

# PEPWAVE

Broadband Possibilities

## User Manual

### **Pepwave AP One Series:**

AP One AC Mini (HW1) / AP One Enterprise (HW 1-2) / AP One Flex (HW2-3) /  
AP One Rugged (HW1) / AP Pro AC (HW1)

**Pepwave AP Firmware 3.6.3**

**June 2025**

# Table of Contents

<b>Introduction and Scope</b>	<b>4</b>
<b>Product Features and Benefits</b>	<b>5</b>
<b>Package Contents</b>	<b>6</b>
AP One Enterprise (APO-ENT)	6
AP One AC mini (APO-AC-MINI)	6
AP One Rugged (APO-RUG)	6
AP One Flex (APO-FLX)	6
<b>Hardware Overview</b>	<b>7</b>
AP One Enterprise	7
AP One AC mini	8
AP One Rugged	9
AP One Flex	10
AP Pro AC	12
<b>Installation</b>	<b>13</b>
Installation Procedures	13
<b>Dashboard</b>	<b>15</b>
General	15
AP	16
<b>Network</b>	<b>18</b>
WAN	18
LAN	20
Interfaces	23
Ethernet Port	23
PepVPN	23
<b>AP</b>	<b>26</b>
Wireless SSID	26

Settings	38
Mesh	41
WDS	42
<b>System Tab</b>	<b>43</b>
Admin Security	43
Firmware	44
Time	45
Event Log	46
SNMP	47
Controller	49
Configuration	50
Feature Add-Ons	51
Operating Mode	51
Reboot	52
Tools	52
PING	52
Traceroute	53
Nslookup	53
<b>Status Tab</b>	<b>54</b>
Device	54
Client List	55
Mesh / WDS Info	55
Portal	56
Rogue AP	56
Event Log	57
<b>Restoring Factory Defaults</b>	<b>58</b>
<b>Appendix</b>	<b>58</b>

# 1 Introduction and Scope

Our AP Series of enterprise-grade 802.11ac/a/b/g/n Wi-Fi access points is engineered to provide fast, dependable, and flexible operation in a variety of environments, all controlled by an easy-to-use centralized management system.

From the small but powerful AP One AC mini to the top-of-the-line AP Pro Duo our AP Series offers wireless networking solutions to suit any business need, and every access point is loaded with essential features such as multiple SSIDs, VLAN, Mesh, WDS, and Guest Protect.

A single access point provides as many as 32 virtual access points (16 on single-radio models), each with its own security policy (WPA, WPA2, etc.) and authentication mechanism (802.1x, open, captive portal, etc.), allowing faster, easier, and more cost-effective network builds.

Each member of the AP Series family also features a high-powered Wi-Fi transmitter that greatly enhances coverage and performance while reducing equipment costs and maintenance.

## 2 Product Features and Benefits

Key features and benefits of AP Series access points:

- High-powered Wi-Fi transmitter enhances coverage and lowers cost of ownership.
- Independent security policies and encryption mechanisms for each virtual access point allow fast, flexible, cost-effective network builds.
- Centralized management via InControl reduces maintenance expense and time.
- Mesh support allows for wireless expansion and enhancement of Wi-Fi coverage.
- WDS support allows secure and fast network expansion.
- Guest Protect support guards sensitive business data and subnetworks.
- WMM (Wi-Fi Multimedia) and QoS (Quality of Service) support keeps video and other bandwidth-intensive data flowing fast and lag-free.
- Air Monitor mode support for troubleshoot remotely and proactively monitor Wi-Fi and WAN performance.

## 3 Package Contents

### **AP One Enterprise (APO-ENT)**

1x AP One Enterprise  
1 x Mounting Bracket

### **AP One AC mini (APO-AC-MINI)**

1 x AP One mini  
1 x 12V2A Power supply  
1 x Mounting Bracket

### **AP One Rugged (APO-RUG)**

1 x AP One Rugged  
1 x 12V2A Power supply  
3 x 5dBi Omni Antenna

### **AP One Flex (APO-FLX)**

1 x AP One Flex  
1 x Cable Tie  
\* Power supply or Pepwave Passive PoE Injector are not included

### **AP Pro AC (APP-AGN3)**

1 x AP Pro AC  
1 x Waterproof Power Connector Kit  
2 x Waterproof Ethernet Kit

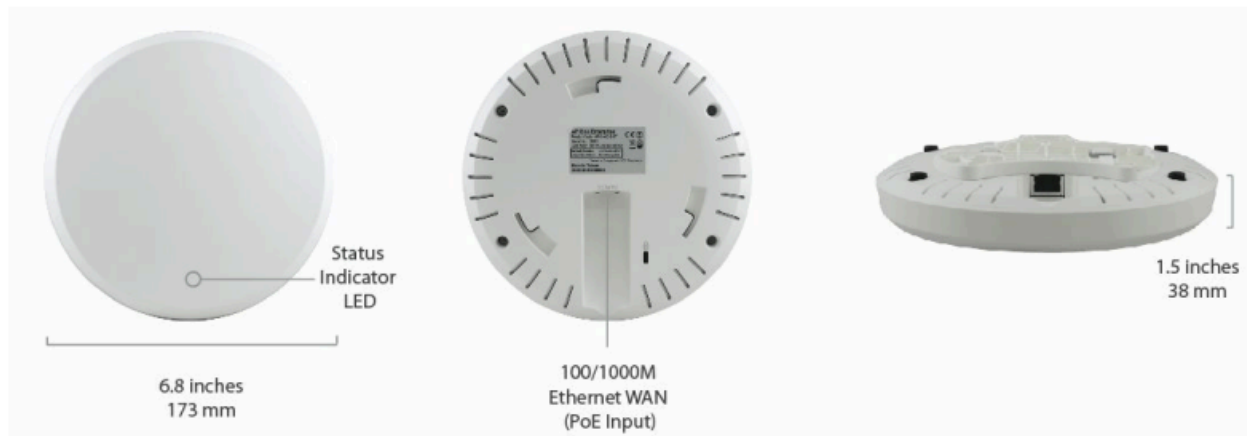
## 4 Hardware Overview

### 4.1 AP One Enterprise

**Bottom View**

**Top View**

**Front View**

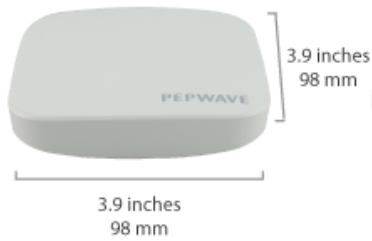


#### LED Indicators

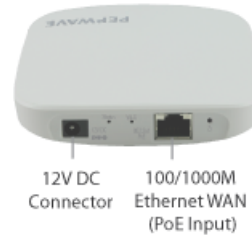
<b>Status</b>	RED – Access point initializing
	GREEN – Access point ready
<b>LAN</b>	OFF – No device connected to Ethernet port
	BLINKING – Ethernet port sending/receiving data
	ON – Powered-on device connected to Ethernet port
	Note that LAN 5 displays the status of the uplink connection

## 4.2 AP One AC mini

Front View



Rear Panel View

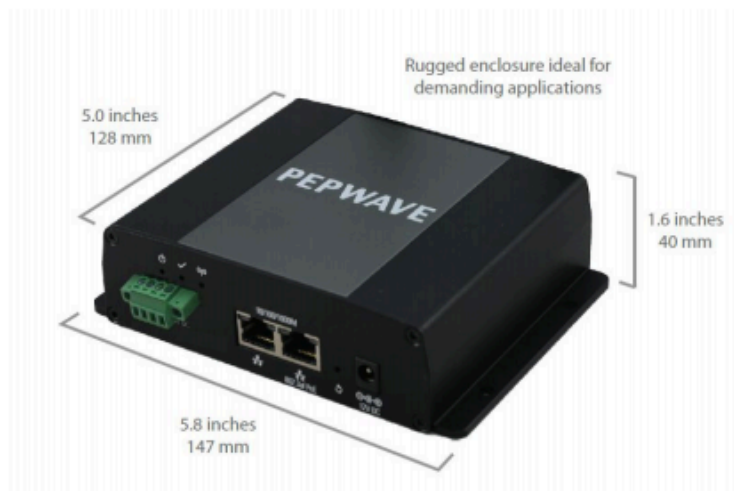


LED Indicators	
<b>Status</b>	RED – Access point initializing
	GREEN – Access point ready
<b>Wi-Fi</b>	OFF – 2.4/5GHz Wi-Fi radio off
	BLINKING – AP sending/receiving data
	GREEN – 2.4/5GHz Wi-Fi radio on
	Note that this model includes a 2.4GHz Wi-Fi radio and a 5GHz Wi-Fi radio that can operate simultaneously to increase speed and reduce interference.

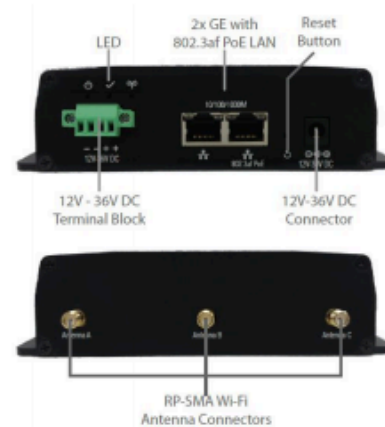


## 4.3 AP One Rugged

### Front View



### Rear Panel View

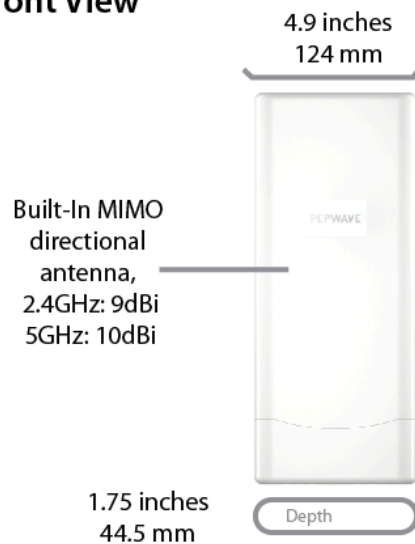


### LED Indicators

<b>Power</b>	On – Power On
	OFF – Power Off
<b>Status</b>	RED – Access point initializing
	GREEN – Access point ready
<b>Wi-Fi</b>	OFF – 2.4/5GHz Wi-Fi radio off
	BLINKING – AP sending/receiving data
	GREEN – 2.4/5GHz Wi-Fi radio on
	Note that this model includes a 2.4GHz Wi-Fi radio and a 5GHz Wi-Fi radio that can operate simultaneously to increase speed and reduce interference.

## 4.4 AP One Flex

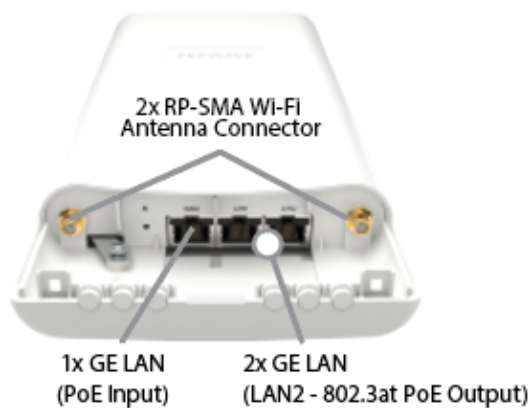
**Front View**



**Rear Panel View**



**Connector Panel (Inside the Lid)**

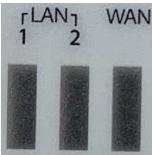
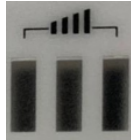


**Accessory – Wall/Pole Mount with Ball Joint for IP55 Outdoor Products ^**

Flexible ball joint allows for high-precision installation



^ Available separately.

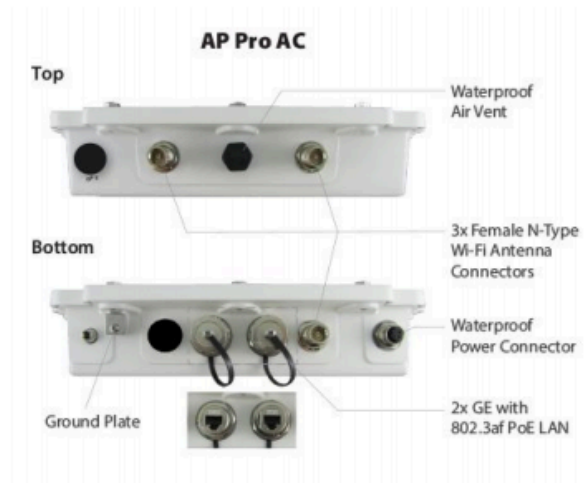
LED Indicators		
Status	RED	Access point initializing
	Blinking Red	Boot up or error
	GREEN	Access point ready
LAN	Green LED	ON – Powered-on device connected to Ethernet port or 1000Mbps OFF – 10Mbps / 100Mbps or No device connected to Ethernet port
	Orange LED	ON – Port is connected without traffic BLINKING – Ethernet port sending/receiving data OFF – No data is being transferred or No device connected to Ethernet port
	Port Type	Auto MDI/MDI-X ports
WAN	Green LED	ON – Powered-on device connected to Ethernet port or 1000Mbps OFF – 10Mbps / 100Mbps or No device connected to Ethernet port
	Orange LED	ON – Port is connected without traffic BLINKING – Ethernet port sending/receiving data OFF – No data is being transferred or No device connected to Ethernet port
	Port Type	Auto MDI/MDI-X ports
		Green LED ON – Powered-on device connected to Ethernet port OFF – No device connected to Ethernet port
		Number of connected clients – SignalBar1: WiFi AP client count > 0 SignalBar2: WiFi AP client count > 10 SignalBar3: WiFi AP client count > 20

## 4.5 AP Pro AC

**Front View**

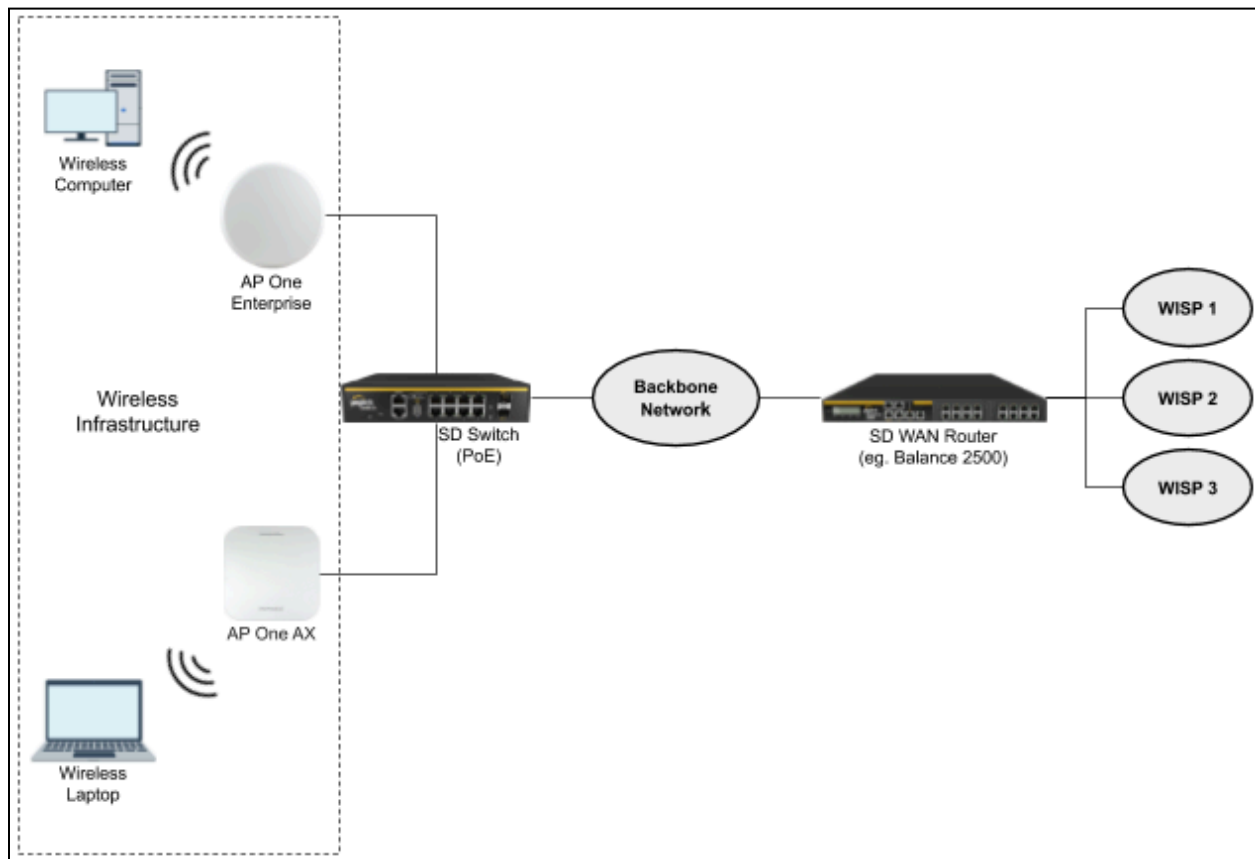


**Top/Bottom View**



## 5 Installation

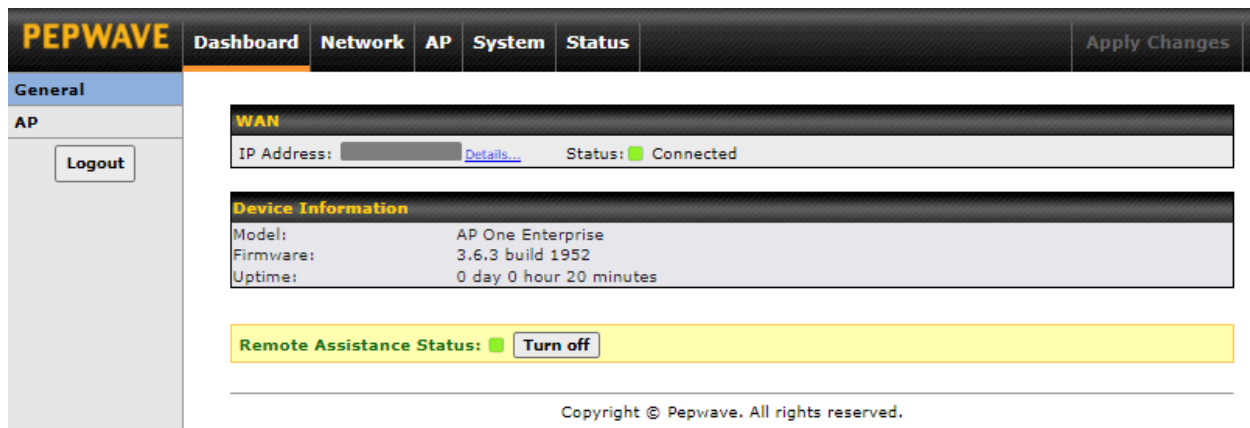
Your access point acts as a bridge between wireless and wired Ethernet interfaces.  
A typical setup follows:



### Installation Procedures

1. Connect the Ethernet port on the unit to the backbone network using an Ethernet cable. The port should auto sense whether the cable is straight-through or crossover.
2. There are two methods to power on the device as below:
  - 2.1 For those Pepwave AP devices having built-in PoE ports only, using an Ethernet cable to connect to the Power over Ethernet (PoE) switch or PoE injector.
  - 2.2 For those Pepwave AP devices that have a DC power source, plug the AC adapter to the DC connector of the unit.
3. Wait for the status LED to turn green.

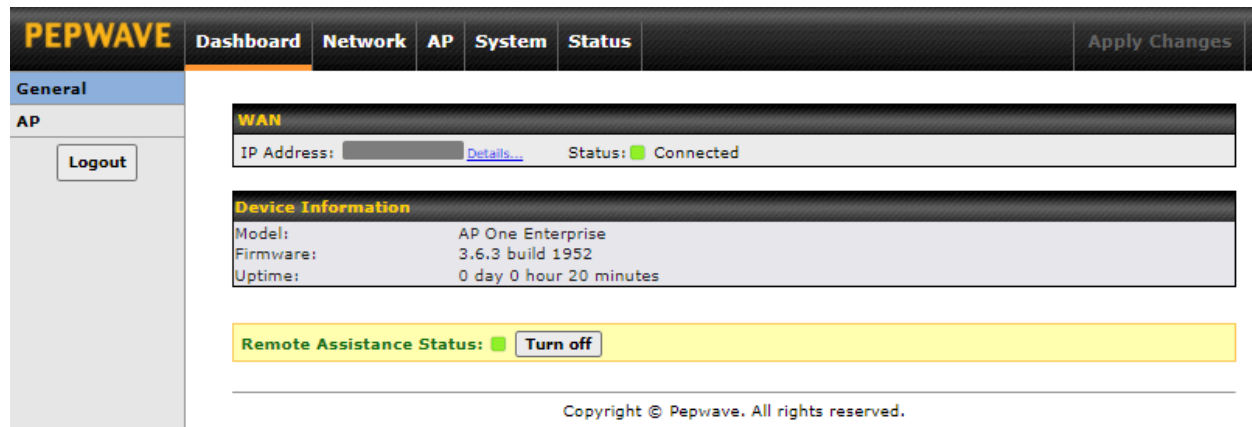
4. Connect a PC to the backbone network. Configure the IP address of the PC to be any IP address between 192.168.0.4 and 192.168.0.254, with a subnet mask of 255.255.255.0.
5. Using your favourite browser, connect to <https://192.168.0.3>.
6. Enter the default admin login ID and password, admin and public respectively.
7. After logging in, the Dashboard appears. Click the System tab to begin setting up your access point.



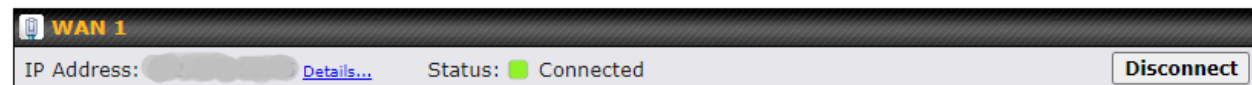
The screenshot shows the Pepwave web interface. The top navigation bar includes tabs for Dashboard, Network, AP, System, and Status, with an 'Apply Changes' button on the right. The left sidebar shows 'General' and 'AP' sections, with a 'Logout' button under 'AP'. The main content area is titled 'System' and contains three sections: 'WAN' showing 'IP Address' and 'Status: Connected'; 'Device Information' showing 'Model: AP One Enterprise', 'Firmware: 3.6.3 build 1952', and 'Uptime: 0 day 0 hour 20 minutes'; and 'Remote Assistance Status' with a 'Turn off' button. A copyright notice 'Copyright © Pepwave. All rights reserved.' is at the bottom.

## 6 Dashboard

The **Dashboard** section contains a number of displays to keep you up-to-date on your access point's status and operation. Remote assistance can also be turned off here, if it has been enabled.



### 6.1 General



This section contains WAN status and general device information.

WAN	
<b>IP Address</b>	When your access point is connected to a WAN, this field displays the WAN IP address. For more information, click the <b>Details</b> link which shows connection type details
<b>Status</b>	This field displays the current WAN connection status.

Device Information	
<b>Model:</b>	AP One Enterprise
<b>Firmware:</b>	3.6.3 build 1952
<b>Uptime:</b>	0 day 0 hour 21 minutes

Device Information	
<b>Model</b>	This field displays your access point's model number.
<b>Firmware</b>	The firmware version currently running on your access point appears here.
<b>Uptime</b>	This field displays your access point's uptime since the last reboot or shutdown.

## 6.2 AP

This section displays a variety of information about your wireless network.

**PEPWAVE**
Dashboard
Network
**AP**
System
Status
Apply Changes

General
AP
Logout

**Wireless Network**
ON

SSID	Radio	Security Policy	Ch.	TX Power	VLAN	MAC Address (BSSID)
	2.4GHz	WPA and WPA2 (PSK)	1	20dBm	0	
	5GHz	WPA and WPA2 (PSK)	36	20dBm	0	
	2.4GHz	WPA and WPA2 (PSK)	1	20dBm	100	
	2.4GHz 5GHz	WPA and WPA2 (PSK)	1 36	20dBm 20dBm	200	

Usage Data Type: Per SSID Hourly Radio: ☒ 2.4GHz ☒ 5GHz

Wireless Network Usage



Number of Wireless Clients

Wireless Network Usage

**AP Status**

<b>Wireless Network SSID</b>	This field displays your access point's SSID.
<b>Radio</b>	The radio frequency currently used by your access point appears here. If you're using the AP One AC mini or the AP One In-Wall and have configured both radios, this displays both radios in use.
<b>Security Policy</b>	This field displays the security policy your access point is currently using. If you're using the AP One AC mini and have configured both radios, this displays channels in use for the 2.4GHz and 5GHz bands.

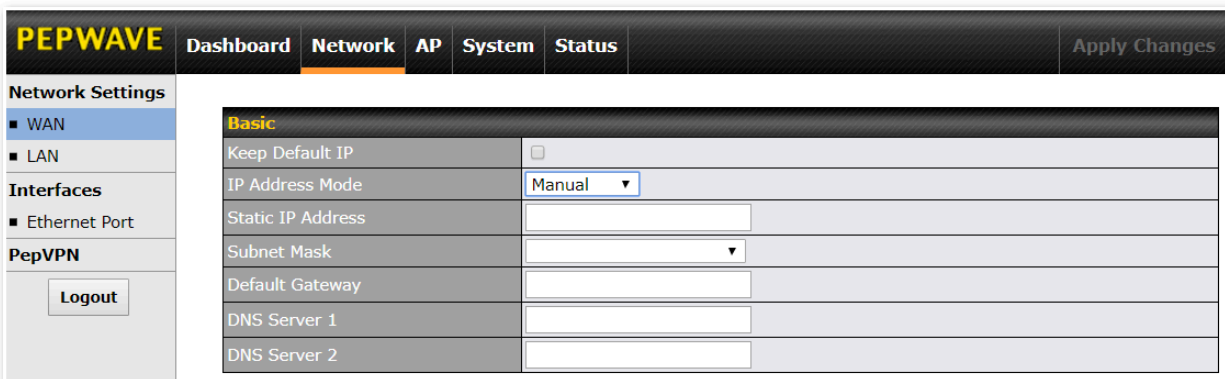


<b>Channel</b>	The channel currently used by your access point is displayed in this field.												
<b>TX Power</b>	This field displays the current transmission power of your access point.												
<b>VLAN</b>	If your access point is using a VLAN ID for management traffic, it will appear here. A value of <b>0</b> indicates that a VLAN ID is not being used.												
<b>MAC Address (BSSID)</b>	Your access point's MAC address appears here. If you're using the AP One AC mini and have configured both radios, this displays a MAC address for both the 2.4GHz and 5GHz radio.												
<b>Info</b> 	<p>Click this link to display the following information panel:</p> <table border="1"> <thead> <tr> <th colspan="2">INFO <a href="#">Close</a></th> </tr> </thead> <tbody> <tr> <td>Broadcast SSID</td><td>Enable</td> </tr> <tr> <td>Web Portal Login</td><td>Disable</td> </tr> <tr> <td>MAC Filter</td><td>None</td> </tr> <tr> <td>Bandwidth Control</td><td>Disable</td> </tr> <tr> <td>Layer 2 Isolation</td><td>Disable</td> </tr> </tbody> </table>	INFO <a href="#">Close</a>		Broadcast SSID	Enable	Web Portal Login	Disable	MAC Filter	None	Bandwidth Control	Disable	Layer 2 Isolation	Disable
INFO <a href="#">Close</a>													
Broadcast SSID	Enable												
Web Portal Login	Disable												
MAC Filter	None												
Bandwidth Control	Disable												
Layer 2 Isolation	Disable												
<b>Stat</b> 	<p>Click this link to display the following statistics panel:</p> <table border="1"> <thead> <tr> <th colspan="2">STAT <a href="#">Close</a></th> </tr> </thead> <tbody> <tr> <td>Packets Sent</td><td>0</td> </tr> <tr> <td>Bytes Sent</td><td>0</td> </tr> <tr> <td>Packets Received</td><td>0</td> </tr> <tr> <td>Bytes Received</td><td>0</td> </tr> </tbody> </table>	STAT <a href="#">Close</a>		Packets Sent	0	Bytes Sent	0	Packets Received	0	Bytes Received	0		
STAT <a href="#">Close</a>													
Packets Sent	0												
Bytes Sent	0												
Packets Received	0												
Bytes Received	0												
<b>Usage Data Type</b>	Select <b>Per SSID</b> or <b>AP Send / Recv</b> to determine the data displayed in the graphs below.												
<b>Hourly</b>	Check this box to graph wireless network usage on an hourly basis.												
<b>Radio</b>	Select the radio 2.4GHz or 5GHz and check the box to graph wireless network usage.												
<b>Wireless Network Usage/Number of Wireless Clients</b>	These graphs detail recent wireless network usage.												

## 7 Network

The settings on the **Network** tab control WAN and LAN settings, as well as allow you to set up PepVPN profiles.

### 7.1 WAN



This section provides basic and advanced WAN settings.

Basic	
<b>Keep Default IP</b>	When enabled, this option maintains <b>192.168.0.3</b> as your access point's IP address.
<b>IP Address Mode</b>	<b>IP Address Mode</b> options are <b>Automatic</b> and <b>Manual</b> . In <b>Automatic</b> mode, the IP address of your access point is acquired from a DHCP server on the Ethernet segment. In <b>Manual</b> mode, a user-specified IP address is used for your access point, as described below.
<b>Static IP Address / Subnet Mask</b>	You can use these fields to specify a unique IP address that your access point will use to communicate on the Ethernet segment. This IP address is distinct from the admin IP address (192.168.0.3) on the Ethernet segment.
<b>Default Gateway</b>	Enter the IP address of the default gateway to the internet.
<b>DNS Server</b>	Enter the DNS server address that your access point will use to resolve host names.

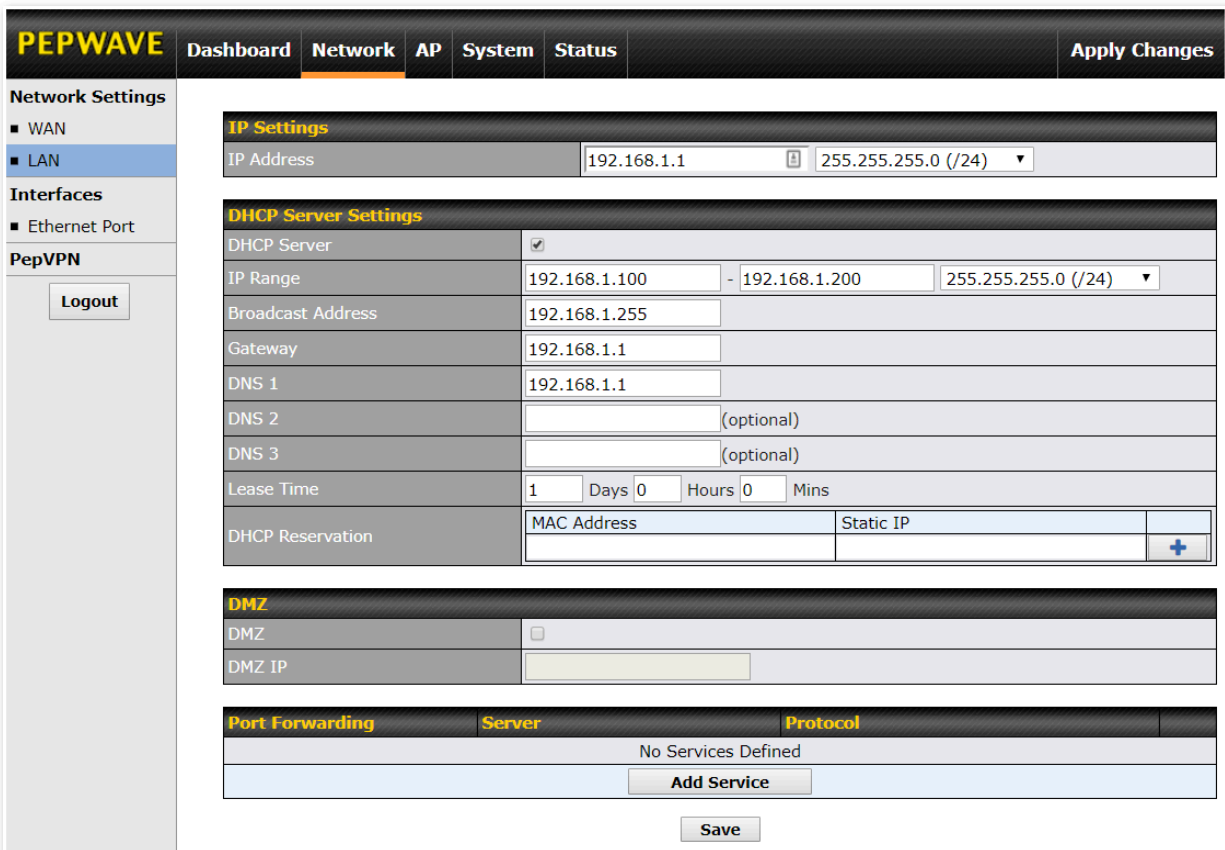
Advanced			
Management VLAN ID	<input type="text" value="0"/>		
Spanning Tree Protocol	<input type="checkbox"/>		
Scheduled Reboot	<input type="checkbox"/>		
	Schedule	Day	Time
	Weekly ▾	Sunday ▾	00 ▾ : 00 ▾
Ethernet Speed/Duplex	Auto ▾		
AP Mode	Bridge ▾		

Advanced	
<b>Management VLAN ID</b>	This field specifies the VLAN ID to tag to management traffic, such as AP-to-AP controller communication traffic. The value is <b>0</b> by default, meaning that no VLAN tagging will be applied. NOTE: change this value with caution as alterations may result in loss of connection to the AP controller.
<b>Spanning Tree Protocol</b>	Checking this box enables spanning tree protocol, used to prevent loops in bridged Ethernet LANs
<b>Scheduled Reboot</b>	When this box is checked, your access point can be scheduled to reboot automatically on a recurring basis, as indicated by the values under the <b>Schedule</b> , <b>Day</b> , and <b>Time</b> headings.
<b>Ethernet Speed/Duplex</b>	<p>This is the port speed of the WAN connection. It should be set to the same speed as the connected device in case of any port negotiation problems.</p> <p>When a static speed is set, you may choose whether to advertise its speed to the peer device or not. Advertise Speed is selected by default. You can choose not to advertise the port speed if the port has difficulty in negotiating with the peer device.</p> <p>Default: Auto</p>
<b>AP Mode</b>	Your access point can act as a bridge or as a router, depending on your selection here. When <b>Router</b> is selected, you can additionally select whether the access point will function in <b>NAT</b> or <b>IP Forwarding</b> mode.

## 7.2 LAN

This section offers a variety of settings that affect your access point's operation on the LAN, such as settings for DHCP, DMZ, and port forwarding.

\*Note that the following settings will be available only when your access point is operating in router mode.





The screenshot shows the PEPWAVE web interface with the 'Network' tab selected. The left sidebar contains 'Network Settings' (WAN, LAN), 'Interfaces' (Ethernet Port), and 'PepVPN' (Logout). The main content area is divided into several sections:

- IP Settings:** IP Address (192.168.1.1), Subnet Mask (255.255.255.0 /24).
- DHCP Server Settings:** DHCP Server (checked), IP Range (192.168.1.100 - 192.168.1.200), Broadcast Address (192.168.1.255), Gateway (192.168.1.1), DNS 1 (192.168.1.1), DNS 2 (optional), DNS 3 (optional), Lease Time (1 Days, 0 Hours, 0 Mins), and a DHCP Reservation table with columns for MAC Address and Static IP.
- DMZ:** DMZ (unchecked), DMZ IP (empty field).
- Port Forwarding:** A table with columns for Server and Protocol, currently showing 'No Services Defined' and an 'Add Service' button.

A 'Save' button is located at the bottom of the settings area.

IP Settings	
<b>IP Address</b>	Enter the LAN IP address and subnet mask to assign to your access point on the LAN.

DHCP Server Settings	
<b>DHCP Server</b>	Check to enable the DHCP server feature of your access point. Enabling DHCP is the best option for most users. The following options will be enabled once you have checked and enabled the DHCP server.
<b>IP Range</b>	Enter the first and last IP addresses of the range of addresses that your access point will make available to DHCP clients. The default range is from <b>192.168.1.100</b> to

	192.168.1.200, with 24-bit subnet mask.
<b>Broadcast Address</b>	Enter the broadcast address that DHCP clients will use when communicating with the entire LAN segment. The default value is <b>192.168.1.255</b> .
<b>Gateway</b>	Enter the default gateway address that DHCP clients will use to access the internet. By default, this address will be the same as your access point's IP address on the LAN.
<b>DNS 1/2/3</b>	In <b>DNS 1</b> , enter the IP address of the primary DNS server offered to DNS clients or accept the default of <b>192.168.1.1</b> , which is your access point's address on the LAN. You can also specify up to two additional DNS servers to use when the primary server is busy or down.
<b>Lease Time</b>	Specify the length of time that an IP address of a DHCP client remains valid. When an address lease time has expired, the assigned IP address is no longer valid, and renewal of the IP address assignment is required. By default, this value is set to one day.
<b>DHCP Reservation</b>	To reserve certain addresses for specific clients, such as network printers, enter the device's MAC Address and a static IP to be assigned to the device. Click  to add the DHCP reservation. To delete a DHCP reservation, click  .

DMZ	
DMZ	<input type="checkbox"/>
DMZ IP	<input type="text"/>

DMZ	
<b>DMZ</b>	Check this box to forward traffic sent to the WAN IP address to the DMZ IP address.
<b>DMZ IP</b>	Enter an IP address clients will use to connect to the DMZ.

Port Forwarding	Server	Protocol
No Services Defined		
<a href="#">Add Service</a>		

To create a port forwarding rule, first click the **Add Service** button, located in the **Port Forwarding** section..

Port Forwarding	
<b>Service Name</b>	Enter a name for the new port forwarding rule. Valid values for this setting consist of alphanumeric and underscore “_” characters only.

## IP Protocol

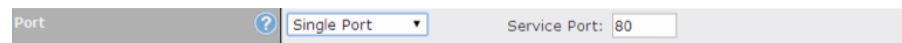
The **IP Protocol** setting, along with the **Port** setting, specifies the protocol of the service as TCP, UDP, ICMP, or IP. Traffic that is received by your access point via the specified protocol at the specified port(s) is forwarded to the LAN hosts specified by the **Servers** setting. Please see 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.

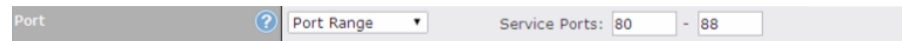
## Port

The **Port** setting specifies the port(s) that correspond to the service, and can be configured to behave in one of the following manners:

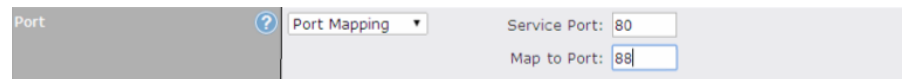
### Single Port, Port Range, Port Mapping



**Single Port:** Traffic that is received by your access point via the specified protocol at the specified port is forwarded via the same port to the servers specified by the **Server IP Address** 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 your access point via the specified protocol at the specified port range is forwarded via the same respective ports to the LAN hosts specified by the **Server IP Address** 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 your access point via the specified protocol at the specified port is forwarded via a different port to the servers specified by the **Server IP Address** setting.

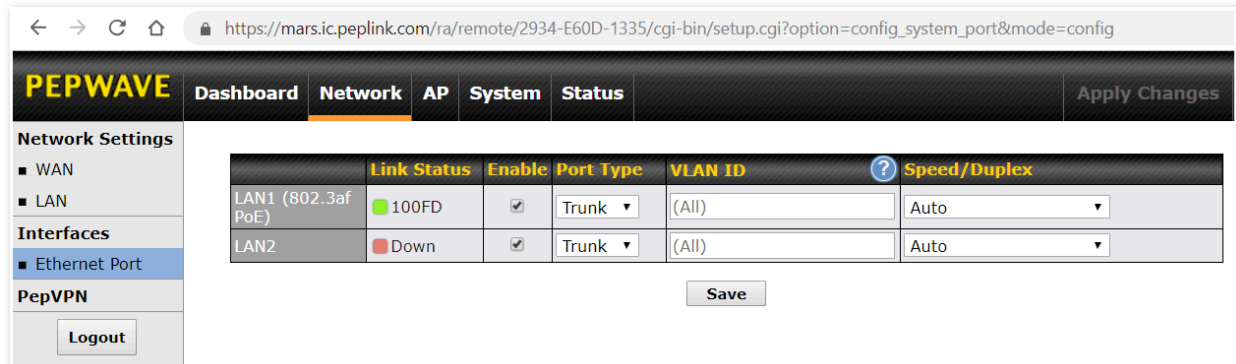
For example, with **IP Protocol** set to **TCP**, and **Port** set to **Port Mapping**, **Service Port** 80, and **Map to Port** 88, TCP traffic on Port 80 is forwarded to the configured server via Port 88.

## Server IP Address

Enter the LAN IP address of the server that handles requests for the forwarded service.

## 7.3 Interfaces

### 7.3.1 Ethernet Port



	Link Status	Enable	Port Type	VLAN ID	Speed/Duplex
LAN1 (802.3af PoE)	Up	<input checked="" type="checkbox"/>	Trunk	(All)	Auto
LAN2	Down	<input checked="" type="checkbox"/>	Trunk	(All)	Auto

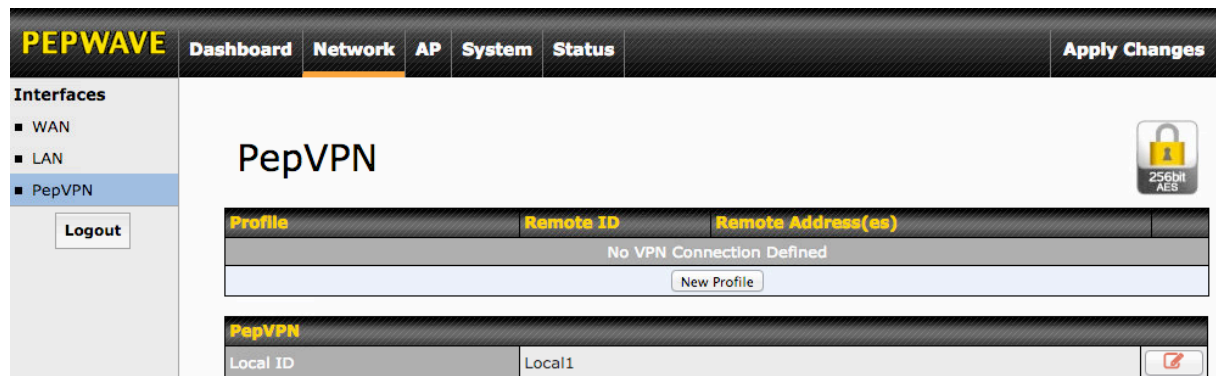
Assign one (or more) specific VLAN(s) to one of the LAN ports.  
Configure the port as Access- or Trunk-port .

For Trunk port, enter multiple VLAN IDs for VLAN filtering (e.g. 1,5-8,10) or keep the field empty for accepting all VLANs.

For Access port, only a single VLAN ID is supported.

## 7.4 PepVPN

PepVPN securely connects one or more remote sites to the site running your access point.



Profile	Remote ID	Remote Address(es)
No VPN Connection Defined		
<a href="#">New Profile</a>		

PepVPN	
Local ID	Local1 <a href="#">Edit</a>

To set up PepVPN, first give your site a local PepVPN ID. To modify an existing local ID,

click 

**PEPWAVE**
Dashboard
Network
AP
System
Status
Apply Changes

Network Settings

- WAN
- LAN

Interfaces

- Ethernet Port

PepVPN
Logout

## PepVPN

PepVPN

Local ID

Please define a local ID before using the PepVPN . Remote units can identify this unit by this "Local ID", in addition to the serial number.

Once you've specified a local ID, click the **New Profile** button to configure PepVPN.

Settings	
Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No
Name	<input type="text"/>
Encryption	<input checked="" type="radio"/> 256-bit AES <input type="radio"/> Off
Remote ID	<input type="text"/>
Authentication	<input checked="" type="radio"/> By Remote ID only <input type="radio"/> Preshared Key
Pre-shared Key	<input type="text"/> (optional) <a href="#">Hide / Show Passphrase</a>
Remote IP Addresses / Host Names	<input type="text"/> (optional)
Layer 2 Bridging	<input type="radio"/> Yes <input checked="" type="radio"/> No
Management VLAN ID	<input type="text" value="0"/>
IP Address Mode	<input type="text" value="None"/>
IP Address	<input type="text"/>
Subnet Mask	<input type="text" value="255.255.255.0 (/24)"/>
Data Port	<input checked="" type="radio"/> Default <input type="radio"/> Custom <input type="text"/>

PepVPN Profile Settings	
<b>Enable</b>	Check this box to enable PepVPN.
<b>Name</b>	Enter 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 ( ).
<b>Encryption</b>	By default, VPN traffic is encrypted with <b>256-bit AES</b> . If <b>Off</b> is selected on both sides of a VPN connection, no encryption will be applied.
<b>Remote ID</b>	To allow your access point to establish a VPN connection with a specific remote peer using a unique identifying number, enter the peer's ID or serial number here.
<b>Authentication</b>	Select <b>By Remote ID Only</b> or <b>Preshared Key</b> to specify the method your access point will use to authenticate peers. When selecting <b>By Remote ID Only</b> , be sure to enter a



	unique peer ID number in the <b>Remote ID</b> field.
<b>Pre-shared Key</b>	This optional field becomes available when <b>Pre-shared Key</b> is selected as the VPN <b>Authentication</b> method, as explained above. <b>Pre-shared Key</b> 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. Click <b>Hide / Show Passphrase</b> to toggle passphrase visibility.
<b>Remote IP Address / Host Names (Optional)</b>	<p>Optionally, you can enter a remote peer's WAN IP address or hostname(s) here. If the remote client 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.</p> <p>With this field filled, your access point will initiate connection to each of the remote IP addresses until it succeeds in making a connection. If the field is empty, your access point 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.</p>
<b>Layer 2 Bridging</b>	When this check box is unchecked, traffic between local and remote networks will be IP forwarded. To bridge the Ethernet network of an Ethernet port on a local and remote network, select <b>Layer 2 Bridging</b> . When this check box is selected, the two networks will become a single LAN, and any broadcast (e.g., ARP requests) or multicast traffic (e.g., Bonjour) will be sent over the VPN.
<b>Management VLAN ID</b>	This field specifies the VLAN ID that will be tagged to management traffic, such as AP-to-AP controller communication traffic. A value of 0 indicates that no VLAN tagging will be applied.
<b>IP Address Mode</b>	Choose <b>Automatic</b> or <b>Manual</b> . In automatic mode, your access point acquires an IP from a DHCP server on the Ethernet segment. In manual mode, your access point uses a user-specified IP address.
<b>IP Address/Subnet Mask</b>	When using manual IP addressing (above), enter an IP address and subnet mask in these fields.
<b>Data Port</b>	This field specifies the outgoing UDP port number for transporting VPN data. If <b>Default</b> is selected, port 4500 will be used by default. Port 32015 will be used if port 4500 is unavailable. If <b>Custom</b> is selected, you can input a custom outgoing port number between 1 and 65535.

## 8 AP

Use the controls on the **AP** tab to set the wireless SSID, AP settings and Mesh, as well as wireless distribution system (WDS) settings.

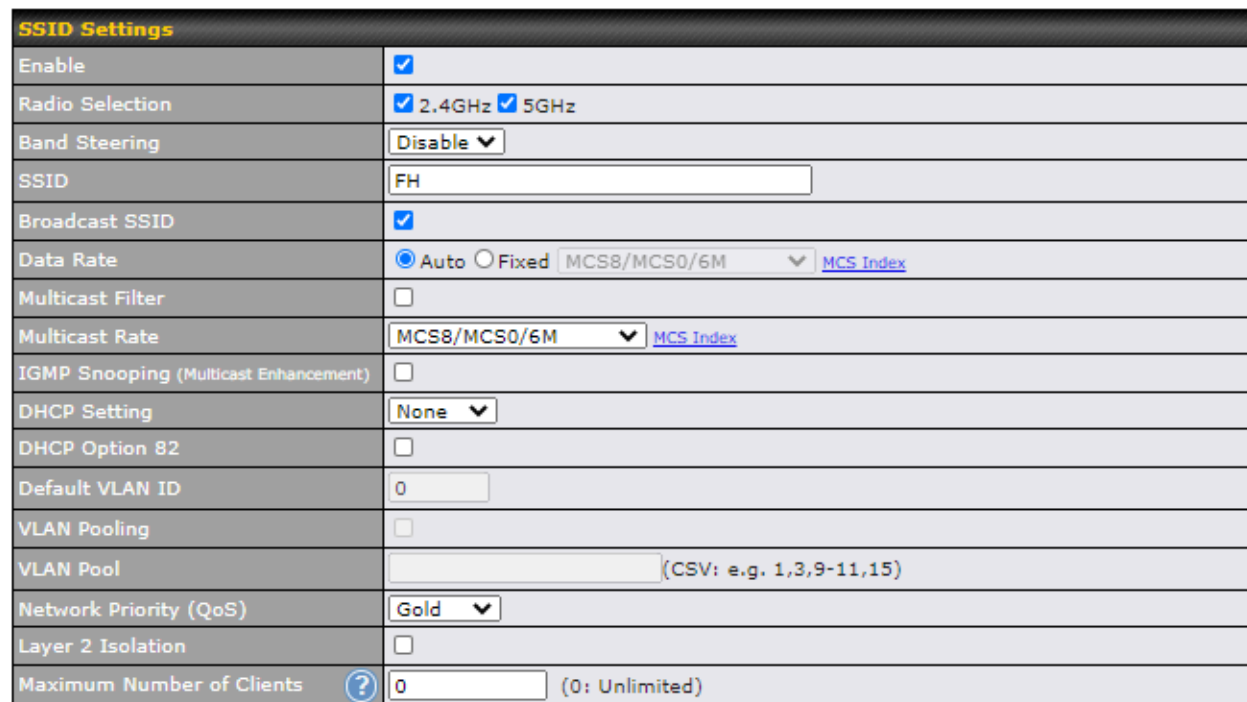
### 8.1 Wireless SSID



The screenshot shows the PEPWAVE web interface with the 'AP' tab selected. The left sidebar contains a menu with 'Wireless SSID', 'Settings', 'Mesh', and 'WDS'. The main content area displays the 'Wireless Network SSID' configuration. It includes a table with columns for 'Wireless Network SSID', 'Security Policy', and 'MAC Address (BSSID)'. The table shows a single entry with SSID 'FH', Security Policy 'WPA2 (PSK)', and MAC Address '00:1A:DD:DA:EB:E2'. A 'New SSID' button is located below the table. An 'Apply Changes' button is in the top right corner.

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

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



The screenshot shows the 'SSID Settings' configuration page. It contains a table with various settings and their values:

SSID Settings	
Enable	<input checked="" type="checkbox"/>
Radio Selection	<input checked="" type="checkbox"/> 2.4GHz <input checked="" type="checkbox"/> 5GHz
Band Steering	Disable ▾
SSID	FH
Broadcast SSID	<input checked="" type="checkbox"/>
Data Rate	<input checked="" type="radio"/> Auto <input type="radio"/> Fixed MCS8/MCS0/6M ▾ <a href="#">MCS Index</a>
Multicast Filter	<input type="checkbox"/>
Multicast Rate	MCS8/MCS0/6M ▾ <a href="#">MCS Index</a>
IGMP Snooping (Multicast Enhancement)	<input type="checkbox"/>
DHCP Setting	None ▾
DHCP Option 82	<input type="checkbox"/>
Default VLAN ID	0
VLAN Pooling	<input type="checkbox"/>
VLAN Pool	(CSV: e.g. 1,3,9-11,15)
Network Priority (QoS)	Gold ▾
Layer 2 Isolation	<input type="checkbox"/>
Maximum Number of Clients	0 (0: Unlimited)

SSID Settings	
<b>Enable</b>	Check this box to enable wireless SSID.
<b>Radio Selection</b>	<p>Available only on the AP One AC mini, this setting, shown below, allows you to enable or disable either of the two on-board radios.</p> <div>Radio Selection <input checked="" type="checkbox"/> 2.4GHz <input checked="" type="checkbox"/> 5GHz</div>
<b>Band Steering</b>	<p>This setting, shown below, allows you to reduce 2.4 GHz band overcrowding, AP with band steering steers clients capable of 5 GHz operation to 5 GHz frequency.</p> <p><b>Force</b> - Clients capable of 5 GHz operation are only offered with 5 GHz frequency.</p> <p><b>Prefer</b> - Clients capable of 5 GHz operation are encouraged to associate with 5 GHz frequency. If the clients insist to attempt on 2.4 GHz frequency, 2.4 GHz frequency will be offered.</p> <p>Default: <b>Disable</b></p> <div>Band Steering <span>Disable ▾</span></div>
<b>SSID</b>	This setting specifies the AP SSID that Wi-Fi clients will see when scanning.
<b>Broadcast SSID</b>	This setting specifies whether or not Wi-Fi clients can scan the SSID of this wireless network. <b>Broadcast SSID</b> is enabled by default.
<b>Data Rate</b>	Select <b>Auto</b> to allow your access point to set the data rate automatically, or select <b>Fixed</b> and choose a rate from the drop-down menu. Click the <b>MCS Index</b> link to display a reference table containing MCS and matching HT20 and HT40 values.
<b>Multicast Filter</b>	This setting enables the filtering of multicast network traffic to the wireless SSID.
<b>Multicast Rate</b>	This setting specifies the transmit rate to be used for sending multicast network traffic.
<b>IGMP Snooping</b>	To allow your access point to convert multicast traffic to unicast traffic for associated clients, select this option.
<b>DHCP Setting</b>	To set your access point as a DHCP server or relay, select <b>Server</b> or <b>Relay</b> . Otherwise, select <b>None</b> .
<b>DHCP Option 82</b>	If you use a distributed DHCP server/relay environment, you can enable this option to provide additional information on the manner in which clients are physically connected to the network.
<b>Default VLAN ID</b>	This setting specifies the VLAN ID to be tagged on all outgoing packets generated from this wireless network (i.e., packets that travel from the Wi-Fi segment through your access point to the Ethernet segment via the LAN port). If 802.1x is enabled and a per-user VLAN ID is specified in <b>authentication reply from the Radius server</b> , then the value specified by <b>Default VLAN ID</b> will be overridden. The default value of this setting is <b>0</b> , which means VLAN tagging is disabled (instead of tagged with zero).
<b>VLAN Pooling</b>	Check this box to enable VLAN pooling using the values specified in <b>VLAN Pool</b> .
<b>VLAN Pool</b>	If VLAN pooling is enabled, enter VLAN pool values separated by commas.

<b>Network Priority (QoS)</b>	Select from <b>Gold</b> , <b>Silver</b> , and <b>Bronze</b> to control the QoS priority of this wireless network traffic.
<b>Layer 2 Isolation</b>	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 the upper communication layer(s). By default, the setting is disabled.
<b>Maximum Number of Clients</b>	The maximum number of clients that can simultaneously connect to your access point, or enter <b>0</b> to allow unlimited Wi-Fi clients.

Security Settings	
<b>Security Policy</b>	This setting configures the wireless authentication and encryption methods. Available options are <b>Open (No Encryption)</b> , <b>WPA2 – Personal</b> , <b>WPA2 – Enterprise</b> , <b>WPA3 - Personal</b> , <b>WPA/WPA2 - Personal</b> , <b>WPA/WPA2 – Enterprise</b> , and <b>WPA2/WPA3 - Personal</b> . To allow any Wi-Fi client to access your AP without authentication, select <b>Open (No Encryption)</b> . Details on each of the available authentication methods follow.

Security Settings	
Security Policy	WPA2 - Personal ▼
Passphrase	<input type="text"/> <a href="#">Hide / Show Passphrase</a>
Fast Transition	<input type="checkbox"/>
Management Frame Protection	Optional ▼

WPA2 – Personal	
<b>Passphrase</b>	Enter a passphrase of between 8 and 63 alphanumeric characters to create a passphrase used for data encryption and authentication. Click <b>Hide / Show Passphrase</b> to toggle visibility.
<b>Fast Transition</b>	Fast Transition [802.11r] The transition process of a mobile client as it moves between access points is improved when this option is ticked.
<b>Management Frame Protection</b>	This feature protects stations against forged management frames spoofed from other devices. Frames that are protected include Disassociation, Deauthentication and QoS Action

Security Settings	
Security Policy	WPA2 - Enterprise ▼
802.1X Version	<input type="radio"/> v1 <input checked="" type="radio"/> v2
Management Frame Protection	Optional ▼

### WPA2 – Enterprise

#### 802.1X Version

Choose **v1** or **v2** of the 802.1x EAPOL. When **v1** is selected, both v1 and v2 clients can associate with the access point. When **v2** is selected, only v2 clients can associate with the access point. Most modern wireless clients support v2. For stations that do not support v2, select **v1**. The default is **v2**.

#### Management Frame Protection

This feature protects stations against forged management frames spoofed from other devices. Frames that are protected include Disassociation, Deauthentication and QoS Action

Security Settings	
Security Policy	WPA3 - Personal ▼
Passphrase	<input type="text"/> <a href="#">Hide / Show Passphrase</a>
Fast Transition	<input type="checkbox"/>

### WPA3 – Personal

#### Passphrase

Enter a passphrase of between 8 and 63 alphanumeric characters to create a passphrase used for data encryption and authentication. Click **Hide / Show Passphrase** to toggle visibility.

#### Fast Transition

[802.11r] The transition process of a mobile client as it moves between access points is improved when this option is ticked.

Security Settings	
Security Policy	WPA/WPA2 - Personal ▼
Passphrase	<input type="text"/> <a href="#">Hide / Show Passphrase</a>
Management Frame Protection	Optional ▼

### WPA/WPA2 – Personal

#### Passphrase

Enter a passphrase of between 8 and 63 alphanumeric characters to create a passphrase used for data encryption and authentication. Click **Hide / Show Passphrase** to toggle visibility.

#### Management

This feature protects stations against forged management frames spoofed from other devices. Frames that are protected include Disassociation, Deauthentication and QoS

## Frame Protection Action

Security Settings	
Security Policy	WPA/WPA2 - Enterprise ▼
802.1X Version	<input type="radio"/> v1 <input checked="" type="radio"/> v2
Management Frame Protection	Optional ▼

### WPA/WPA2 – Enterprise

#### 802.1X Version

Choose **v1** or **v2** of the 802.1x EAPOL. When **v1** is selected, both v1 and v2 clients can associate with the access point. When **v2** is selected, only v2 clients can associate with the access point. Most modern wireless clients support v2. For stations that do not support v2, select **v1**. The default is **v2**.

#### Management Frame Protection

This feature protects stations against forged management frames spoofed from other devices. Frames that are protected include Disassociation, Deauthentication and QoS Action

Security Settings	
Security Policy	WPA2/WPA3 - Personal ▼
Passphrase	<input type="text"/> <a href="#">Hide / Show Passphrase</a>
Fast Transition	<input type="checkbox"/>
Management Frame Protection	Optional ▼

### WPA2/WPA3 – Personal

#### Passphrase

Enter a passphrase of between 8 and 63 alphanumeric characters to create a passphrase used for data encryption and authentication. Click **Hide / Show Passphrase** to toggle visibility.

#### Fast Transition





[802.11r] The transition process of a mobile client as it moves between access points is improved when this option is ticked.

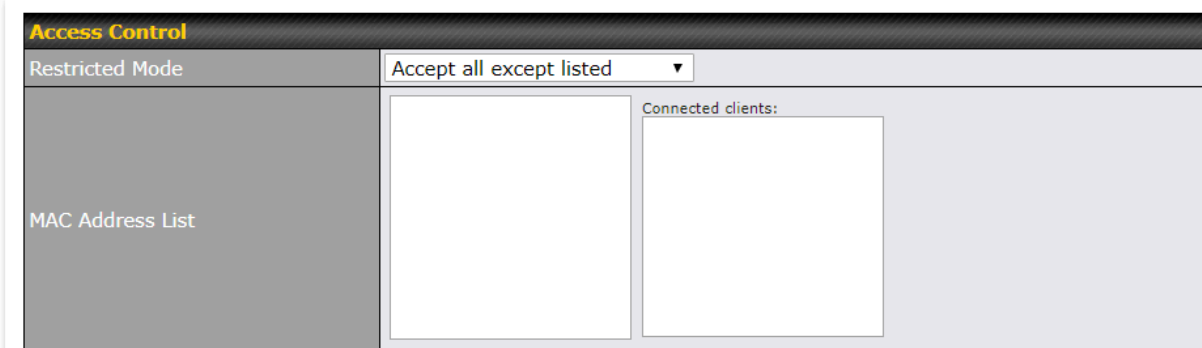
#### Management Frame Protection

This feature protects stations against forged management frames spoofed from other devices. Frames that are protected include Disassociation, Deauthentication and QoS Action

Captive Portal	
Captive Portal	Enable ▾
Authentication Method	RADIUS ▾
RADIUS Security	PAP ▾
CoA-DM	<input type="checkbox"/>
Splash Page	http:// ▾ <input type="text"/>
Landing Page	<input type="checkbox"/>
Landing Page URL	<input type="text"/>
Profile MAC Address	<input checked="" type="radio"/> BSSID <input type="radio"/> LAN MAC Address
Concurrent Login	<input checked="" type="checkbox"/>
Access Quota	<input type="text" value="0"/> minutes (0: Unlimited) <input type="text" value="0"/> MB (0: Unlimited)
Inactive Timeout	<input type="text" value="0"/> minutes
Quota Reset Time	<input checked="" type="radio"/> Disable <input type="radio"/> Daily at: <input type="text" value="00"/> : <input type="text" value="00"/> <input type="radio"/> <input type="text" value="0"/> minutes after quota reached
Allowed Domains / IPs	<div>Domains / IPs</div> <div><input type="text"/></div> <div><input type="button" value="+"/></div>
Allowed Clients	<div>MAC / IP Address</div> <div><input type="text"/></div> <div><input type="button" value="+"/></div>

Captive Portal Login	
<b>Captive Portal</b>	Select <b>Enable</b> to turn on your access point's built-in captive portal functionality.
<b>Authentication Method</b>	Choose <b>Open Access</b> to allow users to connect without authentication or <b>RADIUS</b> to require authentication. If <b>RADIUS</b> is selected, you'll be given the opportunity to select a RADIUS security method in the next field.
<b>RADIUS Security</b>	Select <b>PAP</b> , <b>EAP-TTLS PAP</b> , <b>EAP-TTLS MSCHAPv2</b> , or <b>PEAPv0 EAP-MSCHAPv2</b> .
<b>Splash Page</b>	If your web portal will use a splash page, choose <b>HTTP</b> or <b>HTTPS</b> and enter the splash page's URL.
<b>Landing Page</b>	If your web portal will use a landing page, check this box.
<b>Landing Page URL</b>	If you have checked <b>Landing Page</b> , enter your landing page URL here.
<b>Profile MAC address</b>	<p>Value used on Called-Station-ID. By default the BSSID of the VAP is used.</p> <p>When LAN MAC Address is used the LAN MAC Address of the VAP is used instead of the BSSID.</p> <div> <input checked="" type="radio"/> BSSID           <input type="radio"/> LAN MAC Address         </div>

<b>Concurrent Login</b>	Check this box to allow users to have more than one logged in session active at a time.
<b>Access Quota</b>	Enter a value in minutes to limit access time on a given login or enter <b>0</b> to allow unlimited use time on a single login. Likewise, enter a value in MB for the total bandwidth allowed or enter <b>0</b> to allow unlimited bandwidth on a single login.
<b>Inactive Timeout</b>	Enter a value in minutes to logout following the specified period of inactivity or enter <b>0</b> to disable inactivity logouts.
<b>Quota Reset Time</b>	This menu determines how your usage quota resets. Setting it to <b>Daily</b> will reset it at a specified time every day. Setting a number of <b>minutes after quota reached</b> establishes a timer for each user that begins after the quota has been reached.
<b>Allowed Domains / IPs</b>	To whitelist a domain or IP address, enter the domain name / IP address here and click  . To delete an existing entry, click the  button next to it.
<b>Allowed Client IPs</b>	To whitelist a client IP address, enter the IP address here and click  . To delete an existing entry, click the  button next to it.



Access Control	
<b>Restricted Mode</b>	The settings allow the administrator to control access using Mac address filtering. Available options are <b>None</b> , <b>Deny all except listed</b> , <b>Accept all except listed</b> , and <b>RADIUS MAC Authentication</b> .
<b>MAC Address List</b>	Connections coming from the MAC addresses in this list will be either denied or accepted based on the option selected in the previous field.



RADIUS Server Settings	Primary Server	Secondary Server
Host	<input type="text"/>	<input type="text"/>
Secret	<input type="text"/>	<input type="text"/>
Authentication Port	<input type="text" value="1812"/> <b>Default</b>	<input type="text" value="1812"/> <b>Default</b>
Accounting Port	<input type="text" value="1813"/> <b>Default</b>	<input type="text" value="1813"/> <b>Default</b>
Maximum Retransmission	<input type="text" value="3"/>	
Radius Request Interval	<input type="text" value="3"/> s (initial value, double upon every retransmission)	
NAS-Identifier	<input type="text"/>	

RADIUS Server Settings	
<b>Host</b>	Enter the IP address of the primary RADIUS server and, if applicable, the secondary RADIUS server.
<b>Secret</b>	Enter the RADIUS shared secret for the primary server and, if applicable, the secondary RADIUS server.
<b>Authentication Port</b>	Enter the UDP authentication port(s) used by your RADIUS server(s) or click the <b>Default</b> button to enter <b>1812</b> .
<b>Accounting Port</b>	Enter the UDP accounting port(s) used by your RADIUS server(s) or click the <b>Default</b> button to enter <b>1813</b> .
<b>Maximum Retransmission</b>	Enter the maximum number of allowed retransmissions.
<b>RADIUS Request Interval</b>	Enter a value in seconds to limit RADIUS request frequency. Note the initial value will double on each retransmission.
<b>NAS-Identifier</b>	<p>Information added to access requests to identify the NAS.</p> <p>Select <b>Device Name</b>, <b>LAN MAC Address</b>, <b>Device Serial Number</b> or enter a <b>Custom Value</b></p> <p>When the NAS ID is not defined, the Device Name will be used as the NAS ID in RADIUS requests.</p>

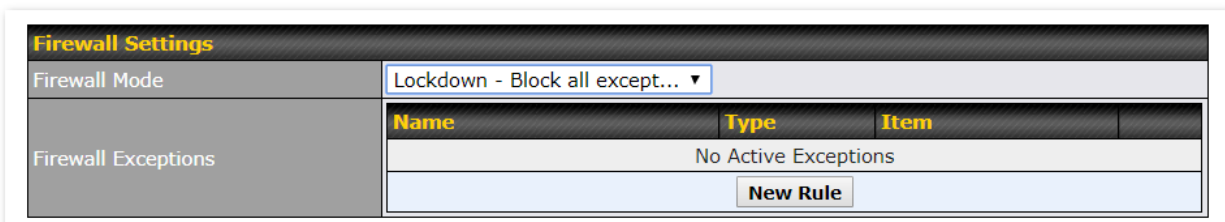
Guest Protect									
Block LAN Access	<input type="checkbox"/>								
Custom Subnet	<input type="checkbox"/> <table border="1"> <tr> <th>Network</th> <th>Subnet Mask</th> <th></th> </tr> <tr> <td><input type="text"/></td> <td>255.255.255.0 (/24) ▼</td> <td><input type="button" value="+"/></td> </tr> </table>	Network	Subnet Mask		<input type="text"/>	255.255.255.0 (/24) ▼	<input type="button" value="+"/>		
Network	Subnet Mask								
<input type="text"/>	255.255.255.0 (/24) ▼	<input type="button" value="+"/>							
Block Exception	<input type="checkbox"/> <table border="1"> <tr> <th>Network</th> <th>Subnet Mask</th> <th></th> </tr> <tr> <td><input type="text"/></td> <td>255.255.255.0 (/24) ▼</td> <td><input type="button" value="+"/></td> </tr> </table>	Network	Subnet Mask		<input type="text"/>	255.255.255.0 (/24) ▼	<input type="button" value="+"/>		
Network	Subnet Mask								
<input type="text"/>	255.255.255.0 (/24) ▼	<input type="button" value="+"/>							
Block PepVPN	<input type="checkbox"/>								

Guest Protect	
<b>Block LAN Access</b>	Check this box to block access from the LAN.
<b>Custom Subnet</b>	To specify a subnet to block, enter the IP address and choose a subnet mask from the drop-down menu. To add the blocked subnet, click <input type="button" value="+"/> . To delete a blocked subnet, click <input type="button" value="X"/> .
<b>Block Exception</b>	To create an exception to a blocked subnet (above), enter the IP address and choose a subnet mask from the drop-down menu. To add the exception, click <input type="button" value="+"/> . To delete an exception, click <input type="button" value="X"/> .
<b>Block PepVPN</b>	To block PepVPN access, check this box.


Bandwidth Management	
Bandwidth Management	<input type="checkbox"/>
Upstream Limit	<input type="text" value="0"/> kbps (0: Unlimited)
Downstream Limit	<input type="text" value="0"/> kbps (0: Unlimited)
Client Upstream Limit	<input type="text" value="0"/> kbps (0: Unlimited)
Client Downstream Limit	<input type="text" value="0"/> kbps (0: Unlimited)

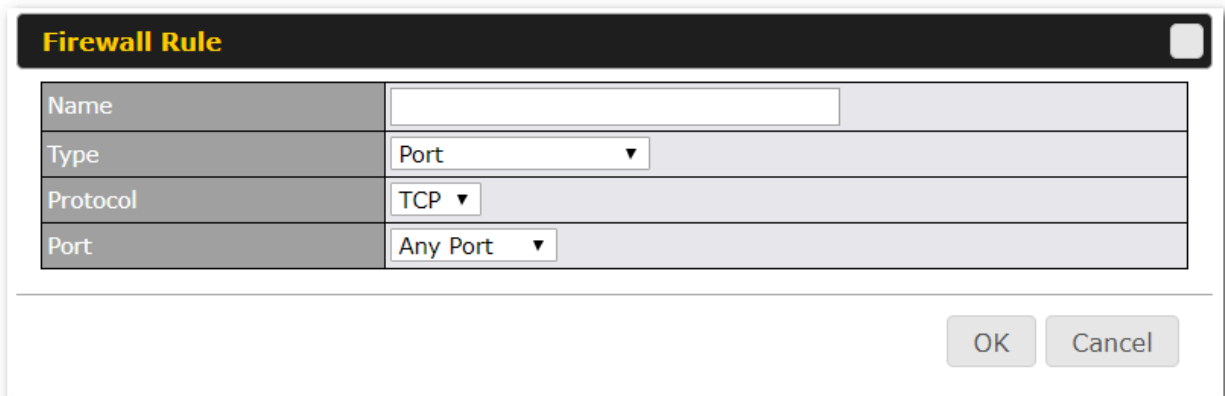
Bandwidth Management	
<b>Bandwidth Management</b>	Check this box to enable bandwidth management.
<b>Upstream Limit</b>	Enter a value in kbps to limit the wireless network's upstream bandwidth. Enter 0 to allow unlimited upstream bandwidth.

<b>Downstream Limit</b>	Enter a value in kbps to limit the wireless network's downstream bandwidth. Enter <b>0</b> to allow unlimited downstream bandwidth.
<b>Client Upstream Limit</b>	Enter a value in kbps to limit connected clients' upstream bandwidth. Enter <b>0</b> to allow unlimited upstream bandwidth.
<b>Client Downstream Limit</b>	Enter a value in kbps to limit connected clients' downstream bandwidth. Enter <b>0</b> to allow unlimited downstream bandwidth.



The screenshot shows the 'Firewall Settings' window. At the top, 'Firewall Mode' is set to 'Lockdown - Block all except...'. Below this is a table for 'Firewall Exceptions' with columns 'Name', 'Type', and 'Item'. The table is currently empty, showing 'No Active Exceptions'. A 'New Rule' button is located at the bottom right of the exceptions table.

Firewall Settings	
<b>Firewall Mode</b>	Choose <b>Flexible – Allow all except...</b> or <b>Lockdown – Block all except...</b> to turn on the firewall, then create rules for the firewall exceptions by clicking <b>New Rule</b> . See the discussion below for details on creating a firewall rule. To delete a rule, click the associated  button. To turn off the firewall, select <b>Disable</b> .



The screenshot shows the 'Firewall Rule' dialog box. It contains four input fields: 'Name' (empty), 'Type' (set to 'Port'), 'Protocol' (set to 'TCP'), and 'Port' (set to 'Any Port'). At the bottom right, there are 'OK' and 'Cancel' buttons.

Firewall Rule	
<b>Name</b>	Enter a descriptive name for the firewall rule in this field.
<b>Type</b>	Choose <b>Port</b> , <b>Domain</b> , <b>IP Address</b> , <b>MAC Address</b> or <b>Application/Service</b> to allow or deny traffic from any of those identifiers. Depending on the option chosen, the following fields

	will vary.
<b>Protocol / Port</b>	Choose <b>TCP</b> or <b>UDP</b> from the <b>Protocol</b> drop-down menu to allow or deny traffic using either of those protocols. From the <b>Port</b> drop-down menu, choose <b>Any Port</b> to allow or deny TCP or UDP traffic on any port. Choose <b>Single Port</b> and then enter a port number in the provided field to allow or block TCP or UDP traffic from that port only. You can also choose <b>Port Range</b> and enter a range of ports in the provided fields to allow or deny TCP or UDP traffic from the specified port range.
<b>IP Address / Subnet Mask</b>	If you have chosen <b>IP Address</b> as your firewall rule type, enter the IP address and subnet mask identifying the subnet to allow or deny.
<b>MAC Address</b>	If you have chosen <b>MAC Address</b> as your firewall rule type, enter the MAC address identifying the machine to allow or deny.
<b>Application/ Service</b>	If you have chosen <b>Application/Service</b> as your firewall rule type, choose <b>TCP</b> or <b>UDP</b> from the <b>Protocol</b> drop-down menu to allow or deny traffic using either of those protocols. Select a service from the <b>Selection Tool</b> drop down list. From the <b>Port</b> drop-down menu, choose <b>Any Port</b> to allow or deny TCP or UDP traffic on any port. Choose <b>Single Port</b> and then enter a port number in the provided field to allow or block TCP or UDP traffic from that port only. You can also choose <b>Port Range</b> and enter a range of ports in the provided fields to allow or deny TCP or UDP traffic from the specified port range.

Schedule

☐ Always On
☒ Custom Schedule

	Midnight	4am	8am	Noon	4pm	8pm
Sunday	✓	✓	✓	✓	✓	✓
Monday	✓	✓	✓	✓	✓	✓
Tuesday	✓	✓	✓	✓	✓	✓
Wednesday	✓	✓	✓	✓	✓	✓
Thursday	✓	✓	✓	✓	✓	✓
Friday	✓	✓	✓	✓	✓	✓
Saturday	✓	✓	✓	✓	✓	✓

Schedule	
Option to schedule SSID availability	
<b>Always on</b>	The SSID is always on
<b>Custom/Schedule</b>	Define a custom schedule by selecting the desired time slots when the SSID should be enabled

ARP Request Control				
Default Handling	<input checked="" type="radio"/> Bypass <input type="radio"/> Drop			
Custom Action	IP	MAC Address	ACTION	
	<input type="text"/>	<input type="text"/>	Reply ▼	<input data-bbox="1344 470 1393 504" type="button" value="+"/>

ARP Request Control	
ARP request control is a Broadcast filter feature which: <ul style="list-style-type: none"> <li>• blocks all broadcast traffic,</li> <li>• relays DHCP requests,</li> <li>• responds to ARP requests asking the MAC address of the gateway</li> </ul>	
<b>Default handling</b>	Choose between <b>Bypass</b> or <b>Drop</b> (default Bypass)
<b>Custom Action</b>	Add IP/ MAC address pairs to this field to either: <b>REPLY</b> : The AP replies to the MAC address itself according to the config <b>DNAT</b> : The AP can translate the destination MAC address from a broadcast to a particular MAC address

## 8.2 Settings

Basic access point operation settings, such as the protocol and channels used, as well as scanning interval and other advanced settings, can be defined and managed in this section

AP Settings	2.4GHz	5GHz
Protocol	802.11ng ▼	802.11n/ac ▼
Operating Country	United Kingdom ▼	
Channel Width	20 MHz ▼	80 MHz ▼
Channel	1 (2.412 GHz) ▼	Auto ▼ <a href="#">Edit</a>
Output Power	Max ▼ Offset: -0 dBm <input type="checkbox"/> Boost	Max ▼ Offset: -0 dBm <input type="checkbox"/> Boost
Beacon Rate	1Mbps ▼ * 6Mbps will be used for 5GHz radio	
Beacon Interval	100ms ▼	
DTIM	1	
RTS Threshold	0	
Fragmentation Threshold	0	
Distance / Time Convertor	<input type="text" value="4050"/> m (input distance for recommended values)	
Slot Time	<input type="radio"/> Auto <input checked="" type="radio"/> Custom <input type="text" value="9"/> μs <a href="#">Default</a>	
ACK Timeout	<input type="text" value="48"/> μs <a href="#">Default</a>	
Frame Aggregation	<input checked="" type="checkbox"/>	
Aggregation Length	<input type="text" value="50000"/>	
Maximum Number of Clients	<input type="text" value="0"/> (0: Unlimited)	<input type="text" value="0"/> (0: Unlimited)
Client Signal Strength Threshold	<input type="text" value="0"/> (0: Unlimited)	<input type="text" value="0"/> (0: Unlimited)

Advanced Features	
Discover Nearby Networks	<input checked="" type="checkbox"/> * Discover Nearby Networks will be enabled if Channel is set to Auto
Scanning Interval	<input type="text" value="10"/> s
Scanning Time	<input type="text" value="50"/> ms
Scheduled Radio Availability	<input checked="" type="radio"/> Always On <input type="radio"/> Custom Schedule
WMM	<input checked="" type="checkbox"/>

AP Settings							
<b>Protocol</b>	<p>Choose <b>802.11ng</b> or <b>802.11n/ac</b> as your access point's Wi-Fi protocol.</p> <p>The AP One AC mini provides the <b>802.11ng</b> protocol for the 2.4 GHz band and the <b>802.11n/ac</b> protocol for the 5GHz band, as shown below.</p> <table border="1"> <thead> <tr> <th>AP Settings</th> <th>2.4GHz</th> <th>5GHz</th> </tr> </thead> <tbody> <tr> <td>Protocol</td> <td>802.11ng ▼</td> <td>802.11n/ac ▼</td> </tr> </tbody> </table>	AP Settings	2.4GHz	5GHz	Protocol	802.11ng ▼	802.11n/ac ▼
AP Settings	2.4GHz	5GHz					
Protocol	802.11ng ▼	802.11n/ac ▼					
<b>Operating Country</b>	<p>This drop-down menu specifies the national / regional regulations the AP should follow. If a North American region is selected, RF channels 1 to 11 will be available and the maximum transmission power will be 26 dBm (400 mW).</p>						

	<p>If European region is selected, RF channels 1 to 13 will be available. The maximum transmission power will be 20 dBm (100 mW).</p> <p>NOTE: Users are required to choose an option suitable to local laws and regulations. Per FCC regulation, the country selection is not available on all models marketed in the US. All US models are fixed to US channels only.</p>
Channel Width	<p>This option defines which channel width the radio will use:  <b>20MHz</b> - Supports clients with 20MHz capability.  This is the default value for 802.11ng.  <b>40MHz</b> - Supports clients with 20/40MHz capability.  <b>20/40MHz</b> - Supports clients with 20/40 MHz capability.  The radio will fall back to 20MHz if it detects APs that only support 20MHz. This is the default value for 802.11na.  <b>80MHz</b> - Supports clients with 20/40/80MHz capability.  This is the default value for 802.11n/ac</p> <div> Channel Width <span>?</span> 20 MHz 80 MHz </div>
Channel	<p>This drop-down menu selects the 2.4 Ghz and 5GHz 802.11 channels to be used.  When <b>Auto</b> is selected, the system will perform channel scanning based on the scheduled time set and choose the most suitable channel automatically.</p> <div> Channel 1 (2.412 GHz) Auto Edit </div>
Output Power	<p>This option enables the configuration of transmission power.  Choose between :Max / High / Medium / Low  <b>Max</b> is the Maximum power supported for that country or Maximum power supported for the device (whichever is the smaller value)  <b>High</b> is 3dBm below the max value.  <b>Medium</b> is 3dBm below high value  <b>Low</b> is 3 dBm below Medium value</p> <div> Output Power <span>?</span> Max Offset: -0 dBm Boost Max Offset: -0 dBm Boost </div>
Antenna Gain	<p>This advanced feature becomes available when selecting this option in the Help section( select the question mark) of the Output Power.</p> <div> Antenna Gain 0 dBi Preserve on restore 0 dBi Preserve on restore </div>
Beacon Rate	<p>This drop-down menu provides the option to send beacons in different transmit bit rates. The bit rates are <b>1 Mbps, 2 Mbps, 5.5 Mbps, 6 Mbps, and 11 Mbps</b>.</p>
Beacon Interval	<p>Set the time between each beacon send. Available options are <b>100 ms, 250 ms, and 500 ms</b>.</p>
DTIM	<p>Set the frequency for the beacon to include delivery traffic indication messages (DTIM). The interval unit is measured in milliseconds.</p>
RTS Threshold	<p>Set the minimum packet size for your access point to send an RTS using the RTS/CTS handshake. Setting <b>0</b> disables this feature.</p>
Fragmentation Threshold	<p>Enter a value to limit the maximum frame size, which can improve performance.</p>

<b>Distance / Time Convertor</b>	This slider and text entry field can be used to interactively set slot time.
<b>Slot Time</b>	This field provides the option to modify the unit wait time before your access point transmits. The default value is <b>9μs</b> .
<b>ACK Timeout</b>	Set the wait time to receive an acknowledgement packet before retransmitting. The default value is <b>48μs</b> .
<b>Frame Aggregation</b>	With this feature enabled, throughput will be increased by sending two or more data frames in a single transmission.
<b>Aggregation Length</b>	This field is only available when <b>Frame Aggregation</b> is enabled. It specifies the frame length for frame aggregation. By default, it is set to <b>50000</b> .
<b>Max number of Clients</b>	Enter the maximum clients that can simultaneously connect to your access point or set the value to <b>0</b> to allow unlimited clients.
<b>Client Signal Strength Threshold</b>	This field determines the minimum acceptable client signal strength, specified in megawatts. If client signal strength does not meet this minimum, the client will not be allowed to connect.

Advanced Features																																																									
Discover Nearby Networks	<input checked="" type="checkbox"/> * Discover Nearby Networks will be enabled if Channel is set to Auto																																																								
Scanning Interval	10 s																																																								
Scanning Time	50 ms																																																								
Scheduled Radio Availability	<input type="radio"/> Always On <input checked="" type="radio"/> Custom Schedule																																																								
	<table border="1"> <thead> <tr> <th></th> <th>Midnight</th> <th>4am</th> <th>8am</th> <th>Noon</th> <th>4pm</th> <th>8pm</th> </tr> </thead> <tbody> <tr><td>Sunday</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr> <tr><td>Monday</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr> <tr><td>Tuesday</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr> <tr><td>Wednesday</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr> <tr><td>Thursday</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr> <tr><td>Friday</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr> <tr><td>Saturday</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr> </tbody> </table>		Midnight	4am	8am	Noon	4pm	8pm	Sunday	✓	✓	✓	✓	✓	✓	Monday	✓	✓	✓	✓	✓	✓	Tuesday	✓	✓	✓	✓	✓	✓	Wednesday	✓	✓	✓	✓	✓	✓	Thursday	✓	✓	✓	✓	✓	✓	Friday	✓	✓	✓	✓	✓	✓	Saturday	✓	✓	✓	✓	✓	✓
		Midnight	4am	8am	Noon	4pm	8pm																																																		
	Sunday	✓	✓	✓	✓	✓	✓																																																		
	Monday	✓	✓	✓	✓	✓	✓																																																		
	Tuesday	✓	✓	✓	✓	✓	✓																																																		
	Wednesday	✓	✓	✓	✓	✓	✓																																																		
	Thursday	✓	✓	✓	✓	✓	✓																																																		
Friday	✓	✓	✓	✓	✓	✓																																																			
Saturday	✓	✓	✓	✓	✓	✓																																																			
WMM	<input checked="" type="checkbox"/>																																																								

Advanced Features	
<b>Discover Nearby Networks</b>	Check this box to enable network discovery. Note that setting <b>Channel</b> to <b>Auto</b> will activate this feature automatically.
<b>Scanning Interval</b>	This setting controls the interval, in seconds, that your access point scans for nearby networks.

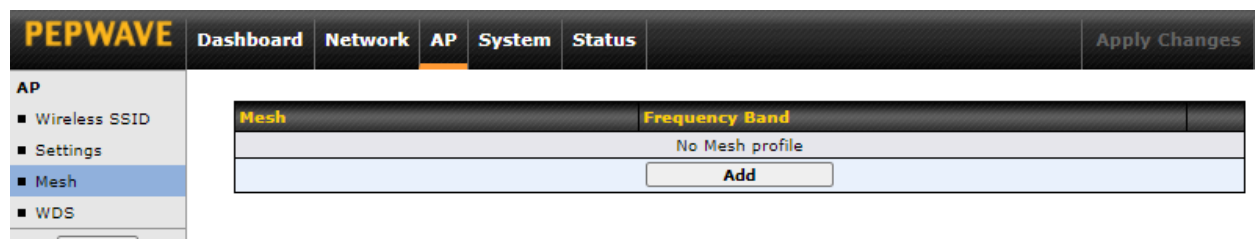


<b>Scanning Time</b>	This setting specifies the time, in milliseconds, that your access point scans any particular channel while searching for nearby networks.
<b>Scheduled Radio Availability</b>	Click <b>Custom Schedule</b> to specify radio availability schedule options or select <b>Always On</b> to make the radio continuously available.
<b>WMM</b>	This checkbox enables Wi-Fi Multimedia (WMM), also known as Wireless Multimedia Extensions (WME), on your access point. The default is <b>enabled</b> .

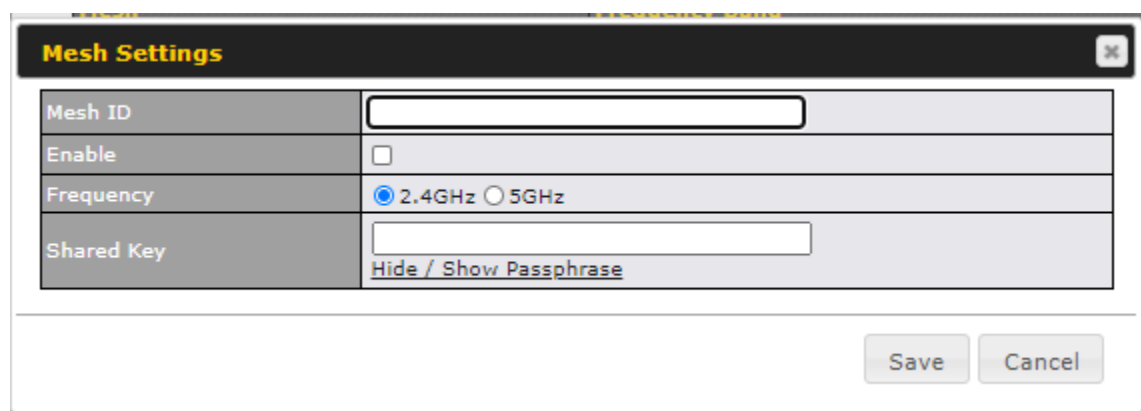
## 8.3 Mesh

Mesh support enables an access point (AP) to connect wirelessly to other wired mesh APs, providing redundancy in the event of AP failure. Mesh support is available for Wi-Fi networks 802.11ac (Wi-Fi 5) and above.

Please note that the AP's Mesh settings need to match the Mesh ID and Shared Key of the selected frequency band in order for the AP to join the network.



To create a new Wireless Mesh profile, go to **AP > Mesh**, and click **Add**.



The screenshot shows the 'Mesh Settings' dialog box. It contains the following fields and options:

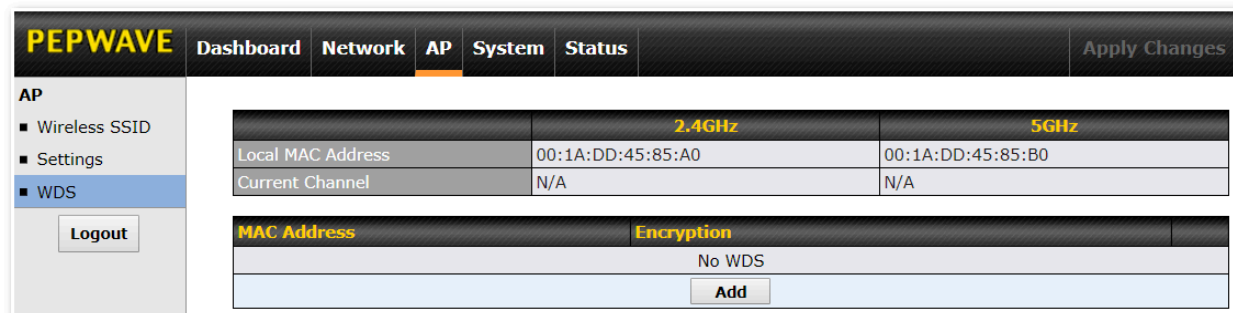
- Mesh ID**: A text input field.
- Enable**: A checkbox.
- Frequency**: Radio buttons for '2.4GHz' (selected) and '5GHz'.
- Shared Key**: A text input field with a 'Hide / Show Passphrase' link below it.
- Buttons**: 'Save' and 'Cancel' buttons at the bottom right.

Mesh Settings	
<b>Mesh ID</b>	Enter a name to represent the Mesh profile.

<b>Enable</b>	Check the box to enable the Mesh Profile.
<b>Frequency</b>	Select the 2.4GHz or 5GHz frequency to be used.
<b>Shared Key</b>	Enter the shared key in the text field. Please note that it needs to match the shared keys of the other APs in the Mesh. Click <b>Hide / Show Passphrase</b> to toggle visibility.

## 8.4 WDS

A wireless distribution system (WDS) provides a way to link access points together when wired or cabled connections are not feasible or desirable. A WDS can also extend wireless network coverage for wireless clients. Please note that your access point's channel setting should not be set to **Auto** when using WDS.



To create a new WDS, go to **AP > WDS**, and click **Add**.



WDS Settings	
<b>Enable</b>	Check this box to enable WDS.
<b>MAC Address</b>	Enter the MAC address of the access point with which to form a WDS link.

<b>Radio Selection</b>	Select the radio frequency (2.4GHz or 5GHz) for the WDS peer connection.
<b>Encryption</b>	Select <b>AES</b> to enable encryption for WDS peer connections. Selecting <b>None</b> disables encryption.

## 9 System Tab

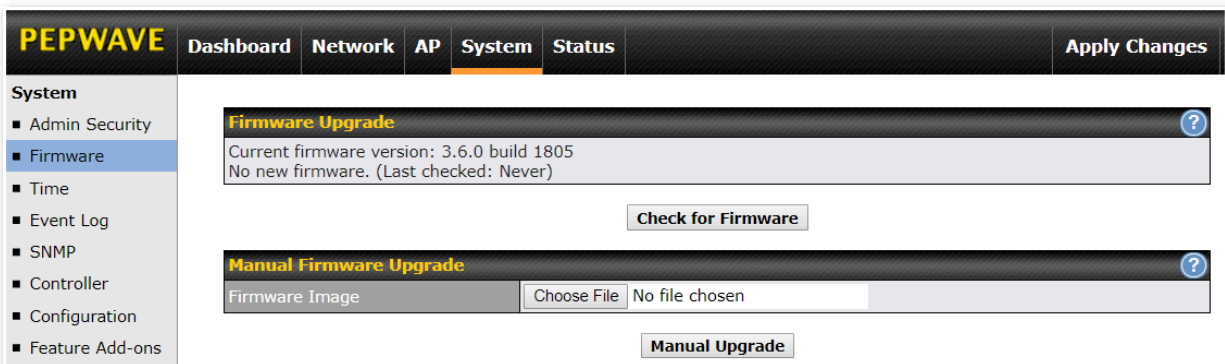
### 9.1 Admin Security

Admin Settings					
Device Name	AP-One-AC-Mini- <input type="text"/> hostname: ap-one-ac-mini- <input type="text"/>				
Location	<input type="text" value="site1"/>				
Admin User Name	<input type="text" value="admin"/>				
Admin Password	<input type="password"/>				
Confirm Admin Password	<input type="password"/>				
Web Session Timeout	<input type="text" value="4"/> Hours <input type="text" value="0"/> Minutes				
Security	HTTPS <input checked="" type="checkbox"/> HTTP to HTTPS Redirection				
Web Admin Port	<input type="text" value="443"/>				
Allowed Source IP Subnets	<input type="radio"/> Any <input checked="" type="radio"/> Allow access from the following IP subnets only				
	<table border="1"> <thead> <tr> <th>IP Address</th> <th>Subnet Mask</th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text" value="255.255.255.0 (/24)"/></td> </tr> </tbody> </table>	IP Address	Subnet Mask	<input type="text"/>	<input type="text" value="255.255.255.0 (/24)"/>
	IP Address	Subnet Mask			
<input type="text"/>	<input type="text" value="255.255.255.0 (/24)"/>				
<input type="button" value="+"/>					
Language	Auto Detect <input type="button" value="v"/>				

Admin Settings	
<b>Device Name</b>	This field allows you to define a name for this Peplink Balance unit. By default, <b>Device Name</b> is set as <b>Model_XXXX</b> , where <b>XXXX</b> refers to the last 4 digits of the serial number of that unit.
<b>Location</b>	This field allows you to add Location name
<b>Admin User Name</b>	<b>Admin User Name</b> is set as <b>admin</b> by default, but can be changed.
<b>Admin Password</b>	This field allows you to specify a new administrator password.
<b>Confirm Admin</b>	This field allows you to verify and confirm the new administrator password.

<b>Password</b>	
<b>Web Session Timeout</b>	<p>A web login session will be logged out automatically when it has been idle longer than the Web Session Timeout</p> <p>Unlimited session timeout: 0 hours 0 minutes</p> <p>Default: 4 hours 0 minutes</p>
<b>Security</b>	<p>This option is for specifying the protocol(s) through which the web admin interface can be accessed:</p> <ul style="list-style-type: none"> <li>• HTTP</li> <li>• HTTPS</li> </ul> <p>HTTP to HTTPS redirection is enabled by default to force HTTPS access to the web admin interface.</p>
<b>Web Admin Port</b>	This field is for specifying the port number on which the web admin interface can be accessed.
<b>Allowed Source IP Subnets</b>	This option is for specifying the IP subnets through which the web admin interface can be accessed.
<b>Language</b>	Set language of the Web Interface

## 9.2 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 Access Point will check online for new firmware. If new firmware is available, the Access Point automatically downloads 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 Access Point. It will then automatically initiate the firmware upgrade process.

Please note that all 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.

### Firmware Upgrade Status

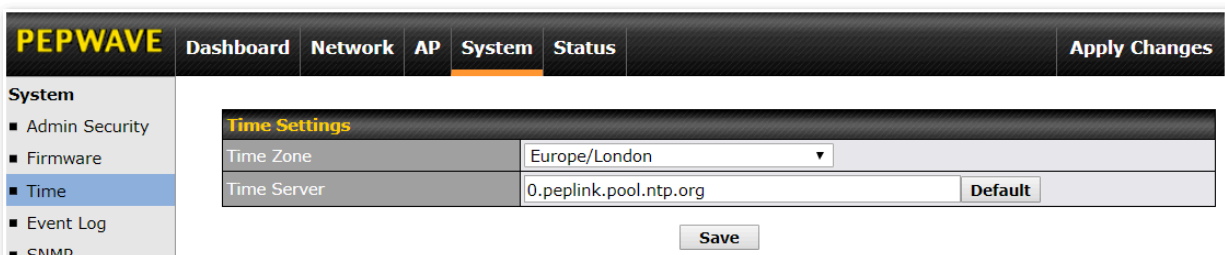
Status LED Information during firmware upgrade:

- OFF – Firmware upgrade in progress (DO NOT disconnect power.)
- **Red** – Unit is rebooting
- **Green** – Firmware upgrade successfully completed

### Important Note

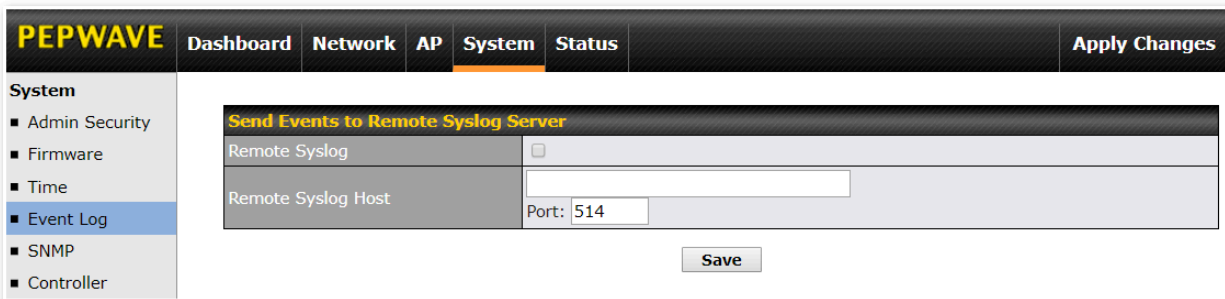
The firmware upgrade process may not necessarily preserve the previous configuration, and the behavior varies on a case-by-case basis. Consult the release notes for the particular firmware version before installing. Do not disconnect the power during the firmware upgrade process. Do not attempt to upload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

## 9.3 Time



The time server functionality enables the system clock of the Access Point to be synchronized with a specified time server. The settings for time server configuration are located at **System > Time**.

## 9.4 Event Log

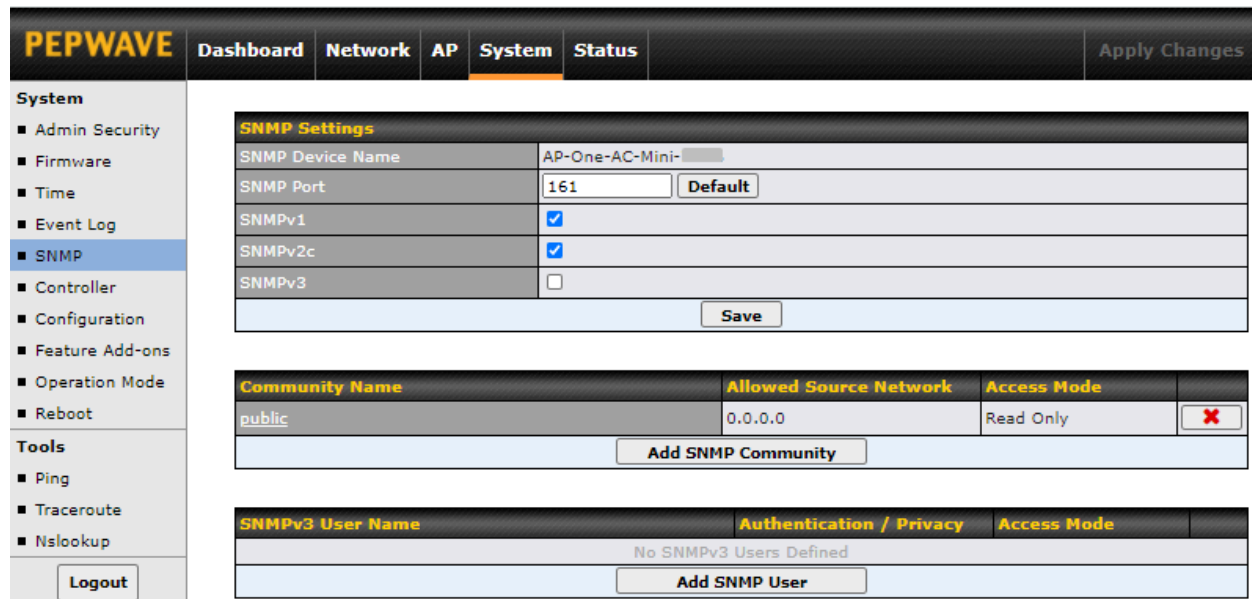


Event log functionality enables event logging at a specified remote syslog server. The settings for configuring the remote system log can be found at **System > Event Log**.

Remote Syslog Settings	
<b>Remote Syslog</b>	This setting specifies whether or not to log events at the specified remote syslog server.
<b>Remote Syslog Host</b>	This setting specifies the IP address or hostname of the remote syslog server. Port: Default 514

## 9.5 SNMP

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



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

Settings	
Enable	<input type="checkbox"/>
Community Name	<input type="text"/>
IP Address	<input type="text" value="0.0.0.0"/>
IP Mask	<input type="text" value="0.0.0.0 (/0)"/> ▼
Access Mode	<input type="text" value="Read Only"/> ▼

SNMP Community Settings	
<b>Enable</b>	Enable the SNMP community
<b>Community Name</b>	This setting specifies the SNMP community name.
<b>IP Address &amp; IP mask</b>	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.
<b>Access Mode</b>	Choose between <b>Read Only</b> and <b>Read and Write</b>

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

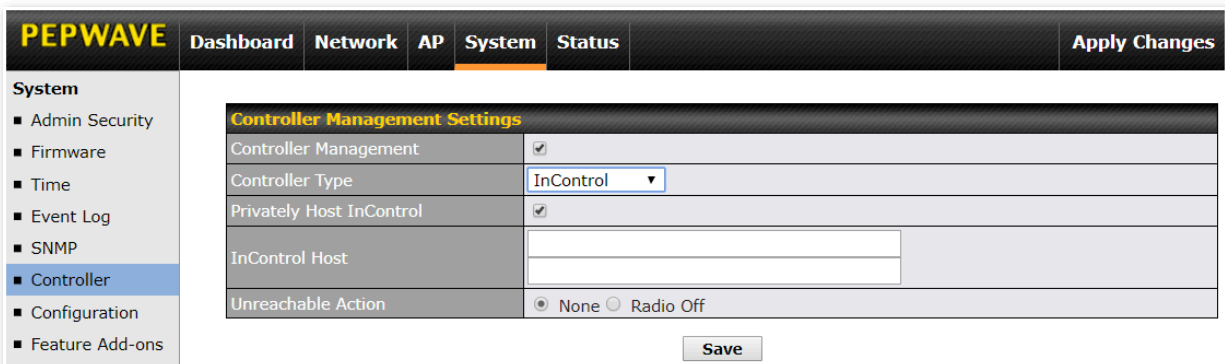
Settings	
Enable	<input type="checkbox"/>
SNMPv3 User Name	<input type="text"/>
Authentication Protocol	<input type="text" value="HMAC-MD5"/> ▼
Authentication Password	<input type="text"/>
Confirm Authentication Password	<input type="text"/>
Privacy Protocol	<input type="text" value="None"/> ▼
Access Mode	<input type="text" value="Read Only"/> ▼

SNMPv3 User Settings	
<b>Enable</b>	Enable the SNMPv3 user.
<b>SNMPv3 User Name</b>	This setting specifies a user name to be used in SNMPv3.
<b>Authentication Protocol</b>	This setting specifies via a drop-down menu one of the following valid authentication protocols: <ul style="list-style-type: none"> <li>• HMAC-MD5</li> <li>• HMAC-SHA</li> </ul>



<b>Authentication Password</b>	Password for SNMPv3 authentication.
<b>Confirm Authentication Password</b>	Confirm password for SNMPv3 authentication.
<b>Privacy Protocol</b>	<p>This setting specifies via a drop-down menu one of the following valid privacy protocols:</p> <ul style="list-style-type: none"> <li>• None</li> <li>• CBC-DES</li> <li>• CFB-AES</li> </ul> <p>When CBC-DES or CFB-AES is selected, an entry field will appear for the password.</p>
<b>Access Mode</b>	Choose between Read Only and Read and Write.

## 9.6 Controller



Option to choose the controller for the Access Point. The available options are:

Controller Management Settings	
<b>Controller Management</b>	Controller management is enabled when ticked, when unticked the Access Point is configured through the Web Admin GUI
<b>Controller Type</b>	<p>This setting specifies via a drop-down menu one of the following valid authentication protocols:</p> <ul style="list-style-type: none"> <li>• Auto - AP automatically assigned to active AP Controller</li> <li>• InControl - AP is controlled by InControl*</li> <li>• AP Controller - AP is controlled by Peplink Valance with AP controller feature</li> </ul>
<b>Privately Host InControl</b>	Privately host InControl Appliance. Check the box beside the “Privately Host InControl” and enter the IP Address or hostname of your InControl Appliance..

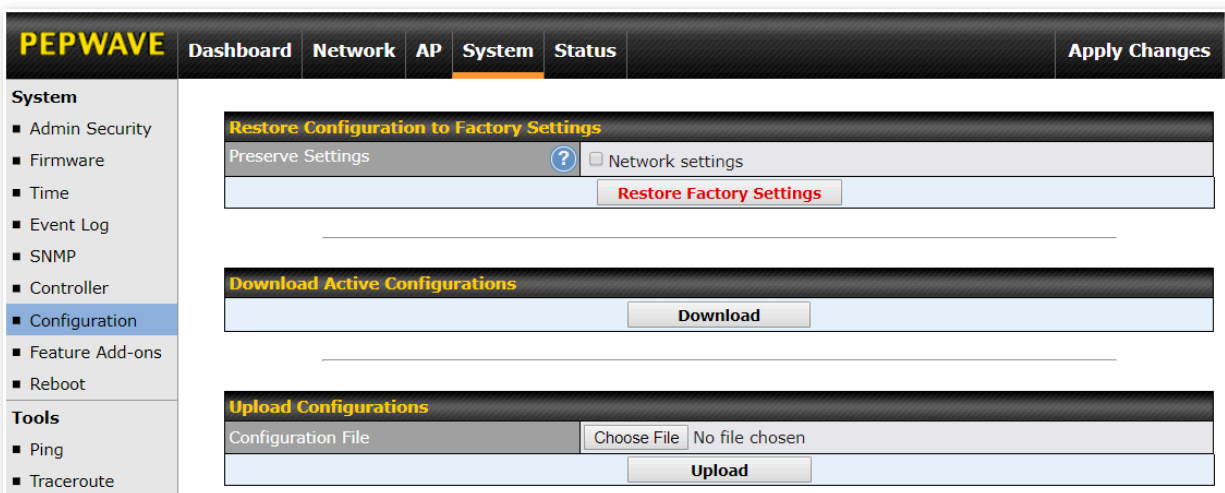
**Unreachable Action** Switch the AP “Radio off” or take no action when the AP is unreachable.

\*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.

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.

## 9.7 Configuration

Backing up your Pepwave Access Point settings immediately after successful completion of the initial setup is strongly recommended. The functionality to download and upload Pepwave Access Point settings is found at **System > Configuration**.



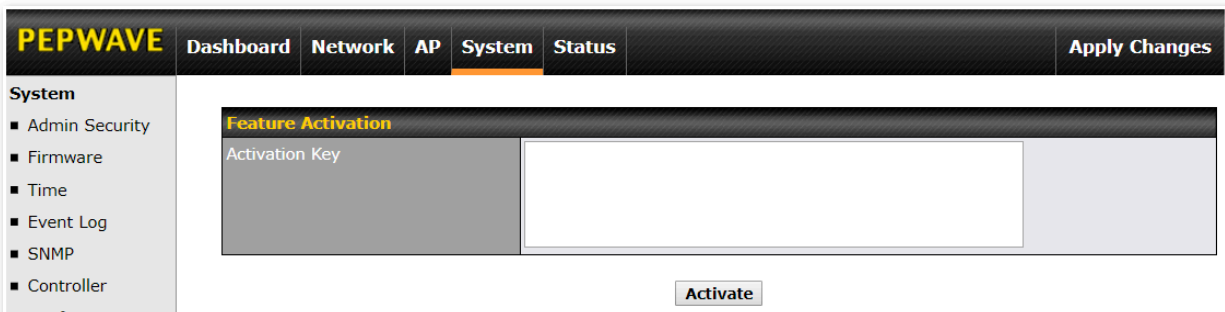
The screenshot shows the Pepwave web interface. The top navigation bar includes 'Dashboard', 'Network', 'AP', 'System' (selected), and 'Status'. On the left, a sidebar lists 'System' options: Admin Security, Firmware, Time, Event Log, SNMP, Controller, Configuration (highlighted), Feature Add-ons, and Reboot. Below this are 'Tools' options: Ping and Traceroute. The main content area has three sections: 'Restore Configuration to Factory Settings' with a 'Restore Factory Settings' button and a 'Network settings' checkbox; 'Download Active Configurations' with a 'Download' button; and 'Upload Configurations' with a 'Choose File' button and an 'Upload' button.

Configuration	
<b>Restore Configuration to Factory Settings</b>	<p>The <b>Restore Factory Settings</b> button is to reset the configuration to factory default settings. After clicking the button, you will need to click the <b>Apply Changes</b> button on the top right corner to make the settings effective.</p> <p>Tick the <b>Network Settings</b> option to include the I P Address, Subnet Mask, Default Gateway, DNS Server and Management VLAN ID</p>
<b>Download Active Configurations</b>	<p>Click <b>Download</b> to backup the current active settings.</p>

## Upload Configurations

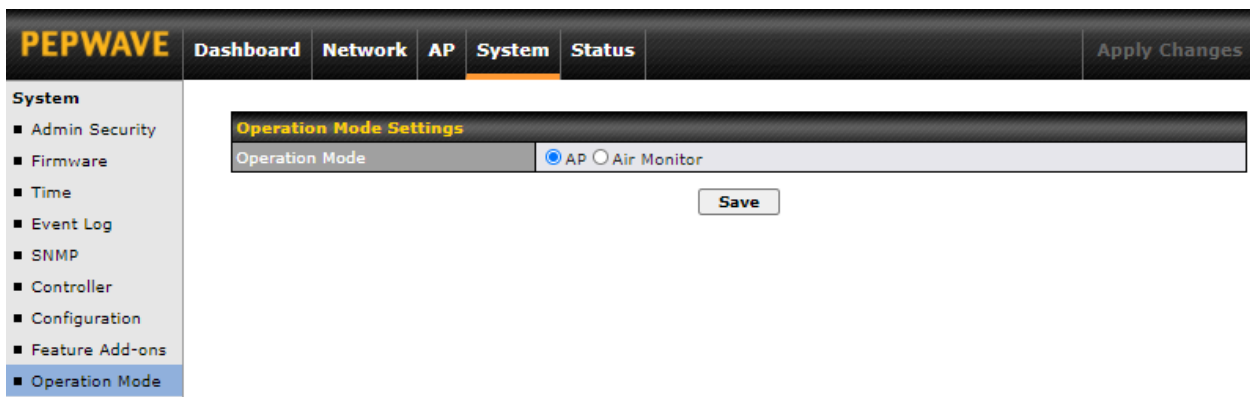
To restore or change settings based on a configuration file, click **Choose File** to locate the configuration file on the local computer, and then click **Upload**. The new settings can then be applied by clicking the **Apply Changes** button on the page header, or you can cancel the procedure by pressing **discard** on the main page of the web admin interface.

## 9.8 Feature Add-Ons



Some Pepwave Access Points models 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, and then click Apply Changes.

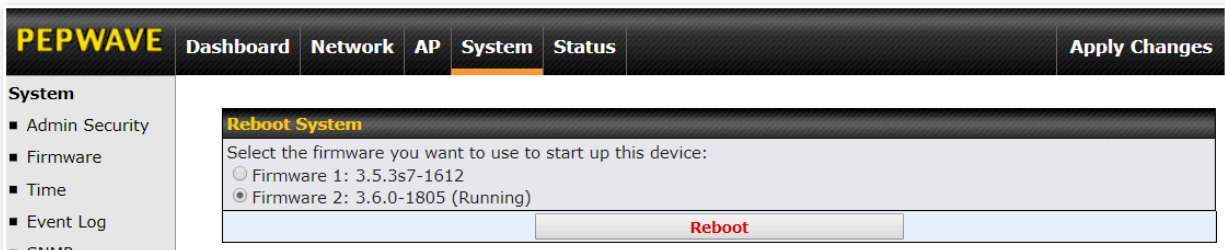
## 9.9 Operating Mode



Operating Mode allows you to select your desired mode of operation between either AP mode or Air Monitor. The settings for Operation Mode are located at **System > Operation Mode**.

- AP mode: The AP device works as an AP and will broadcast an SSID.
- Air Monitor: The AP device works in Air Monitor mode without SSID broadcasting. Air Monitor reports can only be viewed in InControl2.

## 9.10 Reboot

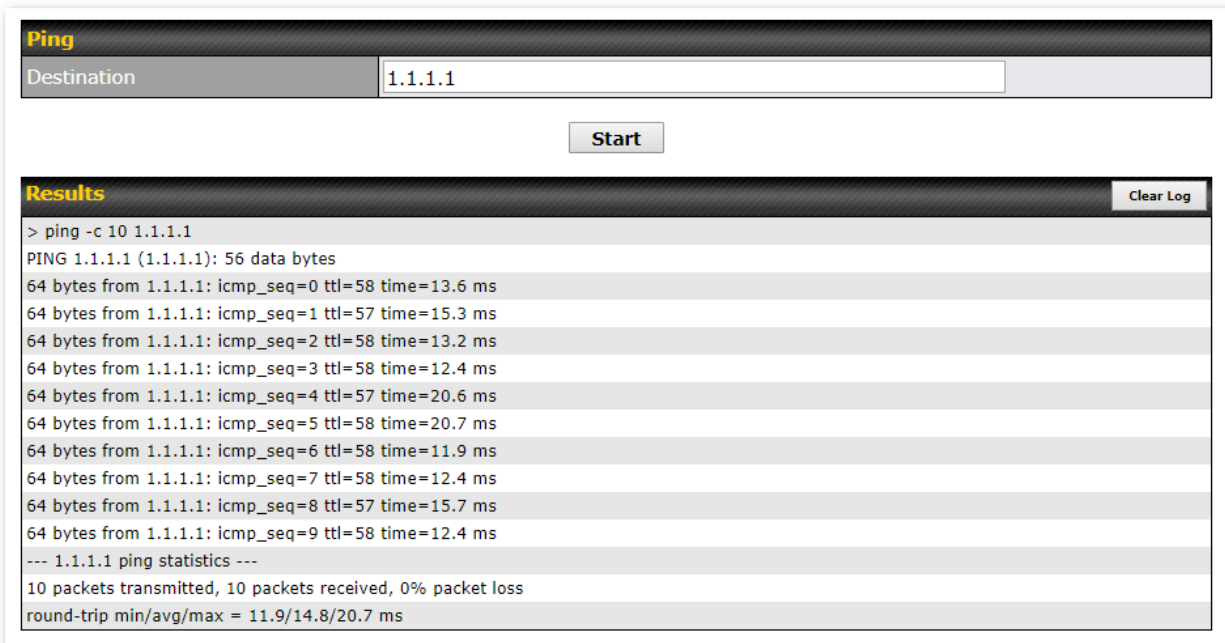


Restart the access point with the **Reboot** button. For maximum reliability, the Pepwave Access Point can contain two copies of firmware; each copy can be a different version. You can select the firmware version you would like to reboot the device with. The firmware marked with **(Running)** is the current system boot up firmware.

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

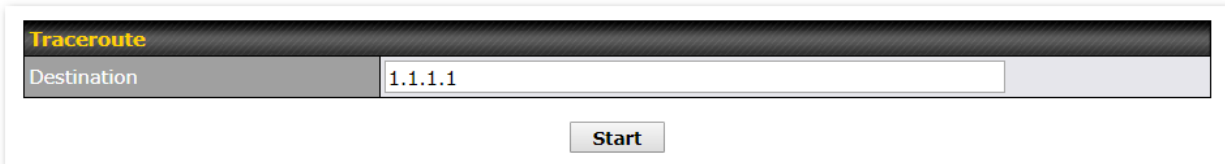
## 9.11 Tools

### 9.11.1 PING



The ping test tool tests connectivity pinging the specified destination IP address. The ping utility is located at **System > Tools > Ping**.

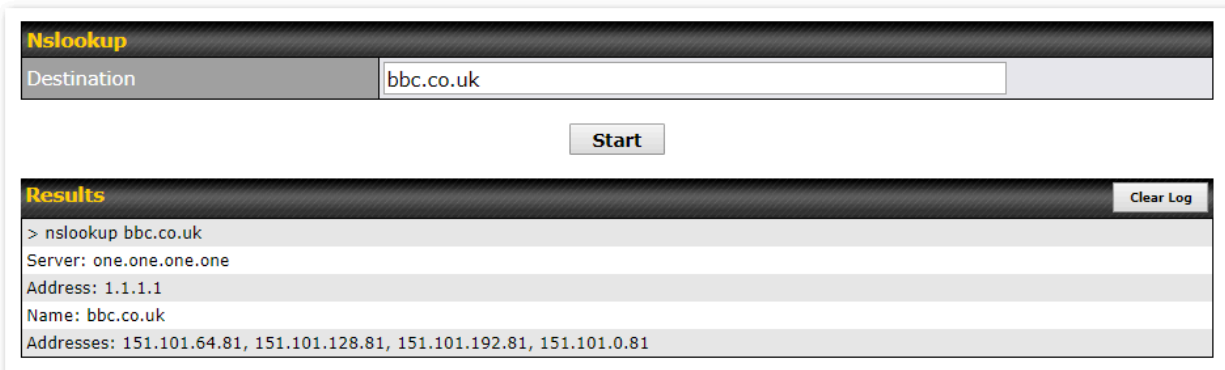
## 9.11.2 Traceroute



The Traceroute utility interface features a title bar labeled "Traceroute". Below it is a "Destination" label followed by a text input field containing "1.1.1.1". At the bottom center is a "Start" button.

The traceroute test tool traces the routing path to the specified IP address. The traceroute test utility is located at **System > Tools > Traceroute**.

## 9.11.3 Nslookup



The Nslookup utility interface has a title bar labeled "Nslookup". It includes a "Destination" label and a text input field with "bbc.co.uk". A "Start" button is positioned below the input field. A "Results" section at the bottom contains a "Clear Log" button and a text area displaying the following output:

```
> nslookup bbc.co.uk
Server: one.one.one.one
Address: 1.1.1.1
Name: bbc.co.uk
Addresses: 151.101.64.81, 151.101.128.81, 151.101.192.81, 151.101.0.81
```

The nslookup tool is used to test DNS name servers. The nslookup utility can be found at **System > Tools > Nslookup**.

## 10 Status Tab

The displays available on the **Status** tab help you monitor device data, client activity, rogue device access, and more.

### 10.1 Device

**PEPWAVE**
Dashboard
Network
AP
System
**Status**
Apply Changes

**Status**

- Device
- Client List
- Mesh / WDS Info
- Portal
- Rogue AP
- Event Log

Logout

System Information

Device Name	AP_
Model	AP
Product Code	
Hardware Revision	2
Location	site1
Serial Number	
Firmware	3.6.3 build 1952
Host Name	ap-one-4e0b
Uptime	0 day 0 hour 13 minutes
System Time	Fri Aug 6 16:58:06 SGT 2021
Diagnostic Report	<a href="#">Download</a>

Interface

MAC Address

WAN	
Radio 2.4GHz	
Radio 5GHz	

System Information	
<b>Device Name</b>	This is the name specified in the <b>Device Name</b> field located at <b>System &gt; Admin Security</b> .
<b>Model</b>	This shows the model name and number of this device.
<b>Product Code</b>	This shows the product name of this device.
<b>Hardware Revision</b>	This shows the hardware version of this device.
<b>Location</b>	This is the location name specified in the <b>Location</b> field located at <b>System &gt; Admin Security</b> .
<b>Serial Number</b>	This shows the serial number of this device.
<b>Firmware</b>	This shows the firmware version this device is currently running.
<b>Host name</b>	This shows the hostname of the device.

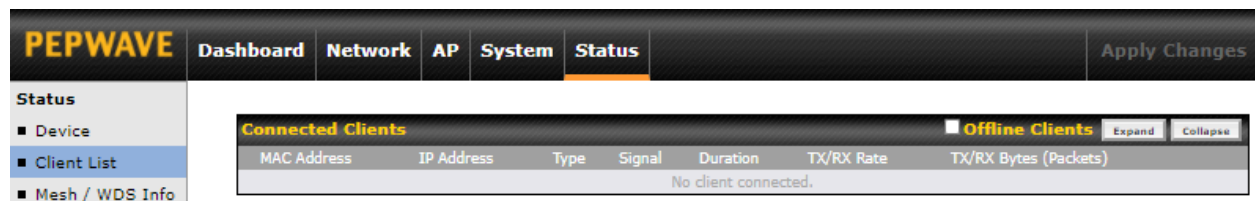
<b>Uptime</b>	This shows the length of time since the device has been rebooted.
<b>System Time</b>	This shows the current system time.
<b>Diagnostic Report</b>	The <b>Download</b> link is for exporting a diagnostic report file required for system investigation.
<b>Remote Assistance</b>	Click <b>Turn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

The second table shows the MAC address of each LAN/WAN interface connected.

**Important Note**

If you encounter issues and would like to contact the Peplink Support Team (<https://contact.peplink.com/secure/create-support-ticket.html>), please download the diagnostic report file and attach it along with a description of your issue.

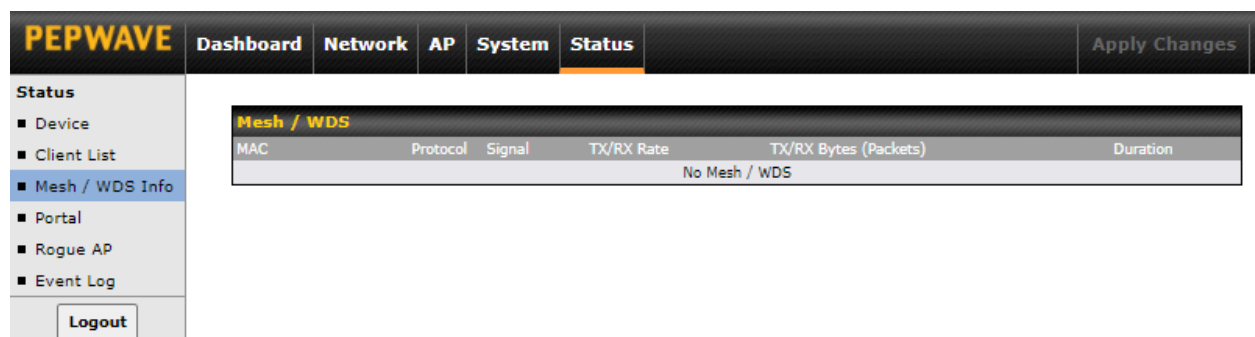
## 10.2 Client List



The screenshot shows the PEPWAVE web interface with the 'Status' tab selected. On the left, a sidebar menu has 'Client List' highlighted. The main content area displays a table titled 'Connected Clients' with columns: MAC Address, IP Address, Type, Signal, Duration, TX/RX Rate, and TX/RX Bytes (Packets). Below the table, it states 'No client connected.' To the right of the table are buttons for 'Offline Clients', 'Expand', and 'Collapse'.

The **Client List** displays all currently connected clients. Use the **Expand** and **Collapse** buttons to control the amount of data displayed.

## 10.3 Mesh / WDS Info

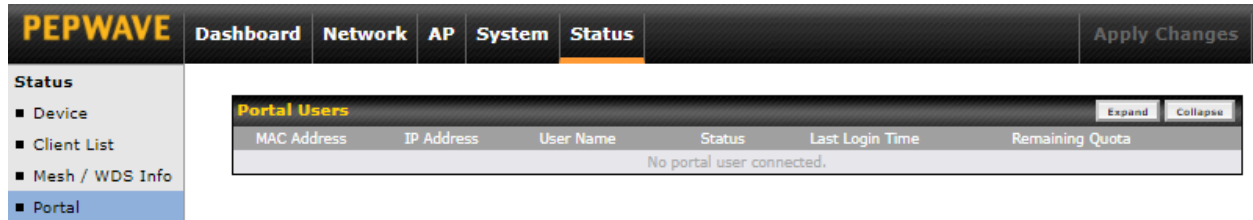


The screenshot shows the PEPWAVE web interface with the 'Status' tab selected. On the left, a sidebar menu has 'Mesh / WDS Info' highlighted. The main content area displays a table titled 'Mesh / WDS' with columns: MAC, Protocol, Signal, TX/RX Rate, TX/RX Bytes (Packets), and Duration. Below the table, it states 'No Mesh / WDS'. At the bottom of the sidebar, there is a 'Logout' button.

Here you can monitor the status of your Mesh or wireless distribution system (WDS) and track

activity by MAC address. This will display information for both the 2.4GHz and 5GHz radios.

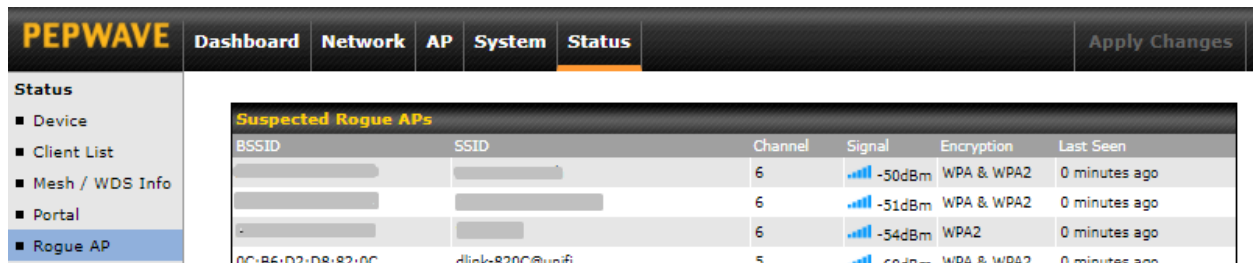
## 10.4 Portal



The screenshot shows the PEPWAVE web interface with the 'Status' tab selected. In the left sidebar, 'Portal' is highlighted under the 'Status' section. The main content area displays 'Portal Users' with a table header: MAC Address, IP Address, User Name, Status, Last Login Time, and Remaining Quota. Below the header, it states 'No portal user connected.' There are 'Expand' and 'Collapse' buttons in the top right of the table area.

If you've turned on your access point's captive portal, client connection data will appear here. Use the **Expand** and **Collapse** buttons to control the amount of data displayed.

## 10.5 Rogue AP



The screenshot shows the PEPWAVE web interface with the 'Status' tab selected. In the left sidebar, 'Rogue AP' is highlighted under the 'Status' section. The main content area displays 'Suspected Rogue APs' with a table header: BSSID, SSID, Channel, Signal, Encryption, and Last Seen. The table lists three suspected rogue access points.

BSSID	SSID	Channel	Signal	Encryption	Last Seen
0C:86:D7:D8:82:0C	dlink-R7000@unifi	6	-50dBm	WPA & WPA2	0 minutes ago
		6	-51dBm	WPA & WPA2	0 minutes ago
		6	-54dBm	WPA2	0 minutes ago

This section displays a list of nearby suspected rogue access points.



## 10.6 Event Log

The screenshot shows the PEPWAVE web interface. The top navigation bar includes 'Dashboard', 'Network', 'AP', 'System', and 'Status' (which is active). A 'Logout' button is in the left sidebar. The 'Status' section on the left lists 'Device', 'Client List', 'Mesh / WDS Info', 'Portal', 'Rogue AP', and 'Event Log' (selected). The main content area is titled 'Device Event Log' and features an 'Auto Refresh' checkbox (checked). It displays a list of events with timestamps and descriptions, such as 'System: Changes applied' and 'System: Time synchronization successful'. A 'Clear Log' button is located at the bottom of the log list.

Timestamp	Event Description
Dec 24 16:20:07	
Dec 24 16:20:02	System: Changes applied
Dec 24 16:15:09	
Dec 24 16:15:08	System: Changes applied
Dec 24 16:12:18	
Dec 24 16:12:17	System: Changes applied
Dec 24 16:11:41	
Dec 24 15:58:52	
Dec 24 15:58:51	System: Changes applied
Dec 24 15:37:04	System: Time synchronization successful
Dec 24 15:36:10	System: Time synchronization successful (InControl)
Jan 01 08:00:55	System: Started up (3.6.2 build 1938)
Dec 24 09:11:01	System: Changes applied
Dec 24 01:10:25	System: InControl has updated the configuration as changes were made on device's side and InControl configuration updated
Dec 23 09:45:40	System: Changes applied
Dec 23 09:07:50	System: Time synchronization successful
Jan 01 00:00:53	System: Started up (3.6.2 build 1938)
Dec 07 04:15:16	System: Time synchronization successful
Dec 07 04:15:16	System: Time synchronization successful (InControl)
Jan 01 00:00:48	System: Started up (3.6.1 build 1889)

The **Event Log** displays a list of all events associated with your access point. Check **Auto Refresh** to refresh log entries automatically. Click the **Clear Log** button to clear the log.

## 11 Restoring Factory Defaults

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

1. Locate the reset button on the front or back panel of the Pepwave AP One router.
2. With a paperclip, press and keep the reset button pressed.

Note: There is a dual function to the reset button.

Hold for 5 seconds for admin password reset (Note: The LED status light blinks in RED 2 times and release the button, green status light starts blinking)

Hold for 5 seconds for factory reset (Note: The LED status light blinks in RED 3 times and release the button, all WAN/LAN port lights start blinking)

After the Pepwave AP One 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.

## 12 Appendix

### Ethernet Cables

We recommend that you use a shielded cable to connect the Ethernet ports for the network.

### Federal Communication Commission Interference Statement ( AP One Rugged )

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.

-Consult the dealer or an experienced radio/TV technician for help.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

### **Radiation Exposure Statement**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

### **Industry Canada Statement ( AP One Rugged )**

This product meets the applicable Innovation, Science and Economic Development Canada technical specifications.

Le présent produit est conforme aux spécifications techniques applicables d'Innovation, Sciences et Développement économique Canada.

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions:

- (1) This device may not cause interference.
- (2) This device must accept any interference, including interference that may cause undesired operation of the device.

Le present appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisee aux deux conditions suivantes:

- (1) l'appareil ne doit pas produire de brouillage, et
- (2) l'utilisateur de l'appareil doit accepter tout brouillage radioelectrique subi, meme si le brouillage est susceptible d'en

(i) The device for operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;

(ii) For devices with detachable antenna(s), the maximum antenna gain permitted for devices in

the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits specified for point-to-point and non-point-to-point operation as appropriate; and

The high-power radars are allocated as primary users (i.e. priority users) of the band 5725-5850 MHz and that these radars could cause interference and/or damage to LE- LAN devices.

(i) Le dispositif fonctionnant dans la bande 5150-5250 MHz est réservé uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;

(ii) Le gain maximal d'antenne permis pour les dispositifs avec antenne(s) amovible(s) utilisant la bande 5725-5850 MHz doit se conformer à la limitation P.I.R.E spécifiée pour l'exploitation point à point et non point à point, selon le cas.

En outre, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour la bande 5725-5850 MHz et que ces radars pourraient causer du brouillage et/ ou des dommages aux dispositifs LAN-EL.

## **Radiation Exposure Statement**


This device complies with the ISED radiation exposure limit set forth for an uncontrolled environment. This device should be installed and operated with minimum distance 20cm between the radiator & your body.

Get équipement est conforme avec l'exposition aux radiations ISED définies pour un environnement non contrôlé. Get équipement doit être installé et utilisé à une distance minimum de 20 cm entre le radiateur et votre corps.

## CE Statement for Pepwave Routers ( AP One Rugged )

# DECLARATION OF CONFORMITY

We affirm the electrical equipment manufactured by us fulfils the requirements of the Radio Equipment Directive 2014/53/EU.

Name of manufacturer	Pismo Labs Technology Limited
Contact information of the manufacturer	Unit A5, 5/F, HK Spinners Ind. Bldg., Phase 6, 481 Castle Peak Road, Cheung Sha Wan, Kowloon, Hong Kong tel. (852) 2990 7600, fax. (852) 3007 0588 e-mail: cs@peplink.com
Description of the appliance	Pepwave / Peplink / Pismo Wireless Product
Model name of the appliance	AP One Rugged, Device Connector, Device Connector Rugged
Trade name of the appliance	 <b>PEPWAVE</b>

The construction of the appliance is in accordance with the following standards:

EN 300 328 V2.1.1  
EN 301 893 V2.1.1  
EN 300 440 V2.1.1  
EN 301 489-1 V2.1.1  
EN 301 489-3 V2.1.1  
EN 301 489-17 V3.1.1  
EN 55032:2015  
EN 61000-3-2:2014  
EN 61000-3-3:2013  
EN 55024:2010+A1: 2015  
EN 50385:2002  
EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013

Yours sincerely,



Antony Chong  
Director of Hardware Engineering  
Peplink Pte. Limited

	AT	BE	BG	HR	CY	CZ	DK	EE	FI	FR	DE	EL	HU	IE
	IT	LV	LT	LU	MT	NL	PL	PT	RO	SK	SI	ES	SE	UK(NI)

**2.4GHz ( 2412 - 2472 MHz ) : 16.20 dBm**

**5GHz ( 5150 - 5250 MHz ) : 19.18 dBm**

**5GHz ( 5725 - 5850 MHz ) : 13.84 dBm**

This equipment complies with CE radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator & your body.

This equipment is restricted to indoor use only when operating in the 5150 to 5250 MHz frequency range in above countries.

**contact as: <https://www.peplink.com/>**