

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.

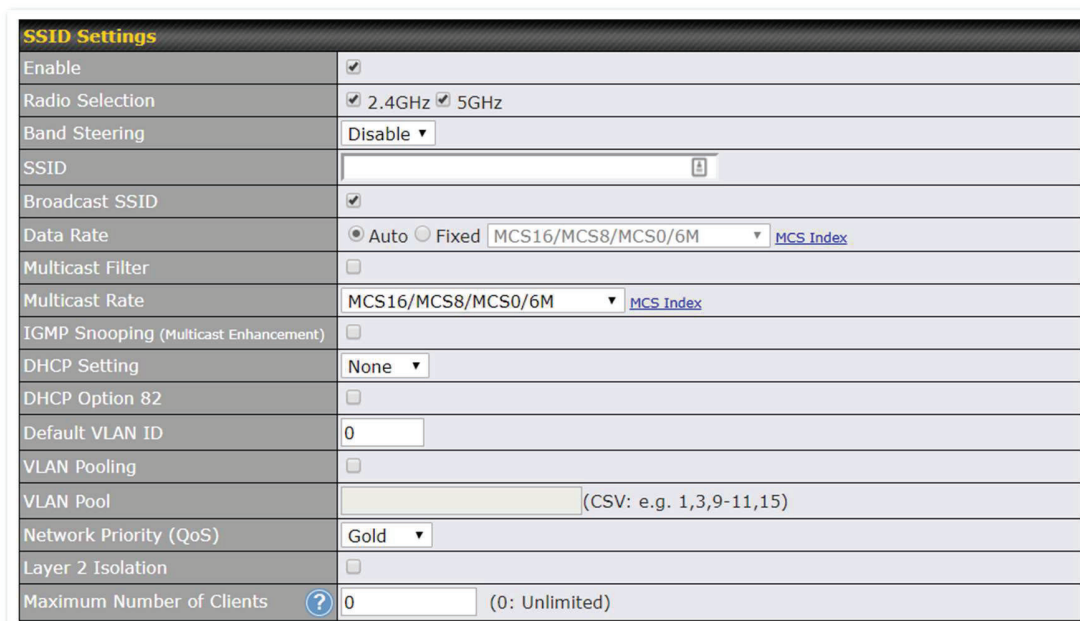
8.1 Wireless SSID



The screenshot shows the PEPWAVE web interface with the 'AP' tab selected. The 'Wireless SSID' sub-tab is active. A message indicates 'InControl management enabled. Wireless SSID can now be configured on InControl.' Below this, there is a table with columns: 'Wireless Network SSID', 'Security Policy', and 'MAC Address (BSSID)'. The first row shows 'PEPLINK_1' as the SSID, 'WPA and WPA2 (PSK)' as the security policy, and two MAC addresses: '00:1A:00:00:00:00' and '00:1A:00:00:00:00'. A 'New SSID' button is located at the bottom right of the table.

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 various settings for the wireless network, including checkboxes for 'Enable', 'Broadcast SSID', 'Multicast Filter', 'IGMP Snooping (Multicast Enhancement)', 'DHCP Option 82', 'VLAN Pooling', and 'Layer 2 Isolation'. There are also dropdown menus for 'Radio Selection' (2.4GHz, 5GHz), 'Band Steering' (Disable), 'Data Rate' (Auto, Fixed), 'Multicast Rate' (MCS16/MCS8/MCS0/6M), 'DHCP Setting' (None), 'Default VLAN ID' (0), 'VLAN Pool' (CSV: e.g. 1,3,9-11,15), 'Network Priority (QoS)' (Gold), and 'Maximum Number of Clients' (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 the 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

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**.

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 – Enterprise

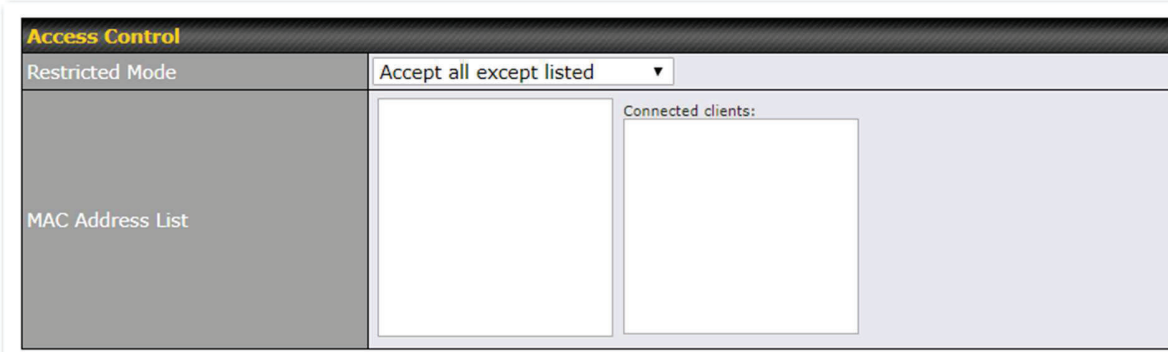
802.1X Version

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**.

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 the 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.



The screenshot shows the 'Access Control' section of a web interface. It features a 'Restricted Mode' dropdown menu currently set to 'Accept all except listed'. Below this, there is a 'MAC Address List' table with two columns: 'MAC Address' and 'Connected clients'. The table is currently empty.

Access Control	
Restricted Mode	The settings allow the 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 X .
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 X .
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 ▼

OK

Cancel

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 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.

Schedule

☐ 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 μ s Default	
ACK Timeout	48 μ s 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	☒

AP Settings

Protocol

Choose **802.11ng** or **802.11n/ac** as your access point's Wi-Fi protocol.
 The AP One AC mini provides the **802.11ng** protocol for the 2.4 GHz band and the **802.11n/ac** protocol for the 5GHz band, as shown below.

AP Settings	2.4GHz	5GHz
Protocol	802.11ng ▼	802.11n/ac ▼

Operating Country

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

	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 802.11n/g. 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 802.11n/a. 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.

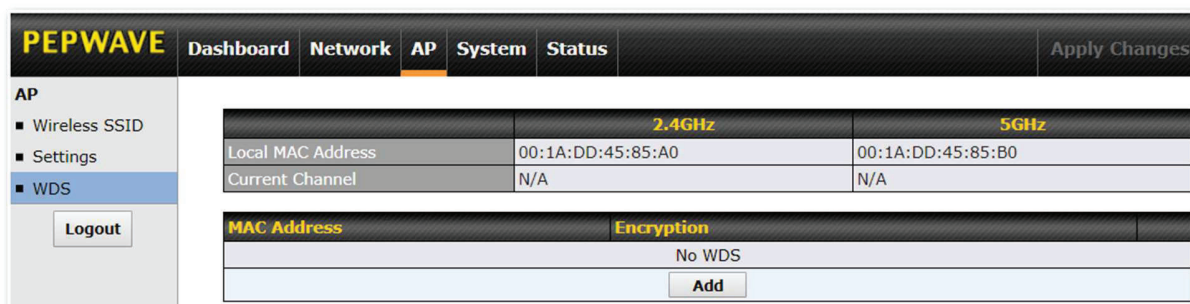
Advanced Features																																																									
Discover Nearby Networks	☒ * Discover Nearby Networks will be enabled if Channel is set to Auto																																																								
Scanning Interval	10 s																																																			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

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 .

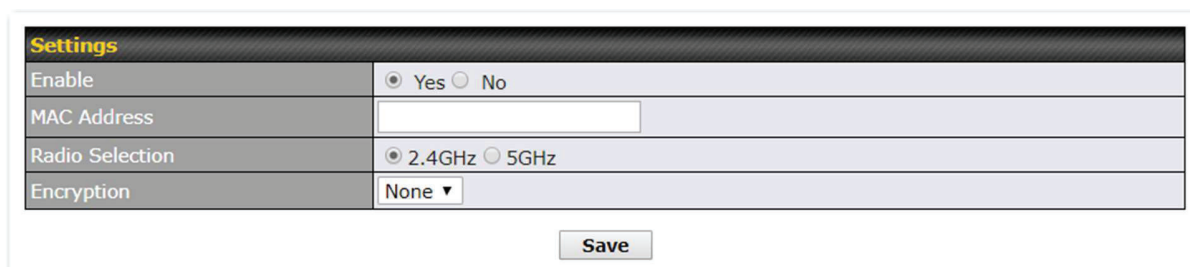
8.3 WDS

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.



The screenshot shows the PEPWAVE web interface. The top navigation bar includes 'Dashboard', 'Network', 'AP' (selected), 'System', and 'Status'. On the left sidebar, 'WDS' is selected under the 'AP' section. The main content area displays WDS configuration for 2.4GHz and 5GHz bands. It shows 'Local MAC Address' as 00:1A:DD:45:85:A0 and 'Current Channel' as N/A. Below this, there's a section for 'MAC Address' and 'Encryption' with a 'No WDS' status and an 'Add' button.

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



The screenshot shows the 'Settings' form for WDS. It includes fields for 'Enable' (radio buttons for Yes/No), 'MAC Address' (text input), 'Radio Selection' (radio buttons for 2.4GHz/5GHz), and 'Encryption' (dropdown menu set to 'None'). A 'Save' button is at the bottom.

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- hostname: ap-one-enterprise
Location	
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.