OPERATION MANUAL

Portable Solar Light Tower

SPLT-.53K-LM45 Series

TABLE OF CONTENTS

DEPLOYING THE UNIT.....**Page 2**

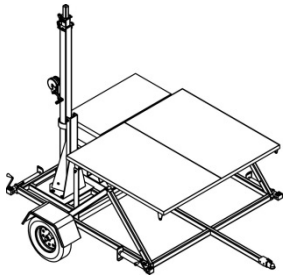
ROTATING THE MAST.....**Page 3**

REMOVING THE HITCH.....**Page 3**

PREPARING FOR TRANSPORT.....**Page 4**

SPLT-.53K-LM45 SERIES OPERATION MANUAL

DEPLOYING THE UNIT



1. Choose a location that is close to level as possible to position the trailer. Drop the trailer from the tow vehicle using the single jack located on the front of the trailer. Ensure that the safety chains and cable have been disconnected from the tow vehicle.



2. Once the trailer has been disconnected from the hitch of the tow vehicle, extend the remaining jacks. There are (2) leveling jacks located on the back and (2) jacks located on the front of the trailer. Pull the pin on the side of the jack to rotate it 90° toward the ground and hand crank the jack clockwise to extend it. Use a bubble level to ensure the trailer is level.



3. Unlatch the solar panel and reposition it 45°. There is a hand screw located on each side of the solar panel. With help, remove each hand screw to free the panels and pivot the solar panels down against the frame at a 45° angle. Insert each hand screw to secure the panels.



4. Locate the hand winch on the mast. Turn the handle clockwise to raise the mast until it stops. Watch for snags during this process if there are any cords attached. The mast is now deployed. To rotate the mast, view **ROTATING THE MAST** on **page 3** of this manual.



5. Open the job box located next to the mast. Locate the keys to both padlocks if it is locked. The job box will open once unlocked and there is no need to remove the padlocks.



6. Move the power switch to its **ON** position to power the internals. Make sure all breakers and switches are moved to the **ON** position at this time. This will enable power to your attached devices and allow the solar panels to begin charging the batteries. A built in cooling system will circulate air when the job box exceeds 90° F (32° C) to help keep the internals cool.

The trailer is now deployed.

ROTATING THE MAST

The mast can be rotated while fully lowered or elevated.



1. Loosen the two bolts located toward the center of the mast on the collar.



2. Once loose, rotate the mast to your desired position

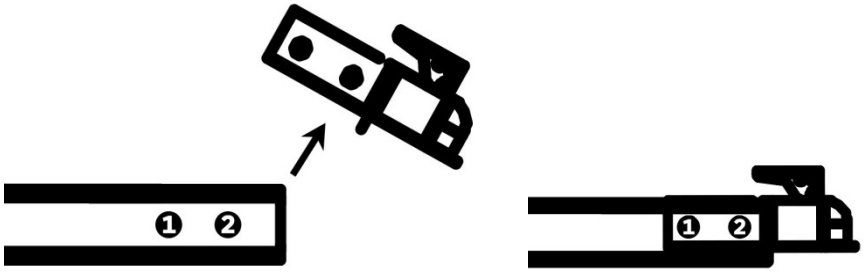


3. Tighten the two bolts in order to hold the mast in place

Note: Pay attention to any attached cords while rotating the unit to prevent tangles or strain around the light mast.

REMOVING THE HITCH

The trailer hitch can be removed preventing the trailer from unauthorized towing. Remove the two bolts ❶ & ❷ from the graphic below holding it in place and lift the hitch off. This can be stored inside the job box when not in use. To install the hitch, place it back on the trailer tongue and replace the two bolts. Be sure both safety chains are attached.



PREPARING FOR TRANSPORT

1. Lower the mast by rotating the hand winch counter-clockwise until the light mast is no longer supported by the winch cable.



2. If previously rotated, return the mast to its original position.



3. Power off all equipment. Open the job box and position the main power switch **OFF**.



4. Lock the job box and take the keys to prevent unauthorized access.



5. Position the solar panels horizontal and secure them with the two hand screws.



6. Lift the (4) jacks on each corner of the trailer by rotating the hand crank counter-clockwise. Pull the pin and rotate each jack 90°.



7. When the mast is fully lowered, powered off, and the (4) main jacks are raised, you are ready to attach a tow vehicle. Once tied to a tow vehicle, raise the tow jack and ensure all other outriggers are raised. Ensure the trailer hookup and safety chains are connected. Test trailer lights to ensure stop/tail/brake lights work before operating on public roadways.

If you have any questions about your trailer please call the manufacturer.

IDCMR-IP-POE-PTZ-20X PTZ Dome Camera Installation Guide



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

CAUTION

FCC Caution: *To assure continued compliance, use only shielded interface cables when connecting to computer or peripheral devices. Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.*

NOTE

This equipment has been tested and found to comply with the limits for a Class "A" digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

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.

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.

Microsoft, **Windows**, and **Internet Explorer** are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

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, Inc.

Regulatory information

FCC information

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

FCC conditions

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

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

Preventive and Cautionary Tips

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

- Ensure environmental conditions meet factory specifications.
- Major shocks or jolts to the unit as a result of dropping it may cause damage to the sensitive electronics within the unit.
- Use the device in conjunction with an UPS if possible.

Safety Instructions

These instructions are intended to ensure that user can use the product correctly to avoid danger or property loss.

The precaution measure is divided into Warnings and Cautions:

- **Warnings**: Neglecting any of the warnings may cause serious injury or death.
- **Cautions**: Neglecting any of the cautions may cause injury or equipment damage.

Warnings

- All the electronic operation should be strictly compliance with the electrical safety regulations, fire prevention regulations and other related regulations in your local region.
- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- Please make sure that the power has been disconnected before you wire, install or dismantle the camera.

- If smoke, odors or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the speed dome yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)

Cautions

- Do not drop the dome or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).
- Do not place the dome in extremely hot, cold, dusty or damp locations, otherwise fire or electrical shock will occur. The operating temperature should be -22 °F ~ 149 °F (-30 °C ~ 65 °C).
- The dome cover for indoor use shall be kept from rain and moisture.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- Do not aim the speed dome at the sun or extra bright places. A blooming or smear may occur otherwise (which is not a malfunction however), and affecting the endurance of sensor at the same time.
- Please use the provided glove when open up the dome cover, avoid direct contact with the dome cover, because the acidic sweat of the fingers may erode the surface coating of the dome cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the dome cover, do not use alkaline detergents.
- Please keep all packaging for future use. In case of a failure, use the original packaging to return the camera to the factory. Transportation without the original packaging may result in damage to the camera and incur additional costs.

Read these instructions and keep them in a safe place for future reference.

- Please refer all work related to the installation of this product to qualified service personnel or system installers.
- Do not operate the camera outside of its specified temperature, humidity or power source ratings.
- Install the unit away from heat sources such as radiators, heat registers and stoves.
- Installation of the unit near consumer electronics devices, such as stereo receiver/amplifiers and televisions, is permitted as long as the air surrounding the terminal does not exceed the above mentioned temperature range.
- Handle the camera with care. Do not drop or shake, as this may damage it.
- Do not use strong or abrasive detergents when cleaning the surfaces of this product. When dirt is hard to remove, use a mild detergent and wipe gently.
- Save your system configuration.
- Distributing, copying, disassembling, reverse compiling, reverse engineering, and exporting, in violation of export laws, the software provided with this product is expressly prohibited.

Table of Contents

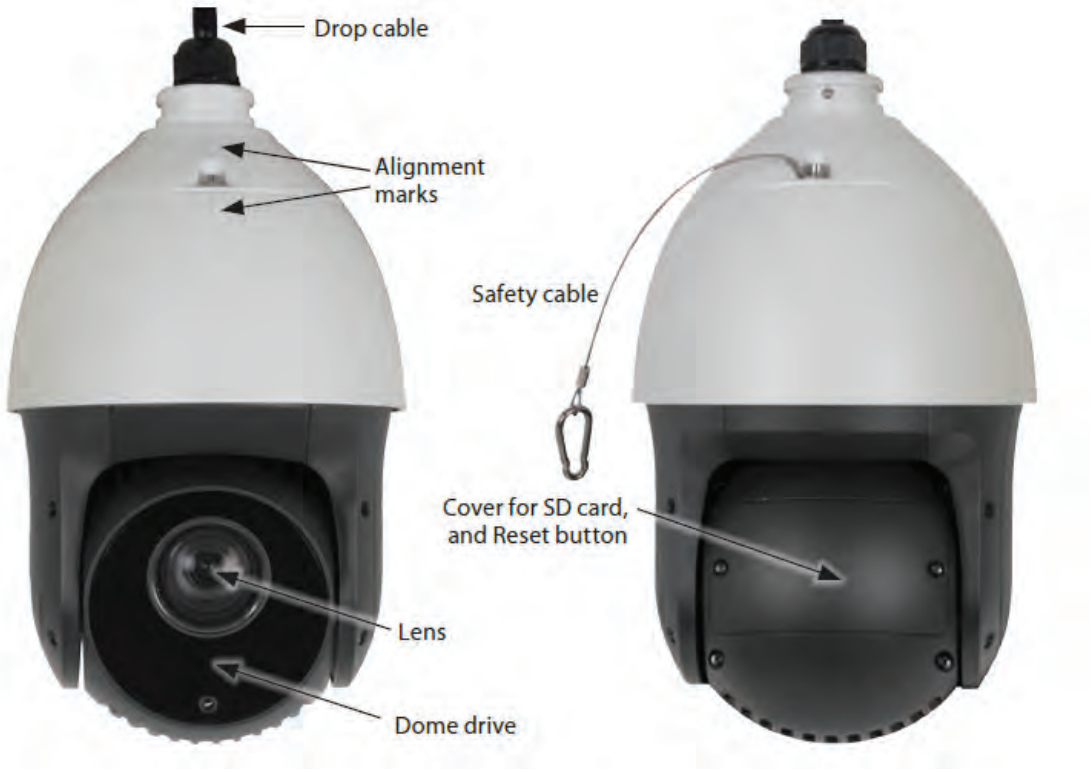
SECTION 1 **Overview** 11
1.1 Features 11
1.2 What's in the box 53
1.3 Accessories 11
SECTION 2 **Installation** 14
2.1 Remove the camera from the packaging 14
2.2 Install an micro-SD card in the camera 15
2.3 Camera wall mount installation 16
2.4 Ceiling mounting 17
2.5 Connecting the cables 18
SECTION 3 **Configure Network Access** 22
SECTION 4 **Remote login** 25
4.1 Additional configuration steps 29
APPENDIX A **Specifications** 30
APPENDIX B **Definitions** 32
APPENDIX C **Lightning and Surge Protection** 34
APPENDIX D **24 Vac Wire Gauge and Transmission Distance** 35

NOTES

SECTION 1
Overview

Congratulations on purchasing your new IP PTZ camera! This installation guide includes procedures for installing and performing the initial setup of the camera.

The PTZ Dome Camera can capture high quality images in low light environment with its black anti-reflective glass. The black anti-reflective glass increase the luminousness for an IR reach of up to nearly 500 feet. Embedded with a 1/2.8'' progressive scan CMOS chip makes DWDR 2MP real-time resolution possible. With the 20× optical zoom Day/Night lens, the camera offers more details over expansive areas. This camera also features a wide range of functions, including intrusion detection, line crossing detection and audio exception, benefitting users with great improvement on security efficiency, more importantly, with key events / objects being recorded for further forensic needs.



1.1 Features

Basic functions

- High performance sensor, up to 1920 x 1080 resolution
- ±0.1° Preset accuracy
- ONVIF (Open Network Video Interface Forum), CGI (Common Gateway Interface), PSIA (Physical Security Interoperability Alliance), to ensure greater interoperability between different platforms and compatibility

- 3D intelligent positioning function
- Power-off memory function: restore PTZ & lens status after reboot
- IP66 compliant

Functions

- Detections: intrusion detection, line crossing detection, audio exception detection, motion detection
- Recording: edge recording, support smart search in smart NVR
- Support low bit rate, ROI

Camera function:

- Auto iris, auto focus, auto white balance, backlight compensation and auto day & night switch
- Min. Illumination: 0.02 Lux @ (F2.0, AGC ON) (Color), 0.002 Lux @ (F2.0, AGC ON) (B/W)
- Supports 8 privacy masks

PTZ function:

- 360° endless pan range and -15° ~ +90° tilt range
- 400°/s Pan Preset Speed and 200°/s Tilt Preset Speed
- 0.1° ~ 400°/s Manual Pan Speed and 0.1° ~ 200°/s Manual Tilt Speed
- 300 programmable presets; preset image freezing capability
- 8 patrols, up to 32 presets per patrol

Network function:

- H.264/ MJPEG video compression and the latest processing chip and platform
- Built-in web server
- Support Micro SD card local storage, up to 128GB
- Support up to 8 NAS storage; transmit videos from the SD card to the NAS after network recovery
- HTTPS encryption and IEEE 802.1X port-based network access control
- Support dual-stream; H.264/ MJPEG video compression; basic and advanced video configuration; real time video at 1080P
- Multiple network protocols supported: IPv4/IPv6, HTTP, HTTPS, 802.1X, QoS, FTP, SMTP, UPnP, SNMP, DNS, DDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, ICMP, DHCP, PPPoE
- 1 audio input and 1 audio output
- 2 alarm inputs and 1 alarm output, alarm linkage support preset, patrol, pattern, recording, relay output, upload center, etc.

IR function:

- 0 Lux minimum illumination
- Up to 492 ft IR distance
- IR light MTBF reaching up to 30,000 hours
- Smart IR mode

1.2 What's in the box

Your camera includes:

- PTZ camera assembly
- Pendant adapter
- Ethernet drop cable seal kit
- Hi-Power PoE injector
- Gloves
- Hex L-wrench
- Thread tape
- Quick installation guide (this document)



Pendant adapter

SECTION 2
Installation

Before you start

- Check the package contents and make sure that the device in the package is in good condition and all the assembly parts are included:
  - PTZ camera assembly
  - Pendant adapter
  - Thread tape
  - Hi-Power PoE injector
  - Gloves
  - Hex L-wrench
  - Quick installation guide (this document)
- Make sure the mounting surface and fasteners are strong enough to withstand at least 8 times the weight of the camera assembly and the mounting bracket.
- For cement walls, use an expansion screw to secure the mounting bracket.

CAUTION

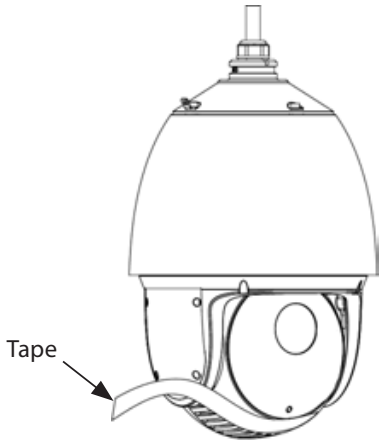
Do not carry the camera by the drop cable.



For outdoor installations, refer to "APPENDIX C Lightning and Surge Protection" on page 28 for additional installation considerations.

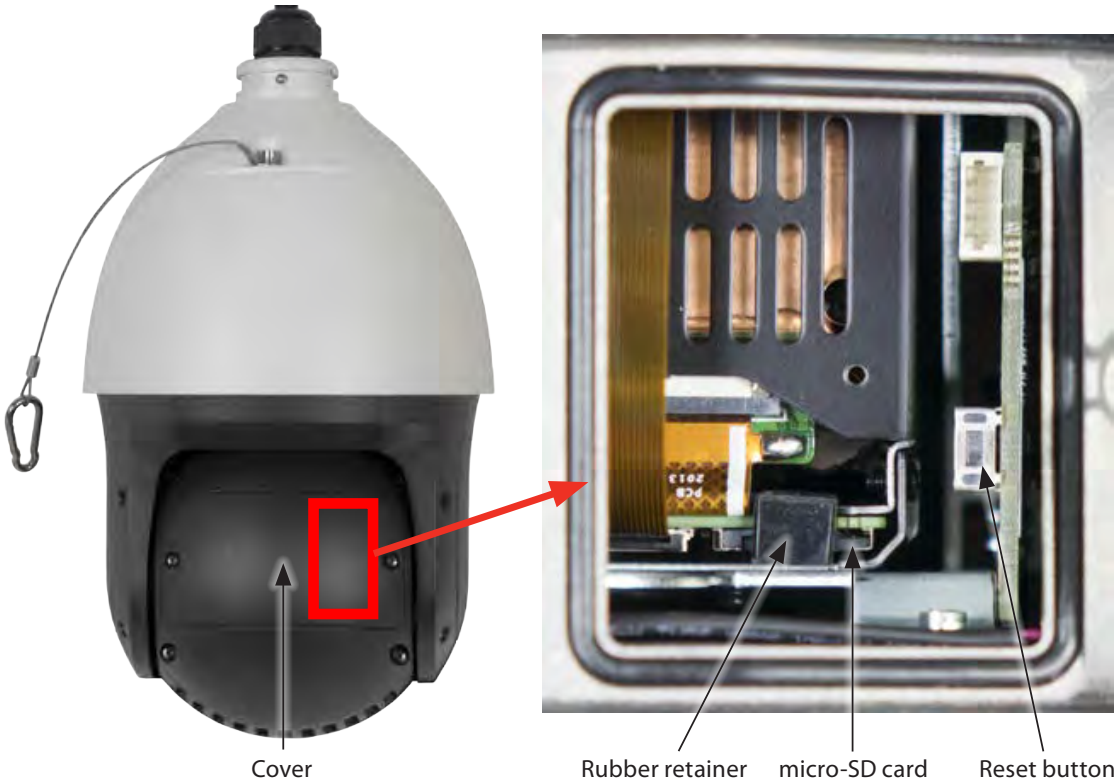
2.1 Remove the camera from the packaging

1. Remove the camera from the protective packaging.
2. Remove tape from the dome drive, if attached.



2.2 Install an micro-SD card in the camera

The micro-SD card in the provides in-camera (local) storage for log information and locally stored video and capture files. Cameras without an SD card cannot provide camera log information, which is valuable for maintenance purposes. Your camera will accommodate a micro-SD card with up to 128 GB of storage. The location of the micro-SD card slot is shown below.



1. Use a Phillips #2 screw driver to remove the back cover of the camera. See the photo above.
2. Insert the micro-SD card into the card slot until it clicks into place.
3. Pull the rubber retainer out and over the edge of the micro-SD card and PC board it attaches to.
4. Reattach the back cover.

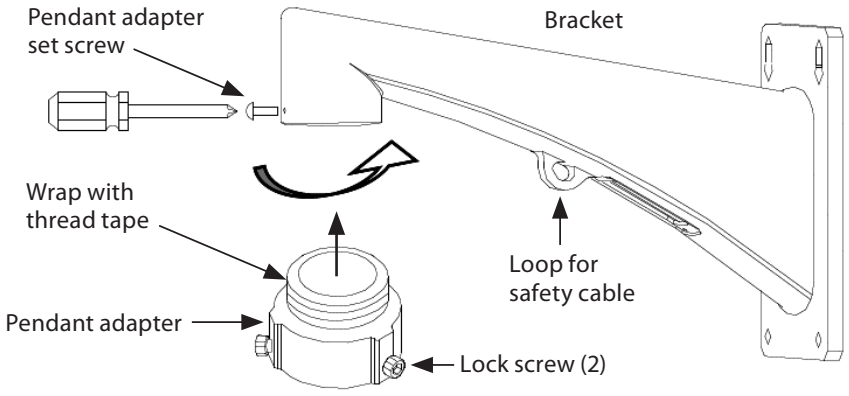
2.3 Camera wall mount installation

Following the instructions below to install the camera using the **Wall Mount Bracket**.

Instructions for mounting the camera with a **Pole Mount PTZ Bracket** or **Corner Mount PTZ Bracket** are very similar.

For these brackets, use the instructions below as a guide. .

1. Determine the best mounting screws and hardware to anchor the mounting bracket with the camera to the mounting surface. Use the following guidelines:
   - For cement wall mounting, use the expansion screw to anchor the bracket.
   - For wooden wall mounting, use self-tapping screw to anchor the bracket.
   - Make sure that the wall is strong enough to withstand more than **8 times** the weight of the camera and the bracket.
2. Using the mounting bracket as a template, mark the location of the mounting screw holes on the mounting surface. Also mark the location of a hole for the camera drop cable. The drop cable will be routed through the mounting bracket and through the mounting surface.
3. Drill holes in the mounting screws and hardware. Also, drill a 1½" diameter hole in the mounting surface for the drop cable.
4. Apply two wrap of the thread tape provided onto the treads of the pendant adapter (see below)

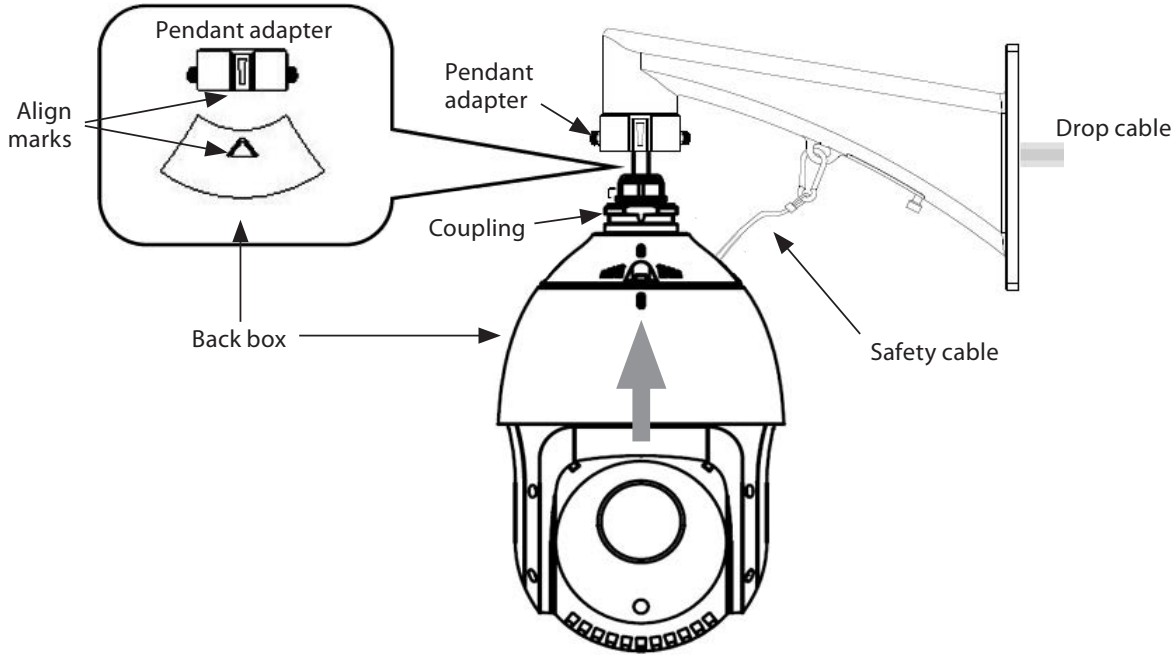


Attach pendant adapter to mounting bracket

5. Screw the pendant adapter onto the end of the mounting bracket. Tighten the set screw to secure the adapter to the bracket.

6. Clip the safety cable to the loop on the camera mounting bracket.

7. Route the camera drop cable through the mounting bracket, then clip the safety cable onto the loop in the mounting bracket.



8. Fit the camera coupling into the pendant adapter, then twist the camera to align the marks on the pendant adapter and the camera back box. See the figure above.

9. Tighten the two lock screws on the pendant adapter to secure the camera to the mounting bracket.

10. Feed the camera drop cable through hole drilled at the mounting location, then anchor the mounting bracket to the wall.

2.4 Ceiling mounting

Following the instructions below to install the camera using the **Ceiling Mount Bracket**.

1. Determine the best mounting screws and hardware to anchor the mounting bracket with the camera to the mounting surface. Use the following guidelines:
   - For cement ceiling mounting, use the expansion screw to anchor the bracket.
   - For wooden ceiling mounting, use self-tapping screw to anchor the bracket.
   - Make sure that the ceiling is strong enough to withstand more than **8 times** the weight of the camera and the bracket.

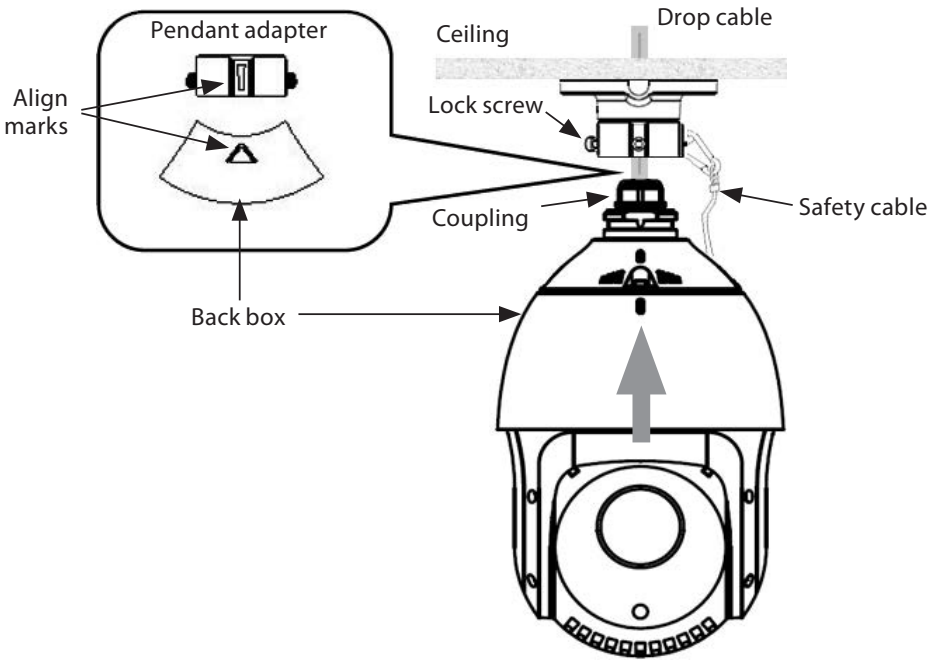
2. Using the mounting bracket as a template, mark the location of the mounting screw holes on the ceiling.

3. If the camera drop cable will be routed through the ceiling, mark the location of a hole for the camera drop cable. The drop cable will be routed through the mounting bracket and can be routed either through the mounting surface or out the side of the mounting bracket.

4. Drill holes in the mounting screws and hardware. Also, drill a 1½" diameter hole in the mounting surface for the drop cable.

5. Clip the safety cable to the loop on the camera mounting bracket.

6. Route the camera drop cable through the mounting bracket, then clip the safety cable onto the loop in the mounting bracket.



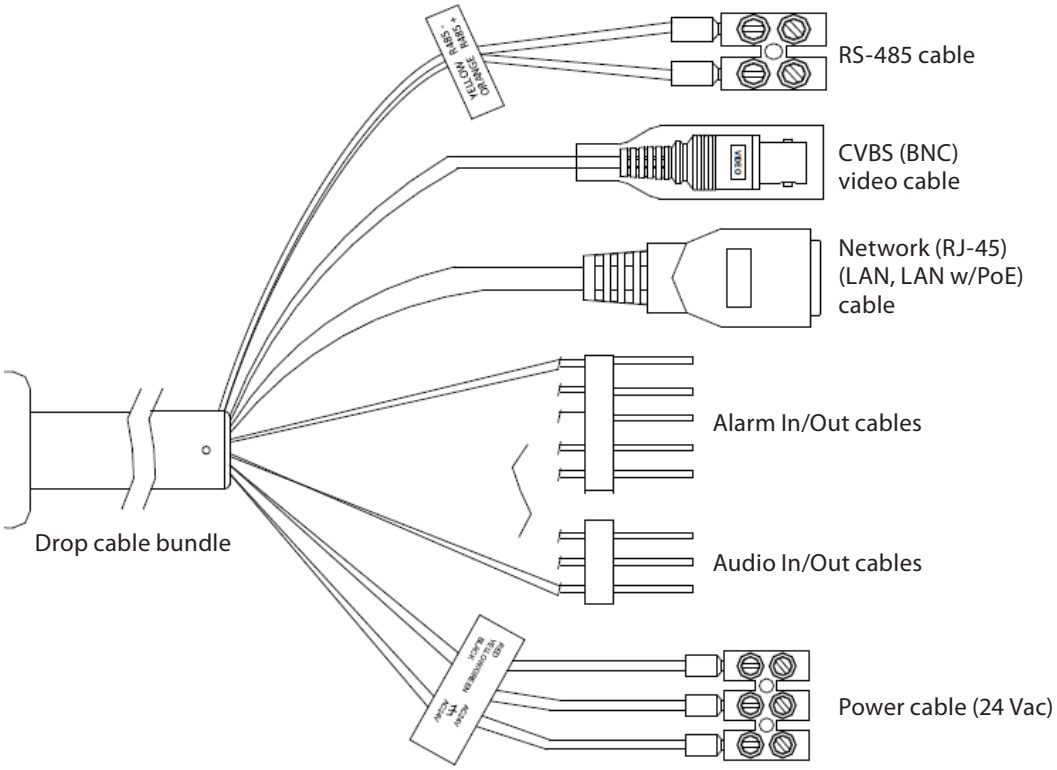
7. Fit the camera coupling into the ceiling mounting bracket, then twist the bracket to align the marks on the bracket and the camera back box. See the figure above.

8. Tighten the two lock screws on the ceiling bracket to secure the camera to the mounting bracket.

9. Feed the camera drop cable through hole drilled at the mounting location, then anchor the mounting bracket to the ceiling.

2.5 Connecting the cables

Drop cables connectors for the IDCMR-IP-POE-PTZ-20X are shown below. Each wire is labeled with its purpose.



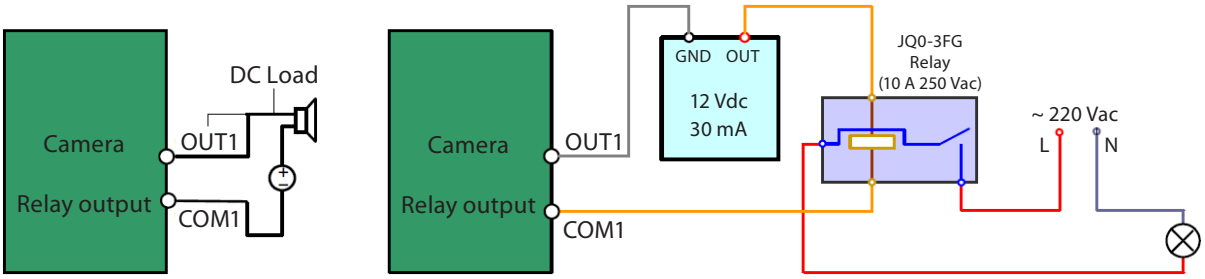
Connect the camera to other devices as needed in the order shown below.

Alarm Input/Output cables

The alarm input/output drop cable bundle provides five wires, ALARM_IN1, ALARM_IN2, ALARM_OUT1, ALARM_COM1 and ALARM_GND. These wires are color coded and labeled.

These connection use the ALARM_IN1 and ALARM_GND wires for alarm input 1, and ALARM_IN2 and ALARM_GND wires for alarm input 2. Alarm inputs normally connect normally open (NO) or normally closed (NC) sensor contacts. The normal contact state is configurable in the camera setup menus.

Connect the camera alarm output drop cables to an alarm reporting device. See the Specifications section for interface requirements and the diagram below. These connection use the ALARM_OUT1 and ALARM_COM1 wires.



The alarm output provides the relay output (no voltage). An external power supply is required when it connects to the alarm device. With a DC power supply (left diagram), the input voltage must be no more than 12 Vdc, 30 mA. For AC power supply (right diagram), the external relay must be used to prevent damages to the camera and avoid the risk of electric shock.

Audio cable

The Audio drop cable provides three wires: AUDIO_OUT, AUDIO_IN and AUDIO_GND (ground). These wires are color coded and labeled.

Connect the AUDIO_IN and AUDIO_GND wires to a line level audio input source. The input signal must be 2 ~ 2.4 Vp-p at 1 KΩ ± 10% input impedance.

Connect the AUDIO_OUT and AUDIO_GND wires to a line level audio receiver (impedance 600 Ω).

RS-485 cables

Connect the RS485+ and RS485- drop cable wires to an RS-485 controller or an NVR with an RS-485 network interface. PTZ features can also be controlled through the camera network (browser) interface, and through a supported NVR PTZ control panel. These wires are color coded and labeled.

Video cables

The video drop cable provides a BNC connector with a CVBS signal for connection to any compatible monitor. The feature is useful for maintenance and for showing the live view display on a local monitor.

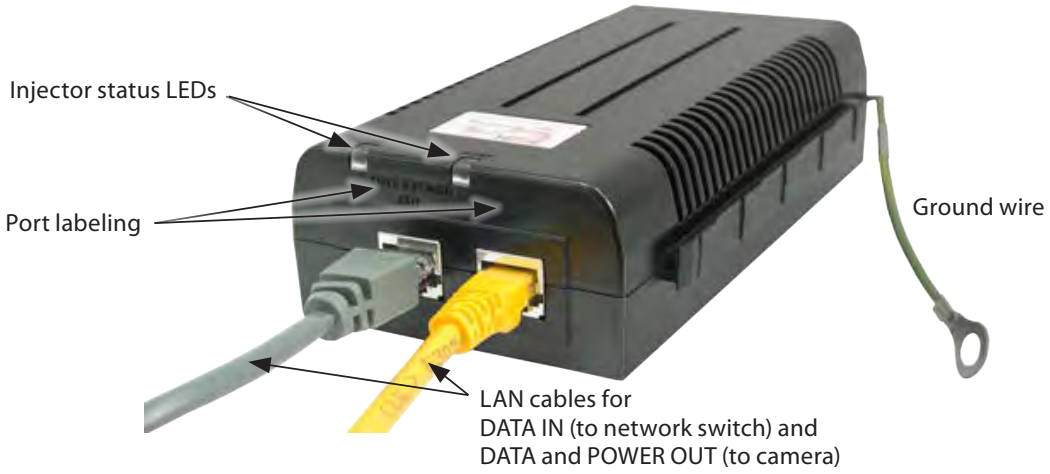
Network (LAN) cable

Connect the network LAN drop cable to a router (switch) through an Ethernet drop cable with an RJ-45 connector. If the drop cable RJ-45 connector is exposed to moisture or dust, apply the Ethernet drop cable seal kit provided. In some network configurations, the LAN cable can connect directly to a Network Video Recorder (NVR) with a built-in network switch.

Power cables

You can power the camera directly by applying 24 Vac power to the drop cable power screw-down connectors. Refer to "APPENDIX D 24 Vac Wire Gauge and Transmission Distance" on page 29 for more information.

The LAN cable can also provide Hi-PoE to the camera. A Hi-PoE injector is provided. A typical PoE injector is shown below.



To use the injector:

1. Connect the injector ground wire to an earth ground terminal. (**NOTE**: Not all PoE injectors have a ground wire.)
2. Connect a LAN drop cable between the network switch and the DATA IN port on the injector.
3. Connect a LAN drop cable between the injector DATA and POWER OUT port and the camera LAN drop cable.
4. Plug the power cable provided (not shown) for the PoE injector into the jack on the injector, then into a standard 120 Vac electrical outlet.

After power is applied to the camera, the camera will perform initial motion checks. Allow these motion checks to complete before continuing (~ 1 minute).

SECTION 3
Configure Network Access

After the camera is powered on, an initial network configuration setup should be performed. This procedure includes:

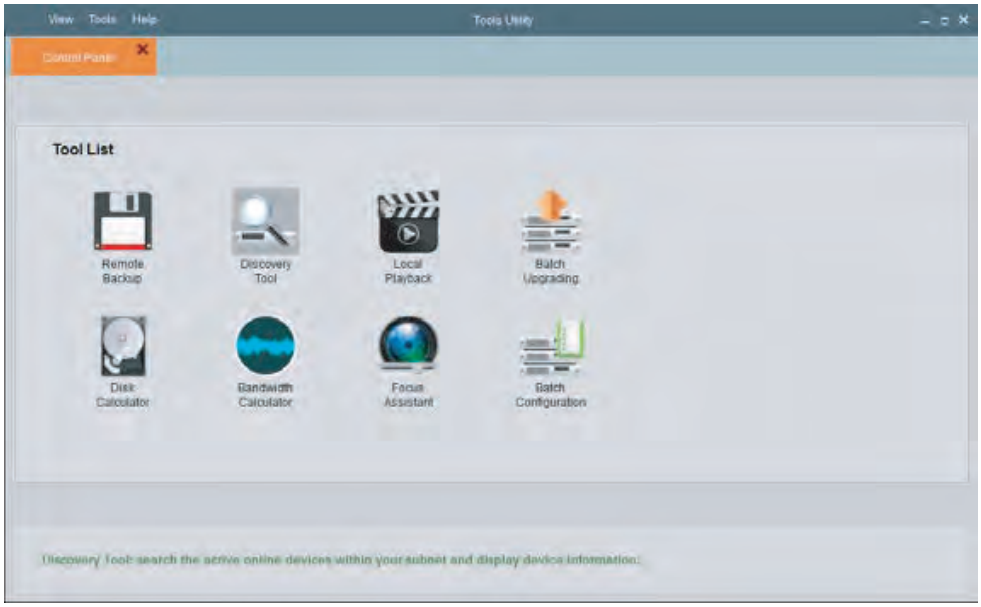
- Installing SADP Tools
- Setting up the camera network configuration

Step 1. Install SADP Tool

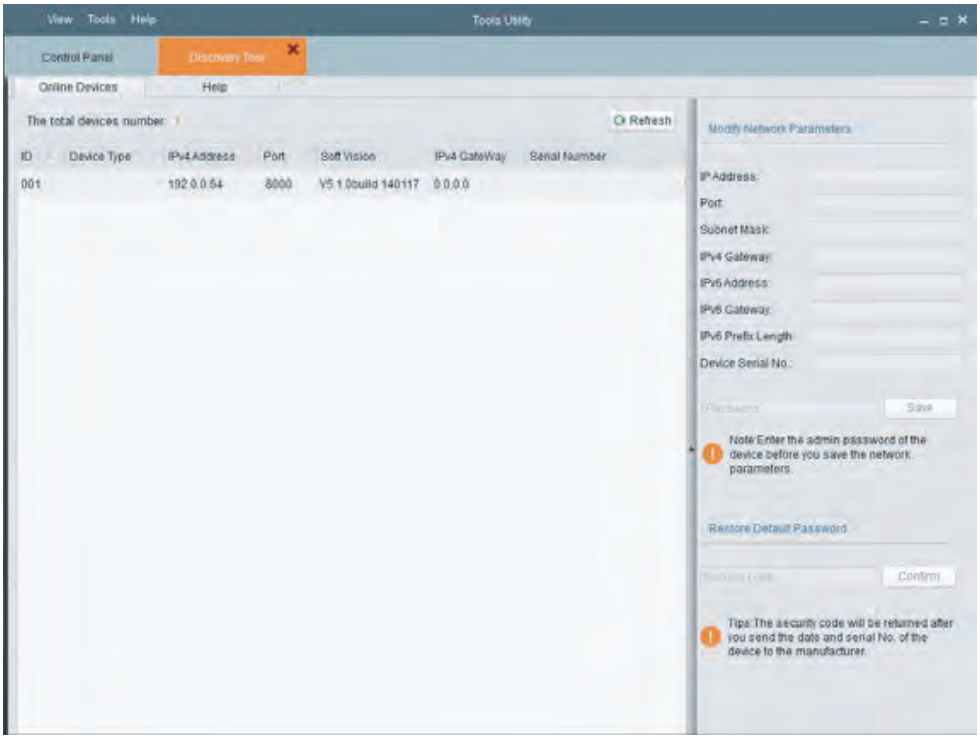
SADP Tool Utility is a collection of useful software programs for use with your IP based cameras and recorders. Within the tool set is the **Discovery Tool** a software utility used to "discover" IP cameras and NVRs/DVRs installed on the LAN and change their network parameters. Use Discovery Tool to setup your camera on a network. See below.
Download: https://www.larsonelectronics.com/images/upload/SADPTool.zip

Tools Utility is provided on the SADP Tool.
Use the Tools Utility Installation and User Manual, and embedded in the **SADP software.**

1. Install the Tools Utility on a PC with access to the LAN where your camera is connected. When the program opens, the following screen appears.

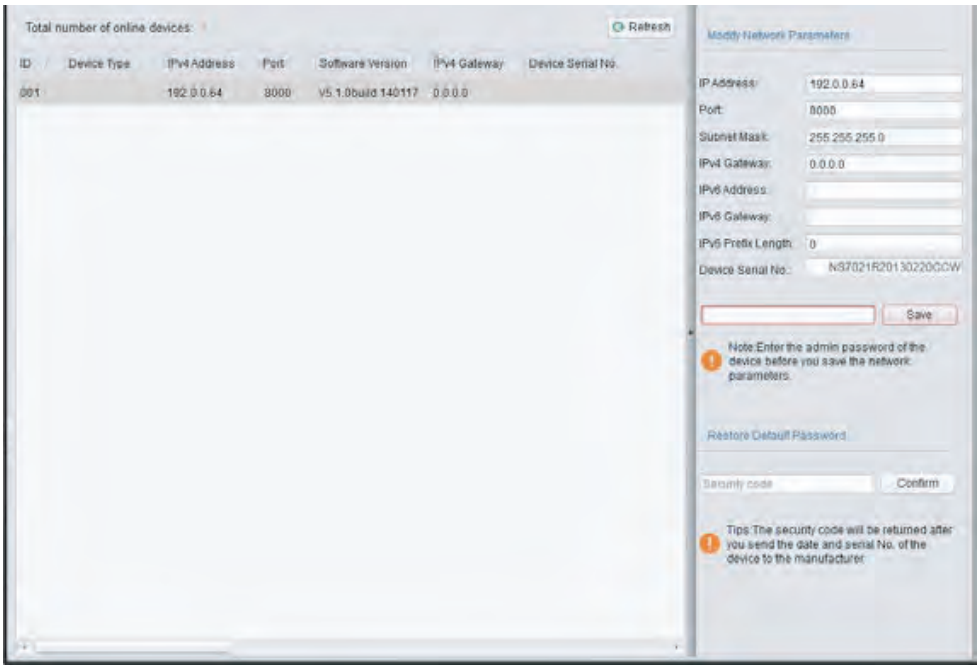


2. Double click the **Discovery Tool** icon to open the program. When the program opens it will automatically list the cameras and recorders installed on the network.

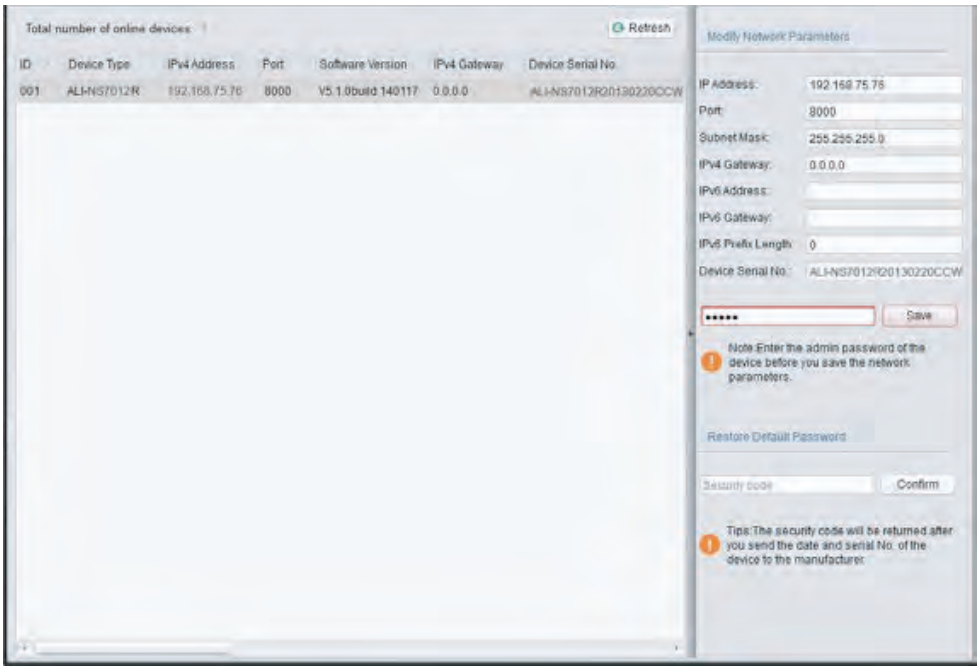


3. To change the network settings of the camera to be compatible with the subnet where it is installed, do the following:

   a. Click the device to highlight it. Notice that the network parameters are shown in the right frame.



b. Modify the network parameters to values compatible with the subnet where it is installed.



c. Enter the **admin** password for the device in the password field. The default **admin** user password for is **ChangeMeNØw**

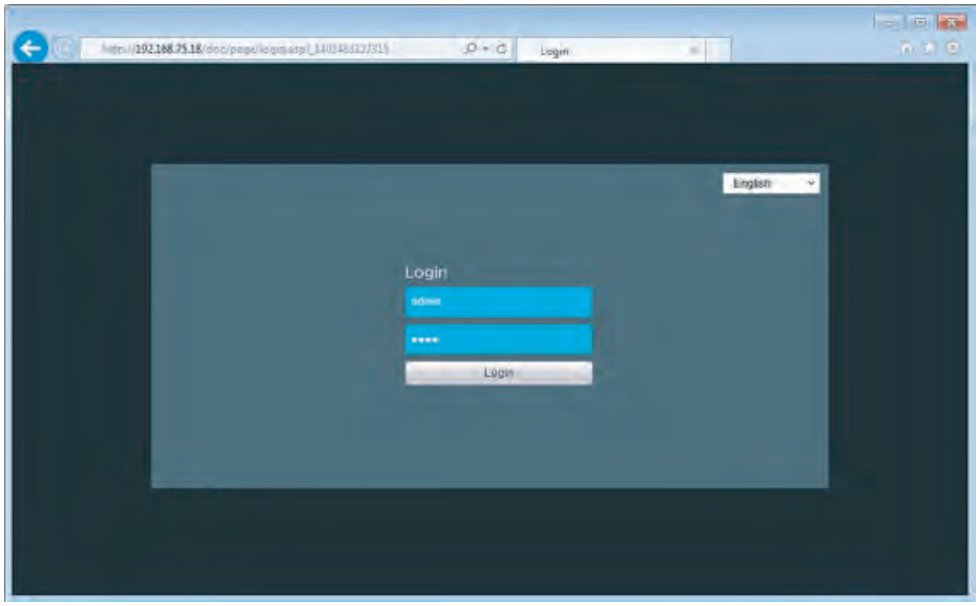
d. Click the **Save** button. The new IP address, port, etc. parameters will appear in the list with the device you modified.

3. Close the Tool Utility by clicking the **Close** icon (☒) in the upper-right corner of the window.

SECTION 4
Remote login

To access the camera from a computer on the LAN:

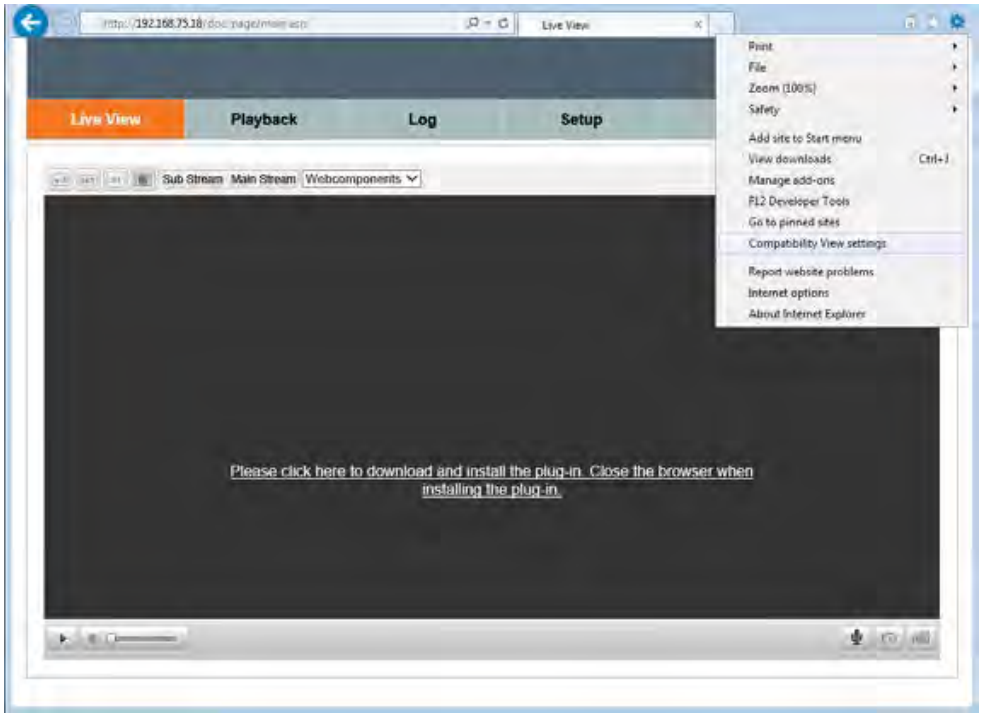
1. Open your Microsoft Internet Explorer browser on your compute and enter the IP address of the camera in the URL field. In the example below, the IP address of the camera is 192.168.75.18.



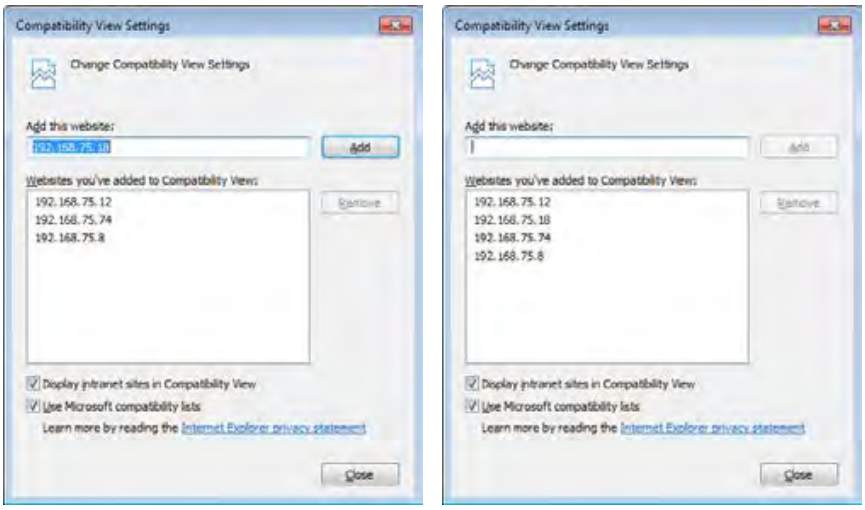
2. In the login window, enter your **User Name** and **Password** in the appropriate fields, then click **Login**. The default **User Name** and **Password** for cameras is **admin** and **ChangeMeNØw**

3. If this is the first time you are logging into the camera at this IP address AND you are using Internet Explorer 10 or newer, you must configure IE for Compatibility mode:

    a. In Internet Explorer, click the Tools icon (located to the right of the tabs), then select Compatibility View settings from the drop-down menu.

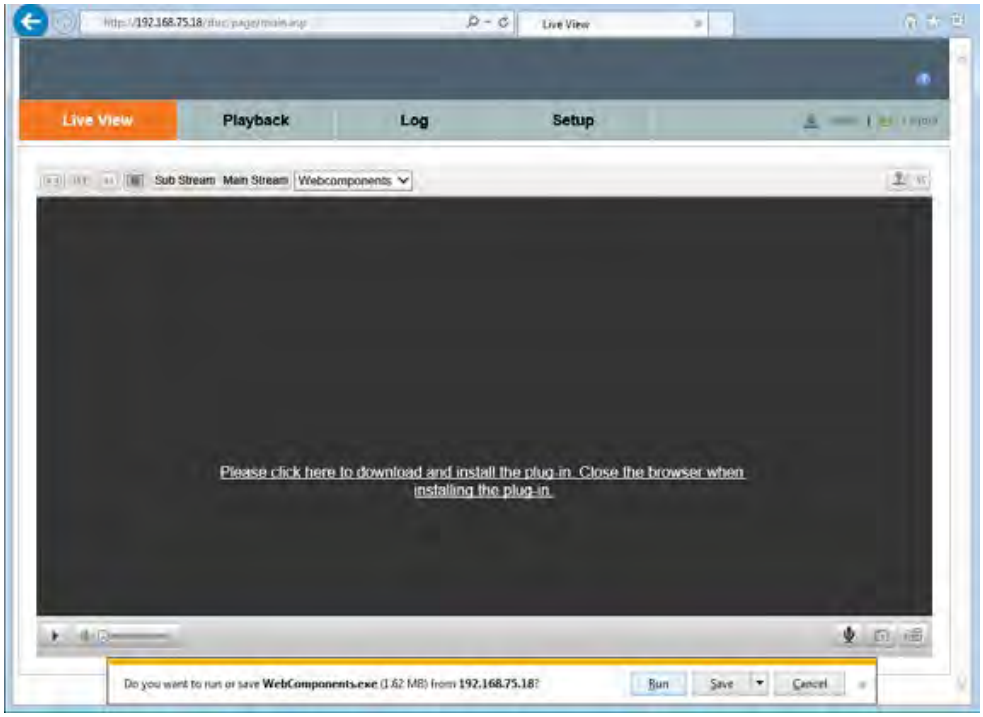


b. In the Compatibility View Settings window, ensure that the IP address of your camera is in the **Add this website** field, then click **Add**.

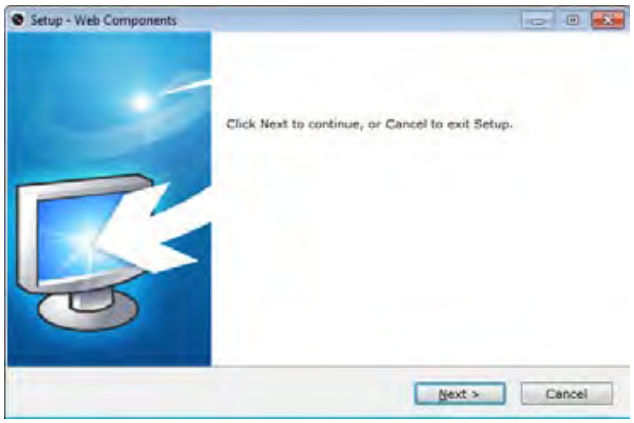


c. After clicking **Add**, the IP address will appear in the Websites list. Click **Close**.

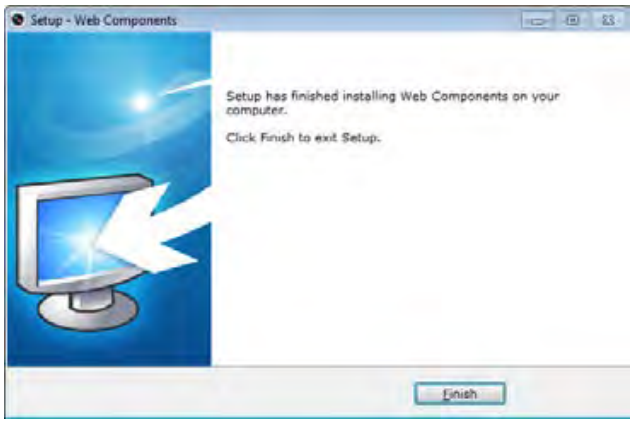
d. If a message on the screen requesting that you install a plug-in (see below), click on the message and continue with the following sub-steps. A message box will appear at the bottom of the window to install the WebComponents plug-in. Otherwise, continue with step "4. In the Live View window shown below, click the PTZ button to open/close the PTZ control panel." on page 22.



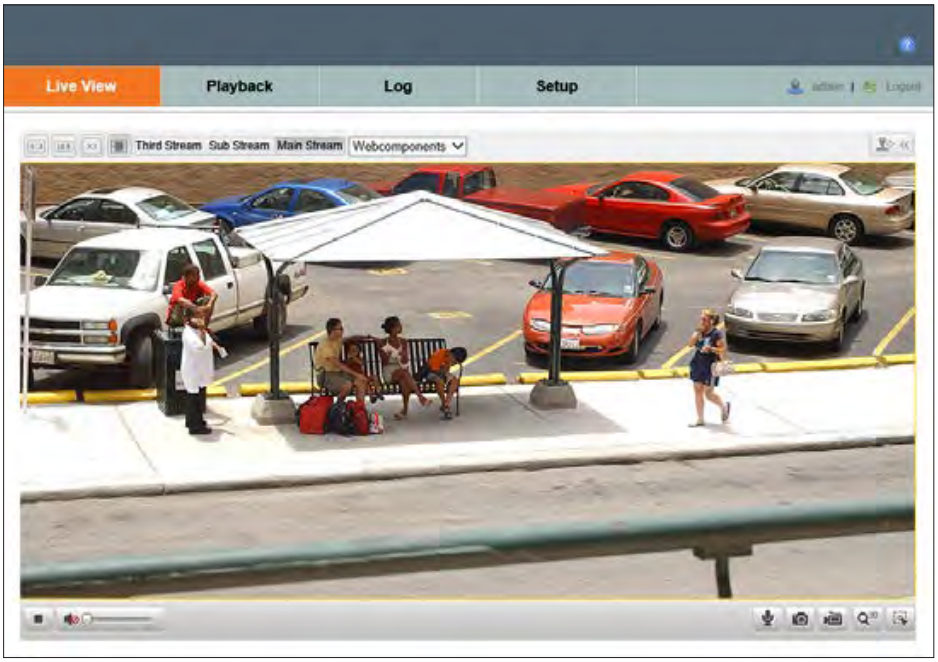
e. In the message box, click **Run** to install WebComponents.exe. The following pop-up window will open. When this window appears, close the browser.



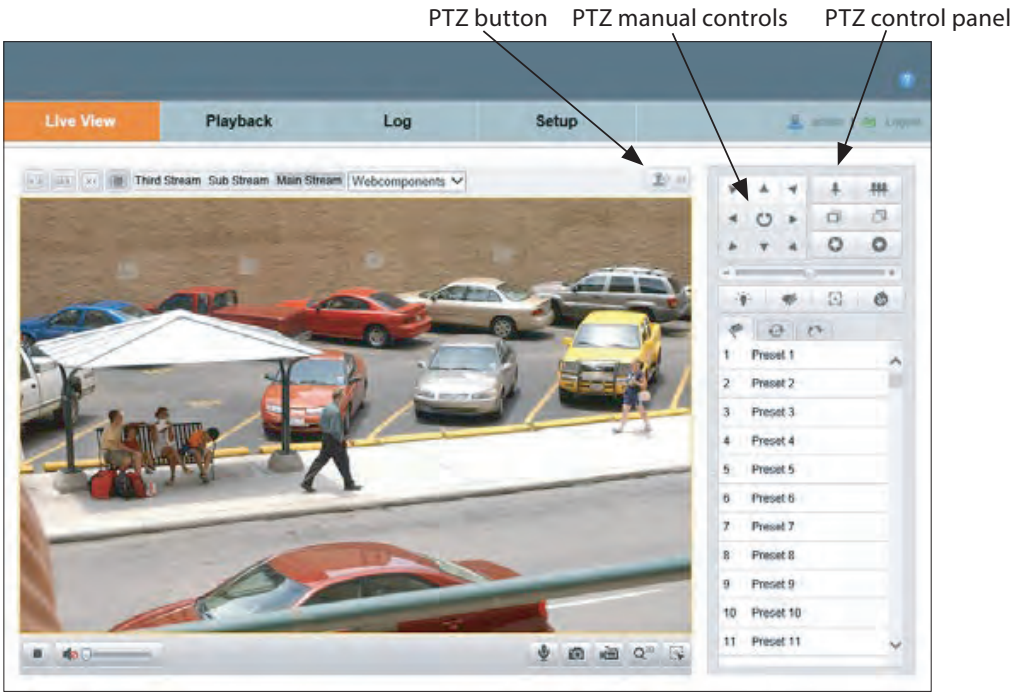
f. Click **Next** to install WebComponents. Allow the plug-in installation to complete. When the following window appears, click **Finish**.



g. Log into the camera again. A **Live View** display will appear.



4. In the Live View window shown below, click the PTZ button to open/close the PTZ control panel.



5. In the PTZ control panel, click the manual control arrows to exercise the pan-tilt-zoom features of the camera.

4.1 Additional configuration steps

Refer to the document IP Camera Software User Manual provided on the software and documentation with your camera to customize the configuration of your camera.

APPENDIX A
Specifications

Camera Module	
Image Sensor	1/2.8" Progressive Scan CMOS
Min. Illumination	F1.5, AGC On: Color: 0.02 lux, B/W : 0.002 lux, 0 lux with IR
Max. Image Resolution	1920 x 1080
Focal Length	4.7 ~ 94.0 mm, 20×
Digital Zoom	16×
Zoom Speed	Approx. 3 s (optical Wide ~ Tele)
Angle of View	58.3 ~ 3.2 degree (Wide ~ Tele)
Min. Working Distance	10 ~ 1,000 mm (Wide~Tele)
Aperture Range	F1.6 ~ F3.5
Focus Mode	Auto / Semiautomatic / Manual
DWDR	Support
S/N Ratio	≥ 52 dB
Shutter Time	1 ~ 1/10,000 s
AGC	Auto / Manual
White Balance	Auto / Manual / ATW / Indoor / Outdoor / Daylight lamp / Sodium lamp
Day & Night	IR Cut Filter
Privacy Mask	8 privacy masks programmable
Enhancement	3D DNR, Defog, HLC/BLC
Pan and Tilt	
Range	Pan: 360° endless; Tilt: -15° ~ 90° (Auto Flip)
Speed	Pan Manual Speed: 0.1° ~ 400°/s, Pan Preset Speed: 400°/s, Tilt Manual Speed: 0.1° ~ 200°/s, Tilt Preset Speed: 200°/s
Number of Preset	300
Patrol	8 patrols, up to 32 presets per patrol
Park Action	Preset / Patrol / Pattern / Pan scan / Tilt scan / Random scan / Frame scan / Panorama scan
Scheduled Task	Auto scan / Frame scan / Random scan / Patrol / Pattern / Preset / Panorama scan / Tilt scan / Dome reboot / Dome adjust / Aux output
Features	
Detection	Intrusion detection, Line crossing detection, Audio exception detection, Motion detection
ROI encoding	Support 4 areas with adjustable levels
Infrared	
IR Distance	Up to 492 ft (150 m)
IR Intensity	Automatically adjusted, depending on the zoom ratio

Alarm	
Alarm I/O	2/1
Alarm Trigger	Intrusion detection, Line crossing detection, Audio exception detection, Motion detection, Dynamic analysis, Tampering alarm, Network disconnect, IP address conflict, Storage exception
Alarm Action	Preset, Patrol, Pattern, Recording, Relay output, Upload center, Upload FTP, Email linkage
Input/Output	
Audio Input	1 Mic in / Line in interface, line input: 2 ~ 2.4 Vp-p; output impedance: 1 KΩ ± 10%
Audio Output	1 Audio output interface, line level, impedance: 600 Ω
Network	
Ethernet	10BASE-T / 100BASE-TX, RJ-45 connector
Main Stream (NTSC)	30 fps (1920 ×1080), 30 fps (1280 ×1720)
Sub Stream (NTSC)	60 Hz: 30 fps (704 ×1480), 30 fps (352 ×1240), 30 fps (320 ×1240)
Image Compression	H.264 / MJPEG
Audio Compression	G.711ulaw / G.711alaw / G.726 / MP2L2 / G.722
Protocols	IPv4 / IPv6, HTTP, HTTPS, 802.1X, QoS, FTP, SMTP, UPnP, SNMP, DNS, DDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, ICMP, DHCP, PPPoE
Simultaneous Live View	Up to 20 users
Mini SD Memory Card	Support up to 128 GB micro-SD / SDHC / SDXC card. Supports edge recording
User/Host Level	Up to 32 users, 3 Levels: Administrator, Operator and User
Security Measures	User authentication (ID and password); Host authentication (MAC address); IP address filtering
System Integration	
Application programming	Open-ended API, support ONVIF, PSIA and CG
Web Browser	Internet Explorer® 7.0 or above, Apple® Safari® 5.02 or above, Mozilla® Firefox® 5 or above, Google Chrome™ 18 or above
Power	High-PoE & 24 Vac, Max. 30 W
Working Temperature	-22°F ~ 149°F (-30°C ~ 65°C)
Humidity	90% or less
Protection Levels	IP66, TVS 4,000V lightning protection, surge protection and voltage transient protection
Certifications	FCC, CE, UL, RoHS, IEC / EN 61000, IEC / EN 55022, IEC / EN 55024, IEC / EN60950-1
Dimensions	Φ10.50 in × 14.38 in (Φ266.6 mm × 365.2 mm)
Weight (approx.)	8.81 lb (4 kg)
Mount options	PTZCL: Ceiling Mount Bracket PTZWB: Wall Mount Bracket PTZPM: Pole Mount PTZ Bracket PTZCM: Corner Mount PTZ Bracket
Supplied accessories	
	Installation Guide, HPoE Midspan injector, installation hardware

APPENDIX B
Definitions

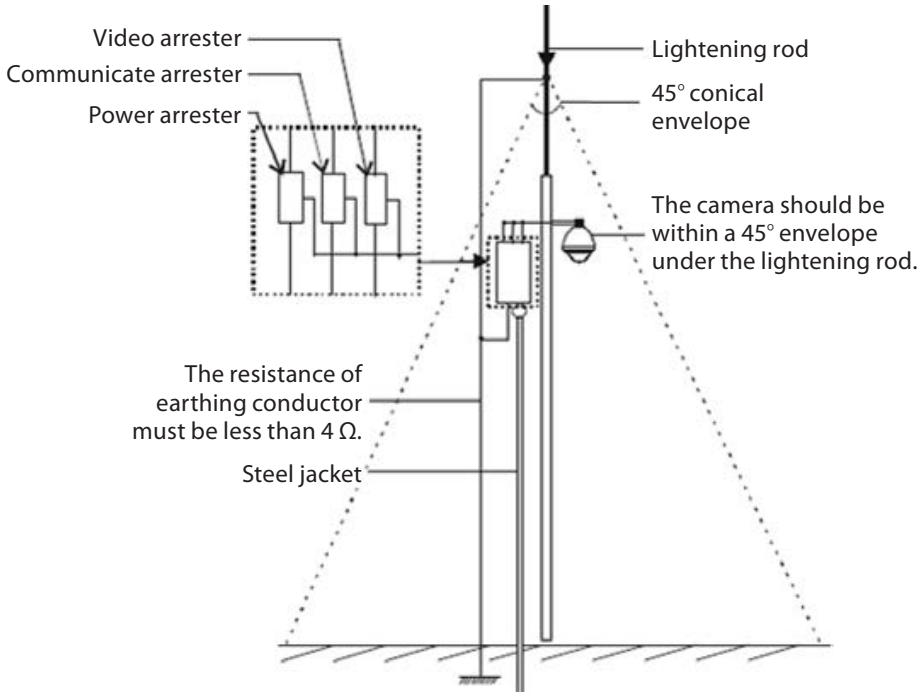
3D Digital Noise Reduction	Comparing with the general 2D digital noise reduction, the 3D digital noise reduction function processes the noise between two frames besides processing the noise in one frame resulting in clearer video.
3D Positioning	In the client software, use the click left mouse button on the desired position in the video image, and then drag a rectangle area in the lower right direction. The dome system will move the position to the center and allow the rectangle area to zoom in. Use the left key of the mouse to drag a rectangle area in the upper left direction to move the position to the center and allow the rectangle area to zoom out.
Auto Flips	In manual tracking mode, when a target object goes directly beneath the dome, the video will automatically flips 180 degrees in horizontal direction to maintain continuity of tracking. This function can also be realized by auto mirror image depending on different camera models.
Auto Focus	The auto focus enables the camera to focus automatically to maintain clear video images.
Backlight Compensation (BLC):	If you focus on an object against strong backlight, the object will be too dark to be seen clearly. The BLC function can compensate light to the object in the front to make it clear. This can cause an over-exposure of the background where the light is strong.
Day/Night Auto Switch	The speed domes deliver color images during the day. And as light diminishes at night, the speed domes switch to night mode and deliver black and white images with high quality.
Label Display	The on-screen label of the preset title, time and dome name can be displayed on the monitor. The displays of time and speed dome name can be programmed.
Limit Stops:	The dome can be programmed to move only within the limit stops (left/right, up/down).
Park Action	This feature allows the dome to start a predefined action automatically after a period of inactivity.
Patrol	A patrol is a memorized series of pre-defined preset function. The scanning speed between two presets and the dwell time at the preset are programmable.
Pattern	A pattern is a memorized series of pan, tilt, zoom, and preset functions. By default the focus and iris are in auto status during the pattern is being memorized.
Power Off Memory	The dome supports the power off memory capability with the predefined resume time. It allows the dome to resume its previous position after power is restored.
Preset Freezing:	This feature freezes the scene on the monitor when the dome is moving to a preset. This allows for smooth transition from one preset scene to another. This also guarantees that a masked area will not be revealed when the dome is moving to a preset.
Presets	A preset is a predefined image position. When the preset is called, the dome will automatically move to the defined position. The presets can be added, modified, deleted and called.
Privacy Mask	This function allows you to block or mask certain area of a scene, for preventing the personal privacy from recording or live viewing. A masked area will move with pan and tilt functions and automatically adjust in size as the lens zooms telephoto and wide.
Proportional Pan/Tilt	Proportional pan/tilt automatically reduces or increases the pan and tilt speeds according to the amount of zoom. At telephoto zoom settings, the pan and tilt speeds will be slower than at wide zoom settings. This keeps the image from moving too fast on the live view image when there is a large amount of zoom.
Scan Modes:	The dome provides five scan modes: auto scan, tilt scan, frame scan, random scan and panorama scan.
Scheduled Task	A time task is a preconfigured action that can be performed automatically at a specific date and time. The programmable actions include: auto scan, random scan, patrol 1-8, pattern 1-4, preset 1-8, frame scan, panorama scan, tilt scan, day, night, reboot, PT adjust, Aux Output, etc.

Slow Shutter	With this feature, the camera will automatically extend the exposure time in low illumination conditions to maintain clear video images. The feature can be enabled or disabled.
User Management	The camera allows you to edit users with different levels of permission. Multiple users are allowed to simultaneously access and control the same camera through the network.
White Balance (WB)	White balance can remove the unrealistic color casts. White balance is the white rendition function of the camera to adjust the color temperature according to the environment automatically.
Wide Dynamic Range (WDR)	The WDR function helps the camera provide clear images even with back lit environments. When there are both very bright and very dark areas in the field of view, WDR balances the brightness level of the whole image and provide clearer images and details.

APPENDIX C
Lightning and Surge Protection

This product includes TVS plate lightning protection technology to prevent damage caused by a pulse signal that is below 3000 watts from sources such as lighting, surging, etc. Protection measures must be taken to ensure electrical safety.

- The distance between signal transmission line and high-voltage equipment or high-voltage cable is at least 50 m.
- Outdoor wiring should better be along the eaves as much as possible.
- In the open field, wiring should be buried underground in sealed steel pipe with one-point grounding. Overhead routing method is not acceptable.
- In regions with thunderstorms or where high induction voltage are present (such as high-voltage transformer substation), high power lightning protection apparatus and lightning conductor are necessary.
- The design for installation and wiring with lightning protection and grounding should be combined with the lightning protection consideration of the building, and conform to the relevant national and industry standards.
- The system should ensure equi-potential grounding. Grounding equipment must satisfy both system anti-jamming and electric safety. It must not allow short circuit and open circuit with the zero conductor of strong grid. When the system is singularly ground, the resistance must less than 4 Ω and the cross-sectional area of the grounding cable must be no less than 25 mm^2. For grounding instructions, refer to local electrical codes and this manual.



Lightning & Surge Protection

APPENDIX D
24 Vac Wire Gauge and Transmission Distance

The following table shows the recommended maximum distance adopted for the different wire sizes when the 24 Vac voltage loss is less than 10%. For the AC driven device, the maximum voltage loss rate allowable is 10%. For example, for a device with the rating power of 80 VA which is installed 35 feet (10 m) from the transformer, the minimum wire gauge required is 0.8000 mm.

Table 1. Table of wire gauge standards

Distance: ft (m)	Wire Gauge (mm)			
Power (VA)	**0.8000**	**1.000**	**1.250**	**2.000**
10	283 (86)	451 (137)	716 (218)	1811 (551)
20	141 (42)	225 (68)	358 (109)	905 (275)
30	94 (28)	150 (45)	238 (72)	603 (183)
40	70 (21)	112 (34)	179 (54)	452 (137)
50	56 (17)	90 (27)	143 (43)	362 (110)
60	47 (14)	75 (22)	119 (36)	301 (91)
70	40 (12)	64 (19)	102 (31)	258 (78)
80	35 (10)	56 (17)	89 (27)	226 (68)
90	31 (9)	50 (15)	79 (24)	201 (61)
100	28 (8)	45 (13)	71 (21)	181 (55)
110	25 (7)	41 (12)	65 (19)	164 (49)
120	23 (7)	37 (11)	59 (17)	150 (45)
130	21 (6)	34 (10)	55 (16)	139 (42)
140	20 (6)	32 (9)	51 (15)	129 (39)
150	18 (5)	30 (9)	47 (14)	120 (36)
160	17 (5)	28 (8)	44 (13)	113 (34)
170	16 (4)	26 (7)	42 (12)	106 (32)
180	15 (4)	25 (7)	39 (11)	100 (30)
190	14 (4)	23 (7)	37 (11)	95 (28)
200	14 (4)	22 (6)	35 (10)	90 (27)

Table 2. Wire Gauge Standards

Bare Wire Gauge (mm)	American Wire Gauge AWG	Cross-sectional Area of Bare Wire (mm^2)
0.750	21	0.4417
0.800	20	0.5027
0.900	19	0.6362
1.000	18	0.7854
1.250	16	1.2266
1.500	15	1.7663
2.000	12	3.1420
2.500		4.9080
3.000		7.0683

Network Video Recorder Setup
Quick Guide

The following serves as a setup quick guide for the purchased equipment. For a more detailed instruction and setup guide, read the detailed guides following this one.

WEB BROWSER

1. Using Internet Explorer, go to your Static IP provided by your mobile carrier.
    a. You can use either HTTP or HTTPS Protocol. Example:
        i. http://your.static.ip
        ii. https://your.static.ip
        NOTE: you would replace 'your.static.ip' with your actual Static IP address.
    b. When using HTTPS Protocol, you need to agree to the self-signed certificate.
        i. You will see "This site is not secure" pop up and you need to select the option of "Go on to the webpage" to continue.
2. To be able to see live video from the camera, you need to install the plugin for the product.
3. Enter login details.
    a. Credentials should be default settings.
        i. User: admin
        Password: Ch@ngeMeN0W
        ii. We recommend after logging in for the first time to change the login credentials from the default settings.
4. The required plugin must be installed in order for the connection to be made.
    a. After the plugin is installed you have to reset the browers window and then re-login to the system.
5. The system is now ready for live viewing See detailed NVR instructions for more details.

DESKTOP APPLICATION

1. Install the software associated with the product purchased.
    a. Software can be found on our website at: **https://www.larsonelectronics.com/download/acms.zip**
2. After software is downloaded, enter login details.
    a. Credentials should be default settings.
        i. User: admin
        Password: Ch@ngeMeN0W
        ii. We recommend after logging in for the first time to change the login credentials from the default settings.
3. The system is now ready for live viewing See detailed NVR instructions for more details.

MOBILE APP — Alibi Witness 3.0

1. Download the mobile app, Alibi Witness 3.0, from your smart phones app store, or use a third part camera app of your choice.
2. Add your product to the app using the IP Address and Port as well as the User Name and Password
    a. Login credentials should be the default settings, or settings you previously set up if you've logged into the unit using a separate method prior.
        i. Default settings are:
        User: admin
        Password: Ch@ngeMeN0W
3. The system is now ready for live viewing See detailed NVR instructions for more details.

Embedded Network Video Recorder Firmware V4.1.50 User Manual



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

NVR-POE SERIES
181116

About this manual

This user manual applies to all Larson 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/I{P 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 Larson NVR, please contact your vendor.

LEGAL NOTICE

Products are designed to meet safety and performance standards with the use of specific Larson 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 Larson video recorders is expressly prohibited.

Larson Electronics 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.

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.

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

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 ***admin*** 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

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 confliction, 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 UPnPTM
- Support access by Larson 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

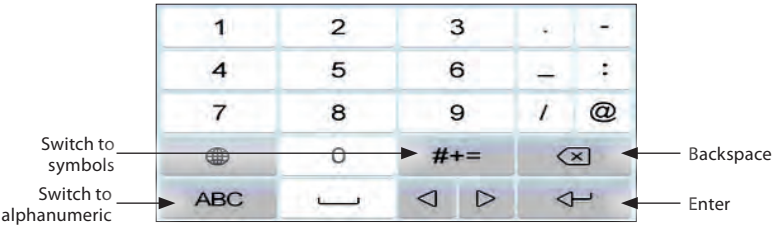
- Alarm and exception information can be sent to the remote host
- Remotely start / stop recording
- Remotely start / stop alarm output
- Remote PTZ control
- Remote JPEG capture
- Virtual host function to access and manage the IP camera directly
- Two-way audio and voice broadcasting
- Embedded Web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

1.1 Soft keyboard

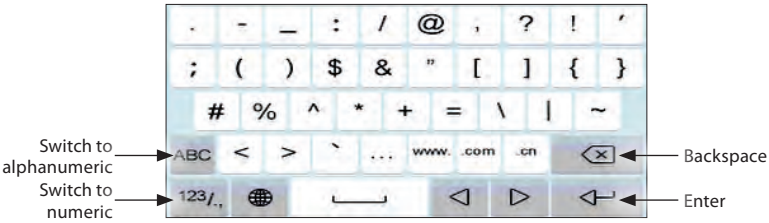
One of two on-screen keyboards appears when you click in a field that accepts a entry, such as a password or name or a numerical value. A third keyboard which includes symbols can also be opened while in the numeric keyboard. The alphanumeric keyboard is shown in the following picture. Some control keys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

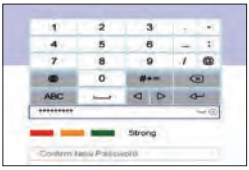
2.1 System activation

1. Power on the NVR. Normally, an Larson 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 loose 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 loose 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, an **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).

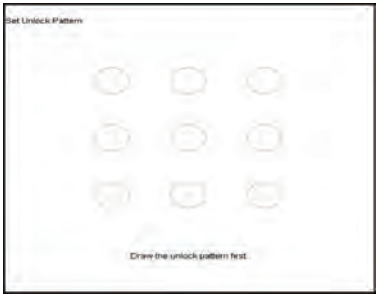
a. In the **GUID Import/Export** window, open the **Device Name** drop down list and then select the device you where you want to save the GUID file. If a list of directories appear, click on the directory you prefer (in the window shown below, the first directory was selected), and then click **Export**.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

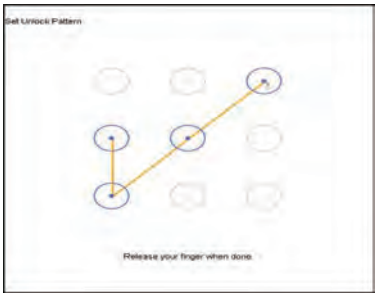


b. After the export operation completes, remove the flash drive from the NVR and store it in a secure location.

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.

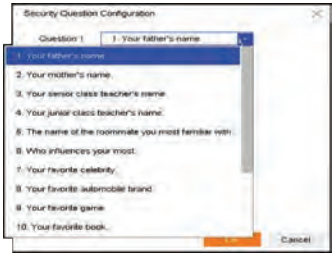




Security Question Configuration: If you selected this option and the **Note** window shown above is still open, click **OK** to close the **Note** window. Then:

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 ad 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.



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.



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 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. **Larson 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.

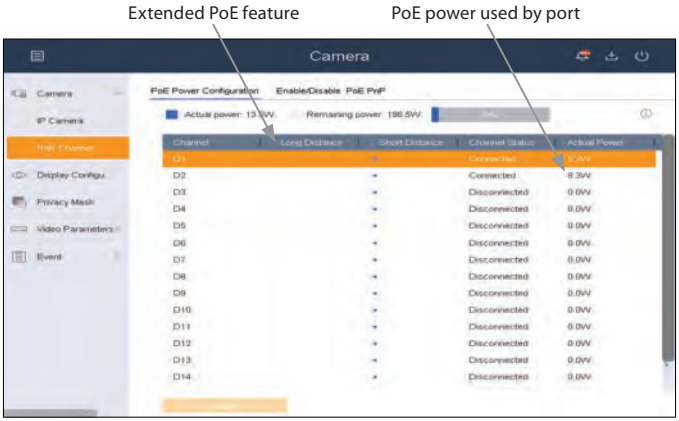
To save your settings and exit the configuration Wizard, click **Finish**. Click **Previous** to return to an another Wizard menu. After clicking Finish, the Live View window will open.



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 featuere, 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.

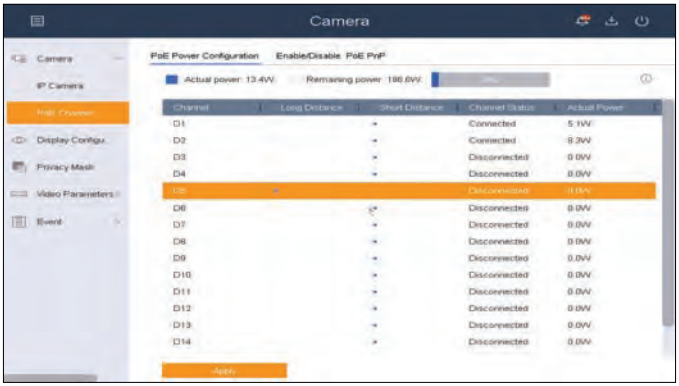


The display shows the real power consumed and the remaining power available for other ports.

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.



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

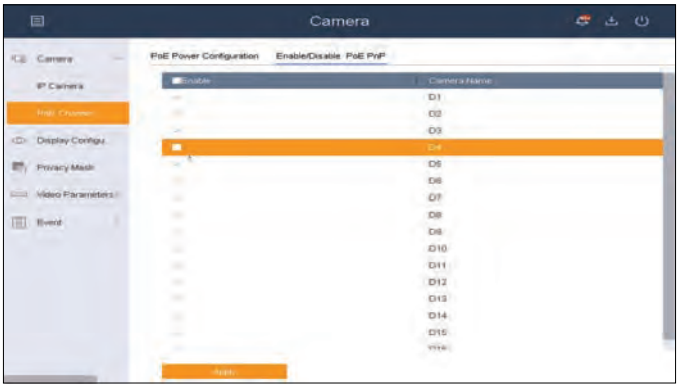
Disable PoE power on a channel

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.



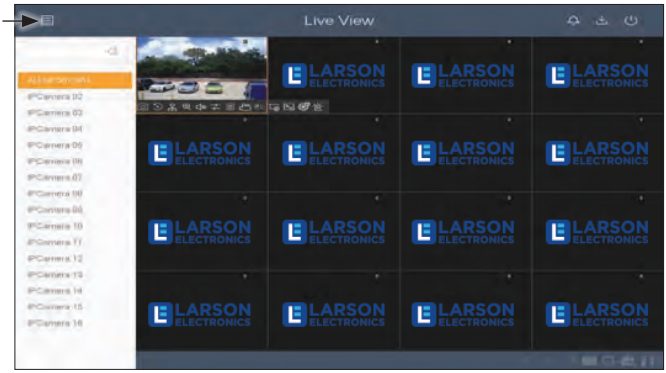
2. Click on the channel where you want to disable PoE, and then click the **Enable** box to **uncheck** it.

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. An 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

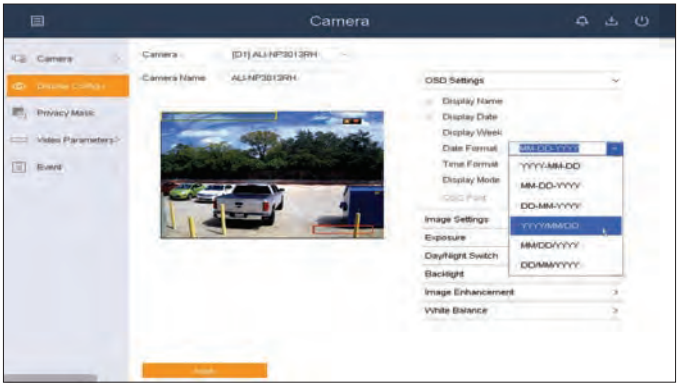
NOTE *Options shown in the menu for cameras may change based on the model of camera used.*

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 Configu** in the left frame.



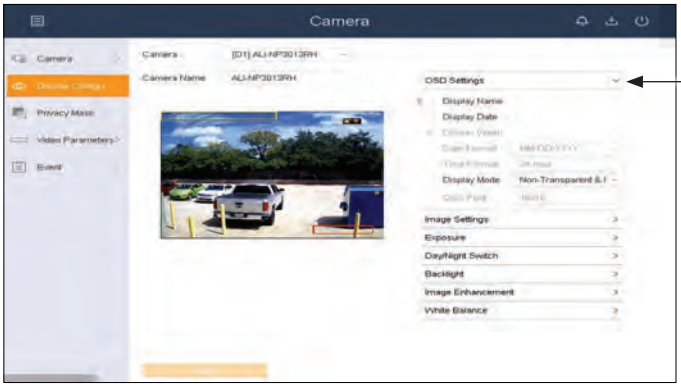
2.5.1 Camera OSD setup

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.

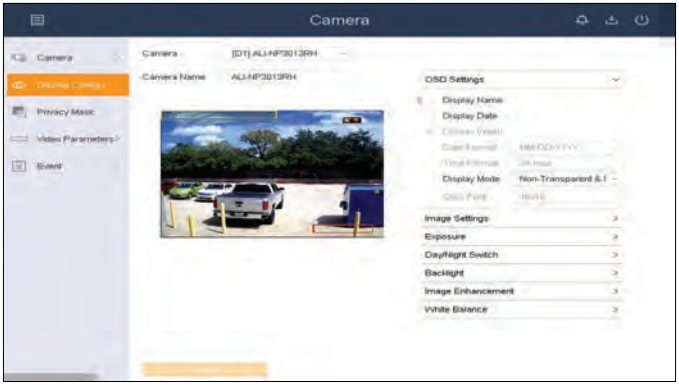
NOTE

- *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.*
- *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 Configu**ration menu, click the **expand-more** icon on the **OSD Settings** line to open the OSD menu.



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 Configu**ration 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 Configu**ration menu, click the **expand-more** icon on the **Exposure** line.

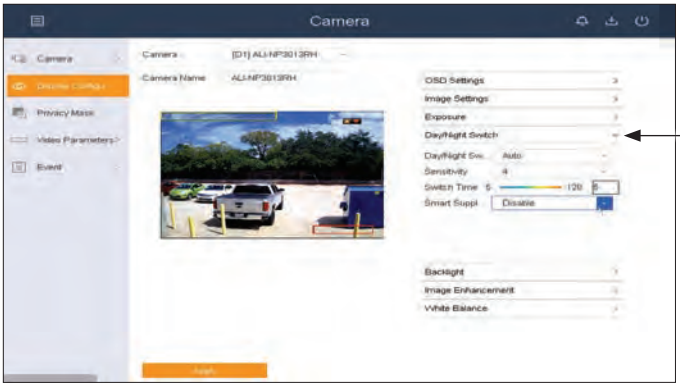


2. In the **Camera** field drop down list, select the camera you want to configure. In the example above, **[D1]IPCamera 01** is selected.
3. Open the **Exposure Time** drop down list, and select the optimal exposure time for the camera (1/100000 to 1 second). Larger exposure time produces a brighter 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 Configu**ration 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.

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

2.5.5 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.

1. In the **Display Configu**ration menu, click the **expand-more** icon on the **Backlight** 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 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**.
   a. If you selected **CLOSE**, you can set WDR ON or OFF, and HLC ON or OFF.
   b. 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 Configu**ration 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 Configu**ration menu, click the **expand-more** icon on the **White Balance** line.

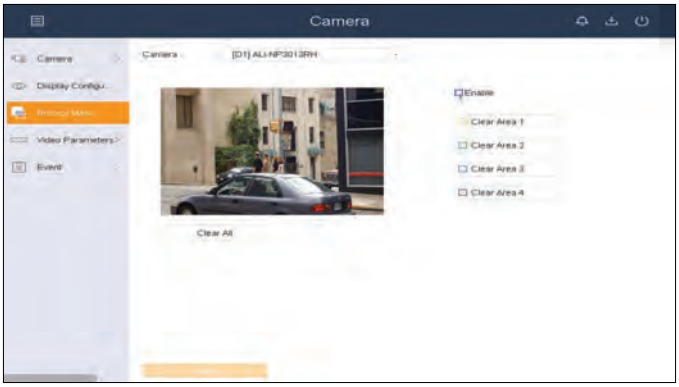


2. In the **Camera** field drop down list, select the camera you want to configure. In the example above, **[D1]IPCamera 01** is selected.
3. Open the **White Balance** drop down list and select the mode that produces the best color.
   a. If you select **MWB** (Manual White Balance), use the sliders 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.

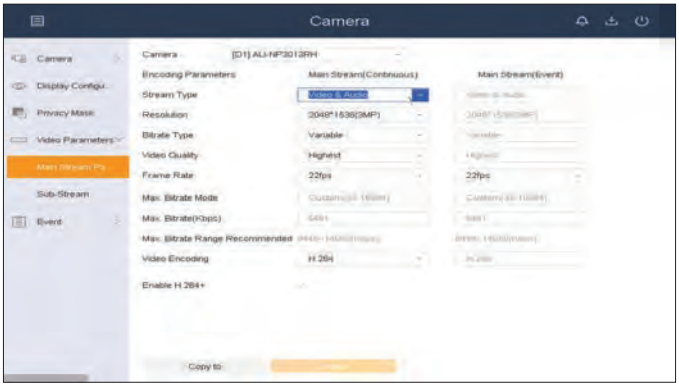
2.5.9 Camera Video Parameters

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. 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.

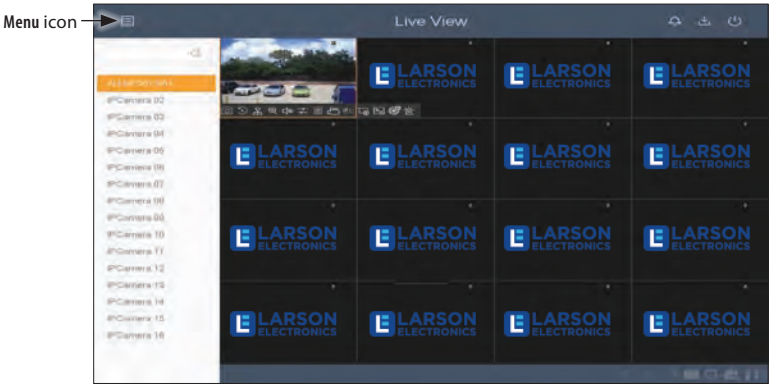
SECTION 3
Event setup

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 will 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 menus.

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.



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.

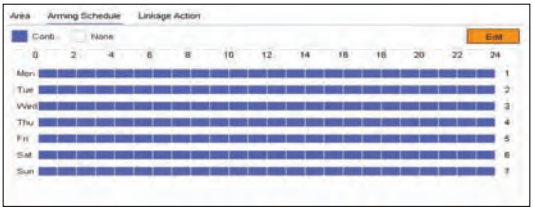
f. Adjust the **Sensitivity** slider as needed to detect the motion of objects moving through the zones. When motion is detected in a segment of the grid, the segment is filled with red. See the screen above.

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.

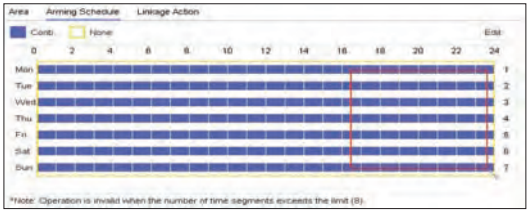
h. In the Edit menu, click **OK** to return to the **Arming Schedule**. Changes you saved will be reflected in the schedule.

Arming Schedule "graphical" method

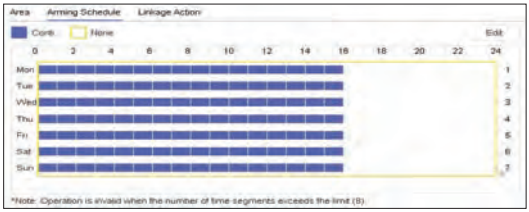
The graphical editing method is used by clicking either **Continuous** or **None**, then dragging a box over the areas of the schedule when you want to either enable or disable arming. For example, to disable arming in an area of the schedule:

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.



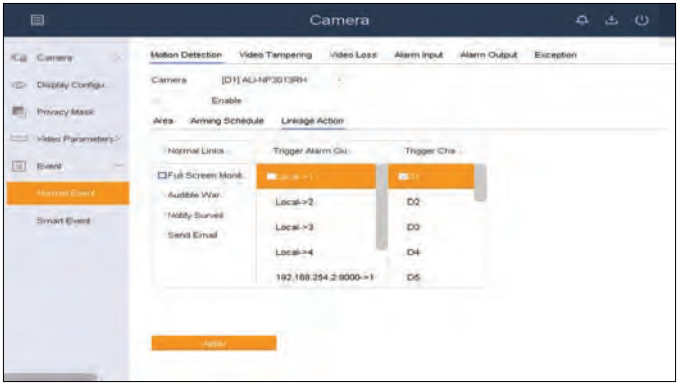
c. Release the mouse button. The part of the schedule you selected is now disarmed.



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

Linkage Action

5. Click the **Linkage Action** tab.

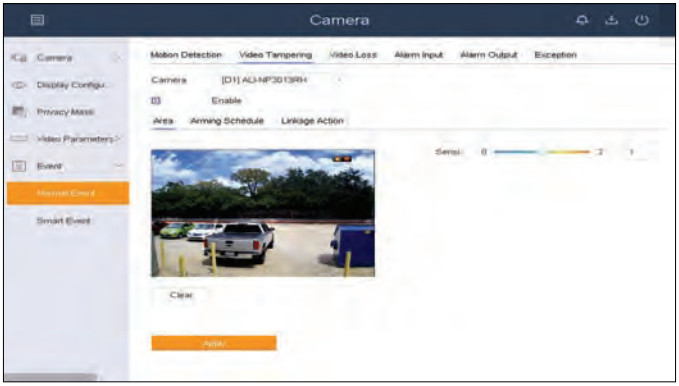


6. In the **Linkage Action** menu, check the boxes for the actions you want to occur when event is detected.
7. Click **Apply** to save your settings.
8. Repeat steps **1** through **7** above for each camera on your surveillance system.

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:

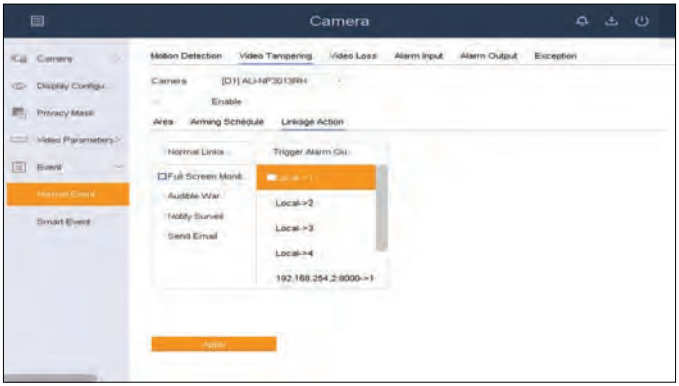
1. Open the Video Tampering menu. Go to **Menu | Camera | Event | Normal Event | Video Tampering**.



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



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

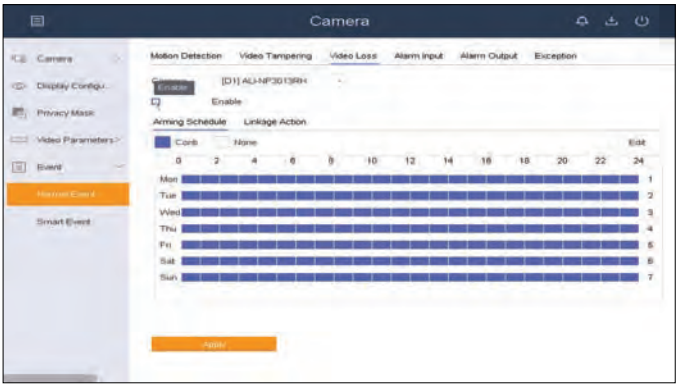


8. In the **Linkage Action** menu, check the boxes for the actions you want to occur when the event is detected.
9. Click **Apply** to save your settings.
10. Repeat steps **1** through **9** above for each camera on your surveillance system.

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:

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



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.

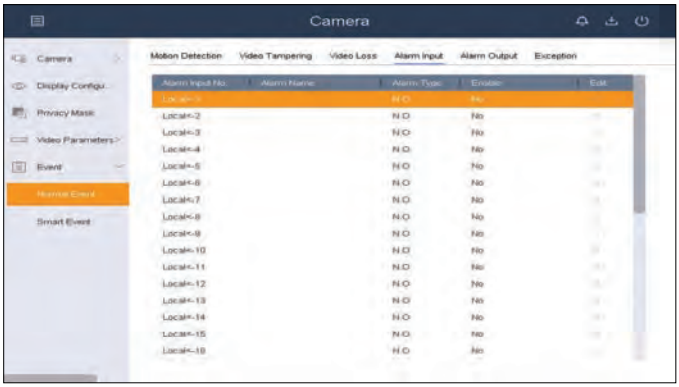


5. In the **Linkage Action** menu, check the boxes for the actions you want to occur when the event is detected.
6. Click **Apply** to save your settings.
7. Repeat steps **1** through **6** above for each camera on your surveillance system.

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**.



2. 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.



3. In the **Alarm Name** field, enter a common name for the alarm.
4. Open the **Type** field, and select either **N.O.** for a Normally Open alarm switch, or **N.C.** for a Normally Closed alarm switch.
5. 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.

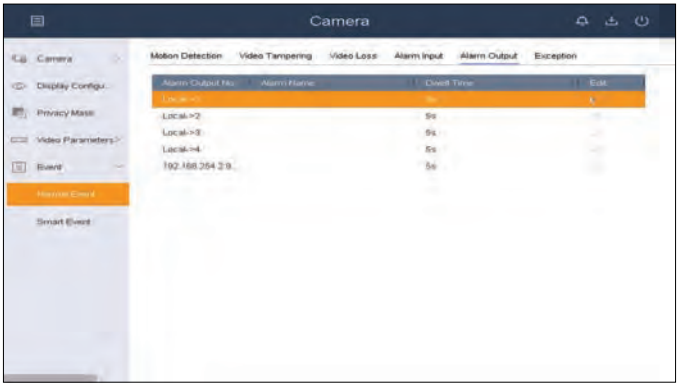
6. Click the Close icon (✕) in the upper right corner of the **Edit** screen to return to the Alarm Input menu.

7. Repeat steps **1** through **6** above for each alarm input on your surveillance system.

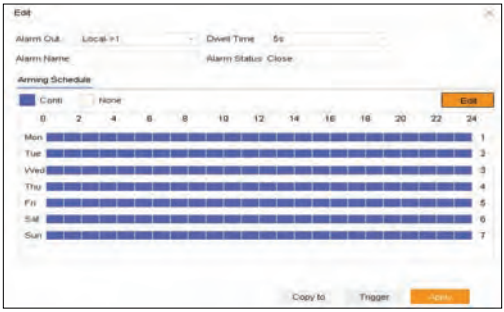
3.1.5 Alarm Output configuration

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**.



2. 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.



3. In the **Alarm Name** field, enter a common name for the alarm.
4. 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**.
5. Click the **Arming Schedule** tab. To configure the arming schedule, refer to the procedure in "3.1.1 Camera Motion Detection" on page 29.
6. Click **Apply**, and then click **Copy to** and use the on-screen menu to use the same schedule for other alarm outputs.
7. Test the alarm output functionality by clicking **Trigger** to activate the alarm, and then **Clear** to deactivate it.
8. Click the Close icon (✕) in the upper right corner of the **Edit** screen to return to the Alarm Input menu.
9. 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:

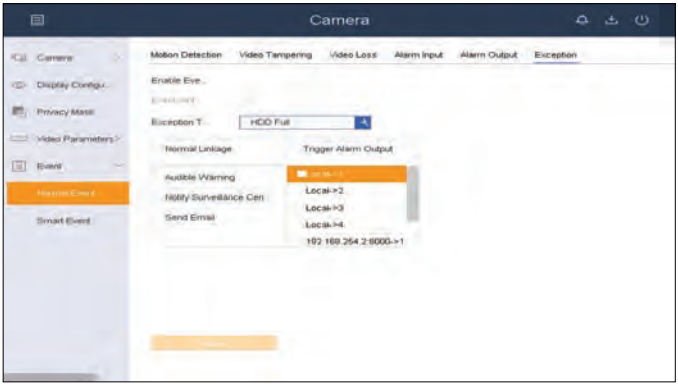
- **HDD Full**: The HDD is full.
- **HDD Error**: Writing HDD error or unformatted HDD.
- **Network Disconnected**: Disconnected network cable.
- **IP Conflicted**: Duplicated IP address.
- **Illegal Login**: Incorrect user ID or password.
- **Record/Capture Exception**: No space exists for saving recorded 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 Larson 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:

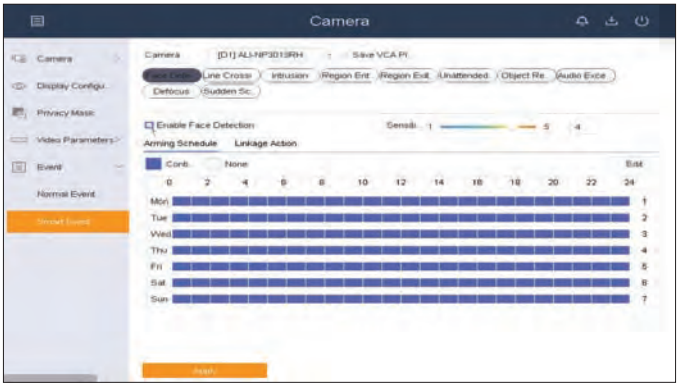
- **Face Detection** - Detects when a face appears in the field of view.
- **Line crossing detection** - You can specify the endpoints of an virtual line in the video image and then detect if something crosses the line from one side to the other (side A to B), vice versa (side B to A) or either way. 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 an 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.

- **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:

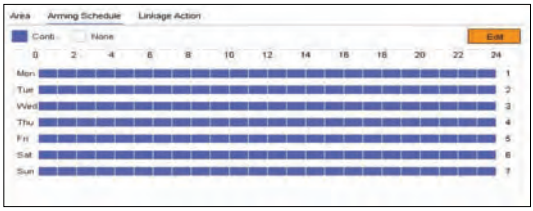
1. Open the Face Detection menu:
   a. Go to **Menu | Camera | Event | Smart Event**



   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.

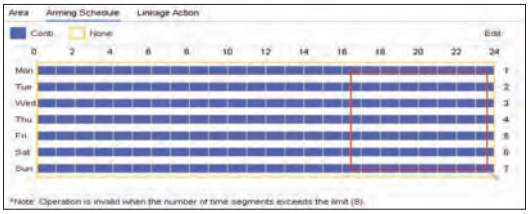
h. In the Edit menu, click **OK** to return to the **Arming Schedule**. Changes you saved will be reflected in the schedule.

Arming Schedule "graphical" method

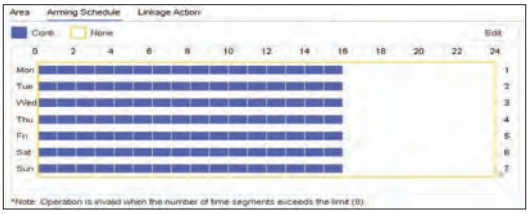
The graphical editing method is used by clicking either **Continuous** or **None**, then dragging a box over the areas of the schedule when you want to either enable or disable arming. For example, to disable arming in an area of the schedule:

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.



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.

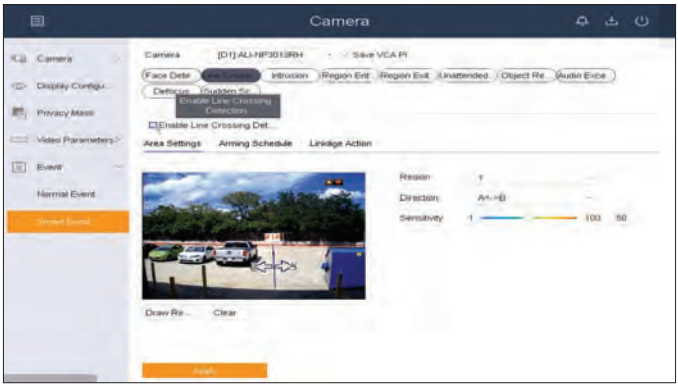
3.2.2 Line Crossing detection

With Line Crossing detection you can specify the endpoints of an 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**

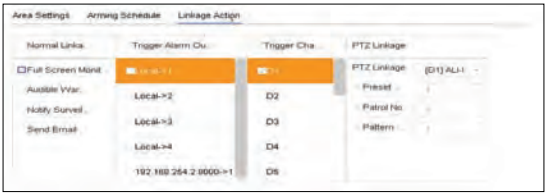


   b. Open the drop down list on the camera line, then select the camera you want to configure.
   c. If the Line Crossing option appears in the VCA list at the top of the screen, click on it to configure this feature.



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).

4. In the **Area Settings** tab:
   a. 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.
   b. 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.
   c. Set the **Sensitivity** slider as needed to detect objects crossing the line. This adjustment may require some testing.
   d. 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.
   e. 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.
   f. Click **Apply** to save your settings.
   g. 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.
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.

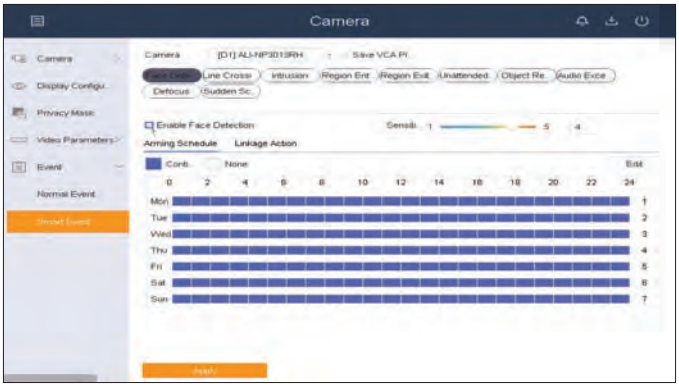


7. In the **Linkage Action** menu, check the boxes for the actions you want to occur when the event is detected.
8. Click **Apply** to save your settings.
9. Repeat steps **1** through **8** above for each camera on your surveillance system as needed.

3.2.3 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:

1. Open the **Intrusion 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 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.

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.

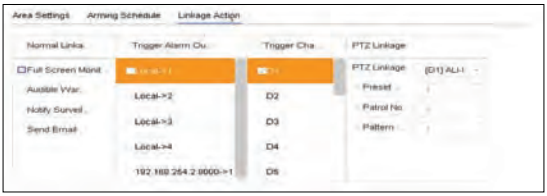


g. Click **Apply** to save your settings.

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.

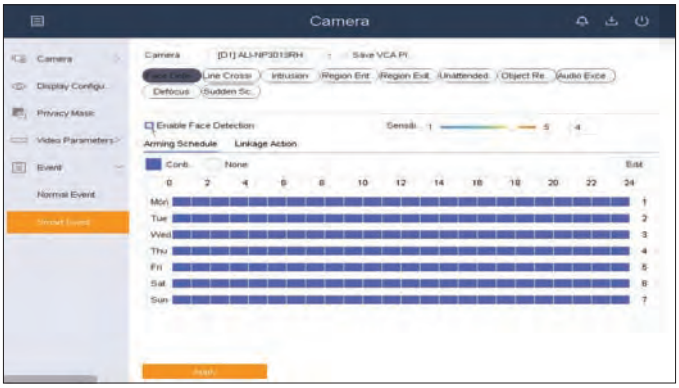
9. Repeat steps **1** through **8** above for each camera on your surveillance system as needed.

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:

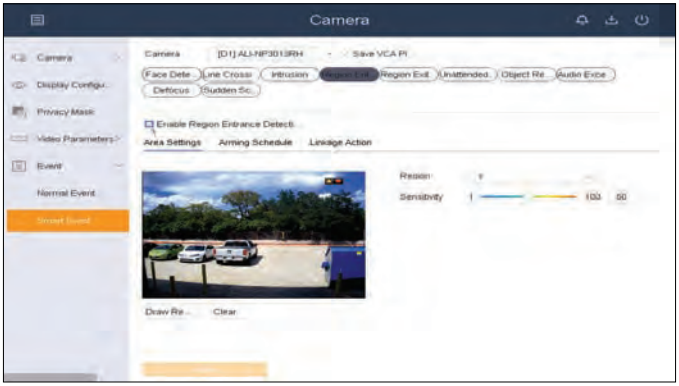
1. Open the **Region Entrance Detection** menu:

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.

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.

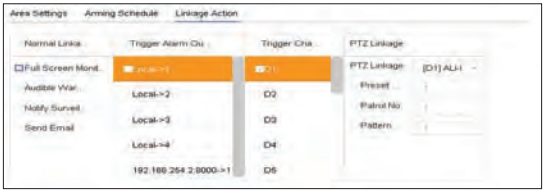


e. Click **Apply** to save your settings.

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.

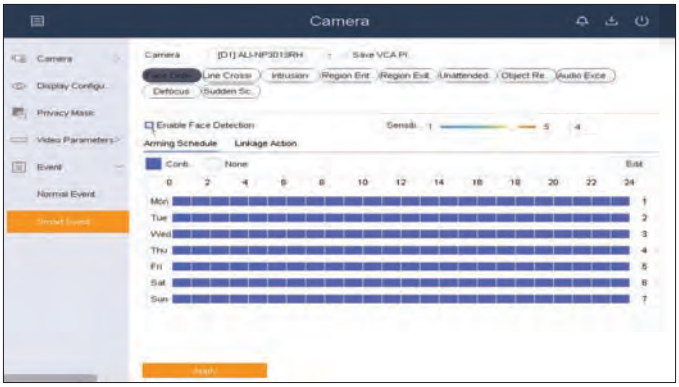
9. Repeat steps **1** through **8** above for each camera on your surveillance system as needed.

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:

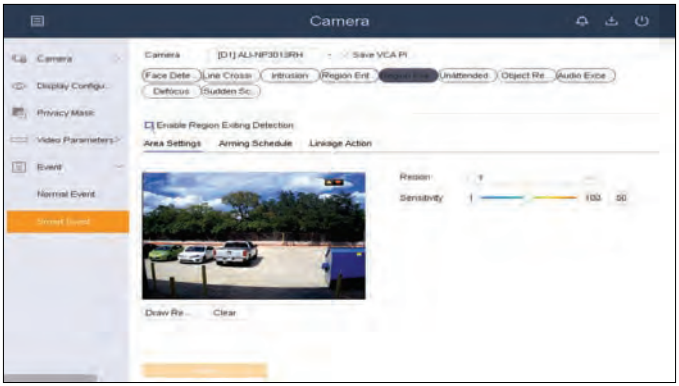
1. Open the **Region Entrance Detection** menu:

   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.

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

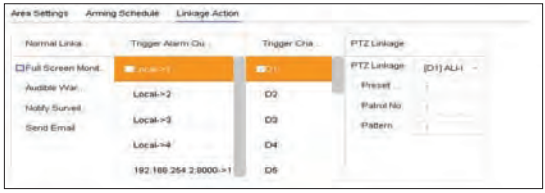


e. Click **Apply** to save your settings.

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.

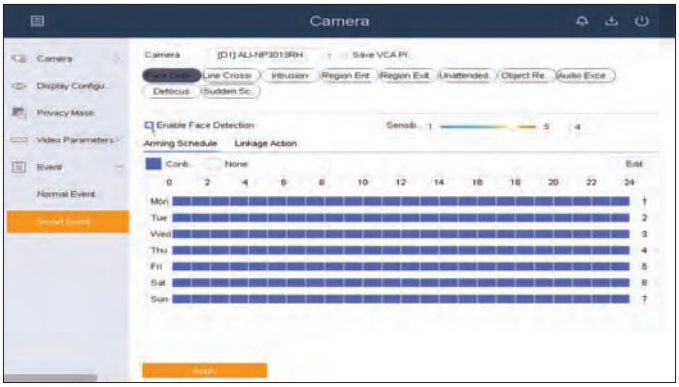
9. Repeat steps **1** through **8** above for each camera on your surveillance system as needed.

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:

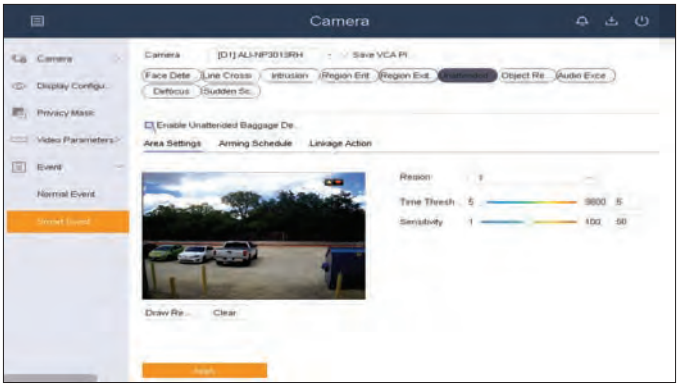
1. Open the **Region Entrance Detection** menu:

   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.

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.

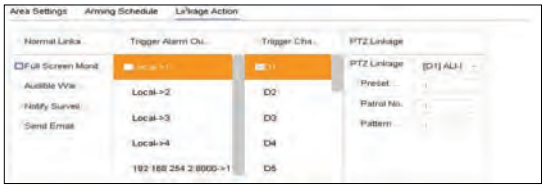


f. Click **Apply** to save your settings.

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.

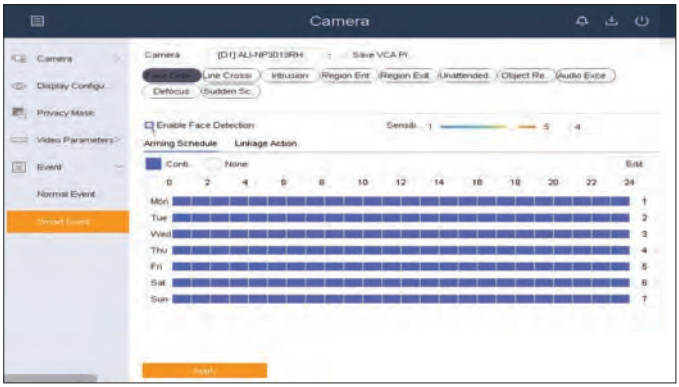
9. Repeat steps **1** through **8** above for each camera on your surveillance system as needed.

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:

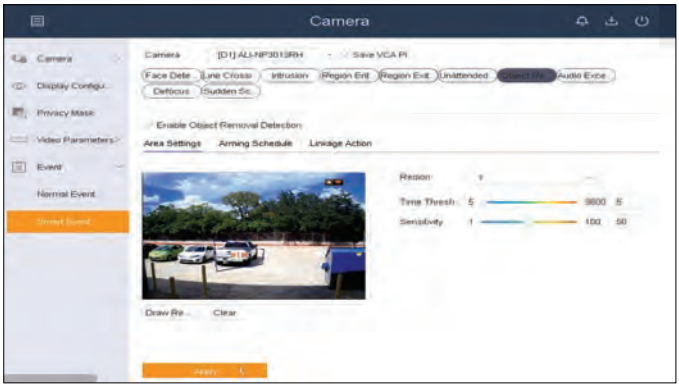
1. Open the **Region Entrance Detection** menu:

   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.

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.

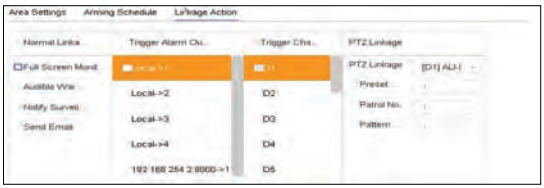


f. Click **Apply** to save your settings.

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.

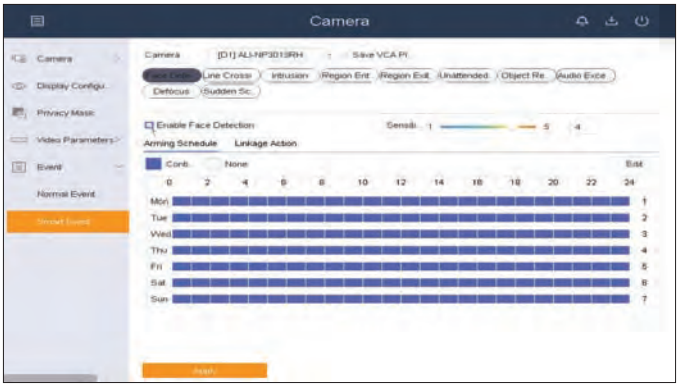
9. Repeat steps **1** through **8** above for each camera on your surveillance system as needed.

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:

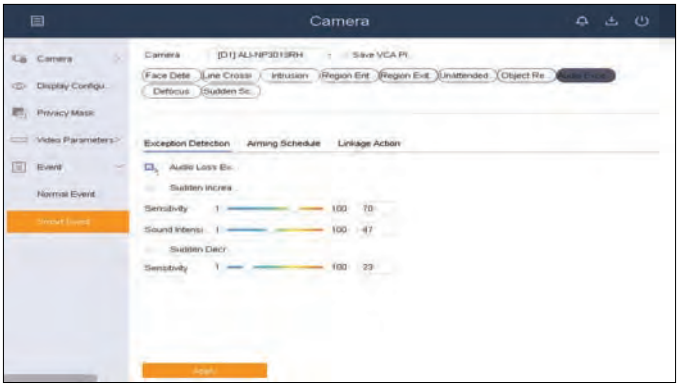
1. Open the **Region Entrance Detection** menu:

   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:

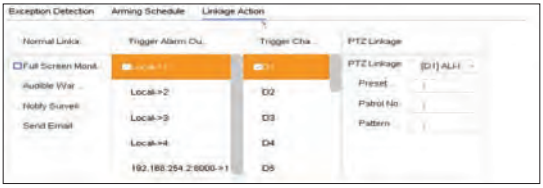
      i. Set the **Sensitivity** slider to set the high sound level minimum threshold (may require testing).

      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).

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

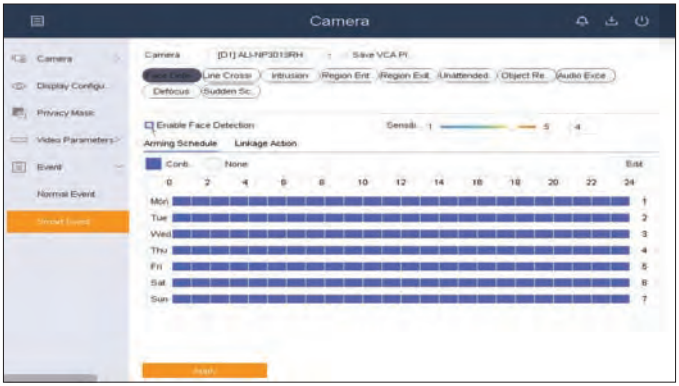


7. In the **Linkage Action** menu, check the boxes for the actions you want to occur when the event is detected.
8. Click **Apply** to save your settings.
9. Repeat steps **1** through **8** above for each camera on your surveillance system as needed.

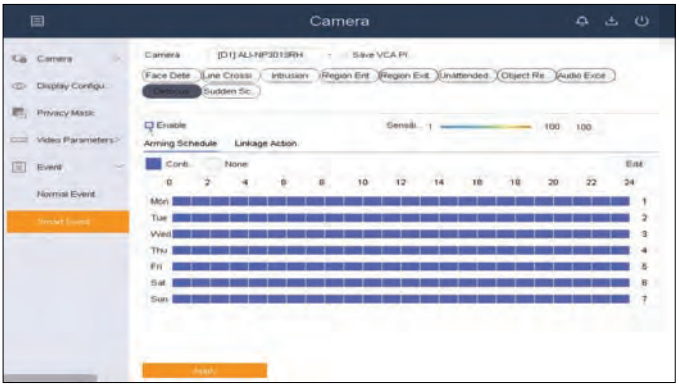
3.2.9 Camera Defocus Detection

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

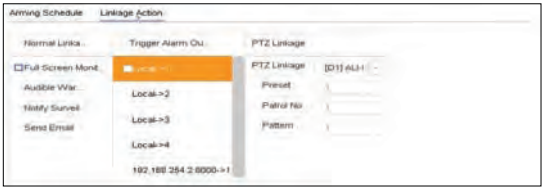
1. Open the **Region Entrance Detection** menu:
   a. Go to **Menu | Camera | Event | Smart Event**



   b. Open the drop down list on the camera line, then select the camera you want to configure.
   c. If the **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.

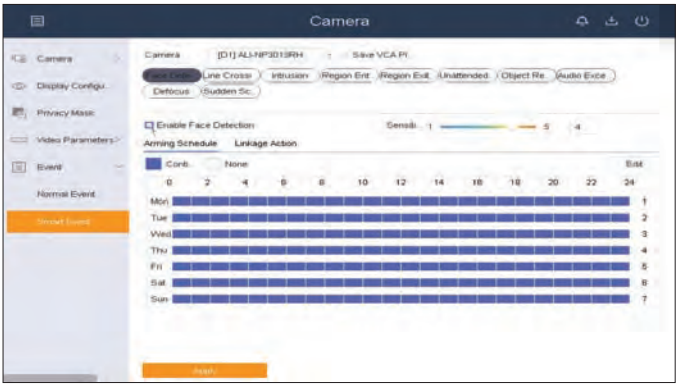


7. In the **Linkage Action** menu, check the boxes for the actions you want to occur when the event is detected.
8. Click **Apply** to save your settings.
9. Repeat steps **1** through **8** above for each camera on your surveillance system as needed.

3.2.10 Camera Sudden Scene Change Detection

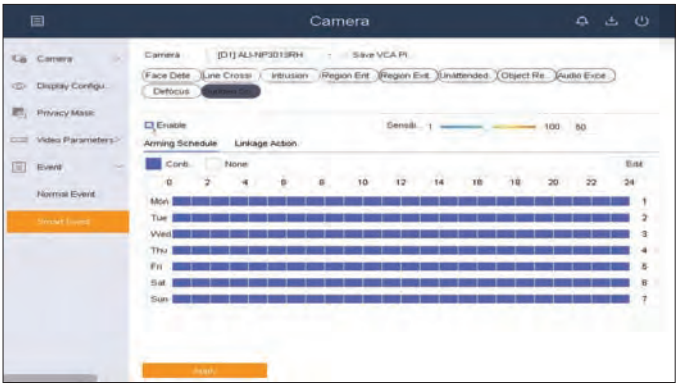
Use Scene change detection to detects the change of surveillance environment affected by an external factor, such as the intentional rotation of the camera. To use Sudden Scene Change Detection:

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

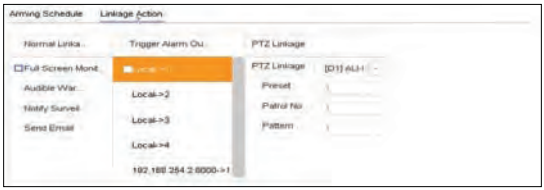


b. Open the drop down list on the camera line, then select the camera you want to configure.

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 screns 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.



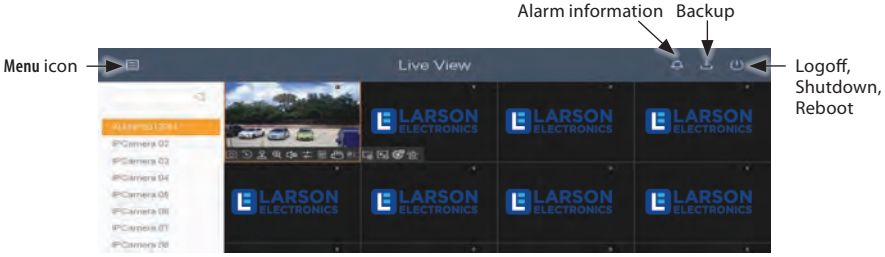
   - If an unlock pattern was not setup during system activation, or you chose to login as a user other than *admin*, a typical login screen will open. Enter your username and password, then click Login.



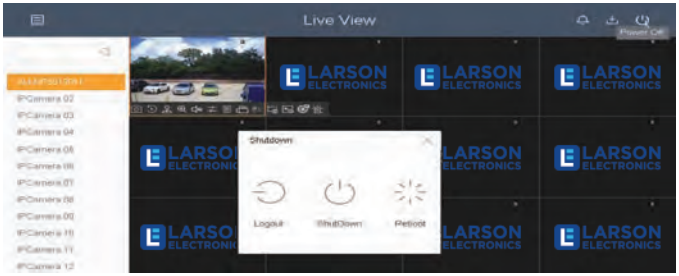
4.2 Shutdown

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.



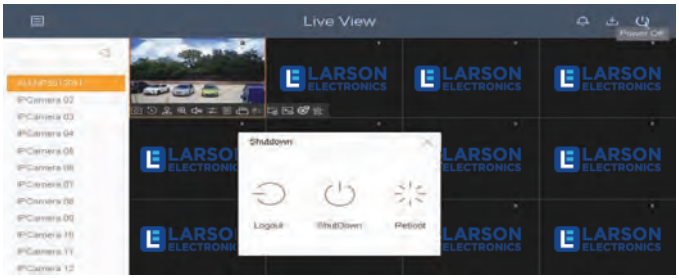
2. Click the **Power Off** icon in the upper right corner, and then click the **Shutdown** icon in the pop-up menu.



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*

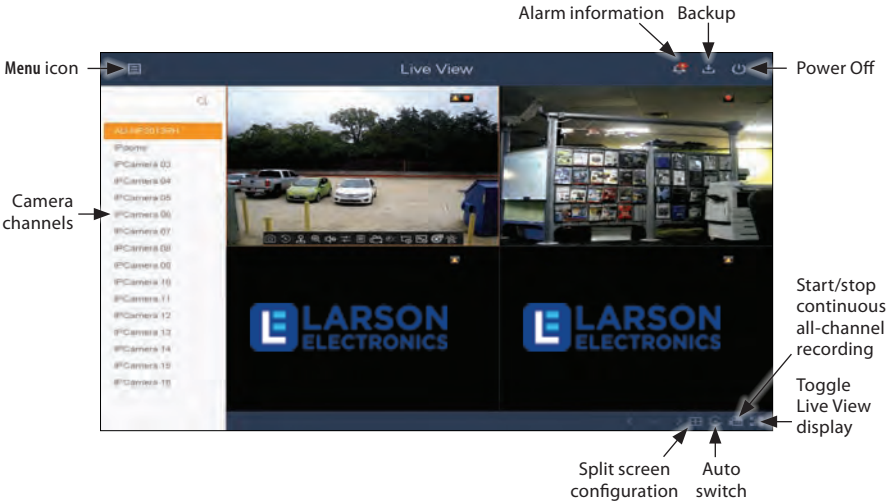
Each camera channel displayed on the Live View screen may contain one, two, or no status icons in the upper-right corner of the viewing frame.

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



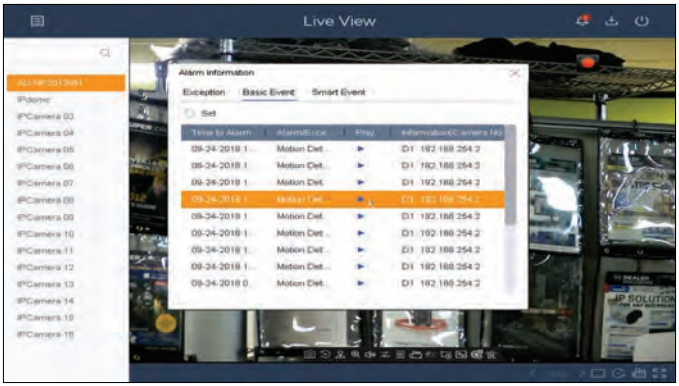
5.1.1 Open Menu screen

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:



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.

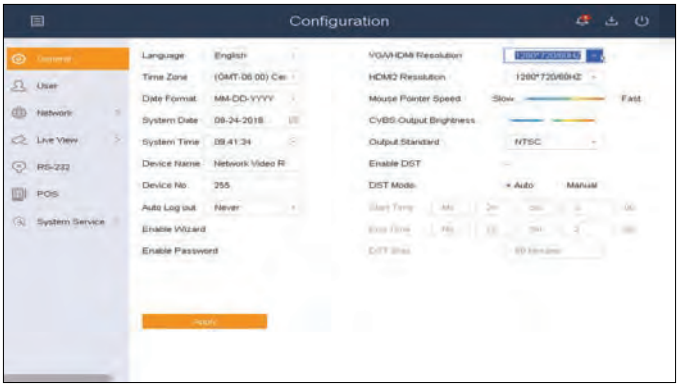
Start and stop continuous recording

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**

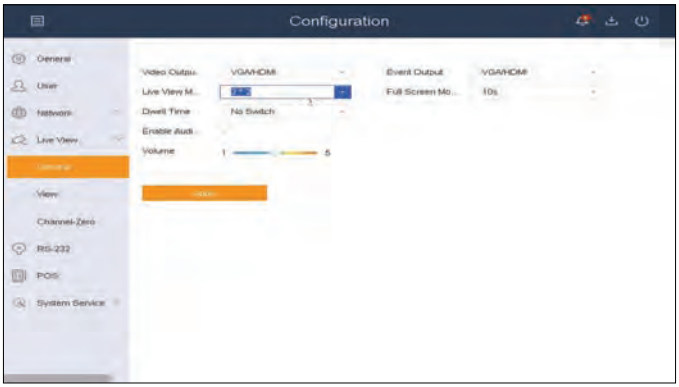


Use the screen above to select the VGA/HDMI and HDMI2 resolutions for the VGA and HDMI monitors you are using, and then click the **Apply** button at the bottom of the screen.

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**

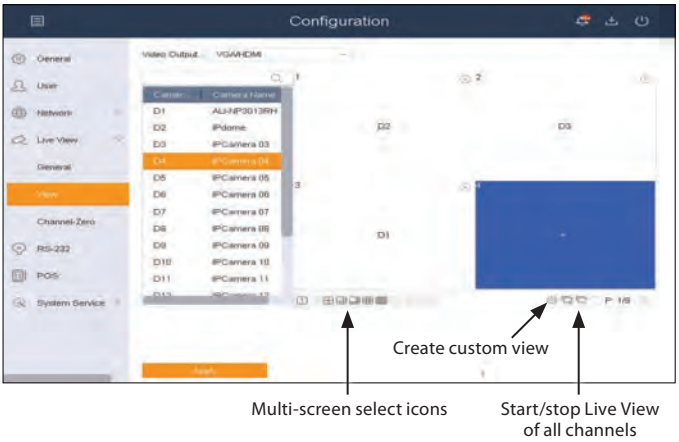


Adjust the settings in the screen as needed:

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

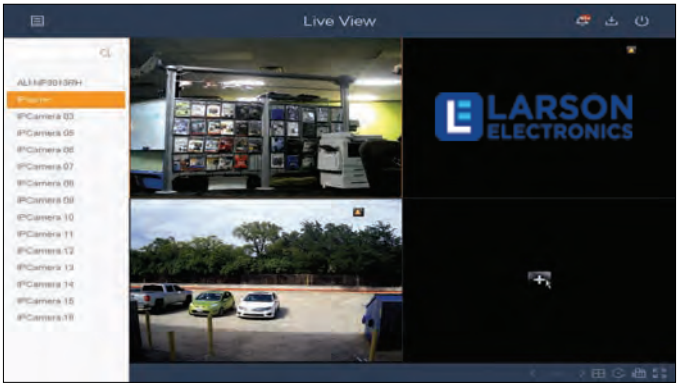
- **Live View Mode**: Designates the display mode (screen split) to be used for Live View. **1 * 1** is a single camera view. Other options are **2 * 2**, **1 + 5**, **1 + 7**, **3 * 3**, etc. Options depend on the number of channels supported by the recorder.
- **Dwell Time**: The time in seconds to 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 screens (D1 or D2 or D3 ..), then double-click the camera in the list on the left that you what 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 sown 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.*

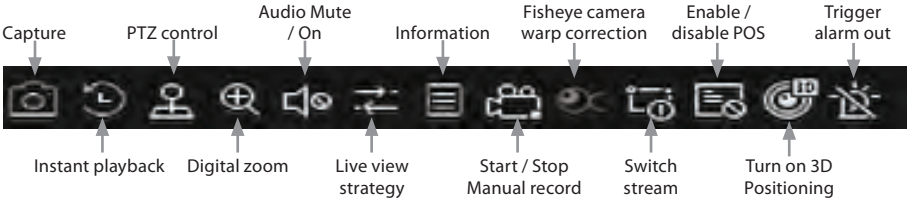
5.4 Live View Status icons

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.

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.

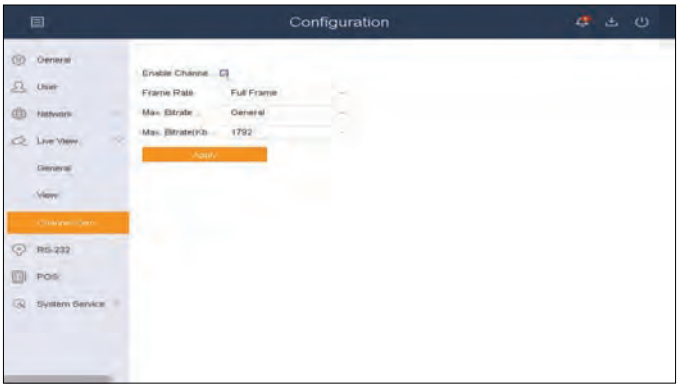
Switch to Sub-Stream: Hover the mouse over this icon to play the sub-stream video. Repeat this action to return to the Main stream.

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.

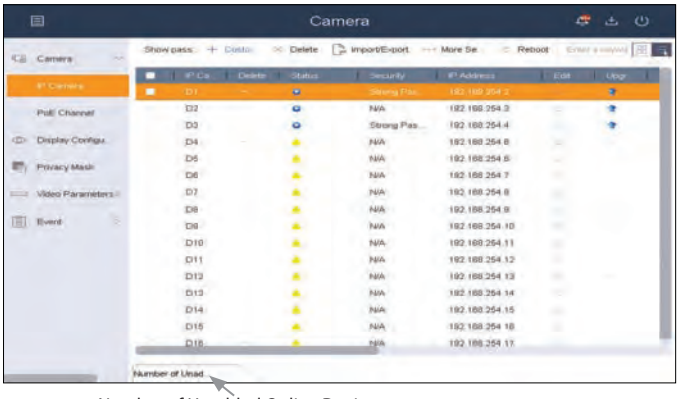
NOTE *For a lists IP cameras compatible with your NVR, refer to: "APPENDIX C NVR Compatible Cameras" on page 208.*

Use the following guidelines to add a camera that was discovered on the LAN to the NVR. In the example below, a Larson camera discovered on the LAN at IP address 192.168.3.3 will be added to NVR channel D4.

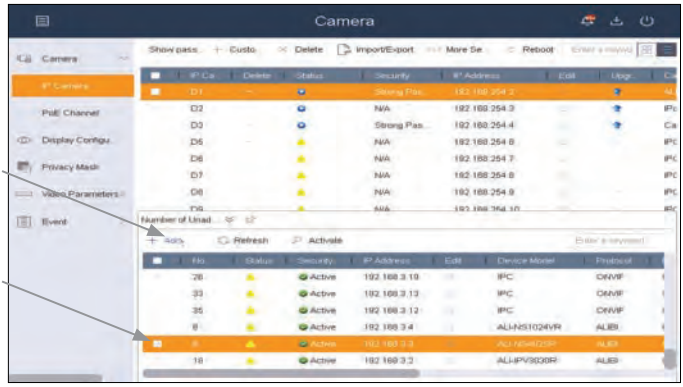
1. Open the IP Camera menu. Go to **Menu | Camera | IP Camera**.



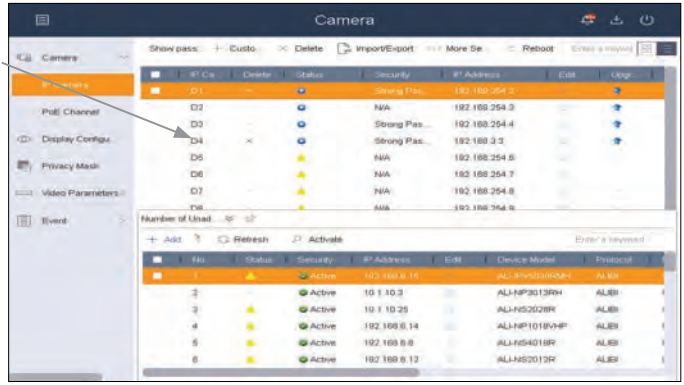
2. Click the **List** button in the upper right corner.



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.



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.

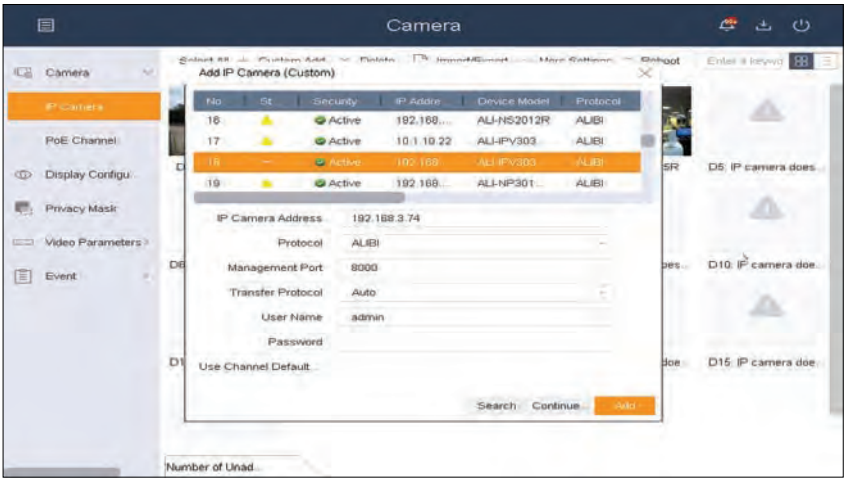


c. Repeat sub-steps **a** and **b** above to add additional cameras. NVRs limit the number of network cameras you can add.

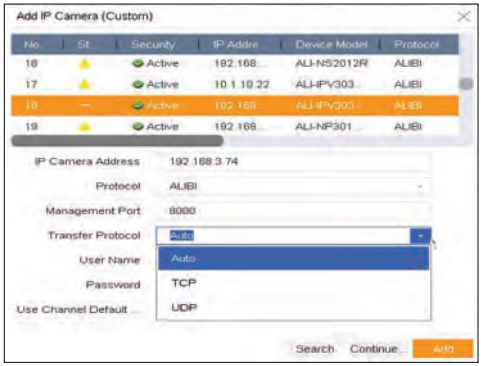
5.7.1 Custom Add IP Camera

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 Larson cameras with default setup parameters. To use this feature:

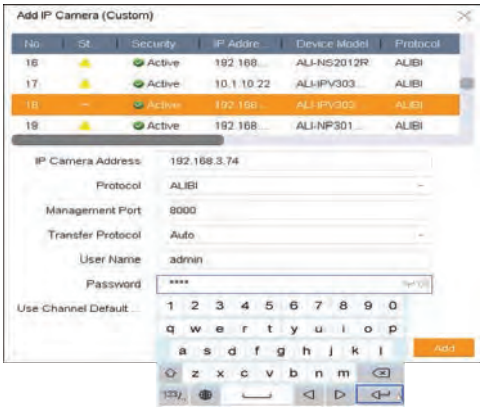
1. Open the IP Camera menu. Go to **Menu | Camera | IP Camera**.
2. Click the **Custom Add** button at the top of the window. The upper portion of the **Add IP Camera (Custom)** popup window lists network cameras that are accessible from the NVR.



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.

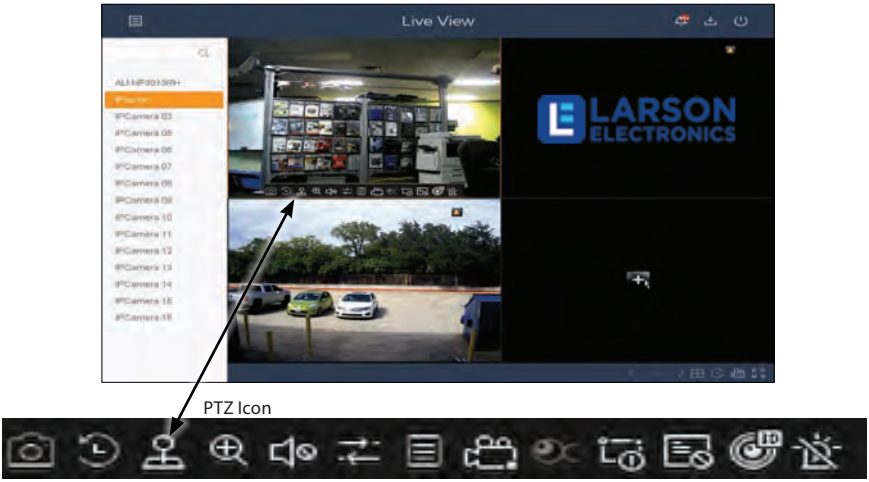


8. Click **Add** to save your settings and connect the camera to the recorder.

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 ✕ in the upper right corner or right click on the video window to return to the **Live View** screen.

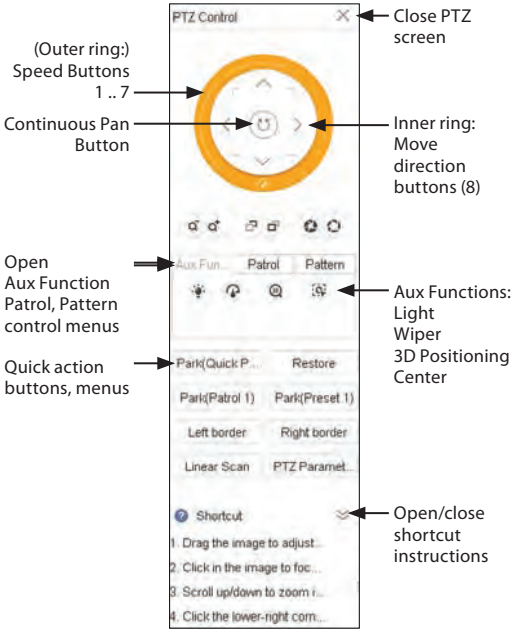
6.1.1 Pointing the camera

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.



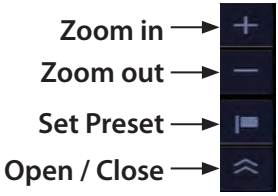
Feature of the PTZ control panel include:

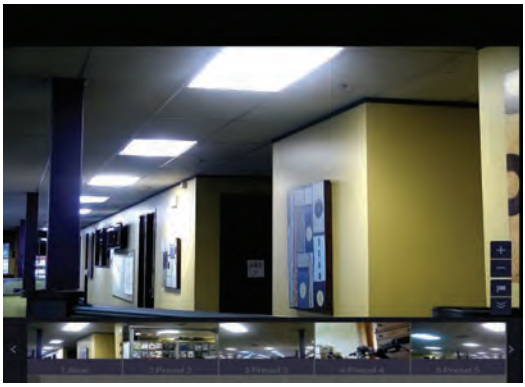
- **Outer ring speed buttons**: Click one of the seven (7) buttons to set the speed at which the camera moves when you click one of the eight (8) direction buttons.
- **Continuous pan button**: Click to start / stop continuous pan to the right.
- **Open Aux Function, Patrol, Pattern control menus**: 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 ✕ 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.





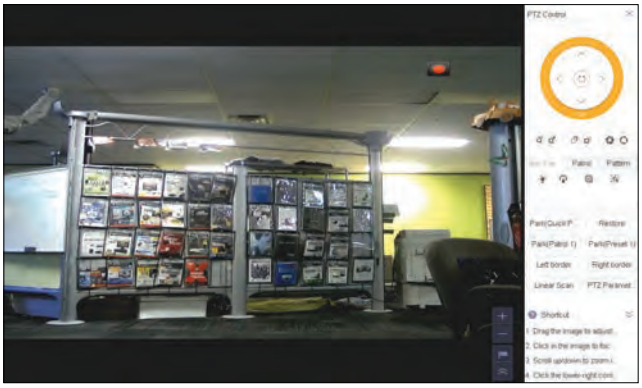
PTZ view with Preset thumbnails open

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.



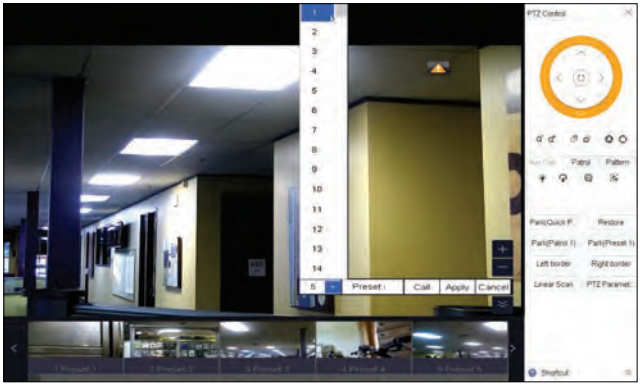
2. Click **OK** to lose the PTZ Control Wizard.

6.2.1 Setting Presets

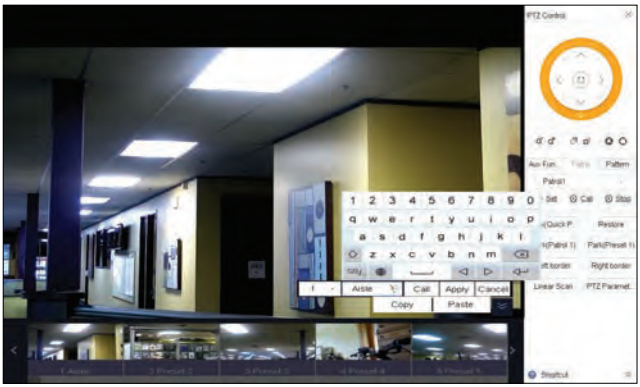
A Preset is a pre-configured setting of a PTZ camera that usually includes, it's direction, zoom, iris setting and focus, and may include other settings. Follow the steps to set the Preset location which you want the PTZ camera to point to when an event takes place. A PTZ camera has up to 255 presets,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

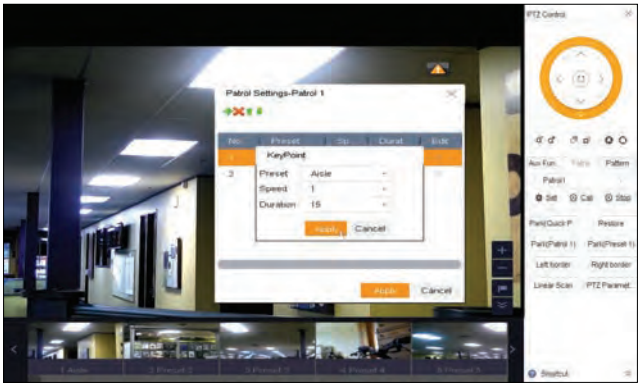
1. Click the **Patrol** tab in the PTZ Control Panel.

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.



4. 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:

a. Open the **Preset** drop down list, and select the first camera view you want the patrol to move to.

b. Open the **Speed** drop down list, and select the speed at which you want the camera to move there.

ii. 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.

c. Click **Apply**. An entry will appear in the Patrol Settings list for the KeyPoint you created.

d. 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.

5. When finished defining all the KeyPoints for the Patrol, click **Apply** in the Patrol Settings menu to save your settings.

6. Click **Cancel** to close the Patrol Settings menu.

Editing a patrol

In the Patrol Settings menu for the patrol you created:

1. Click the KeyPoint you want change.

a. To change the Preset number:

i. Click the Edit icon in the right column.

ii. Open the **Preset** drop down list, then select the preset you want to assign to the KeyPoint.

iii. Open the **Speed** drop down list, then select the speed at which you want to move to the preset.

iv. 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 **Call**ed, the pattern will execute continuously until it is stopped.

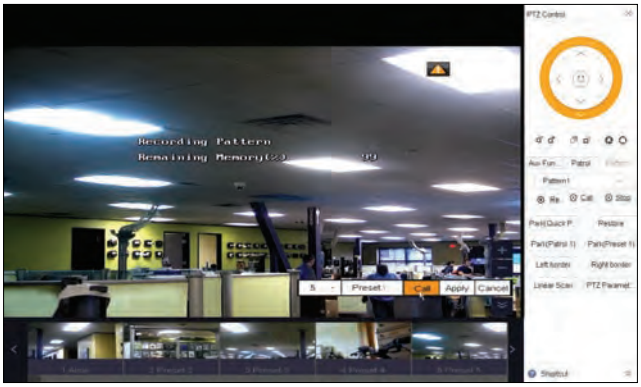
You can record only one pattern (Pattern 1). During the recording, an on-screen display shows how much memory allocated for the recording remains.

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

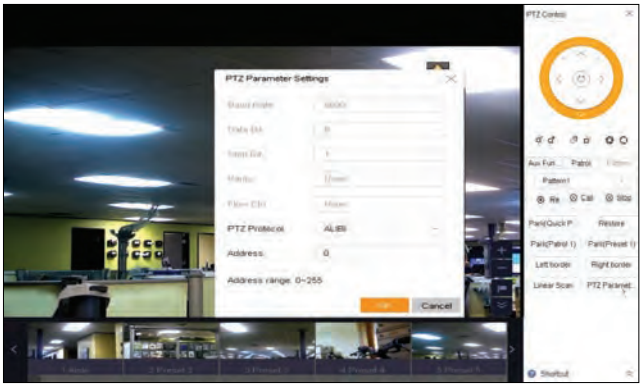
Use Linear Scan to scan the field of view back and forth along a linear path between a "left limit" point and a "right limit" point. To use this feature, you must first define the Left Limit and Right Limit:

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 Larson recorder supports only plain text and XML data through the remote listening port.

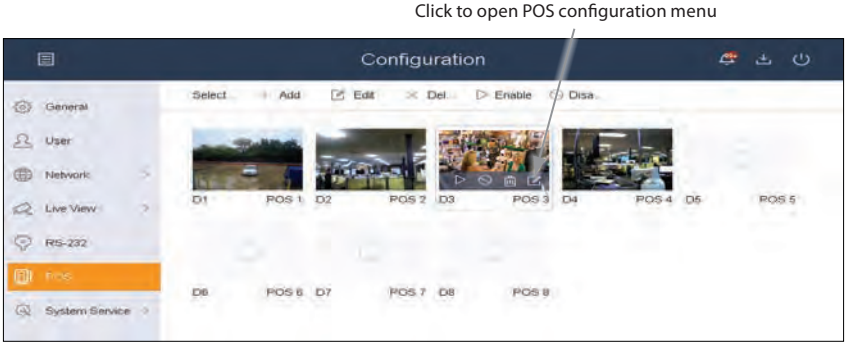
Setting up POS is a two step process, performed in two different NVR menus:

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

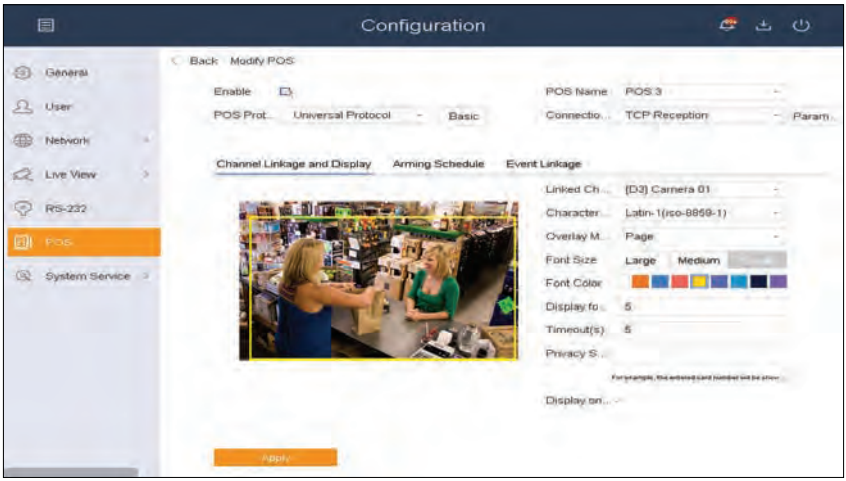
7.1 Assign POS data to a camera

Do the following:

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



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



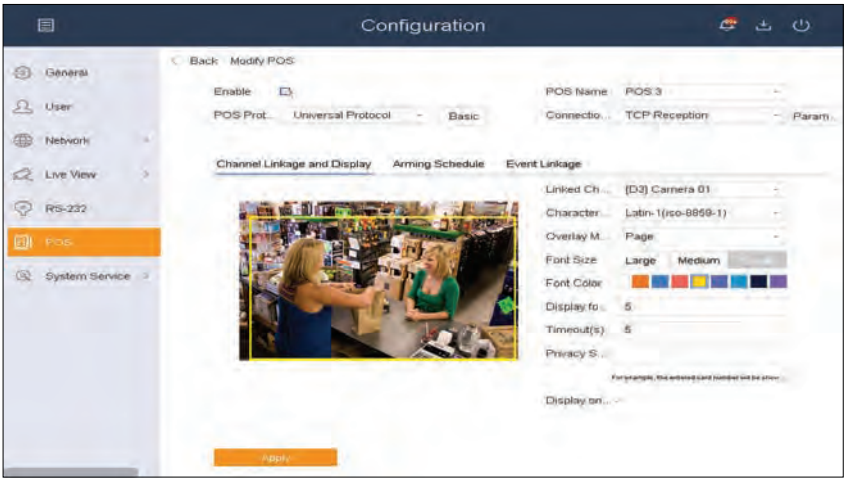
Notice in the mapping shown above, channel D3 is assigned to pos 3, etc.. by default. This indicates that data from POS assigned to POS 3 will be shown over the image in Channel D3. You can change this configuration, if needed, by selecting the POS identifier, and then selecting the cannel to assign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

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

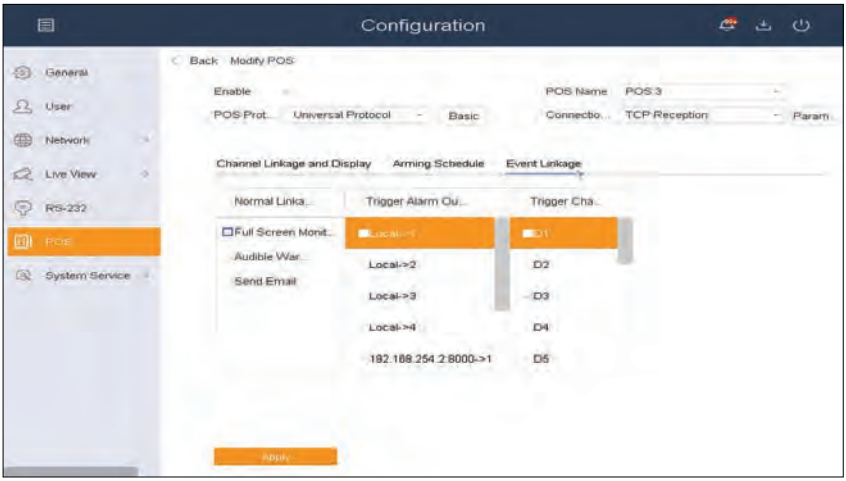
7.2 Configure the POS interface

Do the following:

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



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.cClick **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.

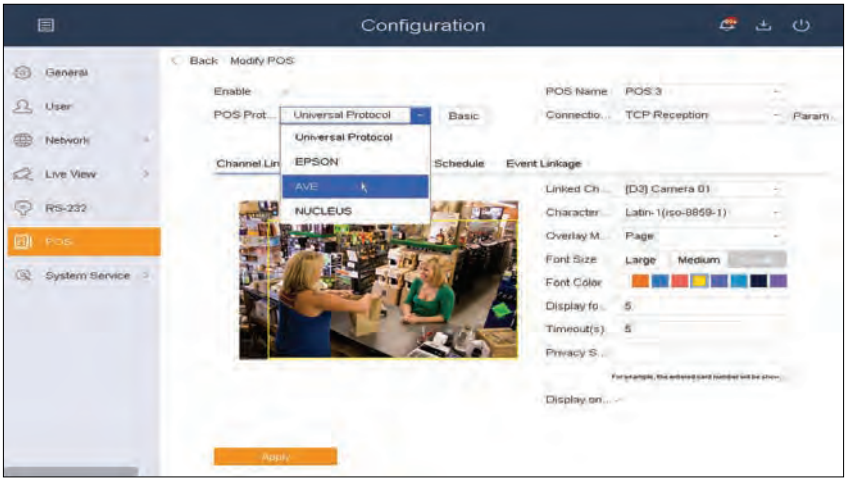




a. Click an entry field, and then enter the label of the data you want to hide.

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.

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



a. Open the POS Protocol drop-down list, and select either **Universal Protocol**, **EPSON**, **AVE** or **NUCLEUS** whichever matches the register.

b. Open the **Connection Type** drop down list, and then select the way the recorder is connected to the POS terminal.

c. 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**.



d. If you selected **EPSON**, no additional parameters are needed.

e. 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.



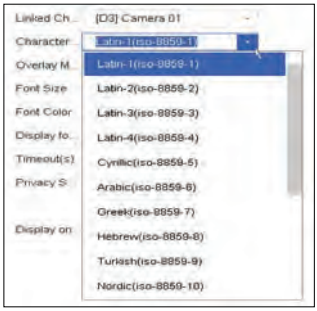
f. If you selected **NUCLEUS**, a restart is required. Follow the on-screen instructions to restart the recorder.

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

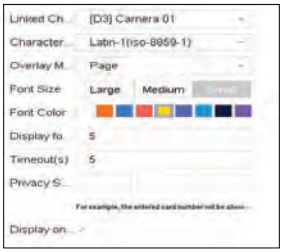
g. Click the **Settings** button, and then set the **Port** number and **Remote IP Address** to match the register. The default port number is 10000. The actual port number you must use depends on the register being integrated. The pcAmerica register used in this example requires port 4201.



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



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

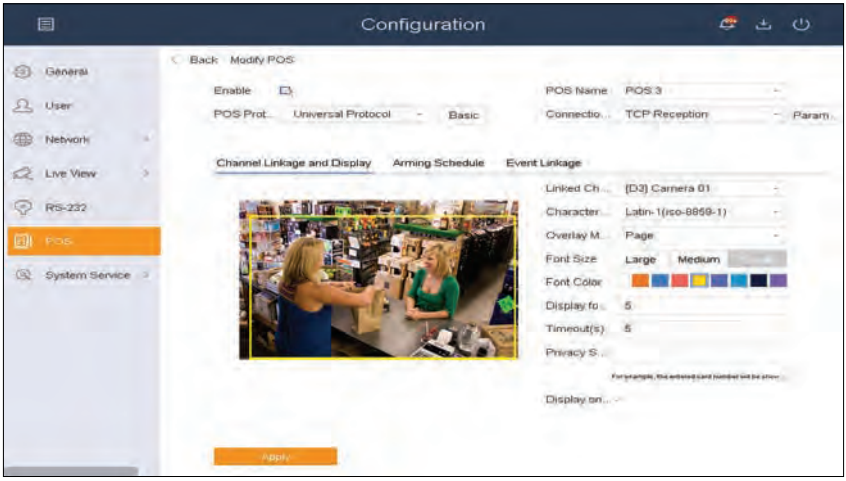


j. Check the **POS Overlay in Live View** box if you want messages from the register to appear over the camera image in Live View mode.

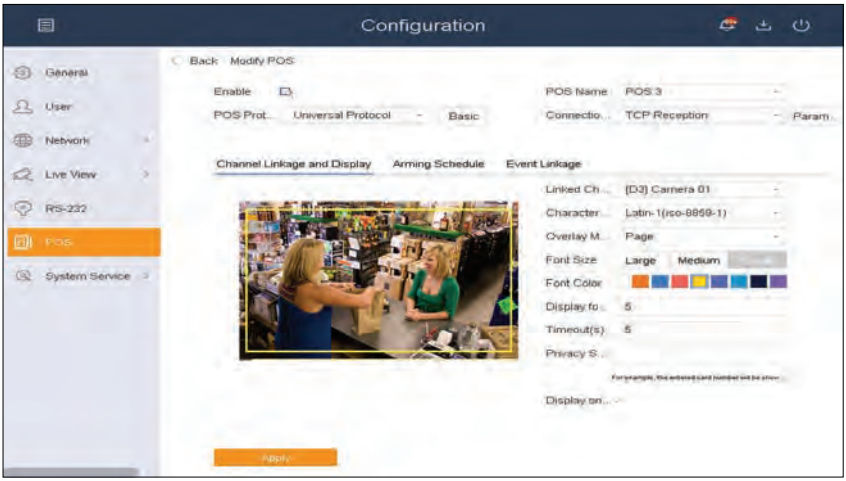
k. Click on the **Color** you prefer for the overlay messages.

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.



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.



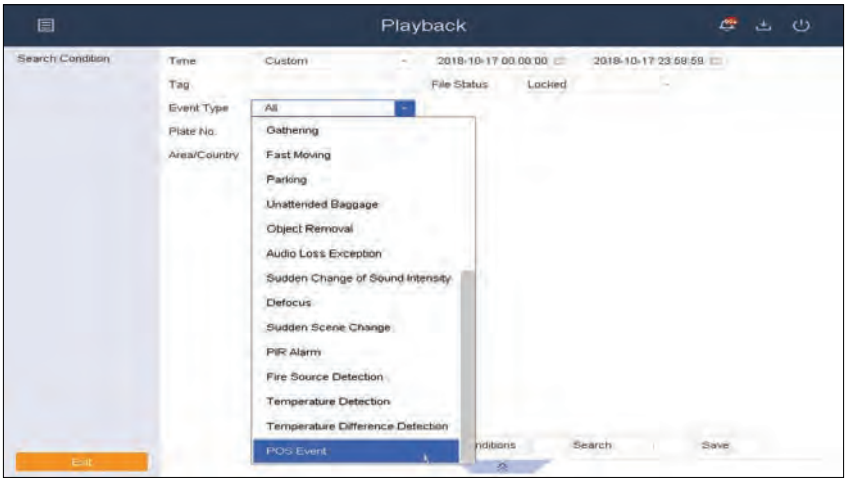
11. Verify that when transactions occur at the POS terminal, overlay text appears in the Live View image and the field below it.
12. Click the **Stop Getting** button to disable this test feature.

7.3 Playback POS recordings

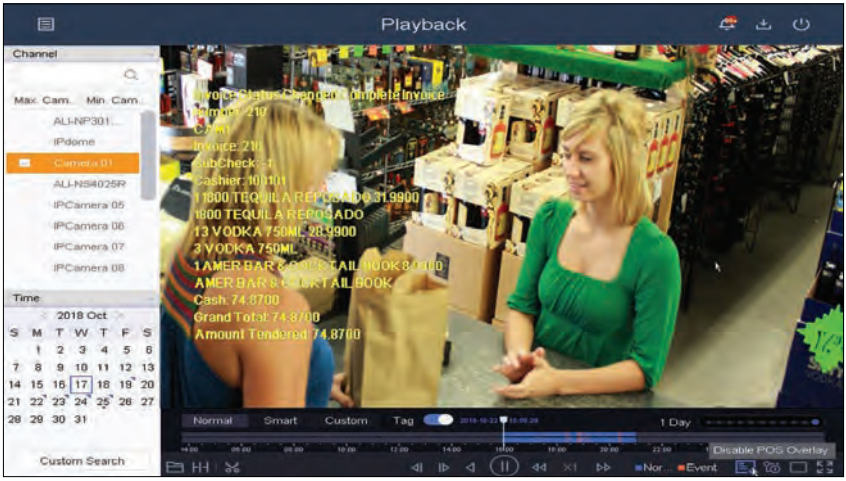
When the POS setup is configured to record video when messages are received from the register, you can use **Custom Playback - POS Event** search features to find the video coupled with message strings received from the register. In the example below, a search is made for register events where "water"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



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.

— **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.

5. 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.

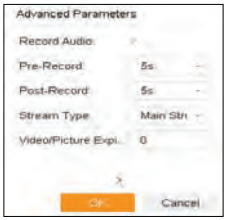
You can setup a record schedule in either of two ways: graphically, where you apply recording modes to sections of the week array (Monday through Sunday × 0 through 24 hours) and by using the Edit menu to more accurately define what mode of recording occurs and when. You can intermix the graphical method 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.*

1. 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.



2. To configure the Record 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:

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.

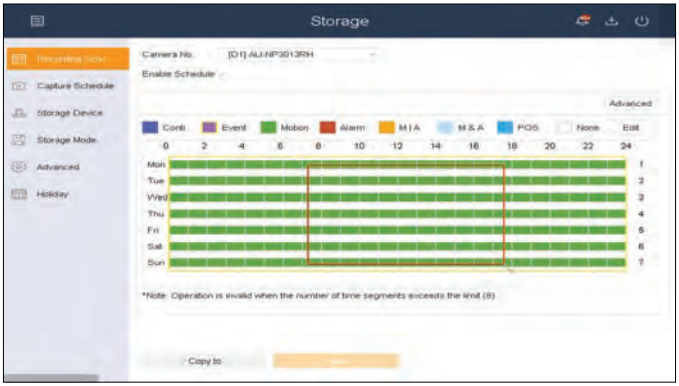
iv. Set the **Video/Picture Expiry** parameter as needed. This parameter sets the expired time for a recorded file to be kept in the HDD. When the deadline is reached, the file will be deleted. If you set the expired time to "0," the file will not be deleted. The retention time for a file is determined 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 PB, Monday through Sunday was selected.



2. 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.



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

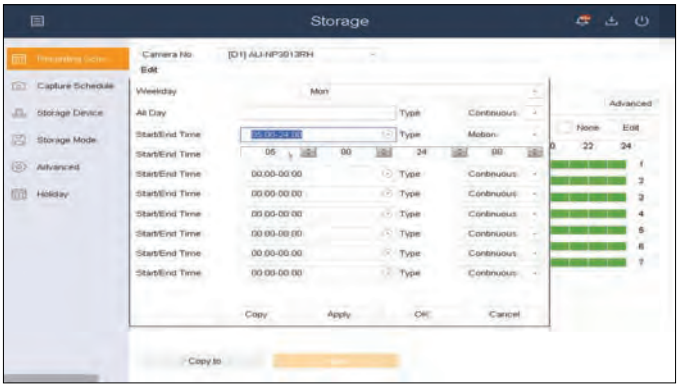
Setting the Recording Schedule using Edit

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:

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



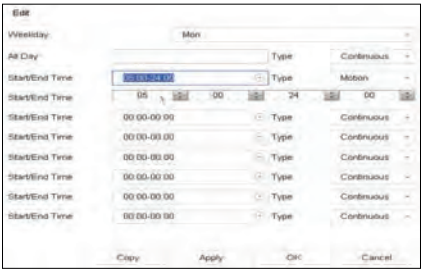
In the **Edit** menu:

i. Open the **Weekday** drop down list, and select the day you want to configure.

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

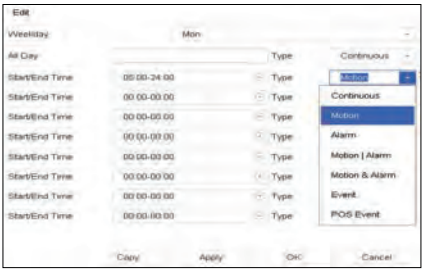
NOTE *Alarm triggered recording is available for only some cameras models supported by the NVR. Consult your vendor support organization for more information.*

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 file 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 × 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.

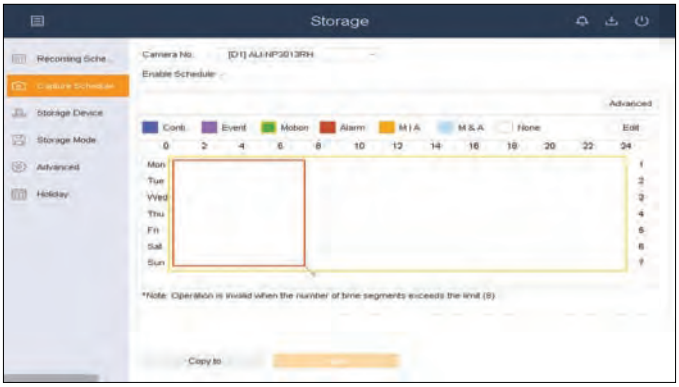
iv. Open the **Capture Delay Time** drop down list and select the duration for capturing pictures.

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:

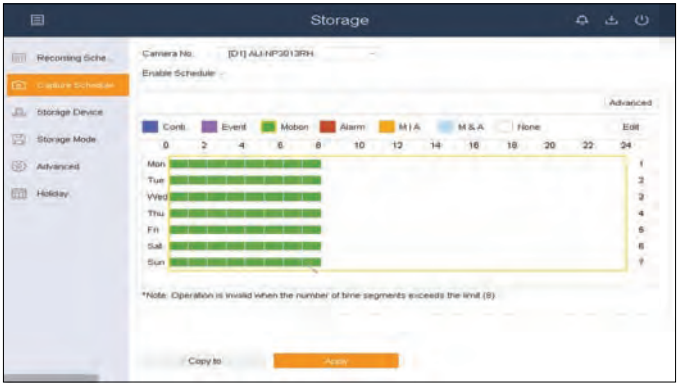
3. Use the mouse to drag a rectangle across the area of the schedule you want to change. A red rectangle will show the area you selected. In this example, the period from 12 AM to 5 AM, Monday through Sunday was selected.



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.

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



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

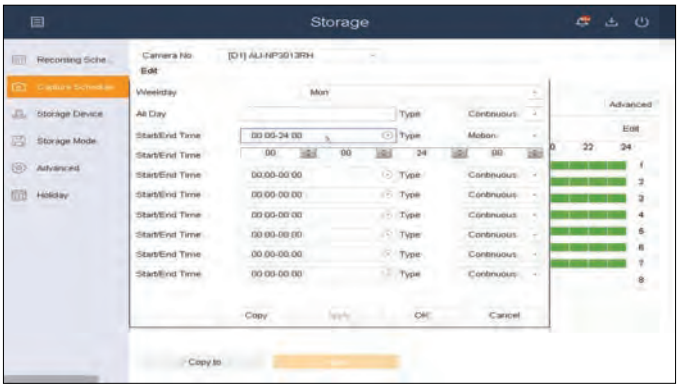
Setting the Capture Schedule using Edit

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:

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

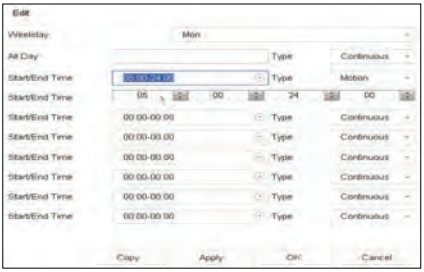


In the **Edit** menu:

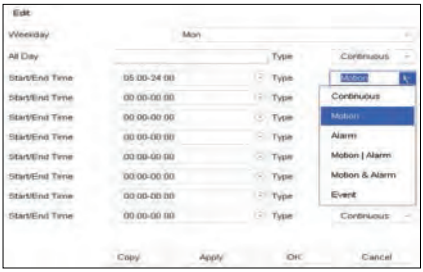
i. Open the **Weekday** drop down list, and select the day you want to configure.

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.

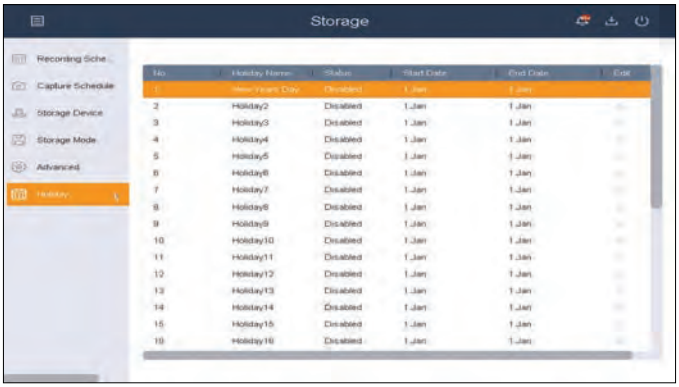
7. Click **Apply** in the Capture Schedule menu.
8. Click **OK** to close the Edit menu.
9. In the **Capture Schedule**, click **Apply**.
10. Repeat the steps above for each camera.

8.4 Defining Holidays

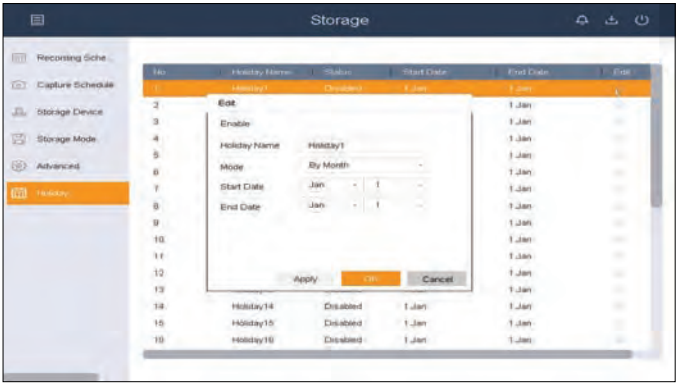
You can create a recording schedule for holidays only after specifying which days are holidays. Holidays can be specified by day (of the year), week or month. When these holidays occur, the Holiday recording schedule will be performed instead of the normal Monday through Sunday recording schedule setup 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**.



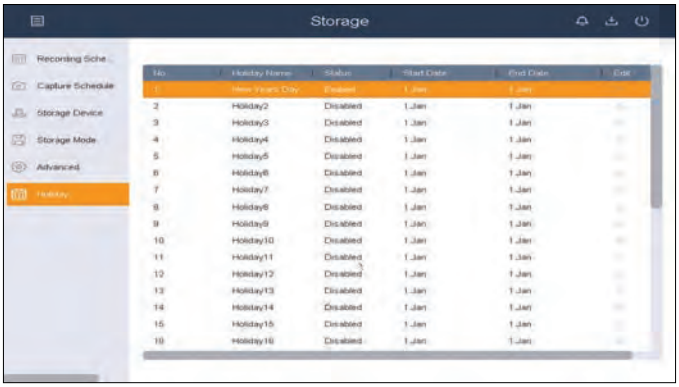
2. Click on the **Edit** icon for the first entry in the list. You can define up to 31 different holidays periods.



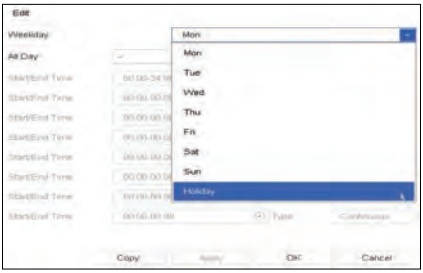
3. In the **Edit** window, click the **Enable** box to check it.
4. Click on the **Holiday Name** field, and then enter a common name for the holiday.



5. 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.
6. 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.
7. Click **Apply** to save your setting, and then click **OK**. The Holiday Settings window will show the holidays you created.



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



10. 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.

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



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

8.6 Playback

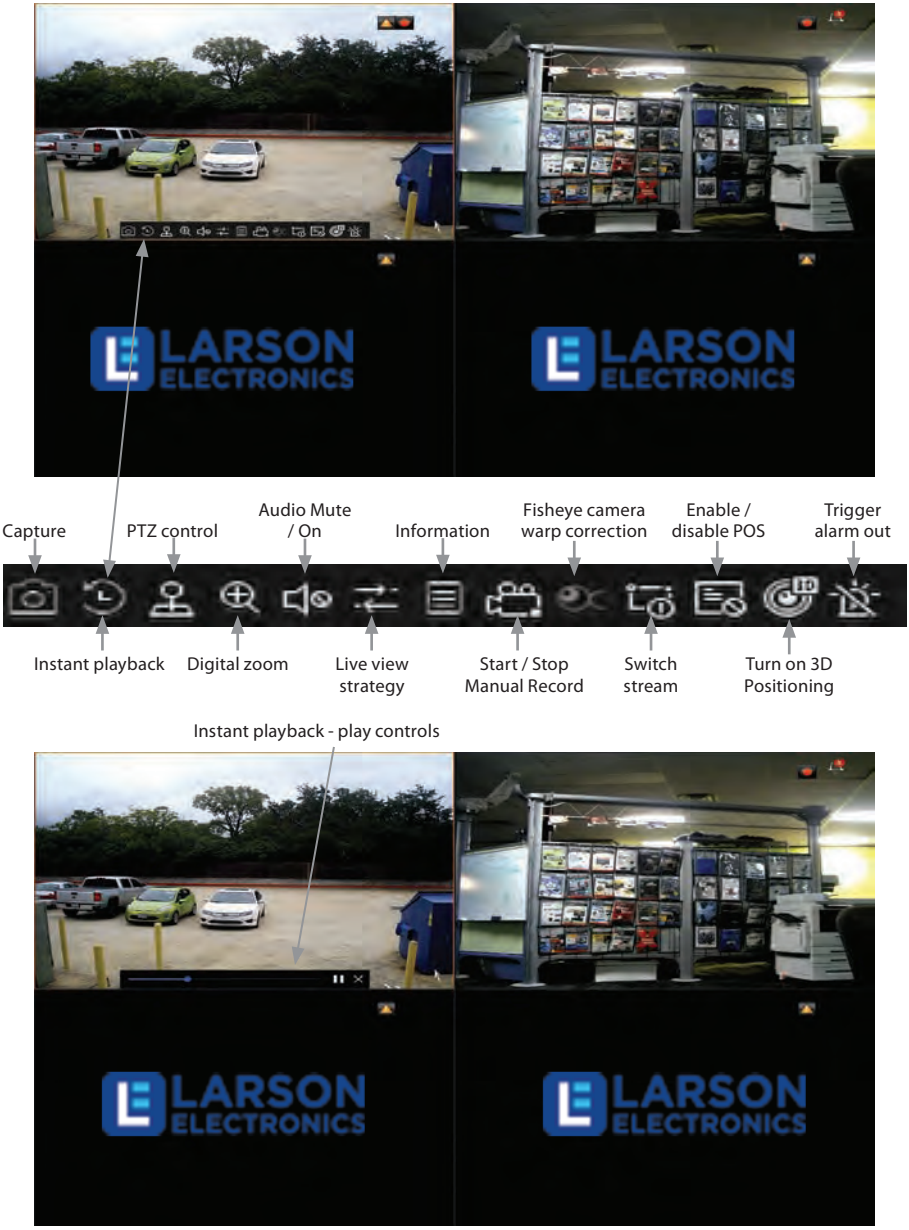
You can playback recorded video files instantly, or in several ways through the Playback menus.

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.


Capture
PTZ control
Audio Mute / On
Information
Fisheye camera warp correction
Enable / disable POS
Trigger alarm out
Instant playback
Digital zoom
Live view strategy
Start / Stop Manual Record
Switch stream
Turn on 3D Positioning
Instant playback - play controls
LARSON ELECTRONICS
LARSON ELECTRONICS
LARSON ELECTRONICS
LARSON ELECTRONICS

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

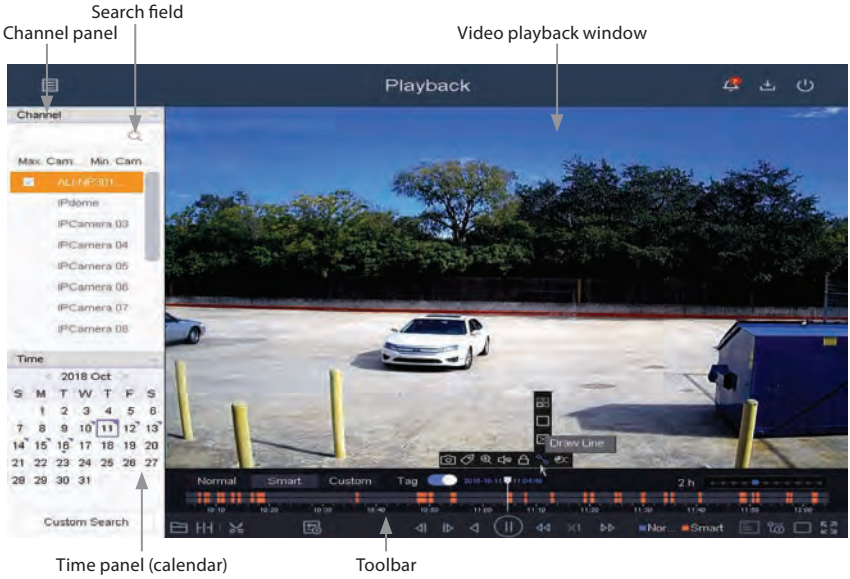
NOTE *In Live View mode, you can click the **Start/Stop Manual Record** icon to instantly record a video clip.*

8.6.2 Using the Playback screen

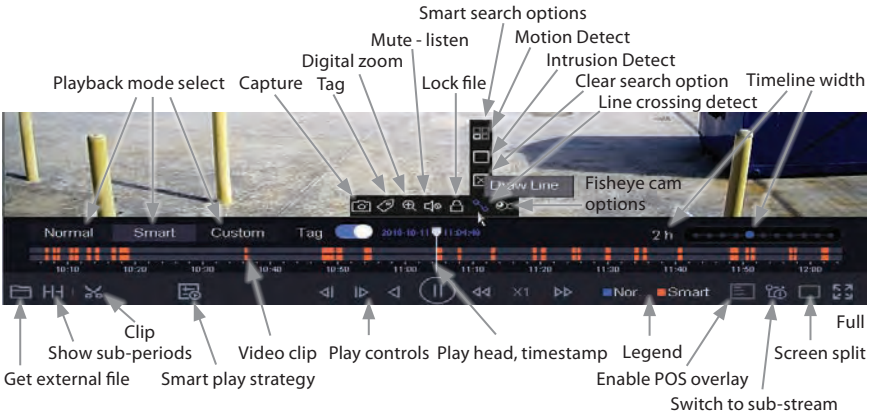
Use the Playback screen to find and replay video recordings. You can synchronously playback up to 16 video streams at a time. Three playback modes are available:

- **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

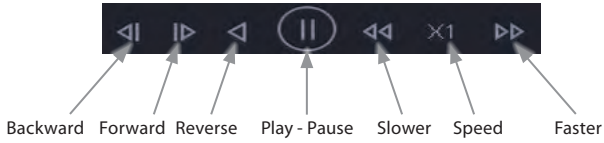


Notes:

- **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.

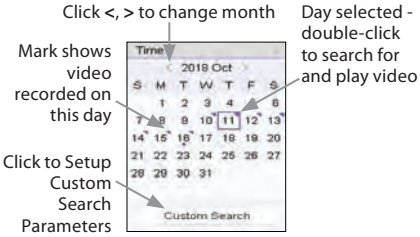


- **Show sub-periods**: Use this feature to divide play long video files into 4 segments and play them concurrently in a 2×2 split window (four frames) within the video playback window. For instance, if you are playing a video file that is 2 hours long, the file will be divided into four 30 minute segments, 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

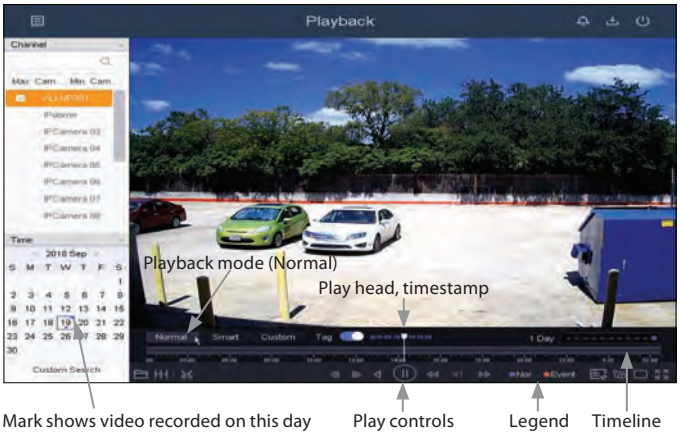
Normal playback shows and plays back all video clips recorded from the selected camera on the selected day.

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



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-NP3013RH (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.

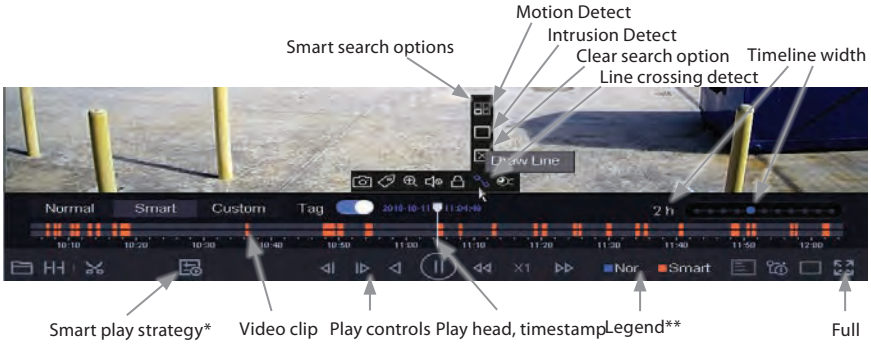
8.6.4 Smart Playback

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.



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 recorded 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 recorded 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.

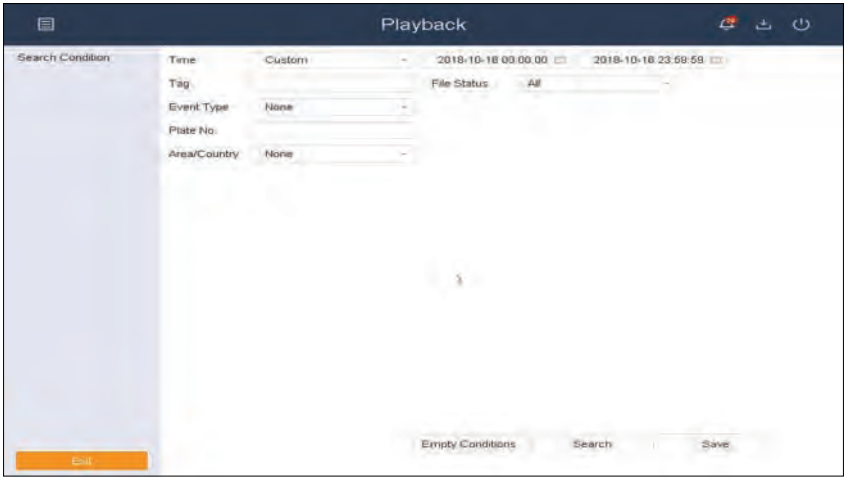
8.6.5 Custom Playback

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:

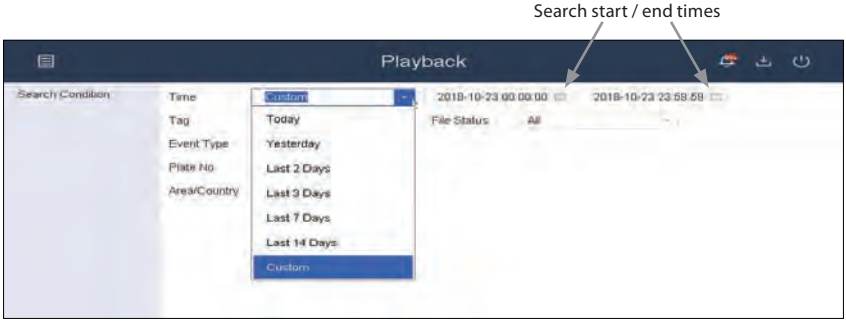
1. Open the Playback screen. Go to **Menu | Playback**.



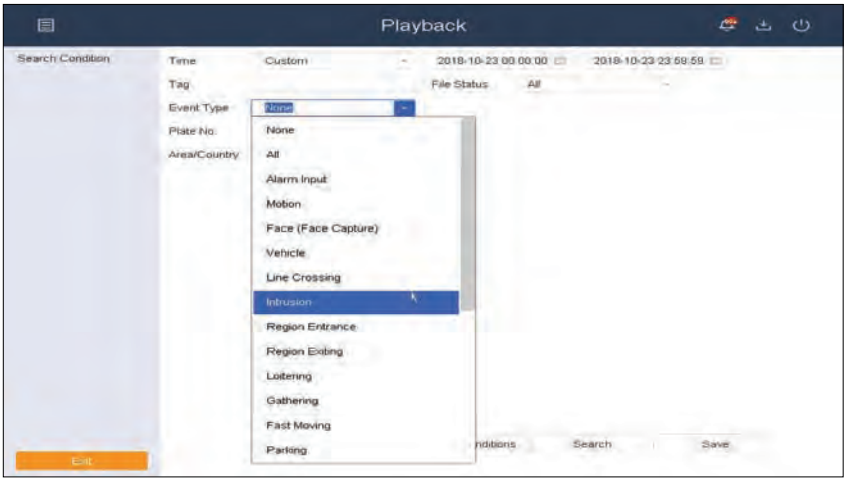
2. Check the select box for the camera in the left frame whose video you want to search.
3. Click the **Custom Search** button in the lower left corner.



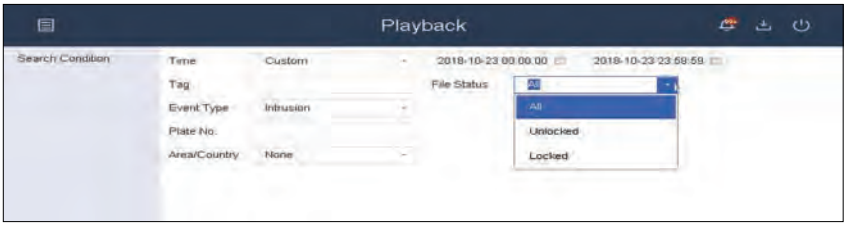
4. In the **Custom Search** menu, open the **Time** drop down list and select the time span you want to search. You can also click the calendar icons in the start and end time fields to select other time spans.



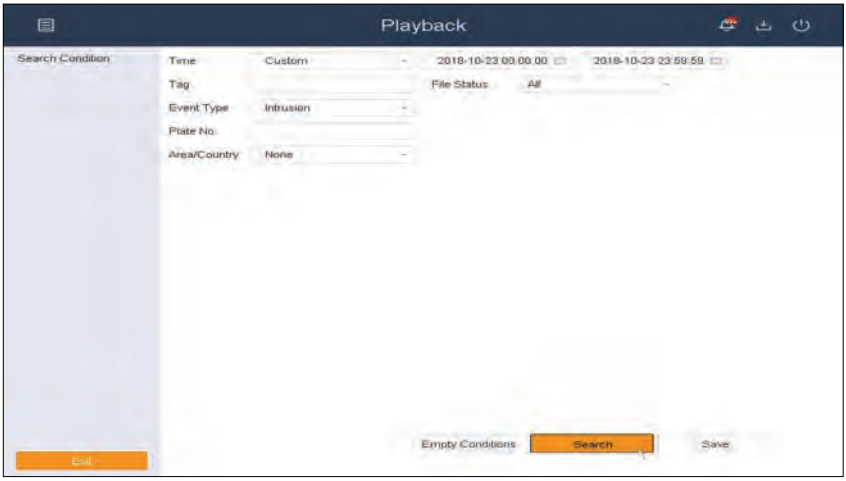
5. Open the Event Type drop down list, and then select the type of event you want to search for. In this example, **Intrusion** was selected.



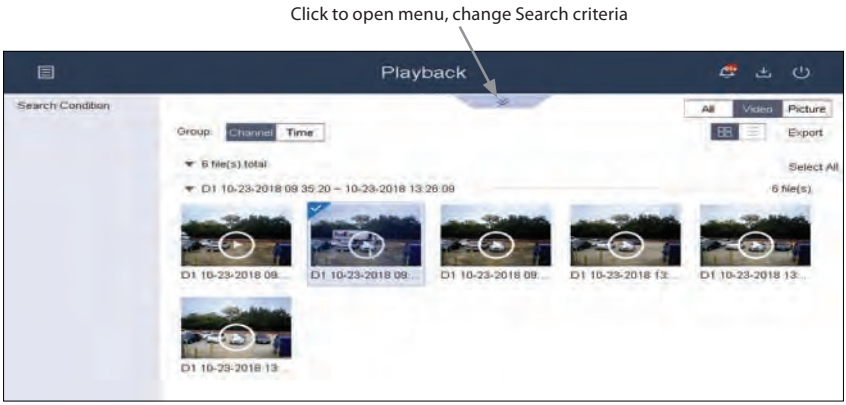
6. You can also open the **File status** drop down list and search for only **locked** or **unlocked** files.



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



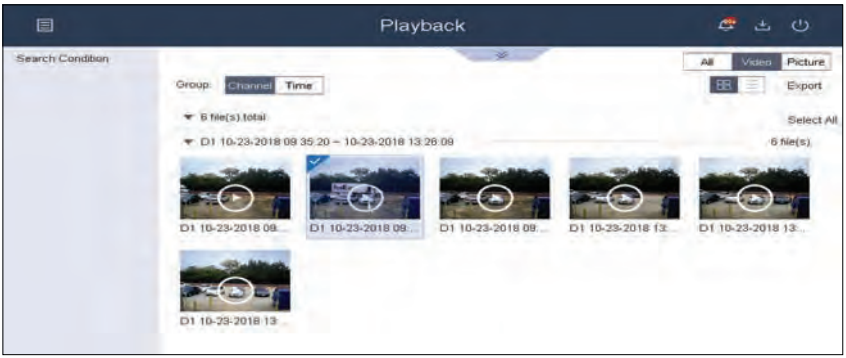
8. Click the **Play** icon on the thumbnail of the video you want to watch. The Playback screen will open to play the video clip. Custom Search results are indicated by red marks on the timeline.



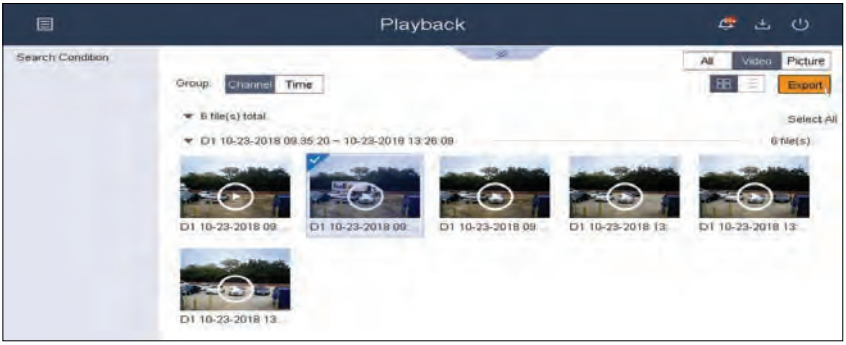
Export Custom Search result

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

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



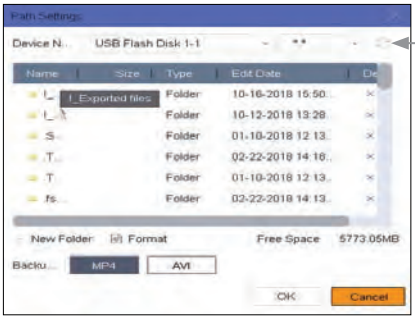
2. Click on the thumbnail for the file you want to export. When selected, the thumbnail will be shaded, and a check mark will appear in the upper left corner.



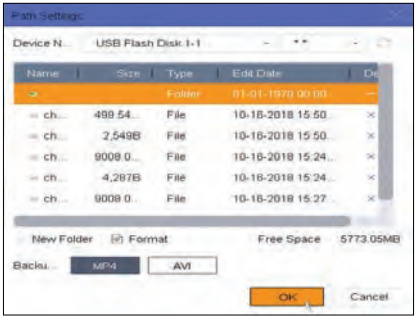
3. To export to a flash drive, insert a USB flash drive into an unused port on the recorder, and then click the Export button in the upper right corner.
4. In the Export popup menu, select the options you want to save, and then click OK.



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.



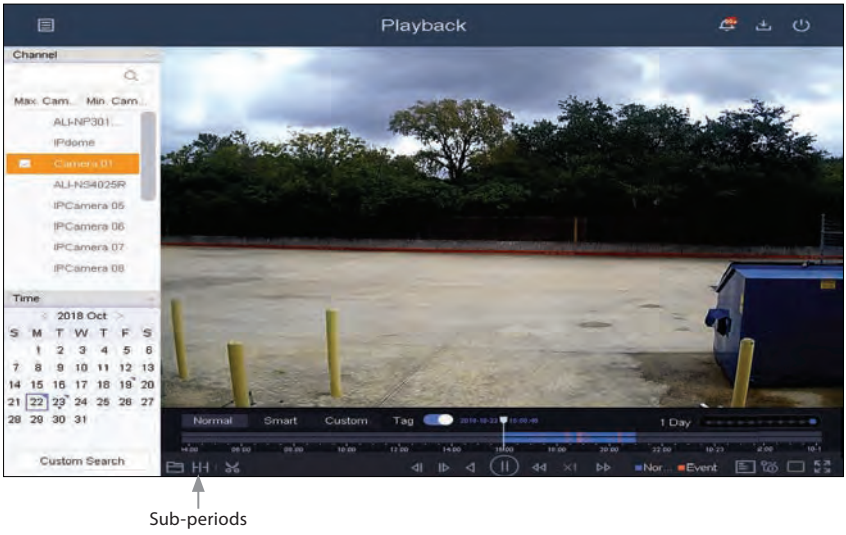
Play Sub-periods

Use this feature to divide play long video files into 4 segments and play them concurrently in a 2×2 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.

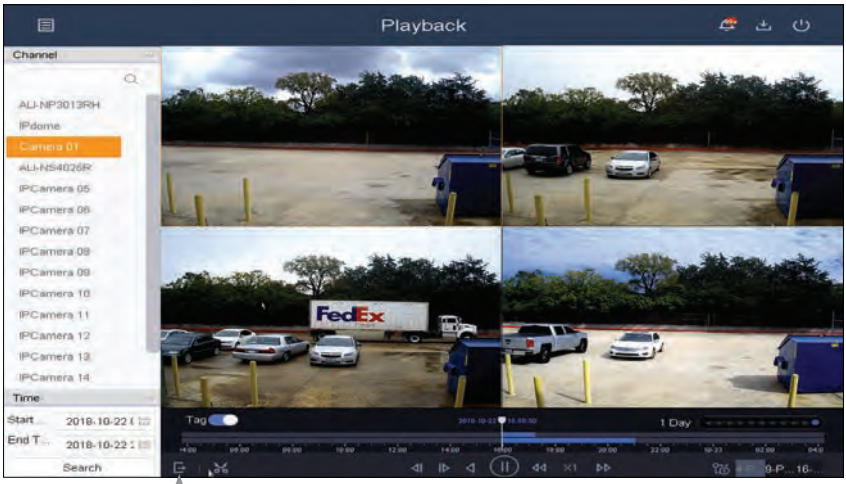
1. Open the Playback screen. Go to **Menu | Playback**.



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 **Sub-Periods** icon.



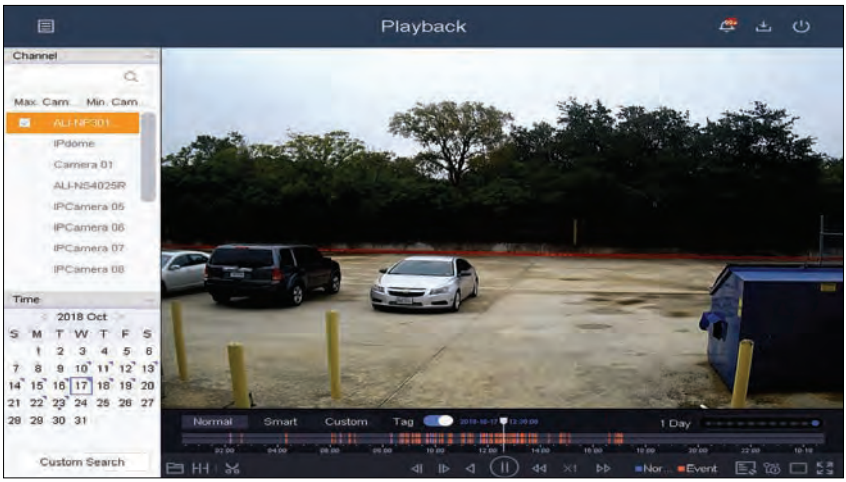
Back icon (exit Sub-periods)

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

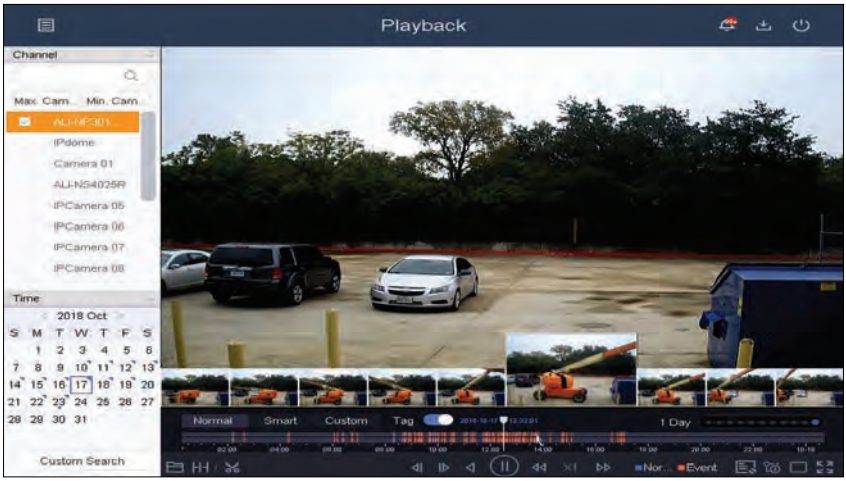
Thumbnails view

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.



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

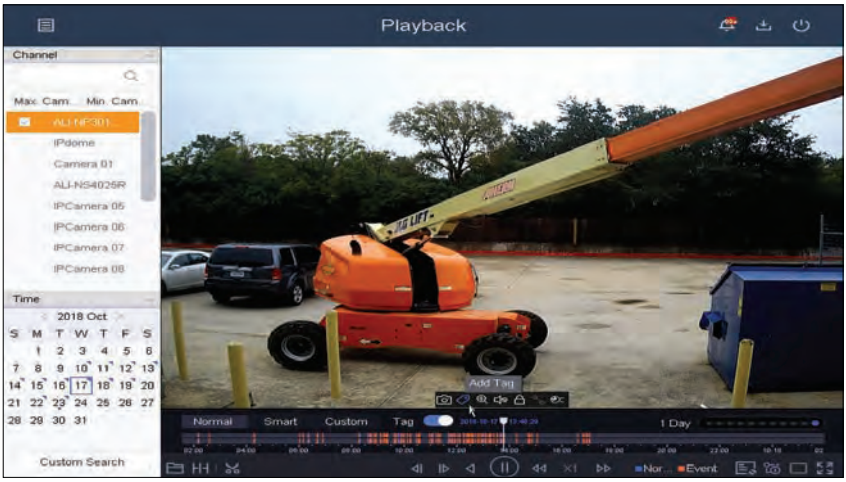


3. Click on the thumbnail of interest to play it in the playback window.

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.



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



Custom search for tag

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

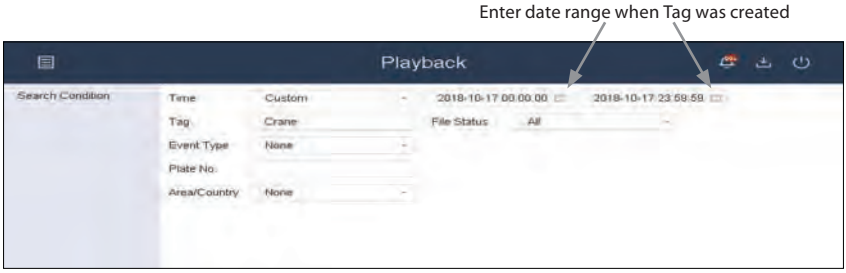
1. Open the Playback screen. Go to **Menu | Playback**.



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.

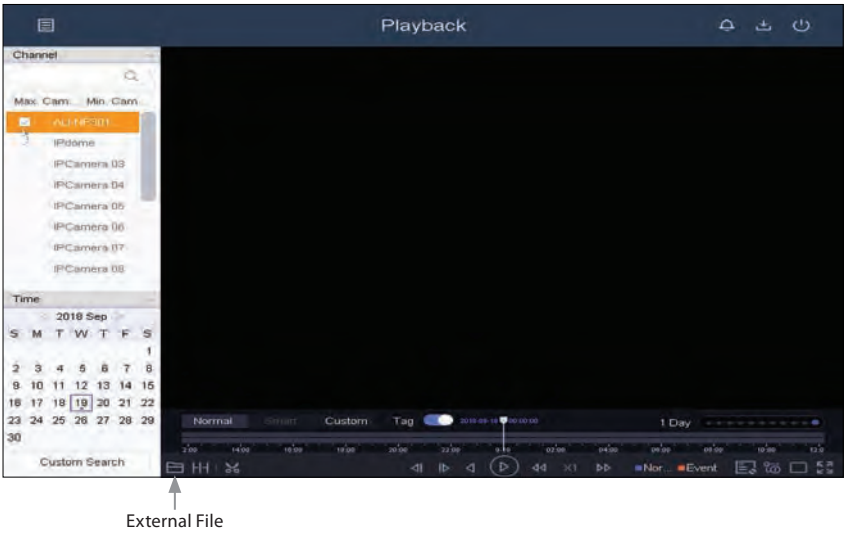


6. Click the **Play** icon in the result thumbnail to play the file in the Playback screen.

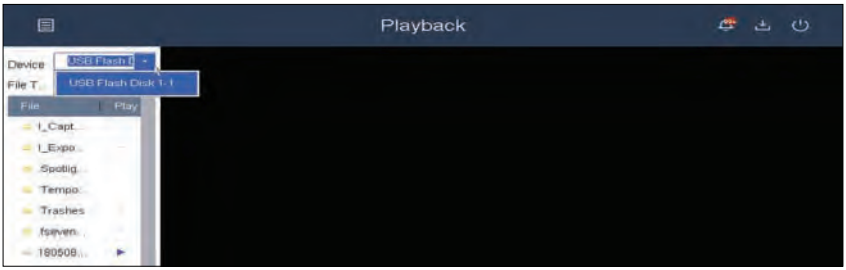
External file

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:

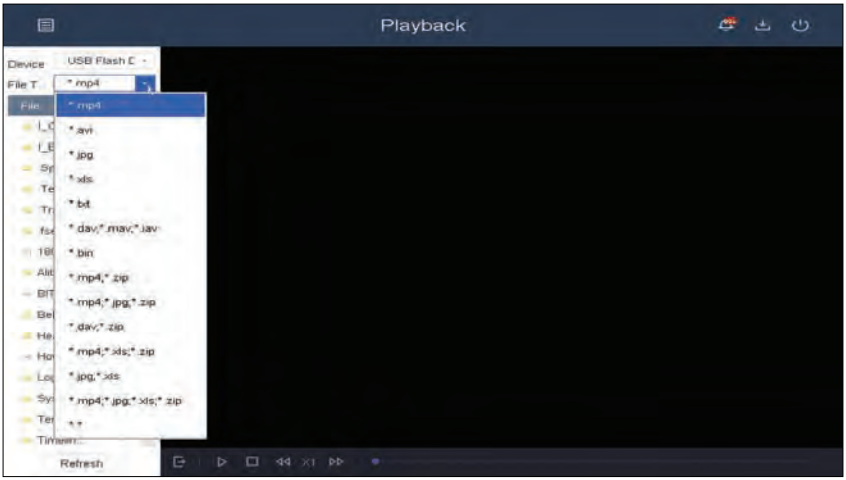
1. Open the Playback screen. Go to **Menu | Playback**.



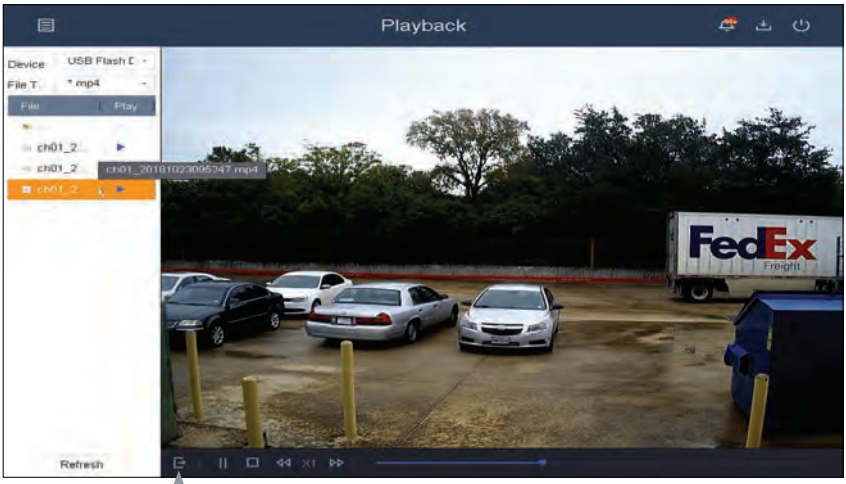
2. Insert a USB flash drive with the file you want to play into an unused USB port on the recorder.
3. Click the **External File** icon.



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.



7. 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

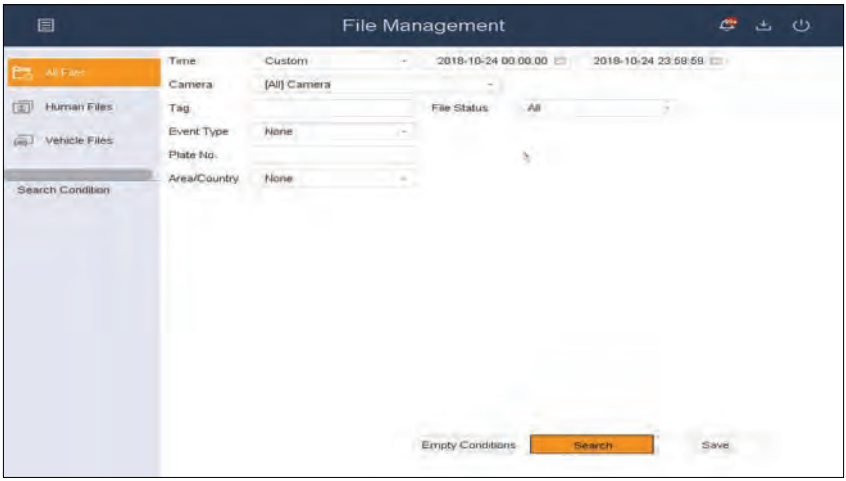
You can use the File Management menus to search for and export files recorded or captured from your cameras.

8.7.1 File Management - All Files

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

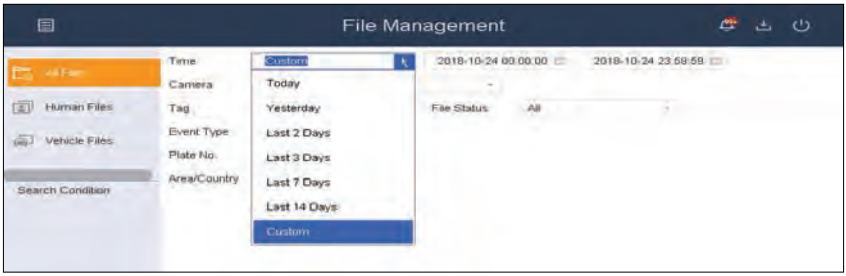
In the procedure below, the camera on channel D1 (ALI-NP3013RH) was previously configured to detect Line Crossing events. Video from these events between 10/22/18 and 10/25/18 was found using the **File Management - All Files** menu. A video resulting from the search was selected and exported to a USB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

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

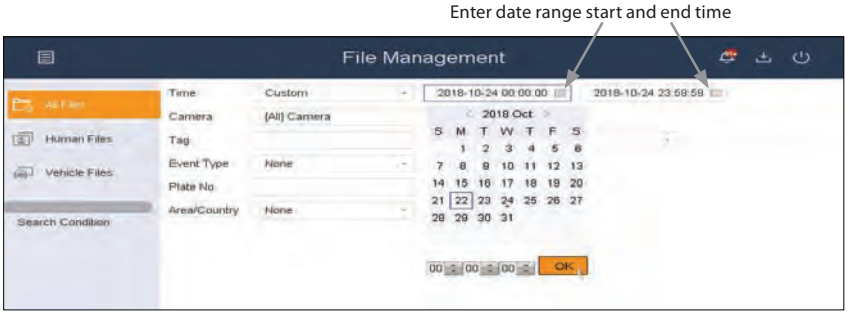


2. Select the time span across which you want to search. The menu provides two methods:

   a. Open the **Time** option drop down list, and select the period back from the current day to search.

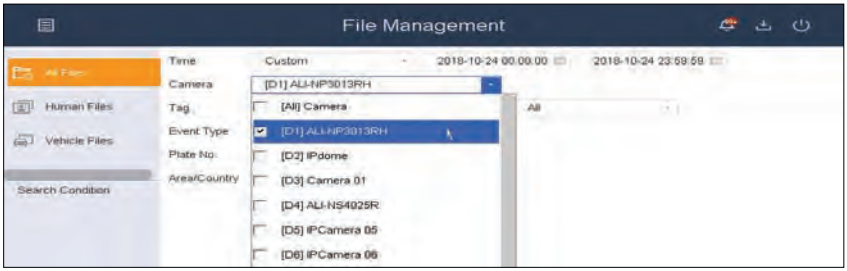


   b. Or, use the Custom (calendar) feature to select the start date and time. Click the calendar icon shown below to open the calendar menu, click on the date for start (or end), and then set the time in GUI at the bottom. Click **OK** to select your settings.



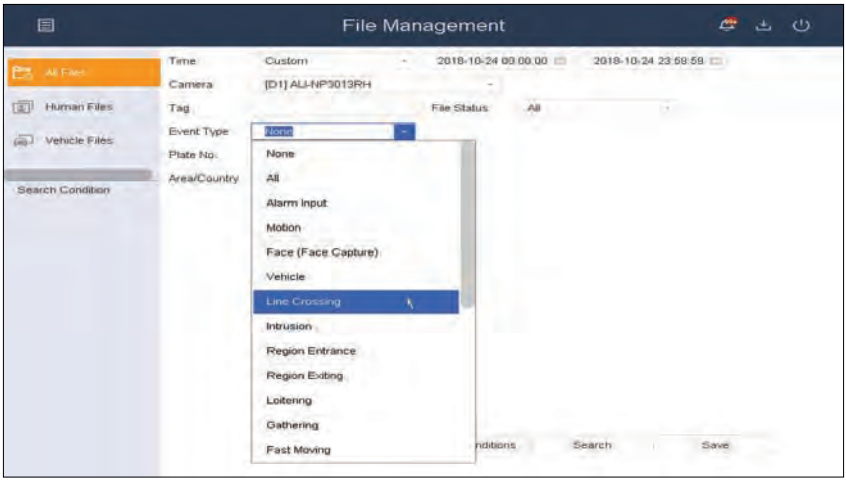
c. Repeat the sub-step above to set the end date and time. Not that time time setup in these menus is 10/22/18 to 10/25/18

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.

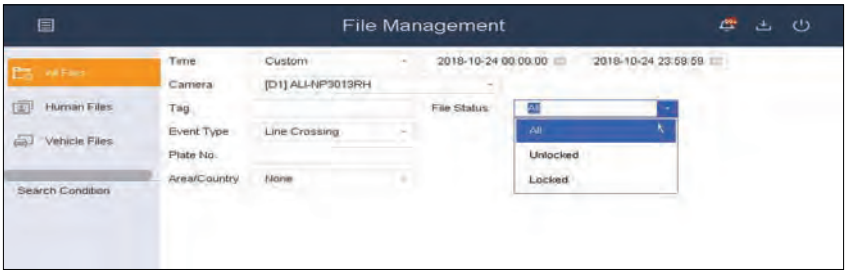


4. In this example, skip the Tag option since we are not searching for a tagged file.

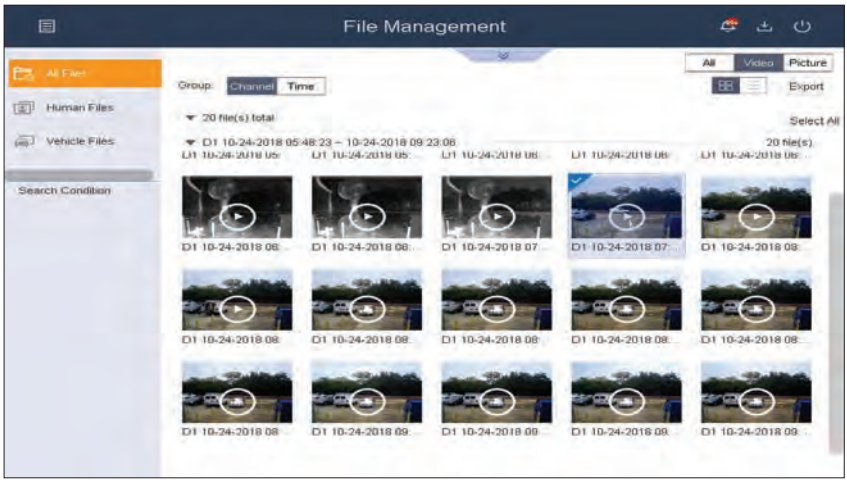
5. Next, open the Event Type drop down list and select **Line Crossing** the event we are looking for.



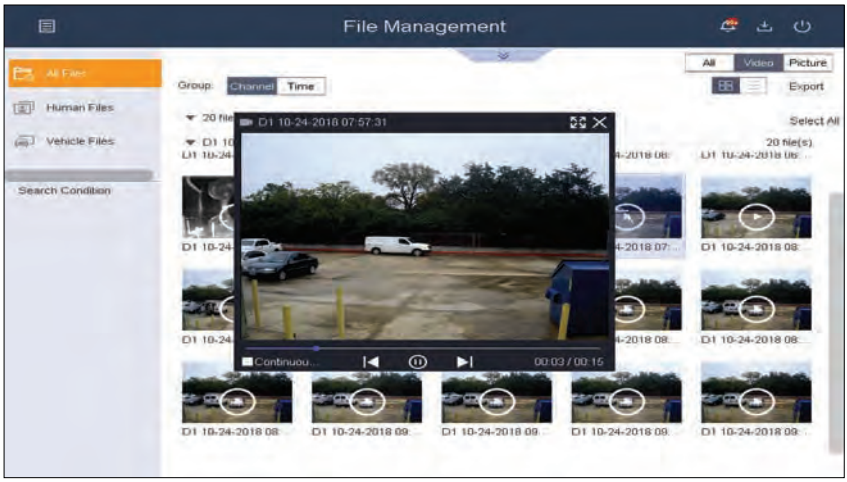
6. Notice that the File Status for the search will look at all files. If the file was locked or unlocked, should select that option. For this examle, we'll select All.



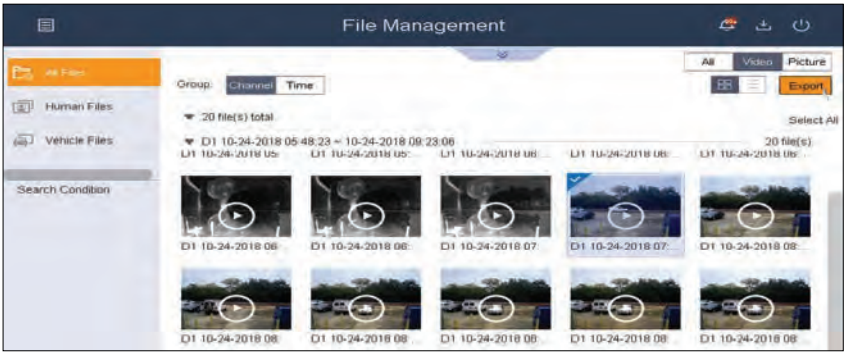
7. Click the Search button at the bottom of the screen. Search results are shown in thumbnails.



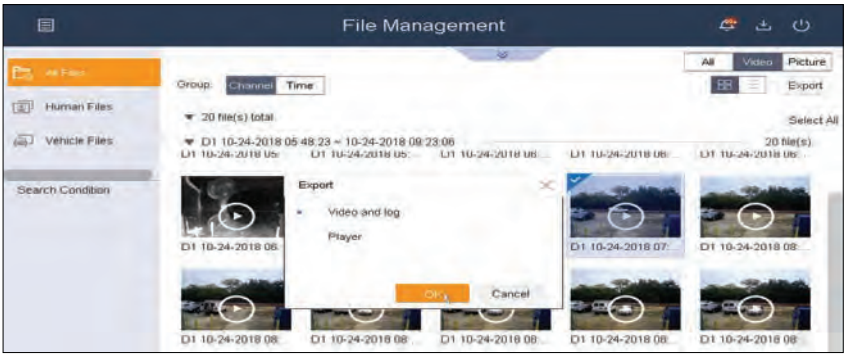
8. Click on the thumbnail for the file you are searching for to select it (see above). When the file is selected, a check mark appears in the upper left corner of the thumbnail, and the thumbnail is shadowed. To watch the video of the file, click the Play icon in the thumbnail.



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.



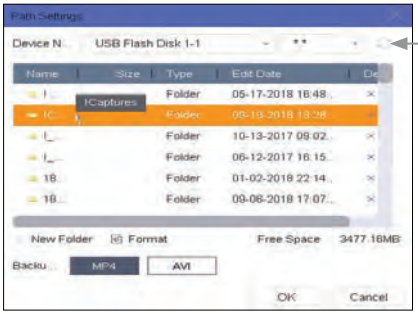
10. In the **Export** popup window, select the options you want to export. Select **Player** to export a video player with the video file and log.



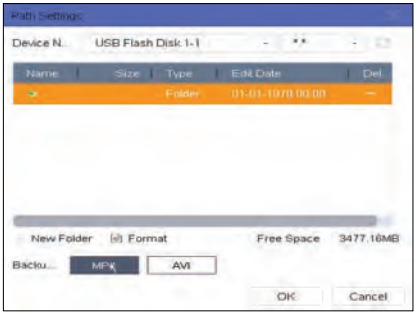
11. In the Export **Path Settings** window:

    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.

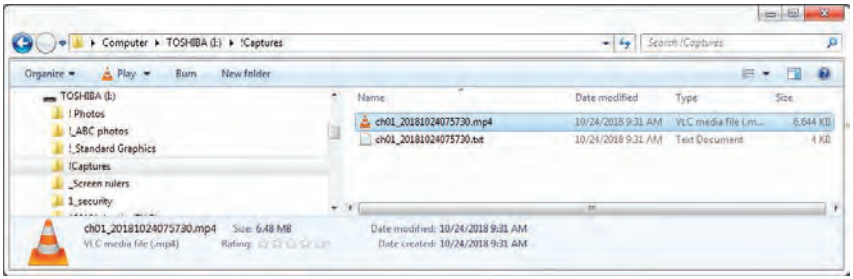


c. Click **AVI** to change the video file format to AVI.

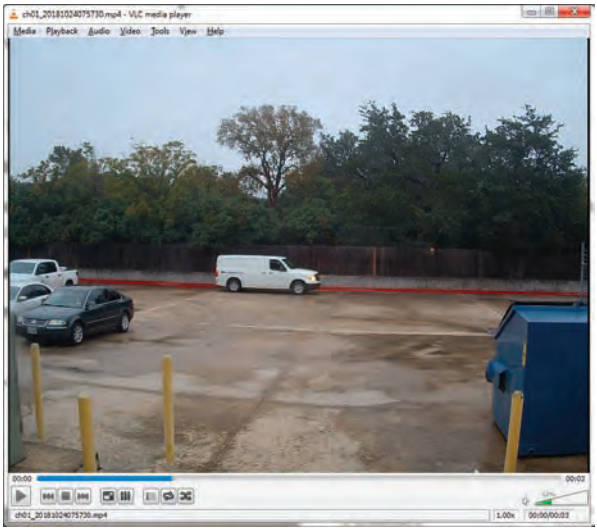


d. Click **OK** to export the file(s). The Path Settings window will close.

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.

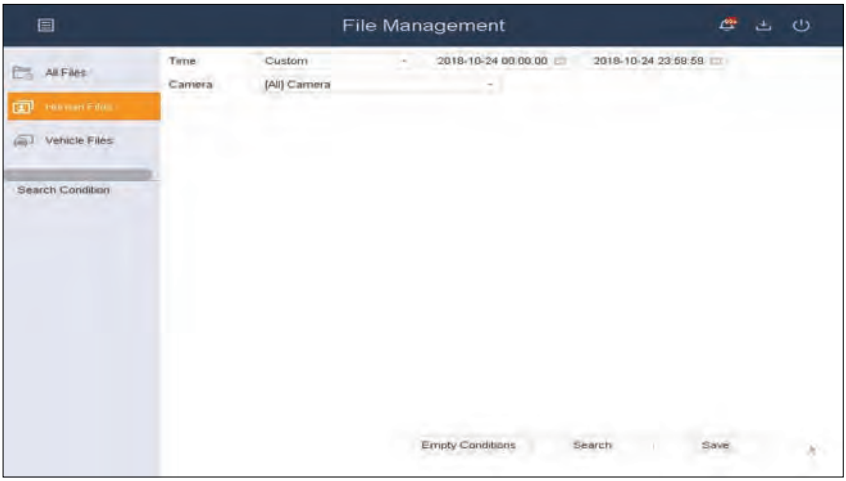


14. Play the file to ensure it is what you need. VLC Media Player was use to play this file (see below).



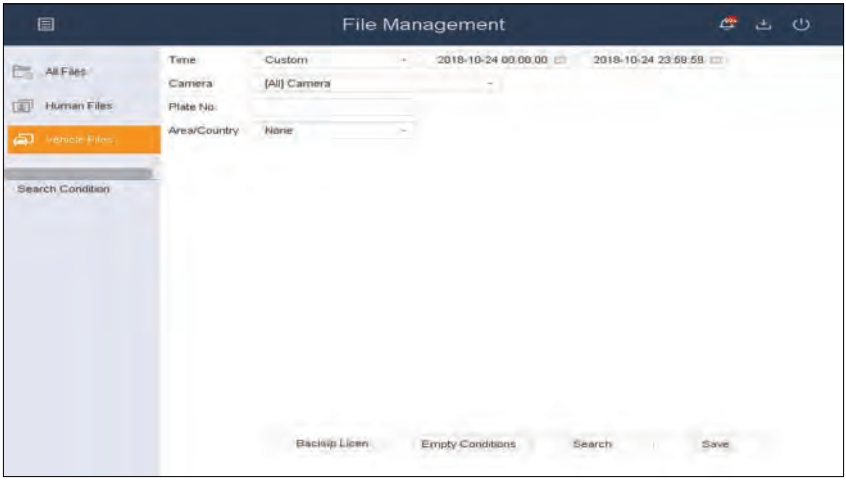
8.7.2 File Management - Human Files

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.



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

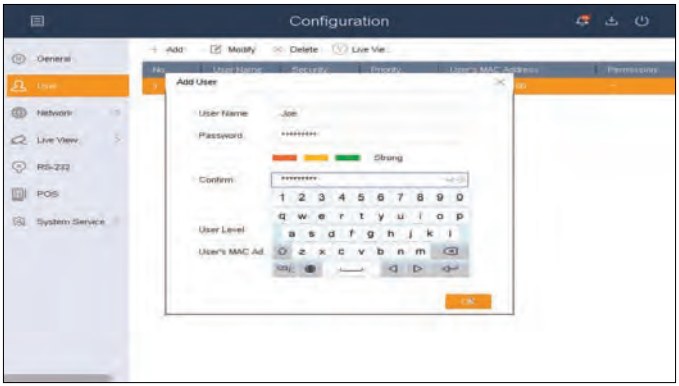
1. Log into the NVR as an administrator.
2. In the Menu display, click the Configuration icon, and then click User in the left frame. Initially, the user name list appears as that shown below.



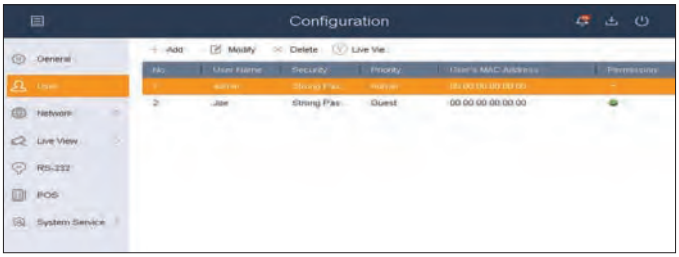
3. Click **Add** to open the Add User menu.
4. In the **Confirm Permission** popup window, enter your administrator user password, and then click **Next**.



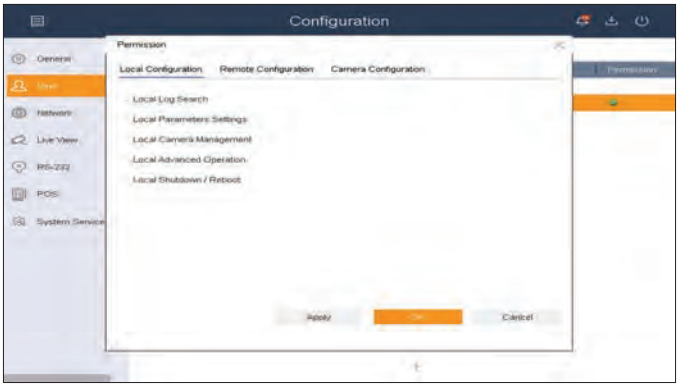
5. In the Add User menu, enter the information for new user, including User Name, Password, Password and Confirm password, Level and User's MAC Address (optional). Ensure that the menu shows that the password you selected is a "**Strong**" password.
6. Click **OK** to continue.



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

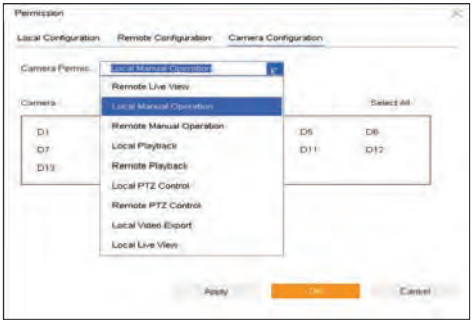


13. Check the select boxes for the additional permissions you want to assign.

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

- **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).

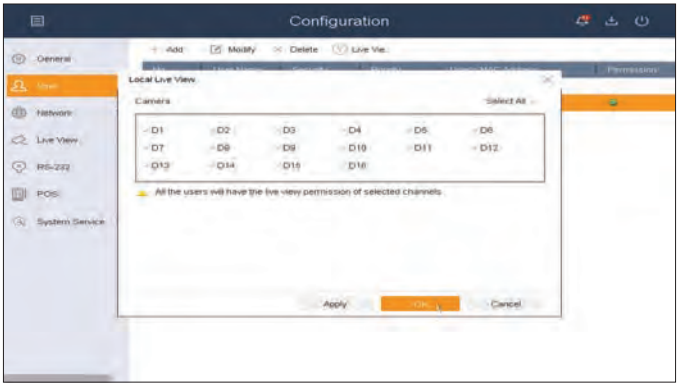
16. Click **Apply** to save your settings for the permission you selected, and the repeat the above step for other permissions, as needed.

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.



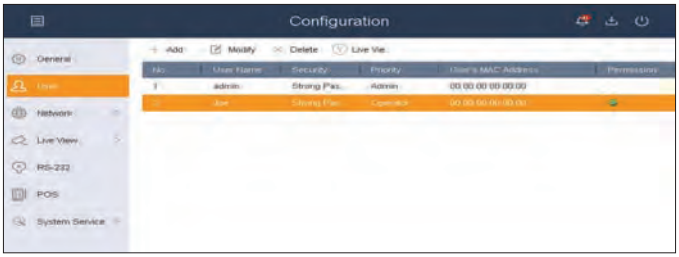
3. In the **Camera** box, check or uncheck the channels you want to grant or restrict, and then click **Apply**.
4. When the normal user (Operator or Guest) has no local live view permission for specific camera (s) (refer to 17.2.2 Set Local Live View Permission for Non-Admin Users), the live view permission 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**.

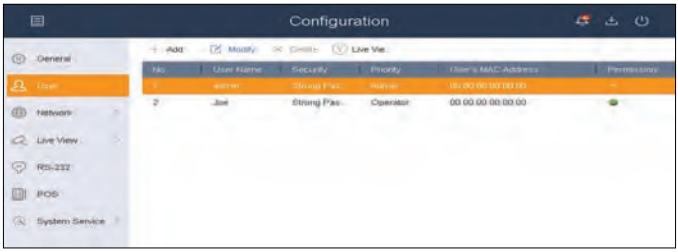


4. In the **User Level** drop-down list, select either **Operator and Guest.** You can edit the user information, including user name, password, permission level and MAC address. To change the password, click **Modify** to the right of the Password field, then enter the new password in the Password and Confirm fields.
5. Click **OK** to save the settings and exit the menu.
6. 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.

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



3. Click **Modify**.



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

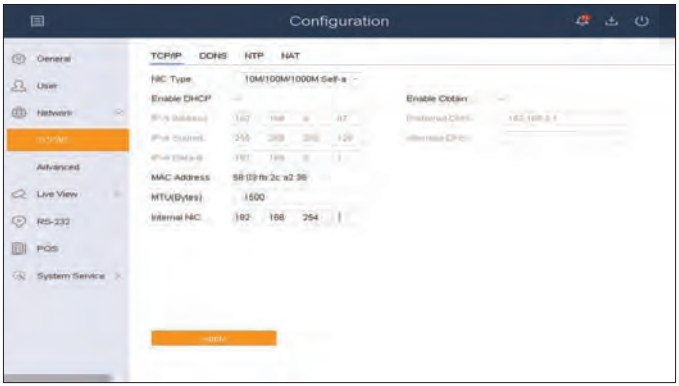
SECTION 10
Network Settings

10.1 Configuring General Network Settings

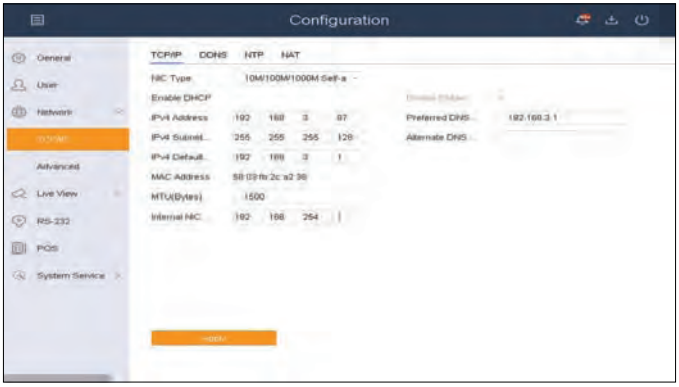
Network settings must be properly configured before you connect the NVR to cameras on the network, or access it remotely. In many cases, the IP address of your recorder should be fixed (unchanging) for easier remote access over time. Consult your network administrator to ensure you setup your recorder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





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.



4. 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.

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



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



     i. Enter Server Address for DynDNS (i.e. members.dyndns.org).
     ii. In the NVR Domain Name text field, enter the domain obtained from the DynDNS website.
     iii. Enter the User Name and Password registered in the DynDNS website.

   - **NO-IP**: Enter the account information in the corresponding fields.
     i. In a browser window, go to the URL: **http : / / alibiddns.com**

ii. In this website, create a **Domain Name**, **User Name** and **Password** for the recorder. Record these for use later.

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



iv. Enter **Server Address** for NO-IP (*dynupdate.no-ip.com*).

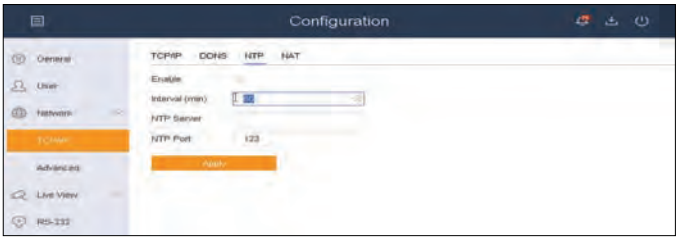
v. In the **Device Domain Name**, **User Name** and **Password** fields, enter the information setup at the *alibiddns.com* website. For example: *<your domain name>.alibiddnbs.com*

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:

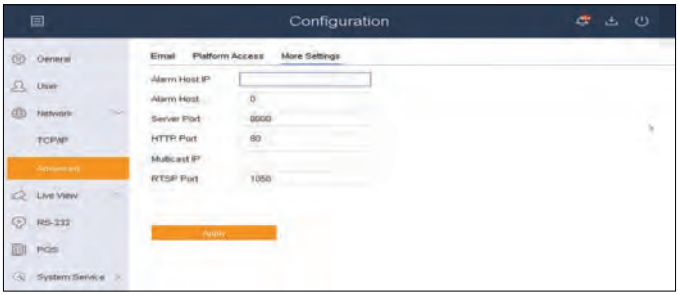
— **Interval**: Interval in minutes between the two synchronizing actions with an NTP server.
NOTE: The synchronization time interval can be set from 1 to 10080 minutes. The default value is 60 min. If the NVR is connected to a public network, use an NTP server that has a time synchronization function, 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.*

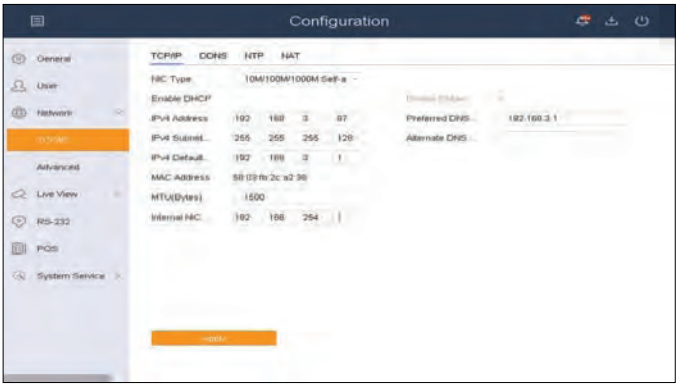
2. Click **Apply** to save your settings and close the menu.

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 men.



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.



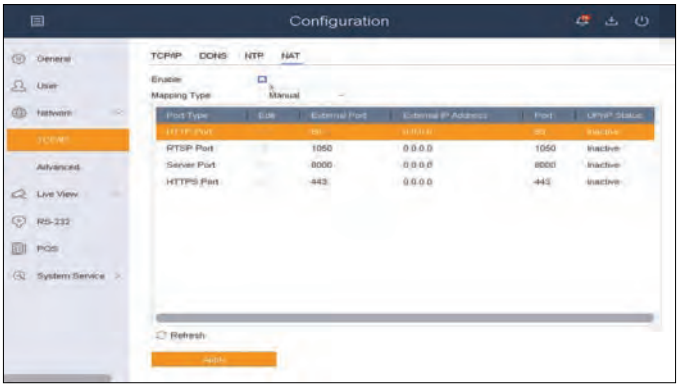


10.2.6 Configuring UPnP™

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.

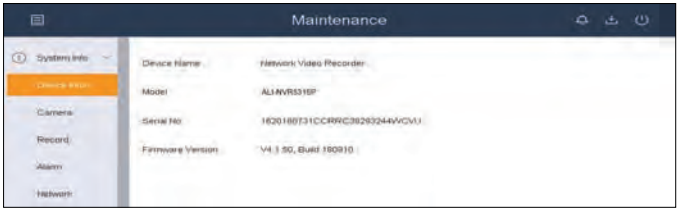
SECTION 11
System Maintenance

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

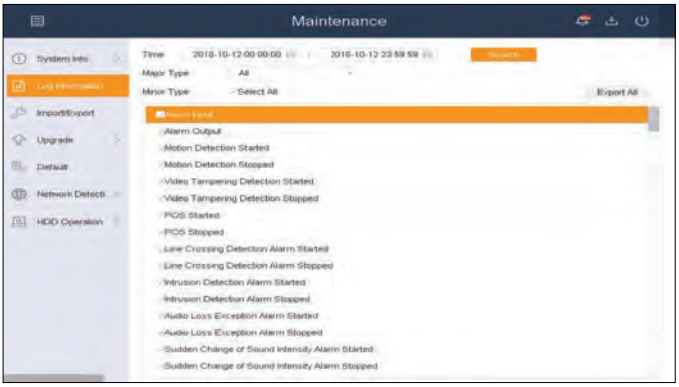
System log information is continuously generated and saved in log records. System logs include the following types of entries:

- **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.

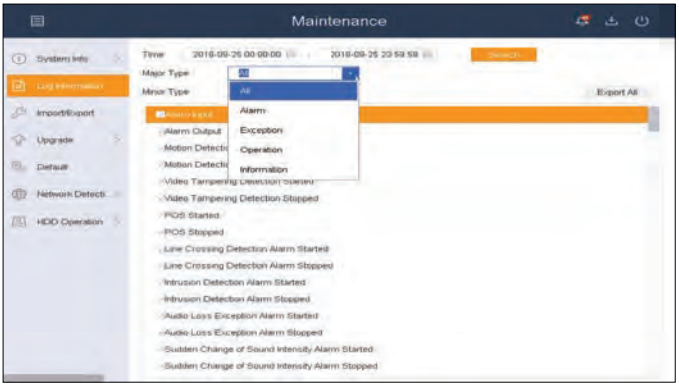
System logs can be searched and sorted for specific entries, and archived for use later. You can also search for video clips through system logs.

11.2.1 Log Search

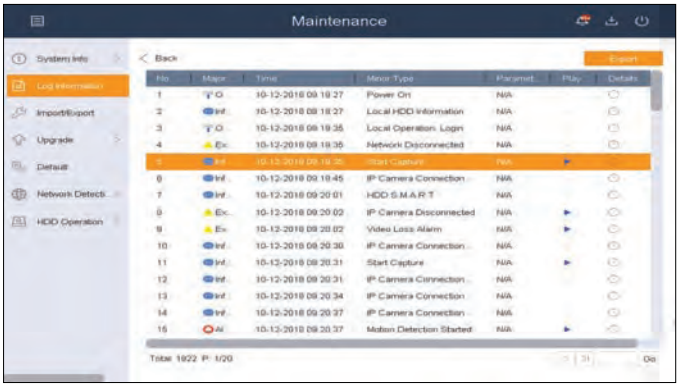
1. Open the Log Information screen. Go to **Menu | Maintenance | Log Information**.



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.



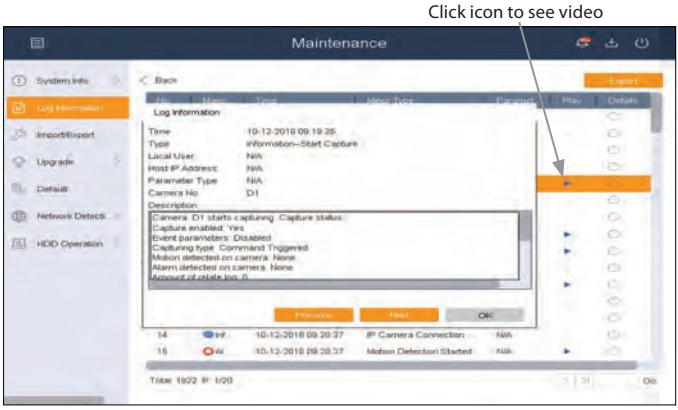
4. In the Minor Type list (see above), check the select boxes for the specific alarms you want to find.
5. Click **Search**. In the example below, the search criterion specified was **All** Major Type alarms and all **Minor Type** alarms on 10/12/18.



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.

6. To view more information about a specific log entry

   — Double click on the alarm entry.



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



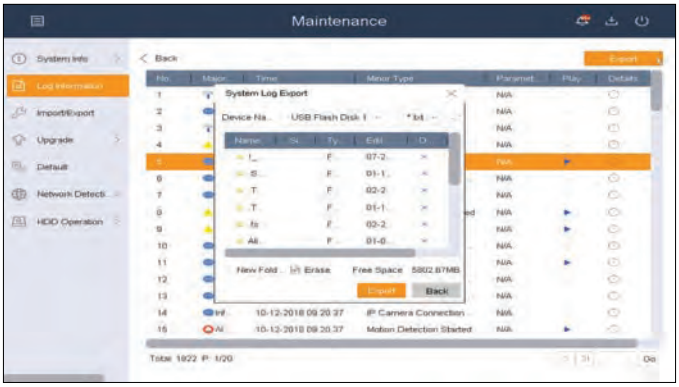
11.2.2 Log Export

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.



4. 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.





5. 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.



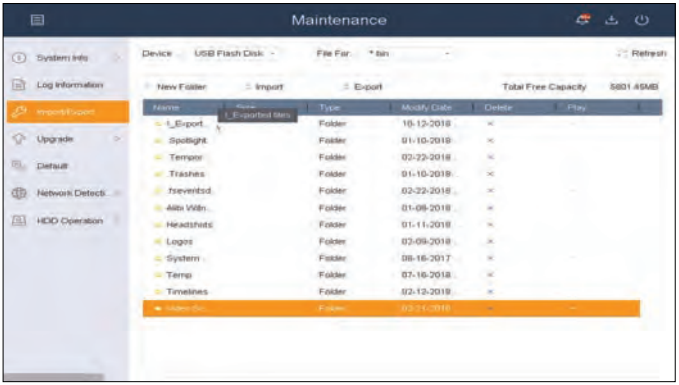


6. Click **Back**, and then remove the flash drive from the NVR.

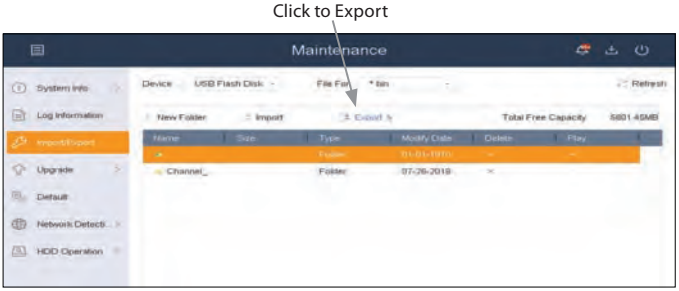
11.3 Export system configuration

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 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).



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.

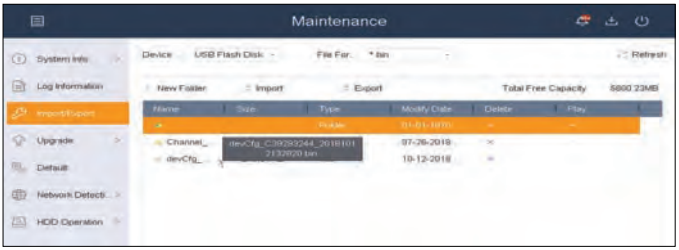




7. A Note popup window will show the export status.



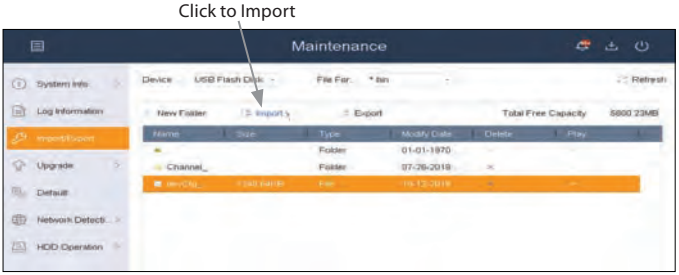
8. You can hover the mouse over the file to see the filename.



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.

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



3. 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.





4. After the configuration file is imported, a system reboot is required. Follow the on-screen instructions to complet 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.**

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

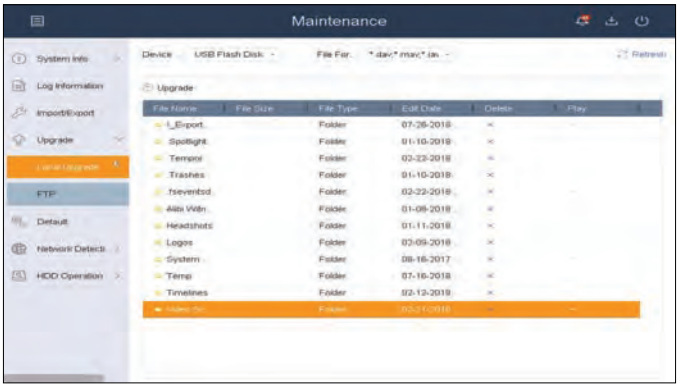


2. Find the firmware version of your recorder on the **Device Info** screen. If a newer version exists, you can install it from a local flash drive or from a server.

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, the 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 and FTP server, do the following:

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



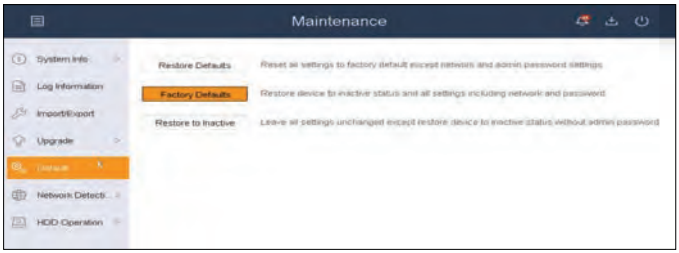
2. Click in the FTP Server Address field to open the virtual keyboard, and then enter the IP address of the server.
3. Click the **Upgrade** button at the bottom of the window, and follow the on-screen instructions to complete the upgrade.

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

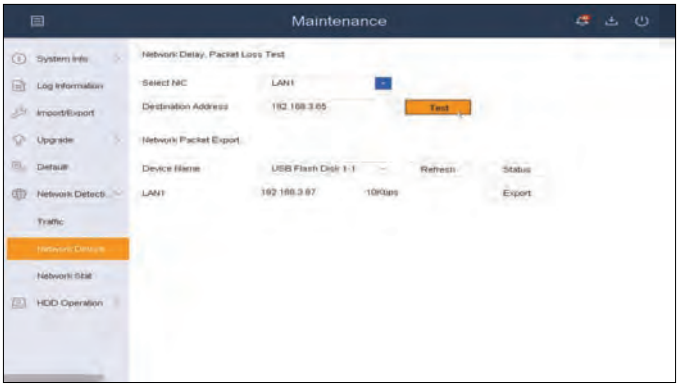
You can see real-time information of your NVR network traffic, such as linking status, MTU, sending / receiving rate, etc. The traffic data is refreshed every 1 second.

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**.



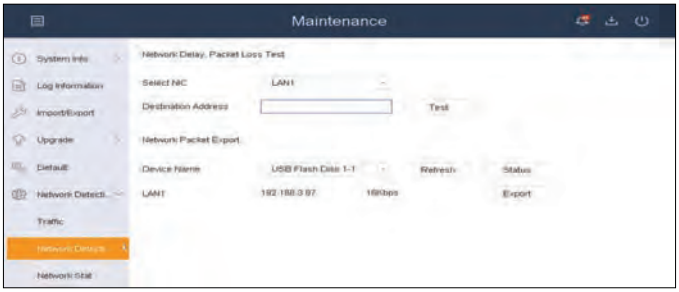
2. Click on the Destination Address field, and then enter the destination IP address the field. In the screen above, the address **192.168.3.65** was entered.
3. Click the **Test** button to begin the test for network delay and packet loss. The testing result appear in the window. If the testing failed,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

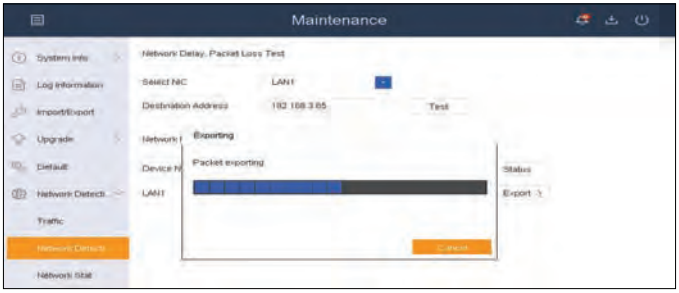
1. Open the Network Traffic menu. Go to **Menu | Maintenance | Net Detect | Net Detection**.



2. 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**.
3. 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.

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



5. 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:

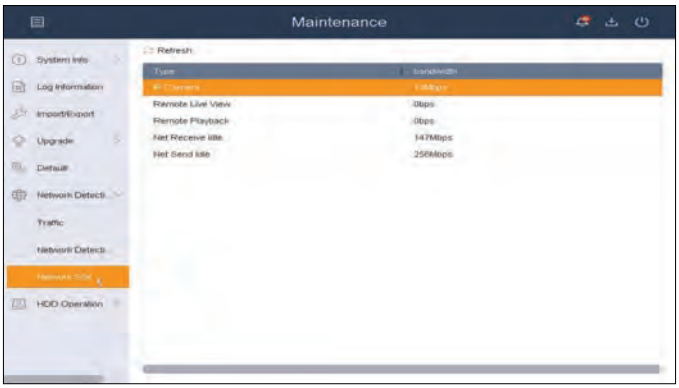
Menu | Maintenance | System Info | Network.



11.7.5 Checking Network Statistics

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

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.

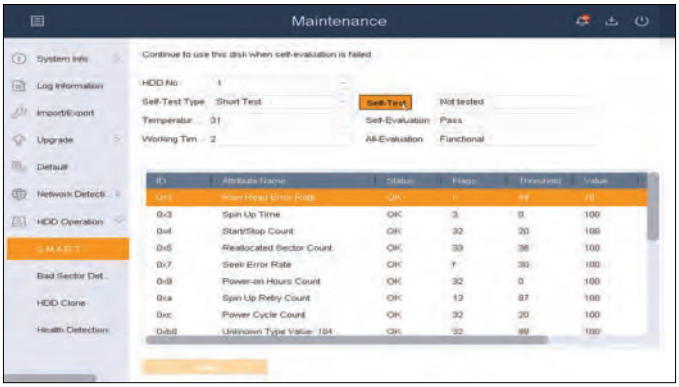


Use this display to check the bandwidth of the IP Camera, bandwidth of Remote Live View, bandwidth of Remote Playback, bandwidth of Net Receive Idle and bandwidth of Net Send Idle. Click the **Refresh** button to show the current status.

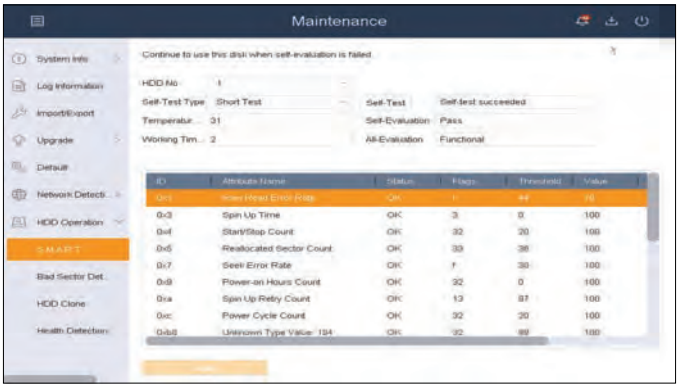
11.7.6 HDD - S.M.A.R.T. testing and monitoring

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.

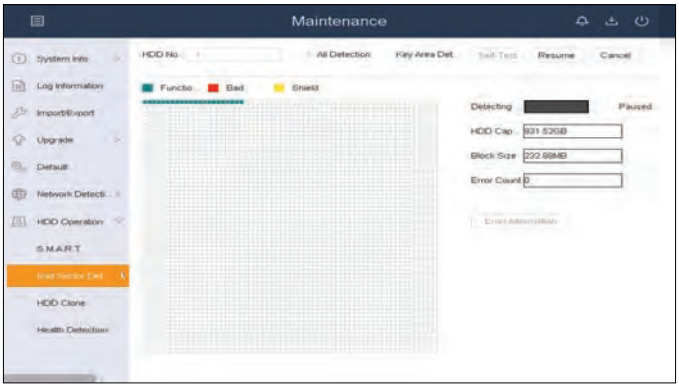


3. Examine the S.M.A.R.T. data provided for the HDD. Check to ensure that the data in the value and Worst column does not exceed the data in the Threshold column.

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

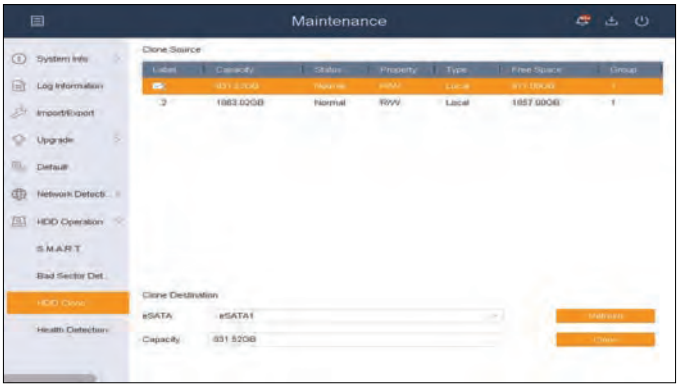
The Disk Clone feature is used to copy an internal HDD to a writable storage device connected to the eSATA port. The capacities of the source drive (internal HDD) and the eSATA storage device must be the same.

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.

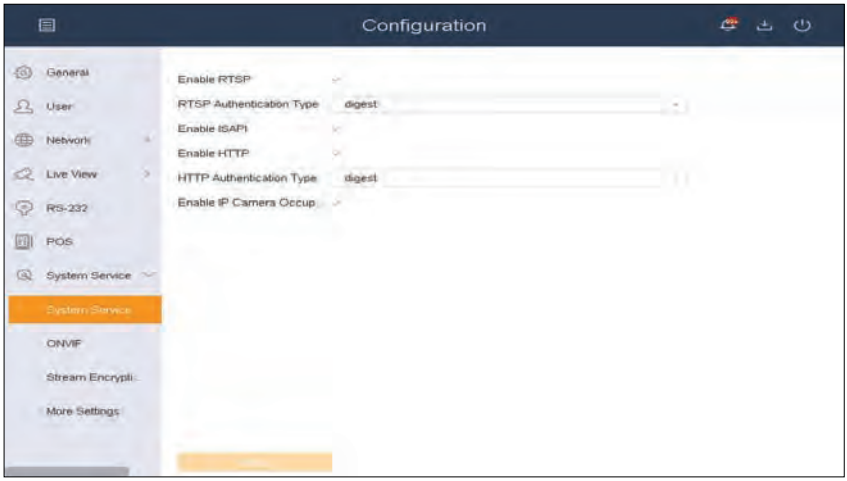
11.9 System Service options

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

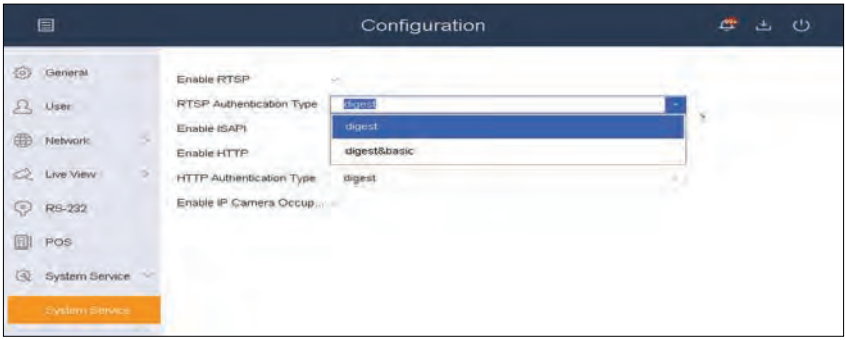
11.9.1 System Service

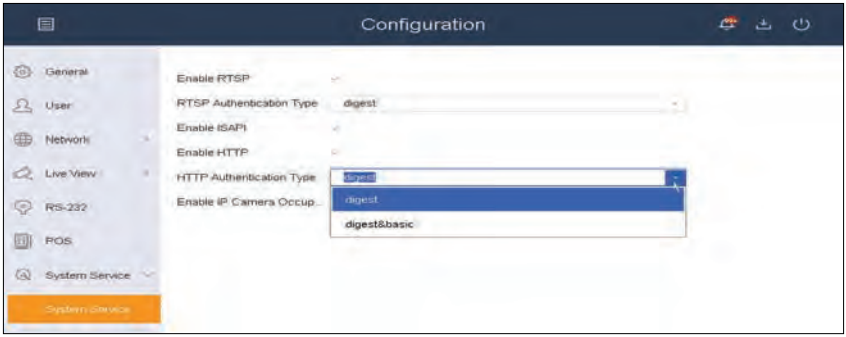
Use the System Service menu to enable/disable remote streaming and/or connectivity.

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**.

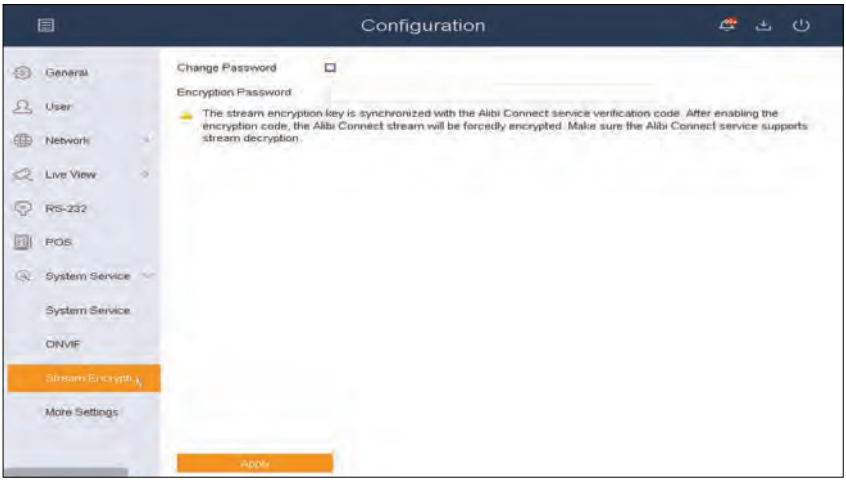


2. To enable the **ONVIF** feature, check the select box, and click **Apply**.
3. To create users who can access the device, click the **Add** button, and follow the menu to register a **User Name** and **Password**.

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

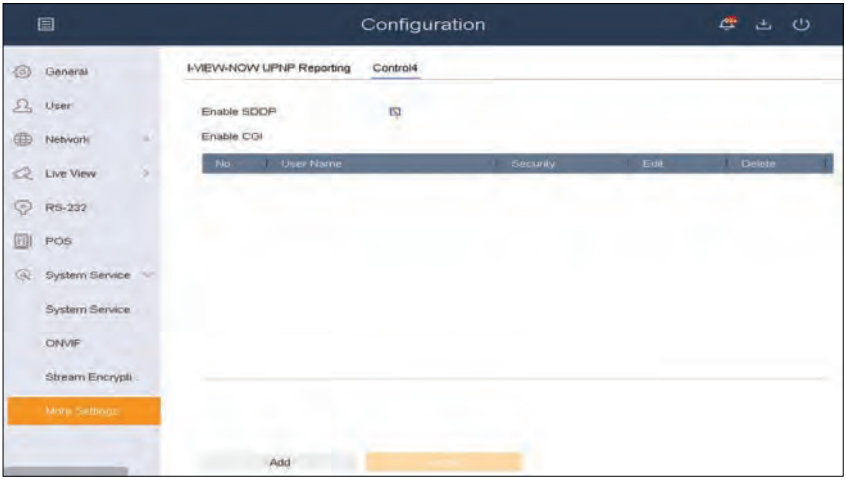
1. To open the More Settings **I-VIEW-NOW UPNP Reporting** menu, go to **Menu | Configuration | System Service | More Settings**.



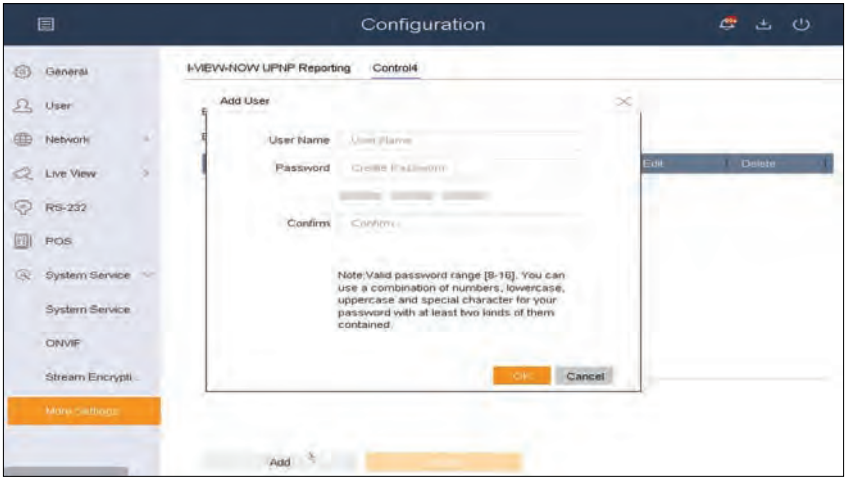
2. To use **I-VIEW-NOW UPNP Reportin**g, check the select box shown above.
3. Click **Apply**.

Control4

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



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



6. 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.



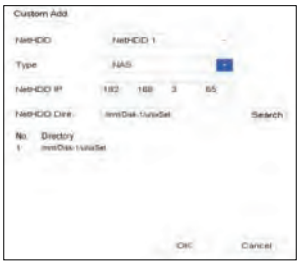
3. In the **NetHDD** drop down list, select the NetHDD ID (NetHDD 1 .. NetHDD 8) you want to add.
4. In the **Type** drop down list select either **NAS** or **IP SAN**.
5. Configure the device type you selected.

12.2.1 For a NAS disk

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

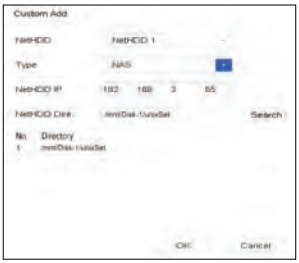
i. Click the **NetHDD IP Address** field to open a virtual keyboard and enter the IP address of the storage device.





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.



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.



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.



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

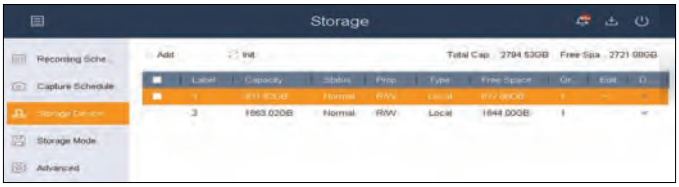
By default, all cameras will record to the one partition(s) of the internal HDD(s). However, the NVR can be configured to allocate space in one of two modes:

- **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:



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

b. Edit the **Max. Record Capacity** and the **Max. Picture Capacity** values to specify the space allocated to each. In the above screen, the **Max. Record Capacity** was set to 140GB.

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

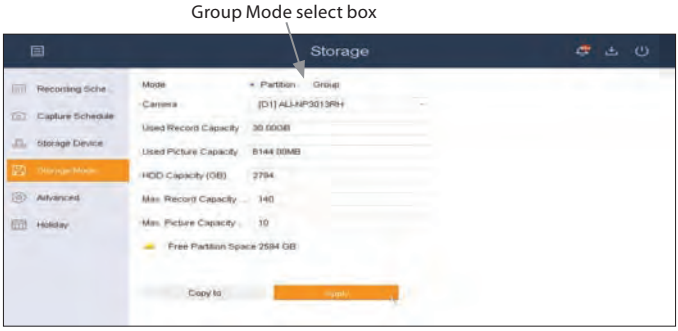
d. Repeat sub-steps a through c above for other cameras monitored by the recorder.

12.3.2 Group Mode recording

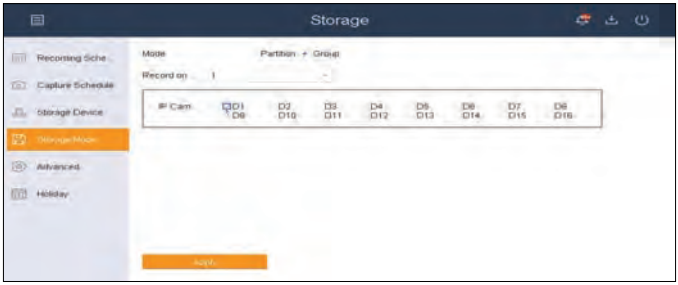
In Group Mode recording, groups of cameras can each be allocated recording space on a storage device or devices. Configuring the HDD(s) for Group recording mode requires an NVR reboot. You must have at least two HDDs (including internal and NAS / IP San HDDS added to the system) to configure 2 Groups, 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:

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



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



4. Check the box(es) for the camera(s) you want to add to the group. IP Cannel D1 was selected.

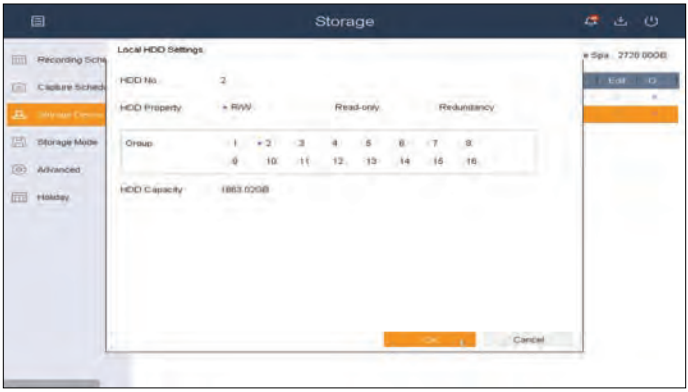
5. Click **Apply**. Since you are changing from Partition to Group, a reboot the system is required. In the Confirm box, click **Yes**, and then allow the system to fully reboot before continuing.



6. 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.



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



8. 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.



9. Open the **Storage Mode** menu.



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

Additional HDDs

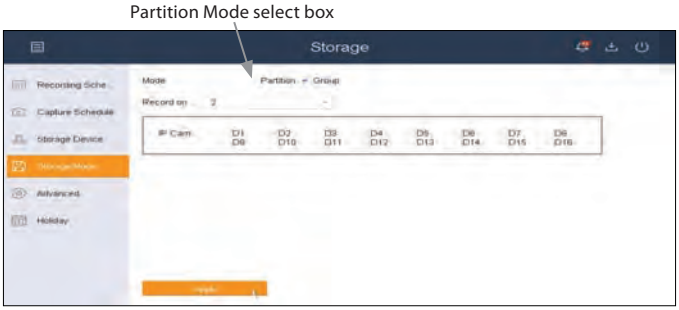
For each additional HDD on your system, click its **Edit** icon in the **Storage Device** screen. You can:

- 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:

1. Open the **Storage Mode** menu.



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**.



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.

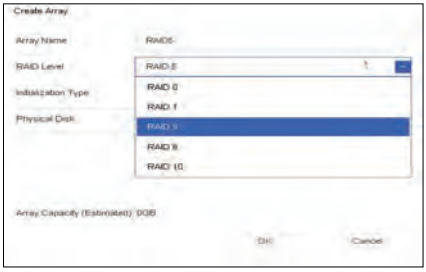


5. Click the **Create** button.



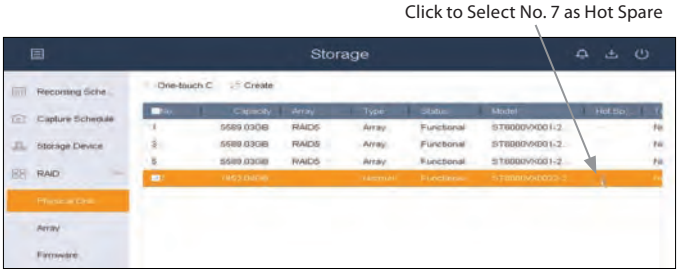
NOTE *If you click **One-touch Config**, a RAID 5 array will be created.*

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 s 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.



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.

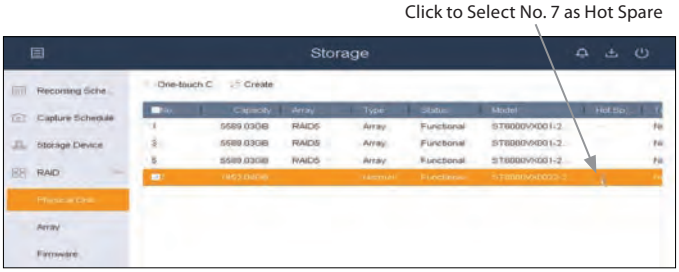


Arrays are automatically rebuilt when the array status is Degraded and a Hot Spare HDD is installed in the system.

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.



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**.



Physical disk configuration after a spare HDD is installed

4. 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.



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**.



CAUTION

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.

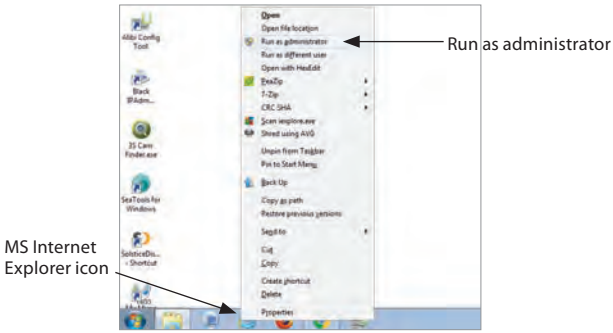
14.1 Using IE to login to the NVR

14.1.1 Configure IE to run in Administrator mode

IE must be run in administrator mode ti 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.

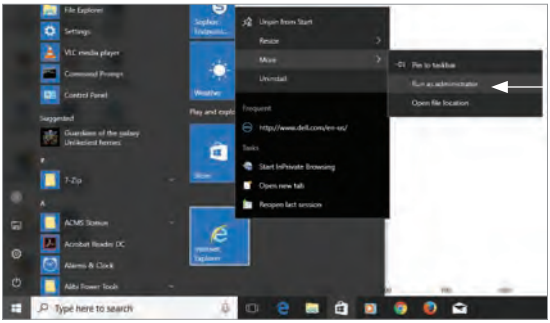


3. Click **Run as administrator** in the pop-up menu.

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**.

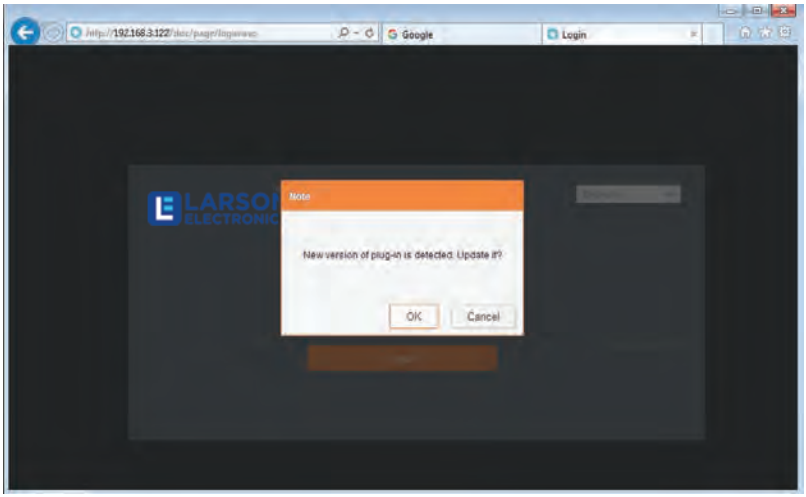
3. Right click on the Internet Explorer tile, and then select **More | Run as administrator**.



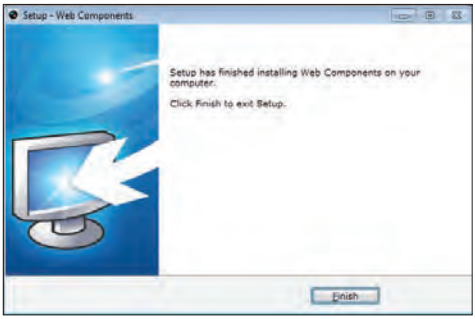
14.1.2 Login with IE

To access the NVR from a computer on the LAN:

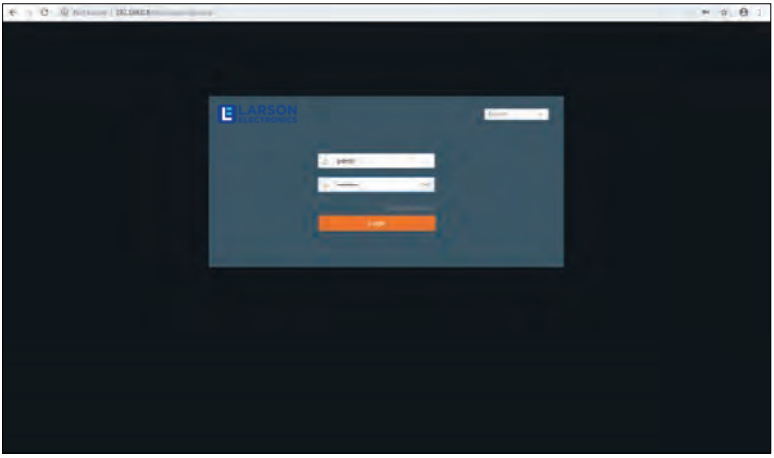
1. Open the IE browser on your remote compute and enter the IP address of the NVR in the URL field. In the example below, the IP address of the NVR is 192.168.2.122. If this is the first time you log into an Larson recorder with this version of firmware, the following screen will appear, requiring you 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.



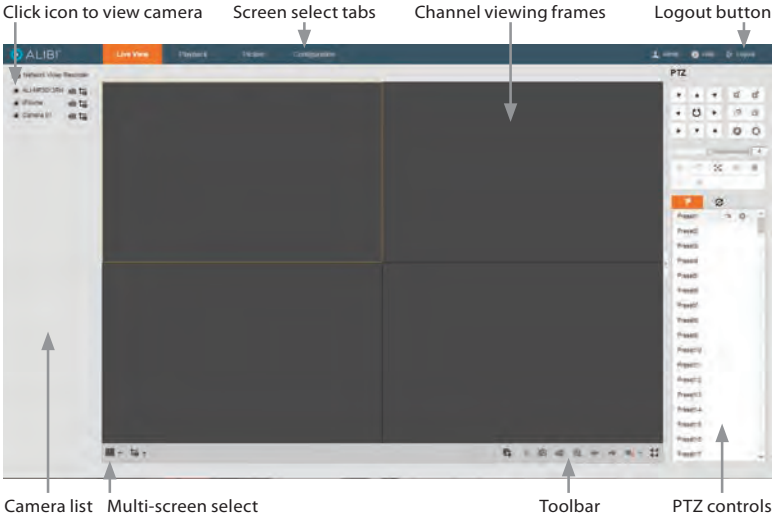
5. In the Login screen shown above, enter your *admin* username and password (see above). A **Live View** window will open.

14.2 Using Firefox or Chrome to login to the NVR

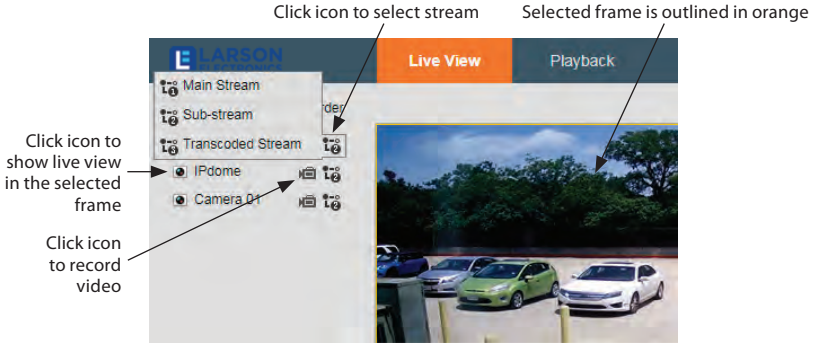
To login to the NVR with either Mozilla Firefox or Google Chrome, open the browser and enter the IP address of the NVR in the URL field. When the Login screen opens, enter your **username** and **password** in the fields shown, and then click **Login**.

14.3 Live View screen

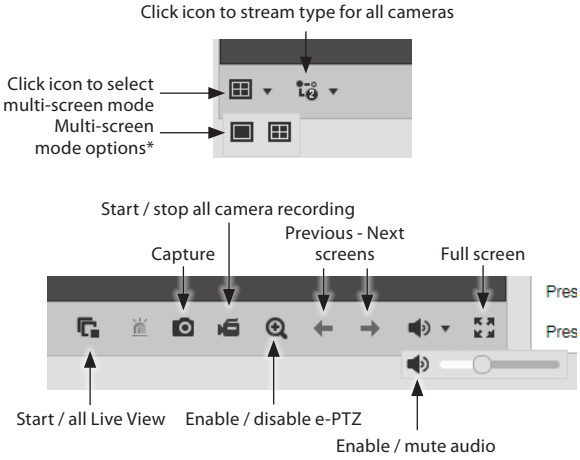
The Live View window initially appears in a multi-screen configuration with no live view images shown. The display lists only the cameras configured in the NVR. In this tab, you can change the viewing screen layout by clicking the multi-screen select button and selecting the icon for a 1 screen a 2 x 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.*



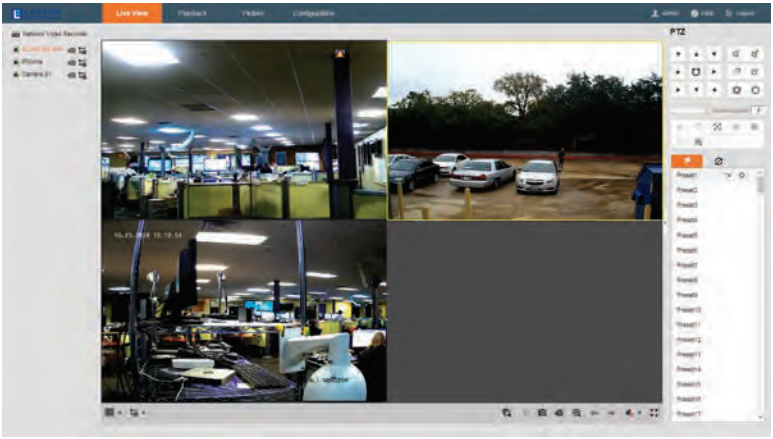
* You can view up to 4 cameras (video streams) at any time.

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).

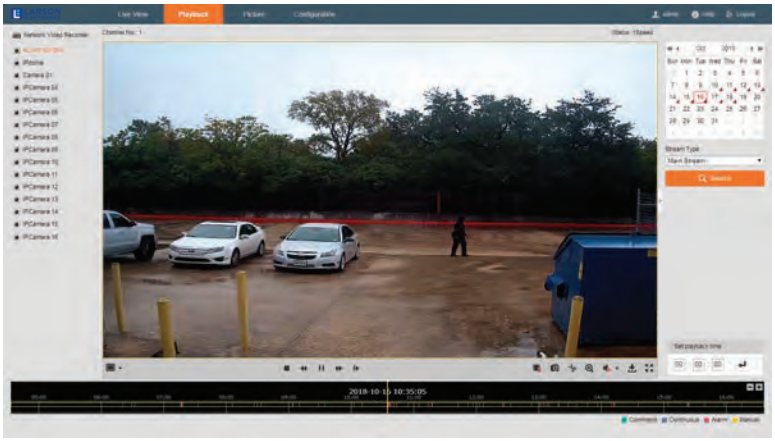
Help

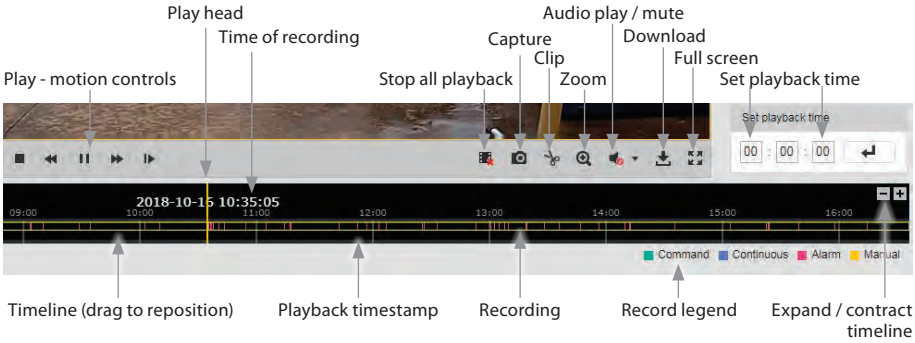
The Help button at the top of the window opens a context sensitive help screen. The screen shown below appears when selecting Help from the Playback menu.



14.4 Playback tab

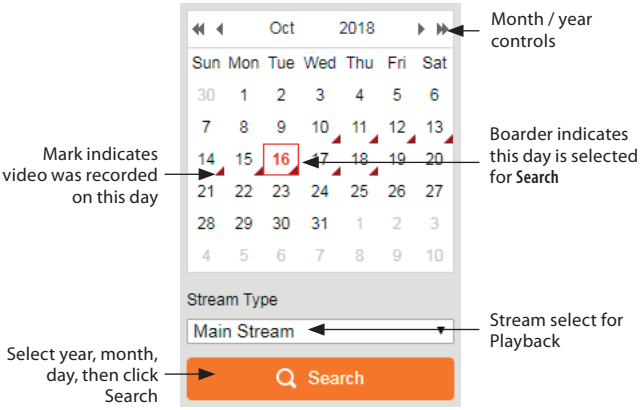
Open the Playback screen by clicking the **Playback** tab in the screen header. The Playback screen allows you to review video recorded from one camera or several cameras concurrently. Also, video files can be downloaded to your local computer.





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).

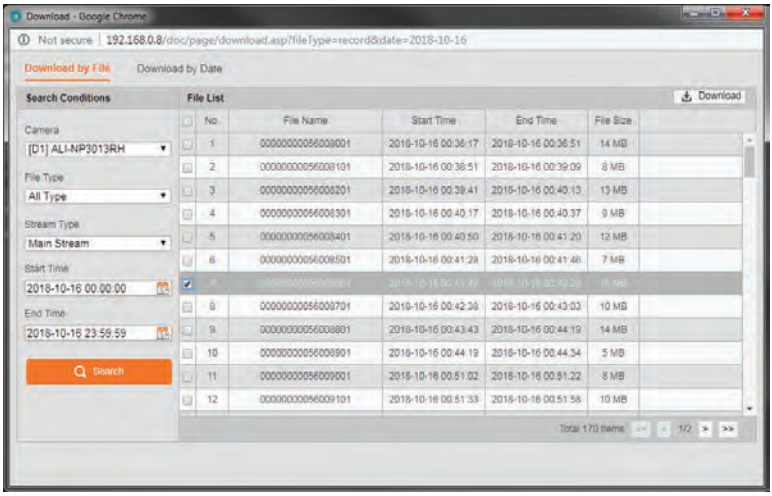


4. Click the **Stream Type** drop down list and select the video stream you want to see, and then click the **Search** button. In the example above, October 16, 2018 and Main Stream was selected.

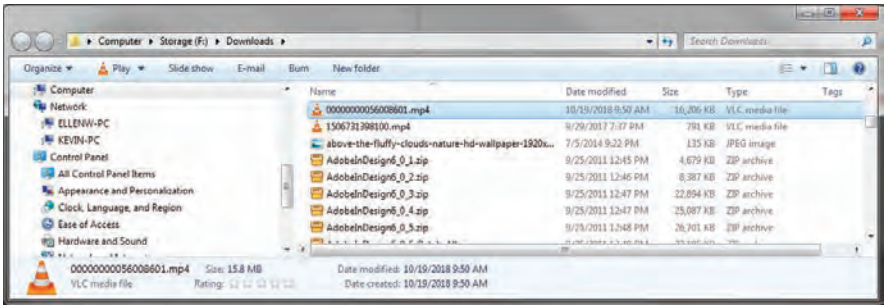
5. At the bottom of the screen, drag the timeline left or right to align the time with the play head. The condition that caused video to be recorded is indicated by a colored band on the timeline. The color legend is shown at the lower right corner of the window.
6. Click the **Play** button to begin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

To Download recorded video:

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

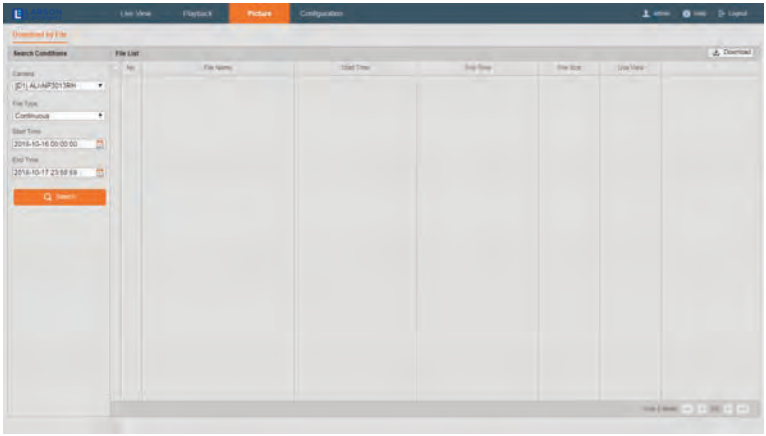


3. By default, the parameters in the search column are set to the search parameters you selected in the Playback screen. Reset the search criteria for the **Camera**, **File Type**, **Stream Type**, **Start Time** and **End Time** as needed to display files from another camera or other days and times, and then click **Search**.
4. 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.
5. 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.



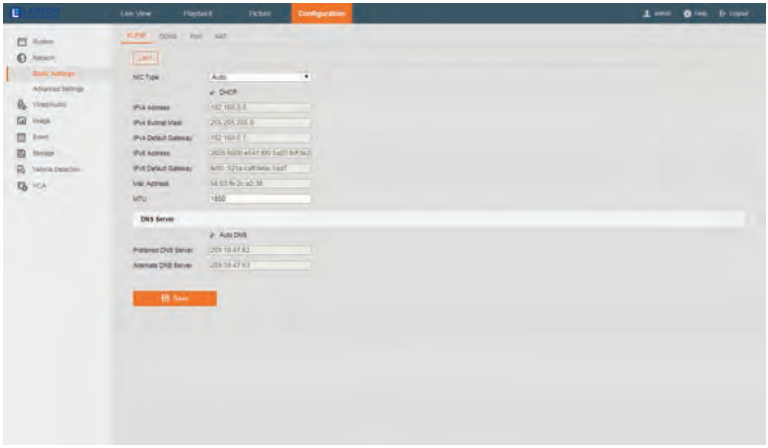
1. By default, the parameters in the search column are set to Channel D1 and the current day. Reset the search criteria for the **Camera**, **File Type** (condition causing the capture), **Start Time** and **End Time** of the search as needed to display files from another camera, conditions or other 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.

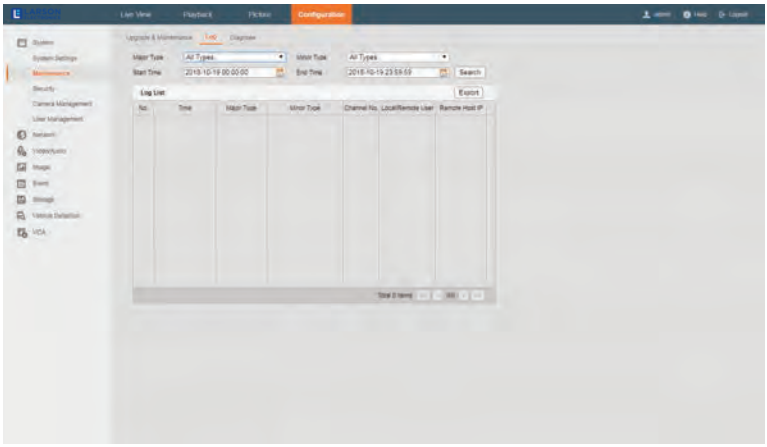
The initial configuration menu that appears is the last menu opened during a remote login, or the **System | System Settings | Basic Information** menu.



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

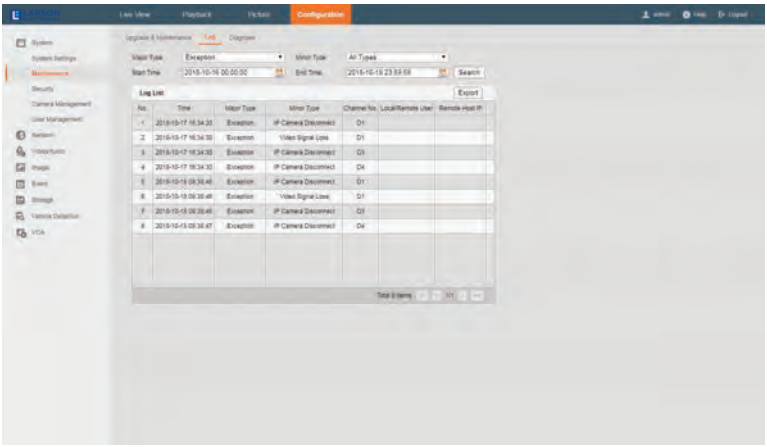
You can video system log information remotely. Open the Log screen by clicking **Configuration | System | Maintenance | Log**.



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).



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 NVF.

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 televisions 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-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

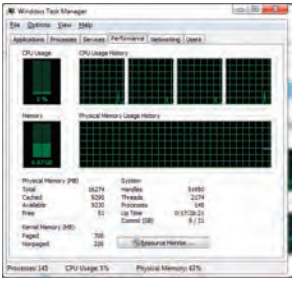
1. When image is stuck, connect the RS-232 ports on PC and the rear panel of device with the RS-232 cable.
2. Open the Super Terminal, and execute the command of "*ping 192.168.0.0 –l 1472 –f*" (the IP address may change according to the real condition), and check if there exists packet loss.

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.



Pepwave Surf SOHO User Manual

Pepwave Product:
Surf SOHO

Pepwave Firmware 7
January 2017

COPYRIGHT & TRADEMARKS
Specifications are subject to change without notice. Copyright © 2017 Pepwave Ltd. All Rights Reserved. Pepwave and the Pepwave logo are trademarks of Pepwave Ltd. Other brands or products mentioned may be trademarks or registered trademarks of their respective owners.

1 Introduction and Scope 234

2 Glossary 235

3 Product Features 237

3.1 Supported Network Features 237

3.1.1 WAN 237

3.1.2 LAN 237

3.1.3 VPN 238

3.1.4 Firewall 238

3.1.5 Outbound Policy 238

3.1.6 oS 238

3.2 Other Supported Features 238

4 Pepwave Surf SOHO Router Overview 239

4.1 Surf SOHO 239

4.1.1 Panel Appearance 239

4.1.2 LED Indicators 241

5 Advanced Feature Summary 243

5.1 oS: Clearer VoIP 243

5.2 USB Modem 244

5.3 Built-In Remote User VPN Support 244

6 Installation 245

6.1 Preparation 245

6.2 Constructing the Network 245

6.3 Configuring the Network Environment 246

7 Connecting to the Web Admin Interface 246

8 Configuring the LAN Interface(s) 248

8.1 Network Settings 248

8.2 Port Settings 256

9 Configuring the WAN Interface(s) 256

9.1 Ethernet WAN 257

 Copyright @ 2017 Pepwave

9.1.1 DHCP Connection 262
9.1.2 Static IP Connection 262
9.1.3 PPPoE Connection 262
9.1.4 L2TP Connection 264
9.2 Wi-Fi WAN 266
9.2.1 Creating Wi-Fi Connection Profiles 274
9.3 WAN Health Check 276
9.4 Dynamic DNS Settings 279

10 PepVPN 281
10.1 Outbound Policy Management 284
10.1.1 Outbound Policy 284
10.1.2 Custom Rules for Outbound Policy 285

11 Port Forwarding 288
11.1 UPnP / NAT-PMP Settings 290

12 NAT Mappings 291

13 QoS 293
13.1 Bandwidth Control 293
13.2 Application 293
13.2.1 Application Prioritization 293
13.2.2 Prioritization for Custom Applications 294
13.2.3 DSL/Cable Optimization 294

14 Firewall 294
14.1 Outbound and Inbound Firewall Rules 295
14.1.1 Access Rules 295
14.1.2 Apply Firewall Rules to PepVpn Traffic 298
14.1.3 Intrusion Detection and DoS Prevention 299
14.2 Content Blocking 300
14.2.1 Application Blocking 300
14.2.2 Web Blocking 301
14.2.3 Exempted Subnets 301

 Copyright @ 2017 Pepwave

14.2.4 URL Logging 301

15 OSPF & RIPv2 301

16 Miscellaneous 303

16.1 Remote User Access 303
16.2 PPTP Server 305
16.3 Certificate Manager 307
16.4 Service Forwarding 307
16.4.1 SMTP Forwarding 308
16.4.2 Web Proxy Forwarding 309
16.4.3 DNS Forwarding 309
16.4.4 Custom Service Forwarding 309
16.5 Service Passthrough 310
16.6 Sim Toolkit 311

17 AP 311

17.1 Wireless SSID 311
17.2 Settings 314

18 System Settings 316

18.1 Admin Security 317
18.2 Firmware 320
18.3 Time 321
18.4 Schedule 321
18.5 Email Notification 322
18.6 Event Log 324
18.7 SNMP 325
18.8 InControl 328
18.9 Configuration 328
18.10 Feature Add-ons 329
18.11 Reboot 330

19 Tools 330

19.1 Ping 330

 Copyright @ 2017 Pepwave

19.2 Traceroute Test 331
19.3 Wake-on-LAN 332

20 Status 332
20.1 Device 332
20.2 Active Sessions 334
20.3 Client List 336
20.4 Event Log 337
20.5 Bandwidth 337
20.5.1 Real Time 337
20.5.2 Hourly 338
20.5.3 Daily 339
20.5.4 Monthly 340

Appendix A: Restoration of Factory Defaults 342

Appendix B: Declaration 342

 Copyright @ 2017 Pepwave

1 Introduction and Scope

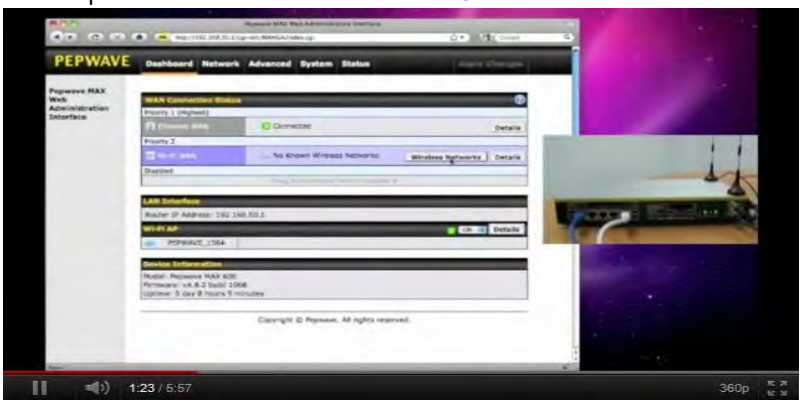
The Surf SOHO is a professional-grade router that is secure, reliable, and easy to use.

With the Surf SOHO, you can connect to the Internet using a USB cellular modem, Ethernet, or Wi-Fi. Hook the Surf SOHO up to Ethernet and Cellular connections, and it will automatically fail over from one to the other as needed. That way, you can stay connected even when a connection breaks

This manual covers setting up Surf SOHO router and provides an introduction to their features and usage.

Tips

Want to know more about Pepwave routers Visit our YouTube Channel for a video introduction



http://youtu.be/UCkV ThLKO4

 Copyright @ 2017 Pepwave

2 Glossary

The following terms, acronyms, and abbreviations are frequently used in this manual:

Term	Definition
3G	3rd Generation standards for wireless communications
4G	4th Generation standards for wireless communications
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EVDO	Evolution-Data Optimized
HSDPA	High-Speed Downlink Packet Access
HTTP	Hyper-Text Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
LAN	Local Area Network
MAC Address	Media Access Control Address
MTU	Maximum Transmission Unit
MSS	Maximum Segment Size
NAT	Network Address Translation

 Copyright @ 2017 Pepwave

PPPoE	Point to Point Protocol over Ethernet
oS	uality of Service
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WINS	Windows Internet Name Service
WLAN	Wireless Local Area Network

 Copyright @ 2017 Pepwave

3 Product Features

Pepwave routers enable all LAN users to share broadband Internet connections, and they provide advanced features to enhance Internet access. Our Surf SOHO routers support one Ethernet, one USB 4G LTE/3G WAN, and Wi-Fi as WAN for failover

It also includes three SMA dual-band antennas that allows better reliability, larger bandwidth, and increased wireless coverage.

Below is a list of supported features on Pepwave routers. Features vary by model. For more information, please see peplink.com/products.

3.1 Supported Network Features

3.1.1 WAN

Ethernet WAN connection in full/half duplex
Static IP support for PPPoE
USB mobile connection(s)
Wi-Fi WAN connection
Network address translation (NAT)/port address translation (PAT)
Inbound and outbound NAT mapping
IPsec NAT-T and PPTP packet pass through
Intelligent Failover
MAC address clone and passthrough
Customizable MTU and MSS values
WAN connection health check
Dynamic DNS (supported service providers: changeip.com, dyndns.org, no-ip.org, tzo.com and DNS-O-Matic)
Ping, DNS lookup, and HTTP-based health check

3.1.2 LAN

Wi-Fi AP
Ethernet LAN ports
DHCP server on LAN

 Copyright @ 2017 Pepwave

Extended DHCP option support
Static routing rules
VLAN on LAN support

3.1.3 VPN

Site-to-Site VPN
256-bit AES Encryption
Dynamic Routing
Pre-shared key authentication
PPTP/L2TP VPN server

3.1.4 Firewall

Outbound (LAN to WAN) firewall rules
Inbound (WAN to LAN) firewall rules per WAN connection
Intrusion detection and prevention
Specification of NAT mappings
Outbound firewall rules can be defined by destination domain name

3.1.5 Outbound Policy

Link load distribution per TCP/UDP service
Persistent routing for specified source and/or destination IP addresses per TCP/UDP service
Traffic prioritization and DSL optimization
Prioritize and route traffic to VPN tunnels with Priority and Enforced algorithms

3.1.6 QoS

Quality of service for different applications and custom protocols
User group classification for different service levels
Bandwidth usage control and monitoring on group- and user-level
Application prioritization for custom protocols and DSL/cable optimization

3.2 Other Supported Features

User-friendly web-based administration interface
HTTP and HTTPS support for web admin interface

 Copyright @ 2017 Pepwave

Configurable web administration port and administrator password
Firmware upgrades, configuration backups, ping, and traceroute via web admin interface
Remote web-based configuration (via WAN and LAN interfaces)
Time server synchronization
SNMP
Email notification
Read-only user for web admin
Shared IP drop-in mode
Authentication and accounting by RADIUS server for web admin
Syslog
SIP passthrough
PPTP packet pass through
Event log
Active sessions
Client list
UPnP / NAT-PMP
Real-time, hourly, daily, and monthly bandwidth usage reports and charts
IPv6 support

4 Pepwave Surf SOHO Router Overview

4.1 Surf SOHO

4.1.1 Panel Appearance

 Copyright @ 2017 Pepwave



Specifications	
WAN Interface	1x 100/1000M Ethernet Port 1x USB 2.0 Interface Wi-Fi as WAN
LAN Interface	4x 100/1000M Ethernet Ports Simultaneous Dual-Band 11ac Wi-Fi AP
Wi-Fi AP Operating Frequency	2412 2472 MHz and 5180 - 5825 MHz

 Copyright @ 2017 Pepwave

Wi-Fi Antenna	3x External Wi-Fi Antenna
Recommended Users	1-25
Router Throughput	120Mbps
Number of PPTP VPN Users	3
Number of PPTP VPN Users	2
Power Input	DC ack: 10V 24VDC AC Adapter: AC Input 100V 240V, DC Output 12V, 1.5A
Power Consumption	26W (max) with USB WAN 22W (max) without USB WAN
Dimensions	9.17 x 5.6 x 1.18 inch 233 x 142 x 30 mm
Weight	0.86 pounds 388 grams
Operating Temperature	-14 113 F -10 45 C
Humidity	15 95 (non-condensing)
Certifications	FCC, CE, RoHS
Warranty	1-Year Limited Warranty

4.1.2 LED Indicators

The statuses indicated by the front panel LEDs are as follows:

Wi-Fi and Status Indicators		
Wi-Fi	OFF	Disabled Intermittent

 Copyright @ 2017 Pepwave

	Blinking	Enabled but no client connected
	ON	Client(s) connected to wireless network
	Continuous blinking	Transferring data to wireless network
Status	OFF	System initializing
	Red	Booting up or busy
	Green	Ready state

LAN and Ethernet WAN Ports		
Green LED	ON	10 / 100 / 1000 Mbps
Orange LED	Blinking	Data is transferring
	OFF	No data is being transferred or port is not connected
Port type	Auto MDI/MDI-X ports	

Wi-Fi Signal	
Off	No connection
Signal strength	Wi-Fi signal strength (low, medium, and high)

 Copyright @ 2017 Pepwave

5 Advanced Feature Summary

5.1 QoS: Clearer VoIP



VoIP and videoconferencing are highly sensitive to latency. With QoS, Peplink routers can detect VoIP traffic and assign it the highest priority, giving you crystal-clear calls.

 Copyright @ 2017 Pepwave

5.2 USB Modem



For increased WAN diversity, plug in a USB LTE modem as backup. Peplink routers are compatible with over 200 modem types.

5.3 Built-In Remote User VPN Support



Use L2TP with IPsec to safely and conveniently connect remote clients to your private network. L2TP with IPsec is supported by most devices, but legacy devices can also connect using PPTP.

 Copyright @ 2017 Pepwave

Click here for full instructions on setting up L2TP with IPsec.

6 Installation

The following section details connecting Pepwave routers to your network.

6.1 Preparation

Before installing your Pepwave router, please prepare the following as appropriate for your installation:

At least one Internet/WAN access account and/or Wi-Fi access information
Depending on network connection type(s), one or more of the following:
Ethernet WAN: A 10/100/1000BaseT UTP cable with R 45 connector
USB: A USB modem
Embedded modem: A SIM card for GSM/HSPA service
Wi-Fi WAN: Wi-Fi antennas
PC Card/Express Card WAN: A PC Card/ExpressCard for the corresponding card slot
A computer installed with the TCP/IP network protocol and a supported web browser. Supported browsers include Microsoft Internet Explorer 8.0 or above, Mozilla Firefox 10.0 or above, Apple Safari 5.1 or above, and Google Chrome 18 or above.

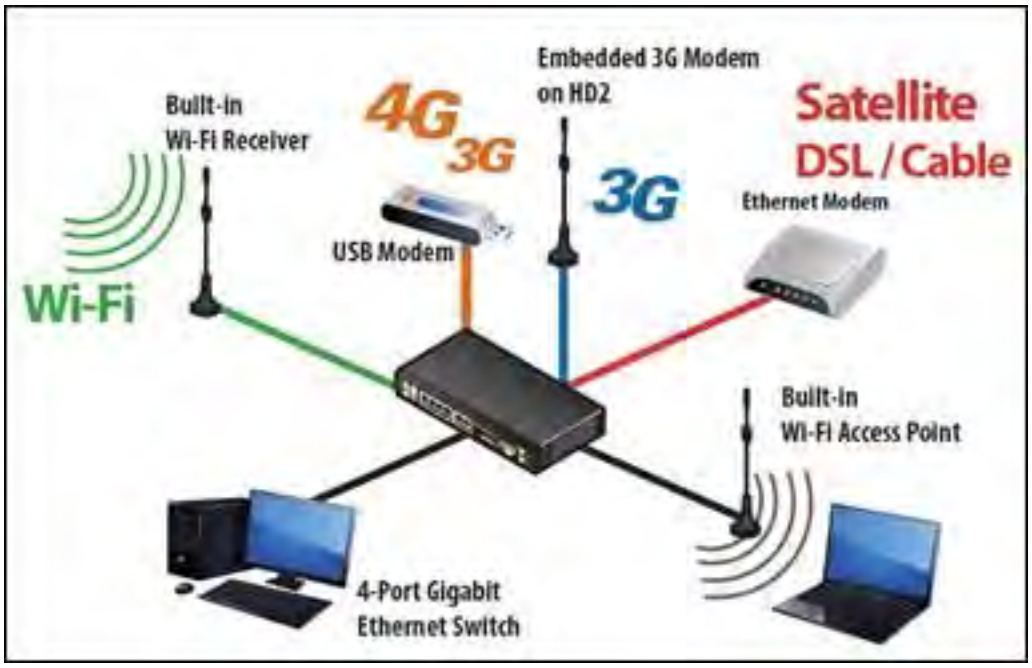
6.2 Constructing the Network

At a high level, construct the network according to the following steps:

1. With an Ethernet cable, connect a computer to one of the LAN ports on the Pepwave router. Repeat with different cables for up to 4 computers to be connected.
2. With another Ethernet cable or a USB modem/Wi-Fi antenna/PC Card/Express Card, connect to one of the WAN ports on the Pepwave router. Repeat the same procedure for other WAN ports.
3. Connect the power adapter to the power connector on the rear panel of the Pepwave router, and then plug it into a power outlet.

The following figure schematically illustrates the resulting configuration:

 Copyright @ 2017 Pepwave

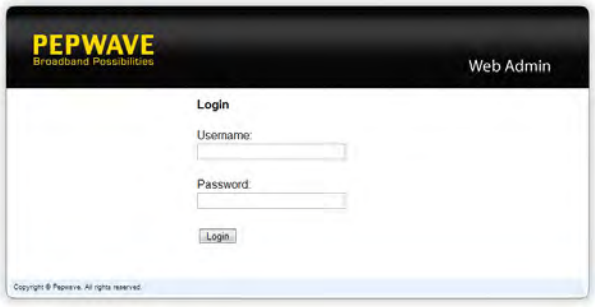


6.3 Configuring the Network Environment

To ensure that the Pepwave router works properly in the LAN environment and can access the Internet via WAN connections, please refer to the following setup procedures:
LAN configuration
For basic configuration, refer to Section 8, Connecting to the Web Admin Interface.
For advanced configuration, go to Section 9, Configuring the LAN Interface(s).
WAN configuration
For basic configuration, refer to Section 8, Connecting to the Web Admin Interface.
For advanced configuration, go to Section 9.2, Captive Portal.

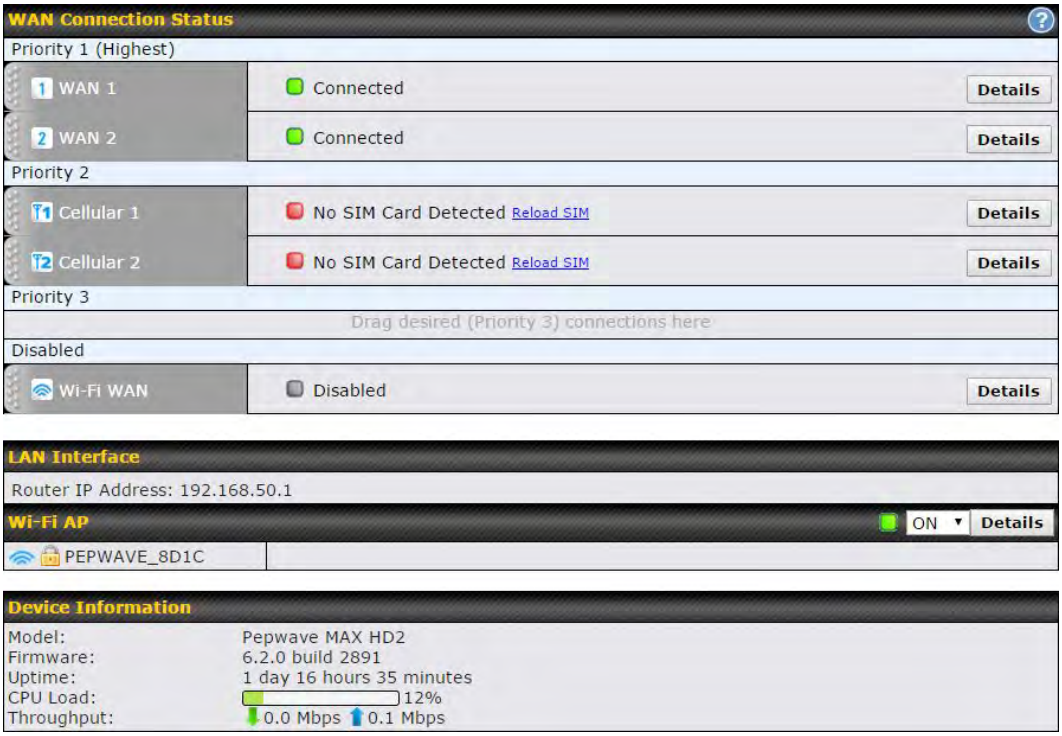
7 Connecting to the Web Admin Interface

1. Start a web browser on a computer that is connected with the Pepwave router through the LAN.
2. To connect to the router's web admin interface, enter the following LAN IP address in the address field of the web browser:
   http://192.168.50.1
   (This is the default LAN IP address for Pepwave routers.)



 Copyright @ 2017 Pepwave

3. Enter the following to access the web admin interface.
   Username: admin
   Password: admin
   (This is the default username and password for Pepwave routers. The admin and read-only user passwords can be changed at **System>Admin Security**.)
4. After successful login, the **Dashboard** will be displayed.



The **Dashboard** shows current WAN, LAN, and Wi-Fi AP statuses. Here, you can change WAN connection priority and switch on/off the Wi-Fi AP.

Device Information displays details about the device, including model name, firmware version, and uptime.

Important Note
Configuration changes (e.g. WAN, LAN, admin settings, etc.) will take effect only after clicking the **Save** button at the bottom of each page. The **Apply Changes** button causes the changes to be saved and applied.

 Copyright @ 2017 Pepwave

8 Configuring the LAN Interface(s)

8.1 Network Settings

LAN interface settings are located at **Network>LAN>Network Settings**. Navigating to that page will result in the following dashboard:



This represents the LAN interfaces that are active on your router (including VLAN). A grey X means that the VLAN is used in other settings and cannot be deleted. You can find which settings are using the VLAN by hovering over the grey X .

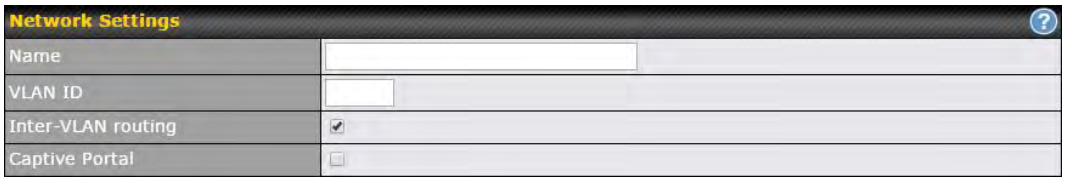
Alternatively, a red X means that there are no settings using the VLAN. You can delete that VLAN by clicking the red X

Clicking any of the existing LAN interfaces (or creating a new one) will result in the following

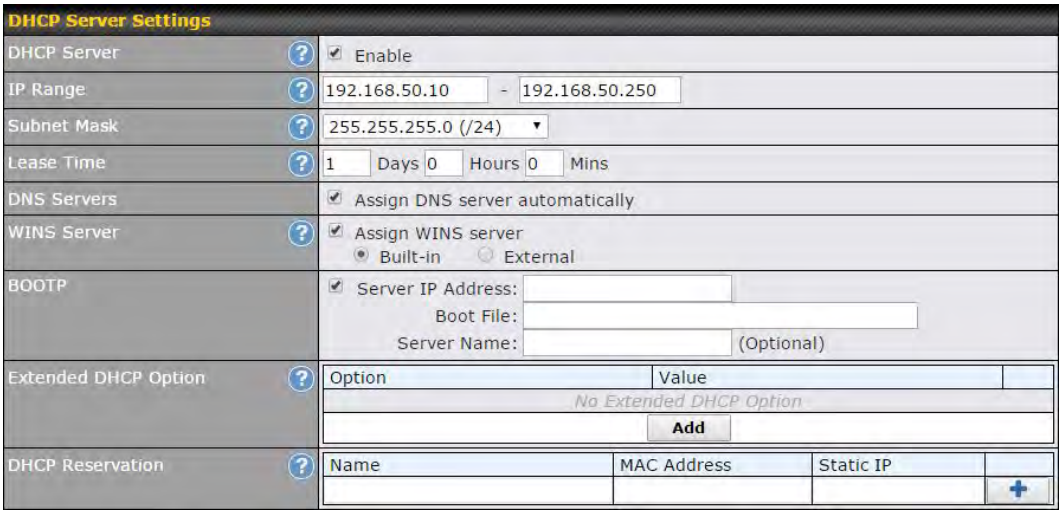


IP Settings	
IP Address	The IP address and subnet mask of the Pepwave router on the LAN.

 Copyright @ 2017 Pepwave



Network Settings	
Name	Enter a name for the LAN.
VLAN ID	Enter a number for your VLAN.
Inter-VLAN routing	Check this box to enable routing between virtual LANs.



DHCP Server Settings	
DHCP Server	When this setting is enabled, the DHCP server automatically assigns an IP address to each computer that is connected via LAN and configured to obtain an IP address via DHCP. The Pepwave router s DHCP server can prevent IP address collision on the LAN.
IP Range &	These settings allocate a range of IP addresses that will be assigned to LAN computers

 Copyright @ 2017 Pepwave

Subnet Mask	by the Pepwave router s DHCP server.
Lease Time	This setting specifies the length of time throughout which an IP address of a DHCP client remains valid. Upon expiration of the lease time, the assigned IP address will no longer be valid and renewal of the IP address assignment will be required.
DNS Servers	This option allows you to input the DNS server addresses to be offered to DHCP clients. If **Assign DNS server automatically** is selected, the Pepwave router s built-in DNS server address (i.e., LAN IP address) will be offered.
WINS Server	This option allows you to optionally specify a Windows Internet Name Service (WINS) server. You may choose to use the **built-in WINS server** or **external WINS servers**. When this unit is connected using SpeedFusion™, other VPN peers can share this unit's built-in WINS server by entering this unit's LAN IP address in their DHCP **WINS Server** setting. Afterward, all PC clients in the VPN can resolve the NetBIOS names of other clients in remote peers. If you have enabled this option, a list of WINS clients will be displayed at **Status>WINS Clients**.
BOOTP	Check this box to enable BOOTP on older networks that still require it.
Extended DHCP Option	In addition to standard DHCP options (e.g., DNS server address, gateway address, subnet mask), you can specify the value of additional extended DHCP options, as defined in RFC 2132. With these extended options enabled, you can pass additional configuration information to LAN hosts. To define an extended DHCP option, click the **Add** button, choose the option to define and enter its value. For values that are in IP address list format, you can enter one IP address per line in the provided text area input control. Each option can be defined once only.
DHCP Reservation	This setting reserves the assignment of fixed IP addresses for a list of computers on the LAN. The computers to be assigned fixed IP addresses on the LAN are identified by their MAC addresses. The fixed IP address assignment is displayed as a cross-reference list between the computers names, MAC addresses, and fixed IP addresses. **Name** (an optional field) allows you to specify a name to represent the device. MAC addresses should be in the format of **00:AA:BB:CC:DD:EE**. Press  to create a new record. Press  to remove a record. Reserved client information can be imported from the **Client List**, located at **Status>Client List**. For more details, please refer to **Section 22.3.**

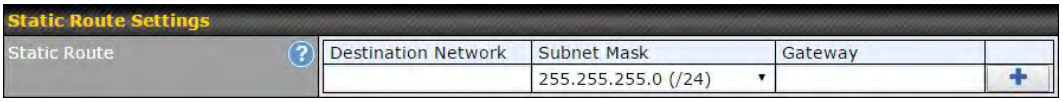


LAN Physical Settings

 Copyright @ 2017 Pepwave

Speed

This is the port speed of the LAN interface. It should be set to the same speed as the connected device to avoid port negotiation problems. When a static speed is set, you may choose whether to advertise its speed to the peer device. **Auto** is selected by default. You can choose not to advertise the port speed if the port has difficulty negotiating with the peer device.

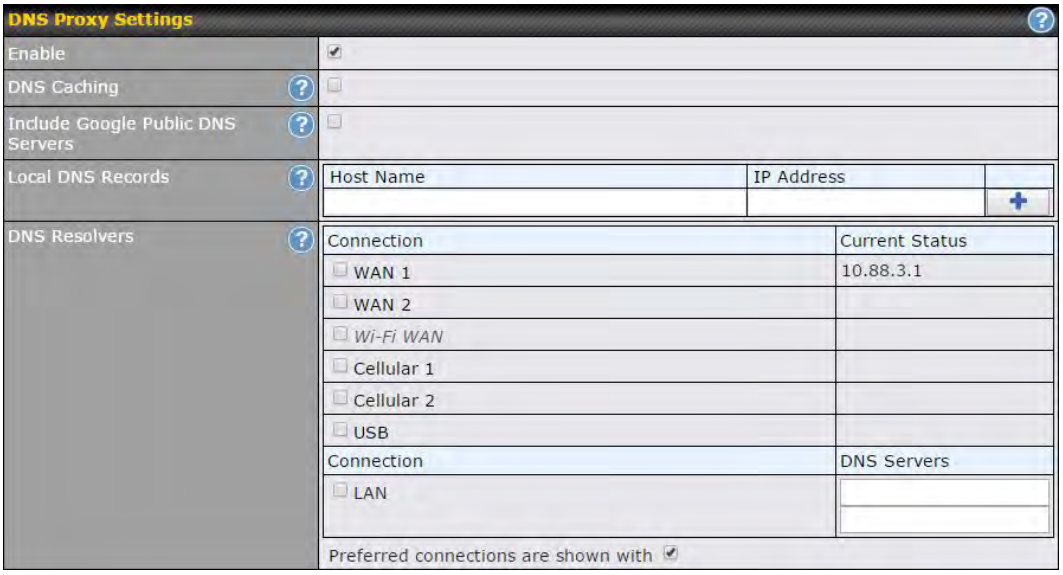


Static Route Settings

Static Route

This table is for defining static routing rules for the LAN segment. A static route consists of the network address, subnet mask, and gateway address. The address and subnet mask values are in *w.x.y.z* format.

The local LAN subnet and subnets behind the LAN will be advertised to the VPN. Remote routes sent over the VPN will also be accepted. Any VPN member will be able to route to the local subnets. Press  to create a new route. Press  to remove a route.



 Copyright @ 2017 Pepwave

DNS Proxy Settings	
Enable	To enable the DNS proxy feature, check this box, and then set up the feature at **Network>LAN>DNS Proxy Settings**. A DNS proxy server can be enabled to serve DNS requests originating from LAN/PPTP/SpeedFusion™ peers. Requests are forwarded to the **DNS servers/resolvers** defined for each WAN connection.
DNS Caching	This field is to enable DNS caching on the built-in DNS proxy server. When the option is enabled, queried DNS replies will be cached until the records TTL has been reached. This feature can help improve DNS lookup time. However, it cannot return the most up-to-date result for those frequently updated DNS records. By default, **DNS Caching** is disabled.
Include Google Public DNS Servers	When this option is **enabled**, the DNS proxy server will also forward DNS requests to Google's Public DNS Servers, in addition to the DNS servers defined in each WAN. This could increase the DNS service's availability. This setting is disabled by default.
Local DNS Records	This table is for defining custom local DNS records. A static local DNS record consists of a host name and IP address. When looking up the host name from the LAN to LAN IP of the Pepwave router, the corresponding IP address will be returned. Press  to create a new record. Press  to remove a record.
DNS Resolvers [A]	Check the box to enable the WINS server. A list of WINS clients will be displayed at **Network>LAN>DNS Proxy Settings>DNS Resolvers**. This field specifies which DNS resolvers will receive forwarded DNS requests. If no WAN/VPN/LAN DNS resolver is selected, all of the WAN s DNS resolvers will be selected. If a SpeedFusion™ peer is selected, you may enter the VPN peer s DNS resolver IP address(es). ueries will be forwarded to the selected connections resolvers. If all of the selected connections are down, queries will be forwarded to all resolvers on healthy WAN connections.

[A] - Advanced feature, please click the  button on the top right hand corner to activate.

To enable VLAN configuration, click the  button in the **IP Settings** section.



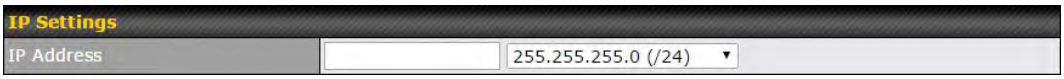
To add a new LAN, click the **New LAN** button. To change LAN settings, click the name of the LAN to change under the **LAN** heading.

 Copyright @ 2017 Pepwave



The following settings are displayed when creating a new LAN or editing an existing LAN.



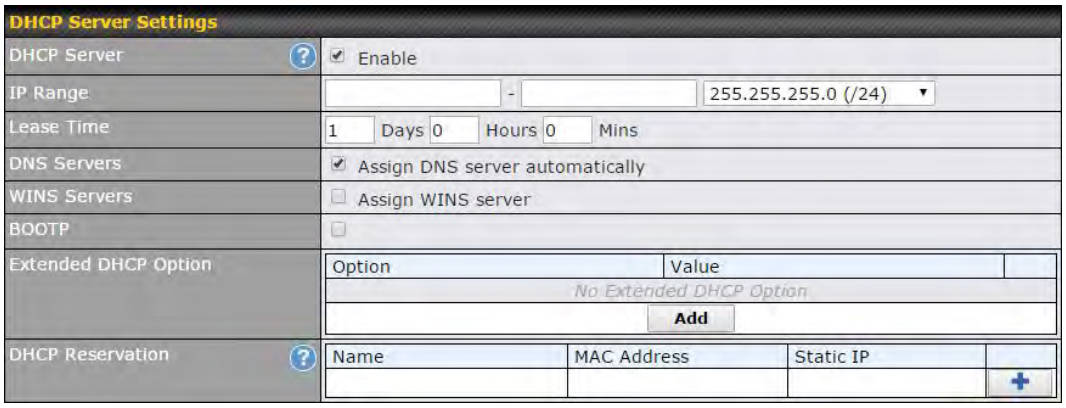


IP Settings	
IP Address & Subnet Mask	Enter the Pepwave router s IP address and subnet mask values to be used on the LAN.



Network Settings	
Name	Enter a name for the LAN.
VLAN ID	Enter a number for your VLAN.
Inter-VLAN routing	Check this box to enable routing between virtual LANs.

 Copyright @ 2017 Pepwave



DHCP Server Settings

DHCP Server

When this setting is enabled, the Pepwave router s DHCP server automatically assigns an IP address to each computer that is connected via LAN and configured to obtain an IP address via DHCP. The Pepwave router s DHCP server can prevent IP address collisions on the LAN.

To enable DHCP bridge relay, please click the icon on this menu item.

IP Range & Subnet Mask

These settings allocate a range of IP address that will be assigned to LAN computers by the Pepwave router s DHCP server.

Lease Time

This setting specifies the length of time throughout which an IP address of a DHCP client remains valid. Upon expiration of **Lease Time**, the assigned IP address will no longer be valid and the IP address assignment must be renewed.

DNS Servers

This option allows you to input the DNS server addresses to be offered to DHCP clients. If **Assign DNS server automatically** is selected, the Pepwave router s built-in DNS server address (i.e., LAN IP address) will be offered.

WINS Servers

This option allows you to specify the Windows Internet Name Service (WINS) server. You may choose to use the built-in WINS server or external WINS servers. When this unit is connected using SpeedFusion™, other VPN peers can share this unit's built-in WINS server by entering this unit's LAN IP address in their **DHCP WINS Servers** setting. Therefore, all PC clients in the VPN can resolve the NetBIOS names of other clients in remote peers. If you have enabled this option, a list of WINS clients will be displayed at **Status>WINS Clients**.

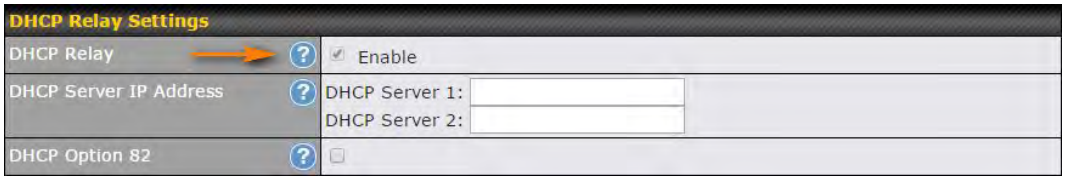
BOOTP

Check this box to enable BOOTP on older networks that still require it.

 Copyright @ 2017 Pepwave

Extended DHCP Option	In addition to standard DHCP options (e.g. DNS server address, gateway address, subnet mask), you can specify the value of additional extended DHCP options, as defined in RFC 2132. With these extended options enabled, you can pass additional configuration information to LAN hosts. To define an extended DHCP option, click the **Add** button, choose the option to define, and then enter its value. For values that are in IP address list format, you can enter one IP address per line in the provided text area input control. Each option can be defined once only.
DHCP Reservation	This setting reserves the assignment of fixed IP addresses for a list of computers on the LAN. The computers to be assigned fixed IP addresses on the LAN are identified by their MAC addresses. The fixed IP address assignment is displayed as a cross-reference list between the computers names, MAC addresses, and fixed IP addresses. **Name** (an optional field) allows you to specify a name to represent the device. MAC addresses should be in the format of **00:AA:BB:CC:DD:EE**. Press  to create a new record. Press  to remove a record. Reserved clients information can be imported from the **Client List**, located at **Status>Client List**.

To configure DHCP relay, first click the  button found next to the **DHCP Server** option to display the settings.



DHCP Relay Settings	
Enable	Check this box to turn on DHCP relay. Click the  icon to disable DHCP relay.
DHCP Server IP Address	Enter the IP addresses of one or two DHCP servers in the provided fields. The DHCP servers entered here will receive relayed DHCP requests from the LAN. For active-passive DHCP server configurations, enter active and passive DHCP server relay IP addresses in **DHCP Server 1** and **DHCP Server 2.**
DHCP Option 82	DCHP Option 82 includes device information as relay agent for the attached client when forwarding DHCP requests from client to server. This option also embeds the device s MAC address and network name in circuit and remote IDs. Check this box to enable DHCP Option 82.

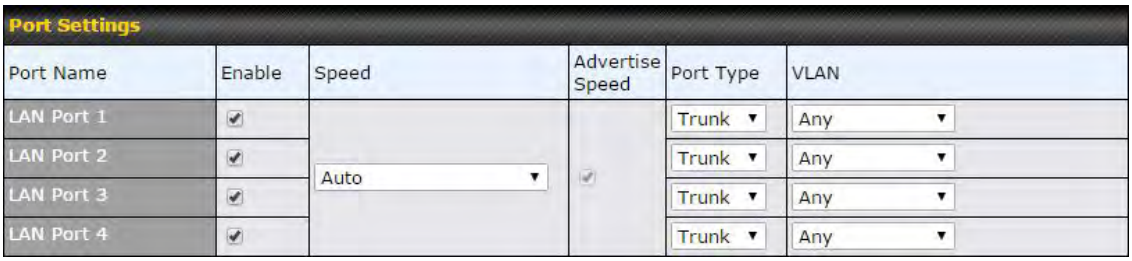
Once DHCP is set up, configure **LAN Physical Settings**, **Static Route Settings** and **DNS**

 Copyright @ 2017 Pepwave

Proxy Settings as noted above.

8.2 Port Settings

To configure port settings, navigate to **Network > Port Settings**



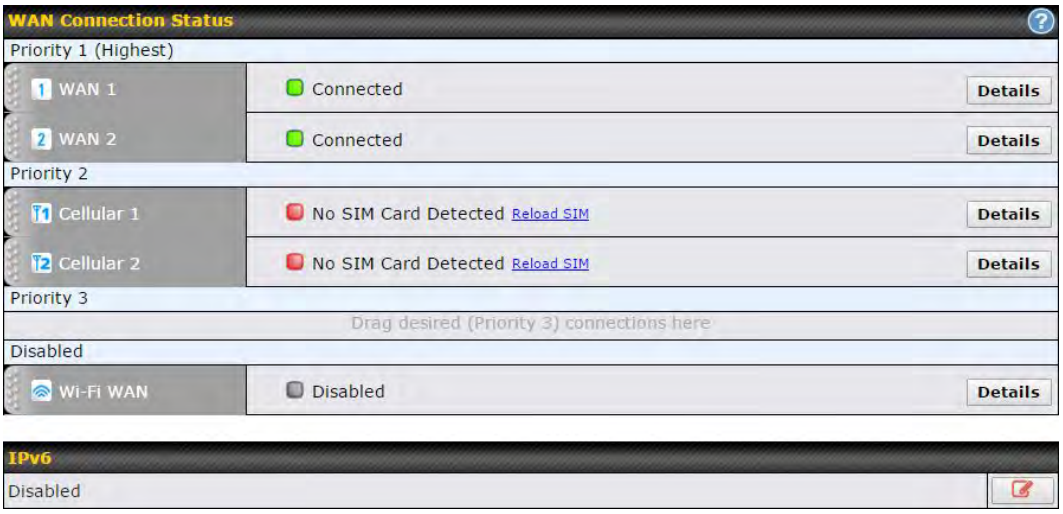
On this screen, you can enable specific ports, as well as determine the speed of the LAN ports, whether each port is a trunk or access port, can well as which VLAN each link belongs to, if any.

LAN Physical Settings	
Speed	This is the port speed of the LAN interface. It should be set to the same speed as the connected device to avoid port negotiation problems. When a static speed is set, you may choose whether to advertise its speed to the peer device. **Auto** is selected by default. You can choose not to advertise the port speed if the port has difficulty negotiating with the peer device.

9 Configuring the WAN Interface(s)

WAN Interface settings are located at **Network>WAN**. To reorder WAN priority, drag on the appropriate WAN by holding the left mouse button, move it to the desired priority (the first one would be the highest priority, the second one would be lower priority, and so on), and drop it by releasing the mouse button.

 Copyright @ 2017 Pepwave



To disable a particular WAN connection, drag on the appropriate WAN by holding the left mouse button, move it the **Disabled** row, and drop it by releasing the mouse button.

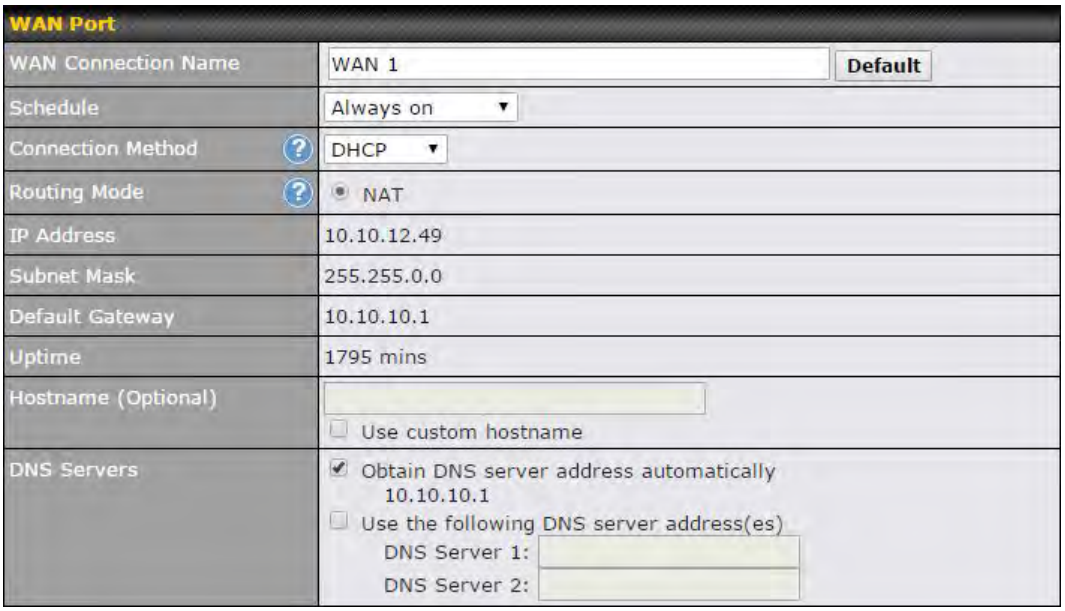
You can also set priorities on the **Dashboard**. Click the **Details** button in the corresponding row to modify the connection setting.

Important Note
Connection details will be changed and become effective immediately after clicking the **Save and Apply** button.

9.1 Ethernet WAN

From **Network>WAN,** choose a WAN connection and then click **Details**.

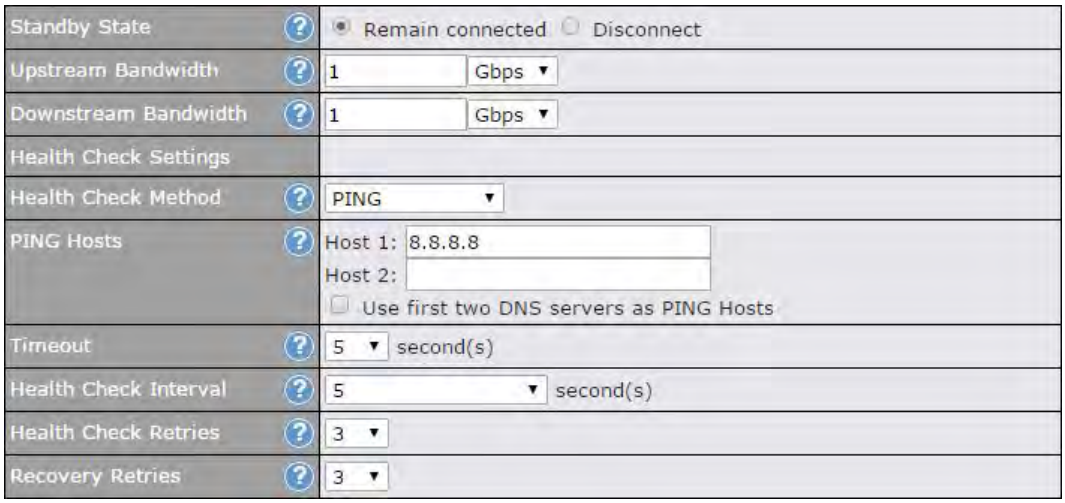
 Copyright @ 2017 Pepwave



WAN Port (Section 1)	
WAN Connection Name	Enter a name to represent this WAN connection.
Schedule	Click the drop-down menu to apply a time schedule to this interface
Connection Method	There are three possible connection methods for Ethernet WAN: **DHCP** **Static IP** **PPPoE** The connection method and details are determined by, and can be obtained from, the ISP. See the following sections for details on each connection method.
Routing Mode	This field shows that **NAT** (network address translation) will be applied to the traffic routed over this WAN connection. **IP Forwarding** is available when you click the link in the help text.
IP Address/Subnet Mask/Default Gateway	Enter the WAN IP address and subnet mask, as well as the IP address of the default gateway, in these fields.

 Copyright @ 2017 Pepwave

Hostname	Enter a hostname for this WAN port if needed.
DNS Servers	Select a DNS server for this port to use. This port can either be automatically selected or manually designated.

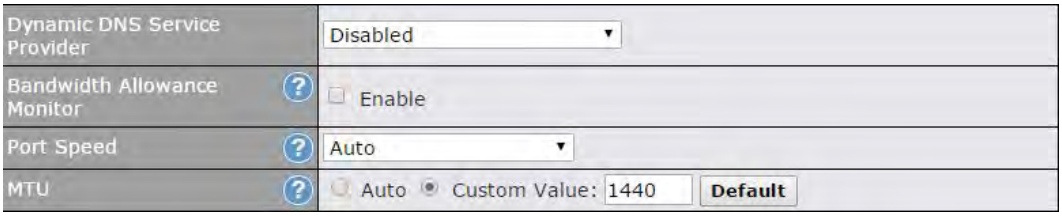


WAN Port (Section 2)

Standby State	This setting specifies the standby state of the WAN connection. The available options are **Remain connected** and **Disconnect**. The default state is **Remain Connected**.
Upstream Bandwidth	This setting specifies the data bandwidth in the outbound direction from the LAN through the WAN interface.
Downstream Bandwidth	This setting specifies the data bandwidth in the inbound direction from the WAN interface to the LAN. This value is referenced as the default weight value when using the algorithm **Least Used** or the algorithm **Persistence (Auto)** in outbound policy with **Managed by Custom Rules** chosen..
Health Check Method	This setting specifies the health check method for the WAN connection. The value of method can be configured as **Disabled**, **Ping**, **DNS Lookup**, or **HTTP**. The default method is **Disabled**. See **Section 10.4** for configuration details.
PING Hosts	These fields are for specifying the target DNS servers where DNS lookups will be sent to for health check. If the box Use first two DNS servers as Health Check DNS Servers is checked, the first two DNS servers will be the DNS lookup targets for checking the connection healthiness. If the box is not checked, the field Host 1 must be filled and the field Host 2 is optional. The connection is considered to be up if DNS responses are received from any one of the

 Copyright @ 2017 Pepwave

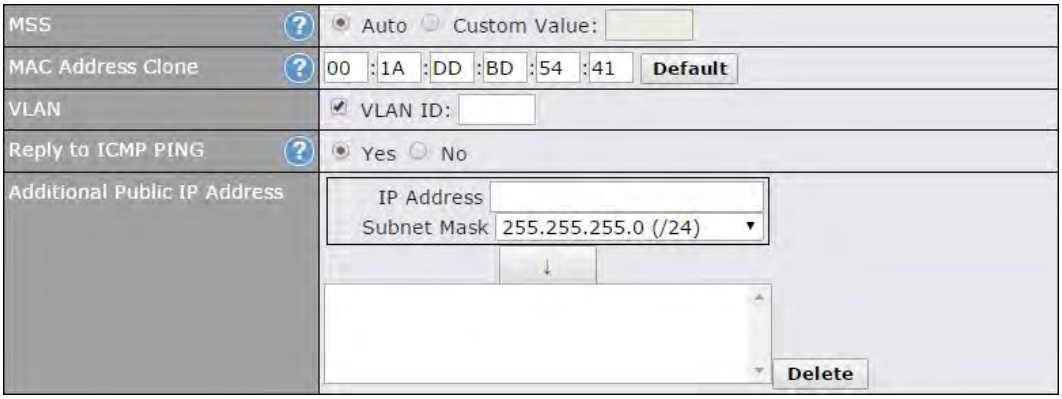
	health check DNS servers, regardless of whether the result is positive or negative.
Timeout	If a health check test cannot be completed within the specified amount of time, the test will be treated as failed.
Health Check Interval	This is the number of consecutive check failures before treating a connection as down.
Health Check Retries	This is the number of consecutive check failures before treating a connection as down.
Recovery Retries	This is the number of responses required after a health check failure before treating a connection as up again.



WAN Port (Section 3)	
Dynamic DNS Service Provider	This setting specifies the dynamic DNS service provider to be used for the WAN based on supported dynamic DNS service providers: changeip.com dyndns.org no-ip.org tzo.com DNS-O-Matic Select **Disabled** to disable this feature. See **Section 9.5** for configuration details.
Bandwidth Allowance Monitor	This option enables bandwidth usage monitoring on this WAN connection for each billing cycle. When this setting is not enabled, each month s bandwidth usage is tracked, but no action will be taken.
Port Speed	This setting specifies port speed and duplex configurations of the WAN port. By default, **Auto** is selected and the appropriate data speed is automatically detected by the Pepwave router. In the event of negotiation issues, the port speed can be manually

 Copyright @ 2017 Pepwave

	specified. You can also choose whether or not to advertise the speed to the peer by selecting the **Advertise Speed** checkbox.
MTU	This setting specifies the maximum transmission unit. By default, MTU is set to **Custom 1440**. You may ad ust the MTU value by editing the text field. Click **Default** to restore the default MTU value. Select **Auto** and the appropriate MTU value will be automatically detected. Auto-detection will run each time the WAN connection establishes.



WAN Port (Section 4)	
MSS	This setting should be configured based on the maximum payload size that the local system can handle. The MSS (maximum segment size) is computed from the MTU minus 40 bytes for TCP over IPv4. If MTU is set to **Auto**, the MSS will also be set automatically. By default, MSS is set to **Auto**.
MAC Address Clone	Some service providers (e.g., cable providers) identify the client s MAC address and require the client to always use the same MAC address to connect to the network. In such cases, change the WAN interface s MAC address to the original client PC s MAC address via this field. The default MAC address is a unique value assigned at the factory. In most cases, the default value is sufficient. Clicking **Default** restores the MAC address to the default value.
VLAN	Click the square if you wish to enable VLAN functionality and enable multiple broadcast domains. Once you enable VLAN, you will be able to enter a name for your network.
Reply to ICMP PING	If this field is disabled, the WAN connection will not respond to ICMP ping requests. By default, this is **enabled**.
Additional	The **IP Address** list represents the list of fixed Internet IP addresses assigned by the ISP,

 Copyright @ 2017 Pepwave

Public IP Address	in the event that more than one Internet IP address is assigned to this WAN connection. Enter the fixed Internet IP addresses and the corresponding subnet mask, and then click the **Down Arrow** button to populate IP address entries to the **IP Address** List.



IPv6	
IPv6	IPv6 support can be enabled on one of the available Ethernet WAN ports. On this screen, you can choose which WAN will support IPv6. To enable IPv6 support on a WAN, the WAN router must respond to stateless address auto configuration advertisements and DHCPv6 requests. IPv6 clients on the LAN will acquire their IPv6, gateway, and DNS server addresses from it. The device will also acquire an IPv6 address for performing ping/traceroute checks and accepting web admin accesses. Note: This feature is only available on the Pepwave MAX 700, HD2, and HD2 IP67.

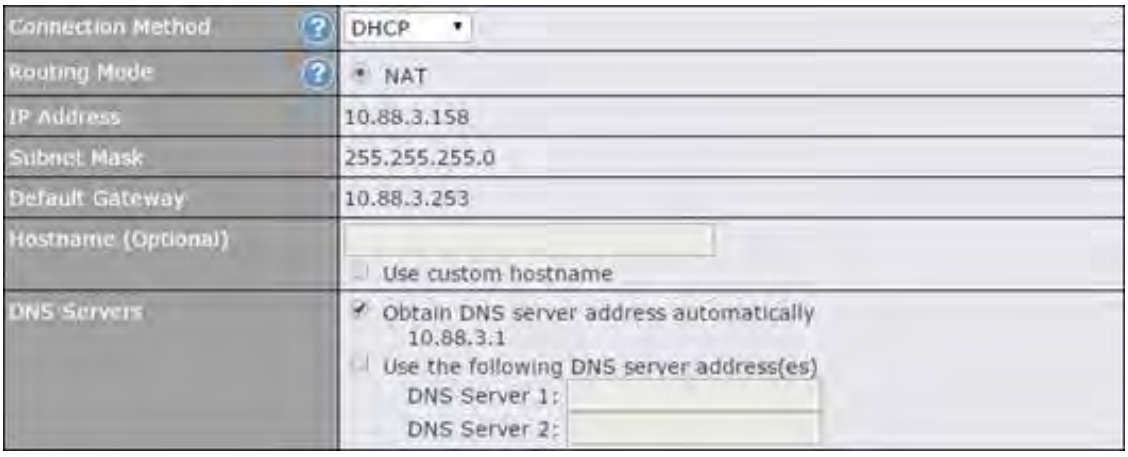
9.1.1 DHCP Connection

There are four possible connection methods:

1. DHCP
2. Static IP
3. PPPoE
4. L2TP

The DHCP connection method is suitable if the ISP provides an IP address automatically using DHCP (e.g., satellite modem, WiMAX modem, cable, Metro Ethernet, etc.).

 Copyright @ 2017 Pepwave

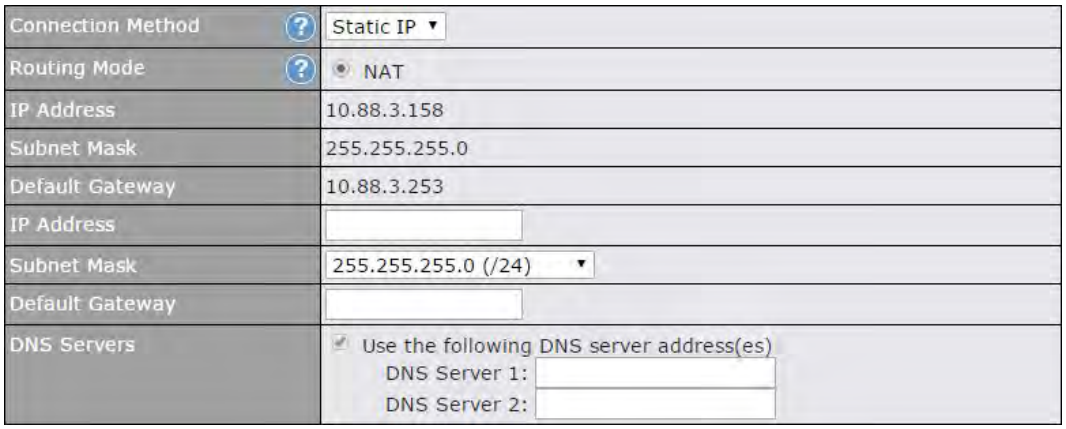


DHCP Connection Settings	
Routing Mode	NAT allows substituting the real address in a packet with a mapped address that is routable on the destination network. By clicking the help icon in this field, you can display the **IP Forwarding** option, if your network requires it.
IP Address/ Subnet Mask/ Default Gateway	This information is obtained from the ISP automatically.
Hostname (Optional)	If your service provider's DHCP server requires you to supply a hostname value upon acquiring an IP address, you may enter the value here. If your service provider does not provide you with the value, you can safely bypass this option.
DNS Servers	Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting **Obtain DNS server address automatically** results in the DNS servers being assigned by the WAN DHCP server to be used for outbound DNS lookups over the connection. (The DNS servers are obtained along with the WAN IP address assigned from the DHCP server.) When **Use the following DNS server address(es)** is selected, you may enter custom DNS server addresses for this WAN connection into the **DNS Server 1** and **DNS Server 2** fields.

 Copyright @ 2017 Pepwave

9.1.2 Static IP Connection

The static IP connection method is suitable if your ISP provides a static IP address to connect directly.

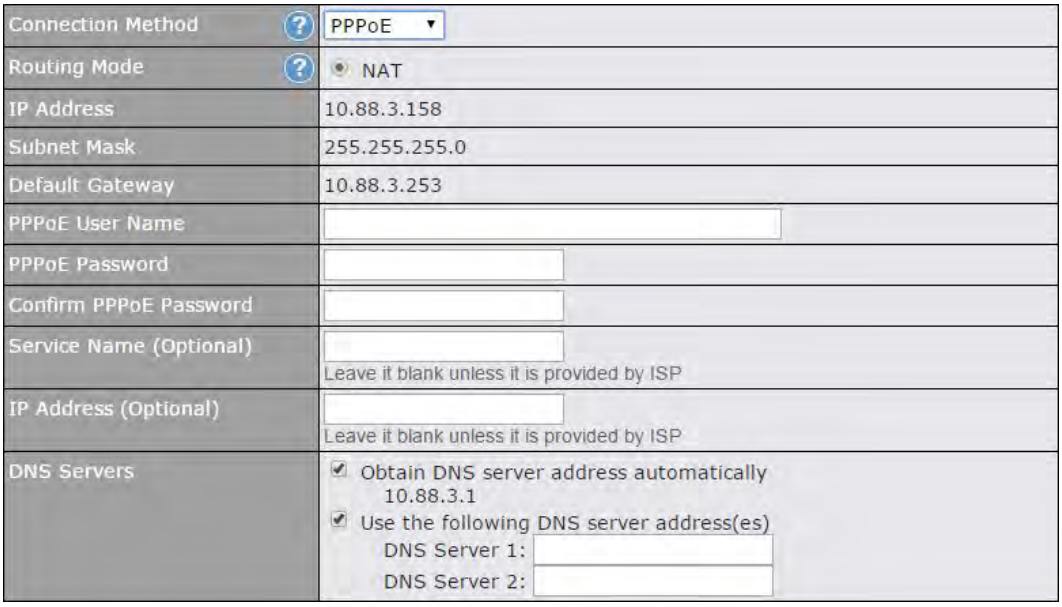


Static IP Settings	
Routing Mode	NAT allows substituting the real address in a packet with a mapped address that is routable on the destination network. By clicking the help icon in this field, you can display the **IP Forwarding** option, if your network requires it.
IP Address / Subnet Mask / Default Gateway	These settings allow you to specify the information required in order to communicate on the Internet via a fixed Internet IP address. The information is typically determined by and can be obtained from the ISP.
DNS Servers	Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting **Obtain DNS server address automatically** results in the DNS servers being assigned by the WAN DHCP server to be used for outbound DNS lookups over the connection. (The DNS servers are obtained along with the WAN IP address assigned from the DHCP server.) When **Use the following DNS server address(es)** is selected, you may enter custom DNS server addresses for this WAN connection into the **DNS Server 1** and **DNS Server 2** fields.

9.1.3 PPPoE Connection

This connection method is suitable if your ISP provides a login ID/password to connect via PPPoE.

 Copyright @ 2017 Pepwave



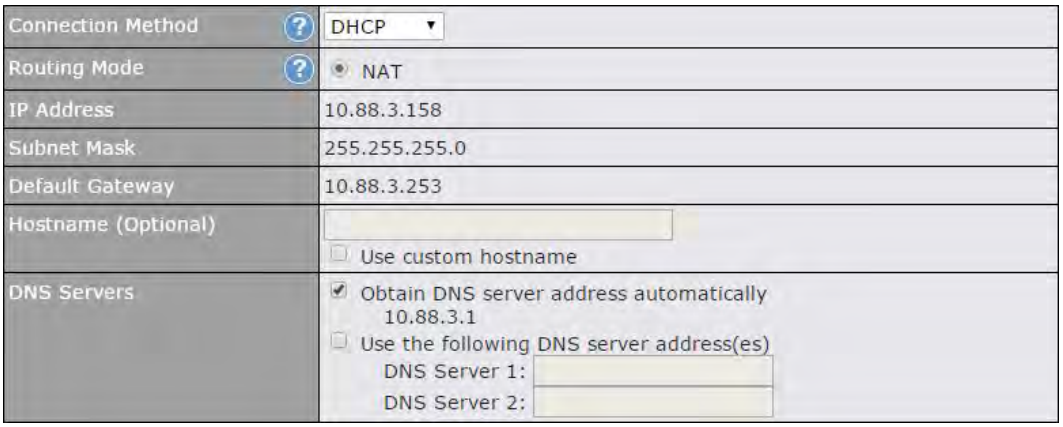
PPPoE Settings	
Routing Mode	NAT allows substituting the real address in a packet with a mapped address that is routable on the destination network. By clicking the help icon in this field, you can display the **IP Forwarding** option, if your network requires it.
IP Address / Subnet Mask / Default Gateway	This information is obtained from the ISP automatically.
PPPoE User Name / Password	Enter the required information in these fields in order to connect via PPPoE to the ISP. The parameter values are determined by and can be obtained from the ISP.
Confirm PPPoE Password	Verify your password by entering it again in this field.
Service Name (Optional)	Service name is provided by the ISP. **Note: Leave this field blank unless it is provided by your ISP.**
IP Address (Optional)	If your ISP provides a PPPoE IP address, enter it here. **Note: Leave this field blank unless it is provided by your ISP.**

 Copyright @ 2017 Pepwave

DNS Servers	Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting **Obtain DNS server address automatically** results in the DNS servers being assigned by the WAN DHCP server to be used for outbound DNS lookups over the connection. (The DNS servers are obtained along with the WAN IP address assigned from the DHCP server.) When **Use the following DNS server address(es)** is selected, you may enter custom DNS server addresses for this WAN connection into the **DNS Server 1** and **DNS Server 2** fields.

9.1.4 L2TP Connection

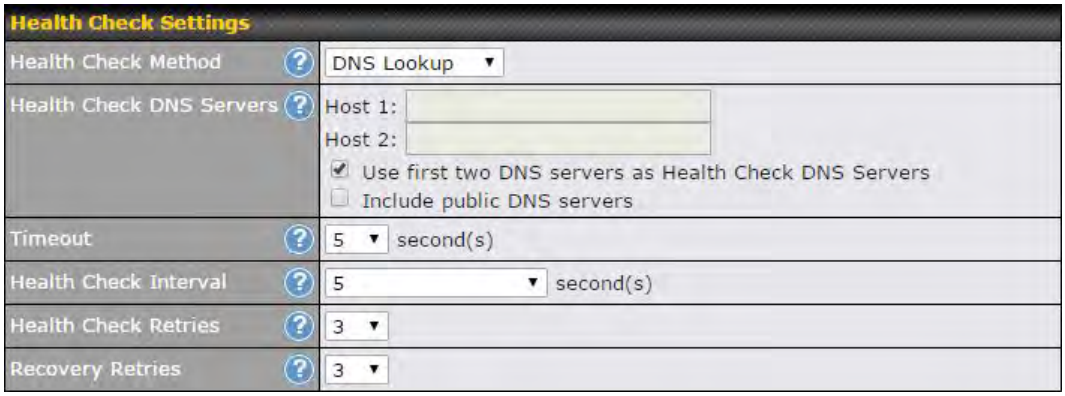
L2TP has all the compatibility and convenience of PPTP with greater security. Combine this with IPsec for a good balance between ease of use and security.



L2TP Settings	
L2TP User Name / Password	Enter the required information in these fields in order to connect via L2TP to your ISP. The parameter values are determined by and can be obtained from your ISP.
Confirm L2TP Password	Verify your password by entering it again in this field.
Server IP Address / Host	L2TP server address is a parameter which is provided by your ISP. Note: Leave this field blank unless it is provided by your ISP.
Address Type	Your ISP will also indicate whether the server IP address is Dynamic or Static. Please click the appropriate value.

 Copyright @ 2017 Pepwave

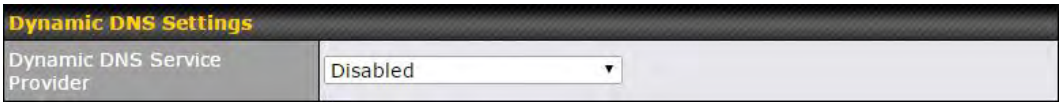
DNS Servers	Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting **Obtain DNS server address automatically** results in the DNS servers assigned by the PPPoE server to be used for outbound DNS lookups over the WAN connection. (The DNS servers are obtained along with the WAN IP address assigned from the PPPoE server.) When **Use the following DNS server address(es)** is selected, you can enter custom DNS server addresses for this WAN connection into the **DNS server 1** and **DNS server 2** fields.



Health Check Settings	
Heath Check Method	This setting allows you to specify the health check method for the cellular connection. Available options are **Disabled, Ping, DNS Lookup, HTTP,** and **SmartCheck**. The default method is **DNS Lookup**. See **Section 10.4** for configuration details.
Timeout	If a health check test cannot be completed within the specified amount of time, the test will be treated as failed.
Health Check Interval	This is the time interval between each health check test.

 Copyright @ 2017 Pepwave

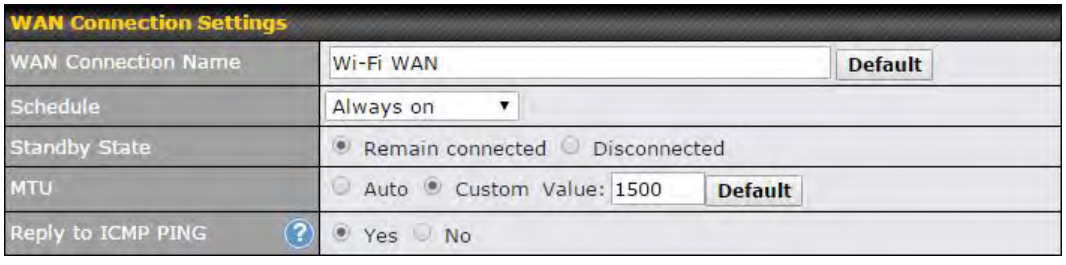
Health Check Retries	This is the number of consecutive check failures before treating a connection as down.
Recovery Retries	This is the number of responses required after a health check failure before treating a connection as up again.



Dynamic DNS Settings	
Dynamic DNS Service Provider	This setting specifies the dynamic DNS service provider to be used for the WAN based on supported dynamic DNS service providers: changeip.com dyndns.org no-ip.org tzo.com DNS-O-Matic Select **Disabled** to disable this feature. See **Section 9.5** for configuration details.

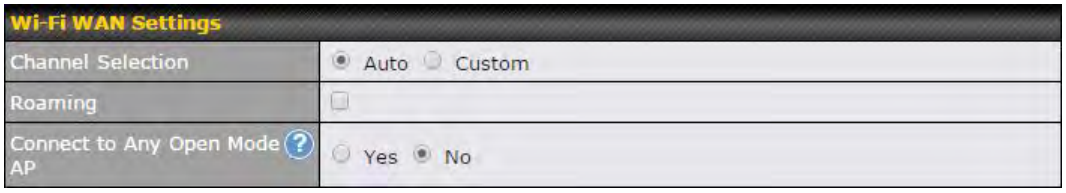
9.2 Wi-Fi WAN

To access Wi-Fi WAN settings, click **Network>WAN>Details**.



 Copyright @ 2017 Pepwave

Wi-Fi Connection Settings	
WAN Connection Name	Enter a name to represent this WAN connection.
Schedule	Click the drop-down menu to apply a time schedule to this interface.
Standby State	This setting specifies the state of the WAN connection while in standby. The available options are **Remain Connected** (hot standby) and **Disconnect** (cold standby).
MTU	This setting specifies the maximum transmission unit. By default, MTU is set to **Custom 1440**. You may ad ust the MTU value by editing the text field. Click **Default** to restore the default MTU value. Select **Auto** and the appropriate MTU value will be automatically detected. The auto-detection will run each time the WAN connection establishes
Reply to ICMP PING	If this setting is disabled, the WAN connection will not respond to ICMP ping requests. By default, this setting is enabled.

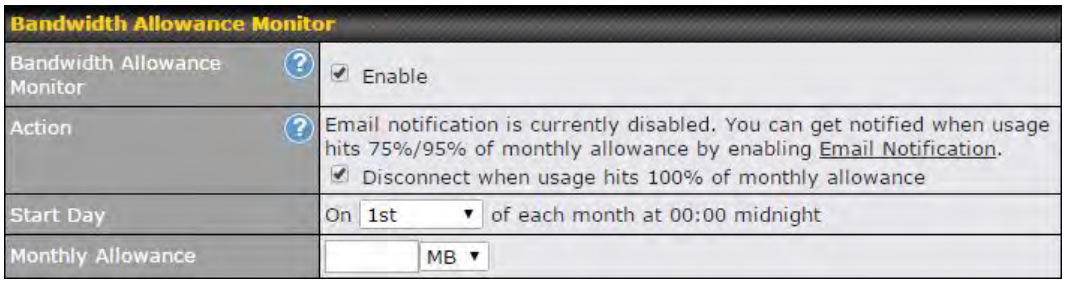


Wi-Fi WAN Settings	
Channel Selection	Determine whether the channel will be automatically selected. If you select custom, the following table will appear:



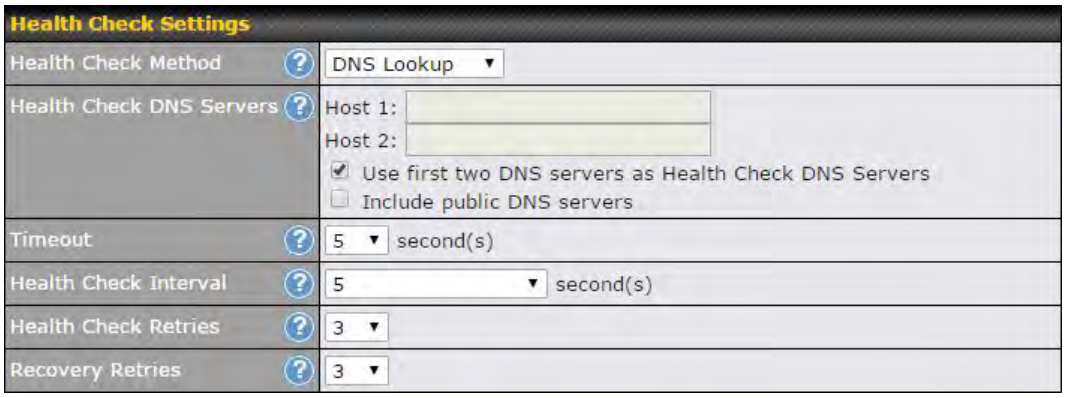
 Copyright @ 2017 Pepwave

Roaming	Checking this box will enable Wi-Fi roaming. Click the icon for additional options.
Connect to Any Open Mode AP	This option is to specify whether the Wi-Fi WAN will connect to any open mode access points it finds.



Bandwidth Allowance Monitor	
Action	If **Error! Reference source not found.** is enabled, you will be notified by email when usage hits 75 and 95 of the monthly allowance. If **Disconnect when usage hits 100% of monthly allowance** is checked, this WAN connection will be disconnected automatically when the usage hits the monthly allowance. It will not resume connection unless this option has been turned off or the usage has been reset when a new billing cycle starts.
Start Day	This option allows you to define which day of the month each billing cycle begins.
Monthly Allowance	This field is for defining the maximum bandwidth usage allowed for the WAN connection each month.

 Copyright @ 2017 Pepwave



Health Check Settings

Method

This setting specifies the health check method for the WAN connection. This value can be configured as **Disabled**, **PING**, **DNS Lookup**, or **HTTP**. The default method is **DNS Lookup**. For mobile Internet connections, the value of **Method** can be configured as **Disabled** or **SmartCheck**.

Health Check Disabled



When **Disabled** is chosen in the **Method** field, the WAN connection will always be considered as up. The connection will **NOT** be treated as down in the event of IP routing errors.

Health Check Method: PING



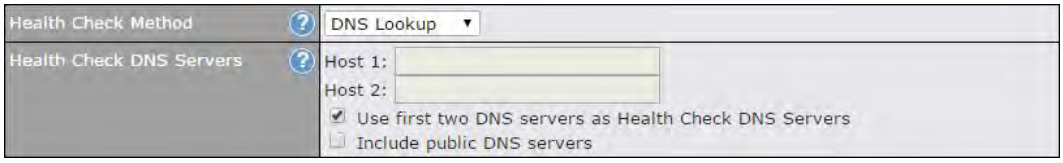
ICMP ping packets will be issued to test the connectivity with a configurable target IP address or hostname. A WAN connection is considered as up if ping responses are received from either one or both of the ping hosts.

PING Hosts

This setting specifies IP addresses or hostnames with which connectivity is to be tested via ICMP ping. If **Use first two DNS servers as Ping Hosts** is checked, the target ping host will be the first DNS server for the corresponding WAN connection. Reliable ping hosts with a high uptime should be considered. By default, the first two DNS servers of the WAN connection are used as the ping hosts.

Health Check Method: DNS Lookup

 Copyright @ 2017 Pepwave



DNS lookups will be issued to test connectivity with target DNS servers. The connection will be treated as up if DNS responses are received from one or both of the servers, regardless of whether the result was positive or negative.

Health Check DNS Servers

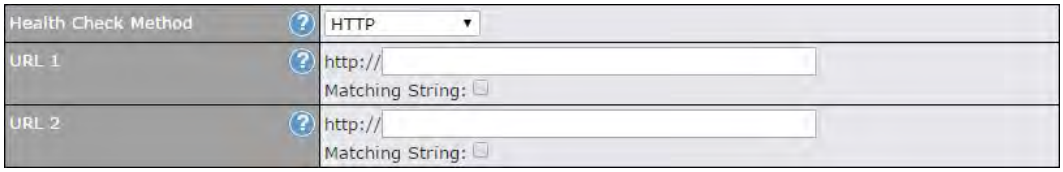
This field allows you to specify two DNS hosts IP addresses with which connectivity is to be tested via DNS Lookup.

If **Use first two DNS servers as Health Check DNS Servers** is checked, the first two DNS servers will be the DNS lookup targets for checking a connection's health. If the box is not checked, **Host 1** must be filled, while a value for **Host 2** is optional.

If **Include public DNS servers** is selected and no response is received from all specified DNS servers, DNS lookups will also be issued to some public DNS servers. A WAN connection will be treated as down only if there is also no response received from the public DNS servers.

Connections will be considered as up if DNS responses are received from any one of the health check DNS servers, regardless of a positive or negative result. By default, the first two DNS servers of the WAN connection are used as the health check DNS servers.

Health Check Method: HTTP



HTTP connections will be issued to test connectivity with configurable URLs and strings to match.

URL1

WAN Settings>WAN Edit>Health Check Settings>URL1

The URL will be retrieved when performing an HTTP health check. When **String to Match** is left blank, a health check will pass if the HTTP return code is between 200 and 299 (Note: HTTP redirection codes 301 or 302 are treated as failures). When **String to Match** is filled, a health check will pass if the HTTP return code is between 200 and 299 and if the HTTP response content contains the string.

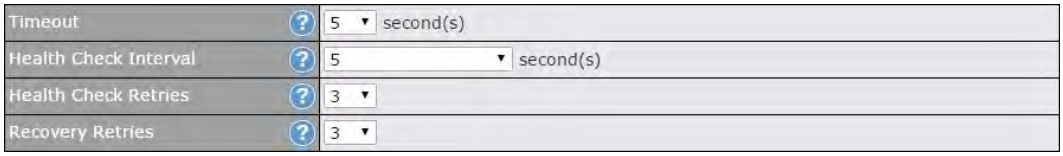
URL 2

WAN Settings>WAN Edit>Health Check Settings>URL2

If **URL2** is also provided, a health check will pass if either one of the tests passed.

 Copyright @ 2017 Pepwave

Other Health Check Settings



Timeout

This setting specifies the timeout in seconds for ping/DNS lookup requests. The default timeout is **5 seconds**.

Health Check Interval

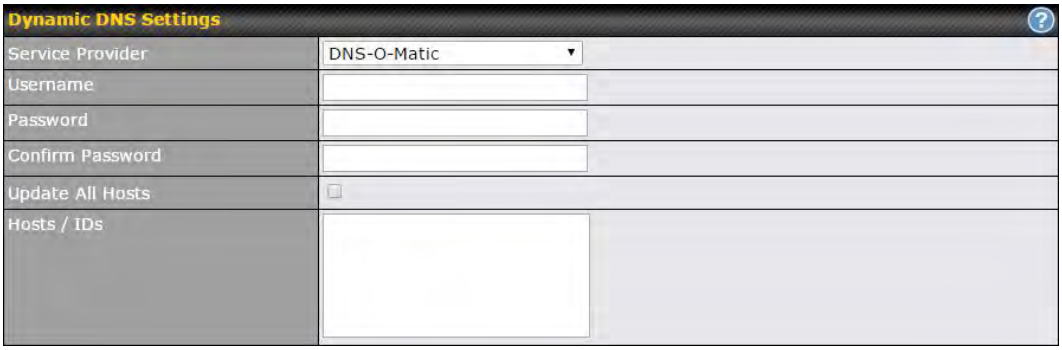
This setting specifies the time interval in seconds between ping or DNS lookup requests. The default health check interval is **5 seconds**.

Health Check Retries

This setting specifies the number of consecutive ping/DNS lookup timeouts after which the Peplink Balance will treat the corresponding WAN connection as down. Default health retries is set to **3**. Using the default **Health Retries** setting of **3**, the corresponding WAN connection will be treated as down after three consecutive timeouts.

Recovery Retries

This setting specifies the number of consecutive successful ping/DNS lookup responses that must be received before the Peplink Balance treats a previously down WAN connection as up again. By default, **Recover Retries** is set to **3**. Using the default setting, a WAN connection that is treated as down will be considered as up again upon receiving three consecutive successful ping/DNS lookup responses.



Dynamic DNS Settings

Service Provider

This setting specifies the dynamic DNS service provider to be used for the WAN. Supported providers are:

changeip.com

dyndns.org

 Copyright @ 2017 Pepwave

	no-ip.org tzo.com DNS-O-Matic Select **Disabled** to disable this feature.
User ID / User / Email	This setting specifies the registered user name for the dynamic DNS service.
Password / Pass / TZO Key	This setting specifies the password for the dynamic DNS service.
Update All Hosts	Check this box to automatically update all hosts.
Hosts / Domain	This setting specifies a list of hostnames or domains to be associated with the public Internet IP address of the WAN connection.

Important Note

In order to use dynamic DNS services, appropriate hostname registration(s), as well as a valid account with a supported dynamic DNS service provider, are required.

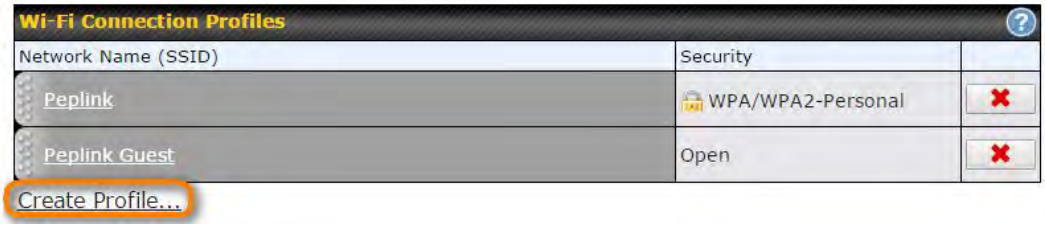
A dynamic DNS update is performed whenever a WAN s IP address is changed, such as when an IP is changed after a DHCP IP refresh or reconnection.

Due to dynamic DNS service providers policies, a dynamic DNS host expires automatically when the host record has not been not updated for a long time. Therefore, the Peplink Balance performs an update every 23 days, even if a WAN s IP address did not change.

9.2.1 Creating Wi-Fi Connection Profiles

You can manually create a profile to connect to a Wi-Fi connection. This is useful for creating a profile for connecting to hidden-SSID access points. Click **Network>WAN>Details>Create Profile…** to get started.

 Copyright @ 2017 Pepwave



This will open a window similar to the one shown below:

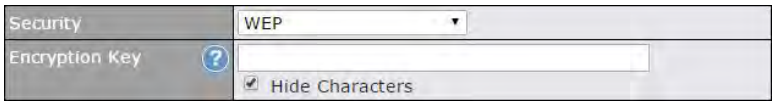


Wi-Fi Connection Profile Settings	
Type	Select whether the network will connect automatically or manually.
Network Name (SSID)	Enter a name to represent this Wi-Fi connection.
	This option allows you to select which security policy is used for this wireless network. Available options:

Open

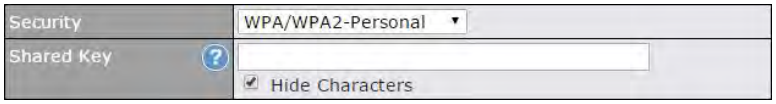


WEP

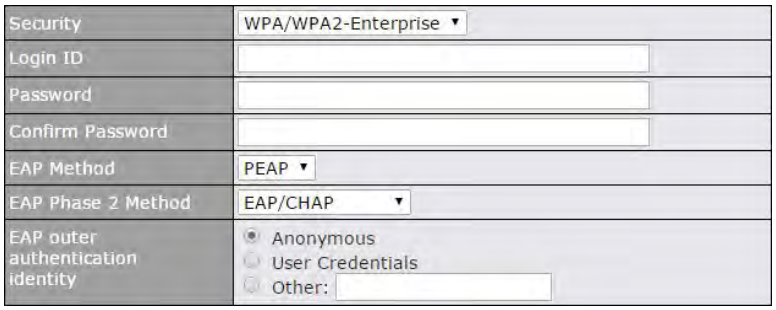


 Copyright @ 2017 Pepwave

WPA/WPA2 – Personal



WPA/WPA2 – Enterprise



9.3 WAN Health Check

To ensure traffic is routed to healthy WAN connections only, the Pepwave router can periodically check the health of each WAN connection. The health check settings for each WAN connection can be independently configured via **Network>WAN>Details**.

Health Check Settings	
Method	This setting specifies the health check method for the WAN connection. This value can be configured as **Disabled**, **PING**, **DNS Lookup**, or **HTTP**. The default method is **DNS Lookup**. For mobile Internet connections, the value of **Method** can be configured as **Disabled** or **SmartCheck**.
Health Check Disabled	



When **Disabled** is chosen in the **Method** field, the WAN connection will always be considered as up. The connection will **NOT** be treated as down in the event of IP routing errors.

Health Check Method: PING

 Copyright @ 2017 Pepwave



ICMP ping packets will be issued to test the connectivity with a configurable target IP address or hostname. A WAN connection is considered as up if ping responses are received from either one or both of the ping hosts.

PING Hosts

This setting specifies IP addresses or hostnames with which connectivity is to be tested via ICMP ping. If **Use first two DNS servers as Ping Hosts** is checked, the target ping host will be the first DNS server for the corresponding WAN connection. Reliable ping hosts with a high uptime should be considered. By default, the first two DNS servers of the WAN connection are used as the ping hosts.

Health Check Method: DNS Lookup



DNS lookups will be issued to test connectivity with target DNS servers. The connection will be treated as up if DNS responses are received from one or both of the servers, regardless of whether the result was positive or negative.

Health Check DNS Servers

This field allows you to specify two DNS hosts IP addresses with which connectivity is to be tested via DNS lookup.

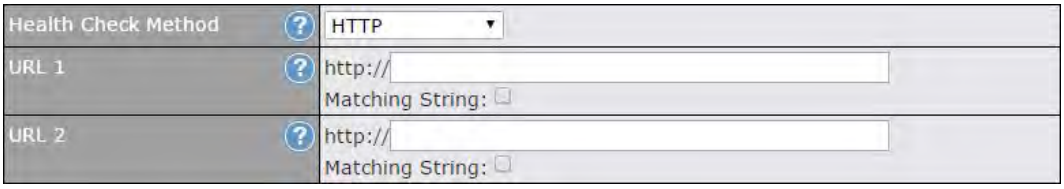
If **Use first two DNS servers as Health Check DNS Servers** is checked, the first two DNS servers will be the DNS lookup targets for checking a connection's health. If the box is not checked, **Host 1** must be filled, while a value for **Host 2** is optional.

If **Include public DNS servers** is selected and no response is received from all specified DNS servers, DNS lookups will also be issued to some public DNS servers. A WAN connection will be treated as down only if there is also no response received from the public DNS servers.

Connections will be considered as up if DNS responses are received from any one of the health check DNS servers, regardless of a positive or negative result. By default, the first two DNS servers of the WAN connection are used as the health check DNS servers.

Health Check Method: HTTP

 Copyright @ 2017 Pepwave



HTTP connections will be issued to test connectivity with configurable URLs and strings to match.

URL1	**WAN Settings>WAN Edit>Health Check Settings>URL1** The URL will be retrieved when performing an HTTP health check. When **String to Match** is left blank, a health check will pass if the HTTP return code is between 200 and 299 (Note: HTTP redirection codes 301 or 302 are treated as failures). When **String to Match** is filled, a health check will pass if the HTTP return code is between 200 and 299 and if the HTTP response content contains the string.
URL 2	**WAN Settings>WAN Edit>Health Check Settings>URL2** If **URL2** is also provided, a health check will pass if either one of the tests passed.



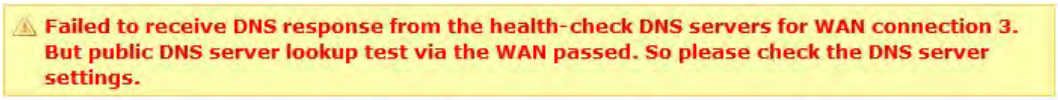
Other Health Check Settings	
Timeout	This setting specifies the timeout in seconds for ping/DNS lookup requests. The default timeout is **5 seconds**.
Health Check Interval	This setting specifies the time interval in seconds between ping or DNS lookup requests. The default health check interval is **5 seconds**.
Health Check Retries	This setting specifies the number of consecutive ping/DNS lookup timeouts after which the Pepwave router will treat the corresponding WAN connection as down. Default health retries is set to **3**. Using the default **Health Retries** setting of **3**, the corresponding WAN connection will be treated as down after three consecutive timeouts.
Recovery Retries	This setting specifies the number of consecutive successful ping/DNS lookup responses that must be received before the Pepwave router treats a previously down WAN connection as up again. By default, **Recover Retries** is set to **3**. Using the default setting, a WAN connection that is treated as down will be considered as up again upon

 Copyright @ 2017 Pepwave

receiving three consecutive successful ping/DNS lookup responses.

Automatic Public DNS Server Check on DNS Test Failure

When the health check method is set to **DNS Lookup** and health checks fail, the Pepwave router will automatically perform DNS lookups on public DNS servers. If the tests are successful, the WAN may not be down, but rather the target DNS server malfunctioned. You will see the following warning message on the main page:



9.4 Dynamic DNS Settings

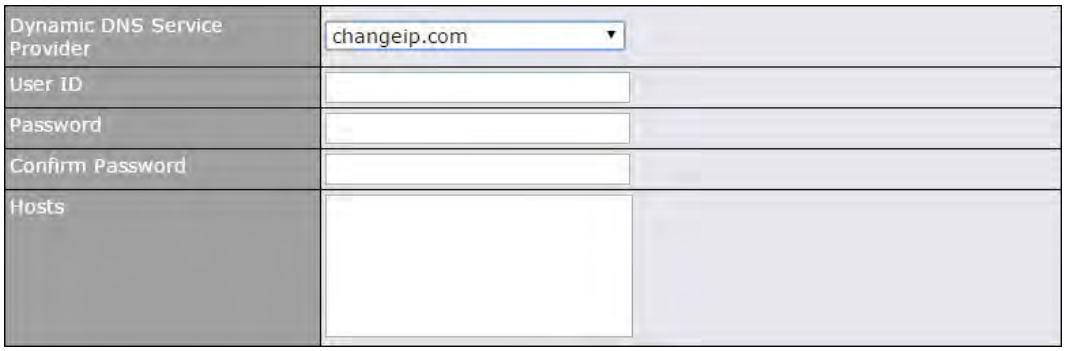
Pepwave routers are capable of registering the domain name relationships to dynamic DNS service providers. Through registration with dynamic DNS service provider(s), the default public Internet IP address of each WAN connection can be associated with a host name. With dynamic DNS service enabled for a WAN connection, you can connect to your WAN's IP address from the external, even if its IP address is dynamic. You must register for an account from the listed dynamic DNS service providers before enabling this option.

If the WAN connection's IP address is a reserved private IP address (i.e., behind a NAT router), the public IP of each WAN will be automatically reported to the DNS service provider.

Either upon a change in IP addresses or every 23 days without link reconnection, the Pepwave router will connect to the dynamic DNS service provider to perform an IP address update within the provider's records.

The settings for dynamic DNS service provider(s) and the association of hostname(s) are configured via **Network>WAN>Details>Dynamic DNS Service Provider/Dynamic DNS Settings**.

 Copyright @ 2017 Pepwave



Dynamic DNS Settings

Dynamic DNS

This setting specifies the dynamic DNS service provider to be used for the WAN based on supported dynamic DNS service providers:

- changeip.com
- dyndns.org
- no-ip.org
- tzo.com
- DNS-O-Matic
- Others

Support custom Dynamic DNS servers by entering its URL. Works with any service compatible with DynDNS API.

Select **Disabled** to disable this feature.

Account Name / Email Address

This setting specifies the registered user name for the dynamic DNS service.

Password / TZO Key

This setting specifies the password for the dynamic DNS service.

Hosts / Domain

This field allows you to specify a list of host names or domains to be associated with the public Internet IP address of the WAN connection. If you need to enter more than one host, use a carriage return to separate them.

Important Note

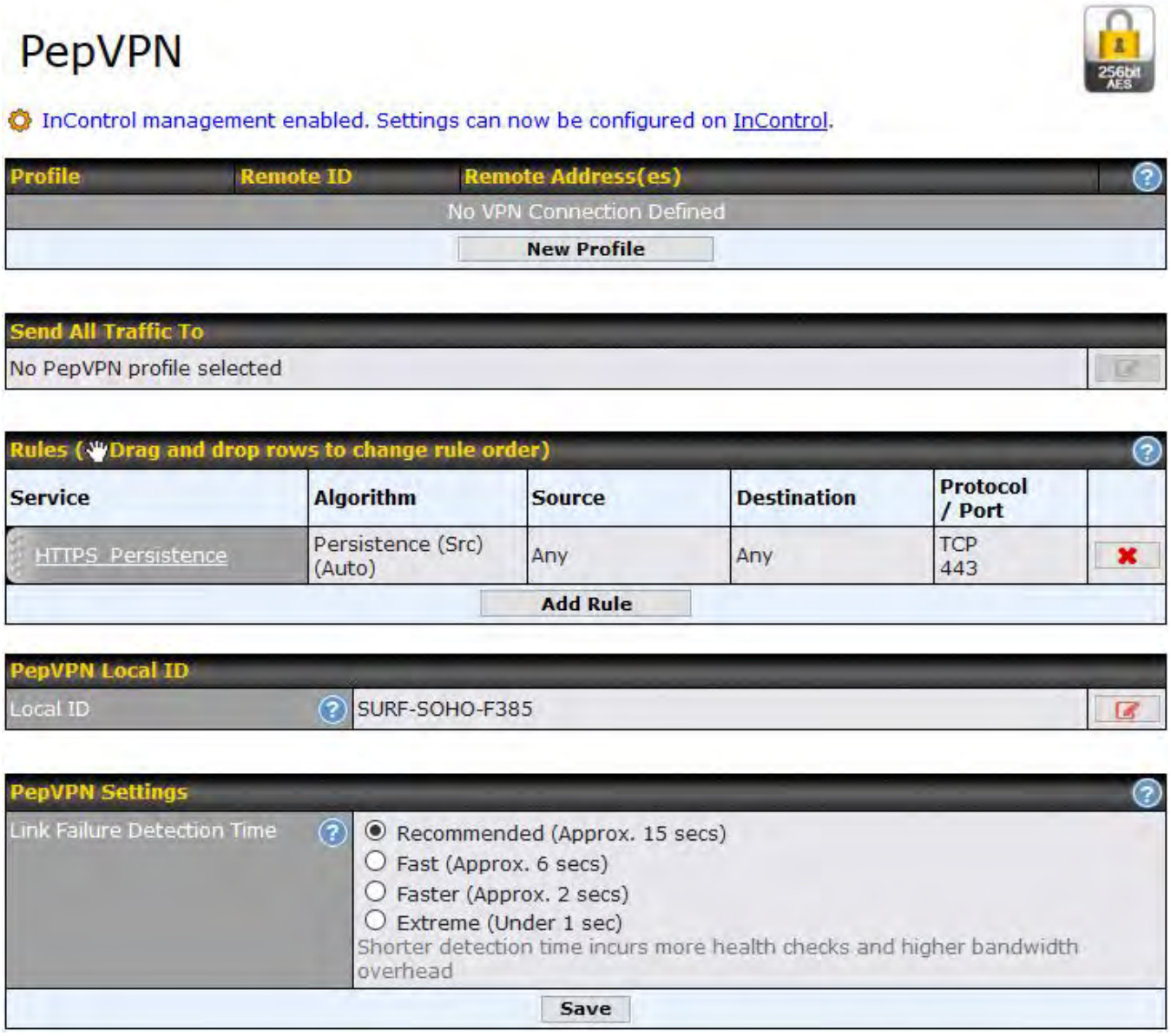
In order to use dynamic DNS services, appropriate host name registration(s) and a valid account with a supported dynamic DNS service provider are required. A dynamic DNS update is performed whenever a WAN s IP address changes (e.g., the IP is changed after a DHCP IP refresh, reconnection, etc.). Due to dynamic DNS service providers policy, a dynamic DNS host will automatically expire if the host record has not been updated for a long

 Copyright @ 2017 Pepwave

time. Therefore the Pepwave router performs an update every 23 days, even if a WAN s IP address has not changed.

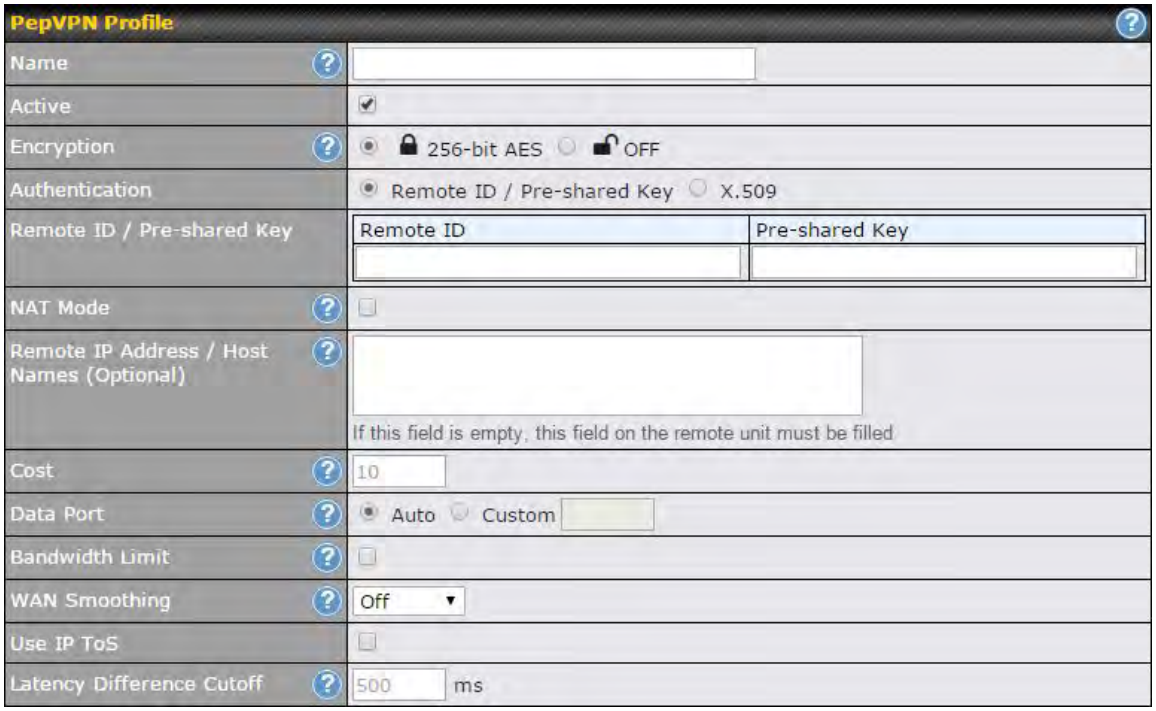
10 PepVPN

To configure PepVPN and SpeedFusion, navigate to **Advanced>PepVPN**



 Copyright @ 2017 Pepwave

The local LAN subnet and subnets behind the LAN (defined under **Static Route** on the LAN settings page) will be advertised to the VPN. All VPN members (branch offices and headquarters) will be able to route to local subnets.
Note that all LAN subnets and the subnets behind them must be unique. Otherwise, VPN members will not be able to access each other.
All data can be routed over the VPN using the 256-bit AES encryption standard. To configure, navigate to **Advanced>PepVPN** and click the **New Profile** button to create a new VPN profile (you may have to first save the displayed default profile in order to access the **New Profile** button). Each profile specifies the settings for making VPN connection with one remote Pepwave or Peplink device.



Click the **Save** button to create and save a new VPN connection profile for making a VPN connection.

PepVPN Profile Settings	
Name	This field is for specifying a name to represent this profile. The name can be any combination of alphanumeric characters (0-9, A-Z, a-z), underscores (_), dashes (-), and/or non-leading/trailing spaces ( ).

 Copyright @ 2017 Pepwave

Active	When this box is checked, this VPN connection profile will be enabled. Otherwise, it will be disabled.
Encryption	By default, VPN traffic is encrypted with **256-bit AES**. If **Off** is selected on both sides of a VPN connection, no encryption will be applied.
Authentication	Select from **By Remote ID Only**, **Preshared Key**. When selecting **By Remote ID Only**, be sure to enter a unique peer ID number in the **Remote ID** field.
Remote ID / Pre-shared Key	This optional field becomes available when **Remote ID / Pre-shared Key** is selected as the Peplink Balance's VPN **Authentication** method, as explained above. **Pre-shared Key** defines the pre-shared key used for this particular VPN connection. The VPN connection's session key will be further protected by the pre-shared key. The connection will be up only if the pre-shared keys on each side match. When the peer is running firmware 5.0+, this setting will be ignored.
NAT Mode	Check this box to allow the local DHCP server to assign an IP address to the remote peer. When **NAT Mode** is enabled, all remote traffic over the VPN will be tagged with the assigned IP address using network address translation.
Remote IP Address / Host Names (Optional)	If **NAT Mode** is not enabled, you can enter a remote peer's WAN IP address or hostname(s) here. If the remote uses more than one address, enter only one of them here. Multiple hostnames are allowed and can be separated by a space character or carriage return. Dynamic-DNS host names are also accepted. This field is optional. With this field filled, the Peplink Balance will initiate connection to each of the remote IP addresses until it succeeds in making a connection. If the field is empty, the Peplink Balance will wait for connection from the remote peer. Therefore, at least one of the two VPN peers must specify this value. Otherwise, VPN connections cannot be established.
Data Port	This field is used to specify a UDP port number for transporting outgoing VPN data. If **Default** is selected, UDP port 4500 will be used. Port 32015 will be used if the remote unit uses Firmware prior to version 5.4 or if port 4500 is unavailable. If **Custom** is selected, enter an outgoing port number from 1 to 65535.
Bandwidth Limit	Define maximum download and upload speed to each individual peer. This functionality requires the peer to use PepVPN version 4.0.0 or above.
Cost	Define path cost for this profile. OSPF will determine the best route through the network using the assigned cost. Default: 10

 Copyright @ 2017 Pepwave

10.1 Outbound Policy Management

Pepwave routers can flexibly manage and load balance outbound traffic among WAN connections.

Important Note
Outbound policy is applied only when more than one WAN connection is active.

The settings for managing and load balancing outbound traffic are located at **Advanced>PepVPN**, depending on the model.



10.1.1 Outbound Policy

Outbound policies for managing and load balancing outbound traffic are located at **Network>Outbound Policy>**  or **Advanced>PepVPN>Outbound Policy.**



There are three main selections for the outbound traffic policy:

High Application Compatibility
Normal Application Compatibility
Custom

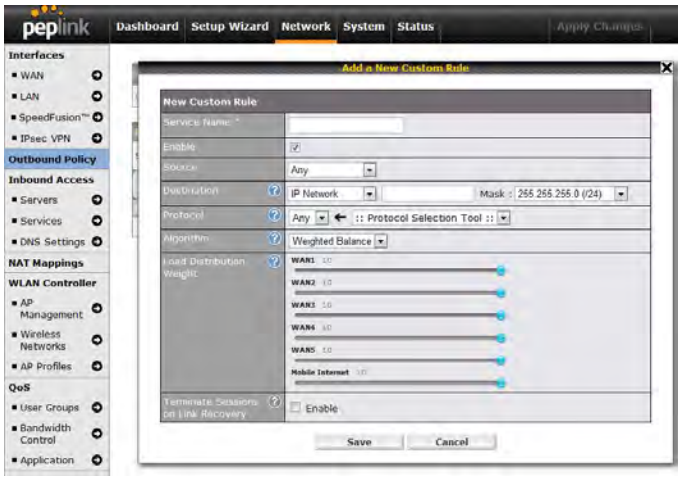
 Copyright @ 2017 Pepwave

Outbound Policy Settings	
High Application Compatibility	Outbound traffic from a source LAN device is routed through the same WAN connection regardless of the destination Internet IP address and protocol. This option provides the highest application compatibility.
Normal Application Compatibility	Outbound traffic from a source LAN device to the same destination Internet IP address will be routed through the same WAN connection persistently, regardless of protocol. This option provides high compatibility to most applications, and users still benefit from WAN link load balancing when multiple Internet servers are accessed.
Custom	Outbound traffic behavior can be managed by defining rules in a custom rule table. A default rule can be defined for connections that cannot be matched with any of the rules.

The default policy is **Normal Application Compatibility**.

Tip

Want to know more about creating outbound rules Visit our YouTube Channel for a video tutorial

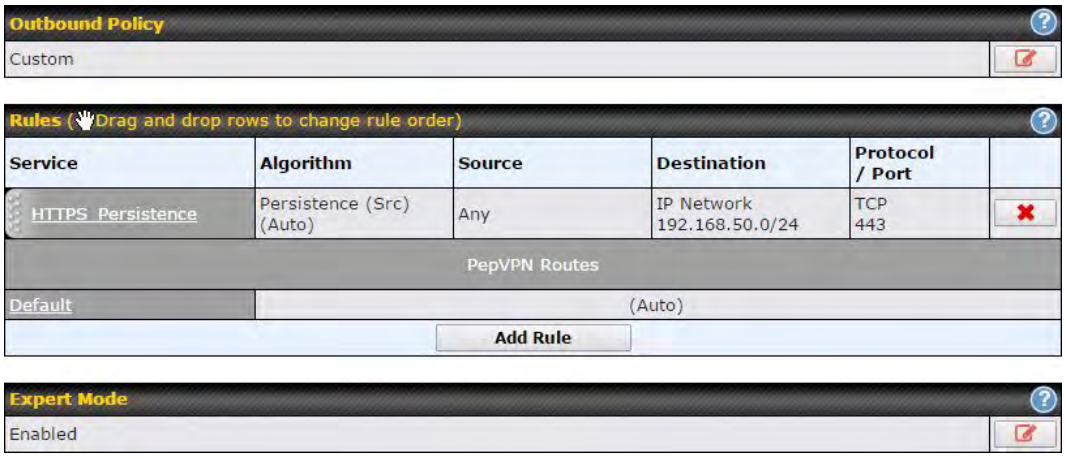


http://youtu.be/rKH4AS b nE

10.1.2 Custom Rules for Outbound Policy

Click  in the **Outbound Policy** form. Choose **Custom** and press the **Save** button.

 Copyright @ 2017 Pepwave



The bottom-most rule is **Default**. Edit this rule to change the device's default manner of controlling outbound traffic for all connections that do not match any of the rules above it. Under the **Service** heading, click **Default** to change these settings.

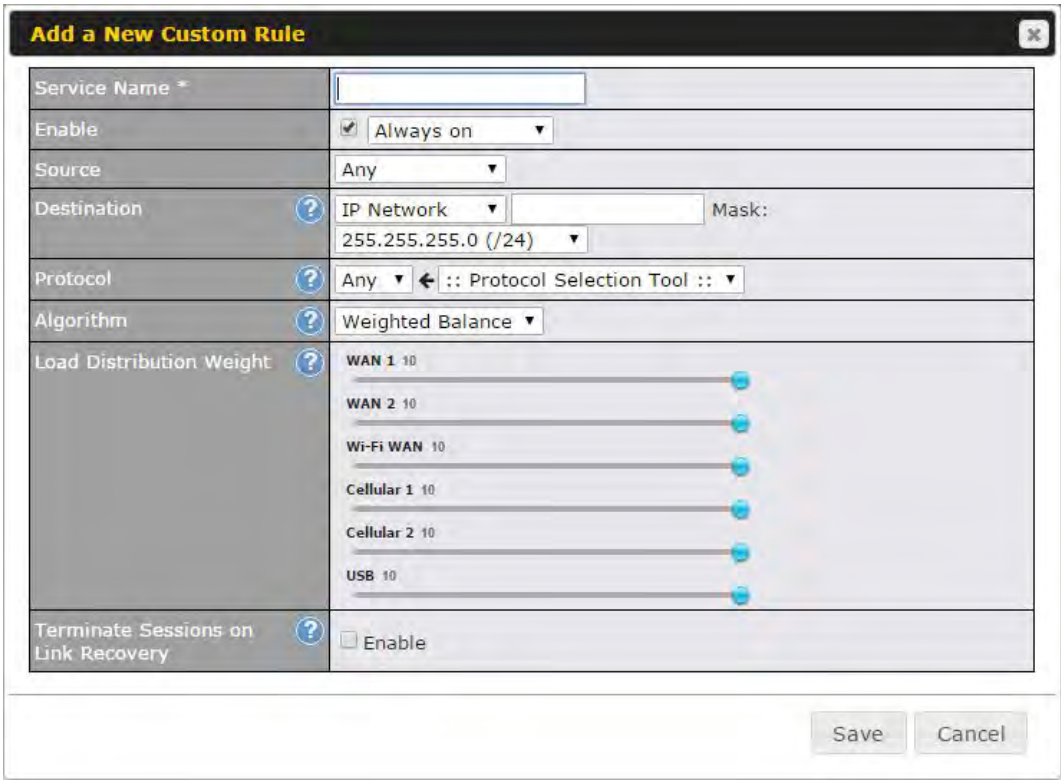
To rearrange the priority of outbound rules, drag and drop them into the desired sequence.



By default, **Auto** is selected as the **Default Rule**. You can select **Custom** to change the algorithm to be used. Please refer to the upcoming sections for the details on the available algorithms.

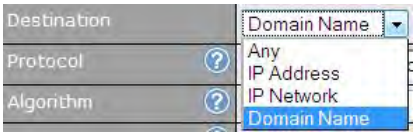
To create a custom rule, click **Add Rule** at the bottom of the table. Note that some Pepwave routers display this button at **Advanced>PepVPN>PepVPN Outbound Custom Rules**.

 Copyright @ 2017 Pepwave



New Custom Rule Settings	
Service Name	This setting specifies the name of the outbound traffic rule.
Enable	This setting specifies whether the outbound traffic rule takes effect. When **Enable** is checked, the rule takes effect: traffic is matched and actions are taken by the Pepwave router based on the other parameters of the rule. When **Enable** is unchecked, the rule does not take effect: the Pepwave router disregards the other parameters of the rule. Click the drop-down menu next to the checkbox to apply a time schedule to this custom rule.
Source	This setting specifies the source IP address, IP network, or MAC address for traffic that matches the rule.
Destination	This setting specifies the destination IP address, IP network, or domain name for traffic that matches the rule.

 Copyright @ 2017 Pepwave



If **Domain Name** is chosen and a domain name, such as *foobar.com*, is entered, any outgoing accesses to *foobar.com* and **.foobar.com* will match this criterion. You may enter a wildcard (.) at the end of a domain name to match any host with a name having the domain name in the middle. If you enter *foobar.*,* for example, *www.foobar.com*, *www.foobar.co.jp*, or *foobar.co.uk* will also match. Placing wildcards in any other position is not supported.

NOTE: if a server has one Internet IP address and multiple server names, and if one of the names is defined here, accesses to any one of the server names will also match this rule.

Protocol and Port

This setting specifies the IP protocol and port of traffic that matches this rule.

Algorithm

This setting specifies the behavior of the Pepwave router for the custom rule.

One of the following values can be selected (note that some Pepwave routers provide only some of these options):

- Weighted Balance
- Persistence
- Enforced
- Priority
- Overflow
- Least Used
- Lowest Latency

The upcoming sections detail the listed algorithms.

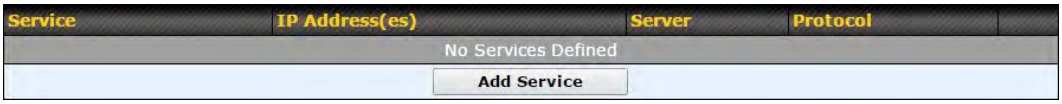
Terminate Sessions on Link Recovery

This setting specifies whether to terminate existing IP sessions on a less preferred WAN connection in the event that a more preferred WAN connection is recovered. This setting is applicable to the **Weighted, Persistence**, and **Priority** algorithms. By default, this setting is disabled. In this case, existing IP sessions will not be terminated or affected when any other WAN connection is recovered. When this setting is enabled, existing IP sessions may be terminated when another WAN connection is recovered, such that only the preferred healthy WAN connection(s) is used at any point in time.

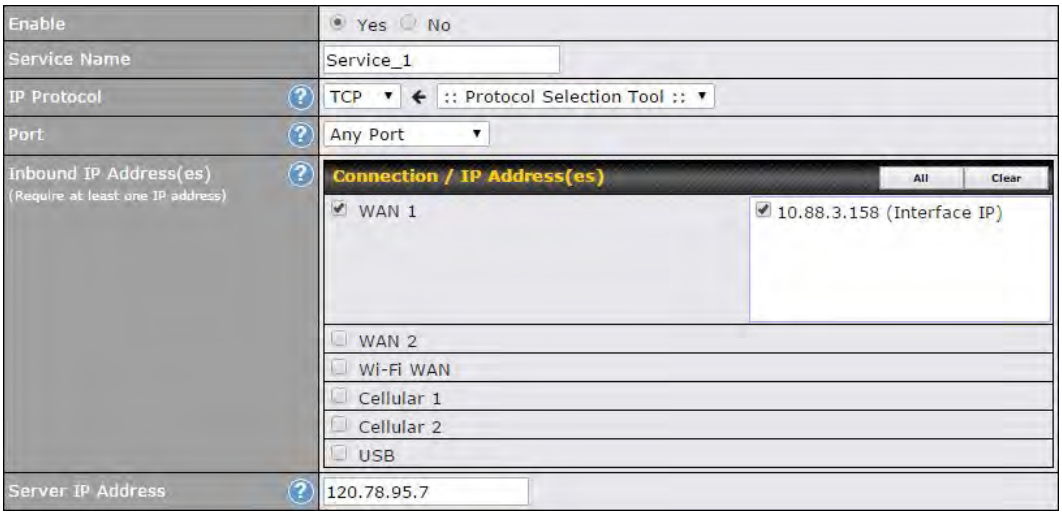
11 Port Forwarding

Pepwave routers can act as a firewall that blocks, by default, all inbound access from the Internet. By using port forwarding, Internet users can access servers behind the Pepwave router. Inbound port forwarding rules can be defined at **Advanced>Port Forwarding**.

 Copyright @ 2017 Pepwave



To define a new service, click **Add Service**.

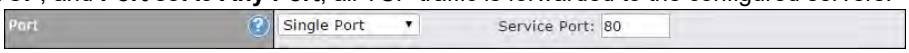


Port Forwarding Settings	
Enable	This setting specifies whether the inbound service takes effect. When **Enable** is checked, the inbound service takes effect: traffic is matched and actions are taken by the Pepwave router based on the other parameters of the rule. When this setting is disabled, the inbound service does not take effect: the Pepwave router disregards the other parameters of the rule.
Service Name	This setting identifies the service to the system administrator. Valid values for this setting consist of only alphanumeric and underscore characters.
IP Protocol	The **IP Protocol** setting, along with the **Port** setting, specifies the protocol of the service as TCP, UDP, ICMP, or IP. Traffic that is received by the Pepwave router via the specified protocol at the specified port(s) is forwarded to the LAN hosts specified by the **Servers** setting. Please see below for details on the **Port** and **Servers** settings. Alternatively, the **Protocol Selection Tool** drop-down menu can be used to automatically fill in the protocol and a single port number of common Internet services (e.g. HTTP, HTTPS, etc.). After selecting an item from the **Protocol Selection Tool** drop-down menu, the protocol and port number remain manually modifiable.
Port	The **Port** setting specifies the port(s) that correspond to the service, and can be configured to behave in one of the following manners: **Any Port**, **Single Port**, **Port Range**, **Port Map**, and **Range Mapping**

 Copyright @ 2017 Pepwave



Any Port: all traffic that is received by the Pepwave router via the specified protocol is forwarded to the servers specified by the **Servers** setting. For example, with **IP Protocol** set to **TCP**, and **Port** set to **Any Port**, all TCP traffic is forwarded to the configured servers.



Single Port: traffic that is received by the Pepwave router via the specified protocol at the specified port is forwarded via the same port to the servers specified by the **Servers** setting. For example, with **IP Protocol** set to **TCP**, and **Port** set to **Single Port** and **Service Port** 80, TCP traffic received on port 80 is forwarded to the configured servers via port 80.



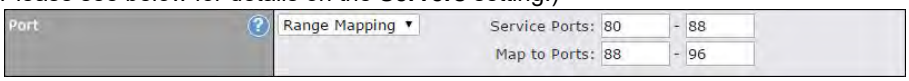
Port Range: traffic that is received by the Pepwave router via the specified protocol at the specified port range is forwarded via the same respective ports to the LAN hosts specified by the **Servers** setting. For example, with **IP Protocol** set to **TCP**, and **Port** set to **Port Range** and **Service Ports** 80-88, TCP traffic received on ports 80 through 88 is forwarded to the configured servers via the respective ports.



Port Mapping: traffic that is received by Pepwave router via the specified protocol at the specified port is forwarded via a different port to the servers specified by the **Servers** setting.

For example, with **IP Protocol** set to **TCP**, and **Port** set to **Port Mapping**, **Service Port** 80, and **Map to Port** 88, TCP traffic on port 80 is forwarded to the configured servers via port 88.

(Please see below for details on the **Servers** setting.)



Range Mapping: traffic that is received by the Pepwave router via the specified protocol at the specified port range is forwarded via a different port to the servers specified by the **Servers** setting.

Inbound IP Address(es)	This setting specifies the WAN connections and Internet IP address(es) from which the service can be accessed.
Server IP Address	This setting specifies the LAN IP address of the server that handles the requests for the service.

11.1 UPnP / NAT-PMP Settings

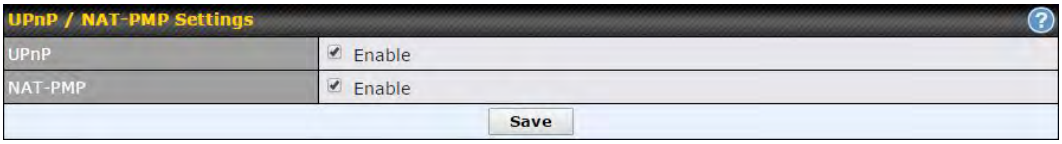
UPnP and NAT-PMP are network protocols which allow a computer connected to the LAN port to automatically configure the router to allow parties on the WAN port to connect to itself. That way, the process of inbound port forwarding becomes automated.

When a computer creates a rule using these protocols, the specified TCP/UDP port of all WAN

 Copyright @ 2017 Pepwave

connections' default IP address will be forwarded.

Check the corresponding box(es) to enable UPnP and/or NAT-PMP. Enable these features only if you trust the computers connected to the LAN ports.



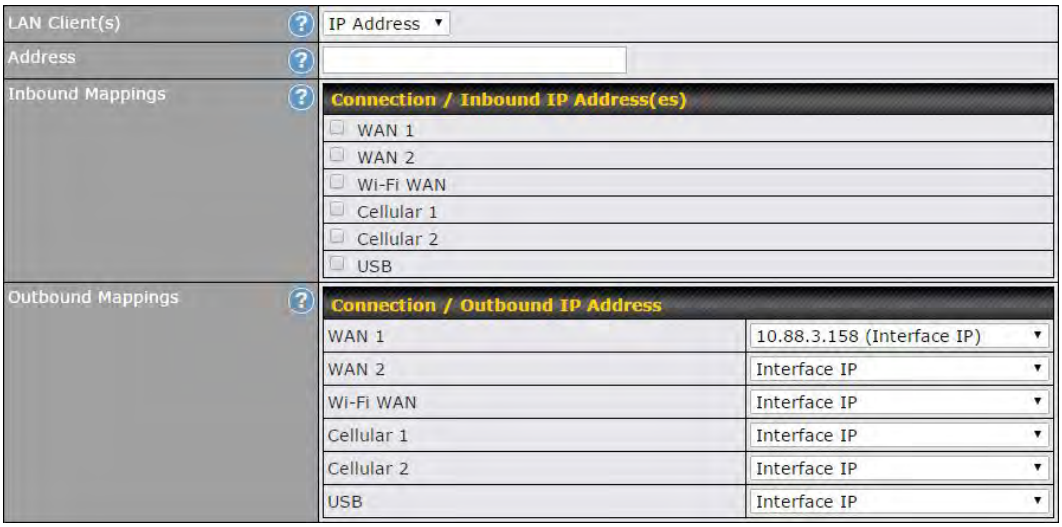
When the options are enabled, a table listing all the forwarded ports under these two protocols can be found at **Status>UPnP / NAT-PMP**.

12 NAT Mappings

NAT mappings allow IP address mapping of all inbound and outbound NAT'd traffic to and from an internal client IP address. Settings to configure NAT mappings are located at **Advanced>NAT Mappings**.



To add a rule for NAT mappings, click **Add NAT Rule**.



 Copyright @ 2017 Pepwave

NAT Mapping Settings	
LAN Client(s)	NAT mapping rules can be defined for a single LAN **IP Address**, an **IP Range**, or an **IP Network**.
Address	This refers to the LAN host s private IP address. The system maps this address to a number of public IP addresses (specified below) in order to facilitate inbound and outbound traffic. This option is only available when **IP Address** is selected.
Range	The IP range is a contiguous group of private IP addresses used by the LAN host. The system maps these addresses to a number of public IP addresses (specified below) to facilitate outbound traffic. This option is only available when **IP Range** is selected.
Network	The IP network refers to all private IP addresses and ranges managed by the LAN host. The system maps these addresses to a number of public IP addresses (specified below) to facilitate outbound traffic. This option is only available when **IP Network** is selected.
Inbound Mappings	This setting specifies the WAN connections and corresponding WAN-specific Internet IP addresses on which the system should bind. Any access to the specified WAN connection(s) and IP address(es) will be forwarded to the LAN host. This option is only available when **IP Address** is selected in the **LAN Client(s)** field. Note that inbound mapping is not needed for WAN connections in drop-in mode or IP forwarding mode. Also note that each WAN IP address can be associated to one NAT mapping only.
Outbound Mappings	This setting specifies the WAN IP addresses that should be used when an IP connection is made from a LAN host to the Internet. Each LAN host in an IP range or IP network will be evenly mapped to one of each selected WAN's IP addresses (for better IP address utilization) in a persistent manner (for better application compatibility). Note that if you do not want to use a specific WAN for outgoing accesses, you should still choose default here, then customize the outbound access rule in the **Outbound Policy** section. Also note that WAN connections in drop-in mode or IP forwarding mode are not shown here.

Click **Save** to save the settings when configuration has been completed.

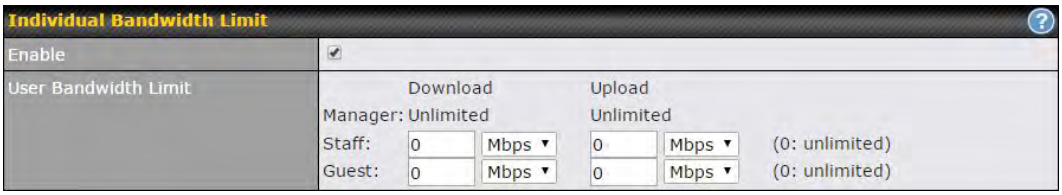
Important Note
Inbound firewall rules override the **Inbound Mappings** settings.

 Copyright @ 2017 Pepwave

13 QoS

13.1 Bandwidth Control

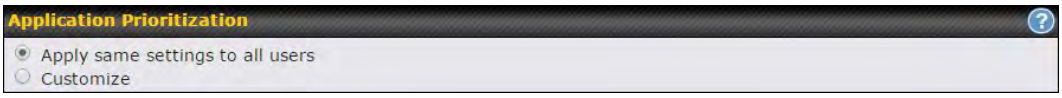
You can define a maximum download speed (over all WAN connections) and upload speed (for each WAN connection) that each individual Staff and Guest member can consume. No limit can be imposed on individual Manager members. By default, download and upload bandwidth limits are set to unlimited (set as **0**).



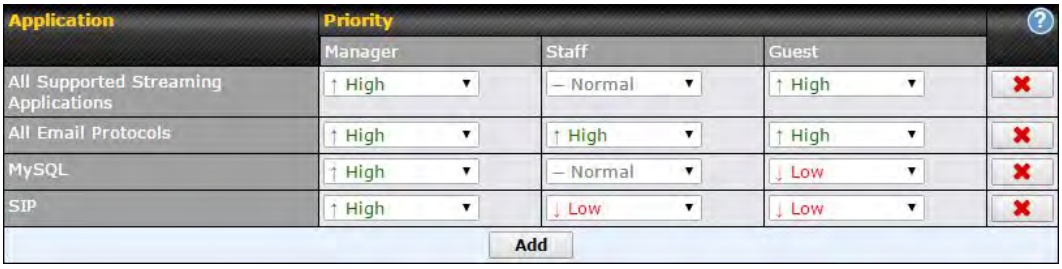
13.2 Application

13.2.1 Application Prioritization

On many Pepwave routers, you can choose whether to apply the same prioritization settings to all user groups or customize the settings for each group.



Three application priority levels can be set: ↑**High**,— **Normal**, and↓**Low**. Pepwave routers can detect various application traffic types by inspecting the packet content. Select an application by choosing a supported application, or by defining a custom application manually. The priority preference of supported applications is placed at the top of the table. Custom applications are at the bottom.

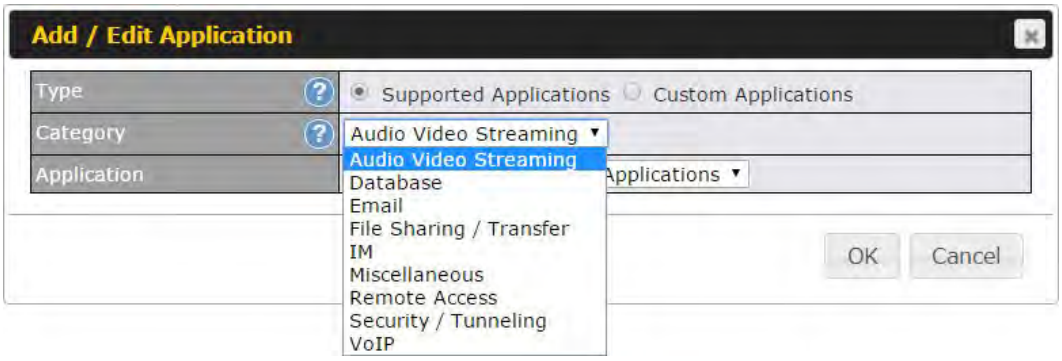


 Copyright @ 2017 Pepwave

13.2.2 Prioritization for Custom Applications

Click the **Add** button to define a custom application. Click the button  in the **Action** column to delete the custom application in the corresponding row.

When **Supported Applications** is selected, the Pepwave router will inspect network traffic and prioritize the selected applications. Alternatively, you can select **Custom Applications** and define the application by providing the protocol, scope, port number, and DSCP value.



13.2.3 DSL/Cable Optimization

DSL/cable-based WAN connections have lower upload bandwidth and higher download bandwidth. When a DSL/cable circuit's uplink is congested, the download bandwidth will be affected. Users will not be able to download data at full speed until the uplink becomes less congested. **DSL/Cable Optimization** can relieve such an issue. When it is enabled, the download speed will become less affected by the upload traffic. By default, this feature is enabled.



14 Firewall

A firewall is a mechanism that selectively filters data traffic between the WAN side (the Internet) and the LAN side of the network. It can protect the local network from potential hacker attacks, access to offensive websites, and/or other inappropriate uses.

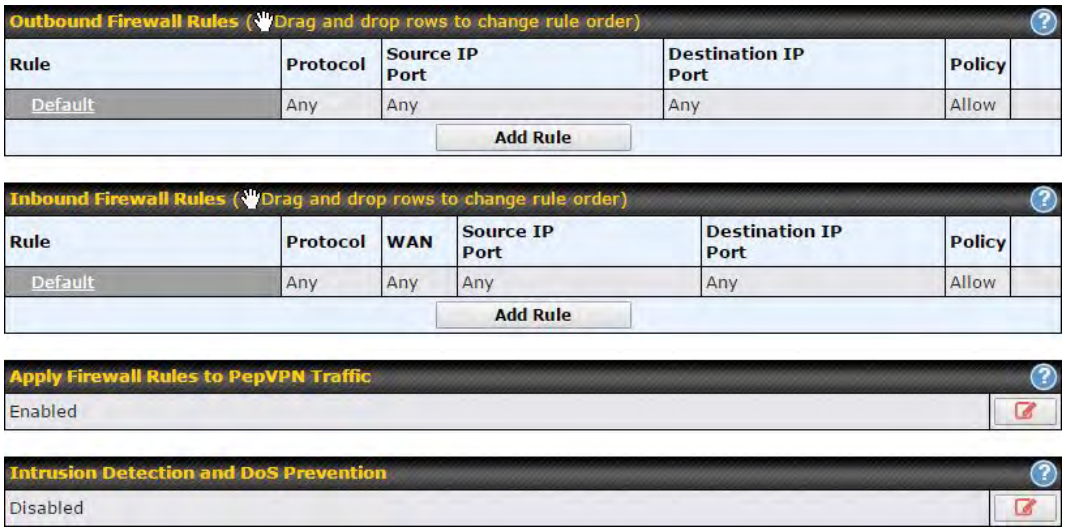
The firewall functionality of Pepwave routers supports the selective filtering of data traffic in both directions:

 Copyright @ 2017 Pepwave

Outbound (LAN to WAN)
Inbound (WAN to LAN)

The firewall also supports the following functionality:

Intrusion detection and DoS prevention
Web blocking



14.1 Outbound and Inbound Firewall Rules

14.1.1 Access Rules

The outbound firewall settings are located at **Advanced>Firewall>Access Rules>Outbound Firewall Rules.**



Click **Add Rule** to display the following screen:

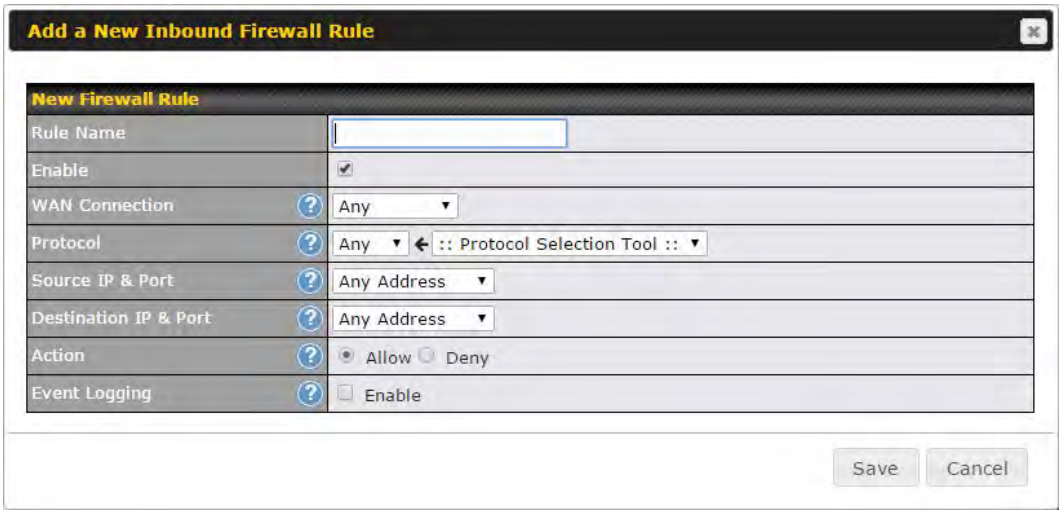
 Copyright @ 2017 Pepwave



Inbound firewall settings are located at **Advanced>Firewall>Access Rules>Inbound Firewall Rules.**

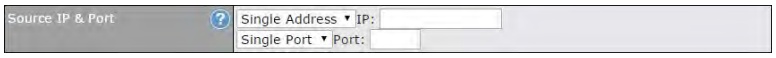
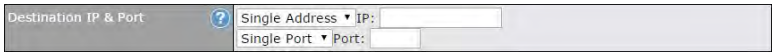


Click **Add Rule** to display the following screen:



Rules are matched from top to bottom. If a connection matches any one of the upper rules, the matching process will stop. If none of the rules match, the **Default** rule will be applied. By default, the **Default** rule is set as **Allow** for both outbound and inbound access.

 Copyright @ 2017 Pepwave

Inbound / Outbound Firewall Settings	
Rule Name	This setting specifies a name for the firewall rule.
Enable	This setting specifies whether the firewall rule should take effect. If the box is checked, the firewall rule takes effect. If the traffic matches the specified protocol/IP/port, actions will be taken by the Pepwave router based on the other parameters of the rule. If the box is not checked, the firewall rule does not take effect. The Pepwave router will disregard the other parameters of the rule. Click the dropdown menu next to the checkbox to place this firewall rule on a time schedule.
WAN Connection (Inbound)	Select the WAN connection that this firewall rule should apply to.
Protocol	This setting specifies the protocol to be matched. Via a drop-down menu, the following protocols can be specified: **TCP** **UDP** **ICMP** **IP** Alternatively, the **Protocol Selection Tool** drop-down menu can be used to automatically fill in the protocol and port number of common Internet services (e.g., HTTP, HTTPS, etc.) After selecting an item from the **Protocol Selection Tool** drop-down menu, the protocol and port number remains manually modifiable.
Source IP & Port	This specifies the source IP address(es) and port number(s) to be matched for the firewall rule. A single address, or a network, can be specified as the **Source IP & Port** setting, as indicated by the following screenshot:  In addition, a single port, or a range of ports, can be specified for the **Source IP & Port** settings.
Destination IP & Port	This specifies the destination IP address(es) and port number(s) to be matched for the firewall rule. A single address, or a network, can be specified as the **Destination IP & Port** setting, as indicated by the following screenshot: 

 Copyright @ 2017 Pepwave

	In addition, a single port, or a range of ports, can be specified for the **Destination IP & Port** settings.
Action	This setting specifies the action to be taken by the router upon encountering traffic that matches the both of the following: Source IP port Destination IP port With the value of **Allow** for the **Action** setting, the matching traffic passes through the router (to be routed to the destination). If the value of the **Action** setting is set to **Deny**, the matching traffic does not pass through the router (and is discarded).
Event Logging	This setting specifies whether or not to log matched firewall events. The logged messages are shown on the page **Status>Event Log**. A sample message is as follows: Aug 13 23:47:44 Denied CONN Ethernet WAN SRC 20.3.2.1 DST 192.168.1.20 LEN 48 PROTO TCP SPT 2260 DPT 80 **CONN:** The connection where the log entry refers to **SRC:** Source IP address **DST:** Destination IP address **LEN:** Packet length **PROTO:** Protocol **SPT:** Source port **DPT:** Destination port

Click **Save** to store your changes. To create an additional firewall rule, click **Add Rule** and repeat the above steps.

To change a rule's priority, simply drag and drop the rule:

Hold the left mouse button on the rule.
Move it to the desired position.
Drop it by releasing the mouse button.

Tip

If the default inbound rule is set to **Allow** for NAT-enabled WANs, no inbound Allow firewall rules will be required for inbound port forwarding and inbound NAT mapping rules. However, if the default inbound rule is set as **Deny**, a corresponding Allow firewall rule will be required.

14.1.2 Apply Firewall Rules to PepVpn Traffic



 Copyright @ 2017 Pepwave

When this option is enabled, Outbound Firew1all Rules will be applied to PepVPN traffic. To turn on this feature, click  , check the **Enable** check box, and press the **Save** button.

14.1.3 Intrusion Detection and DoS Prevention



Pepwave routers can detect and prevent intrusions and denial-of-service (DoS) attacks from the Internet. To turn on this feature, click  , check the **Enable** check box, and press the **Save** button.

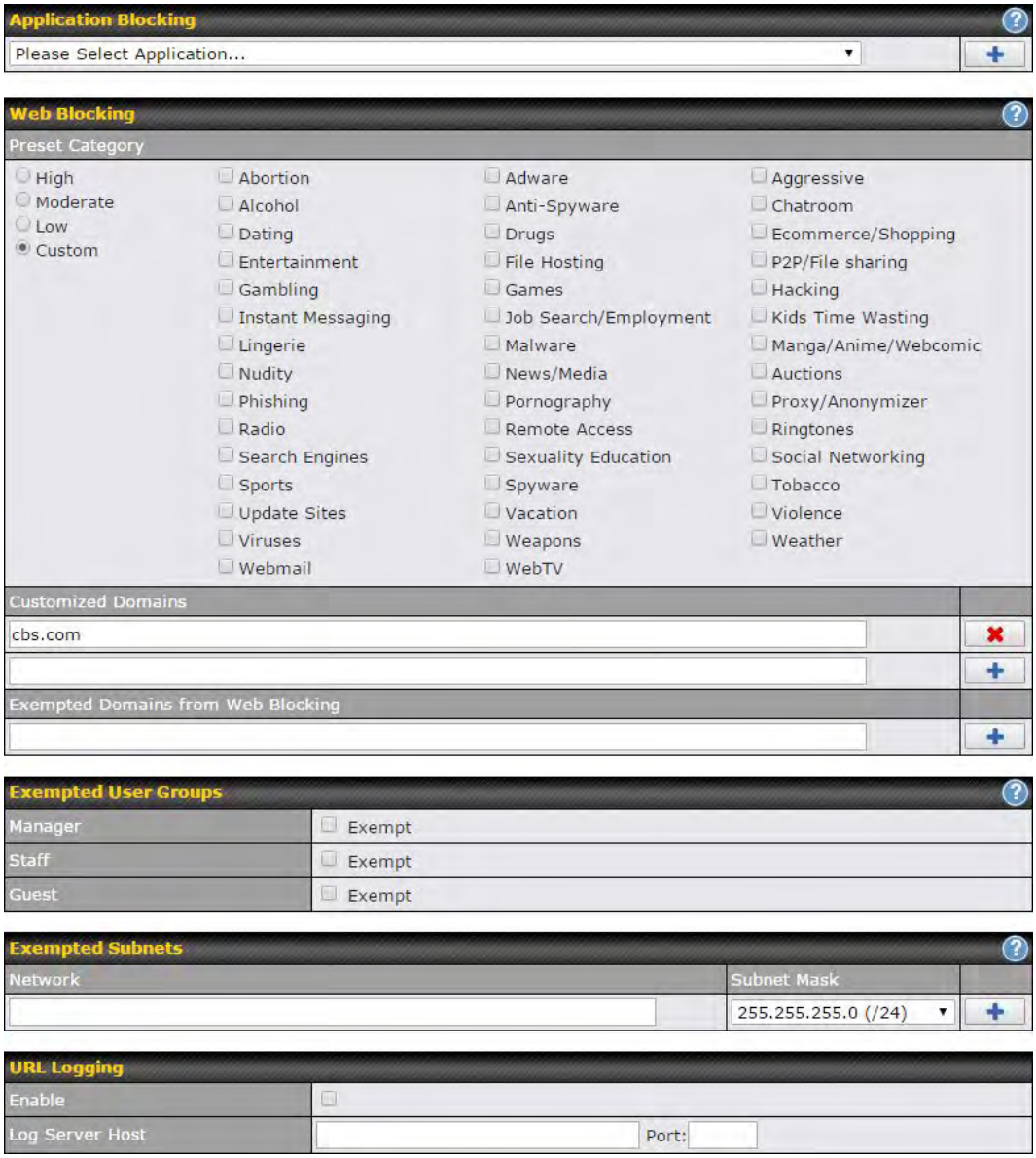
When this feature is enabled, the Pepwave router will detect and prevent the following kinds of intrusions and denial-of-service attacks.

Port scan
- NMAP FIN/URG/PSH
- Xmas tree
- Another Xmas tree
- Null scan
- SYN/RST
- SYN/FIN

SYN flood prevention
Ping flood attack prevention

 Copyright @ 2017 Pepwave

14.2 Content Blocking



14.2.1 Application Blocking

Choose applications to be blocked from LAN/PPTP/PepVPN peer clients' access, except for those on the Exempted User Groups or Exempted Subnets defined below.

 Copyright @ 2017 Pepwave

14.2.2 Web Blocking

Defines web site domain names to be blocked from LAN/PPTP/PepVPN peer clients' access except for those on the Exempted User Groups or Exempted Subnets defined below.

If "foobar.com" is entered, any web site with a host name ending in foobar.com will be blocked, e.g. www.foobar.com, foobar.com, etc. However, "myfoobar.com" will not be blocked.

You may enter the wild card ".*" at the end of a domain name to block any web site with a host name having the domain name in the middle. If you enter "foobar.*", then "www.foobar.com", "www.foobar.co.jp", or "foobar.co.uk" will be blocked. Placing the wild card in any other position is not supported.

The device will inspect and look for blocked domain names on all HTTP traffic. Secure web (HTTPS) traffic is not supported.

14.2.3 Exempted Subnets

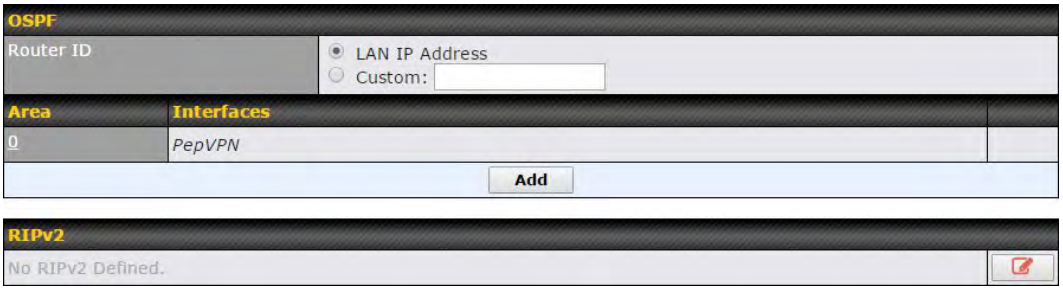
With the subnet defined in the field, clients on the particular subnet(s) can be exempted from the access blocking rules.

14.2.4 URL Logging

Click **enable**, and the enter the ip address and port (if applicable) where your remote syslog server is located.

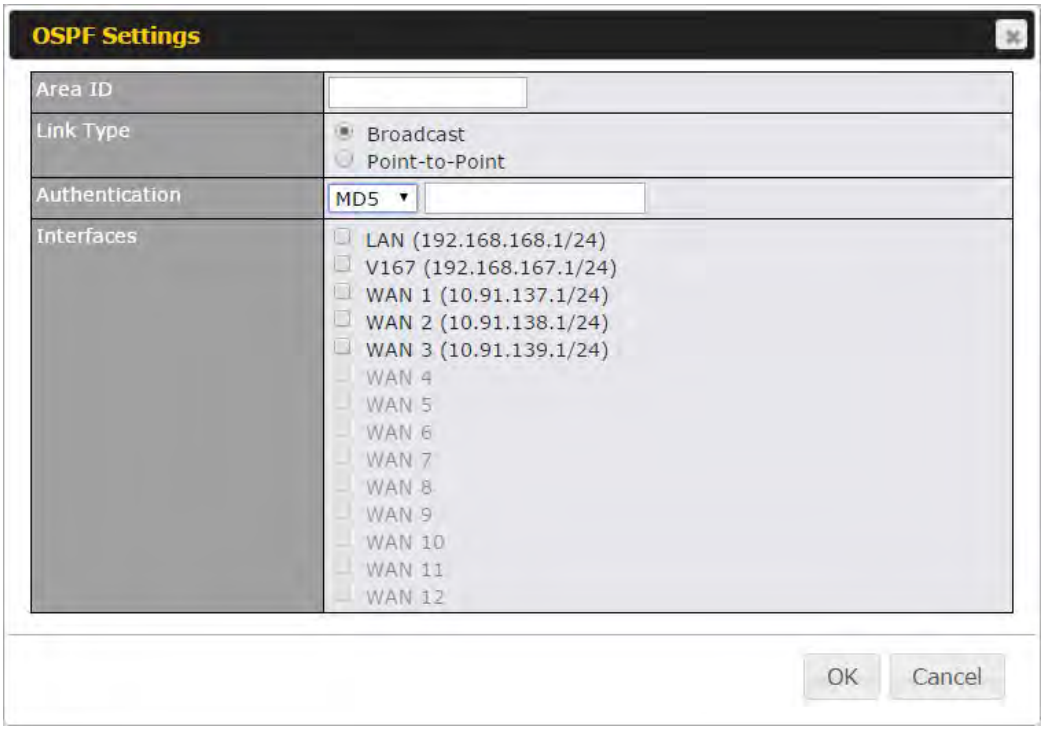
15 OSPF & RIPv2

The Peplink Balance supports OSPF and RIPv2 dynamic routing protocols. Click the **Network** tab from the top bar, and then click the **OSPF & RIPv2** item on the sidebar to reach the following menu:



 Copyright @ 2017 Pepwave

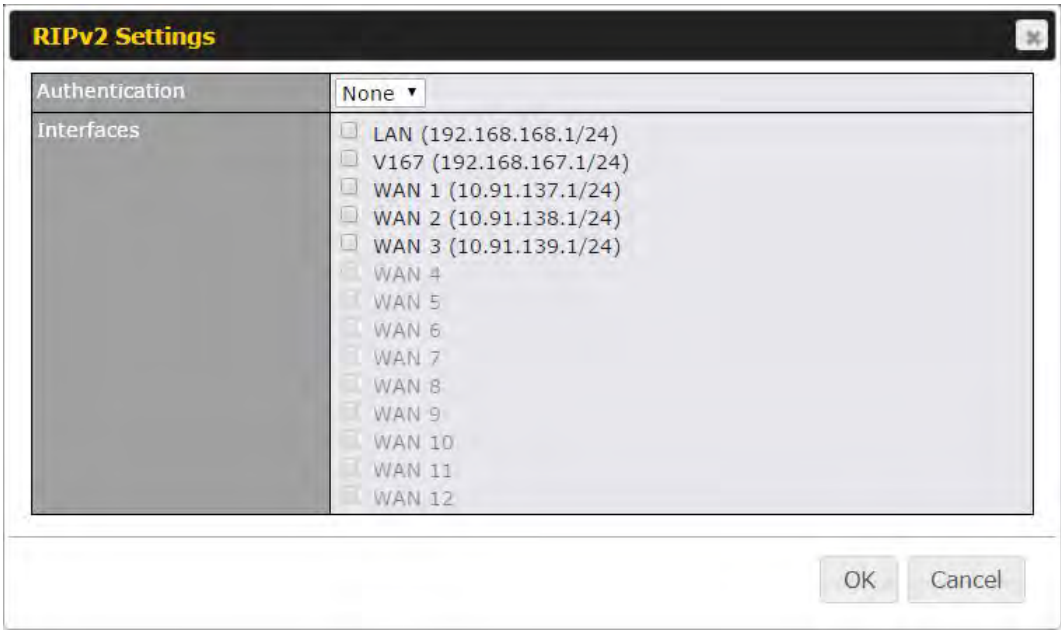
OSPF	
Router ID	This field determines the ID of the router. By default, this is specified as the LAN IP address. If you want to specify your own ID, enter it in the **Custom** field.
Area	This is an overview of the OSPFv2 areas you have defined. Click on the area name to configure it. To set a new area, click **Add**. To delete an existing area, click  .



OSPF Settings	
Area ID	Determine the name of your **Area ID** to apply to this group. Machines linked to this group will send and receive related OSPF packets, while unlinked machines will ignore it.
Link Type	Choose the network type that this area will use.
Authentication	Choose an authentication method, if one is used, from this drop-down menu. Available options are **MD5** and **Text**. Enter the authentication key next to the drop-down menu.
Interfaces	Determine which interfaces this area will use to listen to and deliver OSPF packets

 Copyright @ 2017 Pepwave

To access RIPv2 settings, click  .



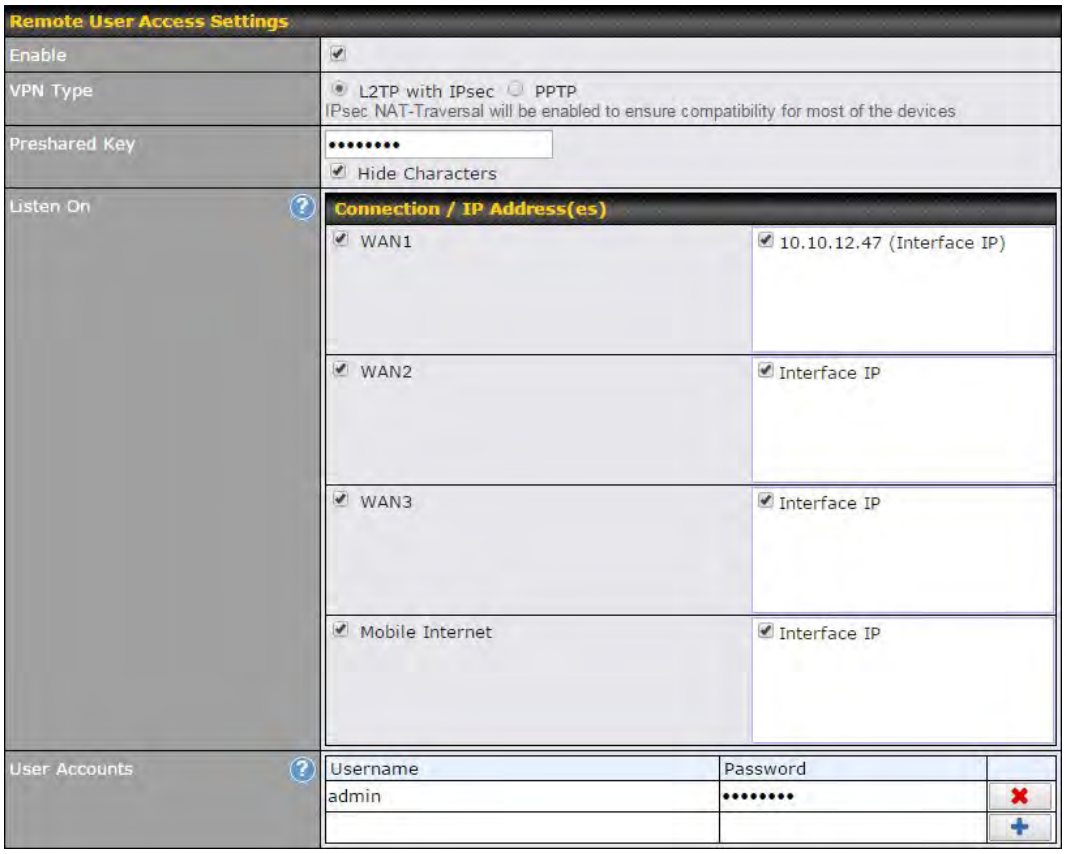
RIPv2 Settings	
Authentication	Choose an authentication method, if one is used, from this drop-down menu. Available options are **MD5** and **Text**. Enter the authentication key next to the drop-down menu.
Interfaces	Determine which interfaces this group will use to listen to and deliver RIPv2 packets.

16 Miscellaneous

16.1 Remote User Access

Networks routed by a Peplink Balance can be remotely accessed via L2TP with IPsec or PPTP. To configure this feature, navigate to **Network > Remote User Access**

 Copyright @ 2017 Pepwave



Remote User Access Settings	
Enable	Click the checkbox to enable Remote User Access.
VPN Type	Determine whether remote devices can connect to the Balance using L2TP with IPsec or PPTP. For greater security, we recommend you connect using L2TP with IPsec.
Preshared Key	Enter your pre-shared key in the text field. Please note that remote devices will need this preshared key to access the Balance.
Listen On	This setting is for specifying the WAN IP addresses where the PPTP server of the router should listen on.
User Accounts	This setting allows you to define the PPTP User Accounts. Click Add to input username and password to create an account. After adding the user accounts, you can click on a username to edit the account password. Click the button X to delete the account in its corresponding row.

 Copyright @ 2017 Pepwave

Click the button to switch to enters user accounts by pasting the information in.CSV format.

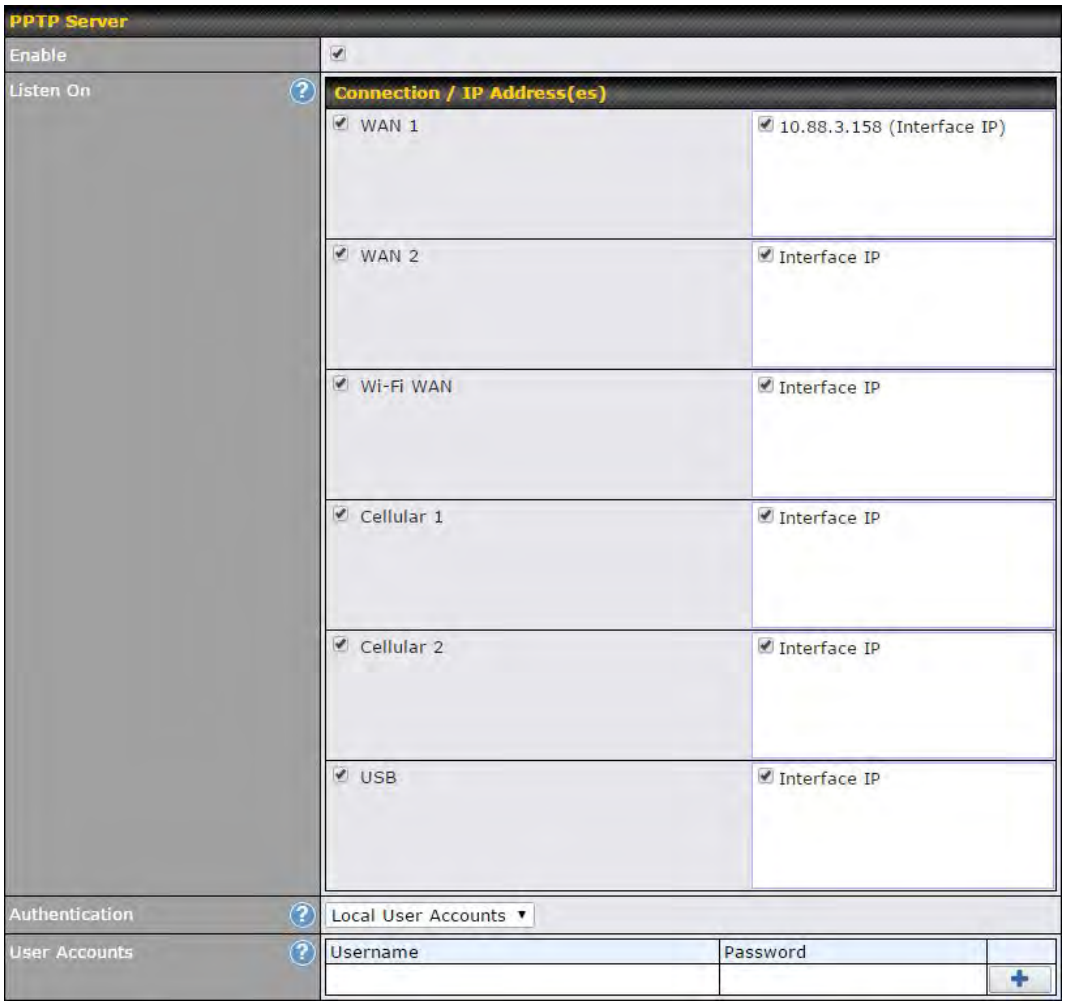
16.2 PPTP Server



Pepwave routers feature a built-in PPTP server, which enables remote computers to conveniently and securely access the local network. PPTP server settings are located at **Advanced>Misc. Settings>PPTP Server.**

Check the box to enable PPTP server functionality. All connected PPTP sessions are displayed at **Status>Client List**.

 Copyright @ 2017 Pepwave



PPTP Server Settings	
Listen On	This setting is for specifying the WAN connection(s) and IP address(es) that the PPTP server should listen on.
Authentication	This setting is for specifying the user database source for PPTP authentication. Three sources can be selected: **Local User Accounts, LDAP Server,** or **RADIUS Server**. **Local User Accounts** - User accounts are stored in the Pepwave router locally. You can add/modify/delete accounts in the **User Accounts** table. **LDAP Server** - Authenticate with an external LDAP server. This has been tested with Open LDAP servers where passwords are NTLM hashed. Active Directory is not supported. (You can choose to use RADIUS to authenticate with a Windows server.)

 Copyright @ 2017 Pepwave

	RADIUS Server - Authenticate with an external RADIUS server. This has been tested with Microsoft Windows Internet Authentication Service and FreeRADIUS servers where passwords are NTLM hashed or in plain text.
User Accounts	This setting allows you to define PPTP user accounts for authentication via local user accounts. Click **Add** to input username and password to create an account. After adding the user accounts, you can click on a username to edit the account password. Click  to delete the account in its corresponding row.

16.3 Certificate Manager



This section allows you to assign certificates for local VPN and web admin SSL. The local keys will not be transferred to another device by any means.

16.4 Service Forwarding

Service forwarding settings are located at **Advanced>Misc. Settings>Service Forwarding**.



Service Forwarding	
SMTP Forwarding	When this option is enabled, all outgoing SMTP connections destined for any host at TCP port 25 will be intercepted. These connections will be redirected to a specified SMTP server and port number. SMTP server settings for each WAN can be specified after selecting **Enable**.
Web Proxy	When this option is enabled, all outgoing connections destined for the proxy server specified in **Web Proxy Interception Settings** will be intercepted. These

 Copyright @ 2017 Pepwave

Forwarding	connections will be redirected to a specified web proxy server and port number. Web proxy interception settings and proxy server settings for each WAN can be specified after selecting **Enable**.
DNS Forwarding	When this option is enabled, all outgoing DNS lookups will be intercepted and redirected to the built-in DNS name server. If any LAN device is using the DNS name servers of a WAN connection, you may want to enable this option to enhance the DNS availability without modifying the DNS server setting of the clients. The built-in DNS name server will distribute DNS lookups to corresponding DNS servers of all available WAN connections. In this case, DNS service will not be interrupted, even if any WAN connection is down.
Custom Service Forwarding	When custom service forwarding is enabled, outgoing traffic with the specified TCP port will be forwarded to a local or remote server by defining its IP address and port number.

16.4.1 SMTP Forwarding

Some ISPs require their users to send e-mails via the ISP's SMTP server. All outgoing SMTP connections are blocked except those connecting to the ISP's. Pepwave routers support intercepting and redirecting all outgoing SMTP connections (destined for TCP port 25) via a WAN connection to the WAN's corresponding SMTP server.



To enable the feature, select **Enable** under **SMTP Forwarding Setup**. Check **Enable Forwarding** for the WAN connection(s) that needs forwarding. Under **SMTP Server**, enter the ISP's email server hostname or IP address. Under **SMTP Port**, enter the TCP port number for each WAN.

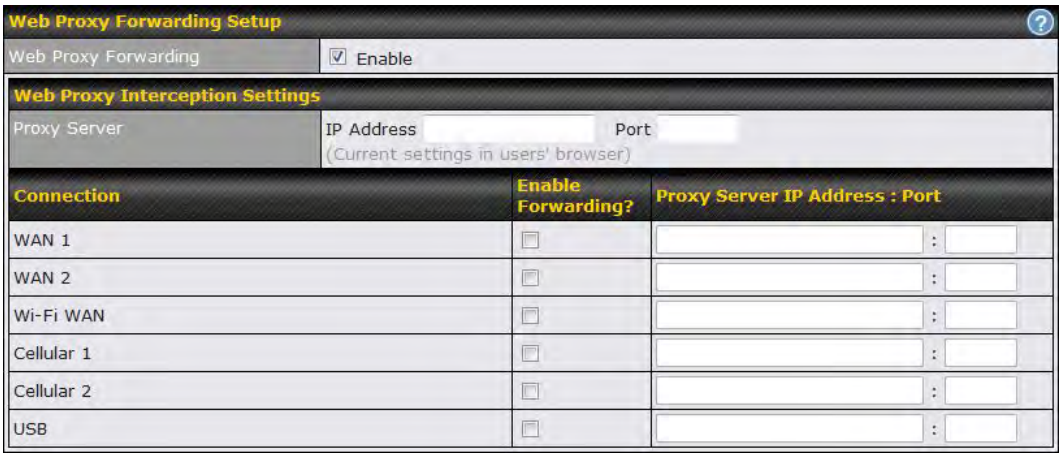
The Pepwave router will intercept SMTP connections. Choose a WAN port according to the outbound policy, and then forward the connection to the SMTP server if the chosen WAN has enabled forwarding. If the forwarding is disabled for a WAN connection, SMTP connections for the WAN will be simply be forwarded to the connection's original destination.

Note

 Copyright @ 2017 Pepwave

If you want to route all SMTP connections only to particular WAN connection(s), you should create a custom rule in outbound policy (see **Section 14.2**).

16.4.2 Web Proxy Forwarding



When this feature is enabled, the Pepwave router will intercept all outgoing connections destined for the proxy server specified in **Web Proxy Interception Settings**, choose a WAN connection with reference to the outbound policy, and then forward them to the specified web proxy server and port number. Redirected server settings for each WAN can be set here. If forwarding is disabled for a WAN, web proxy connections for the WAN will be simply forwarded to the connection's original destination.

16.4.3 DNS Forwarding



When DNS forwarding is enabled, all clients' outgoing DNS requests will also be intercepted and forwarded to the built-in DNS proxy server.

16.4.4 Custom Service Forwarding



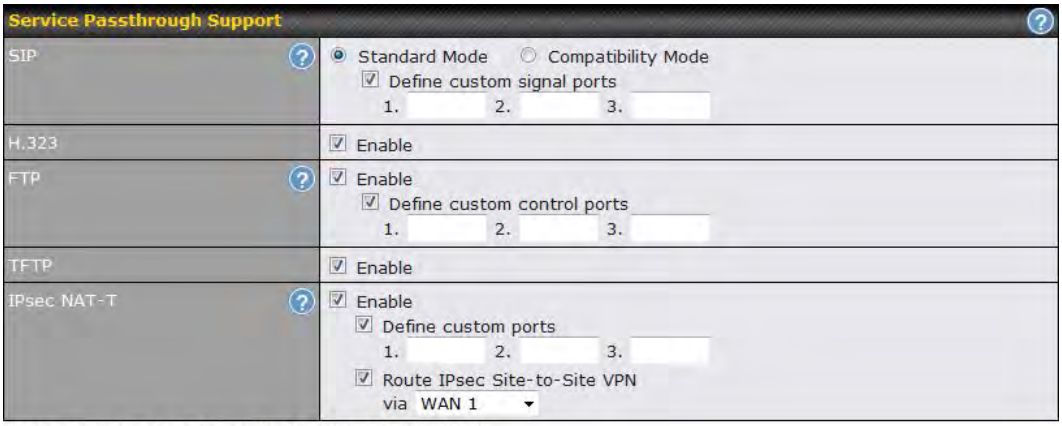
After clicking the **enable** checkbox, enter your TCP port for traffic heading to the router, and then

 Copyright @ 2017 Pepwave

specify the IP Address and Port of the server you wish to forward to the service to.

16.5 Service Passthrough

Service passthrough settings can be found at **Advanced>Misc. Settings>Service Passthrough**.



Some Internet services need to be specially handled in a multi-WAN environment. Pepwave routers can handle these services such that Internet applications do not notice being behind a multi-WAN router. Settings for service passthrough support are available here.

Service Passthrough Support	
SIP	Session initiation protocol, aka SIP, is a voice-over-IP protocol. The Pepwave router can act as a SIP application layer gateway (ALG) which binds connections for the same SIP session to the same WAN connection and translate IP address in the SIP packets correctly in NAT mode. Such passthrough support is always enabled, and there are two modes for selection: **Standard Mode** and **Compatibility Mode**. If your SIP server s signal port number is non-standard, you can check the box **Define custom signal ports** and input the port numbers to the text boxes.
H.323	With this option enabled, protocols that provide audio-visual communication sessions will be defined on any packet network and pass through the Pepwave router.
FTP	FTP sessions consist of two TCP connections; one for control and one for data. In a multi-WAN situation, they must be routed to the same WAN connection. Otherwise, problems will arise in transferring files. By default, the Pepwave router monitors TCP control connections on port 21 for any FTP connections and binds TCP connections of the same FTP session to the same WAN. If you have an FTP server listening on a port number other than 21, you can check **Define custom control ports** and enter the port numbers in the text boxes.

 Copyright @ 2017 Pepwave

TFTP	The Pepwave router monitors outgoing TFTP connections and routes any incoming TFTP data packets back to the client. Select **Enable** if you want to enable TFTP passthrough support.
IPsec NAT-T	This field is for enabling the support of IPsec NAT-T passthrough. UDP ports 500, 4500, and 10000 are monitored by default. You may add more custom data ports that your IPsec system uses by checking **Define custom ports**. If the VPN contains IPsec site-to-site VPN traffic, check **Route IPsec Site-to-Site VPN** and choose the WAN connection to route the traffic to.

16.6 Sim Toolkit

Sim Toolkit option can be found at **Advance>Settings>SIM Toolkit.**

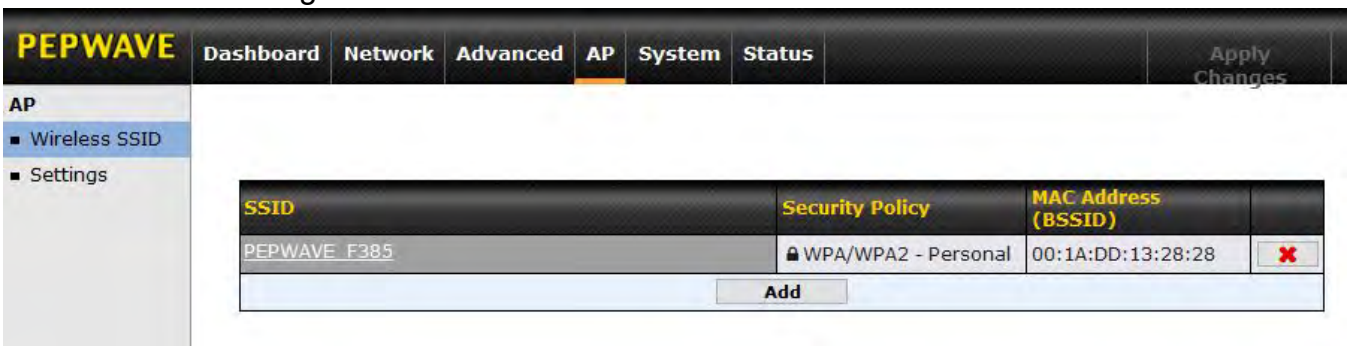


17 AP

Use the controls on the AP tab to set the wireless SSID and AP settings.

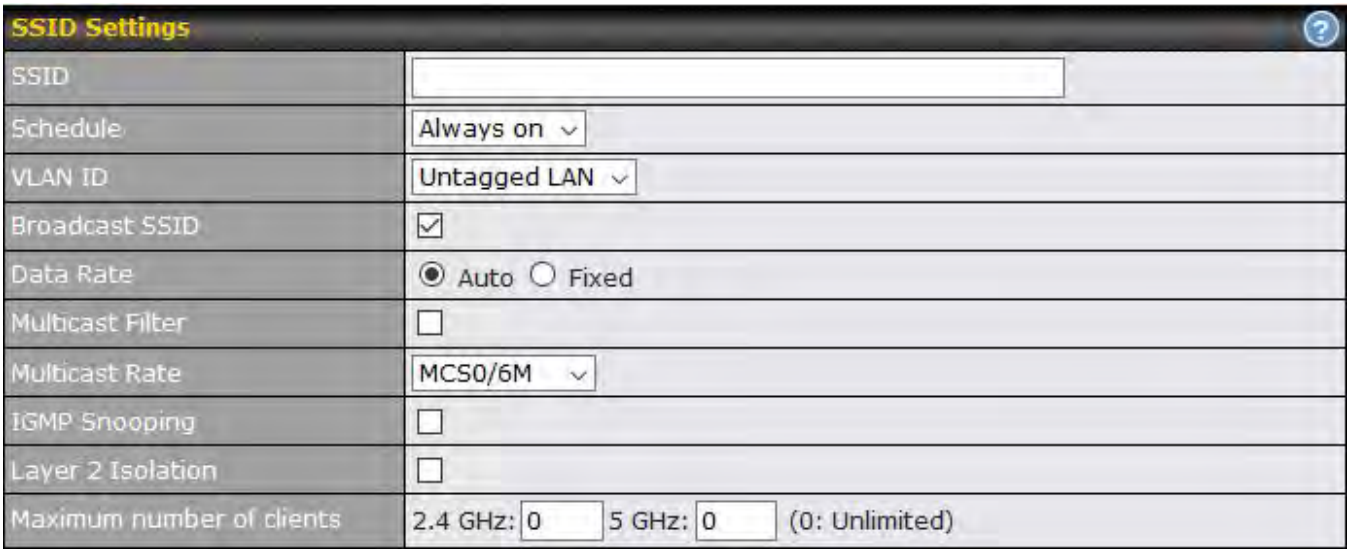
17.1 Wireless SSID

Wireless network settings, including the name of the network (SSID) and security policy, can be defined and managed in this section.



Click **Add** to create a new network profile, or click the existing network profile to modify its settings.

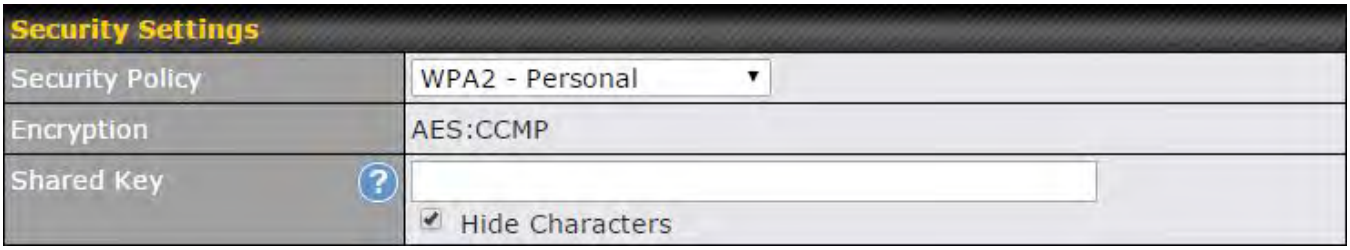
 Copyright @ 2017 Pepwave



SSID Settings	
SSID	This setting specifies the Router SSID that Wi-Fi clients will see when scanning.
Schedule	Click the drop-down menu to choose pre-defined schedules as your starting point. Please note that upon selection, previous changes on the schedule map will be deleted.
VLAN ID	Some service providers require the router to enable VLAN tagging for Internet traffic. If it is required by your service provider, you can enable this field and enter the VLAN ID that the provider requires.
Broadcast SSID	This setting specifies whether or not Wi-Fi clients can scan the SSID of this wireless network. Broadcast SSID is enabled by default.
Data Rate	Select Auto to allow your access point to set the data rate automatically, or select Fixed and choose a rate from the drop-down menu. Click the MCS Index link to display a reference table containing MCS and matching HT20 and HT40 values.
Multicast Filter	This setting enables the filtering of multicast network traffic to the wireless SSID.
Multicast Rate	This setting specifies the transmit rate to be used for sending multicast network traffic.
IGMP Snooping	To allow your access point to convert multicast traffic to unicast traffic for associated clients, select this option.

 Copyright @ 2017 Pepwave

Layer 2 Isolation	Layer 2 refers to the second layer in the ISO Open System Interconnect model. When this option is enabled, clients on the same VLAN, SSID, or subnet are isolated to that VLAN, SSID, or subnet, which can enhance security. Traffic is passed to upper communication layer(s). By default, the setting is disabled.
Maximum no of Clients	Enter the maximum number of clients that can simultaneously connect to your access point, or enter 0 to allow unlimited Wi-Fi clients.



Security Settings	
Security Policy	This setting configures the wireless authentication and encryption methods. Available options are Open (No Encryption), WPA/WPA2 - Personal, WPA/WPA2 Enterprise and Static WEP.



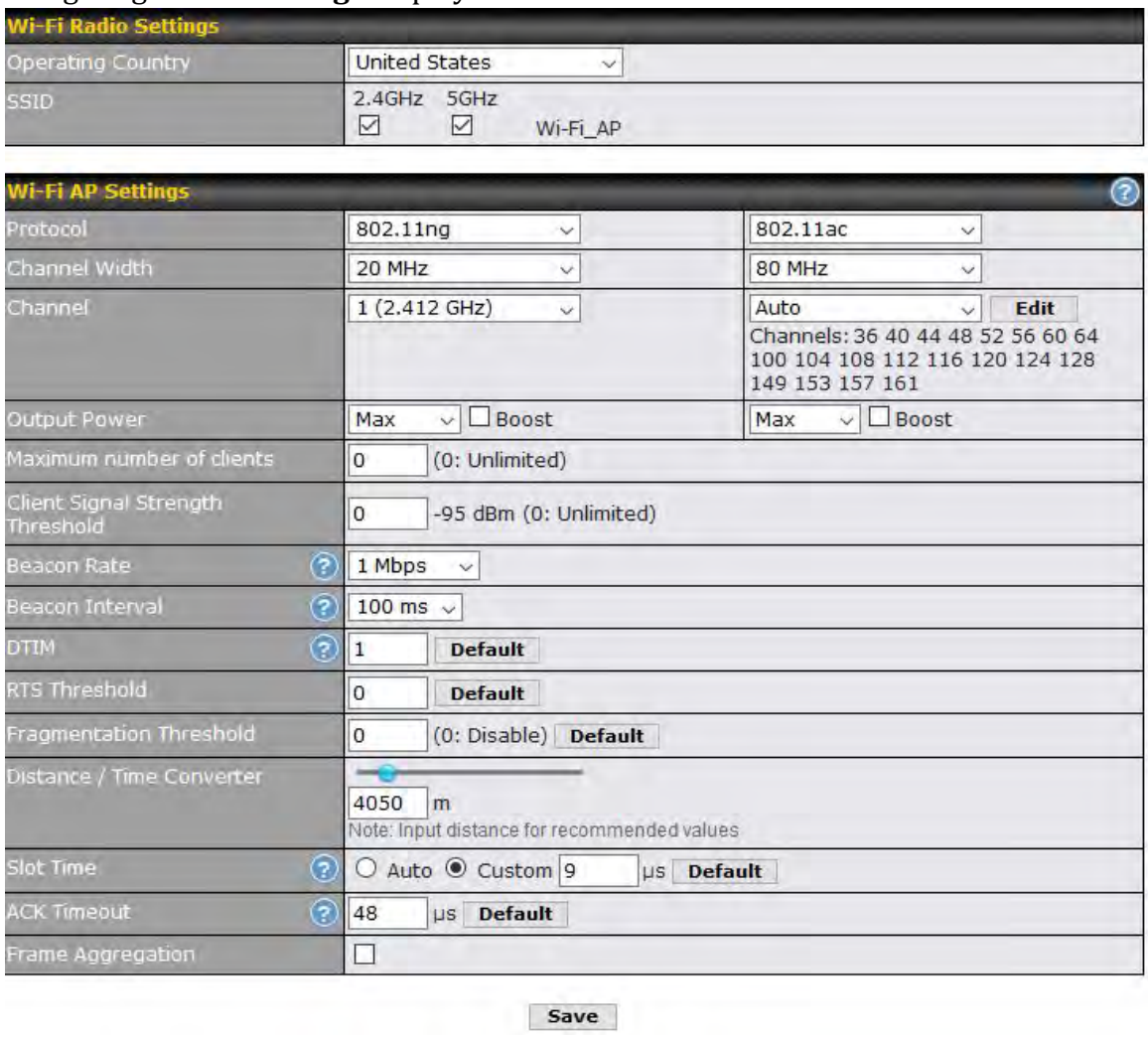
Access Control	
Restricted Mode	The settings allow administrator to control access using Mac address filtering. Available options are None, Deny all except listed, Accept all except listed, and RADIUS MAC Authentication. When WPA/WPA2 - Enterprise is configured, RADIUS-based 802.1 x authentication is enabled. Under this configuration, the Shared Key option should be disabled. When using this method, select the appropriate version using the V1/V2 controls. The security level of this method is known to be very high. When WPA/WPA2- Personal is configured, a shared key is used for data encryption and authentication. When using this configuration, the Shared Key option should be enabled. Key length must be between eight and 63 characters (inclusive). The security level of this method is known to be high. The configuration of Static WEP parameters enables pre-shared WEP key encryption.

 Copyright @ 2017 Pepwave

	Authentication is not supported by this method. The security level of this method is known to be weak.
MAC Address List	Connection coming from the MAC addresses in this list will be either denied or accepted based the option selected in the previous field.

17.2 Settings

Navigating to **AP>Settings** displays a screen similar to the one shown below:



 Copyright @ 2017 Pepwave

Wi-Fi Radio Settings	
Operating Country	This option sets the country whose regulations the Pepwave router follows.
Wi-Fi Antenna	Choose from the router's internal or optional external antennas, if so equipped.

Important Note

Per FCC regulations, the country selection is not available on all models marketed in the US. All US models are fixed to US channels only.

Wi-Fi AP Settings	
Protocol	This option allows you to specify which client association requests will be accepted. By default, **802.11ng** is selected.
Channel Width	**Auto (20/40 MHz)** and **20 MHz** are available. The default setting is **Auto (20/40 MHz),** which allows both widths to be used simultaneously. **Auto (80 MHz)** and **(20/40 MHz)** are available. The default setting is **80 MHz**.
Channel	This option allows you to select which 802.11 RF channel will be used.
Output Power	This option is for specifying the transmission output power for the Wi-Fi AP. There are 4 relative power levels available – **Max**, **High**, **Mid**, and **Low**. The actual output power will be bound by the regulatory limits of the selected country.
Maximum number of clients	Enter the maximum number of clients that can simultaneously connect to the wireless network or enter 0 to allow an unlimited number of connections.
Client Signal Strength Threshold[A]	This field determines that maximum signal strength each individual client will receive. The measurement unit is megawatts.
Beacon Rate[A]	This option is for setting the transmit bit rate for sending a beacon. By default, **1Mbps** is selected.

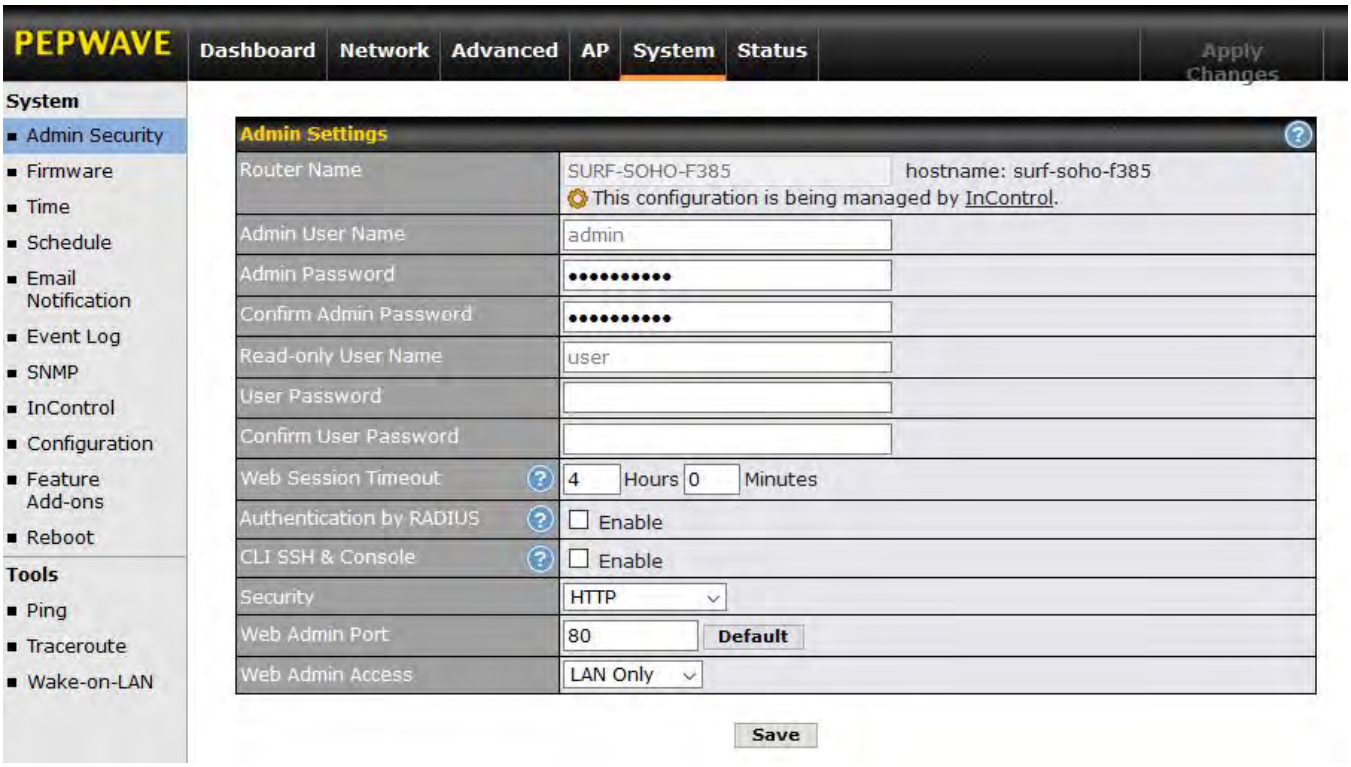
 Copyright @ 2017 Pepwave

Beacon Interval[A]	This option is for setting the time interval between each beacon. By default, **100ms** is selected.
DTIM[A]	This field allows you to set the frequency for the beacon to include a delivery traffic indication message. The interval is measured in milliseconds. The default value is set to **1 ms**.
RTS Threshold	Set the minimum packet size for your access point to send an RTS using the RTS/CTS handshake. Setting 0 disables this feature.
Fragmentation Threshold[A]	Determines the maximum size (in bytes) that each packet fragment will be broken down into. Set 0 to disable fragmentation.
Distance/Time Converter[A]	Select the distance you want your Wi-Fi to cover in order to adjust the below parameters. Default values are recommended.
Slot Time[A]	This field is for specifying the wait time before the Surf SOHO transmits a packet. By default, this field is set to **9 µs**.
ACK Timeout[A]	This field is for setting the wait time to receive an acknowledgement packet before performing a retransmission. By default, this field is set to **48 µs**.
Frame Aggregation[A]	This option allows you to enable frame aggregation to increase transmission throughput.

18 System Settings

The options on the System tab control login and security settings, firmware upgrades, SNMP settings, and other settings.

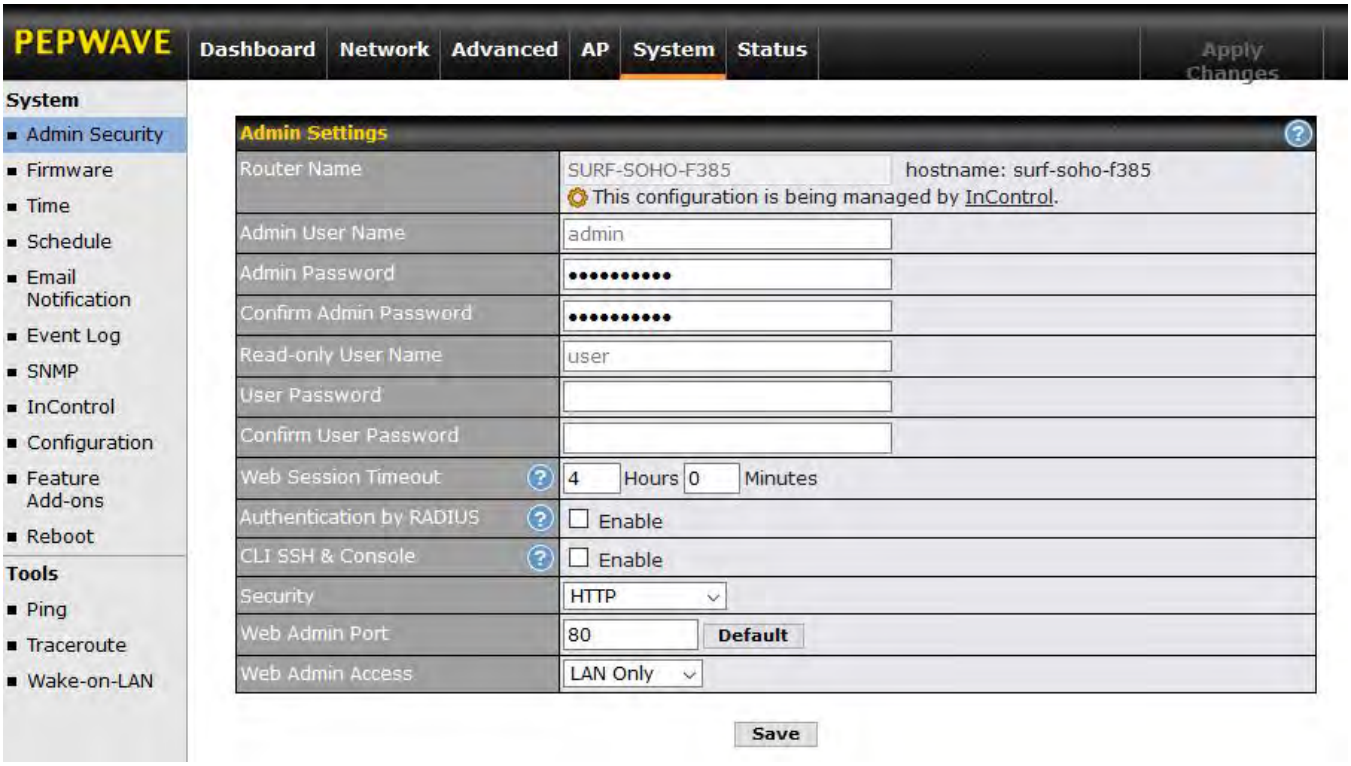
 Copyright @ 2017 Pepwave



18.1 Admin Security

The **Admin Security** section allows you to set up your access point's name, password, security settings, and other options

 Copyright @ 2017 Pepwave



Admin Security	
Router Name	Enter a name to identify your **Router**.
Admin User Name	This field specifies the **administrator username** of the web admin. It is set as **admin** by default
Admin Password	This field allows you to specify a new administrator password. The default **password** is public
Confirm Admin Password	This field allows you to verify and confirm the new administrator password.
Read-only User Name	Read-only User Name is set as **user**
User Password	This field allows you to specify a new user password. Once the user password is set, the read-only user feature will be enabled

 Copyright @ 2017 Pepwave

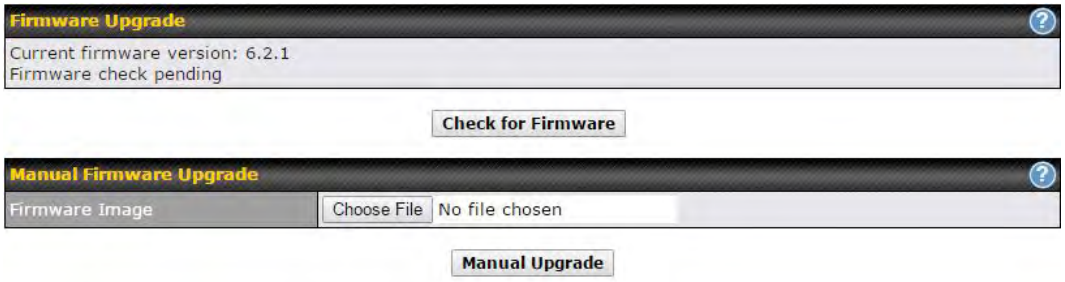
Confirm User Password	This field allows you to verify and confirm the new user password
Web Session Timeout	This field specifies the number of hours and minutes that a web session can remain idle before the Router terminates its access to the web admin interface. By default, it is set to **4 hours.**
Authentication by RADIUS	With this box checked, the web admin will authenticate using an external RADIUS server. Authenticated users are treated as either Admin with full read-write permission or user with read-only access. Local admin and user accounts will be disabled. When the device is not able to communicate with external RADIUS server, local accounts will be enabled again for emergency access. Additional authentication options will be available once this box is checked
Auth Protocol	This specifies the authentication protocol used. Available options are MS-CHAP v2 and PAP.
Auth Server	This specifies the access address and port of the external RADIUS server.
Auth Server Secret	This field is for entering the secret key for accessing the RADIUS server.
Auth Timeout	This option specifies the time value for authentication timeout.
Accounting Server	This specifies the access address and port of the external accounting server.
Accounting Server Secret	This field is for entering the secret key for accessing the accounting server.
CLI SSH & Console	The CLI (command line interface) can be accessed via SSH. This field enables CLI support
Security	This option is for specifying the protocol(s) through which the web admin interface can be accessed: HTTP HTTPS HTTP/HTTPS
Web Admin Port	This field is for specifying the port number on which the web admin interface can be accessed.
Web Admin	This option is for specifying the network interfaces through which the web admin

 Copyright @ 2017 Pepwave

Access	interface can be accessed: LAN only LAN/WAN If LAN/WAN is chosen, the WAN Connection Access Settings form will be displayed.

18.2 Firmware

Pepwave router firmware is upgradeable through the web admin interface. Firmware upgrade functionality is located at **System>Firmware**.



There are two ways to upgrade the unit. The first method is through an online download. The second method is to upload a firmware file manually.

To perform an online download, click on the **Check for Firmware** button. The Pepwave router will check online for new firmware. If new firmware is available, the Pepwave router will automatically download the firmware. The rest of the upgrade process will be automatically initiated.

You may also download a firmware image from the Peplink website and update the unit manually. To update using a firmware image, click **Choose File** to select the firmware file from the local computer, and then click **Manual Upgrade** to send the firmware to the Pepwave router. It will then automatically initiate the firmware upgrade process.

Please note that all Peplink devices can store two different firmware versions in two different partitions. A firmware upgrade will always replace the inactive partition. If you want to keep the inactive firmware, you can simply reboot your device with the inactive firmware and then perform the firmware upgrade.

Important Note

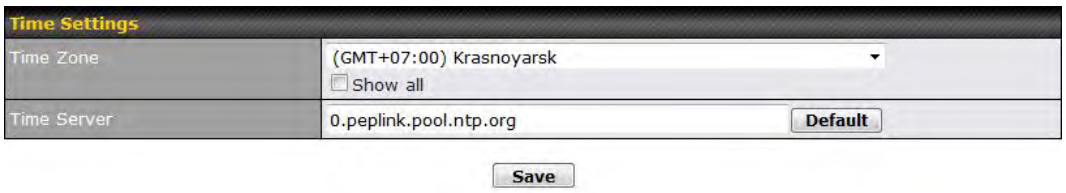
The firmware upgrade process may not necessarily preserve the previous configuration, and the behavior varies on a case-by-case basis. Consult the release notes for the particular firmware version before installing. Do not disconnect the power during firmware upgrade process. Do not attempt to upload a non-firmware file or a firmware file that is not supported by Peplink. Upgrading the Pepwave router with an invalid firmware file will damage the unit and may void the warranty.

 Copyright @ 2017 Pepwave

Important Note
If the firmware is rolled back from 5.x to 4.x, the configurations will be lost.

18.3 Time

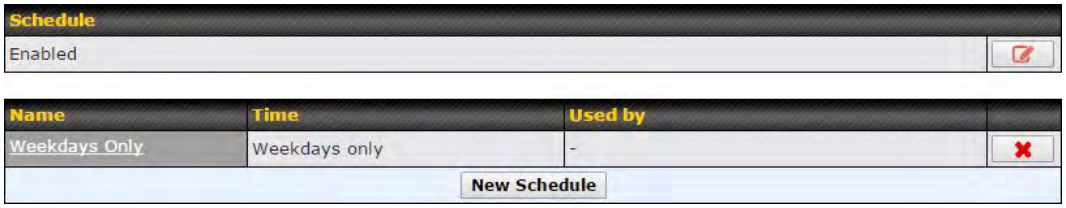
Time Settings enables the system clock of the Pepwave router to be synchronized with a specified time server. Time settings are located at **System>Time**.



Time Settings	
Time Zone	This specifies the time zone (along with the corresponding Daylight Savings Time scheme). The **Time Zone** value affects the time stamps in the Pepwave router s event log and e-mail notifications. Check **Show all** to show all time zone options.
Time Server	This setting specifies the NTP network time server to be utilized by the Pepwave router.

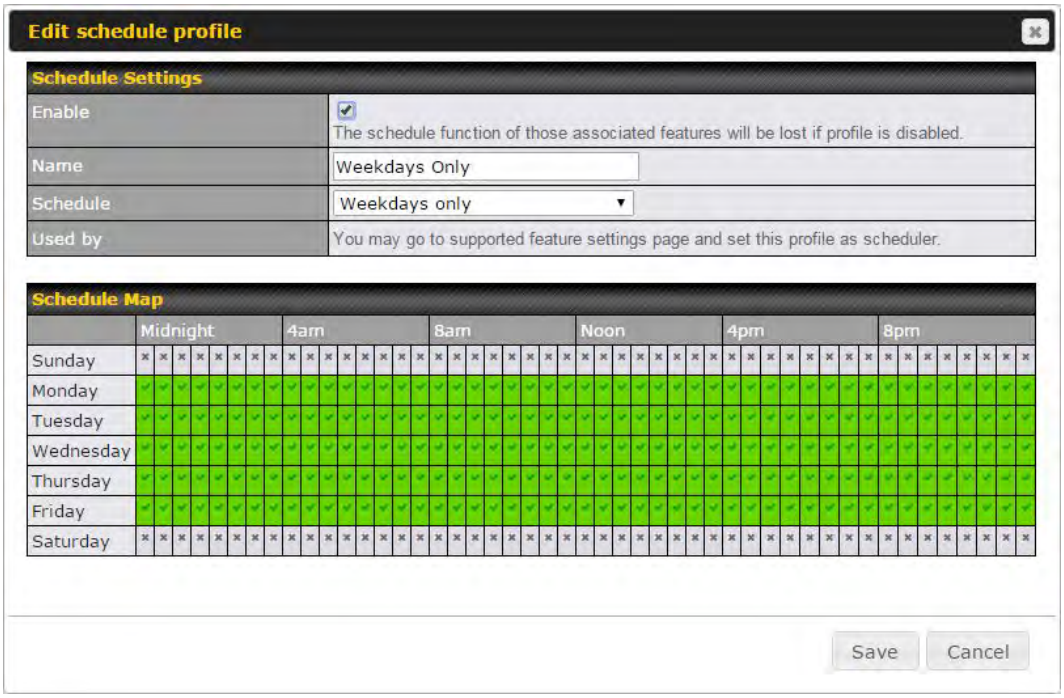
18.4 Schedule

Enable and disable different functions (such as WAN connections, outbound policy, and firewalls at different times, based on a user-scheduled configuration profile. The settings for this are located at **System > Schedule**



Enable scheduling, and then click on your schedule name or on the **New Schedule** button to begin.

 Copyright @ 2017 Pepwave

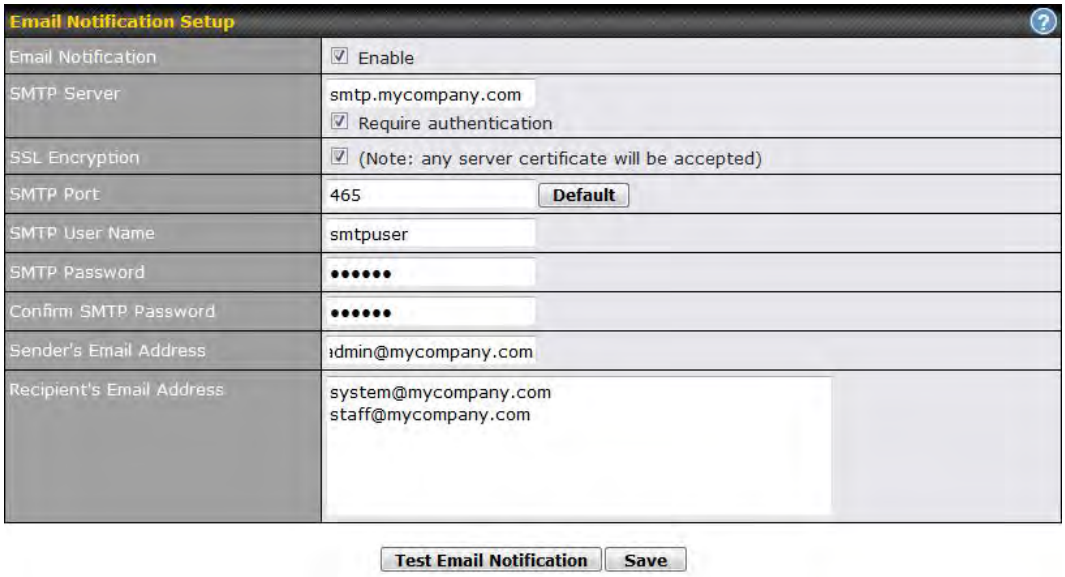


Edit Schedule Profile	
Enabling	Click this checkbox to enable this schedule profile. Note that if this is disabled, then any associated features will also have their scheduling disabled.
Name	Enter your desired name for this particular schedule profile.
Schedule	Click the drop-down menu to choose pre-defined schedules as your starting point. Please note that upon selection, previous changes on the schedule map will be deleted.
Schedule Map	Click on the desired times to enable features at that time period. You can hold your mouse for faster entry.

18.5 Email Notification

Email notification functionality provides a system administrator with up-to-date information on network status. The settings for configuring email notifications are found at **System>Email Notification**.

 Copyright @ 2017 Pepwave



Email Notification Settings	
Email Notification	This setting specifies whether or not to enable email notification. If **Enable** is checked, the Pepwave router will send email messages to system administrators when the WAN status changes or when new firmware is available. If **Enable** is not checked, email notification is disabled and the Pepwave router will not send email messages.
SMTP Server	This setting specifies the SMTP server to be used for sending email. If the server requires authentication, check **Require authentication**.
SSL Encryption	Check the box to enable SMTPS. When the box is checked, **SMTP Port** will be changed to **465** automatically.
SMTP Port	This field is for specifying the SMTP port number. By default, this is set to **25**; when **SSL Encryption** is checked, the default port number will be set to **465**. You may customize the port number by editing this field. Click **Default** to restore the number to its default setting.
SMTP User Name / Password	This setting specifies the SMTP username and password while sending email. These options are shown only if **Require authentication** is checked in the **SMTP Server** setting.
Confirm SMTP Password	This field allows you to verify and confirm the new administrator password.

 Copyright @ 2017 Pepwave

Sender's Email Address	This setting specifies the email address the Pepwave router will use to send reports.
Recipient's Email Address	This setting specifies the email address(es) to which the Pepwave router will send email notifications. For multiple recipients, separate each email addresses using the enter key.

After you have finished setting up email notifications, you can click the **Test Email Notification** button to test the settings before saving. After **Test Email Notification** is clicked, you will see this screen to confirm the settings:



Click **Send Test Notification** to confirm. In a few seconds, you will see a message with detailed test results.



18.6 Event Log

Event log functionality enables event logging at a specified remote syslog server. The settings for configuring the remote system log can be found at **System>Event Log**.

 Copyright @ 2017 Pepwave

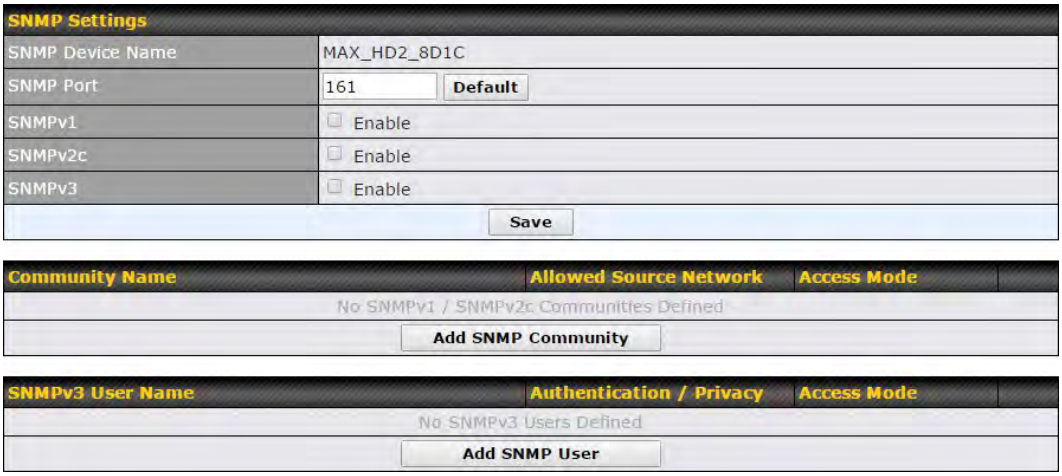


Event Log Settings	
Remote Syslog	This setting specifies whether or not to log events at the specified remote syslog server.
Remote Syslog Host	This setting specifies the IP address or hostname of the remote syslog server.
Push Events	The Pepwave router can also send push notifications to mobile devices that have our Mobile Router Utility installed. Check the box to activate this feature. For more information on the Router Utility, go to: www.peplink.com/products/router-utility

18.7 SNMP

SNMP or simple network management protocol is an open standard that can be used to collect information about the Pepwave router. SNMP configuration is located at **System>SNMP**.

 Copyright @ 2017 Pepwave



SNMP Settings	
SNMP Device Name	This field shows the router name defined at **System>Admin Security**.
SNMP Port	This option specifies the port which SNMP will use. The default port is **161**.
SNMPv1	This option allows you to enable SNMP version 1.
SNMPv2	This option allows you to enable SNMP version 2.
SNMPv3	This option allows you to enable SNMP version 3.

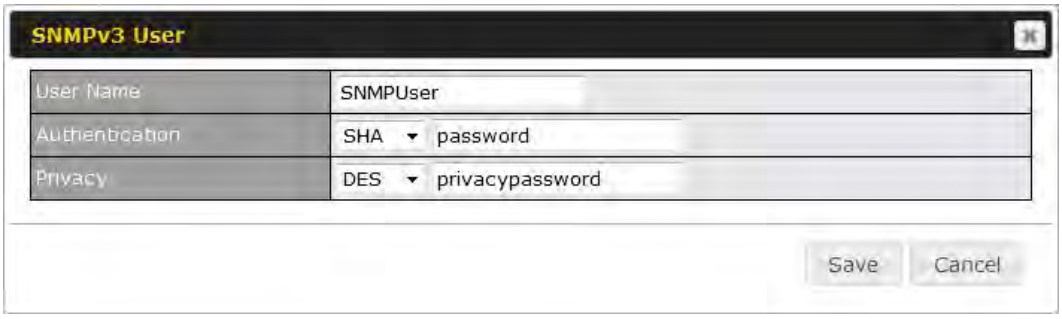
To add a community for either SNMPv1 or SNMPv2, click the **Add SNMP Community** button in the **Community Name** table, upon which the following screen is displayed:



 Copyright @ 2017 Pepwave

SNMP Community Settings	
Community Name	This setting specifies the SNMP community name.
Allowed Source Subnet Address	This setting specifies a subnet from which access to the SNMP server is allowed. Enter subnet address here (e.g., *192.168.1.0*) and select the appropriate subnet mask.

To define a username for SNMPv3, click **Add SNMP User** in the **SNMPv3 User Name** table, upon which the following screen is displayed:



SNMP Community Settings	
Community Name	This setting specifies the SNMP community name.
Allowed Source Subnet Address	This setting specifies a subnet from which access to the SNMP server is allowed. Enter subnet address here (e.g., *192.168.1.0*) and select the appropriate subnet mask.

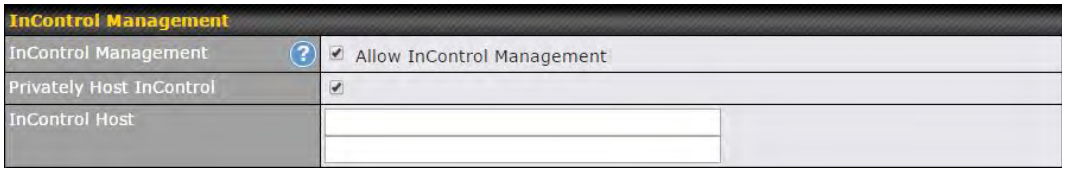
To define a username for SNMPv3, click **Add SNMP User** in the **SNMPv3 User Name** table, upon which the following screen is displayed:

SNMPv3 User Settings	
User Name	This setting specifies a user name to be used in SNMPv3.

 Copyright @ 2017 Pepwave

Authentication Protocol	This setting specifies via a drop-down menu one of the following valid authentication protocols: NONE MD5 SHA When MD5 or SHA is selected, an entry field will appear for the password.
Privacy Protocol	This setting specifies via a drop-down menu one of the following valid privacy protocols: NONE DES When DES is selected, an entry field will appear for the password.

18.8 InControl



InControl is a cloud-based service which allows you to manage all of your Peplink and Pepwave devices with one unified system. With it, you can generate reports, gather statistics, and configure your devices automatically. All of this is now possible with InControl.

When this checkbox is checked, the device's status information will be sent to the Peplink InControl system. This device's usage data and configuration will be sent to the system if you enable the features in the system.

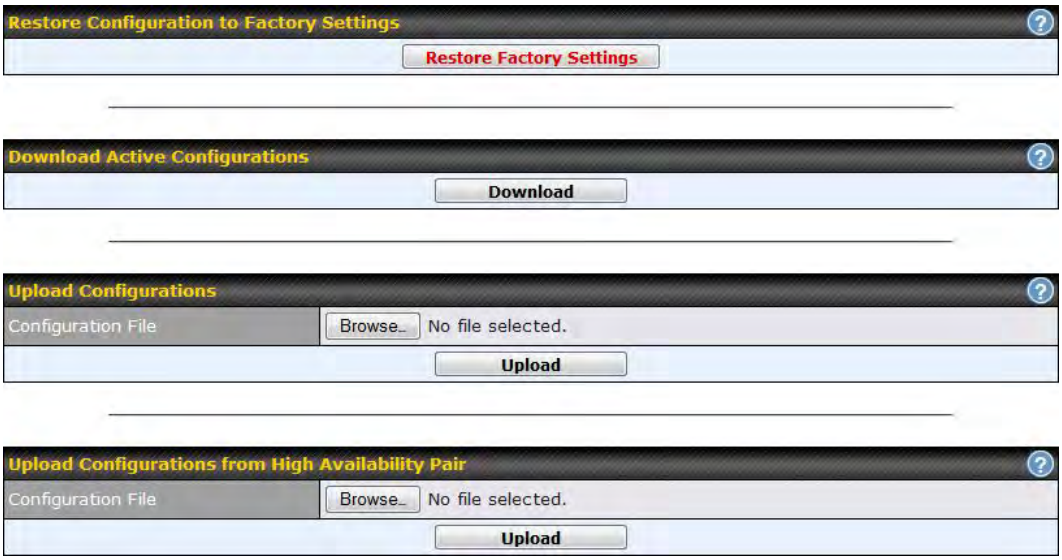
Alternately, you could also privately host InControl. Simply check the box beside the “Privately Host InControl” open, and enter the IP Address of your InControl Host.

You can sign up for an InControl account at https://incontrol2.peplink.com/. You can register your devices under the account, monitor their status, see their usage reports, and receive offline notifications.

18.9 Configuration

Backing up Pepwave router settings immediately after successful completion of initial setup is strongly recommended. The functionality to download and upload Pepwave router settings is found at **System>Configuration**. Note that available options vary by model.

 Copyright @ 2017 Pepwave



Configuration	
Restore Configuration to Factory Settings	The **Restore Factory Settings** button is to reset the configuration to factory default settings. After clicking the button, you will need to click the **Apply Changes** button on the top right corner to make the settings effective.
Download Active Configurations	Click **Download** to backup the current active settings.
Upload Configurations	To restore or change settings based on a configuration file, click **Choose File** to locate the configuration file on the local computer, and then click **Upload**. The new settings can then be applied by clicking the **Apply Changes** button on the page header, or you can cancel the procedure by pressing **discard** on the main page of the web admin interface.
Upload Configurations from High Availability Pair	In a high availability (HA) configuration, a Pepwave router can quickly load the configuration of its HA counterpart. To do so, click the **Upload** button. After loading the settings, configure the LAN IP address of the Pepwve router so that it is different from the HA counterpart.

18.10 Feature Add-ons

Some Pepwave routers have features that can be activated upon purchase. Once the purchase is complete, you will receive an activation key. Enter the key in the **Activation Key** field, click **Activate**,

 Copyright @ 2017 Pepwave

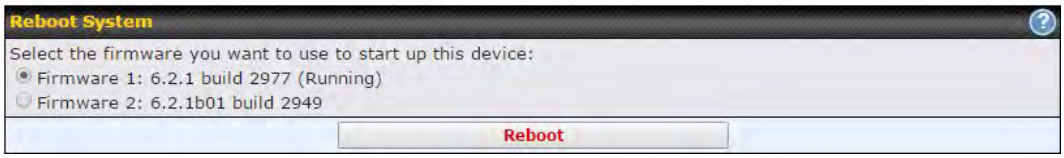
and then click **Apply Changes**.



18.11 Reboot

This page provides a reboot button for restarting the system. For maximum reliability, the Pepwave router can equip with two copies of firmware. Each copy can be a different version. You can select the firmware version you would like to reboot the device with. The firmware marked with **(Running)** is the current system boot up firmware.

Please note that a firmware upgrade will always replace the inactive firmware partition.

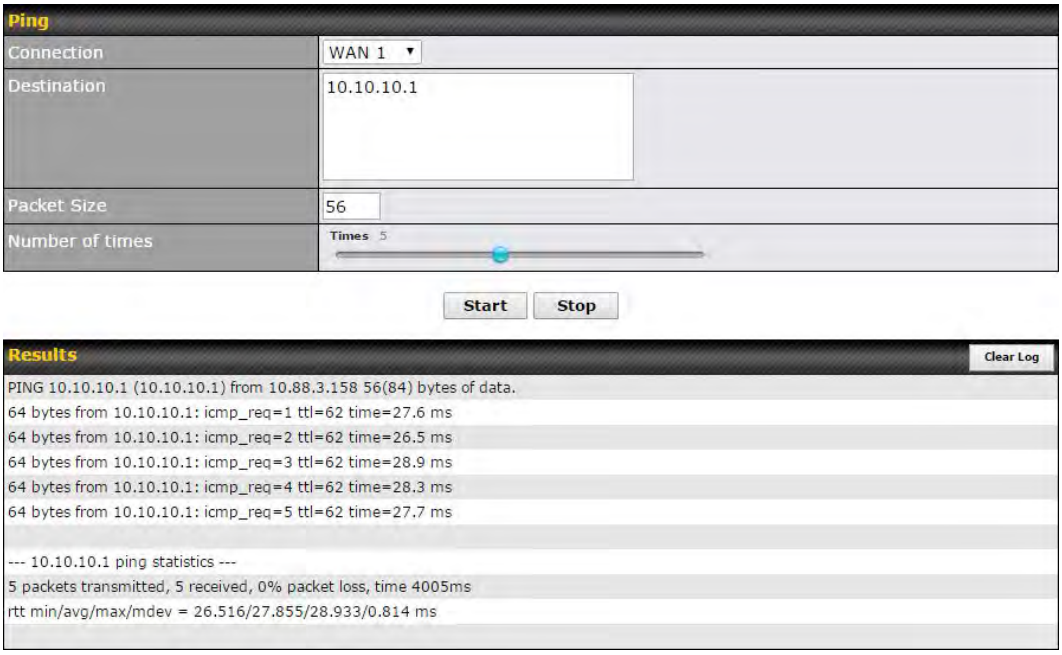


19 Tools

19.1 Ping

The ping test tool sends pings through a specified Ethernet interface or a SpeedFusion™ VPN connection. You can specify the number of pings in the field **Number of times**, to a maximum number of 10 times. **Packet Size** can be set to a maximum of 1472 bytes. The ping utility is located at **System>Tools>Ping,** illustrated below:

 Copyright @ 2017 Pepwave



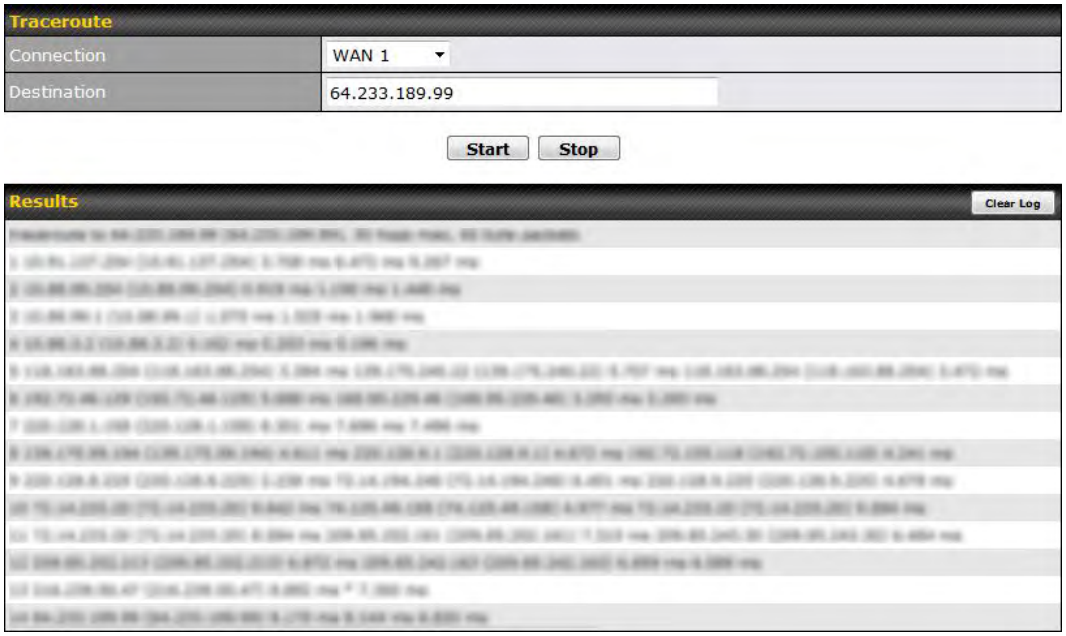
Tip

A system administrator can use the ping utility to manually check the connectivity of a particular LAN/WAN connection.

19.2 Traceroute Test

The traceroute test tool traces the routing path to the destination through a particular Ethernet interface. The traceroute test utility is located at **System>Tools>Traceroute**.

 Copyright @ 2017 Pepwave

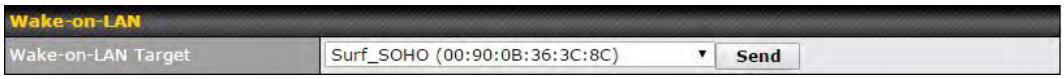


Tip

A system administrator can use the traceroute utility to analyze the connection path of a LAN/WAN connection.

19.3 Wake-on-LAN

Peplink routers can send special "magic packets" to any client specified from the Web UI. To access this feature, navigate to **System > Tools > Wake-on-LAN**



Select a client from the drop-down list and click **Send** to send a "magic packet"

20 Status

20.1 Device

System information is located at **Status>Device**.

 Copyright @ 2017 Pepwave

System Information	
Router Name	SURF-SOHO-F385
Model	Pepwave Surf SOHO MK3
Product Code	SUS-SOHO
Hardware Revision	1
Serial Number	2933-5321-F385
Firmware	7.0.0 build 1133
PepVPN Version	6.0.0
Modem Support Version	1020 (Modem Support List)
Host Name	surf-soho-f385
Uptime	14 days 20 hours
System Time	Wed Jan 25 03:17:55 UTC 2017
Diagnostic Report	Download
Remote Assistance	Turn on

System Information	
Router Name	This is the name specified in the **Router Name** field located at **System>Admin Security**.
Model	This shows the model name and number of this device.
Product Code	If your model uses a product code, it will appear here.
Hardware Revision	This shows the hardware version of this device.
Serial Number	This shows the serial number of this device.
Firmware	This shows the firmware version this device is currently running.
PepVPN Version	This shows the current PepVPN version.
Modem Support Version	This shows the modem support version. For a list of supported modems, click **Modem Support List**.
Hostname	The host name assigned to the Pepwave router appears here.

 Copyright @ 2017 Pepwave

Uptime	This shows the length of time since the device has been rebooted.
System Time	This shows the current system time.
Diagnostic Report	The **Download** link is for exporting a diagnostic report file required for system investigation.
Remote Assistance	Click **Turn on** to enable remote assistance.

Interface	MAC Address
LAN	00:1A:DD:BD:54:40
WAN 1	00:1A:DD:BD:54:41
WAN 2	00:1A:DD:BD:54:42

The second table shows the MAC address of each LAN/WAN interface connected. To view your device's End User License Agreement (EULA), click  .

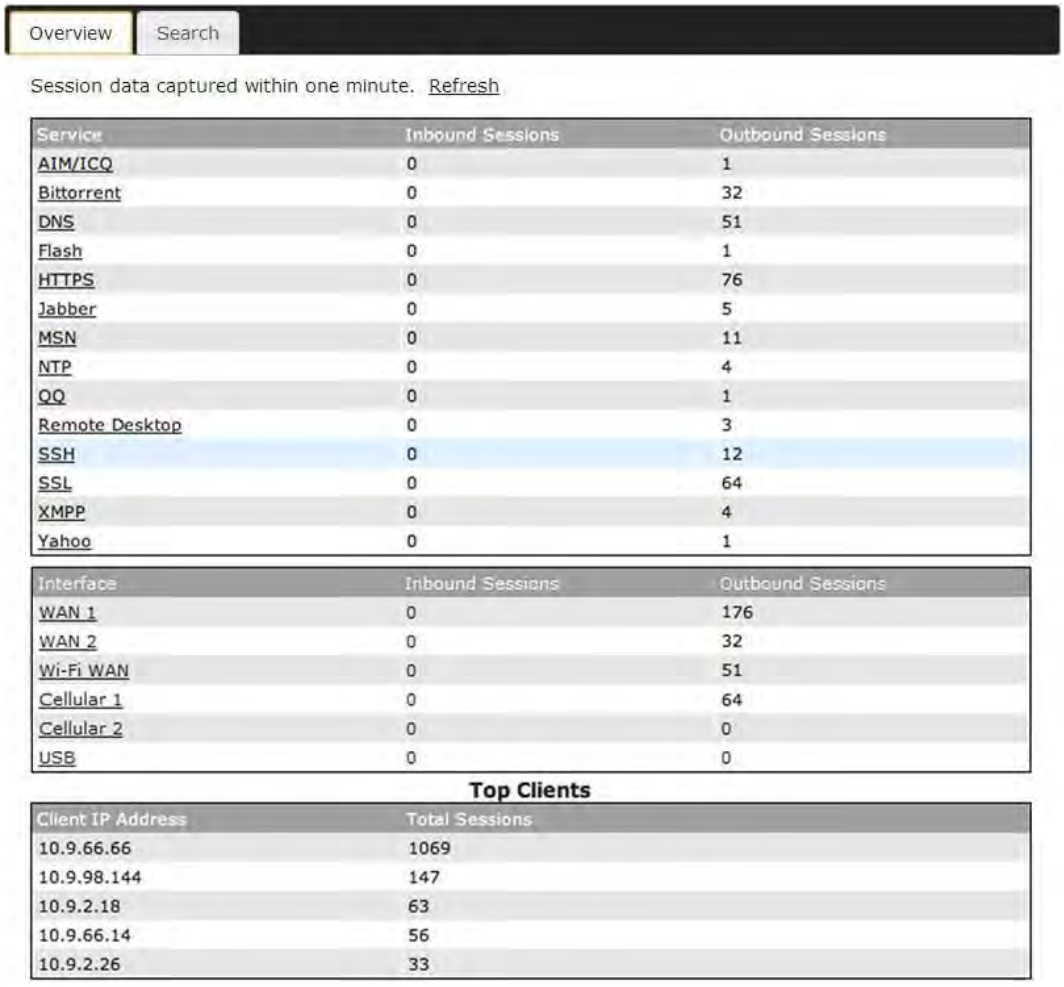
Important Note

If you encounter issues and would like to contact the Pepwave Support Team (http://www.pepwave.com/contact/), please download the diagnostic report file and attach it along with a description of your issue.
In Firmware 5.1 or before, the diagnostic report file can be obtained at **System>Reboot.**

20.2 Active Sessions

Information on active sessions can be found at **Status>Active Sessions>Overview.**

 Copyright @ 2017 Pepwave



Overview | Search

Session data captured within one minute. Refresh

Service	Inbound Sessions	Outbound Sessions
AIM/ICQ	0	1
Bittorrent	0	32
DNS	0	51
Flash	0	1
HTTPS	0	76
Jabber	0	5
MSN	0	11
NTP	0	4
QQ	0	1
Remote Desktop	0	3
SSH	0	12
SSL	0	64
XMPP	0	4
Yahoo	0	1

Interface	Inbound Sessions	Outbound Sessions
WAN 1	0	176
WAN 2	0	32
Wi-Fi WAN	0	51
Cellular 1	0	64
Cellular 2	0	0
USB	0	0

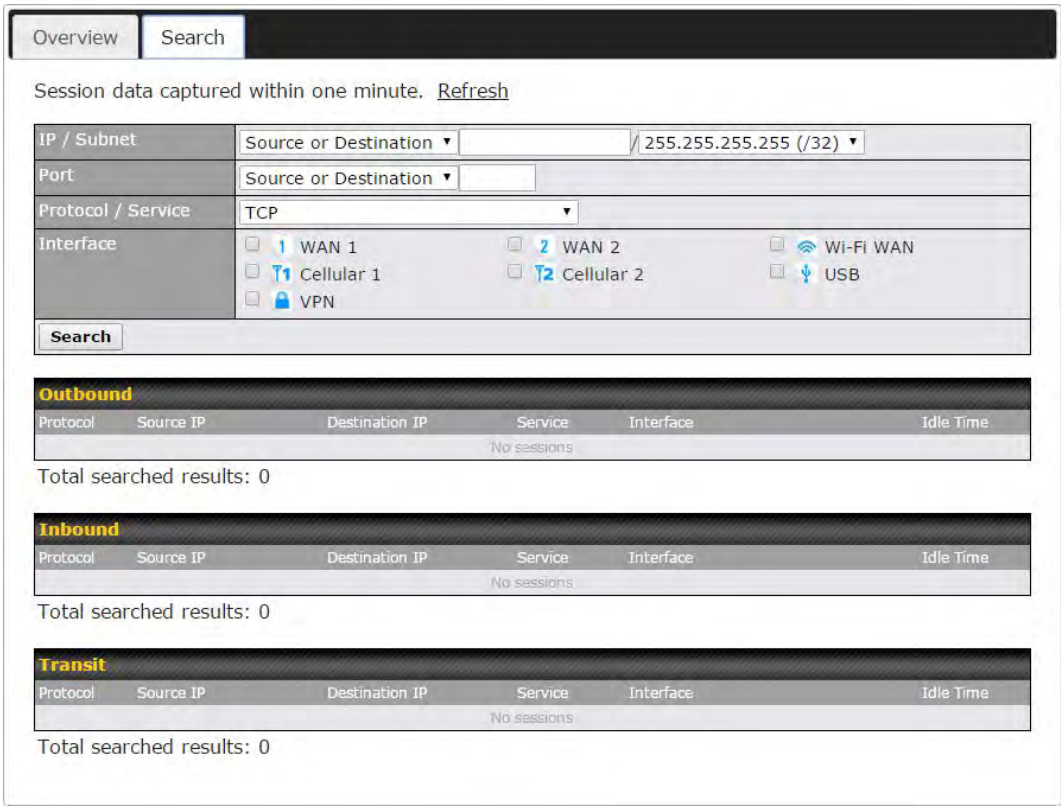
Top Clients

Client IP Address	Total Sessions
10.9.66.66	1069
10.9.98.144	147
10.9.2.18	63
10.9.66.14	56
10.9.2.26	33

This screen displays the number of sessions initiated by each application. Click on each service listing for additional information. This screen also indicates the number of sessions initiated by each WAN port. In addition, you can see which clients are initiating the most sessions.

You can also perform a filtered search for specific sessions. You can filter by subnet, port, protocol, and interface. To perform a search, navigate to **Status>Active Sessions>Search**.

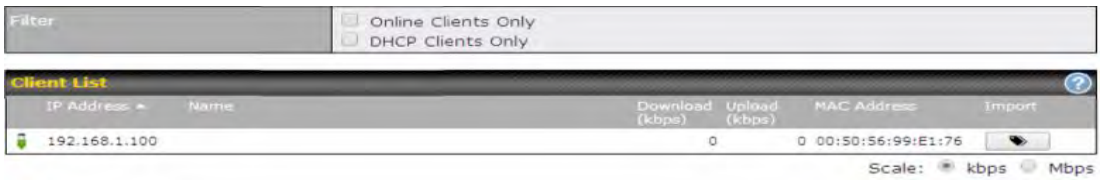
 Copyright @ 2017 Pepwave



This **Active Sessions** section displays the active inbound/outbound sessions of each WAN connection on the Pepwave router. A filter is available to sort active session information. Enter a keyword in the field or check one of the WAN connection boxes for filtering.

20.3 Client List

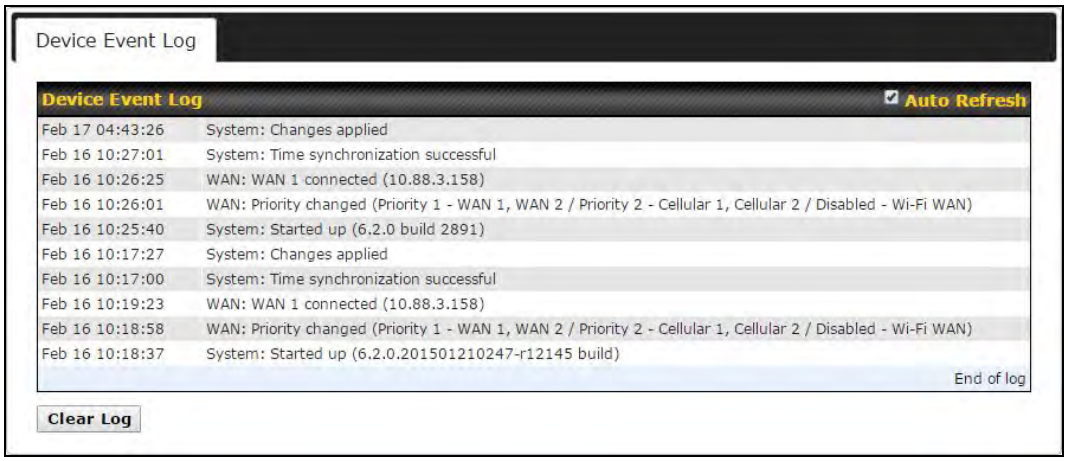
The client list table is located at **Status>Client List**. It lists DHCP and online client IP addresses**,** names (retrieved from the DHCP reservation table or defined by users), current download and upload rate, and MAC address. Clients can be imported into the DHCP reservation table by clicking the button on the right. You can update the record after import by going to **Network>LAN**.



 Copyright @ 2017 Pepwave

20.4 Event Log

Event log information is located at **Status>Event Log**



The log section displays a list of events that has taken place on the Pepwave router. Check **Auto Refresh** to refresh log entries automatically. Click the **Clear Log** button to clear the log.

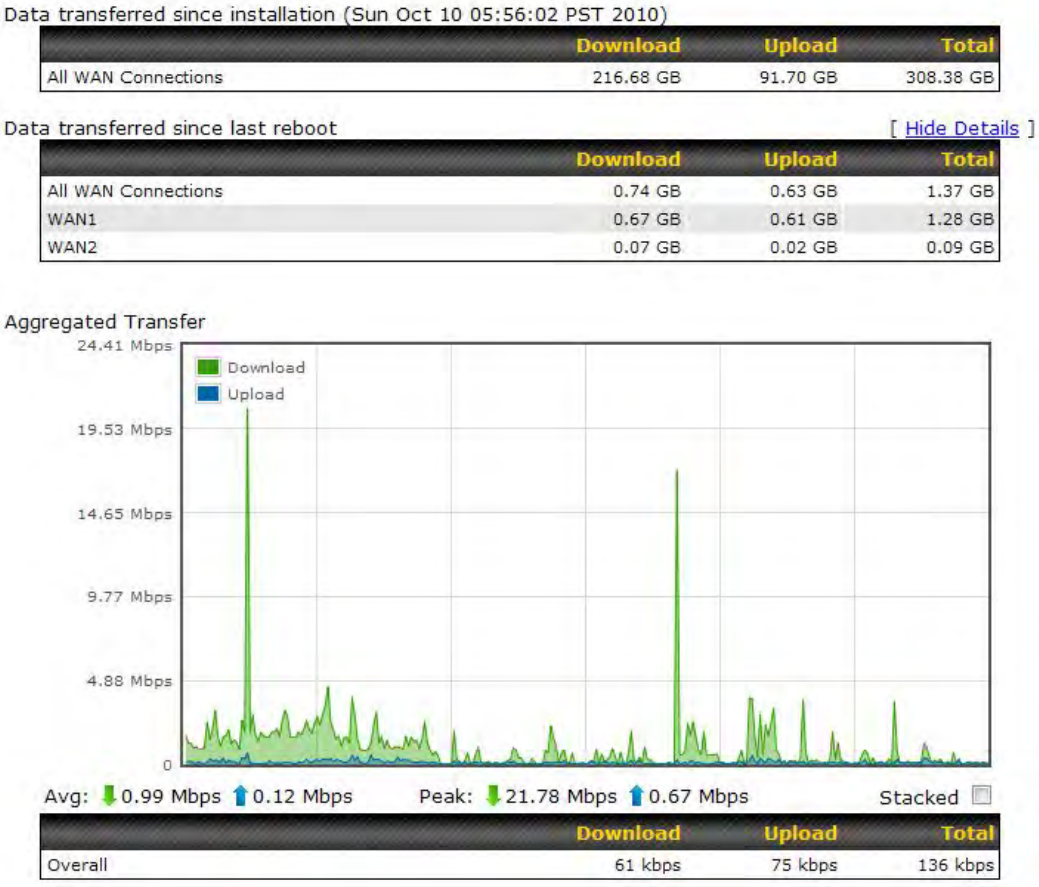
20.5 Bandwidth

This section shows bandwidth usage statistics and is located at **Status>Bandwidth**. Bandwidth usage at the LAN while the device is switched off (e.g., LAN bypass) is neither recorded nor shown.

20.5.1 Real Time

The **Data transferred since installation** table indicates how much network traffic has been processed by the device since the first bootup. The **Data transferred since last reboot** table indicates how much network traffic has been processed by the device since the last boot up.

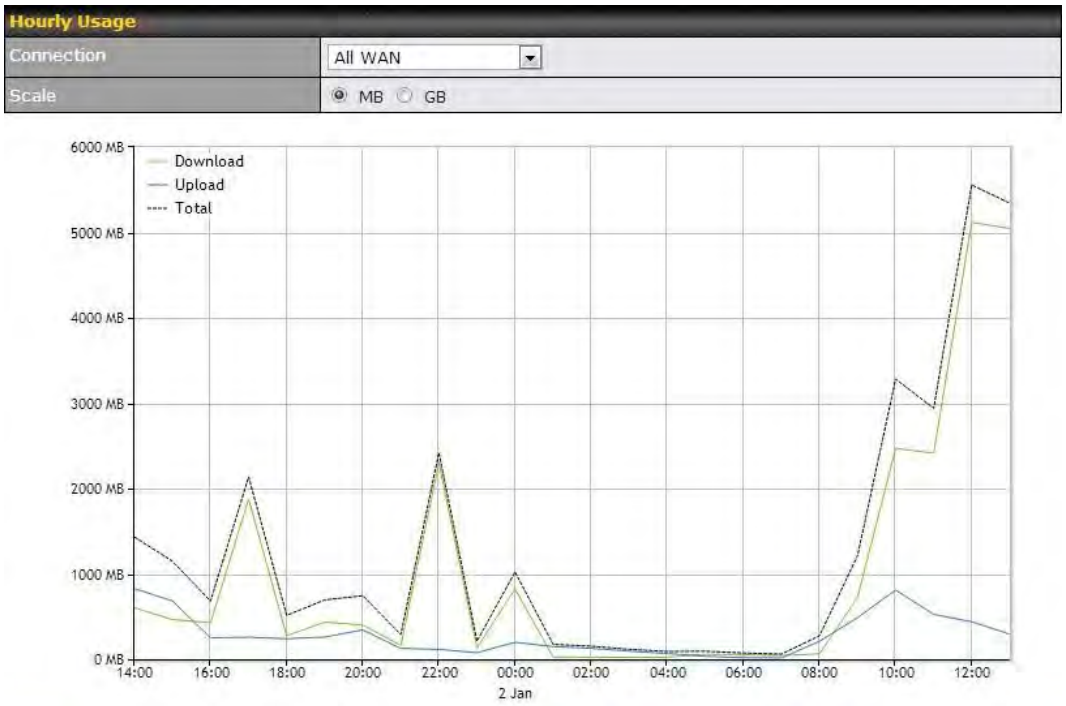
 Copyright @ 2017 Pepwave



20.5.2 Hourly

This page shows the hourly bandwidth usage for all WAN connections, with the option of viewing each individual connection. Select the desired connection to check from the drop-down menu.

 Copyright @ 2017 Pepwave



Date	Download	Upload	Total
13:00	5 047 MB	295 MB	5 342 MB
12:00	5 117 MB	439 MB	5 556 MB
11:00	2 414 MB	526 MB	2 940 MB
10:00	2 470 MB	812 MB	3 282 MB
09:00	725 MB	488 MB	1 213 MB
08:00	64 MB	211 MB	275 MB

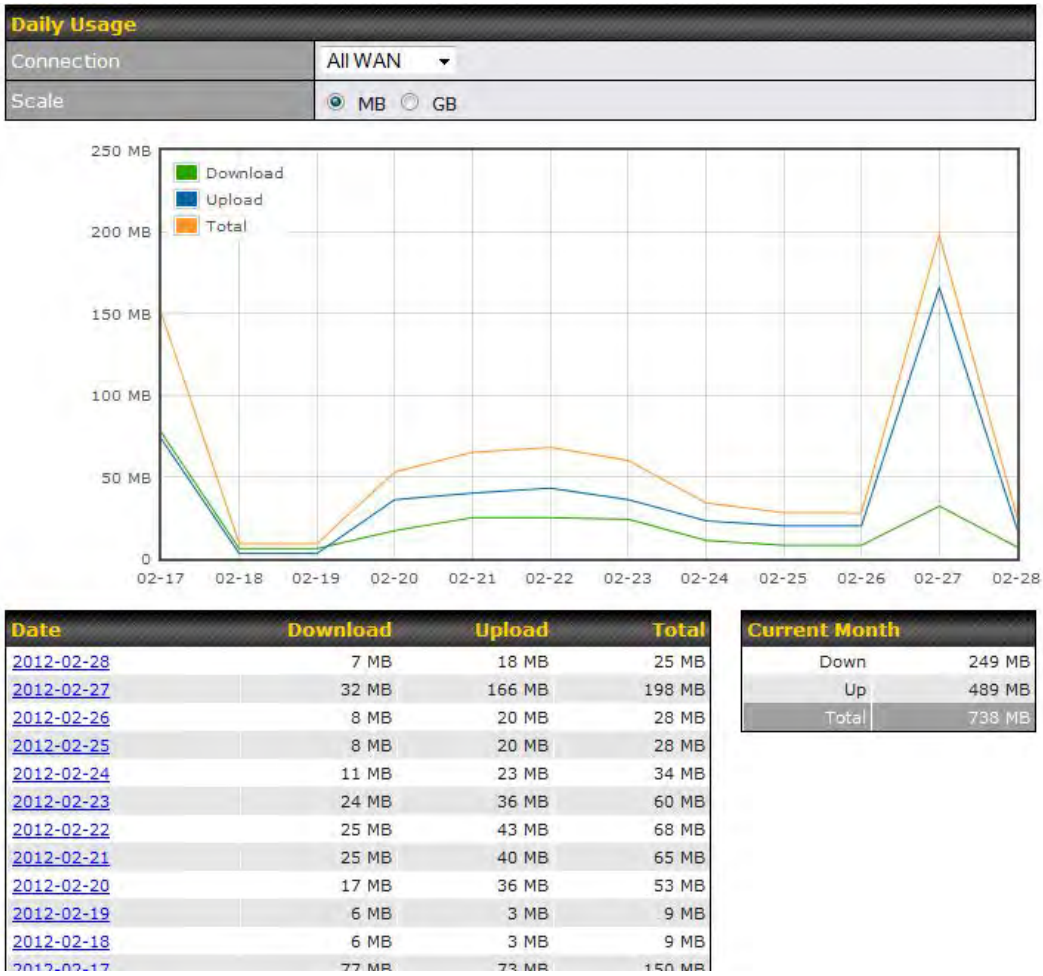
20.5.3 Daily

This page shows the daily bandwidth usage for all WAN connections, with the option of viewing each individual connection.

Select the connection to check from the drop-down menu. If you have enabled the **Bandwidth Monitoring** feature**,** the **Current Billing Cycle** table for that WAN connection will be displayed.

Click on a date to view the client bandwidth usage of that specific date. This feature is not available if you have selected to view the bandwidth usage of only a particular WAN connection. The scale of the graph can be set to display megabytes (**MB**) or gigabytes (**GB**).

 Copyright @ 2017 Pepwave



Date	Download	Upload	Total
2012-02-28	7 MB	18 MB	25 MB
2012-02-27	32 MB	166 MB	198 MB
2012-02-26	8 MB	20 MB	28 MB
2012-02-25	8 MB	20 MB	28 MB
2012-02-24	11 MB	23 MB	34 MB
2012-02-23	24 MB	36 MB	60 MB
2012-02-22	25 MB	43 MB	68 MB
2012-02-21	25 MB	40 MB	65 MB
2012-02-20	17 MB	36 MB	53 MB
2012-02-19	6 MB	3 MB	9 MB
2012-02-18	6 MB	3 MB	9 MB

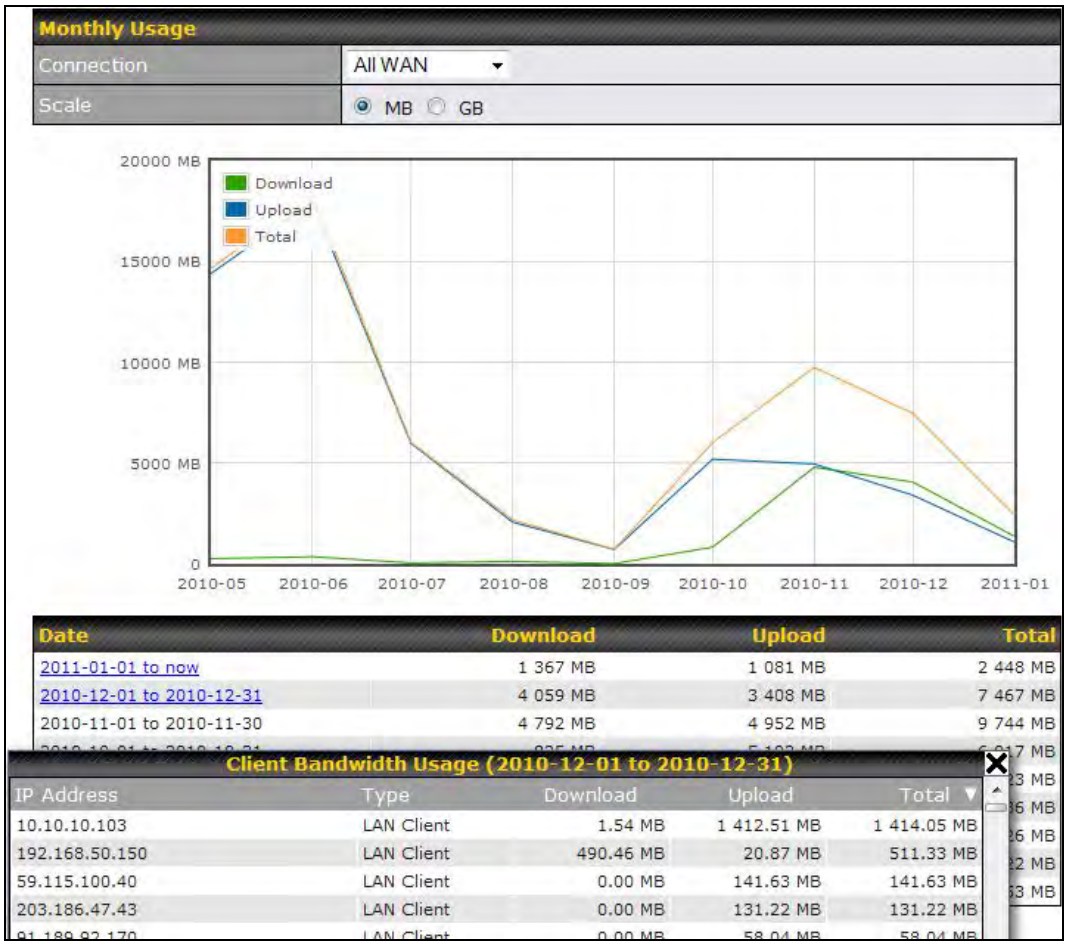
Current Month	
Down	249 MB
Up	489 MB
Total	738 MB

20.5.4 Monthly

This page shows the monthly bandwidth usage for each WAN connection. If you have enabled the **Bandwidth Monitoring** feature, you can check the usage of each particular connection and view the information by **Billing Cycle** or by **Calendar Month**.

Click the first two rows to view the client bandwidth usage in the last two months. This feature is not available if you have chosen to view the bandwidth of an individual WAN connection. The scale of the graph can be set to display megabytes (**MB**) or gigabytes (**GB**).

 Copyright @ 2017 Pepwave



 Copyright @ 2017 Pepwave

Appendix A: Restoration of Factory Defaults

To restore the factory default settings on a Pepwave router, follow the steps below:

1. Locate the reset button on the front or back panel of the Pepwave router.
2. With a paper clip, press the reset button and hold it for at least 10 seconds, until the unit reboots itself.
3. After the Pepwave router finishes rebooting, the factory default settings will be restored.

Important Note
All previous configurations and bandwidth usage data will be lost after restoring factory default settings. Regular backup of configuration settings is strongly recommended.

Appendix B: Declaration

- **The device supports time division technology**
  Federal Communication Commission Interference Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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

- Reorient or relocate the receiving antenna.

- Increase the separation between the equipment and receiver.

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

 Copyright @ 2017 Pepwave

- Consult the dealer or an experienced radio/TV technician for help.FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination.

- **CE Statement for Pepwave Routers**

Europe – EU Declaration of Conformity
This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

❏ EN 60950-1: 2006 + A11 : 2009+A1 : 2010+ A12: 2011

Safety of Information Technology Equipment

❏ EN50385 : 2002 / Article 3(1)(a)

Product standard to demonstrate the compliance of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110MHz - 40 GHz) - General public

❏ EN 300 328 V1.7.1: 2006

Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive

❏ EN 301 908-1 V5.2.1: 2011

Electromagnetic compatibility and Radio spectrum Matters (ERM); Base Stations (BS), Repeaters and User Equipment (UE) for IMT-2000 Third-Generation cellular networks; Part 1: Harmonized EN for IMT-2000, introduction and common requirements, covering essential requirements of article 3.2 of the R&TTE Directive

 Copyright @ 2017 Pepwave

- EN 301 511 V9.0.2: 2003

Global System for Mobile communications (GSM); Harmonized standard for mobile stations in the GSM 900 and DCS 1800 bands covering essential requirements under article 3.2 of the R&TTE directive (1999/5/EC)

- EN 301 489-1 V1.9.2: 2008

Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements

- EN 301 489-7 V1.3.1: 2005

ElectroMagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment ad services; Part 7: Specific conditions for mobile and portable radio and ancillary equipment of digital cellular radio telecommunications systems (GSM and DCS)

- EN 301 489-17 V2.2.1: 2012

Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment

- EN 301 489-24 V1.5.1: 2010

Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 24: Specific conditions for IMT-2000 CDMA Direct Spread (UTRA) for Mobile and portable (UE) radio and ancillary equipment

CE 0081

cs esky Czech	*[Jméno výrobce]* t mto prohla u e, e tento *[typ zařízení]* e ve shod se z kladn mi po adavky a dal mi p slu n mi ustanoven mi sm rnice 1999/5/ES.
da Dansk Danish	Undertegnede *[fabrikantens navn]* erkl rer herved, at f lgende udstyr *[udstyrets typebetegnelse]* overholder de v sentlige krav og vrige

 Copyright @ 2017 Pepwave

	relevante krav i direktiv 1999/5/EF.
de Deutsch German	Hiermit erkl rt *[Name des Herstellers]*, dass sich das Ger t *[Gerätetyp]* in bereinstimmung mit den grundlegenden Anforderungen und den brigen einschl gigen Bestimmungen der Richtlinie 1999/5/EG befindet.
et Eesti Estonian	K esolevaga kinnitab *[tootja nimi = name of manufacturer]* seadme *[seadme tüüp = type of equipment]* vastavust direktiivi 1999/5/E p hin uetele a nimetatud direktiivist tulenevatele teistele as akohastele s tetele.
en English	Hereby, *[name of manufacturer]*, declares that this *[type of equipment]* is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
es Espa ol Spanish	Por medio de la presente *[nombre del fabricante]* declara que el *[clase de equipo]* cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
el Greek	*[name of manufacturer]* *[type of equipment]* 1999/5/ .
fr Fran ais French	Par la pr sente *[nom du fabricant]* d clare que l'appareil *[type d'appareil]* est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
it Italiano Italian	Con la presente *[nome del costruttore]* dichiara che questo *[tipo di apparecchio]* conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
lv Latviski Latvian	Ar o *[name of manufacturer / izgatavotāja nosaukums]* deklar , ka *[type of equipment / iekārtas tips]* atbilst Direkt vas 1999/5/EK b tiska m pras b m un citiem ar to saist ta iem noteikumiem.
lt Lietuvi Lithuanian	iuo *[manufacturer name]* deklaruo a, kad is *[equipment type]* atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
nl	Hierbi verklaart *[naam van de fabrikant]* dat het toestel *[type van toestel]* in

 Copyright @ 2017 Pepwave

Nederlands Dutch	overeenstemming is met de essenti le eisen en de andere relevante bepalingen van richtli n 1999/5/EG.
mt Malti Maltese	Hawnhekk, *[isem tal-manifattur]*, iddik ara li dan *[il-mudel tal-prodott]* ikkonforma mal- ti i iet essenz ali u ma provvedimenti o ra n relevanti li hemm fid-Dirrettiva 1999/5/EC.
hu Magyar Hungarian	Alul rott, *[gyártó neve]* nyilatkozom, hogy a *[... típus]*megfelel a vonatkoz alapvet k vetelm nyeknek s az 1999/5/EC ir nyelv egy b el r sainak.
pl Polski Polish	Ninie szym *[nazwa producenta]* o wiadcza, e *[nazwa wyrobu]* est zgodny z zasadniczymi wymogami oraz pozosta ymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
pt Portugu s Portuguese	*[Nome do fabricante]* declara que este *[tipo de equipamento]* est conforme com os requisitos essenciais e outras disposi es da Directiva 1999/5/CE.
sl Slovensko Slovenian	*[Ime proizvajalca]* iz avl a, da e ta *[tip opreme]* v skladu z bistvenimi zahtevami in ostalimi relevantnimi dolo ili direktive 1999/5/ES.
sk Slovensky Slovak	*[Meno výrobcu]* t mto vyhlasu e, e *[typ zariadenia]*sp a z kladn po iadavky a v etky pr slu n ustanovenia Smernice 1999/5/ES.
fi Suomi Finnish	*[Valmistaja = manufacturer]* vakuuttaa t ten ett *[type of equipment = laitteen tyyppimerkintä]* tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten a sit koskevien direktiivin muiden ehto en mukainen.
sv Svenska Swedish	H rmed intygar *[företag]* att denna *[utrustningstyp]* st r I verensst mmelse med de v sentliga egenskapskrav och vriga relevanta best mmelser som framg r av direktiv 1999/5/EG.

 Copyright @ 2017 Pepwave

ALIBI Witness 3.0 Smartphone App for Apple iOS Mobile Devices User Guide

ALIBI Witness 3.0 is a free application (app) for Apple iOS (requires iOS 7.0 or later). This app is compatible with iPhone, iPad, and iPod touch. It is also available for Android™ platforms. This app is used to access ALIBI NVRs, HVRs, DVRs and IP video surveillance devices that are accessible through the Internet. This app enables you to do the following:

- Remotely monitor live and recorded video on your mobile device
- View up to 16 live video streams simultaneously
- Supports up to 32 devices
- P2P Cloud account for remote device connection
- Take snapshots and record live video directly from your smartphone or tablet
- Add, delete, or modify connected devices from your mobile device
- Manage PTZ camera controls using your touchscreen
- Swipe to pan/tilt and pinch to zoom PTZ cameras
- Digitally zoom in during live video or remote playback modes
- Mix and match live views to access multiple Alibi recorders and IP cameras
- Push notifications alert you in real time to selected events
- Supports multiple languages

Alibi Witness 2 v3 includes the following new features and improvements:

- Optimized Live View and Playback by merging P2P and Local device tabs
- Support for multi-channel live view options listed on the home page
- Includes video sharing and management through Guarding Vision accounts
- Includes support for channel tagging to mark important channels
- Includes Help feature
- Supports 19 languages
- PTZ functions to include preset configuration, speed adjustments, and PTZ operations in full screen view
- Playback supports up to 4 simultaneous channels

This User Guide covers the functionality, installation and usage of ALIBI Witness 3.0.

GUARDING VISION

Guarding Vision platform access allows you to create a peer-to-peer connection with your surveillance equipment. This connection can then be accessed through an Internet connection. Devices you access through this platform must have an identifying QR code and be added through the Alibi Witness 3.0 app. Devices can be added to multiple Guarding Vision accounts, but can be accessed through only one account at a time.

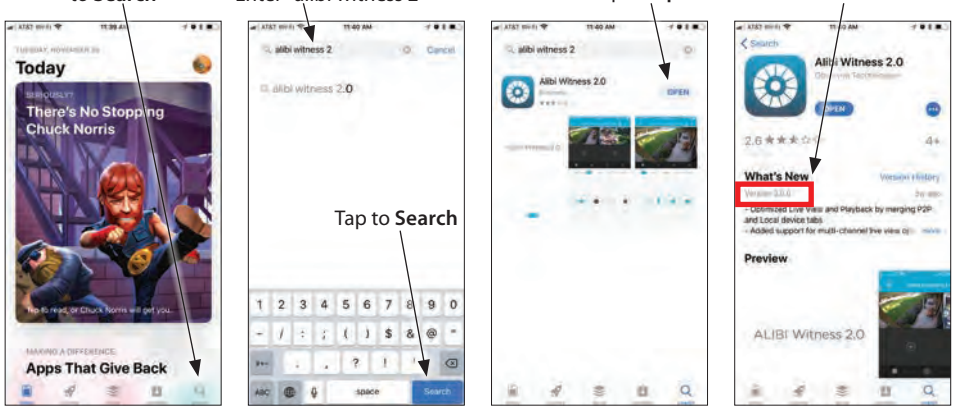
This document includes the following sections:

INSTALLATION	1
ADD - MANUAL ADDING	2
ADD - ONLINE DEVICE	2
ADD - SCAN QR CODE	3
CREATE GUARDING VISION ACCOUNT	4
ADD - SCAN QR CODE	4
ADD - MANUAL ADDING	5
ADD - ONLINE DEVICE	7
PUSH NOTIFICATIONS - MESSAGES	7
NOTIFY SURVEILLANCE CENTER	7
ENABLE ALARM NOTIFICATIONS IN GUARDING VISION	8
SETUP A NOTIFICATION SCHEDULE	8
DELETING MESSAGES	9
USING LIVE VIEW	9
PTZ CAMERA CONTROLS	11
MORE OPTIONS	11
USING PLAYBACK	12
PLAYBACK SCREEN FEATURES	12
REMOTE CONFIGURATION	13
RECORDING SCHEDULE	14
EVENT SETTINGS	14
"MORE" FEATURES	15
ACCOUNT MANAGEMENT	15
SETTINGS FOR ALIBI WITNESS 2 DEVICE	15

INSTALLATION

To install Alibi Witness 3.0 on an iOS phone or tablet, do the following: 1.

With your iOS device (phone or tablet), open the iTunes® app store. Tap to Search



2. Tap the **Search** icon at the bottom of the screen, enter **alibi witness 2**, and then tap **Search** again to open the search results page. See above.
3. On the results page for Alibi Witness 3.0, tap the **Open** button. The installation page will open. Verify that you found version **3.0.0**..
4. Tap **Open**, and then install the app. Follow the on-screen instructions to complete the installation.

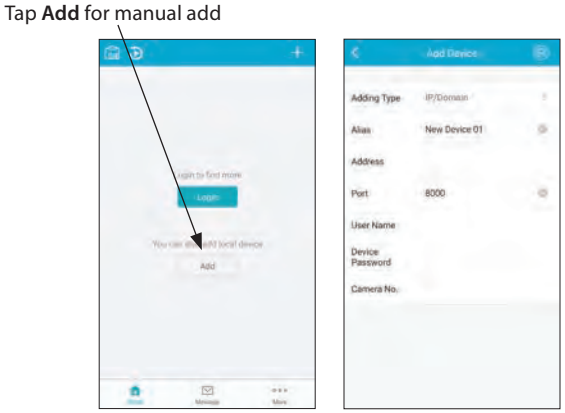
ADD - MANUAL ADDING

Manual adding permits you to add a device to the app for monitoring by manually specifying the network parameters for connecting to the device. In the example shown here, a network camera, setup for access through the internet, is added to the app.

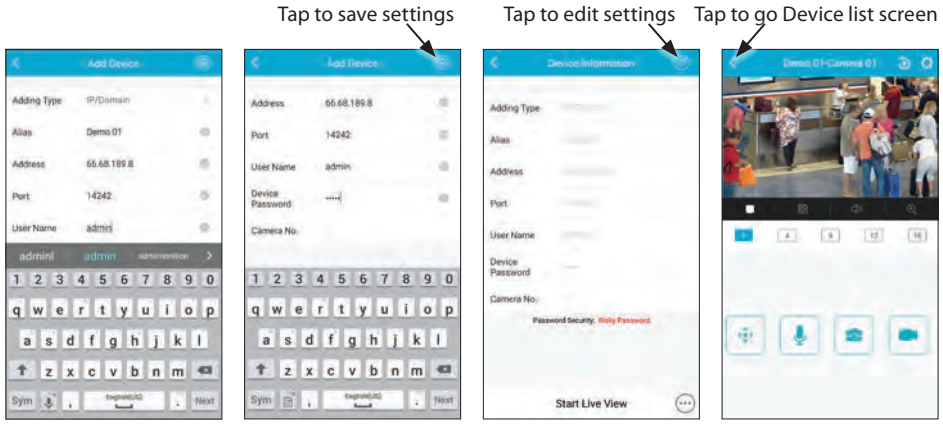
NOTE *To access a device on a local area network (LAN) from the internet, the router servicing the LAN must be setup to open a port or ports in the router's firewall through which the device can be addressed (i.e., Port Forwarded). For more information about Port Forwarding, see the document "**Port Forwarding for ALIBI™ IP Cameras and Recorders**" from Supercircuits and video on YouTube.com.*

To manually add a device to the app after installation, do the following:

1. After installing Alibi Witness 3.0 , tap the Alibi Witness 3.0 icon to open the app.
2. In the Home (middle) screen shown below, tap the **Add** button to perform a manual device add. The **Add Device** screen will open.



3. In the **New Device** screen, tap the **Alias** field, and then enter a name for the device using the virtual keyboard. In this example, the alias Demo 01 was entered. Also, essential information including the Internet (IP) **Address** and **Port** (determined through port forwarding), and the camera administrative **User Name** and **Password** were entered.



4. After completing these entries, tap the **save** icon in the upper right corner. If these entries are all valid, the **Start Live View** button will appear at the bottom the screen. If not, tap the **edit** icon, make changes as needed, then save your settings.

5. Tap the **Start Live View** button open a **Live View** window showing video from the camera (see above). If your phone supports screen rotation, you can view a larger image of the video.

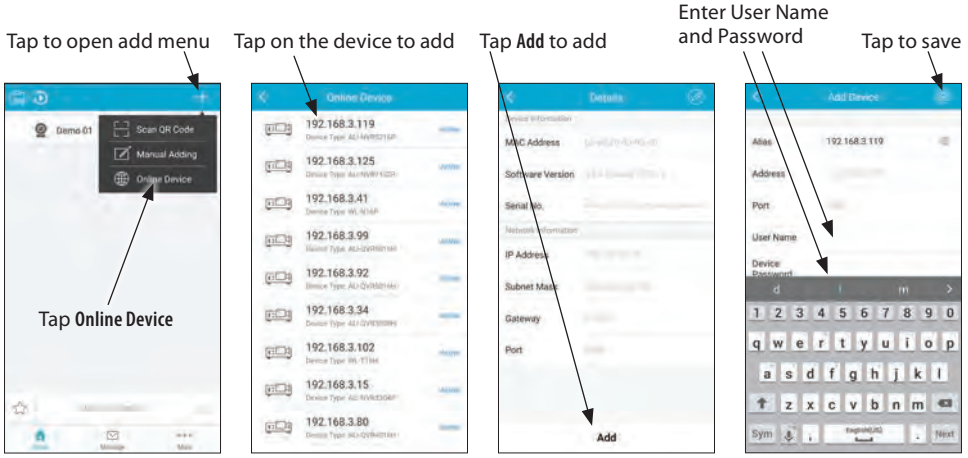


For more information about icons and controls on the Live View screen, see . To go to the Devices list scree, tap the back ( ) icon in the upper left corner.

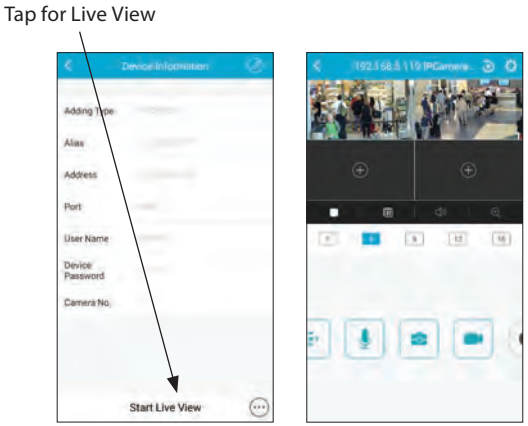
ADD - ONLINE DEVICE

If your phone or tablet is connected to a WiFi network on a LAN where devices you want to monitor are installed, you can easily add then to Alibi Witness 3.0. Adding devices in this way does not allow you to connect to them from the internet, only through a WiFi connection to the LAN. To use this feature:

1. In the Devices screen, tap the **Add** icon in the upper right corner.



2. In the drop-down list, tap **Online Device**.
3. In the **Online Device** screen, tap the device you want to add. In this example, the device identified by its IP address ***192.168.3.119*** was selected.
4. In the **Details** screen tap **Add**.
5. In the **Add Device** screen (see above), enter the **User Name** and **Password** for the device in the appropriate fields, and then tap the **Save** icon. If the User Name, Password, and other parameters are correct for the device, a **Start Live View** button will appear at the bottom of the screen.

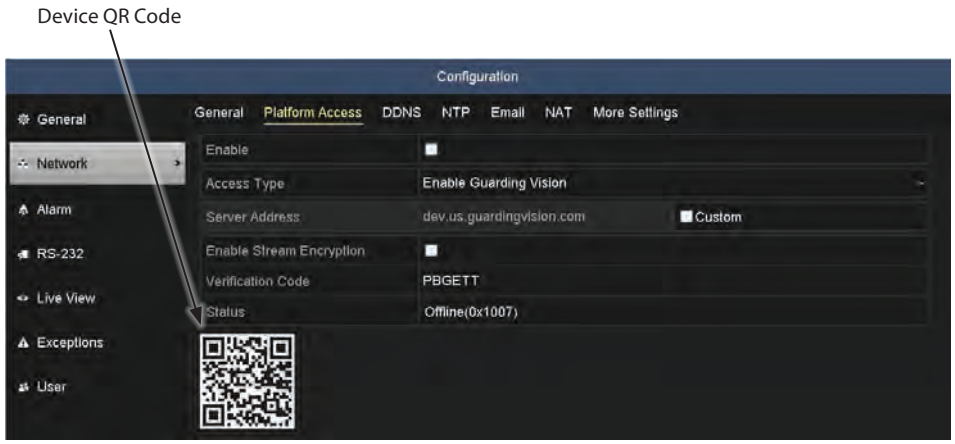


6. To return to the **Device** screen, tap the back ( ) icon.

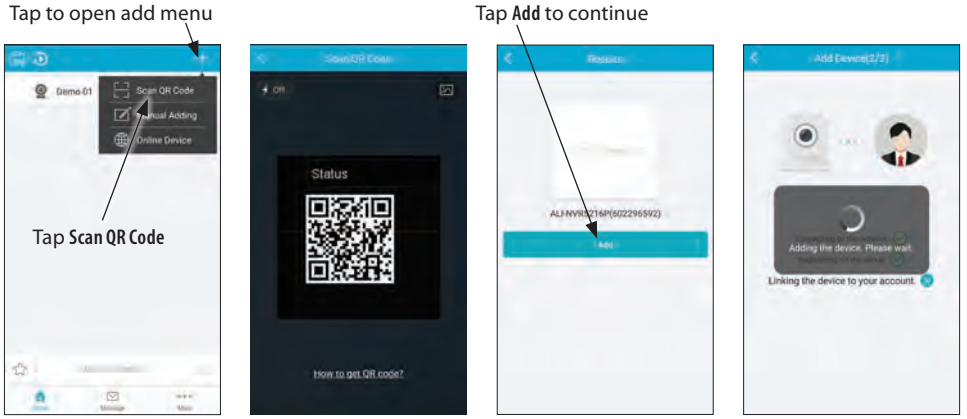
ADD - SCAN QR CODE

If your phone or tablet is connected to a WiFi network on a LAN where devices you want to monitor are installed, and you can log into the device with Internet Explorer, you can easily add the device to Alibi Witness 3.0 by scanning it's QR code. Adding devices in this way does not allow you to connect to them from the internet, only through a WiFi connection to the LAN. To use this feature: Adding devices in this way does not allow you to connect to them from the internet, only through a WiFi connection to the LAN. To use this feature: The QR code is usually found on the firmware **Configuration > Network > Platform Access** screen. To use this feature:

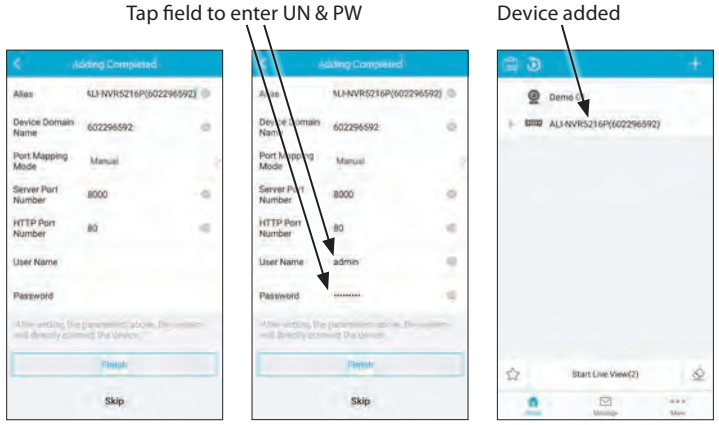
1. Log into the device you want add with a PC and Internet Explorer web browser. Use administrative credentials to login.
2. Display the QR code image in the firmware. It is usually on the **Menu > Configuration > Network > Platform Access** screen.



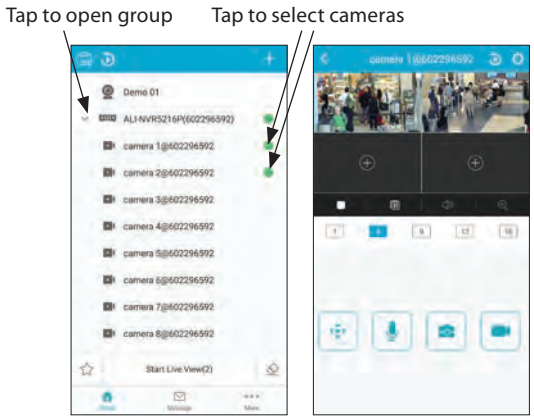
3. If a **Verification Code** was not previously setup for your recorder, create one at this time. Refer to the firmware user manual for the recorder for specific guidelines.
4. In the Alibi Witness 3.0 app **Home** screen, tap the Add (+) icon in the upper right corner, then tap **Scan QR Code**.



5. Position your phone such that the QR code in the firmware appears in the window on the screen. When the code is recognized, it will be automatically read and a status screen will open.
6. Tap the **Add** button to continue. It may take a few seconds for the app to connect to the device. When the connection is established, the **Adding Completed** menu will appear. See below.



7. In the **Adding Completed** menu, enter the administrative **User Name** and **Password** in the fields shown, and then tap the **Finish** button. The **Home** window will open with the device you added.
8. If you added a recorder, tap the icon on the left of the device line to open the camera list, and then tap the select icons on the right for the cameras you want to view. See below.



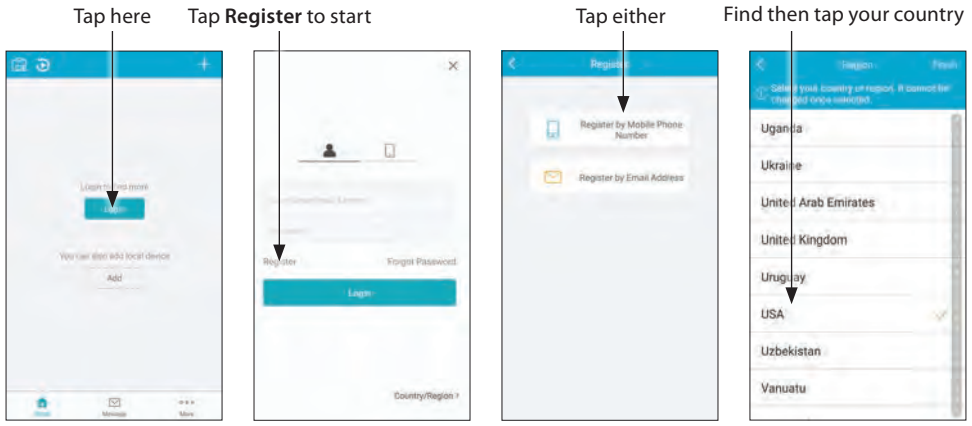
9. Tap the Start Live View button at the bottom of the screen to view video from the cameras.

Create Guarding Vision account

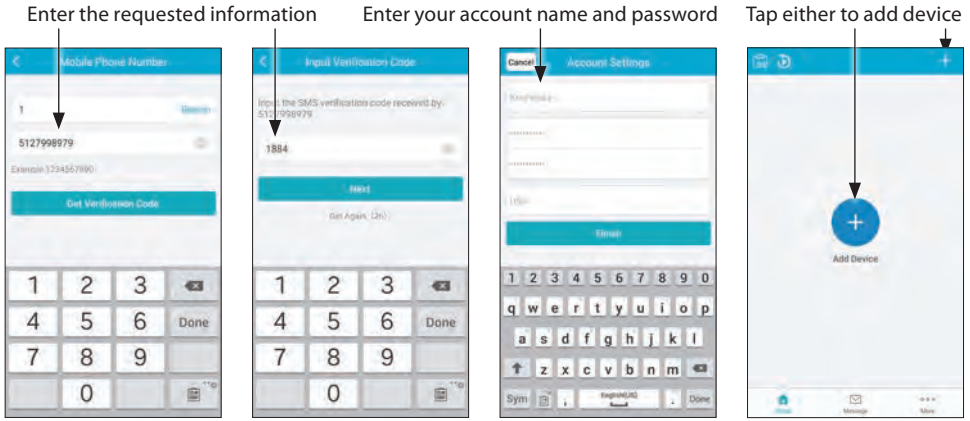
Alibi Witness 3.0 includes P2P Cloud service provided by Guarding Vision that creates a secure Peer-to-Peer connection from the recorder to your mobile device. It also provides Live View, playback of recordings, and push notifications that alert you in real time to events such as motion detection, tampering or video content analytics events. To use this service, you must create a Guarding Vision account, provided free by Observint Technologies, through the app.

After a Guarding Vision account is created, an Alibi device registered in Guarding Vision can easily add the device to Alibi Witness 3.0 r3 for mobile monitoring. You can add devices in either of three ways: **Scan** its **QR Code**, through **Manual Adding**, and by adding it as an **Online Device**. Before adding a device to Alibi Witness 2, Guarding Vision Platform Access must be enabled on the device.

1. To Register a new Guarding Vision account, tap the **Login** icon at the bottom of the Devices screen. See below. The screen shown here appears after installation of Alibi Witness 2. r3.



2. Tap **Register** in the Guarding Vision login screen.
3. In the Register screen, tap either **Register by Mobile Phone Number** or **Register by Email Address**. In this example, I selected to register by mobile phone number.
4. In the Region screen, scroll down to find and tap on your country.
5. Follow the screen messages to complete the registration. For **Register by Mobile Phone Number**:
   a. Enter your mobile phone number in the field shown below, and the tap **Next**. A SMS message containing a verification code will be sent to your phone. **NOTE**: The code you receive will expire with 30 minutes.



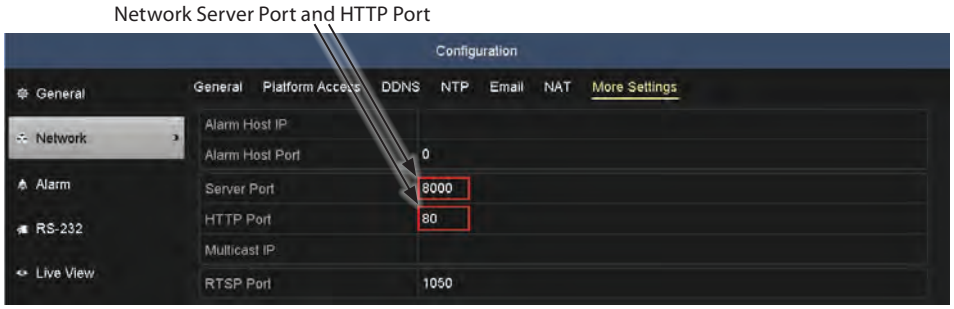
   b. Enter the verification code sent by Guarding Vision in the field shown on the Verification screen, and then tap **Next**.
   c. In the **Account Settings** screen, enter your preferred **Account Name** and **Password**, and then tap **Finish**. The Account Name must at least six characters and cannot contain any of the following: / \ : * ? " < > |. Passwords should have at least eight characters and include upper case letters, lower case letters, numbers and special characters. The **Home** window will open with an **Add Device** icon. See above.

ADD - SCAN QR CODE

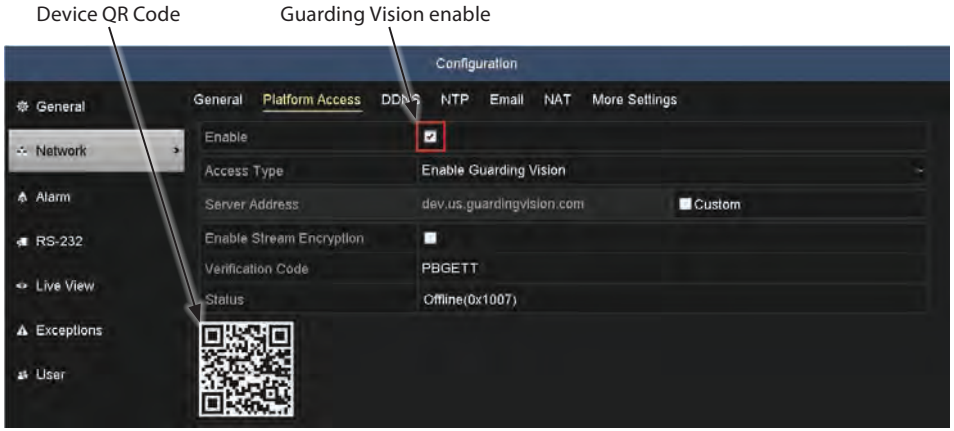
Guarding Vision QR Code Scanning is one of the easiest ways to add devices to Alibi Witness 3.0. To use this feature, you must have the following:

- Device administrative **username** and **password**
- **Server port** and **HTTP port** for the device.
- Device QR code visible or saved as image on your phone.

1. Log into the device you want add with a PC and Internet Explorer web browser. Use administrative credentials to login.
2. Find the **Server Port** and **HTTP Port** for the device. For Alibi DVRs and NVRs, this information is shown on the firmware screen **Menu > Configuration > Network > More Settings**. Usually, these ports are numbered 8000 and 80 respectively. See below.

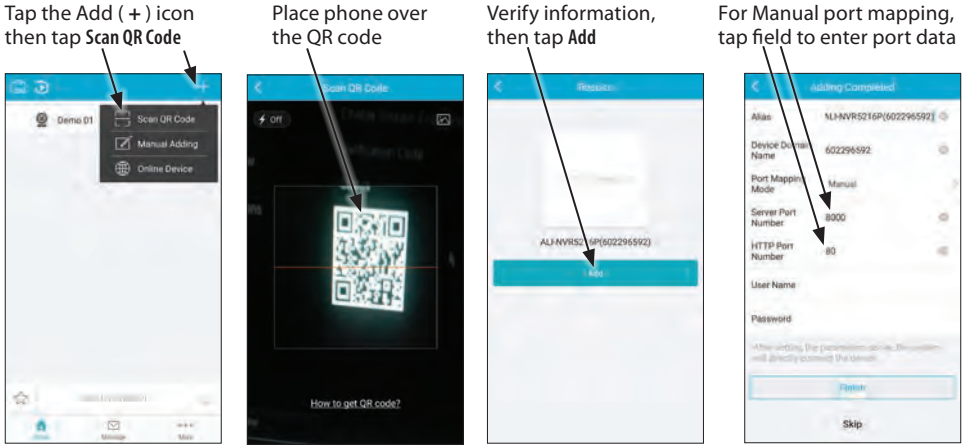


3. Open the firmware menu that shows Platform Access parameters. For Alibi DVRs and NVRs, this information is on the **Menu > Configuration > Network > Platform Access** screen. Verify that the Guarding Vision **Enable** box is checked. See below.



4. If a Verification Code was not previously setup for your recorder, create one at this time. Refer to the firmware user manual for the recorder for specific guidelines.

5. In the Alibi Witness 3.0 app **Home** page, tap the Add (+) icon in the upper right corner, then tap **Scan QR Code**.

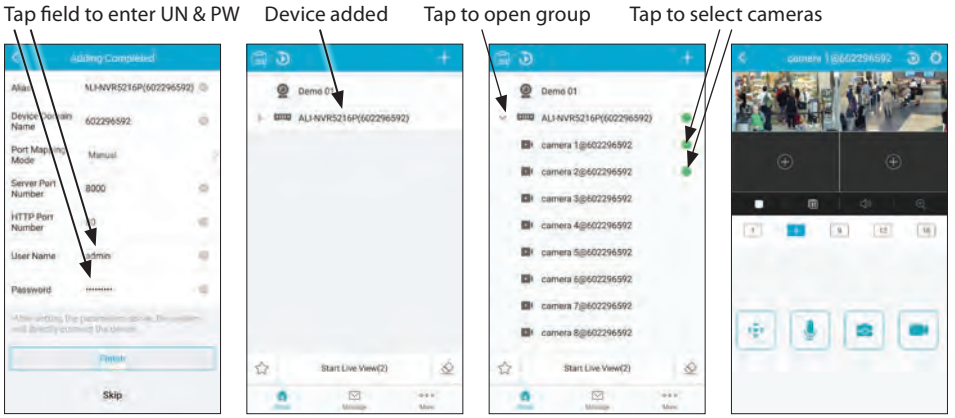


6. Position your phone such that the QR code in the firmware appears in the window on the screen. When the code is recognized, the **Results** screen will open. See above. **NOTE**: If you have the QR code for the device in an image file in your phone, tap the image icon in the upper right corner of the screen, browse to the location of the file, and select it.

7. In the **Results** screen, verify the information displayed, and then tap **Add**.

8. In the **Adding Completed** screen, enter the **Server Port Number** and **HTTP Port Number** if different from that shown. You can enter these port numbers manually, or tap on **Port Mapping Mode** field and then select **Automatic** to automatically populate these fields. Usually, these values are 8000 and 80, respectively.

9. In the same screen, enter the device administrative **User Name** and **Password**.



10. Tap **Finish** to complete the entries. If your setup was correct, the **Home** window will open and the device you entered will **not be** grayed out. See above.

11. To verify that the device camera video streams can appear in the Live View display, tap the open (**>**) icon before the device you added, tap the select boxes for the cameras you want to view, and then tap the **Start Live View** button at the bottom of the screen. The Live View display will open.

ADD - MANUAL ADDING

To manually add a device, you must have the following:

- Device administrative **username** and **password**
- **Guarding Vision Verification Code**. Also, Guarding Vision must be enabled.
- **Server port** and **HTTP port** for the device.
- Device **serial number**

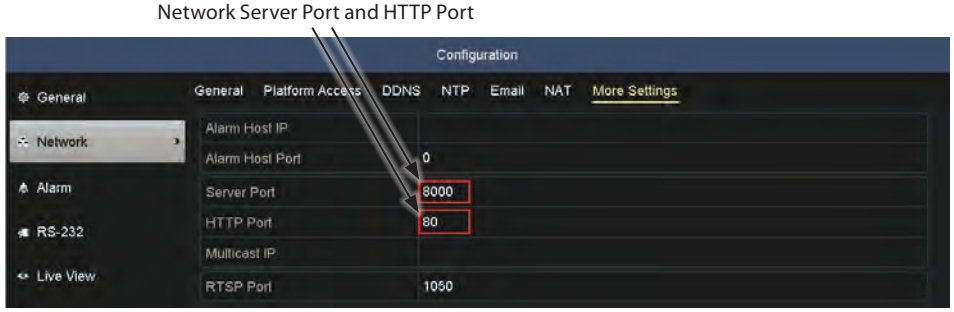
To perform a manual add:

1. Log into the device you want add with a PC and Internet Explorer web browser. Use administrative credentials to login.

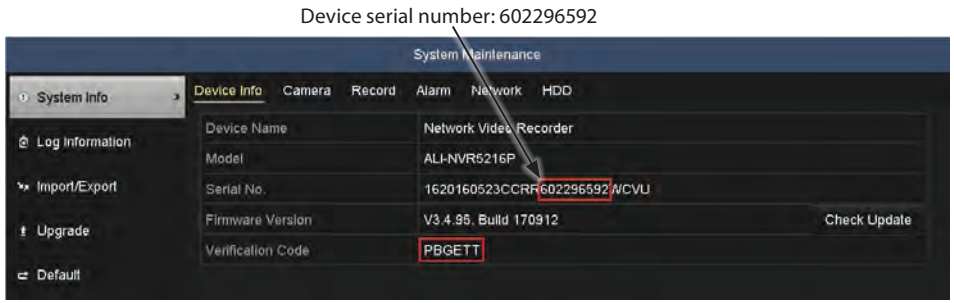
2. Find the **Guarding Vision Verification Code** and ensure that Platform Access for Guarding Vision is **enabled**. For Alibi DVRs and NVRs, this information is shown on the **Menu > Configuration > Network > Platform Access** screen. See below.



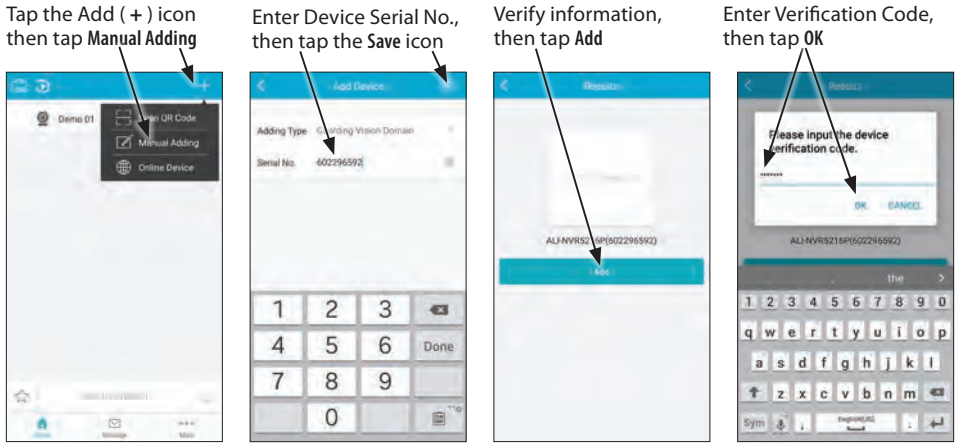
3. Find the **Server Port** and **HTTP Port** for the device. For Alibi DVRs and NVRs, this information on the **Menu > Configuration > Network > More Settings** screen. Usually, these ports are numbered 8000 and 80 respectively. See below.



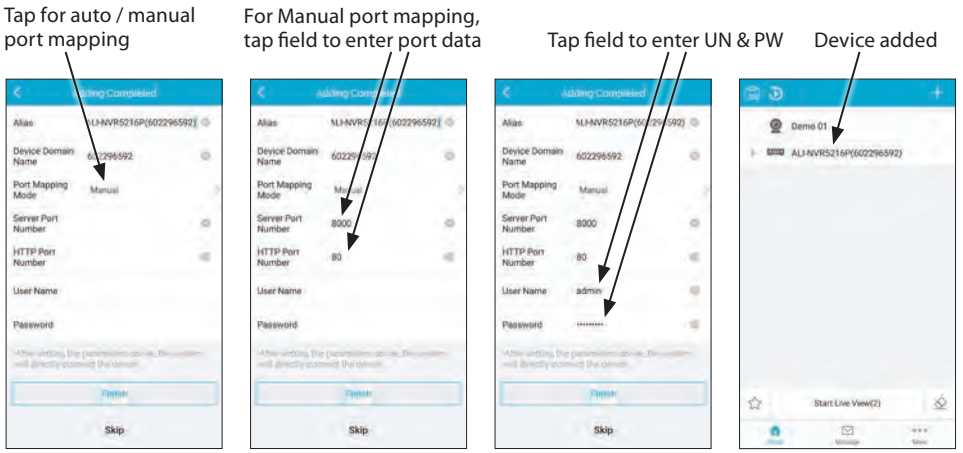
4. Find the Device Serial Number. For Alibi DVRs and NVRs, this information is shown on the **Menu > Maintenance > System Info** screen. See below. The device serial number needed is the last nine contiguous digits embedded in the **Serial No.** field. For this device, the serial number is **602296592**.



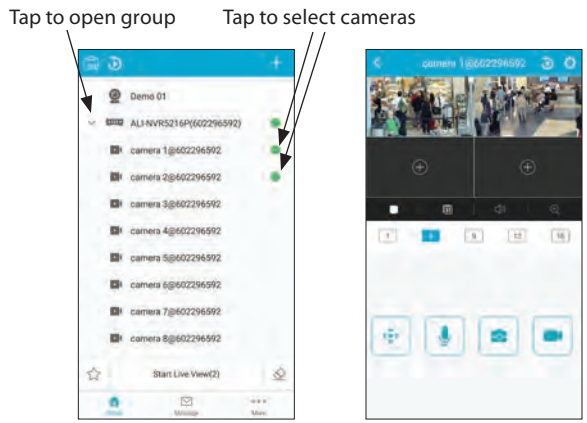
5. In the Alibi Witness 2.0 app Home page, tap the Add (+) icon in the upper right corner, then tap **Manual Adding**.



6. In the **Add Device** menu, enter the serial number determined earlier, and then tap the **Save** icon in the upper right corner.
7. In the **Results** screen, verify the information displayed, and then tap **Add**.
8. In the **Results** screen pop-up window, enter the **Verification Code** determined earlier, and then tap **OK**.
9. In the **Adding Completed** screen, enter the **Server Port Number** and **HTTP Port Number**. You can enter these port numbers manually, or tap on **Port Mapping Mode** field and then select **Auto** to automatically populate these fields. For Alibi DVRs and NVRs, this information can be seen in the firmware screen **Menu > Configuration > Network > More Settings** screen. Usually, these values are 8000 and 80, respectively.



10. In the same screen, enter the device administrative **User Name** and **Password**.
11. Tap **Finish** to complete the entries. If your setup was correct, the **Home** window will open and the device you entered will **not be** grayed out. See above.
12. To verify that the device camera video streams can appear in the Live View display, tap the open (**>**) icon before the device you added, tap the select boxes for the cameras you want to view, and then tap the **Start Live View** button at the bottom of the screen. The Live View display will open.

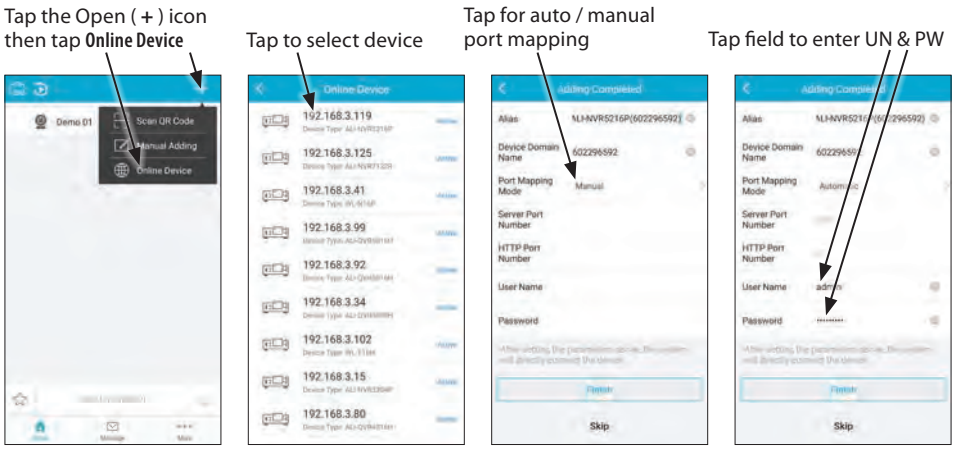


ADD - ONLINE DEVICE

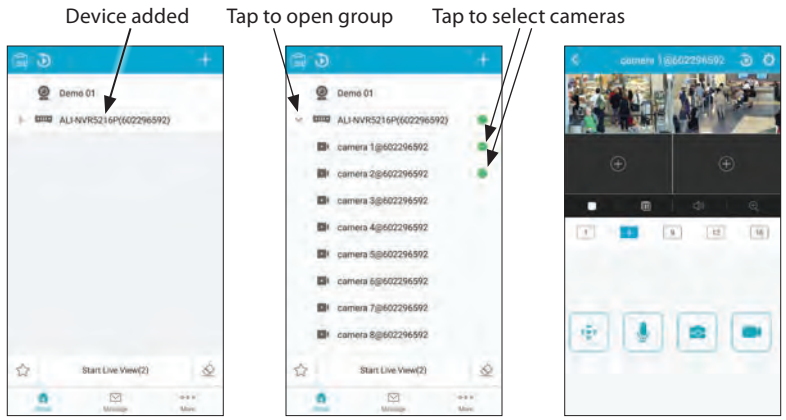
While logged into Guarding Vision, you can add a device to the app for monitoring if you are connected to the same LAN as the device. To use this feature:

1. In the Alibi Witness **3.**0 app Home page, tap the Add (**+**) icon in the upper right corner, then tap **Manual Adding**.

NOTE *After entering information into any menu field, tap the **Done** key on the pop-up keyboard to complete the entry.*



2. Browse the list of devices that were discovered, and then tap on the device you want to add.
3. In the **Adding Completed** screen, enter the **Server Port Number** and **HTTP Port Number**. You can enter these port numbers manually, or tap on **Port Mapping Mode** field and then select **Automatic** to automatically populate these fields. For Alibi DVRs and NVRs, this information can be seen in the firmware screen **Menu > Configuration > Network > More Settings** screen. Usually, these values are 8000 and 80, respectively.
4. In the same screen, enter the administrative device **User Name** and **Password**.
5. Tap **Finish** to complete the entries. If your setup was correct, the **Home** window will open and the device you entered will **not be** grayed out. See below.



6. To verify that the device camera video streams can appear in the Live View display, tap the open (**>**) icon before the device you added, tap the select boxes for the cameras you want to view, and then tap the **Start Live View** button at the bottom of the screen. The Live View display will open.

PUSH NOTIFICATIONS - MESSAGES

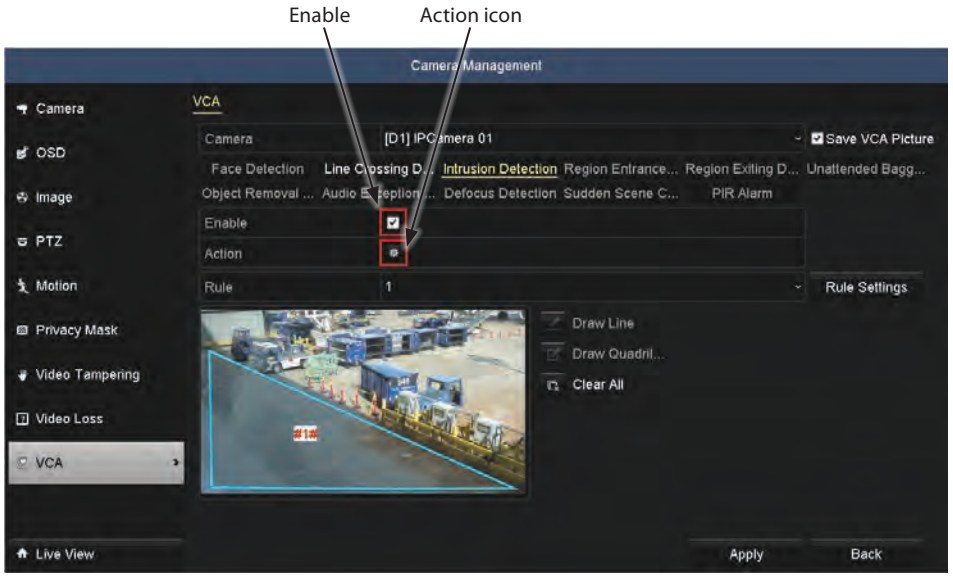
The Message screen displays Push Notifications (alarm messages) from the device or recorder. To receive messages:

- The device must be configured to "Notify Surveillance Center" when a specific alarm condition is sensed.
- Alarm Notifications in Guarding Vision, must be enabled. A notification schedule can be setup.
- To see messages pop-up alert messages appear on your phone, you must enable the **Push Notifications** option in the Applications setting screen. See ""More" features" on page 15.

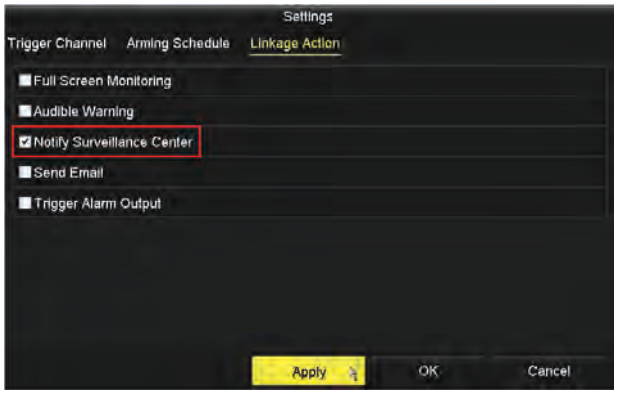
NOTIFY SURVEILLANCE CENTER

You can enable "Notify Surveillance Center" on the device when a specific alarm condition occurs for most types of alarms and for exception conditions in the NVR. In the example shown here, notification is enabled in a camera connected to a NVR when an Intrusion (VCA event) is detected. The process for enabling these notifications for other alarm occurrences is very similar.

1. Log into the NVR where the camera is attached. Use administrator login credentials.
2. Open the **Menu > Camera > VCA > Intrusion Detection** menu.



3. Enable **Intrusion Detection** for the camera of interest, and configure the area you want to sense for intrusions. See above.
4. Click the **Action** icon, and then select the **Linkage** tab.
5. Check the select box for Notify Surveillance Center, click **Apply** and then click **OK** to close the window. **NOTE**: You can use other Action features to setup a schedule for when the alarm is reported, and other cameras that can trigger the event.

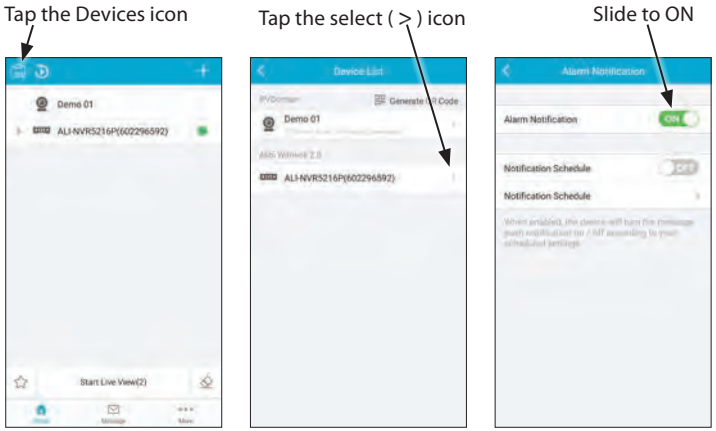


6. In the Intrusion Detection menu, click **Apply** to save your parameters.

ENABLE ALARM NOTIFICATIONS IN GUARDING VISION

Alarm Notifications are enabled for an individual device, such as an NVR or an IP camera attached directly to a LAN. This feature is enabled through the Settings menu for the device. To enable Alarm Notifications for the NVR added above:

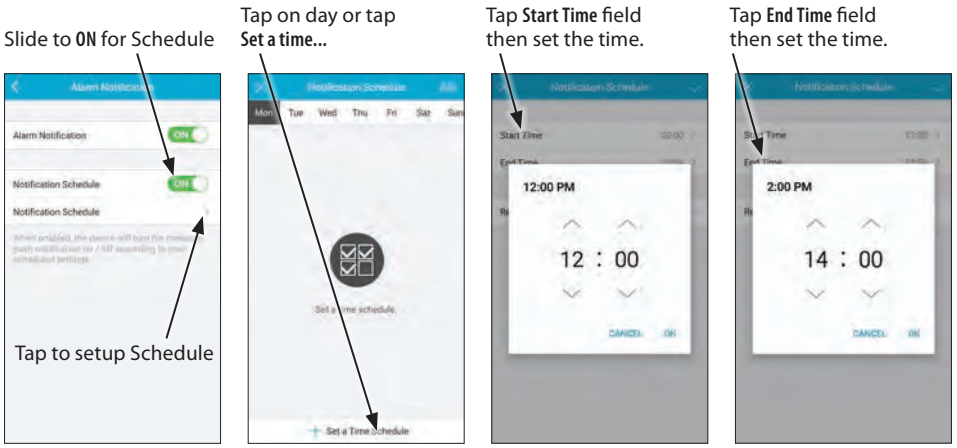
1. Tap the **Home** icon, and then tap the **Device List** icon in the upper left corner of the screen.



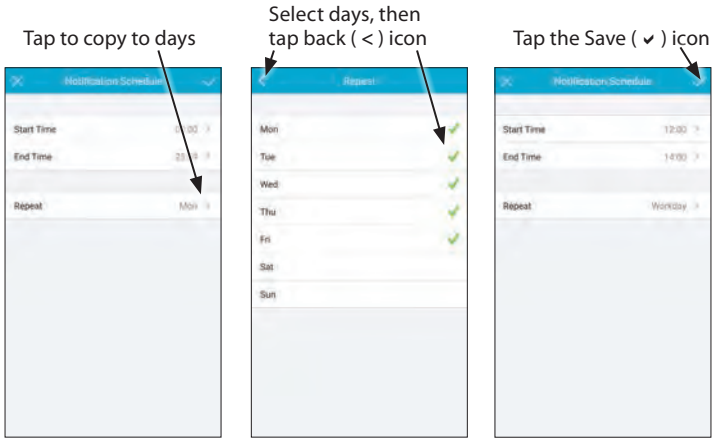
2. For the device you want to enable notification reporting, tap the select icon.
3. In the Alarm Notifications menu, slide the **Alarm Notification** option to **ON**. See above.

SETUP A NOTIFICATION SCHEDULE

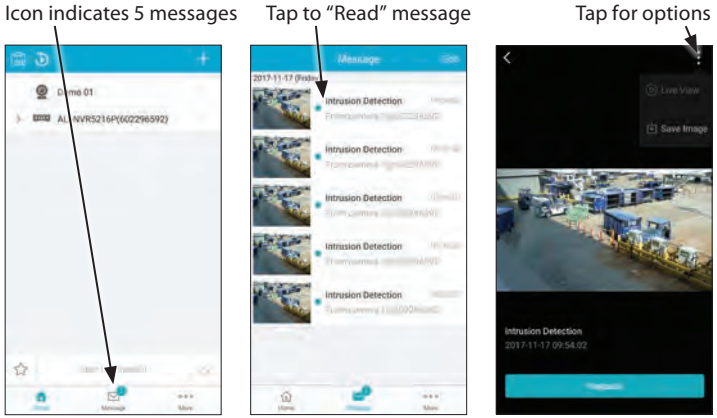
1. In the Alarm Notification screen, slide the **Notification Schedule** option to the right, and then tap the Schedule select (>) icon.



2. In the Notification Schedule screen, tap **+ Set a Time Schedule**, and then tap the **Start Time** field.
3. In the pop-up window, use the up and down icons to set the hour and minute of the start time. Tap **OK** to save the setting. In the example above, 12:00 PM was selected.
4. Tap the **End Time** field, and adjust the end time as needed. Tap **OK** to save the setting. In the example above, 2:00 PM was selected.
5. Tap the select icon in the Repeat field to copy the schedule to different days of the week. See below.



6. In the **Repeat** menu, select the days you want to copy the schedule to, and then select the back icon (<) in the upper left corner.
7. Tap the **Save** icon in the upper right corner to save the schedule. You can tap the **Close** icon (×) in the upper left corner to return to Home menu.
8. When messages occur, they are indicated on the **Messages** icon. The Messages icon in the screen below shows 5 notifications. Tap this icon to open the Messages screen. See below.

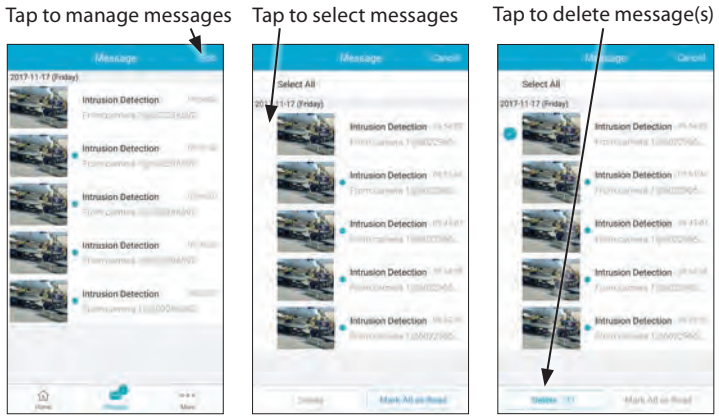


9. To "read" a message, save an image, open the Live View screen of the camera, or playback the video associated with the message, tap on the notification. In the next screen (see above), you can open the options list to save the image or open the Live View video from the camera. Also, tap the **Playback** button to play the video associated with the notification.

DELETING MESSAGES

To delete a message:

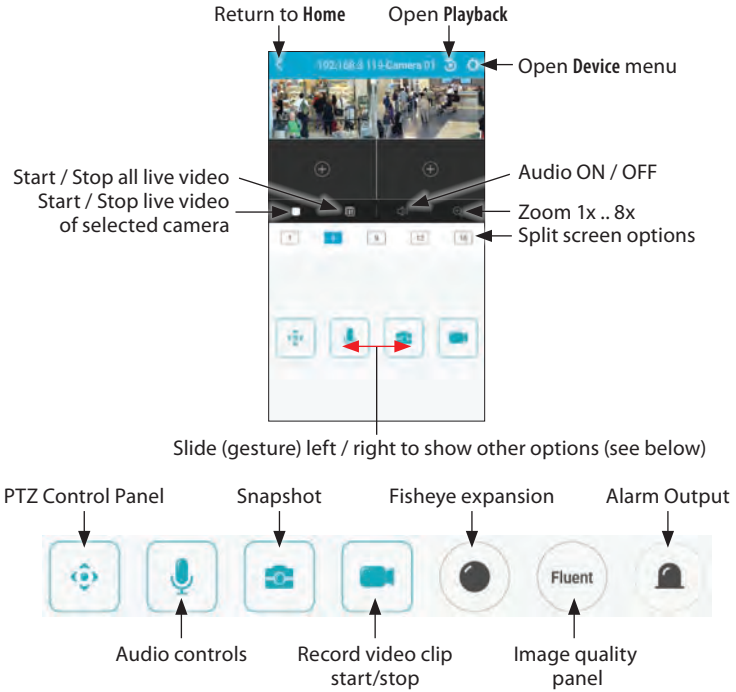
1. In the Messages screen, tap the Edit icon in the upper right corner.
2. Tap the select bullet for the message you want to delete, and then tap the **Delete** button to permanently remove it.



3. Tap **Cancel** to return to the Home screen.

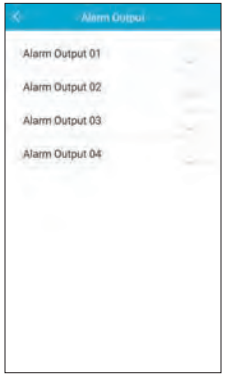
USING LIVE VIEW

Use the Live View screen to watch live video from your cameras and control PTZ cameras. If your camera supports screen rotation, the horizontal orientation provides a larger image of live video.

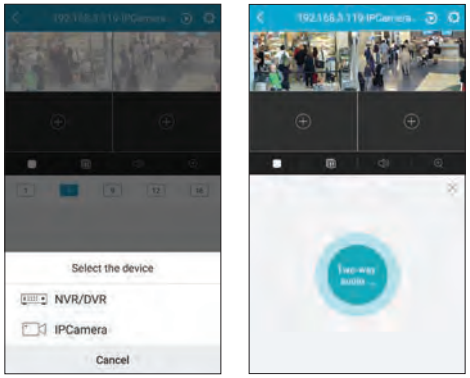


Usage:

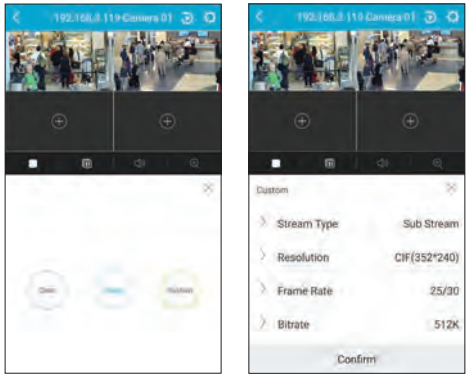
- **Alarm Output** Provides controls to enable or disable alarm outputs. To enable an alarm output, slide the select button to the right.



- **Audio controls**: Start two-way audio with either the recorder or camera.

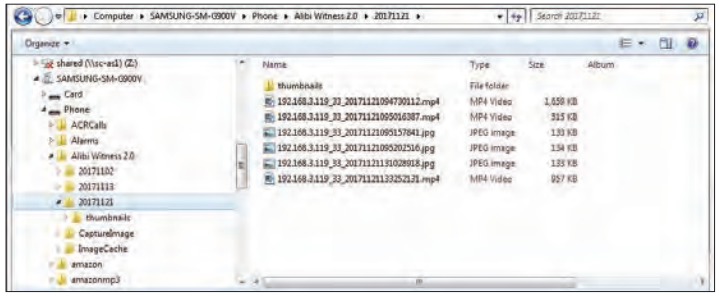


- **Audio ON / OFF**: Enable, disable audio
- **Fisheye expansion**: Opens multi-frame options for fisheye cameras only. The icon shown here changes for the fisheye mode selected: Wall mounting, Ceiling mounting, Dual 180º panorama, 360º panorama, 4 PTZ views, etc. These features depend on the capability of the camera.
- **Image Quality panel**: Opens panel to select either of three video adjustment options, **Clear**, **Fluent**, or **Custom**, for the selected camera. In the Custom menu (see below), you can select the stream, and adjust the resolution, frame rate, and bitrate.



- **Open Device menu**: Opens the Device menu. You can edit the edit the connection settings for the device, if needed.
- **Open Playback**: Opens the Playback menu for the selected camera. By default, the playback timeline is displayed for the current date.
- **PTZ Control Panel**: Opens the control panel for PTZ capable cameras. See "PTZ Camera Controls" on page 11.
- **Record video clip Start / Stop**: Tap this icon to start and stop recording a clip of live video. This video clip can be opened and replayed from the **Pictures and Videos** screen. It can be downloaded from the (Android directory) **Phone > Alibi Witness 3.0 > *YYYYMMDD*** where ***YYYYMMDD*** is the *date when the video clip was recorded.*





Android™ phone directory in Microsoft Windows® Expolorer

- **Return to Home**: Returns to the **Home** screen (lists devices added to the app).
- **Snapshot**: Captures an image of the current video frame. This can be opened from the **Pictures and Videos** screen and can be downloaded from the (Android directory) **Phone > Alibi Witness 3.0 > *YYYYMMDD*** where ***YYYYMMDD*** is the *date when the Snapshot was captured*. See **Record video clip Start / Stop** above.
- **Start / Stop all live video**: Restarts and stops live video retrieval from all cameras. When stopped, the video image shown in each frame is the last frame played from the each camera.
- **Start / Stop live video of selected camera**: Restarts and stops live video retrieval from the selected cameras. When stopped, the video image shown is the last frame played from the camera.
- **Split screen options**: Tap the icon to arrange the Live View screen in 1, 4, 9, 12, or 16 video panels. Each panel can show a different video stream. For fisheye cameras, different frames can show video streams from the same camera, depending on the fisheye mode.
- **Zoom 1x .. 8x**: Tap this icon to expand the video image. Options are 2.0x, 4.0x. 8.0x. The expansion factor is displayed in the upper left corner of the image. When the image is expanded, you can drag the image left, right, up or down to show a different area if the video in the video panel.

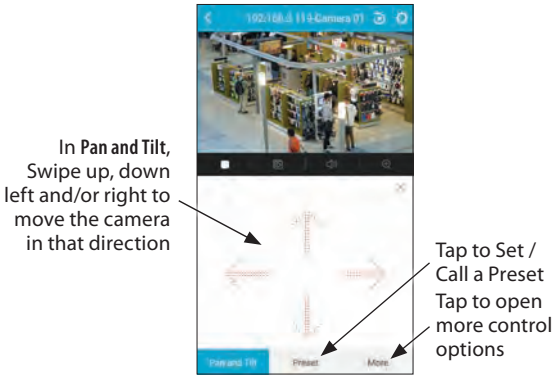
If rotation is enabled on your phone, you can turn the phone sideways to view a larger video image. The pop-up icon menu is shown only for a few seconds after the screen rotates, but can reappear after touching the screen.



For definitions of the icons, see the Live View screens above. You can also playback recorded video in rotated screen mode.

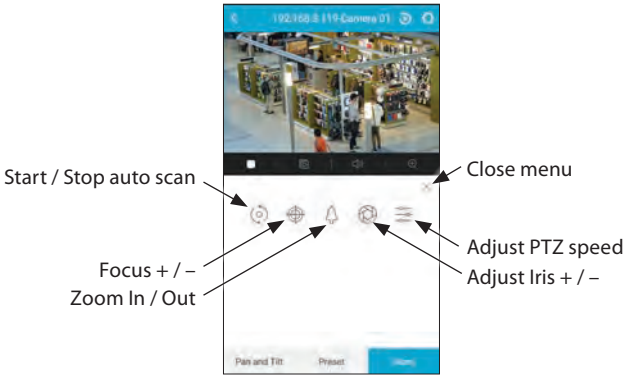
PTZ CAMERA CONTROLS

The PTZ control options (for cameras with PTZ features) are enabled by the PTZ Control Panel icon in the Live View display. When this mode is active, you can use gestures to move the camera up, down, left or right, and zoom in or out. You can also pan continuously, adjust the focus and iris, and Set and Call presets. Refer to your PTZ camera manual for more information about PTZ features. To access PTZ features, select (tap on the video of) a PTZ camera in the Live View display, and then tap the PTZ Control Options icon:



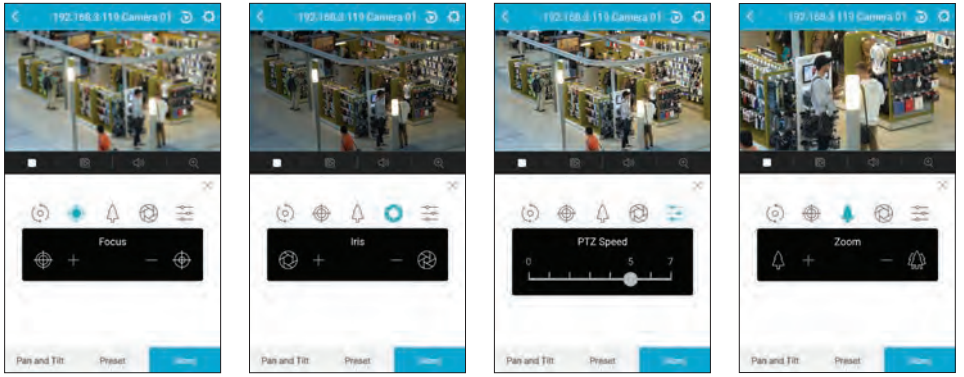
MORE OPTIONS

Tap the More button to open options to perform an endless autoscan, and adjust the Focus, Zoom, Iris and PTZ movement speed.



Usage:

- **Auto Scan**: Tap to start and stop a continuous pan of the camera.
- **Focus**: To adjust the Focus, tap the focus icon, and then tap **+** or **–** to focus in and out. See below.

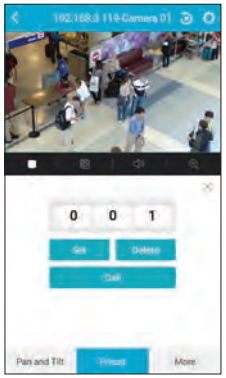


- **Iris**: To adjust the camera iris, tap the Iris icon, and then tap **+** or **–** to brighten or darken the image. See above.
- **PTZ speed**: To adjust the speed of the motion of the camera, tap the PTZ Speed icon, and then slide the dot right or left to quicken or slow the speed of the camera. See above.
- **Zoom**: To adjust the camera zoom, tap the Zoom icon, and then tap **+** or **–** to zoom in or out. See above.

Presets

Preset is a feature of Alibi PTZ cameras that provides a way to quickly move to a preset field of view. You can create more than 200 Presets in most Alibi PTZ cameras. To create and use a Preset:

1. Select a PTZ camera in the Live View display.
2. Tap the PTZ Control Options icon.
3. Use **Pan and Tilt** to move the camera to the field of view for which you want to create a preset. See "PTZ Camera Controls" on page 11.
4. Use **More** options to adjust the zoom, focus and iris to perfect the image (see **More options** above).
5. Tap the **Preset** button at the bottom of the Live View PTZ control screen.



6. Swipe the up and down to select a number for your preset. Presets can be numbered from 1 to 255, with the exclusion of several unchangeable presets between 80 and 120.
7. Tap **Set** to commit save the preset position.

8. To test the preset:

   a. Use **Pan and Tilt** to move the camera to a different position. You can also use **More** options to change the zoom and iris.

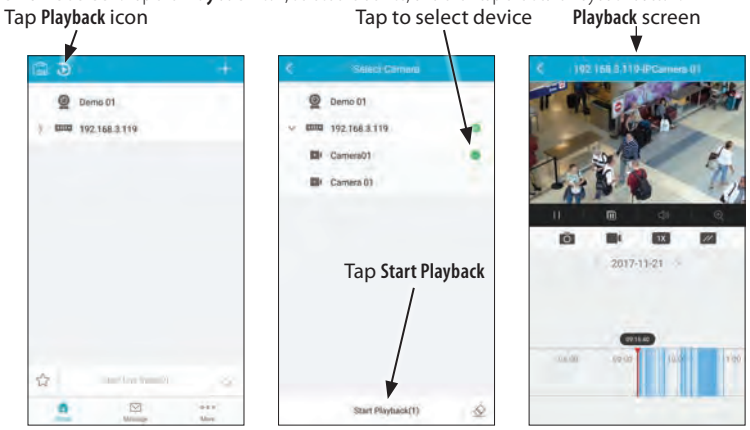
   b. Tap the **Preset** button, and then dial the numbers to the preset number you setup.

   c. Tap **Call**. The camera should move to the preset position you set, with the proper zoom, iris and focus settings.

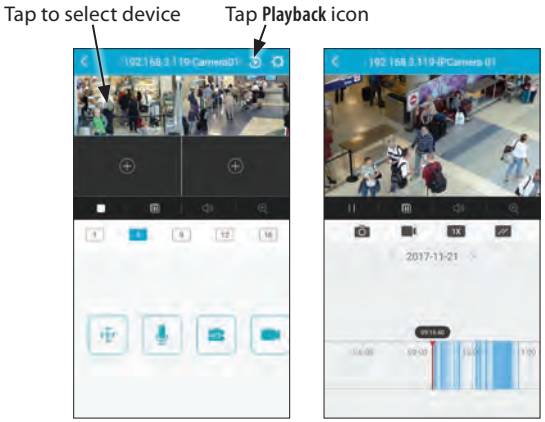
Using Playback

Using the playback feature in Devices, you can playback recorded video that is saved in your recorder. There are two common ways to playback recorded video:

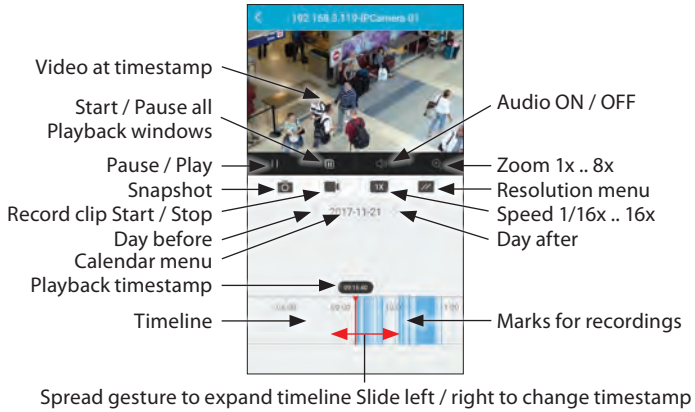
- **From the Home screen**: Tap the **Playback** icon, select the device, and then tap the Start Playback button.



- **From the Live View screen**: Select the device, and then tap the **Playback** icon.

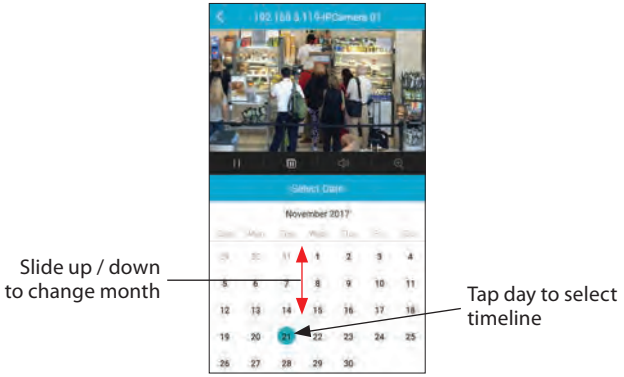


Playback Screen Features

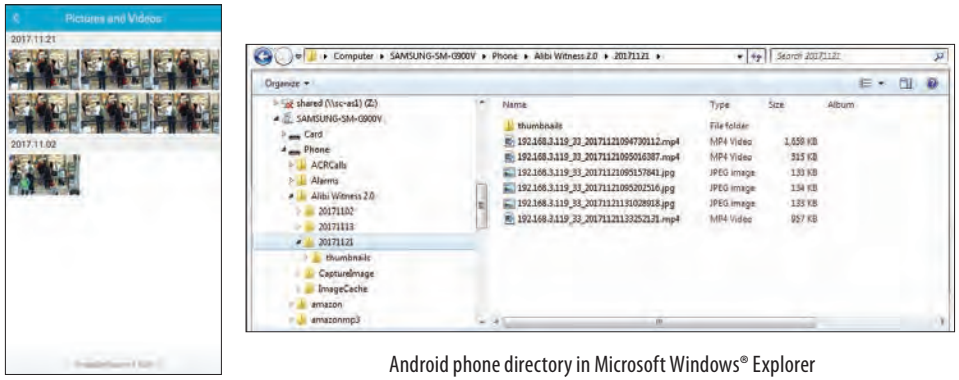


Usage:

- **Audio ON / OFF**: Enable, disable audio
- **Calendar Menu**: Opens a calendar menu. Select the month (gesture up or down) and then tap the day to open the video timeline.

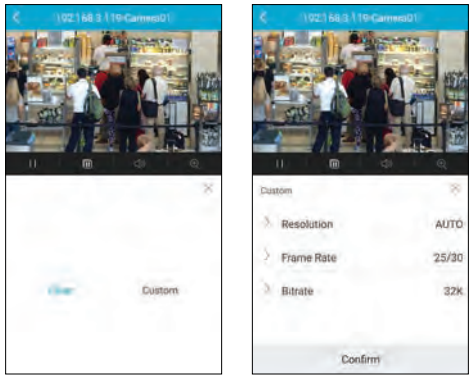


- **Day after**: Opens the video timeline for the day after the timeline shown.
- **Day before**: Opens the video timeline for the day before the timeline shown.
- **Marks for recordings**: Vertical marks show when video was recorded on that day.
- **Pause / Play**: Pause playback, start (resume) playback of video. If the timestamp is not positioned on a video clip when you start playback, playback will begin with the next video clip.
- **Playback timestamp**: Indicates when the current video frame was recorded.
- **Record clip Start / Stop**: Tap this icon to start and stop recording a clip of video being played back. This video clip can be opened and replayed from the **Pictures and Videos** screen. It can be downloaded from the (Android directory) **Phone > Alibi Witness 3.0 > *YYYYMMDD*** where ***YYYYMMDD*** is the *date when the video clip was made* (may not be the date of the video being played back was recorded).

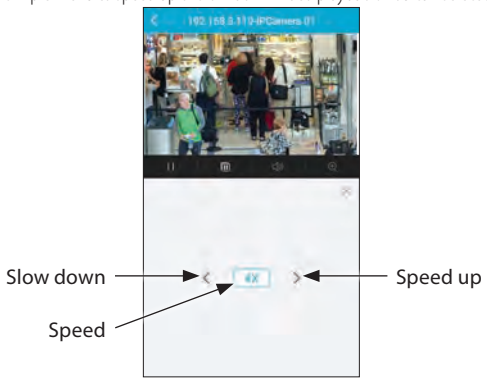


Android phone directory in Microsoft Windows® Explorer

- **Resolution menu**: Opens a menu to change the video playback parameters. After tapping the Resolution icon, tap either **Clear** (return to default settings) or **Custom**, to adjust the playback resolution, frame rate, and/or bit rate. In the Custom menu, tap each option and make adjustments as needed, then tap **Confirm** to retain the settings and close the menu.



- **Snapshot**: Captures an image of the current video frame. This can be opened from the **Pictures and Videos** screen and can be downloaded from the (Android directory) **Phone > Alibi Witness 3.0 > *YYYYMMDD*** where ***YYYYMMDD*** is the *date when the Snapshot was captured* (may not be the date of the video being played back was recorded). See **Record clip Start / Stop** above.
- **Speed 1/16x .. 16x**: Opens a simple menu to speed up or slow down video playback. You can select speeds between 1/16x and 16x.

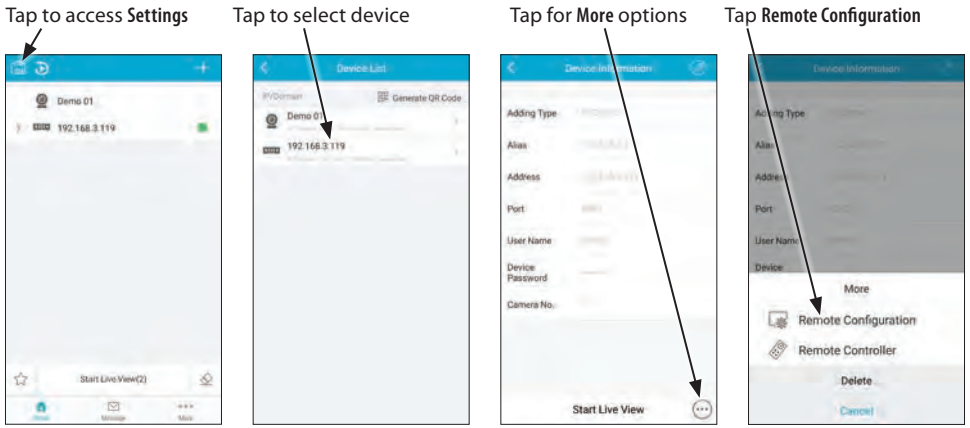


- **Spread gesture... Slide left / right**: To expand or contract the timeline, apply a spread or pinch gesture to the timeline. To change the time of video playback, drag the timeline left or right.
- **Start / Pause all Playback windows**: Use to control all playback streams.
- **Timeline**: Graphical element that shows when video clips were recorded, and when the currently playing video frame was recorded.
- **Video at timestamp**: Timestamp of the video frame that appears in the window.
- **Zoom 1x .. 8x**: Tap this icon to expand the video image. Options are 2.0x, 4.0x. 8.0x. The expansion factor is displayed in the upper left corner of the image. When the image is expanded, you can drag the image left, right, up or down to show a different area in the window.

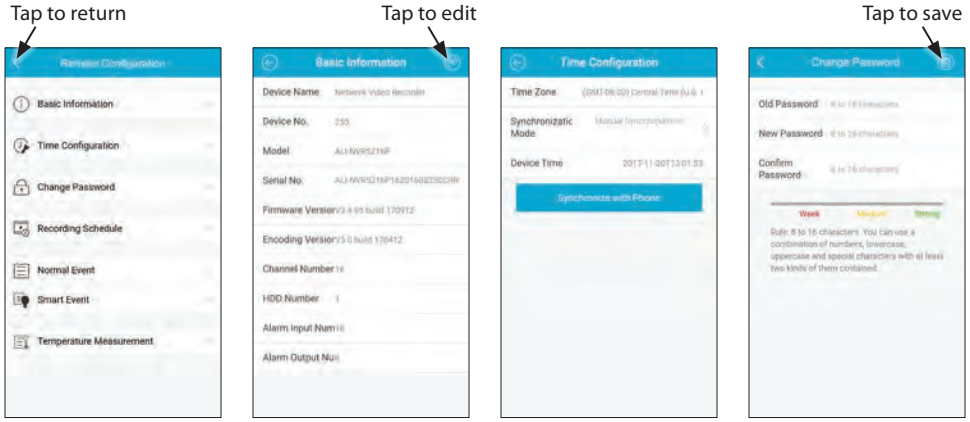
Remote Configuration

The Remote Configuration feature enables you to set basic device parameters, including the device time, password, recording schedule, and basic alarm event options. To access these features:

1. Open the Devices screen to list the devices you added for monitoring.



2. Tap the **Settings** icon in the upper left corner.
3. Select the device to configure. Tap the "**>**" icon to open the **Device Information** screen.
4. Tap the More icon in the lower right corner, and then select **Remote Configuration**.



5. In the **Remote Configuration** screen, tap the "**>**" icon associated with the item to open the configuration screen:

   a. In the **Basic Configuration** screen, you can tap the **Edit** icon in the upper right corner to change the **Device Name** and **Device No**. Tap the **Save** icon to retain your settings.

   b. In the **Time Configuration** screen, tap the field to set the **Time Zone** and **Synchronization Mode**.

   c. In the **Change Password** screen, tap each field and enter the appropriate information to change the password. Tap the **Save** icon to retain the new password.

RECORDING SCHEDULE

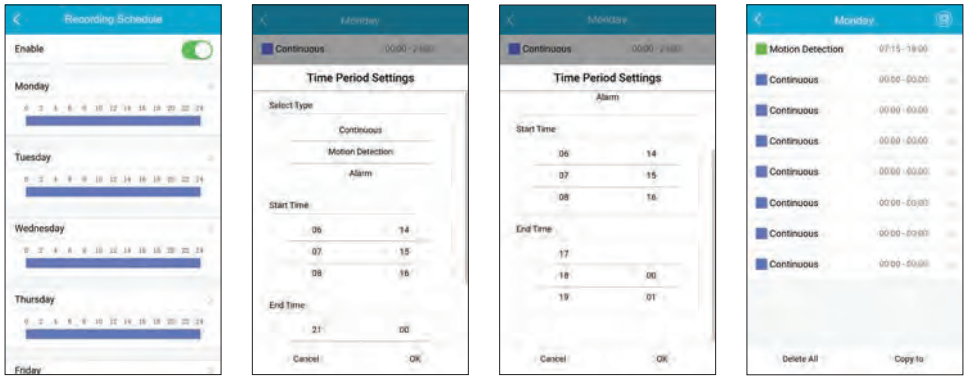
You can configure the recording schedule for each camera monitored by an NVR. In the following example, the recording schedule for a camera is changed from all-day continuous recording to motion recording only from 07:15 to 1800 hours.

NOTE *Recording schedule setup in the Alibi Witness app enables a configurations for Continuous, Motion Detection and Alarm recording only. More options are available through login to the recorder's web interface.*

   d. In the **Recording Schedule** screen, tap the "**>**" icon associated with the day to open the configuration screen. In the Example below, Continuous recording (blue bar) was configured for this device. In this example, Motion Detection recording will be setup. You can select any of the following recording Types:

   - **Continuous**: The video will be recorded continuously between the Start Time and End Time of the schedule.
   - **Motion Detection**: The video will be recorded when motion is detected. To setup motion detection, log into the camera (or video recorder) with your PC and configure the settings appropriately for the field of view.
   - **Alarm**: The video will be recorded when the alarm is triggered through an alarm input channels.
   - **Motion Detection or Alarm**: The video will be recorded when the external alarm is triggered or motion is detected.
   - **Motion Detection and Alarm**: The video will be recorded when motion and alarm are triggered at the same time.
   - **Event**: The video will be recorded when any event is detected.

   The camera you configure must support the Type of recording you select.

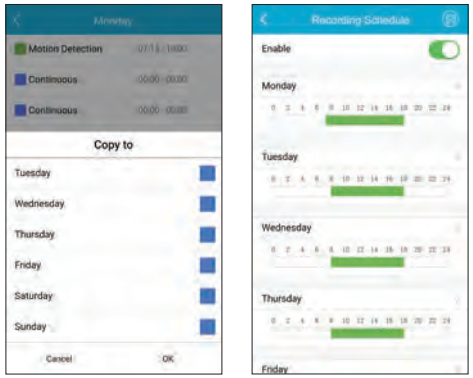


   i. To configure the recording for Monday, tap the "**>**" icon associated with the Monday to open the **Time Period Settings** screen.

   ii. For the **Select Type**, **Start Time** and **End Time** options, drag the each list up and down to center your preference between the middle bars. In the example above, Continuous was changed to Motion Detection, and the Start Time and End Time selections were changed to 07:15 (7:15 am) and 18:00 (6 pm). Tap the **OK** button at the bottom when done.

   iii. In the upper screen on the right, tap the **Save** icon to retain your settings. Similarly, you can configure up to 7 additional time slots during the day for the same or other types of recording. Time slots cannot overlap.

   iv. To copy this day's recording schedule to other days of the week, tap the **Copy to** button at the bottom of the screen.



   v. In the screen above on the right, tap the select boxes for the days you want to copy the schedule to, and then tap the **OK** button at the bottom.

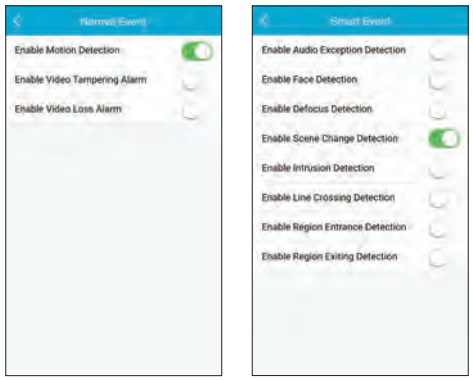
   vi. Tap the **Save** icon at the top to retain your configuration.

   vii. When done, tap the return icon in the upper right corner to return to the Remote Configuration screen.

EVENT SETTINGS

   e. In the **Remote Configuration** screen, tap the "**>**" icon associated with **Normal Event** to configure alarm reporting of these occurrences.

   To enable reporting of a Normal Event occurrence, tap the right of the oval to enable the event reporting. In the example below, Motion Detection is enabled. After selecting the options you prefer, tap the return icon to go back to the Remove Configuration screen.



   f. In the **Remote Configuration** screen, tap the "**>**" icon associated with Smart Event to configure alarm reporting of these occurrences.

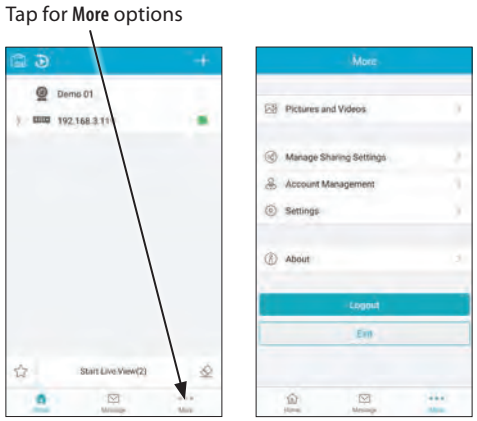
   To enable reporting of a Smart Event occurrence, tap the right of the oval to enable the event reporting. In the example shown above, only Scene Change Detection is enabled. After selecting the options you prefer, tap the return icon to go back to the Remove Configuration screen.

g. In the **Remote Configuration** screen, tap the "**>**" icon associated with Temperature Measurement to configure alarm reporting of these occurrences. **NOTE**: To use this feature, you must have a device that can report temperatures. After configuring this screen, save your settings and return to the Remote Configuration screen.

6. In the **Remote Configuration** screen, tap the "**<**" icon in the upper left corner to return to the **Devices** menus.

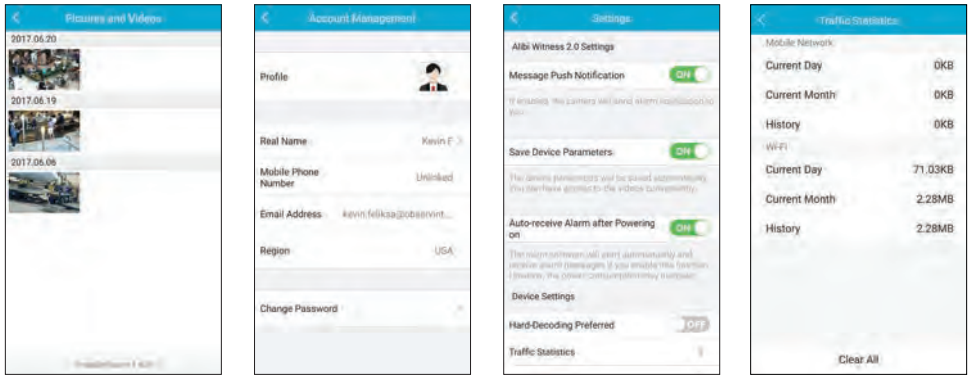
"More" features

The More screen provides links to several management and configuration features for Alibi Witness 3.0. Open the **More** screen by tapping the More icon at the bottom of the window.



1. In the **More** screen, tap the "**>**" icon associated with the item to open the configuration screen:

   a. **Pictures and Videos**: This link opens thumbnail images containing links to pictures and video clips you saved. Tap on the image to open the file. See above.



Account Management

b. **Account Management** (see above): Contains specific information related to your copy of Alibi Witness 3.0. The region setting cannot be changed.

   — To change your Profile picture, tap on the photo thumbnail and then either take a picture or choose a photo from an album.
   — To change your account password, tap the Change Password button, and then follow the on-screen instructions at the bottom from this screen.

Settings for Alibi Witness 2 device

c. **Settings** (see above): The Settings screen includes both settings for Alibi Witness 3.0 and Device settings related to the app. An explanation for each app setting is provided. Device settings include Hard-Decoding Preferred (use hardware stream decoding (for processor stream decoding instead of software decoding), a link to a Traffic Statistics report (see above) and a link to a Wi-Fi Settings screen (link not shown).

   — **Hard-Decoding Preferred**: Hardware Decoding can provide better decoding performance and lower CPU usage when streaming HD video during live view and playback.
      — When the option is switched to ON, hardware decoding is performed.
      — This option is available for smartphones with Android version 4.1 and later.
      — Hardware decoding supports resolutions of 704*576, 704*480, 640*480, 1024*768, 1280*720, 1280*960, 1920*1080, 2048*1536, and 2560*1920. Use software decoding for other resolutions.
      — Hardware decoding is not supported for H265 compression.
   — **Traffic Statistics** (see the screen above)
   — **Wi-Fi Settings**: This feature is not supported.

d. **Feedback**: You can send comments about this app to Observint Technologies. Please report problems you experience and recommendations for improvement.

e. **About**: The about screen shows the app title and the version number.

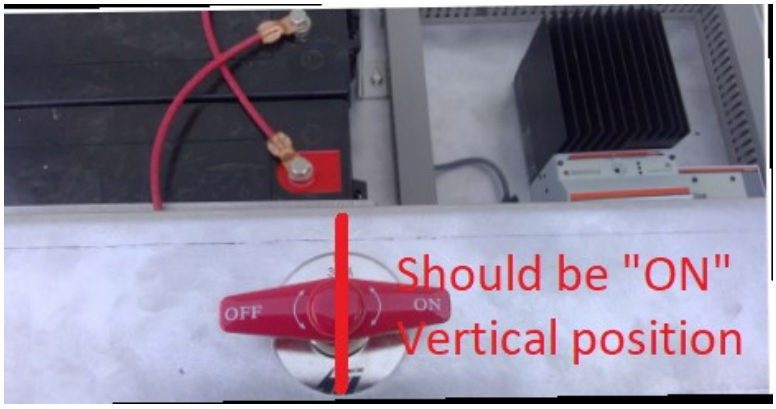
f. **Logout**: Tap **Logout** to log out of **Guarding Vision**. You must log back in to Guarding Vision to use that access platform.

g. **Exit**: Tap **Exit** to close the app.

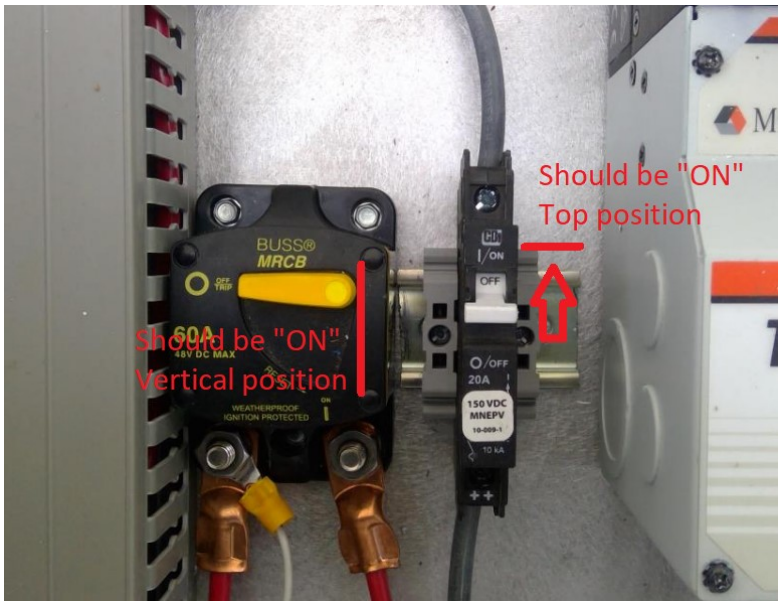
ROUTER TROUBLESHOOTING

Should you lose network connection to your unit, check to make sure the following steps are taken.

- The following switch should be in the vertical positon with the "ON" handle on top.



- Ensure the following two switches are in the 'ON' position as well. The MRCB black and yellow switch, should have the handle in the vertical position. The black and white MNEPV switch should be flipped up showing the 'ON' portion of the switch.



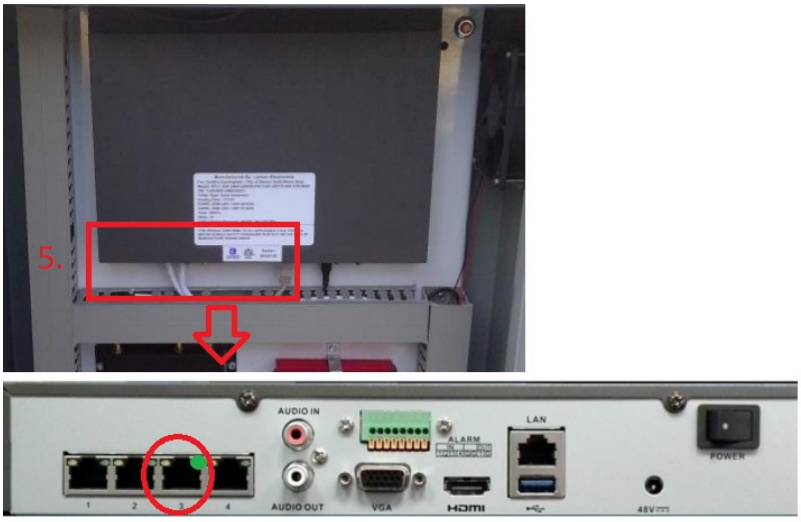
- Locate the following circuit board — the green light should be on.



- Locate the router and ensure the following status lights are on:
  - Status
  - Cellular
  - LAN 1



- Locate the Network Video Recorder and ensure the green lights are on for each camera port.



Following these steps the unit should connect to the network and the user should be able to operate the system again. If problems persist, contact Larson Electronics for further assistance.

MAINTENANCE

Caution: To avoid personal injury, disconnect power to the light and allow the unit to cool down before performing maintenance.

Warning: No user serviceable parts inside of fixture. Risk of electric shock. Removal of the lens will void the warranty.

1. Perform visual, mechanical and electrical inspections on a regular basis. We recommend routine checks to be made on a yearly basis. Frequency of use and environment should determine this. It is recommended to follow an Electrical Preventive Maintenance Program as described in NFPA 70B: Recommended practice for Electrical Equipment.
2. The lens should be cleaned periodically as needed to ensure continued photometric performance. Clean the lens with a damp, non-abrasive, lint-free cloth. If not sufficient, use mild soap or a liquid cleaner.
3. Inspect the cooling fins on the luminaire to ensure that they are free of any obstructions or contamination (i.e. excessive dust build-up). Clean with a non-abrasive cloth if needed.
4. Do not operate if the lens is cracked or damaged. All fasteners should be properly seated.

USE AND CARE

Unauthorized modification may impair the function and/or safety of this device and could affect the life of the equipment. Always check for damaged or worn out parts before using the device. Store it in a secure place out of the reach of children when not in use. Inspect for good working condition prior to storage and before re-use.

REPLACEMENT PARTS

The SPLT-.53K-LM45-2XN3B-PW-TLR7-2XPTZ-20X-2TB-W4G is designed to provide years of reliable performance. Should the need for replacement parts arise, please contact Larson Electronics.

THESE INSTRUCTIONS MAY NOT COVER ALL DETAILS OR VARIATIONS OF THIS PRODUCT FOR YOUR EQUIPMENT OR INSTALLATION REQUIREMENTS. SHOULD FURTHER INFORMATION NOT COVERED BY THESE INSTRUCTIONS BE REQUIRED, PLEASE CONTACT LARSON ELECTRONICS BY EMAIL AT SALES@LARSONELECTRONICS.COM OR BY PHONE AT 1-800-369-6671 FOR FURTHER ASSISTANCE.

PLEASE VISIT LARSONELECTRONICS.COM FOR **WARRANTY** AND **RETURN** INFORMATION.