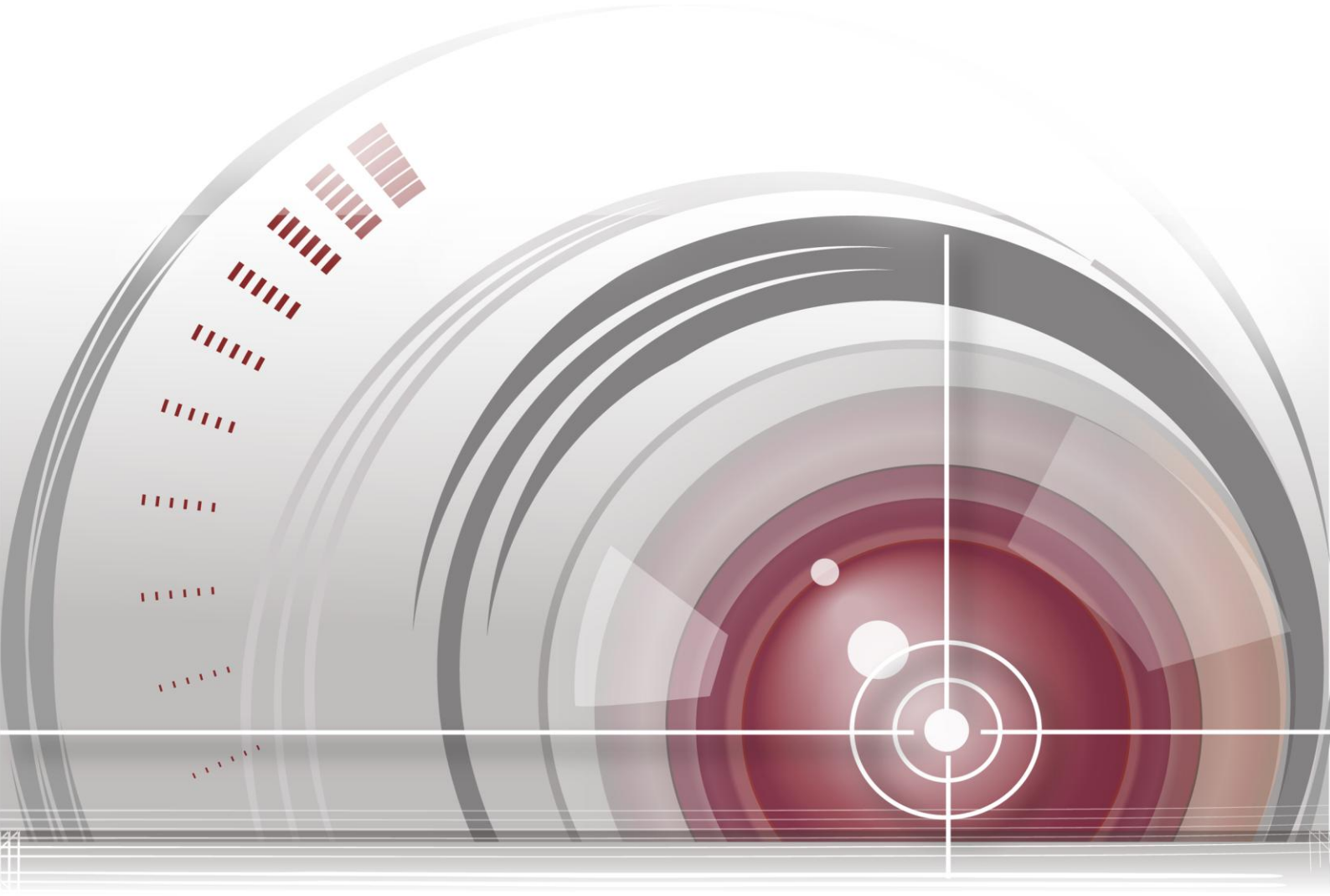


Network Video Recorder

User Manual

Regulatory information

FCC information

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

Note: This product has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This product generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this product does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

—Consult the dealer or an experienced radio/TV technician for help.

This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.

FCC conditions

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

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

EU Conformity Statement

CE

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the Low Voltage Directive 2006/95/EC, the R&TTE Directive 1999/5/EC, the RoHS Directive 2011/65/EU.

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

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

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.

Manufacturer	Type	Capacity
Seagate	WD5000LUCT	500G
Seagate	WD10JUCT	1T
Toshiba	MQ01ABD050V	500G
Toshiba	MQ01ABD100V	1T

Figure 1. 1 Recommended HDDs

- 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.

CHANGE THE DEFAULT PASSWORD

*The default password (12345) for the Admin account is for first-time log-in purposes only. You **must** change this default password to better protect against security risks, such as the unauthorized access by others to the product that may prevent the product from functioning properly and/or lead to other undesirable consequences.*

For your privacy, we strongly recommend changing the password to something 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.

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

Trademarks and Registered Trademarks

- Windows and Windows mark are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.
- HDMI, HDMI mark and High-Definition Multimedia Interface are trademarks or registered trademarks of HDMI Licensing LLC.
- The products contained in this manual are authorized by HDMI Licensing LLC with the use right of the HDMI technology.

- VGA is the trademark of IBM.
- UPnP™ is a certification mark of the UPnP™ Implementers Corporation.
- Other names of companies and product contained in this manual may be trademarks or registered trademarks of their respective owners.

Thank you for purchasing our product. If there is any question or request, please do not hesitate to contact dealer.
The figures in the manual are for reference only.

This manual is applicable to the model **LTN82XX-W**.

Product Key Features

General

- Connectable to network cameras, network dome and encoders.
- Connectable to network cameras like HIKVISION, ACTI, Arecont, AXIS, Bosch, Brickcom, Canon, PANASONIC, Pelco, SAMSUNG, SANYO, SONY, Vivotek and ZAVIO, and cameras that adopt ONVIF or PSIA protocol.
- Connectable to the smart IP cameras.
- Each channel supports dual-stream.
- Up to 8 network cameras can be connected.
- Independent configuration for each channel, including resolution, frame rate, bit rate, image quality, etc.
- The quality of the input and output record is configurable.

Local Monitoring

- Support HDMI™ output.
- HDMI™ output at up to 1920×1080 resolution.
- Multiple screen display in live view is supported, and the display sequence of channels is adjustable.
- Live view screen can be switched in group, and manual switch and automatic switch live view are also provided, and the interval of automatic switch can be adjusted.
- Quick setting menu is provided for live view.
- Motion detection, video tampering, VCA (Video Content Analysis) alarm, video exception alert and video loss alert functions.
- Privacy mask.
- Multiple PTZ protocols supported; PTZ preset, patrol and pattern.
- Zooming in by clicking the mouse and PTZ tracing by dragging mouse.

HDD Management

- Two kinds of HDD capacity are provided: 500G and 1T.
- 8 network disks (8 NAS disks, or 7 NAS disks + 1 IP SAN disk) can be connected.
- Support S.M.A.R.T. and bad sector detection.
- HDD quota management; different capacity can be assigned to different channel.

Recording and Playback

- Holiday recording schedule configuration.
- Continuous and event video recording parameters.
- Multiple recording types: manual, continuous, alarm, motion, motion | alarm, motion & alarm, and VCA.
- 8 recording time periods with separated recording types each day.
- Pre-record and post-record for alarm, motion detection for recording, and pre-record time for schedule and manual recording.
- Searching record files by events (alarm input/motion detection/VCA).
- Tag adding for record files, searching and playing back by tags.
- Locking and unlocking record files.
- Provide a playback interface with easy and flexible operation.
- Searching and playing back record files by camera No., recording type, start time, end time, etc.
- Smart search for the selected area in the video.
- Zooming in when playback.
- Reverse playback of multi-channel.
- Supports pause, play reverse, speed up, speed down, skip forward, and skip backward when playback, and locating by dragging the mouse.

- Up to 8-ch synchronous playback.

Backup

- Export video data by USB device.
- Export video clips when playback.
- Management and maintenance of backup devices.

Alarm and Exception

- Configurable arming time of alarm input/output.
- Alarm for video loss, motion detection, VCA, video tampering, HDD full, HDD error, network disconnected, IP confliction, illegal login and abnormal record.
- Alarm triggers full screen monitoring, audible warning, notifying surveillance center, sending email and alarm output.
- Manually restore default when system is abnormal.

Other Local Functions

- Operable by mouse.
- Three-level user management; admin user is allowed to create many operating accounts and define their operating permission, which includes the limit to access any channel.
- Operation, alarm, exceptions and log recording and searching.
- Manually triggering and clearing alarms.
- Import and export of device configuration information.

Network Functions

- 1 self-adaptive 10M/100M network interfaces is provided.
- IPv6 is supported.
- TCP/IP protocol, PPPoE, DHCP, DNS, DDNS, NTP, SADP, SMTP, SNMP, NFS, and iSCSI are supported.
- TCP, UDP and RTP for unicast.
- Auto/Manual port mapping by UPnP^{TM}.
- Extranet access by HiDDNS and Cloud P2P.
- Remote reverse playback via RTSP.
- Support accessing by the platform via ONVIF.
- Remote search, playback, download, locking and unlocking of the record files, and the breakpoint resume is supported for downloading files.
- Remote parameters setup; remote import/export of device parameters.
- Remote view of the device status, system logs and alarm status.
- Remote HDD formatting and program upgrading.
- Remote system restart and shutdown.
- Alarm and exception information can be sent to the remote host
- Remotely start/stop recording.
- Remotely start/stop alarm output.
- Remote PTZ control.
- Voice broadcasting.
- Embedded WEB server.

Development Scalability:

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

TABLE OF CONTENTS

Chapter 1 Introduction

1.1 Front Panel and Rear Panel

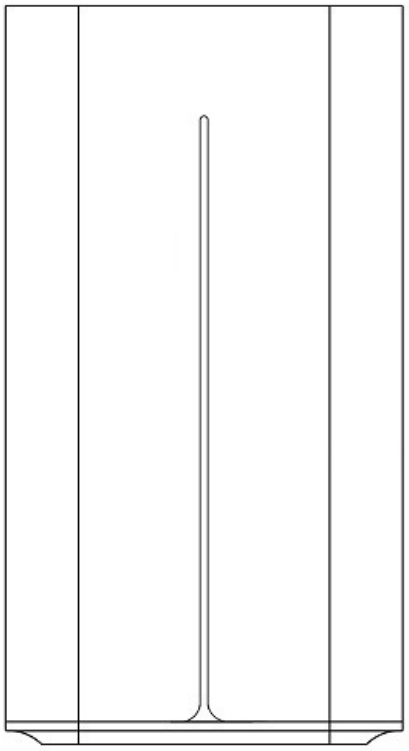


Figure 1. 1 Front Panel

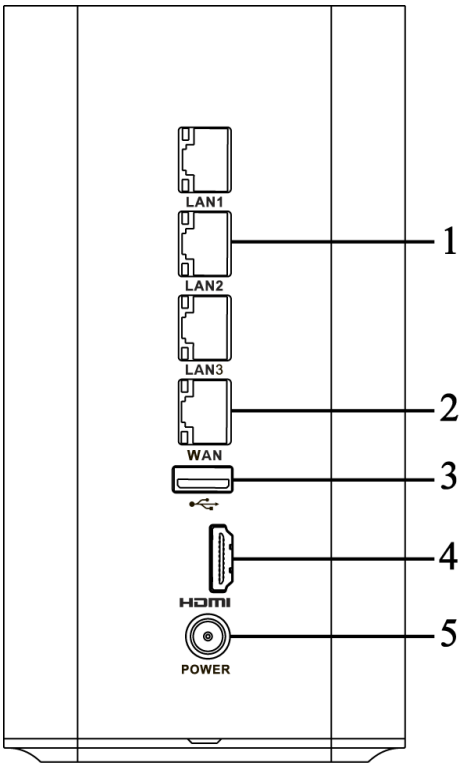


Figure 1. 2 Rear Panel

Table 1. 1 Description of Control Panel Buttons

No.	Name	Description
1	LAN Interface (1 ~ 3)	3 RJ-45 10 /100Mbps network interfaces for LAN (Local Area Networks).
2	WAN Interface	1 RJ-45 10 /100 Mbps network interface for WAN (Wide Area Networks).
3	USB Interface	Universal Serial Bus (USB) ports for additional devices such as USB mouse and USB writer.
4	HDMI	HDMI video output connector.
5	POWER	12VDC Power supply.

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

The operation of the mouse:

Table 1. 2 Description of the Mouse Control

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

1.3 Input Method Description

Figure 1. 3 Soft Keyboard

Description of the buttons on the soft keyboard:

Table 1. 3 Description of the Soft Keyboard Icons

Icon	Description	Icon	Description
A ~ Z	Letters	a / A	Lowercase/Uppercase
0 ~ 9	Numeric Buttons	.,!	Symbols
ESC	Exit		Backspace
	Space	Enter	Enter

Chapter 2 Getting Started

2.1 Starting Up and Shutting Down the NVR

Purpose:

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

Before you start:

1. Install a recommended HDD. For detailed steps, please refer to the Chapter *HDD Installation* of *Quick Start Guide*.
2. Establish the connection between the NVR and Internet via the WAN interface.
3. 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:

Step:

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.

During the starting up program, a splash screen appears on the monitor.

Shutting down the NVR

Steps:

1. Enter the Shutdown menu.

   Menu > Shutdown

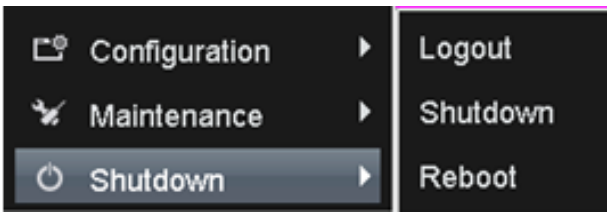


Figure 2. 1 Shutdown Menu

2. Click the **Shutdown** button.
3. Click the **Yes** button.
4. Unplug the power supply when the attention pops up.

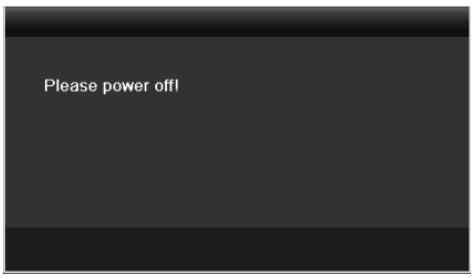


Figure 2. 2 Shutdown Attention

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 Using the Wizard for Basic Configuration

By default, the Setup Wizard starts once the NVR has loaded, as shown in Figure 2. 3.

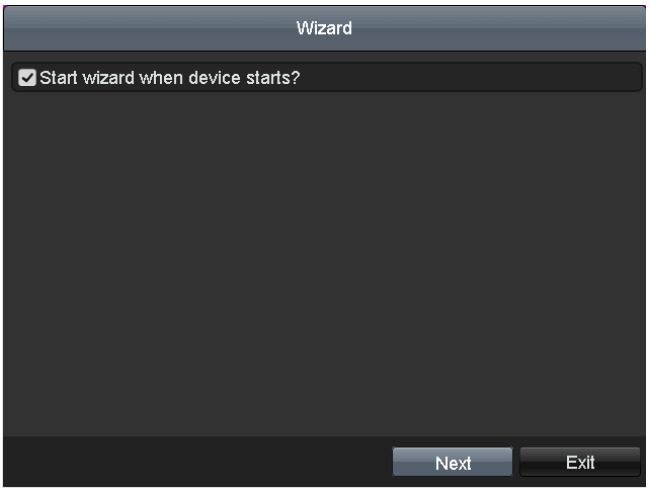


Figure 2. 3 Start Wizard Interface

Operating the Setup Wizard:

1. The Setup Wizard can walk you through some important settings of the NVR. If you do not want to use the Setup Wizard at that moment, click the **Cancel** button. You can also choose to use the Setup Wizard next time by leaving the "Start wizard when the device starts?" checkbox checked.
2. Click **Next** button on the Wizard window to enter the **Login** window, as shown in Figure 2. 4.

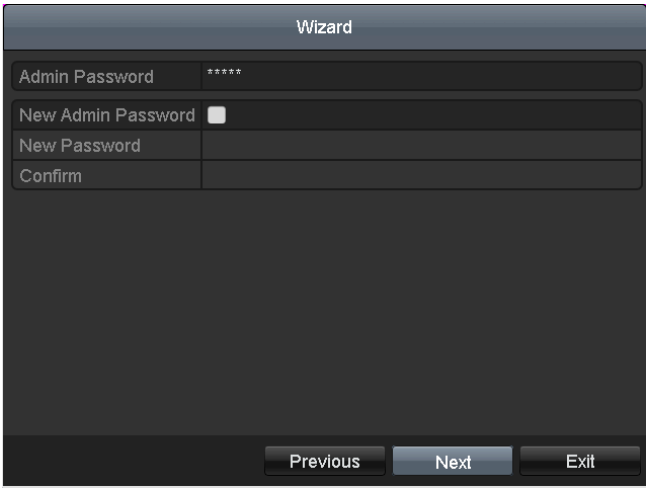


Figure 2. 4 Login Window

3. Input the **Admin Password**. By default, the password is 12345.

The default password (12345) for the Admin account is for first-time log-in purposes only. You must change this default password to better protect against security risks, such as the unauthorized access by others to the product that may prevent the product from functioning properly and/or lead to other undesirable consequences.

4. To change the admin password, check the **New Admin Password** checkbox. Input the **New Password** and **Confirm** the password in the given fields.

For your privacy, we strongly recommend changing the password to something 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.

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

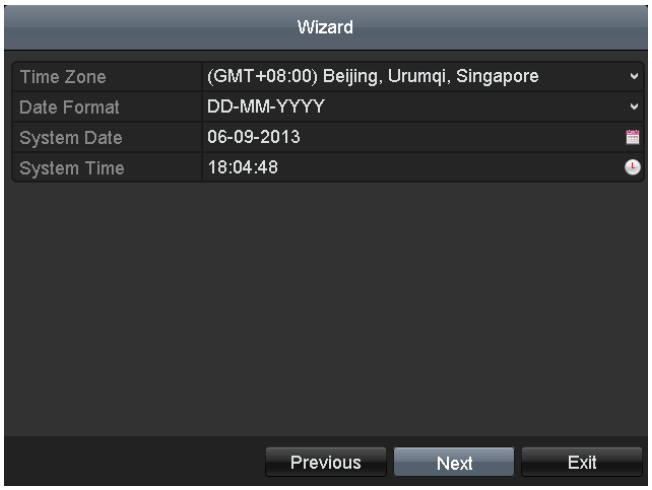


Figure 2. 5 Date and Time Settings

6. After the time settings, click **Next** button which takes you to the WAN Setup Wizard window, as shown in Figure 2. 6.

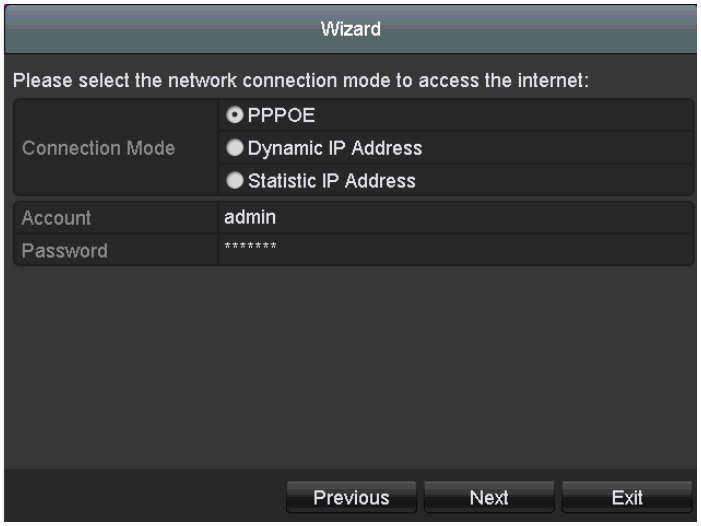


Figure 2. 6 WAN Settings

7. Select the **Connection Mode** as **PPPoE** and input **Account** and **Password**.
8. Click **Next** button to enter WIFI settings interface, as shown in Figure 2. 7.

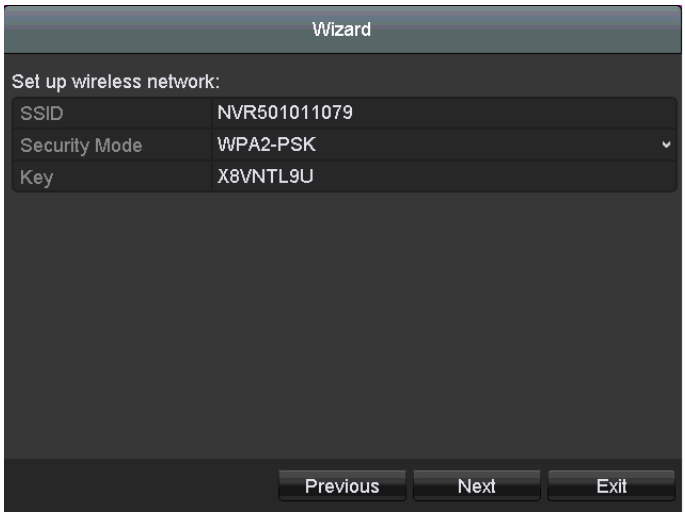


Figure 2. 7 WIFI Settings

9. Input **SSID** and select **Security Type**. Input **Network Security Key** if Security Type is no set as Disable.
10. Click **Next** button which takes you to the General Network Setup Wizard window, as shown in Figure 2. 8.

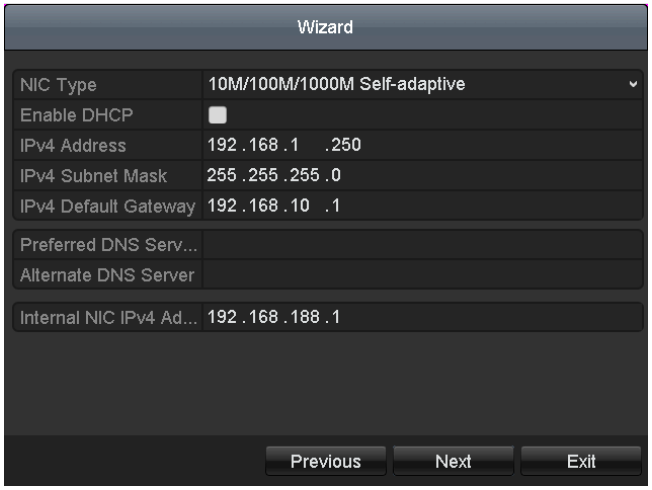


Figure 2. 8 General Network Configuration

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

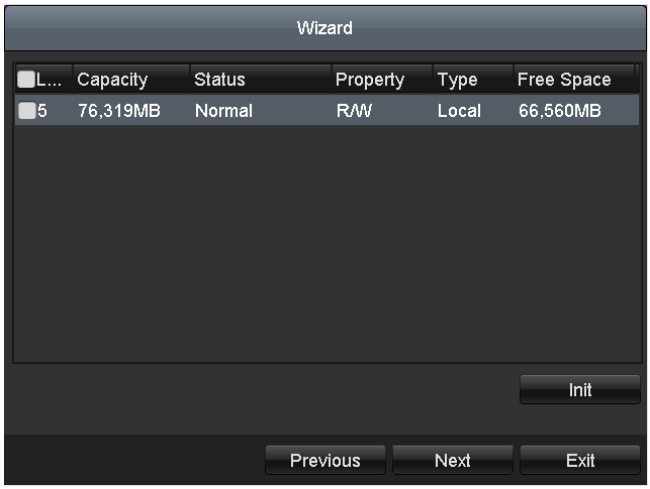


Figure 2. 9 HDD Management

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

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

NOTE

Establish network connection between IP cameras and NVR. For detailed steps, please refer to *before you start* of *Section 2.3.1 Adding the Online IP Cameras*.

14. Click **Search** to find online IP camera. Select the IP camera to be added, and click the **Add** button.

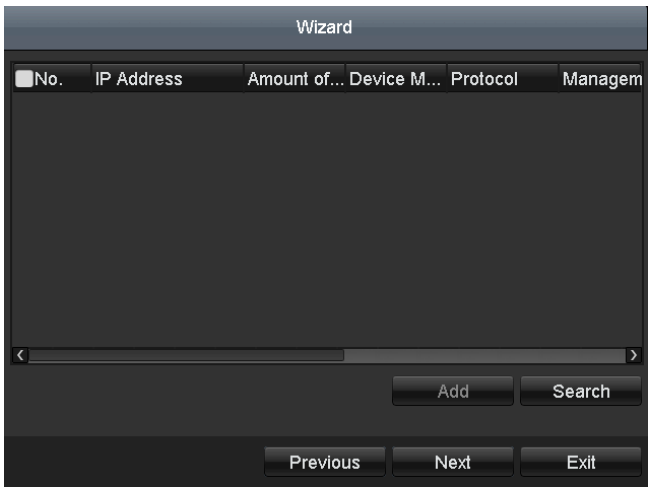


Figure 2. 10 Search for IP Cameras

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

Figure 2. 11 Record Settings

16. Click **Copy** to copy the settings to other channels, as shown in Figure 2. 12.

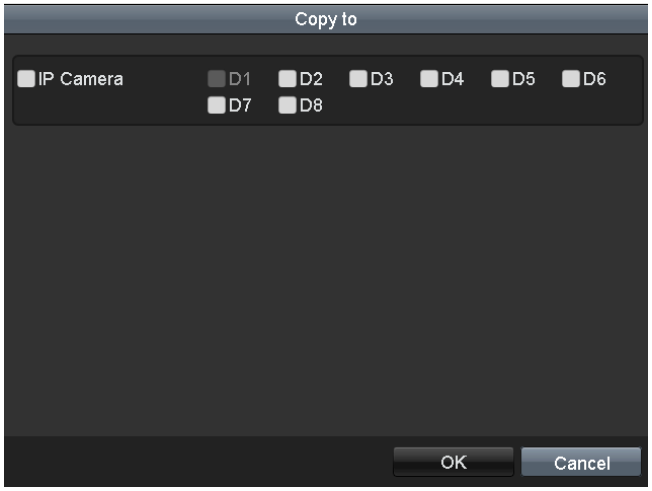


Figure 2. 12 Copy Record Settings

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

2.3 Adding and Connecting the IP Cameras

2.3.1 Adding the Online IP Cameras

Purpose:

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

Before you start:

Establish the network connection between IPC and the NVR via wired or wireless network.

- **Wired network**: connect the Ethernet port of computer to the LAN interface of NVR. And configure the IP address of computer on the principle that the network segment is the same with NVR, that is 192.168.254.×××.
- **Wireless network**: the default SSID and key of wireless network provided by NVR is in the tag of device.

- Hikvision WIFI IP camera which has default user name and password and is within 2m distance from the NVR will be added automatically.
- Ensure the network connection is valid and correct. For detailed checking and configuring of the network, please see *Chapter 9.3 Checking Network Traffic* and *Chapter 9.4 Configuring Network Detection.*

- **OPTION 1:**

Steps:

1. Right-click the mouse when you in the live view mode to show the right-click menu.

Figure 2. 13 Right-click Menu

2. Select **Add IP Camera**  in the pop-up menu to enter the IP Camera Management interface.

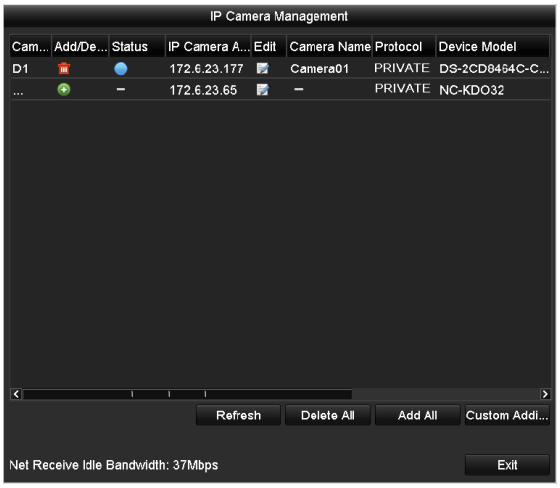


Figure 2. 14 Adding IP Camera Interface

3. The online cameras with same network segment will be displayed in the camera list. Click the button to add the camera.

Table 2. 1 Explanation of Icons

Icon	Explanation	Icon	Explanation
	Edit basic parameters of the camera		Add the detected IP camera.
	The camera is connected.		The camera is disconnected; you can click the icon to get the exception information of camera.
	Advanced settings of the camera.		Delete the IP camera

4. To add other IP cameras:

1) Click the **Custom Adding** button to pop up the Add IP Camera (Custom) interface.

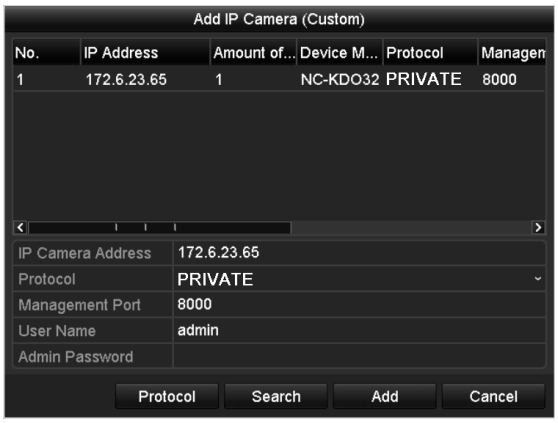


Figure 2. 15 Custom Adding IP Camera Interface

2) Input the **IP Address**, **Protocol**, **Management Port** and other information of the IP camera to be added.

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

- **OPTION 2:**

Steps:

1. Enter the Camera Management interface.

Menu > Camera > Camera

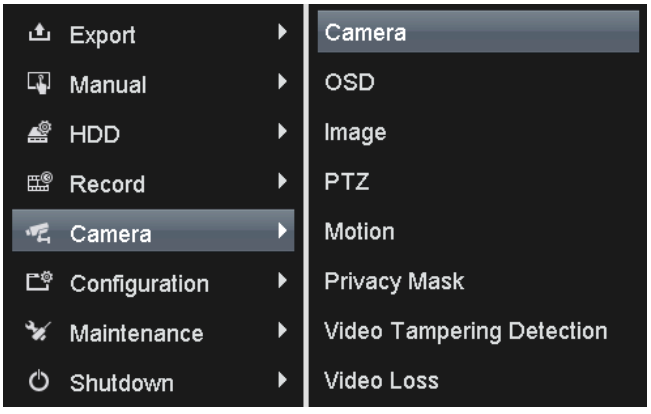


Figure 2. 16 Main Menu

2. Repeat the step 3 and 4 of OPTION 1 to add the camera.

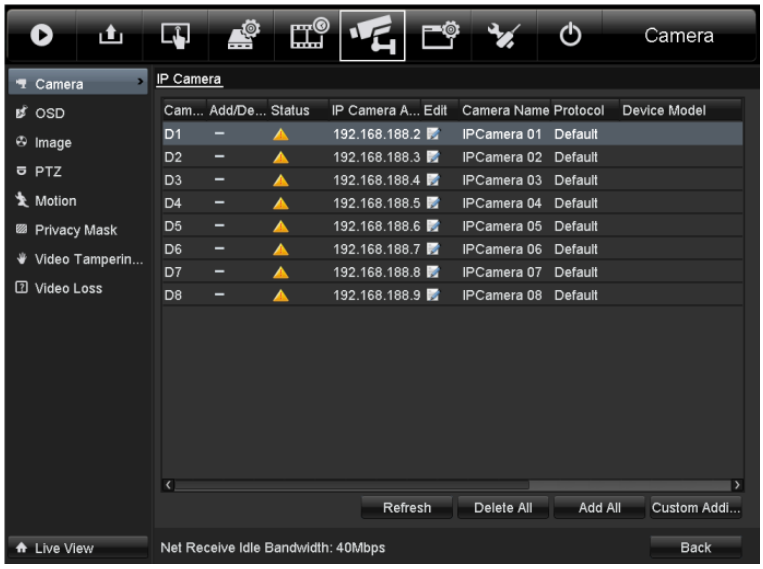


Figure 2. 17 IP Camera Management Interface

Table 2. 2 Explanation of the icons

Icon	Explanation	Icon	Explanation
	Edit basic parameters of the camera		Add the detected IP camera.
	The camera is connected; you can click the icon to get the live view of the camera.		The camera is disconnected; you can click the icon to get the exception information of camera.
	Advanced settings of the camera.		

3. (For the encoders with multiple channels only) check the checkbox of Channel No. in the pop-up window, as shown in the following figure, and click **OK** to finish adding.

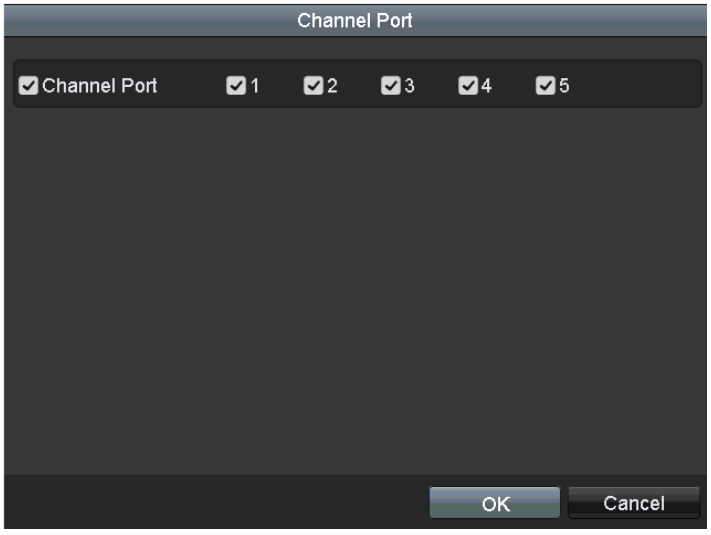


Figure 2. 18 Selecting Multiple Channels

2.3.2 Editing the Connected IP Cameras and Configuring Customized Protocols

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

Steps:

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

Figure 2. 19 Edit the Parameters

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

To edit advanced parameters:

Steps:

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

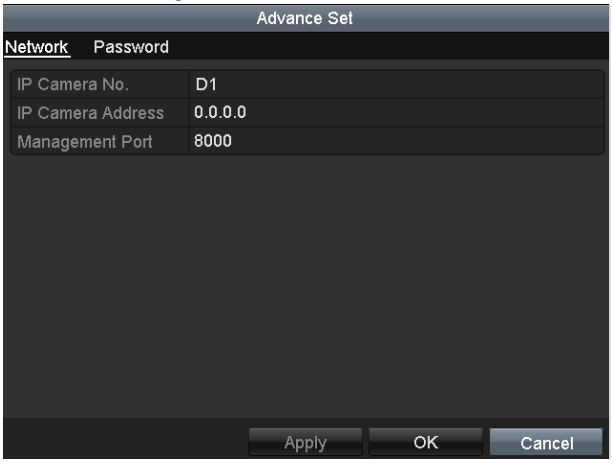


Figure 2. 20 Network Configuration of Camera

2. You can edit the **Network** information and the **Password** of the camera.
3. Click **Apply** to save the settings and click **OK** to exit the interface.

Configuring the customized protocols

Purpose:

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

customized protocols for them.

Steps:

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

Figure 2. 21 Protocol Management Interface

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

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

NOTE

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

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

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

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

NOTE

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

After adding the customized protocols, you can see the protocol name is listed in the drop-down list, please refer to Figure 2. 22.

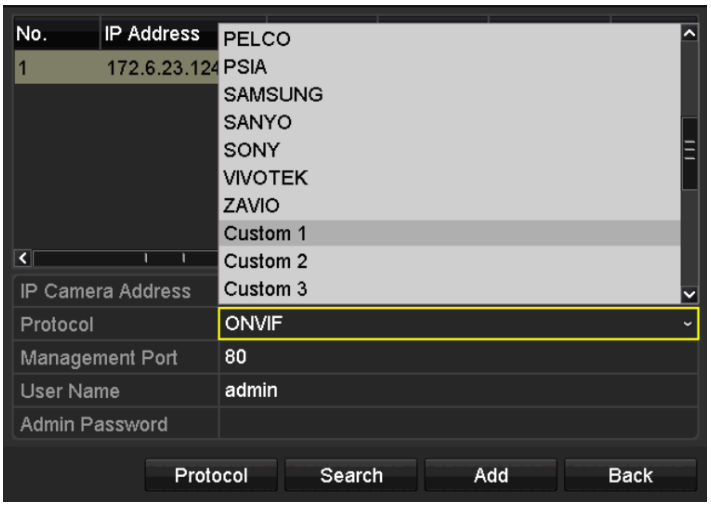


Figure 2. 22 Protocol Setting

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

Chapter 3 Live View

3.1 Introduction of Live View

Live view shows you the video image getting from each camera in real time. The NVR automatically enters Live View mode when powered on. It is also at the very top of the menu hierarchy.

Live View Icons

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

Table 3. 1 Description of Live View Icons

Icons	Description
	Alarm (video loss, video tampering, motion detection, alarm or VCA alarm)
	Record (manual record, continuous record, motion detection, alarm record or VCA alarm triggered record)
	Alarm & Record
	Event/Exception (motion detection, alarm, VCA alarm or exception information, appears at the lower-left corner of the screen. Please refer to *Chapter 8.7 Setting Alarm Response Actions* for details.)

3.2 Operations in Live View Mode

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

- **Single Screen**: showing only one screen on the monitor.
- **Multi-screen:** showing multiple screens on the monitor simultaneously.
- **Auto-switch:** the screen is auto switched to the next one. And you must set the dwell time for each screen on the configuration menu before enabling the auto-switch.
  Menu>Configuration>Live View>Dwell Time.
- **Start Recording:** continuous record and motion detection record are supported.
- **Output Mode:** select the output mode to Standard, Bright, Gentle or Vivid.
- **Playback:** playback the recorded videos for current day.
- **PTZ Control:** enter PTZ control interface to rotate the PTZ.
- **Add IP Camera:** the shortcut to the IP camera management interface.

3.2.1 Using the Mouse in Live View

Table 3. 2 Mouse Operation in Live View

Name	Description
Menu	Enter the main menu of the system by right-clicking the mouse.
	Switch to the single full screen by choosing channel number from the drop-down list.
	Adjust the screen layout by choosing from the drop-down list.
	Switch to the previous screen.
	Switch to the next screen.
/	Enable/disable the auto-switch of the screens.
/	Start continuous recording or motion detection recording of all channels.
	Enter the IP Camera management interface, and manage the cameras.
	Enter the playback interface and start playing back the video of the selected channel immediately.
	Four modes of output supported, including Standard, Bright, Gentle and Vivid.
/	Fix the menu

NOTE

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

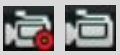
Figure 3. 1 Right-click Menu

3.2.2 Quick Setting Toolbar in Live View Mode

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

Figure 3. 2 Quick Setting Toolbar

Table 3. 3 Description of Quick Setting Toolbar Icons

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

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

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

Figure 3. 3 Digital Zoom

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

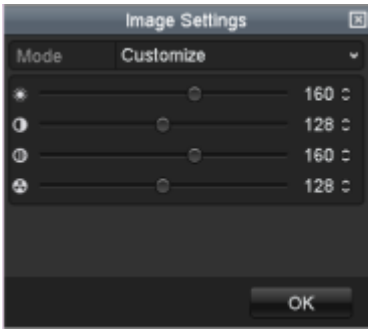


Figure 3. 4 Image Settings- Preset

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

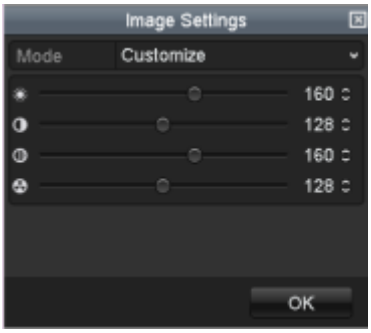


Figure 3. 5 Image Settings- Customize

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

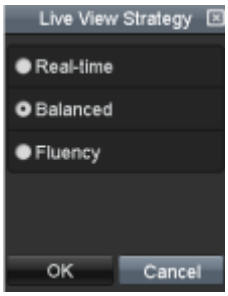


Figure 3. 6 Live View Strategy

3.3 Adjusting Live View Settings

Purpose:

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

Steps:

1. Enter the Live View Settings interface.

   Menu > Configuration > Live View

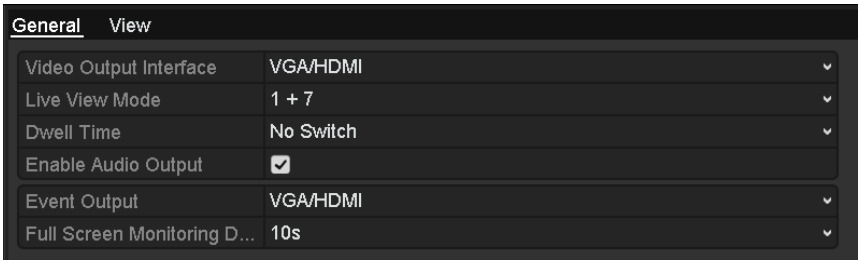


Figure 3. 7 Live View Settings

The settings available in this menu include:

- **Video Output Interface:** Designates the output to configure the settings for, and only HDMI™ is selectable.
- **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:** Enable/disable audio output for the selected video output.
- **Event Output:** Designates the output to show event video.
- **Full Screen Monitoring Dwell Time:** The time in seconds to show alarm event on full screen.

2. Setting Cameras Order

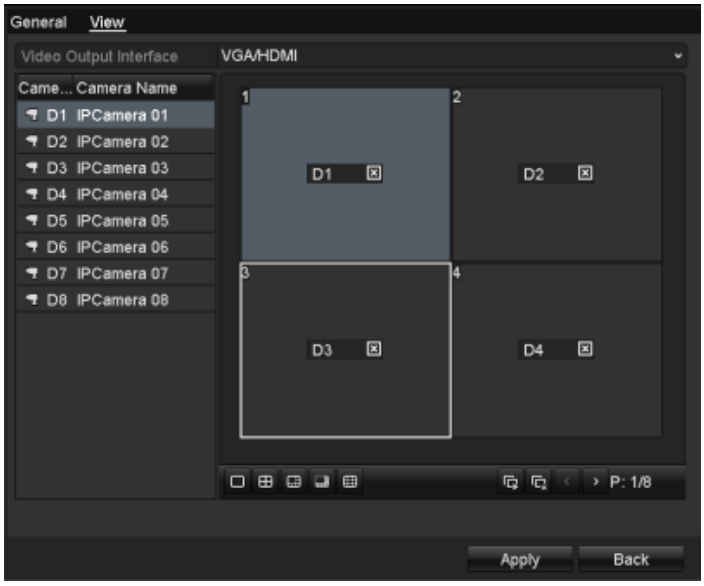


Figure 3. 8 Live View Camera Order

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

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

   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 live view.

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

3.4 User Logout

Purpose:

After logging out, the monitor turns to the live view mode and if you want to do some operation, you need to enter user name and password tog in again.

Steps:

1. Enter the Shutdown menu.

   Menu>Shutdown

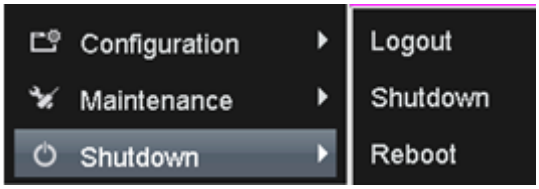


Figure 3. 9 Shutdown Interface

2. Click **Logout**.

   NOTE

   After you have logged out the system, menu operation on the screen is invalid. It is required to input a user name and password to unlock the system.

Chapter 4 PTZ Controls

4.1 Configuring PTZ Settings

Purpose:

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

Steps:

1. Enter the PTZ Settings interface.

   Menu > Camera > PTZ

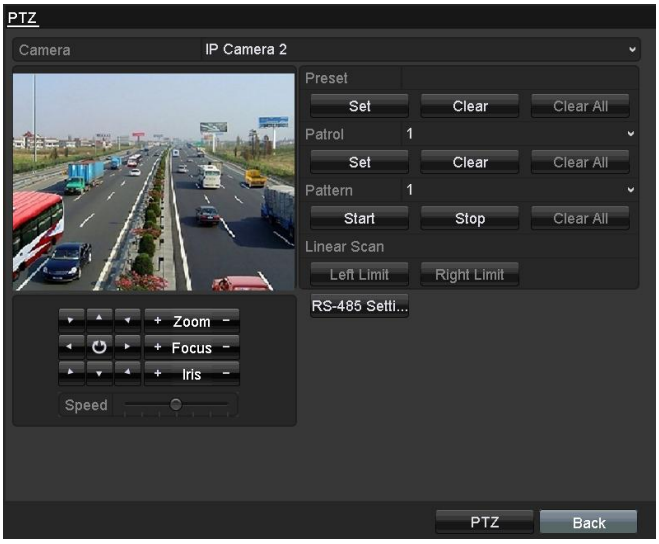


Figure 4. 1 PTZ Settings

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

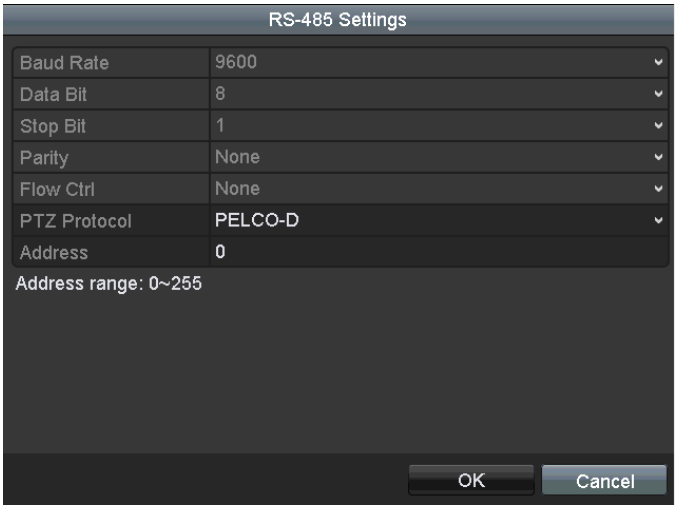


Figure 4. 2 PTZ General Settings

3. Choose the camera for PTZ setting in the **Camera** drop-down list.
4. Enter the parameters of the PTZ camera.

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

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

4.2 PTZ Control Panel

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

OPTION 1:

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

OPTION 2:

In the Live View mode, you can press the PTZ Control button on the front panel or on the remote control, or choose the PTZ Control icon, or select the PTZ option in the right-click menu.

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

NOTE

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

Figure 4. 3 PTZ Panel

Table 4. 1 Description of the PTZ panel icons

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

4.3 Setting PTZ Presets, Patrols & Patterns

Before you start:

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

4.3.1 Customizing Presets

Purpose:

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

Steps:

1. Enter the PTZ Control interface.

   Menu > Camera > PTZ

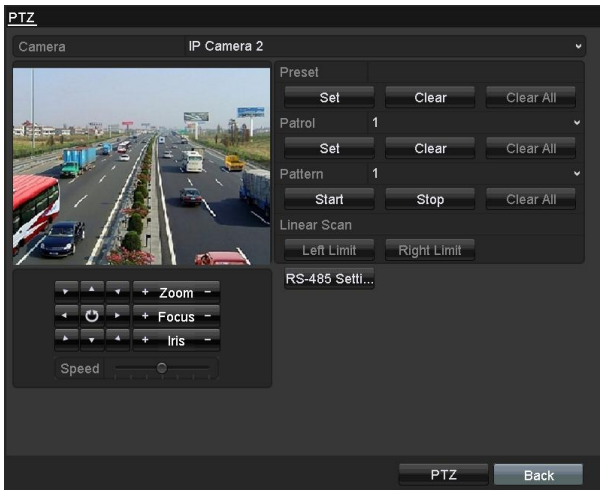


Figure 4. 4 PTZ Settings

2. Use the directional button to wheel the camera to the location where you want to set preset; and the zoom and focus operations can be recorded in the preset as well.
3. Enter the preset No. (1~255) in the preset text field, and click the **Set** button to link the location to the preset.

   Repeat the steps 2-3 to save more presets.

   You can click the **Clear** button to clear the location information of the preset, or click the **Clear All** button to clear the location information of all the presets.

4.3.2 Calling Presets

Purpose:

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

Steps:

1. Enter PTZ Control interface. For details, please refer to *4.2 PTZ Control Panel*.
2. Choose C**amera** in the drop-down list.
3. Click the button to show the general settings of the PTZ control.

Figure 4. 5 PTZ Panel - General

4. Input the preset No. in the corresponding text field.
5. Click the **Call Preset** button to call it.

4.3.3 Customizing Patrols

Purpose:

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

Steps:

1. Enter the PTZ Control interface.

   Menu > Camera > PTZ

Figure 4. 6 PTZ Settings

2. Select patrol No. in the drop-down list of patrol.
3. Click the **Set** button to add key points for the patrol.

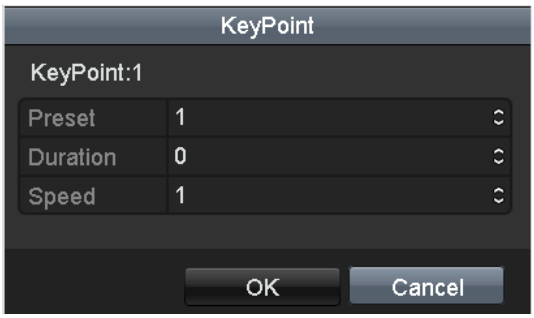


Figure 4. 7 Key point Configuration

4. Configure key point parameters, including the **Preset** No., **Duration** of staying for one key point and **Speed** of patrol.

   KeyPoint No.: determines the order at which the PTZ will follow while cycling through the patrol.

   Preset: PTZ will rotate automatically to the set preset No. when execute the keypoint.

   Duration: refers to the time span to stay at the corresponding key point.

   Speed: defines the speed at which the PTZ will move from one key point to the next.

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

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

4.3.4 Calling Patrols

Purpose:

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

Steps:

1. Enter PTZ Control interface. For details, please refer to *4.2 PTZ Control Panel*.
2. Click the button to show the general settings of the PTZ control.

Figure 4. 8 PTZ Panel - General

3. Select a patrol in the drop-down list and click the **Call Patrol** button to call it.
4. You can click the **Stop Patrol** button to stop calling it.

4.3.5 Customizing Patterns

Purpose:

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

Steps:

1. Enter the PTZ Control interface.

   Menu > Camera > PTZ

Figure 4. 9 PTZ Settings

2. Choose pattern number in the drop-down list.
3. Click the **Start** button and click corresponding buttons in the control panel to move the PTZ camera, and click the **Stop** button to stop it.

   The movement of the PTZ is recorded as the pattern.

4.3.6 Calling Patterns

Purpose:

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

Steps:

1. Enter PTZ Control interface. For details, please refer to *4.2 PTZ Control Panel.*
2. Click the button to show the general settings interface.

Figure 4. 10 PTZ Panel - General

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

4.3.7 Customizing Linear Scan Limit

Purpose:

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

NOTE

This function is supported by some certain IP cameras.

Steps:

1. Enter the PTZ Control interface.

   Menu > Camera > PTZ

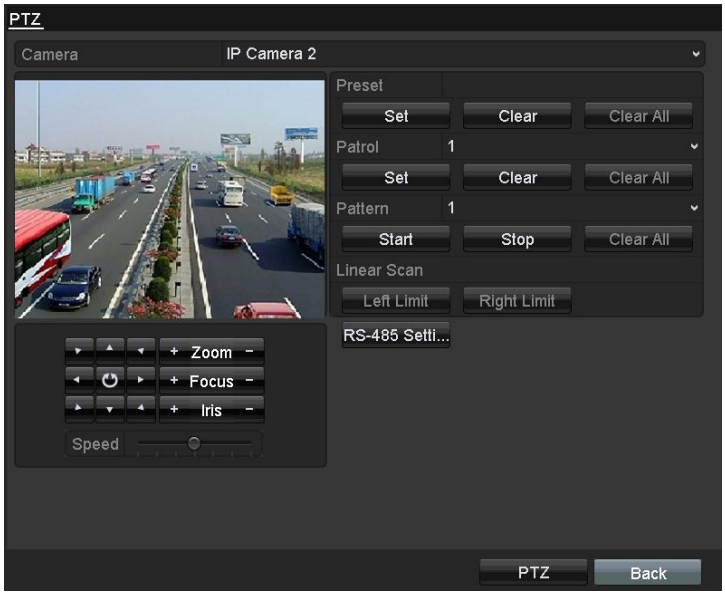


Figure 4. 11 PTZ Settings

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

NOTE

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

4.3.8 Calling Linear Scan

Purpose:

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

Steps:

1. Enter PTZ Control interface. For details, please refer to *4.2 PTZ Control Panel.*
2. Click the button to show the one-touch function of the PTZ control.

Figure 4. 12 PTZ Panel - One-touch

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

4.3.9 One-touch Park

Purpose:

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

Steps:

1. Enter PTZ Control interface. For details, please refer to *4.2 PTZ Control Panel.*
2. Click the button to show the one-touch interface.

Figure 4. 13 PTZ Panel - One-touch

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

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

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

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

   NOTE

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

4. Click the button again to inactivate it.

Chapter 5 Recording Settings

5.1 Configuring Parameters

Purpose:

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

Steps:

1. Enter the Record settings interface to configure the recording parameters.

   Menu > Record > Parameters

Figure 5. 1 Recording Parameters

2. Set parameters for recording.

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

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

NOTE

- The Stream Type, Resolution, Bitrate Type and Video Quality of Main Stream (Event) are read-only.

3. Set parameters for sub-stream.

1) Enter the Sub-stream tab.

Figure 5. 2 Sub-stream Parameters

2) Configure the parameters of the camera.

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

5.2 Configuring Recording Schedule

Purpose:

Set the 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

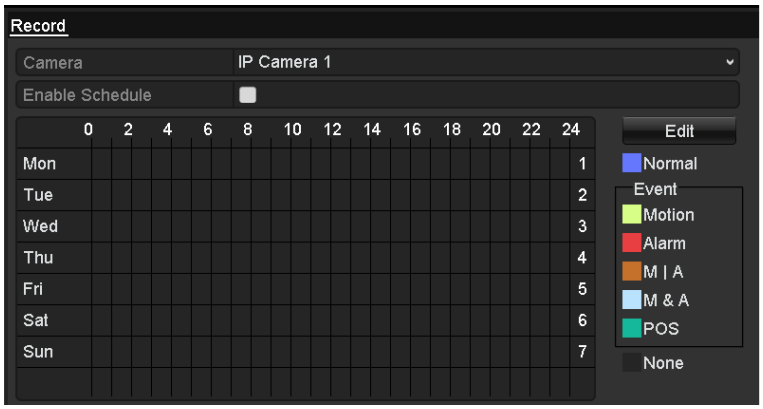


Figure 5. 3 Record Schedule

2. Configure Record Schedule

   1) Choose the camera to configure.

   2) Check the checkbox of **Enable Schedule**.

   3) Edit or draw schedule.

   Edit the schedule:

   I. In the message box, select the day to set schedule in the drop-down list of Schedule.

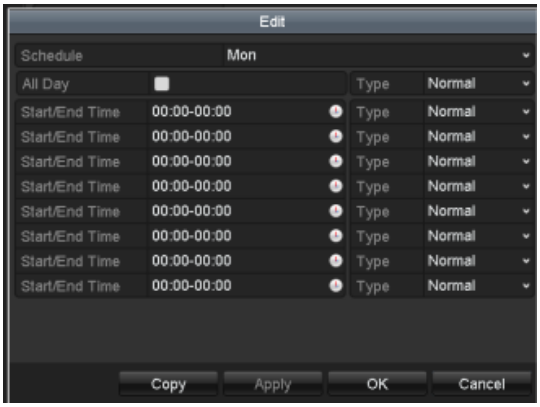


Figure 5. 4 Recording Schedule Interface

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

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

Figure 5. 5 Edit Schedule

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

NOTE

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

IV. Select the record type in the drop-down list.

NOTE

- To enable Motion, Alarm, M | A (motion or alarm), M & A (motion and alarm) and VCA (Video Content Analysis) triggered recording, you must configure the motion detection settings, alarm input settings or VCA settings as well. For detailed information, refer to section *8.1 Setting Motion Detection Alarm*, *8.2 Setting Sensor Alarms* and *8.3 Detecting Video Loss Alarm*.
- The VCA settings are only available to the smart IP cameras.

Repeat the above steps to schedule recording for other days in the week. Or click **Copy** 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 a color icon, you can choose the schedule type as continuous or event.

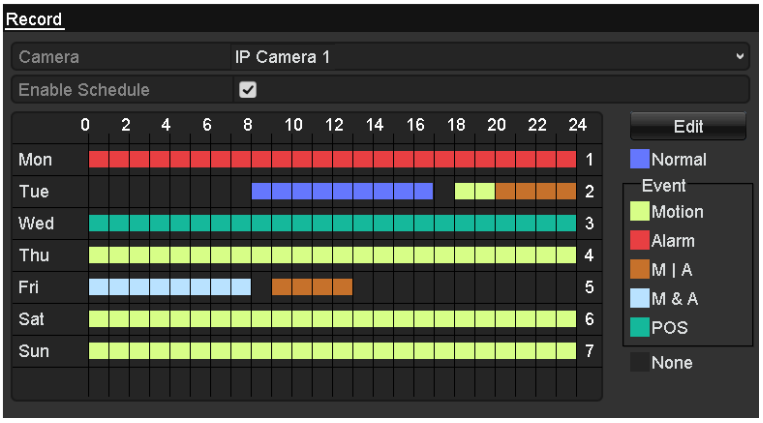


Figure 5. 6 Draw the Schedule

Descriptions of the color icons are shown in the figure below.

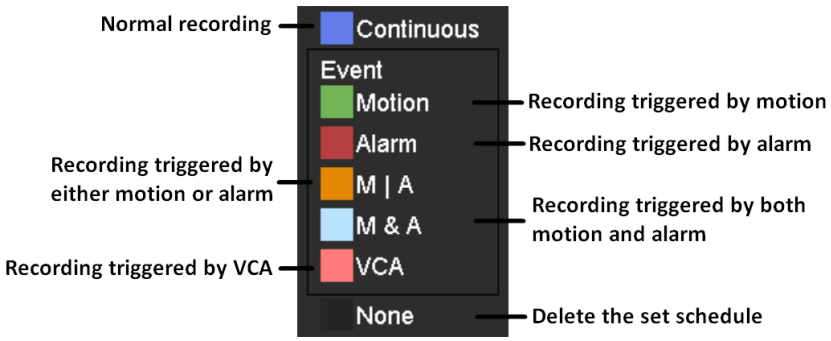


Figure 5. 7 Descriptions of the color icons

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

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

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

5.3 Configuring Motion Detection Recording

Purpose:

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, audible 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.

   1) Choose camera to configure.

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

   3) Use the mouse to drag and draw the motion detection area in the right live view window.

      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**.

Figure 5. 8 Motion Detection- Mask

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

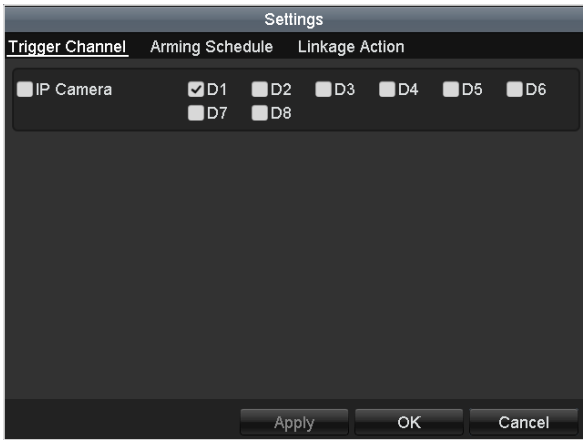


Figure 5. 9 Motion Detection Settings

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

6) Click **Apply** to save the settings.
7) Click **OK** to back to the upper level menu.
8) Exit the Motion Detection menu.

3. Edit the Motion Detection Record Schedule. For the detailed information of schedule configuration, see section *5.2 Configuring Recording Schedule*.

5.4 Configuring VCA Triggered Recording

Purpose:

Perform the following steps to set the VCA alarm and trigger recording of related cameras.

Steps:

1. Enter VCA Alarm interface of Camera Management.

   Menu > Camera > VCA

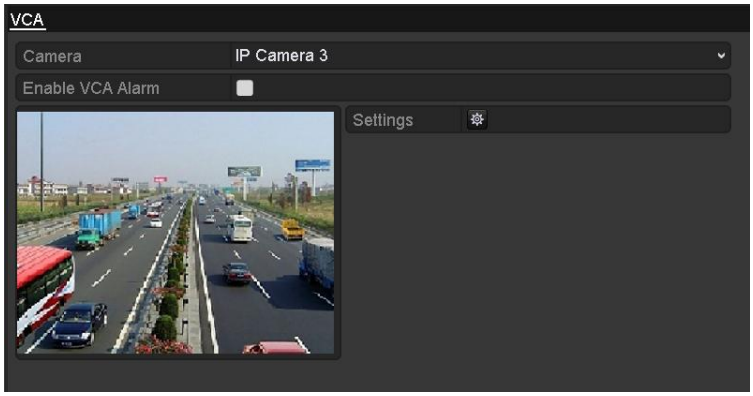


Figure 5. 10 VCA Alarm Setting Interface

2. Select a Camera in the drop-down list.

   NOTE

   The selected camera must support the VCA function.

3. Check the **Enable VCA Alarm** checkbox.
4. Click the icon after **Settings** to set up the alarm response actions.

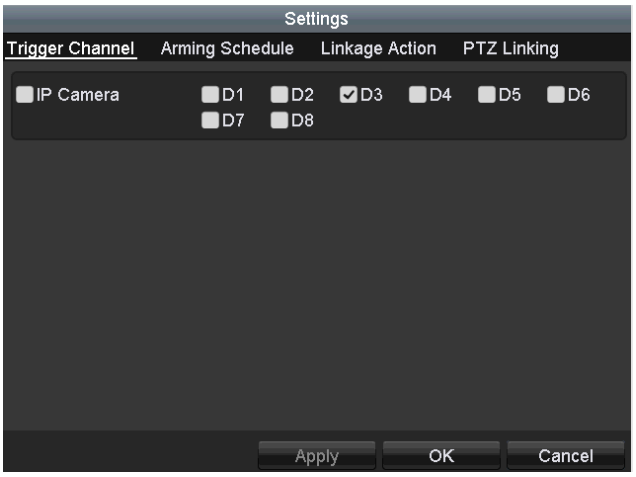


Figure 5. 11 VCA Alarm Handling

5. Check the check of Camera. So the selected camera will be triggered to recording when a VCA occurs.
6. Click **Apply** to save the settings.
7. Edit the VCA Alarm Record Schedule. For the detailed information of schedule configuration, see section *5.2 Configuring Recording Schedule.*

5.5 Manual Recording

Purpose:

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

Steps:

1. Enter the Manual settings interface.

   Menu > Manual

Figure 5. 12 Manual Record

2. Enable the Manual Record.

   1) Select **Record** on the left bar.

   2) Click the status button before camera number to switch OFF to ON.

3. Disable manual record.

   Click the status button to switch ON to OFF.

NOTE

- Green icon ON means that the channel is configured the record schedule.
- After rebooting, all the manual records enabled will be canceled.

5.6 Configuring Holiday Recording

Purpose:

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

Steps:

1. Enter the Record setting interface.

   Menu > Record > Holiday

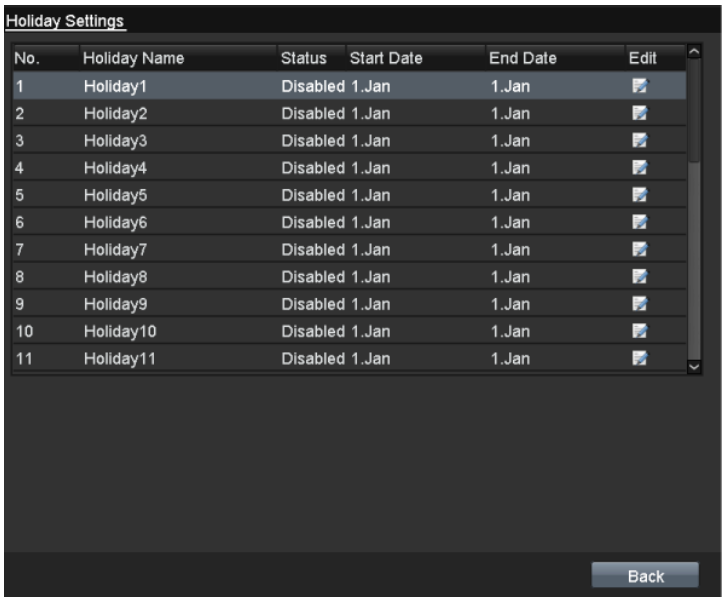


Figure 5. 13 Holiday Settings

2. Enable Edit Holiday schedule.

   1) Click  to enter the Edit interface.

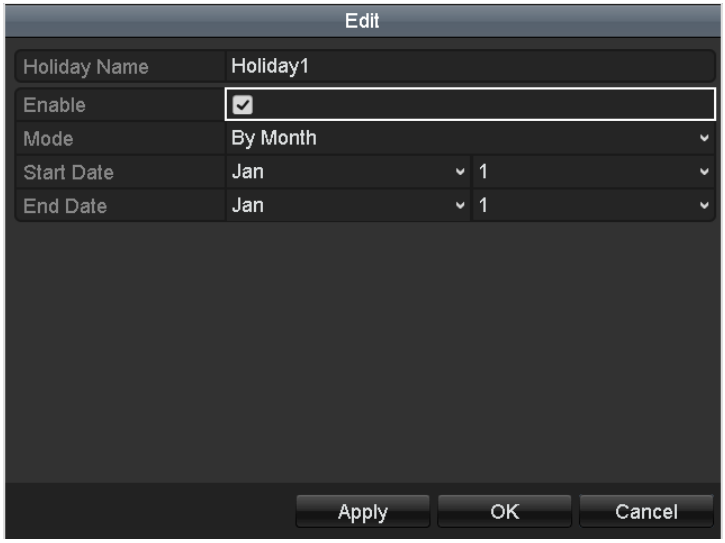


Figure 5. 14 Edit Holiday Settings

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

3) Select **Mode** from the drop-down list.

   There are three different modes: **By Date**, **By Week** and **By Month**.

4) Set the **Start Date** and **End Date**.

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

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

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

5.7 Files Protection

Purpose:

You can lock the recorded files to protect the record files from being overwritten.

Steps:

1. Enter Export setting interface.

   Menu > Export

Figure 5. 15 Export

2. Select the cameras to protect by checking the checkbox.
3. Configure the **Record Type**, **File Type**, **Start Time** and **End Time**.
4. Click **Search** to show the results.

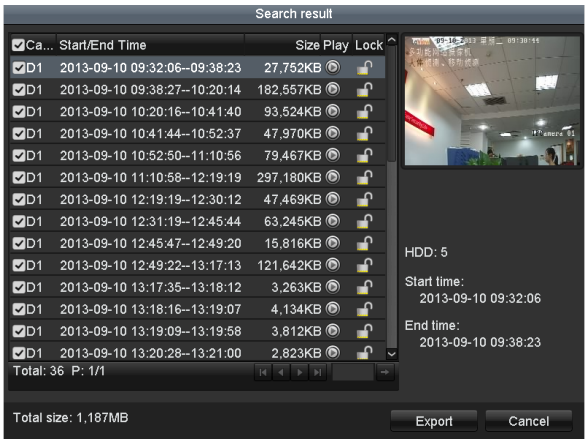


Figure 5. 16 Export- Search Result

5. Protect the record files.

   1) Click the icon of a file to switch it to , indicating that the file is locked.

   NOTE

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

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

Figure 5. 17 Unlocking Attention

Chapter 6 Playback

6.1 Playing Back Record Files

6.1.1 Playing Back by Channel

Purpose:

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

Instant playback by channel

Steps:

In the live view mode, click to select a channel to pop up quick setting toolbar and click the button.

NOTE

Only record files recorded during the last five minutes on this channel will be played back.

Figure 6. 1 Instant Playback Interface

Playback by channel

1. Enter the Playback interface.

   Right click a channel in live view mode and select from the menu as shown in Figure 6. 2.

Figure 6. 2 Right-click Menu

2. Playback management.

   Check the checkbox of the cameras to execute simultaneous playback for multiple channels.

Figure 6. 3 Playback Interface

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

Figure 6. 4 Toolbar of Playback

NOTE

- Use the mouse to click any point of the progress bar or drag the progress bar to locate in special frames.
- The 03-17-2014 17:08:35 -- 03-27-2014 16:12:11 indicates the start and end time of the record.

Table 6. 1 Detailed Explanation of Playback Toolbar

Button	Operation	Button	Operation	Button	Operation
/	Mute / Audio on	/	Start/Stop clipping		30s forward
	30s reverse		Add default tag		Add customized tag
	Tag management		Speed down	/	Reverse play or Single-frame reverse play / Pause reverse play
/	Play or Single-frame play / Pause	/	Scaling up / down the time line		Speed up
	Previous day		Next day		Full Screen
	Exit		Stop		Digital Zoom
	Save the clips		Process bar	Normal	Video type

6.1.2 Playing Back by Time

Purpose:

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

Steps:

1. Enter playback interface.

   Menu > Playback

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

Figure 6. 5 Playback Calendar

NOTE

In calendar, the dates who have record files for selected camera will show as 10, otherwise it will show as 11.

6.1.3 Playing Back by Event Search

Purpose:

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

Steps:

1. Enter the Playback interface.

   Menu > Playback

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

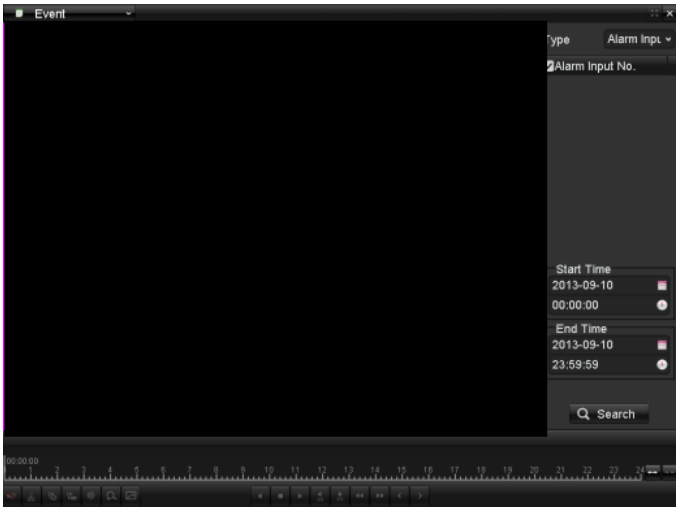


Figure 6. 6 Motion Search Interface

3. Select the **Major Type** as **Alarm Input**, **Motion** or **VCA**.
4. Set the **Start Time** and **End Time**.

   Here we take playback by motion as the example.

5. Click **Search** button to get the search result, as shown below.

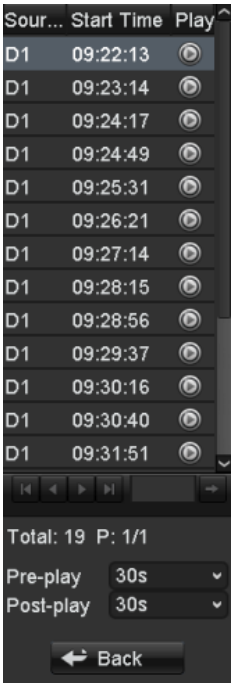


Figure 6. 7 Search Result Bar

6. Click button to play back the file.

NOTE

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

Figure 6. 8 Interface of Playback by Event

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

6.1.4 Playing Back by Tag

Purpose:

Video tag allows you to record related information, like people and location, of a certain time point during playback. You are also allowed to use video tag(s) to search for record files and position time point.

You need to add tags before playing back them.

Before you start:

1. Enter Playback interface.

   Menu > Playback
2. Search and play back the record file(s). For details, please refer to section *6.1.1 Playing Back by Channel*.
3. Add tag.
   - Add default tag: click button in toolbar.
   - Add customized tag: click button in toolbar and input tag name.

   NOTE

   Max. 64 tags can be added to each single video file.
4. Tag management.

   Click button to check, edit or delete tag(s).

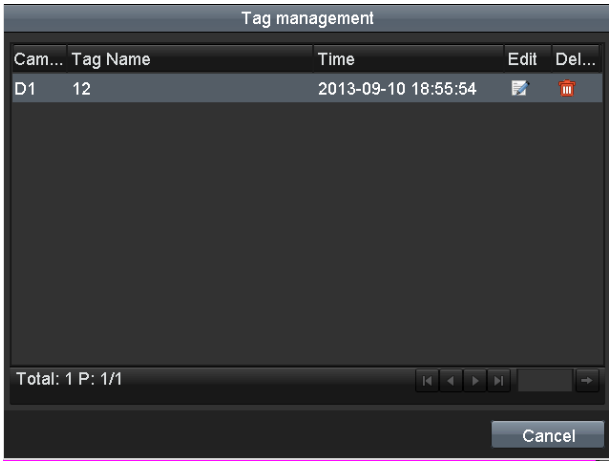


Figure 6. 9 Tag Management Interface

Steps:

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

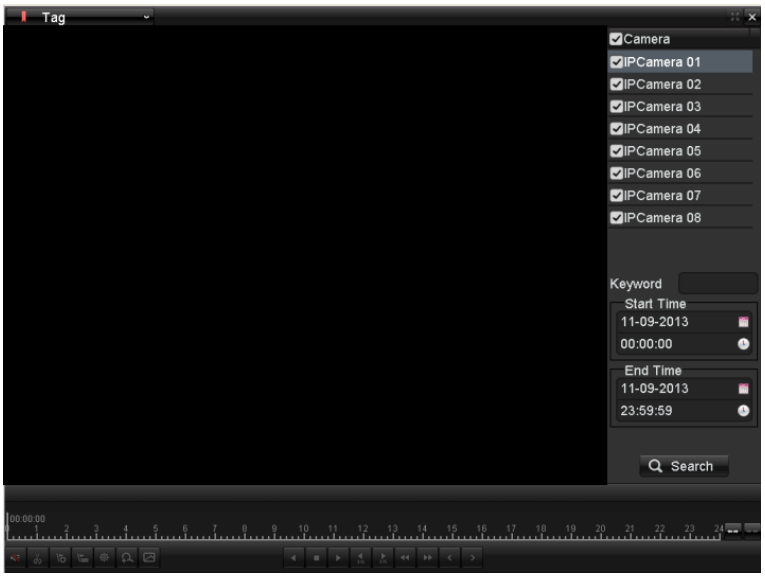


Figure 6. 10 Video Search by Tag

2. Check the checkbox of cameras.
3. Edit **Start Time** and **End Time**.
4. Optionally, you can input **Keyword** to search the tag on your demand.
5. Click **Search** to enter Search Result interface.
6. Click button to play back the file.

NOTE

Pre-play and post-play can be configured.

Figure 6. 11 Interface of Playback by Tag

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

6.1.5 Smart Playback

Purpose:

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

Before you start:

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

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

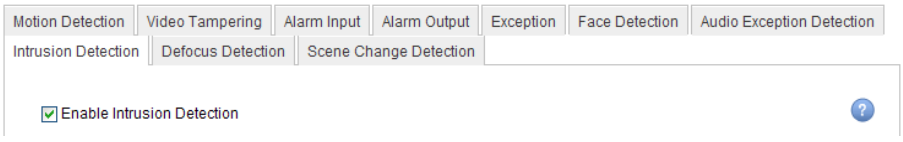


Figure 6. 12 Setting Intrusion Detection on IP Camera

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

Steps:

1. Enter Playback interface.
   Menu > Playback
2. Select the **Smart** in the drop-down list on the top-left side.

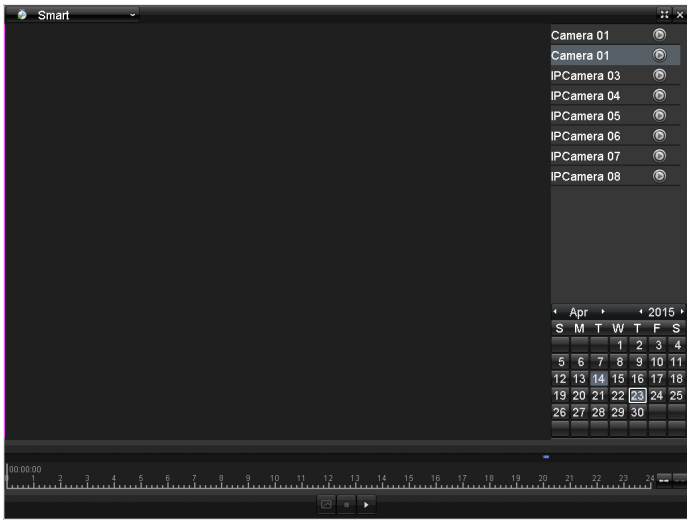


Figure 6. 13 Smart Playback Interface

Table 6. 2 Detailed Explanation of Smart Playback

Button	Operation	Button	Operation	Button	Operation
	Smart search		Stop	/	Pause / Play
	Process bar	/	Scaling up / down the time line	Smart	Playback type

3. Click to select a camera in the camera list.
4. Click to select a date in the calendar.
5. Edit the smart search areas and rules.
   1) Click the button to enter the search area editing interface. The smart search area is set as full screen by default.

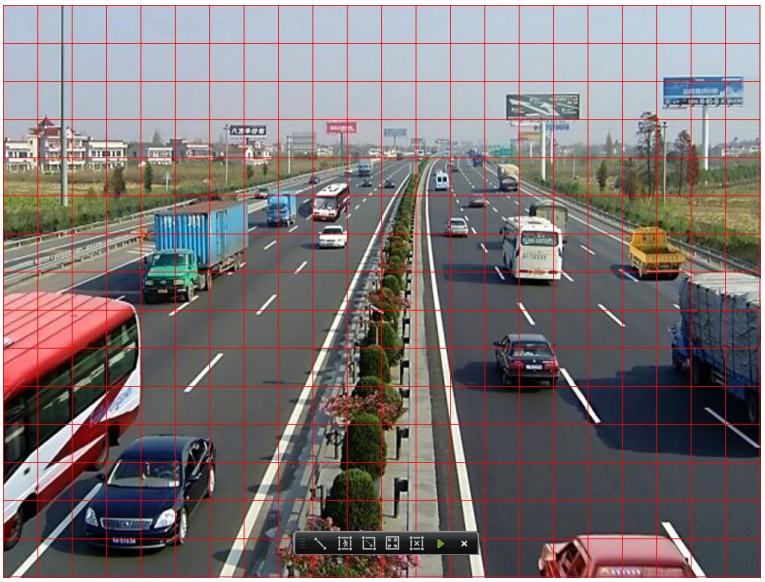


Figure 6. 14 Draw Area of Smart Search

   2) Set the rules and areas.
      - **Line Crossing Detection:**

Click the button and specify 2 points to set a line for line crossing detection.

- **Intrusion Detection**

Click the button, and then specify 4 points to set a quadrilateral region for intrusion detection.

- **Motion Detection**

i. Click the to set the search area manually.

ii. Click and drag the mouse to draw target searching area(s), or click the button to set the full screen as the area.

NOTE

For line crossing detection and intrusion detection, only one region can be set.

3) Click the to search, and then the result will be displayed as in the progress bar of the Smart Playback interface.

Figure 6. 15 Smart Search Result

6.1.6 Playing Back by System Logs

Purpose:

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

Steps:

1. Enter Log Information interface.

   Menu > Maintenance > Log Information

2. Click **Log Search** tab to enter Playback by System Logs.
3. Set the precondition, including **Start Time**, **End Type**, **Major type** and **Minor Type**.
4. Click **Search** button.

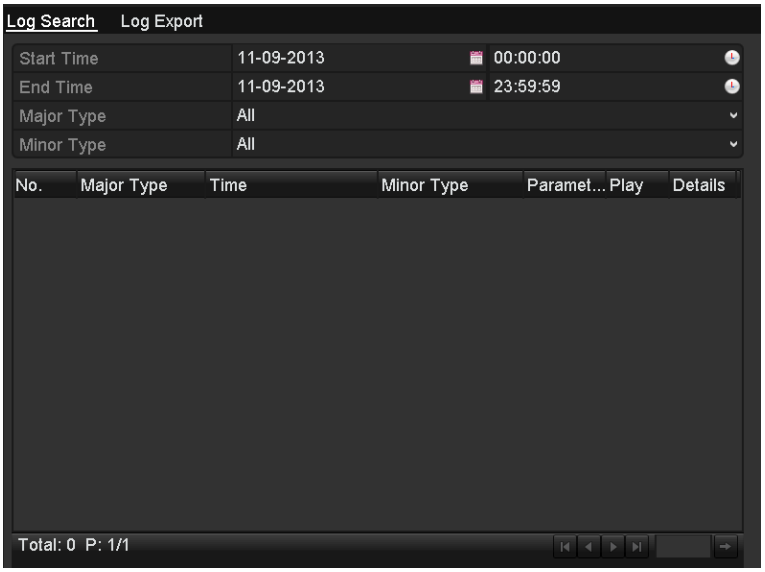


Figure 6. 16 System Log Search Interface

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

NOTE

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

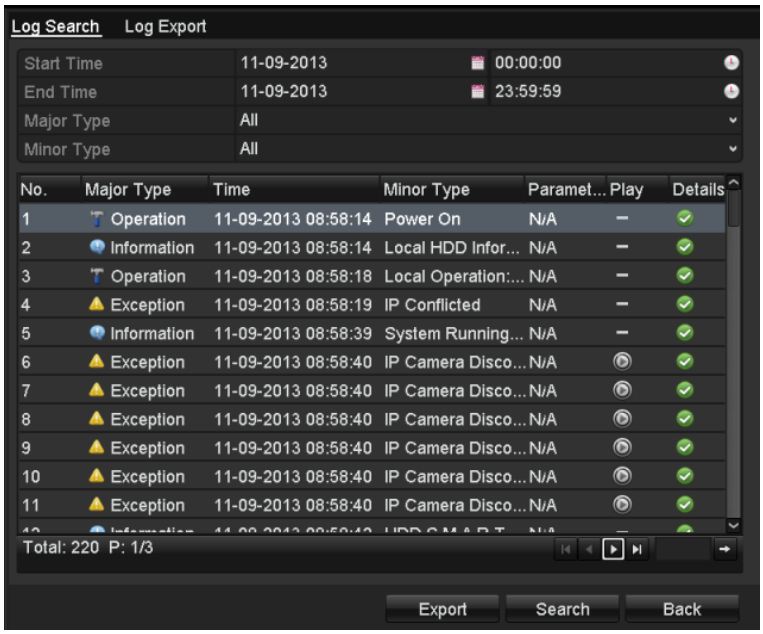


Figure 6. 17 Result of System Log Search

6.1.7 Playing Back External File

Purpose:

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

Steps:

1. Enter Tag Search interface.

Menu > Playback

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

   The files are listed in the right-side list.

   You can click the **Refresh** button to refresh the file list.

3. Click the button to play back record file.

4. You can adjust the playback speed by clicking and .

Figure 6. 18 Interface of External File Playback

6.2 Auxiliary Functions of Playback

6.2.1 Playing Back Frame by Frame

Purpose:

Play video files frame by frame, in case of checking image details of the video when abnormal events happen.

Steps:

1. Enter Playback interface.
   Menu > Playback
2. Start signal frame playback.
   Playback: click button until the speed changes to Single frame and one click on the playback screen to play back by one frame.
   Reverse playback: click button until the speed changes to Single frame and one click on the playback screen to reversely play back by one frame. It is also feasible to use button in toolbar.

6.2.2 Digital Zoom

Steps:

1. Click the button on the playback toolbar to enter Digital Zoom interface.
2. Use the mouse to draw a red rectangle and the image within it will be enlarged up to 16 times.

Figure 6. 19 Draw Area for Digital Zoom

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

6.2.3 Reverse Playback of Multi-channel

Purpose:

You can play back record files of multi-channel reversely. Up to 8-ch (with 1280*720 resolution) simultaneous

reverse playback is supported and up to 6-ch (with 1920*1080P resolution) simultaneous reverse playback is supported.

Steps:

1. Enter Playback interface.

   Menu > Playback

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

Figure 6. 20 4-ch Synchronous Playback Interface

3. Click  to play back the record files reversely.

Chapter 7 Backup

7.1 Backing up Record Files

7.1.1 Quick Export

Purpose:

Export record files to backup device(s) quickly.

Before you start:

You can connect a USB hub to the signal USB interface in rear panel expand it.

Steps:

1. Enter Video Export interface.

   Menu > Export > Normal

2. Choose the channel(s) 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.

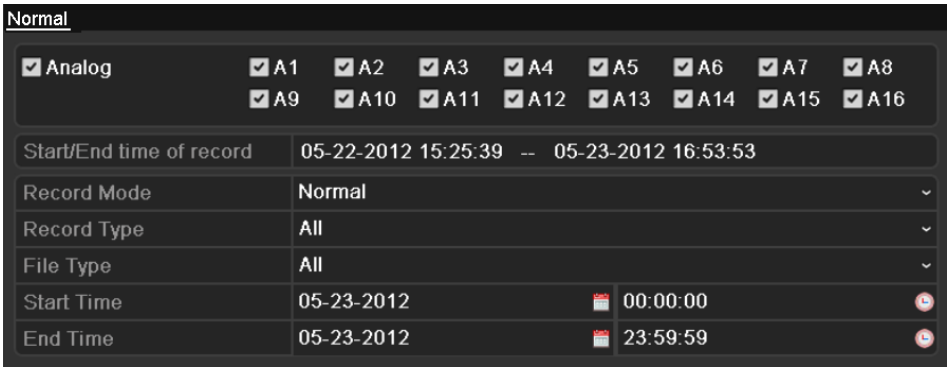


Figure 7. 1 Quick Export Interface

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

   NOTE

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

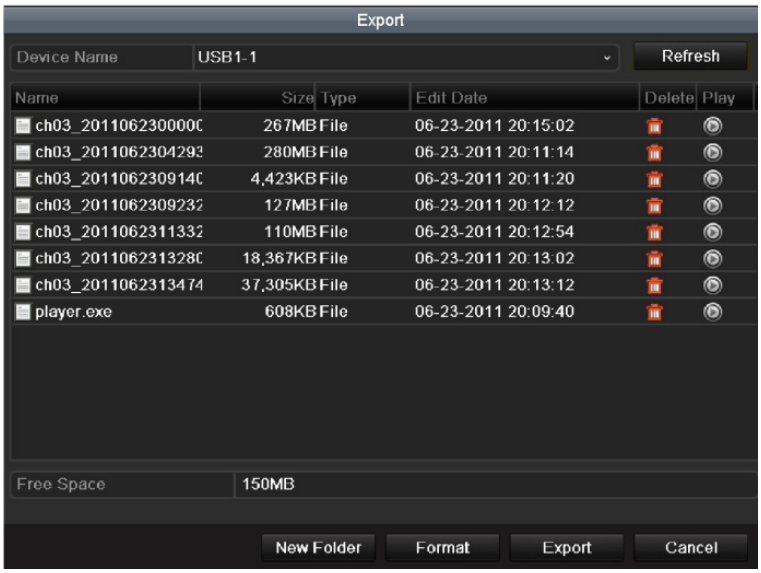


Figure 7. 2 Quick Export using USB1-1

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

4. Check backup result.

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

NOTE

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

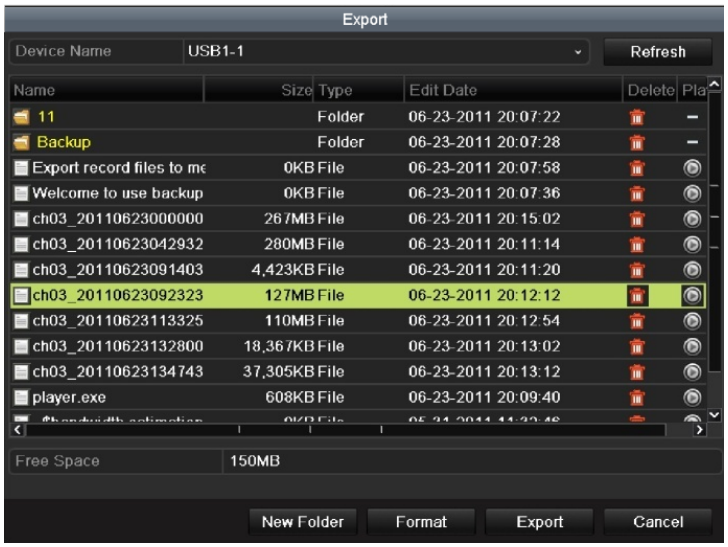


Figure 7. 3 Checkup of Quick Export Result Using USB1-1

7.1.2 Backing up by Normal Video Search

Purpose:

The record files can be backed up to various devices, such as USB flash drives, USB HDDs and USB writer.

Backup using USB flash drives and USB HDDs

Steps:

1. Enter Export interface.

   Menu > Export > Normal

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

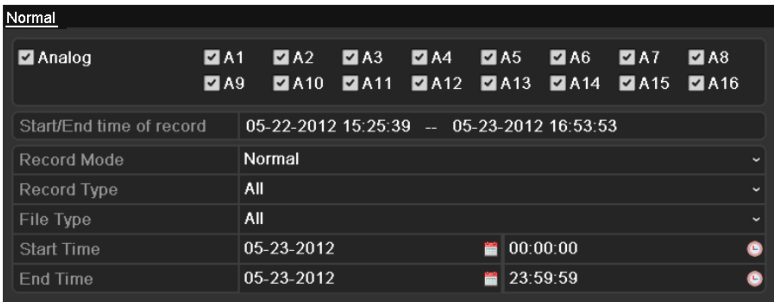


Figure 7. 4 Normal Video Search for Backup

3. Select record files to back up.

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

   Check the checkbox before the record files to back up.

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

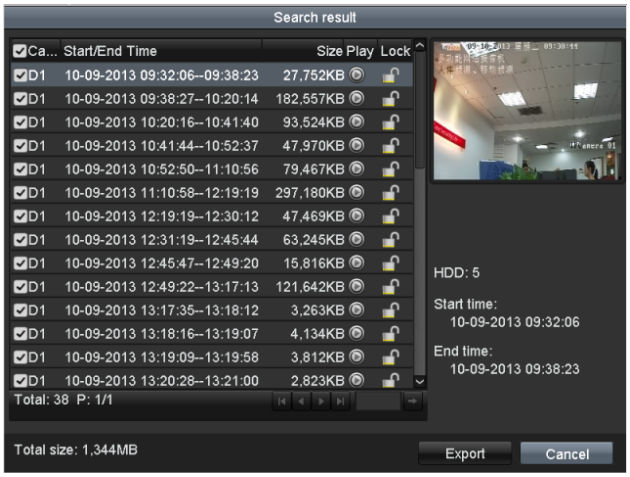


Figure 7. 5 Result of Normal Video Search for Backup

4. Export.

   Click **Export All** button to export all the record files.

   Or you can select record files to back up, and click **Export** button to enter Export interface.

If the inserted USB device is not recognized:

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

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

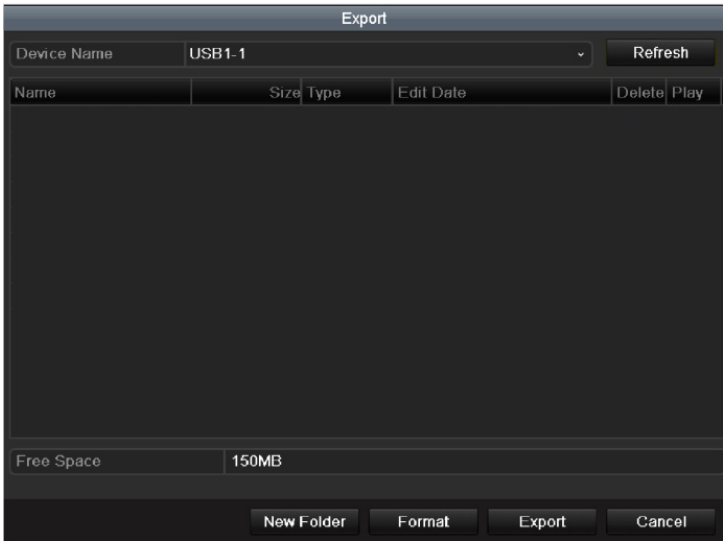


Figure 7. 6 Export by Normal Video Search using USB Flash Drive

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

5. Check backup result.

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

NOTE

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

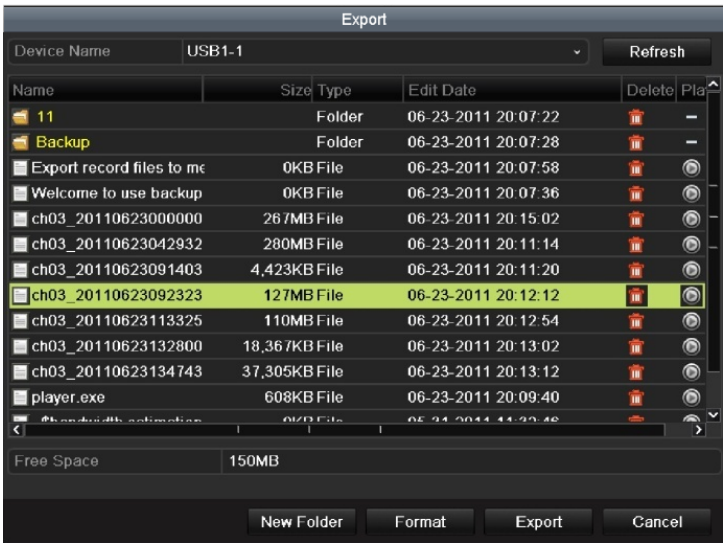


Figure 7. 7 Checkup of Export Result using USB Flash Drive

Backup using USB writer

Steps:

1. Enter Export interface.

   Menu > Export > Normal

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

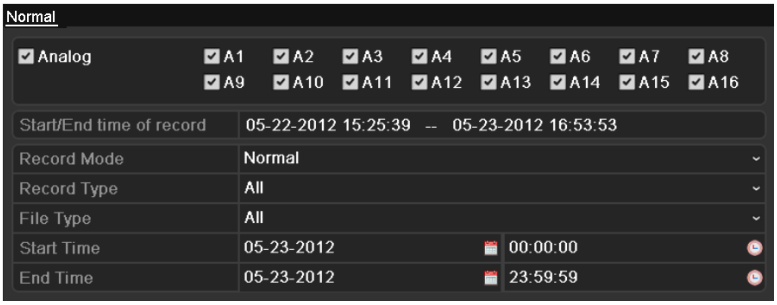


Figure 7. 8 Normal Video Search for Backup

3. Select record files to back up.

- Click button to play the record file to check it.
- Check the checkbox before the record files to back up.

NOTE

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

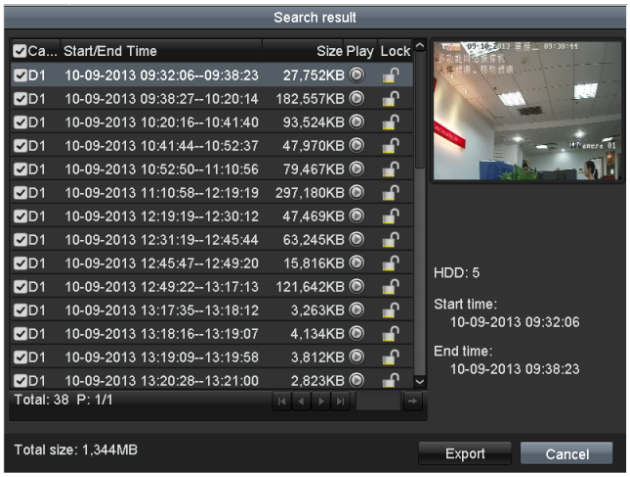


Figure 7. 9 Result of Normal Video Search for Backup

4. Export.

Click **Export** button and start backup.

NOTE

If the inserted USB writer is not recognized:

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

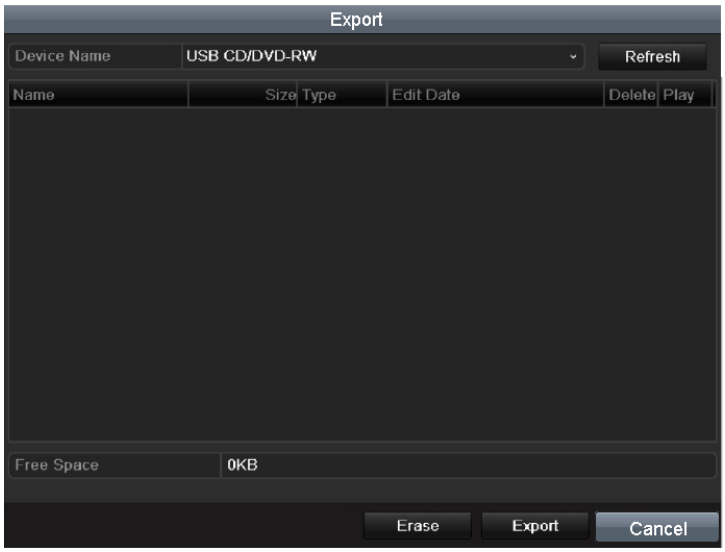


Figure 7. 10 Export by Normal Video Search using USB Writer

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

5. Check backup result.

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

NOTE

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

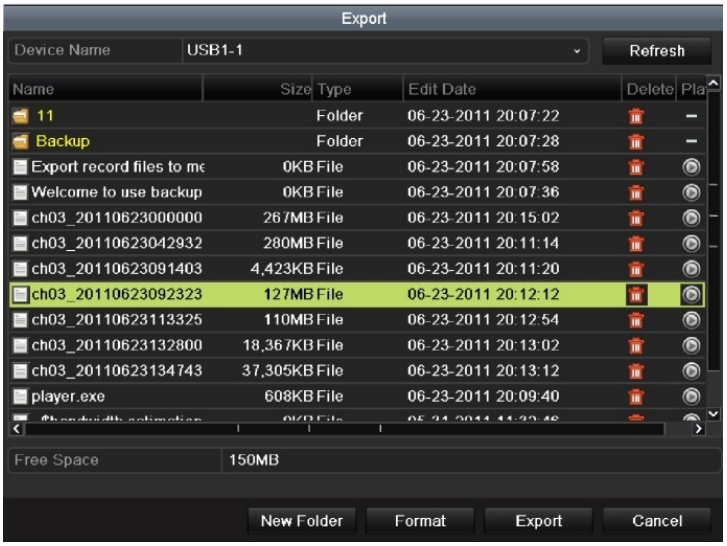


Figure 7. 11 Checkup of Export Result using USB Writer

7.1.3 Backing up by Event Search

Purpose:

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

We take the backing up alarm input events as an example.

Steps:

1. Enter Export interface.

   Menu > Export > Event

2. Set the search precondition.

   1) Select **Alarm Input** from the drop-down list of Event Type.

   2) Select the **Alarm Input No.**, **Start Time** and **End Time**.

   3) Click **Search** button to enter the Search Result interface.

   NOTE

   Event types contain Alarm Input, Motion and VCA.

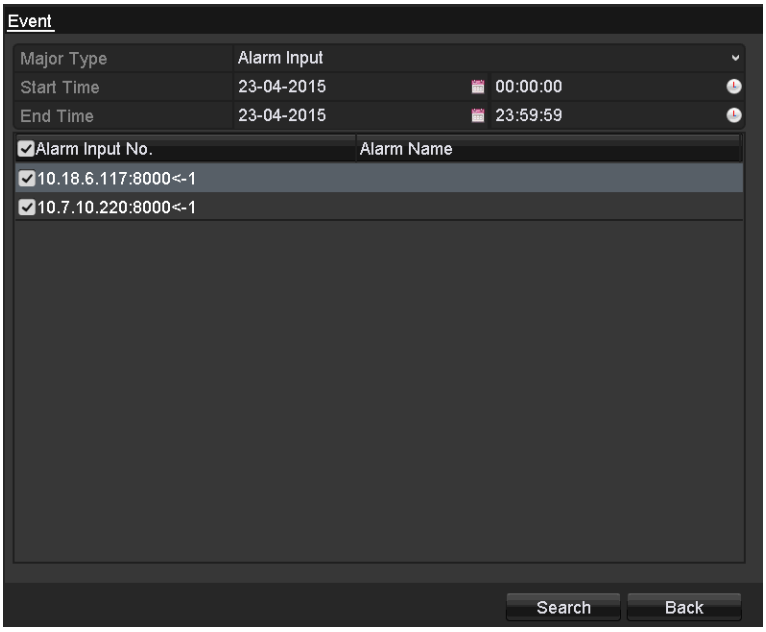


Figure 7. 12 Event Search for Backup

3. Select record files to export.

   1) Clicking **Quick Export** button will export record files of all channels triggered by the selected alarm input.

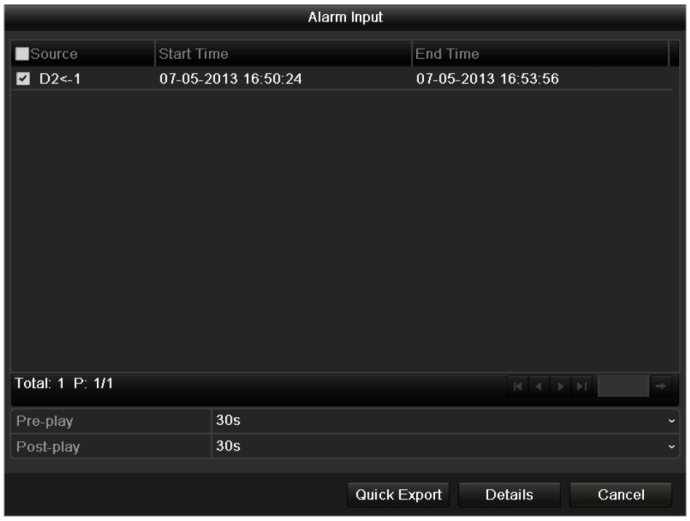


Figure 7. 13 Result of Event Search

2) Click **Details** button to view detailed information of the record file, e.g. start time, end time, file size, etc.

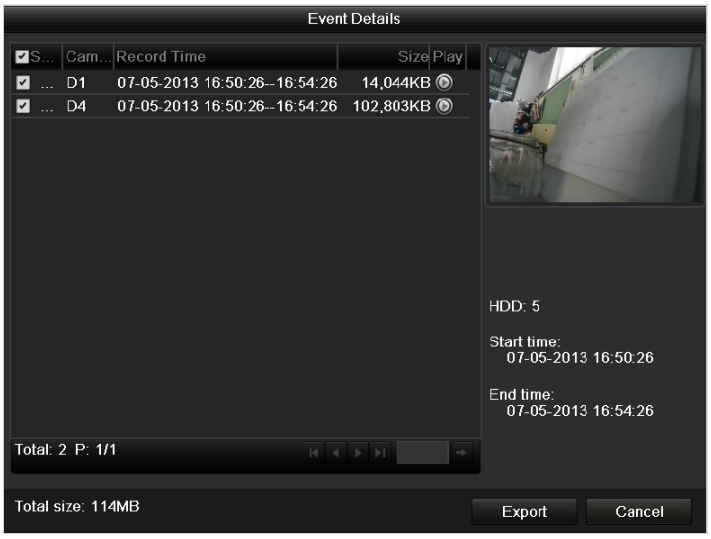


Figure 7. 14 Event Details Interface

4. Export record file.

Click **Export All** button to export all the record files.

Or you can select record files to back up, and click **Export** button to enter Export interface.

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 drive or USB HDDs via the device.

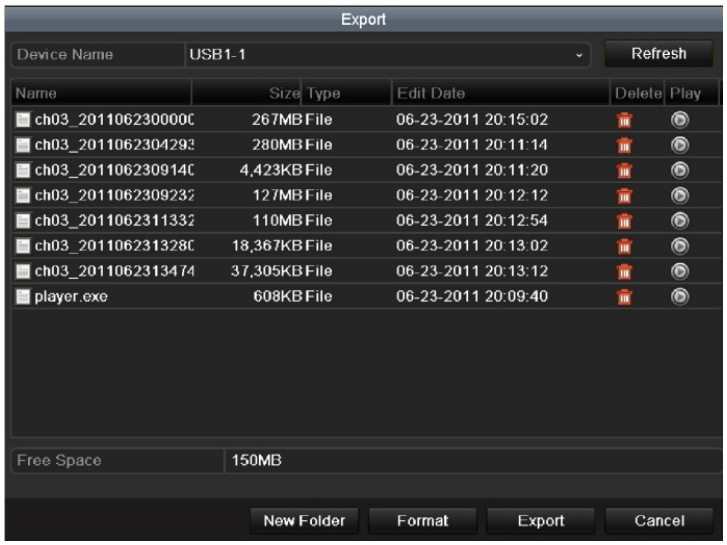


Figure 7. 15 Export by Event Using USB Flash Drive

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

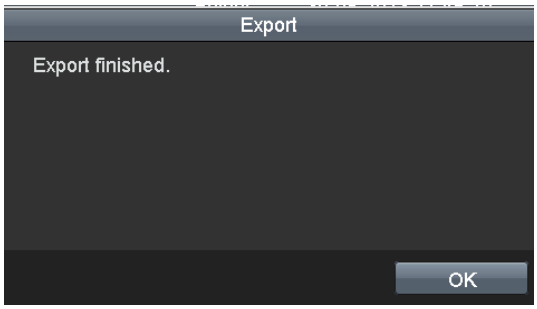


Figure 7. 16 Export Finished

5. Check backup result.

NOTE

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

7.1.4 Backing up Video Clips

Purpose:

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

Steps:

1. Enter Playback interface.

   Please refer to *Chapter 6.1 Playing Back Record Files.*
2. Click the button in playback toolbar to start clipping current playback file.
3. Click stop clipping.
4. Click to enter Export interface.

NOTE

Up to 30 clips can be clipped for each channel.

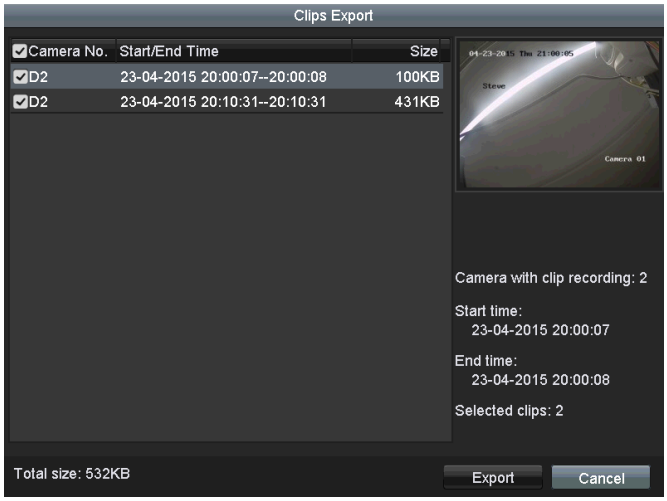


Figure 7. 17 Clips Export Interface

5. Export the clips.

Click **Export** to start backing up.

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 drive or USB HDDs via the device.

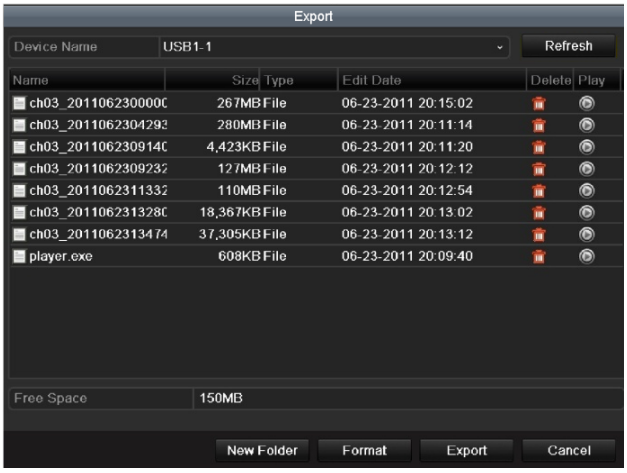


Figure 7. 18 Export Video Clips Using USB Flash Drive

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

6. Check backup result.

NOTE

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

7.2 Managing Backup Devices

Management of USB flash drives and USB HDDs

Steps:

1. Enter Search Result interface of record files.

   Menu > Export > Normal

2. Set search condition, including IP Camera, Record Type, File Type, Start Time and End Time.
3. Click **Search** button to enter Search Result interface.

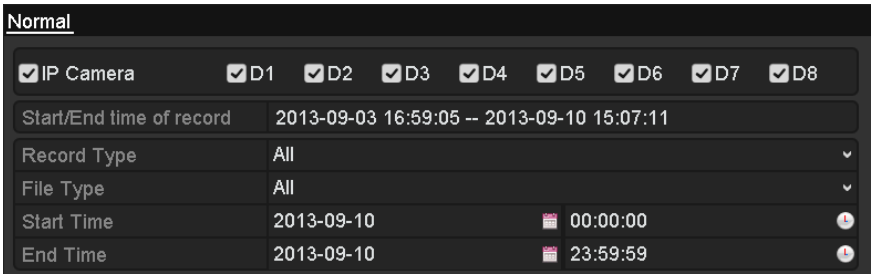


Figure 7. 19 Normal Video Search for Backup

4. Click **Export All** button to export all the record files.

   Or you can select record files to back up, and click **Export** button to enter Export interface.

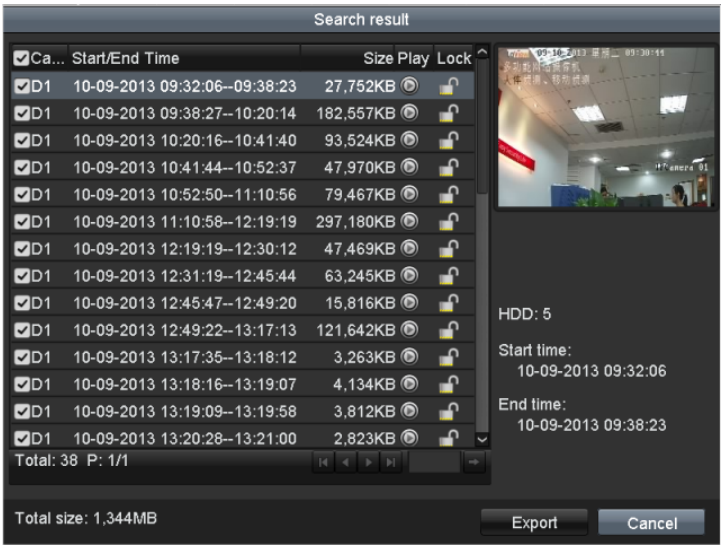


Figure 7. 20 Result of Normal Video Search for Backup

5. Backup device management.

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

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

   Select a record file in the backup device and click button to play it.

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

NOTE

If the inserted USB device is not recognized:

- Click the **Refresh** button.

- Reconnect device.
- Check for compatibility from vendor.

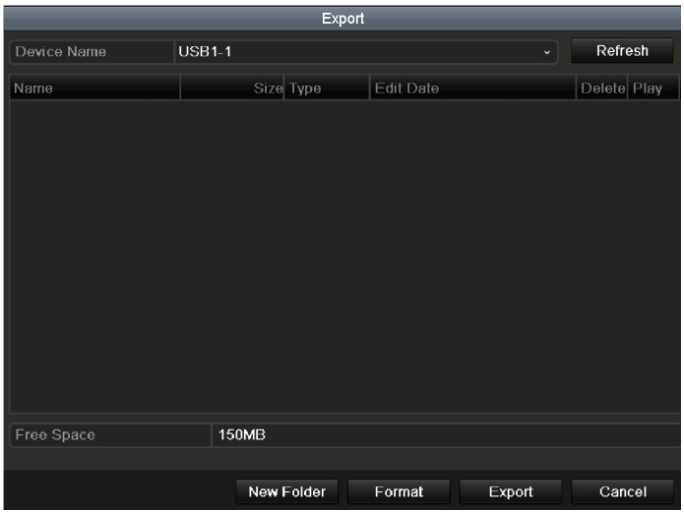


Figure 7. 21 USB Flash Drive Management

Management of USB writers

1. Enter Search Result interface of record files.

   Menu > Export > Normal

2. Set search condition.
3. Click **Search** button to enter Search Result interface.

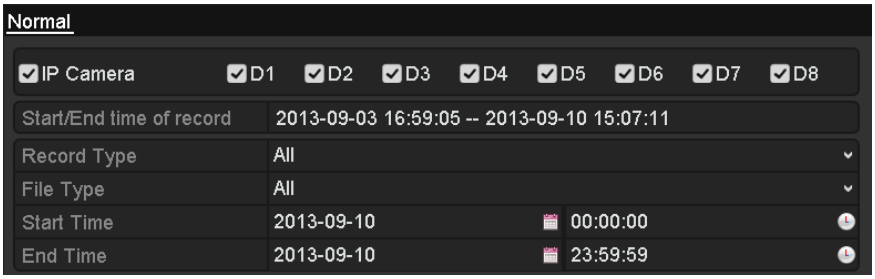


Figure 7. 22 Normal Video Search for Backup

4. Select record files you want to back up.

   Click **Export All** button to export all the record files.

   Or you can select record files to back up, and click **Export** button to enter Export interface.

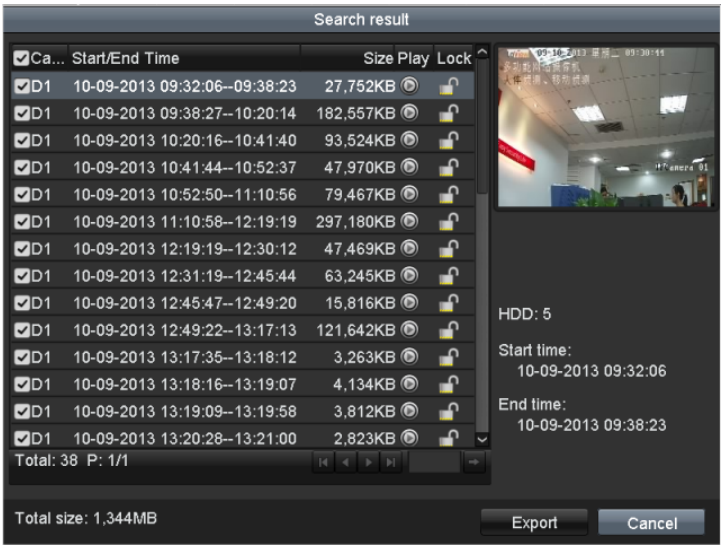


Figure 7. 23 Result of Normal Video Search for Backup

5. Backup device management.

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

NOTE

- There must be a re-writable CD/DVD when you make this operation.
- If the inserted USB writer is not recognized:
  - Click the **Refresh** button.
  - Reconnect device.
  - Check for compatibility from vendor.

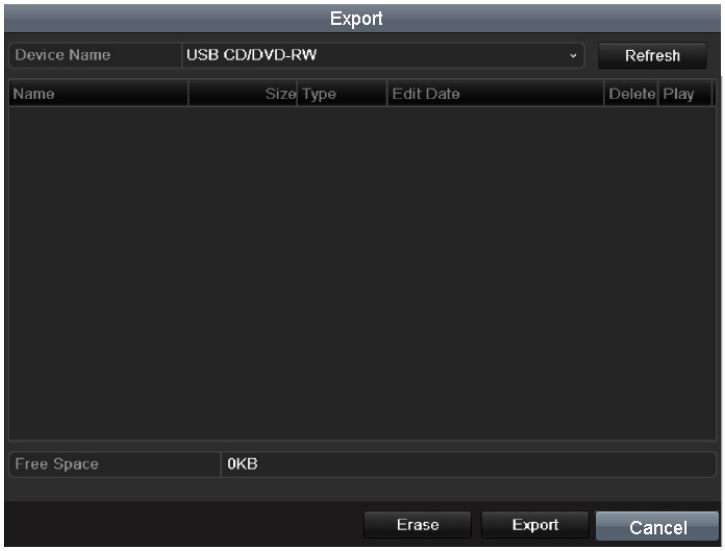


Figure 7. 24 USB Writer Management

Chapter 8 Alarm Settings

8.1 Setting Motion Detection Alarm

Steps:

1. Enter Motion Detection interface of Camera Management.

   Menu > Camera > Motion
2. Select a **Camera** to set up motion detection from the drop-down list.
3. Check **Enable Motion Detection** checkbox.
4. Use the mouse to draw detection area(s) in the right live view window.
5. Drag the scroll bar to set the **Sensitivity**.

   NOTE

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

Figure 8. 1 Motion Detection Setup Interface

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

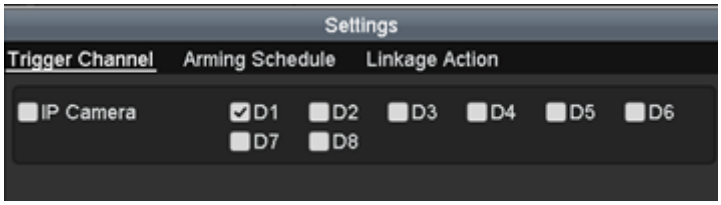


Figure 8. 2 Set Trigger Camera of Motion Detection

8. Configure Arming Schedule of the channel.
   1) Select **Arming Schedule** tab.
   2) Choose one day of a **Week**. Up to eight periods can be set within each day.
   3) Click **Apply** to save the settings

   NOTE

   Time periods shall not be repeated or overlapped.

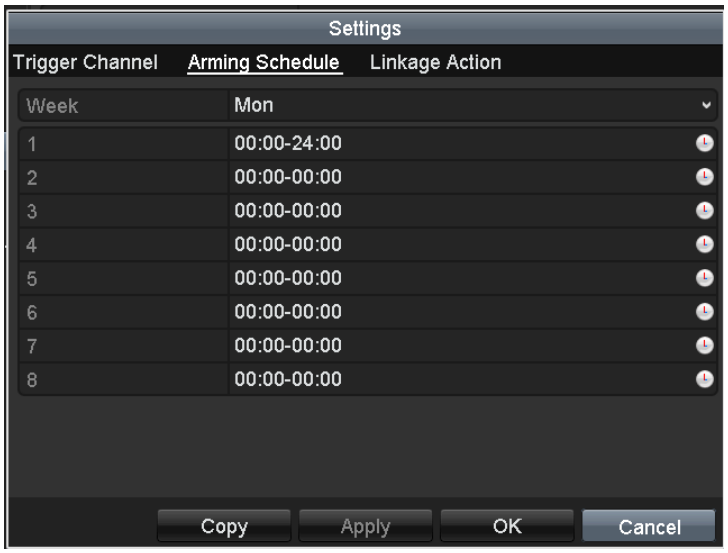


Figure 8. 3 Set Arming Schedule of Motion Detection

9. Click **Linkage Action** tab to configure alarm response actions. For details, please refer to section *8.6 Handling Exceptions Alarm*.
10. If you want to set motion detection for another channel, repeat the above steps or click **Copy** in the Motion Detection interface to copy the above settings to it.

8.2 Setting Sensor Alarms

Purpose:

Set the handling action of an external sensor alarm.

Steps:

1. Enter Alarm Settings of System Configuration.

   Menu > Configuration > Alarm

2. Select **Alarm Input** tab to enter Alarm Input Settings interface.

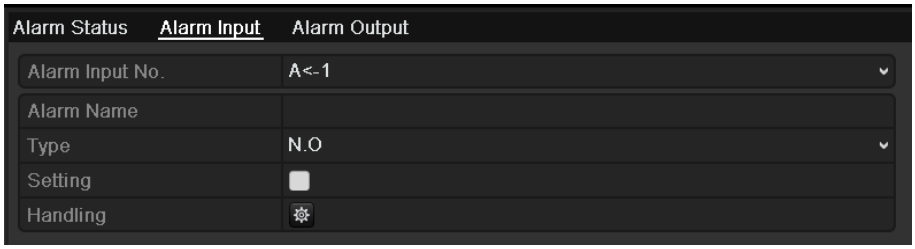


Figure 8. 4 Alarm Input Setup Interface

3. Select **Alarm Input No.** in the drop-down list.
4. Check the **Enable** checkbox.
5. Click the button after **Settings** to set up its alarm response actions.
6. Select **Trigger Channel** tab and select one or more channels which will start to record or become full-screen monitoring when an external alarm is input, and click **Apply** to save the settings.

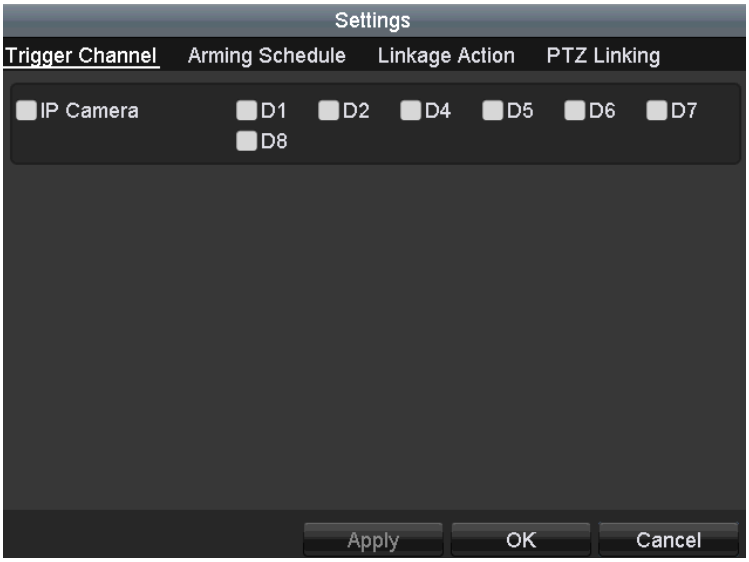


Figure 8. 5 Trigger Channel Settings

7. Select **Arming Schedule** tab to set the arming schedule of handling actions.
   1) Choose one day of a week. Up to eight periods can be set within each day
   2) Click **Apply** to save the settings.

NOTE

Time periods cannot 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.

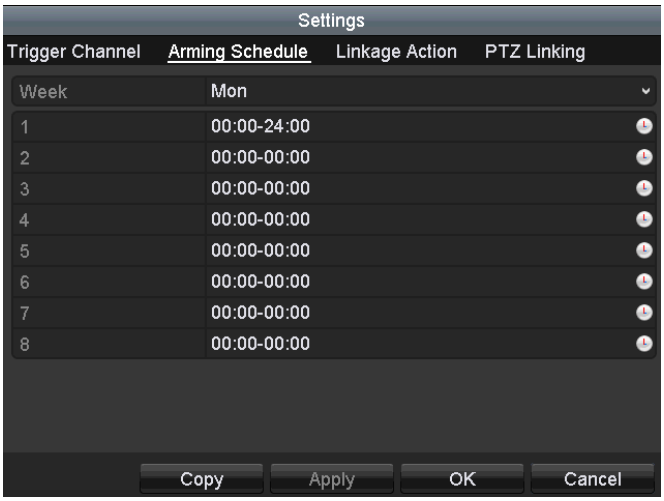


Figure 8. 6 Set Arming Schedule of Alarm Input

8. Select **Linkage Action** tab to configure alarm response actions. For details, please refer to section *8.6 Handling Exceptions Alarm*.
9. If necessary, select **PTZ Linking** tab to set PTZ linkage for the alarm input.

NOTE

Before the setting, check whether the selected speed dome supports PTZ linkage or not.

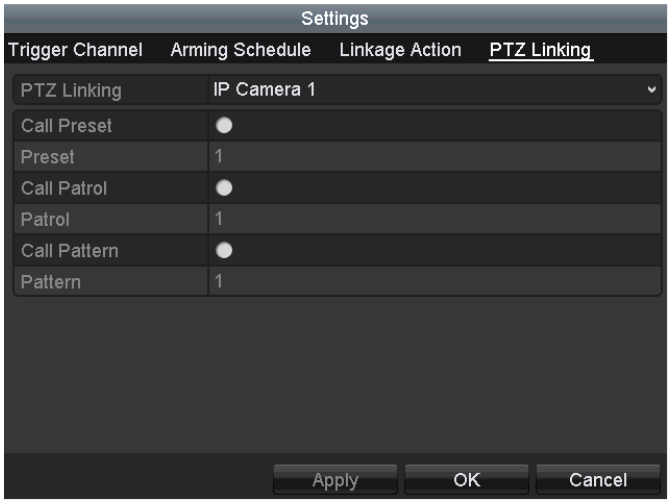


Figure 8. 7 Set PTZ Linking of Alarm Input

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

    One alarm input can trigger presets, patrol or pattern of more than one channel. But presets, patrols and patterns are exclusive.
11. If you want to set handling action of another alarm input, repeat the above steps.

    Or click the **Copy** on the Alarm Input Setup interface and check the checkbox of alarm inputs to copy the settings to them.

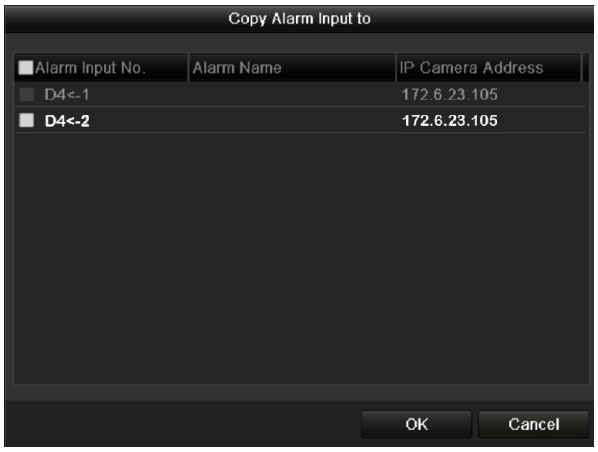


Figure 8. 8 Copy Settings of Alarm Input

8.3 Detecting Video Loss Alarm

Purpose:

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

Steps:

1. Enter Video Loss interface of Camera Management.

   Menu > Camera > Video Loss

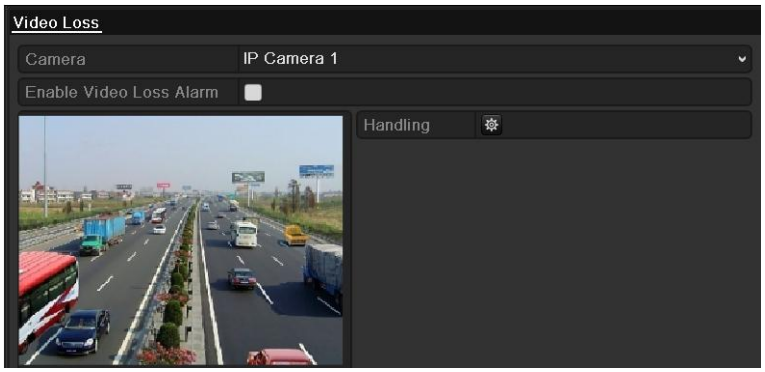


Figure 8. 9 Video Loss Setup Interface

2. Select a **Camera** in the drop-down list.
3. Check the checkbox of **Enable Video Loss Alarm**.
4. Click button after **Settings** to configure handling action of video loss.
5. Configure **Arming schedule** for the Linkage Actions.
   1) Click **Arming Schedule** tab.
   2) Choose one day of a **Week**. Up to eight periods can be set within each day.
   3) Click **Apply** button to save the settings.

NOTE

Time periods shall not be repeated or overlapped.

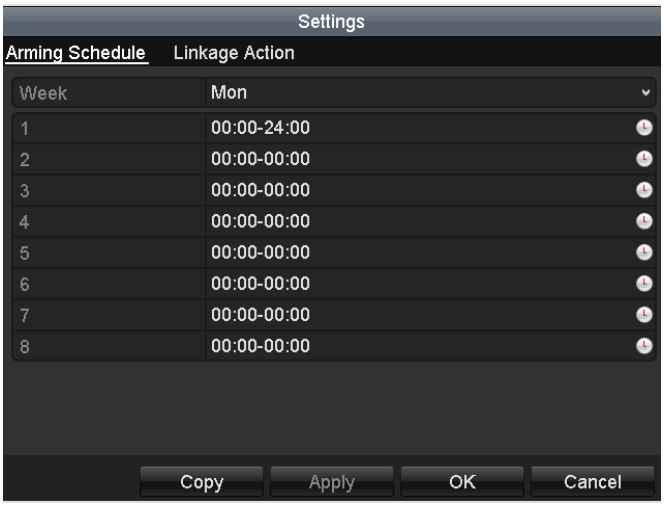


Figure 8. 10 Set Arming Schedule of Video Loss

6. Select **Linkage Action** tab to configure alarm response action. For details, please refer to section *8.6*

Handling Exceptions Alarm.

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

8.4 Detecting Video Tampering Alarm

Purpose:

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

Steps:

1. Enter Video Tampering interface.

   Menu > Camera > Video Tampering

Figure 8. 11 Video Tampering Setup Interface

2. Select the **Camera** in the drop-down list.
3. Check the checkbox of **Enable Video Tampering Detection**.
4. Drag the scroll bar to set the **Sensitivity**.
5. Use the mouse to draw an area in the right live view window to detect video tampering.
6. Click  button to configure handling action.
7. Set **Arming Schedule** parameters.
   1) Click **Arming Schedule** tab.
   2) Choose one day of a **Week**. Up to eight periods can be set within each day.
   3) Click **Apply** button to save the settings.

Time periods cannot be repeated or overlapped.

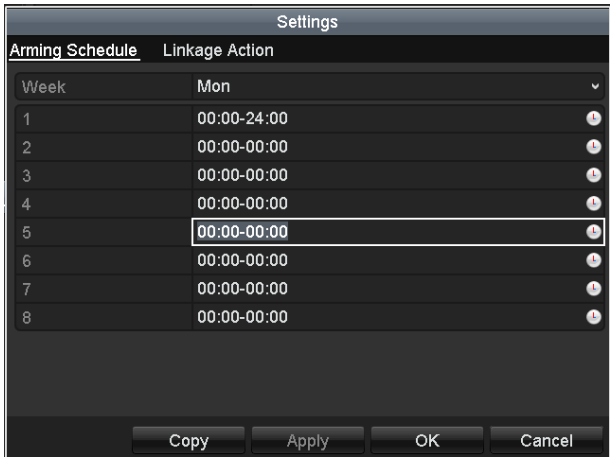


Figure 8. 12 Set Arming Schedule of Video Tampering

8. Select **Linkage Action** tab to configure alarm response actions. For details, please refer to section *8.6*

Handling Exceptions Alarm.

9. Click the **OK** button to save the settings.

8.5 Detecting VCA Alarm

Purpose:

The NVR can receive the VCA alarm sent by IP camera, and the VCA detection must be enabled and configured on the IP camera settings interface first. Refer to the user manual of IP camera for detailed instructions to set the VCA rules.

Steps:

1. Enter VCA Alarm interface of Camera Management.

   Menu > Camera > VCA

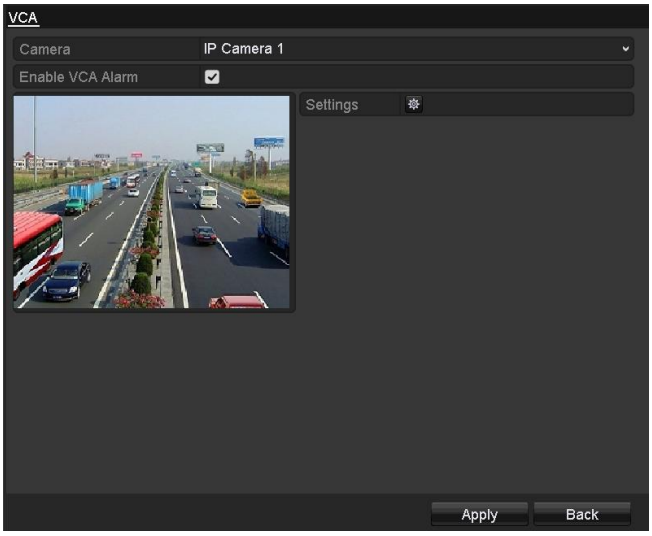


Figure 8. 13 VCA Alarm Setting Interface

2. Select a **Camera** in the drop-down list.
3. Check the **Enable VCA Alarm** checkbox.
4. Click the button after **Settings** to configure alarm response actions.
5. Configure **Trigger Channel** settings.
   1) Select **Trigger Channel** tab.
   2) Select one or more channels which will start to record or become full-screen monitoring when a VCA alarm is triggered.
   3) Click **Apply** to save the settings.
6. Configure **Arming Schedule** settings.
   1) Select **Arming Schedule** tab.
   2) Choose one day of a **Week**. Up to eight periods can be set within each day
   3) Click **Apply** to save the settings.

   NOTE

   Time periods shall not be repeated or overlapped.
   4) Repeat the above steps to set up arming schedule of other days of a week. You can also use **Copy** button to copy the arming schedule to other days.

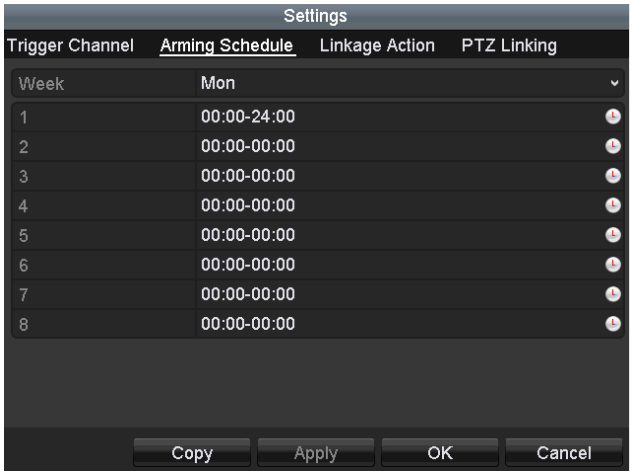


Figure 8. 14 Set Arming Schedule of VCA Alarm

7. Select **Linkage Action** tab to configure alarm response actions. For details, please refer to section *8.6 Handling Exceptions Alarm*.
8. If necessary, select PTZ Linking tab and set PTZ linkage of the VCA alarm, refer to step 6 of *section 8.2 Setting Sensor Alarms.*
9. Click the **OK** button to save the settings.

8.6 Handling Exceptions Alarm

Purpose:

Exception settings refer to the handling action of various exceptions.

Steps:

1. Enter Exception settings interface.

   Menu > Configuration > Exception

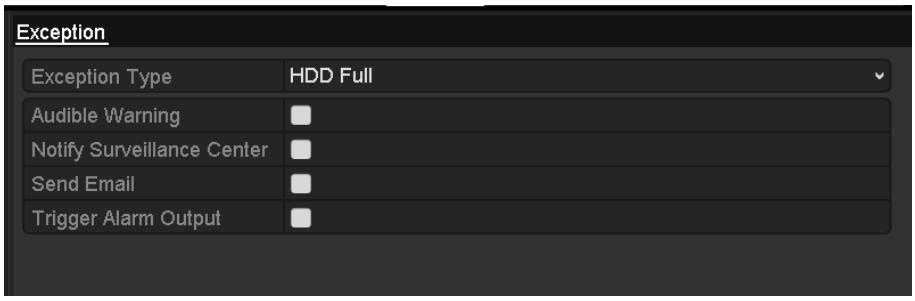


Figure 8. 15 Exception Settings

2. Select the Exception Type in the drop-down list. Up to 6 kinds types are available.
   - **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.
3. Check the checkbox of linkage action. Up to 4 linkage actions are available.
   - **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 section *9.2.5 Configuring Remote Alarm Host* for details of alarm host configuration.
   - **Send Email**

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

     Please refer to section *9.2.9 Configuring Email* for details of Email configuration.
   - **Trigger Alarm Output**

     Trigger an alarm output when an alarm occurs.

     You need to configure the dwell time and arming schedule for the alarm output.

     a) Enter Alarm Output interface.

        Menu > Configuration > Alarm > Alarm Output

     b) Select an **Alarm Output No.**.

c) Input the **Alarm Name** and set the **Dwell Time**.

NOTE

If **Manually Clear** is selected for **Dwell Time**, it only be cleared in Menu > Manual > Alarm.

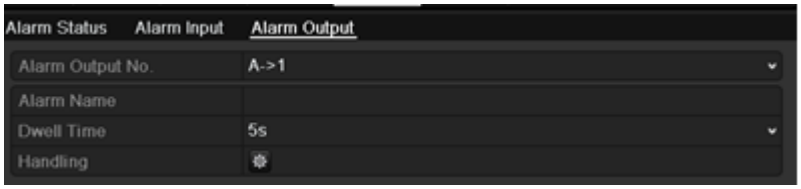


Figure 8. 16 Alarm Output Setup Interface

d) Set the Arming Schedule.

i. Click the button after Settings.

ii. Choose one day of a **Week**. Up to 8 periods can be set within each day.

NOTE

Time periods shall not be repeated or overlapped.

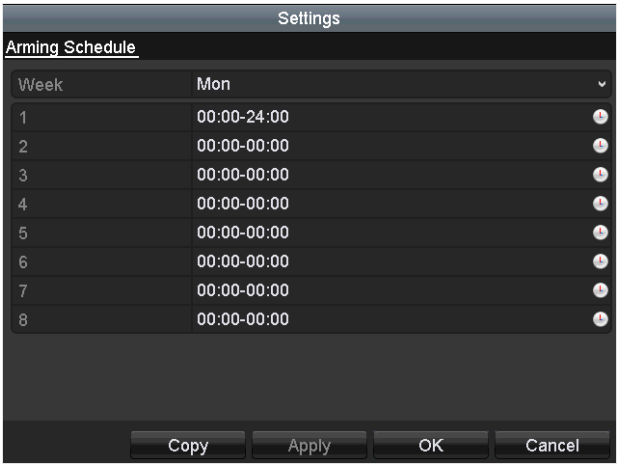


Figure 8. 17 Set Arming Schedule of Alarm Output

iii. Repeat the above steps to configure arming schedule for other days. You can also click **Copy** to copy the arming schedule to other days.

iv. Click the **OK** button to save the settings and back to Alarm Output interface.

e) Optionally, click **Copy** to copy the above settings to other alarm outputs.

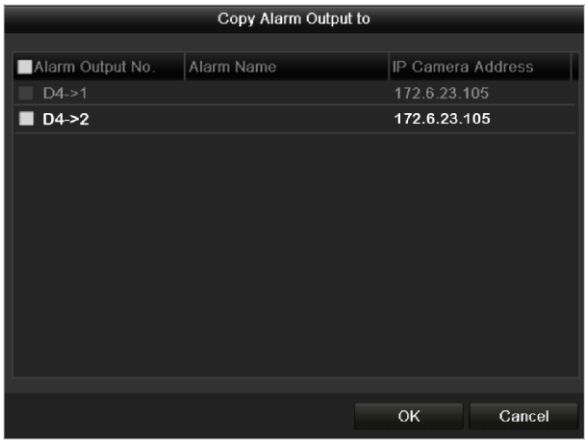


Figure 8. 18 Copy Settings of Alarm Output

8.7 Setting Event Hint Display

Purpose:

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

Steps:

1. Enter the Exception settings interface.

   Menu > Configuration > Exceptions

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

Figure 8. 19 Event Hint Settings Interface

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

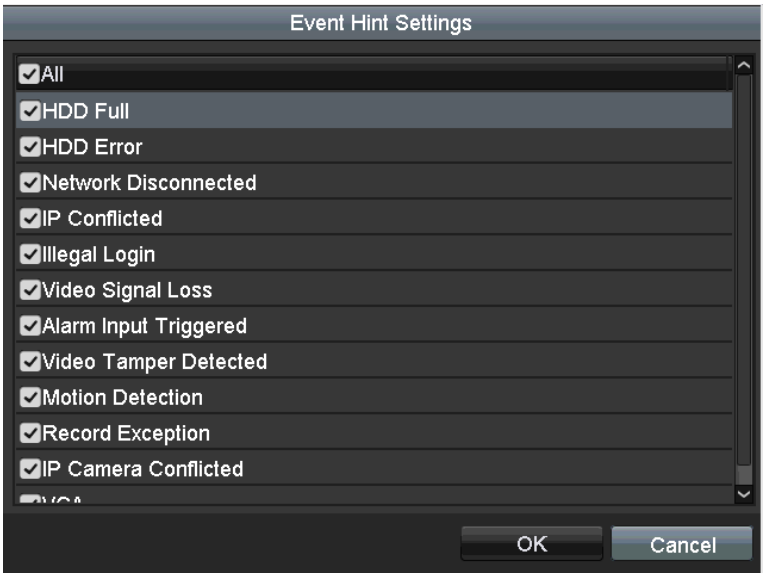


Figure 8. 20 Event Hint Settings Interface

4. Check the checkbox of events to hint.
5. Click the **OK** button to save the settings.

8.8 Triggering or Clearing Alarm Output Manually

Purpose:

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

Steps:

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

   Menu> Manual> Alarm

2. Trigger / clear an alarm output.

   1) Click to select an Alarm Output No..

   2) Click Trigger or Clear to trigger or clear the alarm output.

3. Click **Trigger All** to trigger all and click Clear All to clear all alarm outputs.

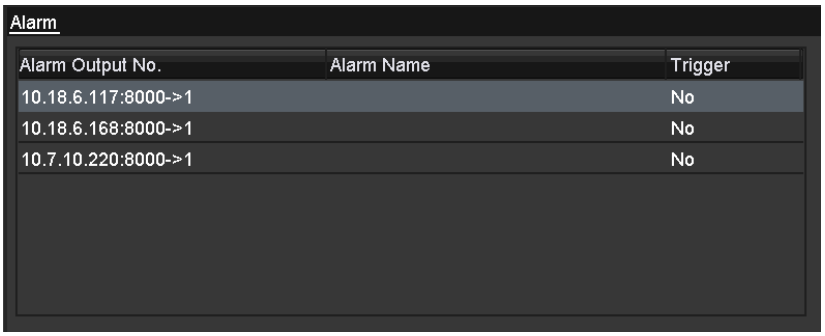


Figure 8. 21 Clear or Trigger Alarm Output Manually

Chapter 9 Network Settings

9.1 Configuring General Settings

Purpose:

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

Steps:

1. Enter the Network Settings interface.

   Menu > Configuration > Network

2. Select the **General** tab.

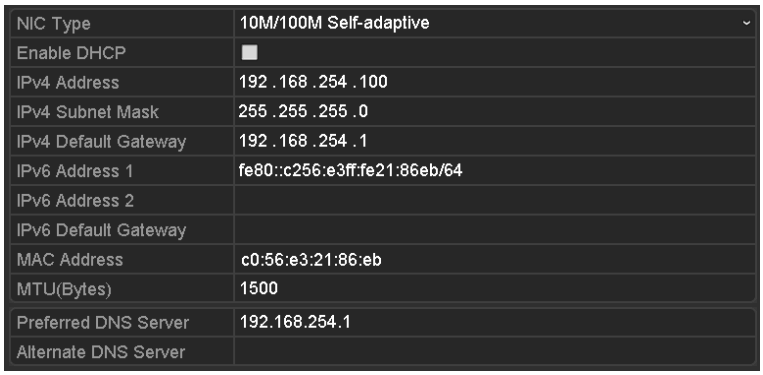


Figure 9. 1 Network Settings Interface

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

   NOTE

   - The valid value range of MTU is 500 ~ 9676.
   - If the DHCP server is available, you can check the checkbox of **Enable DHCP** to automatically obtain an IP address and other network settings.

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

9.2 Configuring Advanced Settings

9.2.1 Configuring Wireless Network

Configuring WAN Settings

Purpose:

The device provides you with wired and wireless network features, just as a wireless router. You can access to internet via NVR instead of a router.

Before you start:

Establish the connection between the NVR and Internet via the WAN interface.

Steps:

1. Enter WAN configuration interface.

   Menu > Configuration > WIFI

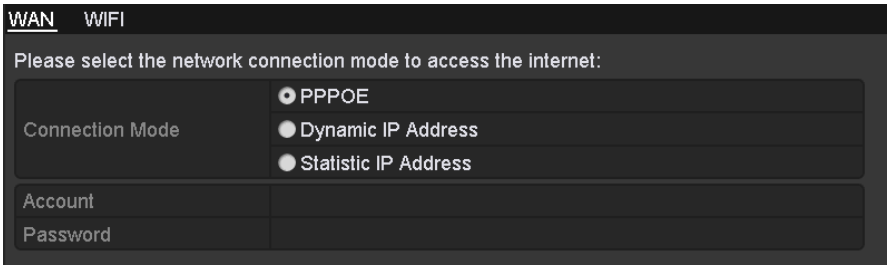


Figure 9. 2 WAN Configuration Interface

2. Select the **Connection Mode** as **PPPoE**.
3. Input **Account** and **Password** in the text field.
4. Click **Apply** to dial up.

Configuring WIFI Settings

Steps:

1. Enter WIFI configuration interface.

   Menu > Configuration > WIFI

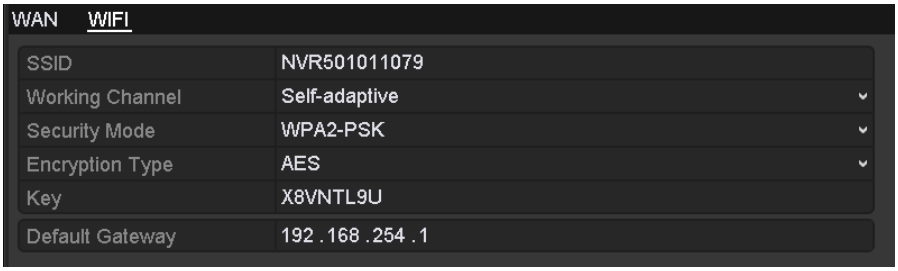


Figure 9. 3 WIFI Configuration Interface

2. Click the **WIFI** tab to enter WIFI configuration interface.
3. Input **SSID** in the text field.
   SSID: the name of WIFI.
4. Select **Working Channel** and **Security Type** in the drop-down list.
5. If **Security Type** is set other one of the four types except **Disable**, select **Encryption Type** and input **Network Security Key**.

   NOTE

   WPA2-PSK and **AES** is more secure than **WPA-PSK** and **TKIP**. However, there may terminals which do not support **WPA2-PSK** and **AES**. When you are not sure whether terminals support or not, you can select WPA-PSK/ WPA2-PSK and TKIP/AES to make NVR do the adaptive selection.
6. Input **Default Gateway**.
7. Click **Apply** to set up a wireless network.

9.2.2 Configuring Extranet Access

Configuring Cloud P2P

Purpose:

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 **Extranet Access** tab to enter the Cloud P2P Settings interface.
3. Check the **Enable Cloud P2P** checkbox to activate this feature.
4. If required, check the **Enable Stream Encryption** checkbox to encrypt the video stream.
5. Enter the **Verification Code** of the device.

   NOTE

   - The Verification Code consists of 6 capital letters and is located at the bottom of the NVR.
   - The device at the version 3.0.4 or above has its Verification Code automatically available in the filed by default; for device of older version, you need to input any 6 capital letters in the text filed.

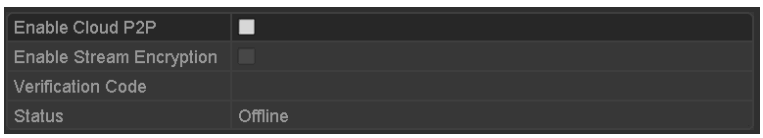


Figure 9. 4 Cloud P2P Settings Interface

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

After configuration, you can access and manage the NVR by your mobile phone on which the Cloud P2P application is installed.

NOTE

For more operation instructions, please refer to the help file.

Configuring DDNS

Purpose:

If your NVR is set to use PPP dialing 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 **Extranet Access** tab to enter the DDNS Settings interface, as shown in Figure 9. 5.

Figure 9. 5 DDNS Settings Interface

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

   - **LTS:**

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

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

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

Figure 9. 6 LTS Settings Interface

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

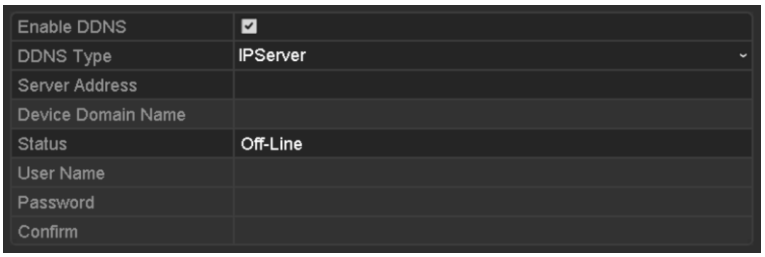


Figure 9. 7 IPServer Settings Interface

Figure 9. 8

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

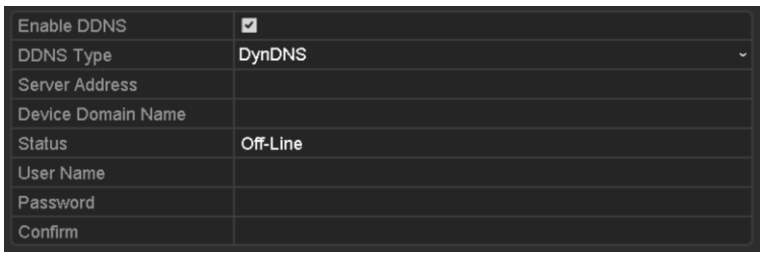


Figure 9. 9 DynDNS Settings Interface

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

Figure 9. 10 PeanutHull Settings Interface

- **NO-IP:**

  Enter the account information in the corresponding fields. Refer to the DynDNS settings.
  1) Enter **Server Address** for NO-IP.
  2) In the NVR Domain Name text field, enter the domain obtained from the NO-IP website (www.no-ip.com).
  3) Enter the **User Name** and **Password** registered in the NO-IP website.

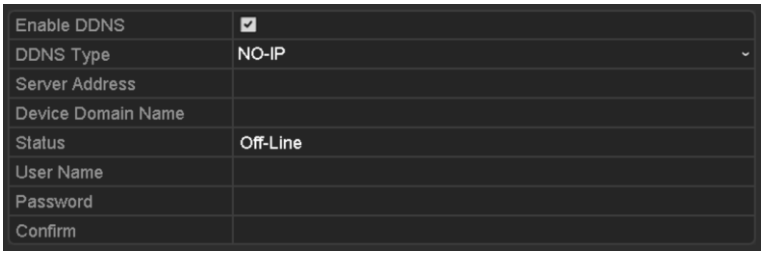


Figure 9. 11 NO-IP Settings Interface

- **HiDDNS:**
  1) The **Server Address** of the HiDDNS server appears by default: www.hiddns.com.
  2) Enter the **Device Domain Name.** You can use the alias you registered in the HiDDNS server or define a new device domain name. If a new alias of the device domain name is defined in the NVR, it will replace the old one registered on the server. You can register the alias of the device domain name in the HiDDNS server first and then enter the alias to the **Device Domain Name** in the NVR; you can also enter the domain name directly on the NVR to create a new one.

Figure 9. 12 HiDDNS Settings Interface

Register the device on the HiDDNS server.

1) Go to the HiDDNS website: www.hiddns.com.
2) Click Register new user to register an account if you do not have one and use the account to log in.

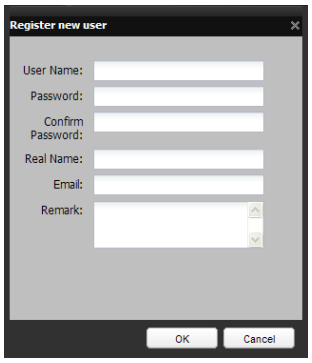


Figure 9. 13 Register an Account

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

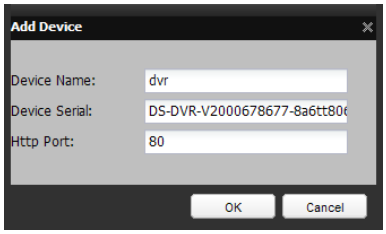


Figure 9. 14 Register the Device

NOTE

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

Access the Device via Web Browser or Client Software

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

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

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

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

NOTE

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

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

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

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

Server Address: www.hiddns.com

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

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

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

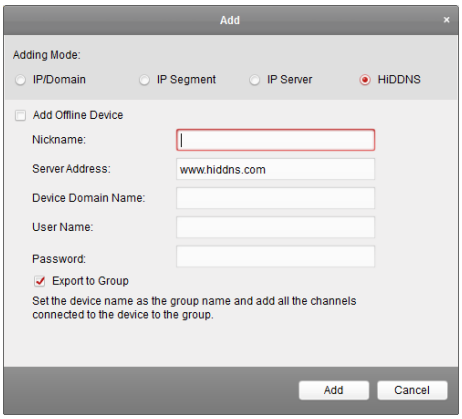


Figure 9. 15 Access Device via NVMS7000

5. Click the **Apply** button to save the settings.
   After setting all the required parameters for the DDNS, you can view the connecting status of the device by checking the **Status** information.

9.2.3 Configuring NTP Server

Purpose:

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

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 Network Settings interface.
   Menu > Configuration > Network
2. Select the **NTP** tab to enter the NTP Settings interface, as shown in Figure 9. 16.

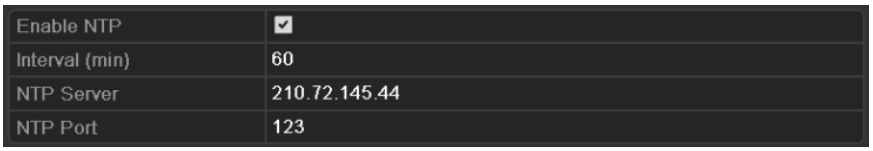


Figure 9. 16 NTP Settings Interface

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.

9.2.4 Configuring SNMP

Purpose:

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

NOTE

The SNMP is not supported by DS-7100NI-SL, DS-7100NI-SN and DS-7600NI-SN series NVR.

Steps:

1. Enter the Network Settings interface.
   Menu >Configuration> Network
2. Select the **SNMP** tab to enter the SNMP Settings interface, as shown in Figure 9. 17.

Figure 9. 17 SNMP Settings Interface

3. Check the **SNMP** checkbox to enable this feature.
4. Configure the following SNMP settings.
   - **Trap Address:** IP Address of SNMP host.
   - **Trap Port:** Port of SNMP host.
5. Click the **Apply** button to save and exit the interface.

NOTE

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

9.2.5 Configuring Remote Alarm Host

Purpose:

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

Steps:

1. Enter the Network Settings interface.
   Menu >Configuration> Network
2. Select the **More Settings** tab to enter the More Settings interface, as shown in Figure 9. 18.

Figure 9. 18 More Settings Interface

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., NVMS7000) 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

Purpose:

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 9. 18.
3. Set **Multicast IP**, as shown in Figure 9. 19. When adding a device to the Network Video Surveillance Software, the multicast address must be the same as the NVR's multicast IP.

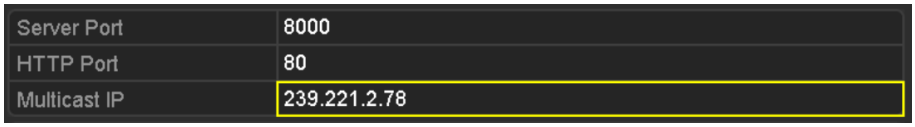


Figure 9. 19 Configure Multicast

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

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

9.2.7 Configuring RTSP

Purpose:

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 9. 18.

Figure 9. 20 RTSP Settings Interface

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

Purpose:

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 9. 18.
3. Enter new **Server Port** and **HTTP Port**.

Figure 9. 21 Host/Others Settings Menu

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

Purpose:

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

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

Steps:

1. Enter the Network Settings interface.
   Menu >Configuration> Network
2. Set the IPv4 Address, IPv4 Subnet Mask, IPv4 Gateway and the Preferred DNS Server in the Network Settings menu, as shown in Figure 9. 22.

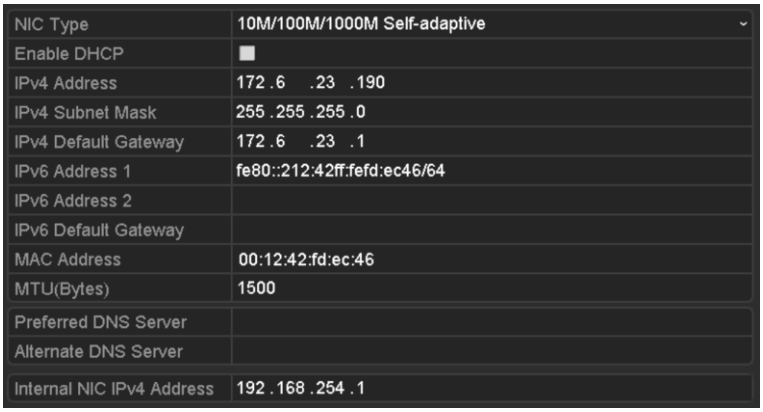


Figure 9. 22 Network Settings Interface

3. Click **Apply** to save the settings.
4. Select the Email tab to enter the Email Settings interface.

Figure 9. 23 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. Refer to Figure 9. 24.

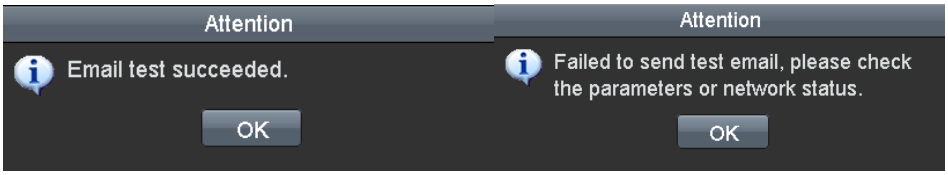


Figure 9. 24 Email Testing Attention

9.2.10 Configuring NAT

Purpose:

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

- **UPnP™**

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

Before you start:

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

Steps:

1. Enter the Network Settings interface.

   Menu > Configuration > Network

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

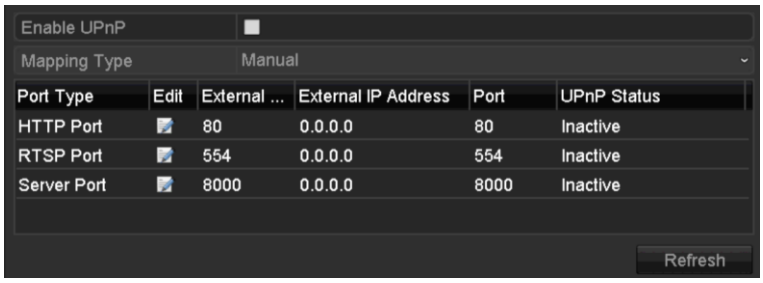


Figure 9. 25 UPnP™ Settings Interface

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

   OPTION 1: Auto

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

   Steps:

   1) Select **Auto** in the drop-down list of Mapping Type.
   2) Click **Apply** button to save the settings.
   3) You can click **Refresh** button to get the latest status of the port mapping.

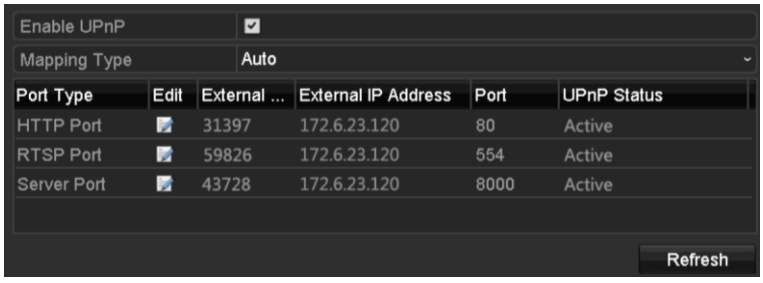


Figure 9. 26 UPnP™ Settings Finished-Auto

OPTION 2: Manual

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

Steps:

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

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

NOTE

- You can use the default port No., or change it according to actual requirements.
- External Port indicates the port No. for port mapping in the router.
- The value of the RTSP port No. should be 554 or between 1024 and 65535, while the value of the other ports should be between 1 and 65535 and the value must be different from each other. If multiple devices are configured for the UPnP™ settings under the same router, the value of the port No. for each device should be unique.

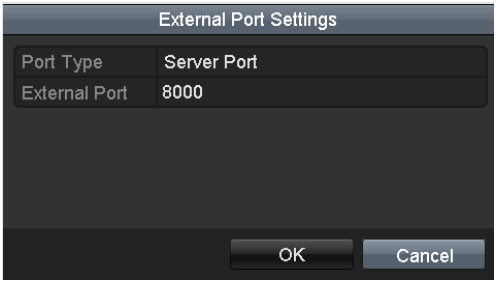


Figure 9. 27 External Port Settings Dialog Box

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

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

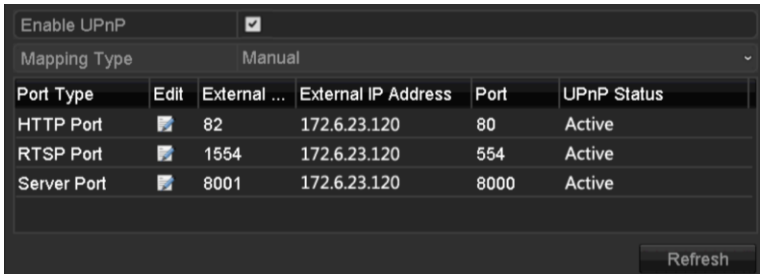


Figure 9. 28 UPnP™ Settings Finished-Manual

- **Manual Mapping**

If your router does not support the UPnP™ 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.

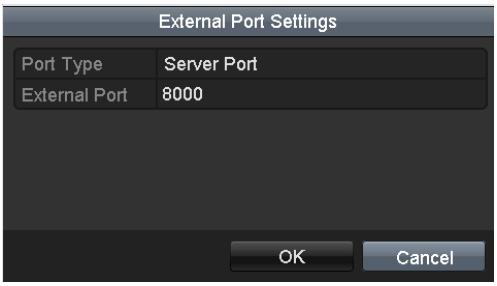


Figure 9. 29 External Port Settings Dialog Box

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

NOTE

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

Delete	External Source Port	Protocol	Internal Source IP	Internal Source Port	Application
☐	81	TCP	192.168.251.101	80	HTTP

Figure 9. 30 Setting Virtual Server Item

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

Purpose:

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

Steps:

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

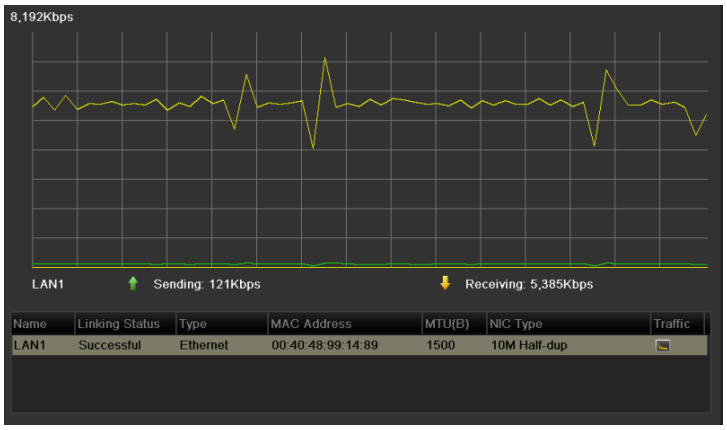


Figure 9. 31 Network Traffic Interface

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

9.4 Configuring Network Detection

Purpose:

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, as shown in Figure 9. 32.

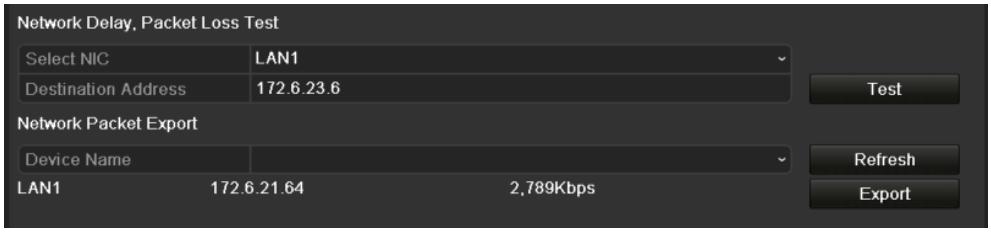


Figure 9. 32 Network Detection Interface

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. Refer to Figure 9. 33.

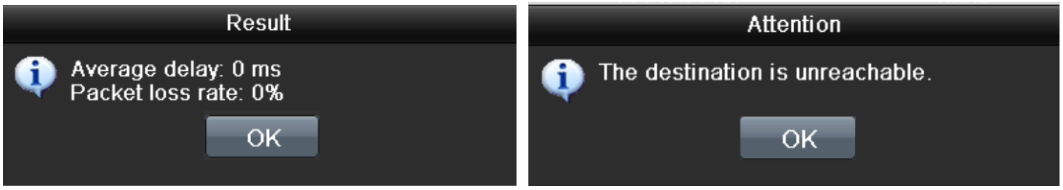


Figure 9. 33 Testing Result of Network Delay and Packet Loss

9.4.2 Exporting Network Packet

Purpose:

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 drop-down list of Device Name, as shown in Figure 9. 34.

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.

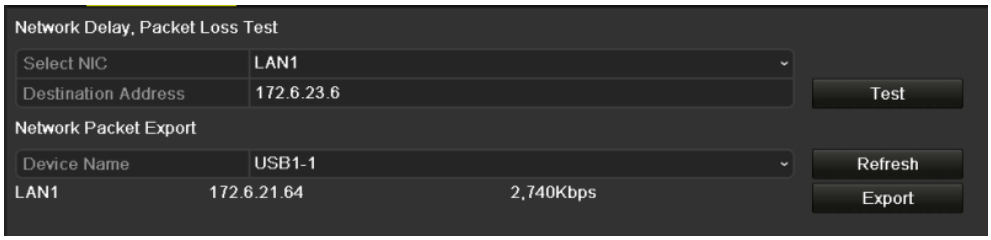


Figure 9. 34 Export Network Packet

4. Click **Export** button to start exporting.
5. After the exporting is complete, click **OK** to finish the packet export, as shown in Figure 9. 35.

Figure 9. 35 Packet Export Attention

Up to 1M data can be exported each time.

9.4.3 Checking the Network Status

Purpose:

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

Steps:

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

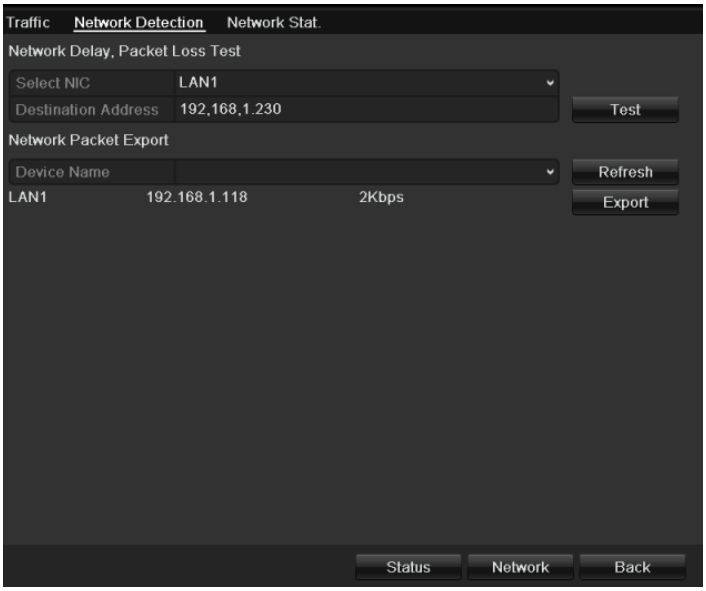


Figure 9. 36 Network Status Checking

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

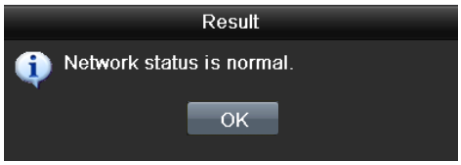


Figure 9. 37 Network status checking result

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

Purpose:

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

Steps:

1. Enter the Network Detection interface.

   Menu>Maintenance>Net Detect

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

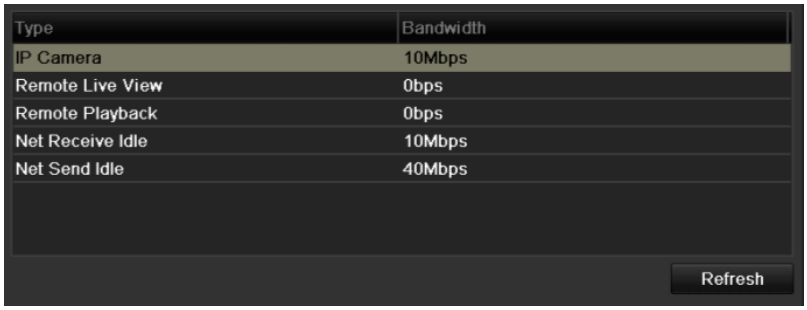


Figure 9. 38 Network Stat. Interface

3. Check the bandwidth of IP Camera, bandwidth of Remote Live View, bandwidth of Remote Playback, bandwidth of Net Receive Idle and bandwidth of Net Send Idle.
4. You can click **Refresh** to get the newest status.

Chapter 10 HDD Management

10.1 Initializing HDDs

Purpose:

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

Steps:

1. Enter the HDD Information interface.

   Menu > HDD> General

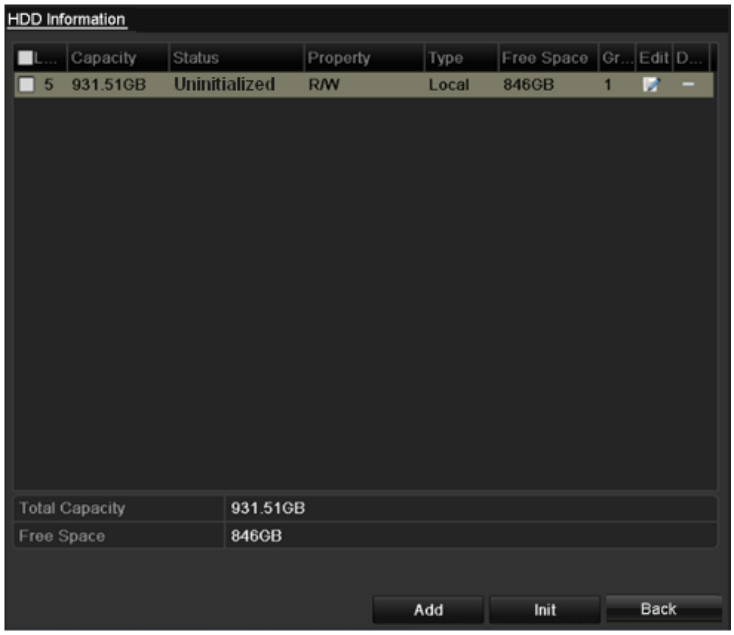


Figure 10. 1 HDD Information Interface

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

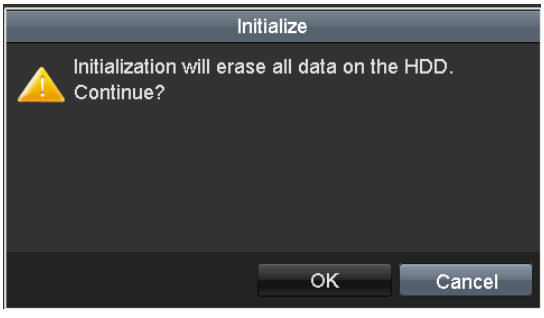


Figure 10. 2 Confirm Initialization

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

Figure 10. 3 Status changes to Initializing

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

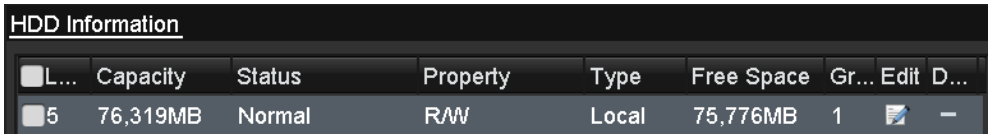


Figure 10. 4 HDD Status Changes to Normal

NOTE

Initializing the HDD will erase all data on it.

10.2 Managing Network HDD

Purpose:

You can add the network HDDs, including NAS and IP SAN, to NVR.

Steps:

1. Enter the HDD Information interface.

   Menu > HDD > General

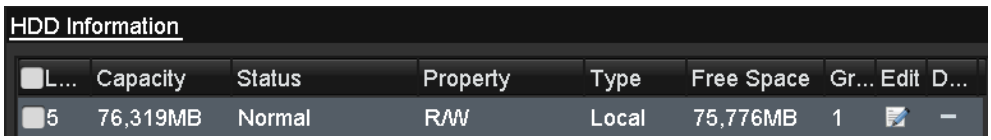


Figure 10. 5 HDD Information Interface

2. Click the **Add** to enter the Add NetHDD interface, as shown in Figure 10. 6.

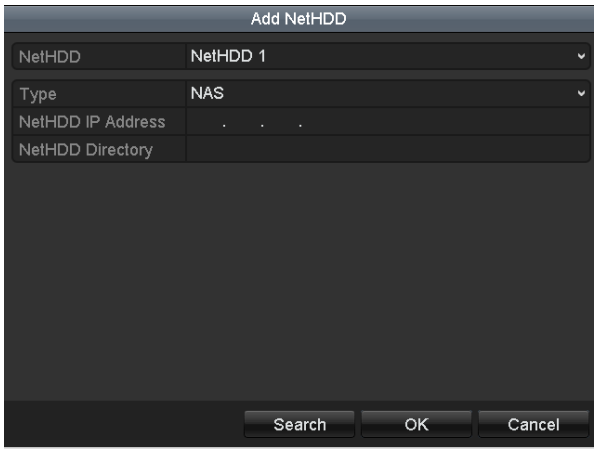


Figure 10. 6 HDD Information Interface

3. Select the **NetHDD** No. in the drop-down list.
4. Select the type as NAS or IP SAN.
5. Configure the NAS or IP SAN settings.

   Up to 8 NAS disks can be added and only 1 IP SAN disk can be added.

   - **Add NAS disk:**

   1) Enter the NetHDD IP address in the text field.
   2) Click the **Search** button to search the online NAS disks.
   3) Click o 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 **OK** to add the configured NAS disk.

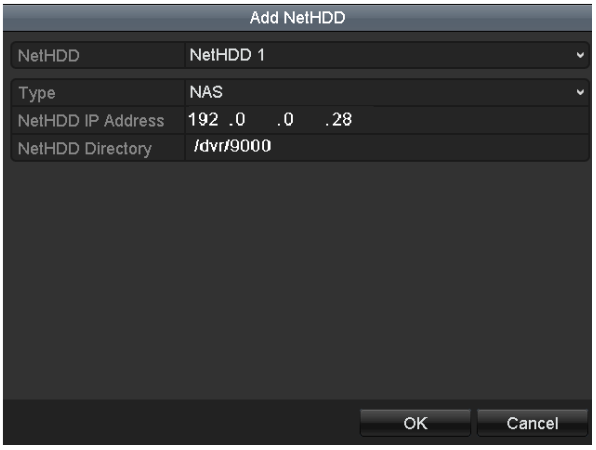


Figure 10. 7 Add NAS Disk

- **Add IP SAN:**

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

Figure 10. 8 Add IP SAN Disk

6. The added NetHDD will be displayed in the list.

NOTE

Initialize the added NetHDD before using. For details, please refer to section *10.2 Managing Network HDD*.

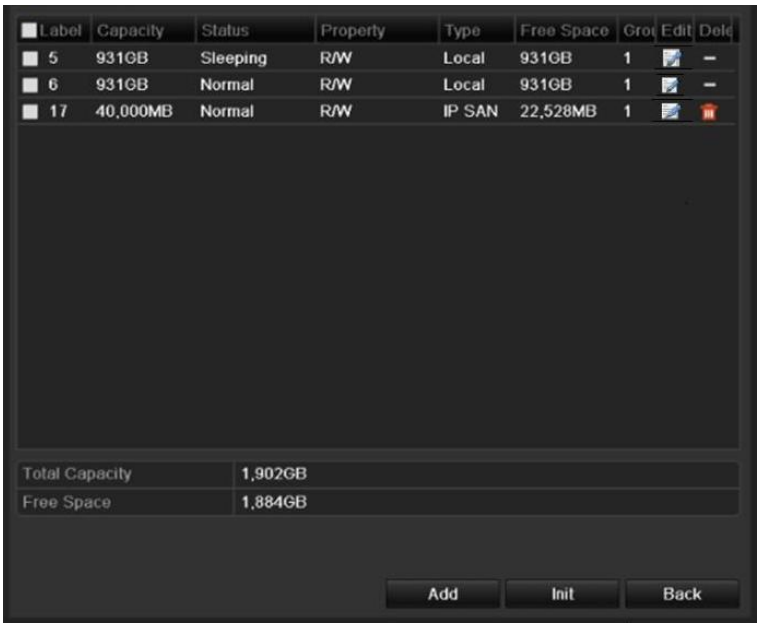


Figure 10. 9 Initialize Added NetHDD

10.3 Configuring Quota Mode

Purpose:

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

Steps:

1. Enter the Storage Mode interface.

   Menu > HDD > Advanced

2. Set the **Mode** to Quota, as shown in Figure 10. 10.

NOTE

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

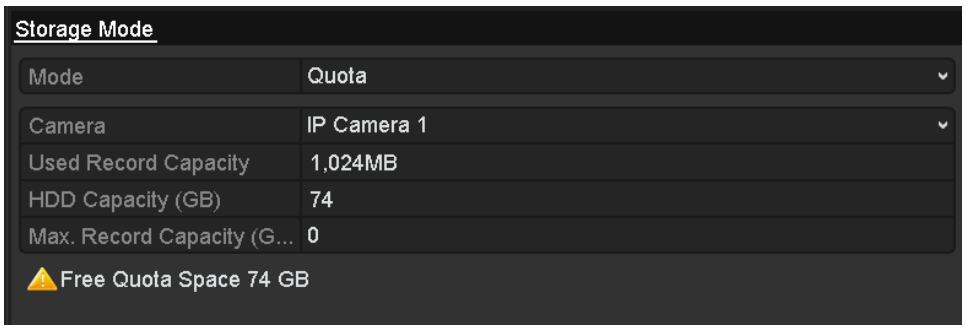


Figure 10. 10 Storage Mode Settings Interface

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)**, as shown in Figure 10. 11.

Figure 10. 11 Configure Record Quota

5. You can copy the quota settings of the current camera to other cameras if required. Click the **Copy** button to enter the Copy Camera menu, as shown in Figure 10. 12.

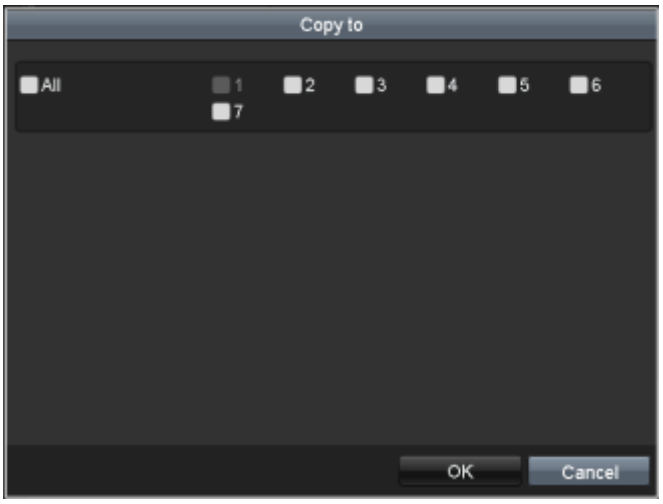


Figure 10. 12 Copy Settings to Other Camera(s)

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

NOTE

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

10.4 Checking HDD Status

Purpose:

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

Checking HDD Status in HDD Information Interface

Steps:

1. Enter the HDD Information interface.

   Menu > HDD > General

2. Check the status of each HDD which is displayed on the list, as shown in Figure 10. 13.

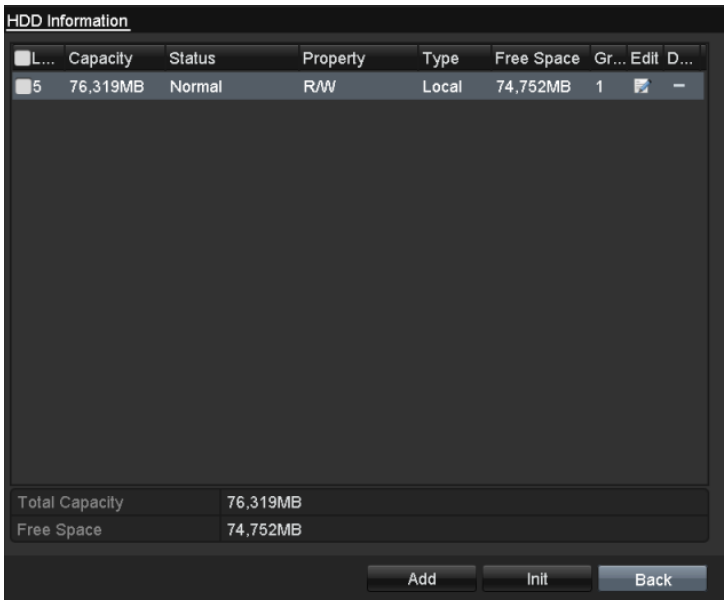


Figure 10. 13 View HDD Status (1)

NOTE

If the status of HDD is *Normal*, 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 HDD status, as shown in Figure 10. 14.

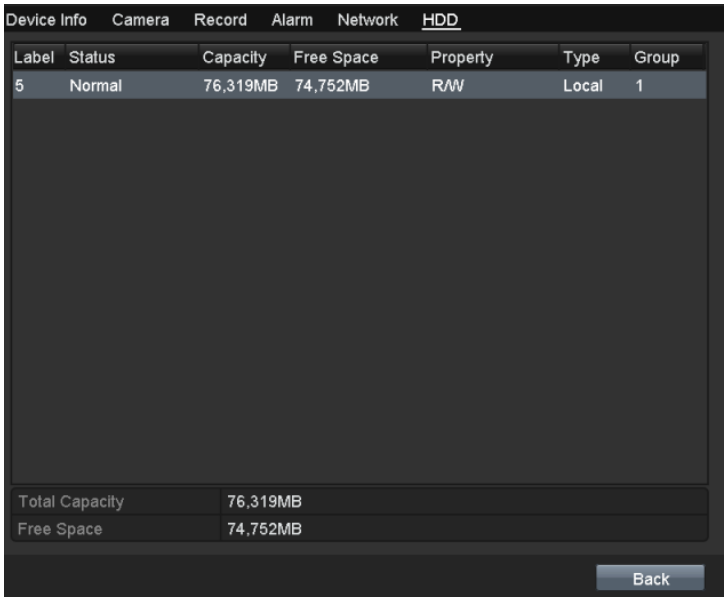


Figure 10. 14 View HDD Status (2)

10.5 HDD Detection

Purpose:

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

S.M.A.R.T. Settings

Steps:

1. Enter the S.M.A.R.T Settings interface.
   Menu > Maintenance > HDD Detect
2. Select the HDD to view its S.M.A.R.T information list, as shown in Figure 10. 15.
   The related information of the S.M.A.R.T. is shown on the interface.
3. Test the HDD.
   1) Select the Self-test Type as Short Test, Expanded Test or the Conveyance Test.
   2) Click the button to start the S.M.A.R.T. HDD self-evaluation.

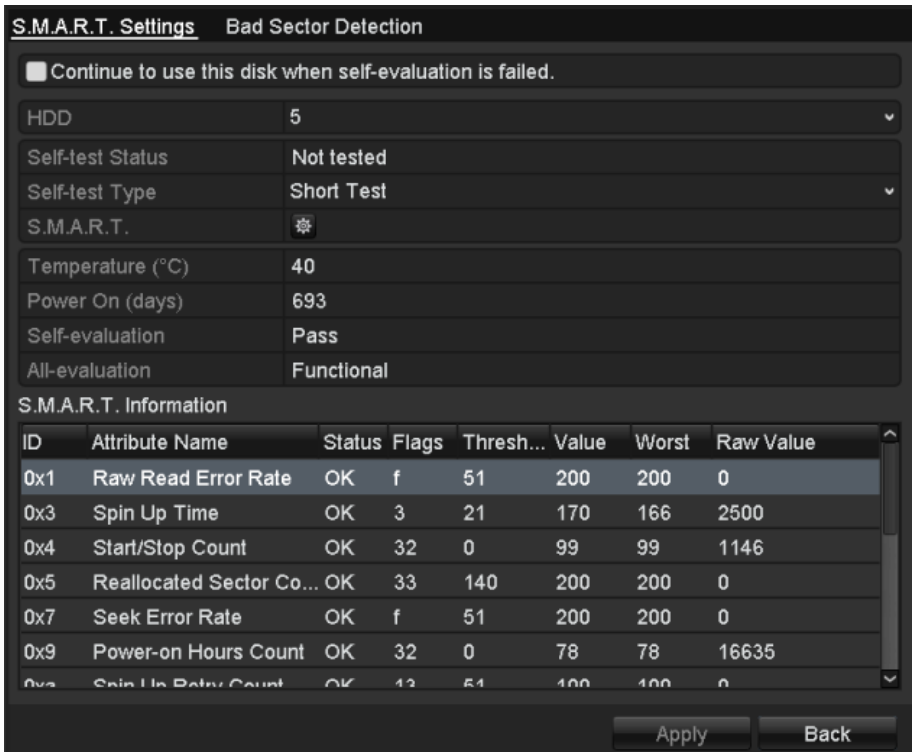


Figure 10. 15 S.M.A.R.T Settings Interface

NOTE

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

Bad Sector Detection

Steps:

1. Click the **Bad Sector Detection** tab.
2. Select the **HDD No.** in the drop-down list.

3. Select the detection type as **Full Detection** or **Key Area Detection**.
4. Click **Detect** to start the detection.

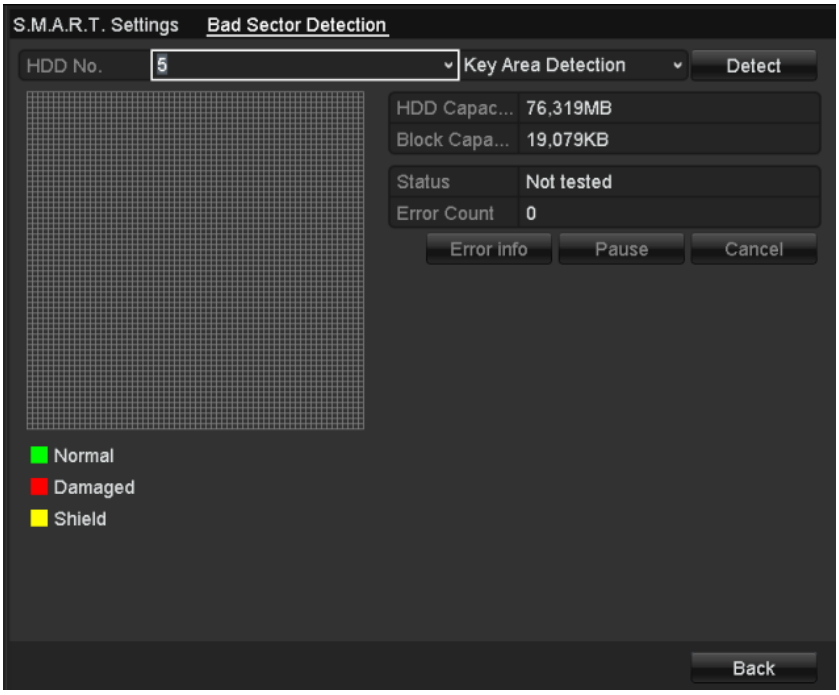


Figure 10. 16 Bad Sector Detection

5. Click **Pause** or **Cancel** to pause or cancel the detection.
6. Click **Error info** button to see the detailed damage information.

10.6 Configuring HDD Error Alarms

Purpose:

You can configure the HDD error alarms when the HDD status is uninitialized or abnormal.

Steps:

1. Enter the Exception interface.

   Menu > Configuration > Exceptions

2. Select the Exception Type as **HDD Error**.
3. Click the checkbox(s) linkage action to set the HDD error alarm type (s), as shown in Figure 10. 17.

NOTE

The alarm type can be selected as **Audible Warning**, **Notify Surveillance Center**, **Send Email** and **Trigger Alarm Output**. For details, please refer to section *8.6 Handling Exceptions Alarm*.

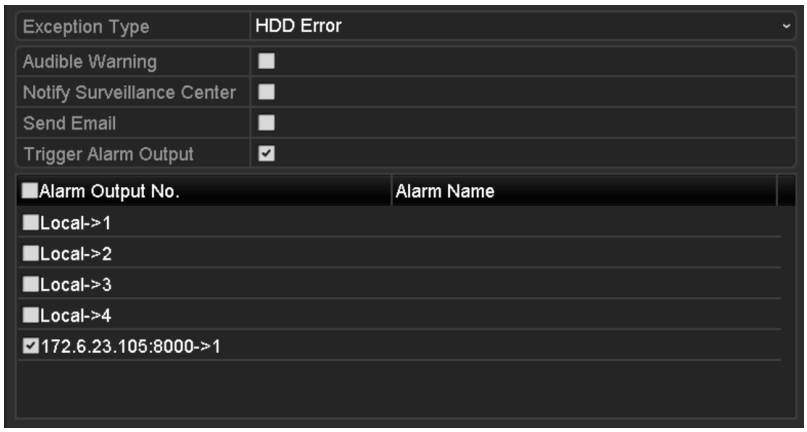


Figure 10. 17 Configure HDD Error Alarm

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

Chapter 11 Camera Settings

11.1 Configuring OSD Settings

Purpose:

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

Steps:

1. Enter the OSD Configuration interface.
   Menu > Camera > OSD
2. Select the **Camera** to configure.
3. Edit the **Camera Name** in the text field.
4. Enable the **Display Name**, **Display Date** and **Display Week** by checking the checkboxes.
5. Select the **Date Format**, **Time Format** and **Display Mode**.

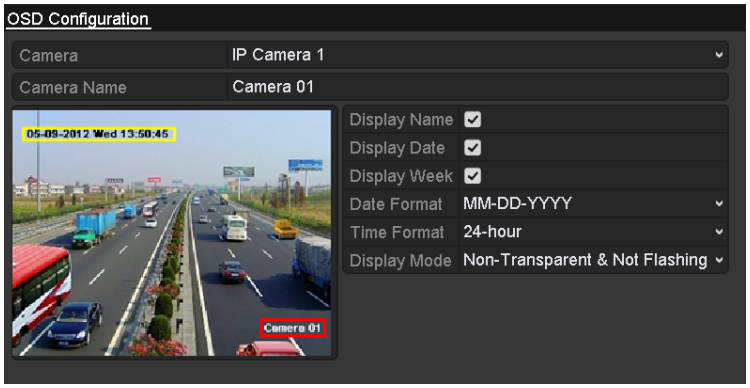


Figure 11. 1 OSD Configuration Interface

6. Adjust OSD position by using the mouse to drag the text frame on the preview window.
7. Click the **Apply** button to save the settings.

11.2 Configuring Privacy Mask

Purpose:

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

Steps:

1. Enter the Privacy Mask Settings interface.

   Menu > Camera > Privacy Mask

2. Select the **Camera** to set privacy mask.
3. Check the checkbox of **Enable Privacy Mask** to enable this feature.

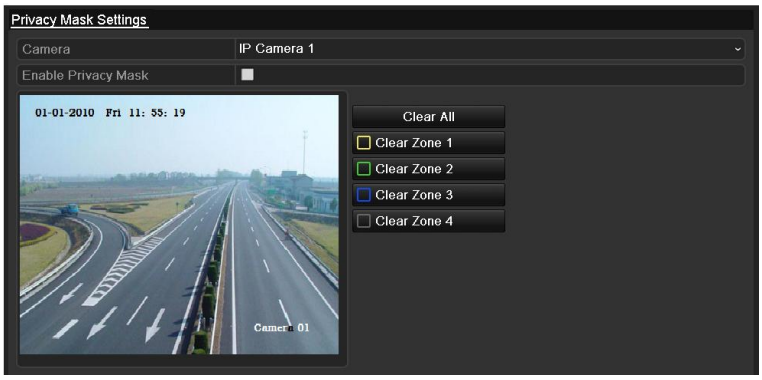


Figure 11. 2 Privacy Mask Settings Interface

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

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

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

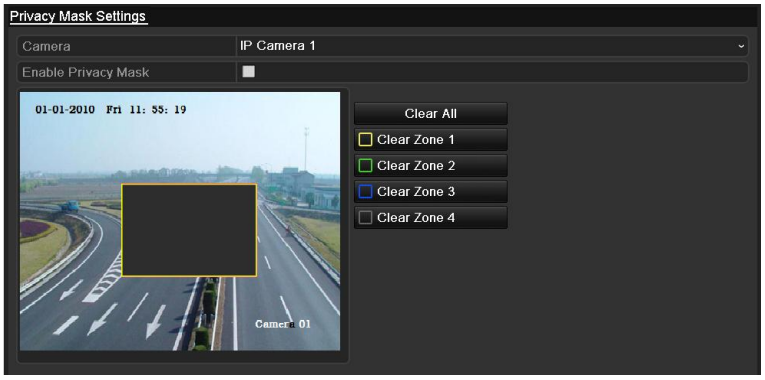


Figure 11. 3 Set Privacy Mask Area

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

11.3 Configuring Video Parameters

Steps:

1. Enter the Image Settings interface.

   Menu > Camera > Image

Figure 11. 4 Image Settings Interface

2. Select the **Camera** to set image parameters.
3. Click the icon or drag the scroll bar to change the value of each parameter.
4. Click the **Apply** button to save the settings.

Chapter 12 NVR Management and Maintenance

12.1 Viewing System Information

12.1.1 Viewing Device Information

Steps:

1. Enter the System Information interface.
   Menu > Maintenance > System Info
2. Click the **Device Info**, **Camera**, **Record**, **Alarm**, **WAN, WIFI, LAN** or **HDD** tabs to view the system information of the device.

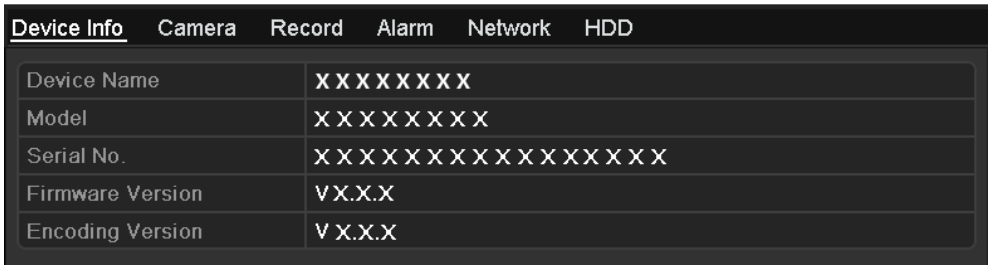


Figure 12. 1 Device Information Interface

12.2 Searching & Export Log Files

Purpose:

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

Steps:

1. Enter the Log Search interface.

   Menu > Maintenance > Log Information

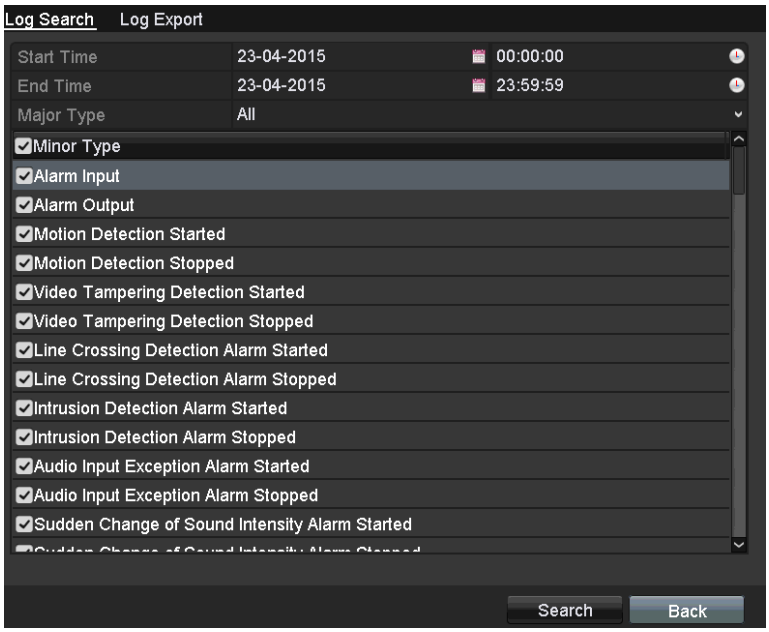


Figure 12. 2 Log Search Interface

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

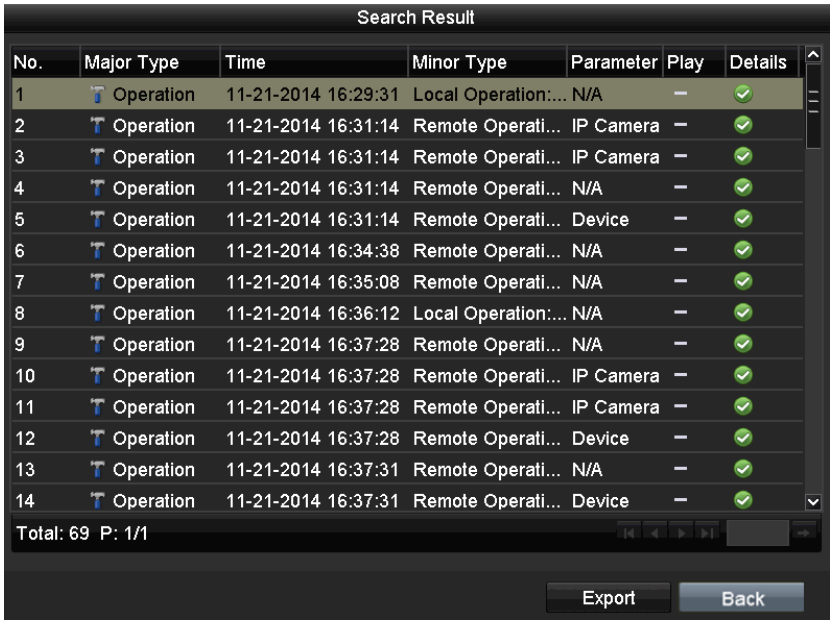


Figure 12. 3 Log Search Results

NOTE

Up to 2000 log files can be displayed each time.

5. Click the button or double click a log to view its detailed information, as shown in Figure 12. 4. And you can also click the button to view the related video files if available.

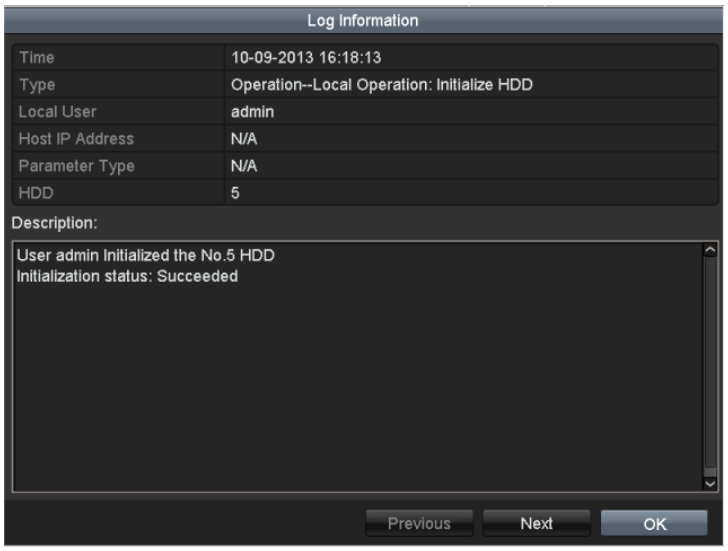


Figure 12. 4 Log Details

6. If you want to export the log files, click **Export** to enter the Export menu, as shown in Figure 12. 5.

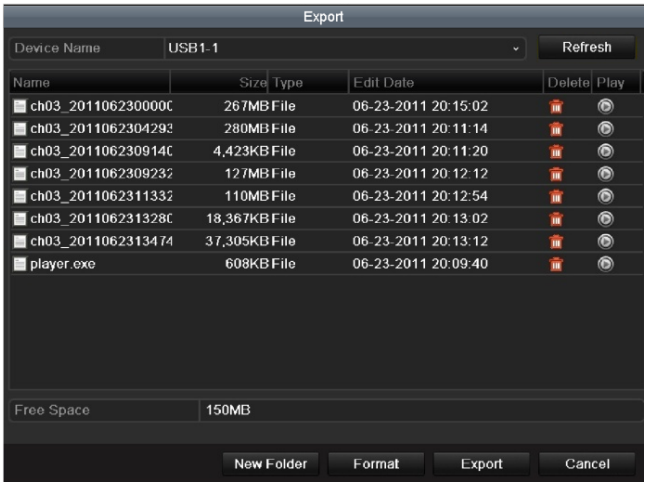


Figure 12. 5 Export Log Files

7. Select the backup device from the drop-down list of **Device Name**.
8. 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.
   - The log files exported to the backup device are named by exporting time, e.g., *20110514124841logBack.txt*.

To export all the log files:

Steps:

1. Enter the Log Information interface.

   Menu > Maintenance > Log Information
2. Click the **Log Export** tab.

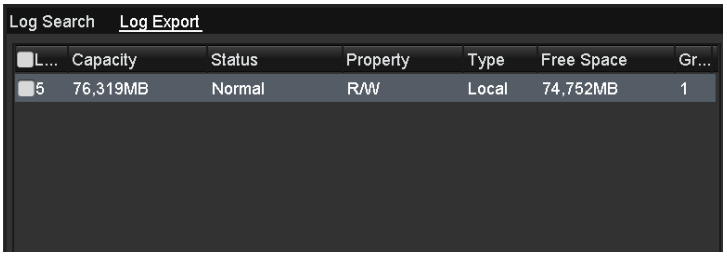


Figure 12. 6 Log Export Interface

3. Check the checkbox of the HDD.
4. Click the **Export** button to export all the log files stored in the HDD.

12.3 Importing/Exporting IP Camera Info

Purpose:

The information of added IP camera, including the IP address, manage port, password of admin, etc., can be generated into an excel file and the file can be exported to the backup device. And the exported file can be edited on your PC, like adding or deleting the content.

Steps:

1. Enter the camera management interface.

   Menu > Camera > IP Camera Import/Export

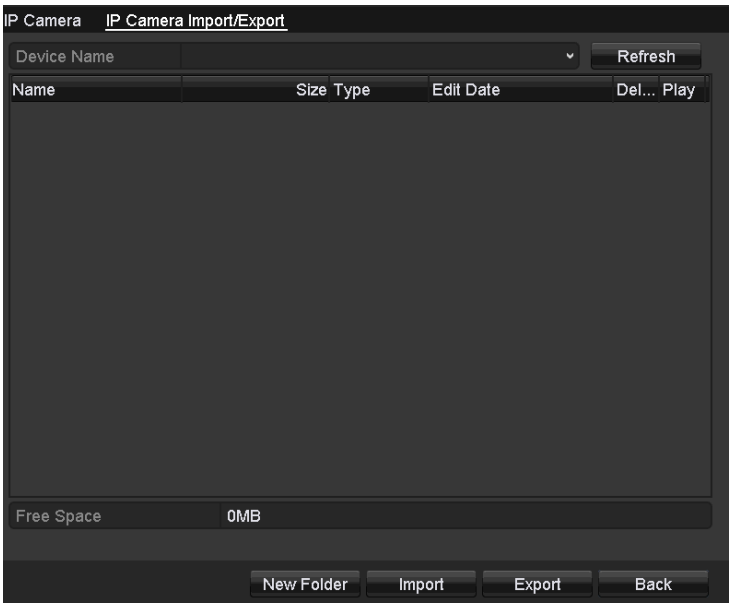


Figure 12. 7 IP Camera Import/Export Interface

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

12.4 Importing/Exporting Configuration Files

Purpose:

The configuration files of the NVR can be exported to local backup device; and the configuration files of one NVR can be imported to multiple NVR devices if they are to be configured with the same parameters.

Steps:

1. Enter the Import/Export Configuration File interface.

   Menu > Maintenance > Import/Export

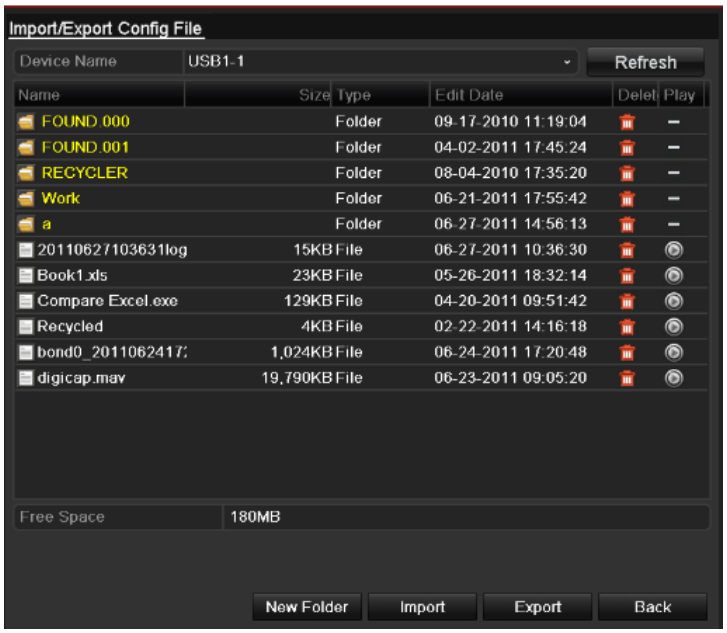


Figure 12. 8 Import/Export Config File

2. Click **Export** to export configuration files to the selected local backup device.
3. To import a configuration file, select the file from the selected backup device and click 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

Purpose:

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

12.5.2 Upgrading by Local Backup Device

Before you start:

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

Steps:

1. Enter the Upgrade interface.

   Menu > Maintenance > Upgrade

2. Click the **Local Upgrade** tab to enter the local upgrade menu, as shown in Figure 12. 9.

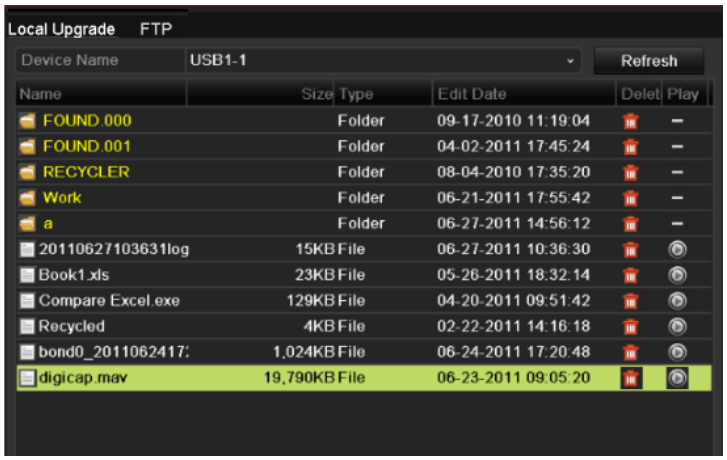


Figure 12. 9 Local Upgrade Interface

3. Click to select the update file in the backup device.
4. Click **Upgrade** to start upgrading.
5. After the upgrading is complete, reboot the NVR to activate the new firmware.

12.5.3 Upgrading by FTP

Purpose:

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

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, as shown in Figure 12. 10.

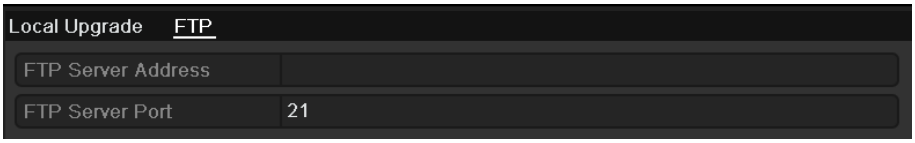


Figure 12. 10 FTP Upgrade Interface

3. Input the **FTP Server Address** in the text field.
4. Click **Upgrade** 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

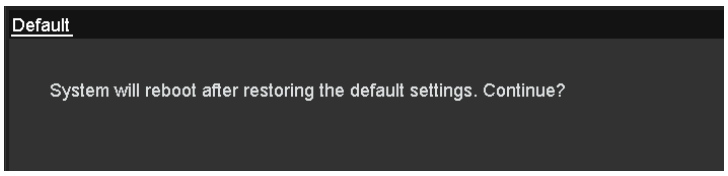


Figure 12. 11 Restore Factory Default

2. Click **OK** to restore the default settings.

NOTE

Except the network parameters (including IP address, subnet mask, gateway, MTU, NIC working mode, default route and server port), all other parameters of the device will be restored to factory default settings.

Chapter 13 Others

13.1 Configuring General Settings

Purpose:

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

Steps:

1. Enter the General Settings interface.

   Menu > Configuration > General

2. Select the **General** tab.

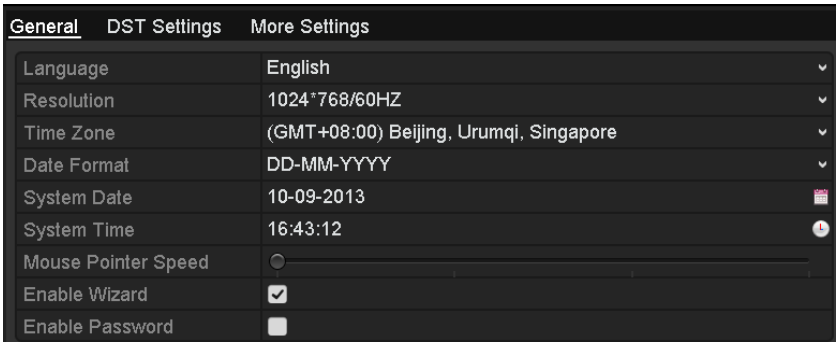


Figure 13. 1 General Settings Interface

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.

13.2 Configuring DST Settings

Steps:

1. Enter the General Settings interface.

   Menu > Configuration > General

2. Choose **DST Settings** tab.

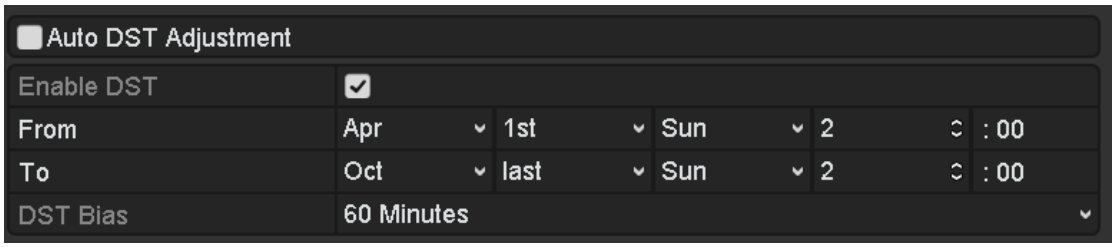


Figure 13. 2 DST Settings Interface

3. Check the checkbox of **Auto DST Adjustment** item.

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

13.3 Configuring More Settings for NVR

Steps:

1. Enter the General Settings interface.

   Menu > Configuration > General

2. Click the **More Settings** tab to enter the More Settings interface, as shown in Figure 13. 3.

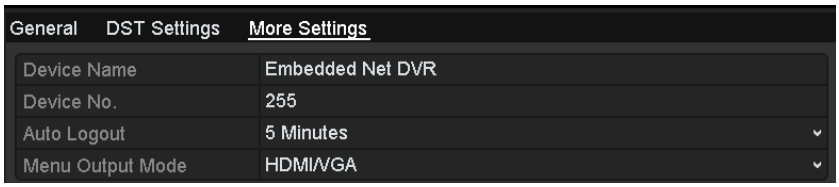


Figure 13. 3 More Settings Interface

3. Configure the following settings:
   - **Device Name:** Edit the name of NVR.
   - **Device No.:** The No. is used for the remote and keyboard control. The Device No. can be set in the range of 1~255, and the default No. is 255.
   - **Auto Logout:** Specify timeout for menu inactivity. E.g., when it is set to *5 Minutes*, then the system will exit from the current operation menu to live view after 5 minutes of menu inactivity.
   - **Menu Output Mode:** You can choose the output for menu display. By default, only HDMI is selectable.
4. Click the **Apply** button to save the settings.

13.4 Managing User Accounts

Purpose:

There is a default account in the NVR: *Administrator*. The *Administrator* user name is *admin* and the password is *12345*. The *Administrator* has the permission to add and delete users and configure user parameters.

13.4.1 Adding a User

Steps:

1. Enter the User Management interface.

   Menu > Configuration > User

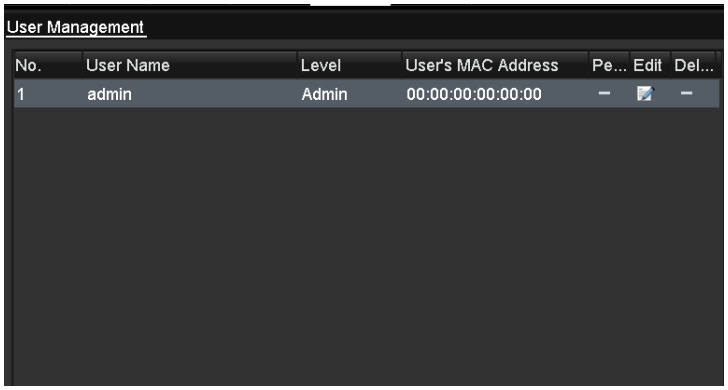


Figure 13. 4 User Management Interface

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

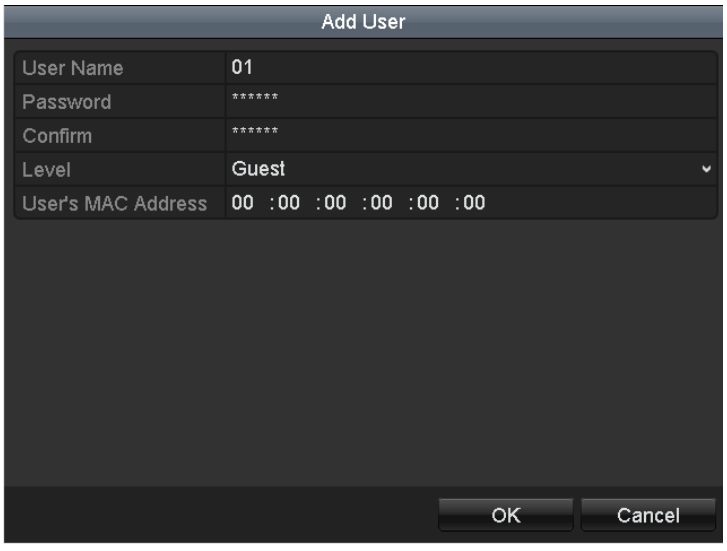


Figure 13. 5 Add User Menu

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

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

   - **Operator:** The *Operator* user level has the permission of all operating permission in Camera

Configuration by default.

- **Guest:** The Guest user has no permission of 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 13. 6.

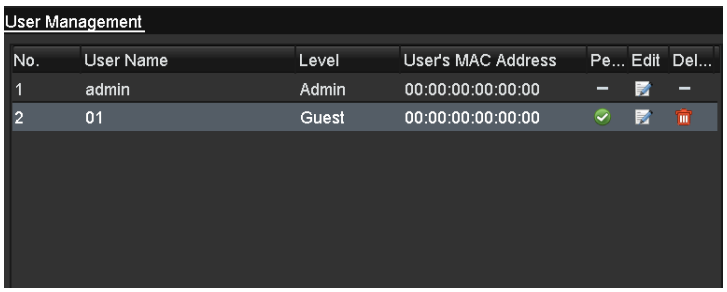


Figure 13. 6 Added User Listed in User Management Interface

5. Click to select the user from the list and then click the button to enter the Permission settings interface, as shown in Figure 13. 7.

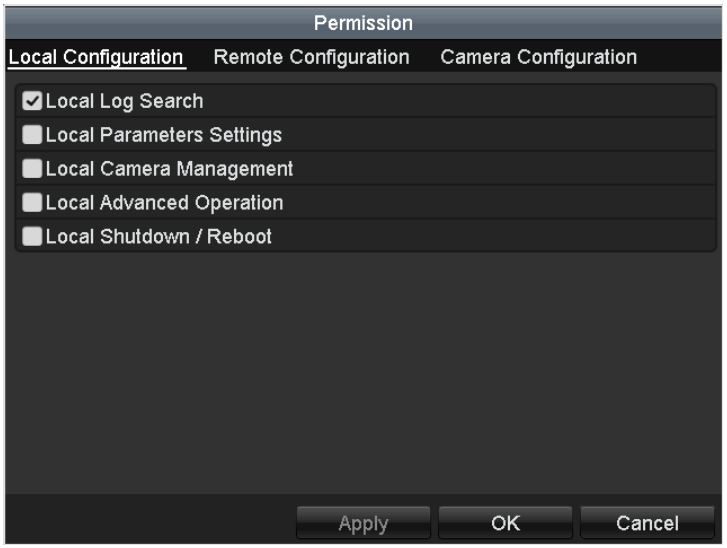


Figure 13. 7 User Permission Settings Interface

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

Local Configuration

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

Remote Configuration

- Remote Log Search: Remotely viewing logs that are saved on the NVR.

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

Camera Configuration

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

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

NOTE

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

13.4.2 Deleting a User

Steps:

1. Enter the User Management interface.

   Menu > Configuration > User

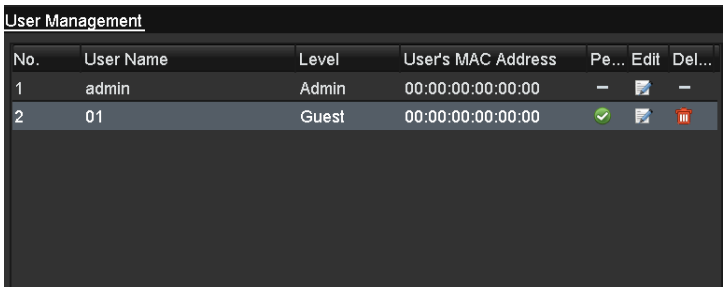


Figure 13. 8 User List

2. Click the icon after the user to delete.
3. Click **OK** to confirm the deletion.

13.4.3 Editing a User

Steps:

1. Enter the User Management interface.
   Menu > Configuration > User
2. Click the icon after the user to delete.

NOTE

The admin user can also be edited.

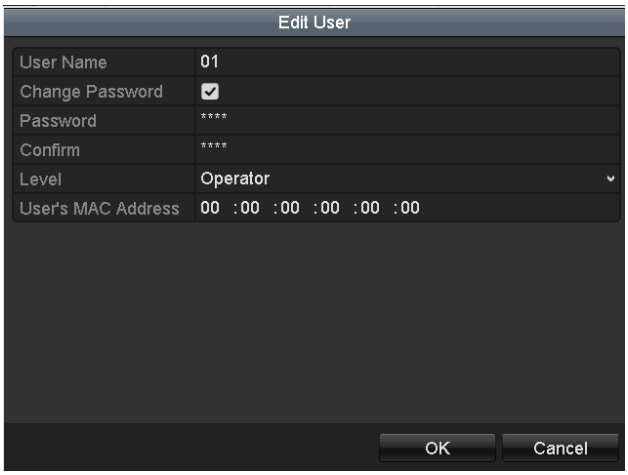


Figure 13. 9 Edit User - Operator and Guest

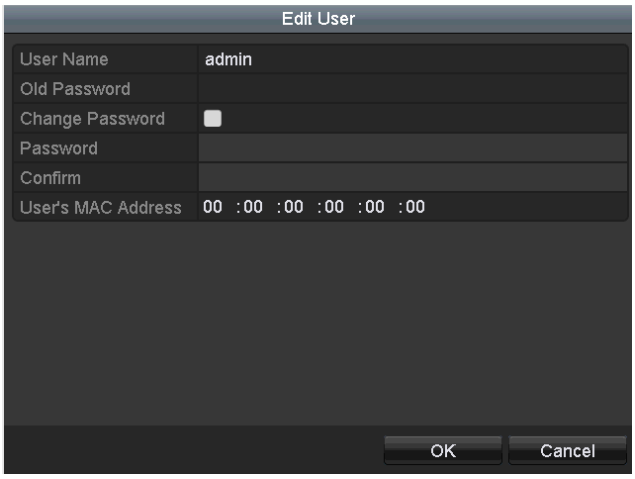


Figure 13. 10 Edit User - Admin

3. 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 one in the text field of **Password** and **Confirm**.
   - **Admin**
     You are only allowed to edit **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 one in the text

field of **Password** and **Confirm**.

For your privacy, we strongly recommend changing the password to something 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.

4. Click the **OK** button to save the settings and exit the menu.

Chapter 14 Appendix

Glossary

- **Dual Stream:** Dual stream is a technology used to record high resolution video locally while transmitting a lower resolution stream over the network. The two streams are generated by the DVR, with the main stream having a maximum resolution of 4CIF and the sub-stream having a maximum resolution of CIF.
- **HDD:** Acronym for Hard Disk Drive. A storage medium which stores digitally encoded data on platters with magnetic surfaces.
- **DHCP:** Dynamic Host Configuration Protocol (DHCP) is a network application protocol used by devices (DHCP clients) to obtain configuration information for operation in an Internet Protocol network.
- **HTTP:** Acronym for Hypertext Transfer Protocol. A protocol to transfer hypertext request and information between servers and browsers over a network
- **PPPoE:** PPPoE, Point-to-Point Protocol over Ethernet, is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with ADSL services where individual users connect to the ADSL transceiver (modem) over Ethernet and in plain Metro Ethernet networks.
- **DDNS:** Dynamic DNS is a method, protocol, or network service that provides the capability for a networked device, such as a router or computer system using the Internet Protocol Suite, to notify a domain name server to change, in real time (ad-hoc) the active DNS configuration of its configured hostnames, addresses or other information stored in DNS.
- **NTP:** Acronym for Network Time Protocol. A protocol designed to synchronize the clocks of computers over a network.
- **NVR:** Acronym for Network Video Recorder. An NVR can be a PC-based or embedded system used for centralized management and storage for IP cameras, IP Domes and other DVRs.
- **PTZ:** Acronym for Pan, Tilt, Zoom. PTZ cameras are motor driven systems that allow the camera to pan left and right, tilt up and down and zoom in and out.
- **USB:** Acronym for Universal Serial Bus. USB is a plug-and-play serial bus standard to interface devices to a host computer.

Troubleshooting

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

  Possible Reasons

  a) No HDMI™ connections.

  b) Connection cable is damaged.

  c)Input mode of the monitor is incorrect.

  Steps

  1. Verify the device is connected with the monitor via HDMI™ cable.

     If not, please connect the device with the monitor and reboot.

  2. Verify the connection cable is good.

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

  3. Verify Input mode of the monitor is correct.

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

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

     If it is solved, finish the process.

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

- **There is an audible warning sound "Di-Di-Di-DiDi" after a new bought NVR starts up.**

  Possible Reasons

  a) The installed HDD has not been initialized.

  b) The installed HDD is not compatible with the NVR or is broken-down.

  Steps

  1. Verify the HDD is initialized.
     1) Select "Menu > HDD > General".
     2) If the status of the HDD is "Uninitialized", please check the checkbox of corresponding HDD and click the "Init" button.
  2. Verify the HDD is detected or is in good condition.
     1) Select "Menu > HDD > General".
     2) If the HDD is not detected or the status is "Abnormal", please replace the dedicated HDD according to the requirement.
  3. Check if the fault is solved by the step 1 to step 2.

     If it is solved, finish the process.

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

- **The status of the added IP camera displays as "Disconnected" when it is connected through Private Protocol. Select "Menu > Camera > Camera" to get the camera status.**

  Possible Reasons

  a) Network failure, and the NVR and IP camera lost connections.

  b) The configured parameters are incorrect when adding the IP camera.

  c)Insufficient bandwidth.

  Steps

  1. Verify the network is connected.

1) Connect the NVR and PC with the RS-232 cable.
2) Open the Super Terminal software, and execute the ping command. Input “ping IP” (e.g. ping 172.6.22.131).

Simultaneously press **Ctrl** and **C** to exit the ping command.

If there exists return information and the time value is little, the network is normal.

2. Verify the configuration parameters are correct.
   1) Select “Menu > Camera > Camera”.
   2) Verify the following parameters are the same with those of the connected IP devices, including IP address, protocol, management port, user name and password.
3. Verify the whether the bandwidth is enough.
   1) Select “Menu > Maintenance > Net Detect > Network Stat.”.
   2) Check the usage of the access bandwidth, and see if the total bandwidth has reached its limit.
4. Check if the fault is solved by the step 1 to step 3.

   If it is solved, finish the process.

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

- **The IP camera frequently goes online and offline and the status of it displays as “Disconnected”.**

Possible Reasons

a) The IP camera and the NVR versions are not compatible.

b) Unstable power supply of IP camera.

c)Unstable network between IP camera and NVR.

d) Limited flow by the switch connected with IP camera and NVR.

Steps

1. Verify the IP camera and the NVR versions are compatible.
   1) Enter the IP camera Management interface “Menu > Camera > Camera>IP Camera”, and view the firmware version of connected IP camera.
   2) Enter the System Info interface “Menu>Maintenance>System Info>Device Info”, and view the firmware version of NVR.
2. Verify power supply of IP camera is stable.
   1) Verify the power indicator is normal.
   2) When the IP camera is offline, please try the ping command on PC to check if the PC connects with the IP camera.
3. Verify the network between IP camera and NVR is stable.
   1) When the IP camera is offline, connect PC and NVR with the RS-232 cable.
   2) Open the Super Terminal, use the ping command and keep sending large data packages to the connected IP camera, and check if there exists packet loss.

Simultaneously press **Ctrl** and **C** to exit the ping command.

Example: Input **ping 172.6.22.131 –l 1472 –f.**

4. Verify the switch is not flow control.

   Check the brand, model of the switch connecting IP camera and NVR, and contact with the manufacturer of the switch to check if it has the function of flow control. If so, please turn it down.
5. Check if the fault is solved by the step 1 to step 4.

   If it is solved, finish the process.

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

- **No monitor connected with the NVR locally and when you manage the IP camera to connect with the device by web browser remotely, of which the status displays as Connected. And then you connect the device with the monitor via HDMI™ interface and reboot the device, there is black screen with the mouse cursor.**

  Connect the NVR with the monitor before startup via HDMI™ interface, and manage the IP camera to connect with the device locally or remotely, the status of IP camera displays as Connect.

  Possible Reasons:

  After connecting the IP camera to the NVR, the image is output via the main spot interface by default.

  Steps:

  1. Enable the output channel.
  2. Select "Menu > Configuration > Live View > View", and select video output interface in the drop-down list and configure the window you want to view.

     - The view settings can only be configured by the local operation of NVR.
     - Different camera orders and window-division modes can be set for different output interfaces separately, and digits like "D1"and "D2" stands for the channel number, and "X" means the selected window has no image output.
  3. Check if the fault is solved by the above steps.

     If it is solved, finish the process.

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

- **Live view stuck when video output locally.**

  Possible Reasons:

  a) Poor network between NVR and IP camera, and there exists packet loss during the transmission.

  b) The frame rate has not reached the real-time frame rate.

  Steps:

  1. Verify the network between NVR and IP camera is connected.
     1) When image is stuck, connect the RS-232 ports on PC and the rear panel of NVR with the RS-232 cable.
     2) Open the Super Terminal, and execute the command of "**ping** *192.168.0.0* **–l 1472 –f**" (the IP address may change according to the real condition), and check if there exists packet loss.

        Simultaneously press **Ctrl** and **C** to exit the ping command.
  2. Verify the frame rate is real-time frame rate.

     Select "Menu > Record > Parameters > Record", and set the Frame rate to Full Frame.
  3. Check if the fault is solved by the above steps.

     If it is solved, finish the process.

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

- **Live view stuck when video output remotely via the Internet Explorer or platform software.**

  Possible Reasons:

  a) Poor network between NVR and IP camera, and there exists packet loss during the transmission.

  b) Poor network between NVR and PC, and there exists packet loss during the transmission.

  c) The performances of hardware are not good enough, including CPU, memory, etc..

  Steps:

  1. Verify the network between NVR and IP camera is connected.

1) When image is stuck, connect the RS-232 ports on PC and the rear panel of NVR with the RS-232 cable.

2) Open the Super Terminal, and execute the command of "**ping** *192.168.0.0* **–l 1472 –f**" (the IP address may change according to the real condition), and check if there exists packet loss.

NOTE

Simultaneously press **Ctrl** and **C** to exit the ping command.

2. Verify the network between NVR and PC is connected.

1) Open the cmd window in the Start menu, or you can press "windows+R" shortcut key to open it.

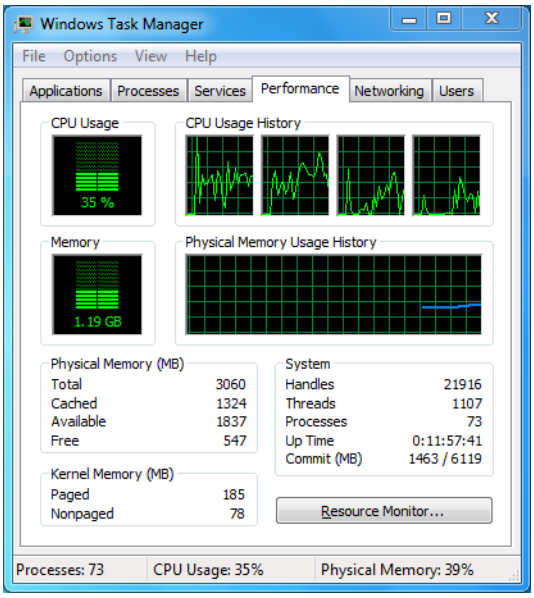
2) Use the ping command to send large packet to the NVR, execute the command of "ping 192.168.0.0 –l 1472 –f" (the IP address may change according to the real condition), and check if there exists packet loss.

NOTE

Simultaneously press **Ctrl** and **C** to exit the ping command.

3. Verify the hardware of the PC is good enough.

Simultaneously press **Ctrl**, **Alt** and **Delete** to enter the windows task management interface, as shown in the following figure.



Windows task management interface

- Select the "Performance" tab; check the status of the CPU and Memory.
- If the resource is not enough, please end some unnecessary processes.

4. Check if the fault is solved by the above steps.

If it is solved, finish the process.

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

- **When using the NVR to get the live view audio, there is no sound or there is too much noise, or the volume is too low.**

Possible Reasons:

a) Cable between the pickup and IP camera is not connected well; impedance mismatches or incompatible.

b) The stream type is not set as "Video & Audio".

c)The encoding standard is not supported with NVR.

Steps:

1. Verify the cable between the pickup and IP camera is connected well; impedance matches and compatible.

   Log in the IP camera directly, and turn the audio on, check if the sound is normal. If not, please contact the manufacturer of the IP camera.

2. Verify the setting parameters are correct.

   Select "Menu > Record > Parameters > Record", and set the Stream Type as "Audio & Video".

3. Verify the audio encoding standard of the IP camera is supported by the NVR.

   NVR supports G722.1 and G711 standards, and if the encoding parameter of the input audio is not one of the previous two standards, you can log in the IP camera to configure it to the supported standard.

4. Check if the fault is solved by the above steps.

   If it is solved, finish the process.

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

- **The image gets stuck when NVR is playing back by single or multi-channel.**

  Possible Reasons:

  a) Poor network between NVR and IP camera, and there exists packet loss during the transmission.

  b) The frame rate is not the real-time frame rate.

  c)The NVR supports up to 16-channel synchronize playback at the resolution of 4CIF, if you want a 16-channel synchronize playback at the resolution of 720p, the frame extracting may occur, which leads to a slight stuck.

  Steps:

  1. Verify the network between NVR and IP camera is connected.
     1) When image is stuck, connect the RS-232 ports on PC and the rear panel of NVR with the RS-232 cable.
     2) Open the Super Terminal, and execute the command of "**ping** *192.168.0.0* **–l 1472 –f**" (the IP address may change according to the real condition), and check if there exists packet loss.

     Simultaneously press the **Ctrl** and **C** to exit the ping command.
  2. Verify the frame rate is real-time frame rate.

     Select "Menu > Record > Parameters > Record", and set the Frame Rate to "Full Frame".
  3. Verify the hardware can afford the playback.

     Reduce the channel number of playback.

     Select "Menu > Record > Encoding > Record", and set the resolution and bitrate to a lower level.
  4. Reduce the number of local playback channel.

     Select "Menu > Playback", and uncheck the checkbox of unnecessary channels.
  5. Check if the fault is solved by the above steps.

     If it is solved, finish the process.

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

- **No record file found in the NVR local HDD, and prompt "No record file found".**

  Possible Reasons:

  a) The time setting of system is incorrect.

  b) The search condition is incorrect.

  c)The HDD is error or not detected.

Steps:

1. Verify the system time setting is correct.

   Select “Menu > Configuration > General > General”, and verify the “Device Time” is correct.

2. Verify the search condition is correct.

   Select “Playback”, and verify the channel and time are correct.

3. Verify the HDD status is normal.

   Select “Menu > HDD > General” to view the HDD status, and verify the HDD is detected and can be read and written normally.

4. Check if the fault is solved by the above steps.

   If it is solved, finish the process.

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

Summary of Changes

Version 3.0.12

Updated

1. Update the figures of wireless network interface. (Chapter 9.2.1 Configuring Wireless Network)
2. Update the figures of wizard interface. (Chapter 2.2 Using the Wizard for Basic Configuration)
3. Optimize the steps of adding IP cameras (Chapter 2.3 Adding and Connecting the IP cameras)
4. Add the description of Cloud P2P function. (Chapter 9.2.2 Configuring Extranet Access)

Version 3.0.7

Updated

1. Optimize the PTZ control panels and operations. (Chapter 9.2.1 Configuring Wireless Network)

Version 3.0.6

Updated

1. Optimize the PTZ control panels and operations. (Chapter 4)
2. Change the Cloud to Cloud P2P. (Chapter 9.2.2)
3. Add the models of DS-7100NI series, DS-7600NI-SE series and DS-7600NI-V(P) series NVR.

Version 3.0.4

Added

1. Connectable to smart IP cameras, and VCA alarm detection and recording are supported. (Chapter 5.2, Chapter 5.5 and Chapter 8.5)
2. Support video searching, playing back and backing up by VCA events. (Chapter 6.1.3 and Chapter 7.1.3)
3. Support smart playback by VCA rules. (Chapter 6.1.5)
4. Support P2P protocol and access by Cloud P2P. (Chapter 9.2.2)

Deleted

- Combine the smart search function with the smart playback function, and the smart search section is deleted. (Chapter 6.2.2 Smart Search)

List of Compatible IP Cameras

- For the list, our company holds right to interpret.
- **ONVIF compatibility** refers to the camera can be supported both when it uses the ONVIF protocol and its private protocols. **Only ONVIF is supported** refers to the camera can only be supported when it uses the ONVIF protocol. **Only AXIS is supported** refers to the function can only be supported when it uses the AXIS protocol.

IP Camera Manufacturer or Protocol	Model	Version	Max. Resolution	Sub-stream	Audio
ACTI	TCM4301-10D-X-00083	A1D-310-V4.12.09-AC	1280×1024	×	√
	TCM5311-11D-X-00023	A1D-310-V4.12.09-AC	1280×960	×	√
	TCM3401-09L-X-00227	A1D-220-V3.13.16-AC	1280×1024	×	×
ARECONT	AV1305M	65175	1600×1200	√	×
	AV2155	65143	1280×1024	√	×
	AV2815	65220	1600×1200	√	×
	AV3105M	65175	1920×1080	√	×
	AV5105	65175	1920×1080	√	×
	AV8185DN	65172	1920×1080	×	×
AXIS	M1114	5.09.1	1024×640	√	×
	M3011(ONVIF compatibility)	5.21	704×576	√ (Only AXIS is supported)	×
	M3014(ONVIF compatibility)	5.21.1	1280×800	√	×
	P3301(ONVIF compatibility)	5.11.2	768×576	√	√ (Only AXIS is supported)
	P3304(ONVIF compatibility)	5.20	1440×900	√	√ (Only AXIS is supported)
	P3343(ONVIF compatibility)	5.20.1	800×600	√	√ (Only AXIS is supported)
	P3344(ONVIF compatibility)	5.20.1	1440×900	√	√ (Only AXIS is supported)
	P5532	5.15	720×576	√	×
	P1346E	5.06.1	1920×1080	√	×
	Q7404	5.02	720×576	√	√

IP Camera Manufacturer or Protocol	Model	Version	Max. Resolution	Sub-stream	Audio
Bosch (ONVIF compatibility)	AutoDome Jr 800HD	39500450	1920×1080	×	√
	Dinion NBN-921-P	10500453	1280×720	×	√
	NBC 265 P	07500452	1280×720	×	√
Brickcom	CB-500Ap (ONVIF compatibility)	V3.2.1.3	1920×1080	×	√
	FB-130Np (ONVIF compatibility)	V3.1.0.8	1280×1024	×	√
	WFB-100Ap	V3.1.0.9	1280×800	×	√
Canon	VB-H410 (ONVIF compatibility)	Ver.+1.0.0	1280×960	×	√
	VB-H6100D	Ver. 1.0.0	1920×1080	×	×
	VB-H7100F	Ver. 1.0.0	1920×1080	×	×
	VB-M400 (ONVIF compatibility)	Ver.+1.0.0	1280×960	×	√
	VB-M6000D (ONVIF compatibility)	Ver.+1.0.0	1280×960	×	×
	VB-M7000F (ONVIF compatibility)	Ver.+1.0.0	1280×960	×	√
	VB-S300D	Ver. 1.0.0	1920×1080	×	×
	VB-S8000	Ver. 1.0.0	1920×1080	×	×
	VB-S9000F	Ver. 1.0.0	1920×1080	×	×
HUNT	HLC_79AD	V1.0.40	1600×1200	×	√
Hikvision	DS-2CD2010F-I(W)	5.2.3 build 141024	1280×960	√	√
	DS-2CD2012F-I(W)	5.2.1 build 140820	1280×960	√	√
	DS-2CD2020F-I(W)	5.2.3 build 141024	1920×1080	√	√
	DS-2CD2032F-I(W)	5.2.1 build 140820	2048×1536	√	√
	DS-2CD2110F(D)-I(W)(S)	5.2.3 build 141024	1280×960	√	√
	DS-2CD2112F(D)-I(W)(S)	5.2.1 build 140820	1280×960	√	√
	DS-2CD2120F(D)-I(W)(S)	5.2.3 build 141024	1920×1080	√	√
	DS-2CD2132F(D)-I(W)(S)	5.2.1 build 140820	2048×1536	√	√
	DS-2CD2E10F-W	5.2.3 build 141024	1280×960	√	√
	DS-2CD2E20F-W	5.2.3 build 141024	1920×1080	√	√
	DS-2CD2410FD-I(W)	5.2.3 build 141024	1280×720	√	√
	DS-2CD2412FD-I(W)	5.2.1 build 140820	1280×960	√	√
	DS-2CD2420FD-I(W)	5.2.3 build 141024	1920×1080	√	√
	DS-2CD2432FD-I(W)	5.2.1 build 140820	2048×1536	√	√
	DS-2CD2512F-I(W)(S)	5.2.1 build 140820	1280×960	√	√
	DS-2CD2532F-I(W)(S)	5.2.1 build 140820	2048×1536	√	√
	DS-2CD2C10F-IW	5.2.3 build 141024	1280×720	√	×
	DS-2CD2942F-(I)(W)(S)	5.2.1 build 140925	2560×1440	√	√
	DS-2CD2Q10FD-IW	5.2.3 build 141024	1280×720	√	√
Panasonic (ONVIF compatibility)	WV-NP502	1.41	1920×1080	×	√
	WV－SC385	Application: 1.0 Image data: 1.09	1280×960	×	×
	WV－SC386	Application: 1.66	1280×960	√	√

IP Camera Manufacturer or Protocol	Model	Version	Max. Resolution	Sub-stream	Audio
		Image data: 1.05			
	WV-SF132	Application: 1.66 Image data: 1.03	640×360	√	×
	WV-SF336H	Application: 1.06 Image data: 1.06	1280×960	√	√
	WV-SF332	Application: 1.66 Image data: 1.06	800×600	√	√
	WV-SF342	Application: 1.66 Image data: 1.06	800×600	√	√
	WV-SF346	Application: 1.66 Image data: 1.06	1280×960	√	√
	WV-SP102	Application: 1.66 Image data: 1.03	640×480	√	×
	WV-SP105	Application: 1.66 Image data: 1.03	1280×960	√	×
	WV-SP302	Application: 1.66 Image data: 1.06	800×600	√	√
	WV-SP306H	Application: 1.34 Image data: 1.06	1280×960	√	√
	WV-SP509	Application: 30 Image data: 2.21	1280×960	√	√
	WV-SW152	Application: 1.66 Image data: 1.05	800×600	√	×
	WV-SW155	Application: 1.66 Image data: 1.05	1280×960	√	×
	WV-SW316	Application: 1.66 Image data: 2.0.3	1280×960	√	√
	WV-SW352	Application: 1.66 Image data: 1.04	800×600	√	√
PELCO	D5118	1.8.2-20120327- 2.9310-A1.7852	1280×960	√	×
	IXE20DN-AAXVUU2	1.8.2-20120327- 2.9081-A1.7852	1920×1080	√	×
	IXE10DN-ACDJV44	1.8.2-20120327- 2.9081-A1.7852	1280×1024	√	×
	IX30DN-ACFZHB3	1.8.2-20120327- 2.9080-A1.7852	2048×1536	√	×
SAMSUNG (ONVIF compatibility)	5000P	3.10_130416	1280×1024	√	√
	SNB-3000P	V1.41_110709	704×576	×	√
	SNB-5000P	V2.00_110727	1280×1024	√	√
	SNB-7000P	V1.10_110819	2048×1536	×	√
	SND-5080	3.10_130416	1280×1024	√	√
	SNP-5200H	V1.04_110825	1280×1024	√	√
	SNZ-5200	V1.04_110825	1280×1024	√	√
SANYO	VCC-HD2300P	2.03-02 (110318-00)	1920×1080	×	×

IP Camera Manufacturer or Protocol	Model	Version	Max. Resolution	Sub-stream	Audio
	VCC-HD2500P	2.02-02 (110208-00)	1920×1080	×	√
	VCC-HD4600P	2.03-02 (110315-00)	1920×1080	×	√
	VCC-HD5400	2.03-06 (110315-00)	1920×1080	×	√
SONY	SNC-CH220	1.50.00	1920×1080	×	×
	SNCDH220T (ONVIF compatibility)	1.50.00	2048×1536	×	×
	SNC-DH260	1.23.00	1920×1080	×	×
	SNC-EP580	1.53.00	1920×1080	√	√
	SNC-ER580	1.42.00	1280×720	×	√
	SNC-RH124	1.73.00	1280×720	√	√
Vivotek	IP7121	0202a	720×576	×	√
	IP7133	0203a	640×480	×	×
	FD8134 (ONVIF compatibility)	0107a	1280×800	×	×
	IP8161 (ONVIF compatibility)	0104a	1600×1200	×	√（Vivotek Protocol）
	IP8331 (ONVIF compatibility)	0102a	640×480	×	×
	IP8332 (ONVIF compatibility)	0105b	1280×800	×	×
	VS8102	0200S	704×576	×	√
ZAVIO	D5110	MG.1.6.03P8	1280×1024	√	×
	F3106	M2.1.6.03P8	1280×1024	√	√
	F3110	M2.1.6.01	1280×720	√	√
	F3206	MG.1.6.02c045	1920×1080	√	√
	F531E	LM.1.6.18P10	640×480	√	√