



# User's Manual

EAP260 V1.20

Enterprise Access Point

## **Copyright & Disclaimer**

### **Copyright**

The contents of this publication may not be reproduced in any part or as a whole, stored, transcribed in an information retrieval system, translated into any language, or transmitted in any form or by any means, mechanical, magnetic, electronic, optical, photocopying, manual, or otherwise, without the prior written permission of 4IPNET, INC.

### **Disclaimer**

4IPNET, INC. does not assume any liability arising out the application or use of any products, or software described herein. Neither does it convey any license under its parent rights not the parent rights of others. 4IPNET further reserves the right to make changes in any products described herein without notice. The publication is subject to change without notice.

### **Trademarks**

4IPNET (4ipnet) is a registered trademark of 4IPNET, INC. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

# Table of Contents

1. Before You Start .....	6
1.1 Preface .....	6
1.2 Document Conventions .....	6
1.3 Package Content .....	7
2. System Overview and Getting Started .....	8
2.1 Introduction of 4ipnet EAP260 .....	8
2.2 Hardware Description .....	9
2.3 Hardware Installation .....	11
2.4 Console Interface .....	12
2.5 Access Web Management Interface .....	14
3. Connect your AP to your Network .....	18
4. Adding Virtual Access Points .....	24
5. Secure Your AP .....	26
6. Create a WDS Bridge between two APs .....	35
7. Web Management Interface Configuration .....	37
7.1 System .....	39
7.1.1 General .....	39
7.1.2 Network Interface .....	41
7.1.3 Port .....	42
7.1.5 CAPWAP .....	45
7.1.6 IPv6 .....	47
7.2 Wireless .....	48
7.2.1 VAP Overview .....	48
7.2.2 General .....	51
7.2.3 VAP Configuration .....	53
7.2.4 Security .....	54
7.2.5 Repeater .....	58
7.2.6 Advanced .....	60
7.2.7 Access Control .....	62
7.2.8 Site Survey .....	66
7.3 Firewall .....	68
7.3.1 Firewall List .....	68
7.3.2 Service .....	72
7.3.3 Advanced .....	73
7.4 Utilities .....	75
7.4.1 Change Password .....	75

7.4.2 Backup & Restore.....	76
7.4.3 System Upgrade .....	77
7.4.4 Reboot .....	78
7.4.5 Upload Certificate .....	79
7.4.6 WAPI Certificate .....	80
7.4.7 Channel Analysis .....	81

## 7.4.7 Channel Analysis




7.5 Status .....	82
7.5.1 Overview .....	82
7.5.2 Associated Clients .....	84
7.5.3 Repeater .....	85
7.5.4 Event Log.....	86
7.6 Online Help .....	87

# 1. Before You Start

## 1.1 Preface

This manual is intended for system integrators, field engineers, and network administrators to set up 4ipnet's EAP260 802.11n/b/g 2.4GHz MIMO Access Point in their network environments. It contains step-by-step procedures and visual examples to guide MIS staff or individuals with basic network system knowledge to complete the installation.

## 1.2 Document Conventions

	Represents essential steps, actions, or messages that should not be ignored.
<b>» Note:</b>	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 for the changes to take effect.
	Indicates that clicking this button will clear what you have set before the settings are applied.

## 1.3 Package Content

The standard package of EAP260 includes:

- 4ipnet EAP260 x1
- Quick Installation Guide (QIG) x1
- CD-ROM (with User's Manual and QIG) x1
- Console Cable x1
- Ethernet Cable x1
- Power Adapter (DC 5V) x1
- Detachable Antenna x2



*It is recommended to keep the original packing materials 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.*

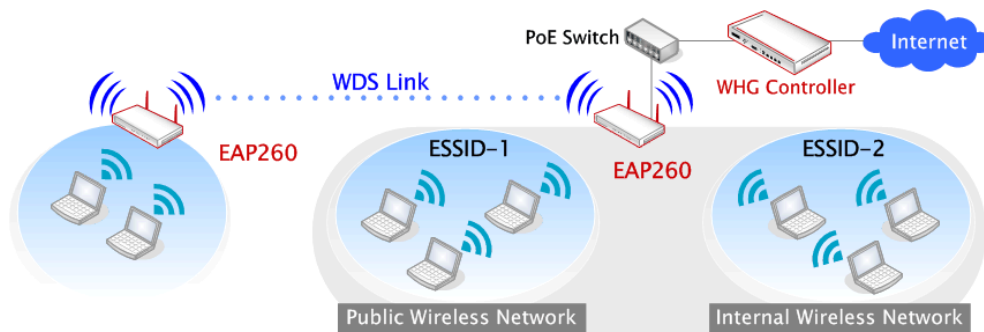


## 2. System Overview and Getting Started

### 2.1 Introduction of 4ipnet EAP260

The 4ipnet EAP260 Enterprise Access Point embedded with 802.11 n/b/g 2.4GHz MIMO radio in dust-proof metal housing is designed for wireless connectivity in enterprise or industrial environments of all dimensions. EAP260 makes the wireless communication fast, secure and easy. It supports business grade security such as 802.1X, and Wi-Fi Protected Access (WPA and WPA2). By pushing a purposely built button, the **4ipWES (Press-n-Connect)** feature makes it easy to bridge wireless links of multiple EAP260s for forming a wider wireless network coverage.

EAP260 also features multiple ESSIDs with VLAN tags and multiple Virtual APs, great for enterprise applications, such as separating traffic from different departments using different ESSIDs. The PoE LAN port is able to receive power from Power over Ethernet (PoE) sourcing devices. Its metal case is IP50 anti-dust compliant, which means that EAP260 is well suited to WLAN deployment in industrial environments.



**Wired and Wireless Network Layout with EAP260s**

## 2.2 Hardware Description

This section depicts the hardware information including all panel description.

### Front Panel

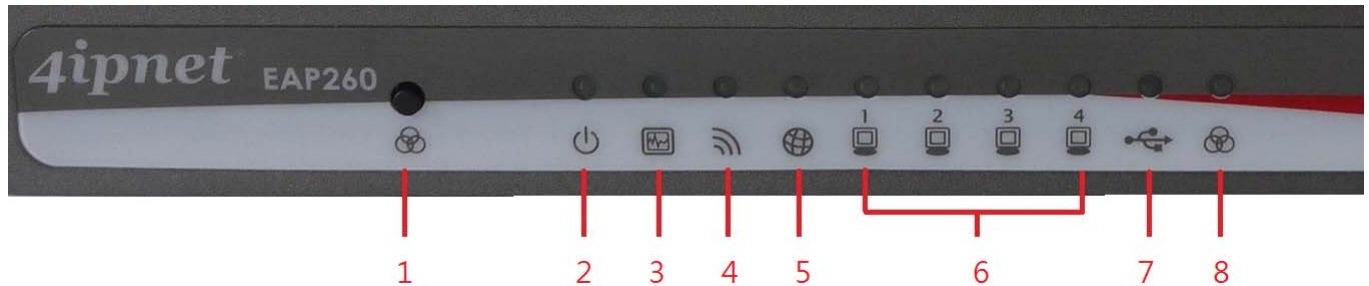


Figure 1 EAP260 Front Panel

1		<b>WES button</b>	Press and hold for 5 seconds to initiate Master WES process. Press and release to initiate Slave WES process.																		
2		<b>Power LED</b>	On indicates power on.																		
3		<b>Status LED</b>	On indicates the system is ready.																		
4		<b>Wireless LED</b>	On indicates wireless network interface is ready for service.																		
5		<b>Uplink LED</b>	On indicates the Uplink is connected.																		
6		<b>LAN1 - 4 LED</b>	Indicates the connection status of each LAN.																		
7		<b>USB LED</b>	Indicates the status of USB connection. The USB port is reserved for future use.																		
8		<b>WES LED</b>	For indicating WDS connection status. <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th></th> <th>Master</th> <th>Slave</th> </tr> </thead> <tbody> <tr> <td>WES Start</td> <td>LED (Green) OFF and then BLINKING SLOWLY</td> <td>LED (Red) OFF and then BLINKING SLOWLY</td> </tr> <tr> <td>WES Negotiate</td> <td>BLINKING NORMALLY (Green)</td> <td>BLINKING NORMALLY (Red)</td> </tr> <tr> <td>WES Timeout</td> <td>LED (Green) ON</td> <td>LED (Red) ON</td> </tr> <tr> <td>WES Success</td> <td>LED (Red) ON</td> <td>LED (Green) ON</td> </tr> <tr> <td>WES Fail</td> <td>LED (Green) ON</td> <td>LED (Red) ON</td> </tr> </tbody> </table>		Master	Slave	WES Start	LED (Green) OFF and then BLINKING SLOWLY	LED (Red) OFF and then BLINKING SLOWLY	WES Negotiate	BLINKING NORMALLY (Green)	BLINKING NORMALLY (Red)	WES Timeout	LED (Green) ON	LED (Red) ON	WES Success	LED (Red) ON	LED (Green) ON	WES Fail	LED (Green) ON	LED (Red) ON
	Master	Slave																			
WES Start	LED (Green) OFF and then BLINKING SLOWLY	LED (Red) OFF and then BLINKING SLOWLY																			
WES Negotiate	BLINKING NORMALLY (Green)	BLINKING NORMALLY (Red)																			
WES Timeout	LED (Green) ON	LED (Red) ON																			
WES Success	LED (Red) ON	LED (Green) ON																			
WES Fail	LED (Green) ON	LED (Red) ON																			

Rear Panel

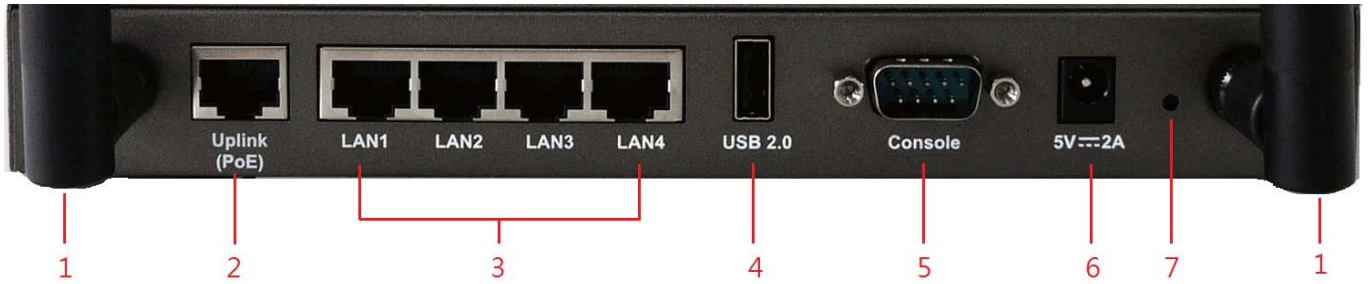


Figure 2 EAP260 Rear Panel

1	<b>Antenna connector</b>	Reverse SMA connectors for attaching antenna as shown in figure 2.
2	<b>Uplink port</b>	Offers uplink connection. This port can be used to connect to a controller, gateway, or directly to the Internet.
3	<b>LAN 1- 4 ports</b>	Attach Ethernet cables here for connecting to the wired local network.
4	<b>USB 2.0 port</b>	Reserved for future use.
5	<b>Console port</b>	Attach the serial cable here to access console interface.
6	<b>5V 2 A</b>	Attach the power adapter here.
7	<b>Reset button</b>	Press once to restart the system; Press and hold for more than 5 seconds to reset to factory default.

## 2.3 Hardware Installation

Please follow the steps mentioned below to install the hardware of EAP260:

**1. Place the EAP260 at the best location.**

The best location for EAP260 is usually at the center of your intended wireless network.

**2. Connect the EAP260 to your network device.**

Connect one end of the Ethernet cable to the Uplink port of EAP260 and the other end of the cable to a switch, a router, or a hub. EAP260 is then connected to your existing wired LAN network.

**3. There are two ways to supply power over to EAP260.**

a) Connect the DC power adapter to the EAP260 power socket.

b) EAP260 Uplink port is capable of receiving DC currents. Connect an IEEE 802.3af-compliant PSE device (e.g. a PoE-switch) to the Uplink port of EAP260 with the Ethernet cable.

Now, the Hardware Installation is complete.

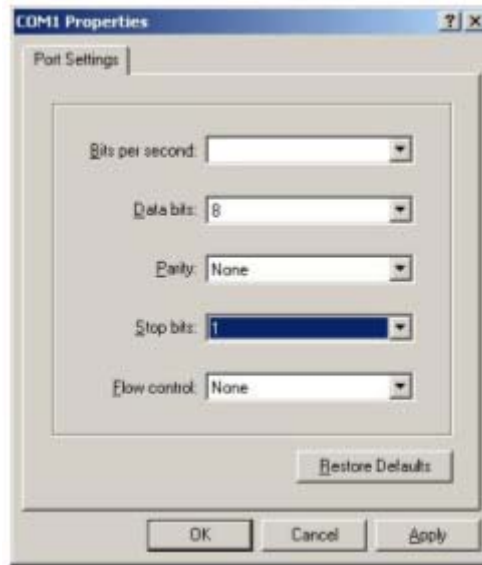


- *Please use only the power adapter supplied with the EAP260 package. Using a different power adapter may damage this system.*
- *To verify the wired connection between EAP260 and you switch / router / hub, please also check the LED status indicator of the respective network devices.*

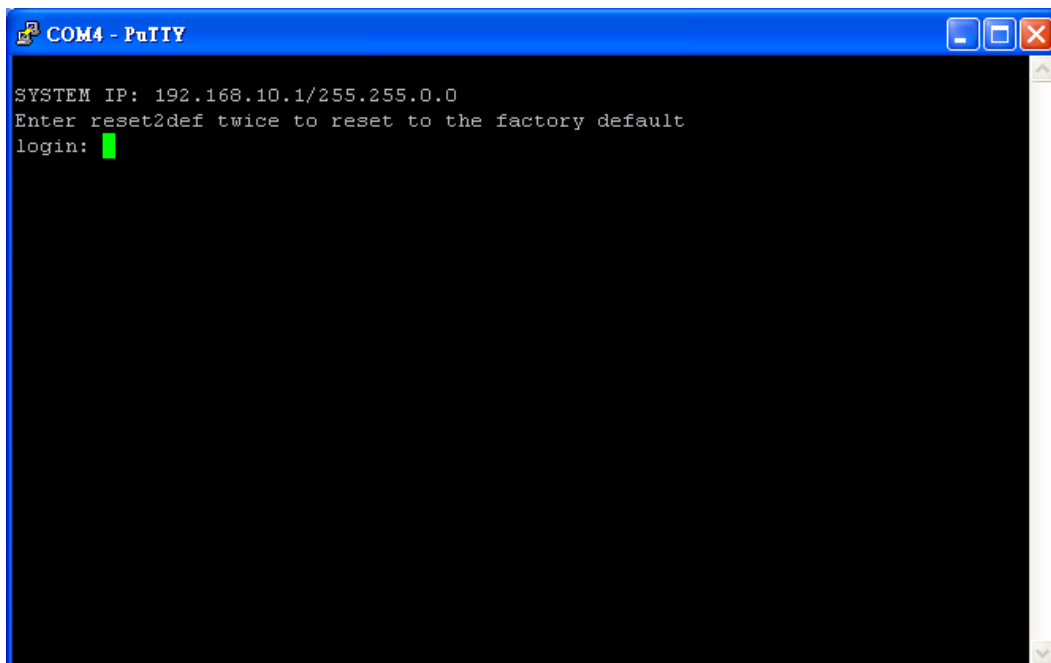
## 2.4 Console Interface

Use this port to enter the console interface for the administrator to check the IP address of EAP260 and reset the device to default if the admin password is forgotten.

1. In order to connect to the console port of EAP260, a console, modem cable and a terminal simulation program, such as the Hyper Terminal are needed.
2. If a Hyper Terminal is used, please set the parameters as **115200, 8, None, 1, None**.

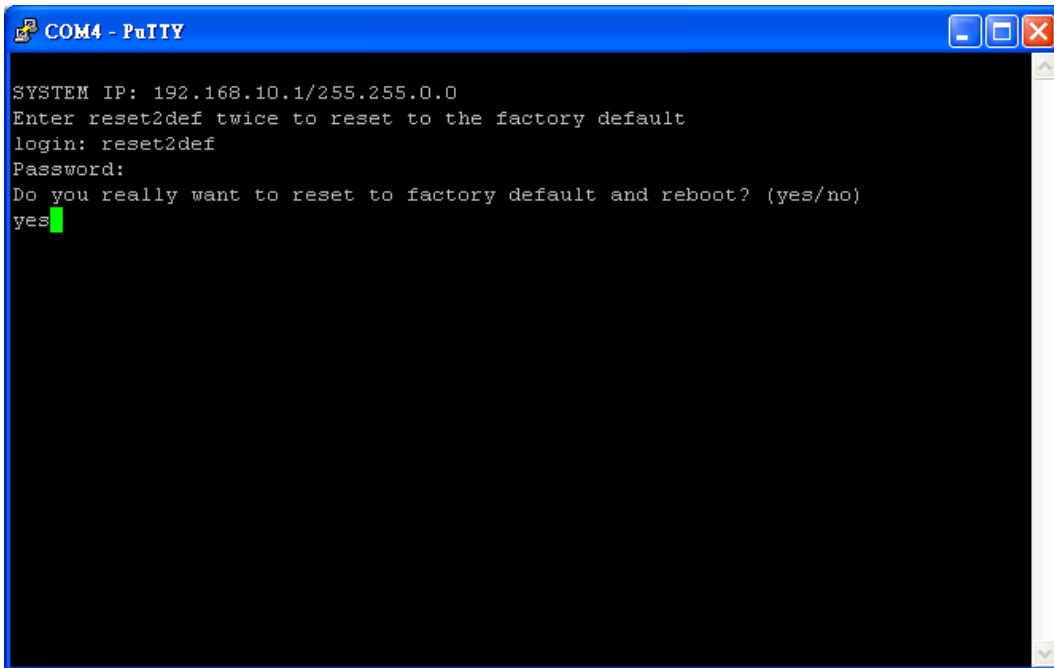


The console interface looks like the screenshot below, displaying the current LAN IP address and the instructions to reset device to default.



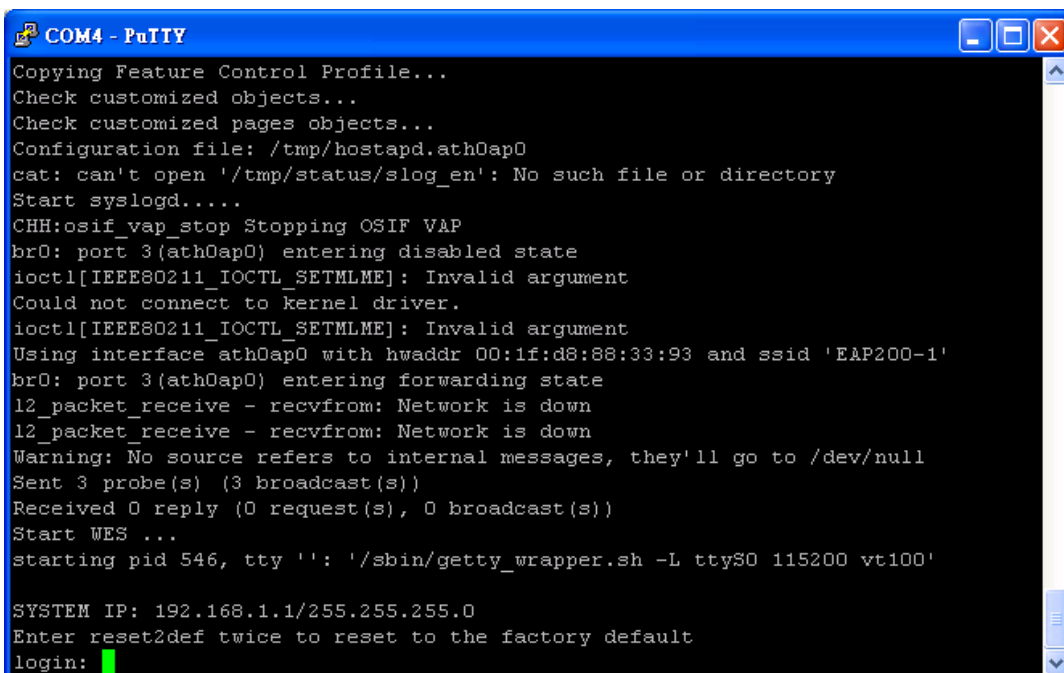
When resetting the device to default from the console interface, enter “reset2def” for login and password.

Confirm “yes” and EAP260 will begin the reset process.



```
COM4 - PuTTY
SYSTEM IP: 192.168.10.1/255.255.0.0
Enter reset2def twice to reset to the factory default
login: reset2def
Password:
Do you really want to reset to factory default and reboot? (yes/no)
yes
```

When the login prompt reappears, the device has completed the reset to default process and the LAN IP is reset to 192.168.1.1.



```
COM4 - PuTTY
Copying Feature Control Profile...
Check customized objects...
Check customized pages objects...
Configuration file: /tmp/hostapd.ath0ap0
cat: can't open '/tmp/status/slog_en': No such file or directory
Start syslogd....
CHH:osif_vap_stop Stopping OSIF VAP
br0: port 3(ath0ap0) entering disabled state
ioctl[IEEE80211_IOCTL_SETMLME]: Invalid argument
Could not connect to kernel driver.
ioctl[IEEE80211_IOCTL_SETMLME]: Invalid argument
Using interface ath0ap0 with hwaddr 00:1f:d8:88:33:93 and ssid 'EAP200-1'
br0: port 3(ath0ap0) entering forwarding state
l2_packet_receive - recvfrom: Network is down
l2_packet_receive - recvfrom: Network is down
Warning: No source refers to internal messages, they'll go to /dev/null
Sent 3 probe(s) (3 broadcast(s))
Received 0 reply (0 request(s), 0 broadcast(s))
Start WES ...
starting pid 546, tty '': '/sbin/getty_wrapper.sh -L ttyS0 115200 vt100'

SYSTEM IP: 192.168.1.1/255.255.255.0
Enter reset2def twice to reset to the factory default
login:
```

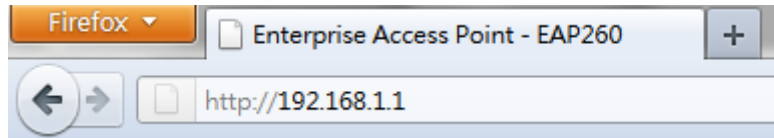
## 2.5 Access Web Management Interface

4ipnet EAP260 supports web-based configuration. When hardware installation is complete, EAP260 can be configured through a PC by using a web browser.

The default values of the EAP260's LAN IP Address and Subnet Mask are:

**IP Address:** 192.168.1.1

**Subnet Mask:** 255.255.255.0



*Example of entering EAP260's default IP Address into a web browser*

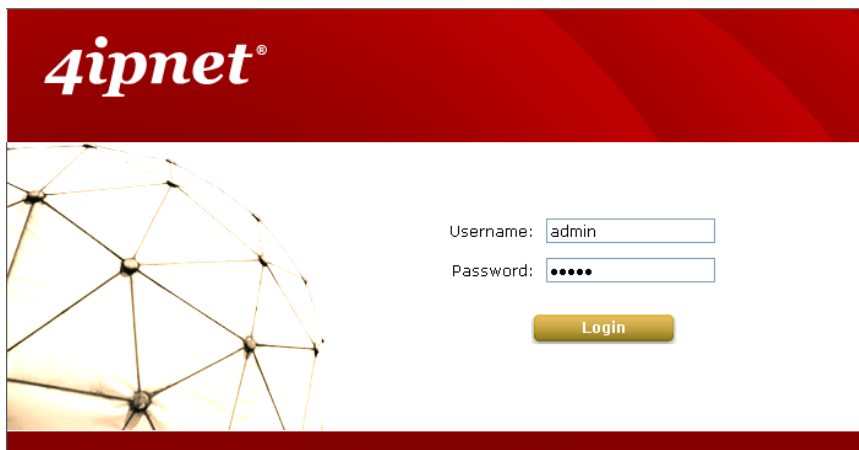
- To access the web management interface (WMI), connect the administrator PC to the LAN port of EAP260 via an Ethernet cable. Then, set a static IP Address on the same subnet mask as the EAP260 in TCP/IP settings of your PC, such as the following example:

**IP Address:** 192.168.1.100

**Subnet Mask:** 255.255.255.0


- ▶ **Note:** Please note that the IP Address used should not overlap with the IP Addresses of any other device within the same network to avoid IP conflict.


- Launch the web browser on your PC and enter the IP Address of the EAP260 (**192.168.1.1**) at the address field, and then press **Enter**. The following Administrator Login Page will appear. Enter "admin" for both the **Username** and **Password** fields, and then click **Login**.





*Administrator Login Page*


- After a successful login into EAP260, a **System Overview** page of the Web Management Interface (WMI) will appear.

  
System

  
Wireless

  
Firewall

  
Utilities

  
Status

Overview

Associated Clients

Repeater

Event Log

[Home](#) > [Status](#) > System Overview

### System Overview

#### System

System Name	Enterprise Access Point - EA...
Firmware Version	1.00.00
Build Number	1.7-1.4754
Location	
Site	EN-A
Device Time	1970/01/01 08:26:49
System Up Time	0 days, 0:26:49


#### Radio Status

MAC Address	00:1F:D3:87:03:03
Band	802.11g+n
Channel	1
TX Power	Highest

#### LAN Interface

MAC Address	00:1F:D3:87:03:01
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	192.168.1.254

#### AP Status

Profile Name	BSSID	ESSID	Security Type	Online Clients	Tun
VAP-1	00:1F:D3:87:03:03	EAP260-1	None	0	

#### CAPWAP

Status Disabled

#### IPv6

Status Disabled

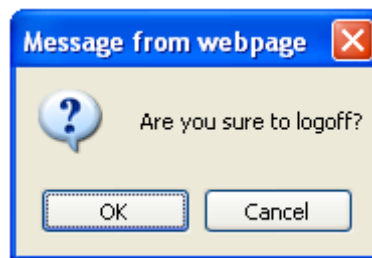
**The Web Management Interface - System Overview Page**



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



**Logout**



**Logout Prompt**



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

Please follow the following steps to change the administrator's password:

Home > Utilities > Change Password

## Change Password

Name : admin

Old Password :

New Password :  \*up to 32 characters

Re-enter New Password :

### **Change Password Page**

- Click on the **Utilities** icon on the main menu, and select the **Change Password** tab.
- Enter the old password and then a new password with a length of up to 32 characters, and retype it in the **Re-enter New Password** field.

### **Congratulation!**

Now, 4ipnet's EAP260 is installed and configured successfully.



- *It is strongly recommended to make a backup copy of your configuration settings.*
- *After the EAP260'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.*

### 3. Connect your AP to your Network

The following instructions depict how to establish the wireless coverage of your network. The AP will connect to the network through its LAN port and provide wireless access to your network.

After having prepared the EAP260's hardware for configuration, set the TCP/IP settings of administrator's computer to have a static **IP Address** of 192.168.1.10 and **Subnet Mask** of 255.255.255.0.

**Step 1: Configuring the AP's System Information**

- Enter the AP's default IP Address (**192.168.1.1**) into the URL of a web browser.
- Log in using **Username: admin** and **Password: admin**.

The WMI will appear as shown below.

The screenshot displays the 'System Overview' page of the EAP260 Web Management Interface. At the top, there are navigation tabs for System, Wireless, Firewall, Utilities, and Status. Below these are sub-tabs for Overview, Associated Clients, Repeater, and Event Log. The main content area is titled 'System Overview' and contains several panels:

- System**: A table listing system details.
 

System Name	Enterprise Access Point - EA...
Firmware Version	1.00.00
Build Number	1.7-1.4754
Location	
Site	EN-A
Device Time	1970/01/01 08:26:49
System Up Time	0 days, 0:26:49
- Radio Status**: A table showing radio configuration.
 

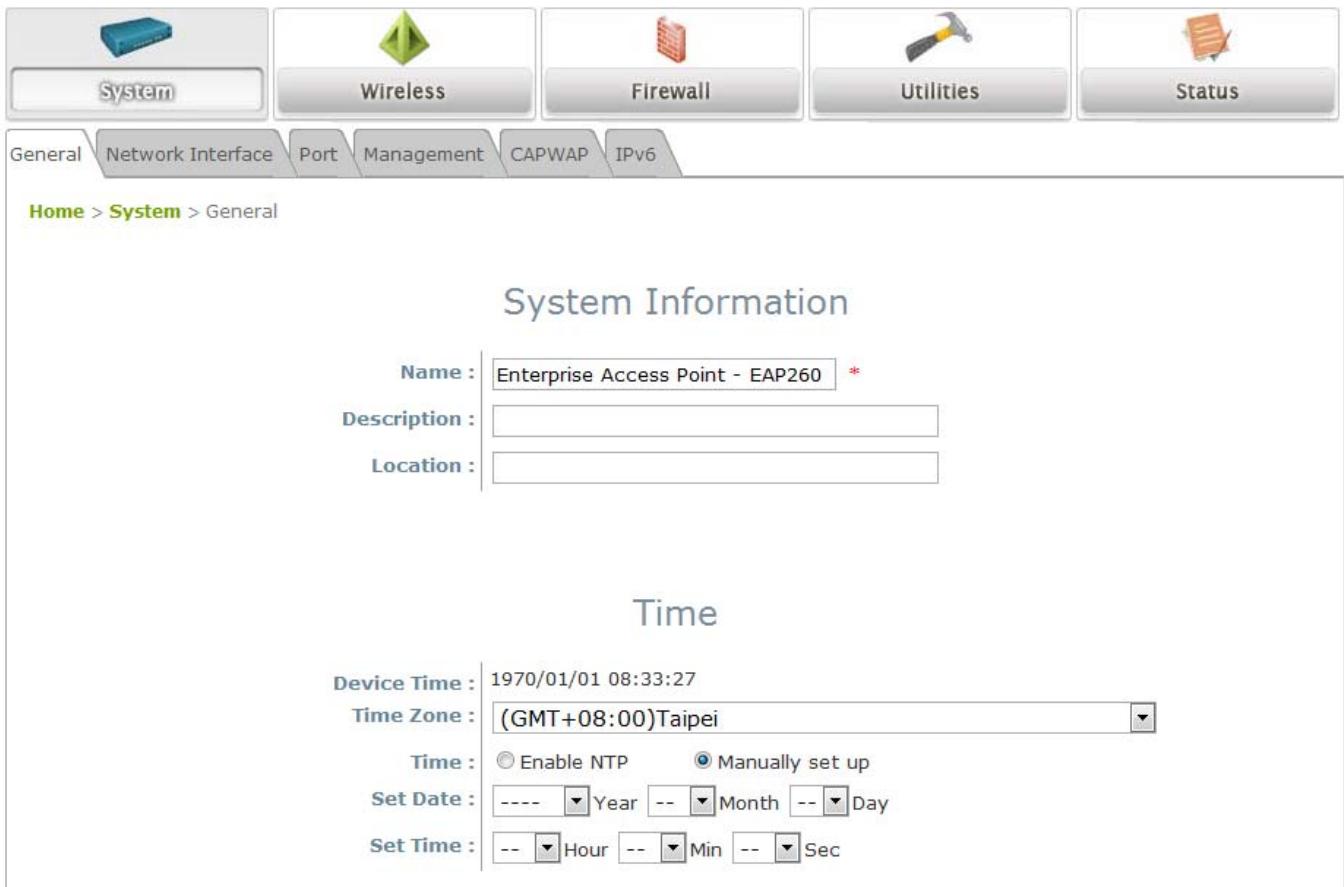
MAC Address	00:1F:D3:87:03:03
Band	802.11g+n
Channel	1
TX Power	Highest
- LAN Interface**: A table showing network settings.
 

MAC Address	00:1F:D3:87:03:01
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	192.168.1.254
- AP Status**: A table listing active profiles.
 

Profile Name	BSSID	ESSID	Security Type	Online Clients	Tun
VAP-1	00:1F:D3:87:03:03	EAP260-1	None	0	<input checked="" type="checkbox"/>
- CAPWAP**: A status field showing 'Status Disabled'.
- IPv6**: A status field showing 'Status Disabled'.

Web Management Interface Main Page (System Overview)

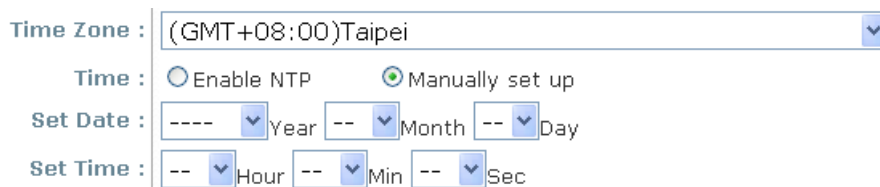
From here, click on the **System** icon to get to the following page. On this Page you can make entries to the **Name**, **Description**, and **Location** fields as well as set the device's time.



**System Information Page**

There are two methods of setting up the time: Manual (indicated by the option **Set Date & Time**) and NTP.

The default is Manual and requires individual setup every time the system starts up. Simply choose a time zone and set the time accordingly. When it is finished, click **SAVE**.



**Manually Time Setup**

The alternative method is **NTP**. Upon selecting **NTP** under the **Time** field, the configuration changes to allow up to two **NTP** servers. Simply enter a local NTP server's IP Address (if available) or search online for an NTP server nearest to you. Set the time zone and click **SAVE**.

Time Zone : (GMT+08:00)Taipei

Time :  Enable NTP  Manually set up

NTP Server 1 :  \*

NTP Server 2 :

### NTP Setup

## Step 2: Configuring the AP's Network Settings

While still on this Page, click on the **Network Interface** tab to begin configuration of the network settings.

General Network Interface Port Management CAPWAP IPv6

Home > System > Network Interface

### Network Settings

Mode :  Static  DHCP

IP Address :  \*

Netmask :  \*

Default Gateway :  \*

Primary DNS Server :  \*

Alternate DNS Server :

Layer2 STP :  Disable  Enable

### Network Settings Page

If the deployment decides that the AP will be getting dynamic IP Addresses from the connected network, set **Mode** to *DHCP*; otherwise, set **Mode** to **Static** and fill in the required fields marked with a red asterisk (**IP Address**, **Netmask**, **Gateway**, and **Primary DNS Server**) with the appropriate values for the network. Click **SAVE** when you are finished to save changes that have been made.

**Step 3: Configure the AP's Wireless General Settings**

Click on the **Wireless** icon followed by the **General** tab. On this page we need to choose the **Band** and **Channel** that we wish to use.

The screenshot shows the configuration interface for the 4IPNET EAP260 Enterprise Access Point. At the top, there are five main menu buttons: System, Wireless (highlighted), Firewall, Utilities, and Status. Below these are sub-menu tabs for VAP Overview, General (selected), VAP Config, Security, Repeater, Advanced, Access Control, and Site Survey. The breadcrumb trail reads 'Home > Wireless > General'. The main content area is titled 'General Settings' and contains the following configuration options:

- Band :** 802.11g+802.11n (dropdown menu)  Pure 11n
- Short Preamble :**  Disable  Enable
- Short Guard Interval :**  Disable  Enable
- Channel Width :** 20 MHz (dropdown menu)
- Channel :** 1 (dropdown menu)
- Max Transmit Rate :** Auto (dropdown menu)
- Transmit Power :** Auto (dropdown menu)
- ACK Timeout :** 0 \*(0 - 255, 0:Auto, Unit:4 micro seconds)
- Beacon Interval :** 100 \*(100 - 500ms )

**Wireless General Settings Page**

On this page, select the **Band** with which the AP is to broadcast its signal. The rest of the fields are optional and can be configured at another time. Click **SAVE** if any changes have been made.

**Step 4: Configuring Wireless Coverage (VAP-1)**

To set up the AP's wireless access, refer to the following VAP-1 configuration (other VAP configuration can refer to the same setup steps as done for VAP-1). Click on the **Overview** tab to proceed.

Home > Wireless > VAP Overview

### VAP Overview

VAP No.	ESSID	State	Security Type	MAC ACL	Advanced Settings
1	EAP260-1	Enabled	None	Disabled	<a href="#">Edit</a>
2	EAP260-2	Disabled	None	Disabled	<a href="#">Edit</a>
3	EAP260-3	Disabled	None	Disabled	<a href="#">Edit</a>
4	EAP260-4	Disabled	None	Disabled	<a href="#">Edit</a>
5	EAP260-5	Disabled	None	Disabled	<a href="#">Edit</a>
6	EAP260-6	Disabled	None	Disabled	<a href="#">Edit</a>
7	EAP260-7	Disabled	None	Disabled	<a href="#">Edit</a>
8	EAP260-8	Disabled	None	Disabled	<a href="#">Edit</a>

**Virtual AP Overview Page**

On this page click the hyperlink in the row and column that corresponds with VAP-1's State. This will bring up the following page.

Home > Wireless > VAP Config

### VAP Configuration

Profile Name :

VAP :  Disable  Enable

Profile Name :

ESSID :

VLAN ID :  Disable  Enable

VLAN ID :  \*( 1 - 4094 )

**VAP Configuration Page (VAP-1 shown)**

The desired VAP profile can be selected from the drop-down menu of Profile Name and VAP-1 configuration will serve as an example for all other VAPs. Before proceeding further, please make sure that the **VAP** field is marked **Enable**; afterwards, enter an **ESSID** to represent the WLAN associated with AP's VAP-1. It is suggested that Profile Name is used to describe what this particular VAP will be used for; otherwise, leave it as default. **VLAN ID** can be chosen at another time. Click **SAVE** to save all changes up to this point and **Reboot** the system to apply these revised settings.

### ***Congratulations!***

After reboot, the AP can start to operate with these revised settings.



## 4. Adding Virtual Access Points

EAP260 possesses the feature of multi-ESSID; namely, it can behave as multiple virtual access points, providing different levels of services from the same physical AP device.

Please click on the **Wireless** icon to review the **VAP Overview** page.

Home > Wireless > VAP Overview

### VAP Overview

VAP No.	ESSID	State	Security Type	MAC ACL	Advanced Settings
1	EAP260-1	Enabled	None	Disabled	Edit
2	EAP260-2	Disabled	None	Disabled	Edit
3	EAP260-3	Disabled	None	Disabled	Edit
4	EAP260-4	Disabled	None	Disabled	Edit
5	EAP260-5	Disabled	None	Disabled	Edit
6	EAP260-6	Disabled	None	Disabled	Edit
7	EAP260-7	Disabled	None	Disabled	Edit
8	EAP260-8	Disabled	None	Disabled	Edit

### VAP Overview Page

To proceed with specific VAP configuration, click on the corresponding cell in the **State** column and row of the VAP; the particular VAP's Configuration page will then appear for further configuration.

Home > Wireless > VAP Config

### VAP Configuration

Profile Name : VAP-1

VAP :  Disable  Enable

Profile Name :

ESSID :

VLAN ID :  Disable  Enable

VLAN ID :  \*( 1 - 4094 )

#### VAP Configuration Page (VAP-1 shown)

Please select the desired VAP profile from the drop-down menu of Profile Name. Choose **Enable** for the **VAP** field. Pick a descriptive **Profile Name** and an appropriate **ESSID** for clients to associate to. A **VLAN ID** can be provided to indicate the traffic through this particular VAP. It may allow further management/control (e.g. access rights and Internet usage, etc) of each VAP with a management gateway. Click **SAVE** and then **Reboot** for the changes to take effect.

## 5. Secure Your AP

Different VAP may require different levels of security. These instructions will guide the user through setting up different types of security for a particular VAP. Simply repeat the following steps for other VAP with security requirement.

### Step 1: Ensure the intended VAP is Enabled

The screenshot shows the 'VAP Overview' page. At the top, there are five main menu items: System, Wireless (selected), Firewall, Utilities, and Status. Below these are sub-menu items: VAP Overview, General, VAP Config, Security, Repeater, Advanced, Access Control, and Site Survey. The breadcrumb trail is 'Home > Wireless > VAP Overview'. The main heading is 'VAP Overview'. Below it is a table with the following data:

VAP No.	ESSID	State	Security Type	MAC ACL	Advanced Settings
1	EAP260-1	Enabled	None	Disabled	Edit
2	EAP260-2	Disabled	None	Disabled	Edit
3	EAP260-3	Disabled	None	Disabled	Edit
4	EAP260-4	Disabled	None	Disabled	Edit
5	EAP260-5	Disabled	None	Disabled	Edit
6	EAP260-6	Disabled	None	Disabled	Edit
7	EAP260-7	Disabled	None	Disabled	Edit
8	EAP260-8	Disabled	None	Disabled	Edit

#### VAP Overview Page

On the **VAP Overview** page, check the table to confirm the VAP State. If it is **Enabled**, skip to **Step 2**. If not, click on to proceed with **VAP Configuration** for that particular VAP.

Home > Wireless > VAP Config

### VAP Configuration

Profile Name : VAP-1

VAP :  Disable  Enable

Profile Name : VAP-1

ESSID : EAP260-1

VLAN ID :  Disable  Enable

VLAN ID : \*( 1 - 4094 )

**VAP Configuration Page (VAP-1 as shown for example)**

Select **Enable** for the **VAP** field and click **SAVE**. Click the **Overview** tab to return to the previous table to begin the next step.

### Step 2: Configure Security Settings for your VAP

The following instructions will guide the user to set up wireless security with a specific VAP. If only restricted access of certain MAC addresses is desired, skip to Step3. MAC restriction can be coupled with wireless security to provide extra protection.

First, click on the corresponding cell in the column labeled **Security Type**. This hyperlink will direct the user to the following **Security Settings** page.

Home > Wireless > Security

### Security Settings

Profile Name : VAP-1

Security Type : None

**Security Settings Page (VAP-1 as shown for example)**

Select the desired **Security Type** from the drop-down menu, which includes **None**, **WEP**, **802.1X**, **WPA-PSK**, and **WPA-RADIUS**.

- **None:** Authentication is not required and data is not encrypted during transmission when this option is selected. This is the default setting as shown in the following figure.

The screenshot shows the 'Security Settings' page with the following configuration:

- Profile Name: VAP-1
- Security Type: None

**Security Settings: None**

- **WEP:** WEP (Wired Equivalent Privacy) is a data encryption mechanism with key length selected from 64-bit, 128-bit, or 152-bit.

The screenshot shows the 'Security Settings' page with the following configuration:

- Profile Name: VAP-1
- Security Type: WEP
- Note! The WEP keys are global setting for all virtual APs. The key value will apply to all VAPs.
- 802.11 Authentication:  Open System  Shared Key  Auto
- WEP Key Length:  64 bits  128 bits  152 bits
- WEP Key Format:  ASCII  Hex
- WEP Key Index: 1
- WEP Keys: 4 empty input fields for key values.

**Security Settings: WEP**

- **802.11 Authentication:** Select from **Open System**, **Shared Key**, or **Auto**.
- **WEP Key Length:** Select from **64-bit**, **128-bit**, **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 is used for the encryption of wireless frames during data transmission.
- **WEP Keys:** Provide the pre-defined WEP key value; the system supports up to 4 sets of WEP keys.

- **802.1X:** When **802.1X Authentication** is selected, RADIUS authentication and enhanced dynamic WEP are provided.

VAP Overview General VAP Config Security Repeater Advanced Access Control Site Survey

Home > Wireless > Security

## Security Settings

Profile Name : VAP-1

Security Type : 802.1X

Dynamic WEP :  Disable  Enable

WEP Key Length :  64 bits  128 bits

Rekeying Period : 300 second(s)

Primary RADIUS Server :

Host :  \*( Domain Name / IP Address )

Authentication Port : 1812 \*

Secret Key :  \*

Accounting Service :  Disable  Enable

Accounting Port : 1813 \*

Accounting Interim Update Interval : 60 second(s) \*

### **Security Settings: 802.1X Authentication**

#### ➤ Dynamic WEP Settings:

- **Dynamic WEP:** For 802.1X security type, Dynamic WEP is always enabled to automatically generate WEP keys for encryption.
- **WEP Key Length:** Select from **64-bits** or **128-bits** key length.
- **Re-keying Period:** The time interval for the dynamic WEP key to be updated; the time unit is in seconds.

#### ➤ 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:** Enabling this option allows accounting of login and logouts through the RADIUS server.
- **Accounting Port:** The port number used by the RADIUS server for accounting purposes. Specify a port number or use the default, 1813.
- **Accounting Interim Update Interval:** The system will update accounting information to the RADIUS server every interval period.

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

VAP Overview | General | VAP Config | **Security** | Repeater | Advanced | Access Control | Site Survey

Home > Wireless > Security

### Security Settings

Profile Name : VAP-1

Security Type : WPA-PSK

Cipher Suite : TKIP (WPA)

Pre-shared Key Type :  PSK(Hex)\*( 64 chars )  Passphrase\*( 8 - 63 chars )

Pre-shared Key :

Group Key Update Period: 600 second(s)

#### **Security Settings: WPA-PSK**

- **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 seconds.

- **WPA-RADIUS:** Authenticates users by RADIUS and provides WPA data encryption.

VAP Overview General VAP Config **Security** Repeater Advanced Access Control Site Survey

Home > Wireless > Security

### Security Settings

Profile Name : VAP-1

Security Type : WPA-RADIUS

Cipher Suite : TKIP (WPA)

Group Key Update Period: 600 second(s)

Primary RADIUS Server :

Host :  \*( Domain Name / IP Address )

Authentication Port : 1812 \*

Secret Key :  \*

Accounting Service :  Disable  Enable

Accounting Port : 1813 \*

Accounting Interim Update Interval : 60 second(s) \*

#### Security Settings: WPA-RADIUS

➤ **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 seconds.

➤ **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:** Enabling this option allows accounting of login and logouts through the RADIUS server.
- **Accounting Port:** The port number used by the RADIUS server for accounting purposes. Specify a port number or use the default, 1813.
- **Accounting Interim Update Interval:** The system will update accounting information to the RADIUS server every interval period.

When these configurations are finished and MAC restriction is not needed, click **SAVE** and **Reboot** the system. Otherwise, click on the **Overview** tab and proceed to the next step.



**Step 3: Configuring MAC ACL (Access Control List)**

Clicking on the hyperlink corresponding with intended VAP in the **MAC ACL** column will bring the user to the **Access Control Settings** page.

The screenshot shows the 'Access Control Settings' page. At the top, there are navigation tabs: VAP Overview, General, VAP Config, Security, Repeater, Advanced, Access Control (selected), and Site Survey. Below the tabs is a breadcrumb trail: Home > Wireless > Access Control. The main heading is 'Access Control Settings'. There are three configuration fields: 'Profile Name' is a dropdown menu set to 'VAP-1'; 'Maximum Number of Clients' is a text input field containing '32' with a red asterisk and '( Range: 1 ~ 32 )' next to it; 'Access Control Type' is a dropdown menu set to 'Disable Access Control'.

**Access Control Settings Page**

Please choose among **Disable**, **Allow**, **Deny**, and **RADIUS ACL** from the drop-down menu of **Access Control Type**.

- 1) **Disable Access Control:** This means that there is no restriction for client devices to access the system.
- 2) **MAC ACL Allow List:** This means that only the client devices (identified by their MAC addresses) listed in the **Allow List** (“allowed MAC addresses”) are granted with access to the system. The administrator can temporarily block any allowed MAC address by checking **Disable**, until the administrator renews the listed MAC.

The screenshot shows the 'Access Control Settings' page with 'MAC ACL Allow List' selected in the 'Access Control Type' dropdown. Below the configuration fields is a table with three columns: 'No.', 'MAC Address', and 'State'. The table contains two rows, each with an empty input field for the MAC address and radio buttons for 'Disable' (selected) and 'Enable'.

No.	MAC Address	State
1	<input type="text"/>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
2	<input type="text"/>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

**MAC ACL Allow List**



*An empty Allow List means that there are no allowed MAC addresses. Make sure at least the MAC of the modifying system is included (e.g. network administrator's computer)*

- 3) **MAC ACL Deny List:** This means that all client devices are granted with access to the system except those listed in the **Deny List** ("denied MAC addresses"). The administrator can allow any denied MAC address to connect to the system temporarily by checking **Enable**.

VAP Overview | General | VAP Config | Security | Repeater | Advanced | Access Control | Site Survey

Home > Wireless > Access Control

### Access Control Settings

Profile Name : VAP-1

Maximum Number of Clients : 32 \*( Range: 1 ~ 32 )

Access Control Type : MAC ACL Deny List

No.	MAC Address	State
1	<input type="text"/>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
2	<input type="text"/>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

**MAC ACL Deny List**

**RADIUS ACL:** Authenticate incoming MAC addresses by an external RADIUS server. When RADIUS ACL is selected, all incoming MAC addresses will be authenticated by an external RADIUS server. Please note that each VAP MAC ACL and its security type (shown on the **Security Settings** page) share the same RADIUS configuration.

VAP Overview | General | VAP Config | Security | Repeater | Advanced | Access Control | Site Survey

Home > Wireless > Access Control

### Access Control Settings

Profile Name : VAP-1

Maximum Number of Clients : 32 \*( Range: 1 ~ 32 )

Access Control Type : RADIUS ACL

Primary RADIUS Server :

Note!!! These settings will also apply to security settings which use RADIUS Server for this VAP.

Host: \*( Domain Name / IP Address )

Authentication Port: 1812 \*( 1 - 65535 )

Secret Key: \*

Secondary RADIUS Server :

Host:

Authentication Port:

Secret Key:

#### **RADIUS ACL**

Click **SAVE** and **Reboot** upon completing the related configurations to take effect.

## 6. Create a WDS Bridge between two APs

WDS link creation is convenient for extending network coverage where running wires is not an option, effectively transferring the traffic to the other end of WLAN/LAN through the EAP260. Since this is a peer to peer connection, both EAP260s will be configured the same way.

### Step 1: Make sure the Band and Channel are matched between the WDS peers

In order to create a valid WDS link, the two EAP260s must be configured to use the same channel and band for their wireless settings. Click the **Wireless** icon and then **General** tab to go to the following page.

The screenshot shows the 'Wireless' tab selected in the top navigation bar. Below it, the 'General' sub-tab is active. The 'General Settings' section contains the following configuration options:

- Band:** 802.11g+802.11n (dropdown menu)  Pure 11n
- Short Preamble:**  Disable  Enable
- Short Guard Interval:**  Disable  Enable
- Channel Width:** 20 MHz (dropdown menu)
- Channel:** 1 (dropdown menu)
- Max Transmit Rate:** Auto (dropdown menu)
- Transmit Power:** Auto (dropdown menu)
- ACK Timeout:** 0 \*(0 - 255, 0:Auto, Unit:4 micro seconds)
- Beacon Interval:** 100 \*(100 - 500ms)

### Wireless General Settings Page

Please make sure both APs are using the same **Band** and **Channel** in order to establish a successful WDS link. Click **SAVE** if any changes have been made.

**Step 2: Prevent Loops when Connecting Multiple APs**

When many APs are linked in this manner, undesired loops may form to lower overall WLAN performance. To prevent such occurrence, please make sure Layer 2 STP is enabled.

To turn on this feature, please click on the **System** icon and the **Network Interface** tab.

The screenshot displays the 'Network Settings' page within a web management interface. At the top, there are navigation tabs: 'General', 'Network Interface', 'Port', 'Management', 'CAPWAP', and 'IPv6'. Below the tabs, a breadcrumb trail reads 'Home > System > Network Interface'. The main heading is 'Network Settings'. Under 'Mode', there are radio buttons for 'Static' (selected) and 'DHCP', along with a 'Renew' button. Below this are input fields for 'IP Address' (192.168.1.1), 'Netmask' (255.255.255.0), 'Default Gateway' (192.168.1.254), 'Primary DNS Server' (192.168.1.254), and 'Alternate DNS Server' (empty). At the bottom, the 'Layer2 STP' section has radio buttons for 'Disable' (selected) and 'Enable'. Red asterisks are visible next to the IP Address, Netmask, Default Gateway, and Primary DNS Server fields.

**Network Settings Page**

Please select **Enable** in the field labeled **Layer2 STP**. This will prevent data from looping or creating a broadcast storm. Click **SAVE** when completed, and then **Reboot** to allow updated settings to take effect.

## 7. Web Management Interface Configuration

This chapter will guide the user through the EAP260's detailed settings. The following table shows all the User Interface (UI) functions of 4ipnet's EAP260 Enterprise Access Point. The Web Management Interface (WMI) is the page where the status is displayed, control is issued and parameters are configured. In the Web Management Interface; there are two main interface areas: **Main Menu** and **Working Area**. The **Working Area** occupies the major area of the WMI, displayed in the center of the interface. It is also referred to as the configuration page. The **Main Menu**, on the top of the WMI, allows the administrator to traverse to various management functions of the system. The management functions are grouped into branches: **System**, **Wireless**, **Firewall**, **Utilities**, and **Status**.

**Table 1 EAP260's Function Organization**

OPTION	FUNCTION
<b>System</b>	General
	Network Interface
	Port
	Management
	CAPWAP
	IPv6
<b>Wireless</b>	VAP Overview
	General
	VAP Config
	Security
	Repeater
	Advanced
	Access Control
	Site Survey
<b>Firewall</b>	Firewall List
	Service
	Advanced
<b>Utilities</b>	Change Password
	Backup & Restore
	System Upgrade
	Reboot
	Upload Certificate
	WAPI Certificate
<b>Status</b>	Overview

	Associated Clients
	Repeater
	Event Log

**» Note:**

On each configuration page, you may click **SAVE** to save the changes of your configured settings, but you must reboot the system for the changes to take effect. After clicking **SAVE**, the following message will appear: **“Some modification has been saved and will take effect after Reboot.”**  
**All online users will be disconnected during reboot or restart.**

## 7.1 System

Upon clicking the **System** icon, users can utilize this section for general configurations of the devices (e.g. Time Setup, Network Configurations, and System Logs). This section includes the following functions:

**General, Network Interface, Management, GRE Tunnel and CAPWAP.**

### 7.1.1 General

General Network Interface Port Management CAPWAP IPv6

Home > System > General

### System Information

Name : Enterprise Access Point - EAP260 \*

Description :

Location :

### Time

Device Time : 1970/01/01 08:27:10

Time Zone : (GMT+08:00)Taipei

Time :  Enable NTP  Manually set up

Set Date : ---- Year -- Month -- Day

Set Time : -- Hour -- Min -- Sec

#### System Information Page

- **System Information**

For maintenance purposes, it is highly recommended to have the following information stated as clearly as possible:

- **Name:** The system name used to identify this system.
- **Description:** Further information about the system (e.g. device model, firmware version, and active date).
- **Location:** The information on geographical location of the system for the administrator to locate the system easily.

- **Time**

- **Device Time:** Display the current time of the system.
- **Time Zone:** Select an appropriate time zone from the drop-down list box.



- **Time:** Synchronize the system time by reachable NTP servers or manual setup.

### 1) **Enable NTP:**

By selecting **Enabled NTP**, EAP260 can synchronize its system time with the NTP server automatically. When this method is chosen, at least one NTP server's IP address or domain name must be provided.

Time

Device Time : 2000/01/03 04:32:49

Time Zone : (GMT+08:00)Taipei

Time :  Enable NTP  Manually set up

NTP Server 1 :  \*

NTP Server 2 :

#### ***NTP Time Configuration Fields***

Generally, networks should have a common NTP server (internal or external). If there isn't, locate a nearby NTP server on the web.

### 2) **Manually set up:**

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

Time

Device Time : 2000/01/03 04:32:49

Time Zone : (GMT+08:00)Taipei

Time :  Enable NTP  Manually set up

Set Date : ---- Year -- Month -- Day

Set Time : -- Hour -- Min -- Sec

#### ***Manual Time Configuration Fields***

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



*Unless Internet connection or NTP becomes unavailable, it is recommended to use NTP server for time synchronization because system time needs to be reconfigured upon reboot.*

## 7.1.2 Network Interface

On this page, the network settings of the device can be configured; fields with a red asterisk (i.e. **IP Address, Netmask, Default Gateway, and Primary DNS Server**) are mandatory.

The screenshot displays the 'Network Settings' page. At the top, there are tabs for 'General', 'Network Interface', 'Port', 'Management', 'CAPWAP', and 'IPv6'. Below the tabs, a breadcrumb trail reads 'Home > System > Network Interface'. The main heading is 'Network Settings'. Under 'Mode', there are radio buttons for 'Static' (selected) and 'DHCP', along with a 'Renew' button. The 'IP Address' field contains '192.168.1.1', 'Netmask' contains '255.255.255.0', 'Default Gateway' contains '192.168.1.254', and 'Primary DNS Server' contains '192.168.1.254'. Each of these four fields has a red asterisk to its right. The 'Alternate DNS Server' field is empty. At the bottom, 'Layer2 STP' has radio buttons for 'Disable' (selected) and 'Enable'.

### Network Settings Page

- **Mode:** Determine the way to obtain the IP address, by **DHCP** or **Static**.
  - **Static:** The administrator can manually set up the static LAN IP address. All required fields are marked with a red asterisk.
    - **IP Address:** The IP address of the LAN port.
    - **Netmask:** The Subnet mask of the LAN port.
    - **Default Gateway:** The Gateway IP address of the LAN port.
    - **Primary DNS Server:** The IP address of the primary DNS (Domain Name System) server.
    - **Alternate DNS Server:** The IP address of the substitute DNS server.
  - **DHCP:** This configuration type is applicable when the system is connected to a network with the presence of a DHCP server; all related IP information required will be provided by the DHCP server automatically.
- **Layer 2 STP:** If the EAP260 is set up to bridge other network components, this option can be enabled to prevent undesired loops because a broadcasting storm may occur in a multi-switch environment where broadcast packets are forwarded in an endless loop between switches. Moreover, a broadcast storm may consume most of available system resources in addition to available bandwidth. Thus, enabling the Layer 2 STP can lower such undesired occurrence and derive the best available data path for network communication.

### 7.1.3 Port

The physical Ethernet ports of EAP260 can be configured to append a VLAN tag for upstream delivery.

General Network Interface Port Management CAPWAP IPv6

Home > System > Port Config

### Port Configuration

Port : LAN1

VLAN ID :  Disable  Enable

VLAN ID : 100 \*( 1 - 4094 )

SAVE CLEAR

- **Port:** Selectable from LAN1 ~ LAN4. For each physical LAN port, administrator can choose to configure a desired VLAN ID to be bundled with traffic going upstream from this particular port.
  - **VLAN ID:** Enable selected implies that network traffic sent upstream from this LAN port will be tagged with the VLAN ID configured in the field below. Disable selected implies that traffic from this LAN port will not be tagged with a VLAN ID.

## 7.1.4 Management

The management services (e.g. **VLAN for Management**, **SNMP**, and **System log**) can be configured here.

Home > System > Management Services

### Management Services

**VLAN for Management:**  Disable  Enable  
 VLAN ID :  \*( 1 - 4094 )

**SNMP Configuration :**  Disable  Enable  
 Community String :  
 Read :   
 Write :   
 Trap :  Disable  Enable  
 Server IP :

**System Log :**  Disable  Enable  
 SYSLOG Server IP :   
 Server Port :   
 SYSLOG Level :

### *Management Services Page*

- VLAN for Management:** When it is enabled, management traffic from the system will be tagged with a VLAN ID. In other words, administrator who wants to access the WMI must send management traffic with the same VLAN ID such as connecting to a specific VAP with the same VLAN ID. Enter a value between 1 and 4094 for the VLAN ID if the option is enabled.

- **SNMP Configuration:** By enabling SNMP function, the administrator can obtain the system information remotely.

**SNMP Configuration :**

Disable  Enable

**Community String :**

Read :

Write :

Trap :  Disable  Enable

Server IP :

#### SNMP Configuration Fields

- **Enable/ Disable:** **Enable** or **Disable** this function.
  - **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:** **Enable** or **Disable** this function.
    - **Server IP Address:** Enter the IP address of the assigned server for receiving the trap report.
- **System Log:** By enabling this function, specify an external SYSLOG server to accept SYSLOG messages from the system remotely.

**System Log :**

Disable  Enable

SYSLOG Server IP :

Server Port :

SYSLOG Level :  ▼

#### System Log Fields

- **Enable/ Disable:** **Enable** or **Disable** this function.
- **Server IP:** The IP address of the Syslog server that will receive the reported events.
- **Server Port:** The port number of the Syslog server.
- **Syslog Level:** Select the desired level of received events from the drop-down menu.

### 7.1.5 CAPWAP

CAPWAP is a standard interoperable protocol that enables a controller to manage a collection of wireless access points. There are 5 methods of auto AP discovery, namely DNS SRV, DHCP option, Broadcast, Multicast, and Static.

General
Network Interface
Port
Management
CAPWAP
IPv6

[Home](#) > [System](#) > CAPWAP

#### CAPWAP Configuration

**CAPWAP :**  Disable  Enable

**Tunnel Interface :**  LAN1  LAN2  LAN3  LAN4  LAN5  
 VAP1  VAP2  VAP3  VAP4  VAP5  VAP6  VAP7  
 VAP8  
 WDS1  WDS2  WDS3  WDS4

**Certificate Date Check:**  Disable  Enable [Manage Certificates](#)

**DNS SRV Discovery :**  Disable  Enable  
 Domain Name Suffix :

**DHCP Option Discovery :**  Disable  Enable

**Broadcast Discovery :**  Disable  Enable

**Multicast Discovery :**  Disable  Enable

**Static Discovery :**  Disable  Enable

Pri.	AC Address	Remark
1	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>
2	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>
3	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>
4	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>
5	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>

- **CAPWAP:** The CAPWAP feature can be turned on by selecting “Enable” or turned off by selecting “Disable”
- **Tunnel Interface:** Select a LAN, VAP or WDS interface to designate its traffic to pass through the CAPWAP Tunnel established between AP and controller. For network interfaces that are unchecked, their traffic will be forwarded locally into the internet if this AP is deployed remotely on the WAN side of a controller.  
Please note that grey out check boxes imply that the particular VAP is not yet enabled for service. For instructions on how to enable VAP items, please refer to section **7.2.3 VAP Configuration** for reference.
- **Certificate Date Check:** To enable this item, select **Enable** and click **Manage Certificates** to enter the **Upload Certificate** page. Please refer to the section **7.4.4. Upload Certificate**.
- **DNS SRV Discovery:** The way of using DNS SRV to discover access controller.
  - **Domain Name Suffix:** Enter the suffix of the access controller, such as example.com.
- **DHCP Option Discovery:** Using DHCP option to discover access controller.
- **Broadcast Discovery:** Using Broadcast to discover access controller.
- **Multicast Discovery:** Using multicast to discover access controller.
- **Static Discovery:** Using Static approach to discover access controller.
  - **AC Address:** The IP address of access controller. If it can not discover the first AC, it will try to discover the second AC.

## 7.1.6 IPv6

EAP260 supports IPv6 and IPv4 dual stack addressing capability. IPv6 by default is disabled but it can be enabled on this tab page.

The screenshot shows the IPv6 Configuration page in the EAP260 web interface. The page has a navigation menu at the top with tabs for General, Network Interface, Port, Management, CAPWAP, and IPv6. The IPv6 tab is selected. Below the navigation menu, there is a breadcrumb trail: Home > System > IPv6 Configuration. The main content area is titled "IPv6 Configuration". It contains two sections: "Status" and "Mode". The "Status" section has two radio buttons: "Disable" (selected) and "Enable". The "Mode" section has two radio buttons: "Static" and "DHCP" (selected). At the bottom of the form, there are two yellow buttons: "SAVE" and "CLEAR".

**Mode:** There are two options for acquiring an IPv6 address for this device.

- **Static:** Configuring IPv6 address manually via this option if you have already acquired a permanent IPv6 address for operation.
- **DHCP:** Acquire IPv6 address automatically from upstream router.



## 7.2 Wireless

This section includes the following functions: **VAP Overview**, **General**, **VAP Configuration**, **Security**, **Repeater**, **Advanced**, **Access Control**, and **Site Survey**. EAP260 supports up to eight Virtual Access Points (VAPs). Each VAP can have its own settings (e.g. ESSID, VLAN ID, security settings, etc.). With such VAP capabilities, different levels of service can be configured to meet network requirements.

### 7.2.1 VAP Overview

An overall status is collected on this page, including **ESSID**, **State**, **Security Type**, **MAC ACL**, and **Advanced Settings**, where EAP260 features 8 VAPs with respective settings. In this table, please click on the hyperlink to further configure each individual VAP.

VAP No.	ESSID	State	Security Type	MAC ACL	Advanced Settings
1	EAP260-1	Enabled	None	Disabled	<a href="#">Edit</a>
2	EAP260-2	Disabled	None	Disabled	<a href="#">Edit</a>
3	EAP260-3	Disabled	None	Disabled	<a href="#">Edit</a>
4	EAP260-4	Disabled	None	Disabled	<a href="#">Edit</a>
5	EAP260-5	Disabled	None	Disabled	<a href="#">Edit</a>
6	EAP260-6	Disabled	None	Disabled	<a href="#">Edit</a>
7	EAP260-7	Disabled	None	Disabled	<a href="#">Edit</a>
8	EAP260-8	Disabled	None	Disabled	<a href="#">Edit</a>

**VAP Overview Page**

- **State:** The hyperlink showing **Enable** or **Disable** links to the **VAP Configuration** page.

VAP Overview | General | VAP Config | Security | Repeater | Advanced | Access Control | Site Survey

Home > Wireless > VAP Config

### VAP Configuration

Profile Name : VAP-1

VAP :  Disable  Enable

Profile Name : VAP-1

ESSID : EAP260-1

VLAN ID :  Disable  Enable

VLAN ID :  \*( 1 - 4094 )

**VAP – State Page**

- **Security Type:** The hyperlink showing the security type links to the **Security Settings** Page.

VAP Overview | General | VAP Config | Security | Repeater | Advanced | Access Control | Site Survey

Home > Wireless > Security

### Security Settings

Profile Name : VAP-1

Security Type : None

**VAP – Security Type Page**

- **MAC ACL:** The hyperlink showing **Allow** or **Disable** links to the **Access Control Settings** Page.

VAP Overview | General | VAP Config | Security | Repeater | Advanced | Access Control | Site Survey

Home > Wireless > Access Control

### Access Control Settings

Profile Name : VAP-1 ▼

Maximum Number of Clients :  \*( Range: 1 ~ 128 per system )

Access Control Type :  ▼

**VAP – MAC ACL Page**

- **Advanced Settings:** The advanced settings hyperlink links to the **Advanced Wireless Settings** Page.

VAP Overview | General | VAP Config | Security | Repeater | Advanced | Access Control | Site Survey

Home > Wireless > Advanced

### Advanced Wireless Settings

Profile Name : VAP-1 ▼

RTS Threshold :  \*(1 - 2346)

Fragment Threshold :  \*(256 - 2346)

DTIM period :  \*(1 - 15)

Broadcast SSID :  Disable  Enable

Wireless Station Isolation :  Disable  Enable

WMM :  Disable  Enable

IAPP :  Disable  Enable

Multicast/Broadcast Rate :  ▼

**VAP – Advanced Settings Page**

## 7.2.2 General

AP's general wireless settings can be configured here:

The screenshot shows the 'General Settings' page for an AP. The navigation tabs at the top are: VAP Overview, General (selected), VAP Config, Security, Repeater, Advanced, Access Control, and Site Survey. The breadcrumb trail is 'Home > Wireless > General'. The settings are as follows:

- Band:** 802.11g+802.11n (dropdown), with a checkbox for 'Pure 11n'.
- Short Preamble:** Radio buttons for 'Disable' and 'Enable' (selected).
- Short Guard Interval:** Radio buttons for 'Disable' and 'Enable' (selected).
- Channel Width:** 20 MHz (dropdown).
- Channel:** 6 (dropdown).
- Max Transmit Rate:** Auto (dropdown).
- Transmit Power:** Highest (dropdown).
- ACK Timeout:** 0 (input field), with a red asterisk and note: \*(0 - 255, 0:Auto, Unit:4 micro seconds).
- Beacon Interval:** 100 (input field), with a red asterisk and note: \*(100 - 500ms).

### AP General Settings Page

- **Band:** Select an appropriate wireless band: **802.11b**, **802.11g**, **802.11b+802.11g**, **802.11g+802.11n** or select **Disable** if the wireless function is not required.
  - **Pure 11n:** Enable 802.11n network only.
- **Short Preamble:** The short preamble with a 56-bit synchronization field can improve WLAN transmission efficiency. Select **Enable** to use Short Preamble or **Disable** to use Long Preamble with a 128-bit synchronization field.
- **Short Guard Interval (available when Band is 802.11g+802.11n):** The guard interval is the space between symbols (characters) being transmitted to eliminate inter-symbol interference. In order to further boost throughput with **802.11n**, short guard interval is half of what it used to be; please select **Enable** to use Short Guard Interval or **Disable** to use normal Guard Interval.
- **Channel Width (available when Band is 802.11g+802.11n):** Double channel bandwidth to 40 MHz is supported to enhance throughput.
- **Channel:** Select the appropriate **channel** from the drop-down menu to correspond with your network settings, for example, Channel 1-11 is available in North American and Channel 1-13 in Europe, or choose the default **6**.
- **Max Transmit Rate:** The maximum wireless transmit rate can be selected from the drop-down menu. The system will use the highest possible rate when **Auto** is selected. Please note that MCS0 ~ MCS15 are transmit rates for n clients only.
- **Transmit Power:** The signal strength transmitted from the system can be selected among **Auto**, **Highest**, **High**, **Medium**, **Low**, and **Lowest** from the drop-down menu.
- **ACK Timeout:** It indicates a period of time when the system waits for an Acknowledgement frame

sent back from a station without retransmission. In other words, upon timeout, if the Acknowledgement frame is still not received, the frames will be retransmitted. This option can be used to tune network performance for extended coverage. For regular indoor deployments, please keep the default setting.

- **Beacon Interval (ms):** The entered amount of time indicates how often the beacon signal will be sent from the access point.

**Table 2 RF Configurations (under normal circumstances in certain countries)**

Band	Channel	Rate	Power
<i>Disable</i>	N/A	N/A	N/A
<i>802.11a</i>	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140	6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M	Auto, Lowest, Low, Medium, High, Highest
<i>802.11b</i>	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	1M, 2M, 5.5M, 11M	
<i>802.11g</i>	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M	
<i>802.11b+802.11g</i>	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	1M, 2M, 5.5M, 6M, 9M, 11M, 12M, 18M, 24M, 36M, 48M, 54M	
<i>802.11a+802.11n</i>	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140	6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M, MCS0~15	
<i>802.11n+802.11g</i>	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13	1M, 2M, 5.5M, 11M, 12M, 18M, 24M, 36M, 48M, 54M, MCS0~15	

\*Please note that available values above will vary depending on the regulation of different countries.

## 7.2.3 VAP Configuration

This section provides configuration of each Virtual Access Point with settings such as **Profile Name**, **ESSID**, and **VLAN ID**.

Home > Wireless > VAP Config

### VAP Configuration

Profile Name : VAP-1

VAP :  Disable  Enable

Profile Name : VAP-1

ESSID : EAP260-1

VLAN ID :  Disable  Enable

VLAN ID :  \*( 1 - 4094 )

#### VAP Configuration Page

To enable specific VAP, select the VAP from the drop-down list of Profile Name. The basic settings of each VAP are collected in the profile as follows:

- **VAP:** *Enable* or *Disable* this VAP.
- **Profile Name:** The profile name of specific VAP for identity / management purposes.
- **ESSID:** ESSID (Extended Service Set ID) serves as an identifier for clients to associate with the specific VAP. It can be coupled with different service level like a variety of wireless security types.
- **VLAN ID:** EAP260 supports tagged VLANs (virtual LANs). To enable VLAN function, each VAP shall be given a unique VLAN ID with valid values ranging from 1 to 4094.

## 7.2.4 Security

EAP260 supports various wireless authentication and data encryption methods in each VAP profile. With this, the administrator can provide different service levels to clients. The security type includes **None**, **WEP**, **802.1X**, **WPA-PSK**, and **WPA-RADIUS**.

- **None:** Authentication is not required and data is not encrypted during transmission when this option is selected. This is the default setting as shown in the following figure.

The screenshot shows the 'Security Settings' configuration page for profile 'VAP-1'. The 'Security Type' dropdown menu is set to 'None'. The breadcrumb trail is 'Home > Wireless > Security'.

**Security Settings: None**

- **WEP:** WEP (Wired Equivalent Privacy) is a data encryption mechanism based on a 64-bit, 128-bit, or 152-bit shared key algorithm.

The screenshot shows the 'Security Settings' configuration page for profile 'VAP-1' with 'Security Type' set to 'WEP'. Under '802.11 Authentication', 'Open System' is selected. 'WEP Key Length' is set to 64 bits, 'WEP Key Format' is ASCII, and 'WEP Key Index' is 1. There are four empty input fields for 'WEP Keys'. A red note states: 'Note! The WEP keys are global setting for all virtual APs. The key value will apply to all VAPs.' The breadcrumb trail is 'Home > Wireless > Security'.

**Security Settings: WEP**

- **802.11 Authentication:** Select from **Open System**, **Shared Key**, or **Auto**.
  - **WEP Key Length:** Select a key length from **64-bit**, **128-bit**, or **152-bit**.
  - **WEP Key Format:** Select a WEP key format from **ASCII** or **Hex**.
  - **WEP Key Index:** Select a key index from **1~4**. The WEP key index is a number that specifies which WEP key will be used for the encryption of wireless frames during data transmission.
  - **WEP Keys:** Provide the pre-defined WEP key value; the system supports up to 4 sets of WEP keys.
- **802.1X:** When **802.1X Authentication** is selected, RADIUS authentication and Dynamic WEP are provided.

VAP Overview
General
VAP Config
Security
Repeater
Advanced
Access Control
Site Survey

Home > AP > Security

## Security Settings

Profile Name : VAP-1

Security Type : 802.1X

Dynamic WEP :  Disable  Enable

WEP Key Length :  64 bits  128 bits

Rekeying Period : 300 second(s)

Primary RADIUS Server :

Host :  \*( Domain Name / IP Address )

Authentication Port : 1812 \*

Secret Key :

Accounting Service :  Disable  Enable

Accounting Port : 1813 \*

Accounting Interim Update Interval : 60 second(s)\*

Secondary RADIUS Server :

Host:  ( Domain Name / IP Address )

### Security Settings: 802.1X Authentication

- **Dynamic WEP Settings:**
  - **Dynamic WEP:** For 802.1X security type, Dynamic WEP is always enabled to automatically generate WEP keys for encryption.
  - **WEP Key Length:** Select a key length from **64-bit** or **128-bit**.
  - **Re-keying Period:** The time interval for the dynamic WEP key to be updated; the time unit is in seconds.
- **RADIUS Server Settings (Primary/Secondary):**
  - **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:** Enabling this option allows accounting of login and logouts through the RADIUS server.
  - **Accounting Port:** The port number used by the RADIUS server for accounting purposes. Specify a port number or use the default, 1813.
  - **Accounting Interim Update Interval:** The system will update accounting information to the RADIUS server every interval period.
- **WPA-PSK:** WPA-PSK (Wi-Fi Protected Access Pre-shared Key) is a pre-shared key authentication method, a special mode of WPA.

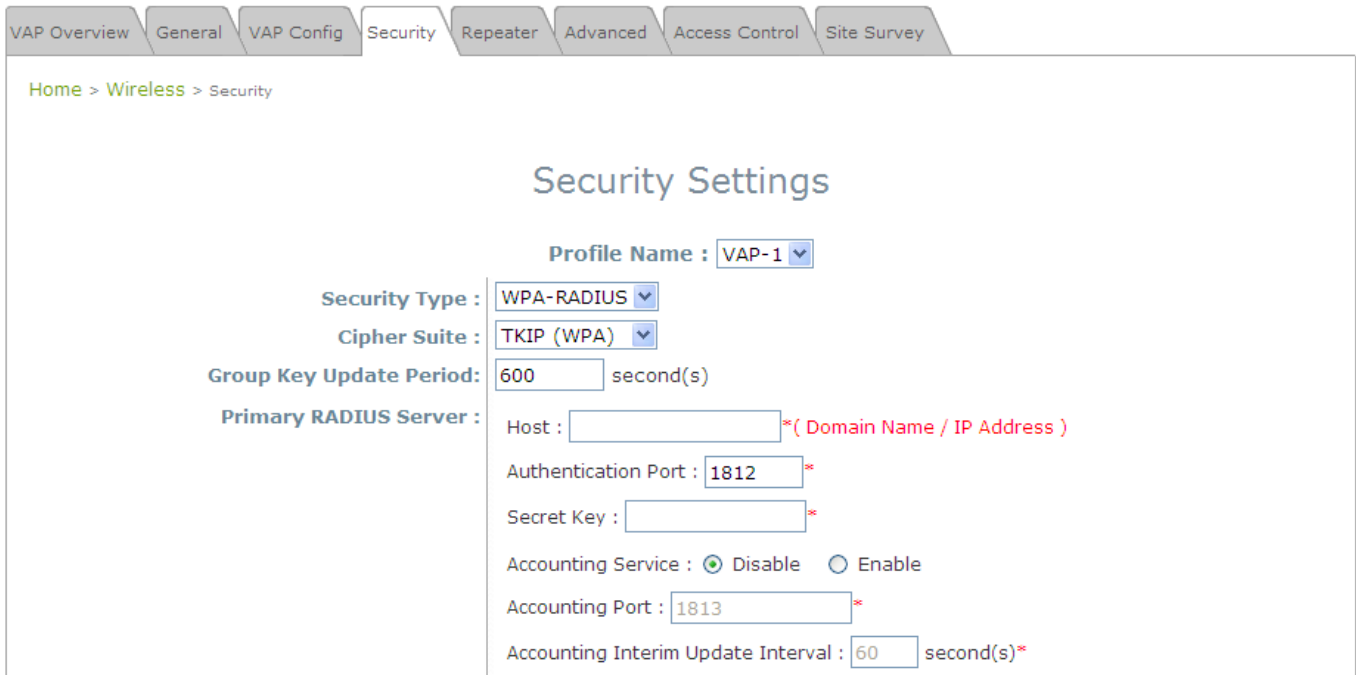
The screenshot shows the 'Security Settings' page for a VAP profile named 'VAP-1'. The configuration is as follows:

- Profile Name:** VAP-1
- Security Type:** WPA-PSK
- Cipher Suite:** TKIP (WPA)
- Pre-shared Key Type:** PSK(Hex)\*( 64 chars ) (selected) and Passphrase\*( 8 - 63 chars )
- Pre-shared Key:** [Empty text box]
- Group Key Update Period:** 600 second(s)

#### Security Settings: WPA-PSK

- **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 seconds.

- **WPA-RADIUS:** If this option is selected, the RADIUS authentication and data encryption will both be enabled.



Home > Wireless > Security

### Security Settings

Profile Name :

Security Type :

Cipher Suite :

Group Key Update Period:  second(s)

Primary RADIUS Server :

Host :  \*( Domain Name / IP Address )

Authentication Port :  \*

Secret Key :  \*

Accounting Service :  Disable  Enable

Accounting Port :  \*

Accounting Interim Update Interval :  second(s) \*

#### Security Settings: WPA-RADIUS

- **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 seconds.
- **RADIUS Server Settings (Primary/Secondary):**
  - **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:** *Enabling* this option allows accounting of login and logouts through the RADIUS server.
  - **Accounting Port:** The port number used by the RADIUS server for accounting purposes. Specify a port number or use the default, 1813.
  - **Accounting Interim Update Interval:** The system will update accounting information to the RADIUS server every interval period.

## 7.2.5 Repeater

To extend wireless network coverage, EAP260 supports 3 options of Repeater type, **None**, **WDS** or **Universal Repeater**; selecting **None** will turn this function off.

### > Universal Repeater

If **Universal Repeater** is selected, please provide the **SSID** of upper-bound AP for uplink connection; **Security Type (None, WEP, or WPA-PSK)** can be configured for this Repeater connection. Please note the security type configured here shall follow upper-bound AP's security settings for intended connection.

VAP Overview General VAP Config Security Repeater Advanced Access Control Site Survey

Home > Wireless > Repeater Config

### Repeater Settings

Repeater Type :   WES

The SSID of Upper-Bound AP : \*

Current wireless channel of the system is set at 1. Repeater connection may fail if the system is set to connect to upper AP with different channels

Security Type :

### **Repeater Settings: Universal Repeater**

- **The SSID of Upper-Bound AP:** Specify the SSID of the upper-bound AP that the system is used to extend that AP's wireless service coverage.
- **Security Type:** None, WEP or WPA-PSK.

**> WDS**

If **WDS** is selected, EAP260 can support up to 4 WDS links to its peer APs. **Security Type (None, WEP, or WPA/PSK)** can be configured to decide which encryption is to be used for WDS connections respectively. Please fill in remote peer's MAC address and click **SAVE** to proceed; if setting revision is necessary, **CLEAR** button can be used to clear the contents in the above WDS connection list.

VAP Overview | General | VAP Config | Security | Repeater | Advanced | Access Control | Site Survey

Home > Wireless > Repeater Config

### Repeater Settings

Repeater Type : WDS  **WES**

WDS Profile : RF Card : WDS Link 1

WDS : Disable

MAC Address :

Security type : None

**Repeater Settings: WDS**

- **WES:** Enable WES.
- **MAC Address:** To input remote peer's MAC address.
- **WDS:** Select **Enable** to enable the respective WDS links; Select **Delete** to remove them.
- **Security Type:** None, WEP, or WPA-PSK.

## 7.2.6 Advanced

The advanced wireless settings for the EAP260'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.

The screenshot shows the 'Advanced Wireless Settings' page for a VAP profile named 'VAP-1'. The page includes a navigation menu at the top with tabs for VAP Overview, General, VAP Config, Security, Repeater, Advanced (selected), Access Control, and Site Survey. Below the navigation, there is a breadcrumb trail: Home > Wireless > Advanced. The main content area is titled 'Advanced Wireless Settings' and contains the following configuration options:

- Profile Name :** VAP-1 (dropdown menu)
- RTS Threshold :** 2346 (input field) \*(1 - 2346)
- Fragment Threshold :** 2346 (input field) \*(256 - 2346)
- DTIM period :** 1 (input field) \*(1 - 15)
- Broadcast SSID :**  Disable  Enable
- Wireless Station Isolation :**  Disable  Enable
- WMM :**  Disable  Enable
- IAPP :**  Disable  Enable
- IGMP Snooping :**  Disable  Enable
- Multicast/Broadcast Rate :** 11M (dropdown menu)

### **Advanced Wireless Settings Page**

- **RTS Threshold:** Enter a value between 1 and 2346. RTS (Request to Send) Threshold determines the packet size at which the system issues a request to send (RTS) before sending the fragment to prevent the hidden node problem. The RTS mechanism will be activated if the data size exceeds the value provided. A lower RTS Threshold setting can be useful in areas where many client devices are associating with EAP260 or in areas where the clients are far apart and can detect only EAP260 but not each other.
- **Fragmentation Threshold:** Enter a value between 256 and 2346. The default is 2346. A packet size larger than this threshold will be fragmented (sent with several pieces instead of one chunk) before transmission. A smaller value results in smaller frames but allows a larger number of frames 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.
- **DTIM Period:** Input the DTIM Interval that is generated within the periodic beacon at a specified frequency. Higher DTIM will let the wireless client save more energy, but the throughput will be lowered.
- **Broadcast SSID:** Disabling this function will prevent the system from broadcasting its SSID. If broadcast of the SSID is disabled, only devices that have the correct SSID can connect to the system.
- **Wireless Station Isolation:** By enabling this function, all stations associated with the system are isolated and 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 that of voice and video. Therefore, WMM decides which data streams are more important and assigns them a higher traffic priority. This option works with WMM-capable clients only.  
**<To receive the benefits of WMM QoS>**
  - The application must support WMM.
  - WMM shall be enabled on EAP260.
  - WMM shall be enabled in the wireless adapter on client's computer.
- **IAPP:** IAPP (Inter Access Point Protocol) is a protocol by which access points share information about the stations 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.
- **IGMP Snooping:** By enabling IGMP snooping, IGMP packets are transferred via the EAP260's network interface and the IP multicast host. Registration information is recorded and sorted into multicast groups. The internal switch can then intelligently forward traffic only to those ports that request multicast traffic. Adversely, without IGMP snooping, multicast traffic is treated like broadcast traffic, with packets forwarded to all ports causing network inefficiencies.
- **Multicast/Broadcast Rate:** Bandwidth configuration for multicast/broadcast packets. If your wireless clients require a larger or smaller bandwidth for sending multicast/ broadcast packets, the administrator can customize the EAP260's multicast/ broadcast bandwidth here.

## 7.2.7 Access Control

On this page, the network administrator can restrict the total number of clients connected to the EAP260, as well as specify particular MAC addresses that can or cannot access the device.

The screenshot shows the 'Access Control Settings' page. At the top, there is a navigation bar with tabs: VAP Overview, General, VAP Config, Security, Repeater, Advanced, Access Control (selected), and Site Survey. Below the navigation bar, the breadcrumb path is 'Home > Wireless > Access Control'. The main heading is 'Access Control Settings'. There are three settings: 'Profile Name' is a dropdown menu set to 'VAP-1'; 'Maximum Number of Clients' is a text input field containing '32' with a red asterisk and the text '\* ( Range: 1 ~ 128 per system )' to its right; and 'Access Control Type' is a dropdown menu set to 'Disable Access Control'.

### *Access Control Settings Page*

- **Maximum Number of Clients**

EAP260 supports various methods of authenticating clients for wireless LAN access. 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, when the number of stations is set to 20, only 20 stations are allowed to connect to the specified VAP.

- **Access Control Type**

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

- **Disable Access Control:** When **Disable** is selected, there is no restriction for client devices to access the system.
- **MAC ACL Allow List:** When selecting **MAC ACL Allow List**, only the client devices (identified by their MAC addresses) listed in the Allow List (“allowed MAC addresses”) are granted with access to the system. The administrator can temporarily block any allowed MAC address by checking **Disable**, until the administrator re-Enables the listed MAC.

VAP Overview | General | VAP Config | Security | Repeater | Advanced | Access Control | Site Survey

Home > Wireless > Access Control

### Access Control Settings

Profile Name : VAP-1

Maximum Number of Clients : 32 \*( Range: 1 ~ 128 per system )

Access Control Type : MAC ACL Allow List

No.	MAC Address	State
1	<input type="text"/>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
2	<input type="text"/>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

#### MAC Allow List

- ▶▶ **Note:** An empty Allow List means that there is no allowed MAC address. Make sure at least the MAC of the management system is included (e.g. network administrator's computer)



- **MAC ACL Deny List:** When selecting **MAC ACL Deny List**, all client devices are granted with access to the system except those listed in the Deny List (“denied MAC addresses”). The administrator can allow any denied MAC address to connect to the system temporarily by checking **Disable**.

VAP Overview | General | VAP Config | Security | Repeater | Advanced | Access Control | Site Survey

Home > Wireless > Access Control

### Access Control Settings

Profile Name : VAP-1 ▼

Maximum Number of Clients :  \*( Range: 1 ~ 128 per system )

Access Control Type : MAC ACL Deny List ▼

No.	MAC Address	State
1	<input type="text"/>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
2	<input type="text"/>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

**Deny List**

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

VAP Overview | General | VAP Config | Security | Repeater | Advanced | Access Control | Site Survey

Home > Wireless > Access Control

### Access Control Settings

Profile Name : VAP-1 ▼

Maximum Number of Clients : 32 \*( Range: 1 ~ 128 per system )

Access Control Type : RADIUS ACL ▼

Primary RADIUS Server :

Note!!! These settings will also apply to security settings which use RADIUS Server for this VAP.

Host:  \*( Domain Name / IP Address )

Authentication Port: 1812 \*( 1 - 65535 )

Secret Key:  \*

#### **RADIUS ACL**

## 7.2.8 Site Survey

Site Survey is a useful tool to provide information about the surrounding wireless environment; available APs are shown with their respective SSIDs, MAC Addresses, Channels, Rate settings, Signal readings, and Security types. The administrator can click **Setup** or **Connect** to configure the wireless connection according to the mentioned readings when the Repeater Type is set as Universal Repeater.

SSID	MAC Address	Channel	Rate	Signal	Security	Setup / Connect
00-1	00:1F:D4:00:2E:56	1	54	43	None	<input type="button" value="Connect"/>
00-5	08:1F:D4:00:2E:56	1	54	49	None	<input type="button" value="Connect"/>

**Site Survey Page**

If **Universal Repeater** function is enabled, the system can scan and display all surrounding available access points (APs). The administrator can then select an AP for connection to extend its wireless service coverage on this page.

- **SSID:** The SSID (Service Set ID) of the AP found in this system's coverage area.
- **MAC Address:** The MAC address of the respective AP.
- **Channel:** The channel number currently used by the respective AP or repeater.
- **Rate:** The transmitting rate of the respective AP.
- **Signal:** The encryption type used by the respective AP.
- **Setup / Connect:**
  - **Connect:** Click **Connect** to associate with the respective AP directly; no further configuration is required.

Cip-893	00:0E:2E:7C:AA:6E	1	54	4	None	<input type="button" value="Connect"/>
---------	-------------------	---	----	---	------	--

- **Setup:** Click **Setup** to configure security settings for associating with the respective AP.
  - **WEP:** Click **Setup** to configure the WEP setting for associating with the target AP.

Cip-wep	00:11:A3:08:09:56	6	54	40	WEP	<input type="button" value="Setup"/>
---------	-------------------	---	----	----	-----	--------------------------------------

The following configuration box will then appear at the bottom of the screen. Security settings configured here must be the same as the target AP.

Note!!! If you set WEP security for Universal Repeater the security of AP will also change to WEP and use the same settings.

WEP Key Type :  Open  Shared  Auto

WEP Key Length :  64 bits  128 bits  152 bits

WEP Key Format :  ASCII  Hex

WEP Key Index : 1 ▾

WEP Keys :

1

2

3

4

- **WPA-PSK:** Click **Setup** to configure the WPA-PSK setting for associating with the target AP.

Cip-psk	0A:1F:D4:39:10:74	11	54	52	WPA-PSK	<input type="button" value="Setup"/>
---------	-------------------	----	----	----	---------	--------------------------------------

The following configuration box will then appear at the bottom of the screen. Information provided here must be consistent with the security settings of the target AP.

Pre-shared Cipher : TKIP ▾

Pre-shared Key Type :  PSK(Hex) \*( 64 chars )

Passphrase \*( 8 - 63 chars )

Pre-shared Key :

## 7.3 Firewall

The system provides an added security feature, Layer2 Firewall, in addition to the typical AP security. Layer2 Firewall offers a firewall function that is tailored specifically for Layer2 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. This section provides information in the following functions: **Firewall Settings**, **Service** and **Advanced Firewall Settings**.

### 7.3.1 Firewall List

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

The screenshot shows the 'Layer 2 Firewall Settings' page. At the top, there are tabs for 'Firewall List', 'Service', and 'Advanced'. Below the tabs, there is a breadcrumb trail: 'Home > Firewall > Firewall List'. The main heading is 'Layer 2 Firewall Settings'. Below the heading, there is a section for 'Enable Layer 2 Firewall' with radio buttons for 'Disable' and 'Enable' (which is selected). Below this is a table with 7 columns: No., State, Action, Name, EtherType, Remark, and Setting. The table contains 3 rows of data.

No.	State	Action	Name	EtherType	Remark	Setting
1	<input type="checkbox"/>	DROP	CDP	IEEE_8023		Del Ed In Mv
2	<input type="checkbox"/>	DROP	STP	IEEE_8023		Del Ed In Mv
3	<input type="checkbox"/>	DROP	GARP	IEEE_8023		Del Ed In Mv

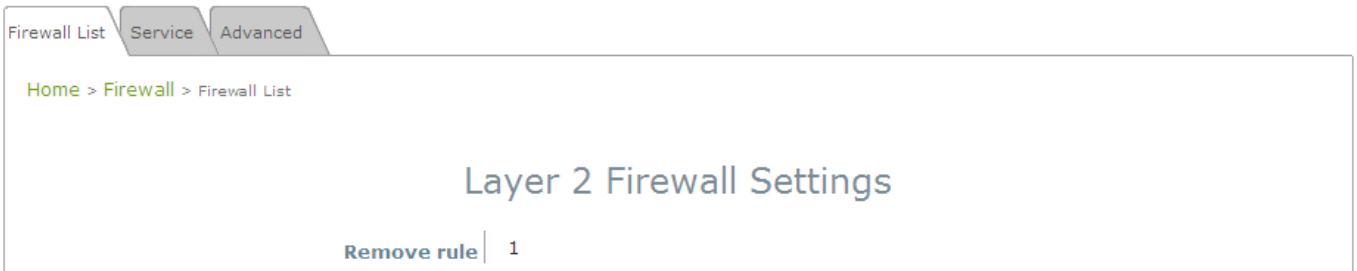
**Firewall List Page**

From the overview table, each rule is designated with the following field;

- **No.:** The numbering will decide the priority for the system to carry out the available firewall rules in the tables.
- **State:** The check marks will enable the respective rules.
- **Action:** **DROP** denotes a block rule; **ACCEPT** denotes a pass rule.
- **Name:** Shows the name of the rule.
- **EtherType:** Denotes the type of traffics subject to this rule.
- **Remark:** 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 the **SAVE** button is clicked and system is rebooted, 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 from 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 traffic subjected to this rule.
- **Interface:** It indicates inbound/outbound direction with desired interfaces.
- **Service** (when EtherType is **IPv4**): Select the available upper layer protocols/services from the drop-down list.
- **DSAP/SSAP** (when EtherType is **IEEE 802.3**): 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 traffic.
- **VLAN ID** (when EtherType is **802.1 Q**): The VLAN ID is provided to associate with certain VLAN-tagging traffic.
- **Priority** (when EtherType is **802.1 Q**): It denotes the priority level with associated VLAN traffic.
- **Encapsulated Type** (when EtherType is **802.1 Q**): It can be used to indicate the type of encapsulated traffic.
- **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 rule is provided; please click **SAVE** and **Reboot** system to let the firewall rule take effect.

### >>To insert a specific rule,

**In** the **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.

Firewall List
Service
Advanced

[Home](#) > [Firewall List](#) > [Rule Config](#)

## Layer 2 Firewall Configuration

**Rule ID :** 1

**Rule name :**

**EtherType :** IPv4

**Interface :**  From  To VAP1

**Service :** ALL

**Source :** MAC Address:  Mask:   
 IP Address :  Mask: 0.0.0.0 /0

**Destination :** MAC Address:  Mask:   
 IP Address :  Mask: 0.0.0.0 /0

**Action :**  Block  Pass

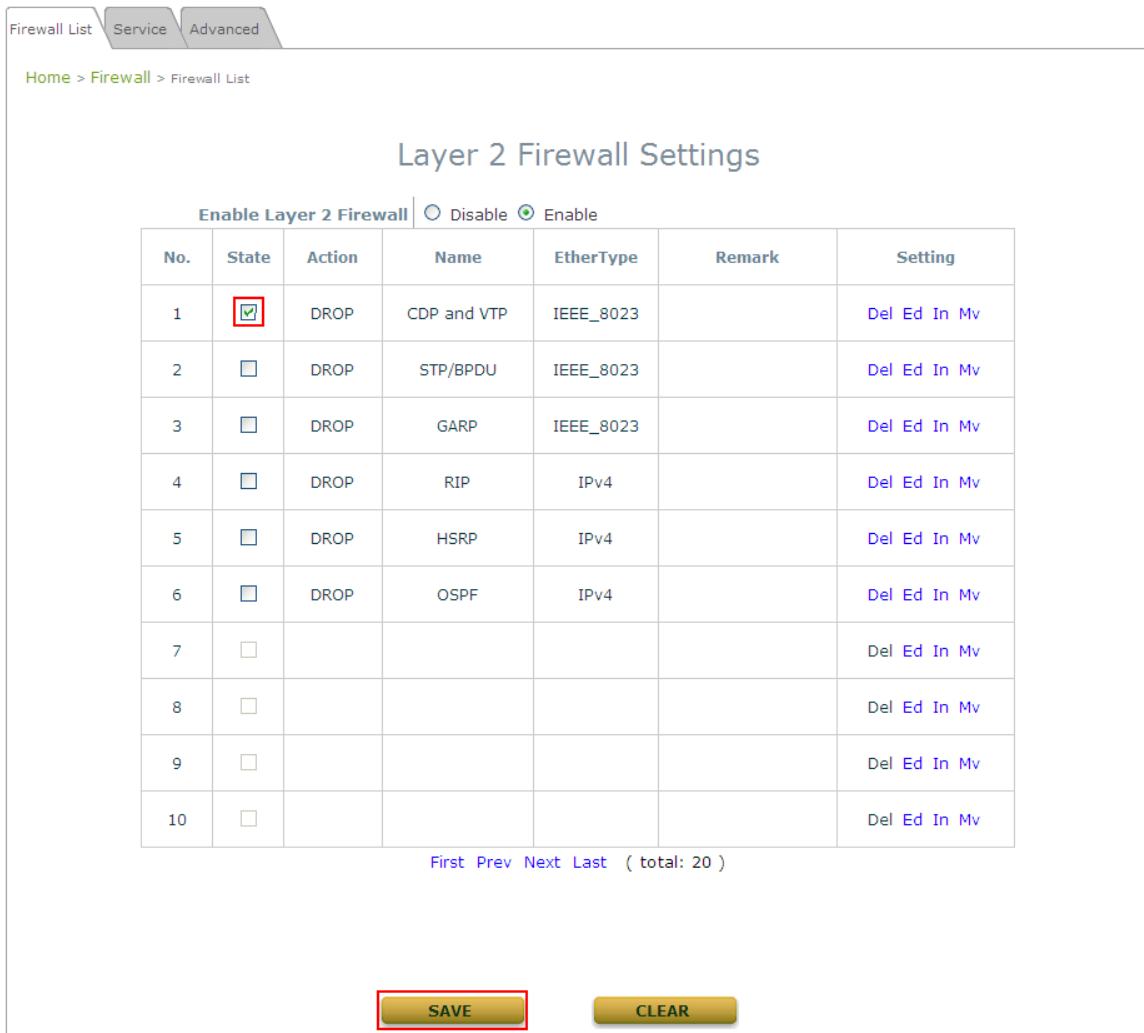
**Remark :**

>>To move a specific rule,

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



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





## 7.3.2 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).

EAP260 provides a list of rules to block or pass traffic of layer-3 or above protocols. These services are available to choose from a drop-down list of layer2 firewall rule edit page with Ether Type IPv4. The first 28 entries are default services and the administrator can add/delete any extra desired 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.

Firewall List
Service
Advanced

[Home](#) > [Firewall](#) > [Service Config](#)

### Firewall Service

No.	Name	Description	Delete
1	ALL	ALL	<input type="checkbox"/>
2	ALL TCP	TCP, Source Port: 0~65535, Destination Port: 0~65535	<input type="checkbox"/>
3	ALL UDP	UDP, Source Port: 0~65535, Destination Port: 0~65535	<input type="checkbox"/>
4	ALL ICMP	ICMP	<input type="checkbox"/>
5	FTP	TCP/UDP, Destination Port: 20~21	<input type="checkbox"/>
6	HTTP	TCP/UDP, Destination Port: 80	<input type="checkbox"/>
7	HTTPS	TCP/UDP, Destination Port: 443	<input type="checkbox"/>
8	POP3	TCP, Destination Port: 110	<input type="checkbox"/>
9	SMTP	TCP, Destination Port: 25	<input type="checkbox"/>
10	DHCP	UDP, Destination Port: 67~68	<input type="checkbox"/>

[First](#) [Prev](#) [Next](#) [Last](#) ( total: 28 )

### Firewall Service Page

### 7.3.3 Advanced

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

Firewall List Service Advanced

Home > Firewall > Advanced

## Advanced Firewall Settings

**Trust Interface :**  VAP1  VAP2  VAP3  VAP4  VAP5  VAP6  VAP7  VAP8

**DHCP Snooping :**  Disable  Enable

**ARP Inspection :**  Disable  Enable

Proxy ARP :  Disable  Enable

Force DHCP :  Disable  Enable

Trust List Broadcast :  Disable  Enable

Static Trust List :  Disable  Enable

- **Trust Interface:** Each VAP 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 rouge DHCP server.
- **ARP Inspection:** When enabled, ARP packets will be validated against ARP spoofing.
  - **Proxy ARP** option when enabled, AP will reply ARP requests on behalf of downlink stations. The ARP table maintained by AP will be used as a look up table upon receipt of ARP request from AP uplink. Adversely, without Proxy ARP, ARP request is broadcasted down into the AP's wireless network causing network inefficiencies.
  - **Force DHCP** option when enabled, the AP only learns MAC/IP pair information through DHCP packets. Since devices configured with static IP address does not send DHCP traffic, any clients with static IP address will be blocked from internet access unless its MAC/IP pair is listed and enabled on the **Static Trust List**.
  - **Trust List Broadcast** can be enabled to let other APs (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 of devices that are trusted to issue ARP request. Other network nodes can still send their ARP requests; however, if their IP appears on 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.



## 7.4 Utilities

The administrator can maintain the system on this page: **Change Password, Backup & Restore, System Upgrade, Reboot, Upload Certificate, WAPI Certificate.**

### 7.4.1 Change Password

To protect the Web Management Interface from unauthorized access, it is highly recommended to change the administrator's password to a secure password. Only alpha-numeric characters are allowed, and it is also recommended to make use of a combination of both numeric and alphabetic characters.

The screenshot shows the 'Change Password' page in a web management interface. At the top, there is a navigation bar with tabs for 'Change Password', 'Backup & Restore', 'System Upgrade', 'Reboot', 'Upload Certificate', and 'WAPI Certificate'. Below the navigation bar, the breadcrumb path is 'Home > Utilities > Change Password'. The main heading is 'Change Password'. The form contains the following fields:

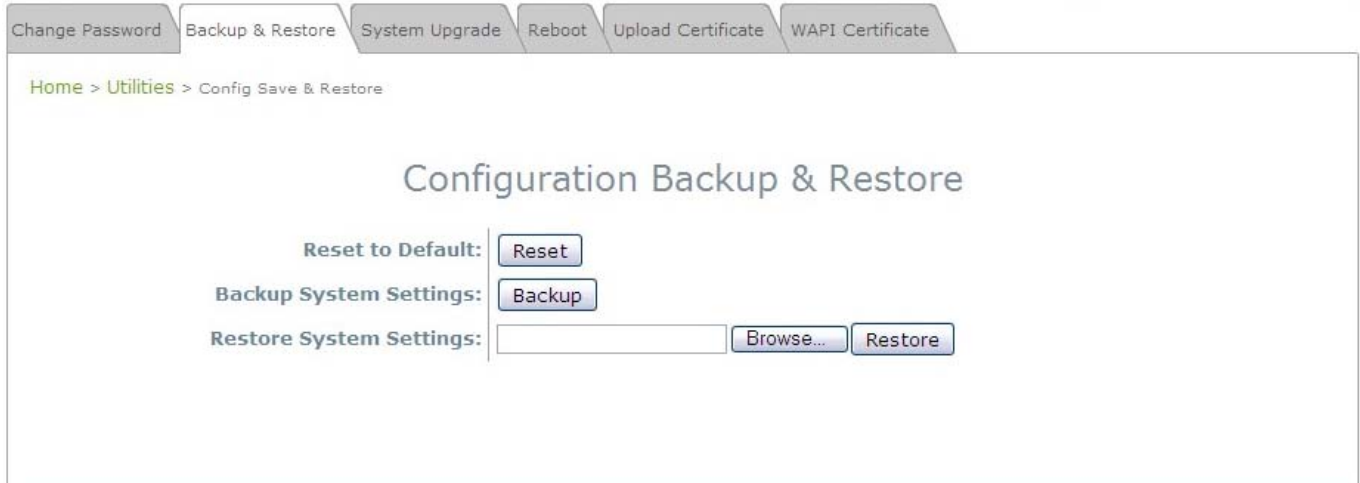
- Name :** admin
- Old Password :**
- New Password :**  \*up to 32 characters
- Re-enter New Password :**

#### **Change Password Page**

The administrator can change password on this page. Enter the original password (“**admin**”) and new password, and then re-enter the new password in the **Re-enter New Password** field. Click **SAVE** to save the new password.

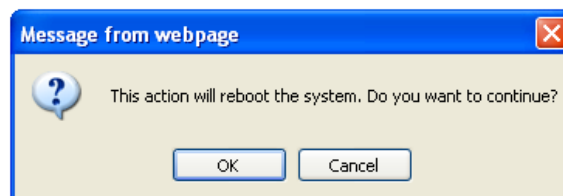
## 7.4.2 Backup & Restore

This function is used to backup and restore the EAP260 settings. The EAP260 can also be restored to factory defaults 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).



**Backup & Restore Page**

- **Reset to Default:**
  - Click **Reset** to load the factory default settings of EAP260. A pop-up Page will appear to re-confirm the request to reboot the system. Click **OK** to proceed, or click **Cancel** to cancel the reboot request.



**Reboot Confirmation Prompt**

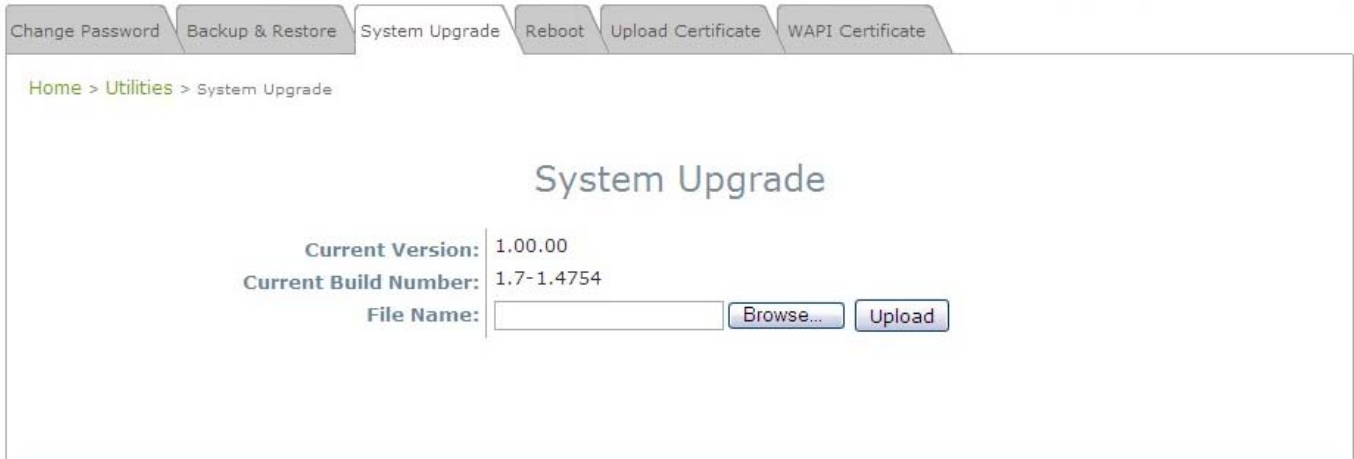
- A warning message as displayed below will appear during the reboot period. The system power must be kept on before the completion of the reboot process.
- The **System Overview** page will appear upon reboot completion.
- **Backup System Settings:** Click **Backup** to save the current system settings to a local disk such as the hard disk drive (HDD) of a local computer or a compact disc (CD).
- **Restore System 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.



*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 the EAP260.*

### 7.4.3 System Upgrade

The EAP260 provides a web firmware upload / upgrade feature. The administrator can download the latest firmware from the website and save it on the administrator's PC. To upgrade the system firmware, click **Browse** to choose the new firmware file you downloaded onto your PC and then click **Upload** to execute the process. There will be a prompt confirmation message to notify the administrator to restart the system after a successful firmware upgrade. Please restart the system after upgrading the firmware.



The screenshot shows the 'System Upgrade' page in the EAP260 web interface. At the top, there is a navigation bar with tabs for 'Change Password', 'Backup & Restore', 'System Upgrade', 'Reboot', 'Upload Certificate', and 'WAPI Certificate'. Below the navigation bar, the breadcrumb path is 'Home > Utilities > System Upgrade'. The main heading is 'System Upgrade'. The page displays the current firmware version as '1.00.00' and the current build number as '1.7-1.4754'. There is a 'File Name:' label followed by an empty text input field, a 'Browse...' button, and an 'Upload' button.

#### ***System Upgrade Page***

- 
- ▶▶ **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 the loss of 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 permanently damage the system.
-

## 7.4.4 Reboot

This function allows the administrator to restart the EAP260 safely. The process takes approximately three minutes. Click **Reboot** to restart the system. Please wait for the blinking timer to complete its countdown before accessing the system's Web Management Interface again. The System Overview page will appear after a successful reboot.

Occasionally, it is necessary to reboot the EAP260 to ensure that parameter changes are submitted.



**Reboot Page**

## 7.4.5 Upload Certificate

This function is used to configure a valid certificate for security validation required in CAPWAP..

Change Password Backup & Restore System Upgrade Reboot Upload Certificate WAPI Certificate

Home > Utilities > Upload Certificate

### Upload Certificate

Upload Private Key	
File Name	<input type="text"/> Browse...

Upload Certificate	
File Name	<input type="text"/> Browse...

Upload Trusted Certificate	
File Name	<input type="text"/> Browse...

Use Default Certificate

- **Upload Certificate:** It provides flexibility to support customer's own Certificate, Private Key, or Trusted Certificate for a means of security verification for CAPWAP or other security needs to ensure the authenticity of this AP to other network entities.
- **Use Default Certificate:** Click **Use Default Certificate** to use the default certificate and key.



## 7.4.6 WAPI Certificate

This function is used to set up a valid WAPI Certificate for identity validation with other WAPI capable network entities.

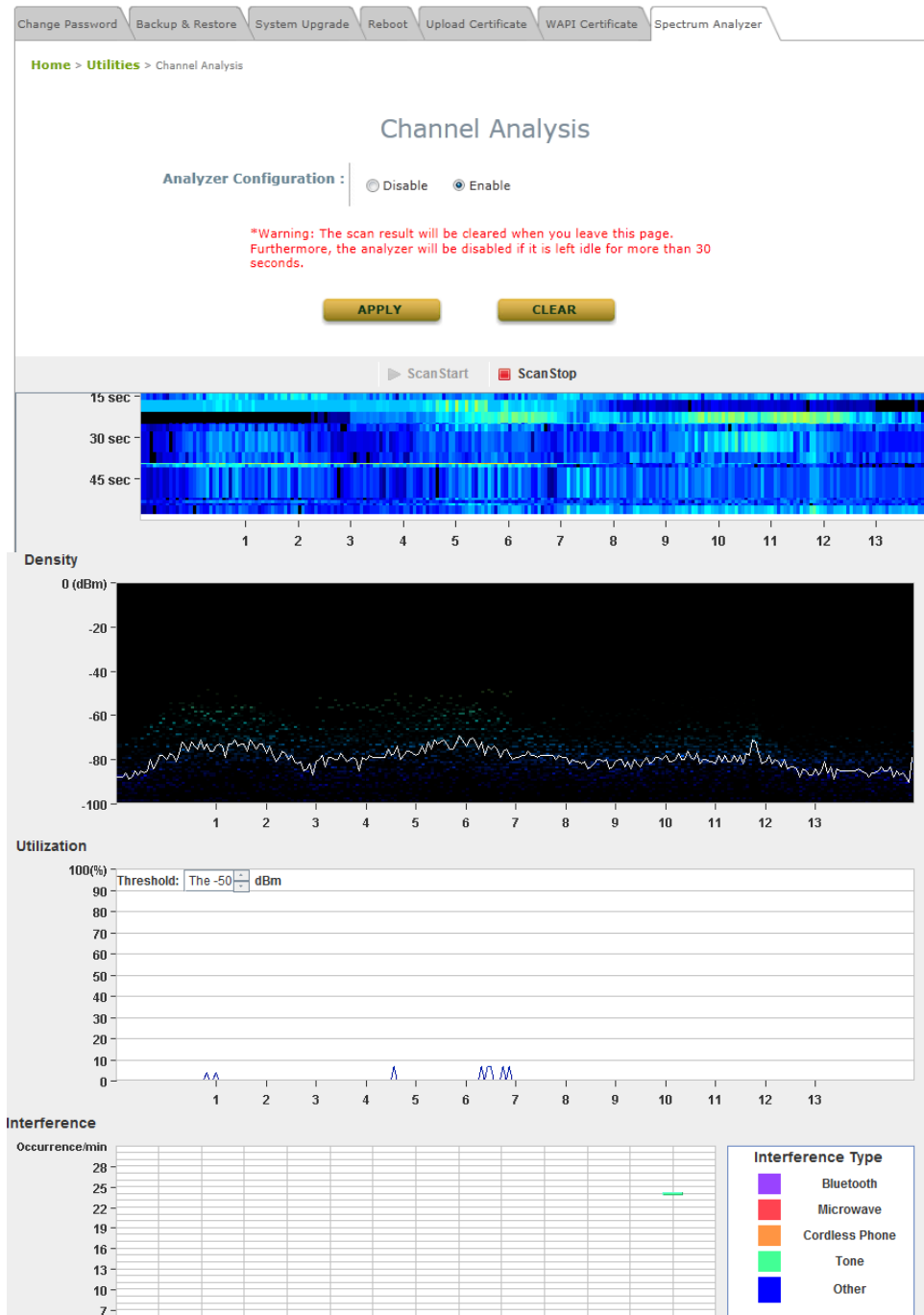
The screenshot shows a web interface for configuring WAPI certificates. At the top, there is a navigation bar with tabs: Change Password, Backup & Restore, System Upgrade, Reboot, Upload Certificate, and WAPI Certificate. Below the navigation bar, the breadcrumb path is Home > Utilities > WAPI Certificate. The main heading is WAPI Certificate. There are two sections for uploading certificates:

- Upload ASU Certificate:** A section with a header bar. Below it, there is a table with one row. The first column is labeled "File Name" and contains an empty text input field. The second column contains a "Browse..." button.
- Upload AE Certificate/Private Key:** A section with a header bar. Below it, there is a table with one row. The first column is labeled "File Name" and contains an empty text input field. The second column contains a "Browse..." button.

- **Upload ASU Certificate:** It provides flexibility to support customer's own ASU Certificate for a means of security verification in order to ensure the authenticity of this AP to other network entities.
- **Upload AE Certificate/Private Key:** It provides flexibility to support customer's own AE Certificate or Private Key for a means of security verification in order to ensure the authenticity of this AP to other network entities.

### 7.4.7 Channel Analysis

This utility Channel Analysis helps an administrator scan the current state of the 2.4GHz wireless environment that he/she is in. Before using it, ensure that the browser to use has installed Java Runtime Environment. When the function is in operation, the AP will fully dedicate to this scanning action. That means, users will not be able to associate to the AP and current online users will be logged off during the process. Thus it is highly recommended that admins turn off the function immediately after the scan.



» Note:

1. The function will be automatically turned off whenever the operator leaves the page for 30 seconds.
2. There can be only one person using this function at the same time.

## 7.5 Status

This page is used to view the current condition and state of the system and it includes the following functions: **Overview**, **Associated Clients**, **Repeater** and **Event Log**.

### 7.5.1 Overview

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

Overview
Associated Clients
Repeater
Event Log

[Home](#) > [Status](#) > System Overview

### System Overview

**System**

System Name	Enterprise Access Poin...
Firmware Ve...	1.00.00
Build Number	1.7-1.4754
Location	
Site	EN-A
Device Time	1970/01/01 10:32:47
System Up Ti...	0 days, 2:32:47

**Radio Status**

MAC Address	00:02:6B:06:4D:2F
Band	802.11g+n
Channel	1
TX Power	Highest

**LAN Interface**

MAC Address	00:02:6B:06:4D:2F
IP Address	10.0.5.200
Subnet Mask	255.255.0.0
Gateway	10.0.1.1

**AP Status**

Profile Name	BSSID	ESSID	Security Type	Online Clients	Jun
VA...	00:02:6B:06:4...	EAP260-1	None	0	

**CAPWAP**

Status Disabled

**IPv6**

Status Disabled

**System Overview Page**

**Table 3 Status Page's Organizational Layout**

Item		Description
System	System Name	The system name of the EAP260.
	Firmware Version	The current firmware version of the EAP260
	Build Number	The current firmware build number of the EAP260
	Location	The location of the EAP260.
	Site	The site of the EAP260
	Device Time	The system time of the EAP260.
	System Up Time	The time that the system has been rebooted in operation.
LAN Interface	MAC Address	The MAC address of the LAN Interface.
	IP Address	The IP address of the LAN Interface.
	Subnet Mask	The Subnet Mask of the LAN Interface.
	Gateway	The Gateway of the LAN Interface.
Radio Status	MAC Address	The MAC address of the RF Card.
	Band	The RF band in use.
	Channel	The channel specified.
	Tx Power	Transmit Power level of RF card.
AP Status	Profile Name	The profile name of AP.
	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.
	Tunnel	The status of the used Tunnel.
IPv6	Status	Enabled/ Disabled
CAPWAP	Status	Enabled/ Disabled

## 7.5.2 Associated Clients

The administrator can remotely oversee the status of all associated clients on this page. When a low SNR is found here, the administrator can tune the corresponding parameters or investigate the settings of associated clients to improve network communication performance.

The screenshot shows the 'Associated Client Status' page. At the top, there are navigation tabs: 'Overview', 'Associated Clients' (selected), 'Repeater', and 'Event Log'. Below the tabs is a breadcrumb trail: 'Home > Status > Wireless Clients'. The main heading is 'Associated Client Status'. Underneath, there is a section titled 'Client List' which contains a table with the following columns: 'Associated VAP', 'ESSID', 'MAC Address', 'SNR (dB)', 'Idle Time (secs)', and 'Disconnect'.

### **Associated Client Status Page**

- **Associated VAP:** The name of a VAP (Virtual Access Point) that the client is associated with.
- **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 for; the time unit is in seconds.
- **Disconnect:** Upon clicking **Kick**, the client will be disconnected from the system.


### 7.5.3 Repeater





The administrator can review detailed information of the repeater function on this page. Information of WDS/repeater's status, traffic statistics, encryption and other details are provided.

Overview Associated Clients Repeater Event Log

Home > Status > Repeater Information

### Repeater Information

 **WDS Link Status**

Item	Status	MAC Address	RSSI	TX Rate	TX Count	TX Error	EncryptionTun	
1	Disabl...		N/A	N/A	N/A	N/A	N/A	
2	Disabl...		N/A	N/A	N/A	N/A	N/A	
3	Disabl...		N/A	N/A	N/A	N/A	N/A	
4	Disabl...		N/A	N/A	N/A	N/A	N/A	

*Repeater Status Page*

## 7.5.4 Event Log

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



### *Event Log Page*

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

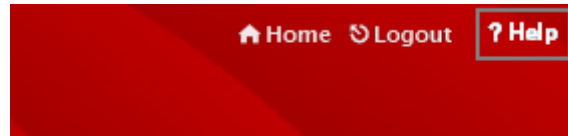
- **Date / Time:** The time & date when the event happened
- **Hostname:** Indicates which host recorded this event. Note that all events on this page are local events, so the hostname in this field is always the same. In remote SYSLOG service however, this field will help the administrator identify which event is from this EAP260.
- **Process name:** Indicate the event generated by the running instance.
- **Description:** Description of the event.

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

## 7.6 Online Help

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

Click **Help** for the **Online Help** window, and then click the hyperlink of the relevant information needed.



*Online Help Corner*