WAB-3003
108M 11g Outdoor PoE AP

User's Manual v1.2

Regulatory Information

CE

Declaration of Conformity with Regard to the 1999/5/EC (R&TTE Directive) for

European Community, Switzerland, Norway, Iceland, and Liechtenstein

Model: WAB-3003

For 2.4 GHz radios, the devices have been tested and passed the requirements of the following standards, and hence fulfills the EMC and safety requirements of R&TTE Directive within the CE marking requirement.

- Radio: EN 300.328:2006
- Radio: EN 50392:2004
- EMC: EN 301.489-1:2005, EN 301.489-17:2002,
- EMC: EN 55022:2006 Class B, EN 55024:1998 + A1:2001 + A2:2003 including the followings:

  EN 61000-3-2, EN 61000-3-3.

  EN 61000-4-2, EN 61000-4-3, EN 61000-4-4,

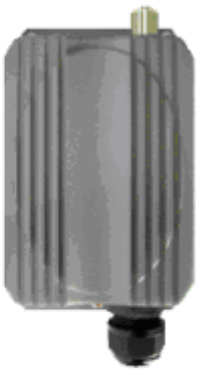
  EN 61000-4-5, EN 61000-4-6, EN 61000-4-11
- Safety: EN 60950-1:2001 + A11:2004,

Table of Contents

1. Introduction

1.1 Overview

This manual is designed for **system integrators**, **field engineers** and **network administrators** to set up **WAB-3003 108M 11g Outdoor PoE AP** in their network environments. It contains step-by-step procedures and graphic examples to guide users with networking knowledge to complete the installation.

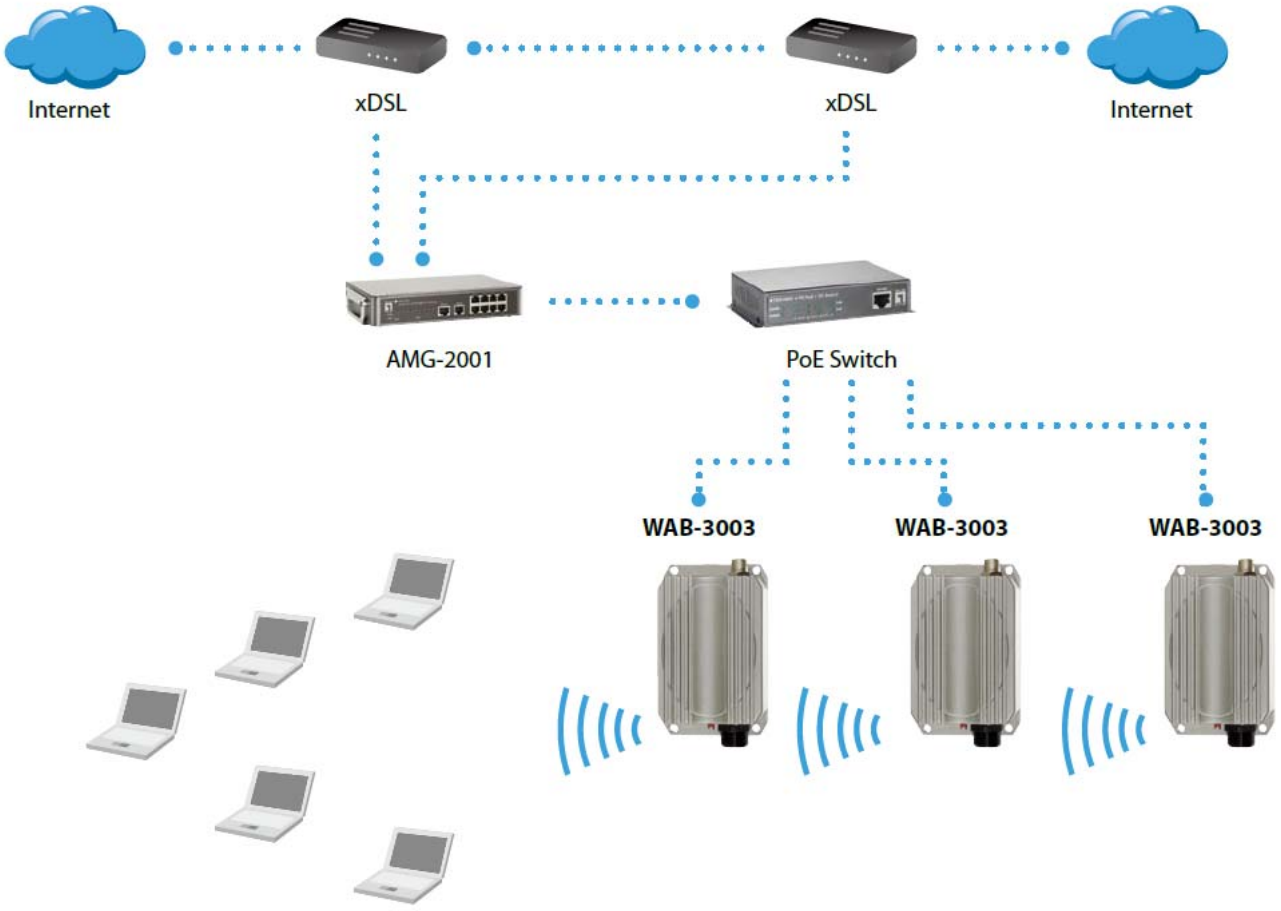


WAB-3003 (with N type antenna)

The 802.11 b/g compliant **WAB-3003** is a Long Range Outdoor AP Device that can be deployed as a traditional fixed wireless Access Point (AP), either indoors or outdoors.

The **WAB-3003** is compact in size and weatherproof. Coming with a mounting kit, it can be mounted on a pole or wall. Specifically developed for outdoor usage, the fully-hardened, IP68-rated **WAB-3003** can withstand wind, rain, lightning, power surges, and extreme temperatures.

The following is a network diagram for an AMG Controller application.



WAB-3003 Long range wireless transmission

The **WAB-3003** can be deployed in various environments, for example:

- Hot zones such as business districts, office complexes, airports, hotels, conference centers, recreation areas, and shopping malls.
- Outdoor access point for school campuses, enterprise campuses, or manufacture plants.
- Indoor access point for hotels, factories, or warehouses where metal industrial grade devices are preferred.
- Public hotspot operation for café, parks, convention centers, shopping malls, or airports.
- Wireless coverage for indoor and outdoor ground for private resorts, acre estate/home's yards, or gulf course communities.

1.2 Functionalities

- Full range of **wireless security** mechanisms such as WEP, WPA and WPA2 (802.11i) that are important for enterprise wireless deployments.
- Purposely built rugged access point for harsh **outdoor / industrial** conditions.
- **Weatherproof** and watertight from its rugged aluminum housing (IP68 Approved).
- **Power over Ethernet (PoE)** built-in for single cable installation.
- On board **Ethernet surge protection**.

1.3 Document Conventions

Caution:	Represents essential steps, actions, or messages that should not be ignored.
Note:	Contains related information that corresponds to a topic.
	Indicates that clicking this button will save the changes you made, but you must reboot the system upon the completion of all configuration settings for the changes to take effect.
	Indicates that clicking this button will clear what you have set before the settings are applied.

2. System Overview

2.1 Package Contents

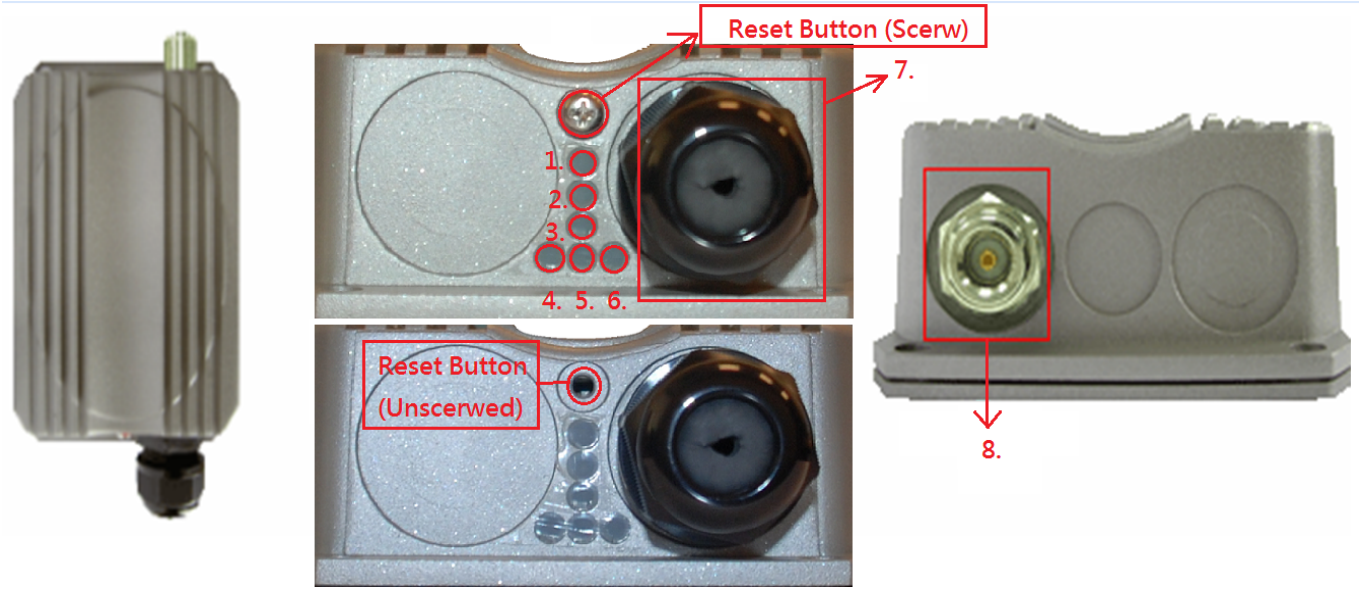
The standard package of **WAB-3003** includes:

- **WAB-3003** x 1
- Quick Installation Guide (QIG) x 1
- CD-ROM (with User's Manual and QIG) x 1
- PSE with AC cable x 1
- Mounting Kit x 1
- Water Proof Connector (installed) x 1

Caution:
It is highly recommended to use all the components supplied to ensure best performance of the system.

2.2 Panel Function Description

WAB-3003



1	Power	Red LED ON indicates Power on, and OFF indicates power off
2~3	Wireless Signal Strength	For showing the signal strength situation (7: Yellow; 8: Green)
4	WLAN	Green LED ON indicates system ready
5	Wireless Signal Strength	For showing the signal strength situation
6	Ethernet	Green LED ON indicates connection, OFF indicates no connection, and BLINKING indicates transmitting data.
7	PoE Connector	For connecting to the Power Sourcing Equipment (PSE)
8	N-type Connector	For connecting to an antenna
9	Reset Button *(Screw)	For resetting the system of AP

Reset Procedure

1. Make sure the WAB-3003 completes booting and is already running
(The booting process of system usually takes 2 minutes)

2. *Unscrew the Screw then you will see a reset button (inside the hole)

3. Use the provided reset pin to press and hold the reset button for 15 seconds

4. Release the reset button and leave the system re-booting for 2 minutes

3. Installation

3.1 Hardware Installation

The following diagram is a **basic network topology** which can be used for testing and configuring the **WAB-3003**.

Installation Steps:

Step 1. Connect an antenna to the connector.

Step 2. Connect the PSE (POWER & DATA OUT) to the PSE 1 connector on the lower panel.

Step 3. Connect one end of an Ethernet cable to the PSE 2 connector on the lower panel and connect the other end to a computer.

Step 4. Connect the power cord to the PSE.

Step 5. Power on the PSE in order to supply power to the **WAB-3003**.

3.2 Basic Configuration

3.2.1 Introduction to Web Management Interface

WAB-3003 provides a user friendly web management interface for configuration. It is required to follow the respective installation procedures provided to properly set up the system.

- **Default IP Address of Web Management Interface:**
  The default IP address and Subnet Mask are as follows:

IP Address	192.168.0.1
Subnet Mask	255.255.255.0

- **Default User Name and Password:**
  The default **User name** and **Password** for the **root** and **admin** accounts are as follows:

Management Account	**Root Account**
User Name	root
Password	admin

Step 1: IP Segment Set-up for Administrator PC

Set a static IP address on the same subnet mask as **WAB-3003** in TCP/IP of the administrator PC, such as the following example. Do not duplicate the IP address used here with the IP address of **WAB-3003** or any other devices within the same network.

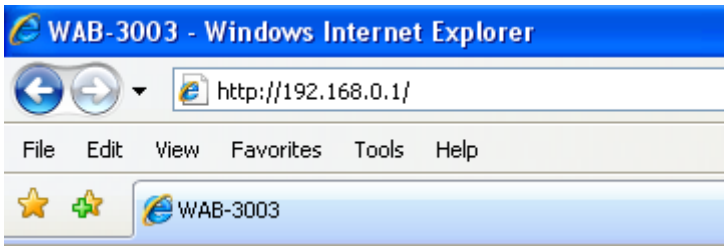
>> Example of IP Segment:

The valid range of IP address is 1 ~ 254. However, **1** must be avoided as it is already used by **WAB-3003**. Below depicts an example of using **100** (the underlined value can be changed as desired).

- IP Address: 192.168.0.100
- Subnet Mask: 255.255.255.0

Step 2: Launch Web Browser

Launch a web browser to access the web management interface of AP mode by entering the default IP address, **http://192.168.0.1/**, in the URL field, and then press ***Enter***.



Caution:
Using an incorrect default IP address will result in no Login page shown on the web browser. Please make sure a correct IP address is used for the desired mode; refer to ***Section 3.2.1 Instruction to Web Management Interface*** *for detailed default IP addresses.*

Step 3: System Login

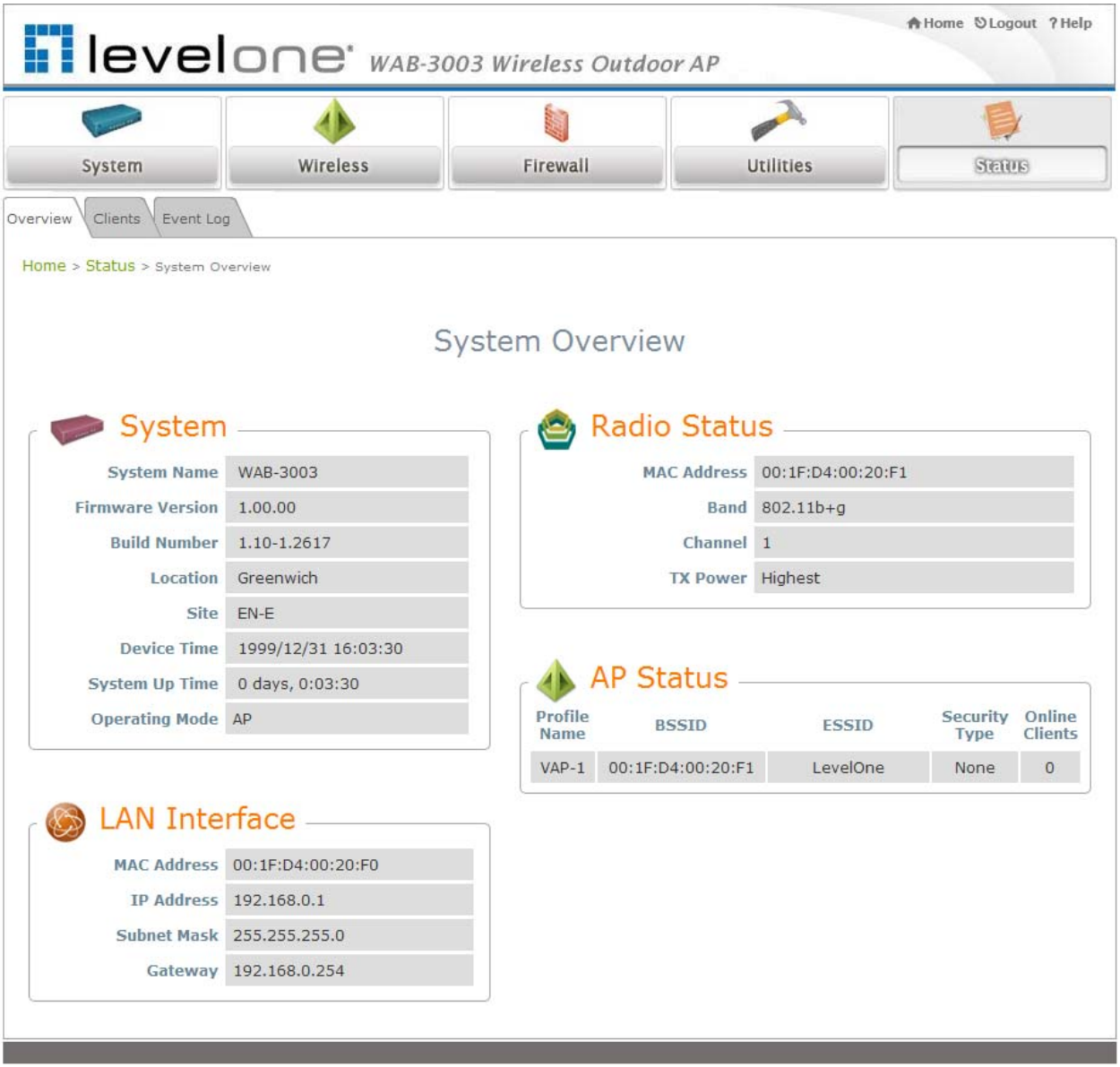
The system manager Login Page will then appear.

Enter **"root"** in the *User name* field and **"admin"** in the *Password* field, and then click ***OK*** to log in.

Step 4: Login Success

The **System Overview** page will appear after a successful login.

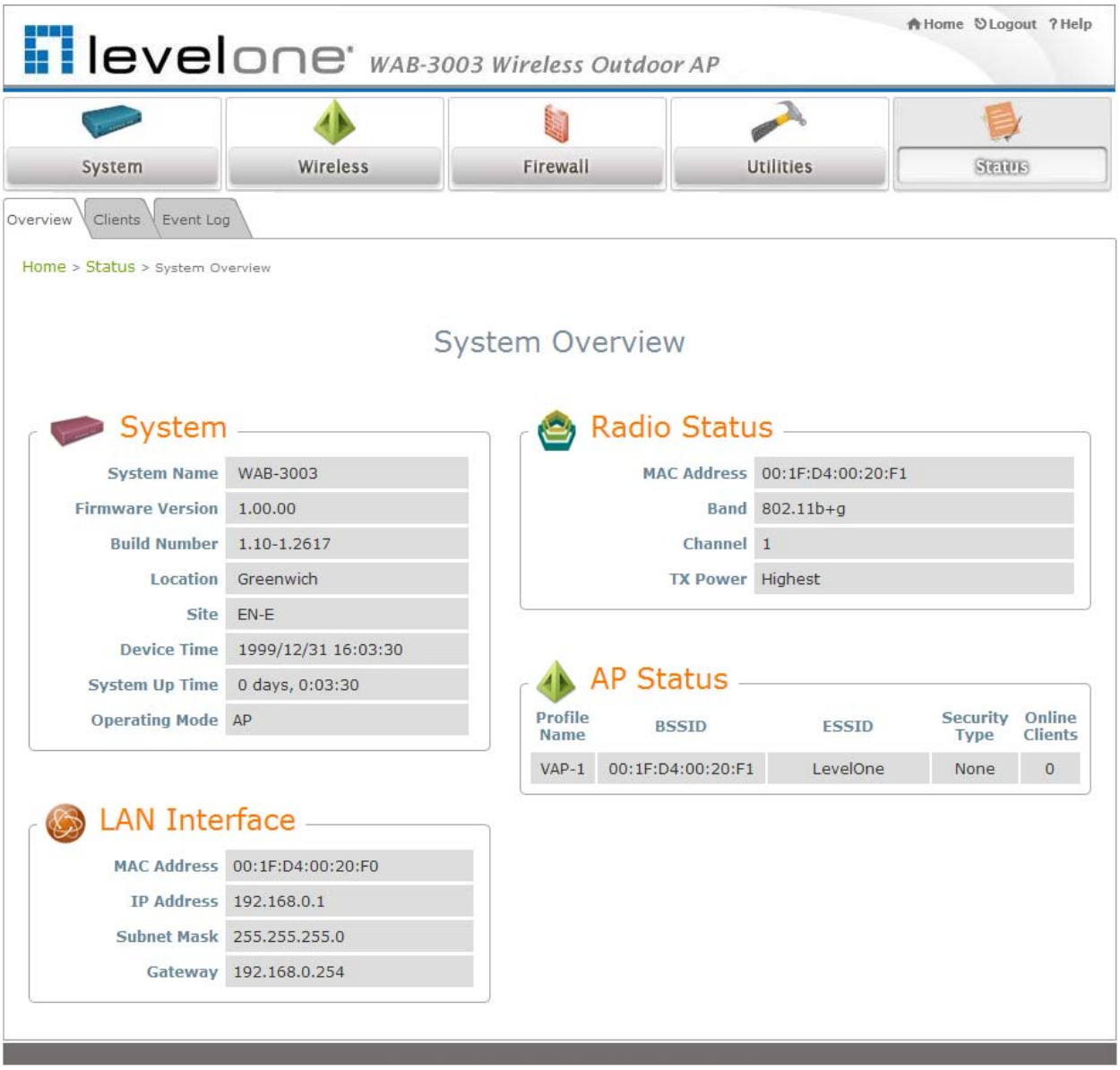
To logout, simply click on the Logout button on the top right hand corner of the management interface.



3.2.2 Quick Configuration

This section provides a step-by-step configuration procedure for installing WAB-3003.

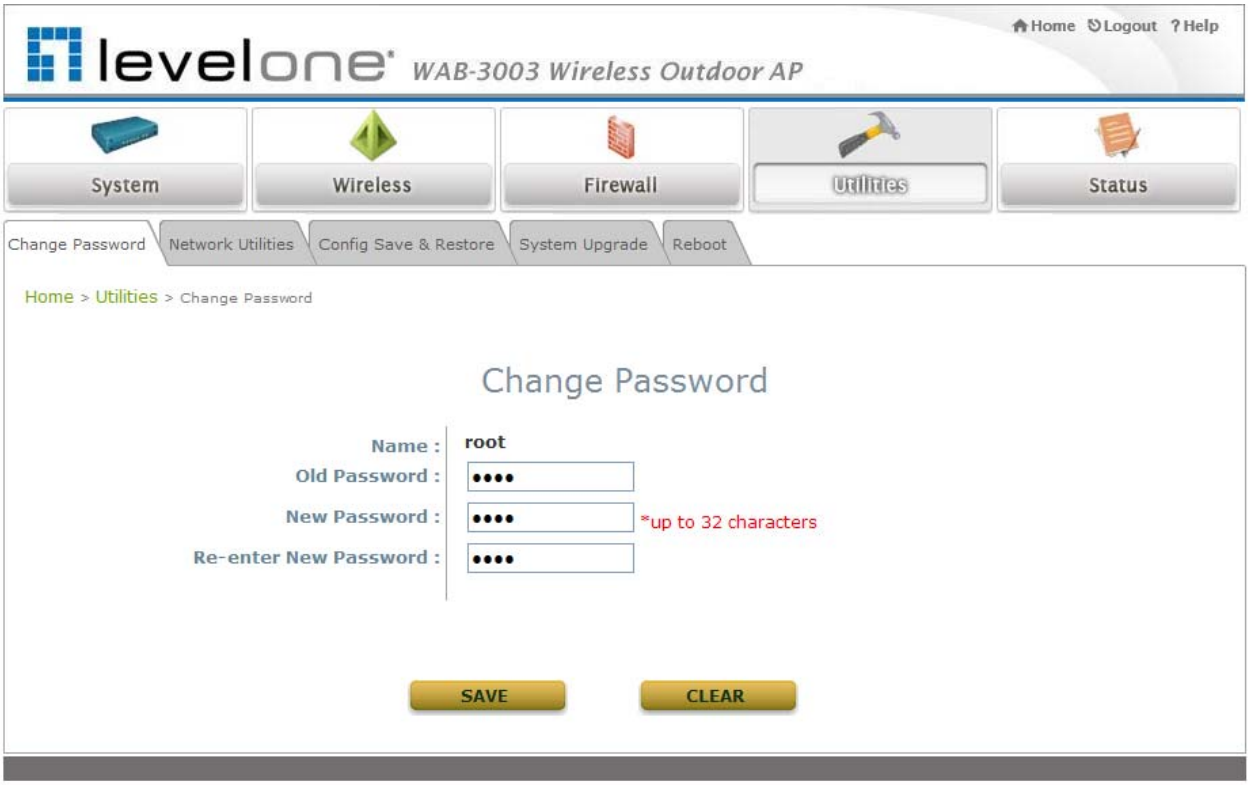
Step 1: Mode Confirmation



➢ Ensure that the *Operating Mode* is currently at **AP** mode.

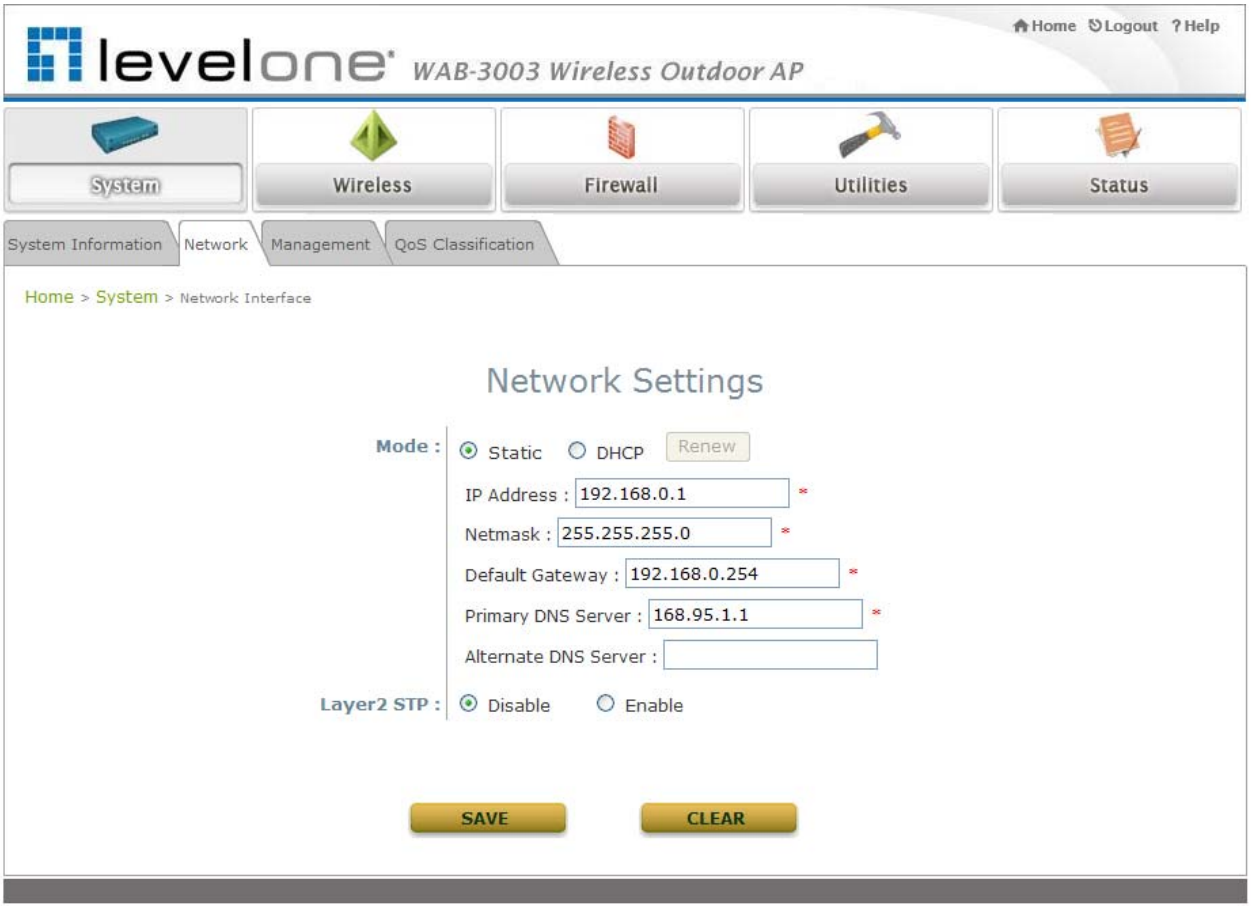
Click on the **Status** button and then select the **System Overview** tab.

Step 2: Change Password



- Click on the **Utilities** button and then select the **Password** tab.
- Enter a new password in the *New Password* field and retype it in the *Re-enter New Password* field.
- Click ***SAVE*** to save the changes.

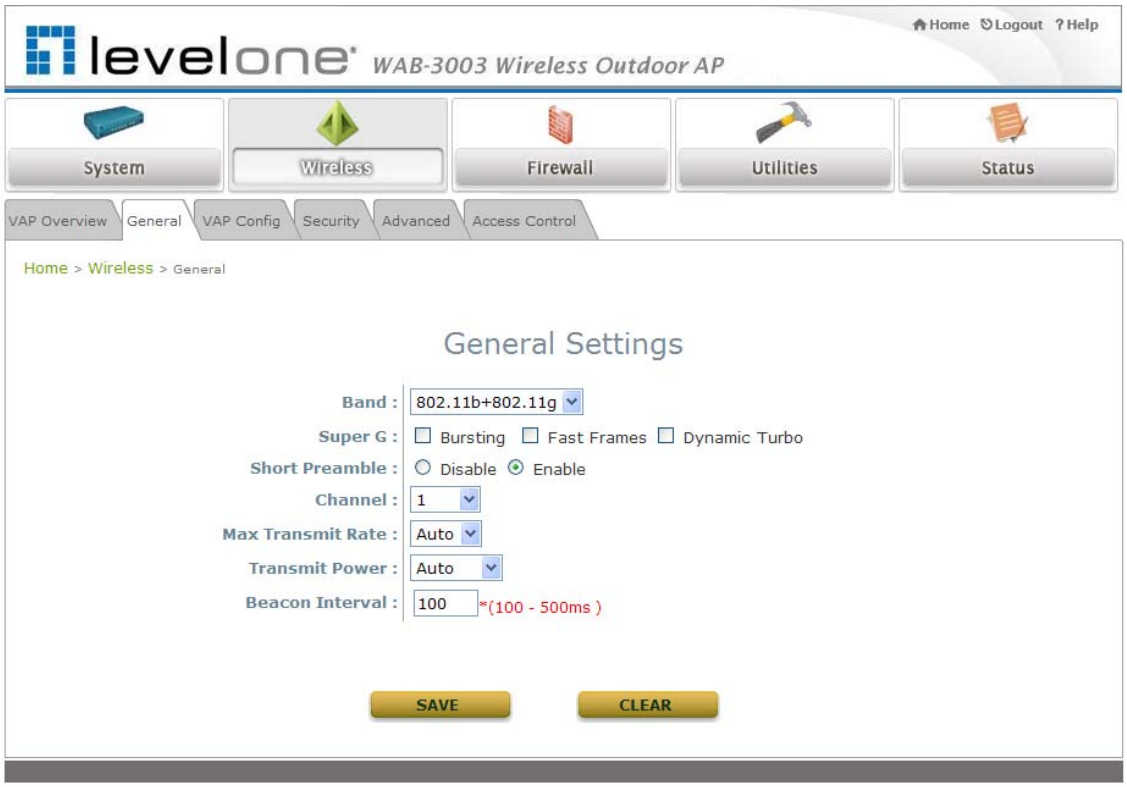
Step 3: Network Settings



【Settings here are for example only. 】

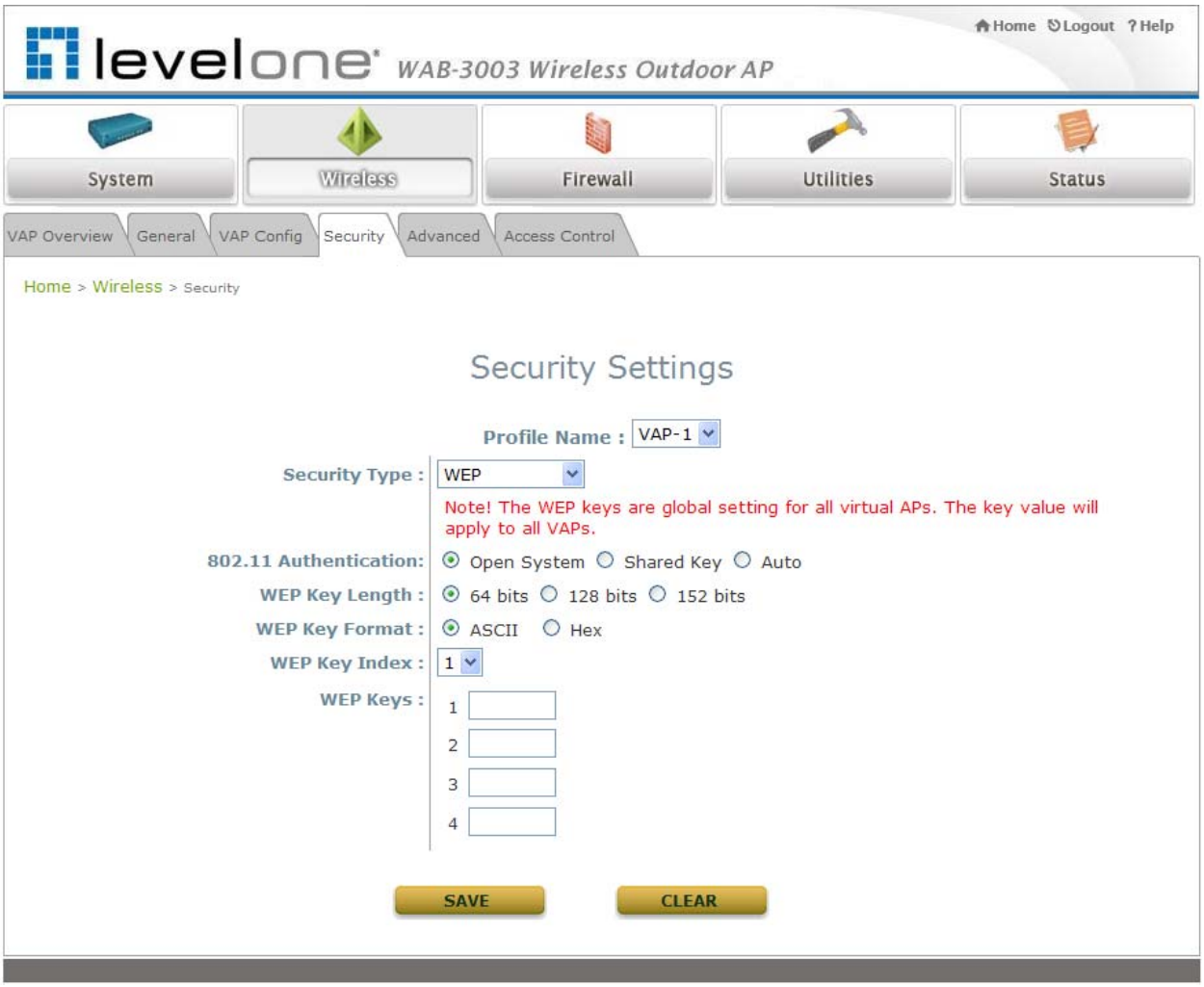
- Click on the **System** button and then select the **Network** tab.
- Enable *Static*, and then enter the related information in the fields marked with red asterisks.
- Click ***SAVE*** to save the settings.

Step 4: SSID Settings



- Click on the **Wireless** button and then select the **General** tab.
- **Band:** Select an appropriate band from the drop-down list box.
- Click ***SAVE*** to save the settings.

Step 5: Security Settings



- Click on the **Wireless** button and then select the **Security** tab.
- Select the desired *VAP Profile and Security Type* from the drop-down list boxes. The above figure depicts an example of selecting VAP-1 and **WEP**.
- Enter the information required in the blank fields.

Caution:
You must use the same information provided here to configure the network devices that are to be associated with ***WAB-3003****.*

- Click ***SAVE*** to save all settings configured so far; all updated settings will take effect upon reboot.

Congratulations!

WAB-3003 is now successfully configured.

*4.*AP Configuration

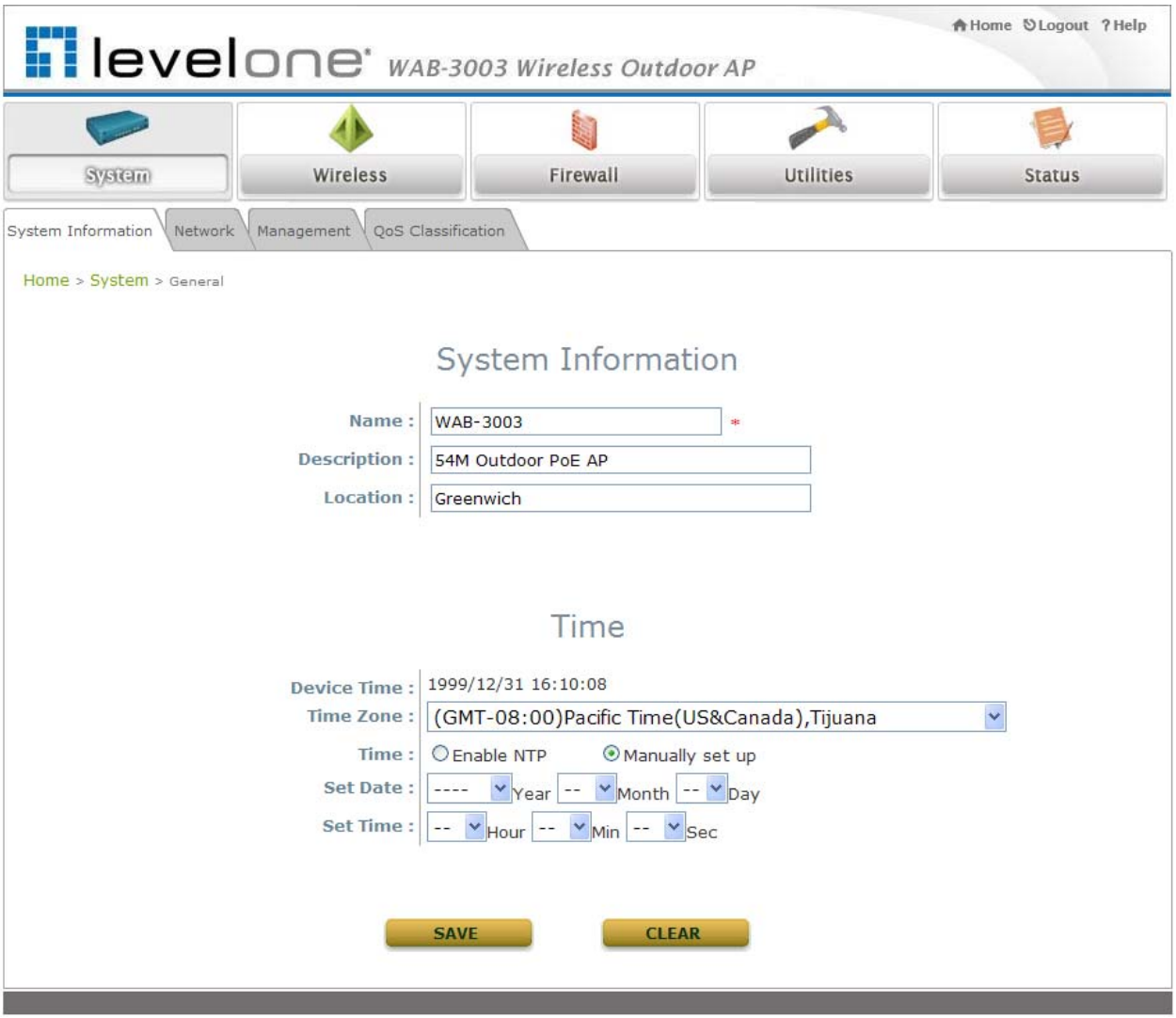
When AP mode is activated, the system can be configured as an Access Point. This chapter will guide you through setting up the AP mode with graphical illustrations. The following table shows all the functions of WAB-3003 in its AP mode.

OPTION	System	Wireless	Firewall	Utilities	Status
FUNCTION	System Information	VAP Overview	Firewall List	Change Password	System Overview
	Network Settings	General Settings	Service	Network Utilities	Associate Client Status
	Management Services	VAP Configuration	Advanced	Configuration Save & Restore	Event Log
	QoS Classification	Security Settings		System Upgrade	
		Advanced Wireless Settings		Reboot	
		Access Control Settings			

Table 4-1: AP Functions

4.1 System

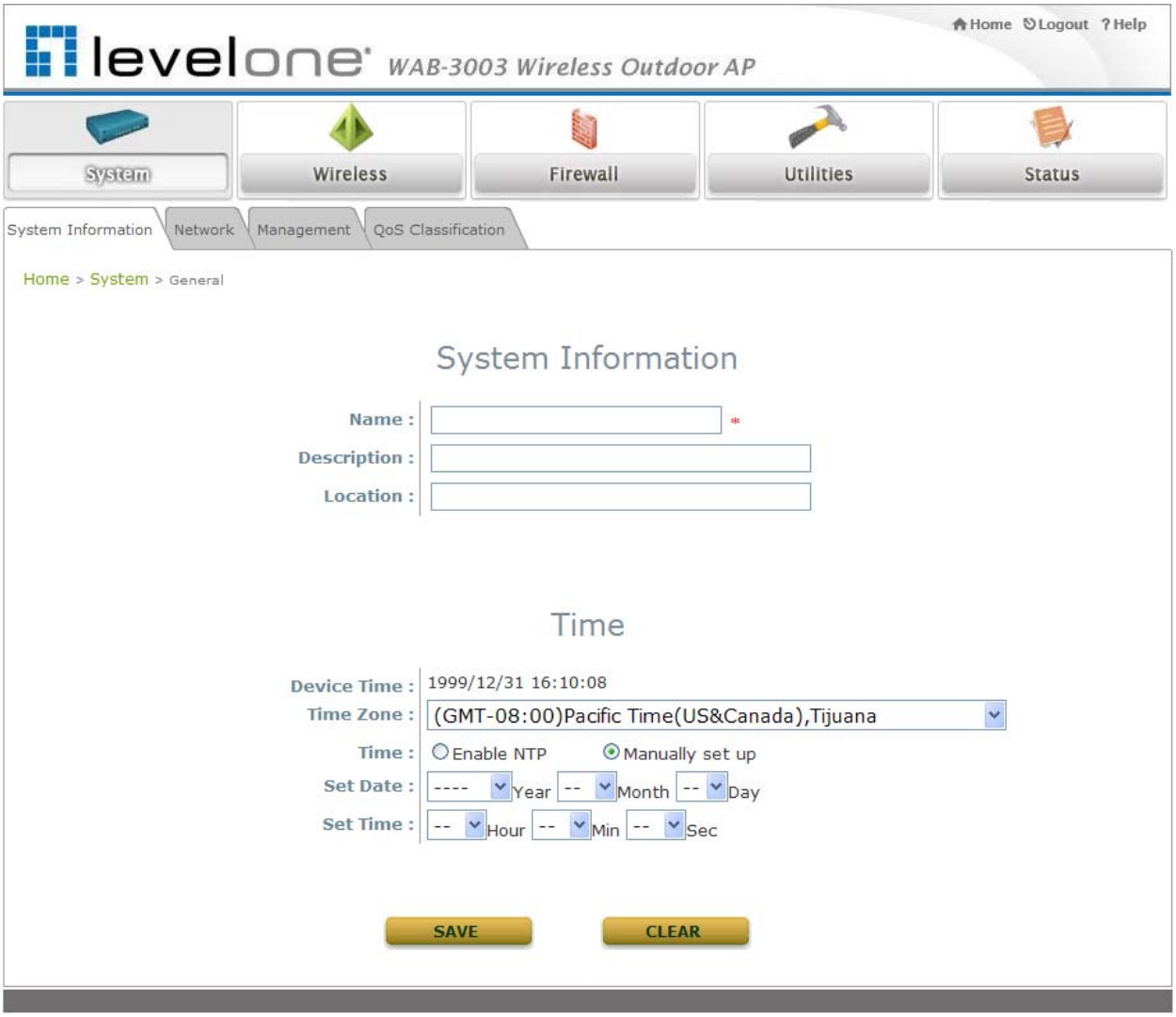
This section provides information for configuring the following functions: **System Information**, **Network Settings**, **Management Services, and QoS Classification**.



Note:
A system restart is required when a reminding message appears after clicking the ***SAVE*** button; all settings entered and saved will take effect only after the system restart.

4.1.1 System Information

For maintenance purpose, it is required to specify the system name, its location and corresponding basic parameters. Fields such as *Name*, *Description* and *Location* are used for mnemonic purpose. It is recommended to have different values in each AP.



- **System Information**

  For maintenance purpose, it is recommended to have the following information stated as clearly as possible. Fields Name, Description, and Location are used for mnemonic purpose. It is recommended to have different values in each wireless device.

  - *Name*: The system name used to identify this system
  - Description: Further information of the system.
  - *Location*: The information on geographical location of the system for the administrator to locate the system easily.

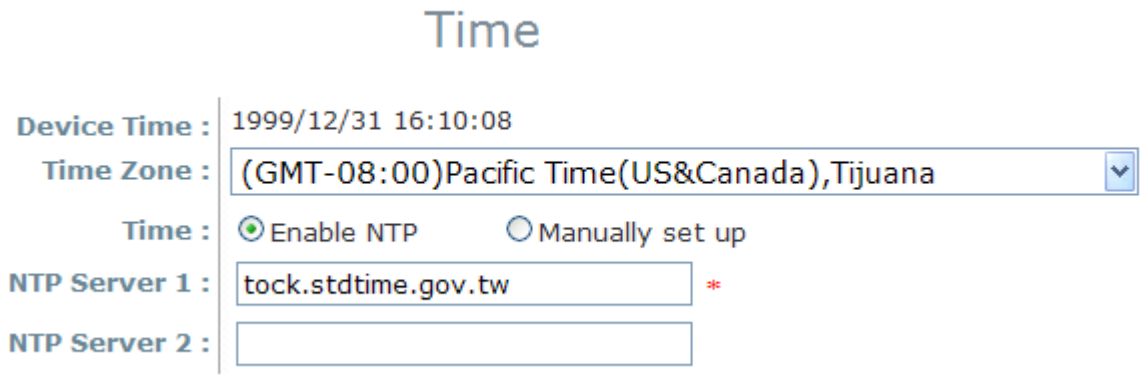
- **Time**

  Time settings allow the system time synchronized with NTP server or manually set.

  - *Device Time*: Display the current time of the system.
  - *Time Zone*: Select an appropriate time zone from the drop-down list box.
  - *Synchronization*: Synchronize the system time either by NTP server or manual setup.

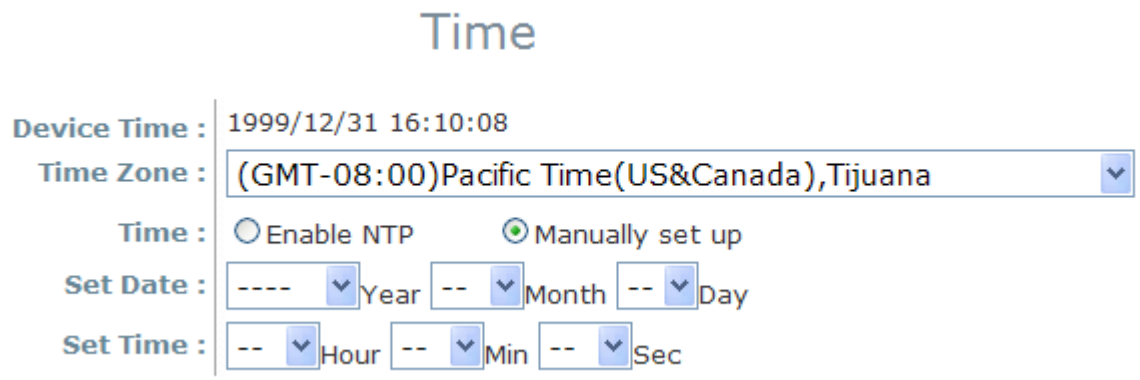
(1) **Enable NTP:**

By selecting ***Enable NTP***, WAB-3003 can synchronize its system time with the NTP server automatically. While this method is chosen, at least one NTP server's IP address or domain name must be provided. If FQDN (full qualified domain name) is used as the IP address of NTP server, the DNS server must also be activated (please refer to **4.1.2 Network Settings**).



(2) **Manually set up:**

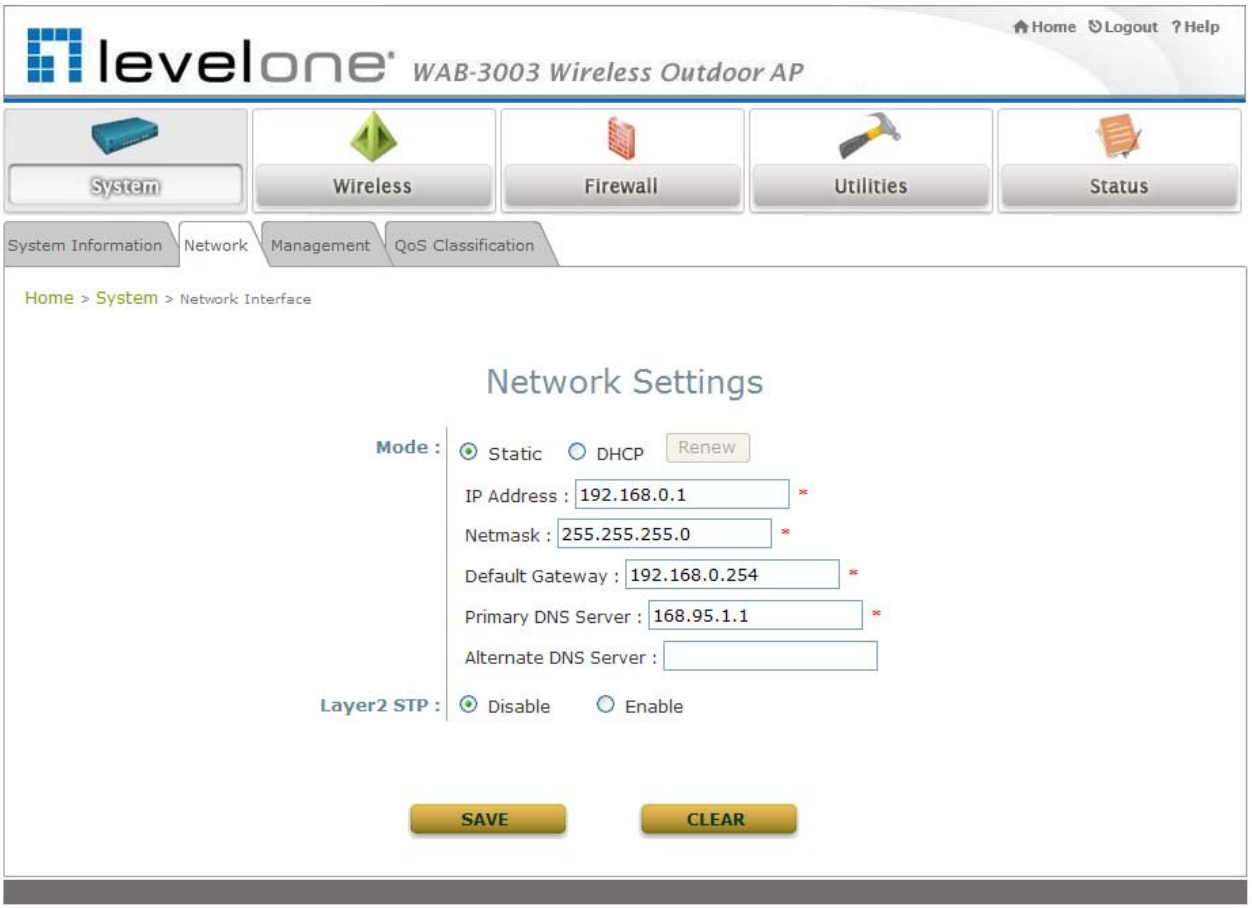
By selecting *Manually set up*, the administrator can manually set the system date and time.



- *Set Date*: Select the appropriate *Year*, *Month*, and *Day* from the drop-down list box.
- *Set Time*: Select the appropriate *Hour*, *Min*, and *Sec* from the drop-down list box.

4.1.2 Network Settings

LAN settings can be configured on this page.

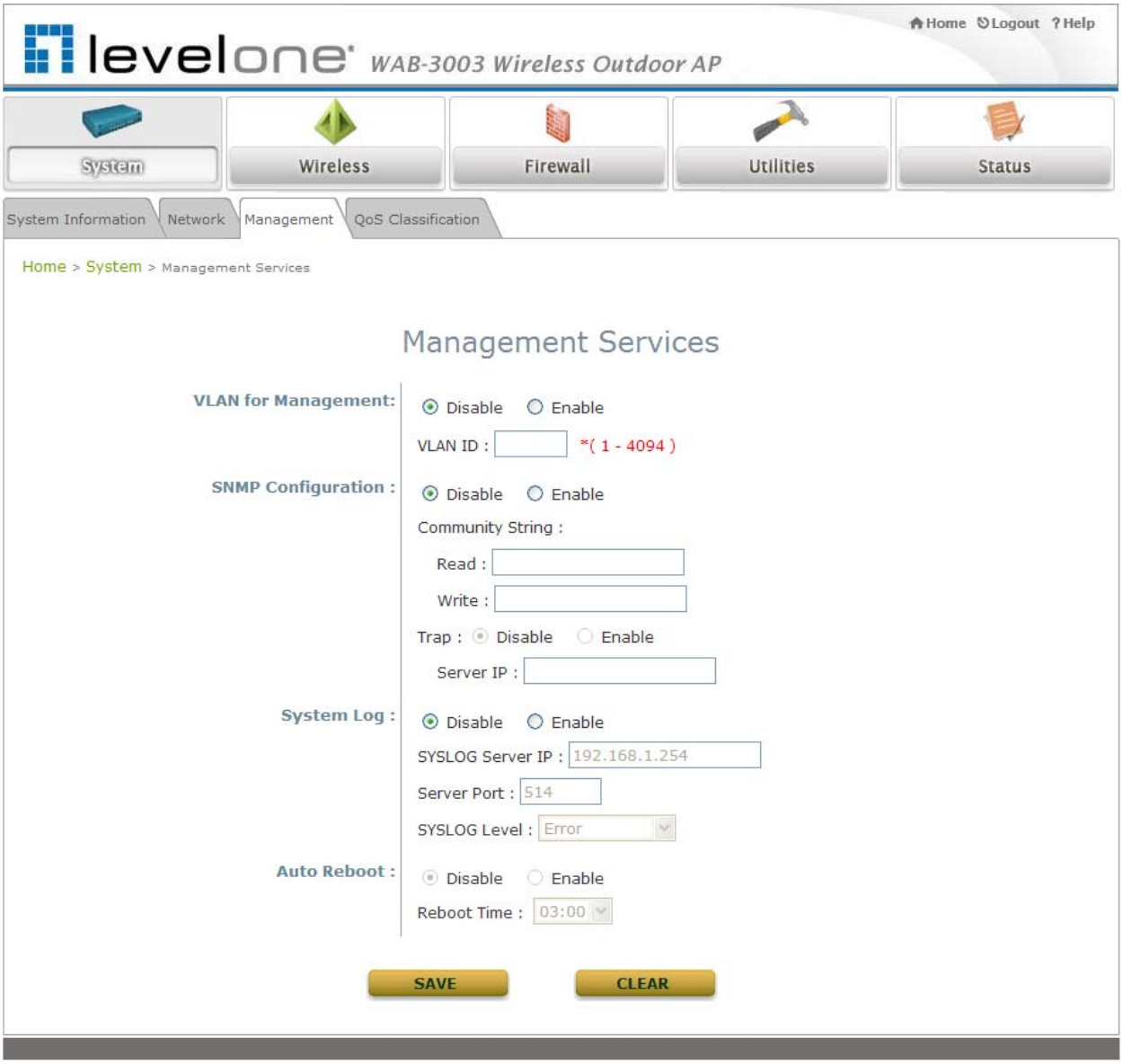


- **Mode:** Determine the way to obtain the IP address, by *DHCP* or *Static* manually set.
  - **Static:** Static setting is set these parameters manually. The basic parameters need to provide such as IP address, subnet mask and Gateway.
    - **IP Address:** The IP address of the LAN port.
    - **Netmask:** The Subnet mask of the LAN port.
    - **Gateway:** The Gateway IP address of the LAN port.
    - **Primary/Secondary DNS Server:** Please provide at least on DNS server's IP address.
  - **DHCP:** The option is provided when a DHCP server is provided in the network. The following IP address/Netmask/Gateway setting will be disabled.

- **Layer 2 STP:** Depends on the configuration of the system including wired and wireless settings, when it is configured to bring several networks, we need enable STP.

4.1.3 Management Services

The system supports **VLAN**, **SNMP**, **Remote Syslog**, and **Auto Reboot** functions for easy management. These functions can be configured on this page.

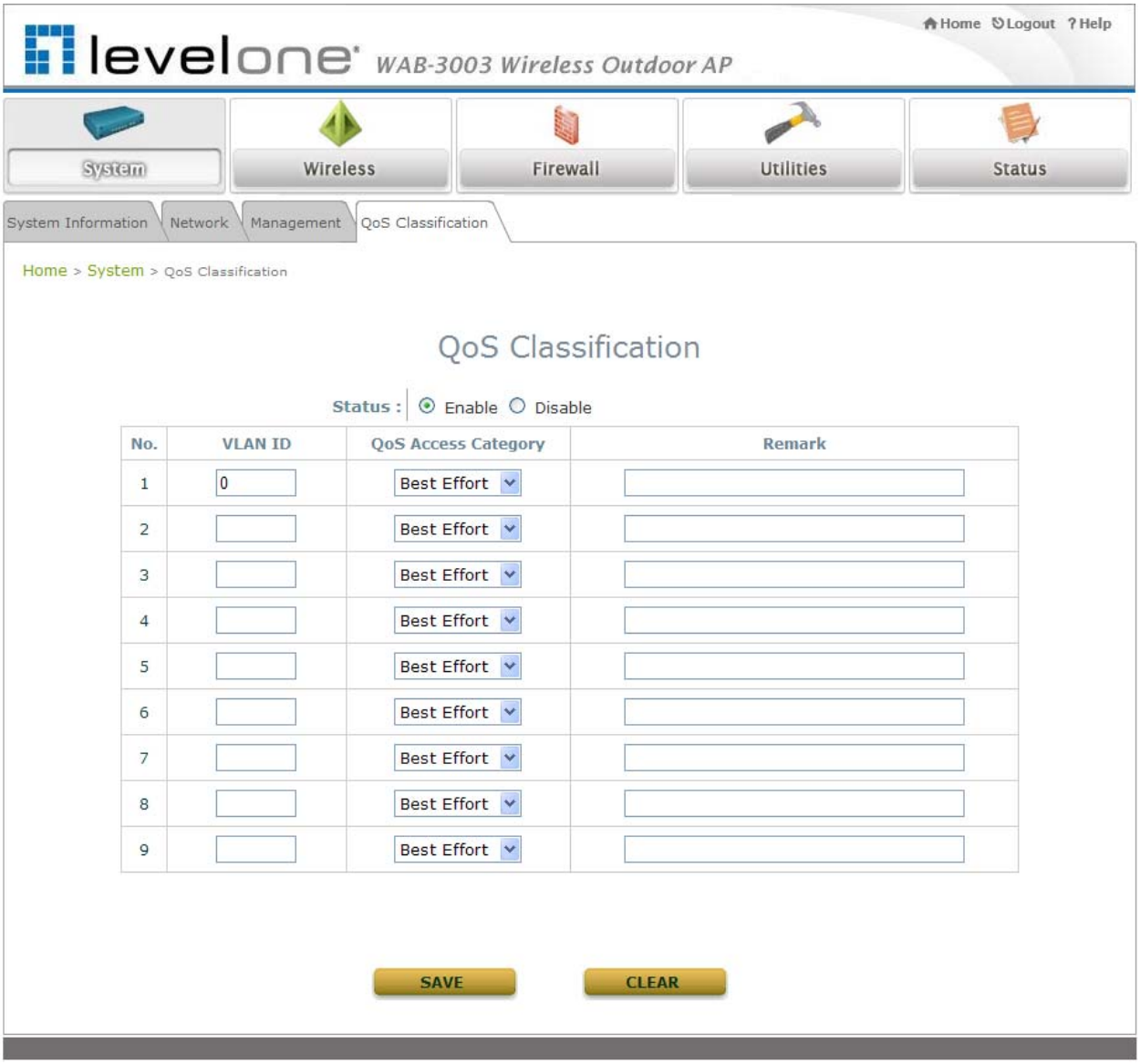


- **VLAN for Management:** The Ethernet traffic from the system can be tagged with VLAN tag with specific ID.
- **SNMP Configuration:** By enabling SNMP service, the remote SNMP manager could obtain the system status.
  - **Enable / Disable:** Select *Enable* to activate this function or *Disable* to inactivate it.
  - **Community String:** The community string is required when accessing the Management Information Base (MIB) of the system.
    - **Read:** Enter the community string to access the MIB with Read privilege.
    - **Write:** Enter the community string to access the MIB with Write privilege.
  - **Trap:** When enabled, events on Cold Start, Interface UP & Down, and Association & Disassociation can be reported to an assigned server.
    - **Enable / Disable:** Select *Enable* to activate this function or *Disable* to inactivate it.
    - **Server IP Address:** Enter the IP address of the assigned server for receiving the trap report.
- **Syslog Configuration:** By enabling this function, specify a remote syslog server which could accept system log messages from the system remotely. Therefore, by reading the syslog message in the remote server, review activities of all installed the system in the network.
  - **Enable / Disable:** Select *Enable* to activate this function or *Disable* to inactivate it.
  - **Server IP:** The IP address of the Syslog server for receiving the reported events.
  - **Server Port:** The port number of the Syslog server.
  - **Log Level:** Select the desired level of received events from the drop-down list box.

- **Auto Reboot:** The option can be enabled to reboot system automatically with preferred Reboot Time from drop-down list.
  - **Enable / Disable:** Select *Enable* to activate this function or *Disable* to deactivate it.
  - **Reboot Time:** Select an appropriate time from the drop-down list box. Since all users on the network will be disconnected during reboot, it is suggested to set the reboot time during an off-peak period to reduce impacts on online users.

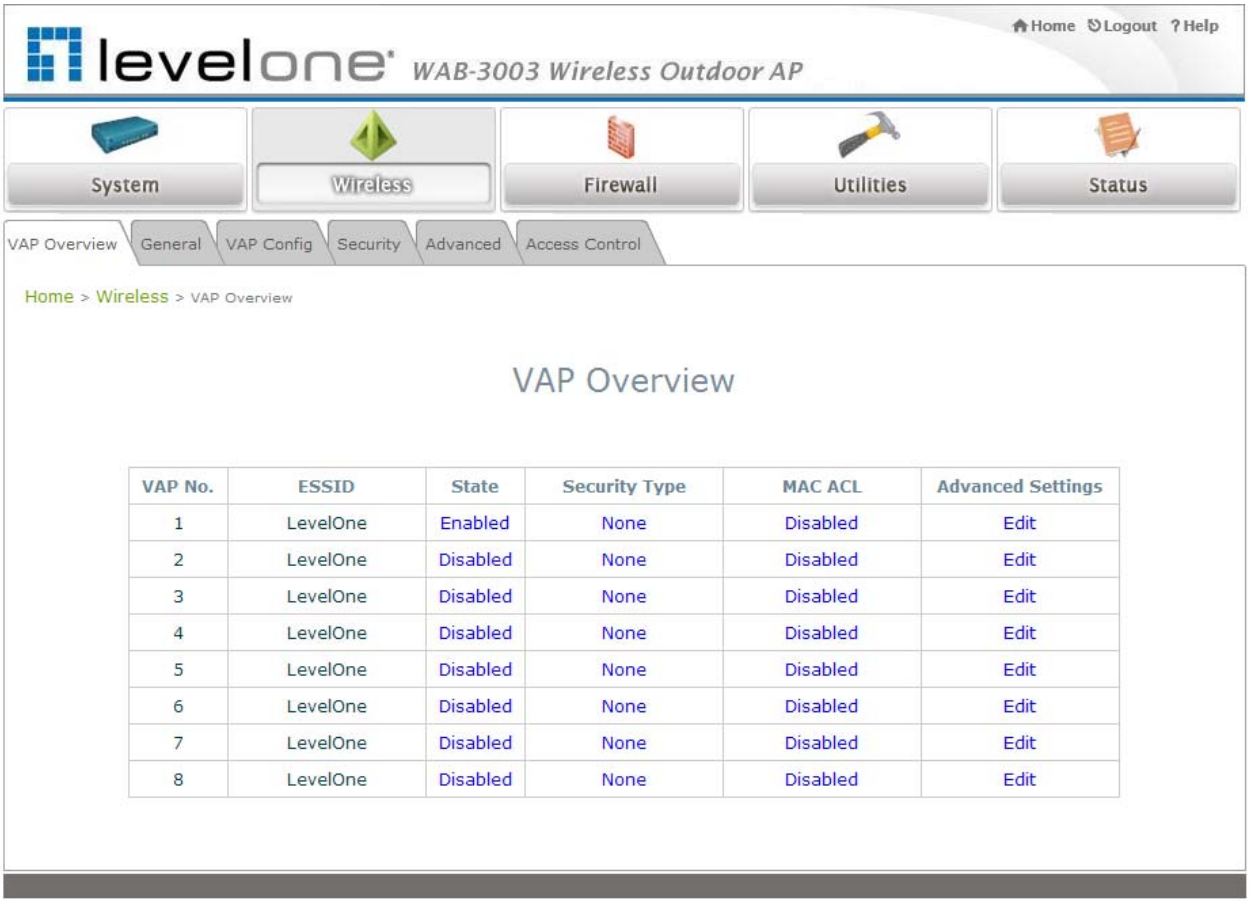
4.1.4 QoS Classification

The system supports function of QoS classification where specified **VLAN ID** can be assigned to a specific **QoS access category** for priority handling of traffics.



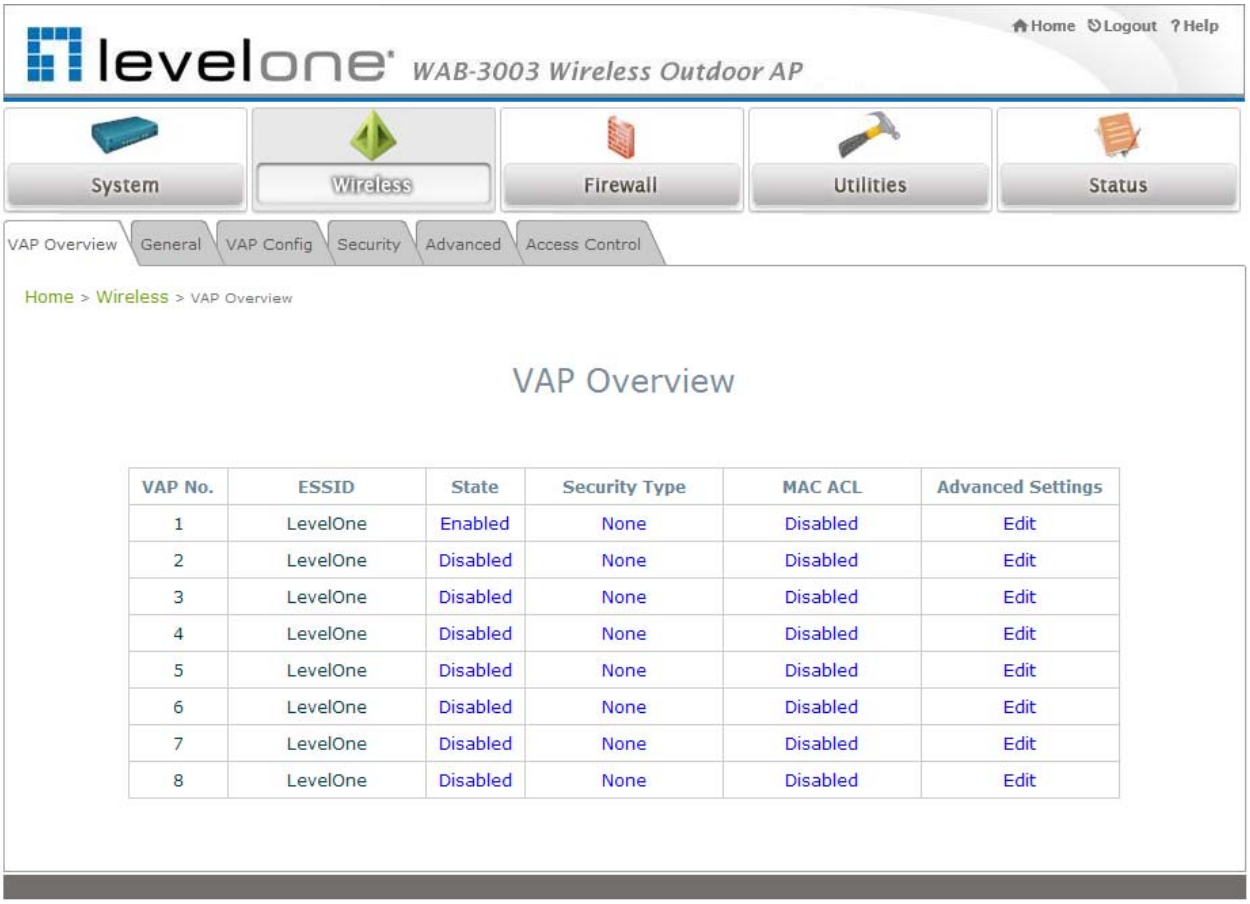
4.2 Wireless

The administrator can configure the following wireless settings on this page: **VAP Overview, General Settings, VAP Configuration, Security Settings, Advanced Wireless Settings, Access Control Settings,** and **Site Survey**. The system supports up to eight Virtual Access Points (VAPs). Each VAP can have its own settings including ESSID, VLAN ID, security settings, etc. Such VAP capability enables different levels of service to meet actual requirements.



4.2.1 Virtual AP Overview

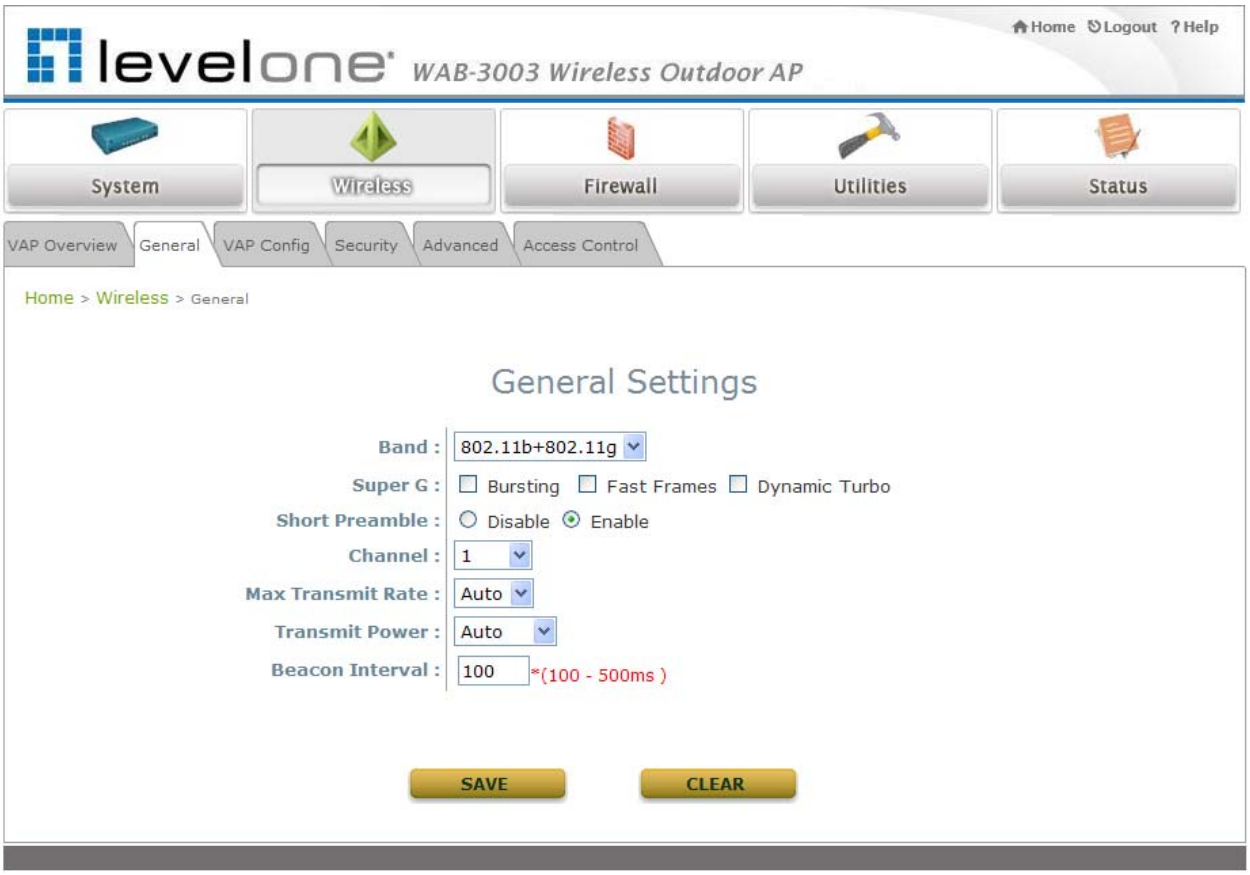
An overall status is collected in this page, including *Enable/Disable State*, *Security Type*, *MAC ACL* state, and *Advanced Settings*. The system has 8 VAPs; each has its own settings. In this table, please click on the hyperlink for further configuration of each VAP respectively.



- **State:** The hyperlink showing *Enable* or *Disable* connects to the screen of **VAP Configuration**.
- **Security Type:** The hyperlink showing security type connects to the screen of **Security Settings**.
- **MAC ACL:** The hyperlink showing *Allow* or *Disable* connects to the screen of **Access Control Settings**.
- **Advanced Settings:** The hyperlink of advanced settings connects to the screen of **Advanced Wireless Settings**.

4.2.2 General Settings

This section is for configuring the system RF settings.



- **Band:** Select an appropriate wireless frequency band of this system. Select one frequency band from *Disable*, *802.11b*, *802.11g* or mixed mode *802.11b+802.11g*.
- **Super G:** Options of Bursting, Fast Frames, and Atheros' featured Dynamic Turbo can be selected to boost wireless throughput.
- **Short Preamble:** The option can be turned on the enable Short-Preamble frames.
- **Channel:** Select the appropriate channel from the drop-down list box to correspond with your network settings, for example, Channel 1-11 is available in North America and Channel 1-13 in Europe, or choose the default *Auto*.
- **Max Transmit Rate:** Select transmit rate from *1M* to *54M* or *Auto*.
- **Transmit Power:** Select from the lowest to highest power level or choose *Auto*.
- **Beacon Interval:** Enter a value between 100 and 500 ms. The default is 100 milliseconds. The specified value represents the amount of time between beacon signal transmissions.

The RF settings in this page will be applied to all VAPs.

Under normal circumstances, the available RF configurations are illustrated as below:

Band	**Super G**	**Short Preamble**	**Channel**	**Max Transmit Rate**	**Transmit Power**
Disable	N/A	N/A	N/A	N/A	N/A
802.11b	N/A	Disable/Enable	Auto, 1~11, 13, or 14	1M, 2M, 5.5M, 11M	Auto, Lowest, Low, Medium, High, Highest
802.11g	Bursting, Compression, Fast Frames, Dynamic Turbo	Disable/Enable	Auto, 1~11 or 13	6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M	
802.11b+802.11g	Bursting, Compression, Fast Frames, Dynamic Turbo	Disable/Enable	Auto, 1~11, 13, or 14	1M, 2M, 5.5M, 6M, 9M, 11M, 12M, 18M, 24M, 36M, 48M, 54M	

4.2.3 VAP Configuration

To enable each VAP, the administrator must configure each VAP manually. The settings of each VAP are collected as its profile.

- **Enable VAP:** Enable or disable VAP function.
- **Profile Name:** The profile name of each VAP for identity/management purpose.
- **ESSID:** ESSID (Extended Service Set ID) indicates a unique SSID used by a client device to associate with a specified VAP. ESSID determines the service level assigned to a client.
- **VLAN ID:** The system supports tagged VLANs (virtual LANs). To enable VLAN function, each VAP must have a unique VLAN ID; valid values are ranged from 1 to 4094.

4.2.4 Security Settings

The system supports various user authentication and data encryption methods in each VAP profile. Thus the administrator can depend on the need to provide different service levels to clients. The security type includes **None**, **WEP**, **802.1X**, **WPA-PSK**, and **WPA-RADIUS**.

- **None:** No authentication is required.

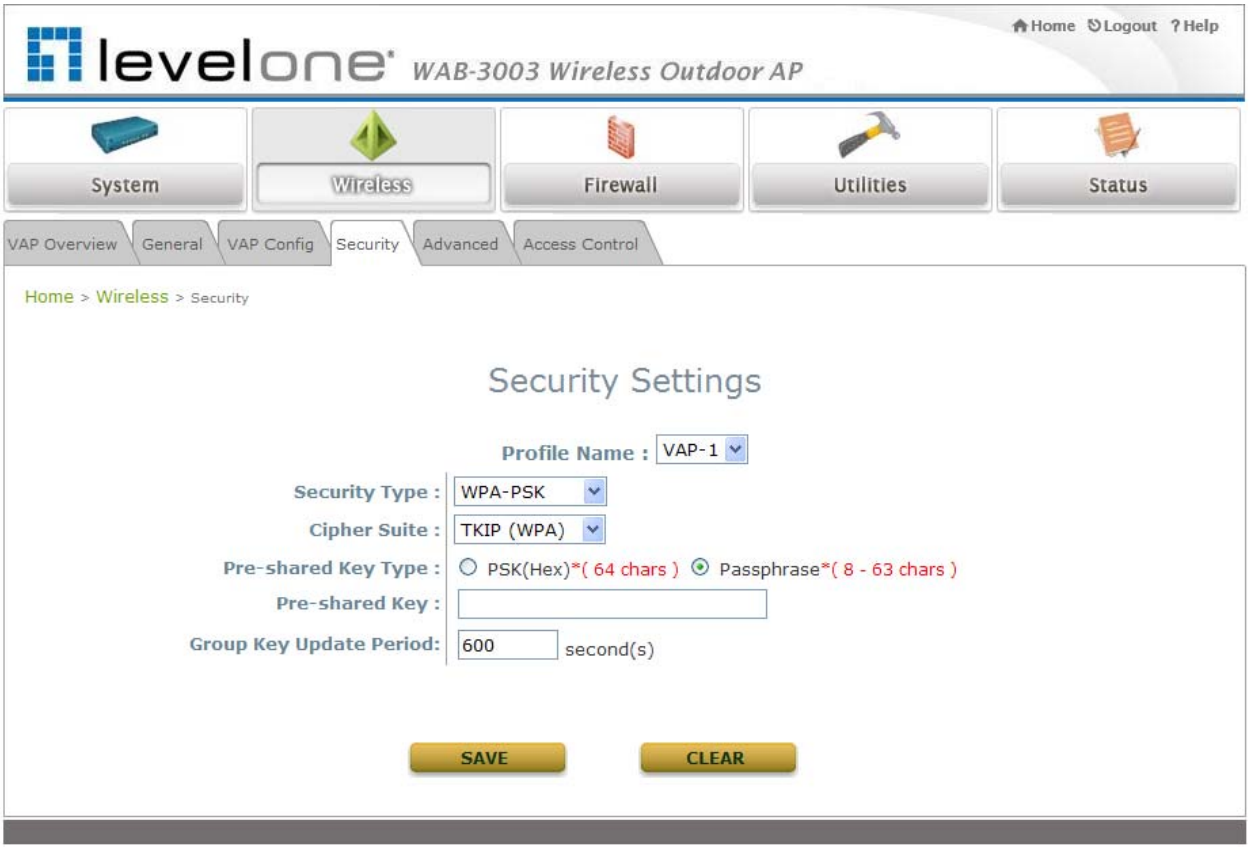
- **WEP:** WEP (Wired Equivalent Privacy) supports key length of 64/128/152 bits.

- **802.11 Authentication:** Select from *Open System*, *Shared Key*, or *Auto*.
- **WEP Key Length:** Select from *64-bit*, *128-bit*, or 152-bit key length.
- **WEP Key Format:** Select from *ASCII* or *Hex* format for the WEP key.
- **WEP Key Index:** Select a key index from 1 through 4. The WEP key index is a number that specifies which WEP key to use for the encryption of wireless frames during data transmission.
- **WEP Keys:** Provide WEP key value; the system supports up to 4 sets of WEP keys.

- **802.1X:** Provide RADIUS authentication and enhanced WEP.

- **Dynamic WEP Settings:**
  - **Dynamic WEP:** By enabling this function, the system will automatically generate WEP keys for encrption.
  - **WEK Key Length:** Select from *64-bit* or *128-bit* key length.
  - **Rekeying Period:** The time interval for the WEP key to be updated; the time unit is in second.
- **Primary RADIUS Server Settings:**
  - **Host:** Enter the IP address or domain name of the RADIUS server.
  - **Authentication Port:** The port number used by the RADIUS server. Specify a port number or use the default, 1812.
  - **Secret Key:** The secret key for the system to communicate with the RADIUS server.
  - **Accounting Service:** Enable or disable the accounting service.
  - **Accountin Port:** The port number used by the RADIUS server. Specify a port number or use the default, 1813.
  - **Accounting Interim Update Interval:** The time interval for the accounting to be updated; the time unit is in second.

- **WPA-PSK:** Provide shared key authenticaiton in WPA data encryption.



- **Cipher Suite:** Select an encryption method from *TKIP (WPA)*, *AES (WPA)*, *TKIP(WAP2)*, *AES (WAP2)*, or *Mixed*.
- **Pre-shared Key Type:** Select a pre-shared key type: *PSK (Hex)* or *Passphrase*.
- **Pre-shared Key:** Enter the key value for the pre-shared key; the format of the key value depends on the key type selected.
- **Group Key Update Period:** The time interval for the Group Key to be renewed; the time unit is in second.

- **WPA-RADIUS:** Authenticate users by RADIUS and provide WPA data encryption.

- **WPA Settings:**
  - **Cipher Suite:** Select an encryption method from *TKIP (WPA)*, *AES (WPA)*, *TKIP(WAP2)*, *AES (WAP2)*, or *Mixed*.
  - **Group Key Update Period:** The time interval for the Group Key to be renewed; the time unit is in second.
- **Primary RADIUS Server Settings:**
  - **Host:** Enter the IP address or domain name of the RADIUS server.
  - **Authentication Port:** The port number used by the RADIUS server. Specify a port number or use the default, 1812.
  - **Secret Key:** The secret key for the system to communicate with the RADIUS server.
  - **Accounting Service:** Enable or disable the accounting service.
  - **Accountin Port:** The port number used by the RADIUS server. Specify a port number or use the default, 1813.
  - **Accounting Interim Update Interval:** The time interval for the accounting to be updated; the time unit is in second.

4.2.5 Advanced Wireless Settings

The advanced wireless settings for the system's VAP profiles allow customization of data transmission settings. The administrator can tune the following parameters to improve network communication performance if a poor connection occurs.

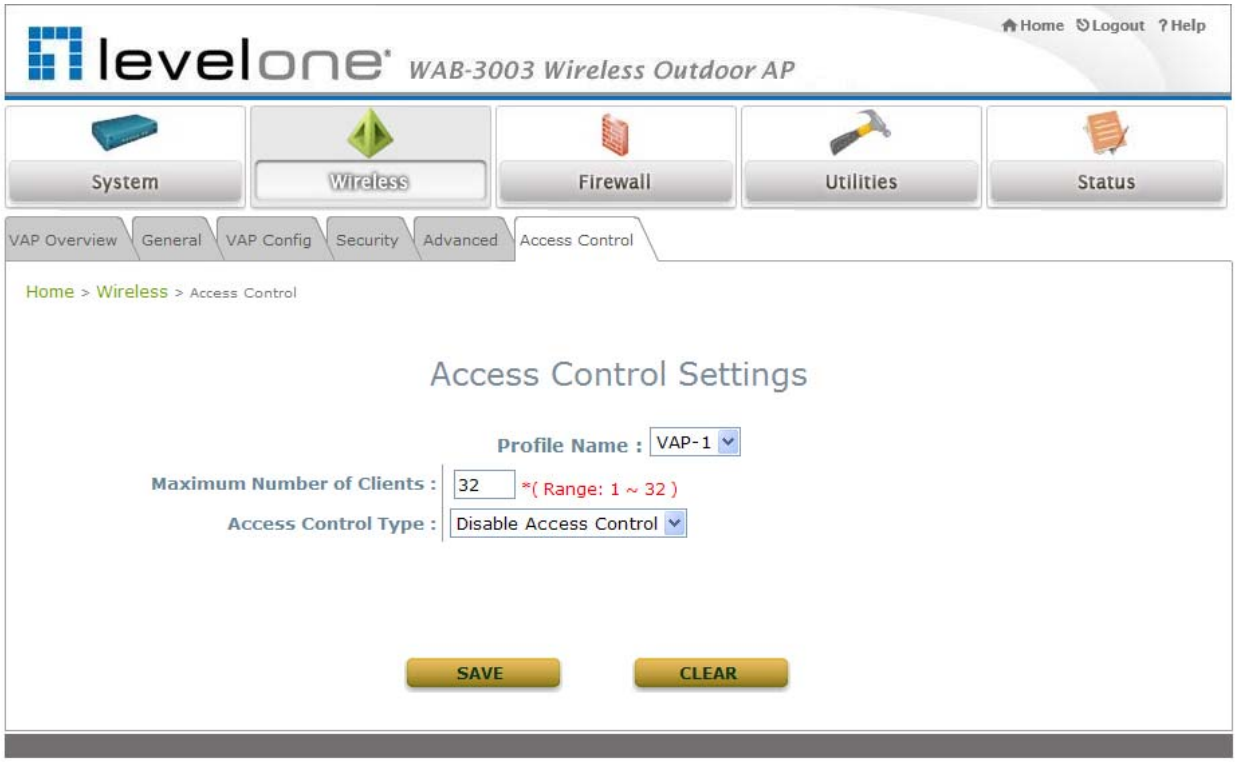
- **RTS Threshold:** To control station access to the medium and to alleviate this effect of the hidden terminal problem, the administrator can tune this RTS threshold value. A lower RTS Threshold setting can be useful in areas where many client devices are associating with WAB-3003 or in areas where the clients are far apart and can detect only WAB-3003 and not each other.
- **Fragmentation Threshold:** A unicast frame larger than this threshold will be fragmented before transmission. If a significant number of collisions are occurring, the administrator can try to set a smaller value of the threshold to see whether it helps. A smaller value results in smaller packets but allows a larger number of packets in transmission. A lower Fragment Threshold setting can be useful in areas where communication is poor or disturbed by a serious amount of radio interference.
- **Broadcast SSID:** Disabling this function will prevent the system from broadcasting its SSID. If you disable broadcast of the SSID, only devices that have the correct SSID can connect to the system.
- **Station Isolation:** By enabling this function, all stations associated with the system can only communicate with the system.
- **WMM**: The default is *Disable*. Wi-Fi Multimedia (WMM) is a Quality of Service (QoS) feature that prioritizes wireless data packets based on four access categories: voice, video, best effort, and background. Applications without WMM and applications that do not require QoS are assigned to the best-effort category, which receives a lower priority than voice and video. In short, WMM decides which data streams are the most important and assign them a higher traffic priority.

  < To receive the benefits of WMM QoS >

  - The application must support WMM.
  - You must enable WMM in this system.
  - You must enable WMM in the wireless adapter in your computer.
- **IAPP:** IAPP (Inter Access Point Protocol) is a protocol by which access points share information about the stations that are connected to them. By enabling this function, the system will automatically broadcast information of associated wireless stations to its peer access points. This will help wireless stations roam smoothly among IAPP-enabled access points in the same wireless LAN.
- **802.11g Protection:** When enabled, the associated 802.11g stations will benefit from this function since their transmission speed will not be affected by the surrounding 802.11b stations.

4.2.6 Access Control Settings

The administrator can restrict the wireless access of client devices based on their MAC addresses.



- **Maximum Number of Clients**

  The system supports various methods of authenticating clients for using wireless LAN. The default policy is unlimited access without any authentication required. To restrict the station number of wireless connections, simply change the **Maximum Number of Stations** to a desired number. For example, while the number of stations is set to 20, only 20 stations are allowed to connect to the specified VAP.

- **Access Control Type**

  The selected **Access Control Type** will be the activated policy while the rest will be omitted. The following is a list of the supported methods for MAC ACL control:

  (1) Disable Access Control

  No MAC address check required.

(2) MAC ACL Allow List

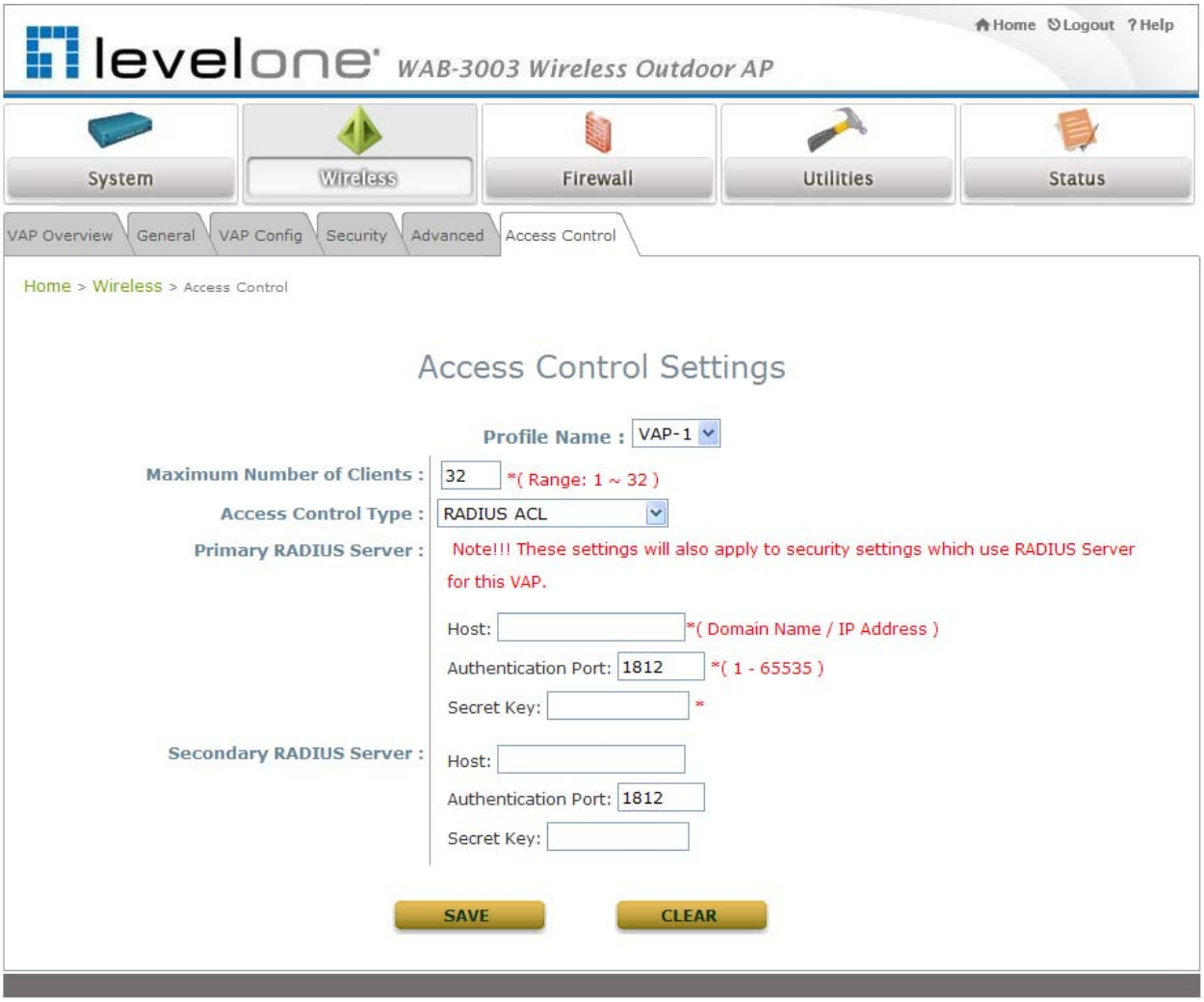
Deny all except those MAC addresses in the Allow List. When selecting *MAC ACL Allow List*, all wireless connections to the specified VAP will be denied except the MAC addresses listed in the Allow List ("allowed MAC addresses"). The administrator can disable any allowed MAC address to connect to the VAP temporarily by checking *Disable*. For example, 11:22:33:44:55:66 is in the Allow List; to temporarily deny its access, check *Disable* in the **State** section.

(3) MAC ACL Deny List

Allow all except those in the Deny List. When selecting *MAC ACL Deny List*, all wireless connections to the specified VAP will be allowed except the MAC addresses listed in the Deny List ("denied MAC addresses"). The administrator can allow any denied MAC address to connect to the VAP temporarily by checking *Enable*.

(4) RADIUS ACL

Authenticate incoming MAC addresses by RADIUS. When selecting *RADIUS ACL*, all incoming MAC addresses will be authenticated by RADIUS. Please note that each VAP's MAC ACL and its security type (showing on the **Security Settings** page) share the same RADIUS configuration.

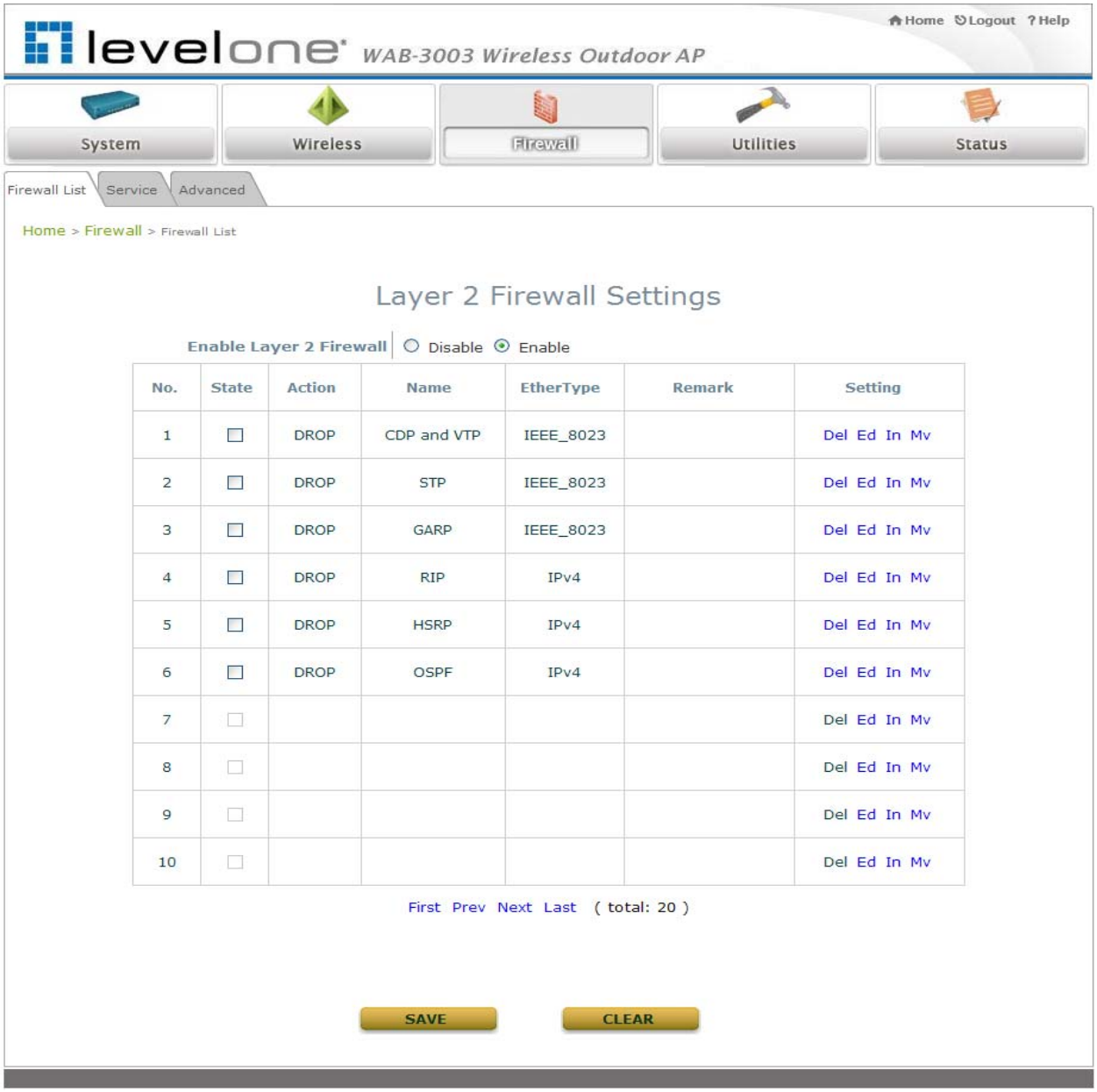


4.3 Firewall

The system provides an added security feature, L2 firewall, in addition to typical AP security. Layer-2 firewall offers a firewall function that is tailored specifically for layer 2 traffics, providing another choice of shield against possible security threats coming from/going to WLAN (AP interfaces); hence, besides firewall policies configured on gateways, this extra security feature will assist to mitigate possible security breach.

4.3.1 Layer 2 Firewall Settings

It provides an overview of firewall rules in the system; 6 default rules with up to total 20 firewall rules are available for configuration.

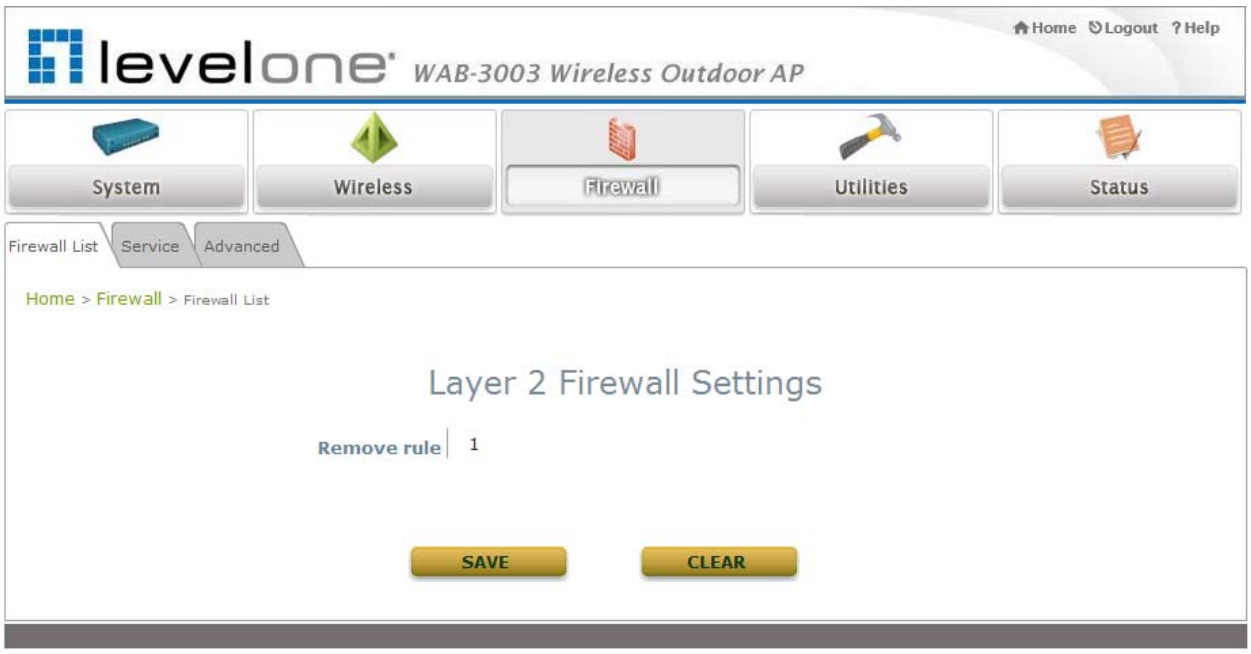


From the overview table, each rule is designated with the following fields:

- **No.:** The numbering will decide the priority to let system carry out the available firewall rules in the table.
- **State:** The check marks will enable the respective rules.
- **Action**: "DROP" denotes a block rule; "ACCEPT" denotes a pass rule.
- **Name:** It shows the name of rule.
- **EtherType:** It denotes the type of traffics subject to this rule.
- **Remark:** It shows the note of this rule.
- **Setting:** 4 actions are available; "Del" denotes to delete the rule, "Ed" denotes to edit the rule, "In" denotes to insert a rule, and "Mv" denotes to move the rule.

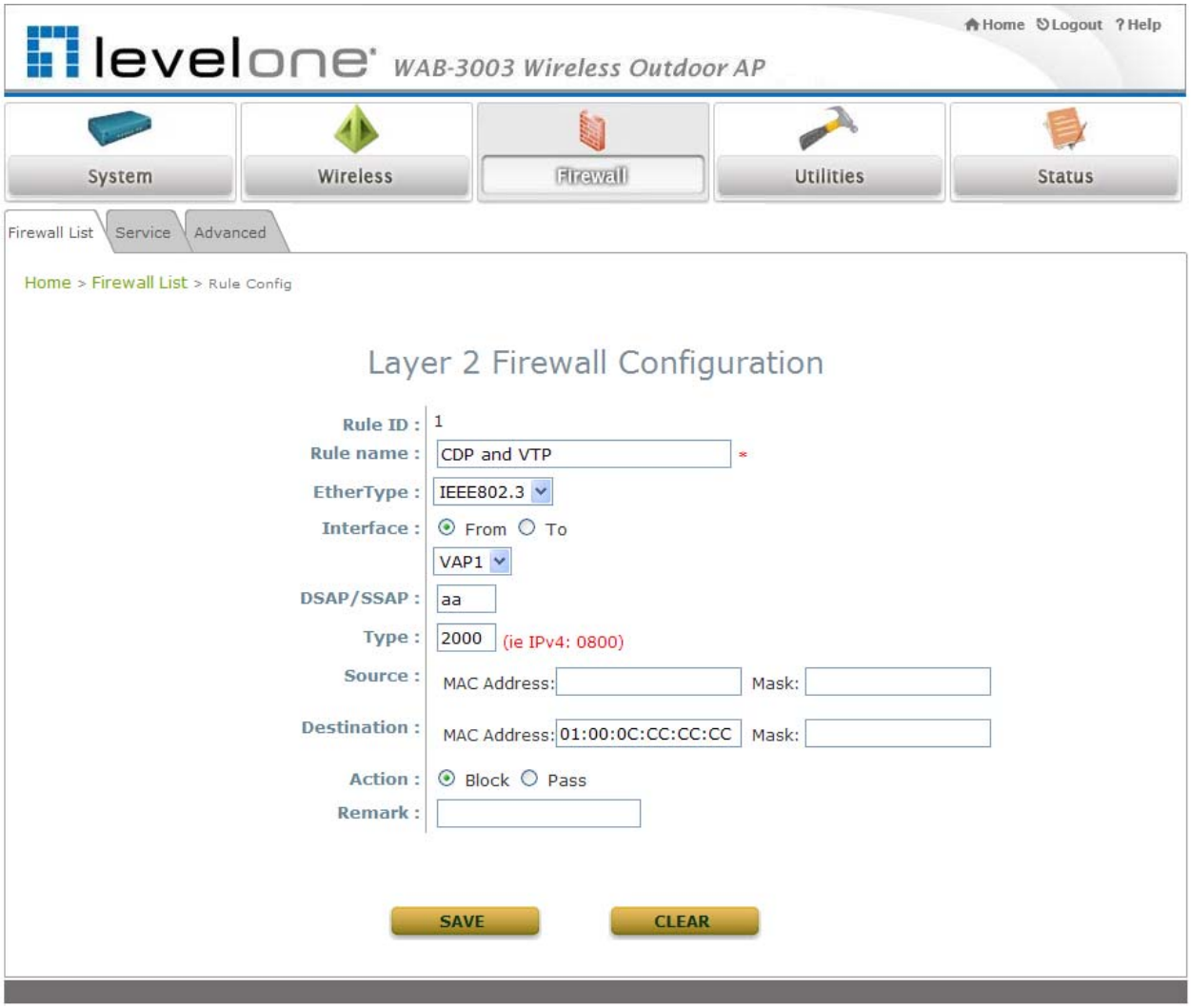
>>To delete a specific rule,

"Del" in "Setting" column of firewall list will lead to the following page for removal confirmation. After "SAVE" button is clicked and system reboot, the rule will be removed.



>>To edit a specific rule,

"Ed" in "Setting" column of firewall list will lead to the following page for detail configuration. From this page, the rule can be edited form scratch or from an existing rule for revision.



- **Rule ID:** The numbering of this specific rule will decide its priority among available firewall rules in the table.
- **Rule name:** The rule name can be specified here.
- **EtherType:** The drop-down list will provide the available types of traffics (ALL, IPv4, IEEE802.3, 802.1Q, ARP, and RARP) subject to this rule.
- **Interface:** It can indicate inbound/outbound direction with desired interfaces (VAP1~VAP8)
- **Service (when EtherType is IPv4):** Select the available upper layer protocols/services from the drop-down list.
- **DSAP/SSAP (when EtherType is IEEE802.3):** The value can be further specified for the fields in 802.2 LLC frame header.
- **Type (when EtherType is IEEE802.3):** The field can be used to indicate the type of encapsulated traffics.

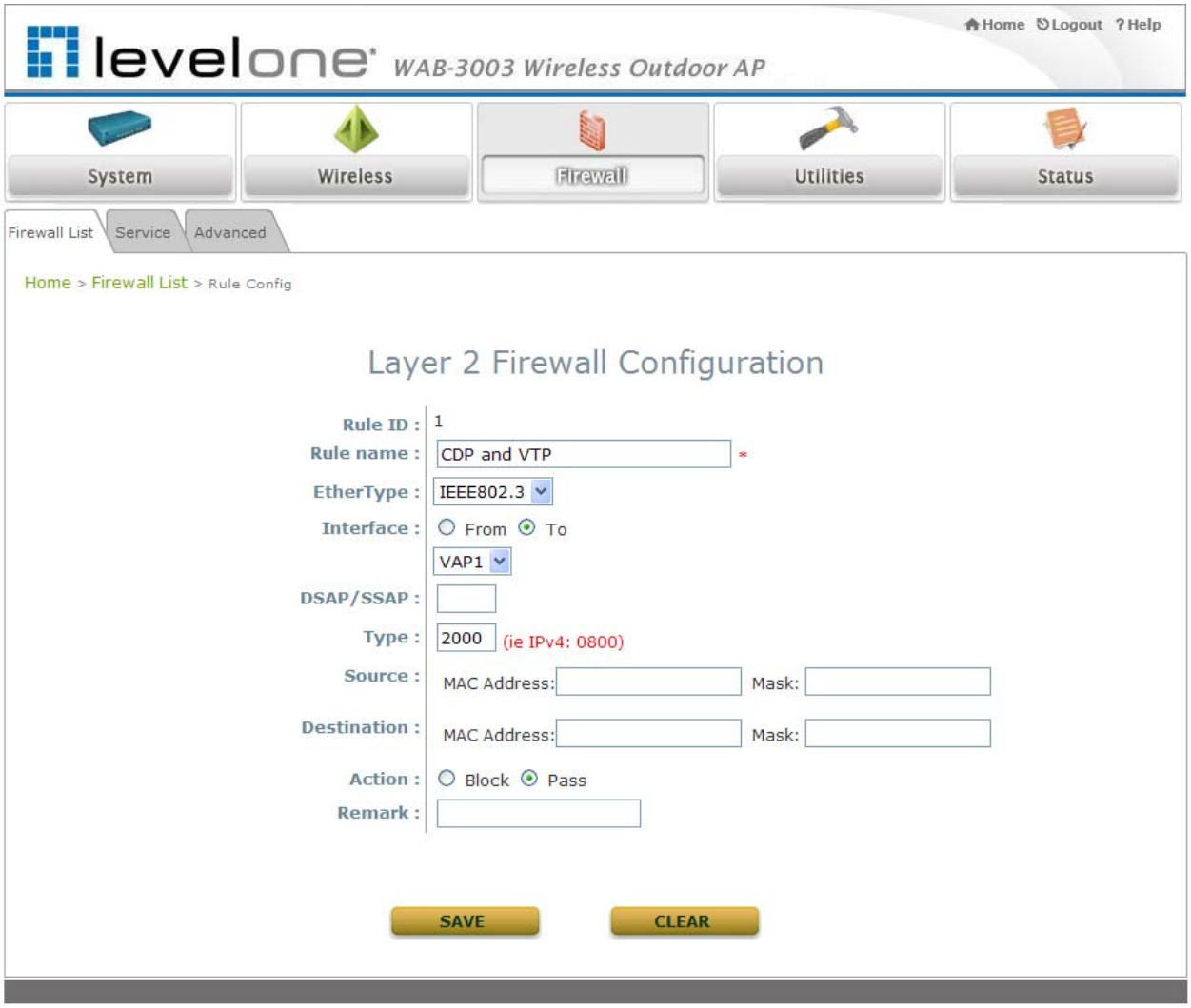
- **Vlan ID (when EtherType is 802.1Q):** The Vlan ID is provided to associate with certain VLAN-tagging traffics.
- **Priority (when EtherType is 802.1Q):** It denotes the priority level with associated VLAN traffics.
- **Encapsulated Type (when EtherType is 802.1Q):** It can be used to indicate the type of encapsulated traffics.
- **Opcode (when EtherType is ARP/RARP):** This list can be used to specify the ARP Opcode in ARP header.
- **Source:** MAC Address/Mask indicates the source MAC; IP Address/Mask indicates the source IP address (when EtherType is IPv4); ARP IP/MAC & MASK indicate the ARP payload fields.
- **Destination:** MAC Address/Mask indicates the destination MAC; IP Address/Mask indicates the destination IP address (when EtherType is IPv4); ARP IP/MAC & MASK indicate the ARP payload fields.
- **Action:** The rule can be chosen to be "Block" or "Pass".
- **Remark:** The note of this rule can be specified here.

When the configuration for firewall rules is provided, please click "**SAVE**" and reboot system to let the firewall rules take effect.

>>To insert a specific rule,

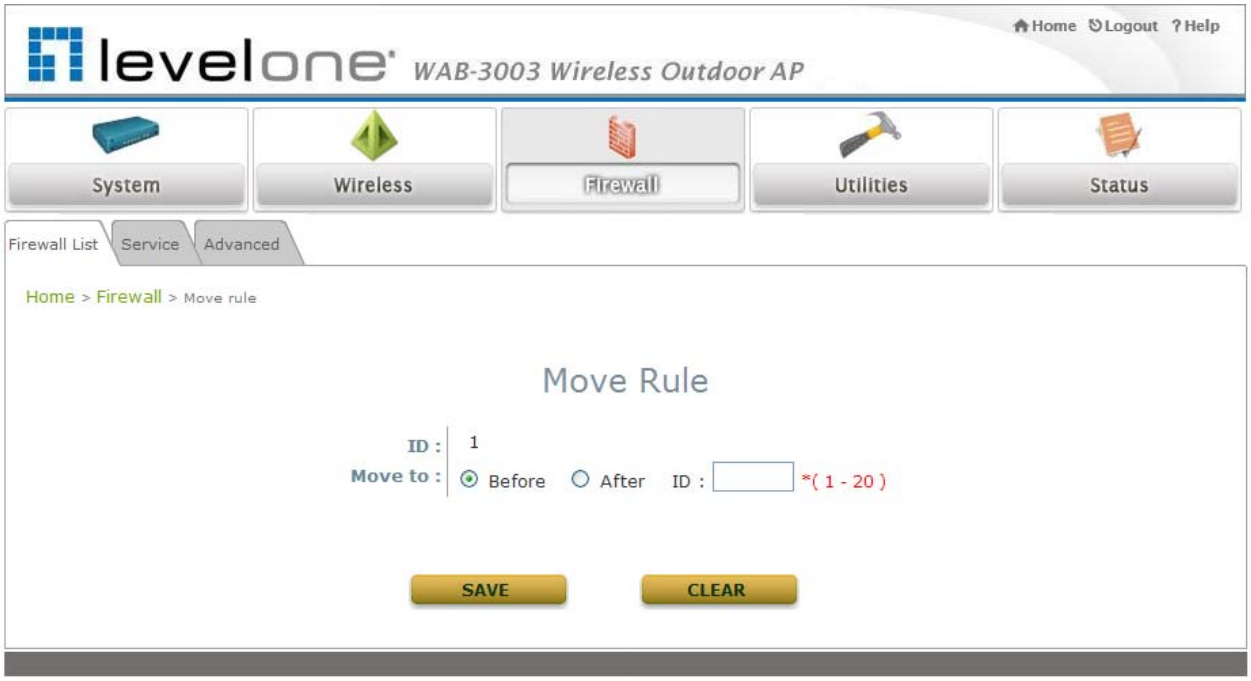
"In" in "Setting" column of firewall list will lead to the following page for detail configuration with rule ID for the current inserted rule.

From this page, the rule can be edited form scratch or from an existing rule for revision.

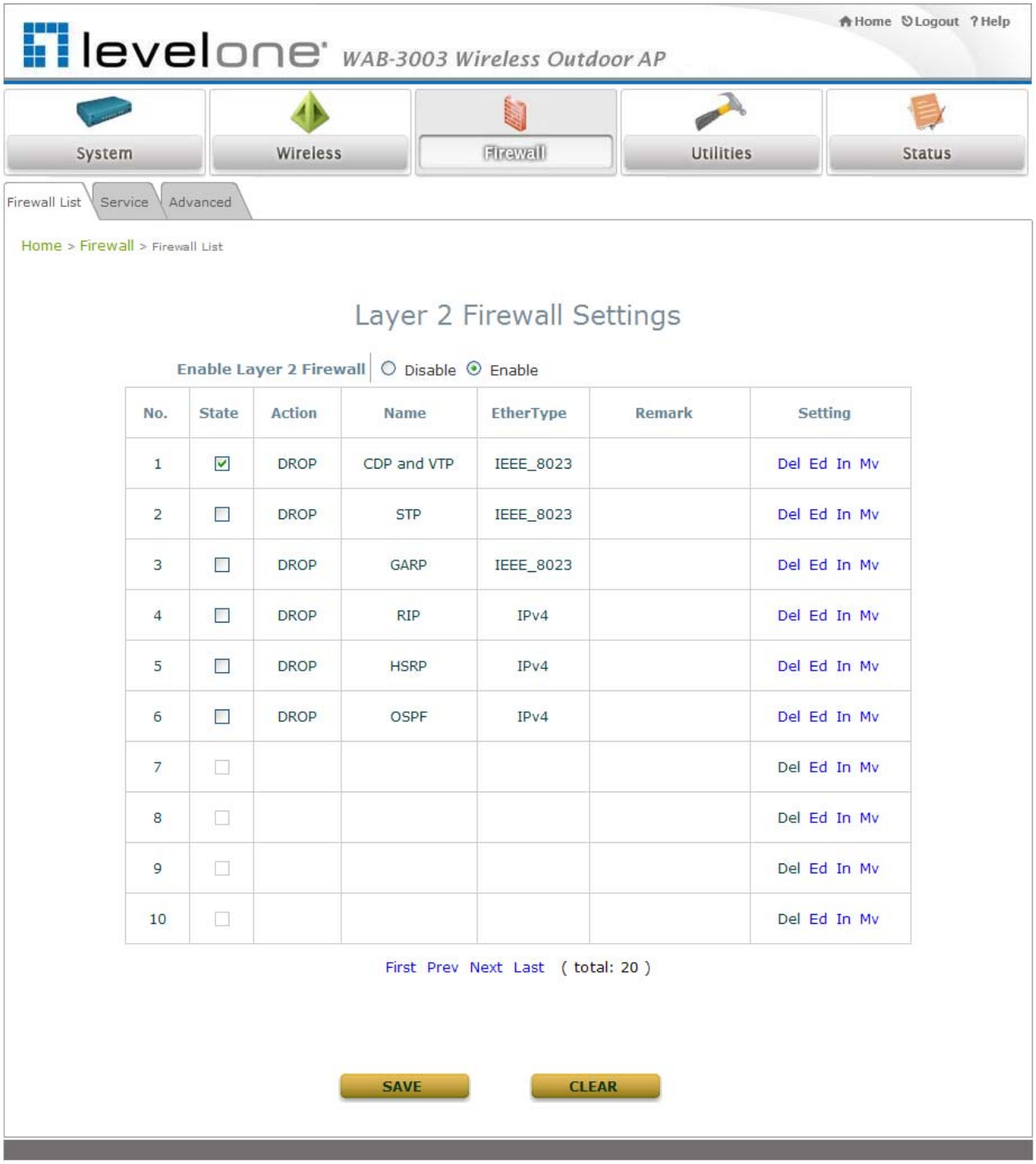


>>To move a specific rule,

"Mv" in "Setting" column of firewall list will lead to the following page for re-ordering confirmation. After "**SAVE**" button is clicked and system reboot, the order of rules will be updated.



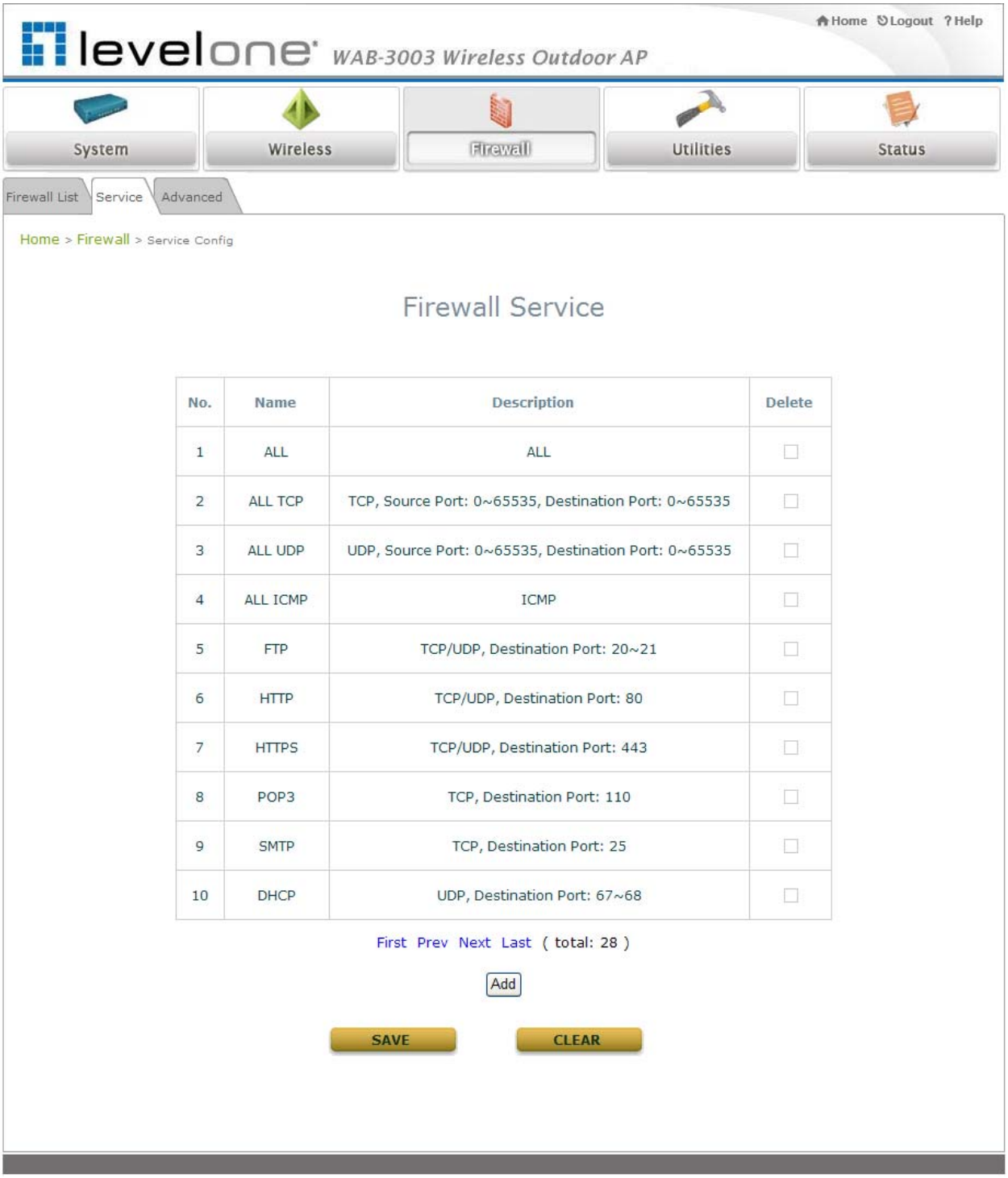
Please make sure all desired rules (state of rule) are **checked** and **saved** in overview page; the rule will be enforced upon system reboot.



Layer 2 Firewall Settings (Check State)

4.3.2 Firewall Service

The administrator can add or delete firewall services here; the services in this list will become options to choose in firewall rule (when EtherType is IPv4).

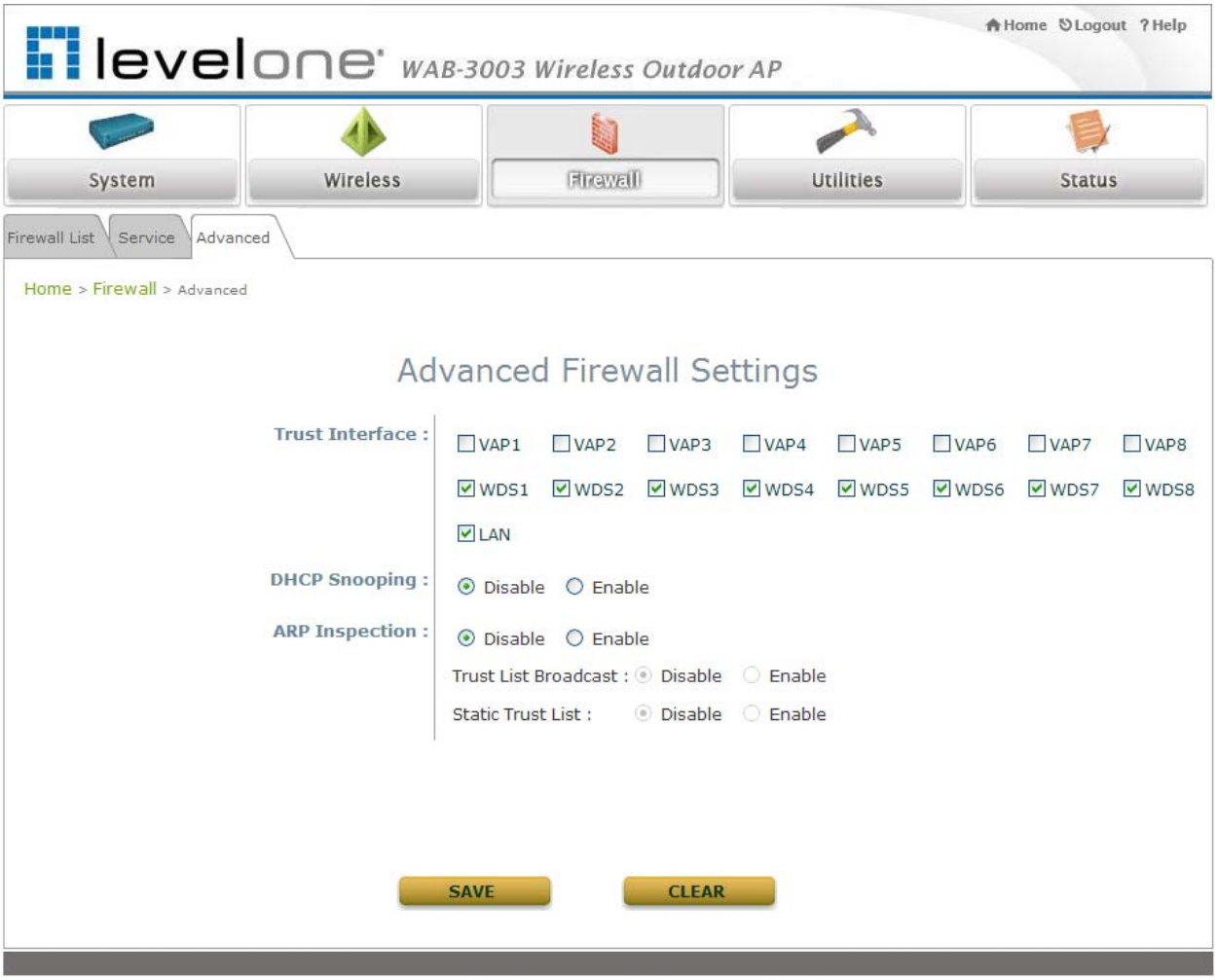


Overview of Firewall Services

There are 28 firewall services available in default settings; these default services cannot be deleted but can be disabled. If changes are made, please click SAVE to save the settings before leaving this page.

4.3.3 Advanced Firewall Settings

Advanced firewall settings are used to supplement the firewall rules, providing extra security enhancement against DHCP and ARP traffics traversing the available interfaces of system.

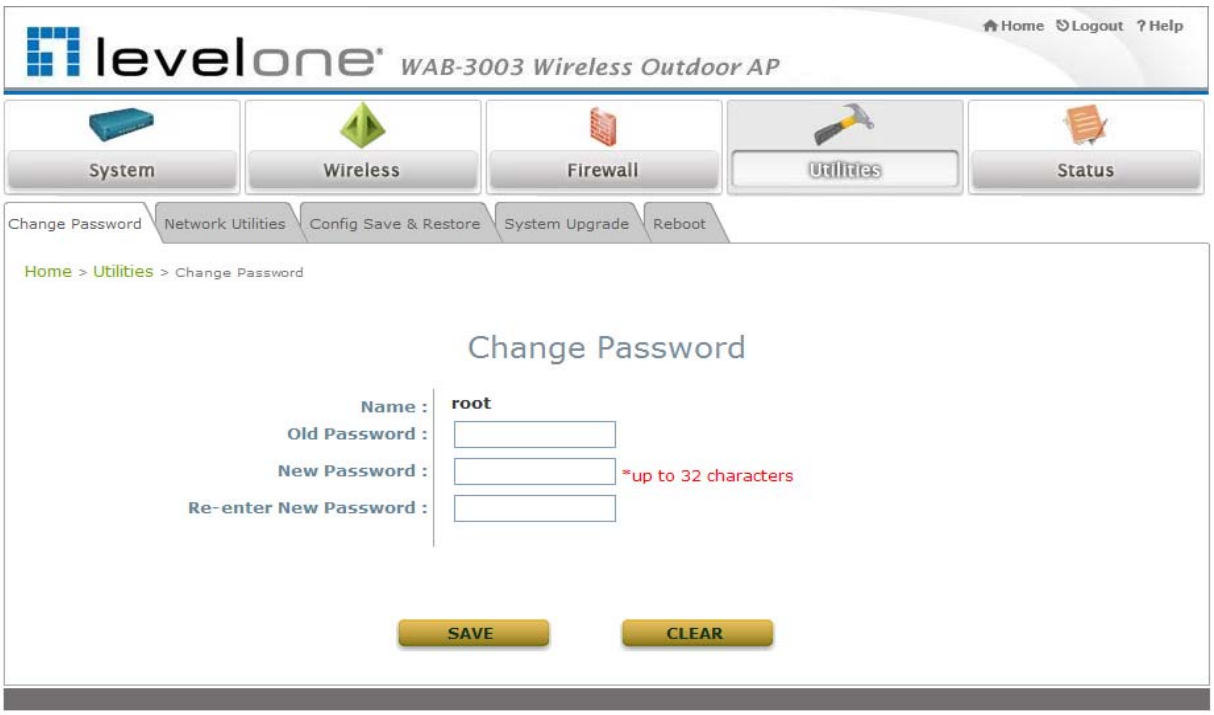


- **Trust Interface:** Each interface can be checked individually to mark as trusted interfaces; security enforcements on DHCP/ARP like DHCP snooping and ARP inspection will be carried out on non-trusted interfaces.
- **DHCP Snooping:** When enabled, DHCP packets will be validated against possible threats like DHCP starvation attack; in addition, the trusted DHCP server (IP/MAC) can be specified to prevent rogue DHCP server.
- **ARP Inspection:** When enabled, ARP packets will be validated against ARP spoofing. **Trust List Broadcast** can be enabled to let other WAB-3003 (with L2 firewall feature) learn the trusted MAC/IP pairs to issue ARP requests. **Static Trust List** can be used to add MAC or MAC/IP pairs to issue ARP request. Other network nodes can still send their ARP requests; however, if their IP appears in the static list (with different MAC), their ARP requests will be dropped to prevent eavesdropping.

If any settings are made, please click ***SAVE*** to save the configuration before leaving this page.

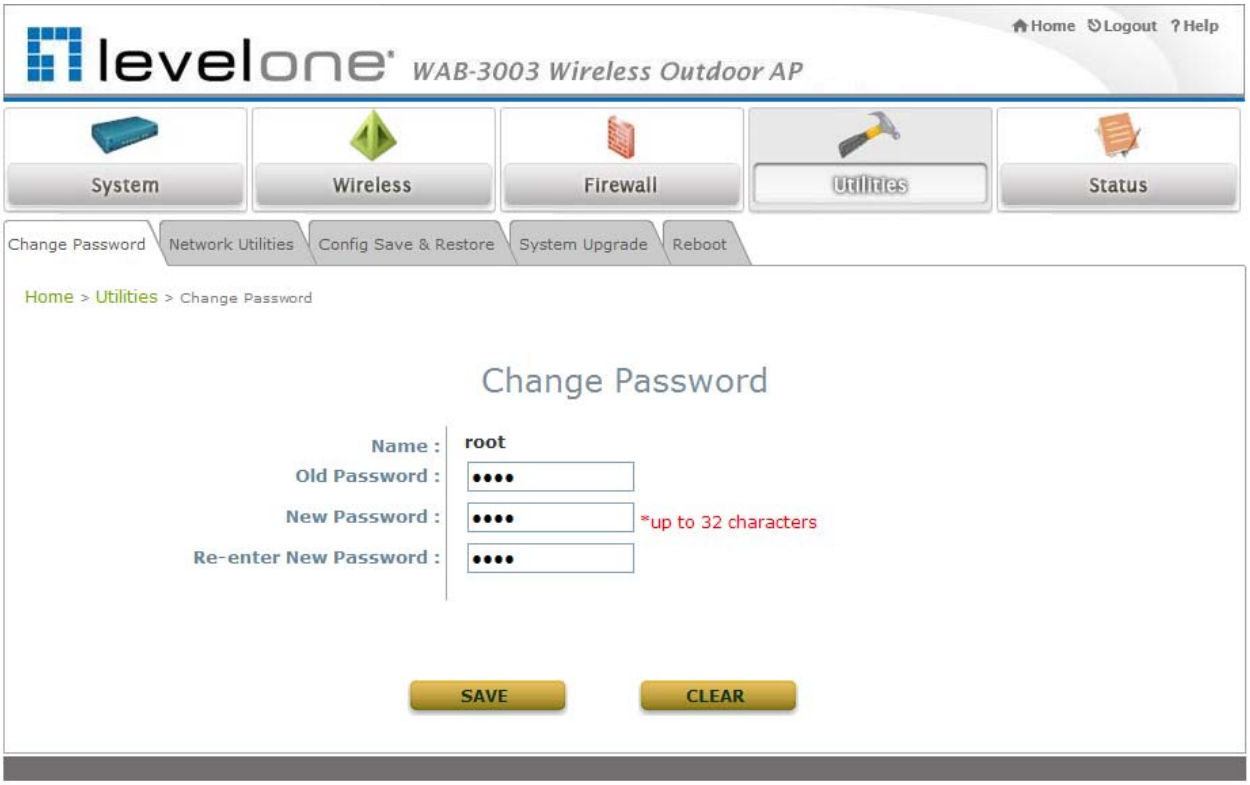
4.4 Utilities

The administrator can maintain the system on this page: **Change Password**, **Network Utilities**, **Configuration Save & Restore**, **System Upgrade**, and **Reboot**.



4.4.1 Change Password

The administrator can update or change password. The system provides one management account for AP mode, **root** account. The administrator can change password on this page.

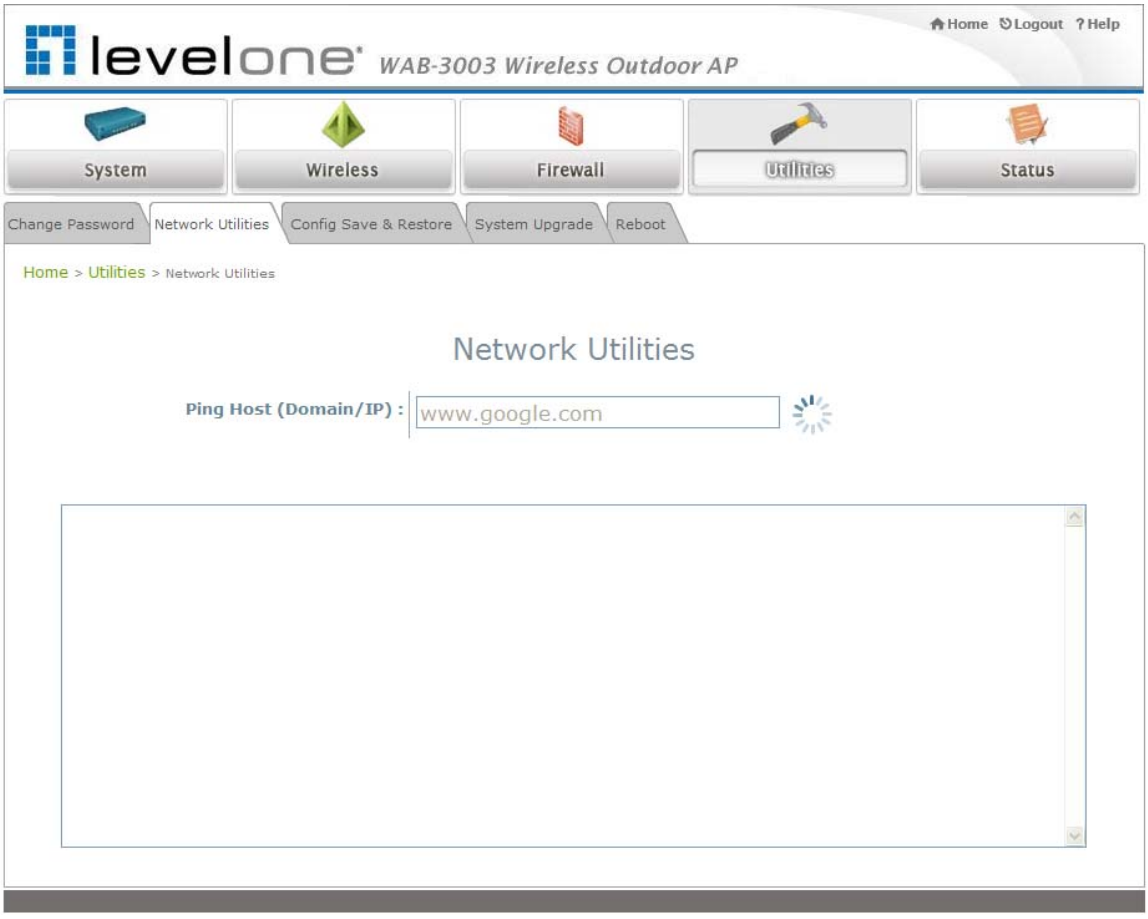


- **"root" account:** Enter the original password (**"admin"**) and a new password, and then re-enter the new password in the *Re-enter New Password* field. Click ***SAVE*** to save the new password.

4.4.2 Network Utilities

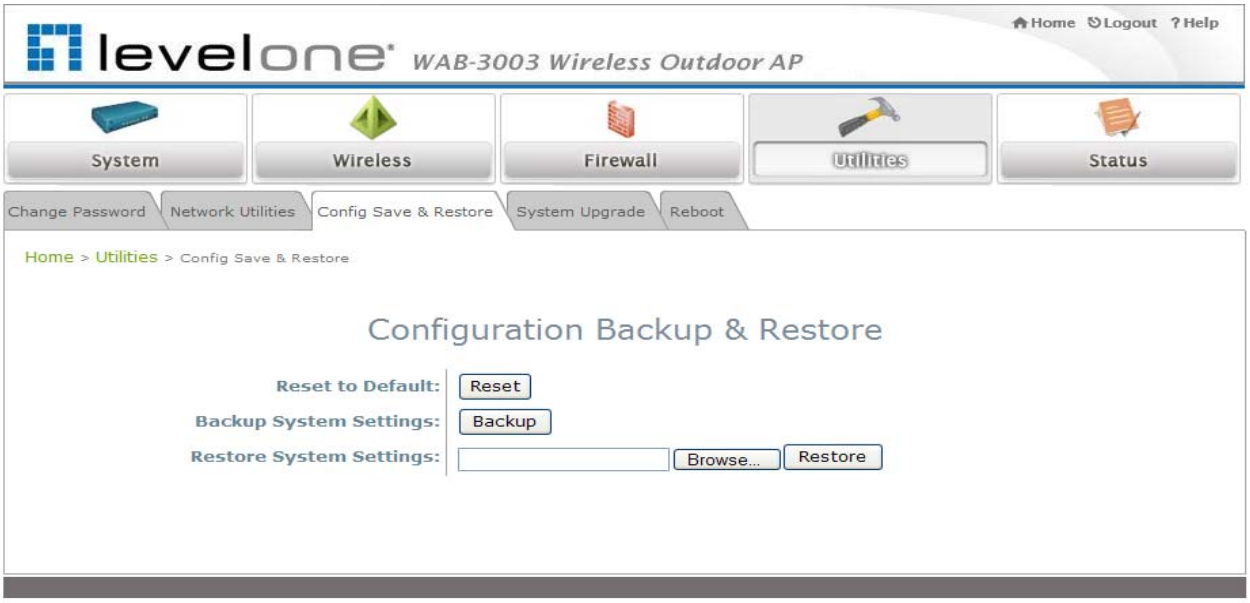
The administrator can check the network connectivity via this function. The current provided network utility is Ping and the target host FQDN-compliant name or IP address can be provided to test network connection.

- **Ping Host (Domain/ IP):** Enter the domain name or IP address of a target device for diagnosis purpose, for example, www.google.com.tw, and click ***Ping*** to proceed. The ping result will be shown in the **Result** field.

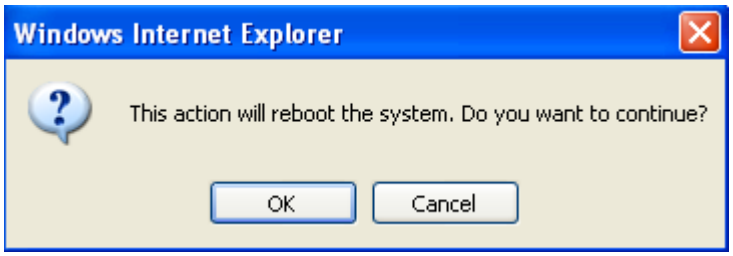


4.4.3 Configuration Save & Restore

This function is used to backup or restore the current settings. The system can be restored to the default setting by clicking on Reset. The setting of the device can be backup to a file. It can be used to duplicate setting to the other WAB-3003 device.



- **Reset to Default:**
  - Click ***Reset*** to load the factory default settings of WAB-3003. A pop-up screen will appear to reconfirm the request to restart the system. Click ***OK*** to proceed, or click ***Cancel*** to cancel the restart request.



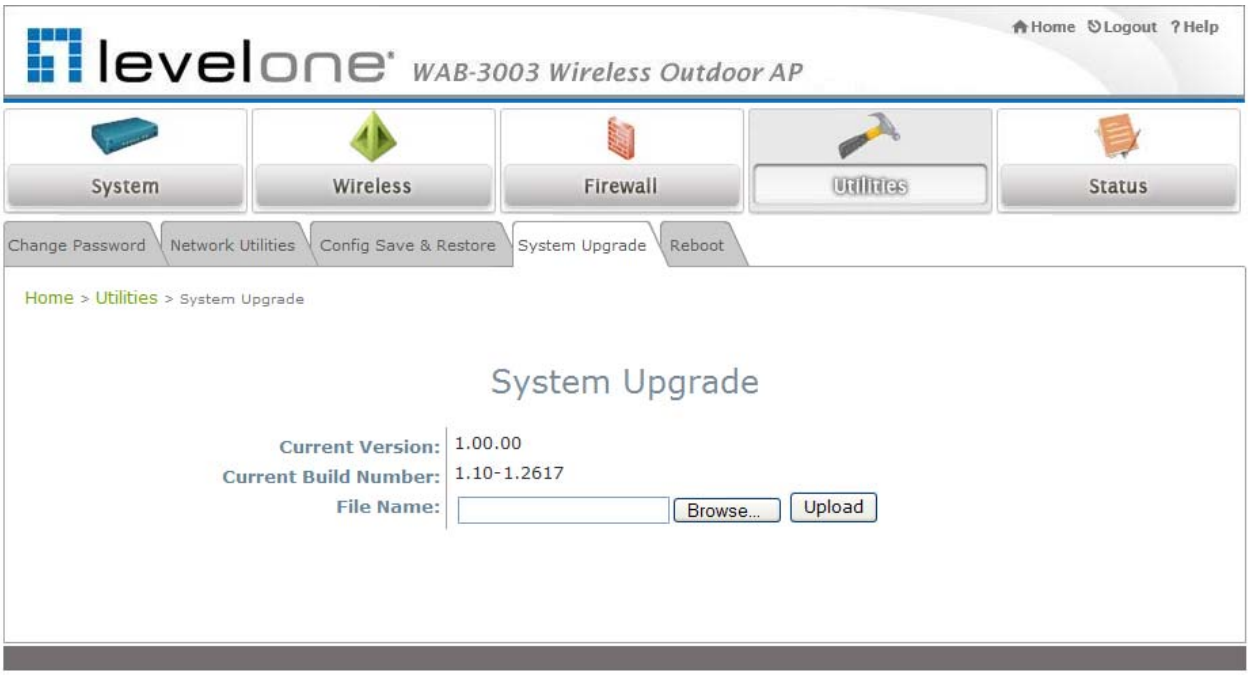
  - A warning message as displayed below will appear during the reboot period. The system power must be turned on before the completion of the reboot process.
  - The **System Overview** page will appear upon the completion of reboot.

- **Backup Settings:** Click ***Save*** to save the current system settings to a local disk such as the hard disk drive (HDD) of a local computer or a compact disc (CD).

- **Restore Settings:** Click ***Browse*** to search for a previously saved backup file, and then click ***Upload*** to restore the settings. The backup file will replace the active configuration file currently running on the system.

4.4.4 System Upgrade

To upgrade the system firmware, click ***Browse*** to search for the new firmware file, and then click ***Apply*** to execute the upgrade process. The first step is to acquire the correct firmware file and supply it in the User Interface field. During firmware update, please don't turn off the power to prevent from damaging the device permanently.

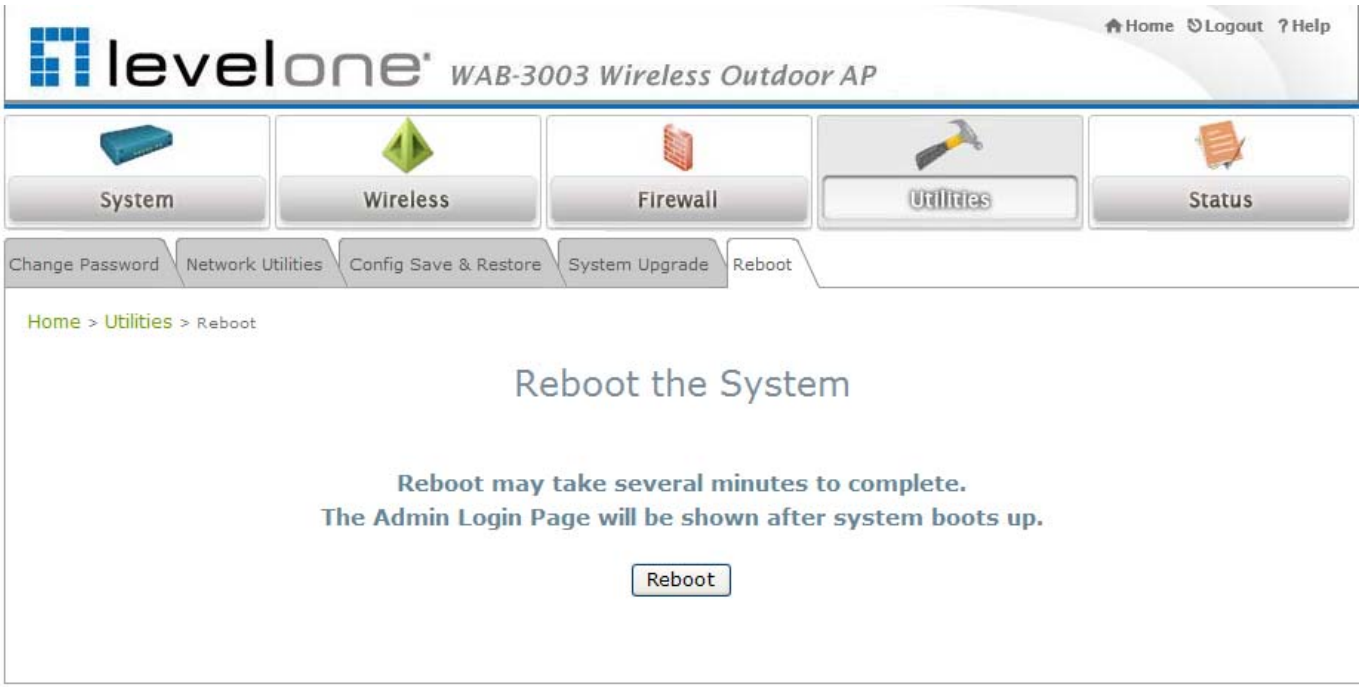


Note:

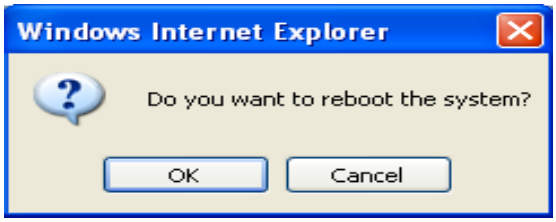
- To prevent data loss during firmware upgrade, please back up the current settings before proceeding further.
- Please restart the system after the upgrade. Do not interrupt the system, i.e. power on/off, during the upgrade or restart process since it may cause damage to the system.

4.4.5 Reboot

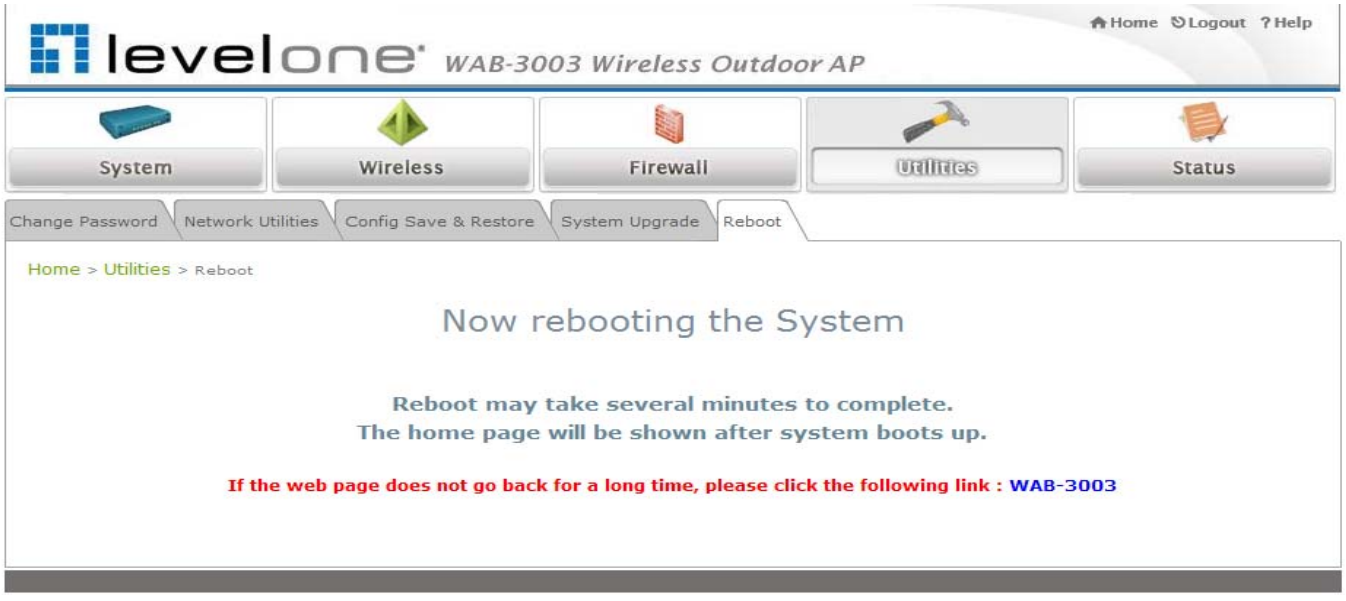
The administrator can reboot the device remotely. Click ***Reboot*** to restart the system immediately.



A pop-up screen will appear to confirm the request to restart the system. Click ***OK*** to proceed, or click ***Cancel*** to cancel the restart request.



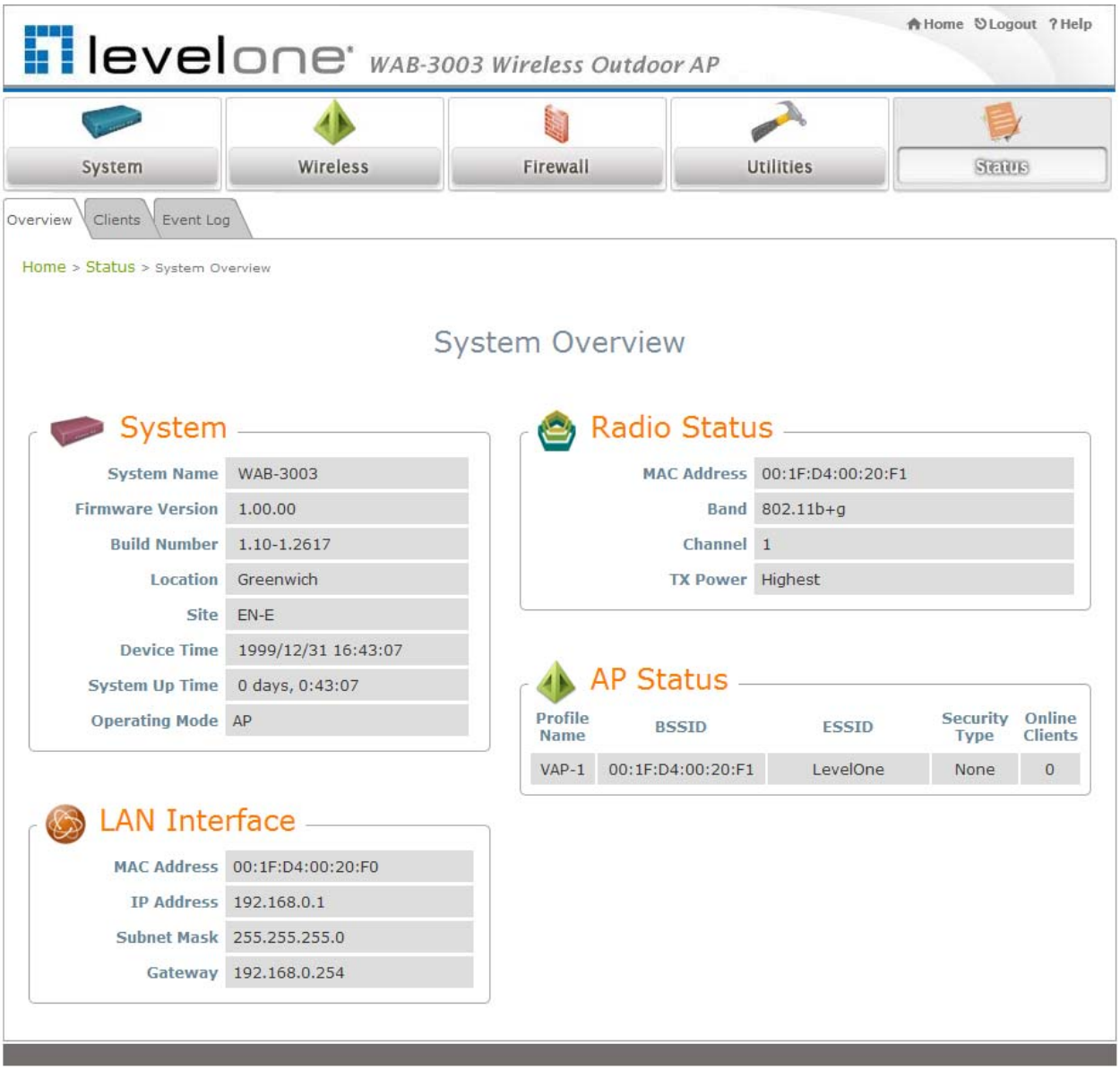
A warning message as displayed below will appear during the reboot period. The system power must be turned on before the completion of the reboot process.



The **System Overview** page will appear upon the completion of reboot.

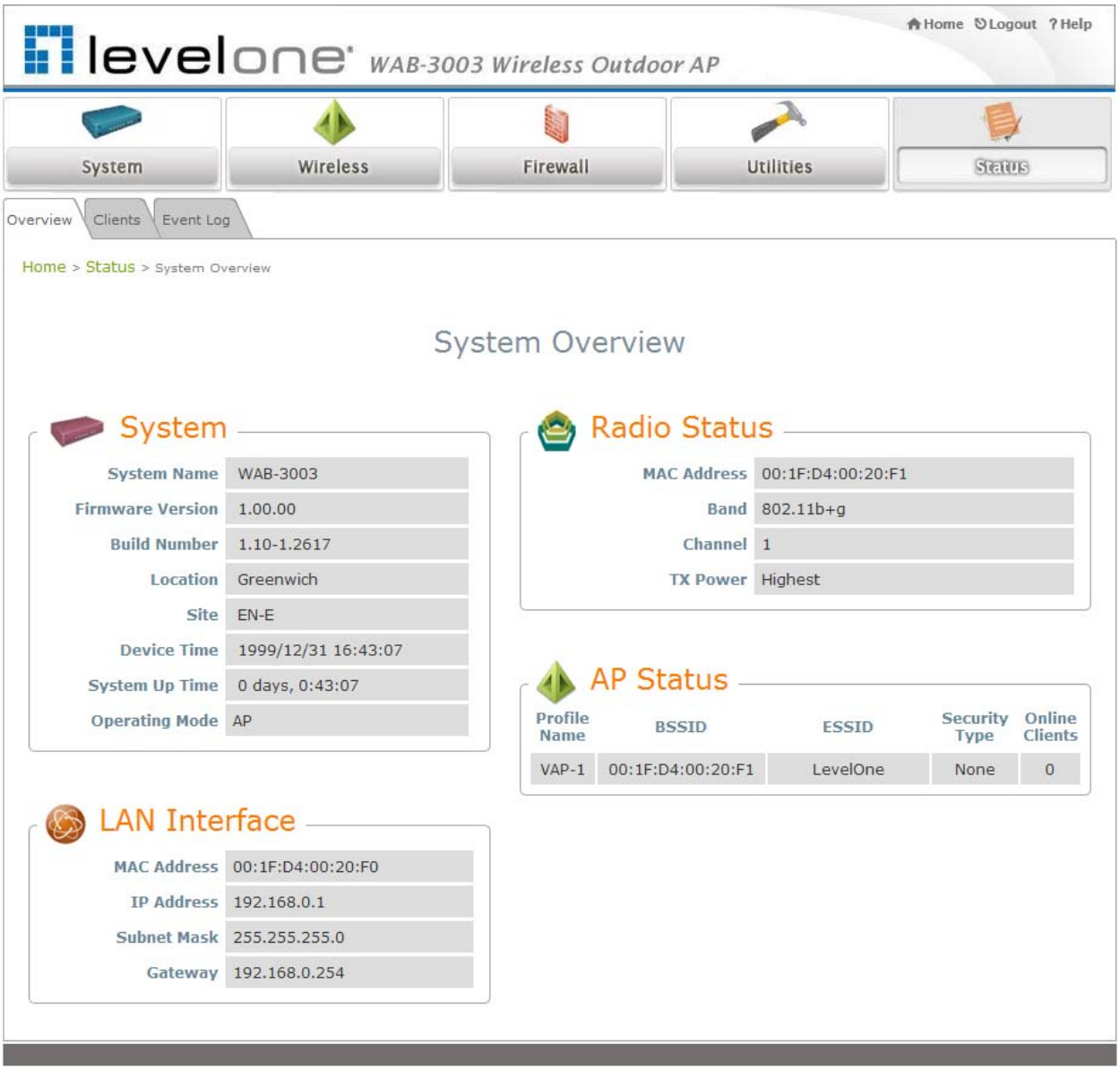
4.5 Status

This section displays the status of **System Overview**, **Clients**, and **Event Log**.



4.5.1. System Overview

The **System Overview** page provides an overview of the system status for the administrator.

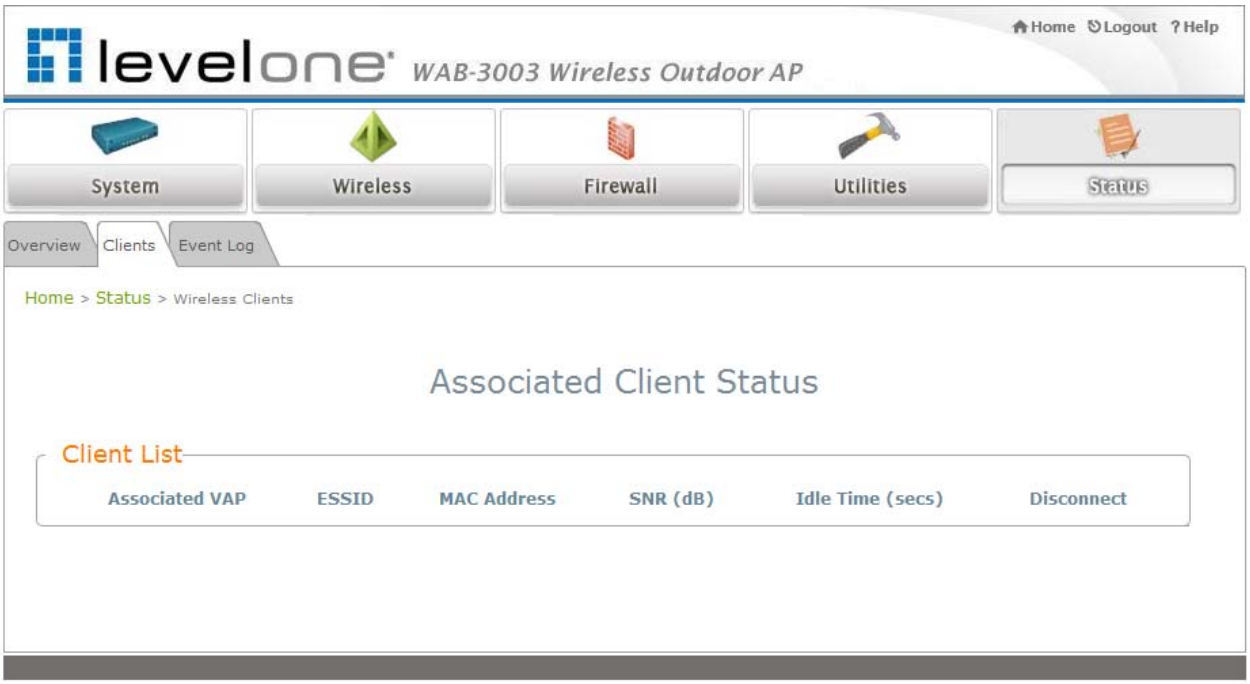


The description of the table is shown below:

ITEM		DESCRIPTION
System	System Name	The name provided in System Information.
	Firmware Version	The present firmware version of the system.
	Build Number	The Build Number of the firmware.
	Location	The location provided in System Information.
	Site	The firmware version for specific region.
	Device Time	The current time on the device.
	System Up Time	The system elapsing time since last reboot.
LAN Interface	MAC Address	The MAC address of LAN Interface.
	IP Address	The IP address of the LAN Interface.
	Subnet Mask	The Subnet Mask of the LAN Interface.
	Gateway	The gateway of LAN interface.
Radio Status	MAC Address	The MAC address of RF interface.
	Band	The operating band.
	Channel	The operating channel.
	Tx Power	The level of transmitted power.
AP Status	BSSID	The BSSID (MAC) of AP.
	ESSID	The assigned ESSID of AP.
	Security Type	The security type of AP.
	Online Client	The number of online clients associated with AP.

4.5.2. Associated Client Status

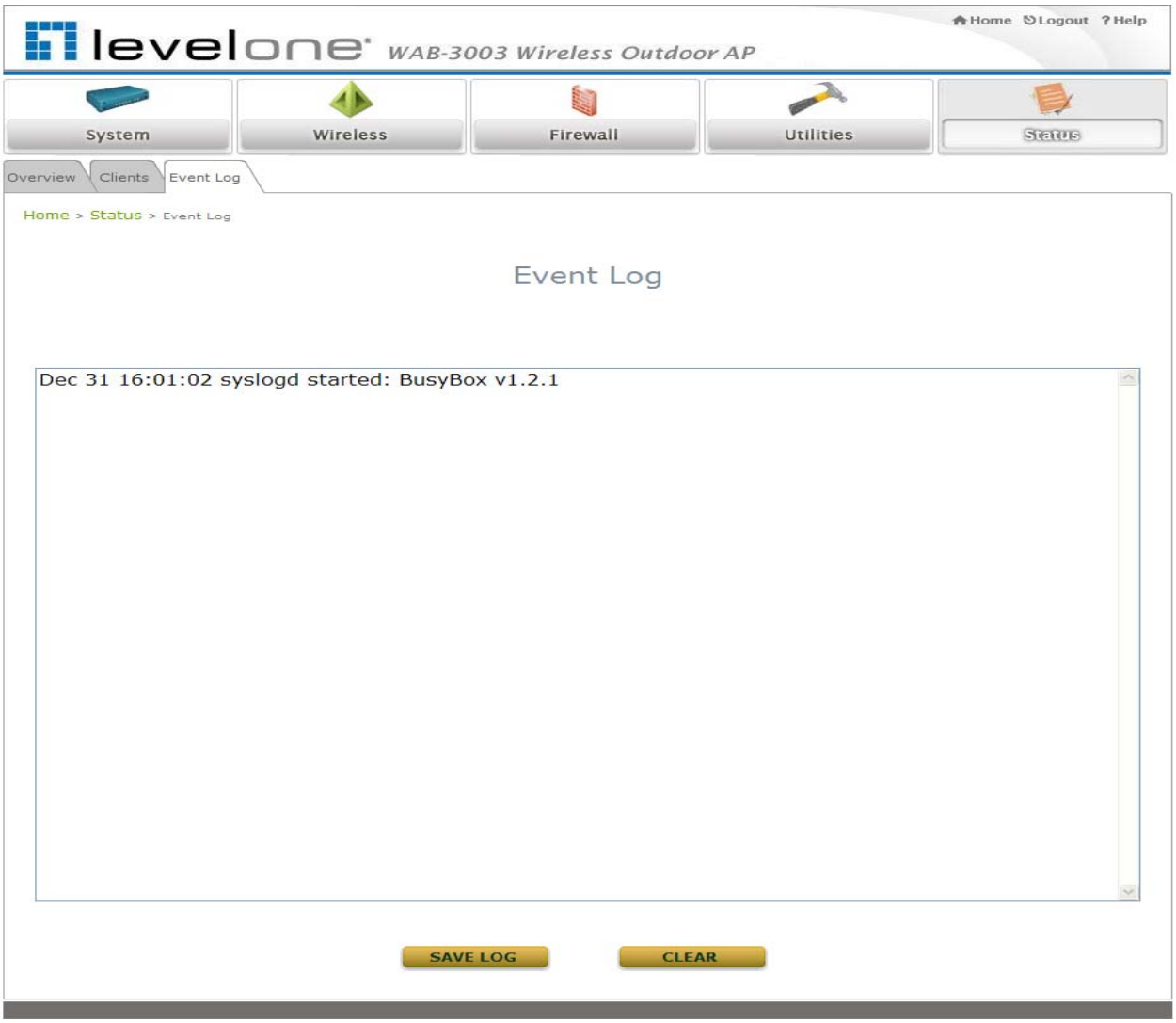
The administrator can remotely oversee the status of all associated clients on this page. Associated client's MAC, SNR and Idle Time are listed in the table.



- **ESSID:** The Extended Service Set ID which the client is associated with.
- **MAC Address:** The MAC address of associated clients.
- **SNR:** The Signal to Noise Ratio of respective client's association.
- **Idle Time:** Time period that the associated client is inactive; the time unit is in second.

4.5.3. Event Log

Event log provides the records of the system activities. All the system events are shown here.



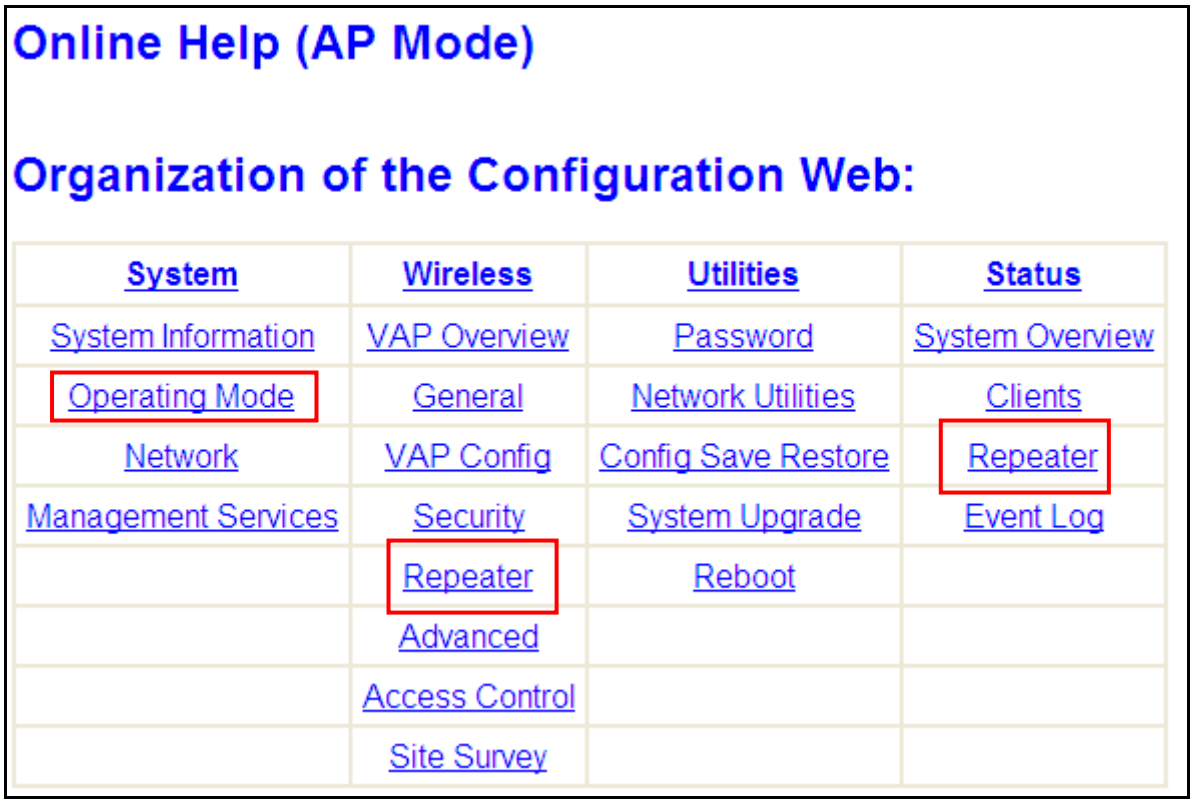
Note:
As the Event Log is stored in RAM, it will be refreshed after the system is restarted. The system also supports a Syslog reporting function of reporting the events to an external Syslog server.

- **Date / Time:** The date and time when the event happened.
- **Hostname:** Indicate which Host records this event. Note that all events in this page are local events and this field of all events is the same. However, in remote Syslog service, this field will help the network administrator identify which event is from this system. For more information, please refer to **Section 4.1.4 Management Services**.
- **Process name (with square brackets):** Indicate which process with the specific event is associated.
- **Description:** Description of the event.

4.6 Online Help

The ***Help*** button is at the upper right hand corner of the display screen.

Click ***Help*** for the **Online Help** window, and then click the hyperlink of the desired topic for further information.



Online Help (AP Mode)

Organization of the Configuration Web:

System	Wireless	Utilities	Status
System Information	VAP Overview	Password	System Overview
Operating Mode	General	Network Utilities	Clients
Network	VAP Config	Config Save Restore	Repeater
Management Services	Security	System Upgrade	Event Log
	Repeater	Reboot	
	Advanced		
	Access Control		
	Site Survey		

*** These features have not officially been released for supports The WAB-3003 (In red square)**

***System=>Operating Mode**

***Wireless=>Repeater**

***Status=>Repeater**