



ALIBI™ ALI-NVR71128R Network Video Recorder Firmware V3.6.22 User Manual



PLEASE READ THIS MANUAL BEFORE USING YOUR SYSTEM, and always follow the instructions for safety and proper use. Save this manual for future reference.

About this manual

This user manual applies to all ALIBI **ALI-NVR71128R** Network Video Recorders (NVR) with firmware version V3.6.22.

Navigation in the firmware is represented by the expression: “**Menu | Configuration | Alarm | Alarm Output**”, which means:

- a. Right click on the Live View display to open the pop-up menu, and then click the **Menu** entry (at the top of the list).
- b. In the Menu window, click the **Configuration** icon.
- c. In the Configuration window, click the **Alarm** entry in the left frame.
- d. Click the **Alarm Output** tab at the top of the screen. This may also indicate a parameter on the screen.

To find the version of the firmware installed in your NVR, open the **Menu | Configuration** screen.

LEGAL NOTICE

Observint Technologies (Observint) products are designed to meet safety and performance standards with the use of specific Observint authorized accessories. Observint disclaims liability associated with the use of non-**Observint** authorized accessories.

The recording, transmission, or broadcast of any person’s voice without their consent or a court order is strictly prohibited by law.

Distributing, copying, disassembling, reverse compiling, reverse engineering, and exporting, in violation of export laws, the software provided with Alibi video recorders is expressly prohibited.

Observint makes no representations concerning the legality of certain product applications such as the making, transmission, or recording of video and/or audio signals of others without their knowledge and/or consent. We encourage you to check and comply with all applicable local, state, and federal laws and regulations before engaging in any form of surveillance or any transmission of radio frequencies.

Alibi and the Alibi logo are trademarks of **Observint**.

Microsoft, **Windows**, and **Internet Explorer** are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. **Android** is a trademark of Google Inc. Use of this trademark is subject to Google Permissions. **Apple**, **iPhone**, **iPod touch**, and **iPad** are registered trademarks of Apple Inc.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. **Observint** disclaims any proprietary interest in trademarks and trade names other than its own.

No part of this document may be reproduced or distributed in any form or by any means without the express written permission of Observint Technologies.

© 2018 by Observint Technologies. All Rights Reserved.

11000 N. Mopac Expressway, Building 300, Austin, TX 78759

For Sales and Support, contact your distributor.

Table of Contents

SECTION 1	Systems Overview	1
	1.1 Soft keyboards	3
SECTION 2	Initial NVR Setup	5
	2.1 Using the setup Wizard	5
	2.2 Access the Menu system	11
	2.3 Customize camera configurations	12
	2.3.1 Camera OSD setup	13
	2.3.2 Camera Image setup	14
	2.3.3 Camera PTZ setup	15
	2.3.4 Camera Motion detection setup	15
	2.3.5 Camera Privacy Mask setup	18
	2.3.6 Camera Video Tampering setup	19
	2.3.7 Camera Video Loss setup	21
	2.3.8 VCA	23
	2.4 Adding cameras manually	23
	2.4.1 Configuring customized protocols	26
	2.5 Checking HDD status	28
	2.5.1 Additional HDD features	29
	2.6 Configuring Exception Alarms	30
	2.7 Setting sensor alarms	31
	2.8 Setting alarm response actions	35
SECTION 3	Startup, Shutdown, Reboot	39
	3.1 Starting Up, Shutting Down and Rebooting the NVR	39
	3.1.1 Startup	39
	3.1.2 Shutdown	39
	3.1.3 Rebooting the NVR	40
SECTION 4	Live View Interface	41
	4.1 Setting monitor resolution	41
	4.2 Dual monitor support - Main and Aux monitors	42
	4.2.1 Setting Menu Output Mode	43
	4.3 Live View settings	45
	4.4 Using the mouse in Live view	46
	4.5 Live View Status icons	47

TABLE OF CONTENTS

	4.6 Quick Setting Toolbar	47
	4.7 Channel-Zero Encoding	49
SECTION 5	PTZ Controls	50
	5.1 PTZ Control Panel	50
	5.2 Configuring PTZ settings	51
	5.3 Setting PTZ presets, patrols and patterns	53
	5.3.1 Customizing Presets	53
	5.3.2 Calling Presets	54
	5.3.3 Customizing Patrols	55
	5.3.4 Calling Patrols in Live View	56
	5.3.5 Creating a Pattern	57
	5.3.6 Calling the Pattern	58
	5.4 Linear Scan	59
	5.4.1 Initiating a Linear Scan	59
SECTION 6	VCA Features	61
	6.1 Face Detection	62
	6.2 Line Crossing Detection	65
	6.3 Intrusion Detection	69
	6.4 Region Entrance Detection	73
	6.5 Region Exiting Detection	77
	6.6 Unattended Baggage Detection	82
	6.7 Object Removal Detection	85
	6.8 Audio Exception Detection	89
	6.9 Defocus Detection	93
	6.10 Sudden Scene Change Detection	96
	6.11 PIR Alarm	99
	6.12 VCA Search features	102
	6.12.1 Behavior search	102
	6.12.2 Face search	104
	6.12.3 Plate Search	105
	6.12.4 Advanced Search	106
	6.12.5 Counting	106
	6.12.6 Heat map	107
SECTION 7	Record, Playback and Video Backup	109
	7.1 Configuring record settings	110

	7.1.1	Setting camera parameters	110
	7.1.2	Configuring Record schedule	112
	7.1.3	Record Holiday settings.....	116
	7.1.4	Record Advanced settings.....	118
	7.1.5	Configuring Motion Detection Recording	119
	7.1.6	Manual record	121
	7.1.7	Configuring HDD Group for Recording.....	123
	7.1.8	Files Protection.....	123
	7.2	Playback.....	125
	7.2.1	Instant playback by channel	125
	7.2.2	Playback by channel - menu and screen controls	125
	7.2.3	Create video tag	130
	7.2.4	Playback by Event Search	131
	7.2.5	Playback by Tag	133
	7.2.6	Playback by Sub-Periods	135
	7.2.7	Playing Back an external file	136
	7.2.8	Playback Pictures	137
	7.2.9	Playback using System logs	138
	7.2.10	Auxiliary Functions - Playback frame by frame	140
	7.2.11	Auxiliary Functions - Reverse Playback Multi-channel	140
	7.2.12	Digital Zoom.....	142
	7.3	Backing up Record Files - Export.....	142
	7.3.1	Quick Export	142
	7.3.2	Export by video search	144
	7.3.3	Export by Event Search	147
	7.3.4	Export by Picture Search	150
	7.3.5	Exporting Video Clips during playback	153
SECTION 8		Managing User Accounts	156
	8.1	Adding a user account	156
	8.2	Deleting a user account	161
	8.3	Editing a user account	161
	8.3.1	Edit admin user	162
SECTION 9		Network Settings	163
	9.1	Configuring General Settings	163
	9.2	Configuring Advanced Settings.....	164

TABLE OF CONTENTS

	9.2.1	Configuring PPPoE	164
	9.2.2	Configuring DDNS	165
	9.2.3	Configuring NTP Server	167
	9.2.4	Configuring Remote Alarm Host	168
	9.2.5	Configuring Multicast	169
	9.2.6	Configuring RTSP	170
	9.2.7	Configuring Server and HTTP Ports	170
	9.2.8	Configuring Email	171
	9.2.9	Configuring UPnP™	173
SECTION 10		System Maintenance	175
	10.1	System Information	175
	10.2	Log Information, Log Export	175
	10.2.1	Log Search	176
	10.3	Import / Export system configuration	180
	10.4	Upgrade Firmware	182
	10.4.1	Upgrade from FTP server	183
	10.5	Default	184
	10.6	Net Detect	185
	10.6.1	Checking Network Traffic	185
	10.6.2	Testing Network Delay and Packet Loss	185
	10.6.3	Exporting Network Packet	186
	10.6.4	Checking the network status	187
	10.6.5	Checking Network Statistics	188
	10.6.6	HDD Detect	189
	10.7	Disk Clone	192
SECTION 11		Managing HDDs (without RAID)	194
	11.1	Initializing HDDs	194
	11.2	Adding network HDDs to the system	195
	11.3	Configuring the HDD Quota/Group mode	197
	11.4	HDD Maintenance	203
	11.4.1	S.M.A.R.T. Display	203
	11.4.2	Bad Sector Detection	204
SECTION 12		RAID Arrays	206
	12.1	Create a RAID array	206
	12.1.1	Installing a Hot Spare disk	209

	12.2 Rebuilding a RAID array (example)	210
	12.2.1 Rebuilding array process - example.....	210
SECTION 13	Remote Access.....	212
	13.1 Configure IE to run in Administrator mode	212
	13.2 Login.....	213
	13.3 Live View screen	214
	13.4 Playback screen.....	217
	13.5 Picture screen	219
	13.6 Configuration screen	220
	13.6.1 Log information	221
APPENDIX A	Glossary	223

NOTES

SECTION 1

Systems Overview

Congratulations on purchasing your new Embedded NVR security system! Your system includes the following key features:

General

- Each channel supports dual-stream video.
- NVR supports cameras from several manufacturers. Consult with your vendor for a list of supported camera.
- 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

- VGA monitor output with resolutions up to 1920 × 1080 / 60 Hz.
- Front panel monitor with resolution up to 1080p
- HDMI monitor output with resolutions up to 4K (3840 × 2160 / 60 Hz).
- Video Wall supports up to 6 monitors through Alibi Central Management System (ACMS) V3.1
- Main / Auxiliary monitor feature determines whether control is on VGA or HDMI screen.
- Multiple screen display in Live view is supported; the display sequence of channels is configurable.
- Configurable Live View display of groups and tours.
- Live view Quick setting menu.
- Motion detection, video tampering, video exception alert and video loss alert functions.
- Privacy mask.
- Camera detected VCA alarm reporting and processing.
- Zooming in by clicking the mouse and PTZ tracing by dragging mouse.

HDD Management

- Supports internal SATA hard disk drive(s), with a maximum of 8 TB storage capacity in each drive.
- 8 network disks (8 NAS disks, or 7 NAS disks+1 IP SAN disk) can be connected.
- Supports RAID 0 / 1 / 5 / 6 / 10 configurations.
- Supports HDD S.M.A.R.T. and bad sector detection.
- Supports HDD group management.
- Supports HDD standby function.
- Supports HDD property: redundancy, read-only, read/write (R/W).
- Supports HDD quota management; a different capacity can be assigned to each camera channel.

Recording and Playback

- Normal and event video encoding parameters.
- Multiple recording types: manual, normal, and Event and Video Content Analytics triggered recording.

SECTION 1: SYSTEM OVERVIEW

- Eight recording time periods with separated recording types.
- Supports pre-record and post-record for motion detection recording, and pre-record time for schedule and manual recording.
- Tag marker insertions, search and playback by tags.
- Lock/unlocking video files.
- Searching and playing back record files by channel number, recording type, start time, end time, etc.
- Motion analysis for the selected area in the video.
- Zoom in/out during playback.
- Forward/reverse, fast/slow playback.
- Forward/reverse multi-channel playback.
- Supports pause, skip forward and skip backward during playback.
- Synchronous multi-channel video playback.

Backup

- Export video data to USB or SATA device.
- Internal HDD clone to eSATA device
- Export video clips during playback.
- Management and maintenance of backup devices.
- Either Normal or Hot Spare working mode is configurable to constitute an N+1 hot spare system.

Alarm and Exception

- Configurable arming time of alarm input/output.
- Alarm for video loss, motion detection, tampering, abnormal signal, video input/output standard mismatch, illegal login, network disconnected, IP confliction, record exception, HDD error, and HDD full, etc.
- Camera detected VCA alarm reporting
- Alarm triggers full screen monitoring, audio alarm, notifying surveillance center, sending email and alarm output.
- Automatic restore when system is abnormal.

Other Local Functions

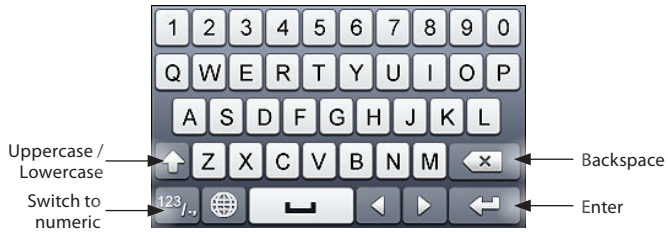
- Supports password reset mechanism option.
- Operable by mouse and control keyboard.
- Three-level user management; administrative user is allowed to create many operating accounts and define their operating permission, which includes the limit to access any channel.
- Operation, alarm, exceptions and log recording and searching.
- Manually triggering and clearing alarms.
- Manual capture operation.
- Import and export of device configuration information.

Network Functions

- Supports FTP based firmware updating.
- Supports Alibi-Connect remote connection.
- IPv6 supported.
- Supports IPv4, TCP/IP, UDP, HTTP, UPnP, RTSP/RTP/RTCP, SMTP, FTP, DHCP, NTP, DNS, ONVIF, HTTP multipart protocols.
- Supports TCP, UDP and RTP for unicast.
- Auto/manual port mapping by UPnP™ (enabled by default).
- Remote web browser access by HTTPS ensures high security.
- Remote reverse playback through the Alibi CMS and remote login.
- Support accessing by platform via ONVIF.
- Remote search, playback, download, locking and unlocking of the record files, and support downloading files broken transfer resume.
- Remote parameters setup; remote import/export of device parameters.
- Remote viewing of the device status, system logs and alarm status.
- Remote keyboard operation.
- Remote locking and unlocking of control panel and mouse.
- Remote HDD formatting and program upgrading.
- Remote system restart and shutdown.
- RS-485 transparent channel transmission.
- Alarm and exception information can be sent to the remote host
- Remotely start/stop recording.
- Remotely start/stop alarm output.
- Remote PTZ control.
- Remote manual JPEG capture.
- Virtual host function is provided to get access and manage the IP camera directly.
- Two-way audio and voice broadcasting.
- Embedded WEB server.

1.1 Soft keyboards

One of two on-screen keyboards appears when you click in a field that accepts an entry, such as a password or name or a numerical value. A third keyboard which includes symbols can also be opened while in the numeric keyboard. The alphanumeric keyboard is shown in the following picture. Some control keys toggle their function when they are clicked. A numerical keyboard, shown beneath, appears for numerical entries such as an IP address.



Soft keyboard - alphanumeric



Soft keyboard - numeric



Soft keyboard - symbols

A USB keyboard attached to the recorder has limited functionality. It can be useful for entering text and numbers.

SECTION 2

Initial NVR Setup

Use this section to setup the initial configuration of your NVR. Refer to the other sections of this manual for procedures for using the extensive features of the system.

2.1 Using the setup Wizard

Important guidelines for using the Wizard:

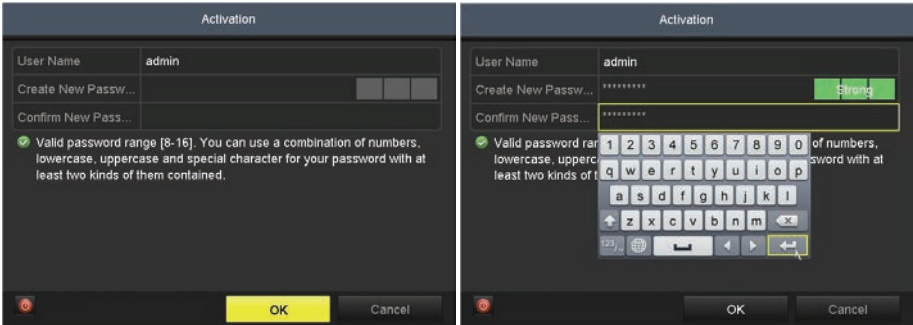
- **Password:** When logging into the recorder for the first time, create a “**Strong**” administrator user password. Follow the on-screen instructions. **NOTE:** There is no factory default password for this device.
 - **Date and Time:** Set the time zone, date and time correctly. All recorded video is time stamped.
 - **Storage - HDD:** In the HDD Management wizard, if a new recorder is shipped with a pre-configured HDD, nothing needs to be done with it in this window. If you installed an HDD or replaced the HDD, that HDD needs to be initialized by the recorder before it can be used to record data. Select (check the box for) that HDD, then click **Init** to initialize the disk. **NOTE: Init** will erase all data from the disk and can take several minutes to complete. When the initialization is complete, click **Next** to continue.
 - **Network Settings:** By default, the recorder acquires its network settings using DHCP (for dynamic network settings). Depending on the configuration of the network, these settings may change. To improve remote access to the recorder, Observint recommends that you configure the NVR with fixed network settings. To easily change the DHCP acquired network settings to fixed network settings, un-check the **Enable DHCP** option in the network setup menu, and then click **Apply**.
1. Power on the NVR using the **POWER** button on the front panel. Normally, an Alibi logo splash screen appears on the system Main monitor and the NVR front panel display within about 2 minutes.
 2. Power on the monitor(s).



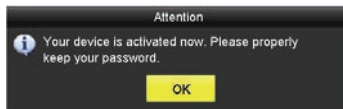
SECTION 2: INITIAL NVR SETUP

By default, the Setup Wizard will open automatically.

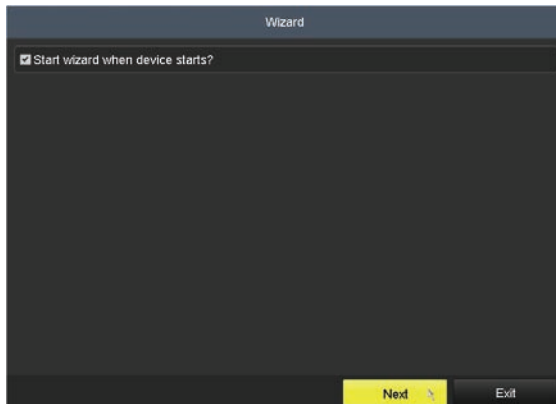
3. The initial **Activation** screen requires you to create the NVR administrative (*admin*) password:
 - a. To enter a password using the virtual keyboard, click inside the entry field, and click on the virtual keyboard to enter characters. Click the Next key in the lower right corner of the keyboard to complete the entry.



- b. Follow the on-screen instructions provided to create a **“Strong”** password, and then enter that in the **Create New Passw...** and **Confirm...** fields.
 - c. Click **OK** to continue. The confirmation window shown below will appear. Click **OK** to continue.



4. In the Wizard window shown below, click **Next** if you want to start the Wizard the next time the NVR is power up or restarted. Otherwise, uncheck the select box and then click **Next**.



5. In the next screen, set the time zone and date format (using the drop down menus), and the date and time in your recorder (using the pop-up graphical menus, see below). **NOTE:** Since video data is time stamped by the recorder, It is very important that this information be set precisely to produce valuable evidence.

The screenshot shows a 'Wizard' window with the following settings:

Time Zone	(GMT-06:00) Central Time(U.S. & Canada)
Date Format	MM-DD-YYYY
System Date	07-27-2017
System Time	10:30:26

Below the System Time field is a graphical time picker showing the hour (10), minute (31), and second (26) with navigation arrows. At the bottom of the window are three buttons: 'Previous', 'Next', and 'Exit'.

After configuring the date and time, click **Next** to start the clock at the time entered.

6. In the **Network** setup Wizard window:
- Open the Working Mode drop-down list and select the way you prefer the LAN ports: Fault tolerant or multi-address (does not allow DHCP).

The screenshot shows a 'Wizard' window with the following settings:

Working Mode	Net Fault-tolerance
Select NIC	bond0
NIC Type	10M/100M/1000M Self-adaptive
Enable DHCP	<input checked="" type="checkbox"/>
IPv4 Address	192.168.3.70
IPv4 Subnet Mask	255.255.255.128
IPv4 Default Gateway	192.168.3.1
Preferred DNS Server	192.168.3.1
Alternate DNS Server	
Main NIC	LAN1

At the bottom of the window are three buttons: 'Previous', 'Next', and 'Exit'. The 'Next' button is highlighted in yellow.

- To enable fixed network settings, first, un-check the **Enable DHCP** box. If a DHCP server is active on your network, the IPv4 Address, IPv4 Subnet Mask, IPv4 Default Gateway fields will be populated with network settings assigned by the

SECTION 2: INITIAL NVR SETUP

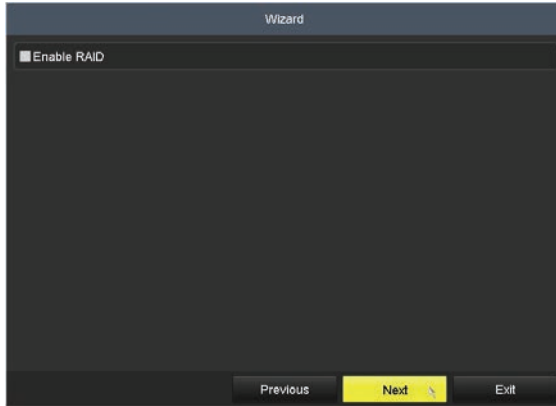
server. These settings are compatible with your network. If the fields are not populated, they will be blank as shown above.

- c. Enter (or modify, if necessary) the IPv4 Address, IPv4 Subnet Mask, IPv4 Default Gateway fields to settings compatible with your network using the virtual keyboard. You can also enter a Preferred DNS Server address (optional, ex. 8.8.8.8 and 8.8.4.4 [Google] DNSs). Consult with your network administrator to determine the best network settings for your NVR.
 - d. Open the **Main NIC** drop-down list and select the LAN port you prefer to be the primary network port. You can select either LAN1 .. LAN 8. The network settings you configured above will be applied to that port.
 - e. Click **Next** to continue.
7. You can reconfigure the network ports you prefer to use and DDNS access. Before changing your port configuration, consult with your network administrator or your vendor for product support.

Wizard	
Server Port	8000
HTTP Port	80
RTSP Port	1050
Enable UPnP	<input type="checkbox"/>
Enable DDNS	<input type="checkbox"/>
DDNS Type	DynDNS
Area/Country	Custom
Server Address	
Device Domain Name	
Status	DDNS is disabled.
User Name	
Password	

Previous **Next** Exit

- a. To change the Server, HTTP or RTSP port numbers, click on the entry field, and then use the pop-up virtual keyboard to enter a new value.
 - b. Check the select boxes to use Universal Plug and Play (UPnP) and DDNS as needed. If you enable DDNS, open the Type drop-down list and select either DynDNS, PeanutHull or NO-IP, and then enter the required information in the fields below.
 - c. After completing the settings in this window, click **Next** to advance to the next window.
8. In the window shown below, you can check the select box to enable RAID for the HDDs storage in the NVR. By default in the Wizard, RAID 5 is used.



To use a RAID configuration:

- RAID 5 disk configurations require at least three HDDs.
- If four HDDs are installed, one RAID array can be created. The fourth HDDs is automatically configured as a hot spare HDD for rebuilding the array when an "abnormal array" condition occurs.
- If more than 10 HDDs are installed in the chassis, 2 RAID arrays can be configured.

NOTE

Other RAID modes can be configured using the NVR firmware menu system.

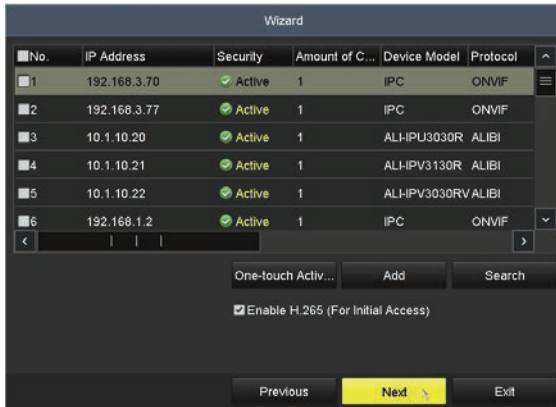
If enabling RAID in the NVR, follow the on-screen instructions to configure and name the array. A reboot of the NVR is required.

9. The HDD management Wizard window will open. If your NVR is a new NVR shipped with a pre-configured HDD, nothing needs to be done in this window. If you installed an HDD or replaced the HDD on the NVR, you must initialize (**Init**) it before it can be used. **CAUTION:** Initialization erases all information on the disk. In the example shown below, three HDDs were installed in the NVR.

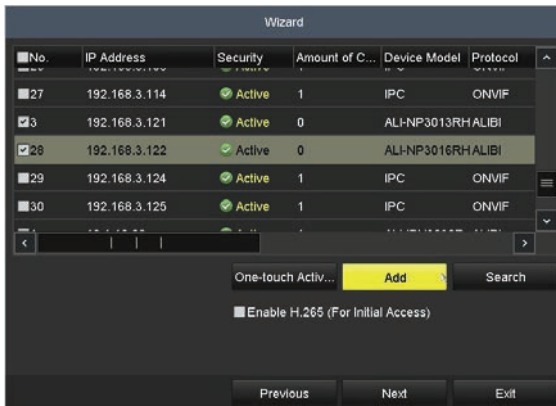


SECTION 2: INITIAL NVR SETUP

- a. To initialize an HDD, select (check the box for) the HDD you need to initialize, and then click **Init**. See above.
 - b. Wait until the initialization is complete, and then click **Next** to continue.
10. In the next window, click **Search** button to discover all compatible cameras on the LAN(s) the NVR is attached to. Other devices, such as NVRs and Alibi compatible storage servers are also listed. You can add cameras to the NVR in two ways:

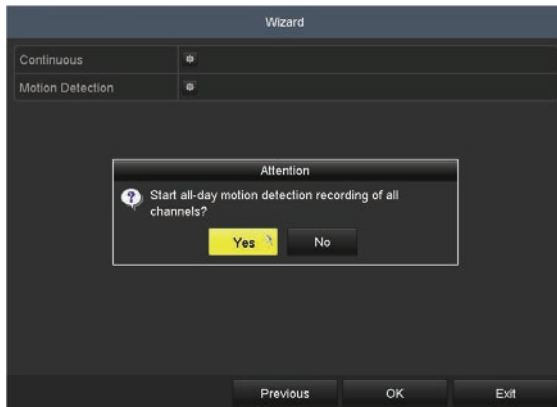


- a. Click the **One-touch Activate** button to add inactive cameras connected to the LAN to the NVR. When the camera is activated, it will be configured with the same *admin* password assigned to the NVR.
- b. Check the select boxes for the camera(s) you want to add, then click **Add**. In the example below, camera numbers 3 and 28 were selected. After camera(s) are added successfully, live video from the camera(s) will appear in the background.



- c. Check the **Enable H.265** select box to use this type of storage data compression. *High Efficiency Video Coding (HEVC)*, or H.265, is a video compression standard designed to substantially improve streaming efficiency with improved video quality.
 - d. Click **Next** to continue.
11. In the next Wizard window, select the kind of recording mode to apply to all cameras added to your recorder. You can select either:
- **Continuous**: The live video from all cameras will be recorded and stored;
 - **Motion Detection**: Live video live video from all cameras will recorded and stored when motion is detected in the video.

NOTE: In the firmware menu system you can configure each camera individually for conditions that will trigger recording, and when recordings are made. Configuring cameras in this way improves the performance of the NVR and reduces storage requirements.

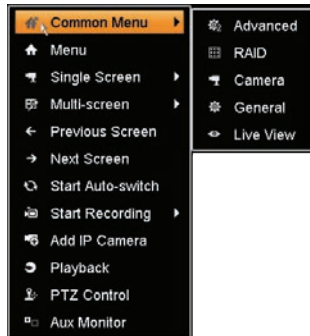


After selecting the recording mode, click **OK**, and then click **Yes** in the **Attention** popup window. The Wizard will close automatically.

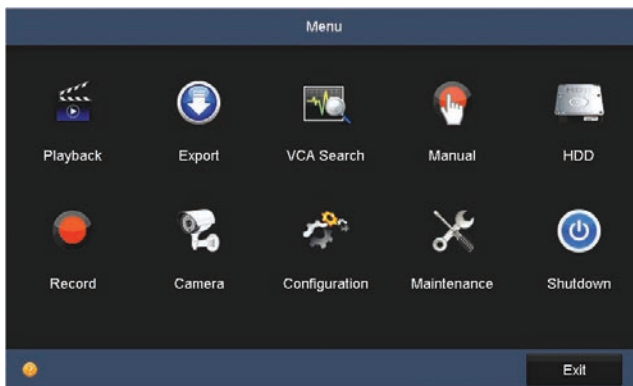
2.2 Access the Menu system

After the initial setup of your NVR using the Wizard, the Menu interface enables you to customize your configuration settings and expand the functionality of the system. To use most menus, the user must log into the NVR system, either locally or remotely, with administrative privileges.

To open the Menu system from the Live View screen, right click anywhere in the screen, then select **Menu**.



If ID Authentication is not disabled (see the **Menu | Configuration | General** settings), a login window will open. In the Login window, select a User Name with administrative privileges, enter its password, then click **OK**. **NOTE:** A window of **Menu** icons will open.



2.3 Customize camera configurations

The **Camera** menu lists all cameras configured in the NVR, and shows the channel, name, timestamp, etc. of each. Using this menu, you can assign names to each camera for easy recognition, select areas for motion detection and privacy blocking, and configure alarm features (if supported by the camera). To customize the configuration settings of each camera, do the following:

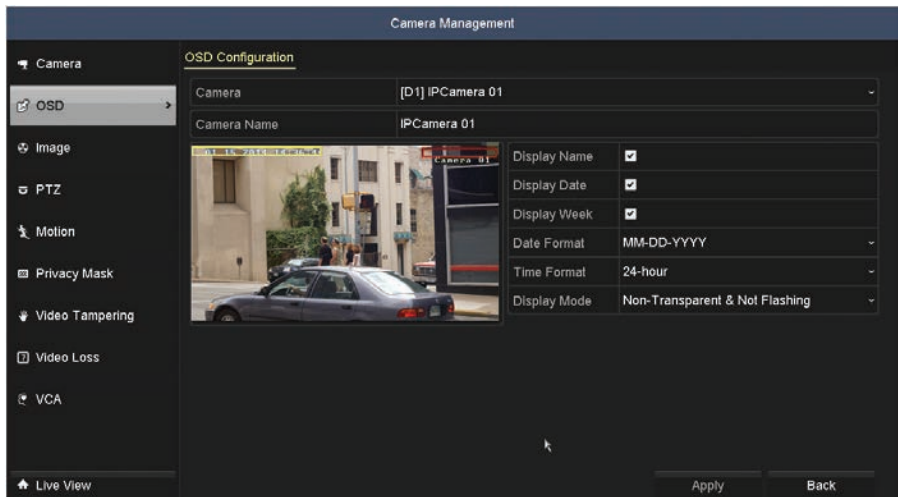
1. Open the Camera menu: right click anywhere on the Live View desktop, then click **Menu | Camera**.



2.3.1 Camera OSD setup

You can configure the OSD (On-Screen Display) settings for the camera, including date, time, day of week, camera name, etc.

1. Click **OSD** in the left frame to open the OSD submenu.



SECTION 2: INITIAL NVR SETUP

In the **Camera** field drop down list, select the camera you want to configure. In the example shown, **[D1]IPCamera 01** is selected.

2. Check or un-check the boxes to display the Name and Date. Also, edit the name in the **Camera Name** field, and select the date and time options you prefer.

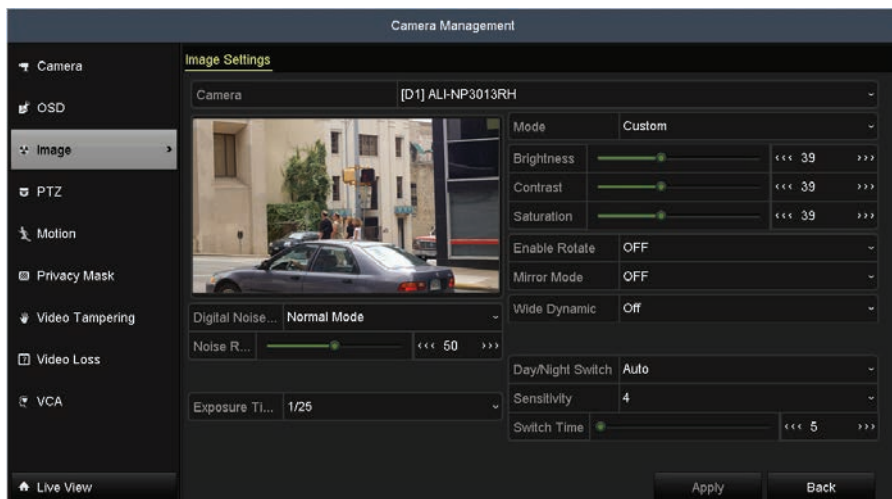
NOTE

Cameras you manage with the NVR may be setup internally to show on-screen information, such as name and timestamp. To change these settings, you must reconfigure the camera directly; the NVR cannot change these internal settings.

3. Drag the both the yellow box for the camera name and the red box for the timestamp data to positions in the window that will not obscure important information.
4. Change the date and time format, and the Display Mode if needed using the drop down menus.
5. Click **Apply** to save your settings for this camera.
6. Repeat sub-steps **2** through **5** above for each camera managed by the NVR.

2.3.2 Camera Image setup

1. Click **Image** in the left frame to open the Image submenu.



2. In the **Camera** field drop down list, select the camera you want to configure. In the example above, **[D1]IPCamera 01** is selected.
3. Drag the **Brightness**, **Contrast**, **Saturation** and **Hue** adjustment markers left or right to perfect the image from the camera. For some adjustments, you can click the up (▲) or down (▼) icons near the adjustment value (on the right side) to incrementally change the value of those adjustment.

4. Click **Apply** to save your settings for this camera.
5. Repeat sub-steps **2** through **4** above for each camera managed by the NVR.

2.3.3 Camera PTZ setup

This option is available only for cameras that support PTZ. See “SECTION 5 PTZ Controls” on page 50 for more information.

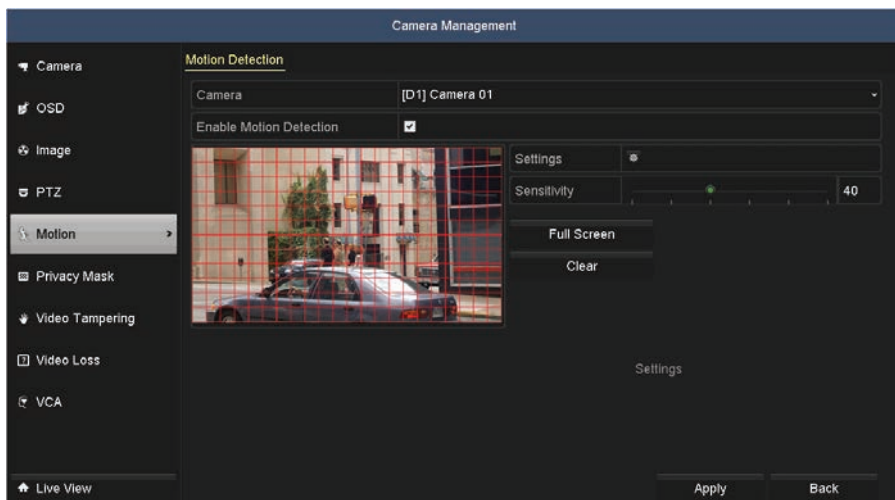


2.3.4 Camera Motion detection setup

Follow the steps to set the motion detection parameters. In the Live view mode, when a motion detection event takes place, the NVR can analyze it and do many actions to handle it. Enabling the motion detection function can trigger certain channels to start recording, or trigger full screen monitoring, audio warning, notify the surveillance center, etc. To setup motion detection for a camera, do the following:

1. Click **Motion** in the left frame to open the Motion submenu.

SECTION 2: INITIAL NVR SETUP



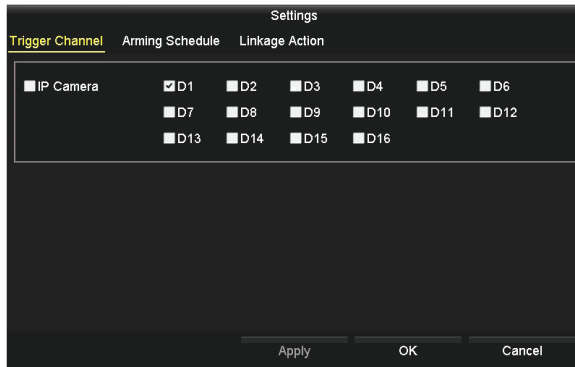
2. In the **Camera** field drop down list, select the camera you want to configure. In the example above, **[D1]IPCamera 01** is selected.
3. Check or un-check the box to **Enable Motion Detection**. If you checked the box, the grid shown over the video image is the area where motion will be detected. To change this area, do the following:

NOTE *Defining a specific area where you want to detect for motion is more efficient for the NVR than searching for motion anywhere in the image.*

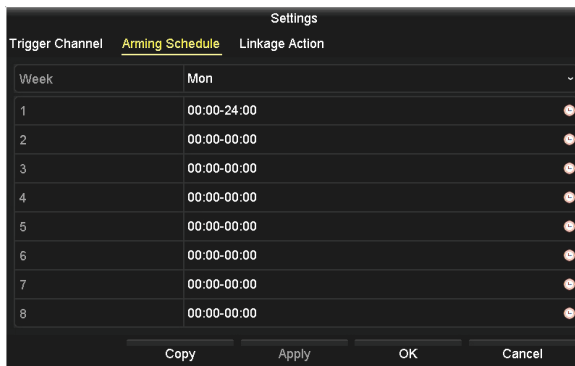
- a. Click **Clear** to erase the grid.
- b. Drag the mouse pointer across a rectangular area of the video image where you want to detect for motion. The area you select will be surrounded by a colored frame. When you release the mouse button, a grid will appear in that area.
- c. Click **Apply** to save your settings.
- d. Adjust the **Sensitivity** slider as needed to detect the motion of objects moving through the zones. When motion is detected in a segment of the grid, the segment is filled with red.

NOTE *Test your settings during broad conditions to ensure that motion in the field of view triggers an action. You may need to return to this menu later to adjust the **Sensitivity** slider to ensure it is working adequately.*

- e. Click **Apply** again to save your settings.
4. Click the **Settings** icon. In the **Trigger Channel** tab:

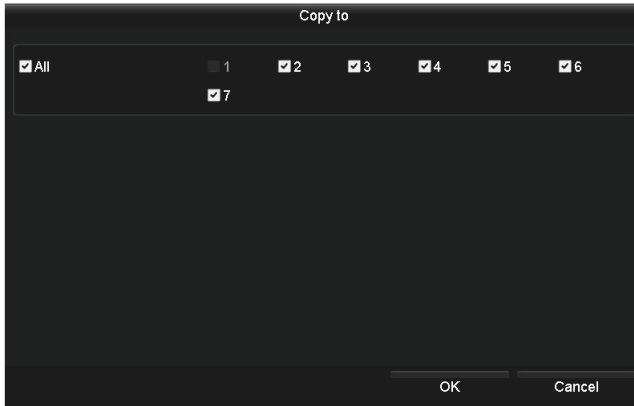


- a. Select the other channels that should trigger recording on this channel, then click **Apply** to save your settings.
- b. Click the **Arming Schedule** tab. In this tab you can define up to eight periods for each day. Periods must not overlap.

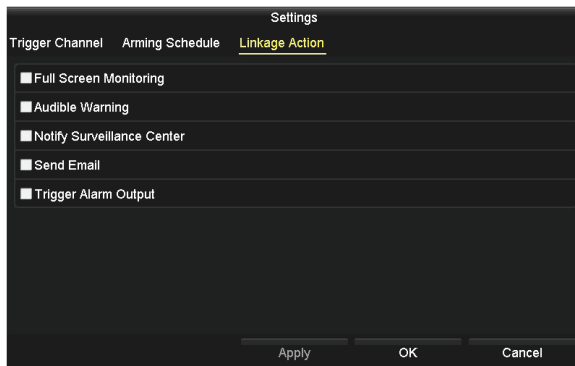


- c. Click the down arrow in the Mon field (see above) to setup the schedule for a different day, and/or click **Copy** to copy the Arming Schedule you setup in the window to other days of the week. Click **OK** to confirm your selections.

SECTION 2: INITIAL NVR SETUP



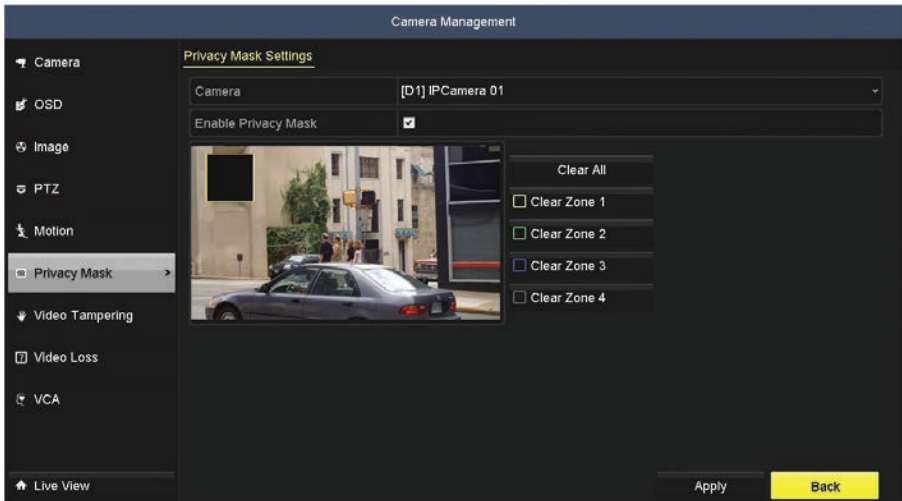
- d. In the Arming Schedule menu, click **Apply** to save the settings.
- e. Click the **Action** tab. In this tab you can cause certain actions to occur when motion triggered recording occurs.



- f. Select the actions you want to occur, then click **Apply** to save your settings, and **OK** to return to the **Motion** menu. The **Notify Surveillance Center** and **Send Email** options require additional network settings.
5. In the **Motion** menu, click **Apply** to save your settings for this camera.
6. Repeat sub-steps **2** through **5** above for each camera managed by the NVR.

2.3.5 Camera Privacy Mask setup

1. Click **Privacy Mask** in the left frame to open the Privacy Mask submenu.



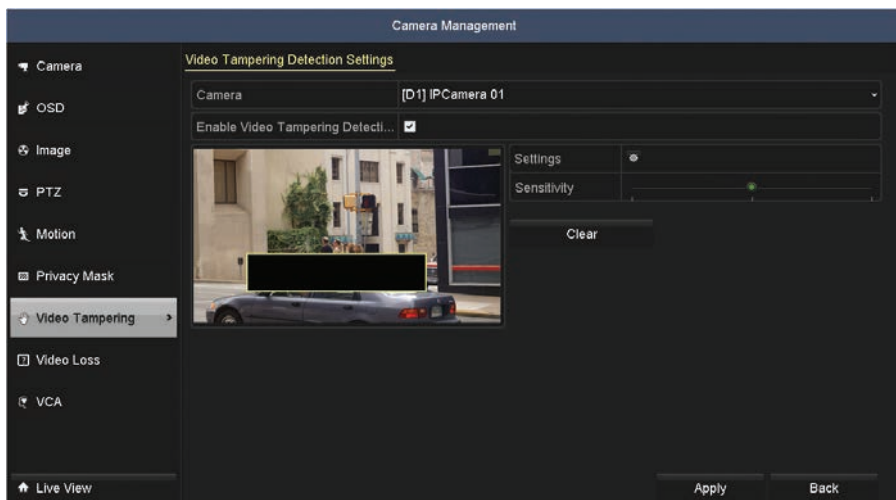
2. In the **Camera** field drop down list, select the camera you want to configure. In the example above, **[D1] IPCamera 01** is selected.
3. Check or un-check the box to **Enable Privacy Mask**. If you checked the box, drag a rectangle across the area of the video that you want to block. In the video image above, the area over the window was blocked.
4. You can create up to four privacy zones for each camera. Use the “clear” buttons to remove zones you created.
5. Click **Apply** to save your settings for this camera.
6. Repeat sub-steps **2** through **5** above for each camera managed by the NVR.

2.3.6 Camera Video Tampering setup

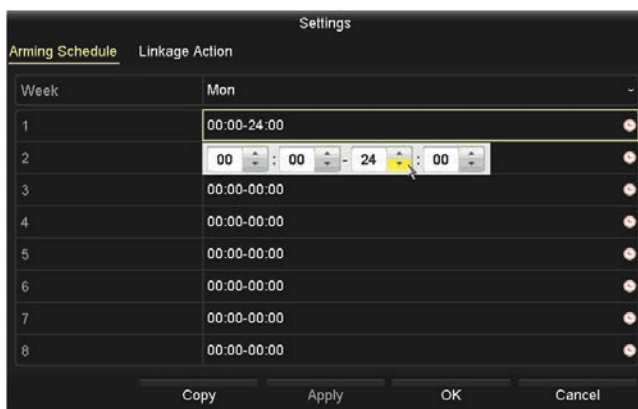
A Video Tampering alarm is created when the lens (an area of the image) is covered. The alarm can cause the NVR to initiate several actions.

1. Click **Video Tampering** in the left frame to open the **Video Tamper Detection Settings** submenu.

SECTION 2: INITIAL NVR SETUP

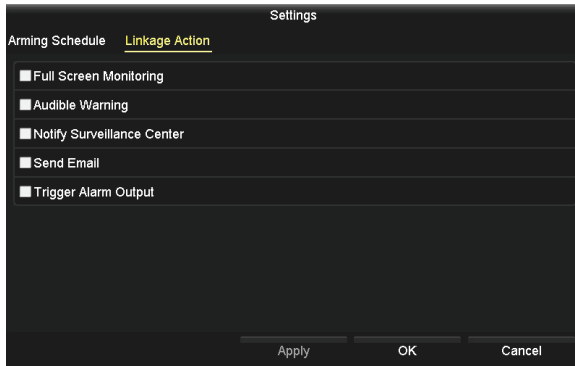


2. In the **Camera** field drop down list, select the camera you want to configure. In the example above, **[D1]IPCamera 01** is selected.
3. Check or un-check the box to **Enable Video Tampering Detection**. If you checked the box, drag a rectangle across the area of the video that you want to monitor.
4. Click the **Settings** icon. In the **Arming Schedule** tab:



- a. In the **Arming Schedule** tab you can define up to eight periods for each day. Periods must not overlap.

- b. Click the down arrow in the Mon field (see above) to setup the schedule for a different day, and/or click **Copy** to copy the Arming Schedule you setup in the window to other days of the week.
- c. Click **Apply** to save the settings.
- d. Click the **Linkage Action** tab. In this tab you can cause certain actions to occur when tampering occurs.



- e. Select the actions you want to occur, then click **Apply** to save your settings, and **OK** to return to the **Tamper-proof** menu. The **Send Email** option require additional network settings. See "SECTION 8 Managing User Accounts" on page 156 for more information.
- f. In the **Tamper-proof** menu, click **Apply** to save your settings for this camera.
- g. Repeat sub-steps **2** through **4** above for each camera managed by the NVR.

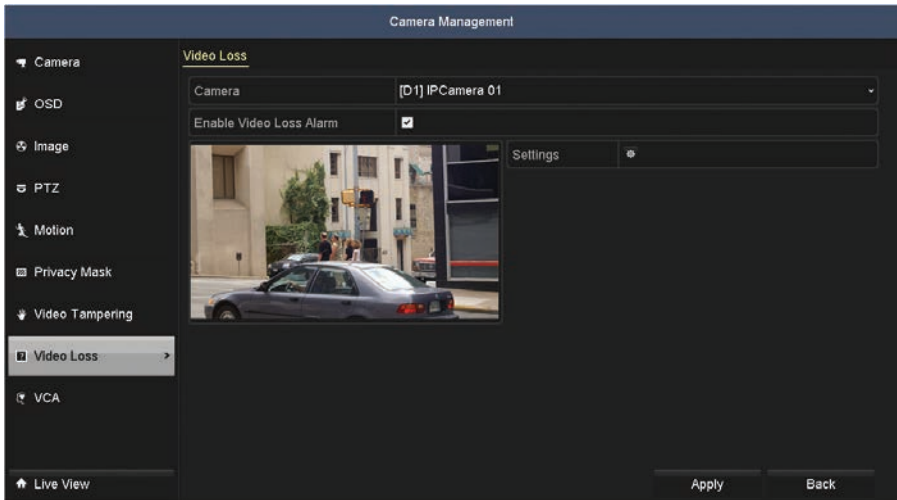
NOTE

*Test your settings during broad conditions to ensure that your tamper-proof settings trigger an action. You may need to return to this menu later to adjust the **Sensitivity** slider to ensure the feature is working properly.*

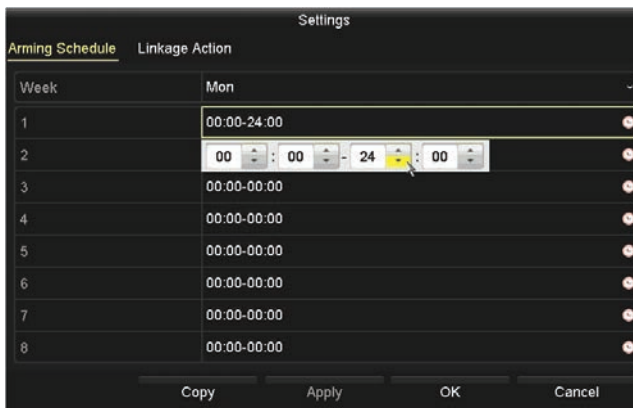
2.3.7 Camera Video Loss setup

1. Click **Video Loss** in the left frame to open the Video loss submenu.

SECTION 2: INITIAL NVR SETUP

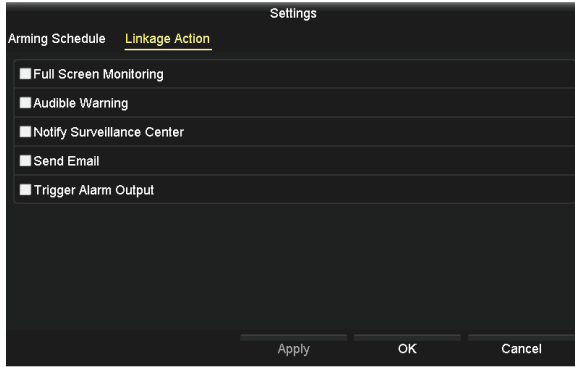


2. In the **Camera** field drop down list, select the camera you want to configure. In the example shown, **IP Camera 1** is selected.
3. Check or un-check the box to **Enable Video Loss**. If you checked the box, do the following:
 - a. Click the **Settings** icon.



- b. In the **Arming Schedule** tab you can define up to eight periods for each day. Periods must not overlap.
- c. Click the down arrow in the Mon field (see above) to setup the schedule for a different day, and/or click **Copy** to copy the Arming Schedule you setup in the window to other days of the week.
- d. Click **Apply** to save the settings.

- e. Click the **Linkage Action** tab. In this tab you can cause certain actions to occur when video loss occurs.



- f. Select the actions you want to occur, then click **Apply** to save your settings, and **OK** to return to the **Video Loss** menu. The **Notify Surveillance Center** and **Send Email** options require additional network settings.
- In the **Video Loss** menu, click **Apply** to save your settings for this camera.
 - Repeat sub-steps **2** through **4** above for each camera managed by the NVR.

2.3.8 VCA

The VCA (Video Content Analysis) features of the NVR are used to configure the VCA features in the camera. The NVR can then retrieve VCA event information from the camera for triggering recording, reporting, generating alerts, etc. The NVR can only configure those VCA features supported by the camera; all VCA features are not supported by all cameras. VCA features supported of the camera can also be configured through remote login to the camera, where available. The recorders support the following VCA features:

Face Detection	Region Entrance Detection	Object Removal Detection	Sudden Scene Change
Line Crossing Detection	Region Exiting Detection	Audio Exception Detection	PIR alarm
Intrusion Detection	Unattended Baggage Detection	Defocus Detection	

For more information about configuring VCA features, refer to “SECTION 6 VCA Features” on page 61.

2.4 Adding cameras manually

IP cameras can connect to the NVR either through the 4-, 8-, or 16-port integrated Ethernet switch on the back panel of the NVR, or through the LAN the NVR is connected to. IP cameras connected to the IP ports on the NVR back panel are automatically added to the system by the NVR. Cameras that exist on the LAN can be added manually through the NVR startup Wizard or Camera menu.


SECTION 2: INITIAL NVR SETUP

The number of cameras connected to the ports on the back of the NVR plus the number of cameras on the LAN added to the NVR cannot exceed the camera limit of the NVR.

NOTE For a lists IP cameras compatible with your NVR, see your product vendor.

Use the following guidelines to add a camera that was discovered on the LAN to the NVR. In the example below, an Alibi camera discovered on the LAN at IP address 192.168.4.3 will be added to NVR channel D2.

1. Open the Camera Management menu. Go to **Main menu | Camera**.



The screenshot displays the 'Camera Management' interface. On the left is a navigation menu with options: Camera, OSD, Image, PTZ, Motion, Privacy Mask, Video Tampering, Video Loss, and VCA. The main area shows a table of IP cameras. The table has columns for Camera ID, Add/Delete, Status, Security, IP Camera Address, Edit, Upgrade, Camera Name, and Protocol. Channel D2 is selected, and a camera with IP 192.168.4.3 is assigned to it. Other channels (D1, D3-D9) are currently empty. Below the table are buttons for Refresh, One-touch Activation, Upgrade, Delete, One-touch Adding, and Custom Adding. At the bottom, there is a checkbox for 'Enable H.265 (For Initial Access)' and a 'Net Receive Idle Bandwidth: 147Mbps' indicator. A 'Reboot' button is also visible at the bottom right.

Camera...	Add/Delete	Status	Security	IP Camera Addr...	Edit	Upgr...	Camera Name	Protoc
D1	—	●	N/A	192.168.4.18	✎	⬆	Camera 01	Alibi
D2	—	▲	N/A	192.168.4.3	✎	⬆	Camera 01	Alibi
D3	—	▲	N/A	192.168.4.4	✎	—	IPCamera 03	Alibi
D4	—	▲	N/A	192.168.4.5	✎	—	IPCamera 04	Alibi
D5	—	▲	N/A	192.168.4.6	✎	—	IPCamera 05	Alibi
D6	—	▲	N/A	192.168.4.7	✎	—	IPCamera 06	Alibi
D7	—	▲	N/A	192.168.4.8	✎	—	IPCamera 07	Alibi
D8	—	▲	N/A	192.168.4.9	✎	—	IPCamera 08	Alibi
D9	—	▲	N/A	192.168.4.10	✎	—	IPCamera 09	Alibi

2. Click on a camera channel where no camera is assigned. To determine if any camera is assigned to a channel, click on the icon in the **Status** column to check the channel status. In the example above, cameras in the list shown above with the yellow alert triangle in the **Status** column are not to any channel.
3. For the example shown above, click on the icon in the **Edit** column for channel D2. The **Edit IP Camera** menu will open.



Configure the Edit menu as follows to add the camera at IP addresses 192.168.4.3:

- In the **Adding Method** line, open the drop down list, and then select **Manual**.
- Click in the Camera IP Address field, and then enter the IP address of the camera to change: 192.168.4.33.



- On the Protocol line, open the drop down list and then select the protocol of the camera shown in the channel table for this camera: **Alibi**. In the window, the User Name for the camera will change to **admin**.
- Click the entry field on the **Admin Password** line, and then enter the camera password for user **admin**.
- Click **OK** to save your settings. The camera list will be updated to show the camera you added.

Camera Management

IP Camera IP Camera Import/Export

Show Password of IP Camera

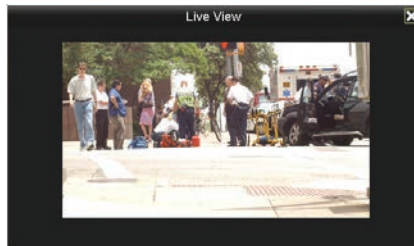
Camera...	Add/Delete	Status	Security	IP Camera Addr...	Edit	Upgr...	Camera Name	Protoc
D1	—	⦿	N/A	192.168.4.18	⚙	⬆	Camera 01	Alibi
D2	—	⦿	N/A	192.168.4.33	⚙	⬆	Camera 01	Alibi
D3	—	⚠	N/A	192.168.4.4	⚙	—	IPCamera 03	Alibi
D4	—	⚠	N/A	192.168.4.5	⚙	—	IPCamera 04	Alibi
D5	—	⚠	N/A	192.168.4.6	⚙	—	IPCamera 05	Alibi
D6	—	⚠	N/A	192.168.4.7	⚙	—	IPCamera 06	Alibi
D7	—	⚠	N/A	192.168.4.8	⚙	—	IPCamera 07	Alibi
D8	—	⚠	N/A	192.168.4.9	⚙	—	IPCamera 08	Alibi
D9	—	⚠	N/A	192.168.4.10	⚙	—	IPCamera 09	Alibi

Refresh One-touch Activ... Upgrade Delete One-touch Adding Custom Adding

Enable H.265 (For Initial Access)

Net Receive Idle Bandwidth: 147Mbps Reboot Back

- f. Verify that the camera status and security are normal for the camera. In the **Status** column, the blue circle with the “play” icon is normal. However, (for Alibi cameras only) the **Security** column indicates a **Risk Pa...** status, meaning that the password has very low security. For Camera channel **D3** shown above, click the icon in the **Security** column to open the **Advanced Set** menu and change the password to one that is secure.
4. For the camera you added, click the “play” icon in the Status column to view live video from the camera. Adjust the direction pan, tilt and horizon of the camera if needed.

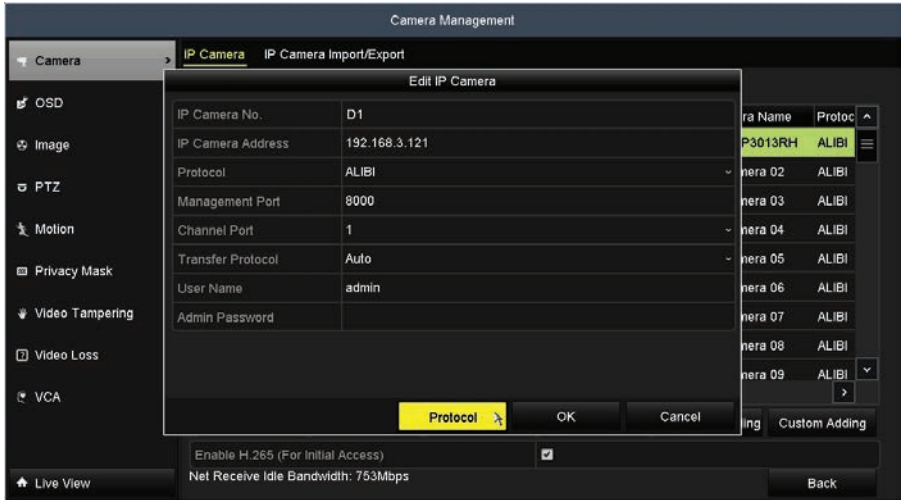


5. Repeat steps 2 through 4 above to add additional cameras.

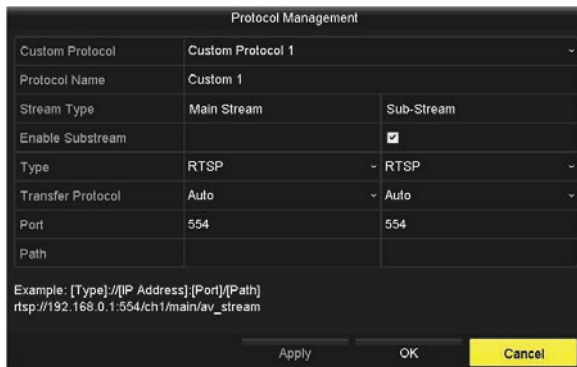
2.4.1 Configuring customized protocols

Protocols in the **Edit IP Camera** window include 16 editable Custom protocols. (Custom Protocol 1 – Custom Protocol 16). It may be necessary (although unusual) to edit a protocol for a camera you are using. You must create the custom protocol before you configure the camera to use it. To create a Custom protocol:

1. Open the **Edit IP Camera** menu for the camera by clicking the icon in the **Edit** column. In the example below, the camera at IP address 192.168.4.2 was selected.



2. Click the Protocol button at the bottom of the window.



3. Edit the **Protocol Management** window as needed. In the window shown above, **Custom Protocol 1** was selected from the drop-down list. Refer to the camera manufacturer for the best options to choose here.
4. Click **Apply**, and then **OK** to save the changes you made to the custom protocol.

Edit IP Camera	
IP Camera No.	D1
Adding Method	Manual
IP Camera Address	192.168.4.18
Protocol	Alibi
Management Port	SANYO
Channel Port	SONY
Transfer Protocol	VIVOTEK
User Name	ZAVIO
Password	Custom 1
	Custom 2
	Custom 3

- Open the **Protocol** drop down list and select one of the unused custom protocols (Custom 1). See above.
- Click the **User Name** field, and then enter an administrative User Name for the camera.

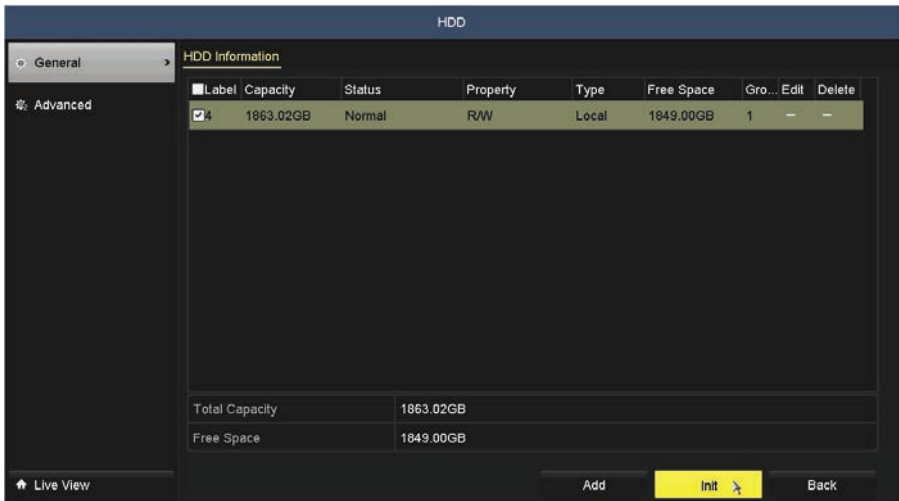
Edit IP Camera	
IP Camera No.	D1
Adding Method	Manual
IP Camera Address	192.168.4.18
Protocol	Custom 1
Management Port	0
Channel Port	1
Transfer Protocol	Auto
User Name	admin
Password	

- Similarly, enter the **Password** for the User name in the field below.
 - Click **OK** to save the settings.
- The NVR will now use the Custom 1 protocol for the camera you configured.

2.5 Checking HDD status

Check the status of the HDD installed in the NVR to assure it is functioning normally.

- Open the HDD Information display. Go to **Menu | HDD | General**.



- Check the status of the HDD. If the status is:
 - **Normal** or **Sleeping** - The HDD is working normally.
 - **Uninitialized** or **Abnormal** - Initialize the HDD before continuing. Check the select box of the HDD to initialize, then click the **Init** button at the bottom of the screen.
 - **Failed** - If the HDD failed during or after initialization, replace the HDD.
- If you installed a new HDD in your NVR chassis, select the HDD in the window then click **Init** to initialize it for use. Allow the initialization procedure to complete before continuing.

2.5.1 Additional HDD features

NVR storage (HDDs) is highly configurable. You can simply save data to the internal HDD(s) in the chassis, or add network based NAS or IP SAN devices to the system and save recordings and other data there. You can also define where data for each camera or groups of cameras is saved, and have 16 different storage groups. Before an HDD is used by the NVR, it must be initialized by the recorder. Preconfigured HDD(s) are already initialized.

If you add an internal HDD to the recorder, or replace an HDD in the recorder, it must be initialized before it can be used. See “11.1 Initializing HDDs” on page 194 for more information.

If HDD storage problems occur, the recorder includes several maintenance features to check the integrity of the storage. See “11.4 HDD Maintenance” on page 203 for more information.

2.6 Configuring Exception Alarms

The NVR monitors for and responds to certain system-related alarm conditions (exception alarms). Monitoring for and response to these exceptions are configurable.

Exception alarm conditions include:

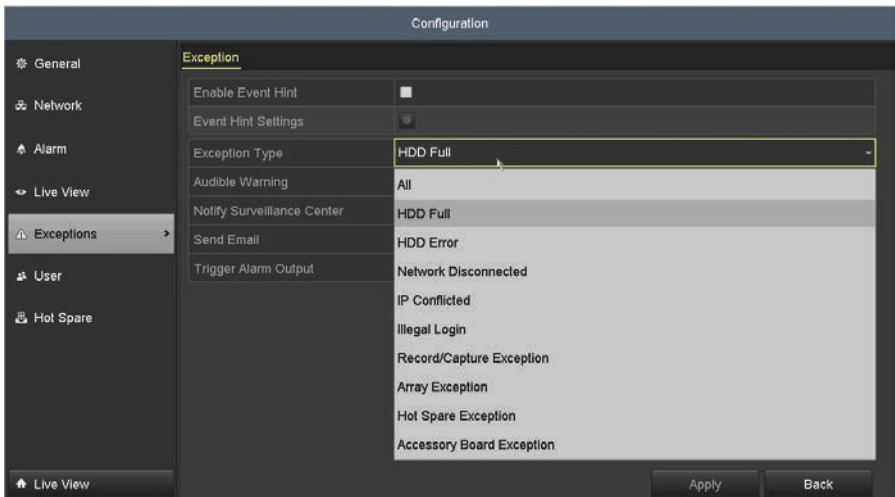
- **HDD Full:** The HDD is full.
- **HDD Error:** Writing HDD error or unformatted HDD.
- **Network Disconnected:** Disconnected network cable.
- **IP Conflicted:** Duplicated IP address.
- **Illegal Login:** Incorrect user ID or password.
- **Record/Capture Exception:** Indicates that there is no more HDD space and overwrite is not enable.
- **Array Exception:** Indicates that a RAID array has failed.
- **Hot Spare Exception:** Indicates that a Hot Spare drive has failed.
- **Accessory Board Exception:** Indicates that either the HDMI decoding board or SFP/Alarm I/O expansion board has failed.

Responses to exception alarms include:

- **Audible Warning:** Trigger an audible beep when an alarm is detected.
- **Send Email:** Send an email with alarm information to a user or users when an alarm is detected.
- **Trigger Alarm Output:** Trigger an alarm output when exception is detected.

To configure exception alarms:

1. Open the **Exception** menu. Go to **Menu | Configuration | Exceptions**.



2. On the **Exception Type** line, open the drop down list and select the exception condition you want to configure. If you select **All**, all exception conditions will be treated the way you configure the response.
3. Select the response options you want to use.
4. Click **Apply** to save your settings.
5. Repeat these steps for other Exception Types you want to configure.

2.7 Setting sensor alarms

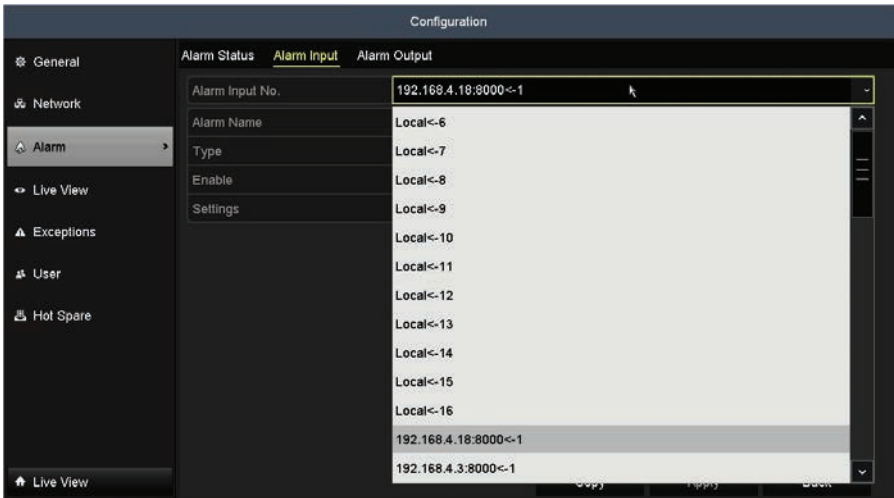
Use this subsection to configure how the NVR reacts to sensor alarms wired to the camera alarm in/out terminations. Alarm inputs can be normally open (N.O.), or normally closed (N.C.).

1. Open the **Alarm Input** menu. Go to **Menu | Configuration | Alarm | Alarm Input** tab.



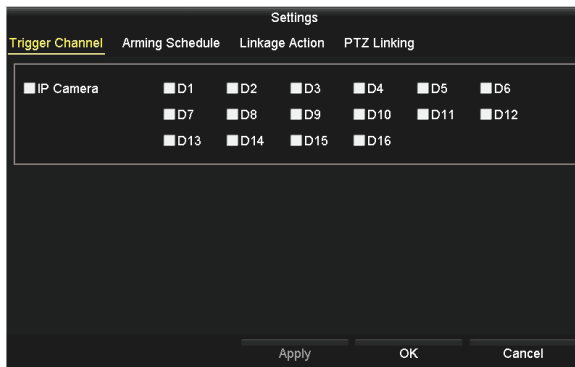
2. Open the **Alarm Input No.** drop down list and select the alarm input you want to configure. In the example above, a camera associated the NVR at **192.168.4.18 (D2)** is selected.

SECTION 2: INITIAL NVR SETUP



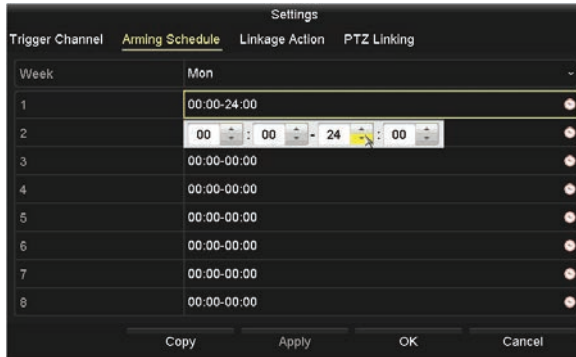
Open the Type drop down list and select the active state of the alarm. Choose either **N.O.** for normally open, **N.C.** for normally closed.

3. Check either the **Enable** box to enable the alarm., or the **Enable One-key Disarming** box to arm and disarm the unit by holding down the **ESC** key.
4. Click **Settings** icon to open the alarm response Settings menus.
5. Select the **Trigger Channel** tab, if not selected. Select one or more camera channels which will start to record or expand to full-screen monitoring when the external alarm is active.

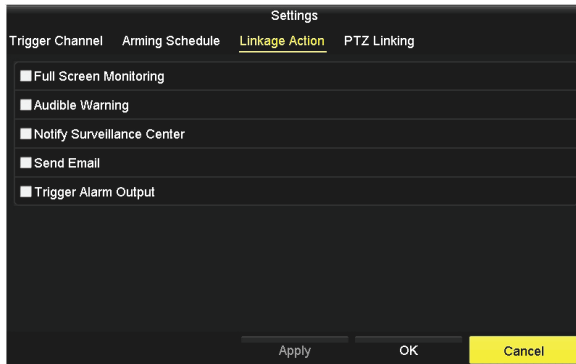


6. Click **Apply** to save the settings.

- Click the **Arming Schedule** tab. In this tab you can define up to eight periods for each day. Periods must not overlap.

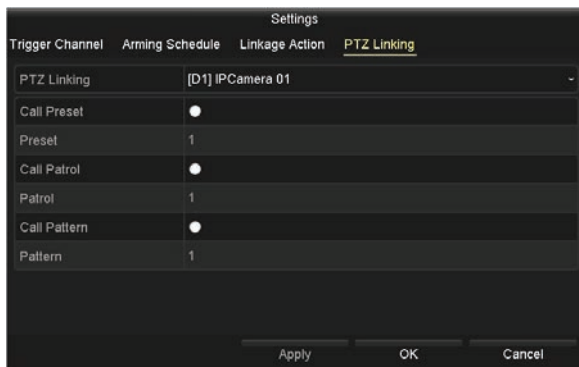


- Click the down arrow in the Mon field (see above) to setup the schedule for a different day, and/or click **Copy** to copy the Arming Schedule you setup in the window to other days of the week.
- Click **Apply** to save the settings.
- Select the **Linkage Action** tab to set up alarm response actions of the alarm input.



- In the **Linkage Action** menu, select the actions you want to occur when the alarm is active, then click **Apply** to save the settings. If PTZ cameras are not installed on your system, click **OK** to return to the **Alarm Input** menu.
- If PTZ cameras are installed on your system, select the **PTZ Linking** tab to set up alarm response actions of PTZ cameras.

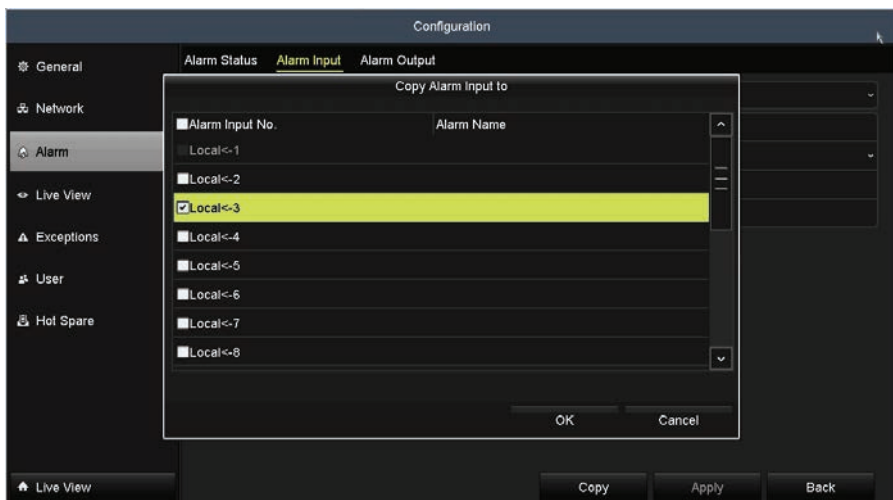
SECTION 2: INITIAL NVR SETUP



NOTE

- Verify that your PTZ or speed dome camera supports PTZ linkage before making these settings.
- One alarm input can trigger presets, patrols or patterns on more than one channel.

13. Select the preferred options in the **PTZ Linking** menu, then click **Apply**.
14. Click **OK** to return to the **Alarm Input** menu.
15. Repeat steps 3 - 15 above to configure additional alarm inputs connected to your NVR. You can also copy an the alarm input setup you saved to other alarm inputs. To do so:
 - a. Click the **Copy** button at the bottom of the Alarm Input menu.



- b. Check the boxes for the alarm inputs you want to copy the configuration to.
- c. Click **OK** to save your settings.

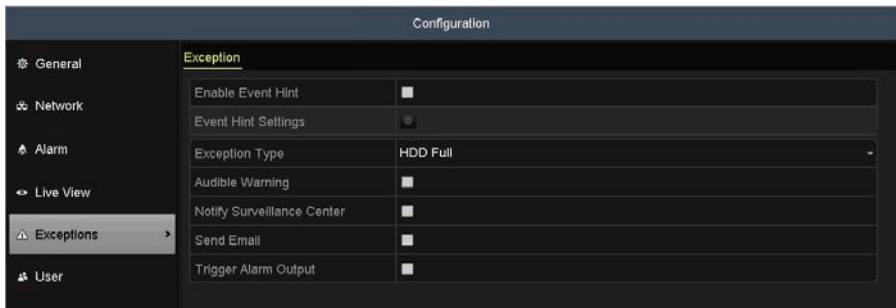
2.8 Setting alarm response actions


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

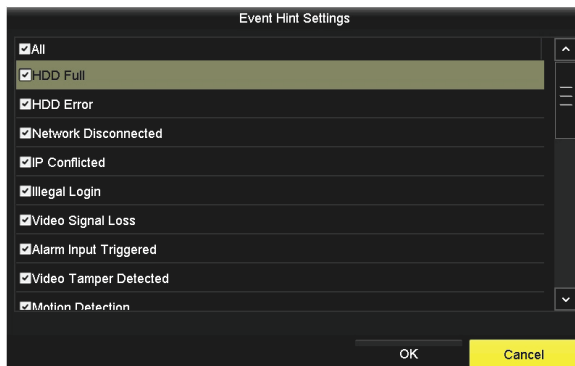
Event Hint Display

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

1. Open the **Exceptions** menu. Go to **Menu | Configuration | Exceptions**.



2. Check the **Enable Event Hint** box. See above.
3. Click the  icon to set the type of event to be displayed on the image.

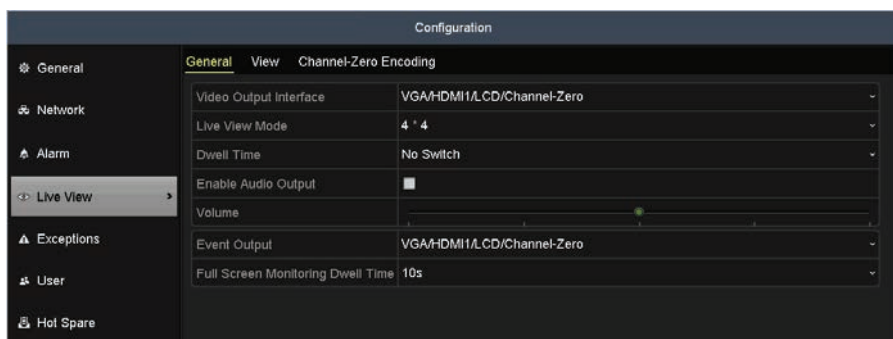


4. Select the type of event you want to be displayed on the image.
5. Click **OK** to save your settings.

Full Screen Monitoring

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

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** and then changing the **Full Screen Monitoring Dwell Time** setting.



Auto-switch will terminate when the alarm condition ends. The NVR will revert to the Live View interface.

NOTE You must select the channel(s) you want to display with full screen monitoring in the "Trigger Channel" settings menu.

Audible Warning

Trigger an audible beep when an alarm is detected.

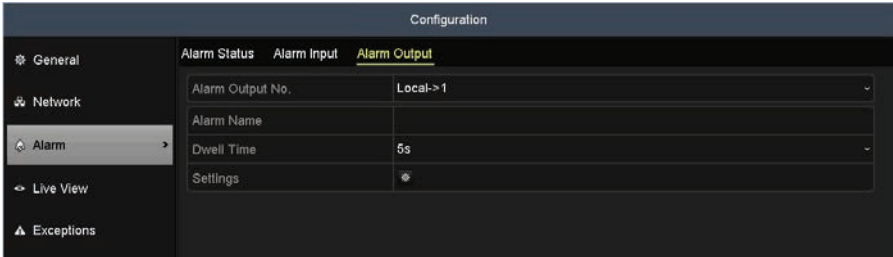
Email Linkage

Send an email with alarm information to a user or users when an alarm is detected. The Email networking feature must be configured for email to be sent.

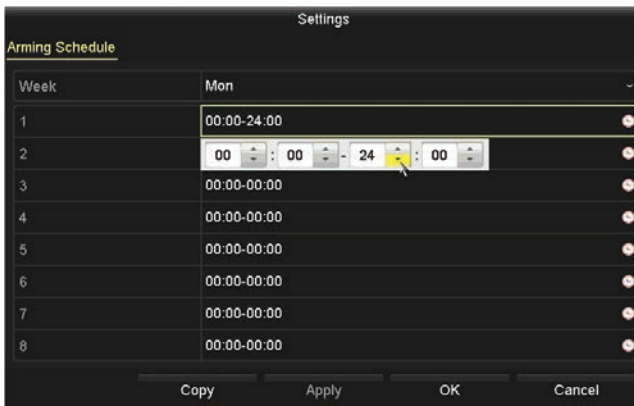
Trigger Alarm Output

Trigger an alarm output when an alarm is triggered.

1. Open the Alarm Output menu. Go to **Menu | Configuration | Alarm | Alarm Output**.



2. In the screen above, open the **Alarm Output No.** drop down list, and then select the alarm output you want to configure.
3. Select an alarm output, set alarm name, then specify a dwell time.
4. Click the **Settings** icon (⚙️) to open the **Arming Schedule** menu.



5. In the **Arming Schedule**, you can define up to eight periods for each day. Periods must not overlap.
6. Click the down arrow in the **Mon** field (see above) to setup the schedule for a different day, and/or click **Copy** to copy the Arming Schedule you setup in the window to other days of the week.
7. Click **Apply** to save the settings, then click **OK** to return to the **Alarm Output** menu.
8. Repeat steps 3 - 7 above to configure additional alarm outputs connected to your NVR. You can also copy an the alarm input setup you saved to other alarm inputs:
 - a. Click the **Copy** button at the bottom of the Alarm Input menu.

SECTION 2: INITIAL NVR SETUP

Copy Alarm Output to

<input type="checkbox"/> Alarm Output No.	Alarm Name
<input checked="" type="checkbox"/> Local->1	
<input type="checkbox"/> Local->2	
<input type="checkbox"/> Local->3	
<input type="checkbox"/> Local->4	
	192.168.4.18:8000->1
<input type="checkbox"/> 192.168.4.3:8000->1	

OK Cancel

- b. Check the boxes for the alarm outputs you want to copy the configuration to.
- c. Click **OK** to save your settings.

SECTION 3

Startup, Shutdown, Reboot

After the NVR and cameras are installed, the NVR system must be configured to function in the surveillance mode(s) that best serve your needs. This chapter includes the essential steps to get your system running, including configuring the NVR date and time, and setting up the LAN interface, cameras and recording modes. Advanced features, including remote access, video export, adding user names and setting user permissions, etc. are described in later sections of this manual.

3.1 Starting Up, Shutting Down and Rebooting the NVR

3.1.1 Startup

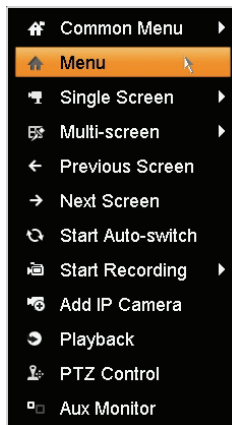
Proper startup and shutdown procedures are essential for getting the most out of your NVR. To startup:

1. Check the power cable is plugged into a standard electrical outlet. It is HIGHLY recommended that an Uninterruptible Power supply (UPS) be used in conjunction with the device.
2. Rock the **POWER** switch on the back panel to the on ("I") position. The Power indicator LED on the front panel should turn green indicating that the unit is powered on.
3. After startup, the Power indicator LED remains green. A splash screen will appear on the monitor.

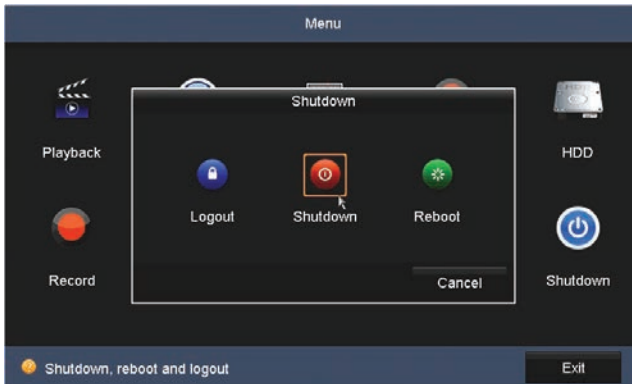
3.1.2 Shutdown

To shut down the NVR:

1. Right click anywhere on the desktop to open the pop-up window, then select **Menu**.



2. If a **Login** window opens, select a User Name with administrative privileges, enter the appropriate Password, then click **OK**.
3. In the **Menu** window, click the **Shutdown** icon, then click **Shutdown** in the pop-up window.

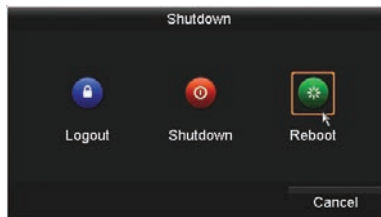


4. Click **Yes** in the **Attention** window.
5. When the message **Please power off!** appears, or three minutes have lapsed, rock the power switch on the back panel to the off ("0") position.

3.1.3 Rebooting the NVR

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

1. Open the Shutdown menu by clicking **Menu | Shutdown**.
2. In the **Menu** window, click the **Shutdown** icon, then click **Reboot** in the pop-up window.
3. Click **Yes** in the **Attention** window.



SECTION 4

Live View Interface

The Live View interface is the primary camera viewing and monitoring mode. It can be configured to present video from the cameras configured in the system singularly or in multi mode, or using a “patrol” feature wherein video from each of a select group of cameras is displayed singularly and sequentially, with each camera view shown for a preset duration (dwell). The Live View screen can be configured to display up to 36 channels at the same time with options to display 1, 4, 6, 8 or more (depending on the NVR capacity) camera channels concurrently, or playback recorded video.



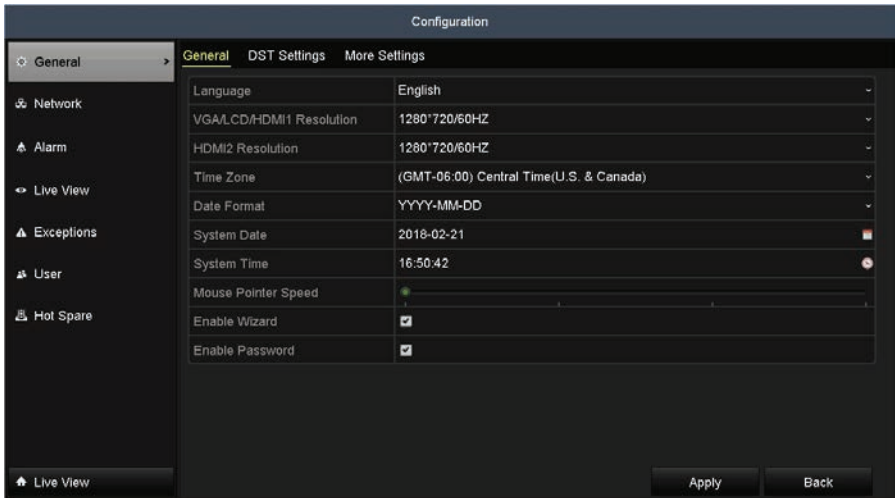
*Live View 2 * 2 multi-screen display*

Each camera channel displayed on the Live View screen may contain one, two, or no status icons in the upper-right corner of the viewing frame.

The recorder can support up to two monitors if it provides both VGA and HDMI video out ports.

4.1 Setting monitor resolution

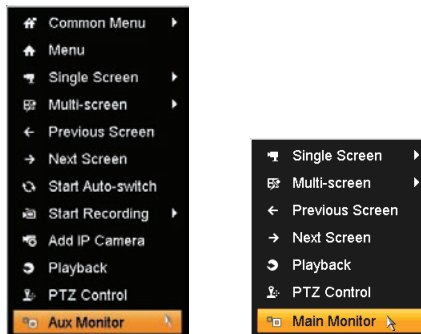
The recorder supports VGA monitor resolutions up to 1080p (1920 x 1080 pixels), and HDMI resolutions up to 4K (3840 x 2160 pixels). To set the monitor resolution, open the **Menu | Configuration | General** display.



Use the screen above to select the resolution for the VGA and HDMI monitors you are using, and then click the **Apply** button at the bottom of the screen.

4.2 Dual monitor support - Main and Aux monitors

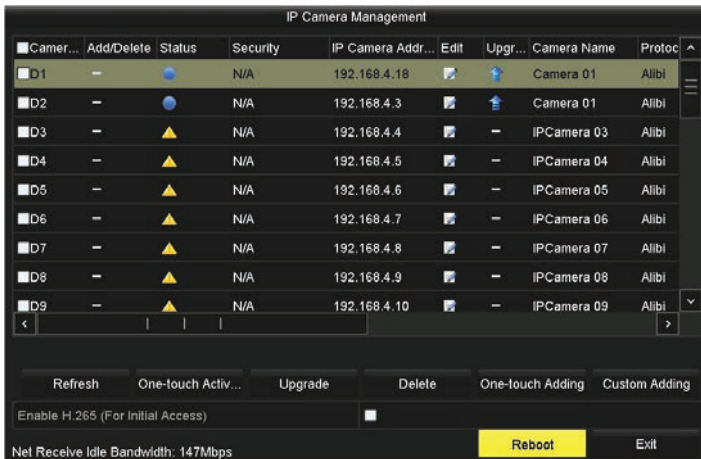
If the recorder supports two monitors (HDMI [default or Auto] and VGA), you can configure either to be the “**Menu Output Mode**” monitor with the other being the “**Aux**” monitor (see “4.2.1 Setting Menu Output Mode” on page 43). The pop-up menu on the **Main** monitor can be used to configure the recorder, control the number of Live View channels, playback video and control PTZ cameras. The pop-up menu on the **Aux** monitor can only be used to control the number of Live View channels, playback video and control PTZ cameras. From the **Main** monitor, you can switch control (mouse pointer and menus) to the **Aux** monitor screen, and vice-versa. The Live View pop-up menus for the **Main** monitor and **Aux** monitor are shown below.



Pop-up menus for the Main monitor (left) and Aux monitor (right)

Clicking one of the items listed produces the result described below.

- **Menu:** Opens the configuration menu window. See “SECTION 7 Record, Playback and Video Backup” on page 109.
- **Single Screen:** showing only one camera channel on the monitor. Open the drop-down list to select the camera channel you want to view.
- **Multi-screen:** opens a submenu where you can choose from several multi-channel screen configurations, including **2*2, 1+5, 1+7, 3*3**. etc. Options depend on the channel capacity of the recorder.
- **Previous screen:** Move to the screen displayed previously.
- **Next screen:** Move to the screen displayed after the current one.
- **Start Auto-switch:** the screen is automatically switched from one camera channel to the next. You must set the dwell time before enabling auto-switch. Go to **Menu | Configuration | Live View | Dwell Time**.
- **Start Recording:** Select Normal Record and Motion Detection record from the drop-down list.
- **Add IP Camera:** Opens the IP Camera Management menu to add a camera to the system. See “2.4 Adding cameras manually” on page 23 for usage of this display.

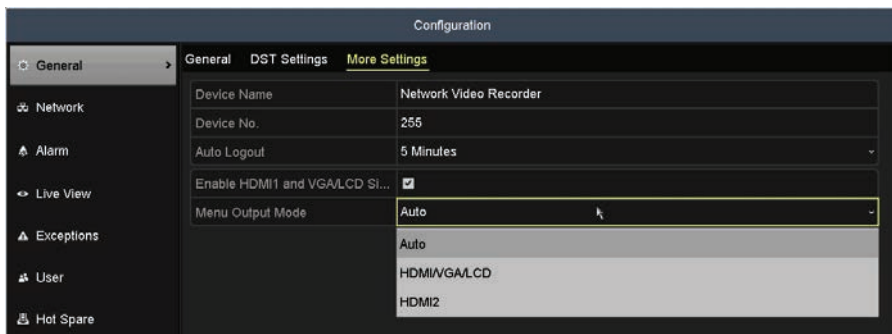


- **Playback:** Opens a playback menu where you can playback video recorded at a specific time of the day.
- **PTZ Control:** The Live View window for the channel expands to full screen and opens the PTZ control menu.
- **Aux/Main Monitor:** Switches menus to other monitor in dual monitor mode.

4.2.1 Setting Menu Output Mode

The Menu Output Mode is configured with the **Menu | Configuration | More Settings** display.

SECTION 4: LIVE VIEW INTERFACE



Menu Output Mode provides three options:

- **Auto:** Main monitor mode is assigned to either the HDMI video output port or the VGA video output port. If monitors are attached to both ports, the HDMI port is the Main monitor. If only one monitor (HDMI or VGA) is attached to the recorder, that monitor is assigned the main monitor.
- **HDMI:** The HDMI port is always assigned as the Main monitor. The mouse pointer and menu control can be switched to the Aux monitor. If no monitor is attached to the HDMI port, there is no visible mouse or menu control of the system.
- **VGA:** The VGA port is always assigned as the Main monitor. The mouse pointer and menu control can be switched to the Main monitor. If no monitor is attached to the VGA port, there is no visible mouse or menu control of the system.

When changing from one **Menu Output Mode** to another, the recorder must be rebooted.

The behavior of **Main** and **Aux** modes is shown in the table below.

Main Output Mode	HDMI monitor	VGA monitor	Notes
AUTO	Main	Aux	
HDMI	Main	Aux	
VGA	Aux	Main	
AUTO	Main	Disconnected	
AUTO	Disconnected	Main	
HDMI	Disconnected	On	No mouse or menu control on VGA monitor
VGA	On	Disconnected	No mouse or menu control on HDMI monitor

When menus are switched to the Aux monitor, nothing can be performed on the Main monitor and vice-versa.

4.3 Live View settings

Live View settings can be customized according to differing needs. You can configure the screen frame split, placement of camera channels on the screen, dwell time for screen to be shown, mute or turning on the audio, the screen number for each channel, etc.

1. Open the Live View Settings menu. Go to **Menu | Configuration | Live View**



Adjust the settings in the screen as needed:

- **Video Output Interface:** Designates the output to configure the settings for. Options include VGA/HDMI1/LCD/Channel-Zero and HDMI2.
 - **Live View Mode:** Designates the display mode (screen split) to be used for Live View. **1 * 1** is a single camera view. Several options are available.
 - **Dwell Time:** The time in seconds to dwell between switching channels when auto-switch is enabled in Live View.
 - **Enable Audio Output:** Enables/disables audio output for the selected video output.
 - **Volume:** When Audio Output volume is enabled, use the slider to adjust the volume.
 - **Event Output:** Designates the output to show event video. Option includes only VGA/HDMI.
 - **Full Screen Monitoring Dwell Time:** The time in seconds to show alarm event screen.
2. After changing settings in the screen shown above, click **Apply**, and then click **Back**.
 3. Click the **View** tab at the top of the screen.



4. Click the single- or multi-screen select icon for the screen split you prefer. In the example shown above, a 16-screen view is selected.
5. Click a viewing screen, then double-click the camera in the list on the left that you want to show there. When the selection is made, the label in the viewing screen changes to the camera channel number. You can also click an icon to Start or Stop Live view of all channels.
6. Click the **Apply** button to save your settings.

4.4 Using the mouse in Live view

Table 1. Mouse operation in Live view





Name	Description
Menu	Enter the main menu of the system by right clicking the mouse.
Single Screen	Switch to single full screen by choosing channel number from the drop down list.
Multi-screen	Select the screen layout 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 feature.
Start Recording	Start continuous recording or motion detection recording of all channels.
Add IP Camera	Enter the IP Camera Management interface to add cameras.

Name	Description
Playback	Enter the playback interface and start playing back the video of the selected channel.
Output Mode	Select one of four output modes: Standard, Bright, Gentle or Vivid.

- NOTE**
- The dwell time of the live view configuration must be set before using Start Auto-switch.
 - If the corresponding camera supports intelligent function, the Reboot Intelligence option is included when right-clicking the mouse on this camera.

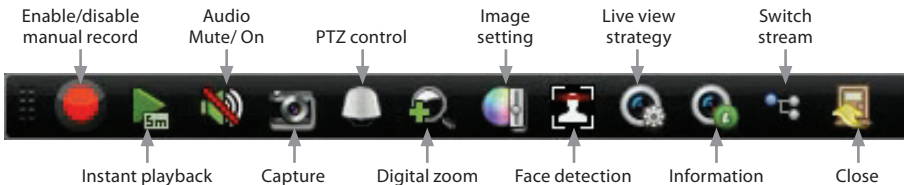
4.5 Live View Status icons

In the **Live** view mode, icons can appear in the upper-right of the screen for each channel, showing the status of the record and alarm in the channel.

Icon	Type	Reason
	Alarm	This icon appears in the upper right corner of the live video stream. It results from video loss, video tampering, motion detection, sensor alarm, etc.
	Record	Manual record, schedule record, motion detection or alarm triggered record
	Record and Alarm	Both alarm and record status
	Event/Exception	For the occurrence of motion detection, sensor alarm or exception information. This icon appears at the lower-left corner of the screen. Click on the icon to display the event/exception reason.

4.6 Quick Setting Toolbar

Left-clicking the mouse on a viewing frame opens a Quick Setting Toolbar at the top or bottom of the frame.



Instant Playback: Plays what was recorded in the previous five minutes. Nothing is played if a recording was not made at that time.

Capture: Click to create a snapshot of the Live View image.

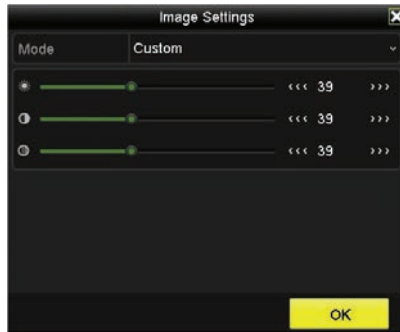
SECTION 4: LIVE VIEW INTERFACE

PTZ Control: This icon is dark if PTZ control is not supported.

Digital Zoom: After selecting this option, a faint slider bar with ⊕ (zoom in) and ⊖ (zoom out) icons will appear in the upper left corner of the video image. To use this feature, do one of the following:

- Click on the spot in the video image, and then use the mouse scroll wheel to zoom in or out at that spot.
- Click the ⊕ icon to zoom in on the video image, and then drag the image the video image with the mouse to zoom on another spot. Click ⊖ to zoom out.
- Drag the slider on the slider bar up or down to zoom in or out, and then drag the video image with the mouse to zoom on another spot.
- Right-click the mouse to cancel the zoom feature.

Image Settings: Click this icon to open menus for creating customized setting for the brightness, contrast, saturation and hue of the camera image. After making an adjustment on in this menu, the NVR will respond within a few seconds. Click **OK** when your adjustments are complete.

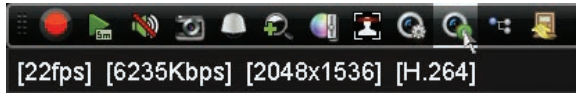


Face Detection: Identifies faces detected in the live view image. After selecting this option, click **Yes** in the pop-up window.

Live View Strategy: Use this feature to select Real-time, Balanced, Fluency. These features can improve the display of the camera channels.



Information: Hover the mouse over this icon to see the frame rate, bit rate, and resolution of the image.



3D Positioning: Clicking a spot can direct the camera position the spot in the center of the image. When a rectangular area is selected with the left mouse button, the camera will move to its center and enlarge it. Right click the mouse to zoom in. The scroll wheel can control lens zoom. Mouse cursor movement can also control zoom effects.

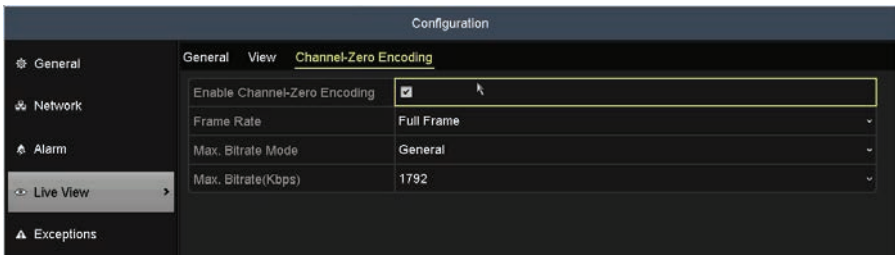
Switch to Sub-Stream: Hover the mouse over this icon to play the sub-stream video. Repeat this action to return to the Main stream.

Trigger Alarm Out: Activates on the camera Alarm Out signal (from a camera with Alarm Out feature).

4.7 Channel-Zero Encoding

Use the Channel-Zero Encoding menu to configure the NVR for viewing multiple video channels simultaneously with a remote client. With this features you can decrease the bandwidth requirement without affecting the image quality. To use Channel-Zero Encoding:

1. Open the **Channel-Zero Encoding** menu. Go to **Menu | Configuration | Live View | Channel-Zero Encoding**.



2. Check the box to **Enable Channel Zero Encoding**.
3. Configure the **Frame Rate**, **Max. Bitrate Mode** and **Max. Bitrate** as needed.
4. Click **Apply**.

After setting Channel-Zero Encoding, you can see up to 16 channels of live video on one screen of the remote client.

SECTION 5


PTZ Controls

PTZ controls are used to control the Pan, Tilt and Zoom features of PTZ cameras. PTZ cameras can usually be configured to point at preset targets (called Presets), perform patrols (i.e., to move from preset to preset), and record and save patterns, a recording of the motion of a camera.

PTZ controls are also used with special features of non-PTZ cameras that have remotely controlled (motorized) zoom, focus and iris adjustments.

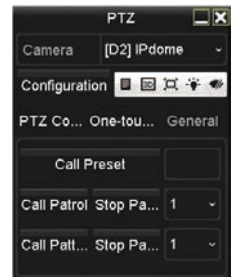
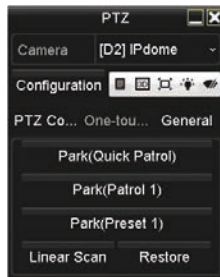
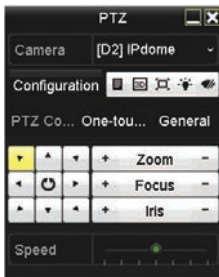
5.1 PTZ Control Panel

You can enter the PTZ control panel either of two ways:

- In the **Menu | Camera | PTZ** menu, click the **PTZ** button on the lower-right corner. It is next to the **Back** button.
- In the **Live View** mode left click on the image from the PTZ camera, and then click the PTZ Control icon  on the Quick Settings toolbar.

The PTZ control panel has Configuration toolset for quickly controlling the camera. A description of these Configuration icons is shown in the table below.

The PTZ menu includes three tabs: **PTZ Control**, **One-touch**, and **General**.



PTZ Control tab

The PTZ Control tab is used to manually move the camera with direction buttons, and to control Zoom, Focus and Iris.

One-touch tab

The One-touch tab is used to initiate either of three kinds of park operations. Park operations can be initiated after a preset period of inactivity of the camera, referred to as Park Time.



















- **Park (Quick Patrol):** The camera initiates a patrol from Preset 1 to Preset 32 (if predefined) after the camera park time. Undefined presets are skipped.
- **Park (Patrol 1):** The camera initiates a start move according to the Patrol 1 after the camera park time. Patrol 1 must be predefined.
- **Park (Preset 1):** The camera initiates a move to Preset 1 after the camera park time. Preset 1 must be predefined.

Park time is set through the camera configuration interface. The default park time is 5 seconds.

You can also select **Restore**. Restore reboots the camera and restores the factory settings for Presets and Patrols.

General tab

The General tab is used to call a preset, patrol, and pattern movement. These movements must be preconfigured.

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

PTZ control panel icons

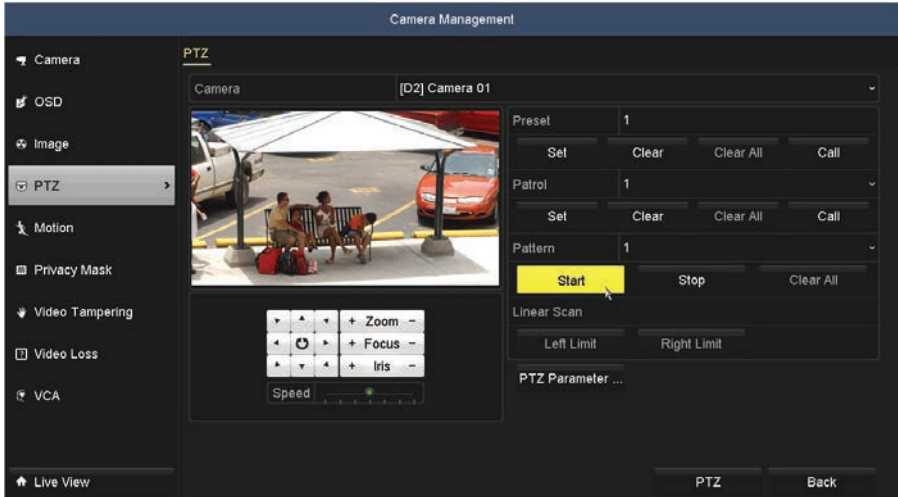
5.2 Configuring PTZ settings

Follow the procedure to set the parameters for control of a PTZ camera installed in the system. Setup of the PTZ parameters should be done before you control the PTZ camera. For a list of compatible cameras, see your product vendor.

SECTION 5: PTZ CONTROLS

If PTZ cameras are controlled through the RS-485 interface, check that the PTZ and the NVR are connected and configured properly.

1. Open the PTZ menu. Go to: **Menu | Camera | PTZ**.



2. Choose the camera for PTZ setting in the Camera drop down list.
3. Click the PTZ Parameter ... button.



- If you are controlling the camera through the RS-485 network, enter the PTZ Protocol and Address parameters of the PTZ camera as needed.
- Click **OK** to save the settings and close the window.

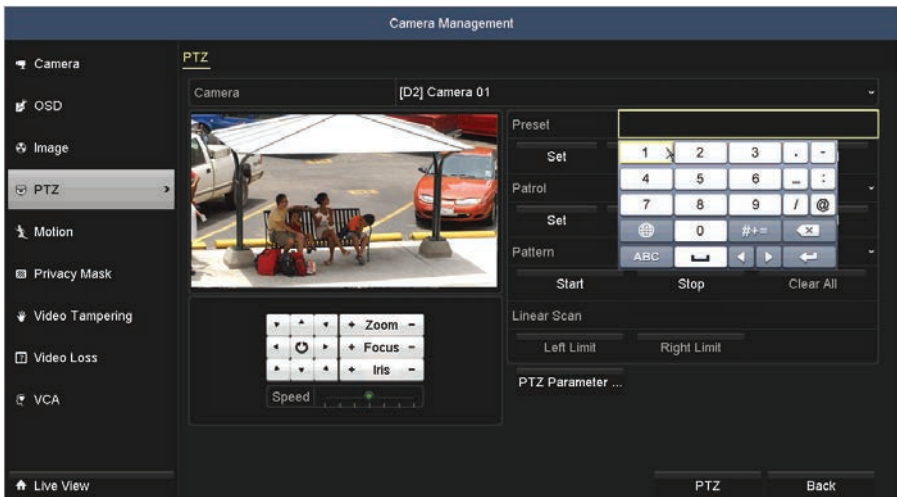
5.3 Setting PTZ presets, patrols and patterns

NOTE *The presets, patrols and patterns you configure must be supported by the PTZ protocols.*

5.3.1 Customizing Presets

A Preset is a pre-configured setting of a PTZ camera that usually includes, it's direction, zoom, iris setting and focus, and may include other settings. Follow the steps to set the Preset location which you want the PTZ camera to point to when an event takes place. You can create up to 255 presets, numbered 1 .. 255.

- Open the PTZ settings menu. Go to: **Menu | Camera | PTZ**.
- Use the directional button to point the camera at the position where you want to create a preset.
- Click the field to the right of **Preset**, use the pop-up virtual keyboard to enter a number to assign to the preset, and then click the **↵** key.



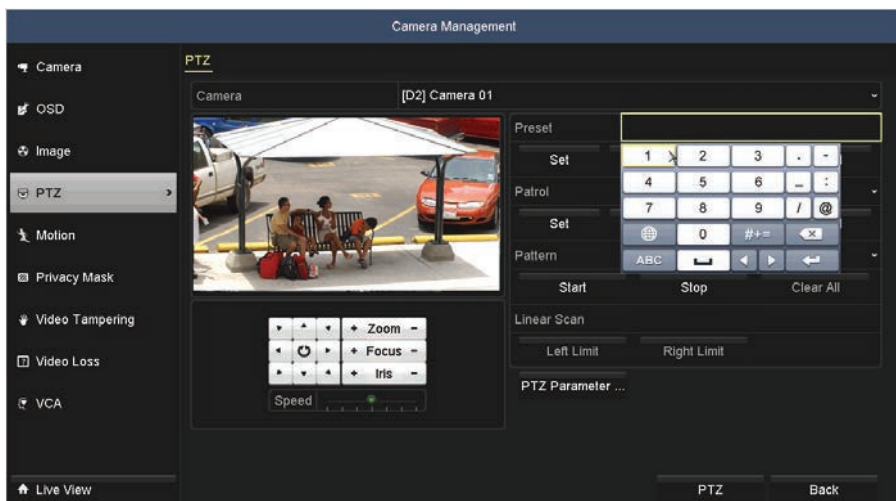
- Click the **Set** button (just beneath the Preset line) to save the preset.

- Repeat the steps 2 – 4 to create more presets. If the number of the presets you want to save is more than 17, you can click [...] and choose the available numbers.

5.3.2 Calling Presets


A camera Preset is a pre-defined camera direction, focus, and zoom setting, and may include other options, depending on the camera. After creating a preset, you can quickly move the camera to that position by “calling” that preset. Use the PTZ More Settings interface to call a preset.

- Click the field to the right of **Preset**, and then use the pop-up virtual keyboard to enter a number to of the preset you want to call. Complete the entry by clicking the ↵ key.



- Click the **Call** button (just below the **Preset** line) to move the camera to that preset.

Call preset in live view mode:

- In the Live View screen, left click on the image from the PTZ camera, and then click the PTZ Control icon  in the quick setting tool bar to open the PTZ menu.

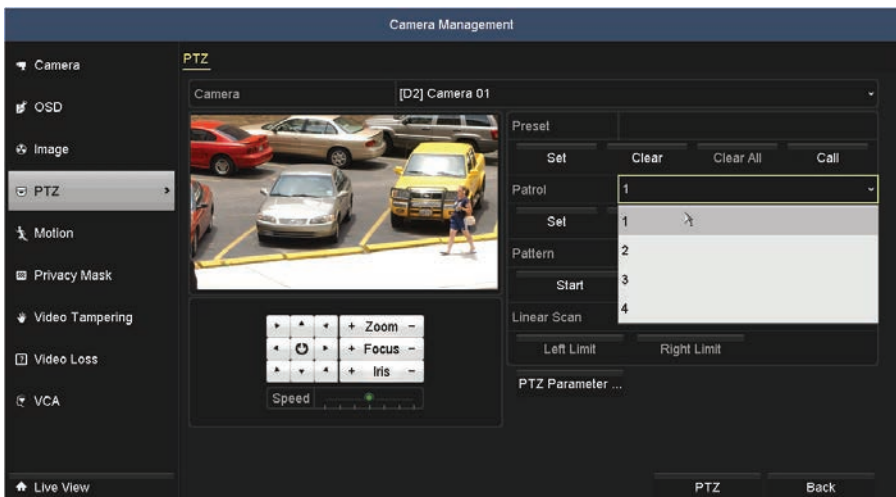


2. Click the **General** tab, and then enter the preset number you want to call in the field to the right of the **Call Preset** button.
3. Click the **Call Preset** button to move the camera.

5.3.3 Customizing Patrols

Patrols can be set to position a PTZ camera to a KeyPoint (Preset number) and hold it there for a set duration (dwell) before moving on to another KeyPoint (Preset number). To create Preset positions for the camera, see “5.3.1 Customizing Presets” on page 53. You can create up to 4 patrols, numbered 1 .. 4.

1. Open the PTZ settings menu. Go to: **Menu | Camera | PTZ**.
2. Click the field to the right of the Patrol line, and then select a Patrol number (1 .. 4) in the drop-down list.



SECTION 5: PTZ CONTROLS

- Click the **Set** button (just under the Patrol line) to open the KeyPoint menu.



- In the KeyPoint menu, enter a **Preset** number, a **Duration** (seconds), and a Speed value. Speed defines the speed at which the camera will move from one preset to another. Speed ranges from 1 (very slow) to 40.
- Click **Add** to create another KeyPoint (see above), and then configure the KeyPoint as before.
- Add additional KeyPoints using the different presets, or any combination of presets you created.
- When the patrol you defined with the KeyPoints menu is complete, click **OK** to save the patrol.
- You can test the patrol in the **Camera | PTZ** menu by selecting the Patrol number from the patrol drop down list, and then clicking **Call**.

5.3.4 Calling Patrols in Live View

Calling a patrol makes the PTZ to move according to the predefined patrol path. To **Call** a patrol in Live View:

- In the Live View screen, left click on the image from the PTZ camera, and then click the PTZ Control icon  in the quick setting toolbar to open the PTZ menu.

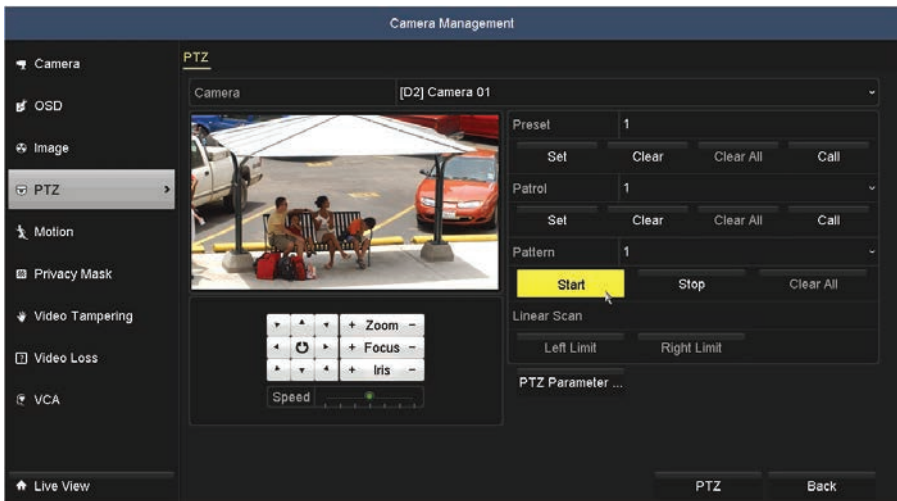


- Click the **General** tab.
- Click the patrol number field, and then select patrol number you want to Call.
- Click the **Call Patrol** button to move the camera in the Patrol pattern. To stop the Patrol, click the **Stop Patrol** button.

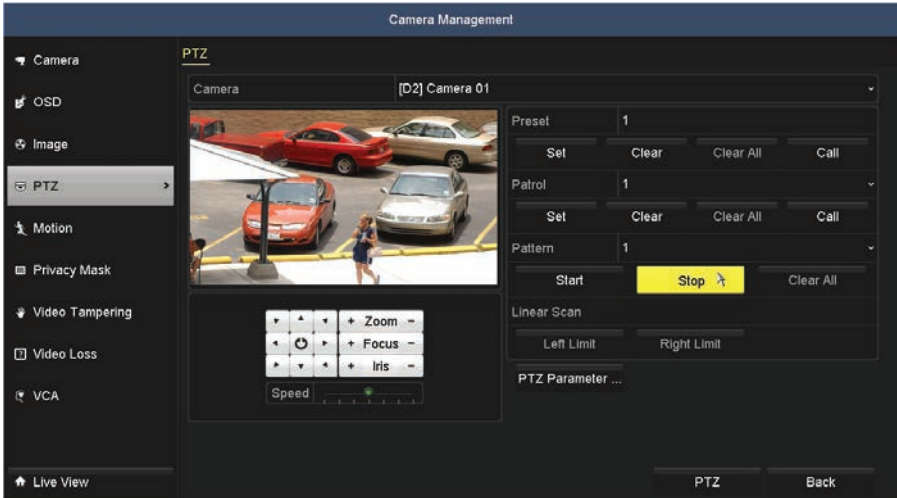
5.3.5 Creating a Pattern

A Pattern can be created by recording the movement of the camera. You can then call the pattern you recorded to repeat the movement. You can record only one pattern (pattern 1).


1. Open the PTZ settings menu. Go to: **Menu | Camera | PTZ**.
2. Click the **Start** button (just underneath the Pattern line) to start recording the camera movement. Use the controls under the camera video window to move the camera. You can also use the Zoom adjustment, if needed.

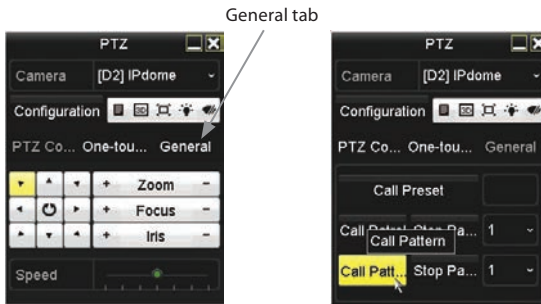


3. You can continue to record camera movement until the memory percentage shown on the video decrements to 0%. Click the **Stop** button to end recording the camera movement and save the pattern.



5.3.6 Calling the Pattern

1. Click the PTZ button in the lower-right corner of the PTZ setting interface or click the PTZ Control icon  in the Quick Setting bar to enter the PTZ setting menu in live view mode.



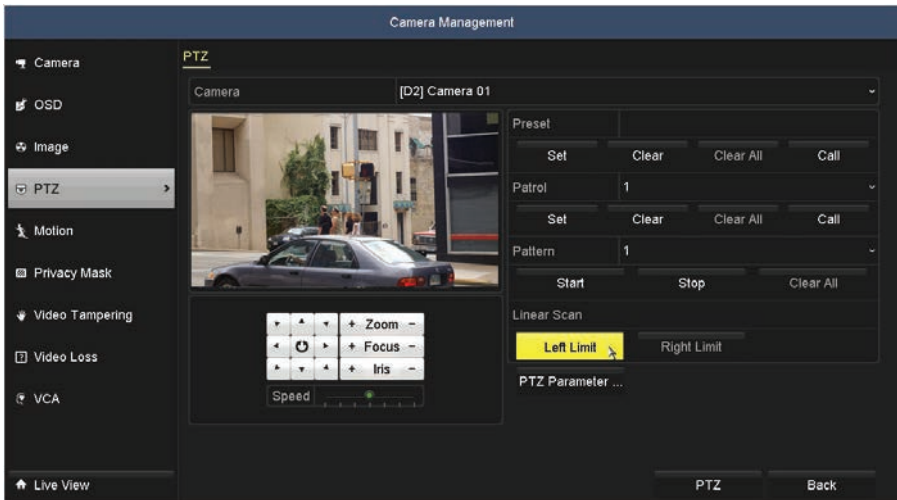
2. Click the **General** tab.
3. Click **Call Pattern** to start moving the camera in the pattern you recorded.
4. Click **Stop Pattern** to start moving the camera.

5.4 Linear Scan

You can set the left limit and right limit of the linear motion of the camera, and then initiate the Linear Scan feature to scan the field of view from the left to the right limit, and then repeat the scan.

To set the left and right scan limits

1. Open the PTZ settings menu. Go to: **Menu | Camera | PTZ**.

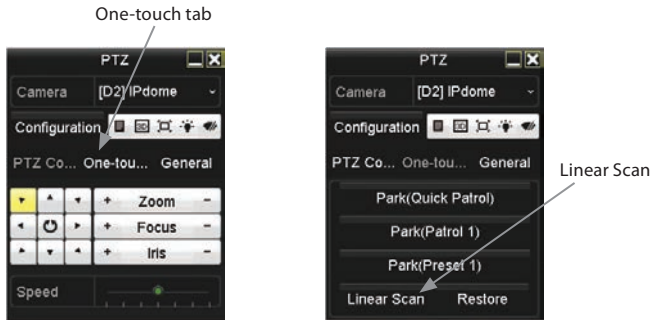


2. Use the direction buttons below the image from the camera to point the camera at the left-most limit of a scan.
3. Click the **Left Limit** button (see above).
4. Use the direction buttons below the image from the camera to point the camera at the right-most limit of a scan.
5. Click the **Right Limit** button.

5.4.1 Initiating a Linear Scan

1. In the Live View screen, left click on the image from the PTZ camera, and then click the PTZ Control icon  in the quick setting toolbar to open the PTZ menu.

SECTION 5: PTZ CONTROLS



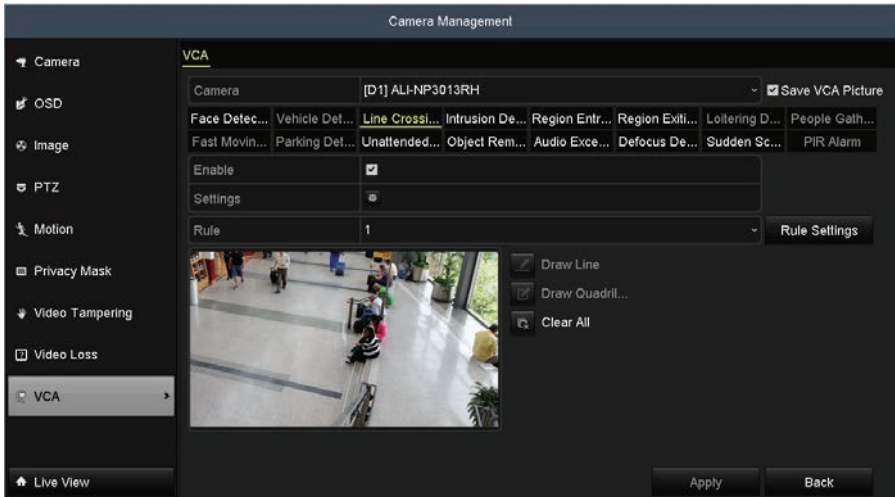
2. Click the **One-touch** tab.
3. Click **Linear Scan** to start moving the camera from the left limit to the right limit and back, repeatedly.
4. Click **Linear Scan** again to stop the scan.

SECTION 6

VCA Features

Alibi recorders can configure Video Content Analysis (VCA) features supported by Alibi cameras.

Alibi cameras that include VCA features usually do not include all features. After selecting a camera in the VCA menu (**Menu | Camera Management | VCA**) only those VCA features supported by the camera will be available (highlighted).



When VCA features are configured by a recorder, the settings are saved in the camera. When a VCA event occurs, the event information is sent immediately to the recorder, and acted upon by recording live video, full screen monitoring, generating an audible alarm and/or sending email.

The ALI-NVR71128R recorder supports the following VCA features. Additional VCA features shown in the display are not available at the time of this printing.

- **Face Detection** - Detects when a face appears in the field of view.
- **Line crossing detection** - You can specify the endpoints of a virtual line in the video image and then detect if something crosses the line from one side to the other (side A to B), vice versa (side B to A) or either way. You can define up to 4 line crossing conditions in the same video channel.
- **Intrusion detection** - You can create a virtual quadrangle in the video image, and then detect if something enters the space within the quadrangle. You can define up to 4 intrusion regions in the same video channel.
- **Region entrance detection** - Region entrance detection function detects people, vehicles or other objects which enter a pre-defined virtual region of the field of view.

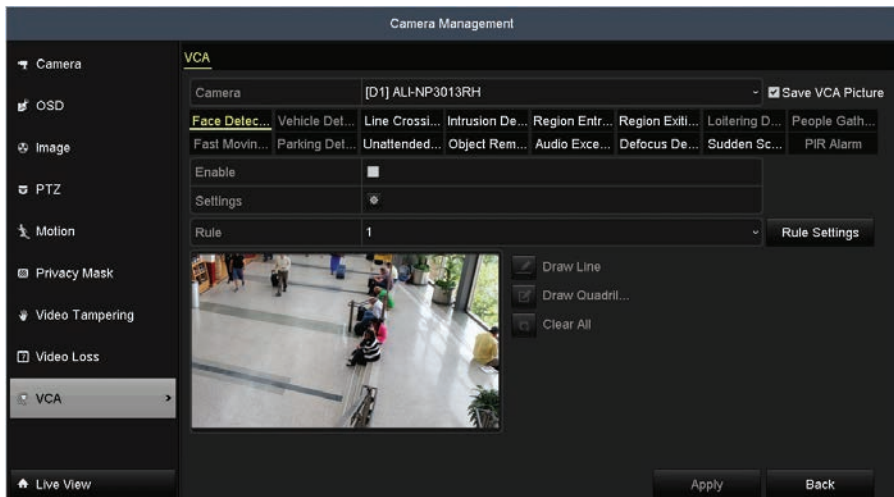
SECTION 6: VCA FEATURES

- **Region exiting detection** - Region exiting detection detects people, vehicles or other objects which exit from a pre-defined virtual region of the field of view.
- **Unattended baggage detection** - Unattended baggage detection can detect when objects such as baggage, a purse, dangerous materials, etc. are left in the pre-defined area of the field of view.
- **Object removal detection** - Object removal detection detects when an object, such as an exhibit on display, is removed from the pre-defined area of the field of view.
- **Audio exception detection** - Audio exception detection detects when an abnormal sound, such as the sudden increase / decrease of the sound intensity, occurs in the surveillance area.
- **Defocus detection** - Defocus detection senses when image blur, caused by defocus of the lens, occurs.
- **Sudden scene change detection** - Scene change detection detects the change of surveillance environment affected by an external factor, such as the intentional rotation of the camera.
- **PIR alarm detection** - An infrared alarm is triggered when heat energy dissipated by a person or any other warm blooded entity such as a dog, cat, etc. moves into the field of view.

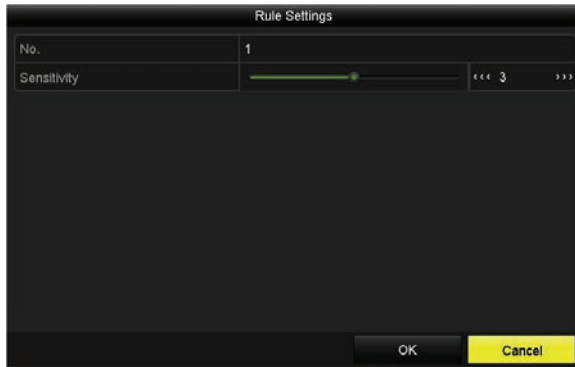
6.1 Face Detection

Face detection function detects when a face appears in the surveillance field of view. Certain actions can be performed when the alarm is triggered. To configure Face Detection in the camera:

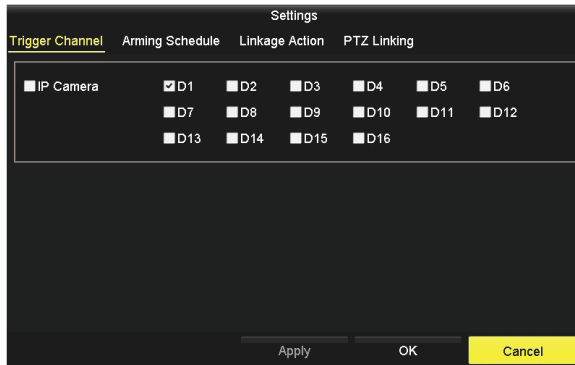
1. Open the VCA menu. Go to **Menu | Camera Management | VCA**.
2. On the **Camera** line, open the drop down list, and then select the camera you want to configure.
3. Check the **Save VCA Picture** box to capture a live view image of the VCA event.
4. In the VCA type selection line, click on **Face Detection**. If the camera supports this feature, it will be highlighted.



5. Check the **Enable** box to select this feature.
6. Click **Rule Settings**.

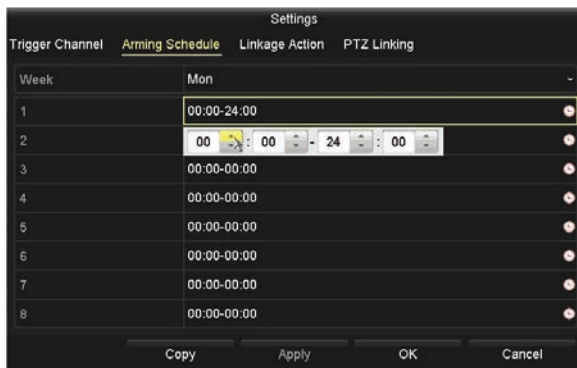


- a. In the Rule Settings window, adjust the **Sensitivity** slider to set the detection sensitivity (range : 1 .. 5). The higher the sensitivity number, the more frequently facial recognition is reported. This setting may require testing.
 - b. Click **OK** to save the Sensitivity setting.
7. Click the icon on the **Settings** line.
 - a. In the **Trigger Channel** window, select the other channels that should trigger recording on this channel, then click **Apply** to save your settings.

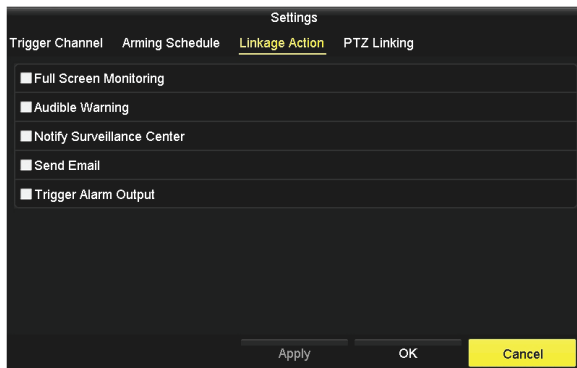


- b. Click the **Arming Schedule** tab. With the Arming Schedule, you can define a schedule for each day of eight weeks (56 days) when face detection is monitored. Time periods cannot overlap.

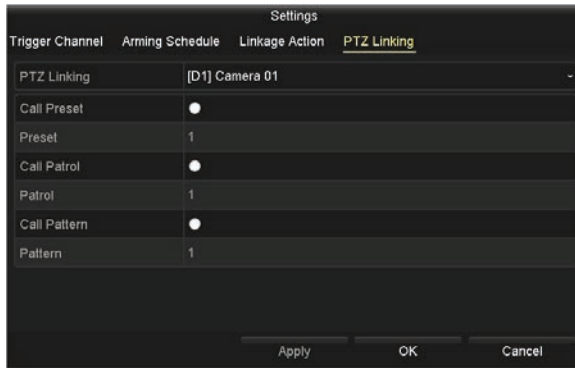
SECTION 6: VCA FEATURES



- c. Click **Apply** to save the settings. You can also click **Copy** to copy the Arming Schedule setup in the window to other days of the week.
- d. Click the **Linkage Action** tab. In this tab you can cause certain actions to occur when face recognition is detected.



- e. Select the actions you want to occur, then click **Apply** to save your settings.
- f. Click the **PTZ Linking** tab. With PTZ linking, you can configure the camera to perform a Preset, Patrol, and/or Pattern when an event occurs.



- g. Select the actions you want to occur, then click **Apply** to save your settings.
 - h. Click **OK** to return to the VCA menu.
8. In the VCA menu, click **Apply** to activate the settings.
 9. Repeat steps 2 through 8 above to create rules for other cameras.

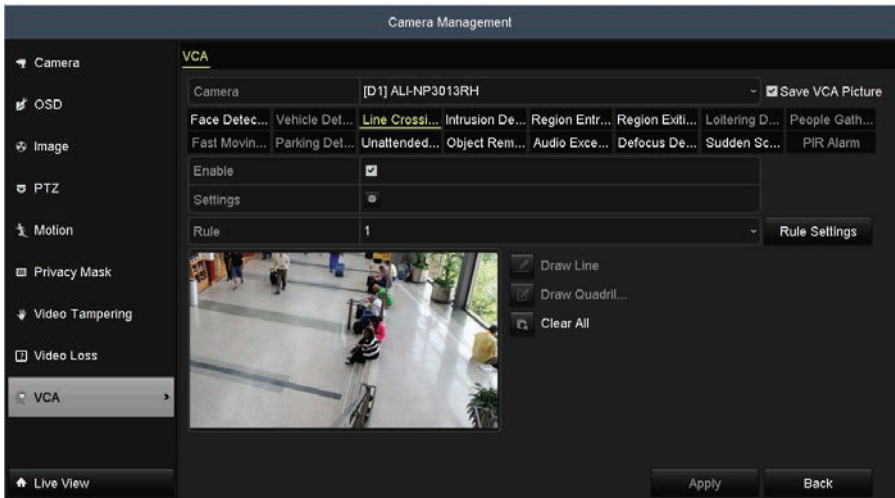
6.2 Line Crossing Detection

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

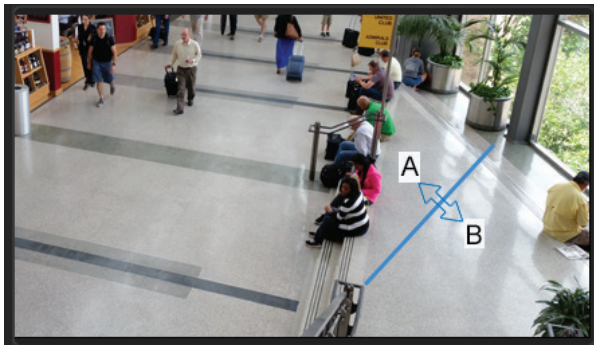
To configure Line Crossing Detection:

1. Open the VCA menu. Go to **Menu | Camera Management | VCA**.
2. On the **Camera** line, open the drop down list, and then select the camera you want to configure.
3. Check the **Save VCA Picture** box to capture a live view image of the VCA event.
4. In the VCA type selection line, click on **Line Crossing Detection**. If the camera supports this feature, it will be highlighted.

SECTION 6: VCA FEATURES



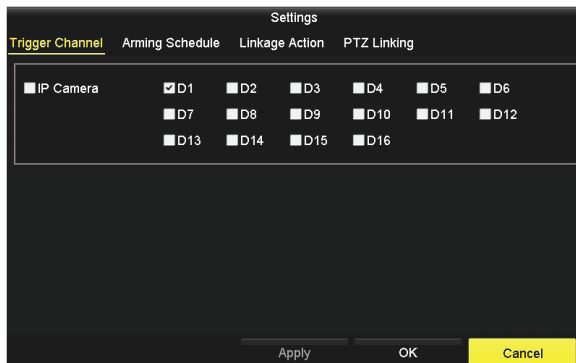
5. Check the **Enable** box to select this feature.
6. Open the **Rule** drop down list and select the rule number you want to configure. You can configure up to 4 line crossing rules.
7. In the image window, create a virtual line by clicking on two points that define the endpoints of the line. A blue line will appear in the image with one side labeled **A** and the other side **B**.



8. Click **Rule Settings**.

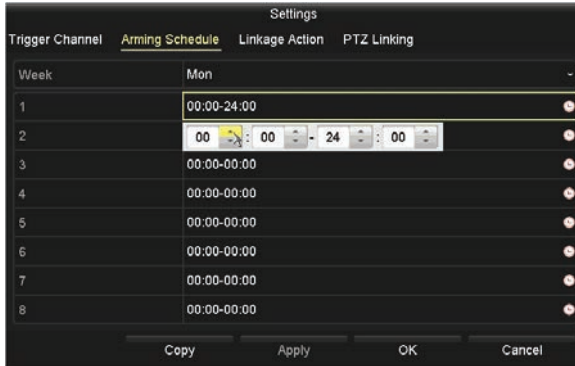


- a. In the **Rule Settings** window, open the **Direction** drop down list and select the direction of line crossing you want to detect: You can select either of the following for the rule you are configuring:
 - * **A<->B**: An arrow on both the A side and the B side of the virtual line. When an object moves across the virtual line in either direction an alarm is triggered.
 - * **A->B**: An arrow appears on only the B side of the virtual line. When an object moves across the virtual line from the A side to the B side an alarm is triggered.
 - * **B->A**: An arrow appears on only the A side of the virtual line. When an object moves across the virtual line from the B side to the A side an alarm is triggered.
 - b. Adjust the **Sensitivity** slider to set the detection sensitivity (range : 1 .. 100). Higher sensitivity (number) detects smaller objects. This setting may require testing.
 - c. Click **OK** to save the Sensitivity setting.
9. Click the icon on the **Settings** line.
 - a. In the **Trigger Channel** window, select the other channels that should trigger recording on this channel, then click **Apply** to save your settings.

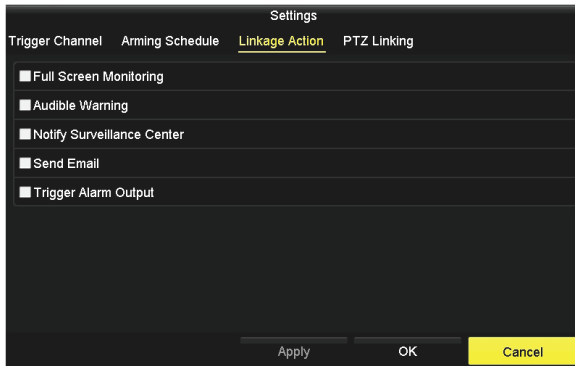


SECTION 6: VCA FEATURES

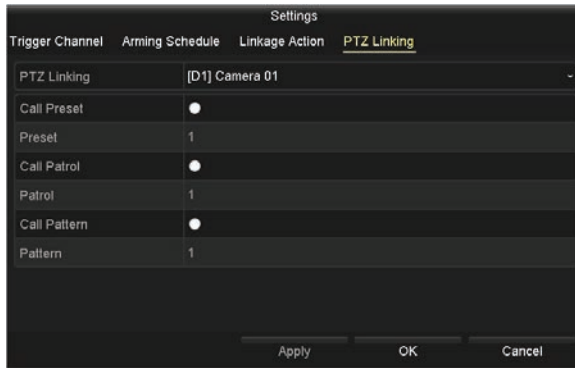
- b. Click the **Arming Schedule** tab. With the Arming Schedule, you can define a schedule for each day of eight weeks (56 days) when line crossing is monitored. Time periods cannot overlap.



- c. Click **Apply** to save the settings. You can also click **Copy** to copy the Arming Schedule setup in the window to other days of the week.
- d. Click the **Linkage Action** tab. In this tab you can cause certain actions to occur when line crossing is detected.



- e. Select the actions you want to occur, then click **Apply** to save your settings.
- f. Click the **PTZ Linking** tab. With PTZ linking, you can configure the camera to perform a Preset, Patrol, and/or Pattern when an event occurs.



- g. Select the actions you want to occur, then click **Apply** to save your settings.
 - h. Click **OK** to return to the VCA menu.
10. In the VCA menu, click **Apply** to activate the settings.
 11. Repeat steps 2 through 10 above to create rules for other cameras.

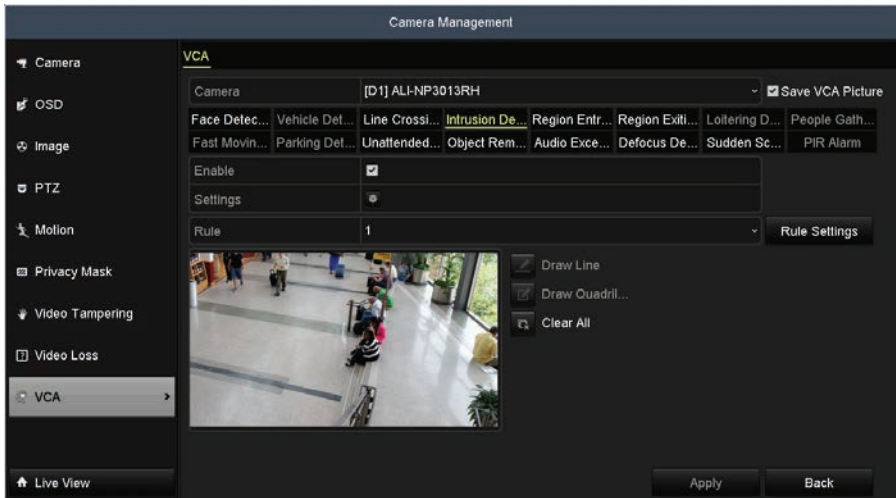
6.3 Intrusion Detection

Intrusion detection detects people, vehicles or other objects which enter and loiter in a pre-defined virtual area of the field of view. Certain actions can be performed when an intrusion alarm is triggered.

To configure Intrusion Detection in the camera:

1. Open the VCA menu. Go to **Menu | Camera Management | VCA**.
2. On the **Camera** line, open the drop down list, and then select the camera you want to configure.
3. Check the **Save VCA Picture** box to capture a live view image of the VCA event.
4. In the VCA type selection line, click on **Intrusion Detection**. If the camera supports this feature, it will be highlighted.

SECTION 6: VCA FEATURES



5. Check the **Enable** box to select this feature.
6. Open the **Rule** drop down list and select the rule number you want to configure. You can configure up to 4 intrusion detection rules.
7. In the image window, create a virtual intrusion zone by clicking on, in a circular manner, the four corners of a quadrangle that define the corners of the zone. A blue quadrangle will appear in the image with a number indicating the rule number.

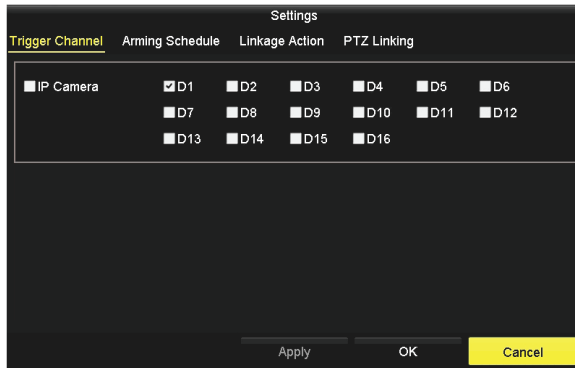


8. Click **Rule Settings**.

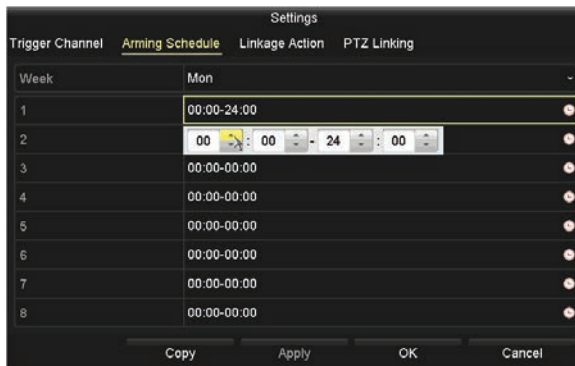


- a. In the **Rule Settings** window, set the following:
 - * **Time Threshold (s):** Range 1 s .. 10 s. If something moves into the zone and stays there for longer than the Time Threshold setting, an alarm can be triggered.
 - * **Sensitivity:** Click-and-drag the slider to set the detection sensitivity. Range 1 .. 100. The value represents the percentage of the body part of an acceptable target that enters the region. The higher the value, the smaller the object that can trigger an alarm.
 - * **Percentage:** Use this option to set size. Range 1 .. 100. Percentage defines the ratio of the in-zone part of the object which can trigger the alarm. For example, if the percentage is set to 50, an object that fills at least 50% of the zone can trigger an alarm. **NOTE:** For some camera models, this option is greyed out in this menu. For those cameras, log into the camera directly and set the percentage value.
 - b. Click **OK** to save your settings.
9. Click the icon on the **Settings** line.
 - a. In the **Trigger Channel** window, select the other channels that should trigger recording on this channel, then click **Apply** to save your settings.

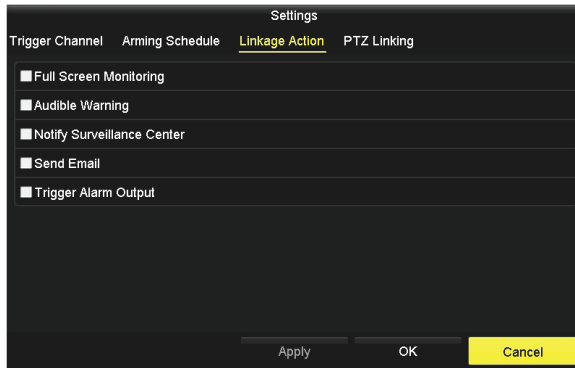
SECTION 6: VCA FEATURES



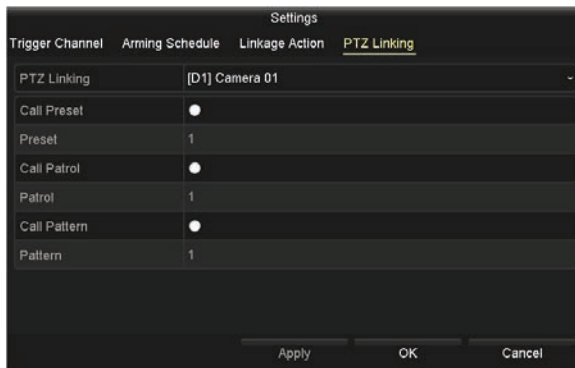
- b. Click the **Arming Schedule** tab. With the Arming Schedule, you can define a schedule for each day of eight weeks (56 days) when intrusion is monitored. Time periods cannot overlap.



- c. Click **Apply** to save the settings. You can also click **Copy** to copy the Arming Schedule setup in the window to other days of the week.
- d. Click the **Linkage Action** tab. In this tab you can cause certain actions to occur when an intrusion is detected.



- e. Select the actions you want to occur, then click **Apply** to save your settings.
- f. Click the **PTZ Linking** tab. With PTZ linking, you can configure the camera to perform a Preset, Patrol, and/or Pattern when an event occurs.



- g. Select the actions you want to occur, then click **Apply** to save your settings.
- h. Click **OK** to return to the VCA menu.
10. In the VCA menu, click **Apply** to activate the settings.
11. Repeat steps 2 through 10 above to configure other cameras.

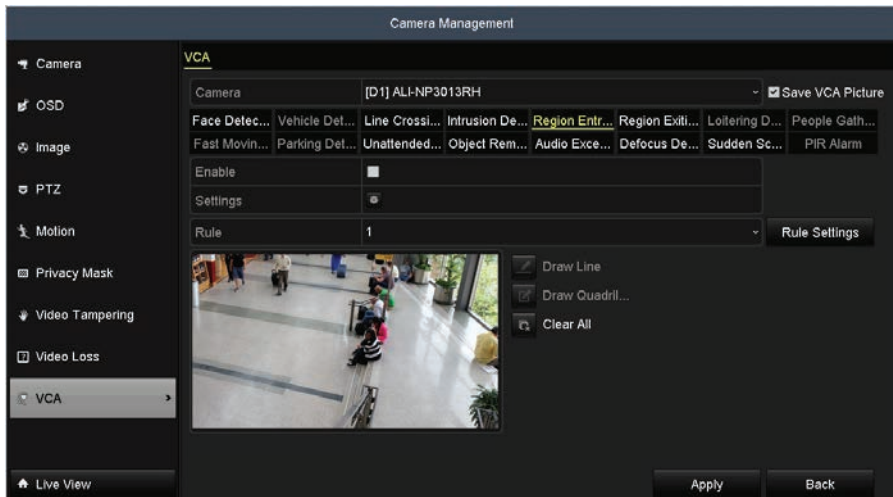
6.4 Region Entrance Detection

Region entrance detection detects people, vehicles or other objects which enter a pre-defined virtual region in the field of view. Certain actions can be taken when the alarm is triggered.

SECTION 6: VCA FEATURES

To configure Region Entrance Detection in the camera:

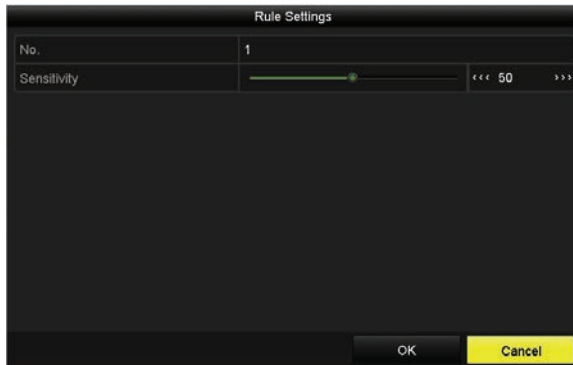
1. Open the VCA menu. Go to **Menu | Camera Management | VCA**.
2. On the **Camera** line, open the drop down list, and then select the camera you want to configure.
3. Check the **Save VCA Picture** box to capture a live view image of the VCA event.
4. In the VCA type selection line, click on **Region Entrance Detection**. If the camera supports this feature, it will be highlighted.



5. Check the **Enable** box to select this feature.
6. Open the **Rule** drop down list and select the rule number you want to configure. You can configure up to 4 region entrance detection rules.
7. In the image window, create a virtual region by clicking on, in a circular manner, the four corners of a quadrangle that define the corners of the region. A blue quadrangle will appear in the image with a number indicating the rule number.

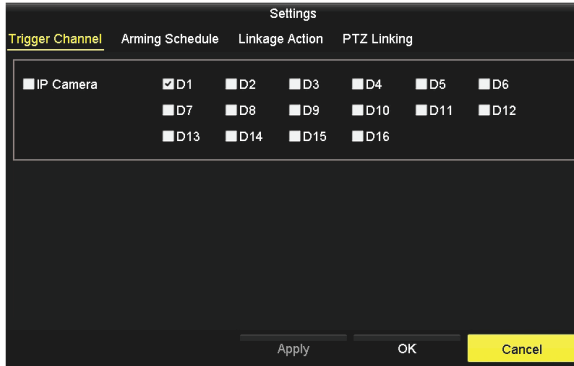


8. Click **Rule Settings**.

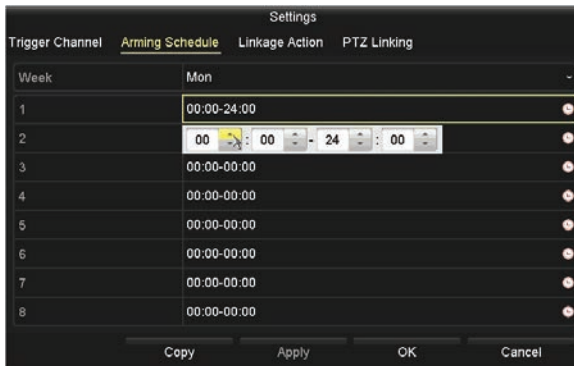


- a. In the **Rule Settings** window, set the **Sensitivity**. Click-and-drag the slider to set the detection sensitivity. Range 1..100. The value of the sensitivity represents the size of the object which can trigger an alarm. The higher the value, the smaller the object that can trigger an alarm.
 - b. Click **OK** to save your settings.
9. Click the icon on the **Settings** line.
 - a. In the **Trigger Channel** window, select the other channels that should trigger recording on this channel, then click **Apply** to save your settings.

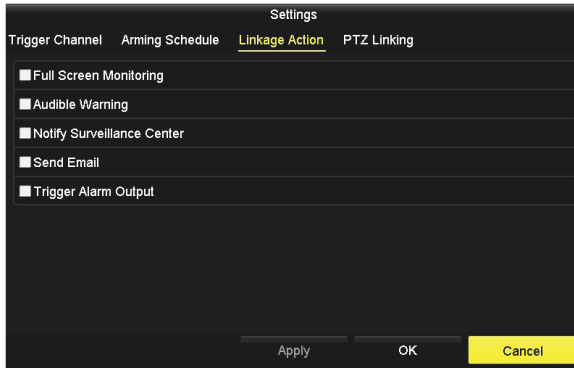
SECTION 6: VCA FEATURES



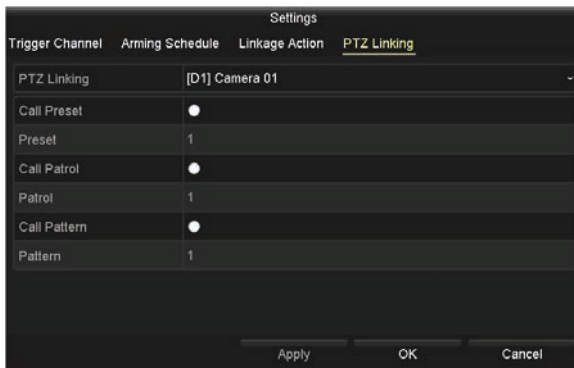
- b. Click the **Arming Schedule** tab. With the Arming Schedule, you can define a schedule for each day of eight weeks (56 days) when entrance detection is monitored. Time periods cannot overlap.



- c. Click **Apply** to save the settings. You can also click **Copy** to copy the Arming Schedule setup in the window to other days of the week.
- d. Click the **Linkage Action** tab. In this tab you can cause certain actions to occur when an entrance is detected.



- e. Select the actions you want to occur, then click **Apply** to save your settings.
- f. Click the **PTZ Linking** tab. With PTZ linking, you can configure the camera to perform a Preset, Patrol, and/or Pattern when an event occurs.



- g. Select the actions you want to occur, then click **Apply** to save your settings.
- h. Click **OK** to return to the VCA menu.
10. In the VCA menu, click **Apply** to activate the settings.
11. Repeat steps 2 through 10 above to create rules for other cameras.

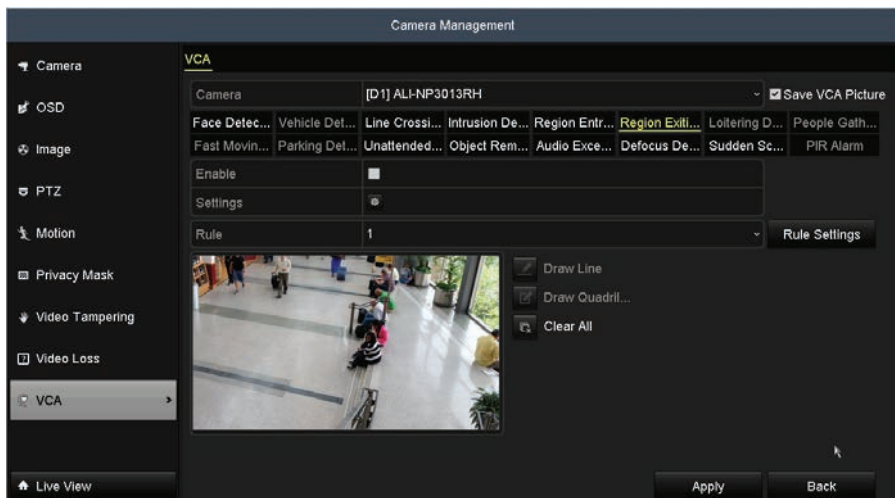
6.5 Region Exiting Detection

Region exiting detection detects people, vehicles or other objects which leave a pre-defined virtual region in the field of view. Certain actions can be taken when the alarm is triggered.

SECTION 6: VCA FEATURES

To configure Region Entrance Detection in the camera:

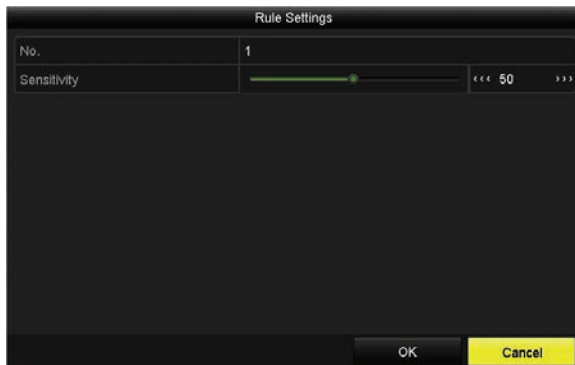
1. Open the VCA menu. Go to **Menu | Camera Management | VCA**.
2. On the **Camera** line, open the drop down list, and then select the camera you want to configure.
3. Check the **Save VCA Picture** box to capture a live view image of the VCA event.
4. In the VCA type selection line, click on **Region Exiting Detection**. If the camera supports this feature, it will be highlighted.



5. Check the **Enable** box to select this feature.
6. Open the **Rule** drop down list and select the rule number you want to configure. You can configure up to 4 region exiting detection rules.
7. In the image window, create a virtual region by clicking on, in a circular manner, the four corners of a quadrangle that define the corners of the region. A blue quadrangle will appear in the image with a number indicating the rule number.

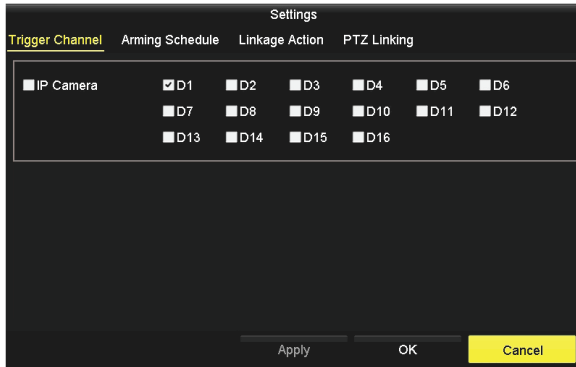


8. Click **Rule Settings**.

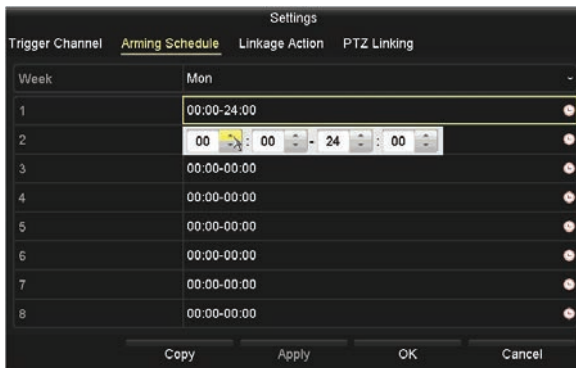


- a. In the **Rule Settings** window, set the **Sensitivity**. Click-and-drag the slider to set the detection sensitivity. Range 1 .. 100. The value of the sensitivity represents the size of the object which can trigger an alarm. The higher the value, the smaller the object that can trigger an alarm.
 - b. Click **OK** to save your settings.
9. Click the icon on the **Settings** line.
 - a. In the **Trigger Channel** window, select the other channels that should trigger recording on this channel, then click **Apply** to save your settings.

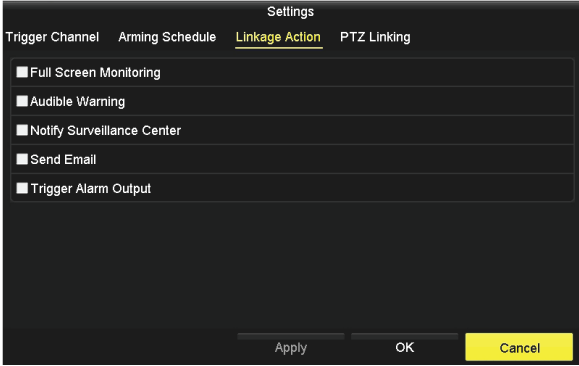
SECTION 6: VCA FEATURES



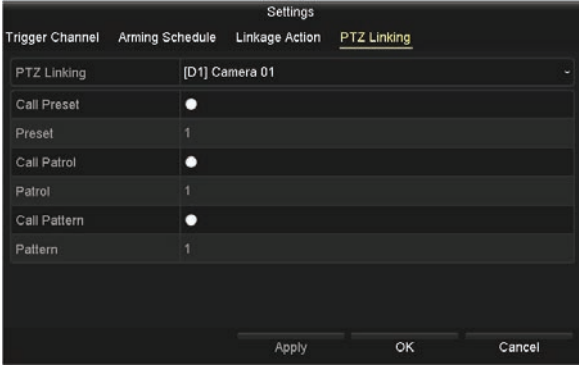
- b. Click the **Arming Schedule** tab. With the Arming Schedule, you can define a schedule for each day of eight weeks (56 days) when exiting detection is monitored. Time periods cannot overlap.



- c. Click **Apply** to save the settings. You can also click **Copy** to copy the Arming Schedule setup in the window to other days of the week.
- d. Click the **Linkage Action** tab. In this tab you can cause certain actions to occur when an entrance is detected.



- e. Select the actions you want to occur, then click **Apply** to save your settings.
- f. Click the **PTZ Linking** tab. With PTZ linking, you can configure the camera to perform a Preset, Patrol, and/or Pattern when an event occurs.

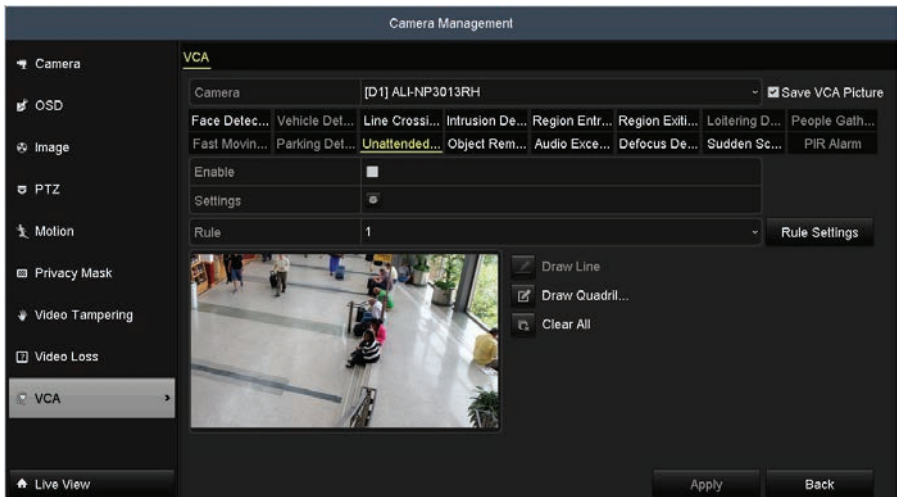


- g. Select the actions you want to occur, then click **Apply** to save your settings.
 - h. Click **OK** to return to the VCA menu.
10. In the VCA menu, click **Apply** to activate the settings.
 11. Repeat steps 2 through 10 above to configure other cameras.

6.6 Unattended Baggage Detection

Unattended baggage detection can detect when objects such as baggage, a purse, dangerous materials, etc. are left in the pre-defined area of the field of view. A series of actions can be taken when the alarm is triggered. To configure Unattended Baggage Detection:

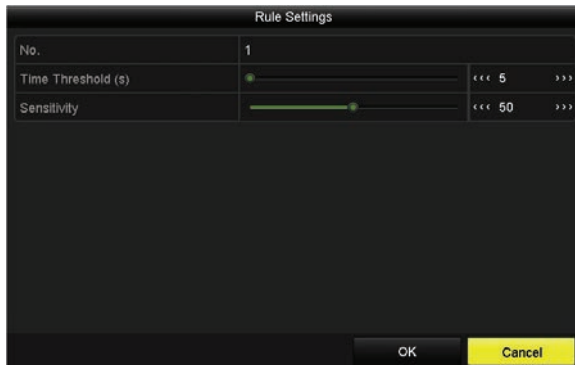
1. Open the VCA menu. Go to **Menu | Camera Management | VCA**.
2. On the **Camera** line, open the drop down list, and then select the camera you want to configure.
3. Check the **Save VCA Picture** box to capture a live view image of the VCA event.
4. In the VCA type selection line, click on **Unattended Baggage Detection**. If the camera supports this feature, it will be highlighted.



5. Check the **Enable** box to select this feature.
6. Open the **Rule** drop down list and select the rule number you want to configure. You can configure up to 4 unattended baggage detection rules.
7. In the image window, create a virtual baggage zone by clicking on, in a circular manner, the four corners of a quadrangle that define the corners of the zone. A blue quadrangle will appear in the image with a number indicating the rule number.

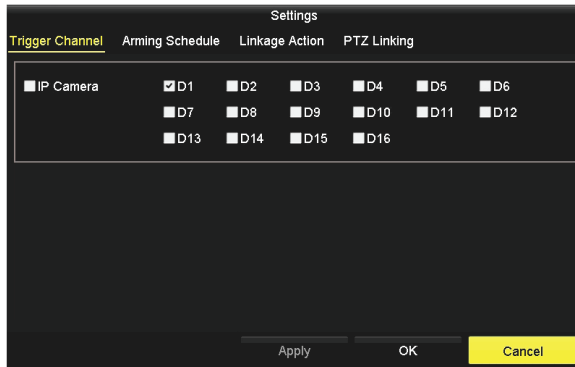


8. Click **Rule Settings**.

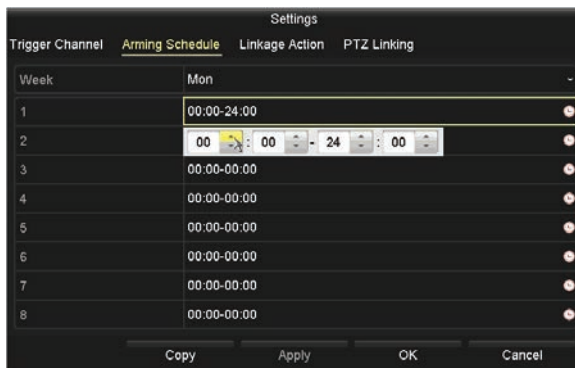


- a. In the **Rule Settings** window, set the following:
 - * **Time Threshold (s):** Range 5 s .. 20 s. If something is left in the zone and stays there for longer than the Time Threshold setting, an alarm can be triggered. If you select "0", and alarm can be reported immediately when the object enters the zone.
 - * **Sensitivity:** Click-and-drag the slider to set the detection sensitivity. Range 1 .. 100. Sensitivity defines the similarity with the background image. Usually, when the sensitivity is high, a very small object left in the region can trigger the alarm.
 - b. Click **OK** to save your settings.
9. Click the icon on the **Settings** line.
- a. In the **Trigger Channel** window, select the other channels that should trigger recording on this channel, then click **Apply** to save your settings.

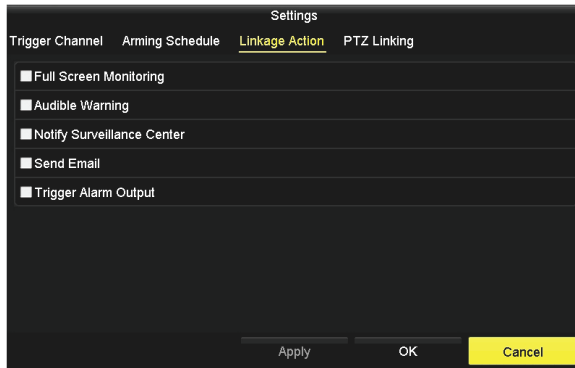
SECTION 6: VCA FEATURES



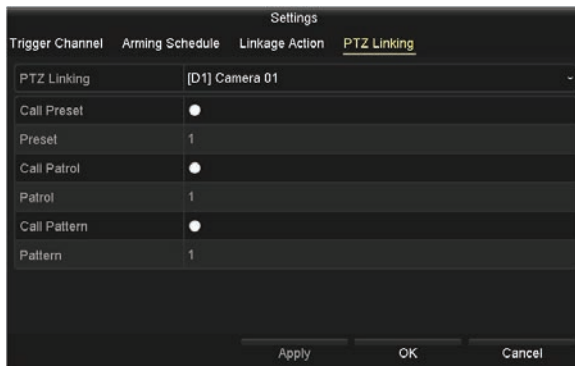
- b. Click the **Arming Schedule** tab. With the Arming Schedule, you can define a schedule for each day of eight weeks (56 days) when parking is monitored. Time periods cannot overlap.



- c. Click **Apply** to save the settings. You can also click **Copy** to copy the Arming Schedule setup in the window to other days of the week.
- d. Click the **Linkage Action** tab. In this tab you can cause certain actions to occur when parking is detected.



- e. Select the actions you want to occur, then click **Apply** to save your settings.
- f. Click the **PTZ Linking** tab. With PTZ linking, you can configure the camera to perform a Preset, Patrol, and/or Pattern when an event occurs.



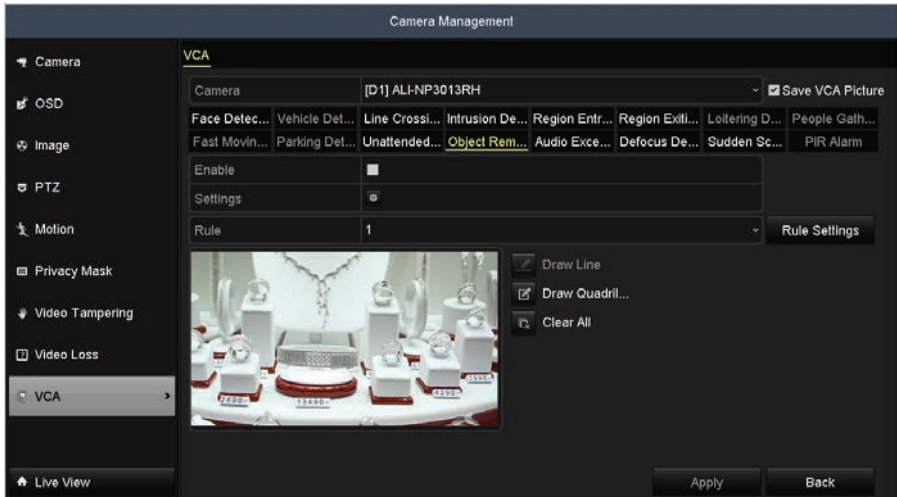
- g. Select the actions you want to occur, then click **Apply** to save your settings.
 - h. Click **OK** to return to the VCA menu.
10. In the VCA menu, click **Apply** to activate the settings.
 11. Repeat steps 2 through 10 above to configure other cameras.

6.7 Object Removal Detection

Object removal detection detects when an object, such as an exhibit on display, is removed from the pre-defined area of the field of view. A series of actions can be taken when the alarm is triggered. To configure Object Removal detection:

SECTION 6: VCA FEATURES

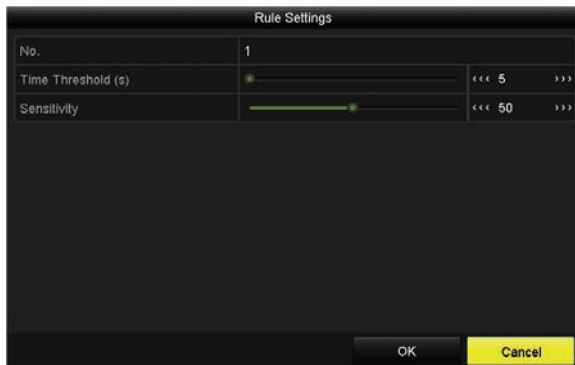
1. Open the VCA menu. Go to **Menu | Camera Management | VCA**.
2. On the **Camera** line, open the drop down list, and then select the camera you want to configure.
3. Check the **Save VCA Picture** box to capture a live view image of the VCA event.
4. In the VCA type selection line, click on **Object Removal Detection**. If the camera supports this feature, it will be highlighted.



5. Check the **Enable** box to select this feature.
6. Open the **Rule** drop down list and select the rule number you want to configure. You can configure up to 4 unattended object removal detection rules.
7. In the image window, create a virtual object zone by clicking on, in a circular manner, the four corners of a quadrangle that define the corners of the zone. A blue quadrangle will appear in the image with a number indicating the rule number.



8. Click **Rule Settings**.



a. In the **Rule Settings** window, set the following:

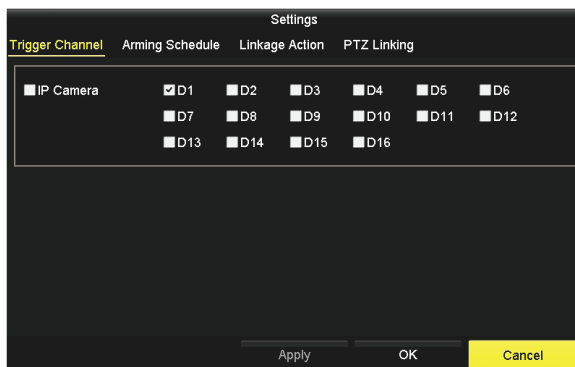
- * **Time Threshold (s):** Range 5 s .. 20 s. If something is removed from the zone for longer than the Time Threshold setting, an alarm can be triggered. If you select "0", an alarm can be reported immediately when the object enters the zone.
- * **Sensitivity:** Click-and-drag the slider to set the detection sensitivity. Range 1 .. 100. Sensitivity defines the similarity degree of the background image. Usually, when the sensitivity is high, a very small object taken from the region can trigger the alarm.

b. Click **OK** to save your settings.

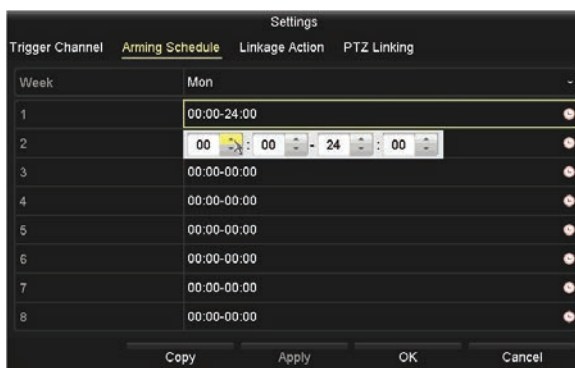
9. Click the icon on the **Settings** line.

- a. In the **Trigger Channel** window, select the other channels that should trigger recording on this channel, then click **Apply** to save your settings.

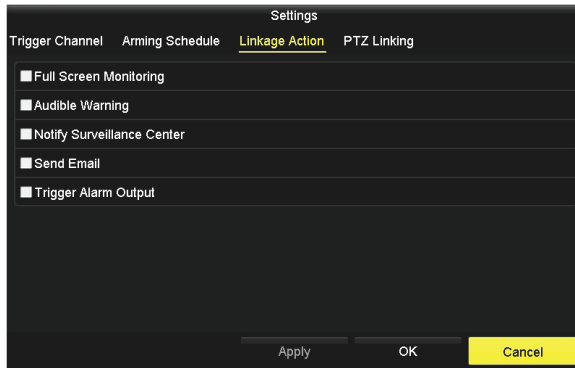
SECTION 6: VCA FEATURES



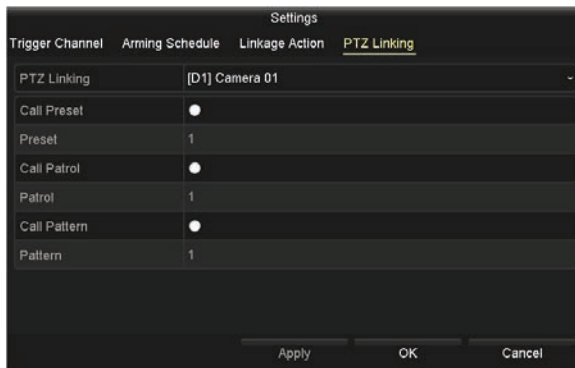
- b. Click the **Arming Schedule** tab. With the Arming Schedule, you can define a schedule for each day of eight weeks (56 days) when parking is monitored. Time periods cannot overlap.



- c. Click **Apply** to save the settings. You can also click **Copy** to copy the Arming Schedule setup in the window to other days of the week.
- d. Click the **Linkage Action** tab. In this tab you can cause certain actions to occur when object removal is detected.



- e. Select the actions you want to occur, then click **Apply** to save your settings.
- f. Click the **PTZ Linking** tab. With PTZ linking, you can configure the camera to perform a Preset, Patrol, and/or Pattern when an event occurs.



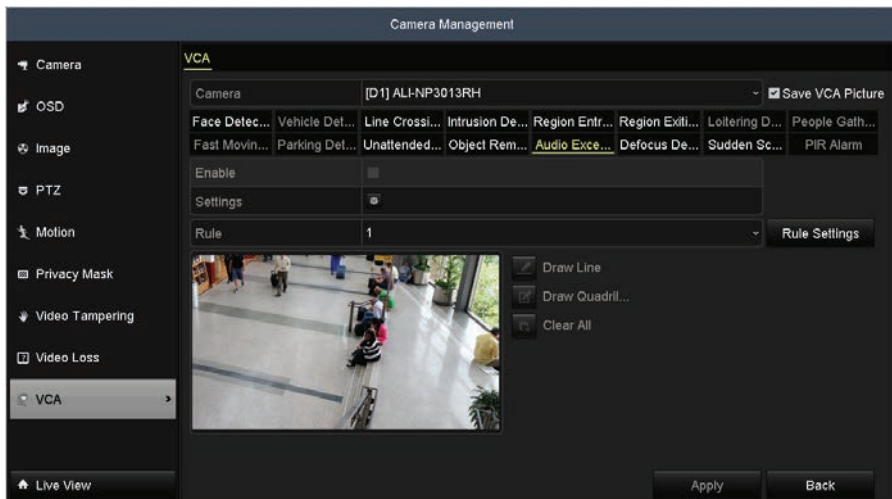
- g. Select the actions you want to occur, then click **Apply** to save your settings.
- h. Click **OK** to return to the VCA menu.
10. In the VCA menu, click **Apply** to activate the settings.
11. Repeat steps 2 through 10 above to configure other cameras.

6.8 Audio Exception Detection

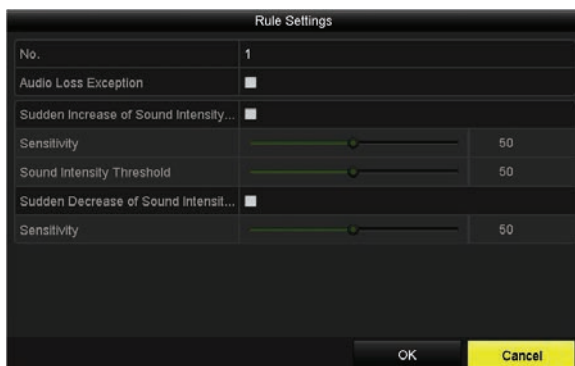
Audio exception detection detects when an abnormal sound, such as the sudden increase / decrease of the sound intensity, occurs in the surveillance area. Certain actions can be performed when the alarm is triggered. To configure Audio Exception Detection:

SECTION 6: VCA FEATURES

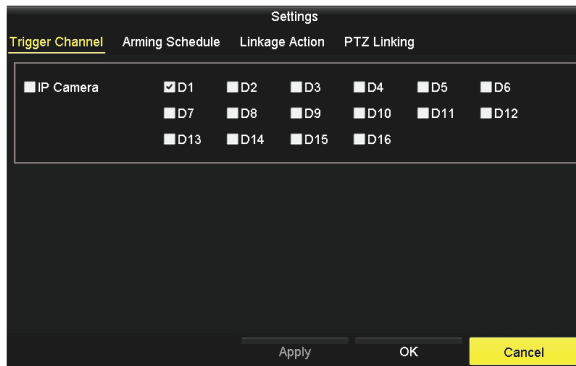
1. Open the VCA menu. Go to **Menu | Camera Management | VCA**.
2. On the **Camera** line, open the drop down list, and then select the camera you want to configure.
3. Check the **Save VCA Picture** box to capture a live view image of the VCA event.
4. In the VCA type selection line, click on **Audio Exception Detection**. If the camera supports this feature, it will be highlighted.



5. On the **Camera** line, open the drop down list and select the camera you want to configure.
6. Check the **Enable** box to select this feature.
7. Click **Rule Settings**.

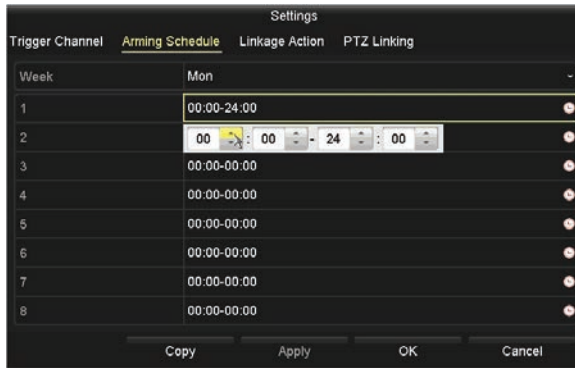


- a. In the **Rule Settings** window, set the following:
 - * **Audio Input Exception:** Check the select box of to enable the audio loss detection function.
 - * **Sudden Increase of Sound Intensity Detection:** Check the select box to detect a steep increase in the sound volume in the surveillance scene.
 - Set the detection sensitivity and threshold for sound steep rise. **Sensitivity:** Range: 1 .. 100. The smaller the value is, the more severe the change must be to trigger the detection.
 - **Sound Intensity Threshold:** Range: 1 .. 100. This option can filter the sound in the environment. The louder the sound, the higher the value should be. Adjust this value with consideration of the actual ambient sound level.
 - * **Sudden Decrease of Sound Intensity Detection:** Check the select box of to detect a steep drop in the sound level in the surveillance area.
 - **Sensitivity:** Range: 1 .. 100. Set the detection sensitivity for a steep drop in volume.
 - b. Click **OK** to save your settings.
8. Click the icon on the **Settings** line.
- a. In the **Trigger Channel** window, select the other channels that should trigger recording on this channel, then click **Apply** to save your settings.

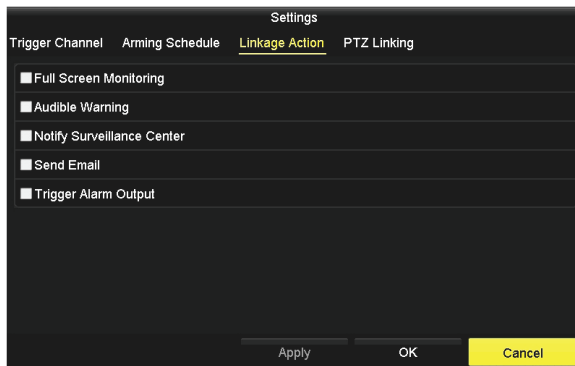


- b. Click the **Arming Schedule** tab. With the Arming Schedule, you can define a schedule for each day of eight weeks (56 days) when parking is monitored. Time periods cannot overlap.

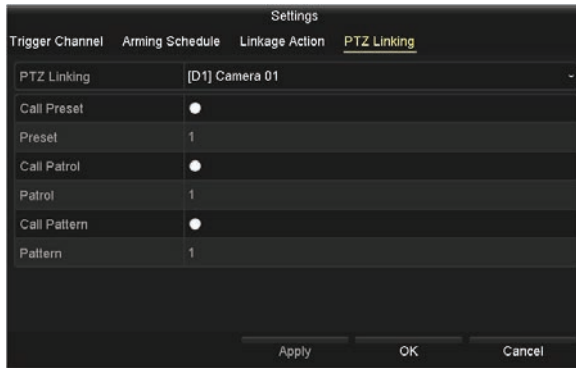
SECTION 6: VCA FEATURES



- c. Click **Apply** to save the settings. You can also click **Copy** to copy the Arming Schedule setup in the window to other days of the week.
- d. Click the **Linkage Action** tab. In this tab you can cause certain actions to occur when an audio exception is detected.



- e. Select the actions you want to occur, then click **Apply** to save your settings.
- f. Click the **PTZ Linking** tab. With PTZ linking, you can configure the camera to perform a Preset, Patrol, and/or Pattern when an event occurs.



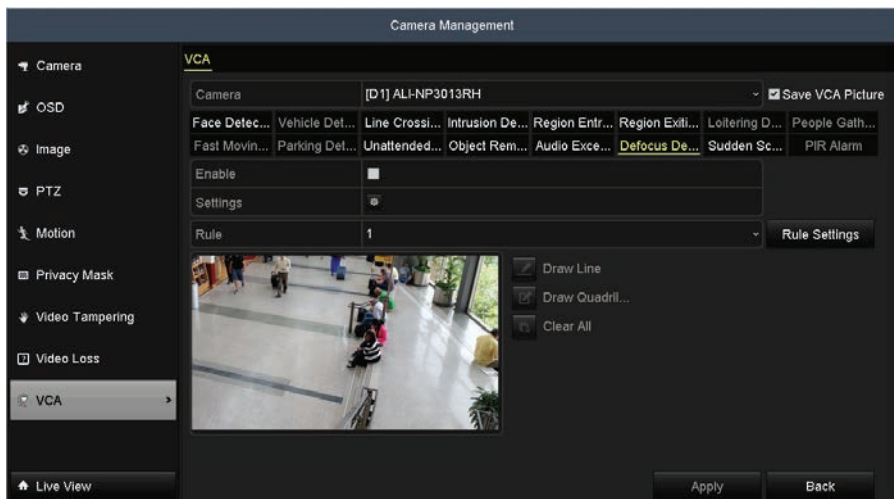
- g. Select the actions you want to occur, then click **Apply** to save your settings.
 - h. Click **OK** to return to the VCA menu.
9. In the VCA menu, click **Apply** to activate the settings.
 10. Repeat steps 5 through 9 above to configure other cameras.

6.9 Defocus Detection

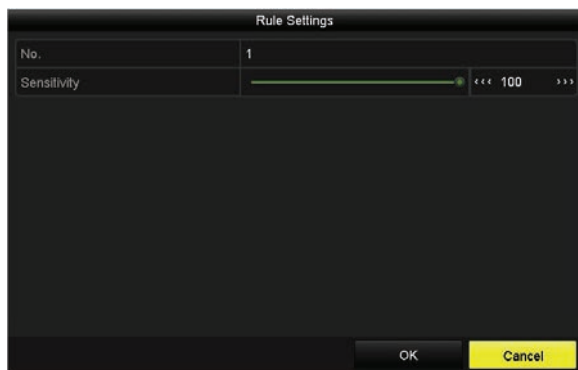
Defocus Detection senses when image blur, caused by defocus of the lens, occurs. Certain actions can be taken when the alarm is triggered. To configure Defocus Detection:

1. Open the VCA menu. Go to **Menu | Camera Management | VCA**.
2. On the **Camera** line, open the drop down list, and then select the camera you want to configure.
3. Check the **Save VCA Picture** box to capture a live view image of the VCA event.
4. In the VCA type selection line, click on **Defocus Detection**. If the camera supports this feature, it will be highlighted.

SECTION 6: VCA FEATURES

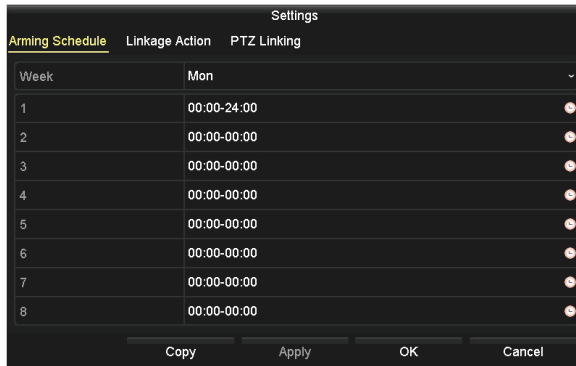


5. On the **Camera** line, open the drop down list and select the camera you want to configure.
6. Check the **Enable** box to select this feature.
7. Click **Rule Settings**.

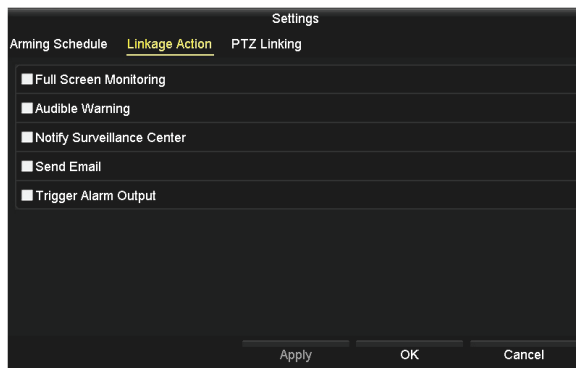


- a. In the Rule Settings window, adjust the **Sensitivity** slider to set the detection sensitivity (range : 1 .. 100). The higher the sensitivity number, the more easily defocus is recognized. This setting may require testing.
 - b. Click **OK** to save the Sensitivity setting.
8. Click the icon on the **Settings** line.

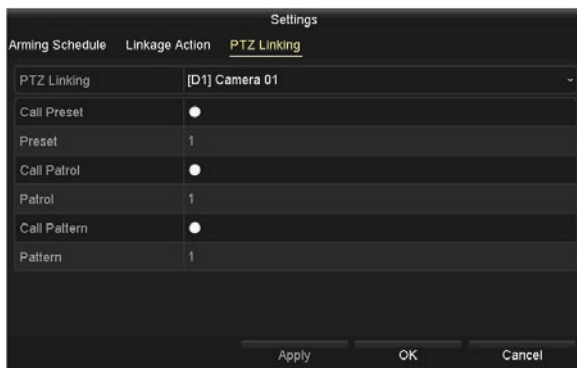
- a. Click the **Arming Schedule** tab. With the Arming Schedule, you can define a schedule for each day of eight weeks (56 days) when defocus is monitored. Time periods cannot overlap.



- b. Click **Apply** to save the settings. You can also click **Copy** to copy the Arming Schedule setup in the window to other days of the week.
- c. Click the **Linkage Action** tab. In this tab you can cause certain actions to occur when defocus is detected.



- d. Select the actions you want to occur, then click **Apply** to save your settings.
- e. Click the **PTZ Linking** tab. With PTZ linking, you can configure the camera to perform a Preset, Patrol, and/or Pattern when an event occurs.

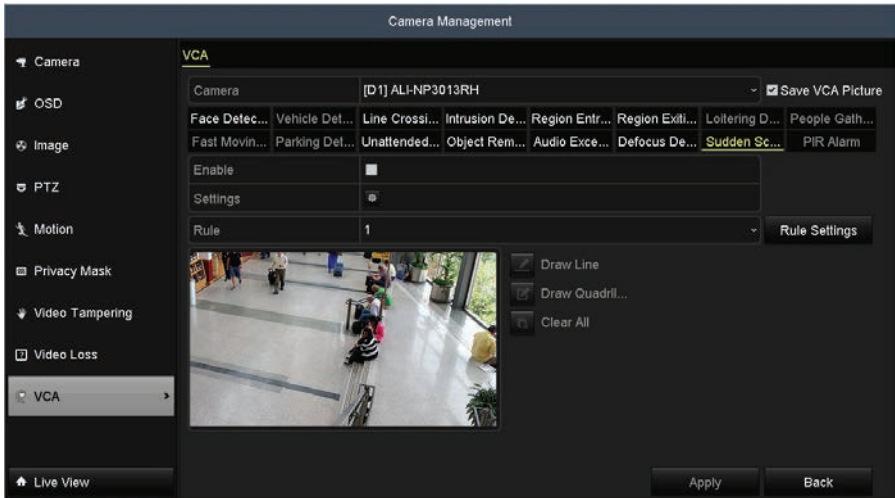


- f. Select the actions you want to occur, then click **Apply** to save your settings.
 - g. Click **OK** to return to the VCA menu.
9. In the VCA menu, click **Apply** to activate the settings.
 10. Repeat steps 2 through 9 above to configure other cameras.

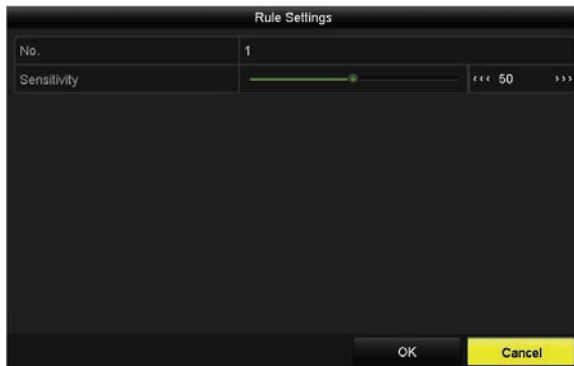
6.10 Sudden Scene Change Detection

Scene change detection detects the change of surveillance environment affected by an external factor, such as the intentional rotation of the camera. Certain actions can be taken when the alarm is triggered. To configure Sudden Scene Change Detection:

1. Open the VCA menu. Go to **Menu | Camera Management | VCA**.
2. On the **Camera** line, open the drop down list, and then select the camera you want to configure.
3. Check the **Save VCA Picture** box to capture a live view image of the VCA event.
4. In the VCA type selection line, click on **Sudden Scene Change Detection**. If the camera supports this feature, it will be highlighted.



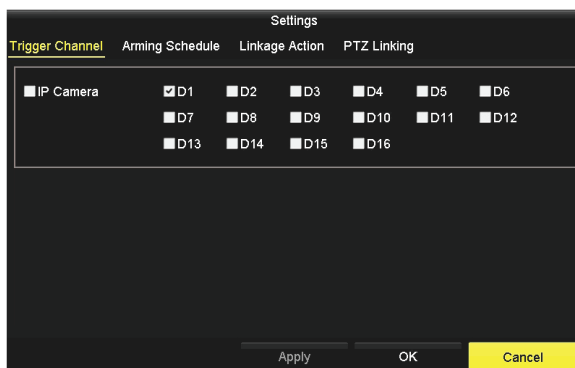
5. On the **Camera** line, open the drop down list and select the camera you want to configure.
6. Check the **Enable** box to select this feature.
7. Click **Rule Settings**.



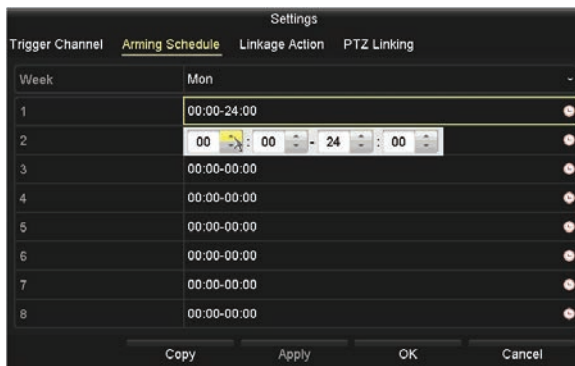
- a. In the Rule Settings window, adjust the **Sensitivity** slider to set the detection sensitivity (range : 1 .. 100). The higher the sensitivity number, the more easily a scene change is recognized. This setting may require testing.
 - b. Click **OK** to save the Sensitivity setting.
8. Click the icon on the **Settings** line.

SECTION 6: VCA FEATURES

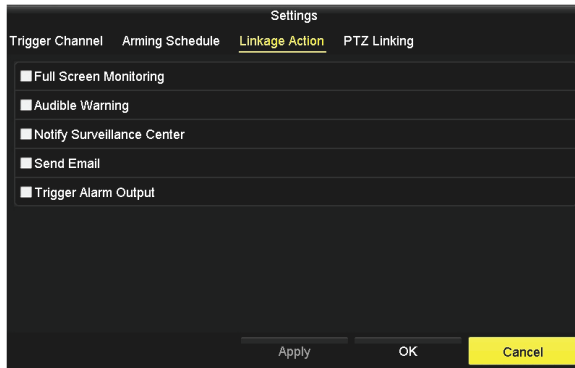
- a. In the **Trigger Channel** window, select the other channels that should trigger recording on this channel, then click **Apply** to save your settings.



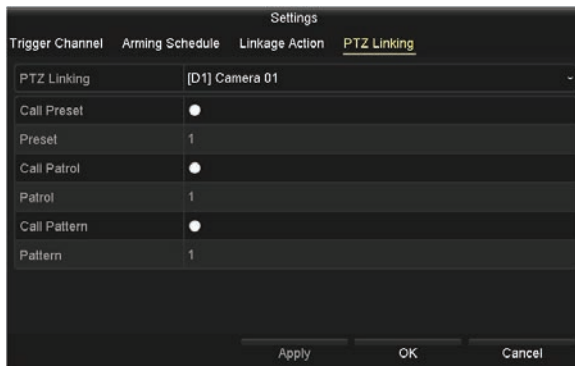
- b. Click the **Arming Schedule** tab. With the Arming Schedule, you can define a schedule for each day of eight weeks (56 days) when scene change is monitored. Time periods cannot overlap.



- c. Click **Apply** to save the settings. You can also click **Copy** to copy the Arming Schedule setup in the window to other days of the week.
- d. Click the **Linkage Action** tab. In this tab you can cause certain actions to occur when a scene change is detected.



- e. Select the actions you want to occur, then click **Apply** to save your settings.
- f. Click the **PTZ Linking** tab. With PTZ linking, you can configure the camera to perform a Preset, Patrol, and/or Pattern when an event occurs.



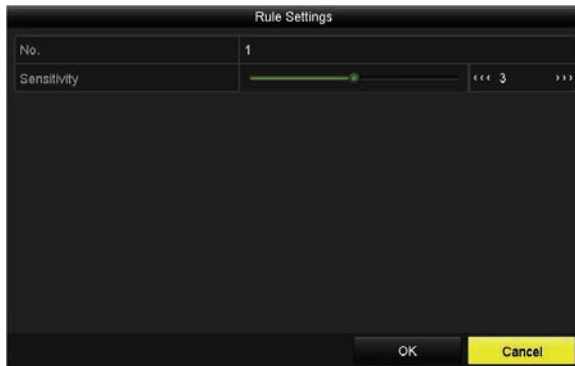
- g. Select the actions you want to occur, then click **Apply** to save your settings.
 - h. Click **OK** to return to the VCA menu.
9. In the VCA menu, click **Apply** to activate the settings.
 10. Repeat steps 2 through 9 above to configure other cameras.

6.11 PIR Alarm

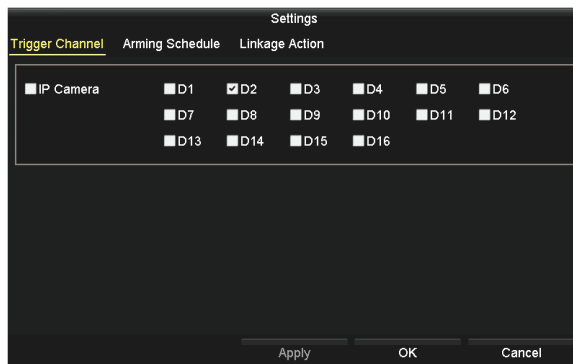
An infrared alarm is generated when heat energy dissipated by a person or any other warm blooded entity such as a dog, cat, etc. moves into the field of view. To configure the camera for infrared alarm detection:

SECTION 6: VCA FEATURES

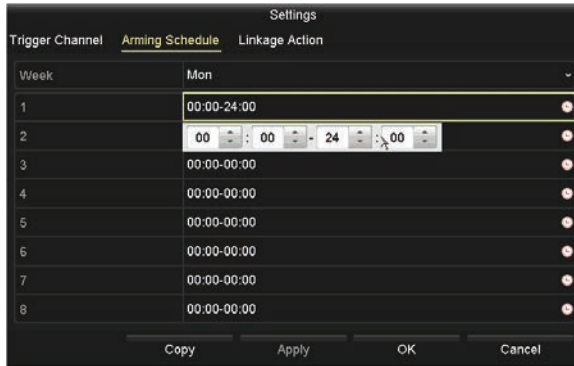
1. Open the VCA menu. Go to **Menu | Camera Management | VCA**.
2. On the **Camera** line, open the drop down list, and then select the camera you want to configure.
3. Check the **Save VCA Picture** box to capture a live view image of the VCA event.
4. In the VCA type selection line, click on **PIR Alarm**. If the camera supports this feature, it will be highlighted.
5. Check the **Enable** box to select this feature.
6. Click **Rule Settings**.



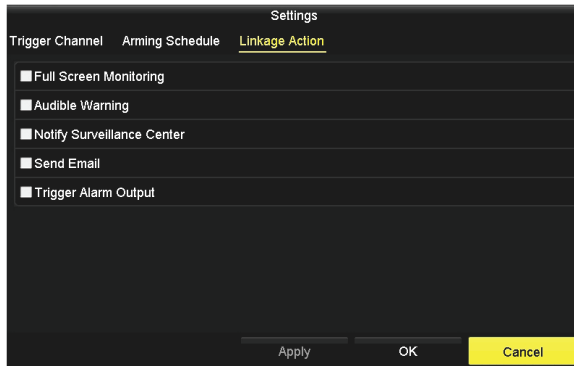
- a. In the Rule Settings window, adjust the **Sensitivity** slider to set the detection sensitivity (range : 1 .. 100). The higher the sensitivity number, the more easily it can recognized a PIR Alarm condition. This setting may require testing.
 - b. Click **OK** to save the Sensitivity setting.
7. Click the icon on the **Settings** line.
 - a. In the **Trigger Channel** window, select the other channels that should trigger recording on this channel, then click **Apply** to save your settings.



- b. Click the **Arming Schedule** tab. With the Arming Schedule, you can define a schedule for each day of eight weeks (56 days) when scene change is monitored. Time periods cannot overlap.



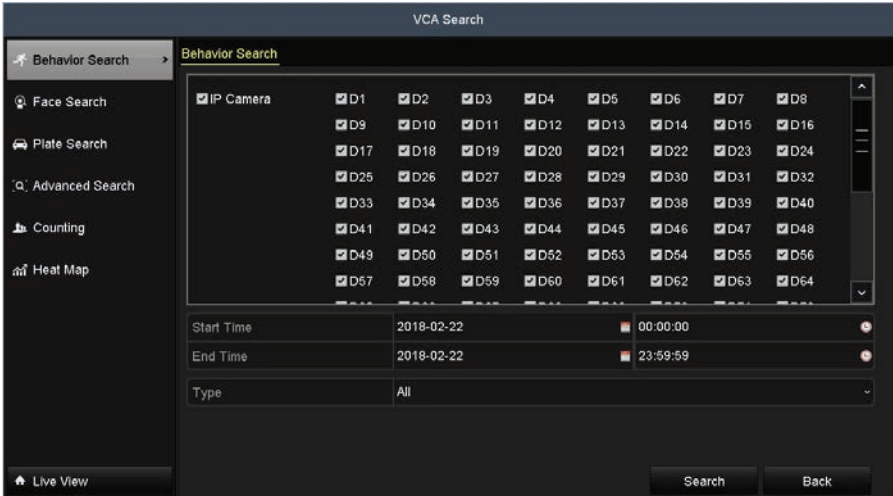
- c. Click **Apply** to save the settings. You can also click **Copy** to copy the Arming Schedule setup in the window to other days of the week.
- d. Click the **Linkage Action** tab. In this tab you can cause certain actions to occur when a PIR Alarm condition is detected.



- e. Select the actions you want to occur, then click **Apply** to save your settings.
8. In the VCA menu, click **Apply** to activate the settings.
9. Repeat steps 2 through 8 above to configure other cameras.

6.12 VCA Search features

VCA Search features are used to quickly analyze data generated from VCA analysis of video images. To use VCA Search features, the VCA feature must first be enabled and configured in the camera(s). **NOTE:** All Alibi cameras do not support all VCA features shown in this section. To open the VCA Search interface, go to **Menu | VCA Search**.



6.12.1 Behavior search

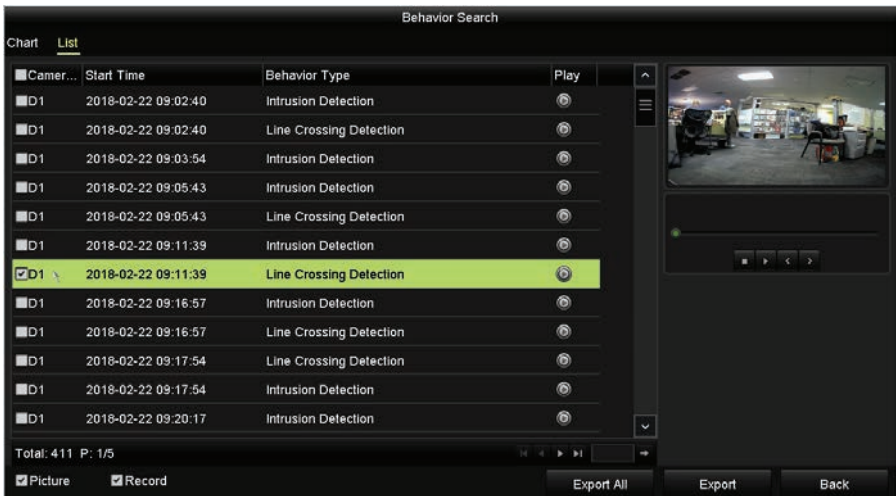
The behavior analysis detects suspicious behavior based on VCA analysis. To use this analysis, specific linkage actions are performed when the VCA alarm is triggered. To use VCA Search - Behavior Search:

1. Configure the camera for any of the following VCA features:
 - Line Crossing detection
 - Intrusion Detection
 - Unattended Baggage Detection
 - Object removal Detection
 - Region Entrance Detection
 - Region Exiting Detection
2. Open the VCA Search Behavior Search menu. Go to **Menu | VCA Search | Behavior Search**. See above.
3. Check the box(es) for the camera(s) you want to search.
4. Click the **Start Time** field and then set the date and time at which you want to search begin the search for data. Similarly, set the End Time field.
5. Open the **Type** drop down list, and then select the type of VCA event you want to search for. You can leave the option at All to find all VCA events.

6. Click the **Search** button at the bottom of the screen. In this screen, you can peruse thumbnails of video clips, play them, and export them to an external device or flash drive. To export a clip, check the box(es) for the clip(s) you want to export, and then click the **Export** button at the bottom of the screen.



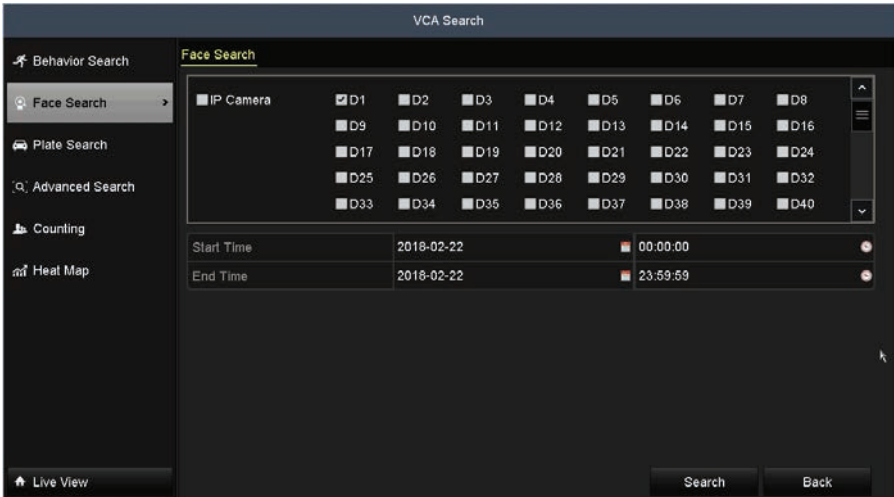
7. You can also view the result in **List** format by click the **List** option in the upper left corner. In this screen, you can play video clips and export them to an external device or flash drive. To export a clip, check the box(es) for the clip(s) you want to export, and then click the **Export** button at the bottom of the screen.



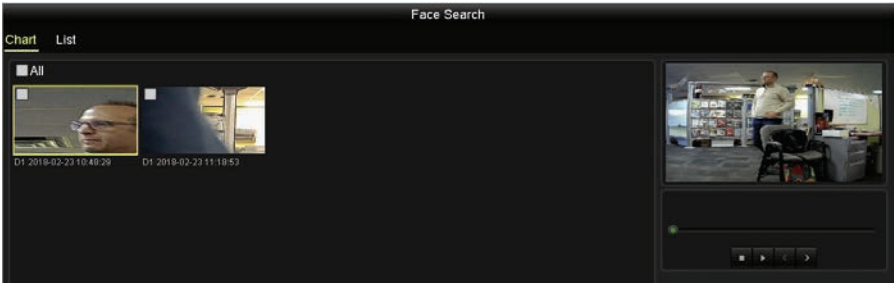
6.12.2 Face search

Face Search displays occurrences of the VCA Face Detection feature. This feature must be enabled and configured in a camera before using a VCA Search. To use VCA Search - Face Search:

1. Configure VCA Face Detection in a camera. See “6.1 Face Detection” on page 62. You can verify that the camera is generating Face Detection alarms through Log Search.
2. Open the VCA Search Face Search menu. Go to **Menu | VCA Search | Face Search**.



3. Check the box(es) for the camera(s) you want to search.
4. Click the **Start Time** field and then set the date and time at which you want to search begin the search for data. Similarly, set the End Time field.
5. Click the **Search** button at the bottom of the screen. In this screen, you can peruse thumbnails of video clips, play them, and export them to an external device or flash drive. To export a clip, check the box(es) for the clip(s) you want to export, and then click the **Export** button at the bottom of the screen.



- You can also view the result in **List** format by click the List option in the upper left corner. In this screen, you can also play video clips and export them to an external device or flash drive.

6.12.3 Plate Search

Advanced Search enables you to detect license plates from specific countries. The camera you use must be capable of using video content analytics (VCA) to detect these kinds of images in the video stream. To use this feature:

- Open the Advanced Search menu. Go to **Menu | VCA Search | Plate Search**.



NOTE Currently Alibi cameras do not support the VCA Plate Recognition feature.

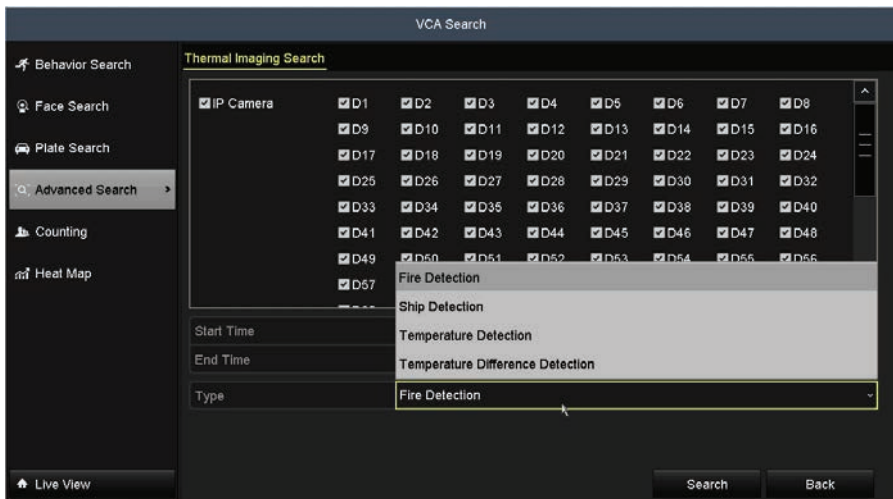
6.12.4 Advanced Search

Advanced Search enables you to find specific types of events, including:

- Fire Source Detection
- Ship Detection
- Temperature Detection
- Temperature Difference Detection.

The camera you use must be capable of detecting these kinds of events. To use this feature:

1. Open the Advanced Search menu. Go to **Menu | VCA Search | Advanced Search**.



2. Click the **Start Time** field and then set the date and time at which you want to search begin the search for data. Similarly, set the End Time field.
3. Open the **Type** drop down list, and then select the type of event you want to search for.
4. Click the **Search** button at the bottom of the screen. In this screen, you can peruse thumbnails of video clips, play them, and export them to an external device or flash drive. To export a clip, check the box(es) for the clip(s) you want to export, and then click the **Export** button at the bottom of the screen.

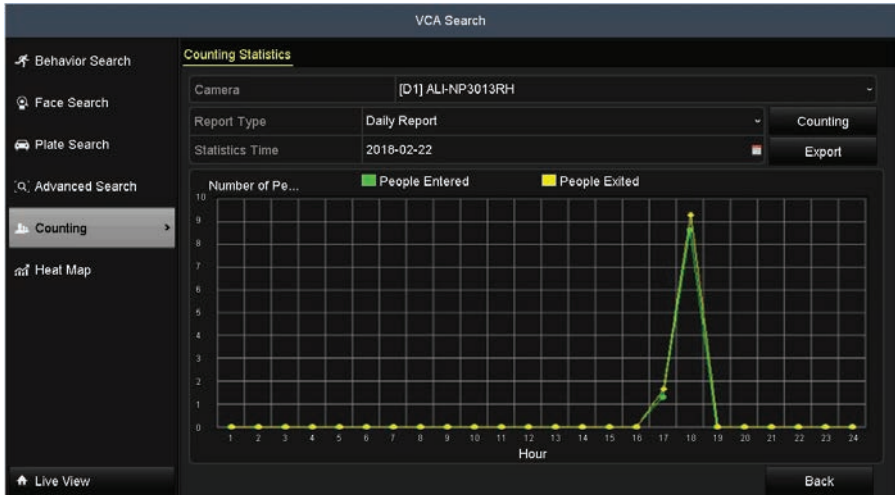
6.12.5 Counting

Counting is used to determine the number of objects entering or leaving a designated area in the field of view. The data can be displayed in a line graph across daily, weekly, monthly or annual time range.

NOTE The IP camera used for Counting must include a microSD card for data accumulation.

To use Counting:

1. Open the VCA Search Counting menu. Go to **Menu | VCA Search | Counting**.



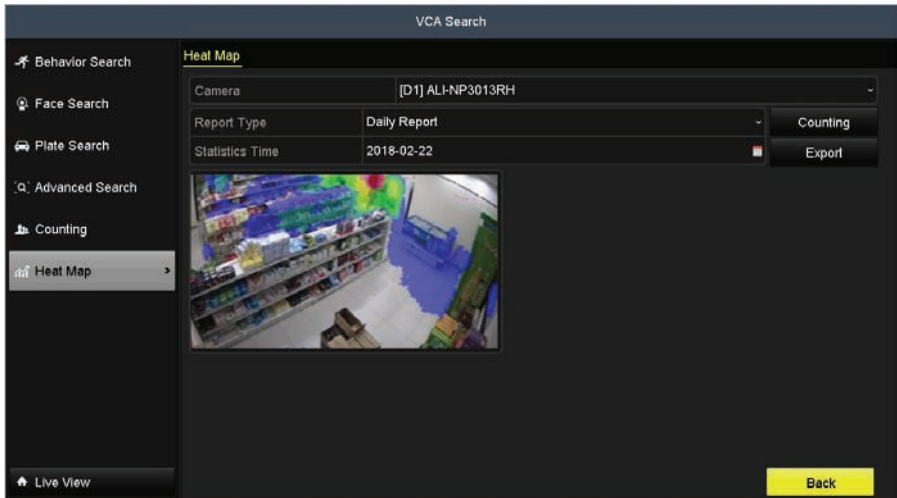
2. Open the **Camera** drop down list, and then select the camera you want to search.
3. Open the **Report Type** drop down list, and then select the time span for which you want to count Region Entrance and/or Exiting alarms. You can select either **Daily Report**, **Weekly Report**, **Monthly Report** or **Annual Report**.
4. Click the **Statistics Time** field, and then select the day for which to generate a report.
5. Click the **Counting** button to start counting across the report type you selected.
6. Click **Export** to save the statistics report in Microsoft® Excel® format.

6.12.6 Heat map

The Heat Map feature presents a graphical representation of loitering data represented by colors. A red color block indicates the most welcome area, and blue color block (0, 0, 255) indicates the less-popular area. Heat map is normally used to analyze the visit times and dwell time of customers in an designated area of the field of view. The heat map function must be supported by the IP camera and the corresponding configuration must be set. Currently, this feature is available with the Alibi fisheye camera only.

1. Configure a camera for the VCA features PIR Alarm. See “6.11 PIR Alarm” on page 99.
2. Open the VCA Search Heat Map menu. Go to **Menu | VCA Search | Heat Map**.

SECTION 6: VCA FEATURES



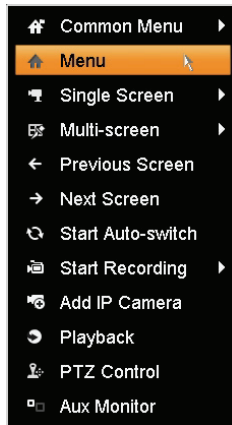
3. Open the **Camera** drop down list, and then select the camera you configured for PIR alarm detection.
4. Open the **Report Type** drop down list, and then select the time span for which you want to count alarms. You can select either **Daily Report**, **Weekly Report**, **Monthly Report** or **Annual Report**.
5. Click the **Statistics Time** field, and then select the day for which to generate a report.
6. Click the **Counting** button to start counting across the report type you selected.
7. Click **Export** to save the statistics report in Microsoft® Excel® format.

SECTION 7

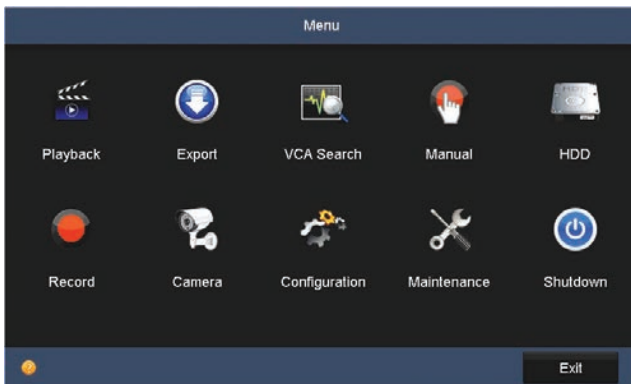
Record, Playback and Video Backup

After the initial setup of your NVR using the Wizard, the Menus interface enables you to refine your configuration settings and expand the functionality of the system. To use most menus, the user must log into the NVR system, either locally or remotely, with administrative privileges.

To open the Menu system from the Live View screen, right click anywhere in the screen, then select **Menu**.



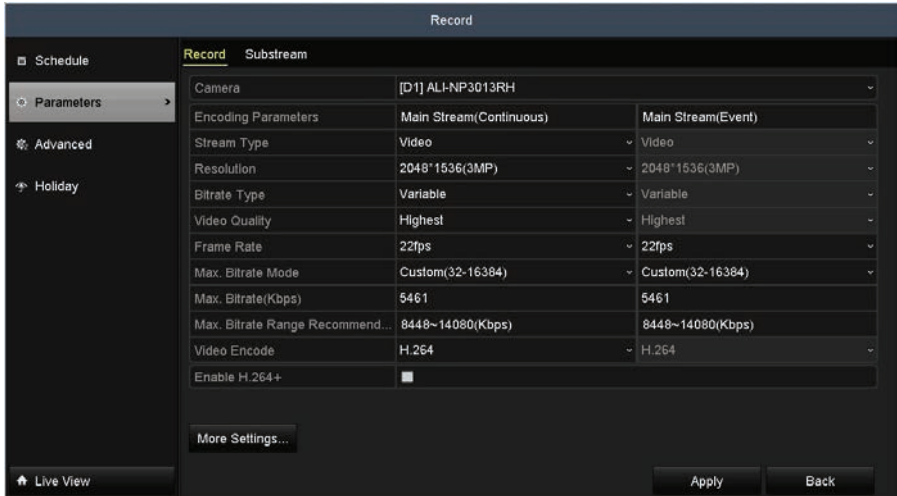
After selecting **Menu**, a login window will open. In the Login window, select a User Name with administrative privileges, enter its password, then click **OK**. A window of Menu icons will open. **NOTE:** When the system option **Enable ID Authentication** is disabled (see the **Configuration - General** settings submenu), the Login window to open the Menu does not appear.



7.1 Configuring record settings

7.1.1 Setting camera parameters

1. Enter the **Record** settings interface to configure the encoding parameters. Go to **Menu | Record | Parameters**.



2. Select the **Record** tab page you want to configure. Use this menu to select different parameters for Continuous recording and Event recording. You can configure the stream type, the resolution, and other parameters.
 - **Enable H264 +**: Uses enhanced H.264 encoding. The camera must be rebooted after this option is selected.
3. Click **Apply** to save your new configuration settings.
4. Click **More Settings** to configure other parameters.

More Settings	
Pre-record	5s
Post-record	5s
Expired Time (day)	0
Record Audio	<input checked="" type="checkbox"/>
Video Stream	Main Stream

OK Back

Parameters include:

- **Pre-record:** The length of time you set to record before the scheduled time or event. For example, when an alarm triggered the recording at 10:00, if you set the pre-record time as 5 seconds, the camera records it at 9:59:55.
 - **Post-record:** The length of time you set to record after the event or the scheduled time. For example, when an alarm triggered the recording ends at 11:00, if you set the post-record time as 5 seconds, it records till 11:00:05.
 - **Expired Time:** The expired time is the longest time a recording is kept on the HDD. If the deadline is reached, the file will be deleted. If you set the expired time to 0, the file will not be deleted. This parameter is usually determined in consideration of the capacity of the HDD.
 - **Record Audio:** Check the checkbox to enable audio recording.
 - **Video Stream:** You can select **Main Stream**, **Sub-Stream** or **Dual Stream** for recording. When you select sub-stream, you can record for a longer time with the same storage space.
- a. Select the options you prefer from the drop down options lists.
 - b. Enter the **Expired Time (day)** length and check **Record Audio** if appropriate.
 - c. Click **OK** to save the settings.
5. Open the **Sub-stream** tab page and then configure the parameters of the camera.

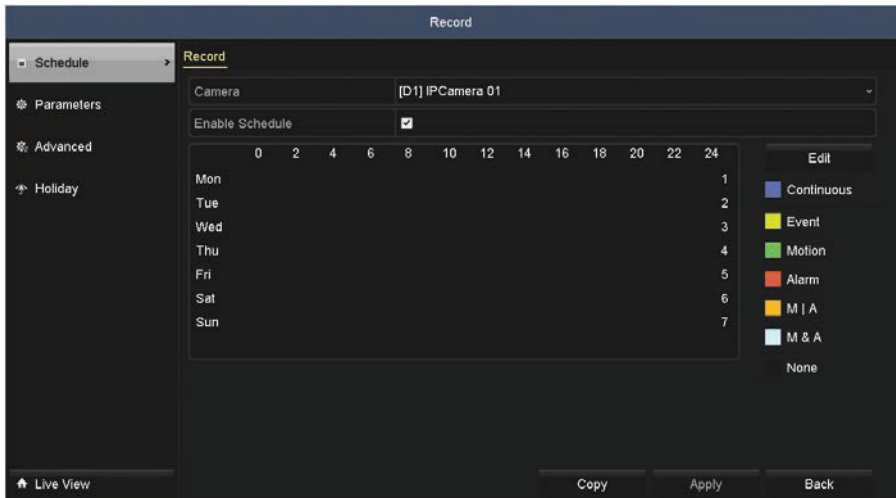


- Click **Apply** to save the settings.

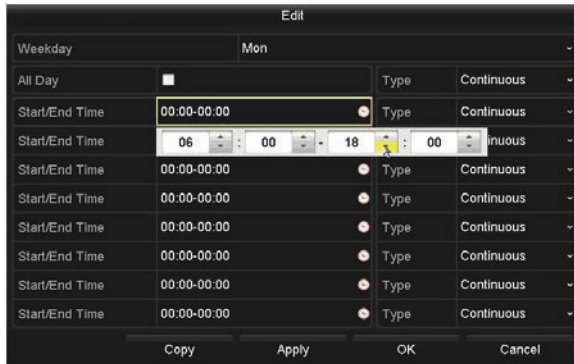
7.1.2 Configuring Record schedule

The record schedule can be used to automatically start and stop recording at preset times.

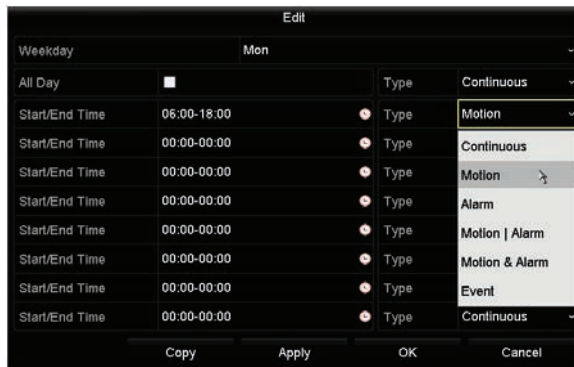
- Open the Record Schedule menu. Go to **Menu | Record | Schedule**.



2. To configure the Record schedule:
 - a. Open the **Camera** drop-down list to select the camera you want to configure.
 - b. Check the **Enable Schedule** box.
 - c. Click **Edit**, or use the graphical method to apply recording modes to hours of the day.
 - i. If you clicked the **Edit** button, a record schedule list opens.



- ii. Open the **Schedule** line drop down list and select the day you want to create a record schedule for.
- iii. To schedule all-day recording, check the checkbox after the All Day item. To setup specific start and end times, click the clock icon to open a time setting popup window.
- iv. In the **Type** column, select the type of recording trigger you want to use. "Motion" recording is recording triggered by some kind of motion detected in the video image.



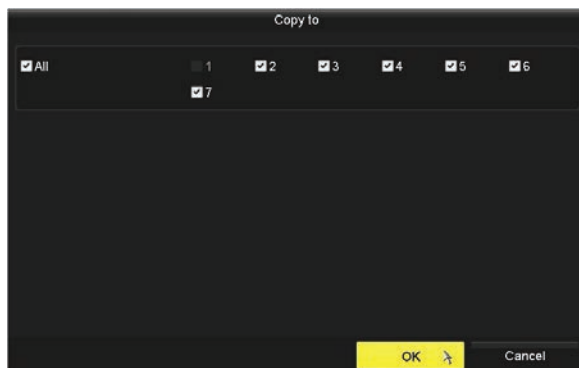
- Click **Apply** to save your settings.

SECTION 7: RECORD, PLAYBACK AND VIDEO BACKUP

NOTE

You can define up to eight recording time periods for each day, each with a specified recording type. Recording time periods cannot overlap with each other. Each recording period can use either Normal or Motion triggered recording.

- v. Repeat the steps above to schedule recording for other days of the week. If the same schedule can also be applied to other days, click **Copy** (see the window below), select the days you want to copy the schedule to, then click **OK**.

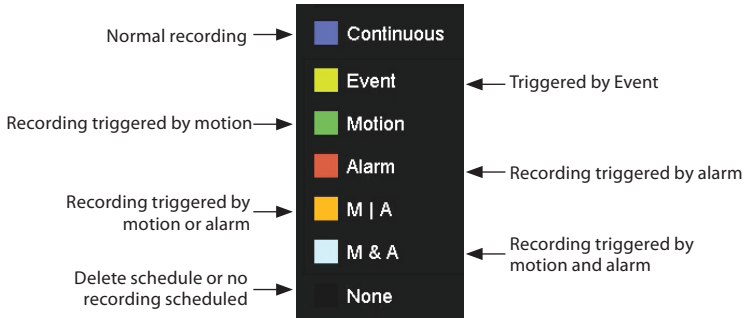


The result will look like the following schedule.



- vi. To use the **graphical method** to draw the schedule:
 - Click the color icons on the right for the recording mode, then drag the mouse pointer across the area of the chart (day of the week, hours of the day) where you want to use that type of recording. Blocks on the chart,

each representing 1 hour of one day, will be colored for the recording mode you selected. A descriptions of the color icons are shown in the figure below.

**NOTE**

Alarm triggered recording is available for only some camera models supported by the Alibi NVR. Consult your vendor support organization for more information.

- Recording schedules can include a combination of different modes. An example of a graphically created schedule is shown below.

The screenshot shows the 'Record' configuration interface for camera [D1] IPCamera 01. The 'Enable Schedule' checkbox is checked. The main area displays a 24-hour grid for each day of the week (Mon-Sun). The grid is divided into segments representing different recording modes. A legend on the right identifies the modes: Continuous (blue), Event (yellow), Motion (green), Alarm (red), M | A (orange), M & A (cyan), and None (white). A note at the bottom states: 'Note: Operation is invalid when the number of time segments exceeds the limit (8)'. Buttons for 'Copy', 'Apply', and 'Back' are visible at the bottom of the screen.

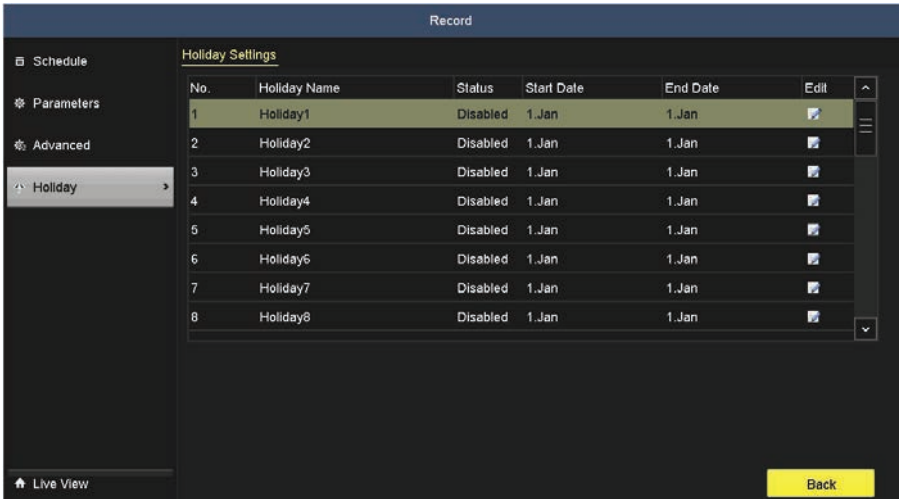
- Click **Apply** to validate the settings.
3. If the settings can be applied to other camera channels, click **Copy**.
 4. In the **Copy** menu, click the channels you to which you want to copy the schedule to, then click **OK**.

7.1.3 Record Holiday settings

You can create a recording schedule for holidays only after specifying which days are holidays. Holidays can be specified by day (of the year), week or month. When these holidays occur, the Holiday recording schedule will be performed instead of the normal Monday through Sunday recording schedule setup using the procedure above in “7.1.2 Configuring Record schedule” on page 112.

To specify which days are holidays and create a recording schedule for these days, do the following:

1. Open the Record Holiday menu. Go to **Menu | Record | Holiday**.



2. Click on the **Edit** icon in an entry in the list. You can define up to 31 different holidays periods.

The screenshot shows the 'Edit' dialog box for a holiday. It contains the following fields:

- Holiday Name: Holiday1
- Enable:
- Mode: By Month (dropdown menu)
- Start Date: Jan (dropdown menu) 1 (dropdown menu)
- End Date: Jan (dropdown menu) 1 (dropdown menu)

At the bottom of the dialog are three buttons: Apply, OK, and Cancel.

- In the Edit window, click on the Holiday Name field, and then enter a common name for the holiday.
- Click the **Enable** box to check it.
- Open the **Mode** drop down list and select either **By Date**, **By Week** or **By Month**. Depending on your selection, the **Start Date** and **End Date** fields will adjust accordingly.
- Edit the **Start Date** and **End Date** fields as needed. A Holiday can be a single day or range of days. In the window below, a New Years Day holiday was specified.

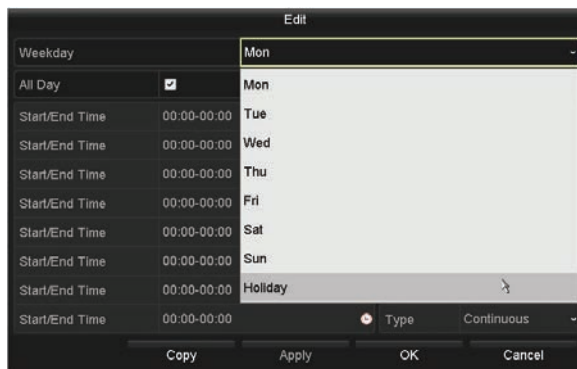
Edit	
Holiday Name	New Years Day
Enable	<input checked="" type="checkbox"/>
Mode	By Date
Start Date	01-01-2017
End Date	01-01-2017

Apply OK Cancel

- Click **Apply** to save your setting, and then click **OK**. The Holiday Settings window will show the holidays you created.

Record					
Holiday Settings					
No.	Holiday Name	Status	Start Date	End Date	Edit
1	New Years Day	Enabled	01-01-2017	01-01-2017	
2	Holiday2	Disabled	1.Jan	1.Jan	
3	Holiday3	Disabled	1.Jan	1.Jan	
4	Holiday4	Disabled	1.Jan	1.Jan	
5	Holiday5	Disabled	1.Jan	1.Jan	
6	Holiday6	Disabled	1.Jan	1.Jan	
7	Holiday7	Disabled	1.Jan	1.Jan	
8	Holiday8	Disabled	1.Jan	1.Jan	

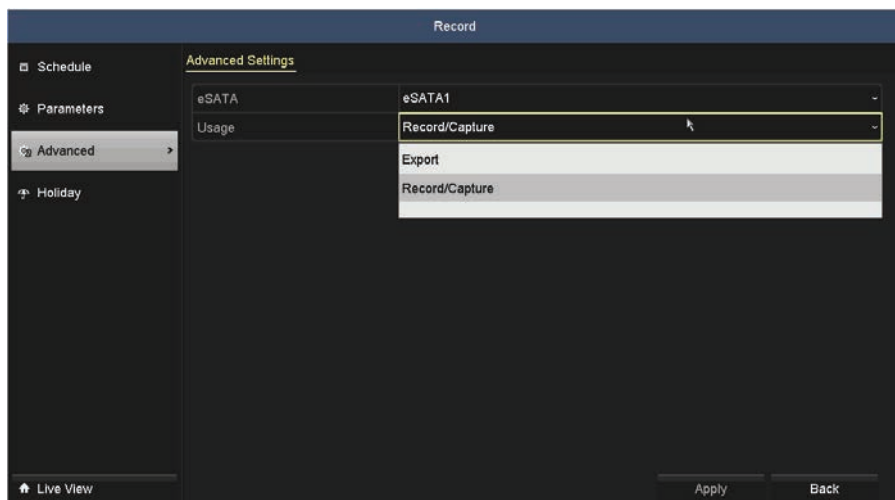
- Open the Record Schedule window. Go to **Menu | Record | Schedule**. See “7.1.2 Configuring Record schedule” on page 112.
- Click **Edit**.



- In the Edit window, open the Weekday drop down list, and then select **Holiday**. Edit the Edit window as needed, and then click Apply and OK to save your settings.

7.1.4 Record Advanced settings

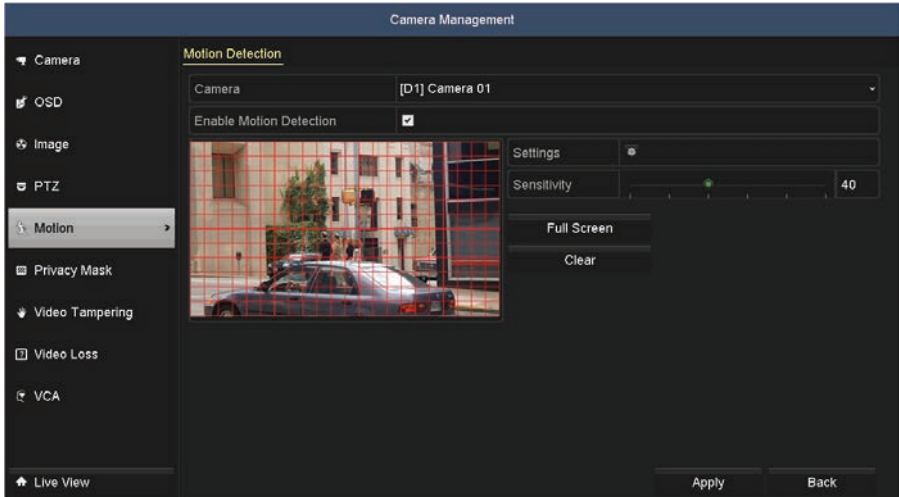
Use the Record Advanced Settings menu to configure the purpose of the storage device connected to the eSATA port.



7.1.5 Configuring Motion Detection Recording

Follow the steps to set the motion detection parameters. Motion detection events can trigger several kinds of actions in the NVR, including channels to start recording, full screen monitoring, an audio warning, notification sent to the surveillance center, etc. Follow the steps below to schedule a recording triggered by a motion detection.

1. Open the Motion Detection menu. Go to **Menu | Camera | Motion**.

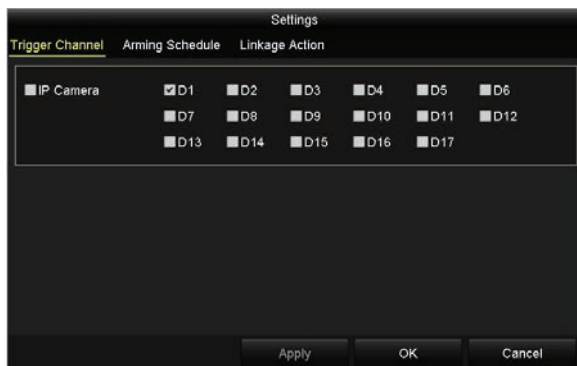


2. To configure Motion Detection (see screen above):
 - a. Choose camera you want to configure from the drop down list.
 - b. Check the **Enable Motion Detection** box.
 - c. Click the **Full Screen** select button.
 - d. If you want to sense for motion detection in all areas of the video, click **Clear All**, and then drag a rectangle over the entire video screen.

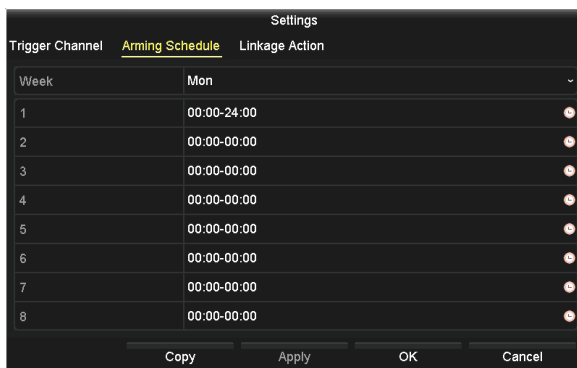
NOTE: The example shown here is for a Alibi™ camera. Other camera brands and models have different methods for designating the motion detection areas.

To deselect an area selected for motion detection, drag a rectangle across that area. To clear all areas selected, click **Clear**.
 - e. Click **Settings** to open the **Settings Trigger Channel** tab window.

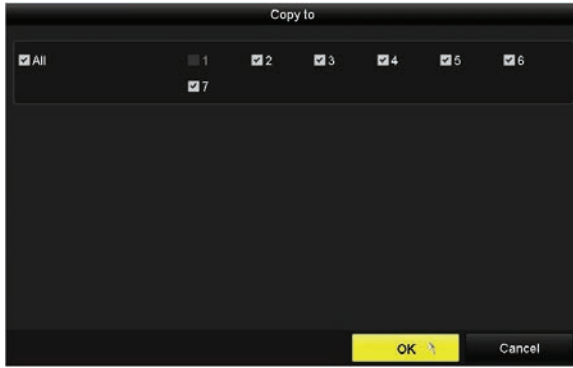
SECTION 7: RECORD, PLAYBACK AND VIDEO BACKUP



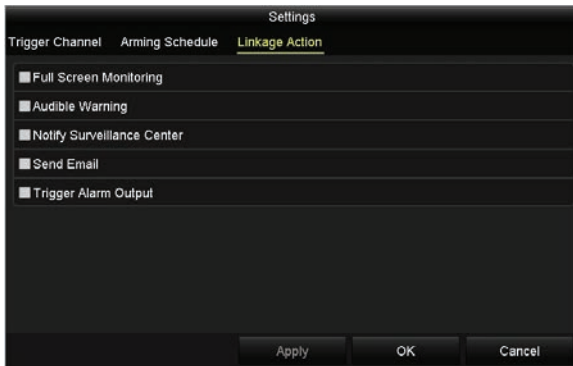
- f. Select the other channels that should trigger recording on this channel, then click **Apply** to save your settings.
- g. Click the **Arming Schedule** tab. In this tab you can define up to eight periods for each day. Periods must not overlap.



- h. Click the down arrow in the Mon field (see above) to setup the schedule for a different day, and/or click **Copy** to copy the Arming Schedule you setup in the window to other days of the week. Click **OK** to confirm your selections.



- i. In the Arming Schedule menu, click **Apply** to save the settings.
- j. Click the **Linkage Action** tab. In this tab you can cause certain actions to occur when motion triggered recording occurs.



- k. Select the actions you want to occur, then click **Apply** to save your settings, and **OK** to return to the **Motion** menu. The **Notify Surveillance Center** and **Send Email** options require additional network settings.
3. In the **Motion** menu, click **Apply** to save your settings for this camera.

NOTE

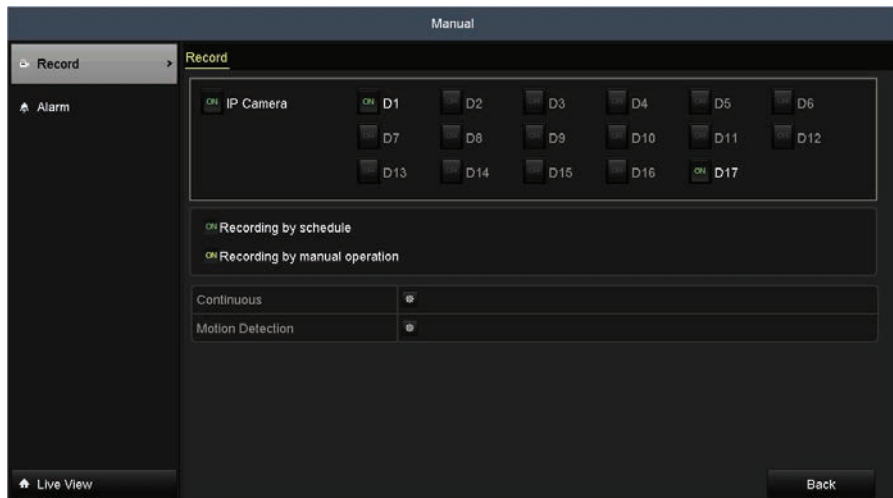
*Test your settings during broad conditions to ensure that motion in the field of view triggers an action. You may need to return to this menu later to adjust the **Sensitivity** slider to ensure it is working adequately.*

7.1.6 Manual record

Follow the steps below to begin manual recording. Manual recording, once initiated, requires a manual cancel of the record. The manual recording can occur prior to the scheduled recording.

SECTION 7: RECORD, PLAYBACK AND VIDEO BACKUP

1. Open the Manual settings menu. Go to **Menu | Manual**.



2. To enable Manual Record:
 - a. Select **Record** on the left menu frame.
 - b. Click the status button before camera number to change the label from **OFF** to **ON**, if necessary. See the example above.
 - c. Click the icon after **Normal** or **Motion Detection**.
 - d. When the Attention window opens, click **Yes**.



3. To disable Manual Record:
 - a. Select **Record** on the left menu frame.
 - b. Click the status button before camera number to change the label from ON to OFF.
 - c. Click the icon after **Normal** or **Motion Detection**.
 - d. When the Attention window opens, click **No**.

NOTE

Green "ON" icon means that the channel is configured with a record schedule.
If the NVR is rebooted, manual record operations are canceled.

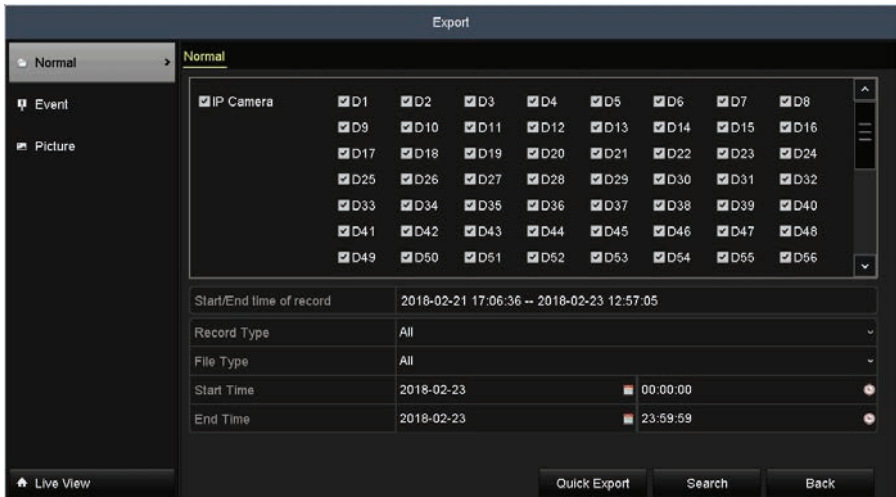
7.1.7 Configuring HDD Group for Recording

You can group the HDDs and save the record files in a specific HDD group. You must have multiple HDDs installed in the system to perform this configuration. For more information, see “11.3 Configuring the HDD Quota/Group mode” on page 197.

7.1.8 Files Protection

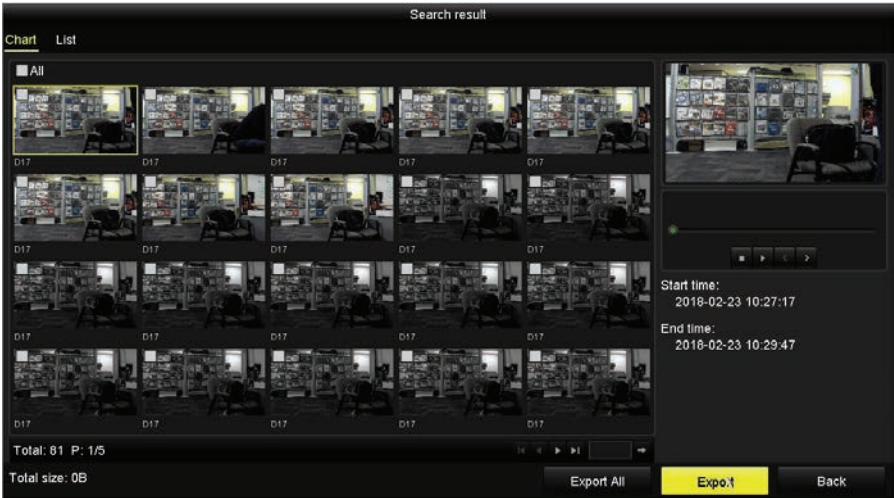
You can lock the recorded files or to protect them from being overwritten when the HDD becomes full.

1. Open the **Export** menu. Go to **Menu | Export**.

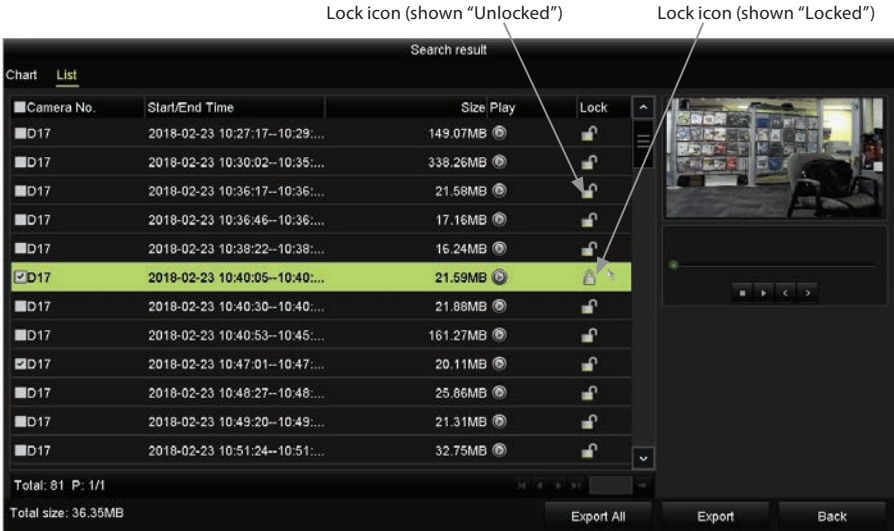


2. Check the box(es) for the channel(s) you want to investigate.
3. Configure the **Record Type**, **File Type** (locked or unlocked), and **Start Time** and **End Time**.
4. Click **Search** to show the results.

SECTION 7: RECORD, PLAYBACK AND VIDEO BACKUP



- Click **List** in the upper left corner.



- To protect the record files, determine which files you want to protect, and then click the icon in the **Lock** column to show a "locked" padlock (indicating that the file is locked). Similarly, unlock files by clicking on the "locked" icon to show an "unlocked" padlock. When unlocking a file, a confirmation window will open.

NOTE *The file of a recording in progress cannot be locked.*

7.2 Playback

You can playback recorded video files instantly, or in several ways including Normal (by setting the channel and time), Event, Tag (tagging and retrieving tagged video clips), and using Smart features in the Alibi firmware. You can also play files on external media. Multi-channel playback supports 4 channels at up to 8 MP resolution and 16 channels at up to 1080p resolution.

7.2.1 Instant playback by channel

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

Instant playback by channel

In Live View mode, click the channel you want to playback, then click the playback icon on the Quick Setting toolbar. In the instant playback mode, only recordings made during the previous five minutes on the channel are played.



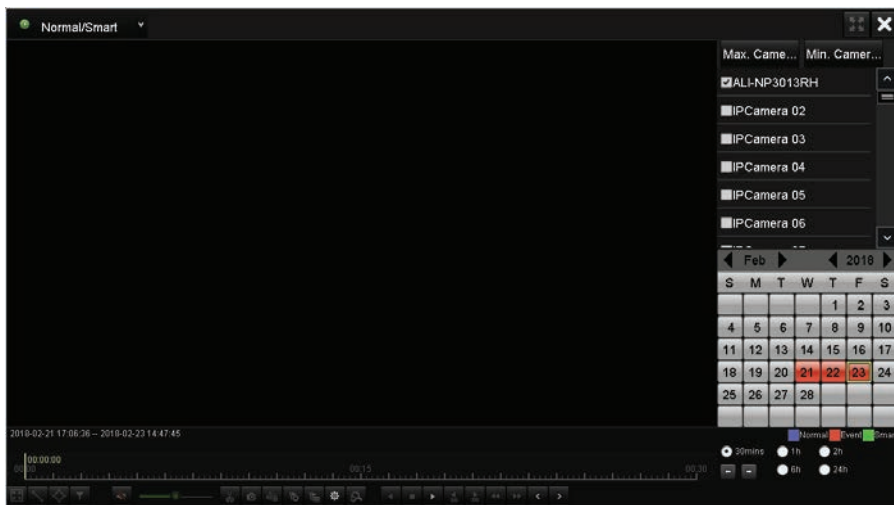
7.2.2 Playback by channel - menu and screen controls

Playback menu screen controls appear after accessing recordings from a camera. To access and play these files:

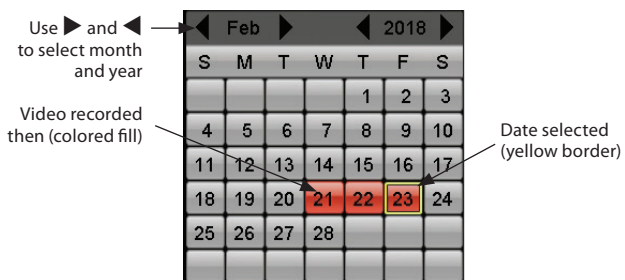
1. Open the Playback menu. Go to **Menu | Playback**.

SECTION 7: RECORD, PLAYBACK AND VIDEO BACKUP

- In the **Playback** screen, check the box for the camera channel(s) you want to playback. In the example shown below, **Camera 01** (at the top of the list) was selected.



- In the calendar section, click the day when the video clip you want to play was recorded. In the example shown below, October 28, 2015 was selected. Notice that colored marks in the timeline at the bottom of the screen appeared. These marks indicate when and what type of recordings were made for that camera(s) selected.

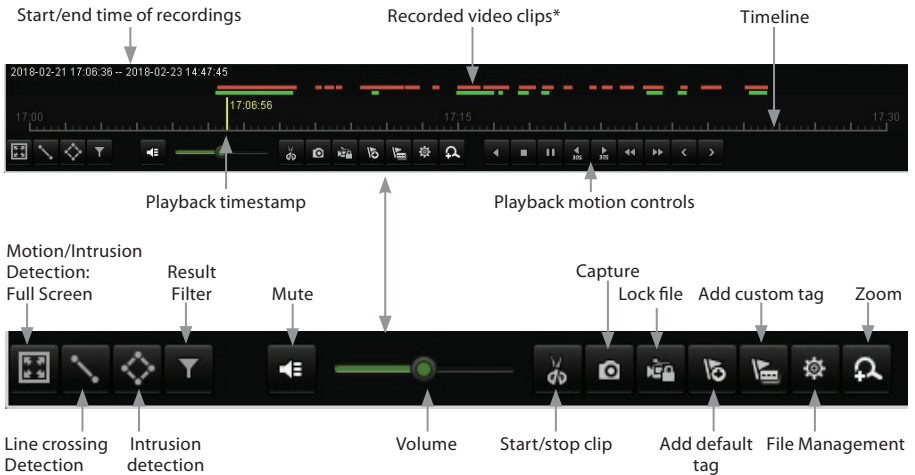


- Click the **Play** button (►) in the playback controls panel at the bottom of the screen.

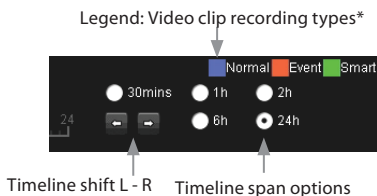
SECTION 7: RECORD, PLAYBACK AND VIDEO BACKUP



Playback toolbar and indicators at the bottom of the window are described below.



SECTION 7: RECORD, PLAYBACK AND VIDEO BACKUP



* Colors marking video clips are shown in the legend. When **Smart** marks () appear, Motion, Line or Intrusion detection is enabled and sensed in the video clip.

Toolbar items

















Start/end time of recordings: Indicates the earliest and latest date and time when recordings for the selected cameras (channels) are available.

Playback timestamp: Indicates the position on the timeline when the frame being played back was recorded. The exact recorder time is also shown.

Recorded video clips: These marks indicate when video was recorded on the timeline. The color legend is shown to the right. When Smart analysis features are enabled, green marks may appear above the timeline.

Timeline: Graphical representation when video clips were recorded across a time span. The timeline can be adjusted to span 30 minute, 1 hours, 2 hours, 6 hours, or 24 hours, and can be shifted left or right using clicking the options to the right of the toolbar.

Playback motion controls: Control the playback of recorded video. See the table below.

Button	Operation	Button	Operation	Button	Operation	Button	Operation
	Audio on/ Mute		Adjust volume		Start/Stop clipping		Capture
	File lock		Add default tag		Add customized tag		File Management
	Digital Zoom		Pause reverse play/ Reverse play/ Single-frame reverse play		Stop		Pause play/ Play/ Single-frame play
	30s forward		30s reverse		Speed down		Speed up

Playback toolbar icons

Motion/Intrusion Detection: Full Screen: Enables Smart motion and intrusion detection across the entire video image. To apply this feature, playback video, and then click this icon. If motion or intrusion is detected in any video clip marked on the timeline, a green “Smart” mark will appear for it above the timeline.

Line Crossing Detection: With this feature you can define a line in the video image and show when an object cross the line in either direction. To apply this feature, playback video, click this icon, and then click on two points in the video frame to set the endpoints of a line. A red line will appear over the video, and green Smart marks will appear above the timeline where motion is detected across the line.

Intrusion Detection: With this feature you can define a quadrilateral area in the video image and show when an object enters or exits the area. To apply this feature, playback video, click this icon, and then click four points in a circular fashion in the video frame to set the four corners of the quadrilateral area. A red quadrilateral will appear over the video, and green Smart marks will appear above the timeline where motion is detected in or out of the area.

Result Filter: Feature that can filter “Smart” results for Gender, Ages, or Glasses. To use this feature, click the **Filter** icon at the bottom of the screen open the drop down lists for each parameter to select the options you prefer, and then click **OK** to save and apply your settings. Results of applying the filter are reflected in the Smart marks above the timeline. Good luck.



Mute: Mutes or un-mutes audio during playback. Functional only when audio is recorded with the video.

Volume: Slider for adjusting the audio during video playback.

Start Clip / Stop Clip: Feature used to create a clip from video being played back. See “7.3.5 Exporting Video Clips during playback” on page 153 for more information.

Lock File: Use this feature during video playback to prevent the video clip being played from being overwritten by newer video recorded on the HDD.

Add Default Tag: Use this feature during video playback to assign an identifier (tag) to the clip being played back. The clip can then be easily retrieved later by searching for tagged video. See “7.2.5 Playback by Tag” on page 133 for more information.

Add Custom Tag: Use this feature during video playback to create a specific identifier (tag) to the clip being played back. The clip can then be easily retrieved later by searching for tagged video. See “7.2.5 Playback by Tag” on page 133 for more information.

SECTION 7: RECORD, PLAYBACK AND VIDEO BACKUP

File Management: Opens the File Management menu. This menu is useful when creating and exporting video clips from video being played back.

Zoom: Use this feature to digitally zoom in on areas of video during video playback. See “7.2.12 Digital Zoom” on page 142 for more information.

Legend: Video clip recording types: Defines colors used to identify the reason(s) why a video clip was recorded. Options are Normal (continuous recording), Event, and Smart (when video meets Smart search criteria).

Timeline shift L - R: Use to shift the timeline window.

Timeline Span options: Click any option to set the length of the timeline.

Thumbnail search

To open the thumbnail search feature, rest the mouse pointer over the timeline during playback to open thumbnail images of the recording in the lower part of the playback screen.



To move to a thumbnail image, click the thumbnail of interest.

7.2.3 Create video tag

Video tags are useful for identifying important video clips and quickly retrieving them. Video tags can be created in several different playback modes, then retrieved in the Playback Tag mode. To playback, see “7.2.5 Playback by Tag” on page 133.

To create a video tag:

1. Open the playback screen and then locate the video you want to tag, and then click the **Add Customized Tag** icon in the lower left corner of the screen.



2. Click the Tag Name field, and then enter a name for the tag using the virtual keyboard. Click the key in the lower right corner of the keyboard to save the **Tag Name**.
3. Click OK to close the **Add Tag** window.

7.2.4 Playback by Event Search

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

1. Open the **Playback** interface. Go to **Menu | Playback**.

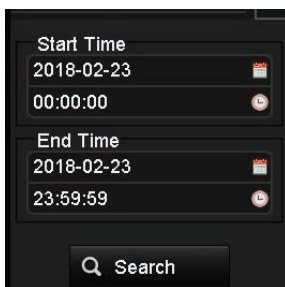


SECTION 7: RECORD, PLAYBACK AND VIDEO BACKUP

2. Open the drop-down list in the upper-left corner of the screen, then select **Event**.
3. Open the Type drop down list (in the upper right corner), then select the kind of event you want to search for. Here, Motion was selected.



4. On the right side of the screen, click the icons to select the **Start Time** and **End Time** within which the event occurred.



5. Click **Search**. A list of events (channel and time) that occurred during the time frame selected will appear on the right side of the screen.
6. Select an entry in the list (camera channel and the time), then click the **Play** icon to show the video associated with the event.



For the definition of icons in the playback toolbar, see “7.2.2 Playback by channel - menu and screen controls” on page 125.

7.2.5 Playback by Tag

Video tags provide a convenient way to identify video clips, then find and replay them later. Tags are associated with video clips during playback using the icons in the lower left corner of the screen.


1. Open the **Playback** interface. Go to **Menu | Playback**.
2. Open the drop-down list in the upper-left corner of the screen, then select **Tag**.





3. Select the camera channel for which the tag was created. If unsure, select all channels.
4. On the right side of the screen, click the icons to select the **Start Time** and **End Time** within which the tag was created. You can also search for the video clip by Keyword.


SECTION 7: RECORD, PLAYBACK AND VIDEO BACKUP



Keyword

Start Time
2018-02-21 

00:00:00 

End Time
2018-02-23 


23:59:59 

 Search 

5. Click **Search**. A list of tag names will appear.
6. Select the tag you want to play, and then click the **Play** icon to view the video.



Using File Management

7. Click the  icon to open the **Tag management** window, and then click the **Tag** tab. In the example below, three tags are shown.



8. In the **Tag management** window, click the **Edit** icon (see above) to edit the **Tag Name**, or click the **Delete** icon to delete it.

7.2.6 Playback by Sub-Periods

According to the configured 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 20:00, and the 4-screen display mode is selected, then it can play the video files for 1 hour on each screen simultaneously.

To use Sub-periods playback:

1. Open the **Playback** interface. Go to **Menu | Playback**.
2. Open the drop-down list in the upper-left corner of the screen, then select **Sub-periods**.



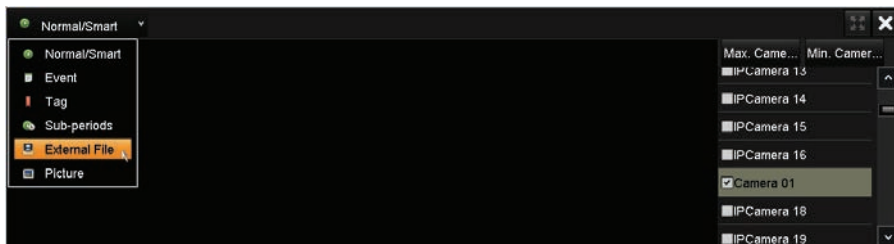
3. Select the camera channel for which you want to use this feature, and the date range.
4. Select the split-screen number from the list, and then click the **Play** icon. In the example below, 4 screens was selected.



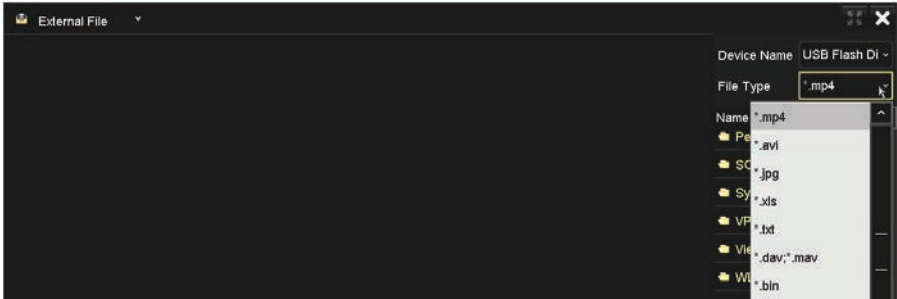
7.2.7 Playing Back an external file

You can playback a file on an external device, such as a video file saved on a backup disk or flash drive.

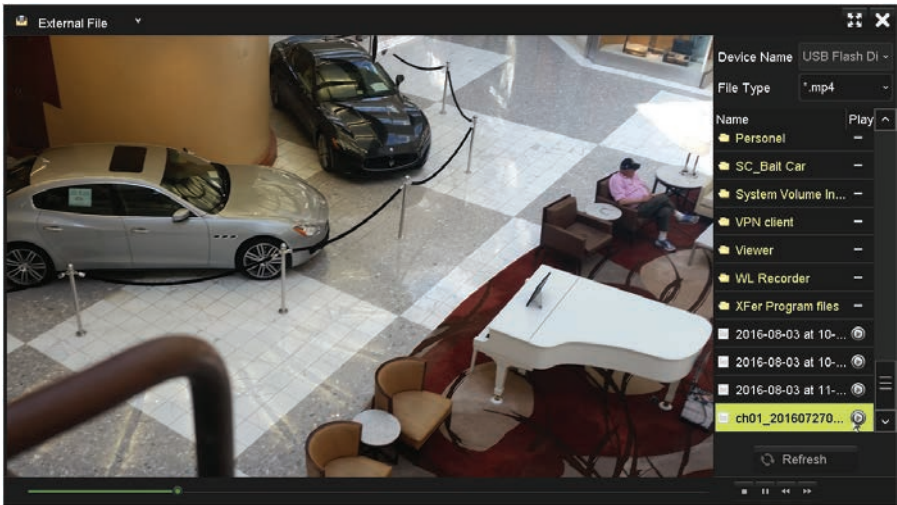
1. Open the **Playback** interface. Go to **Menu | Playback**.
2. Open the drop-down list in the upper-left corner of the screen, then select **External File**.



3. Attach the external storage device containing the file to one of the USB ports. If multiple storage devices are connected to USB ports, open the **Device** drop down list in the upper right corner and select the device containing the file. A USB Flash drive was plugged into one of the USB ports, and then selected here.
4. Open the **File Type** drop down list, and then select the type of file you want to play. Several options are available.



5. Peruse the list shown on the right side of the screen and select (highlight) the file you want to play. If the file is in a directory on the device, click the icon to the left of the directory name to show the contents of the directory.
6. Click the **Play** icon associated with the file you want to play.



7.2.8 Playback Pictures

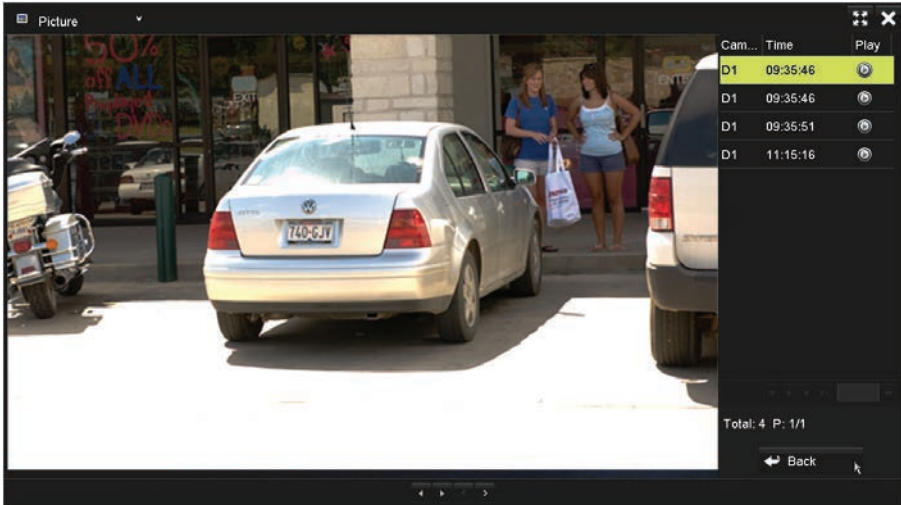
Captures made during playback can be searched, displayed, and exported.

1. Open the **Playback** interface. Go to **Menu | Playback**.
2. Open the drop-down list in the upper-left corner of the screen, then select **Pictures**.

SECTION 7: RECORD, PLAYBACK AND VIDEO BACKUP



3. Select the camera channel for which you want to use this feature, and the date range.
4. Click **Search**. A list of captures taken on the camera selected during the time range will be listed in the right frame.

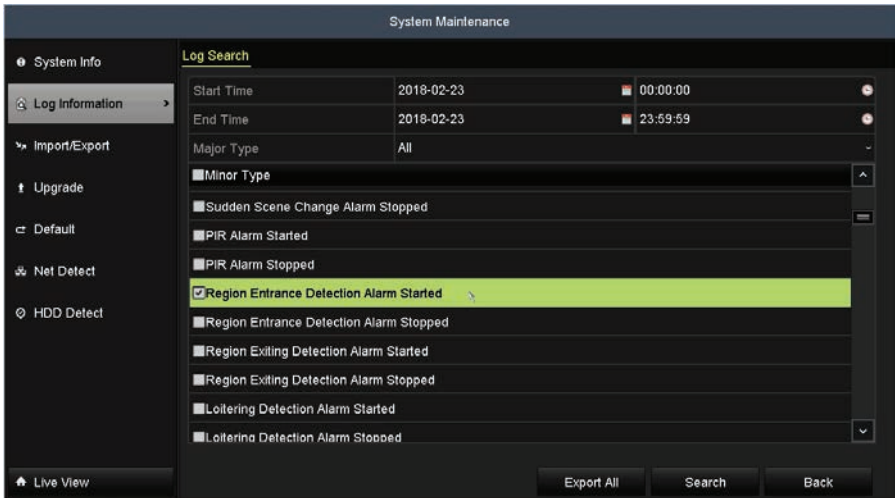


5. Click on the photo you want to display.

7.2.9 Playback using System logs

You can play back video file(s) associated with maintenance log entry.

1. Open the Log Information menu. Go to **Menu | Maintenance | Log Information**.



2. Select a **Start Time**, **End Time** to search, and then select the **Major Type** of log entry and then the **Minor Type** of log entry.
3. Click **Search**. In the example below, the search criterion specified are "All" (Major Type) entries.

The screenshot shows the 'Search Result' table with the following data:

No.	Major Type	Time	Minor Type	Parameter	Play	Details
1	Alarm	2018-02-23 09:15:55	Line Crossing Detecti...	N/A	⏮	✓
2	Alarm	2018-02-23 09:16:51	Line Crossing Detecti...	N/A	⏮	✓
3	Alarm	2018-02-23 09:18:05	Line Crossing Detecti...	N/A	⏮	✓
4	Alarm	2018-02-23 09:19:51	Line Crossing Detecti...	N/A	⏮	✓
5	Alarm	2018-02-23 09:20:51	Line Crossing Detecti...	N/A	⏮	✓
6	Alarm	2018-02-23 09:21:24	Line Crossing Detecti...	N/A	⏮	✓
7	Alarm	2018-02-23 09:30:36	Line Crossing Detecti...	N/A	⏮	✓
8	Alarm	2018-02-23 09:31:46	Line Crossing Detecti...	N/A	⏮	✓
9	Alarm	2018-02-23 09:35:14	Line Crossing Detecti...	N/A	⏮	✓
10	Alarm	2018-02-23 09:35:29	Line Crossing Detecti...	N/A	⏮	✓

Total: 255 P: 1/3

4. Find the entry in the search results list that is associated with a Play icon. See the example above.
5. Click the **Play** icon to watch the video associated with the event.



7.2.10 Auxiliary Functions - Playback frame by frame

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

Using a Mouse

Go to **Menu | Playback**.

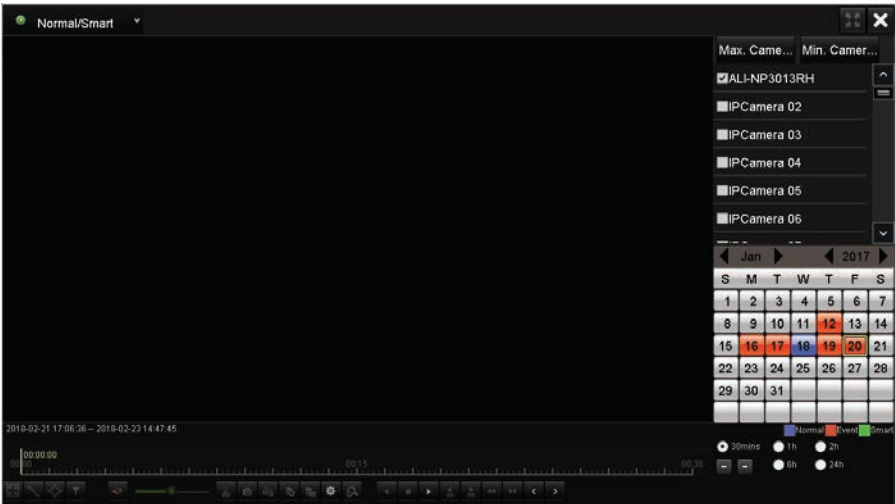
Playback a file. During playback, click the button ◀◀ until the speed changes to **Single**. One click on the playback screen advances playback to the next frame forward. Click ▶▶ to increase the playback speed in forward.

During reverse playback click the button ◀◀ until the speed changes to **Single**. One click on the playback screen advances playback to the next frame in reverse. Click ▶▶ to increase the playback speed in reverse.

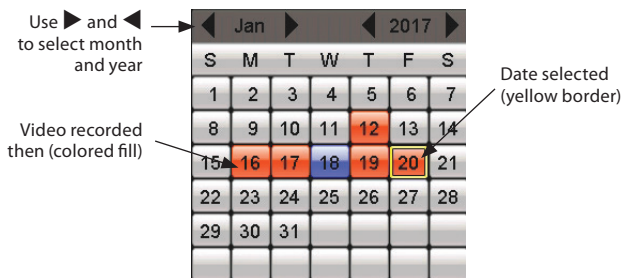
7.2.11 Auxiliary Functions - Reverse Playback Multi-channel

You can play back record files of multi-channel reversely. Multi-channel playback supports 4 channels at up to 8 MP resolution and 16 channels at up to 1080p resolution.

1. Open the Playback interface. Go to **Menu | Playback**.



- In the calendar section, click the day when the video clip you want to play was recorded. In the example shown below, January 20, 2017 was selected. Notice that colored marks in the timeline at the bottom of the screen appeared. These marks indicate when and what type of recordings were made for that camera(s) selected.



- Select the video channels you want to playback.
- To start playback, click the **Play** button (►) in the playback controls panel at the bottom of the screen. These clips also be played in reverse.



For the definition of icons in the playback toolbar, see “7.2.2 Playback by channel - menu and screen controls” on page 125.

7.2.12 Digital Zoom

1. Click the magnifier button on the playback control bar to enter Digital Zoom screen. The video will expand to full screen, and a faint slider bar with ⊕ (zoom in) and ⊖ (zoom out) icons will appear in the upper left corner of the video image. To use this feature, do one of the following:
 - Click on the spot in the video image, and then use the mouse scroll wheel to zoom in or out at that spot.
 - Click the ⊕ icon to zoom in on the video image, and then drag the image the video image with the mouse to zoom on another spot. Click ⊖ to zoom out.
 - Drag the slider on the slider bar up or down to zoom in or out, and then drag the video image with the mouse to zoom on another spot.
 - Right-click the mouse to cancel the zoom feature.

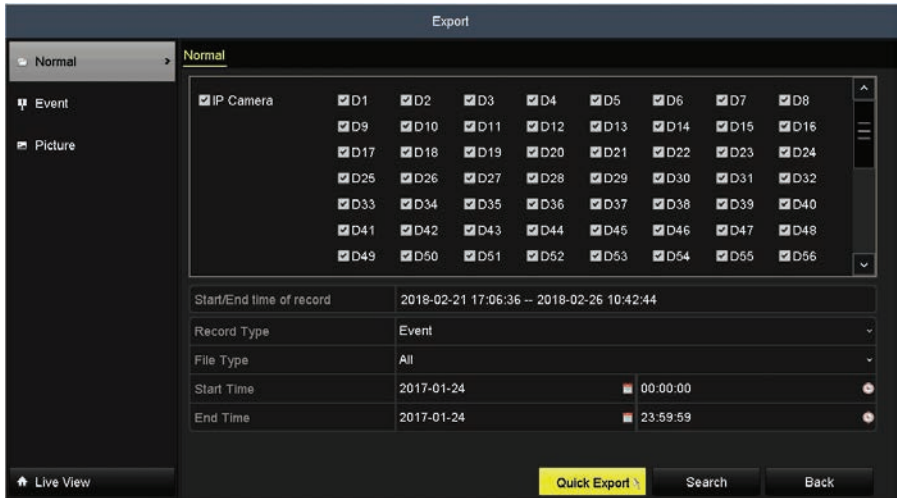
7.3 Backing up Record Files - Export

7.3.1 Quick Export

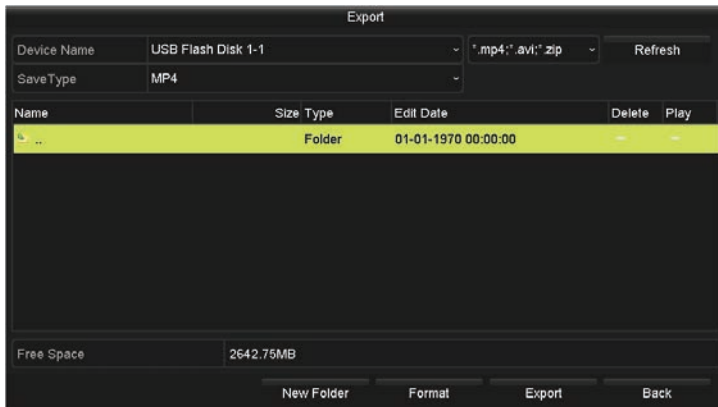
The Quick Export feature allows you to easily export (backup to an external device) video clips recorded over a 24 hours period from up to four selected camera channels.

1. Attach an USB storage device, such as a USB flash drive or USB disk drive, to the NVR USB port.

- Open the Export menu. Go to: **Menu | Export | Normal**.

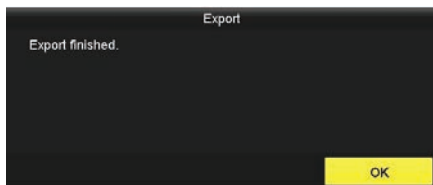


- Check the boxes for the camera channels you want to back up.
- Select the **Start Time** and **End Time** of the period when the video clips of interest were recorded. To change the time, click on the field, then select the target date or time from the pop-up menu. The time span cannot exceed 24 hours.
- Click the **Quick Export** button. A pop-up window will open showing the file structure of your external storage device. If your USB device is not shown in the **Device Name** field, click the **Refresh** button.



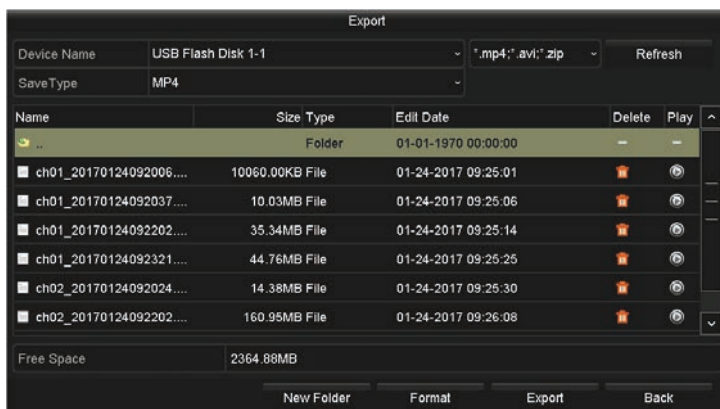
SECTION 7: RECORD, PLAYBACK AND VIDEO BACKUP

- If the device you are exporting to is a re-writable device such as a USB flash drive, select the directory where you want to copy the files, or create a **New Folder**. **NOTE:** Some USB devices types do not include the **New Folder** and **Format** options, but may include an **Erase** option.
- Click the **Export** button to start the **Export**. The Export window will list the files that were transferred. Allow the operation to finish before continuing.



- Check the Export result by playing a file that was exported. In the Export window, click the file you want to play, then click the associated icon in the Play column.

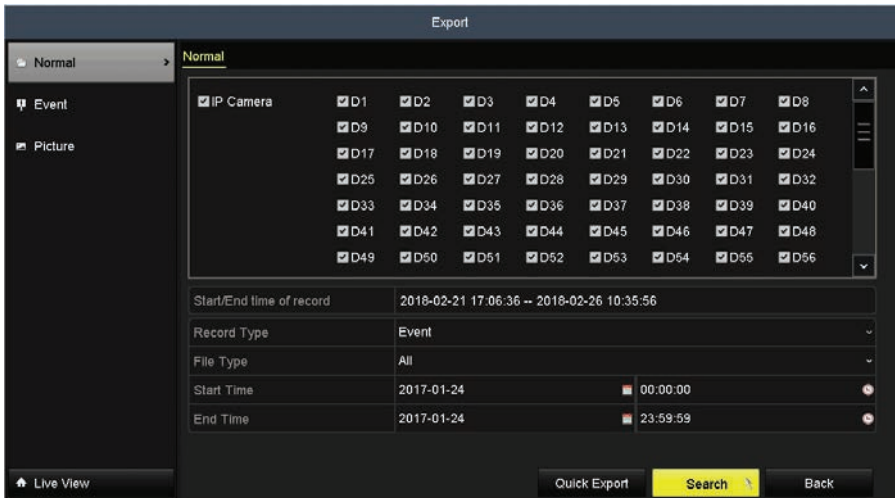
Note: When the *.mp4* video file is exported, *player.zip* is also exported.



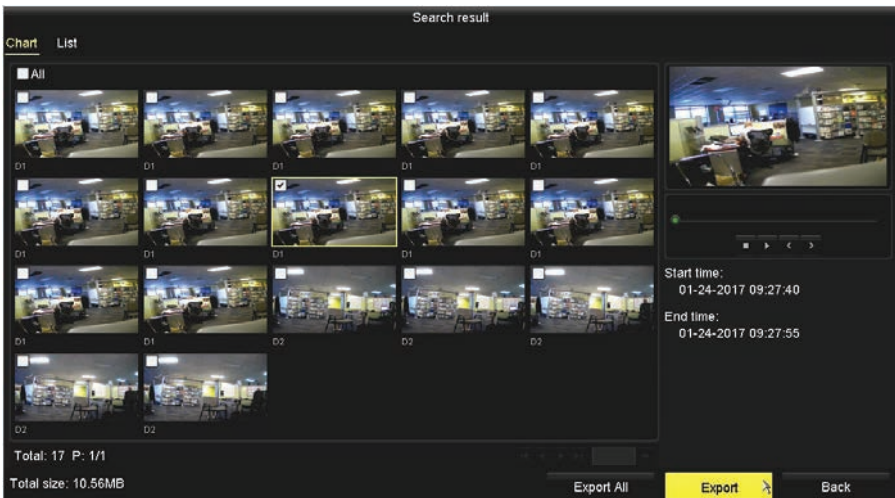
7.3.2 Export by video search

The Export by video search feature allows you to export specific video clips. The export operation writes the selected file(s) to an USB device.

- Attach an USB storage device, such as a USB flash drive or USB disk drive, to the NVR USB port.
- Open the Export menu. Go to: **Menu | Export | Normal**.



3. Check the boxes for the camera channels you want to back up.
4. Open the **Record Type** and **File Type** drop-down lists, and select the best options for your search.
5. Select the **Start Time** and **End Time** of the period when the video clips of interest were recorded. To change the time, click on the field, then select the target date or time from the pop-up menu.
6. Click **Search** to list the video clips recorded during the selected time span. In the **Search Result** list, you can play the video clip by clicking the icon in the Play column associated with the file.



SECTION 7: RECORD, PLAYBACK AND VIDEO BACKUP

- Select the video clips you want to export by checking the box associated with the video thumbnail. You can also check the box for a video thumbnail, and then play the clip in the window in the upper right corner. Click **List** to view the search results in a format that shows the start /end time of the clip, and the size.

The screenshot shows the 'Search result' window with a table of video clips. The table has columns for Camera No., Start/End Time, Size, Play, and Lock. One clip is selected with a checkmark. To the right is a video player showing a scene from a store.

Camera No.	Start/End Time	Size	Play	Lock
D1	01-24-2017 09:20:06--09:20:...	10053.41KB	⏮	🔒
D1	01-24-2017 09:20:37--09:20:...	10.02MB	⏮	🔒
D1	01-24-2017 09:22:02--09:23:...	35.33MB	⏮	🔒
D1	01-24-2017 09:23:21--09:24:...	44.75MB	⏮	🔒
D1	01-24-2017 09:24:58--09:25:...	12.07MB	⏮	🔒
D1	01-24-2017 09:25:20--09:25:...	16.51MB	⏮	🔒
D1	01-24-2017 09:26:52--09:27:...	19.38MB	⏮	🔒
<input checked="" type="checkbox"/> D1	01-24-2017 09:27:40--09:27:...	10.56MB	⏮	🔒
D1	01-24-2017 09:28:02--09:28:...	11.16MB	⏮	🔒
D1	01-24-2017 09:28:31--09:28:...	12.75MB	⏮	🔒
D1	01-24-2017 09:28:59--09:29:...	24.19MB	⏮	🔒
D1	01-24-2017 09:30:04--09:30:...	14.89MB	⏮	🔒

Total: 17 P: 1/1
Total size: 10.56MB

Buttons: Export All, Export, Back

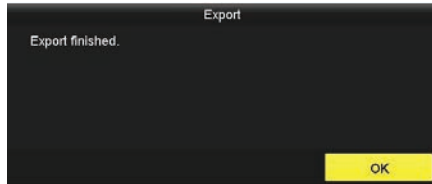
- Select the video clips you want to export by checking the box associated with an entry in the list. You can also play a clip in the window in the upper right corner by clicking the icon associated with the clip in the play column. **NOTE:** You can click the Lock icon to lock a video clip. Locking a video clip prevents it from being erased when the HDD becomes full.
- Check the select box(es) associated with other video clip(s) you want to export, and then click the **Export** button at the bottom of the window. A pop-up window will open showing the file structure of your external storage device. If your USB device is not shown in the **Device Name** field, click the **Refresh** button. **NOTE:** Some USB devices types include the **New Folder** and **Format** options, other types include only an **Erase** option.

The screenshot shows the 'Export' dialog box. It has fields for Device Name (USB Flash Disk 1-1), Save Type (MP4), and a file type dropdown (*.mp4;*.avi;*.zip). Below is a table of files and folders on the device.

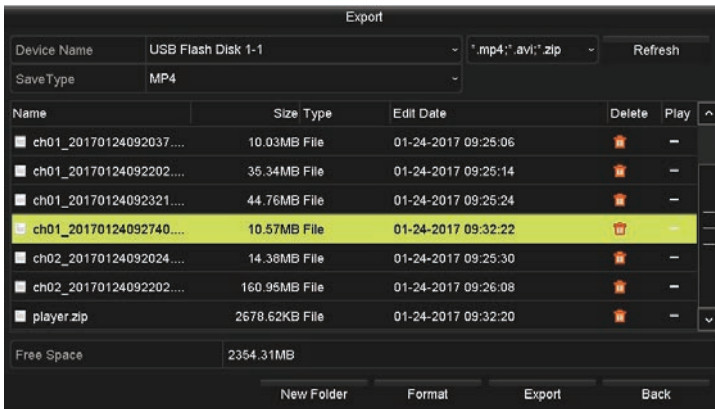
Name	Size	Type	Edit Date	Delete	Play
..		Folder	01-01-1970 00:00:00	—	—
ch01_20170124092006....	10060.00KB	File	01-24-2017 09:25:00	🗑	—
ch01_20170124092037....	10.03MB	File	01-24-2017 09:25:06	🗑	—
ch01_20170124092202....	35.34MB	File	01-24-2017 09:25:14	🗑	—
ch01_20170124092321....	44.76MB	File	01-24-2017 09:25:24	🗑	—
ch02_20170124092024....	14.38MB	File	01-24-2017 09:25:30	🗑	—
ch02_20170124092202....	160.95MB	File	01-24-2017 09:26:08	🗑	—
Free Space	2364.88MB				

Buttons: New Folder, Format, Export, Back

- Click the **Export** button to start the **Export**. The Export window will list the files that were transferred. Allow the process to finish before continuing.



- Check the Export result by playing a file that was exported. In the Export window, click the file you want to play, then click the associated icon in the Play column.



Note: The Player utility *player.zip* will be exported automatically during video clip export.

7.3.3 Export by Event Search

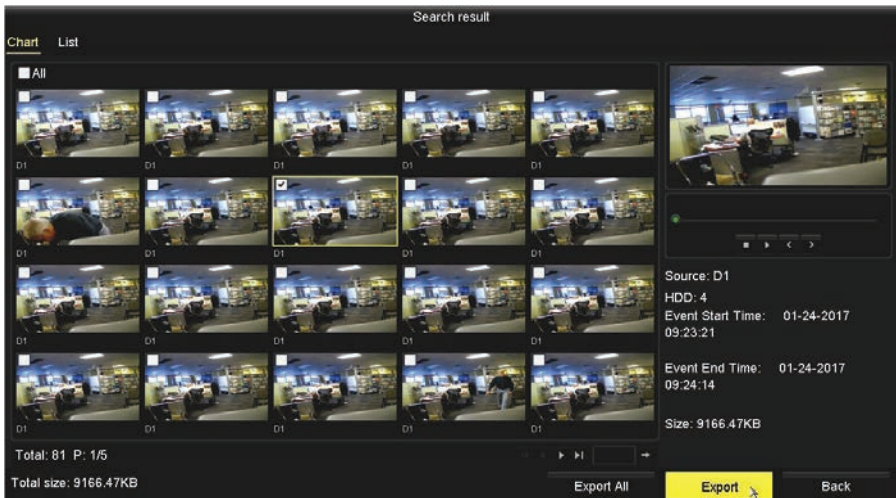
Video recordings triggered by Events, such as motion detection, can be searched for and exported to a USB storage device such as a USB flash drive or USB disk drive, or USB optical drive.

- Attach an USB storage device, such as a USB flash drive or USB disk drive, to the NVR USB port.
- Open the Export menu. Go to: **Menu | Export | Event**.

SECTION 7: RECORD, PLAYBACK AND VIDEO BACKUP



- On the Major Type line, select open the drop down list and select, for example, **Motion**. You can also select either **Alarm Input** or **VCA** to search for those kinds of events.
- Select the **Start Time** and **End Time** of the period when the video clips of interest were recorded. To change the time, click on the field, then select the target date or time from the pop-up menu.
- Check the box(es) of the camera(s) you want to apply the search for.
- Click **Search**. Thumbnails of the search results will be shown. Note that multiple pages of thumbnails may be included.



7. Select the video clips you want to export by checking the box associated with the video thumbnail. You can also check the box for a video thumbnail, and then play the clip in the window in the upper right corner. Click **List** to view the search results in a format that shows the start /end time of the clip and the size. **NOTE:** You can click the Lock icon to lock a video clip. Locking a video clip prevents it from being erased when the HDD becomes full.

Search result

Source	Camera No.	HDD	Event Time	Size	Play
<input type="checkbox"/> D1	D1	4	01-24-2017 09:20:06--09:20:...	10053.41KB	
<input type="checkbox"/> D1	D1	4	01-24-2017 09:20:06--09:20:...	10.02MB	
<input type="checkbox"/> D1	D1	4	01-24-2017 09:20:36--09:20:...	10053.41KB	
<input type="checkbox"/> D1	D1	4	01-24-2017 09:20:36--09:20:...	10.02MB	
<input type="checkbox"/> D1	D1	4	01-24-2017 09:22:02--09:22:...	35.33MB	
<input type="checkbox"/> D1	D1	4	01-24-2017 09:22:43--09:23:...	27.05MB	
<input type="checkbox"/> D1	D1	4	01-24-2017 09:22:43--09:23:...	10.18MB	
<input checked="" type="checkbox"/> D1	D1	4	01-24-2017 09:23:21--09:24:...	9166.47KB	
<input type="checkbox"/> D1	D1	4	01-24-2017 09:23:21--09:24:...	43.82MB	
<input type="checkbox"/> D1	D1	4	01-24-2017 09:24:18--09:24:...	28.71MB	
<input type="checkbox"/> D1	D1	4	01-24-2017 09:24:18--09:24:...	9873.36KB	
<input type="checkbox"/> D1	D1	4	01-24-2017 09:24:58--09:25:...	9191.36KB	

Total: 81 P: 1/1
Total size: 9166.47KB

Export All Export Back

8. Select the video clips you want to export by checking the box associated with an entry in the list. You can also play a clip in the window in the upper right corner by clicking the icon associated with the clip in the play column.
9. Check the select box(es) associated with the video clip(s) you want to export, and then click the **Export** button at the bottom of the window. A pop-up window will open showing the file structure of your external storage device. If your USB device is not shown in the **Device Name** field, click the **Refresh** button. **NOTE:** Some USB devices types include the **New Folder** and **Format** options, other types include only an **Erase** option.

Export

Device Name: USB Flash Disk 1-1 | File Type: *.mp4;*.avi;.zip | Refresh

Save Type: MP4

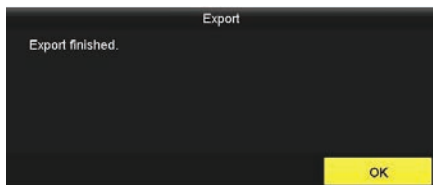
Name	Size	Type	Edit Date	Delete	Play
..		Folder	01-01-1970 00:00:00	—	—
ch01_20170124092006....	10060.00KB	File	01-24-2017 09:25:00		—
ch01_20170124092037....	10.03MB	File	01-24-2017 09:25:06		—
ch01_20170124092202....	35.34MB	File	01-24-2017 09:25:14		—
ch01_20170124092321....	44.76MB	File	01-24-2017 09:25:24		—
ch01_20170124092740....	10.57MB	File	01-24-2017 09:32:22		—
ch02_20170124092024....	14.38MB	File	01-24-2017 09:25:30		—

Free Space: 2354.31MB

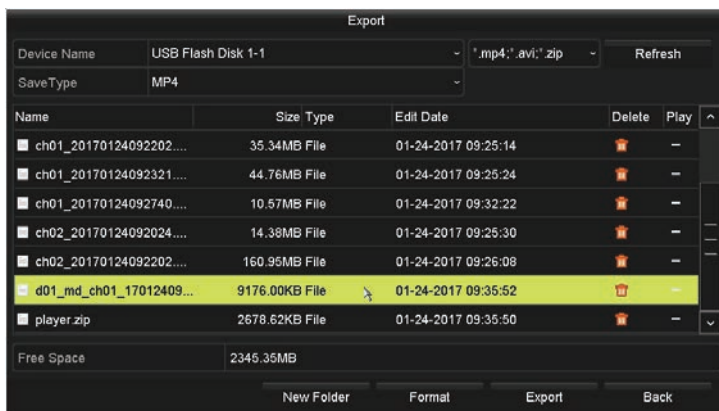
New Folder Format Export Back

SECTION 7: RECORD, PLAYBACK AND VIDEO BACKUP

10. Click the **Export** button to start the **Export**. The Export window will list the files that were transferred. Allow the process to finish before continuing.



11. Check the Export result by playing a file that was exported. In the Export window, click the file you want to play, then click the associated icon in the Play column.

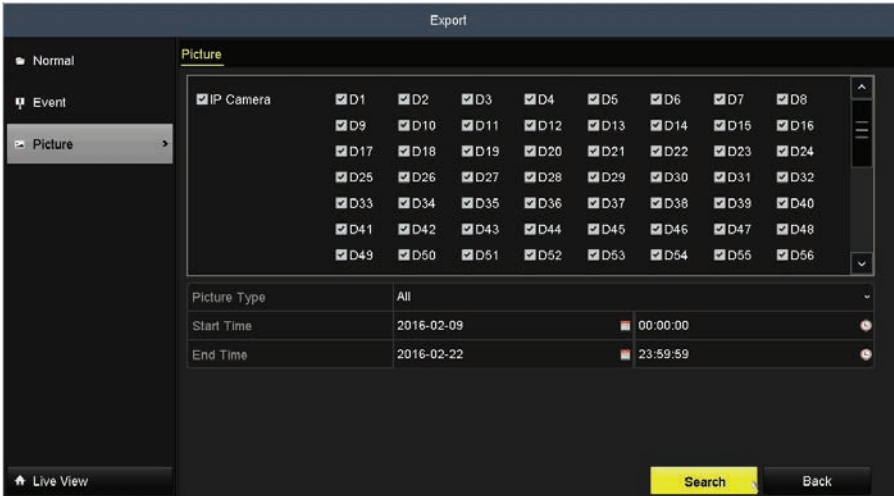


Note: The Player utility *player.zip* is exported automatically during video clip export.

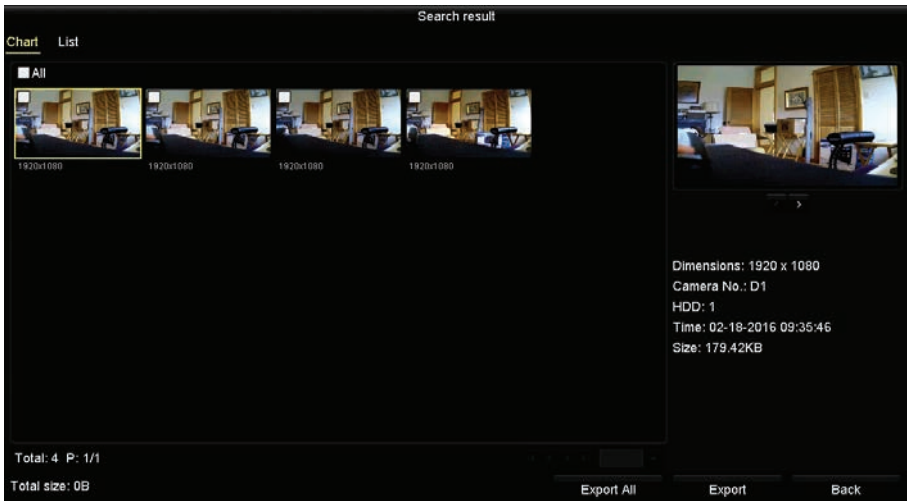
7.3.4 Export by Picture Search

Pictures (captures) created during live view, playback, or through a capture schedule can be searched for and exported to a USB storage device such as a USB flash drive or USB disk drive, or USB optical drive.

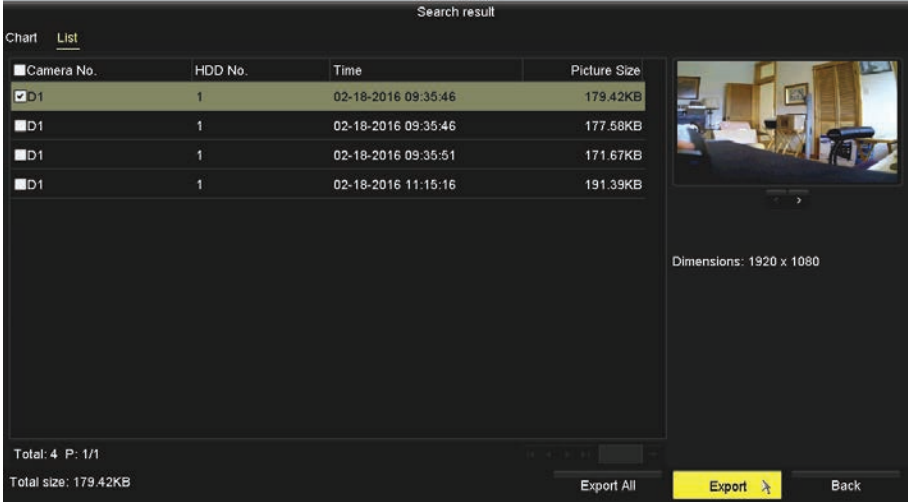
1. Attach an USB storage device, such as a USB flash drive or USB disk drive, to the NVR USB port.
2. Open the Export menu. Go to: **Menu | Export | Picture**.



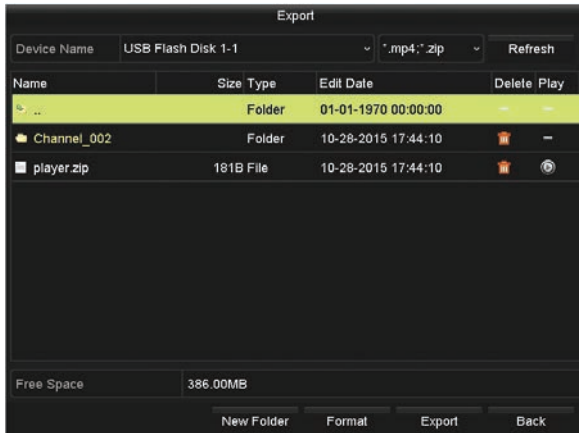
- On the **Picture** line, open the drop down list and select, for example, **Motion**. You can also select either **Event**, **Capture**, **Command Triggered**, etc. to search for those kinds of events.
- Select the **Start Time** and **End Time** of the period when the photos of interest were captured. To change the time, click on the field, then select the target date or time from the pop-up menu.
- Check the box(es) of the camera(s) you want to apply the search for.
- Click **Search**. Thumbnails of the search results will be shown. Note that multiple pages of thumbnails may be included.



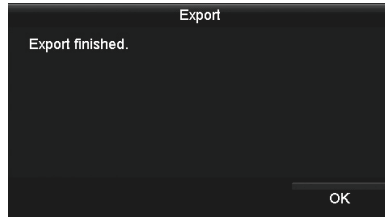
- Select the capture file you want to export by checking the box associated with the thumbnail. You can also check the box for a thumbnail, and then see the photo in the window in the upper right corner. Click **List** to view the search results in a format that shows the time the photo was captured and the size.



- Select the capture file you want to export by checking the box associated with an entry in the list. You can also see the photo in the window in the upper right corner by clicking on the file.
- Check the select box(es) associated with the file(s) you want to export, and then click the Export button at the bottom of the window. A pop-up window will open showing the file structure of your external storage device. If your USB device is not shown in the **Device Name** field, click the **Refresh** button. **NOTE:** Some USB devices types include the **New Folder** and **Format** options, other types include only an **Erase** option.



- Click the **Export** button to start the **Export**. The Export window will list the files that were transferred. Allow the process to finish before continuing.



- Check the Export result by playing a file that was exported. In the Export window, click the file you want to play.

7.3.5 Exporting Video Clips during playback

Segments of video recordings can be backed up (exported) during playback. These files exported to a USB storage device such as a USB flash drive or USB disk drive, or USB optical drive.

- Attach an USB storage device, such as a USB flash drive or USB disk drive or USB optical drive, to the NVR USB port.
- Playback a video file.
- Advance the file playback to the start of the segment you want to export, then click the **Clip** icon (scissors) at the bottom of the screen to mark the start of the clip you want to save.

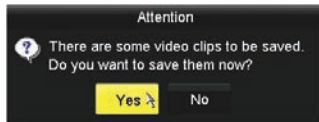


SECTION 7: RECORD, PLAYBACK AND VIDEO BACKUP

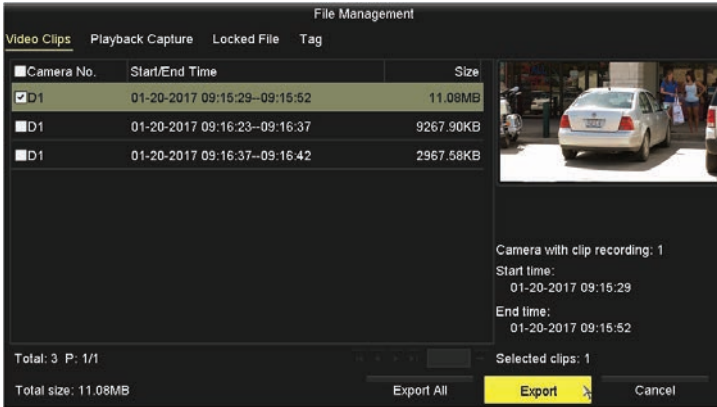
- Advance the file playback to the end of the segment you want to export, then click the **Clip** icon (scissors) at the bottom of the screen to mark the end of the clip you want to save.



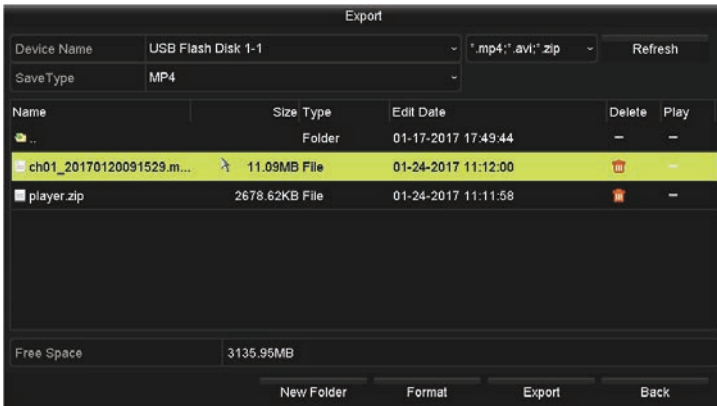
- Right click anywhere in the video window. The Attention pop-up window shown below will appear. (You can also click the File Management icon to export the video clip.)



- Click **Yes** to save the video clip you marked.
- In the File Management window, check the box(es) for the video clip(s) you want to export, and then click the **Export** button.



- In the **Export** window, select the directory where you want to save the file. If your USB device is not shown in the **Device Name** field, click the **Refresh** button. **NOTE:** Some USB devices types include the **New Folder** and **Format** options, other types include only an **Erase** option.



- Click **Export** to save the video clip(s) to the location you chose.
- Click the **Export** button to start the **Export**. Allow the operation to finish before continuing. Click **OK** in the confirmation window to return to the **Menu** window.

SECTION 8

Managing User Accounts

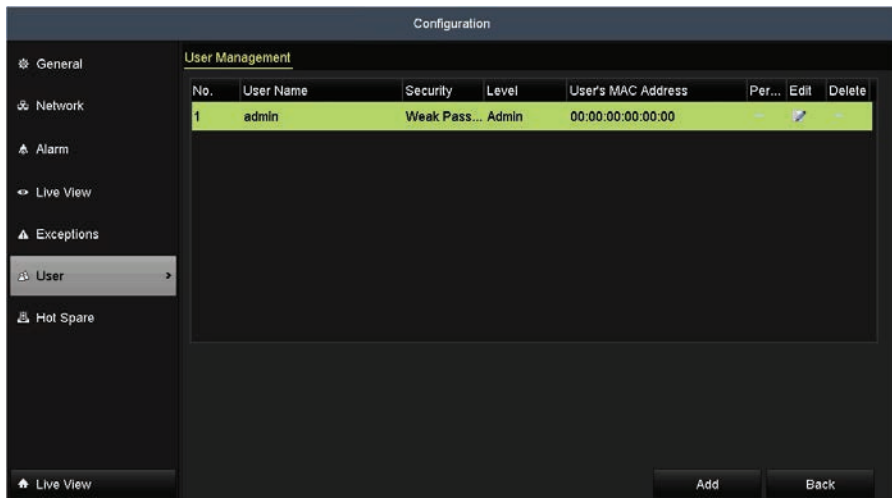
User accounts are created to control access to the system both at the NVR and when logging into the NVR from a remote computer. Each account has a User Name, Password, and a selection of permissions granted to the user.

By default, one user, named *admin*, is provided. The *admin* user is granted all permissions with the system, and can create, modify, and delete other users.

The NVR supports up to 32 user accounts.

8.1 Adding a user account

1. Enter the User Management interface. Go to **Menu | Configuration | User**.



2. Click **Add** to open the Add User menu.

Add User	
User Name	
Admin Password	
Password	
Confirm	
Level	Guest
User's MAC Address	00 :00 :00 :00 :00 :00

Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.

OK Cancel

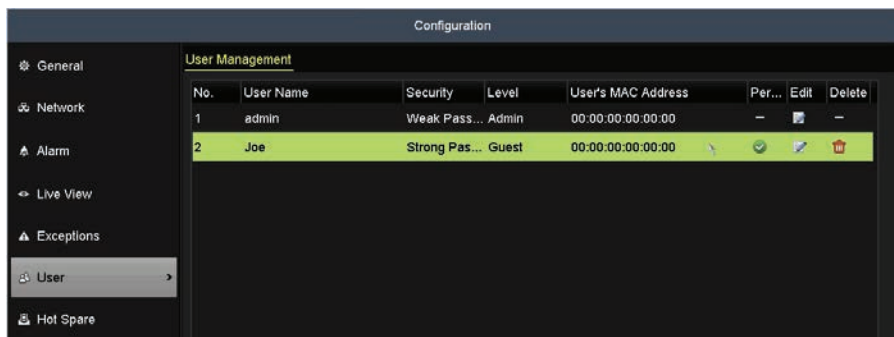
3. Enter the information for new user, including User Name, Admin Password, Password and Confirm password, Level and User's MAC Address (optional).
 - Set the user **Level** to Operator or Guest. Different **Levels** have different operating permission.
 - * **Operator**: The Operator user level has permission of Two-way Audio in Remote Configuration and all operating permission in Camera Configuration by default.
 - * **Guest**: The Guest user has no permission of Two-way Audio in Remote Configuration and only has the local/remote playback in the Camera Configuration by default.
 - **User's MAC Address**: The MAC address of the remote PC which logs onto the NVR. If this option is configured and enabled, a remote user with this MAC address only can access the NVR.

Add User	
User Name	Joe
Admin Password	*****
Password	***** Strong
Confirm	*****
Level	Guest
User's MAC Address	00 :00 :00 :00 :00 :00

Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.

OK Cancel

4. Click the **OK** to save the settings and go back to the User Management interface. The added new user will be displayed on the list. See the screen shown below.



- Select the user from the list and then click the button to enter the Permission settings (**Per** icon) interface. In the example above, user “**Joe**” was selected.

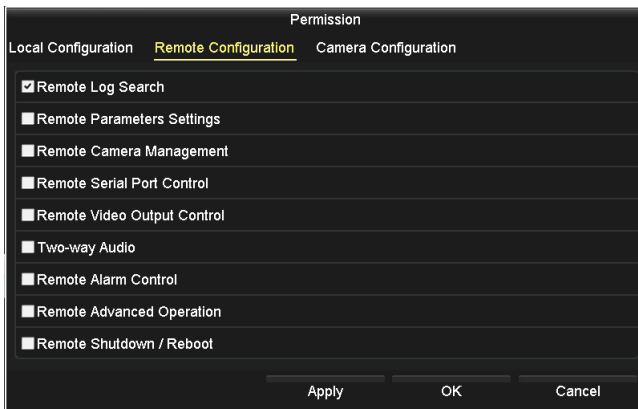


- Set the operating permission of Local Configuration, Remote Configuration and Camera Configuration for the user.

Local Configuration options:

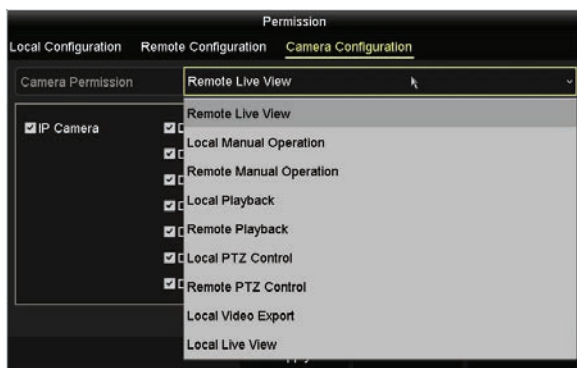
- **Local Log Search:** Searching and viewing logs and system information of NVR.
- **Local Parameters Settings:** Configuring parameters, restoring factory default parameters and importing/exporting configuration files.
- **Local Camera Management:** Use for adding, deleting and editing of IP cameras.
- **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 options



- **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:** Reserved for future expansion.
- **Remote Video Output Control:** Sending remote button control signal.
- **Two-Way Audio:** Enable two-way audio between the remote client and the NVR.
- **Remote Alarm Control:** Remotely arming (notify alarm and exception message to the remote client) and controlling the alarm output.
- **Remote Advanced Operation:** Remotely operating HDD management (initializing HDD, setting HDD property), upgrading system firmware, clearing I/O alarm output.
- **Remote Shutdown/Reboot:** Remotely shutting down or rebooting the NVR.

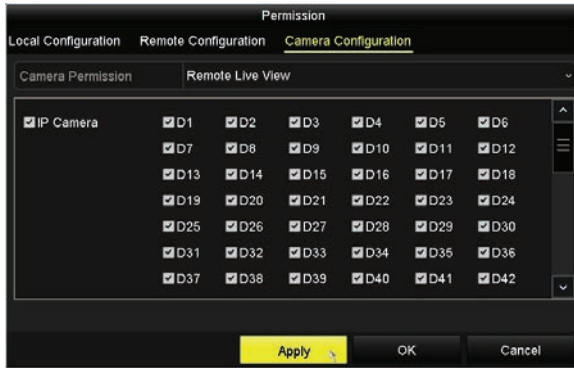
Camera Configuration



- **Remote Live View:** Remotely viewing live video of the selected camera(s).
 - **Local Manual Operation:** Locally starting/stopping manual recording, picture capturing and alarm output of the selected camera(s).
 - **Remote Manual Operation:** Remotely starting/stopping manual recording, picture capturing and alarm output of the selected camera(s).
 - **Local Playback:** Locally playing back recorded files of the selected camera(s).
 - **Remote Playback:** Remotely playing back recorded files of the selected camera(s).
 - **Local PTZ Control:** Locally controlling PTZ movement of the selected camera(s).
 - **Remote PTZ Control:** Remotely controlling PTZ movement of the selected camera(s).
 - **Local Video Export:** Locally exporting recorded files of the selected camera(s).
7. Click **OK** to save your settings and exit the **User** menu.

NOTE Only the *admin* user account has permission to restore the NVR to factory default settings.

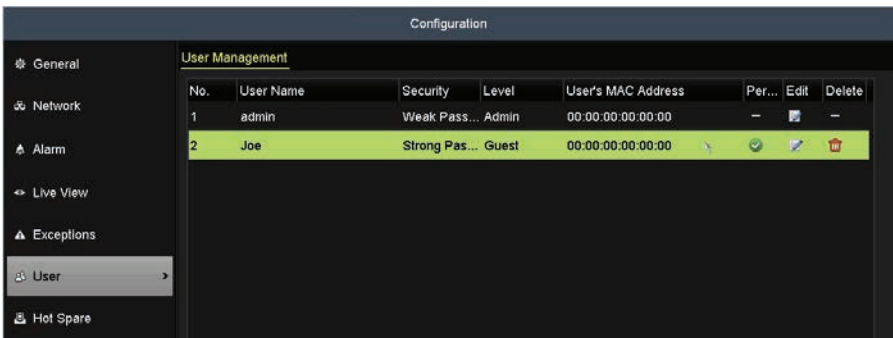
8. Select the IP Camera(s) the user will have access to.



- Click **Apply** to save your settings, then click **OK** to return to the **User** menu.

8.2 Deleting a user account

- Enter the User Management interface. Go to **Menu | Configuration | User**.
- Click the entry for the user to be deleted from the list. When the item is selected, it is highlighted.



- Click the **Delete** (trash can) icon to delete the selected user.

8.3 Editing a user account

- Enter the User Management interface. Go to **Menu | Configuration | User**.
- Select the user to be edited from the list (see the **User Management** window above).

- Click the **Edit** icon to open the Edit User interface. **Note:** The user name **admin** can also be changed.

Add User	
User Name	Joe
Admin Password	*****
Password	***** Strong
Confirm	*****
Level	Guest
User's MAC Address	Guest
	Operator

Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.

- In the Level drop-down list, select either **Operator** and **Guest**. You can edit the user information, including user name, password, permission level and MAC address. To change the password, check the **Change Password** box, then enter the new password in the Password and Confirm fields.
- Click **OK** to save the settings and exit the menu.

8.3.1 Edit admin user

Observint highly recommends that the password for the **admin** user be changed to improve system security. To change the **admin** user password, follow the steps in “8.3 Editing a user account” on page 161. The **admin** username cannot be changed.

Edit User	
User Name	admin
Old Password	*****
Change Password	<input checked="" type="checkbox"/>
Password	***** Strong
Confirm	*****
Export GUID	*
User's MAC Address	00 :00 :00 :00 :00 :00

Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.

After changing the **admin** password, reopen the **Edit User** window for **admin**, and then click **Export GUID** icon. Follow the on-screen instructions to create and save a new GUID file. This file is useful when logging into the as **admin** when you forget the password.

SECTION 9

Network Settings

9.1 Configuring General Settings

Network settings must be properly configured before you connect the NVR to cameras on network, or access it remotely.

1. Open the Network Settings menu. Go to **Menu | Configuration | Network**.
2. Click the **General** tab.

The screenshot shows the 'Configuration' window with the 'General' tab selected. The left sidebar contains menu items: General, Network, Alarm, Live View, Exceptions, User, Hot Spare, and Live View. The main area displays the following settings:

Configuration	
General	PPPOE DDNS NTP Email SNMP NAT More Settings
Working Mode	Net Fault-tolerance
Select NIC	bond0
NIC Type	10M/100M/1000M Self-adaptive
Enable DHCP	<input checked="" type="checkbox"/>
IPv4 Address	IPv6 Address 1 fe80::1a68:cbff:fe86:ce5e/64
IPv4 Subnet ...	IPv6 Address 2
IPv4 Default G...	IPv6 Default G...
MAC Address	18:68:cb:86:ce:5e
MTU(Bytes)	1500
Preferred DNS Server	
Alternate DNS Server	
Main NIC	LAN1

At the bottom right, there are 'Apply' and 'Back' buttons.

3. In the General Settings menu, select or enter the following parameters: NIC Type, IPv4 Address, IPv4 Gateway, MTU (valid range is value range of MTU is 500 ~ 9676) and DNS Server IP addresses. If the DHCP server is available, check the Enable DHCP box to automatically obtain an IP address and other network settings from the network DNS server.
4. Click **Apply** to save your settings.

Configuration

General PPPOE DDNS NTP Email SNMP NAT More Settings

Working Mode Net Fault-tolerance

Select NIC bond0

NIC Type 10M/100M/1000M Self-adaptive

Enable DHCP

IPv4 Address 192.168.0.30 IPv6 Address 1 fe80::1a68:cbff:fe86:ce5e/64

IPv4 Subnet ... 255.255.255.0 IPv6 Address 2

IPv4 Default G... . . . IPv6 Default G...

MAC Address 18:68:cb:86:ce:5e

MTU(Bytes) 1500

Preferred DNS Server

Alternate DNS Server

Main NIC LAN1

Apply Back

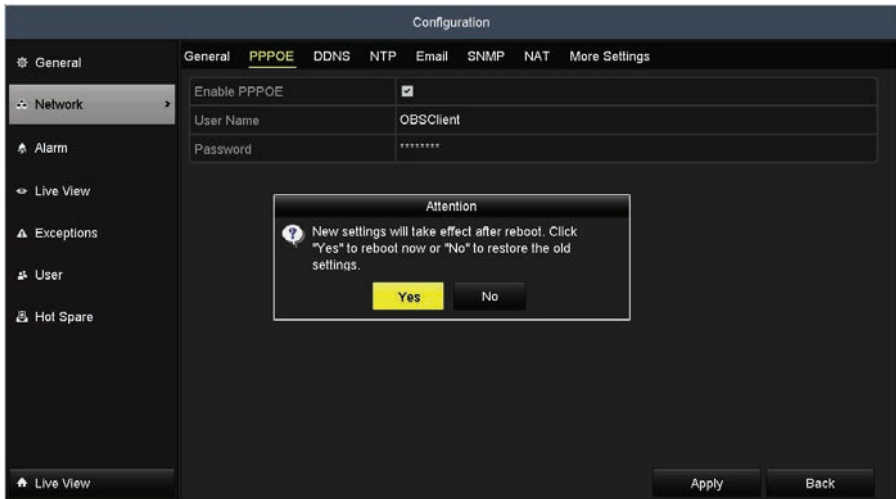
- Click **Apply** to save your settings.

9.2 Configuring Advanced Settings

9.2.1 Configuring PPPoE

Use the following screen to configure your PPPoE (Point-to-Point Protocol over Ethernet) connection.

- Open the PPPoEs menu. Go to **Menu | Configuration | Network**.
 - Click the PPPoE tab.



- b. Click the **Enable PPPOE** box to check it.
 - c. Enter a **User Name** and **Password** in the appropriate fields.
 - d. Click **Apply**.
 - e. In the Attention box, click **Yes** to reboot the NVR.
2. Allow the NVR to reboot before continuing.

9.2.2 Configuring DDNS

If your NVR is set to use PPPoE as its default network connection, you may set Dynamic DNS (DDNS) to be used for network access. Registration with your ISP is required before configuring the system to use DDNS.

1. Open the Network Settings menu. Go to **Menu | Configuration | Network**.
2. Click the **DDNS** tab to open the DDNS Settings menu.

Configuration							
General	PPPOE	DDNS	NTP	Email	SNMP	NAT	More Settings
Enable DDNS		<input checked="" type="checkbox"/>					
DDNS Type		DynDNS					
Area/Country		DynDNS					
Server Address		PeanutHull					
Device Domain Name		NO-IP					
Status							
User Name							
Password							

3. Check the **Enable DDNS** box to enable this feature.
4. Open the **DDNS Type** drop down list and select either DynDNS or NO-IP.

— **DynDNS:**

Configuration							
General	PPPOE	DDNS	NTP	Email	SNMP	NAT	More Settings
Enable DDNS		<input checked="" type="checkbox"/>					
DDNS Type		DynDNS					
Area/Country		Custom					
Server Address							
Device Domain Name							
Status							
User Name							
Password							

- i. Enter Server Address for DynDNS (i.e. members.dyndns.org).
 - ii. In the NVR Domain Name text field, enter the domain obtained from the DynDNS website.
 - iii. Enter the User Name and Password registered in the DynDNS website.
- **NO-IP:** Enter the account information in the corresponding fields.
- i. In a browser window, go to the URL: **http://alibiddns.com**
 - ii. In this website, create a **Domain Name**, **User Name** and **Password** for the recorder. Record these for use later.

- iii. In the recorder DDNS menu, open the **DDNS Type** drop-down list and select **NO-IP**.

The screenshot shows the 'Configuration' window with the 'DDNS' tab selected. The 'Network' menu item is highlighted in the left sidebar. The DDNS settings are as follows:

Field	Value
Enable DDNS	<input checked="" type="checkbox"/>
DDNS Type	NO-IP
Area/Country	Custom
Server Address	dynupdate.no-ip.com
Device Domain Name	
Status	
User Name	
Password	

- iv. Enter **Server Address** for NO-IP (*dynupdate.no-ip.com*).
- v. In the **Device Domain Name**, **User Name** and **Password** fields, enter the information setup at the *alibiddns.com* website. For example: *<your domain name>.alibiddns.com*
- vi. Click **Apply** to save your settings.

— **PeanutHull**: PeanutHull is now part of NO-IP. Use the procedure above in NO-IP to setup a DDNS connection.

The screenshot shows the 'Configuration' window with the 'DDNS' tab selected. The 'Network' menu item is highlighted in the left sidebar. The DDNS settings are as follows:

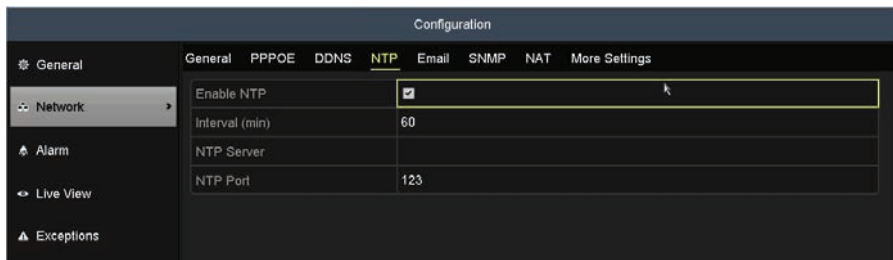
Field	Value
Enable DDNS	<input checked="" type="checkbox"/>
DDNS Type	PeanutHull
Area/Country	Custom
Server Address	
Device Domain Name	
Status	
User Name	
Password	

9.2.3 Configuring NTP Server

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

1. Open the Network Settings menu. Go to **Menu | Configuration | Network**.

- Click the **NTP** tab to open the NTP Settings menu.

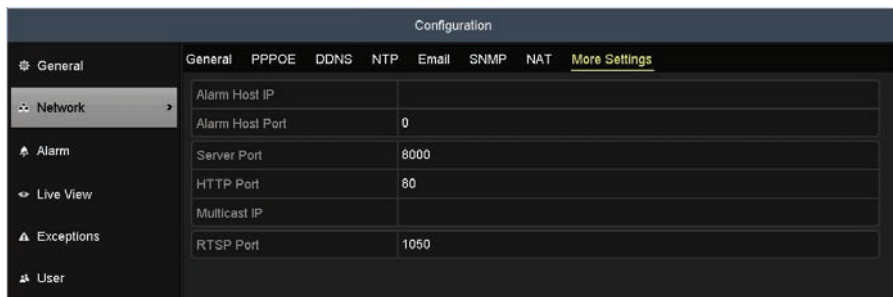


- Check the **Enable NTP** box to enable this feature.
- Select the following NTP settings:
 - Interval:** Interval in minutes between the two synchronizing actions with an NTP server.
NOTE: The synchronization time interval can be set from 1 to 10080 minutes. The default value is 60 min. If the NVR 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 setup in a customized network, NTP software can be used to establish a NTP server used for time synchronization.
 - NTP Server:** IP address of NTP server
 - NTP Port:** Port of NTP server
- Click **Apply** to save your settings and close the menu.

9.2.4 Configuring Remote Alarm Host

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

- Open the Network Settings menu. Go to **Menu | Configuration | Network**.
- Click the More Settings tab to open the **More Settings** menu.

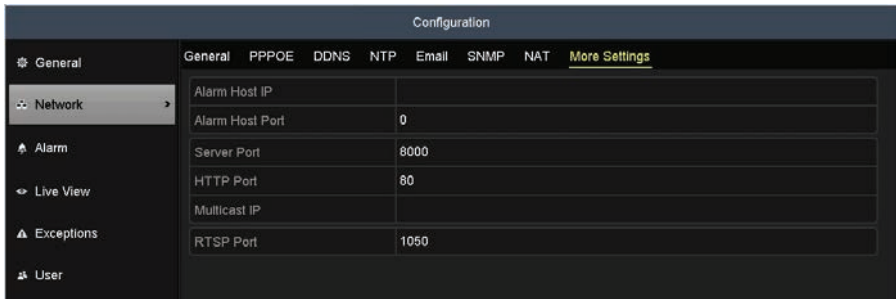


- Enter the Alarm Host IP address and Alarm Host Port in the appropriate fields. The Alarm Host IP address is the IP address of the remote PC on which Network Video Surveillance Software is installed. The Alarm Host Port must be the same as the alarm monitoring port configured in the software.
- Click **Apply** to save your settings and close the menu.

9.2.5 Configuring Multicast

Using the multicast function, more than 64 cameras are connectable. A multicast address spans the Class-D IP range of 224.0.0.0 to 239.255.255.255. We recommend that you use the IP address range from 239.252.0.0 to 239.255.255.255.

- Enter the Network Settings interface. Go to **Menu | Configuration | Network**.
- Click the **More Settings** tab to open the **More Settings** menu.



- Set the Multicast IP address. When adding a device to the Network Video Surveillance Software, the multicast address must be the same as the NVR's multicast IP.

Server Port	8000
HTTP Port	80
Multicast IP	239.221.2.78

- Click **Apply** to save your settings and close the menu.

NOTE *The multicast function must be supported by the network switch to which the NVR is connected.*

9.2.6 Configuring RTSP

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

1. Open the Network Settings menu. Go to **Menu | Configuration | Network**.
2. Click the **More Settings**.

The screenshot shows the 'Configuration' interface with the 'Network' menu item selected. The 'More Settings' sub-tab is active, displaying the following configuration table:

Field	Value
Alarm Host IP	
Alarm Host Port	0
Server Port	8000
HTTP Port	80
Multicast IP	
RTSP Port	1050

3. In the menu shown above, enter the RTSP port number. The default RTSP port is 1050.
4. Click **Apply** to save your settings and close the menu.

9.2.7 Configuring Server and HTTP Ports

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

1. Open the Network Settings menu. Go to **Menu | Configuration | Network**.
2. Click the **More Settings** tab to open the **More Settings** menu.

The screenshot shows the 'Configuration' interface with the 'Network' menu item selected. The 'More Settings' sub-tab is active, displaying the following configuration table:

Field	Value
Alarm Host IP	
Alarm Host Port	0
Server Port	8000
HTTP Port	80
Multicast IP	
RTSP Port	1050

- Enter a new Server Port number and HTTP Port number in the appropriate fields. The default Server Port is 8000 and the HTTP Port is 80.

Server Port	8000
HTTP Port	80
Multicast IP	239.221.2.78
RTSP Port	1050

NOTE

The Server Port number must be in the range 2000..65535. It is used for remote client software access. The HTTP port is used for remote IE access.

- Click **Apply** to save your settings and close the menu.

9.2.8 Configuring Email

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

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

- Open the Network Settings menu. Go to **Menu | Configuration | Network**.
- Set the IPv4 Address, IPv4 Subnet Mask, IPv4 Gateway and the Preferred DNS Server in the Network Settings menu.

The screenshot shows the 'Configuration' menu with 'Network' selected. The settings are as follows:

Setting	Value
Working Mode	Net Fault-tolerance
Select NIC	bond0
NIC Type	10M/100M/1000M Self-adaptive
Enable DHCP	<input type="checkbox"/>
IPv4 Address	192.168.0.30
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	.
IPv6 Address 1	fe80::1a68:cbff:fe86:ce5e/64
IPv6 Address 2	.
IPv6 Default Gateway	.
MAC Address	18:68:cb:86:ce:5e
MTU(Bytes)	1500
Preferred DNS Server	
Alternate DNS Server	
Main NIC	LAN1

SECTION 9: NETWORK SETTINGS

3. Click **Apply** to save your settings and close the menu.
4. Click the **Email** tab to open the email settings menu.

The screenshot shows the 'Configuration' page with the 'Email' tab selected. The left sidebar contains navigation options: General, Network, Alarm, Live View, Exceptions, User, and Hot Spare. The main content area is divided into several sections:

- General:** 'Enable Server...' checkbox (checked), 'User Name', 'Password', 'SMTP Server', 'SMTP Port' (25), 'Enable SSL/T...' checkbox (unchecked).
- Sender:** 'Sender', 'Sender's Address'.
- Select Receivers:** Dropdown menu showing 'Receiver 1'.
- Receiver:** 'Receiver', 'Receiver's Address'.
- Enable Attached Picture:** 'Enable Attached Picture' checkbox (unchecked), 'Interval' (2s).

At the bottom right, there are three buttons: 'Test', 'Apply', and 'Back'.

5. Configure the following Email settings:
 - **Enable Server Authentication** (optional): Check the checkbox to enable the server authentication feature.
 - **User Name:** The user account of sender's Email for SMTP server authentication.
 - **Password:** The password of sender's Email for SMTP server authentication.
 - **SMTP Server:** The SMTP Server IP address or host name (e.g., smtp.263xmail.com).
 - **SMTP Port No.:** The SMTP port. The default TCP/IP port used for SMTP is 25.
 - **Enable SSL/TLS** (optional): Click the checkbox to enable SSL/TLS if required by the SMTP server.
 - **Sender:** The name of sender.
 - **Sender's Address:** The Email address of sender.
 - **Select Receivers:** Select the receiver. Up to 3 receivers can be configured.
 - **Receiver:** The name of user to be notified.
 - **Receiver's Address:** The Email address of user to be notified.
 - **Enable Attached Pictures:** Check the Enable Attached Picture box if you want to send email with attached alarm images. The interval is the time of two adjacent alarm images. You can also set SMTP port and enable SSL/TLS here.
 - **Interval:** The interval refers to the time between two actions of sending attached pictures.
 - **Test:** Click this button to send a test message to verify that the SMTP server can be reached.
6. Click **Apply** to save your settings. A configuration using a Gmail email account may look like the following.

Configuration

General PPOE DDNS NTP **Email** SNMP NAT More Settings

General

Network

Alarm

Live View

Exceptions

User

Hot Spare

Live View

Enable Server...

User Name HVR30H@gmail.com

Password *****

SMTP Server snmp.gmail.com

SMTP Port 587

Enable SSL/T...

Sender Yatch Harbor

Sender's Address Yatchs@ATT.com

Select Receivers Receiver 1

Receiver Joe

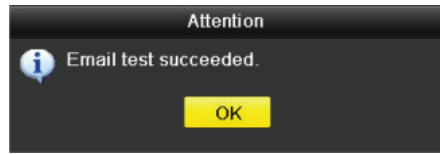
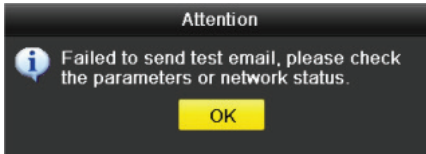
Receiver's Address Joe@Observint.com

Enable Attached Picture

Interval 2s

Test Apply Back

- Click the **Test** button to test your Email settings. The corresponding **Attention** message box will pop up.

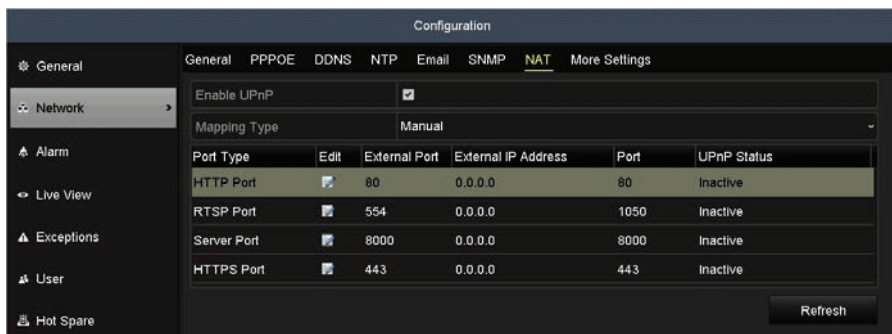


9.2.9 Configuring UPnP™

The Universal Plug and Play (UPnP™) feature allows the device to seamlessly discover other network devices 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.

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

- Open the Network Settings menu. Go to **Menu | Configuration | Network**.
- Click the **NAT** tab to open the NAT settings menu.



- If your router supports UPnP and you want to configure it for port forwarding, check the **Enable UPnP** box. **NOTE:** To use UPnP, UPnP usually must also be enabled in the router.
- Open the **Mapping Type** drop down list, and then select either:
 - Auto:** This option automatically sets the **External Port** numbers for the recorder. The **Ports** (internal network ports) used by the recorder for HTTP (80), RTSP (1050), Server (8000) and HTTPS (443) remain at their default values. The new external port numbers will appear on this display. Use these ports numbers when establishing a connection to the recorder from outside the local network.
 - Manual:** This option allows you to change the **External Port** numbers by clicking the icon in the **Edit** column for the HTTP, RTSP, Server and/or HTTPS ports. The Ports (internal ports) remain unchanged.
- If settings in this menu were changed, click **Refresh**, and then click **Apply** to save the changes.

SECTION 10

System Maintenance

The Maintenance menus provide several displays that report system device information, log information, and network traffic. Features also include the export and import of the system configuration file, firmware upgrade, and factory reset.

10.1 System Information

The System Information displays include status reports of the NVR, cameras, record settings, the network and the HDDs. The configuration settings shown on these displays can only be changed in other areas of the menu system.

- To open the System Information displays, go to **Menu | Maintenance | System Info**. The Device Info tab includes information about the NVR.

System Maintenance	
System Info	Device Info Camera Record Alarm Network HDD Device Status
Log Information	
Import/Export	
Upgrade	
Default	
Net Detect	
Device Name	Network Video Recorder
Model	ALI-NVR7112BR
Extended Circuit Board Model	DS-96000D-H/DS-96000X
Serial No.	1620170522CCR767555004WCVLU
Firmware Version	V3.6.22, Build 170713
Hardware Version	0x20002700

The **System Info | Device Info** screen includes a **Check Update** button for checking for updated firmware. The FTP upgrade server must be operational for this feature to function properly. See “10.4 Upgrade Firmware” on page 182 for more information.

To view information about other parts of the system, click the appropriate tab.

10.2 Log Information, Log Export

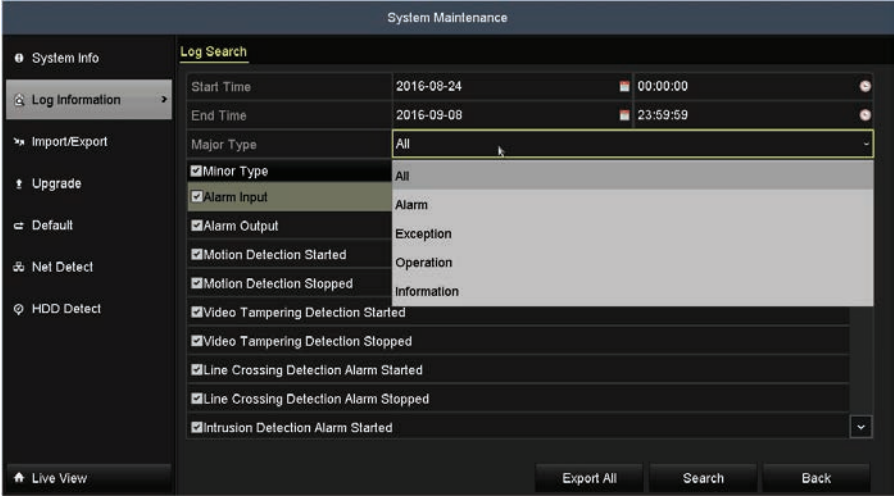
System log information is continuously generated and saved in log records. System logs include the following types of entries:

- Alarms events** - Start/stop motion detection, start/stop tamper detection etc.
- Exception conditions** - Video loss, illegal login, HDD full/error, IP camera disconnected, network disconnected, etc.
- Information events** - Start/stop recording, local/network HDD information, HDD S.M.A.R.T., etc.
- Operation events** - power on, login, local operation logout, etc.

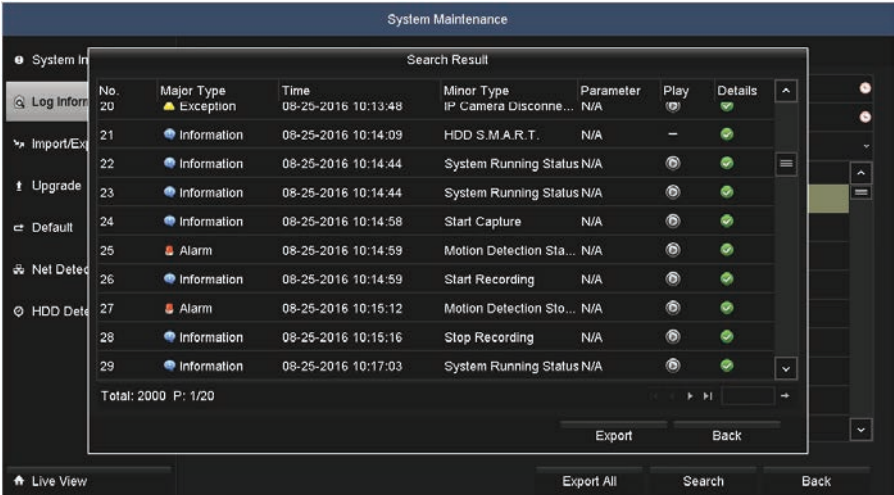
System logs can be searched and sorted for specific entries, and archived for use later. You can also search for video clips through system logs.

10.2.1 Log Search

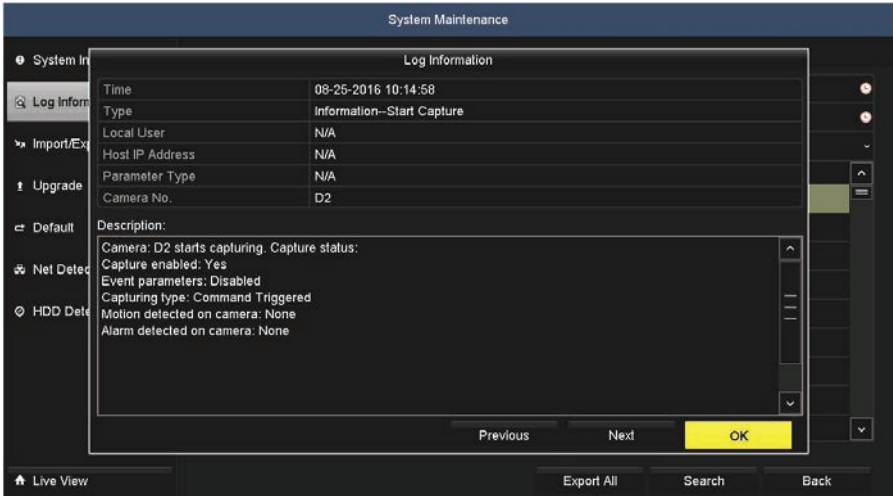
1. Open the Log Information screen. Go to **Menu | Maintenance | Log Information**.



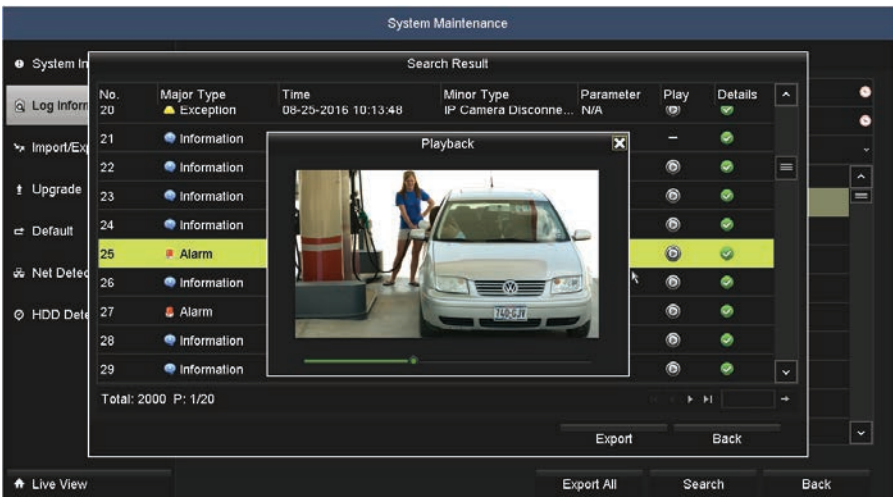
2. Select a Start Time, End Time, Major Type and Minor Type., then click **Search**. In the example below, the search criterion specified are "All" (Major Type) entries.



- You can Export the result of the log search (click Export), choose a log entry with record file and click the playback button to play the file, or click the icon in the Details column to see more information about the entry. Click the icon in the **Details** column (see below) or Play column to see more information about the log entry.



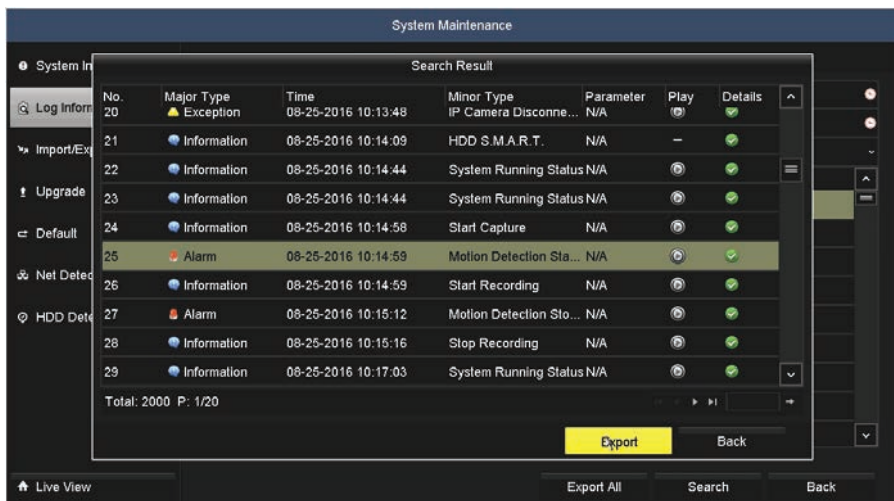
- Click **OK** to return to the **Search Result** window.
- If the log entry is associated with a video clip or capture, click the icon in the **Play** column to playback the video.



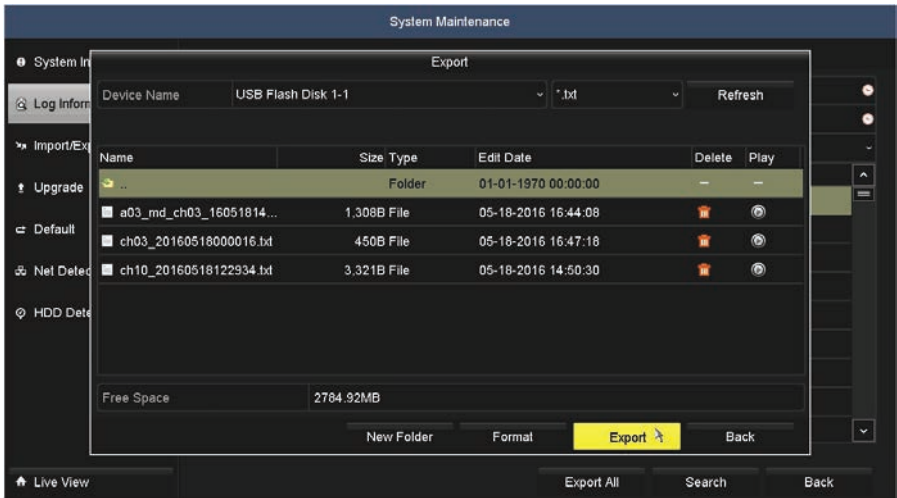
Log Export

Log information can be exported to a backup device such as a USB storage device. The exported log file is in .txt format and readable with an ASCII text viewer such as Microsoft® Windows® Notepad or Wordpad. The filename, prefixed with the date and timestamp, in the format *YYYYMMDDHHMMSSlogBack.txt*. To export the log file:

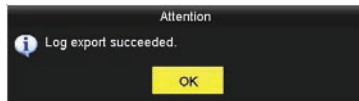
1. In the **Search Result** window, click the **Export** button.



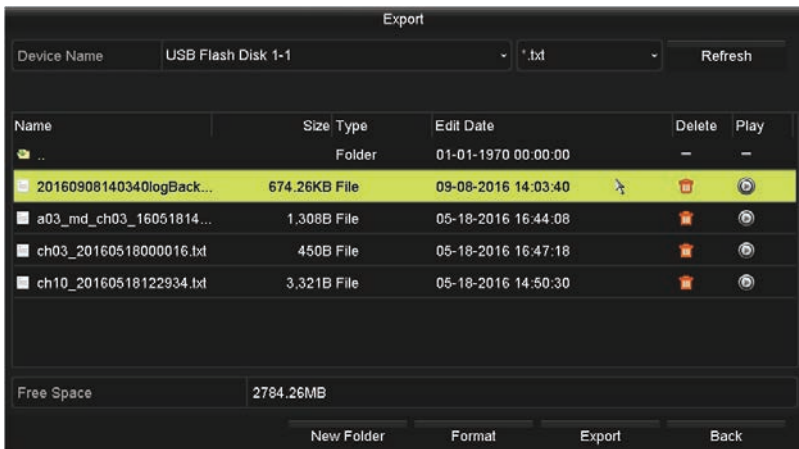
2. On the **Device Name** line, open the drop down list and select the destination for the file export. To export the file to a USB flash drive, insert the flash drive into a USB port (see the example below).



3. Select the directory where you want to copy the files, create a **New Folder**, or save the log file to the root directory (see above).
4. Click the **Export** button to start the **Export**. Allow the operation to finish before continuing.



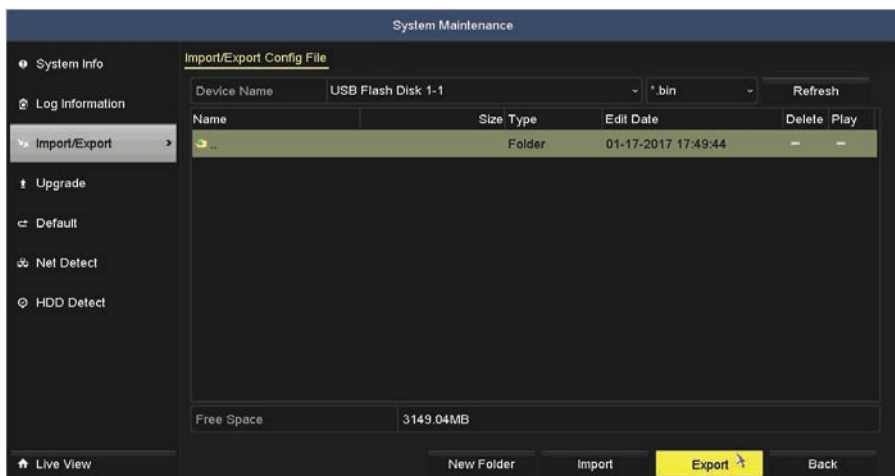
5. Check the Export result on a computer by opening a file that was saved.



10.3 Import / Export system configuration

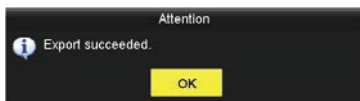
You can export the NVR configuration, then import the file later to restore the earlier configuration.

1. Attach an USB storage device, such as a USB flash drive or USB disk drive, to the NVR USB port.
2. Open the **Import/Export** menu. Go to **Menu | Maintenance | Import/Export**.
3. On the **Device Name** line, open the drop down list and select the destination for the exported configuration file. In this example, a USB drive was selected.

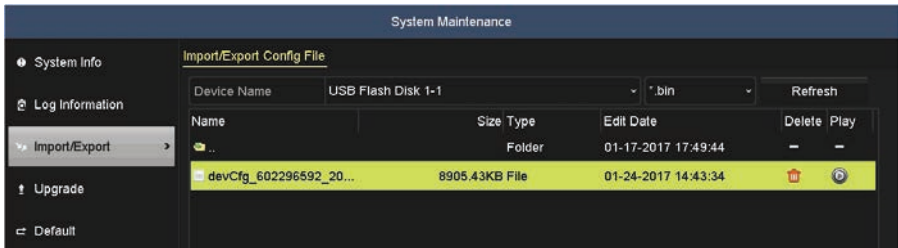


Export configuration file

4. In the Device directory, highlight the location where you want to save the configuration file.
5. Click the **Export** button to start the export. Allow the operation to finish before continuing. When the export operation is successful, an "Attention" "Export succeeded" pop-up window will open.



6. Click **OK** to close the pop-up window.

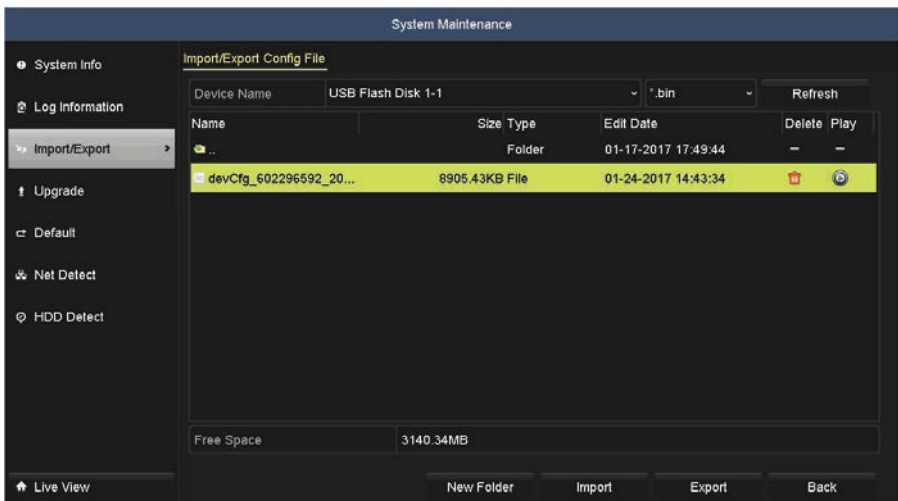


NOTE: The configuration backup file is a binary file with a timestamp in the format `devCfg_<code>_YYYYMMDDHHMMSS.bin`

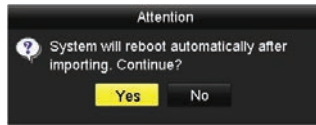
- Record the name of the exported file for future reference.

Import configuration file

- On the **Device Name** line, open the drop down list and select the destination of the exported configuration file. The configuration backup file is a binary file with a timestamp in the format `devCfg_<code>_YYYYMMDDHHMMSS.bin`.
- If the configuration file was saved to a directory, click the folder icon to the left of the directory name to open the directory.
- In the file list, highlight the NVR configuration file you want to load, and then click **Import**.



- You must reboot the recorder to complete the configuration import. Click **Yes** in the **Attention** window.



5. Allow the NVR to fully reboot.

10.4 Upgrade Firmware

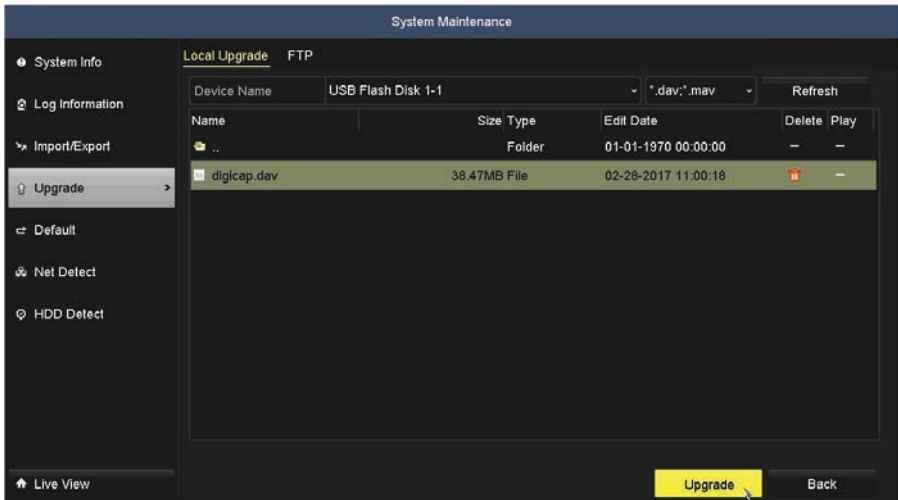
You can upgrade the firmware through a local device or FTP server. You should check the current Firmware version before upgrading your NVR firmware. **Firmware upgrade should only be performed when recommended by your NVR support organization.**

1. To check the current firmware version, open the System information display. Go to **Menu | Maintenance | System Information**.

 A screenshot of the "System Maintenance" web interface. The top navigation bar includes "System Info", "Device Info", "Camera", "Record", "Alarm", "Network", "HDD", and "Device Status". The "System Info" section is expanded, showing a sidebar with "Log Information", "Import/Export", "Upgrade", "Default", and "Net Detect". The main content area displays a table of device information:

Device Name	Network Video Recorder
Model	ALI-NVR71128R
Extended Circuit Board Model	DS-96000D-H/DS-96000X
Serial No.	1620170522CCRR767555004WCVLU
Firmware Version	V3.6.22, Build 170713
Hardware Version	0x20002700

2. Click the **Check Update** button to determine if a firmware update is available for this recorder.
3. If the firmware needs to be upgraded, click the **Upgrade** tab on the left.
4. If installing firmware from a local device such as a USB flash drive or disk:

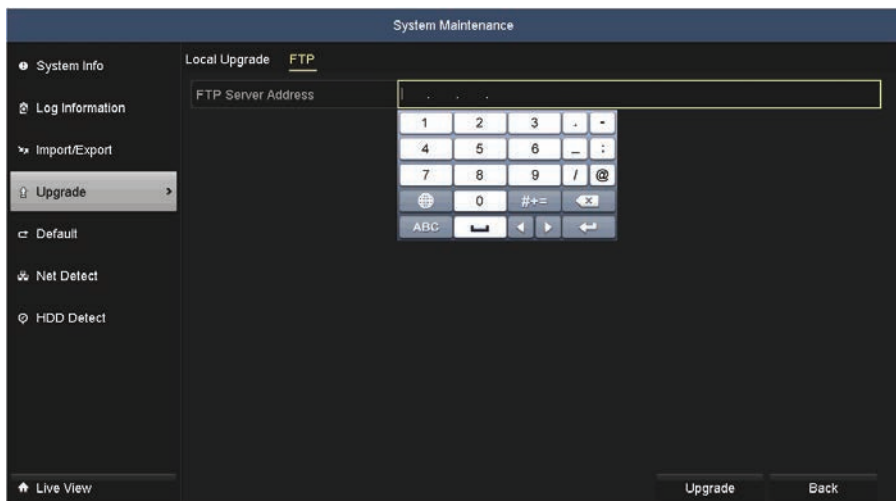


- a. Connect the local device to the NVR, if necessary.
 - b. Open the **Device Name** drop down list and select the device that contains the firmware.
 - c. Click the firmware file you want to load. The firmware file normally has the file name extension **.dav**.
 - d. Click the **Upgrade** button, then follow the on-screen instructions for completing the upgrade. The upgrade may require a reboot of the recorder.
5. If installing firmware from a FTP server:
 - a. Click the FTP upgrade tab at the top of the menu.
 - b. Click the firmware file you want to load.
 - c. Click the **Upgrade** button, then follow the on-screen instructions for completing the upgrade. The upgrade may require a reboot of the recorder.
 6. Open the System Information screen and verify that the new firmware version is installed.

10.4.1 Upgrade from FTP server

If an FTP server contains the firmware upgrade file and the recorder has network access to that device, you can upgrade directly from that location. To upgrade from an FTP server, do the following:

1. Click the **FTP** tab in the **System Maintenance | Upgrade** menu.



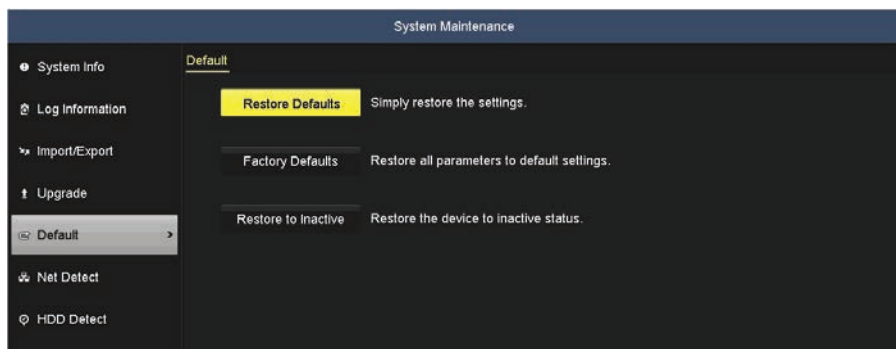
2. Click anywhere in the FTP Server Address field to open the virtual keyboard, and then enter the IP address of the server.
3. Click the **Upgrade** button at the bottom of the window, and follow the on-screen instructions to complete the upgrade.

10.5 Default

The default options enable you to revert the configuration to its original settings in one of three ways. A reboot is often required to complete the operation.

To restore the device to a default configuration:

1. Open the Log Information menu. Go to **Menu | Maintenance | Default**.



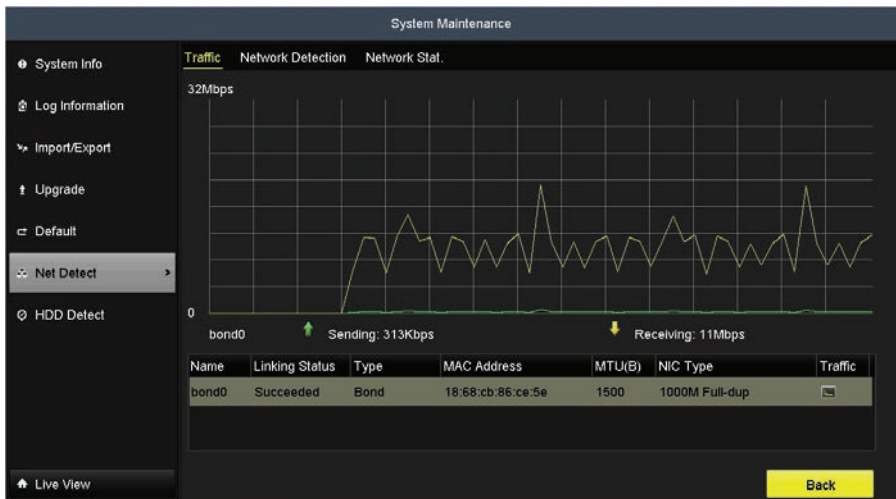
2. Click one of the following options:
 - **Restore Defaults:** Restore all parameters, except the network (including IP address, subnet mask, gateway, MTU, NIC working mode, default route, server port, etc.) and user account parameters, to the factory default settings.
 - **Factory Defaults:** Restore all parameters to the factory default settings.
 - **Restore to Inactive:** Restore the device to inactive status.
3. Follow the on-screen instructions to complete the restore operation.

10.6 Net Detect

10.6.1 Checking Network Traffic

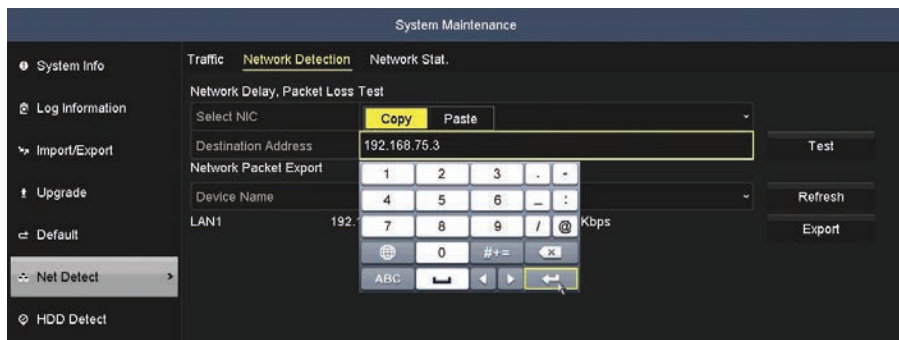
You can see real-time information of your NVR network traffic, such as linking status, MTU, sending/receiving rate, etc. The traffic data is refreshed every 1 second.

1. Open the Network Traffic menu. Go to **Menu | Maintenance | Net Detect**.

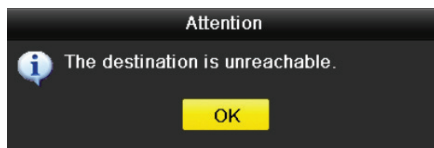
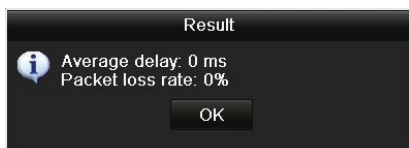


10.6.2 Testing Network Delay and Packet Loss

1. Open the Network Traffic menu. Go to **Menu | Maintenance | Net Detect**.
2. Click the **Network Detection** tab to open the menu.



3. Enter the destination address in the Destination Address field. In the screen above, the address **192.168.75.3** was entered.
4. Click the **Test** button to begin the test for network delay and packet loss. The testing result appear in the window. If the testing is failed, the error message box will open.



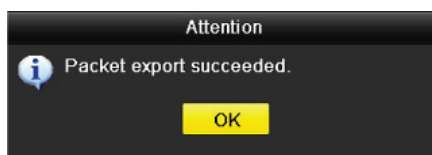
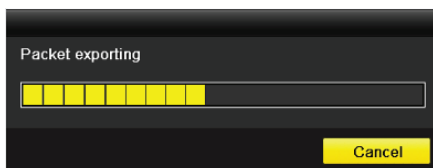
10.6.3 Exporting Network Packet

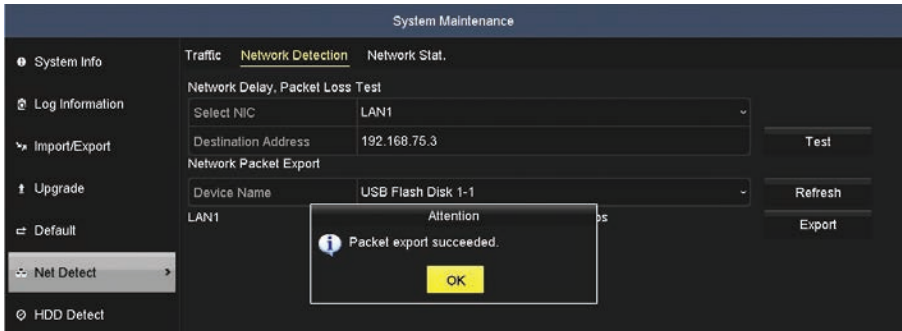
By connecting the NVR to network, the captured network data packet can be exported to a USB device such as a flash drive, HDD, DVD-R/W and other local USB backup devices.

1. Open the Network Traffic menu. Go to **Menu | Maintenance | Net Detect**.
2. Click the **Network Detection** tab to open the Network Detection menu.
3. Select the backup device from the **Device Name** drop down list.

Note: Click the **Refresh** button if the connected local backup device cannot be displayed. When it fails to detect the backup device, verify that it is compatible with the NVR. Format the backup device if the format is incorrect.

4. Click the **Export** button to start the export.



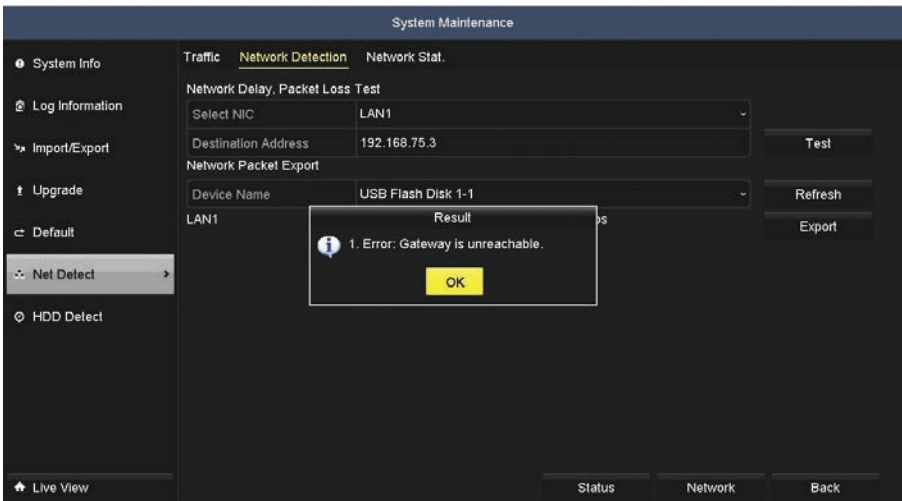


- When the export is complete, click **OK**. Up to 1 M data can be exported during one operation.

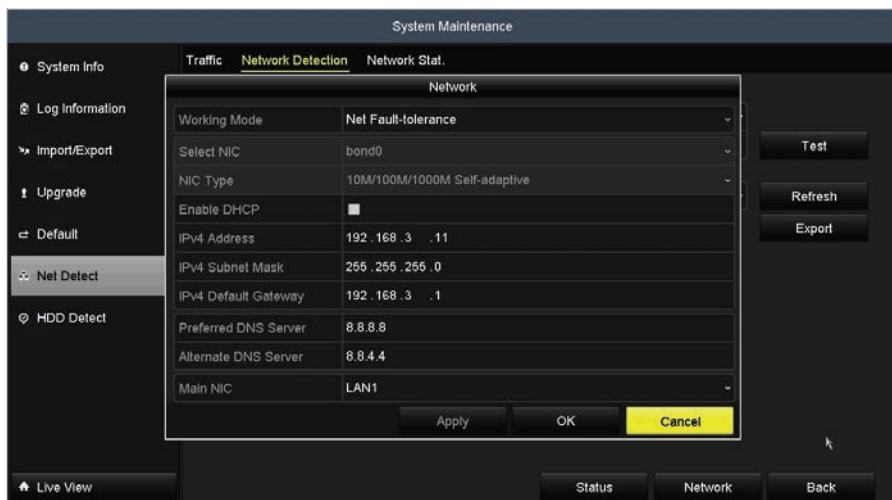
10.6.4 Checking the network status

You can also check the network status and quickly set the network parameters.

- Open the Network Traffic menu. Go to **Menu | Maintenance | Net Detect**.
- Click the **Network Detection** tab to open the Network Detection menu.
- Click the **Status** button in the lower right corner to report the status.



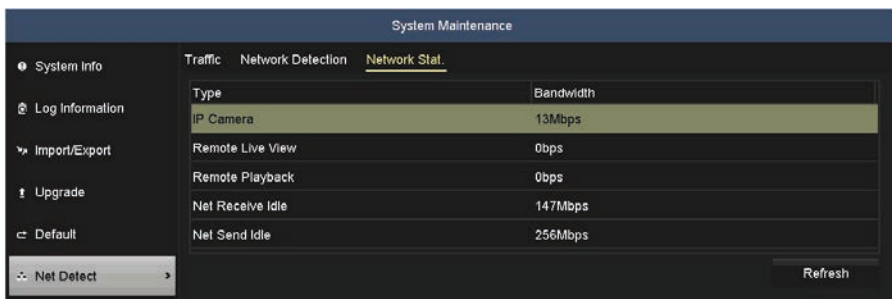
- If the message box shows other information, click the **Network** button to open the **Network** parameters menu. After changing parameters, click **Apply**, and then click **OK** to save your settings and retry this test.



10.6.5 Checking Network Statistics

Use the following procedure to view real time network status of your NVR.

- Open the Network Traffic menu. Go to **Menu | Maintenance | Net Detect**.
- Click the **Network Stat.** tab to open the Network status report.



Use this display to check the bandwidth of the IP Camera, bandwidth of Remote Live View, bandwidth of Remote Playback, bandwidth of Net Receive Idle and bandwidth of Net Send Idle.

- Click the **Refresh** button to show the current status.

10.6.6 HDD Detect

The **HDD Detect** feature provides two methods of monitoring the HDD: display of **S.M.A.R.T.** (Self-Monitoring, Analysis and Reporting Technology) data, and **Bad Sector Detection**. These methods can be used to assure the normal functioning of the disk, and anticipate failures.

S.M.A.R.T. Display

1. Open the S.M.A.R.T. display menu. Go to **Menu | System Maintenance | HDD Detect**. S.M.A.R.T. data may be shown on this display.

The screenshot shows the 'System Maintenance' interface. On the left is a navigation menu with options: System Info, Log Information, Import/Export, Upgrade, Default, Net Detect, and HDD Detect (selected). The main area is titled 'S.M.A.R.T. Settings' and 'Bad Sector Detection'. It displays the following settings:

- HDD: 1
- Self-test Status: Not tested
- Self-test Type: Short Test
- S.M.A.R.T.:
- Temperature(°C): 34
- Power On (days): 46
- Self-evaluation: Pass
- All-evaluation: Functional

Below these settings is the 'S.M.A.R.T. Information' table:

ID	Attribute Name	Status	Flags	Threshold	Value	Worst	Raw Value
0x1	Raw Read Error Rate	OK	b	16	100	100	0
0x2	Throughput Performance	OK	5	54	131	131	116
0x3	Spin Up Time	OK	7	24	206	206	38671155588
0x4	Start/Stop Count	OK	12	0	100	100	99

At the bottom of the screen, there are 'Live View' and 'Back' buttons.

2. To execute a self-evaluation test on an HDD:
 - a. On the **HDD** line, open the drop down list to select the HDD of interest.
 - b. On the **Self-test Type** line, open the drop down list to select the type of test to execute. You can choose either Short Test, Expanded Test or Conveyance Test.
 - c. Click the icon on the **S.M.A.R.T.** line to execute the test. Allow the test to complete before continuing. The result of the test is shown on the Self-evaluation line.

The screenshot shows the 'System Maintenance' interface. On the left is a navigation menu with options: System Info, Log Information, Import/Export, Upgrade, Default, Net Detect, and HDD Detect (selected). The main area is titled 'S.M.A.R.T. Settings' and 'Bad Sector Detection'. It contains several settings: HDD (1), Self-test Status (Not tested), Self-test Type (Short Test), S.M.A.R.T. (a dropdown menu), Temperature (34), Power On (46), Self-evaluation (Pass), and All-evaluation (Functional). Below these is the 'S.M.A.R.T. Information' table.

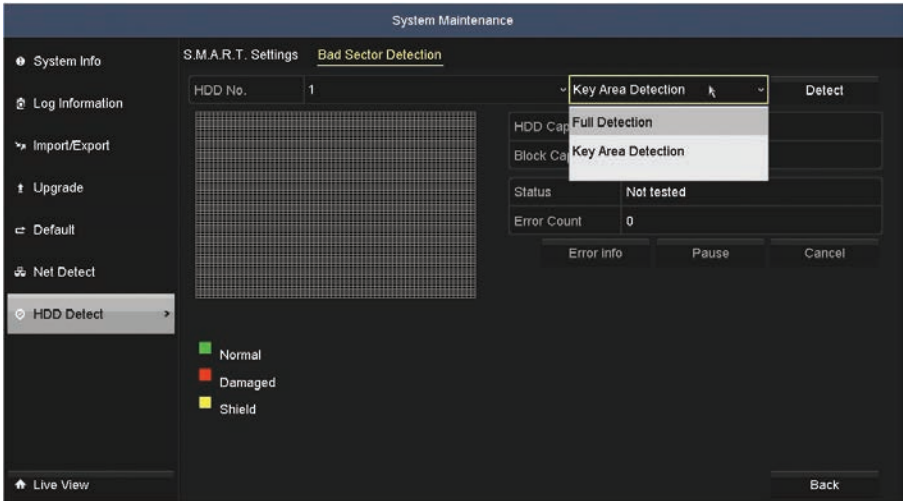
ID	Attribute Name	Status	Flags	Threshold	Value	Worst	Raw Value
0x1	Raw Read Error Rate	OK	b	16	100	100	0
0x2	Throughput Performance	OK	5	54	131	131	116
0x3	Spin Up Time	OK	7	24	206	206	38671155588
0x4	Start/Stop Count	OK	12	0	100	100	99

- Examine the S.M.A.R.T. data provided for the HDD. Check to ensure that the data in the value and Worst column does not exceed the data in the Threshold column.

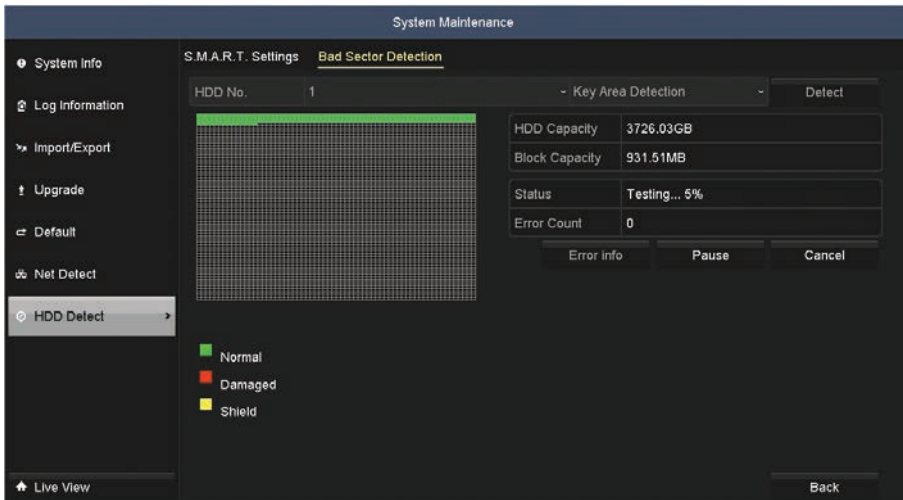
NOTE *S.M.A.R.T. data provided by each HDD manufacturer is usually different. Refer to the manufacturer's website for S.M.A.R.T. data definitions.*

Bad Sector Detection

- Open the Bad Sector Detection menu. Go to **Menu | System Maintenance | HDD Detect | Bad Sector Detection**.
- On the **HDD No.** line, open the drop down list and select the number of the HDD you want to test.
- Open the drop down list to the right of the HDD number, and then select either **Key Area Detection** or **Full Detection**. Key Area Detection will execute an abbreviated surface analysis of the HDD.



- Click the **Detect** button to start the detection. Bad sectors are identified in the array as red colored cells.



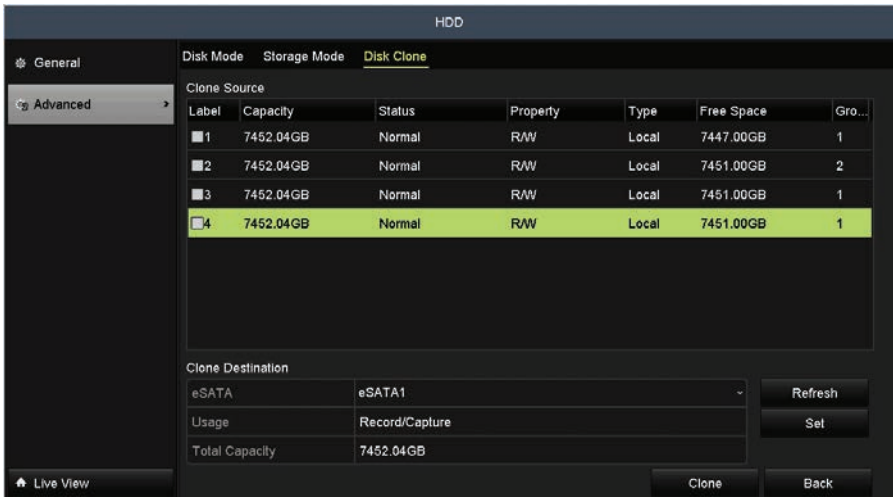
Click **Pause** to temporarily stop the scan, and click **Cancel** to end the scan.

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

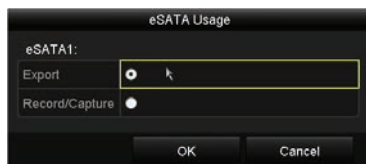
10.7 Disk Clone

If a S.M.A.R.T. detection result finds an HDD is abnormal, you can clone (duplicate) the data on the HDD to a disk connected to the eSATA port. The disk connected to the eSATA port must have the same capacity as the internal HDD you are cloning. This feature is not available when RAID is enabled. To clone an HDD:

1. Install an HDD on the eSATA interface that has the same capacity as the disk you want to clone.
2. Verify that the eSATA HDD is initialized:
 - a. Go to **Menu | HDD | General**.
 - b. Check the status of the eSATA device.
 - c. If Status does not show **NORMAL** status, check the select box for the device, and then click **Init**. Allow the operation to complete before continuing.
3. Open the Disk Clone menu. Go to **Menu | HDD | Advanced | Disk Clone**.



4. Verify that the capacity of the **Clone Source** disk is the same as the **Clone Destination** (eSATA) disk. See above.
5. In the Clone Destination section, click the **Set** button. In the **eSATA Usage** window, select **Export**, and then click **OK**.



6. In the **Clone Source** list, check the select box of the HDD you want to clone.

The screenshot shows the 'HDD' configuration page with the 'Advanced' tab selected. The 'Disk Clone' section is active, displaying a table of available HDDs for cloning. The fourth HDD is selected. Below the table, the 'Clone Destination' section shows 'eSATA1' selected for the destination and 'Export' for the usage. A yellow 'Clone' button is highlighted at the bottom right.

Label	Capacity	Status	Property	Type	Free Space	Gr...
1	7452.04GB	Normal	R/W	Local	7447.00GB	1
2	7452.04GB	Normal	R/W	Local	7451.00GB	2
3	7452.04GB	Normal	R/W	Local	7451.00GB	1
<input checked="" type="checkbox"/> 4	7452.04GB	Normal	R/W	Local	7451.00GB	1

Clone Destination

eSATA1 (Selected)

Usage: Export

Total Capacity: 7452.04GB

Buttons: Refresh, Set, Clone (highlighted), Back

7. Click the **Clone** button at the bottom of the screen. Allow the operation to complete before continuing.

SECTION 11

Managing HDDs (without RAID)

NVR storage (HDDs) is highly configurable. You can simply save data to the internal HDD(s) in the chassis, or add network based NAS or IP SAN devices to the system and save recordings and other data there. You can also define where data for each camera or groups of cameras is saved, and have 16 different storage groups. Before an HDD is used by the NVR, it must be initialized by the recorder. Preconfigured HDD(s) are already initialized.

If you add an internal HDD to the recorder, or replace an HDD in the recorder, it must be initialized before it can be used. See “11.1 Initializing HDDs” on page 194 for more information.

The recorder can also be used in RAID mode. To configure the storage system for RAID, see “SECTION 12 RAID Arrays” on page 206.

11.1 Initializing HDDs

An HDD must be initialized before it can be used by the recorder to store data. Pre-installed HDDs are initialized by your vendor. Check the status of the HDD installed in the NVR to assure it is functioning normally.

1. Open the HDD Information display. Go to **Menu | HDD | General**. The HDD shown here represents the capacity of the RAID storage array.

Label	Capacity	Status	Property	Type	Free Space	Gr...	Edit	Delete
1	7452.04GB	Normal	R/W	Local	7449.00GB	1	—	🗑️
2	7452.04GB	Normal	R/W	Local	7451.00GB	1	—	🗑️
3	7452.04GB	Normal	R/W	Local	7451.00GB	1	—	🗑️
4	7452.04GB	Normal	R/W	Local	7451.00GB	1	—	🗑️

Total Capacity: 29.11TB
Free Space: 29.11TB

Buttons: Add, Init, Back

2. If you installed a new HDD in your NVR chassis, select the HDD in the window then click **Init** to initialize it for use. Allow the initialization procedure to complete before continuing.

11.2 Adding network HDDs to the system

Additional file storage can be added to your NVR using up to 8 NAS disks, or up to 7 NAS disks with 1 IP SAN disk. The NAS device must support NFS and Unix/Linux file formats. To configure this storage:

1. Open the HDD Information interface. Go to **Menu | HDD | General**.
2. Click the **Add** button at the bottom of the screen to open the **Add NetHDD** menu.

3. In the **NetHDD** drop down list, select the NetHDD ID (NetHDD 1 .. NetHDD 8) you want to add.
4. In the **Type** drop down list select either NAS or IP SAN.
5. Configure the device type you selected.

— **For a NAS disk:**

- i. Click the **NetHDD IP Address** field to open a virtual keyboard and enter the IP address of the storage device.

SECTION 11: MANAGING HDDs (WITHOUT RAID)

- ii. Click the **Search** button to search for available NAS disks.
- iii. Select the NAS disk directory from the list shown, or manually enter the directory in the text field of NetHDD Directory.

Add NetHDD

NetHDD	NetHDD 1
Type	NAS
NetHDD IP Address	192.168.75.24
NetHDD Directory	/mnt/Disk-1/unixSet

No.	Directory
1	/mnt/Disk-1/unixSet

Search **OK** Cancel

- iv. Click **OK** to add the NAS disk to your system. The NAS will appear in the HDD Information menu.

NOTE

After adding a storage device to the system, check the status of the device. If the Status is **Uninitialized** or **Abnormal**, initialize the device before continuing. Check the select box of the HDD to initialize, then click the **Init** button at the bottom of the screen.

HDD

General **HDD Information**

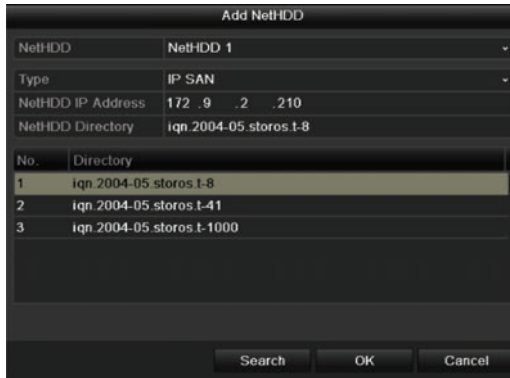
Label	Capacity	Status	Property	Type	Free Space	Gr...	Edit	Delete
1	7452.04GB	Normal	R/W	Local	7449.00GB	1	—	🗑️
2	7452.04GB	Normal	R/W	Local	7451.00GB	1	—	🗑️
3	7452.04GB	Normal	R/W	Local	7451.00GB	1	—	🗑️
4	7452.04GB	Normal	R/W	Local	7451.00GB	1	—	🗑️
<input checked="" type="checkbox"/> 17	7452.04GB	Normal	R/W	NAS	7452.04GB	1	📄	🗑️

Total Capacity: 29.11TB
Free Space: 29.11TB

Live View **Add** **Init** **Back**

— **For an IP SAN disk:**

- i. In the **Add NetHDD** window, click the **Type field**, then select **IP SAN**.
- ii. Enter the NetHDD IP address in the text field.
- iii. Click **Search** to discover the available IP SAN disk directories on the network.
- iv. Select the IP SAN disk directory from the list shown below.



- v. Click **OK** to add the selected IP SAN disk to your system.

NOTE

*After adding a storage device to the system, check the status of the device. If the Status is **Uninitialized** or **Abnormal**, initialize the device before continuing. Check the select box of the HDD to initialize, then click the Init button at the bottom of the screen.*

6. Add additional disks as needed up to a maximum of 8 NAS, or 7 NAS and 1 IP SAN. Note that HDDs added to the system may need to be initialized before use. See "2.5 Checking HDD status" on page 28 for more information.

11.3 Configuring the HDD Quota/Group mode

By default, all cameras will record to the one partition(s) of the internal HDD(s). However, the NVR can be configured to allocate space in one of two modes:

- **Quota** mode: Each camera can be allocated its own storage space for recordings and pictures on a storage device (HDD).
- **Group** mode: Groups of cameras can each be allocated recording space on a storage device. Configuring the HDD for Group recording mode requires an NVR reboot. You must have at least two HDDs (including internal and NAS/IP San HDDs added to the system) to configure Group mode.

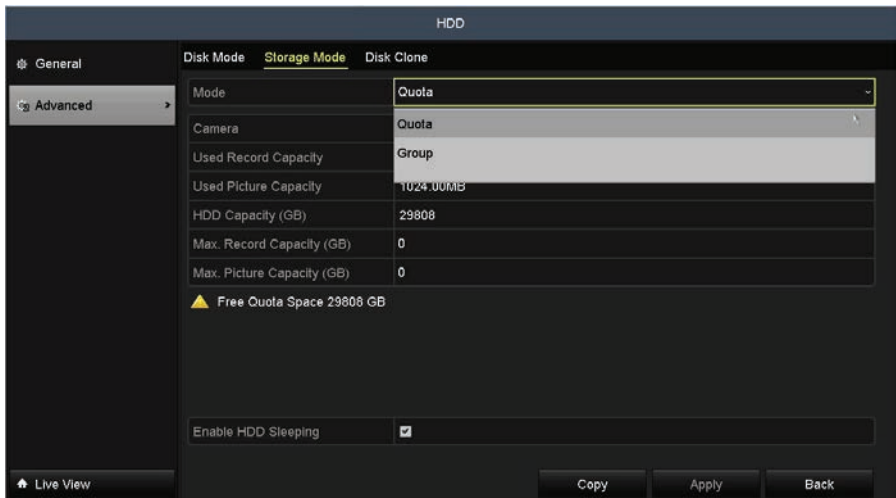
Configure for Quota mode

To configure the recorder for Quota mode:

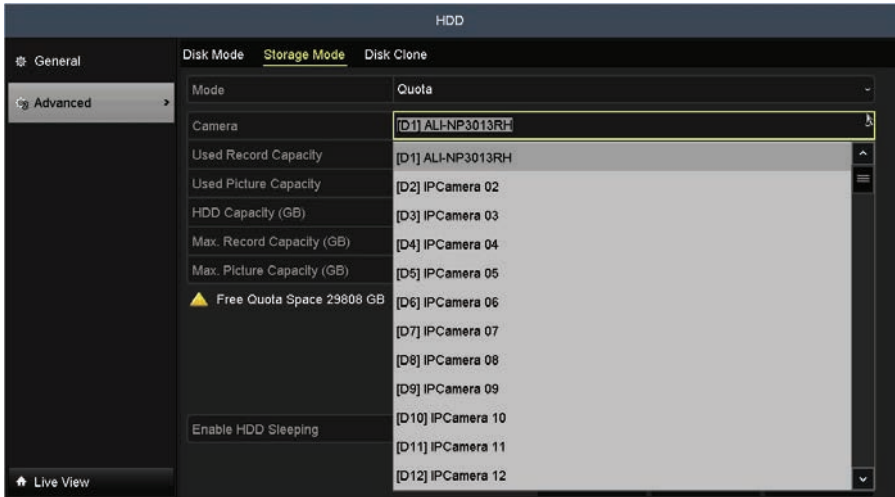
1. Go to **Menu | HDD | Advanced | Storage Mode**.



2. Open the **Mode** drop down list, and then select **Quota**, if not already selected.



- a. Open the Camera drop down list and select the camera for which you want to allocate storage space.

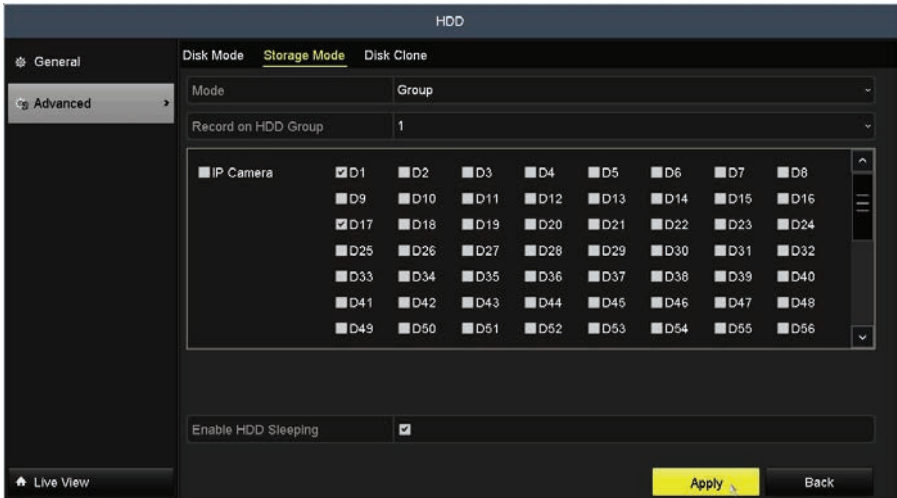


- b. Edit the **Max. Record Capacity** and the **Max. Picture Capacity** values to specify the space allocated to each. If the Quota capacity is 0 (zero), all cameras will use the total capacity of the HDD for recordings and pictures.
- c. Click **Apply** to save the settings.
- d. Repeat sub-steps a through c above for other cameras monitored by the recorder.

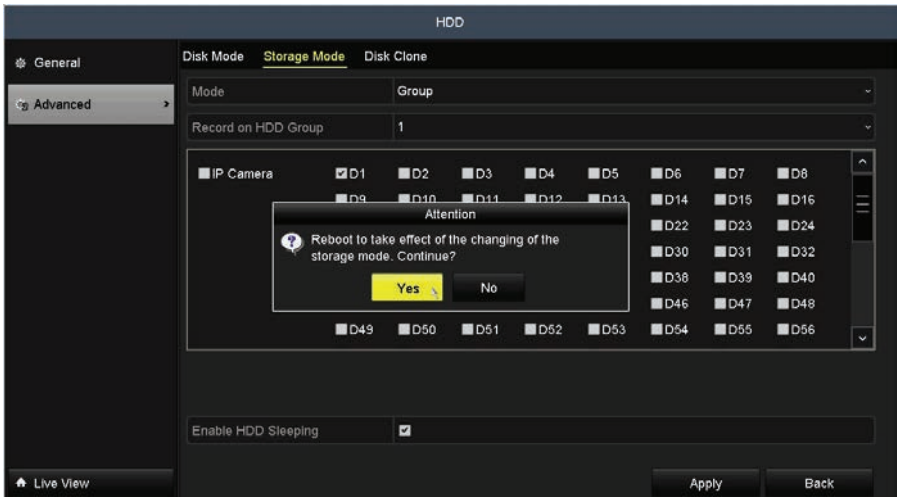
Configure for Group mode

3. If you prefer to use **Group** mode, do the following:
 - a. In the **Mode** select field, select either **Group**.
 - b. Check the box(es) for the camera(s) you want to add to the group.

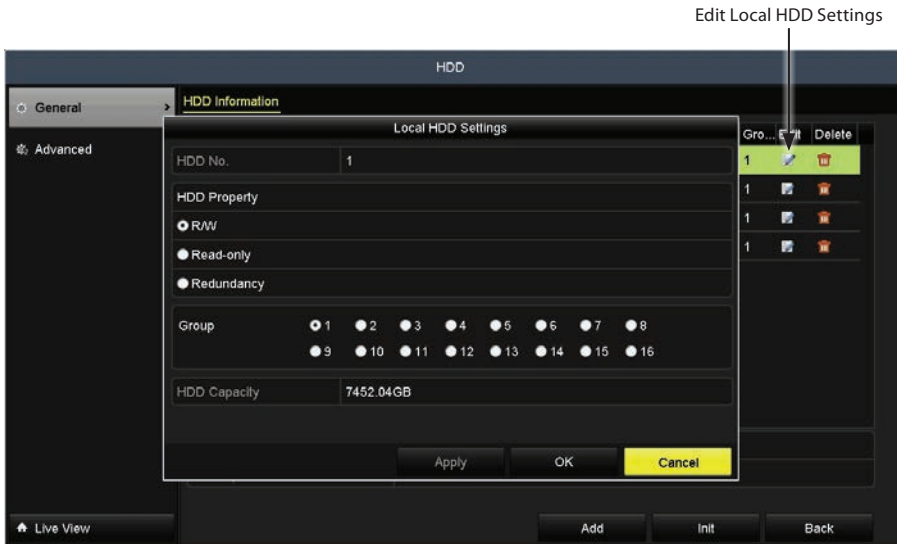
SECTION 11: MANAGING HDDs (WITHOUT RAID)



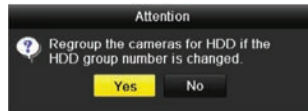
- c. Click **Apply**. If you are changing the mode from Partition to Group, reboot the system.



- d. After the reboot is complete, go to **Menu | HDD | General**.
- e. Select an HDD from the list, and then click the icon in the **Edit** column to open the Local HDD Settings menu. In this example, the **Edit** icon for HDD 1 was selected.



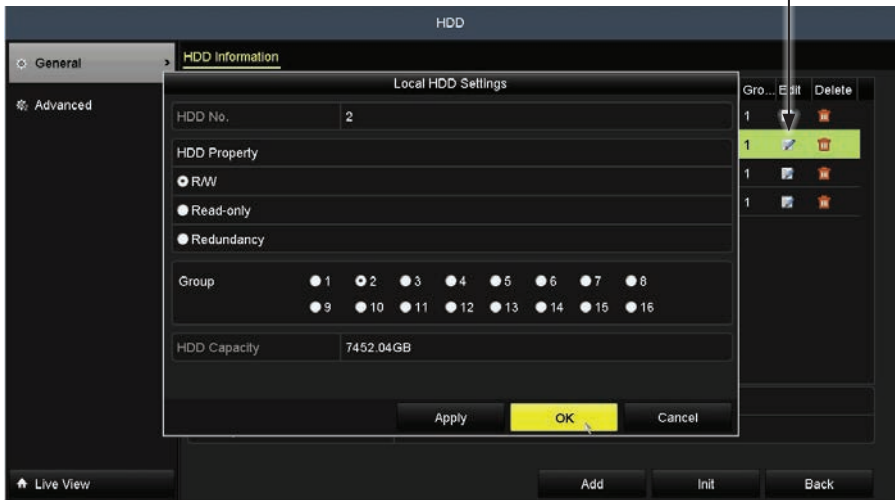
- f. Select the **HDD Property** and **Group** number for the current HDD, and then click **OK** to confirm your settings. The default group number is 1.
- g. In the pop-up Attention window, click **Yes** to complete the setup.



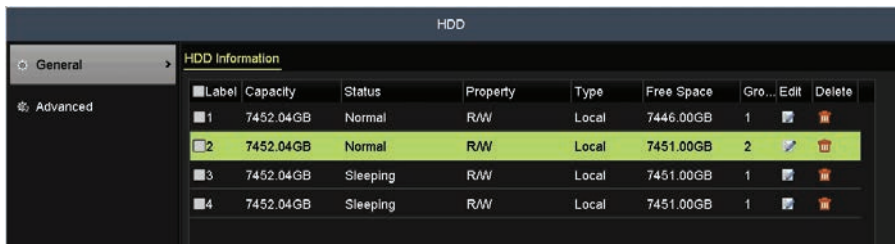
- h. To configure an additional HDD for a different group of cameras, do the following:
 - i. Open the **Menu | HDD | General** menu.
 - ii. Click the icon in the **Edit** column of an HDD not assigned to a group. In this example, the **Edit** icon for HDD 2 was selected.

SECTION 11: MANAGING HDDs (WITHOUT RAID)

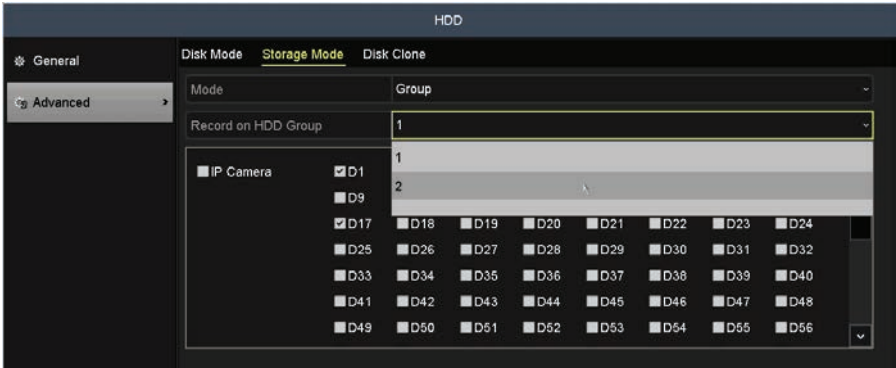
Edit Local HDD Settings



- iii. In the **Local HDD Settings** window, click the HDD property you want to assign to the group.
- iv. Select the Group number to assign to the HDD. In the example above, **Group 2** was selected.
- v. Click **Apply** to create the group, and then click **OK** to close the window.



- vi. Open the **Menu | HDD | Advanced | Storage Mode** menu.
- vii. Open the Record on HDD Group field and select the number of the group you just created (Group 2).



- viii. Check the boxes for the cameras you want to add to the group.
- ix. Click **Apply**.
- x. Repeat steps **h.i.** through **h.ix.** above to create additional groups to unassigned HDDs as needed.

11.4 HDD Maintenance

The **HDD Detect** feature provides two methods of monitoring the HDD: display of **S.M.A.R.T.** (Self-Monitoring, Analysis and Reporting Technology) data, and **Bad Sector Detection**. These methods can be used to assure the normal functioning of the disk, and anticipate failures.

11.4.1 S.M.A.R.T. Display

1. Open the S.M.A.R.T. display menu. Go to **Menu | System Maintenance | HDD Detect**.

SECTION 11: MANAGING HDDs (WITHOUT RAID)

The screenshot shows the 'System Maintenance' interface. On the left is a navigation menu with options: System Info, Log Information, Import/Export, Upgrade, Default, Net Detect, HDD Detect (selected), and Live View. The main area is titled 'S.M.A.R.T. Settings' and 'Bad Sector Detection'. It contains several fields: 'HDD' (set to 1), 'Self-test Status' (Not tested), 'Self-test Type' (Short Test), and 'S.M.A.R.T.' (with a play icon). Below these are two rows of evaluation results: 'Temperature' (34) with 'Self-evaluation' (Pass) and 'Power On (da...)' (46) with 'All-evaluation' (Functional). The 'S.M.A.R.T. Information' section contains a table with the following data:

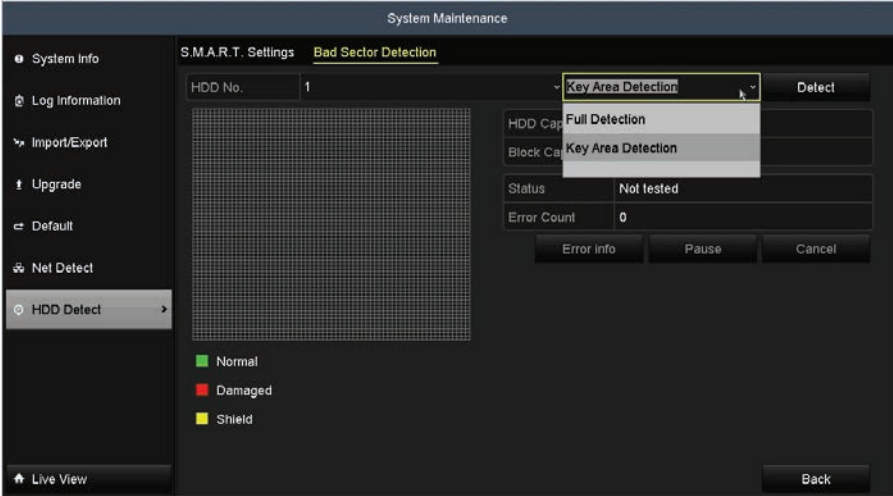
ID	Attribute Name	Status	Flags	Threshold	Value	Worst	Raw Value
0x1	Raw Read Error Rate	OK	b	16	100	100	0
0x2	Throughput Performance	OK	5	54	131	131	116
0x3	Spin Up Time	OK	7	24	206	206	38671155588
0x4	Start/Stop Count	OK	12	0	100	100	99

- To execute a self-evaluation test on an HDD:
 - On the **HDD** line, open the drop down list to select the HDD of interest.
 - On the **Self-test Type** line, open the drop down list to select the type of test to execute. You can choose either Short Test, Expanded Test or Conveyance Test.
 - Click the icon on the **S.M.A.R.T.** line to execute the test. Allow the test to complete before continuing. The result of the test is shown on the Self-evaluation line.
- Examine the S.M.A.R.T. data provided for the HDD. Check to ensure that the data in the value and Worst column does not exceed the data in the Threshold column.

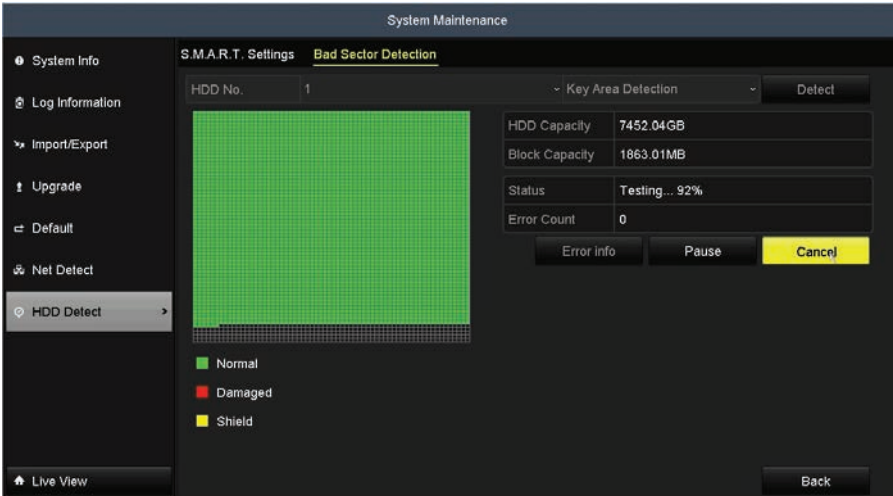
NOTE *S.M.A.R.T. data provided by each HDD manufacturer is usually different. Refer to the manufacturer's website for S.M.A.R.T. data definitions.*

11.4.2 Bad Sector Detection

- Open the Bad Sector Detection menu. Go to **Menu | System Maintenance | HDD Detect | Bad Sector Detection**.
- On the **HDD No.** line, open the drop down list and select the number of the HDD you want to test.
- Open the drop down list to the right of the HDD number, and then select either **Key Area Detection** or **Full Detection**. Key Area Detection will execute an abbreviated surface analysis test of the HDD.



4. Click the **Detect** button to start the detection. Bad sectors are identified in the array as red colored cells.



Click **Pause** to temporarily stop the scan, and click **Cancel** to end the scan.

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

SECTION 12

RAID Arrays

RAID (redundant array of independent disks) is a storage technology that combines multiple disk drive components into a logical unit. A RAID array stores data over multiple hard disk drives to provide enough redundancy so that data can be recovered if one disk fails. The NVR supports RAID types 0, 1, 5, 6 and 10. When a RAID array is created, all data on the HDDs is lost, and the system must be restarted.

The NVR provides two ways for creating the virtual disk, including one-touch configuration, for creating a RAID 5 array, and manual configuration, where you can select a different RAID level and specify the HDD configuration.

NOTE

- The NVR supports creating at most 8 virtual disks.
- At least 2 HDDs must be installed for RAID 0.
- At least 2 HDDs must be installed for RAID 1.
- At least 3 HDDs must be installed for RAID 5. If you install 4 HDDs or above for one-touch configuration, a hot spare disk will be set as default.
- At least 4 HDDs must be installed for RAID 6.
- 4/6/8 HDDs must be installed for RAID 10.
- By default, one-touch configuration creates one array and one virtual disk. If the capacity of the array created by one-touch configuration is larger than 16TB, two arrays and two virtual disks will be created.
- By default, one-touch configuration adopts "foreground" initialization (recommended) to initialize the virtual disk. By using foreground initialization, the virtual disk can be used only after the initialization is complete.

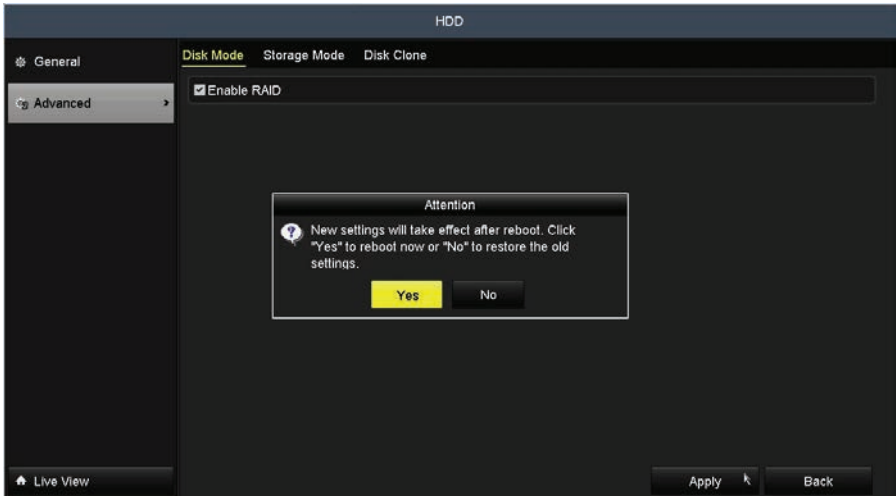
12.1 Create a RAID array

1. With a system without a RAID array, or with HDDs installed in the chassis that are not configured for RAID, open the **Menu | HDD | General** display. Verify that the drives you want to configure for RAID have "**Normal**" or "**Sleeping**" status.

The screenshot shows the 'HDD' configuration window with the 'HDD Information' tab selected. A table lists four drives with their respective properties and status.

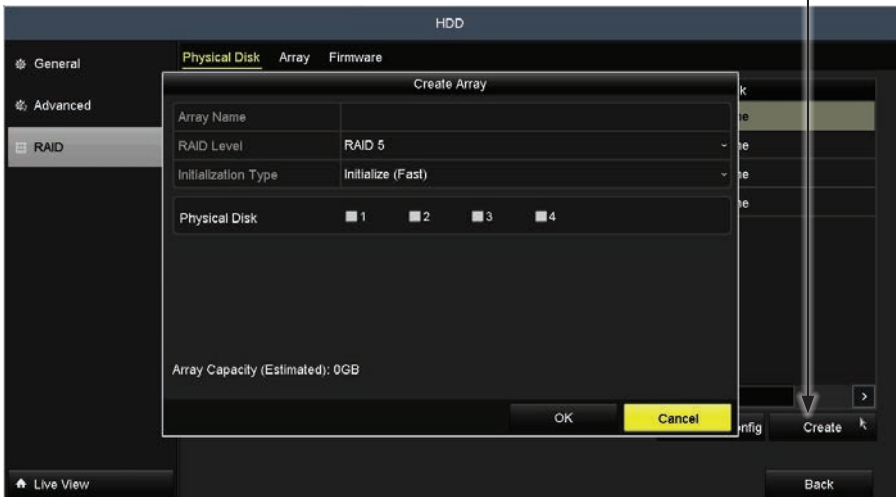
Label	Capacity	Status	Property	Type	Free Space	Gr...	Edit	Delete
1	7452.04GB	Normal	R/W	Local	7447.00GB	1	[Edit]	[Delete]
2	7452.04GB	Sleeping	R/W	Local	7451.00GB	1	[Edit]	[Delete]
3	7452.04GB	Sleeping	R/W	Local	7451.00GB	1	[Edit]	[Delete]
4	7452.04GB	Sleeping	R/W	Local	7451.00GB	1	[Edit]	[Delete]

2. Click the **Advanced** tab, check the box to **Enable RAID**, and then click the **Apply** button at the bottom of the menu.



3. In the pop-up window, click **YES** to reboot the system.
4. After the NVR reboots, open the **MENU | HDD | RAID** menu.
5. Click the **Create** button at the bottom of the screen. NOTE: You can click One-touch Config to create the array automatically.

Click Create (Array)



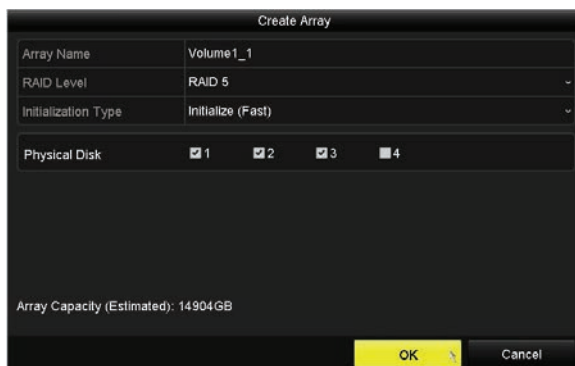
SECTION 12: RAID ARRAYS

6. In the pop-up **Create Array** window:

- a. Click inside the Name field, and then enter a name for the array. In this example, the array was named **Volume1_2**.



- b. Open the RAID Level drop-down list, and then click the kind of RAID you want to create.
- c. The **Initialization Type** defaults to Fast here. Other options are available with some arrays.
 - * **Background:** The background initialization can synchronize the disks, and detect and repair bad sectors. During the background initialization, the virtual disk is allowed to be used.
 - * **Foreground** (recommended): During foreground initialization, the RAID is initialized totally and bad disk sectors can be detected and repaired. The virtual disk can be used only after the initialization completes.
 - * **Fast:** The fast initialization usually takes short time and only initializes part of the RAID. It cannot detect a bad sector.
- d. Check the boxes for the drives that will become part of the array. For RAID 5 configurations, a minimum of three HDDs are needed.
- e. Click **OK** to create the RAID array.



- f. Open the **Menu | HDD | RAID | Array** display to view the **Task** field. Allow the RAID initialization to complete before continuing. See below.



Task status while RAID is initializing.

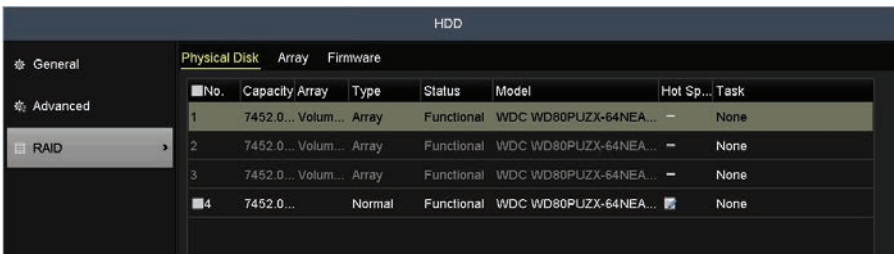


Task status when RAID initialization is complete

12.1.1 Installing a Hot Spare disk

To install a hot spare:

1. Select a disk with the same capacity as the disks in the RAID configuration, and then attach the disk mounting handles (see the Quick Start Guide provided with your recorder).
2. Insert the spare HDD into the chassis. In the example below, the spare HDD was installed in bay 4. The status of the HDD is shown on the **MENU | HDD | RAID** display.

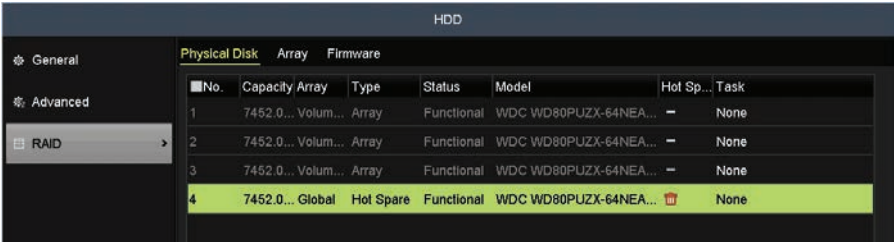


Physical disk configuration with a spare HDD installed

SECTION 12: RAID ARRAYS

NOTE After installing a spare HDD in the chassis, it may need to be initialized before it is used.

- Click the “Edit” (🔧) icon in the Hot Spare column for the spare disk that was installed (here in slot 4). In the screen capture shown below, notice that the **Type** of the spare disk changed from **Normal** to **Hot Spare**, and the icon in the Hot Spare column changed to the **Delete** (🗑️) icon.



HDD							
Physical Disk Array Firmware							
No.	Capacity	Array	Type	Status	Model	Hot Sp...	Task
1	7452.0...	Volum...	Array	Functional	WDC WD80PUZX-64NEA...	—	None
2	7452.0...	Volum...	Array	Functional	WDC WD80PUZX-64NEA...	—	None
3	7452.0...	Volum...	Array	Functional	WDC WD80PUZX-64NEA...	—	None
4	7452.0...	Global	Hot Spare	Functional	WDC WD80PUZX-64NEA...	🗑️	None

The Hot Spare disk is now ready for use.

12.2 Rebuilding a RAID array (example)

The Status of an array can be any of the following:

- Functional:** There is no disk loss in the array.
- Degraded:** The number of lost disks has exceeded the limit. When the virtual disk is in Degraded status, you can restore it to Functional status by rebuilding the array.
- Offline:** All other conditions. When the Status is neither Degraded nor Functional, it is considered Offline.

The Status of the array is shown in the **MENU | HDD | Array** display.



HDD									
Physical Disk Array Firmware									
No.	Name	Free Space	Physical ...	Hot Sp...	Status	Level	Rebu...	Delete	Task
1	test2	3725/3725G	1 2 3	4	Functional	RAID 5	🔧	🗑️	None

Arrays are automatically rebuilt when the array status is Degraded and a Hot Spare HDD is installed in the system.

12.2.1 Rebuilding array process - example

When the chassis is configured with a Hot Spare disk and the array is in **Degraded** status, the system will rebuild the array using the Hot Spare disk. To prepare for automatic rebuilding of the array, the system was configured as shown below, with a Global Hot Spare disk installed in physical slot 4. To configure a Hot Spare, see “12.1.1 Installing a Hot Spare disk” on page 209.

HDD						
General						
Physical Disk						
Advanced						
RAID						
No.	Capacity	Array	Type	Status	Model	Hot Spare
1	1,863GB	test2	Array	Functional	WDC WD20PURX-64P6Z...	—
2	1,863GB	test2	Array	Functional	WDC WD20PURX-64P6Z...	—
3	1,863GB	test2	Array	Functional	WDC WD20PURX-64P6Z...	—
4	1,863GB	Global	Hot Spare	Functional	WDC WD20PURX-64P6Z...	🔥

In the example below, physical disk 2 was lost. The **Menu | HDD | RAID | Physical disk** display appeared as shown below.

HDD						
General						
Physical Disk						
Advanced						
RAID						
No.	Capacity	Array	Type	Status	Model	Hot Spare
1	1,863GB	test2	Array	Functional	WDC WD20PURX-64P6Z...	—
3	1,863GB	test2	Array	Functional	WDC WD20PURX-64P6Z...	—
4	1,863GB	Global	Hot Spare	Functional	WDC WD20PURX-64P6Z...	🔥

As a result of the lost disk 2 in the array, the Status of the array lowered to **Degraded** is shown in the **MENU | HDD | Array** display.

HDD							
General							
Physical Disk							
Advanced							
RAID							
No.	Name	Free Space	Physical ...	Hot Sp...	Status	Level	Rebu... Delete Task
1	test2	3725/3725G	1 4 3		Degraded	RAID 5	Rebuild(Running) 0%

Notice that the current array Task is **Rebuilding**. Rebuilding the array is a background task.



Allow the rebuilding task to complete before powering off the system. Depending on the size of the HDDs, this process can last several hours.

SECTION 13

Remote Access

If your NVR is connected to a local network (LAN), you can access it from another computer on the LAN through Microsoft® Internet Explorer® (IE). IE must be configured to run in Administrator mode to use all features of the web interface.

When connecting to the NVR, you must enter a User Name and Password. Note that some user permissions disallow remote access and/or features of this access method.

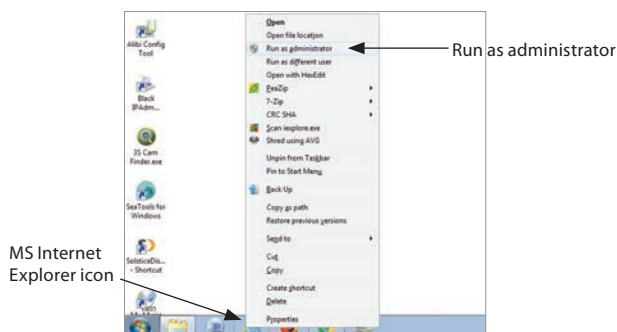
When logging into the NVR from a remote computer for the first time, you must install a plug-in program named WebComponents. The procedure for installing the program using IE 11 is shown below. Subsequent log ins do not require you to reinstall WebComponents.

13.1 Configure IE to run in Administrator mode

You can configure IE to run in Windows 7 and Windows 10. The procedures are different.

Window 7: To run IE as an Administrator:

1. Find or create an IE icon on your computer desktop.
2. Hold down the shift key, and then right-click on the IE icon.

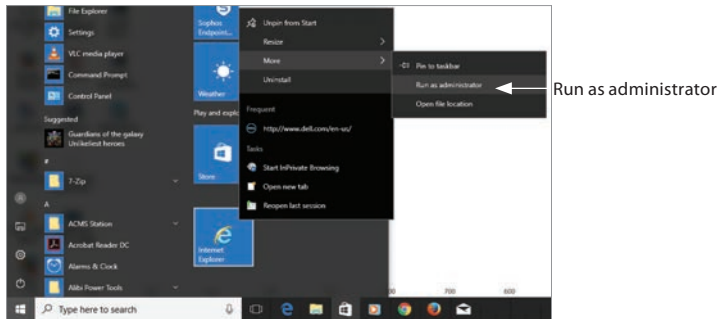


3. Click **Run as administrator** in the pop-up menu.

Window 10: To run IE as an Administrator:

1. Find IE in the start menu. Usually this is found in the **Windows Accessories** group.
2. Pin the entry to **Start**.

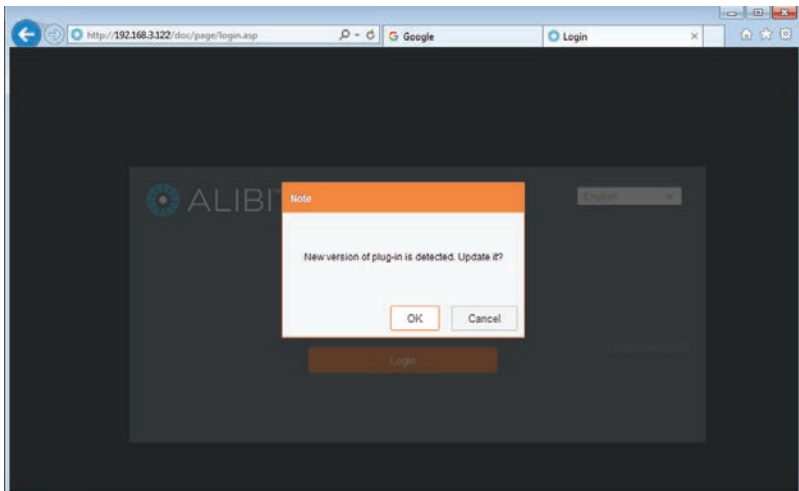
- Right click on the Internet Explorer tile, and then select **More | Run as administrator**.



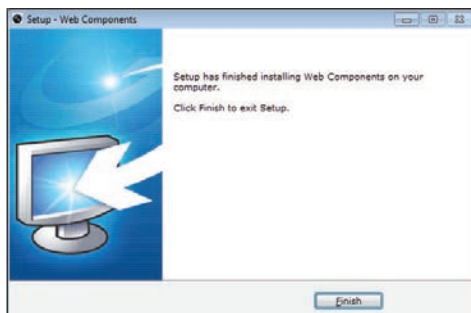
13.2 Login

To access the NVR from a computer on the LAN:

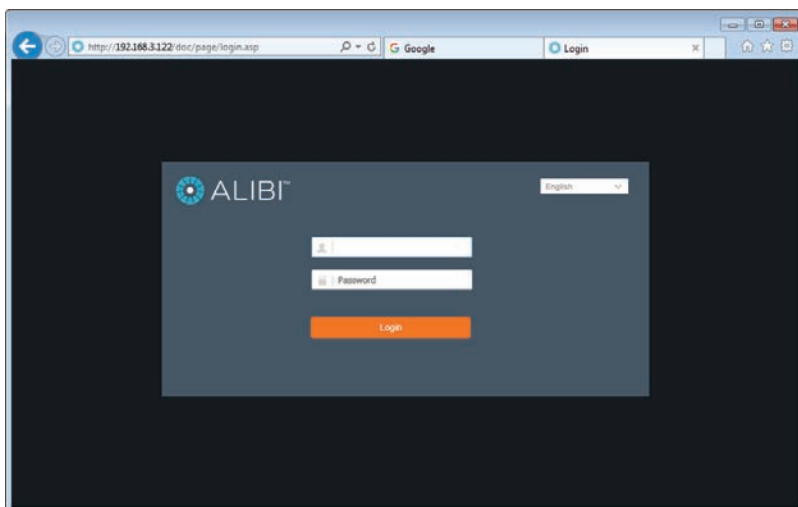
- Open an Internet browser on your remote compute and enter the IP address of the NVR in the URL field. In the example below, the IP address of the NVR is 192.168.2.122. If this is the first time you log into an Alibi recorder with this version of firmware, the following screen will appear, requiring you to install a plugin. If not, go to step 3 below.



- If the screen above appears, click OK, close the browser, and follow the on-screen instructions to install the plugin. When the plugin is successfully installed, the following screen will open.



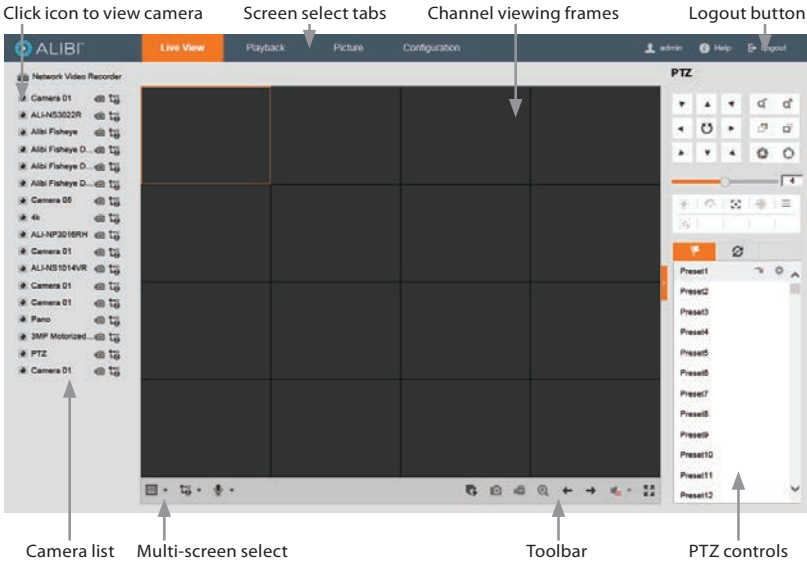
3. In the screen above, click **Finish**.
4. Reopen **Internet Explorer** and then enter the IP address of the recorder in the URL field.



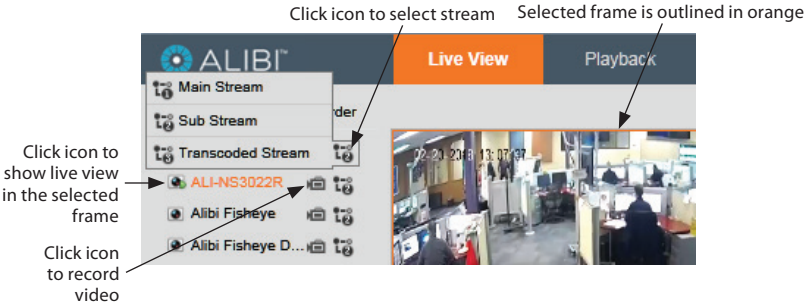
5. In the Login screen shown above, enter your *admin* username and password, and then click **Login**. A **Live View** window will open.

13.3 Live View screen

The Live View window initially appears in a multi-screen configuration with no live view images shown. The display lists only the cameras configured in the NVR. In this tab, you can change the viewing screen layout by clicking the multi-screen select button and selecting the icon for a 1 screen a 2 x 2 layout, or other layouts depending on how many channels the recorder supports.



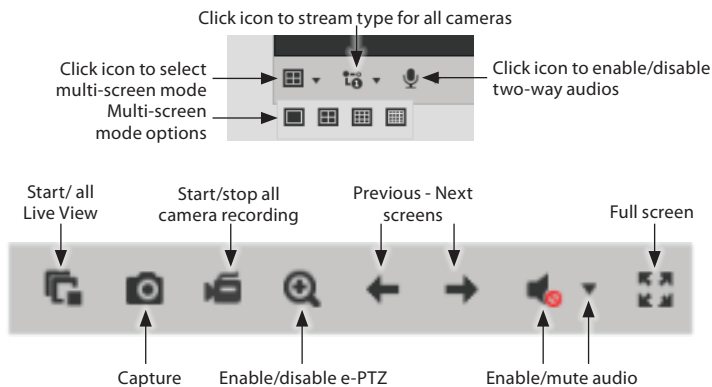
Screen icons



NOTE

The NVR has the ability to create a **Transcoded stream** to help show live video in bandwidth constrained environments. You can configure a Transcoded stream option in the web client **Configuration | Video/Audio** menu. By default it is set to **Auto** negotiate the resolution, causing the NVR to determine if the network resources are large enough to show full resolution and frame rate video. If not, the NVR will auto adjust down both to ensure the stream is delivered OK.

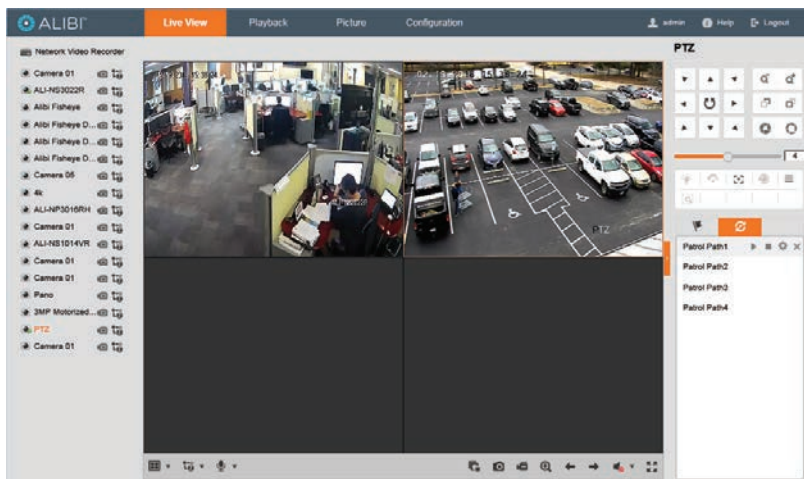
SECTION 13: REMOTE ACCESS



For **PTZ controls**, refer to “5.1 PTZ Control Panel” on page 50.

To view video from a camera in the Live View screen:

- Click a viewing frame to select it. When selected, the frame is surrounded by a bright box.
- Double click the camera channel you want to see.



- To expand the image to full frame, double click the image in the viewing frame. To return to normal viewing mode, press **ESC** (keyboard escape key).

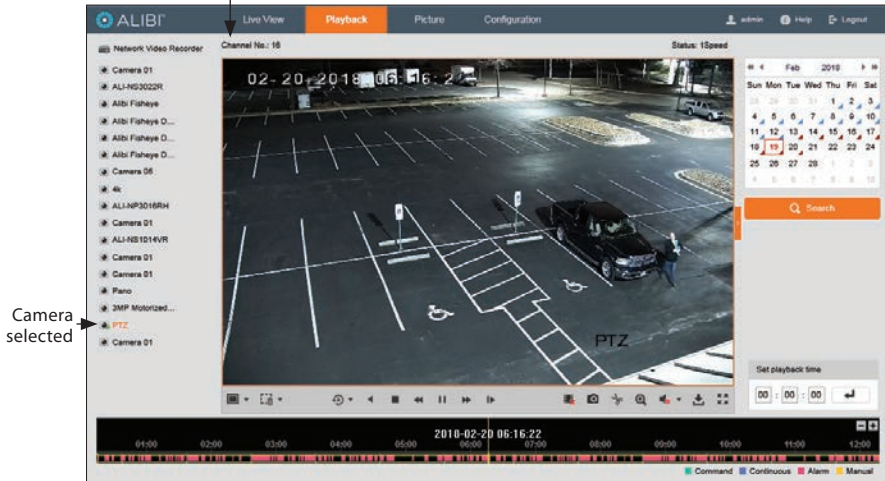
Help

This feature is not available in this release.

13.4 Playback screen

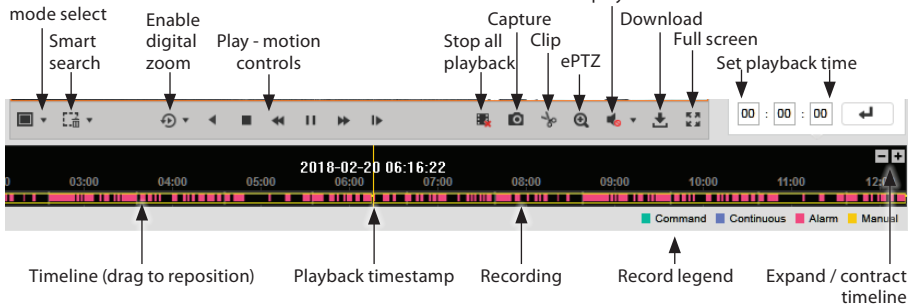
Open the Playback screen by clicking **Playback** in the screen header. The Playback screen allows you to review video recorded from one camera or several cameras concurrently. Also, video can be downloaded to your local computer.

Camera channel selected



Multi-screen mode select

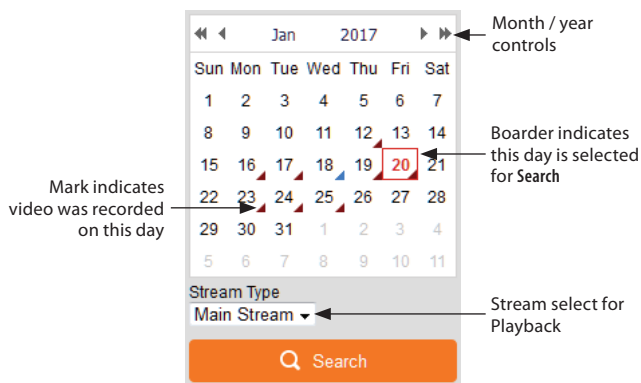
Audio play / mute



SECTION 13: REMOTE ACCESS

To playback recorded video:

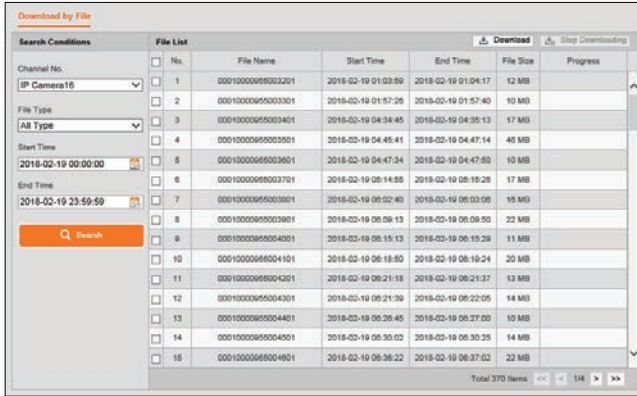
1. Click the multi-screen mode button to select the number of viewing frames you need to display. You can select either a 1, 2 x 2, or 3 x 3 frame pattern, depending on the number of channels in the NVR you are using.
2. In the left frame, click the camera channel you want to play recorded video from. In the example above, *Camera 16* was selected.
3. In the right frame, click the date when the video was recorded, then click the **Search** button. In the example above, February 19, 2018 was selected.



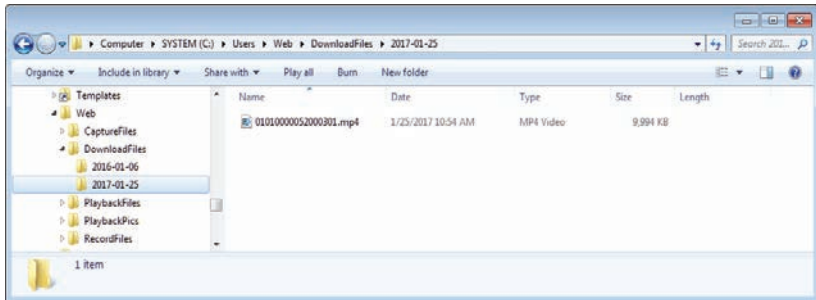
4. At the bottom of the screen, drag the timeline left or right to find when video was recorded for the camera selected. The condition that caused video to be recorded is indicated by a colored band on the timeline. The color legend is shown at the lower right corner of the window.
5. Click the **Play** button to begin playing video.

To Download recorded video:

1. Click the **Download** icon.

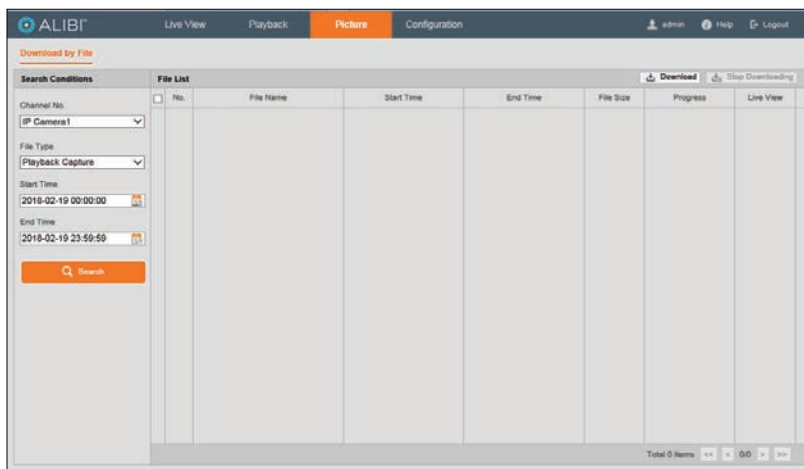


2. Check the box of the video segment you want to download.
3. Click the **Download** button at the top of the window. Download status is shown in the **Progress** column. Downloaded files are saved in the location shown on the **Configuration | Local** screen (see "13.4 Playback screen" on page 217). Allow the download to complete before closing the browser.



13.5 Picture screen

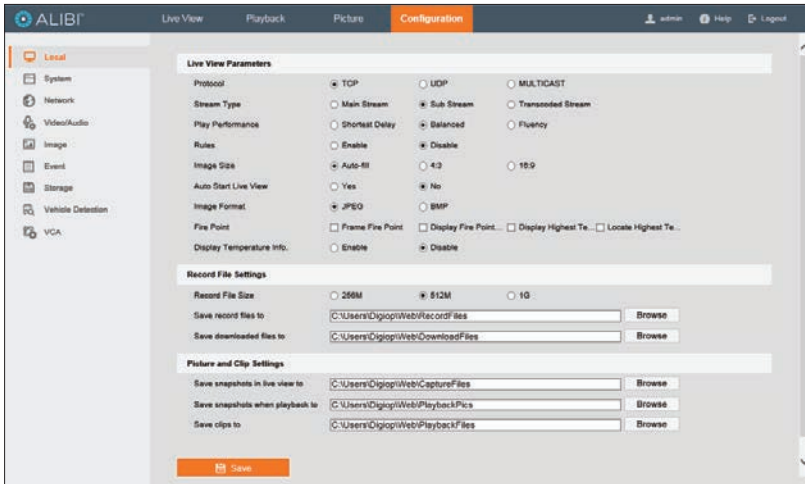
Open the Picture screen by clicking **Picture** in the screen header. The Picture screen allows you to search for, review and download capture files. It functions very similar to the Playback Download screen.



13.6 Configuration screen

Open the Configuration screen by clicking **Configuration** in the screen header. The Configuration menu enables you to view the NVR configuration and make configuration changes. The User Name you use to login to the NVR must have administrative privileges to change the NVR configuration.

Options in the configuration menu are identical to those in the embedded NVR **Menu** system. For more information on how to use these options, refer to the NVR **Menu** descriptions in previous sections of this manual. After making configuration changes click **Save** to apply your changes.



The location of local files (captures and downloads) are specified on the **Configuration | Local** screen. See above.

NOTE

The NVR has the ability to create a **Transcoded stream** to help show live video in bandwidth constrained environments. You can configure a Transcoded stream option in the web client Configuration | Video/Audio menu. By default it is set to **Auto** negotiate the resolution, meaning that the NVR will determine if the network resources are large enough to show full resolution and frame rate video. If not, the NVR will auto adjust down both to ensure the stream is delivered OK.

13.6.1 Log information

Open the Log screen by clicking **Configuration | System | Maintenance | Log**.

SECTION 13: REMOTE ACCESS

The screenshot displays the ALIBI Configuration interface. The top navigation bar includes 'Live View', 'Playback', 'Picture', and 'Configuration' tabs. The left sidebar contains a navigation menu with categories like Local, System, Maintenance, Security, Camera Management, User Management, Network, Video/Audio, Image, Event, Storage, Vehicle Detection, and VCA. The main content area is titled 'Upgrade & Maintenance' and 'Log'. It features search filters for 'Major Type' and 'Minor Type' (both set to 'All Types'), 'Start Time' (2018-02-19 00:00:00), and 'End Time' (2018-02-19 23:59:59). A 'Search' button is present. Below the filters is a 'Log List' table with columns: No, Time, Major Type, Minor Type, Channel No., Local/Remote User, and Remote Host IP. The table contains 12 rows of log entries. An 'Export' button is located to the right of the table. At the bottom right of the table, it says 'Total 2000 items' with navigation arrows.

No	Time	Major Type	Minor Type	Channel No.	Local/Remote User	Remote Host IP
1	2018-02-19 00:00:04	Alarm	Stop Motion Detection	D14		
2	2018-02-19 00:00:08	Information	Stop Record	D14		
3	2018-02-19 00:00:57	Alarm	Start Motion Detection	D3		
4	2018-02-19 00:00:57	Information	Start Record	D2		
5	2018-02-19 00:01:09	Alarm	Start Motion Detection	D13		
6	2018-02-19 00:01:08	Information	Start Record	D13		
7	2018-02-19 00:01:08	Alarm	Start Motion Detection	D12		
8	2018-02-19 00:01:08	Information	Start Record	D13		
9	2018-02-19 00:01:10	Alarm	Stop Motion Detection	D2		
10	2018-02-19 00:01:14	Information	Stop Record	D2		
11	2018-02-19 00:01:20	Alarm	Stop Motion Detection	D13		
12	2018-02-19 00:01:24	Information	Stop Record	D13		

The NVR log report is created by specifying a search criteria using the options at the top of the window, and then clicking the **Search** button. The search criteria menu includes filters to search for Major and Minor type events, and specify the start and end time of the report. Log reports can be saved in either text or Excel formats by clicking the **Save Log** icon.

APPENDIX A 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 NVR, with the main stream having a maximum resolution of the camera and the sub-stream favoring zero-latency encoding.

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: 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.

NTP: Network Time Protocol. A protocol designed to synchronize the clocks of computers over a network.

NVR: 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 NVRs.

PTZ: Pan, Tilt, Zoom. PTZ cameras are motor driven systems that allow the camera to pan left and right, tilt up and down and zoom in and out.

USB: Universal Serial Bus. USB is a plug-and-play serial bus standard to interface devices to a host computer.

