![EnGenius logo]

Business Solutions

User Manual

EnStation2
Version 1.1

N300 2.4GHz Long Range Point to Point CPE

TABLE OF CONTENTS

Product Overview

Installation

Web Configuration

Basic Network Settings

Appendix A

Appendix B

Appendix C

Conventions

The following conventions are used to give the user additional information about specific procedures or content. It is important to pay attention to these conventions as they provide information to prevent damage to equipment or personal injury.

General Conventions

The following general conventions are used in this document:

CAUTION!

CAUTION SIGNS APPEAR BEFORE THE TEXT IT REFERENCES. CAUTION SIGNS APPEAR IN CAPITAL LETTERS TO EMPHASIZE THAT THE MESSAGE CONTAINS VITAL HEALTH AND SAFETY INFORMATION.

WARNING!

Warning information appears before the text it references to emphasize that the content may prevent damage to the device or equipment.

Important:

Indicates information that is important to know for the proper completion of a procedure, choice of an option, or completing a task.

Note:

Indicates additional information that is relevant to the current process or procedure.

Example:

Indicates information used to demonstrate or explain an associated concept.

N/A:

Indicates that a component or a procedure is not applicable to this model.

Prerequisite:

Indicates a requirement that must be addressed before proceeding with the current function or procedure.

Typographical Conventions

The following typographical conventions are used in this document:

Italics

Indicates book titles, directory names, file names, path names, and program/process names.

`Constant width`

Indicates computer output shown on a computer screen, including menus, prompts, responses to input, and error messages.

`Constant width bold`

Indicates commands lines as entered on the computer. Variables contained within user input are shown in angle brackets (<>).

Bold

Indicates keyboard keys that are pressed by the user.

Copyright

Product Overview

Chapter 1

1.1 Package Contents

- The EnStation2 package contains the following items:

- EnStation2 CPE

- PoE Injector with Power Adapter

- 24V PoE Injector

- Quick Installation Guide

- Mounting Screw Set

- Wall Mount Kit

- Pole Mount Strap

1.2 Product Overview

Thank you for choosing EnStation2. The EnStation2 is a long range, high performance IEEE 802.11b/g/n network solution that provides Access Point, Client Bridge, WDS, and Client Router functions in a single device.

In addition to providing the latest wireless technology, the EnStation2 supports Power over Ethernet and Power by Adapter capabilities, which allow the device to be installed easily in nearly any indoor or outdoor location. Advanced features include power level control, traffic shaping, and Real time RSSI indication.

A variety of security features help to protect your data and privacy while you are online. Security features include Wi-Fi Protected Access (WPA PSK/WPA2 PSK), 64/128/156 bit WEP Encryption, and IEEE 802.1x with RADIUS.

Key Features

- High-speed data rates up to 300 Mbps make the EnStation2 ideally suited for handling heavy data payloads such as MPEG video streaming

- A high output power up to 26 dBm delivers superior range and coverage

- Fully interoperability with IEEE 802.11b/IEEE 802.11g/IEEE 802.11n-compliant devices

- Multi-operation modes enable users to utilize Enstaion2 for various environments

- Point-to-point and point-to-multipoint wireless connectivity enable data transfers between two or more buildings

- Channel bandwidth selection allows the appropriate bandwidth to be used to reach various distances

- RSSI indicator makes it easy to select the best signal for Access Point connections

- Power-over-Ethernet capabilities allow for flexible deployment and great savings

- Four SSIDs let clients access different networks through a single Access Point, and assign different policies and functions for each SSID

- WPA2/WPA/ WEP/ IEEE 802.1x support and MAC address filtering ensure secure network connections

- PPPoE/PPTP function support make it easy to access the Internet via Internet Service Provider (ISP) service authentication

- SNMP Remote Configuration Management helps administrators remotely configure or manage the Access Point

- QoS (WMM) support enhances performance and user experiences

Benefits

The EnStation2 is the ideal product around which you can build your WLAN. The following list summarizes a few key advantages that WLANs have over wired networks:

Ideal for Hard-to-Wire Environments

There are many scenarios where cables cannot be used to connect networking devices. Historic and older buildings, open areas, and busy streets, for example, make wired LAN installations difficult, expensive, or impossible.

Temporary Workgroups

WLANs make it easy to provide connectivity to temporary work-groups that will later be removed. Examples include parks, athletic arenas, exhibition centers, disaster-recovery shelters, temporary offices, and construction sites.

Ability to Access Real-time Information

With a WLAN, workers who rely on access to real-time information, such as doctors and nurses, point-of-sale employees, mobile workers, and warehouse personnel, can access the data they need and increase productivity, without having to look for a place to plug into the network.

Frequently Changing Environments

WLANs are well suited for showrooms, meeting rooms, retail stores, and manufacturing sites where workplaces are rear-ranged frequently.

Wireless Extensions to Ethernet Networks

WLANs enable network managers in dynamic environments to minimize overhead caused by moves, extensions to networks, and other changes.

Wired LAN Backup

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

Mobility Within Training/Educational Facilities

Training sites at corporations and students at universities are a few examples where wireless connectivity can be used to facilitate access to information, information exchanges, and learning.

Technical Specifications

Wireless Specifications

- IEEE802.11b/g/n, 300Mbps
- 2.400 to 2.484 GHz

Hardware Specifications

- Physical Interface: 2 x 10/100Mbps LAN Ports, 1 x Reset Button
- Power Supply: Passive PoE, 24V/0.6A Power Adapter
- Dimension: D 190mm (7.48") x H 38mm (1.50")
- Operation Temperature: -4 °F to 140 °F , -20°C ~ 60°C
- Embedded High-Gain Directional Antenna
- IP55-Rated Enclosure

Software Specifications

- Operation Modes: Client Bridge, Access Point, Client Router, WDS AP, WDS Bridge, WDS Station
- Multiple SSIDs, Preferred SSID
- PPPoE, PPTP, L2TP Pass-through
- WMM, Traffic Shaping
- CLI Interface, SNMP v1/v2c/v3
- Recovery Page
- Port Forwarding/DMZ
- Narrow Bandwidth

1.3 Product Interface

Figure 1-1: Back Panel View

BACK PANEL VIEW		DESCRIPTION
A	LAN Port(PoE)	The PoE interface allows EnStation to be powered using the supplied PoE injector.
B	LAN Port	To configure EnStation, connect to an Ethernet adapter in a computer for accessing more information.
C	Reset Button	To reset to factory settings, press the button for more than 10 seconds.
D	Power LED	OFF=EnStation is not receiving power ON=EnStation is receiving power.
E	LAN(2) LEDs	OFF=EnStation is not connected to the network. ON=Enstation is connected to the network but not sending or receiving data.

BACK PANEL VIEW		DESCRIPTION
F	WAN LED	(Access Point or Client Bridge Mode) OFF=EnStation radio is off and the device is not sending or receiving data over the wireless LAN. ON=EnStation radio is on, and the device is not sending or receiving data over the wireless LAN. Blinking=EnStation radio is on, and the device is sending or receiving data over the wireless LAN.
G	Signal Indicator LED	(Client Bridge, WDS Station, and Client Router, Modes)

Installation

Chapter 2

2.1 System Requirements

To install the EnStation2, you need the following:

- Computer (Windows, Linux, Mac OS X Operating System)

- Web Browser (Internet Explorer, FireFox, Chrome, Safari)

- Network Interface equipped: (one of the following)

  - **Wired connectivity:** Network Interface with an open RJ-45 Ethernet Port

  - **Wireless Connectivity:**

    - Embedded 802.11n Wi-Fi wireless networking, IEEE 802.11b/g compatible

    - Wi-Fi Card, USB Wi-Fi Dongle (802.11 b/g/n)

- An existing router or access point (AP) with SSID broadcast

- 1x CAT5e Ethernet Cable

2.2 Installing the Device

Installing the EnStation2 on a pole or wall optimizes the wireless access range.

Note:
Only experienced installation professionals who are familiar with local building and safety codes and, wherever applicable, are licensed by the appropriate government regulatory authorities should install the EnStation2.

Pre-Installation Guidelines

Select the optimal location for the equipment using the following guidelines:

● The EnStation2 should be mounted on a 1"-4" pole. Its location should enable easy access to the unit and its connectors for installation and testing.

● The higher the placement of the antenna, the better the achievable link quality.

● The antenna should be installed to provide a direct, or near line of sight with the Base Station antenna. The antenna should be aligned to face the general direction of the Base Station.

Installing the Device

To install the EnStation2, use the following procedure to mount the device on a pole and refer to the figure below:

1. Remove the bottom cover protecting the RJ-45 connectors.

2. Insert an Ethernet cable into the RJ-45 port labeled LAN.

3. Install the bottom cover to protect the RJ-45 connectors.

4. Remove the power cord and PoE injector from the box and plug the power cord into the DC port of the PoE injector.

CAUTION!
ONLY USE THE POWER ADAPTER SUPPLIED WITH THE ENSTATION2. USING A DIFFERENT POWER ADAPTER MIGHT DAMAGE THE ENSTATION2.

5. Plug the other end of the Ethernet cable into the PoE port of the PoE injector.

Figure 2-1: Installing the EnStation2

6. Turn over the EnStation2. Then insert the pole mounting strap through the middle hole of the EnStation2. Use a screwdriver to unlock the pole-mounting ring putting it through the EnStation2.

7. Mount the EnStation2 securely to the pole by locking the strap tightly.

Wall Mounting the Device

A. Plug the dynamic stick into the bracket.

B. Combine the sealing nut with the assembled kit and tighten it.

C. Put the mock washer on the dynamic stick.

D. Assemble the mounting kit with the CPE.

E. Drill the holes 1.04"/26 mm holes and input the mounting screws.

F. Use the included screws to attach the mounting screws.

G. Use the hole of the bracket to aim for the screws on the wall. Hang and re-adjust the device as necessary.

Figure 2-2: Wall Mounting the Device

Pole Mounting the Device

A. Plug the dynamic stick into the bracket.

B. Combine the sealing nut with the assembled kit.
   Tighten to secure together.

C. Put the mock washer on the dynamic stick.

D. Assemble the mounting kit with the CPE.

E. Thread the open end of the pole strap through the two
   tabs on the bracket.

F. Lock and tighten pole strap to secure bracket to the pole.

Figure 2-3: Pole Mounting the Device

Web Configuration

Chapter 3

3.1 Logging In

The EnStation2 has a built-in Web Configurator that lets you manage the unit from any location using a Web browser that supports HTTP and has Javascript installed for your convenience.

After configuring the computer for TCP/IP using the procedure appropriate for your operating system, use that computer's Web browser to log in to the EnStation2 Web Configurator:

1. Launch your Web browser.

2. In the browser address bar, type **192.168.1.1** and press the Enter key.

Note:
If you changed the EnStation2 LAN IP address, enter the correct IP address.

Figure 3-1: Web Browser Address Bar

3. When the login screen appears, enter **admin** for the username in the top field and **admin** for the password in the bottom field.

Figure 3-2: Windows Security Login Dialog

4. Click `Login` to continue or `Reset` to abort the login.

You are now ready to use the instructions in the following chapters to configure the EnStation2.

Best Practices

Perform the following procedures regularly to make the EnStation2 more secure and manage the EnStation2 more effectively.

- **Change the Default Password:** Use a password that is not easy to guess and that contains different characters, such as numbers and letters. The EnStation2 username cannot be changed. For more information, see *Configuring Administrator Account.*

- **Backup the Configuration:** Be sure you know how to restore it. Restoring an earlier working configuration can be useful if the EnStation2 becomes unstable or crashes. If you forget your password, you will have to reset the EnStation2 to its factory default settings and lose any customized override settings you configured. However, if you back up an earlier configuration, you will not have to completely reconfigure the EnStation2. You can simply restore your last configuration. For more information, see *Configuring Backup/Restore Settings.*

Basic Network Settings

Chapter 4

4.1 System Status

View the summary of the current system status including system (hardware/software version, date/time), wired network (LAN) and wireless network (WLAN) information.

4.1.1 Using Save/Reload

Save and apply the settings shown in the Unsaved changes list, or cancel the unsaved changes and revert to the previous settings that were in effect.

4.1.2 Viewing System Information

Displays status information about the current operating mode:

System Information

Shows the general system information such as operating modes, system up time, firmware version, serial number, kernel version, and application version.

System Information

Device Name	ENSTATION2
Ethernet Main MAC Address	00:02:6F:EE:BB:BA
Ethernet Secondary MAC Address	00:02:6F:EE:BB:BA
Wireless MAC Address	00:02:6F:EE:BB:BA
Country	United States
Current Time	Tue Aug 5 18:56:33 UTC 2014
Firmware Version	1.5.8

LAN Settings

Shows Local Area Network settings such as the LAN IP address, Subnet Mask, and MAC address.

LAN Settings

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
DHCP Client	Disabled
IPv6 IP Address	None
IPv6 Link-Local Address	FE80::202:6FFF:FEEE:BBBA
IPv6 Default Gateway	
IPv6 Primary DNS	
IPv6 Secondary DNS	
RX(Packets)	42.7949 KB (437 PKts.)
TX(Packets)	340.152 KB (396 PKts.)

WAN Settings

Shows Wide Area Network settings such as the MAC address, connection type, connection status, LAN IP Address, Subnet Mask, Primary and Secondary DNS.

WAN Settings	
MAC Address	00:02:6F:E4:61:C0
Connection Type	DHCP
Connection Status	Down
IP Address	
IP Subnet Mask	255.255.255.0
Primary DNS	
Secondary DNS	
RX(Packets)	0 B (0 PKts.)
TX(Packets)	10.3838 KB (217 PKts.)

Current Wireless Settings

Shows wireless information such as frequency and channel. Since the EnStation2 supports multiple- SSIDs, information about each SSID, such as its ESSID and security settings, are displayed.

Current Wireless Settings	
Operation Mode	Client Router
Wireless Mode	IEEE 802.11b/g/n Mixed
Channel Bandwidth	20/40 MHz
Frequency/Channel	2.452 GHz (Channel 9)
Wireless Network Name (SSID)	AP SSID
Security	None
Distance	1 Km
RX(Packets)	0 B (0 PKts.)
TX(Packets)	10.3838 KB (217 PKts.)

4.1.3 Viewing the Wireless Client List

The Client List displays a list of clients associated to the EnStation2, along with the MAC addresses and signal strength for each client. To remove an SSID client from the list, click the button that appears in the Kick and Ban column. Click the `Refresh` button to update the Client List.

4.1.4 Viewing the System Log

The EnStation2 automatically logs events to internal memory.

Note:
The oldest events are deleted from the log when memory is full.

Click the `Refresh` button to update the Client List or the `Clear` button to remove all events.

4.1.5 Viewing the Connection Status

Displays the current status of the network. The WLAN information shown includes network type, SSID, BSSID, Connection Status, Wireless Mode, Current Channel, Security, Tx Data Rate, Current noise level, and Signal Strength.

Wireless

Network Type	Client Router
SSID	AP SSID
BSSID	N/A
Connection Status	N/A
Wireless Mode	N/A
Current Channel	N/A
Security	N/A
Tx Data Rates(Mbps)	N/A
Current noise level	N/A
Signal strength	N/A

The WAN information shown includes the MAC address, connection type, connection status, IP address, IP subnet mask, primary DNS and secondary DNS.

WAN

MAC Address	00:02:6F:E4:61:C0	
Connection Type	DHCP	Renew Release
Connection Status	Down	
IP Address		
IP Subnet Mask	255.255.255.0	
Primary DNS		
Secondary DNS		

Click the `Refresh` button to update the Client List or the `Clear` button to remove all events.

4.1.6 Viewing the DHCP Client Table

The DHCP Client table displays the clients that are associated to the EnStation2 through DHCP. The MAC addresses and signal strength for each client are also shown. Click the `Refresh` button to update the Client List.

4.1.7 Viewing the WDS Link List

The WDS Link List displays the clients that are associated to the EnStation2 through WDS. The MAC addresses, link status and signal strength for each client are also shown. Click the `Refresh` button to update the Client List.

4.2 System Setup

The following sections explain the features and functionality of the EnStation2 in access point mode, client bridge mode, WDS access point mode, WDS bridge mode, WDS station mode and client router mode.

4.2.1 Configuring Operation Mode

Set the primary function of the device by choosing the operation mode. The function that is selected affects which items are available in the main menu:

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 broadcasted to other devices.

Operation Mode

Use the radio button to select an operating mode.

Click `Save & Apply` to save changes or `Cancel` to abort.

4.2.2 Configuring IP Settings

From here you can configure the LAN settings for the EnStation2 using a static or dynamic IP address:

IP Network Settings

Configure the network connection type using either a static IP or dynamic IP.

IP Address

Enter the LAN IP address of the EnStation2.

Subnet Mask

Enter the Subnet mask of the EnStation2.

Default Gateway

Enter the default gateway of the EnStation2.

Primary DNS

Enter the primary DNS address of the EnStation2.

Secondary DNS

Enter the secondary DNS address of the EnStation2.

Use Link-Local Address

Click to enable a link-local address for the device.

IPv6 IP Address

Enter the IPv6 LAN IP address of the EnStation2.

IPv6 Subnet Prefix Length

Enter the IPv6 subnet prefix length of the EnStation2.

IPv6 Default Gateway

Enter the IPv6 default gateway of the EnStation2.

IPv6 Primary DNS

Enter the IPv6 primary DNS of the EnStation2.

IPv6 Secondary DNS

Enter the IPv6 secondary DNS of the EnStation2.

Click `Apply` to save the settings or `Cancel` to discard changes.

4.2.3 Configuring Spanning Tree Settings

Spanning Tree Status

Enables or disables the EnStation2 Spanning Tree function.

Bridge Hello Time

Specifies Bridge Hello Time, in seconds. This value determines how often the EnStation2 sends hello packets to communicate information about the topology throughout the entire Bridged Local Area Network.

Bridge Max Age

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

Bridge Forward Delay

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 looks at some traffic before participating.

Priority

Specifies the Priority number. Smaller numbers have greater priority over larger numbers.

Click `Accept` to confirm the changes or `Cancel` to cancel and return to previous settings.

Spanning Tree Settings

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

[Accept] [Cancel]

4.3 Router Setup

4.3.1 Configuring WAN Settings

Configure the WAN settings for the EnStation2 using a static or dynamic IP address, PPPoE or PPTP.

Static IP

Setting a static IP address allows an administrator to set a specific IP address for the router and guarantees that it can't be assigned a different address.

Account Name

Enter the account name provided by your ISP.

Domain Name

Enter the domain name provided by your ISP.

MTU

The maximum transmission unit (MTU) specifies the largest packet size permitted for an Internet transmission. The factory default MTU size for the static IP is 1500. The MTU size can be set between 576 and 1500.

IP Address

Enter the router's WAN IP address.

Subnet Mask

Enter the router's WAN Subnet mask.

Default Gateway

Enter the WAN gateway address.

Primary DNS

Enter the primary DNS server address.

Secondary DNS
Enter the secondary DNS server address.

Discard Ping on WAN

Check the box to enable pings to be recognized on the EnStation2 interface. Uncheck the box to disable the feature and block pings on the EnStation2 Wan interface.

Note: Pinging IP addresses is a common method used by hackers to test whether the IP address is valid. Blocking pings provides some extra security from hackers.

Click `Accept` to save the settings or `Cancel` to discard changes.

Dynamic IP

Dynamic IP addressing assigns a different IP address each time a device connects to an ISP service provider. The service is most commonly used by ISP cable providers.

Account Name

Enter the account name provided by your ISP.

Domain Name

Enter the domain name provided by your ISP.

MTU

The maximum transmission unit (MTU) specifies the largest packet size permitted for an internet transmission. The factory default MTU size for Dynamic IP is 1500. The MTU size can be set between 576 and 1500.

Get Automatically From ISP

Click the radio button to obtain the DNS automatically from the DHCP server.

Use These DNS Servers

Click the radio button to set up the Primary DNS and Secondary DNS servers manually.

Discard Ping on WAN

Check the box to enable pings to be recognized on the EnStation2 interface. Uncheck the box to disable the feature and block pings on the EnStation2 Wan interface.

Note: Pinging IP addresses is a common method used by hackers to test whether the IP address is valid. Blocking pings provides some extra security from hackers.

Click `Accept` to save the settings or `Cancel` to discard changes.

Point-to-Point Protocol over Ethernet (PPPoE)

Point-to-Point Protocol over Ethernet (PPPoE) is used mainly by ISPs that provide DSL modems to connect to the Internet.

MTU

Enter the maximum transmission unit (MTU). The MTU specifies the largest packet size permitted for an Internet transmission (PPPoE default: 1492). The MTU size can be set between 576 and 1492.

Login

Enter the username assigned by an ISP.

Password

Enter the password assigned by an ISP.

Service Name

Enter the service name of an ISP (optional).

Connect on Demand

Select the radio button to specify the maximum idle time. An Internet connection will disconnect when it reaches the maximum idle time, but it will automatically connect when a user tries to access the network.

Keep Alive

Select whether to keep the Internet connection always on, or enter a redial period once the internet lose it connection.

Get Automatically From ISP

Click the radio button to obtain the DNS automatically from the ISP.

Use These DNS Servers

Click the radio button to set up the Primary DNS and Secondary DNS servers manually.

Discard Ping on WAN

Check the box to enable pings to be recognized on the EnStation2 interface. Uncheck the box to disable the feature and block pings on the EnStation2 Wan interface.

Note: Pinging IP addresses is a common method used by hackers to test whether the IP address is valid.
Blocking pings provides some extra security from hackers.

Click `Accept` to save the settings or `Cancel` to discard changes.

Point-to-Point Tunnelling Protocol (PPTP)

The Point-to-Point Tunnelling Protocol (PPTP) is used in association with Virtual Private Networks (VPNs). There are two parts to a PPTP connection: the WAN interface settings and the PPTP settings.

MTU

Enter the maximum transmission unit (MTU). The MTU specifies the largest packet size permitted for an Internet transmission (PPPoE default: 1400). The MTU size can be set between 1200 and 1400.

IP Address

Enter the router's WAN IP address.

Subnet Mask

Enter the router's WAN subnet IP address.

Default Gateway

Enter the router's WAN gateway IP address.

PPTP Server

Enter the IP address of the PPTP server.

Username

Enter the username provided by your ISP.

Password

Enter the password provided by your ISP.

Connect on Demand

If you want the EnStation2 to end the Internet connection after it has been inactive for a period of time, select this option and enter the number of minutes you want that period of inactivity to last.

Keep Alive

If you want the EnStation2 to periodically check your Internet connection, select this option. Then specify how often you want the EnStation2 to check the Internet connection. If the connection is down, the EnStation2 automatically re-establishes your connection.

Get Automatically From ISP

Obtains the DNS automatically from ISP.
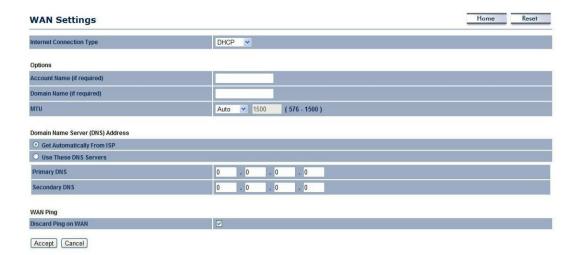
Use These DNS Servers
Click the radio button to set up the Primary DNS and Secondary DNS servers manually.

Discard Ping on WAN

Check the box to enable pings to be recognized on the EnStation2 interface. Uncheck the box to disable the feature and block pings on the EnStation2 Wan interface.

Note: Pinging IP addresses is a common method used by hackers to test whether the IP address is valid.
Blocking pings provides some extra security from hackers.

Click `Accept` to save the settings or `Cancel` to discard changes.

4.3.2 Configuring LAN Settings

IP Address

Enter the LAN IP address.

IP Subnet Mask

Enter the LAN IP Subnet mask.

WINS Server IP

Enter the WINS Server IP.

Use Router As DHCP Server

Check this option to enable the EnStation2 internal DHCP server.

Starting IP Address

Specify the starting IP address range for the pool of allocated for private IP addresses. The starting IP address must be on the same subnet as the ending IP address; that is the first three octets specified here must be the same as the first three octets in End IP Address.

Ending IP Address

Specifies the ending IP address range for the pool of allocated for private IP addresses. The ending IP address must be on the same subnet as the starting IP address; that is the first three octets specified here must be the same as the first three octets in Start IP Address.

WINS Server IP

Enter the IP address of the WINS server.

Click `Accept` to confirm the changes or `Cancel` to cancel and return to previous settings.

LAN Settings

LAN IP Setup

| IP Address | 192 . 168 . 1 . 153 |
| IP Subnet Mask | 255 . 255 . 255 . 0 |

☑ Use Router As DHCP Server

Starting IP Address	192 . 168 . 1 . 100
Ending IP Address	192 . 168 . 1 . 200
WINS Server IP	0 . 0 . 0 . 0

Accept   Cancel

4.3.3 Configuring VPN Pass-Through

VPN Pass-through allows a secure Virtual Private Network (VPN) connection between two computers.

PPTP Pass through

Check this option to enable PPTP Pass-through mode.

L2TP Pass-through

Check this option to enable L2TP Pass-through mode.

IPSec Pass-through

Check this option to enable IPSec Pass-through mode.

Click `Accept` to confirm the changes or `Cancel` to cancel and return to previous settings.

4.3.4 Configuring Port Forwarding

Port forwarding enables multiple server applications on a LAN to serve clients on a WAN over a single WAN IP address. The router accepts incoming client packets, filters them based on the destination WAN, or public port and protocol, and forwards the packets to the appropriate LAN, or local, port. Unlike the DMZ feature Port forwarding protects LAN devices behind the firewall.

Port Forwarding   Home   Reset

#	Name	Protocol	Start Port	End Port	Server IP Address	Enable	Modify	Delete

Add Entry   Accept

NO.

Displays the sequence number of the forwarded port.

Name

Displays the name of the forwarded port.

Protocol

Displays the protocol to use for mapping from the following: `TCP`, `UDP` or `Both`.

Start Port

Displays the LAN port number that WAN client packets will be forward to.

End Port

Displays the port number that the WAN client packets are under received.

Server IP

Displays the IP address of the server for the forwarded port.

Enable

Click to enable or disable the forwarded port profile.

Modify

Click to modify the forwarded port profile.

Delete

Click to delete the forwarded port profile. Click `Add Entry` to add

port forwarding rules. Click `Accept` to confirm the changes.

Port Forwarding

Service Name	
Protocol	BOTH
Starting Port	(1~65535)
Ending Port	(1~65535)
IP Address	. . .

Save | Cancel

Service Name

Enter a name for the port forwarding rule.

Protocol

Select a protocol for the application: Choices are Both, TCP, and UDP.

Starting Port

Enter a starting port number.

Ending Port

Enter an ending port number. All ports numbers between the starting and ending ports will forward users to the IP address specified in the IP Address field.

IP Address

Enter the IP address of the server computer on the LAN network where users will be redirected.

Click `Save` to apply the changes or `Cancel` to return to previous settings

4.3.5 Configuring Demilitarized Zone

Configuring a device on the LAN as a Demilitarized Zone (DMZ) host allows unrestricted two-way Internet access for Internet applications, such as online video games, to run from behind the NAT firewall. The DMZ function allows the router to redirect all packets going to the WAN port IP address to a particular IP address on the LAN. The difference between the virtual server and the DMZ function is that a virtual server redirects a particular service or Internet application, such as FTP, to a particular LAN client or server, whereas a DMZ redirects all packets regardless of the service, going to the WAN IP address to a particular LAN client or server.

> ⚠ **WARNING!**
> The PC defined as a DMZ host is not protected by the firewall and is vulnerable to malicious network attacks. Do not store or manage sensitive information on the DMZ host.

DMZ Hosting

Select `Enable DMZ` to activate DMZ functionality.

DMZ Address

Enter an IP address of a device on the LAN.

Click `Accept` to confirm the changes or `Cancel` to cancel and return to previous settings.

4.4 Configuring Wireless LAN

4.4.1 Configuring Wireless Settings

Below are the Instructions on how to configure the wireless and security settings for each of the possible operating modes:

⚠ **WARNING!**
Incorrectly changing these settings may cause the device to stop functioning. Do not modify the settings in this section without a thorough understanding of the parameters.

Access Point Mode

The EnStation2 supports Access Point Mode. In this mode, users with a wireless client device within range can connect to the EnStation2 to access the WLAN.

Wireless Mode

Wireless mode supports 802.11b/ g/n mixed modes.

Channel HT Mode

The default channel bandwidth is 20/40 MHz. The larger the channel, the better the transmission quality and speed.

Extension Channel

Select upper or lower channel. Your selection may affect the Auto Channel function.

Channel / Frequency

Select the channel and frequency appropriate.

Auto

Check this option to enable Auto Channel selection.

AP Detection

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

Current Profile

Configure up to four different SSIDs. If many client devices will be accessing the network, you can arrange the devices into SSID groups. Click Edit to configure the profile and check whether you want to enable extra SSIDs. Click Accept to confirm the changes or Cancel to cancel and return previous settings.

SSID

Specify the SSID for the current profile.

VLAN ID

Specify the VLAN tag for the current profile.

Suppressed SSID

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

Station Separation

Click the appropriate radio button to allow or prevent communication between client devices.

Wireless Security

See the Wireless Security section.

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

SSID Profile

Wireless Setting

SSID	EnGeniusE461C0	(1 to 32 characters)
VLAN ID	1	(1~4094)
Suppressed SSID	☐	
Station Separation	○ Enable	⦿ Disable

Wireless Security

Security Mode	Disabled	

Save Cancel

Client Bridge Mode

Client Bridge Mode lets you connect two LAN segments via a wireless link as though they are on the same physical network. Since the computers are on the same subnet, broadcasts reach all machines. As a result, DHCP information generated by the server reaches all client computers as though the clients as residing on one physical network.

Wireless Mode

Wireless mode supports 802.11b/ g/n mixed modes.

SSID

Specifies the SSID if known. This field is completed automatically if you select an Access Point in the Site Survey.

Site Survey

Scans nearby locations for Access Points. You can select a discovered Access Point to establish a connection.

Prefer BSSID

Enter the MAC address if known. If you select an Access Point in the Site Survey, this field is completed automatically.

Wireless Security

For details on wireless security settings, see *Configuring Wireless Security*. Click `Accept` to confirm the changes or `Cancel` to cancel and return to previous settings.

Profile If you used the Site Survey, the Web Configurator will show nearby Access Points. To connect to an Access Point, click the Access Point's BSSID.

Wireless Security See *Configuring Wireless Security*.

Click `Refresh` to scan again.

Site Survey

2GHz Site Survey   i:Infrastructure ✎:Ad_hoc

BSSID	SSID	Channel	Signal Level	Type	Security	Mode
08:10:74:96:17:04	DT-200N	6	-93 dBm	11g/n	none	i
00:16:01:93:C8:6F	00160193C86E	11	-81 dBm	11b/g	WEP	i
04:4F:AA:5B:88:C1	annie	1	-93 dBm	11b/g	WEP	i
02:2F:4F:42:BC:41	HPCP1525-9b886b	6	-91 dBm	11b/g	none	✎
90:E6:BA:BE:8A:46	james wifi	1	-84 dBm	11b/g	WPA/WPA2-PSK	i
F0:B4:79:06:0C:8D	AE	1	-96 dBm	11g/n	WPA2-PSK	i
00:19:70:22:05:96	NOVA Technical Institute	7	-55 dBm	11g/n	WPA2-PSK	i
4C:E6:76:43:1E:6B	mike	11	-79 dBm	11g/n	WPA-PSK	i
00:1F:1F:23:F9:F0	kao	11	-86 dBm	11g/n	WPA-PSK	i
34:08:04:DD:81:02	RouterforTecom	11	-83 dBm	11b/g	WPA/WPA2-PSK	i
5C:D9:98:E1:56:94	TW FlyKiwi	6	-94 dBm	11g/n	WPA/WPA2-PSK	i

[Refresh]

WDS Bridge Mode

Unlike traditional bridging, WDS Bridge Mode allows you to create large wireless networks by linking several wireless access points with WDS links. WDS is normally used in large, open areas where pulling wires is cost prohibitive, restricted or physically impossible.

Wireless Mode

Wireless mode supports 802.11b/g/n mixed modes.

Channel HT Mode

The default channel bandwidth is 40 MHz. The larger the channel, the better the transmission quality and speed.

Extension Channel

Select upper or lower channel. Your selection may affect the Auto Channel function.

Channel / Frequency

Select the appropriate channel and frequency.

Security
Select the type of WDS security: None, WEP, or AES.

WEP Key

Enter the WEP key.

AES Pass phrase

Enter the AES pass phrase.

Wireless Network

Wireless Mode	802.11 B/G/N Mixed
Channel HT Mode	40MHz
Extension Channel	Lower Channel
Channel / Frequency	Ch6-2.437GHz

Accept   Cancel

MAC Address

Enter the MAC address of the Access Point to which you want to extend wireless connectivity.

Mode

Select Disable or Enable to disable or enable WDS.

Click `Accept` to confirm the changes or `Cancel` to cancel and return to previous settings.

WDS Link Settings   [Home] [Reset]

Security	None
WEP Key		40/64-bit(10 hex digits)
AES Passphrase	
	(8-63 ASCII characters or 64 hexadecimal digits)

ID	MAC Address	Mode
1	__ : __ : __ : __ : __ : __	Disable
2	__ : __ : __ : __ : __ : __	Disable
3	__ : __ : __ : __ : __ : __	Disable
4	__ : __ : __ : __ : __ : __	Disable

[Accept] [Cancel]

Client Router Mode

In Client Router Mode, you can access the Internet wirelessly with the support of a WISP. In AP Router Mode, the EnStation2 can access the Internet via a cable or DSL modem. In this mode, the EnStation2 can be configured to turn off a wireless network name (SSID) broadcast, so that only stations that have the SSID can be connected. The EnStation2 also provides wireless LAN 64/128/156-bit WEP encryption security, WPA/WPA2, and WPA-PSK/WPA2-PSK authentication, as well as TKIP/AES encryption security. It also supports VPN pass-through for sensitive data secure transmission.

Wireless Mode

Wireless mode supports 802.11b/ g/n mixed modes.

SSID

Specifies the SSID if known. This field is completed automatically if you select an Access Point in the Site Survey.

Site Survey

Scans nearby locations for Access Points. You can select a discovered Access Point to establish a connection.

Prefer BSSID

Enter the MAC address if known. If you select an Access Point in the Site Survey, this field is completed automatically.

Wireless Security

See *Configuring Wireless Security*.

Click `Accept` to confirm the changes or `Cancel` to cancel and return to previous settings.

Profile

If you used the Site Survey, the Web Configurator shows nearby Access Points. To connect to an Access Point, click the Access Point's BSSID.

Wireless Security

See *Configuring Wireless Security*.

Click `Refresh` to scan again.

Site Survey

2GHz Site Survey   **i:Infrastructure** **:Ad_hoc**

BSSID	SSID	Channel	Signal Level	Type	Security	Mode
08:10:74:96:17:04	DT-200N	6	-93 dBm	11g/n	none	i
00:16:01:93:C8:6F	00160193C86E	11	-81 dBm	11b/g	WEP	i
04:4F:AA:5B:88:C1	annie	1	-93 dBm	11b/g	WEP	i
02:2F:4F:42:BC:41	HPCP1525-9b886b	6	-91 dBm	11b/g	none	🖉
90:E6:BA:BE:8A:46	james wifi	1	-84 dBm	11b/g	WPA/WPA2-PSK	i
F0:B4:79:06:0C:8D	AE	1	-96 dBm	11g/n	WPA2-PSK	i
00:19:70:22:05:96	NOVA Technical Institute	7	-55 dBm	11g/n	WPA2-PSK	i
4C:E6:76:43:1E:6B	mike	11	-79 dBm	11g/n	WPA-PSK	i
00:1F:1F:23:F9:F0	kao	11	-86 dBm	11g/n	WPA-PSK	i
34:08:04:DD:81:02	RouterforTecom	11	-83 dBm	11b/g	WPA/WPA2-PSK	i
5C:D9:98:E1:56:94	TW FlyKiwi	6	-94 dBm	11g/n	WPA/WPA2-PSK	i

[Refresh]

4.4.2 Configuring Wireless Security

The Wireless Security Settings section lets you configure the EnStation2's security modes: WEP, WPA-PSK, WPA2-PSK, WPA-PSK Mixed, WPA, WPA2, and WPA Mixed. We strongly recommend you use WPA2-PSK.

Wired Equivalent Privacy (WEP)

Security Mode

Select WEP from the drop-down list to begin the configuration.

Auth Type

Select Open System or Shared.

Input Type

Select an input type of Hex or ASCII.

Key Length

Level of WEP encryption applied to all WEP keys. Select a 64/128/152-bit password length.

Default Key

Specify which of the four WEP keys the EnStation2 uses as its default setting.

Key1 - Key4

Specify a password for the security key index. For more security, each typed character is masked by a dot.

Click Save to save the changes or Cancel to cancel and return to previous settings.

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

Wi-Fi Protected Access Pre-Shared Key (WPA-PSK)

Security Mode

Select WPA-PSK from the drop-down list to begin the configuration.

Encryption

Select Both, TKIP, or AES as the encryption type:

- Both = uses TKIP and AES.

- TKIP = automatic encryption with WPA-PSK; requires pass-phrase.

- AES = automatic encryption with WPA2-PSK; requires passphrase.

Passphrase

Specify the security password. For more security, each typed character is masked by a dot.

Group Key Update Interval

Specify how often, in seconds, the group key changes.

Click `Save` to save the changes or `Cancel` to cancel and return to previous settings.

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

Wi-Fi Protected Access 2 Pre-Shared Key (WPA2-PSK)

Security Mode

Select WPA2-PSK from the drop-down list to begin the configuration.

Encryption

Select Both, TKIP, or AES as the encryption type:

- Both = uses TKIP and AES.

- TKIP = automatic encryption with WPA-PSK; requires passphrase.

- AES = automatic encryption with WPA2-PSK; requires passphrase.

Passphrase

Specify the security password. For more security, each typed character is masked by a dot.

Group Key Update Interval

Specify how often, in seconds, the group key changes.

Click Save to save the changes or Cancel to cancel and return to previous settings.

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

Wi-Fi Protected Access Pre-Shared Key (WPA-PSK) Mixed

Security Mode

Select WPA2-PSK Mixed from the drop-down list to begin the configuration.

Encryption Select Both, TKIP, or AES as the encryption type:

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

- Both = uses TKIP and AES.

- TKIP = automatic encryption with WPA-PSK; requires pass-phrase.

- AES = automatic encryption with WPA2-PSK; requires passphrase.

Passphrase

Specify the security password. For more security, each typed character is masked by a dot.

Group Key Update Interval

Specify how often, in seconds, the group key changes.

Click `Save` to save the changes or `Cancel` to cancel and return to previous settings.

Note:
WPA-PSK Mixed can allow multiple security modes at the same time. 802.11n does not allow WEP/WPA-PSK TKIP/WPA2-PSK TKIP security modes. The connection mode will change from 802.11n to 802.11g to compensate.

Wi-Fi Protected Access (WPA)

Security Mode

Select WPA from the drop-down list to begin the configuration.

Encryption Select Both, TKIP, or AES as the encryption type.

- Both = uses TKIP and AES.

- TKIP = automatic encryption with WPA-PSK; requires passphrase.

- AES = automatic encryption with WPA2-PSK; requires passphrase.

Radius Server

Specify the IP address of the RADIUS server.

Radius Port

Specify the port number that your RADIUS server uses for authentication. The default port is 1812.

Radius Secret

Specify the RADIUS secret furnished by the RADIUS server.

Group Key Update Interval

Specify how often, in seconds, the group key changes.

Radius Accounting Select to enable or disable RADIUS accounting.

Radius Accounting Server

Specify the IP address of the RADIUS accounting server.

Radius Accounting Port

Specify the port number that your RADIUS accounting server uses for authentication. The default port is 1813.

Radius Accounting Secret

Specify RADIUS accounting secret furnished by the RADIUS server.

Interem Accounting Interval

Specify the interem accounting interval (60 ~600 seconds). Click Save to save the changes or

Cancel to cancel and return to previous settings.

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

Wi-Fi Protected Access 2 (WPA2)

Security Mode

Select WPA2 from the drop-down list to begin the configuration.

Encryption

Select Both, TKIP, or AES as the encryption type.

- Both = uses TKIP and AES:

- TKIP = automatic encryption with WPA-PSK; requires passphrase.

- AES = automatic encryption with WPA2-PSK; requires passphrase.

Radius Server

Specify the IP address of the RADIUS server.

Radius Port

Specify the port number that your RADIUS server uses for authentication. The default port is 1812.

Radius Secret

Specify the RADIUS secret furnished by the RADIUS server.

Group Key Update Interval

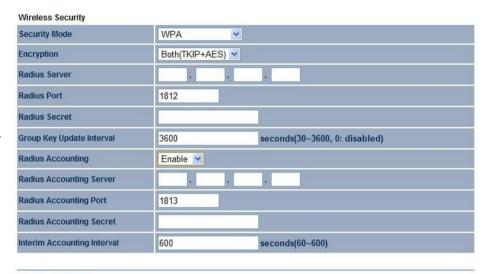Specify how often, in seconds, the group key changes.

Radius Accounting

Select to enable or disable RADIUS accounting.

Radius Accounting Server

Specify the IP address of the RADIUS accounting server.

Wireless Security		
Security Mode	WPA2	
Encryption	Both(TKIP+AES)	
Radius Server	. . .	
Radius Port	1812	
Radius Secret		
Group Key Update Interval	3600	seconds(30~3600, 0: disabled)
Radius Accounting	Enable	
Radius Accounting Server	. . .	
Radius Accounting Port	1813	
Radius Accounting Secret		
Interim Accounting Interval	600	seconds(60~600)

Save Cancel

Radius Accounting Port

Specify the port number that your RADIUS accounting server uses for authentication. The default port is 1813.

Radius Accounting Secret

Specify RADIUS accounting secret furnished by the RADIUS server.

Interem Accounting Interval

Specify the internet accounting interval. The range is from 60~600 seconds.

Click Save to save the changes or Cancel to cancel and return to previous settings.

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

Wi-Fi Protected Access (WPA) Mixed

Security Mode

Select WPA Mixed from the drop-down list to begin the configuration.

Encryption

Select Both, TKIP, or AES as the encryption type:

- Both = uses TKIP and AES.

- TKIP = automatic encryption with WPA-PSK; requires pass-phrase.

- AES = automatic encryption with WPA2-PSK; requires passphrase.

Radius Server

Specify the IP address of the RADIUS server.

Radius Port

Specify the port number that your RADIUS server uses for authentication. The default port is 1812.

Radius Secret

Specify the RADIUS secret furnished by the RADIUS server.

Group Key Update Interval

Specify how often, in seconds, the group key changes.

Radius Accounting

Select to enable or disable RADIUS accounting.

Radius Accounting Server

Specify the IP address of the RADIUS accounting server.

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

Save   Cancel

Radius Accounting Port

Specify the port number that your RADIUS accounting server uses for authentication. The default port is 1813.

Radius Accounting Secret

Specify RADIUS accounting secret furnished by the RADIUS server.

Interem Accounting Interval

Specify the interem accounting interval. The range is from 60 to 600 seconds.

Click Save to save the changes or Cancel to cancel and return to previous settings.

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

4.4.3 Configuring Wireless MAC Filter

Note:
This section applies to Access Point and WDS Access point modes only.

Wireless MAC Filters are used to allow or deny network access to wireless clients according to their MAC addresses. You can manually add a MAC address to restrict the permission to access EnStation2. The default setting is Disable Wireless MAC Filters.

ACL Mode

Determines whether network access is granted or denied to clients whose MAC addresses appear in the MAC Address table on this page. Choices are Disable, Deny MAC in the list, or Allow MAC in the list.

MAC Address Filter

Enter the MAC address of the device. Click `Add` to add the MAC address to the MAC Address table. Click `Apply` to apply the changes.

4.4.4 Configuring WDS Link Settings

Using WDS Link Settings, you can create a wireless backbone link between multiple access points that are part of the same wireless network. This allows a wireless network to be expanded using multiple Access Points without the need for a wired backbone to link them, as is traditionally required.

Security

Select the type of WDS security: None, WEP, or AES.

WEP Key

Enter the WEP key.

AES Passphrase

Enter the AES passphrase.

MAC Address

Enter the MAC address of the Access Point to which you want to extend wireless connectivity.

Mode

Select Disable or Enable to disable or enable WDS.

Click `Accept` to confirm the changes or `Cancel` to cancel and return to previous settings.

> **Note:**
> The Access Point to which you want to extend wireless connectivity must enter the EnStation2's MAC address into its configuration. For more information, refer to the documentation for the Access Point. Not all Access Point support this feature.

4.4.5 Configuring Advanced Network Settings

Configure the advanced wireless settings for your access point using the screens in this section. Leave these settings as their default values if you are not sure what values to enter.

Data Rate

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

Transmit Power

Lets you increase or decrease transmit power. Higher transmit power may prevent connections to the network, while a lower transmit power can prevent clients from connecting to the device.

Wireless Advanced Settings

Data Rate	Auto
RTS/CTS Threshold (1 - 2346)	2346 bytes
Distance (1-30km)	1 km
Aggregation:	Enable Disable 32 Frames 50000 Bytes(Max)

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.

Distance

Specifies the distance between Access Points and clients. Longer distances may drop high-speed connections.

Aggregation

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

Wireless Traffic Shaping

Wireless Traffic Shaping

Enable Traffic Shaping	○ Enable ● Disable
Incoming Traffic Limit	1000 kbit/s (512-99999999)
Outgoing Traffic Limit	180000 kbit/s (512-99999999)
Total Percentage	10 %
SSID #1 : EnGenius1	10 %
SSID #2 : (Off)	10 %
SSID #3 : (Off)	10 %
SSID #4 : (Off)	10 %

Enable Traffic Shaping

Enable or disable the regulation of packet flow leaving an interface for improved QoS.

Incoming Traffic Limit

Specifies the wireless transmission speed used for downloading.

Outgoing Traffic Limit

Specifies the wireless transmission speed used for uploading.

Total Percentage

Specifies the total percentage of the wireless traffic that is shaped.

SSID1 to SSID4

Specifies the percentage of the wireless traffic that is shaped for a specific SSID.

4.5 Management Setup

The Management section lets you configure administrative settings, management VLAN, SNMP settings, backup/restore settings, firmware upgrade, time settings, and log settings.

4.5.1 Configuring Administrator Account

Click the Administration link under the Management menu to change the user name and password used to log on to the EnStation2 Web Configurator. The default user name is `admin` and the default password is `admin`. Changing these settings protects the EnStation2 configuration settings from being accessed by unauthorized users.

New Name

Enter a new username for logging in to the Web Configurator.

New Password

Enter a new password for logging in to the Web Interface.

Confirm Password

Re-enter the new password for confirmation.

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

Remote Management

Enable or disable remote management.

Remote Upgrade

Specify whether the EnStation2 firmware can be upgraded remotely.

Remote Management Port

If remote management is enabled,
enter the port number to be used for remote management. For example: If you specify the port number 8080, enter `http://<IP address>:8080` to access the EnStation2 Web Configurator.

Click `Accept` to apply the changes or `Cancel` to return to previous settings.

4.5.2 Configuring Management VLAN

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

Management VLAN Settings   Home   Reset

Caution: If you reconfigure the Management VLAN ID, you may lose connectivity to the access point. Verify that the switch and DHCP server can support the reconfigured VLAN ID, and then re-connect to the new IP address.
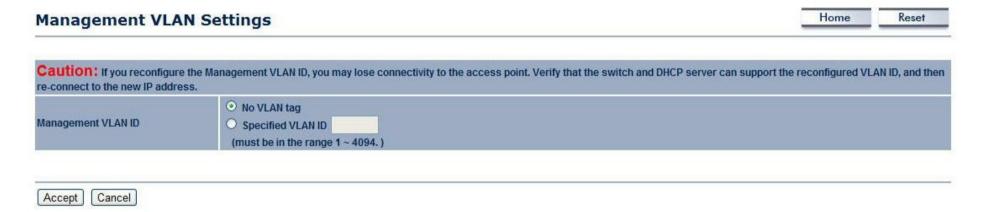
Management VLAN ID
- ⦿ No VLAN tag
- ○ Specified VLAN ID
  (must be in the range 1 ~ 4094.)

Accept   Cancel

Management VLAN ID

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

Click `Accept` to confirm the changes or `Cancel` to cancel and return previous settings.

Note:
If you reconfigure the Management VLAN ID, you may lose your connection to the EnStation2. Verify that the DHCP server supports the reconfigured VLAN ID and then reconnect to the EnStation2 using the new IP address.

4.5.3 Configuring SNMP

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

SNMP

Enable or disable the EnStation2 SNMP function.

Contact

Enter the contact details of the device.

Location

Enter the location of the device.

Community Name (Read Only)

Enter the password for accessing the SNMP community for read-only access.

Community Name (Read/Write)

Enter the password for accessing the SNMP community for read and write access.

Trap Destination Address

Enter the IP address where SNMP traps are to be sent.

Trap Destination Community Name

Enter the password of the SNMP trap community.

SNMPv3

Enable or Disable the SNMPv3 feature.

User Name

Specify the username for SNMPv3.

Auth Protocol

Select the authentication protocol type: MD5 or SHA.

Auth Key (8-32 Characters)

Specify the authentication key for authentication.

Priv Protocol

Select the privacy protocol type: DES.

Priv Key (8-32 Characters)

Specify the privacy key for privacy.

Engine ID Specify the engine ID for SNMPv3.

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

4.5.4 Configuring Backup/Restore Settings

Click the Backup/Restore Settings link under the Management menu to save the EnStation2's current settings in a file on your local disk or load settings onto the device from a local disk. This feature is particularly convenient for administrators who have several EnStation2 devices that need to be configured with the same settings. This page also lets you return the EnStation2 to its factory default settings. If you perform this procedure, any changes made to the EnStation2's custom configuration will be lost.

Save A Copy of Current Settings

Click `Backup` to save the current configured settings.

Restore Saved Settings from A File

To restore settings that have been previously backed up, click `Browse`, select the file, and click `Restore`.

Revert to Factory Default Settings

Click `Factory Default` to restore the EnStation2 to its factory default settings.

4.5.5 Configuring Auto Reboot Settings

Click the Auto Reboot Settings link under the Management menu to enable or disable the Auto Reboot function. This feature is particularly convenient to administrators for the scheduling of auto rebooting the device. This page also allows you to set the frequency of this function.

Auto Reboot Setting

Select `Enable` from the drop-down menu to setup this function.

Frequency of Auto Reboot

Select the frequency interval using the drop-down menus.

Save/Apply

Click `Save/Apply` to set the new configuration.

Cancel

Click `Cancel` to delete the settings.

4.5.6 Configuring Firmware Upgrade

Firmware is system software that operates and allows the administrator to interact with the router device.

⚠️ **WARNING!**
Upgrading firmware through a wireless connection is not recommended. Firmware upgrading must be performed while connected to an Ethernet (LAN port) with all other clients disconnected.

The firmware upgrade procedure can take several minutes. Do not power off the EnStation2 during the firmware upgrade, as it can cause the device to crash or become unusable.

To update the firmware version, follow these steps:

1. Download the appropriate firmware approved by EnGenius Networks from an approved web site, such as the engeniusnetworks.com.

📝 **Note:**
Save the firmware file to a local hard drive.

2. Click `Choose File`.

3. Browse the file system and select the firmware file.

4. Click `Upload`.

5. The EnStation2 restarts automatically after the upgrade completes.

Firmware Upgrade

Current firmware version: 1.1.13

Locate and select the upgrade file from your hard disk:

Choose File No file chosen

Upload

4.5.7 Configuring System Time

Change the system time of the EnStation2 by manually entering the information, synchronizing the device with a PC, or setting up automatic updates through a network time (NTP) protocol server:

Manually Set Date and Time

Enter the date and time values in the date and time fields or click the `Synchronize with PC` button to get the date and time values from the administrator's PC.

Automatically Get Date and Time

Select a time zone from the drop-down list and check whether you want to enter the IP address of an NTP server or use the default NTP server.

Enable Daylight Saving

Click to enable or disable daylight savings time. Select the start and stop times from the `Start Time` and `Stop Time` drop-down lists.

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

4.5.8 Configuring Wi-Fi Schedule

Use the Wi-Fi schedule function to control the wireless power ON/OFF service that operates on a routine basis.

Add a Schedule Service

Create a schedule service type and date/time parameters for a specific service.

Schedule Name

Enter the description of the schedule service.

Service

Select the type of schedule service, either
`Wireless Power ON` or `Wireless Power OFF`.

Day

Select the days of the week to enable the schedule service.

Time of Day

Set the start time that the service is active.

Click `Add` to append the schedule service to the schedule service table, or `Cancel` to discard changes.

Wifi Schedule

Wifi Schedule	Disable ▾
Schedule Name	
Service	⦿ Wireless Power ON ○ Wireless Power OFF
Day	Mon ▾
Time of day	___ : ___ (use 24-hour clock)

[Add] [Cancel]

Schedule Services Table

The Schedule function relies on the GMT time setting acquired from a network time protocol (NTP) server. For details on how to connect the EnStation2 to an NTP server, see *Configuring System Time*.

Scedule Table

#	Name	Service	Schedule	Select

Delete Selected Delete All Reset

Accept Cancel

Schedule Table

Displays a list of scheduled services for the EnStation2. The properties of each service displayed are:

Displays the ID number of the service in the table.

Name

Displays the description of the service.

Service

Displays the type of service, either `Wireless Power ON` or `Wireless Power OFF`.

Schedule

Displays the schedule information of when the service is active.

Select

Select one or more services to edit or delete.

Click `Delete Selected` to delete the selected services or `Delete All` to delete all services. Click `Apply` to save the settings or `Cancel` to discard changes.

4.5.9 Configuring Command Line Interface

Most users will configure the EnStation2 through the graphical user interface (GUI). However, for those who prefer an alternative method there is the command line interface (CLI). The CLI can be access through a command console, modem or Telnet connection.

CLI

Select to enable or disable the ability to modify the EnStation2 via a command line interface (CLI).

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

4.5.10 Configuring Logging

The Log section displays a list of events that are triggered on the EnStation2 Ethernet and wireless interfaces. You can consult this log if an unknown error occurs on the system or when a report needs to be sent to the technical support department for debugging purposes.

Syslog

Enable or disable the EnStation2 Syslog function.
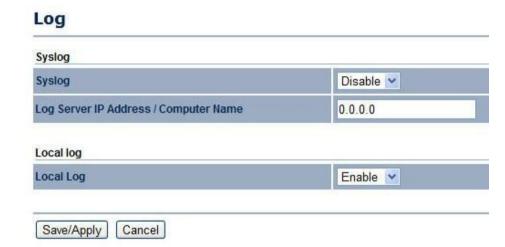
Log Server IP Address

Enter the IP address of the log server.

Local Log

Enable or disable the Local Log service.

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

Log

Syslog

Syslog	Disable
Log Server IP Address / Computer Name	0.0.0.0

Local log

Local Log	Enable

Save/Apply   Cancel

4.5.11 Configuring Diagnostics

The Diagnosis feature allows the administrator to verify that another device is available on the network and is accepting request packets. If the ping result returns `alive`, it means a device is online. This feature does not work if the target device is behind a firewall or has security software installed.

Target IP / Domain Name

Enter the IP address you would like to search.

Ping Packet Size

Enter the packet size of each ping.

Number of Pings

Enter the number of times you want to ping.

Start Ping

Click `Start Ping` to begin pinging.

Trace route target

Enter an IP address or domain name you want to trace.

Start Traceroute

Click `Start Traceroute` to begin the traceroute operation.

Target Address

Enter the IP address of the target PC.

Time period

Enter the time period for the speed test.

Diagnostics

Ping Test Parameters

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

Start Ping

Traceroute Test Parameters

Traceroute target	

Start Traceroute

Speed Test

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

Start Speed Test

Check Interval

Enter the interval for the speed test.

Start Speed Test

Click `Start Speed Test` to begin the speed test operation.

IPv4 Port

Displays the IPv4 port number of the EnStation2.

IPv6 Port

Displays the IPv6 port number of the EnStation2.

4.5.12 Viewing Device Discovery

Device Name

Displays the name of the devices connected to the network.

Operation Mode

Displays the operation mode of the devices connected to the network.

IP Address

Displays the IP address of the devices connected to the network.

System MAC Address

Displays the system MAC address of the devices connected to the network.

Firmware Version

Displays the firmware version of the devices connected to the network.

4.5.13 Configure Denial of Service Protection

Use TCP SYN Cookies Protection

Click to enable TCP SYN cookies protection.

SYN Flood Attack Protection

Click to enable or disable SYN Flood Attack Protection.

Match Interval Per Second

Enter the allowed number of packets per second.

Limit Packets

Enter the maximum number of packets allowed per request.

UDP Flood Attack Protection

Click to enable or disable UDP Flood Attack Protection.

Match Interval Per Second

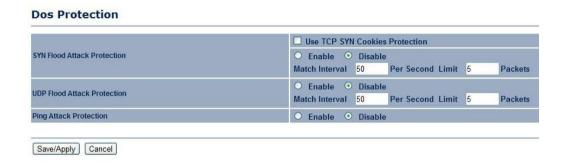Enter the allowed number of packets per second.

Limit Packets

Enter the maximum number of packets allowed per request.

Ping Attack Protection

Click to enable or disable ping attack protection.

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

4.5.14 Logging Out

Click Logout to logout from the EnStation2.

Appendix A

Federal Communication Commission Interference Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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

- Reorient or relocate the receiving antenna.

- Increase the separation between the equipment and receiver.

- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 24cm between the radiator & your body.

Appendix B

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

C€0560

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

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

Appendix C

WorldWide Technical Support

REGION/COUNTRY OF PURCHASE	SERVICE CENTRE		SERVICE INFORMATION
Canada	CANADA	web site	www.engeniuscanada.com
		email	rma@engeniuscanada.com
		contact numbers	Toll Free: (+1) 888-397-2788 Local: (+1) 905-940-8181
		hours of operation	Monday - Friday 9:00AM to 5:30PM EST (GMT-5)
USA	LOS ANGELES, USA	web site	www.engeniustech.com
		email	support@engeniustech.com
		contact numbers	Toll Free: (+1) 888-735-7888 Local: (+1) 714-432-8668
		hours of operation	Monday - Friday 8:00 AM to 4:30 PM PST (GMT-8)

REGION/COUNTRY OF PURCHASE	SERVICE CENTRE	SERVICE INFORMATION	
Mexico, Central and Southern America	MIAMI, USA	web site	[ES] es.engeniustech.com [PT] pg.engeniustech.com
		email	miamisupport@engeniustech.com
		contact numbers	Miami: (+1) 305-887-7378 Sao Paulo, Brazil: (+55)11-3957-0303 D.F., Mexico:(+52)55-1163-8894
		hours of operation	Monday - Friday 8:00 AM to 5:30PM EST (GMT-5)
Europe	NETHERLANDS	web site	www.engeniusnetworks.eu
		email	support@engeniusnetworks.eu
		contact numbers	(+31) 40-8200-887
		hours of operation	Monday - Friday 9:00 AM - 5:00 PM (GMT+1)
Africa Middle East Russia CIS / Armenia, Azerbaijan, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Moldova, Tajikistan, Turkmenistan, Ukraine, Uzbekistan Turkey Afghanistan Pakistan Bangladesh, Maldives, Nepal, Bhutan, Sri Lanka	DUBAI, UAE	web site	www.engenius-me.com
		email me.com	support@engenius-
		contact numbers	Toll Free: U.A.E.: 800-EnGenius 800-364-364-87 General: (+971) 4357-5599
		hours of operation	Sunday - Thursday 9:00 AM - 6:00 PM (GMT+4)

REGION/COUNTRY OF PURCHASE	SERVICE CENTRE		SERVICE INFORMATION
Singapore, Cambodia, Indonesia, Malaysia, Thailand, Philippines, Vietnam China, Hong Kong, Korea India South Africa Oceania	SINGAPORE	web site	www.engeniustech.com.sg/e_warranty_form
		email	techsupport@engeniustech.com.sg
		contact numbers	Toll Free: Singapore: 1800-364-3648
		hours of operation	Monday - Friday 9:00 AM - 6:00 PM (GMT+8)
Others	TAIWAN, R.O.C.	web site	www.engeniusnetworks.com
		email	technology@senao.com

Note:

* Service hours are based on the local time of the service center.

* Please visit the website for the latest information about customer service.