4ipnet EAP100
User's Manual

V1.00

Copyright Notice

Disclaimer

Trademarks

Table of Contents

1. Introduction

1.1 Overview

This manual is intended for system integrators, field engineers and network administrators to set up 4ipnet EAP100 Enterprise Access Points in their network environments. It contains step-by-step procedures and graphic examples to guide MIS staff or individuals with basic network system knowledge to complete the installation.

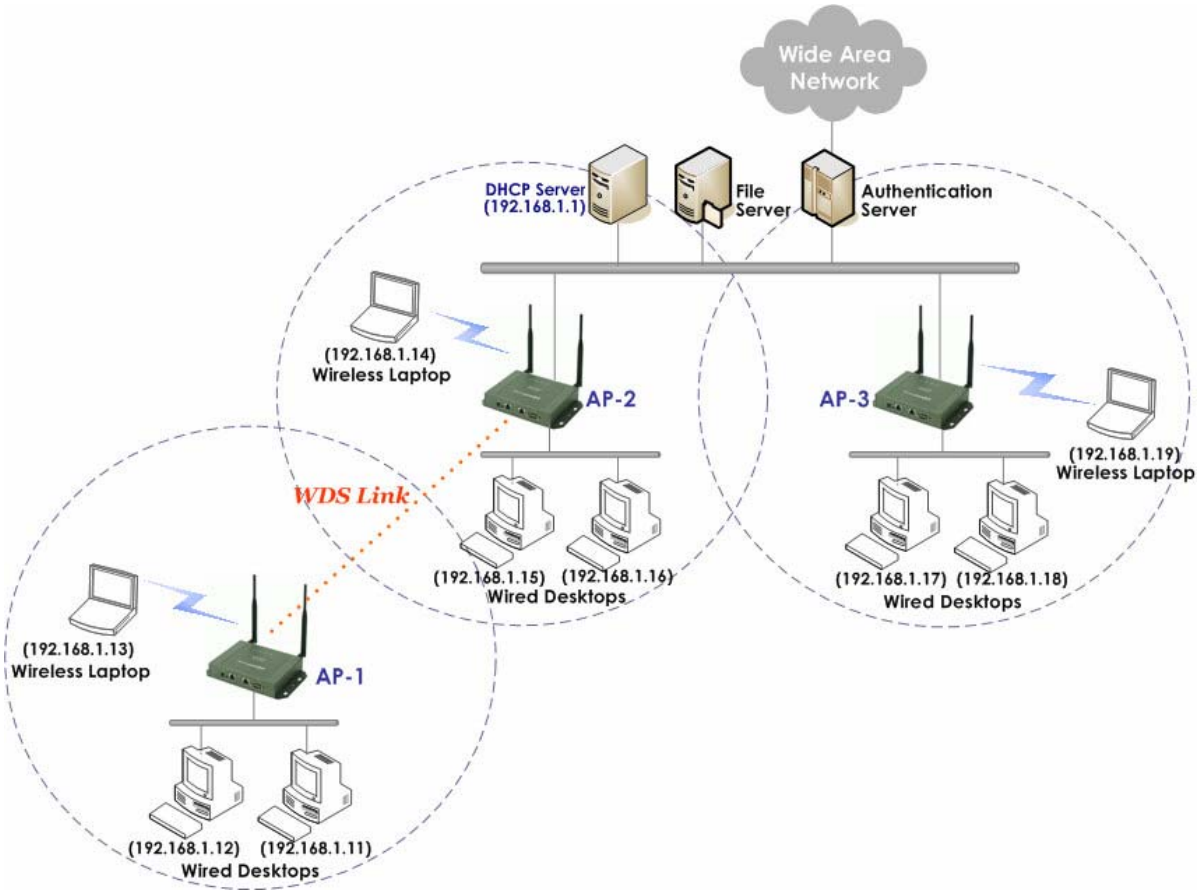
EAP100 is a high-end Access Point (AP) with the best price/ performance for business and industrial applications and is compliant with the latest industrial wireless security standards that are required in the tightly secured enterprise network environments. Its Wireless Distribution System (WDS) feature allows for flexible extension of wireless coverage. The dual-PoE LAN ports, LAN1 and LAN2, can receive Power over Ethernet (PoE) and is capable of providing backups between each other with its failover function. This provides EAP100 with reliable connectivity. Its metal case is IP50 anti-dust compliant, which means that EAP100 is well suited to WLAN deployment in industrial environments.

EAP100 can function in two modes: Access Point (AP) mode and Wireless Distribution System (WDS) mode. In the AP mode, EAP100 supports up to eight Virtual Access Points (VAPs) and each VAP can define its own rule settings, which makes flexible security policy possible by taking advantage of such VAP capability and simultaneously enables different levels of service to meet actual requirements. In the WDS mode, EAP100 supports point-to-point or point-to-multipoint topology to widely extend its wireless coverage.

1.2 Product Features

- High Speed IEEE 802.11g and Backward Compatible with 802.11b
- WDS for Extending Wireless Coverage
- Supporting QoS & 802.11e WMM
- Multiple Virtual APs & Capability of Client Isolation
- Business-class WLAN Security & Client Authentications
- Multiple Administration Interfaces for Network Management
- Dual-PoE with Link Failover
- Antenna Diversity & Field Replaceable Antenna
- IP50 Compliant

1.3 Deployment Topology Diagram



This above deployment scenario illustrates a deployment example using three access points, AP-1, AP-2 and AP-3.

- Three EAP100 systems construct a network comprising wired and wireless segments.
- The AP-2 plays the role as a wireless bridge.
- All devices share the same DHCP server 192.168.1.1.

1.4 Document Conventions

	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 on each and every configuration page will allow the changes you made on the current page to take effect immediately. ▶ Sometimes the system may require a restart after clicking ***Apply***. When a restart message appears, the system must be restarted for the settings 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 EAP100 includes:

- EAP100 x 1
- Quick Installation Guide x 1
- CD-ROM x 1
- Console Cable x 1
- Ethernet Cable x 1
- Power Adapter (DC 12V) x 1
- 5dBi Antenna x 2
- Mounting Kit x 1
- Ground Cable x 1

It is recommended to keep the original packing material for possible future shipment when repair or maintenance is required. Any returned product should be packed in its original packaging to prevent damage during delivery.

2.2 Specification

Standard Conformance

- Wireless:
  (1) IEEE 802.11g (up to 54Mbps)
  (2) IEEE 802.11b (up to 11Mbps)
- Ethernet:
  (1) 802.3
  (2) 802.3u

Wireless Radio

- Frequency band: 2.4 GHz
- Wireless architecture:
  (1) AP mode
  (2) WDS mode (Repeater / Bridge)
- Modulation:
  (1) 802.11b: DSSS (CCK, DBPK, DQPSK)
  (2) 802.11g: OFDM (64-QAM, 16-QAM, QPSK, BPSK)
- Channels:
  (1) USA (Channel 1~11)
  (2) Japan (Channel 1~14)
  (3) Europe (Channel 1~13)
- Transmit Power:
  (1) 802.11g: 16dBm
  (2) 802.11b: 20dBm
- Receiver Sensitivity: -68dBm@54Mbps, -87dBm@11Mbps

Wireless Signal Management

- Number of ESSIDs (Virtual APs): 8
- Number of associated clients per AP: 32
- Setting for maximum number of associated clients
- Network policy based on ESSID

QoS & WMM

- DiffServ / TOS
- IEEE 802.1p/ COS
- IEEE 802.1Q Tag VLAN priority control
- IEEE 802.11e WMM

Handover & Roaming

- IEEE 802.11f IAPP
- IEEE 802.11i pre-auth (PMKSA cache)

- L2 Roaming

System Management

- Web-based administration
- SNMP v1/v2c
- Provides Event Log
- Syslog information support
- Statistics
- Configuration backup and restore
- One-button-click to restore factory default setting
- Firmware upgrade
- Capable of performing RADIUS Accounting and Accounting Update

Security

- WEP (64/128/152 bits)
- EAP-TLS + Dynamic WEP
- EAP-TTLS + Dynamic WEP
- PEAP / MS-PEAP + Dynamic WEP
- WPA (PSK + TKIP)
- WPA (802.1X certification + TKIP)
- 802.11i WPA2 (PSK + CCMP / AES)
- 802.11i WPA2 (802.1X certification + CCMP / AES)
- Setting for TKIP / CCMP / AES key's refreshing period
- Hidden ESSID support
- MAC Address filtering (MAC ACL)
- MAC authentication with RADIUS servers
- Maximum number of registered RADIUS servers: 2

Built-in Servers & Client Interfaces to Other Services

- DHCP client
- DNS client
- Syslog client
- RADIUS client
- SNMP v1/v2c read & write client

Hardware Specifications

- Wireless chipset: Atheros 2317
- Flash Memory: 4 MB
- SDRAM Memory: 16 MB

Physical and Power

- AC Input: 110~220 VAC, 50/60 Hz
- DC Output: 12V, 1.5A
- Form factor: Wall Mountable
- Dimensions (W x D x H): 8.0" x 5.3" x 1.4" (204 mm x 134 mm x 35 mm)

- Weight: 1.3 lbs (0.61 kg)

Connectors and Display

- LAN Port: 2 × 10/100 Base-T Ethernet with IEEE 802.3af PoE
- Console Port: 1 x DB9
- LED Indicators: 1 × Power, 2 × LAN, 1 × WLAN

Environment

- Operation Temperature: 0 ~ 40 ℃
- Storage Temperature: -20 ~ 60 ℃
- Operation Humidity: 10% ~ 80% Non-condensing
- Storage Humidity: 5% ~ 90% Non-condensing

Certifications

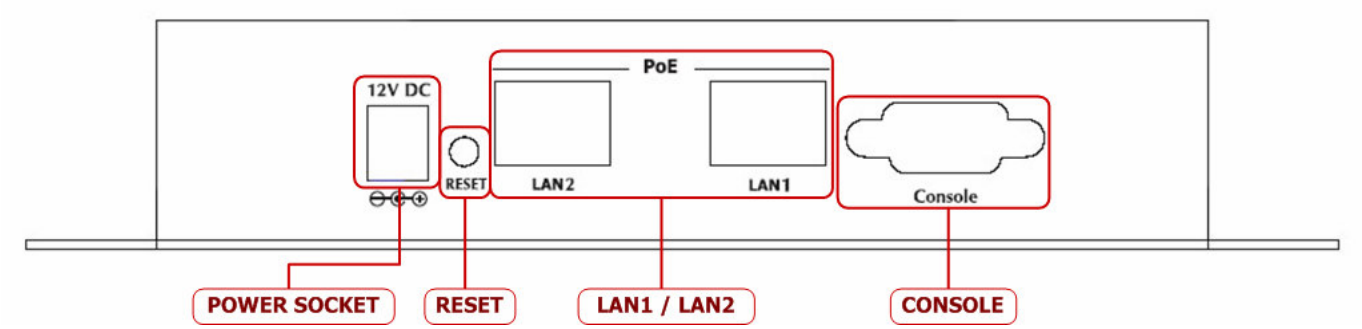
- FCC, CE
- RoHS compliant
- Metal case compliant with IP50 Standard

3. Installation

3.1 Panel Function Description

On the top panel of EAP100, there are four LEDs that are used to indicate the **POWER** status, the **WLAN** status, and the link status of the two **PoE** Fast Ethernet LAN ports. On the front panel, there are: one **POWER** socket, one **RESET** button, two **PoE** LAN ports and one **CONSOLE** port. The antennas are installed on the rear panel.

Front Panel



- **POWER SOCKET**
  - Attach the power adapter here.

- **RESET Button**
  - Press the button to restart the system.

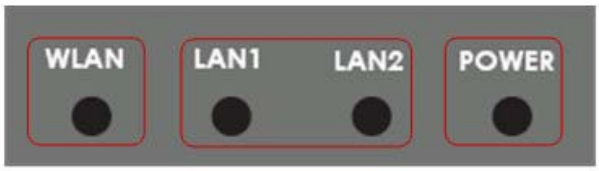
- **LAN 1 / LAN2:**
  - The LAN ports are for connection with wired networks.

- **CONSOLE**
  - Attach the serial cable here. The administrator may also obtain IP address information of Ethernet ports from the console port.

Rear Panel

- **Antenna Connector:**
  - Attach the antennas here. EAP100 supports 1 RF interface and 2 SMA connectors for antenna connection.

Top Panel



LED status indication:

- **Power**
  - Green LED On indicates power on; OFF indicates power off.
- **LAN1/LAN2**
  - OFF indicates no connection; ON indicates connection; BLINKING indicates transmitting data.
- **WLAN**
  - Green LED ON indicates system ready.

3.2 Hardware Installation

Please follow the steps mentioned below to install the hardware of EAP100:

1. **Place the EAP100 at a best location.**
   The best location for EAP100 is usually at the center of your wireless network.

2. **Connect EAP100 to your network device.**
   Connect one end of the Ethernet cable to the LAN1 or LAN2 port of EAP100 and the other end of the cable to a switch, a router or a hub. EAP100 is then connected to your existing wired LAN network.

3. **There are two ways to supply power over to EAP100.**
   (1) Connect the DC power adapter to the EAP100 power socket.
   (2) EAP100 LAN ports are capable of transmitting DC currents via its LAN1 or LAN2 PoE ports. Connect an IEEE 802.3af-compliant PSE device, e.g. a PoE-switch, to the LAN1 or LAN2 port of EAP100 with the Ethernet cable.

Now, the Hardware Installation is completed.

- *Please only use the power adapter supplied with the EAP100 package. Using a different power adapter may damage this system.*
- *To double verify the wired connection between EAP100 and your switch/router/hub, please also check the LED status indication of these network devices.*

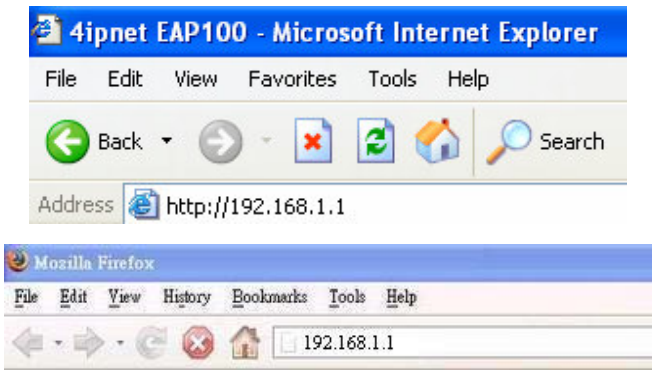
3.3 Basic Configuration

4ipnet EAP100 supports web-based configuration. Upon the completion of hardware installation, EAP100 can be configured through a PC by using its web browser such as Mozilla Firefox 2.0 or Internet Explorer version 6.0 and the above.

The default values of LAN IP address and subnet mask of EAP100 are:

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0



- To access the web management interface, connect the administrator PC to the LAN1 or LAN2 port of EAP100 via an Ethernet cable. Then, set a static IP address on the same subnet mask as EAP100 in TCP/IP of your PC, such as the following example (Please note that the IP address used shall not be duplicated with the IP address of other devices within the same network.):

  IP Address: 192.168.1.100

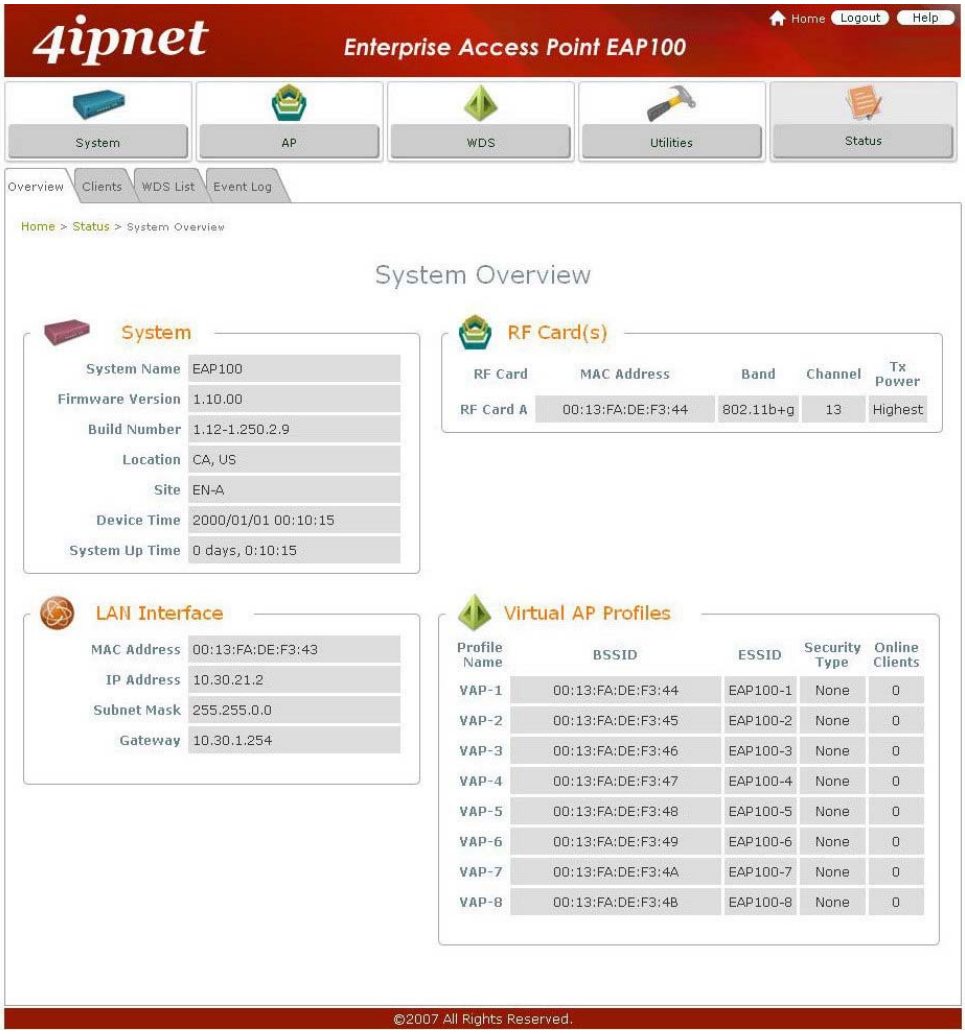
  Subnet Mask: 255.255.255.0

- Launch the web browser on your PC by entering the IP address of EAP100 (**http://192.168.1.1**) at the address field, and then press ***Enter***. The following Administrator Login Page will then appear. Enter **"admin"** for both the *User name* and *Password* fields, and then click ***OK*** to log in.

  User name: **"admin"**

  Password: **"admin"**

- After a successful login into EAP100, a **System Overview** page of web management interface will appear. To logout, simply click on the ***Logout*** button at the upper right hand corner of the interface to return to the Administrator Login Page.



- To logout, simply click on the ***Logout*** button at the upper right hand corner of the interface to return to the Administrator Login Page.

For security concern, it is strongly recommended to change the administrator's password upon the completion of all configuration settings.

Please follow the following steps to complete the basic configuration:

Step 1. Change Administrator's Password:

- Click on the **Utilities** button, and then select the **Admin Password** tab.
- Enter a new password with length up to 32 characters, and then click **Apply** to activate the new password.

Note:

On each and every configuration page, you may

(a) click ***Apply*** to allow the changes you made on the current page to take effect immediately (Sometimes the system may require a restart after clicking ***Apply***. When a restart message appears, the system must be restarted for the settings to take effect.); or

(b) click ***Save*** to save the changes, but you must reboot the system upon the completion of all configuration settings for the changes to take effect. When clicking ***Save***, the following message will appear: **"Some modifications have been saved and will take effect after Reboot."**

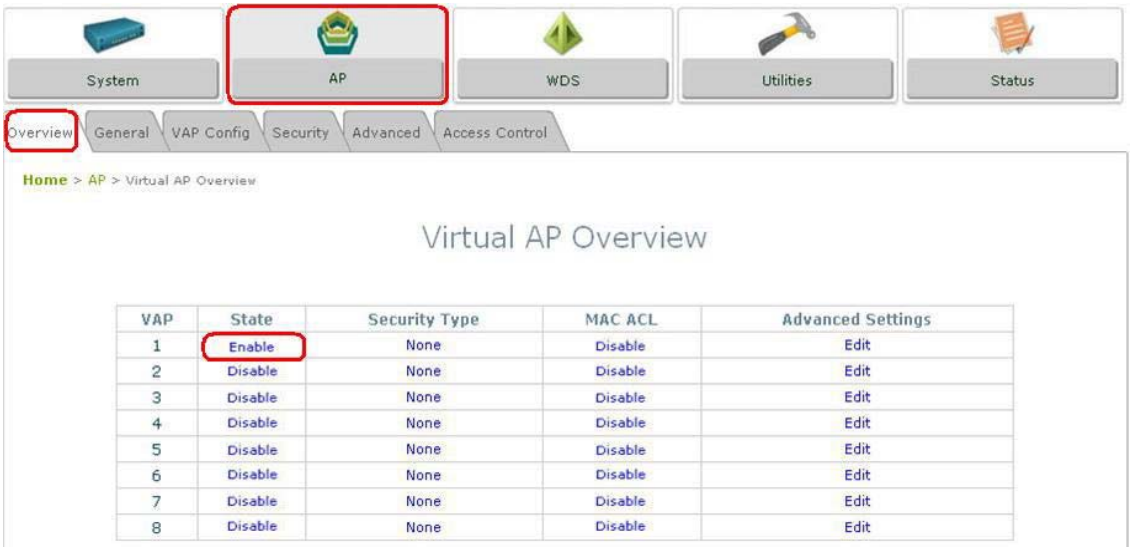
Step 2. Configure AP (Access Point) Settings

- Click on the **AP** button, and then select the **General** tab.
- Determine the *Band* and *Channel* settings:
  Select your preferred *Band* and *Channel* for your wireless connection. For example, select *802.11b+802.11g* for the band and *Auto* for the channel.

Step 3. Configure VAP (Virtual Access Point) Profile Settings

EAP100 Supports up to 8 virtual APs. By default, only 1 VAP are enabled.

- Configure VAP profile settings:
  (a) Select the **VAP Config** tab to configure the settings for each VAP.
  (b) An administrator can enable or disable specific VAP from the drop-down list box of *Profile Name*.
- Check VAP status：
  After finishing the above settings, the status of enabled Virtual APs shall be reflected on the **Virtual AP Overview** page.



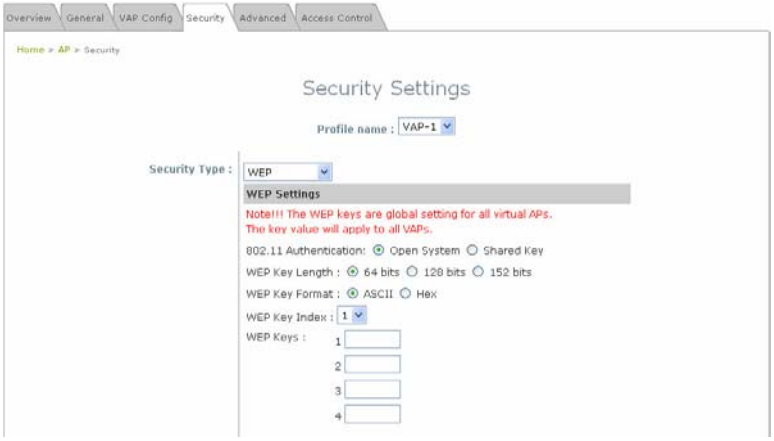
Step 4 (Advanced Optional). Choose Security Type

➤ Click on the **AP** button.

➤ Select the **Security** tab to configure your preferred security types:

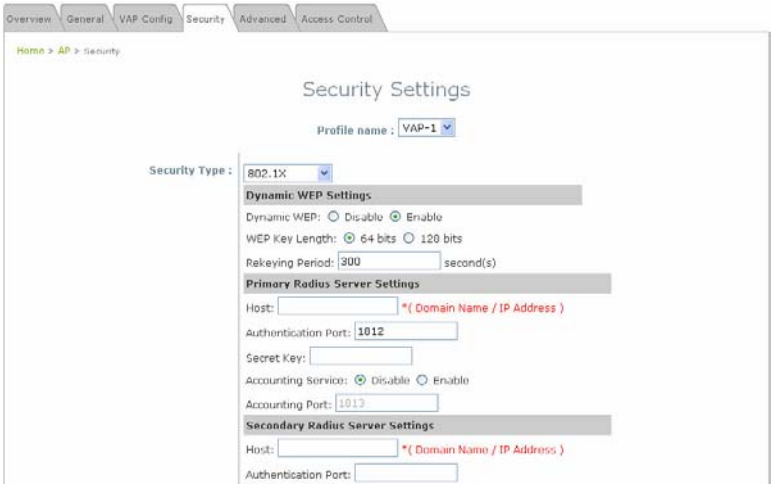
1. Choose **"WEP"** as its *Security Type* :

   While **WEP** is selected, provide the desired **Authentication**, **key length**, **format**, **index** and **values**.



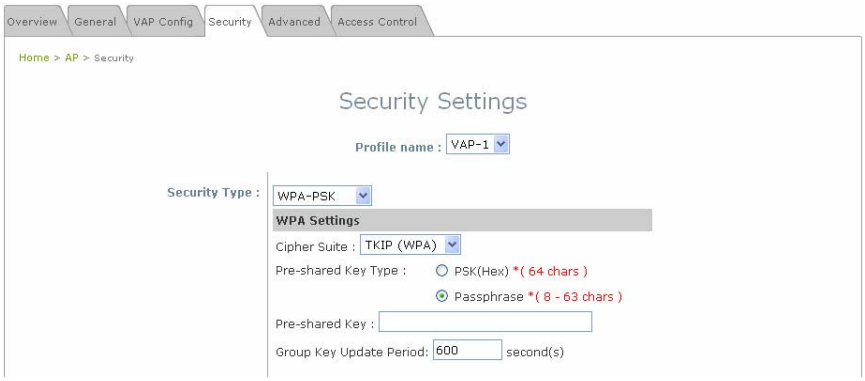
2. Choose **"802.1X"** as its *Security Type* :

   While **802.1X** authentication is selected, provide the desired **WEP key length** and the corresponding settings of RADIUS server.



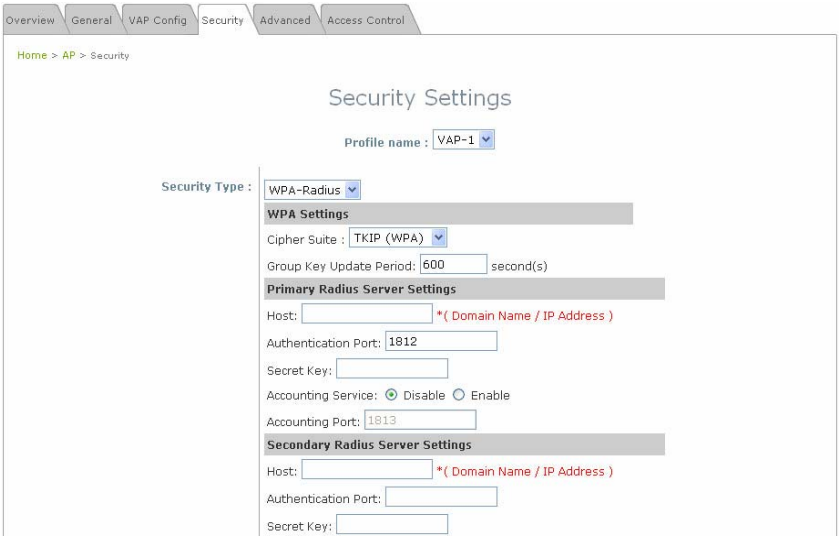
3. Choose **"WPA-PSK"** as its *Security Type* :

   While **WPA-PSK** is preferred, provide the desired **pre-shared key** and **cipher** type.



4. Choose **"WPA-Radius"** as its *Security Type*:

   While **WPA-Radius** is selected, provide the **cipher** type and the corresponding settings of RADIUS server.

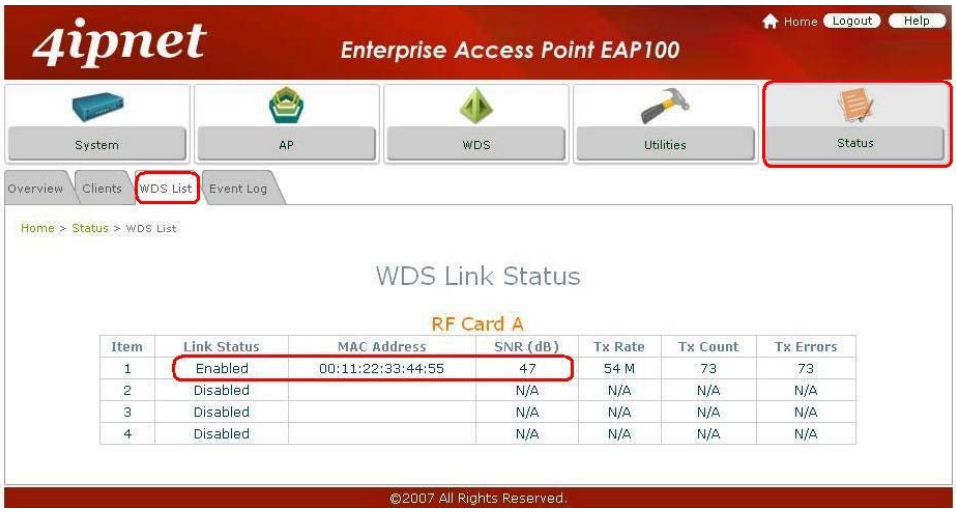


Step 5. Configure WDS (Wireless Distribution System) Settings

To extend its wireless coverage, EAP100's WDS capability is capable of creating WDS links for connecting to other WDS-capable APs (peer APs). EAP100 supports up to 4 WDS links. By default, all WDS profiles are disabled.

- Click on the **WDS** button.
- Select the **WDS Configuration** tab.
- Select WDS link parameters:
  (a) Choose one WDS Profile
  (b) Enable WDS
  (c) Enter *MAC Address of Remote AP* (peer AP)
  (d) Select preferred *Security Type*
- To configure peer AP(s):
  After completing the WDS settings at this EAP100 (functioning as a "primary WDS station"), you must also configure the settings of its peer AP(s).
  If you use another EAP100 as the peer AP, simply repeat the above-mentioned steps with the MAC Address of the primary WDS station for setting WDS link parameters of the peer AP(s).

Step 5 (CONT). Check WDS Link Status



- Click on the **Status** button.
- Select the **WDS List** tab.
- Check the signal strength of WDS link(s)：
  Upon the completion of Step 4, there shall be *SNR* displayed on the **WDS Link Overview** page. If the SNR is shown as *N/A*, check if the wiring is properly connected and please ensure the accurate execution of Step 4 as described above.

Congratulation!

Now, 4ipnet EAP100 is installed and configured successfully.

- *It is strongly recommended to make a backup copy of configuration settings.*
- *After EAP100's network configuration is completed, please remember to change the IP Address of your PC Connection Properties back to its original settings in order to ensure that your PC functions properly in its real network environments.*

4. Web Interface Configuration

This chapter will guide you through further detailed settings. The following table shows all the UI functions of 4ipnet EAP100 Enterprise Access Point. In the web management interface, there are two main interface areas: **Main Menu** and **Working Area**. The **Working Area** occupies the largest area of the web management interface, displayed in the center of the interface. It is also referred as **the configuration page**. The web management interface is the page where status is displayed, control is issued and parameters are configured. The **Main Menu**, on the top of the web management interface, allows the administrator to traverse to various management functions of this system. The management functions are grouped into branches: **System**, **AP**, **WDS**, **Utilities** and **Status**.

OPTION	FUNCTION
System	System Information
	Network Settings
	Management Services
AP	Virtual AP Overview
	General Settings
	VAP Configuration
	Security Settings
	Advanced Wireless Settings
	Access Control Settings
WDS	WDS Link Overview
	WDS Link Settings
Utilities	Change Password
	Configuration Save & Restore
	System Upgrade
	Reboot
Status	System Overview
	Associated Client Status
	WDS Link Status
	Event Log

Note:

On each and every configuration page, you may

(a) click ***Apply*** to allow the changes you made on the current page to take effect immediately (Sometimes the system may require a restart after clicking ***Apply***. When a restart message appears, the system must be restarted for the settings to take effect.); or

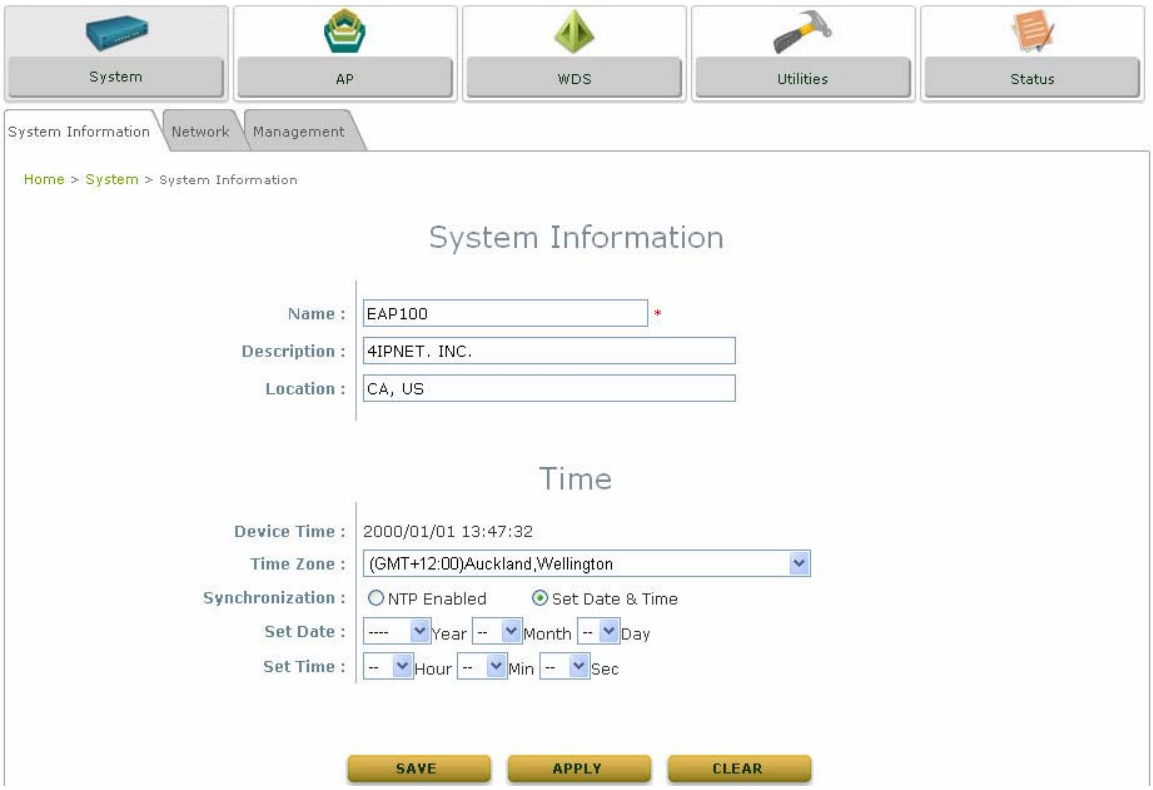
(b) click ***Save*** to save the changes, but you must reboot the system upon the completion of all configuration settings for the changes to take effect. When clicking ***Save***, the following message will appear: **"Some modifications have been saved and will take effect after Reboot."**

All on-line users will be disconnected during reboot/restart.

4.1 System Configuration

This section includes the following functions: **System Information**, **Network Settings** and **Management Services**.

4.1.1 System Information



- **System Information**

  For the purpose of maintenance, 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.

  - *Name*: The system name used to identify this system
  - *Description*: Further information about this installation
  - *Location*: The geographic location

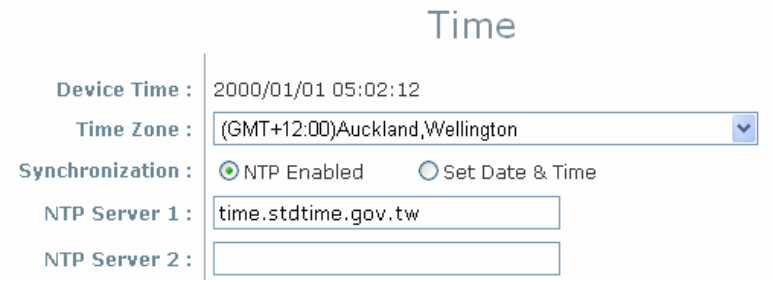
- **Time**

  Synchronize the system time either by using NTP server or by manual setup. When NTP server is used, the information of at least one NTP server 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**).

  - *Device Time*: Current system time
  - *Time Zone*: Select a time zone from the drop-down list box
  - *Synchronization*: There are two options of setting system time

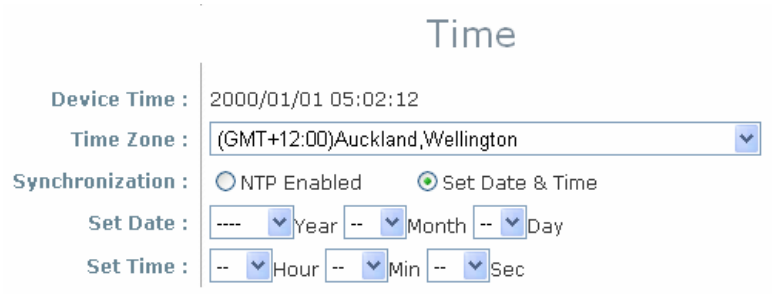
1) *NTP Enabled*:

By selecting *NTP Enabled*, EAP100 can synchronize its system time with the NTP server automatically. While this method is chosen, at least one NTP server's IP address should be provided. It is recommended to provide the IP address of both NET Server 1 and 2 in case of any NTP service failure.



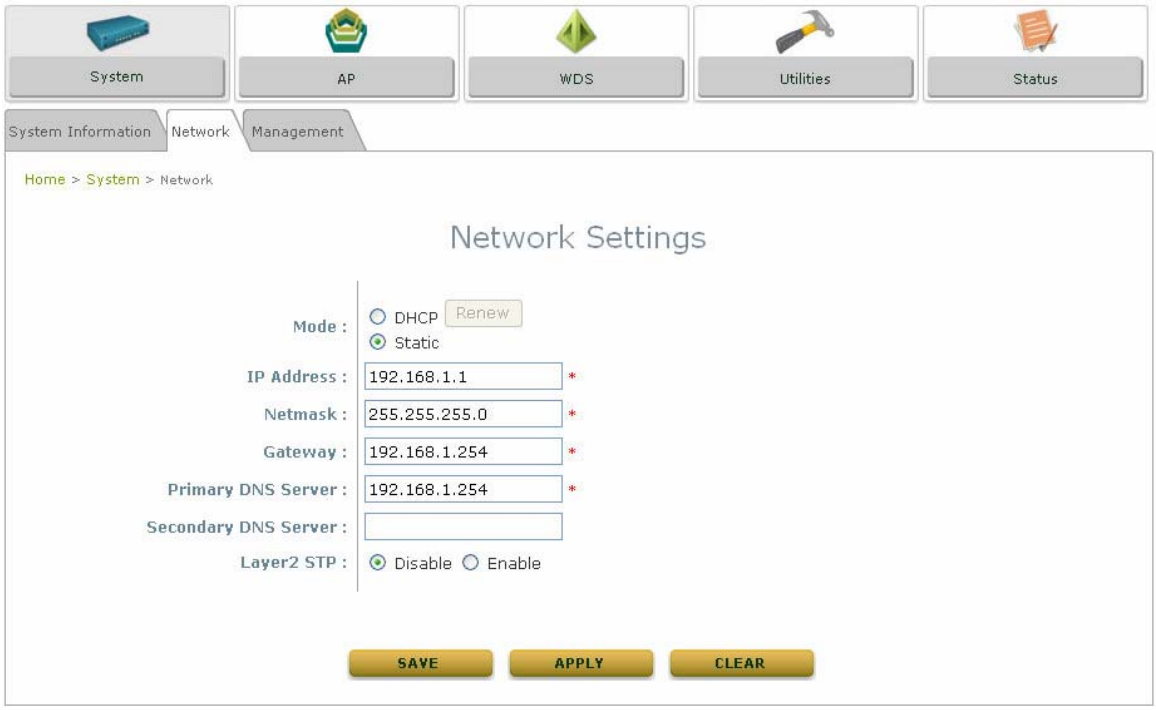
2) *Set Date & Time*:

By selecting *Set Date & Time*, the administrator can manually set the system date and time.



Unless the Internet connection is unavailable, it is recommended to use NTP server for time synchronization.

4.1.2 Network Settings

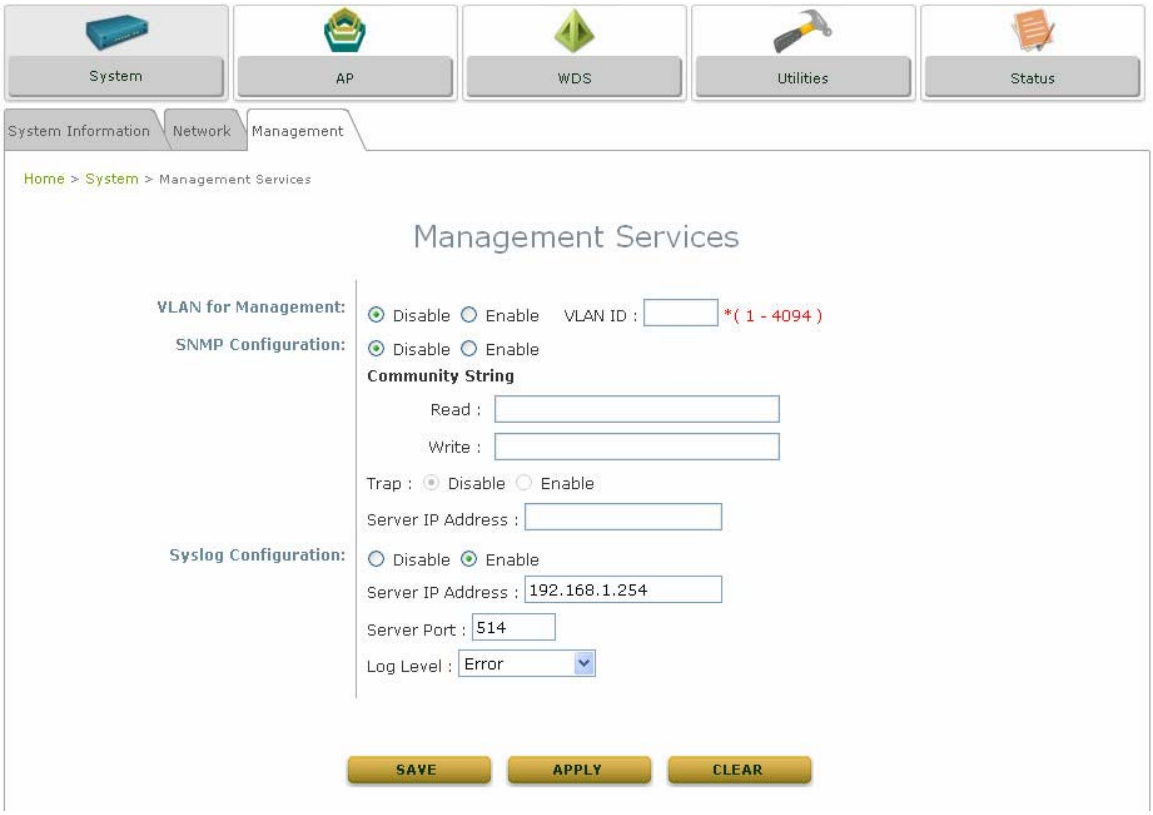


This page is for setting up the wired internet connections. There are two methods of IP configuration available at EAP100. LAN interface configuration determines the way to obtain the IP address, either by DHCP or by manual setup.

- **Mode**: Determine the way to obtain the IP address, by DHCP or Static.
  - *DHCP client*: This option can be selected when there is a DHCP server located on your wired/wireless network. Please make sure the network connection settings are correct and the network connection is active.
  - *Static setting*: When this option is selected, the administrator can set the parameters manually. Enter the *IP Address*, *Netmask* and *Gateway* provided by your ISP.
- **Primary and Secondary DNS Server**: If any host information is given in FQDN format (full qualified domain name), ensure at least one of these DNS (Domain Name Service) server IP is correct.
- **Layer 2 STP**: When the system is configured to bridge several networks (WDS mode), this STP (Spanning Tree Protocol) function must be enabled to avoid a loop condition and to obtain the best data path for network communication optimization purpose.

  Broadcasting storm may occur in a multi-switch environment where broadcast pockets are forwarded in an endless loop between switches. A broadcast storm can consume up all available CPU resources and the Internet and Ethernet bandwidth. Enabling the STP function can prevent the system from encountering such chaos.

4.1.3 Management Services



For the purpose of easy maintenance, SNMP (Simple Network Management Protocol) and remote syslog services are provided in EAP100. The system will be managed remotely in a centralized manner.

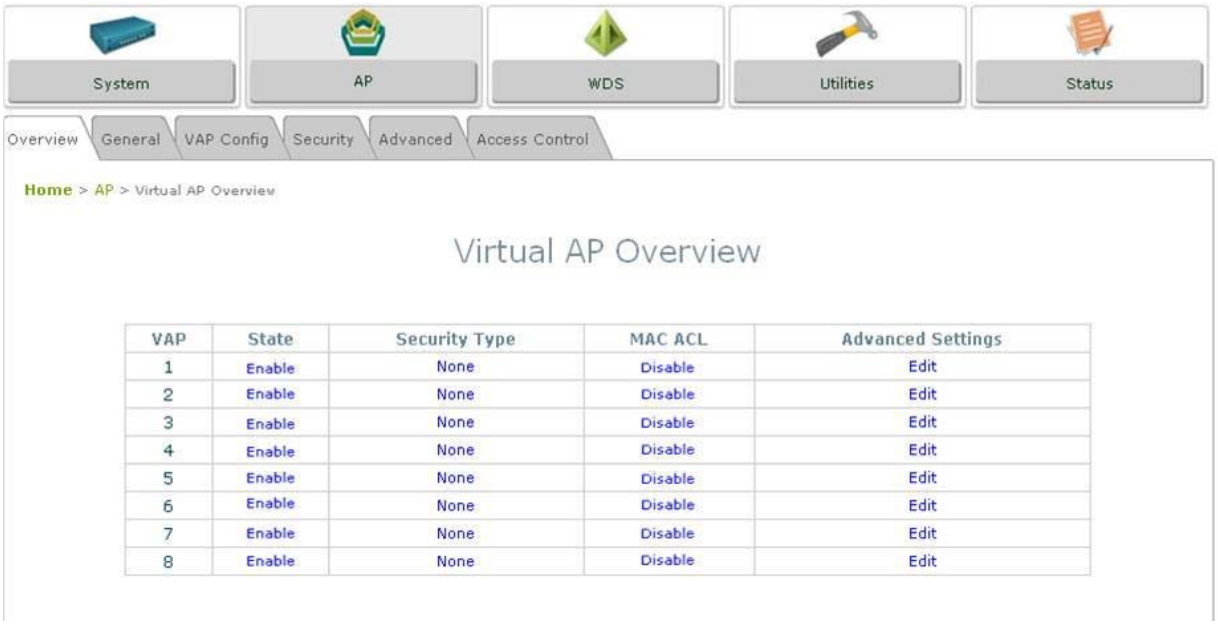
- **VLAN for Management**: The management traffic from the device can be tagged with VLAN ID. If the option is enabled, the VLAN ID can be chosen from 1 to 4094.
- **SNMP Configuration**: By enabling SNMP service, the remote SNMP manager can obtain EAP100's system status.
  - *Community String*: Specify the password for *Read* and *Write*.
  - *Trap***:** Enable or Disable the feature. When enabled, events on Cold Start, Interface UP & Down and Association & Disassociation can be reported to an assigned management station with specified *Server IP Address*.
- **Syslog Configuration**: By enabling this service, specify an external syslog server to accept syslog messages from EAP100 remotely. Thus, by reading the syslog message in the remote server, the administrator can review activities of all installed EAP100s in the network.
  - *Server Port*: The port number of the server.
  - *Log Level*: Select the desired level of received events from the drop-down list box.

4.2 AP

This section includes the following functions: **Overview**, **General**, **VAP Configuration, Security, Advanced** and **Access Control**. EAP100 supports up to four 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.

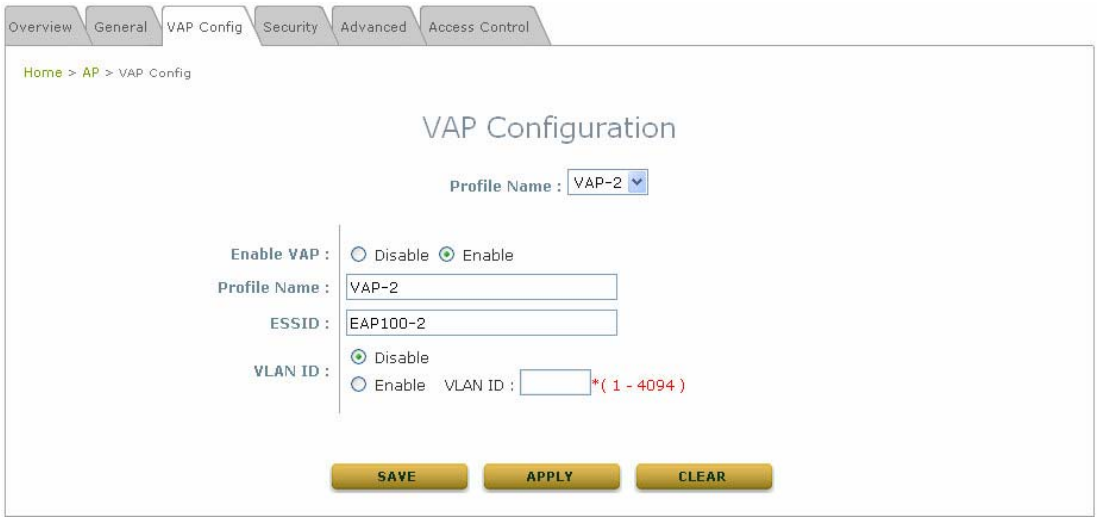
4.2.1 Virtual AP Overview

An overall status is collected in this page, including *Enable/Disable State*, *Security Type*, *MAC ACL* state, and *Advanced Settings*. EAP100 has 8 VAPs; each has its own settings. In this table, please click on the hyperlink for further configuration of each VAP respectively.

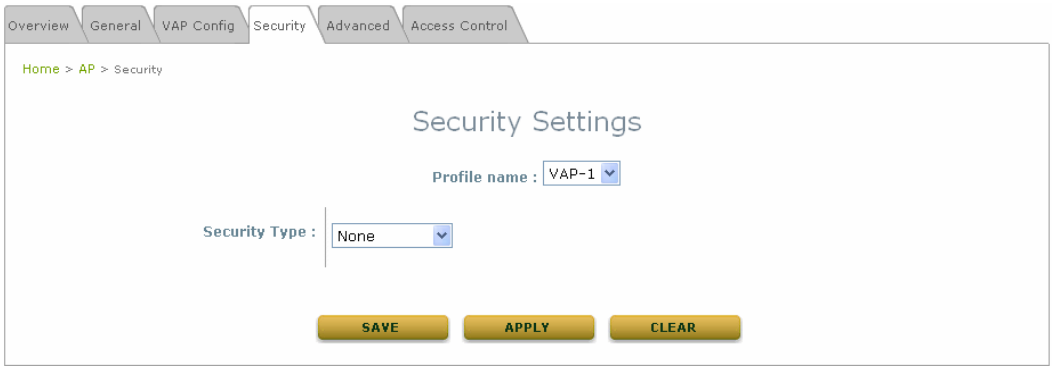


VAP	State	Security Type	MAC ACL	Advanced Settings
1	Enable	None	Disable	Edit
2	Enable	None	Disable	Edit
3	Enable	None	Disable	Edit
4	Enable	None	Disable	Edit
5	Enable	None	Disable	Edit
6	Enable	None	Disable	Edit
7	Enable	None	Disable	Edit
8	Enable	None	Disable	Edit

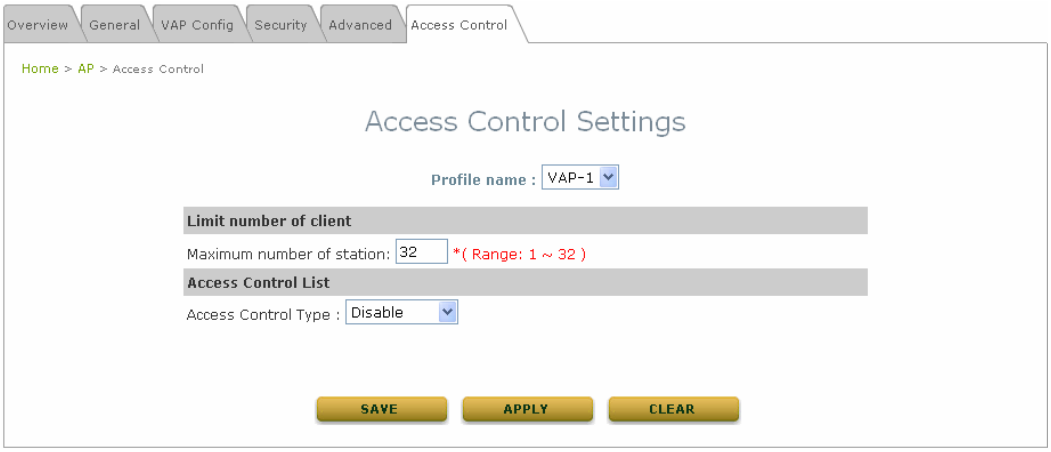
- **State:** The hyperlink showing *Enable* or *Disable* connects to the screen of **VAP Configuration**.



- **Security Type:** The hyperlink showing security type connects to the screen of Security Settings.

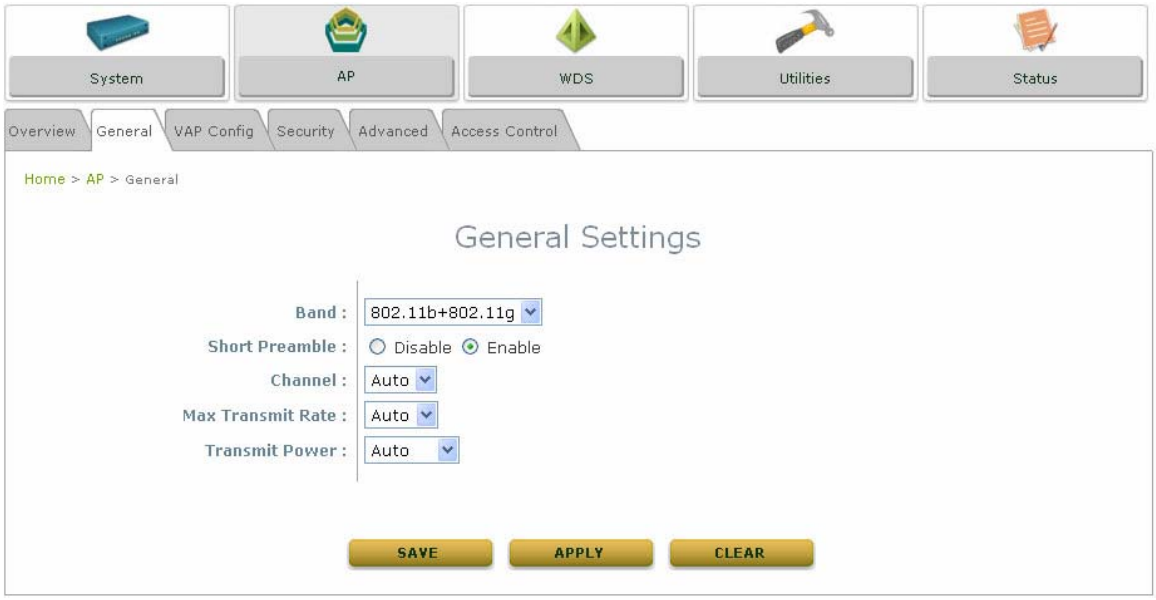


- **MAC ACL:** The hyperlink showing *Allow* or *Disable* connects to the screen of **Access Control Settings**.



- **Advanced Settings:** The hyperlink of advanced settings connects to the screen of **Advanced Wireless Settings**.

4.2.2 General Settings



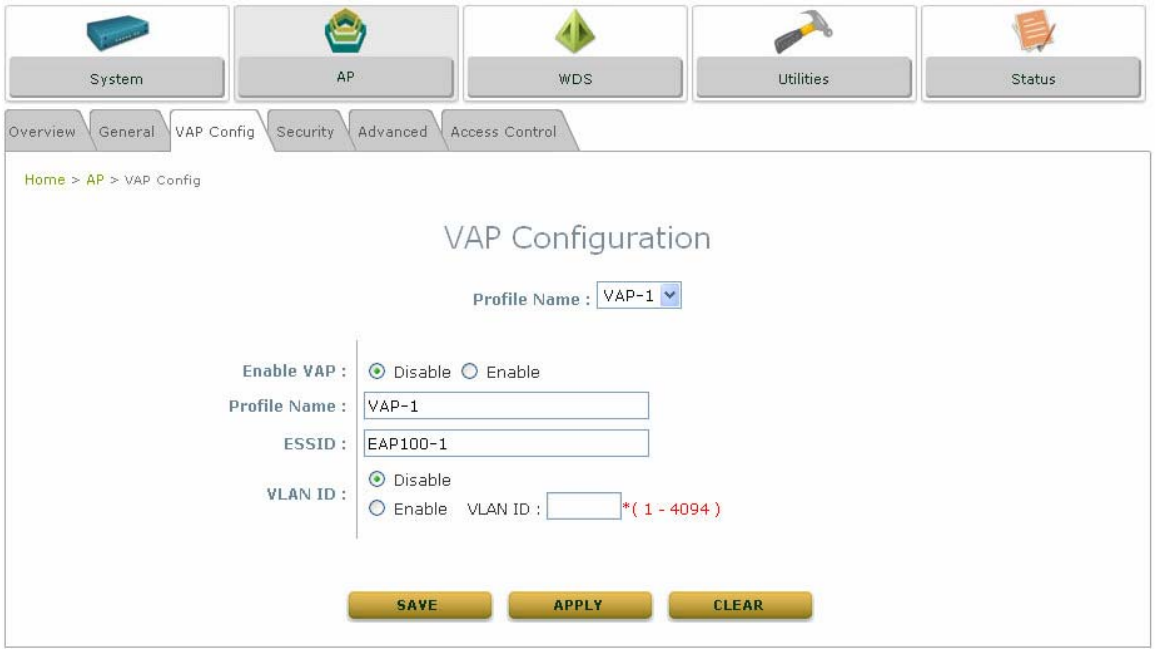
- **Band:** The operating wireless frequency band of this system. Select one frequency band from *Disable*, *802.11b*, *802.11g* or mixed mode *802.11b+802.11g*.
- **Short Preamble:** This option can be turned on to enable Short-Preamble frames.
- **Channel:** Select the appropriate channel from the 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 *Auto*, *802.11b*, *802.11g* or *802.11b+802.11g*.
- **Transmit Power:** Select from the lowest to highest power level or choose *Auto*.

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

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

Mode	Channel	Rate	Power
Disable	*NA*	*NA*	*NA*
802.11b	*1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13*	*1M, 2M, 5.5M, 11M*	*Auto, Lowest, Low, Medium, High, Highest*
802.11b+802.11g	*1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13*	*1M, 2M, 5.5M, 11M, 12M, 18M, 24M, 36M, 48M, 54M*	

4.2.3 VAP Configuration



To enable each VAP at EAP100, the administrator must configure each VAP manually. The settings of each VAP are collected as its profile.

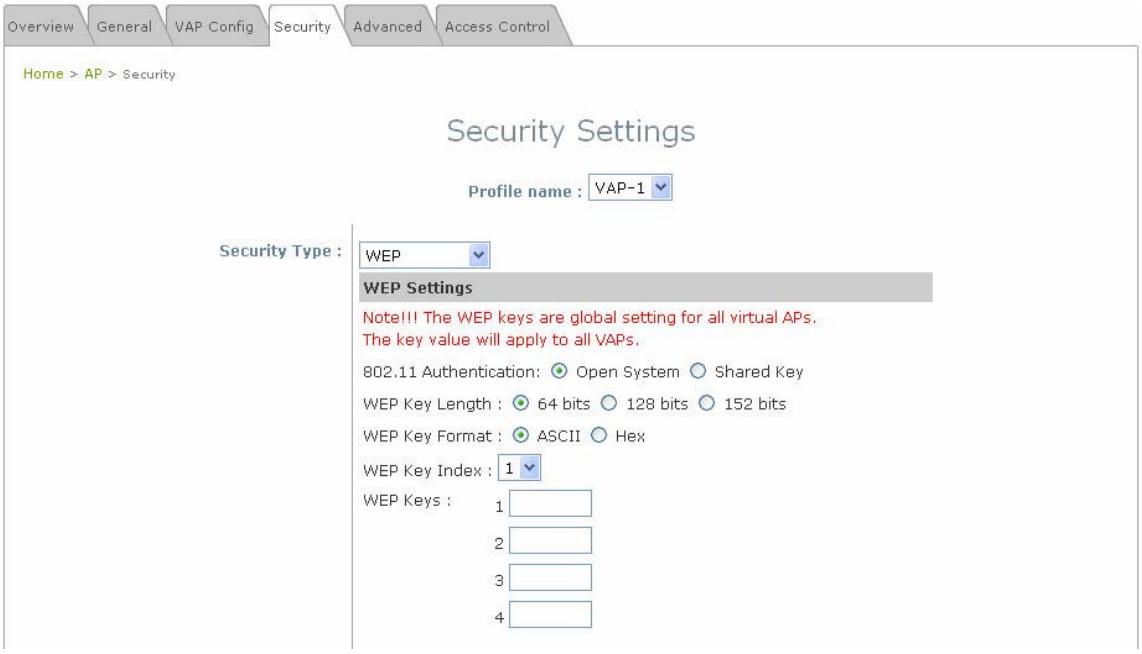
- **Enable VAP:** Enable or disable VAP function.
- **Profile Name:** The profile name of each VAP for identity/management purpose.
- **ESSID:** ESSID (Extended Service Set ID) indicates a unique SSID used by a client device to associate with a specified VAP. ESSID determines the service level assigned to a client.
- **VLAN ID:** EAP100 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

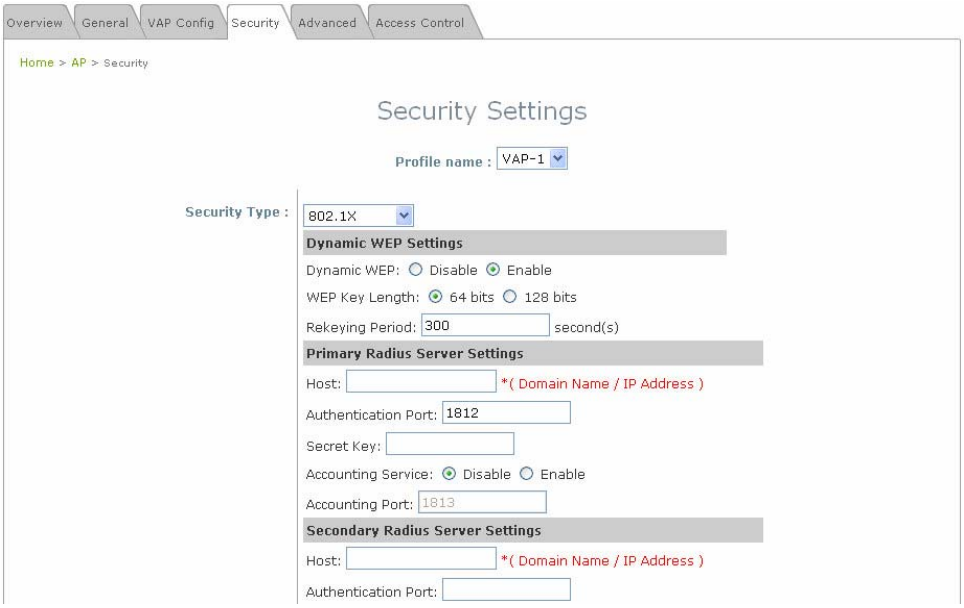
EAP100 supports various user authentication and data encryption methods in each VAP profile. Thus the administrator can depend on the need to provide different service levels to clients. The security type includes **None**, **WEP**, **802.1X**, **WPA-PSK**, **WPA-RADIUS**.

- **None:** No authentication required. This is the default setting as shown in the following figure.

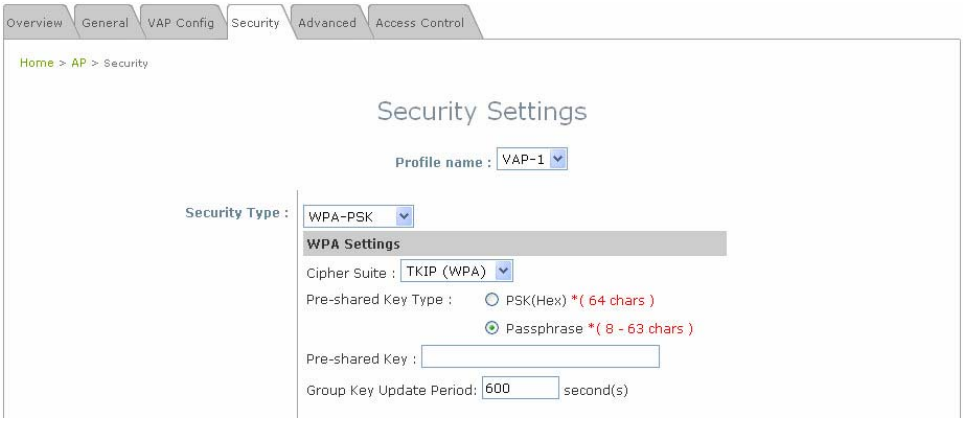
- **WEP:** Support key length of 64/128/152 bits.



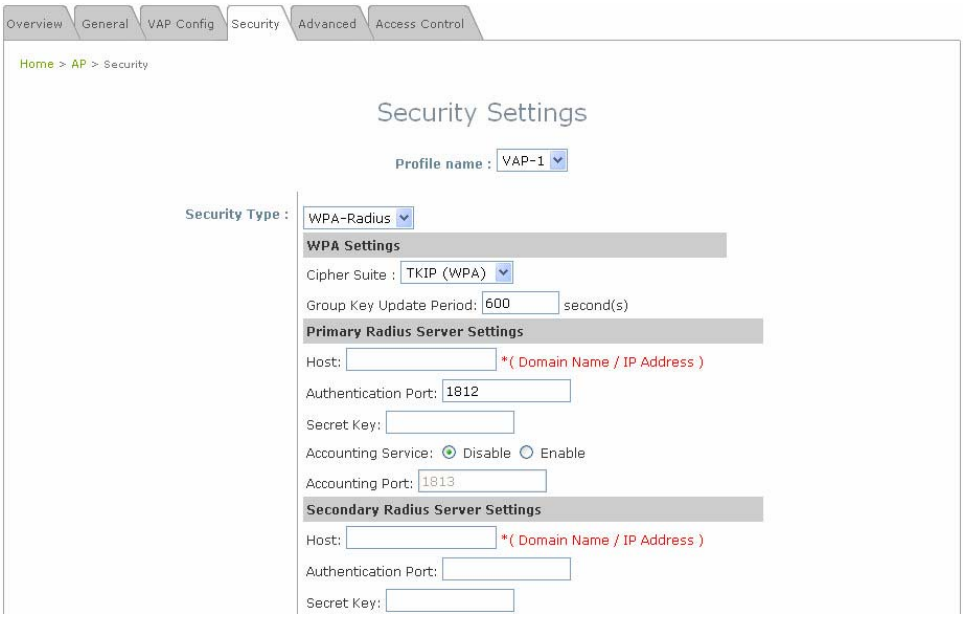
- **802.1X:** Provide RADIUS authentication and enhanced WEP.



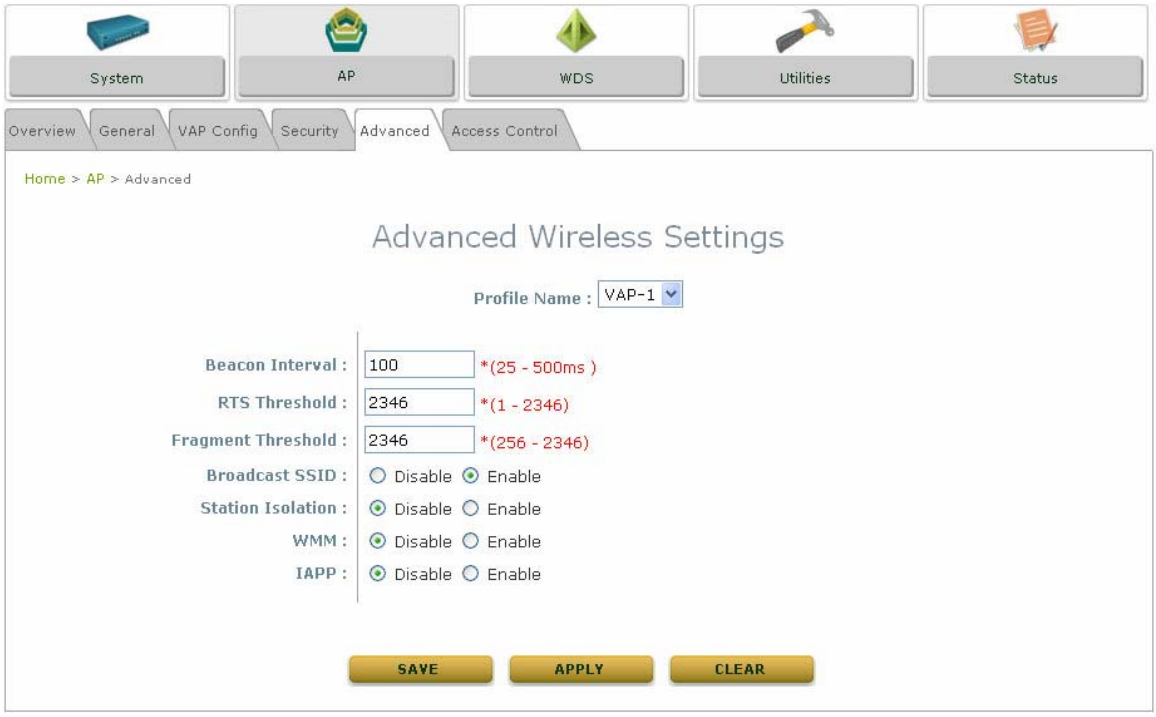
- **WPA-PSK:** Provide shared key authentication in WPA data encryption.



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



4.2.5 Advanced Wireless Settings



The advanced wireless settings for EAP100's VAP (Virtual Access Point) profiles allow customization of data transmission settings. The administrator can tune the following parameters to improve network communication performance if a poor connection occurs.

- **Beacon Interval**: Enter a value between 25 and 500 ms. The default is 100 milliseconds. The specified value represents the amount of time between access point beacon signal transmissions.
- **RTS Threshold**: Enter a value between 1 and 2346. The default is 2346. RTS (Request to Send) Threshold determines the packet size at which the access point (EAP100) issues a request to send (RTS) before sending the packet to prevent the hidden node problem. The RTS mechanism will be activated if the data size exceeds the value you set. A lower RTS Threshold setting can be useful in areas where many client devices are associating with EAP100 or in areas where the clients are far apart and can detect only EAP100 and not each other.

  Fragment Threshold: Enter a value between 256 and 2346. The default is 2346. A packet size larger than this threshold will be fragmented (sent in several pieces instead of one block) before transmission. 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**: The default is *Enable*. Disabling this function will prevent EAP100 from broadcasting its SSID, where only devices that have the correct SSID can connect.
- **Station Isolation**: The default is *Disable*. By enabling this function, all stations associated with EAP100 can only communicate with EAP100.
- **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

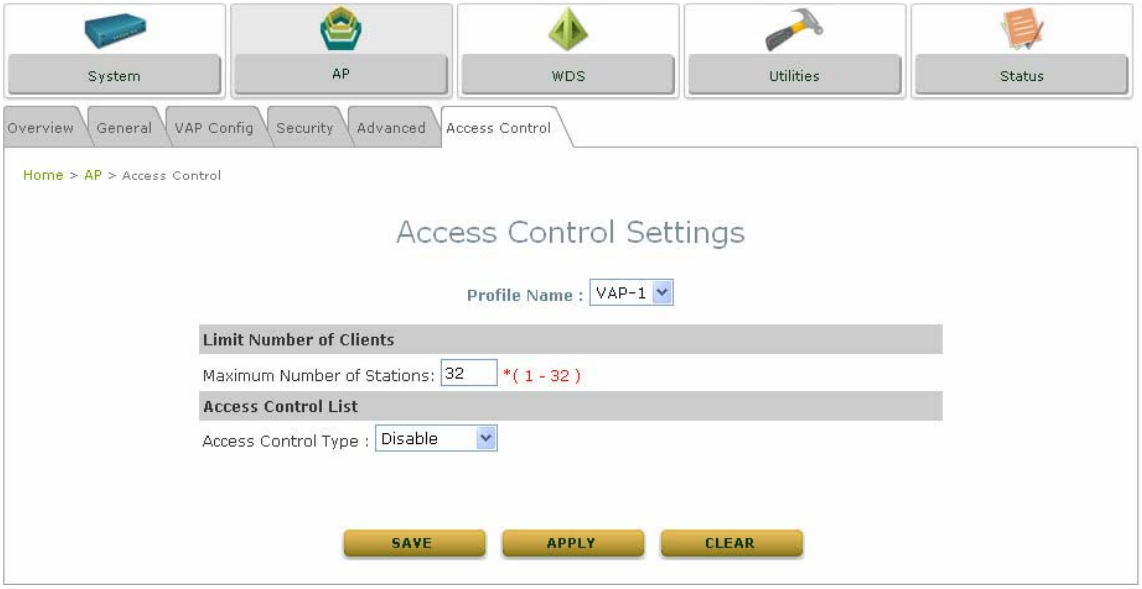
a lower priority than voice and video. In short, WMM decides which data streams are the most important and assign them a higher traffic priority.

< To receive the benefits of WMM QoS >

- The application must support WMM.
- You must enable WMM in this EAP100.
- You must enable WMM in the wireless adapter in your computer.

- **IAPP**: The default is *Disable*. 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, EAP100 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.

4.2.6 Access Control Settings



- **Maximum Number of Clients**

  EAP100 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**

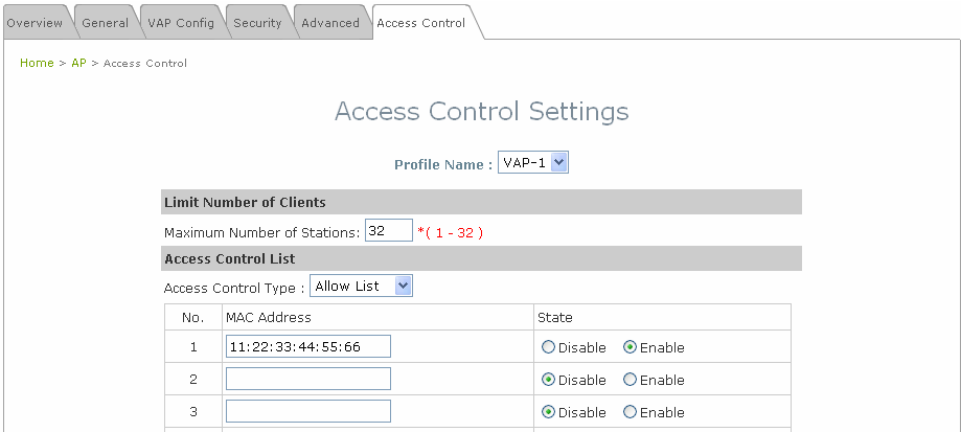
  The selected **Access Control Type** will be the activated policy while the rest will be omitted. The following is a list of the supported methods for MAC ACL control:

  (1) **Disable**

  No MAC address check required.

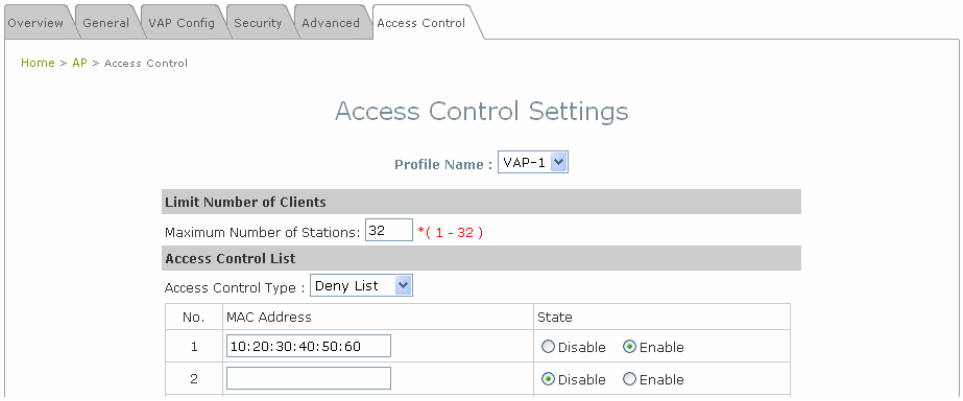
  (2) **Allow List**

  Deny all except those in the Allow List. When selecting *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.



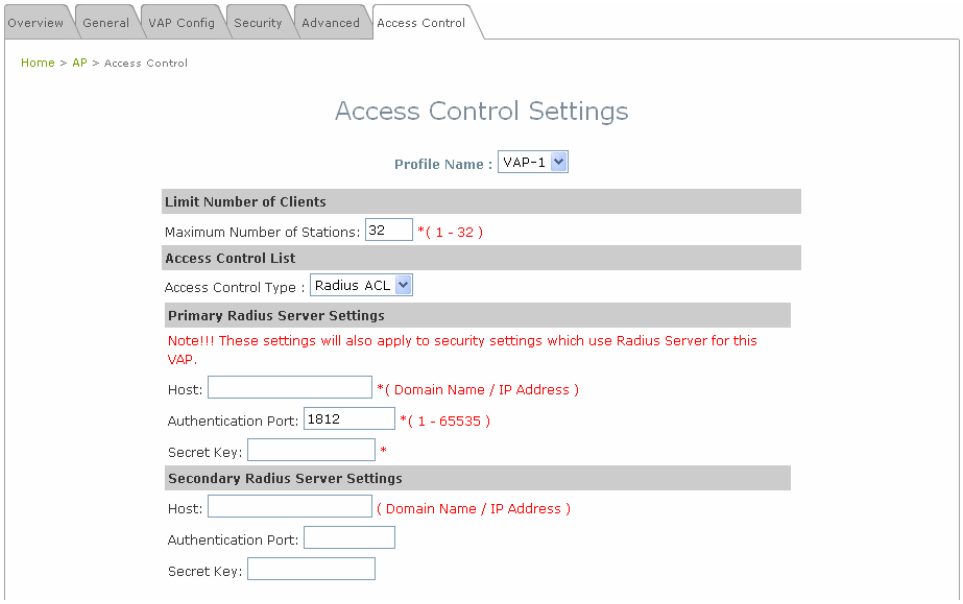
(3) **Deny List**

Allow all except those in the Deny List. When selecting *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 WDS

This section includes the following functions: **Overview** and **WDS Configuration**. The configurations under this category apply to all Virtual Access Points (VAPs) at this system.

4.3.1 WDS Link Overview

The figure provides an overall status of all WDS links.

- **Item**: Corresponding profiles of each WDS interface
- **Status**: Enable or disable a WDS link.
- **MAC Address**: Remote peer's MAC address.
- **Security**: Choose from *Disable* or *WEP* for security type.
- **Delete**: Check the profile you want to remove and click ***Delete*** to remove it.
- **Edit**: Click ***Edit*** to modify the individual setting of each WDS profile.

4.3.2 WDS Link Settings

For each WDS link profile, the remote peer's MAC address and the security type for establishing connection between EAP100 and the peer must be provided.

- **WDS Profile**: Total 8 profiles available for EAP100. Select one profile from the drop-down list box for configuration.
- **WDS Settings**: Enable or disable the specified WDS link.
- **MAC Address of Remote AP**: For each WDS link, type in the MAC address of the remote peer here.
- **Path Cost of STP**: The assigned weighted metric here will determine the best path for data flow.
- **Security:** Choose from *WEP* or *None* for security type.
  - *None*: No encryption is required to establish this WDS link.
  - *WEP*: Establish the WDS link with WEP encryption. The information on the WEP key, key length and format must be provided.

4.4 Utilities

This section includes four utilities used for customizing and maintaining the system, including **Admin Password**, **Config Save Restore**, **System Upgrade** and **Reboot**.

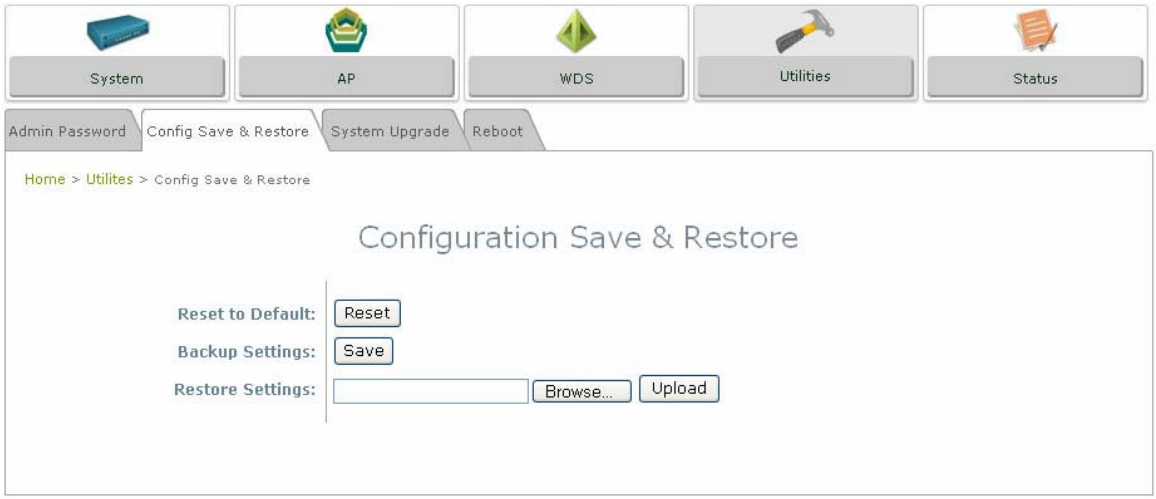
4.4.1 Change Password

To protect the management web site from unauthorized access, it is strongly recommended to change the default administrator's password to a secure password. Only alpha-numeric characters pattern is allowed, and it is strongly recommended to take a combination of both numeric and alphabetic characters.

The administrator can change the password of the system. The login account for the administrator is *admin,* and the default admin password of the system is **"admin"**. The admin password can be changed here by entering the new password. Click ***Apply*** to activate the new password.

4.4.2 Configuration Save & Restore

This function is used to backup and to restore the EAP100 settings. The EAP100 can also be restored to the factory default settings using this function. It can be used to duplicate settings to other access points (backup settings of this system and then restore on another AP).

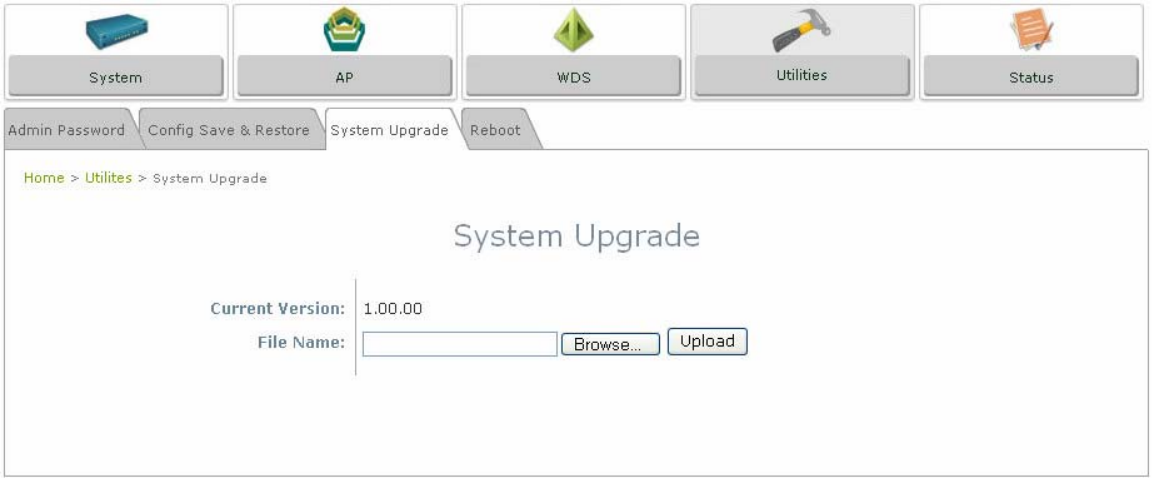


- **Reset to Default:** Click ***Reset*** to load the factory default settings of EAP100. Then, reboot the system to let the default settings take effect.
- **Backup Settings:** Click ***Save*** to save the current system configurations to a backup file on a local disk. It is recommended to make a backup before any configuration changes are made.
- **Restore Settings:** Click ***Browse*** to select a configuration file to restore, and then, press ***Upload*** to proceed. The configuration file will replace the active configuration file currently running on the system. Reboot the system to let the parameter changes take effect.

After network parameters have been reset/restored, the network settings of the administrator PC may need to be changed to ensure that the IP address of the administrator PC is on the same subnet mask as EAP100.

4.4.3 System Upgrade

EAP100 provides Web firmware upload/upgrade feature. The administrator can download the latest firmware from the website and save it on the administrator PC. To upgrade the system firmware, click ***Browse*** to choose the new firmware file you downloaded onto the temporary directory of your PC and then click ***Upload*** to execute the process. There will be a prompt confirmation message appearing to notify the administrator to restart the system after a successful firmware upgrade. Please restart the system after upgrading the firmware.



Note:

- It is recommended to check the firmware version number before proceeding further. Please make sure you have the correct firmware file.
- Firmware upgrade may sometimes result in loss of some data. Please ensure that all necessary settings are written down before upgrading the firmware.
- During firmware upgrade, please do not turn off the power. This may permanent damage this system.

For further information of available firmware version, please contact your local dealers.

4.4.4 Reboot

This function allows the administrator to restart the EAP100 safely. The process shall take about three minutes. Click ***Reboot*** to restart the system. Please wait for the blinking timer to complete its countdown before accessing the system web management interface again.

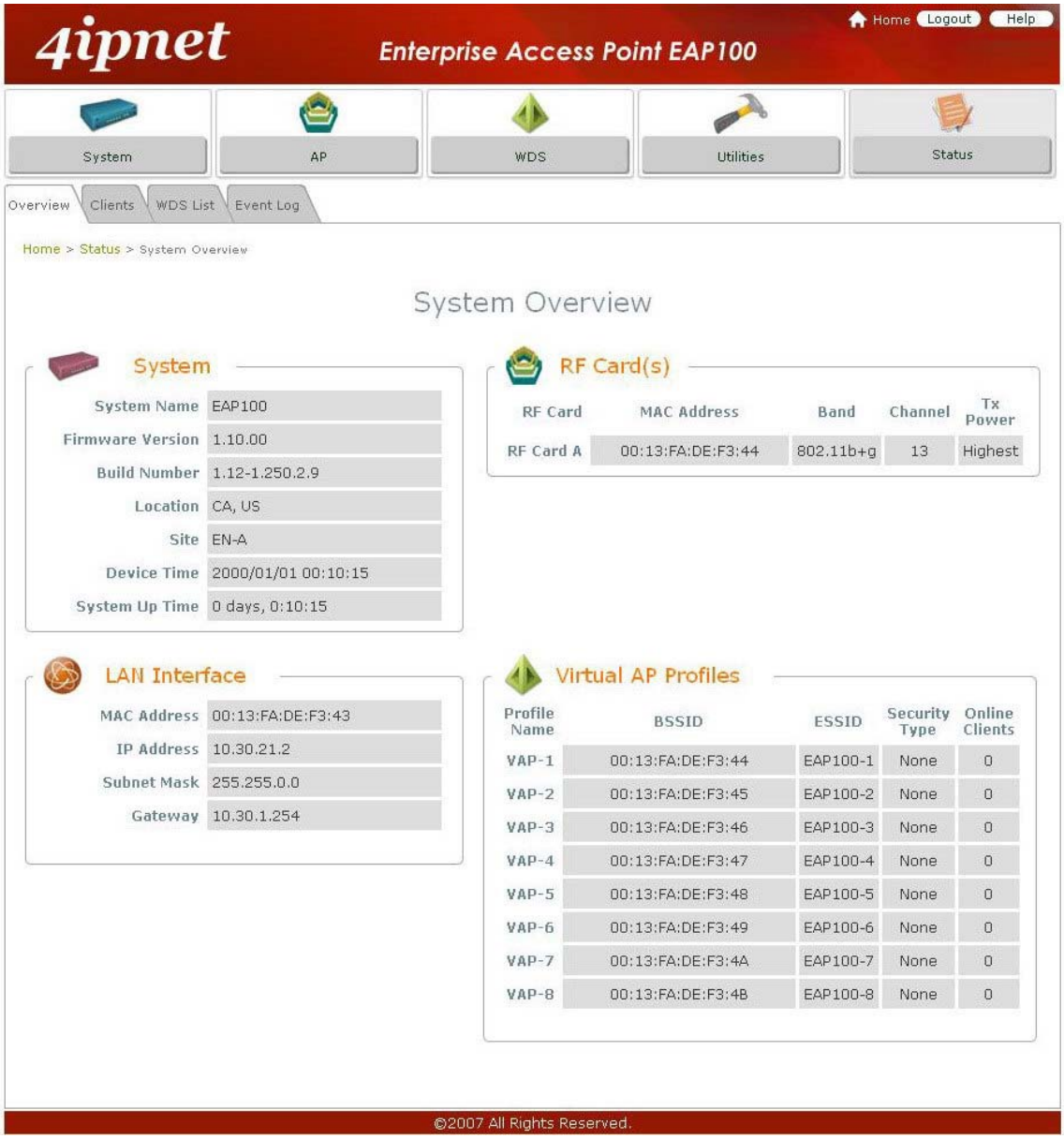
Occasionally, it is necessary to reboot EAP100 to ensure parameter changes being submitted.

4.5 Status

This section includes the following functions: **Overview**, **Clients**, **WDS List** and **Event Log**.

4.5.1 System Overview

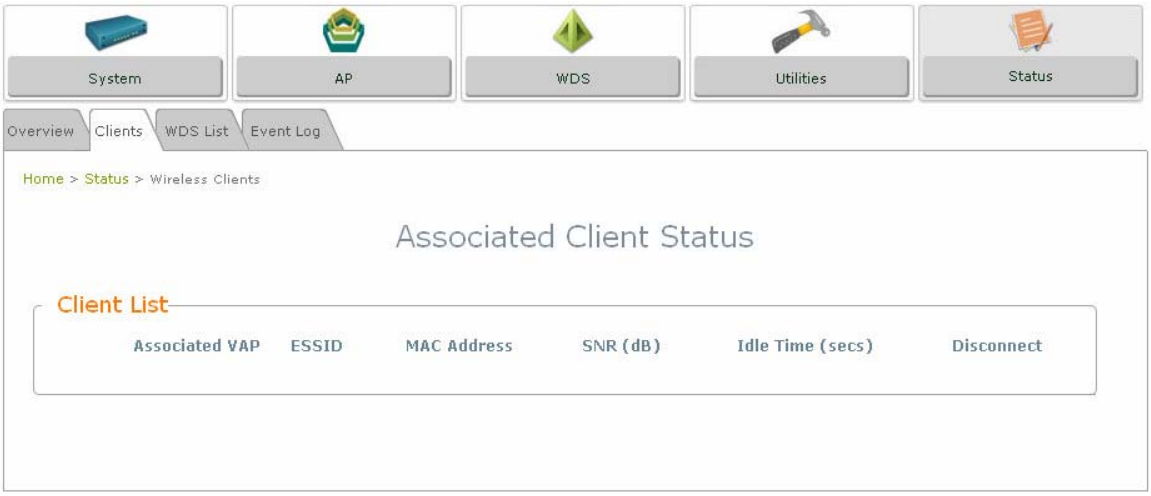
The **System Overview** page provides an overview of the system status for the administrator.



The description of the table is as the following:

ITEM		DESCRIPTION
System	System Name	The system name of EAP100.
	Firmware Version	The present firmware version of EAP100.
	Device Time	The system time of EAP100.
	System Up Time	The time that the system has been in operation
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
RF Card	MAC Address	The MAC address of RF Card
	Band	The RF band (b or g) used
	Channel	The channel specified
	Tx Power	Transmit Power level of RF card
Virtual AP Profiles	BSSID	Basic Service Set ID
	ESSID	Extended Service Set ID
	Security Type	Security type of the Virtual AP
	Online Clients	The number of online clients

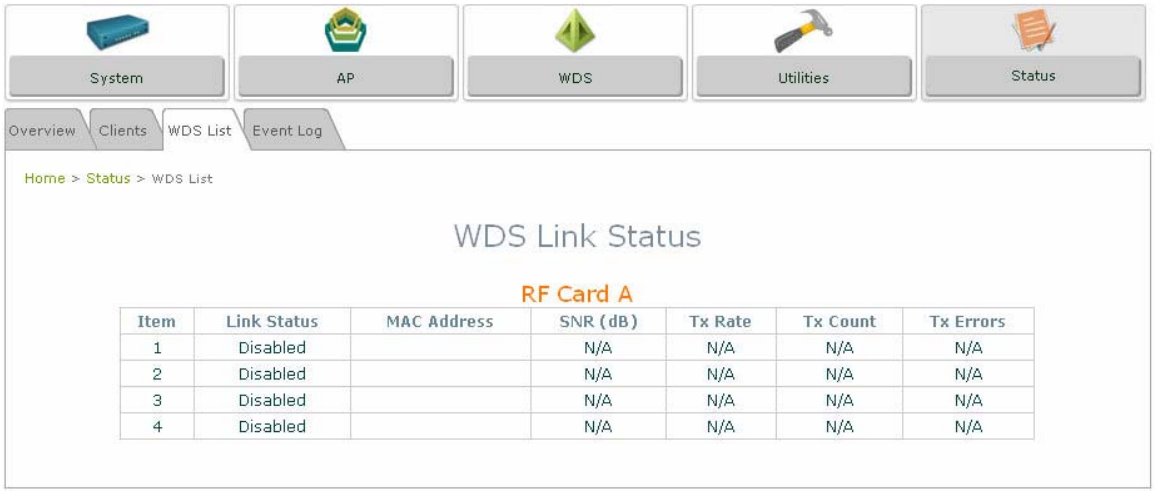
4.5.2 Associated Client Status



This page lists all associated clients of all VAPs to allow administrator to remotely oversee the status of the clients. When a low SNR is found here, the administrator can tune the corresponding parameters or investigate the settings of network devices to improve network communication performance.

- **Associated VAP:** The name of an associated VAP (Virtual Access Point)
- **ESSID:** Extended Service Set ID
- **MAC Address:** The MAC Address of associated clients
- **SNR:** Signal to Noise Ratio
- **Idle Time:** Time of no activity of associated clients in seconds
- **Disconnect:** When clicking ***Kick***, the clients will disconnect with the system.

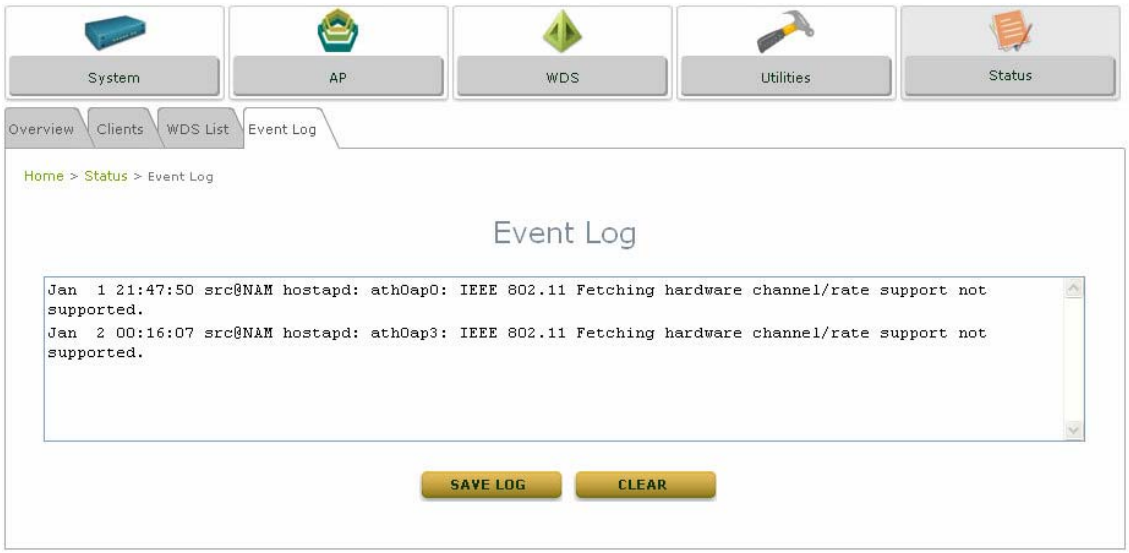
4.5.3 WDS List Status



The list shows the WDS link status with information such as *Link Status*, *MAC Address*, *SNR(dB)*, *Tx Rate*, *Tx Count*, and *Tx Errors*.

- **Link Status:** Show the WDS link status such as *Disconnected*, *Disabled* or *Connected.*
- **MAC Address:** The MAC Address of the WDS peer
- **SNR:** Single to Noise Ratio
- **Tx Rate:** The transmit rate
- **Tx Count:** The number of Transmit Count
- **Tx Errors:** The number of Transmit Errors

4.5.4 Event Log



The Event Log provides the system activities records. The administrator can monitor the system status by checking this log.

In the log, normally, each line represents an event record; in each line, there are 4 fields:

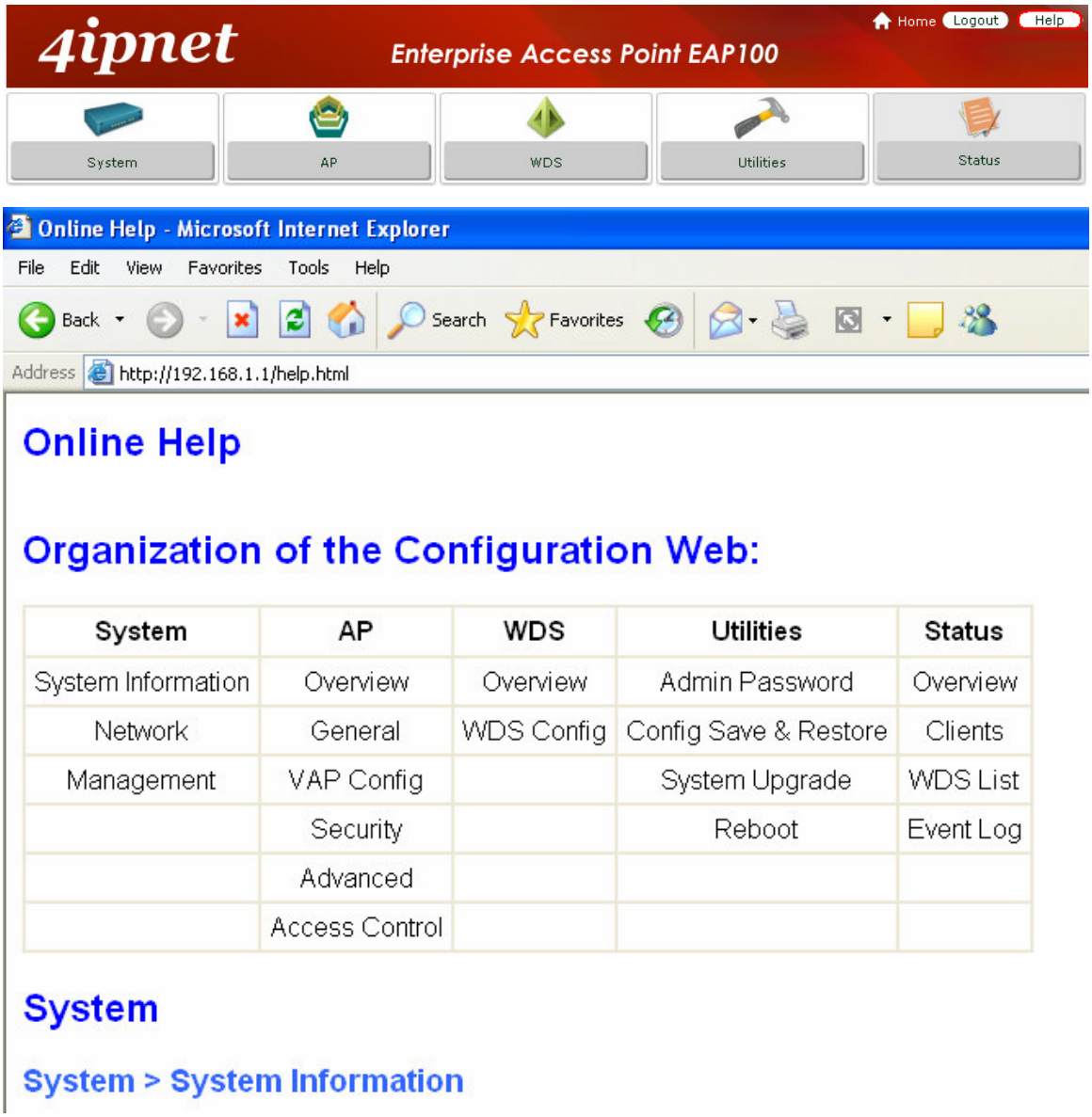
- **Date/Time:** The time & date when the event happened
- **Hostname:** Indicate which host records this event. Note that all events in this page are local event, so the hostname in this field are all the same. However, in remote syslog service, this field will help the administrator identify which event is from this EAP100. Please refer to section *4.1.3 Management Services*.
- **Process name:** Indicate the event generated by the running instance.
- **Description:** Description of this event.

To save the file locally, click ***SAVE LOG***; to clear all the records, click ***CLEAR***.

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 relevant information required.



P/N: V10020080124

Federal Communication Commission Interference Statement

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.

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.

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.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

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

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.