EnGenius®

11N Multi-Function Access Point

EAP300

11N Multi-Function Access Point

V2.0

Table of Contents

1 Introduction 4

1.1 Features and Benefits 4
1.2 Package Contents 5
1.3 System Requirements 5
1.4 Applications 6

2 Before you Begin 8

2.1 Considerations for Wireless Installation 8
2.2 Computer Settings (Windows XP/Windows 7) 9
2.3 Apple Mac X OS 12
2.4 Hardware Installation 13

3 Configuring Your Access Point 14

3.1 Default Settings 14
3.2 Web Configuration 15

4 System 18

4.1 Operation Mode 18
4.2 Status 19
4.3 DHCP 21
4.4 Schedule 24
4.5 Event Log 26
4.6 Monitor 27

5 Wireless 28

5.1 Status 28
5.2 Basic 29
5.3 Advanced 31
5.4 Security 35
5.5 Filter 41

5.6 WPS (Wi-Fi Protected Setup) 43
5.7 Client List 45
5.8 VLAN 46

6 Network 47

6.1 Status 47
6.2 LAN 48
6.3 Spanning Tree 50

7 Management 51

7.1 Admin 51
7.2 SNMP 52
7.3 Firmware Upgrade 54
7.4 Configure 57
7.5 Reset 58

8 Tools 59

8.1 Time Setting 59
8.2 Diagnosis 60
8.3 LED Control 61

9 Logout 62

Appendix A – FCC Interference Statement 63

Revision History

Version	Date	Notes
1.0	2011/06/24	First Release

1 Introduction

EAP300 is a multi-functioned 11n product with 3 major multi-functions, is designed to operate in every working environment for enterprises.

EAP300 is a Wireless Network device that delivers up to 6x faster speeds and 7x extended coverage than 802.11b/g devices. EAP300 supports home network with superior throughput, performance and unparalleled wireless range.

To protect data during wireless transmissions, EAP300 encrypts all wireless transmissions through WEP data encryption and supports WPA/WPA2. Its MAC address filter allows users to select stations with access to connect network. In addition, the function of user isolation protects private network between client users. EAP300 thus is the best product to ensure network safety for enterprises.

1.1 Features and Benefits

Features	Benefits
High Speed Data Rate Up to 300Mbps	**Capable of handling heavy data payloads such as MPEG video streaming.**
10/100 Fast Ethernet	**Support up to 100Mbps networking speed.**
IEEE 802.11n draft Compliant and backward compatible with 802.11b/g	**Fully compatible with IEEE 802.11b/g/n devices.**
Multi-Function, 3 functions	**Allowing users to select AP, WDS AP or WDS Bridge mode in various applications.**
Point-to-point, Point-to-multipoint Wireless Connectivity	**Allowing to transfer data from buildings to buildings.**
Support Multi-SSID function (4 SSID) in AP mode	**Allowing clients to access different networks through a single access point and to assign different policies and functions for each SSID by manager.**

WPA2/WPA/ IEEE 802.1x support	**Powerful data security.**
MAC address filtering in AP mode	**Ensuring secure network connection.**
User isolation support (AP mode)	**Protecting the private network between client users.**
Power-over-Ethernet (IEEE802.3af)	**Flexible Access Point locations and saving cost.**
Keep personal setting	**Keeping the latest setting when firmware upgrade.**
SNMP Remote Configuration Management	**Helping administrators to remotely configure or manage the Access Point easily.**
QoS (WMM) support	**Enhancing user performance and density.**

1.2 Package Contents

The package contains the following items. In case of return, please keep the original box set, and the complete box set must be included for full refund.

- EAP300
- 12V/1A 100V~240V Power Adapter
- RJ-45 Ethernet LAN Cable
- CD-ROM with User's Manual
- Quick Guide

1.3 System Requirements

The following are the minimum system requirements in order configure the device.

- Computer with an Ethernet interface or Wireless Network function.
- Windows, Mac OS or Linux based operating systems

- Internet Explorer or Firefox or Safari Web-Browser Software

1.4 Applications

The wireless LAN products are easy to install and highly efficient. The following list describes some of the many applications made possible through the power and flexibility of wireless LANs:

a) **Difficult-to-wire environments**
There are many situations where wires cannot be laid easily. Historic buildings, older buildings, open areas and across busy streets make the installation of LANs either impossible or very expensive.

b) **Temporary workgroups**
Consider situations in parks, athletic arenas, exhibition centers, disaster-recovery, temporary offices and construction sites where one wants a temporary WLAN established and removed.

c) **The ability to access real-time information**
Doctors/nurses, point-of-sale employees, and warehouse workers can access real-time information while dealing with patients, serving customers and processing information.

d) **Frequently changed environments**
Show rooms, meeting rooms, retail stores, and manufacturing sites where frequently rearrange the workplace.

e) **Small Office and Home Office (SOHO) networks**
SOHO users need a cost-effective, easy and quick installation of a small network.

f) **Wireless extensions to Ethernet networks**
Network managers in dynamic environments can minimize the overhead caused by moves, extensions to networks, and other changes with wireless LANs.

g) **Wired LAN backup**

Network managers implement wireless LANs to provide backup for mission-critical applications running on wired networks.

h) Training/Educational facilities

Training sites at corporations and students at universities use wireless connectivity to ease access to information, information exchanges, and learning.

2 Before you Begin

This section will guide you through the installation process. Placement of the ENGENIUS EAP300 is very important to avoid poor signal reception and performance. Avoid placing the device in enclosed spaces such as a closet, cabinet or wardrobe.

2.1 Considerations for Wireless Installation

The operating distance of all wireless devices cannot be pre-determined due to a number of unknown obstacles in the environment that the device is deployed. These could be the number, thickness and location of walls, ceilings or other objects that the wireless signals must pass through. Here are some key guidelines to ensure that you have the optimal wireless range.

- Keep the number of walls and ceilings between the EnGenius access point and other network devices to a minimum. Each wall or ceiling can reduce the signal strength; the degradation depends on the building's material.

- Building materials makes a difference. A solid metal door or aluminum stubs may have a significant negative effect on range. Locate your wireless devices carefully so the signal can pass through a drywall or open doorways. Materials such as glass, steel, metal, concrete, water (fish tanks), mirrors, file cabinets and brick will also degrade your wireless signal.

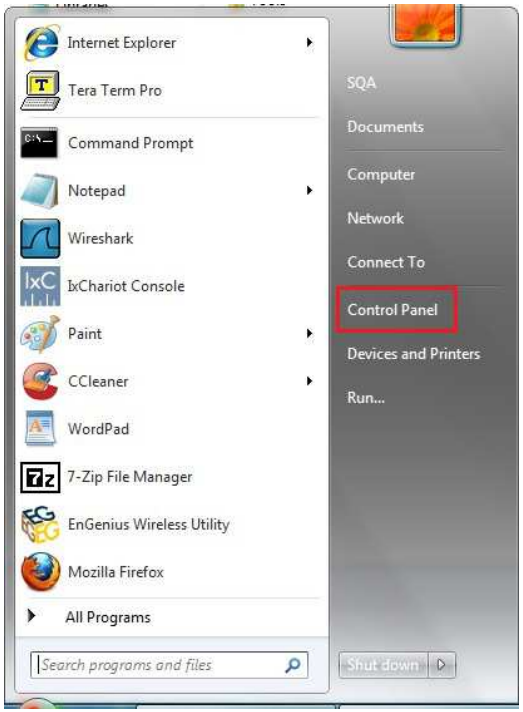
- Interferences can also come from your other electrical devices or appliances that generate RF noise. The most usual types are microwaves, or cordless phones.

2.2 Computer Settings (Windows XP/Windows 7)

This device can be configured as an Access Point, WDS AP or WDS Bridge. The default IP address of the device is **192.168.1.1** (In Access Point Mode as default). In order to log into this device, you must first configure the TCP/IP settings of your PC/Notebook.

- Click Start button and open Control Panel.

Windows XP



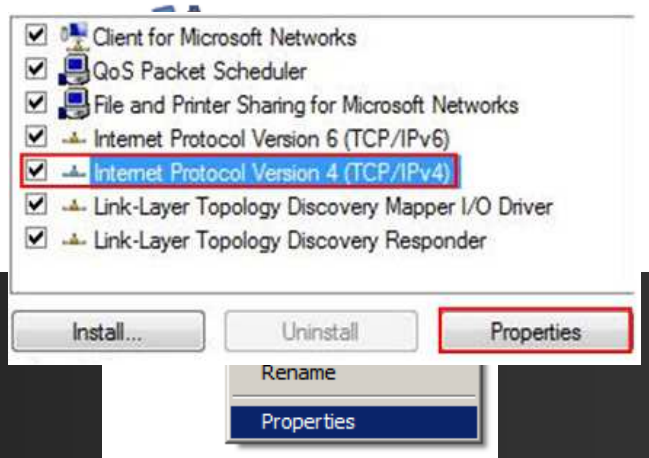
Windows 7

- Windows XP, click [Network Connection]

- Windows 7, click [View Network Status and Tasks] then [Change adapter settings]

- Right click on [Local Area Connection] and select [Properties].

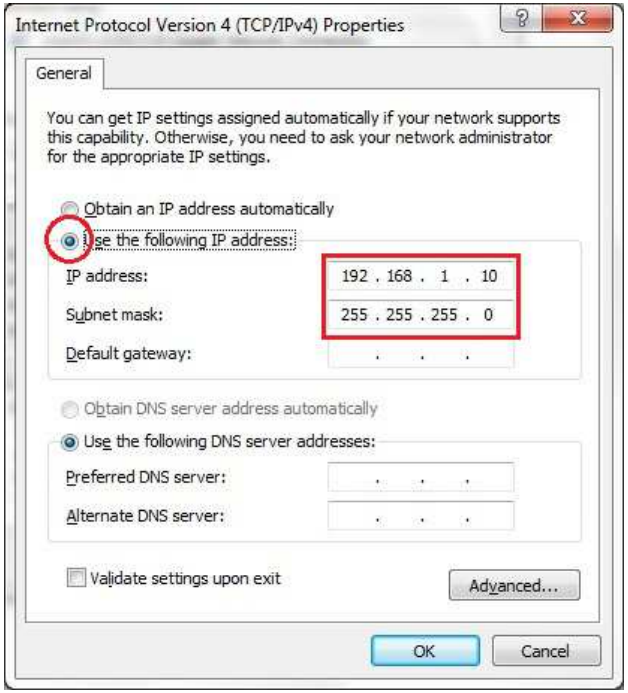
- Select "**Internet Protocol (TCP/IP)**" and click [Properties]



- Select "**Use the following IP address**" and enter IP address and subnet mask then click [OK].

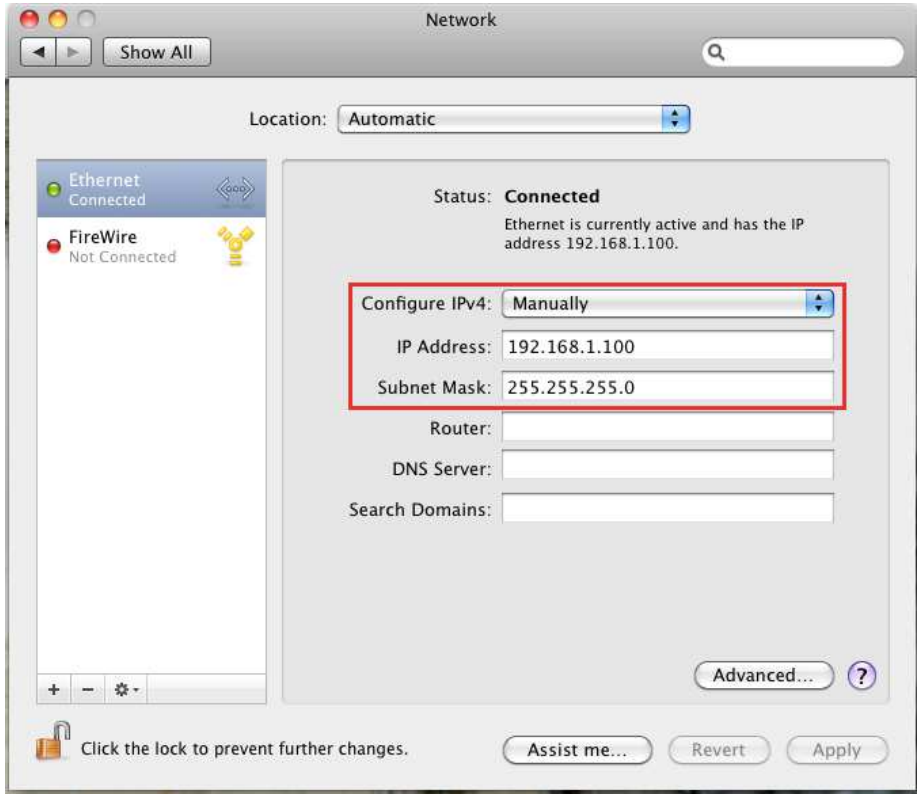
Note: Ensure that the IP address and subnet mask are on the same subnet as the device.

For example: Device IP address: 192.168.1.1
PC IP address: 192.168.1.10
PC subnet mask: 255.255.255.0



2.3 Apple Mac X OS

- Go to **System Preferences** > **Network**



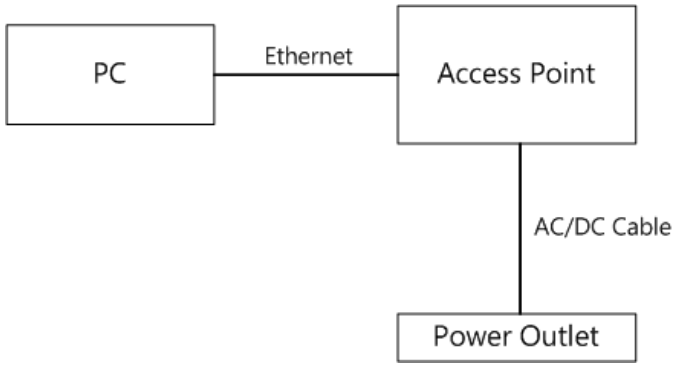
- Under Network setting, select "**Manually**" and enter IP address and subnet mask.

- Click **Apply** when done.

2.4 Hardware Installation

1. Place the unit in an appropriate location after conducting a site survey.
2. Plug one end of the Ethernet cable into the Ethernet port of the device and another end into your PC/Notebook.
3. Insert the DC-inlet of the power adapter into the port labeled “DC-IN” and the other end into the power socket on the wall.

This diagram depicts the hardware configuration.



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 Access Point.

Default Settings

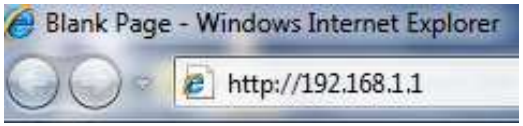
IP Address	192.168.1.1
Username / Password	admin / admin
Operation Mode	Access Point
Wireless SSID	EnGenius*xxxxxx*
Wireless Security	None

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.

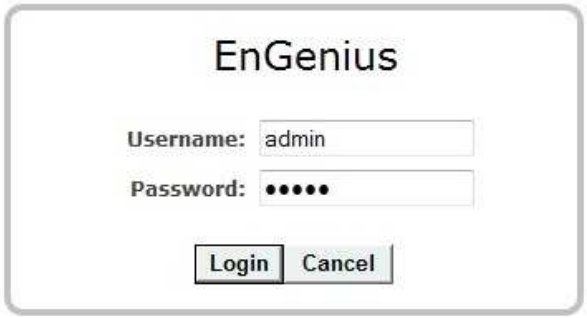
3.2 Web Configuration

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

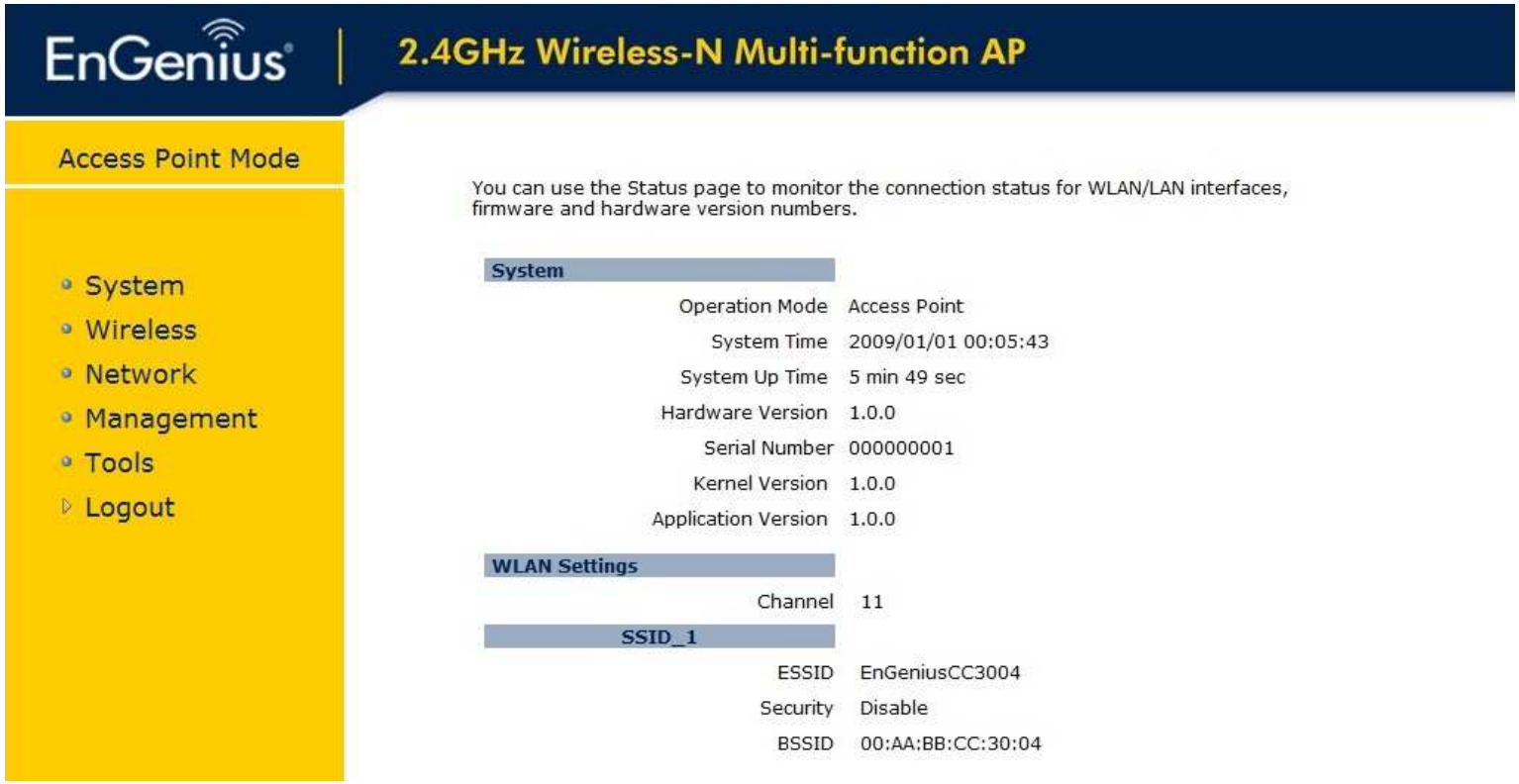
  Note: If you have changed the default LAN IP Address of the Access Point, ensure you enter the correct IP Address.



- 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.



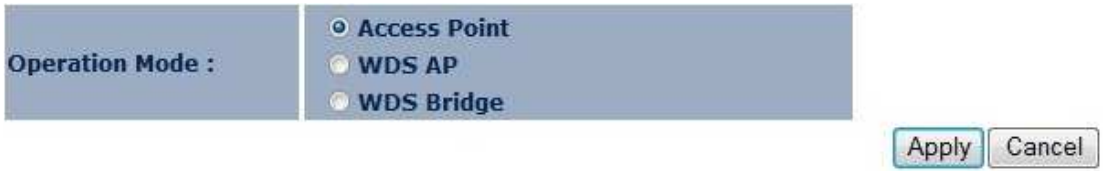
- The navigation drop-down menu on left is divided into seven main sections:

1. **System**: This menu includes the operation mode, status, DHCP, schedule, event log, and monitor. Through this section, you can also change the device operating mode, such as Access Point, WDS AP or WDS Bridge.
2. **Wireless**: This menu includes status, basic, advanced, security, filter, client list and VLAN.
3. **Network**: This menu includes status, LAN and spanning tree.
4. **Management**: This menu includes the admin setup, SNMP, firmware upgrade, save/restore backup and device reset.
5. **Tools**: Displays the time zone, diagnostics and LED control.
6. **Logout**: To logout the system. Need to open up a new browser window in order to login again.

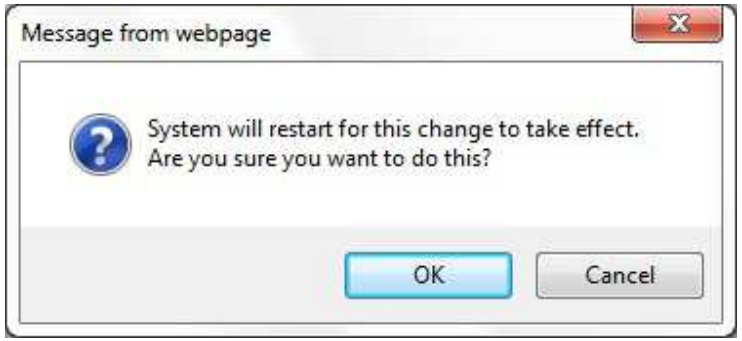
4 System

4.1 Operation Mode

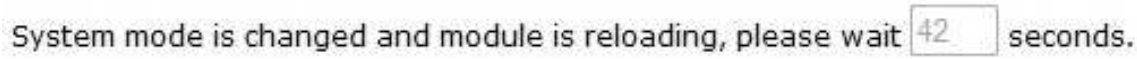
Each of the operating modes offers different features. In order to switch the operating mode, select it from the System >> Operation Mode. There are three operation modes: Access Point, WDS AP and WDS Bridge.



A dialog box will appear to notify you that the system will restart in order for the change to take effect. Click on the **OK** button to continue.



Please wait while the device counts down and restarts into the new operating mode.



4.2 Status

This page will display status of the device.

System

Operation Mode	Access Point
System Time	2009/01/01 00:05:43
System Up Time	5 min 49 sec
Hardware Version	1.0.0
Serial Number	000000001
Kernel Version	1.0.0
Application Version	1.0.0

System	
Operation Mode	The device is currently in which mode.
System Time	The device's system time. If this is incorrect, please set the time in the Tools / Time page.
System Up Time	The duration about the device has been operating without powering down or reboot.
Hardware Version and Serial Number	Hardware information for this device.
Kernel and Application Version	Firmware information for this device.

WLAN Settings	
Channel	11
SSID_1	
ESSID	EnGeniusCC3004
Security	Disable
BSSID	00:AA:BB:CC:30:04

WLAN Settings	
Channel	The wireless channel in use.
ESSID	The SSID (Network Name) of the wireless network. (up to 4 SSIDs are supported)
Security	Wireless encryption is enabled for this SSID.
BSSID	The MAC address of this SSID.

4.3 DHCP

This page shows the status of the DHCP server and also allows you to control how the IP addresses are allocated.

Note: Only in Access Point mode.

DHCP Client Table :

This DHCP Client Table shows client IP address assigned by the DHCP Server.

IP Address	MAC Address	Expiration Time
192.168.1.10	00:C0:9F:26:64:EE	Forever

Refresh

You can assign an IP address to the specific MAC address.

☑ **Enable Static DHCP IP**

IP Address	MAC Address
192.168.1.100	80E3A39B703A

Add Reset

Current Static DHCP Table :

NO.	IP Address	MAC Address	Select
1	192.168.1.50	00:24:E8:C7:41:0D	☐

Delete Selected Delete All Reset

Apply Cancel

The DHCP Client Table shows the LAN clients that have been allocated an IP address from the DHCP Server.

DHCP Client Table :

This DHCP Client Table shows client IP address assigned by the DHCP Server.

IP Address	MAC Address	Expiration Time
192.168.1.10	00:C0:9F:26:64:EE	Forever

Refresh

DHCP Client Table	
IP address	The LAN IP address of the client.
MAC address	The MAC address of the client's LAN interface.
Expiration Time	The time that the allocated IP address will expire.
Refresh	Click this button to update the DHCP Client Table.

☑ **Enable Static DHCP IP**

IP Address	MAC Address
192.168.1.100	80E3A39B703A

Add Reset

Current Static DHCP Table :

NO.	IP Address	MAC Address	Select
1	192.168.1.50	00:24:E8:C7:41:0D	☐

Delete Selected Delete All Reset

Apply Cancel

You can also manually specify the IP address that will be allocated to a LAN client by associating the IP address with its MAC address.

Type the IP address you would like to manually assign to a specific MAC address and click **Add** to add the condition to the Static DHCP Table.

4.4 Schedule

This page allows you to setup the schedule times that the Wireless Active feature will be activated / deactivated.

Click **Add** to create a Schedule entry.

☐ **Enabled Schedule Table (up to 10)**

NO.	Description	Service	Schedule	Select
1	schedule 01	Wireless Active	From 11:00 To 12:00--- Mon, Wed	☐

Add | Edit | Delete Selected | Delete All

Apply | Cancel

Schedule Description :	schedule 01
Service :	☑ Wireless Active
Days :	☐ Every Day ☑ Mon ☐ Tue ☑ Wed ☐ Thu ☐ Fri ☐ Sat ☐ Sun
Time of day :	☐ All Day (use 24-hour clock) From 11 : 0 To 12 : 0

Apply | Cancel

Schedule

Schedule Description	Assign a name to the schedule.
Service	The service provides for the schedule.
Days	Define the Days to activate or deactivate the schedule.
Time of day	Define the Time of day to activate or deactivated the schedule. Please use 24-hour clock format.

4.5 Event Log

This page displays the system log of the device. When powered down or rebooted, the log will be cleared.

View the system operation information.

```
day  1 00:00:07 [SYSTEM]: WLAN, start LLTD
day  1 00:00:06 [SYSTEM]: TELNETD, start Telnet-cli Server
day  1 00:00:06 [SYSTEM]: HTTPS, start
day  1 00:00:06 [SYSTEM]: HTTP, start
day  1 00:00:05 [SYSTEM]: UPnP, Start
day  1 00:00:05 [SYSTEM]: SNMP, start SNMP server
day  1 00:00:05 [SYSTEM]: SCHEDULE, Wireless Radio On
day  1 00:00:04 [SYSTEM]: NTP, start NTP Client
day  1 00:00:04 [SYSTEM]: DHCP, DHCP Server Stoping
day  1 00:00:03 [SYSTEM]: WLAN[2.4G], Channel = 11
day  1 00:00:03 [SYSTEM]: LAN, IP address=192.168.1.1
day  1 00:00:03 [SYSTEM]: LAN, start
day  1 00:00:01 [SYSTEM]: BR, start
day  1 00:00:01 [SYSTEM]: SYS, Application Version: 1.0.0
day  1 00:00:01 [SYSTEM]: Start Log Message Service!
```

Save Clear Refresh

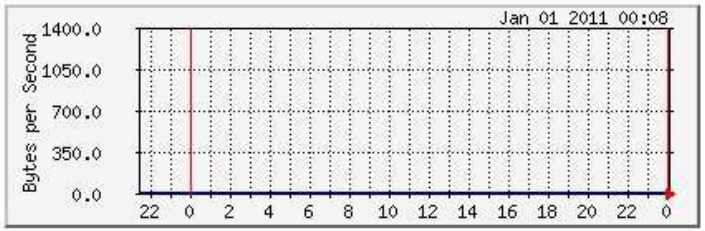
Event Log	
Save	Save the log to a file.
Clear	Clear the log.
Refresh	Update the log.

4.6 Monitor

This page shows a histogram of the Ethernet and Wireless LAN traffic. Click on [**Detail**] to get the detail information.

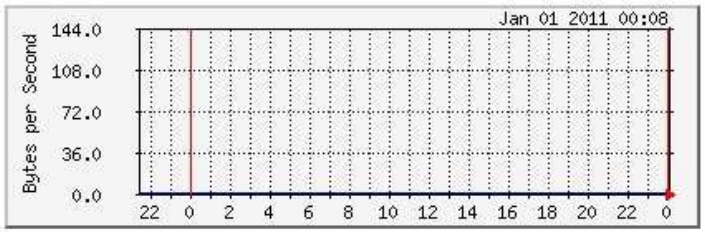
Ethernet Daily Graph (5 Minute Average)

Detail



	Maximum	Average	Current
RX	293 B/sec	293 B/sec	293 B/sec
TX	1365 B/sec	1365 B/sec	1365 B/sec

WLAN Daily Graph (5 Minute Average)



	Maximum	Average	Current
RX	0 B/sec	0 B/sec	0 B/sec
TX	144 B/sec	144 B/sec	144 B/sec

5 Wireless

5.1 Status

This page shows the current status of the device's Wireless settings.

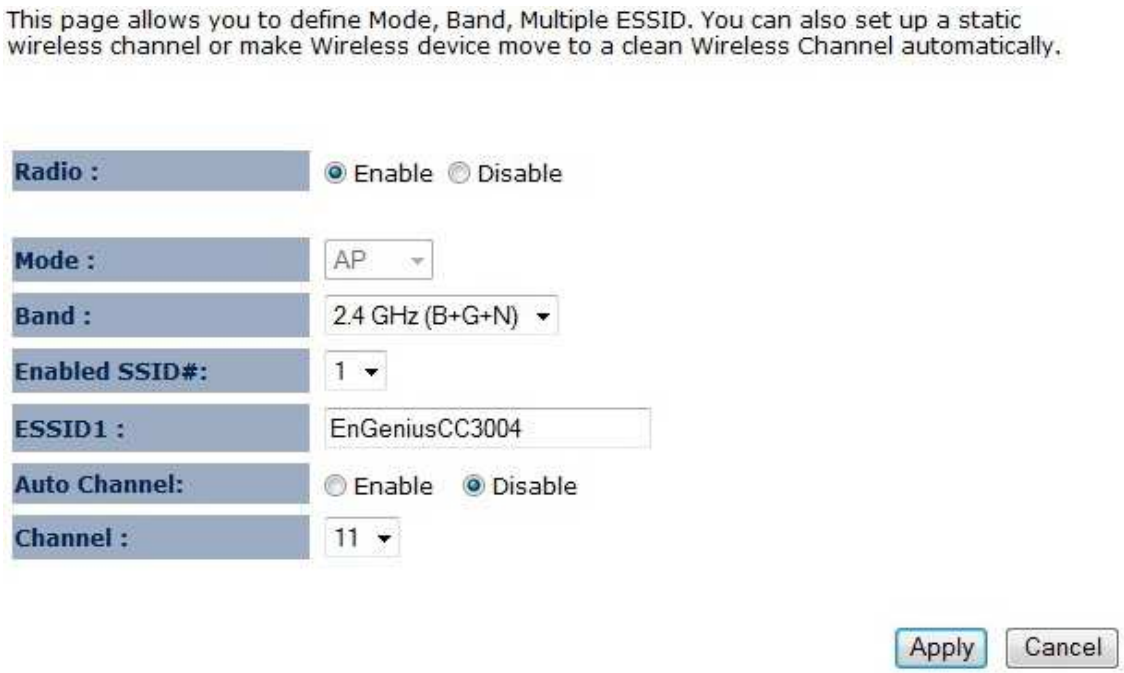
View the current wireless connection status and related information.

WLAN Settings	
Channel	11
SSID_1	
ESSID	EnGeniusCC3004
Security	Disable
BSSID	00:AA:BB:CC:30:04

WLAN Settings	
Channel	The wireless channel in use.
ESSID	The SSID (Network Name) of the wireless network. (up to 4 SSIDs are supported)
Security	Wireless encryption is enabled for this SSID.
BSSID	The MAC address of this SSID.

5.2 Basic

This page shows the current status of the device's Wireless settings.



Basic	
Radio	Enable or Disable the device's wireless signal.
Mode	Select between Access Point or Wireless Distribution System (WDS) modes.
Band	Select the types of wireless clients that the device will accept.
Enable SSID#	Select the number of SSID's (Wireless Network names) you would like.

	You can create up to 4 separate wireless networks.
SSID#	Enter the name of your wireless network. You can use up to 32 characters.
Auto Channel	When enabled, the device will scan the wireless signals around your area and select the channel with the least interference.
Channel	Manually select which channel the wireless signal will use.
Check Channel Time	When Auto Channel is Enabled, you can specify the period of the device will scan the wireless signals around your area.

Wireless Distribution System (WDS)

Using WDS to connect Access Point wirelessly, and in doing so extend a wired infrastructure to locations where cabling is not possible or inefficient to implement.

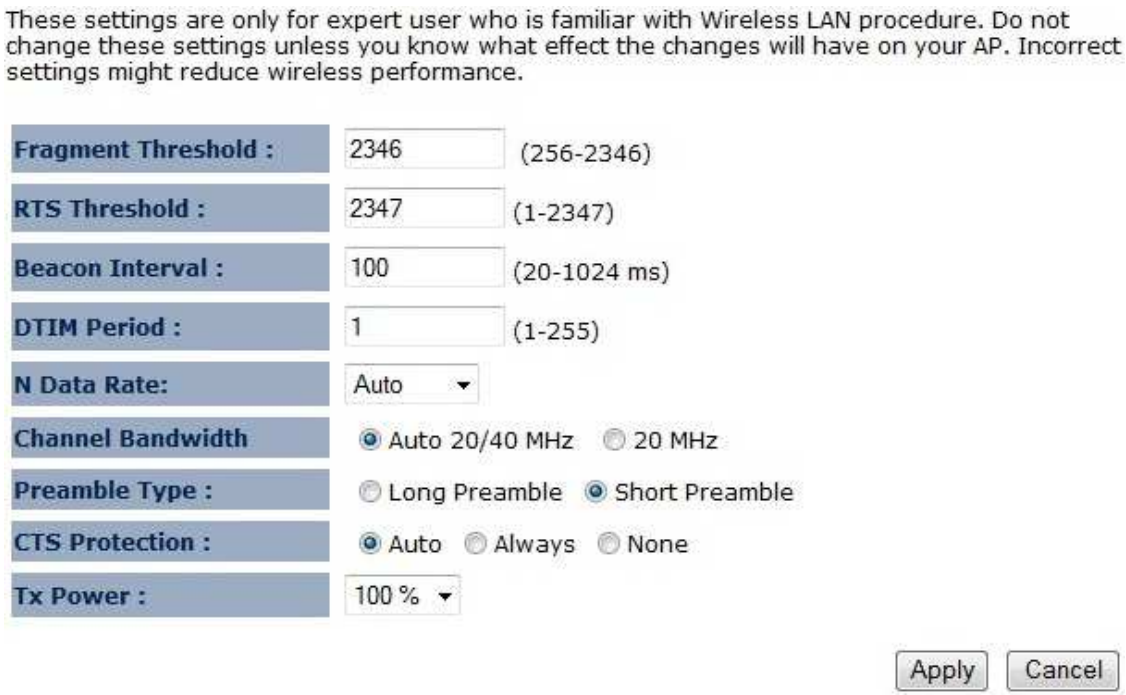
Note that compatibility between different brands and models is not guaranteed. It is recommended that the WDS network be created using the same models for maximum compatibility.

Also note that 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.

5.3 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.



Advanced (Access Point / WDS AP mode)	
Fragment Threshold	Specifies the size of the packet per fragment. This function can reduce the chance of packet collision. However when this value is set too low, there will be increased overheads resulting in poor performance.
RTS Threshold	When the packet size is smaller than the RTS Threshold, then the packet will be sent without RTS/CTS handshake which may result in incorrect transmission.

Beacon Interval	The time interval that the device broadcasts a beacon. This beacon is used to synchronize all wireless clients on the network.
DTIM Period	A Delivery Traffic Indication Message informs all wireless clients that the access point will be sending Multi-casted data.
N Data Rate	You can limit the transfer rates between the device and wireless clients. Each Modulation Coding Scheme (MCS) refers to a specific transfer speed.
Channel Bandwidth	Set whether each channel uses 20 or 40Mhz. To achieve 11n speeds, 40Mhz channels must be used.
Preamble Type	A preamble is a message that helps access points synchronize with the client. Long Preamble is standard based so increases compatibility. Short Preamble is non-standard, so it decreases compatibility but increases performance.
Tx Power	Set the power output of the wireless signal.

These settings are only for expert user who is familiar with Wireless LAN procedure. Do not change these settings unless you know what effect the changes will have on your AP. Incorrect settings might reduce wireless performance.

Fragment Threshold :	2346 (256-2346)
RTS Threshold :	2347 (1-2347)
N Data Rate:	Auto
Channel Bandwidth	Auto 20/40 MHz 20 MHz
Preamble Type :	Long Preamble Short Preamble
CTS Protection :	Auto Always None
Tx Power :	100 %

Apply Cancel

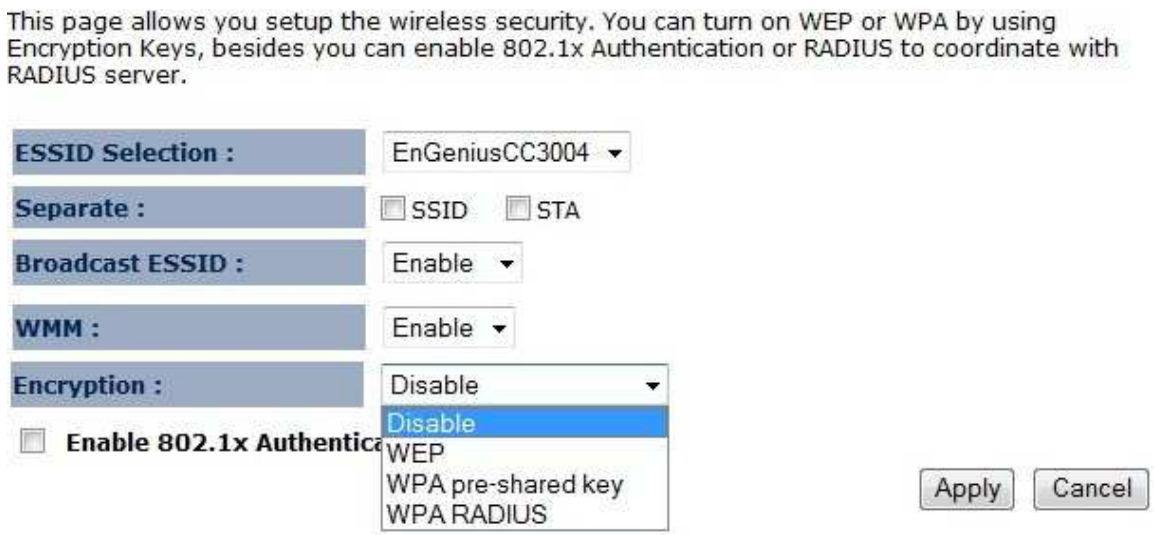
Advanced (WDS Bridge mode)	
Fragment Threshold	Specifies the size of the packet per fragment. This function can reduce the chance of packet collision. However when this value is set too low, there will be increased overheads resulting in poor performance.
RTS Threshold	When the packet size is smaller than the RTS Threshold, then the packet will be sent without RTS/CTS handshake which may result in incorrect transmission.
N Data Rate	You can limit the transfer rates between the device and wireless clients. Each Modulation Coding Scheme (MCS) refers to a specific transfer speed.
Channel Bandwidth	Set whether each channel uses 20 or 40Mhz. To achieve 11n speeds, 40Mhz channels must be used.
Preamble Type	A preamble is a message that helps access points synchronize with the client. Long Preamble is standard based so increases compatibility. Short Preamble is non-standard, so it decreases compatibility but increases performance.

Tx Power	Set the power output of the wireless signal.

5.4 Security

This page allows you to set the wireless security settings.

Note: Only in Access Point and WDS AP mode.



Security (Access Point / WDS AP mode)	
SSID Selection	Select the SSID that the security settings will apply to.
Separate	Tick the box in SSID or STA to Enable Separate feature. Separate prevents communication and data sharing between wireless stations associated with same SSID or different SSID.
Broadcast SSID	If Disabled, then the device will not be broadcasting the SSID. Therefore it will be invisible to wireless clients.
WMM	Wi-Fi Multi-Media is a Quality of Service protocol which prioritizes traffic in the order according to voice, video, best effort, and background.

	Note that in certain situations, WMM needs to be enabled to achieve 11n transfer speeds.
Encryption	The encryption method to be applied. You can choose from WEP, WPA pre-shared key or WPA RADIUS. • **Disabled** - no data encryption is used. • **WEP** - data is encrypted using the WEP standard. • **WPA-PSK** - data is encrypted using the WPA-PSK standard. This is a later standard than WEP, and provides much better security than WEP. If all your Wireless stations support WPA-PSK, you should use WPA-PSK rather than WEP. • **WPA2-PSK** - This is a further development of WPA-PSK, and offers even greater security, using the AES (Advanced Encryption Standard) method of encryption. • **WPA-RADIUS** - This version of WPA requires a Radius Server on your LAN to provide the client authentication according to the 802.1x standard. Data transmissions are encrypted using the WPA standard. If this option is selected: • This Access Point must have a "client login" on the Radius Server. • Each user must have a "user login" on the Radius Server. • Each user's wireless client must support 802.1x and provide the login data when required. • All data transmission is encrypted using the WPA standard. Keys are automatically generated, so no key input is required.

IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this Access Point before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates users by IEEE 802.1x, but it does not encrypt the data during communication.

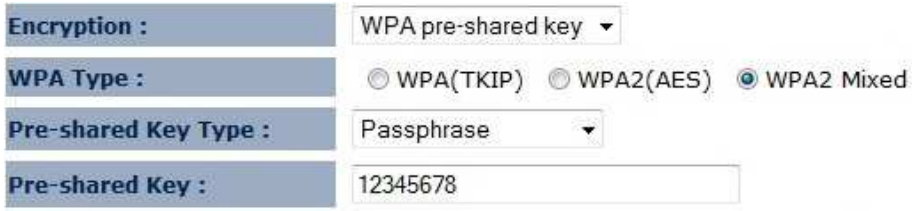
802.1x Authentication	
RADIUS Server IP Address	The IP Address of the RADIUS Server
RADIUS Server port	The port number of the RADIUS Server.
RADIUS Server password	The RADIUS Server's password.

WEP Encryption:

Encryption :	WEP
Authentication Type :	Open System Shared Key Auto
Key Length :	64-bit
Key Type :	Hex (10 characters)
Default Key :	Key 1
Encryption Key 1 :	1234567890
Encryption Key 2 :	
Encryption Key 3 :	
Encryption Key 4 :	

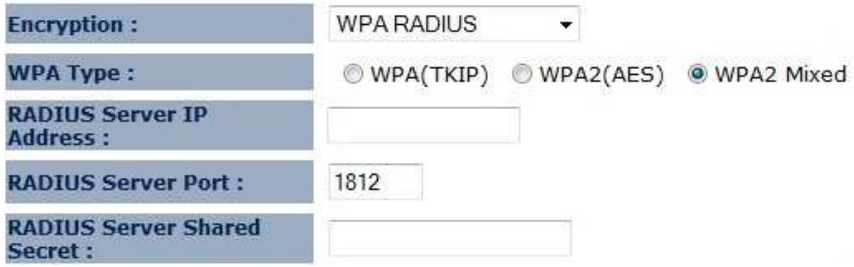
WEP Encryption	
Authentication Type	Please ensure that your wireless clients use the same authentication type.
Key type	**ASCII**: regular text (recommended) **HEX**: for advanced users
Key Length	Select the desired option, and ensure the wireless clients use the same setting. • **64 Bit** - data is encrypted, using the default key, before being transmitted. You must enter at least the default key. For 64 Bit Encryption, the key size is 10 chars in HEX (0~9 and A~F). • **128 Bit** - data is encrypted, using the default key, before being transmitted. You must enter at least the default key. For 128 Bit Encryption, the key size is 26 chars in HEX (0~9 and A~F).
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 Pre-Shared Key Encryption:



WPA Pre-Shared Key Encryption	
Authentication Type	Please ensure that your wireless clients use the same authentication type.
WPA type	Select the WPA encryption you would like. Please ensure that your wireless clients use the same settings.
Pre-shared Key Type	Select whether you would like to enter the Key in HEX or Passphrase format.
Pre-shared Key	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.

WPA RADIUS Encryption:



WPA RADIUS Encryption	
WPA type	Select the WPA encryption you would like. Please ensure that your wireless clients use the same settings.
RADIUS Server IP address	Enter the IP address of the RADIUS Server
RADIUS Server Port	Enter the port number used for connections to the RADIUS server.
RADIUS Server password	Enter the password required to connect to the RADIUS server.

5.5 Filter

This page allows you to create filters to control which wireless clients can connect to this device by only allowing the MAC addresses entered into the Filtering Table.

Note: Only in Access Point and WDS AP mode.

Using MAC Address Filtering could prevent unauthorized MAC Address to associate with the AP.

☑ **Enable Wireless MAC Filtering**

Description	MAC Address
rule02	80A49E837BA2

Add Reset

Only the following MAC Addresses can use network:

NO.	Description	MAC Address	Select
1	rule01	00:21:6A:78:8E:70	☐

Delete Selected Delete All Reset

Apply Cancel

Wireless Filter (Access Point / WDS AP mode)	
Enable Wireless Access Control	Tick the box to Enable Wireless Access Control. When Enabled, only wireless clients on the Filtering Table will be allowed.
Description	Enter a name or description for this entry.

MAC address	Enter the MAC address of the wireless client that you wish to allow connection.
Add	Click this button to add the entry.
Reset	Click this button if you have made a mistake and want to reset the MAC address and Description fields.
MAC Address Filtering Table	
Only clients listed in this table will be allowed access to the wireless network.	
Delete Selected	Delete the selected entries.
Delete All	Delete all entries
Reset	Un-tick all selected entries.

5.6 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.

Wi-Fi Protected Setup (WPS)	
WPS	Tick to Enable the WPS feature.
Wi-Fi Protected Setup Information	
WPS Current Status	Shows whether the WPS function is **Configured** or **Un-configured**. Configured means that WPS has been used to authorize connection between the device and wireless clients.
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.

5.7 Client List

This page shows the wireless clients that are connected to the device.

Note: Only in Access Point and WDS AP mode.

WLAN Client Table :

This WLAN Client Table shows client MAC address associate to this device.

Interface	MAC Address	Rx	Tx	Signal(%)	Connected Time	Idle Time
EnGeniusCC3004	00:02:6F:11:AC:93	1852677	1832060	44	10 min 27 secs	0 secs
EnGeniusCC3004	00:02:6F:47:65:CA	1519236	1493659	36	6 min 50 secs	0 secs

Refresh

5.8 VLAN

This page allows you to configure the VLAN

Note: Only in Access Point and WDS AP mode.

A virtual LAN, commonly known as a VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the same wire, regardless of their physical location.

Virtual LAN :	Enable Disable
SSID 1 Tag:	100 (1~4094)
LAN VLAN MGMT :	Enable Disable
MGMT Tag:	500 (1~4094)

Apply Cancel

VLAN	
Virtual LAN	Choose to Enable or Disable the VLAN feature.
SSID# Tag	Specify the VLAN tag for each SSID.
LAN VLAN MGMT	Choose to Enable or Disable the LAN VLAN MGMT feature.
MGMT Tag	Specify the VLAN tag for LAN.

6 Network

6.1 Status

This page shows the current status of the device's LAN connection.

LAN Settings	
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway IP Address	---
MAC Address	00:AA:BB:CC:30:04

6.2 LAN

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

LAN IP	
Bridge Type	Select Static IP or Dynamic IP from the drop-down list. If you select Static IP, you will be required to specify an IP address and subnet mask. If Dynamic IP is selected, then the IP address is received automatically from the external DHCP server.
IP address	The LAN IP Address of this device.
IP Subnet Mask	The LAN Subnet Mask of this device.
Default Gateway	The Default Gateway of this device. Leave it blank if you are unsure of this setting.
DNS Type	Select Static or Dynamic from the drop-down list.
First / Second DNS Address	The first / second DNS address for this device.

DHCP Server feature is only in Access Point mode.

DHCP Server

DHCP Server :	Disabled
Lease Time :	Forever
Start IP :	192.168.1.100
End IP :	192.168.1.200
Domain Name :	eap300
First DNS Address :	
Second DNS Address :	

DHCP Server (Access Point mode)	
DHCP Server	Enable or disable DHCP feature. The DHCP Server automatically allocates IP addresses to your LAN device. Disabled as default.
Lease Time	The duration of the DHCP server allocates each IP address to a LAN device.
Start / End IP	The range of IP addresses of the DHCP server will allocate to LAN device.
Domain name	The domain name for this LAN network.
First / Second DNS Address	The first / second DNS address for this LAN network.

6.3 Spanning Tree

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

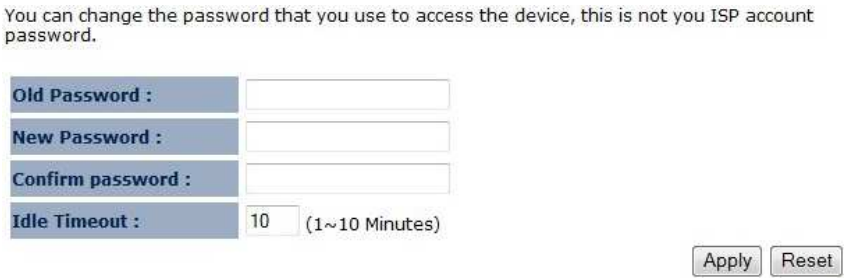
Spanning Tree Settings

Spanning Tree Status :	○ Enable ◉ Disable
Bridge Hello Time :	2 seconds (1-10)
Bridge Max Age :	20 seconds (6-40)
Bridge Forward Delay :	15 seconds (4-30)
Bridge Priority :	32768 (0-65535)

7 Management

7.1 Admin

This page allows you to change the system password and to configure remote management. By default, the password is: **admin**. Password can contain 0 to 12 alphanumeric characters and are case sensitive.



Change Password	
Old Password	Enter the current password.
New Password	Enter your new password.
Confirm Password	Enter your new password again for verification.
Idle Timeout	Enter Administration Page timeout time.

7.2 SNMP

This page allows you to assign the contact details, location, community name and trap settings for 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 a network. Upon receiving these messages, SNMP-compatible devices (called agents) return data stored in their Management Information Bases.

SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

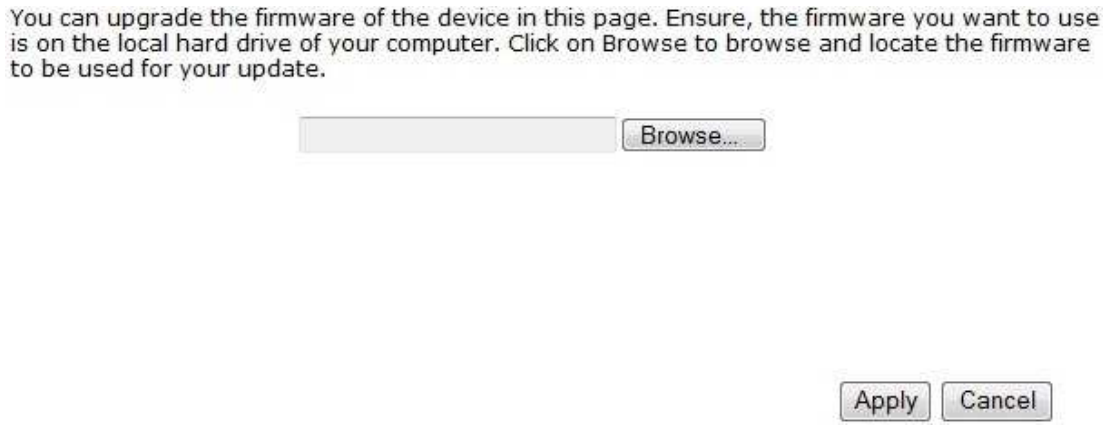
SNMP Active	Disabled
SNMP Version	All
SNMP Manager IP	0.0.0.0
Read Community	public
Set Community	private
System Location	EnGenius Technologies, Inc.
System Contact	SENAO Networks, Inc.
Trap Active	Disabled
Trap Manager IP	192.168.1.100
Trap Community	public

Apply Cancel

SNMP	
SNMP Active	Enable or disable SNMP feature.
SNMP Version	You may select a specific version or select **All** from the drop-down list.
Read Community	Specify the password for access the SNMP community for read only access.
Set Community	Specify the password for access to the SNMP community with read/write access.
System Location	Specify the location of the device.
System Contact	Specify the contact details of the device
Trap	
Trap Active	Enable or disable SNMP trapping feature.
Trap Manager IP	Specify the IP address of the computer that will receive the SNMP traps.
Trap Community	Specify the password for the SNMP trap community.

7.3 Firmware Upgrade

This page allows you to upgrade the device's firmware.



To perform the Firmware Upgrade:

1. Click the [**Browse**] button and navigate to the location of the upgrade file.
2. Select the upgrade file. Its name will appear in the *Upgrade File* field.
3. Click the [**Apply**] 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.

Emergency Upgrade

If you upgrade fail, you may enter Emergency Upgrade WEB page.

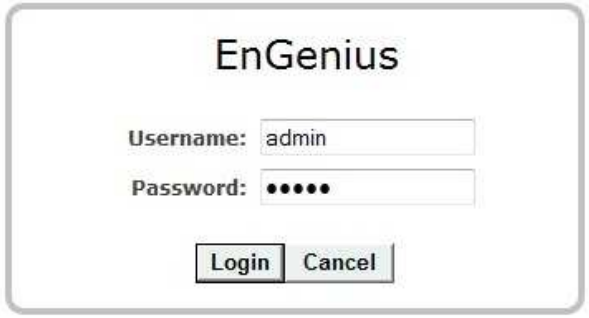
1. Enter IP address: **192.168.99.9** and enter Emergency Upgrade WEB page.

Note: Refer to 2.2 to configure PC/Notebook IP address to 192.168.99.8.

2. Click the [**Browse**] button and navigate to the location of the upgrade file and then click [**Upload**].

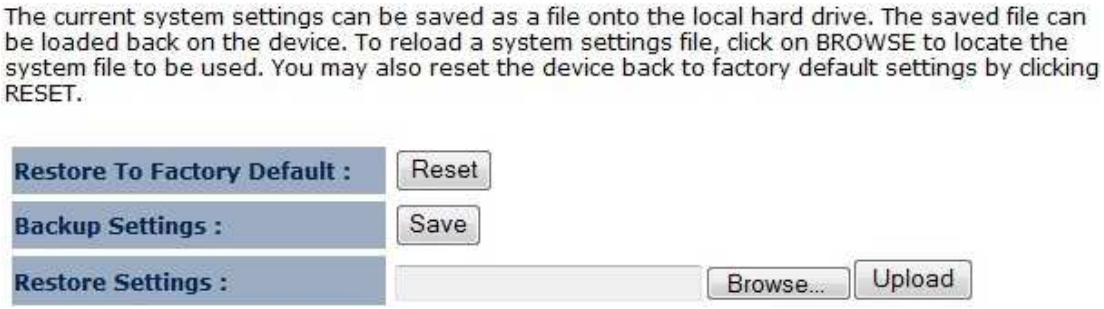
3. Wait for 60 seconds for firmware upgrade and reboot the device.

4. You can access the device again.


EnGenius
Username:
admin
Password:
Login
Cancel

7.4 Configure

This page allows you to save the current device configurations. When you save the configurations, you also can re-load the saved configurations into the device through the [**Restore Settings**]. If extreme problems occur you can use the [**Restore to Factory Defaults**] to set all configurations to its original default settings.



Configure	
Restore to Factory Default	Restores the device to factory default settings.
Backup Settings	Save the current configuration settings to a file.
Restore Settings	Restores a previously saved configuration file. Click **Browse** to select the file. Then **Upload** to load the settings.

7.5 Reset

In some circumstances it may be required to force the device to reboot. Click on [**Apply**] to reboot.

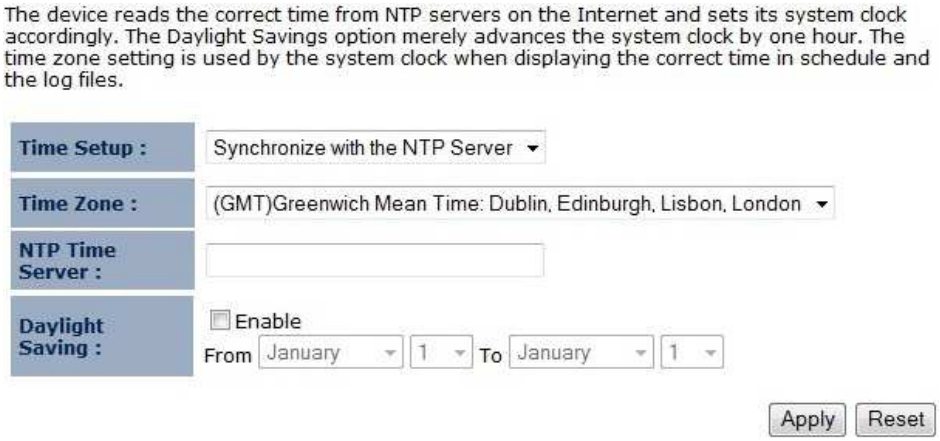
In the event the system stops responding correctly or stops functioning, you can perform a reset. Your settings will not be changed. To perform the reset, click on the APPLY button. You will be asked to confirm your decision. The reset will be completed when the LED Power light stops blinking.

Apply

8 Tools

8.1 Time Setting

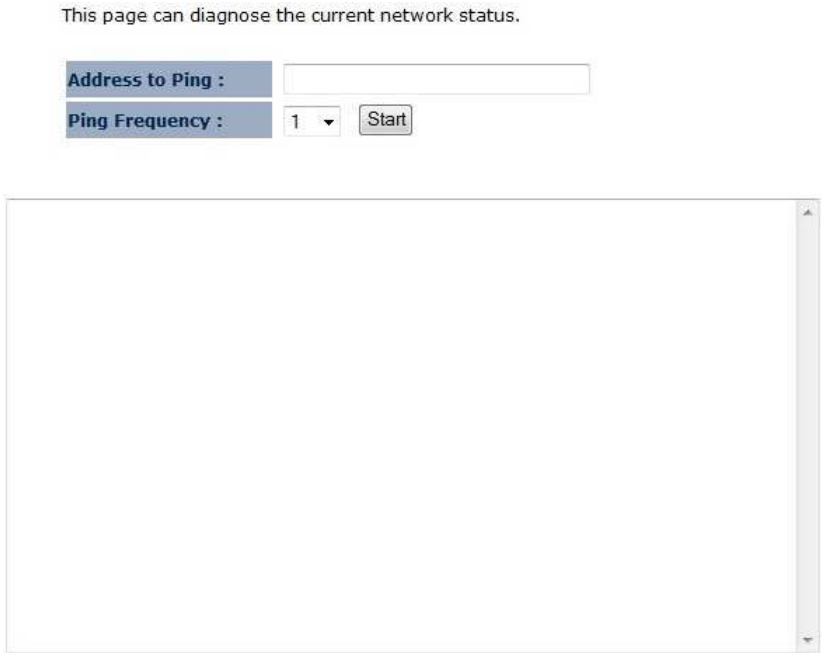
This page allows you to set the system time.



Time	
Time Setup	Select the method you want to set the time.
Time Zone	Select the time zone for your current location.
NTP Time Server	Enter the address of the Network Time Protocol (NTP) Server to automatically synchronize with a server on the Internet.
Daylight Savings	Check whether daylight savings applies to your area.

8.2 Diagnosis

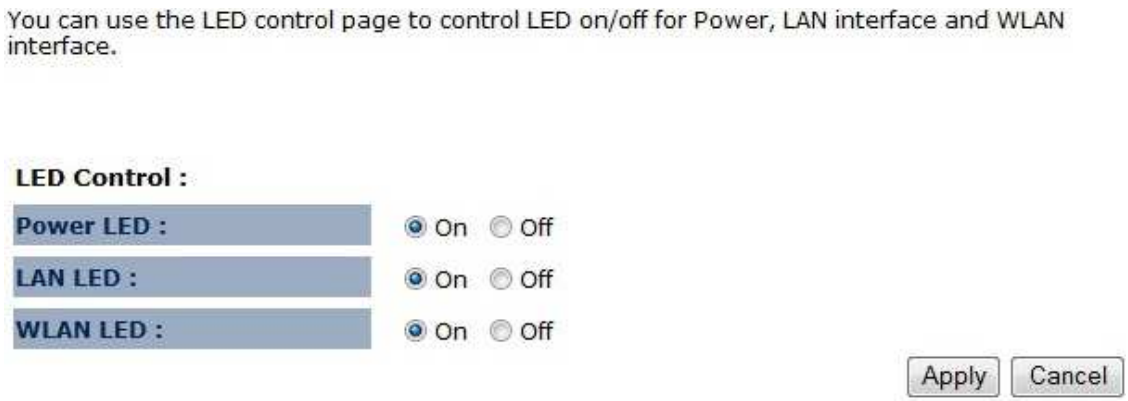
This page allows you to test your network. Type in the address for diagnosis.



Diagnosis	
Address to Ping	Enter the IP address you like to see if a successful connection can be made.
Ping Frequency	Select the frequency for Ping test.
Ping Result	The results of the Ping test.

8.3 LED Control

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



9 Logout

Click on [**Logout**] button to logout.

This page is used to logout this device.

Logout

Appendix A – FCC Interference Statement

Federal Communication Commission 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.

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 B – CE Interference Statement

1.1. 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

CE0560

cs Česky [Czech]	*[Jméno výrobce]* tímto prohlašuje, že tento *[typ zařízení]* je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
da Dansk [Danish]	Undertegnede *[fabrikantens navn]* erklærer herved, at følgende udstyr *[udstyrets typebetegnelse]* overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
de Deutsch [German]	Hiermit erklärt *[Name des Herstellers]*, dass sich das Gerät *[Gerätetyp]* in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
et Eesti [Estonian]	Käesolevaga kinnitab *[tootja nimi = name of manufacturer]* seadme *[seadme tüüp = type of equipment]* vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
en English	Hereby, *[name of manufacturer]*, declares that this *[type of equipment]* is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
es Español [Spanish]	Por medio de la presente *[nombre del fabricante]* declara que el *[clase de equipo]* cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
el Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *[name of manufacturer]* ΔΗΛΩΝΕΙ ΟΤΙ *[type of equipment]* ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
fr Français [French]	Par la présente *[nom du fabricant]* déclare que l'appareil *[type d'appareil]* est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
it Italiano [Italian]	Con la presente *[nome del costruttore]* dichiara che questo *[tipo di apparecchio]* 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.
nl 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.
mt 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.
hu Magyar [Hungarian]	Alulírott, *[gyártó neve]* nyilatkozom, hogy a *[... típus]* megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
pl Polski [Polish]	Niniejszym *[nazwa producenta]* oświadcza, że *[nazwa wyrobu]* jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
pt 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.
sl 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.
fi 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.
sv 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.