



The Neutron Series

User Manual



EWS300AP
version 1.0

EWS Series

Wireless Managed Indoor Access Point

Table of Contents

Chapter 1	5
Key Features	6
Introduction	7
System Requirements	8
Package Contents	8
Applications	9
Technical Specifications	10
Physical Interface	12
Chapter 2	13
Considerations for Wireless Installation	14
Computer Settings	15
Hardware Installation	19
Mounting the Access Point	20
Chapter 3	23
Default Settings	24
Web Configuration	25
Chapter 4	27
Device Status	28
Connections	31
Chapter 5	32
IPv4 Settings	33
IPv6 Settings	34
Spanning Tree Settings	35
Chapter 6	36

2.4GHz SSID Profile.....	37
Wireless Security	38
Wireless MAC Filter	41
Traffic Shaping.....	42
Guest Network	43
Fast Handover	45
Management VLAN Settings.....	46
Chapter 7	47
SNMP Settings.....	48
CLI/SSH Settings.....	50
HTTPS Settings.....	51
Email Alert	52
Date and Time Settings	53
WiFi Scheduler.....	54
Tools.....	56
LED Control.....	59
Device Discovery.....	60
Chapter 8	61
Account Setting.....	62
Firmware Upgrade	63
Backup/Restore	64
System Log	65
Reset.....	66
Logout	67
Appendix	68
Appendix A - FCC Interference Statement	69
Appendix B - IC Interference Statement.....	71

Appendix C - CE Interference Statement..... 72

Chapter 1

Product Overview

Introduction

Key Features

- Deploy and manage with ease using EWS Series Wireless Management Switches.
- Internal Omni-Directional antennas optimized for maximum RF performance.
- Backward compatible with IEEE802.11 a/b/g/n wireless devices.
- Integrated Power over Ethernet (IEEE802.3af) for lowering deploying costs. Can be powered using either the included power adapter or via PoE with PoE 802.3af capable Switches or Injectors.
- SNMP v1/ v2c/v3, MIB I/II supported.
- WEP/WPA/WPA2 wireless encryption.
- IPv4/IPv6 support.
- Effective and flexible bandwidth management.
- Client limiting and fast handover supported.
- Secure Guest Network option available.
- Ideal for audio, video and voice application.
- Stylish low profile design with ceiling mounting kit.

Introduction

This device is an enhanced-powered, long-range wireless access point. It is designed to operate in numerous environments; from large homes, small and medium-sized businesses, multiple-floor offices, hotels, and other venues, to larger enterprise deployments. Its enhanced-powered, long-range characteristics make it a cost-effective alternative to ordinary Access Points that don't have the range and reach to connect to a growing number of wireless users who wish to connect to a large hotspot or business network.

To protect sensitive data during wireless transmissions, the device offers different encryption settings for wireless transmissions, including industry standard WPA and WPA2 encryption. The device also includes MAC address filtering to allow network administrators to offer network access only to known computers and other devices based on their MAC addresses.

Maximum data rates are based on IEEE 802.11 standards. Actual throughput and range may vary depending on many factors including environmental conditions, distance between devices, radio interference in the operating environment, and mix of devices in the network. Features and specifications are subjected to change without prior notice. Trademarks and registered trademarks are the property of their respective owners. For United States of America: Copyright © 2013 EnGenius Technologies, Inc. All rights reserved.

System Requirements

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

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

Package Contents

The package contains the following items (all items must be in package to issue a refund):

- EWS Indoor Access Point
- Power Adapter
- Mounting Bracket
- T-Rail Mounting Kit
- Mounting Screw Set
- Quick Installation Guide

Applications

Wireless LAN (WLAN) 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 WLANs:

- **Difficult-to-Wire Environments:** There are many situations where wires cannot be installed, deployed easily, or cannot be hidden from view. Older buildings, sites with multiple buildings, and/or areas that make the installation of a Ethernet-based LAN impossible, impractical or expensive are sites where WLAN can be a network solution.
- **Temporary Workgroups:** Create temporary workgroups/networks in more open areas within a building; auditoriums, amphitheatres classrooms, ballrooms, arenas, exhibition centers, or temporary offices where one wants either a permanent or temporary Wireless LAN established.
- **The Ability to Access Real-Time Information:** Doctors/Nurses, Point-of-Sale Employees, and/or Warehouse Workers can access real-time information while dealing with patients, serving customers, and/or processing information.
- **Frequently Changing Environments:** Set up networks in environments that change frequently (i.e.: Show Rooms, Exhibits, etc.).
- **Small Office and Home Office (SOHO) Networks:** SOHO users require a cost-effective, easy, and quick installation of a small network.
- **Training/Educational Facilities:** Training sites at corporations or students at universities use wireless connectivity to exchange information between peers and easily access information for learning purposes.

Technical Specifications

Radio Specification

Operation Frequency:

- 2.4GHz: 802.11b/g/n with max data rate up to 300Mbps

Radio Chains / Spatial Streams:

- 2 x 2 / 2

Supported Radio Technology:

- 802.11b: direct-sequence spread-spectrum (DSSS)
- 802.11g/n: orthogonal frequency-division multiplexing (OFDM)

Channelization:

- 802.11n with 20/40 MHz channel width
- 802.11b/g with 20 MHz channel width

Supported Modulation:

- 802.11b: BPSK, QPSK, CCK
- 802.11g/n: BPSK, QPSK, 16-QAM, 64-QAM

Supported data rates (Mbps):

- 802.11b: 1, 2, 5.5, 11
- 802.11g: 6, 9, 12, 18, 24, 36, 48, 54
- 802.11n: 6.5 to 300 (MCS0 to MCS15)

Physical & Environment

Power Source:

- DC Input: 12 VDC/1A
- PoE: compatible with 802.3af

Internal High Gain Antenna:

- 2 x 5dBi 2.4GHz antennas

Interface:

- 1 x 10/100/1000Mbps Ethernet Port with 802.3af PoE

- 1 x DC power connector

- 1 x Reset button

Dimensions (W x D x H):

- 129 x 129 x 43.5mm

Mounting:

- Ceiling mount or wall mount

Environment:

- Operating temperature: 0°C~50°C
- Operating humidity: 0%~90% typical
- Storage temperature: -20°C~60°C

Wireless

Operating Mode:

- AP Mode

Auto Channel Selection:

- Setting varies by regulatory domains

SSIDs:

- Supports up to 8 SSIDs

VLAN Tag / VLAN Pass-through

Wireless Client List

Guest Network:

- Allocates a separate network segment for guest access within the same WLAN

QoS:

- Supports 802.11e/WMM

Mobility:

- PMKSA support for fast roaming

Security:

- WEP encryption: 64/128/152-bit
- WPA/WPA2 Enterprise/PSK
- Hidden SSID
- MAC address filtering (up to 50 MAC)
- Client isolation

Management

Deployment Options

- Standalone Mode
- Managed Mode (by Neutron Switch)

Configuration

- Web interface (HTTP)
- SNMP v1/v2c/v3 with MIB I/II and private MIB
- CLI (Telnet)

Firmware Upgrade

- Web interface or CLI (FTP/HTTP)

Backup / Restore Settings

- Revert to factory default settings

Schedule Reboot:

- Specifies interval to reboot system periodically

E-mail Alert / Syslog Notification

Physical Interface



1. Reset Button: Press and hold for over 10 seconds to reset to factory default settings.
2. LED Indicators: LED lights for WLAN 2.4GHz, LAN, and Power
3. LAN Port (802.3af PoE): Ethernet port for RJ-45 cable.
4. Power Connector: 12V DC IN for Power Adapter.

Chapter 2

Before You Begin

Before You Begin

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

Considerations for Wireless Installation

The operating distance of all wireless devices can often not be pre-determined due to a number of unknown obstacles in the environment in which the device is deployed. Obstacles such as the number, thickness, and location of walls, ceilings, or other objects that the Access Point's wireless signals must pass through can weaken the signal. Here are some key guidelines for allowing the Access Point to have an optimal wireless range during setup.

- Keep the number of walls and/or ceilings between the Access Point and other network devices to a minimum. Each wall and/or ceiling can reduce the signal strength, resulting in a lower overall 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 Access Point. 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 your other electrical devices and/or appliances that generate RF noise can also diminish the Access Point's signal strength. The most common types of devices are microwaves or cordless phones.

Computer Settings

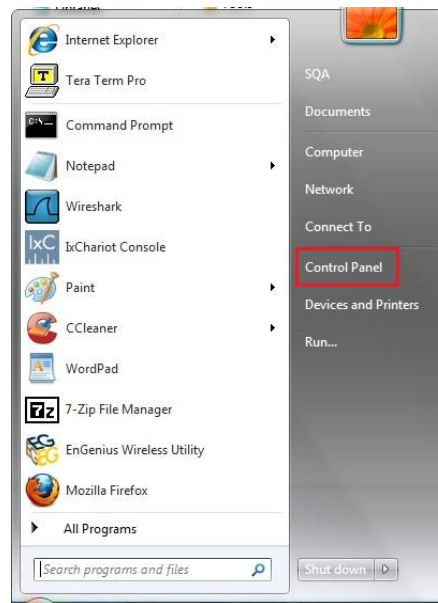
Windows XP/Windows 7

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

1. Click the **Start** button and open the **Control Panel**.



Windows XP



Windows 7

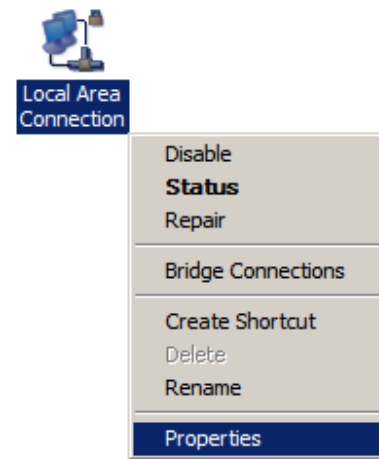
2a. In **Windows XP**, click on Network Connections.



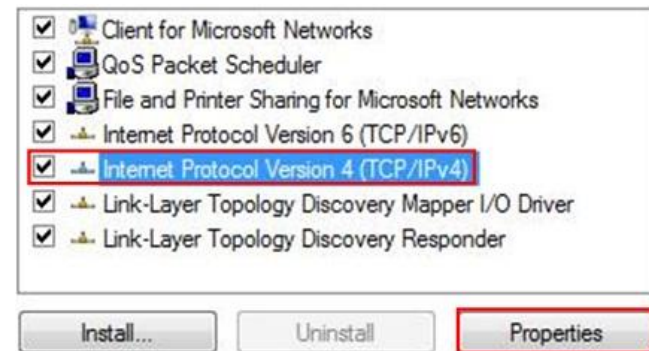
2b. In **Windows 7**, click **View network status and tasks** in the **Network and Internet** section, then select **Change adapter settings**.



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



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



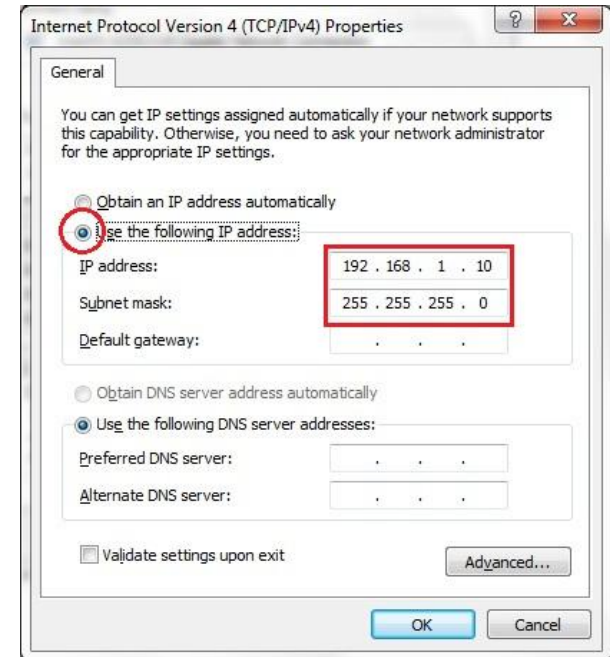
5. Select **Use the following IP address** and enter an IP address that is different from the Access Point and Subnet mask, then click **OK**.

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

For example: Access Point IP address: 192.168.1.1

PC IP address: 192.168.1.2 - 192.168.1.255

PC Subnet mask: 255.255.255.0

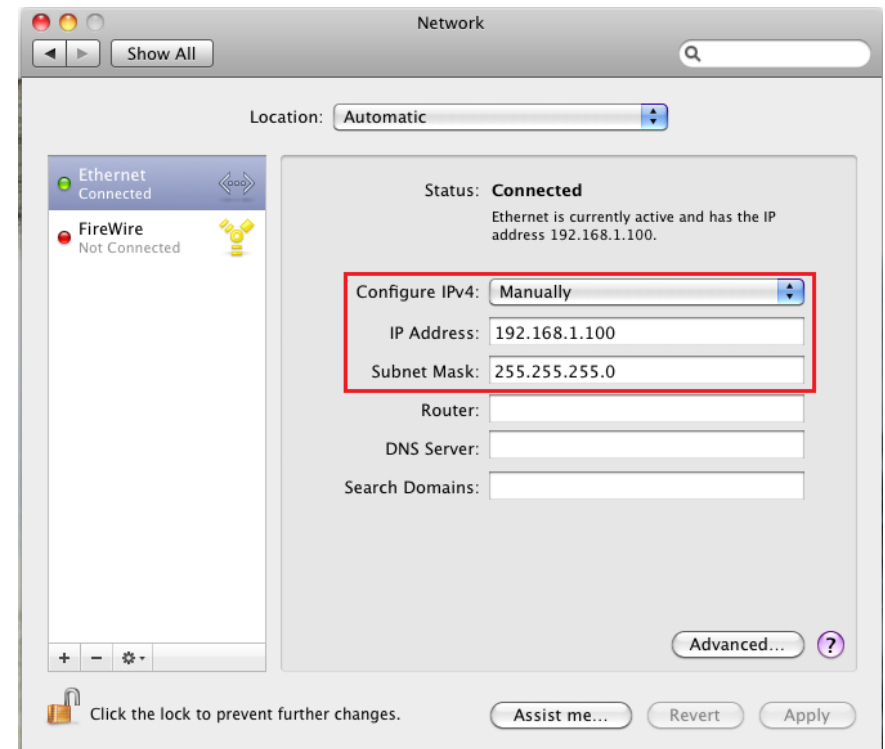


Apple Mac OS X

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

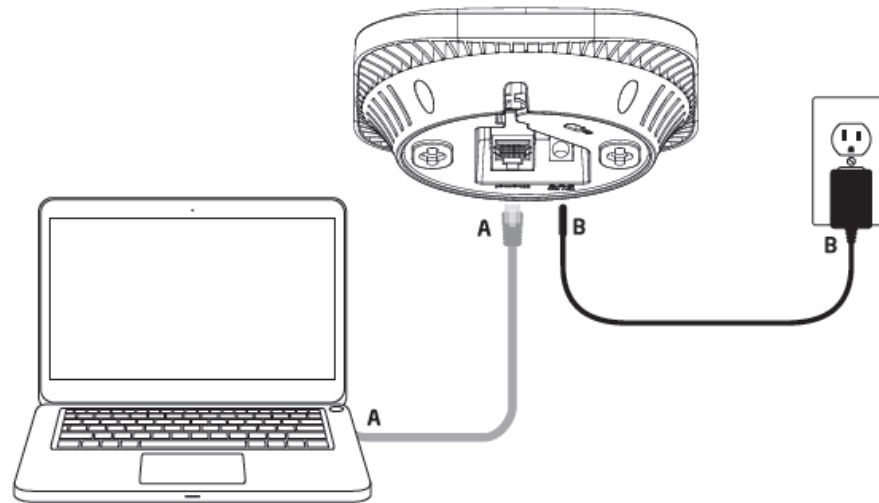


3. Highlight **Ethernet**.
4. In **Configure IPv4**, select **Manually**.
5. Enter an IP address that is different from the Access Point and Subnet mask, then click **OK**.
Note: Ensure that the IP address and Subnet mask are on the same subnet as the device.
For example: Access Point IP address: 192.168.1.1
PC IP address: 192.168.1.2 - 192.168.1.255
PC Subnet mask: 255.255.255.0
6. Click **Apply** when finished.



Hardware Installation

1. Ensure that the computer in use has an Ethernet Controller port (RJ-45 Ethernet 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 Access Point and the other end to the RJ-45 port of the computer. Ensure that the cable is securely connected to both the Access Point and the computer.
3. Connect the Power Adapter DC connector to the DC-IN port of the Access Point and the Power Adapter to an available electrical outlet. Once both connections are secure, verify the following:
 - a) Ensure that the **POWER** LED is on.
 - b) Ensure that the **2.4 GHz** LED is on.
 - c) Ensure that the **LAN** (Computer/ Access Point Connection) light is on.
 - d) Once all three lights are on, proceed to set up the Access Point using the computer.



Mounting the Access Point

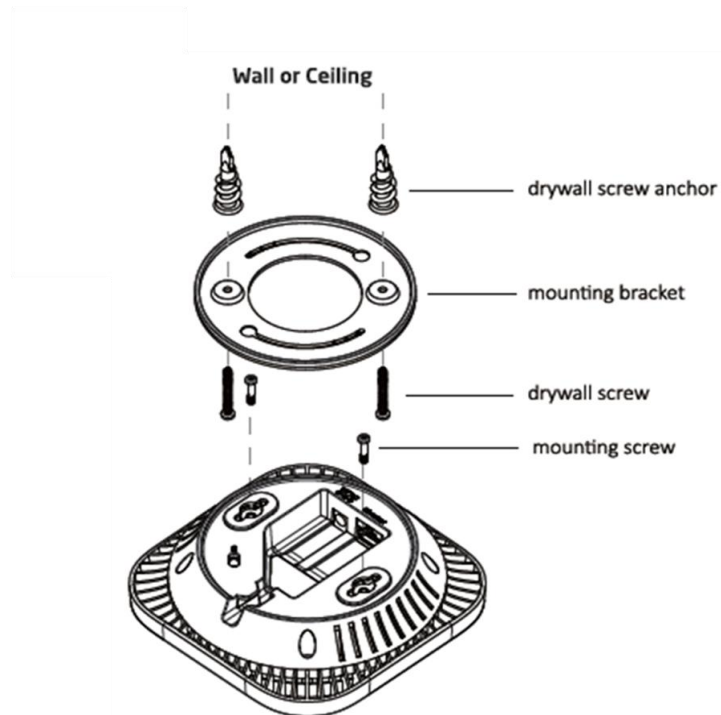
Using the provided hardware, the Access Point can be attached to a ceiling or wall.

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

1. Attach the mounting bracket to the wall or ceiling using the provided wall/ceiling mounting hardware kit.
2. Insert the provided short screws into the bottom cover of the Access Point.

Leave enough of the screws exposed to ensure that the unit can be attached to the mounting bracket.

If extra space is required, use the provided spacers and long screws from the T-Rail mounting hardware kit to increase the space between the unit and the mounting bracket.

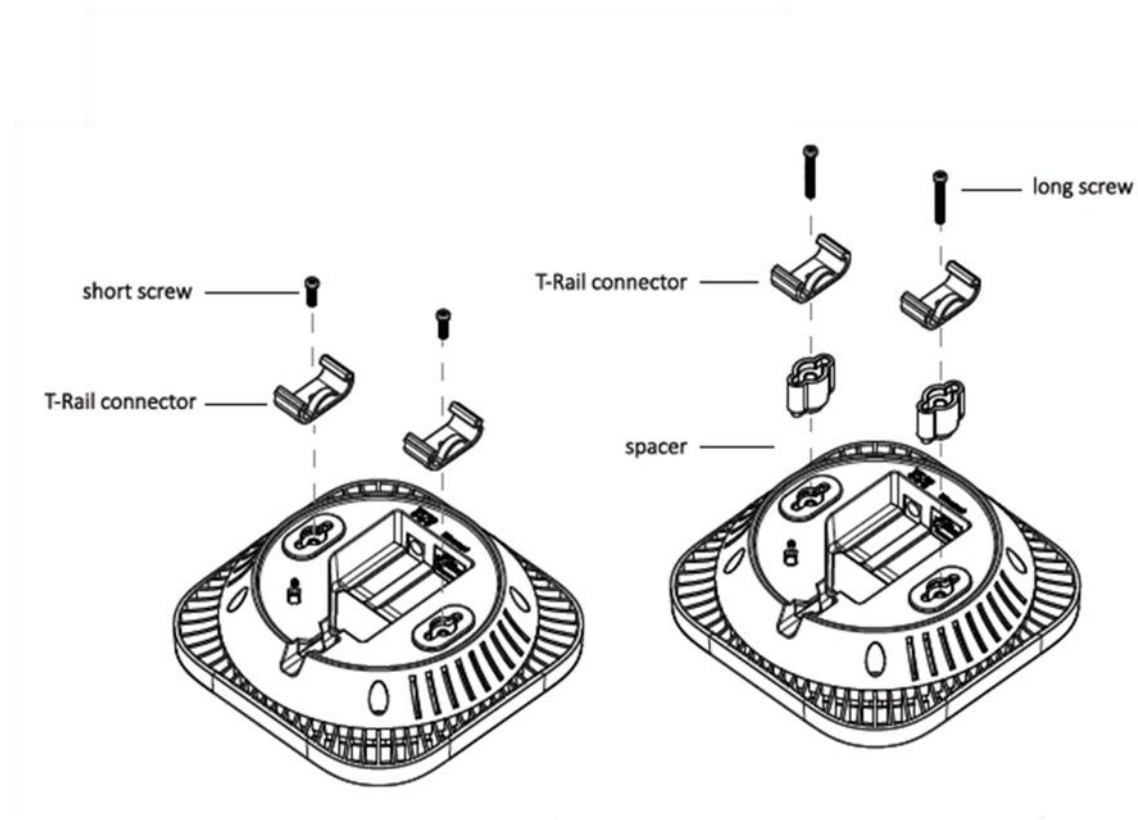


4. Mount the Access Point on the mounting bracket by rotating the unit clockwise about 90 degrees to secure it in place.

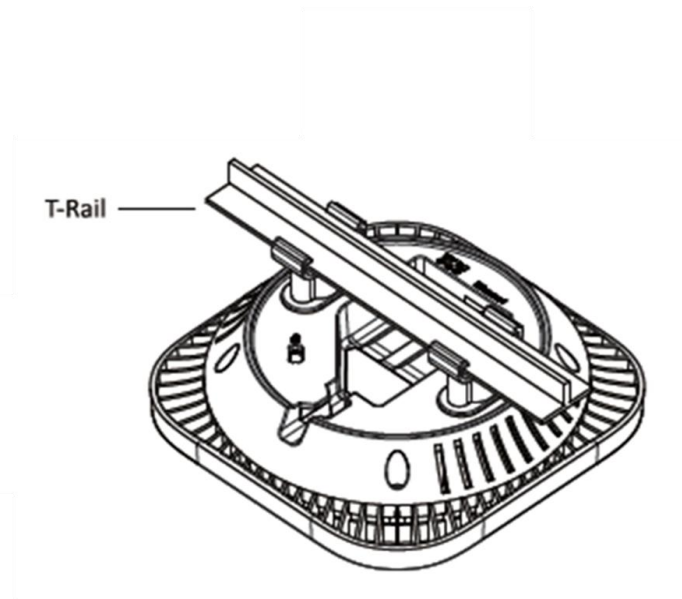
Attaching the Access Point to a ceiling using the provided T-Rail connectors:

1. Attach the T-Rail connectors to the bottom cover of the Access Point using the provided short screws.

Note: Two sizes of T-Rail connectors are included in the mounting hardware kit: 15/16in (2.38cm) and 9/16in (1.43cm). If extra space is required to accommodate drop ceiling tiles, use the provided spacers and long screws.



2. Line up the connected T-Rail connectors with an appropriately sized rail and press the unit onto the rail until it snaps into place.



Note: To protect your Access Point, use the Kensington Security Slot to attach a cable lock (cable lock is not included).

Chapter 3

Configuring Your Access Point

Configuring Your Access Point

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

Default Settings

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

IP Address	192.168.1.1
Username/Password	admin/admin

Web Configuration

1. 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.

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



3. If successful, you will be logged in and see the Access Point User Interface.

Overview

Device Status

Connections

Network

Basic

Wireless

Management

Advanced

Time Zone

WiFi Scheduler

Tools

System Manager

Account

Firmware

Device Information

Device Name	EWS300AP
MAC Address	
LAN	88:DC:96:30:40:17
Wireless LAN - 2.4GHz	88:DC:96:30:40:18
Current Local Time	Wed Jan 28 11:14:27 UTC 2015
Firmware Version	2.0.10 + 1.3.5
Management VLAN ID	Untagged

LAN Information - IPv4

IP Address	192.168.1.1
Subnet Mask	255.255.255.0

Chapter 4

Overview

Overview

The **Overview** section contains the following options:

- Device Status
- Connections

The following sections describe these options.

Device Status

Clicking the **Device Status** link under the **Overview** menu shows the status information about the current operating mode.

- The **Device Information** section shows general system information such as Device Name, MAC address, Current Time, Firmware Version, and Management VLAN ID

Device Information

Device Name	EWS300AP
MAC Address	
LAN	88:DC:96:30:40:17
Wireless LAN - 2.4GHz	88:DC:96:30:40:18
Current Local Time	Wed Jan 28 11:14:27 UTC 2015
Firmware Version	2.0.10 + 1.3.5
Management VLAN ID	Untagged

- The **LAN Information** section shows the Local Area Network settings such as the LAN IP Address, Subnet mask, Gateway, DNS Address, DHCP Client, and STP status.

LAN Information - IPv4

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	192.168.1.1
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
DHCP Client	Disable
Spanning Tree Protocol (STP)	Disable

LAN Information - IPv6

IP Address	N/A
Link-Local Address	fe80::8adc:96ff:fe30:4017
Gateway	N/A
Primary DNS	N/A
Secondary DNS	N/A

- The **Wireless LAN Information 2.4 GHz** section shows wireless information such as Operating Mode, Frequency, and Channel. Since the Access Point supports multiple-SSIDs, information about each SSID and security settings are displayed.

Wireless LAN Information - 2.4GHz

Operation Mode	Access Point				
Wireless Mode	802.11 B/G/N				
Channel Bandwidth	20-40MHz				
Channel	2.437 GHz (Channel 6)				
Profile	SSID	Security	VID	802.1Q	
#1	EnGenius304018_1-2.4GHz	None	1	Disable	
#2	EnGenius304018_2-2.4GHz	None	2	Disable	
#3	EnGenius304018_3-2.4GHz	None	3	Disable	
#4	EnGenius304018_4-2.4GHz	None	4	Disable	
#5	EnGenius304018_5-2.4GHz	None	5	Disable	
#6	EnGenius304018_6-2.4GHz	None	6	Disable	
#7	EnGenius304018_7-2.4GHz	None	7	Disable	
#8	EnGenius304018_8-2.4GHz	None	8	Disable	

Connections

Clicking the **Connections** link under the **Device Status** menu displays the list of clients associated to the Access Point's 2.4GHz band along with the MAC address, TX, RX and signal strength for each client. Clicking **Kick** in the Block column removes this client.

Connection List - 2.4GHz

SSID	MAC Address	TX	RX	RSSI	Block
------	-------------	----	----	------	-------

Refresh

Click **Refresh** to refresh the Connection List page.

Chapter 5

Network

Basic

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

IPv4 Settings

IPv4 Settings

IP Network Setting	<input type="radio"/> DHCP <input checked="" type="radio"/> Static IP
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	192.168.1.1
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0

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.

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.

IPv6 Settings

IPv6 Settings	<input checked="" type="checkbox"/> Link-local Address
IP Address	<input type="text"/>
Subnet Prefix Length	<input type="text"/>
Gateway	<input type="text"/>
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>

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

IP Address: The IPv6 IP Address of this device.

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

Gateway: The IPv6 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.

Spanning Tree Settings

Spanning Tree Protocol (STP) Settings

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

Save

Save current setting(s)

Status: Enables or disables the Spanning Tree function.

Hello Time: Specify Bridge Hello Time, in seconds. This value determines how often the device sends handshake packets to communicate information about the topology throughout the entire Bridged Local Area Network.

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 inactive.

Forward Delay: Specifies 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 analyzes data traffic before participating.

Priority: Specify the Priority Number. A smaller number has greater priority.

Save: Click Save to confirm the changes.

Chapter 6

2.4GHz Wireless

2.4GHz SSID Profile

Under **Wireless Settings**, you can edit the SSID profile to fit your needs. Click **Edit** under the SSID you would like to make changes to.

Wireless Settings - 2.4GHz

No.	Enable	SSID	Edit	Security	Hidden SSID	Client Isolation	VLAN Isolation	VLAN ID
1	<input checked="" type="checkbox"/>	EnGenius05B069_1-2.4GHz	Edit	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1
2	<input type="checkbox"/>	EnGenius05B069_2-2.4GHz	Edit	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2
3	<input type="checkbox"/>	EnGenius05B069_3-2.4GHz	Edit	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	3
4	<input type="checkbox"/>	EnGenius05B069_4-2.4GHz	Edit	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	4
5	<input type="checkbox"/>	EnGenius05B069_5-2.4GHz	Edit	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	5
6	<input type="checkbox"/>	EnGenius05B069_6-2.4GHz	Edit	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	6
7	<input type="checkbox"/>	EnGenius05B069_7-2.4GHz	Edit	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	7
8	<input type="checkbox"/>	EnGenius05B069_8-2.4GHz	Edit	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	8

Enable: Check this option to enable this profile.

SSID: Specifies the SSID for the current profile.

Security: Displays the Security Mode the SSID uses. You can click **Edit** to change the security mode. For more details, see the next section.

Hidden SSID: Check this option to hide the SSID from clients. If checked, the SSID will not appear in the site survey.

Client Isolation: Check this option to prevent communication between client devices.

VLAN Isolation: Check this option to enable VLAN Isolation feature.

VLAN ID: Specifies the VLAN ID for the SSID profile.

Wireless Security

The Wireless Security section lets you configure the Access Point's security modes: WEP, WPA-PSK, WPA2-PSK, WPA-PSK Mixed, WPA-Enterprise, WPA2-Enterprise and WPA Mixed Enterprise.

It is strongly recommended that you use **WPA2-PSK**. Click on the **Edit** button under Wireless Settings next to the SSID to change the security settings.

WEP

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	
Key2	
Key3	
Key4	

Auth Type: Select Open System or Shared Key.

Input Type: ASCII: Regular Text (Recommended) or HEX: Hexadecimal Numbers (For advanced users).

Key Length: Select the desired option and ensure the wireless clients use the same setting. Your choices are: 64, 128, and 152-bit password lengths.

Default Key: Select the key you wish to be 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. The default is none.

WPA-PSK/WPA2-PSK (Pre-Shared Key)

Security Mode	WPA-PSK Mixed	▼
Encryption	Both(TKIP+AES)	▼
Passphrase	<input type="text"/>	
Group Key Update Interval	3600	

Encryption: Select the WPA/WPA2 encryption type you would like to use. Available options are Both, TKIP(Temporal Key Integrity Protocol) and AES(Advanced Encryption Standard). Please ensure that your wireless clients use the same settings.

Passphrase: Wireless clients must use the same Key to associate the device. If using ASCII format, the Key must be from 8 to 63 characters in length. If using HEX format, the Key must be 64 HEX characters in length.

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

WPA/WPA2-Enterprise

Security Mode	WPA Mixed-Enterprise	▼
Encryption	Both(TKIP+AES)	▼
Group Key Update Interval	3600	
Radius Server	<input type="text"/>	
Radius Port	1812	
Radius Secret	<input type="text"/>	
Radius Accounting	Disable	▼
Radius Accounting Server	<input type="text"/>	
Radius Accounting Port	1813	
Radius Accounting Secret	<input type="text"/>	
Interim Accounting Interval	600	

Encryption: Select the WPA/WPA2 encryption type you would like to use. Available options are Both, TKIP(Temporal Key Integrity

Protocol) and AES(Advanced Encryption Standard). Please ensure that your wireless clients use the same settings.

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

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.

Radius Accounting: Enables or disables the 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.

Wireless MAC Filter

Wireless MAC Filter is used to allow or deny network access to wireless clients (computers, tablet PCs, NAS, smart phones, etc.) according to their MAC addresses. You can manually add a MAC address to restrict permission to access the Access Point. The default setting is: Disable Wireless MAC Filter.

Wireless MAC Filter

ACL Mode	Disabled	▼				
	<input type="text"/>	: <input type="text"/>	: <input type="text"/>	: <input type="text"/>	: <input type="text"/>	: <input type="text"/>
	<input type="button" value="Add"/>					
No.	MAC Address					

ACL (Access Control List) Mode: Determines whether network access is granted or denied to clients whose MAC addresses appear in the MAC address table on this page. Choices given 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: Deletes the selected entries.

Traffic Shaping

Traffic Shaping regulates the flow of packets leaving an interface to deliver improved Quality of Service.

Wireless Traffic Shaping

Enable Traffic Shaping	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
Download Limit	<input type="text" value="100"/>	Mbps (1-999)
Upload Limit	<input type="text" value="100"/>	Mbps (1-999)

Save current setting(s)

Enable Traffic Shaping: Select to Enable or Disable Wireless Traffic Shaping.

Download Limit: Specifies the wireless transmission speed used for downloading.

Upload Limit: Specifies the wireless transmission speed used for uploading.

Save: Click **Save** to apply the changes.

Guest Network

The Guest Network function allows administrators to grant Internet connectivity to visitors or guests while keeping other networked devices (computers and hard drives) and sensitive personal or company information private and secure.

Guest Network Settings

Enable	SSID	Edit	Security	Hidden SSID	Client Isolation
<input checked="" type="checkbox"/>	EnGenius-2.4GHz_GuestNetw	Edit	None	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Manual IP Settings					
IP Address		192.168.200.1			
Subnet Mask		255.255.255.0			
Automatic DHCP Server Settings					
Starting IP Address		192.168.200.100			
Ending IP Address		192.168.200.200			
WINS Server IP		0.0.0.0			

Enable SSID: Select to Enable or Disable SSID broadcasting.

SSID: Specify the SSID for the current profile. This is the name visible on the network to wireless clients.

Security: You can use None or WPA-PSK / WPA2-PSK security for this guest network.

Hidden SSID: Check this option to hide the SSID from broadcasting to discourage wireless users from connecting to a particular SSID.

Client Isolation: Check this option to prevent wireless clients associated with your access point to communicate with other wireless devices connected to the AP.

After enabling Guest Network in the SSID Config page, assign an IP Address, Subnet Mask and DHCP server IP address range for this Guest Network.

Manual IP Settings	
IP Address	<input type="text" value="192.168.200.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Automatic DHCP Server Settings	
Starting IP Address	<input type="text" value="192.168.200.100"/>
Ending IP Address	<input type="text" value="192.168.200.200"/>
WINS Server IP	<input type="text" value="0.0.0.0"/>

Manual IP Settings

IP Address: Specify an IP Address for the Guest Network

Subnet Mask: Specify the the Subnet Mask IP Address for the Guest Network

Automatic DHCP Server Settings

Starting IP Address: Specify the starting IP Address range for the Guest Network.

Ending IP Address: Specify the ending IP Address range for the Guest Network.

WINS Server IP: Specify the WINS Server IP Address for the Guest Network. WINS means Windows Internet Name Service. It is Microsoft's implementation of NetBIOS Name Service (NBNS), a name server and service for NetBIOS computer names.

Fast Handover

With Fast Handover enabled, the AP will send a disassociation request to the wireless client and let it find another AP to handover and associate upon detecting the wireless client's RSSI value lower than specified. The RSSI value can be adjusted to allow more clients to stay associated to this AP. Note that setting the RSSI value too low may cause wireless clients to reconnect frequently.

Fast Handover

Status	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
RSSI	<input type="text" value="-70"/> dBm (Range: -60dBm ~ -90dBm)

Management VLAN Settings

This section 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

Status

Enable Disable

4096

Caution: If you encounter disconnection issue during the configuration process, verify that the switch and the DHCP server can support the new VLAN ID and then connect to the new IP address.

Save

Save current setting(s)

Status: If your network includes VLANs and if tagged packets need to pass through the Access Point, select **Enable** and enter the VLAN ID. Otherwise, click **Disable**.

Save: Click **Save** to apply the changes.

Note: If you reconfigure the Management VLAN ID, you may lose your connection to the Access Point. Verify that the DHCP server supports the reconfigured VLAN ID and then reconnect to the Access Point using the new IP address.

Chapter 7

Management

SNMP Settings

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) returns the data stored in their Management Information Bases. To configure SNMP Settings, click under the **Advanced** tab on the side bar under **Management**.

SNMP Settings	
Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Contact	<input type="text"/>
Location	<input type="text"/>
Port	<input type="text" value="161"/>
Community Name (Read Only)	<input type="text" value="public"/>
Community Name (Read Write)	<input type="text" value="private"/>
Trap Destination	
- Port	<input type="text" value="162"/>
- IP Address	<input type="text"/>
- Community Name	<input type="text" value="public"/>
SNMPv3 Settings	
- Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
- Username	<input type="text" value="admin"/> (1-31 Characters)
- Authorized Protocol	<input type="text" value="MD5"/> <input type="button" value="v"/>
- Authorized Key	<input type="text" value="12345678"/> (8-32 Characters)
- Private Protocol	<input type="text" value="DES"/> <input type="button" value="v"/>
- Private Key	<input type="text" value="12345678"/> (8-32 Characters)
- Engine ID	<input type="text"/>

Status: Enables or Disables the SNMP feature.

Contact: Specifies the contact details of the device.

Location: Specifies the location of the device.

Port: Displays the port number.

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

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

Trap Destination Address: Specifies the port and IP address of the computer that will receive the SNMP traps.

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

SNMPv3 Status: Enables or Disables the SNMPv3 feature.

User Name: Specifies the username for the SNMPv3.feature

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: Specifies the privacy key for privacy.

Engine ID: Specifies the Engine ID for SNMPv3.

CLI/SSH Settings

Most users will configure the device 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 accessed through a command console, modem or Telnet connection. For security's concern, you can enable SSH (Secure Shell) to establish a secure data communication.

CLI Setting

Status Enable Disable

SSH Setting

Status Enable Disable

CLI Status: Select **Enable** or **Disable** to enable or disable the ability to modify the Access Point via a command line interface (CLI).
SSH Status: Select **Enable** or **Disable** to enable or disable the ability to modify the Access Point via a command line interface (CLI) with a secure channel.

HTTPS Settings

Hypertext Transfer Protocol Secure (HTTPS) is a communications protocol for secure communication over a computer network, with especially wide deployment on the Internet. Technically, it is not a protocol in and of itself; rather, it is the result of simply layering the Hypertext Transfer Protocol (HTTP) on top of the SSL/TLS protocol, thus adding the security capabilities of SSL/TLS to standard HTTP communications.

HTTPS Settings

Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
HTTPS forward	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Status: Select **Enable** or **Disable** to enable or disable the ability to modify the Access Point via a HTTPS.

HTTPS forward: Enable this option; it will be forwarded to HTTPS if user uses HTTP to access the Access Point.

Email Alert

The Access Point will send email alerts when configurations have been changed.

Email Alert

Status	<input type="checkbox"/> Enable
- From	<input type="text"/>
- To	<input type="text"/>
- Subject	<input type="text" value="[Email-Alert][EWS320AP][88:DC:96:05:B0:68] Configur"/>
Email Account	
- Username	<input type="text"/>
- Password	<input type="text"/>
- SMTP Server	<input type="text"/> Port: <input type="text" value="25"/>
- Security Mode	<input type="text" value="None"/> <input type="button" value="Send Test Mail"/>

Apply

Apply saved settings to take effect

Status: Check **Enable** to enable Email Alert feature.

From: Enter the address to show as the sender of the email.

To: Enter the address to show as the receiver of the email.

Subject: Enter the subject to show as the subject of the email.

Email Account

Username/Password: Enter the username and password required to connect to the SMTP server.

SMTP Server/Port: Enter the IP address/domain name and port of the SMTP server. The default port of SMTP Server is port 25.

Security Mode: Select the mode of security for the Email alert. The options are None, SSL/TLS and STARTTLS.

Send Test Mail: Click **Send Test Mail** button to test the Email Alert setup.

Apply: Click **Apply** to save the changes.

Date and Time Settings

This page allows you to set the internal clock of the Access Point. To access the Date and Time settings, click **Time Zone** under the **Management** tab on the side bar.

Date and Time Settings

Manually Set Date and Time

Date: 2015 / 04 / 08

Time: 14 : 28 (24-Hour)

Automatically Get Date and Time

NTP Server: 209.81.9.7

Time Zone

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

Enable Daylight Saving

Start Time: January 1st Sun 12 am

End Time: January 1st Mon 12 am

Apply saved settings to take effect

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

Synchronize with PC: Click to synchronize the Access Point's internal clock with the computer's time.

Automatically Get Date and Time: Enter the IP address of an NTP server or use the default NTP server to have the internal clock set automatically.

Time Zone: Choose the time zone you would like to use from the drop-down list.

Enable Daylight Savings: Check the box to enable or disable daylight savings time for the Access Point. Next, enter the dates that correspond to the present year's daylight savings time.

Click **Apply** to save the changes.

WiFi Scheduler

Use the schedule function to reboot the Access Point or control the wireless availability on a routine basis. The Schedule function relies on the GMT time setting acquired from a network time protocol (NTP) server. For details on how to connect the Access Point to an NTP server, see Date and Time Settings.

Auto Reboot Settings

You can specify how often you would like to reboot the Access Point.

Auto Reboot Settings

Status	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Timer	<input type="checkbox"/> Sunday <input type="checkbox"/> Monday <input type="checkbox"/> Tuesday <input type="checkbox"/> Wednesday <input type="checkbox"/> Thursday <input type="checkbox"/> Friday <input type="checkbox"/> Saturday
	<input type="text" value="0"/> : <input type="text" value="0"/>

Status: Enables or disables the Auto Reboot function.

Timer: Specifies the time and frequency in rebooting the Access Point by Min, Hour and Day.

WiFi Scheduler

Wi-Fi Scheduler

Enable Disable

Status **NOTE:** Please assure that the Time Zone Settings is synced with your local time when enabling the Wi-Fi Scheduler.

Wireless Radio

SSID Selection

Schedule Templates

Day	Availability	Duration
Sunday	<input type="text" value="available"/>	<input type="text" value="00"/> : <input type="text" value="00"/> ~ <input type="text" value="24"/> : <input type="text" value="00"/>
Monday	<input type="text" value="available"/>	<input type="text" value="00"/> : <input type="text" value="00"/> ~ <input type="text" value="24"/> : <input type="text" value="00"/>
Tuesday	<input type="text" value="available"/>	<input type="text" value="00"/> : <input type="text" value="00"/> ~ <input type="text" value="24"/> : <input type="text" value="00"/>
Wednesday	<input type="text" value="available"/>	<input type="text" value="00"/> : <input type="text" value="00"/> ~ <input type="text" value="24"/> : <input type="text" value="00"/>
Thursday	<input type="text" value="available"/>	<input type="text" value="00"/> : <input type="text" value="00"/> ~ <input type="text" value="24"/> : <input type="text" value="00"/>
Friday	<input type="text" value="available"/>	<input type="text" value="00"/> : <input type="text" value="00"/> ~ <input type="text" value="24"/> : <input type="text" value="00"/>
Saturday	<input type="text" value="available"/>	<input type="text" value="00"/> : <input type="text" value="00"/> ~ <input type="text" value="24"/> : <input type="text" value="00"/>

Save current setting(s)

Status: Enables or disables the WiFi Scheduler function.

SSID Selection: Select a SSID to use WiFi Schedule.

Schedule Templates: There are 3 templates available: Always available, Available 8-5 daily and Available 8-5 daily except weekends. Select Custom schedule if you want to set the schedule manually.

Schedule Table: Set the schedule manually.

Tools

This section allows you to analyze the connection quality of the Access Point and trace the routing table to a target in the network.

Ping Test Parameters

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"/>
<input type="button" value="Start"/>	<div style="border: 1px solid #ccc; height: 150px; width: 100%;"></div>

Target IP/Domain Name: Enter the IP address or Domain name you would like to search.

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

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

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

Traceroute Parameters

Traceroute Test Parameters

Target IP / Domain Name

Target IP/Domain Name: Enter an IP address or domain name you wish to trace.

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

Stop: Halts the traceroute test.

Speed Test Parameters

Speed Test Parameters

Target IP / Domain Name	<input type="text"/>
Time Period	<input type="text" value="20"/> sec
Check Interval	<input type="text" value="5"/> sec
<input type="button" value="Start"/>	<div style="border: 1px solid #ccc; height: 150px; width: 100%;"></div>
IPv4 Port	5001
IPv6 Port	5002

Target IP/Domain Name: Enter an IP address or domain name you wish to run a Speed Test for.

Time Period: Enter the time in seconds that you would like the test to run for and in how many intervals.

Start: Starts the Speed Test.

IPv4 / IPv6 Port: The Access Point uses IPv4 port 5001 and IPv6 port 5002 for the speed test.

LED Control

This section allows you to control the LED control functions: Power status, LAN interface and WLAN interface.

LED Control

Power Enable Disable

LAN Enable Disable

WLAN Enable Disable

Apply

Apply saved settings to take effect

Click **Apply** to save the settings after selecting your choices from the boxes.

Device Discovery

Under Device Discovery, you can choose for the Access Point to automatically scan for local devices to connect to. Click **Scan** to begin the process.

Device Discovery

Device Name	Operation Mode	IP Address	System MAC Address	Firmware Version
<input type="button" value="Scan"/>				

Chapter 8

System Manager

Account Setting

This page allows you to change the username and password of the device. By default, the username is **admin** and the password is **admin**. The password can contain from 0 to 12 alphanumeric characters and is case sensitive.

Account Settings

Administrator Username	<input type="text" value="admin"/>
Current Password	<input type="password"/>
New Password	<input type="password"/>
Verify Password	<input type="password"/>

Apply

Apply saved settings to take effect

Administrator Username: Enter a new username for logging in to the Administrator Username entry box.

Current Password: Enter the old password for logging in to the Current Password entry box.

New Password: Enter the new password for logging in to the New Password entry box.

Verify Password: Re-enter the new password in the Verify Password entry box for confirmation.

Apply: Click **Apply** to save the changes.

Note: it is highly recommended that you change your password to something more unique for greater security.

Firmware Upgrade

This page allows you to upgrade the Firmware of the Access Point.

Firmware Upgrade

Current Firmware Version: 2.0.0

Select the new firmware from your hard disk.

<input type="text"/>	<input type="button" value="Browse..."/>
<input type="button" value="Upload"/>	

To Perform the Firmware Upgrade:

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

Backup/Restore

This page allows you to save the current device configurations. When you save the configurations, you can also reload the saved configurations into the device through the **Restore New Settings** from a file folder. If extreme problems occur, or if you have set the Access Point incorrectly, you can use the **Reset** button in the **Reset to Default** section to restore all the configurations of the Access Point to the original default settings. To Configure the Backup/Restore Settings, click **Firmware** under the **Systems Manager** tab.

Backup/Restore Settings

Factory Setting	
- Backup Setting	<input type="button" value="Export"/>
- Restore New Setting	<input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Import"/>
- Reset to Default	<input type="button" value="Reset"/>
User Setting	
- Back Up Setting as Default	<input type="button" value="Backup"/>
- Restore to User Default	<input type="button" value="Restore"/>

Factory Setting

Backup Setting: Click **Export** to save the current device configurations to a file.

Restore New Setting: Choose the file you wish restore for settings and click **Import**.

Reset to Default: Click the **Reset** button to restore the Access Point to its factory default settings.

User Setting

Back Up Setting as Default: Click **Backup** to backup the user settings you would like to use as the default settings.

Restore to User Default: Click **Restore** to restore the Access Point to user's default settings.

System Log

This page allows you to setup the System Log and local log functions of the Access Point. Click **Log** under the **Systems Manager** tab to open up the System Log page.

System Log

Status Enable Disable

Log type

```
Jan 28 12:02:01 EWS300AP cron.info crond[2067]: crond: USER root pid 1312 cmd kil
Jan 28 12:01:01 EWS300AP cron.info crond[2067]: crond: USER root pid 989 cmd kill
Jan 28 12:00:01 EWS300AP user.notice root: starting ntpd
Jan 28 12:00:01 EWS300AP cron.info crond[2067]: crond: USER root pid 633 cmd ./e
Jan 28 12:00:01 EWS300AP cron.info crond[2067]: crond: USER root pid 629 cmd kill
Jan 28 11:59:01 EWS300AP cron.info crond[2067]: crond: USER root pid 4095 cmd kil
Jan 28 11:58:01 EWS300AP cron.info crond[2067]: crond: USER root pid 3769 cmd kil
Jan 28 11:57:01 EWS300AP cron.info crond[2067]: crond: USER root pid 3509 cmd kil
Jan 28 11:56:01 EWS300AP cron.info crond[2067]: crond: USER root pid 3121 cmd kil
Jan 28 11:55:01 EWS300AP user.notice root: starting ntpd
```

Remote Log Enable Disable

Log Server IP Address

Apply saved settings to take effect

Status: Enables or disables the System Log function.

Log Type: Select the Log Type mode you would like to use.

Remote Log: Enables or disables the Remote Log feature. If enabled, enter the IP address of the Log you would like to remote to.

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

Apply: Click **Apply** to save the changes.

Reset

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

The screenshot shows the EnGenius web interface for an EWS300AP. The top navigation bar includes the EnGenius logo, the device model 'EWS300AP', the description 'Single Radio AP , 2T2R , 300Mbps', and buttons for 'Changes : 0', 'Reset', and 'Logout'. The 'Reset' button is highlighted with a red box. The main content area is divided into three sections: 'Reboot the Device' with a 'Reboot the Device' button and a caution message; 'Restore the device to default settings' with 'Restore to Factory Defaults' and 'Restore to User Default' buttons and a caution message; and a 'Log' button in the bottom left sidebar.

EnGenius®
EWS300AP Single Radio AP , 2T2R , 300Mbps Changes : 0 **Reset** Logout

Overview
Device Status
Connections

Network
Basic
Wireless

Management
Advanced
Time Zone
WiFi Scheduler
Tools

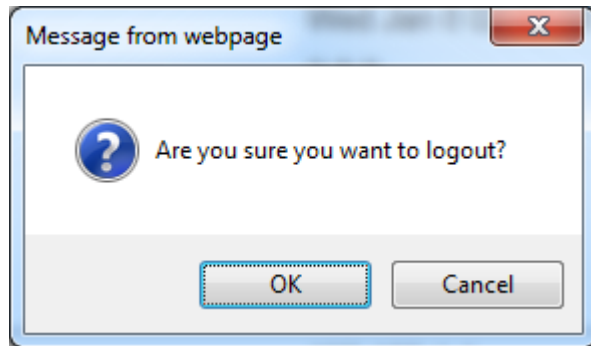
System Manager
Account
Firmware
Log

Reboot the Device
CAUTION: The device will be rebooted when pressing this button.
Reboot the Device

Restore the device to default settings
CAUTION: All settings will be cleared and reset to either factory default or user default.
Restore to Factory Defaults Restore to User Default

Logout

Click **Logout**, it will pop up a warning window. Click **OK** to logout.



Appendix

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.

IMPORTANT NOTE:

Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Appendix B - IC Interference Statement

Industry Canada Statement

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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

Radiation Exposure Statement

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Déclaration d'exposition aux radiations:

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

Appendix C - CE Interference Statement








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



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/EK.
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 <i>[name of manufacturer / izgatavotāja nosaukums]</i> deklarē, ka <i>[type of equipment / iekārtas tips]</i> atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo <i>[manufacturer name]</i> deklaruoja, kad šis <i>[equipment type]</i> atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
nl Nederlands [Dutch]	Hierbij verklaart <i>[naam van de fabrikant]</i> dat het toestel <i>[type van toestel]</i> in overeenstemming is met de essentiële eisen en de

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