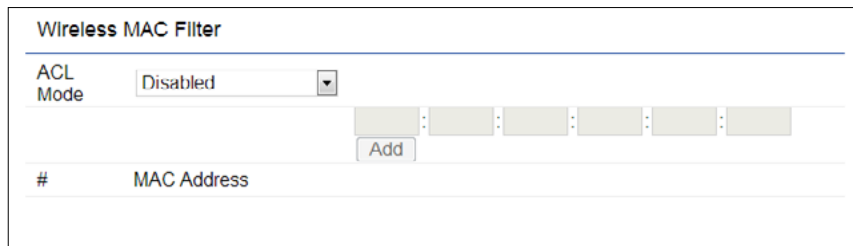


Wireless MAC Filtering

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

Note: Only applicable in Access Point and WDS AP modes.



The image shows a web-based configuration interface for 'Wireless MAC Filter'. At the top, the title 'Wireless MAC Filter' is displayed. Below it, there is a section for 'ACL Mode' with a dropdown menu currently set to 'Disabled'. To the right of the dropdown is a row of six input fields for a MAC address, each followed by a colon. Below this row is an 'Add' button. At the bottom, there is a table with a single header row containing a '#' symbol and the text 'MAC Address'.

ACL Mode: Determines whether network access is granted or denied to clients whose MAC addresses appear in the MAC address table on this page. Your choices are: Disabled, Deny MAC in the list, or Allow MAC in the list.

MAC Address: Enter the MAC address of the wireless client.

Add: Click **Add** to add the MAC address to the MAC address table.

Delete: Delete the selected entries.

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

Wireless Advanced

Wireless Traffic Shaping

Traffic shaping regulates the flow of packets leaving an interface to deliver improved Quality of Service. The function will allow administrators to restrict the wireless bandwidth per SSID.

Wireless Traffic Shaping	
Enable Traffic Shaping	Disable ▾
Download Limit	100 Mbps (1-999)
Upload Limit	100 Mbps (1-999)

Enable Traffic Shaping: Check this option to enable Wireless Traffic Shaping.

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

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

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

WPA-PSK (WPA Pre-Shared Key) Encryption:

Wireless Security - 5GHz	
Security Mode	WPA2-PSK ▾
Encryption	Both(TKIP+AES) ▾
Passphrase	
Group Key Update Interval	3600

Encryption: Select the WPA encryption type you would like. Please ensure that your wireless clients use the same settings.

Passphrase: Wireless clients must use the same Key to associate the device. If using 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: Specifies how often, in seconds, the Group Key changes.

WPA Mixed-Enterprise: Access Point / WDS AP mode

Wireless Security - 5GHz

Security Mode	WPA Mixed-Enterprise ▾
Encryption	Both(TKIP+AES) ▾
Group Key Update Interval	3600
Radius Server	
Radius Port	1812
Radius Secret	
Radius Accounting	Disable ▾
Radius Accounting Server	
Radius Accounting Port	1813
Radius Accounting Secret	
Interim Accounting Interval	600

Encryption: Select the WPA encryption type you would like. Please ensure that your wireless clients use the same settings.

Radius Server: Enter the IP address of the Radius server.

Radius Port: Enter the port number used for connections to the Radius server.

Radius Secret: Enter the secret required to connect to the Radius server.

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

Radius Accounting: Enable or disable accounting feature.

Radius Accounting Server: Enter the IP address of the Radius accounting server.

Radius Accounting Port Enter the port number used for connections to the Radius accounting server.

Radius Accounting Secret: Enter the secret required to connect to the Radius accounting server.

Interim Accounting Interval: Specifies 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 802.11a.

WDS Link Settings

Using the WDS (Wireless Distribution System) feature will allow a network administrator or installer to connect to Access Points wirelessly. Doing so will extend the wired infrastructure to locations where cabling is not possible or inefficient to implement.

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

Also note: All Access Points in the WDS network need to use the same Channel and Security settings.

To create a WDS network, please enter the MAC addresses of the Access Points that you want included in the WDS. There can be a maximum of four Access Points.

Note: Only applicable in WDS AP and WDS Bridge modes.

WDS Link Settings

WDS Link Settings - 5GHz		
Security		None
AES Passphrase		(8-63 ASCII characters or 64 hexadecimal digits)
ID	MAC Address	Mode
1		Disable
2		Disable
3		Disable
4		Disable

Security: Select **None** or **AES** from the drop-down list.

AES Passphrase: Enter the Key Values you wish to use. Other Access Points must use the same Key to establish a WDS link.

MAC Address: Enter the Access Point's MAC address to where you want to extend the wireless area.

Mode: Select to disable or enable from the drop-down list.

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

Client Bridge/WDS Station Settings

Save: Click Save to accept the changes

Wireless Settings - 5GHz

No.	SSID	Edit	Security
AP SSID	AP SSID_5G	Edit	None

No.: Display the setting value

SSID: You can click **scan** under AP detection to search perform the AP detection to select the proper SSID.

Edit: Click it to implement the advanced settings

Wireless Setting - 5GHz

Preferred BSSID

SSID

Wireless Security - 5GHz

Security Mode

Save current setting(s)

Prefer BSSID: You can insert the prefer BSSID or enter the specific SSID to be associated with the Access Point.

SSID: You can implement the AP detection to select the proper SSID.

Security Mode: Select the correct security mode and insert the correct encryption type. Please refer the wireless security section in page 42.

Guest Network Settings

Adding a guest network allows visitors to use the Internet without giving out your office or company wireless security key. You can add a guest network to each wireless network in the 5 GHz ac/a/n frequencies.

Guest Network Settings ⓘ

Enable	SSID	Edit	Security	Hidden SSID	Client Isolation
☐	EnGenius-5GHz_GuestNetwork	Edit	None	☐	☒

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

SSID: Specifies the SSID 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.

IP Address: The IP Address of this device.

Subnet Mask: The IP Subnet mask of this device.

Starting IP Address: The first IP Address in the range of the addresses by the DHCP server.

Ending IP Address: The last IP Address in the range of addresses assigned by the DHCP server.

RSSI Threshold

RSSI Threshold ⓘ

Status	☐ Enable ☒ Disable
RSSI	-85 dBm (Range: -60dBm ~ -100dBm)

RSSI Threshold: Enable the Fast Handover feature by ensuring that each client is served by at least one Access Point at any time. Access Points continuously monitor the connectivity quality of any client in their range and efficiently share this information with other Access Points in the vicinity of that client to coordinate which of them should serve the client best.

RSSI: Enter the RSSI (Received Signal Strength Index) in order to determine the handover procedure which the current wireless link will terminate. RSSI is an indication of the power level being received by the antenna. Therefore, the higher the RSSI number, the stronger the signal.

Chapter 7

Management



Management VLAN Settings

This page allows you to assign a VLAN tag to packets sent over the network. 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.

Note: Only applicable in Access Point and WDS AP modes.

Management VLAN Settings	
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	Enable ☐ 4096

Management VLAN: If your network includes VLANs, you can enable **Management VLAN ID** for packets passing through the Access Point with a tag.

Save: Click **Save** to confirm the changes or **Cancel** to cancel and return to previous settings.

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

Advanced Settings

SNMP Settings

This page allows you to assign the Contact Details, Location, Community Name, and Trap Settings for a Simple Network Management Protocol (SNMP). SNMP 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.

SNMP Settings	
Status	Enable
Contact	
Location	
Port	161
Community Name (Read Only)	public
Community Name (Read Write)	private
Trap Destination	
- Port	162
- IP Address	
- Community Name	public
SNMPv3 Settings	
- Status	Enable
- Username	admin (1-31 Characters)
- Authorized Protocol	MD5
- Authorized Key	12345678 (8-32 Characters)
- Private Protocol	DES
- Private Key	12345678 (8-32 Characters)
- Engine ID	

SNMP Enable/Disable: Enables or disables the SNMP feature.

Contact: Specifies the contact details of the device.

Location: Specifies the location of the device.

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 IP address of the computer that will receive the SNMP traps.

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

SNMPv3: Enables or disables the SNMPv3 feature.

User Name: Specifies the username for SNMPv3.

Auth Protocol: Selects the authentication protocol type: MDS or SHA.

Auth Key: Specifies the authentication key.

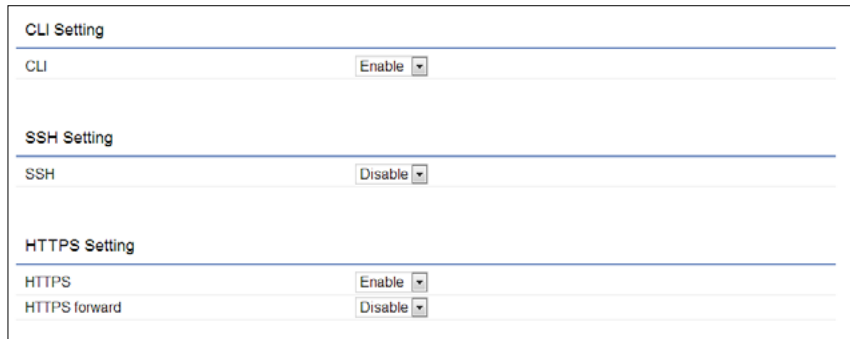
Priv Protocol: Selects the privacy protocol type: DES.

Priv Key: Specifies the privacy key for privacy.

Engine ID: Specifies the engine ID for SNMPv3.

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

CLI Settings



The CLI Settings configuration interface is divided into three sections: CLI Setting, SSH Setting, and HTTPS Setting. Each section contains a label and a dropdown menu. In the CLI Setting section, the CLI dropdown is set to 'Enable'. In the SSH Setting section, the SSH dropdown is set to 'Disable'. In the HTTPS Setting section, the HTTPS dropdown is set to 'Enable' and the HTTPS forward dropdown is set to 'Disable'.

CLI Setting	
CLI	Enable

SSH Setting	
SSH	Disable

HTTPS Setting	
HTTPS	Enable
HTTPS forward	Disable

CLI: The Command Line Interface (CLI) allows you to type commands instead of choosing them from a menu or selecting an icon.

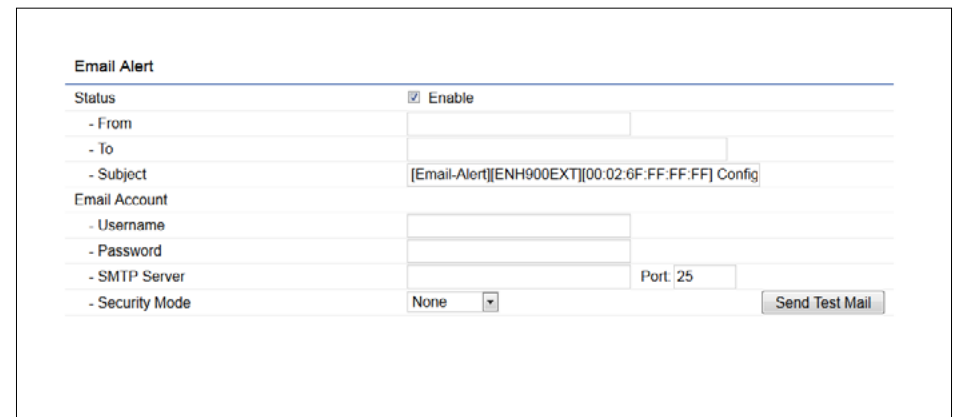
SSH: Enable Secure Shell (SSH) to make secure, encrypted connections in the network. Secure Shell is a network protocol that allows data to be exchanged using a secure channel between two network devices.

HTTPS: Enable HTTPS to transfer and display web content securely. The Hypertext Transfer Protocol over SSL (Secure Socket Layer) is a TCP/IP protocol used by web servers to transfer and display web content securely.

Email Alert

You can use the Email Alert feature to send messages to the configured email address when particular system events occur.

Note: Do **NOT** use your personal email address as it can unnecessarily expose your personal email login credentials. Use a separate email account made for this feature instead



The Email Alert configuration interface includes a 'Status' section with an 'Enable' checkbox checked. Below this are fields for '- From', '- To', and '- Subject'. The '- Subject' field contains the text '[Email-Alert][[ENH900EXT]][00:02:6F:FF:FF:FF] Config'. The 'Email Account' section contains fields for '- Username', '- Password', '- SMTP Server', and '- Security Mode'. The '- SMTP Server' field is followed by a 'Port' field set to '25'. The '- Security Mode' dropdown is set to 'None'. A 'Send Test Mail' button is located at the bottom right of the form.

Email Alert	
Status	☒ Enable
- From	
- To	
- Subject	[Email-Alert][[ENH900EXT]][00:02:6F:FF:FF:FF] Config
Email Account	
- Username	
- Password	
- SMTP Server	
- Security Mode	None
Port	25
Send Test Mail	

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

To: Enter the address that you wish to send emails to.

Subject: Enter the text that you wish to appear in the email's subject line.

Username: Enter the username for the email account that will be used to send emails.

Password: Enter the password for the email account that will be used to send emails.

SMTP Server: Enter the IP address or hostname of the outgoing SMTP server.

Port: Enter the SMTP port number to use for outbound emails.

Time Zone

Time Setting

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

Start: Select the day, month, and time when daylight savings time starts.

End: Select the day, month, and time when daylight savings times ends.

The screenshot shows the 'Date and Time Settings' section with two radio buttons: 'Manually Set Date and Time' (selected) and 'Automatically Get Date and Time'. Under manual settings, there are input fields for Date (2013 / 09 / 25) and Time (08 : 10 (24-Hour)), along with a 'Synchronize with PC' button. The 'Automatically Get Date and Time' section shows an 'NTP Server' field with the value '209.81.9.7'.

Below this is the 'Time Zone' section, which includes a dropdown menu currently set to 'UTC+00:00 Gambia, Liberia, Morocco'. There is an unchecked checkbox for 'Enable Daylight Saving'. When enabled, it would show 'Start' and 'End' settings, each with dropdowns for month, day, and time.

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

Automatically Get Date and Time: Select and check whether you wish to enter the IP address of an NTP server or use the default NTP server to have the internal clock set automatically.

Enable Daylight Saving: Check whether daylight savings applies to your area.

Auto Reboot Settings

You can specify how often you wish to reboot the EnStationAC.

Auto Reboot Setting	
Auto Reboot Status	Disable
Timer	☐ Sunday ☐ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday ☐ Friday ☐ Saturday
	0 : 0

Auto Reboot Setting: Enables or disables the Auto Reboot function.

Frequency of Auto Reboot: Specifies how often you wish to reboot the EnStationAC by Min, Hour, Day or Week.

Timer: Select the day and enter the time you would like to reboot automatically.

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

Wi-Fi Scheduler

The Wi-Fi Scheduler can be created for use in enforcing rules. For example, if you wish to restrict web access to Mon-Fri from 3pm to 8pm, you could create a schedule selecting Mon, Tue, Wed, Thu and Fri while entering a Start time of 3pm and End Time of 8pm to limit access to these times.

WiFi Scheduler

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

EnGenius3A9ADB_1-5GHz

Schedule Templates

Choose a template

Schedule Table

Day	Availability	Duration						
Sunday	available	00	:	00	~	24	:	00
Monday	available	00	:	00	~	24	:	00
Tuesday	available	00	:	00	~	24	:	00
Wednesday	available	00	:	00	~	24	:	00
Thursday	available	00	:	00	~	24	:	00
Friday	available	00	:	00	~	24	:	00
Saturday	available	00	:	00	~	24	:	00

drop-down list.

Day(s): Place a checkmark in the boxes for the desired days or select the **All Week** radio button to select all seven days of the week.

Duration: The Start Time is entered in two fields. The first box is for hours and the second box is for minutes. The End Time is entered in the same format as the Start time.

Status: Enables or disables the Wi-Fi scheduler function.

Wireless Radio: Select 2.4 GHz or 5 GHz from the drop-down list for the preferred band type.

SSID Selection: Select a SSID from the drop-down list.

Schedule Templates: Select a schedule template from the

Tools

Ping Test Parameters

This page allows you to analyze the connection quality of the EnStationAC and trace the routing table to a target in the network.

Ping Test Parameters

Target IP / Domain Name

Ping Packet Size

64

Bytes

Number of Pings

4

Start

Target IP: Enter the IP address you would like to search.

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

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

Traceroute Test Parameter

Traceroute Test Parameters

Target IP / Domain Name

Start

Stop

Target IP: Enter the IP address you would like to trace

Speed Test Parameters

Speed Test Parameters

Target IP / Domain Name

Time Period

20

sec

Check Interval

5

sec

Start

IPv4 Port

5001

IPv6 Port

5002

Target IP: Enter the IP address you would like to test.

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

Traceroute Target: Enter the IP address or domain name you wish to trace.

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

Device Discovery

This page allows you to discover devices from network for Operation Mode, IP Address, System MAC Address and Firmware version.

Device Discovery

Device Name	Operation Mode	IP Address	System MAC Address	Firmware Version
Scan				

Account

This page allows you to change the EnStationAC username and password. 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

Account Settings

Administrator Username	admin
Current Password	
New Password	
Verify Password	

Apply

Apply saved settings to take effect

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

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

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

Firmware

Firmware Upgrade

This page allows you to upgrade the firmware of the EnStationAC.

Firmware Upgrade

Current Firmware Version: 2.0.0

Select the new firmware from your hard disk.

Browse...

No file selected.

Upload

To Perform the Firmware Upgrade:

1. Click the **Choose File** button and navigate the OS file system to the location of the upgrade file.
2. Select the upgrade file. The name of the file will appear in the Upgrade File field.
3. Click the **Upload** button to commence the firmware upgrade.

Note: The device is unavailable during the Firmware upgrade process and must restart when the upgrade is completed. Any connections to or through the device will be lost.

Backup/Restore

Backup/Restore Settings	
Factory Setting	
- Backup Setting	Export
- Restore New Setting	Browse... No file selected. Import
- Reset to Default	Reset
User Setting	
- Back Up Setting as Default	Backup
- Restore to User Default	Restore

Factory Setting

The function allows you to export the current device configurations. When you export your configurations, you also can reload the saved configurations into the device through the Restore Saved Settings from a file section. If extreme problems occur, or if you have set the EnStationAC incorrectly, you can use the Reset button in the Revert to Factory Default Settings section to restore all the configurations of the EnStationAC to the original default settings.

Backup Setting: Click **Export** to save the current configured settings.

Restore New Setting: To restore settings that have been previously backed up, click **Browse**, select the file, and click **Restore**.

Restore to Default: Click **Reset** button to restore the EnStationAC to its factory default settings.

User Setting

The function allows you to backup the current device configurations into the EnStationAC as the default value. If extreme problems occur, or if you have set the EnStationAC incorrectly, you can push the Reset button to revert all the configurations of the EnStationAC to the user default.

Back Up Setting as Default: Click **Backup** to backup the user settings you would like to the device's memory for the default settings.

Restore to User Default: Click **Restore** to restore user settings to the factory standard settings.

Note1: After setting the current settings as the default, you should click the **Restore to Default** on the web interface for reverting the settings into the factory default instead of pushing the reset button.

Note2: Please **write down** your account and password before saving. The user settings will now become the new default settings at the next successful login.

Log

System Log

The EnStationAC automatically logs (records) events of possible interest in its internal memory. To view the logged information, click the **Log** link under the System Manager menu. If there is not enough internal memory to log all events, older events are deleted from the log. When powered down or rebooted, the log will be cleared.

System Log

Status ☒ Enable ☐ Disable

Log type All

```
Aug 25 01:08:01 EnStationAC user.notice root: starting ntpclient
Aug 25 01:08:01 EnStationAC cron.info crond[3577]: crond: USER root pid 1105 cmd . /etc/t
Aug 25 01:07:01 EnStationAC user.notice root: starting ntpclient
Aug 25 01:07:01 EnStationAC cron.info crond[3577]: crond: USER root pid 1068 cmd . /etc/t
Aug 25 01:06:02 EnStationAC user.notice root: starting ntpclient
Aug 25 01:06:02 EnStationAC cron.info crond[3577]: crond: USER root pid 1031 cmd . /etc/t
Aug 25 01:05:02 EnStationAC user.notice root: starting ntpclient
Aug 25 01:05:01 EnStationAC cron.info crond[3577]: crond: USER root pid 994 cmd . /etc/hc
Aug 25 01:04:01 EnStationAC user.notice root: starting ntpclient
Aug 25 01:04:01 EnStationAC cron.info crond[3577]: crond: USER root pid 944 cmd . /etc/hc
```

Remote Log

This page allows you to setup the Remote Log functions for the EnStationAC.

Remote Log

Log Server IP Address 0.0.0.0

Syslog: Enables or disables the syslog function.

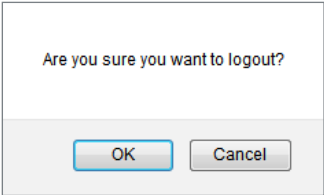
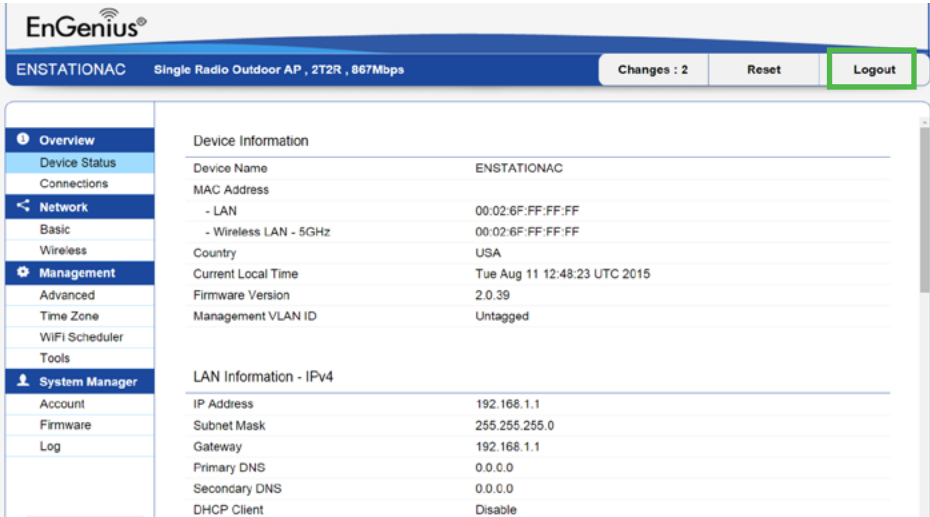
Log Server IP Address: Enter the IP address of the log server.

Remote Log: Enable or disable the remote log service.

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

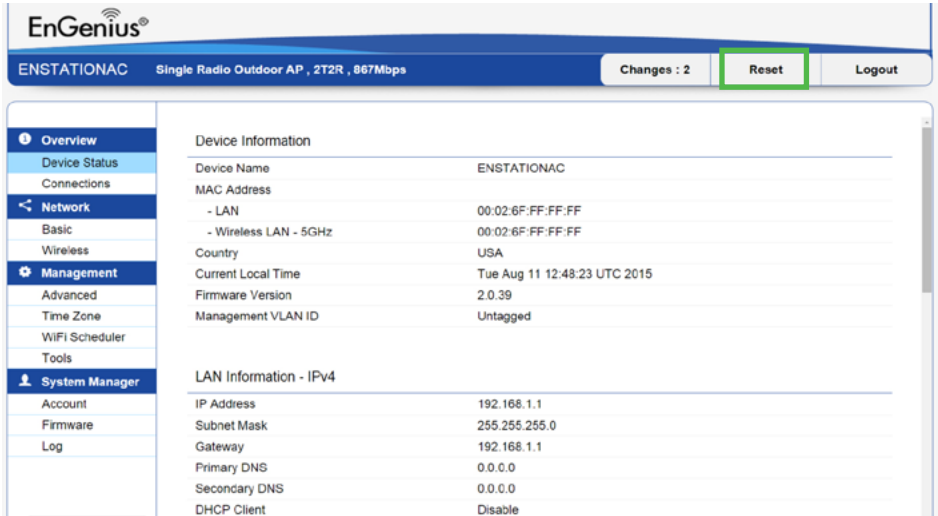
Logout

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



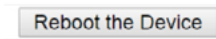
Reset

In some circumstances, it may be required to force the device to reboot. Click on **Reset** to reboot or to reset the EnStationAC.



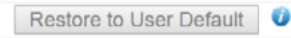
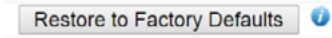
Reboot the Device

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



Restore the device to default settings

CAUTION: All settings will be cleared and reset to either factory default or user default.



Appendix



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.

IMPORTANT NOTE: **Radiation Exposure Statement**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 26 cm between the radiator & your body.

Appendix B - CE Interference Statement

Europe - EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

- **EN60950-1**

Safety of Information Technology Equipment

- **EN50385**

Generic standard to demonstrate the compliance of electronic and electrical apparatus with the basic restrictions related to human exposure to electromagnetic fields (0 Hz - 300 GHz)

- **EN 300 328**

Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive

- **EN 301 893**

Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN; Harmonized EN covering essential requirements of article 3.2 of the R&TTE Directive

- **EN 301 489-1**

Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements

- **EN 301 489-17**

Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment

This device is a 5GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

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

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

CE 0560

Česky [Czech]	[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 erkläre [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 alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
Polski [Polish]	Niniejszym [nazwa producenta] oświadczam, że [nazwa wyrobu] jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	[Nome do fabricante] declara que este [tipo de equipamento] está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	[Ime proizvajalca] izjavlja, da je ta [tip opreme] v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	[Meno výrobcu] týmto vyhlasuje, že [typ zariadenia] spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	[Valmistaja = manufacturer] vakuuttaa täten että [type of equipment = laitteen tyyppimerkintä] tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.