

ALIBI™ Embedded Network Video Recorder Firmware V4.1.50 User Manual

Products: ALI-NVR3308P, ALI-NVR3316P, ALI-NVR5216P, ALI-NVR5232P, ALI-5316P, ALI-NVR7132R and ALI-NVR7164R recorders



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 embedded Network Video Recorders (NVRs) with firmware version V4.1.50.

Navigation in the firmware is represented by the expression: “**Menu | Configuration | Network | TCP/IP**”, which means:

- a. Click the **Menu** icon in the upper left corner of the Live View display to open the Menu screen.
- b. In the Menu screen, click the **Configuration** icon.
- c. In the Configuration menu, click the **Network** entry in the left frame.
- d. Click **TCP/IP**. TCP/IP may be a submenu under Network, or a 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 | Maintenance | System Info | Device Information** screen and find **Firmware Version**.

Some features described herein may apply to some NVRs but not to other models. For specific information about the features and capabilities of your ALIBI NVR, please contact your vendor.

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 keyboard	4
SECTION 2	Basic System Setup	6
	2.1 System activation	6
	2.2 Using the setup Wizard	8
	2.3 PoE channel configuration	13
	2.4 Basic camera setup	15
	2.5 Customize camera configurations	16
	2.5.1 Camera OSD setup	17
	2.5.2 Camera Image Settings	19
	2.5.3 Camera Exposure setup	19
	2.5.4 Camera Day/Night Switch	20
	2.5.5 Camera Backlight setup	21
	2.5.6 Camera Image Enhancement	22
	2.5.7 Camera White Balance adjustment	22
	2.5.8 Camera Privacy Mask	23
	2.5.9 Camera Video Parameters	24
	2.5.10 PTZ camera setup	26
SECTION 3	Event setup	27
	3.1 Normal Event Setup	28
	3.1.1 Camera Motion Detection	29
	3.1.2 Camera Video Tampering	32
	3.1.3 Camera Video Loss	33
	3.1.4 Alarm Input detection	34
	3.1.5 Alarm Output configuration	36
	3.1.6 Exception reporting	38
	3.2 Smart Event Setup	39
	3.2.1 Camera Face Detection	40
	3.2.2 Line Crossing detection	43
	3.2.3 Camera Intrusion Detection	44
	3.2.4 Region Entrance Detection	46
	3.2.5 Camera Region Exiting Detection	48
	3.2.6 Camera Unattended Baggage	50

TABLE OF CONTENTS

	3.2.7	Camera Object Removal Detection	52
	3.2.8	Camera Audio Exception Condition	54
	3.2.9	Camera Defocus Detection	56
	3.2.10	Camera Sudden Scene Change Detection	57
SECTION 4		Startup, Shutdown, Reboot	60
	4.1	Starting Up	60
	4.2	Shutdown	61
	4.3	Reboot	62
SECTION 5		Live View Screen	63
	5.1	Live View utility display	63
	5.1.1	Open Menu screen	64
	5.1.2	View alarm information	64
	5.2	Setting monitor resolution	66
	5.3	Live View settings	67
	5.4	Live View Status icons	69
	5.5	Quick Setting Toolbar	70
	5.6	Channel-Zero Encoding	71
	5.7	Adding network cameras	72
	5.7.1	Custom Add IP Camera	74
SECTION 6		PTZ Controls	77
	6.1	PTZ Control screen	78
	6.1.1	Pointing the camera	79
	6.1.2	PTZ Control panel	79
	6.1.3	Zoom - Preset quick controls	80
	6.2	Configuring PTZ settings	81
	6.2.1	Setting Presets	82
	6.2.2	Setting patrols	83
	6.2.3	Setting a pattern	85
	6.2.4	Configure Linear Scan	86
	6.3	PTZ Parameter Settings	87
SECTION 7		Point of Sale Integration	88
	7.1	Assign POS data to a camera	88
	7.2	Configure the POS interface	89
	7.3	Playback POS recordings	95
SECTION 8		Record, Playback and Video Backup	97

	8.1	Configuring record settings	97
	8.1.1	Setting camera video parameters	97
	8.2	Configuring Record schedule	99
	8.3	Configuring Capture schedule	104
	8.4	Defining Holidays	108
	8.5	Record Advanced settings for eSATA port	110
	8.6	Playback	111
	8.6.1	Instant playback by channel	111
	8.6.2	Using the Playback screen	113
	8.6.3	Normal Playback	115
	8.6.4	Smart Playback	117
	8.6.5	Custom Playback	118
	8.7	File Management - search and export	132
	8.7.1	File Management - All Files	132
	8.7.2	File Management - Human Files	139
	8.7.3	File Management - Vehicle Files	140
SECTION 9		Managing User Accounts	141
	9.1	Adding a user account	141
	9.2	Live View Permissions on Lock screen	145
	9.3	Deleting a user account	145
	9.4	Editing a user account	146
	9.4.1	Modify <i>admin</i> user	147
SECTION 10		Network Settings	148
	10.1	Configuring General Network Settings	148
	10.2	Configuring Advanced Settings	149
	10.2.1	Platform Access setup	149
	10.2.2	Configuring DDNS	151
	10.2.3	Configuring NTP Server	152
	10.2.4	Configuring Remote Alarm Host	153
	10.2.5	Configuring Email	154
	10.2.6	Configuring UPnP™	156
SECTION 11		System Maintenance	157
	11.1	System Information	157
	11.2	Search Log Information, Log Export	157
	11.2.1	Log Search	157

TABLE OF CONTENTS

	11.2.2 Log Export	160
	11.3 Export system configuration	162
	11.4 Import system configuration	163
	11.5 Upgrade Firmware	164
	11.5.1 Upgrade from FTP server	165
	11.6 Default - restore NVR	166
	11.7 Net Detect	167
	11.7.1 Checking Network Traffic	167
	11.7.2 Testing Network Delay and Packet Loss	167
	11.7.3 Exporting Network Packet	168
	11.7.4 Checking the network status	169
	11.7.5 Checking Network Statistics	169
	11.7.6 HDD - S.M.A.R.T. testing and monitoring	170
	11.7.7 HDD - Bad Sector Detection	171
	11.8 HDD Disk Clone	172
	11.9 System Service options	173
	11.9.1 System Service	173
	11.9.2 ONVIF	174
	11.9.3 Stream Encryption	175
	11.9.4 More Settings	176
SECTION 12	Managing HDDs	179
	12.1 Initializing HDDs	179
	12.2 Adding network HDDs to the system	180
	12.2.1 For a NAS disk	180
	12.2.2 For an IP SAN disk:	181
	12.3 Configuring the HDD Partition / Group mode	182
	12.3.1 Partition Mode recording	182
	12.3.2 Group Mode recording	183
	12.3.3 Change from Group Mode recording to Partition Mode	185
SECTION 13	RAID Arrays (RAID capable recorders only)	187
	13.1 Creating a RAID array	187
	13.2 Rebuilding a RAID array	190
	13.2.1 Installing a Hot Spare disk	191
	13.2.2 Array Rebuilding process	192

SECTION 14	Remote Access	193
	14.1 Using IE to login to the NVR	193
	14.1.1 Configure IE to run in Administrator mode	193
	14.1.2 Login with IE	194
	14.2 Using Firefox or Chrome to login to the NVR	195
	14.3 Live View screen	196
	14.4 Playback tab	198
	14.5 Picture tab	201
	14.6 Configuration tab	202
	14.6.1 Log information	202
	14.7 Logout	204
APPENDIX A	Glossary	205
APPENDIX B	Long Distance (Extended) PoE Power	206
APPENDIX C	Troubleshooting	207

NOTES

SECTION 1

Systems Overview

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

General

- Connectable to network cameras, network dome and encoders
- Connectable to the third-party network cameras like Acti, Arecont, Axis, Bosch, Brickcom, Canon, Panasonic, Pelco, Samsung, Sanyo, Sony, Vivotek and Zavio, and cameras that adopt ONVIF or PSIA protocol
- Connectable to smart IP cameras
- H.265+ / H.265 / H.264+ / H.264 / MPEG4 video formats
- PAL / NTSC adaptive video inputs
- Each channel supports dual-stream
- Up to 8 / 16 / 32 / 64 network cameras can be added according to model
- Independent configuration for each channel, including resolution, frame rate, bit rate, image quality, etc.
- The quality of the input and output record is configurable

Local Monitoring

- HDMI / VGA1 and HDMI2 outputs provided
- HDMI video output at up to 4K resolution
- Multi-screen display in live view is supported, and the display sequence of channels is adjustable
- Live view screen can be switched in groups. Manual switch and auto-switch are provided and the auto-switch interval is configurable
- Custom window-division live view layout configuration
- 3D positioning in live view
- Configurable main stream and sub-stream for the live view
- Quick setting menu is provided for live view
- POS information overlay on live view
- Motion detection, video tampering, video exception alert and video loss alert functions
- Privacy mask
- Multiple PTZ protocols supported; PTZ preset, patrol and pattern
- Zooming in by clicking the mouse and PTZ tracing by dragging mouse

HDD Management

- Up to 16 SATA hard disks and 1 eSATA disk can be connected for some recorders
- Up to 8 TB storage capacity for each disk supported (refer to the specifications for your recorder for hardware capabilities)
- 8 network disks (NAS / IP SAN disk)
- S.M.A.R.T. and bad sector detection
- HDD group management

- Supports HDD standby function
- HDD property: redundancy, read-only, read / write (R / W)
- HDD quota management; different capacities can be assigned to different channels
- RAID 0, RAID 1, RAID 5, RAID 6 and RAID 10 are supported
- Hot-swappable RAID storage scheme can be enabled and disabled upon demand for some recorders. Up to 16 arrays can be configured
- Disk clone to the eSATA disk
- HDD health monitoring

Recording, Capture and Playback

- Holiday recording schedule configuration
- Continuous and event video recording parameters
- Multiple recording types: manual, continuous, alarm, motion, motion | alarm, motion & alarm VCA, and POS
- Eight recording time periods with separated recording types
- POS information overlay on image
- Pre-record and post-record for alarm, motion detection for recording, and pre-record time for schedule and manual recording
- Searching record files and captured pictures by events (alarm input / motion detection)
- Tag adding for record files, searching and playing back by tags
- Locking and unlocking record files
- Local redundant recording and capture
- Normal / Smart / custom video playback mode
- Playback by video synopsis
- Searching and playing back record files by channel number, recording type, start time, end time, etc.
- Supports playback by main stream or sub stream
- Smart search for the selected area in the video
- Zooming in when playback
- Reverse playback of multi-channel
- Supports pause, play reverse, speed up, speed down, skip forward, and skip backward when playback, and locating by dragging the mouse
- Supports thumbnails view and fast view during playback
- Up to 16-ch synchronous playback at 1080p real time
- Supports playback by transcoded stream
- Manual capture, continuous capture of video images and playback of captured pictures
- Supports enabling H.264+ to ensure high video quality with lowered bitrate

Files Management

- Search and export vehicle detection files and human appearance files
- Export video data by USB, SATA or eSATA device
- Export video clips when playback
- 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 conflict, abnormal record / capture, HDD error, and HDD full, etc.
- POS triggered alarm
- VCA detection alarm is supported
- Smart analysis for people counting and heat map
- Connectable to the thermal network camera
- Alarm triggers full screen monitoring, audio alarm, notifying surveillance center, sending e-mail and alarm output
- Automatic restore when system is abnormal

Other Local Functions

- Operable by front panel, mouse, remote control, or control keyboard
- Three-level user management; admin user is allowed to create many operating accounts and define their operating permission, which includes the limit to access any channel
- Admin password resetting by exporting / importing a GUID file
- Operation, alarm, exceptions, and log recording and searching
- Manually triggering and clearing alarms
- Import and export device configuration information

Network Function

- Two self-adaptive 10M / 100M / 1000 Mbps network interfaces
- IPv6 is supported
- TCP/IP protocol, DHCP, DNS, DDNS, NTP, SADP, SMTP, NFS, and iSCSI are supported
- TCP, UDP and RTP for unicast
- Auto / Manual port mapping by UPnP
- Support access by Alibi Connect
- Remote Web browser access by HTTPS ensures high security
- ANR (Automatic Network Replenishment) function is supported, which enables the IP camera to save the recording files in the local storage when the network is disconnected, and synchronizes the files to the device when the network is resumed
- Remote reverse playback via RTSP
- Supports accessing the platform via ONVIF
- Remote search, playback, download, locking and unlocking of the record files, and supports downloading files upon 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 HDD formatting and program upgrading
- Remote system restart and shutdown
- RS-232, RS-485 transparent channel transmission

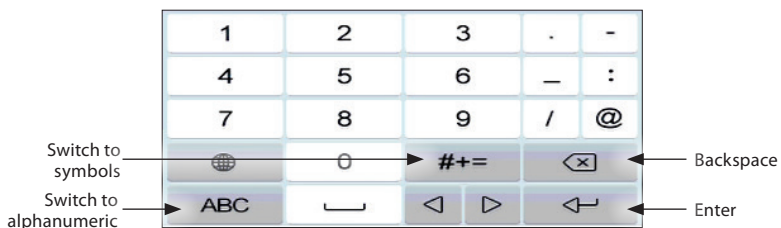
- Alarm and exception information can be sent to the remote host
- Remotely start / stop recording
- Remotely start / stop alarm output
- Remote PTZ control
- Remote JPEG capture
- Virtual host function to access and manage the IP camera directly
- Two-way audio and voice broadcasting
- Embedded Web server

1.1 Soft keyboard

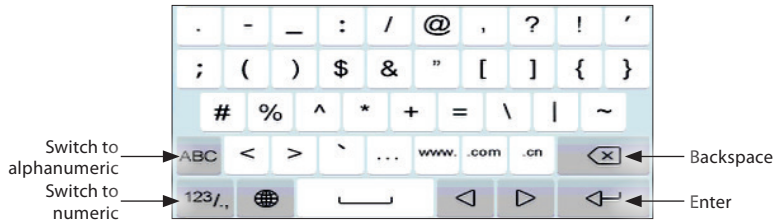
One of two on-screen keyboards appears when you click in a field that accepts a entry, such as a password or name or a numerical value. A third keyboard which includes symbols can also be opened while in the numeric keyboard. The alphanumeric keyboard is shown in the following picture. Some control keys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

Basic System Setup

When the NVR is first powered on, or reset to its Factory default configuration, it is in an “Inactive” state, which means that it is not it doesn’t have an *admin* user password for the recorder or cameras, and it is not configured to record video or log system status messages. The initial configuration screen enables you to activate the recorder.

After activating the recorder and configuring its security options, a configuration Wizard will open. The Wizard helps you to easily configure the recorder for its basic settings, including date and time, network configuration, network cameras, HDD initialization, etc.

After completing system setup with the Wizard, the recorder will record video continuously from all cameras. Additional configuration setup will allow you to customize the system for your needs and operate more efficiently.

2.1 System activation

1. Power on the NVR. Normally, an Alibi logo splash screen appears within 2 minutes. The following screen is used to activate the recorder.

In the screen above:

- a. Click on the **Create New Password** field, and then enter a unique password using the pop-up virtual keyboard. Follow the guidelines in the **Note** at the bottom of the screen. Always use a password that will produce a “**Strong**” rating (green indicator in the status bar).

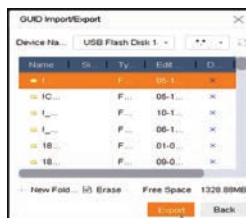
- b. Enter the same New Password in the **Confirm New Password** field.
 - c. Select or deselect the checkboxes to:
 - Export GUID:** This feature enables you to create a GUID file and save it to a flash drive for logging back into the NVR if you lose your *admin* password.
 - Enable Unlock Pattern:** This option allows you to login by dragging the mouse across a 3 x 3 matrix to quickly login to your admin account.
 - Security Question Configuration:** If you lose your password, this option enables you to login by responding correctly to security questions you setup.
 - d. Enter a password in the **Create Channel Default Password** field. This will become the default password of the *admin* user of cameras plugged into the internal switch on the backpanel of the NVR. Follow the guidelines in the **Note** below this field.
2. Click the **OK** button to continue. If passwords were setup properly in the **Activation** menu, a **Note** window will appear showing the NVR is now “activated.” Leave the **Note** window open.



3. If you selected options in the Activation screen for Export GUID, Unlock Pattern and Security Question, use the instructions in this step to configure those features.

Export GUID: If you selected this option, plug a flash drive into an unused USB port on the recorder, and then click **OK** in the **Note** window (see above).

- a. In the **GUID Import/Export** window, open the **Device Name** drop down list and then select the device you where you want to save the GUID file. If a list of directories appear, click on the directory you prefer (in the window shown below, the first directory was selected), and then click **Export**. Some options will appear at the bottom of the screen to manage the storage device.

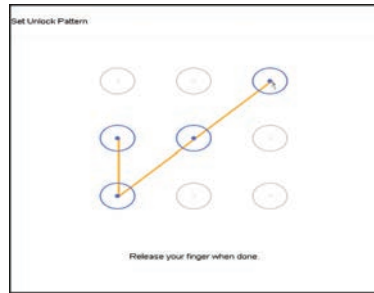
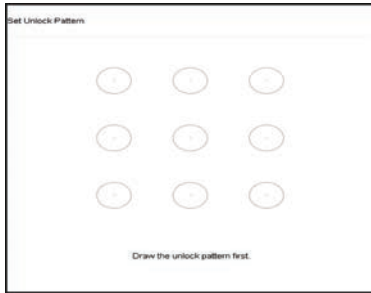


SECTION 2: BASIC SYSTEM SETUP

- b. After the export operation completes, remove the flash drive from the NVR and store it in a secure location.

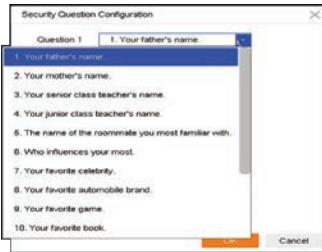
Enable Unlock Pattern: If you selected this option and the **Note** window shown above is still open, click **OK** to close the **Note** window. Then:

- a. Drag the mouse over four of the dots in the matrix shown below to construct an “Unlock” pattern (see right window below). Use this pattern to log into your NVR in the future as the *admin* user.



Security Question Configuration: If you selected this option and the **Note** window shown above is still open, click **OK** to close the **Note** window. Then:

- a. Open the drop down list in the **Question 1** field, and then select the question you want to use.



- b. Enter your answer to Question 1 in the **Answer 1** field.
- c. Repeat the same setup for **Question 2** and **Question 3**, and then click **OK**.
- d. Remember or write down the exact answers you entered, and then save it in a secure location.
- e. Click **OK** to save your configuration.

2.2 Using the setup Wizard

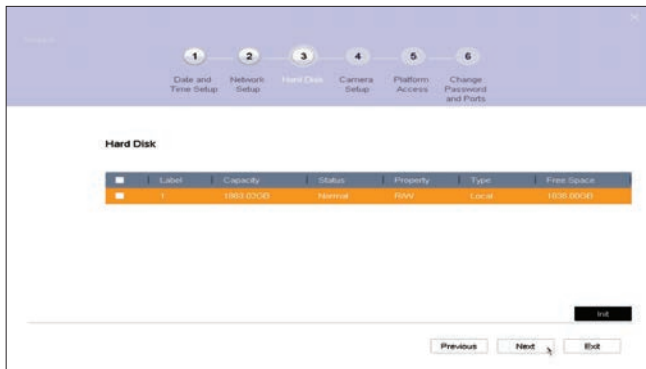
1. Next, the configuration Wizard **Date and Time Setup** menu will open. Since all recordings made by your surveillance system are time stamped, it is very important that the date and time is set precisely to produce valuable evidence from your recorder.

In the screen above:

- a. Select the local **Time Zone** and **Date Format** using the drop down menus.
 - b. Click the System Date field, and then click on the current date.
 - c. Click the **System Time** field, and then use the graphical interface for setting the current time. You can also check the **Enable NTP** box, and then enter the appropriate parameters in the fields below it to configure the recorder retrieve the precise time and date information from a timeserver on the Internet.
 - d. Click **Next** to save your settings and continue.
2. In the **Network Setup** Wizard window, click the field value you want to change, then use the pop-up aid to enter a new value. By default, the NVR uses DHCP (Dynamic Host Configuration Protocol) to acquire compatible (dynamic, changeable) network settings from a network DHCP server (usually a router). You can leave the settings on this menu unchanged, but it is configure the NVR with a fixed network settings to assure the NVR has an unchanging IP address, which is convenient for remote login.

SECTION 2: BASIC SYSTEM SETUP

- a. In the Wizard **2 Network Setup** window, nothing usually has to change in the left column. You can enter your preferred DNS server addresses (optional, ex. 8.8.8.8 and 8.8.4.4 [Google] DNSs) in the **Preferred ..** and **Alternate DNS** fields.
 - b. The column on the right shows that the **Enable DHCP** box is checked (by default) and the recorder acquired network settings from a DHCP server. These settings are compatible with your network and the other devices that share it. To enable fixed network settings, un-check the **Enable DHCP** box. Then you can either use the IPV4 parameters assigned by the DHCP server, or enter your preferred IPV4 parameters (IPV4 Address, IPV4 Subnet Mask, IPV4 Default Gateway).
NOTE: If you enter IPV4 parameters in the fields above, ensure that they do not conflict with other devices in the network.
 - c. Click **Next** to save your settings and continue.
3. In the Wizard **3 Hard Disk (HDD)** menu, the HDDs installed in the recorder are listed, showing their Capacity, Status, Free Space, etc. Usually HDDs will show a **Normal** status. If any HDD shows an **Uninitialized** status, it must be initialized (Init) before it can be used. The screen below shows a single HDD system with Normal Status and maximum Free Space

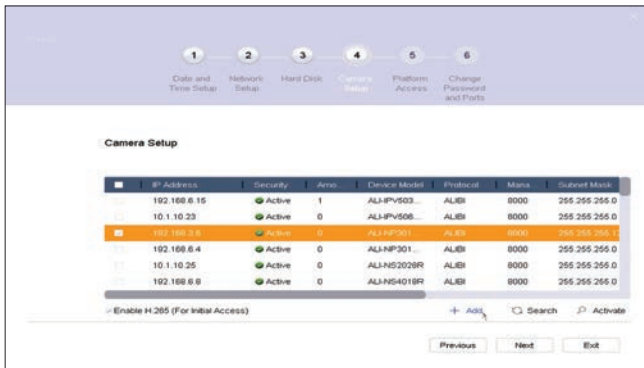


If any HDD listed shows a status of Uninitialized (see screen below) it must be initialized (Init) to restore it to a usable condition.
NOTE: The initialization process erases all data on the disk.



To Initialize an HDD:

- a. Check the select box for the HDD(s) you want to initialize.
 - b. Click the **Init** button.
 - c. Wait for the operation to complete (this could take several minutes), and then click **Next** to continue.
4. In the Wizard **4 Camera Setup** menu, you can select add cameras discovered on the local network to your surveillance system. Most recorders have a limit of how many network cameras can be added to the system. You can also use the recorder to Activate cameras on the network. A camera must be activated before it can be added.



To **activate** a network camera with the NVR:

- a. Click the **Search** button to discover the cameras attached to your local network (network to which the recorder is attached).
- b. Scroll through the list of cameras found on the local network, and then check the select box for the cameras you want to activate.
- c. Click the **Activate** button. Allow the operation to complete before continuing.

To **add** a network camera to the NVR:

- a. Click the **Search** button to discover the cameras attached to your local network (network to which the recorder is attached).
 - b. Scroll through the list of cameras found on the local network, and then check the select box for the cameras you want to add. See above.
 - c. Click the **Add** button. Allow the operation to complete before continuing.
5. In the Wizard **5 Platform Access** menu, you can setup Platform Access, enable DDNS, and/or configure Stream Encryption.

SECTION 2: BASIC SYSTEM SETUP

The screenshot shows the 'Platform Access' configuration screen, which is step 6 of a 6-step setup wizard. The wizard steps are: 1. Date and Time Setup, 2. Network Setup, 3. Hard Disk, 4. Camera Setup, 5. Platform Access, and 6. Change Password and Ports. The 'Platform Access' section includes the following fields and options:

- Access Type:** A dropdown menu set to 'Alibi Connect'.
- Enable:** A checkbox that is currently unchecked.
- Server Address:** A text field containing 'www.alibiconnect.com' with a 'Custom' button to its right.
- Enable DDNS:** A checkbox that is currently unchecked.
- DDNS Type:** A dropdown menu set to 'NO-IP'.
- Server Addr.:** A text field containing 'dyupdate.no-ip.com'.
- Device ID:** An empty text field.
- User Name:** An empty text field.
- Password:** An empty text field.
- Enable Stream Enc.:** A checkbox that is currently unchecked.
- Verification CodeID:** An empty text field.
- Status:** A label indicating 'Offline'.

At the bottom of the screen, there are three buttons: 'Previous', 'Next', and 'Exit'. The 'Next' button is highlighted with a mouse cursor.

Platform Access is used with the Alibi Witness 2 smartphone app to simplify access and control how others can access the system. To enable Platform Access for your recorder, check the **Enable** box (see the screen above). Then follow the on-screen instructions for activating this service. Refer to the **Alibi Witness 2** user documentation for instructions on using the platform access feature.

Enable DDNS enables DDNS (Dynamic Domain Name System) access to the recorder. This feature simplifies access to the recorder, especially when the IP address of the recorder may change. For more information on setting up a DDNS service for the recorder, refer to firmware user manual for the recorder. You can download the firmware user manual for your recorder from AlibiSecurity.com/resources.

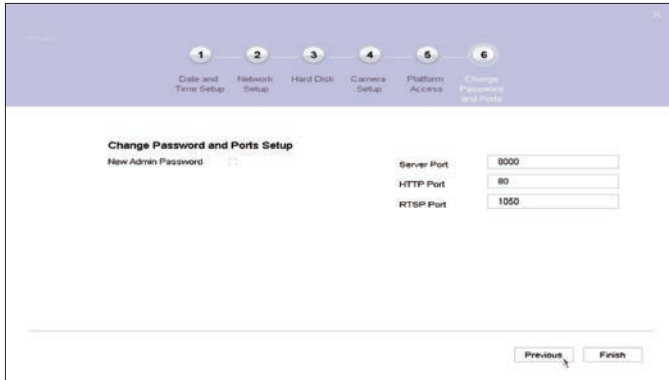
Enable Stream Encryption. Stream encryption enables to encrypt the streams for live view, playback, download, backup, etc. To use stream encryption:

- a. Check the **Enable Stream Encryption** select box.
- b. Create an encryption password.

NOTE

The stream encryption password is synchronized with the Alibi Connect service verification code. After enabling the encryption code, the Alibi Connect stream will be forcedly encrypted. Make sure your Alibi Connect service supports stream encryption.

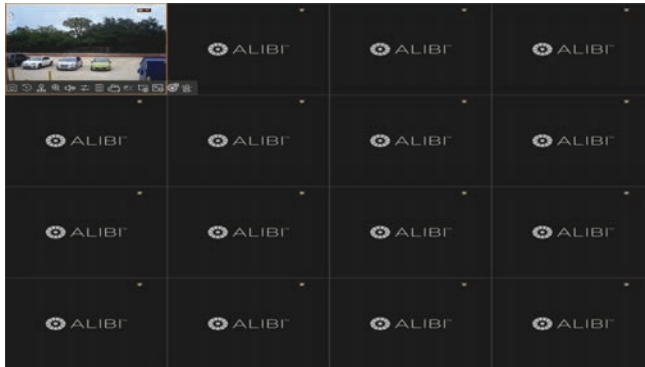
6. In the Wizard **6 Change Password and Ports** menu, you can modify your *admin* password and change the **Server, HTTP** and **RSTP** port numbers. **Alibi Support recommends that you change these port numbers for stronger security.**



To change the password, check the **New Admin Password** box, and then follow the on screen instructions.

To change the port numbers, enter the new port numbers in the field provided.

To save your settings and exit the configuration Wizard, click **Finish**. Click **Previous** to return to an another Wizard menu. After clicking Finish, the Live View window will open.



2.3 PoE channel configuration

Setup the PoE (Power over Ethernet) configuration as you add cameras to the internal switch ports on the back of the NVR. With this feature, you can disable PoE power on ports, and configure ports for long distance (extended) Ethernet reach.

The NVR monitors power consumption on each port of the internal Ethernet switch. This information is displayed by opening the **Menu | Camera | Camera | PoE Configuration** screen.

SECTION 2: BASIC SYSTEM SETUP

Extended PoE feature PoE power used by port

Channel	Long Distance	Short Distance	Channel Status	Actual Power
D1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Connected	5.20W
D2	<input type="checkbox"/>	<input type="checkbox"/>	Connected	8.30W
D3	<input type="checkbox"/>	<input type="checkbox"/>	Disconnected	0.00W
D4	<input type="checkbox"/>	<input type="checkbox"/>	Disconnected	0.00W
D5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Disconnected	0.00W
D6	<input type="checkbox"/>	<input type="checkbox"/>	Disconnected	0.00W
D7	<input type="checkbox"/>	<input type="checkbox"/>	Disconnected	0.00W
D8	<input type="checkbox"/>	<input type="checkbox"/>	Disconnected	0.00W
D9	<input type="checkbox"/>	<input type="checkbox"/>	Disconnected	0.00W
D10	<input type="checkbox"/>	<input type="checkbox"/>	Disconnected	0.00W
D11	<input type="checkbox"/>	<input type="checkbox"/>	Disconnected	0.00W
D12	<input type="checkbox"/>	<input type="checkbox"/>	Disconnected	0.00W
D13	<input type="checkbox"/>	<input type="checkbox"/>	Disconnected	0.00W
D14	<input type="checkbox"/>	<input type="checkbox"/>	Disconnected	0.00W

The display shows the real power consumed and the remaining power available for other ports.

Long Distance (Extended) PoE Power

Long distance PoE allows a maximum power of 7.5W with a maximum main stream and sub-stream combined bitrate of 6 Mb/s. To enable Long Distance PoE Power on a camera channel:

1. Click on the camera channel to extend, then click icon for that channel in the **Long Distance** column. In the example below, the **Long Distance** icon for camera channel D5 was selected.

Channel	Long Distance	Short Distance	Channel Status	Actual Power
D1	<input type="checkbox"/>	<input type="checkbox"/>	Connected	5.10W
D2	<input type="checkbox"/>	<input type="checkbox"/>	Connected	8.30W
D3	<input type="checkbox"/>	<input type="checkbox"/>	Disconnected	0.00W
D4	<input type="checkbox"/>	<input type="checkbox"/>	Disconnected	0.00W
D5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Disconnected	0.00W
D6	<input type="checkbox"/>	<input type="checkbox"/>	Disconnected	0.00W
D7	<input type="checkbox"/>	<input type="checkbox"/>	Disconnected	0.00W
D8	<input type="checkbox"/>	<input type="checkbox"/>	Disconnected	0.00W
D9	<input type="checkbox"/>	<input type="checkbox"/>	Disconnected	0.00W
D10	<input type="checkbox"/>	<input type="checkbox"/>	Disconnected	0.00W
D11	<input type="checkbox"/>	<input type="checkbox"/>	Disconnected	0.00W
D12	<input type="checkbox"/>	<input type="checkbox"/>	Disconnected	0.00W
D13	<input type="checkbox"/>	<input type="checkbox"/>	Disconnected	0.00W
D14	<input type="checkbox"/>	<input type="checkbox"/>	Disconnected	0.00W

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

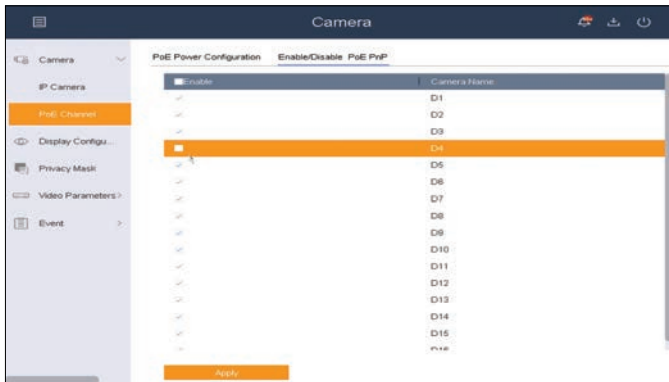
Disable PoE power on a channel

You can disable PoE on channels for cameras that do not use it.

You can also disable PoE on a camera channel, and then attach a switch where additional cameras, such as wireless cameras, are connected. If using this configuration, you cannot exceed the channel capacity of your NVR.

To disable PoE power on a camera channel:

1. Open the **Menu | Camera | Camera | PoE Configuration | Enable/Disable PoE PnP** screen.

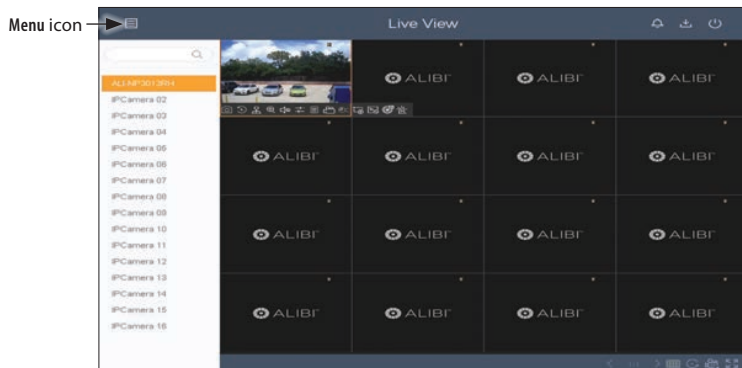


2. Click on the channel where you want to disable PoE, and then click the **Enable** box to **uncheck** it.
3. Click **Apply** to save your settings.

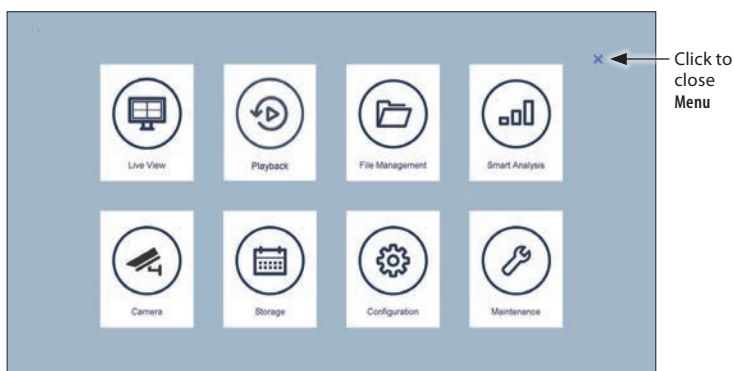
2.4 Basic camera setup

Several customization options are provided for configuring your cameras to function most effectively. Camera menus, and other configuration options, are available through the Menu screen. To open the Menu screen:

1. *Right click* anywhere in the **Live View** screen shown above. A live view utility screen will open.



The **Menu** screen will open.



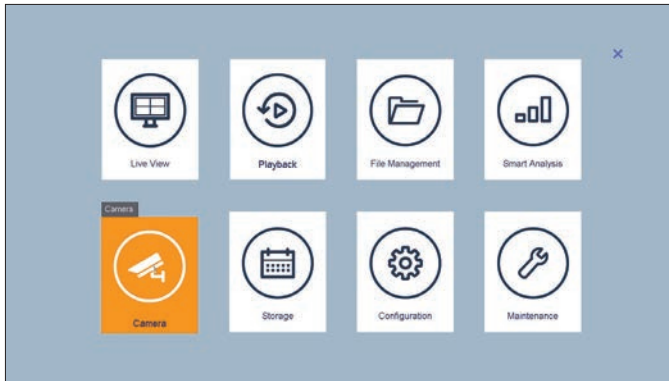
To open a segment of the firmware to configure, click the appropriate icon in the **Menu** screen. Refer to the firmware user manual for your recorder for specific instructions on how to use the **Menu** screen.

2.5 Customize camera configurations

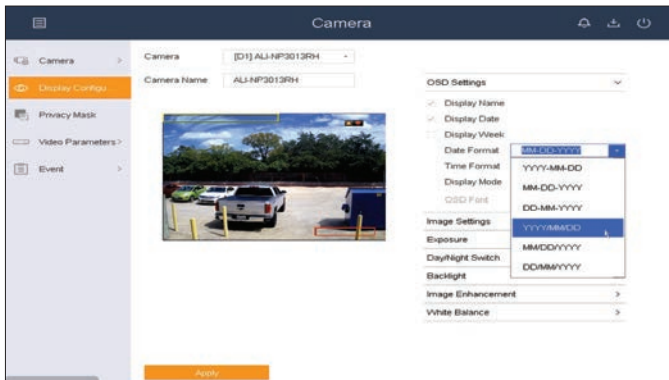
NOTE Options shown in the menu for cameras may change based on the model of camera used.

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. In the **Menu** screen, click the **Camera** icon.



1. In the **Camera** menu, click the link for **Display Config** in the left frame.



2.5.1 Camera OSD setup

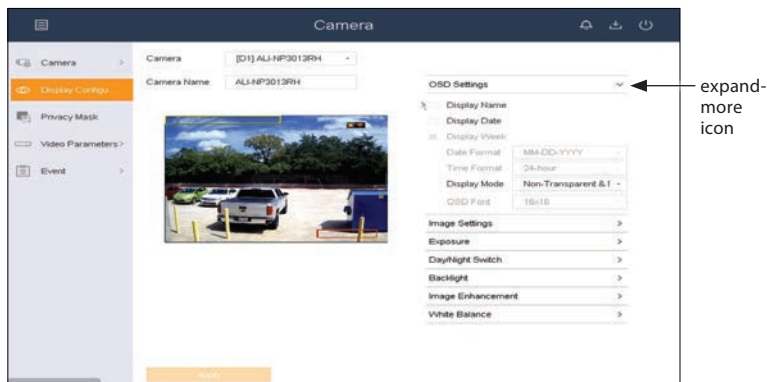
You can configure the OSD Settings (On-Screen Display) settings for the camera, including date, time, day of week, camera name, etc. OSD options you select will be permanently embedded in the recorded video for your camera.

NOTE

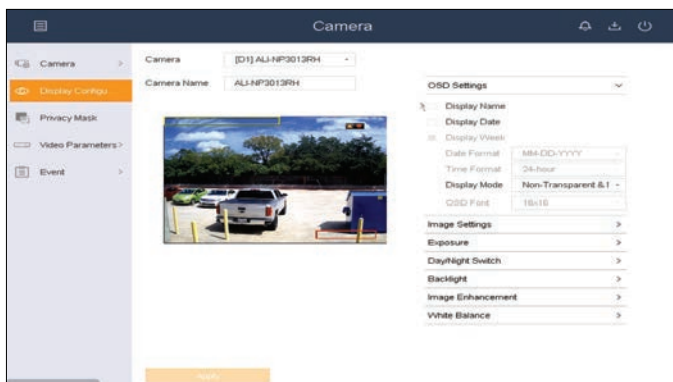
- If you display the date and time, ensure the date and time setup in the recorder is exact so that the video recorded can be used as credible evidence if needed.
- Alibi IP cameras you manage with the NVR may be setup internally to show on-screen information, such as name and timestamp.

1. In the **Display Configuration** menu, click the **expand-more** icon on the **OSD Settings** line to open the OSD menu.

SECTION 2: BASIC SYSTEM SETUP



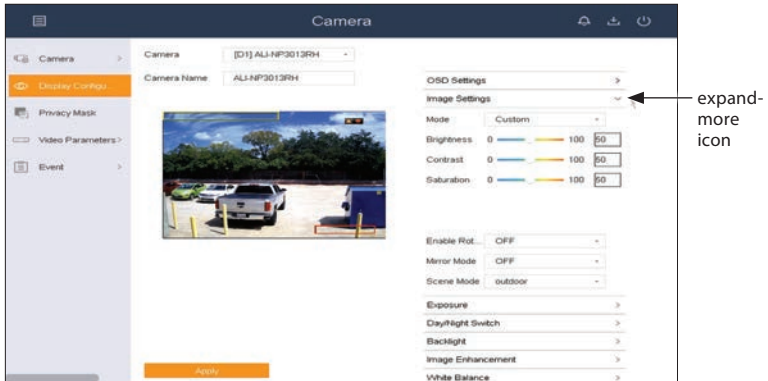
2. Open the **Camera** drop-down list and select the camera you want to configure. In the screen below, camera (D1)ALI-NP3013RH is selected.



3. In the OSD menu, check the select boxes for the information you want to appear on the screen, such as camera name, date and/or week. Information you selected will appear in the text boxes shown in the video window.
 - a. If you selected **Display Name**, enter the name of the camera in the **Camera Name** field near the top of the window.
 - b. For other items you selected, open the drop down lists for the Date/Time Format, Display Mode and OSD Font as needed and select the best choice for your camera.
 - c. Drag the text boxes to the best locations in the camera field of view.
4. Click **Apply** to save your settings.
5. Repeat sub-steps 2 through 4 above for each camera managed by the NVR.

2.5.2 Camera Image Settings

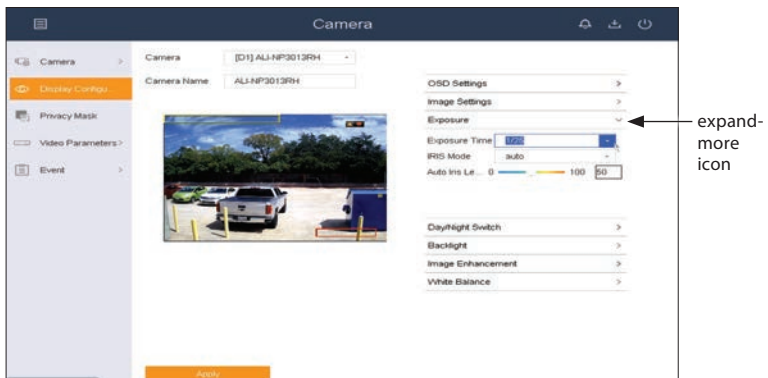
1. In the **Display Configuration** menu, click the **expand-more** icon on the **Image Settings** line.



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. Adjust the sliders for the **Brightness**, **Contrast** and **Saturation** to produce the best image.
4. Open the drop down lists for **Enable Rotation**, **Mirror Mode** and **Scene Mode**, then select best option for each for this camera installation.
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.

2.5.3 Camera Exposure setup

1. In the **Display Configuration** menu, click the **expand-more** icon on the **Exposure** line.



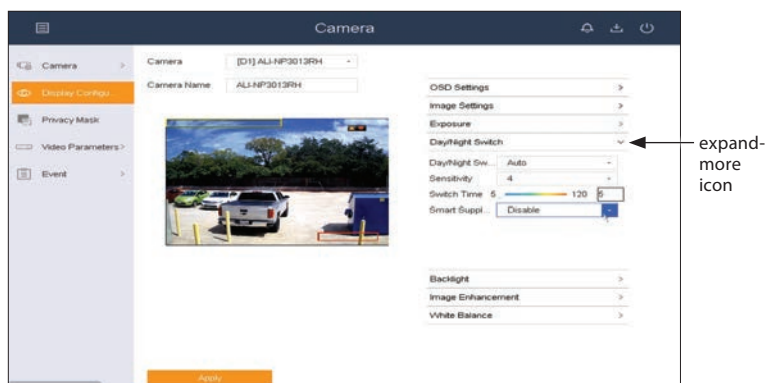
SECTION 2: BASIC SYSTEM SETUP

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. Open the **Exposure Time** drop down list, and select the optimal exposure time for the camera (1/100000 to 1 second). Larger exposure time produces a brighter image.
4. Open the **Iris Mode** drop down list, and select either **Auto** or **Manual**. Auto opens a slider for setting the Auto Iris Level (1 .. 100).
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.

2.5.4 Camera Day/Night Switch

Use the camera Daylight Switch menu to control how the camera employs IR to respond to low ambient light (night) conditions.

1. In the **Display Configuration** menu, click the **expand-more** icon on the **Day/Night Switch** line.



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. Open the **Day/Night Switch** drop down list and select the best option for the camera. Options include: **Day, Night, Auto, Auto-Switch, Triggered by Alarm Input**. Depending on the option you select, related parameters will be presented. Configure the parameters before continuing. **NOTE:** The difference between **Auto** and **Auto-Switch** is described below.

Auto: The camera automatically switches between day mode and night mode according to the illumination. The sensitivity ranges from 0 to 7, and higher sensitivity more easily triggers the mode switch. The switch time refers to the interval time between the day/night switch. You can set it from 5 sec to 120 sec.

Auto-Switch: The camera switches the day mode and the night mode according to the start time and end time you set.

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

2.5.5 Camera Backlight setup

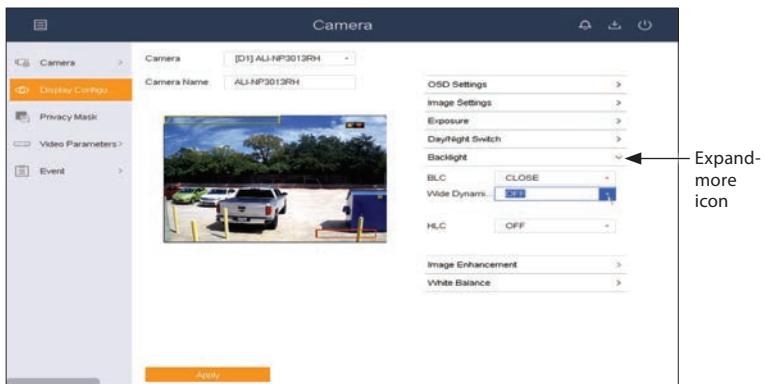
Backlight settings control the camera's dynamic range. Use this feature when the surrounding illumination and the object have large differences in brightness, such as bright light from a window shining in behind your surveillance targets. Settings in this menu largely depend on the capabilities of the camera, and may require testing to find the best performance settings.

HLC: Senses strong sources of light in video and compensates for exposure on these spots to enhance the overall quality. It is effective for preventing very bright spots such as headlights or spotlights from causing the camera to overcompensate its exposure setting.

BLC: Backlight Compensation configures the camera to adjust its exposure appropriately when the target object is in front of a bright background. Essentially, it brightens the darker areas of the image, at the expense of overexposing the brighter areas.

WDR: Wide Dynamic Range sets the camera to adjust the exposure appropriately so that darker areas of the image and brighter areas of the image are exposed optimally. WDR can be ON if BLC is closed. Otherwise, WDR is not selectable.

- In the **Display Configuration** menu, click the **expand-more** icon on the **Backlight** line.



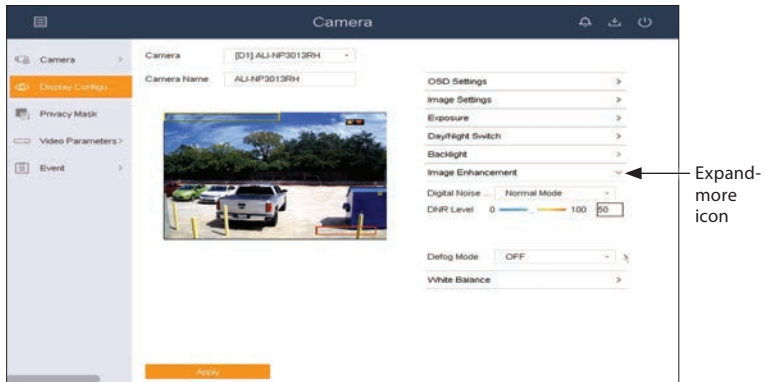
- In the **Camera** field drop down list, select the camera you want to configure. In the example above, **[D1]IPCamera 01** is selected.
- Open the BLC drop down list, and select either **CLOSE** or the best choice for the source of the background light. Choices are **UP, DOWN, LEFT, RIGHT, CENTER, Region, AUTO**.
 - If you selected **CLOSE**, you can set WDR ON or OFF, and HLC ON or OFF.
 - If you did not select CLOSE, you can set HLC ON or OFF.

4. Click **Apply** to save your settings for this camera.
5. Repeat sub-steps **2** through **3** above for each camera managed by the NVR.

2.5.6 Camera Image Enhancement

Use the camera Image Enhancement menu to optimize camera contrast. Finding optimal settings for these options may require testing.

1. In the **Display Configuration** menu, click the **expand-more** icon on the **Image Enhancement** line.

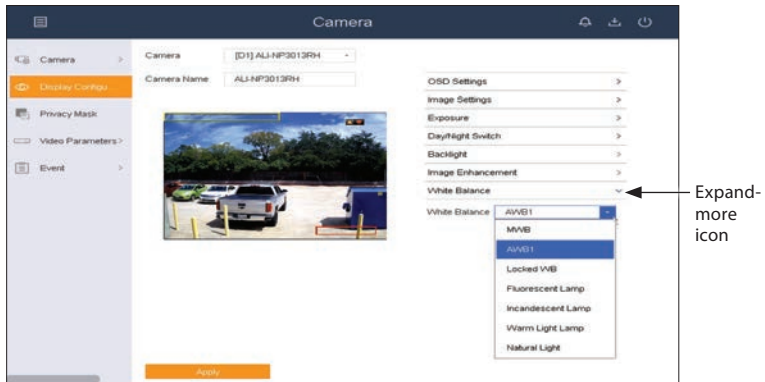


2. In the **Camera** field drop down list, select the camera you want to configure. In the example above, **[D1]IPCamera 01** is selected.
3. Open the **Digital Noise** drop down list and select either **Close**, **Normal Mode**, or **Expert Mode**.
 - a. If you selected **Close**, you can select **Defog Mode** ON or OFF.
 - b. If you selected **Normal Mode**, use the slider to adjust the **Digital Noise Reduction** to produce the best image. With this option, you can also enable **Defog Mode**.
 - c. If you selected **Expert Mode**, you can set the Time DNR level and Space DNR level individually, and turn on Defog mode.
4. Click **Apply** to save your settings for this camera.
5. Repeat sub-steps **2** through **3** above for each camera managed by the NVR.

2.5.7 Camera White Balance adjustment

Adjust the white balance of the camera to display the best color accuracy. Color accuracy depends largely on the ambient light source.

1. In the **Display Configuration** menu, click the **expand-more** icon on the **White Balance** line.

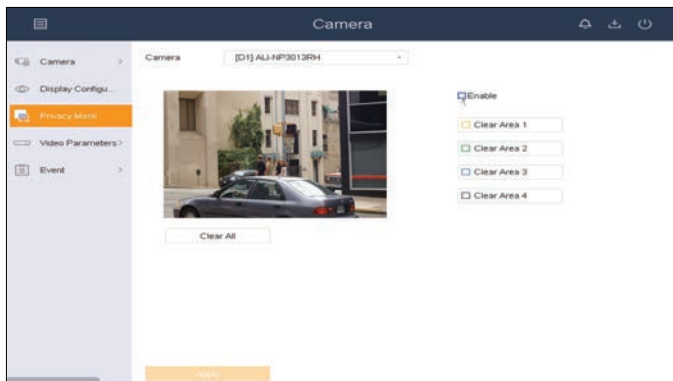


2. In the **Camera** field drop down list, select the camera you want to configure. In the example above, **[D1]IPCamera 01** is selected.
3. Open the **White Balance** drop down list and select the mode that produces the best color.
 - a. If you select **MWB** (Manual White Balance), use the sliders to set the Red and Blue color gains.
 - b. If you select **AWB1**, the color is continuously adjusted by the camera.
 - c. If you select **Locked WB**, the Red and Blue color gains do not change.
 - d. Select any other White Balance mode if the ambient light is largely from those sources.
4. Click **Apply** to save your settings for this camera.
5. Repeat sub-steps **2** through **3** above for each camera managed by the NVR.

2.5.8 Camera Privacy Mask

Privacy masks are rectangular image blocks used to obscure parts of the field of view where privacy must be maintained, such as areas where sensitive information exists, house windows, etc. You can set up to four privacy masks in the video image.

1. In the **Privacy Mask** menu.



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. In the video window, drag a rectangle across the area of the field of view where you want to apply a mask. In the image below, the mask was applied to the area over the window in the upper left corner. The color of the boarder surrounding the rectangle indicates the Area number. The mask in the image below has an orange border, indicating Area 1.



4. You can drag up to three more rectangles across the screen, each assigned to a different area number, for a maximum of four.
5. To clear a mask, click the **Clear Area** button with the color associated with the mask.
6. Click **Apply** to save your settings for this camera.
7. Repeat sub-steps **2** through **6** above for each camera managed by the NVR, if needed.

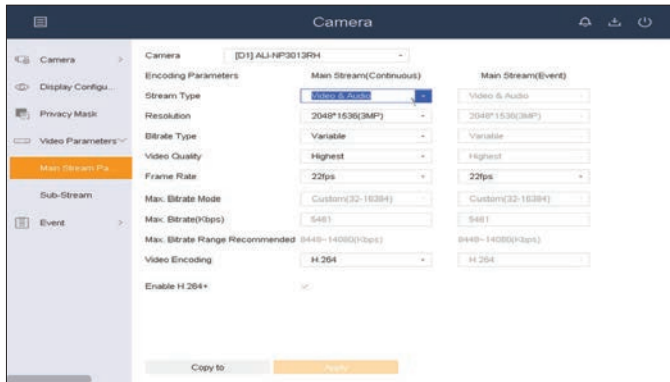
2.5.9 Camera Video Parameters

Use the Video Parameters Main Stream and Sub-Stream menus to control the video resolution of the camera and other transmission parameters. These menus, with the network bandwidth calculator available on AlibiSecurity.com/resources, can help you get the best performance from your security system network.

Main Stream Parameters

In the Main Stream Parameters menu, you can adjust network parameters for both main stream Continuous recording and Event recording. Refer to the Specifications for your camera(s) to see what options for main stream performance are available.

1. In the **Camera** menu, click on **Video Parameters**, and then click on **Main Stream Parameters**.



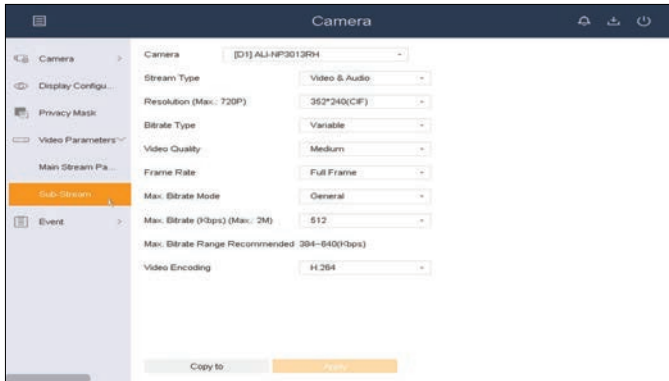
2. In the **Camera** field drop down list, select the camera you want to configure. In the example above, **[D1]IPCamera 01** is selected.
3. In the Stream Type field, select either **Video & Audio** (if streaming with audio), or **Video**. This selection affects the bitrate requirement for the camera.
4. Adjust other parameters as needed for the camera performance needed. Notice that you can set different **Frame Rates** for Continuous and Event recording.
5. Click **Apply** to save your settings for this camera.
6. Click **Copy** to use the same settings for other cameras on your surveillance system.
7. Repeat sub-steps **2** through **7** above for each camera managed by the NVR, if needed.

Sub-Streams

In the Sub-Stream menu, you can adjust network parameters for the camera sub-stream channel. Refer to the Specifications for your camera(s) to see what options for sub-stream performance are available. Sub-stream video is useful for remote login to the recorder and on networks where bandwidth is limited.

1. In the **Camera** menu, click on **Video Parameters**, and then click on **Sub-Stream**.

2: BASIC SYSTEM 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. In the Stream Type field, select either **Video & Audio** (if streaming with audio), or **Video**. This selection affects the bitrate requirement for the camera.
4. Adjust other parameters as needed for the camera performance needed.
5. Click **Apply** to save your settings for this camera.
6. Click **Copy** to use the same settings for other cameras on your surveillance system.
7. Repeat sub-steps **2** through **6** above for each camera managed by the NVR, if needed.

2.5.10 PTZ camera setup

To setup cameras with Pan, Tilt, Zoom (PTZ) capability, refer to "SECTION 6 PTZ Controls" on page 77.

SECTION 3

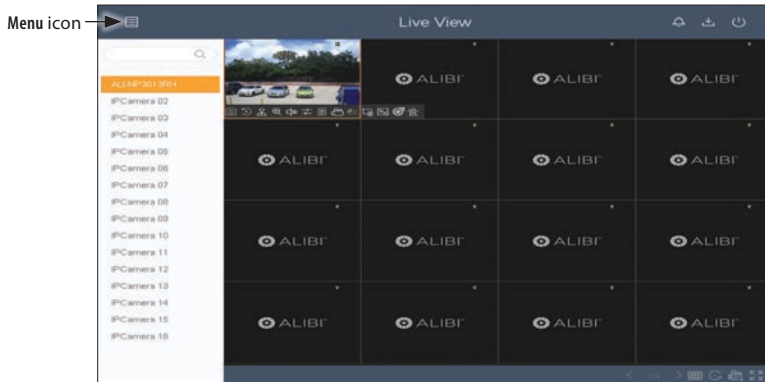
Event setup

Use this section to configure your system to sense for and log information about what your security system is sensing, such as motion in the field of view, hard disk drive (HDD) full, etc. It also includes procedures for configuring Smart events (Video Content Analytic events), such as face detection, line crossing, intrusion detection, object removal, and other conditions determined by analyzing the video or audio stream. Smart events are features available in some cameras.

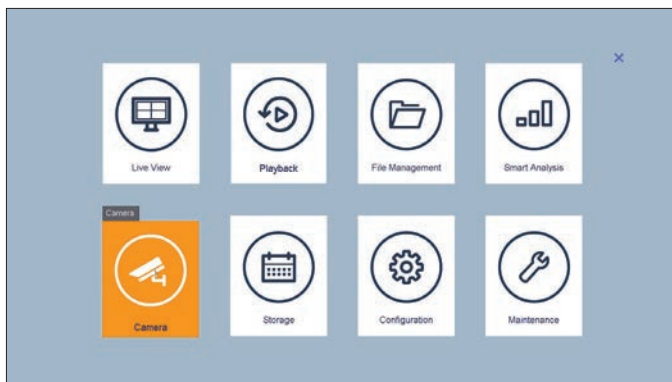
The default factory setup configuration sets up all camera channels to record continuously. Since this configuration may write excessive data on the disk, you can reconfigure your cameras to only write when necessary, such as when motion is detected in a specific area of the video frame.

To access the event setup menus:

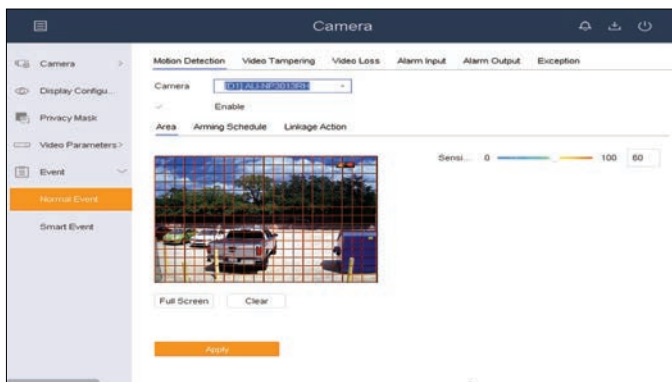
1. *Right click* anywhere in the **Live View** screen to access the Live View header, if necessary, and then click the **Menu** icon.



2. In the **Menu** screen, click the **Camera** icon.



1. In the **Camera** menu, click the link for **Event** in the left frame.



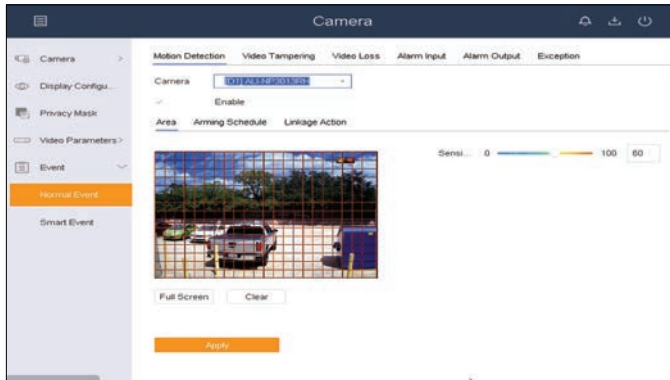
The Event - Normal menu screen will open showing the Motion Detection menu.

3.1 Normal Event Setup

Normal Events include camera Motion Detection, Video Tampering, Video Loss, recorder/camera events including Alarm Input, and recorder Exception conditions. The recorder Alarm Output configuration is also included in this menu.

3.1.1 Camera Motion Detection

Use the Motion Detection feature to detect motion anywhere in the field of view and log a motion detection event. It can be configured to just sense for motion in parts of the field of view, sense for motion at only certain times of the week, and trigger the system to perform actions when motion is sensed. The default Motion Detection menu is shown below.



1. To use Motion Detection, open the **Camera** drop down list and then select the camera you want to configure. In the example above, **[D1] ALI-NP3013RH** is selected.
2. Click the **Enable** box to check it. See the screen above.

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.

3. To efficiently detect for motion in the field of view, select only the parts of the video image where motion is of interest. Some areas of the field of view may trigger false events, such as trees in the wind, etc. The grid shows where the camera will sense for motion:
 - 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.



- c. When you release the mouse button, a grid will appear in that area.

SECTION 3: EVENT SETUP



- d. Repeat the previous sub-step to create setup other areas of video image where you want to sense for motion.
- e. Click **Apply** to save your settings.
- f. 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. See the screen above.

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.

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

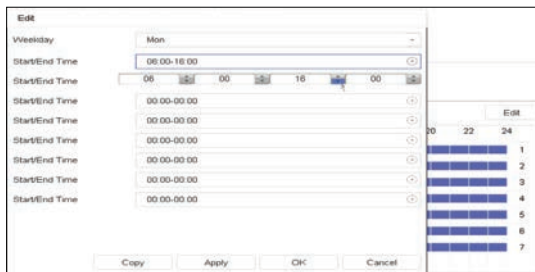
Setup Arming Schedule

4. Click the **Arming Schedule** icon to define the times when motion detection for this camera is sensed (armed). The blue segments in the schedule show when it is armed. By default, when this event is enabled, it is armed continuously.



You can change the Arming Schedule in either of two ways: using the **Edit** and using the graphical method. To use **Edit**:

- a. Click the **Edit** button shown in the screen above. An edit menu will open.

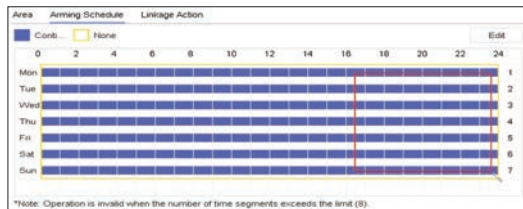


- b. Click **Weekday**, and then select the day of the week you want to edit. For each day of the week, you can define up to seven time segments.
- c. Click the **Start/End Time** field. An adjustment bar will open.
- d. In the adjustment bar, click the up and down carets to set the hour and minute to start arming, and the hour and minute to end arming for this segment. In the example above, the segment starts at 0600 (6:00 am) and ends at 1600 (4:00 pm).
- e. Create additional segments for that day as needed. Segments cannot overlap.
- f. Click **Apply** to save your settings.
- g. Click **Copy** to copy this schedule to other days of the week. Follow the on-screen instructions to use this menu.
- h. In the Edit menu, click **OK** to return to the **Arming Schedule**. Changes you saved will be reflected in the schedule.

Arming Schedule “graphical” method

The graphical editing method is used by clicking either **Continuous** or **None**, then dragging a box over the areas of the schedule when you want to either enable or disable arming. For example, to disable arming in an area of the schedule:

- a. Click the None icon at the top of the Arming Schedule.
- b. Using the mouse, drag a rectangle over the area of the schedule where you want to disable arming. The area you selected is shown by a red rectangle.



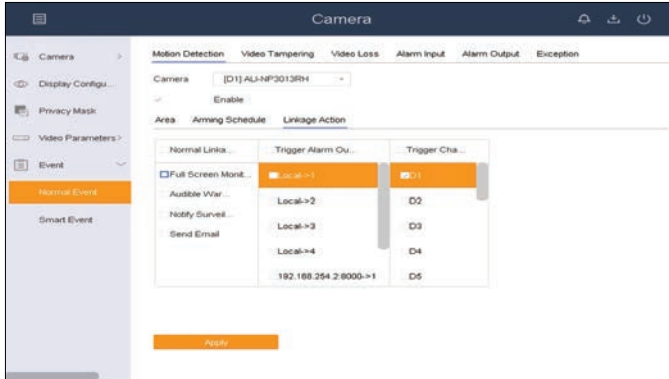
- c. Release the mouse button. The part of the schedule you selected is now disarmed.



- d. Click **Continuous** and repeat this method to restore area to the arming schedule, if needed.

Linkage Action

- Click the **Linkage Action** tab.

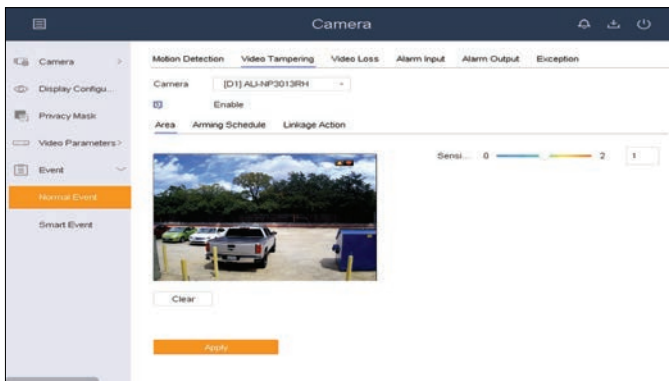


- In the **Linkage Action** menu, check the boxes for the actions you want to occur when event is detected.
- Click **Apply** to save your settings.
- Repeat steps 1 through 7 above for each camera on your surveillance system.

3.1.2 Camera Video Tampering

Video Tampering can log an alarm event when the camera lens, or part of the field of view, is covered. To use this feature:

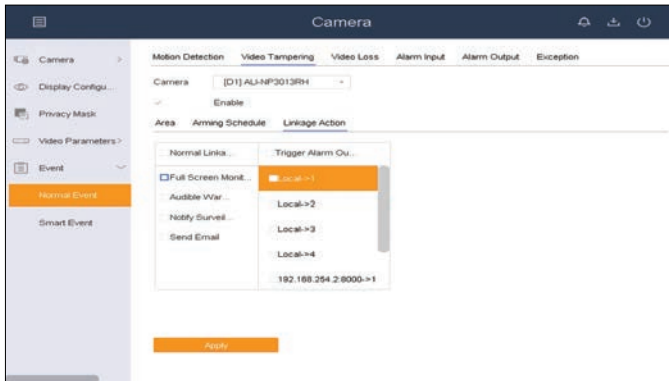
- Open the Video Tampering menu. Go to **Menu | Camera | Event | Normal Event | Video Tampering**.



- Click the **Enable** box to check it.
- Drag a rectangle across the area of the video window where you want to sense for Video Tampering.



- Adjust the **Sensitivity** as needed to effectively sense for tampering. Options are 0, 1, 2.
- Click **Apply** to save your settings.
- Click the **Arming Schedule** tab. To configure the arming schedule, refer to the procedure in "3.1.1 Camera Motion Detection" on page 29.
- Click the **Linkage Action** tab.



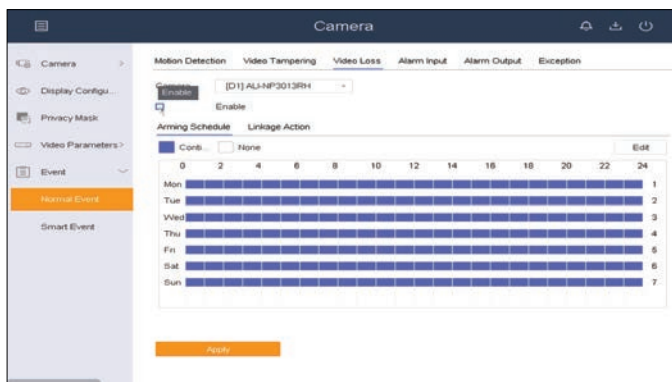
- In the **Linkage Action** menu, check the boxes for the actions you want to occur when the event is detected.
- Click **Apply** to save your settings.
- Repeat steps 1 through 9 above for each camera on your surveillance system.

3.1.3 Camera Video Loss

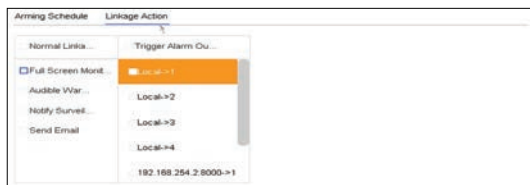
Video loss occurs when the video signal from the camera is no longer detected. This can result from many causes, such as a disconnected cable, hardware or cable failure, power loss, etc. To use this feature:

- Open the Video Loss menu. Go to **Menu | Camera | Event | Normal Event | Video Loss**.

SECTION 3: EVENT SETUP



2. Click the **Enable** box to check it.
3. Click the **Arming Schedule** tab. To configure the arming schedule, refer to the procedure in “3.1.1 Camera Motion Detection” on page 29.
4. Click the **Linkage Action** tab.



5. In the **Linkage Action** menu, check the boxes for the actions you want to occur when the event is detected.
6. Click **Apply** to save your settings.
7. Repeat steps 1 through 6 above for each camera on your surveillance system.

3.1.4 Alarm Input detection

The Alarm Input menu lists all alarm inputs supported by the recorder, plus all alarm inputs of the cameras attached to your surveillance system. An alarm input can generate a log event and trigger actions in the recorder, such as recording camera video or video capture. To configure alarm inputs:

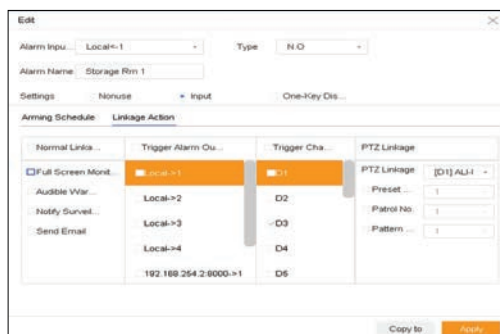
1. Open the Alarm Input menu. Go to **Menu | Camera | Event | Normal Event | Alarm Input**.

Alarm Input No.	Alarm Name	Alarm Type	Enable	Edit
Local<-1		N.O.	No	
Local<-2		N.O.	No	
Local<-3		N.O.	No	
Local<-4		N.O.	No	
Local<-5		N.O.	No	
Local<-6		N.O.	No	
Local<-7		N.O.	No	
Local<-8		N.O.	No	
Local<-9		N.O.	No	
Local<-10		N.O.	No	
Local<-11		N.O.	No	
Local<-12		N.O.	No	
Local<-13		N.O.	No	
Local<-14		N.O.	No	
Local<-15		N.O.	No	
Local<-16		N.O.	No	

- Click the icon in the **Edit** column of the alarm input you want to configure. In the pop-up menu shown below, Local<-1 (Alarm In 1 on the back of the recorder) was selected.

Edit
 Alarm Input: Local<-1 Type: N.O.
 Alarm Name:
 Settings: Nonuse Input One-Key Dis...
 Copy to Apply

- In the **Alarm Name** field, enter a common name for the alarm.
- Open the **Type** field, and select either **N.O.** for a Normally Open alarm switch, or **N.C.** for a Normally Closed alarm switch.
- Click the radial button for either **Nonuse** (disable) or **Input** (enabled). By default, all inputs are in **Nonuse** mode. If you selected **Input**, Arming Schedule and Linkage Action option menu tabs will appear.

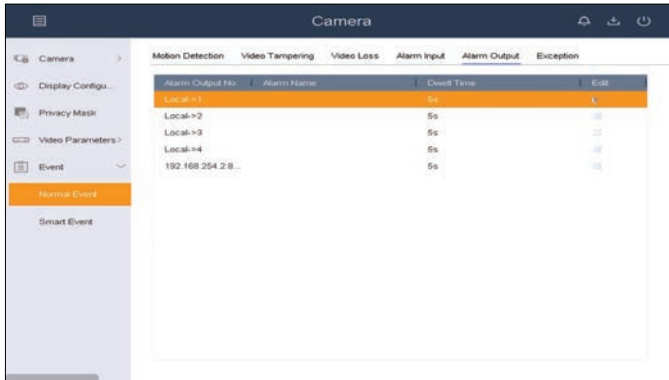


- a. Click the **Arming Schedule** tab. To configure the arming schedule, refer to the procedure in “3.1.1 Camera Motion Detection” on page 29.
 - b. Click **Apply**, and then click **Copy to** and use the on-screen menu to use the same schedule for other alarm inputs.
 - c. Click the **Linkage Action** tab (see above). In the linkage action menu, check the boxes for the actions you want to perform when the input becomes active (N.C switches open or N.O. switches close).
 - d. Click **Apply**, and then click **Copy to** and use the on-screen menu to use the same linkage actions for other alarm inputs.
6. Click the Close icon (✕) in the upper right corner of the **Edit** screen to return to the Alarm Input menu.
 7. Repeat steps 1 through 6 above for each alarm input on your surveillance system.

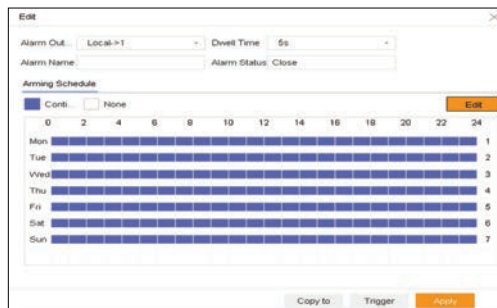
3.1.5 Alarm Output configuration

The Alarm Output menu lists all alarm outputs supported by the recorder, plus all alarm outputs of the cameras attached to your surveillance system. An alarm output can be used to activate an accessory attached to your surveillance system, such as a siren, light, door unlock relay, etc. To configure alarm outputs:

1. Open the Alarm Input menu. Go to **Menu | Camera | Event | Normal Event | Alarm Output**.



- Click the icon in the **Edit** column of the alarm output you want to configure. In the pop-up menu shown below, Local->1 (Alarm OUT 1 on the back of the recorder) was selected.



- In the **Alarm Name** field, enter a common name for the alarm.
- Open the **Dwell Time** drop down list, and then select the time the alarm will remain active after it is initiated. You can also select **Manually clear**.
- Click the **Arming Schedule** tab. To configure the arming schedule, refer to the procedure in "3.1.1 Camera Motion Detection" on page 29.
- Click **Apply**, and then click **Copy to** and use the on-screen menu to use the same schedule for other alarm outputs.
- Test the alarm output functionality by clicking **Trigger** to activate the alarm, and then **Clear** to deactivate it.
- Click the Close icon (X) in the upper right corner of the **Edit** screen to return to the Alarm Input menu.
- Repeat steps 1 through 8 above for each alarm output on your surveillance system.

3.1.6 Exception reporting

The NVR monitors for and responds to certain system-related alarm conditions (exception types). Monitoring for and response to these exceptions are configurable using the Exception menu.

Exception types include:

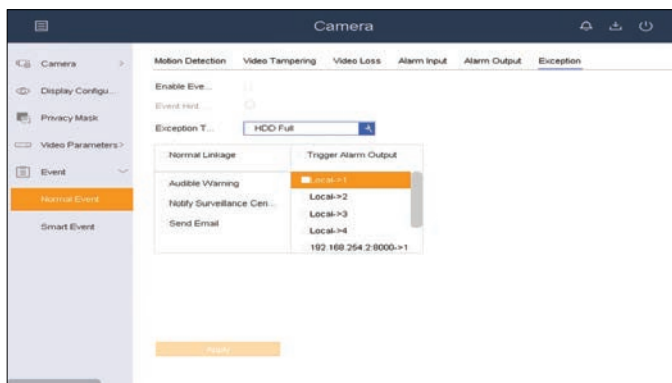
- **HDD Full:** The HDD is full.
- **HDD Error:** Writing HDD error or unformatted HDD.
- **Network Disconnected:** Disconnected network cable.
- **IP Conflicted:** Duplicated IP address.
- **Illegal Login:** Incorrect user ID or password.
- **Record/Capture Exception:** No space exists for saving recorded files.
- **PoE Power Overload:** PoE power consumption of the cameras connected to the internal Ethernet switch exceeds the maximum PoE power.
- **HDD SHM Detection Exception:** Seagate SkyHawk™ Health Management (SHM) exception condition

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. Also sends a push notifications to .Alibi Witness 2.0.
- **Notify Surveillance Center:** Sends a push notifications to Alibi Witness 2.0, message to Alibi Central Management Software (ACMS) system.
- **Trigger Alarm Output:** Trigger an alarm output when exception is detected.

To configure exception alarms:

1. Open the Exception menu. Go to **Menu | Camera | Event | Normal Event | Exception**.



2. Check the **Enable Event Hint** box to use hint reporting. When this feature is enabled and an event or exception occurs, a hint is displayed on the live view image. And you can click on the hint icon to check the details. The event hints to be displayed is configurable:
 - a. Open the **Event Hint** drop down list, and deselect the event hints you don't want to see. By default, all hints are enabled.
3. On the **Exception Type** line, open the drop down list and select the exception condition you want to monitor. If you select **All**, all exception conditions will be treated the way you configure the response. You can deselect the types of exceptions you don't want to see reported.
4. Check the select boxes for the response options you want to use.
5. Click **Apply** to save your settings.

3.2 Smart Event Setup

Smart event detection uses the video or audio stream to sense for line crossing, face detection, intrusion detection, etc. These events are commonly referred to as VCA events, and are available on most Alibi professional grade cameras. The smart features that appear at the top of the Smart Event menu are the features supported by the camera selected at the top of the screen.

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 etc.

These recorders support the following VCA features:

- **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 1 line crossing condition for each NS series IP cameras, and 4 line crossing conditions for each NP series IP cameras and TVI recorders with TVI cameras.
- **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 1 intrusion region for NS series IP cameras, and 4 intrusion regions for NP series IP cameras.
- **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.
- **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.

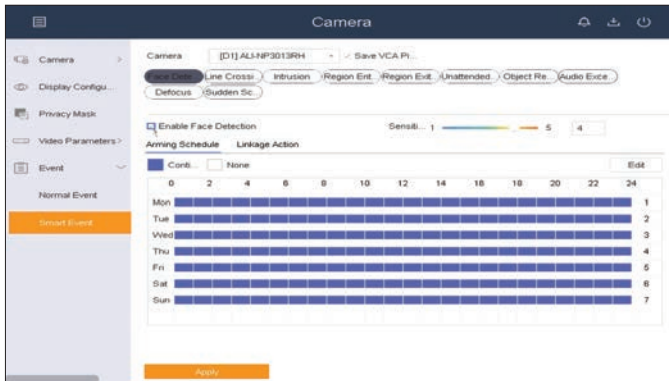
SECTION 3: EVENT SETUP

- **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.

3.2.1 Camera Face Detection

The Face detection analytic detects when a face appears in the surveillance field of view. To configure Face Detection in the camera:

1. Open the Face Detection menu:
 - a. Go to **Menu | Camera | Event | Smart Event**



- b. Open the drop down list on the camera line, then select the camera you want to configure.
 - c. If the Face Detection option appears in the VCA list at the top of the screen, click on it to configure this feature.
2. Check the **Save VCA Picture** box to capture a live view image of the VCA event.
 3. Click the **Enable Face Detection** box to check it.
 4. Set the Sensitivity slider as needed to detect faces in the field of view. This adjustment may require some testing.

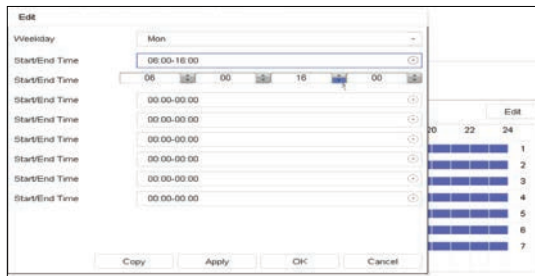
Setup Arming Schedule

5. Click the **Arming Schedule** icon to define the times when motion detection for this camera is sensed (armed). The blue segments in the schedule show when it is armed. By default, when this event is enabled, it is armed continuously.



You can change the Arming Schedule in either of two ways: using the **Edit** and using the **graphical** method. To use **Edit**:

- a. Click the **Edit** button shown in the screen above. An edit menu will open.



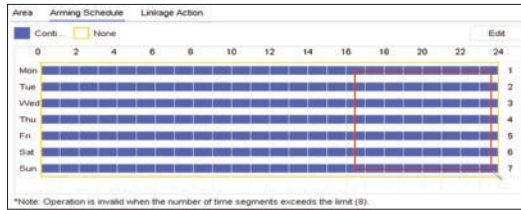
- b. Click **Weekday**, and then select the day of the week you want to edit. For each day of the week, you can define up to seven time segments.
- c. Click the **Start/End Time** field. An adjustment bar will open.
- d. In the adjustment bar, click the up and down carets to set the hour and minute to start arming, and the hour and minute to end arming for this segment. In the example above, the segment starts at 0600 (6:00 am) and ends at 1600 (4:00 pm).
- e. Create additional segments for that day as needed. Segments cannot overlap.
- f. Click **Apply** to save your settings.
- g. Click **Copy** to copy this schedule to other days of the week. Follow the on-screen instructions to use this menu.
- h. In the Edit menu, click **OK** to return to the **Arming Schedule**. Changes you saved will be reflected in the schedule.

Arming Schedule "graphical" method

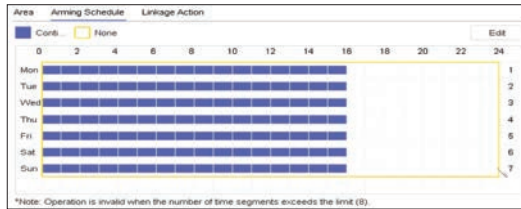
The graphical editing method is used by clicking either **Continuous** or **None**, then dragging a box over the areas of the schedule when you want to either enable or disable arming. For example, to disable arming in an area of the schedule:

- a. Click the **None** icon at the top of the Arming Schedule.
- b. Using the mouse, drag a rectangle over the area of the schedule where you want to disable arming. The area you selected is shown by a red rectangle.

SECTION 3: EVENT SETUP



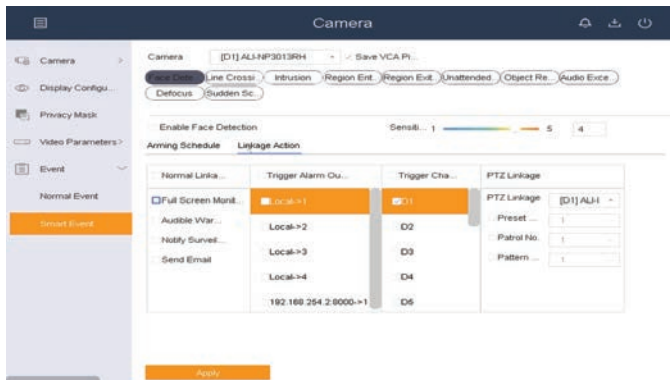
- c. Release the mouse button. The part of the schedule you selected is now disarmed.



- d. Click **Continuous** and repeat this method to restore area to the arming schedule, if needed.

Linkage Action

6. Click the **Linkage Action** tab.

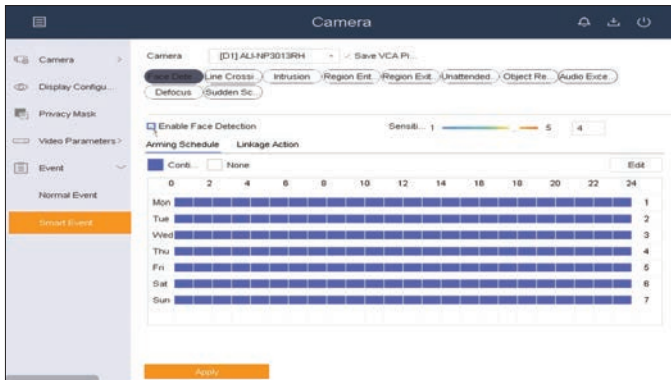


7. In the **Linkage Action** menu, check the boxes for the actions you want to occur when the event is detected.
8. Click **Apply** to save your settings.
9. Repeat steps 1 through 8 above for each camera on your surveillance system as needed.

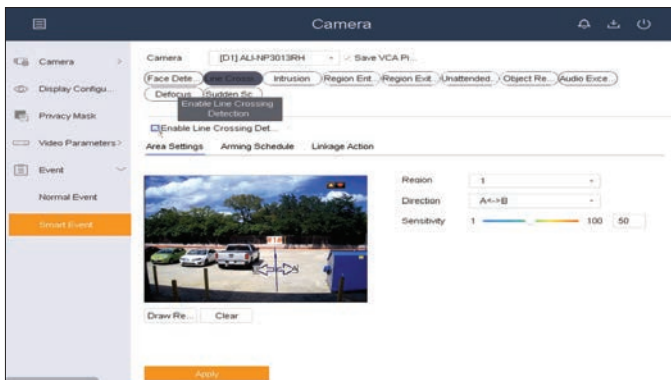
3.2.2 Line Crossing detection

With 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 1 virtual line for each NS series camera, and 4 virtual lines for each NP series IP camera. To use Line Crossing Detection:

1. Open the Line Crossing Detection menu:
 - a. Go to **Menu | Camera | Event | Smart Event**



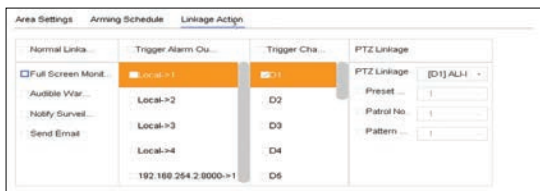
- b. Open the drop down list on the camera line, then select the camera you want to configure.
- c. If the Line Crossing option appears in the VCA list at the top of the screen, click on it to configure this feature.



2. Check the **Save VCA Picture** box to capture a live view image of the VCA event.
3. Click the **Enable Line Crossing Detection** box to check it (see above).

SECTION 3: EVENT SETUP

- In the **Area Settings** tab:
 - Open the **Region** drop down list and select a number to be associated with the virtual line you are creating. For NP series IP cameras you can select either 1, 2, 3 or 4.
 - Open the **Direction** drop down list, and select the direction of line crossing to sense for. After you create the virtual line, an arrow will appear across the line showing the direction it is configured to sense for.
 - Set the **Sensitivity** slider as needed to detect objects crossing the line. This adjustment may require some testing.
 - Click the **Draw Region** button. Then click a point in the video image to identify one endpoint of the virtual line, then click another point to represent the other endpoint of the line.
 - Click the **Stop Drawing** button. A line will appear on video image showing the Region number and direction of crossing you configured it to sense for.
 - Click **Apply** to save your settings.
 - To create another virtual line for crossing detection, repeat sub-steps **a** through **e** above with a different region number. You can create up to four virtual lines in the video channel.
- Click the **Arming Schedule** tab. To configure the arming schedule, refer to **Setup Arming Schedule** in “3.2.1 Camera Face Detection” on page 40.
- Click the **Linkage Action** tab.

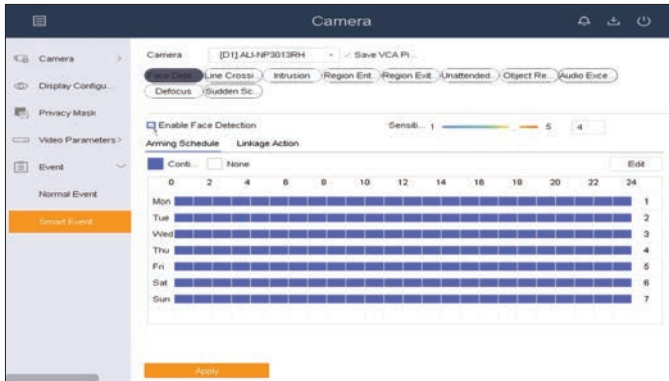


- In the **Linkage Action** menu, check the boxes for the actions you want to occur when the event is detected.
- Click **Apply** to save your settings.
- Repeat steps 1 through 8 above for each camera on your surveillance system as needed.

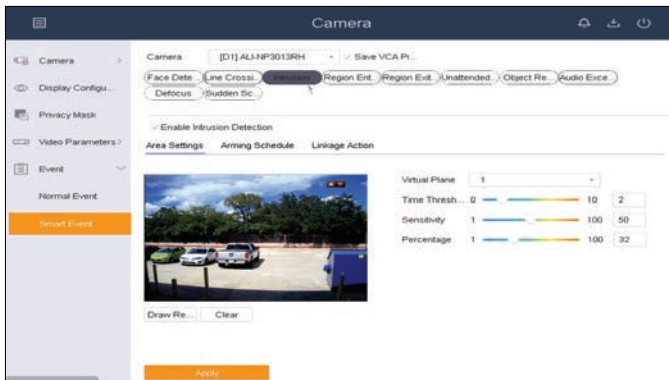
3.2.3 Camera Intrusion Detection

With camera Intrusion Detection, you can create up to four virtual quadrangles (planes) in the video image, and then detect if something enters the space within a plane. To use Intrusion Detection:

- Open the **Intrusion Detection** menu:
 - Go to **Menu | Camera | Event | Smart Event**



- b. Open the drop down list on the camera line, then select the camera you want to configure.
- c. If the Intrusion option appears in the VCA list at the top of the screen, click on it to configure this feature.



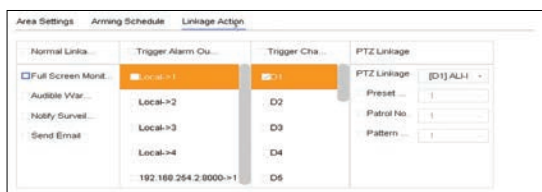
2. Check the **Save VCA Picture** box to capture a live view image of the VCA event.
3. Click the **Enable Intrusion Detection** box to check it (see above).
4. In the **Area Settings** tab:
 - a. Open the **Virtual Plane** drop down list and select a number to be associated with the virtual plane you are creating. For NP series IP cameras you can select either 1, 2, 3 or 4.
 - b. Drag the **Time Threshold** slider left or right to set the minimum amount of time an object must be in the virtual plane to trigger an event.
 - c. Set the **Sensitivity** slider as needed to detect objects entering the plane. This adjustment may require some testing.

SECTION 3: EVENT SETUP

- d. Set the **Percentage** slider as needed. The percentage setting represents the percentage of the plane that needs to be filled by the object entering it to generate an event.
- e. Click the **Draw Region** button. Click a point in the video image to identify one corner of the region, and then click three points in a circular fashion to set the other three corners of the region.
- f. Click the **Stop Drawing** button. A quadrilateral will appear on video image showing the Virtual Plane number you assigned.



- g. Click **Apply** to save your settings.
 - h. To create another virtual line for crossing detection, repeat sub-steps **a** through **f** above with a different region number. You can create up to four virtual planes in the video channel.
5. Click the **Arming Schedule** tab. To configure the arming schedule, refer to **Setup Arming Schedule** in “3.2.1 Camera Face Detection” on page 40.
 6. Click the **Linkage Action** tab.



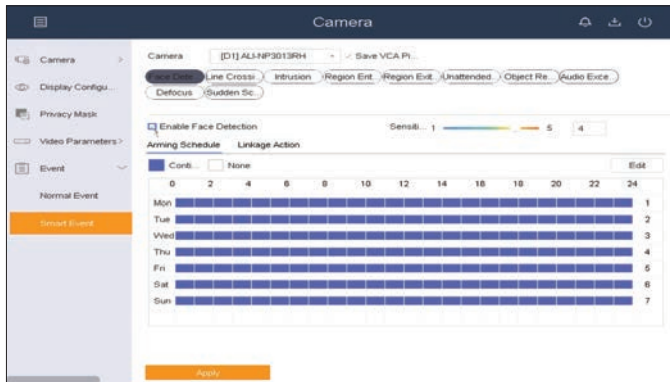
7. In the **Linkage Action** menu, check the boxes for the actions you want to occur when the event is detected.
8. Click **Apply** to save your settings.
9. Repeat steps **1** through **8** above for each camera on your surveillance system as needed.

3.2.4 Region Entrance Detection

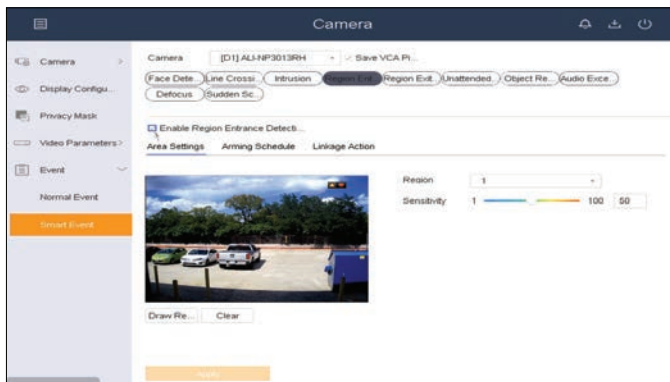
Use Region Entrance detection to detects people, vehicles or other objects which enter a pre-defined virtual plane in the field of view. You can configure up to four virtual planes in on video channel. To use Region Entrance Detection:

1. Open the **Region Entrance Detection** menu:

- a. Go to **Menu | Camera | Event | Smart Event**



- b. Open the drop down list on the camera line, then select the camera you want to configure.
 c. If the Region Entrance option appears in the VCA list at the top of the screen, click on it to configure this feature.



2. Check the **Save VCA Picture** box to capture a live view image of the VCA event.
3. Click the **Enable Region Entrance Detection** box to check it (see above).
4. In the **Area Settings** tab:
 - a. Open the **Region** drop down list and select a number to be associated with the region you are creating. For NP series IP cameras you can select either 1, 2, 3 or 4.
 - b. Set the **Sensitivity** slider as needed to detect objects entering the region. This adjustment may require some testing.

SECTION 3: EVENT SETUP

- c. Click the **Draw Region** button. Click a point in the video image to identify one corner of the region, and then click three points in a circular fashion to set the other three corners of the region.
- d. Click the **Stop Drawing** button. A quadrilateral will appear on video image showing the region number you assigned.



- e. Click **Apply** to save your settings.
 - f. To create another region, repeat sub-steps **a** through **d** above with a different region number. You can create up to four regions in the video channel.
5. Click the **Arming Schedule** tab. To configure the arming schedule, refer to **Setup Arming Schedule** in “3.2.1 Camera Face Detection” on page 40.
 6. Click the **Linkage Action** tab.

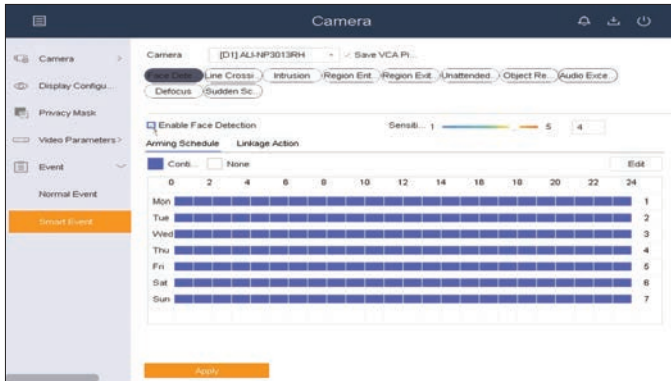


7. In the **Linkage Action** menu, check the boxes for the actions you want to occur when the event is detected.
8. Click **Apply** to save your settings.
9. Repeat steps **1** through **8** above for each camera on your surveillance system as needed.

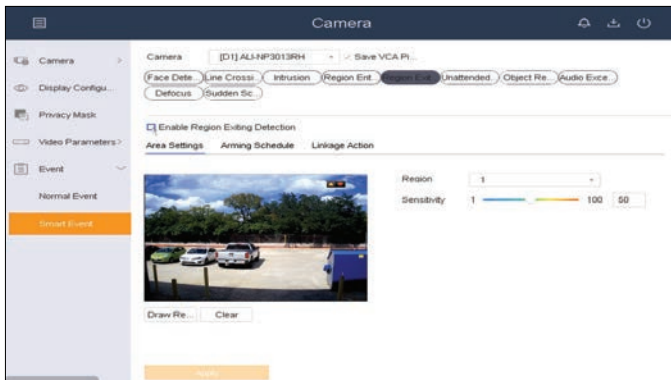
3.2.5 Camera Region Exiting Detection

Use Region exiting detection to detects people, vehicles or other objects which exit from a pre-defined regions of the field of view. You can configure up to four regions in on video channel. To use Region Exit Detection:

1. Open the **Region Entrance Detection** menu:
 - a. Go to **Menu | Camera | Event | Smart Event**



- b. Open the drop down list on the camera line, then select the camera you want to configure.
- c. If the Region Exit option appears in the VCA list at the top of the screen, click on it to configure this feature.



2. Check the **Save VCA Picture** box to capture a live view image of the VCA event.
3. Click the **Enable Region Exiting Detection** box to check it (see above).
4. In the **Area Settings** tab:
 - a. Open the **Region** drop down list and select a number to be associated with the region you are creating. For NP series IP cameras you can select either 1, 2, 3 or 4.
 - b. Set the **Sensitivity** slider as needed to detect objects leaving the region. This adjustment may require some testing.
 - c. Click the **Draw Region** button. Click a point in the video image to identify one corner of the region, and then click three points in a circular fashion to set the other three corners of the region.

SECTION 3: EVENT SETUP

- d. Click the **Stop Drawing** button. A quadrilateral will appear on video image showing the region number you assigned.



- e. Click **Apply** to save your settings.
 - f. To create another region, repeat sub-steps **a** through **d** above with a different region number. You can create up to four regions in the video channel.
5. Click the **Arming Schedule** tab. To configure the arming schedule, refer to **Setup Arming Schedule** in “3.2.1 Camera Face Detection” on page 40.
 6. Click the **Linkage Action** tab.

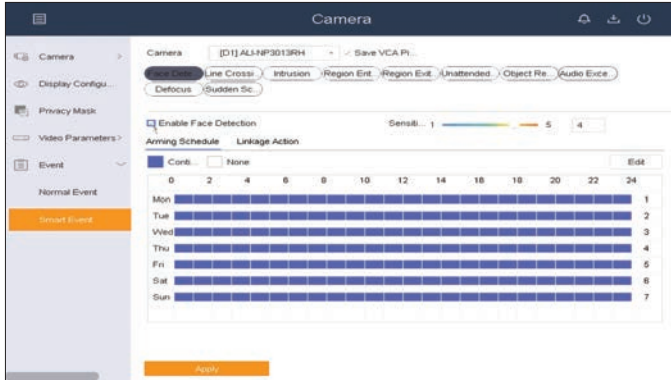


7. In the **Linkage Action** menu, check the boxes for the actions you want to occur when the event is detected.
8. Click **Apply** to save your settings.
9. Repeat steps **1** through **8** above for each camera on your surveillance system as needed.

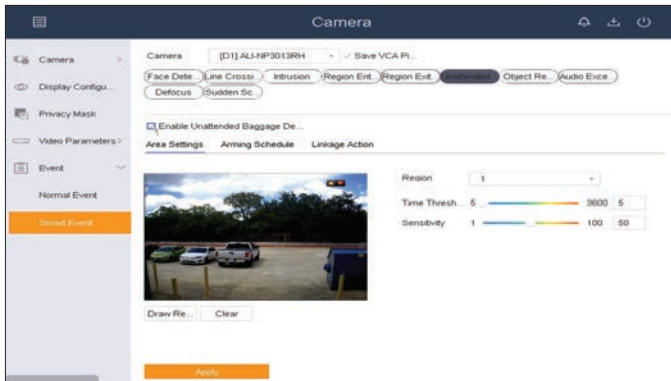
3.2.6 Camera Unattended Baggage

Use Unattended baggage detection to detect when objects such as baggage, a purse, dangerous materials, etc. are left in the pre-defined area of the field of view. To use Unattended Baggage detection:

1. Open the **Region Entrance Detection** menu:
 - a. Go to **Menu | Camera | Event | Smart Event**



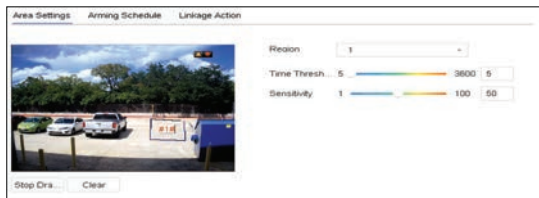
- b. Open the drop down list on the camera line, then select the camera you want to configure.
- c. If the **Unattended** option appears in the VCA list at the top of the screen, click on it to configure this feature.



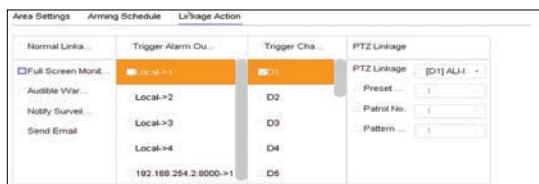
2. Check the **Save VCA Picture** box to capture a live view image of the VCA event.
3. Click the **Enable Unattended Baggage Detection** box to check it (see above).
4. In the **Area Settings** tab:
 - a. Open the **Region** drop down list and select a number to be associated with the region you are creating. You can select either 1, 2, 3 or 4.
 - b. Use the **Time Threshold** slider to set the amount of time the object must stay in the region before an event is generated.
 - c. Set the **Sensitivity** slider as needed to detect objects in the region. This adjustment may require some testing.

SECTION 3: EVENT SETUP

- d. Click the **Draw Region** button. Click a point in the video image to identify one corner of the region, and then click three points in a circular fashion to set the other three corners of the region.
- e. Click the **Stop Drawing** button. A quadrilateral will appear on video image showing the region number you assigned.



- f. Click **Apply** to save your settings.
 - g. To create another region, repeat sub-steps **a** through **e** above with a different region number. You can create up to four regions in the video channel.
5. Click the **Arming Schedule** tab. To configure the arming schedule, refer to **Setup Arming Schedule** in “3.2.1 Camera Face Detection” on page 40.
 6. Click the **Linkage Action** tab.

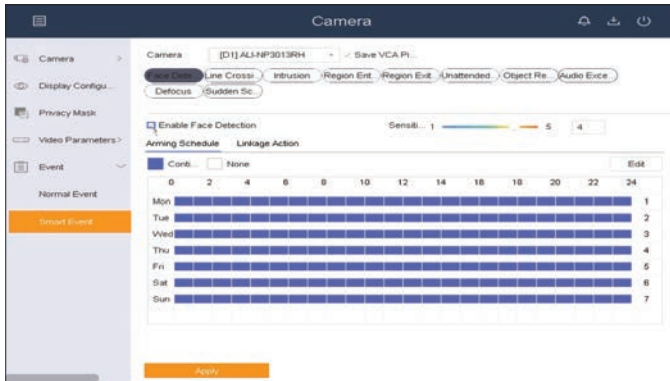


7. In the **Linkage Action** menu, check the boxes for the actions you want to occur when the event is detected.
8. Click **Apply** to save your settings.
9. Repeat steps **1** through **8** above for each camera on your surveillance system as needed.

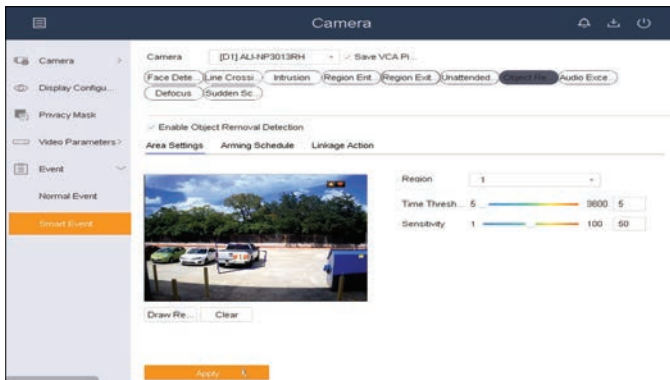
3.2.7 Camera Object Removal Detection

Use Object removal detection to detects when an object, such as an exhibit on display, is removed from the pre-defined area of the field of view. To use Object Removal detection:

1. Open the **Region Entrance Detection** menu:
 - a. Go to **Menu | Camera | Event | Smart Event**



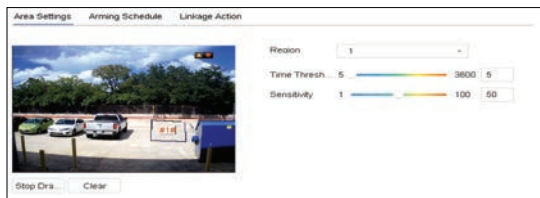
- b. Open the drop down list on the camera line, then select the camera you want to configure.
- c. If the **Object Removal** option appears in the VCA list at the top of the screen, click on it to configure this feature.



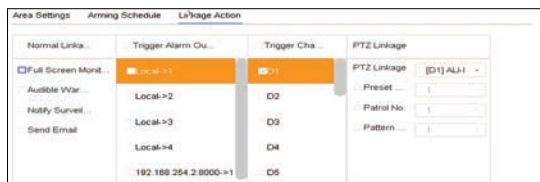
2. Check the **Save VCA Picture** box to capture a live view image of the VCA event.
3. Click the **Enable Object Removal Detection** box to check it (see above).
4. In the **Area Settings** tab:
 - a. Open the **Region** drop down list and select a number to be associated with the region you are creating. For NP series IP cameras you can select either 1, 2, 3 or 4.
 - b. Use the **Time Threshold** slider to set the amount of time the object is removed from the region before an event is generated.
 - c. Set the **Sensitivity** slider as needed to detect objects removed from the region. This adjustment may require some testing.

SECTION 3: EVENT SETUP

- d. Click the **Draw Region** button. Click a point in the video image to identify one corner of the region, and then click three points in a circular fashion to set the other three corners of the region.
- e. Click the **Stop Drawing** button. A quadrilateral will appear on video image showing the region number you assigned.



- f. Click **Apply** to save your settings.
 - g. To create another region, repeat sub-steps **a** through **f** above with a different region number. You can create up to four regions in the video channel.
5. Click the **Arming Schedule** tab. To configure the arming schedule, refer to **Setup Arming Schedule** in “3.2.1 Camera Face Detection” on page 40.
 6. Click the **Linkage Action** tab.

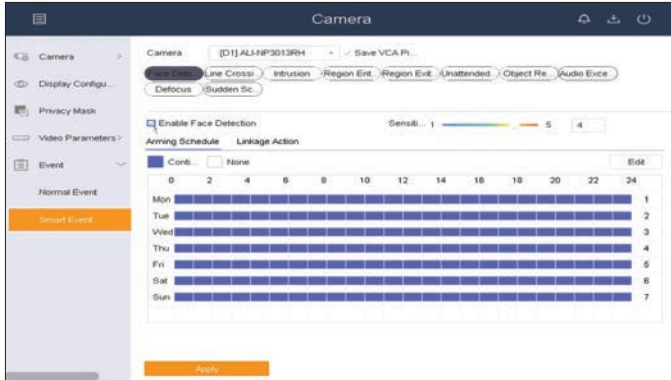


7. In the **Linkage Action** menu, check the boxes for the actions you want to occur when the event is detected.
8. Click **Apply** to save your settings.
9. Repeat steps **1** through **8** above for each camera on your surveillance system as needed.

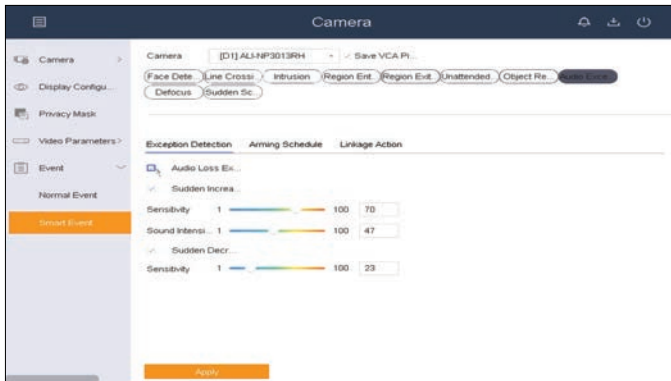
3.2.8 Camera Audio Exception Condition

Use Audio exception detection to detects when an abnormal sound, such as the sudden increase / decrease of the sound intensity, occurs in the surveillance area. A microphone must be attached to the camera you are configuring, and the camera channel must be configured for audio streaming. To configure Audio Exception:

1. Open the **Region Entrance Detection** menu:
 - a. Go to **Menu | Camera | Event | Smart Event**



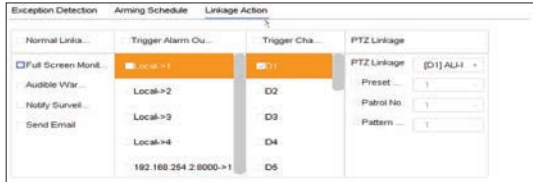
- b. Open the drop down list on the camera line, then select the camera you want to configure.
- c. If the **Audio Exception** option appears in the VCA list at the top of the screen, click on it to configure this feature.



2. Check the **Save VCA Picture** box to capture a live view image of the VCA event.
3. In the Exception Detection tab:
 - a. Click the **Audio Loss Exception** box to check it (see above) to use this feature.
 - b. Click the **Sudden Increase of Sound Intensity Detection** button (see above) to use this feature, then:
 - i. Set the **Sensitivity** slider to set the high sound level minimum threshold (may require testing).
 - ii. Set the **Sound Intensity Threshold** slider to set the minimum threshold (may require testing).
 - c. Click the **Sudden Decrease of Sound Intensity Detection** button (see above) to use this feature, then:
 - i. Set the **Sensitivity** slider to set the a low sound level maximum threshold (may require testing).

SECTION 3: EVENT SETUP

- Click **Apply** to save your settings.
- Click the **Arming Schedule** tab. To configure the arming schedule, refer to **Setup Arming Schedule** in “3.2.1 Camera Face Detection” on page 40.
- Click the **Linkage Action** tab.

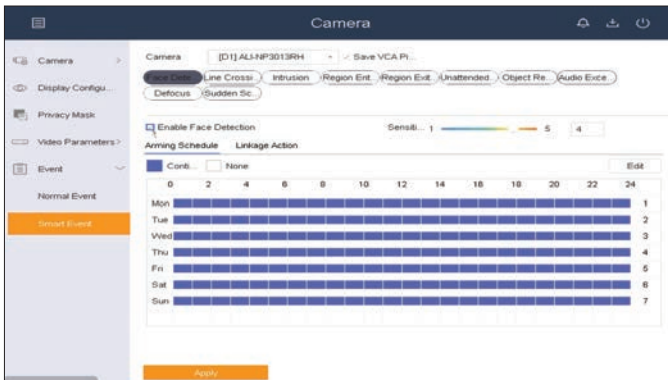


- In the **Linkage Action** menu, check the boxes for the actions you want to occur when the event is detected.
- Click **Apply** to save your settings.
- Repeat steps 1 through 8 above for each camera on your surveillance system as needed.

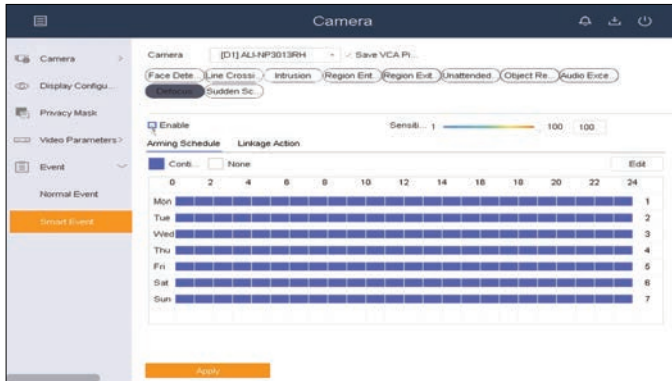
3.2.9 Camera Defocus Detection

Use Defocus detection to sense when image blur, caused by defocus of the lens, occurs. To use camera Defocus Detection:

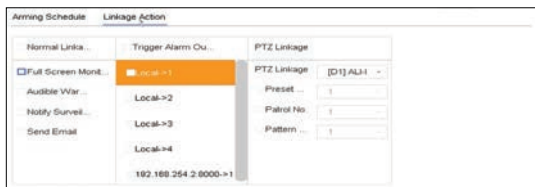
- Open the **Region Entrance Detection** menu:
 - Go to **Menu | Camera | Event | Smart Event**



- Open the drop down list on the camera line, then select the camera you want to configure.
- If the **Defocus** option appears in the VCA list at the top of the screen, click on it to configure this feature.



2. Check the **Save VCA Picture** box to capture a live view image of the VCA event.
3. Click the **Enable** box to check it (see above).
4. Adjust the **Sensitivity** slider to set the amount of defocus threshold (may require testing).
5. Click the **Arming Schedule** tab. To configure the arming schedule, refer to **Setup Arming Schedule** in “3.2.1 Camera Face Detection” on page 40.
6. Click the **Linkage Action** tab.



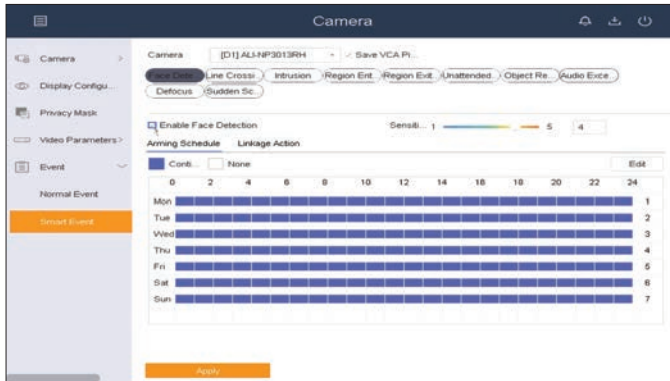
7. In the **Linkage Action** menu, check the boxes for the actions you want to occur when the event is detected.
8. Click **Apply** to save your settings.
9. Repeat steps 1 through 8 above for each camera on your surveillance system as needed.

3.2.10 Camera Sudden Scene Change Detection

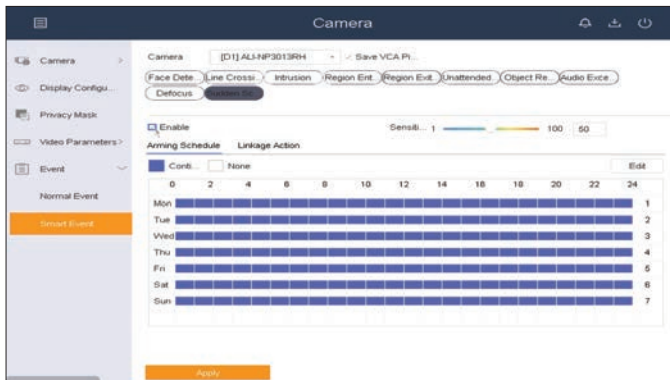
Use Scene change detection to detects the change of surveillance environment affected by an external factor, such as the intentional rotation of the camera. To use Sudden Scene Change Detection:

1. Open the **Region Entrance Detection** menu:
 - a. Go to **Menu | Camera | Event | Smart Event**

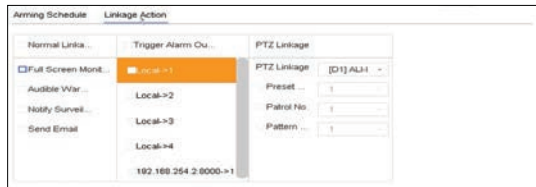
SECTION 3: EVENT SETUP



- b. Open the drop down list on the camera line, then select the camera you want to configure.
- c. If the **Sudden Scene** option appears in the VCA list at the top of the screen, click on it to configure this feature.



2. Check the **Save VCA Picture** box to capture a live view image of the VCA event.
3. Click the **Enable** box to check it (see above).
4. Adjust the **Sensitivity** slider to set the amount of scene change (may require testing).
5. Click the **Arming Schedule** tab. To configure the arming schedule, refer to **Setup Arming Schedule** in “3.2.1 Camera Face Detection” on page 40.
6. Click the **Linkage Action** tab.



7. In the **Linkage Action** menu, check the boxes for the actions you want to occur when the event is detected.
8. Click **Apply** to save your settings.
9. Repeat steps 1 through 8 above for each camera on your surveillance system as needed.

SECTION 4

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.

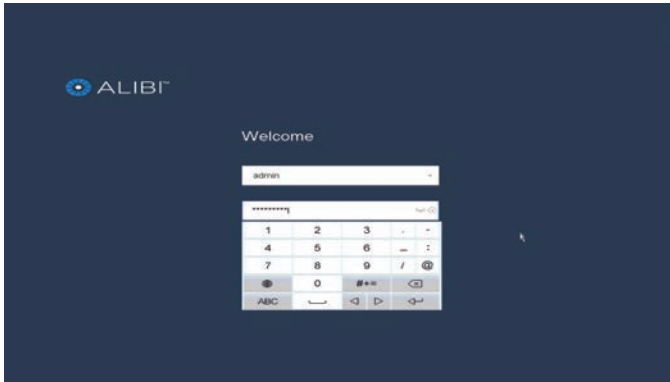
4.1 Starting Up

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 lit. A splash screen will usually appear on the monitor within three minutes.
4. Typically, one of two login screens will appear, depending on how the system was activated:
 - If the unlock pattern was setup during system activation for an *admin* login, the unlock pattern screen will appear. In this screen swipe the unlock pattern across the matrix with the mouse to login as the *admin* user, or click **Switch User** and login with a username and password as shown below.



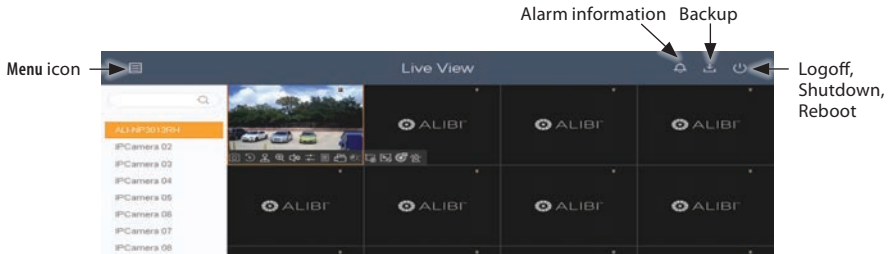
- If an unlock pattern was not setup during system activation, or you chose to login as a user other than *admin*, a typical login screen will open. Enter your username and password, then click Login.



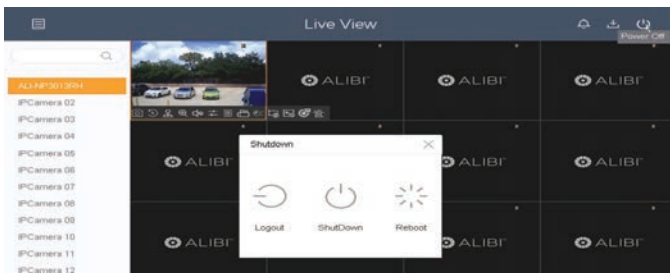
4.2 Shutdown

To shut down the NVR:

1. Right click anywhere on the Live View desktop to open a control bar across the top of the screen. The control bar also appears over most configuration windows.



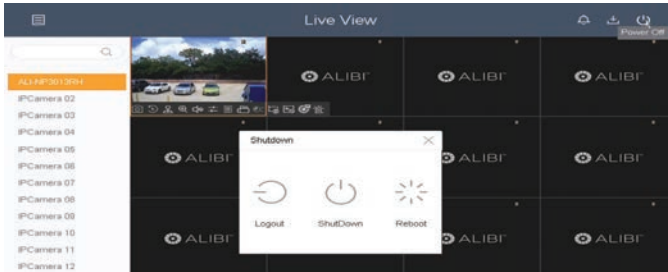
2. Click the **Power Off** icon in the upper right corner, and then click the **Shutdown** icon in the pop-up menu.



4.3 Reboot

In the **Shutdown** menu shown in “4.2 Shutdown” on page 61, you can also reboot the NVR.

1. Open the Shutdown menu by clicking **Power Off** icon.



2. In the **Shutdown** pop-up menu, click **Reboot**.
3. Allow the NVR to fully reboot.
4. Login to the NVR as described in “4.1 Starting Up” on page 60.

SECTION 5

Live View Screen

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-screen mode. The Live View screen can be configured to display up to 64 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.

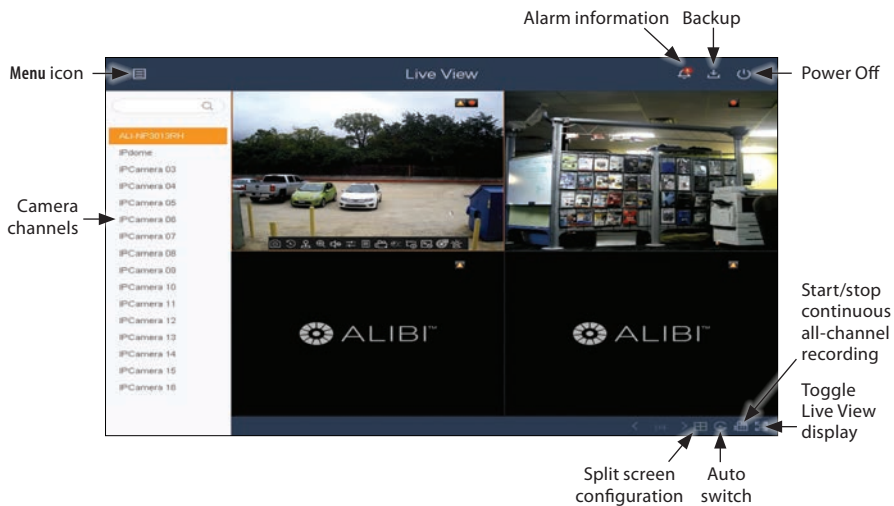
The recorder can support up to three monitors if it provides both VGA, HDMI, and CVBS video out ports.

5.1 Live View utility display

Open the Live View utility display by right-clicking anywhere on the Live View display shown above. Right click on the screen again to return to the normal Live View display. In the Live View utility display, you can:

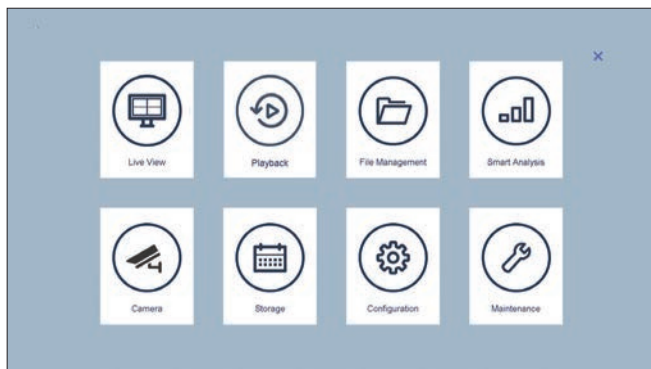
- Access the Menu
- Open the Events list and play video of events.
- Backup video from a camera channel
- Logout, Shutdown or Reboot the system
- Change the split screen configuration and assign camera channels to viewing frames
- Start and stop all-day continuous recording on all channels

SECTION 5: LIVE VIEW SCREEN



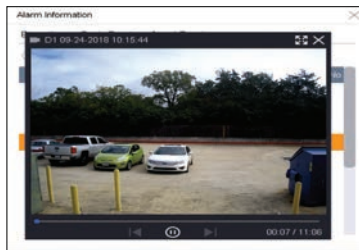
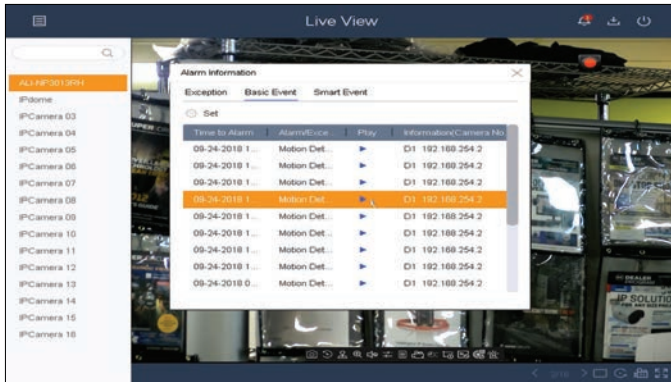
5.1.1 Open Menu screen

In the screen shown above, click the **Menu icon** to open the firmware menu Menu icon display. Click on the icon in this window to open the configuration menus for that area of the system.



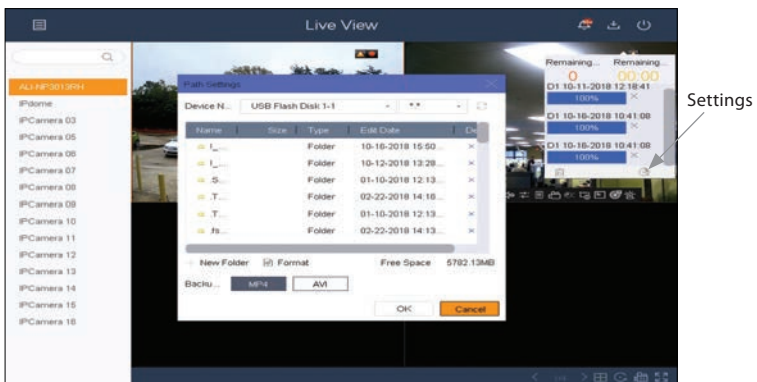
5.1.2 View alarm information

Click the alarm information icon to open the list of recent alarms, You can click the play icon in the list to watch recorded video associated with the alarm.



Backup

Click the **Backup** icon in the Live View header bar to ...**DEFINE HERE WHAT it is about** To export these files:



SECTION 5: LIVE VIEW SCREEN

1. Insert a flash drive into an unused USB port on the recorder.
2. In the Backup popup menu, click to select the files you want to backup, and then click the **Settings** icon. The Path Settings popup window will open.
3. In the **Path Settings** menu, open the **Device** field drop down list, and then select the USB flash drive.
4. Double click on the folder in the drive where you want to backup files (see above). Use the buttons on this menu to create a **New Folder** or **Format** the drive if necessary.
5. Click **MP4** or **AVI** (for files in H.264 format only) to select the exported file format you prefer, and then click **OK** to export the file(s).

NOTE • You can hover the mouse cursor over any shortened file or directory name to reveal the complete name.

Power Off

Click the Power Off icon to Logoff, Shutdown or Reboot the system. See “SECTION 1 Systems Overview” on page 1

Change split screen configuration

- Click the Split icon (see above) to show split configuration options for the Live View screen.
- To re-position a camera in the screen, click on the video frame to highlight it (will be surrounded with an orange border) and then click on the camera channel in the left frame. Video from the camera will appear in (move to) the selected video frame.

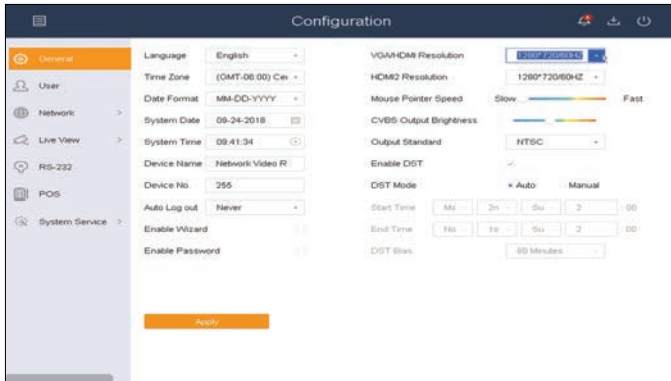
Start and stop continuous recording

Click the camera icon in the footer to start or stop continuous recording on all channels.

5.2 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:

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

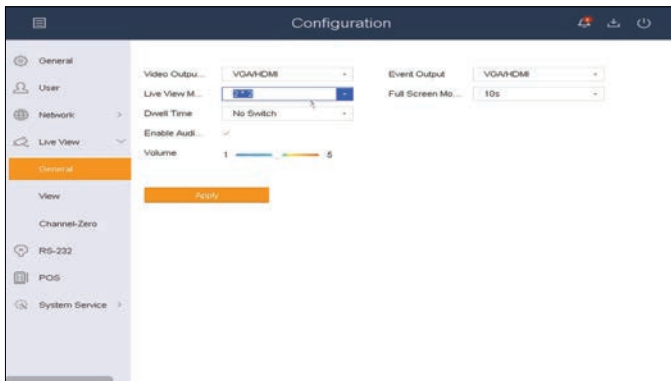


Use the screen above to select the VGA/HDMI and HDMI2 resolutions for the VGA and HDMI monitors you are using, and then click the **Apply** button at the bottom of the screen.

5.3 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 | General**

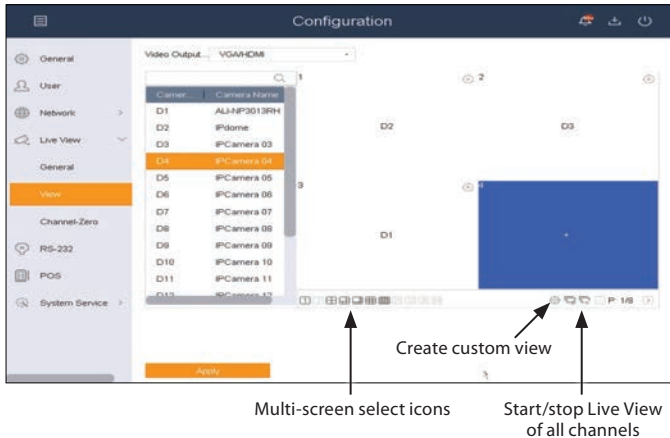


Adjust the settings in the screen as needed:

- **Video Output Interface:** Designates the output to configure the settings for. Option includes only VGA / HDMI and HDMI2 if supported by the recorder.

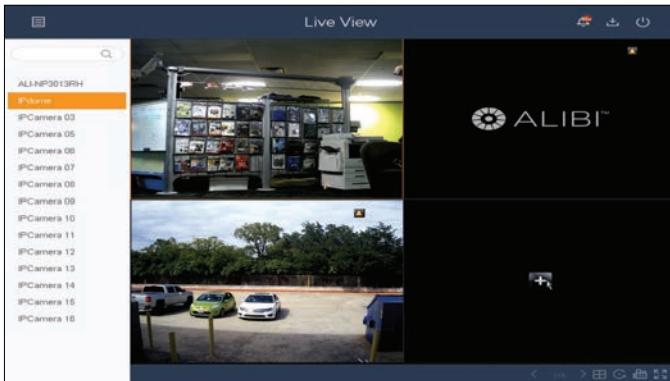
SECTION 5: LIVE VIEW SCREEN

- **Live View Mode:** Designates the display mode (screen split) to be used for Live View. **1 * 1** is a single camera view. Other options are **2 * 2**, **1 + 5**, **1 + 7**, **3 * 3**, etc. Options depend on the number of channels supported by the recorder.
 - **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 CVBS/Channel-Zero, VGA/HDMI, HDMI2 (if supported). **NOTE:** If you configure a camera event with the full-screen monitoring linkage action, the Event Output screen will show full screen video of the camera channel when the event occurs for the duration set in Full Screen Monitoring Dwell Time.
 - **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. Open the Live View **View** screen. Go to **Menu | Configuration | Live View | View**.

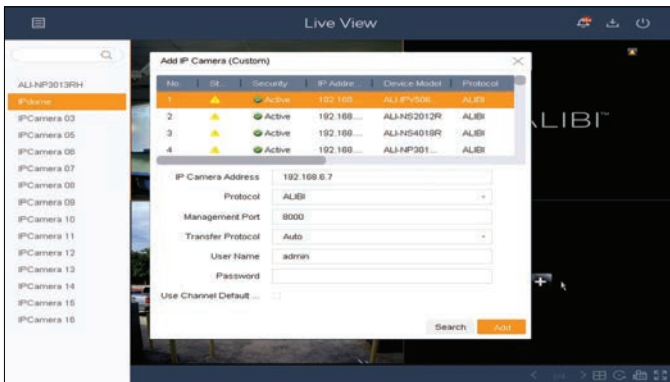


4. To use this screen:
 - a. Click the single- or multi-screen select icon for the screen split you prefer. In the example shown above, a 4-screen (2×2) view is selected.
 - b. Click a viewing screen (D1 or D2 or D3 ..), then double-click the camera in the list on the left that you want to show there. When the selection is made, 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.
 - c. If you click the icon in the upper right corner of a viewing screen (D1 or D2 or D3 ..), the viewing screen number will change to a "+" symbol, and you can assign a network camera to that viewing position from the Live View display.
 - d. Click the **Apply** button to save your settings.

- e. Right click on this menu to return to the Menu display. In the Live View display shown below, notice that the positions of the camera channels changed.



- f. To add a network camera, click the “+” icon the lower right frame. Use the pop-up menu to add a network camera.







- 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.

5.4 Live View Status icons

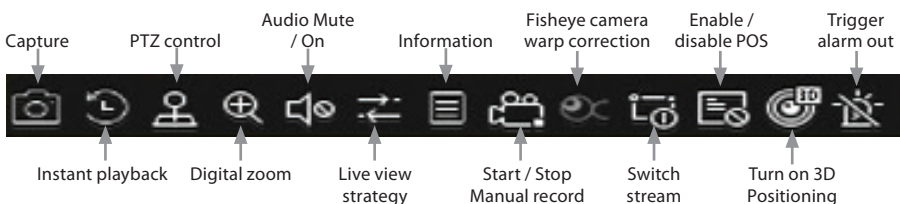
In the **Live** view mode, icons can appear in the upper-right of the screen for each channel, showing the status of the record and alarm in the channel.

SECTION 5: LIVE VIEW SCREEN

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.

5.5 Quick Setting Toolbar

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



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

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

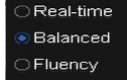
PTZ Control: If the camera supports PTZ control, clicking this icon opens the PTZ screen. See “SECTION 6 PTZ Controls” on page 77 for more information.

Digital Zoom: To use this feature:

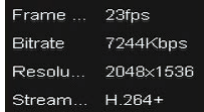
- Click on the spot in the video image, and then use the mouse scroll wheel to zoom in or out at that spot.
- Right-click the mouse to cancel the zoom feature.

Audio mute / ON: Click this icon to enable or disable audio output. When audio is enabled, a volume control slider appears above the icon.

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.



Start - Stop Manual Recording: Click to start, click again to stop manual recording of the camera channel.

Fisheye Camera warp correction: This feature is only available for cameras with fisheye functionality.

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

3D Positioning: Enable this feature to zoom in or zoom out of areas of the video frame. With 3D Positioning ON, drag the mouse cursor down and to the right over the area you want to zoom in on. Or, drag the cursor up and to the left over the area you want to zoom out of. Right click on the video frame to disable this feature.

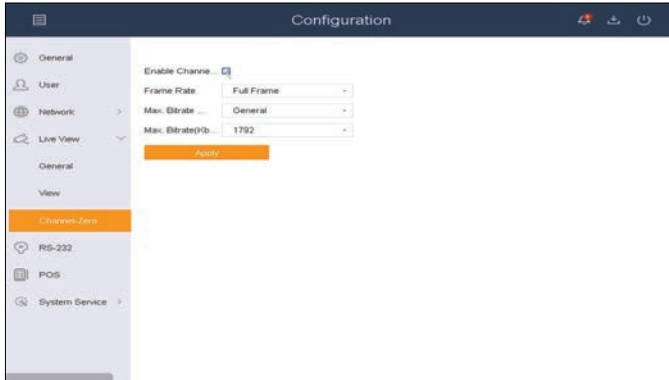
Switch to Sub-Stream: Hover the mouse over this icon to play the sub-stream video. Repeat this action to return to the Main stream.

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

5.6 Channel-Zero Encoding

Use the Channel-Zero 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**



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.

5.7 Adding network cameras

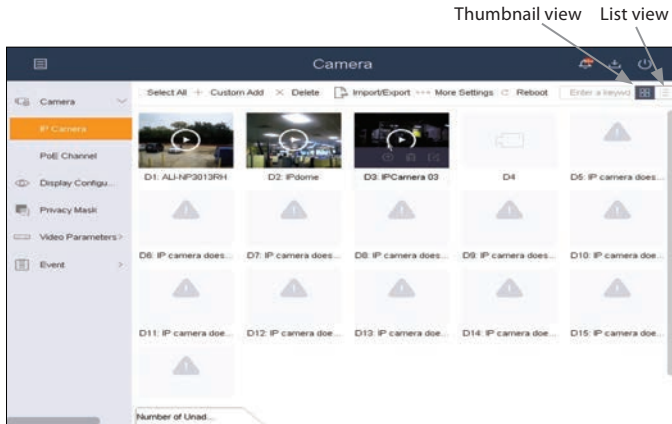
IP cameras can connect to the NVR either through the 4-, 8-, or 16-port integrated Ethernet switch on the back panel of the NVR, or through the LAN the NVR is connected to. IP cameras connected to the IP ports on the NVR back panel are automatically added to the system by the NVR. Cameras that exist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

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. For example, the ALI-NVR5232P NVR can monitor up to 32 cameras, 16 attached to the internal PoE network switch, and 16 accessible across the network.

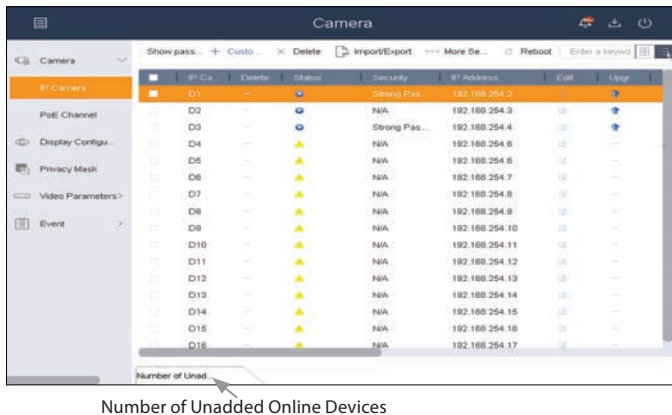
NOTE For a lists IP cameras compatible with your NVR, refer to: "APPENDIX C NVR Compatible Cameras" on page 208.

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 192.168.3.3 will be added to NVR channel D4.

1. Open the IP Camera menu. Go to **Menu | Camera | IP Camera**.

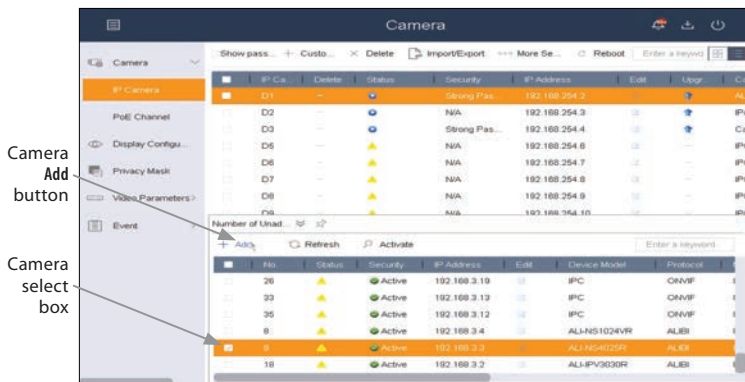


2. Click the **List** button in the upper right corner.

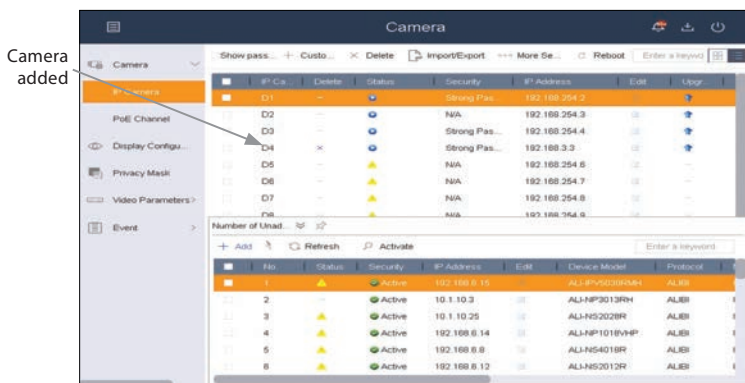


- a. Click the **Number of Unadded Online Devices** button at the bottom of the screen (see above). A split list will open, with the upper list showing the cameras added to the NVR, and the lower list showing the cameras discovered on the network that can be added.

SECTION 5: LIVE VIEW SCREEN



- b. In the screen above, check the select box(es) for the camera(s) you want to add, and then click the **Add** button. In this example, one camera was selected.

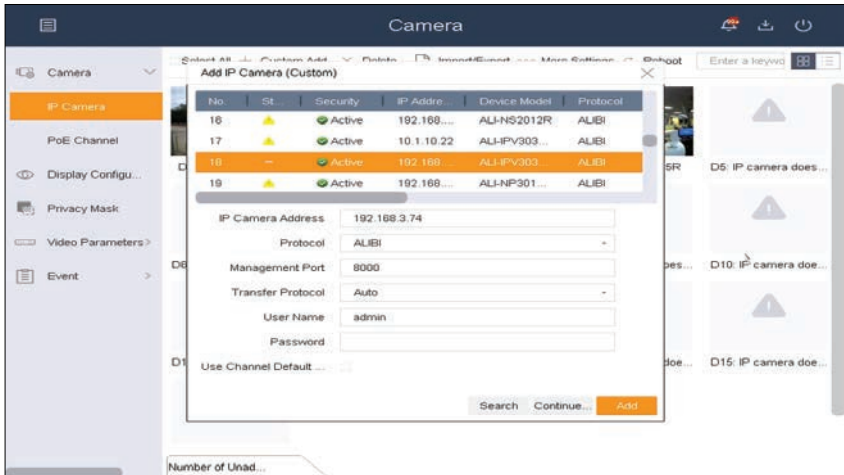


- c. Repeat sub-steps **a** and **b** above to add additional cameras. NVRs limit the number of network cameras you can add.

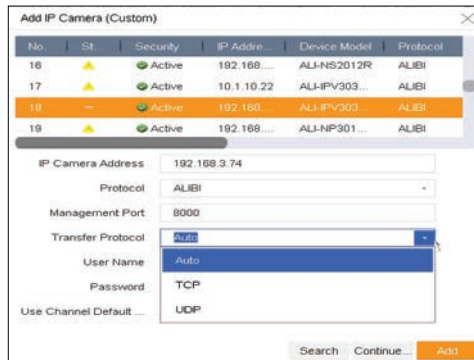
5.7.1 Custom Add IP Camera

The Custom Add feature provides a way to add network cameras to the NVR that have a different protocol, management port, transfer protocol, etc from Alibi cameras with default setup parameters. To use this feature:

1. Open the IP Camera menu. Go to **Menu | Camera | IP Camera**.
2. Click the **Custom Add** button at the top of the window. The upper portion of the **Add IP Camera (Custom)** popup window lists network cameras that are accessible from the NVR.

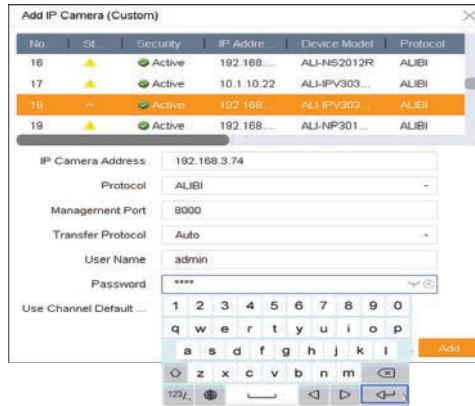


3. Scroll through the list of IP cameras, and then click on the one you want to add (see above).
4. Open the **Protocol** drop down list and select the protocol to use with the camera. You can also define up to 16 custom protocols to use. You can also check the **Use Default Channel Password** select box if applicable.
5. Set the **Management Port**, if different than 8000 (default).
6. Open the **Transfer Protocol** drop down list and select the transfer protocol to use with the camera.



7. Enter the Administrator **User Name** and **Password** in the appropriate fields. You can also check the Use Default Channel Password select box at the bottom of the menu if appropriate.

SECTION 5: LIVE VIEW SCREEN



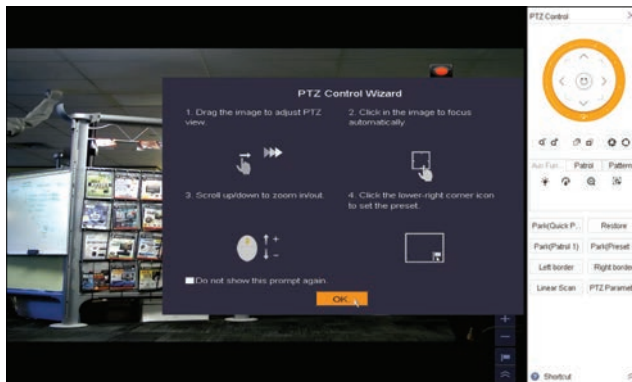
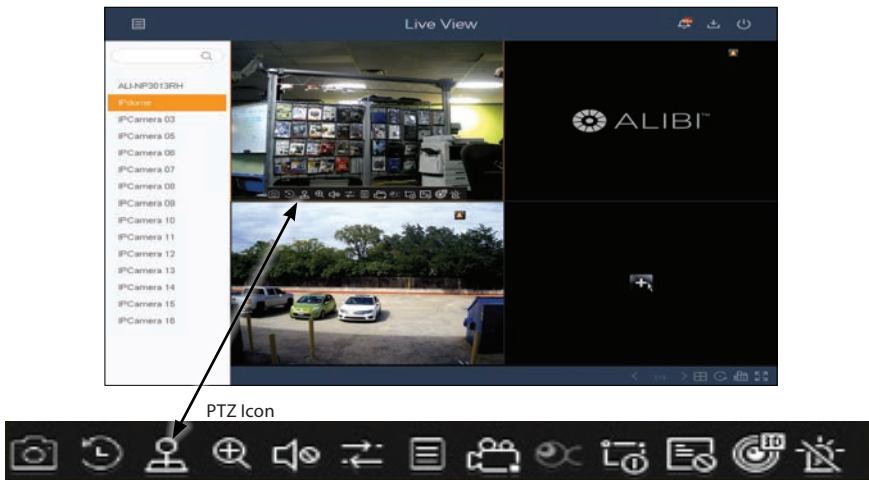
- Click **Add** to save your settings and connect the camera to the recorder.

SECTION 6

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 targets (called Presets), perform patrols (i.e., to move from Preset to Preset with a dwell time), and record and save patterns, a recording of the manually controlled 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.

To open the PTZ Control screen, click the PTZ icon in the camera Quick-setting toolbar.



PTZ Control screen with field of view

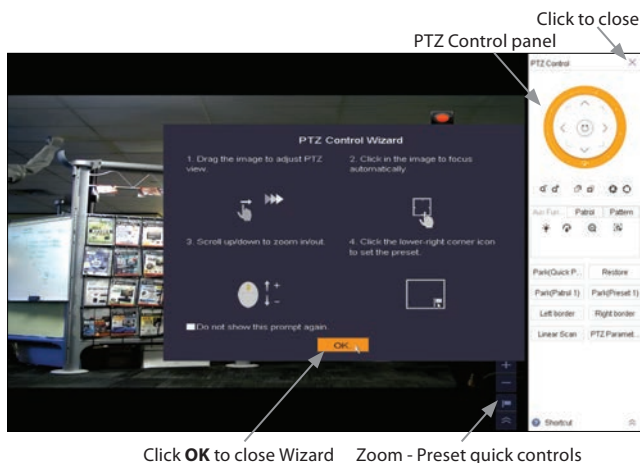
The PTZ Control screen includes features to control your camera manually, and configure it to automatically scan the important surveillance targets it is installed to monitor, and quickly move to those targets on command. PTZ cameras supported by this firmware usually include three types of movement commands that should be configured to use your camera most effectively:

- **Presets:** Presets are easily configurable instruction sets that move when called move the camera to point at a specific surveillance target. Presets include direction, zoom, iris and focus setting, and may include other settings.
- **Patrols:** Patrols are composed of a string of presets, with a dwell time associated with each preset. For instance, when a patrol is executed, it moves the camera to point at the surveillance target of the first preset in the string, for a configurable dwell time (for instance 10 seconds), then it calls the next preset in the string to moves the camera to that target and stay there for its dwell time, etc. You can configure up to four (4) presets, called Patrol1, Patrol2, etc with this firmware.
- **Pattern:** A Pattern is 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 (Pattern1) with this firmware.

NOTE *The presets, patrols and patterns you configure must be supported by the PTZ protocol of your camera.*

6.1 PTZ Control screen

You can open the PTZ Control panel in the **Live View** by left clicking on the image from the PTZ camera, and then click the PTZ icon on the Quick Settings toolbar (see above).



In the screen shown above:

- Click the orange **OK** button to close the **PTZ Control Wizard** pop-up help window.
 - Check the **Do not show this ...** box to block this window when you open the PTZ Control screen.
 - You can drag your finger (for touch screens) or mouse across the screen as shown in the wizard to move the camera view after you close the help window:

- * Drag on the image to move the camera view in that direction.
 - * Click in the image to focus automatically.
 - * Scroll the mouse up / down to zoom in / out.
 - * Click the lower right corner icon to set the preset.
- Click the **x** in the upper right corner or right click on the video window to return to the **Live View** screen.

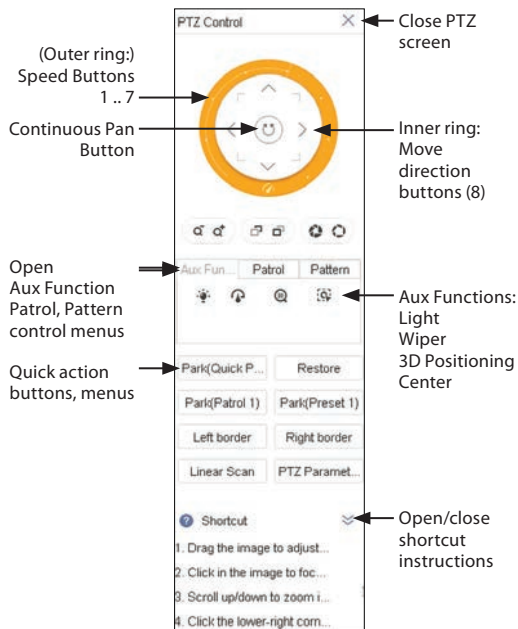
6.1.1 Pointing the camera

You can point the camera at a surveillance target in three ways:

- Dragging your finger (for touch screens) or mouse cursor across the video window in the direction you want the camera to move.
- Clicking any one of the eight (8) direction buttons on the control panel GUI to point the camera in that direction. You can set the speed at which the camera pans or tilts by clicking one of the speed buttons on the outer (orange) ring of the GUI.
- By programming a Preset to point the camera at a specific target, then **Call**ing that preset.

6.1.2 PTZ Control panel

Use the PTZ control panel that appears in the right frame to control motion of the camera, configure and call Presets, Patrols and Patterns, and quickly set the zoom, focus and iris.



SECTION 6: PTZ CONTROLS

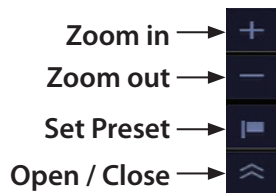
Feature of the PTZ control panel include:

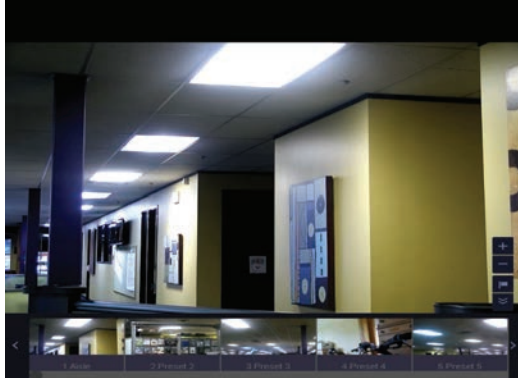
- **Outer ring speed buttons:** Click one of the seven (7) buttons to set the speed at which the camera moves when you click one of the eight (8) direction buttons.
- **Continuous pan button:** Click to start / stop continuous pan to the right.
- **Open Aux Function, Patrol, Pattern control menus:** Click the tab to open the menu for that feature.
- **Quick action buttons:** These buttons include:
 - **Park (Quick Patrol):** The camera initiates a patrol from Preset 1 to Preset 32 (if predefined) after the camera park time*. Undefined preset are skipped.
 - **Restore:** Resets the camera and loads its initial Factory image parameters.
 - **Park (Patrol 1):** The camera initiates a starts move according to the Patrol 1 after the camera park time*. Patrol 1 must be defined.
 - **Park (Preset 1):** The camera initiates a move to Preset 1 after the camera park time*. Preset 1 must be defined.
 - **Linear Scan:** Causes the camera to pan left and right between the limits of the Left border and Right border.
 - **Left border:** Use this button to set the left limit for a Linear Scan.
 - **Right border:** Use this button to set the right limit for a Linear Scan.
- **Close PTZ screen:** Click the **x** to return to the Live View screen.
- **Inner ring speed buttons:** Click repeatedly to move the camera in one of the eight (8) directions shown.
 - **Aux Function** tab shown includes icons to:
 - Turn on / off the **light** and **wiper**, if supported by the camera.
 - Begin **3D Positioning** mode. In this mode, you can drag a rectangle across any area of the video window to command the camera to center on that position. Small rectangles cause the camera to zoom in, large rectangles to zoom out (within the capabilities of the camera).
 - **Patrol** tab: Enables you to **Set, Call, and Stop** Patrols.
 - **Pattern** tab: Enables you to **Record, Call and Stop** a pattern (Pattern1).
- **Open / close shortcut instructions:** When open, provides a list of on-screen features of the PTZ video window.

* **Park Time:** Certain speed dome models can be configured to start a predefined park action (scan, preset, patrol and etc.) automatically after a period of inactivity (park time). The park time can be set only via the PTZ camera configuration interface. The default period is 5 seconds.

6.1.3 Zoom - Preset quick controls

Zoom - Preset quick control buttons are used to quickly zoom in or out, to set a preset and to OPEN and COLAPSE thumbnail views of presets that are configured (see below) and quickly move the camera to that view.





PTZ view with Preset thumbnails open

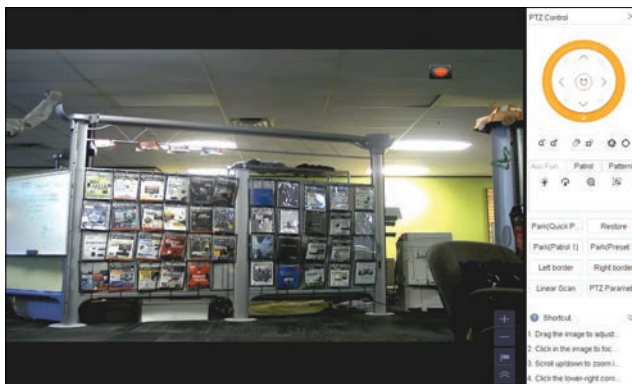
6.2 Configuring PTZ settings

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.

NOTE

If PTZ cameras are controlled through the RS-485 interface, check that the PTZ and the NVR are connected and configured properly. Use the instructions with the controller, and the OSD menus in the camera to configure PTZ settings.

1. To control or setup controls for a PTZ camera, click on the camera you want to control in the Live View interface, and then click the PTZ icon in the quick setting toolbar.



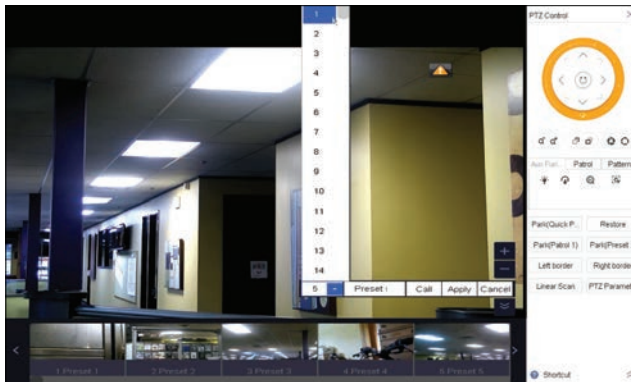
2. Click **OK** to lose the PTZ Control Wizard.

6.2.1 Setting Presets

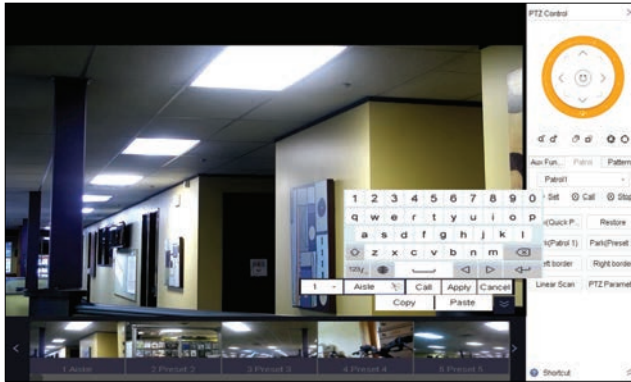
A Preset is a pre-configured setting of a PTZ camera that usually includes, it's direction, zoom, iris setting and focus, and may include other settings. Follow the steps to set the Preset location which you want the PTZ camera to point to when an event takes place. A PTZ camera has up to 255 presets,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

NOTE *Some Presets are factory set, and should not be changed. Refer to the documentation for your PTZ camera to see which Presets you can configure. Additionally, the presets, patrols and patterns you configure must be supported by the PTZ protocol you use.*

1. Open the PTZ Control Screen.
2. Click **OK** in the PTZ Control Wizard to close it.
3. Use the inner ring buttons on the PTZ motion control GUI to point the camera at the field of view you want to create a preset for.
4. Click the **Set Preset** button in the Zoom - Preset quick controls panel.



5. Open the number field drop down list and select the number you want to use for the Preset (see above).
6. Click **Apply**.
7. Click **Preset** in the name field, and then use the virtual keyboard to enter a description for the preset you created. Click the Enter key in the lower right corner of the keyboard.



After saving your entry, the name will be shown in the thumbnail for Preset1.

Call preset - move to a preset

You can quickly move the camera to a preset you've created in two ways:

- Using **Open Preset**: Click the Open Preset icon in the Zoom - Preset quick controls panel, and then click on the Preset thumbnail you want to advance to.
- Using the **Set Preset** panel: Click the Set Preset icon in the Zoom - Preset quick controls panel, open the number field drop down list and select the number of the preset you want to advance to, and then click **Call**.

6.2.2 Setting patrols

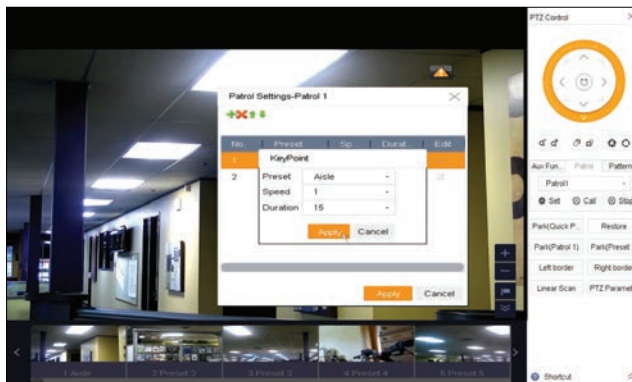
Patrols can be set to position a PTZ camera to a Preset (KeyPoint) and hold it there for a set duration (in seconds) before moving on to another Preset number for a set duration. To create Preset positions for the camera, see "6.2.1 Setting Presets" on page 82. You can create up to 4 patrols, numbered 1 .. 4. To create a Patrol:

1. Click the **Patrol** tab in the PTZ Control Panel.
2. Open the drop down list in the Patrol field, and then select the patrol number you want to define (Patrol1 .. Patrol 4).
3. Click the **Set** icon.



SECTION 6: PTZ CONTROLS

- Click the plus icon (+) to open the Keypoint menu. This menu is used to set a view in the patrol, with a specific duration.



In the KeyPoint menu:

- Open the **Preset** drop down list, and select the first camera view you want the patrol to move to.
 - Open the **Speed** drop down list, and select the speed at which you want the camera to move there.
 - Open the **Duration** drop down list, and use the slider to the right to select the number of seconds you want the camera to dwell on that preset. Click on that number in the **Duration** field.
 - Click **Apply**. An entry will appear in the Patrol Settings list for the KeyPoint you created.
 - Click the plus icon (+) to in the Patrol Settings menu to add an additional KeyPoint to the Patrol, and then repeat the sub-steps above with a different Preset to define the next camera view in the patrol.
- When finished defining all the KeyPoints for the Patrol, click **Apply** in the Patrol Settings menu to save your settings.
 - Click **Cancel** to close the Patrol Settings menu.

Editing a patrol

In the Patrol Settings menu for the patrol you created:

- Click the KeyPoint you want change.
 - To change the Preset number:
 - Click the Edit icon in the right column.
 - Open the **Preset** drop down list, then select the preset you want to assign to the KeyPoint.
 - Open the **Speed** drop down list, then select the speed at which you want to move to the preset.
 - Open the **Duration** drop down list, and use the slider to the right to select the number of seconds you want the camera to dwell on that preset. Click on that number in the **Duration** field.

- v. Click **Apply** in the KeyPoint menu.
- b. To change the order of the KeyPoints:
 - i. Click on the KeyPoint in the list you want to reposition.
 - ii. Click the up arrow or down arrow icon to change the position in the list.
 - iii. Click **Apply** in the KeyPoint menu.
2. Click **Apply** in the Patrol Settings menu.
3. Click **Cancel** to close the Patrol Settings menu.

Call patrol

To execute a Patrol you created:

1. Click the **Patrol** tab in the PTZ Control Panel.
2. Open the drop down list in the **Patrol** field, and then select the number of the patrol you created that you want to execute.
3. Click the **Call** icon. The patrol you selected will execute and repeat indefinitely.
4. To stop the Patrol, click the **Stop** icon.

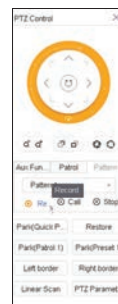
6.2.3 Setting a pattern

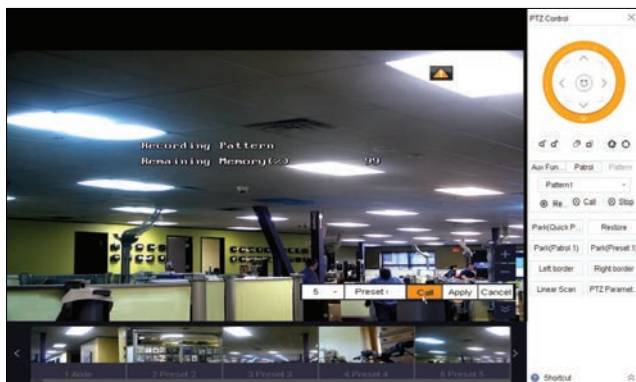
A Pattern can be created by recording the movements of the camera. You can then call the pattern you recorded to repeat the movement. When recording the movements of the camera, you can Call the presets and patrols you created. Once **Called**, the pattern will execute continuously until it is stopped.

You can record only one pattern (Pattern 1). During the recording, an on-screen display shows how much memory allocated for the recording remains.

To define a pattern:

1. Click the **Pattern** tab in the PTZ Control Panel.
2. Click the **Record** icon.





3. Move the camera using manual controls and/or by calling presets you created. You can record the motion of the camera until 0% of recording memory is left.
4. Click the **Stop** icon to halt the recording.

Editing the pattern

To edit the pattern, re-record Pattern1.

Call pattern

To execute the pattern you created, open the **Pattern** tab, and then click the **Call** icon.

6.2.4 Configure Linear Scan

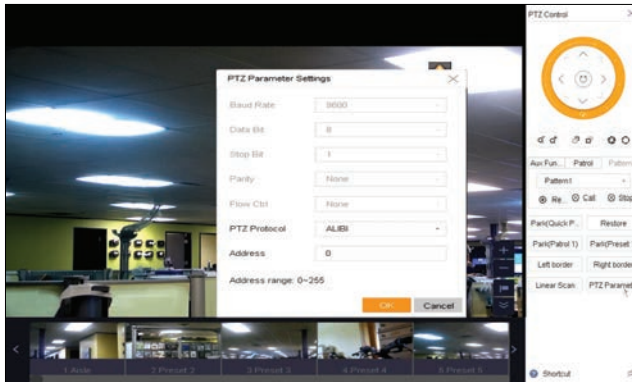
Use Linear Scan to scan the field of view back and forth along a linear path between a “left limit” point and a “right limit” point. To use this feature, you must first define the Left Limit and Right Limit:

1. With the camera still (not executing any patrols or scans), manually point the camera to the left limit of the linear scan you want to define.
2. Click the **Left Limit** button on the PTZ Control panel.
3. Then manually point the camera to the right limit of the linear scan you want to define.
4. Click the **Right Limit** button on the PTZ Control panel.
5. Click the **Linear Scan** button to start and stop the scan. When the scan is stopped, you can point the camera up or down, and then click Linear Scan to scan the view at that elevation between the left and right limits.

6.3 PTZ Parameter Settings

Use the PTZ Parameter Settings menu to configure the communication settings and camera protocol for a PTZ controller connected to the recorder across an RS-485 network. To configure these parameters:

1. Click the PTZ Parameters button in the PTZ Control panel.



2. In the menu, select the parameters as needed to match the controller and camera, and then click **OK**.

SECTION 7

Point of Sale Integration

With the NVR POS (Point of Sale) feature you can overlay cash register transaction data onto a live video display. Currently only 16-, 32- and 64-channel NVRs support the POS feature. 16-channel NVRs support up to eight POS terminals, 32-channel NVRs support 16 POS terminals, etc. The Alibi recorder supports only plain text and XML data through the remote listening port.

Setting up POS is a two step process, performed in two different NVR menus:

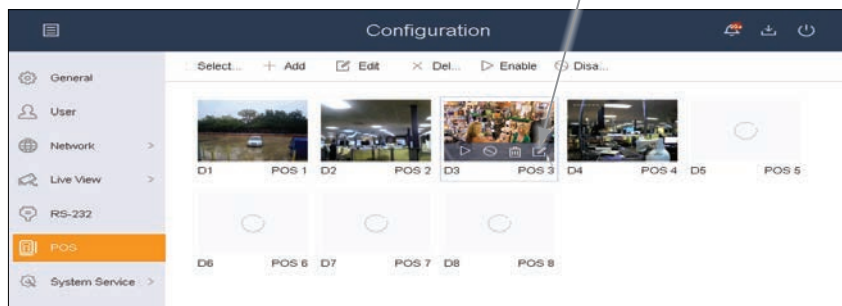
1. Assign POS data to a camera
2. Configure the POS interface

7.1 Assign POS data to a camera

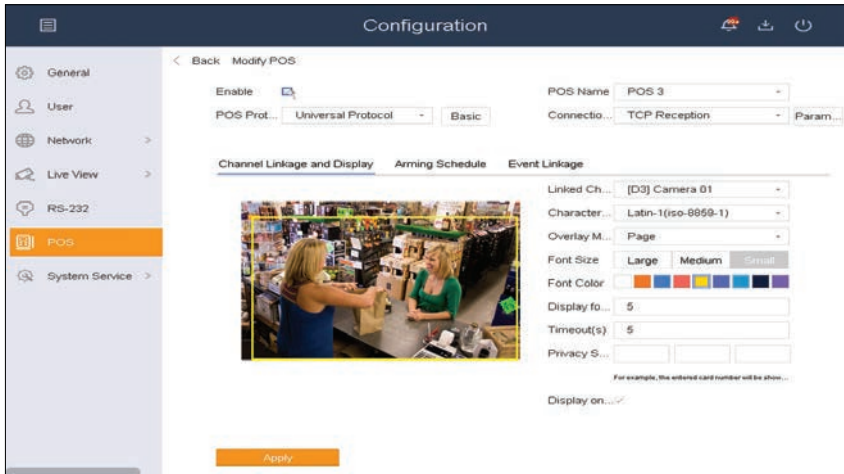
Do the following:

1. Open the POS Overlay menu. Go to **Menu | Configuration | POS | Overlay Channel**.

Click to open POS configuration menu



2. To add an existing camera to a POS system, hover the mouse over a camera thumbnail, then click the Edit icon. See above.



Notice in the mapping shown above, channel D3 is assigned to pos 3, etc.. by default. This indicates that data from POS assigned to POS 3 will be shown over the image in Channel D3. You can change this configuration, if needed, by selecting the POS identifier, and then selecting the channel to assign data to.

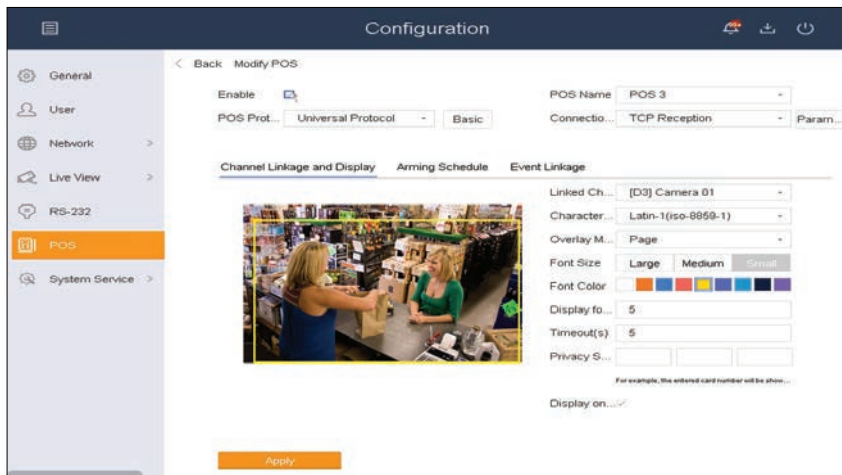
3. If changes were made in the screen above, click **Apply** to save the setting.

7.2 Configure the POS interface

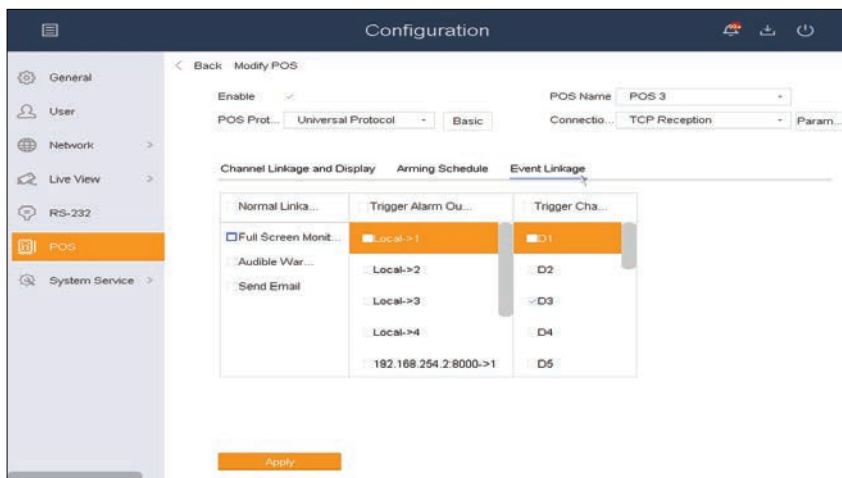
Do the following:

1. Open the POS Overlay menu. Go to **Menu | Configuration | POS**.

SECTION 7: POINT OF SALE INTEGRATION



2. Open the Select **POS name** drop down list, and then select the POS overlay you want to configure (see above). In this example, POS 3 is selected.
3. Check the **Enable** box to select this feature.
4. Select the **Event Linkage** tab, if not selected.
 - a. In the **Normal Linkage** column, select the actions you want to occur when POS data is available. For instance, if you want the monitor to expand to full screen when data is available, check the Full Screen Monitoring box.



- b. In the **Trigger Alarm Output** column, select the output alarms you want to activate when POS data is available. Click **Apply** to save the settings.
 - c. In the **Trigger Channel** column, elect one or more camera channels which will start to record/capture or expand to full-screen monitoring when the POS data available. Click **Apply** to save the settings.
5. Click the **Arming Schedule** tab. In this tab you can define up to eight periods for each day when POS data is used. The periods must not overlap.

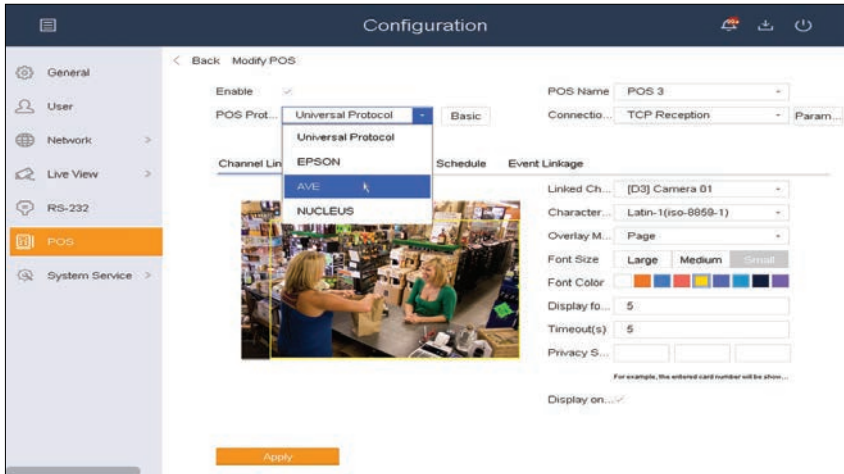
- a. Click the down arrow in the **Mon** field (see above) to setup the schedule for a different day, and/or click **Copy** to copy the Arming Schedule you setup in the window to other days of the week.
 - b. Click **Apply** to save the settings.
6. Click a **Privacy Settings** field in the lower right corner of the **Modify POS** menu. **POS Privacy Information Filtering** allows you to hide additional information when a transaction takes place.

- a. Click an entry field, and then enter the label of the data you want to hide.

For example, a credit card number, except for the last 4 digits, is blocked by a POS system by default when sending data to the NVR. To block the entire number, enter **CardNum** in a privacy field shown above. The CC number shown in the report will then appear as *********. More information about this feature will be provided.

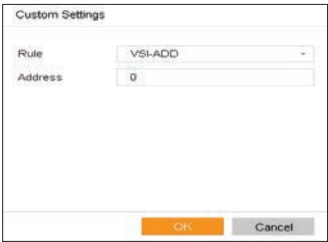
SECTION 7: POINT OF SALE INTEGRATION

7. In the POS menu (see below) do the following:



- Open the POS Protocol drop-down list, and select either **Universal Protocol**, **EPSON**, **AVE** or **NUCLEUS** whichever matches the register.
- Open the **Connection Type** drop down list, and then select the way the recorder is connected to the POS terminal.
- If you selected **Universal Protocol**, click the **Advanced** button to the right and then click **Custom** to view the communication tags options. Set the tags as needed for compatibility with your register. **NOTE:** Clicking the **Advanced** button changes the label to **Basic**.

- If you selected **EPSON**, no additional parameters are needed.
- If you selected **AVE**, click the **Set** button to the right to open the **AVE Settings** window, and then select the Rule from the drop down list, and the Address to match the configuration of the register. The default Rule is VSI-ADD at address 0.



f. If you selected **NUCLEUS**, a restart is required. Follow the on-screen instructions to restart the recorder.

NOTE: NUCLEUS will set some POS configuration parameters to their default values.

g. Click the **Settings** button, and then set the **Port** number and **Remote IP Address** to match the register. The default port number is 10000. The actual port number you must use depends on the register being integrated. The pcAmerica register used in this example requires port 4201.



h. Open the **Character Encoding** drop down list and select the option that is compatible with the register. Refer to your register documentation for the appropriate setting. **NOTE:** Alibi recorders support only plain text messages from the register.



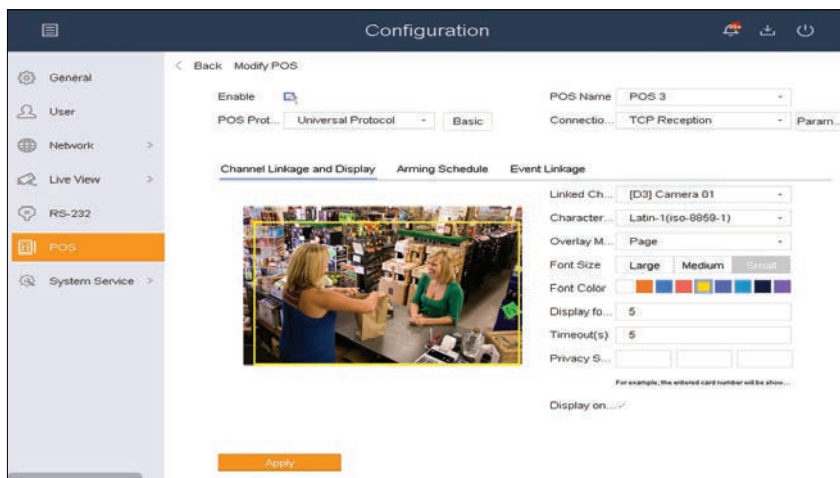
i. Select the **Overlay Mode**, **Font Size**, **Overlay Time** and **Delay Time** you prefer.

SECTION 7: POINT OF SALE INTEGRATION



Linked Ch... [D3] Camera 01
Character... Latin-1(iso-8859-1)
Overlay M... Page
Font Size Large Medium Small
Font Color [Color Selection]
Display fo... 5
Timeout(s) 5
Privacy S...
For example, the entered card number will be show...
Display on...

- j. Check the **POS Overlay in Live View** box if you want messages from the register to appear over the camera image in Live View mode.
 - k. Click on the **Color** you prefer for the overlay messages.
8. Click **Apply** to save your settings.
 9. Click anywhere inside the Live View window, and then reposition or resize the message box as needed.



Configuration

Back Modify POS

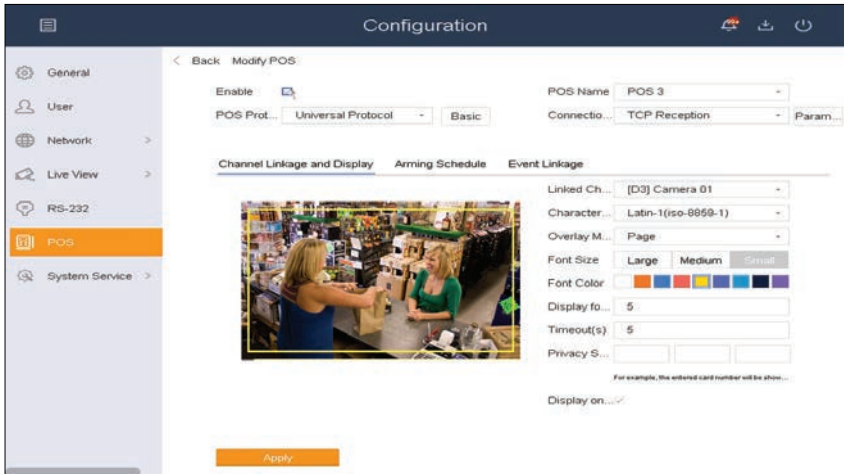
Enable POS Name POS 3
POS Prot... Universal Protocol Basic Connection... TCP Reception Param...

Channel Linkage and Display Arming Schedule Event Linkage

Linked Ch... [D3] Camera 01
Character... Latin-1(iso-8859-1)
Overlay M... Page
Font Size Large Medium Small
Font Color [Color Selection]
Display fo... 5
Timeout(s) 5
Privacy S...
For example, the entered card number will be show...
Display on...

Apply

10. Click the **Get Text** button at the bottom of the window (see below) to start retrieving messages from the register. The **Get Text** button changes to a **Stop Getting** button.



11. Verify that when transactions occur at the POS terminal, overlay text appears in the Live View image and the field below it.
12. Click the **Stop Getting** button to disable this test feature.

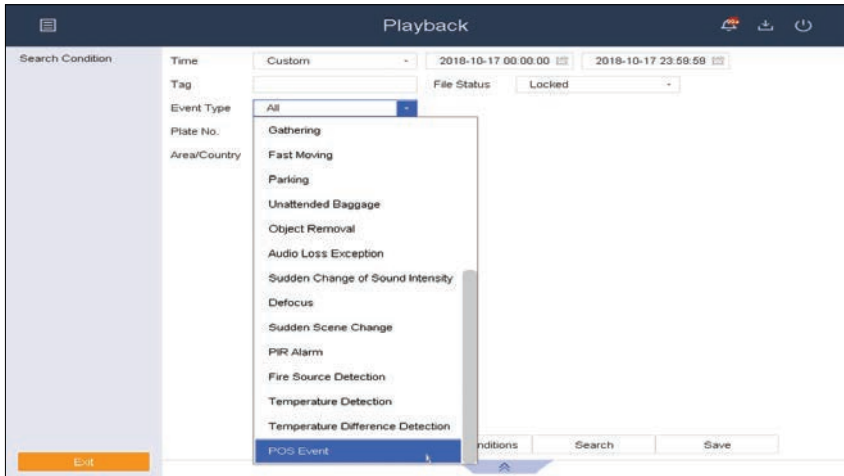
7.3 Playback POS recordings

When the POS setup is configured to record video when messages are received from the register, you can use **Custom Playback - POS Event** search features to find the video coupled with message strings received from the register. In the example below, a search is made for register events where “water” was purchased.

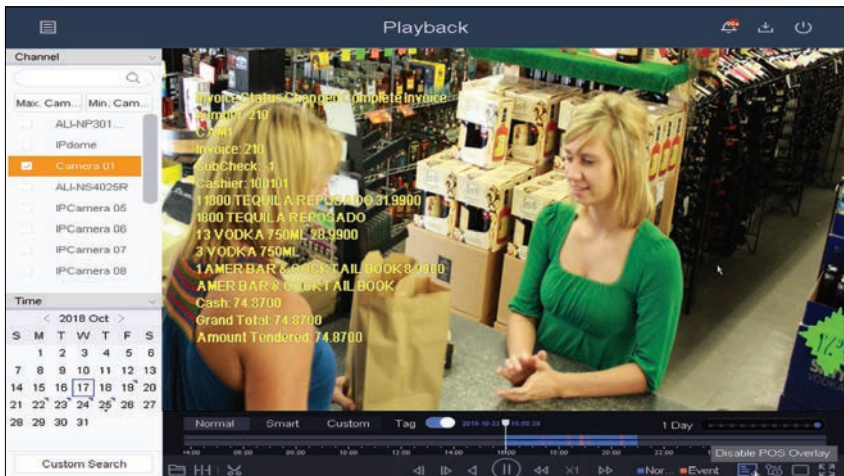
To playback video with specific POS register messages, go the following:

1. Open the Playback menu. Go to **Menu | Playback**.
2. Click the **Custom Search** button, and search for **POS Events**.

SECTION 7: POINT OF SALE INTEGRATION



3. Configure the search screen as needed, and then click the **Search** button. See “8.6.5 Custom Playback” on page 118 for more information.
4. Click the **Search** button. Results of the search will appear in the right panel.
5. Select the search result you want to play, and then click the **Play** icon associated with the search result.



SECTION 8

Record, Playback and Video Backup

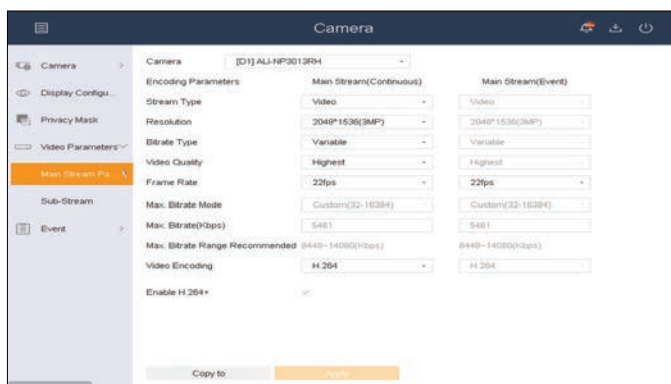
After the initial setup of your NVR using the Wizard, the Menus interface enables you to refine your configuration settings and expand the functionality of the system. To use most menus, the user must log into the NVR system, either locally or remotely, with administrative privileges.

8.1 Configuring record settings

8.1.1 Setting camera video parameters

Video parameter values provided in these menus are dependent on the capabilities of the camera model.

1. Open the **camera main stream parameters** menu to configure the encoding parameters. Go to **Menu | Camera | Video Parameters | Main Stream Pa....**

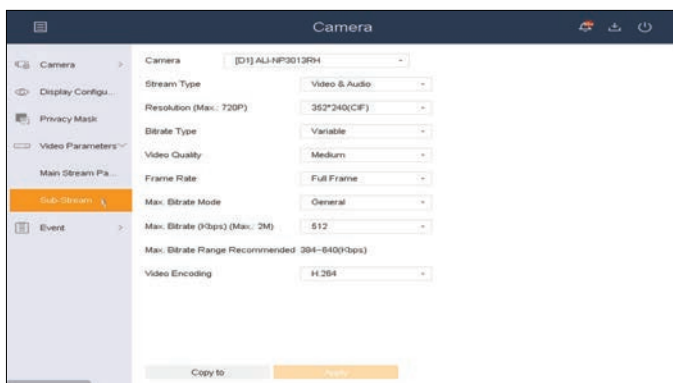


The Main Stream refers to the primary stream that affects data recorded to the hard disk drive. It directly determines the recording quality and image size. Main stream recording can provide a higher quality video with higher resolution and frame rate than sub-stream recording. Parameters are described as:

- **Frame Rate** (FPS - Frames Per Second): refers to how many frames are captured each second. A higher frame rate is advantageous when there is movement in the video stream, since it maintains a higher image quality throughout.
- **Resolution**: Image resolution is a measure of how much detail a digital image can hold: the greater the resolution, the greater the level of detail. Resolution can be specified as the number of pixel-columns (width) by the number of pixel-rows (height), e.g., 1024×768.
- **Bitrate**: The bit rate (in kbit/s or Mbit/s) is often referred to as speed, but actually defines the number of bits/time unit and not distance/time unit.

SECTION 8: RECORD, PLAYBACK AND VIDEO BACKUP

- **Enable H.264+ (or H.265+)** Mode: The H.264+ (or H.265+) mode helps to ensure high video quality with a lower bitrate. It reduces the network bandwidth requirement and HDD storage space.
2. In the menu shown above:
 - a. Open the **Camera** drop down list, and then select the camera you want to configure.
 - b. Adjust the main stream parameters as needed.
 - c. Click **Apply**.
 - d. Click the **Copy to** button to copy your settings to other cameras on your system. Follow the on-screen menu to perform the copy.
 - e. Click **Apply** when finished.
 3. Open the **camera sub-stream parameters** menu to configure the encoding parameters. Go to **Menu | Camera | Video Parameters | Sub-stream**.



The Sub-stream refers to the secondary stream that affects data recorded to the hard disk drive. It directly determines the recording quality and image size where sub-stream video is recorded or displayed, especially on smartphone live video streaming. Sub-stream recording can provide a nominal quality video with a lower resolution and frame rate requiring less network bandwidth than main stream recording. Parameters are described above:

4. In the **Sub-stream** menu shown above:
 - a. Open the **Camera** drop down list, and then select the camera you want to configure.
 - b. Adjust the main stream parameters as needed.
 - c. Click **Apply**.
 - d. Click the **Copy to** button to copy your settings to other cameras on your system. Follow the on-screen menu to perform the copy.
 - e. Click **Apply** when finished.

- Repeat steps 1 through 4 above for each camera on your surveillance system.

8.2 Configuring Record schedule

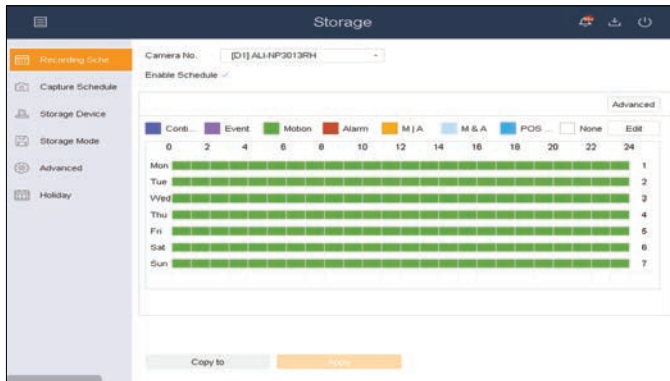
The record schedule can be used to automatically start and stop recording at preset times. Initially, cameras are configured to record either continuously or using motion detection. Managing the record schedule for each camera can save space on the HDD and help the recorder operate more efficiently.

You can setup a record schedule in either of two ways: graphically, where you apply recording modes to sections of the week array (Monday through Sunday \times 0 through 24 hours) and by using the Edit menu to more accurately define what mode of recording occurs and when. You can intermix the graphical method and edit method to configure any camera, and you can define up to 56 different recording segments during a week. The weekly schedule you setup will repeat every week unless changed.

NOTE

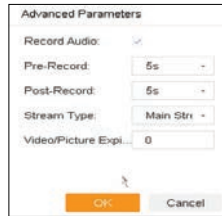
The recording schedule you setup will repeat every week indefinitely unless it is changed. You can also set up a special recording schedule for Holidays, and a separate image capture schedule.

- Open the Record Schedule menu. Go to **Menu | Storage | Recording Schedule**. Note that the schedule shown below is setup to record on motion detection only throughout the week.



- To configure the Record schedule:
 - Open the **Camera No**, drop-down list to select the camera you want to configure.
 - Check the **Enable Schedule** box.
 - Click the **Advanced** button.

SECTION 8: RECORD, PLAYBACK AND VIDEO BACKUP



In the Advanced Parameters menu:

- i. Check the **Record Audio** box if applicable.
- ii. Set the **Pre-Record** and **Post-Record** times using the drop down lists. These parameters set the number of seconds of video before and after an event occurs what will be saved in storage.
- iii. Open the **Steam Type** drop down list to select the video stream you want to record. You can select Dual, but that requires more bandwidth and storage space.
- iv. Set the **Video/Picture Expiry** parameter as needed. This parameter sets the expired time for a recorded file to be kept in the HDD. When the deadline is reached, the file will be deleted. If you set the expired time to "0," the file will not be deleted. The retention time for a file is determined in consideration of the capacity of the HDD.
- v. Click **OK** to save your settings.

Setting the Recording Schedule graphically

To graphically configure the recording schedule, simply drag a rectangle across the areas of the array you want to change, and then click the recording mode you want to apply to that area. Each segment of the array represents 30 minutes. To graphically change the recording schedule:

1. Use the mouse to drag a rectangle across the area of the schedule you want to change. A red rectangle will show the area you selected. In this example, the period from 7 AM to 6 PM, Monday through Sunday was selected.



- Click on the recording mode buttons above the array to change the mode in the rectangle. Mode buttons include:

Continuous: scheduled recording.

Event: recording triggered by all event triggered alarm.

Motion: recording triggered by motion detection.

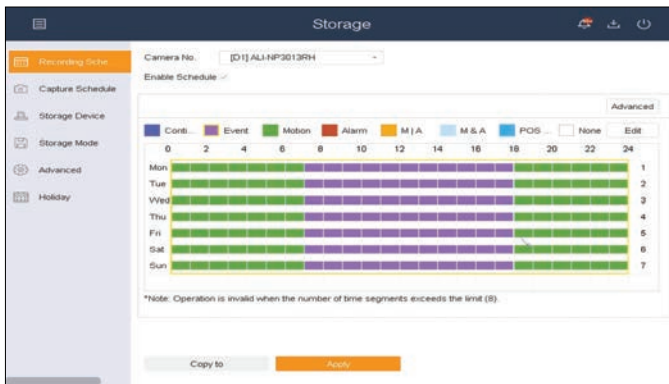
Alarm: recording triggered by alarm.

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

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

POS: recording triggered by Point of Sale (POS) and alarm.

In this example, **Event** (purple code) recording was selected.



- Repeat steps 1 and 2 above for each recording mode you want to apply, and for each camera.

Setting the Recording Schedule using Edit

You can use the edit method to define up to 8 recording periods for each day of the week (56 maximum). A schedule you setup for one day of the week can be copied to any other day of the week. Each time segment in **Edit** is 15 minutes in length.

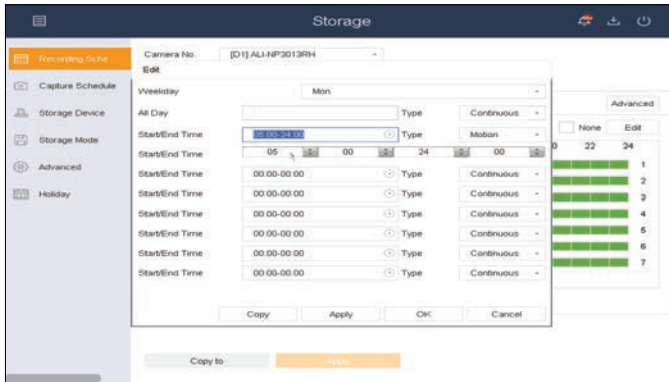
NOTE

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.

To setup a recording schedule using Edit:

- In the Record Schedule menu, click the **Edit** button.

SECTION 8: RECORD, PLAYBACK AND VIDEO BACKUP



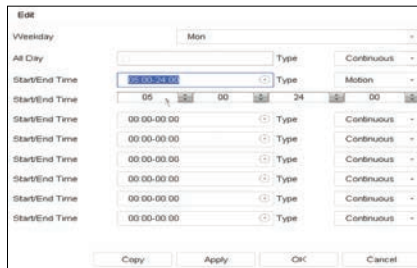
In the **Edit** menu:

- i. Open the **Weekday** drop down list, and select the day you want to configure.
- ii. To schedule all-day recording, check the box for All Day recording, and then open the **Type** drop-down list to the right to select the recording mode.

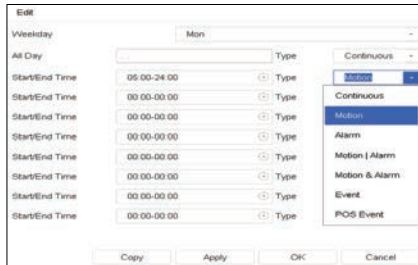
NOTE

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

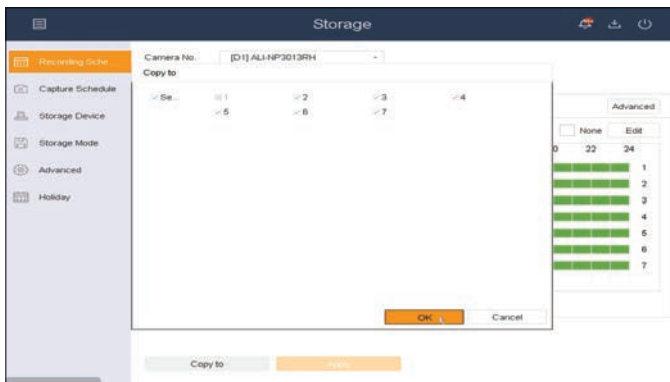
- iii. To setup specific start and end times, click the time field on the first **Start/End Time** line to open a time setting popup window.



- Use the up/down arrow buttons for each time field to set the hour and minute value start time and end time of the recording period you are configuring. In the example above, 05:00-24:00 was selected.
- Open the **Type** field drop down list to select the type of recording mode you want to apply during that period.



- Click **Apply** to save your settings.
- To set additional recording mode segments, repeat the method above for the additional 7 time segments for the day you selected as needed.
- Click **Apply** to save your settings.
- Click the **Copy to** button at the bottom of the window to select other days of the week and copy that schedule to them. In the **Copy to** menu, Monday is day 1 and Sunday is day 7.



- Click **OK** to close the **Copy to** menu.
 - Click **Apply** to save your settings.
 - Repeat the steps above in the **Edit** menu for each day of the week, or use the graphical method.
 - i. Click **OK** to close the **Edit** menu.
2. Click **Apply** in the Recording Schedule menu.
 3. Repeat the steps above for each camera.

8.3 Configuring Capture schedule

The Capture schedule is used to configure when capture files are saved to storage. You can setup a Capture schedule in either of two ways: graphically, where you apply Capture modes to sections of the week array (Monday through Sunday \times 0 through 24 hours) and by using the Edit menu to more accurately define what mode of Capture occurs and when. You can intermix the graphical method and edit method to configure any camera, and you can define up to 56 different recording segments during a week. The weekly schedule you setup will repeat every week indefinitely unless changed.

NOTE

The Capture schedule you setup will repeat every week indefinitely unless it is changed. You can also set up a special recording schedule for Holidays, and a separate image capture schedule.

1. Open the Capture Schedule menu. Go to **Menu | Storage | Capture Schedule**. Note that the schedule shown below is configured for no capture recording (**None**).



2. To configure the Capture schedule:
 - a. Open the **Camera No.** drop-down list to select the camera you want to configure.
 - b. Check the **Enable Schedule** box.
 - c. Click the **Advanced** button.



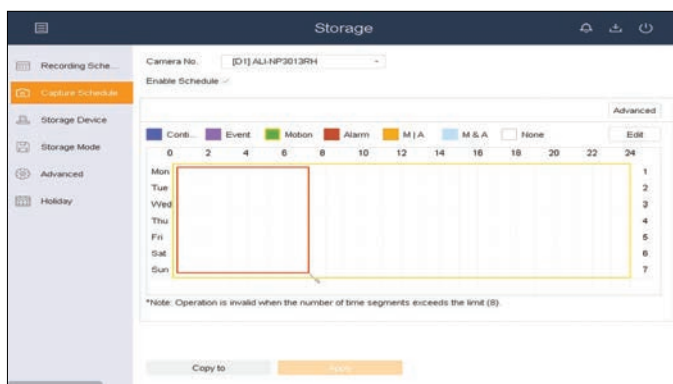
In the Advanced Parameters menu, you can configure the parameters for:

- i. Open the **Resolution** drop down lists for Continuous and Event, and select the resolution of the picture you want to capture.
- ii. Open the **Picture Quality** drop down lists for Continuous and Event, and then select either **Low**, **Medium** or **High** picture quality. Higher picture quality results in more storage space requirement.
- iii. Open the **Interval** drop down list and select the interval of capturing live picture.
- iv. Open the **Capture Delay Time** drop down list and select the duration for capturing pictures.
- v. Click **OK** to save your settings.

Setting the Capture Schedule graphically

To graphically configure the Capture schedule, simply drag a rectangle across the areas of the array you want to change, and then click the Capture mode you want to apply to that area. Each segment of the array represents 30 minutes. To graphically change the Capture schedule:

3. Use the mouse to drag a rectangle across the area of the schedule you want to change. A red rectangle will show the area you selected. In this example, the period from 12 AM to 5 AM, Monday through Sunday was selected.



4. Click on the Capture mode buttons above the array to change the mode in the rectangle. Mode buttons include:

Continuous: scheduled capture mode.

Event: capture triggered by all event triggered alarm.

Motion: capture triggered by motion detection.

Alarm: capture triggered by alarm.

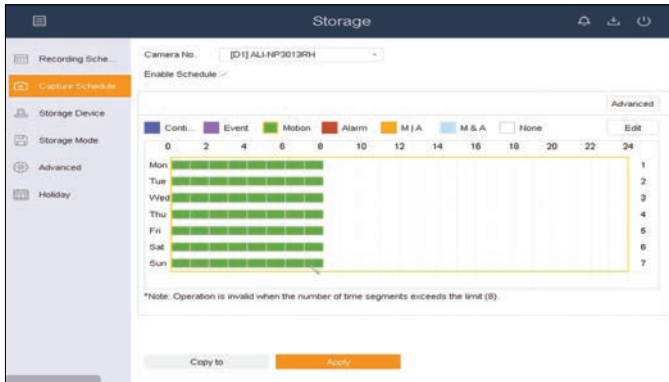
M/A: capture triggered by either motion detection or alarm.

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

None: no captures taken.

SECTION 8: RECORD, PLAYBACK AND VIDEO BACKUP

In this example, **Continuous** (green code) recording was selected.



- Repeat steps 1 and 2 above for each capture mode you want to apply, and for each camera.

Setting the Capture Schedule using Edit

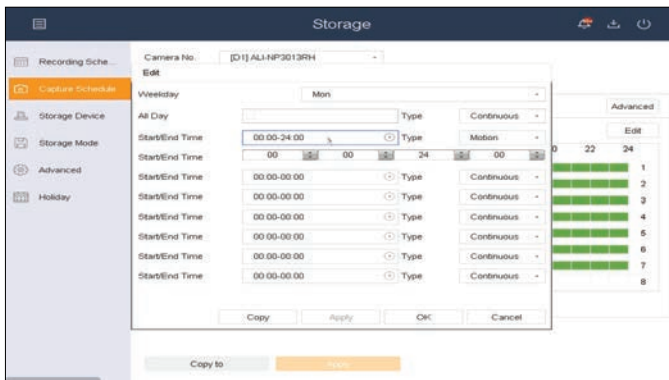
You can use the edit method to define up to 8 recording periods for each day of the week (56 maximum). A schedule you setup for one day of the week can be copied to any other day of the week. Each time segment in **Edit** is 15 minutes in length.

NOTE

You can define up to eight Capture time periods for each day, each with a specified recording type. Capture time periods cannot overlap with each other.

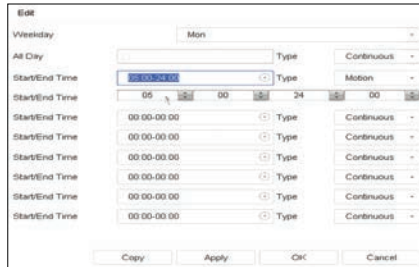
To setup a recording schedule using Edit:

- In the Record Schedule menu, click the **Edit** button.

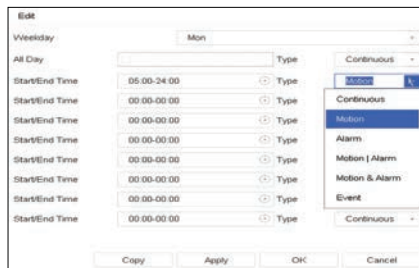


In the **Edit** menu:

- i. Open the **Weekday** drop down list, and select the day you want to configure.
- ii. To schedule all-day capture mode, check the box for **All Day**, and then open the **Type** drop-down list to the right to select the capture mode.
- iii. To setup specific start and end times, click the time field on the first **Start/End Time** line to open a time setting popup window.



- Use the up/down arrow buttons for each time file to set the hour and minute value start time and end time of the capture mode period you are configuring. In the example above, 05:00-24:00 was selected.
- Open the **Type** field drop down list to select the type of capture mode you want to apply during that period.



- Click **Apply** to save your settings.
- To set additional recording mode segments, repeat the method above for the additional 7 time segments for the day you selected as needed.
- Click **Apply** to save your settings.
- Click the **Copy to** button at the bottom of the window to select other days of the week and copy that schedule to them. In the **Copy to** menu, Monday is day 1 and Sunday is day 7.



- Click **OK** to close the **Copy to** menu.
 - Click **Apply** to save your settings.
 - Repeat the steps above in the **Edit** menu for each day of the week, and for each camera.
- i. Click **OK** to close the **Edit** menu.
7. Click **Apply** in the Capture Schedule menu.
 8. Click **OK** to close the Edit menu.
 9. In the **Capture Schedule**, click **Apply**.
 10. Repeat the steps above for each camera.

8.4 Defining Holidays

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 “8.2 Configuring Record schedule” on page 99.

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 | Storage | Holiday**.

ID	Holiday Name	Status	Start Date	End Date	Edit
1	New Year's Day	Disabled	1-Jan	1-Jan	
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	
9	Holiday9	Disabled	1-Jan	1-Jan	
10	Holiday10	Disabled	1-Jan	1-Jan	
11	Holiday11	Disabled	1-Jan	1-Jan	
12	Holiday12	Disabled	1-Jan	1-Jan	
13	Holiday13	Disabled	1-Jan	1-Jan	
14	Holiday14	Disabled	1-Jan	1-Jan	
15	Holiday15	Disabled	1-Jan	1-Jan	
16	Holiday16	Disabled	1-Jan	1-Jan	

- Click on the **Edit** icon for the first entry in the list. You can define up to 31 different holidays periods.



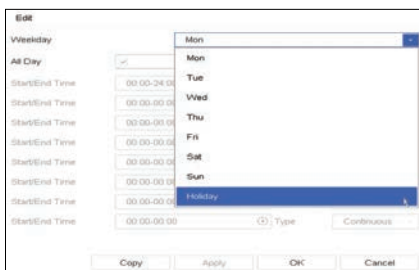
- In the **Edit** window, click the **Enable** box to check it.
- Click on the **Holiday Name** field, and then enter a common name for the holiday.



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

No	Holiday Name	Status	Start Date	End Date	Edit
1	New Year's Day	Enabled	1-Jan	1-Jan	
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	
9	Holiday9	Disabled	1-Jan	1-Jan	
10	Holiday10	Disabled	1-Jan	1-Jan	
11	Holiday11	Disabled	1-Jan	1-Jan	
12	Holiday12	Disabled	1-Jan	1-Jan	
13	Holiday13	Disabled	1-Jan	1-Jan	
14	Holiday14	Disabled	1-Jan	1-Jan	
15	Holiday15	Disabled	1-Jan	1-Jan	
16	Holiday16	Disabled	1-Jan	1-Jan	

- Repeat steps 2 through 7 above for other holidays you want to identify.
- Open the Record Schedule window. Go to **Menu | Storage | Record Schedule**.

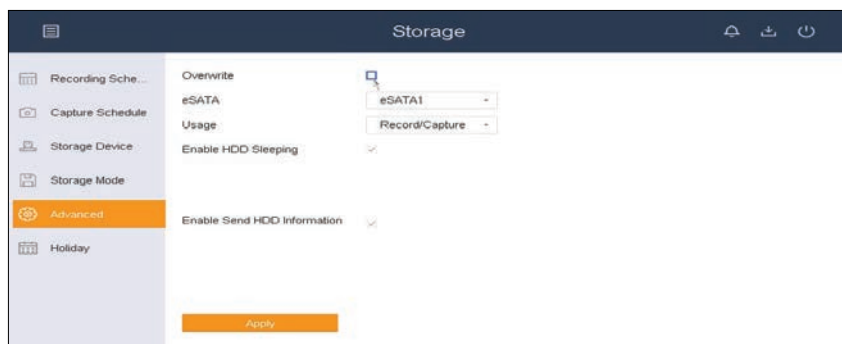


- Use the procedure in “8.2 Configuring Record schedule” on page 99 to setup a recording schedule for Holidays.

8.5 Record Advanced settings for eSATA port

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

- Open the Storage Advanced menu. Go to **Menu | Storage | Advanced**.



2. Click the **Enable** box to check it.
3. Open the Usage drop down list, and then select either **Export** or **Record/Capture**.
4. Click **Apply** to save your settings.

8.6 Playback

You can playback recorded video files instantly, or in several ways through the Playback menus.

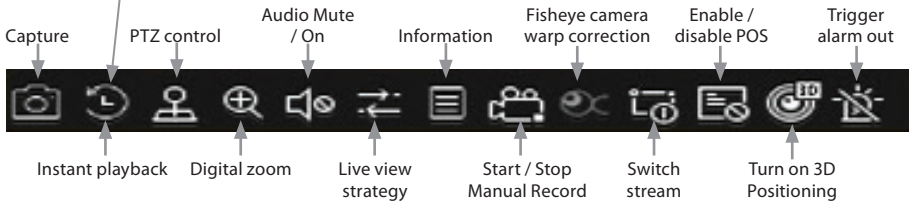
When playing back recordings with the Playback menu, you can tag files for identification and easy retrieval.

Multi-channel playback supports 4 channels at up to 8 MP resolution and 16 channels at up to 1080p resolution.

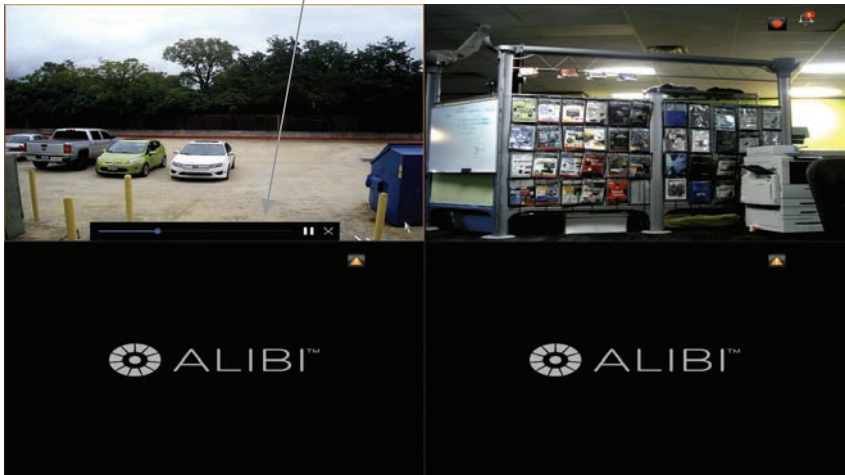
8.6.1 Instant playback by channel

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.

SECTION 8: RECORD, PLAYBACK AND VIDEO BACKUP



Instant playback - play controls



To cancel instant playback mode, right click on the screen.

NOTE In Live View mode, you can click the **Start/Stop Manual Record** icon to instantly record a video clip.

8.6.2 Using the Playback screen

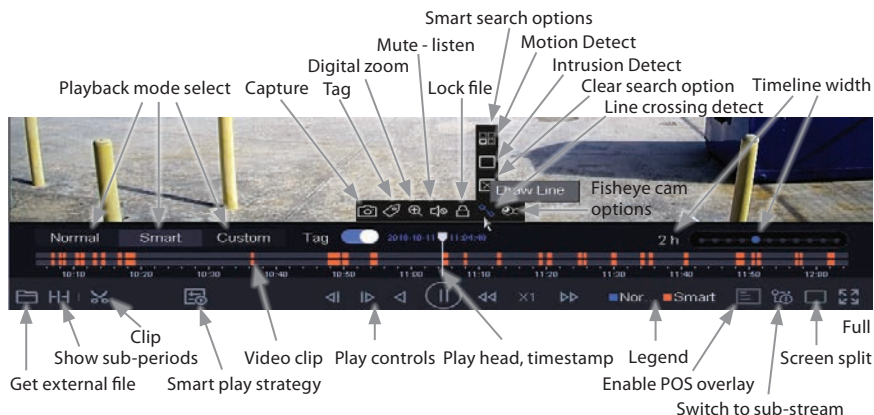
Use the Playback screen to find and replay video recordings. You can synchronously playback up to 16 video streams at a time. Three playback modes are available:

- **Normal:** Normal playback shows and plays back all video clips recorded from the selected camera on the selected day.
- **Smart:** Smart playback is useful with continuous video recordings for quickly finding recorded video that has object motion, object line crossing or object intrusion in any part the video frame. You can select the kind of motion to find and mark it anywhere in the frame. The recorder will make search recorded video to show video clips that match your search criteria. This mode only allows single channel playback.
- **Custom:** Custom mode is used to search for video clips recorded as a result of a specific alarm or event.

Playback screen



Toolbar

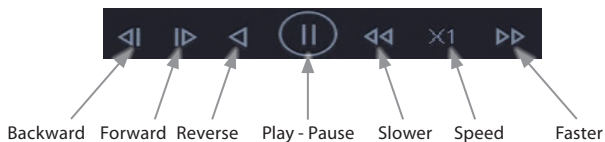


Notes:

- **Legend:** Legend defines the type of video clips marked on the timeline
- **Fisheye Expansion:** For fisheye cameras, these icons display video in the modes supported by the camera. Hover the mouse over the fisheye icon to open the list of options. See below.



- **180° Panorama:** Switch the Live View image to the 180° panorama view.
- **360° Panorama:** Switch the Live View image to the 360° panorama view.
- **PTZ Expansion:** The PTZ Expansion is the close-up view of some defined area in the fisheye view or panorama expansion. It supports electronic PTZ (e-PTZ).
- **Radial Expansion:** In radial expansion mode, the entire wide-angle view of the fisheye camera is displayed. This view mode is called Fisheye View because it approximates the vision of a (fisheye) convex eye. The lens produces curvilinear images of a large area, while distorting the perspective and angles of objects in the image.
- **Play Controls:** Use the Play Control buttons to speed up, slow down, reverse, etc. The Speed icon shows the speed factor.

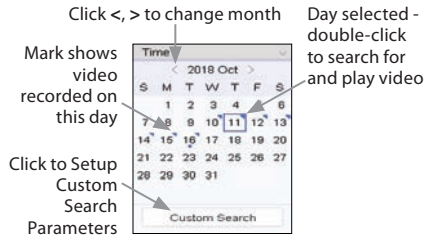


- **Show sub-periods:** Use this feature to divide play long video files into 4 segments and play them concurrently in a 2x2 split window (four frames) within the video playback window. For instance, if you are playing a video file that is 2 hours long, the file will be divided into four 30 minute segments, and each segment will play concurrently in a one of the 4 frames.
- **Smart playback strategy** opens a popup window for setting the playback speed of normal video separate from the playback speed of Smart search video. You can skip normal video during playback.



- **Timeline:** Marks on the timeline indicate video clips. Color of the marks is defined in the Legend. You can drag the timeline left or right to reposition it at the play head, and use the Timeline Width GUI to expand and contract time span of the line.
- **Switch to sub-stream:** Click this icon to switch between main stream video and sub-stream video.

Time panel - calendar



8.6.3 Normal Playback

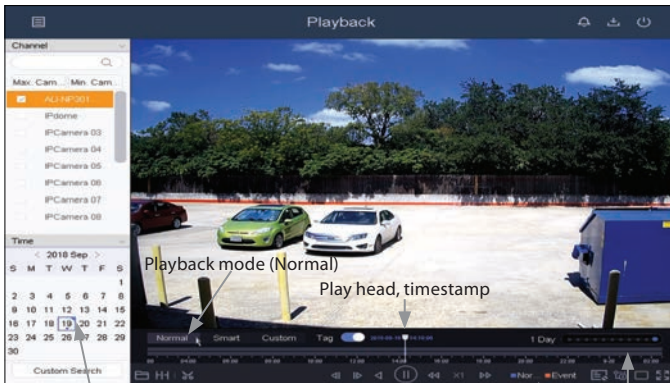
Normal playback shows and plays back all video clips recorded from the selected camera on the selected day.

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

SECTION 8: RECORD, PLAYBACK AND VIDEO BACKUP



2. In the **Playback** screen, check the box for the camera channel(s) you want to playback. In the example shown above, the camera named ALI-NP301RH (channel D1) was selected.
3. In the **Time** frame, the current day is identified. The recorder will search for available video in the selected month and mark each day that has recorded video available. In the screen below, the mark on the date shows video was recorded.



4. Click the Play icon in play controls to watch the recording. Other marks will appear on the timeline if other video recordings are available.

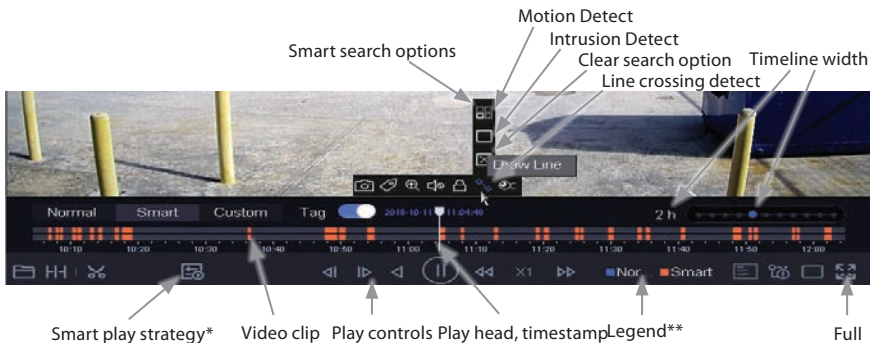
8.6.4 Smart Playback

Smart playback is useful with continuous video recordings for quickly finding recorded video that has object motion, object line crossing or object intrusion in any part the video frame. You can select the kind of motion to find and mark it anywhere in the frame. The recorder will make search recorded video to show video clips that match your search criteria. This mode only allows single channel playback.

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



2. Check the select box for a camera in the left frame.
3. In the **Time** menu, click on a date when video was recorded.
4. Use the play controls in the **Playback** screen to start playing recorded video from the camera.
5. Click the **Smart** button.
6. Move the cursor into the video frame. Icons will appear at the bottom of the video window.



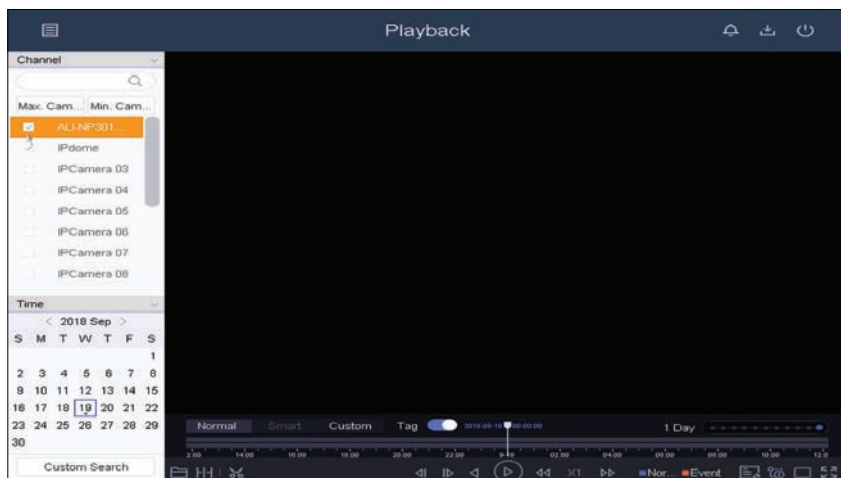
SECTION 8: RECORD, PLAYBACK AND VIDEO BACKUP

7. Select one of the icons for Smart search: **Line crossing**, **Intrusion detection** or **Motion detection**.
8. Determine where in the video window you want to perform a Smart search, and then:
 - For **Line crossing**, click a point in the video window to set one end of the line, and then click a point to set the other end of the line.
 - For **Intrusion detection**, click a point in the video window to set one corner of a quadrilateral, and then click three other points in a circular fashion to set the other corners of the quadrilateral.
 - For **Motion detection**, drag a diagonal line across an area of the screen where you want to search for motion. A grid pattern will form.
9. After establishing the search pattern, the recorder will automatically search for video that matches your search criteria, and begin playing.
 - **To use the same detection method in another area** of the video, just reapply the pattern in a different area. The recorder will automatically re-search the video for motion in that area, and begin playing video.
 - **To change to another search method**, while video is playing, right click the mouse to stop video playback, and then reopen the smart search options toolbar. Click the **Clear** icon, and then click the icon for then new search you want to make. The recorder will automatically re-search the video for motion in that area, and begin playing video.
10. Right click anywhere to return to the **Menu** screen.

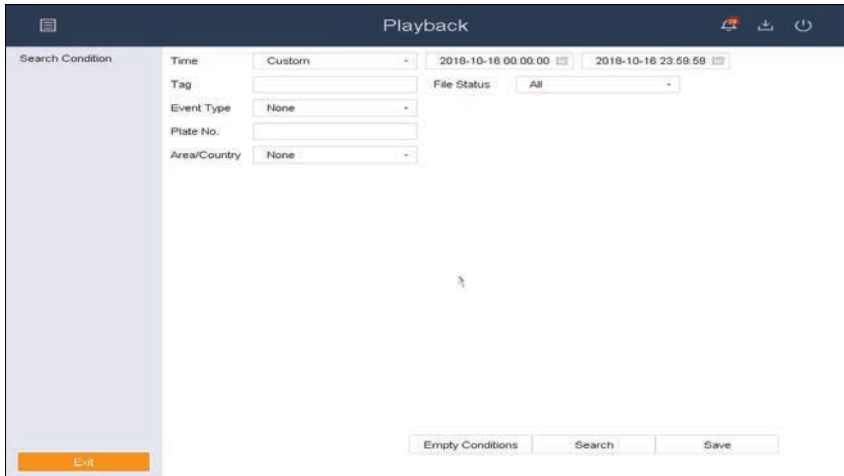
8.6.5 Custom Playback

Custom mode is used to search for video clips recorded as a result of a specific alarm or event. An example of using Custom Playback is shown below. Use this example as a model for other using Custom Playback. To use this feature:

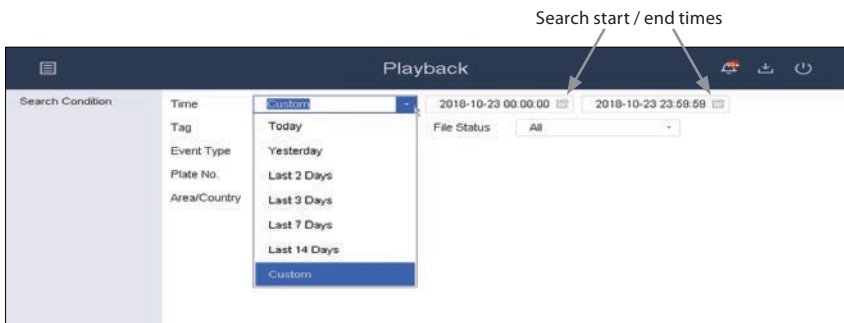
1. Open the Playback screen. Go to **Menu | Playback**.



2. Check the select box for the camera in the left frame whose video you want to search.
3. Click the **Custom Search** button in the lower left corner.

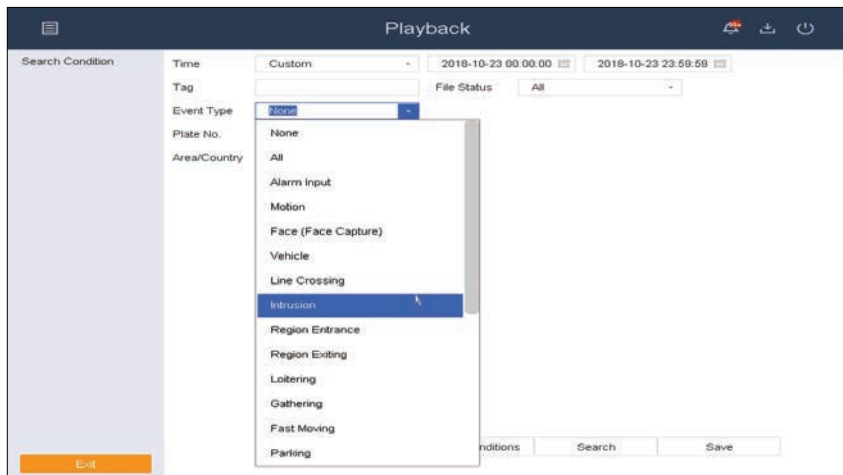


4. In the **Custom Search** menu, open the **Time** drop down list and select the time span you want to search. You can also click the calendar icons in the start and end time fields to select other time spans.

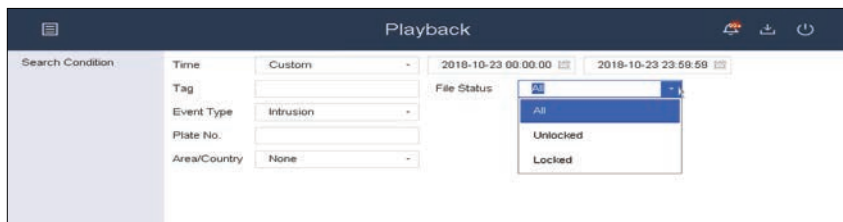


5. Open the Event Type drop down list, and then select the type of event you want to search for. In this example, **Intrusion** was selected.

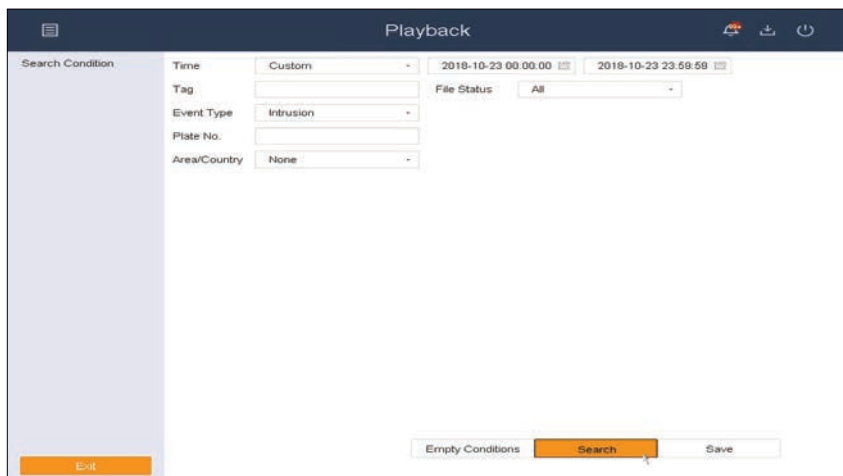
SECTION 8: RECORD, PLAYBACK AND VIDEO BACKUP



6. You can also open the **File status** drop down list and search for only **locked** or **unlocked** files.

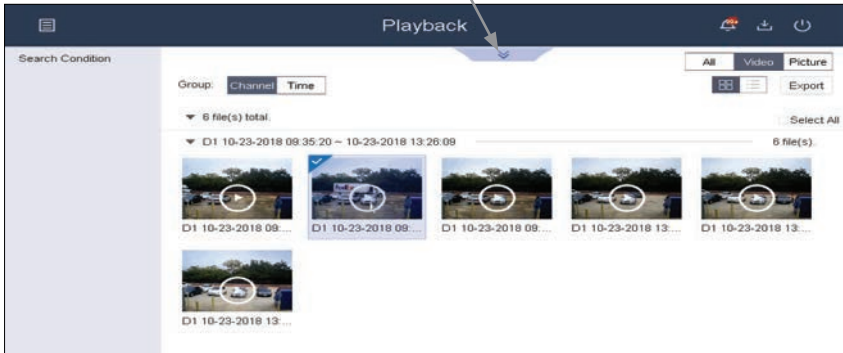


7. After selecting your search criteria, click the **Search** button at the bottom of the screen.



Thumbnails of the search results will appear in the window. You can also click the tab at the top of the window to reset your search criteria.

Click to open menu, change Search criteria



- Click the **Play** icon on the thumbnail of the video you want to watch. The Playback screen will open to play the video clip. Custom Search results are indicated by red marks on the timeline.

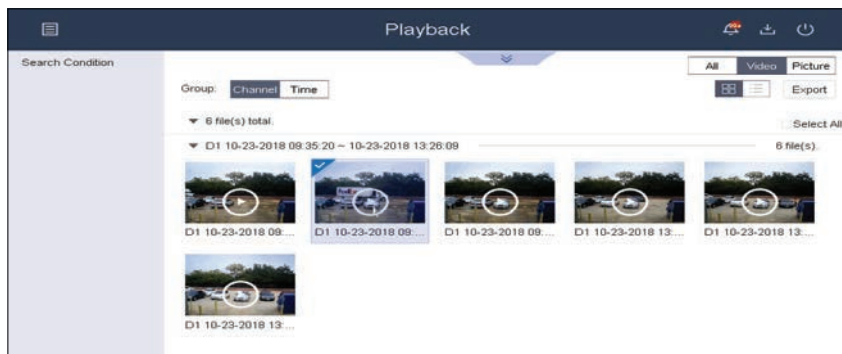


Export Custom Search result

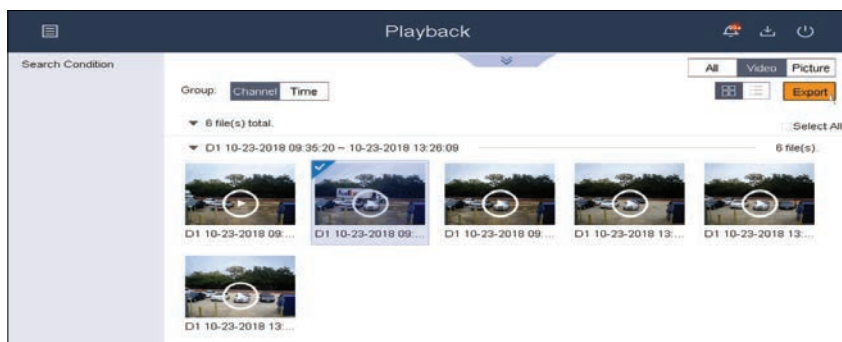
You can export (backup) a Custom search result(s) from the results window. To export a video file from the Playback screen shown above:

SECTION 8: RECORD, PLAYBACK AND VIDEO BACKUP

1. Click the **Custom Search** button in the lower left corner.



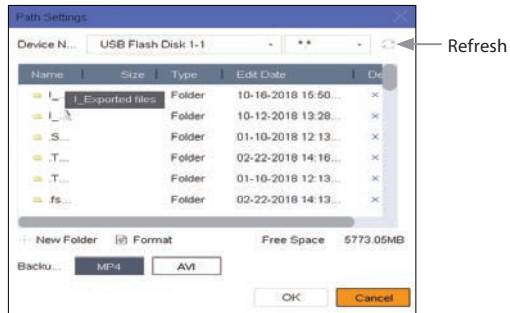
2. Click on the thumbnail for the file you want to export. When selected, the thumbnail will be shaded, and a check mark will appear in the upper left corner.



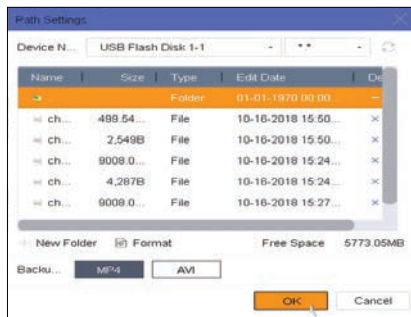
3. To export to a flash drive, insert a USB flash drive into an unused port on the recorder, and then click the Export button in the upper right corner.
4. In the Export popup menu, select the options you want to save, and then click OK.



5. In the Export **Path Settings** window, click the Refresh icon, and then double click on the directory in the media where you want to save the file. Open the **Device N...** drop down list to select another destination, if preferred.



6. Select the **Backup** format (MP4 or AVI), and then click **OK** to export the file.

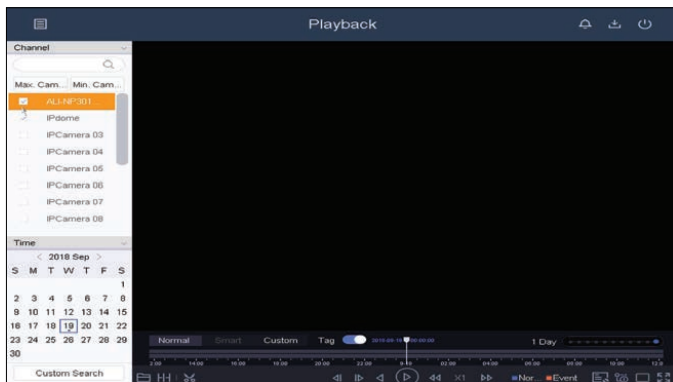


Play Sub-periods

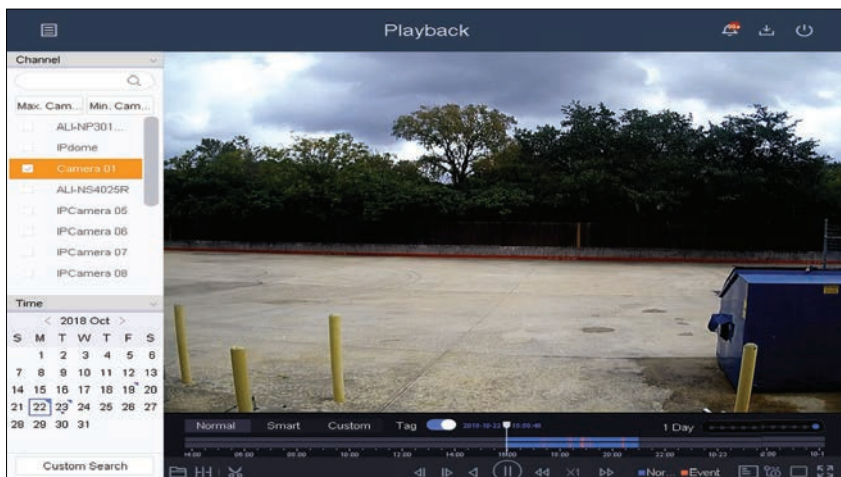
Use this feature to divide play long video files into 4 segments and play them concurrently in a 2x2 split window (four frames) within the video playback window. For instance, if you are playing a video file that is 2 hours long, the file will be divided into four 30 minute segments, and each segment will play concurrently in a one of the 4 frames.

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

SECTION 8: RECORD, PLAYBACK AND VIDEO BACKUP



2. Check the select box for a camera in the left frame.
3. In the **Time** menu, click on a date when video was recorded.
4. Use the play controls in the **Playback** screen to start playing recorded video from the camera.



Sub-periods

5. Click the **Sub-Periods** icon.



Back icon (exit Sub-periods)

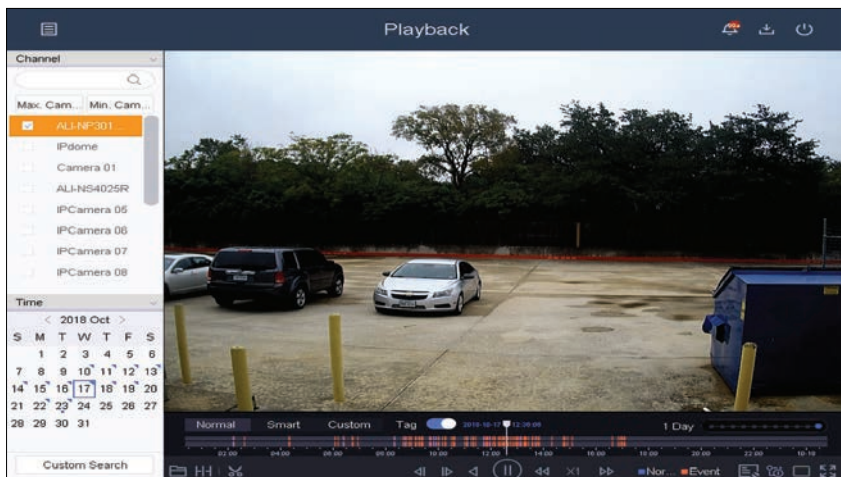
6. Click the **Back** icon (see above) to exit Sub-periods mode.

Thumbnails view

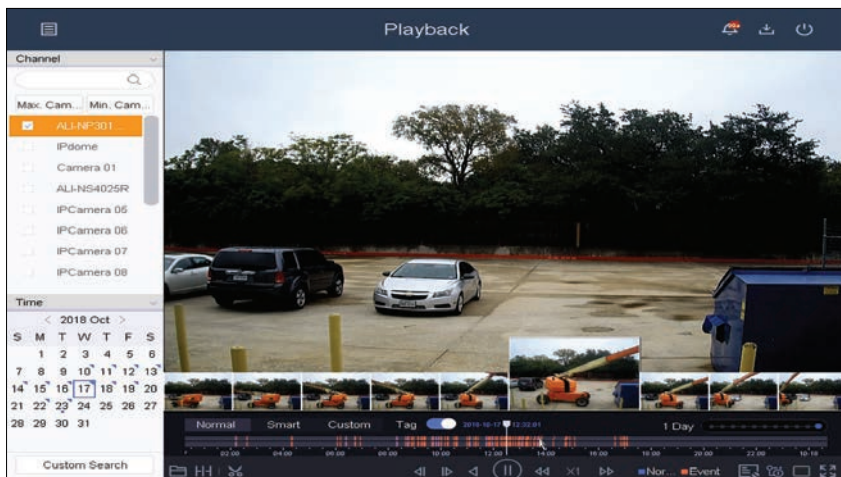
You can quickly open a thumbnails view of the video clips during Playback. This feature is valuable in quickly finding a video of interest. To use the thumbnails view:

1. Open the Playback window and play video from your camera.

SECTION 8: RECORD, PLAYBACK AND VIDEO BACKUP



2. Hover your mouse cursor over a file mark on the timeline. Thumbnails will appear for video clips in the vicinity.



3. Click on the thumbnail of interest to play it in the playback window.

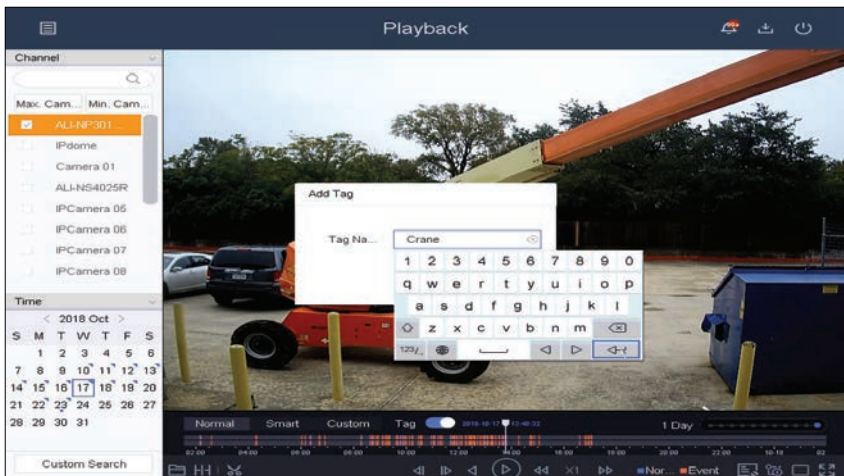
Tagging files

While watching a video file in Playback, you can click the **Tag** icon to associate it with a tag (label). Then, you can search for and retrieve the file later using its Tag.

1. Open the Playback screen to play video recorded from a camera, and then find a section of video you want to Tag.



2. Move the mouse cursor into the video window to open the popup toolbar. Click the **Tag** icon (see above).
3. In the Add Tag popup window, enter a name for the Tag you want to use.



4. Click **OK** to close the window.

SECTION 8: RECORD, PLAYBACK AND VIDEO BACKUP



5. After tagging, the mark on the timeline shows a white dot, and the Tag name appears in the thumbnail.



Thumbnail show Tag name

White mark on timeline shows it is Tagged

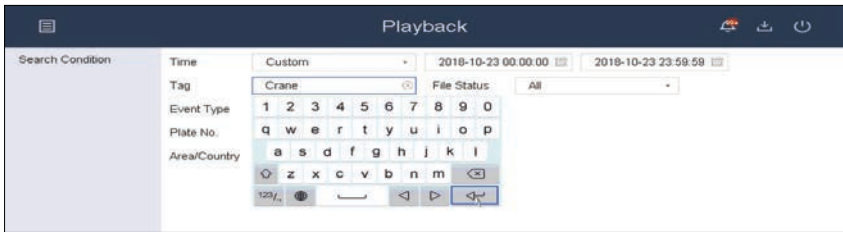
Custom search for tag

You can perform a custom search and find the file with the Tag you assigned. To perform the search:

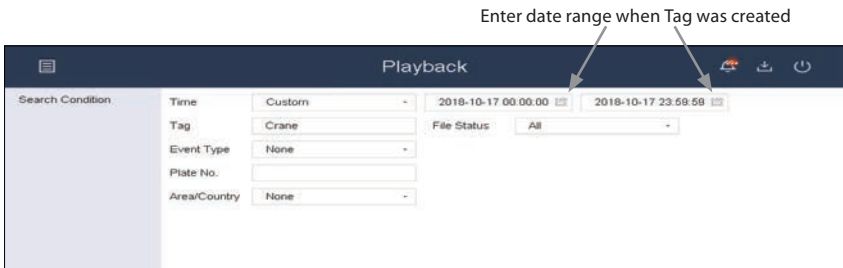
1. Open the Playback screen. Go to **Menu | Playback**.



2. Check the select box for a camera that produced video that was tagged.
3. Click the **CustomSearch** button in the lower right corner, and then enter the Tag name you are searching for in the Tag field.



4. In the date fields, enter the date range spanning when the tag was created.



5. Click the **Search** button at the bottom of the window. The search result will appear in the screen.

SECTION 8: RECORD, PLAYBACK AND VIDEO BACKUP

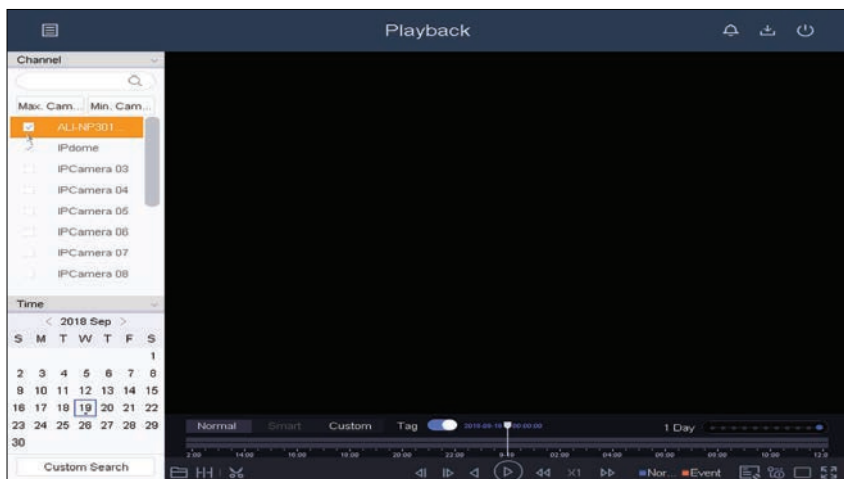


6. Click the **Play** icon in the result thumbnail to play the file in the Playback screen.

External file

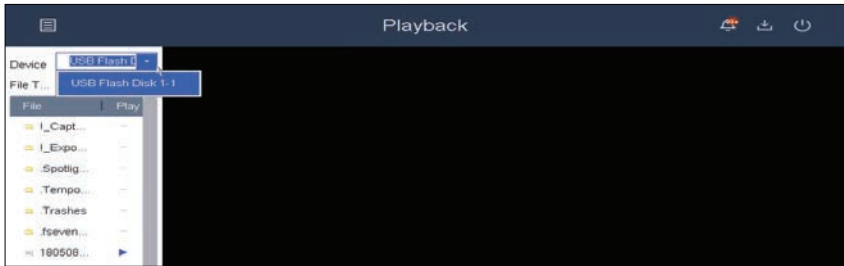
You can play an external file that was saved to some attached device such as a USB flash drive. To play a video file on a USB flash drive:

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

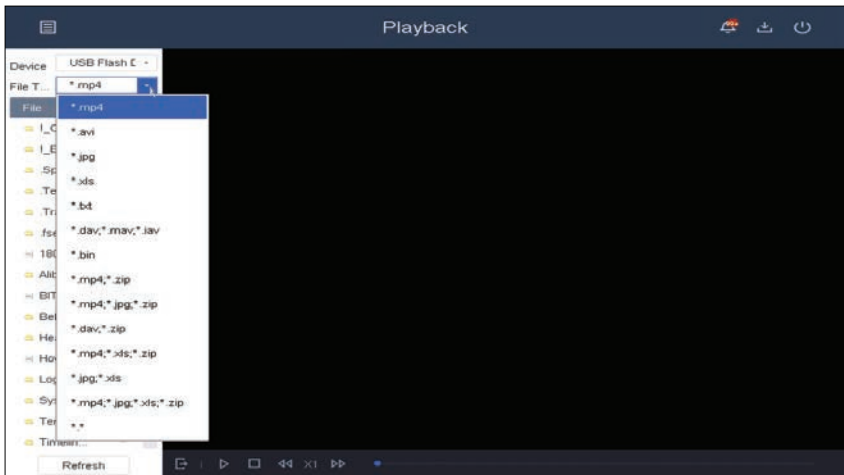


External File

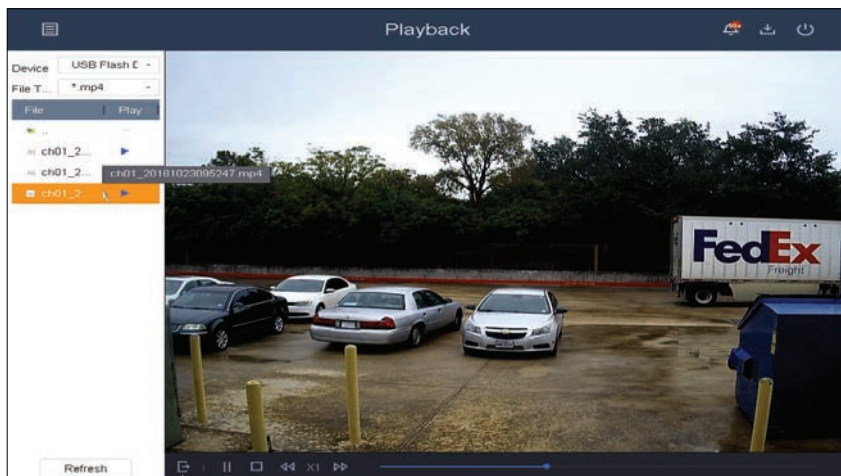
2. Insert a USB flash drive with the file you want to play into an unused USB port on the recorder.
3. Click the **External File** icon.



4. Open the **Device** drop down list and select the USB drive containing the file. See above.
5. Open the **File Type** drop down list, and select the format of the file you want to play.



6. Double click on the directory on the Device where the file is located, and the click the **Play** icon associated with the file.



Back icon (exit Sub-periods)

- Use the playback controls as needed, and click the **Back** icon to return to the Normal playback window.

8.7 File Management - search and export

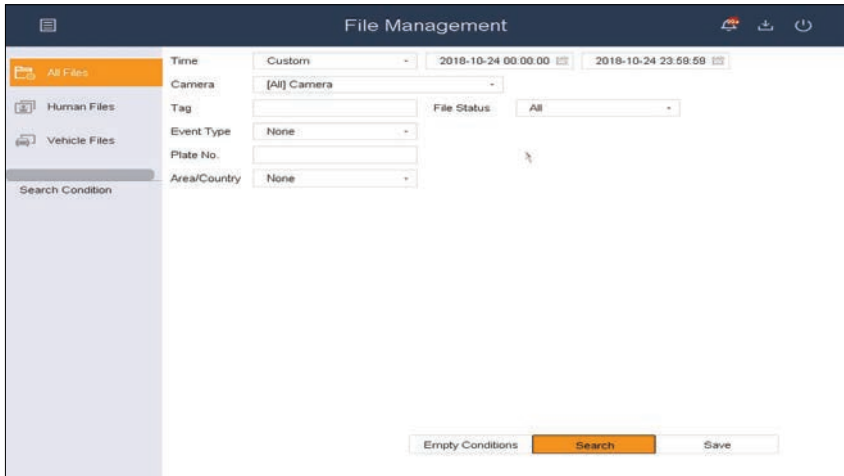
You can use the File Management menus to search for and export files recorded or captured from your cameras.

8.7.1 File Management - All Files

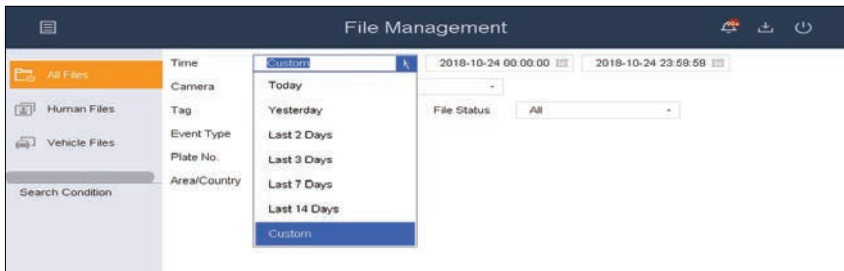
The example shown here can be applied to most search and export needs.

In the procedure below, the camera on channel D1 (ALI-NP3013RH) was previously configured to detect Line Crossing events. Video from these events between 10/22/18 and 10/25/18 was found using the **File Management - All Files** menu. A video resulting from the search was selected and exported to a USB flash drive for backup. To perform this procedure:

- Open the File Management menu. Go to **Menu | File Management | All Files**.

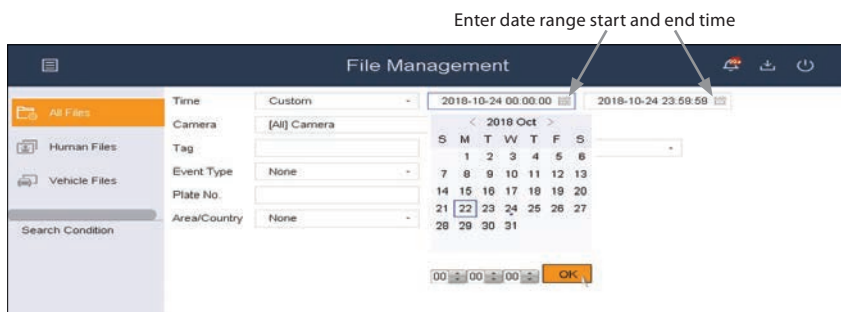


2. Select the time span across which you want to search. The menu provides two methods:
 - a. Open the **Time** option drop down list, and select the period back from the current day to search.

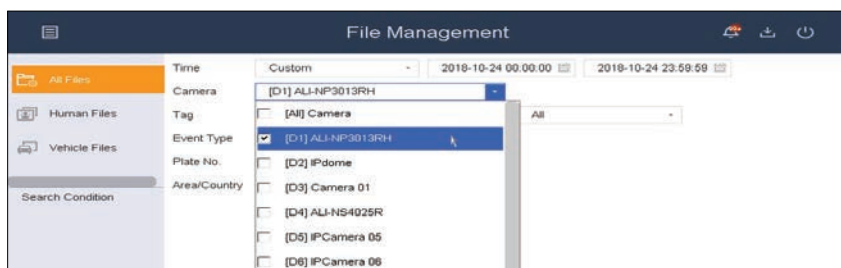


- b. Or, use the Custom (calendar) feature to select the start date and time. Click the calendar icon shown below to open the calendar menu, click on the date for start (or end), and then set the time in GUI at the bottom. Click **OK** to select your settings.

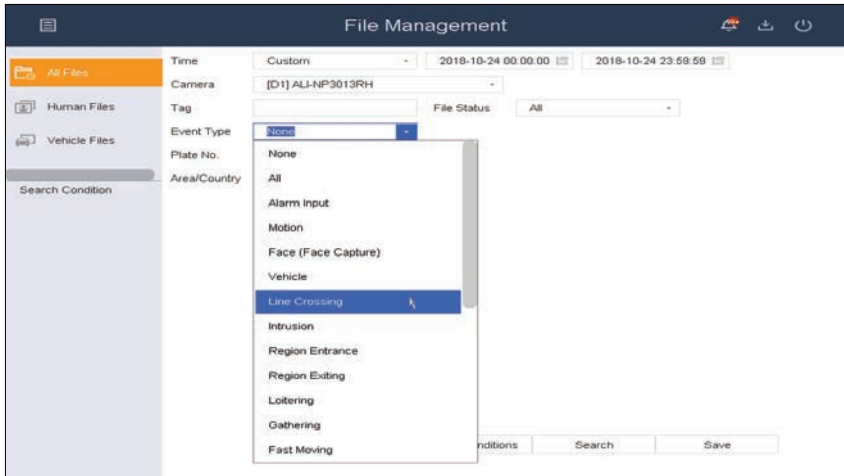
SECTION 8: RECORD, PLAYBACK AND VIDEO BACKUP



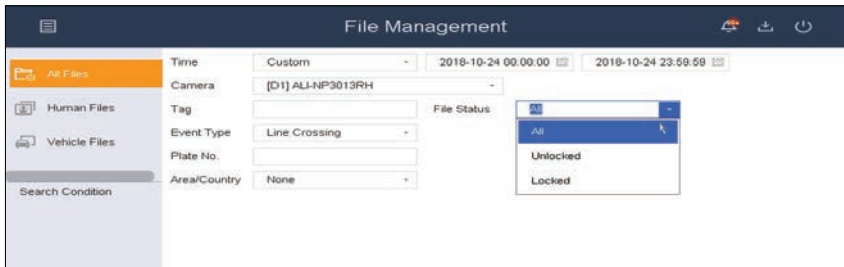
- c. Repeat the sub-step above to set the end date and time. Note that the time setup in these menus is 10/22/18 to 10/25/18.
3. Open the Camera drop-down list and select the camera(s) you want to use in the search. In the menu below, only camera channel D1 was selected.



4. In this example, skip the Tag option since we are not searching for a tagged file.
5. Next, open the Event Type drop-down list and select **Line Crossing** the event we are looking for.

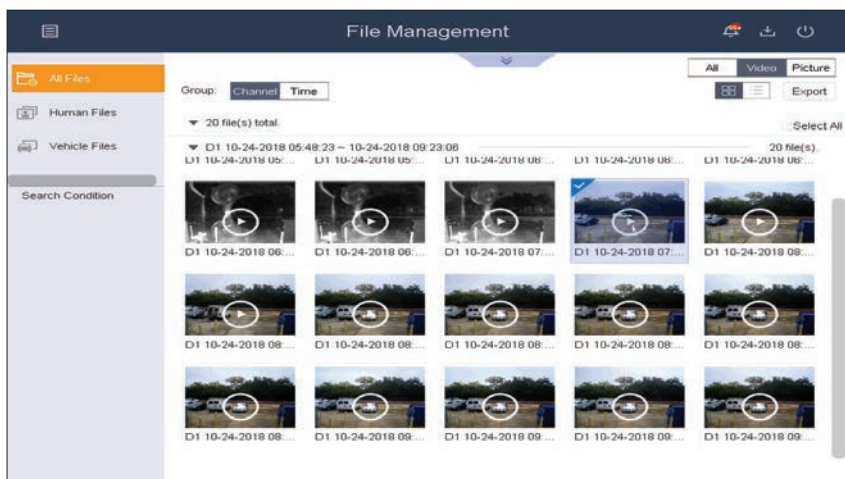


6. Notice that the File Status for the search will look at all files. If the file was locked or unlocked, should select that option. For this example, we'll select All.

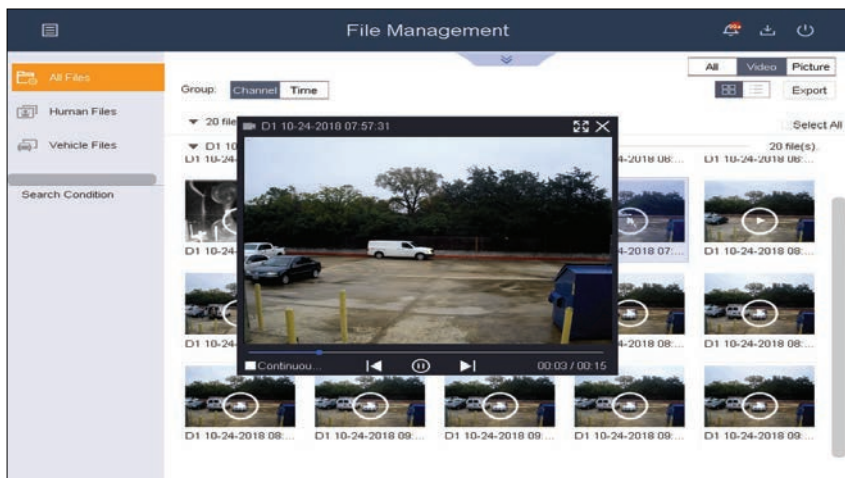


7. Click the Search button at the bottom of the screen. Search results are shown in thumbnails.

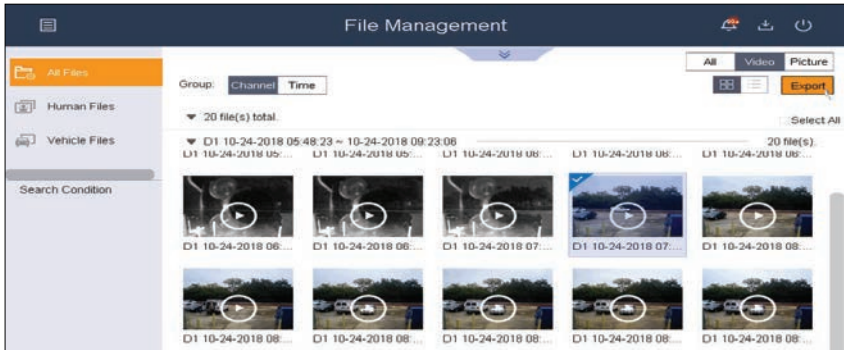
SECTION 8: RECORD, PLAYBACK AND VIDEO BACKUP



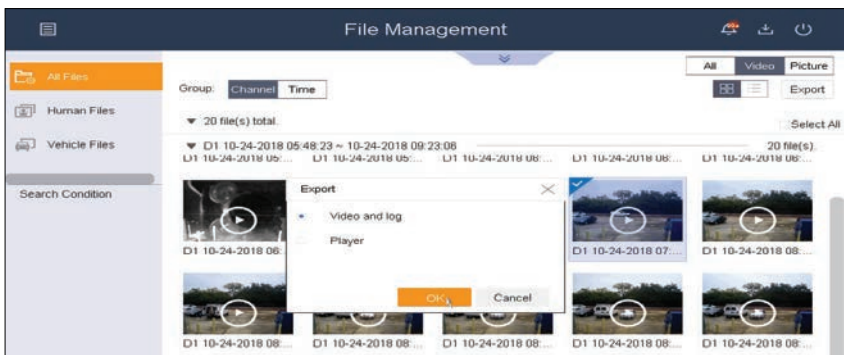
8. Click on the thumbnail for the file you are searching for to select it (see above). When the file is selected, a check mark appears in the upper left corner of the thumbnail, and the thumbnail is shadowed. To watch the video of the file, click the Play icon in the thumbnail.



9. To export the file that is selected (checked) and write it to a USB flash drive, Insert a flash drive into an unused port on the recorder, and then click the Export button.

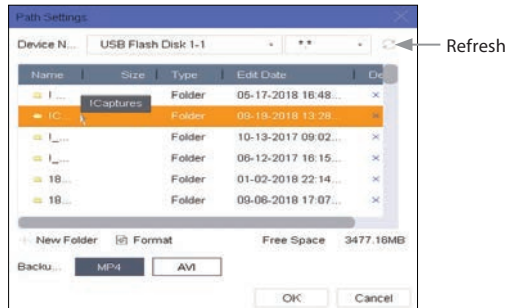


10. In the **Export** popup window, select the options you want to export. Select **Player** to export a video player with the video file and log.

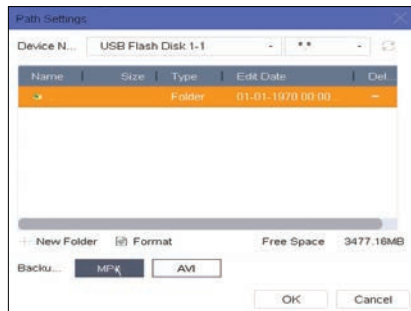


11. In the Export **Path Settings** window:
 - a. Click the **Refresh** icon to update the **Device** list. Open the **Device N...** drop down list to select another destination, if preferred.
 - b. Double click on the directory in the media where you want to save the file. The directory will open. You can hover the mouse cursor over the directory entry to show the full name.

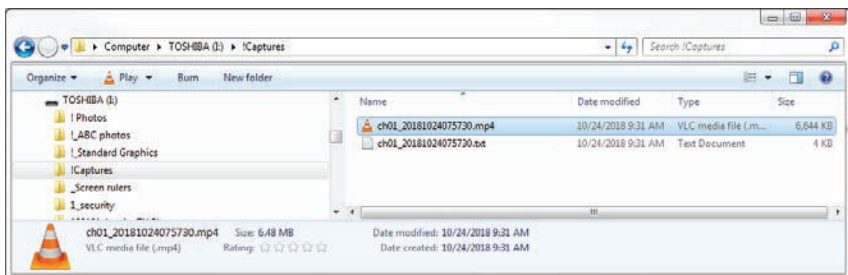
SECTION 8: RECORD, PLAYBACK AND VIDEO BACKUP



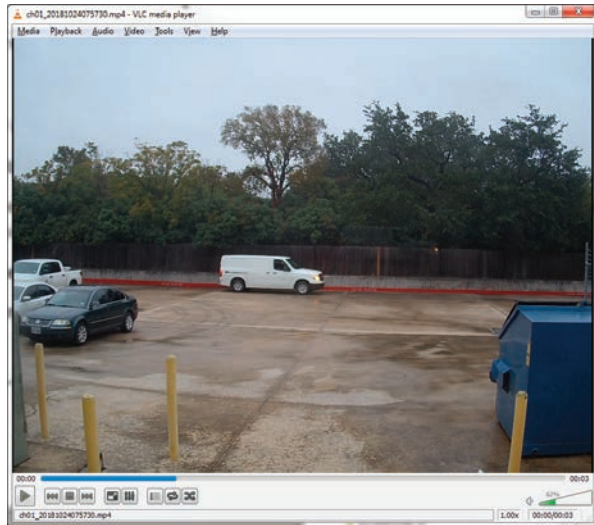
- c. Click **AVI** to change the video file format to AVI.



- d. Click **OK** to export the file(s). The Path Settings window will close.
12. Remove the USB flash drive from the recorder.
13. Plug the USB drive into a computer, and open the directory where the file was saved. The video file is highlighted in the folder shown below.

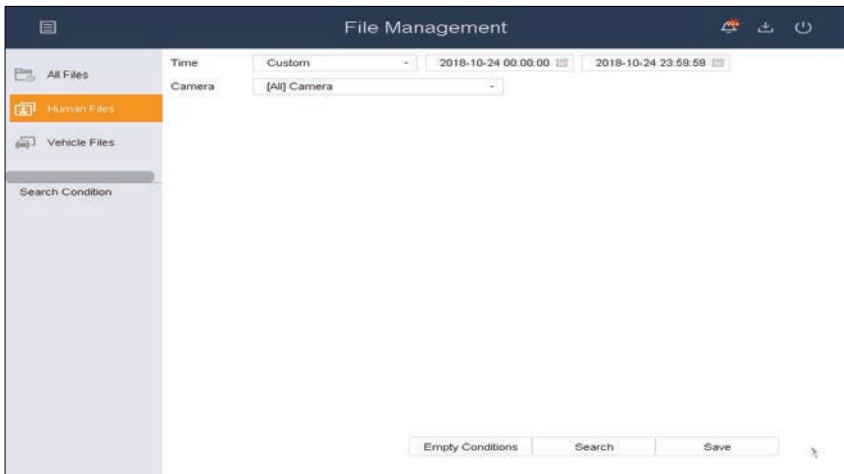


14. Play the file to ensure it is what you need. VLC Media Player was used to play this file (see below).



8.7.2 File Management - Human Files

Use the File Management Human Files menu to search for human pictures and videos. Search and export methods for these types of pictures are very similar to those for **File Management - All Files**. See “8.7.1 File Management - All Files” on page 132 for more information. The camera you use must support this feature. The **File Management - Human Files** menu is shown below.



8.7.3 File Management - Vehicle Files

Use the File Management Vehicle Files menu to search for vehicles and licence plates. Search and export methods for these types of pictures are very similar to those for **File Management - All Files**. See "8.7.1 File Management - All Files" on page 132 for more information. The camera you use must support this feature. The **File Management - Vehicle Files** menu is shown below.

The screenshot shows the 'File Management' application interface. The title bar reads 'File Management' and includes icons for refresh, download, and power. On the left, a sidebar contains three menu items: 'All Files', 'Human Files', and 'Vehicle Files', with 'Vehicle Files' highlighted in orange. Below the sidebar is a 'Search Condition' section. The main area contains search filters: 'Time' (set to 'Custom' with a date range of 2018-10-24 00:00:00 to 2018-10-24 23:59:59), 'Camera' (set to '[All] Camera'), 'Plate No.' (an empty text input), and 'Area/Country' (set to 'None'). At the bottom, there are four buttons: 'Backup Licen...', 'Empty Conditions', 'Search', and 'Save'.

SECTION 9

Managing User Accounts

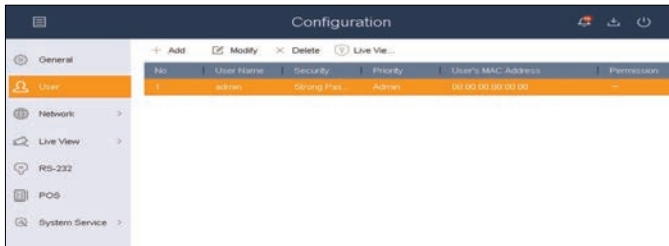
User accounts are created to control access to the system both at the NVR and when logging into the NVR from a remote computer. Each account has a User Name, Password, and a selection of permissions granted to the user.

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.

9.1 Adding a user account

1. Log into the NVR as an administrator.
2. In the Menu display, click the Configuration icon, and then click User in the left frame. Initially, the user name list appears as that shown below.

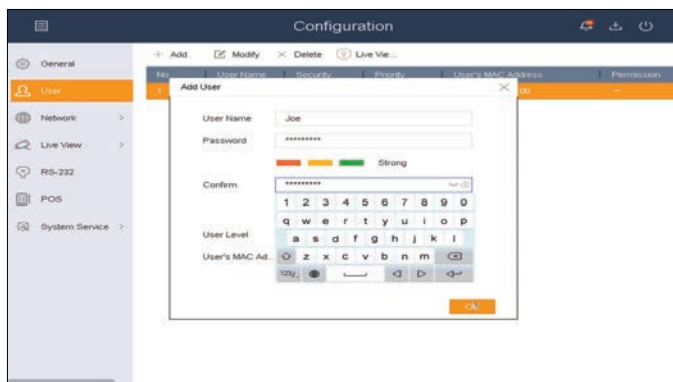


3. Click **Add** to open the Add User menu.
4. In the **Confirm Permission** popup window, enter your administrator user password, and then click **Next**.



5. In the Add User menu, enter the information for new user, including User Name, Password, Password and Confirm password, Level and User's MAC Address (optional). Ensure that the menu shows that the password you selected is a **“Strong”** password.
6. Click **OK** to continue.

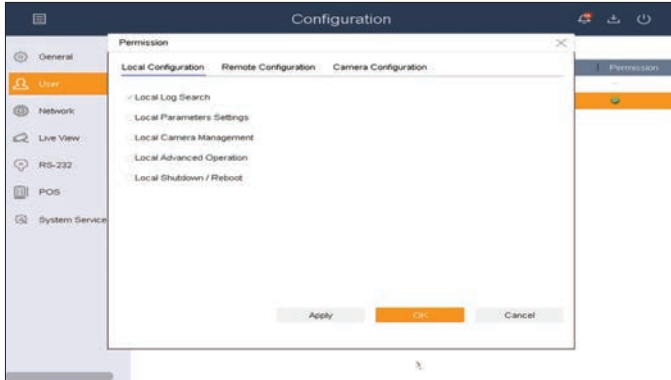
SECTION 9: MANAGING USER ACCOUNTS



7. 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.
8. **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.
9. Click the **OK** to save the settings and close the **Add User** menu. The added new user will be displayed on the list. See the screen shown below.



10. Click the **Permission** icon for the user you created (user **Joe**). The Permission lists initially show the default permissions for the user level you selected during the User Add.



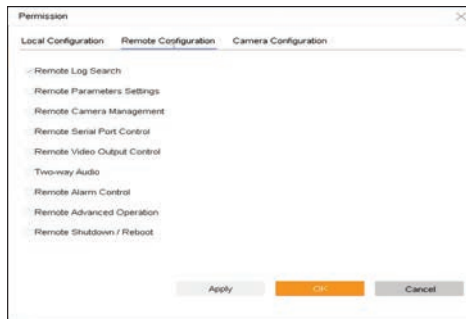
11. Check the select boxes for the additional permissions you want to assign.

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.

12. Click **Apply** and then click the **Remote Configuration** tab.

Remote Configuration options

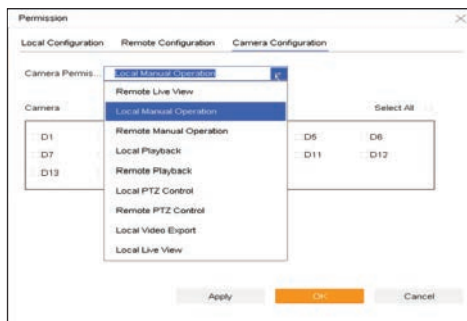


13. Check the select boxes for the additional permissions you want to assign.
 - **Remote Log Search:** Remotely viewing logs that are saved on the NVR.

SECTION 9: MANAGING USER ACCOUNTS

- **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.

14. Click **Apply** and then click the **Camera Configuration** tab.



15. In the Camera Configuration tab, open the **Camera Permis...** drop down list, select the permission you want to allow, and then check the select boxes for the camera you want to grant the permission for.

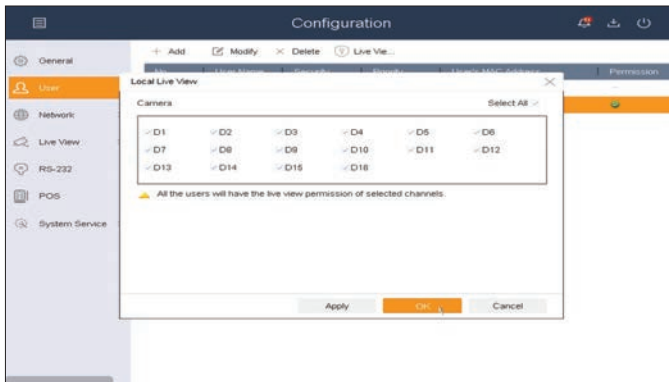
Camera Configuration

- **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).
16. Click **Apply** to save your settings for the permission you selected, and the repeat the above step for other permissions, as needed.
17. Click **OK** to save your settings and exit the **Permission** menus.

9.2 Live View Permissions on Lock screen

You can control which camera channels can be viewed when the Live View screen is locked. By default, all users can see all channels. To change this configuration:

1. In the Menu display, click the **Configuration** icon, and then click **User** in the left frame. You can delete any user account except the *admin* user.
2. Click the **Live View Permission on Lock Screen** link at the top of the screen.



3. In the **Camera** box, check or uncheck the channels you want to grant or restrict, and then click **Apply**.
4. When the normal user (Operator or Guest) has no local live view permission for specific camera (s) (refer to 17.2.2 Set Local Live View Permission for Non-Admin Users), the live view permission for such camera (s) on lock screen status cannot be configured (live view not allowed by default).

NOTE

When the an Operator or Guest user has no local live view permission for specific camera (s), the live view permission for those camera(s) on the lock screen (previous user logged out) cannot be configured (live view not allowed by default).

6. Click **Yes** in the popup window, then click **OK** in the **Local Live View** window to use the changes and continue.

9.3 Deleting a user account

1. In the Menu display, click the **Configuration** icon, and then click **User** in the left frame. You can delete any user account except the *admin* user.
2. Click the entry for the user to be deleted from the list. When the item is selected, it is highlighted.



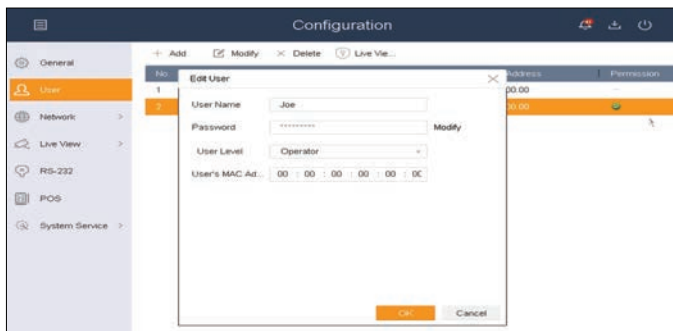
3. Click the **Delete** icon to delete the selected user.
4. Click **Yes** on the confirmation popup window.

9.4 Editing a user account

1. In the Menu display, click the **Configuration** icon, and then click **User** in the left frame. You can delete any user account except the *admin* user.
2. Click the entry for the user to be edited. When the item is selected, it is highlighted.



3. Click **Modify**.

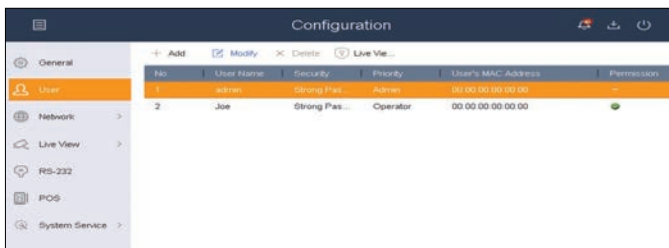


- In the **User Level** drop-down list, select either **Operator and Guest**. You can edit the user information, including user name, password, permission level and MAC address. To change the password, click **Modify** to the right of the Password field, then enter the new password in the Password and Confirm fields.
- Click **OK** to save the settings and exit the menu.
- Click the **Permission** icon on the user line to change the specific permissions for the User Level you granted. See “9.1 Adding a user account” on page 141 for more information.

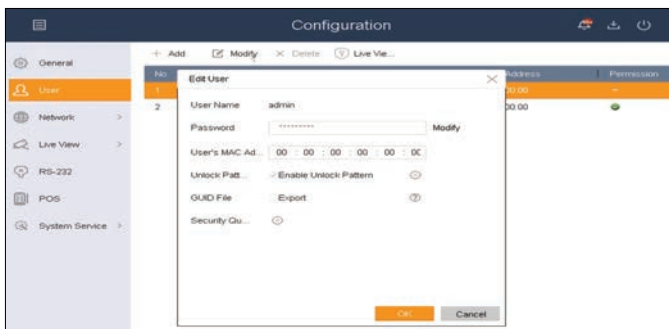
9.4.1 Modify admin user

You can change the *admin* user password and other security settings. You must log into the NVR as an admin user to change admin settings.

- In the Menu display, click the **Configuration** icon, and then click **User** in the left frame.
- Click the entry for the *admin* user to be edited. When the item is selected, it is highlighted.



- Click **Modify**.



- In the *admin* **Edit User** menu, change the settings as needed. See “2.1 System activation” on page 6 for more information.
- Click **OK** to close the menu and continue.

SECTION 10

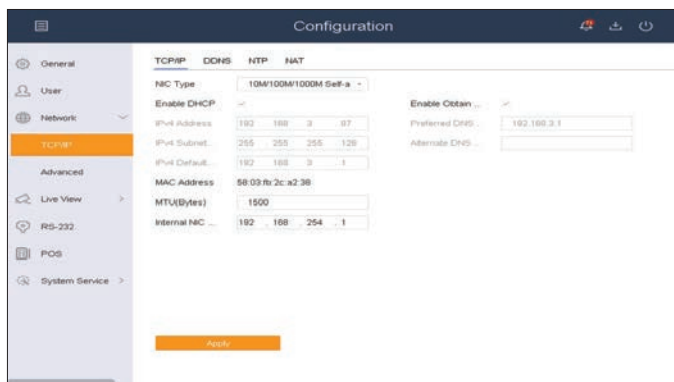
Network Settings

10.1 Configuring General Network Settings

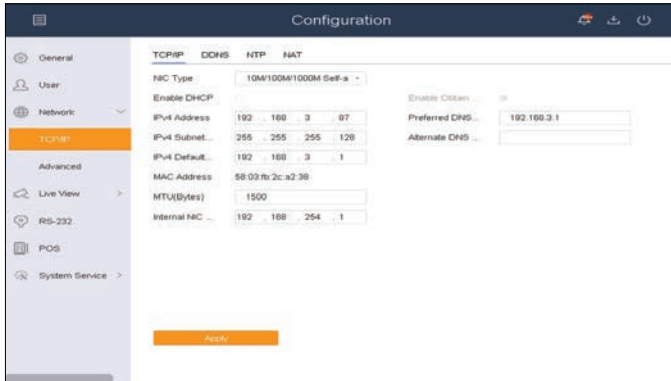
Network settings must be properly configured before you connect the NVR to cameras on the network, or access it remotely. In many cases, the IP address of your recorder should be fixed (unchanging) for easier remote access over time. Consult your network administrator to ensure you setup your recorder with compatible network settings.

If your network includes a DHCP server, you can enable DHCP in the TCP/IP menu to automatically acquire compatible network settings for your recorder from DHCP. DHCP is enabled by default. However, settings from DHCP can change over time (i.e. they are dynamic). To prevent the settings acquired from DHCP from changing (making them "fixed"), simply disable the DHCP option in the menu after acquiring DHCP network settings.

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



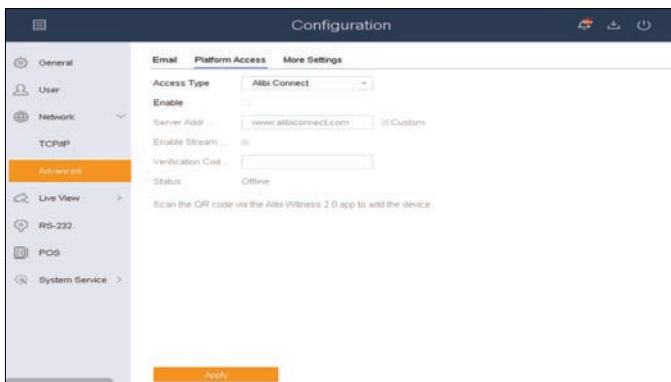
2. In the TCP/IP menu, select or enter the following parameters: NIC Type, IPv4 Address, IPv4 Gateway, MTU (valid range is value range of MTU is 500 ~ 9676) and DNS Server IP addresses. If the DHCP server is available, check the Enable DHCP box to automatically obtain an IP address and other network settings from the network DNS server.
3. Check the **Enable Obtain** select box to obtain the DNS Server Address address automatically.
4. Enter the Internal NIC IPv4 Address, if necessary, to assign IP addresses to the cameras connected to the PoE interfaces.
5. Click **Apply** to save your settings.
6. If you used DHCP to acquire network settings, you can retain those settings by un-checking the **Enable DHCP** box, and then clicking **Apply**. See below.



10.2 Configuring Advanced Settings

10.2.1 Platform Access setup

Alibi Connect access platform can be used for Alibi Witness 2.0 smartphone app access by creating a direct peer-to-peer connection. It can also be used to download recorder firmware updates and enables the DDNS platform.



1. To use the Alibi Connect access platform, check the Enable box, and then click **Apply**. A Terms of Service window will open.
2. In the **Terms of Service** window shown below:

SECTION 10: NETWORK SETTINGS



- a. Scan the QR code to open the **Terms of Service** for using this feature. Read the agreement thoroughly.
- b. If you agree with the ToS, check the box in the middle paragraph to acknowledge it.
- c. In the **Verification Code** field, enter a **unique** identifier for your system, and then click **OK** to return to the **Performance Access** menu. The **Verification Code** should contain 6 to 12 characters with letters (a to z, A to Z) and numbers (0..9) and is case sensitive. The code **OBSdevice** was entered here.



3. In the screen below, check the **Enable Screen Encryption** box to use this feature, if you prefer to do so, and then click **Apply** to continue.

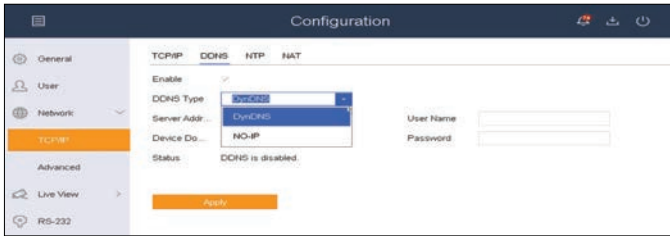


- Click **Apply** to save your settings.

10.2.2 Configuring DDNS

If your NVR is set to use PPPoE as its default network (Internet) connection, you may set Dynamic DNS (DDNS) to be used for network access. **DynDNS** and **NO-IP** are supported. Registration with your ISP is required before configuring the system to use DDNS.

- Open the Network Settings menu. Go to **Menu | Configuration | Network | TCP/IP**.
- Click the **DDNS** tab to open the DDNS Settings menu.



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

— **DynDNS:**



- Enter Server Address for DynDNS (i.e. members.dyndns.org).
 - In the NVR Domain Name text field, enter the domain obtained from the DynDNS website.
 - Enter the User Name and Password registered in the DynDNS website.
- **NO-IP:** Enter the account information in the corresponding fields.
- 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.

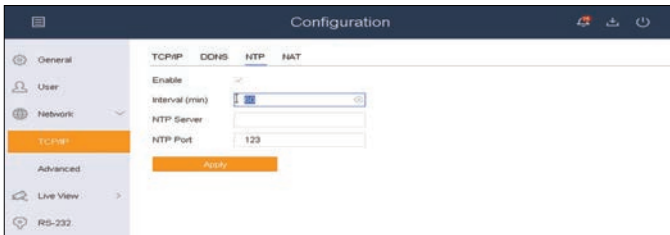


- iv. Enter **Server Address** for NO-IP (*dynupdate.no-ip.com*).
- v. In the **Device Domain Name, User Name** and **Password** fields, enter the information setup at the *alibiddns.com* website. For example: <your domain name>.alibiddns.com
- vi. Click **Apply** to save your settings.

10.2.3 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 | TCP/IP**.
- 2. Click the **NTP** tab to open the NTP Settings menu.

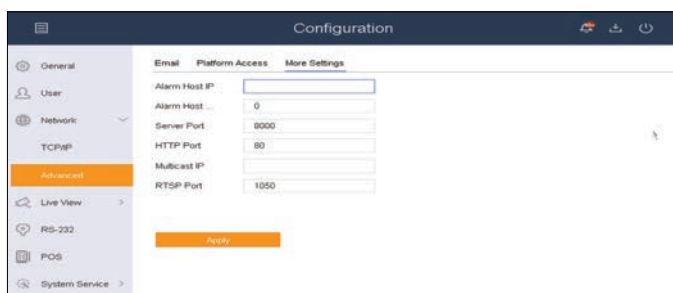


- 3. Check the **Enable NTP** box to enable this feature.
- 4. Select the following NTP settings:
 - **Interval:** Interval in minutes between the two synchronizing actions with an NTP server.
NOTE: The synchronization time interval can be set from 1 to 10080 minutes. The default value is 60 min. If 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
5. Click **Apply** to save your settings and close the menu.

10.2.4 Configuring Remote Alarm Host

With a remote alarm host, **Alibi CMS**, configured, the NVR will send the alarm event or exception messages to the host when an alarm is triggered. This feature is configured on the **Menu | Configuration | Network | Advanced | More Settings** menu.



1. In the menu shown above, configure the following appropriately:
- **Alarm Host IP/Port:** Set the **IP** address and port number of the PC with the Alibi CMS (ACMS) client software. **Port** is the port number configured in ACMS used to receive alarm event and exception messages.
 - **Server Port:** Server port (8000 by default) configured for remote client software access. The valid range is 2000 to 65535.
 - **HTTP Port:** HTTP port (80, default) is configured for remote web browser access.
 - **Multicast IP:** Multicast can be configured to enable Live View for cameras that exceed the maximum number allowed through the network. Using the multicast function, more than 64 cameras are connectable. A multicast IP address covers Class-D IP ranging from 224.0.0.0 to 239.255.255.255 and it is recommended to use an IP address ranging from 239.252.0.0 to 239.255.255.255. When adding a device to the ACMS, the multicast address must be the same as that of the device.
 - **RTSP Port:** RTSP (Real Time Streaming Protocol) is a network control protocol designed to control streaming media servers. The port is 554 by default.

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

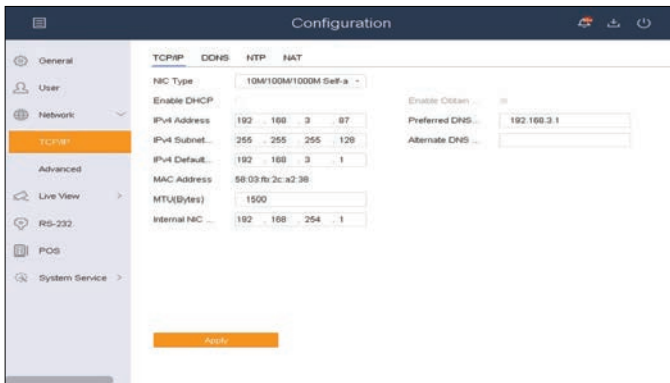
2. Click **Apply** to save your settings and close the menu.

10.2.5 Configuring Email

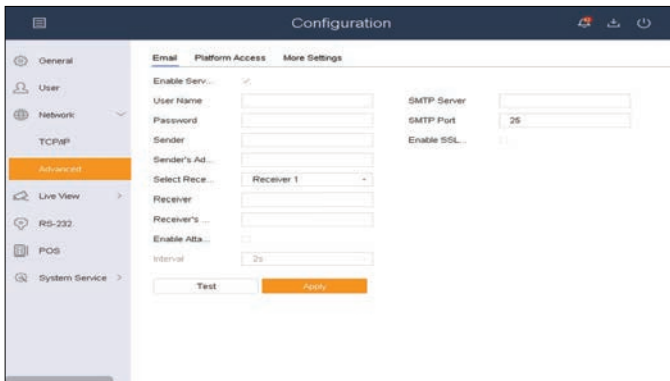
The system can be configured to send an Email notification to up to three designated users if an alarm event is detected, an alarm or motion event is detected or the administrator password is changed.

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.

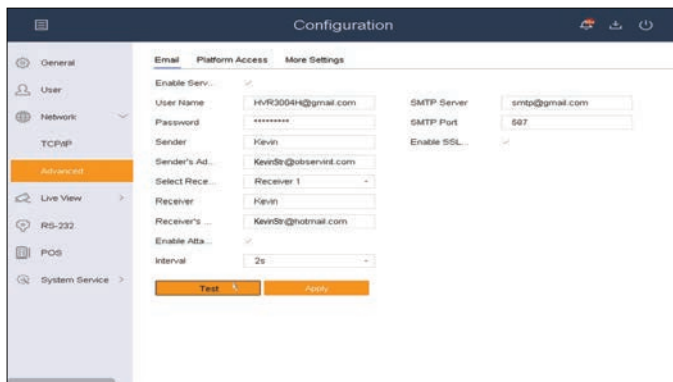
1. Open the Network Settings menu. Go to **Menu | Configuration | Network | TCP/IP**.
2. Set the IPv4 Address, IPv4 Subnet Mask, IPv4 Gateway and the Preferred DNS Server in the Network Settings menu.



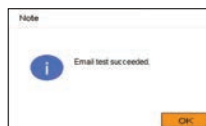
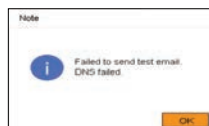
3. Click **Apply** to save your settings and close the menu.
4. Click the **Email** tab to open the email settings menu.



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.



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

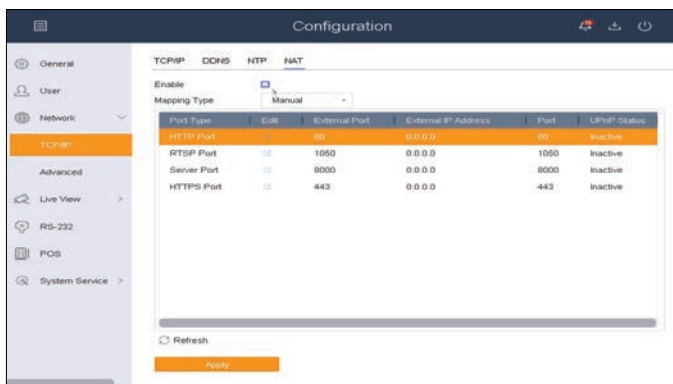


10.2.6 Configuring UPnP™

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.

1. Open the Network Settings menu. Go to **Menu | Configuration | Network | TCP/IP | NAT**.



2. If your router supports UPnP and you want to configure it for port forwarding, check the **Enable** box. **NOTE:** To use UPnP, UPnP usually must also be enabled in the router.
3. 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.
4. If settings in this menu were changed, click **Refresh**, and then click **Apply** to save the changes.

SECTION 11

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.

11.1 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.

1. Open the Device Information display for the NVR. Go to **Menu | Maintenance | System Info | Device Info**.



To view information about other components of the system, click the appropriate link in the left frame.

11.2 Search Log Information, Log Export

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

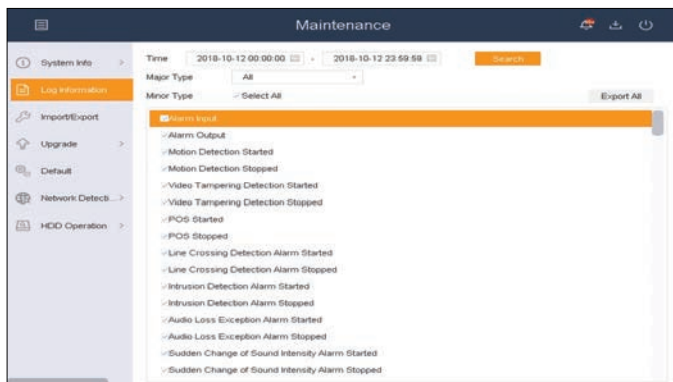
- **Alarms events** - Start / stop motion detection, start / stop tamper detection etc.
- **Exception conditions** - Video loss, illegal login, HDD full / error, IP camera disconnected, network disconnected, etc.
- **Information events** - Start / stop recording, local / network HDD information, HDD 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.

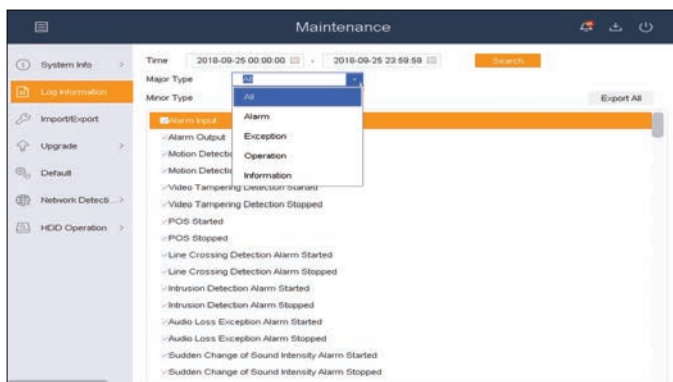
11.2.1 Log Search

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

SECTION 11: SYSTEM MAINTENANCE



2. Click on the left **Time** field, and then use the GUI to select the beginning date and time to search for log entries. Similarly, click the right **Time** field and select the end date and time to search for log entries.
3. Open the **Major Type** drop down list, and select the major type alarms you want to search for. In the example below, **All** was selected. Each major alarm type has its own set of minor type alarms.



4. In the Minor Type list (see above), check the select boxes for the specific alarms you want to find.
5. Click **Search**. In the example below, the search criterion specified was **All** Major Type alarms and all **Minor Type** alarms on 10/12/18.

No.	Major	Time	Minor Type	Parameter	Play	Details
1	IO	10-12-2018 09 19 27	Power On	N/A		
2	Inf	10-12-2018 09 19 27	Local HDD Information	N/A		
3	IO	10-12-2018 09 19 35	Local Operation: Login	N/A		
4	Ex	10-12-2018 09 19 35	Network Disconnect	N/A		
5	Inf	10-12-2018 09 19 25	Start Capture	N/A	▶	
6	Inf	10-12-2018 09 19 45	IP Camera Connection ...	N/A		
7	Inf	10-12-2018 09 20 01	HDD S.M.A.R.T.	N/A		
8	Ex	10-12-2018 09 20 02	IP Camera Disconnect	N/A		
9	Ex	10-12-2018 09 20 02	Video Loss Alarm	N/A		
10	Inf	10-12-2018 09 20 30	IP Camera Connection ...	N/A		
11	Inf	10-12-2018 09 20 31	Start Capture	N/A	▶	
12	Inf	10-12-2018 09 20 31	IP Camera Connection ...	N/A		
13	Inf	10-12-2018 09 20 34	IP Camera Connection ...	N/A		
14	Inf	10-12-2018 09 20 37	IP Camera Connection ...	N/A		
15	Al	10-12-2018 09 20 37	Motion Detection Started	N/A		

Total: 1922 P: 1/20

In the search results list, multiple pages of log entries might be presented here. Use the icons in the lower left corner to navigate between pages. Up to 1000 alarm entries can be displayed from a search.

- To view more information about a specific log entry
 - Double click on the alarm entry.

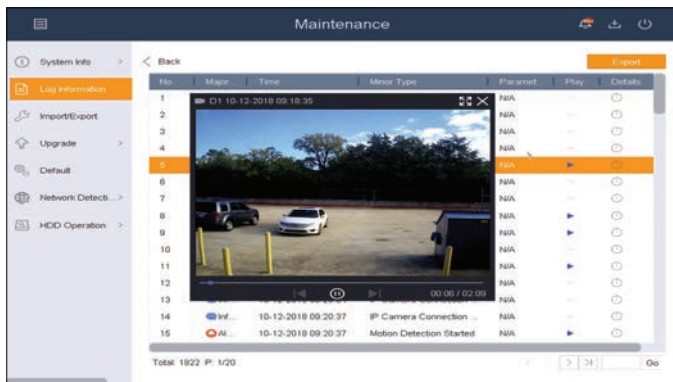
Click icon to see video

No.	Major	Time	Minor Type	Parameter	Play	Details
Log Information						
Time	10-12-2018 09 19 25					
Type	Information-Start Capture					
Local User	N/A					
Host IP Address	N/A					
Parameter Type	N/A					
Camera No.	D1					
Description						
Camera D1 starts capturing. Capture status:						
Capture enabled: Yes						
Event parameters: Disabled						
Capturing type: Command Triggered						
Motion detected on camera: None						
Alarm detected on camera: None						
MicroSD status: No						
<input type="button" value="Previous"/> <input type="button" value="Next"/> <input type="button" value="OK"/>						
14	Inf	10-12-2018 09 20 37	IP Camera Connection ...	N/A		
15	Al	10-12-2018 09 20 37	Motion Detection Started	N/A		

Total: 1922 P: 1/20

- If the log entry includes an icon in the **Play** column, video is associated with the entry. Click the icon to watch the video.

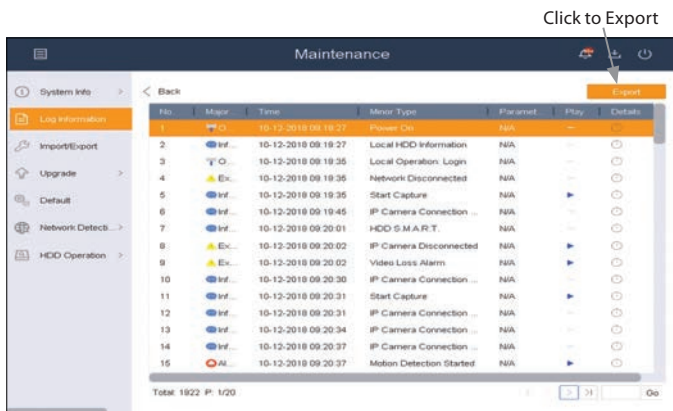
SECTION 11: SYSTEM MAINTENANCE



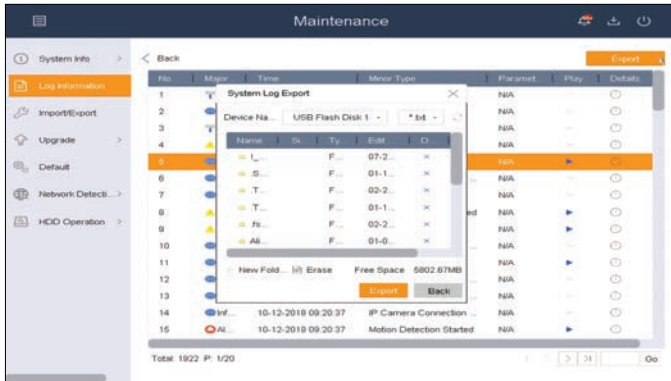
11.2.2 Log Export

You can export the log information resulting from a search (see “11.2.1 Log Search” on page 157) 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:

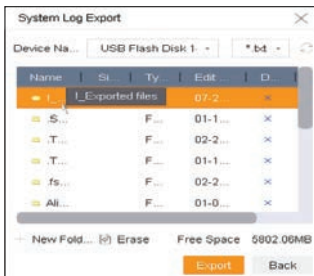
1. Perform a Log Info search for information you want to save.
2. To export the search result to a flash drive, insert the flash drive into any unused USB port on the NVR.



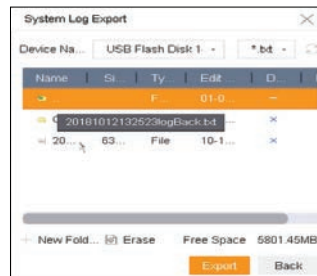
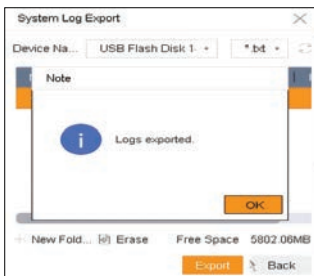
3. In the Search Result window, click the Export button.



- In the **Log Export** window, hover the mouse over the directory entry (see left window below) in the list to see the directory name. Double click on the directory in the flash drive where you want to save the search results (see right window below) to select the directory.



- Click the **Export** button to save the search data. The export status is shown (see left window below). You can hover the mouse over an entry in the folder (see right window below) to see the file name.

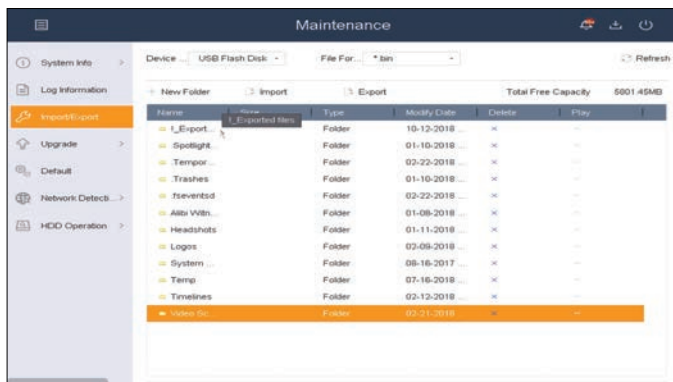


- Click **Back**, and then remove the flash drive from the NVR.

11.3 Export system configuration

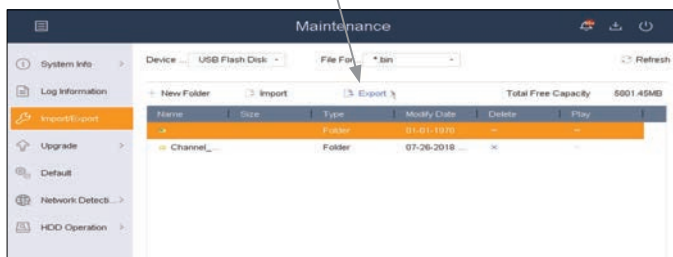
You can export the NVR configuration, then import the file later to restore the earlier configuration if needed. Use this procedure to backup your system settings whenever the configuration is changed. The configuration backup file is a binary file with a timestamp in the format `devCfg_<code>_YYYYMMDDHHMMSS.bin`. You must be logged into the NVR as the system administrator to perform this procedure.

1. Plug an USB storage device, such as a USB flash drive or USB disk drive, into an NVR USB port.
2. Open the **Import / Export** menu. Go to **Menu | Maintenance | Import/Export**.



3. Click **Refresh** if necessary to locate the flash drive. The name list shows the folders available on the flash drive.
4. Locate the folder where you want to save the configuration file, and double click on it to open it. You can hover the mouse over the directory entry in the list to see the directory name (see above).
5. Double click on the directory in the flash drive where you want to save the configuration file (see below).

Click to Export



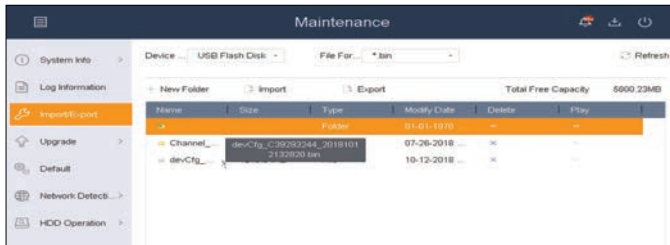
6. Click the **Export** button (see callout above). In the popup Export Encryption window, enter your administrator password, and then click **OK** to perform the export.



- A Note popup window will show the export status.



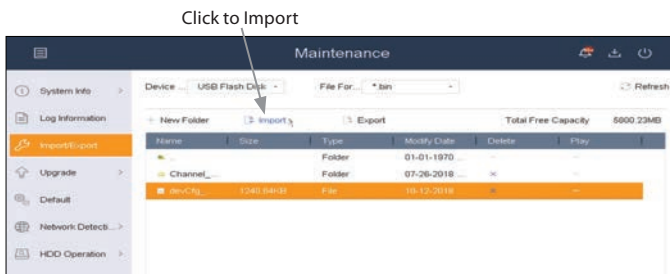
- You can hover the mouse over the file to see the filename.



11.4 Import system configuration

You can import a system configuration file you saved earlier to restore your NVR to that state. See “11.3 Export system configuration” on page 162 for more information. The procedure below uses the configuration file created above to restore the system. You must be logged into the NVR as the system administrator to perform this procedure.

- If the configuration file you saved is on a flash drive, insert the flash drive into an unused USB port on your NVR.
- Locate the file on the flash drive and select (highlight) it.

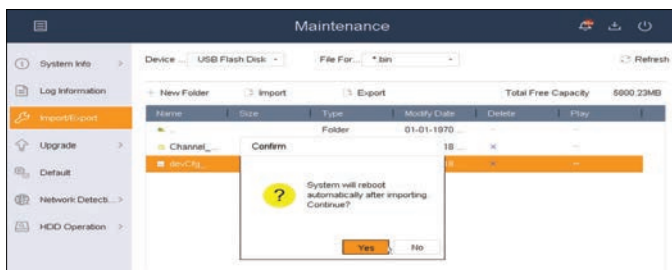


SECTION 11: SYSTEM MAINTENANCE

- Click the Import button (see callout above). In the popup **Import Encryption** window, enter your administrator password, and then click **OK** to perform the export.



- After the configuration file is imported, a system reboot is required. Follow the on-screen instructions to complete the procedure.



11.5 Upgrade Firmware

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

- To check the current firmware version, open the System information display. Go to **Menu | Maintenance | System Info | Device Info**.

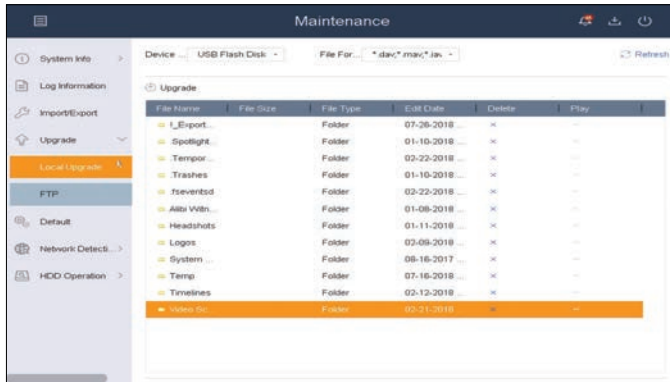


- Find the firmware version of your recorder on the **Device Info** screen. If a newer version exists, you can install it from a local flash drive or from a server.

Local Upgrade - from flash drive

You can upgrade the firmware in your recorder from a local device such as a flash drive:

1. Insert a flash drive with newer NVR firmware into an unused USB port of your recorder.
2. Open the Local Upgrade menu. Go to **Menu | Maintenance | Upgrade | Local Upgrade**.

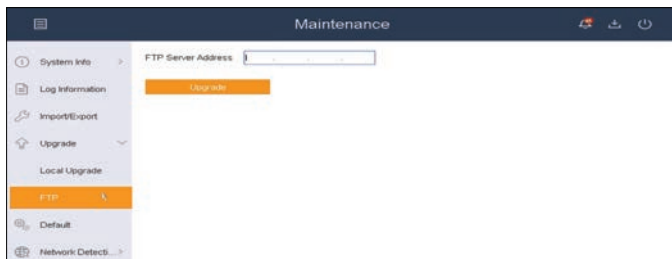


3. Click the Refresh button (located at the top of the menu), and then navigate to the folder that contains the new firmware.
4. Click the firmware file you want to load. The firmware file normally has the file name extension **.dav**.
5. Click the **Upgrade** button, then follow the on-screen instructions for completing the upgrade. The upgrade may require a reboot of the recorder.
6. Allow the upgrade operation to complete before continuing.

11.5.1 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. Open the Upgrade FTP menu. Go to **Menu | Maintenance | Upgrade | FTP**.



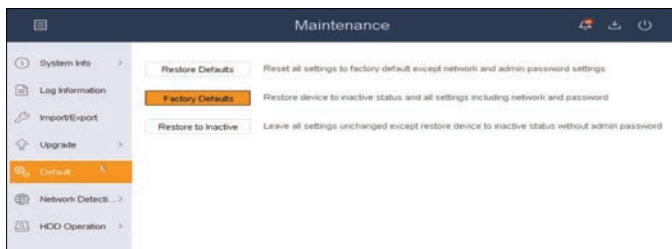
2. Click in the FTP Server Address field to open the virtual keyboard, and then enter the IP address of the server.
3. Click the **Upgrade** button at the bottom of the window, and follow the on-screen instructions to complete the upgrade.

11.6 Default - restore NVR

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 default options menu. Go to **Menu | Maintenance | Default**.



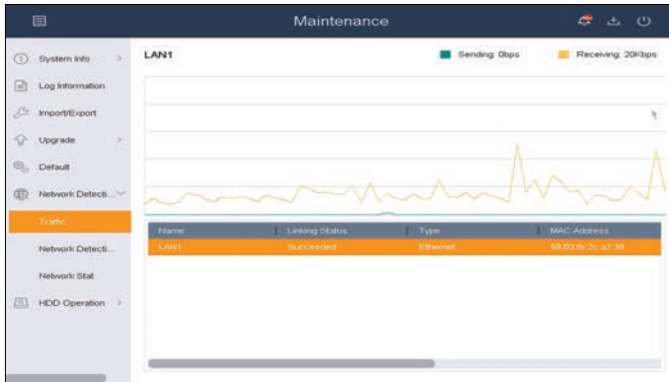
2. Click one of the following options:
 - **Restore Defaults:** Restore all parameters, except the network (including IP address, subnet mask, gateway, MTU, NIC working mode, default route, server port, etc.) and user account parameters, to the factory default settings.
 - **Factory Defaults:** Restore 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.

11.7 Net Detect

11.7.1 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**.



11.7.2 Testing Network Delay and Packet Loss

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

The screenshot shows the 'Maintenance' interface with the 'Network Delay, Packet Loss Test' section. The form includes the following fields and buttons:

- Select NIC:** LAN1
- Destination Address:** 192.168.3.65
- Test:** A prominent orange button.
- Network Packet Export:** A section with:
 - Device Name:** USB Flash Disk 1-1
 - Refresh:** A button.
 - Status:** A button.
- LAN1:** 192.168.3.97 | 10Kbps
- Export:** A button.

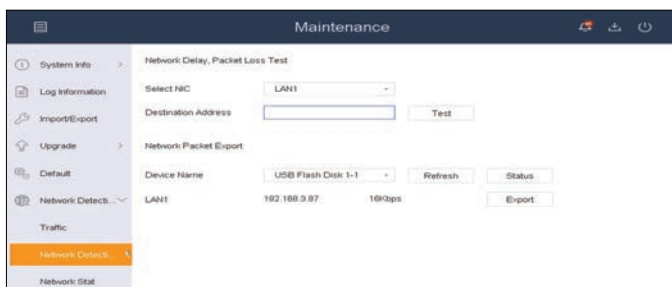
- Click on the Destination Address field, and then enter the destination IP address the field. In the screen above, the address **192.168.3.65** was entered.
- Click the **Test** button to begin the test for network delay and packet loss. The testing result appear in the window. If the testing failed, the error message box will open.



11.7.3 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.

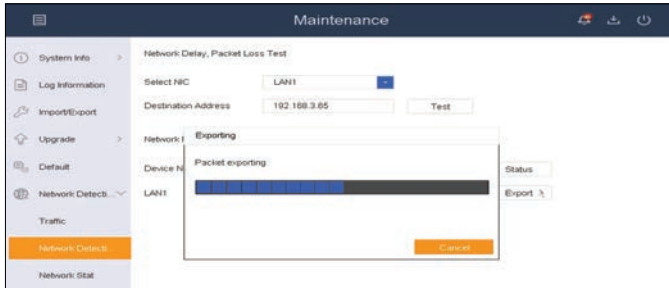
- Open the Network Traffic menu. Go to **Menu | Maintenance | Net Detect | Net Detection**.



- Insert a USB device such as a flash drive, HDD, DVD-R / W and other local USB backup devices into a USB port on the NVR, and then click **Refresh**.
- Select the backup device from the **Device Name** drop down list. **USB Flash Disk 1-1** was selected. See above.

Note: Click the **Refresh** button again 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.

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



- When the export is complete, a **Note** window will open showing the export status. Click **OK**. Up to 1 M data can be exported during one operation.



11.7.4 Checking the network status

If problems are detected during export operation, check the network configuration. Go to:

Menu | Maintenance | System Info | Network.

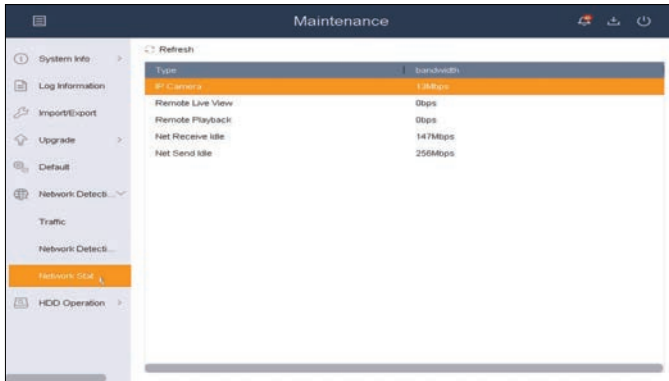


11.7.5 Checking Network Statistics

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

SECTION 11: SYSTEM MAINTENANCE

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

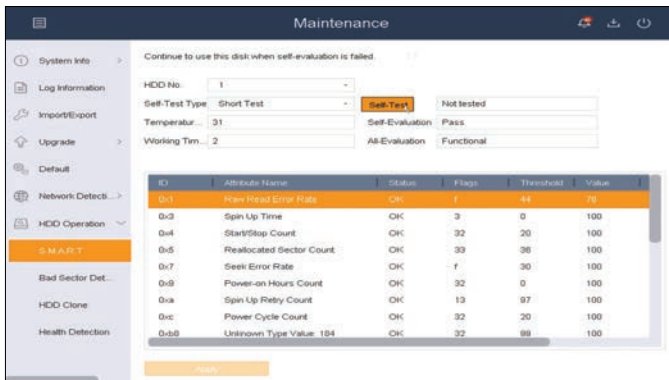


Use this display to check the bandwidth of the IP Camera, bandwidth of Remote Live View, bandwidth of Remote Playback, bandwidth of Net Receive Idle and bandwidth of Net Send Idle. Click the **Refresh** button to show the current status.

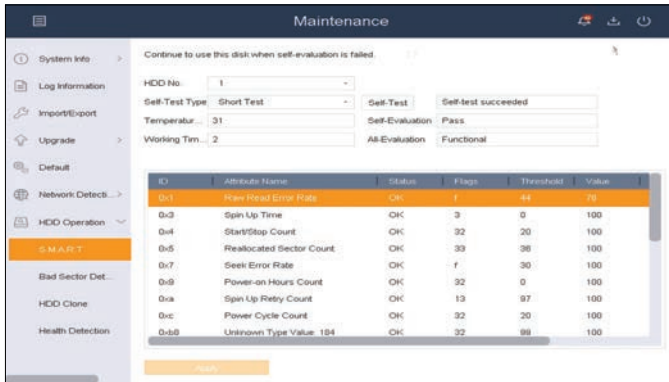
11.7.6 HDD - S.M.A.R.T. testing and monitoring

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.

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.



2. To execute a self-evaluation test on an HDD:
 - a. On the **HDD** line, open the drop down list to select the HDD you want to test.
 - 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 **Self Test** button to execute the test. Allow the test to complete before continuing. The result of the test is shown on the Self-evaluation line.



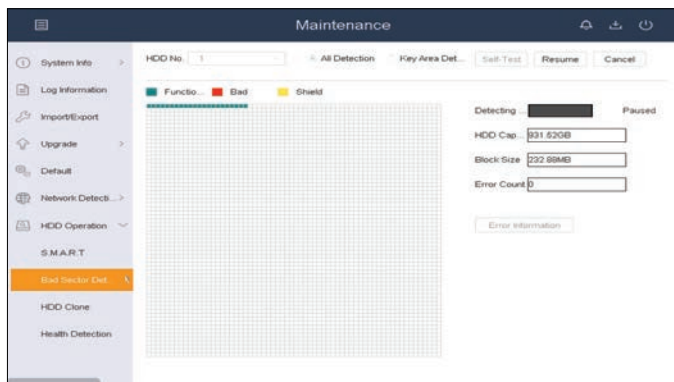
3. Examine the S.M.A.R.T. data provided for the HDD. Check to ensure that the data in the value and Worst column does not exceed the data in the Threshold column.

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.

11.7.7 HDD - Bad Sector Detection

1. Open the Bad Sector Detection menu. Open the Menu screen, and then click the **Maintenance** icon.
2. In the left frame, click **HDD Operation** to open the options list, and then click **Bad Sector Detection**.
3. At the top of the menu, open the HDD No. drop down list and select the HDD you want to test.
4. Check the select box for either **All Detection** or **Key Area Detection**.
5. Click the **Self Test** button to begin the test. 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.

11.8 HDD Disk Clone

The Disk Clone feature is used to copy an internal HDD to a writable storage device connected to the eSATA port. The capacities of the source drive (internal HDD) and the eSATA storage device must be the same.

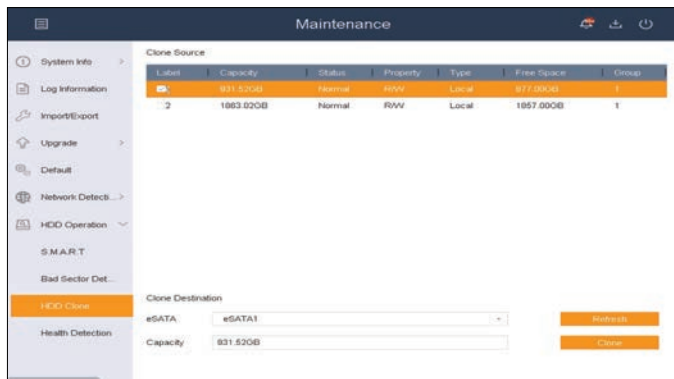


WARNING

- When cloning an internal HDD source drive to the eSATA storage device, no data can be written to the source drive.
- The cloning operation for a typical internal HDD can take several hours.

To use this feature:

1. Open the Disk Clone menu. Go to **Menu | Maintenance | HDD Operation | Disk Clone**.



2. Attach a destination storage device to the eSATA connector on the NVR back panel.
3. In the **Disk Clone** menu, check the select box for the internal HDD you want to clone. In the screen above, the select box for HDD 1 is checked.
4. Open the eSATA drop-down list, and then select the eSATA port where the destination storage device is attached.
5. Click **Clone**.
6. Allow the operation to complete before continuing.

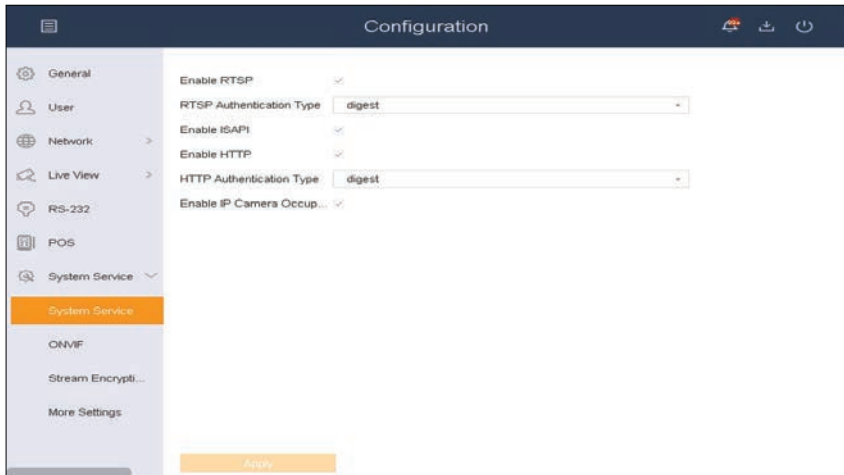
11.9 System Service options

System Service options enables you to control remote access to the different streaming protocols in the system.

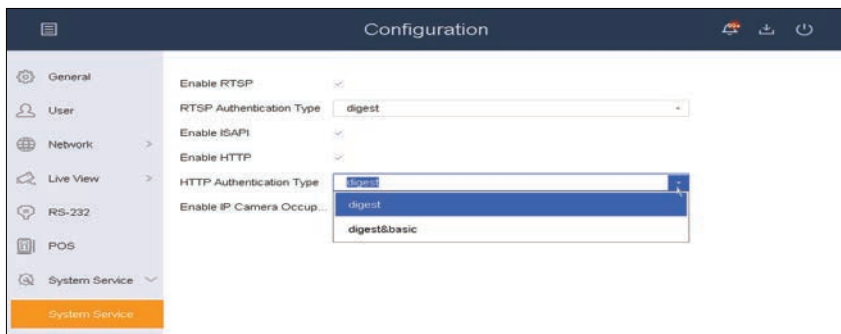
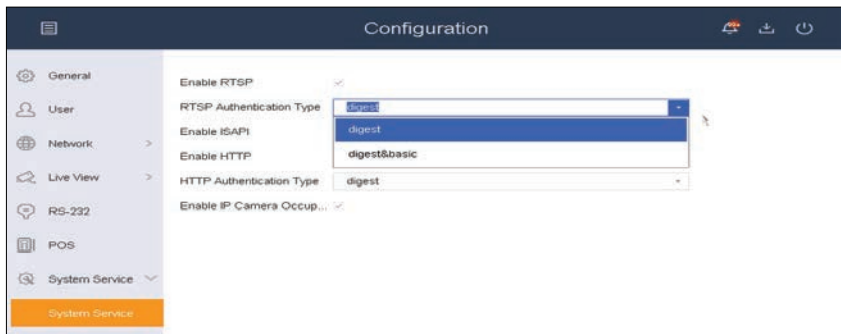
11.9.1 System Service

Use the System Service menu to enable/disable remote streaming and/or connectivity.

1. To open the System Service menu, go to **Menu | Configuration | System Service | System Service**.



2. Uncheck the box(es) next to the protocols to disable those features.
3. Open the **RTSP Authentication Type** and **HTTP Authentication Type** drop down lists, and select either **digest** or **digest&basic** as required by the remote client.

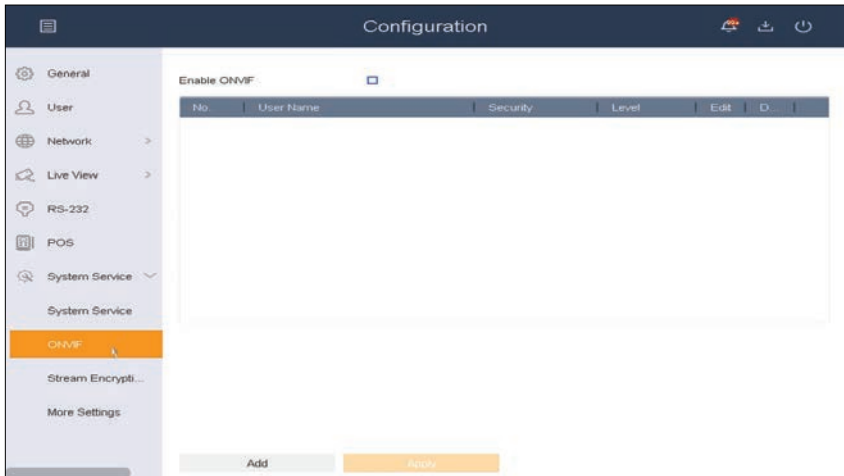


4. Click **Apply** to save the new settings.

11.9.2 ONVIF

ONVIF enables the recorder to be discovered and added to other VMS clients as an ONVIF device. Access to the device is controlled by user authentication.

1. To open the ONVIF menu, go to **Menu | Configuration | System Service | ONVIF**.

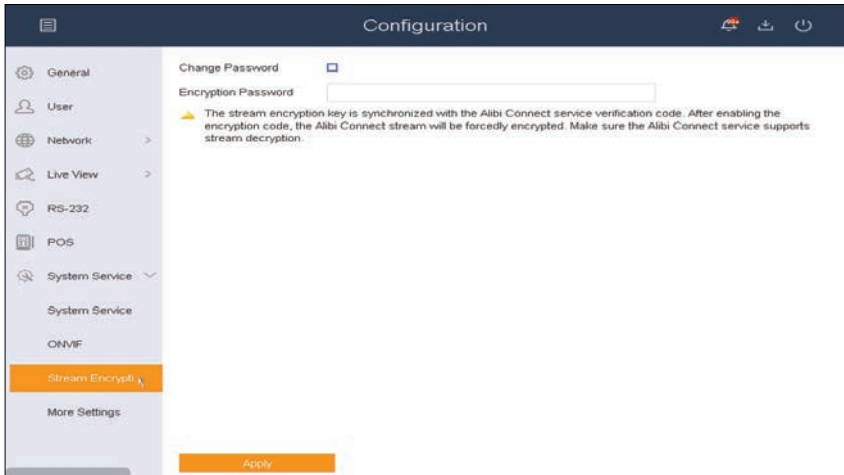


2. To enable the **ONVIF** feature, check the select box, and click **Apply**.
3. To create users who can access the device, click the **Add** button, and follow the menu to register a **User Name** and **Password**.

11.9.3 Stream Encryption

Stream encryption is used to encrypt the streams for live view, playback, download, backup, etc. to improve the security of your system. The stream encryption password is synchronized with the Alibi Connect service verification code. After enabling the encryption code, the Alibi Connect stream will be forcedly encrypted. Make sure your Alibi Connect service supports stream encryption. To use Stream Encryption:

1. Open the Stream Encryption menu. Go to **Menu | Configuration | System Service | Stream Encryption**.



2. Check the select box to enable **Stream Encryption**, and then enter an encryption code in the field shown.
3. Click **Apply**.

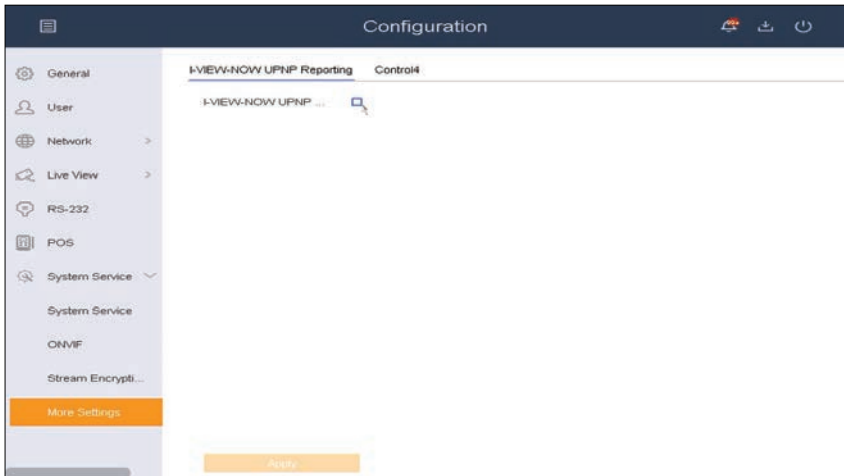
11.9.4 More Settings

More Settings menu includes two tabs:

- The **I-VIEW-NOW UPNP Reporting** is a video verification service that works with numerous central stations for video verified alarm responses. Check with your central station provider to verify support and if you are able to offer this service. If applicable, check the box to enable UPnP reporting to link the recorder to the central station service..
- The **Control4** is a home automation provider. Enabling the SDDP and CGI commands allow the Control 4 system to make changes to the HDMI display out on a display. A user credential must be created and the appropriate Control 4 driver must be installed to support the NVR.

I-VIEW-NOW UPNP Reporting

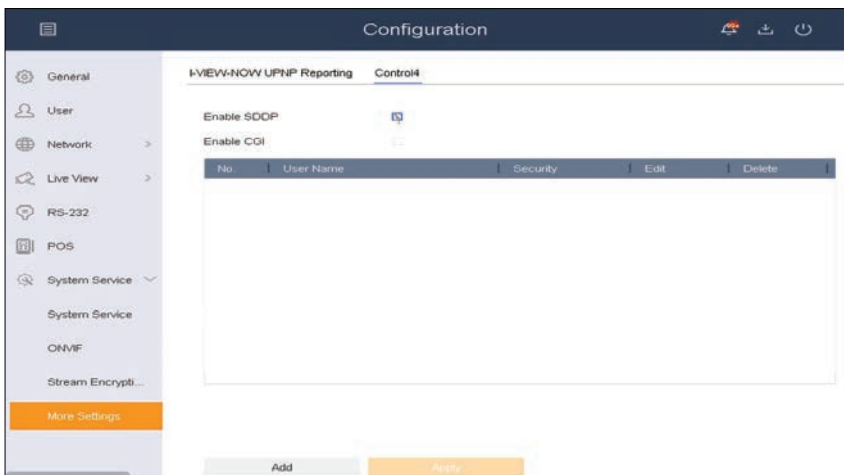
1. To open the More Settings **I-VIEW-NOW UPNP Reporting** menu, go to **Menu | Configuration | System Service | More Settings**.



2. To use **I-VIEW-NOW UPNP Reporting**, check the select box shown above.
3. Click **Apply**.

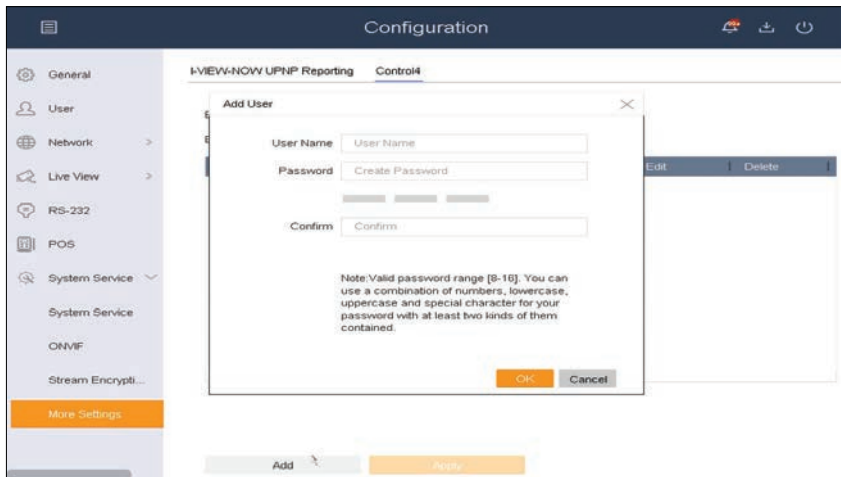
Control4

1. To open the More Settings **Control4** menu, go to **Menu | Configuration | System Service | More Settings**.
2. Click the **Control4** tab.



SECTION 11: SYSTEM MAINTENANCE

- To use **Control4**, check the select box for **Enable SDDP** or **Enable CGI**.
- Click **Apply**.
- Click the **Add** button, and then follow the on-screen instructions setup the credentials for user access to the devices added to Control4



- Click **Apply**.

SECTION 12

Managing HDDs

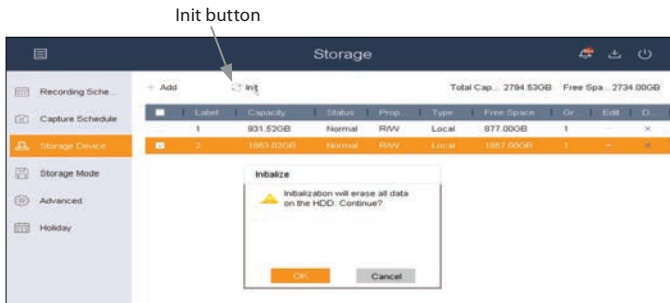
NVR storage (HDDs) is highly configurable. You can simply save data to the internal HDD(s) in the chassis, or add network based NAS or IP SAN devices to the system and save recordings and other data there. You can also define where data for each camera or groups of cameras is saved, and have 16 different 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 “12.1 Initializing HDDs” on page 179 for more information.

12.1 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 Storage Device menu. Go to **Menu | Storage | Storage Device**.

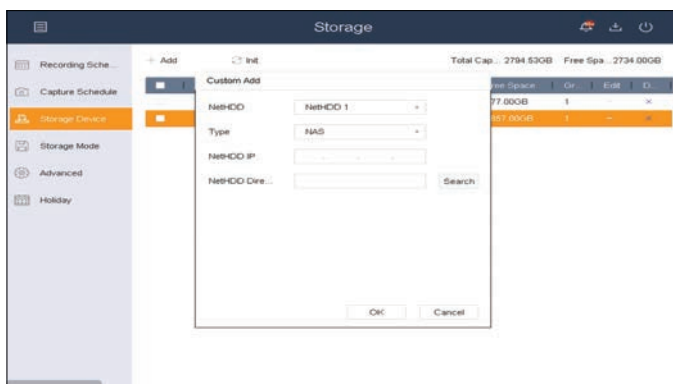


2. Check the status of the HDD. If the status is:
 - **Normal** or **Sleeping** - The HDD is working normally.
 - **Uninitialized** or **Abnormal** - Initialize the HDD before continuing. Check the select box of the HDD to initialize, then click the **Init** button at the bottom of the screen.
 - **Failed**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

12.2 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. Currently, 8TB is the maximum drive size supported for each 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.

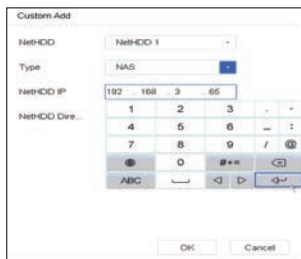


3. In the **NetHDD** drop down list, select the NetHDD ID (NetHDD 1 .. NetHDD 8) you want to add.
4. In the **Type** drop down list select either **NAS** or **IP SAN**.
5. Configure the device type you selected.

12.2.1 For a NAS disk

Currently, 8TB is the maximum drive size supported for NAS disks.

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



- 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.

Custom Add

NetHDD: NetHDD 1

Type: NAS

NetHDD IP: 192.168.3.85

NetHDD Dire...: msdsk-hvmsdsk Search

No.	Directory
1	msdsk-hvmsdsk

OK Cancel

- iv. In the Directory list, select the directory you want to use, and then click **OK** to add the disk to your system. The NAS will appear in the HDD Information menu.

Maintenance

Clone Source

Label	Capacity	Status	Property	Type	Free Space	Group
1	931.57GB	Normal	RW	Local	977.00GB	1
2	1863.02GB	Normal	RW	Local	1867.00GB	1
.17	1863.02GB	Normal	RW	NAS	1867.00GB	1

12.2.2 For an IP SAN disk:

Configuring an IP SAN NetHDD is similar to configuring a NAS. See “12.2.1 For a NAS disk” on page 180 for more information.

1. In the **Add NetHDD** window, click the **Type** field, then select **IP SAN**.
2. Enter the NetHDD IP address in the text field.

Custom Add

NetHDD: NetHDD 2

Type: IP SAN

NetHDD IP: 192.168.3.104

NetHDD Dire... Search

OK Cancel

3. Click **Search** to discover the available IP SAN disk directories on the network.
4. Select the IP SAN disk directory from the list shown below.

- a. Select the directory you want to use, and then click **OK** to add the disk to your system.

NOTE

*If the added NetHDD is uninitialized, select it and click the **Init** button for initialization. Initializing an storage device erases all data saved on the disk.*

5. 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 "16.2 Checking HDD status" on page 214 for more information.

12.3 Configuring the HDD Partition / Group mode

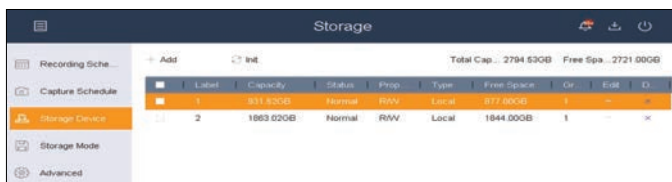
By default, all cameras will record to the one partition(s) of the internal HDD(s). However, the NVR can be configured to allocate space in one of two modes:

- **Partition** mode: Each camera can be allocated it's own recording space on a storage device (HDD).
- **Group** mode: Groups of cameras can each be allocated recording space on a storage device or devices. 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.

12.3.1 Partition Mode recording

In Partition Mode recording, each camera can be allocated it's own recording space on a storage device (HDD).

1. Go to **Menu | Storage | Storage Device**.



2. Click **Storage Mode** in the left frame to check the storage mode of the HDD. If you prefer to use **Partition** mode, do the following:



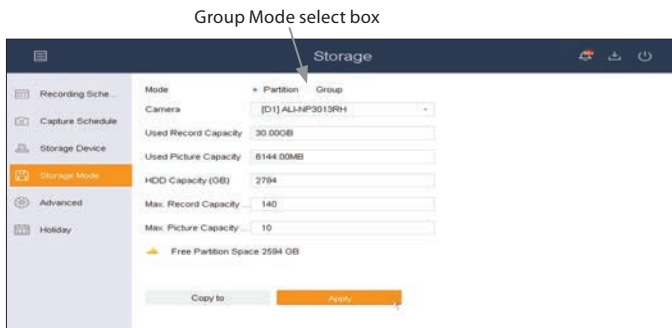
- Open the Camera drop down list and select the camera for which you want to allocate storage space.
- Edit the **Max. Record Capacity** and the **Max. Picture Capacity** values to specify the space allocated to each. In the above screen, the **Max. Record Capacity** was set to 140GB.
- Click **Apply** to save the settings.
- Repeat sub-steps a through c above for other cameras monitored by the recorder.

12.3.2 Group Mode recording

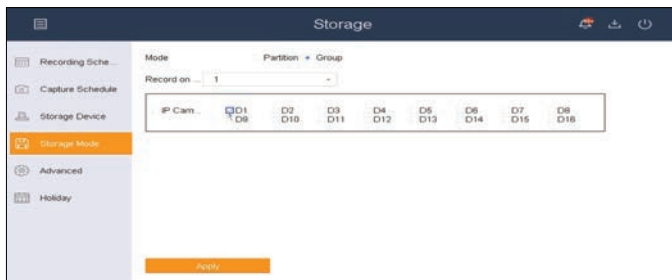
In Group Mode recording, groups of cameras can each be allocated recording space on a storage device or devices. Configuring the HDD(s) for Group recording mode requires an NVR reboot. You must have at least two HDDs (including internal and NAS / IP San HDDS added to the system) to configure 2 Groups, etc. Additional HDDs can be assigned to other groups or used as redundancy for existing groups. Additionally, an HDD use to record data can be reconfigured to read-only.

In the following example, the HDDs will be configured for Group Mode, with camera channel D1 assigned to Group 1 on HDD 1, and camera channel D2 assigned to Group 2 on HDD 2. To change to **Group** mode from Partition Mode (default), do the following:

- In the **Menu | Storage | Storage Device** menu (see above), check the select box for the HDD you want to configure.
- Click the **Storage Mode** Link in the left frame.

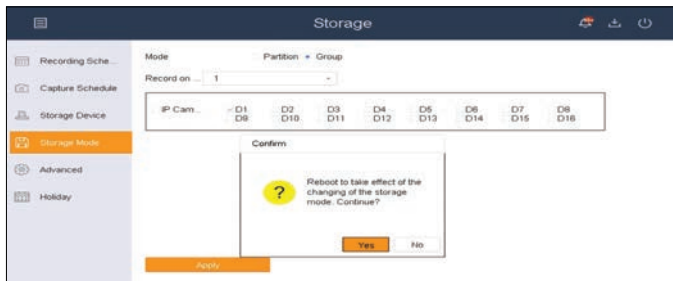


- In the **Mode** select field, select **Group**.



SECTION 12: MANAGING HDDS

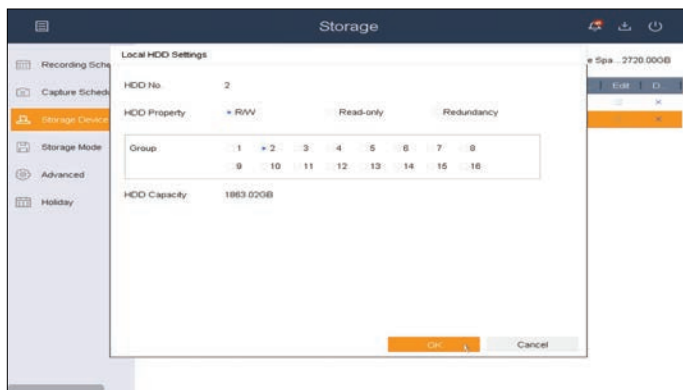
- Check the box(es) for the camera(s) you want to add to the group. IP Cannel D1 was selected.
- Click **Apply**. Since you are changing from Partition to Group, a reboot the system is required. In the Confirm box, click **Yes**, and then allow the system to fully reboot before continuing.



- After the reboot is complete, go to **Menu | Storage | Storage Device** menu. Notice that in this window, an icon now appears for each HDD in the **Edit** column.



- To setup Group 2, click the **Edit** icon for HDD 2. the select box for **HDD2**.



- In the **Group** section, click the select box for Group 2, and then click **OK**. In the Storage Device window, HDD 2 is now Group 2.



- Open the **Storage Mode** menu.



- Open the **Record on** drop down list, and select 2 (for Group 2, see above).
- Check the select boxes for the cameras you only want to assign to Group 2, and then click **Apply**.

Additional HDDs

For each additional HDD on your system, click its **Edit** icon in the **Storage Device** screen. You can:

- Create a new group for cameras not assigned to existing groups (see procedure above)
- Assign the HDD as a:
 - Read / write (R/W) drive for an existing group
 - Redundancy drive for an existing group
 - Read-only drive

12.3.3 Change from Group Mode recording to Partition Mode

To change from Group Mode recording to Partition Mode recording:

- Open the **Storage Mode** menu.

SECTION 12: MANAGING HDDs



2. Click the **Partition** Mode select box.
3. Click **Apply**, and follow the prompt to reboot your system.

SECTION 13

RAID Arrays (RAID capable recorders only)

13.1 Creating a RAID array

RAID (redundant array of independent disks) is a storage technology that combines multiple disk drive components into a single 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. RAID is featured on some multi-HDD recorders.

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.

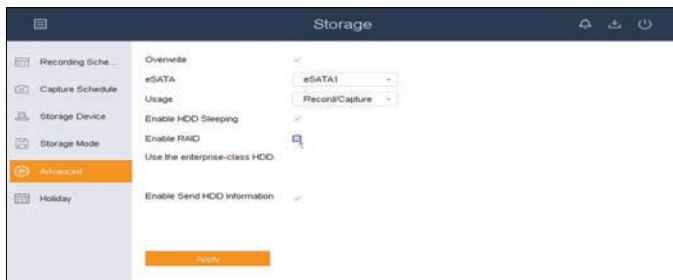
When or after creating the RAID array, you can designate an additional HDD to be a **Hot Spare** drive. If an HDD in the array fails (array Degraded), the Hot Spare is used to automatically rebuild the array with the Hot Spare HDD replacing the failed drive in the array, and with data that was on the failed HDD written to Hot Spare the from the functional drives in the array. The size of the Hot Spare drive must be equal to or larger than the largest capacity drive in the 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 | Storage | RAID | Physical Disk** display. Verify that the drives you want to configure for RAID have "**Functional**" Status.



2. Click the Advanced tab, check the box to **Enable RAID**, and then click **Apply**.

SECTION 13: RAID ARRAYS



3. In the **Confirm** pop-up window, click **YES** to reboot the system.



4. After the NVR reboots, open the **Menu | Storage | RAID | Physical Disk** display again.

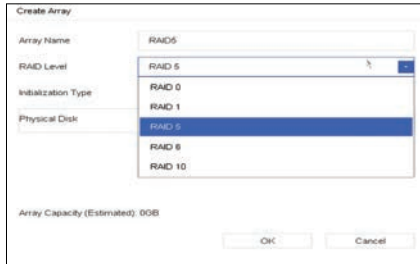


5. Click the **Create** button.



NOTE If you click **One-touch Config**, a RAID 5 array will be created.

6. In the pop-up window:
 - a. Enter an **Array Name**. In the example here, RAID array is named **RAID5**.
 - b. Open the RAID Level drop-down list, and then click the kind of RAID you want to create.



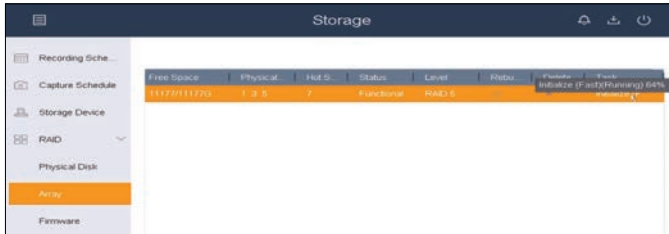
- c. Open the **Initialization Type** field and select one of the following:
 - * **Background**: The background initialization can synchronize the disks, and detect and repair bad sectors. During the background initialization, the virtual disk is allowed to be used.
 - * **Foreground** (recommended): 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. In this example, drives 1, 3 and 5 were selected. Drive 7 will be designated later as the Hot Spare.
- e. Click **OK** to construct the RAID array. This process can take hours, depending on the size of the HDDs.
- f. To designate an unused HDD as a hot spare, find the HDD you want, then click the select box for it in the Hot Spare column. **NOTE** An additional HDD can be installed after the array is built, and then designated as the Hot Spare.

Click to Select No. 7 as Hot Spare



SECTION 13: RAID ARRAYS

- g. Open the **Menu | Storage | RAID | Array** display to view the **Task** field (far right column). Hover the cursor over the task field for the array to see the progress of the array creation. Allow the RAID initialization to complete before continuing. See below.



When the array creation is finished, the Task field shows **None**.



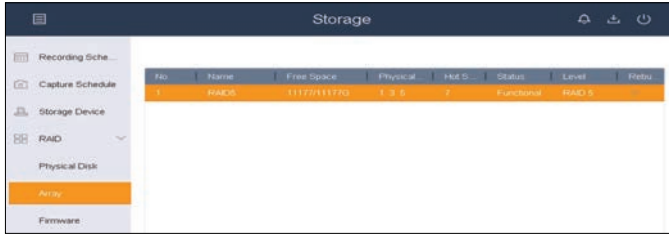
Task status when RAID initialization is complete

13.2 Rebuilding a RAID array

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 | Status | Raid | Array** display.



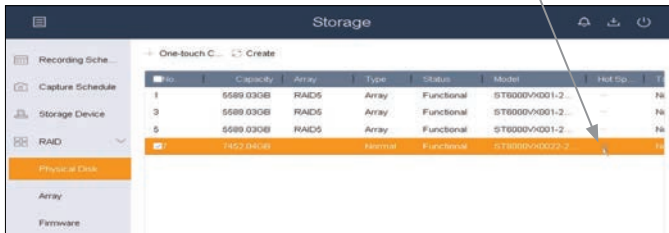
Arrays are automatically rebuilt when the array status is Degraded and a Hot Spare HDD is installed in the system.

13.2.1 Installing a Hot Spare disk

To install a hot spare:

1. Select a disk with the same or larger capacity as the largest HDD in the RAID configuration. Install the HDD in the recorder (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 | Storage | RAID | Physical Disks** display.

Click to Select No. 7 as Hot Spare



NOTE

After installing a spare HDD in the chassis, it may need to be initialized before it can be used. Check the status of the disk in the display above to ensure it is functional.

3. For the HDD you installed, check the select box in the **Hot Spare** column. Click the select box in the Hot Spare column for the spare disk that was installed. The **Array** field will show the HDD as **Global**, and the **Type** field will show it as **Hot Spare**.

SECTION 13: RAID ARRAYS



The screenshot shows the 'Storage' management interface. On the left, there is a sidebar with options: Recording Siche..., Capture Schedule, Storage Device, RAID, Physical Disk (selected), Array, and Firmware. The main area displays a table with columns: #, Capacity, Array, Type, Status, Model, and Hot Sp. The table contains the following data:

#	Capacity	Array	Type	Status	Model	Hot Sp.
1	5688.03GB	RAID5	Array	Functional	ST1000V0001-2	—
3	5688.03GB	RAID5	Array	Functional	ST1000V0001-2	N
5	5688.03GB	RAID5	Array	Functional	ST1000V0001-2	N
7	7452.04GB	Global	Hot Sp.	Functional	ST1000V0002-2	×

Physical disk configuration after a spare HDD is installed

- To remove a Hot Spare HDD, click the “×” icon in the Hot Spare column for it.

13.2.2 Array Rebuilding process

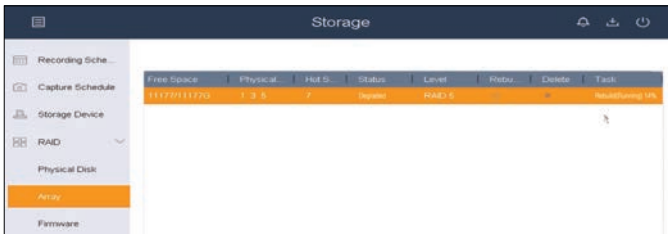
When the chassis is configured with a Hot Spare disk and the array is in **Degraded** status, the system will automatically rebuild the array using the Hot Spare disk. To prepare for automatic rebuilding of the array, the system was configured as shown below, with a Global Hot Spare disk installed in physical slot 7.



The screenshot shows the 'Storage' management interface. On the left, there is a sidebar with options: Recording Siche..., Capture Schedule, Storage Device, RAID, Physical Disk (selected), Array, and Firmware. The main area displays a table with columns: #, Capacity, Array, Type, Status, Model, and Hot Sp. The table contains the following data:

#	Capacity	Array	Type	Status	Model	Hot Sp.
1	5688.03GB	RAID5	Array	Functional	ST1000V0001-2	—
3	5688.03GB	RAID5	Array	Functional	ST1000V0001-2	N
5	5688.03GB	RAID5	Array	Functional	ST1000V0001-2	N
7	7452.04GB	Global	Hot Sp.	Functional	ST1000V0002-2	×

When an array is being rebuilt, open the in the **MENU | Storage | Raid | Array** display. The **Status** field shows **Degraded**, and the **Task** field shows **Rebuild**.



The screenshot shows the 'Storage' management interface. On the left, there is a sidebar with options: Recording Siche..., Capture Schedule, Storage Device, RAID, Physical Disk (selected), Array, and Firmware. The main area displays a table with columns: Free Space, Physical, Hot S., Status, Level, Rebu., Delete, and Task. The table contains the following data:

Free Space	Physical	Hot S.	Status	Level	Rebu.	Delete	Task
11177111703	1 3 5	7	Degraded	RAID 5	—	—	RebuildUsing Hk



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 14

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) (after installing the WebComponents plugin), Mozilla Firefox or Google Chrome browsers. 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. Some user permissions disallow remote access and / or features of this access method.

You can view up to 4 camera video streams at one time.

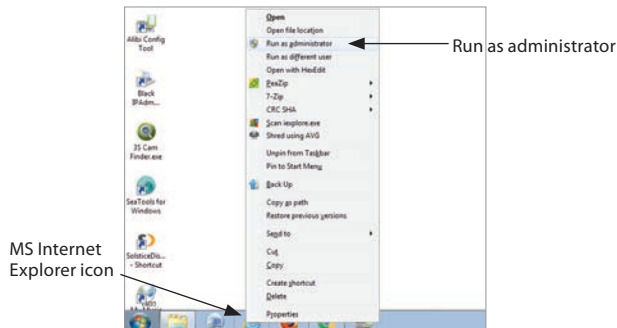
14.1 Using IE to login to the NVR

14.1.1 Configure IE to run in Administrator mode

IE must be run in administrator mode to access the NVR. 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.



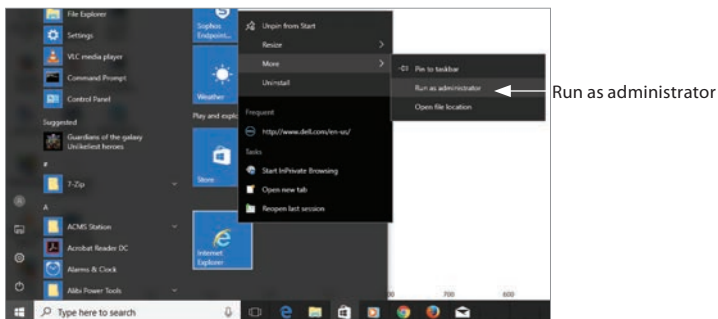
3. Click **Run as administrator** in the pop-up menu.

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**.

SECTION 14: REMOTE ACCESS

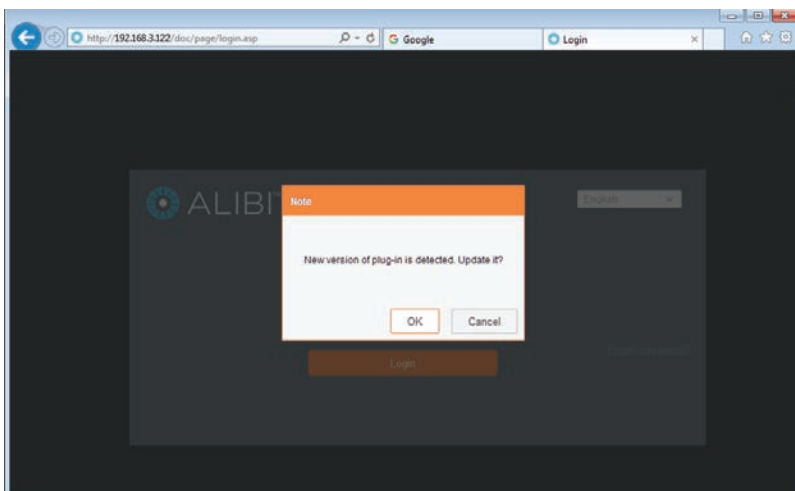
3. Right click on the Internet Explorer tile, and then select **More | Run as administrator**.



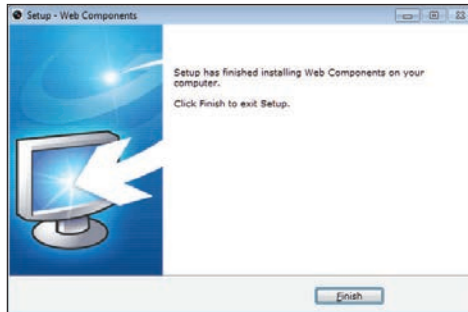
14.1.2 Login with IE

To access the NVR from a computer on the LAN:

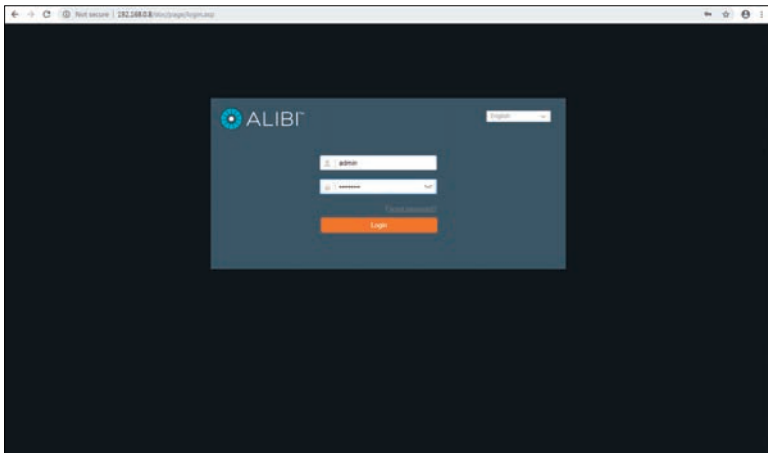
1. Open the IE browser on your remote compute and enter the IP address of the NVR in the URL field. In the example below, the IP address of the NVR is 192.168.2.122. If this is the first time you log into an Alibi recorder with this version of firmware, the following screen will appear, requiring you to install a plugin. If not, go to step 3 below.



2. 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 **IE** 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 (see above). A **Live View** window will open.

14.2 Using Firefox or Chrome to login to the NVR

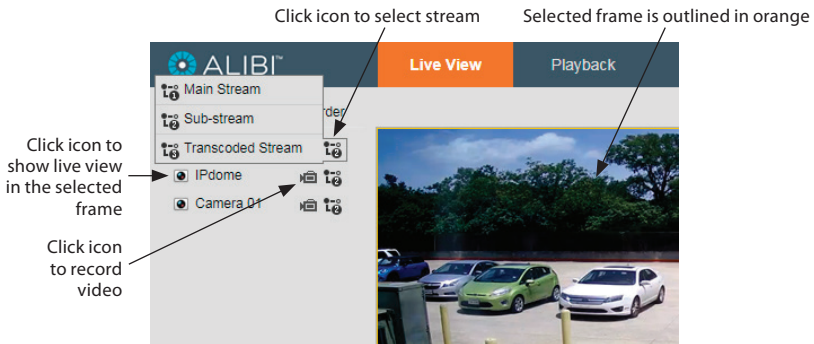
To login to the NVR with either Mozilla Firefox or Google Chrome, open the browser and enter the IP address of the NVR in the URL field. When the Login screen opens, enter your **username** and **password** in the fields shown, and then click **Login**.

14.3 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.

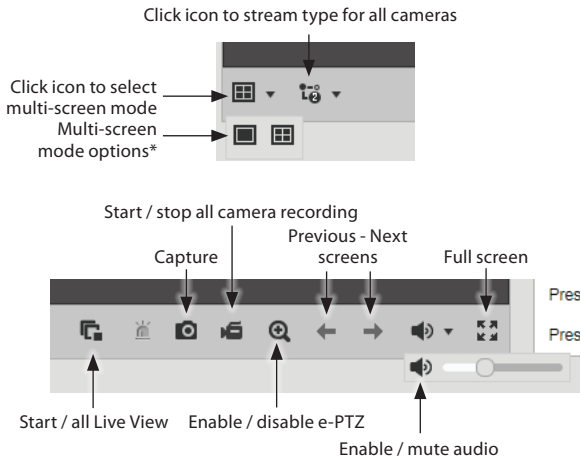


Screen icons



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.



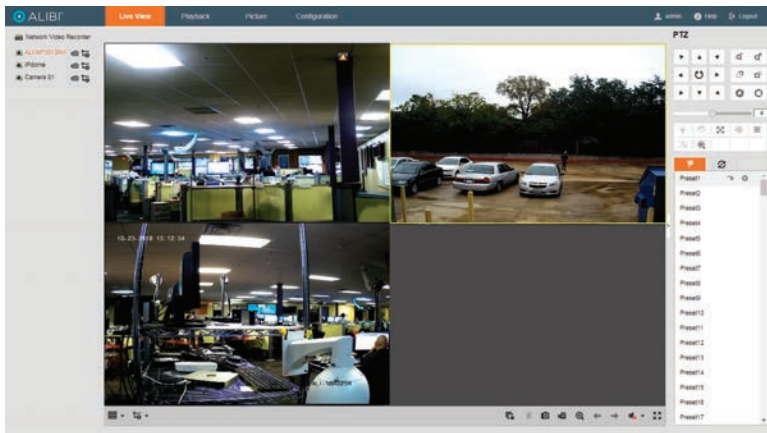
* You can view up to 4 cameras (video streams) at any time.

Additional icons can appear on the toolbar depending on the capabilities of the camera.

For **PTZ controls**, refer to “5.1 PTZ Control Panel” on page 72.

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 the view icon in the left frame for the camera 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

The Help button at the top of the window opens a context sensitive help screen. The screen shown below appears when selecting Help from the Playback menu.

Online Help

Introduction

- Accessing Via Web Browser
- Installing the plug-in

Live View

- **View Page Introduction**
- PTZ

Playback

- Playback

















Parameters Configuration

- Local Configuration
- System
- Network
- Video/Audio
- Image
- Event
- Storage
- VCA Configuration

The live view page allows you to view the real-time video, capture images, realize PTZ control, set/real presets and configure video parameters.

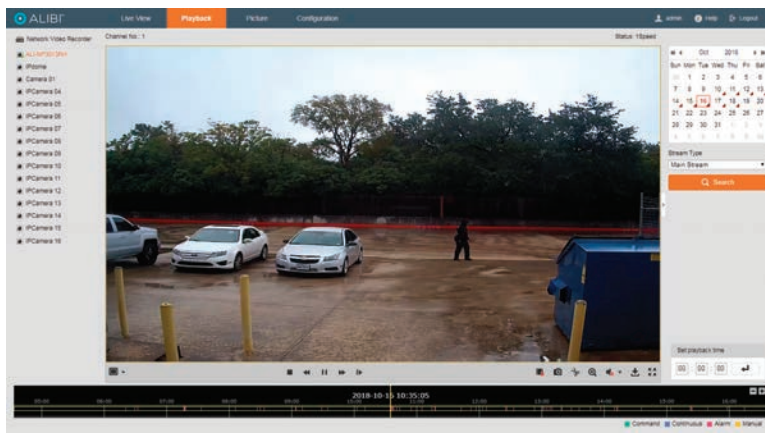
Descriptions of the icons on the Live View Page

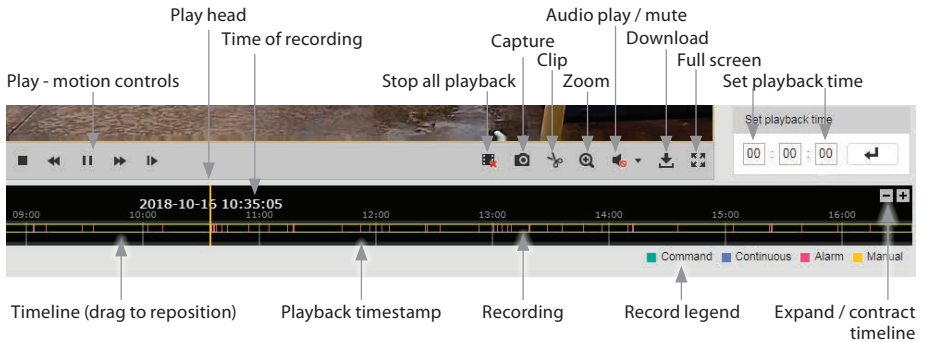
The functions of the buttons on the toolbar are shown in the following table.

Button	Description	Button	Description
	Start All Live View.		Stop All Live View.
	Live view with the main stream.		Live view with the sub stream.
	Live view with the transcoded stream.		Manually capture the picture.
	Manually start all recording.		Manually stop all recording.
	Audio on and adjust the volume.		Mute.
	Start Two-way Audio		Stop Two-way Audio
	Channel 1/Channel 2/Channel 3.		Channel 1/Channel 2/Channel 3.
	Enable Digital Zoom.		Disable Digital Zoom.

14.4 Playback tab

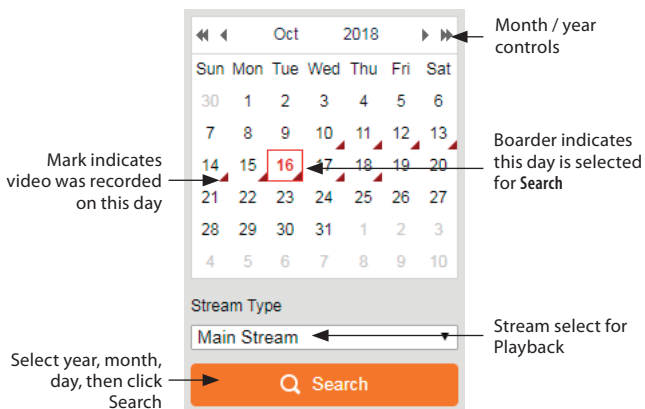
Open the Playback screen by clicking the **Playback** tab in the screen header. The Playback screen allows you to review video recorded from one camera or several cameras concurrently. Also, video files can be downloaded to your local computer.





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 or 2 x 2 frame pattern.
2. If you selected a 2 x 2 frame pattern, click on a video frame, and then click the camera channel you want to play recorded video from. Repeat this method for other video frames in the playback window. In the example above, the *ALI-NP3013RH* camera was selected for a 1 channel playback.
3. In the right frame, click the date when the video you want to see was recorded. Marks on the calendar show when video was recorded (see below).



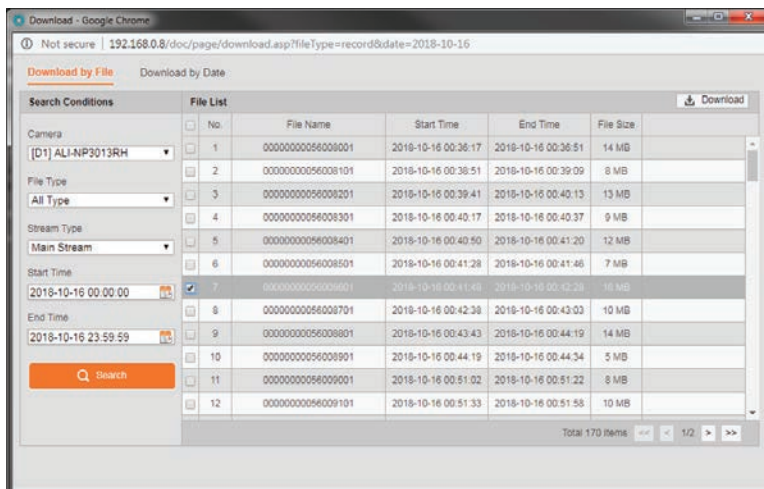
4. Click the **Stream Type** drop down list and select the video stream you want to see, and then click the **Search** button. In the example above, October 16, 2018 and Main Stream was selected.

SECTION 14: REMOTE ACCESS

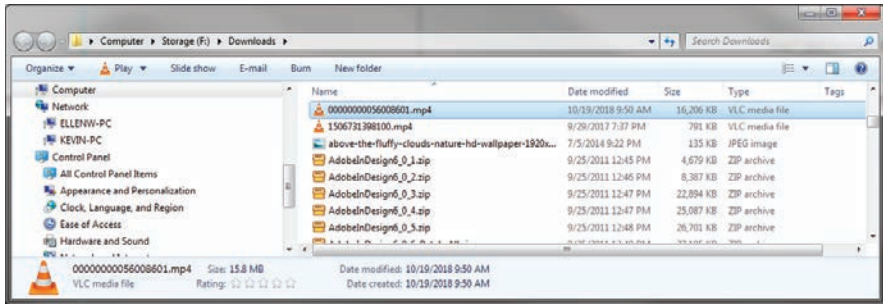
- At the bottom of the screen, drag the timeline left or right to align the time with the play head. The condition that caused video to be recorded is indicated by a colored band on the timeline. The color legend is shown at the lower right corner of the window.
- Click the **Play** button to begin playing video.

To Download recorded video:

- During playback, find the video clip you want to download. Note the date and time of the clip shown above the timeline.
- Click the **Download** icon.

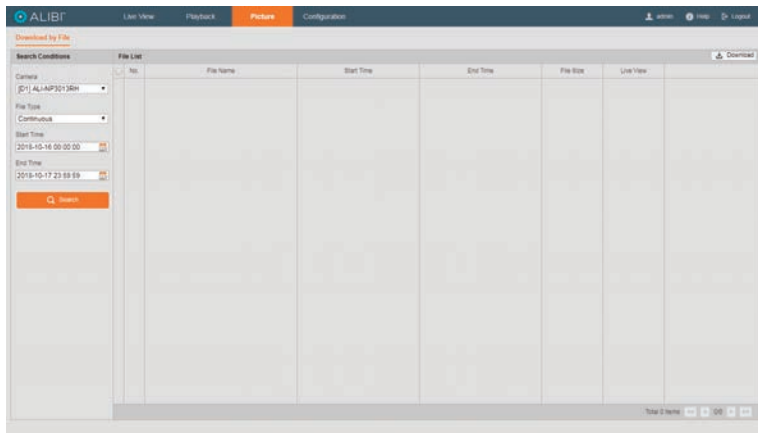


- By default, the parameters in the search column are set to the search parameters you selected in the Playback screen. Reset the search criteria for the **Camera**, **File Type**, **Stream Type**, **Start Time** and **End Time** as needed to display files from another camera or other days and times, and then click **Search**.
- In the search result list, check the box of the video segment(s) you want to download. You can use the **Start Time** and **End Time** fields to determine the specific file(s) you want to save.
- 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 specified by your browser. Allow the download to complete before closing the browser.



14.5 Picture tab

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.



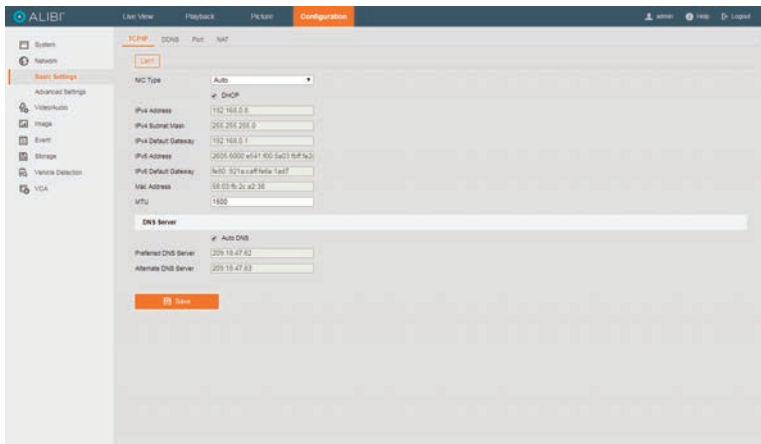
1. By default, the parameters in the search column are set to Channel D1 and the current day. Reset the search criteria for the **Camera**, **File Type** (condition causing the capture), **Start Time** and **End Time** of the search as needed to display files from another camera, conditions or other days and times, and then click **Search**.
2. In the search result list, check the box of the file(s) you want to download. You can use the **Start Time** and **End Time** fields to determine the specific file(s) you want.
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 specified by your browser. Allow the download to complete before closing the browser.

14.6 Configuration tab

Open the Configuration screen by clicking the **Configuration** tab in the screen header. Configuration menus enable you to view the NVR configuration and make changes. The ability to make changes through these menus is determined by the permissions associated with your login credentials.

NVR options in the configuration menu are like 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. Menus associated with a specific camera model are described in the user manual for the camera firmware. After making configuration changes, click **Save** to apply your changes.

The initial configuration menu that appears is the last menu opened during a remote login, or the **System | System Settings | Basic Information** menu.

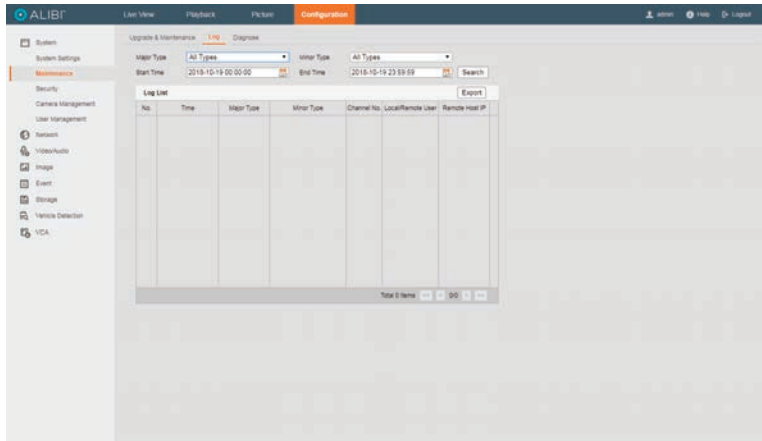


NOTE

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.

14.6.1 Log information

You can video system log information remotely. Open the Log screen by clicking **Configuration | System | Maintenance | Log**.

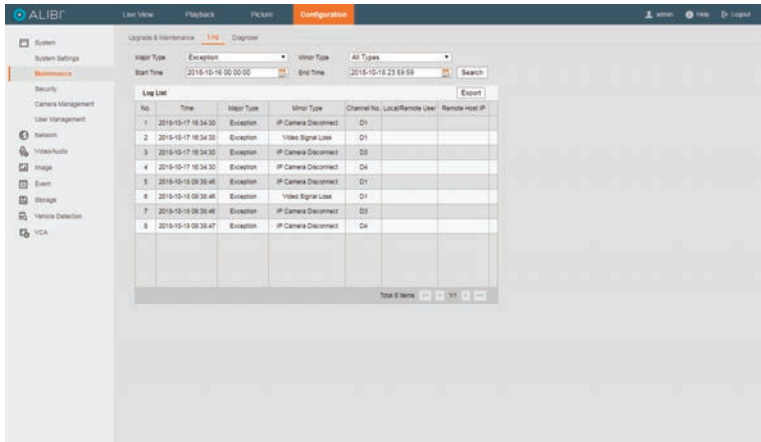


The NVR log report is created by specifying a search criteria using the options at the top of the window, and then clicking the **Search** button. The search criteria menu includes filters to search for Major and Minor type events, and specify the start and end time of the report. Log reports can be saved in either text or Excel formats by clicking the **Save Log** icon:

To search for log information:

1. Open the **Major Type** drop down list, and then select alarm group of the alarms you want to search for.
1. Open the **Minor Type** drop down list, and then select the specific alarm you want to search for.
2. Click the **Start Time** calendar icon, then select the beginning of the time period when you want to begin the log search.
3. Click the **End Time** calendar icon, then select the end of the time period when you want to begin the log search.
4. Click the **Search** button. A list of alarms matching your search criteria will appear. Note that the search result will display at most 4000 log entries, distributed across 40 pages (100 entries / page).

SECTION 14: REMOTE ACCESS



5. Click **Export** to save the search data in a text file (*Log.txt*). The file is downloaded to the download directory of your browser.



14.7 Logout

Click the **Logout** button in the screen header to close the remote connection to the NVE.

APPENDIX A Glossary

Device: Represents the Network Video Recorder. A device can be a PC-based or embedded system used for centralized management and storage for IP cameras, IP Domes and other devices.

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.

NTSC: Acronym for National Television System Committee. NTSC is an analog television standard used in such countries as the United States and Japan. Each frame of an NTSC signal contains 525 scan lines at 60Hz.

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.

PAL: Acronym for Phase Alternating Line. PAL is a video standard, similar to NTSC, that is used in broadcast television systems in large parts of the world. PAL signal contains 625 scan lines at 50Hz.

PPPoE: Stands for "Point-to-Point Protocol over Ethernet." PPPoE is a network configuration used for establishing a PPP connection over an Ethernet protocol.

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.

APPENDIX B Long Distance (Extended) PoE Power

The NVR Extended PoE (Long Distance) feature supports camera connections to the internal Ethernet switch using cable lengths greater than 100 meters (328 ft). These feature requires:

- Ethernet cables can be Cat5E or Cat6 with solid copper conductors. CCA (Copper Clad Aluminum) conductors are not supported.
- The camera power consumption must be ≤ 8 W
- The maximum bit rate (main stream and sub-stream) must be ≤ 8 Mbps
- The camera and NVR combinations shown in the following table are supported for the maximum cable lengths indicated.

replace table

Camera	NVR		
	ALI-NVR3304P	ALI-NVR3308P	ALI-NVR5216P / ALI-NVR5232P
ALI-NS2012VR	Maximum length: 200 m (656 ft)	Maximum length: 250 m (820 ft)	Maximum length: 250 m (820 ft)
ALI-NS2013VR			
ALI-NS2015VR(B)			
ALI-NS2018VR			
ALI-NS2022VR			
ALI-NS2023VR			
ALI-NS2025VR(B)			
ALI-NS2028VR			
ALI-NS4012R			
ALI-NS4013R			
ALI-NS4015R			
ALI-NS4018R			
ALI-NS4022R			

APPENDIX C Troubleshooting

Problem: No image displayed on the monitor after normal startup

Possible Reasons

- No VGA or HDMI connections
- Connecting cable is damaged
- Input mode of the monitor is incorrect

Troubleshooting steps

1. Verify the device is connected to a monitor through an HDMI or VGA cable. If not, connect the device with the monitor and reboot the recorder.
2. Ensure that the connecting cable is good. Change the cable and reboot the recorder.
3. Check the input mode of the monitor. It must match with the output mode of the recorder (e.g. if the output mode of recorder is HDMI output, then the input mode of monitor must be the HDMI input). If not, modify the input mode of monitor.

If the steps above do not resolve the problem, please contact your system support organization.

Problem: There is an audible warning sound “Di-Di-DiDi” after a new recorder starts up

Possible Reasons

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

Troubleshooting steps

1. Verify that at least one HDD is installed in the recorder. If not, please install the compatible HDD. Refer to the Quick Start Guide for the HDD installation steps.
2. Verify the HDD is initialized. Go to **Menu | Storage | Storage Device**. If the status of the HDD is “Uninitialized”, check the select box for the HDD, and then click **Init**.
3. Verify the HDD is detected or is in good condition. Go to **Menu | Storage | Storage Device**. If the HDD is not detected or the status is **Abnormal**, replace the dedicated HDD according to the requirement.

If the steps above do not resolve the problem, please contact your system support organization.

Problem: The status of an IP camera added to the system is *Disconnected* when it is connected through Private Protocol. Check the camera status at: **Menu | Camera | Camera | IP Camera.**

Possible Reasons

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

Troubleshooting steps

1. Verify the network is connected. To verify the network connection:
 - a. Connect the device and PC with the RS-232 cable.
 - b. Open the Super Terminal software, and execute the ping command. Input "ping IP" (e.g. *ping 172.6.22.131*). Simultaneously press **Ctrl + c** to stop the ping command.
If return information appears and the TTL number small (less than 20ms), the network is normal. If there is no Reply, make sure a network cable is connected, and cables are connected to your router.
2. Verify the configuration parameters are correct.
 - a. Go to **Menu | Camera.**
 - b. Verify the network parameters are the compatible with those of other devices on the network, including: IP address, protocol, management port, user name and password.
3. Verify the whether the bandwidth is enough.
 - a. Go to **Menu | Maintenance | Net Detect | Network Stat.**
 - b. Check the access bandwidth usage. Verify that it has not reached the limit.

If the steps above do not resolve the problem, please contact your system support organization.

Problem: The IP camera frequently goes offline and the status of it displays as *Disconnected*

Possible Reasons

- The IP camera and the device versions are not compatible.
- Unstable power supply of IP camera.
- Unstable network between IP camera and device.
- Limited flow by the switch connected with IP camera and device. Step 1 Verify the IP camera and the device versions are compatible.

Troubleshooting steps

1. Go to **Menu | Camera**, and view the firmware version of connected IP camera.
2. Go to **Menu | Maintenance | System Info | Device Info** and view the firmware version of recorder. Verify that the firmware version of the camera is compatible with the recorder.
3. Verify power supply of IP camera is stable:
 - a. Verify the power indicator is normal.
 - b. When the IP camera is offline, execute a ping command from the PC to verify it can reach the IP camera.
4. Verify the network between IP camera and recorder is stable.
 - a. When the IP camera is offline, connect PC and device with the RS-232 cable.
 - b. Open the Super Terminal, use the ping command and keep sending large data packages to the connected IP camera, and check if there exists packet loss.

NOTE Simultaneously press **Ctrl + c** to exit the ping command

Example: Input ping 172.6.22.131 -l 1472 -f.

1. Verify the switch is not flow control.

Check the brand, model of the switch connecting IP camera and device, and contact with the manufacturer of the switch to check if it has the function of flow control. If so, please turn it down.

If the steps above do not resolve the problem, please contact your system support organization.

Problem: Live view stuck when video output locally.

Possible Reasons

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

Troubleshooting steps

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

NOTE Simultaneously press **Ctrl + C** to exit the ping command

2. Verify the frame rate is real-time frame rate. Go to **Menu | Camera | Encoding Parameters**. Set the **Frame rate** to Full Frame.

If the steps above do not resolve the problem, please contact your system support organization.

Problem: No record file found in the device local HDD, with the message "No record file found".

Possible Reasons

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

Troubleshooting steps

1. Verify the system time setting is correct. Go to **Menu | System | General**, and verify the "Device Time" is correct.
2. Verify the search condition is correct. Go to playback interface, and verify the channel and time are correct.
3. Verify the HDD status is normal. Go to **Menu | Storage | Storage Device** to view the HDD status, and verify the HDD is detected and can be read and written normally.

If the steps above do not resolve the problem, please contact your system support organization.

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

Possible Reasons

- Poor network between device and IP camera, and there exists packet loss during the transmission.
- Poor network between device and PC, and there exists packet loss during the transmission.
- The performances of hardware are not good enough, including CPU, memory, etc.. Step 4 Verify the network between device and IP camera is connected.

Troubleshooting steps

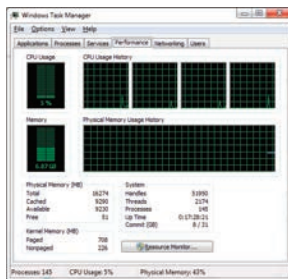
1. When image is stuck, connect the RS-232 ports on PC and the rear panel of device with the RS-232 cable.
2. Open the Super Terminal, and execute the command of "ping 192.168.0.0 -l 1472 -f" (the IP address may change according to the real condition), and check if there exists packet loss.

NOTE Simultaneously press **Ctrl + C** to exit the ping command

3. Verify the network between device and PC is connected.
 - a. Use the keyboard shortcut *windows+r* to open the Command (**cmd**) window.
 - b. Use the ping command to send large packet to the device, execute the command of "ping 192.168.0.0 -l 1472 -f" (the IP address may change according to the real condition), and check if there exists packet loss.

NOTE Simultaneously press **Ctrl + C** to exit the ping command

4. Verify the hardware of the PC is good enough. Simultaneously press **Ctrl+Alt +Delete** to enter the windows task management interface, and then click the Performance tab (see below).



If the resource is insufficient, stop unnecessary processes.

If the steps above do not resolve the problem, please contact your system support organization.

Problem: When using the device to get the live view audio, there is no sound, there is too much noise, or the volume is too low.

Possible Reasons

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

Troubleshooting steps

1. Check the cable between the microphone and the IP camera. Make certain the cable is connected properly, the impedance matches, and the equipment is compatible.

Log in the IP camera directly, and turn the audio on, check if the sound is normal. If not, please contact the manufacturer of the IP camera.
2. Verify the setting parameters are correct. Go to **Menu | Camera | Encoding Parameters**, and set the **Stream Type** to **Audio & Video**.
3. Verify the audio encoding standard of the IP camera is supported by the device.

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

If the steps above do not resolve the problem, please contact your system support organization.

Problem: The image gets stuck when device is playing back by single or multi-channel.

Possible Reasons

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

Troubleshooting steps

1. Verify the network between device and IP camera is connected.
 - a. When image is stuck, connect the RS-232 ports on PC and the rear panel of device with the RS-232 cable.
 - b. Use the keyboard shortcut *windows+r* to open the Command (**cmd**) window.
 - c. Open the Super Terminal, and execute the command of "*ping 192.168.0.0 -l 1472 -f*" (the IP address may change according to the real condition), and check if there exists packet loss.

NOTE Simultaneously press **Ctrl + C** to exit the ping command

2. Verify the frame rate is real-time frame rate. Select **Menu | Record | Parameters | Record**, and set the **Frame Rate** to **Full Frame**.
3. Verify the hardware can afford the playback. Reduce the channel number of playback. Go to **Menu | Camera | Encoding Parameters**, and set the resolution and bitrate to a lower levels.
4. Reduce the number of local playback channel. Go to **Menu | Playback**, and uncheck the select box of unnecessary channels.

If the steps above do not resolve the problem, please contact your system support organization.
