25' Telescoping Mobile Security Tower
6 kW Diesel Gen - (4) LED Lamps, (4) Cameras, 2TB NVR, Router/WAP - Receptacles
Instruction Manual

Thank you for your purchase of the Larson Electronics WCDE-4-4X2MP-PTZ-4X150LTL-LED-2TB-AP-W4G.

WARNING:

READ CAREFULLY BEFORE INSTALLING FIXTURE. RETAIN THESE INSTRUCTIONS FOR FUTURE REFERENCE. CRITICAL SAFETY INSTRUCTIONS:

- INSTALLATION SHOULD ONLY BE CONDUCTED BY A QUALIFIED ELECTRICIAN IN ACCORDANCE WITH NEC AND ANY RELEVANT LOCAL BUILDING CODES.
- RISK OF FIRE OR ELECTRIC SHOCK. FIXTURE INSTALLATION REQUIRES KNOWLEDGE OF FIXTURE'S ELECTRICAL SYSTEMS. IF NOT QUALIFIED, CONTACT A QUALIFIED ELECTRICIAN.
- BE CERTAIN ELECTRICAL POWER IS OFF BEFORE AND DURING INSTALLATION AND MAINTENANCE.
- MAKE SURE THE SUPPLY VOLTAGE IS THE SAME AS THE FIXTURE'S RATED VOLTAGE.
- TO PREVENT WIRING DAMAGE OR ABRASION, DO NOT EXPOSE WIRING TO EDGES OF SHEET METAL OR SHARP OBJECTS. SUITABLE FOR DAMP LOCATIONS.

IMPORTANT

READ CAREFULLY BEFORE INSTALLING THIS FIXTURE. SAVE THESE INSTRUCTIONS FOR FUTURE REFERENCE. THE WCDE-4-4X2MP-PTZ-4X150LTL-LED-2TB-AP-W4G MUST BE WIRED IN ACCORDANCE WITH NATIONAL ELECTRICAL CODE AND ALL APPLICABLE LOCAL CODES. PROPER GROUNDING IS REQUIRED FOR SAFETY.

WE STRONGLY ENCOURAGE ONLY A LICENSED ELECTRICIAN INSTALL, OPERATE AND MAINTAIN THIS PRODUCT. IF YOU ARE NOT QUALIFIED OR UNFAMILIAR WITH ANY ASPECT OF THIS INSTRUCTION SHEET, CONSULT AN ELECTRICIAN. THERE ARE NO SERVICEABLE PARTS INSIDE.

WARNING: MAKE SURE POWER IS TURNED **OFF** BEFORE STARTING THE INSTALLATION OR PERFORMING ANY MAINTENANCE.

RISK OF FIRE/ELECTRIC SHOCK – DISCONNECT POWER AT BREAKER BEFORE INSTALLING OR SERVICING.
RISK OF PERSONAL INJURY – FIXTURE MAY BECOME UNSTABLE OR DAMAGED IF NOT INSTALLED PROPERLY.
RISK OF BURN – ALLOW FIXTURE TO COOL BEFORE SERVICING.

WARNING:

USER SHOULD BE TRAINED IN THE PROPER USE AND MAINTENANCE OF THIS DEVICE. THIS LINE CORD IS INTENDED TO ALLOW OPERATORS TO EXTEND POWER TO EQUIPMENT WHEN STATIONARY OUTLETS ARE NOT READILY AVAILABLE.

IMPROPER USE OF THIS CORD, PLUG, AND RECEPTACLE CAN LEAD TO SERIOUS INJURIES OR DEATH TO PERSONNEL.

PERIODIC INSPECTION OF THE CORD IS NECESSARY.

THE CORD MUST BE ROUTINELY CHECKED FOR CUTS, BREAKS, OR ANY SEVERE ABRASIONS, AND IF ANY ARE FOUND, THE CORD MUST BE REPLACED BEFORE RESUMING USE.

The WCDE-4-4X2MP-PTZ-4X150LTL-LED-2TB-AP-W4G Telescoping Mobile Security Tower from Larson Electronics is a fully standalone security surveillance package with remote monitoring, powered by a water cooled diesel engine turning a single bearing 6,000 watt generator. There are four, PTZ day/night IP cameras mounted on this unit, supported by a 2TB NVR at the base of the tower, four LED flood lights producing 81,000 lumens of intense light, an unlocked professional grade router with an external antenna and wireless access point. The entire system can run continuously for 120+ hours on a full tank of fuel.

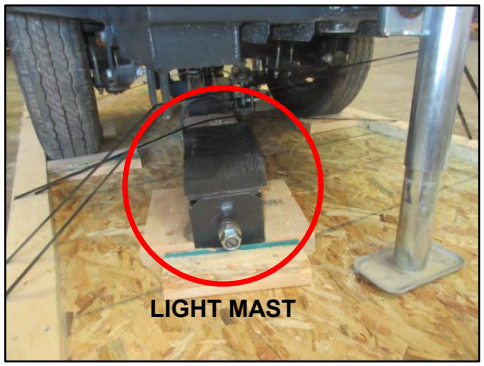
MAST INSTALLATION

Telescoping Mobile Light Tower
Part# WCDE SERIES

This mobile light tower ships with the light head, mast, and winch handle removed to prevent damage during transport. Follow the steps below for installing these parts.

1. Place light tower in an area accessible by forklift or similar lifting device. Remove shipping wrap and straps holding light mast to bottom pallet. Slide light mast out from underneath and set aside.





2. Cut straps and remove the light head from top of light tower and set aside. **<u>WARNING:</u> THERE IS A POWER CABLE ATTACHING THE LIGHT HEAD TO THE TRAILER. DO NOT OVER EXTEND CABLE.**



At this point it is safe to cut any additional straps.

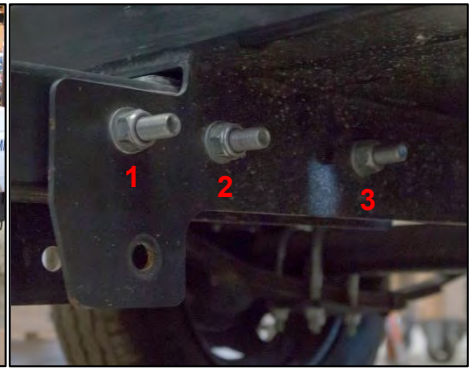
3. Move the tongue down to its tow position. There are 3 bolts near the base of the tongue. Only remove the top(1) and bottom(3) bolts.



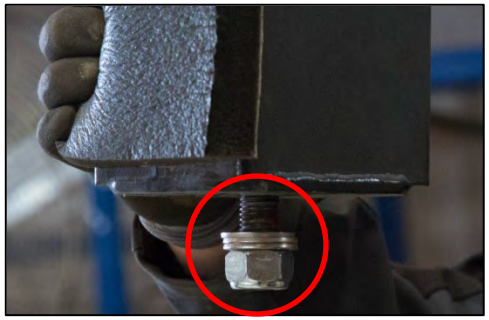
Bolt: 13/16”
Nut: 7/8”

4. Loosen the center bolt and pivot the tongue downward until horizontal with the trailer. Align the holes and replace the 2 bolts removed earlier. Tighten all bolts to secure tongue.

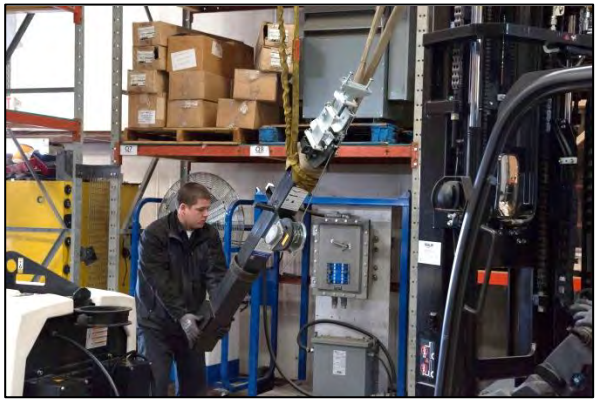




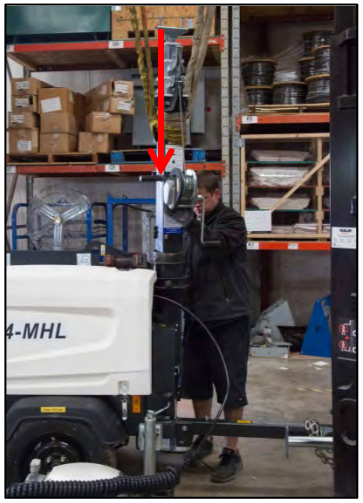
5. Locate light mast and remove bottom nut and 3 washers. Set these aside as they will be used to secure the light mast to trailer.



6. Use a pair of slings to lift and install light mast to trailer. Take appropriate safety precautions when maneuvering equipment on lift.



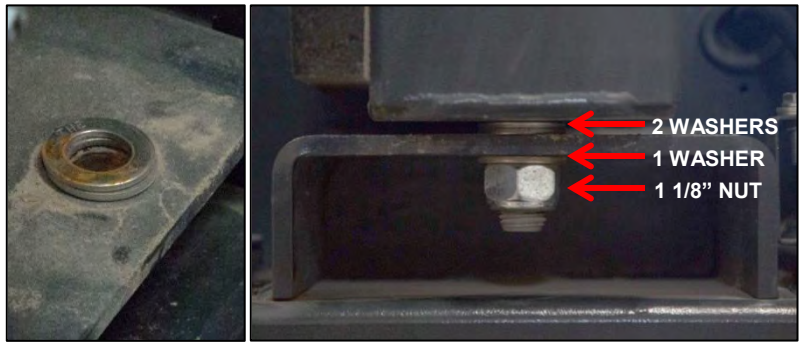
7. Align the mast through the center collar toward the front of the trailer (side with tongue). Be careful not to tear the foam piece while installing light mast. This foam heat shield should face toward the vents on the trailer.



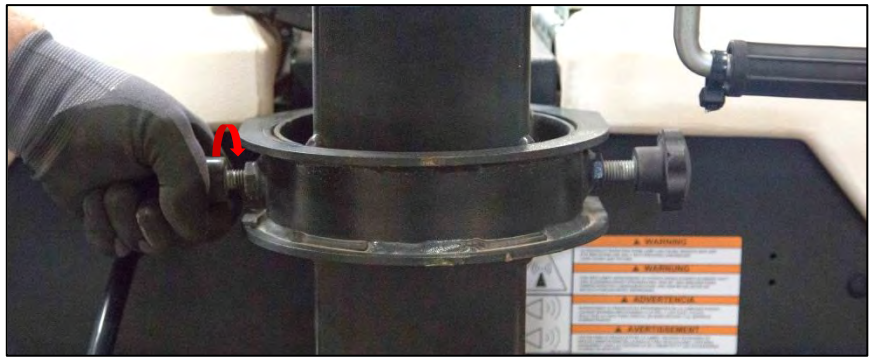


HAND SCREW

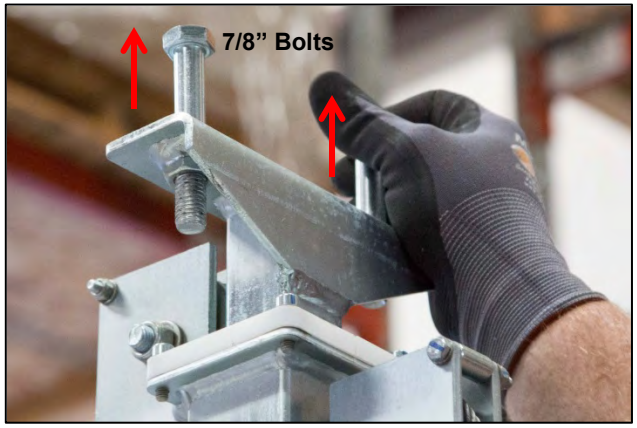
8. Make sure the hand screws of the rotating collar are loosened all the way to allow the light mast to be fully seated.
9. Before inserting bolt of light mast to base, place 2 washers first. Then, slide mast and bolt down all the way. Install last washer and nut to other side and tighten. See reference photos.



10. Next, align the mast center and tighten hand screws for rotating collar. This locks mast in place and will prevent it from rotating while installing light head.



11. Remove the 2 bolts and 2 washers on top of mast for installing the light head.



INSTALLING LIGHT HEAD

1. Locate the light head. Make sure it is able to be removed from the pallet.



2. Using a pair of slings, wrap both slings around the light head in between the lights on both sides.



3. Attach the slings to a forklift or similar lifting device.

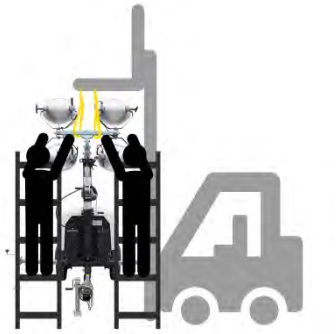


4. With 2 people holding the light head steady, slowly raise the light head above the mast.



5. A ladder will need to be placed on both sides of the mast, in order for 2 people to guide the head in to place.

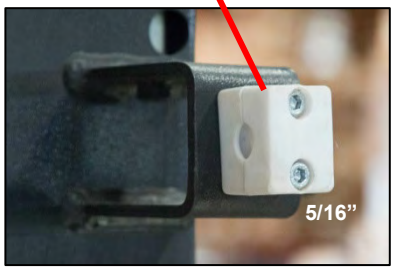
LIGHT HEAD SHOWN MAY VARY



6. Once the light head is on top of the light mast, replace the two bolts, washers, and tighten. Ensure the light head is safely secured to the top of the mast before releasing slack from slings.



7. Using a 5/16” allen wrench, open the cable clamp and place light tower cable inside. See reference photos. Once installed, replace top cover and tighten screws.





8. Repeat this process in reverse order for removing the light head.

INSTALLING WINCH HANDLE

1. The winch handle is located near the winch. It is strapped to the mast for transport. Cut the strap to free the winch handle from the mast.



2. Install winch handle to winch by aligning the two set holes with the screws on the handle. Press the handle into bolt and tighten set screws.







5/16" Socket Screws

Remove trailer from pallet and light tower is ready for deployment.



Proceed to the **OPERATION MANUAL** for operating the unit.

LARSON ELECTRONICS

9419 US-HWY 175
Kemp, TX 75143 USA
P: 800-369-6671 | INTL: 903-498-3363 F: 903-498-3364
sales@larsonelectronics.com
www.larsonelectronics.com

Operator's Manual

Serial Number Range

WCDE-4 SERIES

ANSI/CSA
North America
South America
Asia

with
Maintenance
Information

Important

Read, understand and obey these safety rules and operating instructions before operating this machine. Only trained and authorized personnel shall be permitted to operate this machine. This manual should be considered a permanent part of your machine and should remain with the machine at all times. If you have any questions, contact us.

Contact Us:

Internet: www.larsonelectronics.com

E-mail: sales@larsonelectronics.com

Contents

Introduction 8
Symbol and Hazard Pictorials Definitions 10
General Safety 12
Work Area Safety 16
Legend 21
Controls 23
Inspections 25
Operating Instructions 31
Transport and Lifting Instructions 37
Maintenance 39
Specifications 41
Reporting Safety Defects 43

These machines comply with
ANSI/SIA A92.5
CAN B.354.4

Introduction

Owners, Users and Operators:

Thank you for choosing our machine for your application. Our number one priority is user safety, which is best achieved by our joint efforts. We feel that you make a major contribution to safety if you, as the equipment users and operators:

1 **Comply** with employer, job site and governmental rules.

2 **Read, understand and follow** the instructions in this and other manuals supplied with this machine.

3 **Use good safe work practices** in a commonsense way.

4 **Only have trained/certified operators**, directed by informed and knowledgeable supervision, running the machine.



Danger

Failure to obey the instructions and safety rules in this manual will result in death or serious injury.

Do Not Operate Unless:

☑ You learn and practice the principles of safe machine operation contained in this operator's manual.

1 Avoid hazardous situations.

Know and understand the safety rules before going on to the next section.

2 Always perform a pre-operation inspection.

3 Always perform function tests prior to use.

4 Inspect the workplace.

5 Only use the machine as it was intended.

☑ You read, understand and obey the manufacturer's instructions and safety rules—safety and operator's manuals and machine decals.

☑ You read, understand and obey employer's safety rules and worksite regulations.

☑ You read, understand and obey all applicable governmental regulations.

☑ You are properly trained to safely operate the machine.

Introduction

Hazard Classification

Decals on this machine use symbols, color coding and signal words to identify the following:



Safety alert symbol—used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER Indicates a hazardous situation which, if not avoided, will result in death or serious injury.

⚠ WARNING Indicates a hazardous situation which, if not avoided, could result in death or serious injury.

⚠ CAUTION Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

NOTICE Indicates a property damage message.

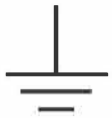
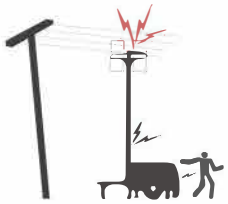
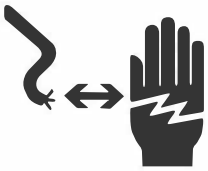
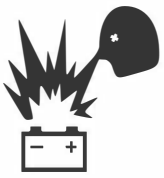
Intended Use

This machine is intended to be used only to provide lighting and electrical power to a work site.

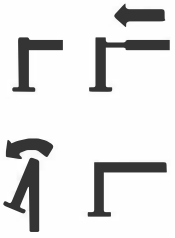
Safety Sign Maintenance

Replace any missing or damaged safety signs. Keep operator safety in mind at all times. Use mild soap and water to clean safety signs. Do not use solvent-based cleaners because they may damage the safety sign material.

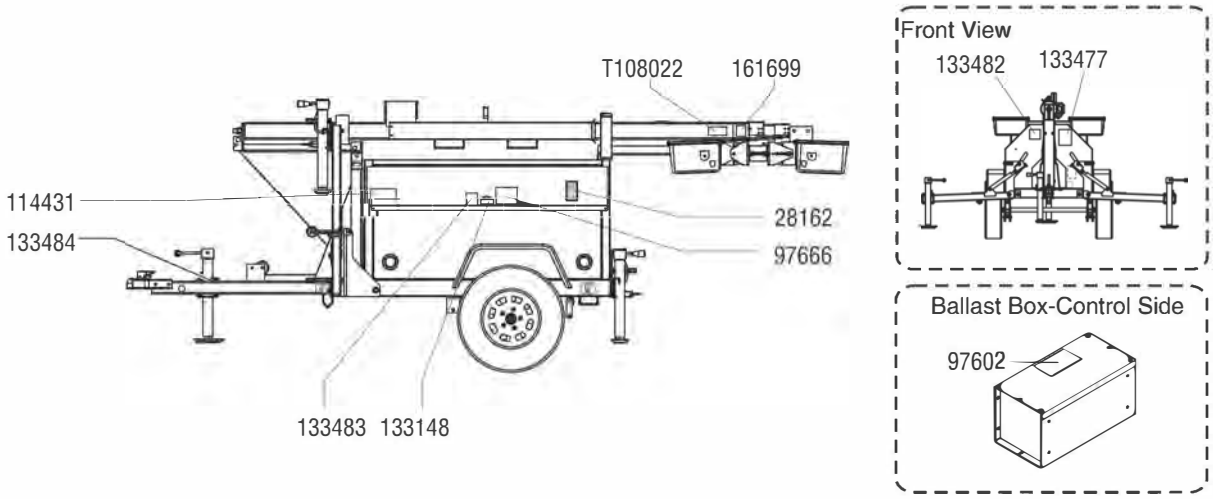
Symbol and Hazard Pictorials Definitions

 Read the operator's manual	 Electrocution hazard	 Stop engine	 Earth ground	 Electrocution hazard
 Maintain required clearance	 Explosion / Burn hazard	 Disconnect battery Read the service manual	 Crush hazard	 Keep away from moving parts
 Keep away from moving parts	 Stay clear of belts and fan	 Burn hazard	 Explosion / Burn hazard	 Corrosive acid.
 Explosion hazard	 Do not use ether or other high energy starting aids on machines equipped with glow plugs	 No smoking	 No flame	 No flame

Symbol and Hazard Pictorials Definitions

 Burn hazard	 Burn hazard	 Burn hazard	 Stay clear of hot exhaust	 Stay clear of hot exhaust
 Burn hazard, hot components	 Stay clear of hot surfaces under cover	 Carbon Monoxide hazard	 Wear protective clothing	 Shattering glass hazard
 Crushing hazard	 Stay clear of descending mast	 Tip-over hazard	 Deploy outriggers before raising mast	 Tip-over hazard, tow speed
 Lifting point	 Tie-down point			

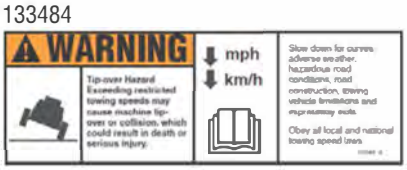
General Safety



133477



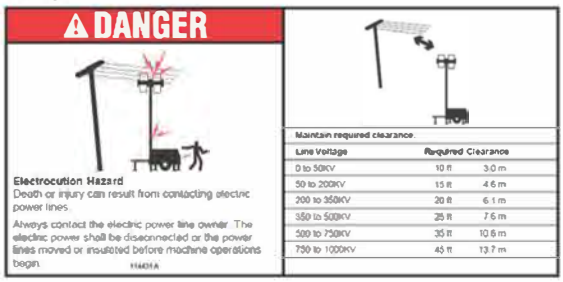
133484



161699



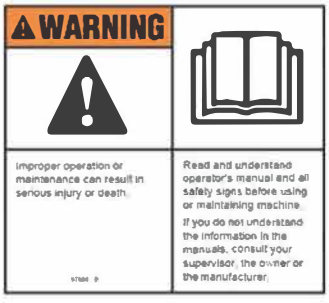
114431



28162



97666



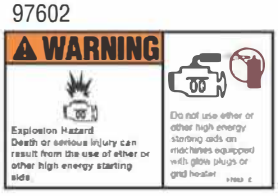
133483



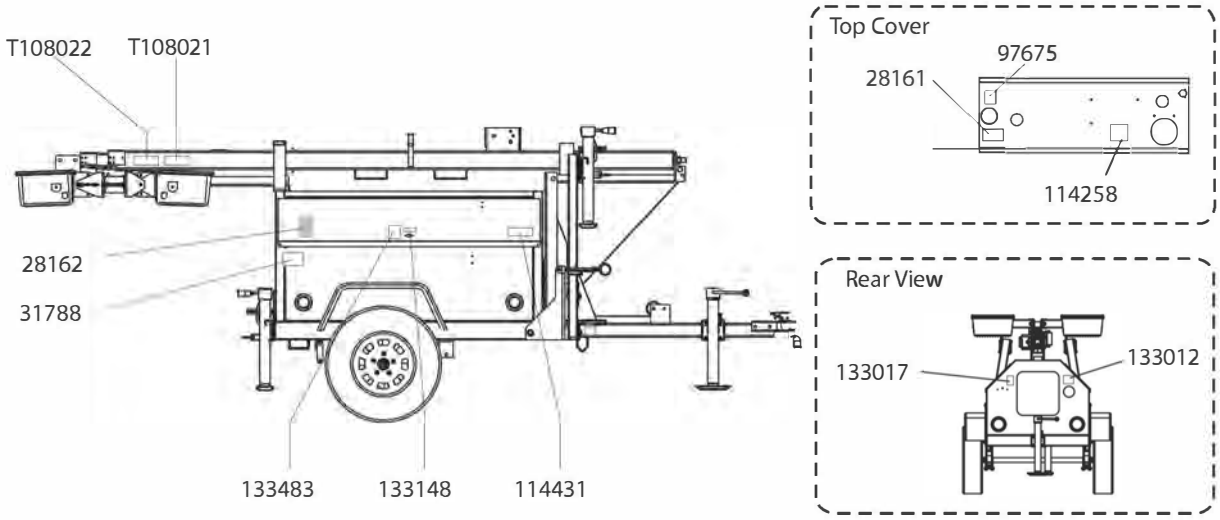
133482



97602



General Safety



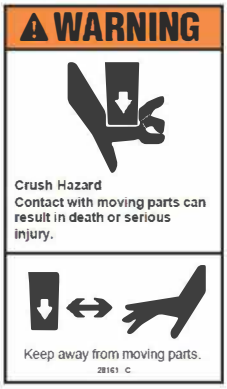
T108022



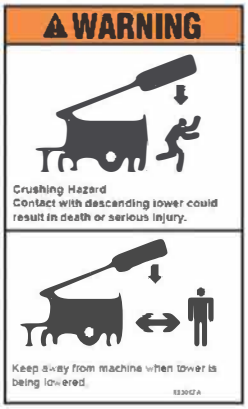
T108021



28161



133017



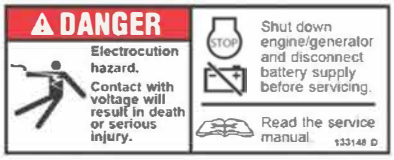
97675



114258



133148



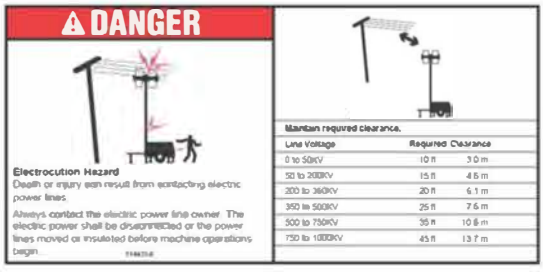
31788



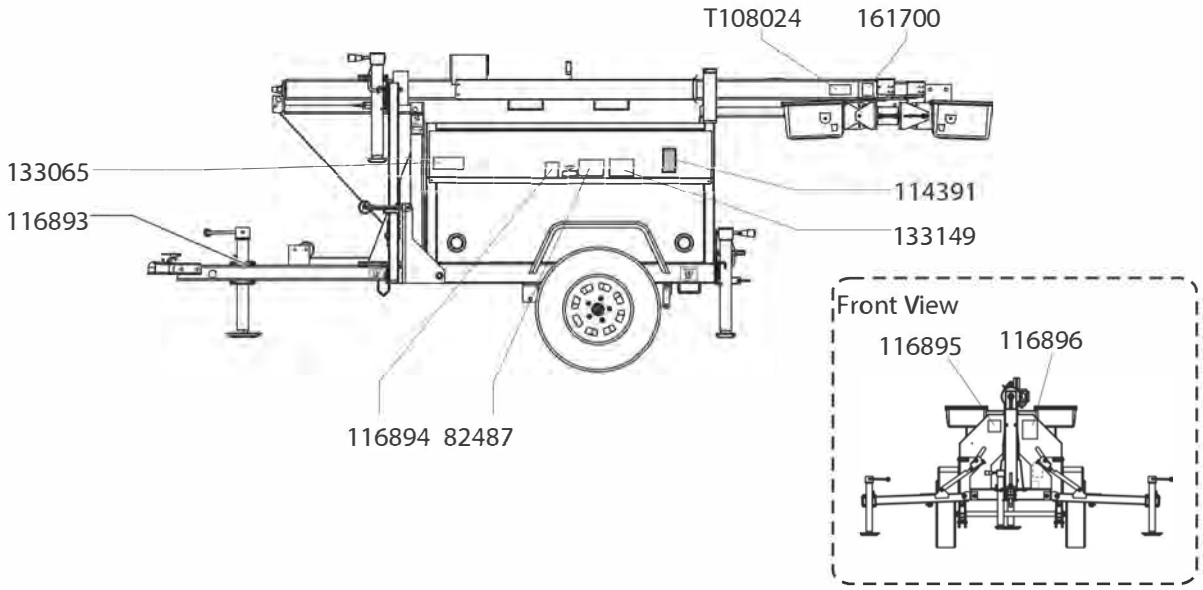
133012



114431



General Safety



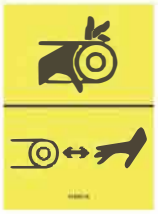
T108024



161700



114391



133149



116895



116896



82487



116894



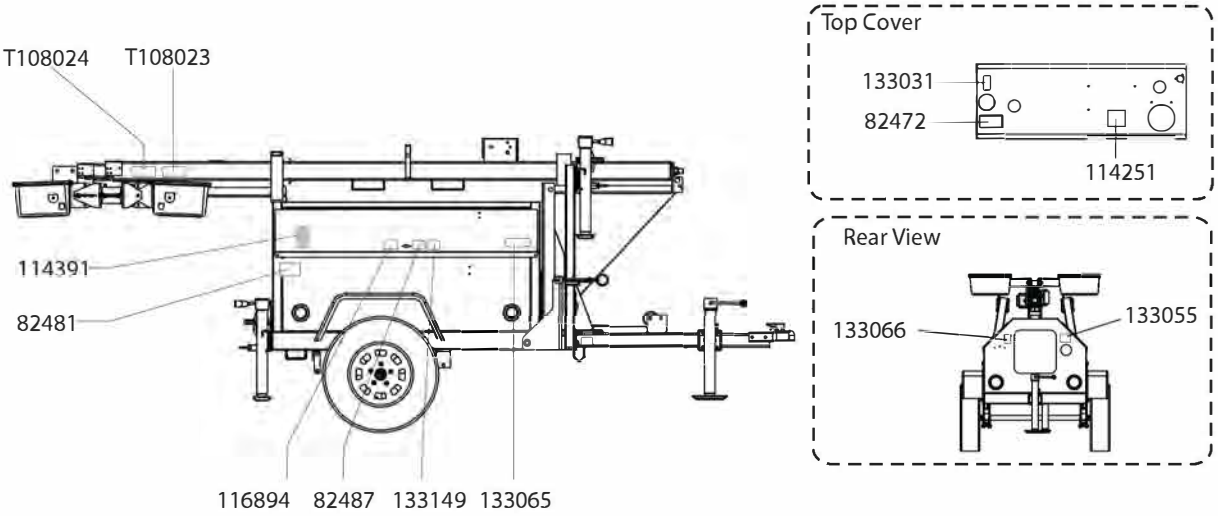
116893



133065



General Safety



114251



T108023



116894



133149



82472



T108024



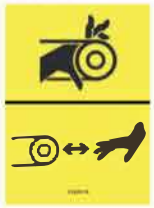
133066



133055



114391



82487



133065



133031



82481



Work Area Safety

⚠ Electrocution Hazards

This machine is not electrically insulated and will not provide protection from contact with or proximity to electrical current.

Obey all local and governmental regulations regarding required clearance from electrical power lines. At a minimum, the required clearance contained in the chart below must be followed.

Line Voltage	Required Clearance	
0 to 50KV	10 ft	3.05 m
50 to 200KV	15 ft	4.60 m
200 to 350KV	20 ft	6.10 m
350 to 500KV	25 ft	7.62 m
500 to 750KV	35 ft	10.67 m
750 to 1000KV	45 ft	13.72 m

Allow for mast movement, electrical line sway or sag, and beware of strong or gusty winds.

Do not operate the machine during lightning or storms.

Do not use the machine as a ground for welding.



Keep away from the machine if it contacts energized power lines. Personnel must not touch or operate the machine until energized power lines are shut off.

Do not connect wires directly to the generator. Connect auxiliary equipment only to the power outlets provided.

Do not perform service or replace the lamps with the engine/generator running or batteries connected.

This machine should be grounded in accordance with all local electrical codes. Consult the local electrical codes or authority having jurisdiction in the area where the machine will be used for specific requirements.

There is a permanent conductor between the generator (static winding) and the frame.

⚠ Explosion and Fire Hazards

Do not start the engine if you smell or detect liquid petroleum gas (LPG), gasoline, diesel fuel or other explosive substances.



Do not refuel the machine with the engine running.

Do not refuel the machine while it is hot. Allow to cool for several minutes before refueling.

Do not spill fuel inside the engine compartment.

Refuel the machine and charge the battery only in an open, well-ventilated area away from sparks, flames and lighted tobacco.

Do not operate the machine in hazardous locations or locations where potentially flammable or explosive gases or particles may be present.



Do not spray ether into engines equipped with glow plugs.

Work Area Safety

⚠ Tip-over Hazards



Do not raise the mast unless all outriggers are properly deployed, the foot pads are in firm contact with the ground and the machine is level.

Do not set the machine up on a surface where it cannot be leveled using only the leveling jacks.

Do not hang objects from the lights or the mast.

Do not use the mast to raise material or personnel.

Do not move the machine unless the mast is lowered to the horizontal position.



Do not raise the mast when wind speeds may exceed 62 mph / 100 km/h. Do not alter or disable machine components that in any way affect safety and stability.

Do not alter or disable machine components that in any way affect safety and stability.

Do not adjust or stow the outriggers when the mast is raised.

Be sure the tires are in good condition and the lug nuts tightened.



Do not place ladders or scaffolds against any part of the machine.

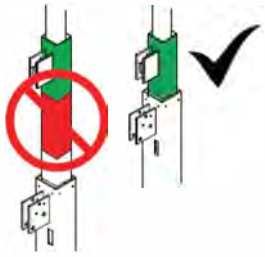
Do not use the machine on a moving or mobile surface or vehicle.

⚠ Crushing Hazard



Do not lower the mast unless the area below is clear of personnel and obstructions.

Keep hands and fingers away from any potential pinch points.



Do not lower the mast until the mast is retracted and the upper retaining bar is locked into the mast. No red should be visible on the mast.

⚠ Collision Hazards

Check the work area for overhead obstructions or other possible hazards.

⚠ Burn Hazards



Do not touch the lamp fixtures while they are turned on. Turn the lamps off and allow them to cool before touching.

Do not touch hot parts of the engine or tailpipe, Use protective gloves when handling hot parts.

⚠ Bodily Injury Hazard

Do not use the machine indoors unless properly ventilated.

Do not breathe exhaust fumes.

Work Area Safety

Do not work on this equipment when mentally or physically fatigued.

Do not work on this equipment when under the influence of drugs or alcohol.

Stay clear of belts and fan when engine is running.

Do not use the machine if the protective barrier on any of the lamps is broken or punctured. Metal halide lamps produce shortwave ultra-violet radiation and can cause serious skin burns or eye inflammation if the protective barrier is not in place.

Do not use where people will remain close to the lamps for more than a few minutes unless adequate shielding or other safety precautions are used.

Stay clear of moving mast.

Do not grasp the cable.

Use proper lifting techniques when lifting and positioning the tongue of the machine.

Always replace the protective lamp cover after replacing the lamp bulbs.

⚠ Fall Hazards

Do not climb or stand on any part of the light tower.

⚠ Traffic Hazards

Stand clear of traffic when starting or checking the unit along the road.

⚠ Damaged Machine Hazards

Do not use a damaged or malfunctioning machine.

Do not use a machine with a worn, frayed, kinked or damaged cable.

Conduct a thorough pre-operation inspection of the machine and test all functions before each work shift. Immediately tag and remove from service a damaged or malfunctioning machine.

Be sure all maintenance has been performed as specified in this manual and the appropriate Larson Electronics service manual.

Be sure the operator's manual is complete, legible and in the storage container located on the machine.

Be sure all decals are in place and legible.

Do not modify or alter the light tower without the prior written permission of the manufacturer.

Work Area Safety

⚠ Component Damage Hazards

Do not turn the lights on unless the engine is running. Always turn the lights off before shutting down the engine.

Do not tow the light tower while the lamps are hot. Hot lamps will break if moved.

Do not replace lamp bulbs with any bulbs other than those specified on the machine and in this manual.

Note: Lamp bulbs contain mercury (Hg). Dispose of lamp bulbs according to local, state and federal laws.

Be sure lamp fixture connections are properly tightened before turning lights on.

⚠ Battery Safety

Burn Hazards



Batteries contain acid. Always wear protective clothing and eye wear when working with batteries.

Avoid spilling or contacting battery acid. Neutralize battery acid spills with baking soda and water.

Do not use any battery charger greater than 12V to charge the battery.

Do not remove the vent caps from the battery when charging.

Do not expose the batteries or the charger to water or rain during charging.

Explosion Hazards



Keep sparks, flames and lighted tobacco away from batteries. Batteries emit explosive gas.

Do not contact the battery terminals or the cable clamps with tools that may cause sparks.

Electrocution/Burn Hazards

Avoid contact with electrical terminals.

Inspect the power cord for damage prior to each use.

Replace any damaged cord before operating.

Do not allow the power cord to become caught or crushed while raising, lowering or rotating the mast.

Avoid electrical shock from contact with battery terminals. Remove all rings, watches and other jewelry.

Lifting Hazard

Use the appropriate number of people and proper lifting techniques when lifting the batteries.

Work Area Safety

⚠ Towing Hazards

Read, understand and obey all of your tow vehicle manufacturer's recommendations, warnings and instructions before towing this machine.

Do not tow the machine unless the mast is retracted and lowered to the horizontal position and the travel lock pin is secured.

Do not tow the machine unless all outriggers have been retracted and stowed.

Do not overload your tow vehicle. Check the manufacturer's Gross Vehicle Weight Rating (GVWR). To obtain the gross vehicle weight, add the tongue weight of the trailer to the vehicle weight (including vehicle, passengers and cargo).

Do not load cargo on the machine. The light tower is not designed to carry any extra cargo.

Be sure the hitch is securely attached to the tow vehicle.

Be sure the safety chains (if required) are securely attached to the tow vehicle.

Be sure that all driving lights are operational.

Be sure all hitch components, lights and mirrors and methods of attaching the trailer to the tow vehicle conform to local, state and federal regulations.

Do not tow the machine on public roads unless it meets all governmental regulations for towing.

Do not exceed 60 mph / 97 km/h. Obey all local and national towing speed laws.

Be sure to chock the wheels when parking on a hill.

Use extreme care and slow speeds while towing across uneven terrain, debris, holes or drop-offs.

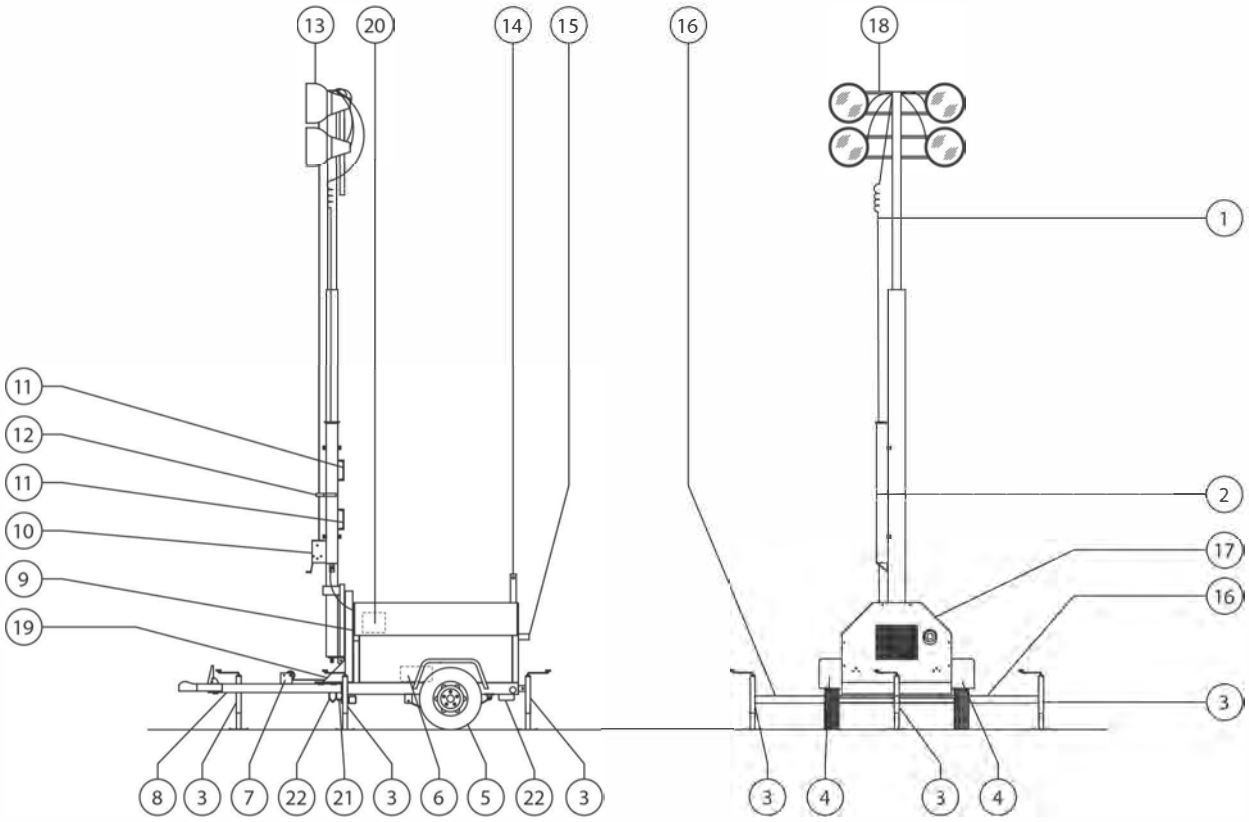
Note: Do not tow machine when engine is running! This can cause severe engine/radiator damage and WILL NOT BE COVERED UNDER WARRANTY!

Lockout After Each Use

When leaving the machine unattended, secure from unauthorized use. Unauthorized personnel may attempt to operate the machine without proper instruction, creating an unsafe condition.

Legend

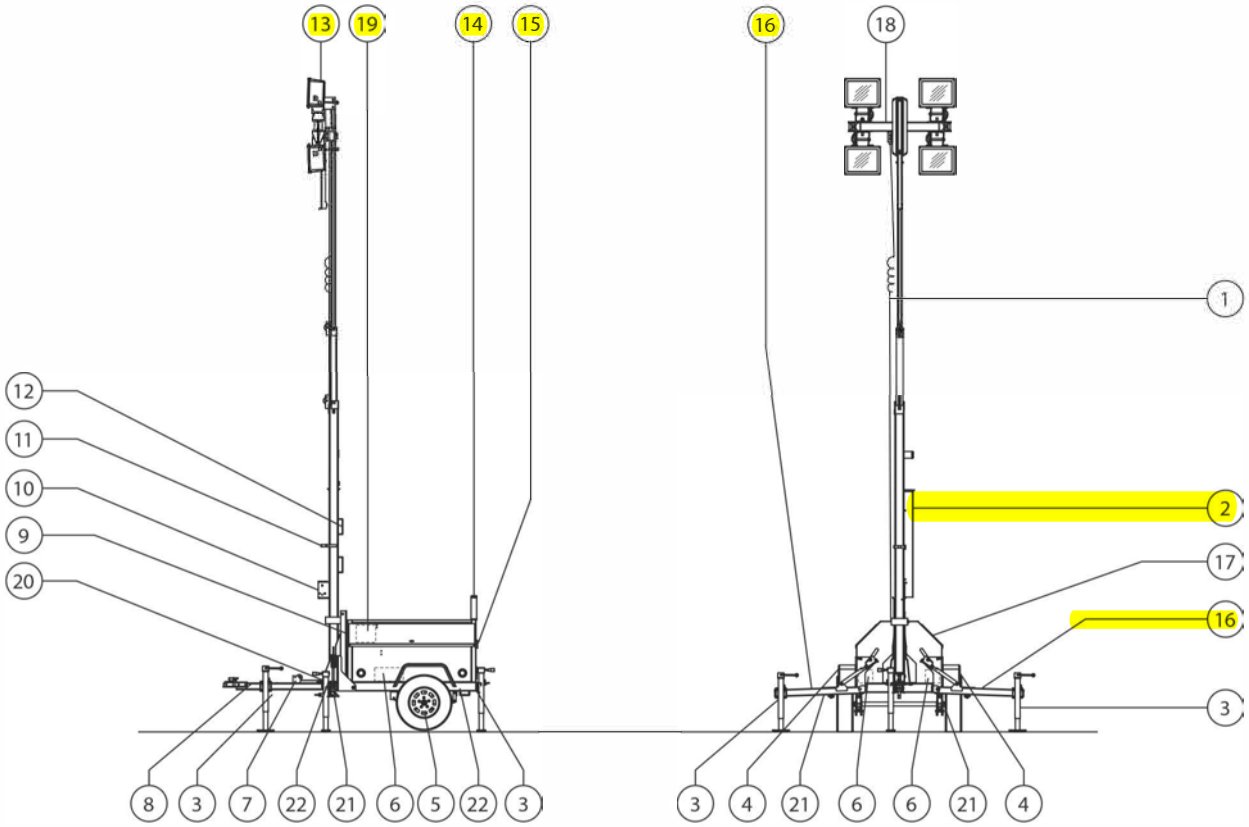
Legend - RL4 & RL4000



1 Coil cord
2 Coil cord sleeve
3 Tongue leveling jack
4 Fender
5 Tire
6 Ballast (located inside cabinet)
7 Raise/lower winch
8 Tongue with trailer hitch
9 Roadside door
10 Extend/retract winch
11 Forklift pockets
12 Lifting eye
13 Lamps
14 Upper retaining bar
15 Muffler
16 Outrigger
17 Curbside door
18 Light bar
19 Lower retaining pin
20 Control panel (located inside cabinet)
21 Spring pin
22 Tie-downs

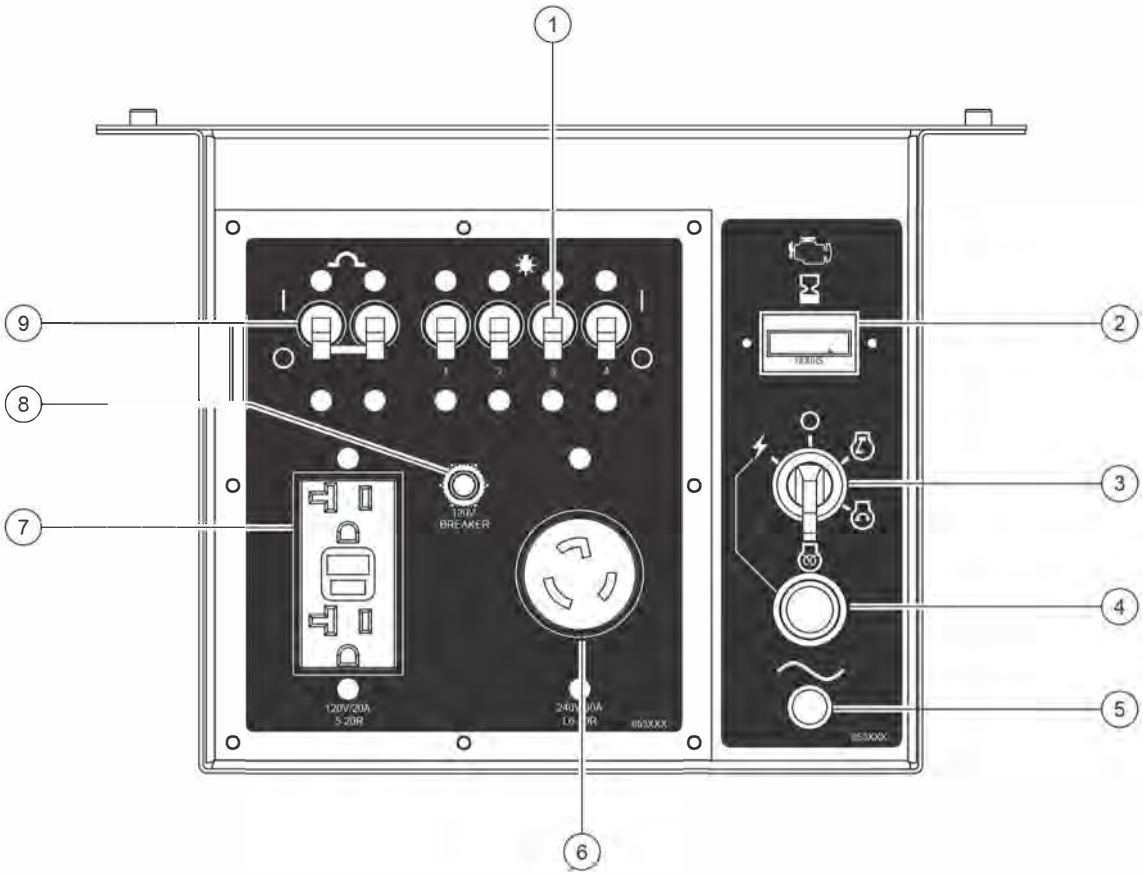
Legend

Legend - TML-4000



1 Coil cord
2 Coil cord sleeve
3 Tongue leveling jack
4 Fender
5 Tire
6 Ballast (located inside cabinet)
7 Raise/lower winch
8 Tongue with trailer hitch
9 Roadside door
10 Extend/retract winch
11 Lifting eye
12 Forklift pockets
13 Lamps
14 Upper retaining bar
15 Muffler
16 Outrigger
17 Curbside door
18 Light bar
19 Control panel (located inside cabinet)
20 Lower retaining pin
21 Outrigger release pin
22 Tie-downs

Controls



Ground Control Panel

1 Light switches
2 Hour meter
3 Ignition switch for engine
4 Engine prime button
5 Alternator failure light
6 T-lock receptacle, 240V/30A
7 Duplex receptacle with GFI, 120V/20A
8 Mini breaker, 120V
9 Main circuit breaker

Controls

Control Panel

1 Light switches

Move each light switch up to turn on the indicated light. Move each light switch down to turn off the indicated light.

2 Hour meter

The hour meter displays the number of hours the machine has operated.

3 Ignition switch for engine

Turn the ignition switch to the prime position and hold the engine prime button down to prime the engine.

Hold the prime button down and turn the ignition switch to the start position to start the engine.

Turn the ignition switch to the off position to turn the engine off.

4 Engine prime button

With the ignition switch in the run position, press and hold the prime button for 15 seconds before starting the engine. Release the prime button when the engine starts.

5 Alternator failure light

Light on indicates that the engine's DC alternator isn't producing enough voltage.

6 T-lock receptacle, 240V/30A

7 Duplex receptacle with GFI, 120V/20A

Convenience duplex receptacle with Ground Fault Interrupter (GFI).

8 Mini breaker, 120V

Pop-out style breaker. Push in button to insure GFI receptacle is ready for use.

9 Main circuit breaker

Move the main circuit breaker switch up on the control panel before turning the individual light switches on or before attempting to use the convenience receptacles.

Inspections



Do Not Operate Unless:

☑ You learn and practice the principles of safe machine operation contained in this operator's manual.

1 Avoid hazardous situations.

2 Always perform a pre-operation inspection.

Know and understand the pre-operation inspection before going on to the next section.

3 Always perform function tests prior to use.

4 Inspect the workplace.

5 Only use the machine as it was intended.

Pre-operation Inspection Fundamentals

It is the responsibility of the operator to perform a pre-operation inspection and routine maintenance.

The pre-operation inspection is a visual inspection performed by the operator prior to each work shift. The inspection is designed to discover if anything is apparently wrong with a machine before the operator performs the function tests.

The pre-operation inspection also serves to determine if routine maintenance procedures are required. Only routine maintenance items specified in this manual may be performed by the operator.

Refer to the list on the next page and check each of the items.

If damage or any unauthorized variation from factory delivered condition is discovered, the machine must be tagged and removed from service.

Repairs to the machine may only be made by a qualified service technician, according to the manufacturer's specifications. After repairs are completed, the operator must perform a pre-operation inspection again before going on to the function tests.

Scheduled maintenance inspections shall be performed by qualified service technicians, according to the manufacturer's specifications and the requirements listed in the responsibilities manual.

Inspections

Pre-operation Inspection

- ❑ Be sure that the operator's manual is complete, legible and in the storage container located on the machine.
- ❑ Be sure that all decals are legible and in place. See Inspections section.
- ❑ Check for engine oil leaks and proper fluid level. Add oil if needed. See Maintenance section.
- ❑ Check for engine coolant leaks and proper coolant level. Add coolant if necessary. See Maintenance section.
- ❑ Check for battery fluid leaks and proper fluid level. Add distilled water if needed. See Maintenance section.
- ❑ Check for proper tire pressure and lug nut torque. Add air to tires if needed. See Maintenance section.

Check the following components or areas for damage, improperly installed or missing parts and unauthorized modifications:

- ❑ Electrical components, wiring and electrical cables
- ❑ Mast components
- ❑ Mast locking pins
- ❑ Latches and pins
- ❑ Tires and wheels
- ❑ Trailer lights and reflectors
- ❑ Outriggers, leveling jacks and foot pads
- ❑ Winch
- ❑ Nuts, bolts and other fasteners
- ❑ Lamp fixtures, connections and bulbs
- ❑ Cable (kinks, frays and abrasions)
- ❑ Safety chains
- ❑ Engine and related components
- ❑ Fuel tanks
- ❑ Generator

Check entire machine for:

- ❑ Cracks in welds or structural components
- ❑ Dents or damage to machine
- ❑ Excessive rust, corrosion or oxidation

- ❑ Be sure that all structural and other critical components are present and all associated fasteners and pins are in place and properly tightened.
- ❑ Be sure the that the battery is in place and properly connected.
- ❑ After you complete your inspection, be sure that all compartment covers are in place and latched.

Inspections



Do Not Operate Unless:

☑ You learn and practice the principles of safe machine operation contained in this operator's manual.

1 Avoid hazardous situations.

2 Always perform a pre-operation inspection.

3 Always perform function tests prior to use.

Know and understand the function tests before going on to the next section.

4 Inspect the workplace.

5 Only use the machine as it was intended.

Function Test Fundamentals

The function tests are designed to discover any malfunctions before the machine is put into service. The operator must follow the step-by-step instructions to test all machine functions.

A malfunctioning machine must never be used. If malfunctions are discovered, the machine must be tagged and removed from service. Repairs to the machine may only be made by a qualified service technician, according to the manufacturer's specifications.

After repairs are completed, the operator must perform a pre-operation inspection and function tests again before putting the machine into service.

Inspections

Function Tests

Setup

1 Position the light tower at the desired work site.

2 Chock the wheels.

3 Disconnect the trailer lights and the safety chains.

4 Open the latch on the trailer hitch.

5 Pull the release pin on the tongue jack and rotate into place.

6 Turn the leveling jack handle to lower the front outrigger foot pad and raise the tongue of the machine enough to clear the tow vehicle.

7 Release the spring pin on the side outriggers and slide them out into the deployed position. Make sure the outriggers are locked in place. Rotate the leveling jack into position.

Pull the release pin on the side outriggers and lower them to the ground. Rotate the leveling jack into position.

Note: the outriggers are not designed to lift the tires of the unit off the ground.

8 Turn the leveling jack handles to level the machine. Level the machine using only the leveling jacks

Note: the outriggers are not designed to lift the tires of the unit off the ground.

9 Check the bubble level (if equipped) on the front of the machine to make sure the machine is level.

Note: This machine should be grounded in accordance with all local electrical codes. Consult the local electrical codes or authority having jurisdiction in the area where the machine will be used for specific requirements.

Test Machine Functions

By raising and extending, then retracting and lowering the mast back to the horizontal position, the following functions will be tested: **winches, latches, mast extension and mast rotation.**

10 Remove the cotter pin and the upper retaining pin from the top of the mast.

11 Turn the raise/lower winch handle clockwise until the mast raises approximately 2 feet / 60 cm.

⊙ Result: A clicking sound should be heard as the mast raises.

12 Release the winch handle.

⊙ Result: The winch brake should hold the mast.

13 Continue to turn the winch handle clockwise until the lower retaining bar locks into the mast.

⊙ Result: The mast sections should raise smoothly, free of hesitation or binding.

14 Insert the lower retaining pin through mast supports. Insert the cotter pin through retaining pin.

Inspections

15 Turn the extend/retract winch handle clockwise until the mast extends approximately 2 feet / 60 cm.

⊙ Result: A clicking sound should be heard as the winch handle is turned.

16 Release the winch handle.

⊙ Result: The winch brake should hold the mast.

17 Continue to turn the winch handle clockwise until the mast reaches full vertical position.

⊙ Result: The mast sections should extend smoothly, free of hesitation or binding.

18 Turn the T-handle to release the mast rotation lock.

19 Rotate the mast clockwise and then counterclockwise as far as it will go in either direction.

⊙ Result: The mast should rotate smoothly and easily in both directions.

20 Rotate the mast to line up the arrows on the front of the mast.

21 Tighten the T-handle to secure the mast.

22 Attempt to rotate the mast in both directions.

⊙ Result: The mast should not rotate.

23 Turn the extend/retract winch handle counterclockwise until the mast sections are fully retracted.

⊙ Result: No clicking sound should be heard when the winch handle is turned.

24 Remove the cotter pin and lower retaining pin.

25 Begin lowering the mast to the horizontal position by turning the raise/lower winch handle counterclockwise.

⊙ Result: No clicking sound should be heard when the winch handle is turned.

26 Turn the winch handle counterclockwise until the mast is lowered into the travel lock.

27 Insert the lower retaining pin into the mast support and install the cotter pin to secure.

Test the Lights

28 Make sure the circuit breakers and the light switches are in the off position.

Note: Be sure the lamp fixture connections are properly tightened before turning the lights on.

29 Start the engine. See Starting the Engine in the Operating Instructions section.

30 Turn the main circuit breakers to the on position.

31 Turn the light switches to the on position.

⊙ Result: The lights should come on.

Note: It can take up to 20 minutes for the lights to reach full intensity. If the lights are turned off and turned back on while they are still warm, they will not light up again for 20-30 minutes.

Note: Make sure the circuit breaker and the light switches are turned off before shutting down the engine.

Inspections



Do Not Operate Unless:

☑ You learn and practice the principles of safe machine operation contained in this operator's manual.

1 Avoid hazardous situations.

2 Always perform a pre-operation inspection.

3 Always perform function tests prior to use.

4 Inspect the workplace.

Know and understand the workplace inspection before going on to the next section.

5 Only use the machine as it was intended.

Workplace Inspection Fundamentals

The workplace inspection helps the operator determine if the workplace is suitable for safe machine operation. It should be performed by the operator prior to moving the machine to the workplace.

It is the operator's responsibility to read and remember the workplace hazards, then watch for and avoid them while moving, setting up and operating the machine.

Workplace Inspection Checklist

Be aware of and avoid the following hazardous situations:

- ❑ drop-offs or holes
- ❑ bumps, floor obstructions or debris
- ❑ sloped surfaces
- ❑ unstable or slippery surfaces
- ❑ overhead obstructions and high voltage conductors
- ❑ hazardous locations
- ❑ inadequate surface support to withstand all load forces imposed by the machine
- ❑ wind and weather conditions
- ❑ the presence of unauthorized personnel
- ❑ other possible unsafe conditions

Operating Instructions



Do Not Operate Unless:

☑ You learn and practice the principles of safe machine operation contained in this operator's manual.

1 Avoid hazardous situations.

2 Always perform a pre-operation inspection.

3 Always perform function tests prior to use.

4 Inspect the workplace.

5 Only use the machine as it was intended.

Fundamentals

The Operating Instructions section provides instructions for each aspect of machine operation. It is the operator's responsibility to follow all the safety rules and instructions in the operator's, safety and responsibilities manuals.

Only trained and authorized personnel should be permitted to operate a machine. If more than one operator is expected to use a machine at different times in the same work shift, they must all be qualified operators and are all expected to follow all safety rules and instructions in the operator's, safety and responsibilities manuals. That means every new operator should perform a pre-operation inspection, function tests, and a workplace inspection before using the machine.

Operating Instructions

Setup

Make sure the machine is set up according to the Setup procedure in the Function Test section.

Starting the Engine

Note: The main circuit breaker and the light switches must be off before starting the engine.

Note: There must be fuel in the fuel tank in order to start the engine.

Note: If the machine is equipped with dual fuel tanks, there must be fuel in both tanks in order to start the engine.

Engine Start

1 Move the ignition switch to the prime position.

2 Press and hold the prime button for 7 seconds.

3 Move the ignition switch to the run position.

4 Press and hold the prime button for 15 seconds.

Note: Never preheat the engine for more than 30 seconds. Damage may be done to the glow plugs.

5 While holding down the prime button, move the ignition switch to engine start position.

Note: To avoid damage, never operate the starter for more than 45 seconds when starting the engine.

Engine Shutdown

1 Turn the lights off using the individual light switches.

Note: After being turned off, the lights must be allowed to cool down before turning them on again. This cool down period can take between 10 and 25 minutes depending on the ambient temperature.

2 Allow the engine to run for 1 to 5 minutes under no load.

Note: Never shut the engine down while under load. This can damage the AC generator.

3 Turn the ignition switch to the engine off position.

Operating Instructions

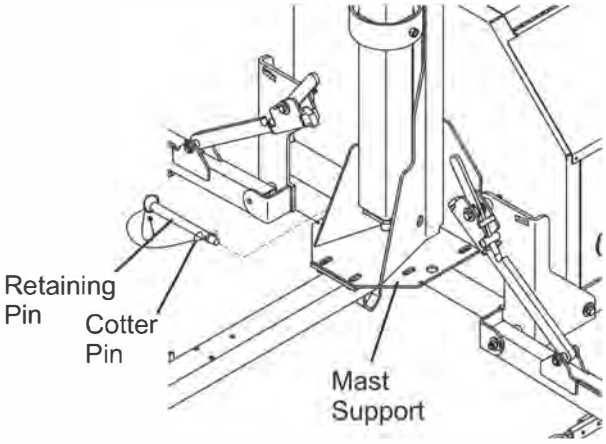
Operation of Tower

1 Remove the cotter pin and the upper retaining pin from the top of the mast.

2 Remove the cotter pin and the retaining pin from the mast support.

3 Turn the raise/lower winch handle clockwise until the mast reaches vertical position.

4 Insert the lower retaining pin through the mast supports. Insert the cotter pin through the retaining pin.



5 Turn the extend/retract winch handle clockwise to extend mast sections.

Mast Rotation

1 Turn the T-handle to release the mast rotation lock.

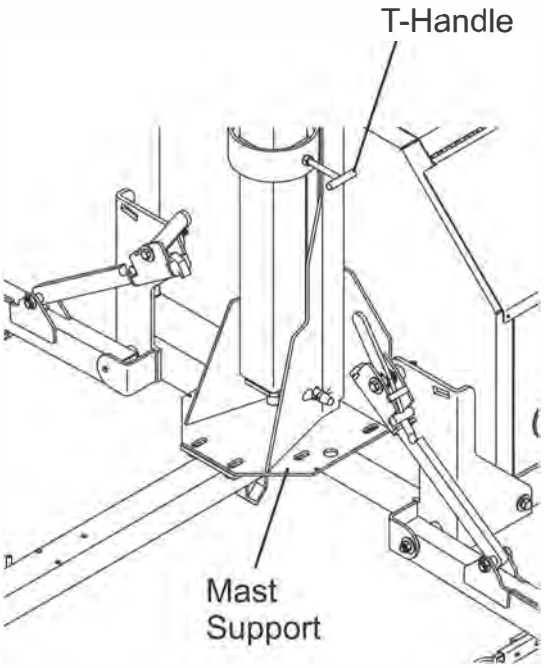
2 Rotate the mast to the desired position.

3 Tighten the T-handle to secure the mast in the desired position.

4 Before lowering the mast sections, the blue arrows on the mast must be aligned.

5 Release the mast rotation lock and rotate the mast to align the arrows.

6 Tighten the T-handle to secure the mast.



Operating Instructions

Operation of Lights

Note: The engine must be running before the lights are turned on.

1 Be sure the position of the lights is adjusted before raising the mast.

2 Start the engine

3 Turn on the main circuit breaker switches on the control panel.

4 Turn on the lights using the individual light switches.

Note:Lights can take up to 20 minutes to reach full intensity.If the lights are turned off and turned back on again while still warm, they will not light up again for 20 to 30 minutes.

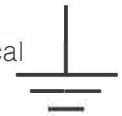
5 Turn the lights off by turning the circuit breaker switches to the off position.

6 Make sure the lights are turned off before engine is shut down.

Grounding

If your light tower has the optional grounding rod, drive the grounding rod into the ground and connect to the grounding lug located on the chassis at the rear of the light tower.

Note: This machine should be grounded in accordance with all local electrical codes. Consult the local electrical codes or authority having jurisdiction in the area where the machine will be used for specific requirements.



Electrical Outlets

A 120V/20 amp GFI duplex receptacle and a 240V/30 amp T-lock receptacle are located on the control panel inside the light tower cabinet.

Note: Before plugging in auxiliary power cords, feed them up through the trailer frame and attach to the receptacles. Close the cabinet doors to protect the control panel and other components from weather.

Operating Instructions

Towing

1 Make sure the mast is rotated to its original position and secured. Line up the arrows on the front of the mast.

2 Turn the extend/retract winch handle counterclockwise until the mast sections are fully retracted.

3 When the mast sections are fully retracted, remove the cotter pin and the lower retaining pin from the lower mast support.

4 Lower the mast by turning the raise/lower winch counterclockwise.

5 When the mast is fully lowered, insert the upper retaining pin and the cotter pin.

6 Insert the lower retaining pin into the storage hole provided in the mast support and insert the cotter pin.

7 Make sure the covers are closed and secured.

8 Raise the side outrigger jacks and the rear leveling jack. Rotate them into the stowed and secured position.

9 Release the spring pin on the side outriggers and slide the outriggers into the stowed and secured position. Make sure the outriggers are locked in place.

10 Pull the release pin on the side outriggers and raise the outriggers into the stowed and secured position. Rotate the leveling jack into the stowed and secured position.

11 If the optional grounding rod has been used, unearth and remove the grounding rod from the grounding lug and stow securely inside the cabinet.

12 Raise the tongue of the light tower by turning the tongue jack handle.

13 Position the transport vehicle under the coupler on the tongue of the light tower.

14 Open the latch on the coupler.

15 Turn the tongue jack handle to lower the tongue onto the transport vehicle.

16 Close the latch on the coupler.

17 Rotate the tongue jack to the stowed position and secure with the lock pin.

18 Attach the safety chains (if required).

19 Connect and test the trailer lights.

Operating Instructions

Towing Information

Driving a vehicle/trailer combination is different from driving a vehicle alone.

Inspect all connections at each stop.

All tires must be properly inflated. Do not overinflate the tires. Tire pressures go up during driving. Checking the tire pressure when the tires are warm will give you an inaccurate pressure reading.

Increase the distance between your vehicle and the vehicle in front of you to twice the normal following distance when towing a trailer. Allow more following distance in adverse weather.

Slow down for downgrades and shift your transmission into a lower gear.

Slow down for curves, hazardous road conditions, freeway exits, and when driving in adverse weather.

Heavy winds, excessive speed, load shifting or passing vehicles can cause a trailer to sway while driving. If this occurs, do not brake, speed up or turn the steering wheel. Turning the steering wheel or applying the brakes can cause the vehicle and trailer to jackknife. Let up on the gas pedal and keep the steering wheel straight.

If the vehicle and/or trailer travels off the paved road, hold the steering wheel firmly and let up on the gas pedal. Do not apply the brakes. Do not turn sharply. Slow down to under 25 mph / 40 km/h. Gradually turn the steering wheel to get back on the road. Proceed with caution when entering traffic.

When passing other vehicles, be sure to leave enough room for the extra length of the trailer. You will need to go much farther beyond the passed vehicle before you can return to your lane.

Avoid sudden movements when turning.

Transport and Lifting Instructions

Observe and Obey:

- ☑ Larson Electronics provides this securement information as a recommendation. Drivers are solely responsible for making sure machines are properly secured and the correct trailer is selected pursuant to US Department of Transportation regulations, other localized regulations, and their company policy.
- ☑ Larson Electronics customers needing to containerize any Larson Electronics product should source a qualified freight forwarder with expertise in preparing, loading and securing construction and lifting equipment for international shipment.
- ☑ The transport vehicle must be parked on a level surface.
- ☑ The transport vehicle must be secured to prevent rolling while the machine is being loaded.
- ☑ Be sure the vehicle capacity, loading surfaces and chains or straps are sufficient to withstand the machine weight. See the serial label for the machine weight.
- ☑ Common sense and planning must be applied to control the movement of the machine when lifting it with a crane or forklift.

Securing to Truck or Trailer for Transit

Fully retract and lower the mast to the stowed position.

Secure the mast for transport with the travel lock pin.

Fully retract, raise and lock all outriggers.

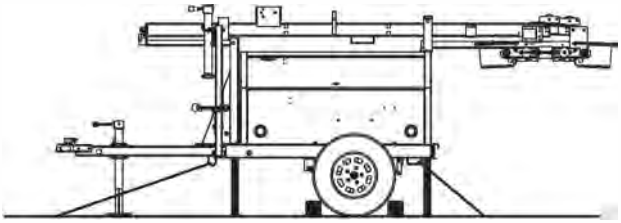
Close and secure the cabinet doors.

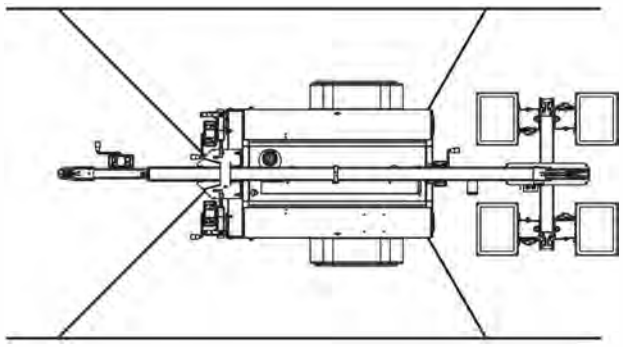
Inspect the entire machine for loose or unsecured items.

Use the four tie-down points for anchoring down to the transport surface.

Use a minimum of four chains to secure the light tower.

Adjust the rigging to prevent damage to the chains.





Transport and Lifting Instructions

Observe and Obey:

☑ Only qualified riggers should rig the machine.

☑ Only certified crane operators should lift the machine and only in accordance with the applicable crane regulations.

☑ Be sure the crane capacity, loading surfaces and straps or lines are sufficient to withstand the machine weight. See the serial label for the machine weight.

☑ Lifting the Machine with a Crane

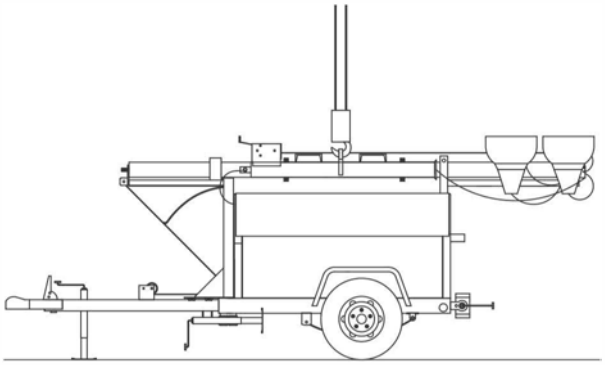
Fully retract and lower the mast to the stowed position.

Secure the mast for transport with the travel lock pin.

Fully retract, raise and lock all outriggers.

Close and secure the cabinet doors.

Use the lifting eye on the mast to lift the machine.



Maintenance



Observe and Obey:

☑ Only routine maintenance items specified in this manual shall be performed by the operator.

☑ Scheduled maintenance inspections shall be completed by qualified service technicians, according to the manufacturer's specifications and the requirements specified in the responsibilities manual.

Maintenance Symbols Legend

The following symbols have been used in this manual to help communicate the intent of the instructions. When one or more of the symbols appear at the beginning of a maintenance procedure, it conveys the meaning below.



Indicates that tools will be required to perform this procedure.



Indicates that new parts will be required to perform this procedure.

Check the Engine Oil Level



Maintaining the proper engine oil level is essential to good engine performance and service life. Operating the machine with an improper oil level can damage engine components.

Note: Check the oil level with the engine off.

1 Check the oil level dipstick. Add oil as needed.

Perkins 403D-11 Engine	
Oil type	15W-40
Oil type - cold conditions	5W-40
Kubota D-1105 Engine	
Oil type	10W-30
Oil type - cold conditions	5W-30

Maintenance

Check the Engine Coolant Level



Maintaining the engine coolant at the proper level is essential to engine service life. Improper coolant level will affect the engine's cooling capability and damage engine components. Daily checks will allow the inspector to identify changes in coolant level that might indicate cooling system problems.

⚠ Burn hazard. Beware of hot engine parts and coolant. Contact with hot engine parts and/or coolant may cause severe burns.

Note: Do not remove the radiator cap.

1 Check the fluid level in the coolant recovery tank. Add fluid as needed.

⊙ Result: The fluid level should be at the FULL mark.

Check the Batteries



Proper battery condition is essential to good machine performance and operational safety. Improper fluid levels or damaged cables and connections can result in component damage and hazardous conditions.

⚠ Electrocution hazard. Contact with hot or live circuits may result in death or serious injury. Remove all rings, watches and other jewelry.

⚠ Bodily injury hazard. Batteries contain acid. Avoid spilling or contacting battery acid. Neutralize battery acid spills with baking soda and water.

1 Put on protective clothing and eye wear.

2 Be sure that the battery cable connections are tight and free of corrosion.

Be sure that the battery hold-down brackets are in place and secure.

Note: Adding terminal protectors and a corrosion preventative sealant will help eliminate the corrosion on the battery terminals and cables.

Maintenance

Check the Tire Pressure



- ⚠ Bodily injury hazard. An over-inflated tire can explode and may cause death or serious injury.
- ⚠ Collision hazard. An excessively worn tire can cause poor handling and continued use could result in tire failure.
- ⚠ Tip-over hazard. Do not use temporary flat tire repair products.

Maintaining the tires and wheels in good condition is essential to safe operation and good performance. Tire and/or wheel failure could result in a machine tip-over. Component damage may also result if problems are not discovered and repaired in a timely fashion.

1 Check the tire surface and sidewalls for cuts, cracks, punctures and uneven or excessive tread wear. Replace the tire if uneven or excessive tread wear is found.

2 Check each wheel for damage, bends and cracks. Replace the wheel if any damage is found.

Note: Tires and wheels must be replaced with tires and wheels of the specifications listed.

3 Check each tire with an air pressure gauge. Add air as needed.

4 Check the torque of each lug nut.

Tire Specifications, U.S.		
Tire Size	ST175/80D13	Load B
Lug nut torque	80 ft/lbs	108 Nm
Tire pressure (cold)	35 psi	241 kpa

Scheduled Maintenance

Maintenance performed quarterly, annually and every two years must be completed by a person trained and qualified to perform maintenance on this machine according to the procedures found in the service manual for this machine.

Machines that have been out of service for more than three months must receive the quarterly inspection before they are put back into service.

Specifications

WCDE-4

Height, stowed	5 ft 9.5 in	1.765 m
Length, stowed	14 ft 2 in	4.331 m
Width, stowed	4 ft 6 in	1.372 m
Extended mast height	30 ft	9.114 m
Weight WCDE-4-8X160WSA-LED	1750 lbs	794 kg
(Machine weights vary with option configurations. See serial label for specific machine weight.)		
Maximum tongue weight	199 lbs	91 kg
Tire size, U.S.	ST175/80D13	Load B
Engine type	Kubota	13.6 HP
	Perkins	13.8 HP
Fuel capacity	30 gallons	114 liters
Run time	Kubota	38.3 hours
	Perkins	37.9 hours
Generator	Marathon 6 kW, 60 Hz	
Total lighting wattage Four lights		600 watts
Replacement bulbs		150 watts CREE LED
Tower rotation		359 degrees non-continuous
Maximum towing speed	60 mph	97 km/h
Maximum wind speed	62 mph	100 km/h
Sound level (dba rating)	71 dba @	23 ft / 7 m

Continuous improvement of our products is a Terex policy. Product specifications are subject to change without notice or obligation.

Reporting Safety Defects

Larson Electronics
9419 E US Highway 175
Kemp, Texas 75143

Reporting Safety Defects

If you believe that your vehicle has a defect which could cause a crash or could cause injury or death, you should immediately inform the National Highway Traffic Safety Administration (NHTSA) in addition to Larson Electronics.

If NHTSA receives similar complaints, it may open an investigation, and if it finds that a safety defect exists in a group of vehicles, it may order a recall and remedy campaign. However, NHTSA cannot become involved in any individual problems between you, your dealer or Larson Electronics.

To contact NHTSA you may either call the Auto Safety Hotline toll-free at 1-800-424-9393 (366-0123 in Washington DC area) or write to:

NHTSA
U.S. Department of Transportation
400 7th Street SW, (NSA-11)
Washington DC 20590

You can also obtain information about motor vehicle safety from the Hotline.

California Proposition 65

Warning

The exhaust from this product contains chemicals known to the State of California to cause cancer, birth defects or other reproductive harm.

Towing Checklist (use at each stop)

Before Towing

- Travel lock is securely locked in place
- Towing hitch is properly secured to tow vehicle
- Safety chans (if required) are properly attached and secure (chains are crossed below hitch)
- All lights are connected and working
- Tires are properly inflated

Before Driving

- Fasten safety restraints
- Properly adjust mirrors

On the Road

- Do not exceed 60 mph / 97 km/h. Obey all local and national towing speed laws
- Check connections and tire pressure at each stop
- Slow down for hazardous conditions
- Allow extra distance for following and passing other vehicles

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

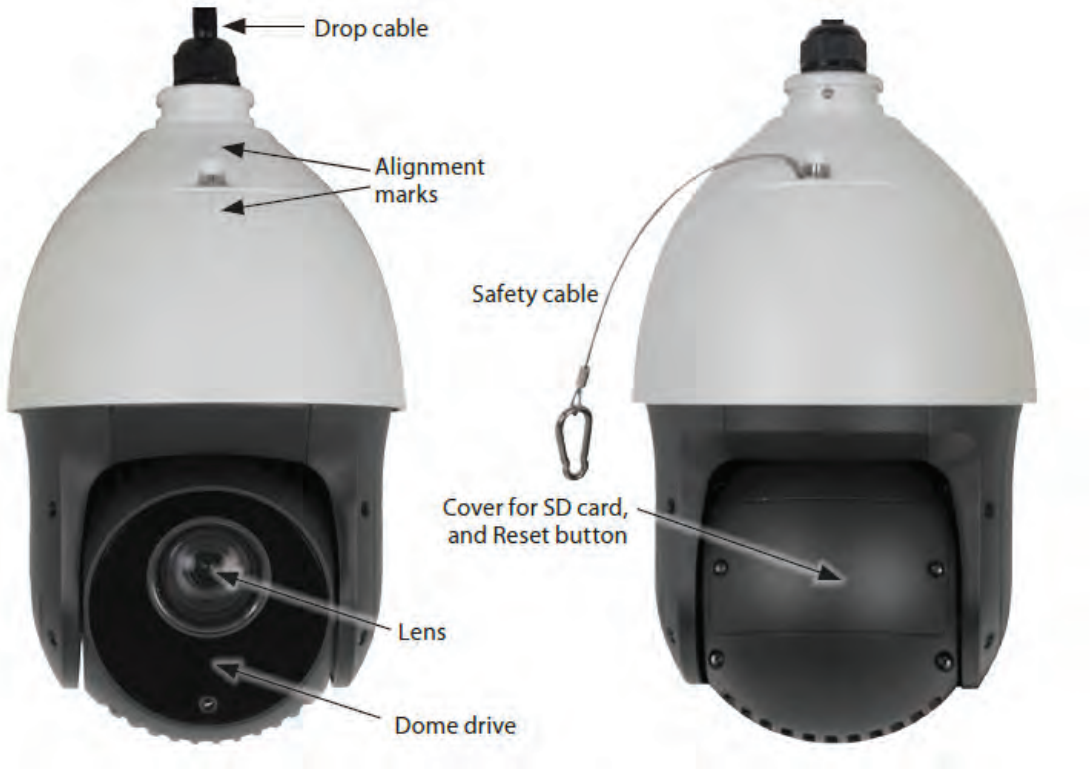
SECTION 1 **Overview** 51
1.1 Features 51
1.2 What's in the box 53
1.3 Accessories 51
SECTION 2 **Installation** 54
2.1 Remove the camera from the packaging 54
2.2 Install an micro-SD card in the camera 55
2.3 Camera wall mount installation 56
2.4 Ceiling mounting 57
2.5 Connecting the cables 58
SECTION 3 **Configure Network Access** 62
SECTION 4 **Remote login** 65
4.1 Additional configuration steps 69
APPENDIX A **Specifications** 70
APPENDIX B **Definitions** 72
APPENDIX C **Lightning and Surge Protection** 74
APPENDIX D **24 Vac Wire Gauge and Transmission Distance** 75

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

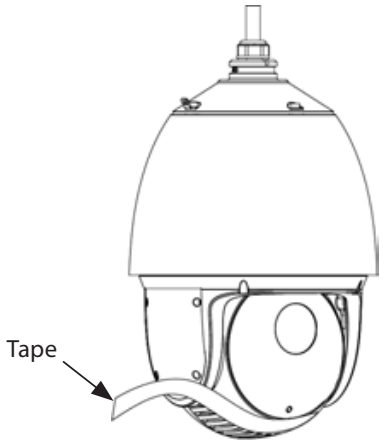
Do not carry the camera by the drop cable.



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

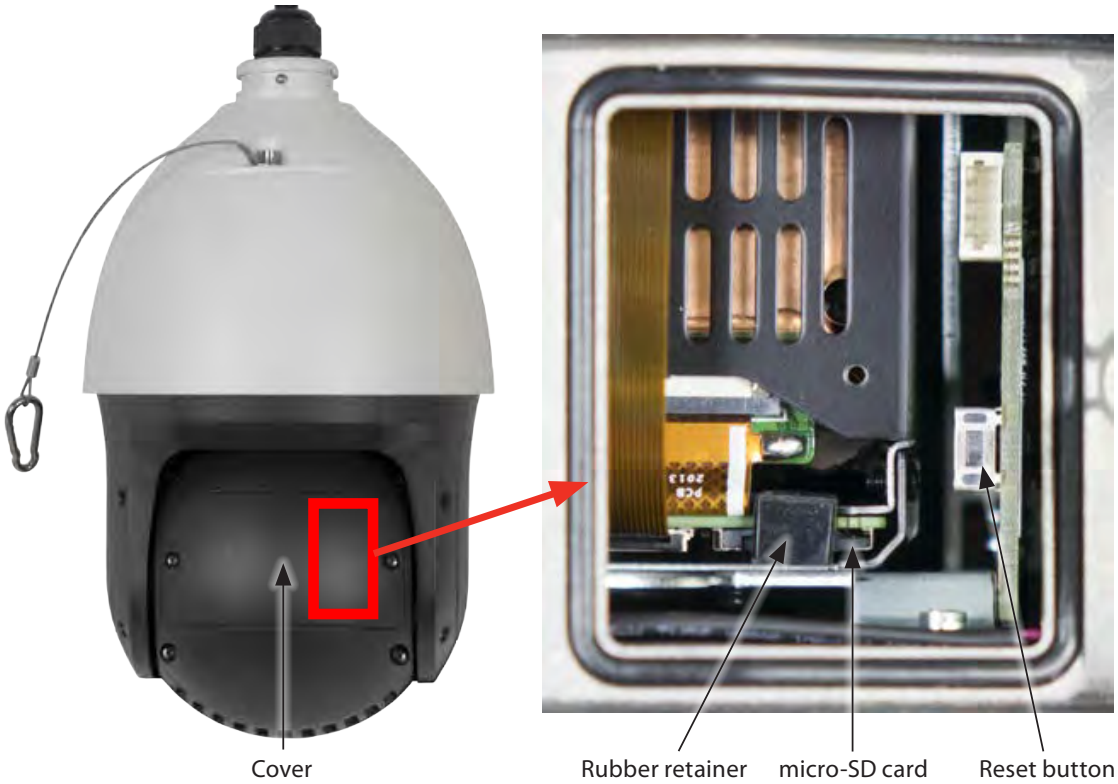
2.1 Remove the camera from the packaging

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.

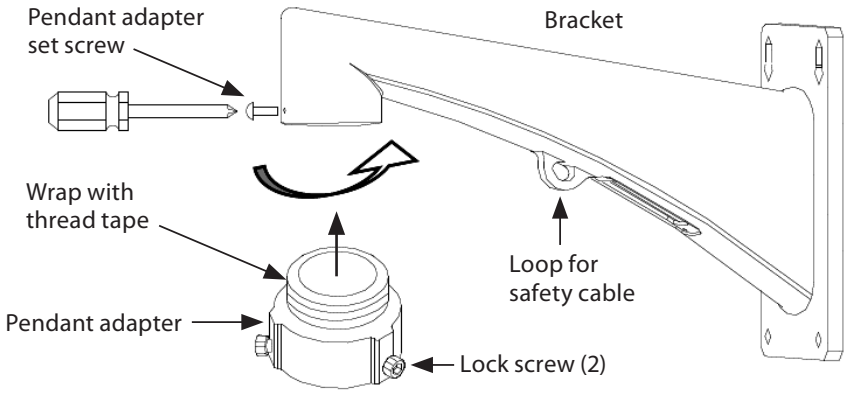
2.3 Camera wall mount installation

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)

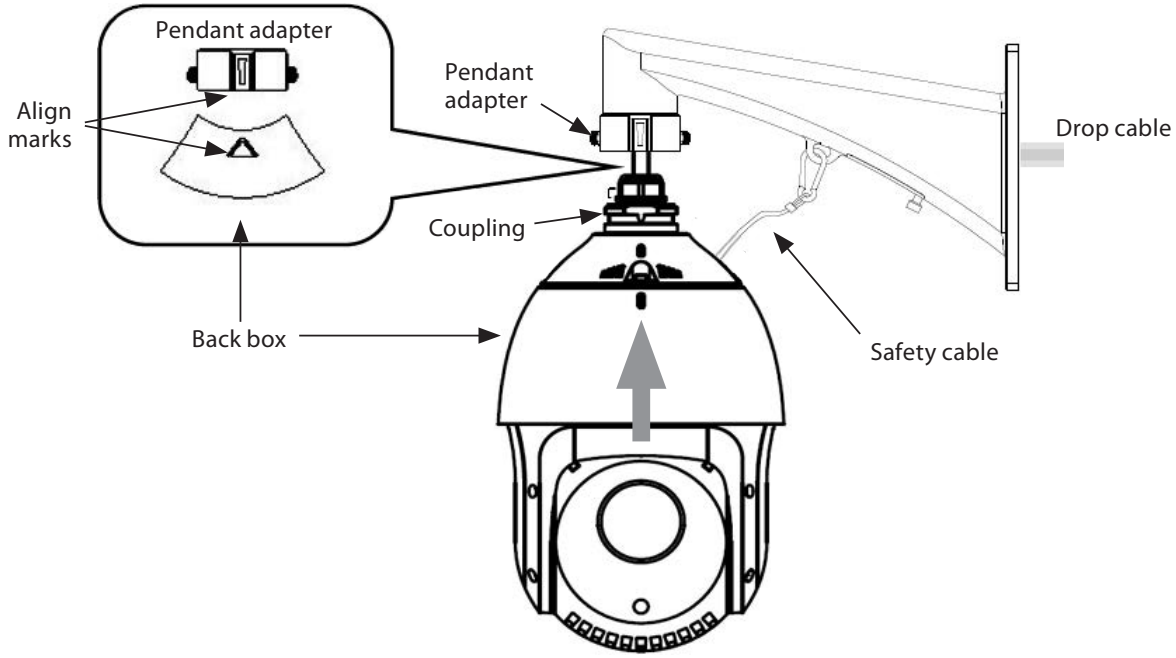


Attach pendant adapter to mounting bracket

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.

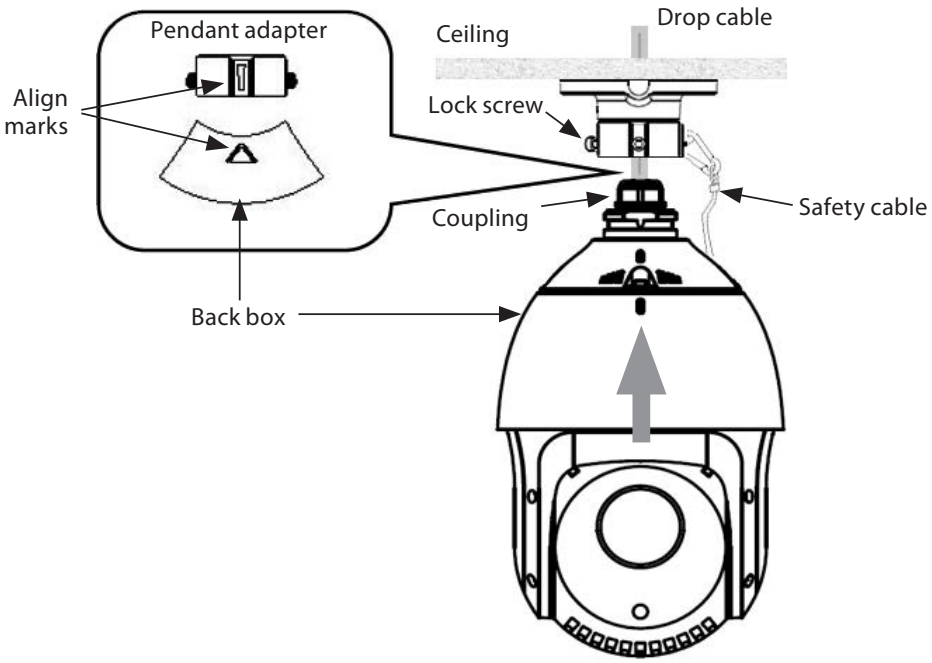
2. Using the mounting bracket as a template, mark the location of the mounting screw holes on the ceiling.

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.



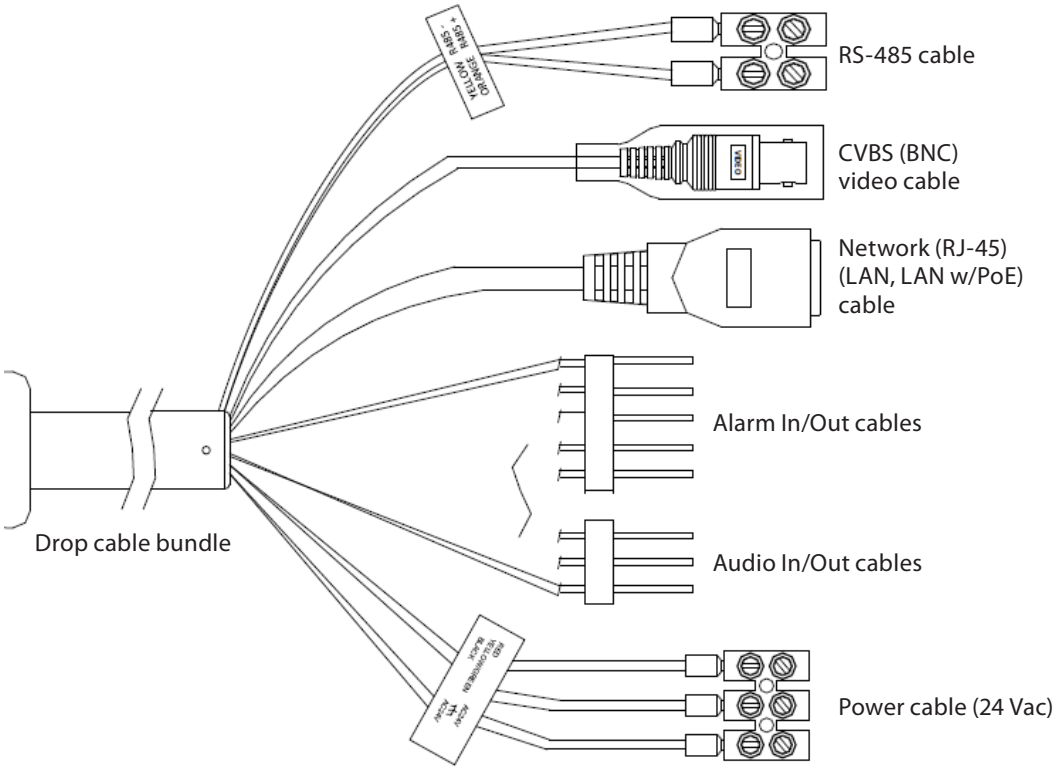
7. Fit the camera coupling into the ceiling mounting bracket, then twist the bracket to align the marks on the bracket and the camera back box. See the figure above.

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.



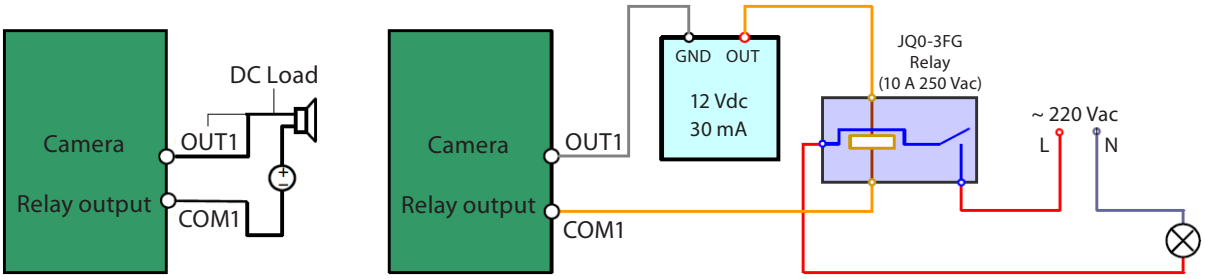
Connect the camera to other devices as needed in the order shown below.

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.

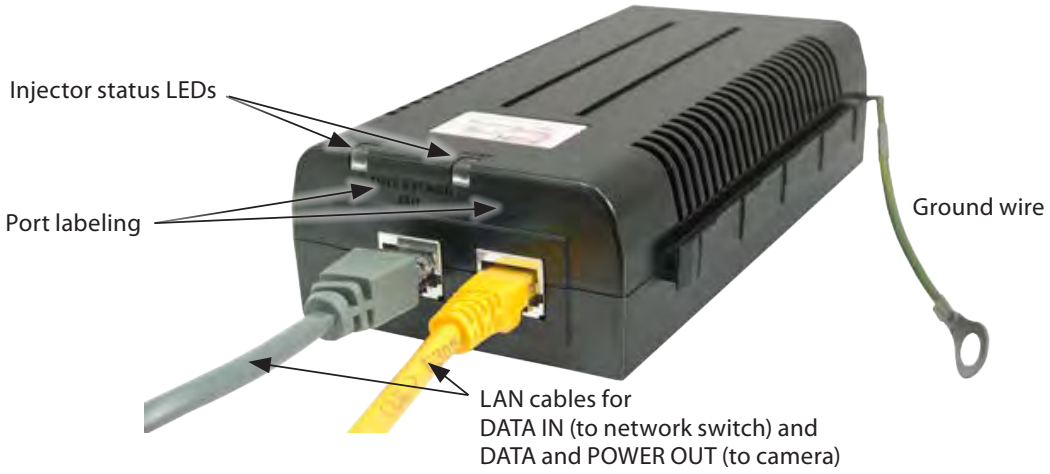
Network (LAN) cable

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:

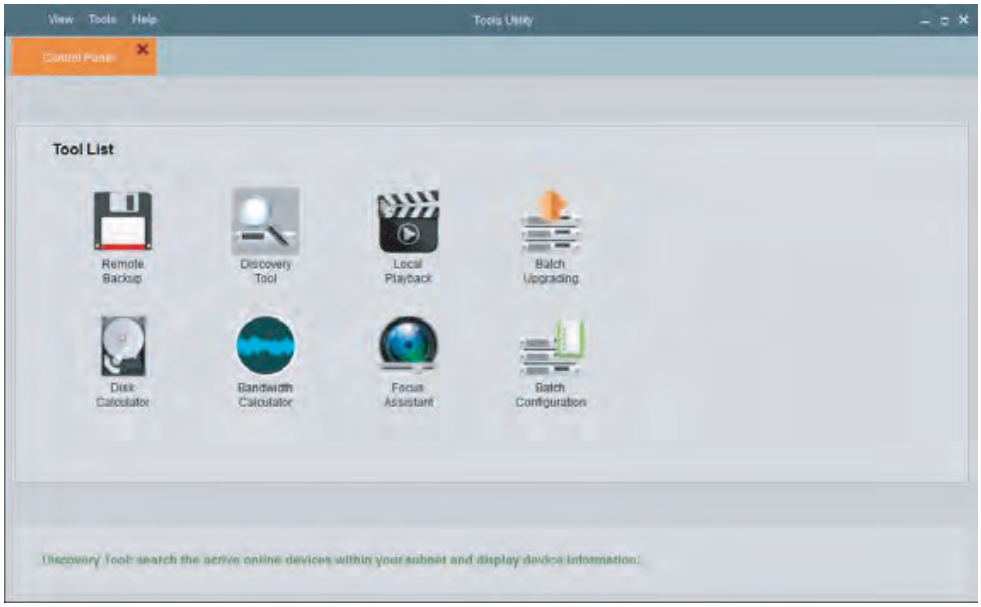
- Installing SADP Tools
- Setting up the camera network configuration

Step 1. Install SADP Tool

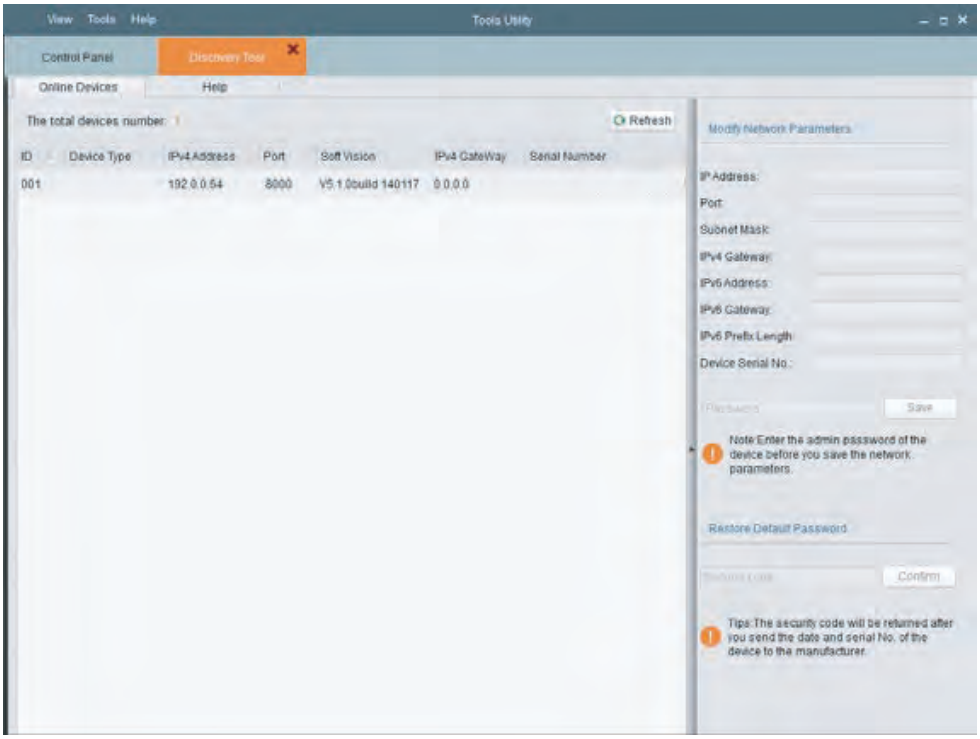
SADP Tool Utility is a collection of useful software programs for use with your IP based cameras and recorders. Within the tool set is the **Discovery Tool** a software utility used to "discover" IP cameras and NVRs/DVRs installed on the LAN and change their network parameters. Use Discovery Tool to 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.

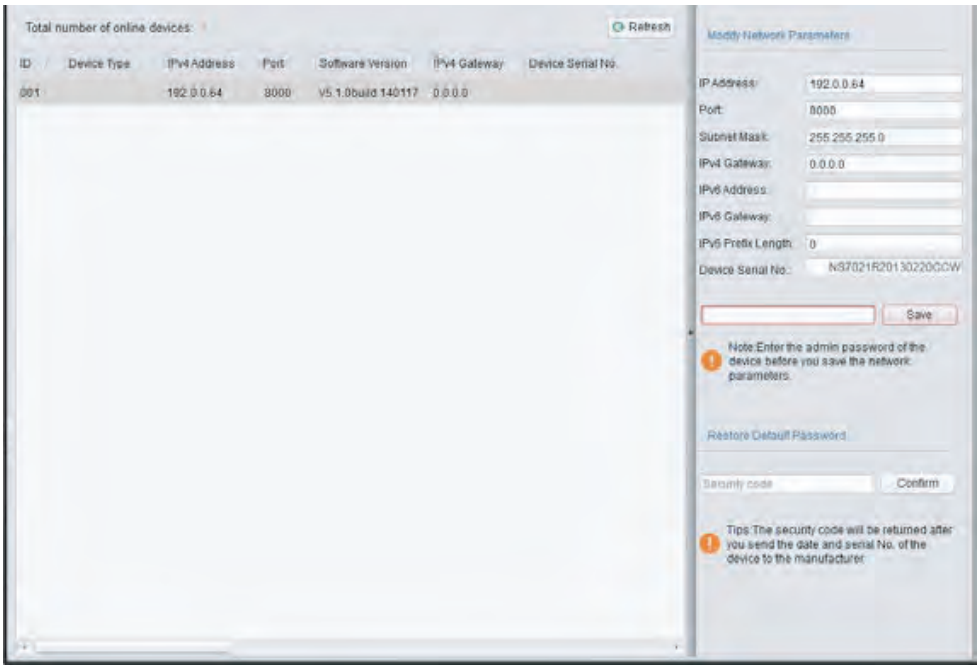


2. Double click the **Discovery Tool** icon to open the program. When the program opens it will automatically list the cameras and recorders installed on the network.

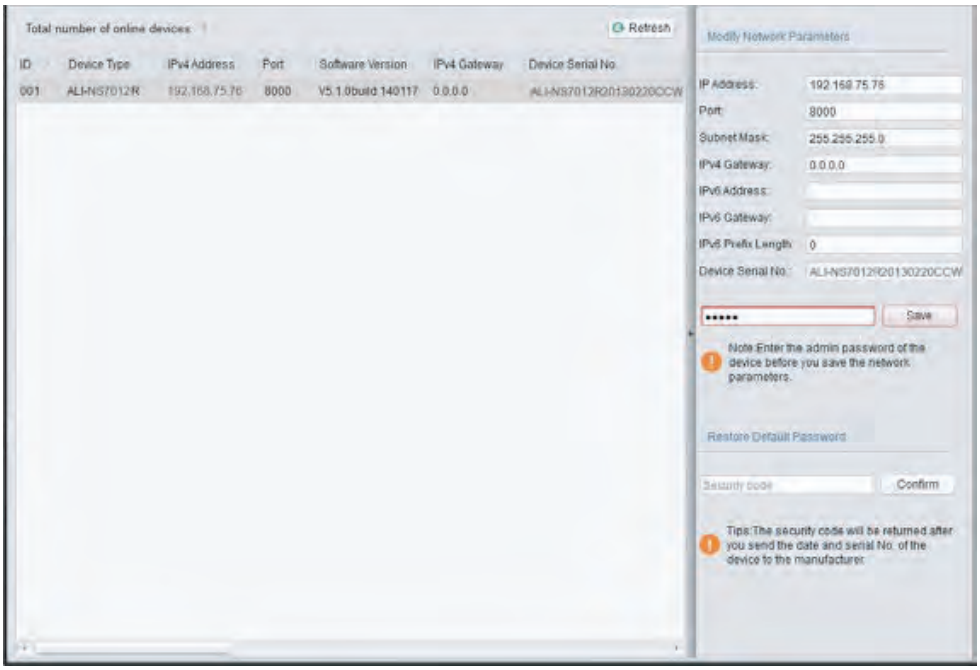


3. To change the network settings of the camera to be compatible with the subnet where it is installed, do the following:

   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**

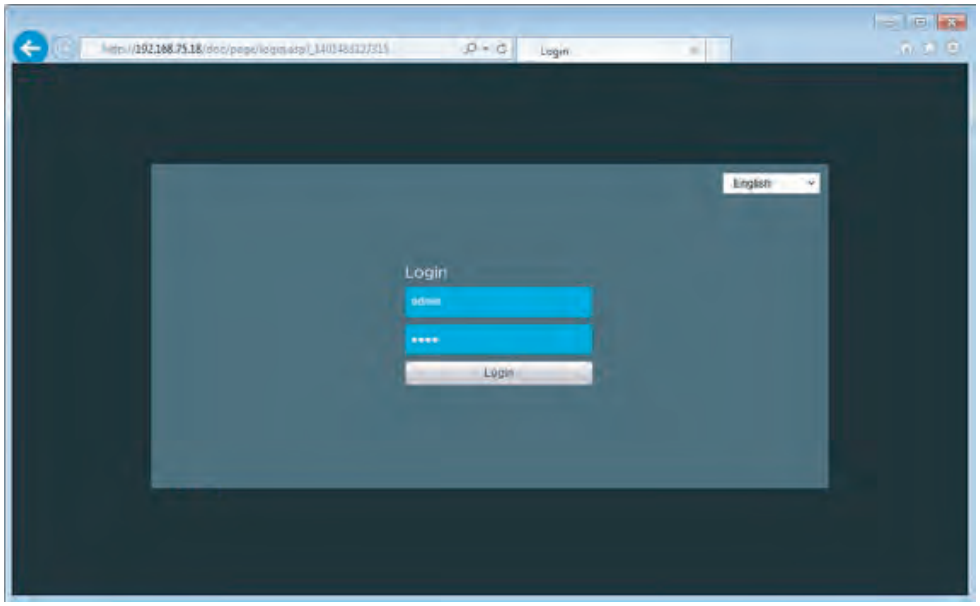
d. Click the **Save** button. The new IP address, port, etc. parameters will appear in the list with the device you modified.

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:

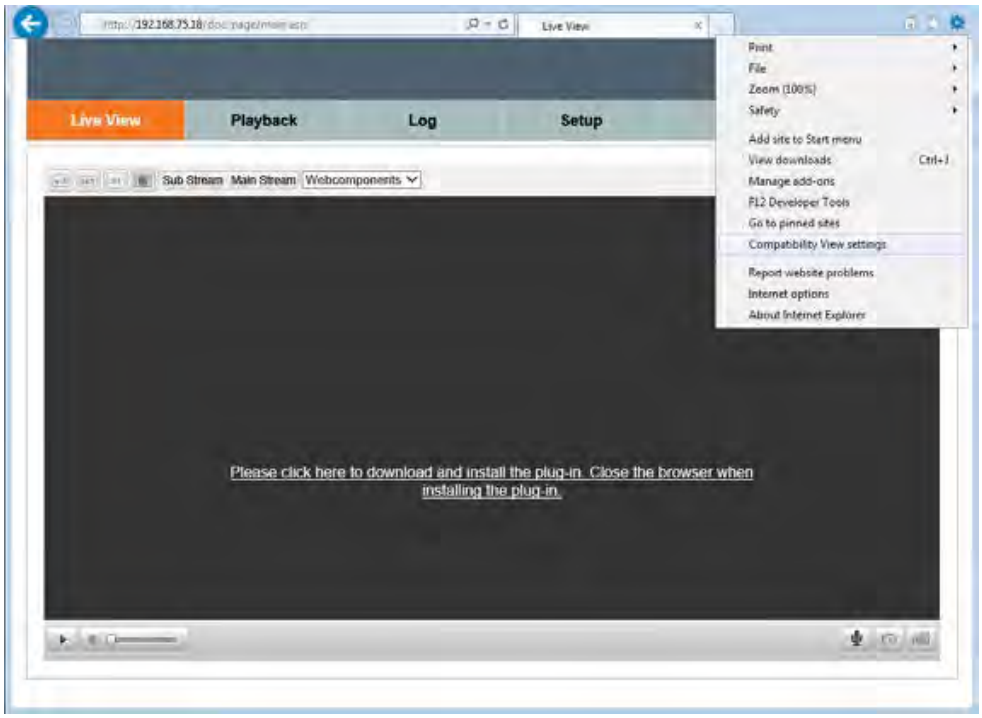
1. Open your Microsoft Internet Explorer browser on your compute and enter the IP address of the camera in the URL field. In the example below, the IP address of the camera is 192.168.75.18.



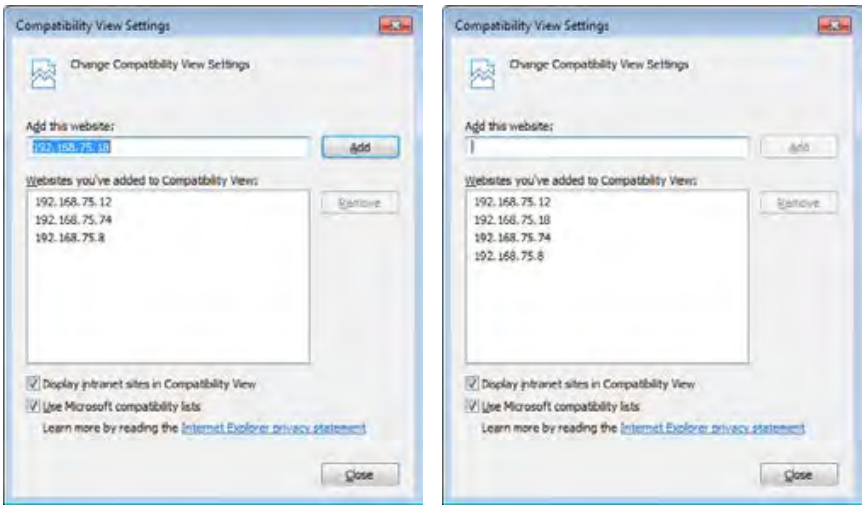
2. In the login window, enter your **User Name** and **Password** in the appropriate fields, then click **Login**. The default **User Name** and **Password** for cameras is **admin** and **ChangeMeNØw**

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.

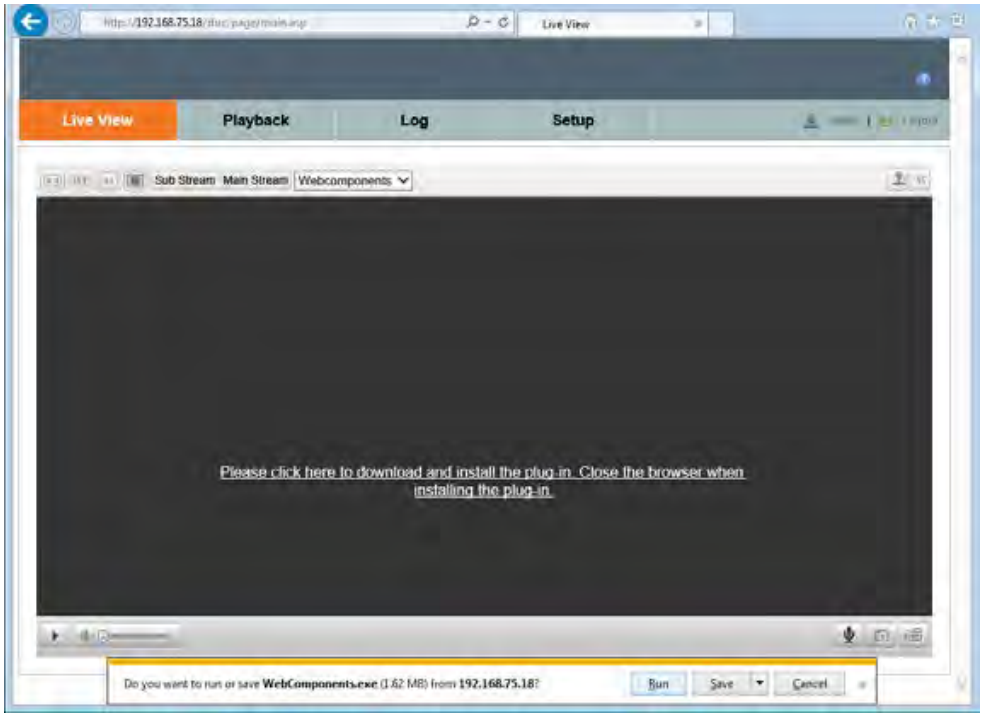


b. In the Compatibility View Settings window, ensure that the IP address of your camera is in the **Add this website** field, then click **Add**.

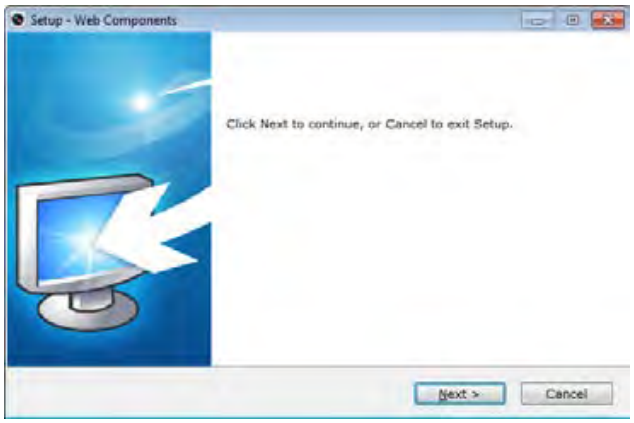


c. After clicking **Add**, the IP address will appear in the Websites list. Click **Close**.

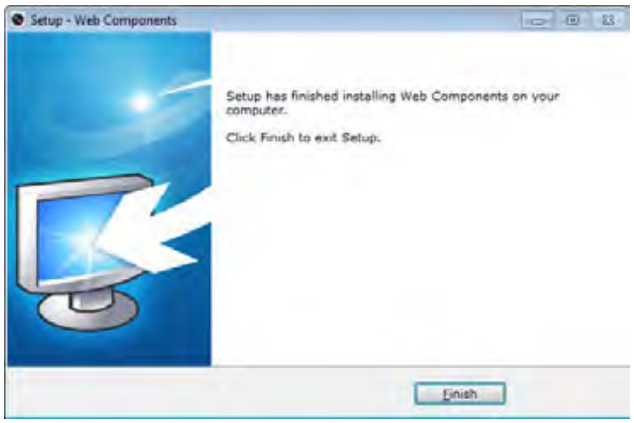
d. If a message on the screen requesting that you install a plug-in (see below), click on the message and continue with the following sub-steps. A message box will appear at the bottom of the window to install the WebComponents plug-in. Otherwise, continue with step "4. In the Live View window shown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



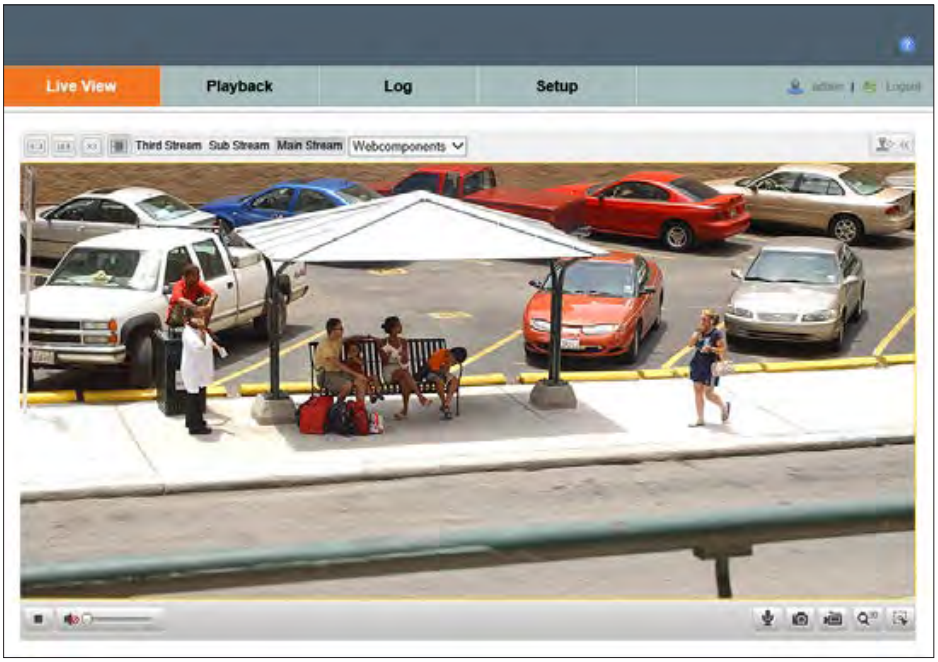
e. In the message box, click **Run** to install WebComponents.exe. The following pop-up window will open. When this window appears, close the browser.



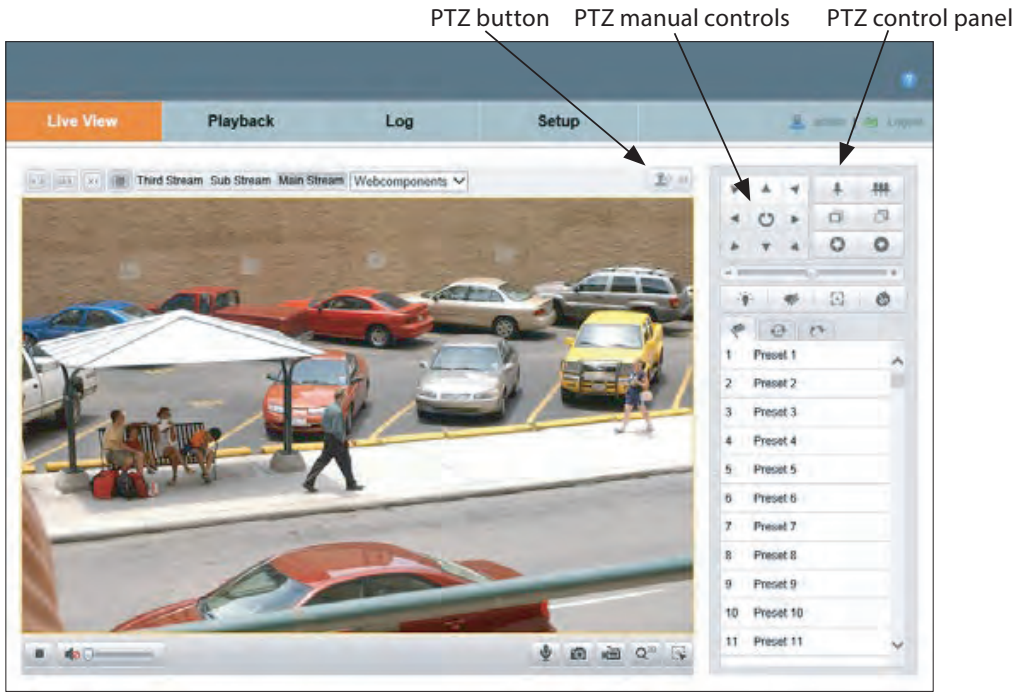
f. Click **Next** to install WebComponents. Allow the plug-in installation to complete. When the following window appears, click **Finish**.



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

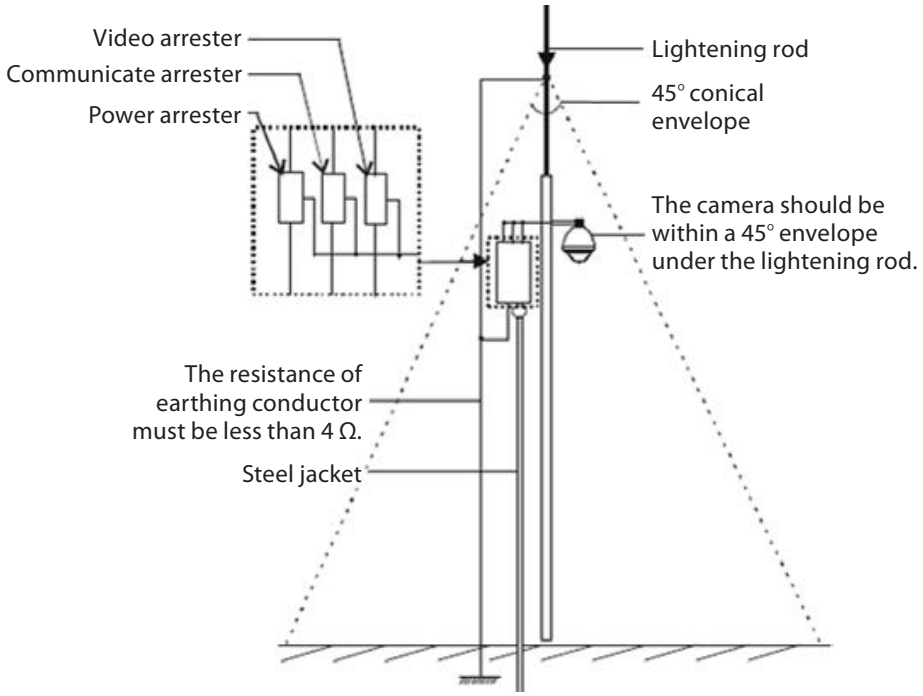
3D Digital Noise Reduction	Comparing with the general 2D digital noise reduction, the 3D digital noise reduction function processes the noise between two frames besides processing the noise in one frame resulting in clearer video.
3D Positioning	In the client software, use the click left mouse button 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 Recorders
User Manual V1.16

SKU HERE

Thank you for purchasing our product. Contact your local dealer if you have any questions or feedback. No part of this manual may be copied, reproduced, translated, or distributed in any form or by any means without prior consent in writing from our company.

Disclaimer

CAUTION!

The default password is intended only for your first login. We strongly recommend you set a strong password to ensure account security.

- **Strong**: contains at least 9 characters that include letters, special characters and numbers.
- **Medium**: contains at least 8 characters that included at least two of the following groups: upper-case letters, lower-case letters, special characters, and numbers.
- **Weak**: contains less than 8 characters only one of the following groups: upper-case letters, lower-case letters, special characters, and numbers.

- To the maximum extent permitted by applicable law, the product described, with its hardware, software, firmware and documents, is provided on an "as is" basis.
- Best effort has been made to verify the integrity and correctness of the contents in this manual, but no statement, information, or recommendation in this manual shall constitute formal guarantee of any kind, expressed or implied. We shall not be held responsible for any technical or typographical errors in this manual. The contents of this manual are subject to change without prior notice. Updates will be added to a new version of this manual.
- Use of this manual and the product and the subsequent result shall be entirely on the user's responsibility. In no event shall we be liable for any special, consequential,

incidental, or indirect damages, including, among others, damages for loss of business profits, business interruption, or loss of data or documentation, or product malfunction or information leakage caused by cyberattack, hacking or virus in connection with the use of this product.

- Video and audio surveillance can be regulated by laws that vary from country to country. Check the law in your local region before using this product for surveillance purposes. We shall not be held responsible for any consequences resulting from illegal operations of the device.
- The illustrations in this manual are for reference only and may vary depending on the version or model of your device. The screenshots in this manual may have been customized to meet specific requirements and user preferences. Some examples and functions shown may differ from those displayed on your monitor.
- This manual is a guide for multiple product models. It is not intended for any specific product.
- Due to uncertainties such as physical environment, a discrepancy may exist between the actual values and reference values provided in this manual. The ultimate right to interpretation resides in our company.

Safety Symbols

The symbols in the following table may be found in this manual. Carefully follow the instructions indicated by the symbols to avoid hazardous situations and use the product properly.

Symbol	Description
WARNING!	Indicates a hazardous situation which, if not avoided, could result in bodily injury or death.

 **CAUTION!**	Indicates a situation which, if not avoided, could result in damage, data loss or malfunction to product.
 **NOTE!**	Indicates useful or supplemental information about the use of product.

Contents

Preface 85

Part I Local Operations 86

1 Before You Begin 87

User Login 87

Local Operations 87

Remote Control 91

2 Initial Configuration 93

Preparation 93

Device Login 93

Wizard 95

3 Live View 97

Live View Status 97

Window Toolbar 97

Screen Toolbar 98

Shortcut Menu 99

Sequence Operation 100

Zoom 101

Image Configuration 102

Preview Configuration 102

Preview Configuration 102

Advanced Configuration 103

4 Channel Configuration 104

Channel Management 104

Adding an IP Device 104

Managing an IP Device 108

Fisheye Configuration 110

Operations Example: Ceiling Mount and Fisheye+3PTZ camera 112

OSD Configuration 113

Image Configuration 114
Privacy Mask Configuration 118

5 PTZ Control 120

PTZ Control Window and PTZ Management Window 120
Setting and Calling a Preset 121
Setting a Preset Patrol 122
Setting a Recorded Patrol 124
Setting Auto Guard 124

6 Recording and Snapshot 126

Encoding Settings 126
Draw or Edit a Schedule 129
Scheduled Recording and Snapshot 130
Motion Detection Recording and Snapshot 130
Alarm Triggered Recording and Snapshot 132
Manual Recording and Snapshot 134
Holiday Recording and Snapshot 134
Other Recording and Snapshot Types 136

7 Playback 137

Instant Playback 137
Playback Toolbar 138
Playback by Camera and Date 139
Playback in Corridor Mode 140
Playback by Tag 141
Playback by Motion Detection 141
Playback by Video Loss 142
Playback by Smart Search 142
Playback by External File 143
Playback by Image 144
Playback by POS 144
File Management 144

8 Backup 146
Recording Backup 146
Image Backup 148
9 Alarm 149
Alarm Input and Output 149
Motion Detection 151
Tampering Detection 152
Human Body Detection 153
Video Loss 154
Alert 154
Buzzer 155
Alarm-Triggered Actions 156
Manual Alarm 157
10 VCA 158
VCA Configuration 158
VCA Search 167
11 Network Configuration 171
Basic Configuration 171
Platform Configuration 177
Advanced Configuration 183
12 Disk Configuration 189
Disk Management 189
Array Configuration 190
Disk Group 193
Space Allocation 193
Advanced Configuration 194
Hard Disk Detection 195
13 System Configuration 197
Basic Configuration 197
Time Configuration 198
POS Configuration 199

Serial Port Configuration....200
User Configuration....200
Security Configuration....202
Hot Spare Configuration....205
14 System Maintenance....207
System Information....207
Network Information....209
Log Query....211
Import/Export....212
System Restoration....213
Automatic Maintenance....214
System Upgrade....214
15 Shutdown....216
Part II Web-Based Operations....217
1 Before You Begin....217
2 Login....218
3 Live View....219
4 Playback....221
5 Configuration....222
Appendix A Typical Applications....223
Typical Application 1....223
Typical Application 2....223
Typical Application 3....224
Appendix B Acronyms....225
Appendix C FAQs....226

Preface

This manual describes how to use your NVR locally and on the Web interface.

In this manual, the terms “IP camera” and “IPC” both refer to “network camera”, which requires a connection to the network. The IP device mentioned in this manual refers to either an IP camera (also known as network camera) or a Digital Video Server (DVS).

Part I Local Operations

An NVR supports two types of operations: local operations and web-based remote operations. With local operations you connect a monitor and a mouse to the NVR and use the mouse to operate the system. If your NVR has buttons on the front panel or is delivered with a remote control, you may also control your NVR by pressing the front panel buttons or using the remote control.

The NVR has an embedded web server that allows web-based operations. To do this, you need a PC that has a network connection to the NVR and is installed with a web browser. You just need to navigate to the NVR's IP address and log in to the Web interface like you log in to the system locally.

This section describes local operations.

1 Before You Begin

Please be aware that the parameters that are grayed out on the system user interface (UI) cannot be modified. The parameters and values displayed may vary with device. Figures in this manual are for illustration purposes only.

User Login

Use the default username *admin* and password **123456** for your first login.

CAUTION!

The default password is intended only for the first login only. It should be immediately changed to a strong password. Strong Passwords contain at least nine characters that include letters, numbers and special characters.

1. Right-click anywhere in the window and then choose **Menu**. The login dialog box is displayed.
2. Select the username from the drop-down list, enter your password, and then click **Login**.

Local Operations

You can refer to Initial Configuration and complete a quick configuration.

NOTE!

Unless otherwise specified, all operations described in this manual are performed with a mouse by the right hand. See Mouse Operations for details.

Mouse Operations

Table 1–1 Mouse Operations

Name	Action	Description
Left button	Click	• Select or confirm an item. • Select to edit digits, symbols, upper-case or lower-case letters in a field.
	Double-click	Enter or exit full screen mode in live view.
	Drag	Draw or move a rectangle on the screen, for example, a motion detection area.
Right button	Click	• Show the shortcut menu. • Exit zoom. • Exit the current window when **Cancel** or **Exit** is displayed.
Wheel	Scroll up or down	Scroll up or down a list or a window; or zoom in or out on a playback progress bar.
	Long press	Restore to lowest resolution

Front Panel Buttons

The front panel buttons may vary with NVR model.

Table 1–2 Front Panel Buttons 1

Button	Description
	Display the main menu.
	Switch to the next tab on the screen or switch the input method.
	Auxiliary function button.
	Exit the current window.

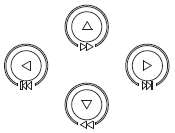
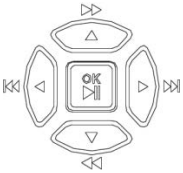
Button	Description
	• △, ▽, ▷, ◁: Switch windows or menu items; or control rotation directions of a PTZ camera when the PTZ toolbar is closed. PTZ stands for pan, tilt, and zoom. • ⏮, ⏭: Rewind or forward 30 seconds in full screen. • ⏩, ⏪: Variable-speed forward or rewind in full screen.
	Confirm an operation, or start/pause the playback.
	Press this button to start up or shut down the NVR. To shut down, press this button and hold until a message appears on the monitor (about 3 seconds). Click **Yes**. **Note:** This shutdown operation can be performed only when you are logged in to the system.

Table 1–3 Front Panel Buttons 2

Button	Description
	Press this button to start up or shut down the NVR. To shut down, press this button and hold until a message appears on your monitor (about 3 seconds). Click **Yes**. **Note:** This shutdown operation can be performed only when you are logged in to the system.
	Enter 1; or display the main menu.
	Enter 2, A, B, or C; or start instant playback.
	Enter 3, D, E, or F; or start manual recording.

Button	Description
	Enter 4, G, H, or I; or enter the PTZ control interface.
	Enter 5, J, K, or L; or switch the screen layout in live view or playback mode.
	Enter 6, M, N, or O; or enable or disable arming.
	Enter 7, P, Q, R, or S; or take a snapshot.
	Enter 8, T, U, or V.
	Enter 9, W, X, Y, or Z.
	Enter 0 or a space.
	Delete
	Switch the input method.
	Auxiliary function button.
	Exit the current window.
	Switch to the next tab.

Button	Description
	• △, ▽, ▷, ◁: Switch windows or menu items; or control rotation directions of a PTZ camera when the PTZ toolbar is closed • ⏮, ⏭: Rewind or forward 30 seconds in full screen. • ⏩, ⏪: Variable-speed forward or rewind in full screen. • OK ⏯: Confirm an operation; or start or pause playback.

Remote Control

Table 1–4 Functions of the Buttons on the Remote Control

Button	Function
Power	Press this button to start up or shut down the NVR. To shut down, press this button and hold until a message appears on your monitor (about 3 seconds). Click **Yes**. **Note:** This shutdown operation can be performed only when you are logged in to the system.
DEV	This button is for reserved functions.
Toolbar	• In live view mode, press this button to show the toolbar for the currently selected window. • In playback mode, press this button to display windows according to the configured screen layout.
Menu	Press this button to display the main menu.
Iris+/Iris-	Adjust the iris, focus and zoom of the PTZ camera in PTZ control mode.
Focus+/Focus-	
Zoom+/Zoom-	

Button	Function
UP, DOWN, LEFT, RIGHT, ENTER	● Press UP, DOWN, LEFT and RIGHT to navigate between menu items or shift focus. ● In PTZ control mode, press UP, DOWN, LEFT, and RIGHT buttons to select the corresponding buttons on the screen, and then press ENTER to activate the selection. ● In live view mode, press UP to start sequence in full screen. Pressing UP again starts sequence with three windows on the screen. Press DOWN to open the playback window. ● Press ENTER to confirm an operation or to display a selected drop-down list. In playback mode, press ENTER to play or pause in full screen mode. ● UP and DOWN: Variable speed forward or rewind in full screen. ● LEFT and RIGHT: Rewind or forward 30 seconds in full screen.
Fn	Press to navigate to the next window when multiple windows are displayed.
Esc	Exit.
Alphanumeric buttons	● Switch to the corresponding channel in live view mode. ● Input numbers and characters in edit mode.
Shift	Switch menu items.
Del	Remove characters or spaces on the left of the cursor.

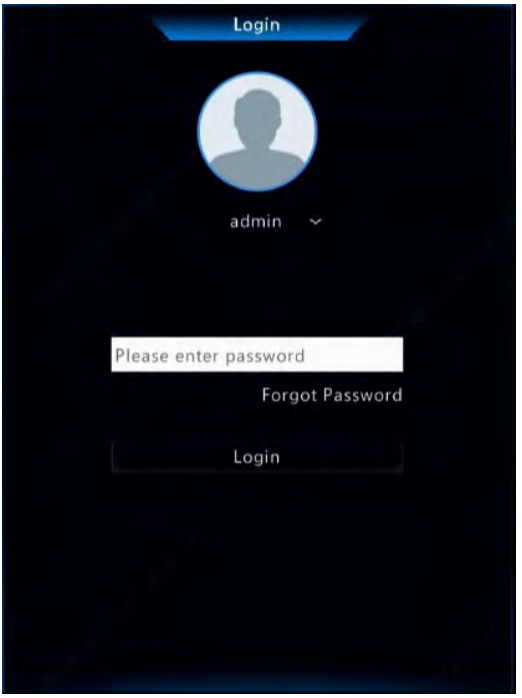
2 Initial Configuration

Preparation

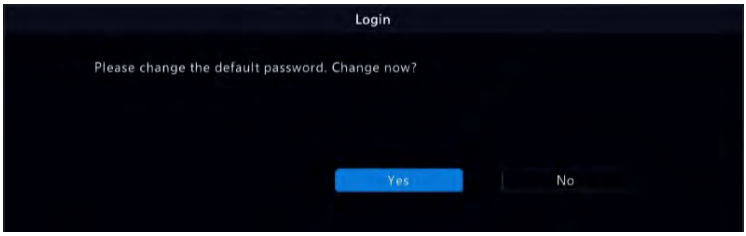
- Make sure that at least one monitor is correctly connected to the VGA or HDMI interface on the rear panel of the NVR.
- Verify that the hard disk(s) are correctly installed. For detailed steps to install a hard disk, please refer to the quick guide shipped with your NVR.

Device Login

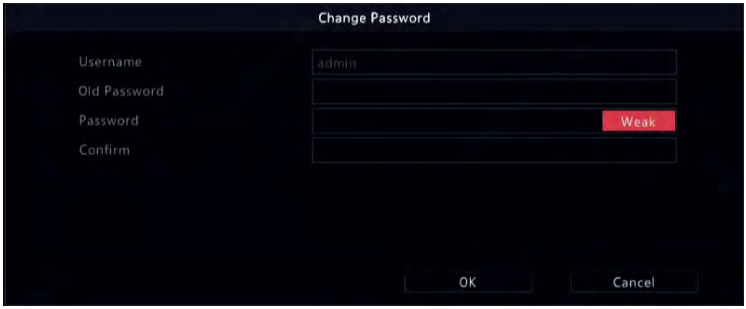
The login page appears after the NVR starts up.



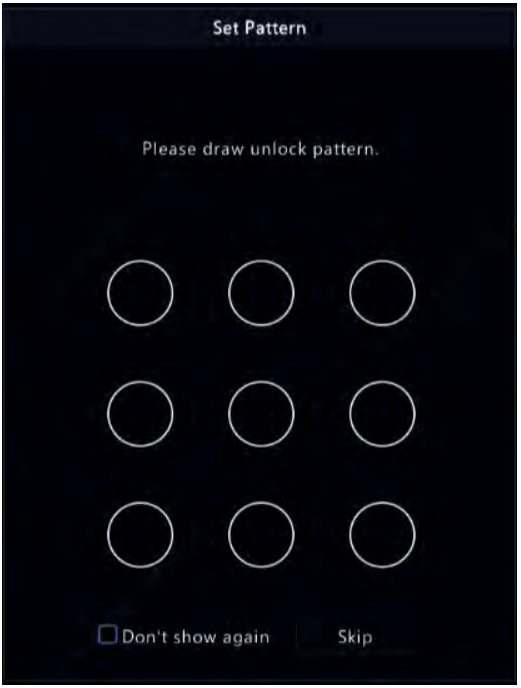
1. Enter the default *admin* password **123456**, click **Login**, and then click **Yes** to change the password.



2. Change the password into a strong one, then click **OK**.



3. Set the unlock pattern.



Note:

To disable unlock pattern, click **System > User**. See User Configuration for details.

Wizard

The wizard can guide you to complete the most basic setup. The following page appears after your login:



1. Enable or disable the wizard as needed and then click **Next**. You may also click [redacted].
2. Select the time zone, date and time format, set the system time, and then click **Next**.
3. Complete network configuration, and then click **Next**.
4. Select the devices to add in the discovered device list, click **Add**, and then click **Yes** to complete configuration.

Note:

- To add devices through PoE ports, see Option 3 in Adding an IP Device for details.
- The devices added can get online and start live view only if the device password is default; if not, you need to modify the device password.
- If the desired device is not in the device list, you may add it in a preview window or under **Camera > Camera > Camera** (see Adding an IP Device).

3 Live View

Live View Status

The following icons are used to indicate alarms, recording status, and audio status in a live view window.

Table 3–1 Live View Window Icons

Icon	Description
	Tampering alarm
	Motion detection alarm
	Recording
	Two-way audio

Window Toolbar

Icon	Description
	Available for PTZ cameras only. Click to display the PTZ control window.
	Set mount mode and display mode for fisheye camera. This icon appears only for fisheye cameras.
	Record live video in the window to the hard disk. Clicking  stops recording.
	Click to play video recorded during the past 5 minutes and 30 seconds.
	Zoom in on an area of interest.
	Click to edit image settings.
	Click to set OSD.
	Click to take a snapshot. The window borders will flash white. You may view and back up snapshots under **Backup > Image**.

Icon	Description
	Rest your mouse pointer on the icon to view bitrate info; click this button to view the camera ID and IP address or to change the username and password used to connect the camera.
	Start two-way audio with the camera. Click  to stop. The sound volume is adjustable. **Note:** Correct audio input and output connections are required.
	Click to turn on audio. Clicking  turns off audio. The sound volume is adjustable. **Note:** When you turn on audio in the current window, audio of the previous window is turned off.

Screen Toolbar

Icon	Description
	Click to access the main menu.
	Select the screen layout.
	Previous or next screen.
	Start or stop sequence.
	Playback.
	Rest the mouse pointer on this icon to view encoding information including frame rate, bit rate, and resolution; or click to view camera status.
	Click to view device alarm status and camera status.
	Rest the mouse pointer on it to view NIC card information. Or click this icon to edit basic network settings.
	Rest the mouse pointer on it to view the date. Or click this icon to edit time settings.
	Available to certain NVR models. Click to display the cloud service window. You may scan the QR code and download an app to manage your NVR.
	Click to automatically hide the toolbar, or click  to lock.

Shortcut Menu

A shortcut menu as shown below appears when you right-click in a window. Some menu items are described in Shortcut Menu Description.

Table 3–2 Shortcut Menu



Table 3–3 Shortcut Menu Description

Menu	Description
Menu	Access the main menu. Most of operations described in this manual are performed start from the main menu; for example, click **Camera > Camera** (with **Menu >** omitted).
Common Menu	Quick access to **Camera, Net Config,** and **Backup.**
Corridor	Choose a corridor mode. Corridor mode can also be set in the **Preview Windows** drop-down list under **System > Preview.** To display images in corridor mode, the camera must be installed correctly (rotated 90° clockwise or counterclockwise), and then use the **Image Rotation** parameter under **Camera > Image** to rotate images accordingly.
Main/Aux Monitor	Switch live video from different video output.
Preview Mode	Switch between **Normal** and **Smart**. The default is **Normal** mode.
Playback	Play the current day's recording for the camera linked to the current window.

Menu	Description
Output Mode	Choose a video output mode, including standard, soft, bright, and vivid.
Manual	Manual settings include manual recording, manual snapshot, and manual alarm.

Sequence Operation

The sequence operation requires you to configure the screen layout, windows, linked cameras, and the sequence interval.

This example describes how to configure sequence for five cameras based on a 4-window screen layout.

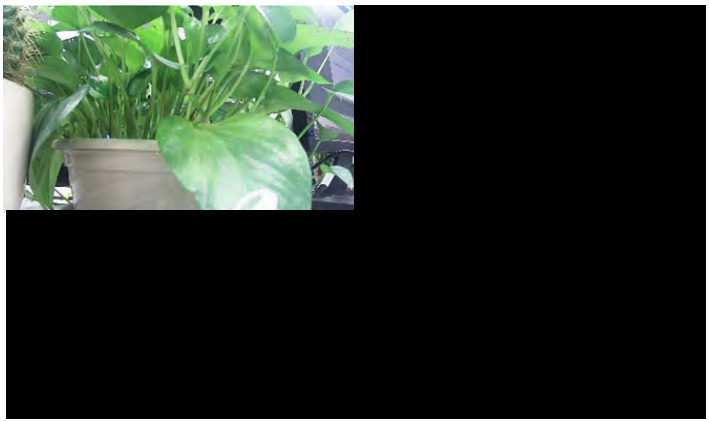
1. Click **4 Windows** on the screen toolbar.

NOTE!

The number of windows that can be displayed may vary with NVR model.

2. Click **Start Sequence** on the screen toolbar. Sequence starts by displaying four windows on the first screen and then the fifth on the second at the set interval.





NOTE!

- The default sequence interval is eight seconds and can be set under **System > Preview.**
- You may drag video to the desired window on the screen.

Zoom

Zoom in on an area of images in a window for details.

1. Click the window and then click on the window toolbar.



2. Move your mouse to the area you want to zoom in, then use your scroll wheel to zoom in and out.

3. Right click to exit zoom.

Image Configuration

Adjust image settings to get optimal images from a camera.

1. Click the window and then click  on the window toolbar.
2. Select a mode from the drop-down list according to the surveillance scenario, and then adjust contrast, hue, saturation and brightness as needed. The settings available may vary with device model.
3. Click **OK** to save the settings and exit.

Preview Configuration

Normally, live view (video) is available after you complete the basic setup by following the wizard. You can click **System > Preview** and edit preview setting as needed, including video output, image resolution, default layout, and sequence interval. The video output and the number of windows supported may vary with NVR model.



NOTE!

Pressing and holding the scroll wheel for at least 3 seconds will restore the default resolution.

Preview Configuration

Each preview window (window for short) links to a camera. By default, window 1 links to camera D1, window 2 links to camera D2, and so on. You may want to change the link to display live video from a camera in another specified window. The following example describes how to link window 1 to camera D2 and link window 2 to camera D1.

Step 1: Click window 1 on the right, and then click **D2** under **Camera** on the left. Now **D2** appears in window 1, and **None** appears in window 2. Meanwhile, ○ is cleared for camera D1, meaning D1 is not linked to any window.



Step 2: Click window 2 on the right, and then click **D1** under **Camera** on the left. Now **D1** appears in window 2. Click **Apply** to save the settings.



Advanced Configuration

Click the **Advanced** tab and then select **Sub Stream First** so the NVR uses the sub stream to establish live video from multiple cameras simultaneously. This function is disabled by default.

4 Channel Configuration

Channel Management

This chapter describes how to add and manage IP devices in your NVR. The IP devices mentioned in this manual mainly refer to IP camera (or network camera); sometimes they can also be Digital Video Server (DVS). Before you start, make sure the IP devices are connected to your NVR via network.

CAUTION!

An IP device should be connected to one NVR only. An IP device managed by multiple NVRs may cause unwanted issues.

Adding an IP Device

This section provides multiple options to add an IP device. Some options are only applicable to certain NVR models. Choose one as appropriate.

Option 1

1. Click **Camera > Camera > Camera**. The system automatically searches for IP devices and lists the discovered.
2. (Optional) To search a specified network segment, click **Search Segment** and then set the address range.
3. You may choose one of the following ways to add an IP device:

- Click **Add All** to add all the discovered IP devices allowed (depending on channels supported by the NVR).
- Click **Custom Add**. In the window displayed, enter the IP address and complete other settings, and then click **Add**. You may also click **Search Segment** and add discovered cameras in the list.

NOTE!

For a Digital Video Server (DVS), a window appears when you click **Add**, and you need to select channels to add the connected cameras.

Option 2

This option is not applicable to NVRs with PoE ports or switching ports.

1. Click  in a window.
2. Select the desired IP device and then click **Add**.

Option 3

This option is only applicable to NVRs with PoE ports or switching ports. Connect an IP camera to a PoE port or a switching port with a network cable. The connected camera will be added to the NVR automatically. Check status under **Camera > Camera > Camera.**  means live video from the camera is available. Click  to view live video.

If the camera is connected via a network switch, click  under **Cam Config** in the window displayed, set **Add Mode** to **Manual** and then complete the settings correctly.

NOTE!

 appears under **Status** if the power output from a PoE port is below or above the rated power of the connected camera.

Option 4

Use this option to add an IP device that is connected to a different router, for example, when the NVR and the IP device are connected across the Internet.

NOTE!

First you need to enable port mapping at **Setup > Port > Port Mapping** on the IP device's Web interface.

1. Click **Camera > Camera,** click **Custom Add**.
2. Choose an option:

- By IP

  a. On the IP device's Web interface, go to **Setup > Port > Port Mapping,** find the external IP (public IP) and external port number.

  b. On the NVR: Select a protocol, enter the above-mentioned IP address and port number, enter the username and password.

  c. Click **OK**.

- By MyDDNS

  a. On the IP device's Web interface, go to Setup > Network > DDNS, enable DDNS, select MyDDNS, set a domain name and get the server address.

NOTE!

- After setting the domain name, check that you can use the device address to access the IP device's Web interface.
- Make sure the MyDDNS server and the NVR are connected (ping the MyDDNS server from the NVR).

  b. On the NVR: Select a protocol, enter the above-mentioned server address, domain name, username and password.

  c. Click **OK.**

- By a domain name

a. On the IP device's Web interface, go to **Setup > Network > DDNS,** enable DDNS, select **DynDNS** or **NO-IP**, enter the domain name that you set up on the DNS website, enter the username and password, and then click **Save**.

b. On the NVR: Select a protocol, enter the domain name mentioned above, and then enter the username and password. The port is the external port of the IP device.

c. Click **OK.**



NOTE!

- If **Custom** is selected for **Protocol**, the port is the mapped external RTSP port of the IP device.
- Do not add an IP device to an NVR using different methods (e.g., IP and MyDDNS) at the same time.
- When an IP device is added by MyDDNS, domain name (NO-IP or DynDNS), or IP (public IP+public port) and it is not connected to the same router as the NVR, alarm is configurable, but alarm push is not available.

Option 5

Use this option only when the IP device to add supports the standard RTSP, and all you need from the IP device are just view live and playback. IP devices added in this way cannot be configured from the NVR.

1. Click **Camera > Camera.**
2. Click **Custom Add**.
3. Click to select a camera in the list, select **Custom** from the **Protocol** drop-down list, and then click the **Protocol** button.
4. In the **Protocol** window, name the protocol, enter the RTSP port number, select a transmission protocol, input the resource paths, and then click **Apply**.

NOTE!

Contact the camera manufacturer for resource paths.

5. Edit settings in the **Add/Modify** window as needed, including the IP address, username and password, and then click **Add**. Check status in the camera list.

Managing an IP Device

Manage IP devices under **Camera > Camera > Camera.**

- Click  to edit settings including the protocol, IP address, port number, username and password. The **Camera IP** field displays the IP address that the current channel links to, and you may change the address so the channel links to another device. The username and password must be consistent with that of the IP camera.
- Click  to delete an IP device, or select multiple IP devices and then click **Delete**. Channels corresponding to PoE ports or switching ports cannot be deleted.
- Click  to change the IP address of an IP camera and the default gateway. A DVS' IP address cannot be editted from the NVR. ⁻ means this function is not available.

Sort Cameras

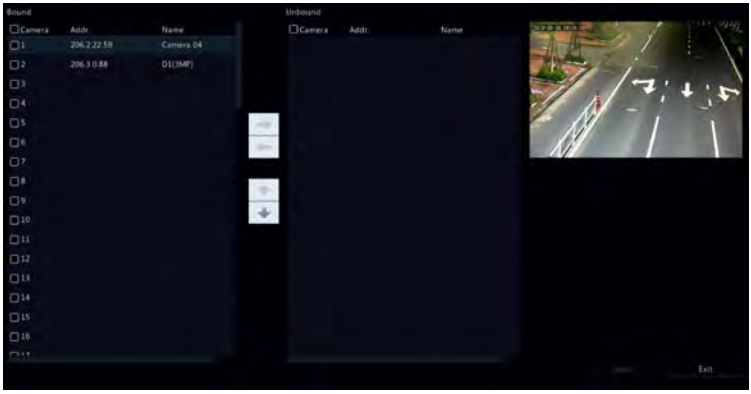
Sort cameras to display in the desired order.

NOTE!

- This function is unavailable to NVRs with PoE ports or switching ports.
- This chapter describes how to sort cameras on an NVR with more than 32 channels. For NVRs with 32 channels or less, you can sort cameras by dragging the mouse.

For example, to switch channel 1 with channel 4, click **Sort Camera**, and then follow the steps below:

1. In the left list, select the check box for channel 1, and then click . Channel 1 now appears in the right list. Perform the same operations to channel 4.
2. In the right list, select channel 4 and then click . Now channel 4 appears at the previous line of channel 1 in the list. Perform the same operations to channel 1, so channel 1 appears at the previous line of channel 4 in the list.
3. Click **Apply** to save the setting, and then click **Yes**.



NOTE!

- To move a channel left or right, select the check box first; otherwise, the buttons are grayed.
- To move a channel up or down, click the channel first; otherwise, the buttons are grayed.
- A channel will be inserted to the first blank line in the left list unless you specified another line in the list by selecting the corresponding check box.
- **Save** cannot be clicked when the right list is not empty. You need to clear the list first.

Fisheye Configuration

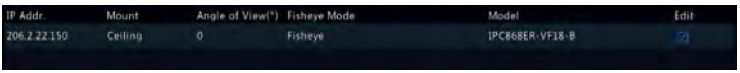
Only certain NVR models can dewarp images from fisheye cameras.

NOTE!

Fisheye configuration is supported only by certain fisheye cameras.

Configuration

1. Click **Camera > Camera > Fisheye.**



2. Click  under **Edit**. The **Fisheye** window appears.
3. Select a correct mounting mode and complete other settings accordingly.
4. Click **OK**.

Dewarping

NOTE!

Dewarping is available in live view and playback (in normal and corridor playback modes). The operations are similar. The following describes dewarping in live view.

Click **Fisheye Mode** on the window toolbar. The figure below appears. Set mounting mode and display mode.

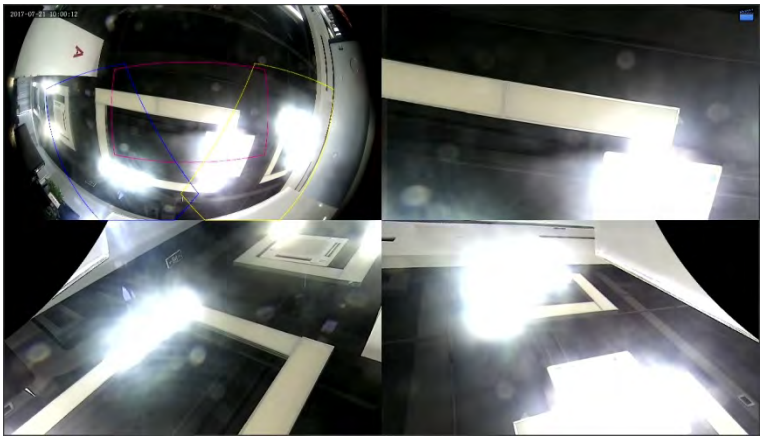


Three mounting modes are available: ceiling, wall, desktop. Ceiling and desktop mounting modes use the same dewarping method.

Mounting Mode	Display Mode	Description
Ceiling mount  Desktop mount 		Original Image
		360° Panoramic+1PTZ
		180° Panoramic
		Fisheye+3PTZ
		Fisheye+4PTZ

Mounting Mode	Display Mode	Description
		360° Panoramic+6PTZ
		Fisheye+8PTZ
Wall mount 		Original Image
		Panoramic
		Panoramic+3PTZ
		Panoramic+4PTZ
		Panoramic+8PTZ

Operations Example: Ceiling Mount and Fisheye+3PTZ camera



On a PTZ image, drag the mouse to rotate the image or use the scroll wheel to zoom in or out. A box appears on the fisheye image as the image rotates, and as you drag the box or move the scroll wheel on the fisheye image, the corresponding PTZ image rotates or zooms in or out as well.

Advanced Functions

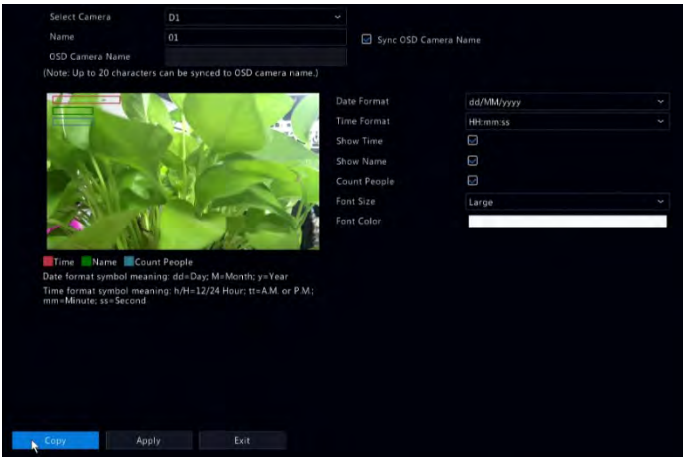
Upgrade connected IP cameras or restore factory default settings for cameras under **Camera > Camera > Advanced.**

Click **Check** to see if the version of the connected IP camera is up to date. You may upgrade cameras by cloud ( ) or by disk ( ) one by one, or select multiple cameras and then click **Upgrade by Cloud** or **By Disk** to upgrade cameras in batches.

OSD Configuration

On Screen Display (OSD) are characters displayed with video images, for example, camera name, date and time, and people counting statistics.

Click Camera > OSD; or click OSD on the preview window toolbar.



1. Select the desired camera.
2. Set camera name to display. Enable **Show Name** first, and set OSD camera name as needed:

- If camera name is less than 20 characters, and camera name and **OSD Camera Name** (i.e., the camera name you want to overlay on video image) are same:

a. Select **Sync OSD Camera Name**, then the OSD name will be synchronized with the camera name. This function is enabled by default.

b. Enter the camera name in the **Name** field. The name will be displayed on video image.

NOTE!

If camera name exceeds 20 characters, only the first 20 characters will be used as the OSD camera name.

- If camera name exceeds 20 characters, and you want to overlay a different camera name on video image:
  a. Deselect **Sync OSD Camera Name**.
  b. Enter the camera name in **Name** field.
  c. Enter the OSD camera name.

3. Set time to display. Select **Show Time**, and select date and time formats.
4. Set people counting statistics to display. Select **Count People**. You need to configure people counting function first. See People Counting for details.
5. Set font size and color as needed.

NOTE!

You may click **Copy** to apply the same settings to other cameras.

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

Image Configuration

1. Click **Camera > Image.**
2. Select the desired camera and scene.



3. Adjust settings on the tabs as needed to achieve optimal images. See the following sections for detailed information.

NOTE!

- A scene can be selected only when supported by the IP camera.
- To restore default image settings, click **Default** in the lower right corner. This function is available only when the camera is connected to the NVR via the private protocol.
- Image settings apply to both live and recorded videos.

Image enhancement

1. Click the **Image Enhancement** tab.
2. Adjust the settings as needed. Some important parameters are described in the table below.

Parameter	Description
Brightness	The greater the value, the brighter the images appear.
Saturation	The amount of color in a specified hue.
Contrast	The degree of difference between the lightest (white) and darkest (black) parts of an image. Setting a greater value increases contrast.
Hue	Purity of colors in an image.
Sharpness	Contrast of boundaries of objects in an image.
Noise Reduction	Reduce noises in images to improve image quality.

Parameter	Description
Image Rotation	• Normal: Displays images without rotation. • Flip Vertical: Displays images flipped vertically. • Flip Horizontal: Displays images flipped horizontally. • 180°: Displays images flipped vertically and horizontally. • 90° CW and 90° CCW: Display images in corridor format. The camera must be installed correctly (rotated 90° clockwise or counterclockwise).

Exposure

1. Click the **Exposure** tab.



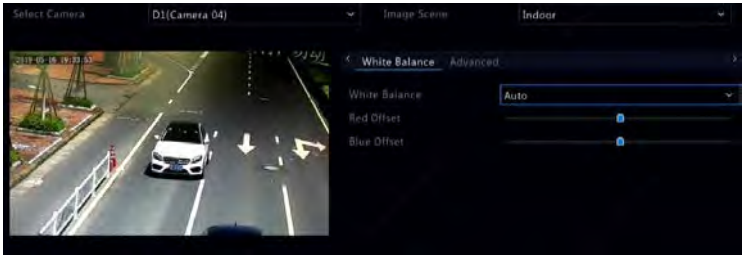
2. Adjust the settings as needed. Some important parameters are described in the table below.

Parameter	Description
Exposure Mode	Select the correct exposure mode to achieve the desired exposure effect.
Shutter(s)	Shutter is used to control the light that comes into the lens. A fast shutter speed is ideal for scenes in quick motion. A slow shutter speed is ideal for scenes that change slowly.

Parameter	Description
Gain(dB)	Control image signals so that the camera can output standard video signals in different light conditions.
Iris	Adjust iris opening of the lens to control the amount of incoming light.
Slow Shutter	Improves image brightness in low light conditions.
Slowest Shutter	Set the slowest shutter speed for the camera during exposure.
Compensation	Adjust the compensation value as required to achieve the desired image effects.
Day/Night Mode	• **Automatic**: In this mode, the camera can automatically switch between night mode and day mode according to the ambient lighting condition to output optimum images. • **Night**: The camera outputs high-quality black and white images according to the ambient lighting condition. • **Day**: The camera outputs high-quality color images according to the ambient lighting condition.
Day/Night Sensitivity	Light threshold for switching between day mode and night mode. A higher sensitivity value means that the camera is more sensitive to the change of light and is therefore more easily to switch between day mode and night mode.
Day/Night Switching(s)	Set the length of time before the camera switches between day mode and night mode after the switching conditions are met.
WDR	Enable WDR to ensure clear images in high contrast conditions.
WDR Level	After enabling WDR, you can improve image quality by adjusting the WDR level.

White balance

1. Click the **White Balance** tab.

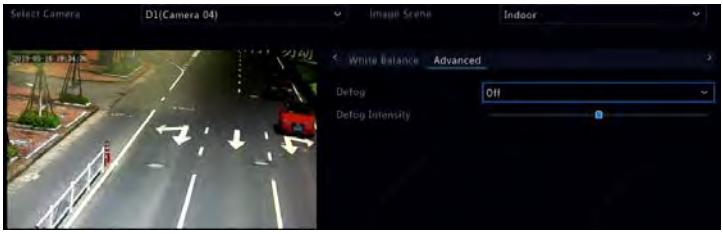


2. Adjust the settings on this tab. Some important parameters are described in the table below.

Parameter	Description
White Balance	Adjust the red or blue offset of the image: ● **Auto**: The camera adjusts the red or blue offset automatically according to the lighting condition (the color tends to be blue). ● **Finetune**: Allow you to adjust the red or blue offset manually.
Red Offset	Adjust the red offset manually.
Blue Offset	Adjust the blue offset manually.

Advanced settings

1. Click the **Advanced** tab.
2. Use defog to improve image quality in foggy days.

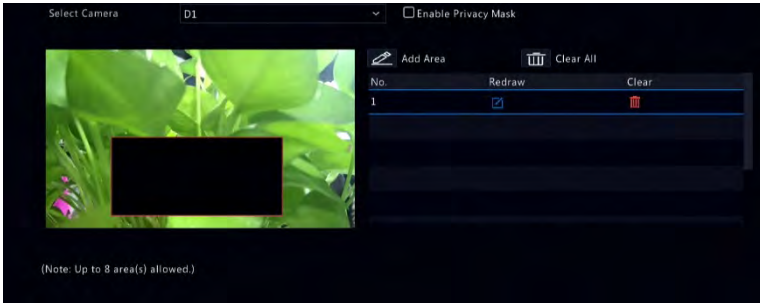


Privacy Mask Configuration

A privacy mask is an area of solid color covering certain parts of the monitored area. Privacy mask protects specified areas of

images from being viewed and recorded. Multiple mask areas are allowed.

1. Click **Camera > Privacy Mask.**
2. Select the desired camera, select **Enable Privacy Mask**, click **Add Area** and then use the mouse to specify areas to mask. Up to eight areas are allowed. The areas are differentiated by different colors.



3. (Optional) To clear a mask area, click .
4. Click **Apply** to save the settings.

5 PTZ Control

PTZ (pan, tilt and zoom) control is applicable to PTZ cameras only and may vary depending on the functions and protocols supported by the PTZ cameras. Refer to PTZ camera specifications for more details.

PTZ Control Window and PTZ Management Window

1. Click  on the window toolbar. The **PTZ Control** window appears. See PTZ Control Window Buttons for detailed descriptions.
2. Click the **Set** button. The **PTZ Management** window appears (can also be opened by clicking **Camera > PTZ**).

Table 5–1 PTZ Control Window Buttons

Button	Description
	Control the rotation direction of the PTZ camera or stop rotation.
	Adjust the zoom, focus, and iris of the PTZ camera. **Note:** You can also zoom in or out using the scroll wheel on your mouse.
	Control the rotation speed of the camera. 1 means the slowest, and 9 means the fastest.
	Click to display the **PTZ Management** window.
	• Turn on/off the light. • Turn on/off the wiper. • Use 3D positioning. • Turn on/off the heater.

Button	Description
	• Turn on/off the function to remove snow. • Turn on/off PTZ shortcut operations. **Note:** • Check that the 3D positioning, heater and snow removal functions are supported by the camera before using. • Use 3D positioning to zoom in or out. Dragging from top down zooms in. Dragging the other way zooms out.
	Preset button.
	• Call a preset so the PTZ camera goes to the preset position. • Delete a preset **Note:**  and  are displayed for saved presets only.
	Preset patrol, recorded patrol and auto guard. For detailed information, see Setting a Preset Patrol, Setting a Recorded Patrol, and Setting Auto Guard.
	Start or stop.

Setting and Calling a Preset

A preset position (preset for short), is a saved view used to quickly steer the PTZ camera to a specific position. A preset consists of the following settings: pan and tilt positions, zoom, focus, and iris.

1. Access the **PTZ Management** window. For the detailed steps, see PTZ Control Window and PTZ Management Window.



2. Add presets.
   a. Click the directional buttons to steer the PTZ camera to the desired position.
   b. Adjust the zoom, focus, and iris as needed.
   c. Select a preset number not in use, and then click under **Edit**.
   d. Repeat the above steps to add all the presets.
3. To call a preset, click for the corresponding number. The camera rotates to the preset position.

NOTE!

Presets can also be triggered by alarms. See Alarm-Triggered Actions for details.

Setting a Preset Patrol

Set the PTZ camera to patrol by presets (go from one preset to the next in specified order). Set presets first and then select some as keypoints.

Up to four patrol routes (Preset Patrol 1, 2, 3 and 4) are allowed for each PTZ camera. Each patrol route can have up to eight presets (keypoints).

After setting presets, follow the steps to set a preset patrol. The following uses preset patrol 1 as an example.

1. In the **PTZ Management** window, click . A window is displayed as follows.



2. Select a preset from the drop-down list, set the duration (time the camera stays at the preset, unit: second), and then set the rotation speed (1: slowest, 9: fastest). Click **OK** to save the settings. The preset is added as a keypoint.
3. Repeat the above steps to add all presets (keypoints), and adjust the sequence of these presets by clicking 

or 

. Modify or delete a preset by clicking  or . Clicking 

will delete all the added keypoints.
4. After completing the configuration, click **Apply** to save the settings. Now keypoints for preset patrol 1 is complete.
5. Click  right to the drop-down list to start preset patrol 1. To stop, click .

NOTE!

The duration ranges from 0 to 1800 seconds (default: 10). The rotation speed ranges from 1 to 9 levels (default: 5).

Setting a Recorded Patrol

This function requires the camera's support. The drop-down list and the buttons on the right are hidden if this function is not supported by the camera. Currently only one recorded patrol route is allowed.

Record a patrol, including the patrol route, the time that the camera stays at a certain direction, rotation speed, zoom, focus and focus.

1. Click to start recording. Steer the camera to the desired directions, adjust the zoom, focus, iris as needed during the process.



2. Click to stop recording. All the patrol actions have been recorded.

3. To start the recorded patrol, click . Click to stop.

Setting Auto Guard

The auto guard function instructs the PTZ camera to automatically perform a pre-configured operation after some period of inactivity.

This function is available in some cameras. The **Auto Guard** tab is hidden if it is not supported.

1. Click **Auto Guard** and then select **Enable**.
2. Select the desired mode from the drop-down list and then complete other settings accordingly. Click **Apply** to save the settings.



6 Recording and Snapshot

Video recording has different levels of priority, which from high to low is: event recording, manual recording, and scheduled recording.

Encoding Settings

Recording

The parameters and options displayed may vary with camera model and version. Some functions may be unavailable if the camera version is too low. In this case, you need to upgrade the camera first.

1. Click **Camera > Encoding.**



Select the camera and then edit settings as needed. Some parameters are described in the table below.

Table 6–1 Encoding Settings

Parameter	Description
Storage Mode	Five storage modes are available: Main Stream, Sub Stream, Main and Sub Stream, Main and Third Stream, Sub and Third Stream. **Note:** Only certain models support all the five modes.
Capture Mode	Combinations of resolutions and frame rates. **Note:** This parameter is effective only when the camera is connected to the NVR via the private protocol.
Stream Type	• **Normal**: main stream is intended for scheduled recording. • **Event**: main stream is intended for recording triggered by events such as alarm inputs or motion detection alarms. • **Sub Stream**: low resolution video is intended for local or remote real-time monitoring.
Video Compression	Video compression standard, for example, H.264, H.265. The listed options depend on the standards supported by the camera.
Resolution	Image resolution.
Bitrate Type	• **CBR**: Constant Bit Rate (CBR) is used to maintain a specific bit rate by varying the quality of video streams. CBR is preferred when limited bandwidth is available. The disadvantage is that video quality will vary and may decrease significantly with increased motion in the scene. • **VBR**: When using Variable Bit Rate (VBR), video quality is kept as constant as possible, at the cost of a varying bit rate, regardless of whether or not there is motion in the image. VBR is ideal when

Parameter	Description
	high quality is a requirement, especially when there is motion in the picture.
Bit Rate(Kbps)	Number of bits transferred per second. Select a value or select **Custom** and then set a value as needed.
Range	Bit rate range. Currently the range is fixed.
Frame Rate(fps)	Number of frames per second.
Image Quality	This parameter is effective only when **Bitrate Type** is set to **VBR**. 9 levels are provided.
I Frame Interval	Number of frames between two adjacent I frames.
I Frame Range	Range of I frames. Currently the range is fixed.
Smoothing	Use the slider to control the sudden increase of bit rate.
Audio Stream	Enable or disable audio stream.
Smart Encoding	The advanced mode achieves higher compression ratios.

2. (Optional) Click **Copy** to apply some current settings such as bit rate and frame rate to other cameras.
3. Click **Apply** to save the settings.

Snapshot

Set resolution, image quality and snapshot interval for snapshots taken according to schedule or triggered by an event.

1. Click **Camera > Snapshot.**
2. Set the parameters as needed.



NOTE!

- Scheduled snapshot uses the **Normal** type of schedule. Event-triggered snapshot is triggered by an event such as an alarm input and a motion detection alarm. Settings effective to event-triggered snapshot also apply to manual snapshot.
- Snapshot interval is the length of time between two snapshots.

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

Draw or Edit a Schedule

Make a recording or snapshot schedule by drawing (pressing and dragging) or by editing (using the **Edit** button). The operations for recording and snapshot are similar, so this section only describes how to make a recording schedule.

1. Click **Storage > Recording.**
2. Select the camera from the list. Schedule is enabled by default. If it is disabled, select to enable it.
3. Set **Pre-Record** and **Post-Record** as needed.
4. (Applicable to some NVR models) To save a redundant copy of recordings, select **Enable Redundant Recording** and configure a redundant hard disk (see Disk Management for details).



5. Click a color icon on the right under the **Edit** button and then draw a schedule on the left. You may also click **Edit** and set schedule details in the **Edit Schedule** window.

NOTE!

When editing a schedule, you may clear the **All Day** check box and set up to eight different periods for each day. To apply the settings to other day(s), select the day(s) right to **Copy To**.

6. Click **Apply**.
7. (Optional) Click **Copy** to apply the same settings to other cameras.

Scheduled Recording and Snapshot

Scheduled Recording

Scheduled recording records video according to the set schedule. It is different from manual recording and alarm-triggered recording. A 24×7 recording schedule is enabled by default and may be edited as needed to record video in specified periods only.

See Draw or Edit a Schedule for the detailed steps. Make sure the schedule type is **Normal**. The set schedule appears in blue, which stands for scheduled recording.

Scheduled Snapshot

Configure scheduled snapshot under **Storage > Snapshot.** Scheduled snapshot is similar to scheduled recording (see Scheduled Recording for details). Make sure the schedule type is **Normal**.

Motion Detection Recording and Snapshot

When enabled, a motion detection alarm occurs if an object inside the detection area moves to a certain extent (see Motion Detection for more details). Motion detection alarms can trigger actions including recording and snapshot.

Motion Detection Recording

1. Click **Alarm > Motion.**
2. Select the camera from the list, and then select the check box to enable motion detection.

NOTE!

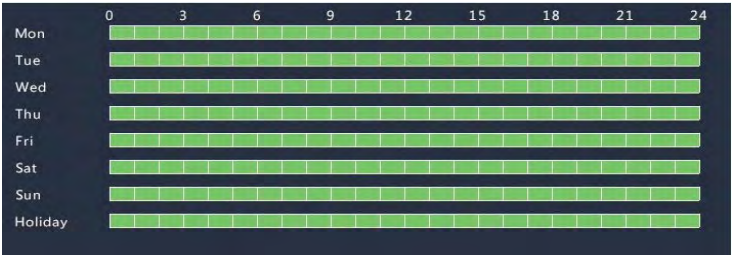
- Motion detection is enabled on the NVR by default. Unless modified, the detection area covers the full screen, and recording is triggered only for the current camera. The settings remain if you disable motion detection and then enable it.
- An alarm icon appears in the upper right corner when motion is detected.

3. In the preview window on the left side, click and drag your mouse to specify a motion detection area (red grid). Use the slider to adjust detection sensitivity.



4. Configure motion detection recording: click  right to **Trigger Actions**, click the **Recording** tab, select the desired camera, and then click **OK**.
5. (Optional) Configure an arming schedule (time when actions will be triggered): click  right to **Arming Schedule** and then set time periods as needed.
6. Set a recording schedule under **Storage > Recording**. For the detailed steps, see Draw or Edit a Schedule. Make sure the schedule type is **Motion**. The set schedule appears in green,

which stands for motion detection recording. The following figure shows an example.



Motion Detection Snapshot

Motion detection snapshot is similar to motion detection recording. Enable and configure motion detection alarm first (see steps 1 to 3 in Motion Detection Recording for details), and then proceed with the following steps.

1. Set motion detection snapshot under **Alarm > Motion:** click  right to **Trigger Actions**. In the window displayed, click the **Snapshot** tab, select the desired camera, and then click **OK**.
2. Set a snapshot schedule under **Storage > Snapshot.** For the detailed steps, see Draw or Edit a Schedule. Make sure the schedule type is **Motion**.

Alarm Triggered Recording and Snapshot

Set input alarms to trigger recording and snapshot. See Alarm Input and Output for more details.

Alarm Triggered Recording

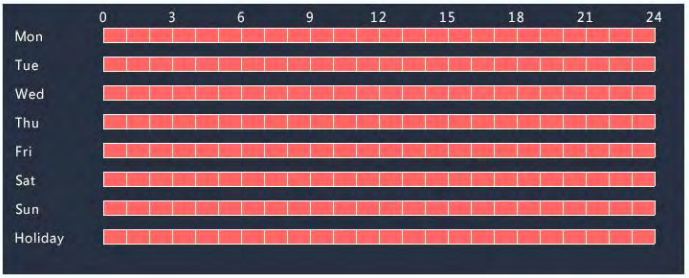
1. Click **Alarm > Input/Output > Alarm Input.**
2. Set alarm input: click  for the desired camera. In the window displayed, select **Enable**, select N.O. (normally open) or N.C. (normally closed) trigger mode, and then click **OK**.



NOTE!

To apply the same settings to other camera(s), click **Copy** and then select the desired camera(s).

3. Set alarm triggered recording: click  under **Trigger Actions**. In the window displayed, click the **Recording** tab, select the desired camera, and then click **OK**.
4. Set a schedule under **Storage > Recording**. For the detailed steps, see Draw or Edit a Schedule. Make sure the schedule type is **Alarm**. The set schedule appears in red, which stands for alarm-triggered recording. The following shows an example.



Alarm Triggered Snapshot

Alarm triggered snapshot is similar to alarm triggered recording. Enable and configure alarm input first (see steps 1 to 2 in Alarm Triggered Recording for details), and then proceed with the following steps.

1. Set alarm triggered snapshot: Click  under **Trigger Actions**.

   In the window displayed, click the **Snapshot** tab, select the desired camera, and then click **OK**.

2. Set a snapshot schedule under **Storage > Snapshot**. For the detailed steps, see Draw or Edit a Schedule. Make sure the schedule type is **Alarm**.

Manual Recording and Snapshot

Manual Recording

Right click on the preview window, select **Manual** in the shortcut menu. Click the **Manual Recording** tab, select the desired camera and then click **Start**. To stop manual recording, select the camera and then click **Stop**.



Manual Snapshot

Manual snapshot is similar to manual recording. Right click and select **Manual > Manual Snapshot,** select the desired camera, and then click **Start**. Click **Stop** to stop.

Holiday Recording and Snapshot

Holiday recording and snapshot allows you to specify certain time periods as holidays for scheduled recording and snapshot. Specify

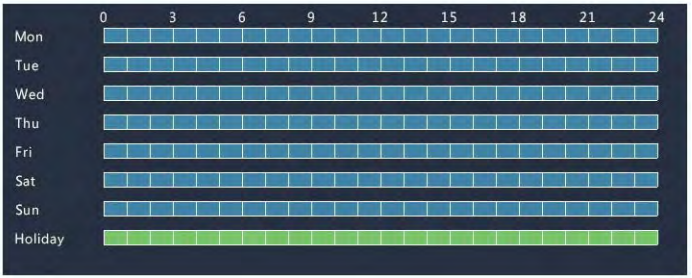
certain date(s) as holidays first, and then configure recording or snapshot schedules for these days.

Holiday Recording

1. Click **System > Time > Holiday.**
2. Click the **Add** button in the lower right corner. The **Holiday** window is displayed. Complete the settings including the holiday name, start and end dates. By default a holiday is enabled when added and does not repeat.



3. Click **OK**. The holiday appears in the list.
4. Click **Storage > Recording** and then set a recording schedule as described in Draw or Edit a Schedule. Make sure **Holiday** is selected in the **Select Day** drop-down list. In the following example, motion detection recording is enabled on the set holiday.



Holiday Snapshot

Holiday snapshot is similar to holiday recording. First you set holidays under **System > Time > Holiday,** and then configure a snapshot schedule under **Storage > Snapshot.** Set a snapshot schedule as described in Scheduled Recording. Make sure **Holiday** is selected from the **Select Day** drop-down list.

Other Recording and Snapshot Types

Other recording and snapshot types:

- **Event**: Including the types below and VCA. Any of these types will trigger event recording/snapshot.
- **Motion detection and alarm** triggered (**M and A** for short): recording or snapshot is triggered only when a motion detection alarm AND an input alarm occur simultaneously.
- **Motion detection or alarm** triggered (**M or A** for short): recording or snapshot is triggered when a motion detection alarm OR an input alarm occurs.

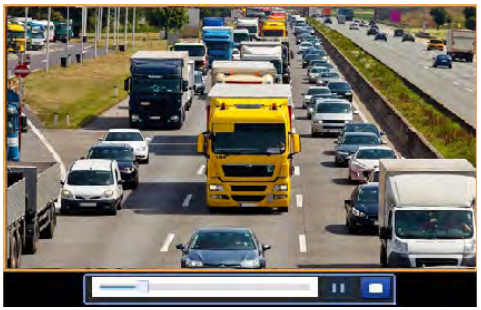
When you choose an Event type of recording or snapshot, enable the corresponding alarm function and configured alarm-triggered recording/snapshot. The configuration steps are similar. See Motion Detection Recording and Snapshot for more details.

7 Playback

Instant Playback

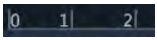
Instant playback plays the video recorded during the last 5 minutes and 30 seconds. If no recording is found, there is no recording during this period.

1. Click the desired window, and then click  on the toolbar to start instant playback.
2. You may drag the slider to control the progress. Pause and resume as needed.



Playback Toolbar

Table 7–1 Playback Toolbar Buttons

Button	Description
	Show playback progress. **Note**: • A small window displaying video of the selected window is displayed as you drag the slider, helping locate the part of the video you want to view. • The first progress bar indicates playback progress of the video playing in the highlighted window. The second indicates the overall playback progress for all the selected cameras.
	Timeline.
	Zoom in or out on the timeline. **Note:** Alternatively, scroll your mouse wheel.
	Play, pause, stop, and reverse.
	Rewind or forward 30 seconds.
	Slow down or speed up. **Note:** Click  to restore the normal playback speed after clicking , and vice versa.
	Forward by frame.
	Start or stop clipping video.
	Take a snapshot. The window borders will flash white.
	Lock.
	Manage files (clips, snapshots, locked files, tags).

Button	Description
	Zoom in on images. For more details, see Zoom.
	Set fisheye mounting mode and display mode.
	Enable/disable POS (available to certain NVR models). When enabled, POS OSD appears on the screen, and some toolbar buttons are deactivated. These buttons only appear in two playback modes: playback by camera and data and playback by POS. POS OSD duration (how long POS OSD appears on screen) varies with playback mode. For playback by camera and date, the duration is fixed to 5 seconds. For playback by POS, the duration is configurable. See Playback by Camera and Date and Playback by POS for more details.
	Turn off/on audio.
	Adjust sound volume for the current window.

Playback by Camera and Date

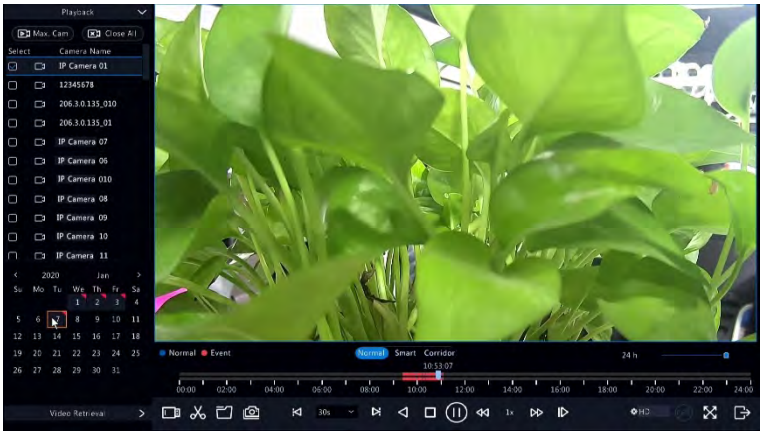
Use this method to search and play recordings by camera and date.

1. Click on the preview window, then right click and choose **Playback** to start playback.

NOTE!

In playback window, you can select multiple cameras for synchronous playback. Clicking **Max. Camera** selects the maximum number of cameras allowed, and clicking **Close All** stops playback for all cameras. The performance varies with NVR model.

2. Select the desired date on the calendar and then click to start playback. Double-clicking the date will start playback directly.



NOTE!

- The calendar uses different flags to indicate different recording types. No flag means no recording. The blue flag means normal recording. The red flag means event-triggered recording.
- In the drop-down list right to playback mode: **HD** means video recorded with the main or sub stream; **SD** means video recorded with the third stream.

Playback in Corridor Mode

Play recordings in corridor mode in multiple windows.

1. In the playback window, select **Corridor** above the progress bar.
2. Select cameras and then double-click the desired date to start playback.

Playback by Tag

Add tags named with keywords such as event name and location to a recording and use tags to quickly locate the part of the video you need during playback.

Adding a Tag

1. Right-click and then click choose **Playback**.
2. Click  on the window toolbar, and then set the tag name.
3. To manage the added tags, click  on the screen toolbar, and then rename or delete tags as needed.

Playback by Tag

1. In the playback window, click **Video Retrieval**, select **Tag Search** from the drop-down list in the upper left corner.
2. Select cameras, set the time period, and then click **Search**. Search results, if there are any, are displayed with names of cameras and tags.
3. Click  for the desired tag to start playback. You may use the **Start Before** and **Stop After** drop-down lists to set when the tagged video starts and ends.

Playback by Motion Detection

Search for and play recordings triggered by motion detection during a specified time period.

NOTE!

Make sure motion detection is enabled and alarm-triggered recording has been configured before you use this function. See Motion Detection and Alarm-Triggered Actions for details.

1. In the playback window, click **Video Retrieval**, select **Motion** from the drop-down list in the upper left corner.
2. Select the desired camera, set the time period, and then click **Search**.
3. Click  for the desired recording to start playback.

Playback by Video Loss

Search for and play recordings triggered by video loss during a specified time period.

NOTE!

Make sure video loss alarm is enabled and alarm-triggered recording has been configured before you use this function. See Video Loss and Alarm-Triggered Actions for details.

1. In the playback window, click **Video Retrieval**, select **Video Loss** from the drop-down list in the upper left corner.
2. Select the desired camera, set the time period, and then click **Search**.
3. Click  for the desired recording to start playback.

Playback by Smart Search

This function provides an efficient way to review recordings containing smart search results such as detected motions. In smart playback mode, the system analyzes recordings for smart

search results. If such results are detected, the progress bar is highlighted in green, and the video plays at the normal speed, allowing you enough time to catch details; otherwise, the video plays at 16x speed to save time.

1. In the playback window, select **Smart** above the progress bar.
2. Click  for the desired camera to start smart playback.
3. Click . The smart search window is displayed. By default, the full screen is the smart search area. To clear all, click ; to restore the full-screen search area, click .
4. Set smart search rules, including detection area and sensitivity.
5. Click  to start search. To quit, click .

Playback by External File

Use this function to play recordings stored in an external storage device, for example, a USB drive or a portable USB hard drive.

1. In the playback window, click  on the screen toolbar.
2. Click **Refresh** and then wait for the NVR to read the external storage device.
3. Select the desired recording file and then click  to start playback.

Playback by Image

Specify an image type (for example, Normal or Motion) to search for and play images from one or more cameras during a specified time period.

1. In the playback window, click **Video Retrieval**, select **Picture Search** from the drop-down list in the upper left corner.
2. Select a type from the **Type** drop-down list in the upper right corner.
3. Select the desired camera(s), set the desired time period, and then click **Search**.
4. Click the desired file to start playback.

Playback by POS

Use this function to play recordings of a POS machine.

1. In the playback window, click **Video Retrieval**, select **POS Search** from the drop-down list in the upper left corner.
2. Select the desired camera, set the time period, enter keywords and then click **Search**.



NOTE!

Keywords allow special characters & (means AND) and | (means OR).

3. Click  to display overlay content.
4. Click  to start playback.

File Management

File management allows you to manage video clips, tags, snapshots taken during playback, and lock or unlock files.

1. Take snapshot during playback.

a. In playback page, play the recording until the desired image appears.

b. Click  in the playback window to take a snapshot.

c. Click  and then click the **Playback Image** tab to view the snapshot.

d. Select the desired image file(s) and then click **Backup** to save them to the storage device.



NOTE!

The image resolution depends on the resolution from the output interface and the number of windows displayed when the snapshot is taken.

2. Lock files. Use this function to lock a recording file so it will not be overwritten. To lock a recording file will prevent all the files stored in the same disk partition (254.4MB in size) from being overwritten.

a. Play the recording you want to lock.

b. Click  in the playback window.

c. Click  and then click the **Locked File** tab to view the locked file. To unlock a file, click , and the icon changes to . To back up a file, select the file and then click **Backup**.

8 Backup

Recording Backup

Backup, also known as recording backup, is the process of querying video stored on a hard disk of the NVR and then saving to a USB storage device or a DVD-R disc as a file.

Recording backup has the following conditions:

- Back up using a USB storage device: format the partition in FAT32 or NTFS format; connect the storage device correctly to the NVR.
- Back up using a disc: use a GP65NB60 DVD burner. Make sure the DVD-R disc is empty, and the burner is correctly connected to the NVR.
- Permission is required.
- The recording to back up is stored on a hard disk of the NVR.

NOTE!

- The default file format is .mp4 when you back up recordings to a USB storage device.
- When backing up using a disc, recordings are saved as .TS files only.

Normal Backup

1. Click **Backup > Recording.** All cameras are selected by default.
2. Set search conditions and then click **Search**. Search results are displayed.

NOTE!

You can lock/unlock and play recording files in this window.

3. Select the desired recording(s) and then click **Backup**.

4. Select a partition.

   - Back up to USB storage device. Set the destination in the USB storage device and then click **Backup**. The recording(s) will be saved to the specified directory.



NOTE!

- You may want to create a new folder for the recording(s) by clicking **New Folder**.
- If the connected storage device has a capacity that is greater than 2T, clicking **Format** will format the device to NTFS file system; if the capacity is 2T or less, the device will be formatted to FAT32 or NTFS. Only certain devices can format a storage device that has a greater capacity than 2T.
- A progress bar (e.g., **Exporting** *X/Y*) is displayed to indicate the progress, where *X* indicates the current number being backed up, and *Y* indicates the total number of recordings. To cancel the operation, click **Cancel**.
- A backup file is named in this format:
  camera name-recording start time.file extension.
  For example, *Ch9-20150630183546.mp4.*

- Back up to a DVD-R disc: Set the destination and then click **Backup**. The recording(s) will be saved to the specified directory.



NOTE!

- Before you start burning, check that the video to back up was not compressed using smart encoding.
- Clicking **Cancel** before burning is finished will cause the disc unusable.
- When burning is finished, wait for the drive to eject itself. Do not eject the drive manually.
- The NVR does not support playback of recordings saved on a disc.

Video Clip Backup

A recording can be clipped and saved to a USB storage device.

1. Open the playback window. For the detailed steps, see Playback.
2. After playback starts, click  on the playback toolbar to clip videos.
3. Click  and then click the **Video Clip** tab to view video clips.
4. Select the desired video clip(s) and then click **Backup**.
5. Select a destination in the USB storage device and then click **Backup**. The selected video clips are saved to the specified directory.

Image Backup

The default format of image backup is JPG.

1. Click **Backup > Image.**
2. Set search conditions and then click **Search**. Search results are displayed.



NOTE!

The image resolution depends on the resolution from the output interface and the number of windows displayed when the snapshot is taken.

3. Select the desired file(s) and then click **Backup**.
4. Select a destination in the USB storage device and then click **Backup**. The selected files are saved to the specified directory.

9 Alarm

Alarm Input and Output

Alarm Input

1. Click **Alarm > Input/Output > Alarm Input.**
2. Click  for the desired camera. In the **Alarm Input** window, select **Enable** to enable alarm input.
3. Select the normally open (N.O.) or normally closed (N.C.) trigger mode, and then click **OK**.



4. Click  under **Trigger Actions** and then set action(s) to trigger. For more details, see Alarm-Triggered Actions.



NOTE!

- The number of cameras that can be connected may vary with NVR model.
- Actions that can be triggered may vary with alarm type.

5. Click  under **Arming Schedule** and then set the time when actions will be triggered.



NOTE!

- The default schedule is 24×7. You may change it as needed and set up to eight different periods for each day. Time periods cannot overlap.
- To apply the same arming schedule to other days, select the intended days and then click **Copy To**.
- To apply the same settings to other cameras, click **Copy**, select cameras, and then click **OK**.

Alarm Output

1. Click **Alarm > Input/Output > Alarm Output.**
2. Click  under **Edit** for the desired camera, and then set the default status and duration. After you have completed the settings, click **OK**.
3. Click  under **Arming Schedule** and then set the time when actions will be triggered.

NOTE!

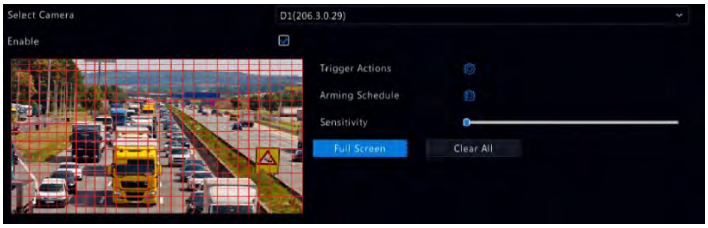
To apply the same settings to other cameras, click **Copy**, select cameras, and then click **OK**.

Motion Detection

When enabled, a motion detection alarm occurs if an object inside the detection area moves to certain extent, and an alarm icon appears in the upper right corner.

Motion detection is enabled on the NVR by default. Unless modified, the detection area covers the full screen, and recording is triggered only for the current camera. The settings remain if you disable motion detection and then enable it.

1. Click **Alarm > Motion.**
2. Select the desired camera and then select **Enable** to enable motion detection.
3. Use the mouse to draw a detection area, and drag the slider to set detection sensitivity, target object size, and duration. The higher the sensitivity, the more likely a moving object will be detected.



4. Click  right to **Trigger Actions** and set action(s) to trigger.

   For more details, see Alarm-Triggered Actions.

NOTE!

- The number of cameras that can be connected may vary with NVR model.
- Actions that can be triggered may vary with alarm type.

5. (Optional) Click right to **Arming Schedule** and then set the time when actions will be triggered.

NOTE!

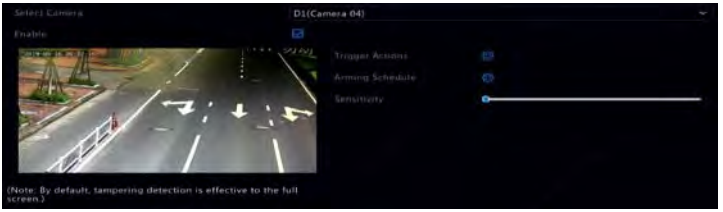
- The default schedule is 24×7. You may change it as needed and set up to eight different periods for each day. Time periods cannot overlap.
- To apply the same arming schedule to other days, select the intended days and then click **Copy To**.

6. Click **Apply** to save the settings.
7. (Optional) Click **Copy** to apply the same settings to other cameras.

Tampering Detection

A tampering detection alarm occurs when the camera lens is covered.

1. Click **Alarm > Tampering.**
2. Select the desired camera and then select **Enable** to enable tampering detection.



3. Click right to **Trigger Actions** and set action(s) to trigger.

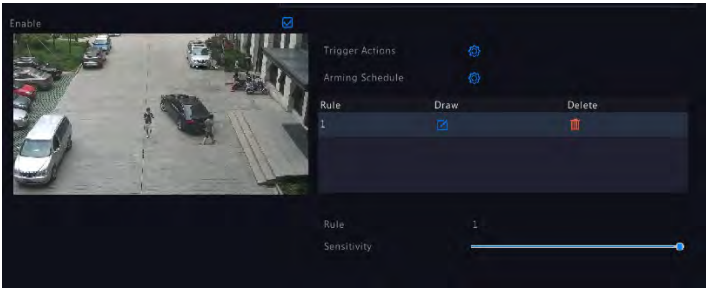
   For more details, see Alarm-Triggered Actions.

4. (Optional) Click right to **Arming Schedule** and then set the time when actions will be triggered.
5. (Optional) Click **Copy** to apply the same settings to other cameras.
6. Click **Apply** to save the settings.

Human Body Detection

Human body detection alarms occur when the presence of human beings is detected in the specified area.

1. Click **Alarm > Human Body Detection.**



2. Enable human body detection by selecting the check box
3. Click , and then draw detection area.

Note:

Only one detection area is allowed for each camera.

4. Set detection sensitivity. The higher the sensitivity, the more likely a human body will be detected.

5. Click  right to **Trigger Actions** and set action(s) to trigger.

   For more details, see Alarm-Triggered Actions.

6. (Optional) Click  right to **Arming Schedule** and then set the time when actions will be triggered.
7. Click **Apply** to save the settings.

Video Loss

A video loss alarm occurs when the NVR loses video signals from a camera. Video loss alarm is enabled by default.

1. Click **Alarm > Video Loss**. To disable video loss alarm for a channel, click , which then changes to .
2. Click  under **Trigger Actions** and set action(s) to trigger.

   For more details, see Alarm-Triggered Actions.



NOTE!

Video loss alarm cannot trigger recording, preset, preview (live view) and snapshot actions for the current camera.

3. Click  under **Arming Schedule** and then set the time when actions will be triggered.
4. (Optional) Click **Copy** to apply the same settings to other cameras.

Alert

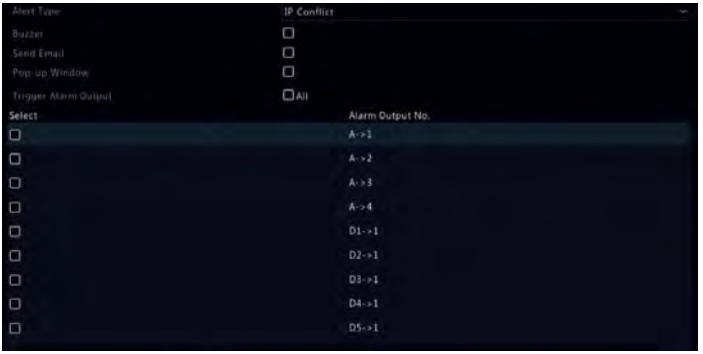
The NVR reports an alert when an event occurs in the system. The following are some alerts and their definitions in the system.

- **Running Out of Space:** Less than 10% of disk space remains.

- **Space Used Up:** No disk space.
- **Disk Offline:** A disk is not properly connected or is damaged.
- **Disk Abnormal:** A disk can be detected but cannot be accessed.
- **Illegal Access:** A failed login attempt for a username that does not exist or a password that is incorrect.
- **Network Disconnected:** Network connection is lost.
- **IP Conflict:** Devices on the network use the same IP address.
- **Recording/Snapshot Abnormal:** Storage resource cannot be found, for example, when all hard disks are removed, or when there is no disk in disk group 1 (see Disk Group for more information).

Perform the following steps to configure an alert:

1. Click **Alarm > Alert.**
2. Select an alert type, select the desired actions, and then select the camera(s) for which you want to enable alarm output.



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

Buzzer

The buzzer can be triggered by alarms to alert the user. Follow the steps to set how long the buzzer will buzz after it is triggered.

1. Click **Alarm > Buzzer.**



2. Set the duration as needed. The range is from 1 to 600 seconds.
3. Click **Apply** to save the settings.

Alarm-Triggered Actions

An alarm can trigger actions, for example, buzzer, recording, and preview. The supported actions may vary with NVR model.

Alarm-Triggered Buzzer

The NVR makes a buzzing sound when an alarm occurs.

Alarm-Triggered E-mail

The NVR e-mails an alarm message to a specified email address when an alarm occurs.

Alarm-Triggered Pop-up Window

A window pops up when an alarm occurs.

Alarm-Triggered Recording

The NVR records video from a specified camera when an alarm occurs.

Alarm-Triggered Snapshot

The NVR takes a snapshot when an alarm occurs.

Alarm-Triggered Preset

A PTZ camera rotates to a preset position when an alarm occurs.

Alarm-Triggered Preview

The NVR plays live video in full screen when an alarm occurs.

Alarm-Triggered Alarm Output

The NVR outputs an alarm to trigger actions by a third-party device when an alarm occurs.

Manual Alarm

Manual Alarm Output

Follow the steps to trigger or clear an alarm output manually.

1. Right click and select **Manual > Manual Alarm.**
2. To trigger an alarm output manually, select the desired channel and then click **Trigger**. To clear an alarm output manually, select the desired channel and then click **Clear**.

Manual Buzzer

Follow the steps to stop the buzzer manually.

1. Right click and select **Manual > Buzzer.**
2. Select the buzzer (in Started status) and then click **Stop**.

10 VCA

VCA Configuration

Basic Configuration

Click **VCA > VCA Config.** The **Basic** page is displayed. Select the camera and then select **Save VCA Images** if you want to use the VCA search function.

Face Detection

Face detection is used to detect human faces in a specified surveillance area.

1. Click **VCA > VCA Config > Face Detection.**



2. Select the camera and then select **Enable Face Snapshot**.
3. Select the detection area. You may choose full screen or specify an area to detect. If you select **Specify Area**, click **Draw Area** and then draw a detection area using the mouse.
4. Set face detection sensitivity. The higher the sensitivity, the more likely a face will be detected.

Note:

The lower the sensitivity, the less likely a side face or blurring face will be detected. Adjust detection sensitivity as needed to achieve optimal effects.

5. Configure trigger actions. Click right to **Trigger Actions** and set action(s) to trigger. For more details, see Alarm-Triggered Actions.

6. Configure an arming schedule. Click right to **Arming Schedule** and then set the time when actions will be triggered.

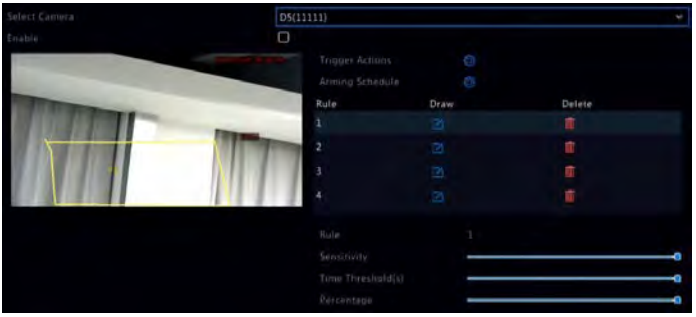
7. Click right to **Advanced**, and complete the settings.

   - Set the total number of snapshots to take for a face during the detection. Up to 30 snapshots are allowed.
   - Set the maximum and minimum face width. Face width in the picture within this range will be detected. The larger the range, the more likely a face will be detected. Adjust the width as needed to achieve optimal effects.

Intrusion Detection

Intrusion detection is used to detect objects entering specified area(s) and trigger actions as needed.

1. Click **VCA > VCA Config > Intrusion Detection.**



2. Select the camera and then select **Enable** to enable intrusion detection.
3. Draw detection areas on the screen and set detection rules including sensitivity, threshold and percentage. Up to four areas are allowed. The threshold means the minimum length of time an object stays in the detection area(s). The percentage means the proportion of target object size to the size of the detection area. An alarm occurs when the threshold or the percentage is exceeded.
4. Click  right to **Trigger Actions** and set action(s) to trigger.

   For more details, see Alarm-Triggered Actions.
5. (Optional) Click  right to **Arming Schedule** and then set the time when actions will be triggered.
6. Click **Apply** to save the settings.

Cross Line Detection

Cross line detection is used to detect whether any object crosses a virtual line on the screen and trigger alarms as needed.

1. Click **VCA > VCA Config > Cross Line Detection.**



2. Select the camera and then select **Enable** to enable cross line detection.

3. Draw detection line(s). Up to four are allowed. Set detection rules, including entrance direction, sensitivity.

4. Click right to **Trigger Actions** and set action(s) to trigger.

   For more details, see Alarm-Triggered Actions.

5. (Optional) Click right to **Arming Schedule** and then set the time when actions will be triggered.

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

Audio Detection

An audio detection alarm occurs when a camera detects a sudden change in sound volume.

1. Click **VCA > VCA Config > Audio Detection.**

2. Select the camera and then select **Enable** to enable audio detection.



3. Click right to **Trigger Actions** and set action(s) to trigger.

   For more details, see Alarm-Triggered Actions.

4. (Optional) Click right to **Arming Schedule** and then set the time when actions will be triggered.

5. Select a detection type and adjust the settings as needed.

Detection Type	Description
Sudden Rise	An alarm occurs when the rise of volume exceeds the set value.
Sudden Fall	An alarm occurs when the fall of volume exceeds the set value.

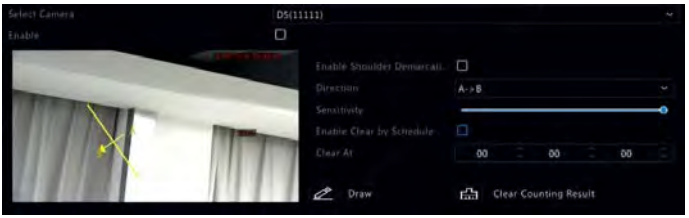
Detection Type	Description
Sudden Change	An alarm occurs when the rise or fall of volume exceeds the set value.
Threshold	An alarm occurs when the volume exceeds the set value.

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

People Counting

People counting is used to count people entering or leaving an area. Only certain NVR models support this function. This function cannot be used at the same time with other VCA functions (face detection, intrusion detection, cross line detection, defocus detection and scene change detection).

1. Click **VCA > VCA Config > People Counting.**

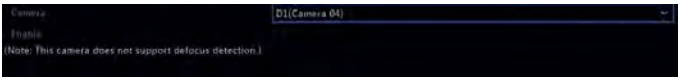


2. Select the camera and then select **Enable Shoulder Demarcation**. Draw a virtual line on the screen to set the minimum width of detection. People narrower than the set width will be ignored.
3. Click the **Draw** button and then draw rules on the left. Set entrance direction and sensitivity as needed.
4. By selecting **Enable Clear by Schedule**, you can have people counting OSD reset at a specified time every day. You may also click **Clear Counting Result** to clear the OSD immediately. Resetting people counting OSD only changes the OSD. It does not change report statistics.
5. Click **Apply** to save the settings.

Defocus Detection

Use defocus detection to check whether the camera focuses properly.

1. Click **VCA > VCA Config > Defocus Detection.**
2. Select the desired camera and then select **Enable** to enable defocus detection.



3. Click right to **Trigger Actions** and set action(s) to trigger.

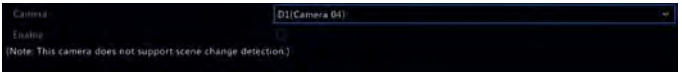
   For more details, see Alarm-Triggered Actions.

4. (Optional) Click right to **Arming Schedule** and then set the time when actions will be triggered.
5. Set detection sensitivity and then click **Apply** to save the settings.

Scene Change Detection

Use scene change detection to detect the change of surveillance environment caused by external factors such as intentional rotation of the camera.

1. Click **VCA > VCA Config > Scene Change Detection.**
2. Select the desired camera and then select **Enable** to enable scene change detection.



3. Click right to **Trigger Actions** and set action(s) to trigger.

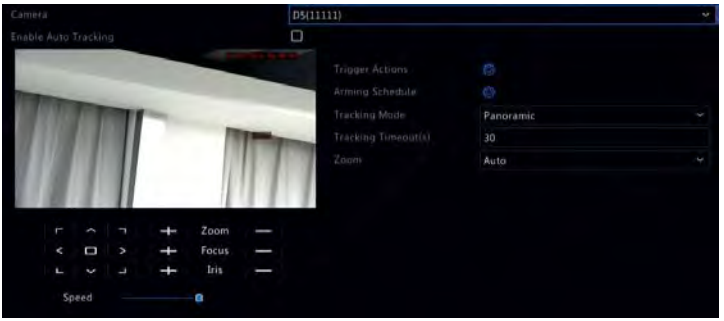
   For more details, see Alarm-Triggered Actions.

4. (Optional) Click right to **Arming Schedule** and then set the time when actions will be triggered.
5. Set detection sensitivity and then click **Apply** to save the settings.

Auto Tracking

Auto tracking detects moving objects in the scene and automatically tracks the first object detected.

1. Click **VCA > VCA Config > Auto Tracking.**
2. Select the desired camera and then select **Enable** to enable auto tracking.



3. Click right to **Trigger Actions** and set action(s) to trigger. For more details, see Alarm-Triggered Actions.
4. (Optional) Click right to **Arming Schedule** and then set the time when actions will be triggered.
5. Set tracking mode (currently only **Panoramic**). Set tracking timeout and zoom ratio.

NOTE!

- Tracking Timeout(s) means the maximum length of time the camera tracks an object automatically. The range is 1-300 seconds and the default is 30 seconds. When the tracking timeout is over, the camera stops tracking and restores the original scene and status.
- Zoom means zoom ratio and includes **Auto** (default) and **Current Zoom**. **Auto** means the camera automatically adjusts the zoom ratio according to the tracking distance and thus captures more details on the tracking object; **Current Zoom** means the camera maintains the original zoom ratio during tracking and thus attends to the whole scene.

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

Object Left Behind

Detect object left behind in specified areas and trigger an alarm.

1. Click **VCA > VCA Config > Object Left Behind.**



2. Select the camera and select **Enable** to enable detection of objects left behind.

3. Click  to draw detection areas.

NOTE!

When drawing a detection area, you can use up to 6 points to specify the area. Up to 4 detection areas area allowed.

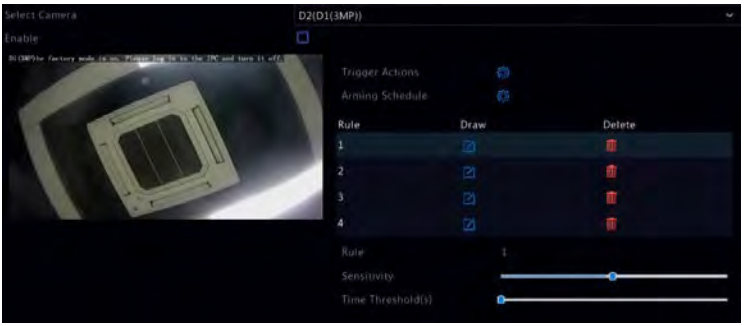
4. Set sensitivity and time threshold:
   - **Sensitivity**: The higher the sensitivity, the more likely an object left behind will be detected.
   - **Time Threshold**: An alarm will be triggered when the length of time an object is left behind in a detection area exceeds this value.
5. Click  right to **Trigger Actions** and set action(s) to trigger.

   For more details, see Alarm-Triggered Actions.
6. (Optional) Click  right to **Arming Schedule** and then set the time when actions will be triggered.
7. Click **Apply** to save the settings.

Object Removed

Detect object removed from specified areas and trigger an alarm.

1. Click **VCA > VCA Config > Object Removed.**



2. Select the camera and select **Enable** to enable detection of objects removed.
3. Click  to draw detection areas.

NOTE!

When drawing a detection area, you can use up to 6 points to specify the area. Up to 4 detection areas area allowed.

4. Set sensitivity and time threshold:
   - **Sensitivity**: The higher the sensitivity, the more likely an object will be detected.
   - **Time Threshold**: An alarm will be triggered when the length of time an object is missing in specified areas exceeds this value.
5. Click  right to **Trigger Actions** and set action(s) to trigger.

   For more details, see Alarm-Triggered Actions.
6. (Optional) Click  right to **Arming Schedule** and then set the time when actions will be triggered.
7. Click **Apply** to save the settings.

VCA Search

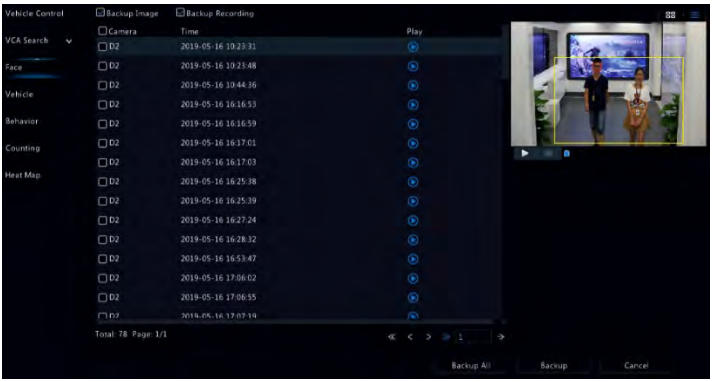
VCA means Video Content Analysis. VCA search searches VCA data including behavior, human face, and people counting. Only certain NVR models support this function. You need to select **Save VCA Images** under **VCA > VCA Config > Basic** before using behavior search and face search functions.

Face Search

Use face search to search for recordings triggered by detected faces.

1. Click **VCA > VCA Search > Face.**
2. Select cameras, set a search period, and then click **Search**. Search results are displayed.

3. View search results in a chart or table. Back up search results (including images and recordings) as needed. To view videos recorded when the face was detected (around 10 seconds before and after), click the play button. The following shows an example.



Vehicle Search

Search vehicle snapshots based on vehicle control events.

1. Click **VCA > VCA Search > Vehicle.**



2. Select the camera, set the time range, license plate number, vehicle color, and plate number.
3. Click **Search**.

Note:

Double click to zoom in on the snapshot.

Behavior Search

Use behavior search to search for recordings triggered by detected behaviors including cross line and intrusion.

1. Click **VCA > VCA Search > Behavior.**
2. Select camera(s), set a search period, select a search type, and then click **Search**. Search results are displayed.
3. View search results in a chart or table. Back up search results (including images and recordings) as needed. To view videos recorded when the behavior was detected (around 10 seconds before and after), click the play button.

People Counting

Use people counting to count people entering and/or leaving an area during a specified period (day, week or year).

1. Click **VCA > VCA Search > Counting.**
2. Select the camera, counting type (people entered or left), report type (daily, weekly, monthly or yearly), set a time period, and then click **Count**. Search results are displayed. You may choose to display search results in a chart or table. When you click a bar, statistics of the selected camera(s) are displayed
3. (Optional) To save the counting statistics to a connected USB storage device, click **Backup**.

Heat Map

Heat map is used to monitor passenger flow in specified area and to display the data in the form of an image by using warm-to-cool color spectrums. The warmer the color, the higher the density of the passenger flow.

1. Click **VCA > VCA Search > Heat Map.**
2. Select the camera and the report type, then click **Count**.

3. Click **Backup** to export the counting statistics to a storage device.

11 Network Configuration

Network configuration is required if your NVR operates in a network shared by other devices.



NOTE!

The default IP address is 192.168.1.30 for NIC 1 and 192.168.2.30 for NIC 2.

Basic Configuration

TCP/IP

1. Click **Network > Basic**.
2. Set the network parameters as needed. DHCP is enabled by default.

   You can choose a working mode if the NVR has two NICs:

   - **Multi-address mode**: The two NICs work independently and can be configured separately. Either NIC can be chosen as the default route; data will be forwarded through this NIC when the NVR connects to the extranet.
   - **Load balance mode**: The two NICs are bound to the same IP address and work together to share network traffic.
   - **Net fault-tolerance mode**: The two NICs are bound to the same IP address. In cases where one NIC fails, the other takes over service seamlessly from the faulty one to ensure network connectivity.



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

NOTE!

- For an NVR with multiple NICs, you can configure the NICs and choose a default route (currently NIC1).
- If your NVR has a PoE port or a switching port, you can configure an internal NIC IPv4 address.

CAUTION!

- If you switch the working mode, the enabled 802.1x and ARP protection will be disabled automatically.
- The valid MTU ranges from 576 to 1500 (1280-1500 for IPv6). To use IPv6, make sure the NVR and PC can connect to each other using IPv6 addresses. To view live or recorded videos, make sure the IPv4 addresses are also connectable.

P2P

The NVR allows access from the cloud website or from the mobile surveillance app. You need to sign up for a cloud account at www.star4live.com first.

1. Click **Network** > **Basic** > **P2P**.
2. P2P is enabled by default.
3. To add the NVR to cloud at the cloud website: Log in to your account at www.star4live.com and then add the NVR by entering the register code and device name.
4. To add the NVR to cloud using the app: Scan the QR code with the app. You need to download and install the app on your mobile phone first. Contact your dealer for details.



NOTE!

- You may access the NVR through cloud if the device status is Online. The username is your cloud account name, and the device name is the name you entered at the cloud website.
- If the device is offline, the possible causes will be displayed for your reference.
- To delete the NVR from cloud, click **Delete**.

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

DDNS

If your NVR is connected to the Internet through PPPoE, the IP address of the network changes every time it connects to the ISP server without your awareness. This is inconvenient when you remotely access your NVR with an IP address. To avoid this issue, you can register with an DDNS server to obtain a domain name for your NVR and then access your NVR by visiting the domain name instead of an IP address (http://*DDNS server address/NVR's domain name*) using a web browser.

1. Click **System > Network > DDNS.**
2. Enable DDNS, select a DDNS type, and then complete other settings.
   - If the DDNS type is DynDNS or No-IP, enter the domain name, username and password. The domain name is the one that you successfully registered at a domain name registration website (e.g., DynDNS). The username and password are those of the account you registered at the domain name registration website (e.g., DynDNS).



- If the DDNS type is **MyDDNS**, enter a valid domain name for your NVR and then click **Test** to see if the domain name is available.

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

Port Mapping

Two port mapping methods are available:

- Universal Plug and Play (UPnP)
- Internal and external mapping

UPnP

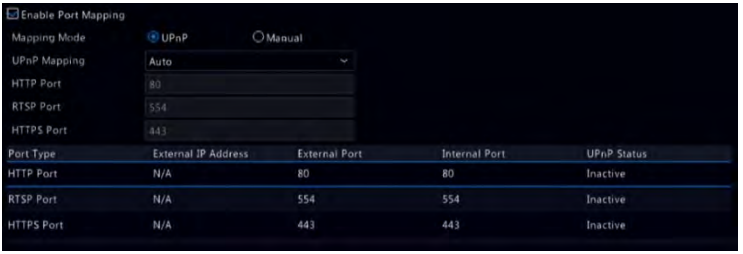
UPnP enables the NVR to discover other devices on the network and establish network services such as data sharing and communication.

To use UPnP in your NVR, enable UPnP in the connected router. With UPnP enabled for Network Address Translation (NAT), the ports on the NVR can be mapped automatically to the router, and computers can access your NVR from outside the LAN.

1. Click **Network > Basic.**
2. UPnP is enabled by default. Select the desired mapping type from the drop-down list. To map ports manually, select **Manual** and then set external ports for the router.

NOTE!

- Automatic mapping (Auto) is recommended. Ports will conflict if not configured properly.
- For an NVR with multiple NICs, port mapping should be configured based on the NIC specified as the default route.



3. Click **Refresh** and check that **Active** is displayed for these ports under **UPnP Status.**
4. Click **Apply** to save the settings.

Manual Port Mapping

If your router does not support UPnP, configure the internal and external ports manually.

NOTE!

- The principle of port mapping is that the internal and external ports of the NVR are consistent with that of the router.
- Some routers may require the same internal and external ports for the NVR and the router.

1. Click **Network > Basic.**
2. Select **Manual** for **Mapping Mode**, and then set external ports manually.



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

NOTE!

After port mapping is completed, you can access the Web client of your NVR by entering the following information in the address bar of your web browser: router's WAN port IP address: external HTTP port. For example, if 10.2.2.10 is the IP address and 82 is the HTTP port, then you enter http://10.2.2.10:82.

Platform Configuration

SNMP

Use SNMP to connect to a platform and obtain system time.

1. Click **Network > Platform.** Select **Enable SNMP**.



2. Select an SNMP type.

- **Snmp V2**: Set Read Community Name and Write Community Name, which are used by the platform to read data on NVR.
- **Snmp V3**: Set authentication password (for the platform to access the NVR) and encryption password (for encrypting data sent from the NVR to the platform).

3. Click **Apply**.

Alarm Service

Use this function to send alarm signals to an external alarm device (for example, alarm control panel) when an alarm or an alert occurs on the NVR.

1. Click **Network > Platform > Alarm Service.**



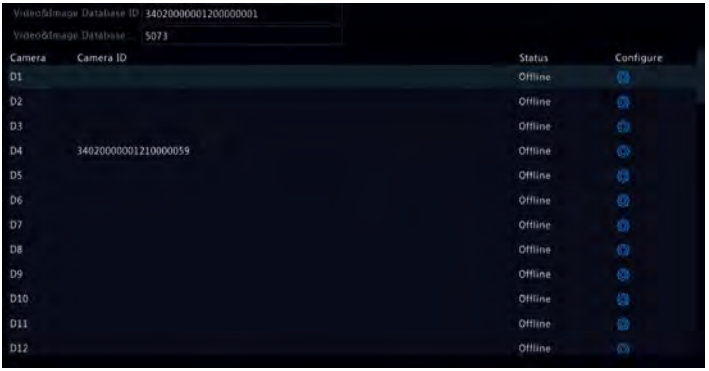
2. Select **Enable Alarm Service**, and set the server address and SIP server port.

NOTE!

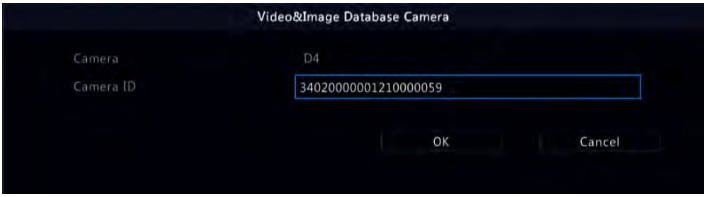
The NVR only sends alarm signals when an alarm or alert occurs; users need to implement alarm receiving and reporting for the external alarm device separately.

Video&Image Database

1. Click **Network > Platform > Video&Image Database.**



2. Use the default database ID and port. Click  to set camera ID.



3. Click **OK**.
4. Log in to the camera's Web interface and complete settings on **Setup > Config Management > Photo Server.** The settings may vary depending on the platform communication type you choose. Some settings are described below.
   - **TMS Server**: IP address of the NVR
   - **TMS Server Port**: Database port configured on the NVR.
   - **Platform Communication Type**: Choose the correct type.
   - **LPR ID**: Database ID configured on the NVR.
   - **Device ID**: Camera ID configured on the NVR.
   - **Platform Access Code**: Use the default setting.
   - **Username**: Use the default setting.

5. Click **Save**. Check management server status in the page's lower left corner. A green icon means the camera is connected to the Video&Image database. Now configuration on the camera is complete.

Vehicle Control

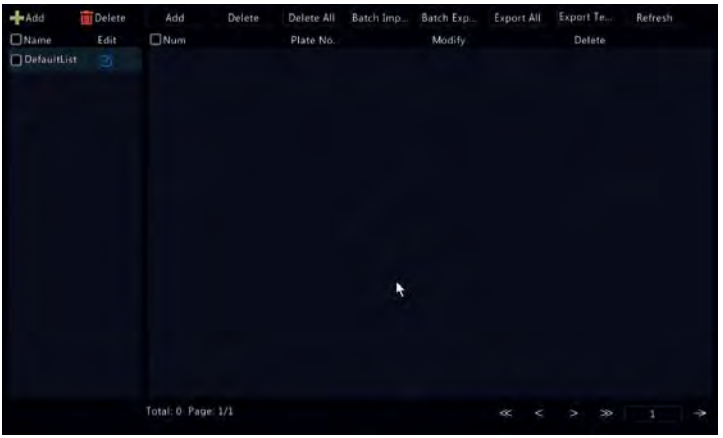
Vehicle control allows you to view license plate recognition results. To use this function, you need to configure in Video&Image Database, add plate list, and set vehicle monitoring task.

Video&Image Database

See Video&Image Database for details.

Add Plate List

1. Click **VCA > Vehicle Control > Plate List.**



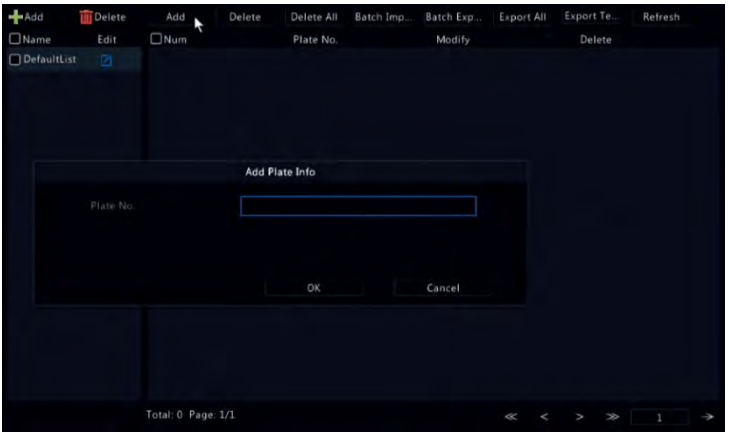
2. Click  to add a plate list.

Note:

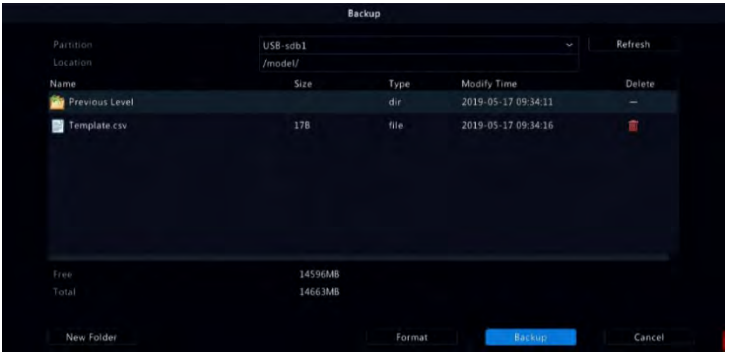
DefaultList is created by default. Click  to modify the list name.

3. Add plate number(s) to plate list.

- To add a single plate, click **Add**, and then enter the plate number in the window displayed.



- To batch add plates, click **Export Template** to export the template to a USB storage device first. Then edit the list, and click **Batch Import** to import the edited file.



After importing is completed, click **Cancel** to return to **Plate List**.

Note:

The import failures and the causes are displayed in **Import Status** window. No result in the window means all plate numbers are exported successfully.

Add Vehicle Monitoring Task

1. Click **VCA > Vehicle Control > Vehicle Alarm Control.**
2. Click **Add** to add a monitoring task.



3. View license plate recognition results.

- In preview window, click  on the screen toolbar.
- Right click and select **Preview Mode > Smart.**

Note:

- In smart mode, click  in the upper right corner to set the display content.
- To exit smart mode, right click and select **Preview Mode > Normal.**

Video&Image Database Server

Video&Image database server is used to connect to an upper platform for unified management of face and plate data.

1. Click **Network > Platform > Video&Image Database Server.**



2. Select **Enable Video&Image Database Server**, and complete the settings.

Note:

The server address, port number, username and password should be consistent with those configured on the platform.

Advanced Configuration

PPPoE

The NVR allows access through Point-to-Point over Ethernet (PPPoE).

1. Click **Network > Advanced > PPPoE.**
2. Enable PPPoE by selecting the check box.
3. Enter the username and password provided by your Internet Service Provider (ISP). Network information including IP address appears when dial-up succeeds.

NOTE!

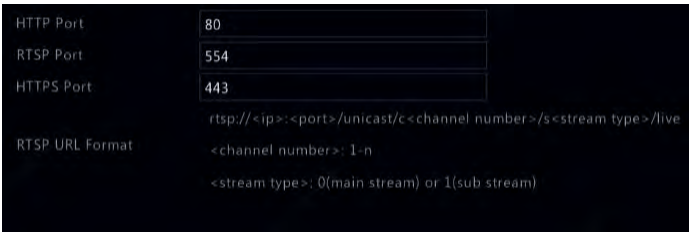
If your NVR has multiple NICs, PPPoE dial-up will be implemented through the NIC specified as the default route.

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

Port

Normally the default port numbers need no modification. This function is mainly used together with the port mapping function. See Port Mapping for more details.

1. Click **Network > Advanced > Port.**
2. Configure ports as planned. Each port number must be unique.



NOTE!

- A valid port number ranges from 1 to 65535, among which 21, 23, 2000, 3702 and 60000 are reserved.
- An RTSP URL can be used to view live video of a channel of the current NVR from another NVR. See Option 5 in Adding an IP Device for more information.

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

Email

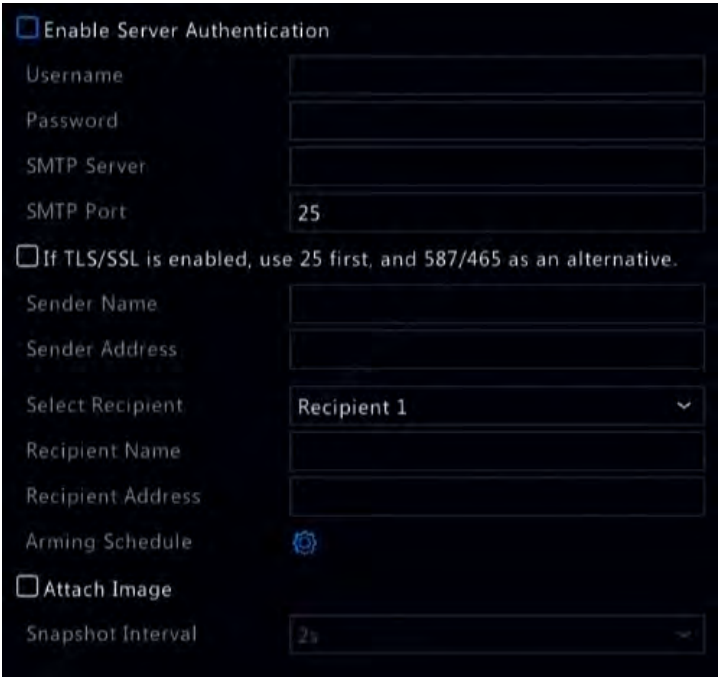
After Email is enabled as a triggered action (in Trigger Actions windows) and configured properly, the NVR sends an email notification to specified email address(es) if an alarm occurs within the time period(s) set in the arming schedule. The email contains basic alarm information such as alarm type, alarm time, camera ID, and camera name, etc.

Before using this function, make sure the NVR has a functional connection to an SMTP server with which you have a valid email

account. Depending on the intended recipients, a connection to the Internet may be required.

Only certain NVR models support this function.

1. Click **Network > Advanced > Email.**
2. Configure the related parameters. If server authentication is required, you need to enter the correct username and password. Click **Test** to send a test email.



NOTE!

- Enter a valid SMTP server address and port number, and then select **Enable TLS/SSL** if required.
- Select **Attach Image** if you want snapshots to be sent via email. Make sure Email and snapshot have been enabled in the **Trigger Actions** window.
- Only certain NVR models support image attachment. You may click **Test** to check whether the email can be sent successfully.

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

FTP

Use this function to automatically upload images to a preconfigured FTP server. Only certain NVR models support this function.

1. Click **Network > Advanced > FTP.**
2. Select the check box to enable FTP.
3. Enter the IP address of the FTP server, username and password, remote directory, and upload interval.

NOTE!

- Click **Test** to verify whether an FTP connection can be established.
- If the remote directory is not specified, the system will create different folders directly by IP, time and camera. You may also specify a remote directly, for example, FTPtest/*xxx*/*xxx*, then the system will create the directory first and then create folders by IP, time and camera.

4. Select the desired camera and then click right to **Upload Schedule**. In the **Upload Schedule** window, select the desired image type and set time periods.



NOTE!

- If you select Event, Motion, Alarm or Video Loss, you also need to configure the corresponding alarm-triggered snapshot. For example, if you select Motion, you need to configure alarm-triggered snapshot (select Motion in the Edit Schedule window).
- To apply the same settings to other days in a week, select the days on the **Copy To** line.

5. (Optional) Apply the same settings to other cameras by clicking right to **Copy** and then selecting desired cameras.
6. Click **Apply** to save the settings.

NOTE!

To apply the same settings to other cameras, click right to **Copy**, select cameras and then click **OK**.

Multicast

Multicast can be used to realize live view when the number of connecting Web clients exceeds the limit the NVR can accommodate.

1. Click **Network > Advanced > Multicast.**
2. Select the check box to enable multicast, and then enter the multicast IP and port number.



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

4. Log in to the Web client and set **Live View Protocol** to **Multicast** under **Setup > Client.**



NOTE!

Set the multicast IP correctly. Multicast address is class D address with the range 224.0.0.0 through 239.255.255.255; some are for special use:

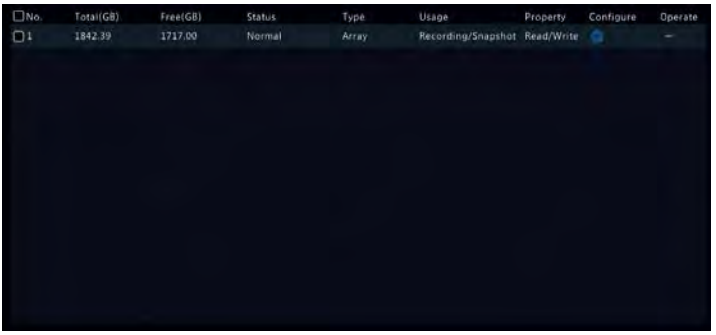
- 224.0.1.0--238.255.255.255 can be used on the Internet.
- 224.0.0.0-244.0.0.255: only for use on LAN.
- 224.0.0.1: all-hosts group address, which refers to all the multicast-capable hosts and routers on a physical network.
- 224.0.0.2: for all routers on this subnet.
- 224.0.0.5: for all OSPF routers.
- 224.0.0.13: for all PIMv2 routers.
- 239.0.0.0--239.255.255.255 are for private use like 192.168.x.x.

12 Disk Configuration

Disk Management

View disk information, including total and free disk space, disk status, disk type, disk usage, and disk property. *admin* users can format disks and edit disk property

1. Click **Storage > Hard Disk.**



2. To add a disk, click **Add**. In the dialog box displayed, select disk usage (recording/snapshot or backup) and disk type (currently NAS only), enter the server address and directory, and then click **Add**. Up to eight NAS disks are allowed.



3. To edit disk property, click , and then modify disk usage (recording/snapshot or backup) and disk property (**Read/Write, Read Only** or **Redundant**) as needed.

NOTE!

- Disk property can be edited if the disk is used for recording/snapshot.
- The Redundant property is available to certain NVR models.
- You may use external eSATA disks for recording/snapshot or backup purpose and unmount them if necessary. eSATA disks and NAS disks cannot be used to create arrays.

4. To format a disk, select the disk and then click **Format**. When a confirmation message appears. Click **Yes**.

NOTE!

- Local disks will be formatted automatically when installed. Extended disks will not.
- Format a disk with caution. All data will be removed.

Array Configuration

Only certain NVR models support RAID. The table below lists the supported RAID types and hard disks required.

RAID	HDD Qty
RAID 0	2-8
RAID 1	2
RAID 5	3-8
RAID 6	4-8
RAID 10	4-16 (Must be an integral multiple of 2, e.g., 4, 8, 10, etc).
RAID 50	6-16
RAID 60	8-16

Enabling RAID

You need to enable RAID first.

1. Click **Storage > Array.**

2. Select the check box to enable RAID. A confirmation message appears. Click **Yes**.

Creating an Array

It is recommended to configure a hot spare disk to ensure reliable system operation and successful rebuilding in case an array fails.

1. Click **Storage > Array.**
2. To create an array automatically, click **One-click Create**.



NOTE!

- There is no need to select disks when creating an array with **One-click Create**. The system identifies all usable disks. RAID 1 is created when two disks are available. When three or more disks are available, RAID 5 is created. If more than four disks are available, a global hot spare disk will be created.
- Arrays created in this way are named ARRAY*x*, for example, ARRAY1, ARRAY2.

3. To create an array manually, select the desired disks and then click **Create**. In the window displayed, enter the array name, select the array type, and select local disks. Click **OK** to complete the setup. Note that no hot spare disk will be created automatically. Make sure all disks are selected to create array(s); otherwise, disk space will be wasted (because disks that are not selected will not be used for storage).

Rebuilding an Array

By checking array status you can determine whether maintenance is necessary.

NOTE!

To be alerted when an array is degraded or damaged, you can configure alarm-triggered action at **Alarm > Alert.**

An array is in one of four statuses: normal, degraded, damaged, rebuild. The status is normal if no physical disk is lost. When the number of physical disks lost reaches the specified value, the array is considered damaged. The status between normal and damaged is degraded. A degraded array can be recovered to normal status through rebuilding.

NOTE!

Take RAID 5 that consists of 4 disks as an example. The array is degraded when one disk is lost. When two disks are lost, the array is damaged.

A degraded array can be automatically rebuilt in ten minutes if these conditions are met: a hot spare disk is available; the capacity of the hot spare disk is not less than that of any disk in the array. A degraded array without a hot spare disk can only be rebuilt manually under **Storage > Array > Array.** By default the first local disk that satisfies requirements is selected.

Deleting an Array

CAUTION!

Deleting an array will erase all data on it.

1. Click **Storage > Array > Array.**
2. Click for the array to delete. A confirmation message appears. Click **Yes**.

Disk Group

Assign hard disks to a disk group and use the disk group to store recordings and snapshots of specified cameras. Different arrays can be assigned to different disk groups.

Redundant disks cannot be assigned to any disk group. Disk group information will be initialized if any disk in the group is formatted.

1. Click **Storage > Disk Group.**



2. Select **Enable Disk Group**. By default all disks belong to Disk Group 1. Click  for the disk to edit, and then select a group to which the disk will be assigned.

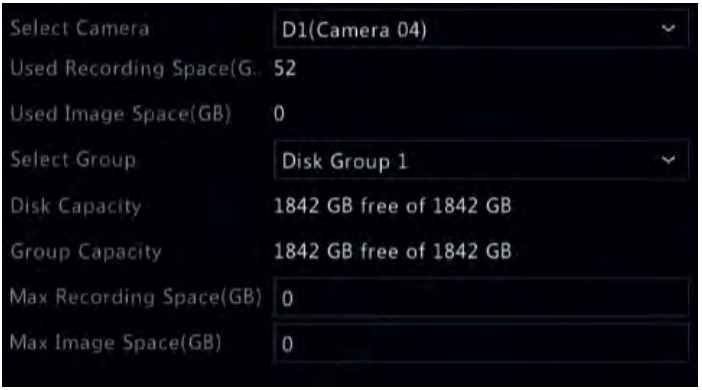


3. Click **Apply** to save the settings.

Space Allocation

Allocate space to store videos and snapshots of a specified camera.

1. Click **Storage > Allocate Space.**

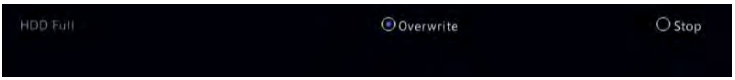


2. Select the desired camera and then set the maximum recording space and maximum image space. You can select a disk group only when disk group is enabled under **Storage > Disk Group.** For more information, see Advanced Configuration.
3. Click **Apply** to save the settings.
4. (Optional) Click **Copy** to apply the same settings to other camera(s).

Advanced Configuration

Set whether to overwrite recordings or snapshots when storage is full.

1. Click **Storage > Advanced.**



2. Choose an option.

Option	Allocated Space	Description
Overwrite	0	The camera shares unallocated space, and its oldest recordings/snapshots will be overwritten when the space is used up.
	Other values	The camera's oldest recordings/snapshots will be overwritten when its allocated space is used up.
Stop	0	The camera shares unallocated space, and its oldest recordings/snapshots will still be overwritten when the space is used up.
	Other values	The camera's new recordings/snapshots will not be saved when its allocated space is used up.

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

Hard Disk Detection

S.M.A.R.T. Test

Click **Maintain > HDD > S.M.A.R.T. Test** to do S.M.A.R.T. test.

S.M.A.R.T. (enabled by default) checks the head, platter, motor, and circuit of hard disks to evaluate their health status. The overall evaluation results include **Healthy, Failure,** and **Bad Sectors**. Replace the disk immediately if the status is **Failure**.



NOTE!

- Some hard disks only support some of the test items.
- The system provides three test types: **Short**, **Extended**, and **Conveyance**. Extended tests detect more thoroughly and thus take longer time than Short tests. Conveyance tests mainly detect data transmission problems.

CAUTION!

Using a faulty disk is risky. Faulty disks should be replaced immediately. Contact your local dealer for information about hard disks.

Bad Sector Detection

Bad sector detection checks for bad sectors in hard disks.

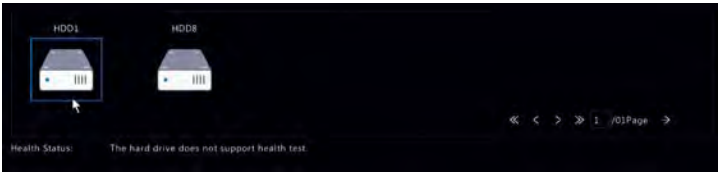
1. Click **Maintain > HDD > Bad Sector Detect.**
2. Select the desired disk and detection type, and then click **Detect** to start detection. Click **Stop** if you want to stop.

CAUTION!

The detection stops automatically when the error count reaches 100.

Health Test

Health test is supported by certain NVR models.



13 System Configuration

Basic Configuration

1. Click **System > Basic.**
2. Configure the parameters.



NOTE!

- Only users with administrative credentials can set **Enable Password**.
- If **Enable Password** is not selected, no password is required for local login at system startup. However, a username and password are still required when you log in after a logout.
- Some NVR models support Intelligent Mark. When the NVR and IP camera are both enabled, the latest areas/lines or VCA data configured for face detection, intrusion detection, and cross line detection will be displayed on the **Preview, Behavior** and **Alarm** windows in real time.
- Intelligent mark is displayed on the screen as areas/lines in different colors. Yellow means areas/lines configured for face detection, intrusion detection, and cross line detection; green means VCA data has changed but not triggered rules; red means rules are triggered in the configured area (rules are configured for VCA alarms), and VCA alarm has occurred.
- You may also set startup Wizard here by clicking **Wizard**.

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

Time Configuration

Time

1. Click **System > Time > Time.**
2. Select the correct time zone, and then set date and time formats and the system time. See the example below.



3. To use Network Time Protocol (NTP), enable auto update, set the address and port number of the NTP server, and the update interval.
4. Click **Apply** to save the settings.

DST

1. Click **System > Time > DST.**
2. Enable DST by selecting the check box, and then set the start time, end time, and DST bias correctly.
3. Click **Apply** to save the settings.

Time Synchronization

Use this function to synchronize camera time with the NVR. Time sync is enabled by default, and cameras will synchronize time with the NVR after getting online, and then synchronize once every 30 minutes.

1. Click **System > Time > Time Sync.**
2. Select **Sync Camera Time** and then click **Apply**.

CAUTION!

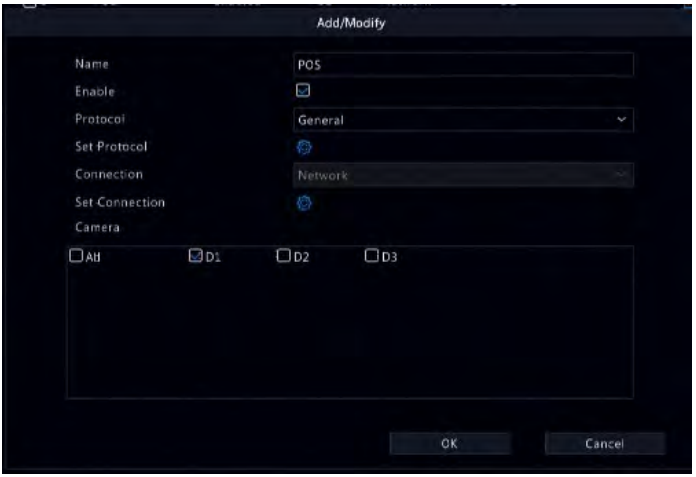
Use this function with caution if you have more than one NVR on the network. An IP camera synchronizing time with multiple NVRs at the same time will cause chaotic recordings.

POS Configuration

This function is intended for the scenario such as in a café or a supermarket where the NVR is connected to a POS machine. When configured properly, the NVR obtains data from the POS machine and displays information in form of text with video images on the monitor.

Only certain NVR models support this function.

1. Click **System > POS.**
2. Click **Add** and then complete settings in the window displayed.



NOTE!

- The name entered should be unique.
- The start identifier, end identifier, and line delimiter should be hexadecimal characters. The ignore characters are character strings that cannot be displayed.
- The source address is the IP address of the POS machine, and the destination address is that of a settlement center that receives POS data. An empty destination address means it is necessary for the NVR to forward POS data.

3. Set POS OSD under **System > POS > POS OSD,** including the position, font and color of POS information displayed on the screen.

Serial Port Configuration

Only certain NVR models support this function.

Serial port settings in the NVR should be consistent with those in the connected serial device. Serial port configuration is required for PTZ control.

1. Click **System > Serial.**
2. Configure the parameters for the serial port.

NOTE!

You may set **Port Usage** to **Keyboard** to control a PTZ camera with a specialized surveillance keyboard.

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

User Configuration

Add, delete users or edit user permissions. Only administrative users can perform these operations. Device password is required for user configuration.

A user type is a set of permissions in the system. When a user type is assigned to a user, this user has all the permissions specified for the user type.

There are four user types in the system:

- ***admin***: Default super administrator in the system, has full system access. Its initial password is **123456**.
- **Default**: Default user reserved in the system, cannot be created or deleted, and only has access to live view and two-way audio. If the default user is denied access, the corresponding channel is locked when no user is logged in, and  appears in the window.
- **Operator**: Has basic permissions and access to cameras.
- **Guest**: Only has access to cameras by default.

1. Click **System > User.**
2. To add a user, click **Add**, and then set the username and password, select user type, permissions and whether to enable unlock pattern as needed. Click **OK** to save the settings.



3. To edit or delete a user, click  or  as needed. If you change the password for a user, the new password takes effect at the user's next login.

Security Configuration

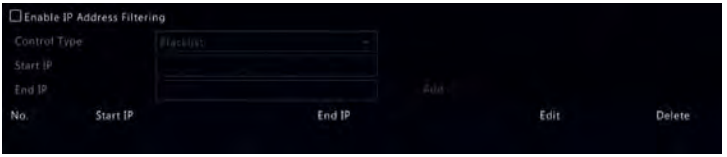
IP Address Filtering

Use this function to enhance security by allowing or forbidding access to the NVR from specified IP addresses.

1. Click **System > Security > IP Address Filtering.**
2. Select **Enable IP Address Filtering**, select **Blacklist** or **Whitelist** from the drop-down list, set the start and end IP addresses, and then click **Add**.

NOTE!

- If **Blacklist** is selected, the NVR denies remote access from the IP address(es) on the list.
- If **Whitelist** is selected, the NVR only allows remote access from the IP address(es) on the list. However, if **Whitelist** is selected with no IP address specified, remote access to the NVR will be denied.

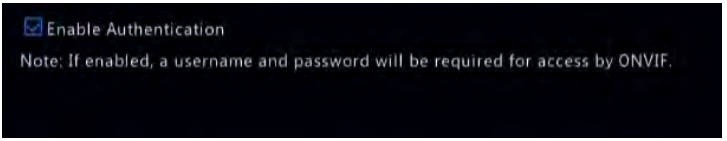


3. Click **Apply** to save the settings.

ONVIF Authentication

Enable ONVIF authentication under **System > Security > ONVIF Auth** so a username and password will be required for ONVIF-based device access.

Select the check box and then click **Apply**.



ARP Protection

ARP protocol is used to associate an IP address to a hardware MAC address. ARP attacks mainly occur on LAN, in which attackers use forged IP and MAC addresses. APR protection prevents this kind of attacks by verifying the gateway's MAC address in all access requests.

Note that changing the NIC working mode will disable ARP protection automatically.

1. Click **System > Security > ARP Protection.**



2. Select the desired NIC and then select **Enable ARP Protection**.
3. Obtain the gateway's MAC address automatically, or select **Custom** and input the MAC address.
4. Click **Apply** to save the settings.

802.1x

802.1x is a port-based network access control protocol mainly used to solve authentication and security issues on LAN.

Only certain NVR models support this function. Note that changing the NIC working mode will disable 802.1x automatically.

1. Click **System > Security > 802.1x.**
2. Select the desired NIC and select the check box to enable 802.1x.
3. Select the EAPOL version, and then enter the username and password of the authentication server.

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

Video Watermark

Encrypt custom information in videos to prevent unauthorized alteration.

1. Click **System > Security.**

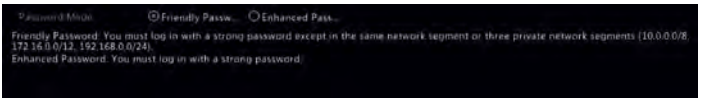


2. Select the desired camera and then select **Enable Watermark.**
3. Enter watermark content.
4. Click **Apply** to save the settings.

Password Mode

Password mode specifies the permission of strong or weak password in different modes: friendly password and enhanced password.

1. Click **System > Security > Password Mode.**



2. Friendly password is enabled by default. You may enable **Enhanced Password** as needed.
   - **Friendly Password**: If this option is selected, a strong password must be used except when login from the same network segment or one of the three private network segments (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/24).

- **Enhanced Password**: If this option is selected, a prompt for a strong password will appear when a weak password is detected. Also, only strong passwords are allowed for new users.

NOTE!

Only administrative users can configure secure password.

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

Hot Spare Configuration

Only certain NVR models support this function.

With hot spare configured, when the working device fails, the hot spare takes over service of the working data. When the working device restores normal status, it takes over service from the hot spare, and data saved to the hot spare during the period of failure is transferred back to the working device to ensure reliable and consistent data storage.

1. Click **System > Hot Spare.**
2. Select a working mode, **Normal** (default mode) for working device, or **Hot Spare** for hot spare device.



Normal

Add a hot spare device after choosing this mode; otherwise, hot spare does not take effect. Click **Custom Add** and then enter

device information, including IP address, port number and password. The username is fixed to *admin*. Click **Add**.

Hot Spare

Select **Hot Spare**, and the current device will be a hot spare for other working devices. All the working devices that the current hot spare serves are listed.



NOTE!

- After the working mode is changed, the NVR will restart with some parameters and settings changed.
- For a working device that switches to a hot spare, some of its functions will be unavailable, and some settings will be reset to defaults.
- If multiple working device fail at the same time with only one hot spare device available, one working device gets backup at a time.

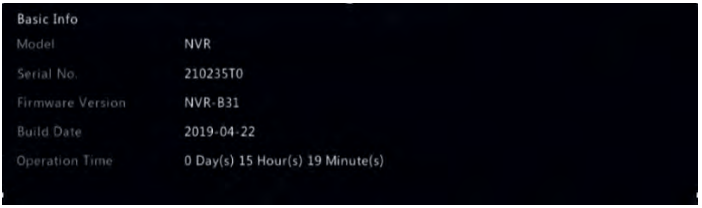
14 System Maintenance

System Information

Click **Maintain > System Info** to view the basic NVR information for maintenance purpose.

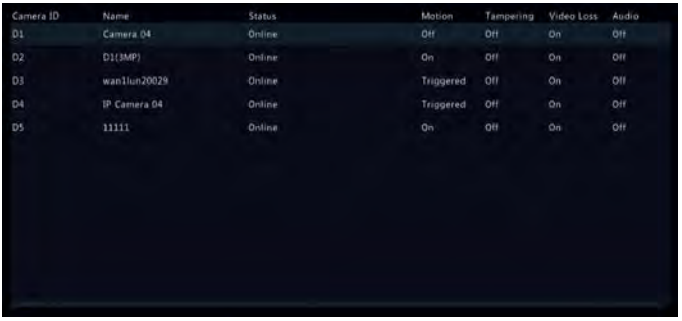
System Info

View the basic information such as the device model, serial number, firmware version, build date and operation time.



Camera status

Click the **Camera** tab to view camera status (online or offline with possible offline cause) and status of alarm functions such as motion detecion, tampering, video loss and audio detection. **Off** means disabled, and **On** means enabled.



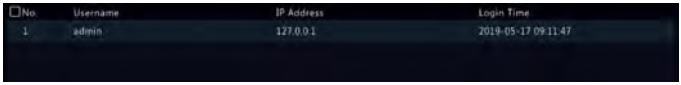
Recording status

Click the **Recording** tab to view recording status and stream settings.



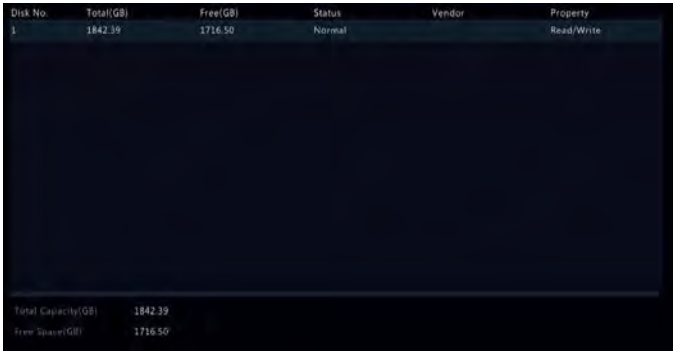
Online user

Click the **Online User** tab for information about users who are currently logged in.



Disk status

Click the **Disk** tab to view the hard disk status and disk properties.



Decoding card status

Click the **Slot Status** tab to view the decoding card status. This function is available to certain NVR models only.

Network Information

Traffic

Click **Maintain > Network Info > Traffic** to view network traffic information.



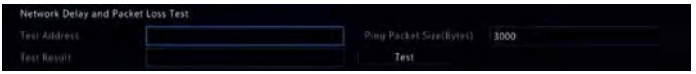
Network Detection

Click **Maintain > Network Info > Net Detect.**

To test network delay and packet loss rate, enter the test address and then click **Test**.

NOTE!

The test packet size is 3000 bytes by default and can be changed as needed.



To capture and save packets, select the USB storage device, specify the port number and IP address, and then click right to the desired NIC. The captured packets are saved as a backup file in the root directory of the USB storage device. You may click **Open** to view the file.

NOTE!

- The packet size is 1520 byes by default and can be changed as needed.
- The backup file of the captured packets is named in *NIC name_time*.pcap format.
- Packets cannot be captured if it is already started on the Web interface.
- If you use PPPoE, a virtual NIC will appear in the list after the dial-up succeeds, and you may capture packets sent to and from this NIC.

Network Settings

Click **Maintain > Network Info > Network** to view network settings.

PoE/Network Port Status

Only certain NVR models support this function.

Click **System > Network Info** to view port status. A blue port indicates that the port is in use. For PoE models, power information will be displayed.

Network Statistics

Click **Maintain > Network Info > Network Statistics.** Bandwidth usage statistics are displayed.



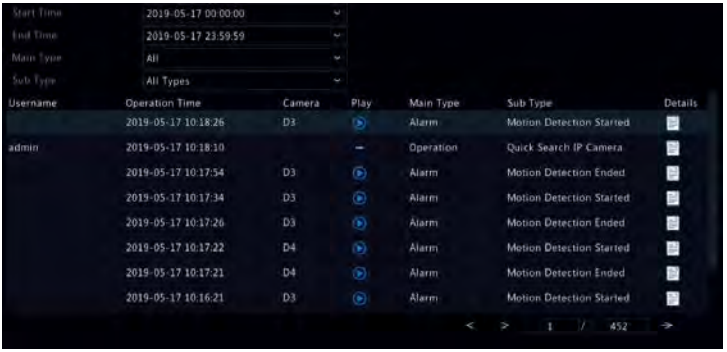
NOTE!

- Insufficient receiving bandwidth (**Idle Receive Bandwidth**) may cause the connected cameras to be offline.
- When the sending bandwidth (**Idle Send Bandwidth**) is insufficient, remote live view, playback or download may fail on the NVR.

Log Query

Logs contain information about user-performed operations and device status. By analyzing logs, you can keep track of device operation status and view detailed alarm information.

1. Click **Maintain > Log.**
2. Set query conditions, including the start and end times, main type and sub type.
3. Click **Query**.



4. If  is displayed under **Play**, you may click  to view the recording that started one minute before the alarm time and ended ten minutes after the alarm time.  means this function is not available.

5. To export logs to an external storage device, click **Export**, set the export destination and format, and then click **Backup**.

Import/Export

System Import/Export

Configurations and diagnosis information can be exported to a storage device and saved as files for backup. A configuration file can also be imported to the NVR to restore configurations. The configuration file of an NVR can be imported to multiple NVRs of the same model if you want them to use the same settings. If the imported configuration file contains camera information, the related camera will be added to all the NVRs.

Only administrative users can perform these operations.

1. Click **Maintain > Import/Export.**
2. To export device configurations, specify the destination directory and then click **Export**. An .xml file will be created in the specified directory when export is completed.
3. To import device configurations, double-click the target folder containing the .xml file, select the file, and then click **Import**.

CAUTION!

Delete files with caution. Deleted files cannot be recovered.

Diagnosis Info

The device can save diagnosis info for 14 days and will overwrite the oldest when space is full.

1. Click **Maintain > History Diagnosis Info.**



2. Select a device type:

   - **NVR**: For NVRs, history diagnosis info is generated at 00:00 every day. To export history diagnosis info, click **Export** at the bottom. To export current diagnosis info, click **Export** right to **Current Diagnosis Info**.
   - **IPC**: For IPC, history diagnosis info is generated at 00:05 every day. Select channels and then click **Export** at the bottom. To export current diagnosis info, click **Export** right to **Current Diagnosis Info**.

NOTE!

For IPC, diagnosis info is recorded based on channel, which means, if an IPC is added to multiple channels, all the channels will record diagnosis info for the IPC.

System Restoration

Use this function to restore some or all factory default settings. The NVR will restart automatically to complete this operation. Recordings and operation logs will not be deleted.

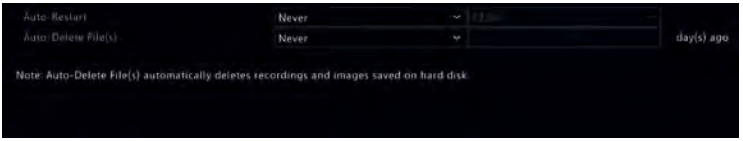
1. Click **Maintain > Restore.**

2. Click **Default** to restore factory default settings except network and user settings, or click **Factory Default** to restore all factory default settings.

Automatic Maintenance

Set the NVR to restart as scheduled and delete files (including recordings and snapshots) as needed. Only administrative users can perform this operation.

3. Click **Maintain > Auto-Function.**
4. Set an auto-restart time, and choose a way to delete files automatically.



CAUTION!

Files deleted automatically cannot be recovered.

System Upgrade

Upgrade the NVR under **Maintain > Upgrade** locally (using an upgrade file saved in a USB storage device) or by cloud (through a cloud server).

To upgrade by cloud, ensure that the NVR is connected to a fully functional DNS server (configured under **System > Network > Basic**), and click **Check** to see whether a newer version is available. The time that a cloud upgrade takes is affected by network connection status.

CAUTION!

- Make sure power is not interrupted during upgrade. A power failure during system upgrade may cause startup failure. Use an Uninterrupted Power Supply (UPS) if necessary.
- Ensure network connectivity for a cloud upgrade.

15 Shutdown

Click **Shutdown** to log out, restart or shut down as needed. To shut down the NVR, you may also long-press the power button on the front panel (if available) for about three seconds untill an on-screen message appears, and then click **Yes**.

CAUTION!

Unsaved settings will be lost if the NVR is shut down unexpectedly, for example, due to a power failure. An incorrect shutdown during a system upgrade may cause startup failures.

Part II Web-Based Operations

1 Before You Begin

You may access and manage your NVR remotely using a web browser on a PC (through the Web interface). Check the following before you begin:

- Access will be authenticated during login, and operation permissions will be required.
- The PC is operating properly and has a network connection to the NVR.
- The PC uses the Windows 7, Windows 8 or Windows 10 operating system.
- A Web browser has been installed on the PC. Microsoft® Internet Explorer® 8.0 or higher is recommended. Mozilla® Firefox, Google® Chrome and Apple® Opera browsers are also supported. You must use a 32-bit web browser, even if you are using a 64-bit operating system.
- Make sure the IP address of the recorder does not conflict with any other device on the network.



NOTE!

- The parameters that are grayed out on the Web GUI cannot be modified. The parameters and values displayed may vary with NVR model.
- The figures are for illustration purpose only and may vary with NVR model.

2 Login

1. Open a Web browser on your PC and browse to the login page by entering the IP address (**192.168.1.30** by default) of your NVR.

   You may need to install a plug-in as prompted at your first login. Close the Web browser when the installation starts.

2. In the login dialog box, enter the correct username and password (**123456** for admin) and then click **Login**.

CAUTION!

The default password is intended only for your first login. We strongly recommend you set a strong password to ensure account security.

- Strong: contains at least 8 characters from at least three of the four character types: upper-case letter, lower-case letter, special character, and number.
- Medium: contains at least 8 characters from two of the four character types: upper-case letter, lower-case letter, special character, and number.
- Weak: contains less than 8 characters from only one of the four types: upper-case letter, lower-case letter, special character, and number.

3 Live View

The **Live View** page is displayed when you are logged in. The following figure shows an example.

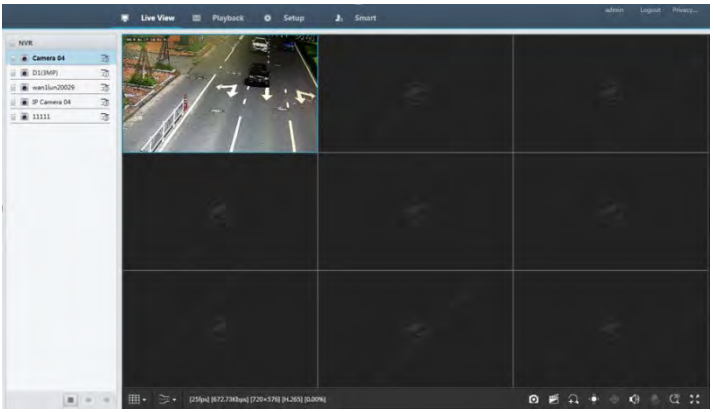


Table 3–1 Live View Window Control Buttons

Button	Description	Button	Description
	Two-way audio	/	Main/Sub stream
/	Start or stop live view in all windows	/	Previous and next screen
	Switch screen layout		Full screen
	Select stream type	[25fps] [3.96Mbps] [1920×1088]	Shows the current frame rate, bit rate, resolution, and packet loss rate
	Take a snapshot		Start zoom
	Local recording	/	Turn on or off audio; adjust sound volume.
/	Adjust MIC volume		3D positioning

Button	Description	Button	Description
	Open or close the control panel	–	–

NOTE!

- The icon means two-way audio is available. Click to start two-way audio with the NVR or a camera (depending on where the icon is displayed).
- Only the main stream is displayed when the camera is offline or it supports only one stream.
- A snapshot file is named in this format: *IP_camera ID_snapshot time.* The snapshot time is in *YYYYMMDDHHMMSSMS* format.
- By default, snapshots are saved in this directory: C:\Users*username*\Surveillance\Snap*system date*. The system date is in *yyyy-mm-dd* format.
- A local recording is named in this format: *IP_camera ID_S recording start time* E *recording end time.* The recording start and end times are in *hh-mm-ss* format.
- By default, local recordings are saved in this directory: C:\Users*username*\Surveillance\Record*system date*. The system date is in *yyyy-mm-dd* format.

4 Playback

Click **Playback** on the top to show the **Playback** page. The following figure shows an example.

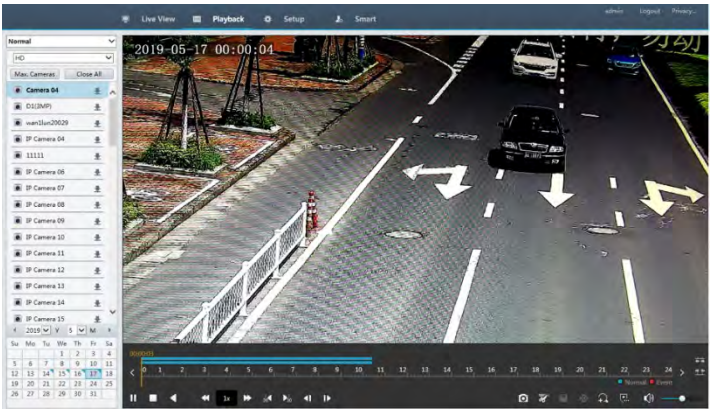
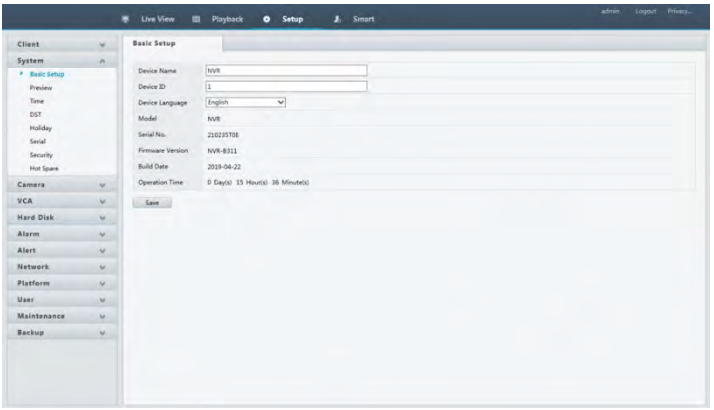


Table 4–1 Playback Control Buttons

Button	Description	Button	Description
	Play/Pause		Stop
	Reverse		Slow down or speed up
	Rewind or forward 30 seconds		Rewind or forward by frame
	Previous or next period		Clip video/pause
	Save video clip		Take a snapshot
	Zoom		Adjust sound volume; turn on or off sound

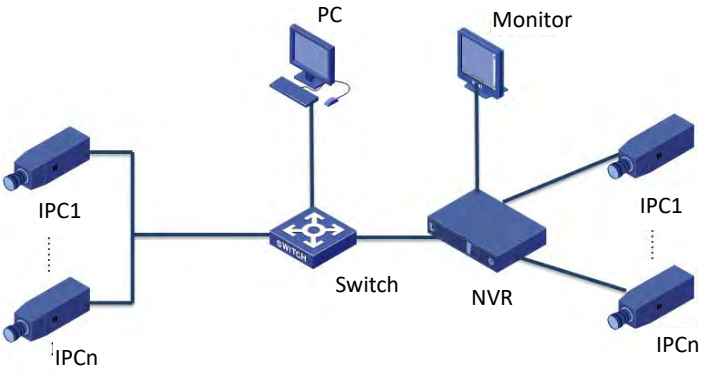
5 Configuration

Click **Setup** on the top, and then click the menus on the left to configure parameters.



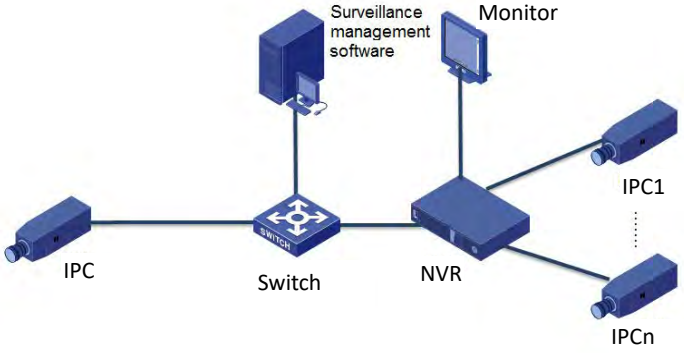
Appendix A Typical Applications

Typical Application 1



The NVR, IP cameras, and PC are connected on a private network (or LAN). The IP cameras can be connected to the NVR directly or via a switch. And you manage the NVR and the connected IP cameras through the monitor or using a web browser on the PC.

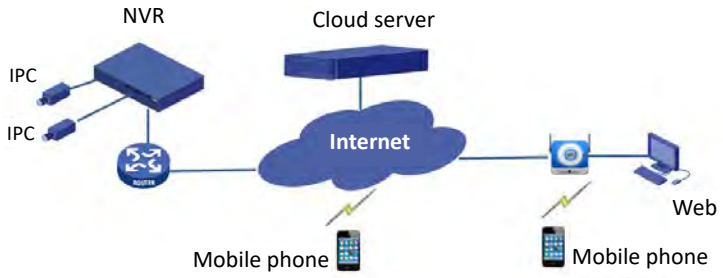
Typical Application 2



The NVR, IP cameras, and PC are connected on a private network (or LAN). The IP cameras can be connected to the NVR directly or

via a switch. The PC is installed with surveillance management software. You can manage the NVR and the connected IP cameras using the surveillance software or through the monitor.

Typical Application 3



The NVR and the connected IP cameras are located on a private network (or LAN), and you manage these devices through the cloud server, a cloud solution for device management over Internet. After registering a cloud account and properly configuring your network devices (including router), you can manage your NVR and the connected IP cameras from a PC or a mobile phone.

Appendix B Acronyms

Acronym	Description
CBR	Constant Bit Rate
DDNS	Dynamic Domain Name Service
DHCP	Dynamic Host Configuration Protocol
DST	Daylight Saving Time
DVS	Digital Video Server
FTP	File Transfer Protocol
HDMI	High Definition Multimedia Interface
HTTPS	Hypertext Transfer Protocol Over Secure Sockets Layer
IPC	IP Camera
JPEG	Joint Photographic Experts Group
MTU	Maximum Transfer Unit
NAT	Network Address Translation
NIC	Network Interface Card
NTP	Network Time Protocol
NVR	Network Video Recorder
ONVIF	Open Network Video Interface Forum
PoE	Power over Ethernet
PPPoE	Point-to-Point Protocol over Ethernet
PTZ	Pan, Tilt, Zoom
P2P	Peer-to-Peer
RAID	Redundant Arrays of Independent Disks
RTSP	Real-Time Streaming Protocol
SDK	Software Development Kit
S.M.A.R.T.	Self-Monitoring, Analysis and Reporting Technology
UPnP	Universal Plug-and-Play
USB	Universal Serial Bus
VGA	Video Graphics Array
VBR	Variable Bit Rate

Appendix C FAQs

Problem	Possible Cause and Solution
Forgot the login password	Double-click the lower left corner of the login dialog box as admin. A dialog box appears. • Note down the serial number and then contact your dealer for a temporary password. Log in with the temporary password and then reset your password. • Use your mobile surveillance app to scan the QR code **(Settings > Forgot Device Password).**
The Web plugin (ActiveX) cannot be loaded.	• Close your web browser when the installation starts. • Disable the firewall and close the anti-virus program on your computer. • Enable your Internet Explorer (IE) to check for newer versions of the stored pages every time you visit the webpage (**Tools > Internet Options > General > Settings**). • Add your NVR's IP address to the trusted sites in your IE (**Tools > Internet Options > Security**). • Add your NVR's IP address to the Compatibility View list in your IE (**Tools > Compatibility View Settings**). • Clear your IE's cache.
No images are displayed in live view on the Web interface.	Check if the bit rate is 0Mbps in the live view window. • If yes, check if the firewall has been disabled, and the anti-virus program has been stopped on your computer. • If not, maybe it is because the graphics card driver on your computer is not working properly. Try installing the driver again.

Problem	Possible Cause and Solution
A camera is offline, and **No Link** is displayed.	Click **Maintain > System Info > Camera.** The cause is displayed under **Status**. Common causes include disconnected network, incorrect username or password, weak password, insufficient bandwidth. • Check network connection and network configurations. • If it indicates incorrect username or password, check that the camera password set in the NVR is the one used to access the camera's Web interface. • If it indicates denied access for weak password, log in to the camera's Web interface and set a strong password. • If it indicates insufficient bandwidth, delete other online IP devices in the NVR.
The NVR displays live video for some cameras and **No Resource** for others.	• Set the camera to encode the sub stream, and decrease its resolution to D1. • Set the NVR to use the sub stream first for live view.
A camera goes online and offline repeatedly.	• Check if network connection is stable. • Upgrade the firmware for the camera and the NVR. Contact your dealer for the latest versions.
Live view is normal, but the recording cannot be found.	• Check that a recording schedule has been properly configured. • Check if the time and time zone configured in the NVR are correct. • Check if the hard disk storing the recording has been damaged. • Check if the desired recording has been overwritten.

Problem	Possible Cause and Solution
Motion detection is not effective.	• Check that motion detection is enabled, and the motion detection area is properly configured. • Check that detection sensitivity is properly set. • Check that the arming schedule is properly configured.
A hard disk cannot be identified by the NVR.	• Use the power adapter delivered with your NVR. • Power down the NVR and then mount the hard disk again. • Try another disk slot. • The disk is not compatible with your NVR. Contact your dealer for a list of compatible disk models.
The mouse does not work.	• Use the mouse delivered with your NVR. • Make sure no cable is extended.



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 QoS 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 QoS: 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

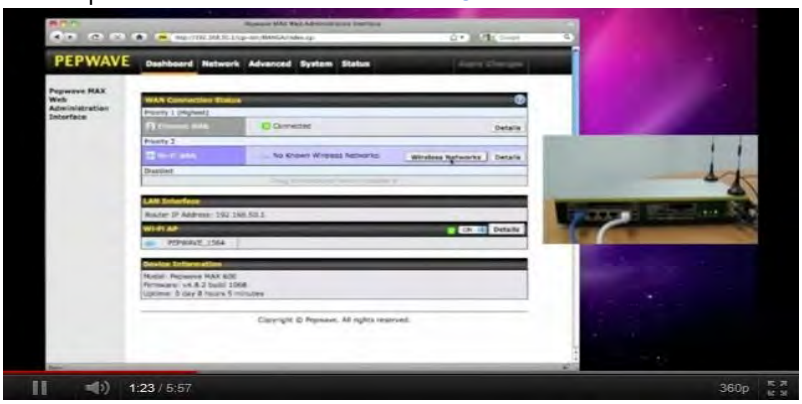
The Surf SOHO is a professional-grade router that is secure, reliable, and easy to use.

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/UCkVQThLKO4

 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
QoS	Quality 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 Jack: 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 RJ45 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.

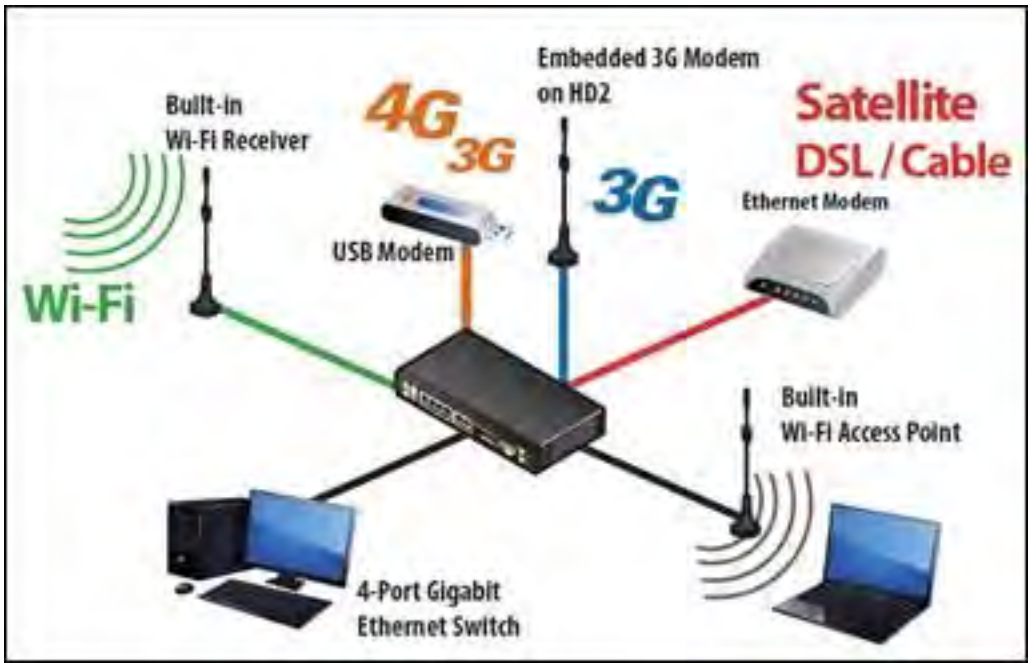
6.2 Constructing the Network

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

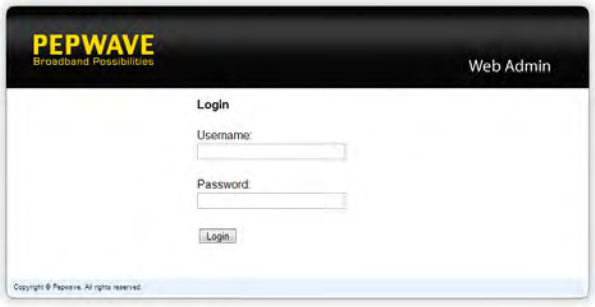


6.3 Configuring the Network Environment

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.

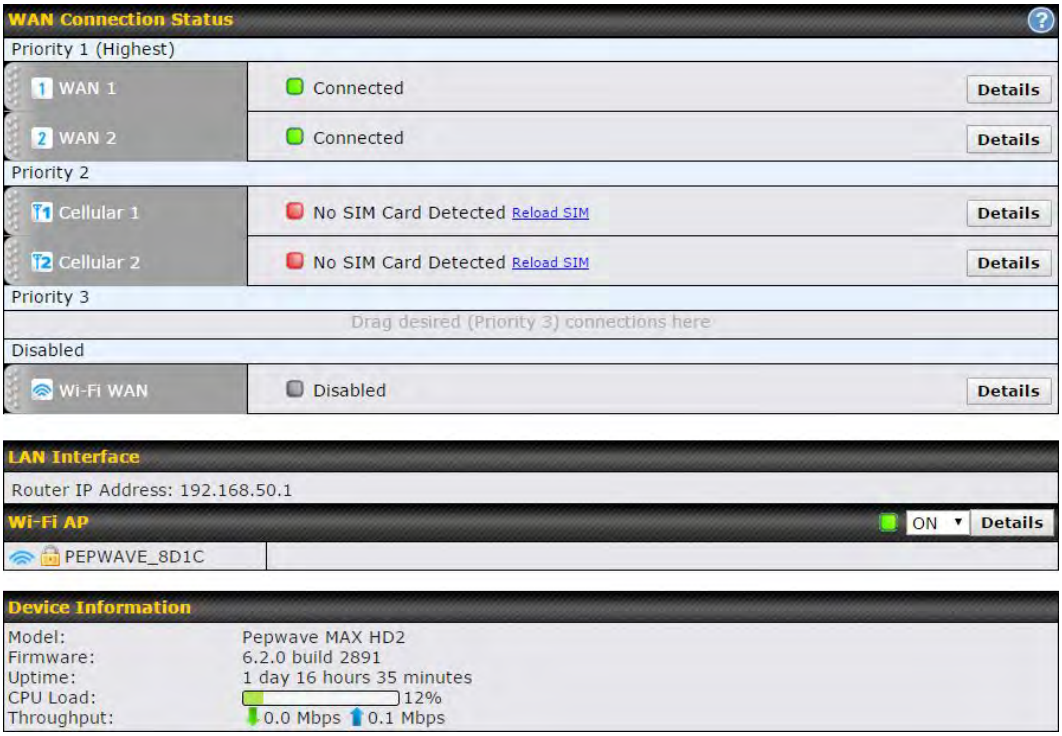
7 Connecting to the Web Admin Interface

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".

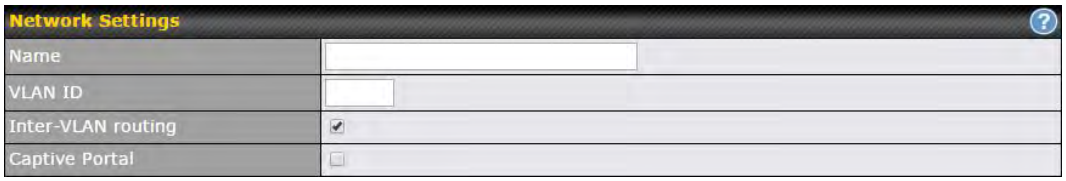
Alternatively, a red "X" means that there are no settings using the VLAN. You can delete that VLAN by clicking the red "X"

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

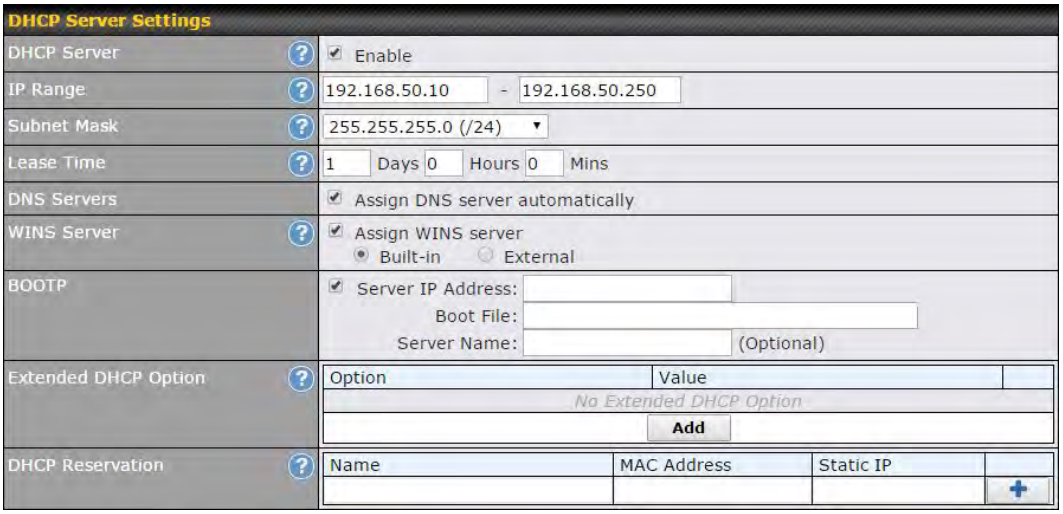


IP Settings	
IP Address	The IP address and subnet mask of the Pepwave router on the LAN.

 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.**

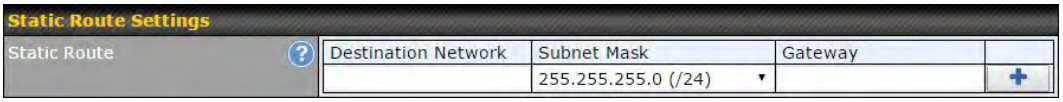


LAN Physical Settings

 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.

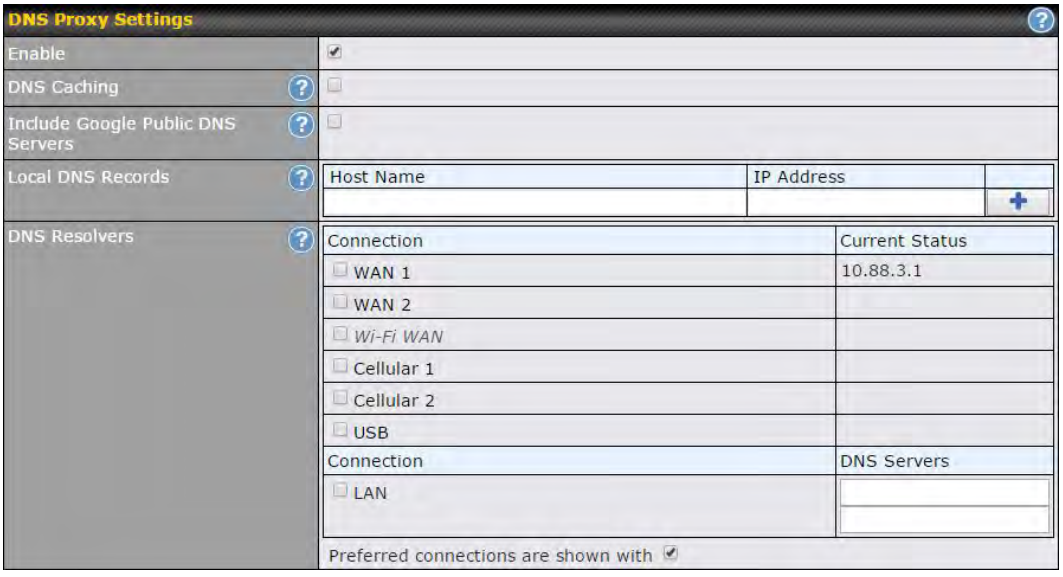


Static Route Settings

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). Queries 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.



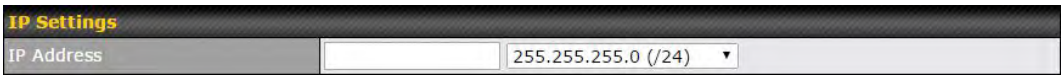
To add a new LAN, click the **New LAN** button. To change LAN settings, click the name of the LAN to change under the **LAN** heading.

 Copyright @ 2017 Pepwave



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



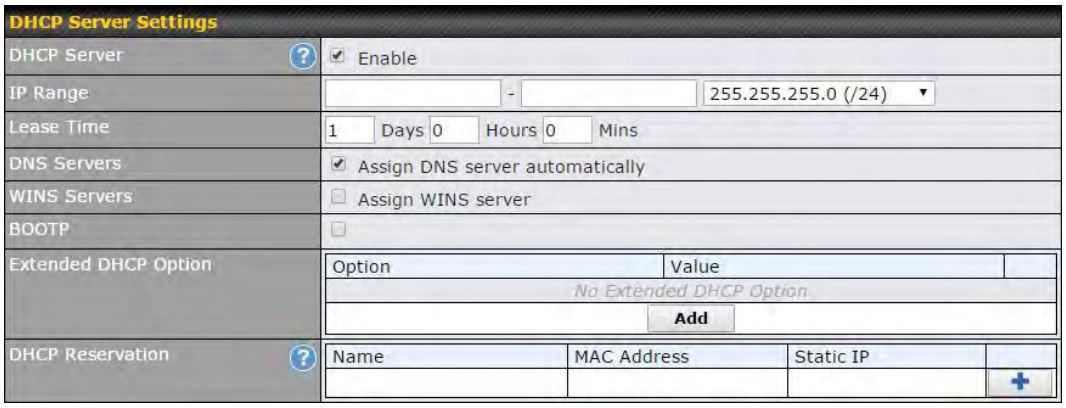


IP Settings	
IP Address & Subnet Mask	Enter the Pepwave router's IP address and subnet mask values to be used on the LAN.



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**.

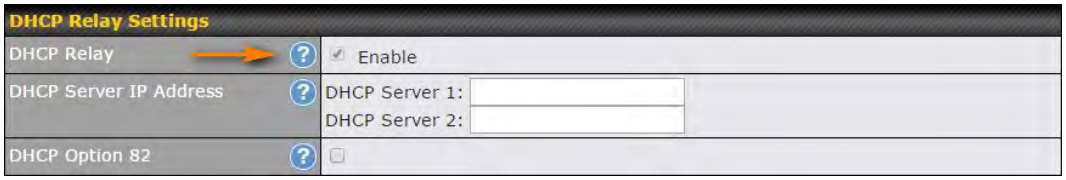
BOOTP

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.

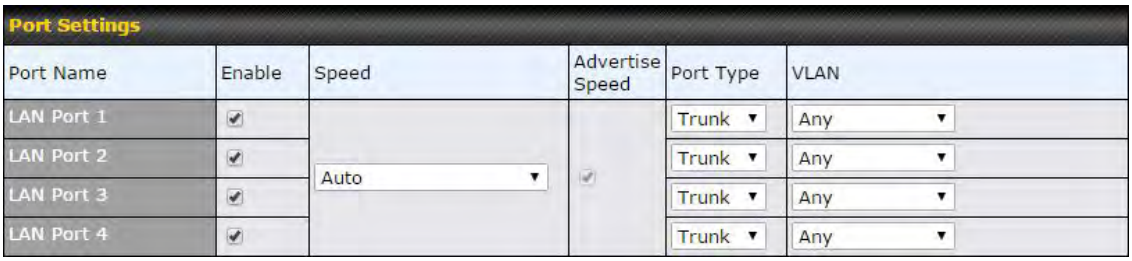
Once DHCP is set up, configure **LAN Physical Settings**, **Static Route Settings** and **DNS**

 Copyright @ 2017 Pepwave

Proxy Settings as noted above.

8.2 Port Settings

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



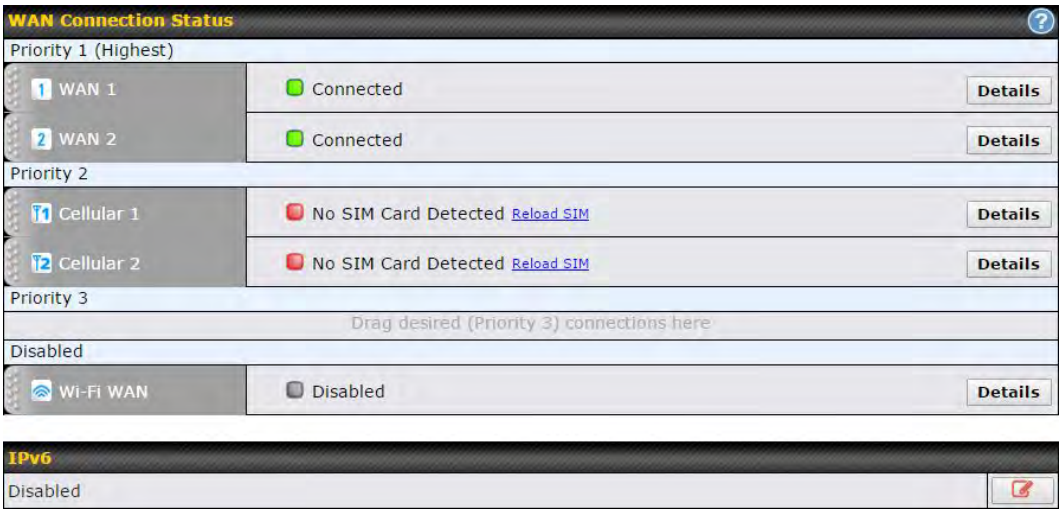
On this screen, you can enable specific ports, as well as determine the speed of the LAN ports, whether each port is a trunk or access port, can well as which VLAN each link belongs to, if any.

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.

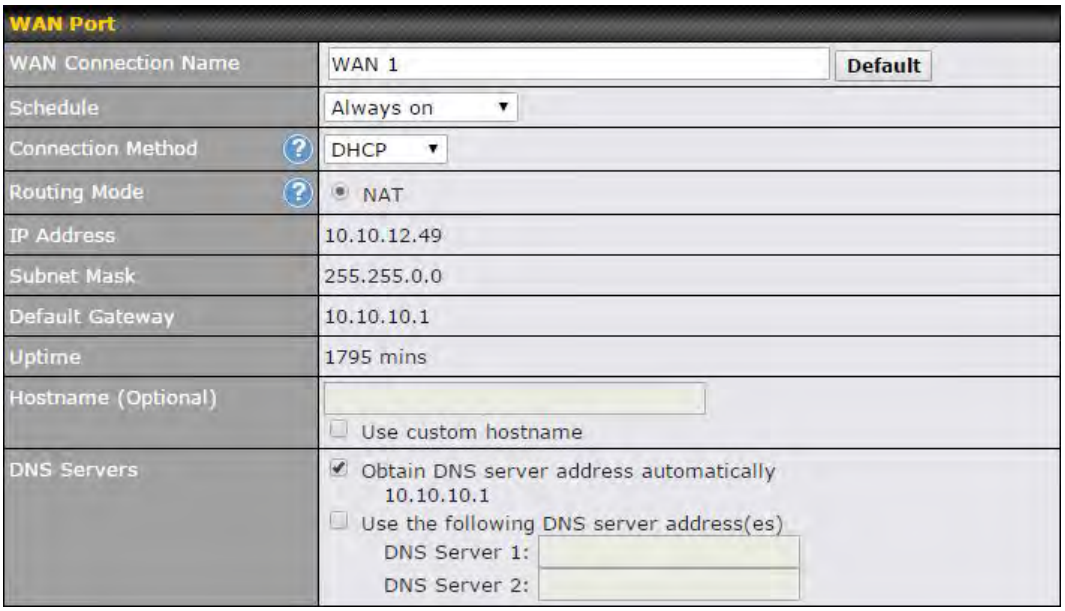
You can also set priorities on the **Dashboard**. Click the **Details** button in the corresponding row to modify the connection setting.

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**.

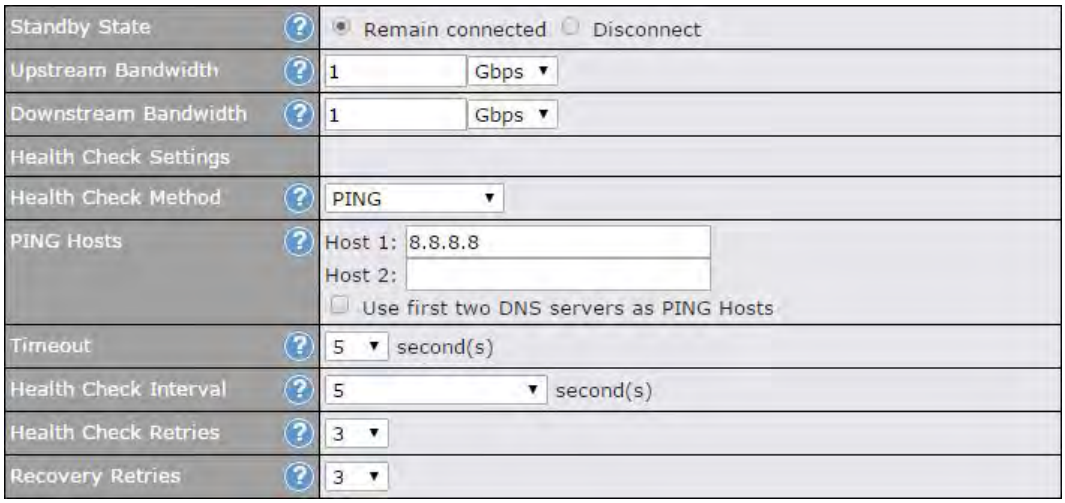
 Copyright @ 2017 Pepwave



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.

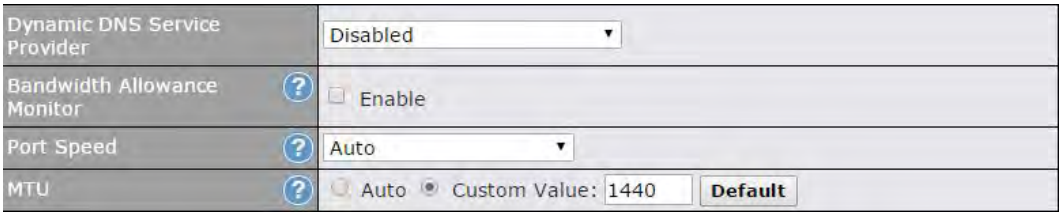


WAN Port (Section 2)

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

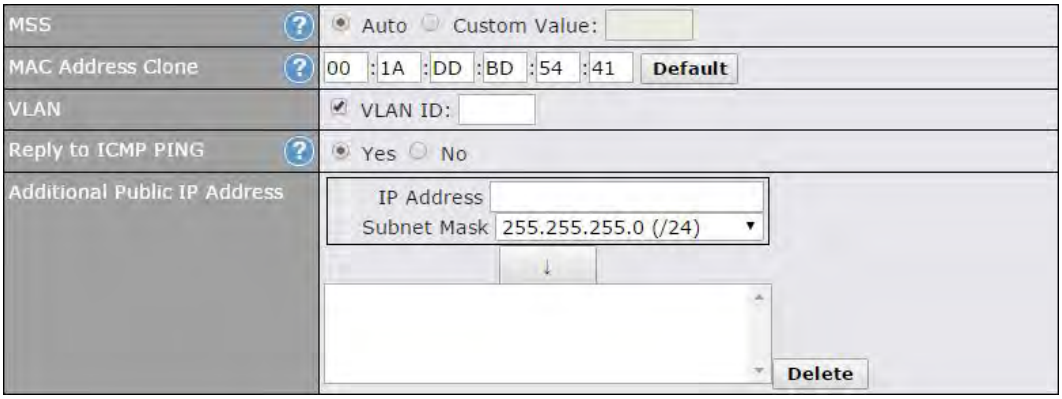
	health check DNS servers, regardless of whether the result is positive or negative.
Timeout	If a health check test cannot be completed within the specified amount of time, the test will be treated as failed.
Health Check Interval	This is the number of consecutive check failures before treating a connection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

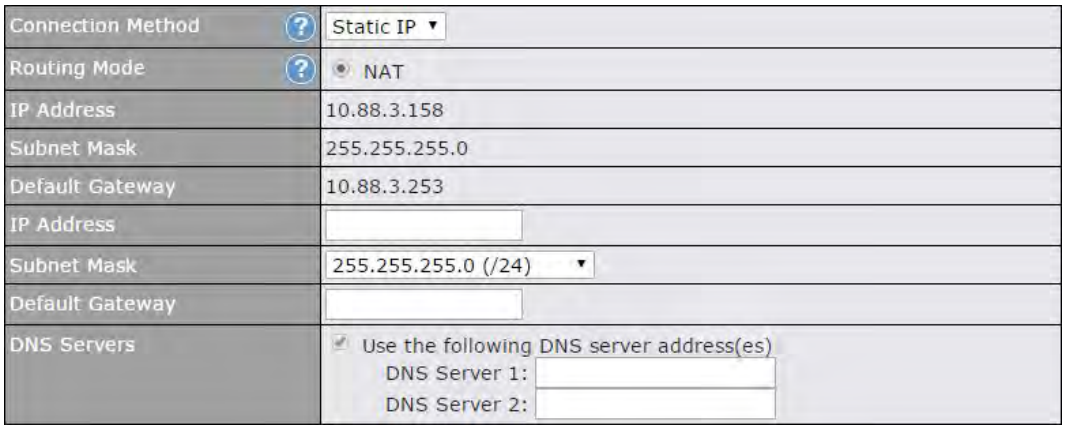


DHCP Connection Settings	
Routing Mode	NAT allows substituting the real address in a packet with a mapped address that is routable on the destination network. By clicking the help icon in this field, you can display the **IP Forwarding** option, if your network requires it.
IP Address/ Subnet Mask/ Default 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.

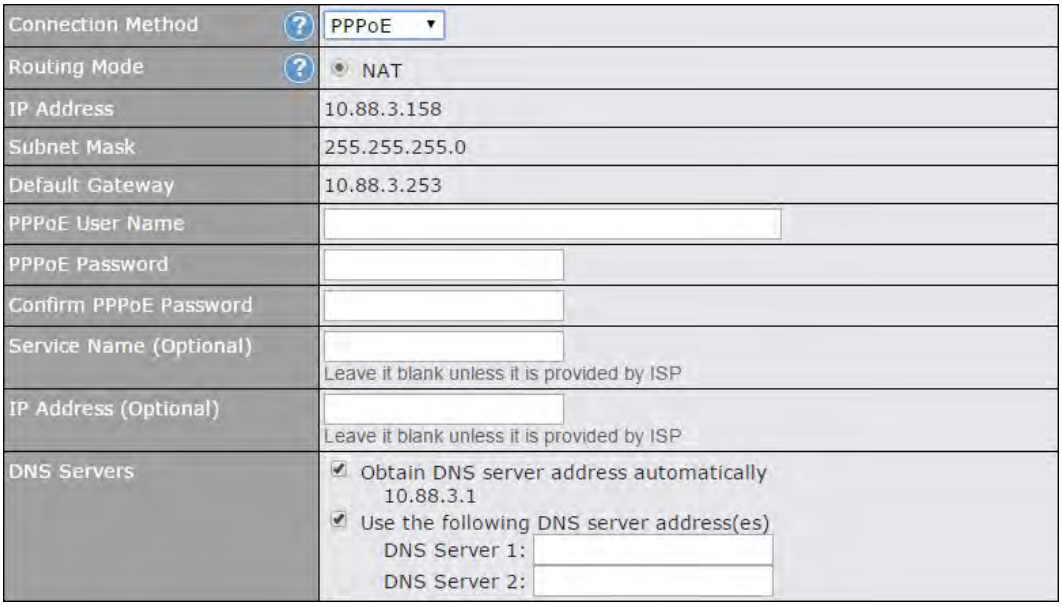


Static IP Settings	
Routing Mode	NAT allows substituting the real address in a packet with a mapped address that is routable on the destination network. By clicking the help icon in this field, you can display the **IP Forwarding** option, if your network requires it.
IP Address / Subnet Mask / Default 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



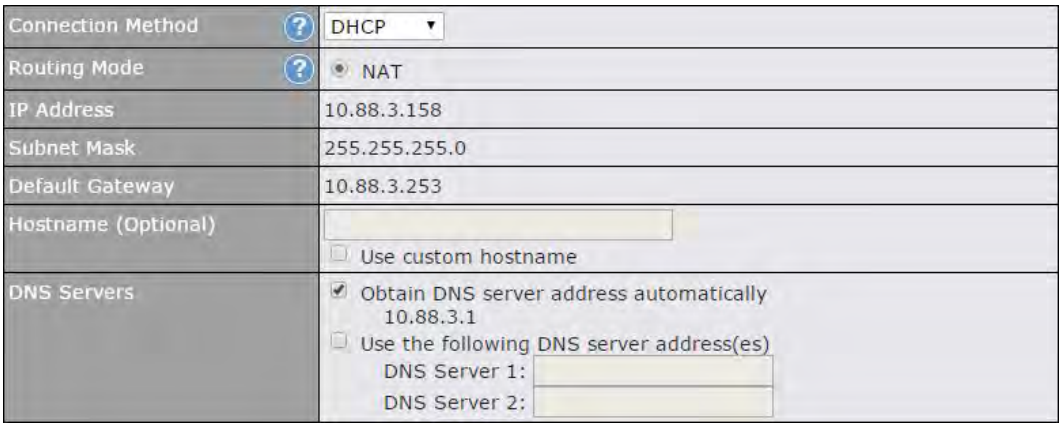
PPPoE Settings	
Routing Mode	NAT allows substituting the real address in a packet with a mapped address that is routable on the destination network. By clicking the help icon in this field, you can display the **IP Forwarding** option, if your network requires it.
IP Address / Subnet Mask / Default Gateway	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

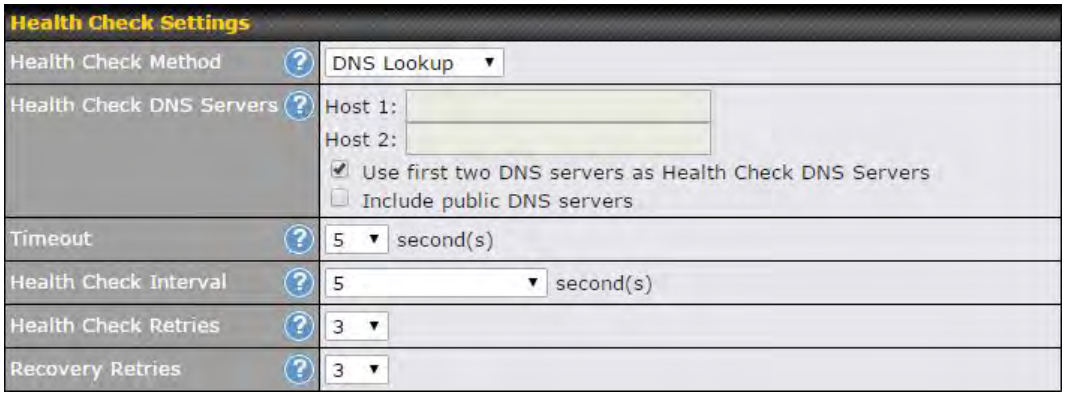
L2TP has all the compatibility and convenience of PPTP with greater security. Combine this with IPsec for a good balance between ease of use and security.



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

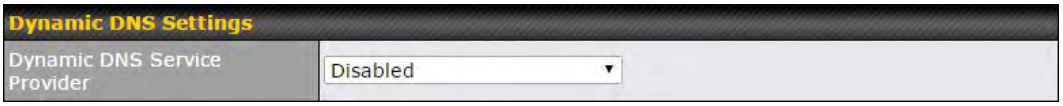
DNS Servers	Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting **Obtain DNS server address automatically** results in the DNS servers assigned by the PPPoE server 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

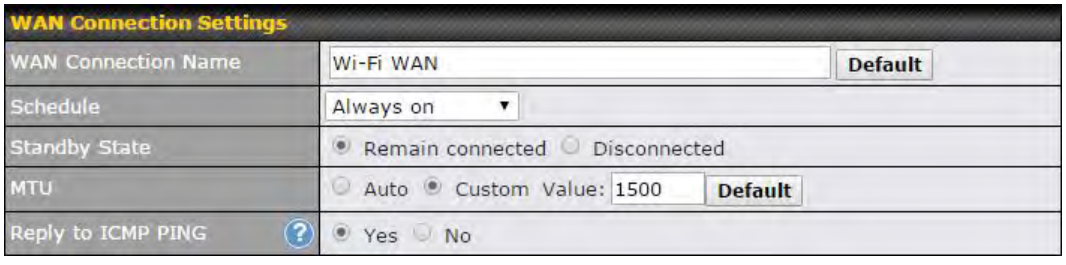
Health Check Retries	This is the number of consecutive check failures before treating a connection as down.
Recovery Retries	This is the number of responses required after a health check failure before treating a connection as up again.



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.

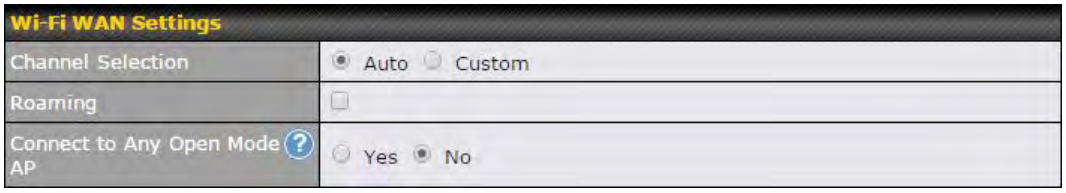
9.2 Wi-Fi WAN

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 adjust 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.

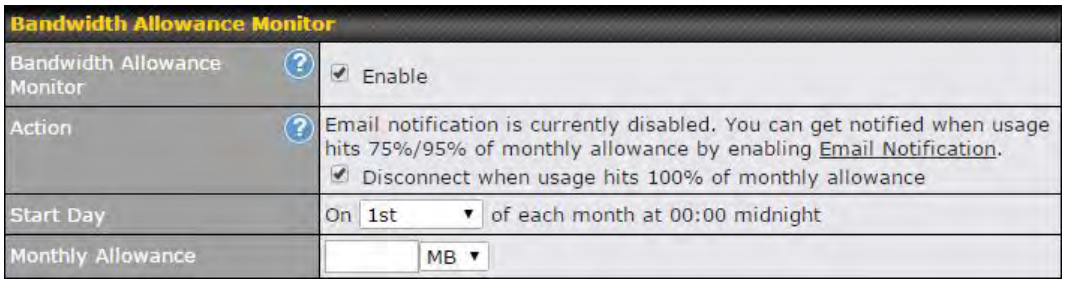


Wi-Fi WAN Settings	
Channel Selection	Determine whether the channel will be automatically selected. If you select custom, the following table will appear:



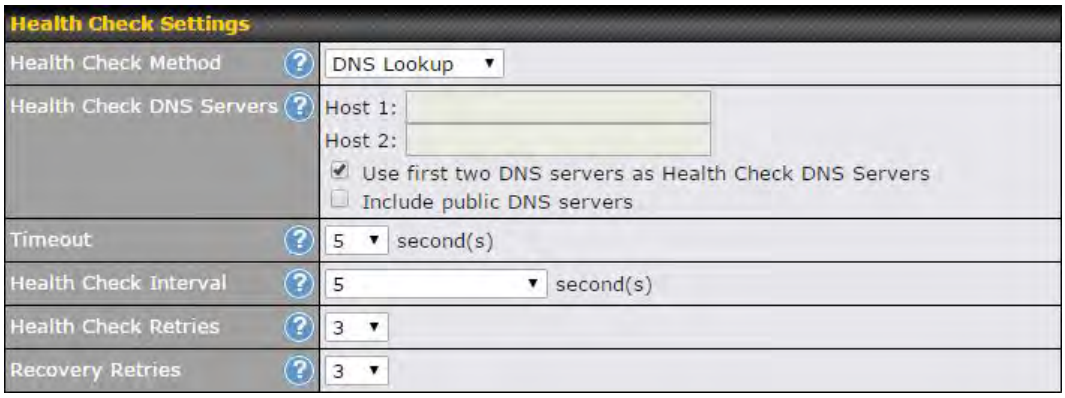
 Copyright @ 2017 Pepwave

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



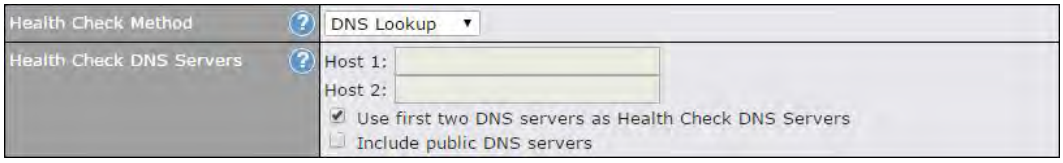
ICMP ping packets will be issued to test the connectivity with a configurable target IP address or hostname. A WAN connection is considered as up if ping responses are received from either one or both of the ping hosts.

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

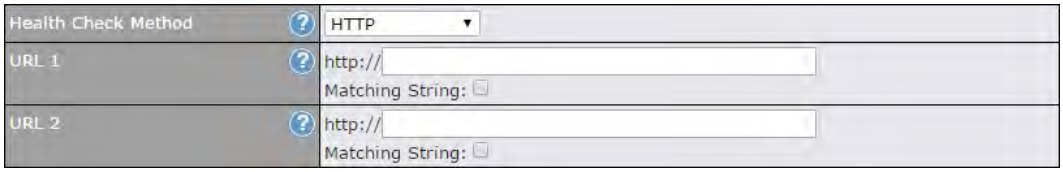
This field allows you to specify two DNS hosts' IP addresses with which connectivity is to be tested via DNS Lookup.

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.

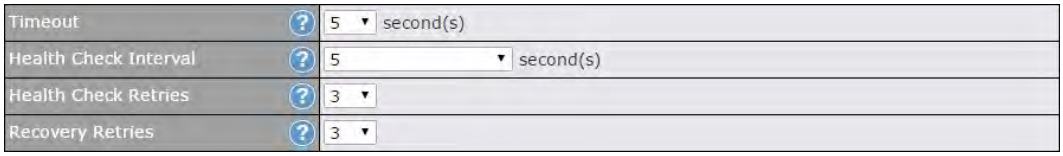
URL 2

WAN Settings>WAN Edit>Health Check Settings>URL2

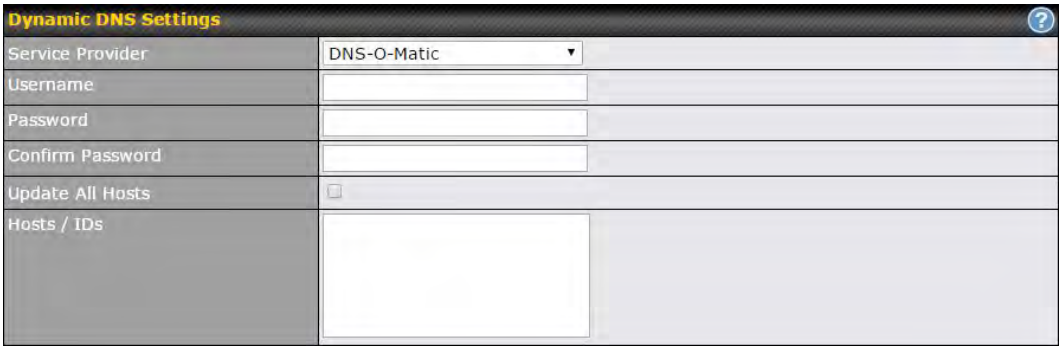
If **URL2** is also provided, a health check will pass if either one of the tests passed.

 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.

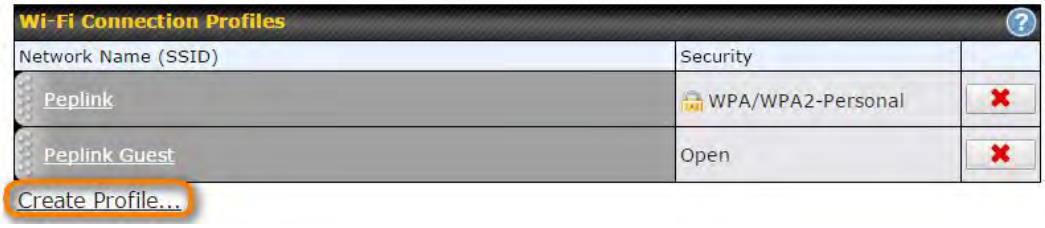
A dynamic DNS update is performed whenever a WAN's IP address is changed, such as when an IP is changed after a DHCP IP refresh or reconnection.

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:

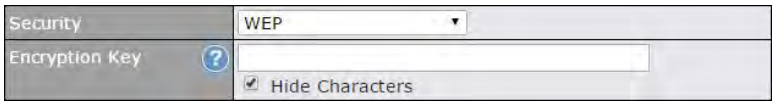


Wi-Fi Connection Profile Settings	
Type	Select whether the network will connect automatically or manually.
Network Name (SSID)	Enter a name to represent this Wi-Fi connection.
	This option allows you to select which security policy is used for this wireless network. Available options:

- **Open**

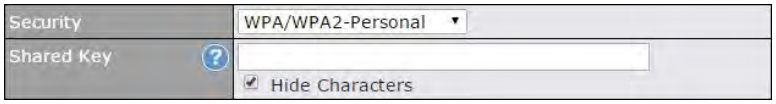


- **WEP**

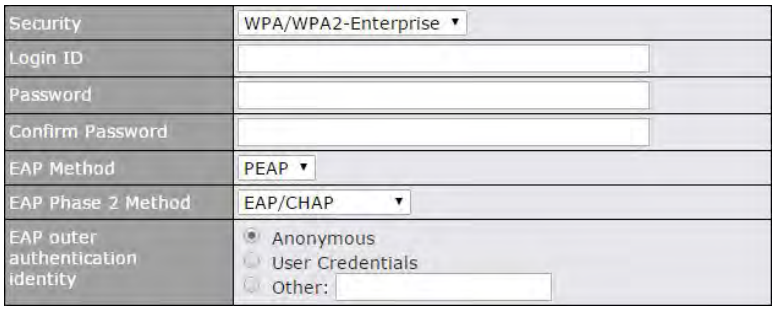


 Copyright @ 2017 Pepwave

- **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

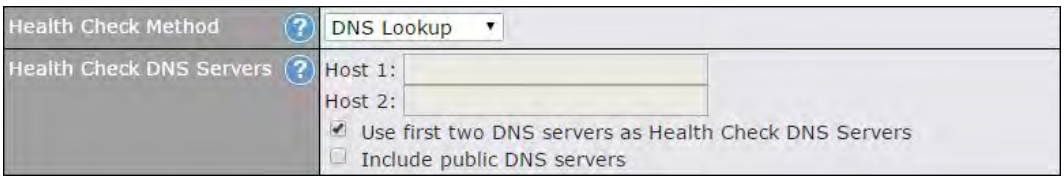


ICMP ping packets will be issued to test the connectivity with a configurable target IP address or hostname. A WAN connection is considered as up if ping responses are received from either one or both of the ping hosts.

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.

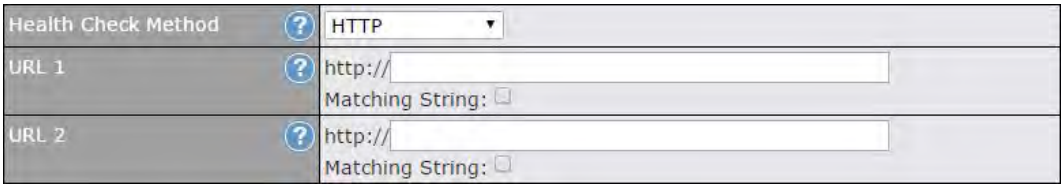
If **Use first two DNS servers as Health Check DNS Servers** is checked, the first two DNS servers will be the DNS lookup targets for checking a connection's health. If the box is not checked, **Host 1** must be filled, while a value for **Host 2** is optional.

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.

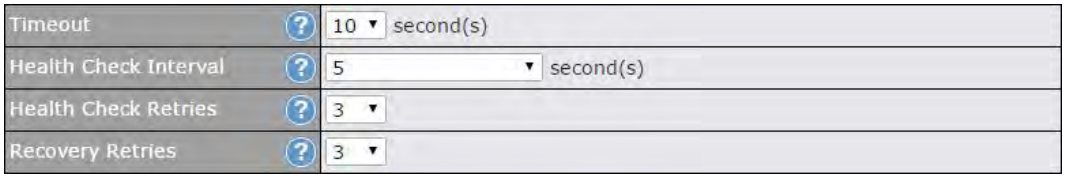
Health Check Method: HTTP

 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.



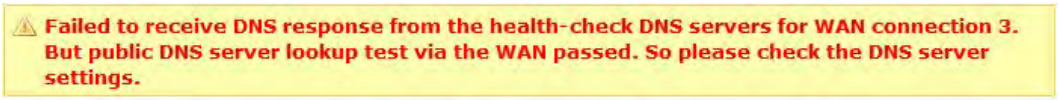
Other Health Check Settings	
Timeout	This setting specifies the timeout in seconds for ping/DNS lookup requests. The default timeout is **5 seconds**.
Health Check Interval	This setting specifies the time interval in seconds between ping or DNS lookup requests. The default health check interval is **5 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

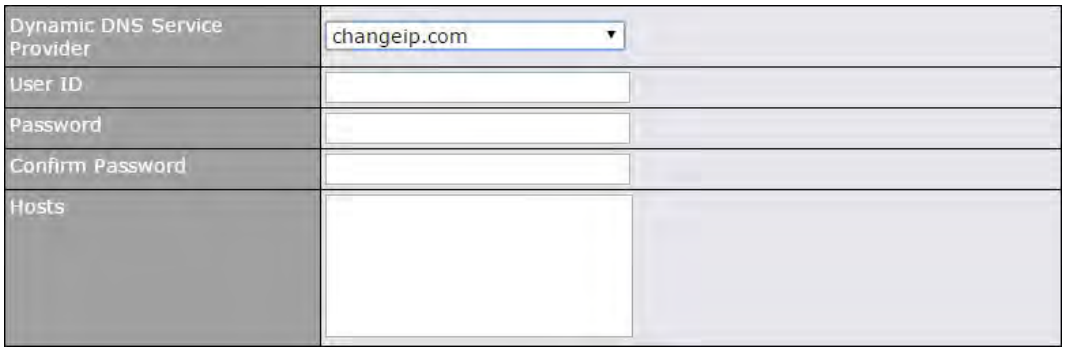
Pepwave routers are capable of registering the domain name relationships to dynamic DNS service providers. Through registration with dynamic DNS service provider(s), the default public Internet IP address of each WAN connection can be associated with a host name. With dynamic DNS service enabled for 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

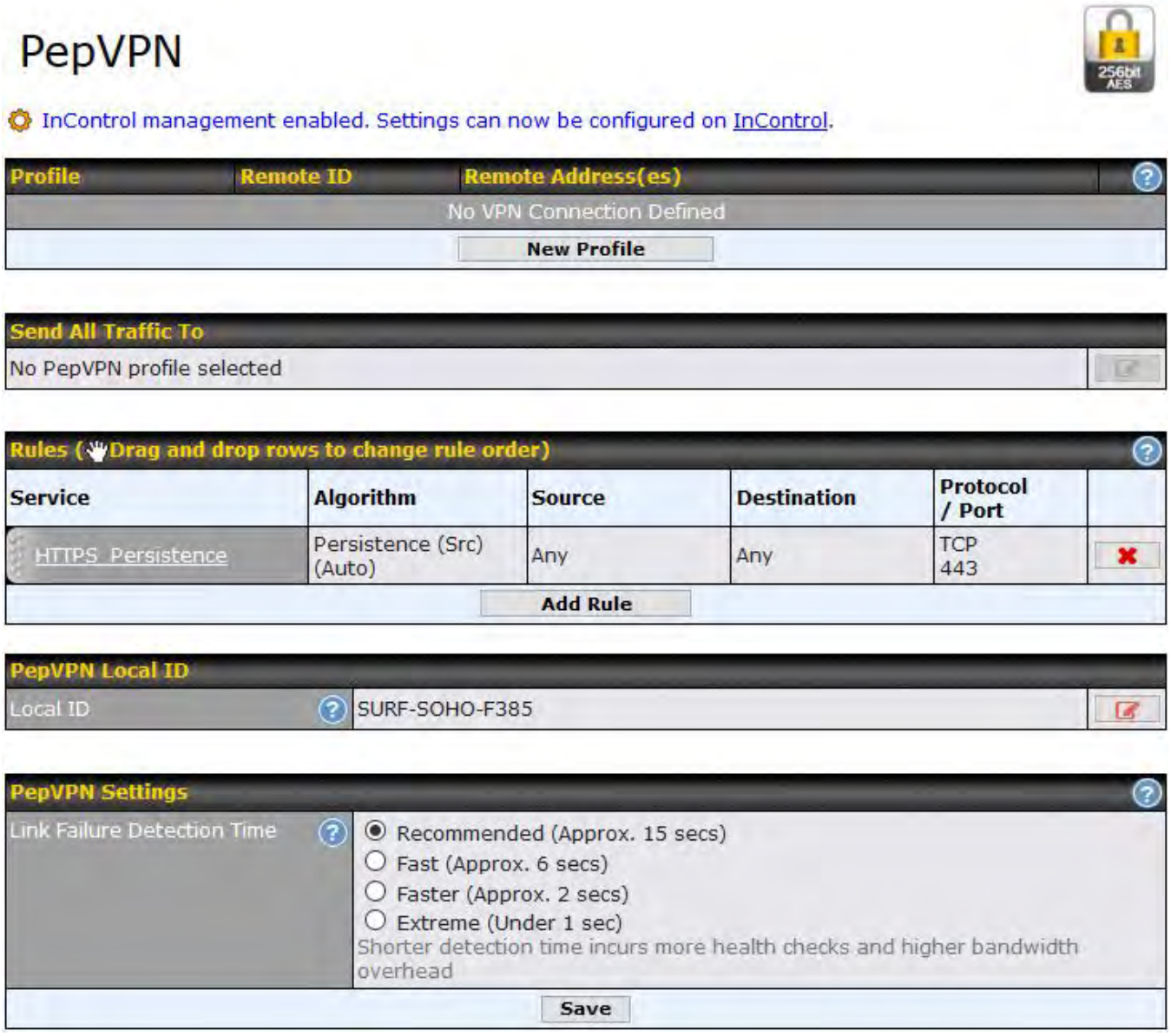
In order to use dynamic DNS services, appropriate host name registration(s) and a valid account with a supported dynamic DNS service provider are required. A dynamic DNS update is performed whenever a WAN's IP address changes (e.g., the IP is changed after a DHCP IP refresh, reconnection, etc.). Due 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.

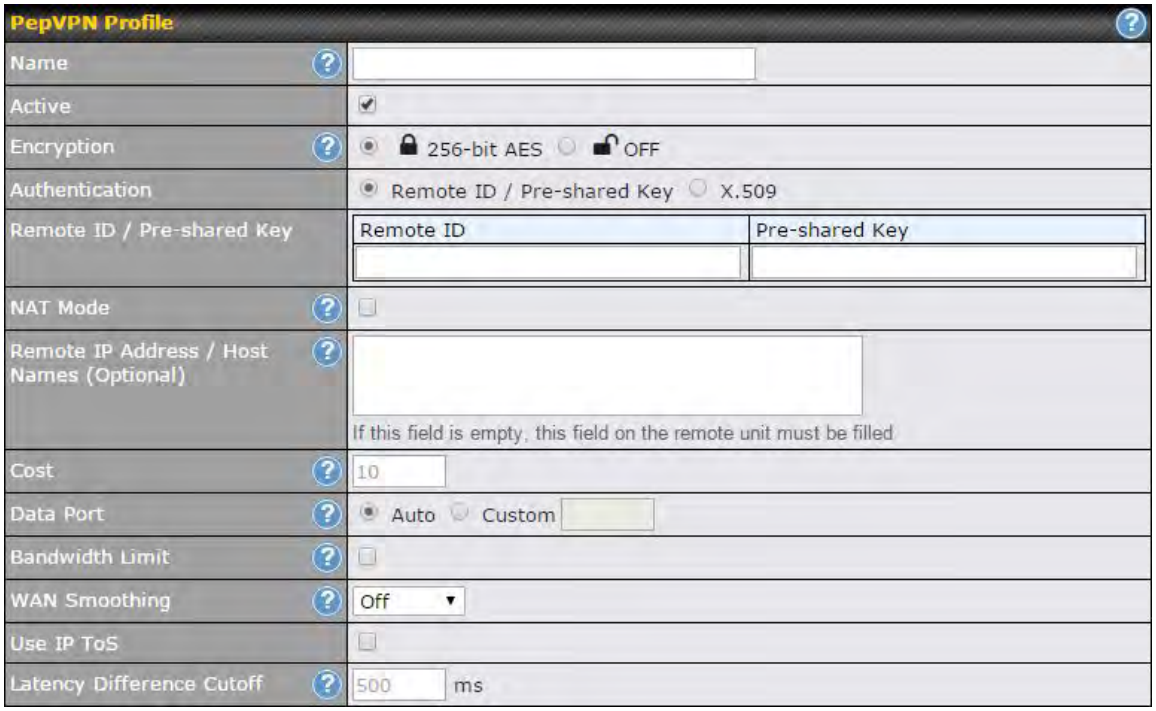
10 PepVPN

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

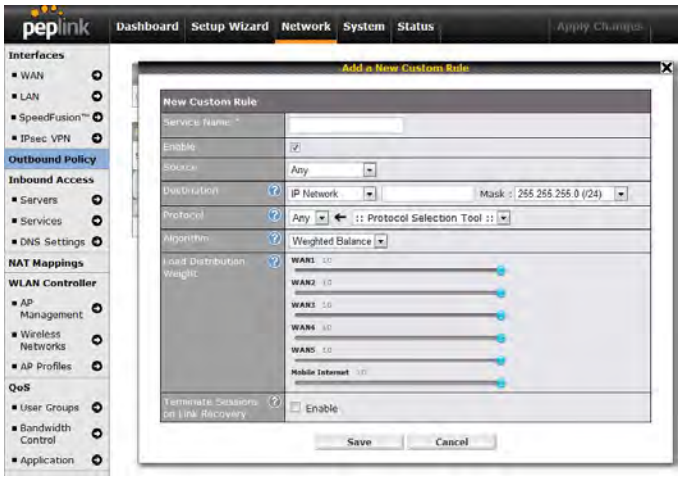
 Copyright @ 2017 Pepwave

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!

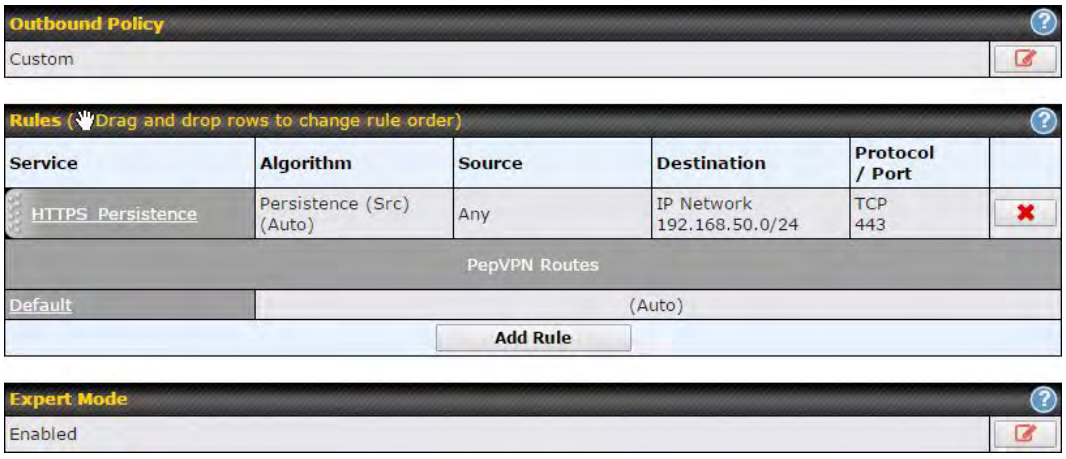


http://youtu.be/rKH4AS_bQnE

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.

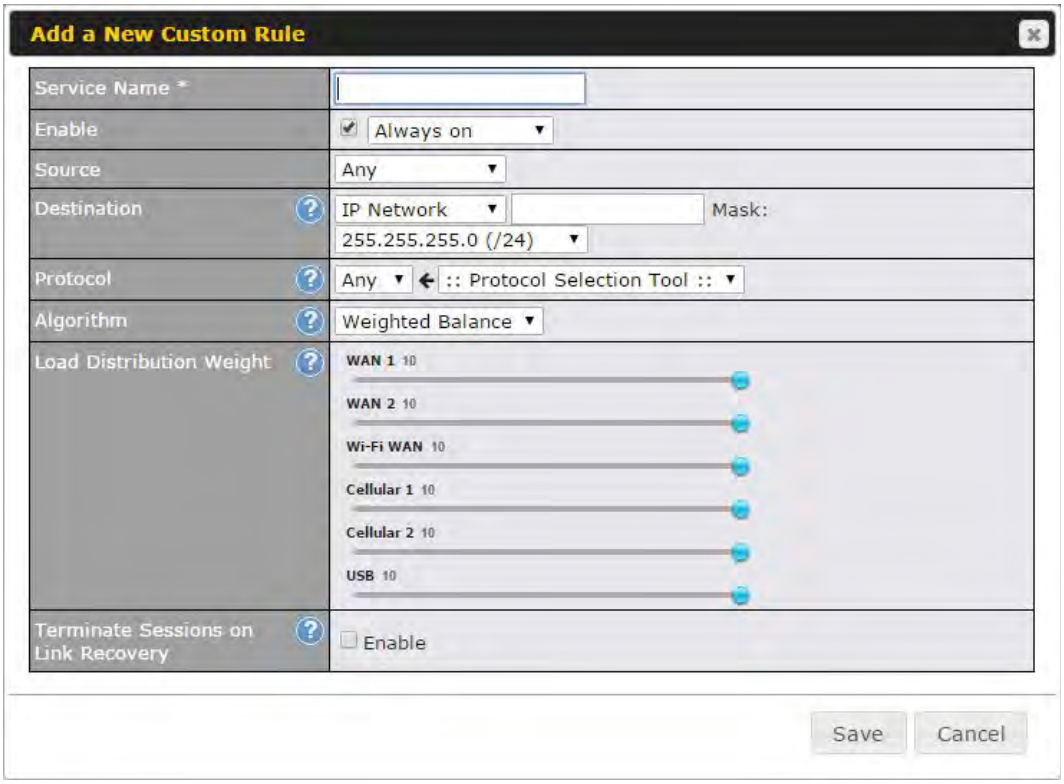
To rearrange the priority of outbound rules, drag and drop them into the desired sequence.



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.

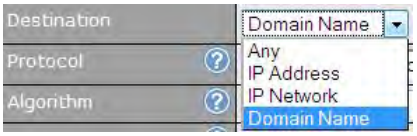
To create a custom rule, click **Add Rule** at the bottom of the table. Note that some Pepwave routers display this button at **Advanced>PepVPN>PepVPN Outbound Custom Rules**.

 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.

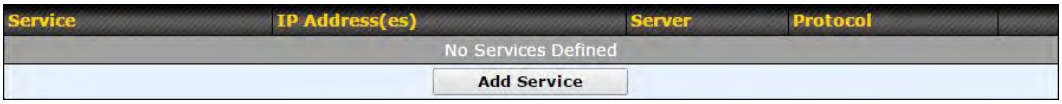
Terminate Sessions on Link Recovery

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.

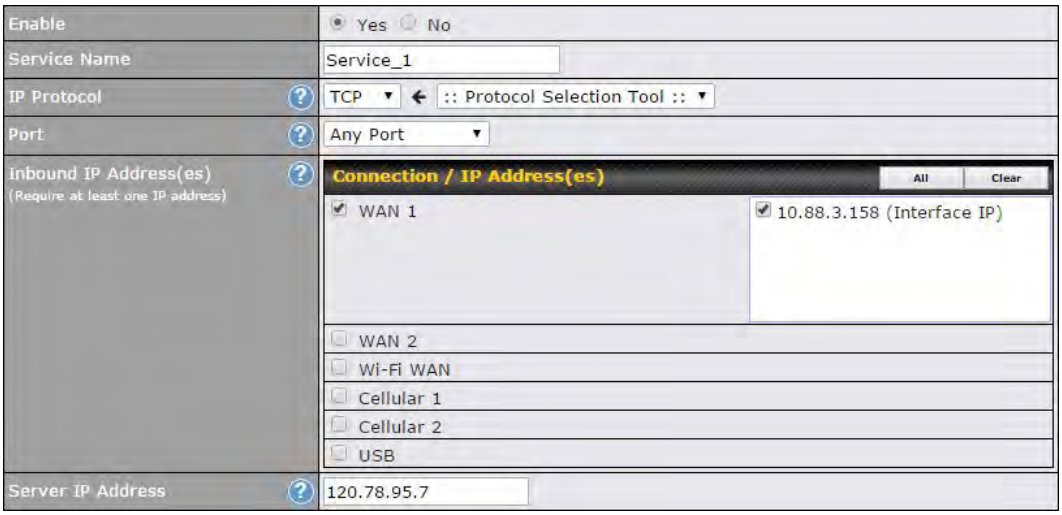
11 Port Forwarding

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**.

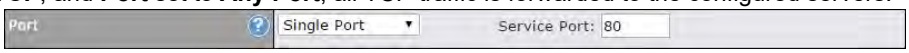


Port Forwarding Settings	
Enable	This setting specifies whether the inbound service takes effect. When **Enable** is checked, the inbound service takes effect: traffic is matched and actions are taken by the Pepwave router based on the other parameters of the rule. When this setting is disabled, the 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.



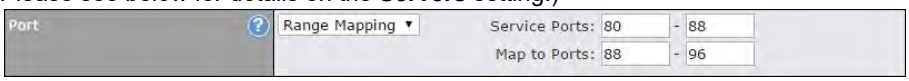
Port Range: traffic that is received by the Pepwave router via the specified protocol at the specified port range is forwarded via the same respective ports to the LAN hosts specified by the **Servers** setting. For example, with **IP Protocol** set to **TCP**, and **Port** set to **Port Range** and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

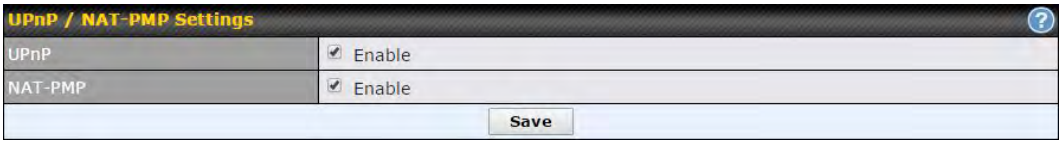
UPnP and NAT-PMP are network protocols which allow a computer connected to the LAN port to automatically configure the router to allow parties on the WAN port to connect to itself. That way, the process of inbound port forwarding becomes automated.

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.



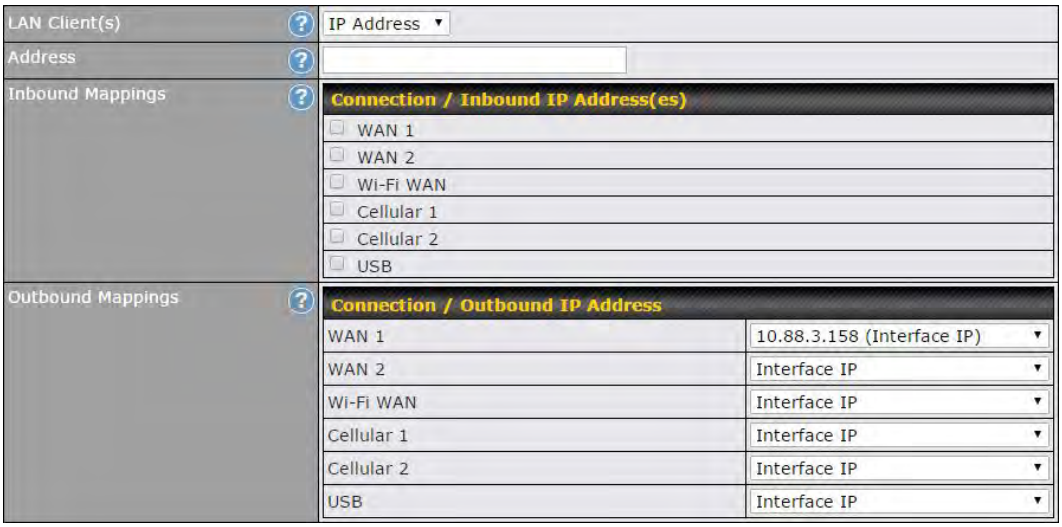
When the options are enabled, a table listing all the forwarded ports under these two protocols can be found at **Status>UPnP / NAT-PMP**.

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.

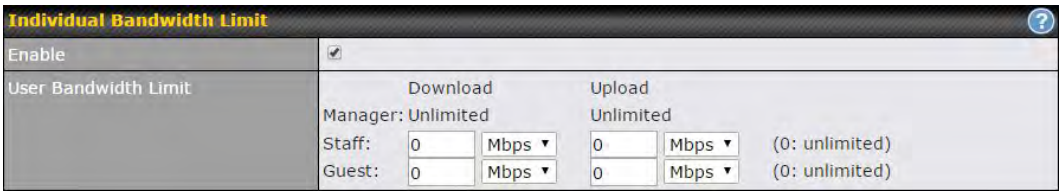
Important Note
Inbound firewall rules override the **Inbound Mappings** settings.

 Copyright @ 2017 Pepwave

13 QoS

13.1 Bandwidth Control

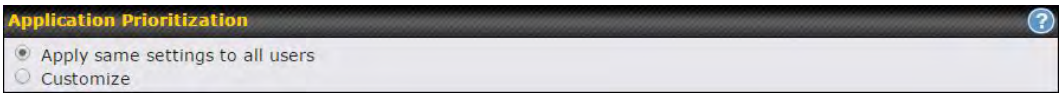
You can define a maximum download speed (over all WAN connections) and upload speed (for each WAN connection) that each individual Staff and Guest member can consume. No limit can be imposed on individual Manager members. By default, download and upload bandwidth limits are set to unlimited (set as **0**).



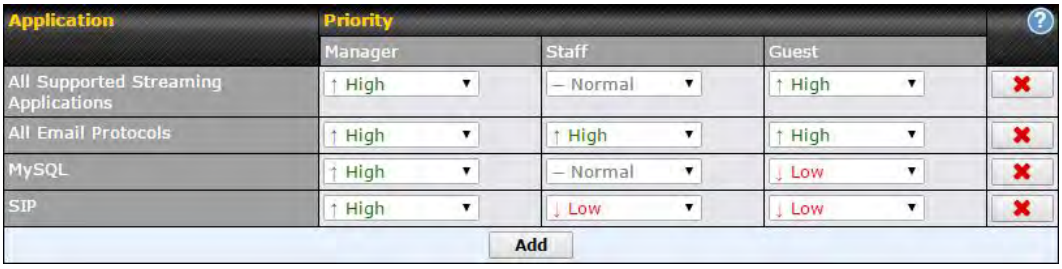
13.2 Application

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.

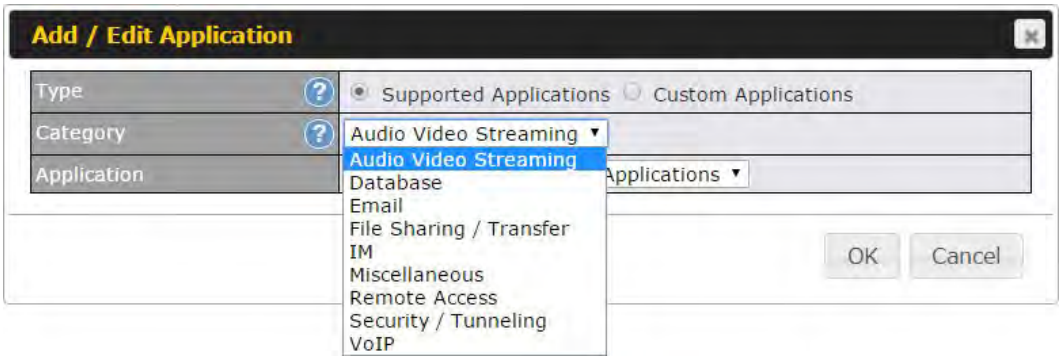


 Copyright @ 2017 Pepwave

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.

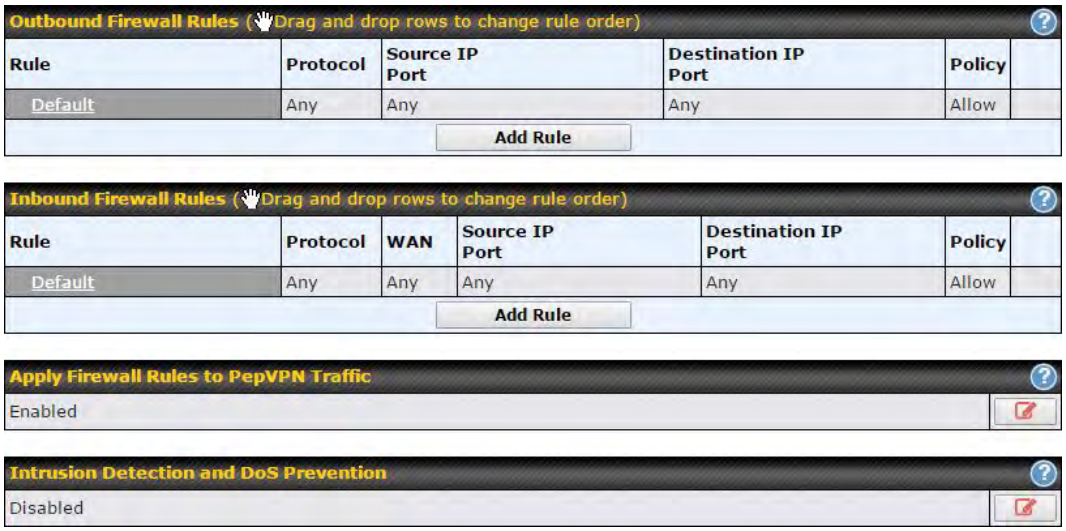
The firewall functionality of Pepwave routers supports the selective filtering of data traffic in both directions:

 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:

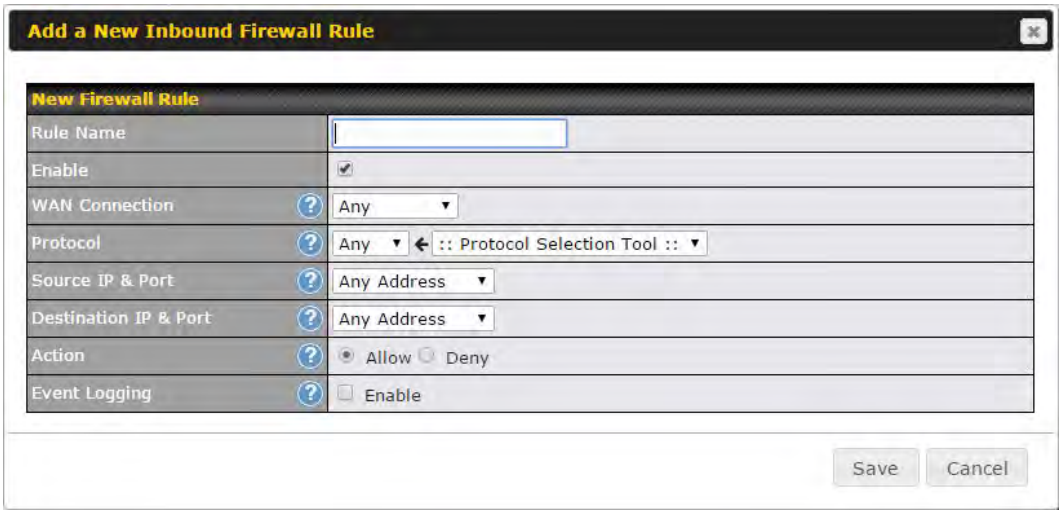
 Copyright @ 2017 Pepwave



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

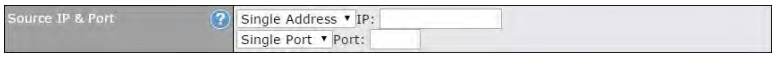
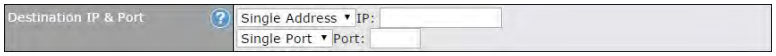


Click **Add Rule** to display the following screen:



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



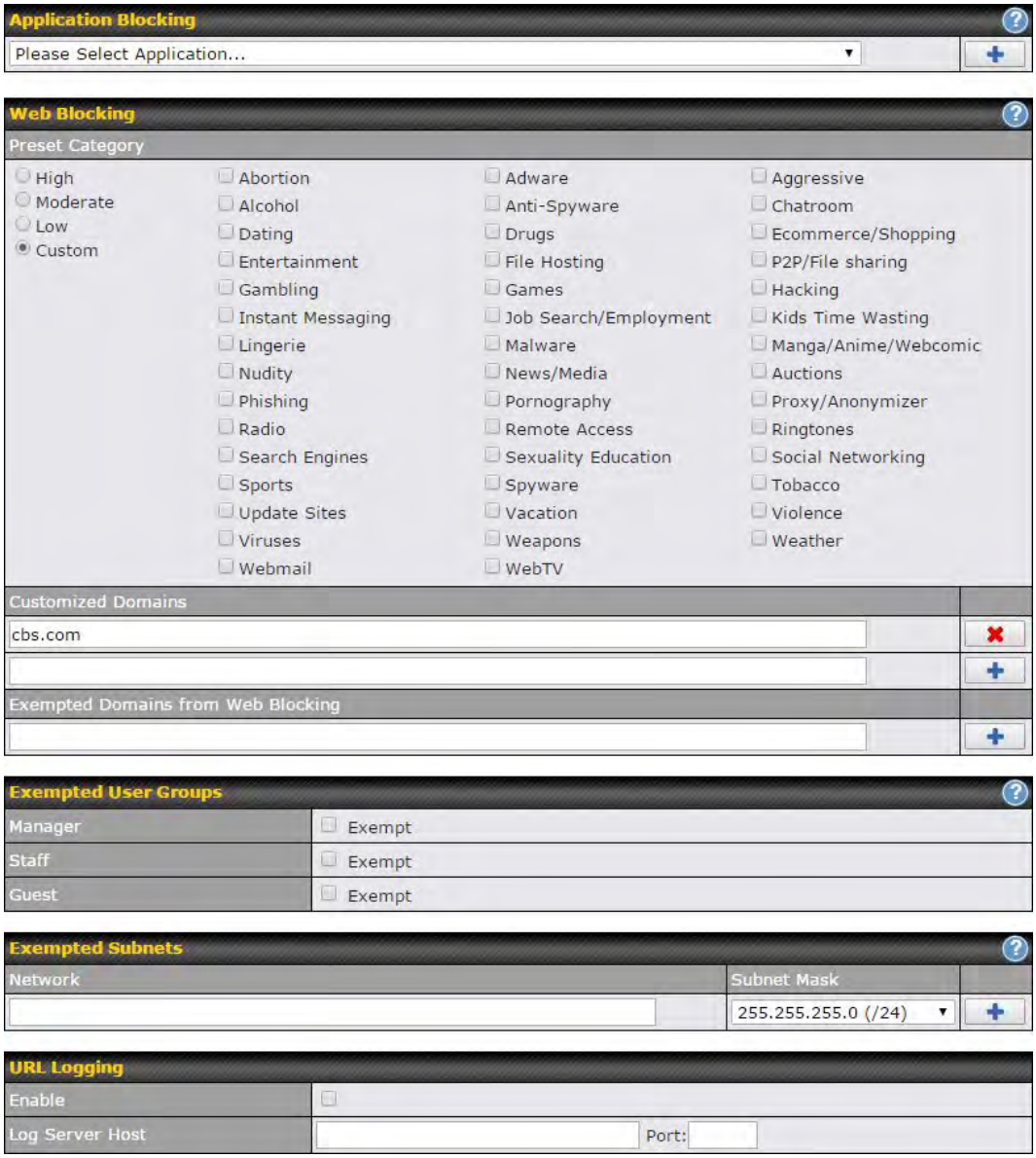
Pepwave routers can detect and prevent intrusions and denial-of-service (DoS) attacks from the Internet. To turn on this feature, click , check the **Enable** check box, and press the **Save** button.

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

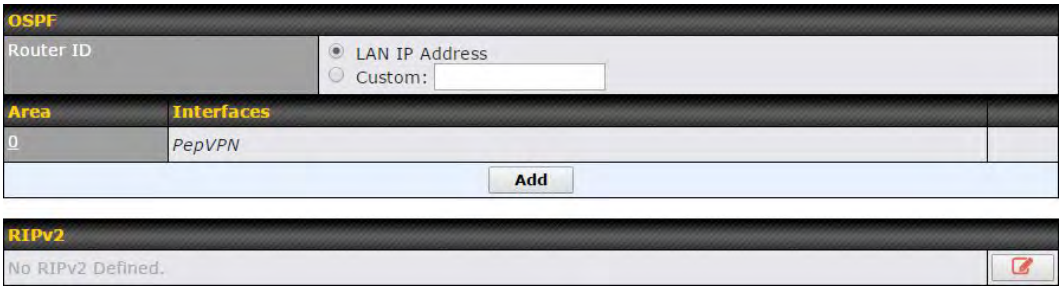
With the subnet defined in the field, clients on the particular subnet(s) can be exempted from the access blocking rules.

14.2.4 URL Logging

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

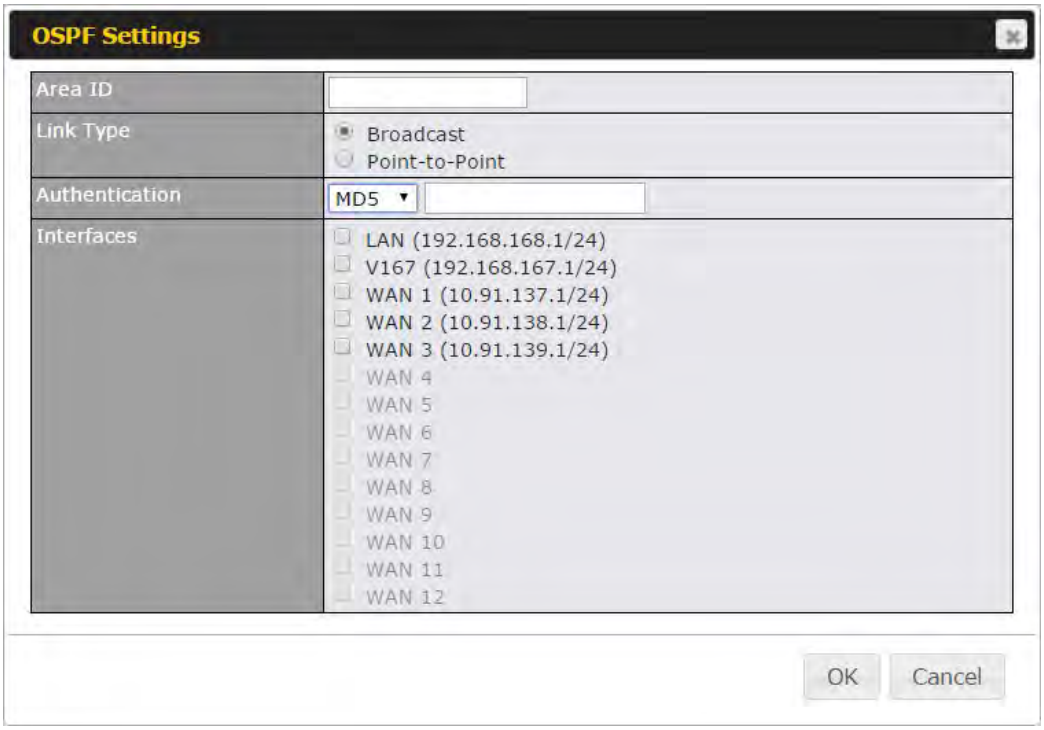
15 OSPF & RIPv2

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

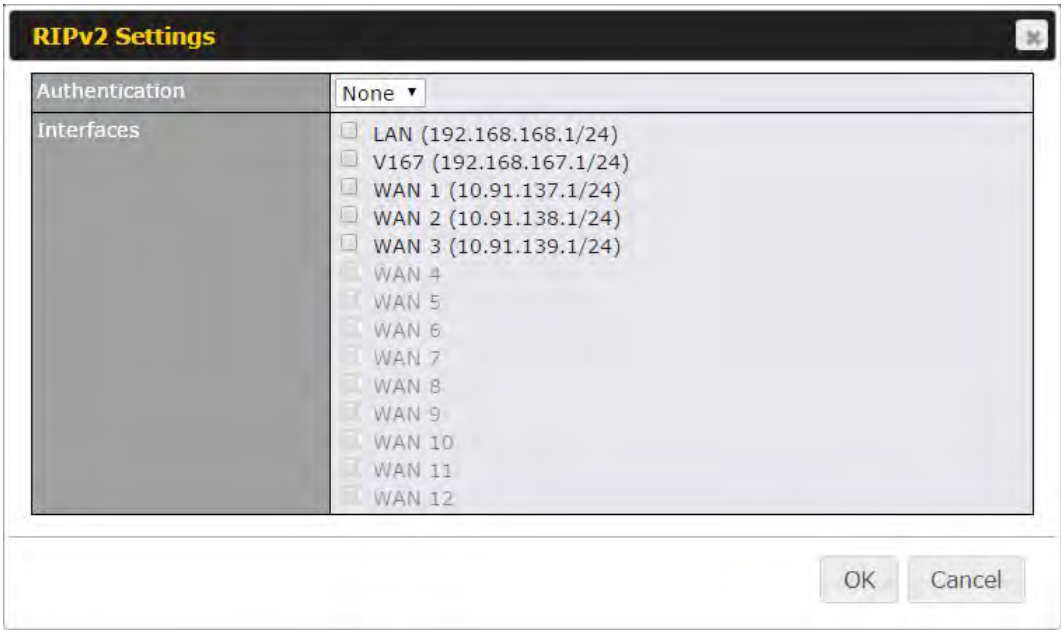
OSPF	
Router ID	This field determines the ID of the router. By default, this is specified as the LAN IP address. If you want to specify your own ID, enter it in the **Custom** field.
Area	This is an overview of the OSPFv2 areas you have defined. Click on the area name to configure it. To set a new area,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



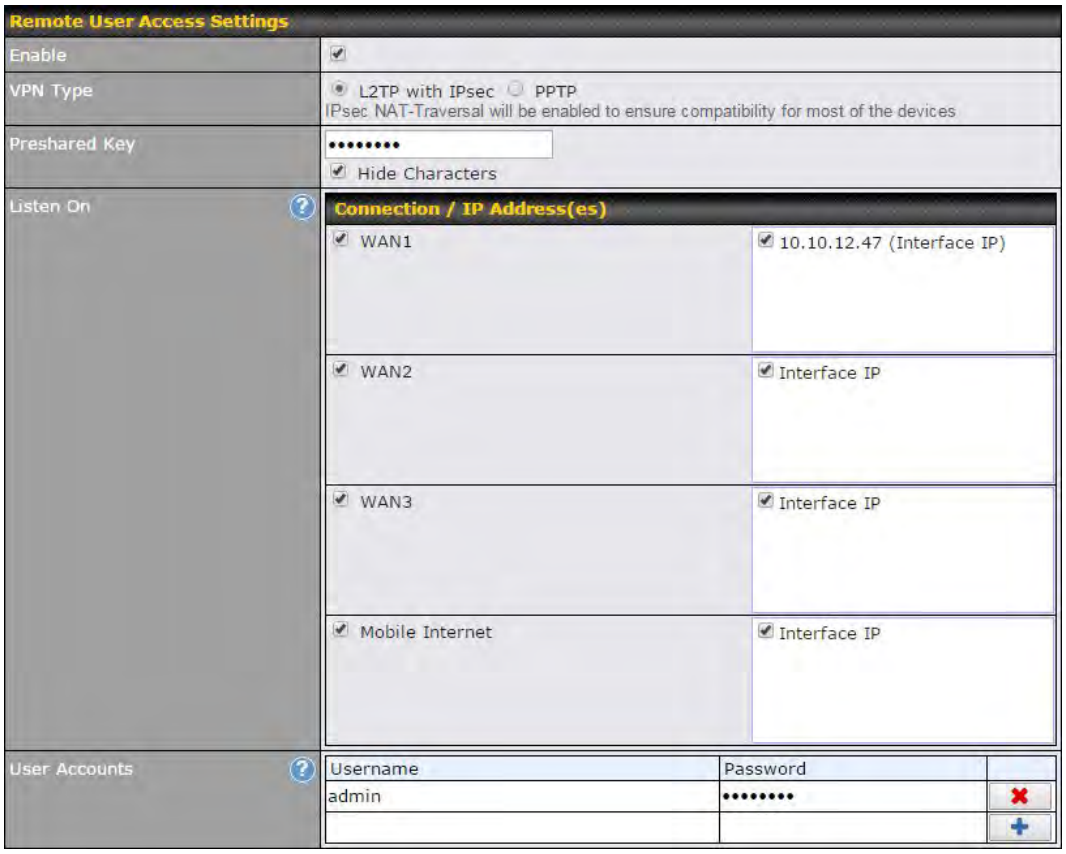
RIPv2 Settings	
Authentication	Choose an authentication method, if one is used, from this drop-down menu. Available options are **MD5** and **Text**. Enter the authentication key next to the drop-down menu.
Interfaces	Determine which interfaces this group will use to listen to and deliver RIPv2 packets.

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.

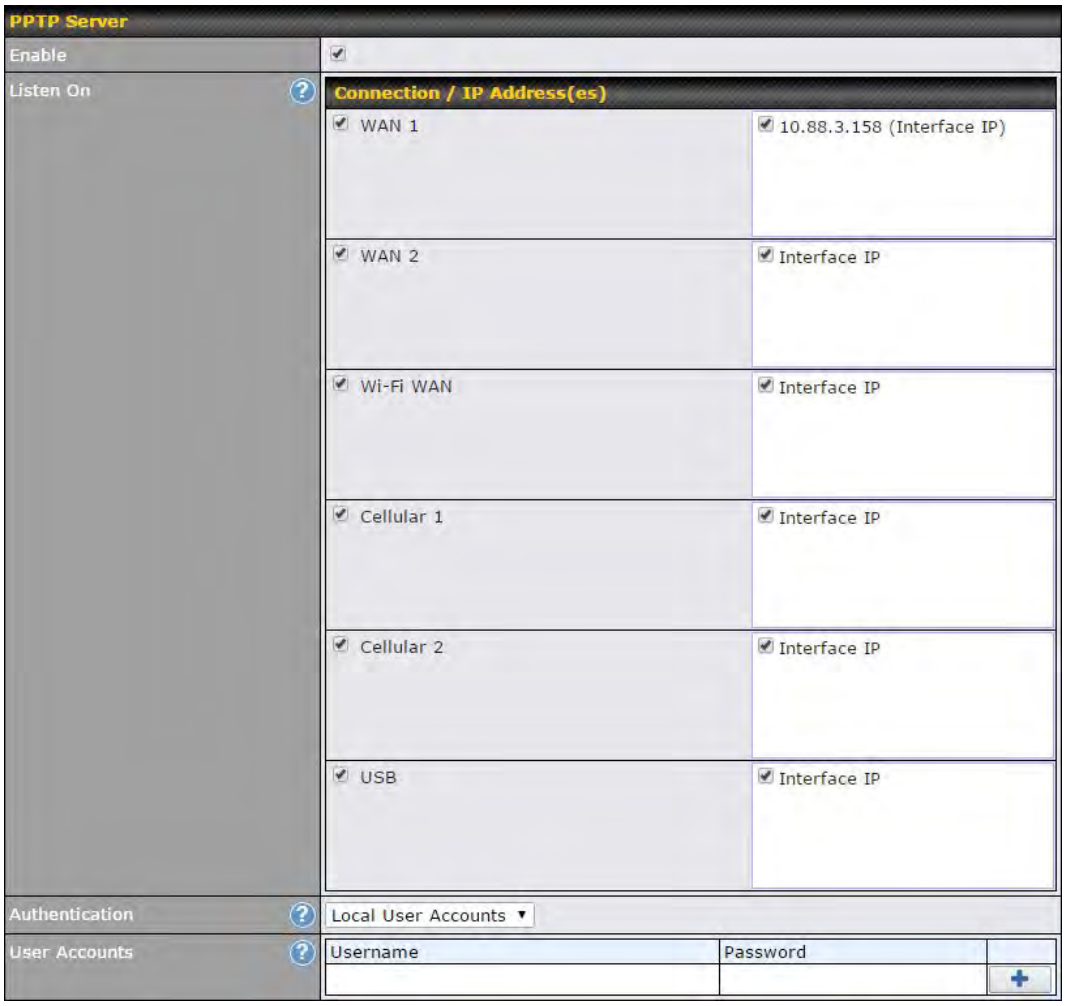
16.2 PPTP Server



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.

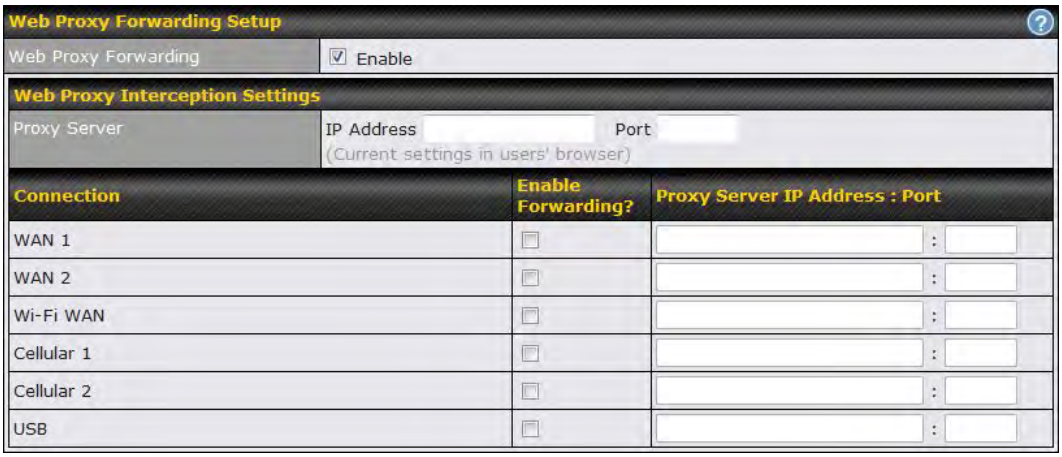
The Pepwave router will intercept SMTP connections. Choose a WAN port according to the outbound policy, and then forward the connection to the SMTP server if the chosen WAN has enabled forwarding. If the forwarding is disabled for a WAN connection, SMTP connections for the WAN will be simply be forwarded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



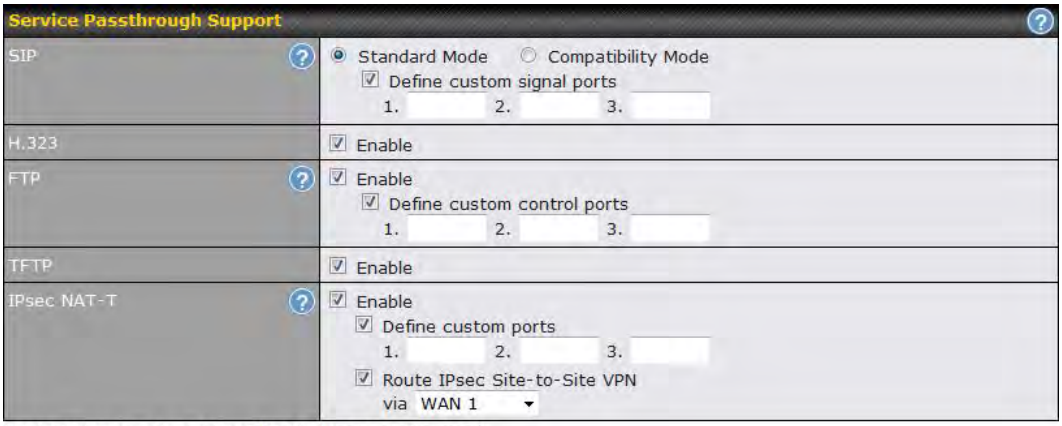
After clicking the **enable** checkbox, enter your TCP port for traffic heading to the router, and then

 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**.



(Registered trademarks are copyrighted by their respective owner)

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.**

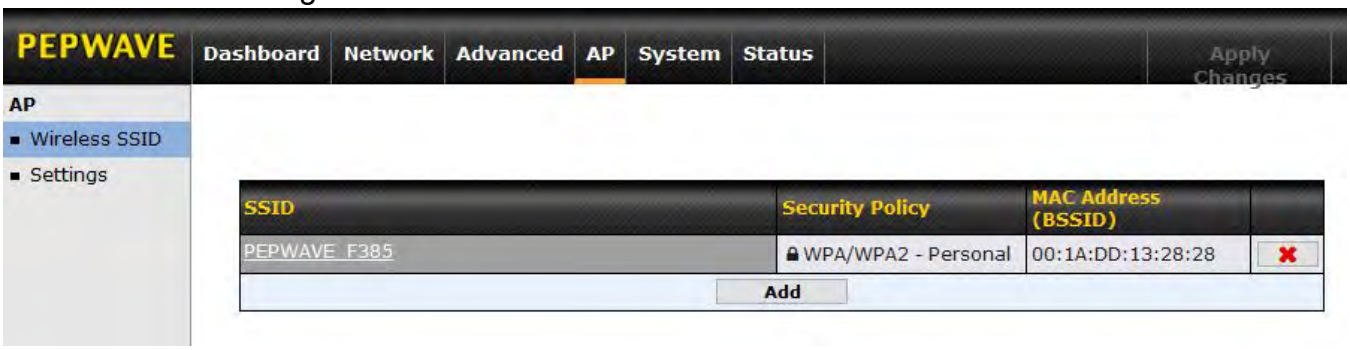


17 AP

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

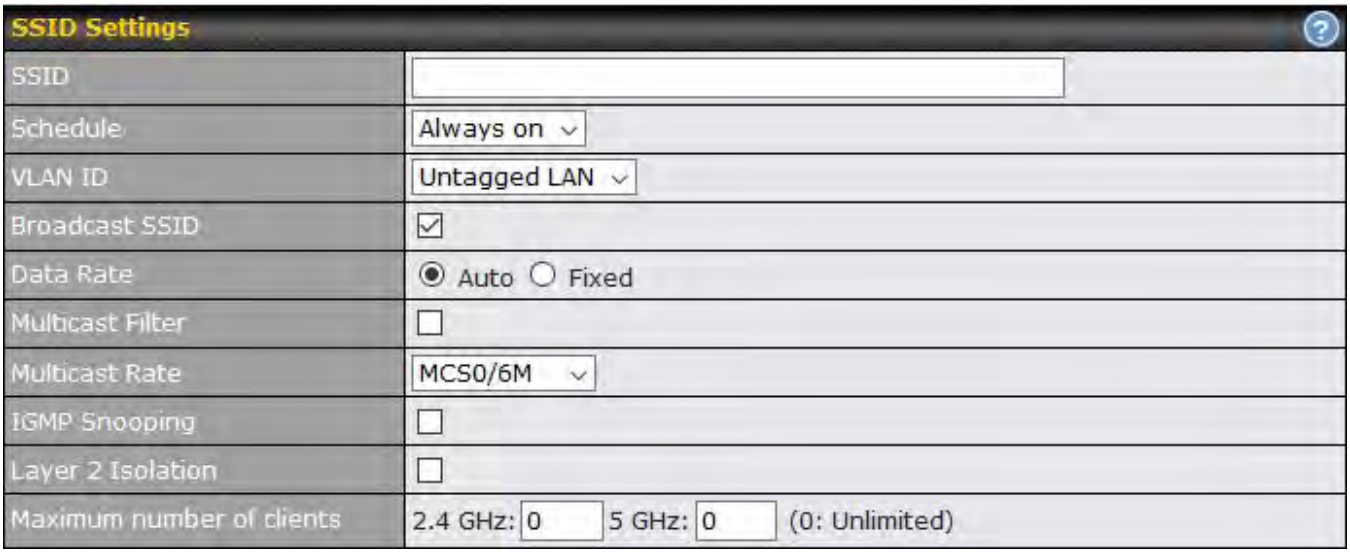
17.1 Wireless SSID

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.

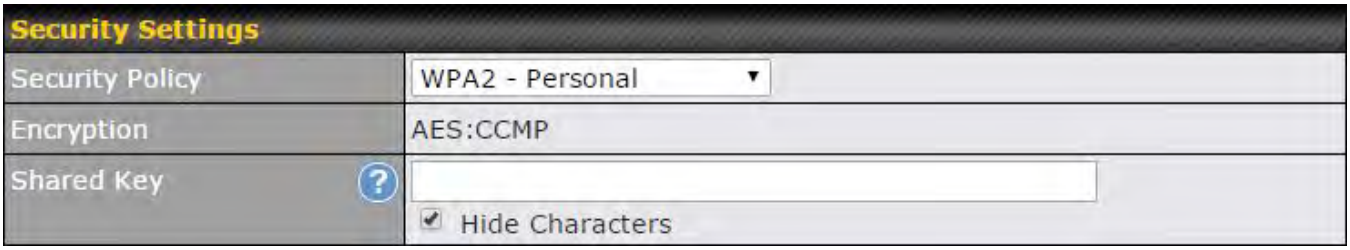
 Copyright @ 2017 Pepwave



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.



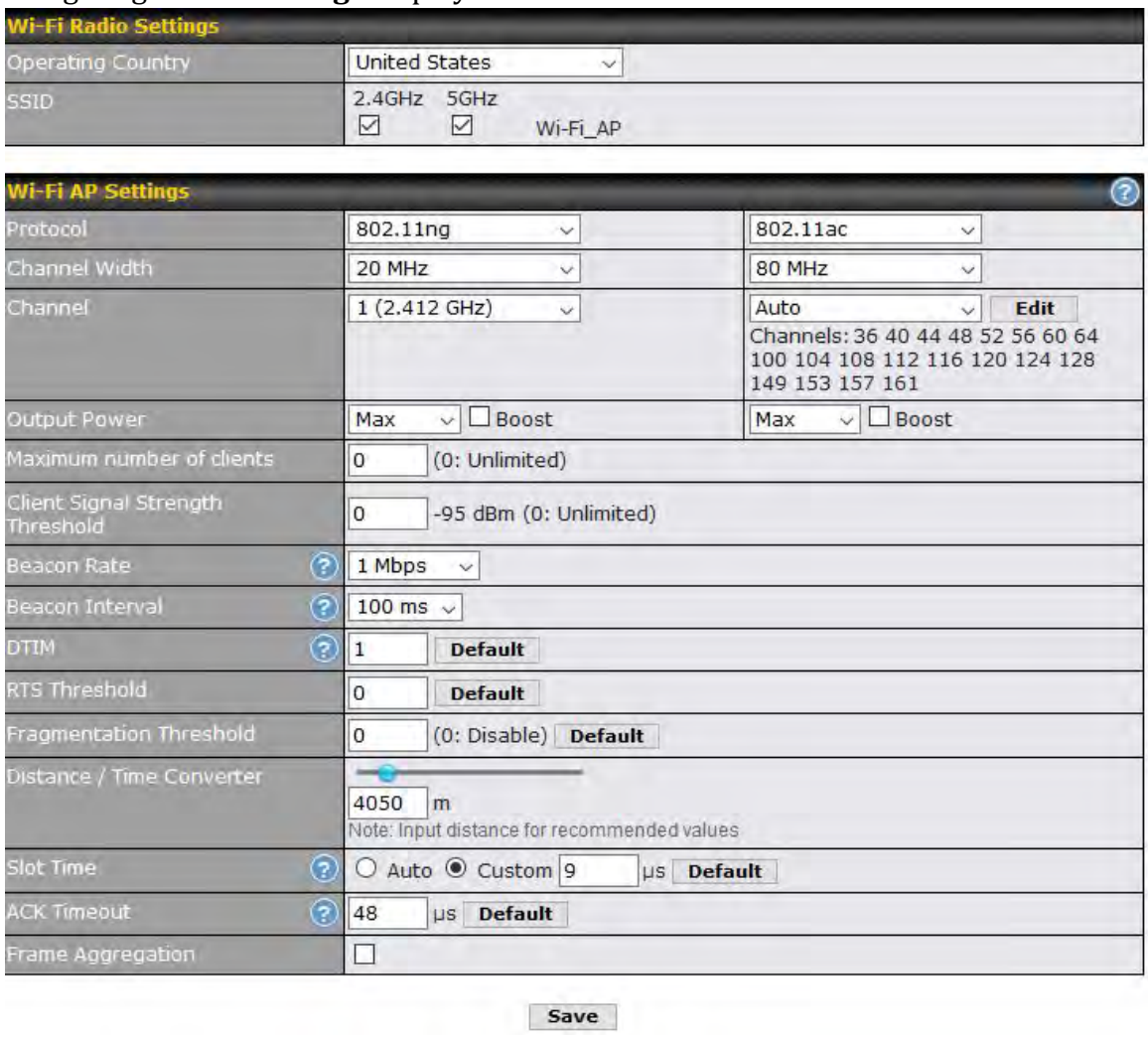
Access Control	
Restricted Mode	The settings allow administrator to control access using Mac address filtering. Available options are None, Deny all except listed, Accept all except listed, and RADIUS MAC Authentication. When WPA/WPA2 - Enterprise is configured, RADIUS-based 802.1 x authentication is 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.

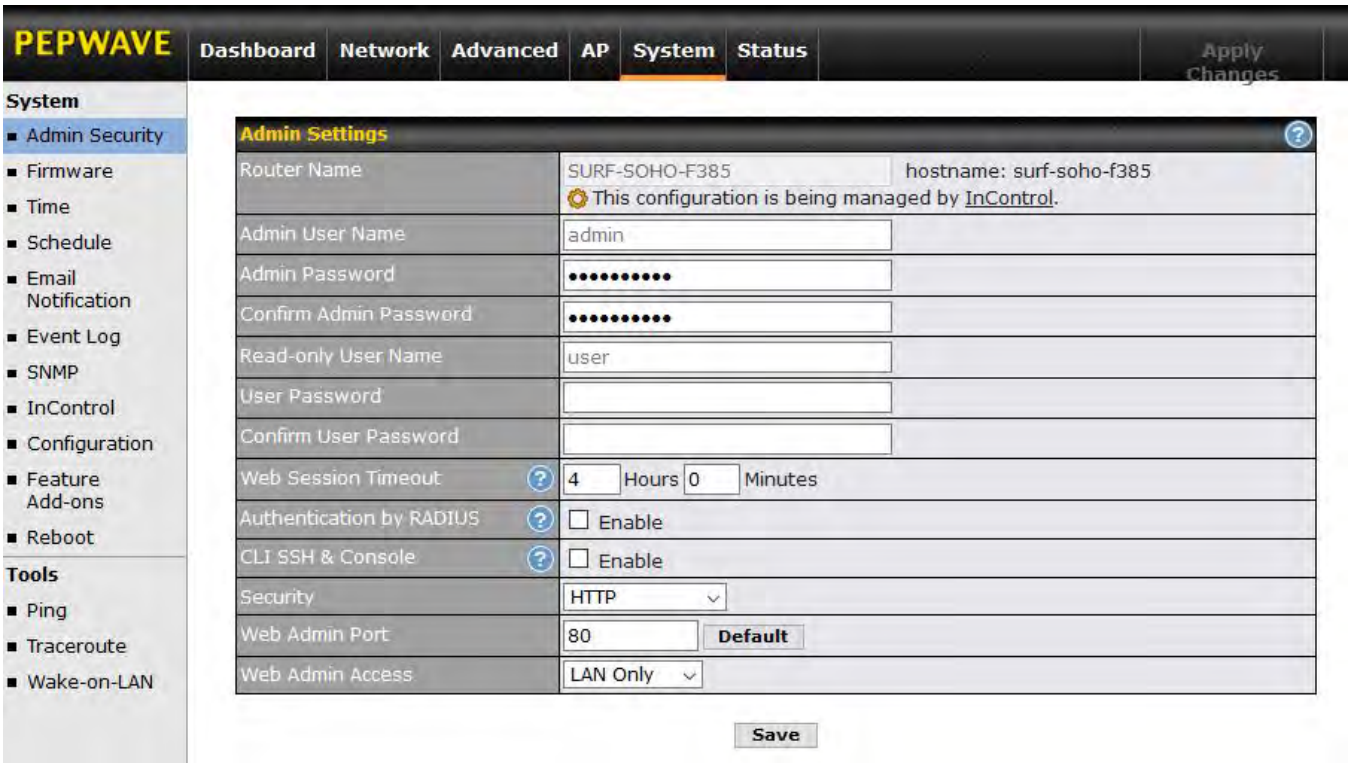
 Copyright @ 2017 Pepwave

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.

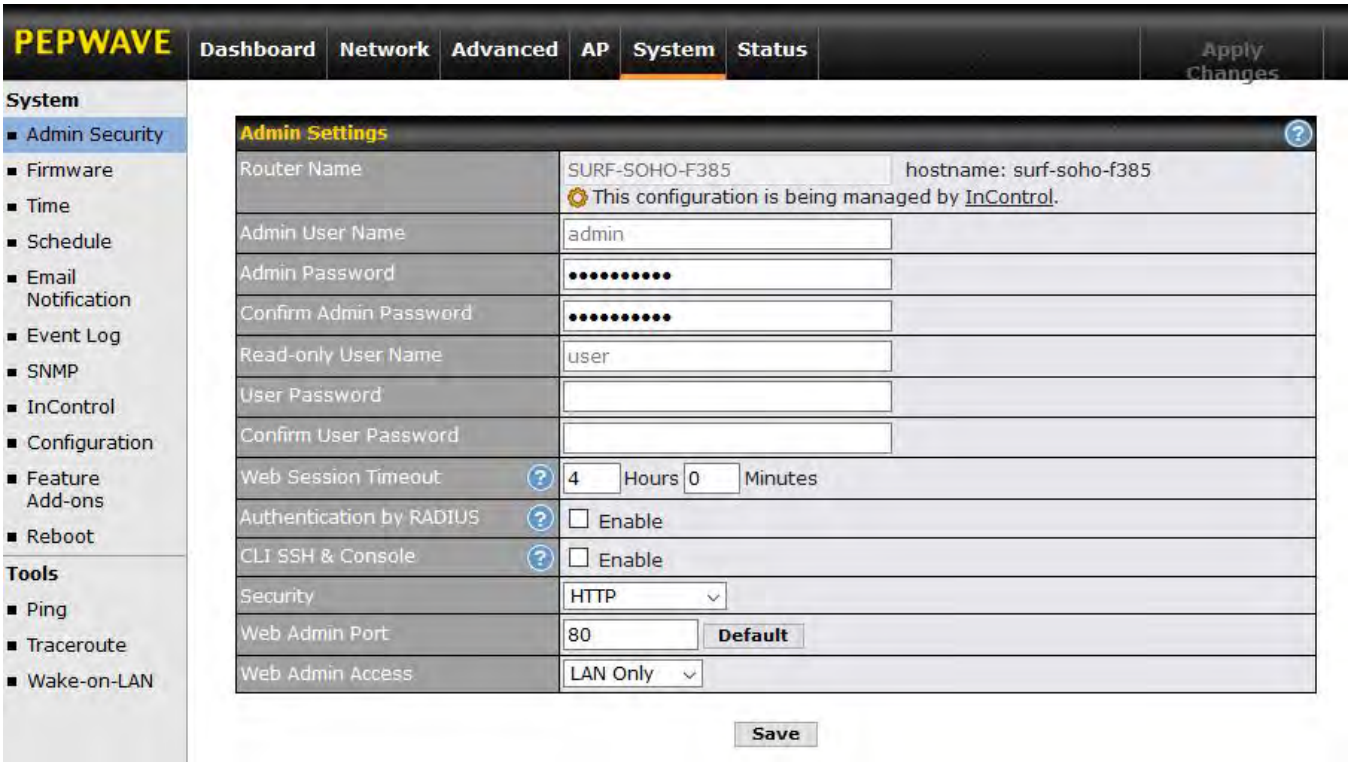
 Copyright @ 2017 Pepwave



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

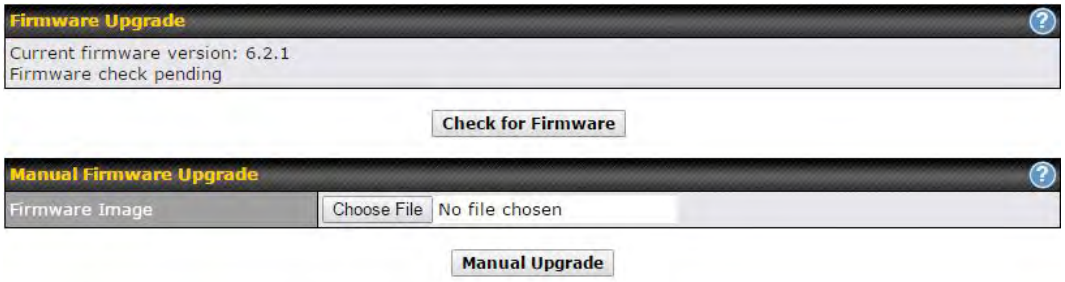
Confirm User Password	This field allows you to verify and confirm the new user password
Web Session Timeout	This field specifies the number of hours and minutes that a web session can remain idle before the Router terminates its access to the web admin interface. By default, it is set to **4 hours.**
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

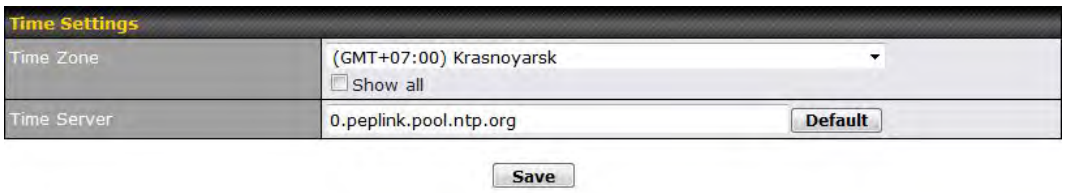
The firmware upgrade process may not necessarily preserve the previous configuration, and the behavior varies on a case-by-case basis. Consult the release notes for the particular firmware version before installing. Do not disconnect the power during firmware upgrade process. Do not attempt to upload 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

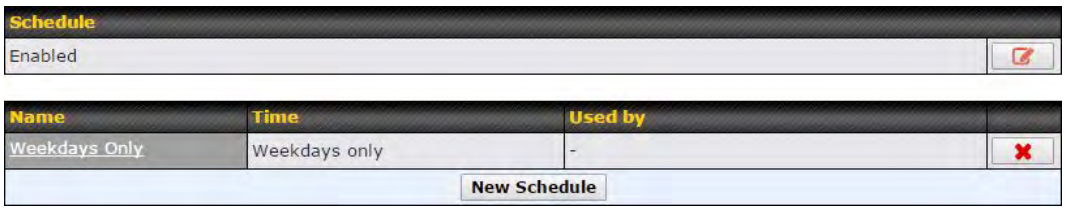
Time Settings enables the system clock of the Pepwave router to be synchronized with a specified time server. Time settings are located at **System>Time**.



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.

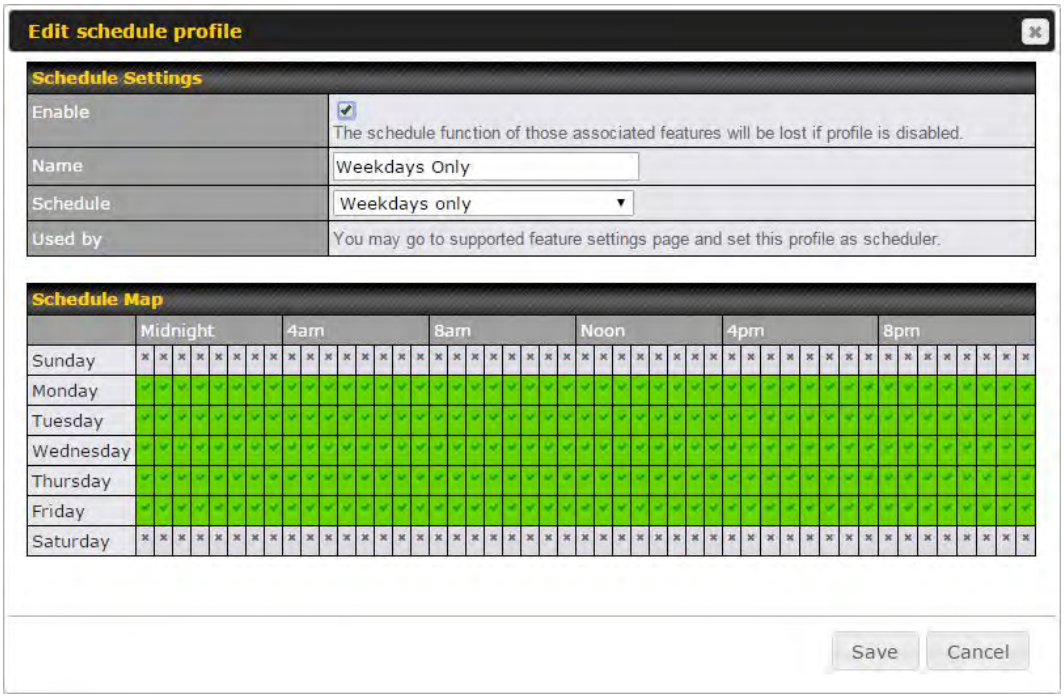
18.4 Schedule

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

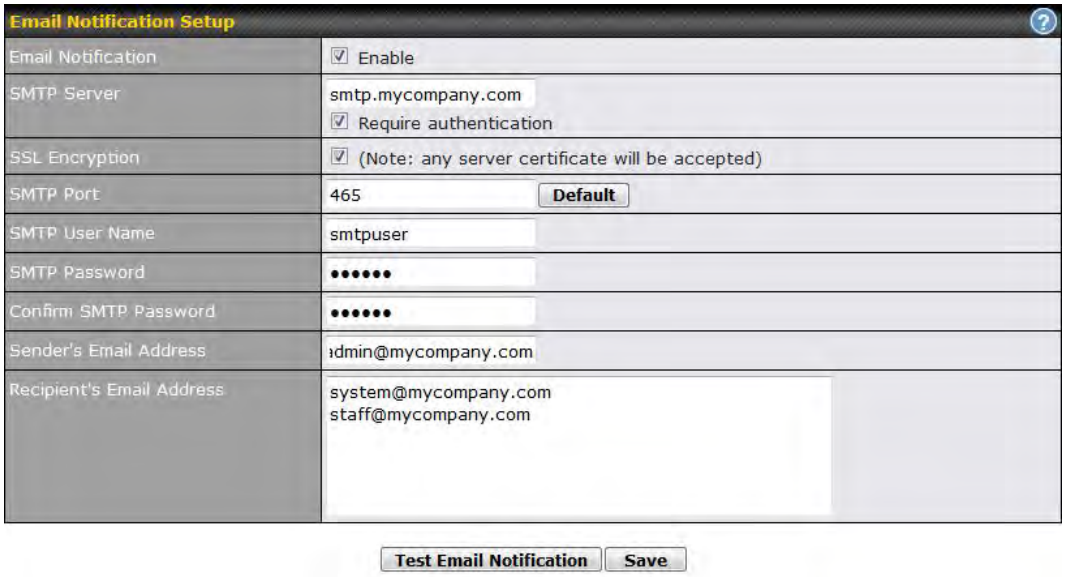


Edit Schedule Profile	
Enabling	Click this checkbox to enable this schedule profile. Note that if this is disabled, then any associated features will also have their scheduling disabled.
Name	Enter your desired name for this particular schedule profile.
Schedule	Click the drop-down menu to choose pre-defined 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

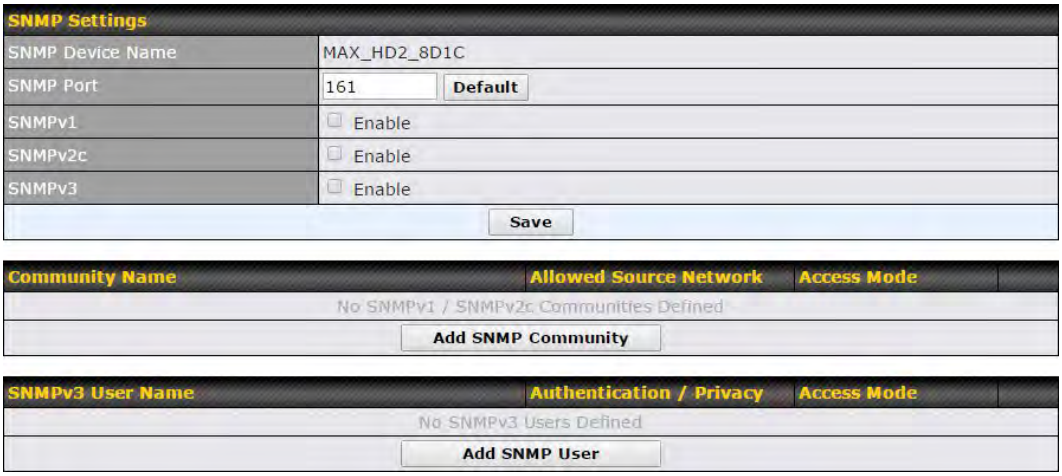


Event Log Settings	
Remote Syslog	This setting specifies whether or not to log events at the specified remote syslog server.
Remote Syslog Host	This setting specifies the IP address or hostname of the remote syslog server.
Push Events	The Pepwave router can also send push notifications to mobile devices 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.

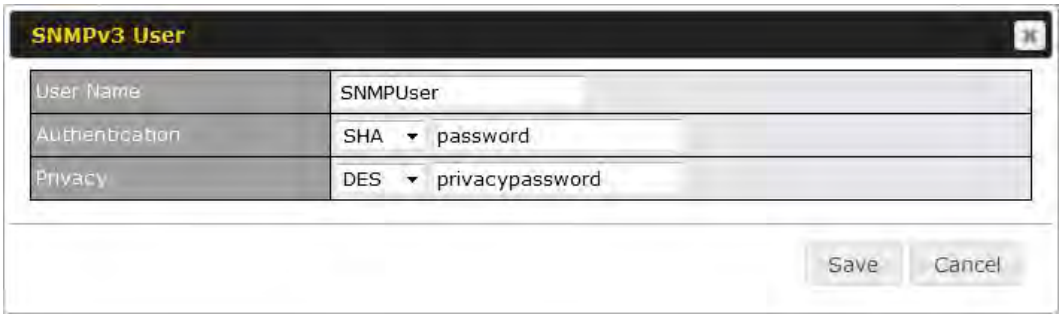
To add a community for either SNMPv1 or SNMPv2, click the **Add SNMP Community** button in the **Community Name** table, upon which the following screen is displayed:



 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.

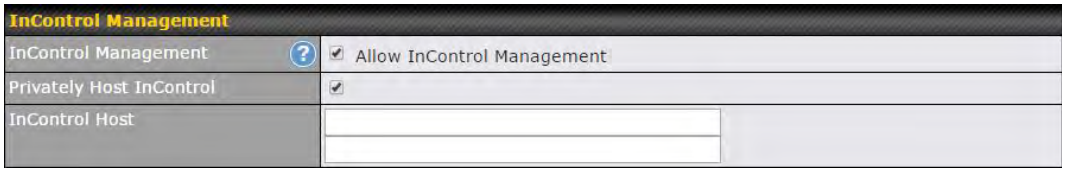
To define a username for SNMPv3, click **Add SNMP User** in the **SNMPv3 User Name** table, upon which the following screen is displayed:

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.

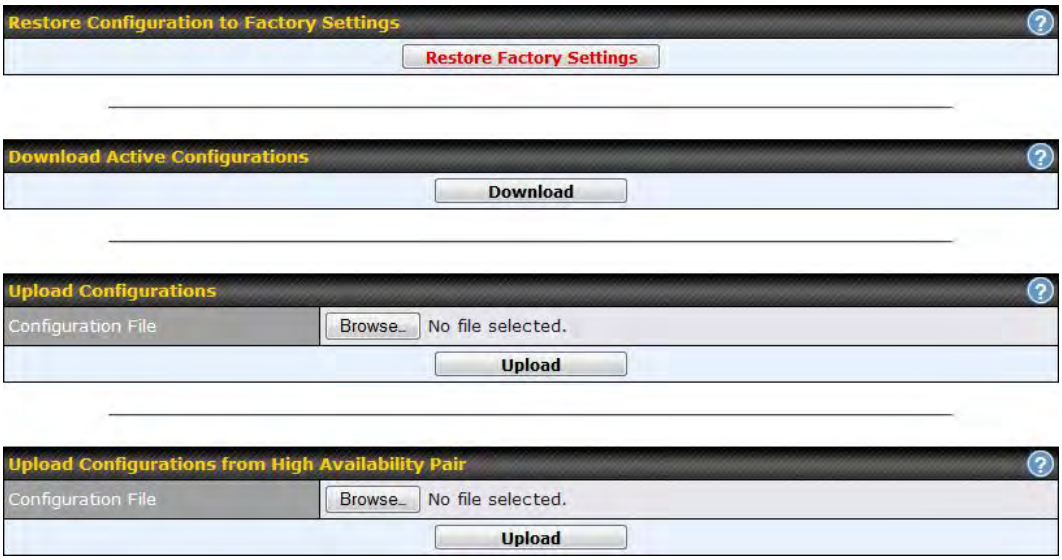
Alternately, you could also privately host InControl. Simply check the box beside the "Privately Host InControl" open, and enter the IP Address of your InControl Host.

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

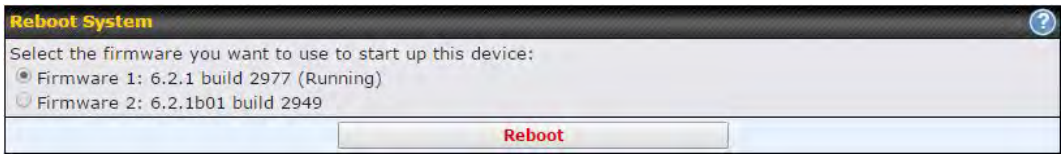
and then click **Apply Changes**.



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.

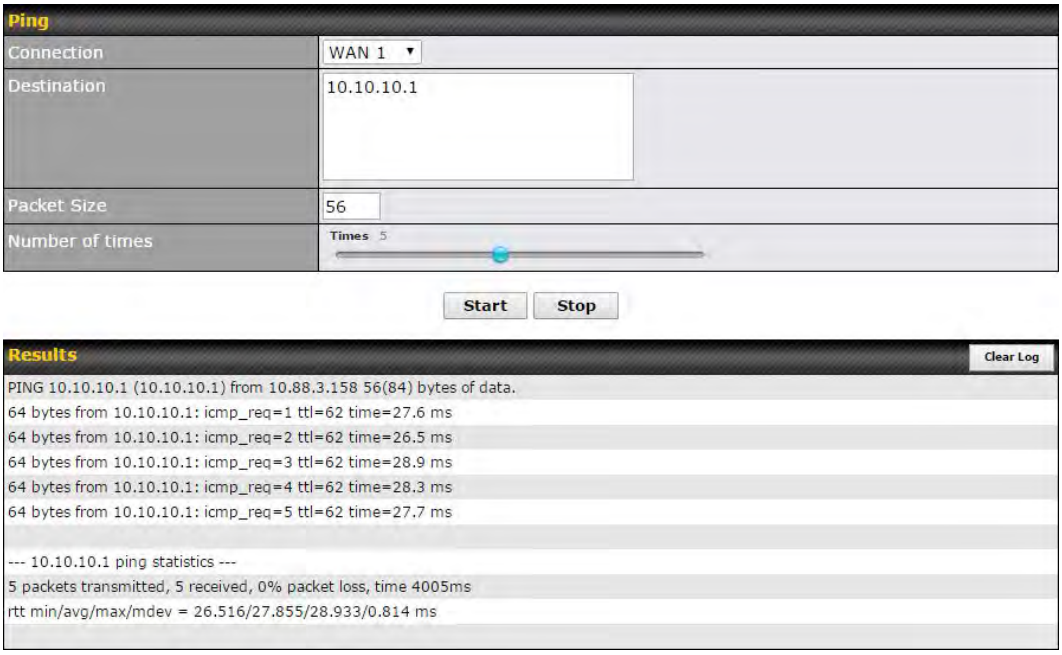


19 Tools

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



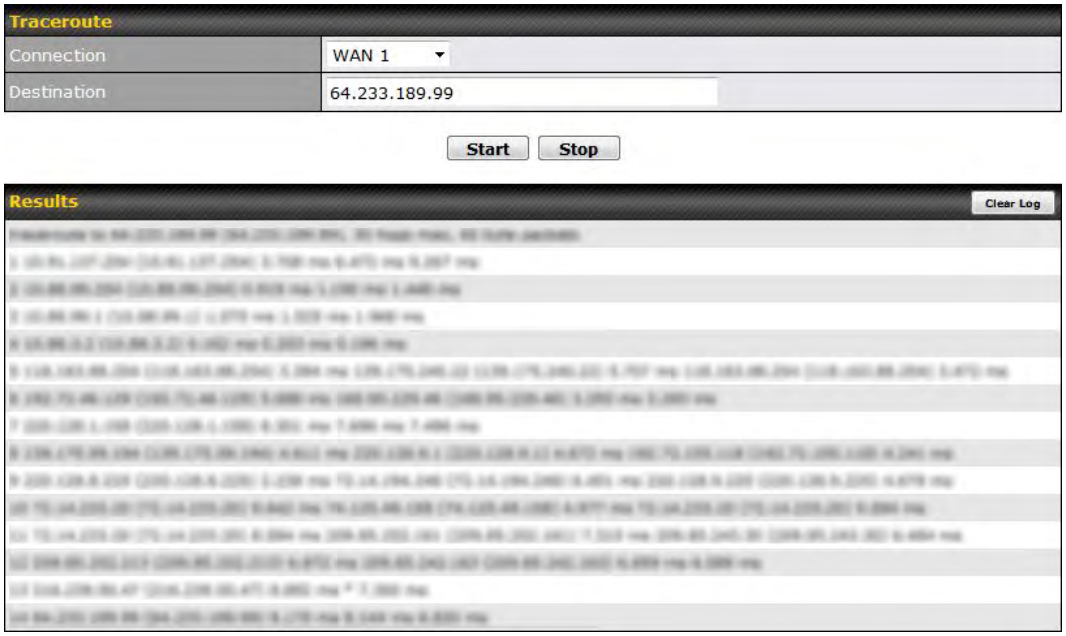
Tip

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

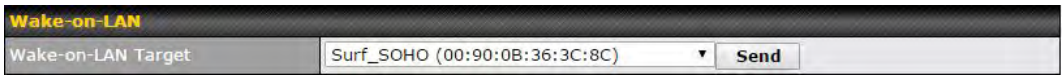


Tip

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 .

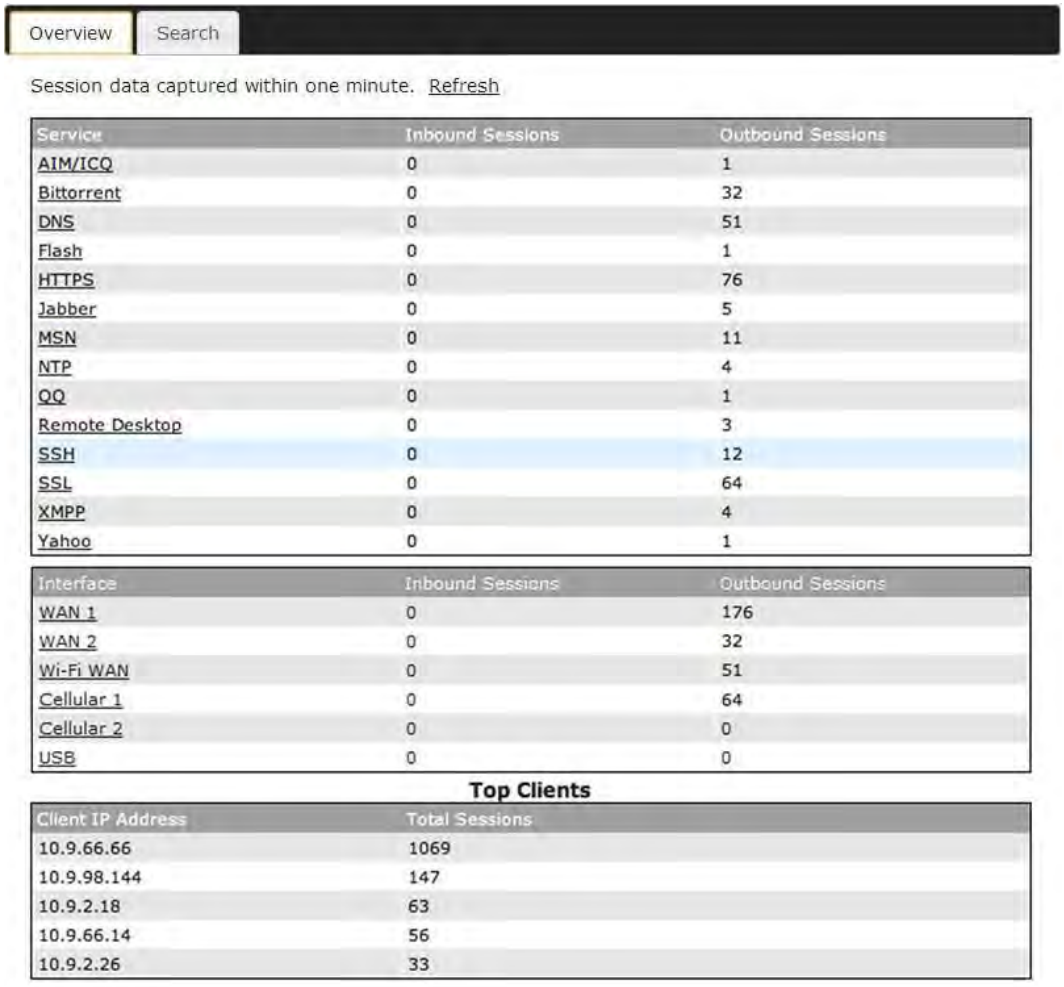
Important Note

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

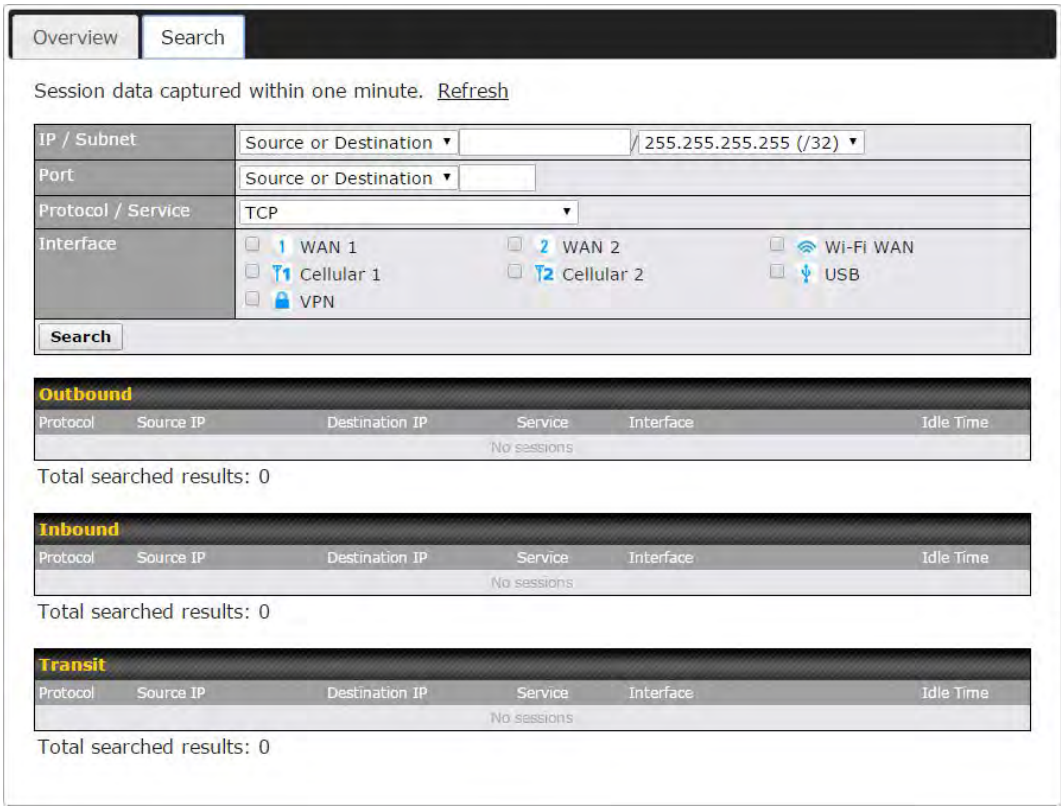
Top Clients

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**.

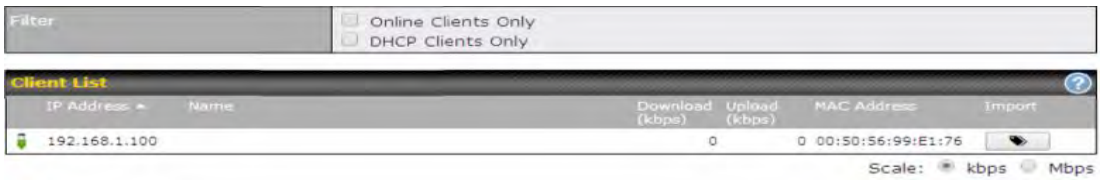
 Copyright @ 2017 Pepwave



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

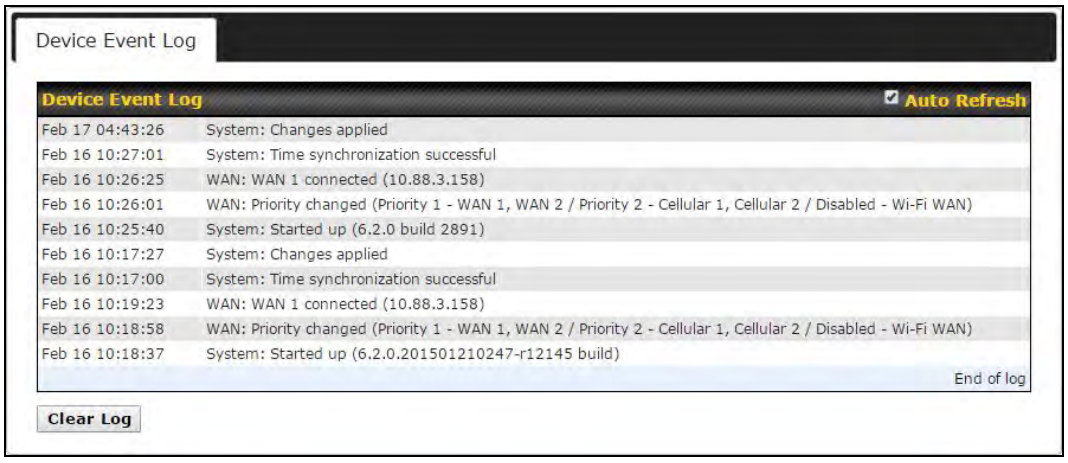
The client list table is located at **Status>Client List**. It lists DHCP and online client IP addresses**,** names (retrieved from the DHCP reservation table or defined by users), current download and upload rate, and MAC address. Clients can be imported into the DHCP reservation table by clicking the 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.

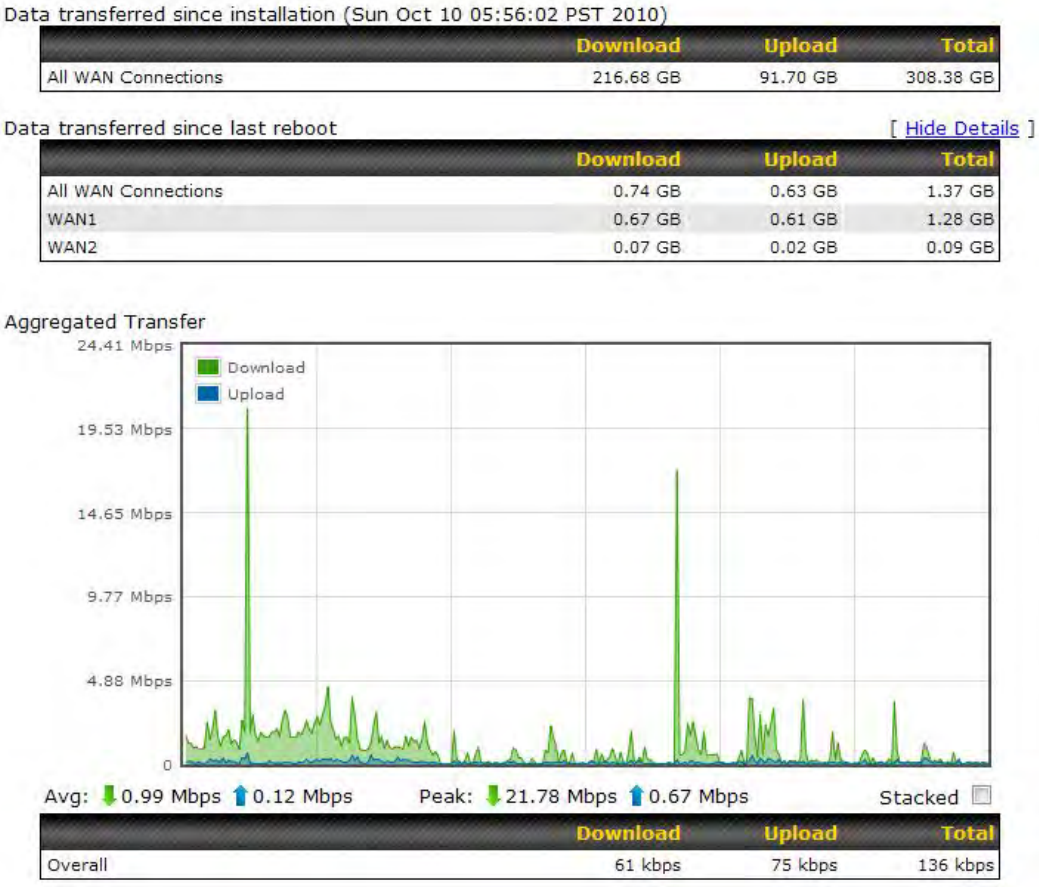
20.5 Bandwidth

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.

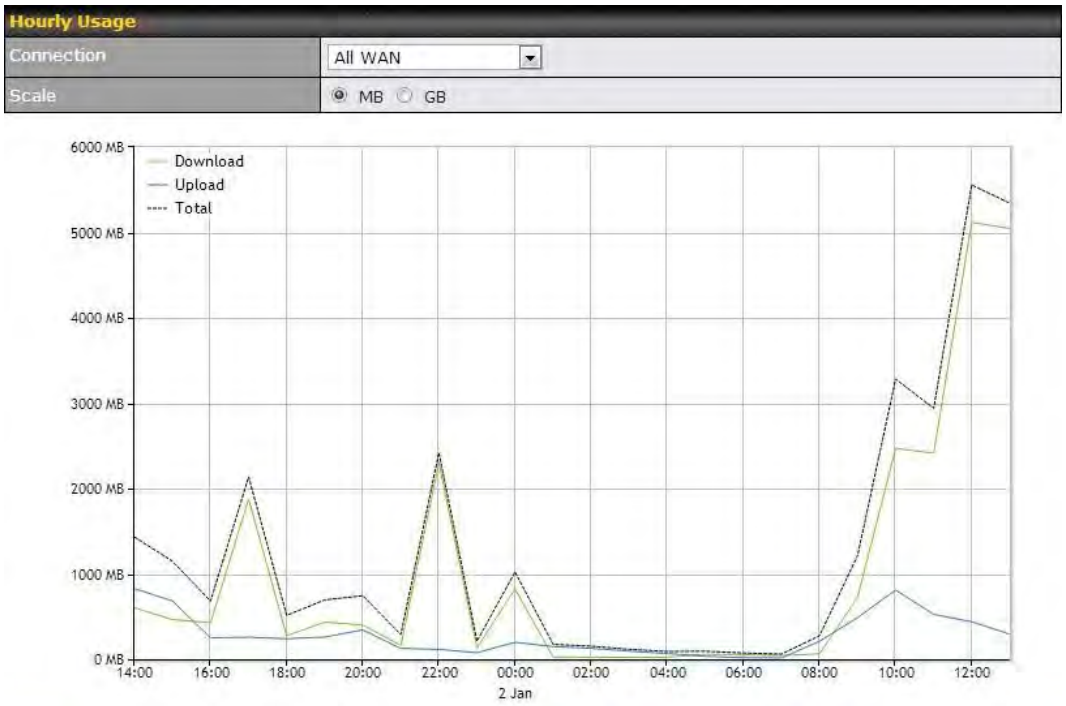
 Copyright @ 2017 Pepwave



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

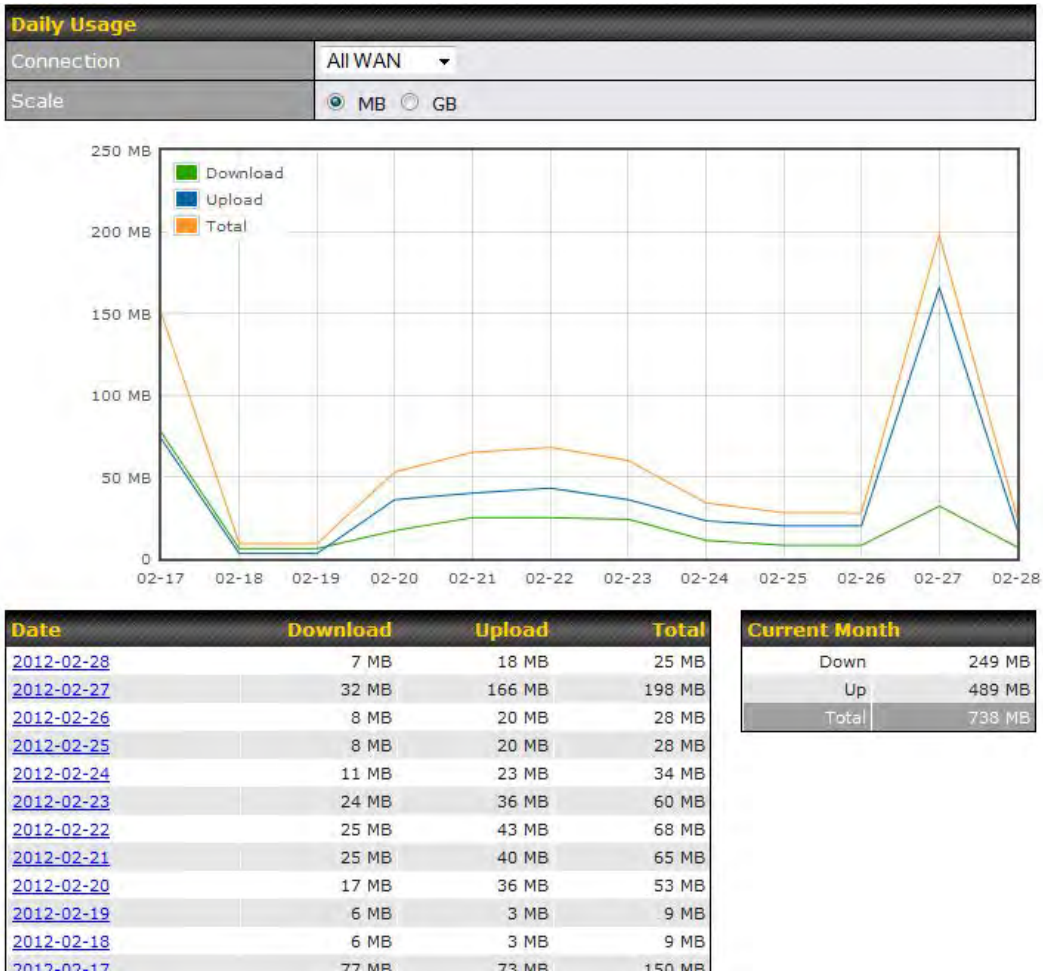
20.5.3 Daily

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

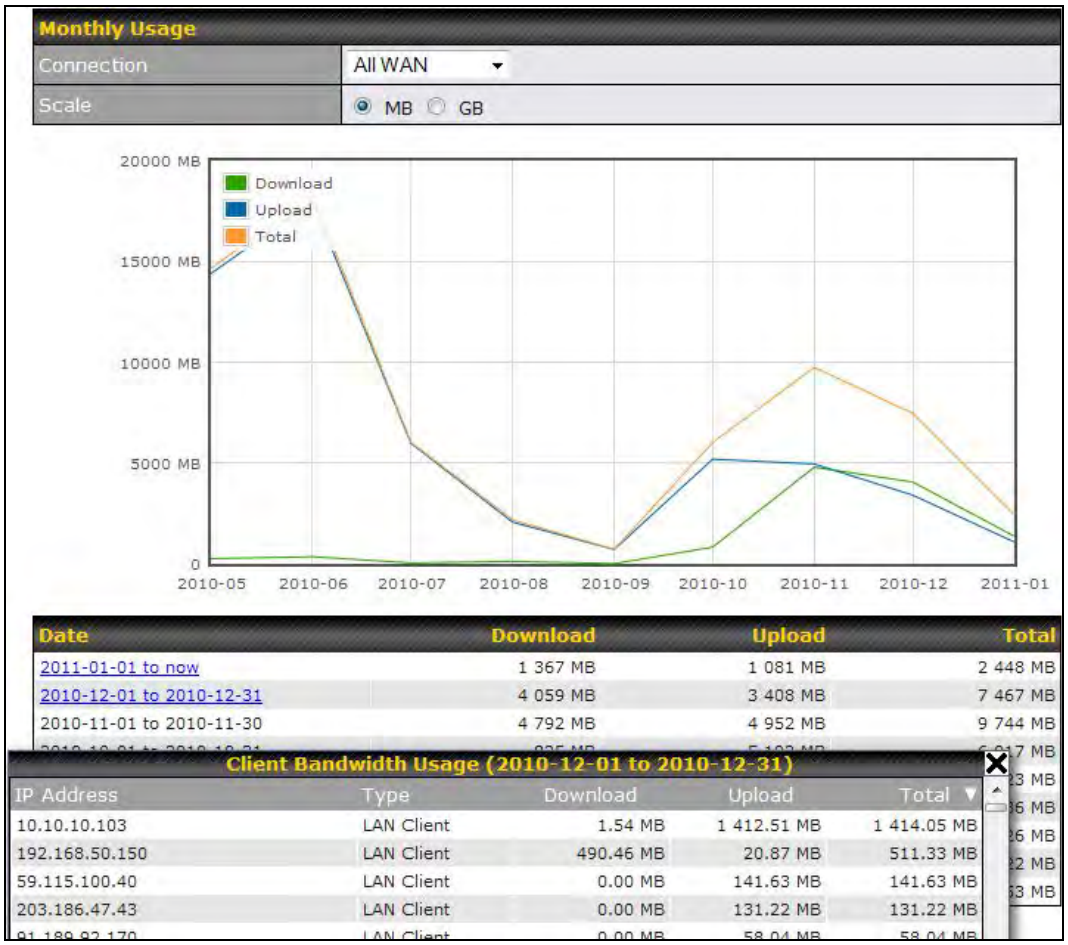
Current Month	
Down	249 MB
Up	489 MB
Total	738 MB

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 Česky [Czech]	*[Jméno výrobce]* tímto prohlašuje, že tento *[typ zařízení]* je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
da Dansk [Danish]	Undertegnede *[fabrikantens navn]* erklærer herved, at følgende udstyr *[udstyrets typebetegnelse]* overholder de væsentlige krav og øvrige

 Copyright @ 2017 Pepwave

	relevante krav i direktiv 1999/5/EF.
de Deutsch [German]	Hiermit erklärt *[Name des Herstellers]*, dass sich das Gerät *[Gerätetyp]* in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
et Eesti [Estonian]	Käesolevaga kinnitab *[tootja nimi = name of manufacturer]* seadme *[seadme tüüp = type of equipment]* vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
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 Español [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 Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *[name of manufacturer]* ΔΗΛΩΝΕΙ ΟΤΙ *[type of equipment]* ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
fr Français [French]	Par la présente *[nom du fabricant]* déclare 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]* è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
lv Latviski [Latvian]	Ar šo *[name of manufacturer / izgatavotāja nosaukums]* deklarē, ka *[type of equipment / iekārtas tips]* atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
lt Lietuvių [Lithuanian]	Šiuo *[manufacturer name]* deklaruoja, kad šis *[equipment type]* atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
nl	Hierbij verklaart *[naam van de fabrikant]* dat het toestel *[type van toestel]* in

 Copyright @ 2017 Pepwave

Nederlands [Dutch]	overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
mt Malti [Maltese]	Hawnhekk, *[isem tal-manifattur]*, jiddikjara li dan *[il-mudel tal-prodott]* jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
hu Magyar [Hungarian]	Alulírott, *[gyártó neve]* nyilatkozom, hogy a *[... típus]*megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
pl Polski [Polish]	Niniejszym *[nazwa producenta]* oświadcza, że *[nazwa wyrobu]* jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
pt Português [Portuguese]	*[Nome do fabricante]* declara que este *[tipo de equipamento]* está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
sl Slovensko [Slovenian]	*[Ime proizvajalca]* izjavlja, da je ta *[tip opreme]* v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
sk Slovensky [Slovak]	*[Meno výrobcu]* týmto vyhlasuje, že *[typ zariadenia]*spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
fi Suomi [Finnish]	*[Valmistaja = manufacturer]* vakuuttaa täten että *[type of equipment = laitteen tyyppimerkintä]* tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
sv Svenska [Swedish]	Härmed intygar *[företag]* att denna *[utrustningstyp]* står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

 Copyright @ 2017 Pepwave

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 WCDE-4-4X2MP-PTZ-4X150LTL-LED-2TB-AP-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.