

# User Manual

**Smart Terminal with LCD Display**

**April 2017**

#### **COPYRIGHT & TRADEMARKS**

Specifications are subject to change without notice. Copyright © 2017 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

<b>1</b>	<b>Package Contents .....</b>	<b>3</b>
<b>2</b>	<b>Hardware Overview.....</b>	<b>3</b>
<b>2.1</b>	<b>Installation Procedures.....</b>	<b>4</b>
<b>3</b>	<b>Using the Dashboard .....</b>	<b>5</b>
<b>3.1</b>	<b>General.....</b>	<b>5</b>
<b>4</b>	<b>Configuration.....</b>	<b>6</b>
<b>4.1</b>	<b>System .....</b>	<b>6</b>
<b>4.1.1</b>	<b>Admin Security .....</b>	<b>6</b>
<b>4.1.2</b>	<b>Firmware.....</b>	<b>8</b>
<b>4.1.3</b>	<b>Time .....</b>	<b>9</b>
<b>4.1.4</b>	<b>Event Log .....</b>	<b>9</b>
<b>4.1.5</b>	<b>Controller .....</b>	<b>10</b>
<b>4.1.6</b>	<b>Configuration .....</b>	<b>11</b>
<b>4.1.7</b>	<b>Reboot.....</b>	<b>12</b>
<b>5</b>	<b>Monitoring Device Status .....</b>	<b>13</b>
<b>5.1</b>	<b>Device .....</b>	<b>13</b>
<b>5.2</b>	<b>Event Log .....</b>	<b>14</b>
<b>6</b>	<b>Restoring Factory Defaults .....</b>	<b>14</b>
<b>7</b>	<b>Appendix.....</b>	<b>15</b>

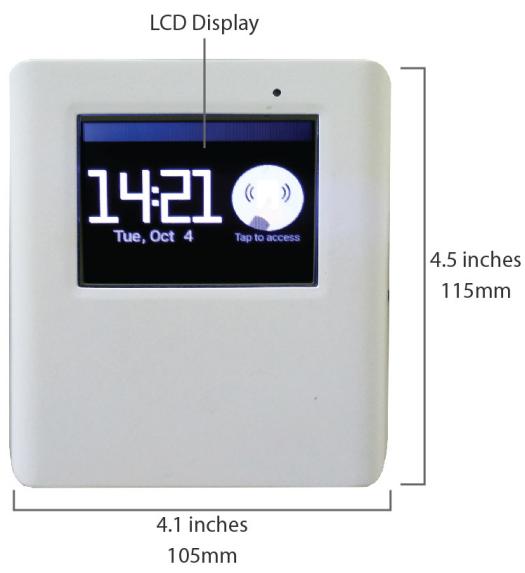
# 1 Package Contents

1 x Smart Terminal

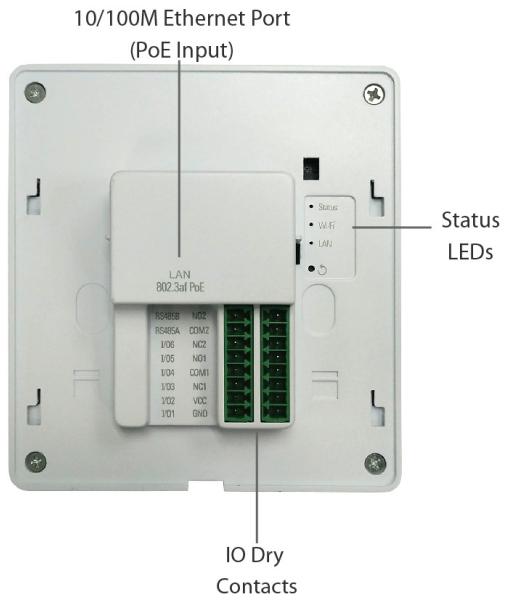
1 x Instruction sheet

# 2 Hardware Overview

## Front/Top View

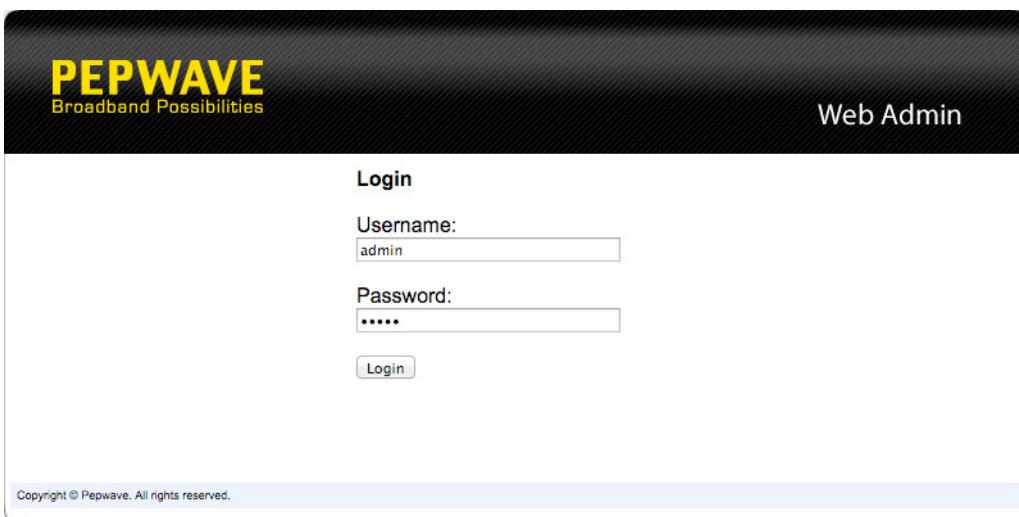


## Rear Panel View

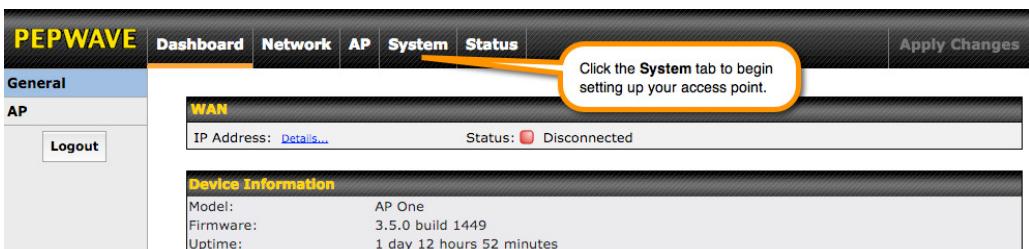


## 2.1 Installation Procedures

1. Connect the Ethernet port on the unit to the backbone network using an Ethernet cable. The port should auto sense whether the cable is straight-through or crossover.
2. Plug in the PoE Cable.
3. Wait for the status LED to turn green.
4. Connect a PC to the backbone network. Configure the IP address of the PC to be any IP address between 192.168.0.4 and 192.168.0.254, with a subnet mask of 255.255.255.0.
5. Using Microsoft Internet Explorer 6 or above, Mozilla Firefox 2.0 or above, or Google Chrome 2.0 or above, connect to <https://192.168.0.3>.
6. Enter the default admin login ID and password, **admin** and **public** respectively.

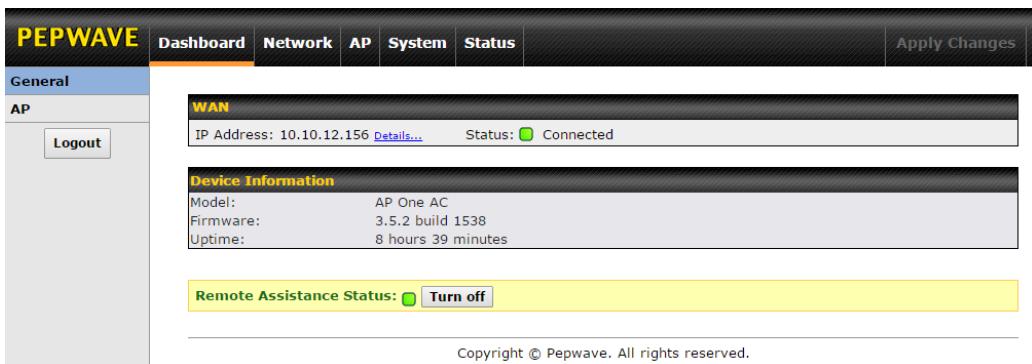


7. After logging in, the Dashboard appears. Click the **System** tab to begin setting up your access point.



## 3 Using the Dashboard

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



### 3.1 General

This section contains WAN status and general device information.

The screenshot shows a detailed view of the WAN status. The top section displays the WAN IP address (10.10.12.156) and status (Connected). Below this, a 'WAN' section provides a general description: 'When your access point is connected to a WAN, this field displays the WAN IP address. For more information, click the Details... link, which displays the following:'. A 'Details of WAN' table is shown, listing connection type (DHCP), IP address (10.10.12.156), subnet mask (255.255.0.0), default gateway (10.10.10.1), and DNS servers (10.10.10.1). The table includes a 'Close' button in the top right corner. The bottom section, labeled 'Status', states: 'This field displays the current WAN connection status.'

Details of WAN	
Connection Type	DHCP
IP Address	10.10.12.156
Subnet Mask	255.255.0.0
Default Gateway	10.10.10.1
DNS Servers	10.10.10.1

Device Information	
Model:	AP One AC
Firmware:	3.5.2 build 1538
Uptime:	8 hours 49 minutes

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

## 4 Configuration

### 4.1 System

The options on the **System** tab control login and security settings, firmware upgrades, SNMP settings, and other settings.

Admin Settings	
AP Name	AP One
Location	site1
Admin User Name	admin
Admin Password	*****
Confirm Admin Password	*****
Web Admin Interface	<input checked="" type="checkbox"/>
Security	HTTPS <input checked="" type="checkbox"/> HTTP to HTTPS Redirection
Web Admin Port	443
Allowed Source IP Subnets	<input checked="" type="radio"/> Any <input type="radio"/> Allow access from the following IP subnets only
Language	English

#### 4.1.1 Admin Security

The **Admin Security** section allows you to set up your access point's name, password, security settings, and other options.

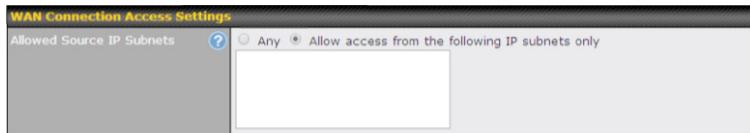
Admin Settings	
AP Name	AP One
Location	site1
Admin User Name	admin
Admin Password	*****
Confirm Admin Password	*****
Web Admin Interface	<input checked="" type="checkbox"/>
Security	HTTPS <input checked="" type="radio"/> HTTP to HTTPS Redirection
Web Admin Port	443
Allowed Source IP Subnets	<input checked="" type="radio"/> Any <input type="radio"/> Allow access from the following IP subnets only
Language	English

Admin Security	
<b>Device Name</b>	Enter a name to identify your Smart Terminal. This name can be retrieved via SNMP.
<b>Location</b>	Enter a name to identify the location of your access point. This name can be retrieved via SNMP.
<b>Admin User Name</b>	This field specifies the administrator username of the web admin. It is set as <i>admin</i> by default.
<b>Admin Password</b>	This field allows you to specify a new administrator password. The default password is <i>public</i> .
<b>Confirm Admin Password</b>	Re-enter the admin password.
<b>Web Admin Interface</b>	Check this box to turn on the web administration interface, which allows remote AP management.
<b>Security</b>	Choose <b>HTTP</b> or <b>HTTPS</b> as the protocol to use when accessing the web admin interface. To automatically redirect HTTP access to HTTPS, check <b>HTTP to HTTPS Redirection</b> .
<b>Web Admin Port</b>	Specify the port number on which the web admin interface can be accessed.

## Allowed Source IP Subnets

This field allows you to restrict access to the web admin to only defined IP subnets.

- **Any** - Allow web admin accesses from anywhere, without IP address restrictions.
- **Allow access from the following IP subnets only** – Restricts the ability to access web admin to only defined IP subnets. When this option is chosen, a text input area will appear:



Enter your allowed IP subnet addresses into this text area. Each IP subnet must be in the form of  $w.x.y.z/m$ .  $w.x.y.z$  represents an IP address (e.g., 192.168.0.0), and  $m$  represents the subnet mask in CIDR format, which is between 0 and 32 inclusively. For example: 192.168.0.0/24. To define multiple subnets, separate each IP subnet, one per line. For example:

192.168.0.0/24

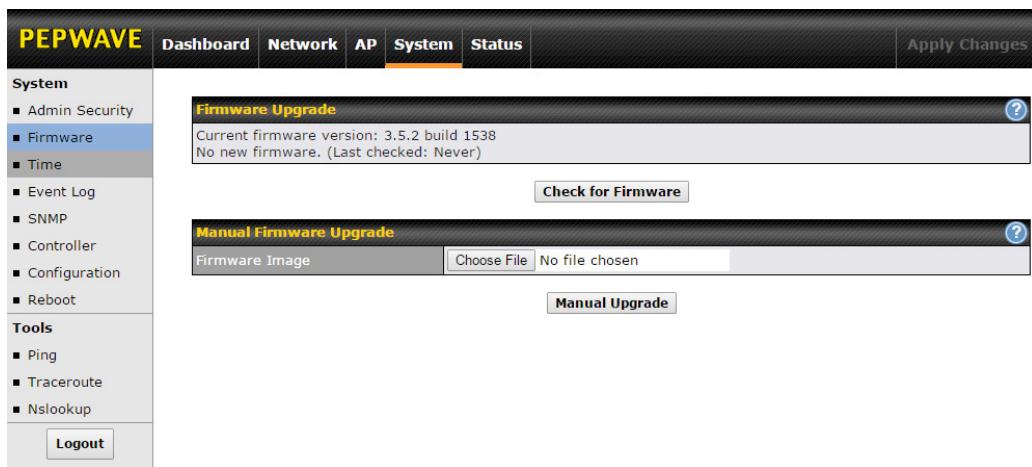
10.8.0.0/16

## Language

Choose a language for the administration interface.

### 4.1.2 Firmware

The **Firmware** section lets you check the firmware version currently used by your access point, as well as check for and install new firmware via online download. You can also upgrade your firmware using a firmware file stored locally.



To check for new firmware, click the **Check for Firmware** button. If new firmware is

available, your access point will automatically download and install it.

To upgrade your access point using a firmware file on your network, click **Choose File** to select the firmware file. Then click **Manual Upgrade** to initiate the firmware upgrade process using the selected file.

Note that your access point can store two different firmware versions in two different partitions. A firmware upgrade will always replace the inactive partition. If you want to keep the inactive firmware, simply reboot your device with the inactive firmware and then perform the firmware upgrade.

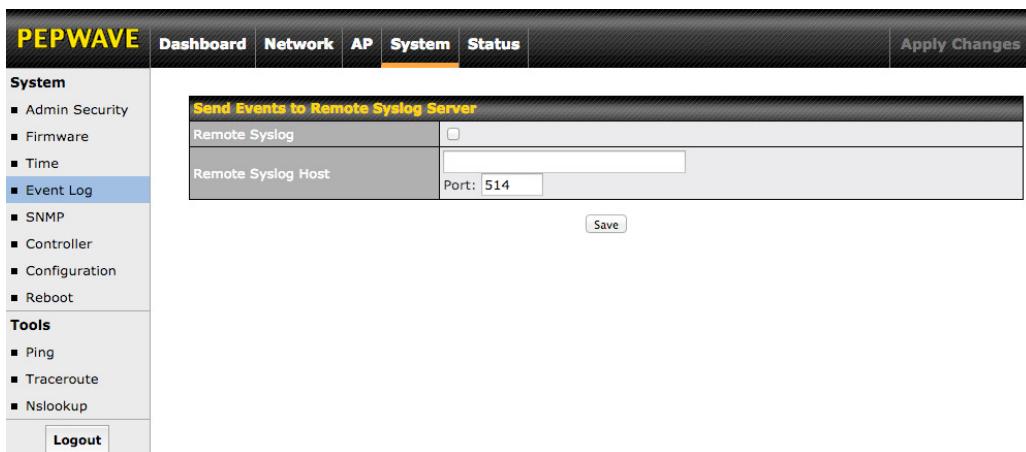
#### 4.1.3 Time

The settings in this section govern the access point's system time zone and allow you to specify a custom timeserver.

Time	
<b>Time Zone</b>	Time region used by the system. All choices are based on UTC.
<b>Time Server</b>	To choose a time server other than the default, enter the URL here. To restore the default time server, click the <b>Default</b> button.

#### 4.1.4 Event Log

The section allows you to turn on event logging at a specified remote syslog server.



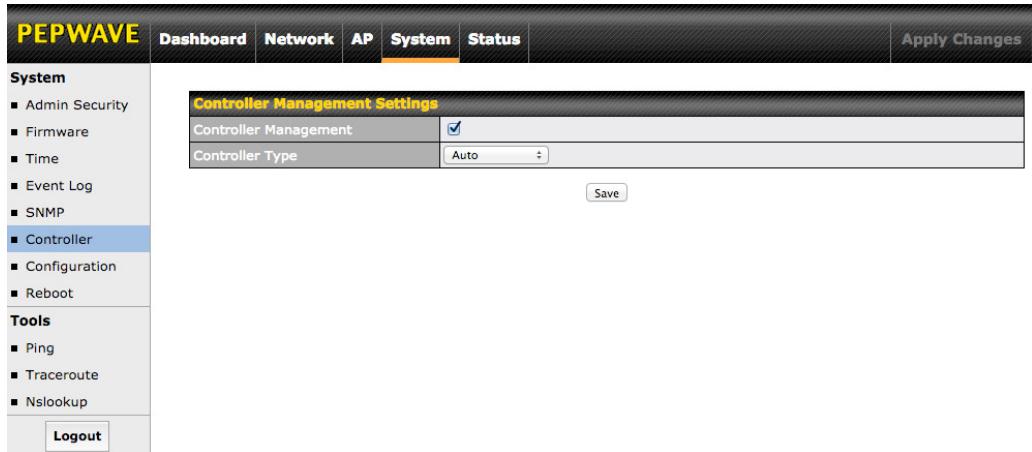
The screenshot shows the PEPWAVE web interface with the following details:

- Header:** PEPWAVE, Dashboard, Network, AP, System (highlighted in yellow), Status, Apply Changes.
- Left Sidebar (System):** Admin Security, Firmware, Time, Event Log (highlighted in blue), SNMP, Controller, Configuration, Reboot.
- Left Sidebar (Tools):** Ping, Traceroute, Nslookup.
- Logout button:** Located at the bottom of the sidebar.
- Main Content:**
  - Section Title:** Send Events to Remote Syslog Server
  - Form Fields:** Remote Syslog (checkbox), Remote Syslog Host (input field with value "514"), Port: 514.
  - Buttons:** Save (button).

Event Log	
<b>Remote Syslog</b>	Check this box to turn on remote system logging.
<b>Remote Syslog Host</b>	Enter the IP address or hostname of the remote syslog server, as well as the port number.

#### 4.1.5 Controller

In the **Controller** section, you can set up Peplink InControl or AP Controller remote management.



The screenshot shows the Peplink InControl web interface. The left sidebar has a 'System' section with 'Controller' selected. The main content area is titled 'Controller Management Settings' and contains two fields: 'Controller Management' with a checked checkbox and 'Controller Type' with a dropdown set to 'Auto'. A 'Save' button is at the bottom.

Controller Management Settings	
<b>Controller Management</b>	Check this box to enable remote management.
<b>Controller Type</b>	Select <b>Auto</b> , <b>InControl</b> , or <b>AP Controller</b> as your remote AP management method. When <b>Auto</b> is selected, your access point will automatically choose the appropriate mode.

## 4.1.6 Configuration

In this section, you can manage and backup access point configurations, as well as reset your access point to its factory configuration. Backing up your access point's settings immediately after successful initial setup is strongly recommended.

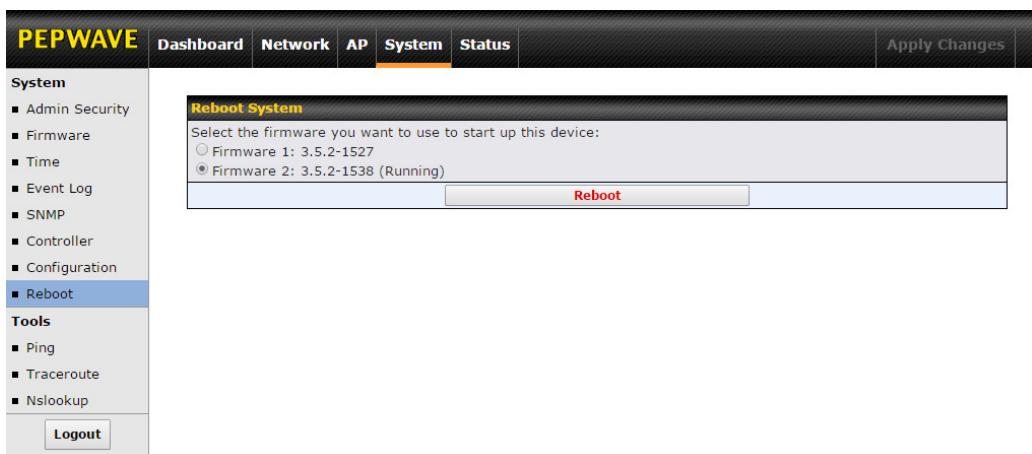
The screenshot shows the PEPWAVE web admin interface. The top navigation bar includes links for Dashboard, Network, AP, System (which is highlighted in orange), and Status, along with an 'Apply Changes' button. The left sidebar has a 'System' section with options like Admin Security, Firmware, Time, Event Log, SNMP, Controller, Configuration (which is selected and highlighted in blue), and Reboot. It also includes a 'Tools' section with Ping, Traceroute, and Nslookup, and a 'Logout' button. The main content area has three sections: 'Restore Configuration to Factory Settings' (with a 'Preserve Settings' checkbox and a 'Restore Factory Settings' button), 'Download Active Configurations' (with a 'Download' button), and 'Upload Configurations' (with a 'Choose File' button and a 'No file chosen' message, and an 'Upload' button).

Configuration	
<b>Restore Configuration to Factory Settings</b>	The <b>Restore Factory Settings</b> button resets the configuration to factory default settings. After clicking the button, click the <b>Apply Changes</b> button on the top right corner to make the settings effective. To save existing network settings when restoring factory settings, check the <b>Network Settings</b> box before clicking <b>Restore Factory Settings</b> .
<b>Download Active Configurations</b>	Click <b>Download</b> to backup the current active settings.
<b>Upload Configurations</b>	To restore or change settings based on a configuration file, click <b>Choose File</b> to locate the configuration file on the local computer, and then click <b>Upload</b> . The new settings can then be applied by clicking the <b>Apply Changes</b> button on the page header, or you can cancel the procedure by pressing <b>discard</b> on the main page of the web admin interface.

#### 4.1.7 Reboot

This section provides a reboot button for restarting the system. For maximum reliability, your access point can equip with two copies of firmware, and each copy can be a different version. You can select the firmware version you would like to reboot the device with. The firmware marked with **(Running)** is the current system boot up firmware.

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

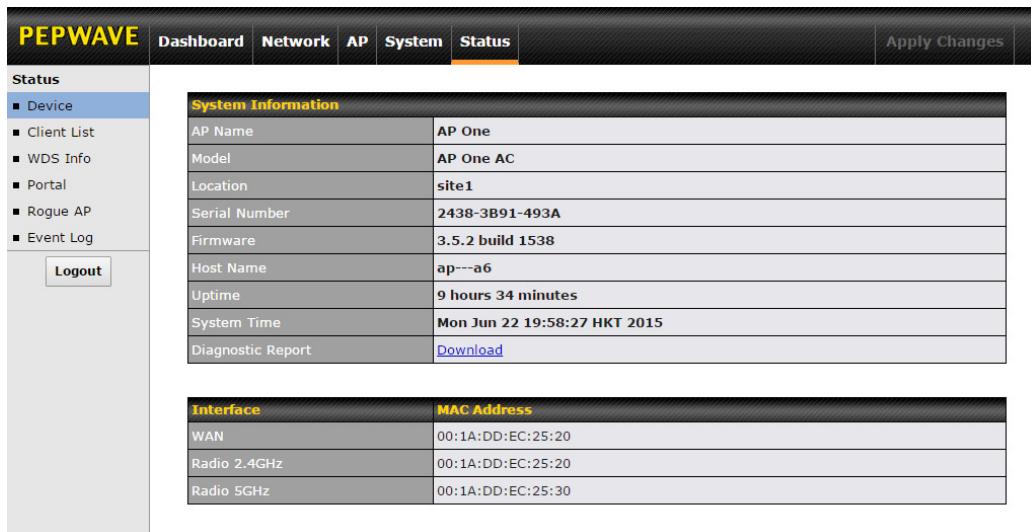


## 5 Monitoring Device Status

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

### 5.1 Device

Here you can access a variety of data about your access point, download a diagnostic report, and check MAC addresses. To download a diagnostic report, click the **Download** link.



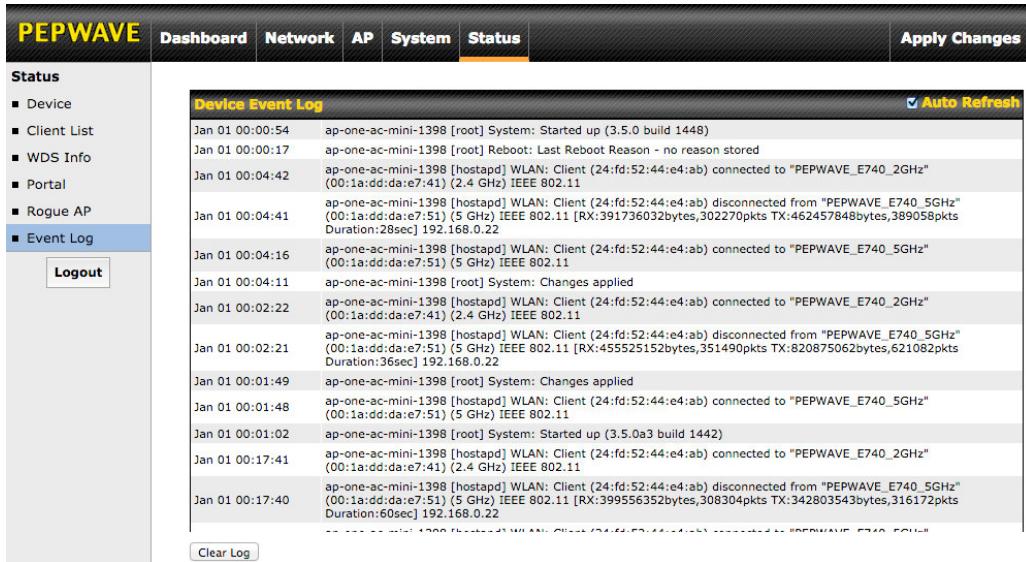
The screenshot shows the PEPWAVE Status interface. The left sidebar has a 'Status' section with links for Device, Client List, WDS Info, Portal, Rogue AP, and Event Log, and a Logout button. The main content area has tabs for Dashboard, Network, AP, System, and Status, with Status selected. The Status tab displays two tables: 'System Information' and 'Interface MAC Address'.

System Information	
AP Name	AP One
Model	AP One AC
Location	site1
Serial Number	2438-3B91-493A
Firmware	3.5.2 build 1538
Host Name	ap---a6
Uptime	9 hours 34 minutes
System Time	Mon Jun 22 19:58:27 HKT 2015
Diagnostic Report	<a href="#">Download</a>

Interface	MAC Address
WAN	00:1A:DD:EC:25:20
Radio 2.4GHz	00:1A:DD:EC:25:20
Radio 5GHz	00:1A:DD:EC:25:30

## 5.2 Event Log

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



The screenshot shows the PEPWAVE Status interface. The left sidebar has a 'Status' section with links for Device, Client List, WDS Info, Portal, Rogue AP, and Event Log, with 'Event Log' being the active tab. The main content area is titled 'Device Event Log' and shows a list of log entries. A checkbox for 'Auto Refresh' is checked. A 'Clear Log' button is located at the bottom of the log table. The log entries are as follows:

Time	Event Description
Jan 01 00:00:54	ap-one-ac-mini-1398 [root] System: Started up (3.5.0 build 1448)
Jan 01 00:00:17	ap-one-ac-mini-1398 [root] Reboot: Last Reboot Reason - no reason stored
Jan 01 00:04:42	ap-one-ac-mini-1398 [hostapd] WLAN: Client (24:fd:52:44:e4:ab) connected to "PEPWAVE_E740_2GHz" (00:1a:dd:da:c7:41) (2.4 GHz) IEEE 802.11
Jan 01 00:04:41	ap-one-ac-mini-1398 [hostapd] WLAN: Client (24:fd:52:44:e4:ab) disconnected from "PEPWAVE_E740_5GHz" (00:1a:dd:da:c7:51) (5 GHz) IEEE 802.11 (RX:391736032bytes,302270pkts TX:462457848bytes,389058pkts Duration:28sec) 192.168.0.22
Jan 01 00:04:16	ap-one-ac-mini-1398 [hostapd] WLAN: Client (24:fd:52:44:e4:ab) connected to "PEPWAVE_E740_5GHz" (00:1a:dd:da:c7:51) (5 GHz) IEEE 802.11
Jan 01 00:04:11	ap-one-ac-mini-1398 [root] System: Changes applied
Jan 01 00:02:22	ap-one-ac-mini-1398 [hostapd] WLAN: Client (24:fd:52:44:e4:ab) connected to "PEPWAVE_E740_2GHz" (00:1a:dd:da:c7:41) (2.4 GHz) IEEE 802.11
Jan 01 00:02:21	ap-one-ac-mini-1398 [hostapd] WLAN: Client (24:fd:52:44:e4:ab) disconnected from "PEPWAVE_E740_5GHz" (00:1a:dd:da:c7:51) (5 GHz) IEEE 802.11 (RX:455525152bytes,351490pkts TX:820875062bytes,621082pkts Duration:36sec) 192.168.0.22
Jan 01 00:01:49	ap-one-ac-mini-1398 [root] System: Changes applied
Jan 01 00:01:48	ap-one-ac-mini-1398 [hostapd] WLAN: Client (24:fd:52:44:e4:ab) connected to "PEPWAVE_E740_5GHz" (00:1a:dd:da:c7:51) (5 GHz) IEEE 802.11
Jan 01 00:01:02	ap-one-ac-mini-1398 [root] System: Started up (3.5.0a3 build 1442)
Jan 01 00:17:41	ap-one-ac-mini-1398 [hostapd] WLAN: Client (24:fd:52:44:e4:ab) connected to "PEPWAVE_E740_2GHz" (00:1a:dd:da:c7:41) (2.4 GHz) IEEE 802.11
Jan 01 00:17:40	ap-one-ac-mini-1398 [hostapd] WLAN: Client (24:fd:52:44:e4:ab) disconnected from "PEPWAVE_E740_5GHz" (00:1a:dd:da:c7:51) (5 GHz) IEEE 802.11 (RX:399556352bytes,308304pkts TX:342803543bytes,316172pkts Duration:60sec) 192.168.0.22

## 6 Restoring Factory Defaults

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

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

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

## 7 Appendix

### **Federal Communication Commission Interference Statement**

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

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

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

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.

5.15 ~ 5.25GHZ is for indoor user only.

### **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.

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

## Industry Canada Statement

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

To maintain compliance with the RF exposure guidelines, place the unit at least 20cm from nearby persons. Mise en garde : Pour assurer la conformité aux directives relatives à l'exposition aux fréquences radio, le jouet doit être placé à au moins 20\_cm des personnes à proximité.

## Caution :

- (i) the device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;
- (ii) the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits specified for point-to-point and non-point-to-point operation as appropriate; and
- (iii) Users should also be advised that high-power radars are allocated as primary users (i.e. priority users) of the bands 5650-5850 MHz and that these radars could cause ***interference and/or damage to LE-LAN devices.***

Avertissement:

- (i) les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
- (ii) le gain maximal d'antenne permis (pour les dispositifs utilisant la bande de 5725 à 5 850MHz) doit être conforme à la limite de la p.i.r.e. spécifiée pour l'exploitation point à point et l'exploitation non point à point, selon le cas;
- (iii) De plus, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des **dommages aux dispositifs LAN-EL**.

**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/](http://www.pepwave.com/partners/channel-partner-program/)