

# User Manual



**EAP350**  
version 1.0

Ceiling Mount, Multi-Function  
Wireless N300 Indoor Access Point

## Table of Contents

---

<b>1</b>	<b>Introduction</b>	<b>5</b>
1.1	Key Features	5
1.2	Package Contents	5
1.3	System Requirements	6
1.4	Package Contents	6
1.5	Applications	6
1.6	Technical Specification	8
1.7	Physical Interface	9
<b>2</b>	<b>Before you Begin</b>	<b>10</b>
2.1	Considerations for Wireless Installation	10
2.2	Computer Settings (in Windows XP/Windows 7/Windows 8)	11
2.3	Computer Settings in Apple Mac OS X	14
2.4	Hardware Installation	15
2.5	Mounting the EAP350	16
<b>3</b>	<b>Configuring Your Access Point</b>	<b>17</b>
3.1	Default Settings	17
3.2	Web Configuration	17
<b>4</b>	<b>Building a Wireless Network</b>	<b>19</b>
4.1	Access Point Mode	19
4.2	WDS AP Mode	19
4.3	WDS Bridge Mode	19
4.4	Repeater mode	20
<b>5</b>	<b>Status</b>	<b>21</b>
5.1	Save/Reload	21

5.2	Main .....	21
5.3	Wireless Client List.....	22
5.4	Connection Status.....	22
5.5	WDS Link List.....	23
5.6	System Log .....	23
<b>6</b>	<b>System .....</b>	<b>24</b>
6.1	Operation Mode.....	24
6.2	IP Settings.....	24
6.3	Spanning Tree Setting.....	25
<b>7</b>	<b>Wireless .....</b>	<b>26</b>
7.1	Wireless Network .....	26
7.2	Wireless Security .....	27
7.3	Site Survey .....	29
7.4	Wireless MAC Filter .....	30
7.5	Wireless Advanced .....	32
7.6	WPS (Wi-Fi Protected Setup).....	33
7.7	WDS Link Settings.....	33
<b>8</b>	<b>Management.....</b>	<b>35</b>
8.1	Administration.....	35
8.2	Management VLAN.....	35
8.3	SNMP.....	37
8.4	Backup/Restore.....	38
8.5	Firmware Upgrade.....	39
8.6	Time Setting.....	39
8.7	Schedule.....	40
8.8	CLI Setting .....	40
8.9	Log.....	41

8.10	Diagnostics.....	41
8.11	Device Discovery.....	42
8.12	LED Control.....	42
8.13	Logout.....	42
8.14	Reset.....	43
<b>Appendix A – FCC Interference Statement .....</b>		<b>44</b>
<b>Appendix B – Industry Canada Statement.....</b>		<b>45</b>
<b>Appendix C – CE Interference Statement.....</b>		<b>46</b>

# 1 Introduction

## 1.1 Key Features

- High Transmit Power, enabling long range connectivity
- Supports IEEE 802.11 b/g/n wireless standards with up to 300Mbps data rate.
- Monitor after deployment with EnGenius EZ Controller™ software. (Free Online download)
- Supports both the included adapter or IEEE 802.3af PoE (Power over Ethernet) – capable Switches or Injectors
- Multiple Application – Access Point / WDS / Repeater

The **EAP350** is a high-powered, long-range 802.11b/g/n Wireless Indoor Access Point with multiple operation modes. It can be deployed in a number of different businesses from a small office to large hotels and multi-story office, hospital or university buildings.

The EAP350 can also be used in large homes to extend the range of an existing network and help to eliminate wireless dead zones caused by certain architectural materials.

To protect data during wireless transmissions, the EAP350 supports industry-standard WPA/WPA2 encryption and



MAC address filtering to authorize only specific devices to access the network.

## 1.2 Package Contents

The EAP350 package contains the following items (Resellers and dealers require that all items must be in the

package to issue a refund):

- EAP350
- 12V/1A 100V~240V Power Adapter
- RJ-45 Ethernet Cable
- CD with User Manual
- Quick Installation Guide
- Wall Mount Screw kit

### **1.3 System Requirements**

The following are the Minimum System Requirements in order to configure the device:

- Computer with an Ethernet interface or wireless network capability.
- Windows OS (XP, Vista, 7, 8), Mac OS X, or Linux-based operating systems.
- Web-Browsing Application (i.e.: Internet Explorer, Firefox, Safari, or other similar browser application).

### **1.4 Package Contents**

- The EAP350 package contains the following items
- EAP350 Access Point
- Power Adapter
- RJ-45 Ethernet Cable
- Quick Installation Guide
- Ceiling and Wall Mount Screw Kit

## **1.5 Applications**

Wireless LAN (WLAN) products are easy to install and highly efficient. The following list describes the benefits of deploying a wireless access point:

### **a) Difficult-to-Wire Environments**

There are many situations where wires cannot be installed, deployed easily or cannot be hidden from view. Many older buildings sites, or areas within a building may make the installation of an Ethernet-based LAN impossible, impractical or expensive.

### **b) Temporary Workgroups**

A deployed wireless access point or several access points, gives businesses the flexibility to create temporary workgroups/networks in more open areas within a building – auditoriums, amphitheater classrooms, ballrooms, arenas, exhibition centers, and temporary offices.

### **c) The Ability to Access Real-Time Information**

Doctors/Nurses, Point-of-Sale Employees, and/or Warehouse Workers can access real-time information on their network via the access point while dealing with patients, serving customers, and/or processing information.

### **d) Frequently Changing Environments**

Setting up an access point, like the EAP350, to provide access to a company network or its Internet connection is quick and easy which also makes it ideal for establishing network access in temporary venues like exhibits, special events, or show rooms.

**e) Small Office and Home Office (SOHO) Networks**

A wireless access point, like the EAP350, is ideal for SOHO users who need a cost-effective way to expand their existing network to provide more access for more devices, easy and quick installation of a small network.

**f) Wireless Extensions to Existing Ethernet-based Networks**

Wireless access points, like the EAP350, enable network administrators, installers and end-users to extend the range and reach of an existing Ethernet-based network.

**g) Training/Educational Facilities**

Training sites at corporations and universities deploy wireless access points to provide connectivity their networks and the Internet connection for their employees and students.

## 1.6 Technical Specification

### Standard

IEEE802.11 b/g/n

### Physical Interface

1 x 10/100/1000 Gigabit Ethernet Port

1 x Reset Button

1 x Power Connector

### LED Indicator

Power

WAN (Wireless Connection)

LAN

### Power Requirement

DC 12V/1A Input

### Operation Modes

Access Point

WDS

Repeater

### Security

WEP (64/128/152bits)

WPA/WPA2(TKIP/AES)

Hidden SSID

MAC Filtering Up to 50 SSIDs

802.1X Authenticator (MD5/TLS/TTLS/PEAP)

### QoS (Quality of Service)

WMM (Wireless Multimedia)

### Physical/Environment Condition

Operating

- Temperature: 0°C to +50°C (-32°F to 104°F)

- Humidity: 0%~90%

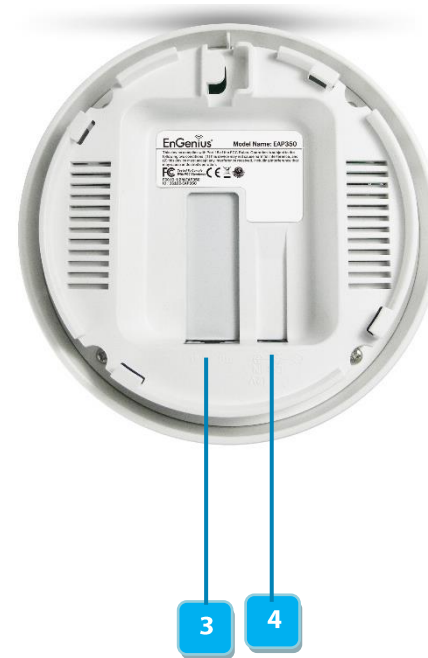
Storage

- Temperature: -20°C ~ +60°C (-4°F to 140°F)

- Humidity: 0%~90%



## 1.7 Physical Interface



Top Side		Bottom Side	
1	LED Signal	3	Gigabit Ethernet Port
2	Reset Button	4	DC Jack (12V/1A Input)

## 2 Before you Begin

This section will guide you through the installation process. Placement of the EnGenius EAP350 is essential to maximize the access point's performance. Avoid placing the EAP350 in an enclosed space such as a closet, cabinet, or stairwell.

### 2.1 Considerations for Wireless Installation

Generally, the exact operating distance of a wireless device, like the EAP350, cannot be pre-determined due to a number of unknown variables or obstacles in the environment in which the device will be deployed. These could be the number, thickness, and location of walls, ceilings, elevator shafts, stairwells, or other objects that the device's wireless signals must pass through. Here are some key guidelines to allow the EAP350 to have optimal wireless range.

- Keep the number of walls and/or ceilings between the EAP350 and other network devices to a minimum.
- Each wall and/or ceiling can reduce the signal strength, resulting in lower signal strength.
- Building materials make a difference. A solid metal door and/or aluminum studs may have a significant negative effect on the signal strength of the EAP350. Locate your wireless devices carefully so the signal can pass through drywall and/or open doorways. Materials such as glass, steel, metal, concrete, water (example: fish tanks), mirrors, file cabinets and/or brick can also diminish wireless signal strength.
- Interference from other electrical devices and/or appliances that generate RF noise can also diminish the EAP350's signal strength. The most common types of devices are microwaves or cordless phones.

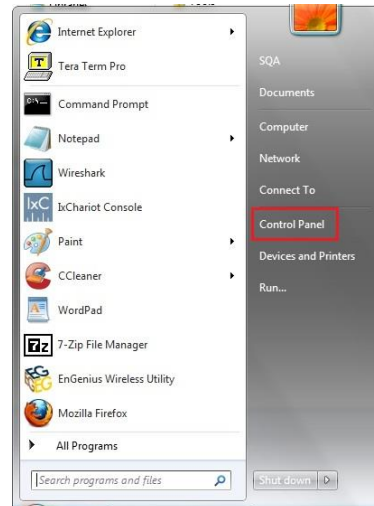
## 2.2 Computer Settings (in Windows XP/Windows 7/Windows 8)

In order to use the EAP350, you must first configure the TCP/IPv4 connection of your Windows OS computer system.

- Click **Start** button and open **Control Panel** in **Windows XP/Windows 7**

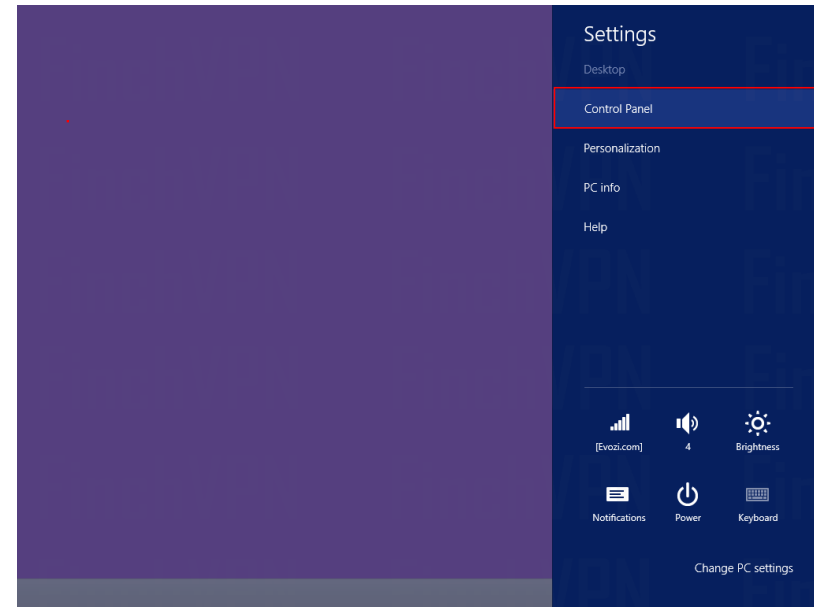


Windows XP



Windows 7

- Move your mouse to the lower right hot corner to display the Charms Bar and select the **Control Panel** in **Windows 8**

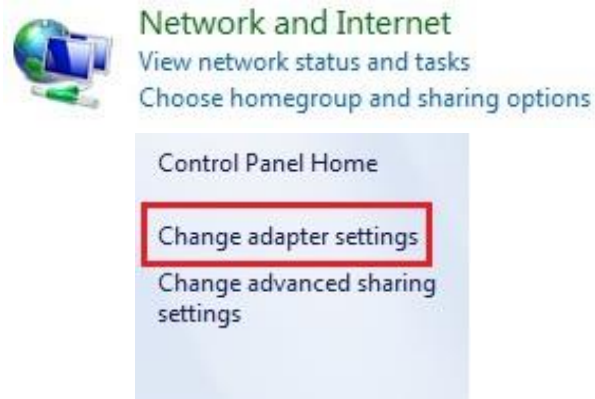


Windows 8

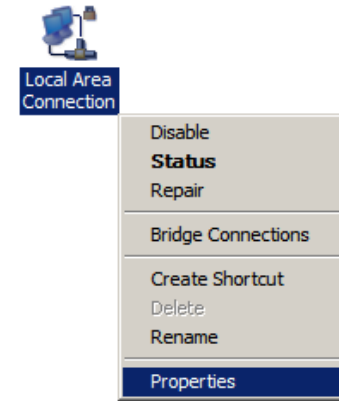
- In **Windows XP**, click **Network Connection**



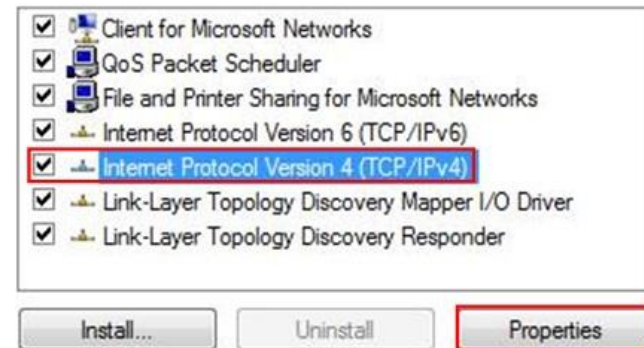
- In **Windows 7 and Windows 8**, click **View Network Status and Tasks** in the **Network and Internet** section and then select **Change adapter settings**.



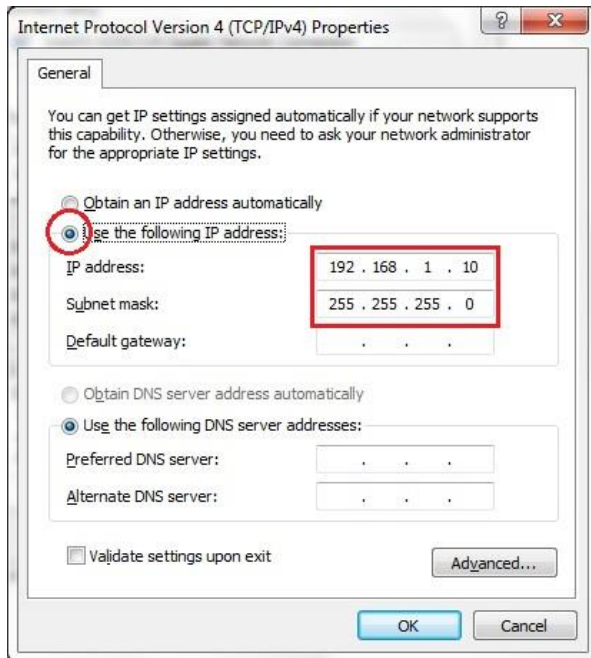
- Right click on **Local Area Connection** and select **Properties**.



- Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.



- Select **Use the following IP address** and enter an IP address that is different from the EAP350 and subnet mask then click **OK**.



**Note:** Ensure that the IP address and subnet mask are on the same subnet as the device.

For example: Device IP address: 192.168.1.1

PC IP address: 192.168.1.2 – 192.168.1.255

PC subnet mask: 255.255.255.0

## 2.3 Computer Settings in Apple Mac OS X

- Go to **System Preferences** (can be opened in the **Applications** folder or selecting it in the Apple Menu).
- Select **Network** in the **Internet & Network** section.



- Highlight **Ethernet**.
- In **Configure IPv4**, select **Manually**.
- Enter an IP address that is different from the EAP350 and subnet mask then press **OK**.

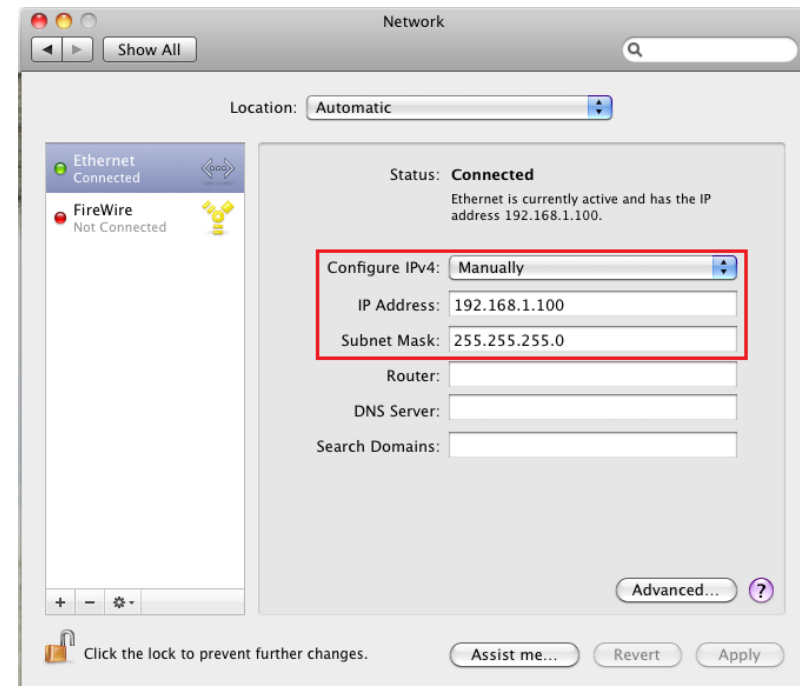
**Note:** Ensure that the IP address and subnet mask are on the same subnet as the device.

For example: Device IP address: 192.168.1.1

PC IP address: 192.168.1.2 – 192.168.1.255

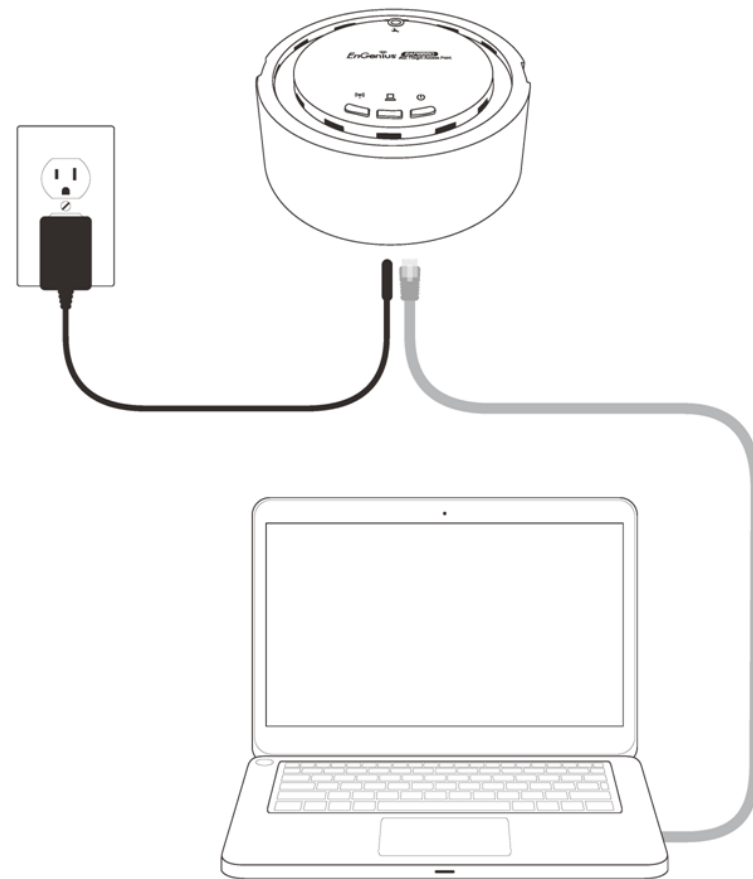
PC subnet mask: 255.255.255.0

- Click **Apply** when done.



## 2.4 Hardware Installation

1. Ensure that the computer in use has an available Ethernet (RJ-45) Port. For more information, verify with your computer's user manual.
2. Connect one end of the Category 5e Ethernet cable into the RJ-45 port of the EAP350 and the other end to the RJ-45 port of the computer. Ensure that the cable is securely connected to both the EAP350 and the computer.
3. Connect the Power Adapter DC connector to the DC-IN port of the EAP350 and the Power Adapter to an available electrical outlet. Once both connections are secure, verify the following:
  - a) Ensure that the **POWER** light is on (it will be blue).
  - b) Ensure that the **WLAN** light is on (they will be blue).
  - c) Ensure that the **LAN** (Computer/EAP350 Connection) light is on (it will be blue).
  - d) Once all lights are on, proceed to set up the EAP350 using the computer.

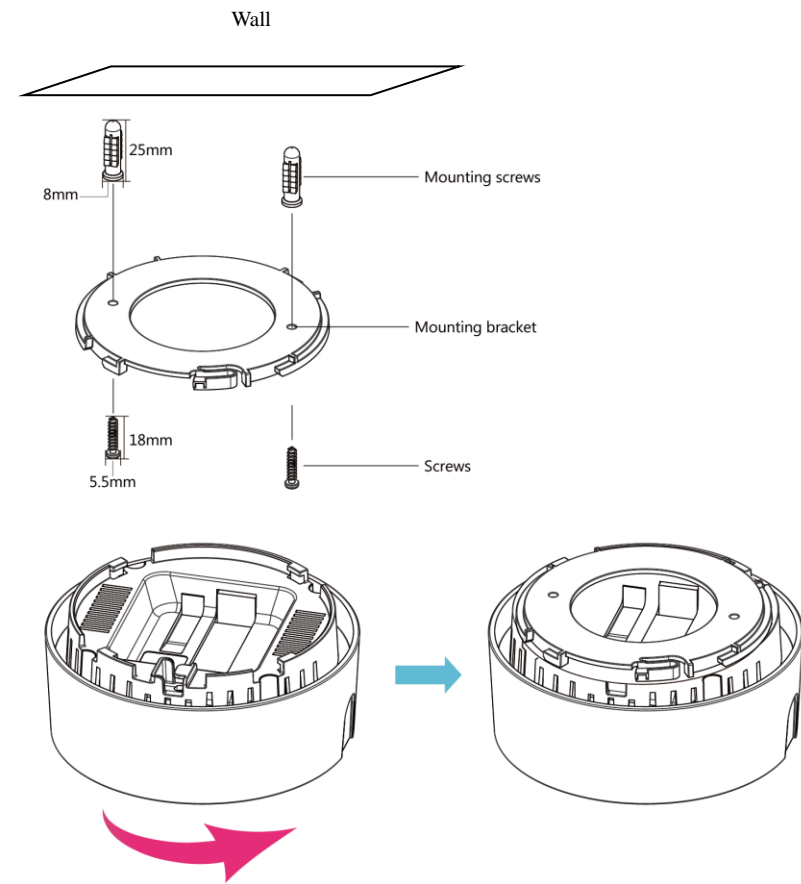


## 2.5 Mounting the EAP350

Using the provided device to be mounted on the ceiling or wall.

To attach the EAP350 to a ceiling or wall using the mounting bracket:

1. Attach the mounting bracket to the wall or ceiling using the provide wall/ceiling mounting hardware kit.
2. Drill the holes to input the mounting screws.
3. Use the included screws to cross the mounting bracket and attach the mounting bracket with the mounting screws.
4. Mount the EAP350 on the mounting bracket by rotating the device clockwise to secure it in place.





## 3 Configuring Your Access Point

This section will show you how to configure the device using the web-based configuration interface.

### 3.1 Default Settings

Please use your Ethernet port or wireless network adapter to connect the EAP350.

#### Default Settings

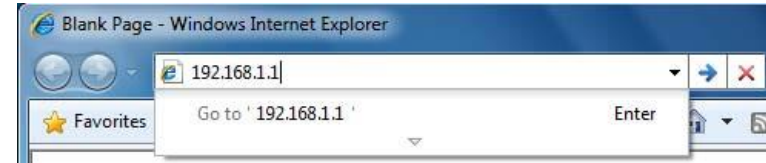
IP Address	192.168.1.1
Username / Password	admin / admin
Operation Mode	Access Point
Wireless SSID	EnGeniusxxxxxx
Wireless Security	None

**Note:** xxxxxx represented in the wireless SSID above is the last 6 characters of your device MAC Address. This can be found on the device body label and is unique for each device.

### 3.2 Web Configuration

- Open a web browser (Internet Explorer/Chrome/Firefox/Safari) and enter the IP Address **http://192.168.1.1**

**Note:** If you have changed the default LAN IP Address of the Access Point, ensure you enter the correct IP Address.



- The default username and password are **admin**. Once you have entered the correct username and password, click the **Login** button to open the web-base configuration page.



- You will see the following webpage if login successfully.

Access Point

Status

- Save/Reload:0
- Main
- Wireless Client List
- System Log

System

- Operation Mode
- IP Settings
- Spanning Tree Settings

Wireless

- Wireless Network
- Wireless MAC Filter
- Wireless Advanced Settings
- WPS

Management

- Administration
- Management VLAN
- SNMP Settings
- Backup/Restore Settings
- Firmware Upgrade
- Time Settings
- Schedule
- CLI Settings
- Log
- Diagnostics
- Device Discovery
- Led Control
- Logout

Main

[Home](#)

[Reset](#)

System Information

Device Name	EAP150
Ethernet Main MAC Address	88-DC-96-10-2D-12
Ethernet Secondary MAC Address	88-DC-96-10-2D-12
Wireless MAC Address (SSID/MAC)	1 88-DC-96-10-2D-12
	2 N/A
	3 N/A
	4 N/A
	5 N/A
	6 N/A
	7 N/A
	8 N/A
Country	N/A
Current Time	Thu Dec 12 07:05:32 UTC 2013
Firmware Version	1.5.1
Management VLAN ID	Untagged

LAN Settings

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
DHCP Client	Disabled
IPv6 IP Address	None
IPv6 Link-Local Address	FE80::8ADC:96FF:FE10:2D12
IPv6 Default Gateway	
IPv6 Primary DNS	
IPv6 Secondary DNS	
RX(Packets)	1,11984 MB (9562 PKts.)
TX(Packets)	889,544 KB (1258 PKts.)

## 4 Building a Wireless Network

The EAP350 has the ability to operate in various modes. This chapter describes the operating modes of the EAP350.

### 4.1 Access Point Mode

In Access Point Mode, EAP350 behaves like a central connection for stations or clients that support IEEE 802.11b/g/n networks. The stations and clients must be configured to use the same SSID (Service Set Identifier) and security password to associate with the EAP350. The EAP350 supports up to eight SSIDs at the same time for secure access.



### 4.2 WDS AP Mode

The EAP350 also supports WDS AP mode. This operating mode allows wireless connections to the EAP350 using WDS technology. In this mode, configure the MAC addresses in both Access Points to enlarge the wireless area by enabling WDS Link settings. WDS supports four AP MAC addresses.



### 4.3 WDS Bridge Mode

In WDS Bridge Mode, the EAP350 can wirelessly connect different LANs by configuring the MAC address and security settings of each EAP350 device. Use this mode when two wired LANs located a small distance apart want to communicate with each other. The best solution is to

use the EAP350 to wirelessly connect two wired LANs, as shown in the following figure. WDS Bridge Mode can establish four WDS links, creating a star-like network.



**Note:** WDS Bridge Mode does not act as an Access Point. Access Points linked by WDS are using the same frequency channel. More Access Points connected together may lower throughput. This configuration can be susceptible to generate endless network loops in your network, so it is recommended to enable the Spanning Tree setting (see 6.3 Spanning Tree Setting, below) to prevent this from happening.

## 4.4 Repeater mode

The Repeater mode is used to regenerate or replicate signals from a wireless router or other access point/station that is unable to reach certain areas in a

building. When this mode is activated in the EAP350, the EAP350 receives the wireless signal from an existing router or AP and relays it to other devices within its range so they can join the network.



## 5 Status

The **Status** section contains the following options: Main, Wireless Client List and System Log.

The following sections describe these options.

### 5.1 Save/Reload

This page lets you save and apply the settings shown under **Unsaved changes list**, or cancel the unsaved changes and revert to the previous settings that were in effect.

The screenshot shows a web interface for the 'Save/Reload' section. At the top right is a 'Home' button. Below it is a section titled 'Unsaved changes list' containing a list of configuration changes for network and wireless settings. At the bottom are two buttons: 'Save & Apply' and 'Revert'.

```
-network.1.ifname
-network.3.ifname
network.lan.ifname=eth0
-network.5.ifname
-network.4.ifname
-network.7.ifname
-network.6.ifname
-network.8.ifname
-network.2.ifname
-wireless.cfg23cb63.WLANWDSPeer
wireless.cfg03237d.wps_configured=1
wireless.cfg03237d.ssid=EnGenius
wireless.cfg03237d.encryption=psk-mixed tkip+aes
wireless.cfg03237d.key=12345678
wireless.cfg03237d.WLANWpaRadiusAccSrvIP=...
wireless.cfg03237d.hidden=0
wireless.cfg03237d.server=...
```

### 5.2 Main

Clicking the **Main** link under the **Status** menu or clicking

**Home** at the top-right of the EAP350 Page shows the status information about the current operating mode.

**System Information:** Show the general system information such as Device Name, MAC Address, Current Time, Firmware Version, and Management VLAN ID (**Note:** VLAN ID is only applicable in Access Point / WDS AP mode).

System Information	
Device Name	EAP150
Ethernet Main MAC Address	88:DC:96:10:2D:12
Ethernet Secondary MAC Address	88:DC:96:10:2D:12
Wireless MAC Address (SSID/MAC)	1 88:DC:96:10:2D:12
	2 N/A
	3 N/A
	4 N/A
	5 N/A
	6 N/A
	7 N/A
	8 N/A
Country	N/A
Current Time	Thu Dec 12 07:05:32 UTC 2013
Firmware Version	1.5.1
Management VLAN ID	Untagged

**LAN Settings:** Show the Local Area Network settings such as the LAN IP Address, Subnet Mask, DNS Address.

LAN Settings	
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
DHCP Client	Disabled
IPv6 IP Address	None
IPv6 Link-Local Address	FE80::8ADC:96FF:FE10:2D12
IPv6 Default Gateway	
IPv6 Primary DNS	
IPv6 Secondary DNS	
RX(Packets)	1.11984 MB (9562 PKts.)
TX(Packets)	889.544 KB (1258 PKts.)

**Current Wireless Settings:** Show the wireless information such as Operating Mode, Frequency, Channel, Distance, RX and TX. Since the EAP350 supports multiple-SSIDs, information about each SSID, the ESSID and security settings, are displayed (**Note:** Profile Settings is only applicable in Access Point / WDS AP mode).

Current Wireless Settings	
Operation Mode	Access Point
Wireless Mode	IEEE 802.11b/g/n Mixed
Channel Bandwidth	20.40 MHz
Frequency/Channel	2.437 GHz (Channel 6)
Profile Settings (SSID/Security/VID/802.1Q)	1 EnGenius102D12/None/1/OFF
	2 N/A
	3 N/A
	4 N/A
	5 N/A
	6 N/A
	7 N/A
	8 N/A
Spanning Tree Protocol	Disabled
Distance	1 Km
RX(Packets)	0 B (0 PKts.)
TX(Packets)	474.337 KB (2008 PKts.)

## 5.3 Wireless Client List

Clicking the **Wireless Client List** link under the **Status** menu displays the list of clients associated to the EAP350, along with the MAC address, TX, RX and signal strength for each client. Clicking **Kick** in the Kick and Ban column removes this client. Clicking **Refresh** updates the client list.

**Note:** Only applicable in Access Point, WDS AP, and Repeater mode.

Client List						
					<a href="#">Home</a>	<a href="#">Reset</a>
SSID:#	MAC Address	TX(Bytes)	RX(Bytes)	RSSI(dBm)	Kick and Ban	
SSID1:#1	00:02:6f:63:69:19	0Kb	1Kb	-28	<a href="#">Kick</a>	
<a href="#">Refresh</a>						

## 5.4 Connection Status

Click on the **Connection Status** link under the **Status** menu. This page displays the current status of the Network, including Network Type, SSID, BSSID, Connection Status, Wireless Mode, Current Channel, Security, Data Rate, Noise Level, and Signal Strength.

**Note:** Only applicable in Repeater mode.

## Connection Status

Home Reset

Network Type	Repeater
SSID	EnGenius
BSSID	00:0F:C9:08:87:CB
Connection Status	Associated
Wireless Mode	IEEE 802.11b/g/n Mixed
Current Channel	2.437 GHz(Channel 6 )
Security	WPA2-PSK AES
Tx Data Rates(Mbps)	52 Mbps
Current noise level	-95 dBm
Signal strength	-57 dBm

Refresh

## 5.5 WDS Link List

Click on the **WDS Link List** link under the **Status** menu. This page displays the current status of the WDS link, including WDS Link ID, MAC Address, Link Status and RSSI.

**Note:** Only applicable in WDS AP and WDS Bridge mode.

## WDS Link Status

Home Reset

WDS Link ID	MAC Address	Link Status	RSSI (dBm)
1	00:0f:c9:08:87:cb	UP	-25

Refresh

## 5.6 System Log

The EAP350 automatically logs (records) events of possible interest in its internal memory. To view the logged information, click the **System Log** link under the **Status** menu. If there is not enough internal memory to log all events, older events are deleted from the log. When powered down or rebooted, the log will be cleared.

## System Log

Home Reset

```
Show log type All
Dec 12 07:30:01 EAP150 user.notice root: starting ntpd
Dec 12 07:30:01 EAP150 cron.info crond[1791]: crond: USER root pid 1395 cmd . /etc/hotplug.d/iface/20-
Dec 12 07:25:01 EAP150 user.notice root: starting ntpd
Dec 12 07:25:01 EAP150 cron.info crond[1791]: crond: USER root pid 770 cmd . /etc/hotplug.d/iface/20-n
Dec 12 07:24:59 EAP150 user.info kernel: br-lan: port 3(ath1) entering forwarding state
Dec 12 07:24:59 EAP150 user.info kernel: br-lan: port 2(ath0) entering forwarding state
Dec 12 07:24:59 EAP150 daemon.warn dnsmasq[647]: ignoring nameserver 127.0.0.1 - local interface
Dec 12 07:24:59 EAP150 daemon.info dnsmasq[647]: using local addresses only for domain lan
Dec 12 07:24:59 EAP150 daemon.info dnsmasq[647]: reading /tmp/resolv.conf
Dec 12 07:24:54 EAP150 user.notice dhcp6c: stopping dhcp6c
Dec 12 07:24:53 EAP150 daemon.warn dnsmasq[647]: failed to access /tmp/resolv.conf: No such file or di
Dec 12 07:24:53 EAP150 daemon.warn dnsmasq[1678]: failed to access /tmp/resolv.conf: No such file or d
Dec 12 07:24:53 EAP150 daemon.info dnsmasq[647]: using local addresses only for domain lan
Dec 12 07:24:53 EAP150 daemon.info dnsmasq[647]: started, version 2.52 cachesize 150
Dec 12 07:24:53 EAP150 daemon.info dnsmasq[647]: read /etc/hosts - 1 addresses
Dec 12 07:24:53 EAP150 daemon.info dnsmasq[647]: compile time options: IPv6 GNU-getopt no-DBus no-i18N
Dec 12 07:24:53 EAP150 daemon.info dnsmasq[1678]: exiting on receipt of SIGTERM
Dec 12 07:24:52 EAP150 user.info kernel: device ath1 entered promiscuous mode
Dec 12 07:24:50 EAP150 user.warn kernel: wlan_vap_create : exit. devhandle=0x82a942c0, opmode=IEEE8021
Dec 12 07:24:50 EAP150 user.warn kernel: wlan_vap_create : enter. devhandle=0x82a942c0, opmode=IEEE802
Dec 12 07:24:50 EAP150 user.warn kernel: DES SSID SET=AP SSID
Dec 12 07:24:50 EAP150 user.warn kernel:
```

Save Refresh Clear

**Save:** Save the log as the specific file

**Refresh:** Update the log to the latest status

**Clear:** Clean up the all logs

## 6 System

### 6.1 Operation Mode

The EAP350 supports four operating modes: Access Point, WDS Access Point, WDS Bridge and Repeater.

System Properties		Home	Reset
Device Name	EAP350 ( 1 to 32 characters ) <span>Green</span>		
Country/Region	United States		
Operation Mode	<input checked="" type="radio"/> Access Point <input type="radio"/> WDS <input type="radio"/> Repeater		
Save & Apply		Cancel	

**Device Name:** Enter a name for the device. The name you type appears in SNMP management. This name is not the SSID and is not broadcast to other devices..

**Operation Mode:** Use the radio button to select an operating mode.

**Accept / Cancel:** Click Save & Apply to confirm the changes or Cancel to cancel and return previous settings.

### 6.2 IP Settings

This page allows you to modify the device's IP settings.

IP Settings		Home	Reset
System Information			
IP Network Setting	<input type="radio"/> Obtain an IP address automatically (DHCP) <input checked="" type="radio"/> Specify an IP address		
IP Address	192	168	1 . 1
IP Subnet Mask	255	255	255 . 0
Default Gateway	192	168	1 . 1
Primary DNS	0	0	0 . 0
Secondary DNS	0	0	0 . 0
Use Link-Local Address	<input checked="" type="checkbox"/>		
IPv6 IP Address			
IPv6 Subnet Prefix Length			
IPv6 Default Gateway			
IPv6 Primary DNS			
IPv6 Secondary DNS			
Accept		Cancel	

**IP Network Setting:** Select whether the device IP address will use the static IP address specified in the IP Address field or be obtained automatically when the device connects to a DHCP server.

**IP Address:** The IP Address of this device

**IP Subnet Mask:** The IP Subnet Mask of this device.

**Default Gateway:** The Default Gateway of this device. Leave it blank if you are unsure of this setting.

**Primary/Secondary DNS:** The primary / secondary DNS address for this device.

**Use Link-Local Address:** Check this if you want to use Link-Local Address.

**IPv6 IP Address:** The IPv6 IP Address of this device.

**IPv6 Subnet:** The IPv6 Subnet Prefix Length of this device.



**IPv6 Default Gateway:** The IPv6 Default Gateway of this device. Leave it blank if you are unsure of this setting.

**IPv6 Primary / Secondary DNS:** The primary / secondary DNS address for this device.

### 6.3 Spanning Tree Setting

This page allows you to modify the Spanning Tree settings. Enabling Spanning Tree protocol will prevent network loops in your LAN network.

**Spanning Tree Settings** Home Reset

Spanning Tree Status	<input checked="" type="radio"/> On <input type="radio"/> Off
Bridge Hello Time	<input type="text" value="2"/> seconds (1-10)
Bridge Max Age	<input type="text" value="20"/> seconds (6-40)
Bridge Forward Delay	<input type="text" value="4"/> seconds (4-30)
Priority	<input type="text" value="32768"/> (0-65535)

Accept Cancel

**Spanning Tree Status:** Enable or disable the Spanning Tree function.

**Bridge Hello Time:** Specify Bridge Hello Time, in seconds. This value determines how often the device sends

**Bridge Max Age:** Specify Bridge Max Age, in seconds. If another bridge in the spanning tree does not send a hello packet for a long period of time, it is assumed to be dead.

**Bridge Forward Delay:** Specify Bridge Forward Delay, in seconds. Forwarding delay time is the time spent in each of the

Listening and Learning states before the Forwarding state is entered. This delay is provided so that when a new bridge comes onto a busy network, it looks at some traffic before participating.

**Priority:** Specify the Priority number. Smaller number has greater priority.

**Accept / Cancel:** Click **Accept** to confirm the changes or **Cancel** to cancel and return previous settings.

# 7 Wireless

## 7.1 Wireless Network

This page displays the current status of the Wireless settings.

### Access Point / WDS AP mode:

**Wireless Network** Home Reset

Wireless Mode	802.11 B/G/N Mixed
Channel HT Mode	20/40MHz
Extension Channel	Lower Channel
Channel / Frequency	Ch5-2.432GHz <input checked="" type="checkbox"/> Auto
AP Detection	<input type="button" value="Scan"/>

**Current Profiles**

SSID	Security	Isolation	VID	Enable	Edit
EnGenius102D12	None	<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/>
EnGenius102D12_2	None	<input type="checkbox"/>	2	<input type="checkbox"/>	<input type="button" value="Edit"/>
EnGenius102D12_3	None	<input type="checkbox"/>	3	<input type="checkbox"/>	<input type="button" value="Edit"/>
EnGenius102D12_4	None	<input type="checkbox"/>	4	<input type="checkbox"/>	<input type="button" value="Edit"/>
EnGenius102D12_5	None	<input type="checkbox"/>	5	<input type="checkbox"/>	<input type="button" value="Edit"/>
EnGenius102D12_6	None	<input type="checkbox"/>	6	<input type="checkbox"/>	<input type="button" value="Edit"/>
EnGenius102D12_7	None	<input type="checkbox"/>	7	<input type="checkbox"/>	<input type="button" value="Edit"/>
EnGenius102D12_8	None	<input type="checkbox"/>	8	<input type="checkbox"/>	<input type="button" value="Edit"/>

**Wireless Mode:** Wireless mode supports 802.11b/g/n mixed mode.

**Channel HT Mode:** The default channel bandwidth is 20/40MHz. The larger the channel, the better the transmission quality and speed.

**Extension Channel:** Select upper or lower channel. Your

selection may affect the Auto channel function.

**Channel / Frequency:** Select the channel and frequency appropriate.

**Auto:** Check this option to enable auto-channel selection.

**AP Detection:** AP Detection can select the best channel to use by scanning nearby areas for Access Points.

**Current Profile:** Configure up to eight different SSIDs. If many client devices will be accessing the network, you can arrange the devices into SSID groups. Click **Edit** to configure the profile and check whether you want to enable extra SSID.

**Accept / Cancel:** Click **Accept** to confirm the changes or **Cancel** to cancel and return previous settings.

### SSID Profile

#### SSID Profile

**Wireless Setting**

SSID	EnGenius102D12	(1 to 32 characters)
VLAN ID	1	(1~4094)
Suppressed SSID	<input type="checkbox"/>	
Station Separation	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable

**Wireless Security**

Security Mode	Disabled
---------------	----------

**SSID:** Specify the SSID for the current profile.

**VLAN ID:** Specify the VLAN tag for the current profile.

**Suppressed SSID:** Check this option to hide the SSID from

clients. If checked, the SSID will not appear in the site survey.

**Station Separation:** Click the appropriate radio button to allow or prevent communication between client devices.

**Wireless Security:** See the Wireless Security section.

**Save / Cancel:** Click **Save** to accept the changes or **Cancel** to cancel and return previous settings.

### Repeater mode:

**Wireless Network** Home Reset

Wireless Mode	802.11 B/G/N Mixed
SSID	Specify the static SSID : AP SSID ( 1 to 32 characters ) Or press the button to search for any available WLAN Service. <span>Site Survey</span>
Repeater SSID	AP SSID ( 1 to 32 characters )
Preferred BSSID	<input type="checkbox"/> . . . . .
Wireless Security	
Changing the wireless security settings may cause this wireless client to associate with a different one. This may temporarily disrupt your configuration session.	
Security Mode	Disabled
<span>Accept</span> <span>Cancel</span>	

**Wireless Mode:** Wireless mode supports 802.11b/g/n mixed mode.

**SSID:** The SSID is a unique named shared amongst all the points of the wireless network. The SSID must be identical on all points of the wireless network and cannot exceed 32 characters. You may specify an SSID or select one from the **Site Survey**.

**Site Survey:** Click on **Site Survey** to search the existing Access Points.

**Preferred SSID:** Specify the SSID for the repeater. It can be different from Access Point's SSID.

**Preferred BSSID:** Specify the BSSID (Access Point's MAC Address).

**Wireless Security:** The encryption is using. It must the same as Access Point's encryption.

**Accept / Cancel:** Click **Accept** to confirm the changes or **Cancel** to cancel and return previous settings.

## 7.2 Wireless Security

The Wireless Security section lets you configure the EAP350's security modes: WEP, WPA-PSK, WPA2-PSK, WPA-PSK Mixed, WPA, WPA2, and WPA Mixed. We strongly recommend using WPA2-PSK.

**Note:** Only in Access Point and WDS AP mode.

### WEP Encryption:

Wireless Security	
Security Mode	WEP
Auth Type	Open System
Input Type	Hex
Key Length	40/64-bit (10 hex digits or 5 ASCII char)
Default Key	1
Key1	1234567890
Key2	
Key3	
Key4	

**Auth Type:** Select **Open System** or **Shared Key**.

**Input type:** **ASCII:** regular text (recommended), **HEX:** for advanced users

**Key Length:** Select the desired option, and ensure the wireless clients use the same setting.

Choices are 64, 128, 152-bit password lengths.

**Default Key:** Select the key you wish to be the default. Transmitted data is ALWAYS encrypted using the Default Key; the other Keys are for decryption only.

You must enter a **Key Value** for the **Default Key**.

**Encryption Key #:** Enter the key value or values you wish to use. Only the Key selected as Default is required. The others are optional.

### WPA-PSK (WPA Pre-Shared Key) Encryption:

Wireless Security	
Security Mode	WPA-PSK Mixed ▾
Encryption	Both(TKIP+AES) ▾
Passphrase	12345678 (8 to 63 characters) or (64 Hexadecimal characters)
Group Key Update Interval	3600 seconds(30~3600, 0: disabled)

**Encryption:** Select the WPA encryption you would like.

Please ensure that your wireless clients use the same settings.

**Passphrase:** Wireless clients must use the same key to associate the device.

If using passphrase format, the Key must be from 8 to 63

characters in length.

**Group Key Update Interval:** Specify how often, in seconds, the group key changes.

### WPA Encryption: Only in Access Point / WDS AP mode

Wireless Security	
Security Mode	WPA Mixed ▾
Encryption	Both(TKIP+AES) ▾
Radius Server	
Radius Port	1812
Radius Secret	
Group Key Update Interval	3600 seconds(30~3600, 0: disabled)
Radius Accounting	Enable ▾
Radius Accounting Server	
Radius Accounting Port	1813
Radius Accounting Secret	
Interim Accounting Interval	600 seconds(60~600)

**Encryption:** Select the WPA encryption to type you would like to use. Please ensure that your wireless client use the same settings.

**Radius Server:** Enter the IP address of the Radius server.

**Radius Port:** Enter the port number used for connections to the Radius server.

**Radius Secret:** Enter the secret required to connect to the Radius server.

**Group Key Update Interval:** Specify how often, in seconds, the group key changes.

**Radius Accounting:** Enable or disable accounting feature.

**Radius Accounting Server:** Enter the IP address of the Radius accounting server.

**Radius Accounting Port:** Enter the port number used for connections to the Radius accounting server.

**Radius Accounting Secret:** Enter the secret required to connect to the Radius accounting server.

**Interim Accounting Interval:** Specify how often, in seconds, the accounting data sends.

**Note:** 802.11n does not allow WEP/WPA-PSK TKIP/WPA2-PSK TKIP security mode. The connection mode will automatically change from 802.11n to 802.11g.

## 7.3 Site Survey

Use this feature to scan for nearby access points.

**Note:** Only applicable in Repeater mode.

1. Click **Site Survey**.

**Wireless Network** Home Reset

Wireless Mode: 802.11 B/G/N Mixed

Specify the static SSID :  
SSID: AP SSID ( 1 to 32 characters )  
Or press the button to search for any available WLAN Service.  
Site Survey

Repeater SSID: AP SSID ( 1 to 32 characters )

Preferred BSSID:  : : : : :

Wireless Security

Changing the wireless security settings may cause this wireless client to associate with a different one. This may temporarily disrupt your configuration session.

Security Mode: Disabled

Accept Cancel

2. Scanning for the nearby access points

## Scanning

Please wait...

3. The EAP350 will list the available access points after site survey.

**Site Survey**

2GHz Site Survey i:Infrastructure Ad\_hoc

BSSID	SSID	Channel	Signal Level	Type	Security	Mode
00:02:6F:BF:32:2C	SENAOWL	1	-90 dBm	11bg	WEP	i
00:02:6F:D7:AC:6C	EnGeniusD7AC6C-2.4G	1	-85 dBm	11gn	none	i
00:02:6F:CC:FD:A6	SENAOWL	1	-87 dBm	11bg	WEP	i
02:02:6F:DB:9F:C7	SENAOWL	1	-86 dBm	11gn	WPA2-PSK	i
02:02:6F:DB:9F:E5	SENAOWL	1	-85 dBm	11gn	WPA2-PSK	i
00:0F:C9:08:87:CB	EnGenius	6	-52 dBm	11gn	WPA2-PSK	i
BE:CF:CC:0F:82:2A	HTCc	2	-79 dBm	11gn	WPA2-PSK	i

Refresh

4. Select an Access Point and click that Access Point's BSSID.

#### Site Survey

2GHz Site Survey i:Infrastructure Ad\_hoc

BSSID	SSID	Channel	Signal Level	Type	Security	Mode
00:02:6F:BF:32:2C	SENAOWL	1	-90 dBm	11b/g	WEP	i
00:02:6F:D7:AC:6C	EnGeniusD7AC6C-2.4G	1	-85 dBm	11g/n	none	i
00:02:6F:CC:FD:A6	SENAOWL	1	-87 dBm	11b/g	WEP	i
02:02:6F:DB:9F:C7	SENAOWL	1	-86 dBm	11g/n	WPA2-PSK	i
02:02:6F:DB:9F:E5	SENAOWL	1	-85 dBm	11g/n	WPA2-PSK	i
00:0F:C9:08:87:CB	EnGenius	6	-52 dBm	11g/n	WPA2-PSK	i
BE:CF:CC:0F:82:2A	HTCc	2	-79 dBm	11g/n	WPA2-PSK	i

Refresh

**BSSID:** MAC address of the Access Point

**SSID:** The SSID which the Access Point broadcasting.

**Channel:** The channel which the Access Point uses.

**Signal Level (dBm):** Signal strength from the Access Point to your station.

**Type:** The band that the Access Point is using.

**Security:** Encryption method that the Access Point is using to secure data over the WLAN.

**Refresh:** Click **Refresh** to rescan nearby Access Point.

5. Enter the correct security setting and then click **Accept**.

#### Wireless Network

Home Reset

Wireless Mode: 802.11 B/G/N Mixed

Specify the static SSID :  
 EnGenius ( 1 to 32 characters )  
 Or press the button to search for any available WLAN Service.  
 Site Survey

Repeater SSID: AP SSID ( 1 to 32 characters )

Preferred BSSID:  00 : 0F : C9 : 08 : 87 : CB

Wireless Security

Changing the wireless security settings may cause this wireless client to associate with a different one. This may temporarily disrupt your configuration session.

Security Mode: WPA2-PSK

Encryption: AES

Passphrase: 12345678 (8 to 63 characters) or (64 Hexadecimal characters)

Accept Cancel

## 7.4 Wireless MAC Filter

Wireless MAC Filtering is used to allow or deny network access to wireless clients (computers, tablet PCs, NAS, smartphones, etc.) according to their MAC addresses. You can manually add a MAC address to restrict the permission to access EAP350. The default setting is **Disabled**.

**Note:** Only in Access Point, WDS AP and Repeater mode.

#### Wireless MAC Filter

Home Reset

ACL Mode: Disabled

00 : 02 : 6f : 00 : 35 : 01 Add

#	MAC Address	Delete
1	00:02:6F:32:54:AC	Delete

Accept

**ACL Mode:** Determines whether network access is granted or denied to clients whose MAC addresses appear in the MAC Address table on this page. Choices are **Disabled**, **Deny MAC in the List** or **Allow MAC in the List**.

**MAC Address:** Enter the MAC address of the wireless client.

**Add:** Click **Add** to add the MAC address to the **MAC Address** table.

**Delete:** Click **Delete** to delete the MAC address from the **MAC Address** table.

**Apply:** Click **Accept** to apply the changes.

## 7.5 Wireless Advanced

This page allows you to configure wireless advanced settings. It is recommended the default settings are used unless the user has experience with these functions.

Wireless Advanced Settings		Home	Reset
Data Rate	Auto		
Transmit Power	Auto		
RTS/CTS Threshold (1 - 2346)	2346 bytes		
Distance (1-30km)	1 km		
Aggregation:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable 32 Frames 50000 Bytes(Max)		
Wireless Traffic Shaping			
Enable Traffic Shaping	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
Incoming Traffic Limit	1000 kbit/s (512-9999999)		
Outgoing Traffic Limit	180000 kbit/s (512-9999999)		
Total Percentage	10 %		
SSID #1 : EnGenius102D12	10 %		
SSID #2 : (Off)	10 %		
SSID #3 : (Off)	10 %		
SSID #4 : (Off)	10 %		
SSID #5 : (Off)	10 %		
SSID #6 : (Off)	10 %		
SSID #7 : (Off)	10 %		
SSID #8 : (Off)	10 %		
Client limit			
Frequency	Enable	Max Client	
2.4G	<input checked="" type="checkbox"/>	127	
<input type="button" value="Accept"/> <input type="button" value="Cancel"/>			

**Data Rate:** Select a data rate from the drop-down list. The data rate affects throughput. If you select a low data rate value, for example, the throughput is reduced but the transmission distance increases.

**Transmit Power:** Set the power output of the wireless signal.

**RTS/CTS Threshold:** Specify the threshold package size for RTS/CTS. A small number causes RTS/CTS packets to be sent more often and consumes more bandwidth.

**Distance:** Specify the distance between Access Points and clients. Longer distances may drop high-speed connections.

**Aggregation:** Merges data packets into one packet. This option reduces the number of packets, but increases packet sizes.

**Wireless Traffic Shaping:** Check this option to enable wireless traffic shaping. Traffic shaping regulates the flow of packets leaving an interface to deliver improved Quality of Service.

**Incoming Traffic Limit:** Specify the wireless transmission speed used for downloading.

**Outgoing Traffic Limit:** Specify the wireless transmission speed used for uploading.

**Total Percentage:** It shows how much percentage has been used.

**SSID #1~#8:** Specify the wireless transmission speed used for each SSID.

**Client Limit:** Check **Enable** and enter a number to limit the maximum client connection (The maximum is 127). **Note:** Only applicable in Access Point, WDS AP and Repeater mode.

**Accept / Cancel:** Click **Accept** to confirm the changes or **Cancel** to cancel and return previous settings.



## 7.6 WPS (Wi-Fi Protected Setup)

WPS feature is following the Wi-Fi Alliance WPS standard and it eases the set up of security-enabled Wi-Fi networks in the home and small office environment.

It reduces the user steps required to configure a network and supports two methods that are familiar to most consumers to configure a network and enable security.

**Note:** Only in Access Point and WDS AP mode.

WPS Setting		Home	Reset
WPS			
WPS	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
WPS current status	Configured	Release Configuration	
Self Pin Code	44690427		
SSID	EnGenius102D12		
Authentication Mode	WPA2-PSK AES		
Passphrase Key	12345678		
WPS Via Push Button	Start to Process		
WPS Via Pin	<input type="text"/>	Start to Process	
Accept Cancel			

**WPS:** Select Enable or Disable the WPS feature.

**WPS Current Status:** Shows whether the WPS function is **Configured** or **unConfigured**.

When it is **Configured**, the WPS has been used to authorize connection between the device and wireless clients.

**Self Pin Code:** The PIN code of this device.

**SSID:** The SSID (**wireless** network name) used when connecting using WPS.

**Authentication Mode:** Shows the encryption method used by the WPS process.

**Passphrase Key:** This is the passphrase key that is randomly generated during the WPS process. It is required if wireless clients that do not support WPS attempts to connect to the wireless network.

**WPS Via Push Button:** Click this button to initialize WPS feature using the push button method.

**WPS Via PIN:** Enter the PIN code of the wireless device and click this button to initialize WPS feature using the PIN method

## 7.7 WDS Link Settings

Using WDS (Wireless Distribution System) will allow a network administrator or installer to connect to Access Points wirelessly. Doing so will extend the wired infrastructure to locations where cabling is not possible or inefficient to implement.

**Note:** Compatibility between different brands and models of access points is not guaranteed. It is recommended that the WDS network be created using the same models for maximum compatibility.

**Also note:** All Access Points in the WDS network needs to use the same Channel and Security settings.

To create a WDS network, please enter the MAC addresses of the Access Points that you want included in

the WDS. There can be a maximum of four access points in WDS AP mode and eight access points in WDS Bridge mode.

**Note:** Only applicable in WDS AP and WDS Bridge mode.

**WDS Link Settings** Home Reset

---

Security:  ▼

WEP Key:  40/64-bit(10 hex digits) ▼

AES Passphrase:  (8-63 ASCII characters or 64 hexadecimal digits)

---

ID	MAC Address	Mode
1	<input type="text" value="00"/> : <input type="text" value="0F"/> : <input type="text" value="C9"/> : <input type="text" value="08"/> : <input type="text" value="87"/> : <input type="text" value="CB"/>	<input type="text" value="Enable"/> ▼
2	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	<input type="text" value="Disable"/> ▼
3	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	<input type="text" value="Disable"/> ▼
4	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	<input type="text" value="Disable"/> ▼
5	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	<input type="text" value="Disable"/> ▼
6	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	<input type="text" value="Disable"/> ▼
7	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	<input type="text" value="Disable"/> ▼
8	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	<input type="text" value="Disable"/> ▼

**Security:** Select **None** or **WEP** or **AES** from drop-down list.

**WEP Key:** Enter the key values you wish to use if selecting WEP.

**Note:** Only applicable in WDS Bridge mode.

**AES Passphrase:** Enter the key values you wish to use if selecting AES.

**MAC Address:** Enter the Access Point's MAC address to which you want to extend the wireless area.

**Mode:** Select **Disable** or **Enable** from the drop-down list.

**Accept / Cancel:** Click **Accept** to confirm the changes or **Cancel** to cancel and return previous settings.

**Note:** Other AP(s) must use the same security and key to establish WDS link.

WDS AP mode supports four WDS links and WDS Bridge mode supports eight WDS links.

## 8 Management

### 8.1 Administration

This page allows you to change the EAP350 username and password. By default, the user name is **admin** and the password is: **admin**. Password can contain 0 to 12 alphanumeric characters and is case sensitive.

Login Setting		Home	Reset
New Name	admin		
New Password			
Confirm Password			
Save/Apply		Cancel	Logout

**New Name:** Enter a new username for logging in to the Web Configuration.

**New Password:** Enter a new password for logging in to the Web Configuration.

**Confirm Password:** Re-enter the new password for confirmation.

**Save/Apply / Cancel:** Click **Save/Apply** to apply the changes or **Cancel** to return previous settings.

**Logout:** Click **Logout** to logout

### 8.2 Management VLAN

This page allows you to assign a VLAN tag to the packets. A VLAN is a group of computers on a network whose software has been configured so that they behave as if they were on a separate Local Area Network (LAN). Computers on VLAN do not have to be physically located next to one another on the LAN.

Management VLAN Settings		Home	Reset
<b>Caution:</b> If you reconfigure the Management VLAN ID, you may lose connectivity to the access point. Verify that the switch and DHCP server can support the reconfigured VLAN ID, and then re-connect to the new IP address.			
Management VLAN ID	<input type="radio"/> No VLAN tag <input type="radio"/> Specified VLAN ID <input type="text"/>		
(must be in the range 1 ~ 4094.)			
Accept		Cancel	

**Management VLAN ID:** If your network includes VLANs and if tagged packets need to pass through the Access Point, enter the VLAN ID. Otherwise, click **No VLAN tag**.

**Accept / Cancel:** Click **Accept** to confirm the changes or **Cancel** to cancel and return previous settings.

**Note:**

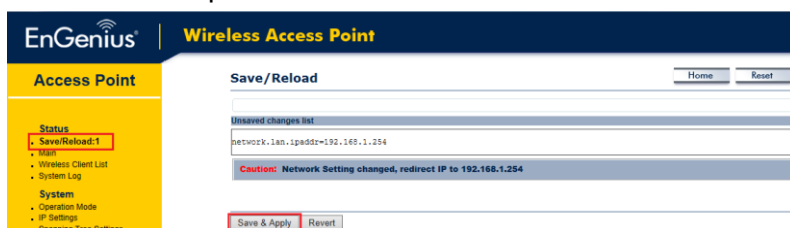
1. If you reconfigure the Management VLAN ID, you may lose your connection to the EAP350. Verify that the DHCP server supports the reconfigured VLAN ID and then reconnect to the EAP350 using the new IP address.
2. Clicking **Accept** does not apply the changes. To apply them, use Status > Save/Load (see section 5.1).

## VLAN Setup

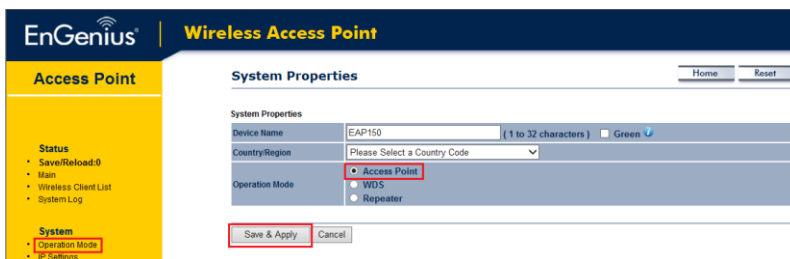
Below is a sample network diagram for VLAN.



Please note that in order for the settings to save on this unit you need to click **Save & Apply** under the **Save/Reload** option under **Status**.



Step 1. Setup Operation mode to **Access Point**.



Step 2. Setup the wireless settings. Click **Edit** on the SSID

you want to configure. Note The **Isolation** checkbox tells the unit that you want the SSID to be mapped to a VID specified in the **VID** field. If the Isolation box is not checked the SSID will not be tied to the VLAN that is not tagged off the trunk port. The **Enable** checkbox is checked if you want the AP to have an SSID accessible via the wireless side of the AP.



Step 3. Configure the AP with the SSID you want, and the type of encryption you desire.

## SSID Profile

Wireless Setting

SSID	Private (1 to 32 characters)
VLAN ID	20 (1~4094)
Suppressed SSID	<input type="checkbox"/>
Station Separation	<input type="radio"/> Enable <input type="radio"/> Disable

Wireless Security

Security Mode	WPA2-PSK
Encryption	AES
Passphrase	12345678 (8 to 63 characters) or (64 Hexadecimal characters)
Group Key Update Interval	3600 seconds(30~3600, 0: disabled)

Step 4. Click **Accept** to ensure your settings apply to the **Save/Reload** list

EnGenius Wireless Access Point

Access Point

Wireless Network

Wireless Mode	802.11 B/G/N Mixed
Channel HT Mode	20/40MHz
Extension Channel	Lower Channel
Channel / Frequency	Ch62 432GHz Auto
AP Detection	Scan

SSID	Security	Isolation	VID	Enable	Edit
Public	None	<input checked="" type="checkbox"/>	10	<input checked="" type="checkbox"/>	Edit
Private	WPA2-PSK AES	<input checked="" type="checkbox"/>	20	<input checked="" type="checkbox"/>	Edit
EnGenius115578_3	None	<input type="checkbox"/>	3	<input type="checkbox"/>	Edit
EnGenius115578_4	None	<input type="checkbox"/>	4	<input type="checkbox"/>	Edit
EnGenius115578_5	None	<input type="checkbox"/>	5	<input type="checkbox"/>	Edit
EnGenius115578_6	None	<input type="checkbox"/>	6	<input type="checkbox"/>	Edit
EnGenius115578_7	None	<input type="checkbox"/>	7	<input type="checkbox"/>	Edit
EnGenius115578_8	None	<input type="checkbox"/>	8	<input type="checkbox"/>	Edit

Step 5. Please set your unit to be in the subnet that you

want to manage the device in, pointing to the proper default gateway and outside of your DHCP scope.

EnGenius Wireless Access Point

Access Point

IP Settings

System Information

IP Network Setting

Obtain an IP address automatically (DHCP)  Specify an IP address

IP Address	192 168 1 1
IP Subnet Mask	255 255 255 0
Default Gateway	192 168 1 254
Primary DNS	0 0 0 0
Secondary DNS	0 0 0 0
Use Link Local Address	<input checked="" type="checkbox"/>
IPv6 IP Address	
IPv6 Subnet Prefix Length	
IPv6 Default Gateway	
IPv6 Primary DNS	
IPv6 Secondary DNS	

Optional:

If using a tagged VLAN to manage the unit then please place unit in the proper subnet and set the management VLAN tag to the tagged LAN you want to manage the device from.

**Caution:** If you reconfigure the Management VLAN ID, and then re-connect to the new IP address.

Management VLAN ID

No VLAN tag

Specified VLAN ID: 100 (must be in the range 1 - 4094.)

## 8.3 SNMP

This page allows you to assign the Contact Details, Location, Community Name, and Trap Settings for Simple Network Management Protocol (SNMP). This is a networking management protocol used to monitor

network-attached devices. SNMP allows messages (called protocol data units) to be sent to various parts of the network. Upon receiving these messages, SNMP compatible devices (called agents) return the data stored in their Management Information Bases.

**SNMP Enable/Disable:** Enable or Disable SNMP feature.

**Contact:** Specify the contact details of the device

**Location:** Specify the location of the device.

**Community Name (Read Only):** Specify the password for the SNMP community for read only access.

**Community Name (Read/Write):** Specify the password for the SNMP community with read/write access.

**Trap Destination Address:** Specify the IP address of the computer that will receive the SNMP traps.

**Trap Destination Community Name:** Specify the password for the SNMP trap community.

**SNMPv3 Enable/Disable:** Enable or Disable SNMPv3 feature.

**User Name:** Specify the username for SNMPv3.

**Auth Protocol:** Select the authentication protocol type: **MD5** or **SHA**.

**Auth Key:** Specify the authentication key for authentication.

**Priv Protocol:** Select the privacy protocol type: **DES**.

**Priv Key:** Specify the privacy key for privacy.

**Engine ID:** Specify the engine ID for SNMPv3.

**Save/Apply / Cancel:** Click **Save/Apply** to apply the changes or **Cancel** to return previous settings.

## 8.4 Backup/Restore

This page allows you to save the current device configurations. When you save the configurations, you also can reload the saved configurations into the device through the **Restore Saved Settings from A File** section. If extreme problems occur, or if you have set up the EAP350 incorrectly, you can use the **Factory Default** button in the **Revert to Factory Default Settings** section to restore all the configurations of the EAP350 to the original default settings.

**Backup/Restore Settings** Home Reset

---

Save A Copy of Current Settings Backup

---

Restore Saved Settings from A File Browse... Restore

---

Revert to Factory Default Settings Factory Default

---

**Save A Copy of Current Settings:** Click **Backup** to save the current configured settings

**Restore Saved Settings from A File:** To restore settings that have been previously backed up, click **Browse**, select the file, and click **Restore**.

**Revert to Factory Default Settings:** Click **Factory Default** button to restore the EAP350 to its factory default settings.

## 8.5 Firmware Upgrade

This page allows you to upgrade the firmware of EAP350.

**Firmware Upgrade** Home Reset

---

Current firmware version: 1.5.1

Locate and select the upgrade file from your hard disk:

Browse...

---

Upload

**To perform the Firmware Upgrade:**

1. Click the **Browse** button and navigate the OS File System to the location of the upgrade file.

2. Select the upgrade file. The name of the file will appear in the *Upgrade File* field.
3. Click the **Upload** button to commence the firmware upgrade.

**Note:** The device is unavailable during the upgrade process and must restart when the upgrade is completed. Any connections to or through the device will be lost.

## 8.6 Time Setting

This page allows you to set the internal clock of the EAP350.

**Time Settings** Home Reset

---

**Time**

**Manually Set Date and Time**

2013 / 02 / 22 12 : 07

**Automatically Get Date and Time**

Time Zone: UTC+00:00 Gambia, Liberia, Morocco

User defined NTP Server: 209.81.9.7

**Enable Daylight Saving**

Start Time: January 1st Sun 12 am

End Time: January 1st Mon 12 am

---

Save/Apply Cancel

**Manually Set Date and Time:** Manually specify the date and time.

**Automatically Get Date and Time:** Select a time zone from the drop-down list and check whether you want to enter the IP

address of an NTP server or use the default NTP server to get have the internal clock set automatically.

**Enable Daylight Saving:** Check whether daylight savings applies to your area.

**Save/Apply / Cancel:** Click **Save/Apply** to apply the changes or **Cancel** to return previous settings.

## 8.7 Schedule

Use the Schedule function to control the wireless power

active or reboot EAP350 that operates on a routine basis.

**Schedule** Home Reset

Wifi Schedule: Disable

Schedule Name:

Service:  Reboot  Wireless Active

Day:  Every Day  
 Mon  Tue  Wed  Thu  Fri  Sat  Sun

Time of day:  :

Add Cancel

Schedule Table

#	Name	Service	Schedule	Select
1	schedule01	Reboot	00:01--Mon, Tue, Wed, Thu, Fri, Sat, Sun	<input type="checkbox"/>

Delete Selected Delete All Reset

Accept Cancel

**Wifi Schedule:** Enable or Disable schedule feature.

**Schedule Name:** Enter the description of the schedule service.

**Service:** Select the type of schedule service, either Reboot or wireless active.

**Day:** Select the days of the week to enable the schedule

service.

**Time of Day:** Set the start time that the service is active.

**Add / Cancel:** Click **Add** to append the schedule service to the schedule service table, or **Cancel** to discard changes.

**#:** Displays the ID number of the service in the table

**Name:** Displays the description of the service.

**Service:** Displays the type of service, either Reboot or Wireless Active.

**Schedule:** Displays the schedule information of when the service is active.

**Select:** Select one or more services to delete.

**Delete Selected / Delete All:** Click **Delete Selected** to delete the selected services or **Delete All** to delete all services.

**Accept / Cancel:** Click **Accept** to save the settings or **Cancel** to discard changes.

## 8.8 CLI Setting

Most users will configure the EAP350 through the graphical user interface (GUI). However, for those who prefer an alternative method there is the command line interface (CLI). The CLI can be access through a command console, modem or Telnet connection.



**CLI Setting** Home Reset

---

CLI  ON  OFF

---

Save/Apply Cancel

**CLI:** Select **ON** or **OFF** to enable or disable the ability to modify the EAP350 via a command line interface (CLI).

**Save/Apply / Cancel:** Click **Save/Apply** to apply the changes or **Cancel** to return previous settings.

## 8.9 Log

Display a list of events that are triggered on the EAP350 Ethernet and wireless interfaces. You can consult this log if an unknown error occurs on the system or when a report needs to be sent to the technical support department for debugging purposes.

**Log** Home Reset

---

Syslog

Syslog	Disable ▾
Log Server IP Address / Computer Name	0.0.0.0

Local log

Local Log	Enable ▾
-----------	----------

---

Save/Apply Cancel

**Syslog:** Enable or disable the syslog function.

**Log Server IP Address:** Enter the IP address of the log server.

**Local Log:** Enable or disable the local log service.

**Save/Apply / Cancel:** Click **Save/Apply** to apply the changes or **Cancel** to return previous settings.

## 8.10 Diagnostics

The diagnostics feature allows the administrator to verify that another device is available on the network and is accepting request packets. If get ping packet response, it means a device is on line. This feature does not work if the target device is behind a firewall or has security software installed.

**Diagnostics** Home Reset

---

Ping Test Parameters

Target IP / Domain Name	
Ping Packet Size	64 Bytes
Number of Pings	4

Start Ping

Traceroute Test Parameters

Traceroute target	
-------------------	--

Start Traceroute

Speed Test

Target Address	
Time period	20 Sec
Check Interval	5 Sec
IPv4 Port	5001
IPv6 Port	5002

Start Speed Test

**Target IP:** Enter the IP address you would like to search.

**Ping Packet Size:** Enter the packet size of each ping.

**Number of Pings:** Enter the number of times you want to ping.

**Start Ping:** Click **Start Ping** to begin pinging target device (via IP).

**Traceroute Target:** Enter an IP address or domain name you want to trace.

**Start Traceroute:** Click **Start Traceroute** to begin the trace route operation.

**Target Address:** Enter the IP address of the target PC.

**Time period:** Enter time period for the speed test.

**Check Interval:** Enter the interval for the speed test.

**Start Speed Test:** Click **Start Speed Test** to begin the speed test operation.

**IPv4 / IPv6 Port:** EAP350 use IPv4 port 5001 and IPv6 port 5002 for the speed test.

Please run iperf server (iperf -s) in the target PC.

## 8.11 Device Discovery

This page shows the EnGenius device(s) connected with EAP350 same network.

### Device Discovery

Device Name	Operation Mode	IP Address	System MAC Address	Firmware Version
EAP350	Access Point	192.168.1.18	00:02:6F:0B:A0:7D	1.2.5
EAP350	Access Point	192.168.1.19	00:02:6F:E8:08:80	1.2.5

Refresh

**Device Name:** Displays the name of the devices connected to the network.

**Operation Mode:** Displays the operation mode of the devices connected to the network.

**IP Address:** Displays the IP address of the devices connected to the network.

**System MAC Address:** Displays the system MAC address of the devices connected to the network.

**Firmware Version:** Displays the firmware version of the devices connected to the network.

## 8.12 LED Control

This page allows you to control LED on/off for Power, LAN interface and WLAN interface.

**LED Control** Home Reset

---

LED Control

Power LED	<input type="radio"/> ON <input checked="" type="radio"/> OFF
LAN LED	<input type="radio"/> ON <input checked="" type="radio"/> OFF
WLAN LED	<input type="radio"/> ON <input checked="" type="radio"/> OFF

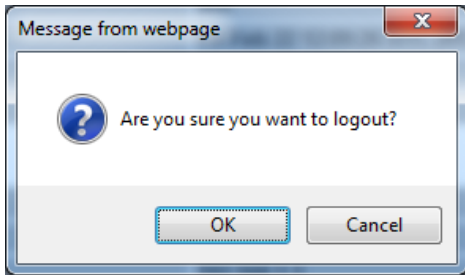
---

Save/Apply Cancel

## 8.13 Logout

Click **Logout** in **Management** menu to logout.

- Management
  - Administration
  - Management VLAN
  - SNMP Settings
  - Backup/Restore Settings
  - Firmware Upgrade
  - Time Settings
  - Schedule
  - CLI Settings
  - Log
  - Diagnostics
  - Device Discovery
  - Led Control
  - Logout



## 8.14 Reset

In some circumstances, it may be required to force the device to reboot. Click on **Reboot the Device** to reboot the EAP350.

### Reset

Home Reset

The System Settings section allows you to reboot the device, or restore the device to the factory default settings. Restoring the unit to the factory default settings will erase all settings, including any rules you have created.

System Commands

Reboot the Device

Restore to Factory Defaults

## Appendix A – FCC Interference Statement

---

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.

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:

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

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.

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

### **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.

## Appendix B – Industry Canada Statement

---

This device complies with RSS-210 of the Industry Canada 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.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

### **Radiation Exposure Statement:**

This equipment complies with IC 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.

**Déclaration d'exposition aux radiations:**  
Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

## Appendix C – CE Interference Statement








---

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

- EN60950-1  
Safety of Information Technology Equipment
  
- EN50385
- Generic standard to demonstrate the compliance of electronic and electrical apparatus with the basic restrictions related to human exposure to electromagnetic fields (0 Hz - 300 GHz)
  
- EN 300 328
- Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive
  
- EN 301 489-1  
Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements
  
- EN 301 489-17
- Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment



 Český [Czech]	<i>[Jméno výrobce]</i> tímto prohlašuje, že tento <i>[typ zařízení]</i> je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
 Dansk [Danish]	Undertegnede <i>[fabrikantens navn]</i> erklærer herved, at følgende udstyr <i>[udstyrets typebetegnelse]</i> overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
 Deutsch [German]	Hiermit erklärt <i>[Name des Herstellers]</i> , dass sich das Gerät <i>[Gerätetyp]</i> in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
 Eesti [Estonian]	Käesolevaga kinnitab <i>[tootja nimi = name of manufacturer]</i> seadme <i>[seadme tüüp = type of equipment]</i> vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
 English	Hereby, <i>[name of manufacturer]</i> , declares that this <i>[type of equipment]</i> is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
 Español [Spanish]	Por medio de la presente <i>[nombre del fabricante]</i> declara que el <i>[clase de equipo]</i> cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
 Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ <i>[name of manufacturer]</i> ΔΗΛΩΝΕΙ ΟΤΙ <i>[type of equipment]</i> ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
 Français [French]	Par la présente <i>[nom du fabricant]</i> déclare que l'appareil <i>[type d'appareil]</i> est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
 Italiano [Italian]	Con la presente <i>[nome del costruttore]</i> dichiara che questo <i>[tipo di apparecchio]</i> è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo <i>[name of manufacturer / izgatavotāja nosaukums]</i> deklarē, ka <i>[type of equipment / iekārtas tips]</i> atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo <i>[manufacturer name]</i> deklaruoja, kad šis <i>[equipment type]</i> atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
 nl	Hierbij verklaart <i>[naam van de fabrikant]</i> dat het toestel <i>[type van toestel]</i> in

Nederlands [Dutch]	overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
 Malti [Maltese]	Hawnhekk, [ <i>isem tal-manifattur</i> ], jiddikjara li dan [ <i>il-mudel tal-prodott</i> ] jikkonforma mal-htigijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Dirrettiva 1999/5/EC.
 Magyar [Hungarian]	Alul írott, [ <i>gyártó neve</i> ] nyilatkozom, hogy a [ <i>... típus</i> ] megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
 Polski [Polish]	Niniejszym [ <i>nazwa producenta</i> ] oświadcza, że [ <i>nazwa wyrobu</i> ] jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
 Português [Portuguese]	[ <i>Nome do fabricante</i> ] declara que este [ <i>tipo de equipamento</i> ] está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
 Slovensko [Slovenian]	[ <i>Ime proizvajalca</i> ] izjavlja, da je ta [ <i>tip opreme</i> ] v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovenský [Slovak]	[ <i>Meno výrobcu</i> ] týmto vyhlasuje, že [ <i>typ zariadenia</i> ] spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
 Suomi [Finnish]	[ <i>Valmistaja = manufacturer</i> ] vakuuttaa täten että [ <i>type of equipment = laitteen tyyppimerkintä</i> ] tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
 Svenska [Swedish]	Härmed intygar [ <i>företag</i> ] att denna [ <i>utrustningstyp</i> ] står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.