

PEP WAVE

Broadband Possibilities

User Manual

Pismolabs 101 mini

October 09

COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice. Copyright © 2009 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	COPYRIGHT	3
2	DISCLAIMER.....	3
3	PRODUCT DESCRIPTION	4
3.1	PRODUCT FEATURES	4
3.2	HARDWARE SETUP.....	5
3.3	LED DESCRIPTION.....	6
4	USING THE PEPWAVE DEVICES.....	7
4.1	PRE-CONFIGURING PC SETUP.....	7
4.2	FIRST TIME SETUP.....	8
4.3	SETTINGS DETAILS	12
4.4	INTEGRATED WI-FI ACCESS POINT CONFIGURATION	17
4.5	TEST THE SETUP.....	20
4.6	PORT FORWARDING	21
4.7	QOS	23
4.8	FIRMWARE UPGRADE	24
4.9	DEBUG AND SYSTEM INFORMATION	25
4.10	RESTORE TO DEFAULT SETTINGS.....	26
APPENDIX:	27
	FEDERAL COMMUNICATION COMMISSION INTERFERENCE STATEMENT	27

1 Copyright

Copyright © 2009 by Pepwave Ltd.

The content of this documentation may not be reproduced in any part or as a whole without the prior written permission of Pepwave Ltd.

2 Disclaimer

Pepwave does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent right nor the patent rights of others. Pepwave further reserves the right to make changes in any products described herein without notice. This documentation is subject to change without notice.

3 Product Description

3.1 Product Features

- Signal strength LED for showing the current signal strength
- Always-on, integrated Wi-Fi access point (Pismolabs 101 mini AP Series)
- WPA/WPA2-Personal and WPA/WPA2-Enterprise security support
- Wi-Fi Multimedia (WMM) support
- Built-in DHCP server and NAT routing to manage client devices
- Customizable, built-in web portal for simple web-based configuration



3.2 Hardware Setup

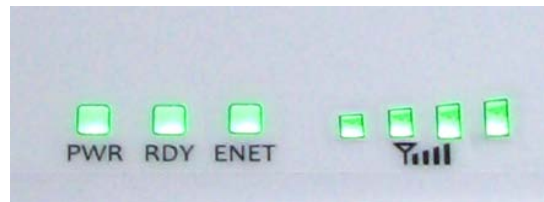
3.2.1 Pismolabs 101 mini




1. Attach the provided antenna to the left most antenna connector
2. Connect the LAN port to the computer's Ethernet port with an Ethernet cable.
3. Connect the end of the included power adapter to the power socket on Pismolabs 101 mini.
4. Power on the power adaptor.

3.3 LED Description

3.3.1 Pismolabs 101 mini



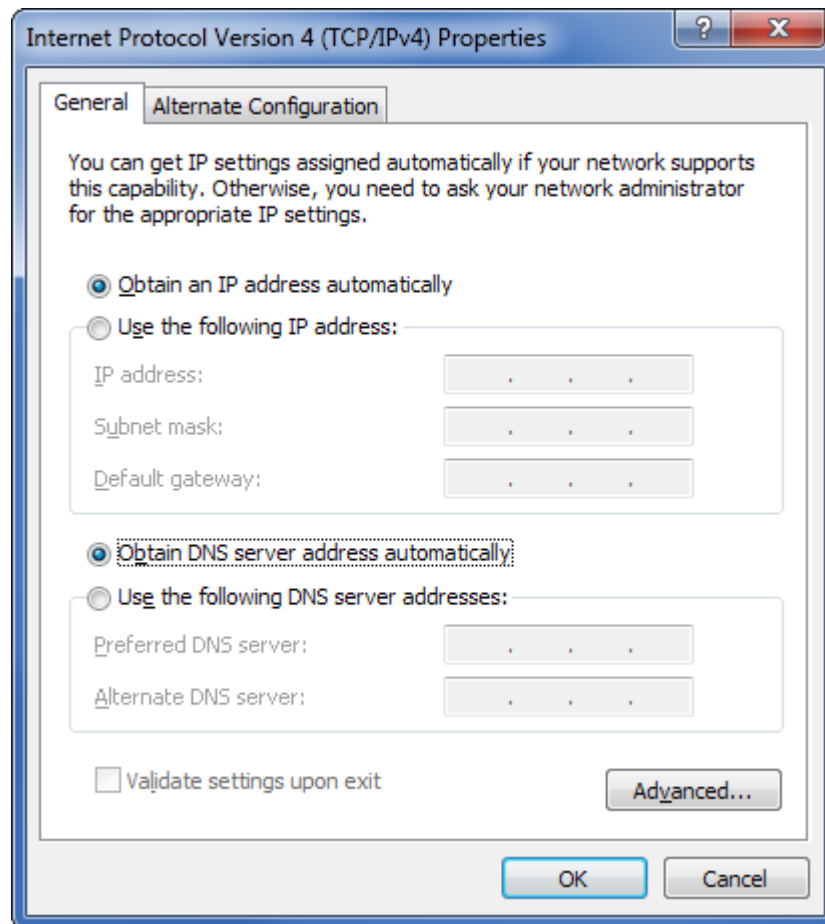
LED	Color	Status	Description	
PWR	Green	On	Power is on	
		Off	Power is off	
RDY	Green	Solid	Received signal is Excellent, Very Good and Good	
		Blinking	Received signal is Low	
		Amber	Blinking	Received signal is Very Low
		Amber	Solid	No wireless signal is detected
		Off	Booting up / Upgrading firmware	
ENET	Green	On	Ethernet is connected	
		Blinking	Sending/Receiving data	
		Off	Ethernet is not connected	
Wi-Fi 	Green	On	Associated with an access point	
		Blinking	Sending/Receiving data	
		Off	Not associated with any access point	
Signal Bars	Green	N/A	The number of lit signal bars depends on the strength of the received signal. A larger number of lit signal bars indicate stronger signals.	

4 Using the Pepwave Devices

4.1 Pre-configuring PC Setup

You should set up your computer's LAN interface to obtain an IP address automatically. If you do so, you should have set it up correctly.

In order to do so, select the **Start menu, Control Panel** and then **Network Connections**. Right click on the **Local Area Connection** icon, choose **Properties**, and double-click on the item **Internet Protocol (TCP/IP)** from the list. On the screen, just set it as follows:



Click the **OK** button to confirm the change.

4.2 First Time Setup

On your PC, start a web browser, e.g. Internet Explorer, Mozilla Firefox, etc. Visit an Internet web site. If you are not associated to an access point, you should be redirected to a logon page. Or you can go also go to this URL

http://192.168.20.1/

The page will look like this.



Illustration 1: Welcome Page

Click the **Advanced Config** button to enter the parameters of the access point to associate to. You should see this screen:

The screenshot displays the 'Advanced Config' page for the Pismolabs 101 mini access point. The page is organized into several sections, each with a list of configuration parameters and their current values or settings.

- Navigation:** Connect | CPE Setup | **Port Forward** | QoS | Firmware Upgrade | Debug
- LAN Interface:** IP Address (192.168.20.1), Subnet Mask (255.255.255.0)
- DHCP Server:** Enable (selected), Start IP Address (192.168.20.10), Stop IP Address (192.168.20.250), Subnet mask (255.255.255.0), DHCP Reservations (Config), Disable
- Wireless Settings:**
 - SSID: MySSID (MySSID)
 - Radio Mode: 802.11b/g
 - Channel Scanning Mode: Full
 - Bit Rate: auto Mbps (auto)
 - Authentication: Open (open)
 - Encryption Key: None
 - MAC: (empty)
 - Preferred AP: (empty)
 - Min Signal Strength: (empty) dBm (e.g. -75)
- Roaming Settings:**
 - Disable (selected), Enable
 - Background Scanning Interval: 24 Hours (24)
 - Roaming Threshold (Signal Level Gain): 10 dBm (10)
- IP Settings:**
 - Configure Manually
 - Obtain an IP Address using DHCP (selected)
 - Obtain an IP Address using PPPoE
- MTU Size:** 1500
- AP Settings:**
 - Disable (selected), Configure Manually, Configure Automatically
 - Keep AP: Enable (selected), Disable
 - Broadcast SSID: Enable (selected), Disable
 - Client Isolation: Enable, Disable (selected)
 - AP Transmit Power Adjustment: default (default)
- WAI Redirection:** Enable (selected), Disable (Note: you need to reboot CPE for this change to take effect)
- Web Password Protection:** Enable, Disable (selected), Password: ***** (admin) (Note: login name is 'root')
- Restore Factory Settings:** Restore & Reboot
- Reboot CPE:** Reboot
- Save:** Save

Illustration 2: Pismolabs 101 mini AP Setup Page

In the field **SSID** under *Wireless Settings*, input the access point's SSID (sometimes it is called the "network name"). According to the setting of the Access Point you are associating to, you may choose a different **Authentication** setting.

If **Static WEP key or WPA/WPA2-Personal** is selected for **Authentication**, input the Encryption Key field as well. (There are also options of **802.1x with dynamic WEP key** and **WPA/WPA2-Enterprise**. You do not need to use these settings unless instructed to do so by your ISP.)

Click the **Save** button at the bottom to complete.

You can now click the **Connect** link on the top bar and then click the **Connect** button to associate with the access point.

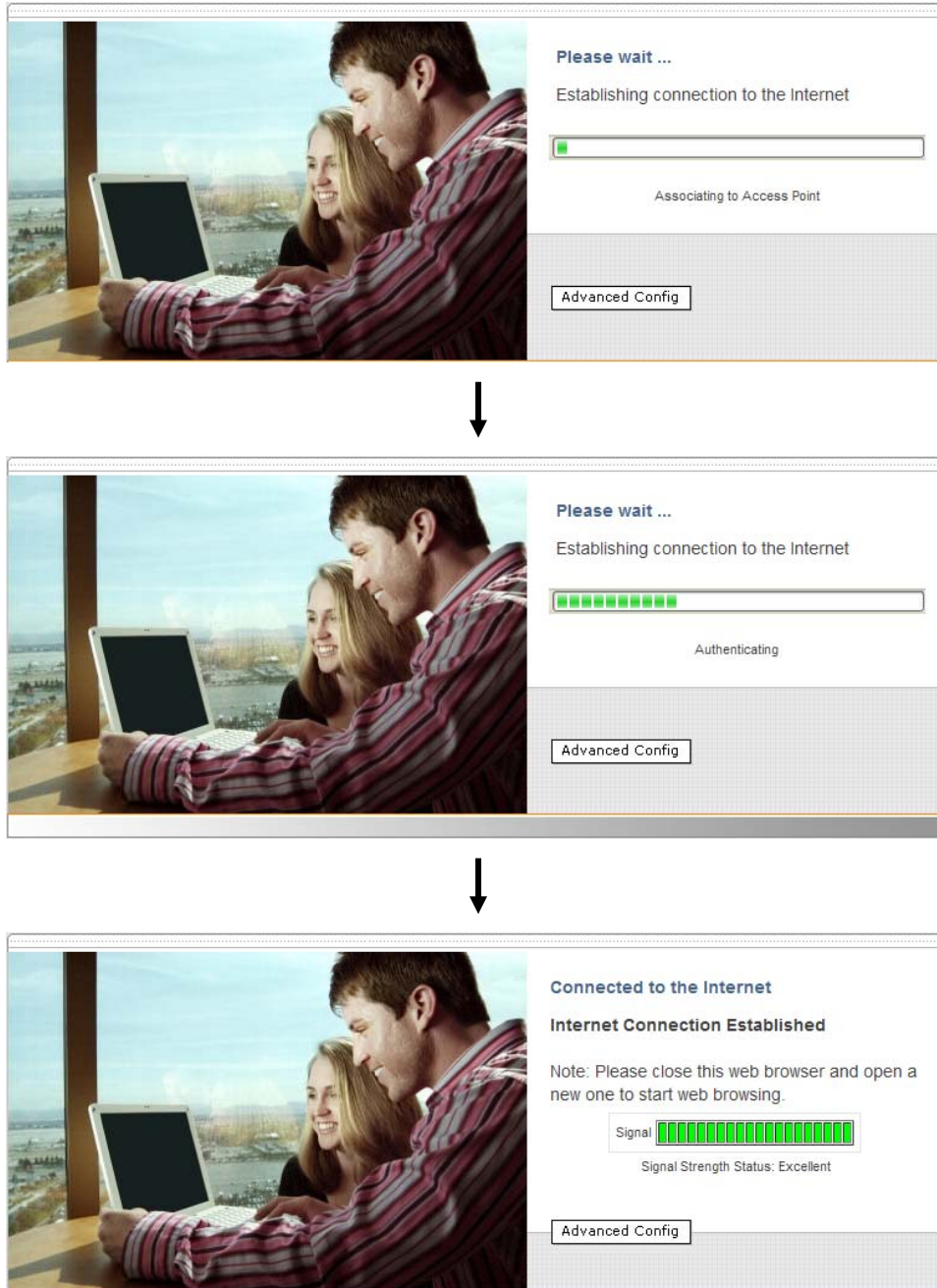


Illustration 3: Establishing Connection to the Internet

At this point, you are associated with the access point. You may now close the web browser and open a new one to start web browsing.

4.3 Settings Details

4.3.1 IP Settings

LAN Interface	IP Address	192.168.20.1
	Subnet mask	255.255.255.0
DHCP Server	<input checked="" type="radio"/> Enable	
	Start IP address	192.168.20.10
	Stop IP address	192.168.20.250
	Subnet mask	255.255.255.0
	DHCP Reservations	Config
	<input type="radio"/> Disable	

Illustration 4: IP Settings

IP Settings

LAN Interface

To configure the LAN interface's IP address and subnet mask.

DHCP Server

(Applicable to Pismolabs 101 mini AP Series)

To configure and enable the built-in DHCP server or not. If enabled, the IP address range can be configured. Configure DHCP Reservation if there is a need to assign a specific IP address to a specific MAC address using DHCP.

4.3.2 Wireless Settings

Wireless Settings	SSID	<input type="text" value="MySSID"/> (MySSID)
	Radio Mode	<input type="text" value="802.11b/g"/> ▼
	Channel Scanning Mode	<input type="text" value="Full"/> ▼
	Bit Rate	<input type="text" value="auto"/> ▼ Mbps (auto)
	Authentication	<input type="text" value="Open"/> ▼ (open)
	Encryption Key	None
	Preferred AP	MAC <input type="text"/> (e.g. 00116E1014A0) Min Signal Strength <input type="text"/> dBm (e.g. -75)

Illustration 5: Wireless Settings

Wireless Settings	
SSID	To configure the SSID / ESSID / Network Name of the wireless network to associate to.
Radio Mode	It allows the user to choose between radio modulations support. E.g. 802.11b/g, 802.11g only, 802.11b, etc. The available settings depend on the Wi-Fi module installed on the device.
Channel Scanning Mode	To select different channels that preferred to scan.
Bit Rate	To fix the 802.11 transmit bit rate. Available options depend on the Radio Mode chosen. If auto is chosen, the device will choose the best bit rate dynamically and automatically.
Authentication	Available options are Open, Static WEP Key, 802.1x with dynamic WEP key, WPA/WPA2-Enterprise and WPA/WPA2-Personal. The selection should be according to the setting of the access point you are associating to. Data transferred are encrypted under all modes except in Open mode. When Static WEP Key or WPA/WPA2-Personal is chosen, you should enter an encryption key in the Encryption Key field. You do not need to use 802.1x and WPA/WPA2-Enterprise unless instructed to do so by your ISP.
Preferred AP	The MAC address of a preferred access point can be entered here. When the preferred access point is found and its signal strength is higher than the Min Signal Strength, it will connect to this preferred access point, no matter the other access points are found even they have higher signal strength or the same SSID.

4.3.3 Roaming Settings for Pismolabs 101 mini:

Roaming Settings	<input checked="" type="radio"/>	Disable	
	<input type="radio"/>	Enable	
		Background Scanning Interval	<input type="text" value="24"/> Hours (24)
		Roaming Threshold (Signal Level Gain)	<input type="text" value="10"/> dBm (10)

Illustration 6: Roaming Settings

Roaming Settings	
Roaming Settings	To configure and enable roaming among APs with the same SSID and authentication method.
Background Scanning Interval	The time interval between background scans.
Roaming Threshold (Signal Level Gain)	If there is another AP with a signal level greater than the signal level of connected AP by the specified value, it will reconnect to the AP with better signal.

4.3.4 Wireless IP Settings

IP Settings	<input checked="" type="radio"/> Configure Manually	
	IP Address	<input type="text" value="0.0.0.0"/>
	Subnet Mask	<input type="text" value="0.0.0.0"/>
	Default Gateway	<input type="text" value="0.0.0.0"/>
	Preferred DNS Server	<input type="text" value="0.0.0.0"/>
	Alternate DNS Server	<input type="text" value="0.0.0.0"/>
	<input type="radio"/> Obtain an IP Address using DHCP	
<input type="radio"/> Obtain an IP Address using PPPOE		
MTU Size	<input type="text" value="1500"/>	
AP Settings	<input checked="" type="radio"/> Disable	
	<input type="radio"/> Configure Manually	
	<input type="radio"/> Configure Automatically	
	Keep AP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
	Broadcast SSID	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
	Client Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
	AP Transmit Power Adjustment	<input type="text" value="default"/> (default)

Illustration 7: Wireless IP Settings

Wireless IP Settings	
IP Settings	The IP address can be obtained automatically or configured manually. If you choose to manually configure the IP address for your unit, enter the fields IP Address, Subnet Mask, Default Gateway, Preferred DNS Server and Alternate DNS Server.
MTU Size	You may also set the MTU Size to increase the data packet size your unit can handle at one time.
AP Settings	(Applicable to Pismolabs 101 mini AP Series) The AP Settings will be covered in detail in the subsequent section Integrated Wi-Fi Access Point Configuration .

4.3.5 Restore and Reboot

WAI Redirection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <small>(Note: you need to reboot CPE for this change to take effect)</small>
Web Password Protection	<input type="radio"/> Enable <input checked="" type="radio"/> Disable Password <input type="password" value="*****"/> (admin) <small>(Note: login name is "root")</small>
Restore Factory Settings	<input type="button" value="Restore & Reboot"/>
Reboot CPE	<input type="button" value="Reboot"/>
<input type="button" value="Save"/>	

Illustration 8: Restore and Reboot

Restore and Reboot

WAI Redirection

If the device is not connected to an access point, and the user is accessing an Internet web site, the settings control whether to redirect the web access to the web admin interface page or not. If this is disabled and the device is not connected, the browser will show a web access error message. The user can still access the web admin interface by accessing to the device's LAN IP address. By default, the LAN IP address is set as *http://192.168.20.1*.

Web Password Protection

Sets the password to protect the web user interface.

Restore Factory Settings

To restore the device to default settings. When this option is clicked, default settings will be restored and the unit will be restarted.

Reboot CPE

To restart the device.

4.4 Integrated Wi-Fi Access Point Configuration

Integrated Wi-Fi Access Point is configured via the **CPE Setup** tab. The following sections will provide information as a guide through the configuration.

The available Access Point (AP) settings for the Integrated Wi-Fi Access Point functionality are as follows:

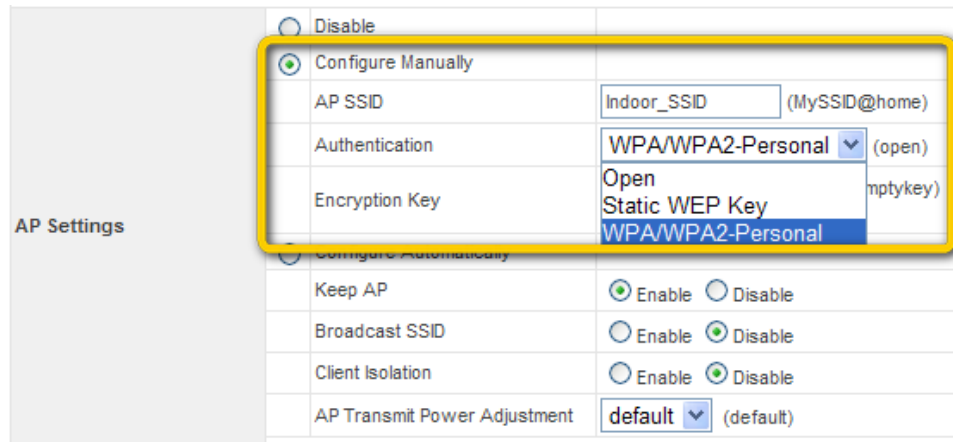
- **Disable**
Integrated Wi-Fi Access Point functionality is disabled.
- **Configure Manually**
Manual configuration of the SSID, Authentication, and Encryption Key values corresponding to the Access Point.
- **Configure Automatically**
The SSID, Authentication, and Encryption Key values corresponding to the Access Point are automatically configured to be the same as the respective values that correspond to the ISP's network.

4.4.1 Access Point Disabled

AP Settings	<input checked="" type="radio"/> Disable	
	<input type="radio"/> Configure Manually	
	<input type="radio"/> Configure Automatically	
	Keep AP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
	Broadcast SSID	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
	Client Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
	AP Transmit Power Adjustment	default <input type="button" value="v"/> (default)

Illustration 9: Access Point Disabled

4.4.2 Access Point configure Manually



<input type="radio"/> Disable	
<input checked="" type="radio"/> Configure Manually	
AP SSID	Indoor_SSID (MySSID@home)
Authentication	WPA/WPA2-Personal (open)
Encryption Key	Open Static WEP Key WPA/WPA2-Personal
<input type="radio"/> Configure Automatically	
Keep AP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Broadcast SSID	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Client Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
AP Transmit Power Adjustment	default (default)

Illustration 10: Access Point Configure Manually

Configure Manually

AP SSID In Manual Configuration mode, the SSID is manually entered.

It can be one of three configurable values:

Authentication

- **Open**
No Encryption Key is necessary.
- **Static WEP Key**
A 64- or 128-bit Encryption Key is required, and can be entered in either an ASCII or HEX representation.
- **WPA/WPA2-Personal**
An Encryption Key, of at least 8 characters, is required.

4.4.3 Access Point Configure Automatically

AP Settings	<input type="radio"/> Disable	
	<input type="radio"/> Configure Manually	
	<input checked="" type="radio"/> Configure Automatically	
	Keep AP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
	Broadcast SSID	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Client Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
AP Transmit Power Adjustment	default ▼ (default)	

Illustration 11: Access Point Configure Automatically

AP Settings	
Broadcast SSID	With this option enabled, the configured SSID will be broadcast such that it can be detected by an SSID scan. Otherwise, the configured SSID will not be broadcast such that it cannot be detected by an SSID scan. In order to connect with the access point, the SSID needs to be known by the client.
Client Isolation	Prevent wireless clients connected to the AP from communicating with each other.
Keep AP	With this option enabled, the Wi-Fi Access Point will always on even if there is no connection to the mesh network.
AP Transmit Power Adjustment	An option to retain a lower power setting for indoor home devices. Available options are between -1 dBm and -15dBm.

With the Access Point Configuration set to **Configure Automatically**, the **SSID**, **Authentication**, and **Encryption Key** values of the Integrated Wi-Fi Access Point will be configured to be the same as in the *4.3.2 Wireless IP Settings* section.

This configuration mode is effectively equivalent to directly connecting 802.1b/g devices on the customers' premises with Citywide Wi-Fi.

Important Note

In the *Wireless Settings* section, if Authentication is set to either **802.1x with dynamic WEP key** or **WPA/WPA2-Enterprise**, then the Configure Automatically option of the Access Point Configuration becomes unavailable, because the Integrated Wi-Fi Access Point functionality currently does not support authentication via the 802.1x with dynamic WEP key and WPA/WPA2-Enterprise methods.

4.5 Test the Setup

To test the setup, you can now go to the unit's main page, enter the user name and password. The realm (the text box next to the "@" sign) value can be left empty. Then click the Connect button.

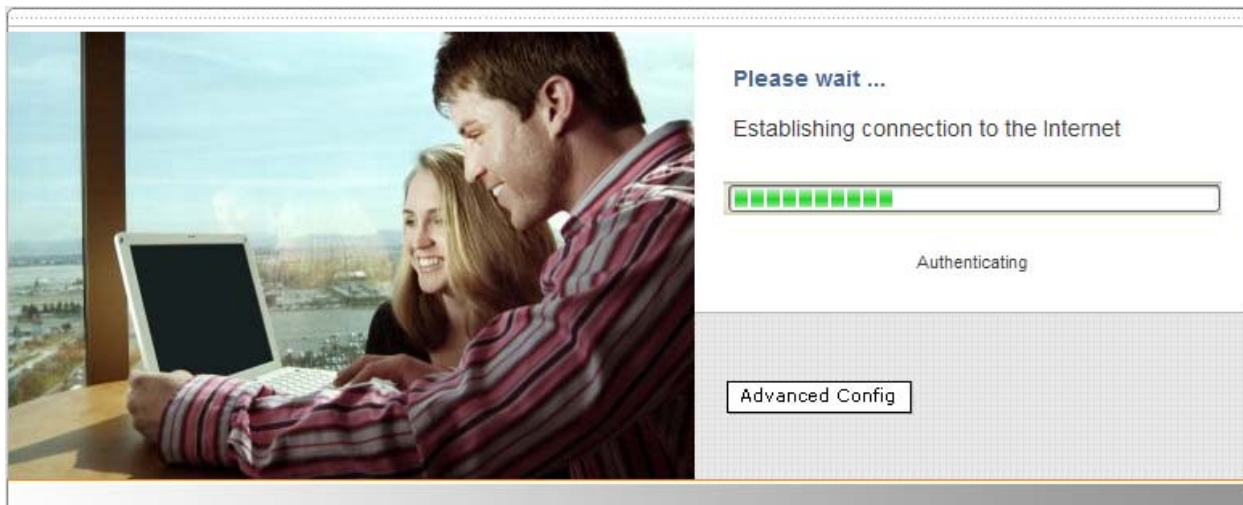


Illustration 12: Establishing Connection to the Internet

After connected, you should see:




Illustration 13: Internet Connection Established

4.6 Port Forwarding

The Pismolabs devices can forward traffic from different port(s) to a specific IP address.

Port Forwarding Settings	
Service Port Range	Enter a port or a range of ports that would like to forward.
Protocol	The Protocol for the above port(s) forwarding. You should select at least one protocol between TCP and UDP .
IP Address	The IP address that you would like the traffics forwarded to.
Del	By clicking the button, you can delete the corresponding rows of port forwarding rules.

[Connect](#) | [CPE Setup](#) | [Port Forward](#) | [QoS](#) | [Firmware Upgrade](#) | [Debug](#)



Service Port Range	Protocol	IP Address	
0 ~ 0	<input type="checkbox"/> TCP <input type="checkbox"/> UDP		Del
0 ~ 0	<input type="checkbox"/> TCP <input type="checkbox"/> UDP		Del
0 ~ 0	<input type="checkbox"/> TCP <input type="checkbox"/> UDP		Del
0 ~ 0	<input type="checkbox"/> TCP <input type="checkbox"/> UDP		Del
0 ~ 0	<input type="checkbox"/> TCP <input type="checkbox"/> UDP		Del
0 ~ 0	<input type="checkbox"/> TCP <input type="checkbox"/> UDP		Del
0 ~ 0	<input type="checkbox"/> TCP <input type="checkbox"/> UDP		Del
0 ~ 0	<input type="checkbox"/> TCP <input type="checkbox"/> UDP		Del
0 ~ 0	<input type="checkbox"/> TCP <input type="checkbox"/> UDP		Del
0 ~ 0	<input type="checkbox"/> TCP <input type="checkbox"/> UDP		Del
0 ~ 0	<input type="checkbox"/> TCP <input type="checkbox"/> UDP		Del
0 ~ 0	<input type="checkbox"/> TCP <input type="checkbox"/> UDP		Del
0 ~ 0	<input type="checkbox"/> TCP <input type="checkbox"/> UDP		Del
0 ~ 0	<input type="checkbox"/> TCP <input type="checkbox"/> UDP		Del
0 ~ 0	<input type="checkbox"/> TCP <input type="checkbox"/> UDP		Del
0 ~ 0	<input type="checkbox"/> TCP <input type="checkbox"/> UDP		Del
0 ~ 0	<input type="checkbox"/> TCP <input type="checkbox"/> UDP		Del
0 ~ 0	<input type="checkbox"/> TCP <input type="checkbox"/> UDP		Del
0 ~ 0	<input type="checkbox"/> TCP <input type="checkbox"/> UDP		Del
0 ~ 0	<input type="checkbox"/> TCP <input type="checkbox"/> UDP		Del
0 ~ 0	<input type="checkbox"/> TCP <input type="checkbox"/> UDP		Del
0 ~ 0	<input type="checkbox"/> TCP <input type="checkbox"/> UDP		Del

Well-known ports
(commonly used ports)

- 7 (Echo)
- 21 (FTP)
- 23 (TELNET)
- 25 (SMTP)
- 53 (DNS)
- 79 (finger)
- 80 (HTTP)
- 110 (POP3)
- 119 (NNTP)
- 161 (SNMP)
- 162 (SNMP Trap)

DMZ Host

Enable Disable

IP Address

0.0.0.0

Save

Below the port forwarding table is an option called **DMZ Host**. If you **Enable** this function, you can manually enter an IP address, which will be the IP address of the device that expose to the Internet. The purpose of a DMZ is adding an additional layer of security to your LAN, which may make all external users can only has access to the device in the DMZ, rather than the whole of the network.

Tip

Below is a table showing some well-known ports, which is officially registered with IANA.

Port Number	Description	Protocol
7	Echo	TCP, UDP
21	FTP	TCP
23	TELNET	TCP
25	SMTP	TCP, UDP
53	DNS	TCP, UDP
79	Finger	TCP
80	HTTP	TCP, UDP
110	POP3	TCP
119	NNTP	TCP
161	SNMP	TCP, UDP
162	SNMP Trap	TCP, UDP

4.8 Firmware Upgrade

The Pepwave devices are able to check whether a newer firmware (the software running on the unit) is available.

However, it is recommended that you do not update the firmware unless specifically instructed by your ISP to do so. When a firmware upgrade is needed, your ISP will either give you instructions or upgrade the firmware remotely.

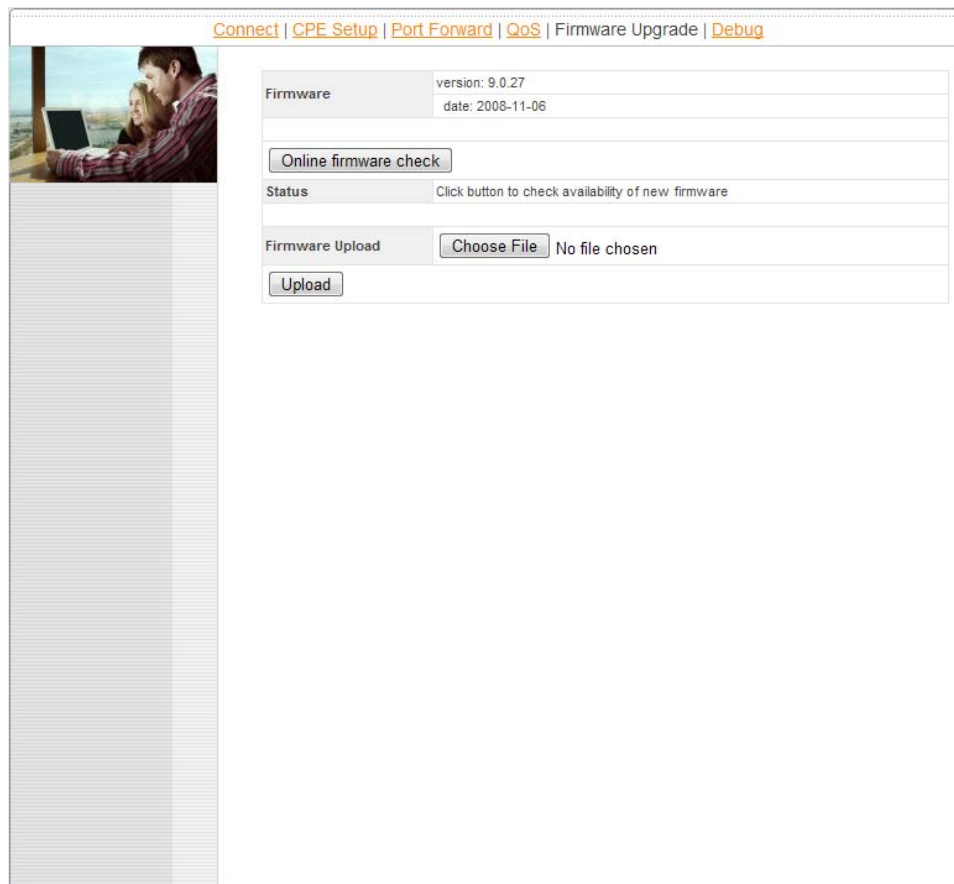


Illustration 14: Firmware tab showing the system information

Tip

It is highly recommended users to download the configuration file (download directory can be found in the next section) for backup propose before doing firmware upgrade.

4.9 Debug and System information

The screenshot displays the 'Debug' tab of the Pismolabs 101 mini web interface. It features a navigation menu at the top with options: Connect, CPE Setup, Port Forward, QoS, Firmware Upgrade, and Debug. The main content area is divided into several sections:

- System Information:** A table listing device details such as Firmware Version (9.0.27), Hardware Version (1.1), Model (Surf AP 200 (Router)), Serial Number (2800-1122-AABB), LAN MAC Address (00:11:AA:22:BB:11), Wi-Fi MAC Address (00:11:AA:22:BB:22), Supported Modes (802.11b/g), and Connection Uptime (9 mins 55 secs).
- Scanned APs:** A table showing detected access points. The first entry is 'PLHQ_BALANCE' with BSSID '00:11:ab:cb:db:11', Channel '1', Signal Level '-51', Encryption 'WPA-Personal', and Bit Rates 'All 802.11b/g rates'. An 'Auto Refresh' button is set to 'Off' with a '10' second interval.
- Total APs:** A bar chart showing 'Total APs: 1'. A list of channels (CH 1 to CH 11) is shown with corresponding signal levels, where CH 1 has a level of '1' and others are '0'.
- WAN Connection Info:** A detailed table of network parameters including Signal level (-51 dBm), Bit rate (54), Missed beacon (20), ESSID (PLHQ_BALANCE), Mode (802.11g), Frequency (2.412GHz), Channel (1), AP BSSID (00:11:AA:22:BB:33), Encryption Key (ABCD-AAA-1234-0000-BBBB-CCCC-1234-ABCD), and various statistics like Rx invalid crypt (0), Tx excessive retries (0), and Invalid misc (0).
- DHCP Client List:** A table listing active DHCP clients with IP Address (192.168.20.10) and MAC Address (00:aa:11:bb:22:33).
- Download Links:** Two buttons at the bottom are highlighted with yellow boxes: 'Click here to download the configuration file' and 'Click here to download a debug dump'. A larger button to the right says 'Click the links to download files'.

Illustration 15: Debug tab showing the system information

Tip

Debug dump and **configuration file** can be downloaded through clicking the links illustrated above. If you encounter issues and would like to contact Technical Support Team, please download the above files and attach it along with a description of your encountered issue.

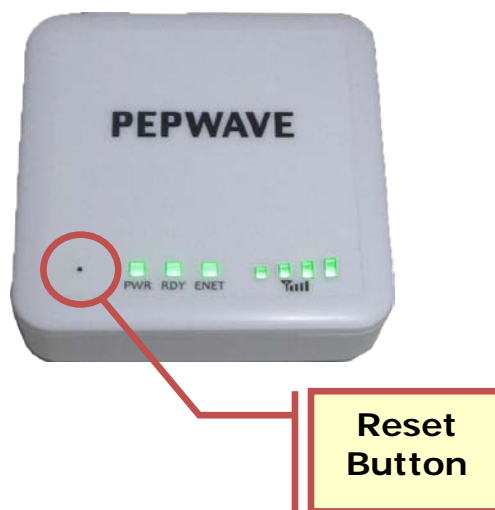
4.10 Restore to Default Settings

4.10.1 Pismolabs 101 mini Indoor Series

There are two ways to restore the Pismolabs 101 mini Indoor unit 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 also power up the unit and wait for about 1 min. Then press the **Reset Button** at the rear side of the unit using a pin and then hold it for 5 seconds. The unit will restore the settings to factory default and reboot.



Appendix:

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

sales@pepwave.com

Support

support@pepwave.com

Business Development and Partnerships

partners@pepwave.com

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