTIVE & DATA SOLUTIONS SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES. IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Regulatory Information

FCC Information

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

FCC Conditions

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

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

EU Conformity Statement

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2004/108/EC, the RoHS Directive 2011/65/EU.

2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsortedmunicipal 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 manufacturer.

Contents

1.0 Introduction 7
1.1 Front Panel 7
1.2 USB Mouse Operation 7
1.3 Input Method Description 8
1.4 Rear Panel 9
2.0 GETTING STARTED 10
2.1 Starting Up and Shutting Down the NVR 10
2.2 Setting Admin Password 11
2.3 Using the Wizard for Basic Configuration 12
2.3 Login and Logout 16
2.4 Adding and Connecting the IP Cameras 16
3.0 Live View 17
3.1 Introduction of Live View 17
3.2 Operations in Live View Mode 17
3.2.1 Using the Mouse in Live View 18
3.2.2 Quick Setting Toolbar in Live View Mode 19
3.3 Adjusting Live View Settings 22
3.4 Channel-zero Encoding 23
4.0 Recording Settings 23
4.1 Configuring Parameters 23
4.2 Configuring Recording Schedule 25
4.3 Configuring Motion Detection Recording 27
4.4 Configuring VCA Event Recording 29
4.5 Configuring Holiday Recording 30
4.6 Files Protection 31
4.6.1 Locking the Recording Files 31
5.0 Playback 34
5.1 Playing Back Record Files 34
5.1.1 Instant Playback 34
5.1.2 Playing Back by Normal Search 35
5.1.3 Playing Back by Event Search 37
5.1.4 Playing Back by Tag 38

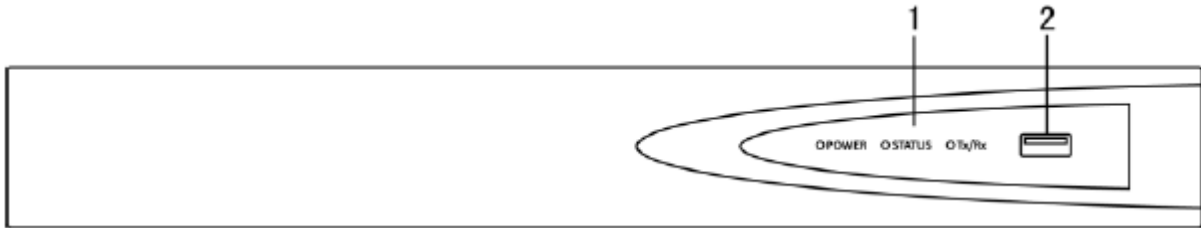
6.0 Backup 41
6.1 Backing up Record Files 41
6.1.1 Quick Export 41
6.1.2 Backing up by Normal Video Search 43
6.1.3 Backing up Video Clips 45
7.0 Alarm Settings 46
7.1 Setting Motion Detection Alarm 46
7.2 Detecting Video Loss Alarm 47
7.3 Detecting Video Tampering Alarm 48
7.4 Handling Exceptions Alarm 49
7.5 Setting Alarm Response Actions 50
8.0 VCA Alarm 52
8.1 Line Crossing Detection 52
8.2 Intrusion Detection 54
9.0 Network Settings 55
9.1 Configuring General Settings 55
9.2 Configuring Advanced Settings 56
9.2.1 PPPoE Settings 56
9.2.2 Configuring EZVIZ Cloud P2P 56
9.2.3 Configuring DDNS 57
9.2.4 Configuring NTP Server 60
9.2.5 Configuring Remote Alarm Host 60
9.2.6 Configuring Multicast 61
9.2.7 Configuring RTSP 61
9.2.8 Configuring Server and HTTP Ports 62
9.2.9 Configuring Email 62
9.2.10 Configuring NAT 64
9.3 Checking Network Traffic 67
9.4 Configuring Network Detection 67
9.4.1 Testing Network Delay and Packet Loss 68
9.4.2 Exporting Network Packet 68
9.4.3 Checking the Network Status 69
9.4.4 Checking Network Statistics 70
10.0 HDD Management 71
10.1 Initializing HDDs 71

10.2 Managing Network HDD 72
10.3 Managing HDD Group 74
10.3.1 Setting HDD Groups 74
10.3.2 Setting HDD Property 75
10.4 Configuring Quota Mode 76
10.5 Checking HDD Status 77
10.6 Configuring HDD Error Alarms 78
11.0 Camera Settings 79
11.1 Configuring OSD Settings 79
11.2 Configuring Privacy Mask 80
11.3 Configuring Video Parameters 81
12.0 NVR Management and Maintenance 82
12.1 Viewing System Information 82
12.2 Searching & Export Log Files 82
12.3 Importing/Exporting IP Camera Info 85
12.4 Importing/Exporting Configuration Files 85
12.5 Upgrading System 86
12.5.1 Upgrading by Local Backup Device 86
12.5.2 Upgrading by FTP 87
12.6 Restoring Default Settings 88
13.0 Others 88
13.1 Configuring RS-232 Serial Port 88
13.2 Configuring General Settings 89
13.3 Configuring DST Settings 90
13.4 Configuring More Settings for Device Parameters 90
13.5 Managing User Accounts 90
13.5.1 Adding a User 91
13.5.2 Deleting a User 94
13.5.3 Editing a User 95

1.0 Introduction

1.1 Front Panel

SW-0820154N & SW-0820158N Series



No.	Name		Description
1	Status Indicator	Power	Power indicator turns yellow when system is running.
		Status	Status indicator blinks red when data is being read from or written to HDD
		Tx/Rx	Tx/Rx indicator blinks yellow when network connection is functioning properly
2	USB Interface		Universal Serial Bus (USB) ports for additional devices such as USB Mouse and USB Hard Disk Drive (HDD

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:

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 zoon-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

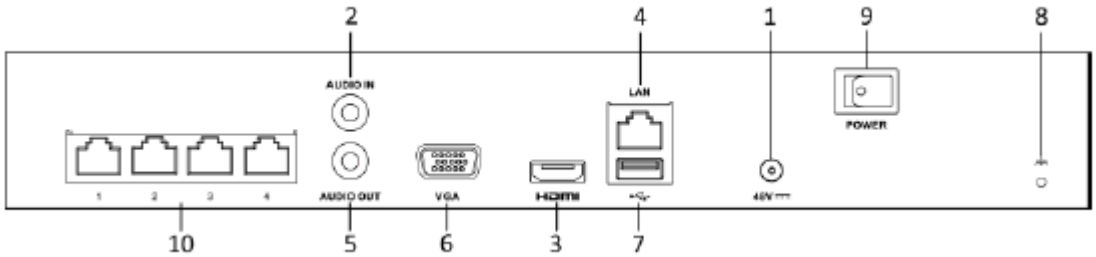
Description of the buttons on the soft keyboard:

Icon	Description	Icon	Description
0 ~ 9	Number	A ~ Z	English Letter
	Lowercase / Uppercase		Backspace
123/., ABC	Switch the Keyboard		Space
	Positioning the cursor		Exit
#+=	Symbols		Reserved

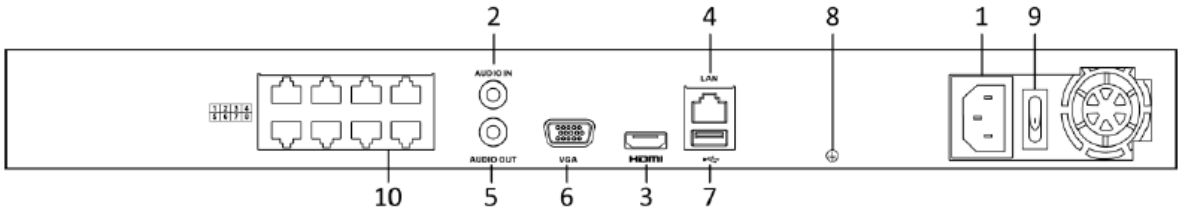
1.4 Rear Panel

The rear panel varies according to different models

SW-0820154N



SW-0820158N



No.	Item	Description
1	**Power Supply**	DC 48V power supply for SW-0820154N and AC 100~240V for SW-0820158N
2	**Audio In**	RCA connector for audio input
3	**HDMI Interface**	HDMI video output connector
4	**LAN Network Interface**	1 10/100/1000 Mbps self-adaptive Ethernet interface
5	**Audio Out**	RCA connector for audio output
6	**VGA Interface**	DB9 connector for VGA output. Display local video output and menu
7	**USB Interface**	Universal Serial Bus (USB) ports for additional devices such as USB mouse and USB Hard Disk Drive (HDD)
8	**Ground**	Ground (needs to be connected when NVR starts up)
9	**Power Switch**	Switch for turning on/off the device
10	**Network Interfaces with PoE function**	Network interfaces for the cameras and to provide power over Ethernet

2.0 GETTING STARTED

2.1 Starting Up and Shutting Down the NVR

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. Check the power supply is plugged into an electrical outlet. It is HIGHLY recommended that an Uninterruptible Power Supply (UPS) be used in conjunction with the device. The Power indicator LED on the front panel should be red, indicating the device gets the power supply.

2. Turn on the power switch on the rear panel if the device starts up for the first time, or press the button on the front panel. The Power indicator LED should turn blue indicating that the unit begins to start up.

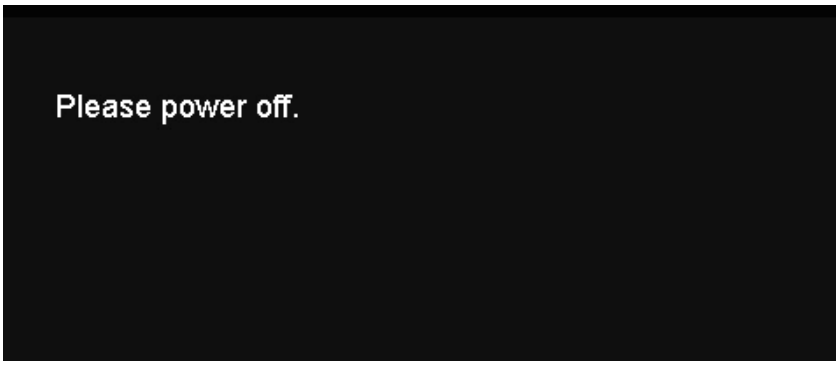
3. After startup, the Power indicator LED remains blue. A splash screen with the status of the HDD appears on the monitor. The row of icons at the bottom of the screen shows the HDD status. 'X' means that the HDD is not installed or cannot be detected.

Shutting down the NVR
There are two proper ways to shut down the NVR.

Steps:

1. Enter the Shutdown menu.
   Menu > Shutdown

2. Click the **Shutdown** button.
3. Click the **Yes** button.
4. Turn off the power switch on the rear panel when the attention pops up.

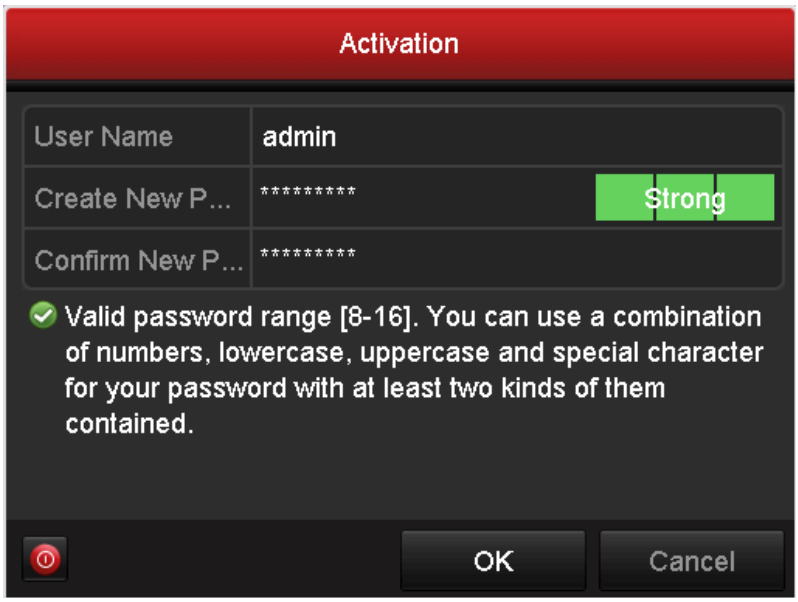


Rebooting the NVR
In the Shutdown menu, you can also reboot the NVR.
Steps:
1. Enter the **Shutdown** menu by clicking Menu > Shutdown.
2. Click the **Logout** button to lock the NVR or the **Reboot** button to reboot the NVR.

2.2 Setting Admin Password

For the first-time access, you need to activate the device by setting an admin password. No operation is allowed before activation.

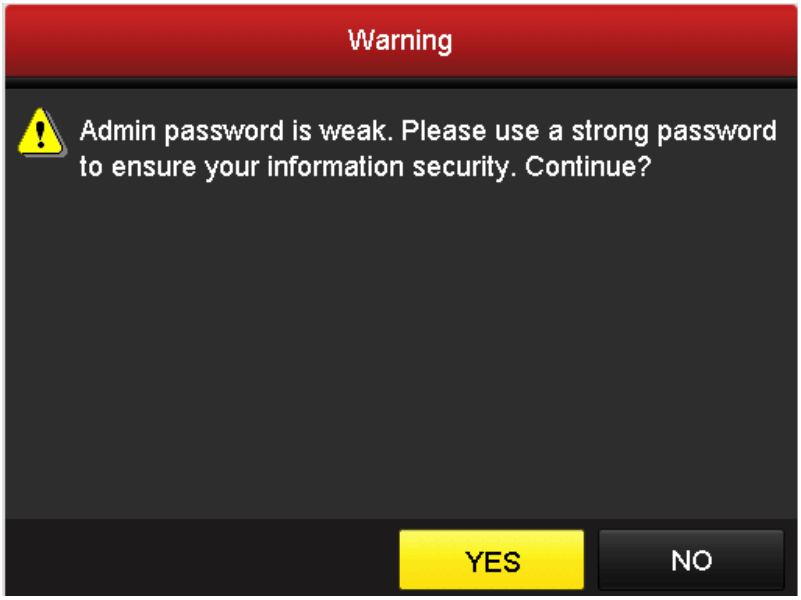
Steps:
1. Input the same password in the text field of **Create New Password** and **Confirm New Password**.



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

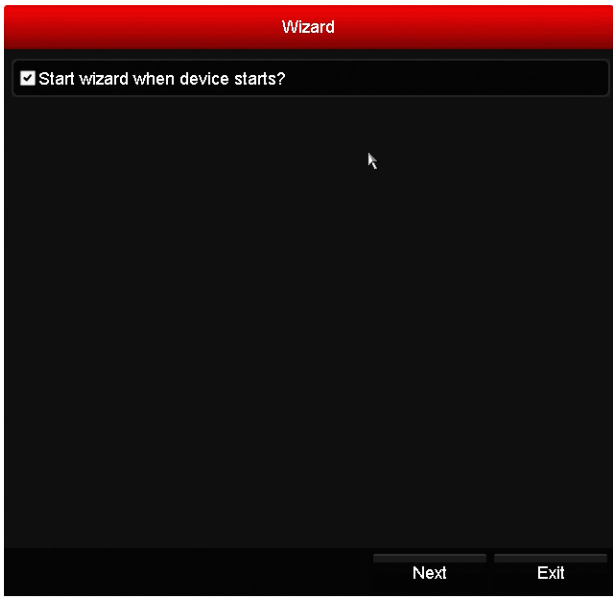
2. Click **OK** to save the password and activate the device.

Note: 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.



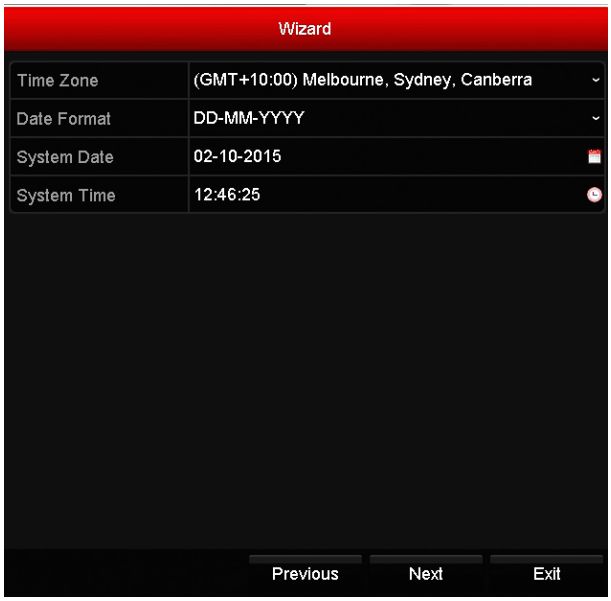
2.3 Using the Wizard for Basic Configuration

After admin password is set, the setup wizard pops up automatically. It can walk you through some basic settings of the NVR.

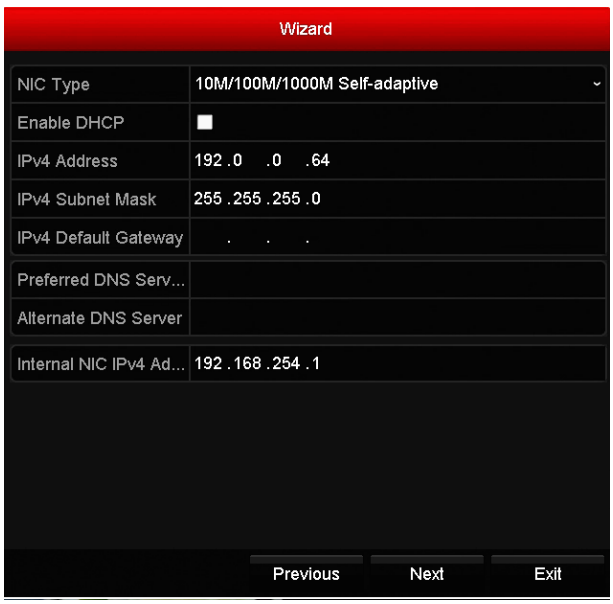


Steps:

1. If you don't want to use the setup wizard at that moment, click the **Exit** 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 the **Next** button to enter the **Date and Time Settings** interface.



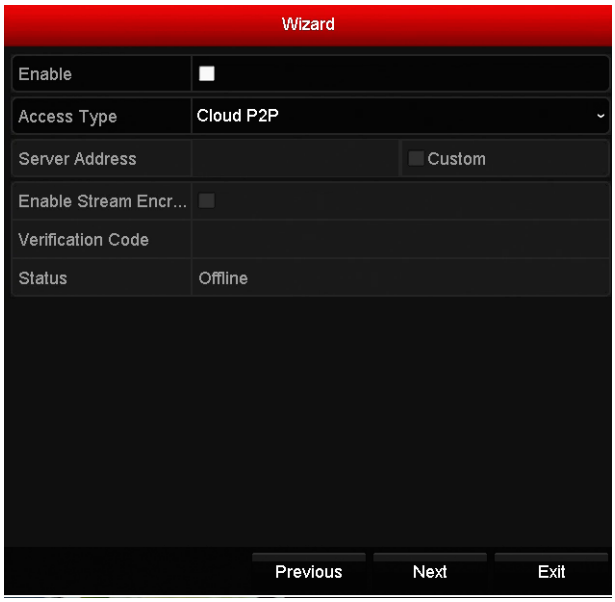
3. After the time settings, click **Next** button which takes you back to the **Basic Network Setup Wizard** interface.



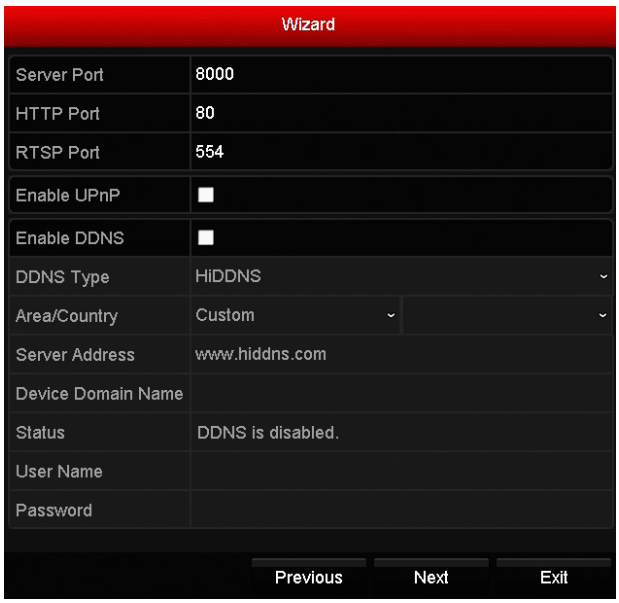
Note:

- one 10 /100 Mbps self-adaptive Ethernet interface for SW-0820154N & SW-0820158N series NVR;
- For the models have the PoE or built-in switch network interfaces, the internal NIC IPv4 address should be configured for the cameras connecting to the PoE or built-in switch network interface of the NVR.

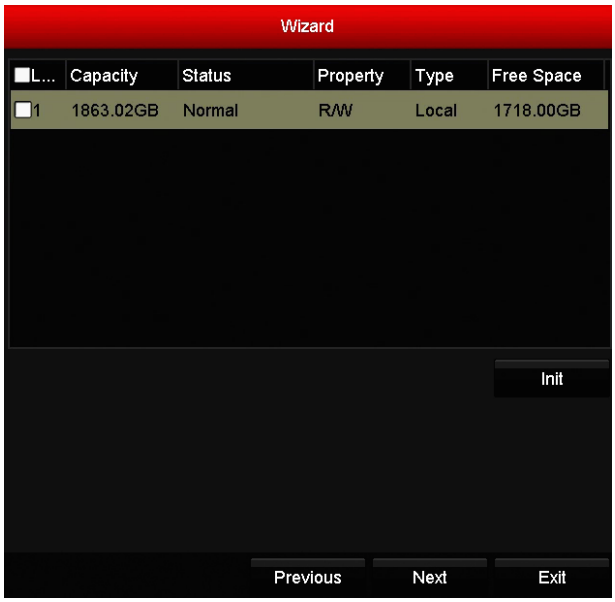
4. Click **Next** button after you configured the basic network parameters. Then you will enter the **EZVIZ Cloud P2P** interface. Configure the EZVIZ Cloud P2P according to your need.



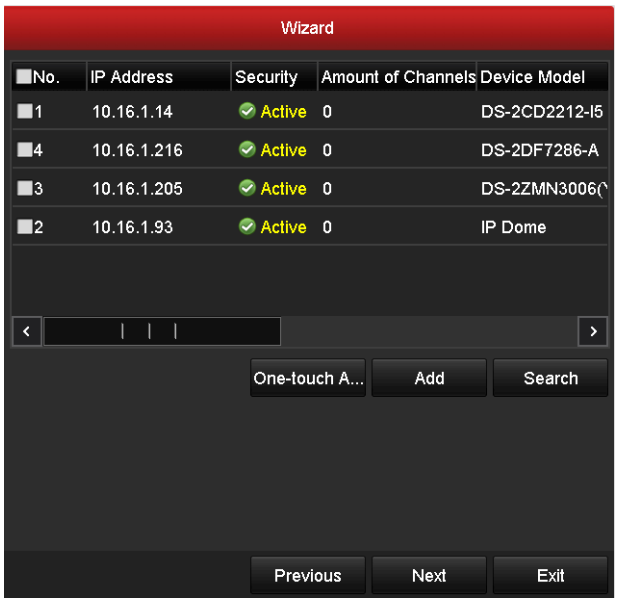
5. Click **Next** button to enter the **Advanced Network Parameter** interface. You can enable PPPoE, enable DDNS and set other ports according to your need.



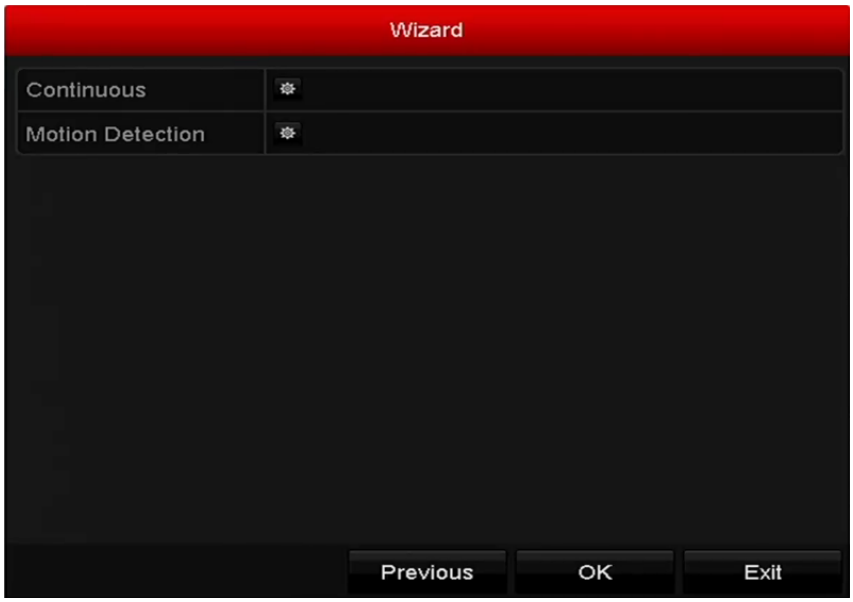
6. After configuration finishes, click **Next** button to enter **HDD Management** interface.



7. To initialize the HDD, click the **Init** button. Initialization removes all the data saved in the HDD.
8. Click **Next** button to enter the **IP Camera Management** 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.



10. Click **Next** button. Configure the recording for the searched IP Cameras.



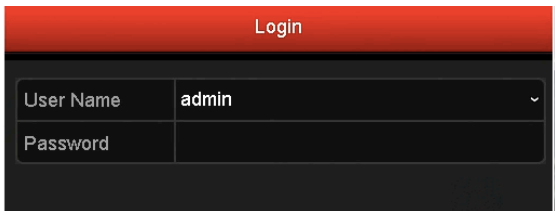
11. Click **OK** to complete the startup Setup Wizard.

2.3 Login and Logout

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

Steps:

1. Select the **User Name** in the dropdown list.



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

NOTE: The device gets locked for 60 seconds if the admin user performs 7 failed password attempts (5 attempts for the guest/operator).

2.4 Adding and Connecting the IP Cameras

Steps:

1. Plug in the IP camera into the PoE interface at the rear of the NVR with the Cat5e cable supplied
2. Once plugged in and the NVR is on wait 60seconds for the image to appear on screen.

Note: The PoE interfaces enables the NVR system to pass electrical power safely, along with data, on Ethernet cabling to the connected network cameras. The cameras are 'plug and play it's that simple.

3.0 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.

Icons	Description
	Alarm (video loss, video tampering, motion detection, sensor alarm or VCA alarm)
	Record (manual record, continuous record, motion detection , sensor alarm or VCA alarm triggered record)
	Alarm & Record
	Event/Exception (motion detection, sensor alarm, VCA alarm 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

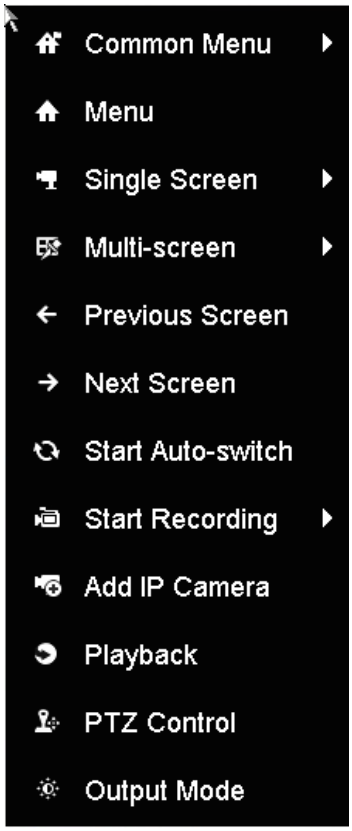
In live view mode, there are many functions provided. The functions are listed below.

• **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 onthe 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.

3.2.1 Using the Mouse 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
Output Mode	Four modes of output supported including Standard, Bright, Gentle and Vivid

- 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.



Note: The right-click menu varies according to different models, please refer to the actual GUI menu of the device.

3.2.2 Quick Setting Toolbar in Live View Mode

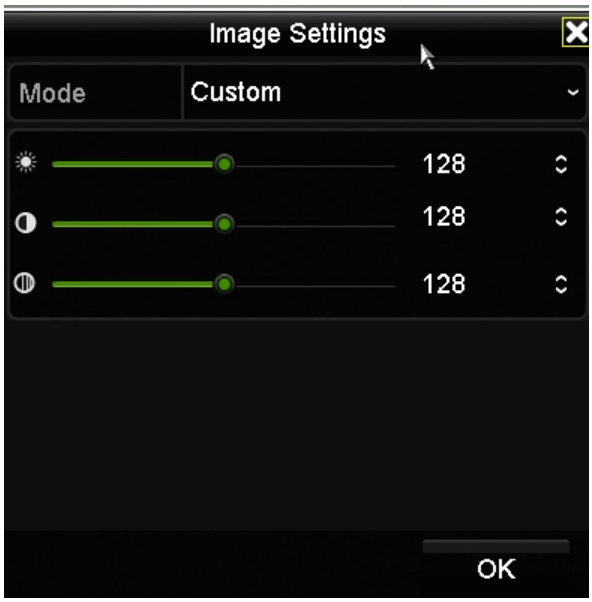
On the screen of each channel, there is a quick setting toolbar which shows when you single click the mouse in the corresponding screen.

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

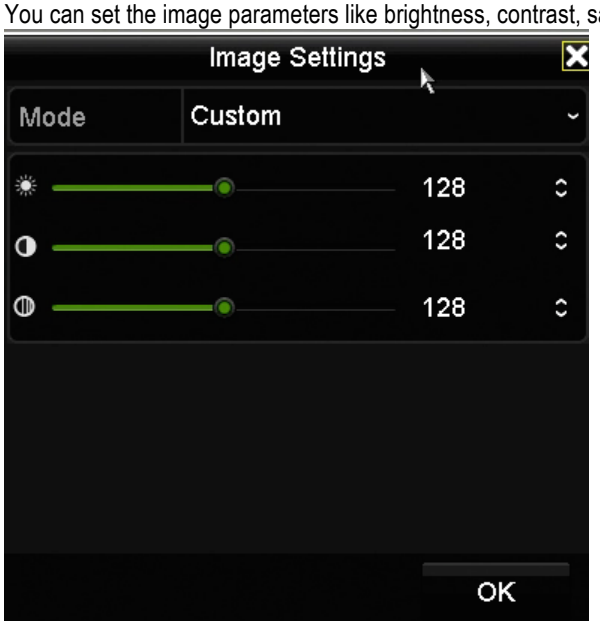

Instant Playback only shows the record in last five minutes. If no record is found, it means there is no record during the last five minutes.


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

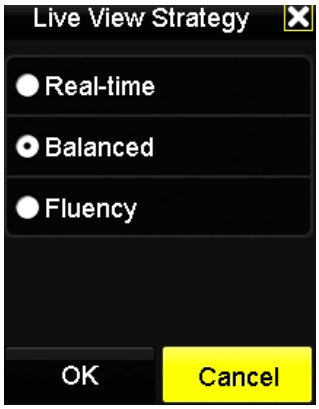

Image Settings icon can be selected to enter the Image Settings menu.



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



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



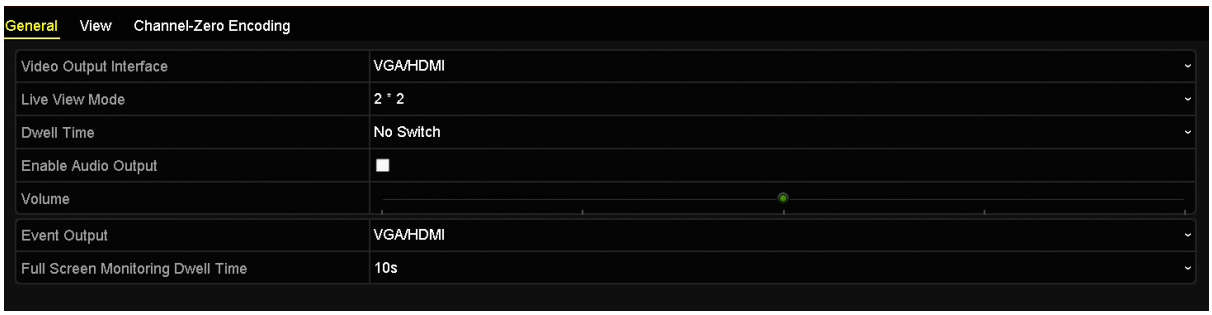
 Move the mouse onto the icon to show the real-time stream information, including the frame rate, bitrate, resolution and stream type.

3.3 Adjusting Live View Settings

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

Steps:

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



The settings available in this menu include:

• **Video Output Interface:** Designates the output to configure the settings for, and only VGA/ HDMITM is selectable by default.
• **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.
• **Volume:** Adjust the volume of live view, playback and two-way audio for the selected output interface.
• **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

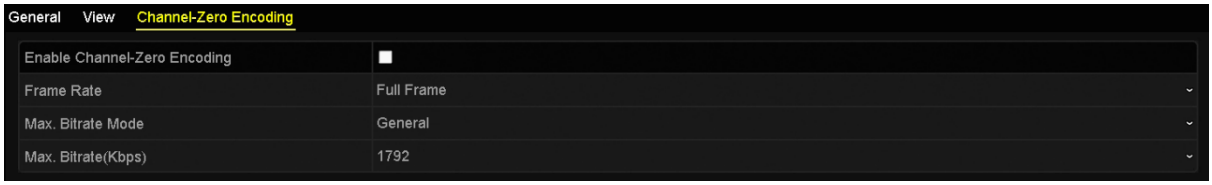
1) Select a **View** mode in 
2) Select the small window, and double-click on the channel number to display the channel on the window. If you do not want the camera to be displayed on the live view interface, click the corresponding  to stop it. You can also click  button to start live view for all the channels and click  to stop all the liveview.
3) Click the **Apply** button to save the setting.

3.4 Channel-zero Encoding

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

Steps:

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



3. Check the checkbox after **Enable Channel Zero Encoding.**
4. Configure the Frame Rate, Max. Bitrate Mode and Max. Bitrate.

After you set the Channel-Zero encoding, you can get a view in the remote client or web browser of 16 channels in one screen.

4.0 Recording Settings

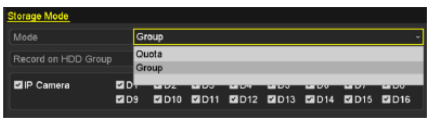
4.1 Configuring Parameters

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:

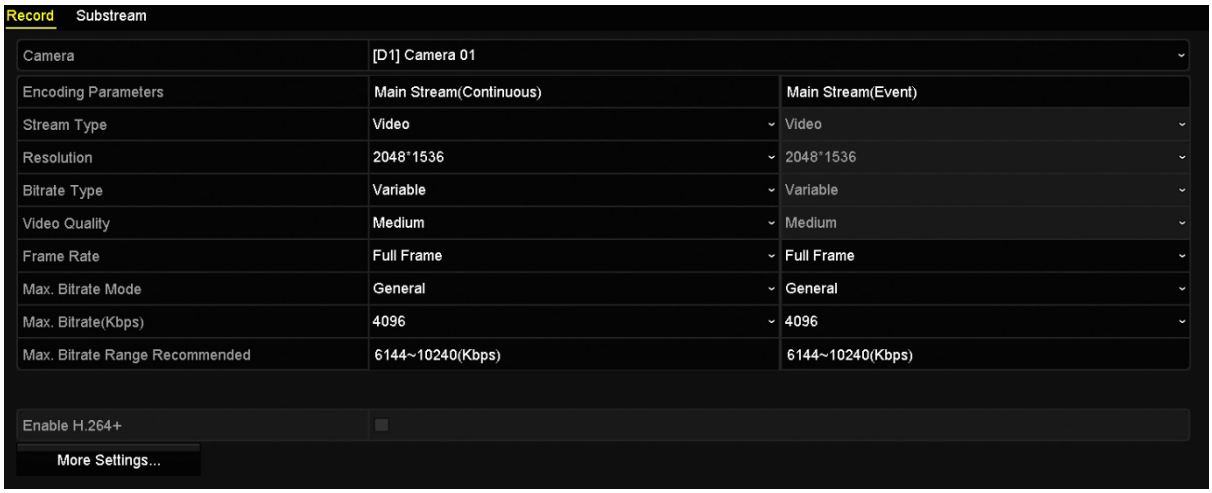
1. Make sure that the HDD has already been installed. If not, please install a HDD and initialize it. (Menu >HDD > General)

2. Check the storage mode of the HDD.
   2.1 Click **Advanced** to check the storage mode of the HDD.
   2.2 If the HDD mode is *Quota*, please set the maximum record capacity For detailed information, see *10.4 Configuring Quota Mode*.
   2.3 If the HDD mode is **Group**, you should set the HDD group. For detailed information, see *10.3.1 Configuring HDD Group for Recording*.



Steps:

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



2. Parameters Setting for Recording

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

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

NOTE: The function is only available for IP cameras which support H.264+ stream.

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

• **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.

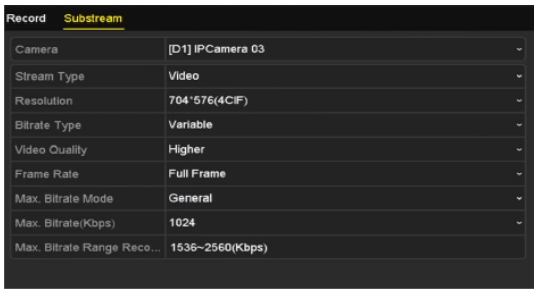
• **Record Audio:** Check the checkbox to enable or disable audio recording.
• **Video Stream:** Main stream and sub-stream are selectable for recording. When you select sub-stream, you can record for a longer time with the same storage space.

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

NOTE:

- The redundant record is to decide whether you want the camera to save the recording files in the redundant HDD. You must configure the redundant HDD in HDD settings. For detailed information, see *10.3.2 Setting HDD Property.*
- The parameters of Main Stream (Event) are read-only.

3. Parameters Settings for Sub-stream
3.1 Enter the Sub-stream tab page.



3.2 Configure the parameters of the camera.
3.3 Click **Apply** to save the settings.

4.2 Configuring Recording Schedule

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

Steps:

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

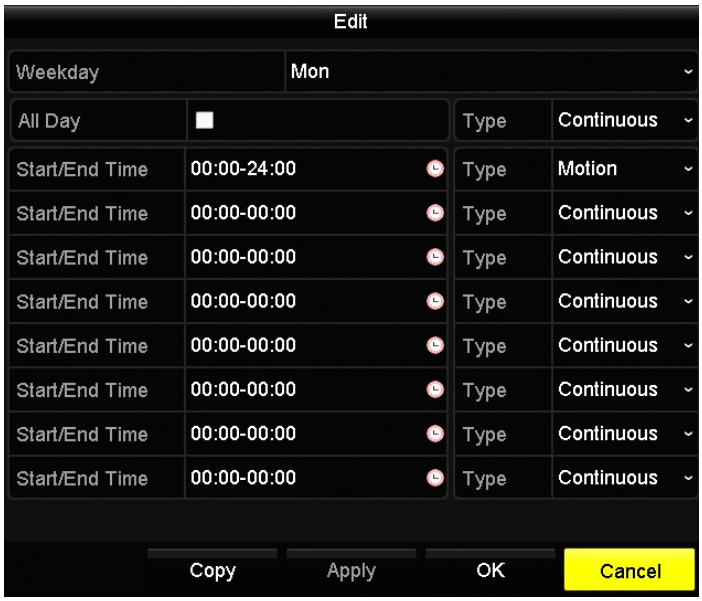
2. Configure Record Schedule
2.1 Select Record Schedule.

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.

2.2 Choose the camera you want to configure.
2.3 Select the check box after the **Enable Schedule** item.
2.4 Click **Edit** button or click on the color icon under the edit button and draw the schedule line on the panel.

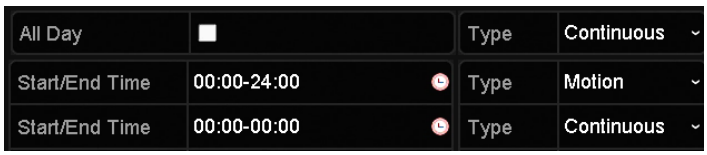
Edit the schedule:

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



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.



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 cannot be overlapped each other.

IV. Select the record type in the dropdown list.

- To enable Motion, Alarm, M | A (motion or alarm), M & A (motion and alarm) and VCA (Video Content Analysis) triggered recording and capture, you must configure the motion detection settings, alarm input settings or VCA settings as well. For detailed information, refer to *7.0 7.1, and 4.4*
- The VCA settings are only available to the smart IP cameras. Repeat the above edit schedule steps to schedule recording for other days in the week. You can click **Copy** to enter the Copy to interface to copy the schedule settings to other days

V. 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.

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

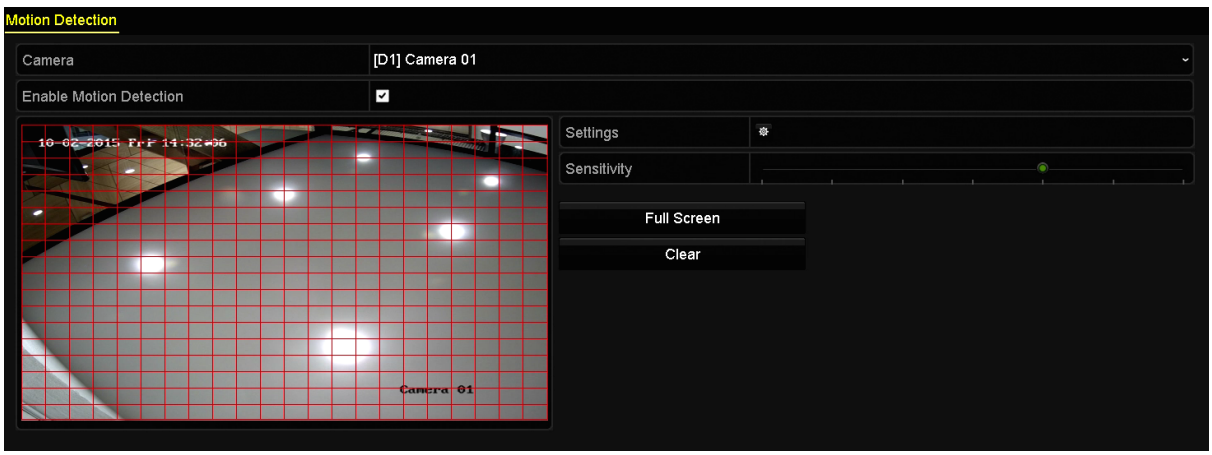
3. (Optional) If the settings can also be used to other channels, click **Copy**, and then choose the channel to which you want to copy.
4. Click **Apply** to save the settings.

4.3 Configuring Motion Detection Recording

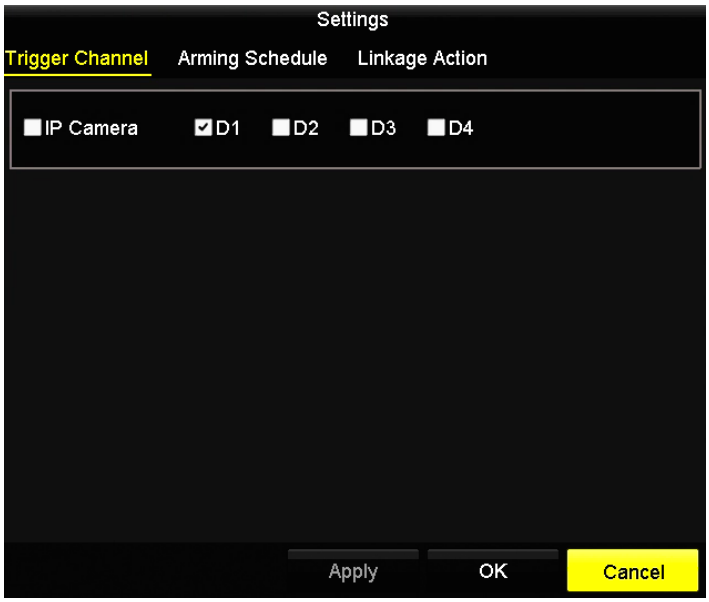
Follow the steps to set the motion detection parameters. In the live view mode, once a motion detection event takes place, the NVR can analyze it and do many actions to handle it. Enabling motion detection function can trigger certain channels to start recording, or trigger full screen monitoring, audio 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
2. Configure Motion Detection
   2.1 Choose camera you want to configure.
   2.2 Check the checkbox after **Enable Motion Detection**.
   2.3 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**.



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



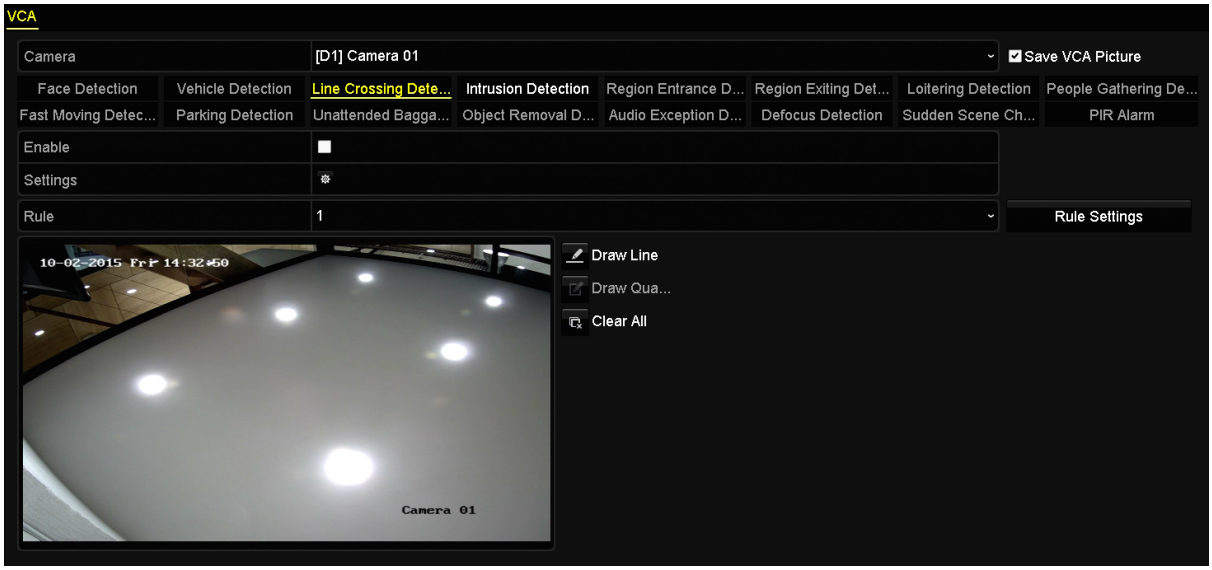
2.5 Select the channels which you want the motion detection event to trigger recording.
2.6 Click **Apply** to save the settings.
2.7 Click **OK** to back to the upper level menu.
2.8 Exit the Motion Detection menu.
2.9 Edit the Motion Detection Record Schedule. For the detailed information of schedule configuration, see *4.2 Configuring Recording Schedule*.

4.4 Configuring VCA Event Recording

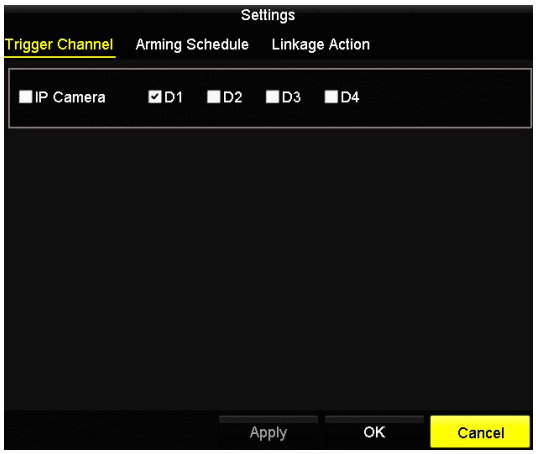
The event triggered recording can be configured through the menu. Then events include the motion detection, alarm and VCA events (face detection/face capture, line crossing detection, intrusion detection, region entrance detection, region exiting detection, loitering detection, people gathering detection, 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



2. Configure the detection rules for VCA events. For details, see the step 2 in *8.0 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



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

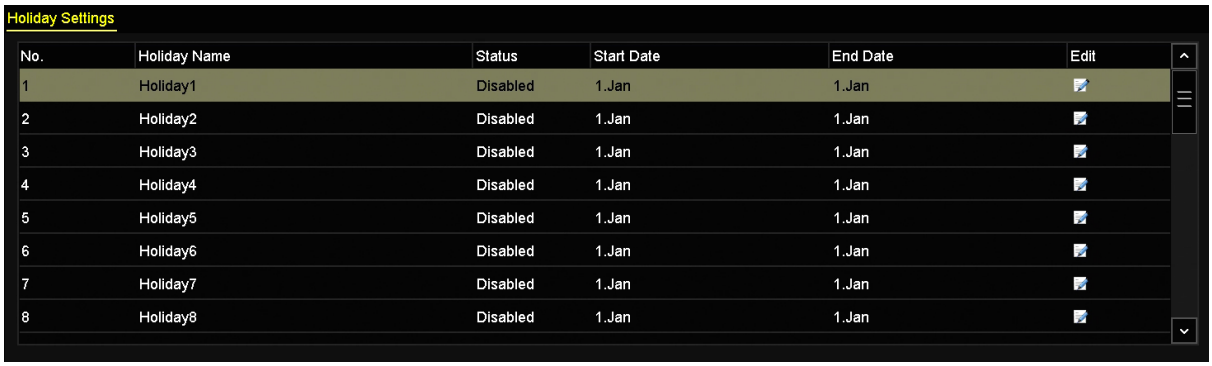
4. Enter Record Schedule settings interface (Menu > Record > Schedule > Record Schedule), and then set VCA as the record type. For details, see step 2 in *4.2 Configuring Recording Schedule.*

4.5 Configuring Holiday Recording

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

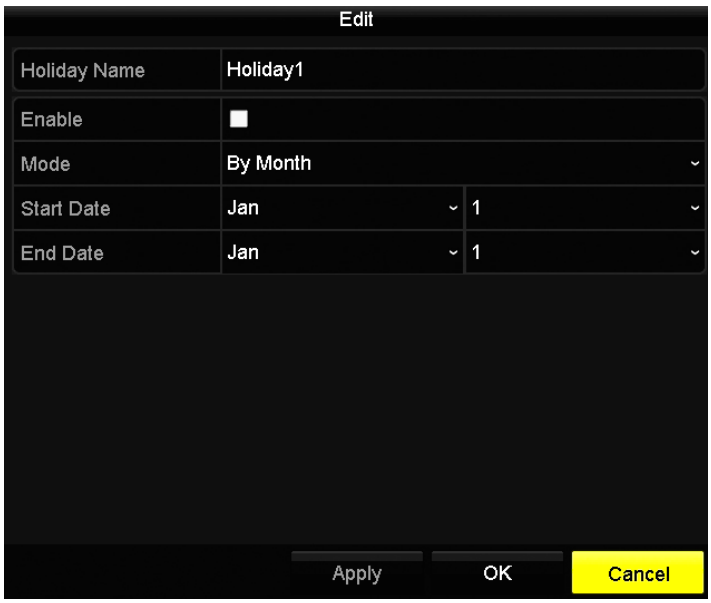
Steps:

1. Enter the Record setting interface.
   Menu > Record > Holiday



2. Enable Edit Holiday schedule.

   2.1 Click  to enter the Edit interface.



   2.2 Check the checkbox after **Enable Holiday**.
   2.3 Select Mode from the dropdown list.
   There are three different modes for the date format to configure holiday schedule.
   2.4 Set the start and end date.
   2.5 Click **Apply** to save settings.
   2.6 Click **OK** to exit the Edit interface.

3. Enter Record Schedule settings interface to edit the holiday recording schedule. See *4.2 Configuring Recording Schedule.*

4.6 Files Protection

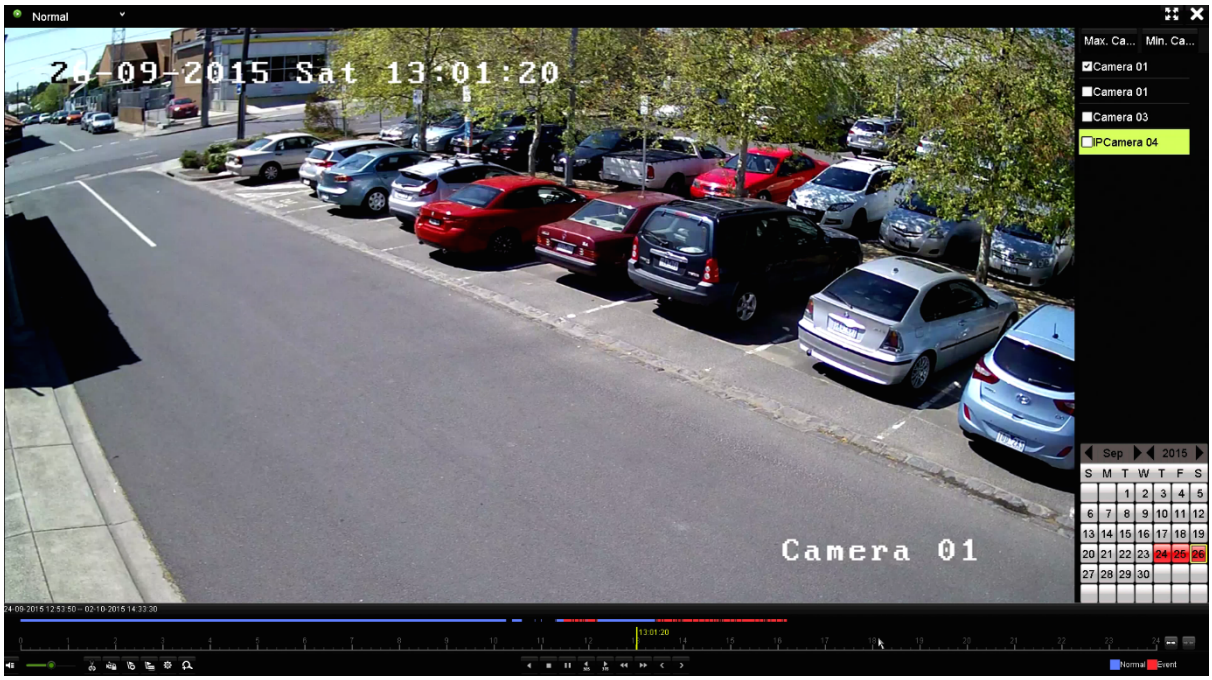
You can lock the recording files or set the HDD property to Read-only to protect the record files from being overwritten.

4.6.1 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.



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

Note: In the multi-channel playback mode, 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.

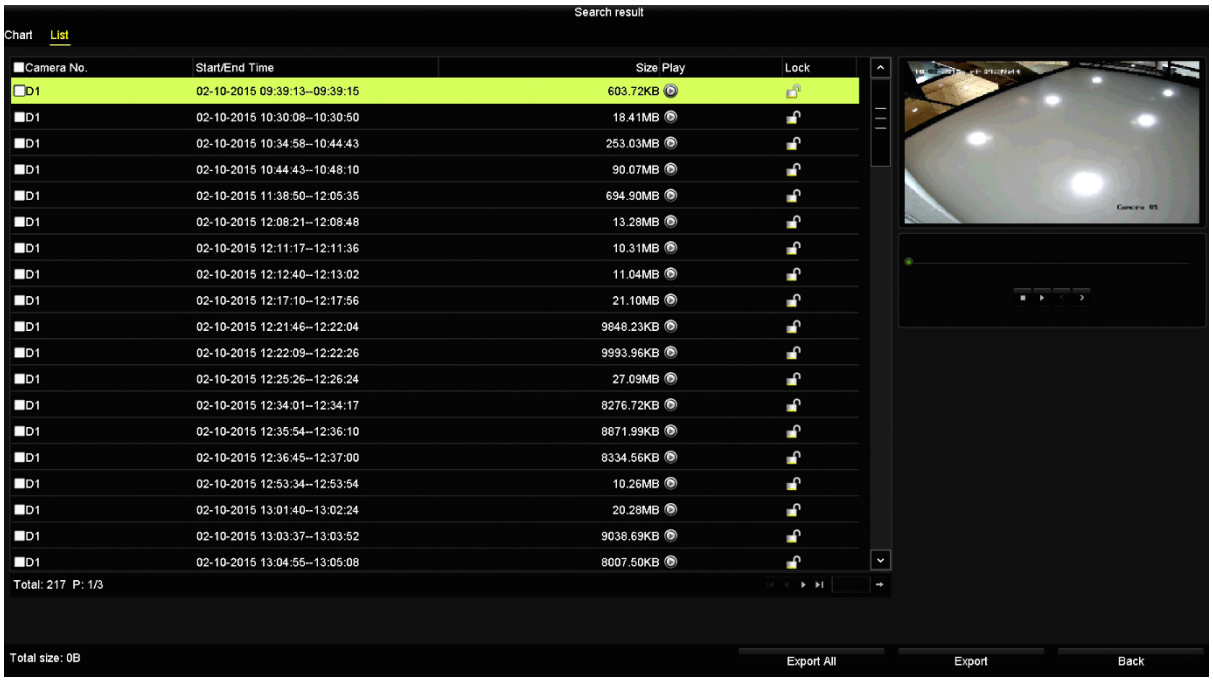
In the File Management interface, you can also click  to change it to  to unlock the file and the file is not protected

- **Lock File when Export**

Steps:

1. Enter Export setting interface.
   Menu > Export

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



5. Protect the record files.

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

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

5.2 Click  to change it to  to unlock the file and the file is not protected.

5.0 Playback

5.1 Playing Back Record Files

5.1.1 Instant Playback

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

Instant playback by channel
Step:

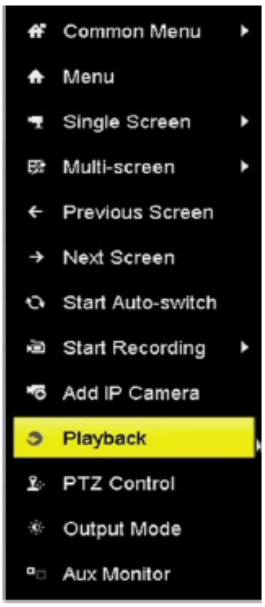
Choose a channel in live view mode and click the  button in the quick setting toolbar.

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

5.1.2 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



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

Playback by Time

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.

Note: 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.

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

Note:

The 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.

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

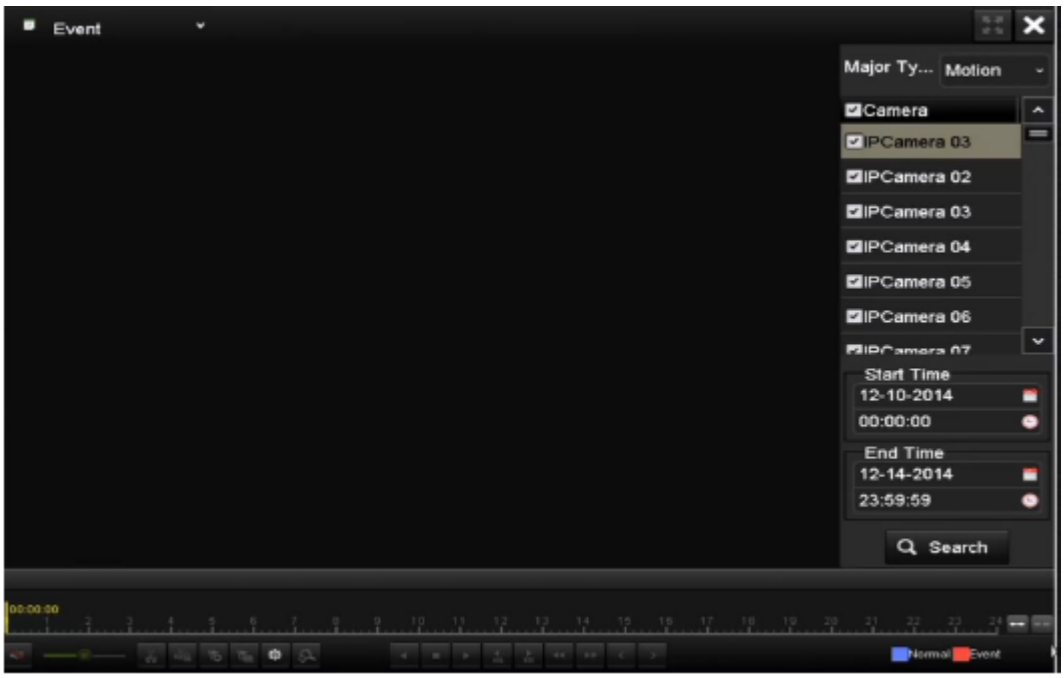
5.1.3 Playing Back by Event Search

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

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.



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

Note: For configuring the VCA recording, please refer to *4.4 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.

You can click ‹ or › button to select the previous or next event.

5.1.4 Playing Back by Tag

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 *5.1* for the detailed information about searching and playback of the record files.

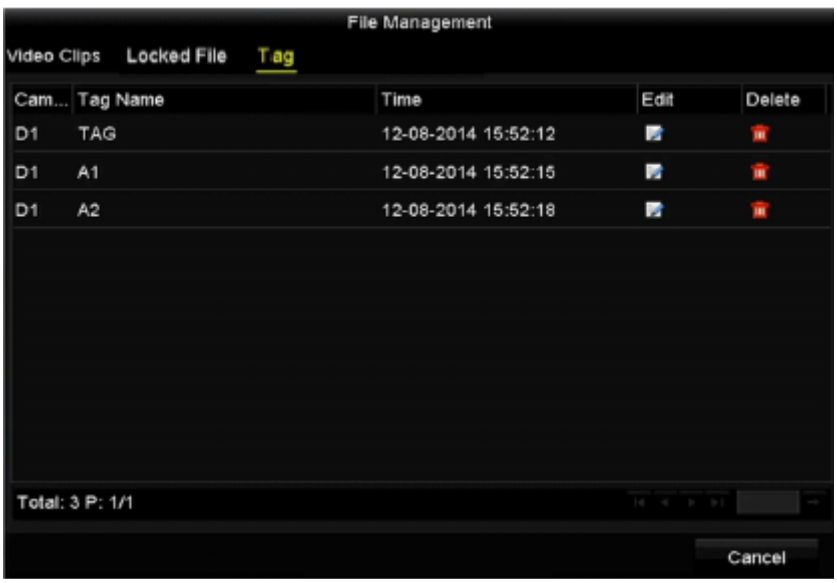
Click button to add default tag.

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



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 

to search the tag on your command.

3. Click button to play back the selected tag file.
   You can click the **Back** button to back to the search interface.

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

You can click or button to select the previous or next tag.

6.0 Backup

6.1 Backing up Record Files

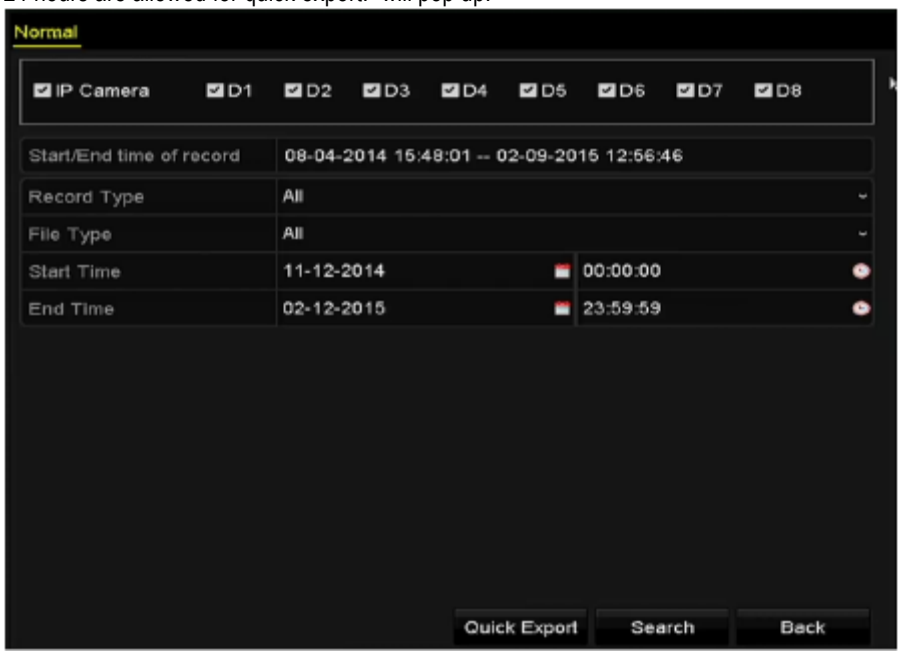
6.1.1 Quick Export

Export record files to backup device(s) quickly.

Steps:

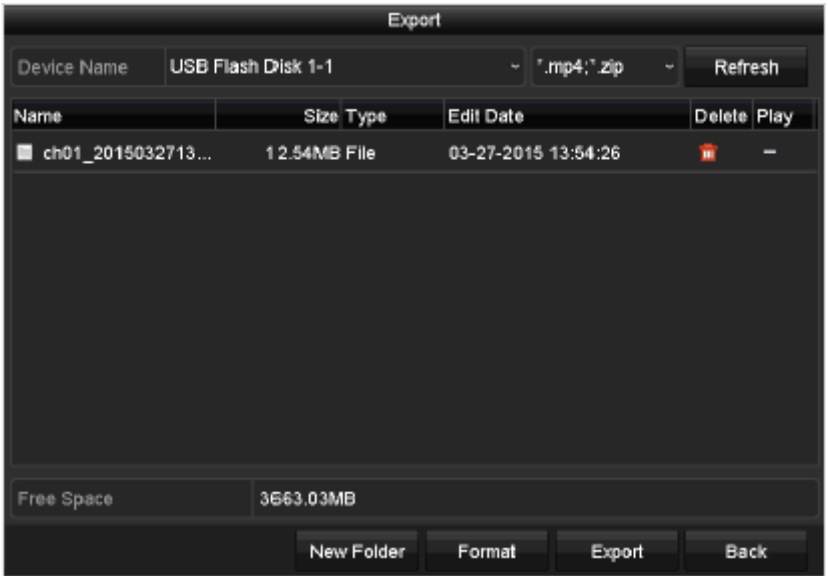
1. Enter Video Export interface.
   Menu > Export > Normal
   Choose the channel(s) you want to back up and click **Quick Export** button.

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.

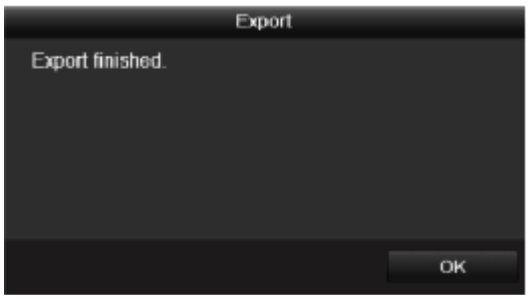


2. Select the format of the log files to be exported. Up to 9 formats are selectable.
3. Click the **Export** to start exporting.

Note: Here we use USB Flash Drive and please refer to the next section Normal Backup for more backup devices supported by the NVR.

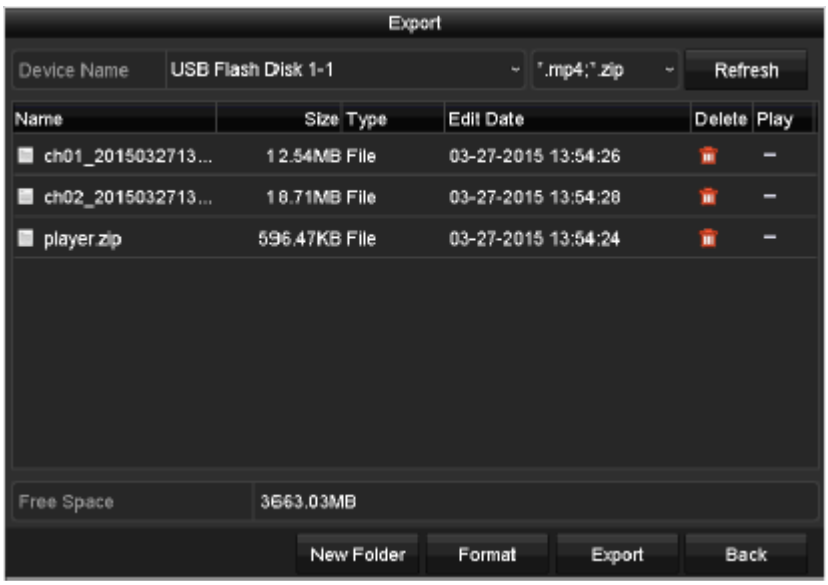


Stay in the Exporting interface until all record files are exported.



4. Check backup result.

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



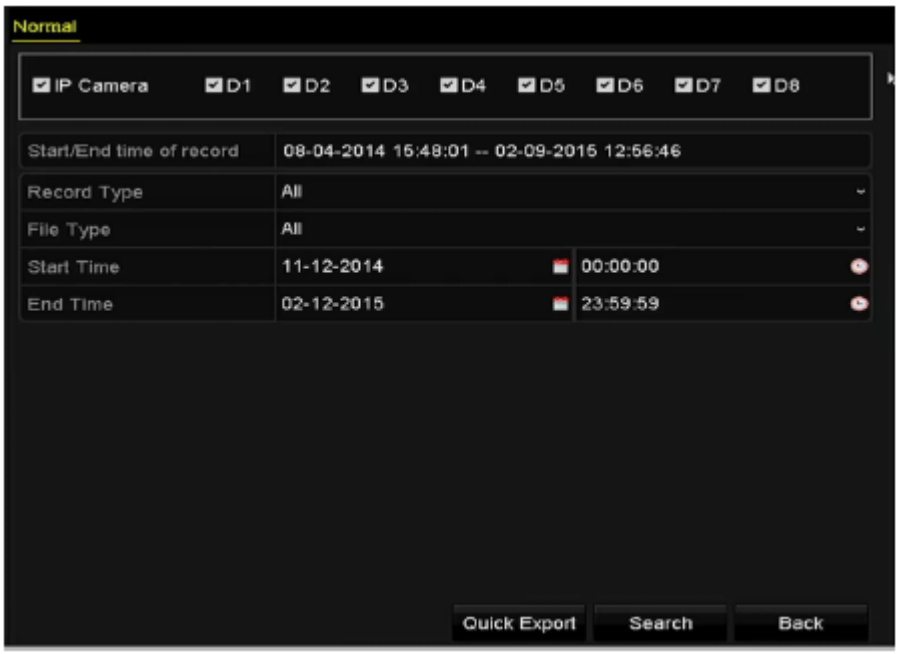
6.1.2 Backing up by Normal Video Search

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.

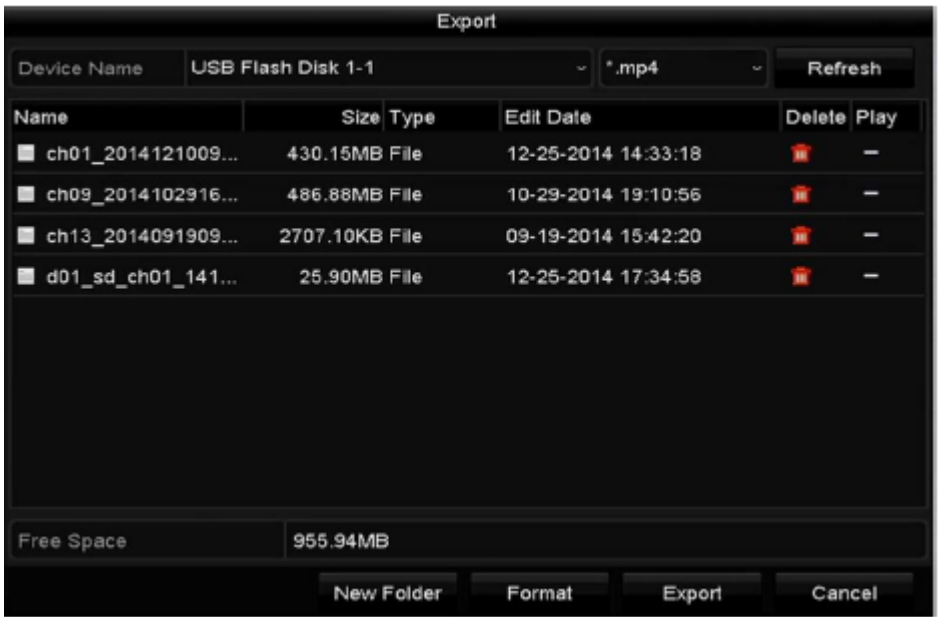


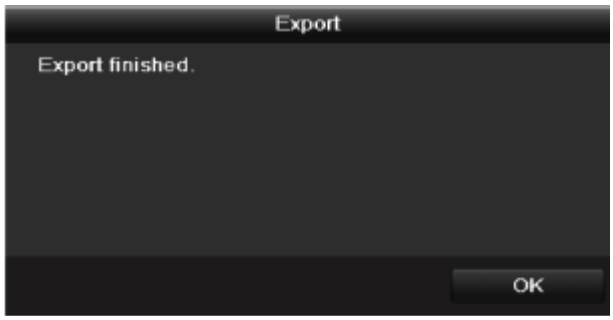
4. Select video files or pictures from the Chart or List to export.
   Click  to play the record file if you want to check it.
   Check the checkbox before the record files you want to back up.

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

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.





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

6.1.3 Backing up Video Clips

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

Steps:

1. Enter Playback interface.
   Please refer to *5.1 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.

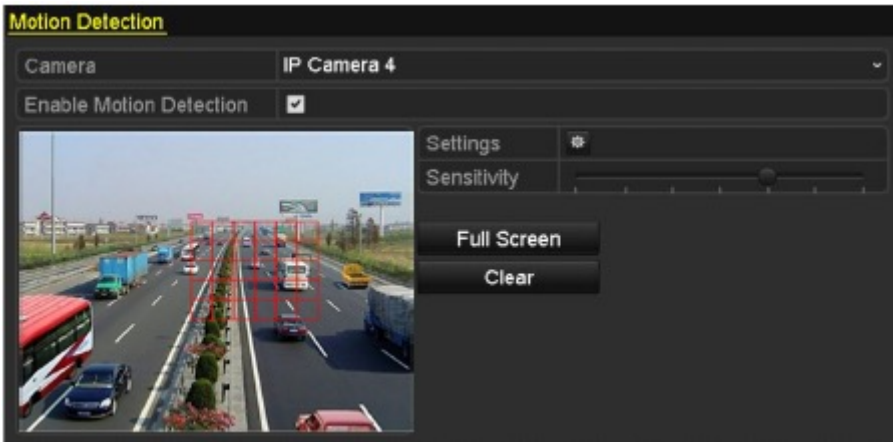
7.0 Alarm Settings

7.1 Setting Motion Detection Alarm

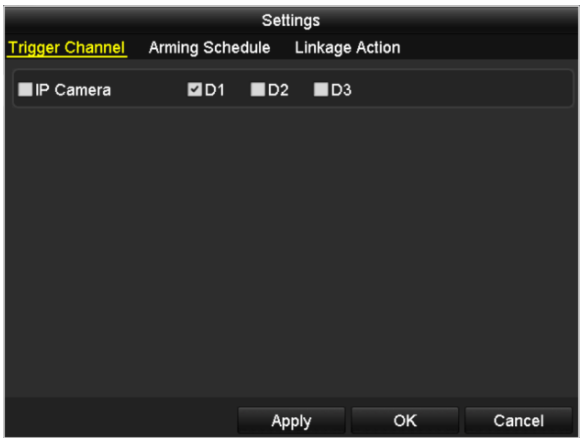
Steps:

1. Enter Motion Detection interface of Camera Management and choose a camera you want to set up motion detection.
   Menu > Camera > Motion
2. Set up detection area and sensitivity.
   Tick **Enable Motion Detection**, and use the mouse to draw detection area(s) and drag the sensitivity bar to set sensitivity.

Note: By default, the motion detection is enabled and configured in full screen.
Click button and set alarm response actions.

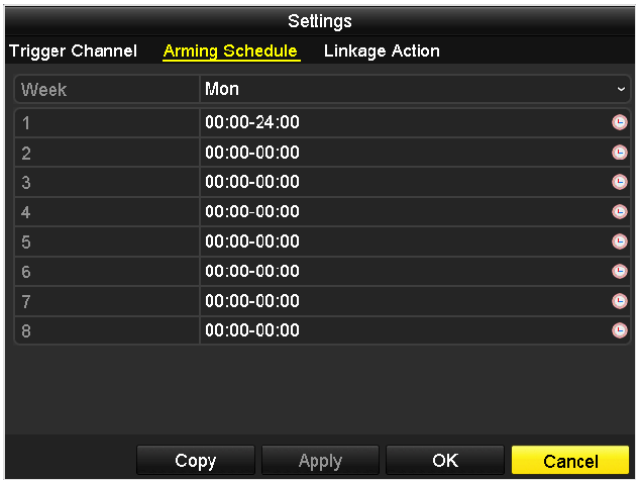


3. Click **Trigger Channel** tab and select one or more channels which will start to record or become full-screen monitoring when motion alarm is triggered, and click **Apply** to save the settings.



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

Note: Time periods shall not be repeated or overlapped.



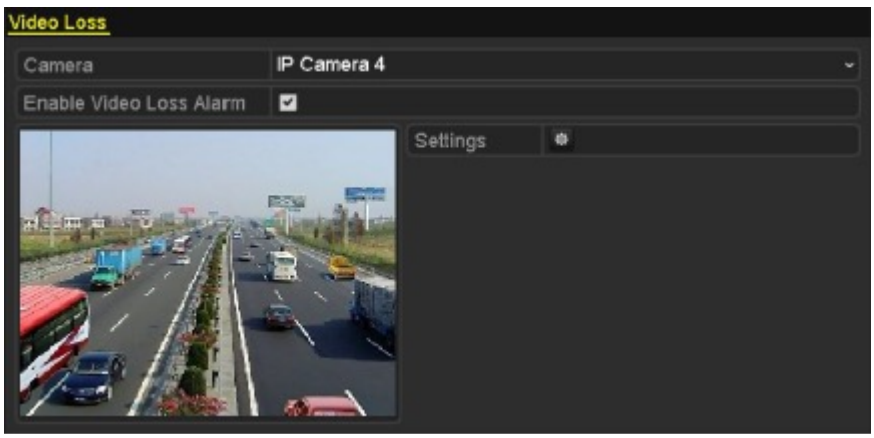
5. Click **Handling** tab to set up alarm response actions of motion alarm (please refer to *7.5 Setting Alarm Response Actions*).
6. If you want to set motion detection for another channel, repeat the above steps or just click **Copy** in the Motion Detection interface to copy the above settings to it.

7.2 Detecting Video Loss Alarm

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

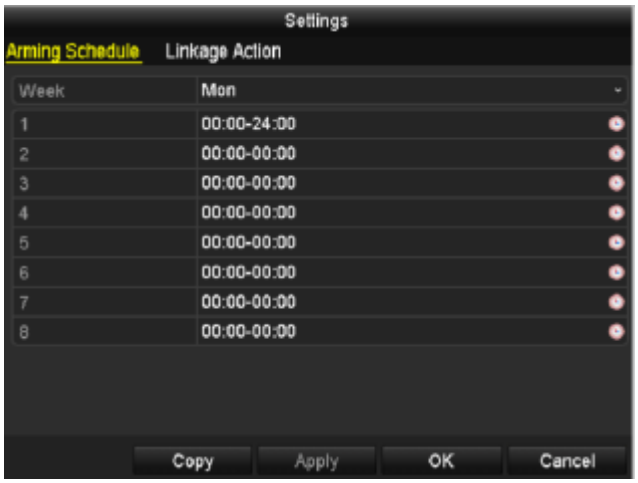
Steps:

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



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.



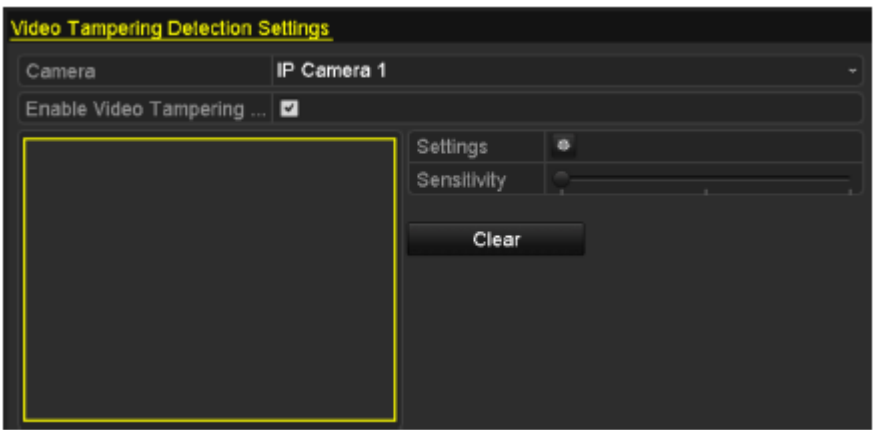
4. Select **Linkage Action** tab to set up alarm response action of video loss (please refer to *7.5 Setting Alarm Response Actions*).
5. Click the **OK** button to complete the video loss settings of the channel

7.3 Detecting Video Tampering Alarm

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

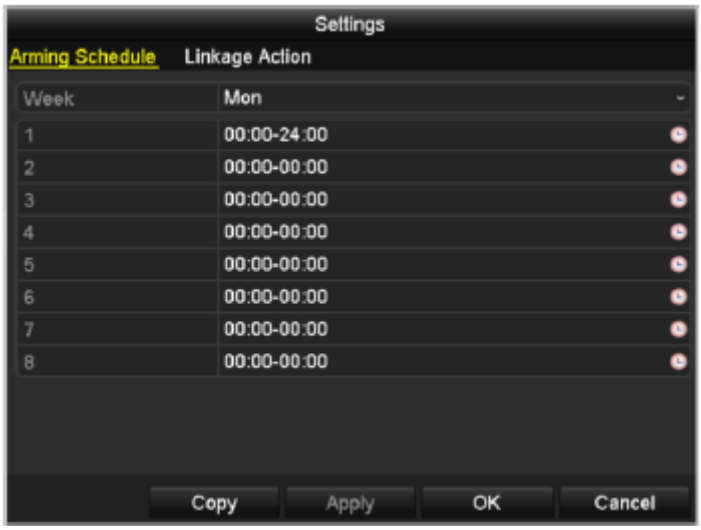
Steps:

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



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.
   3.1 Click Arming Schedule tab to set the arming schedule of handling actions.
   3.2 Choose one day of a week and max. eight time periods can be set within each day.
   3.3 Click **Apply** button to save the settings.

Note: Time periods shall not be repeated or overlapped.



4. Select **Linkage Action** tab to set up alarm response actions of video tampering alarm (please refer to *7.5 Setting Alarm Response Actions*).
5. Click the **OK** button to complete the video tampering settings of the channel.

7.4 Handling Exceptions Alarm

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.
• **PoE Power Overload:** The power consumption of the connected cameras via the PoE interface exceeds the maximum PoE power.

NOTE: PoE Power Overload is note supported by SW-0820154N & SW-0820158N series NVR.

Steps:
Enter Exception interface of System Configuration and handle various exceptions.
Menu> Configuration> Exceptions
Please refer to *7.5 Setting Alarm Response Actions* for detailed alarm response actions.

7.5 Setting Alarm Response Actions

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**.

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

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

Full Screen Monitoring

When an alarm is triggered, the local monitor (VGA and HDMITM monitor) 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.

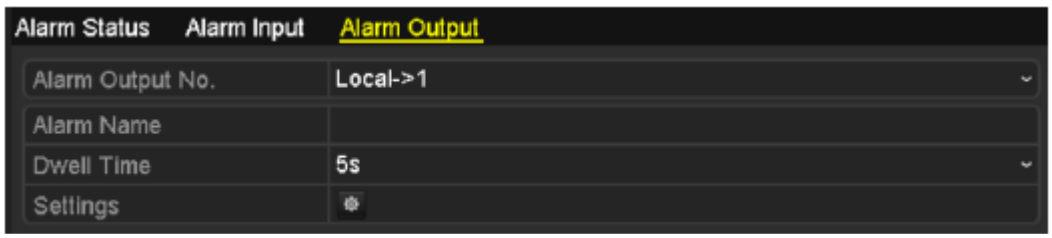
Note: The alarm signal will be transmitted automatically at detection mode when remote alarm host is configured. Please refer to *9.2.5 Configuring Remote Alarm Host* for details of alarm host configuration.

Email Linkage
Send an email with alarm information to a user or users when an alarm is detected.
Please refer to 9.2.9 for details of Email configuration

Trigger Alarm Output
Trigger an alarm output when an alarm is triggered.

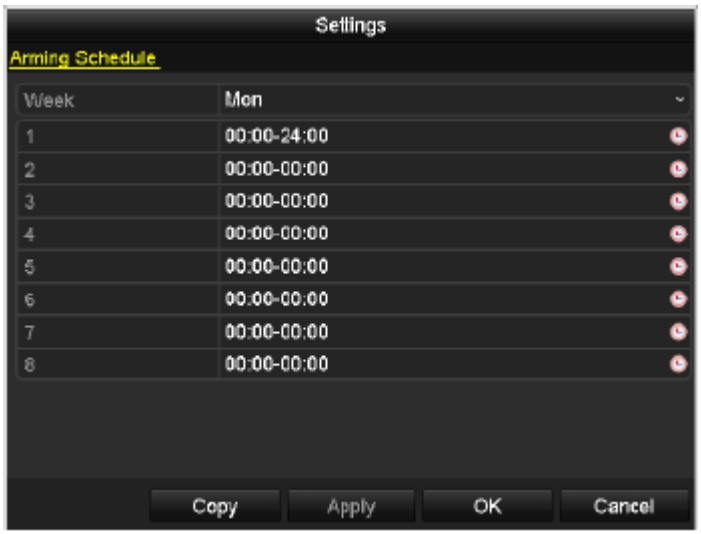
1. Enter Alarm Output interface.
   Menu> Configuration> Alarm> Alarm Output
   Select an alarm output and set alarm name and dwell time. Click **Schedule** button to set the arming schedule of alarm output.

Note: If "Manually Clear" is selected in the dropdown list of Dwell Time, you can clear it only by going to Menu>Manual> Alarm.



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.



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.

8.0 VCA Alarm

8.1 Line Crossing Detection

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.

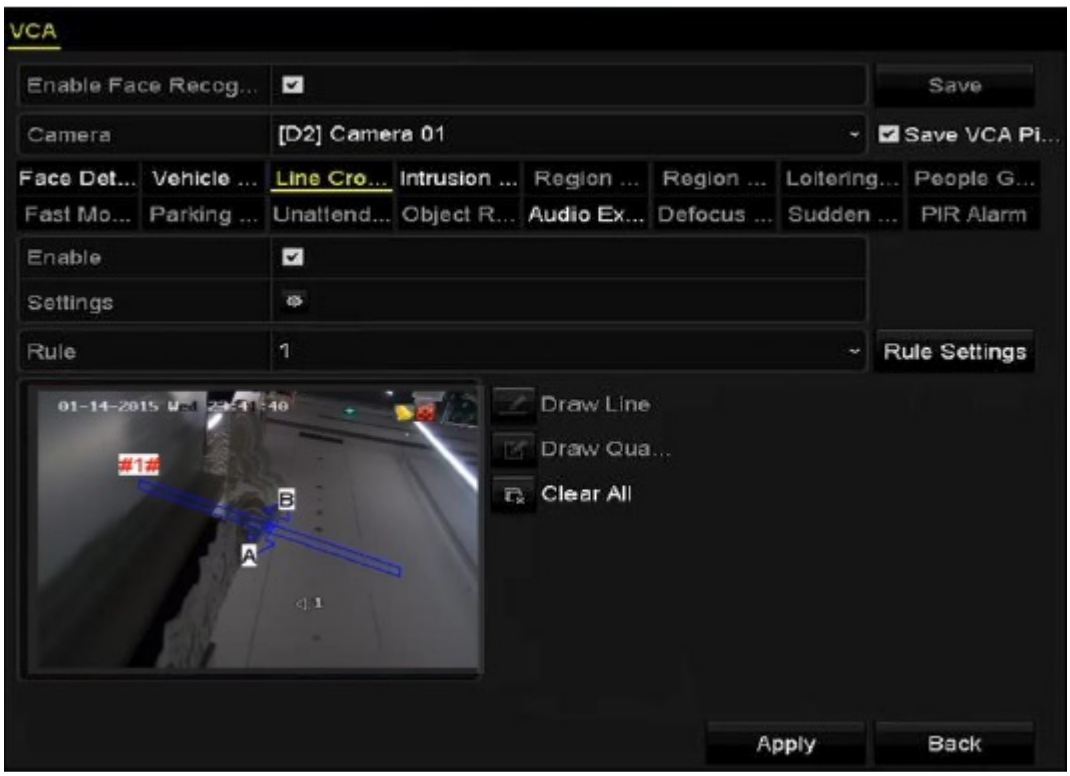
Steps:

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.
   6.1 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.
   6.2 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.
   6.3 Click-**OK** to save the rule settings and back to the line crossing detection settings interface.

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

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

Note: Up to 4 rules can be configured.



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

8.2 Intrusion Detection

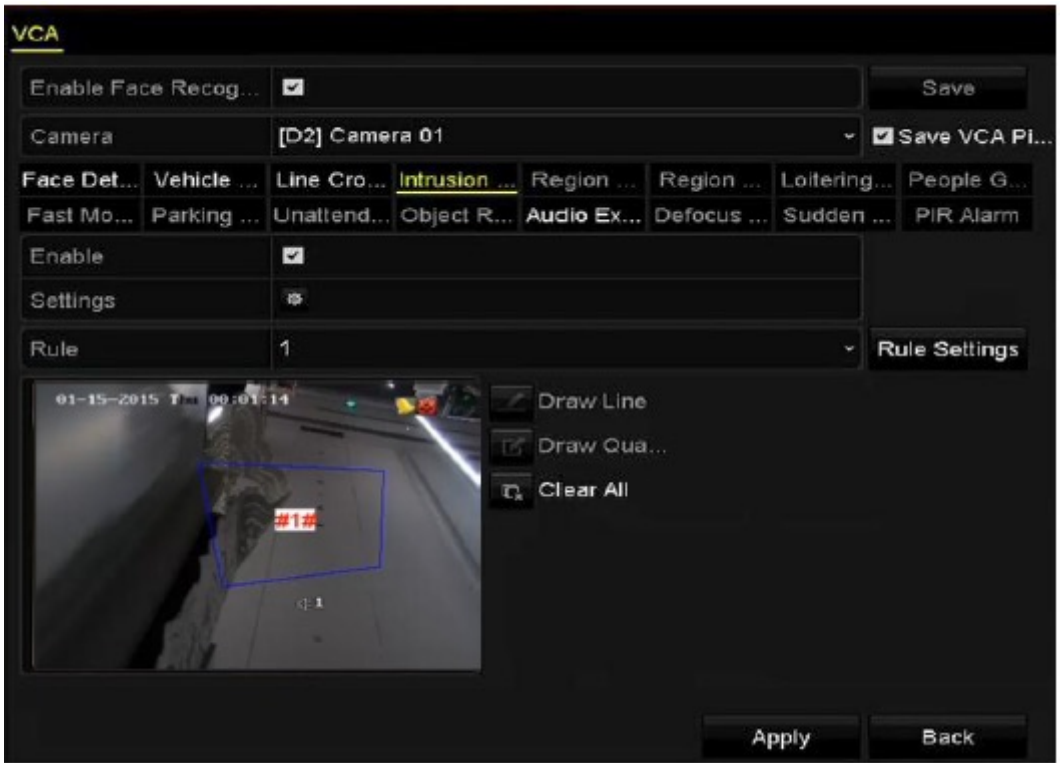
Intrusion detection function detects people, vehicle or other objects which enter and loiter in a pre-defined virtual region, and some certain actions can be taken when the alarm is triggered.

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 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.
   6.1 **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.
   6.2 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.
   6.3 **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.

   6.4 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.



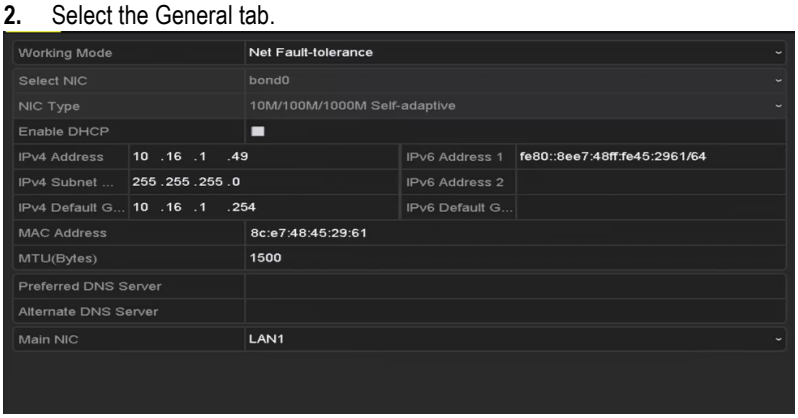
8. Click **Apply** to save the settings

9.0 Network Settings

9.1 Configuring General Settings

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.



- one 10 /100 Mbps self-adaptive Ethernet interface for SW-0820154N & SW-0820158N series NVR;

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.

Note:

- For the models which have the PoE or built-in switch network interfaces, the internal NIC IPv4 address should be configured for the cameras connecting to the PoE or built-in switch network interface of the NVR.
- The valid value range of MTU is 500 ~ 9676.

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

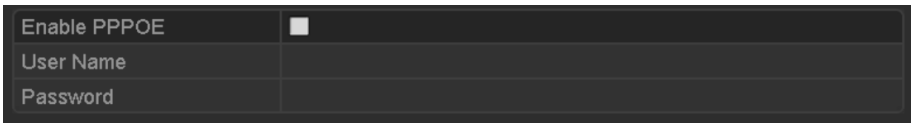
9.2 Configuring Advanced Settings

9.2.1 PPPoE Settings

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



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 12.1 Viewing System Information for PPPoE status.

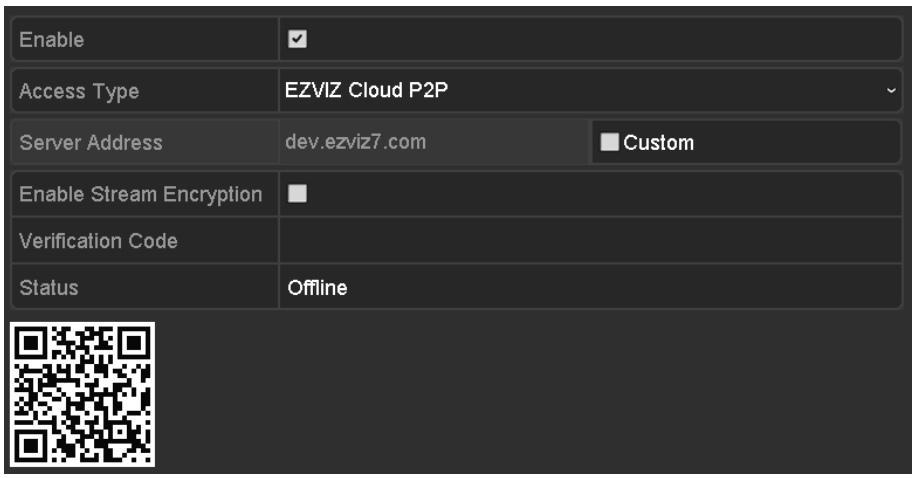
9.2.2 Configuring EZVIZ Cloud P2P

EZVIZ Cloud P2P provides the mobile phone application and as well the service platform page to access and manage your connected NVR, which enables you to get a convenient remote access to the surveillance system. Steps:

1. Enter the Network Settings interface. Menu > Configuration > Network
2. Select the Platform Access tab to enter the EZVIZ Cloud P2P Settings interface.
3. Check the Enable check box to activate this feature.
4. If required, select the check box of Custom and in put the Server Address.
5. To turn the Enable Stream Encryption on, you can select its checkbox.
6. Enter the Verification Code of the device.

Note: The verification code consists of 6 capital letters and is located at the bottom of the DVR. You can also use the

scanning tool of your phone to quickly get the code by scanning the QR code below.



7. Click the Apply button to save and exit the interface. After configuration, you can access and manage the NVR by your mobile phone on which the EZVIZ Cloud P2P application is installed or by the EZVIZ website (www.ezviz7.com).

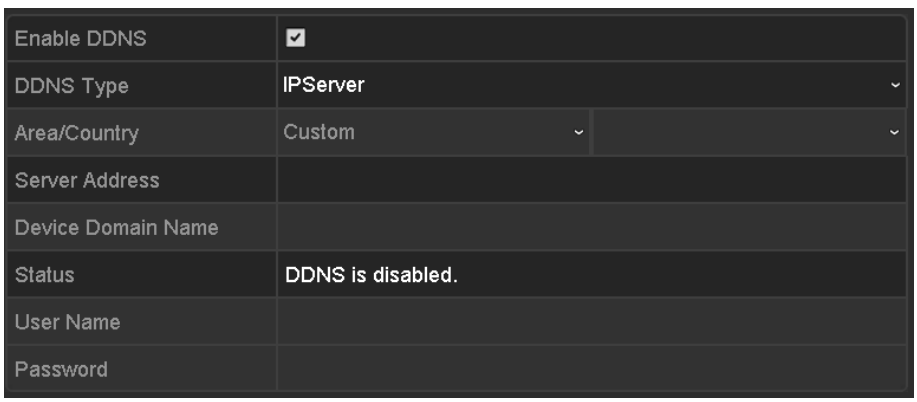
Note: For more operation instructions, please refer to the help file on the EZVIZ official website (www.ezviz7.com).

9.2.3 Configuring DDNS

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.
3. Check the Enable DDNS checkbox to enable this feature.
4. Select DDNS Type. Five different DDNS types are selectable: IPServer, DynDNS, PeanutHull, NO-IP and HiDDNS.

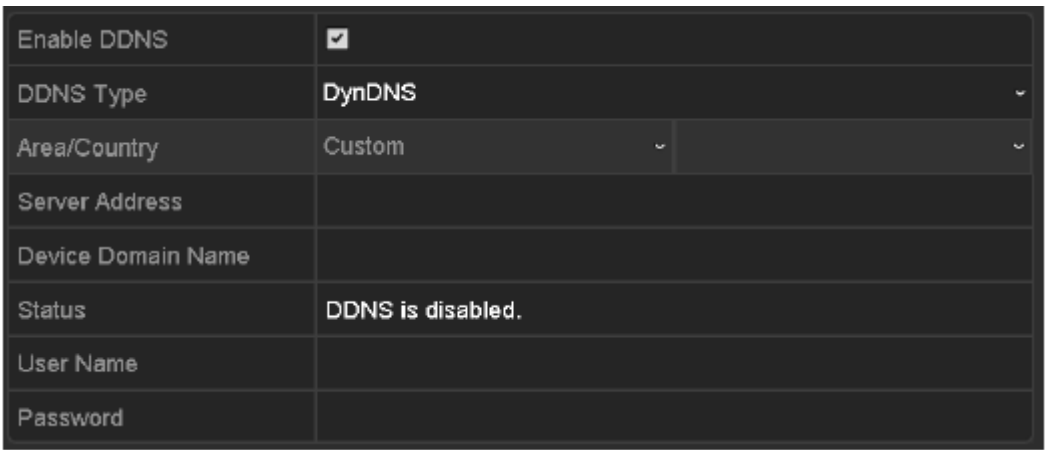
• IPServer: Enter Server Address for IPServer.



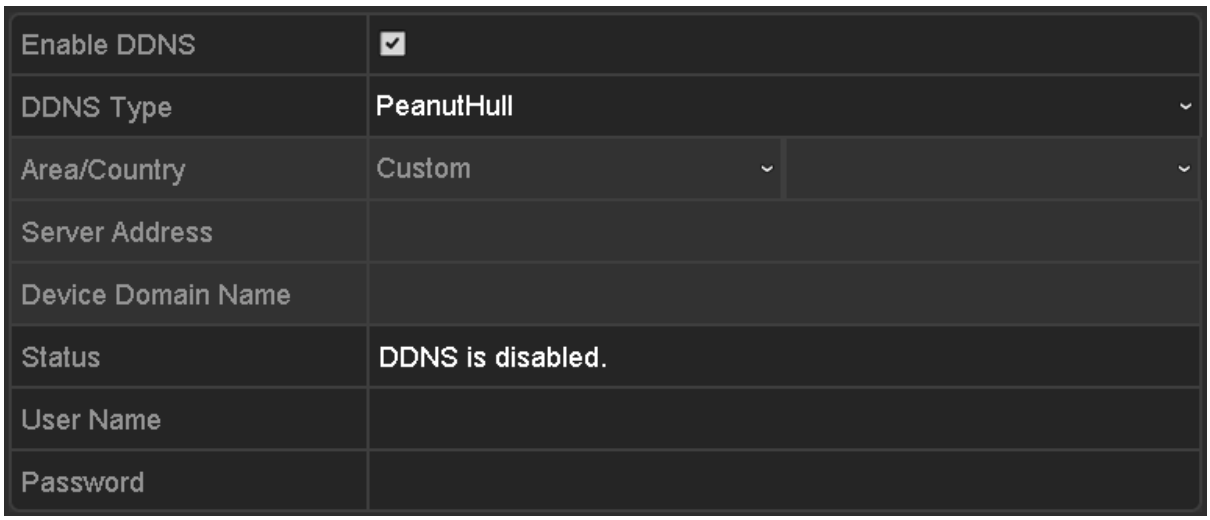
• DynDNS:

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.



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



• **NO-IP:**
Enter the account information in the corresponding fields. Refer to the DynDNS settings.

1. Enter **Server Address** for NO-IP.
2. In the 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.

Enable DDNS	☑
DDNS Type	NO-IP
Area/Country	Custom
Server Address	
Device Domain Name	
Status	DDNS is disabled.
User Name	
Password	

• **HiDDNS:**

1. Select the continent/country of the server on which the device is registered.
2. The **Server Address** of the HiDDNS server appears by default: www.hik-online.com.
3. 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.

Enable DDNS	☑
DDNS Type	HiDDNS
Area/Country	Custom
Server Address	www.hik-online.com
Device Domain Name	
Status	DDNS is disabled.
User Name	
Password	

OPTION 1: Access the Device via Web Browser

Open a web browser, and enter *http://www.hik-online.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.hik-online.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.hik-online.com/alias:HTTP port* in the address bar to access the device. You can refer to 9.2.8 for the mapped HTTP port No.

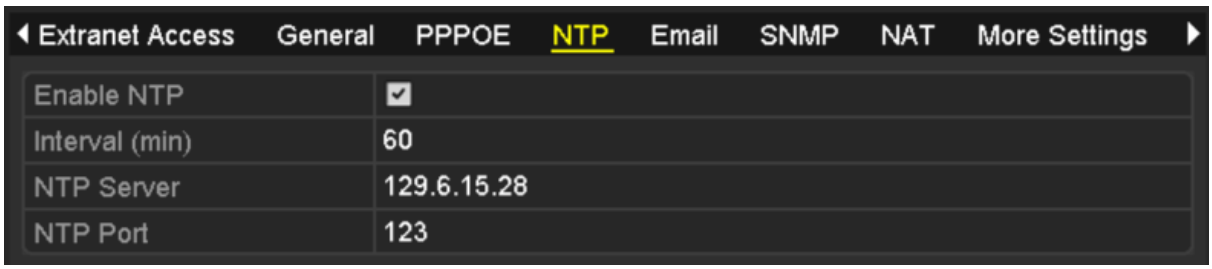
OPTION 2: Access the devices via iVMS-4200

For iVMS-4200, in the Add Device window, select and then edit the device information.
Nickname: Edit a name for the device as you want.
Server Address: www.hik-online.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.
Password: Enter the password of the device.

9.2.4 Configuring NTP Server

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 Network Settings interface.
   Menu >Configuration> Network
2. Select the **NTP** tab to enter the 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.

Note: 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.

9.2.5 Configuring Remote Alarm Host

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

Alarm Host IP	
Alarm Host Port	0
Server Port	8000
HTTP Port	80
Multicast IP	
RTSP Port	554
Enable High-speed Dow...	☐

3. Enter **Alarm Host IP** and **Alarm Host Port** in the text fields.
   The **Alarm Host IP** refers to the IP address of the remote PC on which the Network Video Surveillance Software (e.g., iVMS-4200) is installed, and the **Alarm Host Port** must be the same as the alarm monitoring port configured in the software.
4. Click the **Apply** button to save and exit the interface.

9.2.6 Configuring Multicast

The multicast can be configured to realize live view for more than 128 connections through network for the device. A multicast address spans the Class-D IP range of 224.0.0.0 to239.255.255.255. It is recommended to use the IP address ranging from 239.252.0.0 to 239.255.255.255.

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. 16.
3. Set **Multicast IP**, as shown in Figure 11. 17. When adding a device to the Network Video Surveillance Software, the multicast address must be the same as the NVR's multicast IP.

Server Port	8000
HTTP Port	80
Multicast IP	239.221.2.78

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

Note: The multicast function should be supported by the network switch to which the NVR is connected.

9.2.7 Configuring RTSP

The RTSP (Real Time Streaming Protocol) is a network control protocol designed for use in communication systems to control streaming media servers.

Steps:

1. Enter the Network Settings menu
   Menu >Configuration> Network
2. Select the **More Settings** tab to enter the More Settings menu, as shown in Figure 11. 16.

RTSP Port	554

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

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

9.2.8 Configuring Server and HTTP Ports

You can change the server and HTTP ports in the Network Settings menu. The default server port is 8000 and the default HTTP port is 80.

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. 16.
3. Enter new **Server Port** and **HTTP Port**.

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

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 web browser access.

9.2.9 Configuring Email

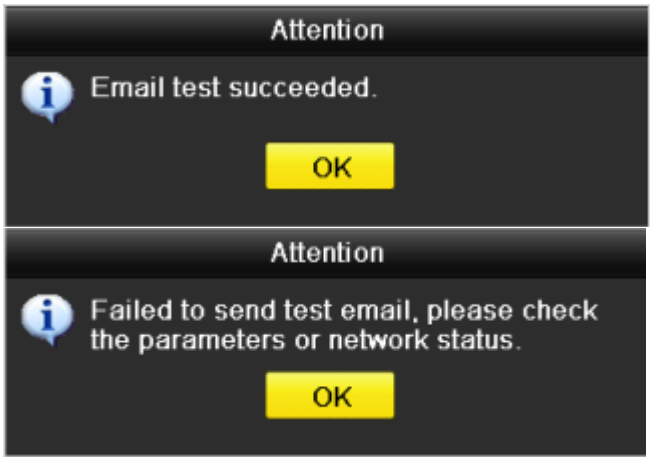
The system can be configured to send an Email notification to all designated users if an alarm event is detected, etc., an alarm or motion event is detected or the administrator password is changed.
Before configuring the Email settings, the NVR must be connected to a local area network (LAN) that maintains 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 men.

3. Click **Apply** to save the settings.
4. Select the Email tab to enter the 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. The corresponding Attention message box will pop up.



9.2.10 Configuring NAT

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

- **UPnPTM**

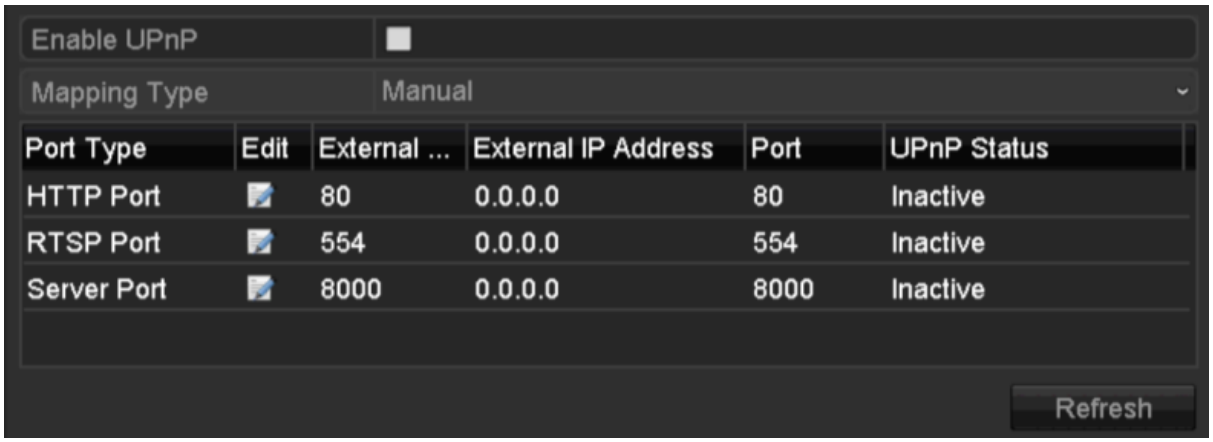
Universal Plug and Play (UPnP™) can permit the device seamlessly discover the presence of other network devices on the network and establish functional network services for data sharing, communications, etc. You can use the UPnP™ function to enable the fast connection of the device to the WAN via a router 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.

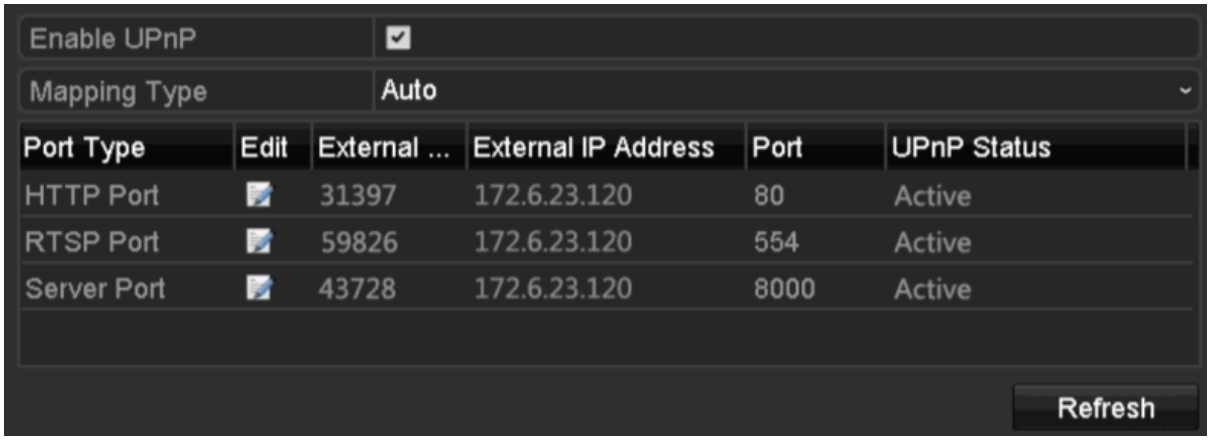
Steps:

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



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.



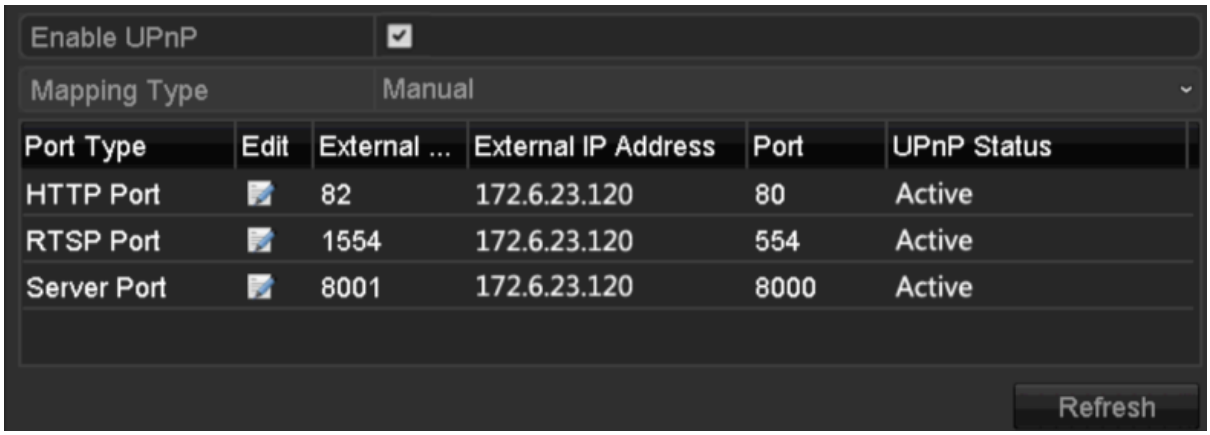
OPTION 2: Manual
If you select Manual as the mapping type, you can edit the external port on your demand by clicking to activate the External Port Settings dialog box.

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.

- 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.

3. Click **Apply** button to save the settings.
4. You can click **Refresh** button to get the latest status of the port mapping.



- **Manual Mapping**

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

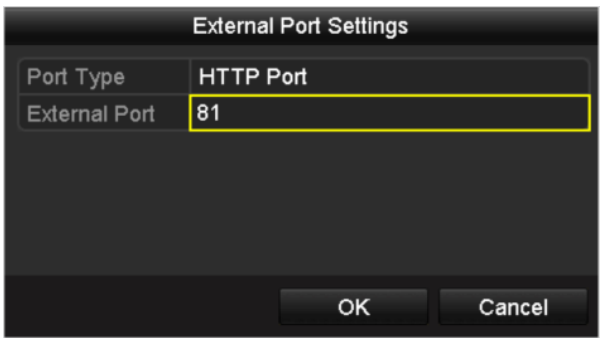
Before you start:

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

Steps:

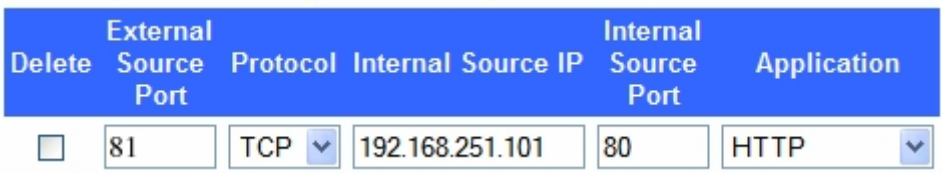
1. Enter the Network Settings interface.
   Menu > Configuration > Network
2. Select the **NAT** tab to enter the port mapping interface.
3. Leave the Enable UPnP checkbox unchecked.
4. Click to activate the External Port Settings dialog box. Configure the external port No. for server port,http port, 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.



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.



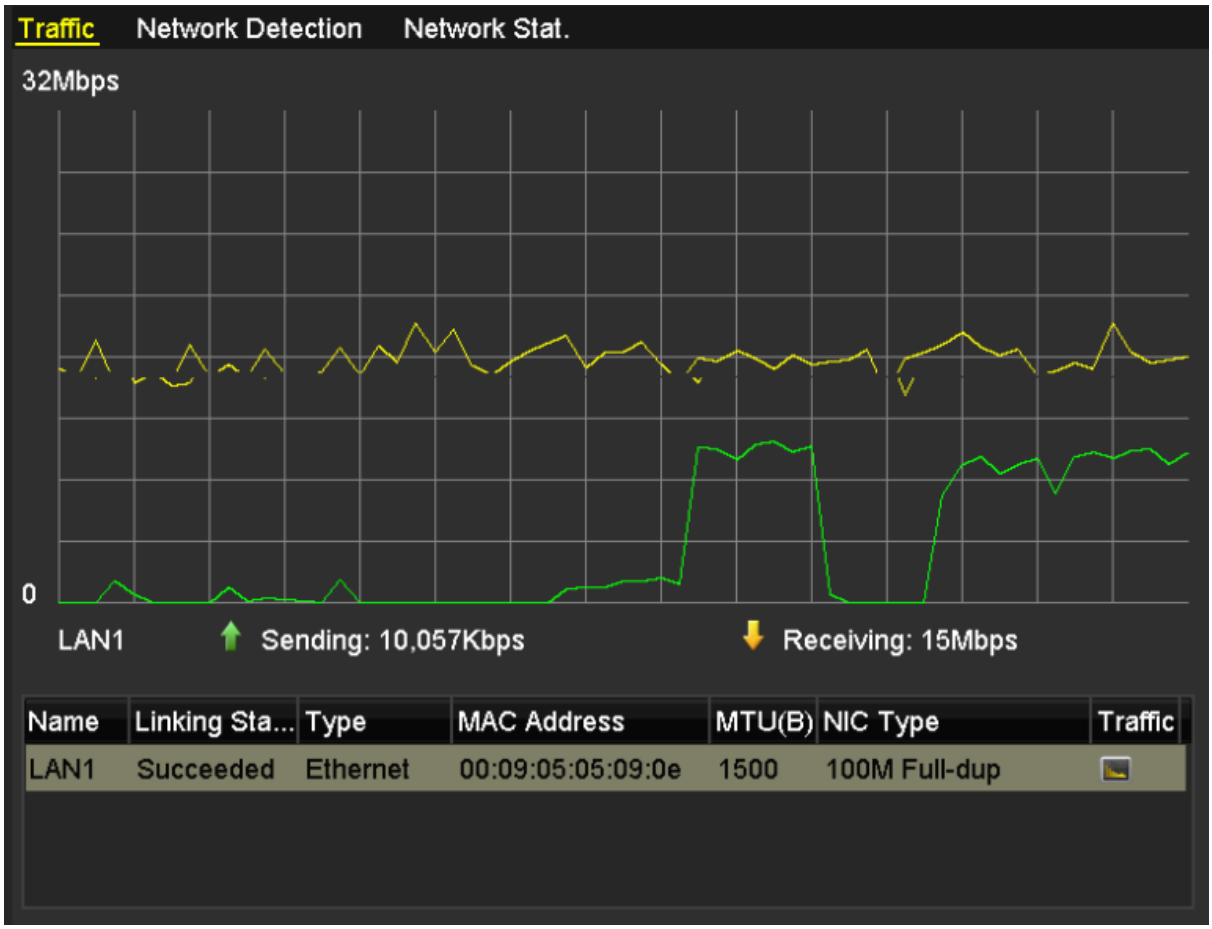
Note: The above virtual server setting interface is for reference only, it may be different due to different router manufactures. Please contact the manufacture of router if you have any problems with setting virtual server.

9.3 Checking Network Traffic

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



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

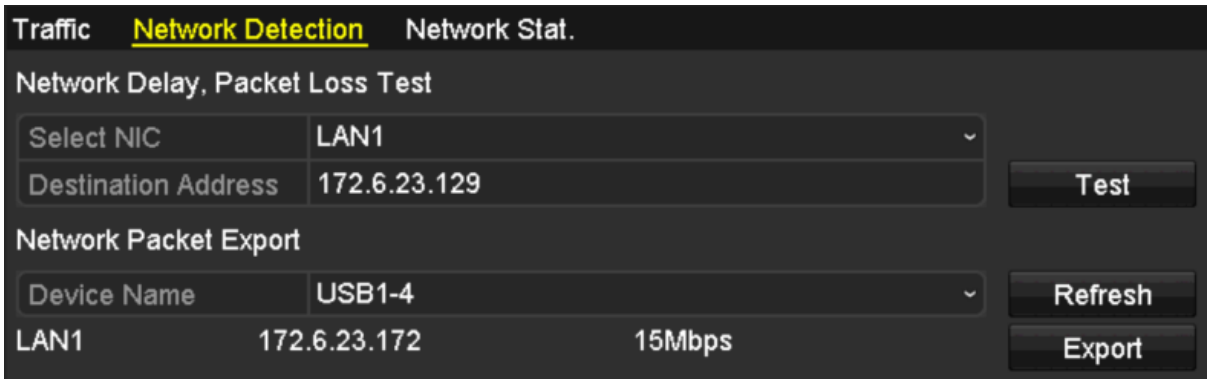
9.4 Configuring Network Detection

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

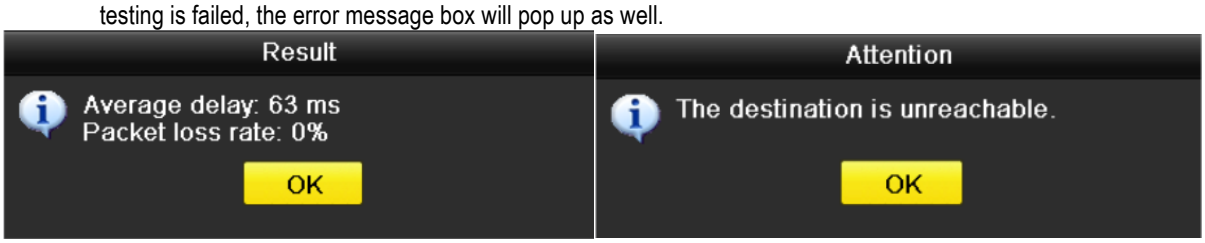
9.4.1 Testing Network Delay and Packet Loss

Steps:

1. Enter the Network Traffic interface.
   Menu >Maintenance>Net Detect
2. Click the **Network Detection** tab to enter the Network Detection menu



3. Enter the destination address in the text field of **Destination Address**.
4. Click **Test** button to start testing network delay and packet loss. The testing result pops up on the window. If the testing is failed, the error message box will pop up as well.



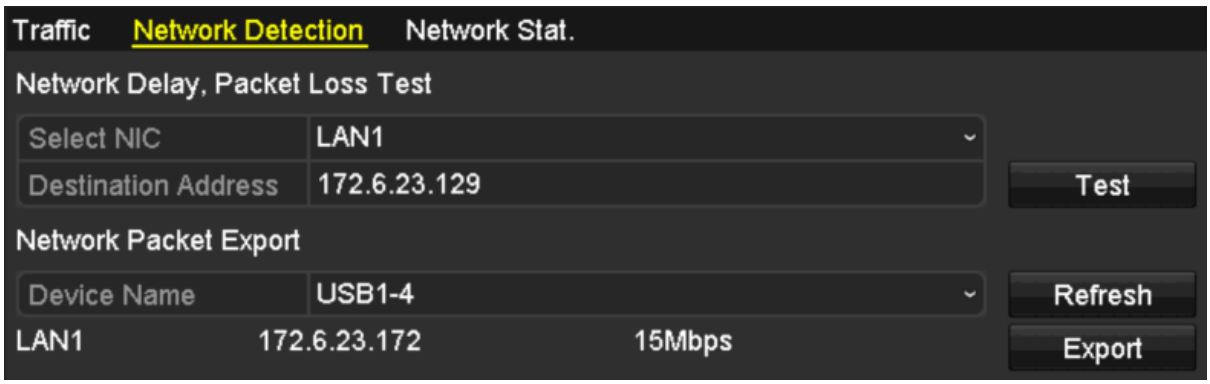
9.4.2 Exporting Network Packet

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

Steps:

1. Enter the Network Traffic interface.
   Menu >Maintenance>Net Detect
2. Click the **Network Detection** tab to enter the Network Detection interface.
3. Select the backup device from the dropdown list of Device Name

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



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

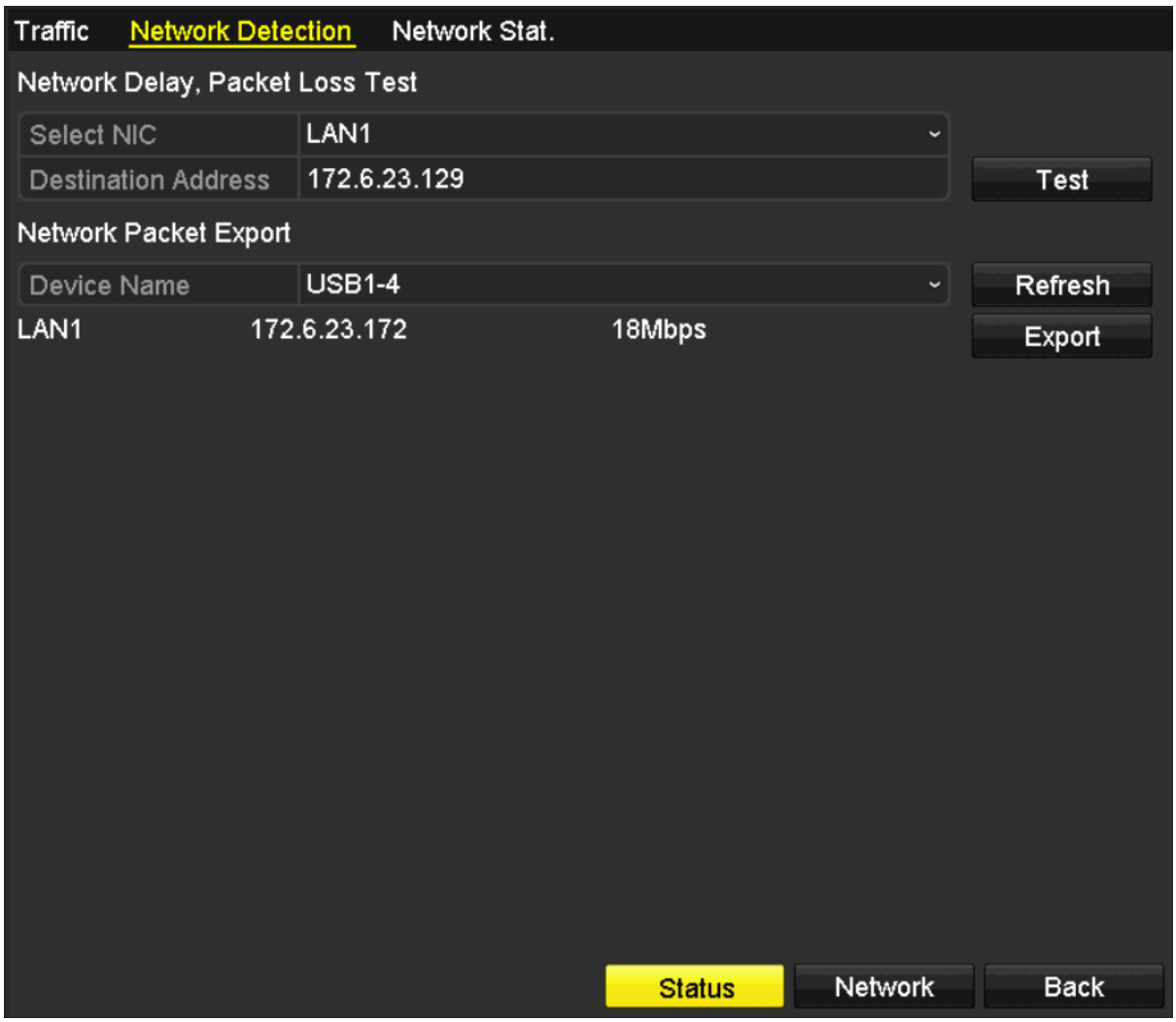
5. After the exporting is complete, click **OK** to finish the packet export

Note: Up to 1M data can be exported each time.

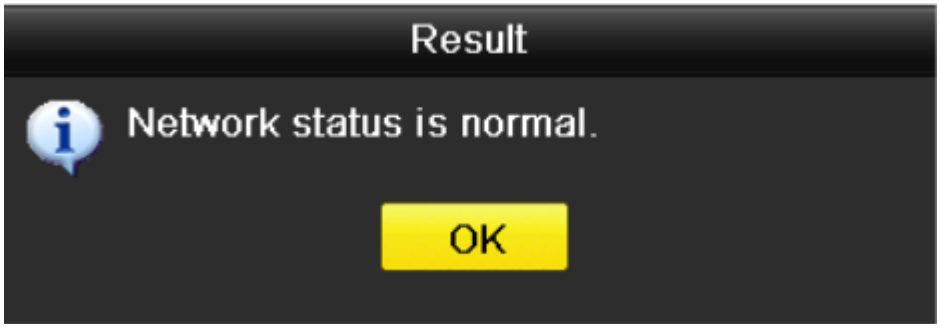
9.4.3 Checking the Network Status

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

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



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



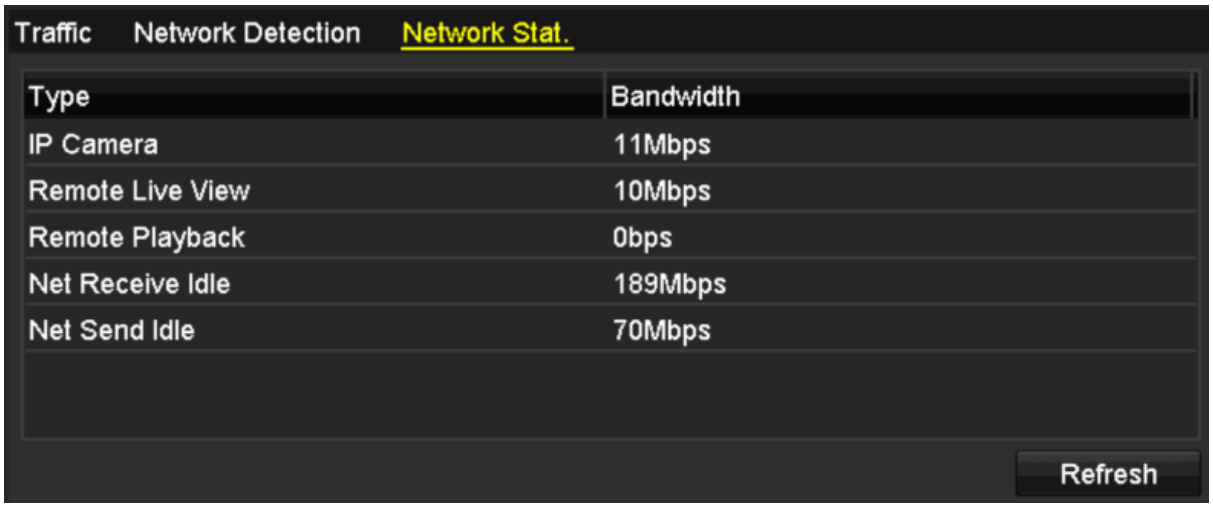
If the message box pops out with other information instead of this one, you can click **Network** button to show the quick setting interface of the network parameters.

9.4.4 Checking Network Statistics

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



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.

10.0 HDD Management

10.1 Initializing HDDs

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

Note: A message box pops up when the NVR starts up if there exits any uninitialized HDD.

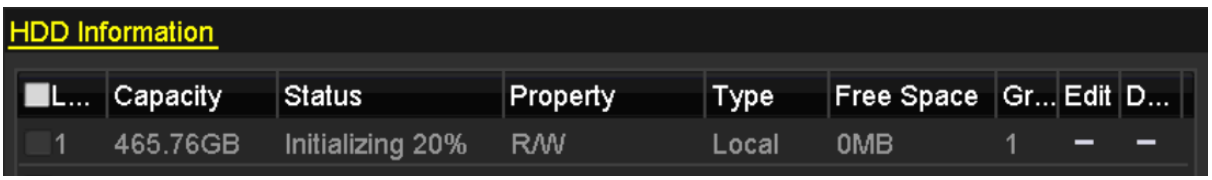
Click **Yes** button to initialize it immediately or you can perform the following steps to initialize the HDD.

Steps:

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

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

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



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

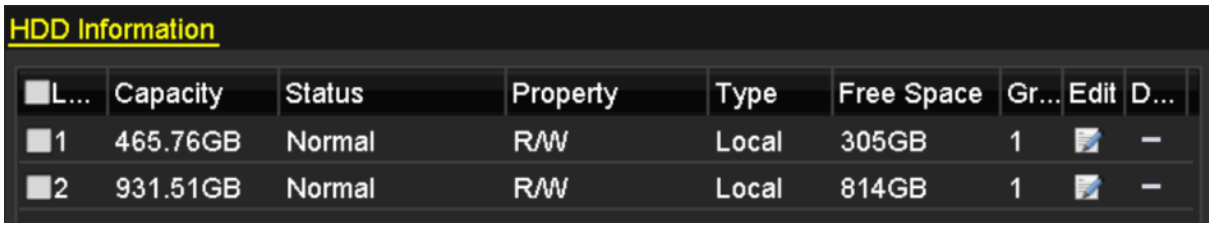
Note: Initializing the HDD will erase all data on it.

10.2 Managing Network HDD

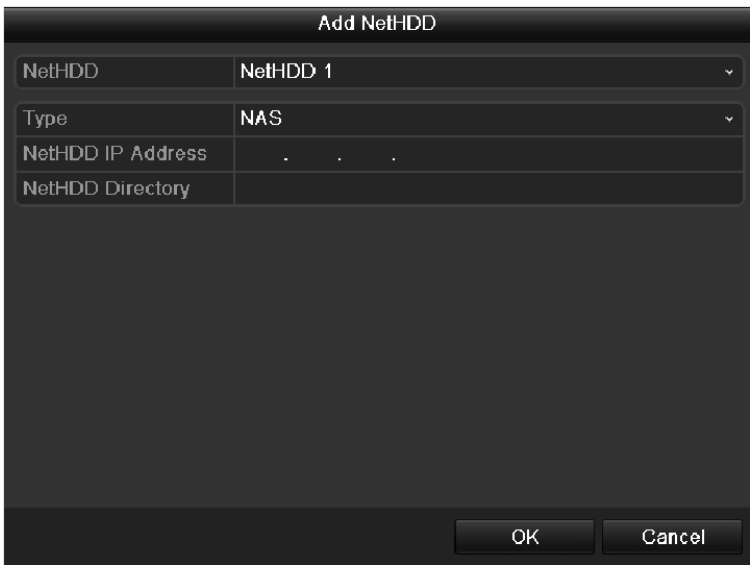
You can add the allocated NAS or disk of IP SAN to NVR, and use it as network HDD.

Steps:

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



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

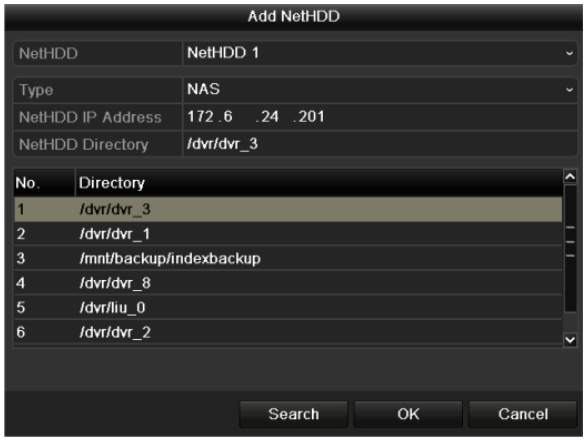


3. Add the allocated NetHDD.
4. Select the type to NAS or IP SAN.
5. Configure the NAS or IP SAN settings.

• 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.

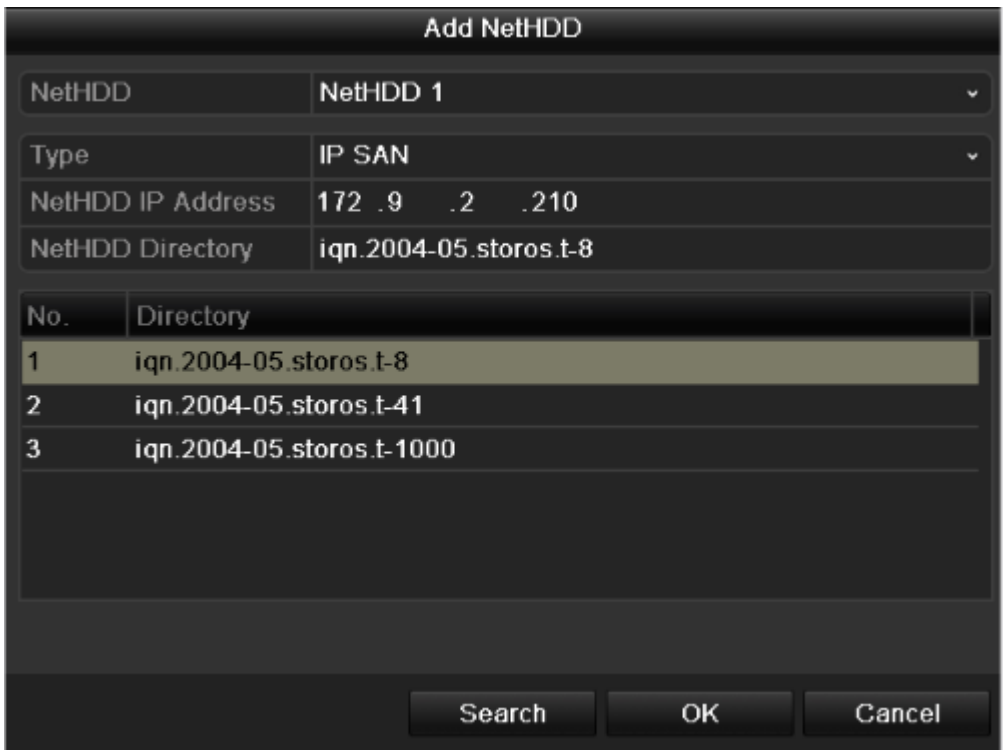
Note: Up to 8 NAS disks can be added.



• Add IP SAN:

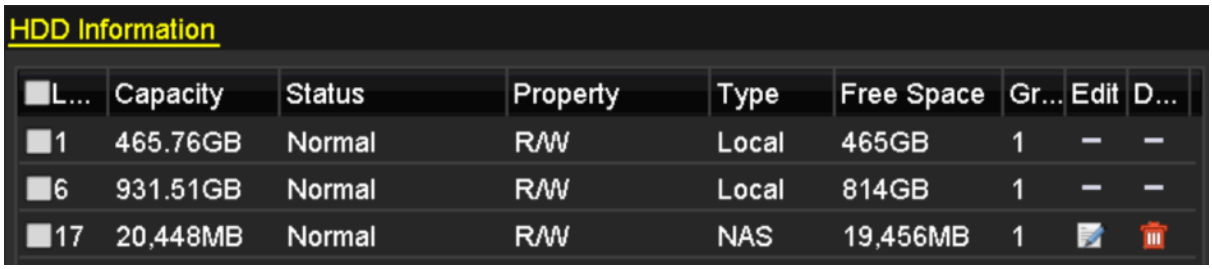
1) Enter the NetHDD IP address in the text field.
2) Click the **Search** button to search the available IP SAN disks.
3) Select the IP SAN disk from the list shown below.
4) Click the **OK** button to add the selected IP SAN disk

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



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.



10.3 Managing HDD Group

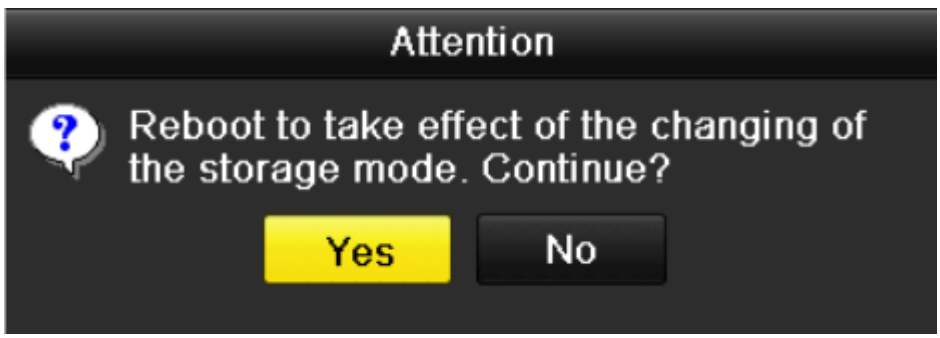
10.3.1 Setting HDD Groups

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

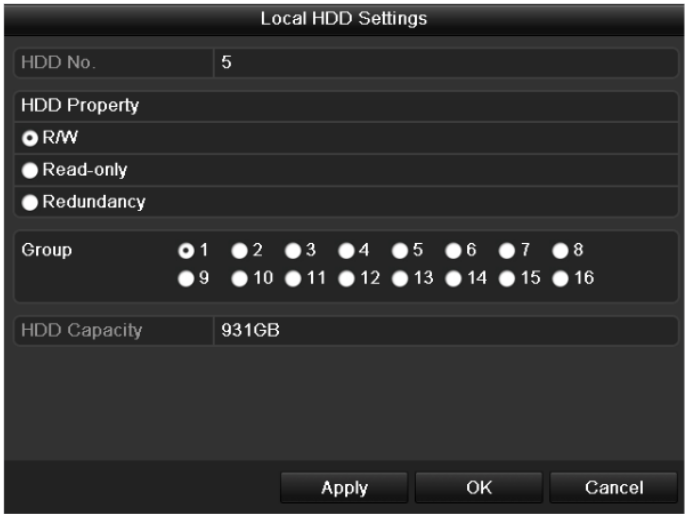
Steps:

1. Enter the Storage Mode interface.
   Menu > HDD > Advanced
2. Set the **Mode** to Group, as shown in Figure 12. 11.

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



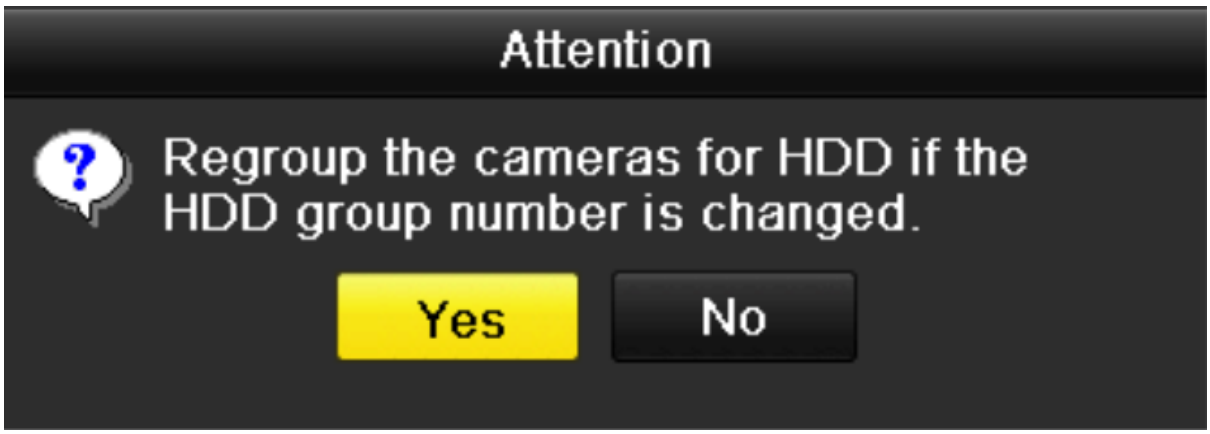
4. Click the **Yes** button to reboot the device to activate the changes.
5. After reboot of device, enter the HDD Information interface.
   Menu > HDD> General
6. Select HDD from the list and click icon to enter the Local HDD Settings interface



7. Select the Group number for the current HDD.

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

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



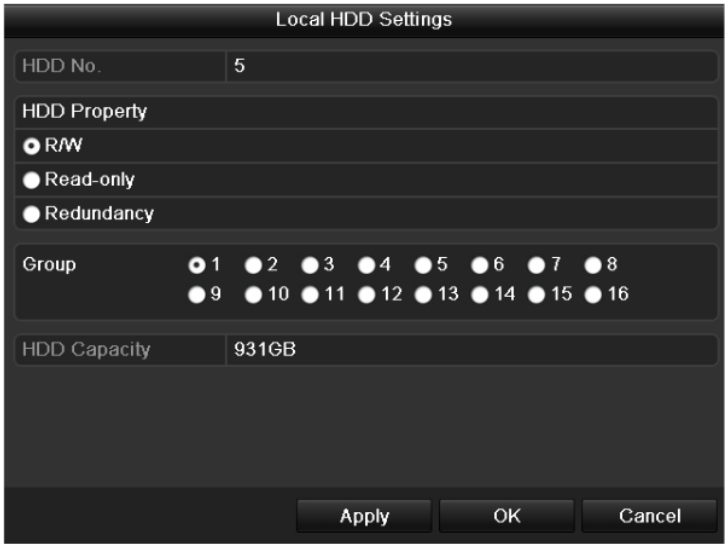
9. In the pop-up Attention box, click the **Yes** button to finish the settings.

10.3.2 Setting HDD Property

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 *10.3.1 Setting HDD Groups*). A HDD can be set to read-only to prevent important recorded files from being overwritten when the HDD becomes full in overwrite recording mode. When the HDD property is set to redundancy, the video can be recorded both onto the redundancy HDD and the R/W HDD simultaneously so as to ensure high security and reliability of video data.

Steps:

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



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.

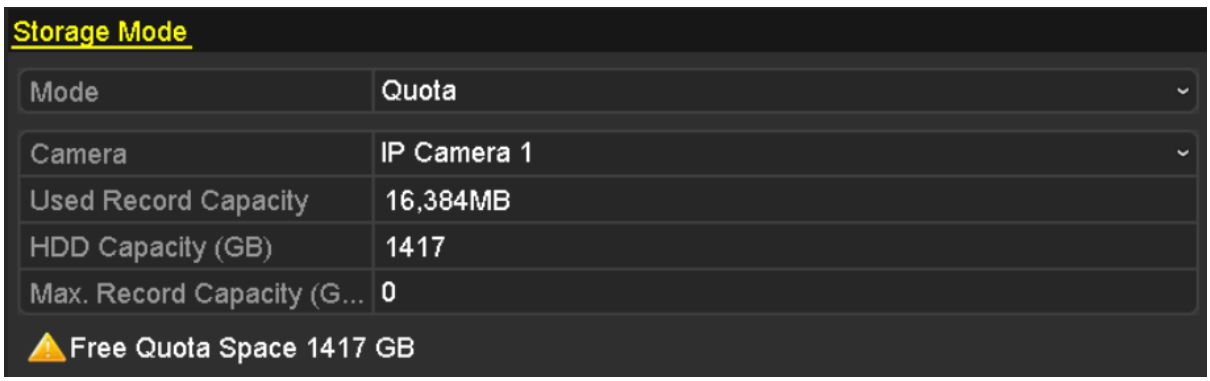
Note: At least 2 hard disks must be installed on your NVR when you want to set a HDD to Redundancy, and there is one HDD with R/W property.

10.4 Configuring Quota Mode

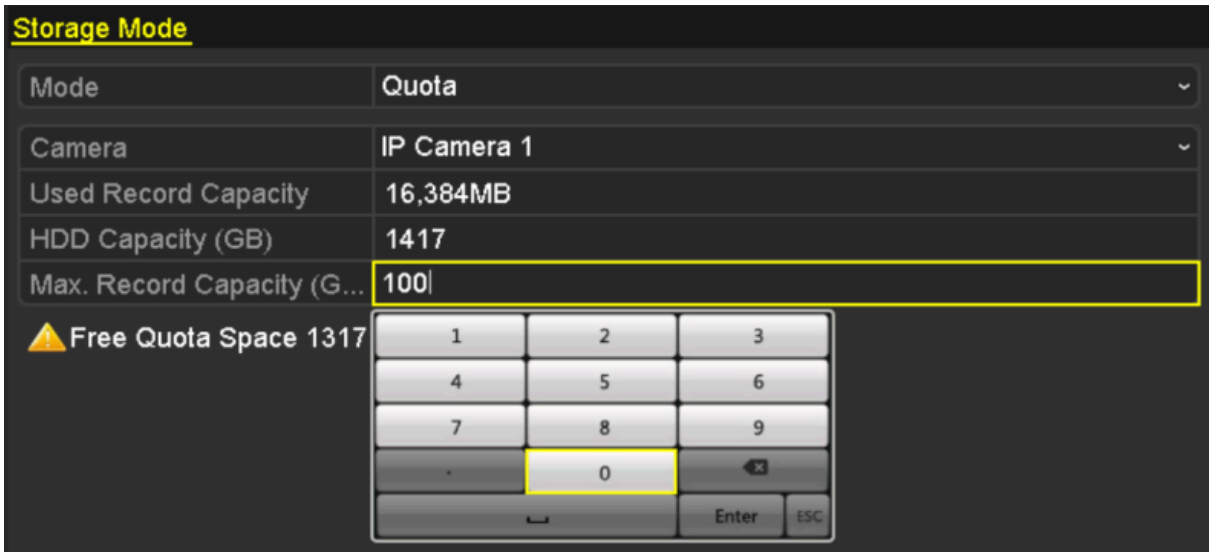
Each camera can be configured with allocated quota for the storage of recorded files.

Steps:

1. Enter the Storage Mode interface.
   Menu > HDD > Advanced
2. Set the **Mode** to Quota
   The NVR must be rebooted to enable the changes to take effect.



3. Select a camera for which you want to configure quota.
4. Enter the storage capacity in the text fields of **Max. Record Capacity (GB)**



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.

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.

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

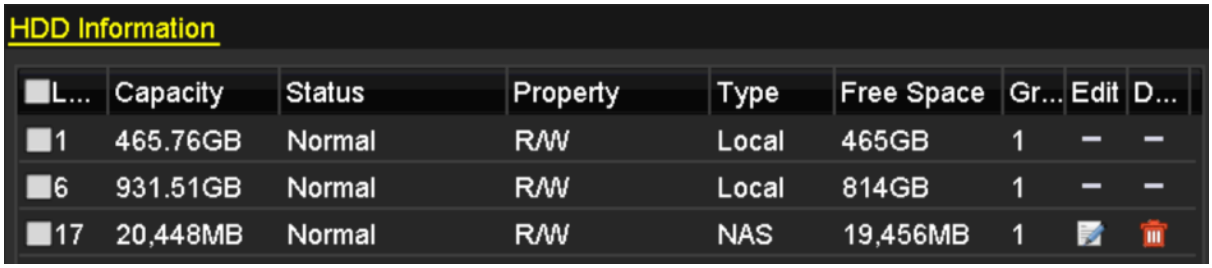
10.5 Checking HDD Status

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

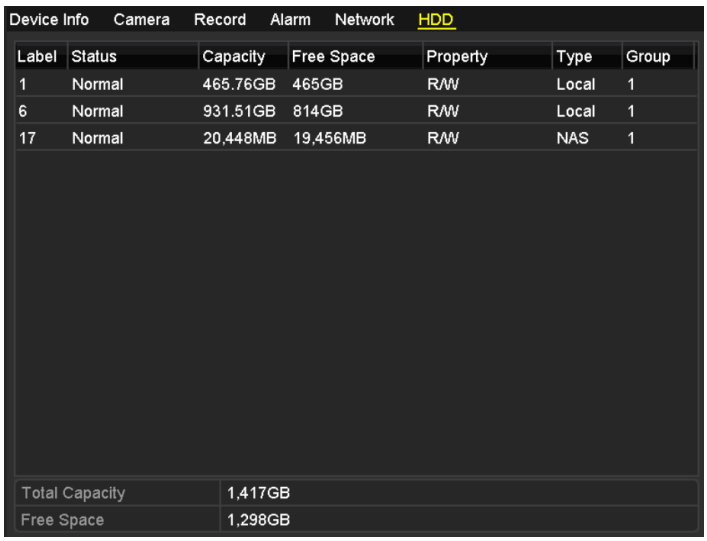


Note: If the status of HDD is *Normal* or *Sleeping*, it works normally. If the status is *Uninitialized* or *Abnormal*, please initialize the HDD before use. And if the HDD initialization is failed, please replace it with a new one.

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



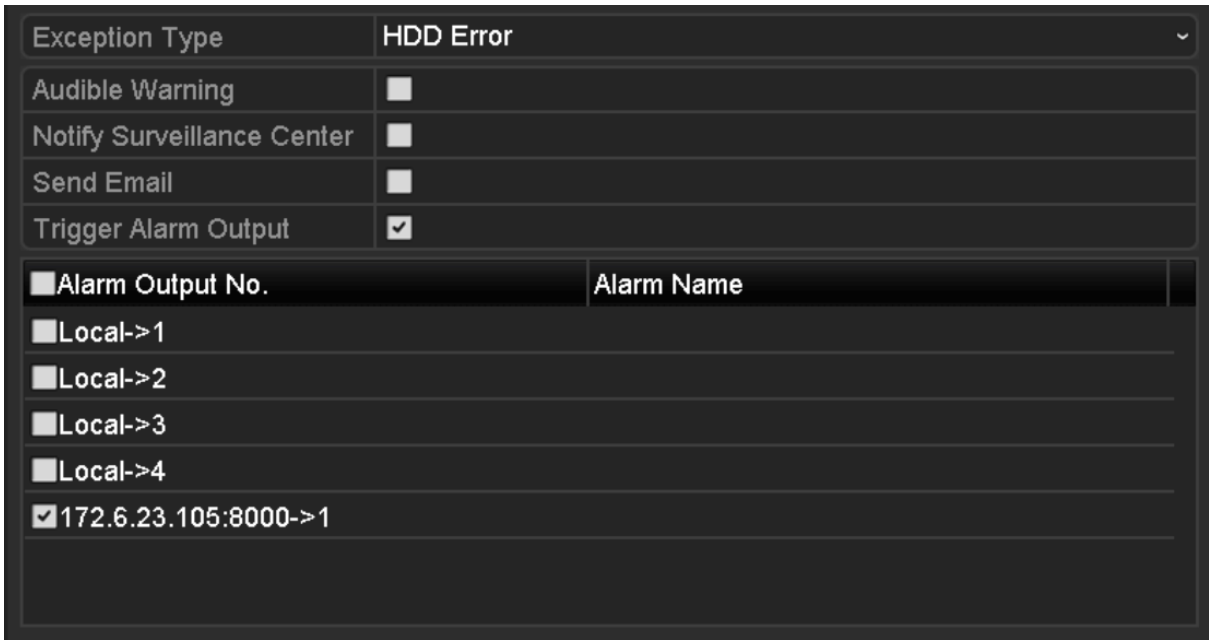
10.6 Configuring HDD Error Alarms

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).

Note: The alarm type can be selected to: Audible Warning, Notify Surveillance Center, Send Email and Trigger Alarm Output. Please refer to *7.5 Setting Alarm Response Actions.*



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

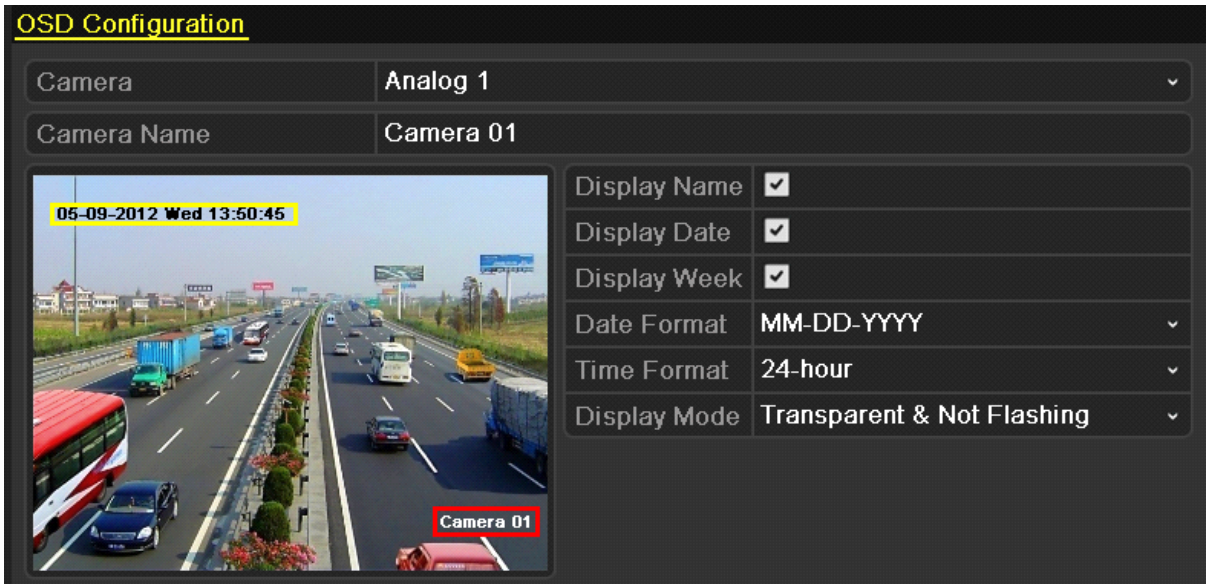
11.0 Camera Settings

11.1 Configuring OSD Settings

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.



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.

11.2 Configuring Privacy Mask

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

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.

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.

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

11.3 Configuring Video Parameters

Steps:

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

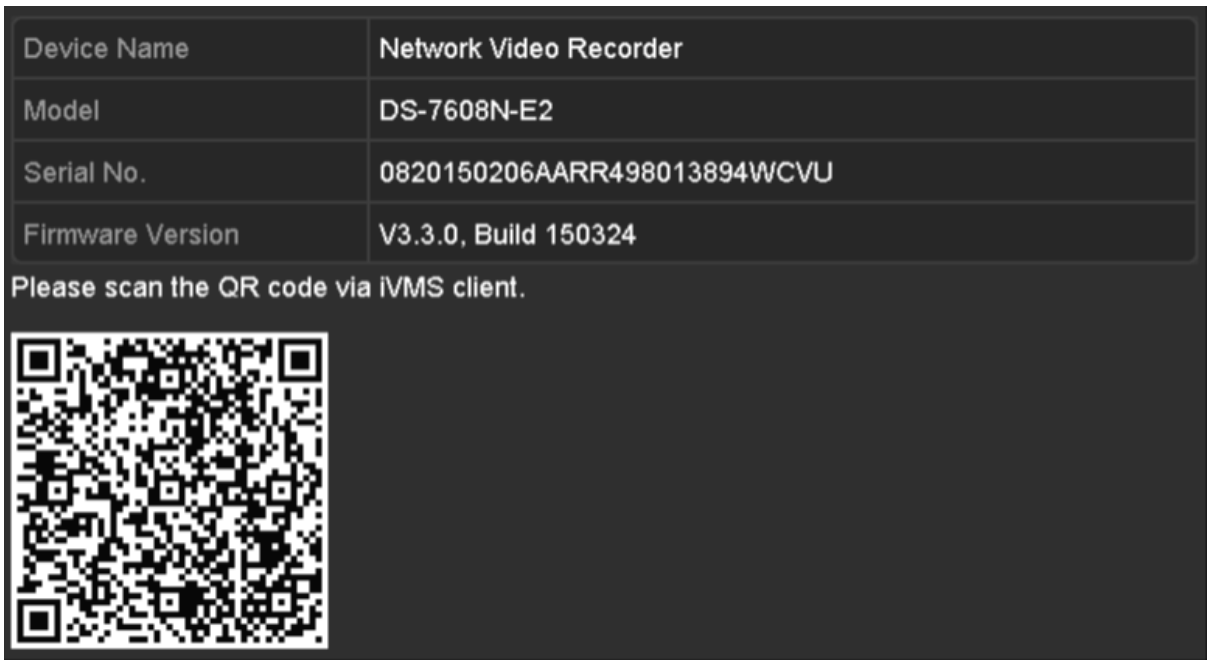
2. Select the camera to set image parameters.
3. You can click on the arrow to change the value of each parameter.
4. Click the **Apply** button to save the settings.

12.0 NVR Management and Maintenance

12.1 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.

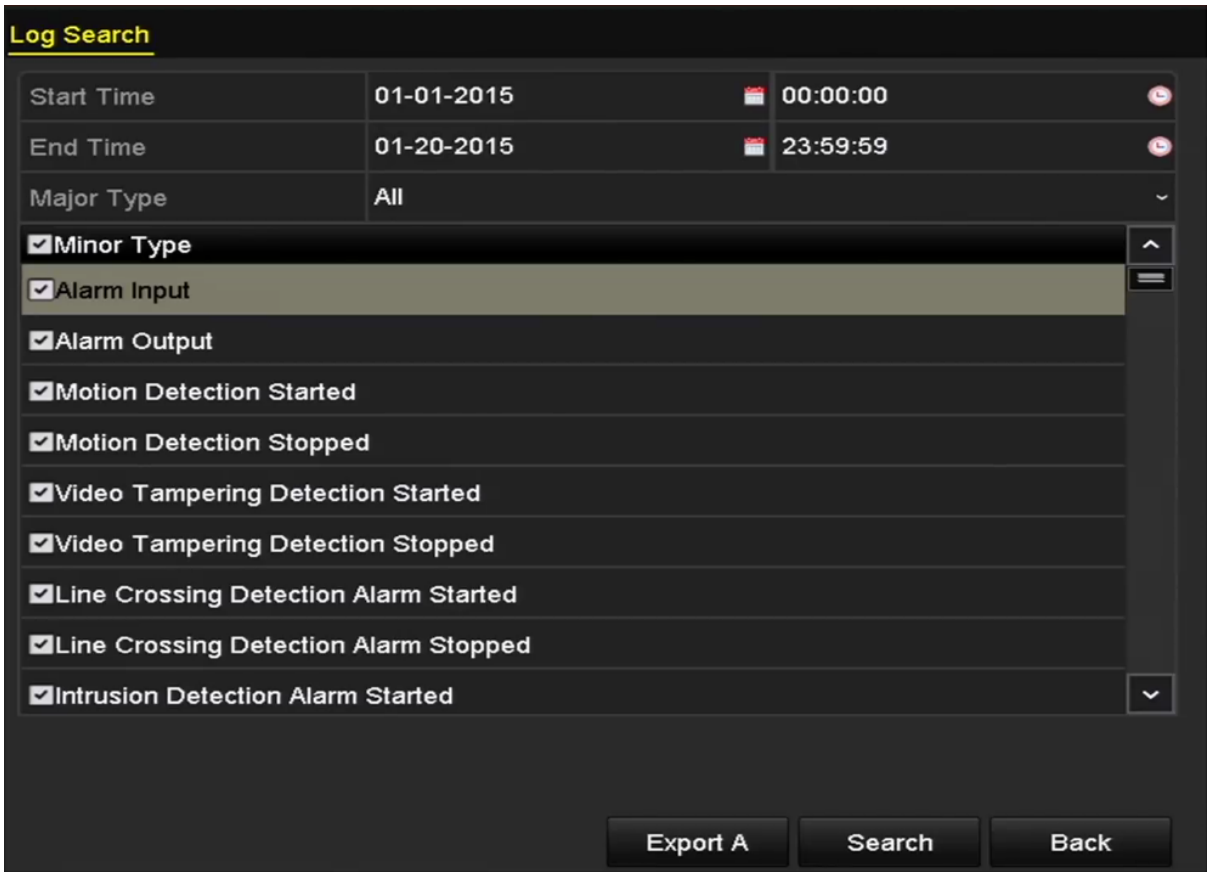


12.2 Searching & Export Log Files

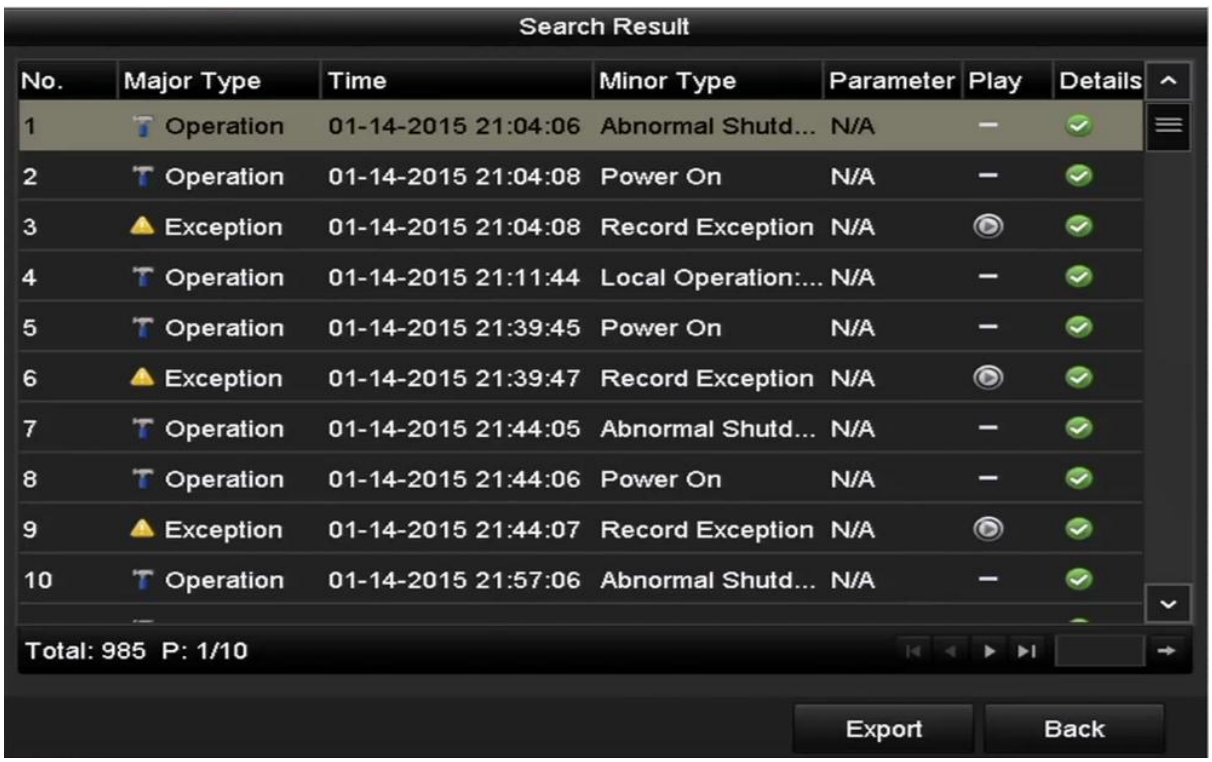
The operation, alarm, exception and information of the NVR can be stored in log files, which can be viewed and exported at any time.

Steps:

1. Enter the Log Search interface.
   Menu > Maintenance > Log Information

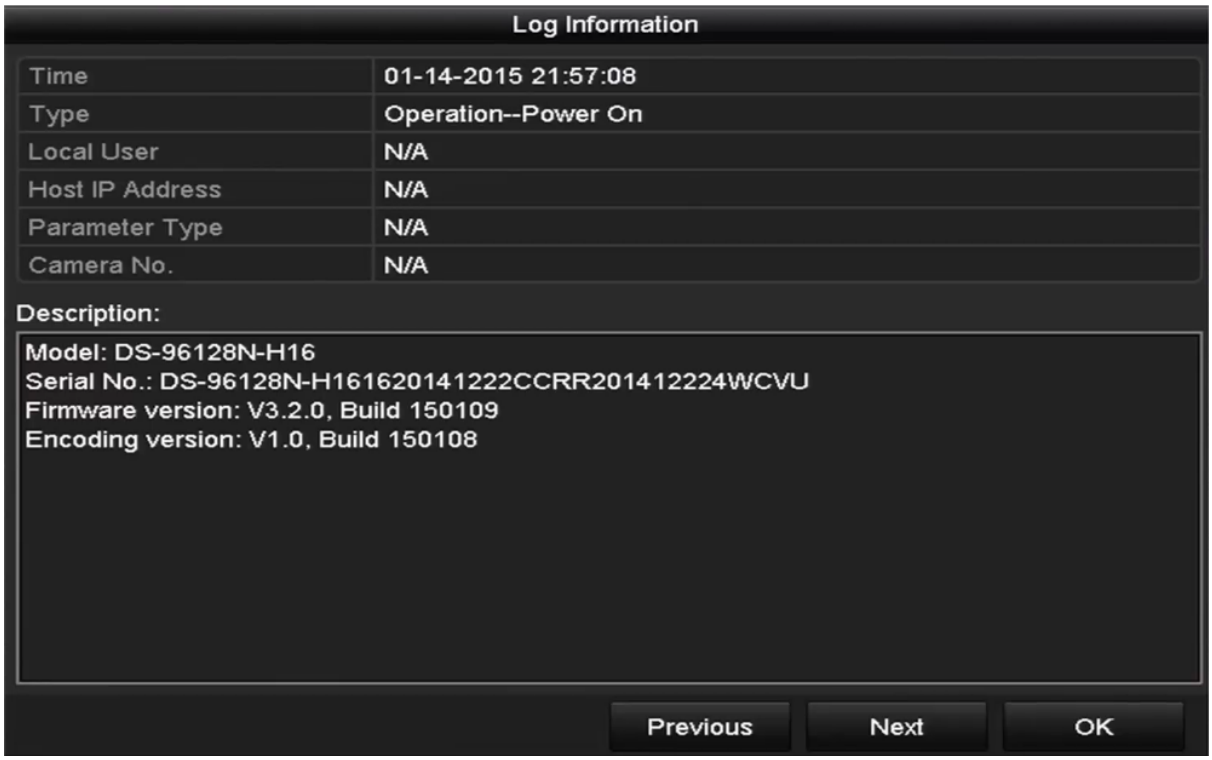


2. Set the log search conditions to refine your search, including the Start Time, End Time, Major Type and Minor Type.
3. Click the **Search** button to start search log files.
4. The matched log files will be displayed on the list shown below.

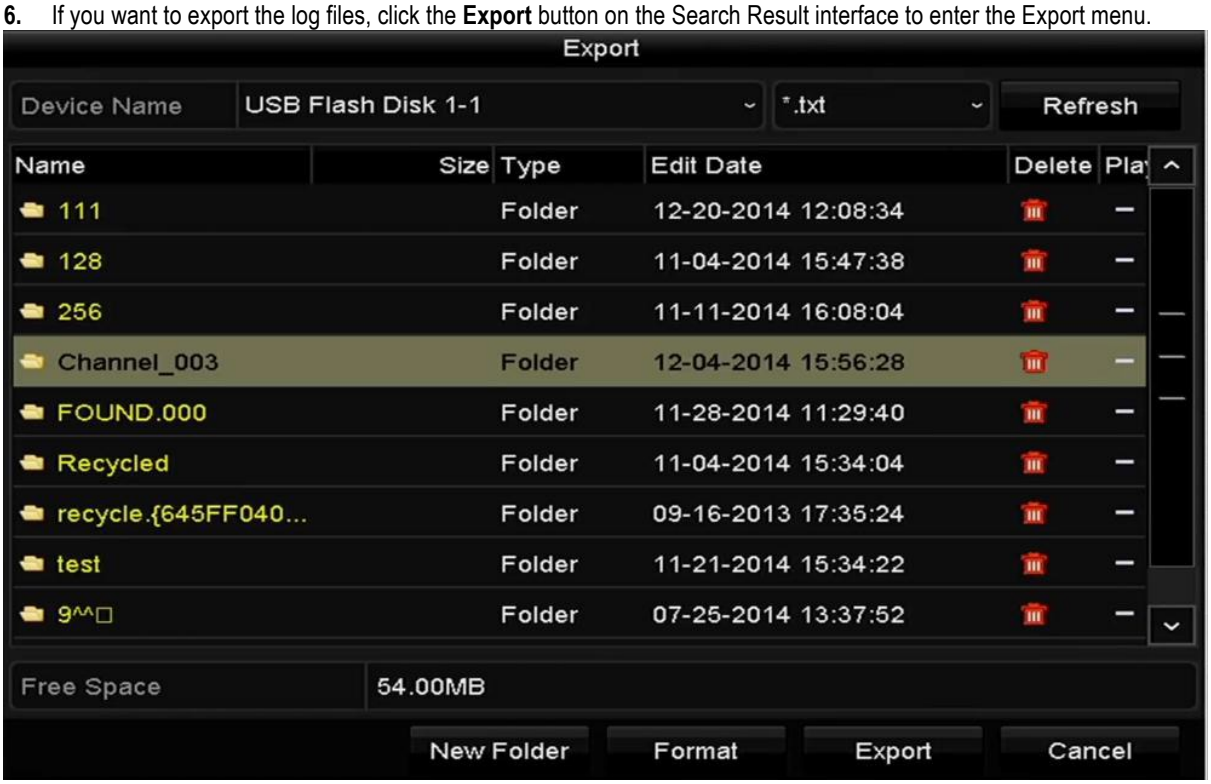


Note: Up to 2000 log files can be displayed each time.

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



6. If you want to export the log files, click the **Export** button on the Search Result interface to enter the Export menu.



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.

Note: Please connect the backup device to NVR before operating log export

12.3 Importing/Exporting IP Camera Info

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:

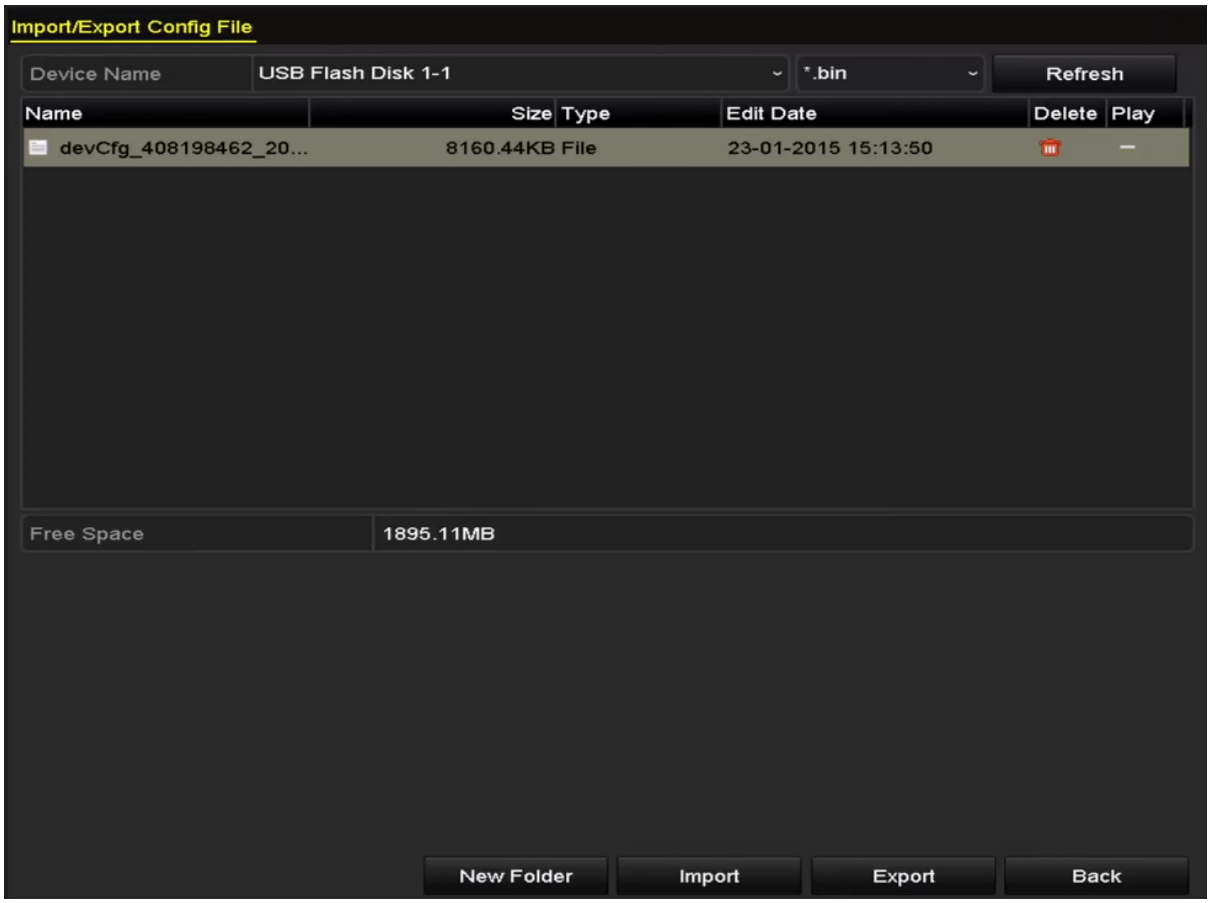
1. Enter the camera management interface.
   Menu > Camera > IP Camera Import/Export
2. Click the IP Camera Import/Export tab, the content of detected plugged external device appears.
3. Click the **Export** button to export configuration files to the selected local backup device.
4. To import a configuration 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.

12.4 Importing/Exporting Configuration Files

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



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.

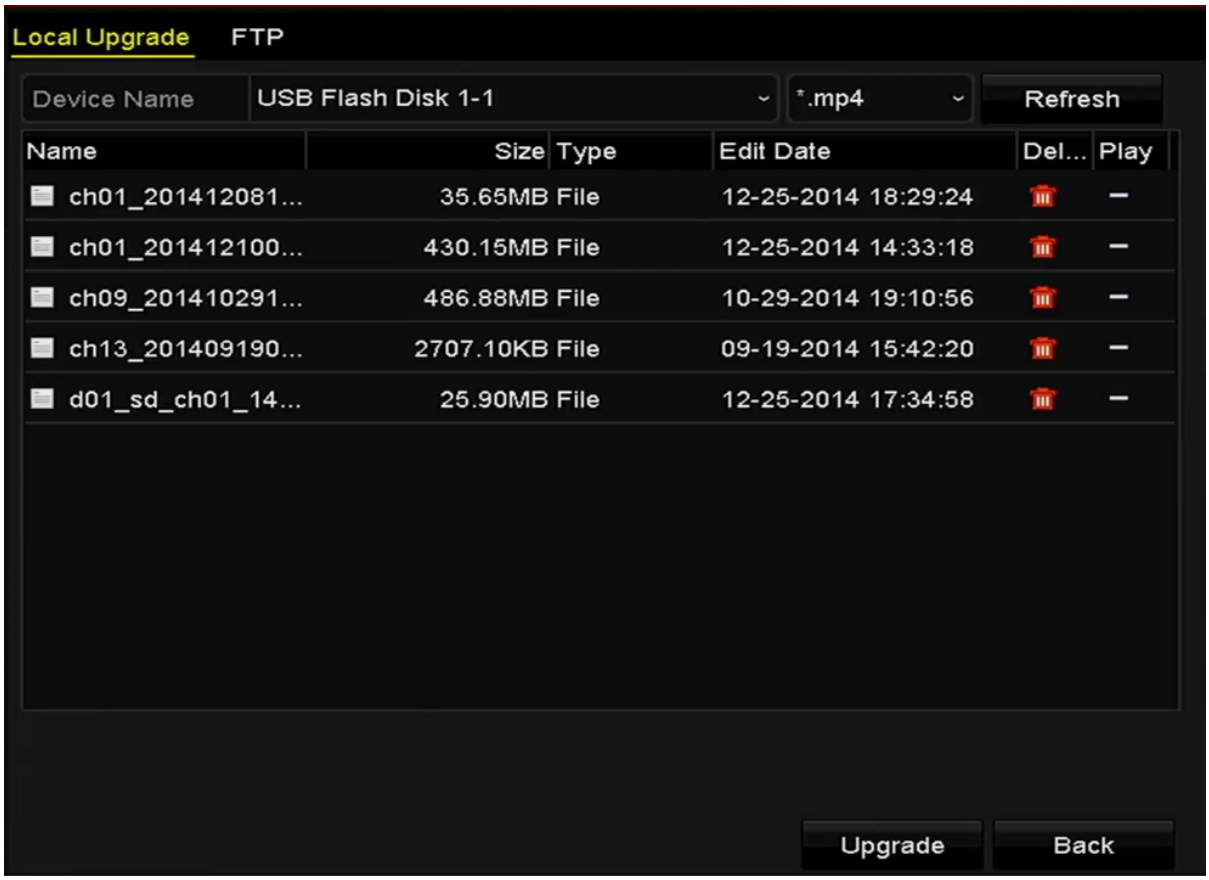
12.5 Upgrading System

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

12.5.1 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



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.

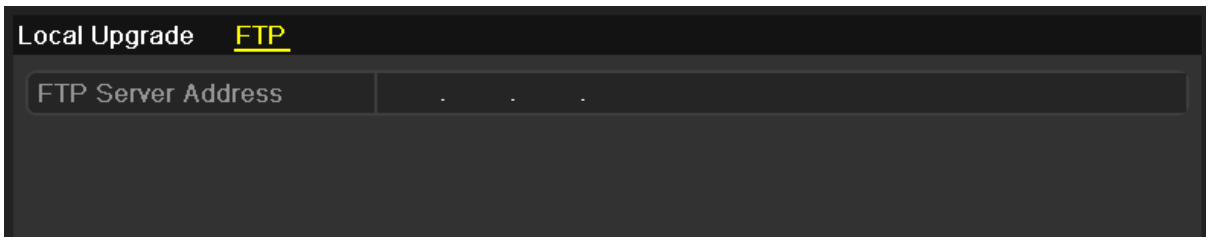
12.5.2 Upgrading by FTP

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

Note: 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



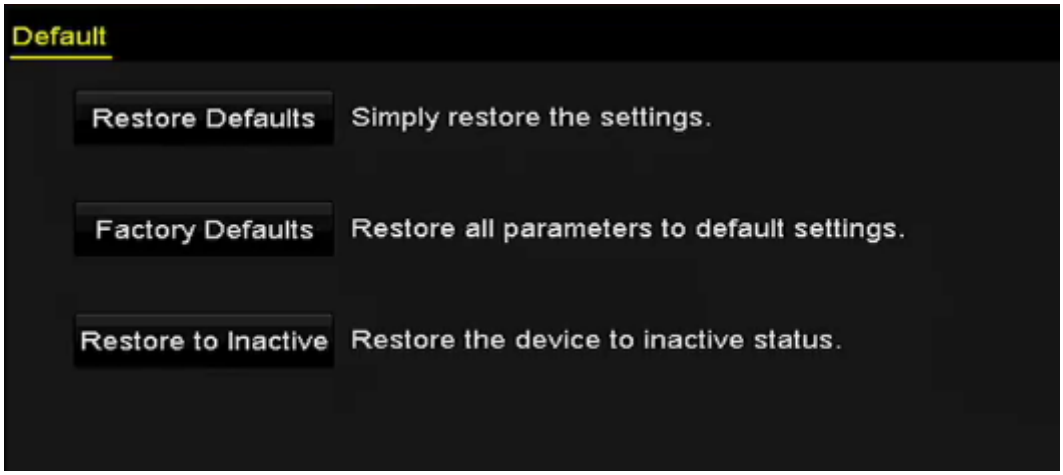
3. Enter the FTP Server Address in the text field.
4. Click the **Upgrade** button to start upgrading.

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

12.6 Restoring Default Settings

Steps:

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



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.

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

13.0 Others

13.1 Configuring RS-232 Serial Port

The RS-232 is provided by the SW-0820154N and SW-0820158N series NVR only.

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

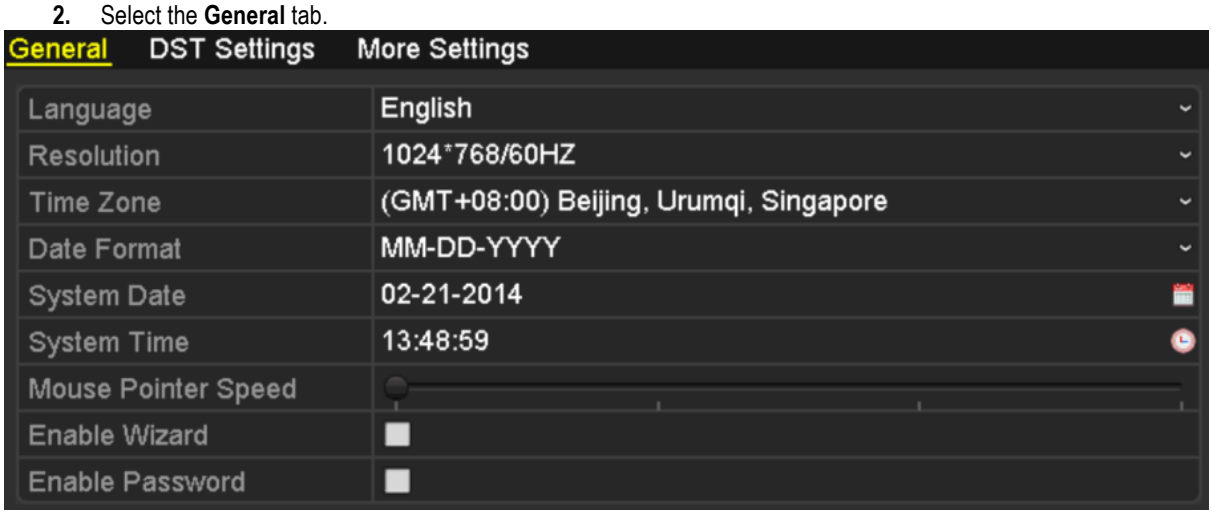
2. Configure RS-232 parameters, including baud rate, data bit, stop bit, parity, flow control and usage.
3. Click the **Apply** button to save the settings.

13.2 Configuring General Settings

You can configure the BNC output standard, VGA output resolution, mouse pointer speed through the Menu >Configuration > General interface.

Steps:

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

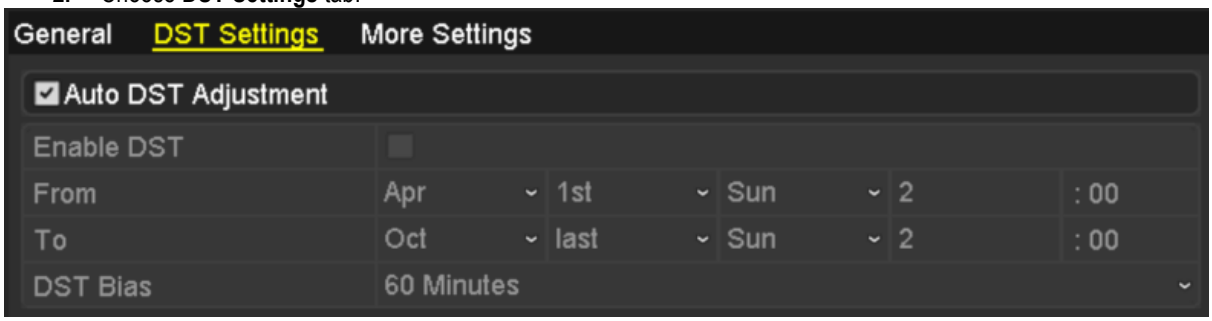


3. Configure the following settings:
   • **Language:** The default language used is *English*.
   • **Resolution:** Select the resolution for the video output, which must be the same with the resolution of the monitor screen.
   • **Time Zone:** Select the time zone.
   • **Date Format:** Select the 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.

13.3 Configuring DST Settings

Steps:

1. Enter the General Settings interface.
   Menu >Configuration>General
2. Choose **DST Settings** tab.

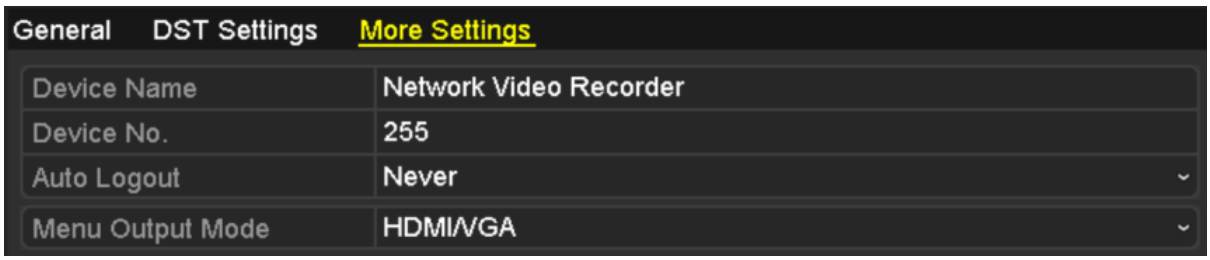


You can check the checkbox before the Auto DST Adjustment item.
Or you can manually check the Enable DST checkbox, and then you choose the date of the DST period.

13.4 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.



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.
   • **Menu Output Mode:** You can choose the menu display on different video output. By default, only HDMITM /VGA is selectable.

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

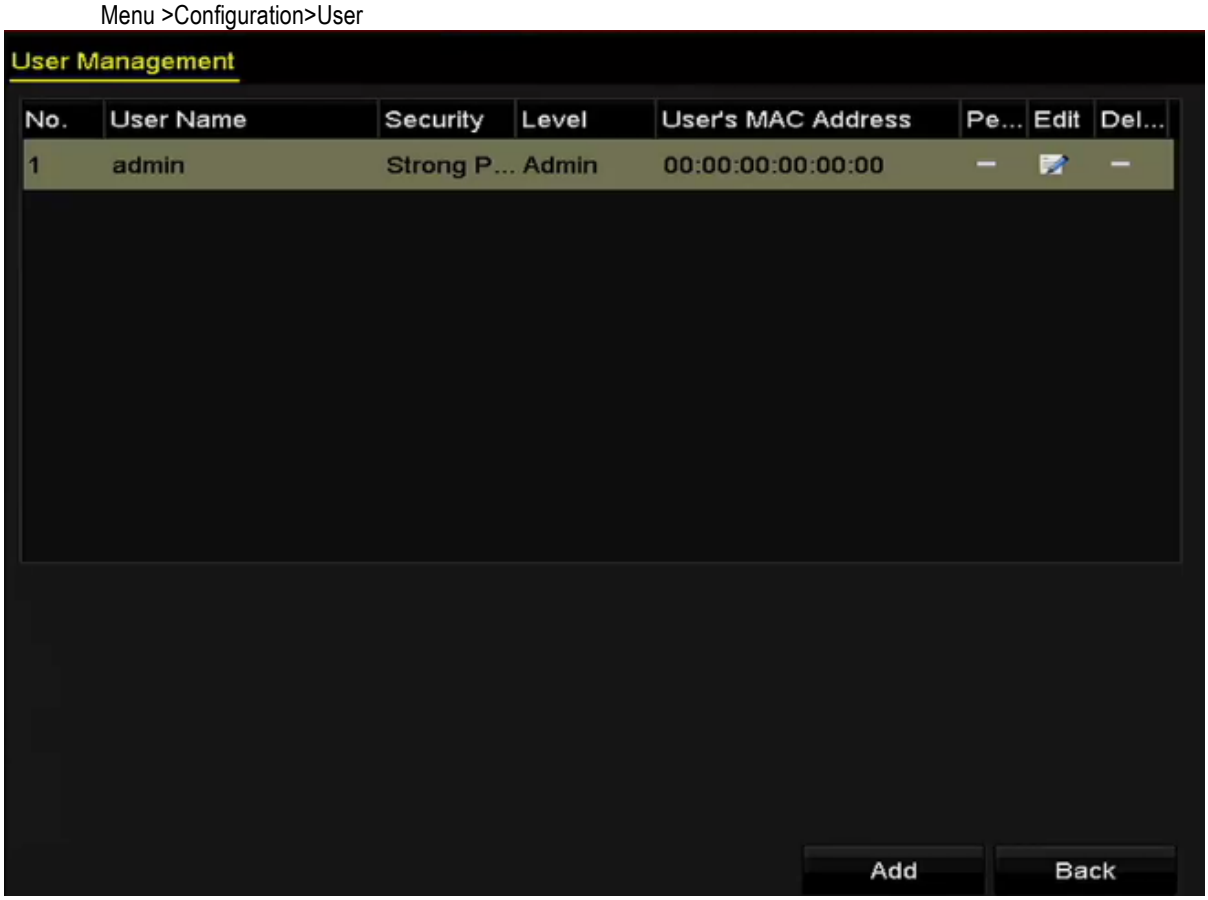
13.5 Managing User Accounts

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

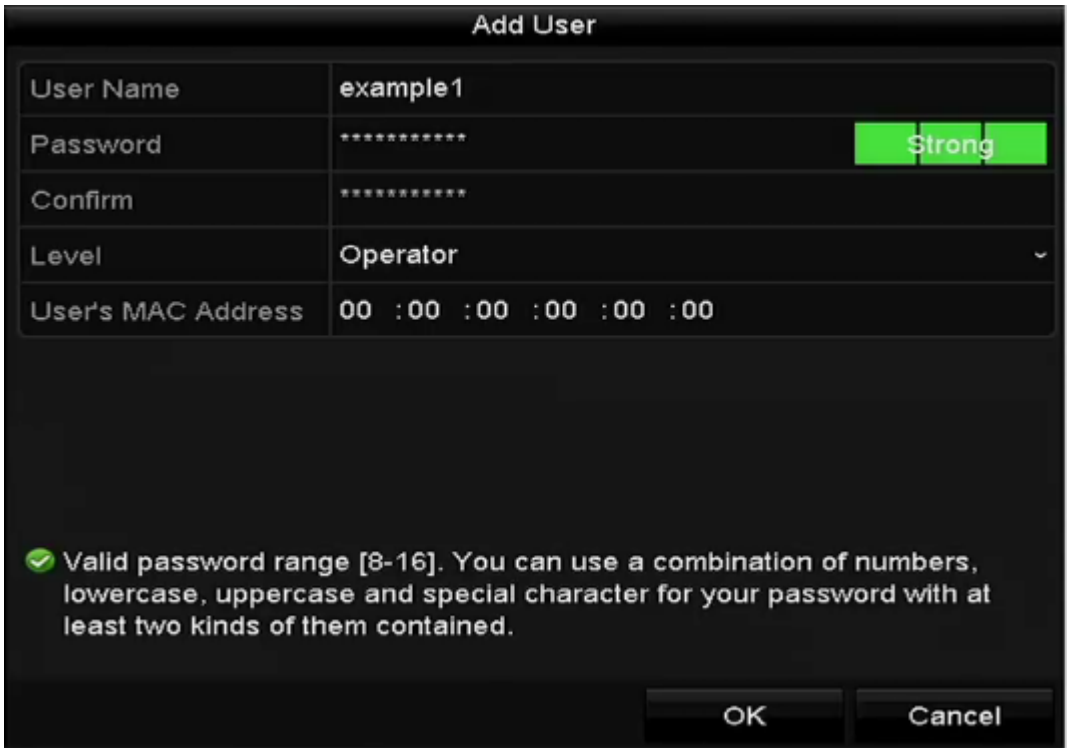
13.5.1 Adding a User

Steps:

1. Enter the User Management interface.
   Menu >Configuration>User



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

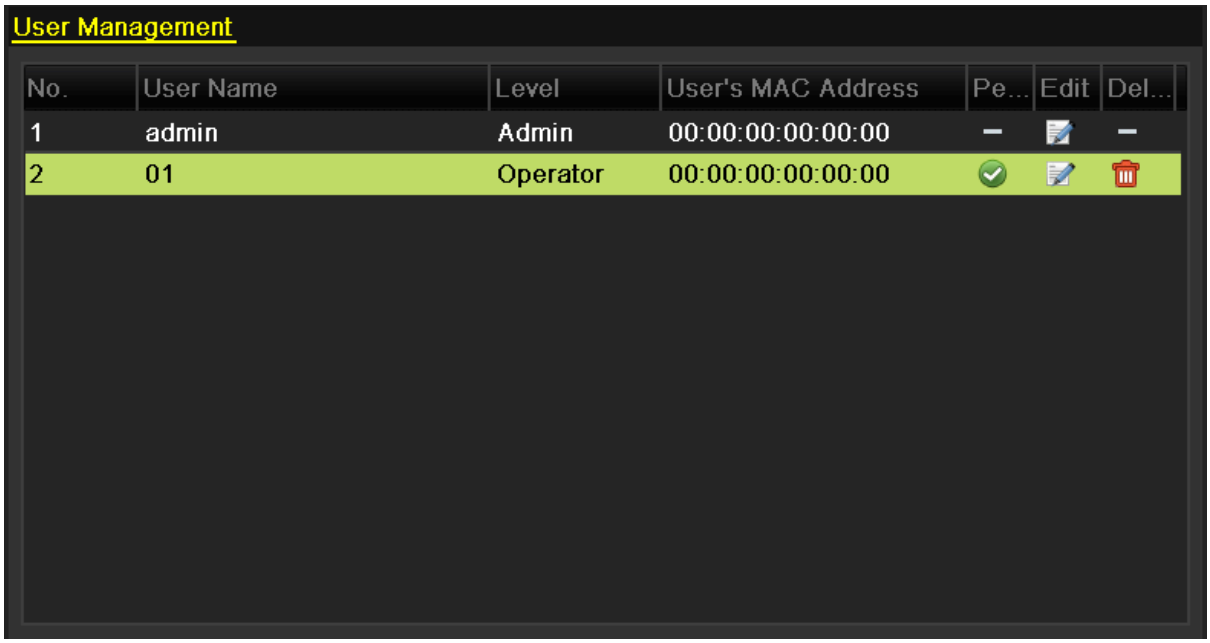


3. Enter the information for new user, including **User Name**, **Password**, **Confirm**, **Level** and **User's MAC Address**.

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 15. 7.



5. Select the user from the list and then click the button to enter the 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 theselected 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).

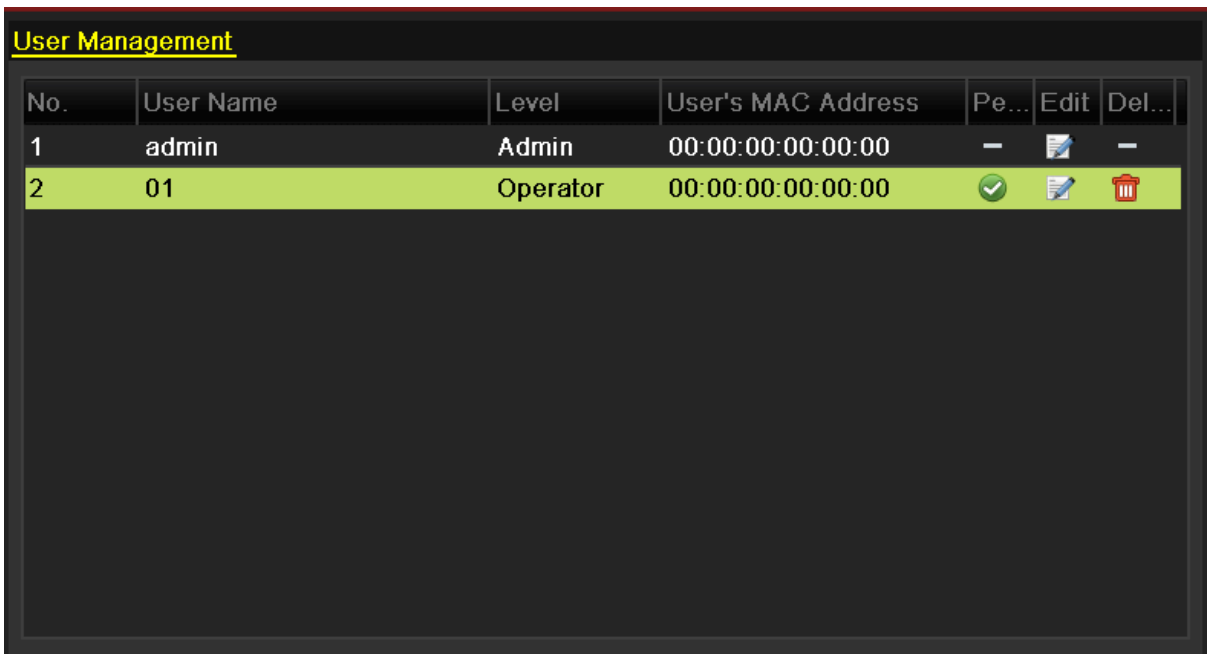
7. Click the **OK** button to save the settings and exit interface.

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

13.5.2 Deleting a User

Steps:

1. Enter the User Management interface.
   Menu >Configuration>User
2. Select the user to be deleted from the list



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

13.5.3 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
3. Click the icon to enter the 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 the 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 the user management interface to edit the permission.