

User Manual



EAP300
version 2.0

Ceiling Mount, Multi-Function
Wireless N300 Access Point

Table of Contents

1	Introduction	5
1.1	Features and Benefits	5
1.2	Package Contents	6
1.3	System Requirements.....	7
1.4	Applications	7
2	Before you Begin	9
2.1	Considerations for Wireless Installation	9
2.2	Computer Settings (in Windows XP/Windows 7).....	10
2.3	Computer Settings in Apple Mac OS X.....	13
2.4	Hardware Installation.....	14
3	Configuring Your Access Point	17
3.1	Default Settings	17
3.2	Web Configuration.....	18
4	Building a Wireless Network	20
4.1	Access Point Mode	20
4.2	WDS AP Mode	21
4.3	WDS Bridge Mode.....	22
4.4	Repeater mode	23
5	Status	24
5.1	Save/Reload	24
5.2	Main.....	25
5.3	Wireless Client List.....	28
5.4	Connection Status.....	29
5.5	WDS Link List.....	30

5.6	System Log	31
6	System	32
6.1	Operation Mode.....	32
6.2	IP Settings.....	33
6.3	Spanning Tree Setting.....	35
7	Wireless	37
7.1	Wireless Network.....	37
7.2	Wireless Security	41
7.3	Site Survey	45
7.4	Wireless MAC Filter	49
7.5	Wireless Advanced	50
7.6	WPS (Wi-Fi Protected Setup).....	52
7.7	WDS Link Settings.....	54
8	Management.....	56
8.1	Administration.....	56
8.2	Management VLAN.....	57
8.3	SNMP.....	65
8.4	Backup/Restore.....	67
8.5	Auto Reboot	68
8.6	Firmware Upgrade.....	69
8.7	Time Setting.....	70
8.8	CLI Setting	71
8.9	Log.....	72
8.10	Diagnosis.....	73
8.11	Device Discovery	75
8.12	LED Control	76
8.13	Logout.....	77

8.14 Reset..... 78

Appendix A – FCC Interference Statement 79

Appendix B – Industry Canada Statement..... 80

Appendix C – CE Interference Statement..... 81

Revision History

Version	Date	Notes
1.0	2013/04/22	First Release

1 Introduction

The **EAP300** 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 EAP300 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 EAP300 supports industry-standard WPA/WPA2 encryption and MAC address filtering to authorize only specific devices to access the network.

1.1 Features and Benefits

Features	Benefits
High Speed Data Rate Up to 300Mbps	Capable of handling heavy data payloads including video multimedia streaming.
10/100 Fast Ethernet	Supports up to 100 Mbps wired networking speed.
IEEE 802.11n Compliant and Backwards Compatible with 802.11 b/g devices	Fully compatible with IEEE 802.11b/g/n devices.
Multiple Operation Modes	Allows users to configure the device in any one of the following modes: Access Point, WDS AP, WDS Bridge and Repeater.
Point-to-point, Point-to-Multipoint Wireless Connectivity	Allows transfer of data to and from other access points or wireless bridges.
Support VLAN Tagging of Multiple SSIDs in Access Point mode (up to 8)	Allows clients in specified VLANs to access different portions of the networks based on their specific authorization policies.

WPA/WPA2/IEEE 802.1x Support	Supports industry-standard wireless encryption and RADIUS authentication.
MAC Address Filtering in Access Point mode	Can be configured to grant access to only known devices based on their MAC addresses.
User Isolation Support (Access Point mode)	Offers an additional layer of protection within the network by isolating specific clients.
Power-over-Ethernet (IEEE802.3af)	Enables the EAP300 to be powered via Ethernet cable so it can be deployed on ceilings or in crawlspaces where electrical outlets may not be available.
Save User Settings	Enables network administrators to save their device settings so firmware upgrades do not permanently delete previous device settings.
SNMP Remote Configuration Management	Allows remote connection to configure or manage the EAP300 easily.
QoS (WMM) support	Prioritizes bandwidth-intensive and sensitive data traffic.
IPv6	Supports IPv6 addresses.

1.2 Package Contents

The EAP300 package contains the following items (Resellers and dealers require that all items must be in the package to issue a refund):

- EAP300
- 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), Mac OS X, or Linux-based operating systems.
- Web-Browsing Application (i.e.: Internet Explorer, Firefox, Safari, or other similar browser application).

1.4 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 EAP300, 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 EAP300, 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 EAP300, 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.

2 Before you Begin

This section will guide you through the installation process. Placement of the EnGenius EAP300 is essential to maximize the access point's performance. Avoid placing the EAP300 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 EAP300, 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 EAP300 to have optimal wireless range.

- Keep the number of walls and/or ceilings between the EAP300 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 EAP300. 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 EAP300's signal strength. The most common types of devices are microwaves or cordless phones.

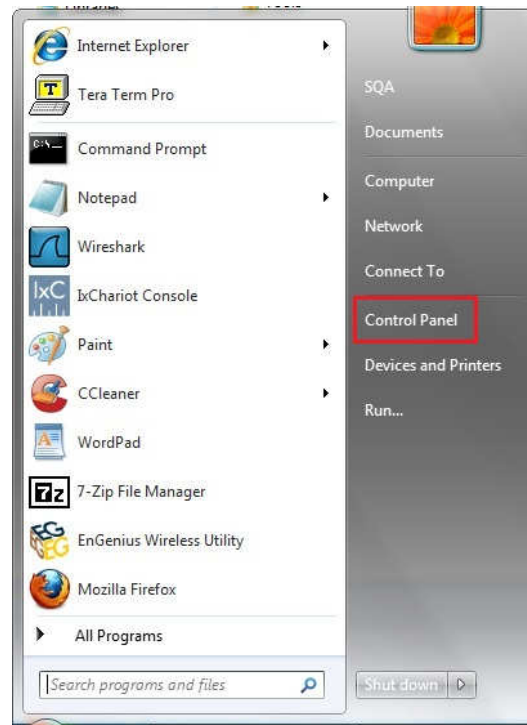
2.2 Computer Settings (in Windows XP/Windows 7)

In order to use the EAP300, you must first configure the TCP/IPv4 connection of your Windows OS computer system.

- Click **Start** button and open **Control Panel**.



Windows XP



Windows 7

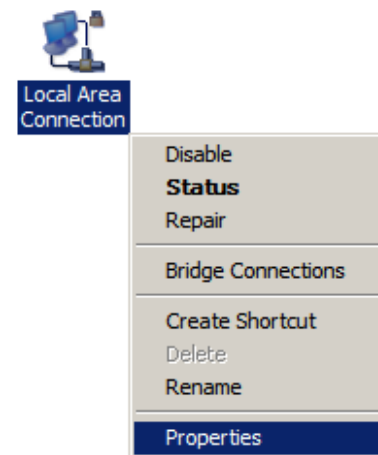
- In **Windows XP**, click **Network Connection**



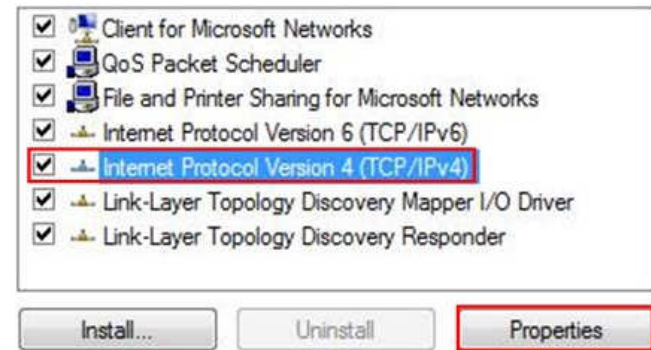
- In **Windows 7**, click **View Network Status and Tasks** in the **Network and Internet** section and then select **Change adapter settings**.



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



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



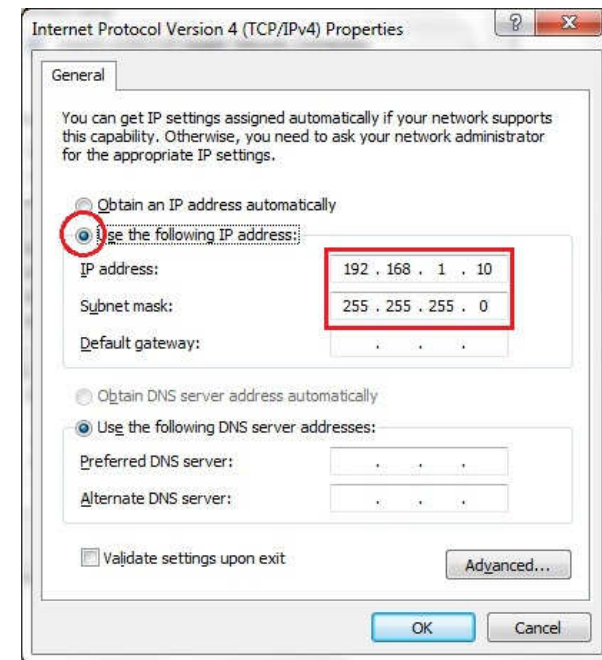
- Select **Use the following IP address** and enter an IP address that is different from the EAP300 and subnet mask then click **OK**.

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 EAP300 and subnet mask then press **OK**.

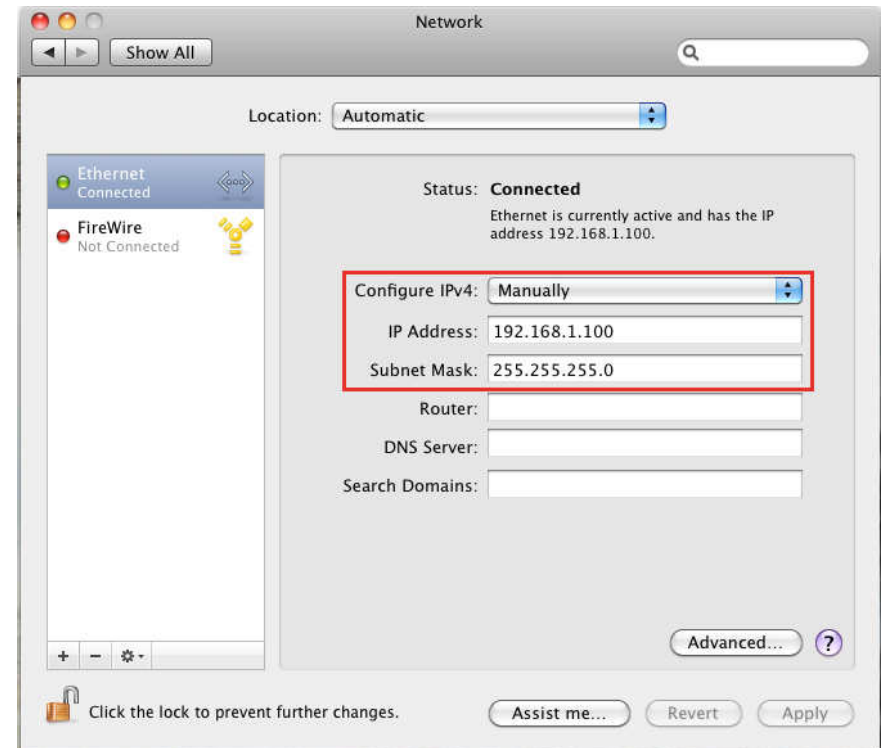
Note: Ensure that the IP address and subnet mask are on the same subnet as the device.

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

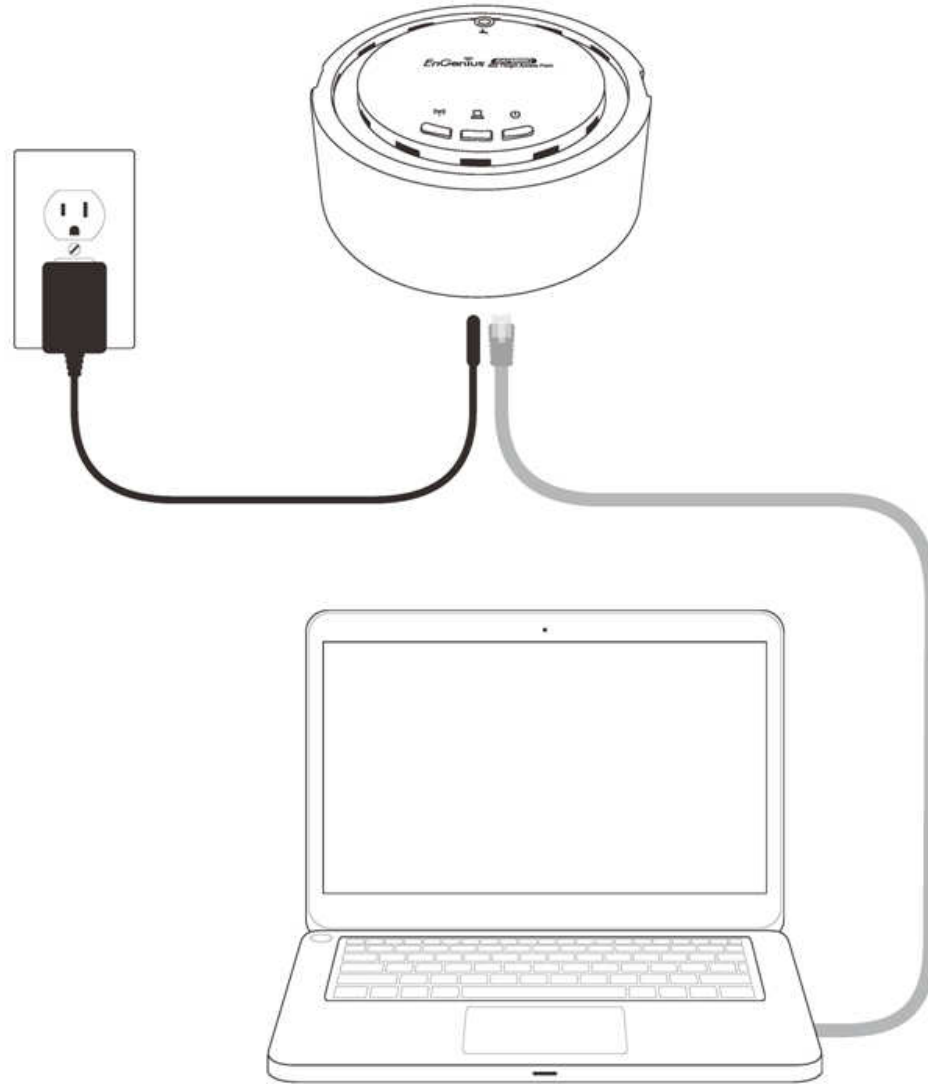
- Click **Apply** when done.



2.4 Hardware Installation

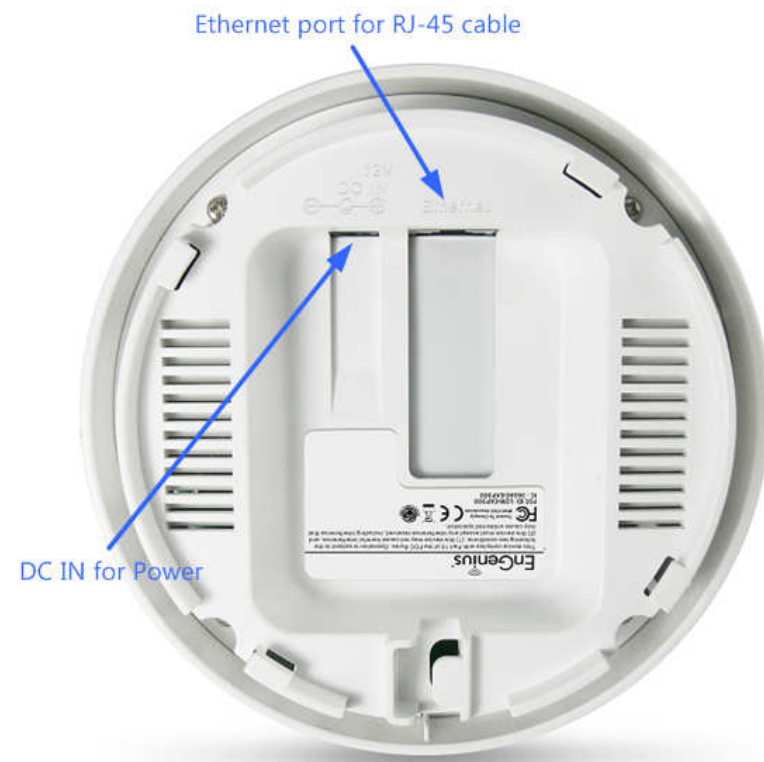
1. Ensure that the computer in use has an available Ethernet (RJ-45) Port. For more information, verify with your computer's user manual.
2. Connect one end of the Category 5e Ethernet cable into the RJ-45 port of the EAP300 and the other end to the RJ-45 port of the computer. Ensure that the cable is securely connected to both the EAP300 and the computer.
3. Connect the Power Adapter DC connector to the DC-IN port of the EAP300 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/EAP300 Connection) light is on (it will be blue).
 - d) Once all lights are on, proceed to set up the EAP300 using the computer.

This diagram depicts the hardware configuration.





Front Panel



Rear Panel

Front Panel	
Reset Button	One click for reset the device. Press over 10 seconds for reset to factory default.
LED Lights	LED lights for Wireless, Ethernet port and Power.
Rear Panel	
DC IN	DC IN for Power.
Ethernet Port	Ethernet port for RJ-45 cable.

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 EAP300.

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.

A screenshot of the EnGenius login page. The page has a light gray background with a rounded rectangular border. At the top center, the text "EnGenius" is displayed. Below it, there are two input fields: "Username:" with the text "admin" entered, and "Password:" with five black dots. At the bottom, there are two buttons: "Login" and "Reset".

- You will see the following webpage if login successfully.

EnGenius®
Wireless Access Point

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
- Auto Reboot Settings
- Firmware Upgrade
- Time Settings
- CLI Settings
- Log
- Diagnostics
- Device Discovery
- Led Control
- Logout

[Home](#)
[Reset](#)

Main

System Information

Device Name	EAP300V2
Ethernet Main MAC Address	00:02:13:15:64:64
Ethernet Secondary MAC Address	00:02:13:15:64:64
Wireless MAC Address (SSID/MAC)	1 00:02:13:15:64:64
	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	Fri Apr 19 10:07:04 UTC 2013
Firmware Version	1.3.3
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::202:13FF:FE15:6464
IPv6 Default Gateway	
IPv6 Primary DNS	
IPv6 Secondary DNS	
RX(Packets)	74.4248 KB (669 PKts.)
TX(Packets)	268.138 KB (478 PKts.)

4 Building a Wireless Network

The EAP300 has the ability to operate in various modes. This chapter describes the operating modes of the EAP300.

4.1 Access Point Mode

In Access Point Mode, EAP300 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 EAP300. The EAP300 supports up to eight SSIDs at the same time for secure access.



4.2 WDS AP Mode

The EAP300 also supports WDS AP mode. This operating mode allows wireless connections to the EAP300 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 EAP300 can wirelessly connect different LANs by configuring the MAC address and security settings of each EAP300 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 EAP300 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 EAP300, the EAP300 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.

Save/Reload

[Home](#)[Reset](#)

Unsaved changes list

```
-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=...
```

[Save & Apply](#)[Revert](#)

5.2 Main

Clicking the **Main** link under the **Status** menu or clicking **Home** at the top-right of the EAP300 Page shows the status information about the current operating mode.

- The **System Information** section shows 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	EAP300V2
Ethernet Main MAC Address	00:02:13:15:64:64
Ethernet Secondary MAC Address	00:02:13:15:64:64
Wireless MAC Address (SSID/MAC)	1 00:02:13:15:64:64
	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	Fri Apr 19 10:07:04 UTC 2013
Firmware Version	1.3.3
Management VLAN ID	Untagged

- The **LAN Settings** section shows 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::202:6FFF:FE11:5578
IPv6 Default Gateway	
IPv6 Primary DNS	
IPv6 Secondary DNS	
RX(Packets)	104.755 KB (1048 PKts.)
TX(Packets)	484.877 KB (879 PKts.)

- The **Current Wireless Settings** section shows wireless information such as Operating Mode, Frequency, Channel, Distance, RX and TX. Since the EAP300 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 EnGenius115578/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)	34.5303 KB (147 PKts.)

5.3 Wireless Client List

Clicking the **Wireless Client List** link under the **Status** menu displays the list of clients associated to the EAP300, 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

[Home](#)[Reset](#)

SSID:#	MAC Address	TX(Bytes)	RX(Bytes)	RSSI(dBm)	Kick and Ban
SSID1:#1	00:02:6f:63:69:19	0Kb	1Kb	-28	Kick

[Refresh](#)

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 EAP300 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

```

Apr 19 10:10:01 EAP300V2 user.notice root: starting ntpd
Apr 19 10:10:01 EAP300V2 cron.info crond[2020]: crond: USER root pid 2472 cmd . /etc/hotplug.d/iface
Apr 19 10:06:30 EAP300V2 user.notice root: starting ntpd
Apr 19 10:06:30 EAP300V2 daemon.warn dnsmasq[1866]: ignoring nameserver 127.0.0.1 - local interface
Apr 19 10:06:30 EAP300V2 daemon.info locator[1993]: daemonize: Unable to read pid file [/var/run/loc
Apr 19 10:06:30 EAP300V2 daemon.info dnsmasq[1866]: using local addresses only for domain lan
Apr 19 10:06:30 EAP300V2 daemon.info dnsmasq[1866]: reading /tmp/resolv.conf
Apr 19 10:06:30 EAP300V2 cron.info crond[2020]: crond: crond (busybox 1.19.4) started, log level 5
Apr 19 10:06:27 EAP300V2 user.warn kernel: done.
Apr 19 10:06:27 EAP300V2 user.info kernel: mini_fo: using storage directory: /jffs
Apr 19 10:06:27 EAP300V2 user.info kernel: mini_fo: using base directory: /
Apr 19 10:05:49 EAP300V2 user.warn kernel: enet1 port0 up 100Mbps Full duplex
Apr 19 10:05:49 EAP300V2 user.warn kernel: WASP ----> S27 PHY MDIO
Apr 19 10:05:49 EAP300V2 user.warn kernel: Setting Drop CRC Errors, Pause Frames and Length Error fr
Apr 19 10:05:49 EAP300V2 user.warn kernel: ATHR_GMAC: done cfg2 0x7215 ifctl 0x0 miictrl
Apr 19 10:05:49 EAP300V2 user.warn kernel: ATHR_GMAC: Enet Unit:1 PHY:0 is UP RGMii 1000Mbps full du
Apr 19 10:05:44 EAP300V2 user.warn kernel: enet1 port0 down
Apr 19 10:05:44 EAP300V2 user.warn kernel: ATHR_GMAC:unit 1: phy 0 not up carrier 1
Apr 19 10:05:43 EAP300V2 user.debug kernel: ath0: no IPv6 routers present
Apr 19 10:05:39 EAP300V2 user.warn kernel: CT not confirmed ct=83b87000
Apr 19 10:05:39 EAP300V2 user.warn kernel: CT not confirmed ct=83b87000
Apr 19 10:05:39 EAP300V2 user.warn kernel: CT not confirmed ct=83b87000
  
```


System Log	
Refresh	Update the log.
Clear	Clear the log.

6 System

6.1 Operation Mode

The EAP300 supports four operating modes: Access Point, WDS Access Point, WDS Bridge and Repeater.

System Properties

[Home](#)
[Reset](#)

System Properties

Device Name	<input type="text" value="EAP300V2"/> (1 to 32 characters)
Country/Region	<input type="text" value="Please Select a Country Code"/> ▼
Operation Mode	<input type="radio"/> Access Point <input checked="" type="radio"/> WDS <input checked="" type="radio"/> Access Point <input type="radio"/> Bridge <input type="radio"/> Repeater

System Properties	
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.
Country/Region	Select a Country/Region to conform to local regulations.
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 Settings	
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 Prefix Length	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)

Spanning Tree	
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 hello packets to communicate information about the topology throughout the entire Bridged Local Area Network.
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
EnGenius115578	None	<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/>
EnGenius115578_2	None	<input type="checkbox"/>	2	<input type="checkbox"/>	<input type="button" value="Edit"/>
EnGenius115578_3	None	<input type="checkbox"/>	3	<input type="checkbox"/>	<input type="button" value="Edit"/>
EnGenius115578_4	None	<input type="checkbox"/>	4	<input type="checkbox"/>	<input type="button" value="Edit"/>
EnGenius115578_5	None	<input type="checkbox"/>	5	<input type="checkbox"/>	<input type="button" value="Edit"/>
EnGenius115578_6	None	<input type="checkbox"/>	6	<input type="checkbox"/>	<input type="button" value="Edit"/>
EnGenius115578_7	None	<input type="checkbox"/>	7	<input type="checkbox"/>	<input type="button" value="Edit"/>
EnGenius115578_8	None	<input type="checkbox"/>	8	<input type="checkbox"/>	<input type="button" value="Edit"/>

Wireless Network (Access Point / WDS AP mode)	
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 for your country's regulation.
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	<input type="text" value="EnGenius115578"/> (1 to 32 characters)
VLAN ID	<input type="text" value="1"/> (1~4094)
Suppressed SSID	<input type="checkbox"/>
Station Separation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Wireless Security

Security Mode	<input type="text" value="Disabled"/> ▼
---------------	---

<input type="button" value="Save"/>	<input type="button" value="Cancel"/>
-------------------------------------	---------------------------------------

SSID Profile	
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 : <input type="text" value="AP SSID"/> (1 to 32 characters) Or press the button to search for any available WLAN Service. <input type="button" value="Site Survey"/>
Repeater SSID	<input type="text" value="AP SSID"/> (1 to 32 characters)
Prefered BSSID	<input type="checkbox"/> <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/>

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 ▼

Wireless Network (Repeater mode)	
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 EAP300'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	

WEP Encryption	
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)

WPA-PSK (WPA Pre-Shared Key) Encryption	
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	<input type="text"/>
Radius Port	1812 <input type="text"/>
Radius Secret	<input type="text"/>
Group Key Update Interval	3600 <input type="text"/> seconds(30~3600, 0: disabled)
Radius Accounting	Enable ▼
Radius Accounting Server	<input type="text"/>
Radius Accounting Port	1813 <input type="text"/>
Radius Accounting Secret	<input type="text"/>
Interim Accounting Interval	600 <input type="text"/> seconds(60~600)

WPA Encryption	
Encryption	Select the WPA encryption type you would like. Please ensure that your wireless clients 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 ▾
SSID	Specify the static SSID : <input type="text" value="AP SSID"/> (1 to 32 characters) Or press the button to search for any available WLAN Service. <input type="button" value="Site Survey"/>
Repeater SSID	<input type="text" value="AP SSID"/> (1 to 32 characters)
Preferred BSSID	<input type="checkbox"/> <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/>

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 ▾
---------------	------------

2. Scanning for the nearby access points

Scanning








Please wait...

3. The EAP300 will list the available access points after site survey.

Site Survey

2GHz Site Survey

:Infrastructure :Ad_hoc

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



Refresh








Site Survey (Repeater mode)	
BSSID	Access Point's wireless MAC address.
SSID	SSID that the Access Point is broadcasting.
Channel	Channel that the Access Point is using.
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.

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

Site Survey

2GHz Site Survey

:Infrastructure :Ad_hoc

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

Refresh

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

Wireless Network

[Home](#)[Reset](#)

Wireless Mode	802.11 B/G/N Mixed ▼
SSID	Specify the static SSID : <input type="text" value="EnGenius"/> (1 to 32 characters) Or press the button to search for any available WLAN Service. <input type="button" value="Site Survey"/>
Repeater SSID	<input type="text" value="AP SSID"/> (1 to 32 characters)
Preferred BSSID	<input type="checkbox"/> <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"/>

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	<input type="text" value="12345678"/> (8 to 63 characters) or (64 Hexadecimal characters)

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 EAP300. The default setting is **Disabled**.

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

Wireless MAC Filter

[Home](#)
[Reset](#)

 ACL Mode
 : : : : :

#	MAC Address	
1	00:02:6F:32:54:AC	<input type="button" value="Delete"/>

Wireless Filter (Access Point / WDS AP / Repeater mode)	
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 advance 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	20 dBm <input type="checkbox"/> Obey Regulatory Power
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 type="radio"/> Enable <input checked="" type="radio"/> Disable
Incoming Traffic Limit	1000 kbit/s (512-99999999)
Outgoing Traffic Limit	180000 kbit/s (512-99999999)
Total Percentage	10 %
SSID #1 : EnGenius115578	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

[Accept](#)
[Cancel](#)

Wireless Advanced	
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 RTC/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 checked="" type="radio"/> Enable <input type="radio"/> Disable
WPS current status	Configured Release Configuration
Self Pin Code	45998621
SSID	EnGeniusBEEF06
Authentication Mode	WPA-PSK Mixed TKIP/AES
Passphrase Key	12345678
WPS Via Push Button	Start to Process
WPS Via Pin	<input type="text"/> Start to Process

[Accept](#)
[Cancel](#)

WPS (Wi-Fi Protected Setup)	
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.

Home
Reset

WDS Link Settings

Security	None ▾
WEP Key	<input type="text" value=""/> 40/64-bit(10 hex digits) ▾
AES Passphrase	<input type="text" value=""/> (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"/>	Enable ▾
2	<input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/>	Disable ▾
3	<input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/>	Disable ▾
4	<input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/>	Disable ▾
5	<input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/>	Disable ▾
6	<input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/>	Disable ▾
7	<input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/>	Disable ▾
8	<input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/> : <input type="text" value=""/>	Disable ▾

Accept
Cancel

WDS Link Settings	
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 EAP300 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	<input type="text" value="admin"/>
New Password	<input type="password"/>
Confirm Password	<input type="password"/>
<input type="button" value="Save/Apply"/> <input type="button" value="Cancel"/> <input type="button" value="logout"/>	

Login Setting	
New Name	Enter a new username for logging in to the Web Configurator.
New Password	Enter a new password for logging in to the Web Configurator.
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](#)

Caution: 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 checked="" 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	
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 EAP300. Verify that the DHCP server supports the reconfigured VLAN ID and then reconnect to the EAP300 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**.

EnGenius® | Wireless Access Point

Access Point

Status

- . Save/Reload:1
- . Main
- . Wireless Client List
- . System Log

System

- . Operation Mode
- . IP Settings
- . Spanning Tree Settings

Home Reset

Save/Reload

Unsaved changes list

network.lan.ipaddr=192.168.1.254

Caution: Network Setting changed, redirect IP to 192.168.1.254

Save & Apply Revert

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

The screenshot displays the EnGenius Wireless Access Point configuration web interface. The page title is "Wireless Access Point" and the current section is "Access Point". The "System Properties" section is active, showing the following fields:

- Device Name:** EAP300V2 (1 to 32 characters)
- Country/Region:** Please Select a Country Code
- Operation Mode:** Access Point, WDS, Repeater

At the bottom of the form, there are two buttons: "Save & Apply" and "Cancel".

Left Sidebar:

- Status**
 - Save/Reload:0
 - Main
 - Wireless Client List
 - System Log
- System**
 - Operation Mode
 - IP Settings

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.

EnGenius®
Wireless Access Point

Access Point

- Status**
- Save/Reload:24
- 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

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	Scan				

Current Profiles					
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

Accept
Cancel

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 checked="" 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)

Save	Cancel
------	--------

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

EnGenius®
Wireless Access Point

Access Point

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

Status

- Save/Reload:24
- 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

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.

The screenshot displays the EnGenius Wireless Access Point configuration interface. The left sidebar shows the navigation menu with 'IP Settings' highlighted under the 'System' section. The main content area is titled 'IP Settings' and includes 'Home' and 'Reset' buttons. The 'System Information' section contains a table of IP-related settings. The 'IP Network Setting' is set to 'Specify an IP address'. The 'IP Address' is 192.168.1.1, 'IP Subnet Mask' is 255.255.255.0, and 'Default Gateway' is 192.168.1.254. The 'Use Link-Local Address' checkbox is checked. At the bottom, there are 'Accept' and 'Cancel' buttons.

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 . 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, 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 checked="" type="radio"/> Specified VLAN ID <input type="text" value="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 Settings

[Home](#)
[Reset](#)

SNMP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Contact	<input type="text"/>
Location	<input type="text"/>
Community Name (Read Only)	<input type="text" value="public"/>
Community Name (Read/Write)	<input type="text" value="private"/>
Trap Destination Address	<input type="text"/>
Trap Destination Community Name	<input type="text" value="public"/>
SNMPv3	<input checked="" type="radio"/> v3Enable <input type="radio"/> v3Disable
User Name (1-31 Characters)	<input type="text" value="admin"/>
Auth Protocol	<input type="text" value="MD5"/>
Auth Key (8-32 Characters)	<input type="text" value="12345678"/>
Priv Protocol	<input type="text" value="DES"/>
Priv Key (8-32 Characters)	<input type="text" value="12345678"/>
Engine ID	<input type="text"/>

[Save/Apply](#)
[Cancel](#)

SNMP	
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	
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	
SNMPv3 Enable/Disable	Enable or Disable SNMPv3 feature.
User Name	Specify the username for SNMPv3.
Auth Protocol	Select the authentication protocol type: MDS 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 EAP300 incorrectly, you can use the **Factory Default** button in the **Revert to Factory Default Settings** section to restore all the configurations of the EAP300 to the original default settings.

Backup/Restore Settings

Save A Copy of Current Settings

Restore Saved Settings from A File

Revert to Factory Default Settings

Backup/Restore	
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 EAP300 to its factory default settings.

8.5 Auto Reboot

This page allows you to enable or disable the Auto Reboot function. This feature is particularly convenient to administrators for the scheduling of auto rebooting on the device.

This page also allows you to set the frequency of this function.

Auto Reboot Settings

[Home](#)
[Reset](#)

Auto Reboot Setting	Disable ▾
Frequency of Auto Reboot	Min ▾ 10 Mins ▾

Auto Reboot	
Auto Reboot Setting	Select Enable from the drop-down menu to setup this function.
Frequency of Auto Reboot	Select the frequency interval using the drop-down menus.
Save/Apply / Cancel	Click Save/Apply to apply the changes or Cancel to return previous settings.

8.6 Firmware Upgrade

This page allows you to upgrade the firmware of EAP300.

Firmware Upgrade Home Reset

Current firmware version: 1.3.1

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.

8.7 Time Setting

This page allows you to set the internal clock of the EAP300.

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](#)

Time	
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.

8.8 CLI Setting

Most users will configure the EAP300 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

CLI Setting	
CLI	Select ON or OFF to enable or disable the ability to modify the EAP300 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 EAP300 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.

Home
Reset

Log

Syslog

Syslog	Disable ▾
Log Server IP Address / Computer Name	0.0.0.0

Local log

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

Save/Apply
Cancel

Log	
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 Diagnosis

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	<input type="text"/>
Ping Packet Size	<input type="text" value="64"/> Bytes
Number of Pings	<input type="text" value="4"/>

Traceroute Test Parameters

Traceroute target	<input type="text"/>
-------------------	----------------------

Speed Test

Target Address	<input type="text"/>
Time period	<input type="text" value="20"/> Sec
Check Interval	<input type="text" value="5"/> Sec
IPv4 Port	5001
IPv6 Port	5002

Diagnostics	
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	EAP300 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 EAP300 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:DB:A0:7D	1.2.5
EAP350	Access Point	192.168.1.19	00:02:6F:E8:08:80	1.2.5

Refresh

Device Discovery	
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](#)

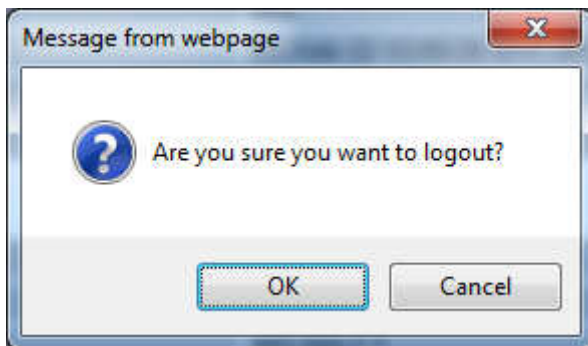
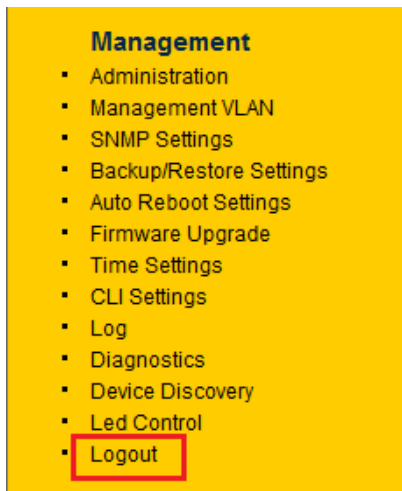
LED Control

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

[Save/Apply](#)[Cancel](#)

8.13 Logout

Click **Logout** in **Management** menu to 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 EAP300.

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

Federal Communication Commission Interference Statement

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

- 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 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.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

This device complies with FCC RF Exposure limits set forth for an uncontrolled environment, under 47 CFR 2.1093 paragraph (d)(2).

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

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.

Important:

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

Europe – EU Declaration of Conformity

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









This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

CE 0560!

cs Česky [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.
da 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.
de Deutsch [German]	Hiermit erkläre <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.
et 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.
en 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.
es 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.
el 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.
fr 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.
it 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 [name of manufacturer / izgatavotāja nosaukums] deklarē, ka [type of equipment / iekārtas tips] atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo [manufacturer name] deklaruoja, kad šis [equipment type] atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
 Nederlands [Dutch]	Hierbij verklaart [naam van de fabrikant] dat het toestel [type van toestel] in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
 Malti [Maltese]	Hawnhekk, [isem tal-manifattur], jiddikjara li dan [il-mudel tal-prodott] jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
 Magyar [Hungarian]	Alulírott, [gyártó neve] nyilatkozom, hogy a [... típus] megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
 Polski [Polish]	Niniejszym [nazwa producenta] oświadcza, że [nazwa wyrobu] jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
 Português [Portuguese]	[Nome do fabricante] declara que este [tipo de equipamento] está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
 Slovensko [Slovenian]	[Ime proizvajalca] izjavlja, da je ta [tip opreme] v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	[Meno výrobcu] týmto vyhlasuje, že [typ zariadenia] spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
 Suomi [Finnish]	[Valmistaja = manufacturer] vakuuttaa täten että [type of equipment = laitteen tyyppimerkintä] tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
 Svenska [Swedish]	Härmed intygar [företag] att denna [utrustningstyp] står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.