ERI-Q104-P4 • ERI-Q108-P8
Network Video Recorder
User Manual

Manual Illustrations and Features

Graphics (screen shots, product pictures, etc.) in this document are for illustrative purposes only. Your actual product may differ in appearance. Your product might not support all features discussed in this document.

Hikvision USA Inc., 18639 Railroad St., City of Industry, CA 91748, USA • Hikvision Canada, 4848 rue Levy, Saint Laurent, Quebec, Canada, H4R 2P1

Telephone: +1-909-895-0400 • Toll Free in USA: +1-866-200-6690 • E-Mail: sales.usa@hikvision.com • www.hikvision.com

© 2018 Hikvision USA Inc. • All Rights Reserved • Any and all information, including, among others, wordings, pictures, and graphs are the properties of Hangzhou Hikvision Digital Technology Co., Ltd., or its subsidiaries (hereinafter referred to as “Hikvision”).

ALL RIGHTS RESERVED.

This user manual (hereinafter referred to be “the Manual”) cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision. Unless otherwise stipulated, Hikvision does not make any warranties, guarantees or representations, express or implied, regarding to the Manual.

About this Manual

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

Please use this user manual under the guidance of professionals.

Trademarks Acknowledgement

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

Legal Disclaimer

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

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

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

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

Regulatory Information

FCC Information

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

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

FCC Conditions

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

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

EU Conformity Statement

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

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

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

Industry Canada ICES-003 Compliance

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

Mandatory Electrical Requirements

Hikvision requires the following conditions and equipment for all of its electronic equipment:

- **Grounding**
  Ensure good conductivity for all ground paths; examine ground path contact surfaces for defects, dirt, corrosion, or non-conductive coatings that may impede conductivity. Repair or clean contact surfaces as necessary to assure good metal-to-metal contact. Ensure fasteners are properly installed and tightened.

- **Electrical Wiring**
  Ensure your outlets are properly wired. They can be checked with an electrical outlet tester.

- **Surge Suppressor (Required)**
  Hikvision is not responsible for any damage to equipment caused by power spikes in the electrical power grid. Use of a surge suppressor meeting the following specifications is mandatory for all Hikvision electronic equipment:

- **Specifications**
  - Listed by Underwriter's Laboratories, meeting the UL 1449 Voltage Protection Rating (VPR)
  - Minimum protection of 1,000 joules or higher
  - Clamping voltage of 400 V or less
  - Response time of 1 nanosecond or less
- **Usage**
  - Surge suppressors must not be daisy chained with power strips or other surge suppressors
- **Maintenance**
  - Replace after a serious electrical event (e.g., lighting blew out a transformer down the street)
  - Replace yearly in storm-prone areas
  - Replace every two years as routine maintenance

Mandatory Electrical Requirements

Hikvision requires the following conditions and equipment for all of its electronic equipment:

- **Grounding**

  Ensure good conductivity for all ground paths; examine ground path contact surfaces for defects, dirt, corrosion, or non-conductive coatings that may impede conductivity. Repair or clean contact surfaces as necessary to assure good metal-to-metal contact. Ensure fasteners are properly installed and tightened.

- **Electrical Wiring**

  Ensure your outlets are properly wired. They can be checked with an electrical outlet tester.

- **Surge Suppressor (Required)**

  Hikvision is not responsible for any damage to equipment caused by power spikes in the electrical power grid. Use of a surge suppressor meeting the following specifications is mandatory for all Hikvision electronic equipment:

- **Specifications**
  - Listed by Underwriter's Laboratories, meeting the UL 1449 Voltage Protection Rating (VPR)
  - Minimum protection of 1,000 joules or higher
  - Clamping voltage of 400 V or less

  - Response time of 1 nanosecond or less
- **Usage**
  - Surge suppressors must not be daisy chained with power strips or other surge suppressors
- **Maintenance**
  - Replace after a serious electrical event (e.g., lighting blew out a transformer down the street)
  - Replace yearly in storm-prone areas
  - Replace every two years as routine maintenance

Safety Instructions

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

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

Input voltage should meet both the SELV (Safety Extra Low Voltage) and the Limited Power Source with 100 to 240 VAC, 48 VDC or 12 VDC according to the IEC60950-1 standard. Please refer to technical specifications for detailed information.

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

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

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

Preventive and Cautionary Tips

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

Ensure unit is installed in a well-ventilated, dust-free environment.

Unit is designed for indoor use only.

Keep all liquids away from the device.

Ensure environmental conditions meet factory specifications.

Ensure unit is properly secured to a rack or shelf. Major shocks or jolts to the unit as a result of dropping it may cause damage to the sensitive electronics within the unit.

Use the device in conjunction with an UPS if possible.

Power down the unit before connecting and disconnecting accessories and peripherals.

A factory recommended HDD should be used for this device.

Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the manufacturer.

Applicable Models

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

Series	Model
ERI-Q10x	ERI-Q104-P4
	ERI-Q108-P8

Symbol Conventions

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

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

Product Key Features

General

- Connectable to network cameras, network dome and encoders
- Connectable to the third-party network cameras via HIK, ONVIF, private RTSP protocols
- Connectable to the smart IP cameras
- PAL/NTSC adaptive video inputs
- Supports H.264+/H.264 video streams
- Each channel supports dual-stream
- Up to eight 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

- HDMI™/VGA outputs 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 cycle live view are also provided, and the interval of automatic cycle can be adjusted
- Configurable main stream and sub-stream for the live view
- 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

- 1 SATA hard disk can be connected, with a maximum of 6TB storage capacity
- Supports 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
- Eight 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).
- Playback by sub-periods
- Tag adding for record files, searching and playing back by tags
- Locking and unlocking record files
- Provides new 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
- Supports thumbnails view and fast view during playback
- Supports playback by transcoded stream
- Up to 4/8-ch synchronous playback

Backup

- Export video data by USB or SATA 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, abnormal record, and PoE power overload (for the models supports PoE interfaces only), etc.
- Alarm triggers full screen monitoring, notifying surveillance center, sending email
- Automatic restore when system is abnormal
- Supports line crossing detection and intrusion detection
- VCA alarm message push via iVMS-4500 mobile client software

Other Local Functions

- 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
- Admin password resetting by exporting/importing the GUID file
- Operation, alarm, exceptions and log recording and searching
- Manually triggering and clearing alarms
- Import and export of device configuration information

Network Functions

- 10 /100/1000 Mbps self-adaptive Ethernet interface
- Four independent PoE network interfaces are provided for /4P series
- Eight independent PoE network interfaces are provided for /8P series
- IPv6 is supported
- TCP/IP protocol, DHCP, DNS, DDNS, NTP, SADP, and SMTP are supported
- TCP, UDP, and RTP for unicast
- Auto/Manual port mapping by UPnP™
- Supports access by Hik-Connect
- Remote reverse playback via RTSP
- Supports 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 viewing of the device status, system logs and alarm status
- Remote keyboard operation
- Remote locking and unlocking of control panel and mouse
- Remote HDD formatting and program upgrading
- Remote system restart and shutdown
- Alarm and exception information can be sent to the remote host
- Remotely start/stop recording
- Remotely start/stop alarm output
- Remote PTZ control (depending on models)
- Remote JPEG capture
- Embedded Web server
- Upgrade by FTP 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 11
1.2 USB Mouse Operation 11
1.3 Rear Panel 12
Chapter 2 Getting Started 13
2.1 Device Startup and Activation 13
2.1.1 Starting Up and Shutting Down the NVR 13
2.1.2 Activating Your Device 14
2.1.3 Using the Unlock Pattern for Login 16
2.1.4 Login and Logout 18
2.1.5 Resetting Your Password 20
2.2 Using the Setup Wizard for Basic Configuration 21
2.3 Adding and Connecting IP Cameras 23
2.3.1 Activating IP Cameras 23
2.3.2 Adding Online IP Cameras 24
2.3.3 Editing the Connected IP Cameras and Configuring Customized Protocols 27
2.3.4 Editing IP Cameras Connected to the PoE Interfaces 30
Chapter 3 Live View 33
3.1 Live View Status Icons 33
3.2 Operations in Live View Mode 33
3.2.1 Right-Click Menu 33
3.2.2 Quick Setting Toolbar in Live View Mode 34
3.3 Adjusting Live View Settings 36
Chapter 4 PTZ Controls 39
4.1 Configuring PTZ Settings 39
4.2 Setting PTZ Presets, Patrols, and Patterns 40
4.2.1 Customizing Presets 40
4.2.2 Calling Presets 41
4.2.3 Customizing Patrols 41
4.2.4 Calling Patrols 42
4.2.5 Customizing Patterns 43
4.2.6 Calling Patterns 44
4.2.7 Customizing Linear Scan Limit 44
4.2.8 Calling Linear Scan 45
4.2.9 One-Touch Park 45
4.2.10 PTZ Control Panel 46
Chapter 5 Recording Settings 48
5.1 Configuring Parameters 48
5.2 Configuring Recording Schedule 51
5.3 Configuring Motion Detection Recording 53
5.4 Configuring Alarm Triggered Recordings 55

5.5 Configuring VCA Event Recording 57
5.6 Manual Recording 58
5.7 Configuring Holiday Recording 59
5.8 Files Protection 60
5.8.1 Locking the Recording Files 60
5.8.2 Setting HDD Property to Read-only 62
Chapter 6 Playback 64
6.1 Playing Back Record Files 64
6.1.1 Instant Playback 64
6.1.2 Playing Back by Normal Search 64
6.1.3 Playing Back by Smart Search 67
6.1.4 Playing Back by Event Search 69
6.1.5 Playing Back by Tag 71
6.1.6 Playing Back by System Logs 73
6.1.7 Playing Back External Files 75
6.1.8 Playing Back by Sub-Periods 75
6.2 Auxiliary Playback Functions 76
6.2.1 Playing Back Frame-by-Frame 76
6.2.2 Fast View 77
6.2.3 Digital Zoom 77
6.2.4 File Management 78
Chapter 7 Backup 79
7.1 Backing up Record Files 79
7.1.1 Backing up by Normal Video Search 79
7.1.2 Backing up by Event Search 81
7.1.3 Backing Up Video Clips 82
7.2 Managing Backup Devices 83
Chapter 8 Alarm Settings 84
8.1 Setting Motion Detection Alarm 84
8.2 Setting Sensor Alarms 86
8.3 Detecting Video Loss Alarm 88
8.4 Detecting Video Tampering Alarm 90
8.5 Line Crossing Detection Alarm 91
8.6 Intrusion Detection Alarm 93
8.7 Handling Exceptions Alarm 94
8.8 Setting Alarm Response Actions 95
8.9 Triggering or Clearing Alarm Output Manually 98
Chapter 9 Network Settings 99
9.1 Configuring General Settings 99
9.2 Configuring Advanced Settings 99
9.2.1 Configuring Hik-Connect 99
9.2.2 Configuring DDNS 102
9.2.3 Configuring NTP Server 104

9.2.4 Configuring More Settings 105
9.2.5 Configuring E-Mail 106
9.2.6 Configuring NAT 107
9.2.7 Checking Network Traffic 111
9.3 Configuring Network Detection 111
9.3.1 Testing Network Delay and Packet Loss 111
9.3.2 Exporting Network Packet 112
9.3.3 Checking the Network Status 113
9.3.4 Checking Network Statistics 113
Chapter 10 HDD Management 115
10.1 Initializing HDDs 115
10.2 Configuring Quota Mode 116
10.3 HDD Detection 117
10.4 Configuring HDD Error Alarms 119
Chapter 11 Camera Settings 121
11.1 Configuring OSD Settings 121
11.2 Configuring Privacy Mask 121
11.3 Configuring Video Parameters 122
Chapter 12 Device Management and Maintenance 124
12.1 Viewing System Information 124
12.2 Searching and Exporting Log Files 124
12.3 Importing/Exporting Configuration Files 126
12.4 Upgrading System 127
12.4.1 Upgrading by Local Backup Device 128
12.4.2 Upgrading by FTP 128
12.5 Restoring Default Settings 129
Chapter 13 Others 130
13.1 Configuring General Settings 130
13.2 Configuring DST Settings 131
13.3 Configuring More Settings for Device Parameters 131
13.4 Managing User Accounts 132
13.4.1 Adding a User 132
13.4.2 Deleting a User 135
13.4.3 Editing a User 136
Chapter 14 Appendix 139
14.1 Glossary 139
14.2 Troubleshooting 140

Chapter 1 Introduction



Table 1-1 Description of Front Panel

No.	Icon	Description
1		Indicator turns green when NVR is powered up.
2		Indicator lights when data is being read from or written to HDD.
3		Indicator blinks when network connection is functioning properly.

1.2 USB Mouse Operation

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

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

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

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 Rear Panel

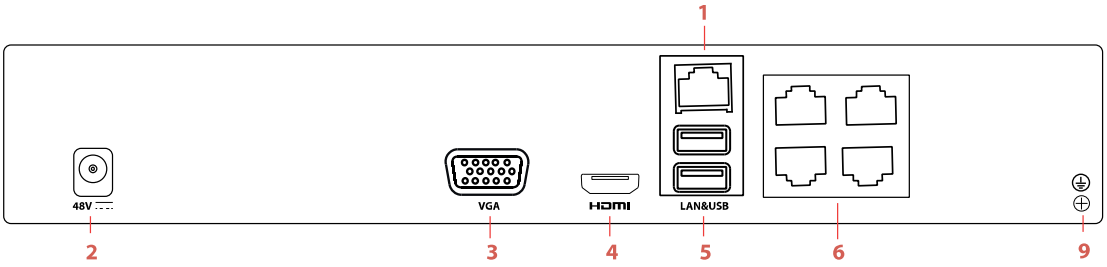


Figure 1-2 ERI-Q104-P4 Rear Panel

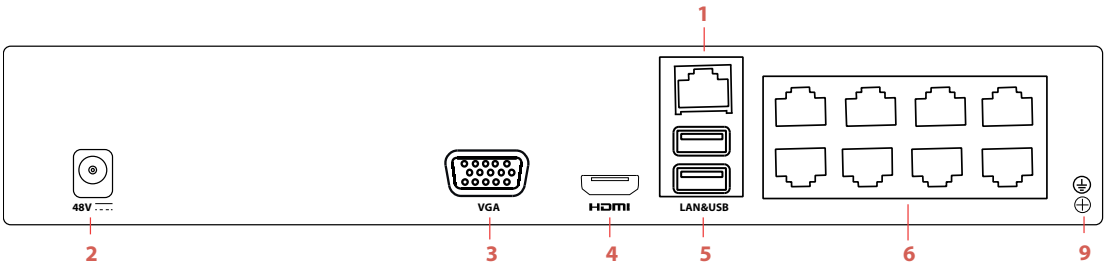


Figure 1-3 ERI-Q108-P8 Rear Panel

Table 1-3 Description of Rear Panel

No.	Item	Description
1	Power Supply	12 VDC power supply
2	VGA Interface	DB-9 connector for VGA output displays local video output and menu
3	HDMI Interface	HDMI video output connector
4	USB Interface	Universal Serial Bus (USB) ports for additional devices such as USB mouse and USB Hard Disk Drive (HDD)
5	LAN Network Interface	(1) 10 /100 /1000 Mbps self-adaptive Ethernet interface
6	Ground	Ground (needs to be connected when NVR starts up)
7	Network Interfaces with PoE function	Network interfaces for the cameras and to provide power over Ethernet 4 interfaces for /4P models and 8 interfaces for /8P models

Chapter 2 Getting Started

2.1 Device Startup and Activation

2.1.1 Starting Up and Shutting Down the NVR

Purpose:

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

Before You Start:

Check that the power supply voltage matches the NVR's requirement, and the ground connection is working properly.

Starting Up the NVR

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

2. The row of icons at the bottom of the screen shows the HDD status. "X" means that the HDD is not installed or cannot be detected.

Shutting Down the NVR

1. Go to **Menu > Shutdown**.



Figure 2-1 Shutdown Menu

2. Click **Shutdown**.

3. Click **Yes**.

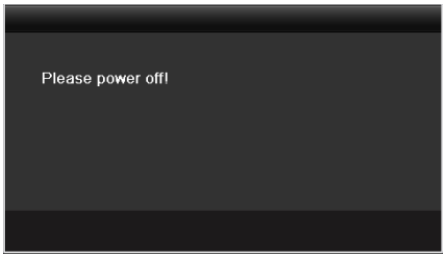


Figure 2-2 Shutdown Attention

Rebooting the NVR

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

1. Go to **Menu > Shutdown**.

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

2.1.2 Activating Your Device

Purpose:

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

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

2. Input a password in the **IP Camera Activation** field, to be used to activate connected IP cameras.

NOTE

Click the icon to show the **IP Camera Activation** password as you input it to ensure that it is input correctly.

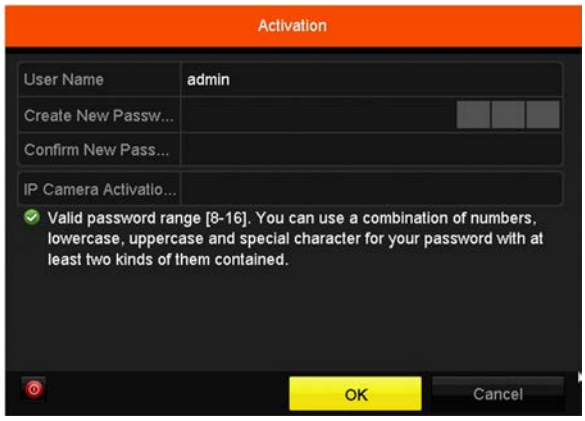


Figure 2-3 Settings Admin Password

WARNING

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

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

4. When the device is activated, the system pops up the message box to remind you to remember the password. You can click **Yes** to continue to export the GUID file for the future password resetting.



Figure 2-4 Export GUID File Remind

Insert the flash drive to your device, and export the GUID file to the flash drive in the Reset Password interface.

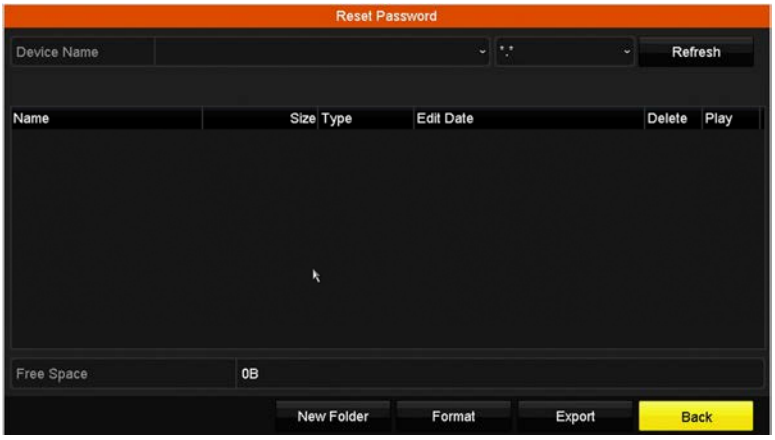


Figure 2-5 Export GUID File

NOTE

Keep your GUID file safely for future password resetting.

5. When the device is activated, the system pops up a message box to remind you to remember the password.

NOTE

For an old version device updated to the new version, the following dialog box will pop up once the device starts. Click **YES** and follow the wizard to set a strong password.

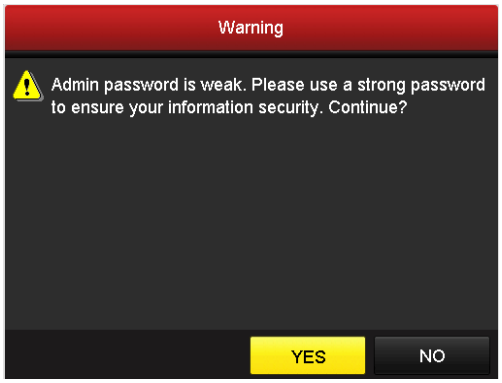


Figure 2-6 Warning

2.1.3 Using the Unlock Pattern for Login

Configure the unlock pattern for device login.

Configuring the Unlock Pattern

After the device is activated, configure the device unlock pattern.

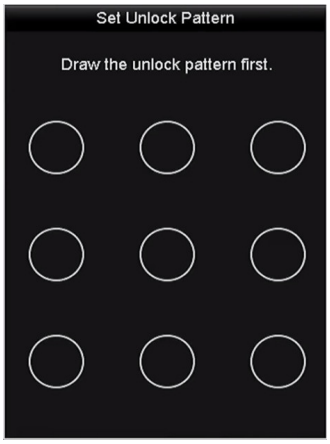


Figure 2-7 Set Unlock Pattern

1. Use the mouse to draw a pattern among the nine dots on the screen. Release the mouse when done.

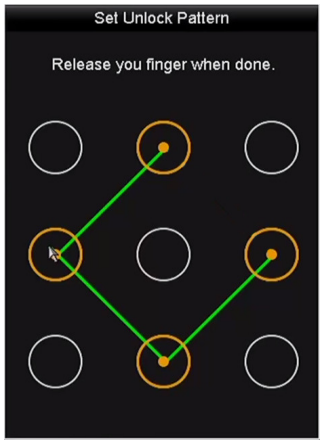


Figure 2-8 Draw the Pattern

NOTE

Connect at least four dots to draw the pattern.

Each dot can be connected only once.

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

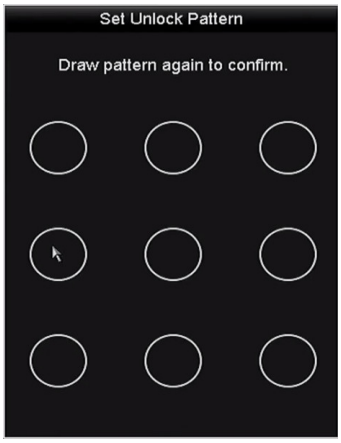


Figure 2-9 Confirm the Pattern

NOTE

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

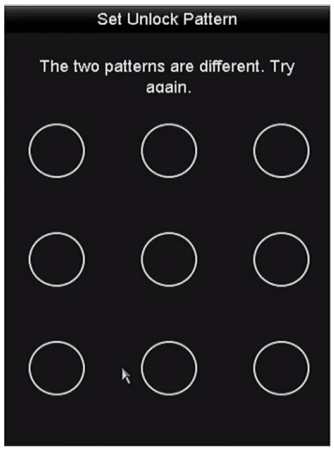


Figure 2-10 Re-set the Pattern

Logging in via Unlock Pattern

NOTE

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

Configure the pattern first before unlocking. Refer to Configuring the Unlock Pattern**.**

1. Right click the mouse on the screen and select the menu to enter the interface as shown in Figure 2.8.

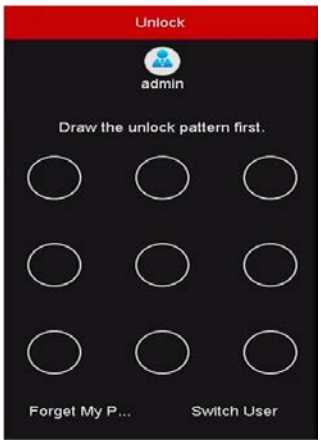


Figure 2-11 Draw the Unlock Pattern

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

NOTE

If you forget your pattern, select the **Forgot My Pattern** or **Switch User** option to enter the normal login dialog box.

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

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

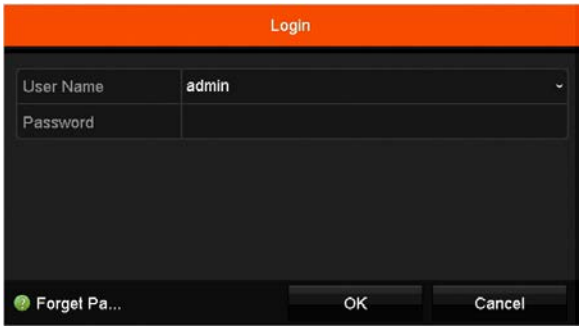


Figure 2-12 Normal Login Dialog Box

2.1.4 Login and Logout

User Login

Purpose:

If the NVR logs out, you must log in to the device before operating the menu and other functions.

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

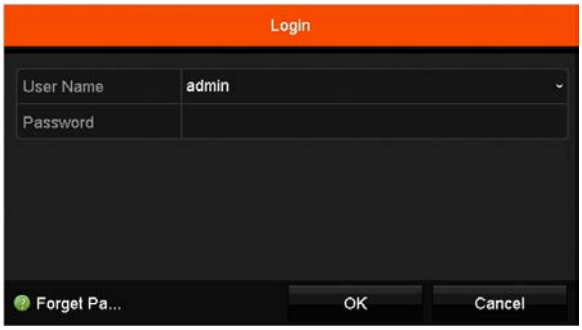


Figure 2-13 Login Interface

2. Input password.

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

NOTE

If you forget the admin password, click **Forgot Password** to reset the password.

NOTE

The device locks for 60 seconds if the admin user performs seven failed password attempts (five attempts for the guest/operator).

User Logout

Purpose:

After logging out, the monitor turns to the live view mode. To perform operations, you need to enter your user name and password to log in again.

1. Go to **Menu > Shutdown**.



Figure 2-14 Logout

2. Click **Logout**.

NOTE

After you log out of the system, menu operation on the screen is invalid. You are required to input a user name and password to unlock the system.

2.1.5 Resetting Your Password

If you forget the admin password, you can reset the password by importing the GUID file. The GUID file must be exported and saved in the local flash drive after you have activated the device (refer to Chapter 2.1.2 Activating Your Device).

1. On the user login interface, click **Forgot Password** to enter the Reset Password interface.

NOTE

Insert the flash drive containing the GUID file into the NVR before resetting the password.

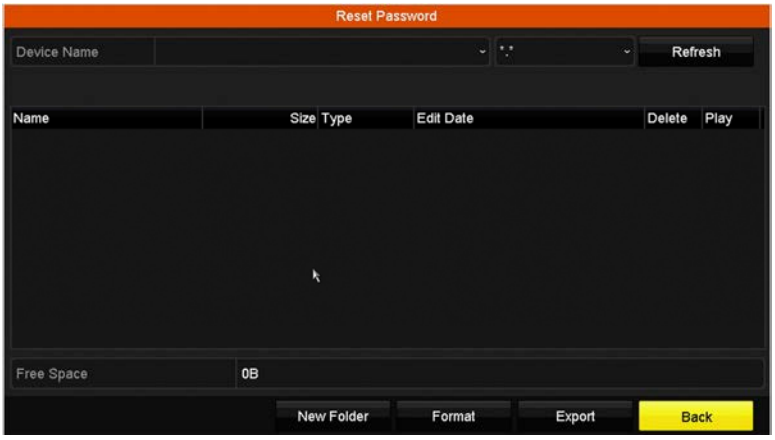


Figure 2-15 Reset Password

2. Select the GUID file from the USB flash drive and click **Import** to import the file to the device.

NOTE

If you import the wrong GUID file seven times, you will be not allowed to reset the password for 30 minutes.

3. After the GUID file is successfully imported, enter the reset password interface to set the new admin password.

4. Click **OK** to set the new password. You can export the new GUID file to the USB flash drive for future password resetting.

NOTE

When the new password is set, the original GUID file will be invalid. The new GUID file should be exported for future password resetting. You can also enter the **User > User Management** interface to edit the admin user and export the GUID file.

2.2 Using the Setup Wizard for Basic Configuration

The Setup Wizard can guide you to configure the system resolution, system date/time, HDD initialization, IP camera management, etc.

NOTE

To cancel the Setup Wizard, click **Exit**. You can choose to use the Setup Wizard next time by leaving the "Start wizard when the device starts?" checkbox checked.

1. Enter the general settings interface to configure the VGA/HDMI resolution, system date and time, and HDD initialization.

Initialize HDD

1. Check to initialize a new HDD used for the first time (factory-installed HDDs are already initialized).

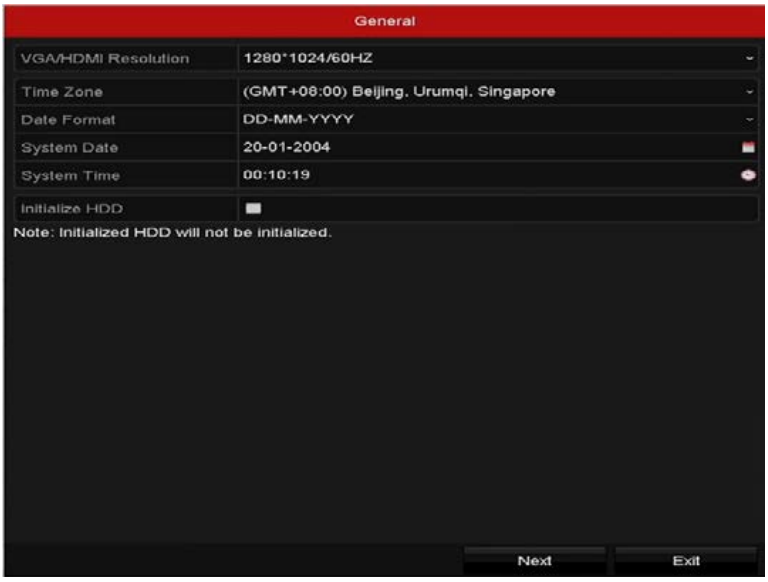


Figure 2-16 Start Wizard Interface

2. Click **Next** to enter the IP Camera Management interface.

Automatically Add Cameras (for Non-PoE Models)

1. For non-PoE devices, you can quickly add one or more IP cameras that are searched within the same network and have the same user name and password with the device.

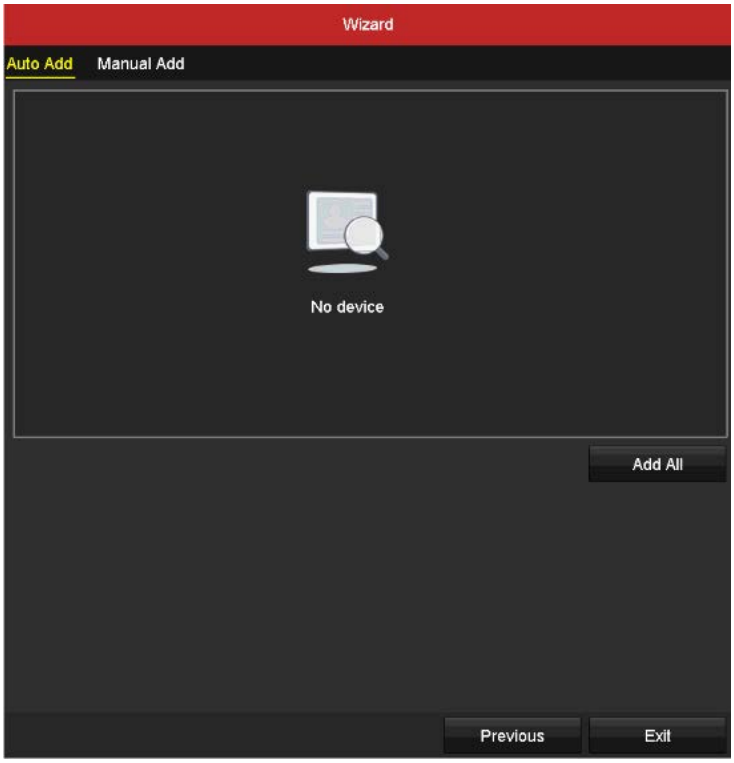


Figure 2-17 Start Wizard Interface

2. Click **Add All**. The device starts to search and add the matched cameras automatically.

3. Click **OK** when the cameras are added.

Manually Add Cameras

1. Click **Search** to search for online IP cameras within the same network.

2. Click **Add** to add the cameras that have the same user name and password as the device.

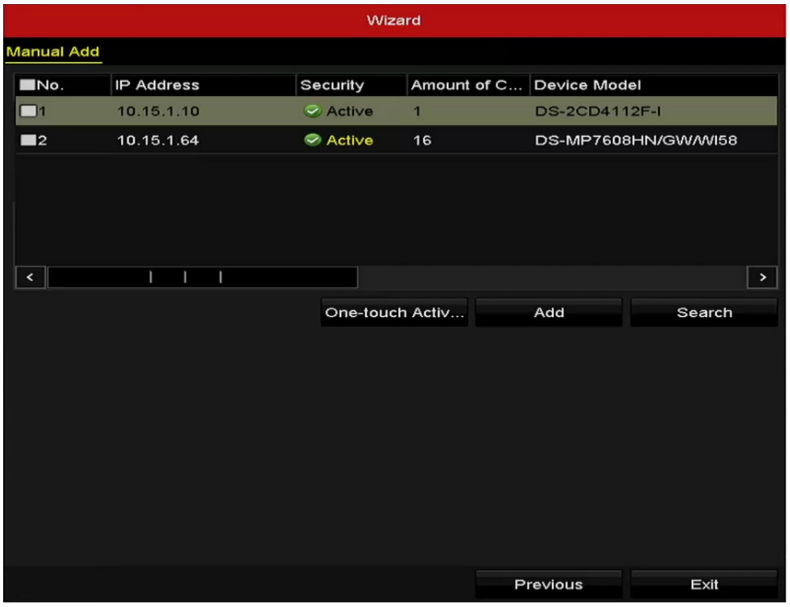


Figure 2-18 IP Camera Management

NOTE

Before adding a camera, make sure the IP camera to be added is in active status. If the camera is in inactive status, click the inactive icon of the camera to set the password to activate it. You can also select multiple cameras from the list and click **One-touch Activate** to activate the cameras in batch.

3. Click **Exit** to complete the Setup Wizard.

2.3 Adding and Connecting IP Cameras

2.3.1 Activating IP Cameras

Purpose:

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

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

NOTE

For detected online IP cameras in the same network segment, the **Password** status shows whether it is active or inactive.

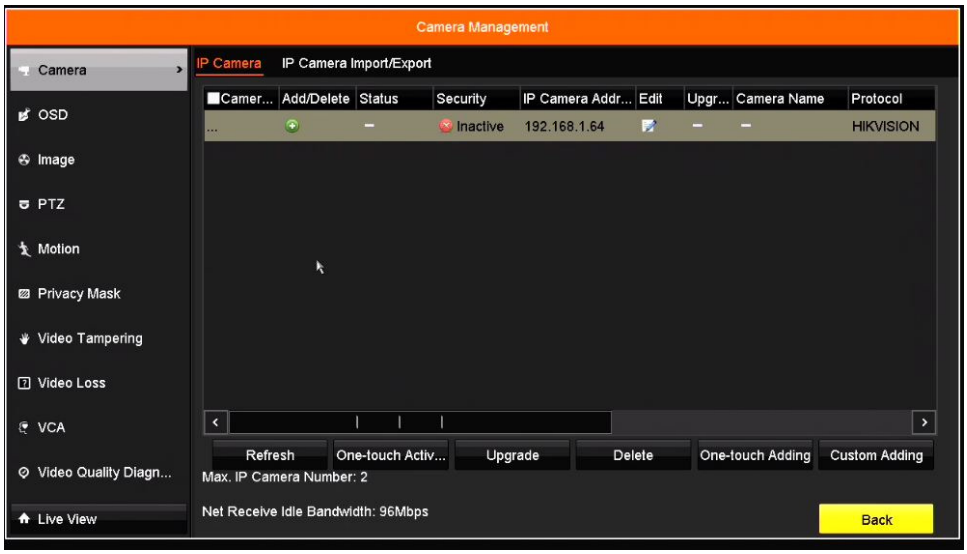


Figure 2-19 IP Camera Management Interface

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

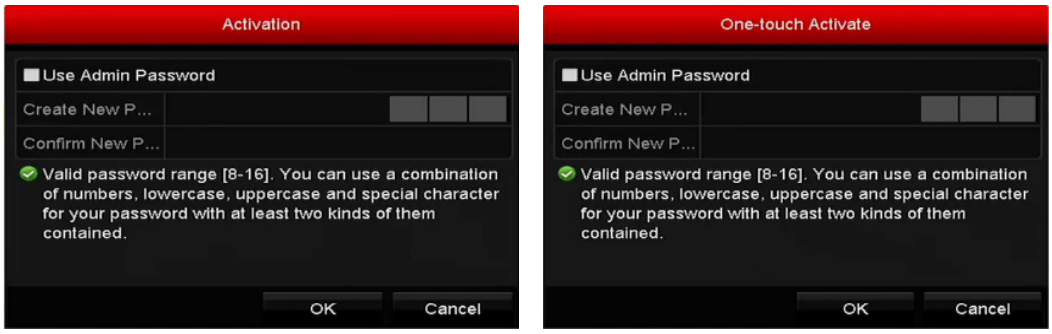


Figure 2-20 Activate the Camera

3. Set the camera password to activate it.

- **Use Admin Password**

  If you check the checkbox, the camera(s) will be configured with the same admin password as the operating NVR.



Figure 2-21 Set New Password

- **Create New Password**

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

WARNING

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

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

2.3.2 Adding Online IP Cameras

Purpose:

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

Before You Start:

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

Adding IP Cameras

- **OPTION 1**

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

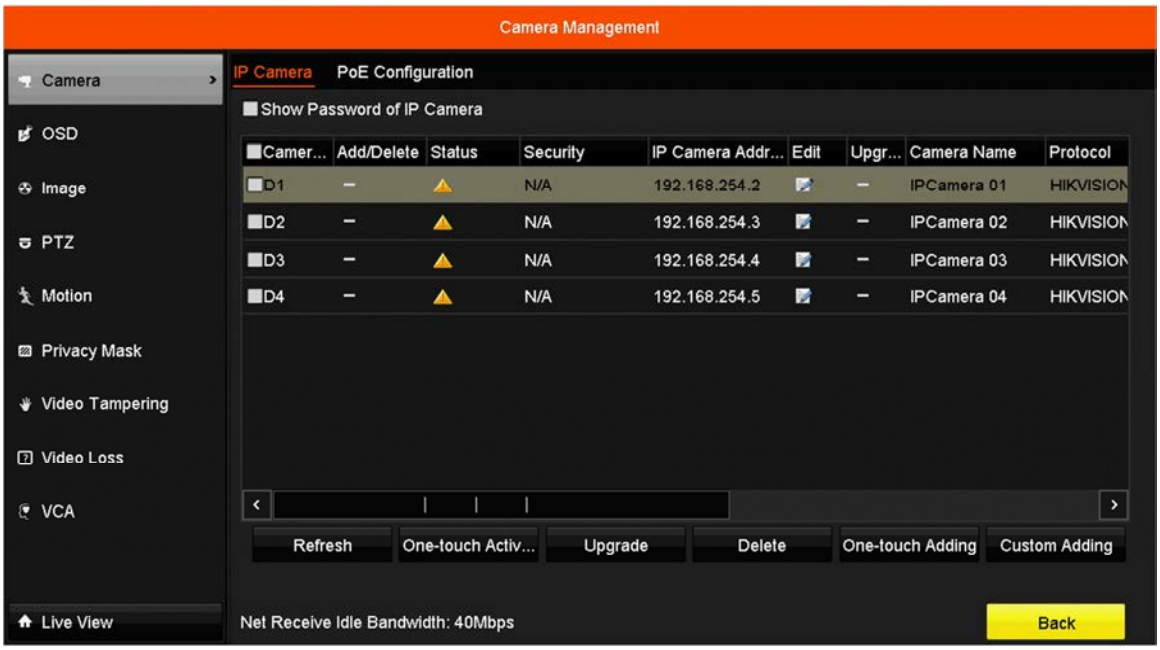


Figure 2-22 Adding IP Camera Interface

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

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

NOTE

Make sure the camera to add has already been activated.

- **OPTION 2**

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

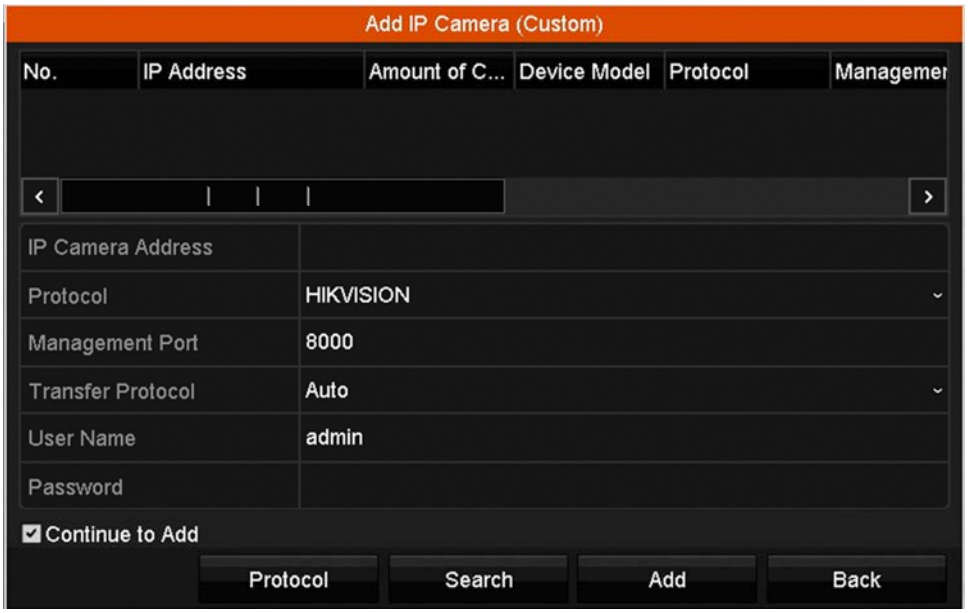


Figure 2-23 Custom Adding IP Camera Interface

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

NOTE

If the IP camera to add has not been activated, activate it from the IP camera list on the camera management interface.

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

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

5. Refer to the following table for the description of the icons

Table 2-1 Description of Icons

Icon	Explanation	Icon	Explanation
	Edit basic camera parameters		Upgrade the connected camera
	Camera disconnected; click icon to get camera's exception information		Delete the IP camera
	Play connected camera's live video		Camera connected

NOTE

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

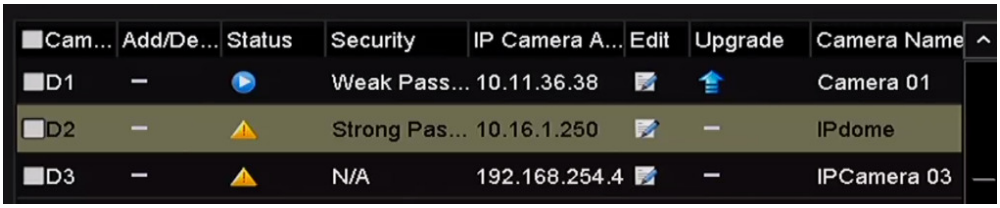


Figure 2-24 Security Level of IP Camera's Password

Showing the IP Camera Password

For the admin login user account, you can check **Show Password of IP Camera** to make the successfully added IP cameras' passwords visible.

You must enter the admin password to confirm permission.

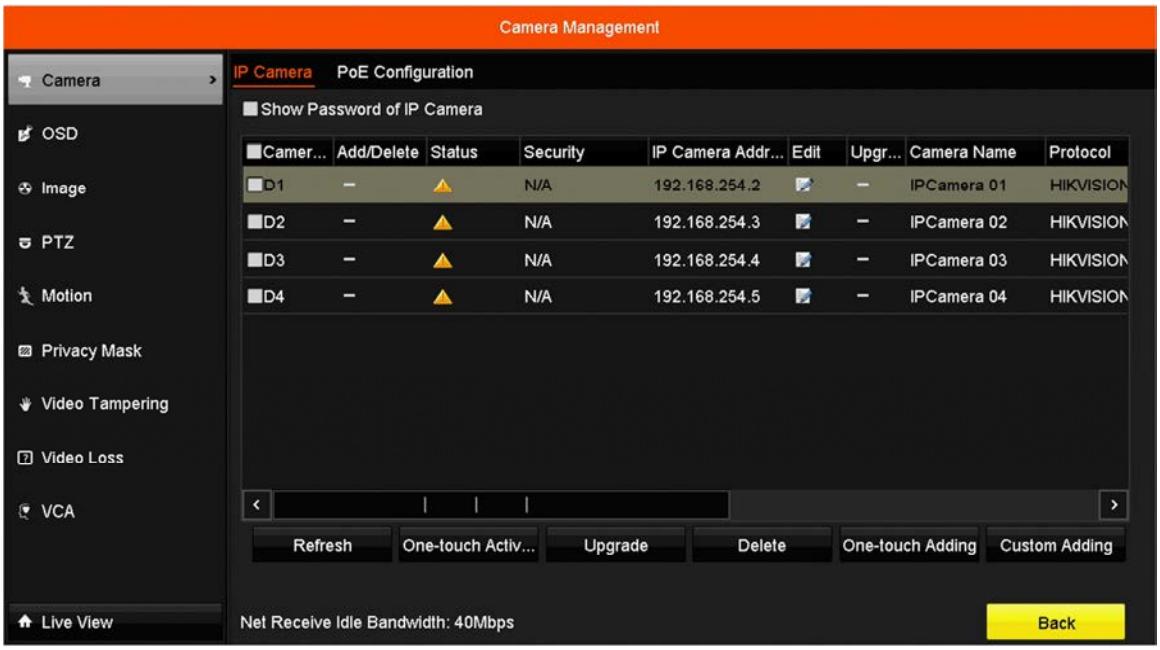


Figure 2-25 Show Password of IP Camera

2.3.3 Editing the Connected IP Cameras and Configuring Customized Protocols

After adding IP cameras, the basic camera information is listed. You can configure the basic IP camera settings.

Editing the IP Camera Parameters

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

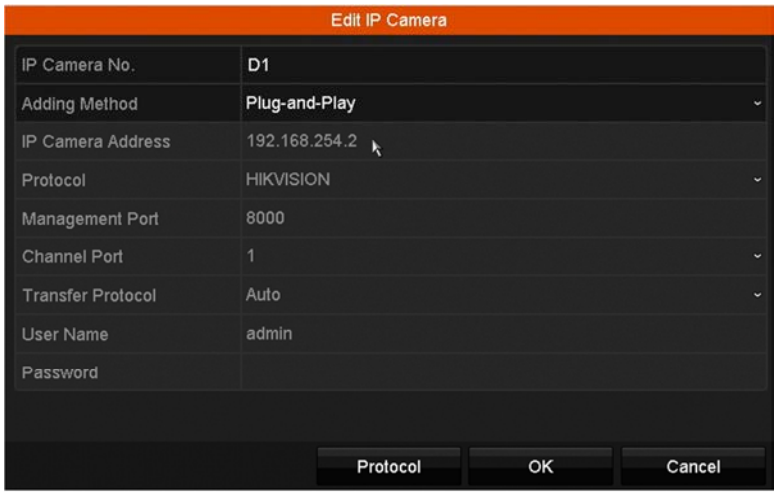


Figure 2-26 Edit the Parameters

- **Channel Port**

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

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

Editing the Advanced Parameters

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

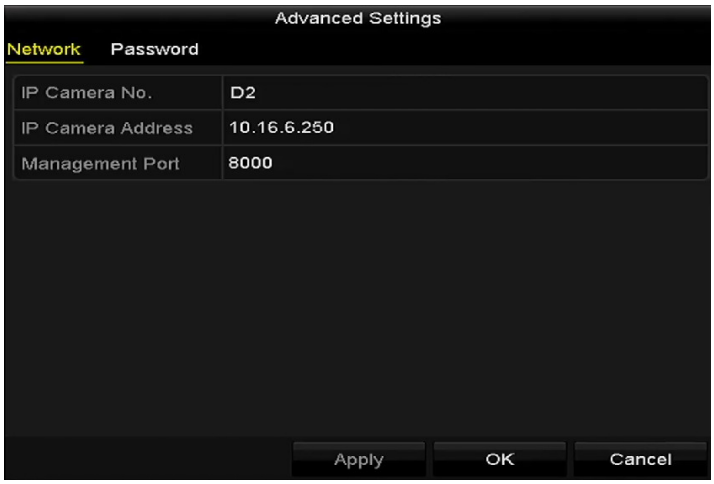


Figure 2-27 Network Configuration of the Camera

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

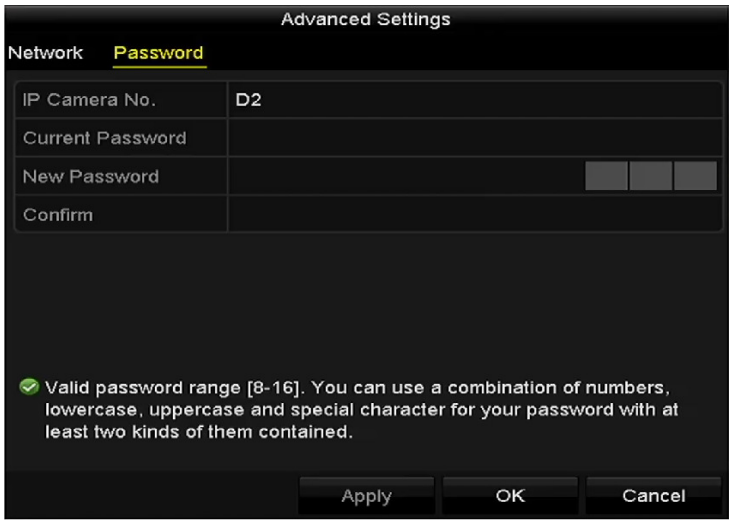


Figure 2-28 Password Configuration of the Camera

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

Configuring the Customized Protocols

Purpose:

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

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

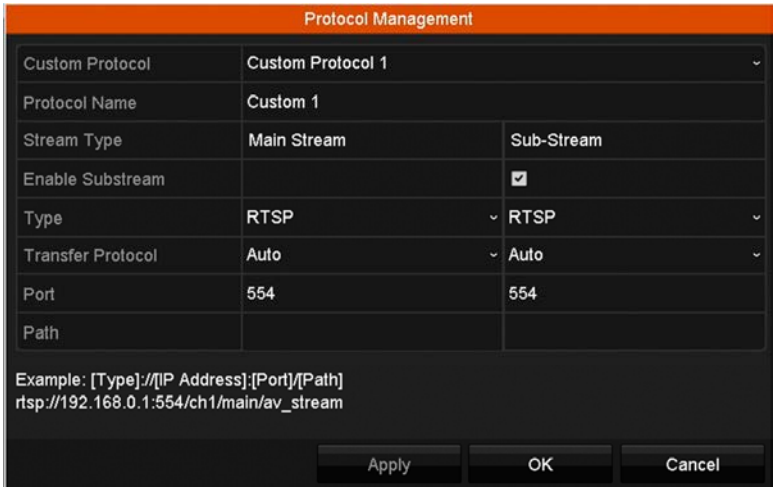


Figure 2-29 Protocol Management Interface

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

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

NOTE

Before customizing the protocol for the network camera, contact the network camera manufacturer to consult the URL (uniform resource locator) for getting the 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, the protocol name is listed in the drop-down protocol list.

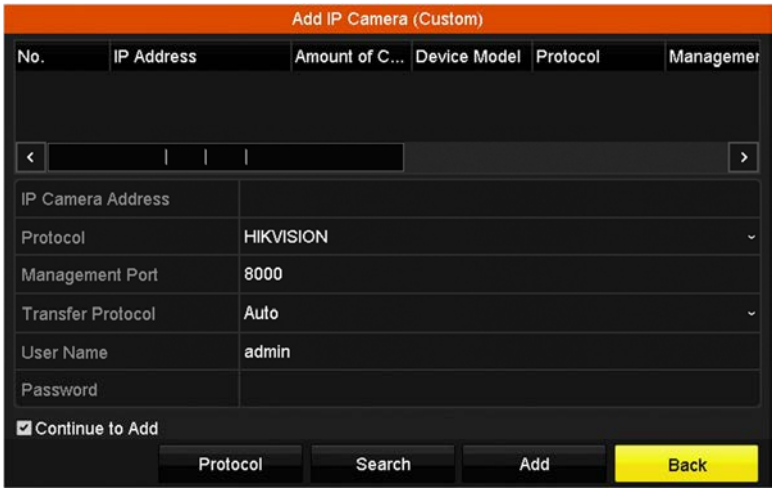


Figure 2-30 Protocol Setting

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

2.3.4 Editing IP Cameras Connected to the PoE Interfaces

NOTE

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

Up to four network cameras can be connected to /4P models, and eight network cameras to /8P models. If you disable the PoE interface, you can also connect to the online network cameras. The PoE interface supports the Plug-and-Play function.

To Add Cameras to NVRs that Support the PoE Function

Before You Start:

Connect the network cameras via the PoE interfaces.

1. Go to **Menu > Camera > Camera**.

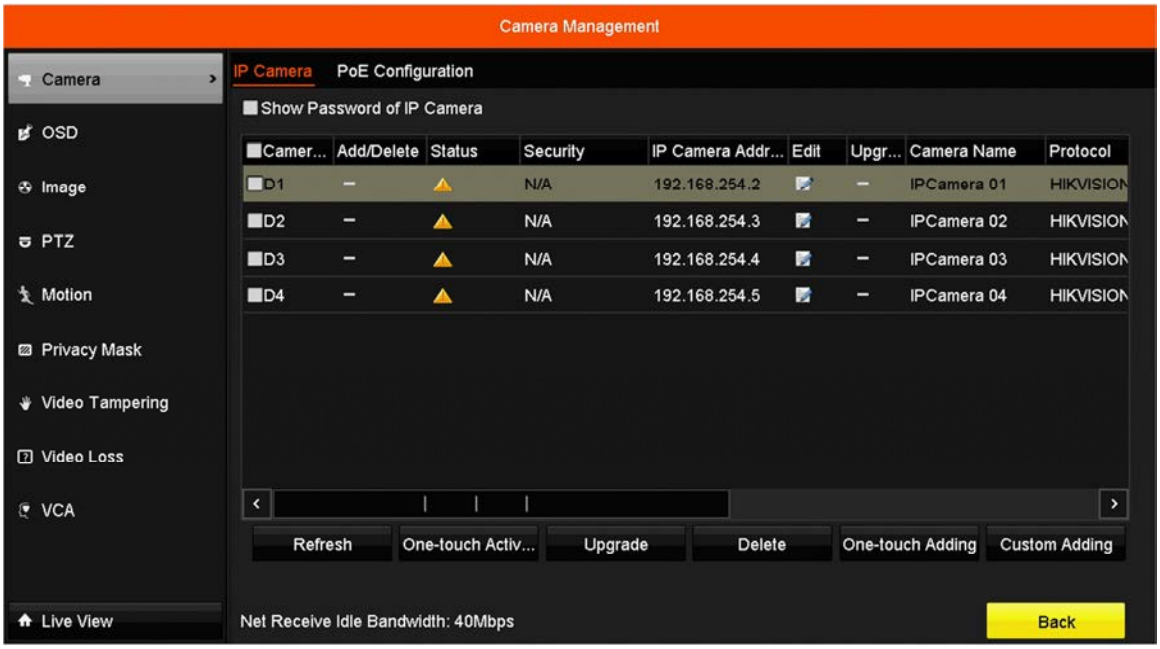


Figure 2-31 List of Connected Cameras

NOTE

Cameras connecting to the PoE interface cannot be deleted in this menu.

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

- **Plug-and-Play:** This means that the camera is connected to the PoE interface, so in this case, the camera parameters can't be edited. The camera's IP address can be edited only in the Network Configuration interface, see *Chapter 11.1 Configuring General Settings* for detailed information.

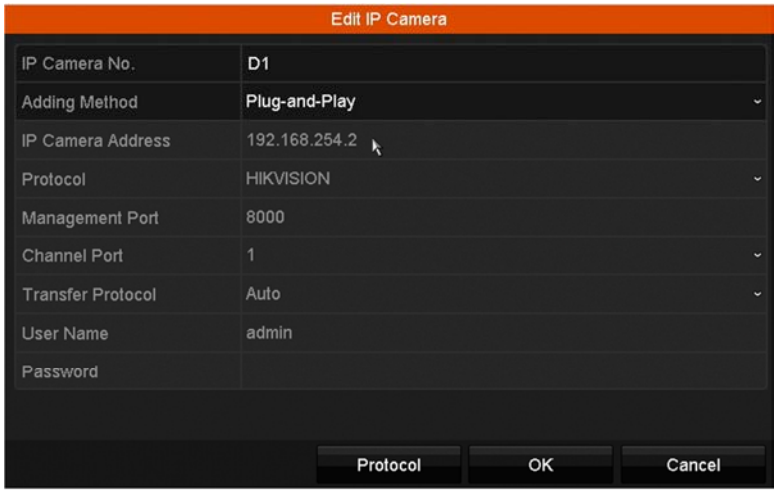


Figure 2-32 Edit IP Camera Interface - Plug-and-Play

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

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

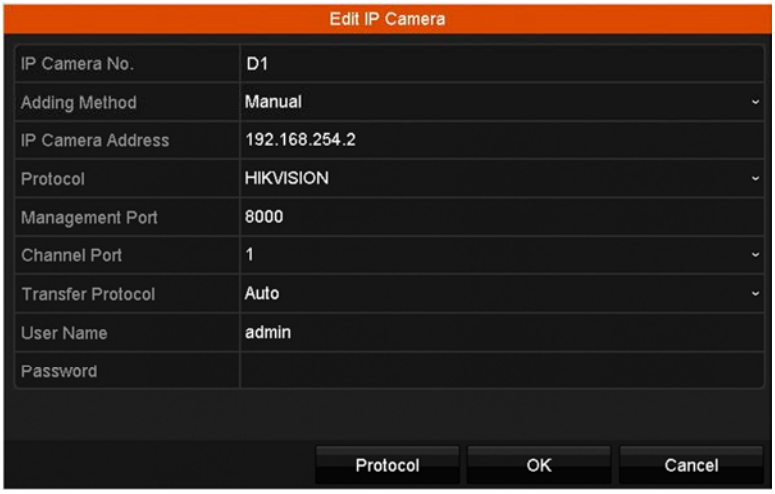


Figure 2-33 Edit IP Camera Interface - Manual

Chapter 3 Live View

Live View displays the video image getting from each camera in real time.

3.1 Live View Status Icons

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

Table 3-1 Description of Live View Icons

Icons	Description
	Alarm (video loss, video tampering, motion detection, sensor alarm, or VCA alarm)
	Record (manual record, continuous record, motion detection, sensor alarm, or VCA alarm triggered record)
	Alarm & Record
	Event/Exception (motion detection, sensor alarm, VCA alarm, or exception information appears at the lower-left corner of the screen. Refer to *Chapter 8.8 Setting Alarm Response Actions* for details.)

3.2 Operations in Live View Mode

3.2.1 Right-Click Menu

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

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

Table 3-2 Mouse Operation in Live View

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

NOTE

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

NOTE

The right-click menu varies by model. Refer to the actual GUI menu of the device.

3.2.2 Quick Setting Toolbar in Live View Mode

On each channel's screen, single click the mouse in the corresponding screen to display a quick setting toolbar.



Figure 3-1 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
	Face Detection		Live View Strategy		Information
	Close		Main/Sub-Stream		

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

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



Figure 3-2 Digital Zoom

Image Settings icon can be selected to enter the Image Settings menu. You can set the image parameters such as brightness, contrast, saturation, and hue.



Figure 3-3 Image Settings – Customize

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



Figure 3-4 Live View Strategy

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



Figure 3-5 Information

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, the screen number for each channel, etc.

1. Go to **Menu > Configuration > Live View**.



Figure 3-6 Live View-General

The settings available in this menu include:

- **Video Output Interface:** Designates the output for which to configure the settings. Only VGA/ HDMI™ is selectable by default.
- **Live View Mode:** Designates the display mode to be used for Live View.
- **Dwell Time:** The time in seconds to *dwell* between switching of channels when enabling auto-switch in Live View.
- **Volume:** Adjust the volume of live view, playback for the selected output interface.
- **Event Output:** Designates the output to show event video.
- **Full Screen Monitoring Dwell Time:** The time in seconds to show alarm event screen.

2. Set camera order.

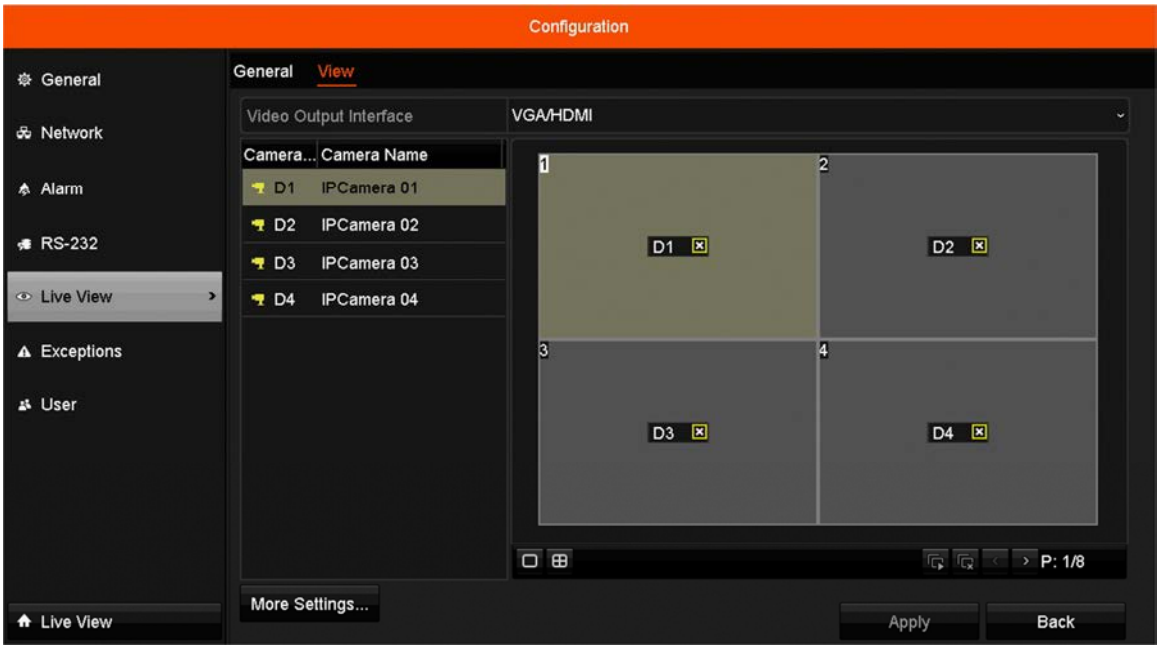


Figure 3-7 Live View Camera Order

- Select a View mode in . Up to 36-screen display is supported for 32-ch NVR.
- 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 the  icon to start live view for all the channels and click  to stop all live views.
- Click Apply to save the settings.

3. Set the stream type for the camera's live view.
   - Click **More Settings** to enter the more settings interface.
   - Select the camera to configure from the list.
   - Set the stream type to Main Stream, Sub-Stream, or Auto.

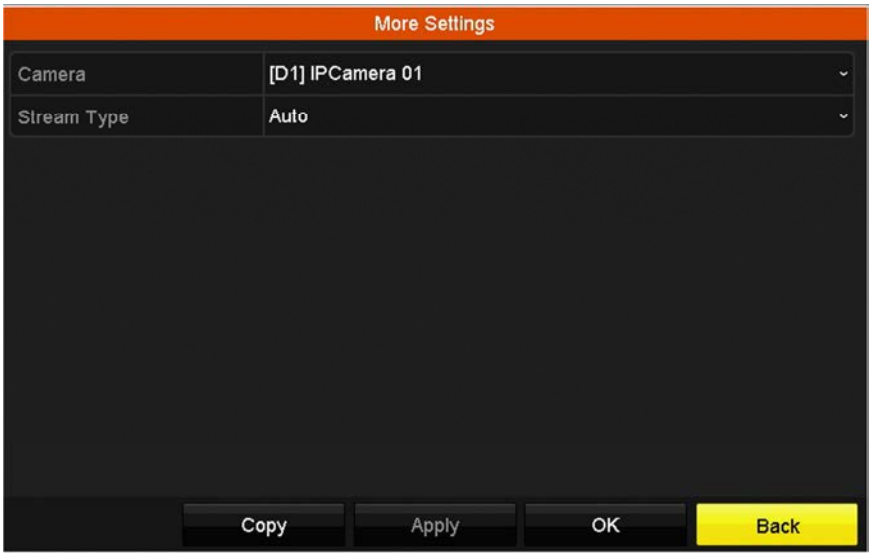


Figure 3-8 Stream Type Settings

- Click **Apply** to save the settings.
- (Optional) Click **Copy** to copy the stream type settings of the current camera to other camera(s).

Chapter 4 PTZ Controls

4.1 Configuring PTZ Settings

Purpose:

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

1. Go to **Menu > Camera > PTZ**.



Figure 4-1 PTZ Settings

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



Figure 4-2 PTZ- General

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

4. Enter the PTZ camera parameters.

NOTE

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

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

4.2 Setting PTZ Presets, Patrols, and Patterns

Before You Start:

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

4.2.1 Customizing Presets

Purpose:

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

1. Go to **Menu > Camera > PTZ**.



Figure 4-3 PTZ Settings

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

3. Enter the preset no. (1 to 255) in the preset text field.

4. Click **Set** to link the location to the preset.

5. Repeat steps 2-3 to save more presets.

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

4.2.2 Calling Presets

Purpose:

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

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

2. Choose **Camera** in the drop-down list.

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



Figure 4-4 PTZ Panel - General

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

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

4.2.3 Customizing Patrols

Purpose:

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

1. Go to **Menu > Camera > PTZ**.



Figure 4-5 PTZ Settings

2. Select patrol no. in the drop-down patrol list.

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

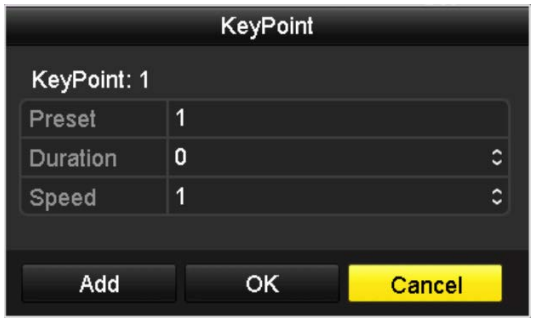


Figure 4-6 Key point Configuration

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

5. Click **Add** to add the next key point to the patrol. Click **OK** to save the key point to the patrol.

6. To delete all the key points, click **Clear** for the selected patrol, or click **Clear All** to delete all the key points for all patrols.

4.2.4 Calling Patrols

Purpose:

Calling a patrol moves the PTZ according the predefined patrol path.

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

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



Figure 4-7 PTZ Panel - General

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

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

4.2.5 Customizing Patterns

Purpose:

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

1. Go to **Menu > Camera > PTZ**.



Figure 4-8 PTZ Settings

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

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

4.2.6 Calling Patterns

Purpose:

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

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

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



Figure 4-9 PTZ Panel - General

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

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

4.2.7 Customizing Linear Scan Limit

Purpose:

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

1. Go to **Menu > Camera > PTZ**.



Figure 4-10 PTZ Settings

2. Use the directional button to wheel the camera to the location you want to set as 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 180°.

4.2.8 Calling Linear Scan

NOTE

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

Purpose:

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

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

2. Click the button to show the one-touch function of the PTZ control.



Figure 4-11 PTZ Panel - One-touch

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

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

4.2.9 One-Touch Park

NOTE

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

Purpose:

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

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

2. Click the button to show the one-touch function of the PTZ control.



Figure 4-12 PTZ Panel – One-touch

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

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

   NOTE

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

4. Click the button again to deactivate it.

4.2.10 PTZ Control Panel

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

- **OPTION 1**

  In the PTZ settings interface, click **PTZ** on the lower-right corner (next to the **Back** button).

- **OPTION 2**

  In Live View mode, press 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 **Configuration** on the control panel to enter the **PTZ Settings** interface.

NOTE

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



Figure 4-13 PTZ Panel

Table 4-1 Description of the PTZ panel icons

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

Chapter 5 Recording Settings

5.1 Configuring Parameters

Purpose:

Define the parameters that affect the image quality such as transmission stream type, resolution, etc.

Before You Start:

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

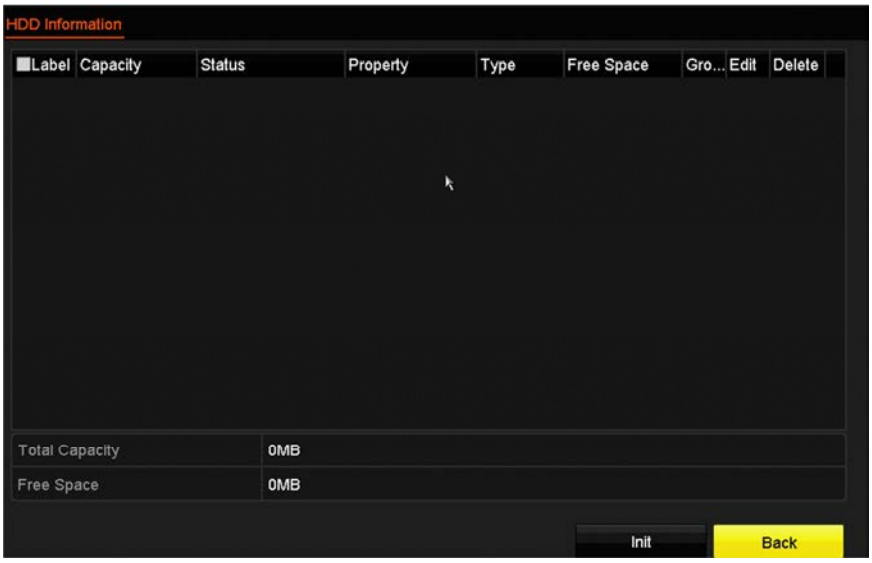


Figure 5-1 HDD- General

2. Check the storage HDD mode.

   - Click **Advanced** to check the HDD storage mode.
   - If the HDD mode is Quota, set the maximum record capacity. For detailed information, see Chapter 10.2 Configuring Quota Mode.

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



Figure 5-2 Recording Parameters

4. Set recording parameters.

- Select **Record** to configure. You can configure the stream type, the resolution, and other parameters upon demand.
- **Enable H.264+ Mode**: check the checkbox to enable this mode. Once enabled, the **Max. Bitrate Mode**, **Max. Bitrate (Kbps),** and **Max. Bitrate Range Recommend** are not configurable. Enabling it helps to ensure high video quality with a lowered bitrate.

NOTE

The function is available only for IP cameras that support H.264+ streaming.

- Click **More Settings** to set advanced recording parameters, and then click **OK** to finish editing.



Figure 5-3 Recording Parameters-More Settings

- **Pre-Record:** The time set to record before the scheduled time or event. For example, if an alarm triggers the recording at 10:00, if you set the pre-record time to 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 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 retention time for the file should be determined by the capacity of the HDD..
- **Record Audio**: Check the checkbox to enable 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.
- Click **Apply** to save the settings.

NOTE

You can enable the ANR (Automatic Network Replenishment) function via the Web browser (**Configuration** > **Storage** > **Schedule Settings** > **Advanced**) to save the video files in the IP camera when the network is disconnected, and synchronize the files to the NVR when the network is resumed.

NOTE

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

- Parameter Settings for Sub-stream
- Enter the Sub-stream tab page.



Figure 5-4 Sub-stream Parameters

- Configure the camera parameters.
- 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.

1. Go to **Menu > Record > Schedule**.

2. Configure the Record Schedule.

   - Select Record Schedule.



Figure 5-5 Record Schedule

Different recording types are marked in different color icons.

- **Continuous:** scheduled recording.
- **Event**: recording triggered by all event triggered alarm.
- **Motion**: recording triggered by motion detection.
- **Alarm:** recording triggered by alarm.
- **M/A:** recording triggered by either motion detection or alarm.
- **M&A:** recording triggered by motion detection and alarm.

Choose the camera you want to configure.

Select the **Enable Schedule** checkbox.

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

3. Edit the Schedule

   - In the message box, choose the day for which you want to set schedule.

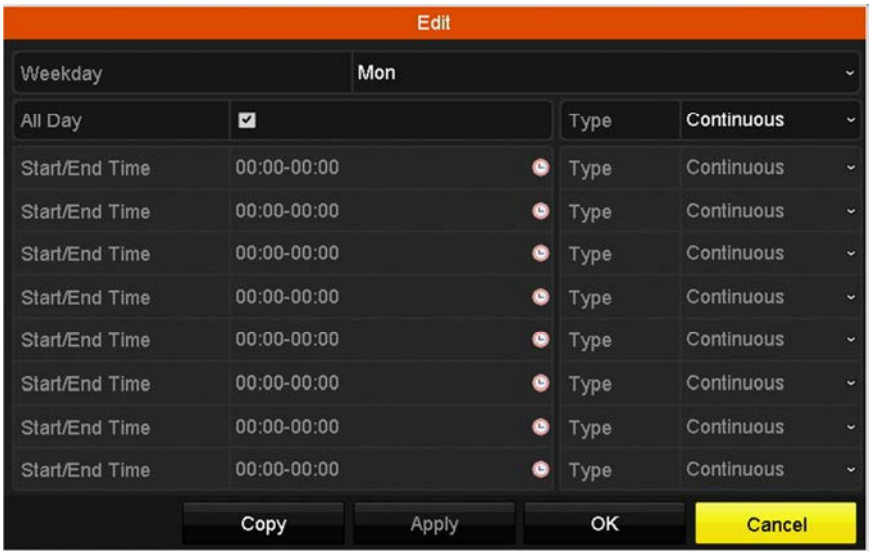


Figure 5-6 Recording Schedule Interface

- Click the icon to set the accurate time of the schedule.
- To schedule an all-day recording, check the **All Day** checkbox.

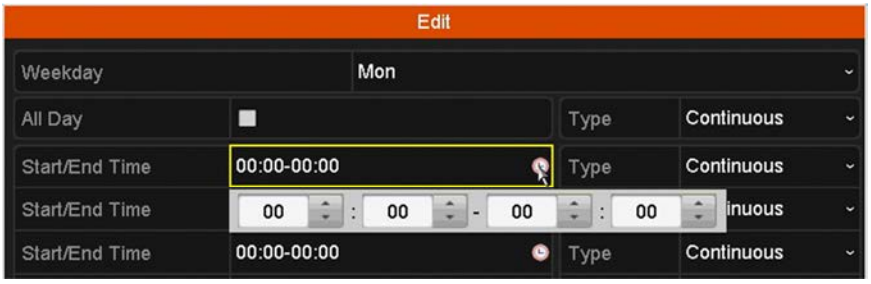


Figure 5-7 Edit Schedule

- To arrange other schedule(s), leave the **All Day** checkbox blank and set the Start/End time.

NOTE

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

4. 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 and capture, you must configure the motion detection settings, alarm input settings or VCA settings as well. For detailed information, refer to *Chapter 8.1* , *Chapter 8.2 , and Chapter 5.5 .*

VCA settings are available only to smart IP cameras.

Repeat the above edit schedule steps to schedule recording for other days of the week. Click **Copy** to enter the **Copy to** interface to copy the schedule settings to other days.

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

6. Draw the Schedule

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



Figure 5-8 Draw the Schedule

   - Click **Apply** to validate the settings.
   - (Optional) To use the settings for other channels, click **Copy** and choose the channel to copy to.

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

5.3 Configuring Motion Detection Recording

Purpose:

Follow the steps to set the motion detection parameters. In live view mode, if a motion detection event takes place, the NVR can analyze it and perform actions to handle it. Enabling motion detection can trigger certain channels to start recording or trigger full screen monitoring, audio warning, notify the surveillance center, etc.

1. Go to **Menu > Camera > Motion**.



Figure 5-9 Motion Detection

2. Configure Motion Detection

- Choose camera you want to configure.
- Check the **Enable Motion Detection** checkbox.
- Drag and draw the area for motion detection with the mouse. To set motion detection for the entire area shot by the camera, click **Full Screen**. To clear the motion detection area, click **Clear**.

NOTE

By default, **Dynamic Analysis for Motion** is enabled. When motion detection is triggered, green frames around the moving targets in the motion detection area will be displayed on the live video.

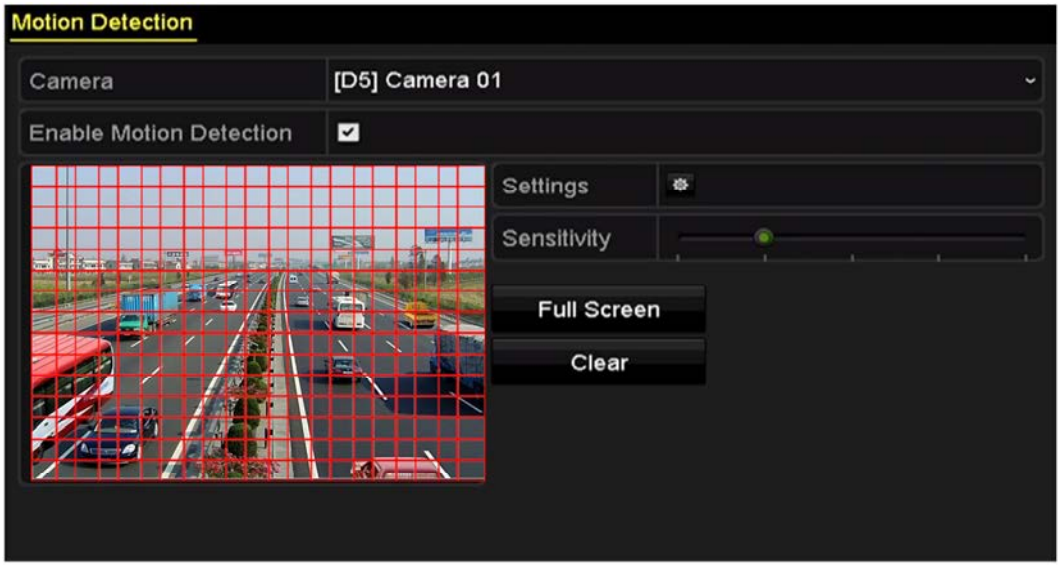


Figure 5-10 Motion Detection- Mask

- Click **Settings**, and the channel information message box pops up.



Figure 5-11 Motion Detection Handling

- Select the channels for which you want the motion detection event to trigger recording.
- Click **Apply** to save the settings.
- Click **OK** to go back to the upper level menu.
- Exit the Motion Detection menu.

3. Edit the Motion Detection Record Schedule. For detailed configuration information.

5.4 Configuring Alarm Triggered Recordings

NOTE

Alarm triggered recordings are possible only if using cameras with alarm inputs.

Purpose:

Follow the procedure to configure alarm triggered recordings.

1. Go to **Menu > Configuration > Alarm.**

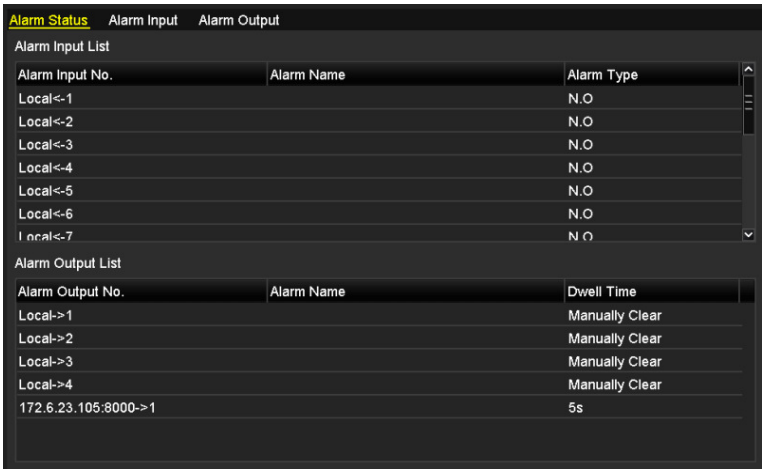


Figure 5-12 Alarm Settings

2. Click the **Alarm Input** tab and set the alarm parameters.



Figure 5-13 Alarm Settings- Alarm Input

- Select Alarm Input number and configure alarm parameters.
- Choose N.O. (normally open) or N.C. (normally closed) for alarm type.
- Check the **Enable** checkbox.
- Click **Settings**.

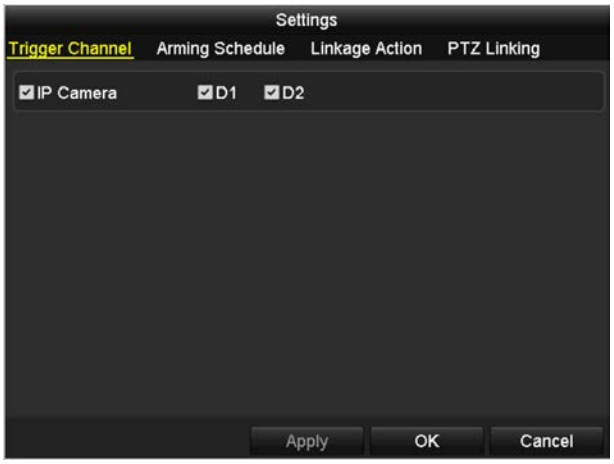


Figure 5-14 Alarm Settings

- Choose the alarm triggered recording channel.
- Check the checkbox to select channel.
- Click **Apply** to save settings.
- Click **OK** to back to the upper level menu.

3. Repeat the above steps to configure other alarm input parameters.

4. If the settings can also be applied to other alarm inputs, click **Copy** and choose the alarm input number.



Figure 5-15 Copy Alarm Input

5. Edit the Alarm triggered record in the Record Schedule setting interface. For the detailed schedule configuration information.

5.5 Configuring VCA Event Recording

Purpose:

You can configure the recording triggered by the line crossing detection and intrusion detection alarm events.

1. Go to **Menu > Camera > VCA**.

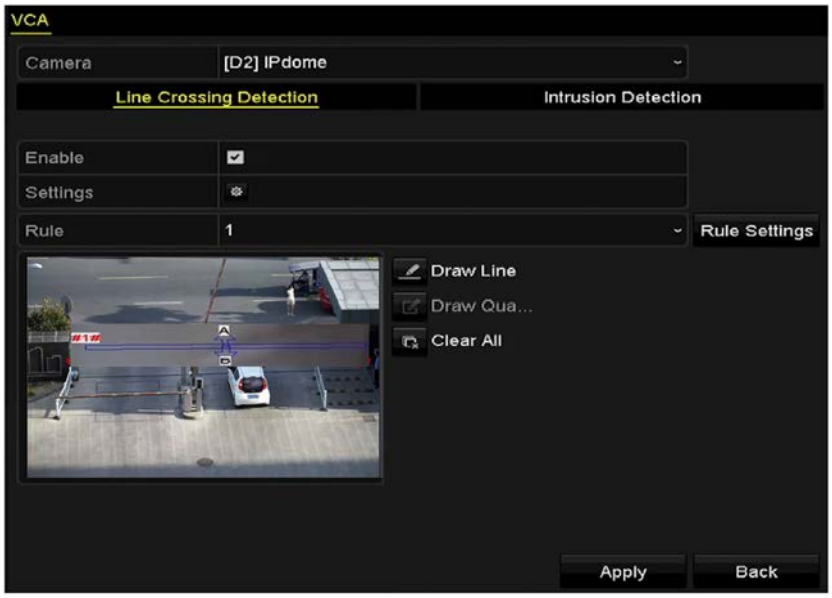


Figure 5-16 VCA Settings

2. Configure the detection rules for the line crossing detection or intrusion detection.
3. Click the icon to configure the alarm linkage actions for the VCA events.
   - Select **Trigger Channel** tab and channel(s) to start to record when a VCA alarm is triggered.
   - Click **Apply** to save the settings



Figure 5-17 Set Trigger Camera of VCA Alarm

4. Enter Record Schedule settings interface (**Menu** > **Record** > **Schedule** > **Record Schedule**), and then set VCA as the record type.

5.6 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.

1. Go to **Menu > Manual**, or press the **REC/SHOT** button on the front panel.

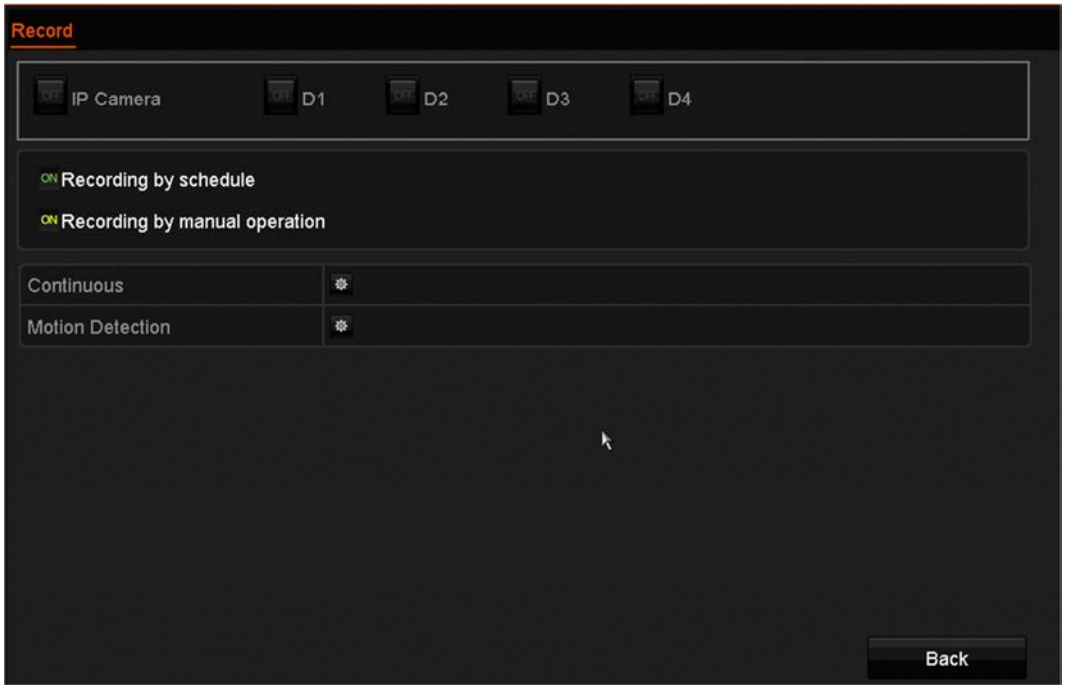


Figure 5-18 Manual Record

2. Enable Manual Record.
   - Select **Record** on the left bar.
   - Click the **status** button before camera number to change OFF to ON.
3. Disable manual record.
4. Click the **status** button to change 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.

5.7 Configuring Holiday Recording

Purpose:

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

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

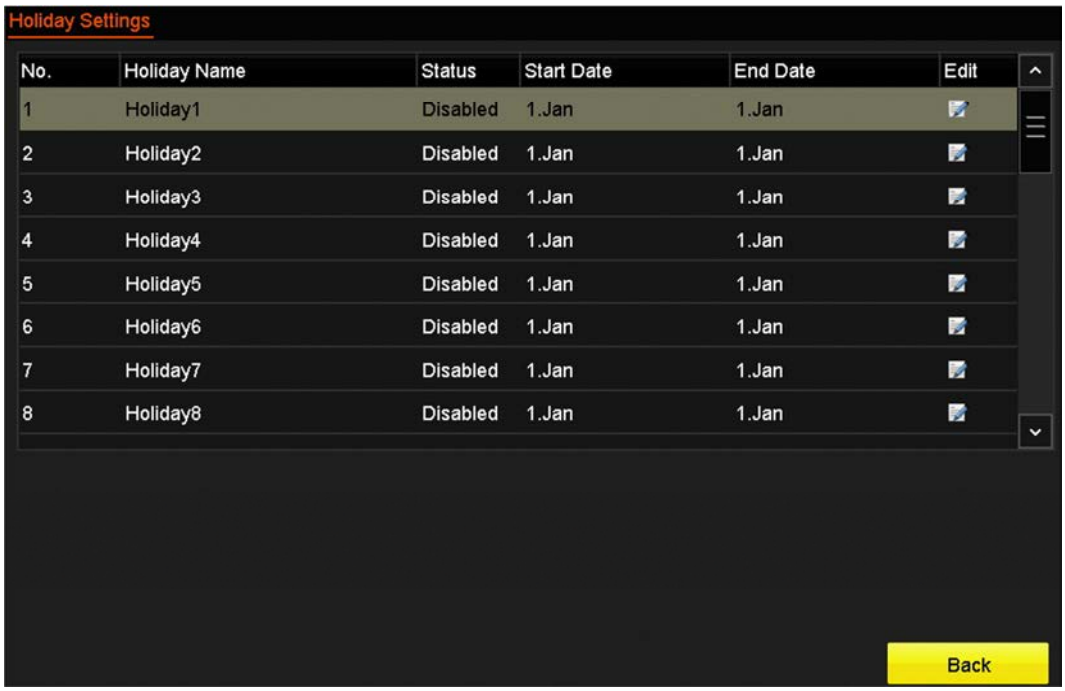


Figure 5-19 Holiday Settings

2. Enable Edit Holiday schedule.

   - Click  to enter the Edit interface.

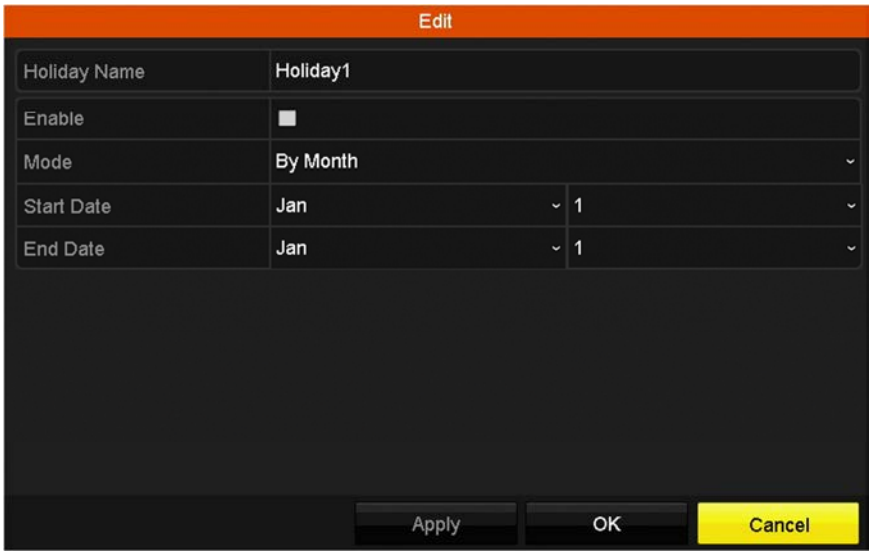


Figure 5-20 Edit Holiday Settings

- Check the **Enable Holiday** checkbox.
- Select **Mode** from the drop-down list.
- There are three different modes for the date format to configure holiday schedule.
- Set the start and end date.
- Click **Apply** to save settings.

3. Click **OK** to exit the Edit interface.
4. Enter the Record Schedule settings interface to edit the holiday recording schedule.

5.8 Files Protection

Purpose:

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

5.8.1 Locking the Recording Files

Lock File when Playback

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



Figure 5-21 Normal Playback

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

NOTE

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

4. Click to pop up the file management interface. Click **Locked File** to check and export the locked files.

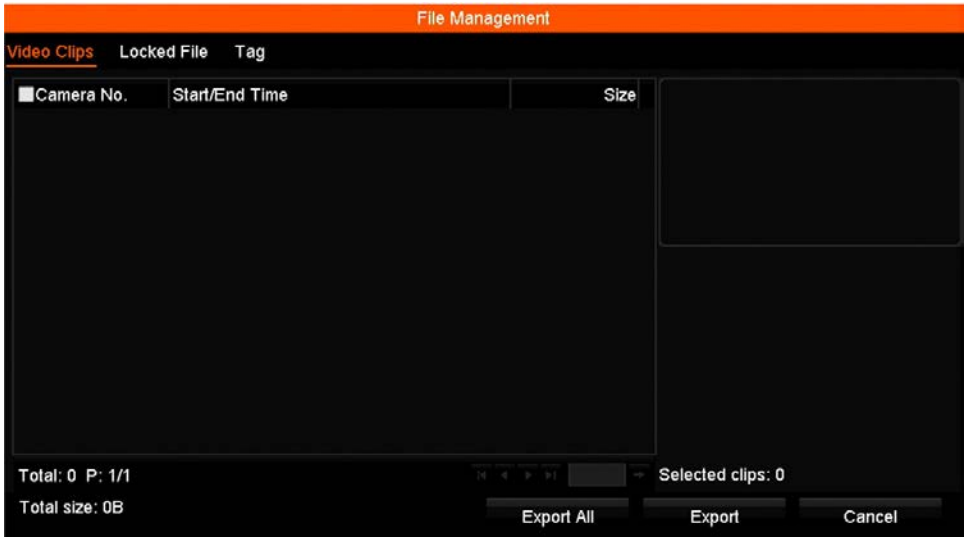


Figure 5-22 Locked File Management

5. In the File Management interface, click to change it to to unlock the (unprotect) the file.

Lock File when Exporting

1. Go to **Menu > Export**.

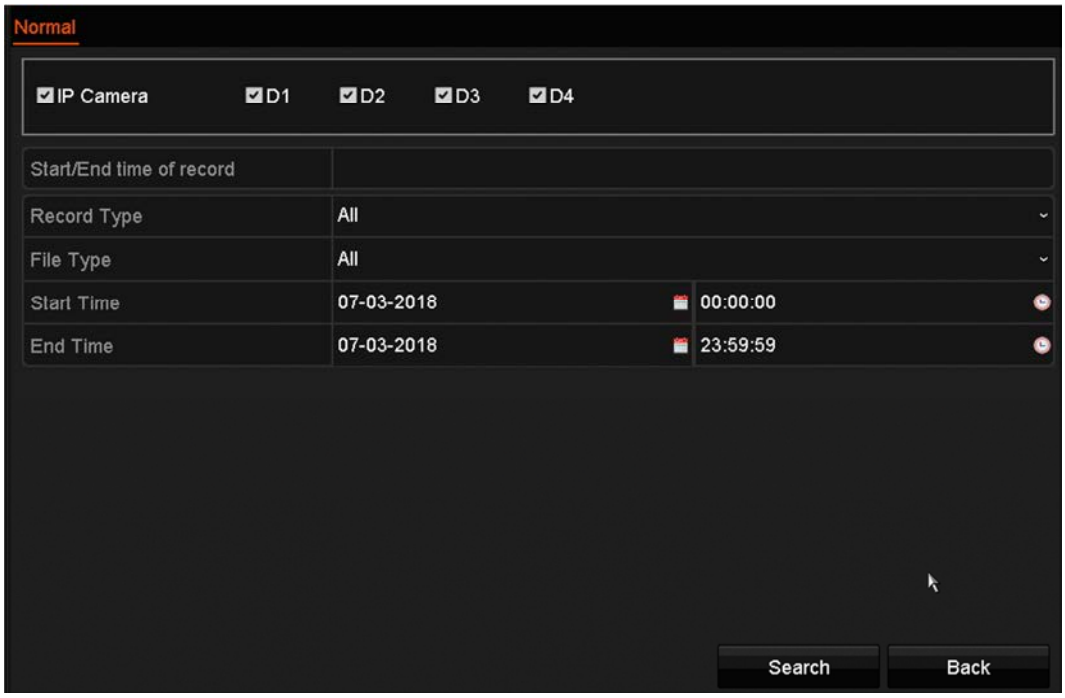


Figure 5-23 Export

2. Select the channels you want to investigate by checking the checkbox.

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

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



Figure 5-24 Export Search Result

5. Protect the record files.

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

   NOTE

   Incomplete record files cannot be locked.

   - Click to change it to to unlock the file. The file is not protected.



Figure 5-25 Unlocking Attention

5.8.2 Setting HDD Property to Read-only

1. Go to **Menu** > **HDD**.

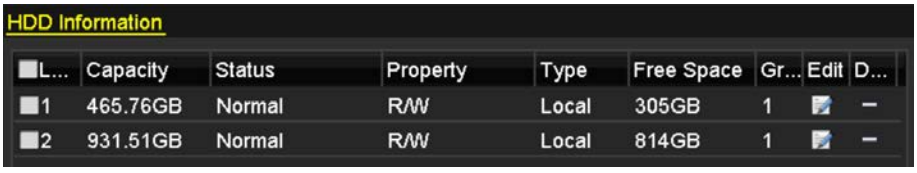


Figure 5-26 HDD General

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



Figure 5-27 HDD General- Editing

3. Set the HDD property to **Read-only**.

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

NOTE

You cannot save files to a read-only HDD. To save files to the HDD, change the property to R/W.

If there is only one HDD and it is set to Read-only, the NVR can't record any files. Only live view mode is available.

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

Chapter 6 Playback

6.1 Playing Back Record Files

6.1.1 Instant Playback

Purpose:

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

Instant Playback by Channel

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

NOTE

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



Figure 6-1 Instant Playback Interface

6.1.2 Playing Back by Normal Search

Playback by Channel

1. Enter the Playback interface.
2. Right-click a channel in live view mode and select **Playback** from the menu.

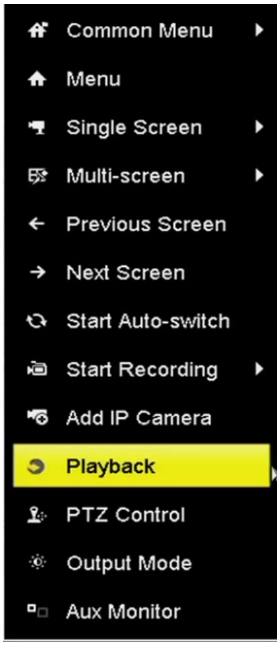


Figure 6-2 Right-click Menu under Live View

NOTE

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

Playback by Time

Purpose:

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

1. Go to **Menu > Playback**.
2. Select **Normal/Smart** in the drop-down list on the top-left side.
3. Select a camera in the camera list.
4. Select a date in the calendar and click the button on the left toolbar to play the video.



Figure 6-3 Playback Calendar

If there are record files for that camera in that day, in the calendar, the icon for that day is displayed in different colors for different recording types: blue for continuous recording and red for event recording.

5. Click Normal to start playing the continuous recorded files.

Playback Interface

Use the toolbar on the bottom of the playback interface to control the playing progress.



Figure 6-4 Playback Interface



Figure 6-5 Toolbar of Playback

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

NOTE

The 01-01-2016 00:00:23 -- 04-07-2016 19:37:29 indicates the start/end time of the recorded video files.

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

Table 6-1 Detailed Explanation of Playback Toolbar

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

NOTE

Refer to *Chapter 3.2.4 Fisheye Expansion* for description and operation of the fisheye expansion.

NOTE

256x playing speed is supported.

6.1.3 Playing Back by Smart Search

Purpose:

The smart playback function provides an easy way to get through the less relevant information. When you select smart playback mode, the system will analyze the video containing the motion or VCA information, mark it in green, and play it at normal speed while the video without motion will be played at 16x 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.

1. Go to **Menu > Playback**.
2. Select the **Normal/Smart** in the drop-down list on the top-left side.
3. Select a camera in the camera list.
4. Select a date in the calendar and click on the left toolbar to play the video file.



Figure 6-6 Playback by Smart Search

5. Click Smart to switch to playback by smart search.
6. Set the rules and areas for smart search of line crossing detection, intrusion detection, or motion detection event triggered recording.
   - **Motion Detection**

     Click , and then hold the mouse on the image to draw the mouse to set the detection area manually. You can also click the button to set the full screen as the detection area.
   - **Line Crossing Detection**

     Select , and click on the image to specify the start point and end point of the line.
   - **Intrusion Detection**

     Click , and specify four points to set a quadrilateral region for intrusion detection. Only one region can be set.
7. (Optional) Click to filter the searched video files by setting the target characters, including the gender and age of the human and whether he/she wears glasses.



Figure 6-7 Set Result Filter

6.1.4 Playing Back by Event Search

Purpose:

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

1. Go to **Menu > Playback**.

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

3. Set the major type to **Alarm Input**, **Motion**, or **VCA** as the event type.

NOTE

We take playback by VCA as the example in the following instructions.



Figure 6-8 Event Search Interface

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

NOTE

For configuring the VCA recording, refer to *Chapter 5.5 Configuring VCA Event Recording and Capture*; for VCA detection type details, refer to *Chapter 9 VCA Alarm*.

5. Select the camera(s) to search, and set the Start time and End time.

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

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

NOTE

Pre-play and post-play can be configured.

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



Figure 6-9 Synch Playback Interface

9. Enter the playback interface. Use the toolbar on the bottom of the playback interface to control playing.



Figure 6-10 Interface of Playback by Event

10. Click or to select the previous or next event. Refer to Table 6.1 for the description of buttons on the toolbar.

6.1.5 Playing Back by Tag

Purpose:

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

Before playing back by tag:

1. Go to **Menu > Playback**.

2. Search and play back the record file(s). Refer to *Chapter 6.1.1* for detailed information about searching for and playing back record files.



Figure 6-11 Interface of Playback by Time

3. Click to add the default tag.

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

NOTE

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

Tag Management

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



Figure 6-12 Tag Management Interface

Playing Back by Tag

1. Select **Tag** from the drop-down list in the Playback interface.
2. Choose channels, edit the start time and end time, and click **Search** to enter the Search Result interface.

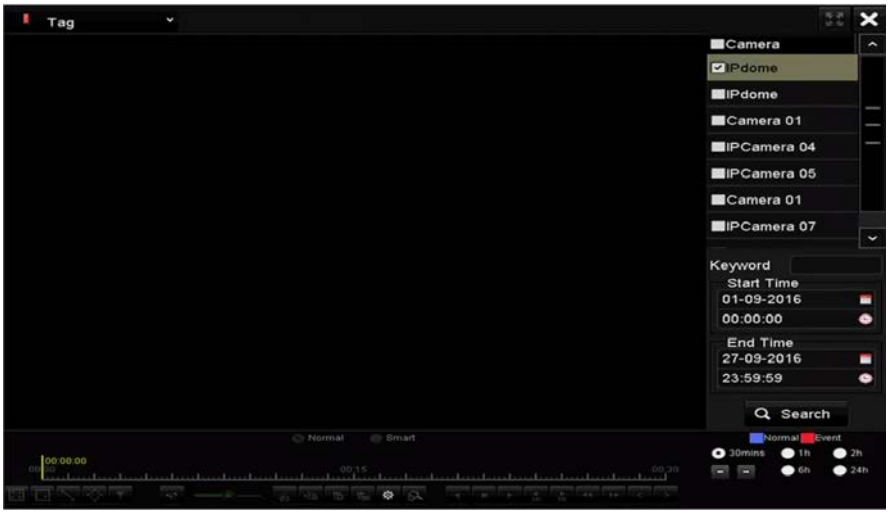


Figure 6-13 Interface of Playback by Tag

NOTE

You can enter keywords into the Keyword textbox to search for tags on command.

3. Click to play back the selected tag file.
4. Click **Back** to go back to the search interface.



Figure 6-14 Interface of Playback by Tag

NOTE

Pre-play and post-play can be configured.

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

6.1.6 Playing Back by System Logs

Purpose:

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

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

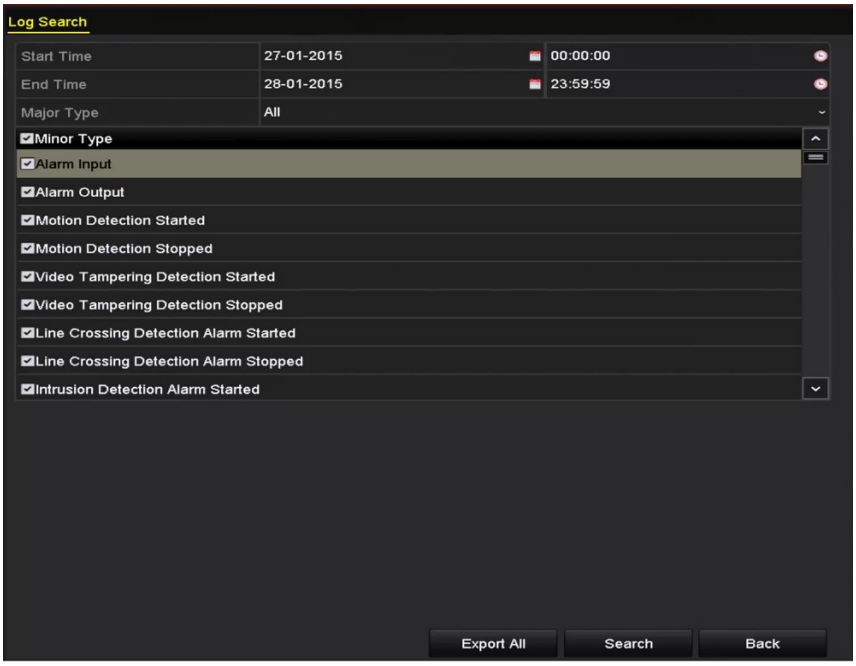


Figure 6-15 System Log Search Interface

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

NOTE

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

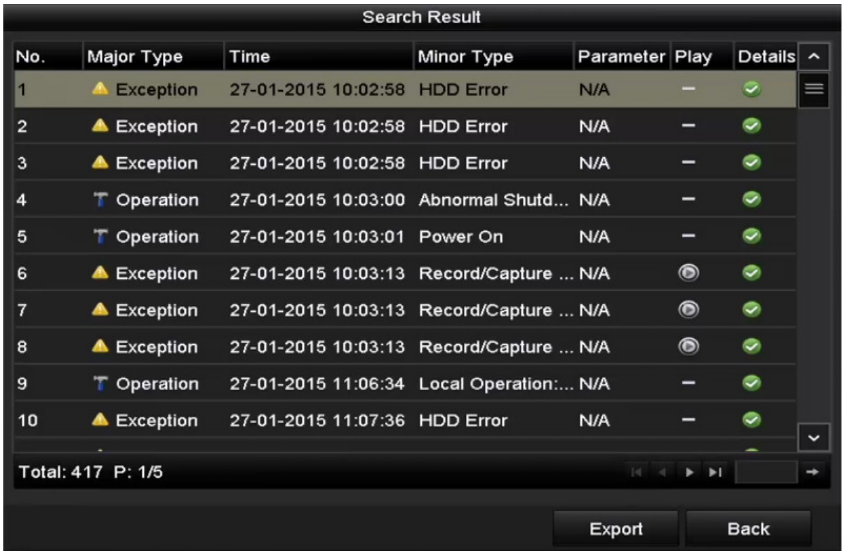


Figure 6-16 Result of System Log Search

5. **Playback Interface.** Use the Playback interface bottom toolbar to control playing.



Figure 6-17 Interface of Playback by Log

6.1.7 Playing Back External Files

Purpose:

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

1. Go to **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.
   - Click Refresh to refresh the file list.
3. Select and click to play the file. Adjust playback speed by clicking and .



Figure 6-18 Interface of External File Playback

6.1.8 Playing Back by Sub-Periods

Purpose:

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

1. Go to **Menu > Playback**.

2. Select **Sub-periods** from the drop-down list in the upper-left corner of the page to enter the Sub-periods Playback interface.

3. Select a date and start playing the video file.

4. Select the **Split-Screen Number** from the drop-down list. Up to 16 screens are configurable.



Figure 6-19 Interface of Sub-periods Playback

NOTE

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

6.2 Auxiliary Playback Functions

6.2.1 Playing Back Frame-by-Frame

Purpose:

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

Using a Mouse:

Go to **Menu > Playback**.

- **To Play Back the Record File:** Click the ◀◀ button until the speed changes to **Single Frame,** then one click on the playback screen represents playback of one frame.

- **To Reverse Play Back the Record File:** Click the button until the speed changes to **Single Frame** and one click on the playback screen represents reverse playback of one frame. It is also possible to use the button in the toolbar.

Using the Front Panel

Click the to set the speed to **Single Frame**. One click on the button, one click on the playback screen or **Enter** button on the front panel, represents playback or reverse playback of one frame.

6.2.2 Fast View

Hold the mouse down and drag on the time bar to get a fast view of the video files.

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



Figure 6-20 Playback Interface

2. Use the mouse to hold and drag through the playing time bar to fast view the video files.

3. Release the mouse at the required time point to enter the full-screen playback.

NOTE

The fast view is supported only in the 1x single-camera playback mode.

6.2.3 Digital Zoom

1. Click the on the playback control bar to enter the Digital Zoom interface.

2. You can zoom into the image at different magnifications (1 to 16x) by moving the sliding bar from to . You can also scroll the mouse wheel to control the zoom in/out.



Figure 6-21 Draw Area for Digital Zoom

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

6.2.4 File Management

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

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



Figure 6-22 File Management

3. You can view saved video clips, lock/unlock files, and edit the tags that you added in the playback mode.
4. (Optional) Select items and click **Export All** or **Export** to export clips/files/tags to the local storage device.

Chapter 7 Backup

7.1 Backing up Record Files

7.1.1 Backing up by Normal Video Search

Purpose:

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

Back up using USB flash drives or USB HDDs.

1. Go to **Menu > Export > Normal**.
2. Select the cameras to search.
3. Set search condition and click **Search** to enter the search result interface. The matched video files are displayed in Chart or List display mode.

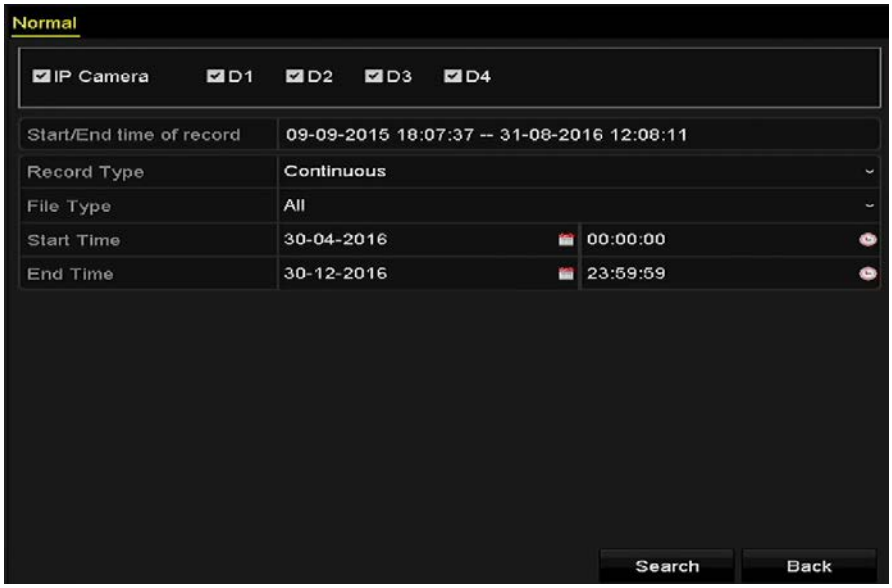


Figure 7-1 Normal Video Search for Backup

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

NOTE

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

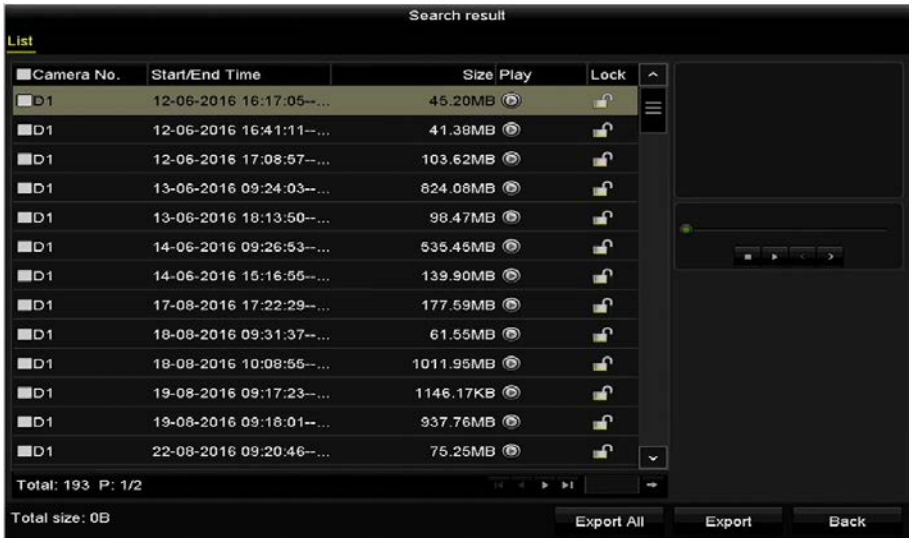


Figure 7-2 Result of Normal Video Search for Backup

7. Export the video files or picture files.

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

NOTE

If the inserted USB device is not recognized, do the following:

1) Click **Refresh**.

2) Reconnect device.

3) Check for compatibility from vendor.

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

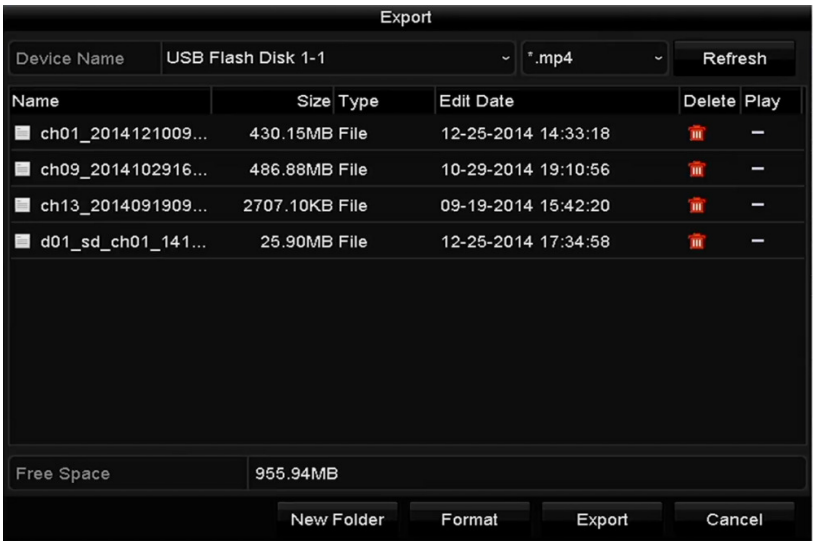


Figure 7-3 Export by Normal Video Search using USB Flash Drive

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

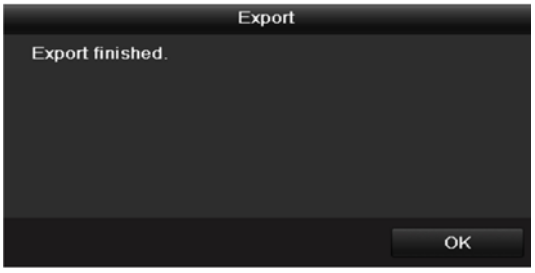


Figure 7-4 Export Finished

NOTE

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

7.1.2 Backing up by Event Search

Purpose:

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

1. Go to **Menu > Export > Event**.

2. Select the cameras to search.

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

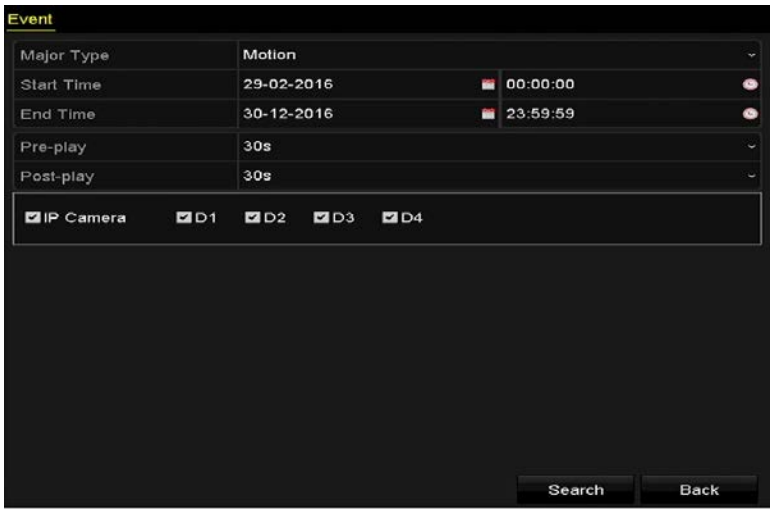


Figure 7-5 Event Search for Backup

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

5. Select video files from the chart or list interface to export.

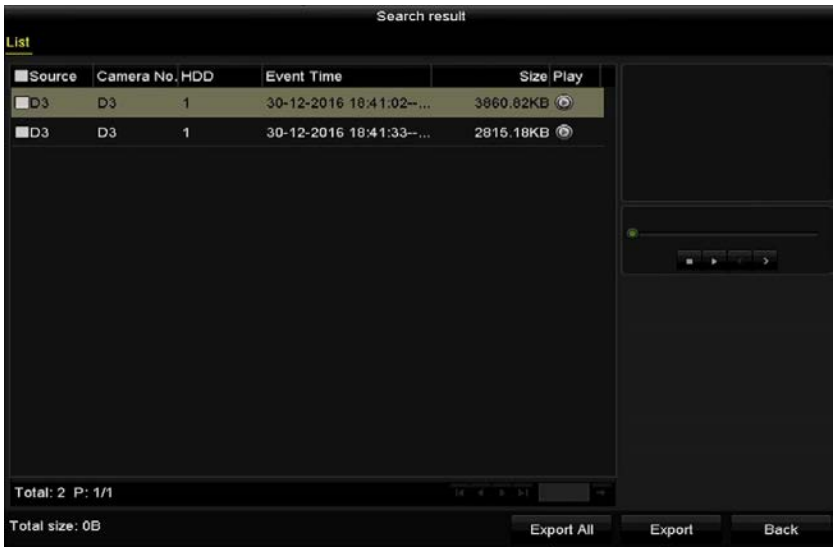


Figure 7-6 Result of Event Search

6. Export the video files. Refer to step 5 of Chapter 7.1.1 Backing up by Normal Video Search for details.

7.1.3 Backing Up Video Clips

Purpose:

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

1. Enter the Playback interface (refer to Chapter 6.1 Playing Back Record Files).
2. During playback, use the or buttons in the playback toolbar to start or stop clipping record file(s).
3. Click to enter the file management interface.



Figure 7-7 Video Clips Export Interface

4. Export the video clips in playback. Refer to step 5 of Chapter 7.1.1 Backing up by Normal Video Search.

7.2 Managing Backup Devices

Manage USB flash drives, USB HDDs, and eSATA HDDs.

1. Enter the Export interface.



Figure 7-8 Storage Device Management

2. Backup device management.

   1) Click **New Folder** to create a new folder in the backup device.

   2) Select a record file or folder in the backup device, and click the button to delete it.

   3) Click **Erase** to erase the files from a re-writable CD/DVD.

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

NOTE

If the inserted storage device is not recognized:

1) Click **Refresh**.

2) Reconnect device.

3) Check for compatibility from vendor.

Chapter 8 Alarm Settings

8.1 Setting Motion Detection Alarm

1. Go to **Menu** > **Camera** > **Motion** to enter the Camera Management Motion Detection interface and choose a camera for which to set up motion detection.

2. Set up detection area and sensitivity.

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

   NOTE

   By default, motion detection is enabled and configured to full screen.

   2) Click  and set alarm response actions.



Figure 8-1 Motion Detection Setup Interface

NOTE

By default, **Dynamic Analysis for Motion** is enabled. When the motion is detected, a green frame identifying moving targets in the motion detection area will be displayed on the live video.

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

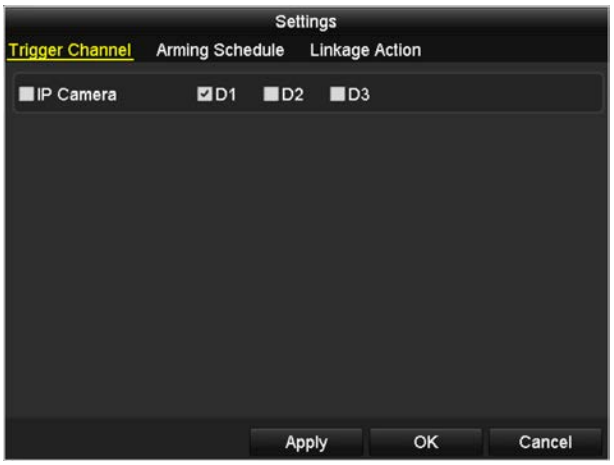


Figure 8-2 Set Trigger Camera of Motion Detection

4. Set up the channel's arming schedule.

   - Select the Arming Schedule tab to set the handling actions arming schedule for the motion detection.
   - Choose a day of the week (up to eight time periods can be set within each day).
   - Click **Apply** to save the settings

   NOTE

   Time periods cannot repeat or overlap.

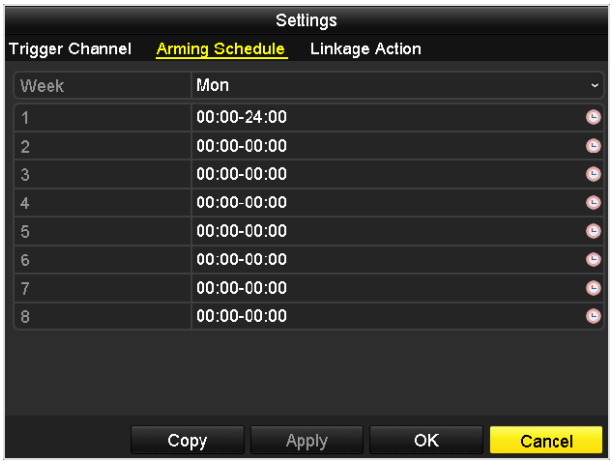


Figure 8-3 Set Arming Schedule of Motion Detection

5. Click **Handling** to set up alarm response actions of motion alarm (refer to *Chapter 8.8 Setting Alarm Response Actions*).

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

8.2 Setting Sensor Alarms

NOTE

Setting sensor alarms are possible only if using cameras with alarm inputs/outputs.

Purpose:

Set the handling action of an external sensor alarm.

1. Go to **Menu > Configuration > Alarm**.
2. Select the Alarm Input tab to enter the Alarm Input Settings interface.

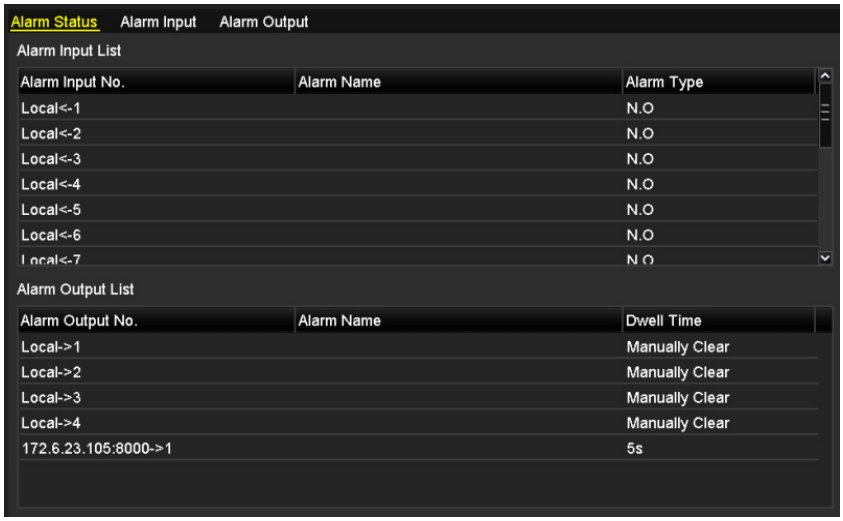


Figure 8-4 Alarm Status Interface of System Configuration

3. Set up the handling action of the selected alarm input.
   1) Check **Enable** and click **Setting** to set up its alarm response actions.



Figure 8-5 Alarm Input Setup Interface

4. (Optional) Enable the one-key disarming for local alarm input 1 (Local <- 1).
   1) Check **Enable One-Key Disarming**.
   2) Click **Settings** to enter the linkage action settings interface.

3) Select the alarm linkage action(s) you want to disarm for local alarm input 1. The selected linkage actions include Full Screen Monitoring, Audible Warning, Notify Surveillance Center, Send Email, and Trigger Alarm Output.

NOTE

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

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

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

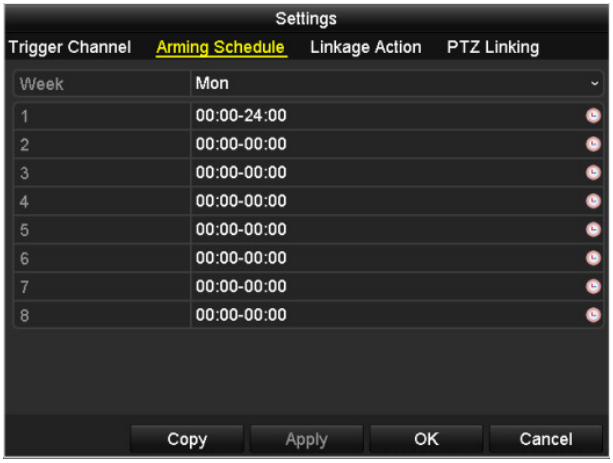


Figure 8-6 Set Arming Schedule of Alarm Input

7. Choose a day of the week (a maximum of eight time periods can be set within each day), and click **Apply** to save the settings.

NOTE

Time periods cannot repeat or overlap.

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

8. Select **Linkage Action** to set up alarm response actions of the alarm input (refer to *Chapter 8.8 Setting Alarm Response Actions*).

9. If necessary, select the PTZ Linking tab and set the PTZ linkage of the alarm input.

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

NOTE

Check whether the PTZ or speed dome supports PTZ linkage.

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

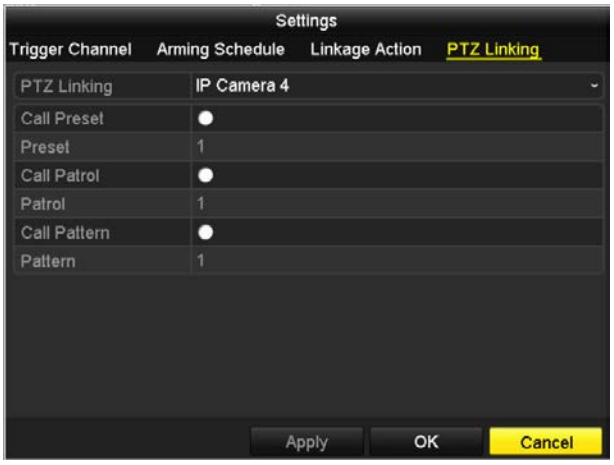


Figure 8-7 Set PTZ Linking of Alarm Input

11. To set the handling action of another alarm input, repeat the above steps, or you can click the **Copy** button on the Alarm Input Setup interface and check the checkbox of alarm inputs to copy the settings to them.



Figure 8-8 Copy Settings of Alarm Input

8.3 Detecting Video Loss Alarm

Purpose:

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

1. Go to **Menu** > **Camera** > **Video Loss** to enter the Camera Management Video Loss interface, and select a channel you want to detect.

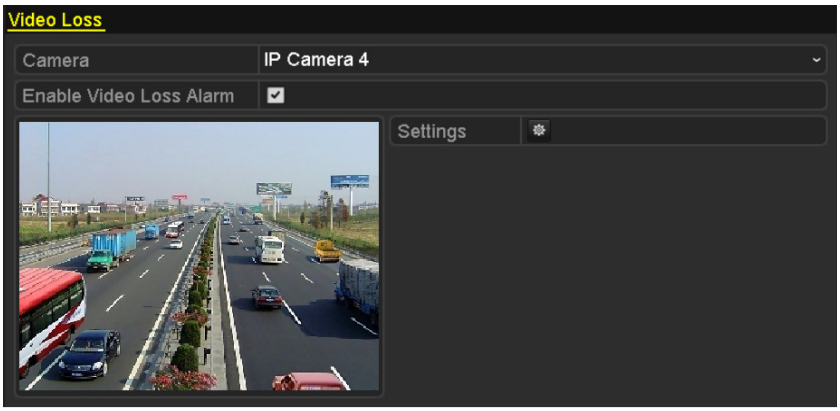


Figure 8-9 Video Loss Setup Interface

2. Set up handling action of video loss.

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

3. Set up the arming schedule of the handling actions.

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

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

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

NOTE

Time periods cannot repeat or overlap.

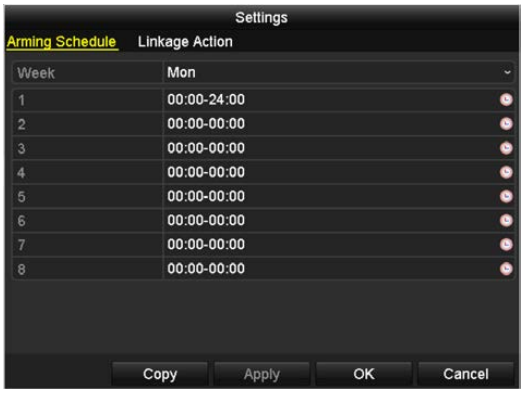


Figure 8-10 Set Arming Schedule of Video Loss

4. Select **Linkage Action** to set up alarm response action of video loss (refer to *Chapter 8.8 Setting Alarm Response Actions*).

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

8.4 Detecting Video Tampering Alarm

Purpose:

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

1. Go to **Menu** > **Camera** > **Video Tampering** to enter the Video Tampering interface of Camera Management and select a channel for which you want to detect video tampering.

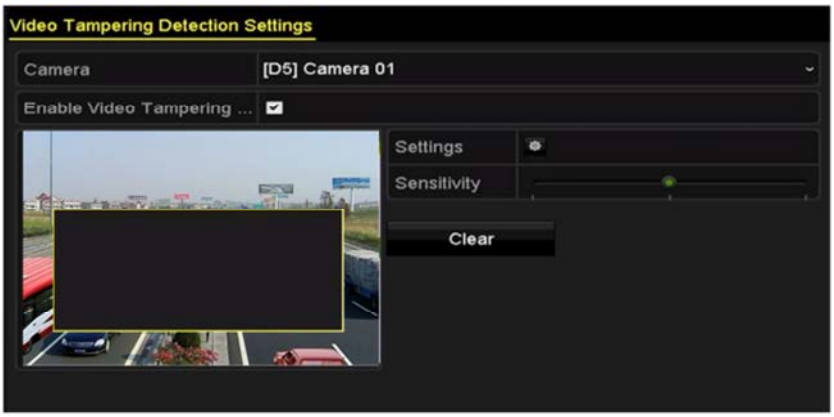


Figure 8-11 Video Tampering Setup Interface

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

   1) Check **Enable Video Tampering Detection**.

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

   3) Click the button to set up handling action of video tampering.

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

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

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

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

NOTE

Time periods cannot repeat or overlap.

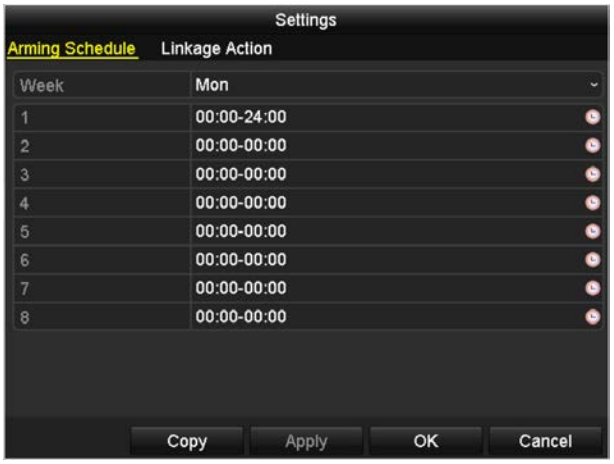


Figure 8-12 Set Arming Schedule of Video Tampering

4. Select **Linkage Action** to set up alarm response actions of video tampering alarm (refer to *Chapter 8.8 Setting Alarm Response Actions*).

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

8.5 Line Crossing Detection Alarm

Purpose:

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

1. Go to **Menu > Camera > VCA**.

2. Select the camera to configure the VCA.

3. Set the VCA detection type to **Line Crossing Detection**.

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

5. Click  to configure the trigger channel, arming schedule, and linkage actions for the line crossing detection alarm.

6. Click the **Rule Settings** button to set the line crossing detection rules.

   - Select the direction to A<->B, A->B or A<-B.
   - **A<->B**: Only the arrow on the B side shows; when an object crosses the configured line in either direction will be detected and alarms triggered.
   - **A->B:** Only an object crossing the configured line from the A side to the B side can be detected.
   - **B->A:** Only an object crossing the configured line from the B side to the A side can be detected.
   - Click-and-drag the slider to set the detection sensitivity.

- **Sensitivity:** Range [1-100]. The higher the value, the more easily the detection alarm is triggered.
- Click **OK** to save the rule settings and return to the line crossing detection settings interface.



Figure 8-13 Set Line Crossing Detection Rules

7. Click and set two points in the preview window to draw a virtual line.
8. Use to clear the existing virtual line and re-draw it.

NOTE

Up to four rules can be configured.

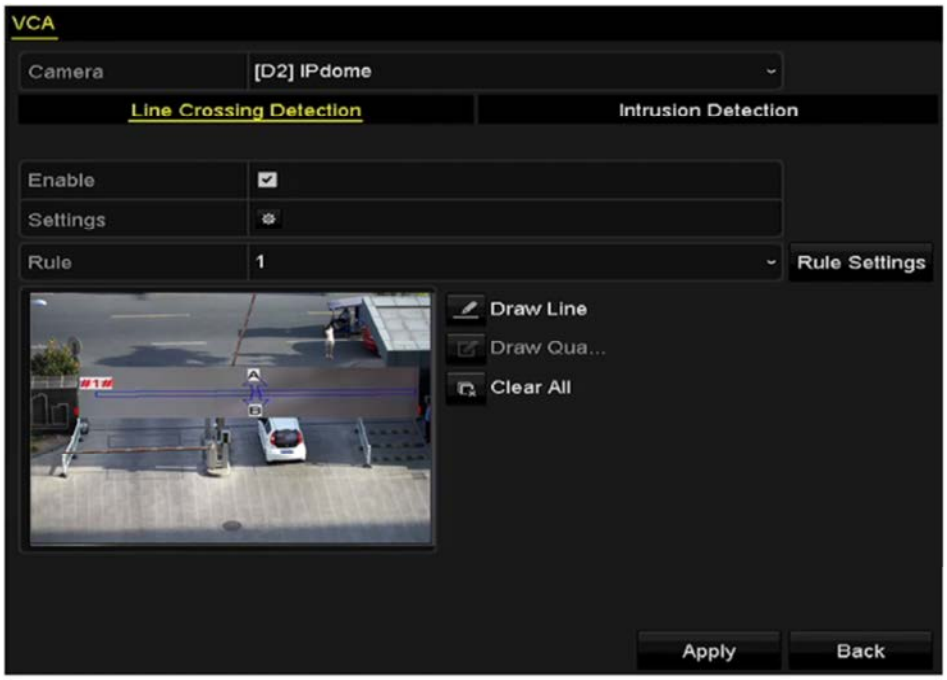


Figure 8-14 Draw Line for Line Crossing Detection

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

8.6 Intrusion Detection Alarm

Purpose:

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

1. Go to **Menu > Camera > VCA**.
2. Select the camera to configure the VCA.
3. Select the VCA detection type to **Intrusion Detection**.
4. Check **Enable** to enable this function.
5. Click  to configure the trigger channel, arming schedule and linkage actions for the line crossing detection alarm.
6. Click the **Rule Settings** button to set the intrusion detection rules. Set the following parameters.
   - **Threshold:** Range [1s-10s], the threshold for the time of the object loitering in the region. When the duration of the object in the defined detection area is longer than the set time, the alarm will be triggered.
   - **Sensitivity:** Range [1-100]. Click-and-drag the slider to set the detection sensitivity. The value defines the size of the object that will trigger the alarm. The higher the value, the more easily the detection alarm can be triggered.
   - **Percentage:** Range [1-100]. Percentage defines the ratio of the in-region part of the object which can trigger the alarm. For example, if the percentage is set as 50 percent, when the object enters the region and occupies half of the whole region, the alarm is triggered.



Figure 8-15 Set Intrusion Crossing Detection Rules

7. Click **OK** to save the rule settings and go back to the line crossing detection settings interface.
8. Click  and draw a quadrilateral in the preview window by specifying four vertexes of the detection region, and right click to complete drawing. Only one region can be configured. You can use the  to clear the existing virtual line and re-draw it.

NOTE

Up to four rules can be configured.

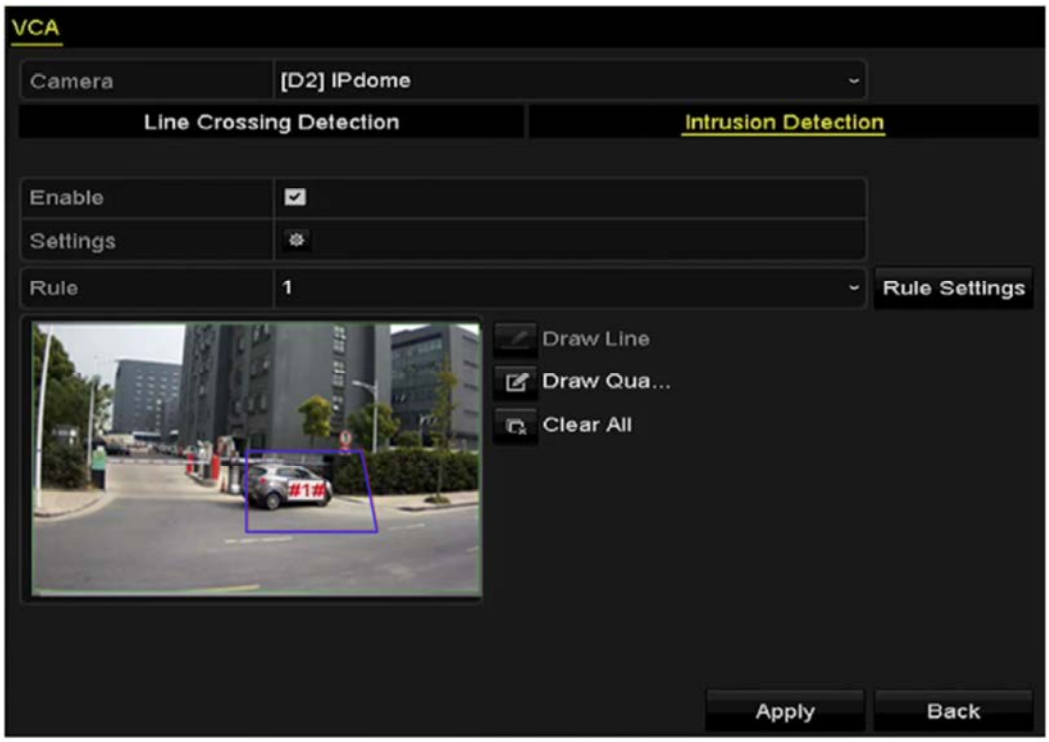


Figure 8-16 Draw Area for Intrusion Detection

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

8.7 Handling Exceptions Alarm

Purpose:

Exception settings refer to the handling action of various exceptions, including the following examples:

- **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

1. Go to **Menu** > **Configuration** > **Exceptions** to enter the System Configuration Exception interface and handle various exceptions (refer to *Chapter 8.8 Setting Alarm Response Actions* for detailed alarm response actions).

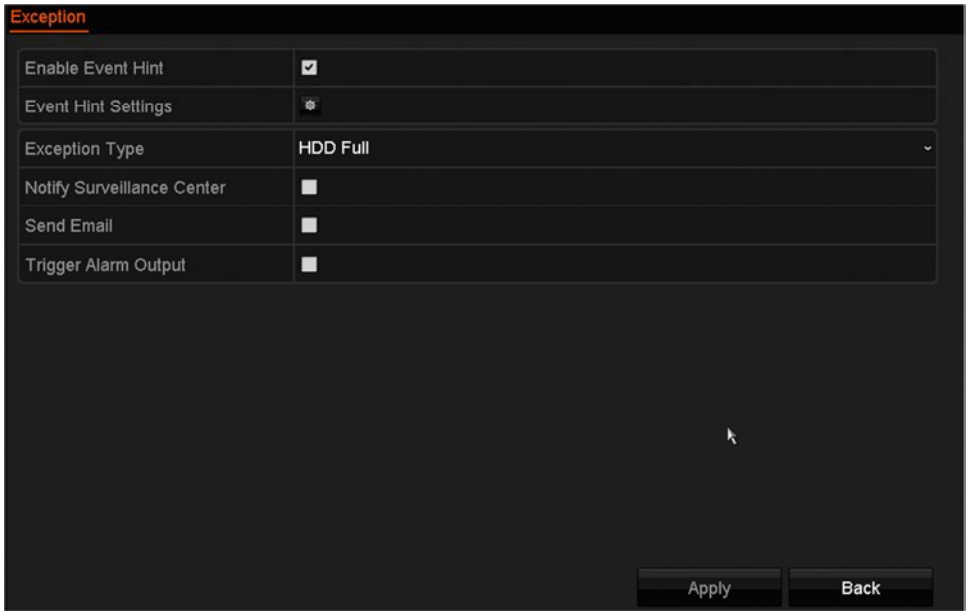


Figure 8-17 Exceptions Setup Interface

8.8 Setting Alarm Response Actions

Purpose:

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

Event Hint Display

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

1. Go to **Menu > Configuration > Exceptions**.

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



Figure 8-18 Event Hint Settings Interface

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

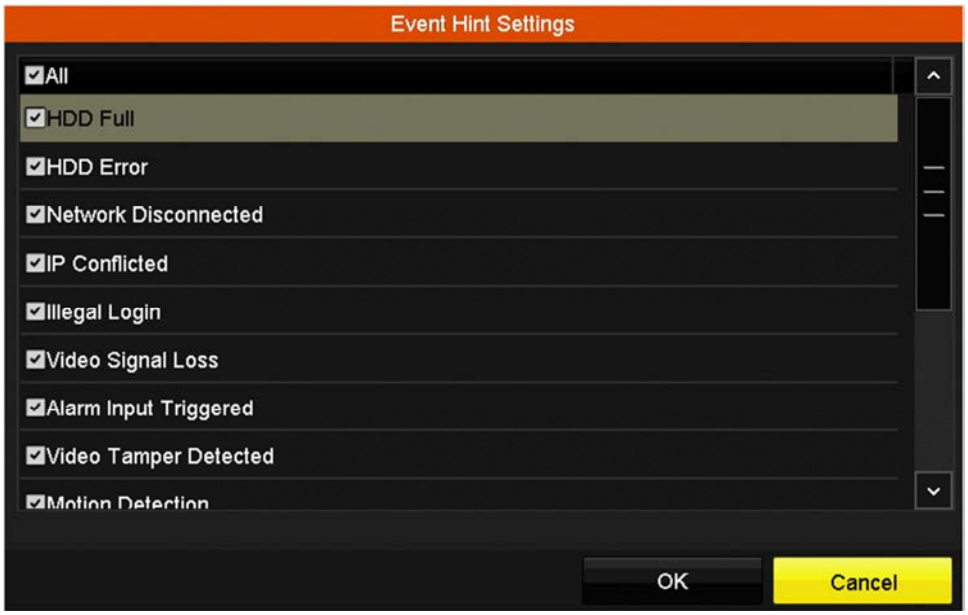


Figure 8-19 Event Hint Settings Interface

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

Full Screen Monitoring

When an alarm is triggered, the local monitor (VGA and HDMI™ monitor) displays in full screen the video image from the alarming channel configured for full screen monitoring.

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

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

NOTE

Select the channel(s) you want to make full screen monitoring in the **Trigger Channel** settings.

Audible Warning

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

Notify Surveillance Center

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

NOTE

The alarm signal will be transmitted automatically at detection mode when the remote alarm host is configured. Refer to *Chapter 11.2.6* Configuring More Settings for details.

E-Mail Linkage

Send an e-mail with alarm information to a user or users when an alarm is detected. Refer to *Chapter* 9.2.5 for e-mail configuration details.

Trigger Alarm Output

Trigger an alarm output when an alarm is triggered.

1. Go to **Menu > Configuration > Alarm > Alarm Output**.

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

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

NOTE

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

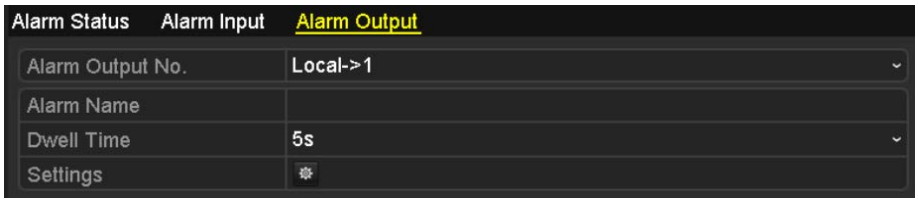


Figure 8-20 Alarm Output Setup Interface

4. Set up arming schedule of the alarm output.

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

NOTE

Time periods cannot repeat or overlap.

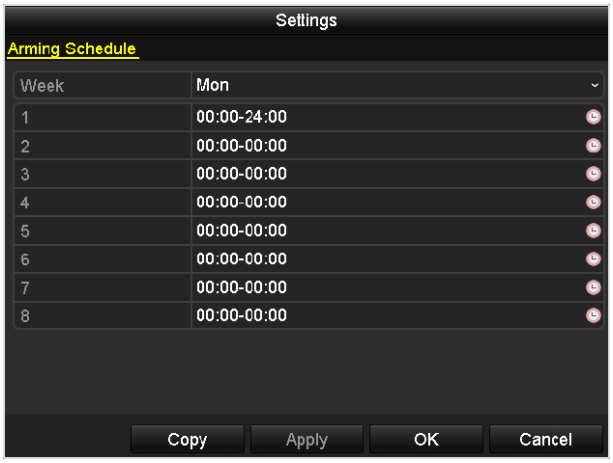


Figure 8-21 Set Arming Schedule of Alarm Output

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

6. Click **OK** to complete the video tampering settings of the alarm output no.

7. You can also copy the above settings to another channel.

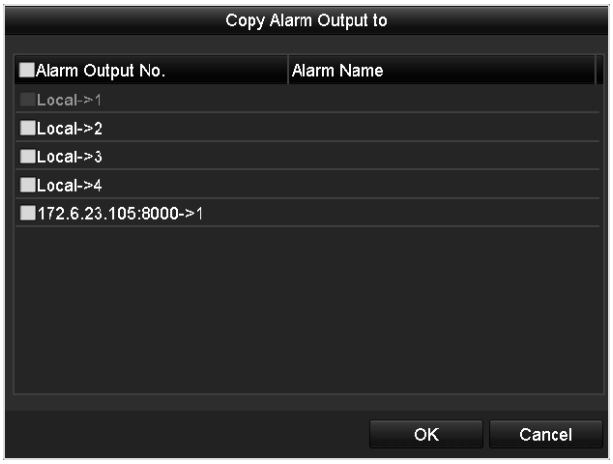


Figure 8-22 Copy Settings of Alarm Output

8.9 Triggering or Clearing Alarm Output Manually

Purpose:

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

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

2. Go to **Menu > Manual > Alarm**.

3. Click **Trigger/Clear** to trigger or clear an alarm output.

4. Click **Trigger All** to trigger all alarm outputs.

5. Click **Clear All** to clear all alarm outputs.

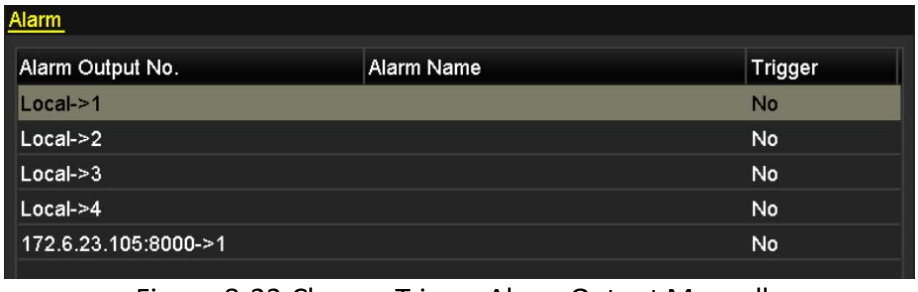


Figure 8-23 Clear or Trigger Alarm Output Manually

Chapter 9 Network Settings

9.1 Configuring General Settings

Purpose:

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

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

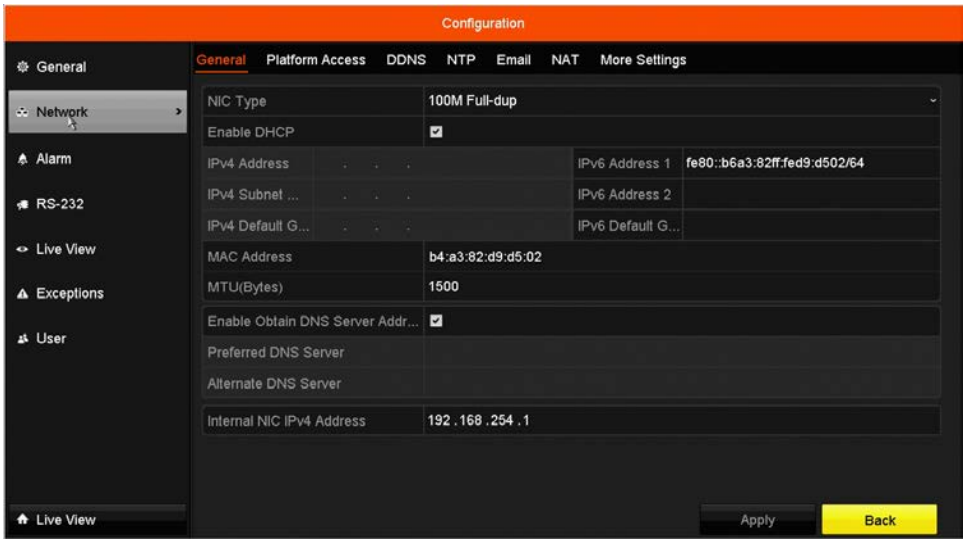


Figure 9-1 Network Settings

2. Configure the following settings: Working Mode, NIC Type, IPv4 Address, IPv4 Gateway, MTU, and DNS Server.

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

NOTE

The internal NIC IPv4 address should be configured for the cameras connecting to the PoE or built-in switch network interface of the NVR.

The valid value range of MTU is 500 to 9676.

4. Click **Apply**.

9.2 Configuring Advanced Settings

9.2.1 Configuring Hik-Connect

Purpose

Hik-Connect enables the mobile phone app and the service platform page (www.hik-connect.com) to access and manage your connected NVR, providing convenient remote access to the surveillance system.

NOTE

Hik-Connect can be enabled via operation on SADP software, the GUI, and a Web browser. We introduce the operation steps on the GUI in this section.

1. Go to **Menu > Configuration > Network > Platform Access**.

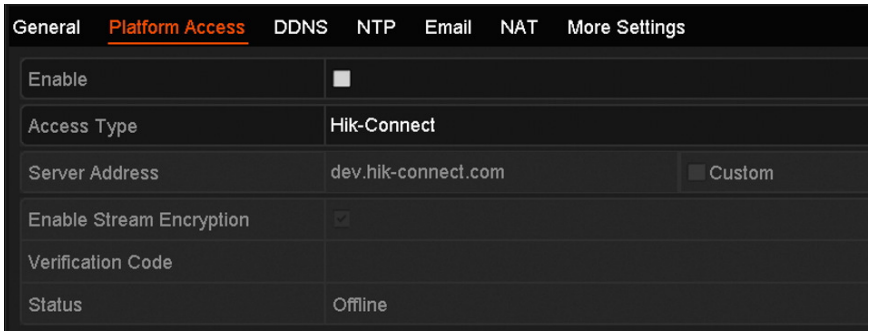


Figure 9-2 Hik-Connect Settings

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

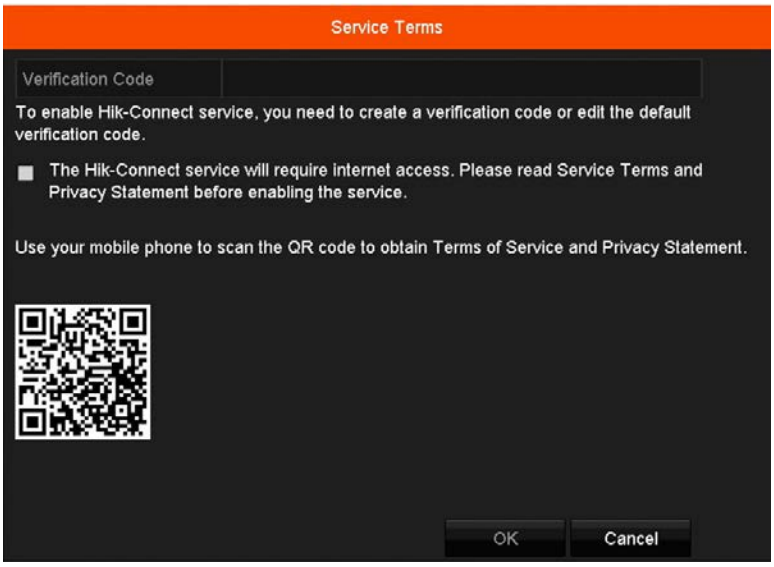


Figure 9-3 Service Terms

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

4. Check the **The Hik-Connect service will require internet access** checkbox**.** Read the Service Terms and Privacy Statement before enabling the service.

5. Scan the QR code on the interface with your mobile phone to read the Service Terms and the Privacy Statement.

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

NOTE

Hik-Connect is disabled by default.

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

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

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

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

8. (Optional) Check **Enable Stream Encryption**. If this feature is enabled, the verification code is required for remote access and live view.

NOTE

Use your phone's scanning tool to quickly get the code by scanning the QR code below.

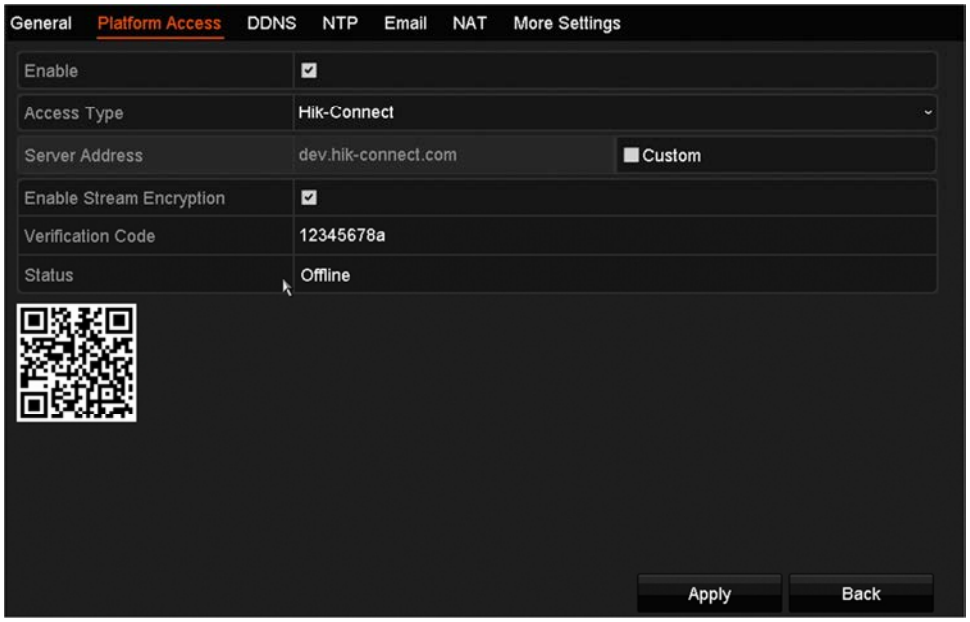


Figure 9-4 Hik-Connect Settings Interface

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

10. After configuration, you can access and manage the DVR with your mobile phone or the Web site (*www.hik-connect.com*).

IOS Users

Scan the QR code below to download the Hik-Connect application for subsequent operations.



Figure 9-5 QR Code for iOS Users

Android Users

Scan the QR code below to download the Hik-Connect application for subsequent operations. You must install *googleplay* on your Android mobile phone to access the address successfully.



Figure 9-6 QR Code for Android Users

NOTE

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

After configuration, you can access and manage the NVR with the mobile phone on which the Hik-Connect app is installed or the Web site (www.hik-connect.com).

NOTE

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

9.2.2 Configuring DDNS

Purpose:

You can set the Dynamic DNS (DDNS) to be used for network access.

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

1. Go to **Menu > Configuration > Network**.

2. Select **DDNS** to enter the DDNS Settings interface.

3. Check **Enable DDNS** to enable this feature.

4. Select **DDNS Type**. Different DDNS types are selectable: DynDNS, PeanutHull, NO-IP.

- **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 Web site.

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

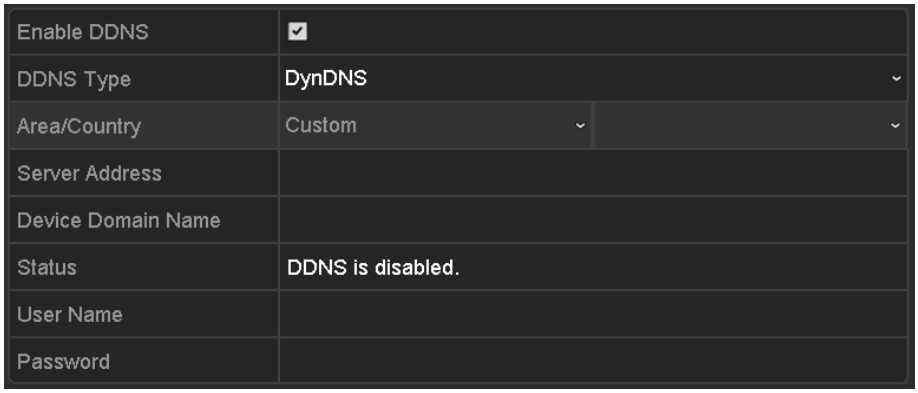


Figure 9-7 DynDNS Settings Interface

- **PeanutHull**

  1) Enter the **User Name** and **Password** obtained from the PeanutHull Web site.

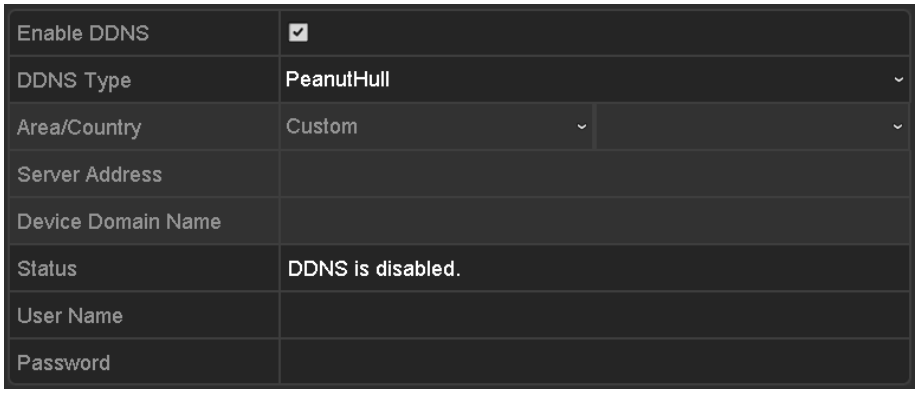


Figure 9-8 PeanutHull Settings Interface

- **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 Web site (www.no-ip.com).

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



Figure 1. 1 NO-IP Settings Interface

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

6. 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 the FTP server) and the device is valid and correct. Run the FTP server on the PC and copy the firmware into the corresponding directory of your PC.

NOTE

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

1. Go to **Menu > Configuration > Network**.

2. Select **NTP** to enter the NTP Settings interface, as shown in Figure 9-9.



Figure 9-9 NTP Settings Interface

3. Check **Enable NTP** 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 **Apply** to save and exit the interface.

NOTE

The time synchronization interval can be set from1 to 10080 min, and the default value is 60 min. If the NVR is connected to a public network, use an NTP server that has a time synchronization function such as the server at the National Time Center (IP Address: 210.72.145.44). If the NVR is set up in a more customized network, NTP software can be used to establish an NTP server for time synchronization.

9.2.4 Configuring More Settings

1. Go to **Menu > Configuration > Network**.

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

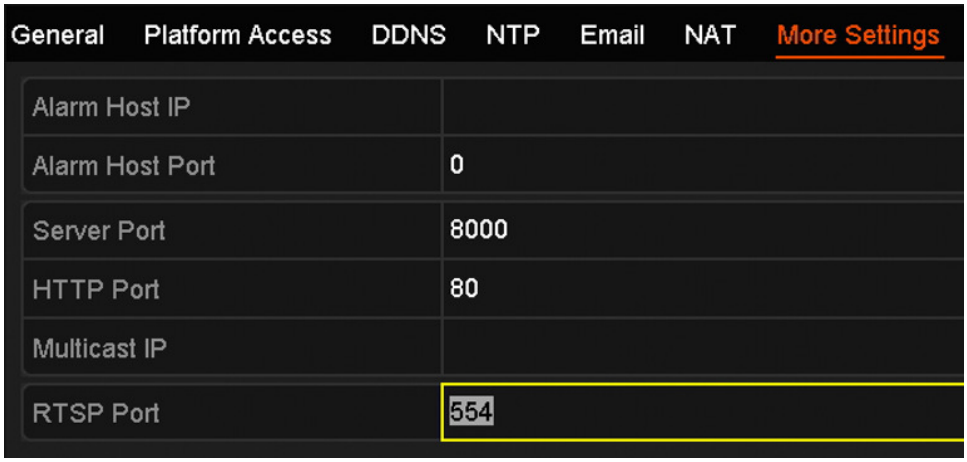


Figure 9-10 More Settings Interface

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

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

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

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

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

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

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

- **Server Port** and **HTTP Port**: Enter the **Server Port** and **HTTP Port** in the text fields. The default Server Port is 8000 and the HTTP Port is 80, and you can change them according to different requirements.

NOTE

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



Figure 9-11 Configure More Settings

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

9.2.5 Configuring E-Mail

Purpose:

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

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

1. Go to **Menu > Configuration > Network**.

2. Set the IPv4 Address, IPv4 Subnet Mask, IPv4 Gateway, and Preferred DNS Server in Network Settings.

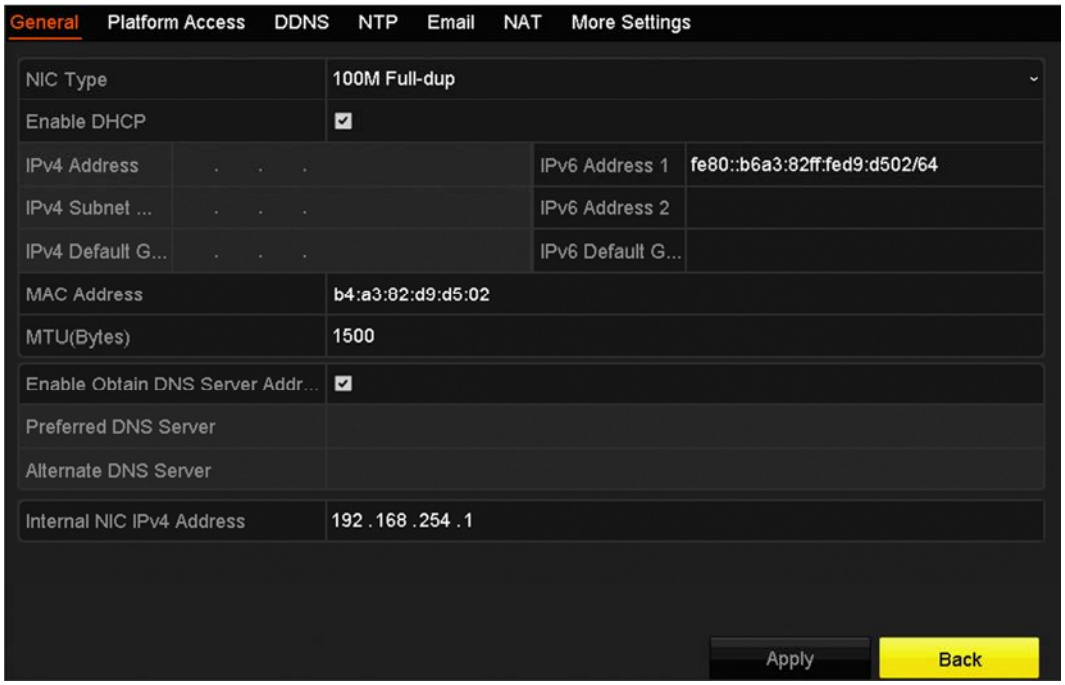


Figure 9-12 Network Settings Interface

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

4. Select the **Email** tab to enter the **Email Settings** interface.

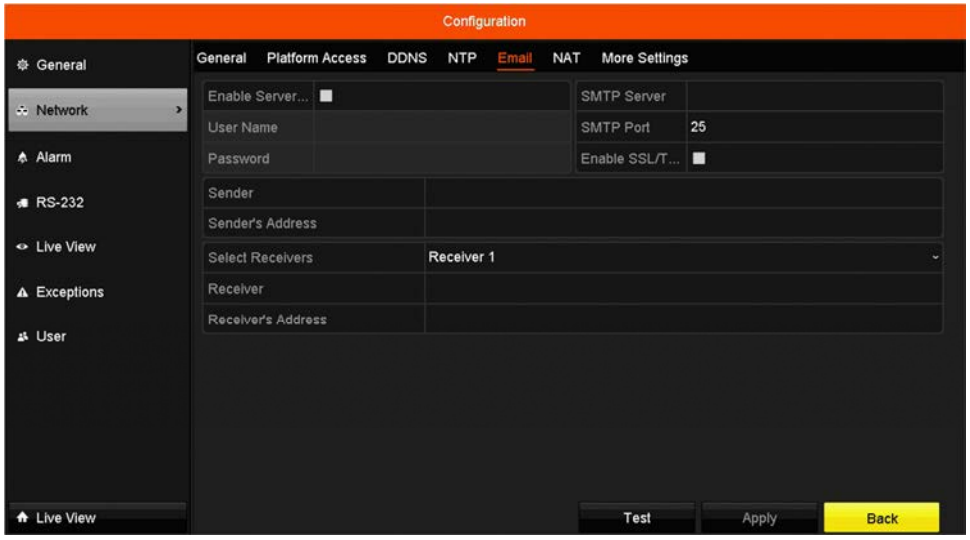


Figure 9-13 E-Mail Settings Interface

5. Configure the following e-mail settings:

   - **Enable Server Authentication (optional):** Check the checkbox to enable the server authentication feature.
   - **User Name**: The user account of sender's e-mail for SMTP server authentication
   - **Password**: The password of sender's e-mail for SMTP server authentication
   - **SMTP Server:** The SMTP Server IP address or host name (e.g., smtp.263xmail.com)
   - **SMTP Port No.:** The SMTP port. The default TCP/IP port used for SMTP is 25.
   - **Enable SSL/TLS (optional):** Check the checkbox to enable SSL/TLS if required by the SMTP server.
   - **Sender:** The name of sender
   - **Sender's Address:** The e-mail address of sender
   - **Select Receivers:** Select the receiver. Up to three receivers can be configured.
   - **Receiver:** The name of user to be notified
   - **Receiver's Address:** The e-mail address of the user to be notified
   - **Test:** Send a test message to verify that the SMTP server can be reached.

6. Click **Apply** to save the e-mail settings.

7. Click **Test** to check your e-mail settings. The corresponding Attention message box will pop up.

9.2.6 Configuring NAT

Purpose:

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

- **UPnP™**
  Universal Plug and Play (UPnP™) can permit the device to seamlessly discover the presence of other 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:

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

  1. Go to **Menu > Configuration > Network**.

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

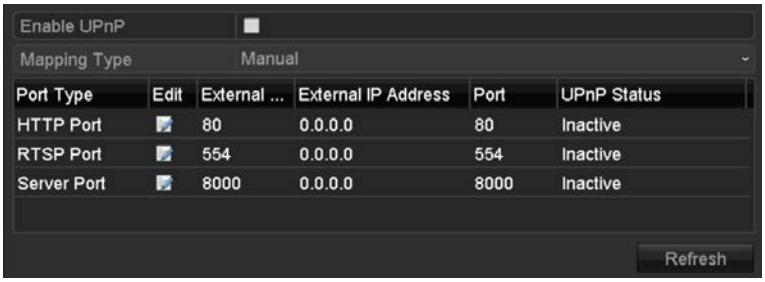


Figure 9-14 UPnP™ Settings Interface

  3. Check ☑ checkbox to enable UPnP™.

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

     - **OPTION 1: Auto**

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

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

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

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

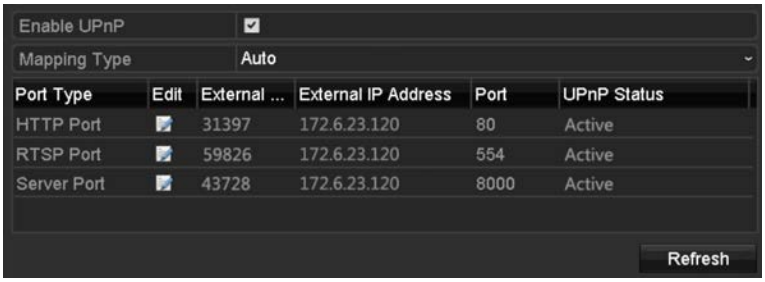


Figure 9-15 UPnP™ Settings Finished-Auto

- **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.

  1. Select **Manual** in the **Mapping Type** drop-down list.
  2. Click to activate the External Port Settings dialog box. Configure the external port no. for server port, http port, RTSP port, and https port respectively.

NOTE

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

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

The value of the RTSP port no. should be 554 or between 1024 and 65535, while the value of the other ports should be between 1 and 65535 and the values must differ 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 9-16 External Port Settings Dialog Box

3. Click **Apply** to save the settings.
4. Click **Refresh** to get the latest port mapping status.

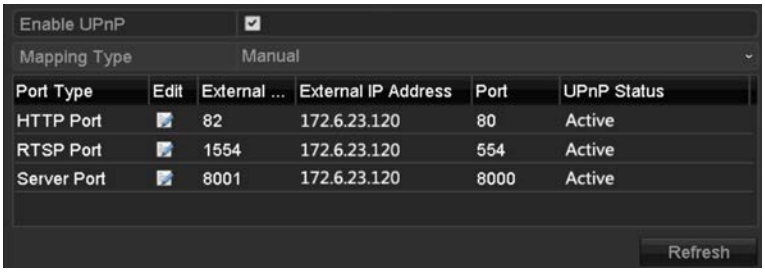


Figure 9-17 UPnP™ Settings Finished-Manual

- **Manual Mapping**

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

  Before You Start:

  Make sure the router supports configuring the internal port and external port in the Forwarding interface.

  1. Go to **Menu > Configuration > Network**.

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

3. Leave the **Enable UPnP** checkbox unchecked.

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

NOTE

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

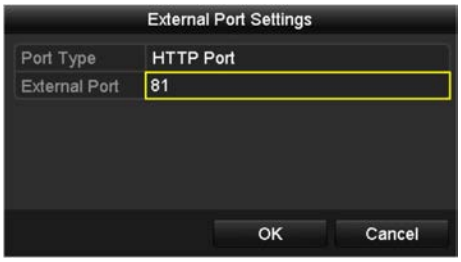


Figure 9-18 External Port Settings Dialog Box

5. Click **OK** to save the setting for the current port and return to the upper-level menu.

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

7. Enter the virtual server setting page of the router; fill in the blank of the Internal Source Port with the internal port value, the blank of the External Source Port with the external port value, and other required contents.

NOTE

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

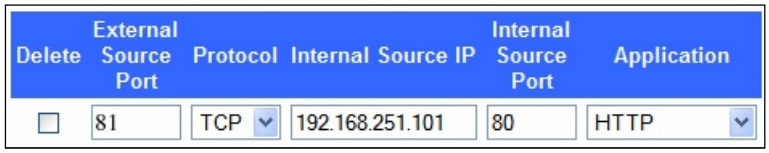


Figure 9-19 Setting Virtual Server Item

NOTE

The above virtual server setting interface is for reference only and may be different due to different router manufacturers. Contact the router manufacturer if you have any problems setting a virtual server.

9.2.7 Checking Network Traffic

Purpose:

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

1. Go to **Menu > Maintenance > Net Detect**.

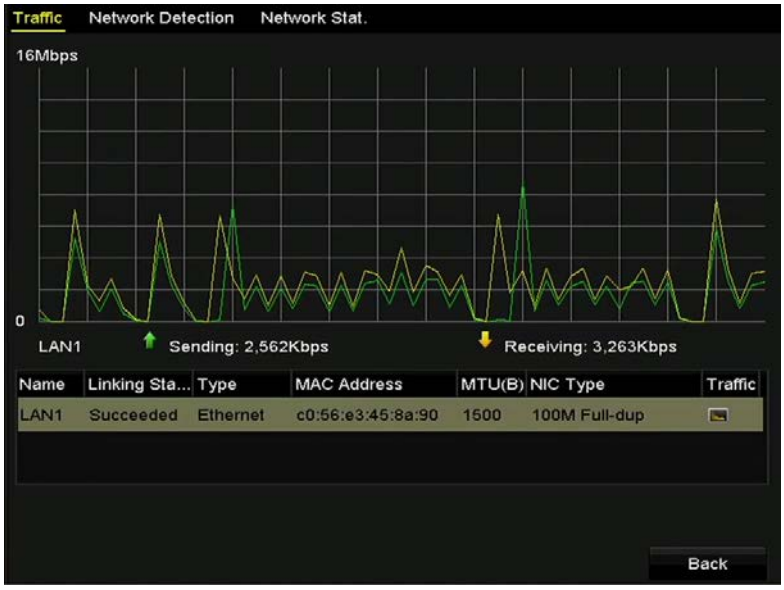


Figure 9-20 Network Traffic Interface

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

9.3 Configuring Network Detection

Purpose:

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

9.3.1 Testing Network Delay and Packet Loss

1. Go to **Menu > Maintenance > Net Detect**.

2. Click the **Network Detection** tab to enter the Network Detection menu, as shown in Figure 9-21.

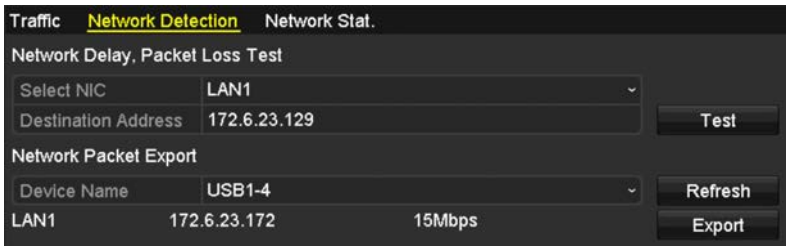


Figure 9-21 Network Detection Interface

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

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

9.3.2 Exporting Network Packet

Purpose:

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

1. Go to **Menu > Maintenance > Net Detect**.

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

3. Select the backup device from the **Device Name** drop-down list, as shown in Figure 9-22.

NOTE

Click **Refresh** if the connected local backup device is not displayed. If the backup device cannot be detected, check whether it is compatible with the NVR. Format the backup device if the format is incorrect.

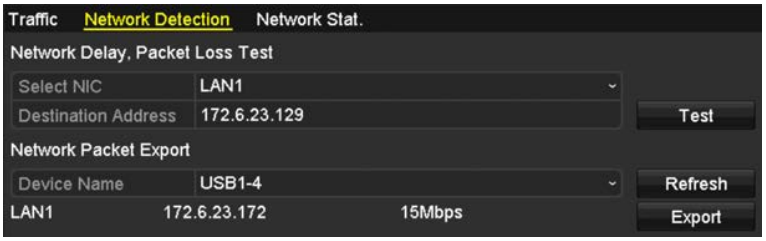


Figure 9-22 Export Network Packet

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

5. After exporting is complete, click **OK** to finish the packet export, as shown in Figure 9-23.



Figure 9-23 Packet Export Attention

NOTE

Up to 1 MB of data can be exported each time.

9.3.3 Checking the Network Status

Purpose:

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

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

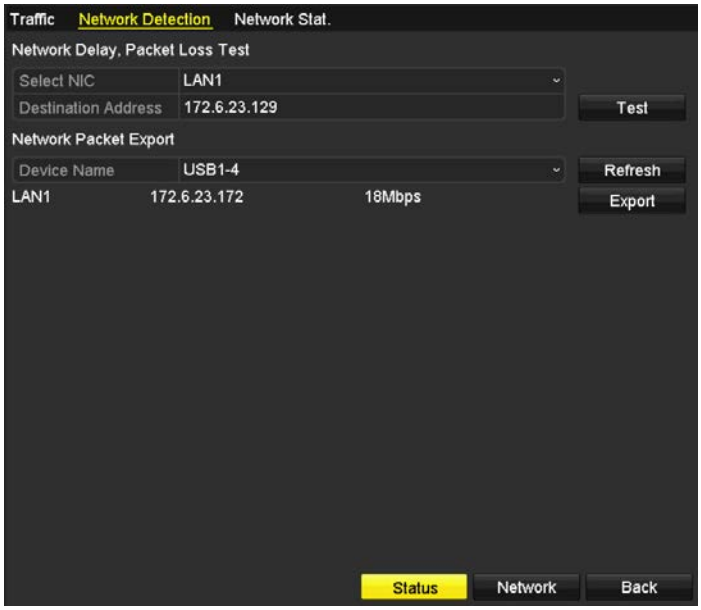


Figure 9-24 Network Status Checking

2. If the network is normal, the following message box appears.



Figure 9-25 Network status checking result

3. If the message box appears with other information instead of this one, click **Network** to show the quick setting interface of the network parameters.

9.3.4 Checking Network Statistics

Purpose:

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

1. Go to **Menu > Maintenance > Net Detect**.

2. Choose **Network Stat**.

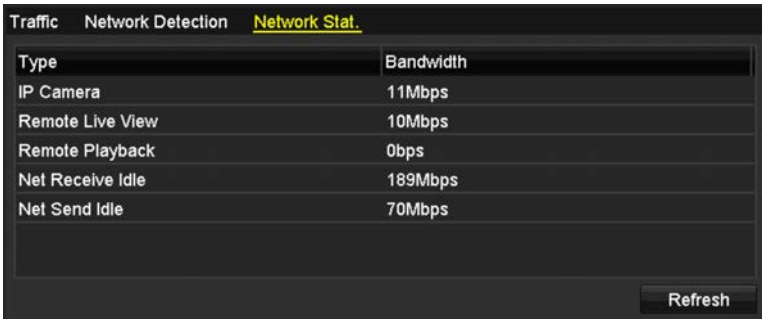


Figure 9-26 Network Stat. Interface

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

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

Chapter 10 HDD Management

10.1 Initializing HDDs

Purpose:

A newly installed hard disk drive (HDD) must be initialized before use.

Option 1: Initialize HDD from the Startup Wizard

When the device starts up, the Setup Wizard can guide you to configure basic settings.

In the General settings interface, check **Initialize HDD** to initialize the HDD when it is used for the first time.

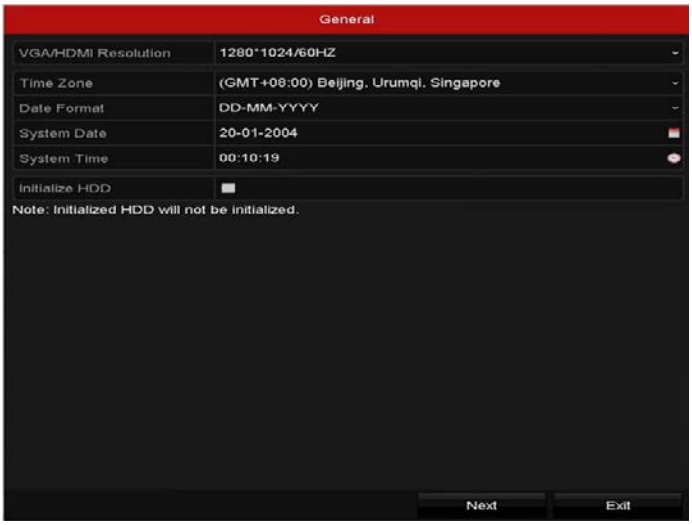


Figure 10-1 Initialize HDD

Option 2: Initialize HDD from the HDD Management Interface

1. Go to **Menu > HDD > General**.

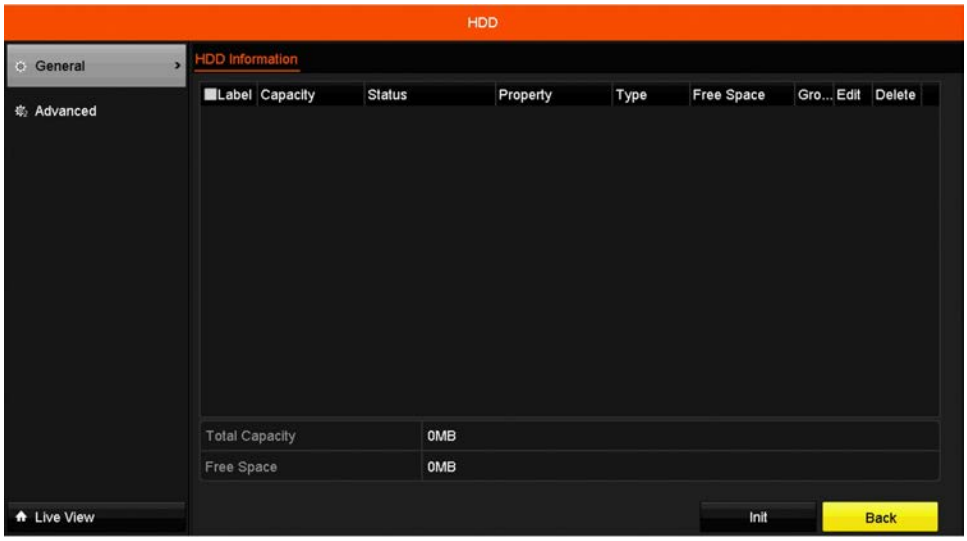


Figure 10-2 HDD Information Interface

2. Select the HDD to be initialized.

3. Click **Init**.



Figure 10-3 Confirm Initialization

4. Click **OK** to start initialization.

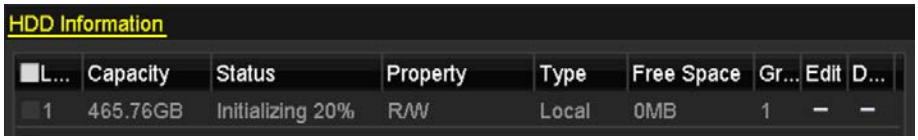


Figure 10-4 Status changes to Initializing

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



Figure 10-5 HDD Status Changes to Normal

NOTE

Initializing the HDD will erase all data on it.

10.2 Configuring Quota Mode

Purpose:

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

1. Go to **Menu > HDD > Advanced**.

2. Set **Mode** to Quota, as shown in Figure 10-6.

NOTE

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



Figure 10-6 Storage Mode Settings Interface

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

4. Enter the storage capacity in the **Max. Record Capacity (GB)** text fields.

5. Copy the quota settings of the current camera to other cameras if desired. Click **Copy** to enter the Copy Camera menu, as shown in Figure 10-7.



Figure 10-7 Copy Settings to Other Camera(s)

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

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

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

NOTE

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

10.3 HDD Detection

Purpose:

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

S.M.A.R.T. Settings

1. Go to **Menu > Maintenance > HDD Detect**.

2. Select the HDD to view its S.M.A.R.T. information list, as shown in Figure 10-8.

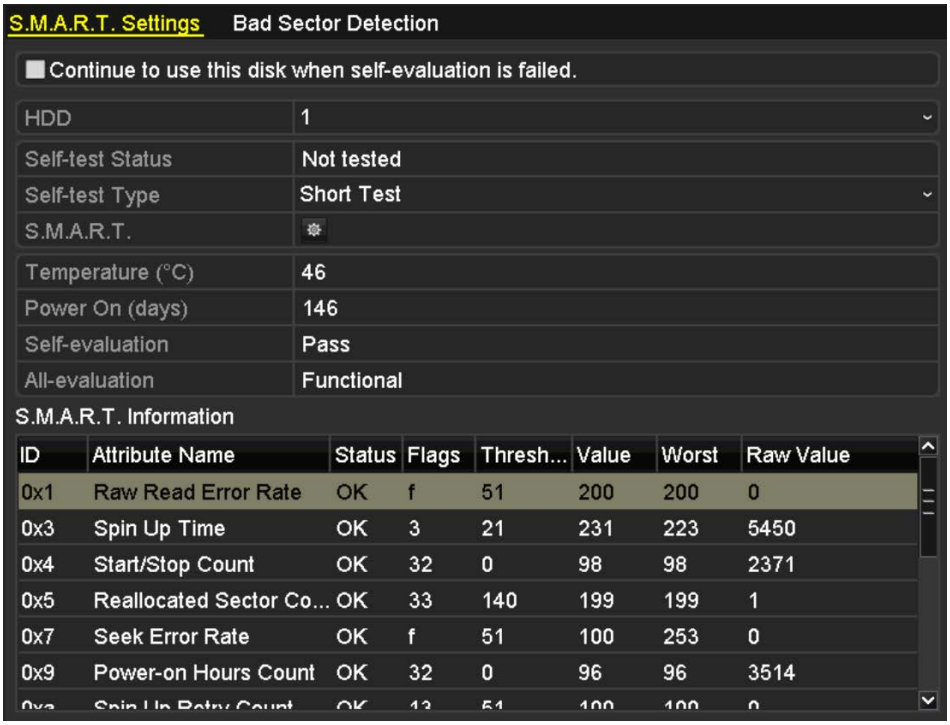


Figure 10-8 S.M.A.R.T Settings Interface

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

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

5. Click **Start** to start the S.M.A.R.T. HDD self-evaluation.



NOTE

To use the HDD even when S.M.A.R.T. checking has failed, check the **Continue to use the disk when self-evaluation is failed** checkbox.

Bad Sector Detection

1. Click **Bad Sector Detection**.

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

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

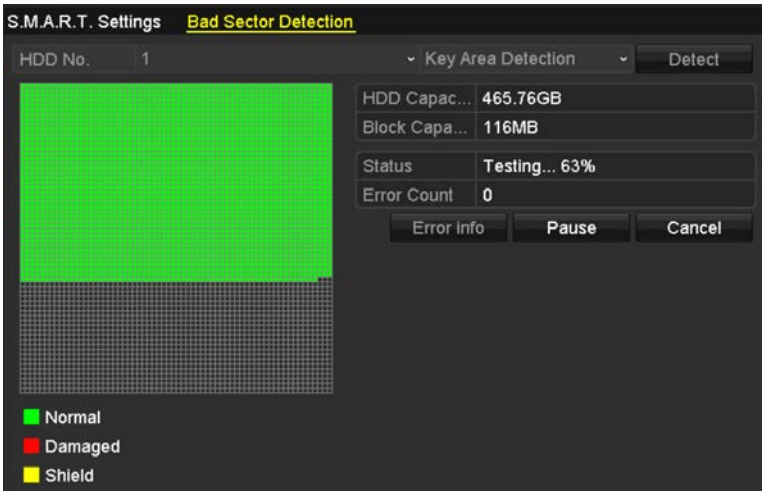


Figure 10-9 Bad Sector Detection

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

5. You can also pause/resume or cancel the detection as desired.

10.4 Configuring HDD Error Alarms

Purpose:

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

1. Go to **Menu > Configuration > Exceptions**.

2. Set the **Exception Type** to **HDD Error** on the drop-down list.

3. Click the checkbox(s) to select the HDD error alarm type(s), as shown in Figure 10-10.

NOTE

The alarm type can be set to: Audible Warning, Notify Surveillance Center, Send Email, and Trigger Alarm Output. Refer to *Chapter 8.8 Setting Alarm Response Actions*.

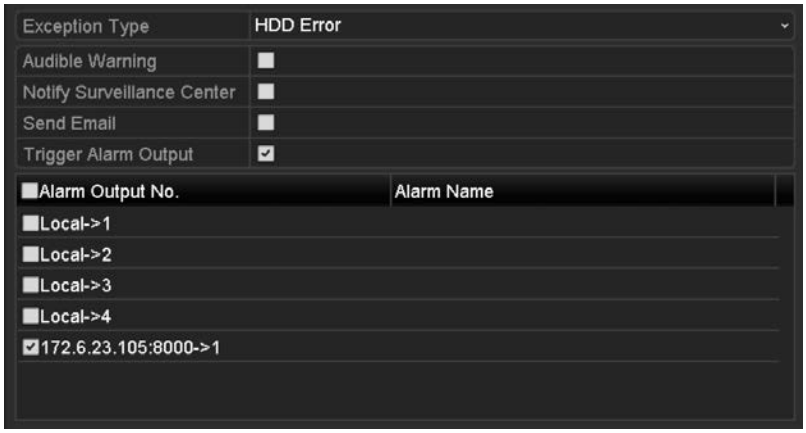


Figure 10-10 Configure HDD Error Alarm

4. When **Trigger Alarm Output** is selected, you can also select the alarm output to be triggered from the list below.

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

Chapter 11 Camera Settings

11.1 Configuring OSD Settings

Purpose:

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

1. Go to **Menu > Camera > OSD**.
2. Select the camera for which to configure OSD settings.
3. Edit the Camera Name in the text field.
4. Configure the Display Name, Display Date, and Display Week by clicking the checkbox.
5. Select the Date Format, Time Format, and Display Mode.

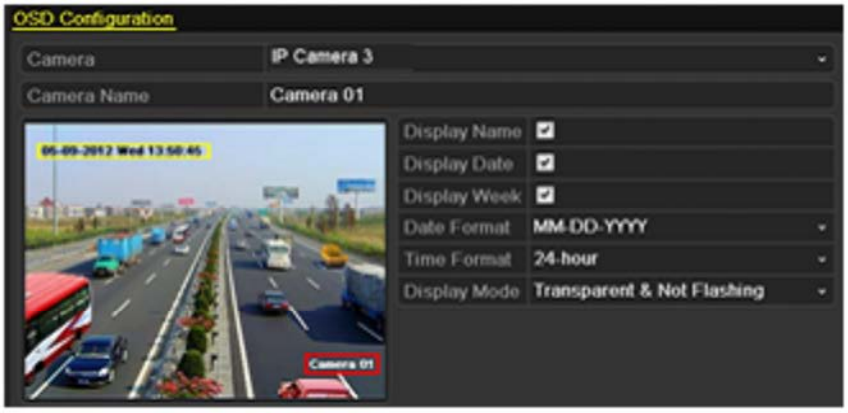


Figure 11-1 OSD Configuration Interface

6. Use the mouse to click-and-drag the text frame on the preview window to adjust the OSD position.
7. Click **Apply** to apply the settings.

11.2 Configuring Privacy Mask

Purpose:

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

1. Go to **Menu > Camera > Privacy Mask**.
2. Select the camera for which to set privacy mask.
3. Click the **Enable Privacy Mask** checkbox 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 in different frame colors.

NOTE

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

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



Figure 11-3 Set Privacy Mask Area

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

11.3 Configuring Video Parameters

Purpose:

You can customize the image parameters including brightness, contrast, saturation, image rotate, and mirror for live view and recording effect.

1. Go to **Menu > Camera > Image**.

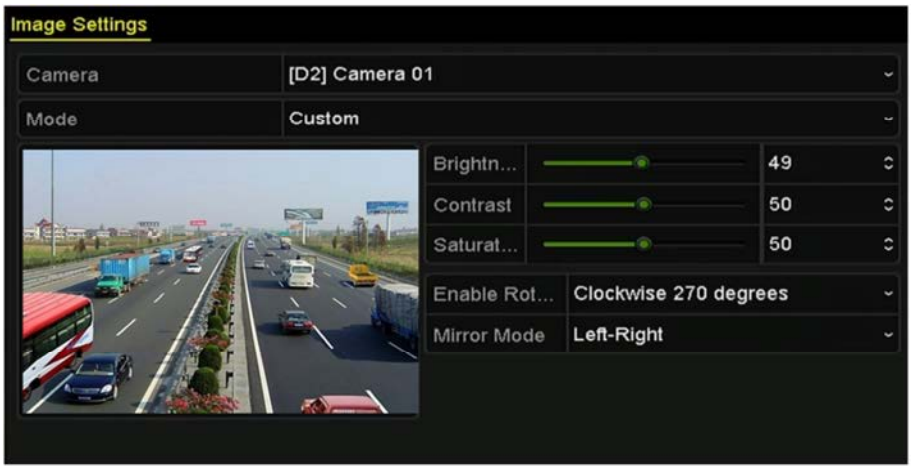


Figure 11-4 Image Settings Interface

2. Select the camera for which to set image parameters.
3. Adjust the slider or click on the up/down arrow to set the brightness, contrast, or saturation value.
4. Set the **Enable Rotate** function to **Clockwise 270 degrees** or **OFF**. If **OFF** is selected, the image is restored to original.
5. Set the **Mirror Mode** to **Left-Right**, **Up-Down**, **Center**, or **OFF**. If **OFF** is selected, the image is restored to original.

NOTE

The Rotate and Mirror functions must be supported by the connected IP camera.

The image parameters adjustment can affect both the live view and the recording quality.

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

Chapter 12 Device Management and Maintenance

12.1 Viewing System Information

1. Go to **Menu > Maintenance > System Info**.
2. Click the **Device Info**, **Camera**, **Record**, **Alarm**, **Network,** and **HDD** tabs to view the device information.

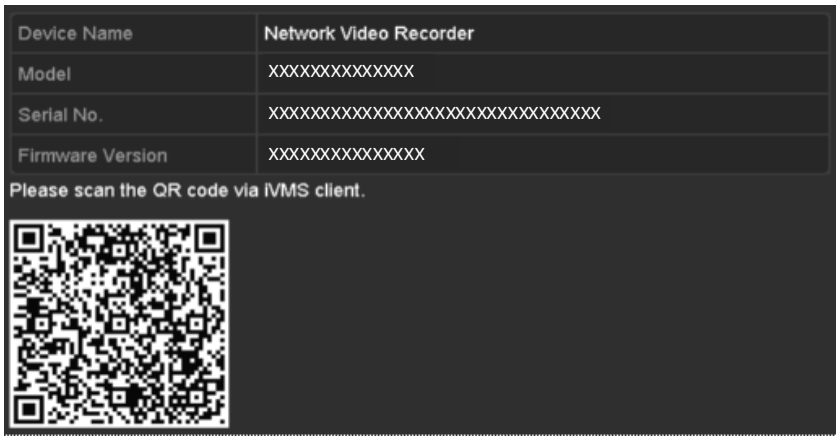


Figure 12-1 Device Information Interface

12.2 Searching and Exporting Log Files

Purpose:

Store the NVR's operation, alarm, exception, and information in log files that can be viewed or exported.

1. Go to **Menu > Maintenance > Log Information**.

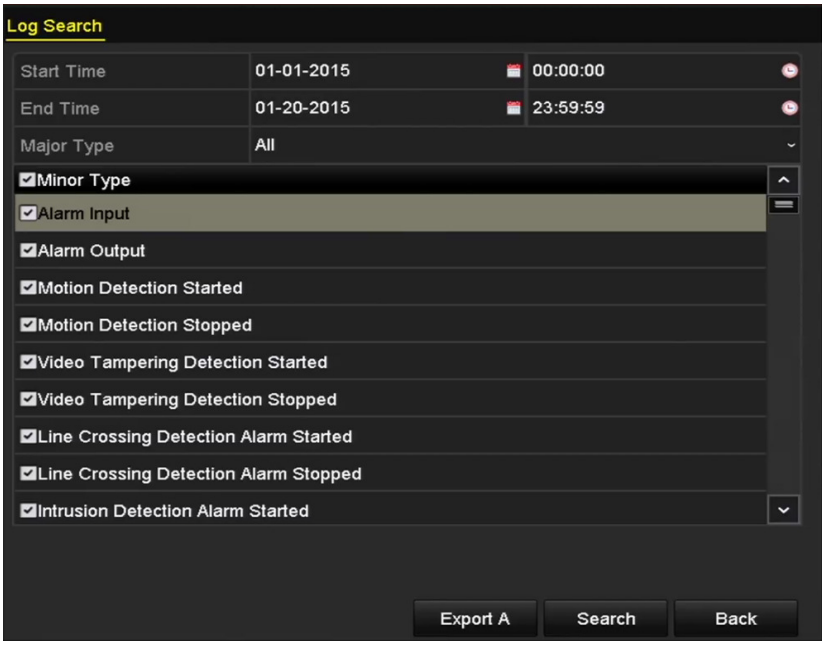


Figure 12-2 Log Search Interface

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

3. Click **Search** to start searching log files.

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



Figure 12-3 Log Search Results

NOTE

Up to 2,000 log files can be displayed each time.

5. Click the button of each log or double-click it to view its detailed information, as shown in Figure 12-4. You can click the button to view the related video files if available.

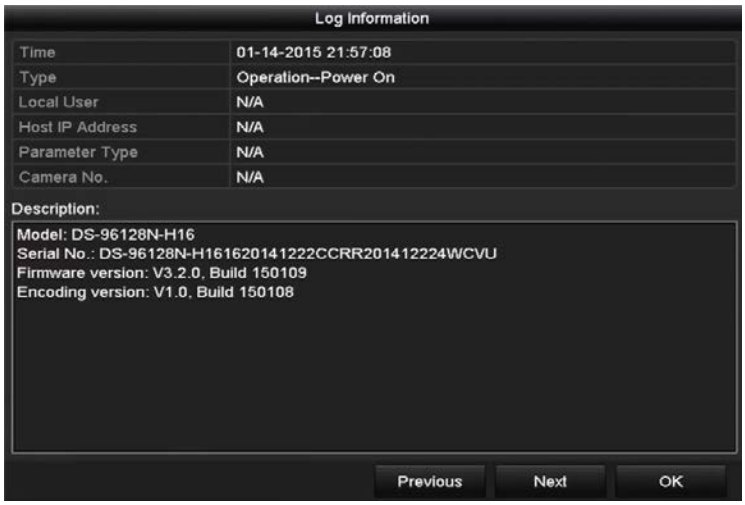


Figure 12-4 Log Details

6. To export the log files, click **Export** on the Search Result interface to enter the Export menu (Figure 12-5).



Figure 12-5 Export Log Files

7. Select the backup device from **Device Name**.

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

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

NOTE

Click **New Folder** to create a new folder in the backup device, or click **Format** to format the backup device before log export.

NOTE

Connect the backup device to the NVR before operating log export.

12.3 Importing/Exporting Configuration Files

Purpose:

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

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

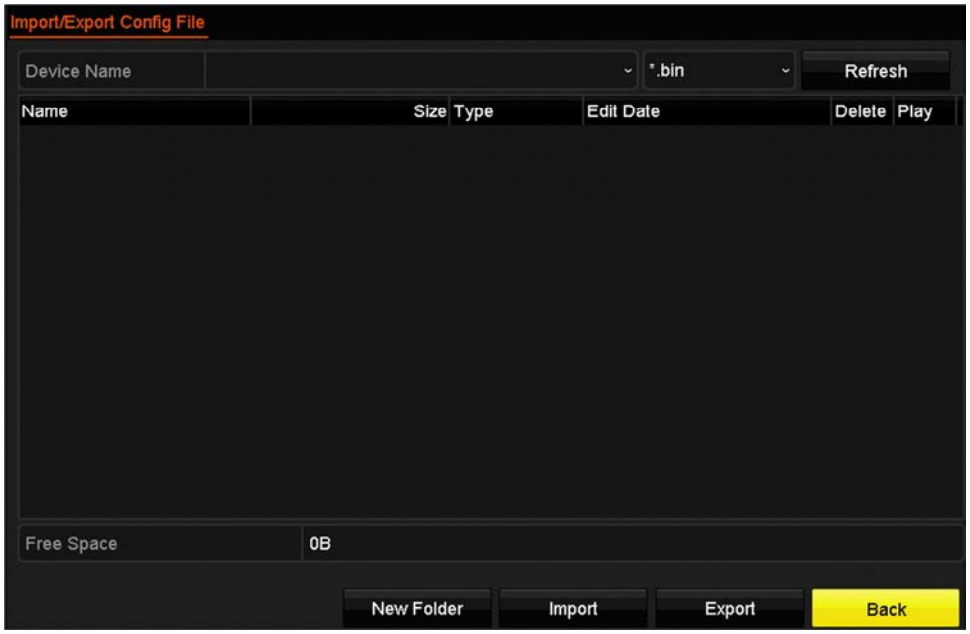


Figure 12-6 Import/Export Config File

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

3. Enter a password for the file.



Figure 12-7 Export Encryption Password Window

4. Click **OK** to save the file.

5. To import a configuration file, select the file from the selected backup device and click **Import**. After the import process is complete, you must reboot the NVR.

NOTE

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

12.4 Upgrading System

Purpose:

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

12.4.1 Upgrading by Local Backup Device

1. Connect your NVR to a local backup device containing the update firmware file.
2. Go to **Menu > Maintenance > Upgrade**.
3. Click the **Local Upgrade** tab to enter the local upgrade menu, as shown in Figure 12-8.

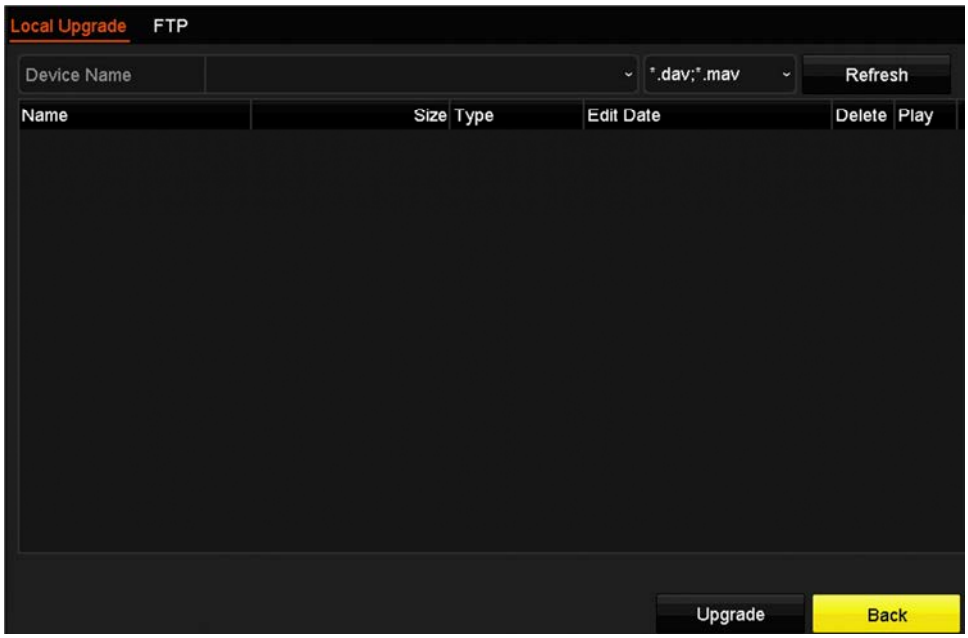


Figure 12-8 Local Upgrade Interface

4. Select the update file from the backup device.
5. Click **Upgrade** to start upgrading.
6. After the upgrading is complete, reboot the NVR to activate the new firmware.

12.4.2 Upgrading by FTP

Purpose:

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

NOTE

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

1. Go to **Menu > Maintenance > Upgrade**.
2. Click the **FTP** tab to enter the local upgrade interface, as shown in Figure 12-9.

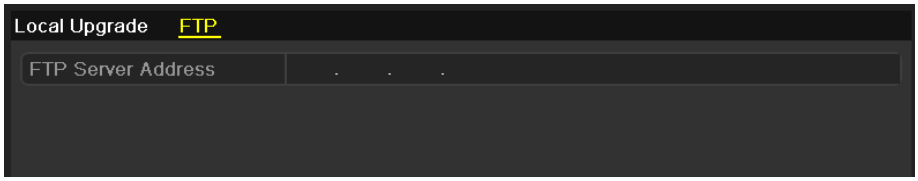


Figure 12-9 FTP Upgrade Interface

3. Enter 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.

12.5 Restoring Default Settings

1. Go to **Menu > Maintenance > Default**.

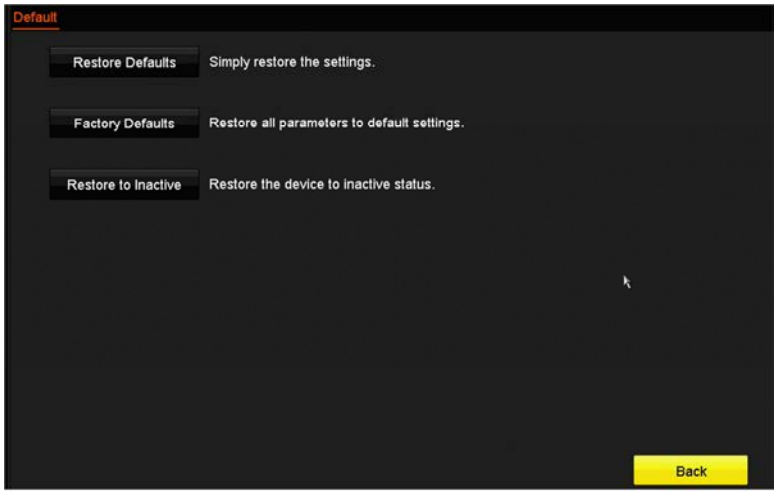


Figure 12-10 Restore Defaults

2. Select the restore type from the following three options.
   - **Restore Defaults**: Restore all parameters, except the network (including IP address, subnet mask, gateway, MTU, NIC working mode, default route, server port, etc.) and user account parameters, to the factory default settings.
   - **Factory Defaults**: Restore all parameters to the factory default settings.
   - **Restore to Inactive**: Restore the device to inactive status.
3. Click **OK** to restore the default settings.

NOTE

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

Chapter 13 Others

13.1 Configuring General Settings

Purpose:

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

1. Go to **Menu > Configuration > General**.

2. Select the **General** tab.

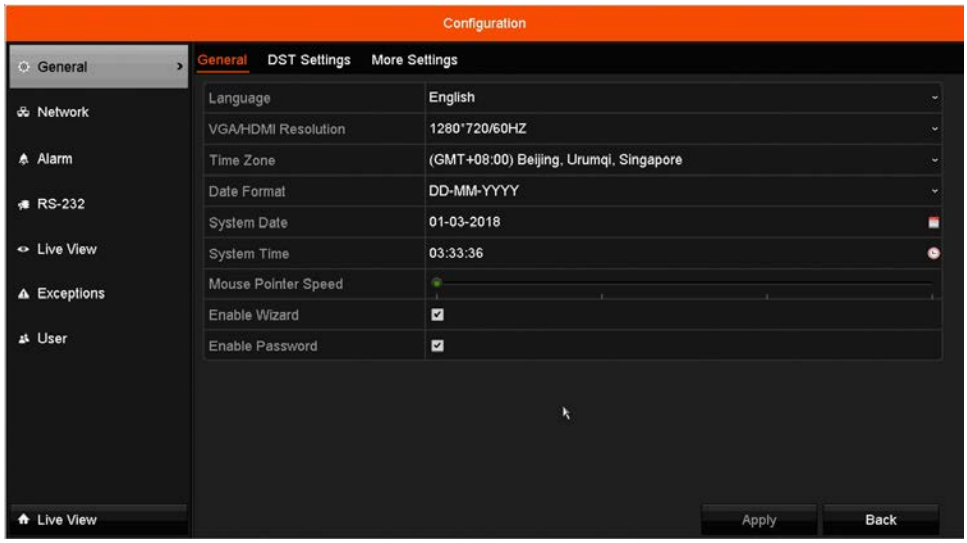


Figure 13-1 General Settings Interface

3. Configure the following settings:

   - **Language:** The default language used is *English*.
   - **Resolution:** Configure the VGA resolution and HDMI resolution respectively.
   - **Time Zone:** Select the time zone.
   - **Date Format:** Select the date format.
   - **System Date:** Select the system date.
   - **System Time:** Select the system time.
   - **Mouse Pointer Speed:** Set the speed of mouse pointer; four levels are configurable.
   - **Enable Wizard:** Enable/disable the Wizard when the device starts up.
   - **Enable Password:** Enable/disable the use of the login password.

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

13.2 Configuring DST Settings

1. Go to **Menu > Configuration > General**.
2. Choose **DST Settings**.

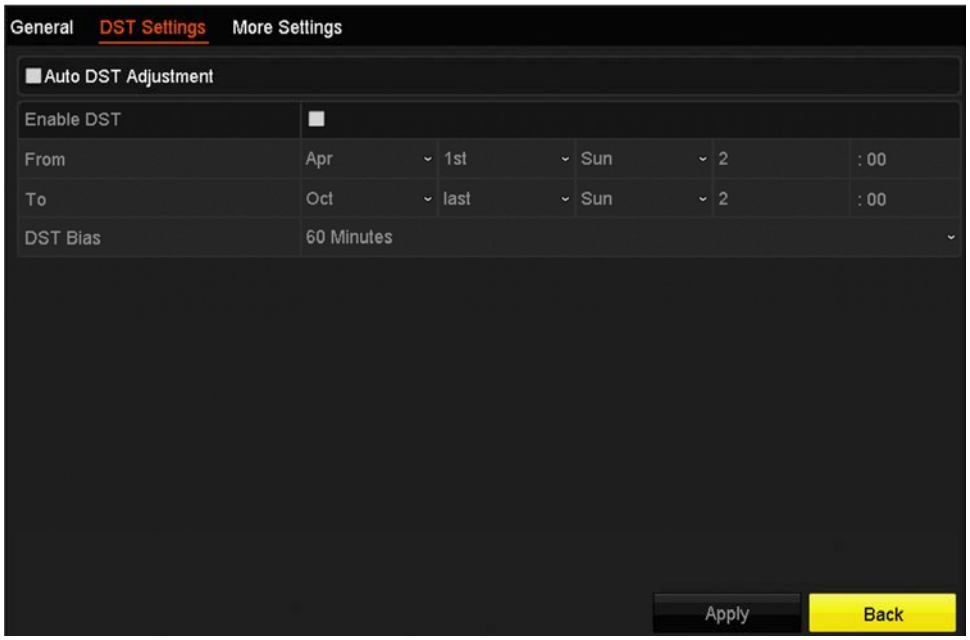


Figure 13-2 DST Settings Interface

3. Check the checkbox before the **Auto DST Adjustment** item, or manually check the **Enable DST** checkbox, and then choose the DST period date.

13.3 Configuring More Settings for Device Parameters

1. Go to **Menu > Configuration > General**.
2. Click **More Settings** to enter the More Settings interface, as shown in Figure 13-3.

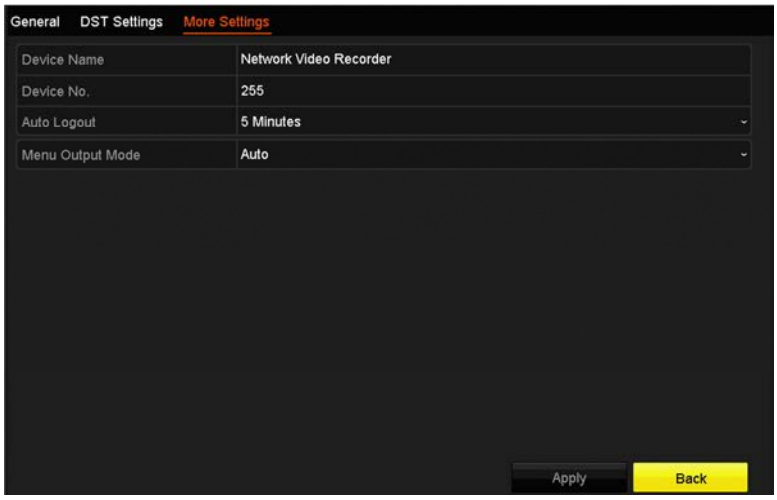


Figure 13-3 More Settings Interface

3. Configure the following settings:

- **Device Name:** Edit the name of the NVR.
- **Device No.:** Edit the serial number of the NVR. The Device No. can be set in the range of 1 to 255, and the default no. is 255. The number is used for the remote and keyboard control.
- **Auto Logout:** Set timeout time for menu inactivity. E.g., when the timeout time is set to *5 Minutes*, then the system will exit from the current operation menu to live view screen after 5 minutes of menu inactivity.
- **Menu Output Mode:** You can choose the menu display on different video outputs. By default, only HDMI™/VGA is selectable.
- Click **Apply** 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 you create the password when you start the device for the first time. The *Administrator* has the permission to add and delete users and configure user parameters.

13.4.1 Adding a User

1. Go to **Menu > Configuration > User**.

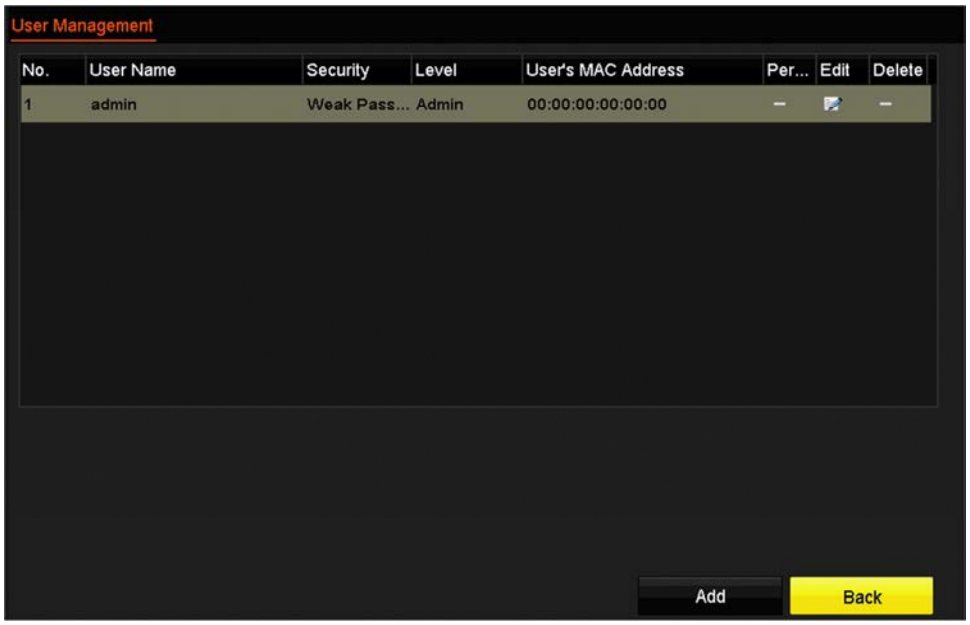


Figure 13-4 User Management Interface

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

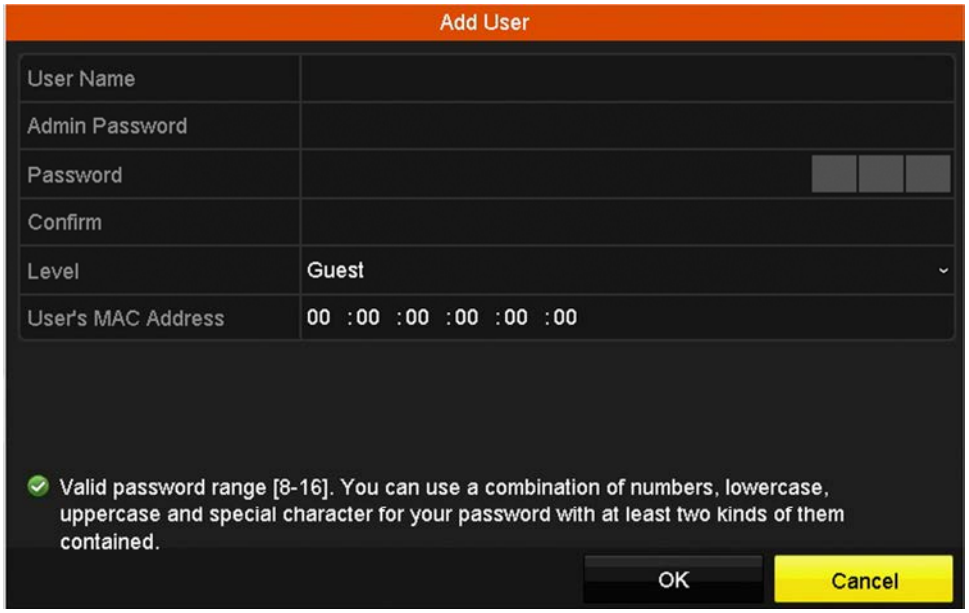


Figure 13-5 Add User Menu

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

   - **Password**: Set the password for the user account.

WARNING

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

   - **Level:** Set the user level to Operator or Guest. Different user levels have different operating permission.
   - **Operator:** The *Operator* user level has all operating permission in Camera Configuration by default.
   - **Guest:** The Guest user only has the local/remote playback in the Camera Configuration by default.
   - **User's MAC Address:** The MAC address of the remote PC which logs onto the NVR. If it is configured and enabled, it only allows the remote user with this MAC address to access the NVR.

1. Click **OK** to save the settings and go back to the User Management interface. The added new user will be displayed on the list, as shown in Figure 13-6.

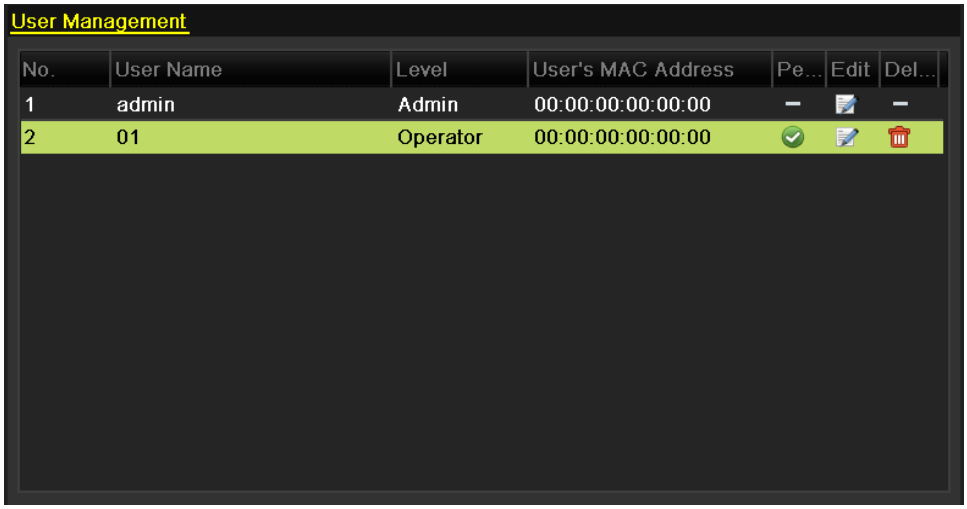


Figure 13-6 Added User Listed in User Management Interface

2. Select the user from the list and then click the button to enter the Permission settings interface.



Figure 13-7 User Permission Settings Interface

3. 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
  - **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)

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

NOTE

Only the admin user account has permission to restore the factory default parameters.

13.4.2 Deleting a User

1. Go to **Menu > Configuration > User**.

2. Select the user to be deleted from the list, as shown in Figure 1. 2.

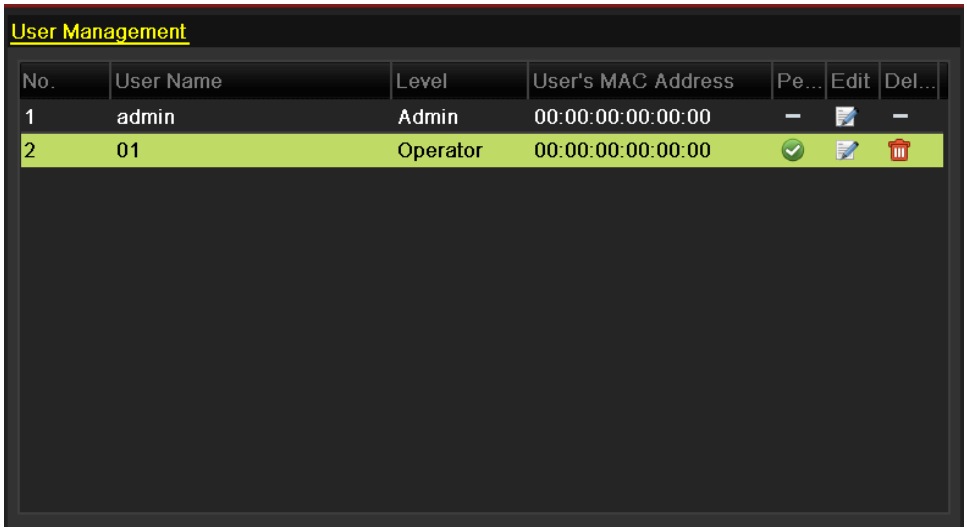


Figure 1. 2 User List

3. Click to delete the selected user account.

13.4.3 Editing a User

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

1. Go to **Menu > Configuration > User**.
2. Select the user to be edited from the list, as shown in Figure 1. 2.
3. Click to enter the Edit User interface.

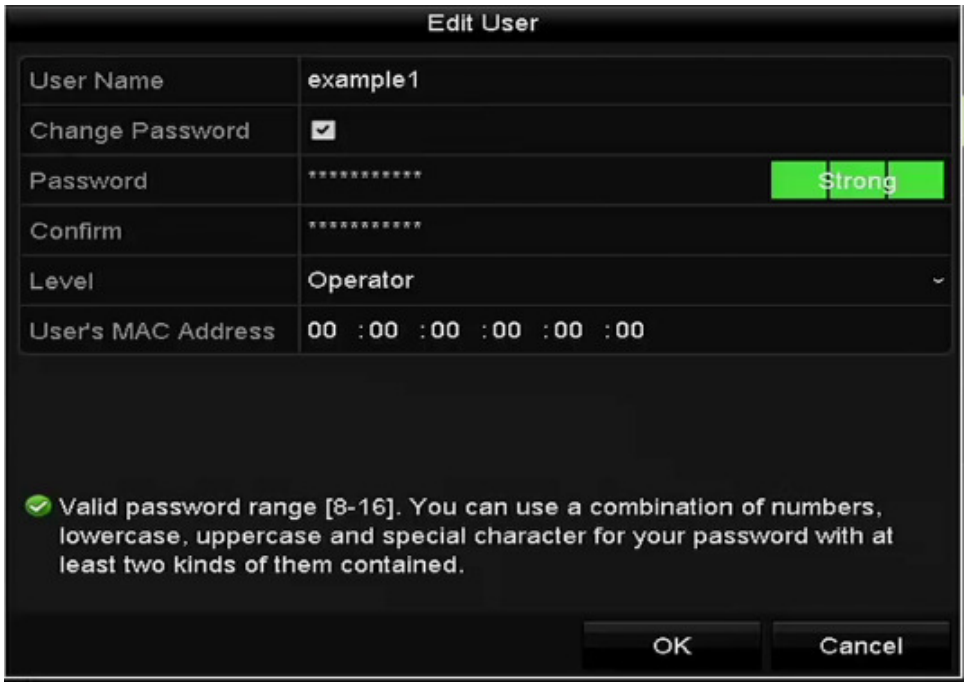


Figure 13-8 Edit User (Operator/Guest)

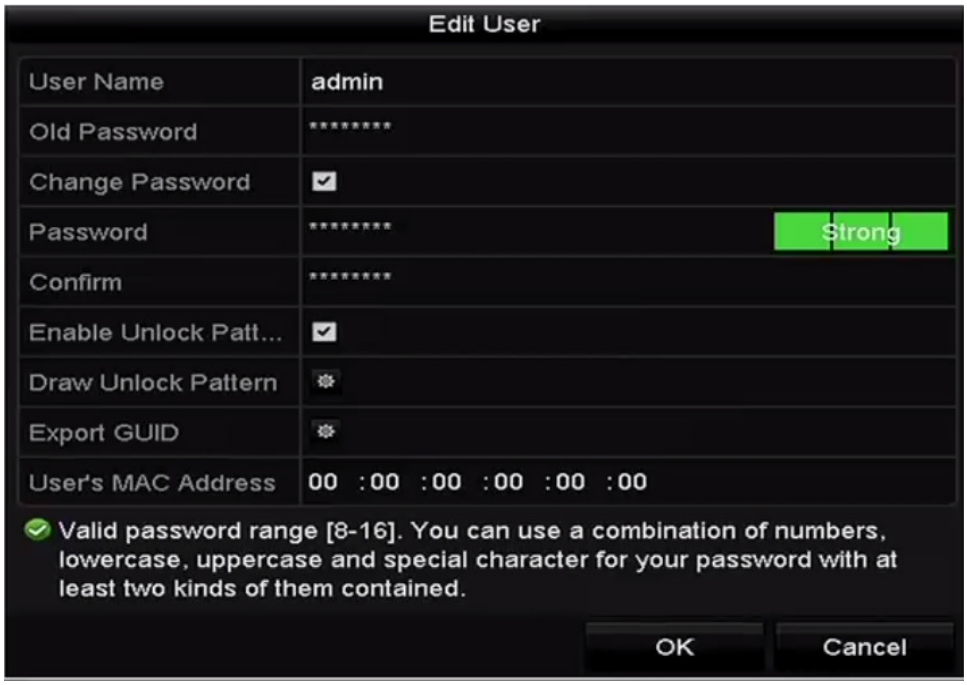


Figure 13-9 Edit User (admin)

4. Edit the corresponding parameters.

Operator and Guest

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

Admin

You are allowed only to edit the password and MAC address. Check the **Change Password** checkbox if you want to change the password, and input the correct old password, and the new password, in the **Password** and **Confirm** text fields.

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

---

5. Edit the unlock pattern for the admin user account.

    1) Check the **Enable Unlock Pattern** checkbox to enable the use of an unlock pattern when logging in to the device.

    2) Use the mouse to draw a pattern among the nine dots on the screen. Release the mouse when the pattern is done.

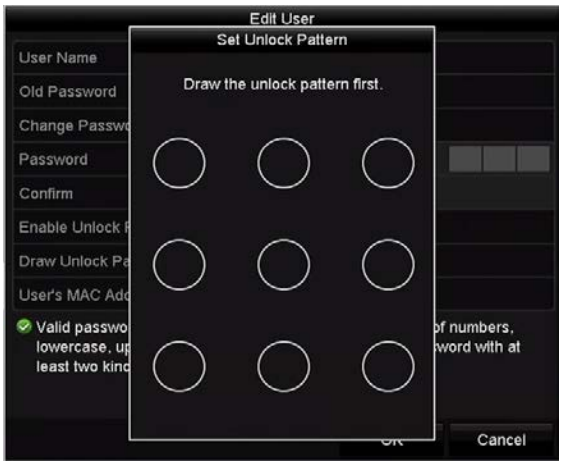


Figure 13-10 Set Unlock Patter for Admin User

6. Click of **Export GUID** to enter the reset password interface to export the GUID file for the admin user account.

NOTE

If the admin password is changed, you can re-export the GUID file to the connected flash drive for the future password resetting.

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

8. For the **Operator** or **Guest** user account, click the button on the user management interface to edit the permission.

Chapter 14 Appendix

14.1 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
- **DDNS:** Dynamic DNS is a method, protocol, or network service that provides the capability for a networked device, such as a router or computer system using the Internet Protocol Suite, to notify a domain name server to change, in real time (ad-hoc) the active DNS configuration of its configured hostnames, addresses or other information stored in DNS.
- **Hybrid DVR:** A hybrid DVR is a combination of a DVR and NVR.
- **NTP:** Acronym for Network Time Protocol. A protocol designed to synchronize the clocks of computers over a network.
- **NTSC:** Acronym for National Television System Committee. NTSC is an analog television standard used in such countries as the United States and Japan. Each frame of anNTSC signal contains 525 scan lines at 60Hz.
- **NVR:** Acronym for Network Video Recorder. An NVR can be a PC-based or embedded system used for centralized management and storage for IP cameras, IP Domes and other DVRs.
- **PAL:** Acronym for Phase Alternating Line. PAL is also another video standard used in broadcast televisions systems in large parts of the world. PAL signal contains 625 scan lines at 50Hz.
- **PTZ:** Acronym for Pan, Tilt, Zoom. PTZ cameras are motor driven systems that allow the camera to pan left and right, tilt up and down and zoom in and out.
- **USB:** Acronym for Universal Serial Bus. USB is a plug-and-play serial bus standard to interface devices to a host computer.

14.2 Troubleshooting

No image displayed on the monitor after starting up normally.

Possible Reasons

- No VGA or HDMI™ connections.
- Connection cable is damaged.
- Input mode of the monitor is incorrect.

1. Verify the device is connected to the monitor via an HDMI™ or VGA cable.
   If not, connect the device to 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, contact the engineer from our company for further processing.

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

Possible Reasons

- No HDD is installed in the device.
- The installed HDD has not been initialized.
- The installed HDD is not compatible with the NVR or is broken-down.

1. Verify at least one HDD is installed in the NVR. If not, please install the compatible HDD.

   NOTE

   Refer to the “Quick Operation Guide” for the HDD installation steps.

   If you don’t want to install an HDD, select Menu > Configuration > Exceptions, and uncheck the **HDD Error > Audible Warning** checkbox.

2. Verify the HDD is initialized.

3. Select **Menu > HDD > General**.

4. If the HDD status is “Uninitialized,” check the corresponding HDD checkbox and click Init.

5. Verify the HDD is detected and is in good condition.
6. Select **Menu > HDD > General**.
7. If the HDD is not detected or the status is Abnormal, replace the dedicated HDD according to the requirement.
8. Check if the fault is solved by step 1 to step 3.
9. If it is solved, finish the process. If not, contact an engineer from our company for further processing.

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

Possible Reasons

- Network failure, and the NVR and IP camera lost connections.
- The configured parameters are incorrect when adding the IP camera.
- Insufficient bandwidth.

1. Verify the network is connected.
2. Connect the NVR and PC with the RS-232 cable.
3. Open the Super Terminal software, and execute the ping command. Input "ping IP" (e.g. ping 172.6.22.131).

   NOTE

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

   If there exists return information and the time value is low, the network is normal.
4. Verify the configuration parameters are correct.
5. Select **Menu > Camera > Camera > IP Camera**.
6. Verify the following parameters are the same with those of the connected IP devices, including IP address, protocol, management port, user name, and password.
7. Verify the bandwidth is enough.
8. Select **Menu > Maintenance > Net Detect > Network Stat**.
9. Check the usage of the access bandwidth and see if the total bandwidth has reached its limit.
10. Check if the fault is solved by steps 1 to step 3.
11. If it is solved, finish the process. If not, contact an engineer from our company for further processing.

The IP camera frequently goes online and offline and the status of it displays as "Disconnected."

Possible Reasons

- The IP camera and the NVR versions are not compatible.
- Unstable power supply of IP camera.
- Unstable network between IP camera and NVR.
- Limited flow by the switch connected with IP camera and NVR.

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

   NOTE

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

   Example: Input ping 172.6.22.131 –l 1472 –f.

10. Verify the switch is not flow control.
11. Check the brand, model of the switch connecting IP camera and NVR, and contact the manufacturer of the switch to check if it has the flow control function. If so, turn it down.
12. Check if the fault is solved by the step 1 to step 4.
13. If it is solved, finish the process. If not, contact an engineer from our company for further processing.

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

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

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

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

   NOTE

   The view settings can only be configured by the local operation of NVR.

   Different camera orders and window-division modes can be set for different output interfaces separately, and digits like “D1”and “D2” stand for the channel number, and “X” means the selected window has no image output.
3. Check if the fault is solved by the above steps.
4. If it is solved, finish the process. If not, contact an engineer from our company for further processing.

Live view stuck when video output locally.

Possible Reasons:

- Poor network between NVR and IP camera, and there exists packet loss during the transmission.
- The frame rate has not reached the real-time frame rate.

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

   NOTE

   Simultaneously press **Ctrl** and **C** to exit the ping command.
2. Verify the frame rate is real-time frame rate.
3. Select **Menu > Record > Parameters > Record** and set the Frame rate to Full Frame.
4. Check if the fault is solved by the above steps.
5. If it is solved, finish the process. If not, contact an engineer from our company for further processing.

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

Possible Reasons:

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

- Poor network between NVR and PC, and there exists packet loss during the transmission.
- The performances of hardware are not good enough, including CPU, memory, etc.

1. Verify the network between NVR and IP camera is connected.
2. When image is stuck, connect the RS-232 ports on PC and the rear panel of NVR with the RS-232 cable.
3. 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.

4. Verify the network between the NVR and PC is connected.
5. Open the cmd window in the Start menu, or you can press “windows+R” shortcut key to open it.
6. 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.

7. Verify the hardware of the PC is good enough.
8. Simultaneously press **Ctrl**, **Alt** and **Delete** to enter the windows task management interface, as shown in the following figure.

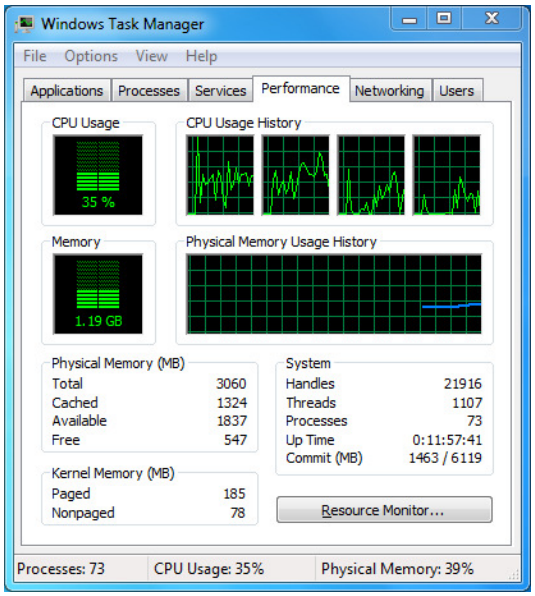


Figure 14-1 Windows task management interface

9. Select the “Performance” tab; check the status of the CPU and Memory.

10. If the resource is not enough, end some unnecessary processes.

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

12. If it is solved, finish the process. If not, contact an engineer from our company for further processing.

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:

- Cable between the pickup and IP camera is not connected well; impedance mismatches or incompatible.
- The stream type is not set as "Video & Audio."
- The encoding standard is not supported with NVR.

1. Verify the cable between the pickup and IP camera is connected well; impedance matches and compatible.
2. Log in the IP camera directly, and turn the audio on, check if the sound is normal. If not, contact the manufacturer of the IP camera.
3. Verify the setting parameters are correct.
4. Select **Menu > Record > Parameters > Record** and set the Stream Type to Audio & Video.
5. Verify the audio encoding standard of the IP camera is supported by the NVR.
6. 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.
7. Check if the fault is solved by the above steps.
8. If it is solved, finish the process. If not, contact an engineer from our company for further processing.

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

Possible Reasons:

- Poor network between NVR and IP camera, and there exists packet loss during the transmission.
- The frame rate is not the real-time frame rate.
- The NVR supports up to 16-channel synchronize playback at 4CIF resolution. If you want 16-channel synchronized playback at 720p resolution, frame extracting may occur, which leads to slight sticking.

1. Verify the network between NVR and IP camera is connected.
2. When image is stuck, connect the RS-232 ports on PC and the rear panel of NVR with the RS-232 cable.
3. 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** keys to exit the ping command.

4. Verify the frame rate is real-time frame rate.
5. Select **Menu > Record > Parameters > Record**, and set the Frame Rate to “Full Frame.”
6. Verify the hardware can afford the playback.
7. Reduce the channel number of playback.
8. Select **Menu > Record > Encoding > Record**, and set the resolution and bitrate to a lower level.
9. Reduce the number of local playback channels.
10. Select **Menu > Playback**, and uncheck the checkbox(es) of unnecessary channels.
11. Check if the fault is solved by the above steps.
12. If it is solved, finish the process. If not, contact an engineer from our company for further processing.

No record file found in the NVR local HDD, and prompt “No record file found.”

Possible Reasons:

- The time setting of system is incorrect.
- The search condition is incorrect.
- The HDD is error or not detected.

1. Verify the system time setting is correct.
2. Select **Menu > Configuration > General > General**, and verify the “Device Time” is correct.
3. Verify the search condition is correct.
4. Select **Playback**, and verify the channel and time are correct.
5. Verify the HDD status is normal.
6. Select **Menu > HDD > General** to view the HDD status, and verify the HDD is detected and can be read and written to normally.
7. Check if the fault is solved by the above steps.
8. If it is solved, finish the process. If not, contact an engineer from our company for further processing.