PEPWAVE

Broadband Possibilities

User Manual

Pepwave AP One Series:

AP One Enterprise / AP One AC mini / AP One Rugged / AP One Flex / AP Pro AC

October 2018

Table of Contents

Introduction and Scope 5

Product Features and Benefits 6

Package Contents 7

AP One Enterprise (APO-ENT) 7

AP One AC mini (APO-AC-MINI) 7

AP One Rugged (APO-RUG) 7

AP One Flex (APO-FLX) 7

AP Pro AC (APP-AGN3) 7

Hardware Overview 8

AP One Enterprise 8

AP One AC mini 9

AP One Rugged 10

AP One Flex 11

AP Pro AC 12

Installation 13

Installation Procedures 13

Dashboard 15

General 16

AP 17

Network 19

WAN 19

LAN 21

Interfaces > Ethernet Port 24

PepVPN 24

AP 27

Wireless SSID 27

Settings 38
WDS 41
System Tab 43
Admin Security 43
Firmware 44
Time 45
Event Log 46
SNMP 46
Controller 49
Configuration 50
Feature Add-Ons 52
Reboot 52
Tools > Ping 53
Tools > Traceroute 53
Tools > Nslookup 54
Status 54
Device 55
Client List 56
WDS Info 56
Portal 57
Rogue AP 57
Event Log 58
Restoring Factory Defaults 58
Appendix 59
Datasheets 60

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, 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.

This manual includes Pepwave AP models supporting firmware 3.6.0.
Other Pepwave AP models are described in the Pepwave ap v3.5.4 user manual.

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.
- 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.

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

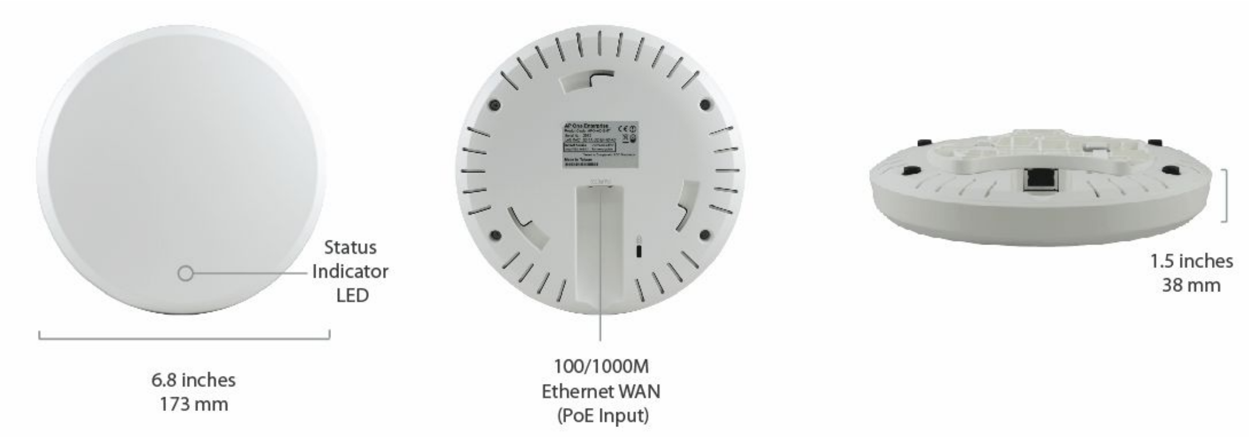
AP Pro AC (APP-AGN3)

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

4 Hardware Overview

4.1 AP One Enterprise

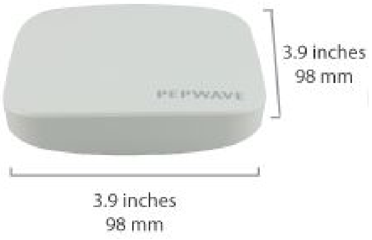
Bottom View **Top View** **Front View**



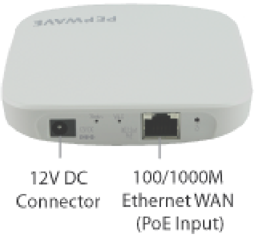
LED Indicators	
Status	RED – Access point initializing GREEN – Access point ready
LAN 1	OFF – No device connected to Ethernet port BLINKING – Ethernet port sending/receiving data ON – Powered-on device connected to Ethernet port Note that LAN 5 displays the status of the uplink connection

4.2 AP One AC mini

Front View



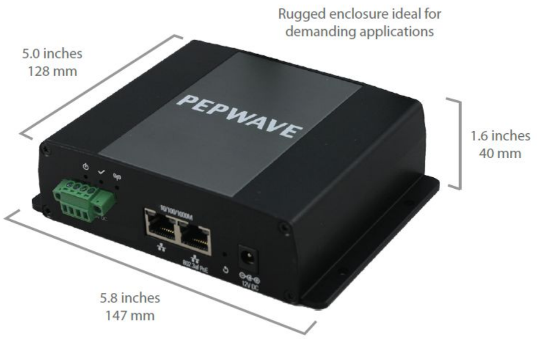
Rear Panel View



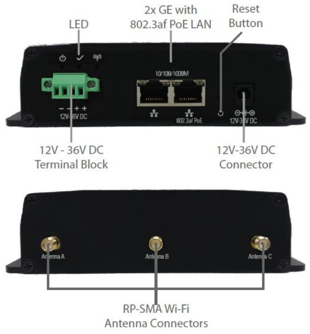
LED Indicators	
Status	RED – Access point initializing GREEN – Access point ready
Wi-Fi	OFF – 2.4/5GHz Wi-Fi radio off BLINKING – AP sending/receiving data GREEN – 2.4/5GHz Wi-Fi radio on Note that this model includes a 2.4GHz Wi-Fi radio and a 5GHz Wi-Fi radio that can operate simultaneously to increase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

4.3 AP One Rugged

Front View



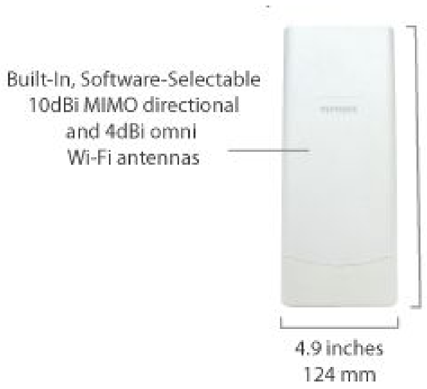
Rear Panel View


LED
2x GE with 802.3af PoE LAN
Reset Button
12V - 36V DC Terminal Block
12V-36V DC Connector
Antenna A
Antenna B
Antenna C
RP-SMA Wi-Fi Antenna Connectors

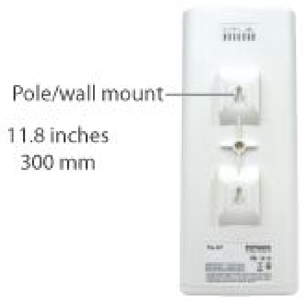
LED Indicators	
Power	On – Power On OFF – Power Off
Status	RED – Access point initializing GREEN – Access point ready
Wireless	OFF – 2.4/5GHz Wi-Fi radio off BLINKING – AP sending/receiving data GREEN – 2.4/5GHz Wi-Fi radio on Note that this model can operate in either 2.4GHz or 5GHz mode, depending on Wi-Fi radio settings.

4.4 AP One Flex

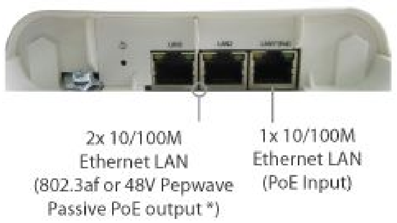
Front View



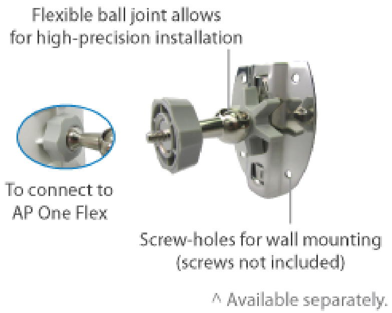
Rear Panel View



Connector Panel (Inside the Lid)



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


Flexible ball joint allows
for high-precision installation
To connect to
AP One Flex
Screw-holes for wall mounting
(screws not included)

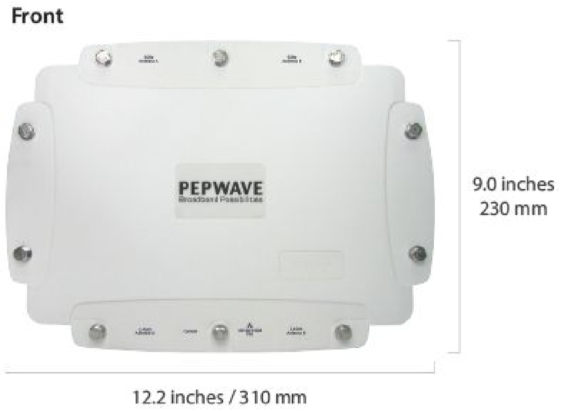
^ Available separately.

LED Indicators	
Status	RED – Access point initializing GREEN – Access point ready
LAN	OFF – No device connected to Ethernet port BLINKING – Ethernet port sending/receiving data ON – Powered-on device connected to Ethernet port
📶	Number of connected clients (1-10, 11-20, 21-30, 31-40)

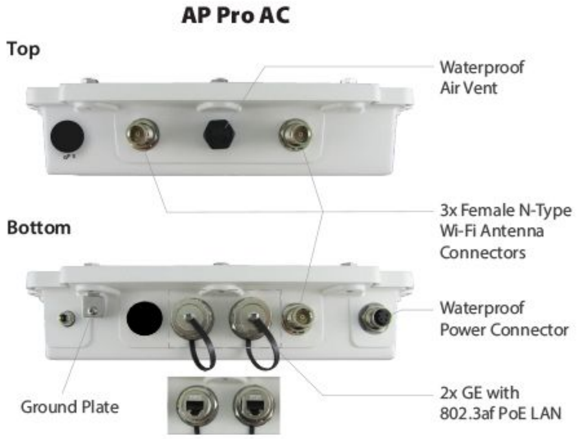
Copyright & Trademarks

4.5 AP Pro AC

Front View

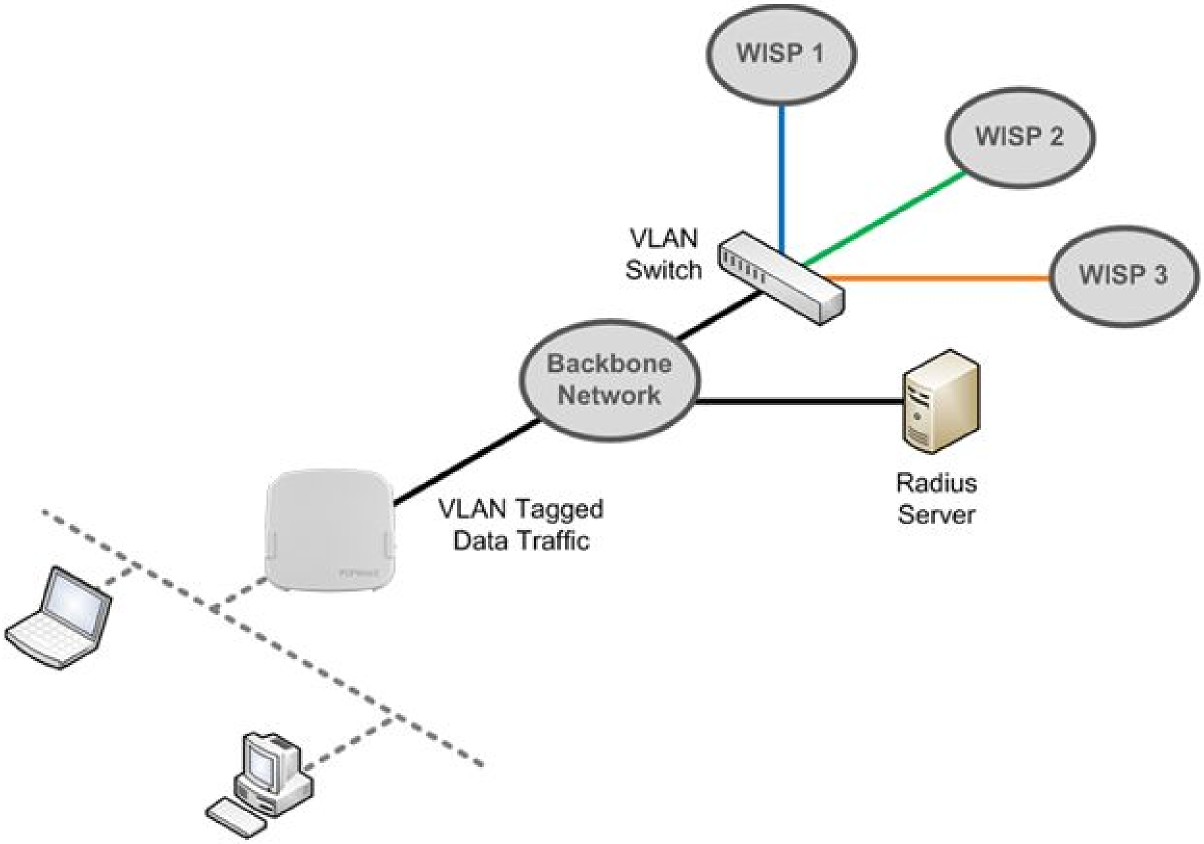


Top/Bottom View



5 Installation

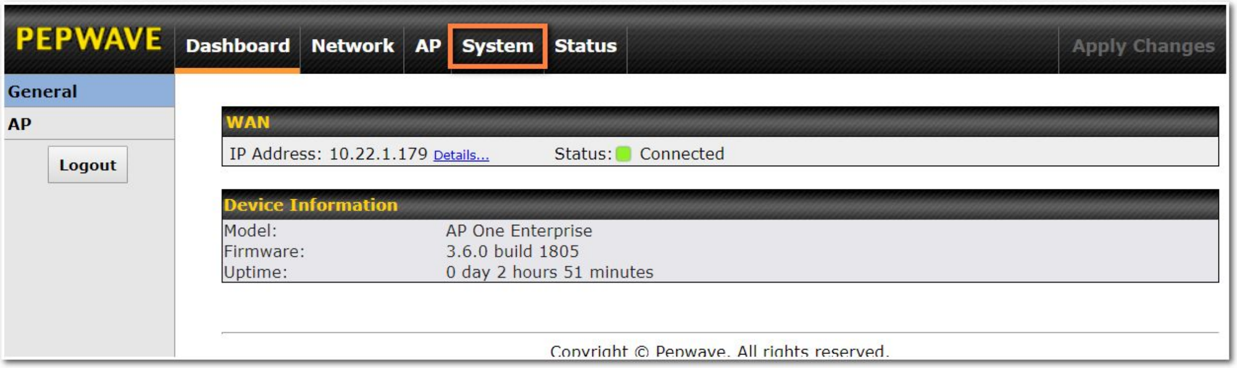
Your access point acts as a bridge between wireless and wired Ethernet interfaces.
A typical setup follows:



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. Connect the power adapter to the power connector of the unit. Plug the power adapter into a power source.

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.



WAN

IP Address: 10.22.1.179 Details... Status: 🟩 Connected

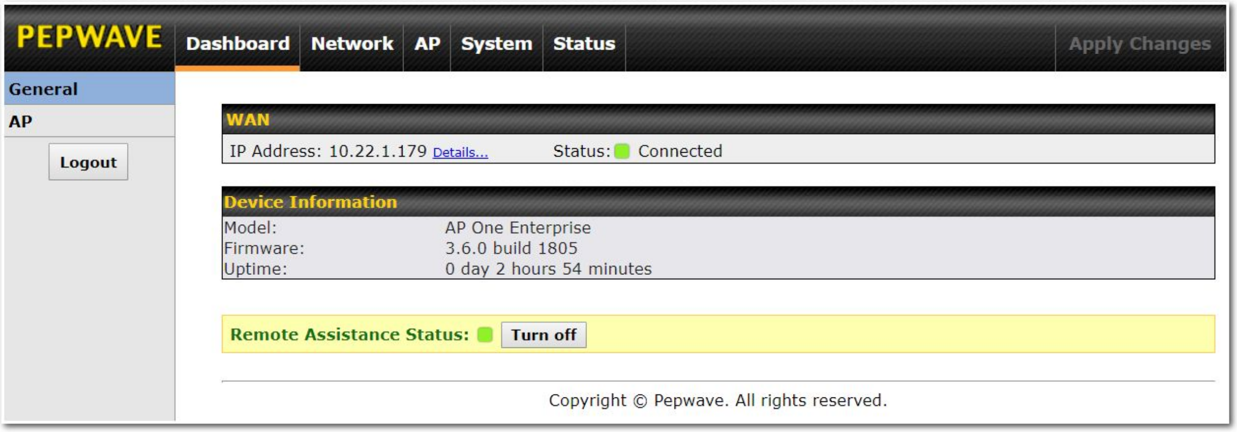
Device Information

Model:	AP One Enterprise
Firmware:	3.6.0 build 1805
Uptime:	0 day 2 hours 51 minutes

Copyright © Pepwave. All rights reserved.

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.



WAN

IP Address: 10.22.1.179 Details... Status: 🟩 Connected

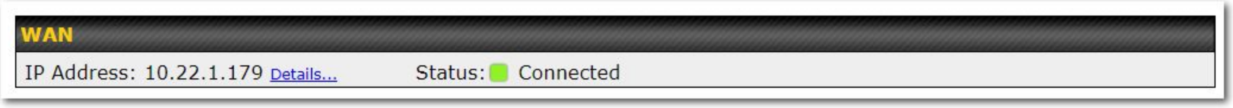
Device Information

Model:	AP One Enterprise
Firmware:	3.6.0 build 1805
Uptime:	0 day 2 hours 54 minutes

Remote Assistance Status: 🟩 Turn off

Copyright © Pepwave. All rights reserved.

6.1 General

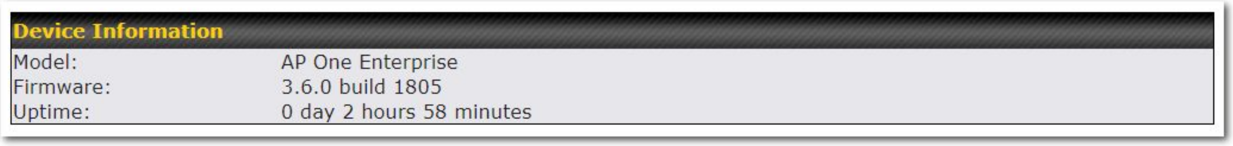


WAN

IP Address: 10.22.1.179 Details... Status: 🟩 Connected

This section contains WAN status and general device information.

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



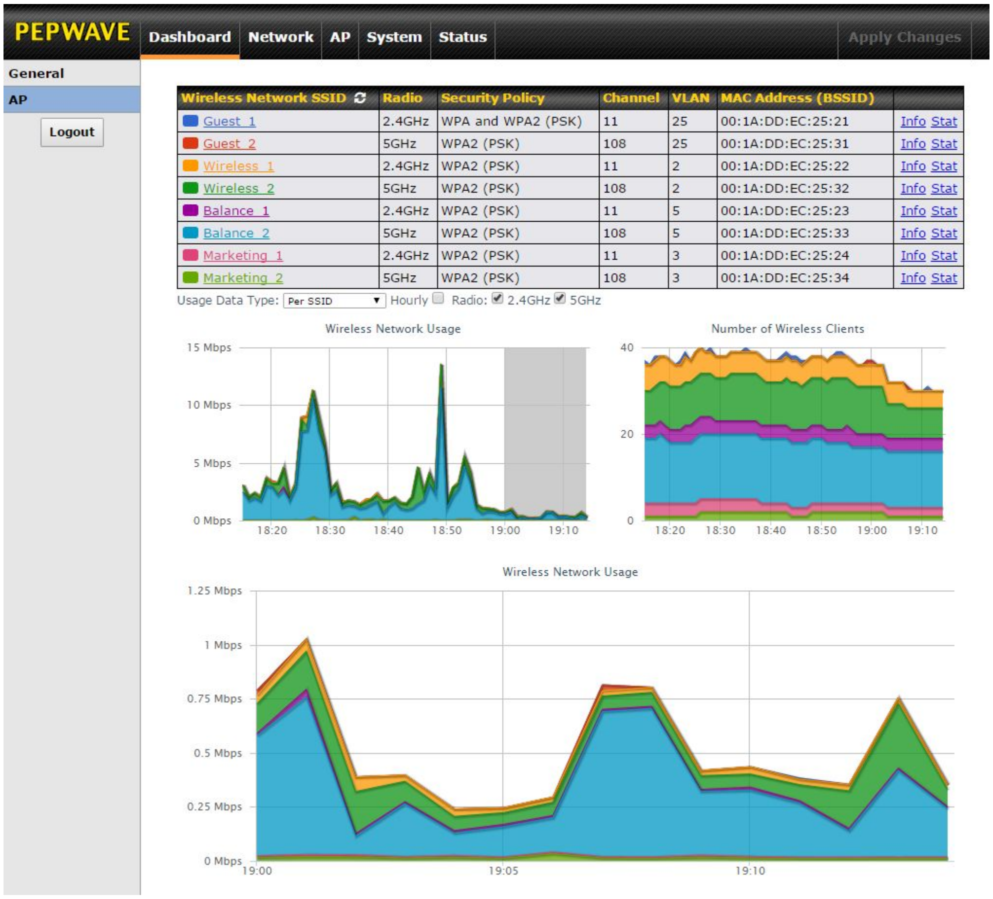
Device Information

Model:	AP One Enterprise
Firmware:	3.6.0 build 1805
Uptime:	0 day 2 hours 58 minutes

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

6.2 AP

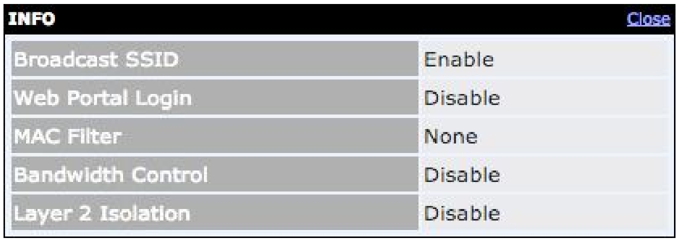
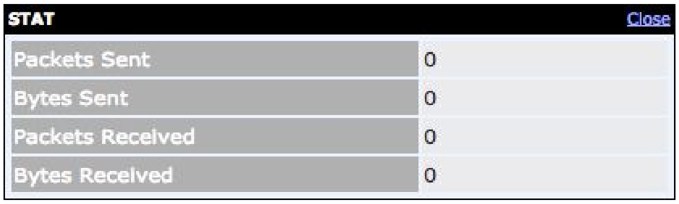
This section displays a variety of information about your wireless network.



Wireless Network SSID	Radio	Security Policy	Channel	VLAN	MAC Address (BSSID)	
🟦 Guest_1	2.4GHz	WPA and WPA2 (PSK)	11	25	00:1A:DD:EC:25:21	Info Stat
🟥 Guest_2	5GHz	WPA2 (PSK)	108	25	00:1A:DD:EC:25:31	Info Stat
🟧 Wireless_1	2.4GHz	WPA2 (PSK)	11	2	00:1A:DD:EC:25:22	Info Stat
🟩 Wireless_2	5GHz	WPA2 (PSK)	108	2	00:1A:DD:EC:25:32	Info Stat
🟪 Balance_1	2.4GHz	WPA2 (PSK)	11	5	00:1A:DD:EC:25:23	Info Stat
🟦 Balance_2	5GHz	WPA2 (PSK)	108	5	00:1A:DD:EC:25:33	Info Stat
🟥 Marketing_1	2.4GHz	WPA2 (PSK)	11	3	00:1A:DD:EC:25:24	Info Stat
🟩 Marketing_2	5GHz	WPA2 (PSK)	108	3	00:1A:DD:EC:25:34	Info Stat

Usage Data Type: Per SSID ▾ Hourly □ Radio: ☑ 2.4GHz ☑ 5GHz

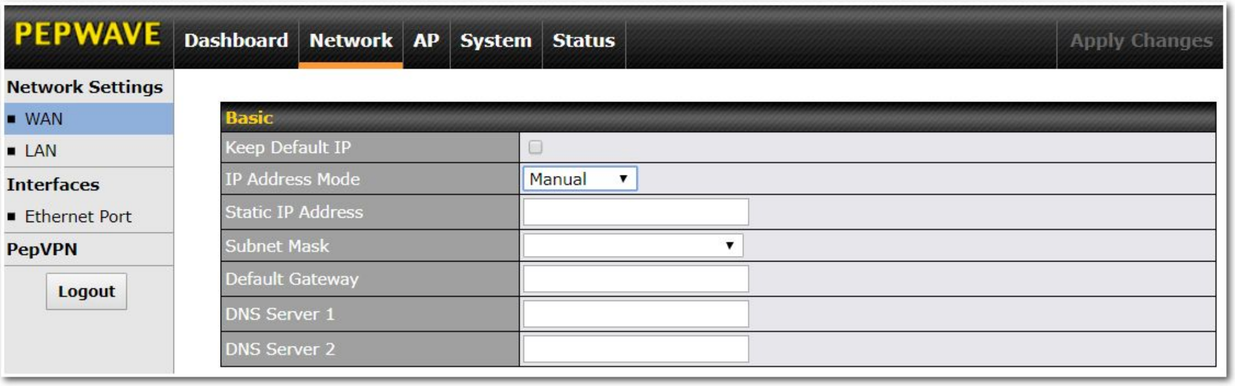
AP Status	
Wireless Network SSID	This field displays your access point's SSID.
Radio	The radio frequency currently used by your access point appears here. If you're using the AP One AC mini or the AP One In-Wall and have configured both radios, this displays both radios in use.
Security Policy	This field 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.
Channel	The channel currently used by your access point is displayed in this field.
VLAN	If your access point is using a VLAN ID for management traffic, it will appear here. A

	value of **0** indicates that a VLAN ID is not being used.
MAC Address (BSSID)	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.
Info	Click this link to display the following information panel:  INFO Close Broadcast SSID: Enable Web Portal Login: Disable MAC Filter: None Bandwidth Control: Disable Layer 2 Isolation: Disable
Stat	Click this link to display the following statistics panel:  STAT Close Packets Sent: 0 Bytes Sent: 0 Packets Received: 0 Bytes Received: 0
Usage Data Type	Select **Per SSID** or **AP Send / Recv** to determine the data displayed in the graphs below.
Hourly	Check this box to graph wireless network usage on an hourly basis.
Wireless Network Usage/Number of Wireless Clients	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.

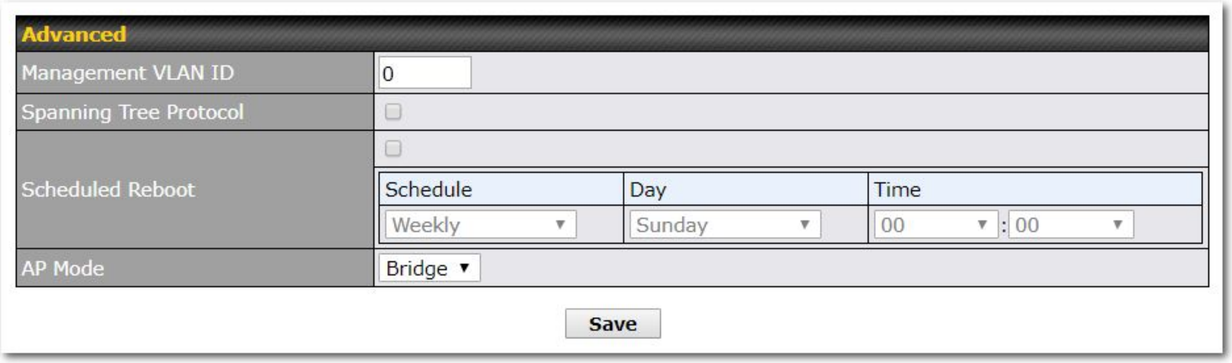
7.1 WAN



Basic	
Keep Default IP	□
IP Address Mode	Manual ▾
Static IP Address	
Subnet Mask	▾
Default Gateway	
DNS Server 1	
DNS Server 2	

This section provides basic and advanced WAN settings.

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

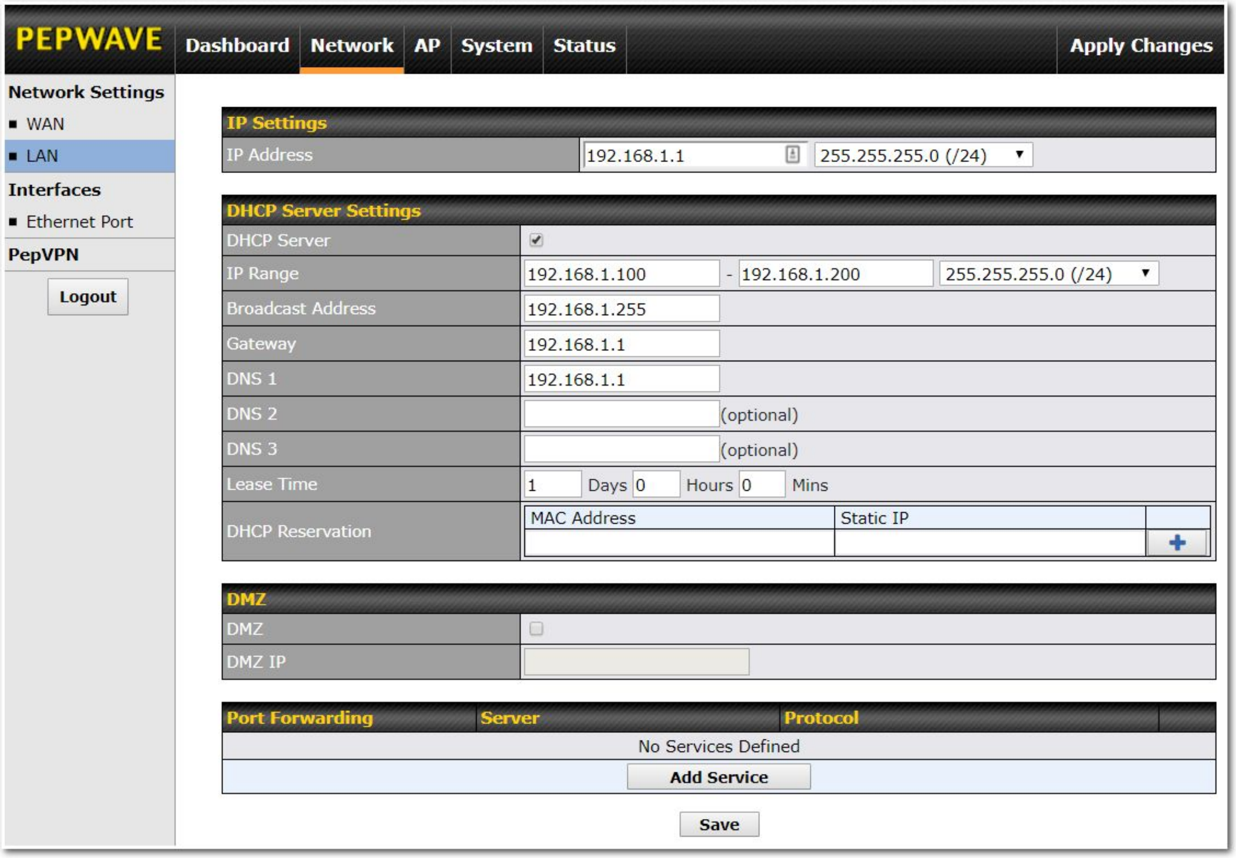


Advanced	
Management VLAN ID	0
Spanning Tree Protocol	□
Scheduled Reboot	□
	Schedule: Weekly ▾ | Day: Sunday ▾ | Time: 00 ▾ : 00 ▾
AP Mode	Bridge ▾

Advanced	
Management VLAN ID	This field specifies the VLAN ID to tag to management traffic, such as AP-to-AP controller communication traffic. The value is **0** 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.
Spanning Tree Protocol	Checking this box enables spanning tree protocol, used to prevent loops in bridged Ethernet LANs
Scheduled Reboot	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 **Schedule**, **Day**, and **Time** headings.
AP Mode	Your access point can act as a bridge or as a router, depending on your selection here. When **Router** is selected, you can additionally select whether the access point will function in **NAT** or **IP Forwarding** 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.



IP Settings

IP Address	192.168.1.1 255.255.255.0 (/24)

DHCP Server Settings

DHCP Server	☑
IP Range	192.168.1.100 - 192.168.1.200 255.255.255.0 (/24)
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
DHCP Reservation	MAC Address / Static IP

DMZ

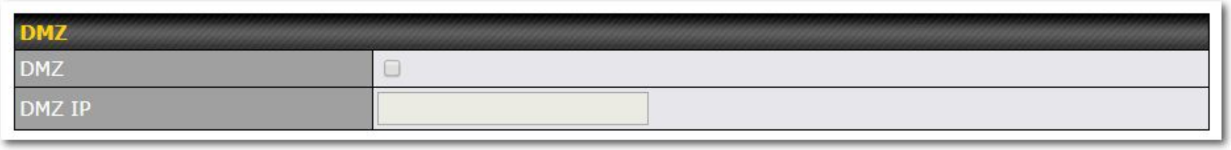
DMZ	□
DMZ IP	

Port Forwarding	Server	Protocol
No Services Defined		

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

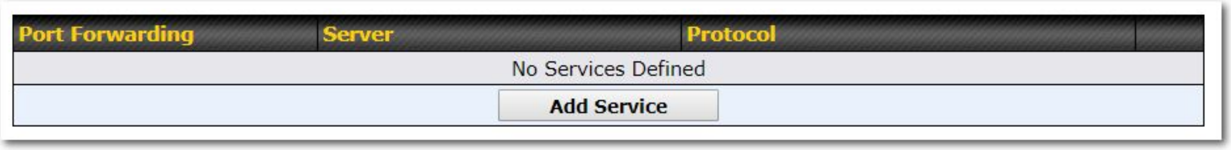
DHCP Server Settings	
DHCP Server	Check to enable the DHCP server feature of your access point. Enabling DHCP is the best option for most users. The following options will be enabled once you have checked and enabled the DHCP server.
IP Range	Enter the first and last IP addresses of the range of addresses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

	192.168.1.200, with 24-bit subnet mask.
Broadcast Address	Enter the broadcast address that DHCP clients will use when communicating with the entire LAN segment. The default value is **192.168.1.255**.
Gateway	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.
DNS 1/2/3	In **DNS 1**, enter the IP address of the primary DNS server offered to DNS clients or accept the default of **192.168.1.1**, 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.
Lease Time	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.
DHCP Reservation	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	□
DMZ IP	

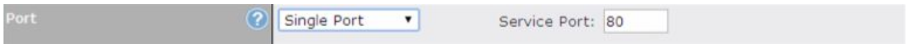
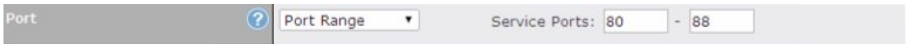
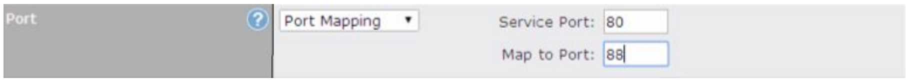
DMZ	
DMZ	Check this box to forward traffic sent to the WAN IP address to the DMZ IP address.
DMZ IP	Enter an IP address clients will use to connect to the DMZ.



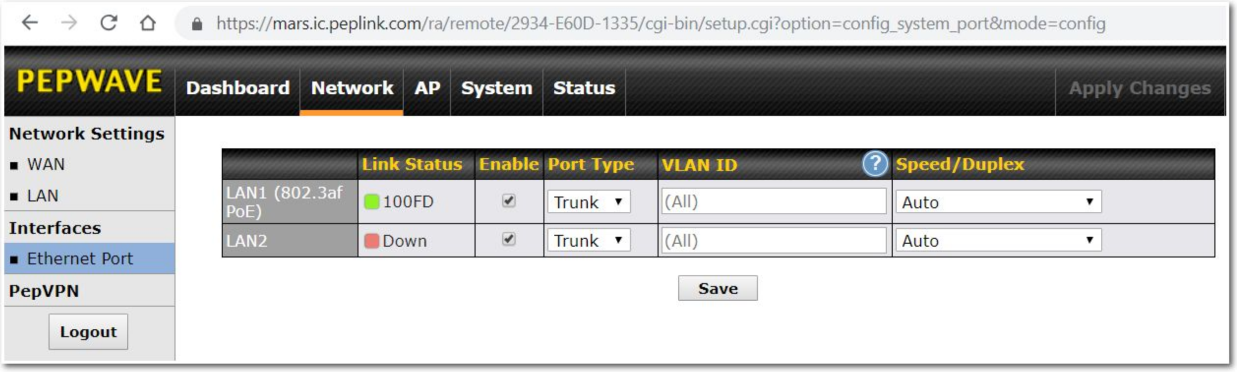
Port Forwarding	Server	Protocol	
No Services Defined			

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

Port Forwarding	
Service Name	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**  Port: Single Port ▾ Service Port: 80 **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: Port Range ▾ Service Ports: 80 - 88 **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: Port Mapping ▾ Service Port: 80 Map to Port: 88 **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 > Ethernet Port



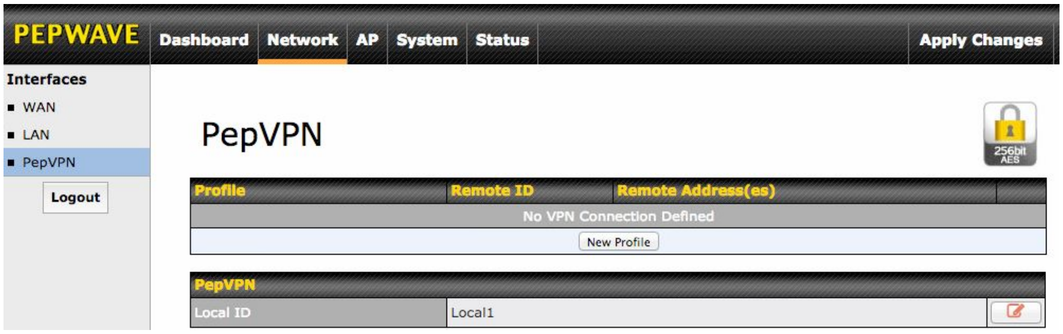
	Link Status	Enable	Port Type	VLAN ID	Speed/Duplex
LAN1 (802.3af PoE)	🟩 100FD	☑	Trunk	(All)	Auto
LAN2	🟥 Down	☑	Trunk	(All)	Auto

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 single VLAN ID is supported.

7.4 PepVPN

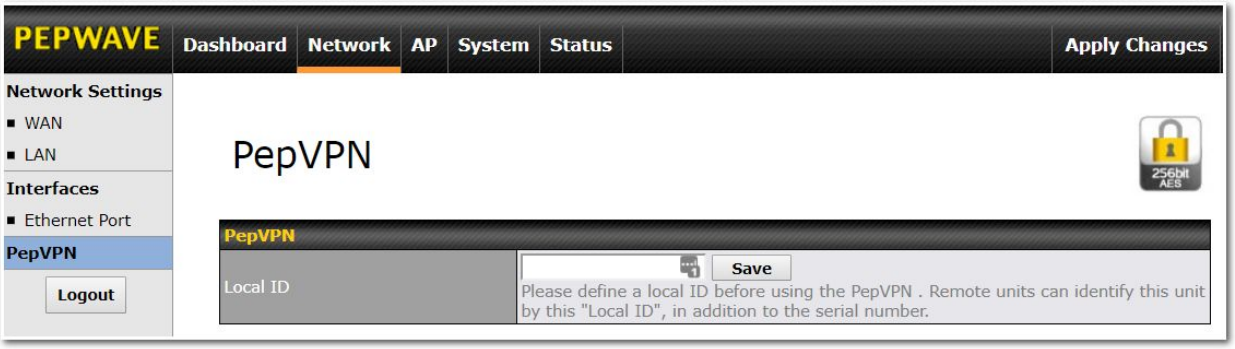
PepVPN securely connects one or more remote sites to the site running your access point.



Profile	Remote ID	Remote Address(es)	
No VPN Connection Defined			

PepVPN		
Local ID	Local1	✎

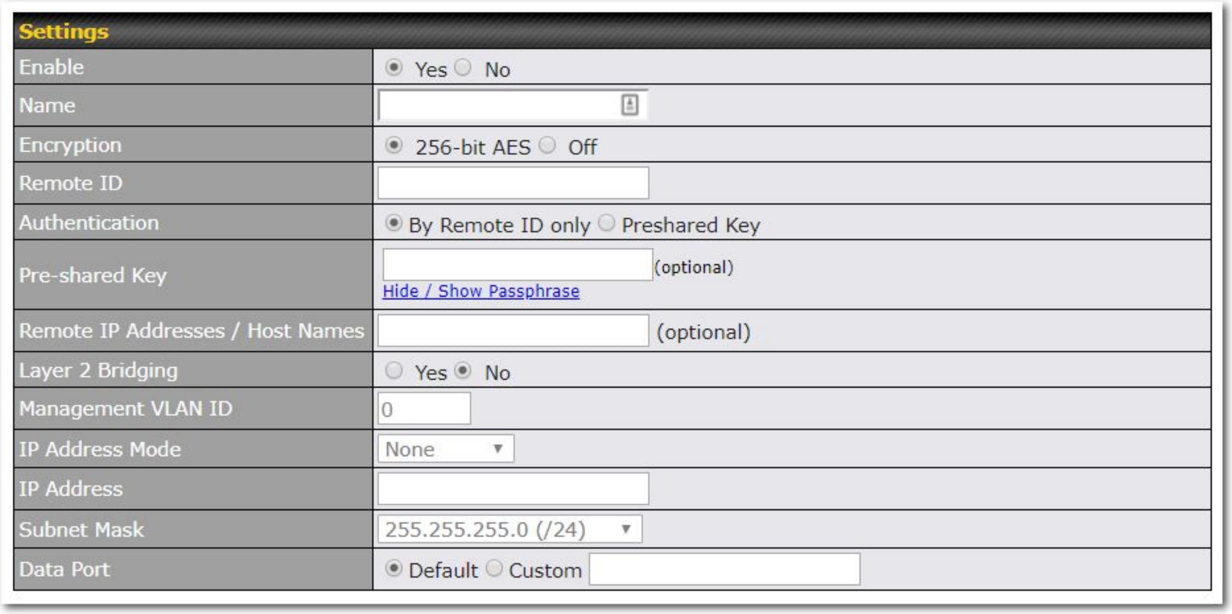
To set up PepVPN, first give your site a local PepVPN ID. To modify an existing local ID, click ✎



PepVPN

PepVPN	
Local ID	Save 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	● Yes ○ No
Name	
Encryption	● 256-bit AES ○ Off
Remote ID	
Authentication	● By Remote ID only ○ Preshared Key
Pre-shared Key	(optional) Hide / Show Passphrase
Remote IP Addresses / Host Names	(optional)
Layer 2 Bridging	○ Yes ● No
Management VLAN ID	0
IP Address Mode	None ▼
IP Address	
Subnet Mask	255.255.255.0 (/24) ▼
Data Port	● Default ○ Custom

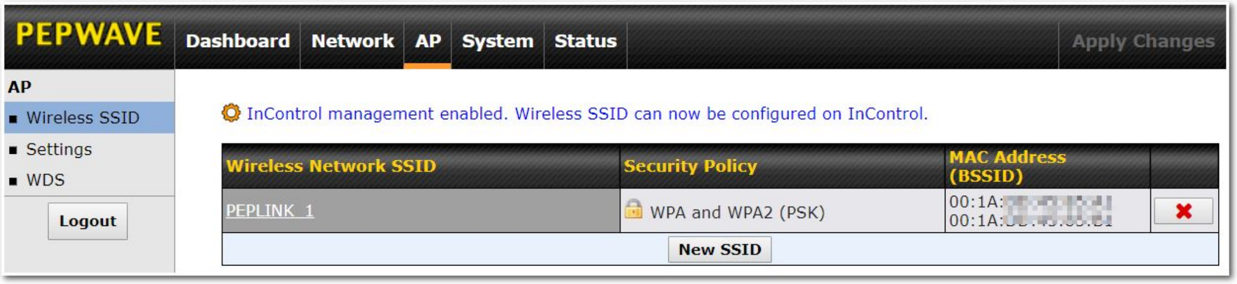
PepVPN Profile Settings	
Enable	Check this box to enable PepVPN.
Name	Enter a name to represent this profile. The name can be any combination of alphanumeric characters (0-9, A-Z, a-z), underscores (_), dashes (-), and/or non-leading/trailing spaces ( ).
Encryption	By default, VPN traffic is encrypted with **256-bit AES**. If **Off** is selected on both sides of a VPN connection, no encryption will be applied.
Remote ID	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.
Authentication	Select **By Remote ID Only** or **Preshared Key** to specify the method your access point will use to authenticate peers. When selecting **By Remote ID Only**, be sure to enter a

	unique peer ID number in the **Remote ID** field.
Pre-shared Key	This optional field becomes available when **Pre-shared Key** is selected as the VPN **Authentication** method, as explained above. **Pre-shared Key** defines the pre-shared key used for this particular VPN connection. The VPN connection's session key will be further protected by the pre-shared key. The connection will be up only if the pre-shared keys on each side match. Click **Hide / Show Passphrase** to toggle passphrase visibility.
Remote IP Address / Host Names (Optional)	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. 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.
Layer 2 Bridging	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 **Layer 2 Bridging**. 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.
Management VLAN ID	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.
IP Address Mode	Choose **Automatic** or **Manual**. 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.
IP Address/Subnet Mask	When using manual IP addressing (above), enter an IP address and subnet mask in these fields.
Data Port	This field specifies the outgoing UDP port number for transporting VPN data. If **Default** is selected, port 4500 will be used by default. Port 32015 will be used if port 4500 is unavailable. If **Custom** 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 and AP settings, as well as wireless distribution system (WDS) settings.

8.1 Wireless SSID

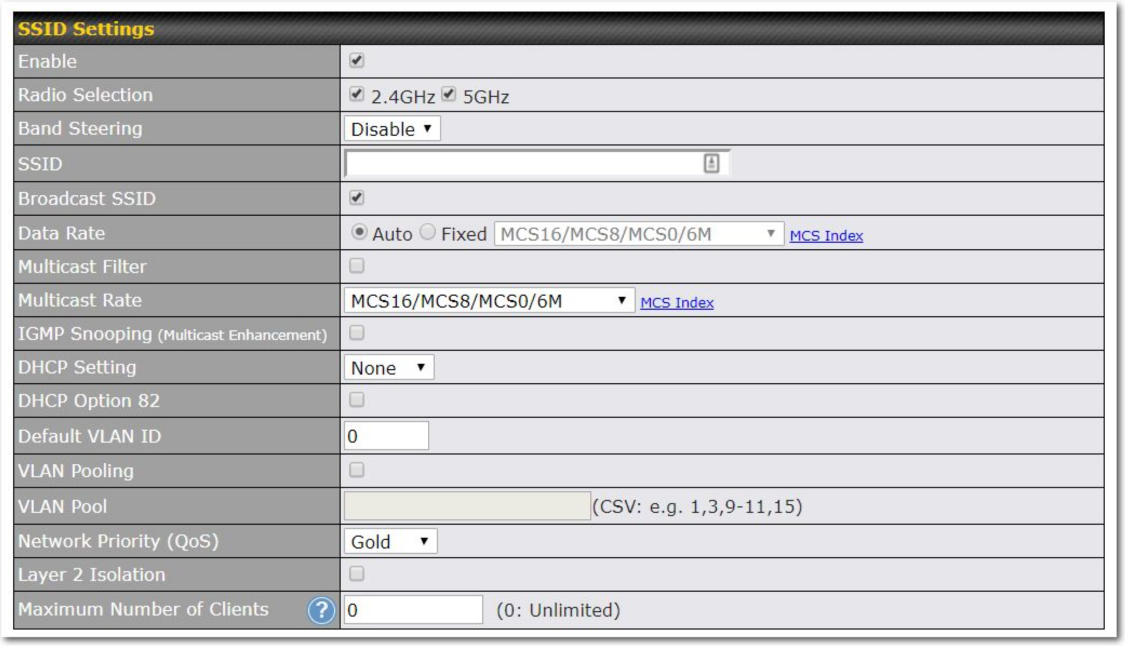


InControl management enabled. Wireless SSID can now be configured on InControl.

Wireless Network SSID	Security Policy	MAC Address (BSSID)	
PEPLINK_1	WPA and WPA2 (PSK)	00:1A:[redacted] 00:1A:[redacted]	✖
New SSID			

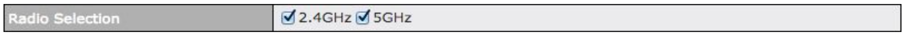
Wireless network settings, including the name of the network (SSID) and security policy, can be defined and managed in this section.

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



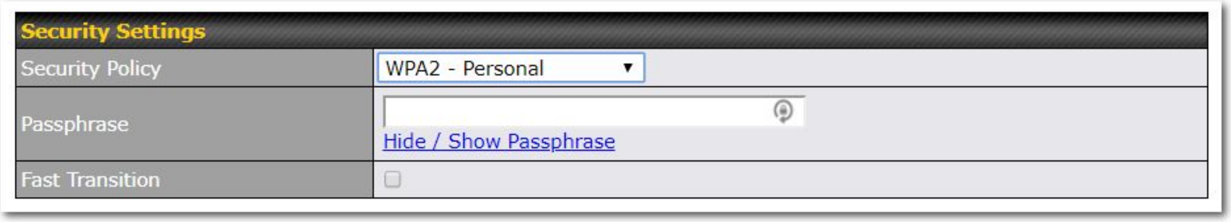
SSID Settings	
Enable	☑
Radio Selection	☑ 2.4GHz ☑ 5GHz
Band Steering	Disable ▾
SSID	
Broadcast SSID	☑
Data Rate	● Auto ○ Fixed MCS16/MCS8/MCS0/6M ▾ MCS Index
Multicast Filter	□
Multicast Rate	MCS16/MCS8/MCS0/6M ▾ MCS Index
IGMP Snooping (Multicast Enhancement)	□
DHCP Setting	None ▾
DHCP Option 82	□
Default VLAN ID	0
VLAN Pooling	□
VLAN Pool	(CSV: e.g. 1,3,9-11,15)
Network Priority (QoS)	Gold ▾
Layer 2 Isolation	□
Maximum Number of Clients ?	0 (0: Unlimited)

SSID Settings	
Enable	Check this box to enable wireless SSID.

Radio Selection	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.  Radio Selection ☑2.4GHz ☑5GHz
Band Steering	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. **Force** - Clients capable of 5 GHz operation are only offered with 5 GHz frequency. **Prefer** - 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. Default: **Disable** Band Steering Disable ▾
SSID	This setting specifies the AP SSID that Wi-Fi clients will see when scanning.
Broadcast SSID	This setting specifies whether or not Wi-Fi clients can scan the SSID of this wireless network. **Broadcast SSID** is enabled by default.
Data Rate	Select **Auto** to allow your access point to set the data rate automatically, or select **Fixed** and choose a rate from the drop-down menu. Click the **MCS Index** link to display a reference table containing MCS and matching HT20 and HT40 values.
Multicast Filter	This setting enables the filtering of multicast network traffic to the wireless SSID.
Multicast Rate	This setting specifies the transmit rate to be used for sending multicast network traffic.
IGMP Snooping	To allow your access point to convert multicast traffic to unicast traffic for associated clients, select this option.
DHCP Setting	To set your access point as a DHCP server or relay, select **Server** or **Relay**. Otherwise, select **None**.
DHCP Option 82	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.
Default VLAN ID	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 **authentication reply from the Radius server**, then the value specified by **Default VLAN ID** will be overridden. The default value of this setting is **0**, which means VLAN tagging is disabled (instead of tagged with zero).
VLAN Pooling	Check this box to enable VLAN pooling using the values specified in **VLAN Pool**.
VLAN Pool	If VLAN pooling is enabled, enter VLAN pool values separated by commas.
Network Priority (QoS)	Select from **Gold**, **Silver**, and **Bronze** to control the QoS priority of this wireless network traffic.

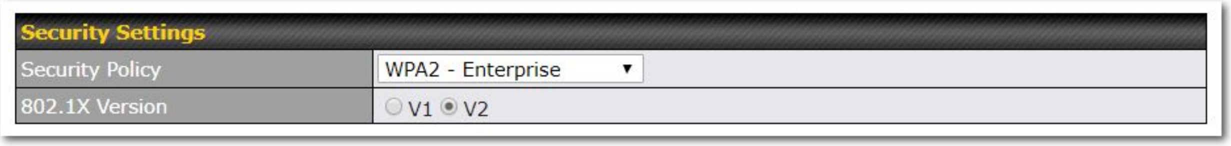
Layer 2 Isolation	Refers to the second layer in the ISO Open System Interconnect model. When this option is enabled, clients on the same VLAN, SSID, or subnet are isolated to that VLAN, SSID, or subnet, which can enhance security. Traffic is passed to upper communication layer(s). By default, the setting is disabled.
Maximum Number of Clients	The maximum number of clients that can simultaneously connect to your access point, or enter **0** to allow unlimited Wi-Fi clients.

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



Security Settings	
Security Policy	WPA2 - Personal ▾
Passphrase	Hide / Show Passphrase
Fast Transition	□

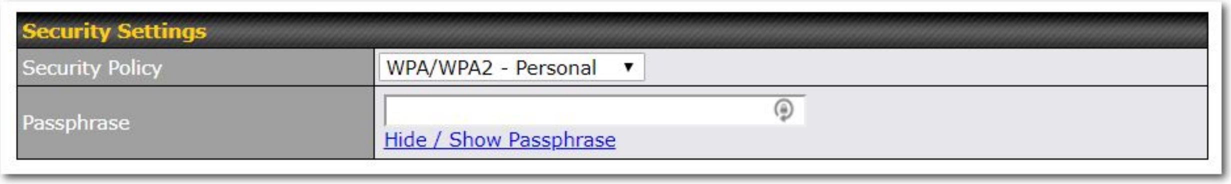
WPA2 – Personal	
Passphrase	Enter a passphrase of between 8 and 63 alphanumeric characters to create a passphrase used for data encryption and authentication. Click **Hide / Show Passphrase** to toggle visibility.
Fast Transition	Fast Transition [802.11r] The transition process of a mobile client as it moves between access points is improved when this option is ticked.



Security Settings	
Security Policy	WPA2 - Enterprise ▾
802.1X Version	○ V1 ● V2

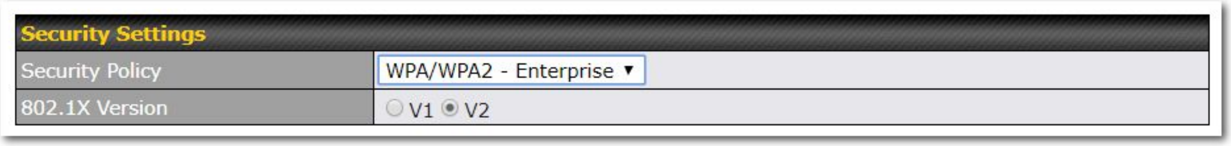
WWPA2 – Enterprise

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**.



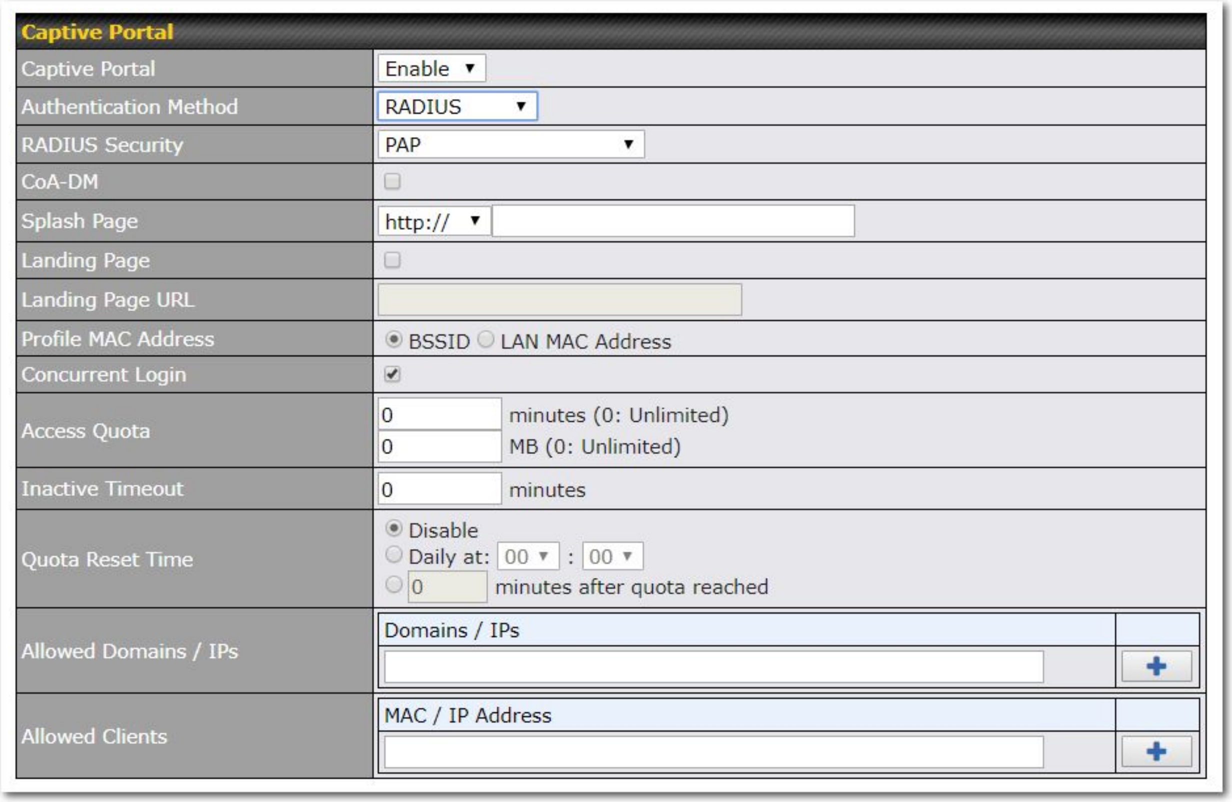
Security Settings	
Security Policy	WPA/WPA2 - Personal ▼
Passphrase	Hide / Show Passphrase

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.



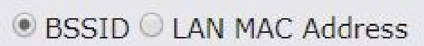
Security Settings	
Security Policy	WPA/WPA2 - Enterprise ▼
802.1X Version	○ V1 ● V2

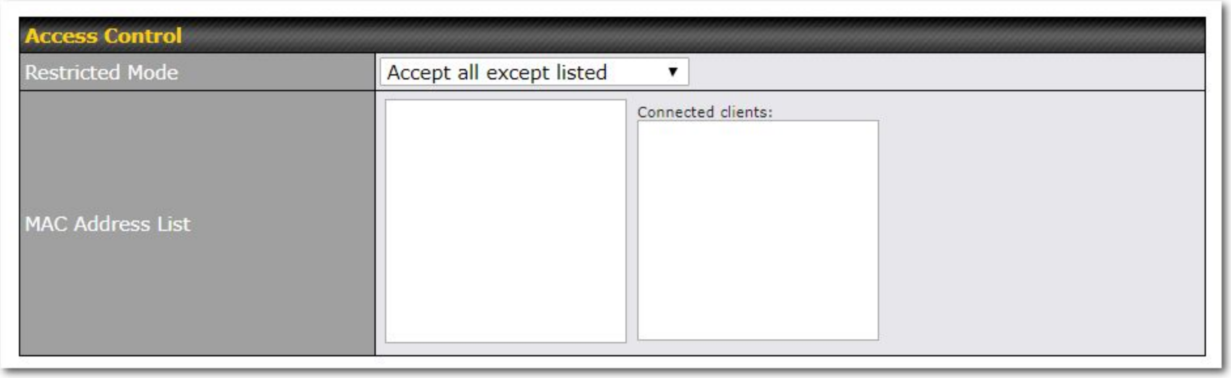
WPA/WPA2 – Enterpise	
802.1X Version	Choose **v1** or **v2** of the 802.1x EAPOL. When **v1** is selected, both v1 and v2 clients can associate with the access point. When **v2** is selected, only v2 clients can associate with the access point. Most modern wireless clients support v2. For stations that do not support v2, select **v1**. The default is **v2**.



Captive Portal	
Captive Portal	Enable ▾
Authentication Method	RADIUS ▾
RADIUS Security	PAP ▾
CoA-DM	□
Splash Page	http:// ▾
Landing Page	□
Landing Page URL	
Profile MAC Address	● BSSID ○ LAN MAC Address
Concurrent Login	☑
Access Quota	0 minutes (0: Unlimited) 0 MB (0: Unlimited)
Inactive Timeout	0 minutes
Quota Reset Time	● Disable ○ Daily at: 00 ▾ : 00 ▾ ○ 0 minutes after quota reached
Allowed Domains / IPs	Domains / IPs ✚
Allowed Clients	MAC / IP Address ✚

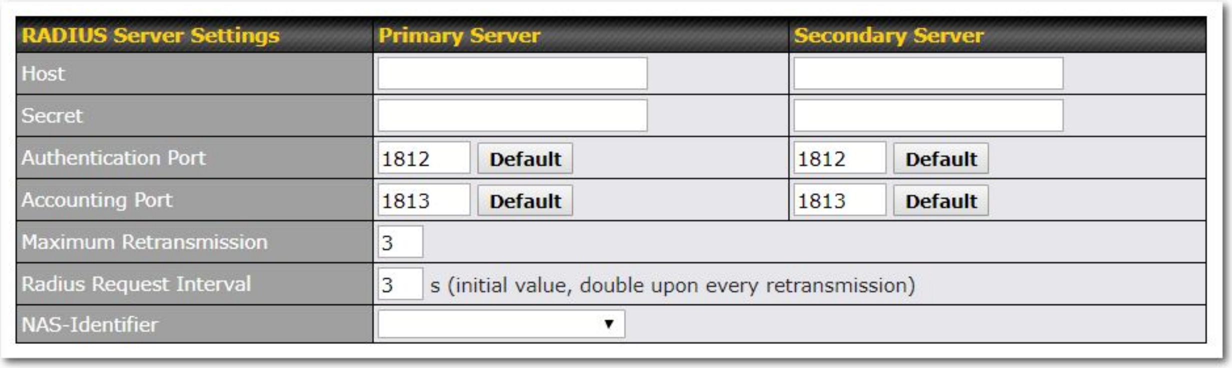
Captive Portal Login	
Captive Portal	Select **Enable** to turn on your access point's built-in captive portal functionality.
Authentication Method	Choose **Open Access** to allow users to connect without authentication or **RADIUS** to require authentication. If **RADIUS** is selected, you'll be given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

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



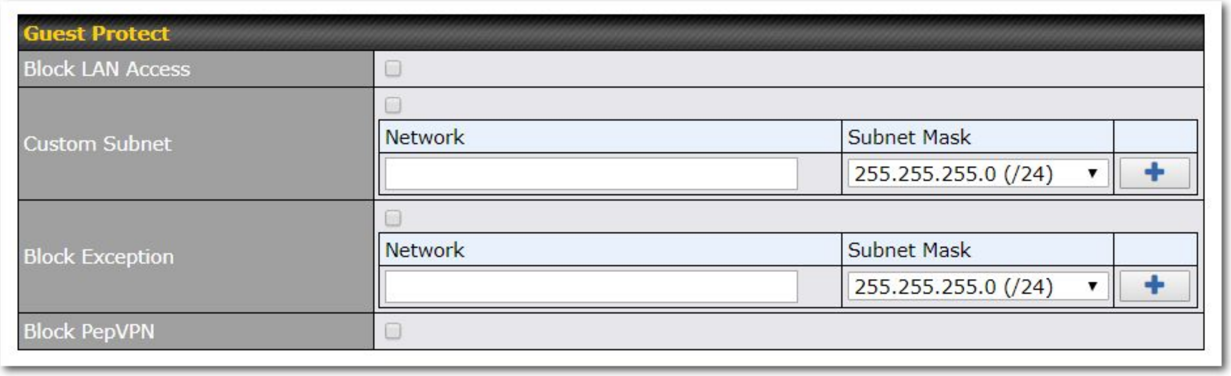
Access Control	
Restricted Mode	Accept all except listed ▾
MAC Address List	Connected clients:

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



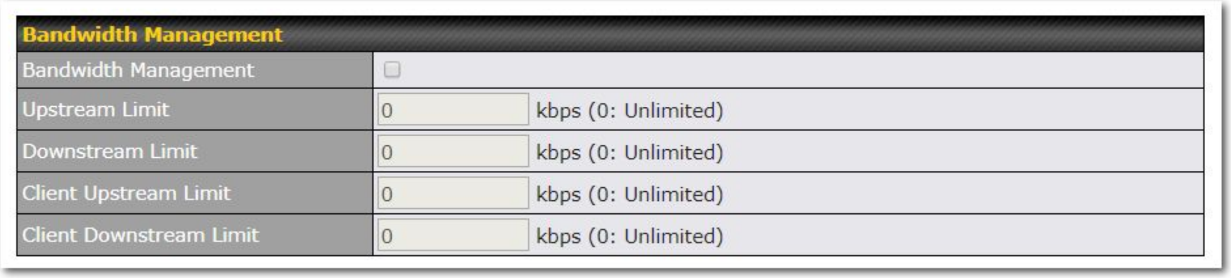
RADIUS Server Settings	Primary Server	Secondary Server
Host		
Secret		
Authentication Port	1812 Default	1812 Default
Accounting Port	1813 Default	1813 Default
Maximum Retransmission	3	
Radius Request Interval	3 s (initial value, double upon every retransmission)	
NAS-Identifier	▾	

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



Guest Protect	
Block LAN Access	□
Custom Subnet	□ Network: [ ] Subnet Mask: 255.255.255.0 (/24) ▾ +
Block Exception	□ Network: [ ] Subnet Mask: 255.255.255.0 (/24) ▾ +
Block PepVPN	□

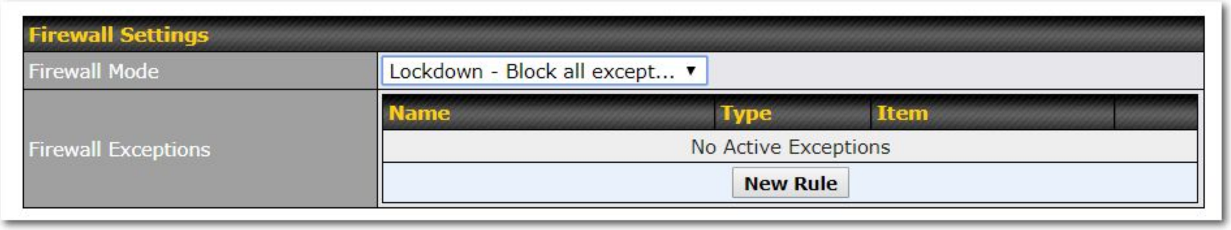
Guest Protect	
Block LAN Access	Check this box to block access from the LAN.
Custom Subnet	To specify a subnet to block, enter the IP address and choose a subnet mask from the drop-down menu. To add the blocked subnet, click +. To delete a blocked subnet, click ✖.
Block Exception	To create an exception to a blocked subnet (above), enter the IP address and choose a subnet mask from the drop-down menu. To add the exception, click +. To delete an exception, click ✖.
Block PepVPN	To block PepVPN access, check this box.



Bandwidth Management	
Bandwidth Management	□
Upstream Limit	0 kbps (0: Unlimited)
Downstream Limit	0 kbps (0: Unlimited)
Client Upstream Limit	0 kbps (0: Unlimited)
Client Downstream Limit	0 kbps (0: Unlimited)

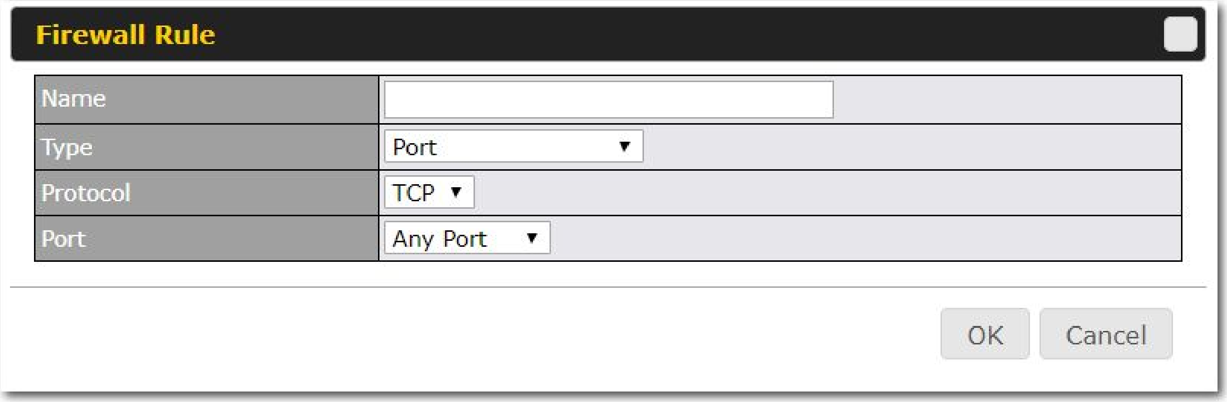
Bandwidth Management	
Bandwidth Management	Check this box to enable bandwidth management.
Upstream Limit	Enter a value in kbps to limit the wireless network's upstream bandwidth. Enter **0** to allow unlimited upstream bandwidth.

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



Firewall Settings	
Firewall Mode	Lockdown - Block all except... ▼
Firewall Exceptions	Name | Type | Item No Active Exceptions New Rule

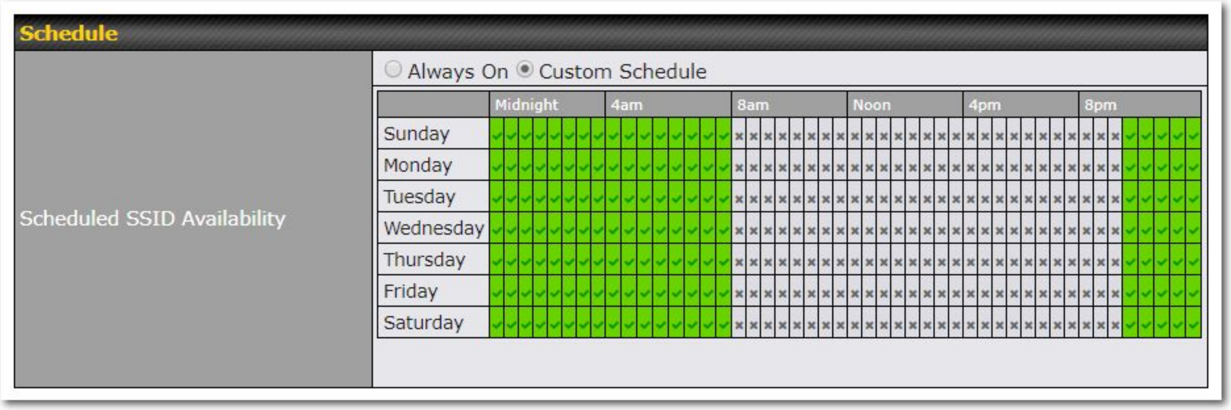
Firewall Settings	
Firewall Mode	Choose **Flexible – Allow all except…** or **Lockdown – Block all except…** to turn on the firewall, then create rules for the firewall exceptions by clicking New Rule . See the discussion below for details on creating a firewall rule. To delete a rule, click the associated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



Firewall Rule	
Name	
Type	Port ▼
Protocol	TCP ▼
Port	Any Port ▼

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

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



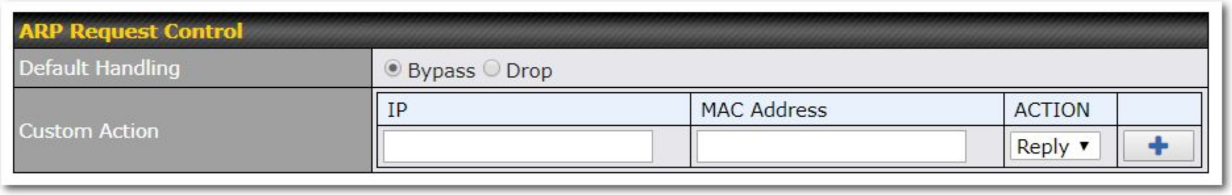
Schedule

Scheduled SSID Availability

○ Always On ● Custom Schedule

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

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



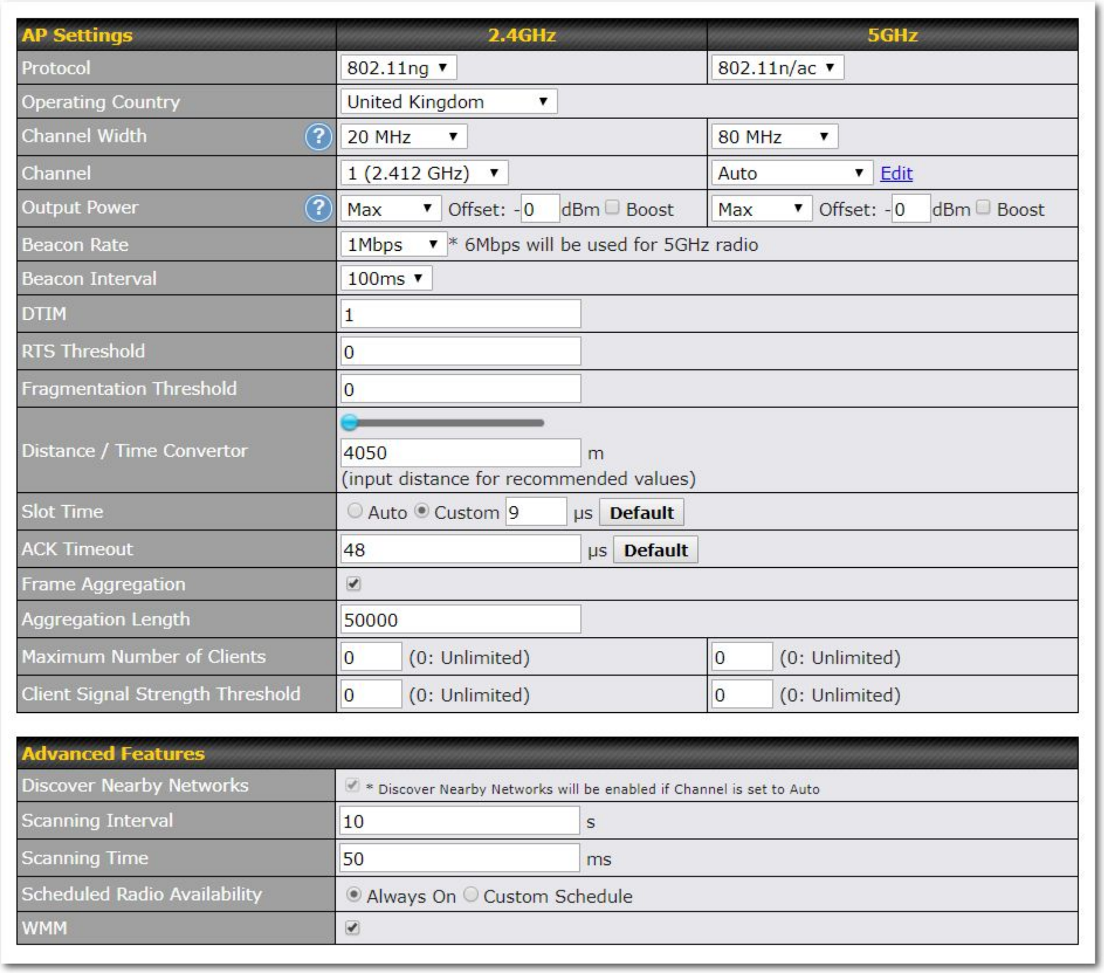
ARP Request Control

Default Handling	● Bypass ○ Drop			
Custom Action	IP	MAC Address	ACTION	
			Reply ▼	+

ARP Request Control	
ARP request control is a Broadcast filter feature which: ● blocks all broadcast traffic, ● relays DHCP requests, ● responds to ARP requests asking the MAC address of the gateway	
Default handling	Choose between **Bypass** or **Drop** (default Bypass)
Custom Action	Add IP/ MAC address pairs to this field to either: **REPLY** : The AP replies to the MAC address itself according to the config **DNAT :** The AP can translate the destination MAC address from a broadcast to a particular MAC address

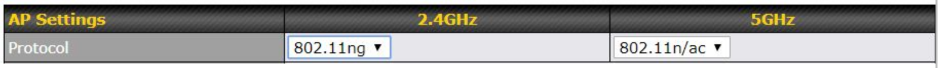
8.2 Settings

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

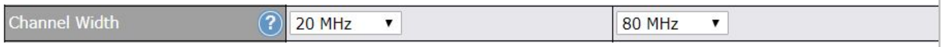
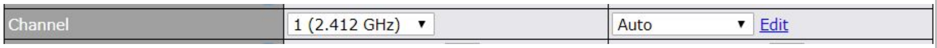
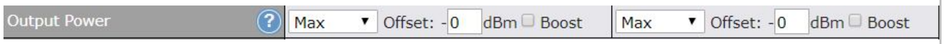
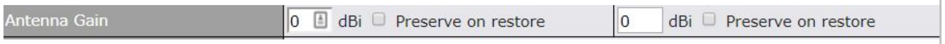


AP Settings	2.4GHz	5GHz
Protocol	802.11ng ▾	802.11n/ac ▾
Operating Country	United Kingdom ▾	
Channel Width ?	20 MHz ▾	80 MHz ▾
Channel	1 (2.412 GHz) ▾	Auto ▾ Edit
Output Power ?	Max ▾ Offset: -0 dBm □ Boost	Max ▾ Offset: -0 dBm □ Boost
Beacon Rate	1Mbps ▾ * 6Mbps will be used for 5GHz radio	
Beacon Interval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

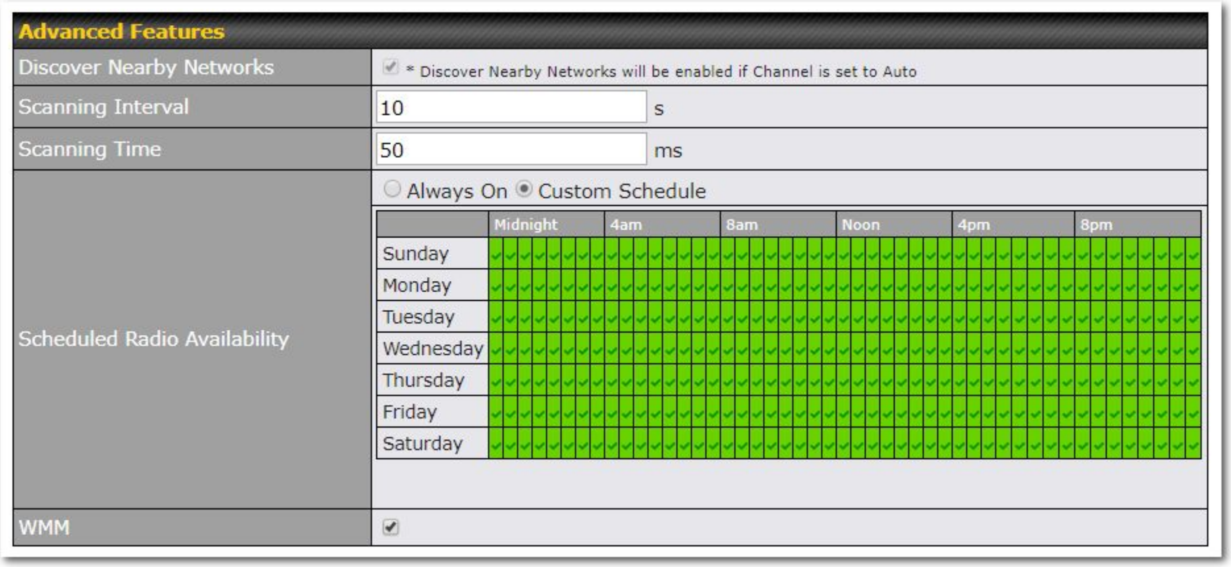
Advanced Features	
Discover Nearby Networks	☑ * Discover Nearby Networks will be enabled if Channel is set to Auto
Scanning Interval	10 s
Scanning Time	50 ms
Scheduled Radio Availability	● Always On ○ Custom Schedule
WMM	☑

<table>
<tr><th colspan="2">AP Settings</th></tr>
<tr><td><b>Protocol</b></td><td>Choose <b>802.11ng</b> or <b>802.11n/ac</b> as your access point’s Wi-Fi protocol.
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.
<table><tr><th>AP Settings</th><th>2.4GHz</th><th>5GHz</th></tr><tr><td>Protocol</td><td>802.11ng ▾</td><td>802.11n/ac ▾</td></tr></table></td></tr>
<tr><td><b>Operating Country</b></td><td>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).
If European region is selected, RF channels 1 to 13 will be available. The maximum transmission power will be 20 dBm (100 mW).

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</td></tr>
</table>

	US. All US models are fixed to US channels only.
Channel Width	This option defines which channel width the radio will use: **20MHz** - Supports clients with 20MHz capability. This is the default value for 802.11ng. **40MHz** - Supports clients with 20/40MHz capability. **20/40MHz** - 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. **80MHz** - Supports clients with 20/40/80MHz capability. This is the default value for 802.11n/ac  Channel Width ? 20 MHz ▼ 80 MHz ▼
Channel	This drop-down menu selects the 2.4 Ghz and 5GHz 802.11 channels to be used. When **Auto** is selected, the system will perform channel scanning based on the scheduled time set and choose the most suitable channel automatically.  Channel 1 (2.412 GHz) ▼ Auto ▼ Edit
Output Power	This option enables the configuration of transmission power. Choose between :Max / High / Medium / Low **Max** is the Maximum power supported for that country or Maximum power supported for the device (whichever is the smaller value) **High** is 3dBm below the max value. **Medium** is 3dBm below high value **Low** is 3 dBm below Medium value  Output Power ? Max ▼ Offset: -0 dBm □ Boost Max ▼ Offset: -0 dBm □ Boost
Antenna Gain	This advanced feature becomes available when selecting this option in the Help section(select the question mark) of the Output Power.  Antenna Gain 0 dBi □ Preserve on restore 0 dBi □ Preserve on restore
Beacon Rate	This drop-down menu provides the option to send beacons in different transmit bit rates. The bit rates are **1 Mbps**, **2 Mbps**, **5.5 Mbps**, **6 Mbps**, and **11 Mbps**.
Beacon Interval	Set the time between each beacon send. Available options are **100 ms**, **250 ms**, and **500 ms**.
DTIM	Set the frequency for the beacon to include delivery traffic indication messages (DTIM). The interval unit is measured in milliseconds.
RTS Threshold	Set the minimum packet size for your access point to send an RTS using the RTS/CTS handshake. Setting **0** disables this feature.
Fragmentation Threshold	Enter a value to limit the maximum frame size, which can improve performance.
Distance / Time Convertor	This slider and text entry field can be used to interactively set slot time.
Slot Time	This field provides the option to modify the unit wait time before your access point

	transmits. The default value is **9µs.**
ACK Timeout	Set the wait time to receive an acknowledgement packet before retransmitting. The default value is **48µs.**
Frame Aggregation	With this feature enabled, throughput will be increased by sending two or more data frames in a single transmission.
Aggregation Length	This field is only available when **Frame Aggregation** is enabled. It specifies the frame length for frame aggregation. By default, it is set to **50000**.
Max number of Clients	Enter the maximum clients that can simultaneously connect to your access point or set the value to **0** to allow unlimited clients.
Client Signal Strength Threshold	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	☑ * Discover Nearby Networks will be enabled if Channel is set to Auto
Scanning Interval	10 s
Scanning Time	50 ms
Scheduled Radio Availability	○ Always On ● Custom Schedule
WMM	☑

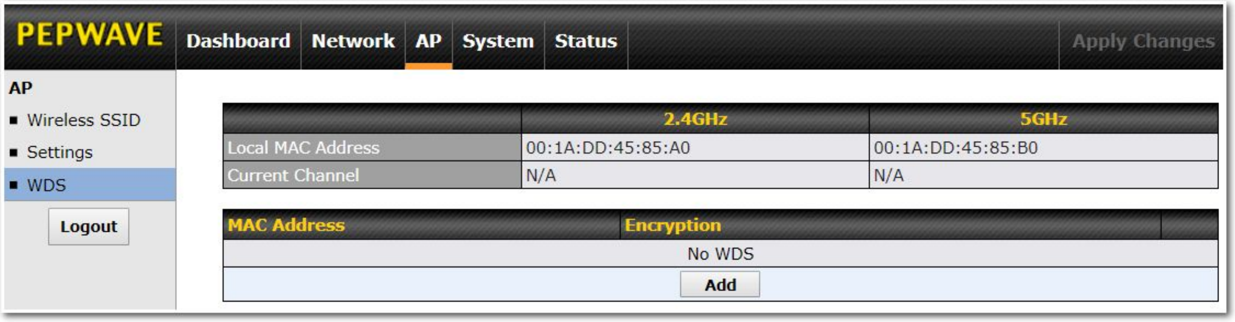
	Midnight	4am	8am	Noon	4pm	8pm
Sunday	✓✓✓✓✓✓✓✓	✓✓✓✓✓✓✓✓	✓✓✓✓✓✓✓✓	✓✓✓✓✓✓✓✓	✓✓✓✓✓✓✓✓	✓✓✓✓✓✓✓✓
Monday	✓✓✓✓✓✓✓✓	✓✓✓✓✓✓✓✓	✓✓✓✓✓✓✓✓	✓✓✓✓✓✓✓✓	✓✓✓✓✓✓✓✓	✓✓✓✓✓✓✓✓
Tuesday	✓✓✓✓✓✓✓✓	✓✓✓✓✓✓✓✓	✓✓✓✓✓✓✓✓	✓✓✓✓✓✓✓✓	✓✓✓✓✓✓✓✓	✓✓✓✓✓✓✓✓
Wednesday	✓✓✓✓✓✓✓✓	✓✓✓✓✓✓✓✓	✓✓✓✓✓✓✓✓	✓✓✓✓✓✓✓✓	✓✓✓✓✓✓✓✓	✓✓✓✓✓✓✓✓
Thursday	✓✓✓✓✓✓✓✓	✓✓✓✓✓✓✓✓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

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

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

8.3 WDS

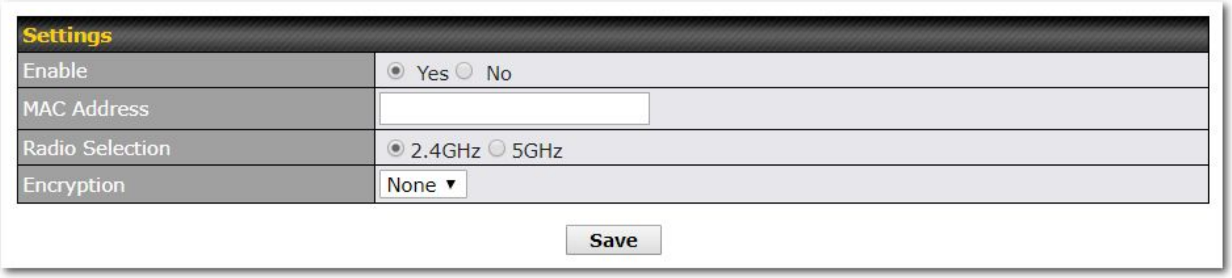
A wireless distribution system (WDS) provides a way to link access points when wires are not feasible or desirable. A WDS can also extend wireless network coverage for wireless clients. Note that your access point's channel setting should not be set to **Auto** when using WDS.



	2.4GHz	5GHz
Local MAC Address	00:1A:DD:45:85:A0	00:1A:DD:45:85:B0
Current Channel	N/A	N/A

MAC Address	Encryption
No WDS	

To create a new WDS, click **Add**.



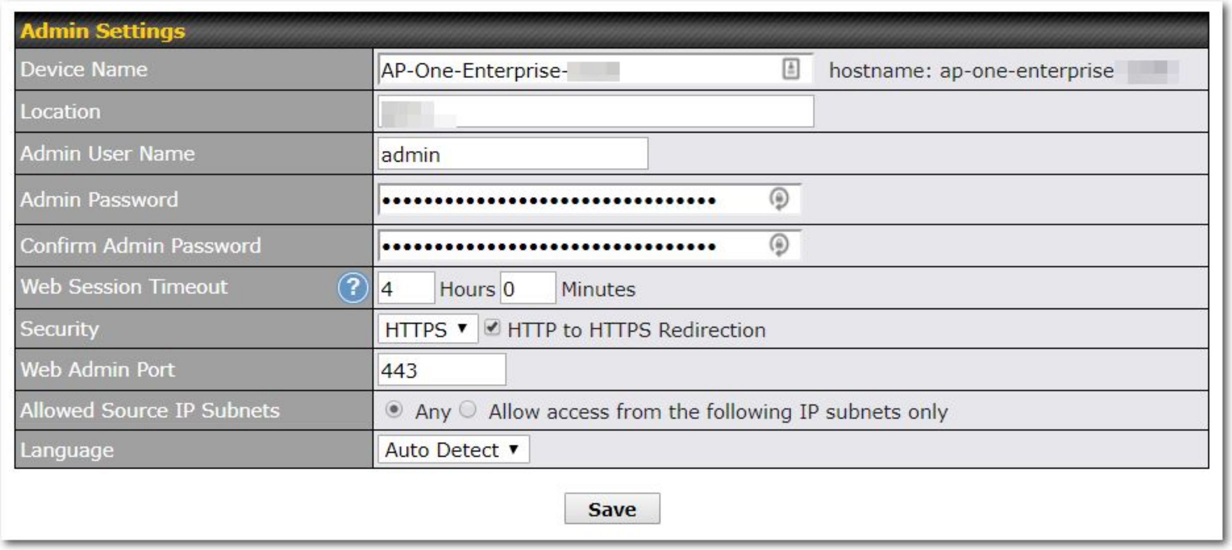
Settings	
Enable	● Yes ○ No
MAC Address	
Radio Selection	● 2.4GHz ○ 5GHz
Encryption	None ▾

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

Encryption	Select **AES** to enable encryption for WDS peer connections. Selecting **None** disables encryption.

9 System Tab

9.1 Admin Security

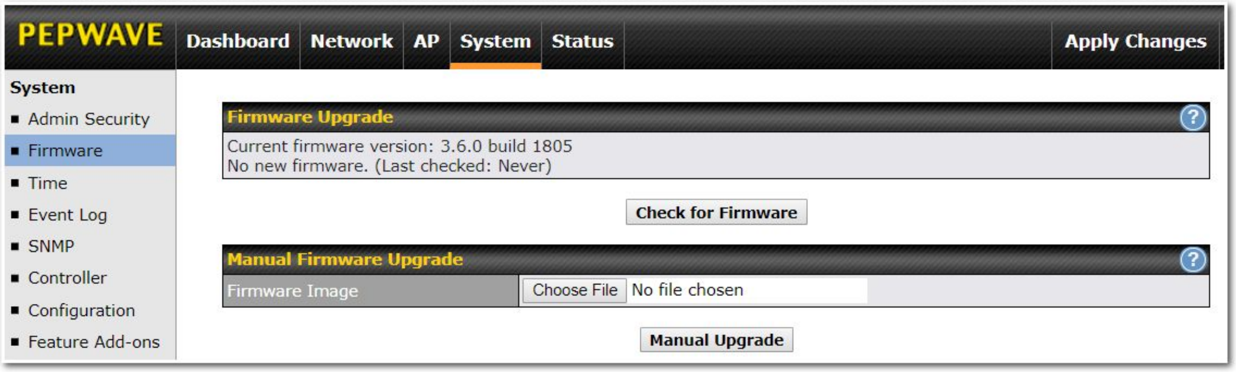


Admin Settings	
Device Name	AP-One-Enterprise-[redacted] hostname: ap-one-enterprise[redacted]
Location	[redacted]
Admin User Name	admin
Admin Password	••••••••••••••••••••••••••••••••
Confirm Admin Password	••••••••••••••••••••••••••••••••
Web Session Timeout	4 Hours 0 Minutes
Security	HTTPS ▾ ☑ HTTP to HTTPS Redirection
Web Admin Port	443
Allowed Source IP Subnets	● Any ○ Allow access from the following IP subnets only
Language	Auto Detect ▾

Admin Settings	
Devicer Name	This field allows you to define a name for this Peplink Balance unit. By default, **Device Name** is set as **Model_XXXX**, where *XXXX* refers to the last 4 digits of the serial number of that unit.
Location	field to add Location name
Admin User	**Admin User Name** is set as **admin** by default, but can be changed.

Name	
Admin Password	This field allows you to specify a new administrator password.
Confirm Admin Password	This field allows you to verify and confirm the new administrator password.
Web Session Timeout	A web login session will be logged out automatically when it has been idle longer than the Web Session Timeout Unlimited session timeout: 0 hours 0 minutes Default: 4 hours 0 minutes
Security	This option is for specifying the protocol(s) through which the web admin interface can be accessed: ● HTTP ● HTTPS ● HTTP/HTTPS
Web Admin Port	This field is for specifying the port number on which the web admin interface can be accessed.
Allowed Source IP Subnets	This option is for specifying the IP subnetss through which the web admin interface can be accessed.
Language	Set language of the Web Interface

9.2 Firmware



Firmware Upgrade

Current firmware version: 3.6.0 build 1805
No new firmware. (Last checked: Never)

Manual Firmware Upgrade

Firmware Image: No file chosen

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, ateh Access Point automatically download the firmware. The rest of the upgrade process will be automatically initiated.

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

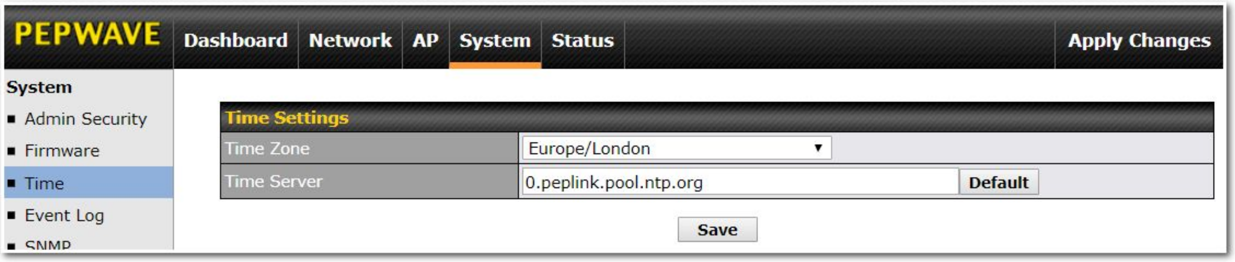
Status LED Information during firmware upgrade:

- 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 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.

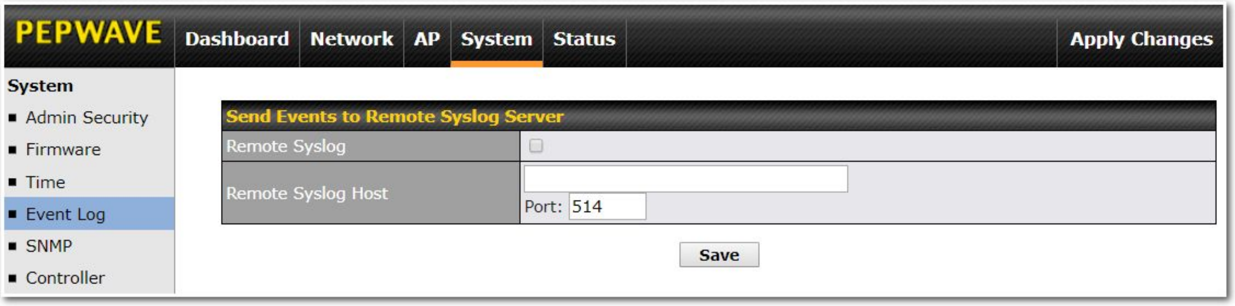
9.3 Time



Time Settings	
Time Zone	Europe/London
Time Server	0.peplink.pool.ntp.org

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



Send Events to Remote Syslog Server

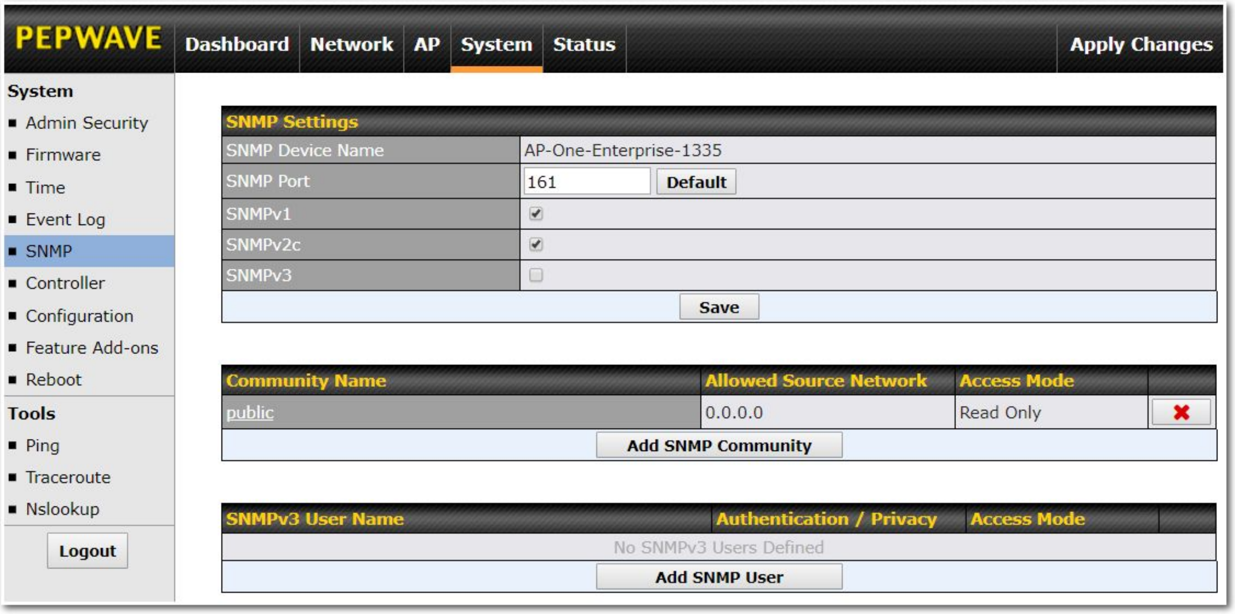
Remote Syslog	□
Remote Syslog Host	Port: 514

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	
Remote Syslog	This setting specifies whether or not to log events at the specified remote syslog server.
Remote Syslog Host	This setting specifies the IP address or hostname of the remote syslog server. 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	
SNMP Device Name	AP-One-Enterprise-1335
SNMP Port	161 Default
SNMPv1	☑
SNMPv2c	☑
SNMPv3	☐

Save

Community Name	Allowed Source Network	Access Mode	
public	0.0.0.0	Read Only	✖

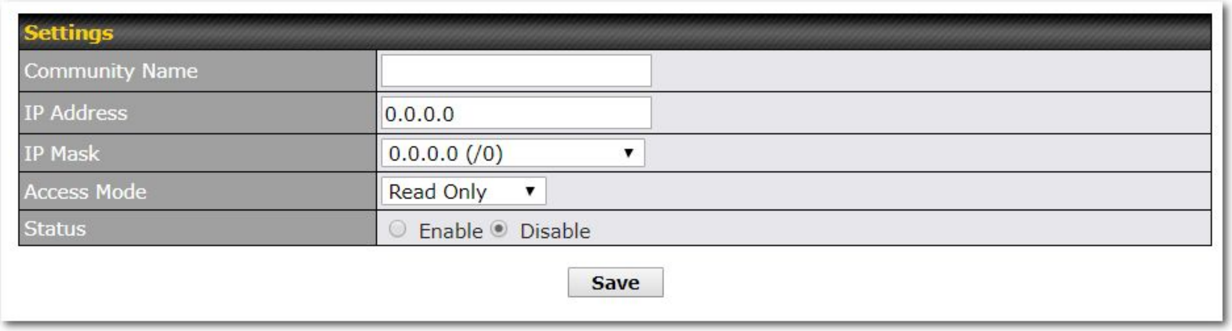
Add SNMP Community

SNMPv3 User Name	Authentication / Privacy	Access Mode	
No SNMPv3 Users Defined			

Add SNMP User

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

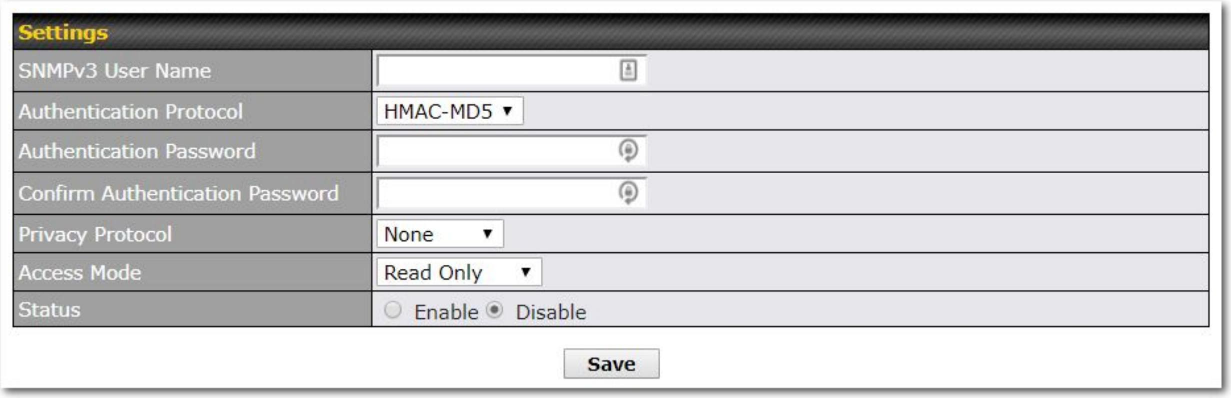
To add a community for either SNMPv1 or SNMPv2, click the **Add SNMP Community** button in the **Community Name** table, upon which the following screen is displayed:



Settings	
Community Name	
IP Address	0.0.0.0
IP Mask	0.0.0.0 (/0) ▾
Access Mode	Read Only ▾
Status	○ Enable ● Disable

SNMP Community Settings	
Community Name	This setting specifies the SNMP community name.
IP Address & IP mask	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.
Access Mode	Choose between **Read Only** and **Read and Write**
Status	Enable or Disable SNMP community

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

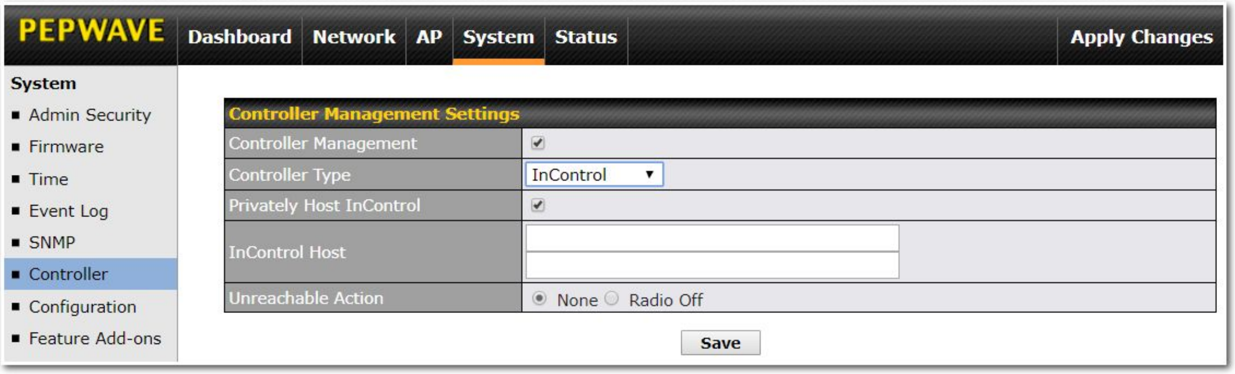


Settings	
SNMPv3 User Name	
Authentication Protocol	HMAC-MD5 ▾
Authentication Password	
Confirm Authentication Password	
Privacy Protocol	None ▾
Access Mode	Read Only ▾
Status	○ Enable ● Disable

SNMPv3 User Settings	
SNMPv3 User Name	This setting specifies a user name to be used in SNMPv3.
Authentication Protocol	This setting specifies via a drop-down menu one of the following valid authentication protocols:

	- HMAC-MD5 - HMAC-SHA
Authentication Password	Password for SNMPv3 authentication.
Confirm Authentication Password	Confirm password for SNMPv3 authentication.
Privacy Protocol	This setting specifies via a drop-down menu one of the following valid privacy protocols: - None - CBC-DES When CBC-DES is selected, an entry field will appear for the password.
Access Mode	Choose between Read Only and Read and Write.
Status	Enable or Disable SNMPv3 user

9.6 Controller



Controller Management Settings

Controller Management	☑
Controller Type	InControl ▾
Privately Host InControl	☑
InControl Host	
Unreachable Action	● None ○ Radio Off

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

Controller Management Settings

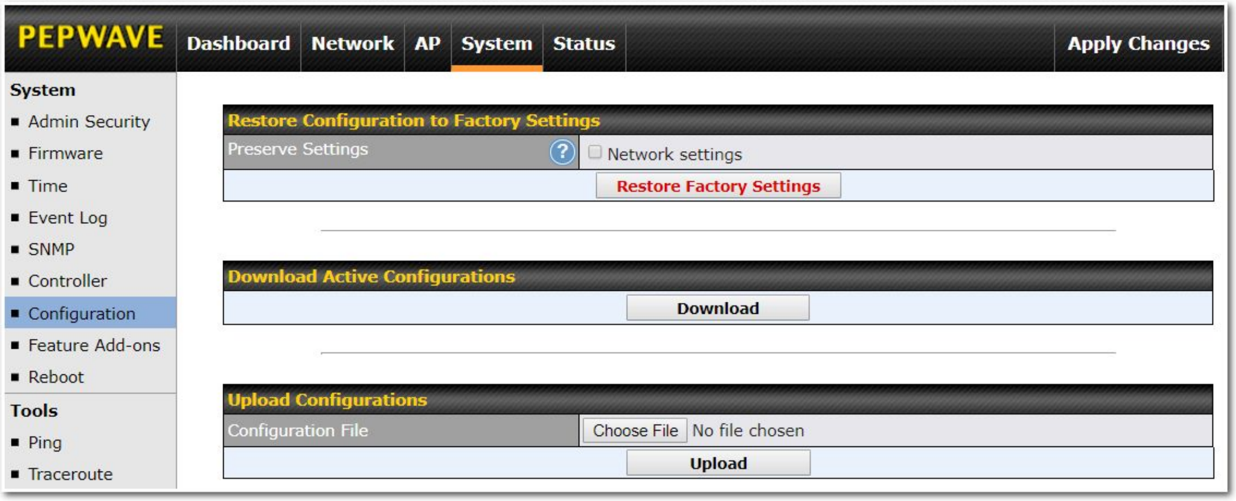
Controller Management	Controller management is enabled when ticked, when untickerd the Access Point is configured through the Web Admin GUI
Controller Type	This setting specifies via a drop-down menu one of the following valid authentication protocols: ● Auto - AP automatically assigned to active AP Controller ● InControl - AP is controlled by InControl* ● AP Controller - AP is controlled by Peplink Valance witH AP controller feature
Privately Host InControl	Pprivately host InContro Appliancel.Check the box besidse 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**.



Restore Configuration to Factory Settings

Preserve Settings ? □ Network settings

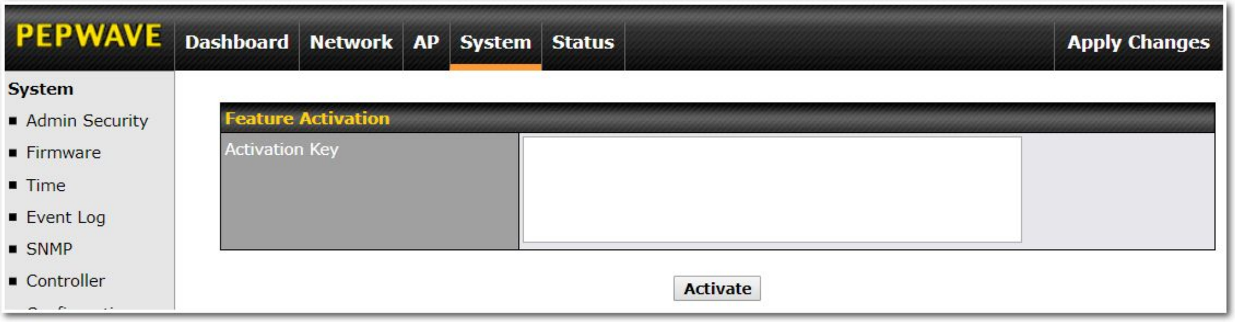
Download Active Configurations

Upload Configurations

Configuration File: No file chosen

Configuration	
Restore Configuration to Factory Settings	The **Restore Factory Settings** button is to reset the configuration to factory default settings. After clicking the button, you will need to click the **Apply Changes** button on the top right corner to make the settings effective. Tick the **Network Settings** option to include the I P Address, Subnet Mask, Default Gateway, DNS Server and Management VLAN ID
Download Active Configurations	Click **Download** to backup the current active settings.
Upload Configurations	To restore or change settings based on a configuration file, click **Choose File** to locate the configuration file on the local computer, and then click **Upload**. The new settings can then be applied by clicking the **Apply Changes** button on the page header, or you can cancel the procedure by pressing **discard** on the main page of the web admin interface.

9.8 Feature Add-Ons

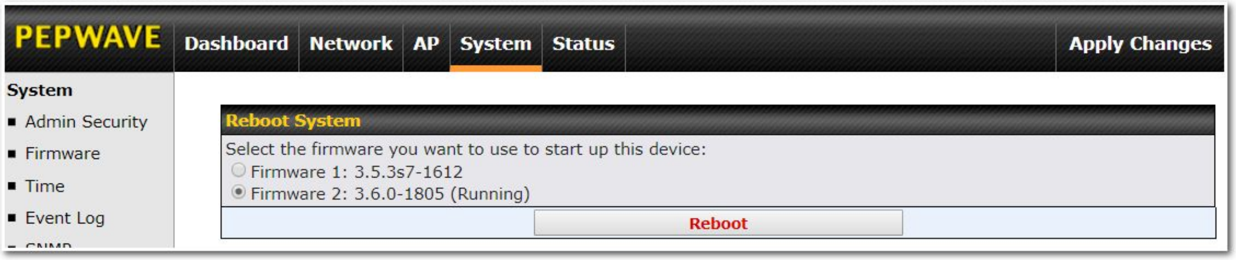


Feature Activation

Activation Key

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 Reboot



Reboot System

Select the firmware you want to use to start up this device:

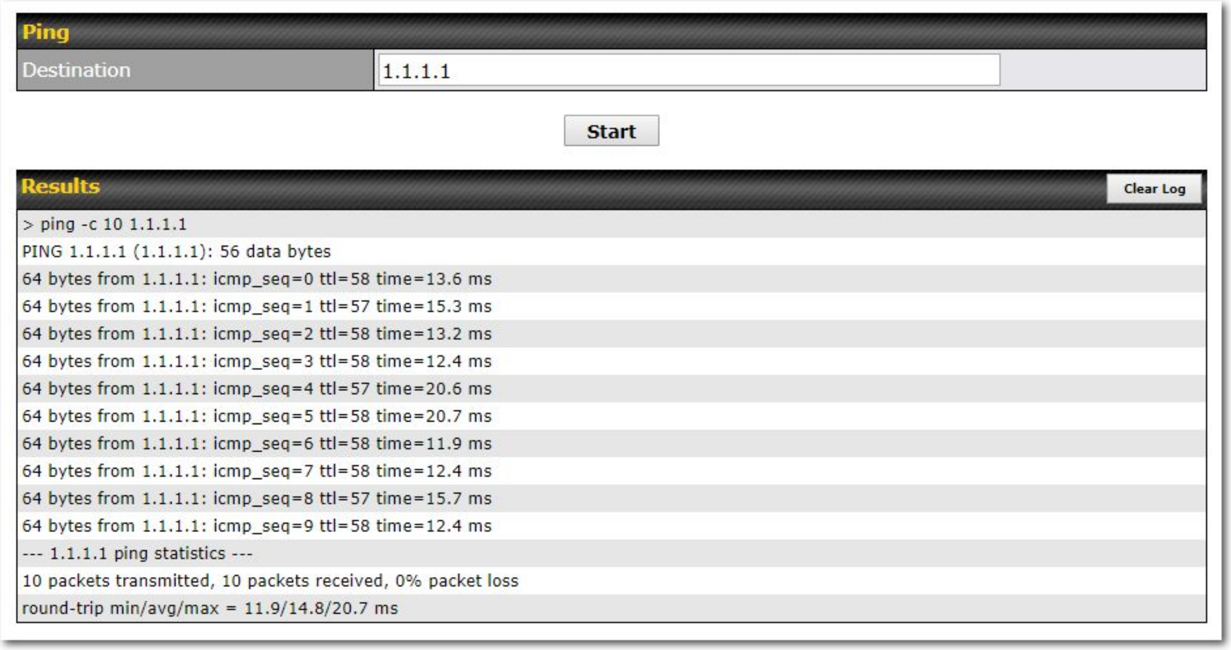
○ Firmware 1: 3.5.3s7-1612

● Firmware 2: 3.6.0-1805 (Running)

Restart the Access Point with the **Reboot** button. For maximum reliability, the Pepwave Access Point can contains 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.

9.10 Tools > Ping

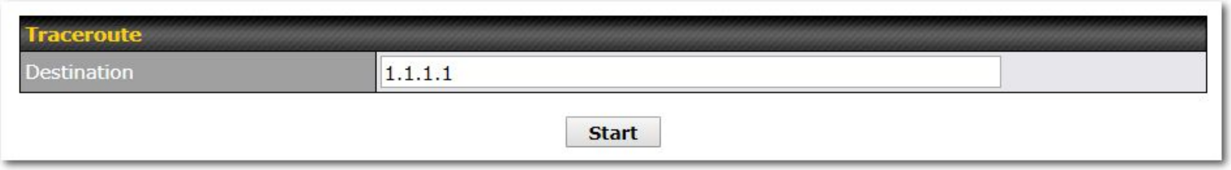


Destination: 1.1.1.1

```
> ping -c 10 1.1.1.1
PING 1.1.1.1 (1.1.1.1): 56 data bytes
64 bytes from 1.1.1.1: icmp_seq=0 ttl=58 time=13.6 ms
64 bytes from 1.1.1.1: icmp_seq=1 ttl=57 time=15.3 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=58 time=13.2 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=58 time=12.4 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=57 time=20.6 ms
64 bytes from 1.1.1.1: icmp_seq=5 ttl=58 time=20.7 ms
64 bytes from 1.1.1.1: icmp_seq=6 ttl=58 time=11.9 ms
64 bytes from 1.1.1.1: icmp_seq=7 ttl=58 time=12.4 ms
64 bytes from 1.1.1.1: icmp_seq=8 ttl=57 time=15.7 ms
64 bytes from 1.1.1.1: icmp_seq=9 ttl=58 time=12.4 ms
--- 1.1.1.1 ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 11.9/14.8/20.7 ms
```

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

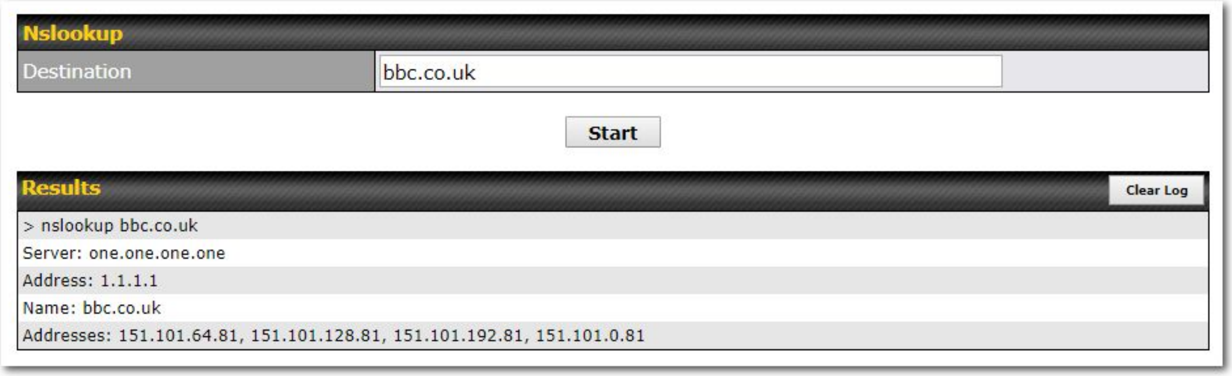
9.11 Tools > Traceroute



Destination: 1.1.1.1

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

9.12 Tools > Nslookup



Destination: bbc.co.uk

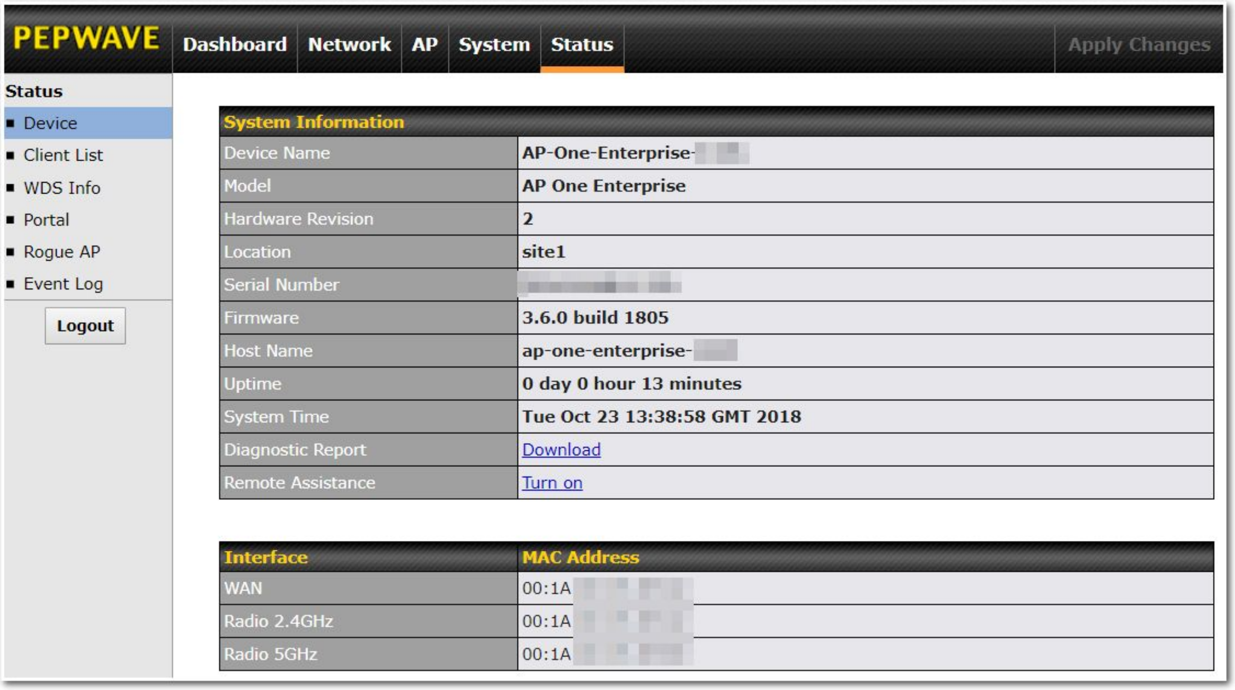
```
> nslookup bbc.co.uk
Server: one.one.one.one
Address: 1.1.1.1
Name: bbc.co.uk
Addresses: 151.101.64.81, 151.101.128.81, 151.101.192.81, 151.101.0.81
```

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

10 Status

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

10.1 Device



System Information	
Device Name	AP-One-Enterprise-[redacted]
Model	AP One Enterprise
Hardware Revision	2
Location	site1
Serial Number	[redacted]
Firmware	3.6.0 build 1805
Host Name	ap-one-enterprise-[redacted]
Uptime	0 day 0 hour 13 minutes
System Time	Tue Oct 23 13:38:58 GMT 2018
Diagnostic Report	Download
Remote Assistance	Turn on

Interface	MAC Address
WAN	00:1A[redacted]
Radio 2.4GHz	00:1A[redacted]
Radio 5GHz	00:1A[redacted]

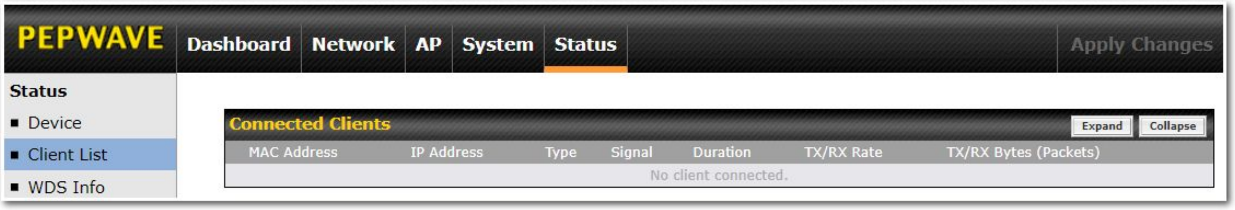
System Information	
Device Name	This is the name specified in the **Router Name** field located at **System>Admin Security**.
Model	This shows the model name and number of this device.
Hardware Revision	This shows the hardware version of this device.
Serial Number	This shows the serial number of this device.
Firmware	This shows the firmware version this device is currently running.
Host name	This shows the hostname of the device.
Uptime	This shows the length of time since the device has been rebooted.
System Time	This shows the current system time.
Diagnostic Report	The **Download** link is for exporting a diagnostic report file required for system investigation.

Remote Assistance	Click **Turn on** to enable remote assistance.

The second table shows the MAC address of each LAN/WAN?Radio 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

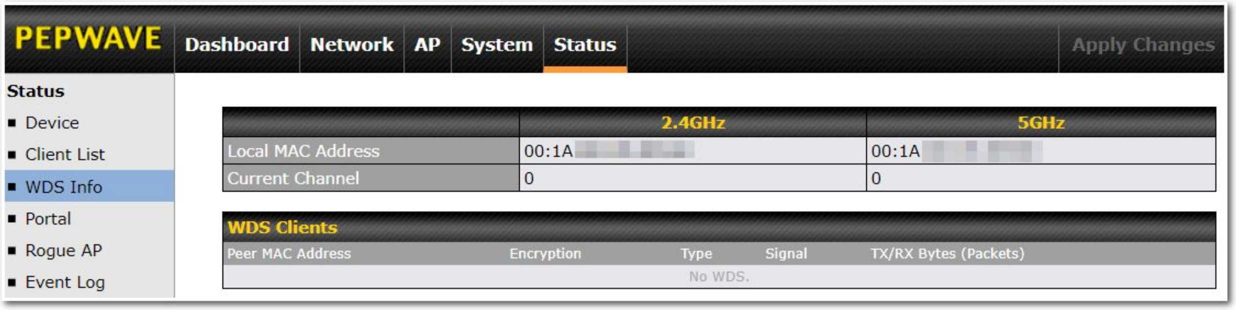


Connected Clients

MAC Address	IP Address	Type	Signal	Duration	TX/RX Rate	TX/RX Bytes (Packets)
No client connected.						

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

10.3 WDS Info



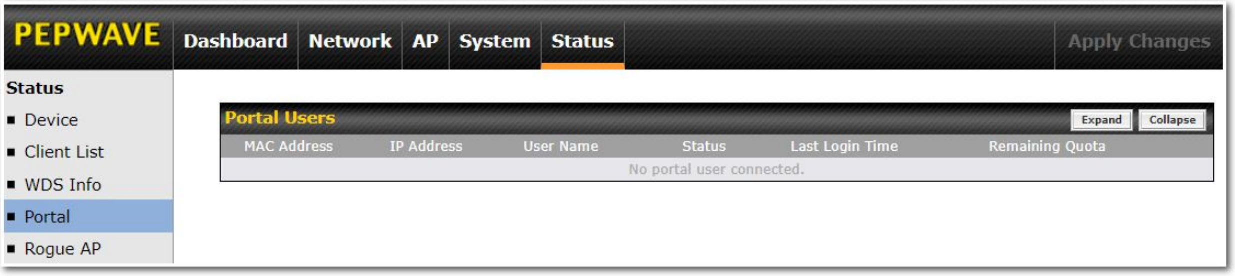
	2.4GHz	5GHz
Local MAC Address	00:1A[redacted]	00:1A[redacted]
Current Channel	0	0

WDS Clients

Peer MAC Address	Encryption	Type	Signal	TX/RX Bytes (Packets)
No WDS.				

Here you can monitor the status of your wireless distribution system (WDS) and track activity by MAC address. This section will display information for both the 2.4GHz and 5GHz radios.

10.4 Portal

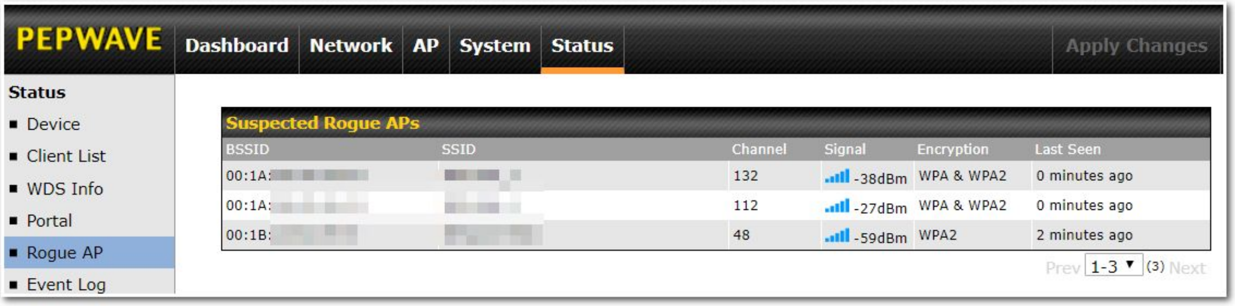


Portal Users Expand Collapse

MAC Address	IP Address	User Name	Status	Last Login Time	Remaining Quota
No portal user connected.					

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



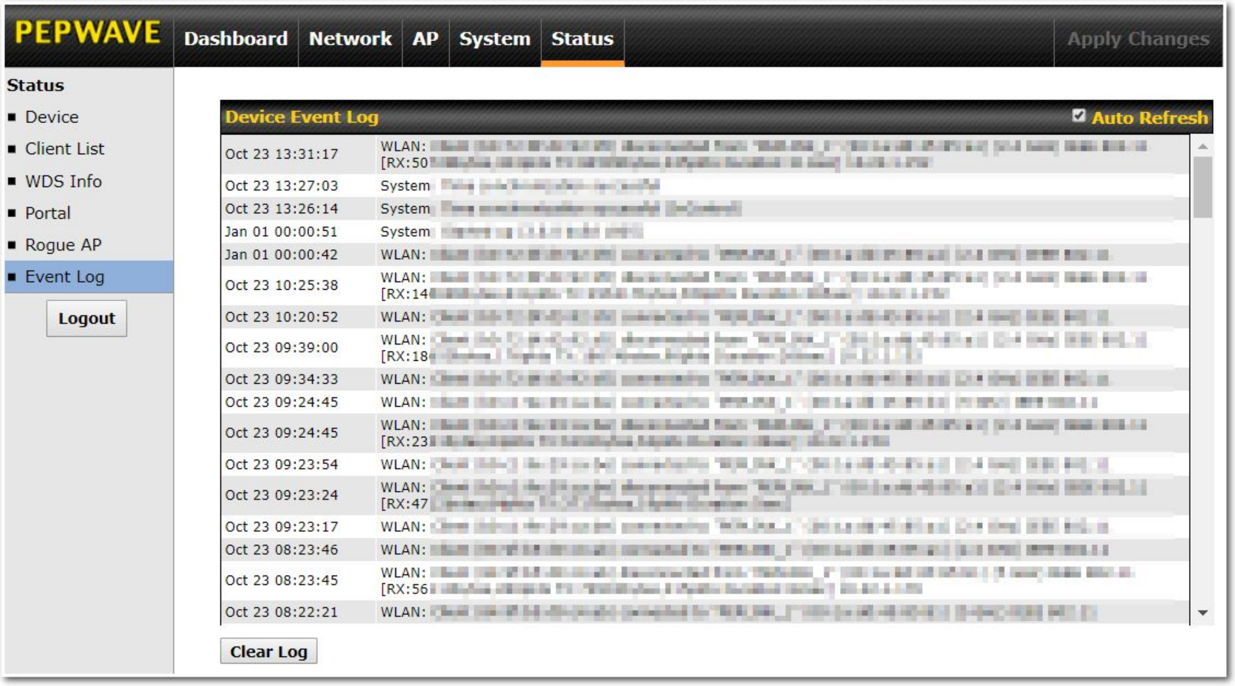
Suspected Rogue APs

BSSID	SSID	Channel	Signal	Encryption	Last Seen
00:1A:[redacted]	[redacted]	132	-38dBm	WPA & WPA2	0 minutes ago
00:1A:[redacted]	[redacted]	112	-27dBm	WPA & WPA2	0 minutes ago
00:1B:[redacted]	[redacted]	48	-59dBm	WPA2	2 minutes ago

Prev 1-3 ▼ (3) Next

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

10.6 Event Log



```
Oct 23 13:31:17   WLAN: [redacted]
                  [RX:50[redacted]
Oct 23 13:27:03   System [redacted]
Oct 23 13:26:14   System [redacted]
Jan 01 00:00:51   System [redacted]
Jan 01 00:00:42   WLAN: [redacted]
Oct 23 10:25:38   WLAN: [redacted]
                  [RX:14[redacted]
Oct 23 10:20:52   WLAN: [redacted]
Oct 23 09:39:00   WLAN: [redacted]
                  [RX:18[redacted]
Oct 23 09:34:33   WLAN: [redacted]
Oct 23 09:24:45   WLAN: [redacted]
Oct 23 09:24:45   WLAN: [redacted]
                  [RX:23[redacted]
Oct 23 09:23:54   WLAN: [redacted]
Oct 23 09:23:24   WLAN: [redacted]
                  [RX:47[redacted]
Oct 23 09:23:17   WLAN: [redacted]
Oct 23 08:23:46   WLAN: [redacted]
Oct 23 08:23:45   WLAN: [redacted]
                  [RX:56[redacted]
Oct 23 08:22:21   WLAN: [redacted]
```

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

The following procedure restores the settings of your access point to factory defaults:

- Power on the unit and wait for one minute.
- Press and hold the reset button for at least 20 seconds, then release.
- The unit will automatically reboot.
- Wait for one minute or until the status LED turns green, upon which the settings of the device will have been restored to the factory defaults.

By default, the unit will acquire an IP address from a DHCP server.

12 Appendix

Federal Communication Commission Interference Statement

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

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

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

IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

IMPORTANT NOTE

FCC 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 of 20cm between the radiator & your body.

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

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

13 Datasheets

Installation guide for AP One In-Wall :

http://download.peplink.com/resources/pepwave-ap-one-in-wall-installation-guide.pdf

COPYRIGHT & TRADEMARKS

Contact Us:

Saleshttp://www.pepwave.com/contact/sales
/