

EnGenius®

The Neutron Series

User Manual



EWS860AP
version 1.0

Dual Band
Wireless AC1750 Managed Outdoor 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	22
Default Settings.....	23
Web Configuration.....	24
Chapter 4	26
Device Status.....	27
Connections.....	30
Chapter 5	31
IPv4 Settings	32
IPv6 Settings	33
Spanning Tree Settings.....	34
Chapter 6	35

Wireless Settings.....	36
2.4GHz/5GHz SSID Profile.....	39
Wireless Security	41
Wireless MAC Filter.....	44
Traffic Shaping.....	45
Guest Network	46
Fast Handover	48
Management VLAN Settings.....	49
Chapter 7.....	50
SNMP Settings.....	51
CLI/SSH Settings.....	53
HTTPS Settings.....	54
Email Alert	55
Date and Time Settings	56
WiFi Scheduler.....	57
Tools.....	59
Device Discovery.....	62
Chapter 8.....	63
Account Setting.....	64
Firmware Upgrade	65
Backup/Restore	66
System Log	67
Reset.....	68
Logout	69
Appendix.....	70
Appendix A - FCC Interference Statement	71
Appendix B - IC Interference Statement.....	72











Chapter 1

Product Overview

Introduction

Key Features



-  Deploy and manage with ease using EWS Series Wireless Management Switches.
-  Up to 29 dBm transmit power enabling long range connectivity.
-  Supports IEEE802.11ac/a/b/g/n wireless standards with up to 450 Mbps data rate on 2.4GHz band and 1300Mbps on 5GHz band
-  Three detachable 5 dBi 2.4 GHz Omni-directional antennas
-  Three detachable 7 dBi 5 GHz Omni-directional antennas
-  Backward compatible with IEEE802.11a/b/g/n wireless devices.
-  Integrated Power over Ethernet (IEEE802.3at) for lowering deploying costs. Can be powered using either the included power adapter or via PoE with PoE 802.3af/at capable Switches or Injectors.
-  Dual Band/Three Stream.
-  Band Steering to load balance clients between 2.4GHz and 5 GHz for better throughput performance.¹
-  Secured Guest Network option available.

Introduction

The EWS860AP is a high-powered, long-range 3x3 Dual-Band Wireless 802.11 ac/a/b/g/n Outdoor Access Point with speeds up to 450 Mbps on 2.4GHz and 1300Mbps on 5GHz band.. This Access Point is designed to operate in a variety of outdoor environments. Its high-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 business network. The EWS860AP supports 2.4GHz frequency band under 802.11 b/g/n mode while at the same time provides 5GHz band under 802.11 ac/a/n mode for communicating to and from 5GHz capable computers, tablets or smart phones or transferring files. Several EWS860APs can be deployed in a campus setting using the 5GHz band as a backhaul to provide multiple 2.4GHz wireless cells for computers or mobile devices in common outdoor areas.

The EWS860AP is easy to install in virtually any location with its included PoE (Power over Ethernet) injector for quick outdoor installation. The EWS860AP enables network administrators to control its transmit power and feature settings for selecting narrow bandwidth and traffic shaping. The EWS860AP also supports wireless encryption including Wi-Fi Protected Access(WPA-PSK/WPA2-PSK) Encryption, and IEEE 802.1x with RADIUS.

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):

- EWS860AP Access Point
- 3 detachable 5 dBi 2.4 GHz Omni-directional Antenna
- 3 detachable 7 dBi 5 GHz Omni-directional Antenna
- Power Adapter (48V/0.8A)
- PoE Injector (EPE-48GR)
- Grounding Cable
- Pole Mount Bracket
- Wall Mount Base
- 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

Standard:

IEEE802.11ac/a/n on 5 GHz
IEEE802.11b/g/n on 2.4 GHz
IEEE802.3at

Antenna:

6 External N-type Antenna
3 x detachable 5 dBi 2.4 GHz Omni-directional Antennas
3 x detachable 7 dBi 5 GHz Omni-directional Antennas

Physical Interface:

2 x 10/100/1000 Gigabit Ethernet Port with PoE support
LAN1 Port: IEEE802.3at PoE Input
LAN2 Port: IEEE802.3af PoE Output
Both Ethernet Ports support Surge Protection to 6KV

LED Indicators:

Power
LAN 1
LAN 2
2.4 GHz
5 GHz

Power Requirements:

External Power Adapter, DC IN, 48V/0.8A
IEEE802.3at support

Management:

Auto Channel Selection
Multiple SSID: 16 SSIDs, 8 SSIDs per Radio
BSSID
SNMP V1/V2c/V3
MIB I/II, Private MIB
VLAN Tag/VLAN Pass-through
Clients Statistics
Save Configuration as User Default
Fast Roaming
E-Mail Alert
RADIUS Accounting
Guest Network
Control
CLI Supported
Distance Control (ACK Timeout)
Multicast Supported
Auto Reboot
Obey Regulatory Power

Security:

WEP Encryption - 64/128/152 bit
WPA/WPA2 Personal (WPA-PSK using TKIP or AES)
WPA/WPA2 Enterprise (WPA-PSK using TKIP or AES)
Hides SSID in beacons
MAC address filtering, up to 50 MACs

Wireless STA (Client) connection list

Https Support

SSH Support

QoS (Quality of Service):

Compliant with IEEE 802.11e standard

Physical/Environment Conditions:

Operating:

Temperature: -4 °F to 158 °F (-20 °C to 70 °C)

Humidity (non-condensing): 90% or less

Storage:

Temperature: -22 °F to 176 °F (-30 °C to 80 °C)

Humidity (non-condensing): 90% or less

Physical Interface

Dimensions and Weights

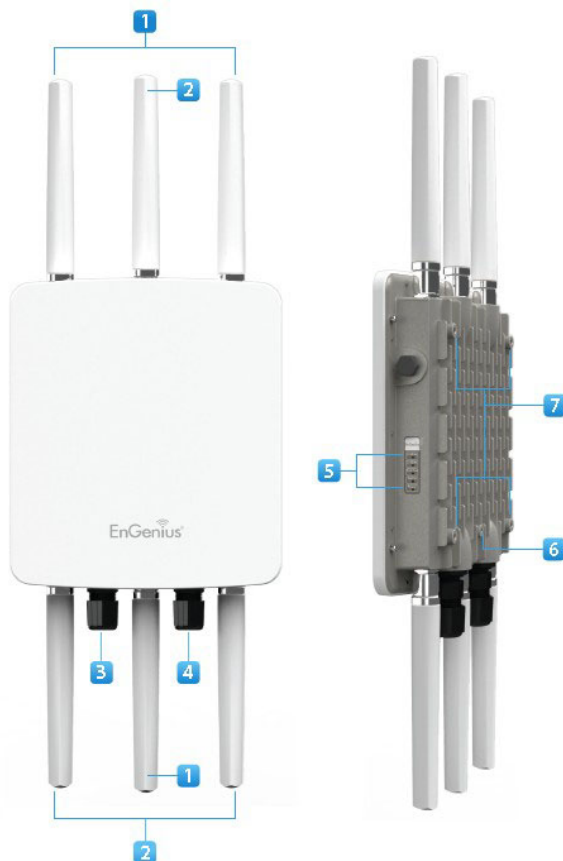
Length: 11.22"

Width: 8.58"

Depth: 2.1"

Weight: 4.17 lbs

1. 2.4 GHz Antennas: Detachable 5 dBi 2.4 GHz Omni-directional
2. 5 GHz Antennas Detachable 7 dBi 5 GHz Omni-directional
3. LAN Port 1 (802.3at PoE Input): Ethernet port for RJ-45 cable.
4. LAN Port 2 (802.3af PSE Output): Ethernet port for RJ-45 cable.
5. LED Indicators: LED lights for Power, LAN Port 1, LAN Port 2, 2.4 GHz Connection and 5 GHz Connection.
6. Ground
7. Mounting Holes: Using the provided hardware, the ENH1750EXT can be attached to a wall or pole.



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

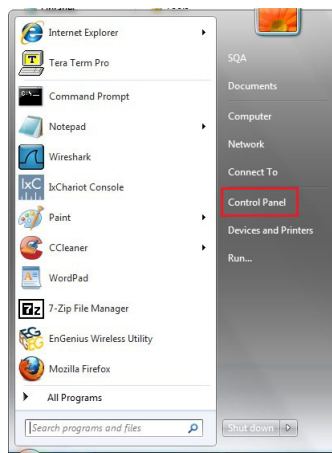
Windows XP/Windows 7

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

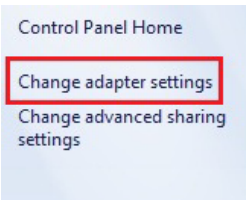
2a. In **Windows XP**, click on Network Connections.



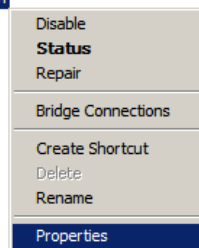
2b. In **Windows 7**, click **View network status and tasks** in the **Network and Internet** section, then select **Change adapter settings**.



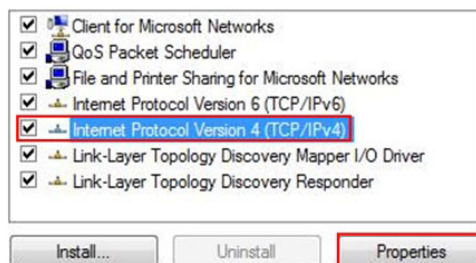
Network and Internet
View network status and tasks
Choose homegroup and sharing options



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



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



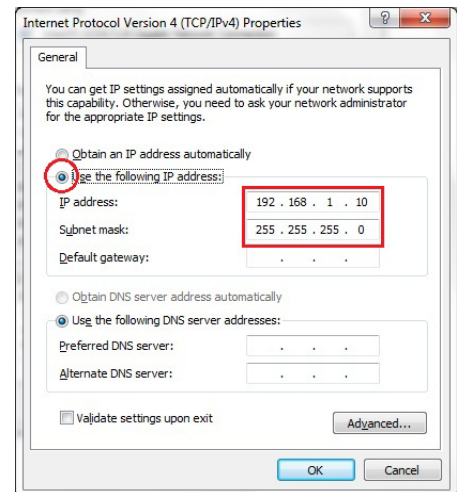
5. Select **Use the following IP address** and enter an IP address that is different from the Access Point and Subnet mask, then click **OK**.

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

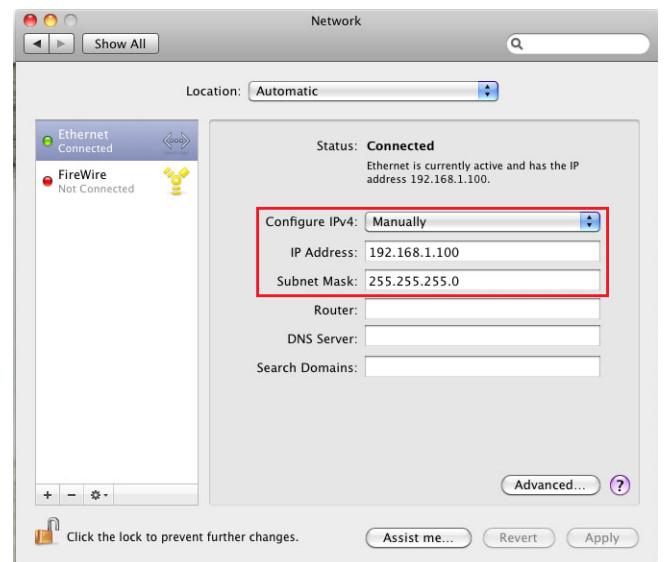


Apple Mac OS X

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.



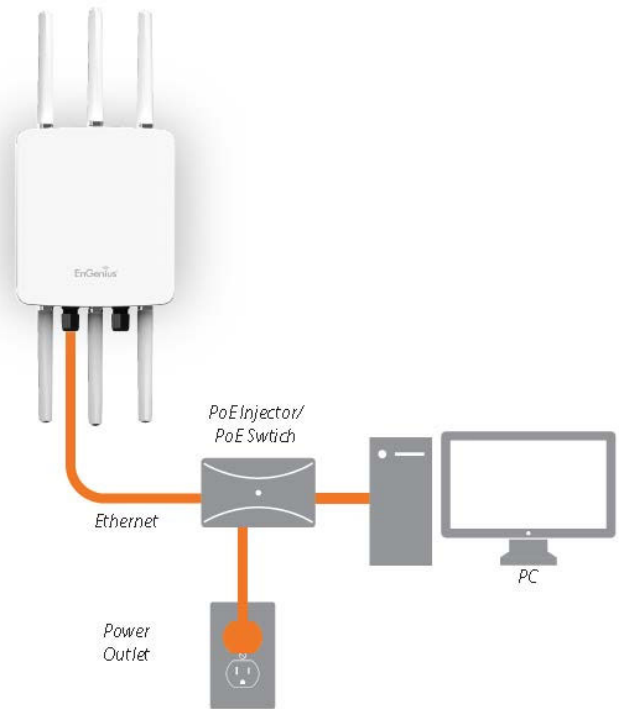
3. Highlight **Ethernet**.
4. In **Configure IPv4**, select **Manually**.
5. Enter an IP address that is different from the Access Point and Subnet mask, then click **OK**.
Note: Ensure that the IP address and Subnet mask are on the same subnet as the device.
For example: Access Point IP address: 192.168.1.1
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. Connect one end of the Ethernet cable into the main LAN port (PoE) of the Access Point and the other end to the AP Ethernet port on the PoE injector.
2. Connect the **Power Adapter** to the **DC-IN** port of the PoE injector and plug the other end in to an electrical outlet.
3. Connect the second Ethernet cable into the **LAN port** of the PoE injector and the other end to the Ethernet port on the computer.
4. Screw on the provided antennas to the device. Once both connections are secure, verify the following:
 - a) Ensure that the **POWER** light is on (it will be green).
 - b) Ensure that the 2.4 GHz/5 GHz WLAN light is on (it will be green for both 5 GHz and 2.4 GHz).
 - c) Ensure that the LAN (Computer/AP Connection) light is on (it will be green).
 - d) Once all three lights are on, proceed to set up the Access Point using the computer.

Note: The Access Point supports both IEEE 802.3at PoE (Power over Ethernet) or the included power injector. You may use either one as the power source. **Do NOT use both at the same time.**

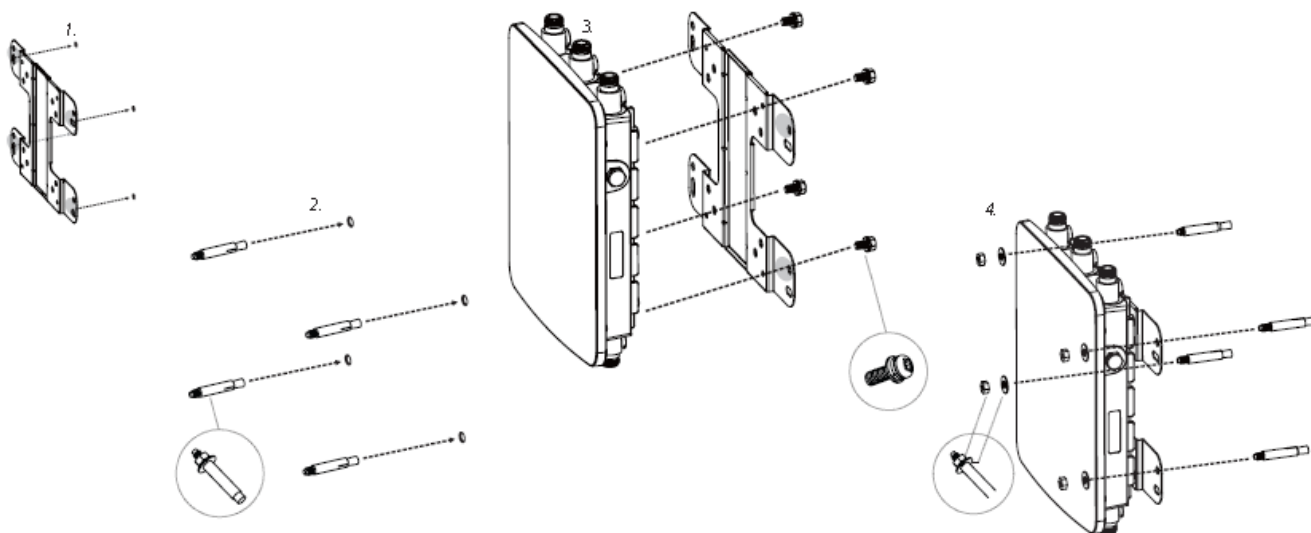


Mounting the Access Point

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

To attach the Access Point to a wall using the wall mounting kit:

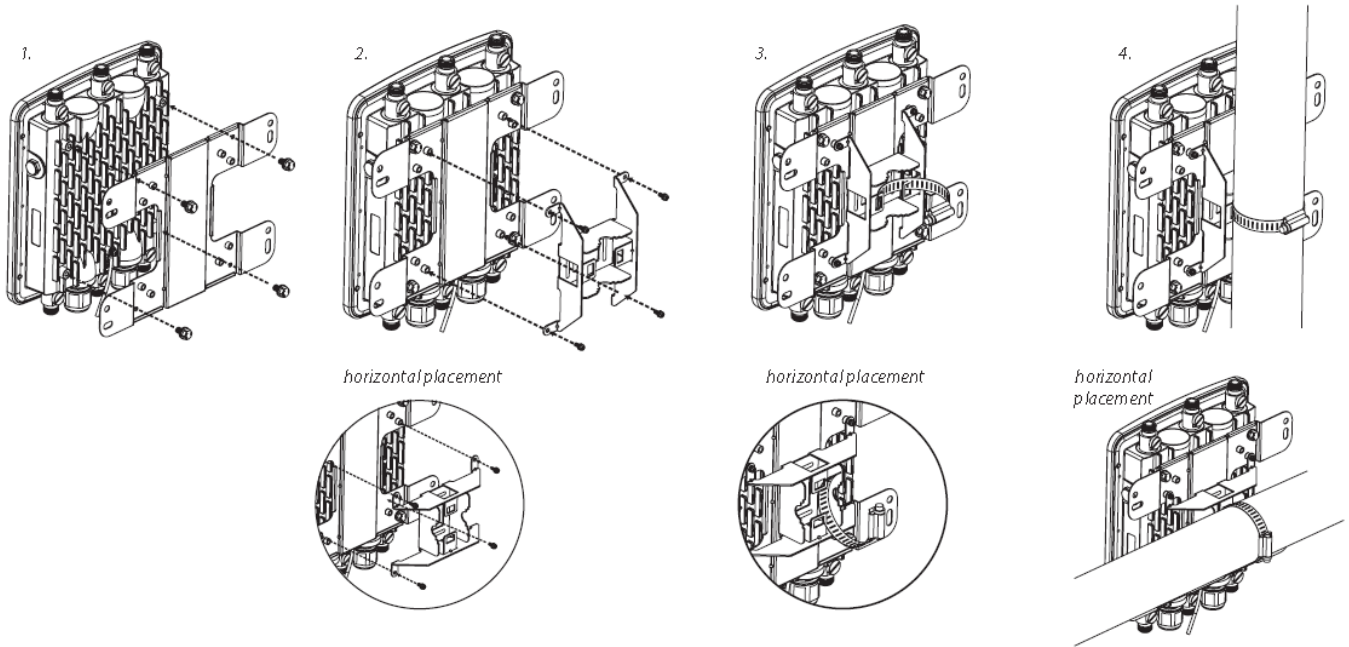
1. Mark the four locations of the mounting holes on the flat mounting surface.
2. Drill a 37 mm deep 8 mm hole in the markings and hammer the bolts into the openings.
3. Place the lock and flat washers on the four hex cap screws and drive the screws to attach the bracket to the back of the Access Point.
4. Tighten the flat washers to secure the bracket to the mounting surface.



To attach the Access Point to a pole using the provided pole mounting kit:

1. Place the lock and flat washers on the four hex cap screws and drive the screws to attach the bracket to the back of the Access Point.
2. Drive the four round head screws to attach the Pole Mount Bracket to the bracket.
3. Thread the open end of the Pole Strap through the two tabs on the Pole Mount Bracket .
4. Lock and tighten the Pole Strap to secure the Pole Mount Bracket to the pole.

Note: See diagram below for vertical and horizontal placements.



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

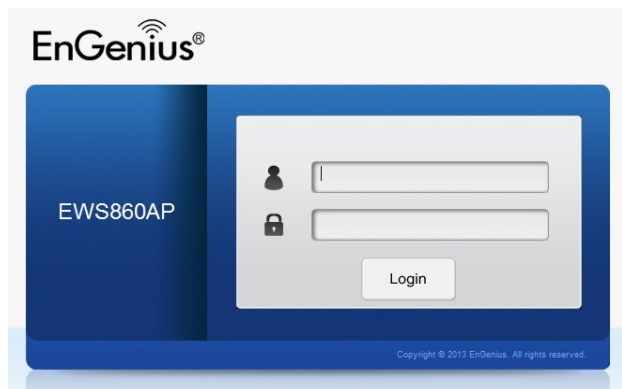
Web Configuration

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.

*Model name varies depending on model.

Overview

Device Status

Connections

Network

Basic

Wireless

Management

Advanced

Time Zone

WiFi Scheduler

Tools

System Manager

Account

Firmware

Log

Device Information

Device Name	EWS860AP
MAC Address	
- LAN	00:02:6F:04:04:01
- Wireless LAN - 2.4GHz	00:02:6F:04:04:03
- Wireless LAN - 5GHz	00:02:6F:04:04:04
Country	Default
Current Local Time	Thu Jun 26 04:45:26 UTC 2014
Firmware Version	2.0.0 + 1.0.6
Management VLAN ID	Untagged

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

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	EWS860AP
MAC Address	
- LAN	00:02:6F:04:04:01
- Wireless LAN - 2.4GHz	00:02:6F:04:04:03
- Wireless LAN - 5GHz	00:02:6F:04:04:04
Country	Default
Current Local Time	Thu Jun 26 04:45:26 UTC 2014
Firmware Version	2.0.0 + 1.0.6
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::202:6fff:fe04:401
Gateway	N/A
Primary DNS	N/A
Secondary DNS	N/A

 The **Wireless LAN Information 2.4 GHz/5GHz** 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 - 5GHz only available for 5GHz capable models.

Wireless LAN Information - 2.4GHz

Operation Mode	Access Point				
Wireless Mode	802.11 B/G/N				
Channel Bandwidth	20-40 MHz				
Channel	2.412 GHz (Channel 1)				
Distance	1000 M				
Profile	SSID	Security	VID	802.1Q	
#1	EnGenius040403_1-2.4GHz	None	1	Disable	
#2	EnGenius040403_2-2.4GHz	None	2	Disable	
#3	EnGenius040403_3-2.4GHz	None	3	Disable	
#4	EnGenius040403_4-2.4GHz	None	4	Disable	
#5	EnGenius040403_5-2.4GHz	None	5	Disable	
#6	EnGenius040403_6-2.4GHz	None	6	Disable	
#7	EnGenius040403_7-2.4GHz	None	7	Disable	
#8	EnGenius040403_8-2.4GHz	None	8	Disable	

Wireless LAN Information - 5GHz

Operation Mode	Access Point			
Wireless Mode	802.11 AC/N			
Channel Bandwidth	80 MHz			
Channel	5.54 GHz (Channel 108)			
Distance	1000 M			
Profile	SSID	Security	VID	802.1Q
#1	EnGenius040404_1-5GHz	None	51	Disable
#2	EnGenius040404_2-5GHz	None	52	Disable
#3	EnGenius040404_3-5GHz	None	53	Disable
#4	EnGenius040404_4-5GHz	None	54	Disable
#5	EnGenius040404_5-5GHz	None	55	Disable
#6	EnGenius040404_6-5GHz	None	56	Disable
#7	EnGenius040404_7-5GHz	None	57	Disable
#8	EnGenius040404_8-5GHz	None	58	Disable

Connections

Clicking the **Connections** link under the **Device Status** menu displays the list of clients associated to the Access Point's 2.4GHz/5GHz, 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
------	-------------	----	----	------	-------

Connection List - 5GHz

SSID	MAC Address	TX	RX	RSSI	Block
EnGenius05B06A_1-5GHz	00:02:6F:93:47:5C	162Kb	30Kb	-42dBm	<input type="button" value="Kick"/>

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	
Subnet Prefix Length	
Gateway	
Primary DNS	
Secondary DNS	

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 checked="" type="radio"/> Enable <input 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 & 5GHz Wireless

Wireless Network

This page displays the current status of the Wireless settings of the Access Point.

Wireless Settings

Wireless Settings

Device Name	<input type="text" value="EWS860AP"/>
Country / Region	<input type="text" value="Please Select a Country Code"/> <input type="button" value="v"/>
Band Steering	<input type="radio"/> Enable <input checked="" type="radio"/> Disable NOTE: In order for Band Steering function to work properly, both 2.4GHz and 5GHz SSID and Security Settings must be the same.

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

Country/Region: Select a Country/Region to conform to local regulations.

Band Steering: Enable Band Steering to sends 802.11n clients to the 5GHz band, where 802.11b/g clients cannot go, and leaves the 802.11b/g clients in 2.4GHz to operate at their slower rates. Band Steering works within the Access Point by directing 5GHz-capable clients to that band.

*In order for the Band Steering function to work properly, both the 2.4GHz and the 5GHz SSID and security settings must be under the same selection settings.

	2.4GHz	5GHz
Operation Mode	Access Point <input type="checkbox"/> Green	Access Point <input type="checkbox"/> Green
Wireless Mode	802.11 B/G/N	802.11 AC/N
Channel HT Mode	20/40 MHz	80 MHz(AC Only)
Extension Channel	Upper Channel	Lower Channel
Channel	Auto	Auto
Transmit Power	Auto	Auto
Data Rate	Auto	Auto
RTS / CTS Threshold (1 - 2346)	2346	2346
Client Limits	127 <input checked="" type="radio"/> Enable <input type="radio"/> Disable	127 <input checked="" type="radio"/> Enable <input type="radio"/> Disable
Aggregation	<input checked="" type="radio"/> Enable <input type="radio"/> Disable 32 Frames 50000 Bytes(Max)	
AP Detection	Scan	Scan
Distance (1-30km)	1	1

Wireless Mode: Supports 802.11b/g/n mixed mode in 2.4GHz and 802.11a/n mixed mode in 5GHz. Note that 5GHz settings are only available for dual radio models.

Channel HT Mode: The default channel bandwidth is 20/40MHz. The larger the channel bandwidth, the better the transmission quality and speed. This option is only available for 802.11n modes only.

Extension Channel: Use the drop-down menu to set the Extension Channel as Upper or Lower channel. An extension channel is a secondary channel used to bond with the primary channel to increase this range to 40MHz allowing for greater bandwidth. This option is only available when Wireless Mode is 802.11n and Channel HT Mode is 20/40 MHz or 40MHz.

Channel: Select the channel appropriate for your country's regulation.

Transmit Power: Select the transmit power for the radio. Increasing the power improves performance, but if two or more access points are operating in the same area on the same channel, it may cause interference.

Data Rate: Use the drop-down list to set the available transmit data rates permitted for wireless clients. The data rate affects the throughput of the access point. The lower the data rate, the lower the throughput, but the longer transmission distance.

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

Client Limits: Limits the total number of clients.

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

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

Distance: Specifies the distance between the Access Points and clients. Note that longer distances may drop higher speed connections.

2.4GHz/5GHz 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

Wireless Settings - 5GHz

No.	Enable	SSID	Edit	Security	Hidden SSID	Client Isolation	VLAN Isolation	VLAN ID
1	<input checked="" type="checkbox"/>	EnGenius05B06A_1-5GHz	Edit	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	51
2	<input type="checkbox"/>	EnGenius05B06A_2-5GHz	Edit	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	52
3	<input type="checkbox"/>	EnGenius05B06A_3-5GHz	Edit	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	53
4	<input type="checkbox"/>	EnGenius05B06A_4-5GHz	Edit	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	54
5	<input type="checkbox"/>	EnGenius05B06A_5-5GHz	Edit	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	55
6	<input type="checkbox"/>	EnGenius05B06A_6-5GHz	Edit	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	56
7	<input type="checkbox"/>	EnGenius05B06A_7-5GHz	Edit	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	57
8	<input type="checkbox"/>	EnGenius05B06A_8-5GHz	Edit	None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	58

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

: : : : :

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

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 type="checkbox"/>	EnGenius-2.4GHz_GuestNetw	Edit	None	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	EnGenius-5GHz_GuestNetwo	Edit	None	<input type="checkbox"/>	<input checked="" type="checkbox"/>

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	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

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

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"/> ▼
- Authorized Key	<input type="text" value="12345678"/> (8-32 Characters)
- Private Protocol	<input type="text" value="DES"/> ▼
- 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="password"/>
- 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: 2014 / 01 / 07

Time: 11 : 16 (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: January 1st Sun 12 am

End: 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

Status Enable Disable
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						
Schedule Table	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.

Wireless Radio: Select 2.4GHz or 5GHz* to use WiFi Schedule.

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: 100px; 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 gray; height: 100px; width: 100%;"></div>	
IPv4 Port	<input type="text" value="5001"/>	
IPv6 Port	<input type="text" value="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.

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
-------------	----------------	------------	--------------------	------------------

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.