

PEP WAVE

User Manual

Pepwave OfficePoint Indoor Series

200 / 400

Pepwave OfficePoint Outdoor Series

400-DX

Document Rev.2.1.6

Dec-10

COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice. Copyright © 2010 Pepwave Ltd. All Rights Reserved. Pepwave and the Pepwave logo are trademarks of Pepwave Ltd. Other brands or products mentioned may be trademarks or registered trademarks of their respective owners.

Table of Contents

1	INTRODUCTION AND SCOPE	3
2	PRODUCT FEATURES	4
3	PACKAGE CONTENTS	5
4	PEPWAVE OFFICEPOINT OVERVIEW	6
4.1	FRONT VIEW	6
4.2	REAR PANEL VIEW	7
5	INSTALLATION	9
5.1	INSTALLATION PROCEDURES	9
6	INFORMATION	10
6.1	SYSTEM	10
6.2	WIRELESS	11
6.3	AUTOMESH	15
7	CONFIGURATION	16
7.1	SYSTEM	16
7.2	WIRELESS NETWORKS	20
7.3	ADVANCED WIRELESS SETTINGS	33
7.4	AUTOMESH	36
7.5	SNMP	37
7.6	WEB ADMINISTRATION	40
8	TOOLS - DIAGNOSTIC TOOLS	42
9	COMMANDS	43
9.1	ACTIVATE CHANGES	43
9.2	FIRMWARE	44
9.3	CONFIGURATION	45
9.4	MISC	46
10	RESTORATION OF FACTORY DEFAULTS	47
10.1	OFFICEPOINT INDOOR SERIES	47
10.2	OFFICEPOINT OUTDOOR SERIES	47
	APPENDIX A	48
	APPENDIX B	49

1 Introduction and Scope

Pepwave OfficePoint is an enterprise grade 802.11b/g Wi-Fi access point with centralized management system. It is a powerful solution for building wireless networks for all business needs. Each Pepwave OfficePoint is loaded with essential features such as Multiple SSID, VLAN, AutoMesh and Guest Protect.

One Pepwave OfficePoint can masquerade up to 4 different access points. Each virtual access point can have its own security policy (e.g. WPA, WPA2, etc.) and authentication mechanism (e.g. 802.1x, open, captive portal, etc), to facilitate building your network much faster, easier and more cost-effective than ever before. Pepwave OfficePoint comes with a high-power Wi-Fi transmitter which greatly enhances coverage and performance.

This manual applies to Pepwave OfficePoint indoor models 200, 400 and outdoor models 400-DX.

2 Product Features

Key features of Pepwave OfficePoint:

- High-power output enhances coverage and lowers cost of ownership
- Independent security policies and encryption mechanisms per virtual AP
- Centralized management via InControl
- AutoMesh Support for secure and fast network expansion
- Guest Protect Support
- WMM (Wi-Fi Multimedia) and QoS (Quality of Service) Support

3 Package Contents

The following items are the contents of a Pepwave OfficePoint indoor package:

- 1 x Pepwave OfficePoint indoor unit
- 1 x Omni-directional antenna
- 1 x Power Supply Unit
- 1 x Passive PoE
- 1 x Instruction Sheet

The following items are the contents of a Pepwave OfficePoint outdoor package:

- 1 x Pepwave OfficePoint outdoor unit
- 1 x 13dBi patch antenna
- 1 x Power Supply Unit
- 1 x Passive PoE
- 1 x Mounting Kit
- 1 x Instruction Sheet
- 1 x Installation Guide

4 Pepwave OfficePoint Overview

4.1 Front View



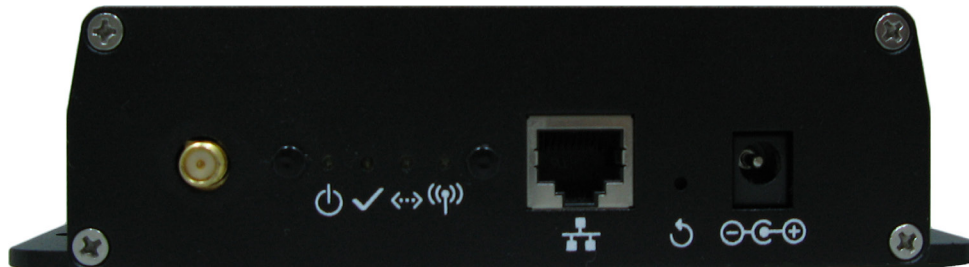
OfficePoint 200, 400



OfficePoint 400-DX

4.2 Rear Panel View

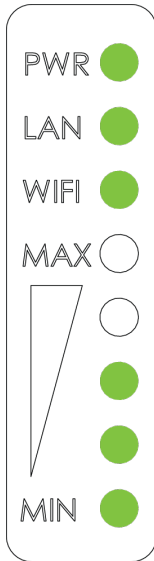
4.2.1 OfficePoint indoor series



Connectors	
Antenna (Left-most Connector)	A RP-SMA connector for connecting the antenna.
LAN	A 10/100BaseT Ethernet connector, normally to be connected to back haul network.
Reset	Reset button to be depressed with a pin. Depress and hold for at least 5 seconds to restore factory defaults. For further details, please refer to Section 11, Restoration of Factory Defaults .
Power Connector	A connector for DC 12V power input, to be connected with the supplied power adaptor.

LED Indicators	
Power	OFF – Power off ON – Power on
Status	OFF – The unit is initializing. ON – The unit is ready.
Ethernet	OFF – The Ethernet port is not connected. ON – The Ethernet port is connected.
Wireless	OFF – Wireless is not ready. On – Wireless is ready.

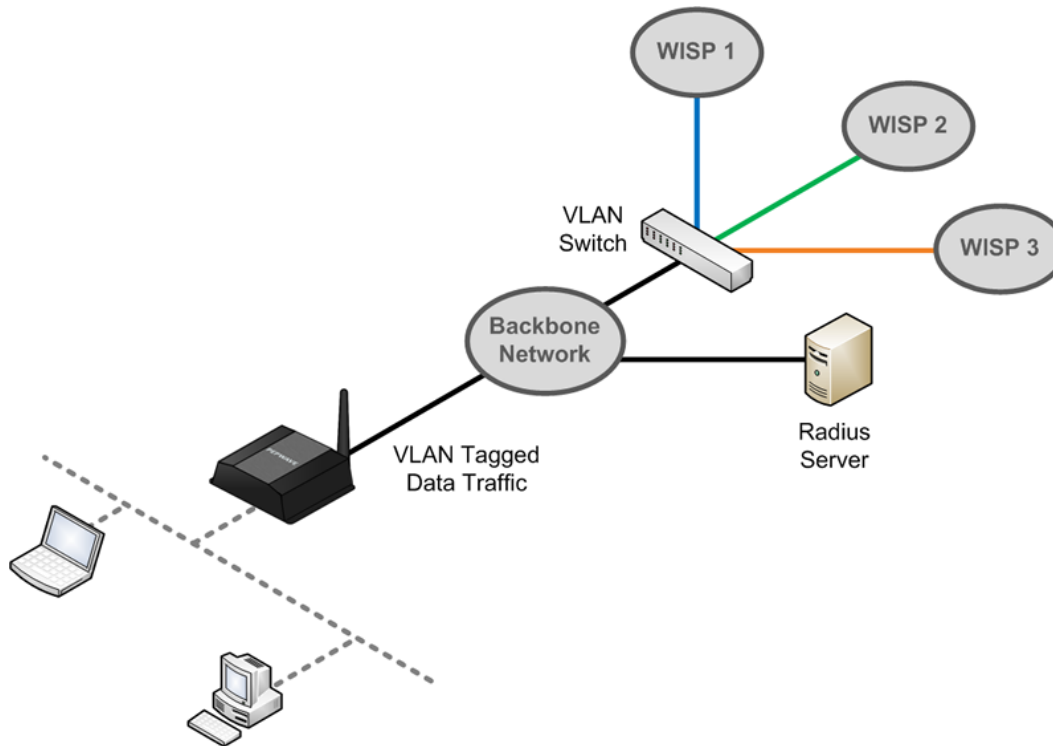
4.2.2 OfficePoint 400-DX



LED Indicators	
PWR	OFF – Power off ON – Power on
LAN	OFF – Ethernet is not connected ON – Ethernet is connected
WIFI	Wi-Fi is ready. The number of Wi-Fi LED lights from “MIN” to “MAX” indicates the number of clients associated. One LED on: 1-10 clients; Two LEDs on: 11-20 clients; Three LEDs on: 21-30 clients; Four LEDs on: 31-40 clients; Five LEDs on: 40 clients above. Off: Wi-Fi is not ready

5 Installation

Pepwave OfficePoint acts as a bridge between the wireless and the wired Ethernet interface. A typical setup is as follows:



5.1 Installation Procedures

1. Attach the antenna to the Pepwave OfficePoint unit.
2. Connect the LAN port on the unit with the backbone network using an Ethernet cable. The port could auto sense the cable is straight-through or cross-over.
3. Connect the power adapter to the power connector of the unit, and then plug in the power adapter.
4. Wait for the status LED to turn green.
5. Connect a PC to the backbone network, and configure the IP address of the PC to be any IP address between 192.168.0.4 and 192.168.0.254, with subnet mask of 255.255.255.0.
6. With Microsoft Internet Explorer 6 or above, or Mozilla Firefox 2.0 or above, connect to the URL <https://192.168.0.3>.
7. When prompted, enter the default admin login ID and password, admin and public respectively.
8. After logging in, the following Information main page appears. Please go to **Configure > System** to facilitate further configuration of the Pepwave OfficePoint unit.

6 Information

PEPWAVE OfficePoint

Information

- System
- Wireless
- AutoMesh

Configure

- System
- Wireless Networks
- Advanced Wireless
- AutoMesh
- SNMP
- Web Administration

Tools

- Diagnostic Tools

Commands

- Activate Changes
- Firmware
- Configuration
- Misc

Real Time Status

Status: Running

System Information

System

AP Name	OfficePoint
Location	site1
Network IP Information	192.168.1.77 / 24 (Detail)
System Time	Tue Jun 22 20:48:48 PST 2010
Up Time	0 day, 20:58:49

PePWave OfficePoint (2.1.1)

6.1 System

Information

- System
- Wireless
- AutoMesh

Configure

- System
- Wireless Networks
- Advanced Wireless
- AutoMesh
- SNMP
- Web Administration

Tools

- Diagnostic Tools

Commands

- Activate Changes
- Firmware
- Configuration
- Misc

Real Time Status

Status: Running

System Information

System

AP Name	OfficePoint
Location	site1
Network IP Information	192.168.1.77 / 24 (Detail)
System Time	Tue Jun 22 20:48:48 PST 2010
Up Time	0 day, 20:58:49

PePWave OfficePoint (2.1.1)

System Information	
AP Name	This field shows the name of the system entered in the configuration.
Location	This field shows the location entered in the configuration.
Network IP Information	This shows the current IP used on the system.
System Time	This shows the time of day in respect to the time zone selected.
Up Time	This shows the time has been up since boots up.

Click on the **Detail** link beside the **Network IP Information** to check the following system information: IP Address Mode, IP Address, Subnet Mask, Default Gateway, DNS Server.

6.2 Wireless

Wireless Information

AP Info | Connected Clients | Nearby Networks

Number of Wireless Networks: 1
 Number of Connected Clients: 0
 Current Channel: 1

Wireless Network SSID	Broadcast SSID	Security Policy	Default VLAN ID	MAC Address(BSSID)
OfficePoint	Enable	Open - No Encryption	0	00:1A:DD:A6:4E:81 Info Stat

PePWave OfficePoint (2.1.1)

Real Time Status
 Status: Running

6.2.1 AP Info

Wireless Information – AP Info	
Number of Wireless Networks	This indicates the number of wireless networks.
Number of Connected Clients	This indicates the number of associated clients.
Current Channel	This shows which 802.11 channel the system is using.
Wireless Network SSID	This shows which SSID the client is associated.
Broadcast SSID	This setting shows whether or not the ESSID of the virtual AP can be scanned by Wi-Fi clients.
Security Policy	This setting shows the wireless authentication and encryption methods.
Default VLAN ID	This setting shows the VLAN ID tagged on all outgoing packets generated from the virtual AP.
MAC Address (BSSID)	This shows the detailed BSSIDs.

Click on the **Info** link to check the following wireless information: **Web Portal Login**, **Wireless Network Firewall**, **MAC Filter**, **Bandwidth Control**, **Layer 2 Isolation**.

INFO Close	
Web Portal Login	InControl
MAC Filter	None
Bandwidth Control	Disable
Layer 2 Isolation	Disable

Click on the **Stat** link to check the following networking statistics: **Packets Sent**, **Bytes Sent**, **Packets Received**, **Bytes Received**.

STAT Close	
Packets Sent	142
Bytes Sent	19025
Packets Received	0
Bytes Received	0

User Manual

Pepwave OfficePoint Series

6.2.2 Connected Clients

Manufacturer	MAC Address	Signal	Network SSID	Authentication Status	Type	Connection Length	
Client A	00:11:aa:bb:cc:dd	Good	Pepwave OfficePoint Wi-Fi	Open - No Encryption (authenticated)	802.11g	associated (00:00:15)	Details

Wireless Information – Connected Clients	
Manufacturer	This shows the manufacturer based on the MAC prefix.
MAC address	This shows the client MAC address.
Signal	This shows the signal strength.
Network SSID	This shows which SSID the client is associated.
Authentication Status	This shows the client authentication method(s).
Type	This shows the radio mode of the client.
Connection Length	This shows the associated duration.

Click on the **Details** link, more networking statistics will be provided.

DETAIL Close	
Vendor	Client A
MAC Address	00:11:aa:bb:cc:dd
Protocol	802.11g
IP Address	192.168.1.10
Network SSID	Pepwave Office Point Wi-Fi
Connection Length	associated (00:00:05)
Authentication Status	Open - No Encryption (authenticated)
Username	
Domain	
VLAN ID	0
Network Priority Level	Gold
Bytes Received	70185
Bytes Sent	32421
Packets Received	642
Packets Sent	512
Receive Errors	0
Transmit Errors	0
Duplicates Received	2
Receive Retries	27
Transmit Retries	74
Transmit Excessive Retries	0
Receive Data Rate	54M
Transmit Data Rate	54M
Signal (RSSI)	Excellent (58)

User Manual

Pepwave OfficePoint Series

Wireless Information – Connected Clients - Details	
Vendor	This shows the manufacturer based on the MAC prefix.
MAC Address	This shows the client MAC address.
Protocol	This shows the radio mode of the client.
IP Address	This shows the IP address of connected client.
Network SSID	This shows which SSID the client is associated.
Connection Length	This shows the associated duration.
Authentication Status	This shows the client authentication method(s).
Username	This shows the user name of the connected client.
Domain	This shows the domain name of the connected client.
VLAN ID	This shows the VLAN ID of the connected client.
Network Priority Level	This shows the priority level of internet transfers of this connect client.
Bytes Received	This shows the transmitted size this client received from the AP.
Bytes Sent	This shows the transmitted size this client sent out to the AP.
Packets Received	This shows the packet number this client received from the AP.
Packets Sent	This shows the packet number this client sent out to the AP.
Receive Errors	This shows the number of errors this client received from the AP.
Transmit Errors	This shows the number of errors this client transmitted to the AP.
Duplicates Received	This shows the number of duplicates received by the client from the AP.
Receive Retries	This shows the number of retries this client received from the AP.
Transmit Retries	This shows the number of retries this client transmitted to the AP.
Transmit Excessive Retries	This shows the number of excessive retries this client transmitted to the AP.
Receive Data Rate	This shows the receive data rate of the client from the AP.
Transmit Data Rate	This shows the transmit data rate of the client to the AP.
Signal (RSSI)	This shows the signal strength received by the client.

6.2.3 Nearby Networks

Network Discovery	Enable						
Scanning Interval	10 s						
Scanning Time	50 ms						
Group by: <input type="button" value="None"/>							
Manufacturer	SSID	Security	MAC Address	Channel	Signal (RSSI)	Last Seen	Status
PePWave Ltd	SSID_Home	wpa	00:1a:2b:3c:4d:5	1	Excellent (37)	14:14 07-30	down

Wireless Information – Nearby Networks	
Network Discovery	This shows if the AP would scan and discover nearby network.
Scanning Interval	This shows how often the AP goes to other channels to discover nearby AP.
Scanning Time	This shows how long the AP stays on the other channels to discover a nearby AP.
Manufacturer	This shows the manufacturer based on the MAC prefix.
SSID	This shows which SSID the client is associated.
Security	This shows the client authentication method(s).
MAC address	This shows the client MAC address.
Channel	This shows the channel of the existing Bssid.
Signal (RSSI)	This shows the signal strength.
Last Seen	This indicates the time stamp of the access point sc
Status	This shows the current status of this nearby network.

6.3 AutoMesh

6.3.1 AutoMesh Info

AutoMesh Info	
Mesh ID (MAC Address)	This shows the MAC address of the AutoMesh node.
Parent	This shows the parent node of the wireless node.
Channel	This shows the channel of the existing Bssid.
Level	This shows the hop level of the wireless node.
State	This shows the state of the node: wired or wireless.

6.3.2 Neighbor AutoMesh Members

Mesh ID	Parent	Channel	Signal (SNR)	Level	State
00:1a:2b:3c:4d:5e	00:11:22:33:44:55	3	Excellent (26)	1	wireless
00:aa:bb:cc:dd:ee	00:11:22:33:44:56	3	Good (18)	1	wireless
00:ab:cd:ef:11:22	00:11:22:33:44:57	3	Poor (5)	2	wireless

AutoMesh Status – Neighbor AutoMesh Members	
Mesh ID	This shows the wireless MAC address of the Neighbor WDS node.
Parent	This shows the parent node of the Neighbor WDS node.
Channel	This shows the channel of the existing Bssid.
Signal (SNR)	This value shows the signal strength of the neighbor AutoMesh members.
Level	This shows the signal strength of the node.
State	This shows the hop level of the node.

7 Configuration

PEPWAVE OfficePoint

The screenshot shows the configuration page for the PePWave OfficePoint system. The left navigation bar has the 'Configure' section expanded, with 'System' highlighted. The main content area is titled 'System' and has two tabs: 'Basic' and 'Advanced'. The 'Basic' tab is active, showing a form with the following fields: 'AP Name' (OfficePoint), 'Location' (site1), 'Timezone' (US/Pacific), 'Domain Name' (empty), 'Keep Default IP' (checked, Enable), and 'IP Address Mode' (Automatic). Below the form are 'Save' and 'Save to flash and activate' buttons. At the bottom, it says 'PePWave OfficePoint (2.1.1)'.

7.1 System

Upon selecting **System** under **Configure** section from the navigation bar on the left, the following page shows the configuration options:

This screenshot is identical to the one above, but the 'System' option in the left navigation bar is highlighted with a yellow box, indicating it is the selected configuration section.

7.1.1 Basic

System Settings - Basic	
AP Name	A user-specified name for the access point. This value can be retrieved via SNMP.
Location	A user-specified name for the location of the access point. This value can be retrieved via SNMP.
Time zone	This option specifies the time region to be used for representing the time on the system.

User Manual

Pepwave OfficePoint Series

Domain Name	Domain name can be set for wireless clients to have a readable name for the web management.
Keep Default IP	With this option disabled, default IP 192.168.0.3 of the device will be disabled.
IP Address Mode	<p>The options are Automatic and Manual.</p> <p>Automatic: IP address of the Pepwave OfficePoint unit is acquired from a DHCP server on the Ethernet segment.</p> <p>Manual: A user-specified IP address is used.</p> <p>PPPoE: IP address is obtained through PPPoE. PPPoE is only supported on Router mode, please refer to the below table: System Settings - Advanced for more details.</p>
IP Address Mode – Manual	
Static IP Address	<p>This specifies the unique IP address for the Pepwave OfficePoint unit to communicate on the Ethernet segment.</p> <p>This IP address is distinct from the admin IP address 192.168.0.3 on the Ethernet segment.</p>
Subnet Mask	This setting specifies the subnet mask of the Pepwave OfficePoint unit.
Default Gateway	This setting specifies the default gateway of the Pepwave OfficePoint unit.
DNS Server	This is the DNS server address to be used by the Pepwave OfficePoint unit for resolving host names.
IP Address Mode – PPPoE	
PPPoE Username	This specifies the username required in order to connect via PPPoE to acquire Internet connectivity. The information is typically determined by and can be obtained from the ISP.
PPPoE Password	This specifies the password required in order to connect via PPPoE to acquire Internet connectivity. The information is typically determined by and can be obtained from the ISP.
PPPoE Service Name	<p>This is a PPPoE parameter which is provided by the ISP.</p> <p>Note: Leave this field empty if you are not sure.</p>

7.1.2 Advanced

Basic Advanced

Management VLAN ID: 0

NTP Server: pool.ntp.org
 Enable

Scheduled Reboot
Schedule: Weekly Day: Sunday Time: 00:00

Ethernet Speed/Duplex: auto

AP Mode: Bridge
Bridge
Router

Save Save to flash and activate

System Settings - Advanced

Management VLAN ID	This specifies the VLAN from which management sessions are allowed. The establishment of management sessions is restricted only to the specified VLAN ID. If Management VLAN ID is set to zero, no VLAN restriction is applied. The default value of this setting is zero . It means no tagging is enabled (instead of tagged with zero).
NTP Server	This is the Network Time Protocol (NTP) Server hostname to be used for synchronizing system clock of Pepwave OfficePoint. The default value of this setting is pool.ntp.org .
Scheduled Reboot	The system would perform reboot based on the scheduled time set. Click the box above the Schedule to Enable this feature.
Ethernet Speed/Duplex	This setting provides the option to set the speed of the Ethernet.
AP Mode	Available options are Bridge and Router . With this option set as Router, the following Manual Router Settings will be available.

7.1.3 Manual Router Settings

Manual Router Settings will only be available when the AP Mode in the previous section had been selected as **Router** mode. You can use the OfficePoint as a DHCP server for other devices behind.

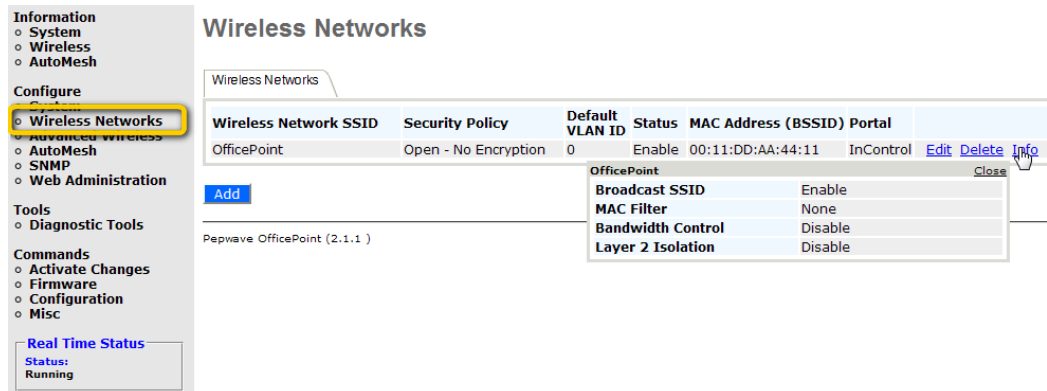
Manual Router Settings

LAN IP	192.168.1.1
LAN Subnet Mask	255.255.255.0
DHCP Server	<input checked="" type="checkbox"/> Enabled
IP Start Range	192.168.1.100
IP Stop Range	192.168.1.200
Subnet Mask	255.255.255.0
Broadcast Address	192.168.1.255
Gateway	192.168.1.1
DNS 1	192.168.1.1
DNS 2	
DNS 3	
Lease Time	3600 seconds

DHCP Server Parameters	
LAN IP	This setting specifies the DHCP server IP address.
LAN Subnet Mask	This setting specifies the subnet mask of the DHCP server.
IP Start Range	This setting specifies the first address in the range of IP addresses to be assigned to DHCP clients.
IP Stop Range	This setting specifies the last address in the range of IP addresses to be assigned to DHCP clients.
Subnet Mask	This setting specifies the subnet mask to be used by DHCP clients.
Broadcast Address	This setting specifies the broadcast address to be used by DHCP clients.
Gateway	This setting specifies the default routing gateway to be used by DHCP clients.
DNS 1	This setting specifies the IP address of the primary DNS Server to be offered to DHCP clients.
DNS 2	This setting specifies the IP address of the secondary DNS Server to be offered to DHCP clients.
DNS 3	This setting specifies the IP address of the tertiary DNS Server to be offered to DHCP clients.
Lease Time	This setting specifies the length of time throughout which an IP address of a DHCP client remains valid. Upon expiration of the Lease Time, the assigned IP address will no longer be valid and the renewal of the IP address assignment will be required.

7.2 Wireless Networks

Upon selecting **Wireless Networks** under Configure section from the navigation bar on the left, the following shows the configured SSID available on the system:



General Wireless Networks Settings	
Wireless Network SSID	The SSID of the virtual Access Point (AP).
Security Policies	Shows the configured wireless authentication and encryption methods.
Default VLAN ID	This setting specifies the VLAN ID to be tagged on all outgoing packets generated from the virtual AP (i.e. packets that travel from the Wi-Fi segment, through the Pepwave OfficePoint unit to Ethernet segment via the LAN port). If 802.1x is enabled, a per-user VLAN ID can be specified in the authentication reply from the Radius server. If it is set, the value specified via Default VLAN ID will be overridden.
Status	Shows whether the virtual AP is enabled or disabled.
MAC Address (BSSID)	Shows the detailed BSSIDs.
Portal	Shows if the InControl Guest Portal is enabled. Please refer to section 7.2.2 for details.

To add a new virtual AP, click the **Add** button. To modify the settings for a virtual AP, click the link **Edit** on the right of the desired WLAN SSID, upon which the following **Wireless Network Details** is displayed.

Click on the **Info** link to check the following networking statistics: **Broadcast SSID**, **MAC Filter**, **Bandwidth Control**, **Layer 2 Isolation**.

General Wireless Networks Settings – Info	
Broadcast SSID	This shows if the Broadcast SSID feature of this network is enabled.
MAC Filter	This shows if the MAC Filter feature of this network is enabled.
Bandwidth Control	This shows if the Bandwidth Control feature of this network is enabled.
Layer 2 Isolation	This shows if the Layer 2 Isolation feature of this network is enabled.

7.2.1 Wireless Network Details - Basic

Wireless Networks Details - Basic	
Enable	Select Yes to enable the virtual AP, or No to disable the virtual AP. By default, the virtual AP is enabled .
Wireless Network SSID	This setting specifies the SSID of the virtual AP to be scanned by Wi-Fi clients.
Broadcast SSID	This setting specifies whether or not the ESSID of the virtual AP can be scanned by Wi-Fi clients. Note that the BSSID (i.e. the MAC address of the virtual AP) cannot be hidden from the scan. To associate with the virtual AP, clients must specify the correct ESSID upon association. Broadcast SSID is enabled by default.
Security Level	This setting configures the wireless authentication and encryption methods. Available options are: Open - No Encryption, Static WEP, 802.1X, WPA-TKIP, WPA2-AES:CCMP. Selecting Open - No Encryption disables encryption. For details on the other options, please refer to: 7.2.1.1 - Static WEP Parameters 7.2.1.2 - 802.1x Parameters 7.2.1.3 - WPA Parameters

7.2.1.1 Static WEP

The configuration of Static WEP parameters enables pre-shared WEP key encryption. Authentication is not supported by this method.

The security level of this method is known to be weak.

Static WEP parameters are entered via the following screen upon selection:

Security Level	Static WEP
Key Size	40 bits (64-bit WEP)
Key Format	ASCII
Passphrase	<input type="text"/> <input type="button" value="Generate Key"/>
Encryption Key	<input type="text"/>
Shared Key Authentication	<input type="checkbox"/> Enable

Static WEP Parameters	
Key Size	The setting can be configured as either 40 bits (64-bit WEP) or 104 bits (128-bit WEP) .
Key Format	The setting can be configured as either ASCII or HEX .
Passphrase	Combination of words and characters used to generate an encryption key. Click Generate Key to create the key.
Encryption Key	This setting specifies a user-specified encryption key value. For ASCII format, key length is either 5 or 13 . For HEX format, key length is either 10 or 26 .
Shared Key Authentication	This setting enables the use of shared key authentication. Open authentication is the default authentication.

7.2.1.2 802.1X Parameters

The configuration of 802.1X parameters enables Radius-based 802.1X authentication with a dynamic WEP key. Once selected, Radius Server Setting will be available.

The configuration screen is as follows:

Security Level	802.1X
802.1X Version	<input type="radio"/> V1 <input checked="" type="radio"/> V2
WEP Key Size	40 bits (64-bit WEP)
Re-keying Period	0 seconds (0: Disable)

802.1x Parameters	
802.1X Version	<p>This setting selects between v1 or v2 of the 802.1x EAPOL.</p> <p>When v1 is selected, both v1 and v2 clients can associate with the access point. However, when v2 is selected, only v2 clients can associate with the access point.</p> <p>Most modern wireless clients support v2. In the event that there are stations that do not support v2, select the option v1.</p> <p>By default, the value of the setting is v2.</p>
WEP Key Size	<p>The setting can be configured as either 40 bits or 104 bits.</p>
Re-keying Period	<p>This setting specifies the length of time throughout which the broadcast key remains valid. Upon expiration of Re-keying Period, the broadcast key will no longer be valid and the renewal of the broadcast key will be required.</p> <p>The default is 14400 seconds (i.e. 4 hours).</p> <p>A value of 0 disables re-keying.</p>

7.2.1.3 WPA parameters

The configuration of WPA parameters enables **WPA-TKIP** or **WPA2-AES**.

To enable WPA and WPA-PSK, configure WPA-TKIP. To enable WPA2 and WPA2-PSK, configure WPA2-AES.

When WPA or WPA2 is configured, Radius-based 802.1x authentication with TKIP encryption method is enabled. Under this configuration, the **Pre-Shared Key** option should be disabled.

The security level of this method is known to be very high.

Security Level	WPA-TKIP
Pre-Shared Key	<input checked="" type="checkbox"/> Enable
Passphrase	<input type="text"/> Hide / Show Passphrase

When WPA-PSK or WPA2-PSK is configured, a **Pre-Shared Key**, or **Passphrase**, is used for data encryption and authentication. Under this configuration, the Pre-Shared Key option should be enabled. Key length must be between 8 and 63 characters (inclusive).

The security level of this method is known to be high.

7.2.1.4 Radius Server Settings

Primary Host	<input type="text"/>	
Secret	<input type="text"/>	
Authentication Port	<input type="text"/>	Default AuthPort
Accounting Port	<input type="text"/>	Default AcctPort
Secondary Host	<input type="text"/>	
Secret	<input type="text"/>	
Authentication Port	<input type="text"/>	Default AuthPort
Accounting Port	<input type="text"/>	Default AcctPort
Maximum Retransmission	<input type="text" value="3"/>	
Radius Request Interval	<input type="text" value="3"/>	s (initial value, double upon every retransmission)

Radius Server Settings	
Primary Host	When 802.1x authentication is configured, the Radius server specified by this setting will be used for authentication and accounting.
Secret	This is the secret for accessing the Radius server.
Authentication Port	This specifies the UDP port number for the Authentication port of the Radius server.
Accounting Port	This specifies the UDP port number for the Accounting port of the Radius server.
Secondary Host	This setting specifies the Radius server to used for authentication and accounting in the event that the host specified by Primary Host is unavailable.
Maximum Retransmission	This specifies the maximum number of retry for RADIUS authentication. By default, it is set as 3 .
Radius Request Interval	This specifies the time interval in second between each RADISU request attempt. Note that the request time interval would be doubled every retransmission. By default, it is set as 3s .

7.2.2 Web Portal Login

Basic Web Portal Login Guest Protect MAC Filter Advanced

Enabling the InControl Web Portal will allow you to generate unique login accounts for your guests. This allows you to provide guest wi-fi access with a simple way to track and manage users.

Setup a Free InControl account now at <http://incontrol.pepwave.com> to start using this feature.

Simply registering the devices with Pepwave InControl, users can apply configurations, firmware, and monitor network activity remotely through this centralized management system. For more details, you can refer to Pepwave website at: <http://www.pepwave.com/products/incontrol/>.

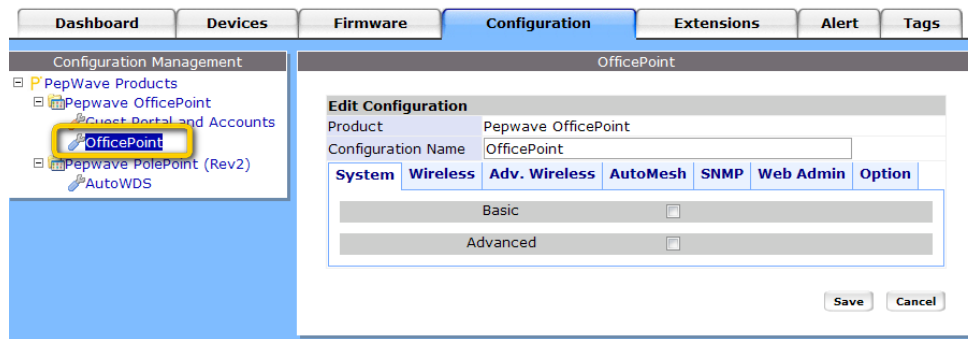
Tip: How to Set Up OfficePoint Guest Portal in InControl

To set up Guest Portal, you need to (1) enable guest portal function and (2) create guest accounts and set up portal page.

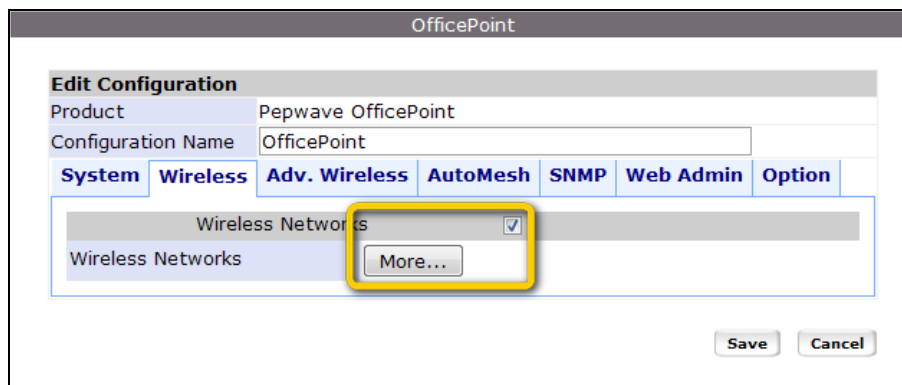
Step One: Enable Guest Portal

1. Log in [InControl](https://incontrol.pepwave.com/) using your username and password. <<https://incontrol.pepwave.com/>>
2. Click "Configuration" tab and find the desired configuration profile.

InControl



3. To find your wireless network, click "Wireless" tab, check the box next to "Wireless Networks" and click "More..." button.

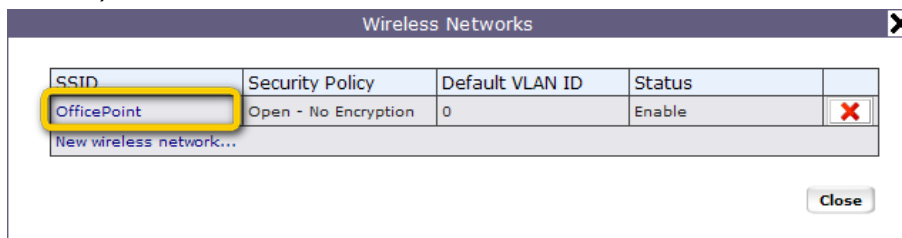


User Manual

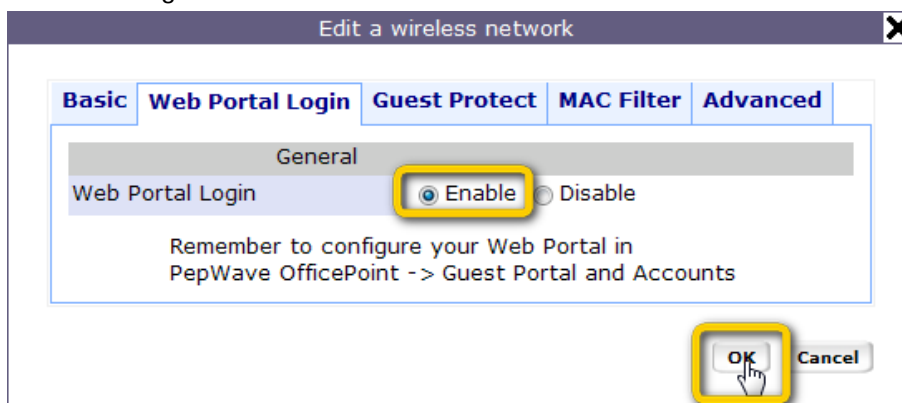
Pepwave OfficePoint Series

4. Click on the name of the SSID you have set up.

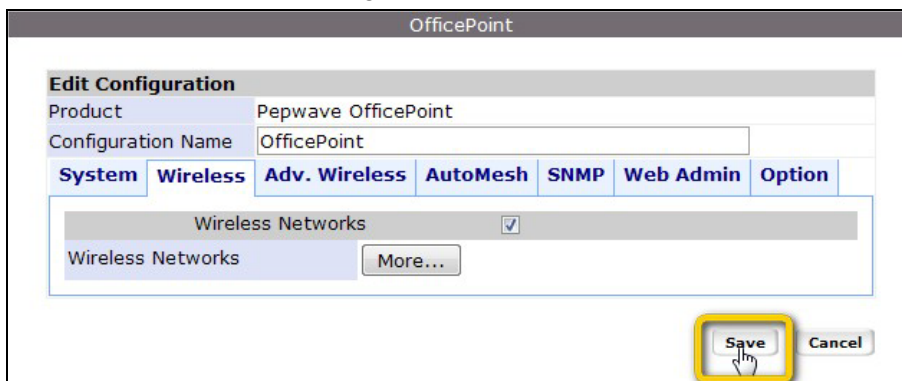
(Note: If you have not added a wireless network, you can click "New wireless network..." to set up a new one.)



5. On the "Edit a wireless network" screen, click "Web Portal Login" tab. Click "Enable" to enable the Web Portal Login function. Click "OK" to continue.



6. Click "Save" button to save the changes.



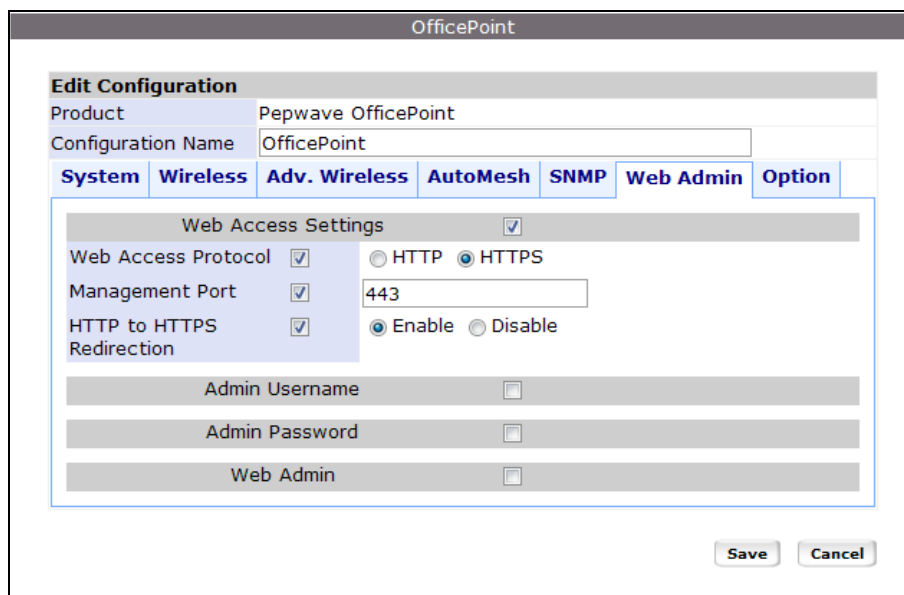
7. Click the "Web Admin" tag, and setup the web access as follows:

Web Access Protocol: HTTPS

Management Port: 443

HTTP to HTTPS Redirection: Enable

Click Save button to save the settings.



The screenshot shows the "OfficePoint" configuration window. The "Edit Configuration" section is active, showing the product name as "Pepwave OfficePoint" and the configuration name as "OfficePoint". The "Web Admin" tab is selected, and the "Web Access Settings" section is expanded. The settings are as follows:

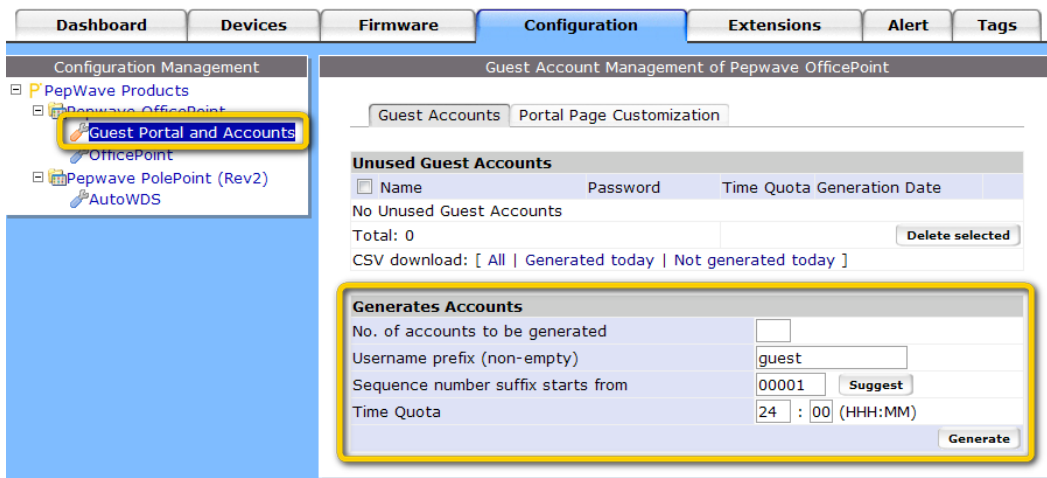
Setting	Value
Web Access Protocol	<input checked="" type="checkbox"/> HTTP <input checked="" type="radio"/> HTTPS
Management Port	443
HTTP to HTTPS Redirection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Admin Username	<input type="checkbox"/>
Admin Password	<input type="checkbox"/>
Web Admin	<input type="checkbox"/>

Buttons for "Save" and "Cancel" are visible at the bottom right.

Step Two: Create Guest Accounts and Set Up Portal Page

8. Go to "Guest Portal and Accounts" by clicking on the link at the left panel.

InControl



The screenshot shows the "InControl" configuration interface. The "Configuration" tab is selected, and the "Guest Account Management of Pepwave OfficePoint" section is active. The "Guest Accounts" sub-tab is selected, and the "Generates Accounts" section is highlighted with a yellow box. The settings are as follows:

Field	Value
No. of accounts to be generated	<input type="text"/>
Username prefix (non-empty)	guest
Sequence number suffix starts from	00001 <input type="button" value="Suggest"/>
Time Quota	24 : 00 (HHH:MM)

A "Generate" button is visible at the bottom right of the "Generates Accounts" section.

9. You can generate more than one account at one time. Change the parameters in the fields No. of accounts to be generated, Username prefix, Sequence number suffix and Time Quota. Default time limit is set to 24 hours. You can change the time limit.

10. Click "Generate" button.

11. You should now have some guest accounts generated as shown in the table "Unused Guest Accounts". You can download the accounts information in CSV file by clicking the "All", "Generated today" or "Not generated today" links.

The screenshot shows the 'Guest Account Management of Pepwave OfficePoint' interface. At the top, there are two tabs: 'Guest Accounts' and 'Portal Page Customization'. The 'Guest Accounts' tab is active, displaying a table titled 'Unused Guest Accounts'. The table has four columns: Name, Password, Time Quota, and Generation Date. Below the table, there is a 'Total: 5' label and a 'Delete selected' button. A 'CSV download:' section contains three links: 'All', 'Generated today', and 'Not generated today', with the 'All' link highlighted by a yellow box. Below the table is a 'Generates Accounts' form with fields for 'No. of accounts to be generated', 'Username prefix (non-empty)', 'Sequence number suffix starts from', and 'Time Quota'. A 'Generate' button is located at the bottom right of the form.

Name	Password	Time Quota	Generation Date
guest1	12056794	24 hours	2010/06/22
guest2	29873041	24 hours	2010/06/22
guest3	47910583	24 hours	2010/06/22
guest4	45981067	24 hours	2010/06/22
guest5	48761325	24 hours	2010/06/22

12. A standard portal page will be generated automatically after guest accounts are generated (<http://guest.pepwave.com>). You can customize the portal page by clicking on the "Portal Page Customization" tab. In the screen upload your logo image and enter message for guests. You can preview your portal page and then publish the portal page.

The screenshot shows the 'Guest Account Management of Pepwave OfficePoint' interface with the 'Portal Page Customization' tab active. The 'Update Portal Page Information' form is displayed. It includes a 'Logo Image' field with a 'Browse...' button and an 'Upload' button. Below this is a note: 'Note: Max size: 2 MB. Supported image types: JPEG, PNG and GIF.' The 'Message' field contains the text: 'You can customize the message shown on the login page.' At the bottom right, there are 'Preview' and 'Publish' buttons.

Your guest accounts and portal page are now ready for use.

7.2.3 Guest Protect

The screenshot shows the 'Guest Protect' configuration page. It features several sections:

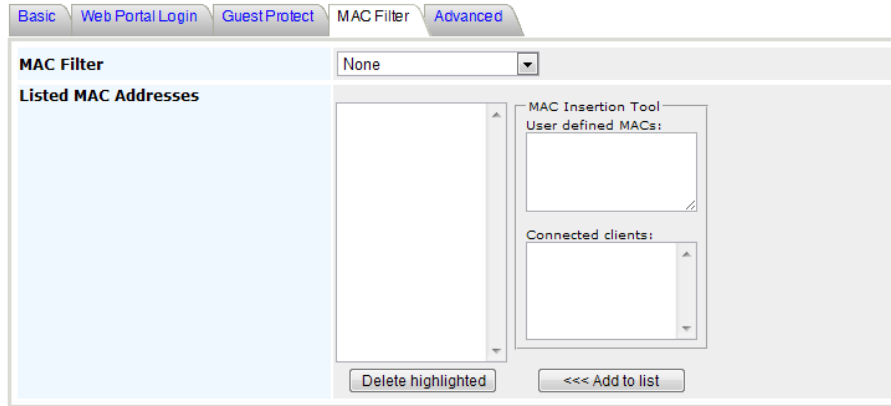
- Block LAN Access:** Includes radio buttons for 'Block all private IPs', 'Custom Subnet', and 'Block Exception'. Below is an 'Enable' checkbox.
- Bandwidth Management:** Includes an 'Enable' checkbox.
- Upstream Limit:** Includes radio buttons for 'Per VAP' and 'Per Client', and a text input field set to '0 kbps (0: Unlimited)'.
- Downstream Limit:** Includes radio buttons for 'Per VAP' and 'Per Client', and a text input field set to '0 kbps (0: Unlimited)'.
- Maximum Number of Clients:** Includes a text input field set to '0 (0: unlimited)'.
- Firewall Mode:** Includes radio buttons for 'Lockdown - Block all traffic except for the following exceptions:', 'Flexible - Allow all traffic except for the following exceptions:', and 'Disable' (which is selected).
- Exceptions:** A table with columns 'Name', 'Type', and 'Item'. Below the table, there are input fields for 'Port', 'TCP', and 'UDP port', along with an 'Apply' button.

Wireless Networks Details - Guest Protect

Block LAN Access	<p>This option enables the settings to Block all private IPs / Custom Subnet / Block Exception.</p> <p>If you have selected Block all private IPs or Custom Subnet, these IPs / Subnets will be blocked no matter what "Firewall Mode" selected. When Block Exception is selected, IPs entered will be excluded from the blocking list.</p> <p>Private IP -- This includes the commonly known private IPs: 192.168.0.0 - 192.168.255.255 172.16.0.0 - 172.31.255.255 10.0.0.0 - 10.255.255.255</p> <p>Custom Subnet -- This includes user specified IP subnets to be blocked.</p> <p>Block Exception – Only IPs specified will NOT be blocked.</p>
Bandwidth Management	<p>This option enables the settings to control upstream and downstream limits. You can select to either control the bandwidth usage Per VAP or Per Client.</p>
Maximum Number of Clients	<p>This setting specifies the maximum number of clients that can be connected to the OfficePoint simultaneously. By default, it is set to unlimited (which is 0 in number).</p>
Firewall Mode	<p>This setting specifies three options: Lockdown, Flexible, and Disable.</p> <p>Lockdown – Block all traffic except for the pre-defined exceptions; Flexible – Allow all traffic except for the pre-defined exceptions; Disable – Firewall mode is disabled. (Default option)</p>
Exceptions	<p>This setting specifies the exceptions when Lockdown or Flexible Firewall Mode is selected. Exceptions can be added by <i>types</i>, including <i>Port</i>, <i>Domain</i>, <i>IP Address</i>, <i>MAC Address</i>, <i>Application /Service</i>.</p>

7.2.4 MAC Filter

The settings allow administrator to control the access through Mac address filtering. Available options are: **None**, **Deny all except listed**, **Accept all except listed**.



7.2.5 Advanced

Basic	Web Portal Login	Guest Protect	MAC Filter	Advanced
Data Rate	<input type="radio"/> Fixed <input checked="" type="radio"/> Auto 1M (Minimum auto rate)			
Multicast Filter	<input type="checkbox"/> Enable			
Multicast Rate	1M			
DHCP Relay	Server			
IP Start Range	0.0.0.0			
IP Stop Range	0.0.0.0			
Subnet Mask	0.0.0.0			
Broadcast Address				
Gateway	0.0.0.0			
DNS 1	0.0.0.0			
DNS 2	0.0.0.0			
DNS 3	0.0.0.0			
Domain				
Lease Time	0 seconds			
Default VLAN ID	0			
Network Priority (QoS)	Gold			
Layer 2 Isolation	<input type="checkbox"/> Enable			

Wireless Networks Details -Advanced	
Data Rate	<p>There are two options on data rate: Fixed, Auto</p> <p>Fixed will forced all data packets to be transmitted into the selected transmit rate. Auto will automatically select the best transmit rate with a condition to use the selected transmit rate as the minimum auto transmit rate.</p>
Multicast Filter	<p>This setting enables the filtering of multicast network traffic to the wireless SSID.</p>
Multicast Rate	<p>This setting specifies the transmit rate to used for sending multicast network traffic.</p>
DHCP Relay	<p>The OfficePoint will forward DHCP requests to a specified DHCP Server. This option prevents broadcast messages from being propagated on the Ethernet segment. Upon selecting this option, the DHCP Server IP address (or DHCP Server settings) will be prompted.</p>
Default VLAN ID	<p>This setting specifies the VLAN ID to be tagged on all outgoing packets generated from the virtual AP (i.e. packets that travel from the Wi-Fi segment, through the Pepwave OfficePoint unit to Ethernet segment via the LAN port).</p> <p>If 802.1x is enabled and a per-user VLAN ID is specified in the <i>authentication reply from the Radius server</i>, then the value specified via Default VLAN ID will be overridden.</p> <p>The default value of this setting is 0. That means VLAN tagging is disabled (instead of tagged with zero).</p>

User Manual

Pepwave OfficePoint Series

Network Priority (QoS)	<p>The 802.1p QoS value to be marked on all outgoing packets generated from the virtual AP (i.e. packets that travel from the Wi-Fi segment, through the Pepwave OfficePoint unit to Ethernet segment via the LAN port).</p> <p>If per-user or per-domain QoS value is specified, the Default Quality of Service value will be overridden.</p> <p>Possible values are Gold, Silver and Bronze.</p>
Layer 2 Isolation	<p>Layer 2 is in reference to the second layer in the ISO Open System Interconnect model.</p> <p>When this option is enabled, clients on the same VLAN, SSID or subnet are not allowed to communicate directly via the Layer 2 Protocol(s). Traffic is passed to upper communication layer(s).</p> <p>With this option disabled, clients on the same VLAN are allowed to communicate with each other directly. (Windows network resources browsing will be possible.)</p> <p>By default, the setting is disabled.</p>

7.3 Advanced Wireless Settings

Advanced Wireless Settings provides more options to fine tune the parameters on the system to achieve the optimal performance.

Advanced Wireless Settings

Radio Settings	Advanced Features	Performance Tuning
Protocol	802.11b/g	
Operating Country	United States	
Channel	1 (2.412 GHz)	
Output Power	Max	
Antenna Selection	Main	

[Save](#) [Save to flash and activate](#)

PePWave OfficePoint (2.1.1)

7.3.1 Radio Settings

Radio Settings	Advanced Features	Performance Tuning
Protocol	802.11b/g	
Operating Country	United States	
Channel	1 (2.412 GHz)	
Output Power	Max	
Antenna Selection	Main	

Radio Settings	
Protocol	Three options are available: 802.11b/g: Pepwave OfficePoint accepts both 802.11b and 802.11g client association requests. 802.11b Only: Pepwave OfficePoint accepts only 802.11b client association requests. 802.11g Only: Pepwave OfficePoint accepts only 802.11g client association requests.
Operating Country	This setting specifies the country / region whose regulations the Pepwave OfficePoint unit should follow. If United States is selected, RF channels 1 to 11 are available. Maximum transmission power is 26 dBm (400 mW) for models of MPW-4xx, or 23dBm (200 mW) for models of MPW-2xx. If Europe region is selected, RF channels 1 to 13 are available. Maximum transmission power is 20 dBm (100 mW).
Channel	This option selects the 802.11 channel to be utilized. Available options for 802.11b or 802.11g are from 1 to 11, and from 1 to 13 for the country setting of Default (US) and Europe, respectively. The system would perform channel scanning based on the scheduled time set.

User Manual

Pepwave OfficePoint Series

Output Power	This option enables the configuration of transmission power. Available options are Max , High , Medium , and Low .
Antenna Selection	For Pepwave OfficePoint Outdoor units, the hardware may be equipped with two antennas for transmit and receive diversity. If the Pepwave OfficePoint unit is equipped with two antennas, users can select Main, Aux. and Both (antenna diversity). By default, Main is selected.

7.3.2 Advanced Features

Radio Settings	Advanced Features	Performance Tuning
Discover Nearby Networks	<input checked="" type="checkbox"/>	Enable
Scanning Interval	10	s
Scanning Time	50	ms
WMM	<input checked="" type="checkbox"/>	Enable

[Save](#) [Save to flash and activate](#)

Advanced Wireless Settings – Advanced Features	
Discover Nearby Network	The AP would scan and discover nearby network if this option is enabled.
Scanning Interval	This setting determines how often the access point goes to other channels to discover Neighbor AP.
Scanning Time	This setting determines how long the access point stays on the other channels to discover Neighbor AP.
WMM	This option enables the Wi-Fi Multimedia (WMM), as known as Wireless Multimedia Extensions (WME) on the access point.

7.3.3 Performance Tuning

Radio Settings
Advanced Features
Performance Tuning

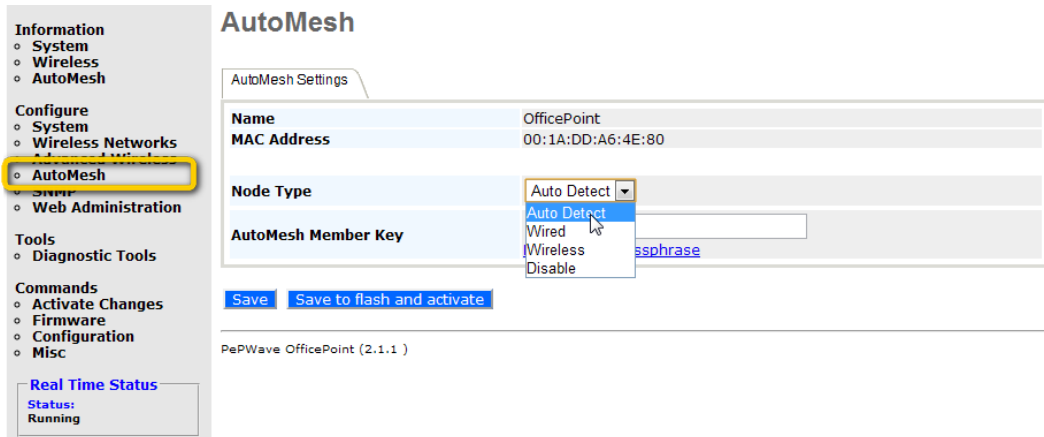
Beacon Rate	2Mbps
Beacon Interval	250ms
DTIM	15
RTS Threshold	0
Distance / Time Convertor	4050 m <small>(input distance for recommended values)</small>
Slot Time	9 μ s Default
ACK Timeout	48 μ s Default
CTS Timeout	48 μ s Default
802.11g Protection	<input checked="" type="checkbox"/> Enable <small>(In favor of 802.11g devices in mixed mode (11g and 11b) networks)</small>

Save
Save to flash and activate

Advanced Wireless Settings – Performance Tuning	
Beacon Rate	This setting provides the option to send beacon in different transmit bit rate and the bit rates are: 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps.
Beacon Interval	This setting provides the option to set the time between each beacon send.
DTIM Period	This setting provides the option to set the frequency for beacon to include Delivery Traffic Indication Message, DTIM. The interval unit is in millisecond.
RTS Threshold	This setting provides the option to set the minimum packet size for the unit to send an RTS using the RTS/CTS handshake. Setting zero would disable this feature.
Distance / Time Convertor	This is a convertor which will automatically adjust the Slot Time, ACK Timeout and CTS Timeout based on the distance you have entered.
Slot Time	This setting provides the option to modify the unit wait time before it transmits.
ACK Timeout	This setting provides the option to set the wait time to receive acknowledgement packet before doing retransmission.
CTS Timeout	This setting provides the option to specify the timeout for the unit to wait for CTS response in the RTS/CTS handshake.
802.11g Protection	Enable this setting to in favor of 802.11g devices in mixed mode (11g and 11b) networks.

7.4 AutoMesh

AutoMesh provides a way to link APs together when wired cabling is not preferable. This also extends the wireless coverage of the wireless network for the wireless clients.

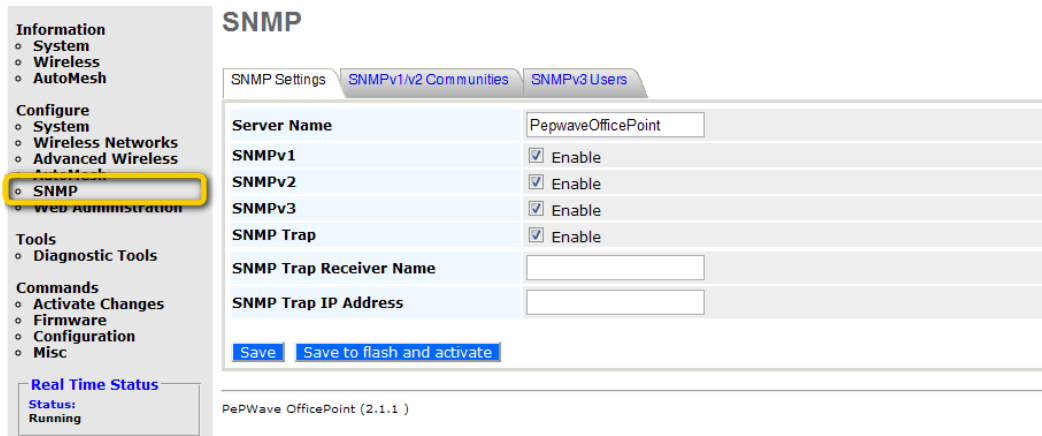


AutoMesh Settings	
Node Type	<p>There are four options: Auto Detect, Wired, Wireless and Disable.</p> <p>Auto Detect - the unit would check the connectivity to the default gateway via wired Ethernet to determine the node type. If there is connectivity to the default gateway, the unit would state its node type as gateway. Otherwise, the unit would state its node type as node.</p> <p>Wired- the unit is expected to be wire connected to provide public network access to other wireless nodes.</p> <p>Wireless - the unit would search for the best gateway or node wirelessly in order to gain public network access.</p> <p>Disable – the unit would not link to any AP.</p>
AutoMesh Number Key	<p>This setting gives the encryption key to secure the data between APs. You can click the link Hide / Show Passphrase to show or hidden the above encryption key.</p>

7.5 SNMP

7.5.1 SNMP Settings

Upon selecting **SNMP** from the navigation bar on the left-hand-side of the Main Menu, the following page is displayed to enable the configuration of SNMP server settings:



SNMP Settings	
Server Name	This setting specifies the name that identifies the SNMP server.
SNMPv1	This setting specifies whether to enable or disable the support for Version 1 of SNMP.
SNMPv2	This setting specifies whether to enable or disable the support for Version 2 of SNMP.
SNMPv3	This setting specifies whether to enable or disable the support for Version 3 of SNMP.
SNMP Trap	SNMP Trap is a message initiated from a client and sent to the PolePoint device. Once this option is enabled, the following two options for SNMP Trap will be available for configuration.
SNMP Trap Receiver Name	This setting specifies the name that identifies the SNMP Trap Receiver.
SNMP Trap IP Address	This setting specifies the IP address of the SNMP Trap Receiver.

7.5.2 SNMPv1 / SNMPv2 Communities

Community Name	IP Address	IP Mask	Access Mode	Status	
internal	10.10.10.1	255.255.255.0	Read & Write	Enable	Edit Remove
office	210.10.10.1	255.0.0.0	Read Only	Disable	Edit Remove

[New](#)

By adding SNMPv1/v2 Communities, access rights can be controlled. Click on the **New** button to add one.

SNMPv1/v2 Community

Settings

Community Name	internal
IP Address	10.10.10.1
IP Mask	255.255.255.0
Access Mode	Read & Write
Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

[Save](#) [Save to flash and activate](#)

SNMPv1 / SNMPv2 Communities	
Community Name	The password for getting or setting SNMP values.
IP Address and IP Mask	The allowed IP and subnet address which can access the SNMP server.
Access Mode	Choose either Read Only or Read & Write .
Status	Enable or Disable this community.

7.5.3 SNMPv3 Users

User Name	Authentication Protocol	Privacy Protocol	Access Mode	Status	
user1	HMAC-SHA	CBC-DES	Read Only	Enable	Edit Remove
user2	HMAC-MD5	None	Read & Write	Disable	Edit Remove

[New](#)

By adding SNMPv3 users, access rights can be controlled. Click on the **New** button to add one.

SNMPv3 User

Settings

SNMPv3 User Name user2

Authentication Protocol HMAC-MD5

Authentication Password [masked] (Retype)

Privacy Protocol None

Access Mode Read & Write

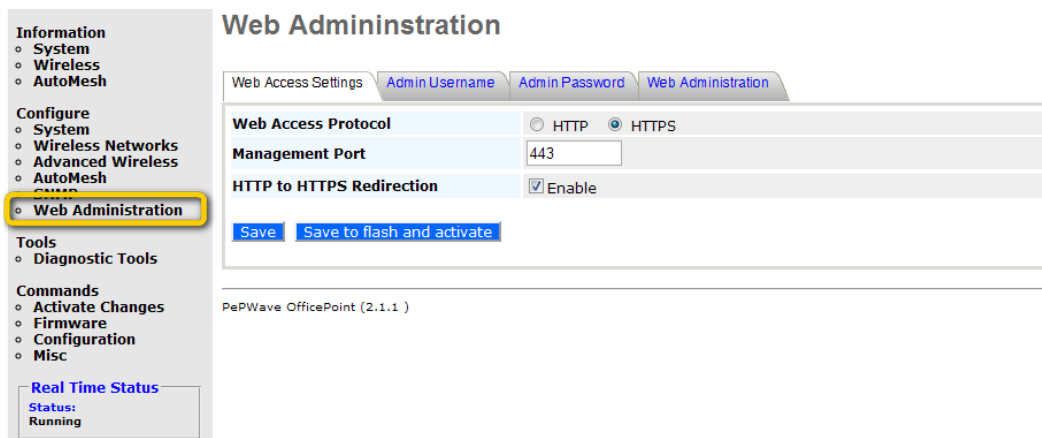
Status Enable Disable

[Save](#) [Save to flash and activate](#)

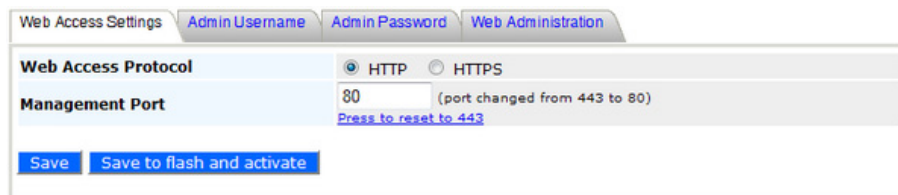
SNMPv3 User Setting	
SNMPv3 User Name	The user ID to be allowed to access the SNMP agent.
Authentication Protocol	The protocol for authenticating the user. Available options are: HMAC-MD5 and HMAC-SHA .
Authentication Password	Users provided with a correct password will be granted the right to access the SNMP agent.
Privacy Protocol	The encryption method to be used in SNMPv3 communication. Available options are: None and CBC-DES .
Privacy Password	This option is shown only if CBC-DES is chosen as the Privacy Protocol. This is the key for decrypting the encrypted data.
Access Mode	Grant Read or Read & Write access to this user.
Status	Enable or Disable this user.

7.6 Web Administration

Upon selecting **Web Administration** from the navigation bar on the left-hand-side of the Main Menu, the tabs of configuring the management interface are displayed.

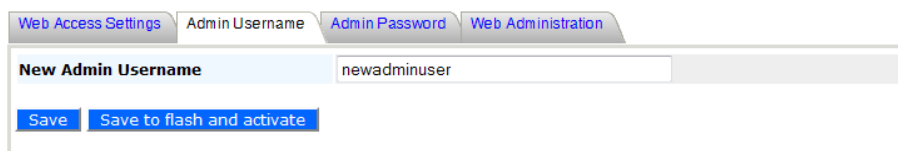


7.6.1 Web Access Settings



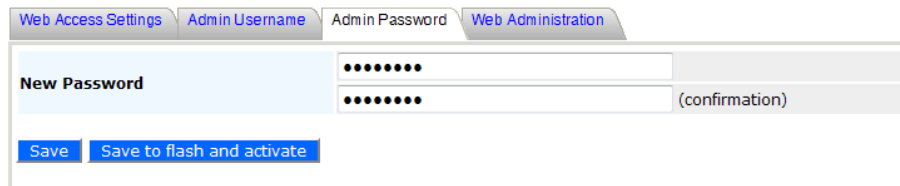
The selection **Web Access Settings** configures the protocol and TCP port number of the web server. If **HTTPS** is enabled, **HTTP to HTTPS Redirection** option will be provided.

7.6.2 Admin Username



The selection **Admin Username** configures the administrator username for entering Web Admin Interface. To change to the Username, enter the new username into the **Username** input fields.

7.6.3 Admin Password



The screenshot shows the 'Admin Password' configuration page. At the top, there are four tabs: 'Web Access Settings', 'Admin Username', 'Admin Password', and 'Web Administration'. The 'Admin Password' tab is selected. Below the tabs, there are two input fields for 'New Password', each containing seven dots. The second field is labeled '(confirmation)'. At the bottom of the form, there are two buttons: 'Save' and 'Save to flash and activate'.

The selection **Admin Password** configures the administrator password for entering Web Admin Interface. To change to the password, enter the same new password into the **New Password** and **New Password (Retype)** input fields.

7.6.4 Web Administration

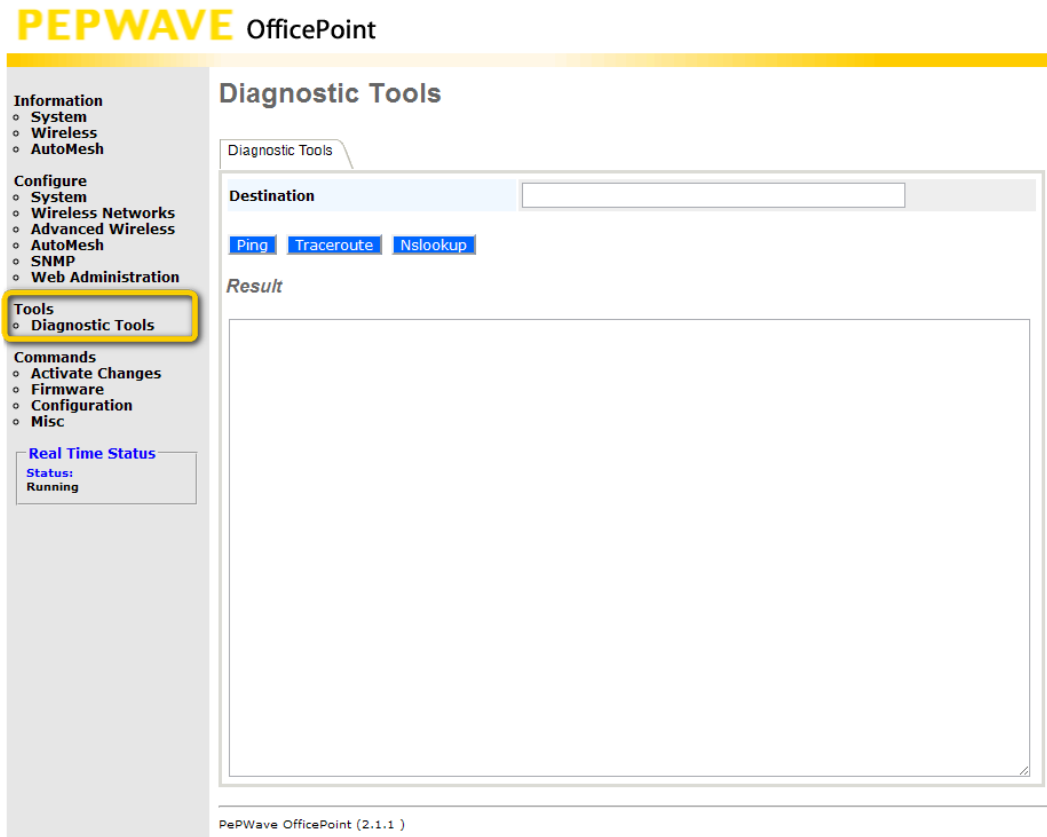


The screenshot shows the 'Web Administration' configuration page. At the top, there are four tabs: 'Web Access Settings', 'Admin Username', 'Admin Password', and 'Web Administration'. The 'Web Administration' tab is selected. Below the tabs, there is a section titled 'Web Admin Interface' with two radio buttons: 'Enable' (which is selected) and 'Disable'. At the bottom of the form, there are two buttons: 'Save' and 'Save to flash and activate'.

The selection **Disable Web Administration** turns off the access to Web Administration Interface. After being turned off, Web Administration Interface can be re-enabled using SNMP.

8 Tools - Diagnostic Tools

This provides three useful tools for diagnosing the network. The three available options are: **Ping**, **Traceroute** and **Nslookup**.

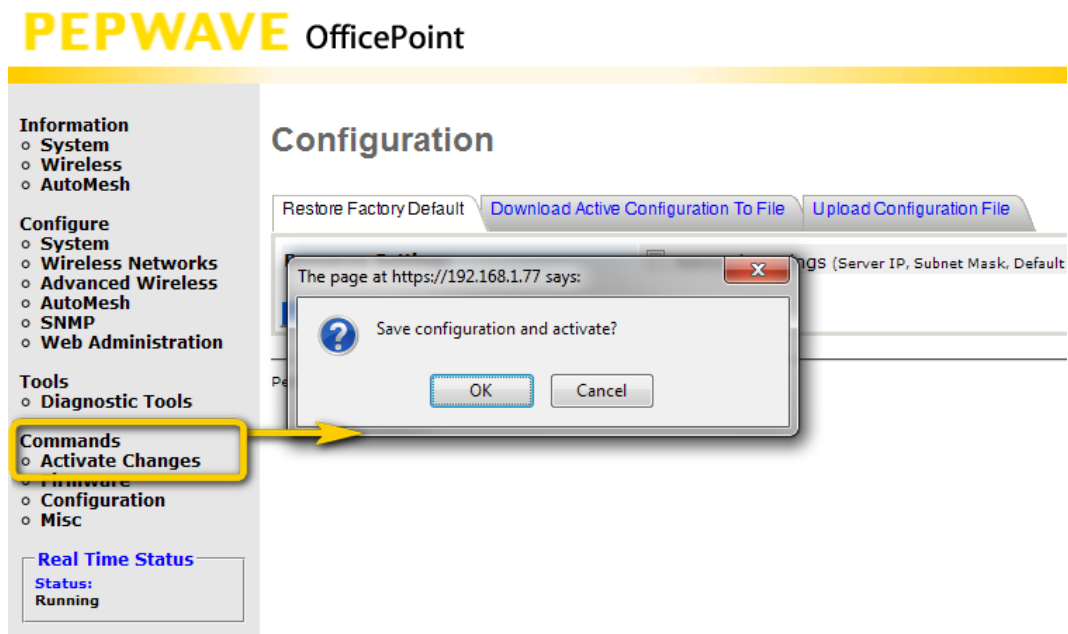


9 Commands

Upon selecting **Commands** from the navigation bar on the left-hand-side of the Main Menu, a list of commands is displayed, as follows:

9.1 Activate Changes

Click on **Activate Changes** and a prompt will ask and confirm to save configuration and activate the OfficePoint unit.



9.2 Firmware

Information

- System
- Wireless
- AutoMesh

Configure

- System
- Wireless Networks
- Advanced Wireless
- AutoMesh
- SNMP
- Web Administration

Tools

- Diagnostic Tools

Commands

- Administer Changes
- Firmware**
- Configuration
- Misc

Real Time Status

Status:
Activating

Firmware

Upgrade Firmware

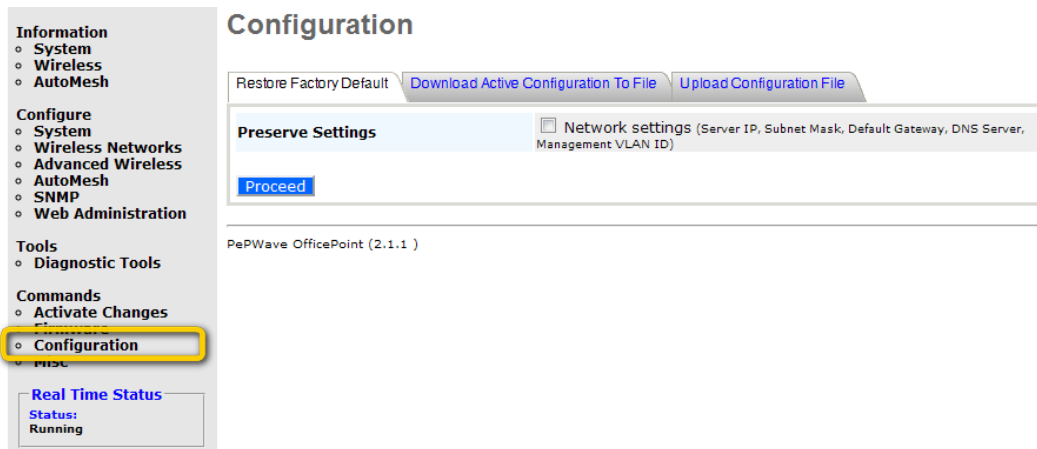
	Flash 1	Flash 2
Firmware Version	2.1.1	Recovery
Flash Status	Bootable	Bootable
Boot from	⚙	
Firmware Upgrade Target	⚙	

Firmware Image File No file chosen

PePWave OfficePoint (2.1.1)

Commands - Firmware	
Firmware Version	This shows the firmware version loaded into the flash partitions.
Flash Status	This shows the firmware status on the flash partitions.
Boot from	This indicates which flash partition boots up the system.
Firmware Upgrade Target	This shows which flash partition is used for firmware upgrade.
Firmware Image File	Upload a firmware file for upgrading the unit's software. A reboot is required after upgrading the firmware.

9.3 Configuration



Commands - Configuration	
Restore Factory Default	This command is for restoring factory default settings of the OfficePoint. Preserve the network settings by enabling Preserve Settings .
Download Active Configuration To File	Select this command to download the active configuration for backup purposes.
Upload Configuration File	Select this command to upload the configuration from a backed up configuration file.

9.4 Misc

Information

- System
- Wireless
- AutoMesh

Configure

- System
- Wireless Networks
- Advanced Wireless
- AutoMesh
- SNMP
- Web Administration

Tools

- Diagnostic Tools

Commands

- Activate Changes
- Firmware
- Configuration
- **Misc**

Real Time Status

Status:
Running

Miscellaneous

Download Debug Information Reboot AP

Proceed

PePWave OfficePoint (2.1.1)

Commands - Misc	
Download Debug Information	Select this comment to download debugging information from the Pepwave OfficePoint unit. In the event of technical issues, to facilitate prompt resolution by technical support from Pepwave, please send along with a debug file with the support request.
Reboot AP	This option is for rebooting the Pepwave OfficePoint unit.

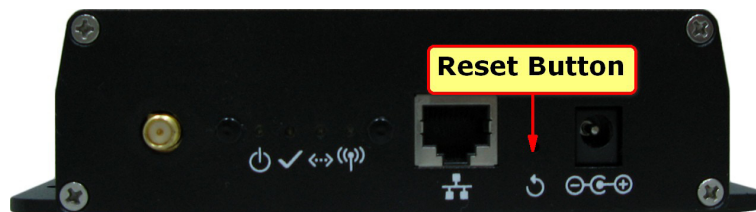
10 Restoration of Factory Defaults

10.1 OfficePoint Indoor Series

The following procedure restores the settings of Pepwave OfficePoint indoor device to factory defaults:

1. Power on the unit, wait for 1 minute until the Status LED turns green.
2. Press and hold the reset button on the rear panel for at least 5 seconds, then release.
3. The Status LED will blink, and then the unit will automatically reboot.
4. 4. Wait for 1 minute or until the Status LED turns green, upon which the settings of Pepwave OfficePoint will have been restored to the factory defaults.

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



10.2 OfficePoint Outdoor Series

There are two ways to restore the Pepwave OfficePoint outdoor device to default settings.

If you are able to access the web admin interface, go to the "CPE Setup" page, and click the **Restore and Reboot** button.

Otherwise, you can power up the unit and wait for about 1 min. Then push the **Reset Button** at the panel side of the unit and then hold it for 5 seconds. The unit will restore the settings to factory default and reboot.



Appendix A.

Radius Server Setup

Pepwave OfficePoint has been test to be functional with Radiator version 3.9, using the EAP-TTLS protocol.

For Pepwave OfficePoint, configure the authentication protocol of the virtual access point to **WPA-AES:CCMP**.

Sample Radiator Settings

```
AuthPort          1812
AcctPort          1813
LogDir            /var/log/radius
DbDir             /etc/radiator
Trace             4
<Client DEFAULT>
  Secret          testing123
  DupInterval     0
</Client>
<Realm DEFAULT>
  <AuthBy FILE>
    Filename       /etc/radiator/users
    EAPType        TTLS
    EAPTLS_CAFfile /etc/1x/cert/demoCA/cacert.pem
    EAPTLS_CertificateFile /etc/1x/cert/cert-srv.pem
    EAPTLS_CertificateType PEM
    EAPTLS_PrivateKeyFile /etc/1x/cert/cert-srv.pem
    EAPTLS_RandomFile /dev/urandom
    EAPTLS_PrivateKeyPassword whatever
    EAPTLS_MaxFragmentSize 1000
    AutoMPPEKeys
  </AuthBy>
  AcctLogFileName /etc/1x/radius_detail
</Realm>
```

Appendix B.

Federal Communication Commission Interference Statement

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

- 1) Reorient or relocate the receiving antenna.
- 2) Increase the separation between the equipment and receiver.
- 3) Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- 4) Consult the dealer or an experienced radio/TV technician for help.

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.

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 20cm between the radiator & your body.

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

PEP WAVE

Broadband Possibilities

www.pepwave.com

Contact Us:

Sales

<http://www.pepwave.com/contact/sales/>

Support

<http://www.pepwave.com/contact/>

Business Development and Partnerships

<http://www.pepwave.com/partners/channel-partner-program/>

Address:

United States Office

800 West El Camino Real,
Mountain View
CA 94040
United States
Tel: +1 (650) 331 0641
Fax: +1 (650) 625 4664

Hong Kong Office

17/F, Park Building,
476 Castle Peak Road
Cheung Sha Wan
Hong Kong
Tel: +852 2990 7600
Fax: +852 3007 0588