

User's Manual

EAP200 v1.00

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.....	4
1.1 Preface.....	4
1.2 Document Conventions.....	4
1.3 Package Content	5
2. System Overview and Getting Started	6
2.1 Introduction of 4ipnet EAP200.....	6
2.2 Deployment Topology.....	7
2.3 Hardware Description	8
2.4 Hardware Installation.....	10
2.5 Access Web Management Interface.....	11
3. Connect your AP to your Network.....	15
4. Adding Virtual Access Points.....	21
5. Secure Your AP	23
6. Create a WDS Bridge between two APs	32
7. Web Management Interface Configuration.....	34
7.1 System.....	36
7.1.1 General	36
7.1.2 Network Interface	38
7.1.3 Management.....	39
7.2 AP.....	41
7.2.1 VAP Overview.....	41
7.2.2 General	44
7.2.3 VAP Configuration	46
7.2.4 Security.....	47
7.2.5 Repeater	51
7.2.6 Advanced.....	52
7.2.7 Access Control.....	54
7.2.8 Site Survey	58
7.3 Firewall.....	60
7.3.1 Firewall List.....	60
7.3.2 Service	65
7.3.3 Advanced.....	66
7.4 Utilities.....	67
7.4.1 Change Password.....	67
7.4.2 Backup & Restore	68
7.4.3 System Upgrade.....	69




7.4.4 Reboot	70
7.5 Status.....	71
7.5.1 Overview	71
7.5.2 Associated Clients.....	73
7.5.3 Repeater	74
7.5.4 Event Log	75
7.6 Online Help.....	76

1. Before You Start

1.1 Preface

This manual is intended for system integrators, field engineers, and network administrators to set up 4ipnet's EAP200 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.
» Note:	Contains related information that corresponds to a topic.
	Indicates that clicking this button will save the changes you made, but you must reboot the system upon the completion of all configuration settings for the changes to take effect.
	Indicates that clicking this button will clear what you have set before the settings are applied.

1.3 Package Content

The standard package of EAP200 includes:

- | | |
|---------------------------------------|----|
| • 4ipnet EAP200 | x1 |
| • Quick Installation Guide (QIG) | x1 |
| • CD-ROM (with User's Manual and QIG) | x1 |
| • Console Cable | x1 |
| • Ethernet Cable | x1 |
| • Power Adapter (DC 12V) | x1 |
| • Antenna | x2 |
| • Screw Pack | x1 |
| • Ground Cable | x1 |



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 EAP200

The **4ipnet EAP200 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. EAP200 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 EAP200s for forming wider wireless network coverage.

EAP200 also features multiple ESSIDs with VLAN tags and multiple Virtual APs, great for enterprise applications, such as separating the traffics of different departments using different ESSIDs. The PoE LAN port can receive power from Power over Ethernet (PoE) sourcing device. Its metal case is IP50 anti-dust compliant, which means that EAP200 is well suited to WLAN deployment in industrial environments.

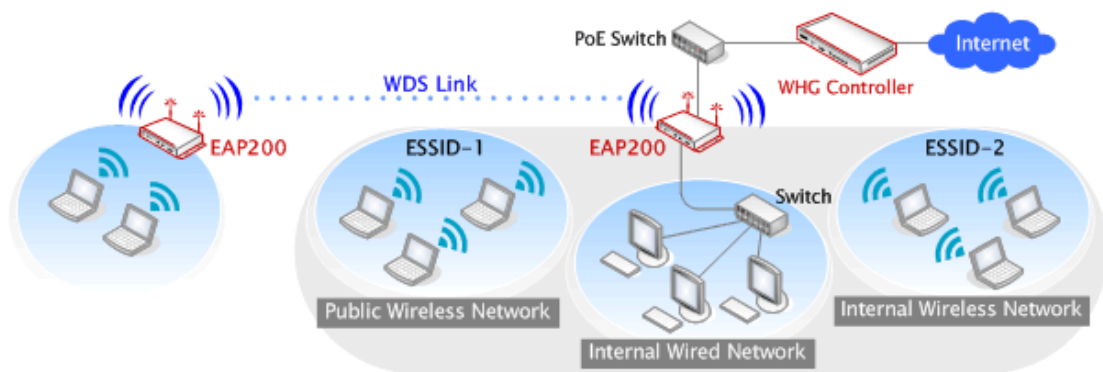


Figure 1 *Wired and Wireless Network Layout with EAP200s*

2.2 Deployment Topology

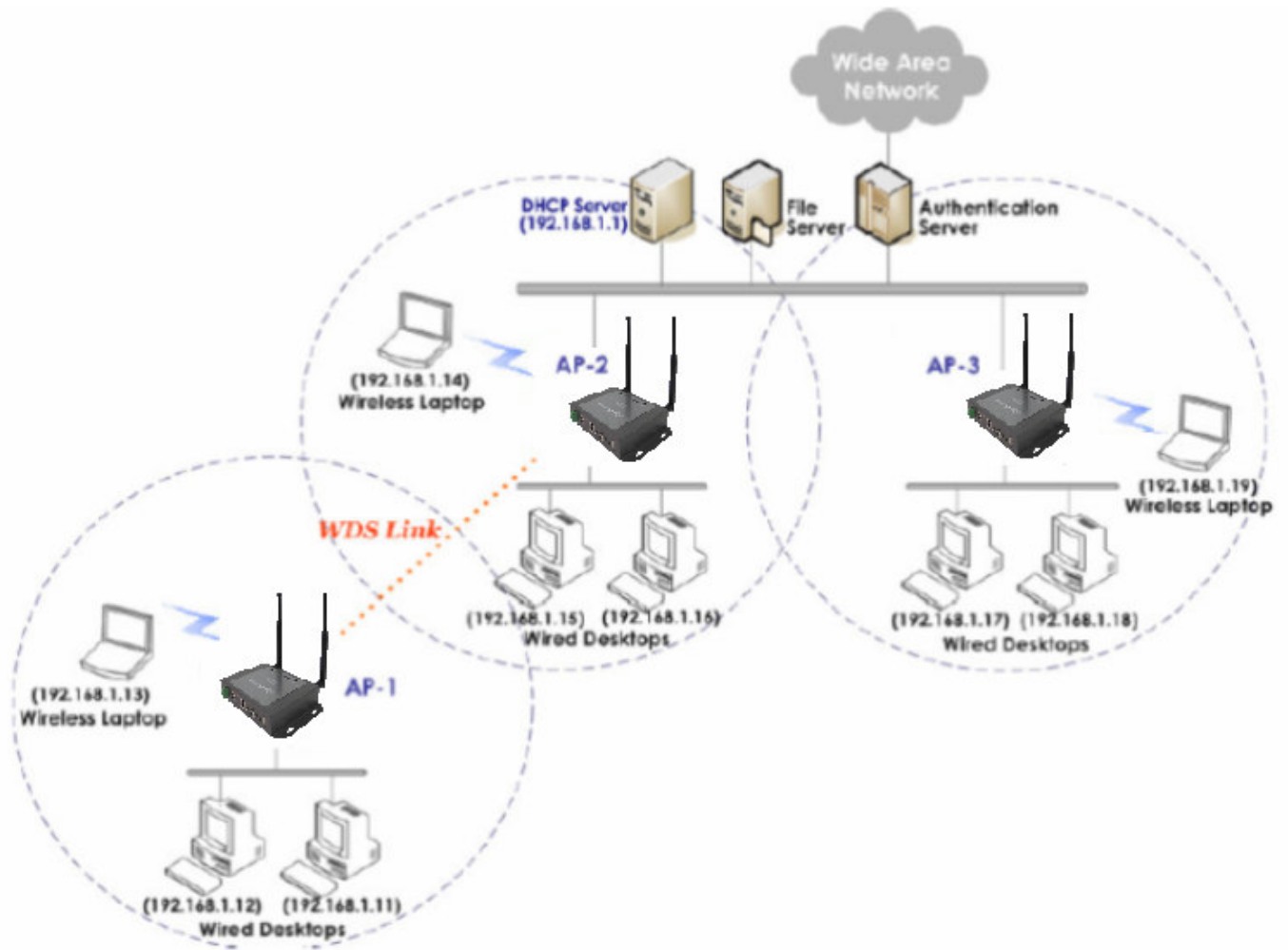


Figure 2 Common Network Layout with EAP200s

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

- Three EAP200 systems construct a network comprising of wired and wireless segments
- **AP-2** plays the role of a wireless bridge.
- All devices share the same DHCP server **192.168.1.1**.

2.3 Hardware Description

This section depicts the hardware information including all panel description.

Connector Panel

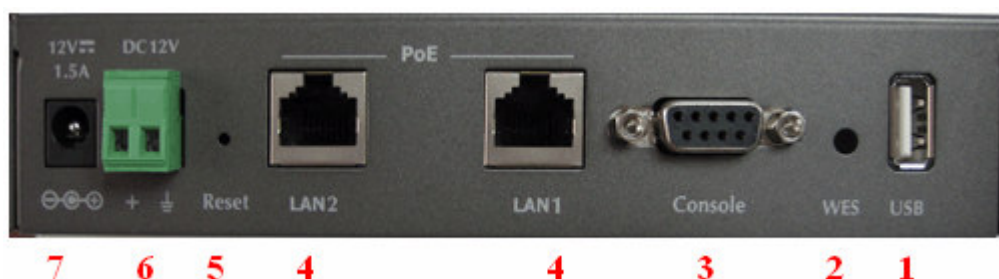


Figure 3 EAP200 Connector Panel

1	USB	Disabled for future usage only.
2	WES	Press to start running WES process.
3	Console	Attach the serial cable here.
4	LAN1 / LAN2	Attach the Ethernet cable here for connection with wired local networks.
5	Reset	Press and hold for more than 10 seconds to reset to factory default configurations.
6	DC 12V	Attach the power socket here.
7	12V 1.5A	Attach the power adapter here.

Antenna Panel



Figure 4 EAP200 Antenna Panel

Antenna Connector:	Attach the antennas here. The system supports one RF interface with two SMA connectors.
---------------------------	---

LED Panel

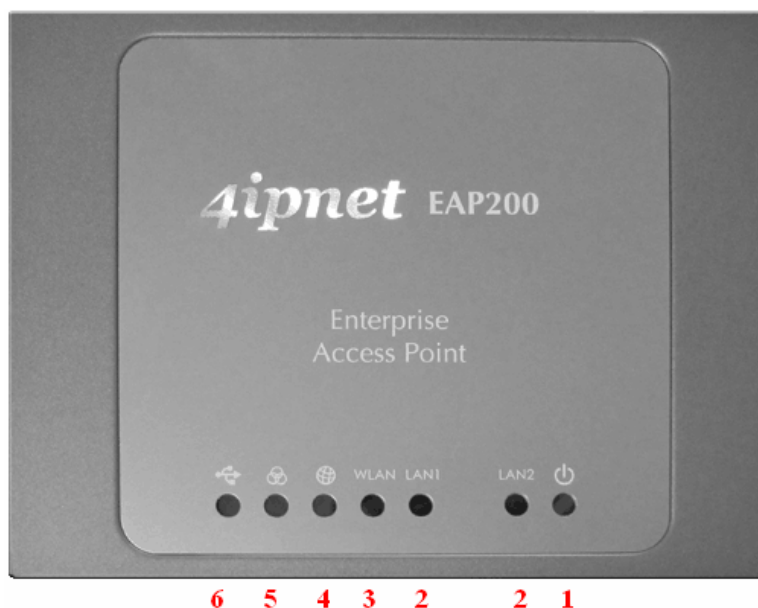


Figure 5 EAP200 LED Panel

1	Power LED	LED ON indicates power on; OFF indicates power off.		
2	LAN LED	LED ON indicates LAN cable connected; OFF indicates no connection; BLINKING indicates transmitting data.		
3	WLAN LED	LED ON indicates wireless ready.		
4	WDS LED	LED ON indicates WDS ready.		
5	WES LED	To indicate WES status.		
			Master	Slave
		WES Start	LED BLINKING SLOWLY	LED BLINKING QUICKLY
		WES Success	LED ON constantly for 5 seconds	LED ON constantly for 5 seconds
		WES Fail	LED OFF	LED OFF
6	USB LED	Disabled for future usage only.		

2.4 Hardware Installation

Please follow the steps mentioned below to install the hardware of EAP200:

1. Place the EAP200 at the best location.

The best location for EAP200 is usually at the center of your intended wireless network.

2. Connect the EAP200 to your network device.

Connect one end of the Ethernet cable to LAN port of EAP200 and the other end of the cable to a switch, a router, or a hub. EAP200 is then connected to your existing wired LAN network.

3. There are two ways to supply power over to EAP200.

a) Connect the DC power adapter to the EAP200 power socket.

b) EAP200 LAN port is capable of transmitting DC currents. Connect an IEEE 802.3af-compliant PSE device (e.g. a PoE-switch) to the LAN port of EAP200 with the Ethernet cable.

Now, the Hardware Installation is complete.



- *Please only use the power adapter supplied with the EAP200 package. Using a different power adapter may damage this system.*
- *To double verify the wired connection between EAP200 and you switch / router / hub, please also check the LED status indicator of the respective network devices.*

2.5 Access Web Management Interface

4ipnet EAP200 supports web-based configuration. Upon the completion of hardware installation, EAP200 can be configured through a PC by using its web browser such as Mozilla Firefox 2.0 (and higher) or Internet Explorer version 6.0 (and higher).

The default values of the EAP200's LAN IP Address and Subnet Mask are:

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

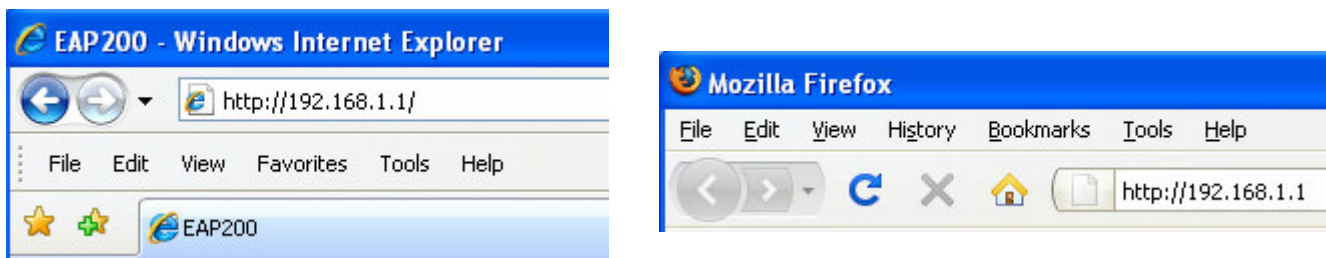


Figure 6 Example of entering EAP200's default IP Address into a web browser

- To access the web management interface (WMI), connect the administrator PC to the LAN port of EAP200 via an Ethernet cable. Then, set a static IP Address on the same subnet mask as the EAP200 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.

- Launch the web browser on your PC and enter the IP Address of the EAP200 (**192.168.1.1**) at the address field, and then press **Enter**. The following Administrator Login Page will then appear. Enter "admin" for both the **Username** and **Password** fields, and then click **Login**.

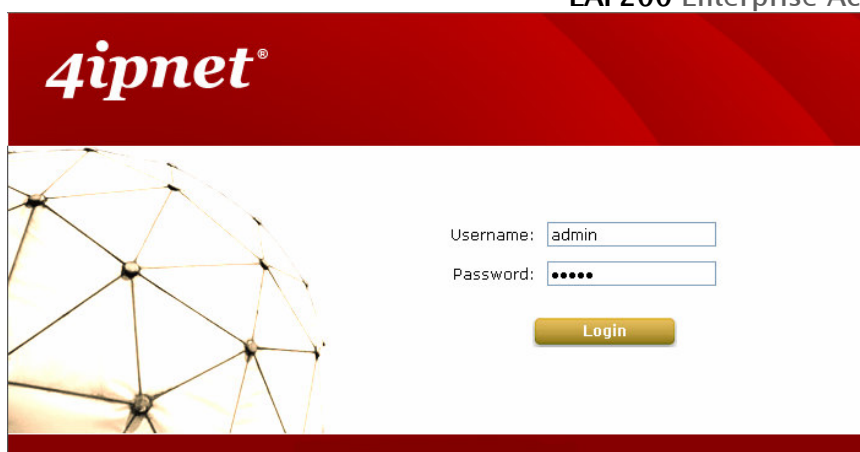


Figure 7 Administrator Login Page

- After a successful login into EAP200, a **System Overview** page of the Web Management Interface (WMI) will appear.

Home > Status > System Overview

System Overview

System

System Name	EAP200
Firmware Version	
Build Number	
Location	
Site	EN-A
Device Time	
System Up Time	0 days, 0:04:49

Radio Status

MAC Address	00:1F:D4:03:22:20
Band	802.11b+g
Channel	6
TX Power	18 dBm

LAN Interface

MAC Address	1E:1F:D4:03:22:20
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
VAP-1	00:1F:D4:03:22:20	EAP200-1	None	0
VAP-2	06:1F:D4:03:22:20	EAP200-2	None	0
VAP-3	0A:1F:D4:03:22:20	EAP200-3	None	0
VAP-4	0E:1F:D4:03:22:20	EAP200-4	None	0
VAP-5	12:1F:D4:03:22:20	EAP200-5	None	0
VAP-6	16:1F:D4:03:22:20	EAP200-6	None	0
VAP-7	1A:1F:D4:03:22:20	EAP200-7	None	0
VAP-8	1E:1F:D4:03:22:20	EAP200-8	None	0

Figure 8 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.



Figure 9 Logout

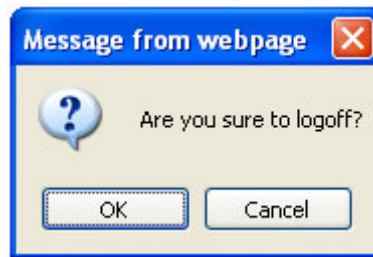
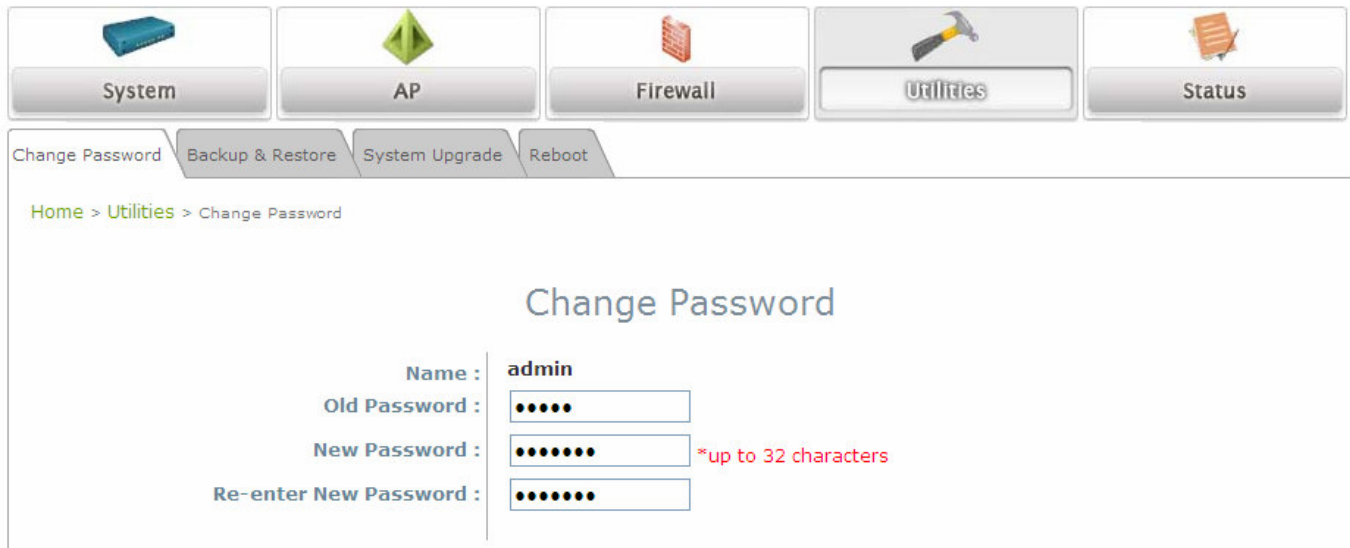


Figure 10 Logout Prompt



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:



Change Password

Home > Utilities > Change Password

Change Password

Name : admin

Old Password :

New Password : *up to 32 characters

Re-enter New Password :

Figure 11 Change Password Page

- Click on the **Utilities** main menu button, and then 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 EAP200 is installed and configured successfully.



- It is strongly recommended to make a backup copy of configuration settings.
- After the EAP200'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 EAP200'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.
- Login via using **Username: admin** and **Password: admin**.

The WMI appears as shown below.

Home > Status > System Overview

System Overview

System

System Name	EAP200
Firmware Version	
Build Number	
Location	
Site	EN-A
Device Time	
System Up Time	0 days, 0:04:49

Radio Status

MAC Address	00:1F:D4:03:22:20
Band	802.11b+g
Channel	6
TX Power	18 dBm

LAN Interface

MAC Address	1E:1F:D4:03:22:20
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
VAP-1	00:1F:D4:03:22:20	EAP200-1	None	0
VAP-2	06:1F:D4:03:22:20	EAP200-2	None	0
VAP-3	0A:1F:D4:03:22:20	EAP200-3	None	0
VAP-4	0E:1F:D4:03:22:20	EAP200-4	None	0
VAP-5	12:1F:D4:03:22:20	EAP200-5	None	0
VAP-6	16:1F:D4:03:22:20	EAP200-6	None	0
VAP-7	1A:1F:D4:03:22:20	EAP200-7	None	0
VAP-8	1E:1F:D4:03:22:20	EAP200-8	None	0

Figure 12 Web Management Interface Main Page (System Overview)

From here, click on the **System** icon to arrive at 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

Name : EAP200 *

Description :

Location :

Time

Device Time : 2000/01/03 05:41:24

Time Zone : (GMT+08:00)Taipei

Time : ☒ Enable NTP ☐ Manually set up

NTP Server 1 : *

NTP Server 2 :

Figure 13 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 finished, click **SAVE**.

Time Zone : (GMT+08:00)Taipei

Time : ☐ Enable NTP ☒ Manually set up

Set Date : Year Month Day

Set Time : Hour Min Sec

Figure 14 Manually Time Setup

The alternative 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 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 :

Figure 15 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.

System AP Firewall Utilities Status

General Network Interface Management

Home > System > Network Interface

Network Settings

Mode : ☒ Static ☐ DHCP Renew

IP Address : 192.168.1.1 *

Netmask : 255.255.255.0 *

Default Gateway : 192.168.1.254 *

Primary DNS Server : 192.168.1.254 *

Alternate DNS Server :

Layer2 STP : ☒ Disable ☐ Enable

Figure 16 Network Settings Page

If the deployment decides 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 only need to choose the **Band** and **Channel** that we wish to use.

The screenshot displays the configuration interface for the 4IPNET EAP200 Enterprise Access Point. At the top, there are five main tabs: System, AP (selected), Firewall, Utilities, and Status. Below these, there are seven sub-tabs: VAP Overview, General (selected), VAP Config, Security, Repeater, Advanced, Access Control, and Site Survey. The breadcrumb trail shows 'Home > AP > General'. The main heading is 'General Settings'. The configuration fields are as follows:

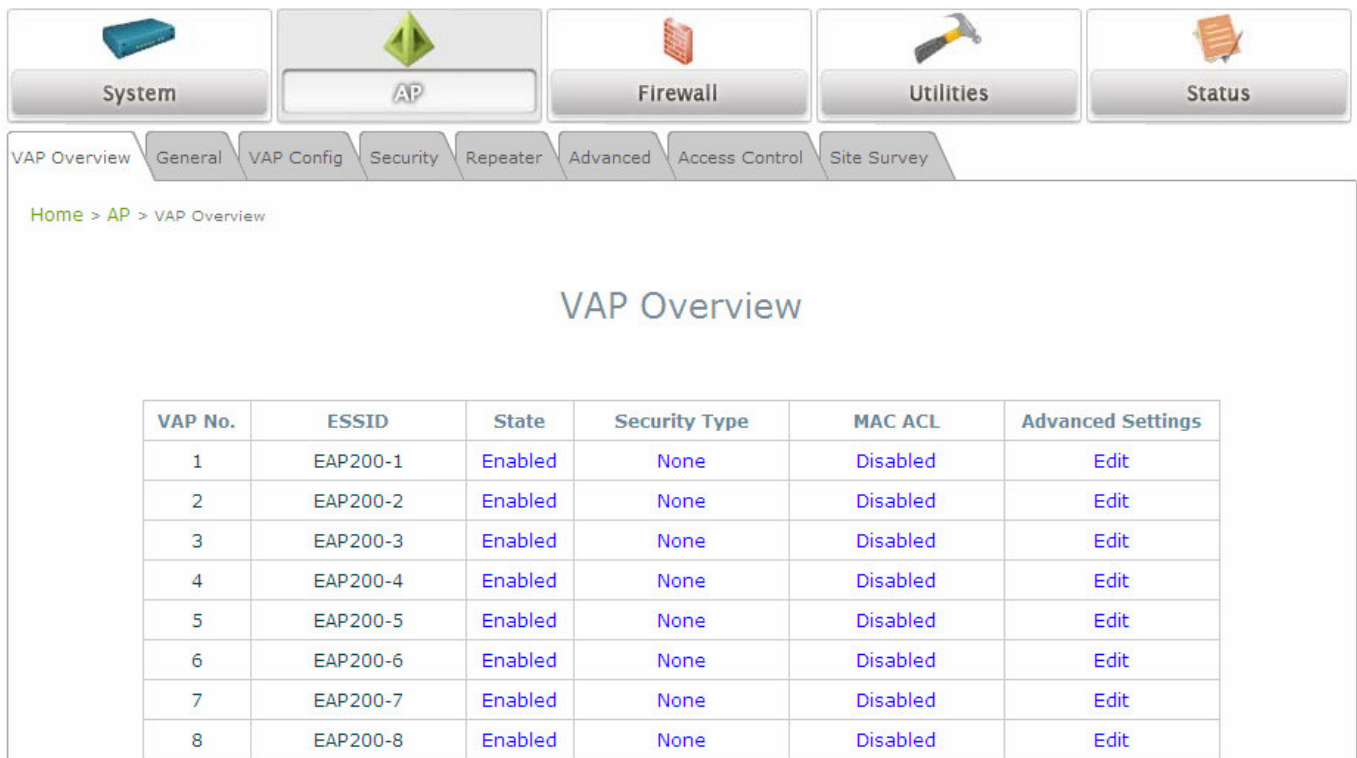
Band :	802.11b+802.11g
Short Preamble :	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Channel :	6
Max Transmit Rate :	Auto
Transmit Power :	Auto
ACK Timeout :	0 <small>*(0 - 255, 0:Auto, Unit:4 micro seconds)</small>
Beacon Interval :	100 <small>*(100 - 500ms)</small>

Figure 17 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 setup 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.



System AP Firewall Utilities Status

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

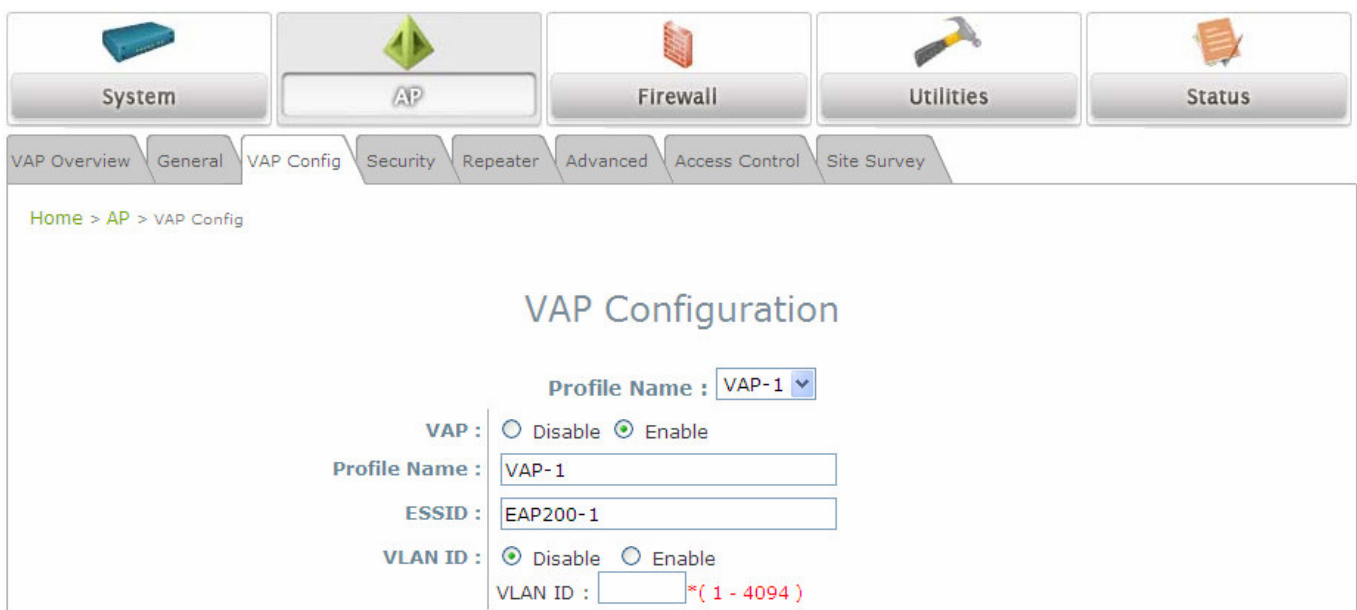
Home > AP > VAP Overview

VAP Overview

VAP No.	ESSID	State	Security Type	MAC ACL	Advanced Settings
1	EAP200-1	Enabled	None	Disabled	Edit
2	EAP200-2	Enabled	None	Disabled	Edit
3	EAP200-3	Enabled	None	Disabled	Edit
4	EAP200-4	Enabled	None	Disabled	Edit
5	EAP200-5	Enabled	None	Disabled	Edit
6	EAP200-6	Enabled	None	Disabled	Edit
7	EAP200-7	Enabled	None	Disabled	Edit
8	EAP200-8	Enabled	None	Disabled	Edit

Figure 18 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.



System AP Firewall Utilities Status

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

Home > AP > VAP Config

VAP Configuration

Profile Name : VAP-1

VAP : ☐ Disable ☒ Enable

Profile Name :

ESSID :

VLAN ID : ☒ Disable ☐ Enable

VLAN ID : *(1 - 4094)

Figure 19 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 **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 work with these revised settings.

4. Adding Virtual Access Points

EAP200 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 **AP** icon to review the **VAP Overview** page.


Home > AP > VAP Overview


VAP Overview


VAP No.	ESSID	State	Security Type	MAC ACL	Advanced Settings
1	EAP200-1	Enabled	None	Disabled	Edit
2	EAP200-2	Enabled	None	Disabled	Edit
3	EAP200-3	Enabled	None	Disabled	Edit
4	EAP200-4	Enabled	None	Disabled	Edit
5	EAP200-5	Enabled	None	Disabled	Edit
6	EAP200-6	Enabled	None	Disabled	Edit
7	EAP200-7	Enabled	None	Disabled	Edit
8	EAP200-8	Enabled	None	Disabled	Edit


Figure 20 VAP Overview Page


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


System


AP


Firewall


Utilities


Status

VAP Overview

General

VAP Config

Security

Repeater

Advanced

Access Control

Site Survey

[Home](#) > [AP](#) > VAP Config

VAP Configuration

Profile Name : VAP-1

VAP :

☐ Disable
 ☒ Enable

Profile Name :

VAP-1

ESSID :

EAP200-1

VLAN ID :

☒ Disable
 ☐ Enable

VLAN ID :

*(1 - 4094)

Figure 21 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 traffics through this particular VAP. Doing so 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 level 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

Home > AP > VAP Overview

VAP Overview

VAP No.	ESSID	State	Security Type	MAC ACL	Advanced Settings
1	EAP200-1	Enabled	None	Disabled	Edit
2	EAP200-2	Enabled	None	Disabled	Edit
3	EAP200-3	Enabled	None	Disabled	Edit
4	EAP200-4	Enabled	None	Disabled	Edit
5	EAP200-5	Enabled	None	Disabled	Edit
6	EAP200-6	Enabled	None	Disabled	Edit
7	EAP200-7	Enabled	None	Disabled	Edit
8	EAP200-8	Enabled	None	Disabled	Edit

Figure 22 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 it, to proceed with **VAP Configuration** for that particular VAP.

Home > AP > VAP Config

VAP Configuration

Profile Name : VAP-1

VAP : ☐ Disable ☒ Enable

Profile Name : VAP-1

ESSID : EAP200-1

VLAN ID : ☒ Disable ☐ Enable

VLAN ID : *(1 - 4094)

Figure 23 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 the 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 > AP > Security

Security Settings

Profile Name : VAP-1

Security Type : None

Figure 24 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 in the 4IPNET management interface. The breadcrumb trail is 'Home > AP > Security'. The 'Security Type' dropdown menu is set to 'None'. The 'Profile Name' dropdown menu is set to 'VAP-1'.

Figure 25 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 'Security Type' set to 'WEP'. A red note states: 'Note! The WEP keys are global setting for all virtual APs. The key value will apply to all VAPs.' The configuration options are as follows:

- 802.11 Authentication:** Radio buttons for 'Open System' (selected), 'Shared Key', and 'Auto'.
- WEP Key Length:** Radio buttons for '64 bits' (selected), '128 bits', and '152 bits'.
- WEP Key Format:** Radio buttons for 'ASCII' (selected) and 'Hex'.
- WEP Key Index:** A dropdown menu set to '1'.
- WEP Keys:** Four input fields labeled 1, 2, 3, and 4 for entering the WEP key values.

Figure 26 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.

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)

Figure 27 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-bit** or **128-bit** key length.
- **Rekeying Period:** The time interval for the dynamic WEP key to be updated; the time unit is in second.

➤ **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:** Provide shared key authentication in WPA data encryption.

The screenshot shows the 'Security Settings' page in a web interface. At the top, there is a navigation bar with tabs: VAP Overview, General, VAP Config, Security (selected), Repeater, Advanced, Access Control, and Site Survey. Below the navigation bar, a breadcrumb trail reads 'Home > AP > Security'. The main heading is 'Security Settings'. The configuration fields are as follows: 'Profile Name' is a dropdown menu set to 'VAP-1'; 'Security Type' is a dropdown menu set to 'WPA-PSK'; 'Cipher Suite' is a dropdown menu set to 'TKIP (WPA)'; 'Pre-shared Key Type' has two radio buttons: 'PSK(Hex)*(64 chars)' (unselected) and 'Passphrase*(8 - 63 chars)' (selected); 'Pre-shared Key' is a text input field; and 'Group Key Update Period' is a text input field set to '600' with the unit 'second(s)'.

Figure 28 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:** Authenticate users by RADIUS and provide WPA data encryption.

Home > AP > 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) *

Secondary RADIUS Server :

Host: (Domain Name / IP Address)

Figure 29 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 then **Reboot** the system. Otherwise, click on the **Overview** tab and proceed with the next step.

Step 3: Configuring MAC ACL (Access Control List)

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

Figure 30 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 re-Enables the listed MAC.

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
3	<input type="text"/>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
4	<input type="text"/>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
5	<input type="text"/>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

Figure 31 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 > AP > 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
3	<input type="text"/>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
4	<input type="text"/>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
5	<input type="text"/>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

Figure 32 MAC ACL Deny List

- 4) **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's MAC ACL and its security type (shown on the **Security Settings** page) share the same RADIUS configuration.

The screenshot displays 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 > AP > Access Control'. The main title is 'Access Control Settings'. The configuration is organized into two columns. The left column contains labels: 'Profile Name:', 'Maximum Number of Clients:', 'Access Control Type:', 'Primary RADIUS Server:', and 'Secondary RADIUS Server:'. The right column contains the corresponding input fields and values. 'Profile Name' is a dropdown menu set to 'VAP-1'. 'Maximum Number of Clients' is a text box with '32' and a note '*(Range: 1 ~ 32)'. 'Access Control Type' is a dropdown menu set to 'RADIUS ACL'. 'Primary RADIUS Server' has a red note: 'Note!!! These settings will also apply to security settings which use RADIUS Server for this VAP.' Below this, there are three fields: 'Host:' (empty), 'Authentication Port:' (set to '1812' with note '*(1 - 65535)'), and 'Secret Key:' (empty with an asterisk). 'Secondary RADIUS Server' has three empty fields for 'Host:', 'Authentication Port:', and 'Secret Key:'.

Figure 33 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 will assist to extend network coverage where running wires is not an option, effectively transferring the traffics to the other end of WLAN/LAN through the EAP200. Since this is a peer to peer connection, both EAP200s will be configured by 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 EAP200s must be configured to use the same channel and band for their wireless settings. Click the **AP** icon and then **General** tab to go to the following page.

The screenshot shows the 'General Settings' page for the AP. The top navigation bar includes icons for System, AP (selected), Firewall, Utilities, and Status. Below this is a sub-navigation bar with tabs: VAP Overview, General (selected), VAP Config, Security, Repeater, Advanced, Access Control, and Site Survey. The breadcrumb trail reads 'Home > AP > General'. The 'General Settings' section contains the following configuration options:

- Band :** 802.11b+802.11g (dropdown menu)
- Short Preamble :** ☐ Disable ☒ Enable
- Channel :** 6 (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)

Figure 34 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 if Connecting Many 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** and then **Network Interface** tab.

General Network Interface Management

Home > System > Network Interface

Network Settings

Mode : ☒ Static ☐ DHCP Renew

IP Address : *

Netmask : *

Default Gateway : *

Primary DNS Server : *

Alternate DNS Server :

Layer2 STP : ☒ Disable ☐ Enable

Figure 35 Network Settings Page

Please select **Enable** in the field labeled **Layer2 STP**. This will prevent data from looping or 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 EAP200's detailed settings. The following table shows all the User Interface (UI) functions of 4ipnet's EAP200 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**, **AP**, **Firewall**, **Utilities**, and **Status**.

Table 1 EAP200's Function Organization

OPTION	FUNCTION
System	General
	Network Interface
	Management
AP	VAP Overview
	General
	VAP Configuration
	Security
	Repeater
	Advanced
	Access Control
	Site Survey
Firewall	Firewall List
	Service
	Advanced
Utilities	Change Password
	Backup & Restore
	System Upgrade
	Reboot
Status	Overview
	Associated Clients
	Repeater
	Event Log

On each configuration page, the user may

» **Note:** Click **SAVE** to save the changes, but the user must reboot the system upon the completion of all configurations for the changes to take effect. Upon 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 on the **System** button, users can work on 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**, and **Management**.

7.1.1 General

General Network Interface Management

Home > System > General

System Information

Name : EAP200

Description :

Location :

Time

Device Time : 2000/01/04 04:48:39

Time Zone : (GMT+08:00)Taipei

Time : ☐ Enable NTP ☒ Manually set up

Set Date : Year Month Day

Set Time : Hour Min Sec

Figure 36 System Information Page

- **System Information**

For maintenance purpose, 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 NTP server or manual setup.

1) Enable NTP:

By selecting **Enabled NTP**, EAP200 can synchronize its system time with the NTP server automatically. While this method is chosen, at least one NTP server's IP address or domain name must be provided.

Time

Device Time :	2000/01/03 04:32:49
Time Zone :	(GMT+08:00)Taipei
Time :	<input checked="" type="radio"/> Enable NTP <input type="radio"/> Manually set up
NTP Server 1 :	<input type="text"/> *
NTP Server 2 :	<input type="text"/>

Figure 37 NTP Time Configuration Fields

Generally networks would have a common NTP server (internal or external). If there is, use that one, otherwise 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 :	<input type="radio"/> Enable NTP <input checked="" type="radio"/> Manually set up
Set Date :	<input type="text"/> Year <input type="text"/> Month <input type="text"/> Day
Set Time :	<input type="text"/> Hour <input type="text"/> Min <input type="text"/> Sec

Figure 38 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 either Internet connection or NTP server may become 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**, **Gateway**, and **Primary DNS Server**) are mandatory.

General Network Interface Management

Home > System > Network Interface

Network Settings

Mode : ☒ Static ☐ DHCP

IP Address : *

Netmask : *

Default Gateway : *

Primary DNS Server : *

Alternate DNS Server :

Layer2 STP : ☒ Disable ☐ Enable

Figure 39 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 EAP200 is set up to bridge other network components, this option can be enabled to prevent undesired loops because 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 Management

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

General Network Interface Management

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 : 192.168.1.254
Server Port : 514
Syslog Level : Error

Figure 40 Management Services Page

- **VLAN for Management:** When it is enabled, management traffics from the system will be tagged with a VLAN ID. In other words, administrator who wants to access the WMI must send management traffics 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.

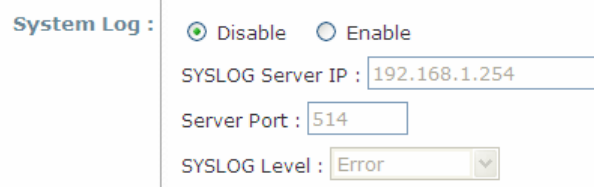
- **SNMP Configuration:** By enabling SNMP function, the administrator can obtain the system information remotely.



The image shows a web interface for SNMP Configuration. It includes a title 'SNMP Configuration :', two radio buttons for 'Disable' (selected) and 'Enable', a section for 'Community String' with 'Read' and 'Write' text boxes, a 'Trap' section with 'Disable' (selected) and 'Enable' radio buttons, and a 'Server IP' text box.

Figure 41 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.



The image shows a web interface for System Log configuration. It includes a title 'System Log :', two radio buttons for 'Disable' (selected) and 'Enable', a 'SYSLOG Server IP' text box containing '192.168.1.254', a 'Server Port' text box containing '514', and a 'SYSLOG Level' dropdown menu set to 'Error'.

Figure 42 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.

7.2 AP

This section includes the following functions: **VAP Overview**, **General**, **VAP Configuration**, **Security**, **Repeater**, **Advanced**, **Access Control**, and **Site Survey**. EAP200 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 EAP200 features 8 VAPs with respective settings. In this table, please click on the hyperlink to further configure each individual VAP.

VAP Overview	General	VAP Config	Security	Repeater	Advanced	Access Control	Site Survey
Home > AP > VAP Overview							
VAP Overview							
VAP No.	ESSID	State	Security Type	MAC ACL	Advanced Settings		
1	EAP200-1	Enabled	None	Disabled	Edit		
2	EAP200-2	Enabled	None	Disabled	Edit		
3	EAP200-3	Enabled	None	Disabled	Edit		
4	EAP200-4	Enabled	None	Disabled	Edit		
5	EAP200-5	Enabled	None	Disabled	Edit		
6	EAP200-6	Enabled	None	Disabled	Edit		
7	EAP200-7	Enabled	None	Disabled	Edit		
8	EAP200-8	Enabled	None	Disabled	Edit		

Figure 43 VAP Overview Page

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

Home > AP > VAP Config

VAP Configuration

Profile Name : VAP-1

VAP : ☐ Disable ☒ Enable

Profile Name : VAP-1

ESSID : EAP200-1

VLAN ID : ☒ Disable ☐ Enable

VLAN ID : *(1 - 4094)

Figure 44 VAP Overview Page – State

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

Home > AP > Security

Security Settings

Profile Name : VAP-1

Security Type : None

Figure 45 VAP Overview Page – Security Type

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

Home > AP > Access Control

Access Control Settings

Profile Name : VAP-1

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

Access Control Type : Disable Access Control

Figure 46 VAP Overview Page – MAC ACL

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

Home > AP > Advanced

Advanced Wireless Settings

Profile Name : VAP-1

RTS Threshold : 2346 *(1 - 2346)

Fragment Threshold : 2346 *(256 - 2346)

DTIM period : 1 *(1 - 15)

Broadcast SSID : ☐ Disable ☒ Enable

Wireless Station Isolation : ☒ Disable ☐ Enable

WMM : ☒ Disable ☐ Enable

IAPP : ☒ Disable ☐ Enable

Figure 47 VAP Overview Page – Advanced Settings

7.2.2 General

AP's general wireless settings can be configured here:

Figure 48 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.
- **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 **Auto**.
- **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.
- **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 that 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 deployment, 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.

**Due to RF regulation in different nations, available values in the above table will differ.

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

Band	SSID	Short Preamble	Channel	Max Transmit Rate	Transmit Power
Disable	N/A	N/A	N/A	N/A	N/A
802.11b	Associated AP's SSID	Disable/Enable	Auto, 1~11, 13 or 14	1M, 2M, 5.5M, 11M	Auto, Lowest, Low, Medium, High, Highest
802.11g	Associated AP's SSID	Disable/Enable	Auto, 1~11 or 13	6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M	
802.11b+ 802.11g	Associated AP's SSID	Disable/Enable	Auto, 1~11, 13 or 14	1M, 2M, 5.5M, 6M, 9M, 11M, 12M, 18M, 24M, 36M, 48M, 54M	
802.11g+ 802.11n	Associated AP's SSID	Disable/Enable	Auto, 1~11, or 13	1M, 2M, 5.5M, 6M, 9M, 11M, 12M, 18M, 24M, 36M, 48M, 54M, MCS0~15	

7.2.3 VAP Configuration

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

Figure 49 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:** EAP200 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

EAP200 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' page for a VAP profile named 'VAP-1'. The 'Security Type' is set to 'None'. The breadcrumb trail is 'Home > AP > Security'.

Figure 50 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' page for a VAP profile named 'VAP-1'. The 'Security Type' is set to 'WEP'. Below this, there are several configuration options:

- 802.11 Authentication:** Radio buttons for 'Open System' (selected), 'Shared Key', and 'Auto'.
- WEP Key Length:** Radio buttons for '64 bits' (selected), '128 bits', and '152 bits'.
- WEP Key Format:** Radio buttons for 'ASCII' (selected) and 'Hex'.
- WEP Key Index:** A dropdown menu set to '1'.
- WEP Keys:** Four input fields labeled 1, 2, 3, and 4.

 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 > AP > Security'.

Figure 51 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 **1~4**. 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

Security Type :

Dynamic WEP :

Primary RADIUS Server :

Secondary RADIUS Server :

Profile Name : VAP-1

802.1X

☐ Disable ☒ Enable

WEP Key Length : ☒ 64 bits ☐ 128 bits

Rekeying Period : second(s)

Host : *(Domain Name / IP Address)

Authentication Port : *

Secret Key :

Accounting Service : ☒ Disable ☐ Enable

Accounting Port : *

Accounting Interim Update Interval : second(s) *

Host: (Domain Name / IP Address)

Figure 52 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-bit** or **128-bit** key length.
- **Re-keying Period:** The time interval for the dynamic WEP key to be updated; the time unit is in second.

➤ **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 displays the 'Security Settings' page within a web management interface. At the top, there are tabs for 'VAP Overview', 'General', 'VAP Config', 'Security' (which is active), 'Repeater', 'Advanced', 'Access Control', and 'Site Survey'. Below the tabs, a breadcrumb trail reads 'Home > AP > Security'. The main heading is 'Security Settings'. The configuration area includes:

- Profile Name:** A dropdown menu showing 'VAP-1'.
- Security Type:** A dropdown menu showing 'WPA-PSK'.
- Cipher Suite:** A dropdown menu showing 'TKIP (WPA)'.
- Pre-shared Key Type:** Two radio buttons: 'PSK(Hex)*(64 chars)' (unselected) and 'Passphrase*(8 - 63 chars)' (selected).
- Pre-shared Key:** A text input field.
- Group Key Update Period:** A text input field containing '600' followed by the unit 'second(s)'.

Figure 53 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 be both enabled.

The screenshot shows the 'Security Settings' page in a web interface. At the top, there are tabs: VAP Overview, General, VAP Config, Security (selected), Repeater, Advanced, Access Control, and Site Survey. Below the tabs, a breadcrumb trail reads 'Home > AP > Security'. The main heading is 'Security Settings'. The configuration is for 'Profile Name : VAP-1'. Under 'Security Type', 'WPA-RADIUS' is selected. Under 'Cipher Suite', 'TKIP (WPA)' is selected. 'Group Key Update Period' is set to '600 second(s)'. For the 'Primary RADIUS Server', the 'Host' field is empty with a red asterisk and '(Domain Name / IP Address)' in red text. The 'Authentication Port' is set to '1812' with a red asterisk. The 'Secret Key' field is empty. The 'Accounting Service' has 'Disable' selected. The 'Accounting Port' is set to '1813' with a red asterisk. The 'Accounting Interim Update Interval' is set to '60 second(s)*'. For the 'Secondary RADIUS Server', the 'Host' field is empty with a red asterisk and '(Domain Name / IP Address)' in red text.

Figure 54 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, EAP200 supports either **WDS** or **Universal Repeater** as options of repeater types; selecting **None** will turn off this function.

➤ 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 for intended connection.

The screenshot shows the 'Repeater Settings' page in the EAP200 web interface. The breadcrumb trail is 'Home > Wireless > Repeater Config'. The 'Repeater Type' is set to 'Universal Repeater'. Below this, there is a field for 'The SSID of Upper-Bound AP' with the value 'N/A' and a red asterisk. A red warning message states: 'Current wireless channel of the system is set at 6. Repeater connection may fail if the system is set to connect to upper AP with different channels'. The 'Security Type' is set to 'None'.

Figure 55 Repeater Settings: Universal Repeater

➤ WDS

If **WDS** is selected, EAP200 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 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 is used to clear the contents in the above WDS connection list.

The screenshot shows the 'Repeater Settings' page in the EAP200 web interface. The breadcrumb trail is 'Home > Wireless > Repeater Config'. The 'Repeater Type' is set to 'WDS'. Below this, the 'WDS Profile' is set to 'RF Card : WDS Link 1'. The 'WDS' status is set to 'Disable'. There is an empty field for 'MAC Address' and the 'Security type' is set to 'None'.

Figure 56 Repeater Settings: WDS

7.2.6 Advanced

The advanced wireless settings for the EAP200'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.

Home > AP > Advanced

Advanced Wireless Settings

Profile Name : VAP-1

RTS Threshold : 2346 *(1 - 2346)

Fragment Threshold : 2346 *(256 - 2346)

DTIM period : 1 *(1 - 15)

Broadcast SSID : ☐ Disable ☒ Enable

Wireless Station Isolation : ☒ Disable ☐ Enable

WMM : ☒ Disable ☐ Enable

IAPP : ☒ Disable ☐ Enable

Figure 57 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 frame 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 EAP200 or in areas where the clients are far apart and can detect only EAP200 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 energy more, 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 EAP200.
 - 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 that are connected to them. By enabling this function, the system will automatically broadcast information of associated wireless stations to its peer access points. This will help wireless stations roam smoothly among IAPP-enabled access points in the same wireless LAN.

7.2.7 Access Control

On this page, the network administrator can restrict the total number of clients connected to the EAP200, 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, a breadcrumb trail reads 'Home > AP > Access Control'. The main title 'Access Control Settings' is centered. Below the title, 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 note '* (Range: 1 ~ 32)'; and 'Access Control Type' is a dropdown menu set to 'Disable Access Control'.

Figure 58 Access Control Settings Page

- **Maximum Number of Clients**

EAP200 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, while 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 > AP > Access Control

Access Control Settings

Profile Name : VAP-1

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

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
3	<input type="text"/>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
4	<input type="text"/>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
5	<input type="text"/>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

Figure 59 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 > AP > 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
3	<input type="text"/>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
4	<input type="text"/>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
5	<input type="text"/>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

Figure 60 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](#) > [AP](#) > [Access Control](#)

Access Control Settings

Maximum Number of Clients :

Access Control Type :

Primary RADIUS Server :

Secondary RADIUS Server :

Profile Name : VAP-1

*(Range: 1 ~ 32)

RADIUS ACL

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

Host: *(Domain Name / IP Address)

Authentication Port: *(1 - 65535)

Secret Key: *

Host:

Authentication Port:

Secret Key:

Figure 61 RADIUS ACL

7.2.8 Site Survey

Sit Survey is a useful tool to provide information about the surrounding wireless environment; available APs are shown with their respective SSID, MAC Address, Channel, Rate setting, Signal reading, and Security type. The administrator can click **Setup** or **Connect** to configure the wireless connection according to the mentioned readings when Repeater Type is Universal Repeater.

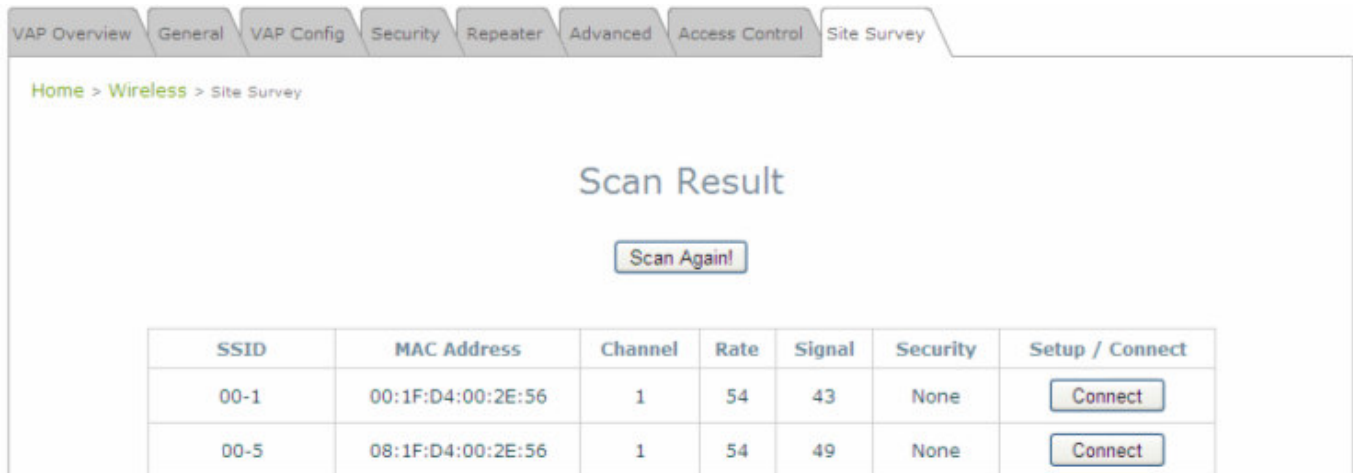


Figure 62 Site Survey Page

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 to 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	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	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 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.

Firewall List
Service
Advanced

Home > Firewall > Firewall List

Layer 2 Firewall Settings

Enable Layer 2 Firewall ☐ Disable ☒ Enable

No.	State	Action	Name	EtherType	Remark	Setting
1	<input type="checkbox"/>	DROP	CDP and VTP	IEEE_8023		Del Ed In Mv
2	<input type="checkbox"/>	DROP	STP/BPDU	IEEE_8023		Del Ed In Mv
3	<input type="checkbox"/>	DROP	GARP	IEEE_8023		Del Ed In Mv
4	<input type="checkbox"/>	DROP	RIP	IPv4		Del Ed In Mv
5	<input type="checkbox"/>	DROP	HSRP	IPv4		Del Ed In Mv
6	<input type="checkbox"/>	DROP	OSPF	IPv4		Del Ed In Mv
7	<input type="checkbox"/>					Del Ed In Mv
8	<input type="checkbox"/>					Del Ed In Mv
9	<input type="checkbox"/>					Del Ed In Mv
10	<input type="checkbox"/>					Del Ed In Mv

First
Prev
Next
Last
(total: 20)

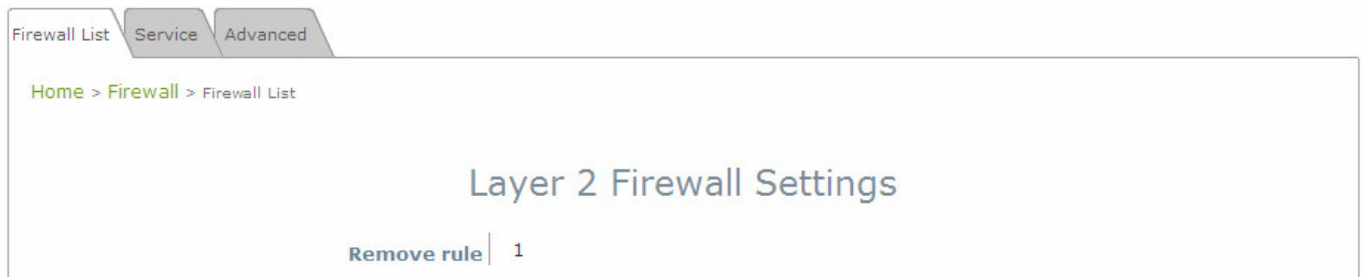
Figure 63 Firewall List Page

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

- **No.:** The numbering will decide the priority to let system 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:** It shows the name of rule.
- **EtherType:** It denotes the type of traffics subject to this rule.
- **Remark:** It shows the note of this rule.
- **Setting:** 4 actions are available; **Del** denotes to delete the rule, **Ed** denotes to edit the rule, **In** denotes to insert a rule, and **Mv** denotes to move the rule.

>>To delete a specific rule,

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



>>To edit a specific rule,

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

Layer 2 Firewall Configuration

Rule ID : 1
Rule name : CDP and VTP *
EtherType : IEEE802.3 ▾
Interface : ☒ From ☐ To
 VAP1 ▾
DSAP/SSAP : aa
Type : 2000 (ie IPv4: 0800)
Source : MAC Address: Mask:
Destination : MAC Address: 01:00:0C:CC:CC:CC Mask:
Action : ☒ Block ☐ Pass
Remark :

- **Rule ID:** The numbering of this specific rule will decide its priority among available firewall rules in the table.
- **Rule name:** The rule name can be specified here.
- **EtherType:** The drop-down list will provide the available types of traffics subject to this rule.
- **Interface:** It can indicate 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 traffics.
- **VLAN ID** (when EtherType is **802.1 Q**): The VLAN ID is provided to associate with certain VLAN-tagging traffics.
- **Priority** (when EtherType is **802.1 Q**): It denotes the priority level with associated VLAN traffics.
- **Encapsulated Type** (when EtherType is **802.1 Q**): It can be used to indicate the type of encapsulated traffics.
- **Opcode** (when EtherType is **ARP/RARP**): This list can be used to specify the ARP Opcode in ARP header.
- **Source:** MAC Address/Mask indicates the source MAC; IP Address/Mask indicates the source IP address (when EtherType is **IPv4**); ARP IP/MAC & MASK indicate the ARP payload fields.
- **Destination:** MAC Address/Mask indicates the destination MAC; IP Address/Mask indicates the destination IP address (when EtherType is **IPv4**); ARP IP/MAC & MASK indicate the ARP payload fields.
- **Action:** The rule can be chosen to be **Block** or **Pass**.

- **Remark:** The note of this rule can be specified here.

When the configuration for firewall rule is provided; please click **SAVE** and **Reboot** system to let the firewall rule take effect.

>>To insert a specific rule,

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

From this page, the rule can be edited from 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 **Setting** column of firewall list will lead to the following page for reordering confirmation. After **SAVE** button is clicked and system reboot, the order of rules will be updated.

Firewall List Service Advanced

Home > Firewall > Move rule

Move Rule

ID : 1

Move to : ☒ Before ☐ After ID : *(1 - 20)

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

Firewall List Service Advanced

Home > Firewall > Firewall List

Layer 2 Firewall Settings

Enable Layer 2 Firewall ☐ Disable ☒ Enable

No.	State	Action	Name	EtherType	Remark	Setting
1	<input checked="" type="checkbox"/>	DROP	CDP and VTP	IEEE_8023		Del Ed In Mv
2	<input type="checkbox"/>	DROP	STP/BPDU	IEEE_8023		Del Ed In Mv
3	<input type="checkbox"/>	DROP	GARP	IEEE_8023		Del Ed In Mv
4	<input type="checkbox"/>	DROP	RIP	IPv4		Del Ed In Mv
5	<input type="checkbox"/>	DROP	HSRP	IPv4		Del Ed In Mv
6	<input type="checkbox"/>	DROP	OSPF	IPv4		Del Ed In Mv
7	<input type="checkbox"/>					Del Ed In Mv
8	<input type="checkbox"/>					Del Ed In Mv
9	<input type="checkbox"/>					Del Ed In Mv
10	<input type="checkbox"/>					Del Ed In Mv

First Prev Next Last (total: 20)

SAVE

CLEAR

7.3.2 Service

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

EAP200 provides a list of rules to block or pass traffics of layer-3 or above protocols. These services are available to choose from drop-down list of layer2 firewall rule edit page with Ether Type to be 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"/>

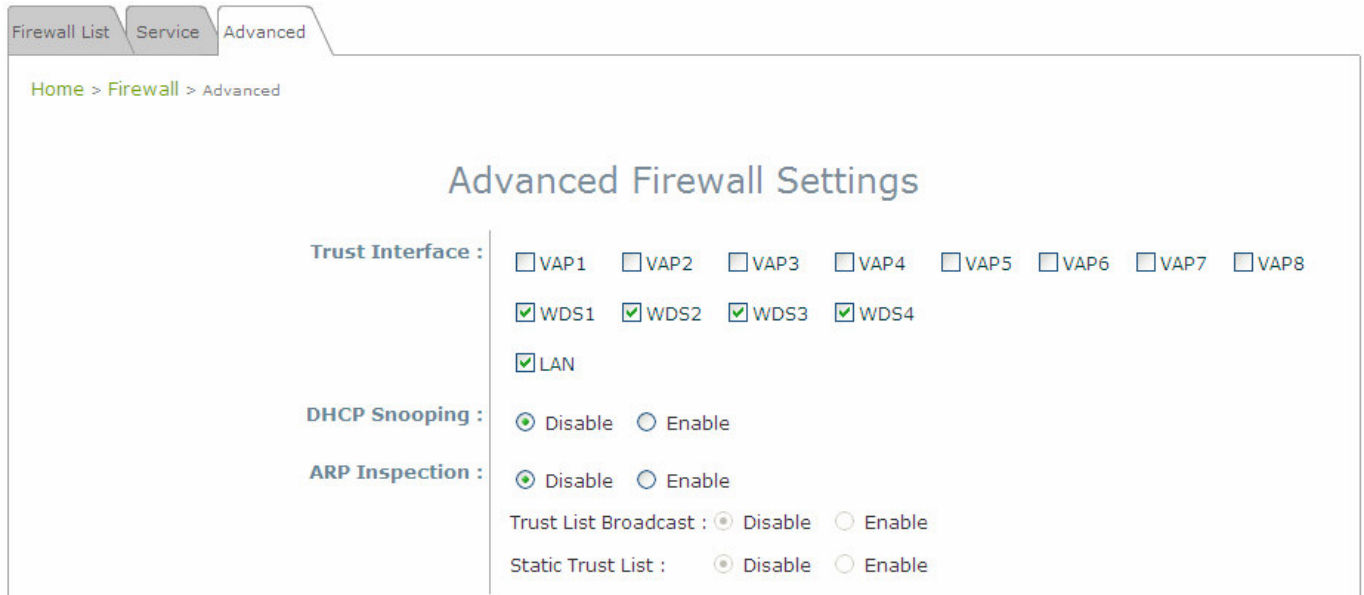
First
Prev
Next
Last
(total: 28)

Add

Figure 64 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 system.



Firewall List Service Advanced

Home > Firewall > Advanced

Advanced Firewall Settings

Trust Interface : ☐ VAP1 ☐ VAP2 ☐ VAP3 ☐ VAP4 ☐ VAP5 ☐ VAP6 ☐ VAP7 ☐ VAP8
☒ WDS1 ☒ WDS2 ☒ WDS3 ☒ WDS4
☒ LAN

DHCP Snooping : ☒ Disable ☐ Enable

ARP Inspection : ☒ Disable ☐ Enable

Trust List Broadcast : ☒ Disable ☐ Enable

Static Trust List : ☒ Disable ☐ Enable

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

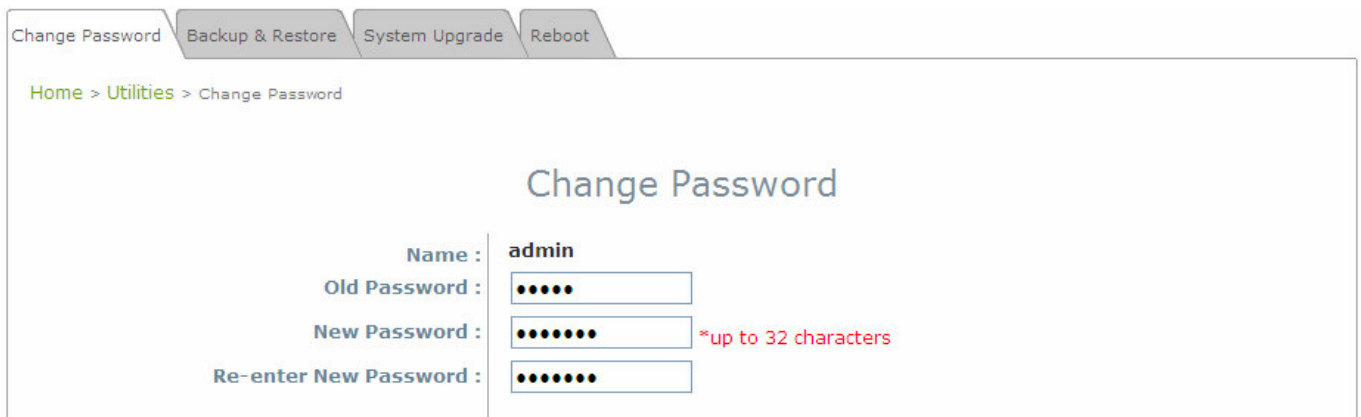
If any settings are made, please click **SAVE** to save the configuration before leaving this page.

7.4 Utilities

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

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 within a web management interface. At the top, there are four tabs: 'Change Password' (selected), 'Backup & Restore', 'System Upgrade', and 'Reboot'. Below the tabs, a breadcrumb trail reads 'Home > Utilities > Change Password'. The main heading is 'Change Password'. The form contains four fields: 'Name' with the value 'admin', 'Old Password' with five dots, 'New Password' with seven dots and a red note '*up to 32 characters', and 'Re-enter New Password' with seven dots.

Figure 65 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 EAP200 settings. The EAP200 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).

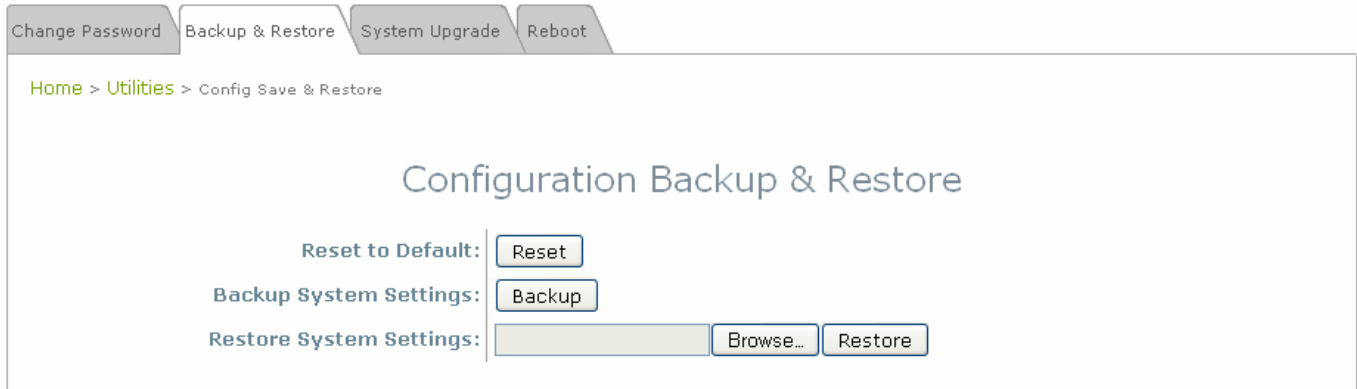


Figure 66 Backup & Restore Page

- **Reset to Default:**

- Click **Reset** to load the factory default settings of EAP200. A pop-up Page will appear to reconfirm the request to reboot the system. Click **OK** to proceed.

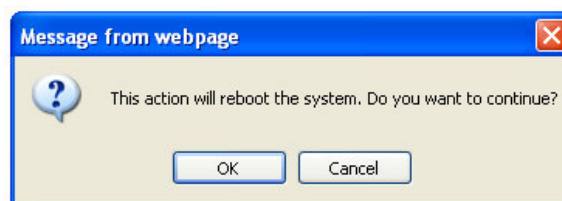


Figure 67 Reboot Confirmation Prompt

- A warning message as displayed below will appear during the reboot period. The system power must be kept turn on before the completion of the reboot process.
- The **System Overview** page will appear upon the completion of reboot.
- **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 EAP200.

7.4.3 System Upgrade

The EAP200 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 appearing to notify the administrator to restart the system after a successful firmware upgrade. Please restart the system after upgrading the firmware.

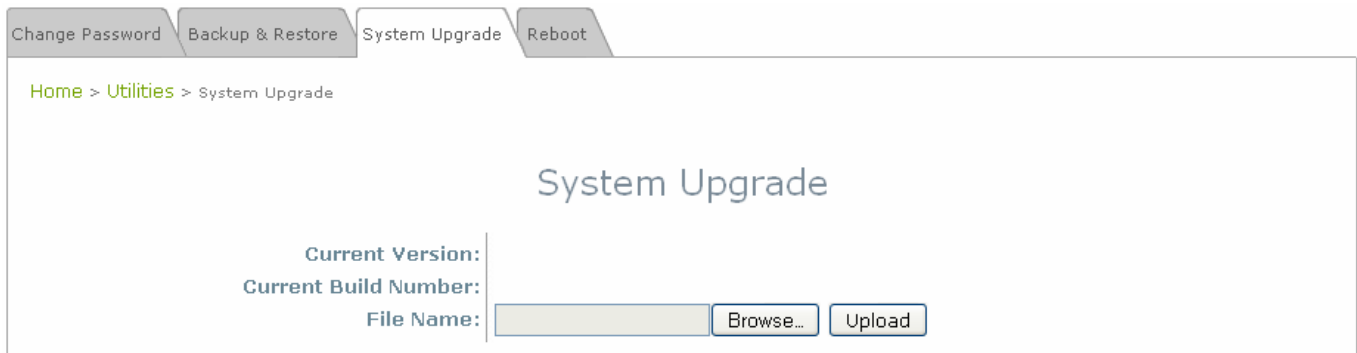


Figure 68 System Upgrade Page

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

7.4.4 Reboot

This function allows the administrator to restart the EAP200 safely. The process shall take about three minutes. Click **Reboot** to restart the system. Please wait for the blinking timer to complete its countdown before accessing the system's Web Management Interface again. The System Overview page will appear after reboot successfully.

Occasionally, it is necessary to reboot the EAP200 to ensure that parameter changes are submitted.

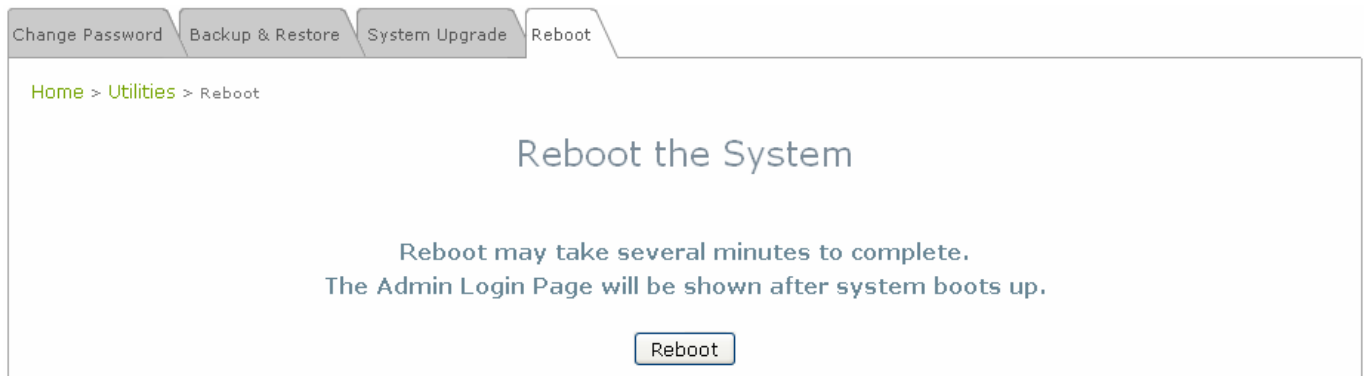


Figure 69 Reboot Page

7.5 Status

This page is used to view the current condition and state of the system and 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.

Home > Status > System Overview

System Overview

System

System Name	EAP200
Firmware Version	
Build Number	
Location	
Site	EN-A
Device Time	
System Up Time	0 days, 0:04:49

Radio Status

MAC Address	00:1F:D4:03:22:20
Band	802.11b+g
Channel	6
TX Power	18 dBm

LAN Interface

MAC Address	1E:1F:D4:03:22:20
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
VAP-1	00:1F:D4:03:22:20	EAP200-1	None	0
VAP-2	06:1F:D4:03:22:20	EAP200-2	None	0
VAP-3	0A:1F:D4:03:22:20	EAP200-3	None	0
VAP-4	0E:1F:D4:03:22:20	EAP200-4	None	0
VAP-5	12:1F:D4:03:22:20	EAP200-5	None	0
VAP-6	16:1F:D4:03:22:20	EAP200-6	None	0
VAP-7	1A:1F:D4:03:22:20	EAP200-7	None	0
VAP-8	1E:1F:D4:03:22:20	EAP200-8	None	0

Figure 70 System Overview Page

Table 3 Status Page's Organizational Layout

Item		Description
System	System Name	The system name of the EAP200.
	Firmware Version	The present firmware version of the EAP200
	Build Number	The present firmware build number of the EAP200
	Location	The location of the EAP200.
	Site	The site of the EAP200
	Device Time	The system time of the EAP200.
	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.

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.

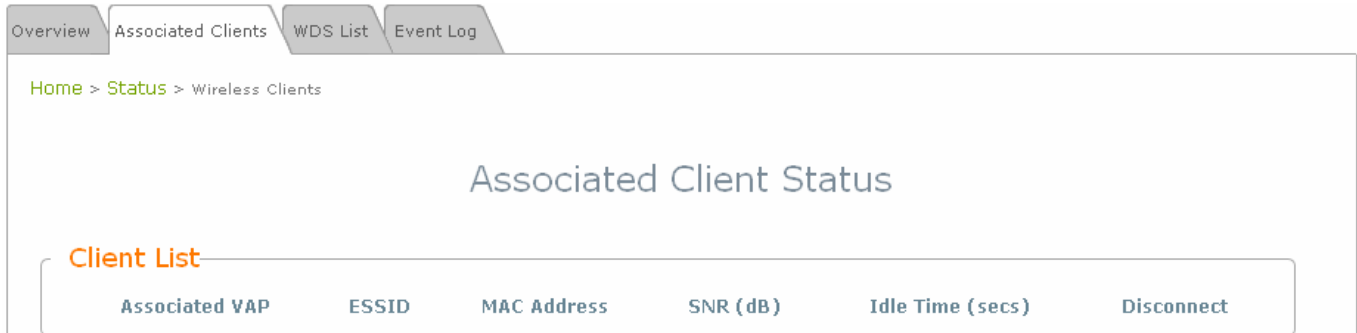


Figure 71 Associated Client Status Page

- **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; the time unit is in second.
- **Disconnect:** Upon clicking **Kick**, the client will be disconnected with the system.


7.5.3 Repeater

The system supports 3 options of Repeater types including status of **MAC Address**, **SNR**, **TX Rate**, **TX Count** and **TX Errors**.

OverviewAssociated ClientsRepeaterEvent Log

Home > Status > Repeater Information

Repeater Information



WDS Link Status

Item	Status	MAC Address	RSSI	TX Rate	TX Count	TX Error	Encryption
1	Disabled		N/A	N/A	N/A	N/A	N/A
2	Disabled		N/A	N/A	N/A	N/A	N/A
3	Disabled		N/A	N/A	N/A	N/A	N/A
4	Disabled		N/A	N/A	N/A	N/A	N/A

Figure 72 WDS Link Status Page

- **WDS Link Status:** The table will indicate the link status of all WDS interfaces.
 - **Status:** The status of the WDS link either **Enabled** or **Disabled**.
 - **MAC Address:** The MAC Address of the WDS peer.
 - **RSSI:** Received Signal Strength Indication, a measurement of received radio signal over WDS link.
 - **TX Rate:** The transmit rate of the WDS link.
 - **TX Count:** The accumulative number of transmission counts.
 - **TX Errors:** The accumulative number of transmission errors.

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.

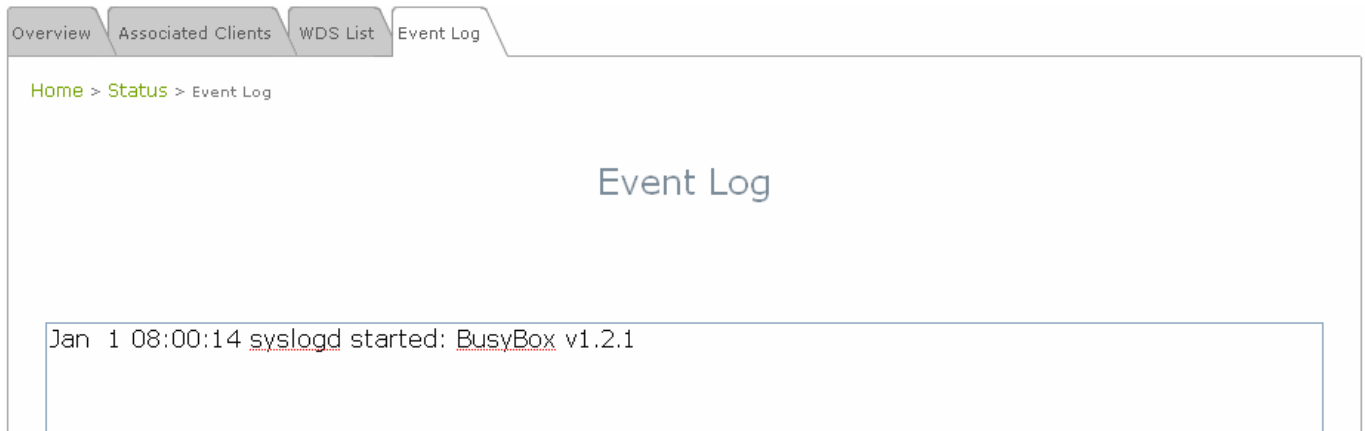


Figure 73 Event Log Page

In the log each line 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. However, in remote SYSLOG service, this field will help the administrator identify which event is from this EAP200.
- **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.



Figure 74 Online Help Corner

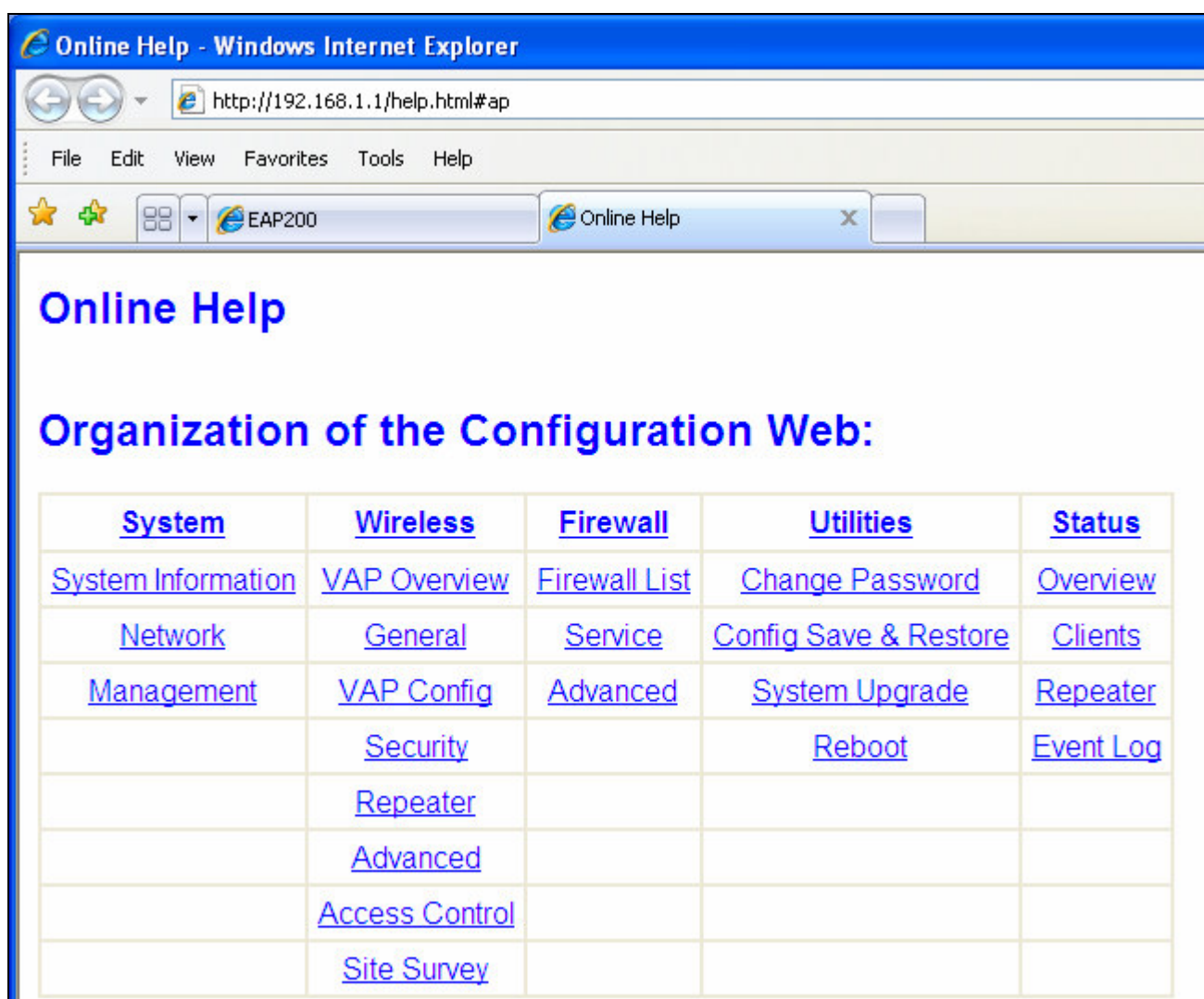


Figure 75 Online Help Page