

User's Manual

EAP701 / EAP717

v1.11

Enterprise Access Point

Copyright & Disclaimer

Copyright

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

Disclaimer

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

Trademarks

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

Table of Contents

1. Before You Start	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.....	6
2.2 Hardware Description	7
2.3 Hardware Installation.....	11
2.4 Access Web Management Interface.....	13
3. Connect your AP to your Network.....	16
4. Adding Virtual Access Points	22
5. Securing the AP	24
6. Creating a WDS Bridge between two APs.....	33
7. Web Management Interface Configuration.....	36
7.1 System.....	38
7.1.1 General	38
7.1.2 Network Interface.....	40
7.1.3 Port.....	41
7.1.4 Management	42
7.1.5 CAPWAP	44
7.2 Wireless.....	45
7.2.1 VAP Overview	45
7.2.2 General	48
7.2.3 VAP Configuration	50
7.2.4 Security.....	51
7.2.5 Repeater	56
7.2.6 Advanced.....	57
7.2.7 Access Control	59
7.3 Firewall.....	62
7.3.1 Firewall List	62
7.3.2 Service	66
7.3.3 Advanced.....	67
7.4 Utilities	68
7.4.1 Change Password.....	68
7.4.2 Backup & Restore.....	68
7.4.3 System Upgrade	71

7.4.4 Reboot	71
7.4.5 Upload Certificate	72
7.5 Status	73
7.5.1 Overview	73
7.5.2 Associated Clients	75
7.5.3 WDS Link Status	75
7.5.4 Event Log.....	76
8. Console Interface Configuration.....	77

1. Before You Start




1.1 Preface

This manual is intended for using by system integrators, field engineers and network administrators to help them set up Access Points in their network environments. It contains step by step procedures and pictures to guide users with basic network system knowledge to complete the installation.

Corresponding Software Versions for each Model

EAP701	Up to software version 1.11
EAP717	Up to software version 1.11

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 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 EAP717 includes:

- 4ipnet EAP717 x1
- Quick Installation Guide (QIG) x1
- Ethernet Cable x1
- Console Cable x1
- Power Adaptor (5V) (Optional) x1
- Mounting Kit x1

The standard package of EAP701 includes:

- 4ipnet EAP701 x1
- Quick Installation Guide (QIG) x1
- Ethernet Cable x1
- Power Adaptor (5V) (Optional) x1
- Flat Surface Mounting Panel x1
- Face Plate Mounting Panel x1
- Mounting Plate Unfastening Tool 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

The 4ipnet EAP717 Enterprise Access Point is an on-the-wall as well as a ceiling-mounted Wi-Fi IEEE 802.11n/a/b/g 2 x 2 MIMO access point, designed to blend into a working or a living environment practically and elegantly with its simplistic yet classy design. The EAP717 is ideal for appearance accentuated applications such as hotels as it has a small and inconspicuous form factor. The RH11 telephone pass through socket is yet another convenient feature for hotel applications. The two Ethernet LAN Ports eliminates the need for a network switch for additional IP Device connections.

The 4ipnet EAP701 Wall Jack Access Point is an in/on-the-wall Wi-Fi IEEE 802.11b/g/n 2.4GHz 2 X 2 MIMO access point, designed specifically for hospitality. The compact EAP701 in a small form factor lays snug in a standard wall outlet box. Its side panel features LED status indicators and two RJ45 ports. It has the interfaces to serve both wireless and wired LAN access.

When coupled with the 4ipnet WHG series Controller, the EAP701/EAP717 supports Tunnel-based AP Management, and comes with all standards demanded by enterprise applications, including business-grade security (802.1X, WPA and WPA2), and multiple ESSIDs with VLAN tags to separate the traffics of different departments. A centralized WLAN management allows enterprises and organizations to support a wide array of value added applications, such as load balancing, bandwidth control, and access control. The patent-pending 4ipWES (Press-n-Connect) technology bridges multiple EAPEAP701/717s at the touch of a button, which enables a quick and automatic WDS Easy Setup by pressing the WES button on Access Point. Extending wireless network coverage is a breeze, be it across conference rooms or along hallways.

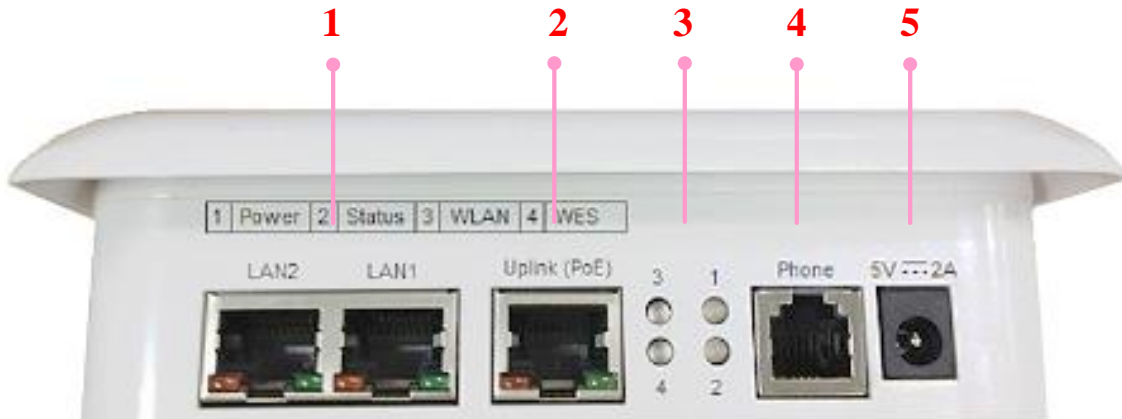
EAP701/EAP717's high throughput, security and optimal invisibility make it a perfect choice of wireless connectivity for your business.

2.2 Hardware Description

This section depicts the hardware information including all panel description.

EAP717

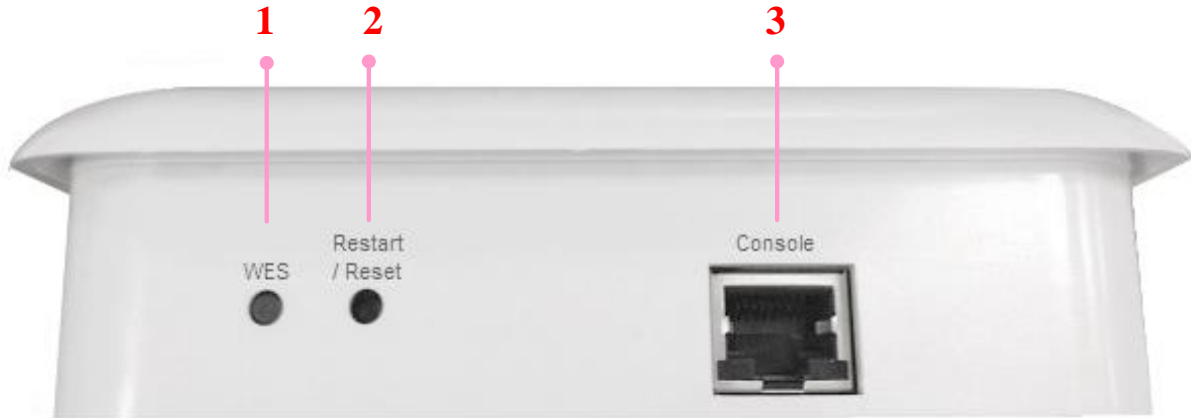
Front Panel



EAP717 Front Panel

1	LAN 1 – 2 Ports	Attach Ethernet cables here to connect to the wired local network.
2	Uplink (PoE) Port	For Uplink connection. This port can be used to connect to a controller, gateway, or directly to the internet. PoE is supported.
3	LED Indicators	4 LED lights. Representation is listed at the top of the panel.
4	Phone Jack	A telephone can bypass to a connected phone line in the back of the AP when connected to the socket.
5	5V 2 A	Attach the power adaptor here.

Rear Panel

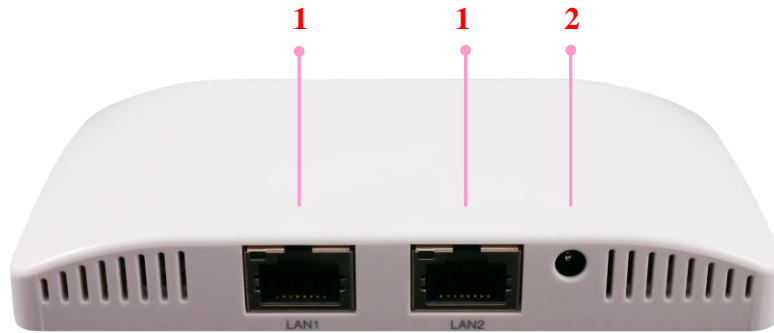


EAP717 Rear Panel

1	WES Button	WDS Easy Setup. Press the button to build up a WDS link with another peer.
2	Restart / Reset Button	Press once to restart the system; Press and hold for more than 5 seconds to reset to factory default.
3	Console Port	To access EAP717 via the console interface.

EAP701

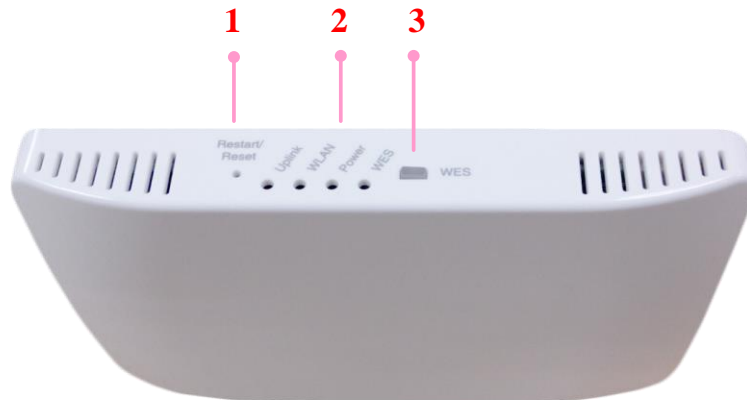
Lower Panel



EAP701 Lower Panel

1	LAN 1 – 2 Ports	Attach Ethernet cables here to connect to the wired local network.
2	DC Jack 5V 2 A	Attach the power adaptor here.

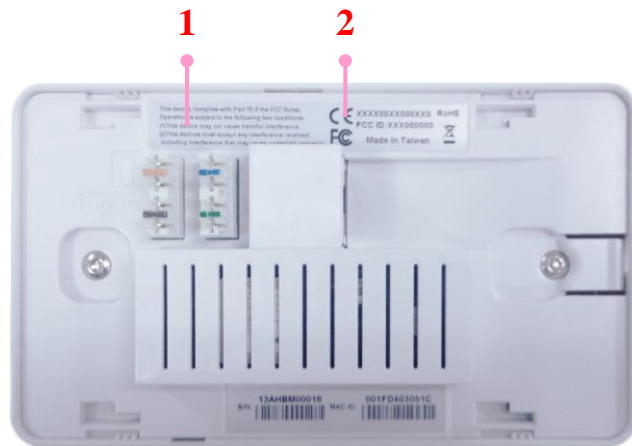
Upper Panel



EAP701 Upper Panel

1	Restart / Reset Button	Press once to restart the system; Press and hold for more than 5 seconds to reset to factory default.
2	LED Indicators	4 LED lights. Representation is listed at the top of the panel.
3	WES Button	WDS Easy Setup. Press the button to build up a WDS link with another peer.

Back Panel



EAP701 Lower Panel

1	110 Punchdown Block	Copper wire punch down for in-wall application
2	Uplink (PoE) Port	For Uplink connection. This port can be used to connect to a controller, gateway, or directly to the internet. PoE is supported.

2.3 Hardware Installation

Please follow the steps mentioned below to install the hardware of **EAP717**:

Step 1. Place the EAP717 at the best location which is usually at the center of your intended wireless network. If admin would like to mount the AP on the wall (on a socket), screw the metal panel to the wall, and then turn the EAP717 clockwise to fasten to the panel. For installation instructions on the Ceiling Mount Kit, please refer to the Quick Installation Guide and the Mounting Guide.

Step 2. Connect one end of the Ethernet cable to the Uplink port and the other end of the cable to a switch, a router, or a hub. The EAP717 is now connected to your existing wired LAN network.

Step 3. There are two ways to supply power to EAP717

- a) Connect the DC power adaptor to the power jack socket.
- b) The Uplink port is capable of receiving PoE. Connect an IEEE 802.3af-compliant PSE device (e.g. a PoE-switch) to the Uplink port of EAP717 with the Ethernet cable.

Please follow the steps mentioned below to install the hardware of **EAP701**:

Step 1. Place the EAP701 at the best location which is usually at the center of your intended wireless network. The EAP701 supports two types of mounting. For mounting installation instructions, please refer to the included EAP701 Quick Installation Guide.

Step 2. Connect one end of the Ethernet cable to the Uplink port and the other end of the cable to a switch, a router, or a hub; Or use the 110 punchdown block as your uplink connection. The EAP701 is now connected to your existing wired LAN network.

Step 3. There are three ways to supply power to EAP701

- a) Connect the DC power adaptor to the power jack socket.
- b) The Uplink port is capable of receiving PoE. Connect an IEEE 802.3af-compliant PSE device (e.g. a PoE-switch) to the Uplink port of EAP701 with the Ethernet cable.
- c) Use a standard 110 punchdown tool to punch copper wires onto the punchdown block (pin assignment 568A)

Now, the Hardware Installation is complete.



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

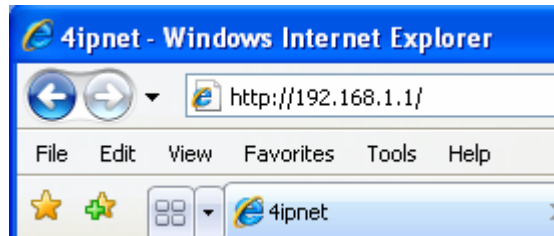
2.4 Access Web Management Interface

4ipnet Access Points support web-based configuration. When hardware installation is complete, the AP can be configured through a PC by using a web browser.

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

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0



Example of entering the AP's default IP Address into a web browser

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

IP Address: 192.168.1.100

Subnet Mask: 255.255.255.0

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

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



Administrator Login Page

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

Overview | Associated Clients | WDS Link Status | Event Log

Home > Status > System Overview

System Overview

System

System Name	Enterprise Access Point
Firmware Version	1.00.00
Build Number	1.5-1.6477
Location	
Site	EN-A
Device Time	1970/01/01 08:15:39
System Up Time	0 days, 0:15:39

Radio Status

MAC Address	00:1F:D4:02:32:F7
Band	802.11g+n
Channel	6
TX Power	Highest

LAN Interface

MAC Address	00:1F:D4:02:32:F6
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	192.168.1.254

AP Status

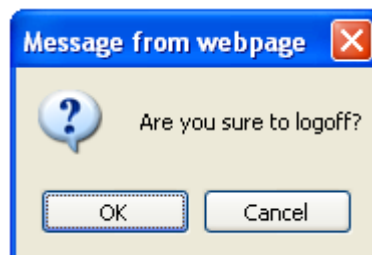
Profile Name	BSSID	ESSID	Security Type	Online Clients	Tun
VAP-1	00:1F:D4:02:32:F7	4ipnetAP-A1	Open	0	

CAPWAP

Status	Disabled
--------	----------

The Web Management Interface – System Overview Page

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



Logout 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 Backup & Restore System Upgrade Reboot Upload Certificate

Home > Utilities > Change Password

Change Password

Name : admin

Old Password :

New Password : *up to 32 characters

Re-enter New Password :

SAVE **CLEAR**

Change Password Page

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

Congratulation!

Now, the 4ipnet Access Point is installed and configured successfully.



- *It is strongly recommended to make a backup copy of your configuration settings.*
- *After the AP'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 AP's hardware for configuration, set the TCP/IP settings of administrator's computer to have a static **IP Address** of 192.168.1.10 and **Subnet Mask** of 255.255.255.0.

Step 1: Configuring the AP's System Information

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

The Web Management Interface will appear as shown below.

Overview Associated Clients WDS Link Status Event Log

Home > Status > System Overview

System Overview

System

System Name	Enterprise Access Point
Firmware Version	1.00.00
Build Number	1.5-1.6477
Location	
Site	EN-A
Device Time	1970/01/01 08:15:39
System Up Time	0 days, 0:15:39

Radio Status

MAC Address	00:1F:D4:02:32:F7
Band	802.11g+n
Channel	6
TX Power	Highest

LAN Interface

MAC Address	00:1F:D4:02:32:F6
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	192.168.1.254

AP Status

Profile Name	BSSID	ESSID	Security Type	Online Clients	Tun
VAP-1	00:1F:D4:02:32:F7	4ipnetAP-A1	Open	0	

CAPWAP

Status	Disabled
--------	----------

Web Management Interface Main Page (System Overview)

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

Home > System > General

System Information

Name : *

Description :

Location :

Time

Device Time : 1970/01/01 08:22:30

Time Zone :

Time : Enable NTP Manually set up

Set Date : Year Month Day

Set Time : Hour Min Sec

System Information Page

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

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

Time Zone :

Time : Enable NTP Manually set up

Set Date : Year Month Day

Set Time : Hour Min Sec

Manually Time Setup

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

Time Zone :

Time : Enable NTP Manually set up

NTP Server 1 : *

NTP Server 2 :

NTP Setup

Step 2: Configuring the AP's Network Settings

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

General Network Interface Port Management CAPWAP

Home > System > Network Interface

Network Settings

Mode : Static DHCP

IP Address : *

Netmask : *

Default Gateway : *

Primary DNS Server : *

Alternate DNS Server :

Layer2 STP : Disable Enable

Network Settings Page

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

Step 3: Configure the AP's Wireless General Settings

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

Home > Wireless > General

General Settings

Band : 802.11g+802.11n Pure 11n

Short Preamble : Disable Enable

Short Guard Interval : Disable Enable

Channel Width : 20 MHz

Channel : 6

Max Transmit Rate : Auto

Transmit Power : Highest

Beacon Interval : 100 *(100 - 500ms)

Transmission Rate Threshold : 0 kbps *(0:Disable. Only applicable when Max Transmit Rate is set to Auto)

Wireless General Settings Page

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

Step 4: Configuring Wireless Coverage (VAP-1)

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

System **Wireless** Firewall Utilities Status

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

Home > Wireless > VAP Overview

VAP Overview

VAP No.	ESSID	State	Security Type	MAC ACL	Advanced Settings
1	4ipnetAP-A1	Enabled	Open	Disabled	Edit
2	4ipnetAP-A2	Disabled	Open	Disabled	Edit
3	4ipnetAP-A3	Disabled	Open	Disabled	Edit
4	4ipnetAP-A4	Disabled	Open	Disabled	Edit
5	4ipnetAP-A5	Disabled	Open	Disabled	Edit
6	4ipnetAP-A6	Disabled	Open	Disabled	Edit
7	4ipnetAP-A7	Disabled	Open	Disabled	Edit
8	4ipnetAP-A8	Disabled	Open	Disabled	Edit

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 **Wireless** Firewall Utilities Status

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

Home > Wireless > VAP Config

VAP Configuration

Profile Name : VAP-1

VAP : Disable Enable

Profile Name : VAP-1

ESSID : 4ipnetAP-A1

VLAN ID : Disable Enable

VLAN ID : *(1 - 4094)

CAPWAP Tunnel Interface :

VAP Configuration Page

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

Congratulations!

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

4. Adding Virtual Access Points

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

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

VAP No.	ESSID	State	Security Type	MAC ACL	Advanced Settings
1	4ipnetAP-A1	Enabled	Open	Disabled	Edit
2	4ipnetAP-A2	Disabled	Open	Disabled	Edit
3	4ipnetAP-A3	Disabled	Open	Disabled	Edit
4	4ipnetAP-A4	Disabled	Open	Disabled	Edit
5	4ipnetAP-A5	Disabled	Open	Disabled	Edit
6	4ipnetAP-A6	Disabled	Open	Disabled	Edit
7	4ipnetAP-A7	Disabled	Open	Disabled	Edit
8	4ipnetAP-A8	Disabled	Open	Disabled	Edit

VAP Overview Page

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

Home > Wireless > VAP Config

VAP Configuration

Profile Name : VAP-1

VAP : Disable Enable

Profile Name : VAP-1

ESSID : 4ipnetAP-A1

VLAN ID : Disable Enable

VLAN ID : *(1 - 4094)

CAPWAP Tunnel Interface :

VAP Configuration Page (VAP-1 shown)

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

5. Securing the AP

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

Step 1: Ensure the intended VAP is Enabled

VAP No.	ESSID	State	Security Type	MAC ACL	Advanced Settings
1	4ipnetAP-A1	Enabled	Open	Disabled	Edit
2	4ipnetAP-A2	Disabled	Open	Disabled	Edit
3	4ipnetAP-A3	Disabled	Open	Disabled	Edit
4	4ipnetAP-A4	Disabled	Open	Disabled	Edit
5	4ipnetAP-A5	Disabled	Open	Disabled	Edit
6	4ipnetAP-A6	Disabled	Open	Disabled	Edit
7	4ipnetAP-A7	Disabled	Open	Disabled	Edit
8	4ipnetAP-A8	Disabled	Open	Disabled	Edit

VAP Overview Page

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

Home > Wireless > VAP Config

VAP Configuration

Profile Name : VAP-1

VAP : Disable Enable

Profile Name : VAP-1

ESSID : 4ipnetAP-A1

VLAN ID : Disable Enable

VLAN ID : *(1 - 4094)

CAPWAP Tunnel Interface :

VAP Configuration Page (RF Card A : VAP-1 as shown for example)

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

Step 2: Configure Security Settings for your VAP

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

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

Home > Wireless > Security

Security Settings

Profile Name : VAP-1

Security Type :

- Open
- WEP
- 802.1X
- WPA-Personal
- WPA-Enterprise

CLEAR

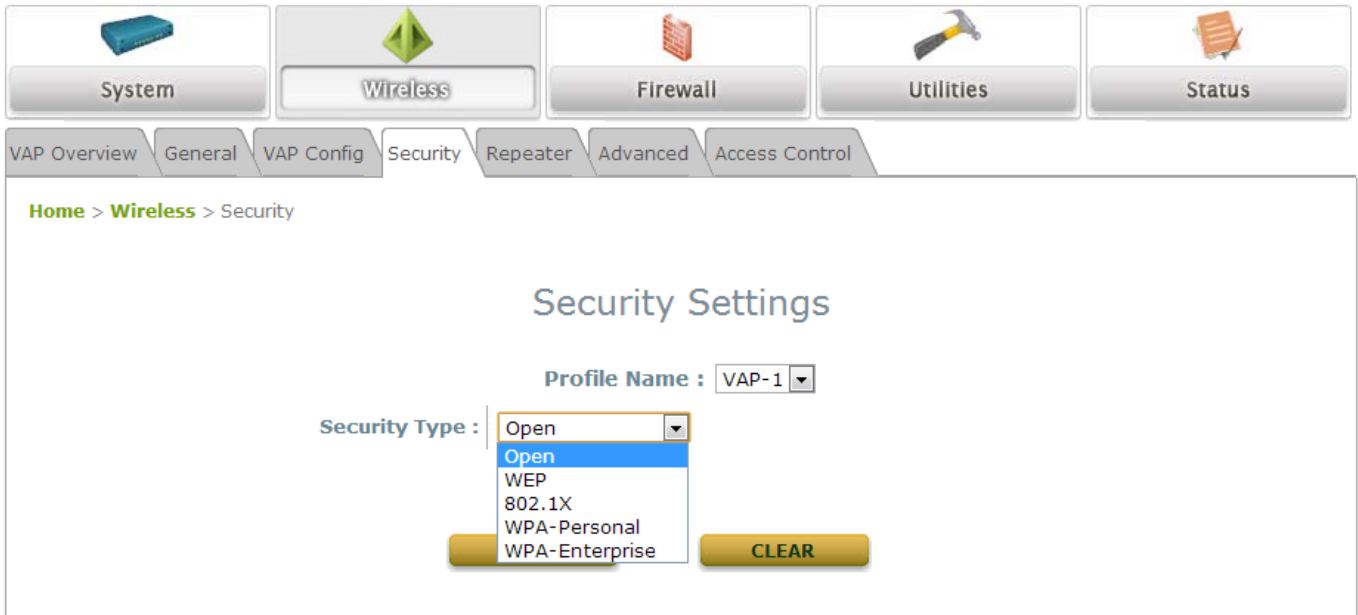
Security Settings Page (VAP-1 shown)

Select the desired **Security Type** from the drop-down menu, which includes **Open**, **WEP**, **802.1X**, **WPA-Personal**, and **WPA-Enterprise**.



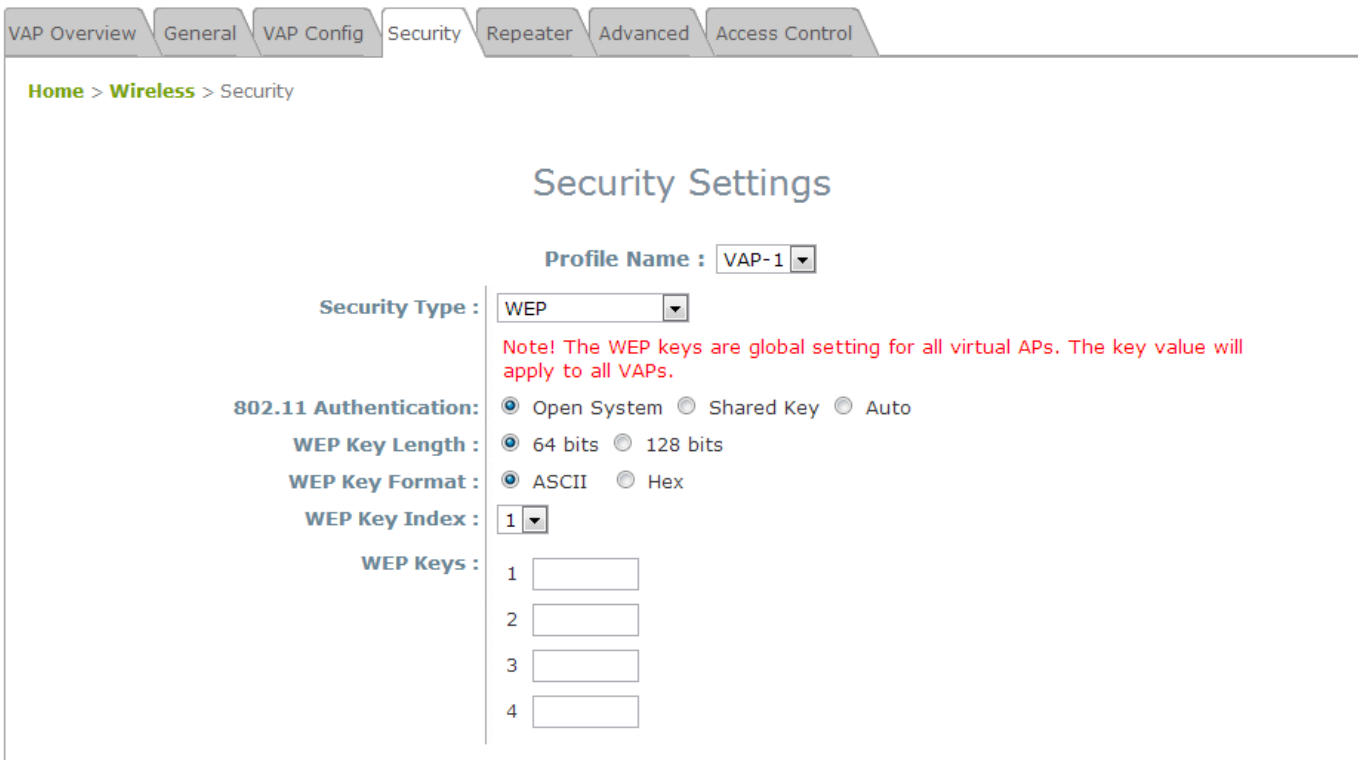
- *802.11n band does not support WEP nor WPA-PSK running TKIP. When the Security Type is set as such, the wireless link is only able to run at maximum 54Mbps.*

- **Open:** 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.



Security Settings: Open

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



Security Settings: WEP

- **802.11 Authentication:** Select from **Open System**, **Shared Key**, or **Auto**.
 - **WEP Key Length:** Select a key length from **64-bit**, **128-bit**, **152-bit**.
 - **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.

The screenshot shows the 'Security Settings' configuration page. At the top, there are tabs for 'VAP Overview', 'General', 'VAP Config', 'Security', 'Repeater', 'Advanced', and 'Access Control'. The 'Security' tab is active. Below the tabs, the breadcrumb 'Home > Wireless > Security' is visible. The main heading is 'Security Settings'. The 'Profile Name' is set to 'VAP-1'. The 'Security Type' is '802.1X'. Under 'Dynamic WEP', 'Enable' is selected. 'WEP Key Length' is set to '64 bits'. 'Rekeying Period' is '300 second(s)'. Under 'Primary RADIUS Server', 'Host' is empty with a red asterisk and the note '* (Domain Name / IP Address)'. 'Authentication Port' is '1812 *'. 'Secret Key' is empty with a red asterisk. 'Accounting Service' is 'Disable'. 'Accounting Port' is '1813 *'. 'Accounting Interim Update Interval' is '60 second(s)**'.

Security Settings: 802.1X Authentication

- **Dynamic WEP Settings:**
 - **Dynamic WEP:** For 802.1X security type, Dynamic WEP is always enabled to automatically generate WEP keys for encryption.
 - **WEP Key Length:** Select a key length from **64-bits** or **128-bits**.
 - **Re-keying Period:** The time interval for the dynamic WEP key to be updated; the time unit is in seconds.
- **RADIUS Server Settings (A redundant server can also be added to the system):**
 - **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-Personal:** Provides shared key authentication in WPA data encryption.

VAP Overview General VAP Config Security Repeater Advanced Access Control

Home > Wireless > Security

Security Settings

Profile Name : VAP-1

Security Type : WPA-Personal

Cipher Suite : WPA2

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

Pre-shared Key :

Group Key Update Period: 600 second(s)

Security Settings: WPA-Personal

- **Cipher Suite:** Select an encryption method from **WPA2**, or **WPA2/WPA**.
- **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-Enterprise:** Authenticates users by RADIUS and provides WPA data encryption.

VAP Overview General VAP Config Security Repeater Advanced Access Control

Home > Wireless > Security

Security Settings

Profile Name : VAP-1 ▾

Security Type : WPA-Enterprise ▾

Cipher Suite : WPA2 ▾

Group Key Update Period: 600 second(s)

Primary RADIUS Server :

Host : *(Domain Name / IP Address)

Authentication Port : 1812 *

Secret Key : *

Accounting Service : Disable Enable

Accounting Port : 1813 *

Accounting Interim Update Interval : 60 second(s)*

Security Settings: WPA-Enterprise

➤ **WPA Settings:**

- **Cipher Suite:** Select an encryption method from **WPA2** or **WPA2/WPA**.
- **Group Key Update Period:** The time interval for the Group Key to be renewed; the time unit is in seconds.

➤ **RADIUS Server Settings:**

- **Host:** Enter the IP address or domain name of the RADIUS server.
- **Authentication Port:** The port number used by the RADIUS server. Specify a port number or use the default, 1812.
- **Secret Key:** The secret key for the system to communicate with the RADIUS server.
- **Accounting Service:** Enabling this option allows accounting of login and logouts through the RADIUS server.
- **Accounting Port:** The port number used by the RADIUS server for accounting purposes. Specify a port number or use the default, 1813.
- **Accounting Interim Update Interval:** The system will update accounting information to the RADIUS server every interval period.

When these configurations are finished and MAC restriction is not needed, click **SAVE** and **Reboot** the system. Otherwise, click on the **Overview** tab and proceed to the next step. Note that the number of supported RADIUS Servers is model dependent.

Step 3: Configuring MAC ACL (Access Control List)

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

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

Home > Wireless > Access Control

Access Control Settings

Profile Name : VAP-1

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

Access Control Type :

Access Control Settings Page

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

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

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

Home > Wireless > Access Control

Access Control Settings

Profile Name : VAP-1

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

Access Control Type :

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

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

Home > Wireless > Access Control

Access Control Settings

Profile Name : VAP-1

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

Access Control Type : MAC ACL 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

MAC ACL Deny List

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

6. Creating a WDS Bridge between two APs

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

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

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

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

- Band :** 802.11g+802.11n (dropdown menu) Pure 11n
- Short Preamble :** Disable Enable
- Short Guard Interval :** Disable Enable
- Channel Width :** 20 MHz (dropdown menu)
- Channel :** 6 (dropdown menu)
- Max Transmit Rate :** Auto (dropdown menu)
- Transmit Power :** Highest (dropdown menu)
- Beacon Interval :** 100 *(100 - 500ms)
- Transmission Rate Threshold :** 0 kbps *(0:Disable. Only applicable when Max Transmit Rate is set to Auto)

Wireless General Settings Page

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

Step 2: Prevent Loops when Connecting Multiple APs

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

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

Home > System > Network Interface

Network Settings

Mode : Static DHCP

IP Address : *

Netmask : *

Default Gateway : *

Primary DNS Server : *

Alternate DNS Server :

Layer2 STP : Disable Enable

Network Settings Page

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

Step 3: Building the WDS Link

To extend the wireless coverage, each RF card supports up to 4 WDS links for connecting wirelessly to other WDS-capable APs (peer APs). By default, all WDS profiles are disabled.

Home > Wireless > Repeater Config

Repeater Settings

Repeater Type : WDS WES

WDS Profile : RF Card A : WDS Link 1

WDS : Disable

MAC Address :

Security type : None

CAPWAP Tunnel Interface :

1. Click on the **Wireless** button on the main menu.
2. Select the **Repeater Settings** tab.
3. Choose **WDS** as the **Repeater Type**.
4. Choose the desired WDS profile:
 - (a) Enable **WDS**.
 - (b) Enter the **MAC Address** (peer AP) and then Click **SAVE**.

If you are using another 4ipnet APs as the peer AP, simply repeat the above-mentioned steps to configure another peer AP(s).

►► **Note:** Cross brand/model WES/WDS link performance may vary with different Access Points depending on hardware compatibility.

7. Web Management Interface Configuration

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

Table 1 4ipnet Access Points' Function Organization

OPTION	FUNCTION
System	General
	Network Interface
	Port
	Management
	CAPWAP
Wireless	VAP Overview
	General
	VAP Config
	Security
	Repeater
	Advanced
	Access Control
Firewall	Firewall List
	Service
	Advanced
Utilities	Change Password
	Backup & Restore
	System Upgrade
	Reboot
	Upload Certificate
Status	Overview
	Associated Clients
	WDS Link Status
	Event Log

» Note:

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

All online users will be disconnected during reboot or restart.

7.1 System

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

General, Network Interface, Port, Management, and CAPWAP.

7.1.1 General

General Network Interface Port Management CAPWAP

Home > System > General

System Information

Name : Enterprise Access Point *

Description :

Location :

Time

Device Time : 1970/01/01 09:01:04

Time Zone : (GMT+08:00)Taipei

Time : Enable NTP Manually set up

Set Date : Year Month Day

Set Time : Hour Min Sec

System Information Page

- **System Information**

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

 - **Name:** The system name used to identify this system.
 - **Description:** Further information about the system (e.g. device model, firmware version, and active date).
 - **Location:** The information on geographical location of the system for the administrator to locate the system easily.
- **Time**
 - **Device Time:** Display the current time of the system.
 - **Time Zone:** Select an appropriate time zone from the drop-down list box.
 - **Time:** Synchronize the system time by reachable NTP servers or manual setup.
 - 1) **Enable NTP:**

By selecting **Enabled NTP**, the AP can synchronize its system time with the NTP server

automatically. When this method is chosen, at least one NTP server's IP address or domain name must be provided.

Time

Device Time : 2000/01/03 04:32:49
Time Zone : (GMT+08:00)Taipei
Time : Enable NTP Manually set up
NTP Server 1 : *
NTP Server 2 :

NTP Time Configuration Fields

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

2) Manually set up:

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

Time

Device Time : 2000/01/03 04:32:49
Time Zone : (GMT+08:00)Taipei
Time : Enable NTP Manually set up
Set Date : ---- Year -- Month -- Day
Set Time : -- Hour -- Min -- Sec

Manual Time Configuration Fields

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



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

7.1.2 Network Interface

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

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 AP is set up to bridge other network components, this option can be enabled to prevent undesired loops because a broadcasting storm may occur in a multi-switch environment where broadcast packets are forwarded in an endless loop between switches. Moreover, a broadcast storm may consume most of the available system resources in addition to available bandwidth. Thus, enabling the Layer 2 STP can lower such undesired occurrence and derive the best available data path for network communication.

7.1.3 Port

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

General
Network Interface
Port
Management
CAPWAP

Home > System > Port Config

Port Configuration

Port :
LAN1

VLAN ID :

 Disable
 Enable

VLAN ID :

*(1 - 4094)

CAPWAP Tunnel Interface :

TIP:
 *For tunneled LAN ports, Service Zones to VLAN ID Mappings are:
 Default Zone = 1000, SZ1 = 1001, SZ2 = 1002, SZ3 = 1003, SZ4 = 1004, SZ5 = 1005, SZ6 = 1006, SZ7 = 1007, SZ8 = 1008.
 *LAN port traffic tunneled back to a WHG Controller without a VLAN ID will be suspended from access to any network service.

- **VLAN ID:** Enable selected implies that network traffic sent upstream from this LAN port will be tagged with the VLAN ID configured in the field below. Disable selected implies that traffic from this LAN port will not be tagged with a VLAN ID.
- **CAPWAP Tunnel Interface:** Select a LAN, VAP or WDS interface to designate its traffic to pass through the CAPWAP Tunnel established between the AP and the controller. For network interfaces that are unchecked, their traffic will be forwarded locally into the internet if this AP is deployed remotely on the WAN side of a controller.
- The '**TIP**' in red at the bottom of the page explains that each service zone, from default to Service Zone 8, has its fixed, pre-determined VLAN ID number when utilizing CAPWAP. Admin needs to enter one of the numbers in order to direct traffic back to a certain Service Zone.

7.1.4 Management

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

General
Network Interface
Port
Management
CAPWAP

[Home](#) > [System](#) > Management Services

Management Services

VLAN for Management:

SNMP Configuration :

System Log :

Disable Enable
 VLAN ID : *(1 - 4094)

Disable Enable
 Community String :
 Read :
 Write :

Trap : Disable Enable
 Server IP :

Disable Enable
 SYSLOG Server IP :
 Server Port :
 SYSLOG Level :

Management Services Page

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

-
-
-

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

SNMP Configuration :

Disable Enable

Community String :

Read :

Write :

Trap : Disable Enable

Server IP :

SNMP Configuration Fields

- **Enable/ Disable:** *Enable* or *Disable* this function.
 - **Community String:** The community string is required when accessing the Management Information Base (MIB) of the system.
 - **Read:** Enter the community string to access the MIB with Read privilege.
 - **Write:** Enter the community string to access the MIB with Write privilege.
 - **Trap:** When enabled, events on Cold Start, Interface UP & Down, and Association & Disassociation can be reported to an assigned server.
 - **Enable/ Disable:** *Enable* or *Disable* this function.
 - **Server IP Address:** Enter the IP address of the assigned server that will receive the trap report.
- **System Log:** When this function is enabled, specify an external SYSLOG server to accept SYSLOG messages from the system remotely.

System Log :

Disable Enable

SYSLOG Server IP :

Server Port :

SYSLOG Level : ▼

System Log Fields

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

7.1.5 CAPWAP

CAPWAP is a standard interoperable protocol that enables a controller to manage a collection of wireless access points. There are 5 methods of auto AP discovery, namely DNS SRV, DHCP option, Broadcast, Multicast, and Static. Please refer to the Web page at **System > CAPWAP**.

General
Network Interface
Port
Management
CAPWAP

Home > System > CAPWAP

CAPWAP Configuration

CAPWAP : Disable Enable

Certificate Date Check: Disable Enable Manage Certificates

DNS SRV Discovery : Disable Enable

Domain Name Suffix :

DHCP Option Discovery : Disable Enable

Broadcast Discovery : Disable Enable

Multicast Discovery : Disable Enable

Static Discovery : Disable Enable

Pri.	AC Address	Remark
1	<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>
2	<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>
3	<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>
4	<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>
5	<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>

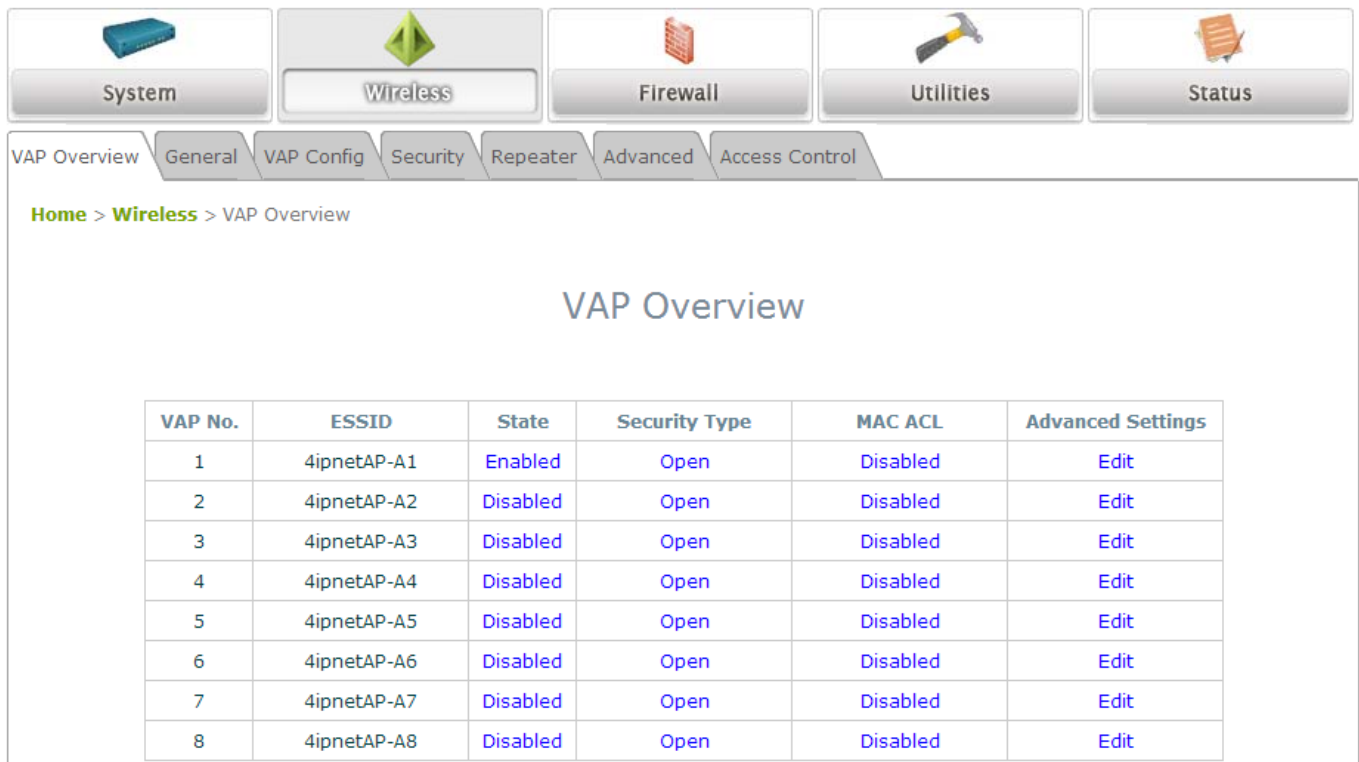
- **CAPWAP:** The CAPWAP feature can be turned on by selecting “Enable” or turned off by selecting “Disable”
- **Certificate Date Check:** To enable this item, select **Enable** and click **Manage Certificates** to enter the **Upload Certificate** page. Please refer to the section **7.4.4. Upload Certificate**.
- **DNS SRV Discovery:** Using DNS SRV to discover access controller.
 - **Domain Name Suffix:** Enter the suffix of the access controller, such as example.com.
- **DHCP Option Discovery:** Using DHCP option to discover access controller.
- **Broadcast Discovery:** Using Broadcast to discover access controller.
- **Multicast Discovery:** Using muticast to discover access controller.
- **Static Discovery:** Using Static approach to discover access controller.
 - **AC Address:** The IP address of the access controller. If it can not discover the first AC, it will try to discover the second AC.

7.5 Wireless

This section includes the following functions: **VAP Overview**, **General**, **VAP Configuration**, **Security**, **Repeater**, **Advanced**, and **Access Control**. The 4ipnet Access Point supports up to eight Virtual Access Points (VAPs) per RF card. 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 the AP features 8 VAPs with respective settings. In this table, please click on the hyperlink to further configure each individual VAP.



The screenshot displays the VAP Overview page. At the top, there are five main navigation buttons: System, Wireless (selected), Firewall, Utilities, and Status. Below these are sub-navigation tabs for VAP Overview, General, VAP Config, Security, Repeater, Advanced, and Access Control. The breadcrumb path is Home > Wireless > VAP Overview. The main heading is 'VAP Overview'. Below the heading is a table with the following data:

VAP No.	ESSID	State	Security Type	MAC ACL	Advanced Settings
1	4ipnetAP-A1	Enabled	Open	Disabled	Edit
2	4ipnetAP-A2	Disabled	Open	Disabled	Edit
3	4ipnetAP-A3	Disabled	Open	Disabled	Edit
4	4ipnetAP-A4	Disabled	Open	Disabled	Edit
5	4ipnetAP-A5	Disabled	Open	Disabled	Edit
6	4ipnetAP-A6	Disabled	Open	Disabled	Edit
7	4ipnetAP-A7	Disabled	Open	Disabled	Edit
8	4ipnetAP-A8	Disabled	Open	Disabled	Edit

VAP Overview Page

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

Home > Wireless > VAP Config

VAP Configuration

Profile Name : VAP-1

VAP : Disable Enable

Profile Name : VAP-1

ESSID : 4ipnetAP-A1

VLAN ID : Disable Enable

VLAN ID : *(1 - 4094)

CAPWAP Tunnel Interface :

VAP – State Page

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

Home > Wireless > Security

Security Settings

Profile Name : VAP-1

Security Type : Open

Open
WEP
802.1X
WPA-Personal
WPA-Enterprise

CLEAR

VAP – Security Type Page

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

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

Home > Wireless > Access Control

Access Control Settings

Profile Name :

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

Access Control Type :

VAP – MAC ACL Page

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


System


Wireless


Firewall


Utilities


Status

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

Home > Wireless > Advanced

Advanced Wireless Settings

Profile Name :

RTS Threshold : *(1 - 2346)

DTIM period : *(1 - 15)

Broadcast SSID : Disable Enable

Wireless Station Isolation : Disable Enable

WMM : Disable Enable

IGMP Snooping : Disable Enable

VAP – Advanced Settings Page

7.2.2 General

AP's general wireless settings can be configured here:

Home > Wireless > General

General Settings

Band : 802.11g+802.11n Pure 11n

Short Preamble : Disable Enable

Short Guard Interval : Disable Enable

Channel Width : 20 MHz

Channel : 6

Max Transmit Rate : Auto

Transmit Power : Highest

Beacon Interval : 100 *(100 - 500ms)

Transmission Rate Threshold : 0 kbps *(0:Disable. Only applicable when Max Transmit Rate is set to Auto)

AP General Settings Page

- **Band:** Select an appropriate wireless band: **802.11a**, **802.11b**, **802.11g**, **802.11b+802.11g**, **802.11g+802.11n**, **802.11a+802.11n** or select **Disable** if the wireless function is not required.
 - **Pure 11n:** Enable 802.11n network only.
- **Short Preamble:** The short preamble with a 56-bit synchronization field can improve WLAN transmission efficiency. Select **Enable** to use Short Preamble or **Disable** to use Long Preamble with a 128-bit synchronization field.
- **Short Guard Interval (available when Band is 802.11g+802.11n or 802.11a+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 or 802.11a+802.11n):** Double channel bandwidth to 40 MHz to enhance throughput.
- **Channel:** Select the appropriate **channel** from the drop-down menu to correspond with your network settings, for example, Channel 1-11 is available in North American and Channel 1-13 in Europe, or choose the default **6**.
- **Max Transmit Rate:** The maximum wireless transmit rate can be selected from the drop-down menu. The system will use the highest possible rate when **Auto** is selected. Please note that MCS0 ~ MCS15 are transmit rates only for n bands.

- **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.
- **Beacon Interval (ms):** The entered amount of time indicates how often the beacon signal will be sent from the access point.
- **Transmission Rate Threshold:** The client will be kicked when transmission rate is lower than the configured threshold. This ensures high connection speed for all associated clients. Note that this feature is only applicable when Max. Transmit Rate is set to Auto.

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

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

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

7.2.3 VAP Configuration

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

Home > Wireless > VAP Config

VAP Configuration

Profile Name :

VAP : Disable Enable

Profile Name :

ESSID :

VLAN ID : Disable Enable

VLAN ID : *(1 - 4094)

CAPWAP Tunnel Interface :

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 a specific RF card and its 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 levels like a variety of wireless security types.
- **VLAN ID:** The 4ipnet Access Point 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.
- **CAPWAP Tunnel Interface:** Select Checkbox to designate traffic for the VAP to pass through CAPWAP Tunnel established between the AP and the controller.

7.2.4 Security

The Access Point 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 **Open**, **WEP**, **802.1X**, **WPA-Personal**, and **WPA-Enterprise**.

- **Open:** 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 displays the configuration page for the 'Security' settings of a VAP profile named 'VAP-1'. The breadcrumb trail is 'Home > Wireless > Security'. The page title is 'Security Settings'. The 'Profile Name' is set to 'VAP-1'. The 'Security Type' dropdown menu is open, showing the following options: Open (selected), WEP, 802.1X, WPA-Personal, and WPA-Enterprise. There is a 'CLEAR' button next to the dropdown menu.

Security Settings: Open

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

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

Home > Wireless > Security

Security Settings

Profile Name : VAP-1

Security Type : WEP

Note! The WEP keys are global setting for all virtual APs. The key value will apply to all VAPs.

802.11 Authentication: Open System Shared Key Auto

WEP Key Length : 64 bits 128 bits

WEP Key Format : ASCII Hex

WEP Key Index : 1

WEP Keys :

1

2

3

4

Security Settings: WEP

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

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

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

Home > Wireless > Security

Security Settings

Profile Name :

Security Type :

Dynamic WEP : Disable Enable

WEP Key Length : 64 bits 128 bits

Rekeying Period : second(s)

Primary RADIUS Server :

Host : *(Domain Name / IP Address)

Authentication Port : *

Secret Key : *

Accounting Service : Disable Enable

Accounting Port : *

Accounting Interim Update Interval : second(s)*

Security Settings: 802.1X Authentication

➤ **Dynamic WEP Settings:**

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

➤ **RADIUS Server Settings:**

- **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-Personal:** WPA-Personal is a pre-shared key authentication method.

VAP Overview General VAP Config Security Repeater Advanced Access Control

Home > Wireless > Security

Security Settings

Profile Name : VAP-1

Security Type : WPA-Personal

Cipher Suite : WPA2

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

Pre-shared Key :

Group Key Update Period: 600 second(s)

Security Settings: WPA-Personal

- **Cipher Suite:** Select an encryption method from **WPA2** or **WPA2/WPA**.
- **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-Enterprise:** If this option is selected, the RADIUS authentication and data encryption will both be enabled.

VAP Overview General VAP Config Security Repeater Advanced Access Control

Home > Wireless > Security

Security Settings

Profile Name : VAP-1

Security Type : WPA-Enterprise

Cipher Suite : WPA2

Group Key Update Period: 600 second(s)

Primary RADIUS Server :

Host : *(Domain Name / IP Address)

Authentication Port : 1812 *

Secret Key : *

Accounting Service : Disable Enable

Accounting Port : 1813 *

Accounting Interim Update Interval : 60 second(s)*

Security Settings: WPA-Enterprise

➤ WPA Settings:

- **Cipher Suite:** Select an encryption method from **WPA2** or **WPA2/WPA**.
- **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.

7.2.5 Repeater

4ipnet Access Points are capable of utilizing WDS to extend wireless network coverage.

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

Home > Wireless > Repeater Config

Repeater Settings

Repeater Type : WDS

WDS Profile : RF Card A : WDS Link 1

WDS : Disable

MAC Address :

Security type : None

CAPWAP Tunnel Interface :

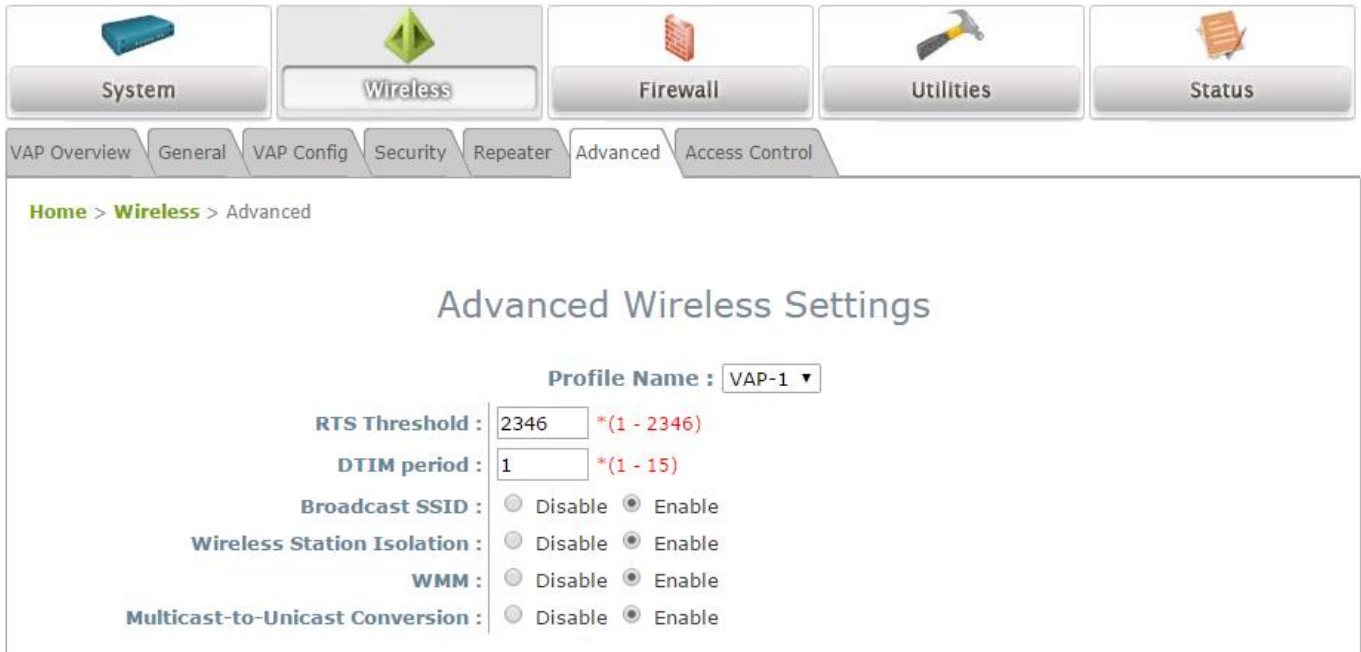
SAVE CLEAR

Repeater Settings: WDS

- **WDS:** Select **Enable** to enable the respective WDS links; Select **Disable** to remove them.
- **MAC Address:** To input remote peer's MAC address.
- **Security Type:** None, WEP, or WPA-PSK.
- **CAPWAP Tunnel Interface:** Select Checkbox to designate WDS traffic to pass through CAPWAP Tunnel established between the AP and the controller.

7.2.6 Advanced

The advanced wireless settings for the Access Point'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 > Wireless > Advanced

Advanced Wireless Settings

Profile Name : VAP-1 ▼

RTS Threshold : 2346 *(1 - 2346)

DTIM period : 1 *(1 - 15)

Broadcast SSID : Disable Enable

Wireless Station Isolation : Disable Enable

WMM : Disable Enable

Multicast-to-Unicast Conversion : Disable Enable

Advanced Wireless Settings Page

- **RTS Threshold:** Enter a value between 1 and 2346. RTS (Request to Send) Threshold determines the packet size at which the system issues a request to send (RTS) before sending the fragment to prevent the hidden node problem. The RTS mechanism will be activated if the data size exceeds the value provided. A lower RTS Threshold setting can be useful in areas where many client devices are associating with the AP or in areas where the clients are far apart and can detect only the AP but not each other.
- **Fragment Threshold (802.11a, 802.11b and 802.11g Modes):** Enter a value between 256 and 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 allow the wireless client to save more energy, but the throughput will be lowered.
- **Broadcast SSID:** Disabling this function will stop 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 the Access Point.
 - WMM shall be enabled in the wireless adapter on client's computer.
- **Multicast-to-Unicast Conversion:** When Multicast-to-Unicast Conversion is enabled, IGMP packets are transferred via the Access Point's network interface and the IP multicast host. Registration information is recorded and sorted into multicast groups. The internal switch can then intelligently forward traffic only to those ports that request multicast traffic. Adversely, without this feature, multicast traffic is treated like broadcast traffic, with packets forwarded to all ports causing network inefficiencies.

7.5.4 Access Control

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

System Wireless Firewall Utilities Status

VAP Overview General VAP Config Security Repeater Advanced Access Control

Home > Wireless > Access Control

Access Control Settings

Profile Name : VAP-1

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

Access Control Type : Disable Access Control

Access Control Settings Page

- **Maximum Number of Clients**

The 4ipnet Access Point supports various methods of authenticating clients for wireless LAN access. The default policy is unlimited access without any authentication requirement. To restrict the station number of wireless connections, simply change the **Maximum Number of Stations** to a desired number. For example, when the number of stations is set to 20, only 20 stations are allowed to connect to the specified VAP.

• **Access Control Type**

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

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

Home > Wireless > Access Control

Access Control Settings

Profile Name : VAP-1

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


Access Control Type : MAC ACL 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


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 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**.


System


Wireless


Firewall


Utilities


Status

VAP Overview

General

VAP Config

Security

Repeater

Advanced

Access Control

Home > Wireless > Access Control

Access Control Settings

Profile Name : VAP-1

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

Access Control Type : MAC ACL Deny List

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

Deny List

7.3 Firewall

The system provides an added security feature, Layer2 Firewall, in addition to the typical AP security. Layer2 Firewall offers a firewall function that is tailored specifically for Layer2 traffic, 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 Lists**, **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 a total of 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	IEEE_8023		Del Ed In Mv
2	<input type="checkbox"/>	DROP	STP	IEEE_8023		Del Ed In Mv
3	<input type="checkbox"/>	DROP	GARP	IEEE_8023		Del Ed In Mv

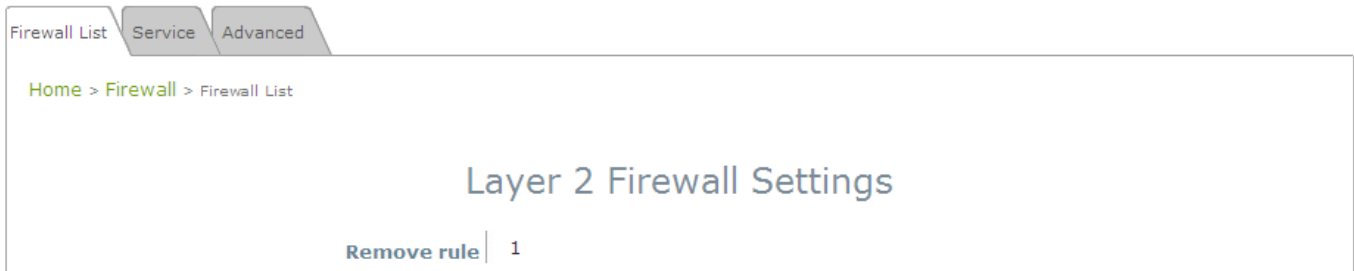
Firewall List Page

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

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

>>To delete a specific rule,

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



>>To edit a specific rule,

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

- **Rule ID:** The numbering of this specific rule will decide its priority among available firewall rules in the table.
- **Rule name:** The rule name can be specified here.
- **EtherType:** The drop-down list will provide the available types of traffic subjected to this rule.
- **Interface:** It indicates inbound/outbound direction with desired interfaces.
- **Service** (when EtherType is **IPv4**): Select the available upper layer protocols/services from the drop-down list.
- **DSAP/SSAP** (when EtherType is **IEEE 802.3**): The value can be further specified for the fields in 802.2 LLC frame header.
- **Type** (when EtherType is **IEEE802.3**): The field can be used to indicate the type of encapsulated traffic.
- **VLAN ID** (when EtherType is **802.1 Q**): The VLAN ID is provided to associate with certain VLAN-tagging traffic.
- **Priority** (when EtherType is **802.1 Q**): It denotes the priority level with associated VLAN traffic.
- **Encapsulated Type** (when EtherType is **802.1 Q**): It can be used to indicate the type of encapsulated traffic.
- **Opcode** (when EtherType is **ARP/RARP**): This list can be used to specify the ARP Opcode in ARP header.
- **Source:** MAC Address/Mask indicates the source MAC; IP Address/Mask indicates the source IP address (when EtherType is **IPv4**); ARP IP/MAC & MASK indicate the ARP payload fields.
- **Destination:** MAC Address/Mask indicates the destination MAC; IP Address/Mask indicates the destination IP address (when EtherType is **IPv4**); ARP IP/MAC & MASK indicate the ARP payload fields.

- **Action:** The rule can be chosen to be **Block** or **Pass**.
- **Remark:** Any note of this rule can be specified here.

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

>>To insert a specific rule,

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

From this page, a rule can be added or edited from an existing rule for revision.

>>To move a specific rule,

Mv in the **Setting** column of the firewall list will lead to the following page for reordering confirmation.

After the **SAVE** button is clicked and system is rebooted, the order of rules will be updated.

The screenshot shows the 'Move Rule' configuration page. At the top, there are three tabs: 'Firewall List', 'Service', and 'Advanced'. Below the tabs is a breadcrumb trail: 'Home > Firewall > Move rule'. The main heading is 'Move Rule'. Below the heading, there is a form with the following fields:

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

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

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 services here; the services in this list will become options to choose in firewall rule (when EtherType is IPv4).

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

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

Firewall List
Service
Advanced

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

Firewall Service

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

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

Firewall Service Page

7.3.3 Advanced

At **Firewall > Advanced**, more advanced settings on firewall rules can be configured, providing extra security enhancement against DHCP and ARP traffic traversing the available interfaces of the system.

- **Trust Interface:** Each VAP interface can be checked individually to mark as trusted interfaces; security enforcements on DHCP/ARP like DHCP snooping and ARP inspection will be carried out on non-trusted interfaces.
- **DHCP Snooping:** When enabled, DHCP packets will be validated against possible threats like DHCP starvation attack; in addition, the trusted DHCP server (IP/MAC) can be specified to prevent rouge DHCP server.
- **ARP Inspection:** When enabled, ARP packets will be validated against ARP spoofing.
 - **Proxy ARP** option when enabled, AP will reply ARP requests on behalf of downlink stations. The ARP table maintained by the AP will be used as a look up table upon receipt of ARP request from AP uplink. Adversely, without Proxy ARP, ARP request is broadcasted down into the AP's wireless network causing network inefficiencies.
 - **Force DHCP** option when enabled, the AP only learns MAC/IP pair information through DHCP packets. Since devices configured with static IP address does not send DHCP traffic, any clients with static IP address will be blocked from internet access unless its MAC/IP pair is listed and enabled on the **Static Trust List**.
 - **Trust List Broadcast** can be enabled to let other APs (with L2 firewall feature) learn the trusted MAC/IP pairs to issue ARP requests.
 - **Static Trust List** can be used to add MAC or MAC/IP pairs of devices that are trusted to issue ARP request. Other network nodes can still send their ARP requests; however, if their IP appears on the static list (with different MAC), their ARP requests will be dropped to prevent eavesdropping.

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

7.4 Utilities

The following utility features on this page allow the administrator to maintain the system: **Change Password**, **Backup & Restore**, **System Upgrade**, **Reboot**, and **Upload Certificate**.

7.4.1 Change Password

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

The screenshot shows the 'Utilities' section of the web management interface. At the top, there are five main utility buttons: System, Wireless, Firewall, Utilities (highlighted), and Status. Below these are five sub-buttons: Change Password, Backup & Restore, System Upgrade, Reboot, and Upload Certificate. The 'Change Password' sub-button is selected, leading to a page with the breadcrumb 'Home > Utilities > Change Password'. The main heading is 'Change Password'. The form contains the following fields:

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

Change Password Page

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

7.4.2 Backup & Restore

This function is used to backup and restore the Access Point's settings. The AP can also be restored to factory default 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).

Home > Utilities > Config Save & Restore

Configuration Backup & Restore

Reset to Default:

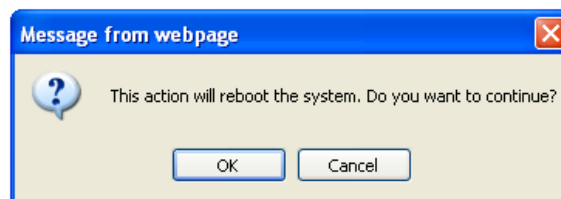
Backup System Settings:

Restore System Settings: No file selected.

Backup & Restore Page

- **Reset to Default:**

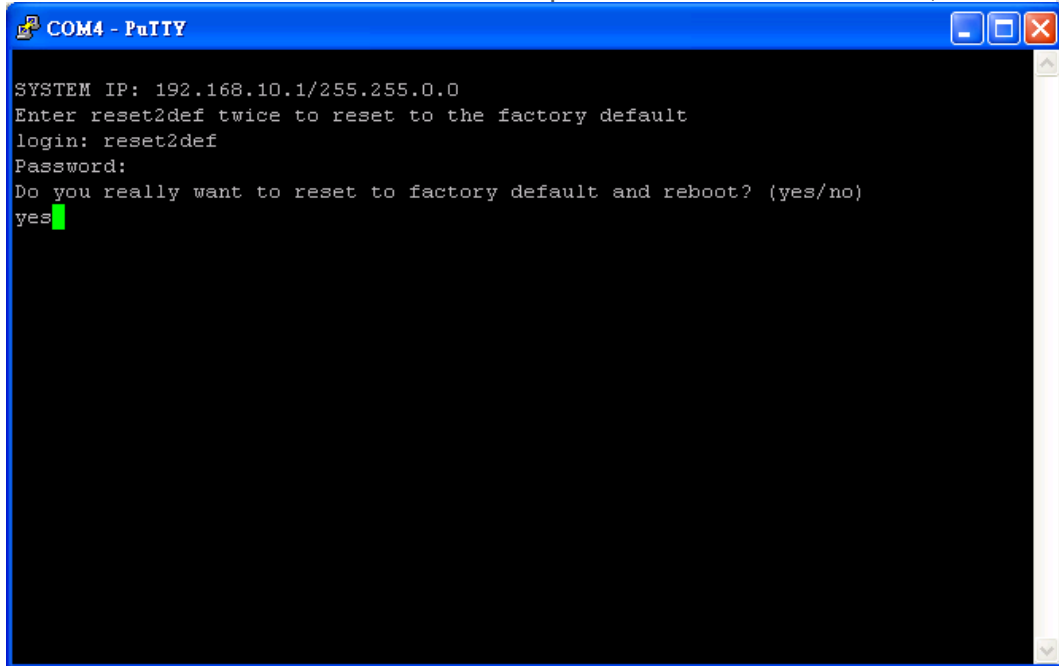
- Click **Reset** to load the factory default settings of the Access Point. A pop-up Page will appear to re-confirm the request to reboot the system. Click **OK** to proceed, or click **Cancel** to cancel the reboot request.



Reboot Confirmation Prompt

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

The system can be reset to default from the console interface (COM Port connection) should the administrator forget the AP's IP address. With the right baud rate and a termination simulation program such as PuTTY or Hyper Terminal, a login prompt should be seen as such:



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

Login as “reset2def” and enter “reset2def” as your password. Type “yes” to reset the AP to factory default.

If the console connection is not readily available, the IP address of the AP can be retrieved with an IP Discovery Utility provided by 4ipnet. Simply connect via an Ethernet cable and run the Discovery Utility. Note that the laptop/PC connecting to the AP must run in Windows XP compatible mode and a static IP must be set.

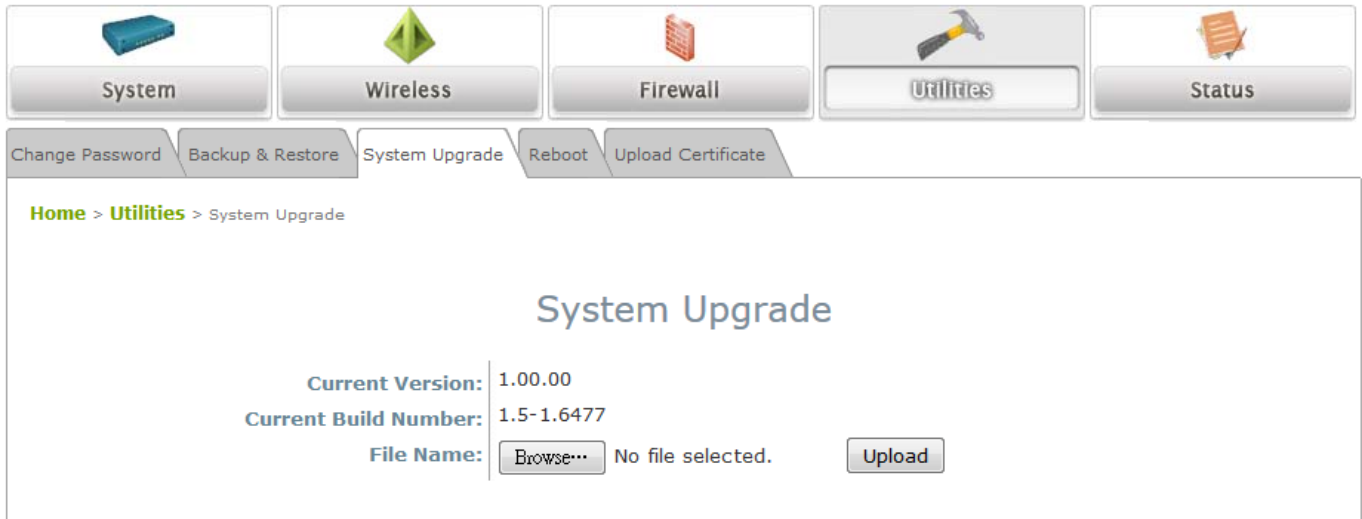
- **Backup System Settings:** Click **Backup** to save the current system settings to a local disk such as the hard disk drive (HDD) of a local computer or a compact disc (CD).
- **Restore System Settings:** Click **Browse** to search for a previously saved backup file, and then click **Upload** to restore 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 AP.

7.4.3 System Upgrade

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



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

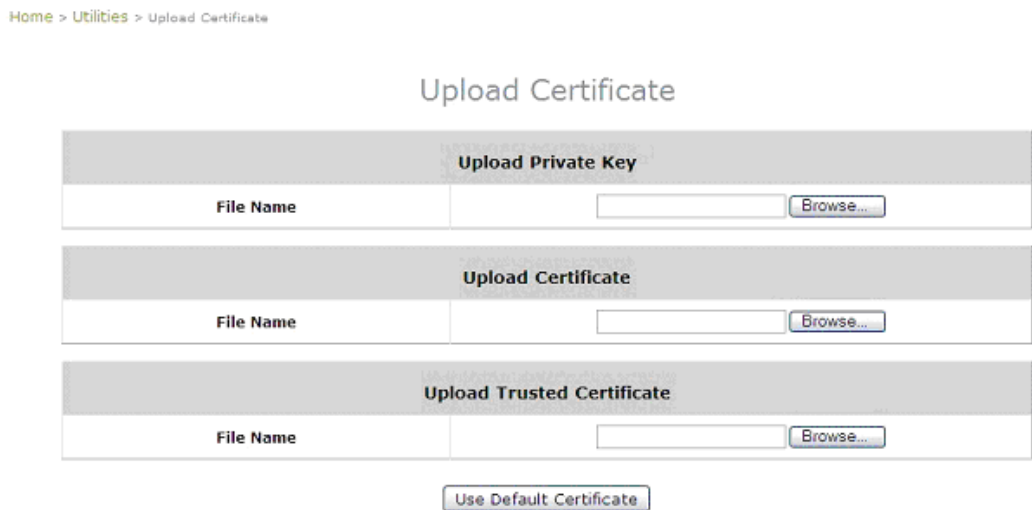
Occasionally, it is necessary to reboot the AP to ensure that parameter changes are submitted.



Reboot Page

7.4.5 Upload Certificate

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



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

7.5 Status

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

7.5.1 Overview

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

Overview
Associated Clients
WDS Link Status
Event Log

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

System Overview

System

System Name	Enterprise Access Point
Firmware Version	1.00.00
Build Number	1.5-1.6477
Location	
Site	EN-A
Device Time	1970/01/01 08:15:39
System Up Time	0 days, 0:15:39

Radio Status

MAC Address	00:1F:D4:02:32:F7
Band	802.11g+n
Channel	6
TX Power	Highest

LAN Interface

MAC Address	00:1F:D4:02:32:F6
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	192.168.1.254

AP Status

Profile Name	BSSID	ESSID	Security Type	Online Clients	Tun
VAP-1	00:1F:D4:02:32:F7	4ipnetAP-A1	Open	0	

CAPWAP

Status	Disabled
--------	----------

System Overview Page

Table 3 Status Page's Organizational Layout

Item		Description
System	System Name	The system name of the Access Point.
	Firmware Version	The current firmware version of the Access Point.
	Build Number	The current firmware build number of the Access Point.
	Location	The location of the Access Point.
	Site	The site of the Access Point.
	Device Time	The system time of the Access Point.
	System Up Time	The time that the system has been in operation.
LAN Interface	MAC Address	The MAC address of the LAN Interface.
	IP Address	The IP address of the LAN Interface.
	Subnet Mask	The Subnet Mask of the LAN Interface.
	Gateway	The Gateway of the LAN Interface.
Radio Status	MAC Address	The MAC address of the RF Card.
	Band	The RF band in use.
	Channel	The channel specified.
	Tx Power	Transmit Power level of RF card.
AP Status	Profile Name	The profile name of AP.
	BSSID	Basic Service Set ID.
	ESSID	Extended Service Set ID.
	Security Type	Security type of the Virtual AP.
	Online Clients	The number of online clients.
	Tunnel	The status of the used Tunnel.
CAPWAP	Status	Enabled/ Disabled.

7.5.2 Associated Clients

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

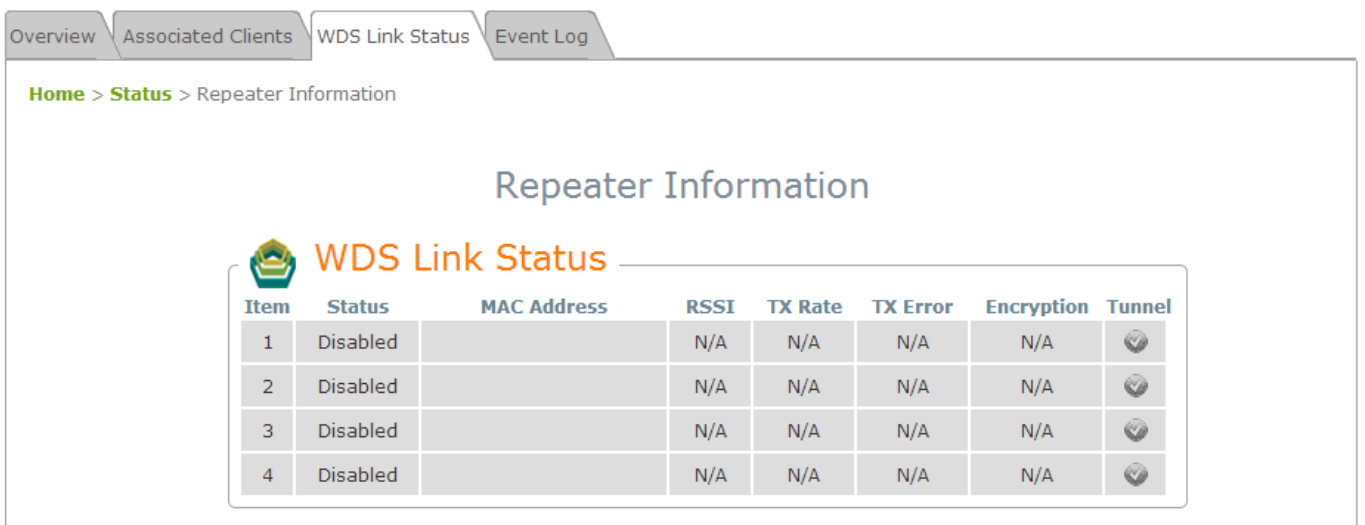


Associated Client Status Page

- **Associated VAP:** The name of a VAP (Virtual Access Point) that the client is associated with.
- **ESSID:** The Extended Service Set ID which the client is associated with.
- **MAC Address:** The MAC address of associated clients.
- **SNR:** The Signal to Noise Ratio of respective client's association.
- **Idle Time:** Time period that the associated client is inactive for; the time unit is in seconds.
- **Disconnect:** Upon clicking **Kick**, the client will be disconnected from the system.

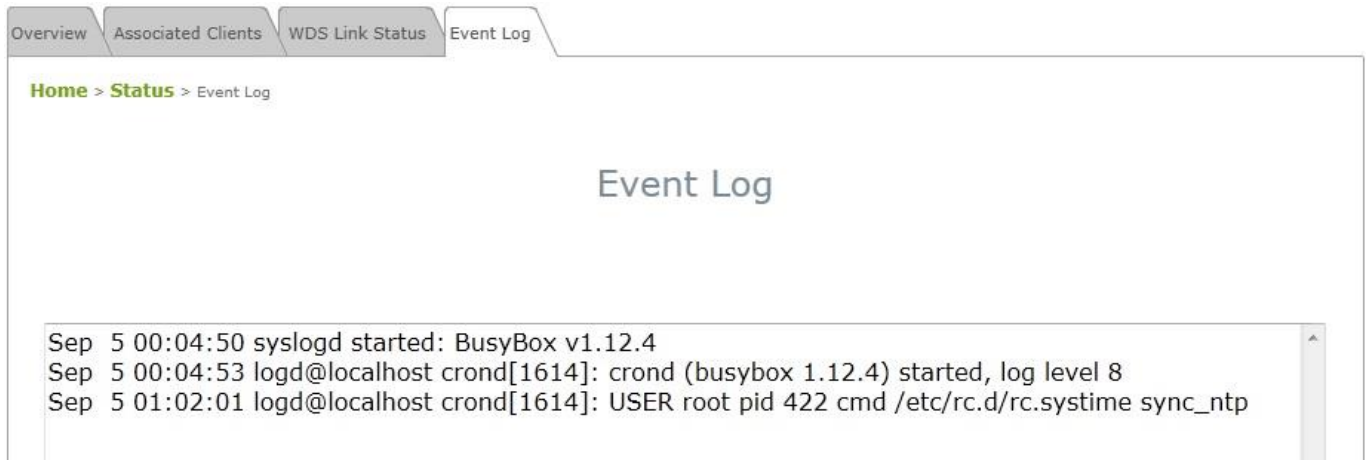
7.5.3 WDS Link Status

The administrator can review detailed information of the repeater function at **Status > WDS Link Status**. Information of WDS status, traffic statistics, encryption and other details are provided.



7.5.4 Event Log

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



Event Log Page

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

- **Date / Time:** The time & date when the event happened.
- **Hostname:** Indicates which host recorded this event. Note that all events on this page are local events, so the hostname in this field is always the same. In remote SYSLOG service however, this field will help the administrator identify which event is from this Access Point.
- **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**.

8. Console Interface Configuration

Via the console port, administrators are able to enter the console interface to reset the access point to its factory default settings. In order to connect to the console port of a 4ipnet access point, a console, modem cable, and a terminal simulation program, such as PuTTY are needed. There are 2 ways to access the console interface:

1. Direct Connection (EAP717 Only)

Notebook > USB-to-RS232 with DB9 connector > Console Cable > Console Port

The USB-to-RS232 cable is not supplied with standard packaging. It is recommended to use only the console cable provided with the packaging.



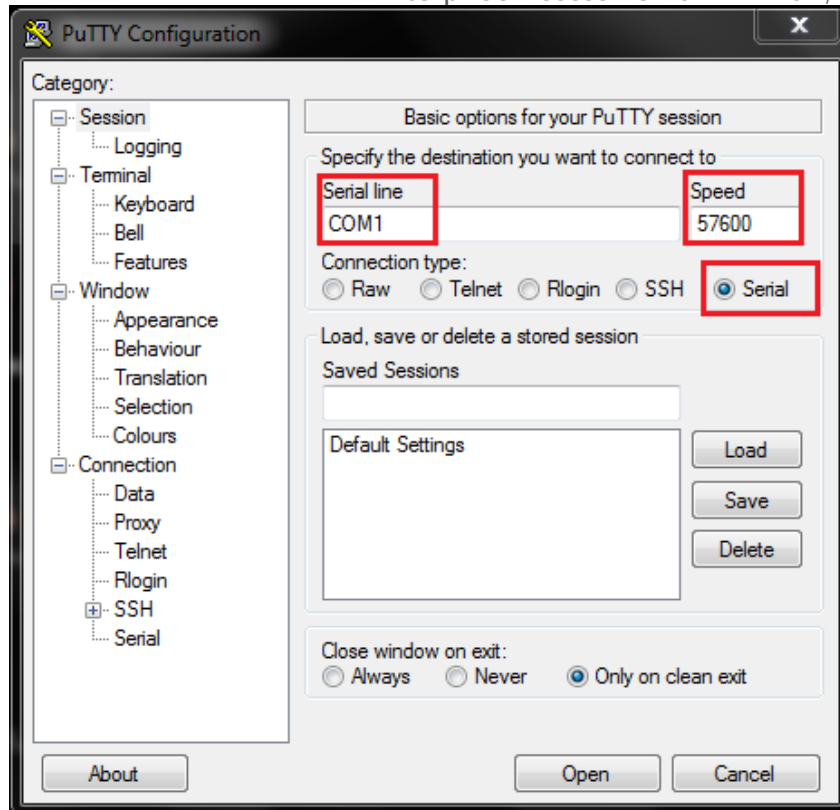
USB-RS232



Console Cable – RJ45

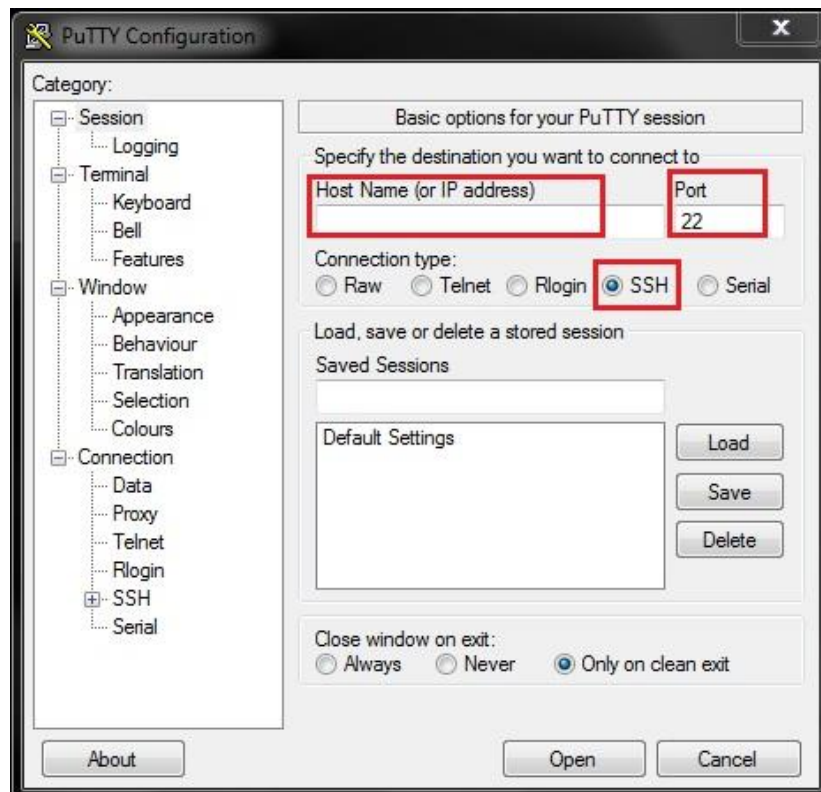
The speed (baud rate) needs to be selected for direct connections and the baud rate is as follows:

Model	Baud Rate (bps)
EAP717	57600

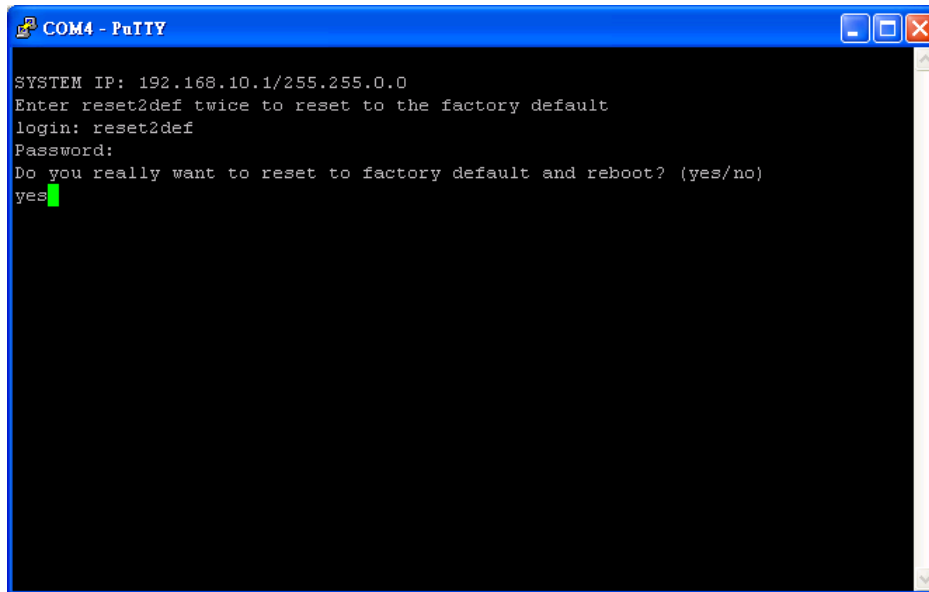


2. Remote Connection

The system supports access to the console interface via SSH. Typically SSH utilizes Port 22 and would require the WAN IP address for access.



To reset the system to factory default through the console interface, Login as “reset2def” and enter “reset2def” as your password.



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

If the console connection is not readily available, the IP address of the AP can be retrieved with an IP Discovery Utility provided by 4ipnet. Simply connect via an Ethernet cable and run the Discovery Utility. Note that the laptop/PC connecting to the AP must run in Windows XP compatible mode and a static IP must be set.

P/N: V11120150311