DrayTek

VigorAP 920R Series

Ruggedized Outdoor AP with Extreme 802.11ac Power

USER'S GUIDE

V1.2

VigorAP 920R Series

Ruggedized Outdoor AP with Extreme 802.11ac Power

User's Guide

Version: 1.2

Firmware Version: V1.3.3

Date: May 12, 2020

Intellectual Property Rights (IPR) Information

Copyrights

© All rights reserved. This publication contains information that is protected by copyright. No part may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language without written permission from the copyright holders.

Trademarks

The following trademarks are used in this document:

- Microsoft is a registered trademark of Microsoft Corp.
- Windows, Windows 7,8, 10 and Explorer are trademarks of Microsoft Corp.
- Apple and Mac OS are registered trademarks of Apple Inc.
- Other products may be trademarks or registered trademarks of their respective manufacturers.

Safety Instructions and Approval

Safety Instructions

- Read the installation guide thoroughly before you set up the modem.
- The modem is a complicated electronic unit that may be repaired only be authorized and qualified personnel. Do not try to open or repair the modem yourself.
- Do not place the modem in a damp or humid place, e.g. a bathroom.
- The modem should be used in a sheltered area, within a temperature range of +5 to +40 Celsius.
- Do not expose the modem to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources.
- Do not deploy the cable for LAN connection outdoor to prevent electronic shock hazards.
- Keep the package out of reach of children.
- When you want to dispose of the modem, please follow local regulations on conservation of the environment.

Warranty

We warrant to the original end user (purchaser) that the modem will be free from any defects in workmanship or materials for a period of one (1) year from the date of purchase from the dealer. Please keep your purchase receipt in a safe place as it serves as proof of date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, we will, at our discretion, repair or replace the defective products or components, without charge for either parts or labor, to whatever extent we deem necessary tore-store the product to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be offered solely at our discretion. This warranty will not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions. The warranty does not cover the bundled or licensed software of other vendors. Defects which do not significantly affect the usability of the product will not be covered by the warranty. We reserve the right to revise the manual and online documentation and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

Be a Registered Owner

Web registration is preferred. You can register your Vigor modem via http://www.draytek.com.

Firmware & Tools Updates

Due to the continuous evolution of DrayTek technology, all modems will be regularly upgraded. Please consult the DrayTek web site for more information on newest firmware, tools and documents.

http://www.draytek.com

Table of Contents

Chapter I Installation VII

I-1 Introduction 1

I-1-1 LED Indicators and Connectors 2

I-2 Mounting the Access Point 3

I-2-1 Antennas Installation 3
I-2-2 Connecting Ethernet Cable(s) 4
I-2-3 Access Point Installation – Pole Mount 6
I-2-4 Grounding Access Point 8
I-2-5 Powering Access Point 9

I-3 Network IP Configuration 10

I-3-1 Windows 7 IP Address Setup 10
I-3-2 Windows 2000 IP Address Setup 12
I-3-3 Windows XP IP Address Setup 13
I-3-4 Windows Vista IP Address Setup 14

I-4 Accessing to Web User Interface 15

I-5 Changing Password 18

I-6 Dashboard 19

I-7 Quick Start Wizard 20

I-7-1 Settings for Access Point 21
I-7-2 Settings for Mesh Root 24
I-7-3 Settings for Mesh Node 28
I-7-4 Settings for Range Extender 29

Chapter II Connectivity 33

II-1 Operation Mode 34

II-2 General Concepts for Wireless LAN (2.4GHz/5GHz) 35

II-3 Wireless LAN (2.4GHz/5GHz) Settings for AP Mode 38

II-3-1 General Setup 39
II-3-2 Security 42
II-3-3 Access Control 45
II-3-4 WPS 46
II-3-5 Advanced Setting 47
II-3-6 AP Discovery 50
II-3-7 WDS AP Status 51
II-3-8 Bandwidth Management 51
II-3-9 Airtime Fairness 52
II-3-10 Station Control 55
II-3-11 Roaming 56
II-3-12 Band Steering 58
II-3-13 Station List 63

II-4 Mesh Settings for Mesh Mode 69

II-4-1 Mesh Setup 70
II-4-2 Mesh Status 72
II-4-3 Mesh Discovery 73
II-4-4 Basic Configuration Sync 74
II-4-5 Advanced Config Sync 77

II-5 Universal Repeater Settings for Range Extender Mode 78

II-6 LAN 81

II-6-1 General Setup 81

II-6-2 Web Portal 84
II-6-3 Port Control 86

Chapter III Management 87

III-1 System Maintenance 88

III-1-1 System Status 89
III-1-2 TR-069 90
III-1-3 Administrator Password 92
III-1-4 User Password 93
III-1-5 Configuration Backup 94
III-1-6 Syslog/Mail Alert 96
III-1-7 Time and Date 97
III-1-8 SNMP 98
III-1-9 Management 99
III-1-10 Reboot System 101
III-1-11 Firmware Upgrade 102

III-2 Central AP Management 103

III-2-1 General Setup 103
III-2-2 APM Log 104
III-2-3 Overload Management 105
III-2-4 Status of Settings 106

III-3 Mobile Device Management 107

III-3-1 Station List 107
III-3-2 Station Statistics 113
III-3-3 Station Nearby 114
III-3-4 Policies 115
III-3-5 Station Control List 116

Chapter IV Others 117

IV-1 RADIUS Setting 118

IV-1-1 RADIUS Server 118
IV-1-2 Certificate Management 119

IV-2 Applications 122

IV-2-1 Schedule 122
IV-2-2 Apple iOS Keep Alive 125
IV-2-3 Wi-Fi Auto On/Off 126
IV-2-4 Sensor 127

Chapter V Mobile APP, DrayTek Wireless 129

V-1 Introduction of DrayTek Wireless 130

V-2 Select a VigorAP 131

V-3 Quick Start Wizard 132

V-4 Login 141

Chapter VI Troubleshooting 145

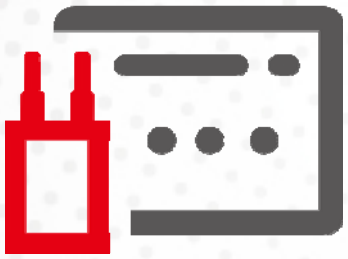
VI-1 Diagnostics 146

VI-1-1 System Log 147
VI-1-2 Speed Test 147
VI-1-3 Traffic Graph 148
VI-1-4 WLAN (2.4GHz) Statistics 149
VI-1-5 WLAN (5GHz) Statistics 150
VI-1-6 Interference Monitor 151
VI-1-7 Support Area 152

VI-2 Checking the Hardware Status 153

VI-3 Checking the Network Connection Settings 154
VI-3-1 For Windows 154
VI-3-2 For Mac Os 156
IV-4 Pinging the Device 157
VI-4-1 For Windows 157
VI-4-2 For Mac Os (Terminal) 157
VI-5 Backing to Factory Default Setting 159
VI-5-1 Software Reset 159
VI-5-2 Hardware Reset 159
VI-6 Contacting DrayTek 160
Index 161

Chapter I Installation



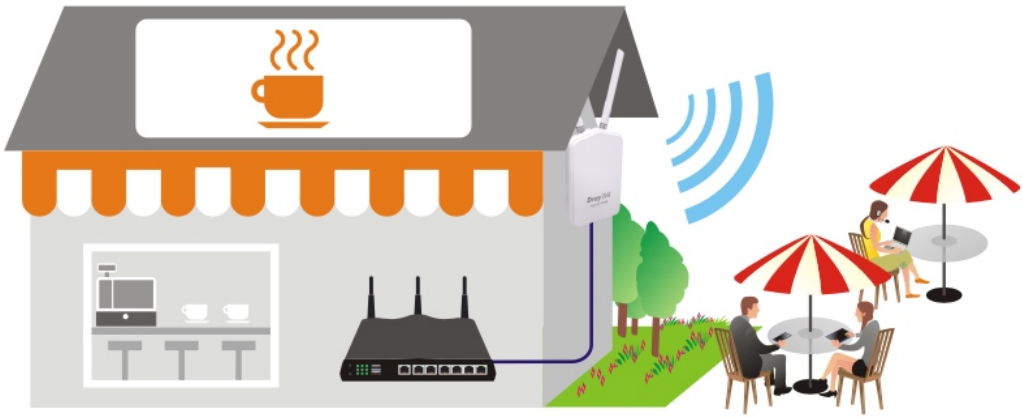
I-1 Introduction

This is a generic International version of the user guide. Specification, compatibility and features vary by region. For specific user guides suitable for your region or product, please contact local distributor.

Thank you for purchasing VigorAP 920R series.

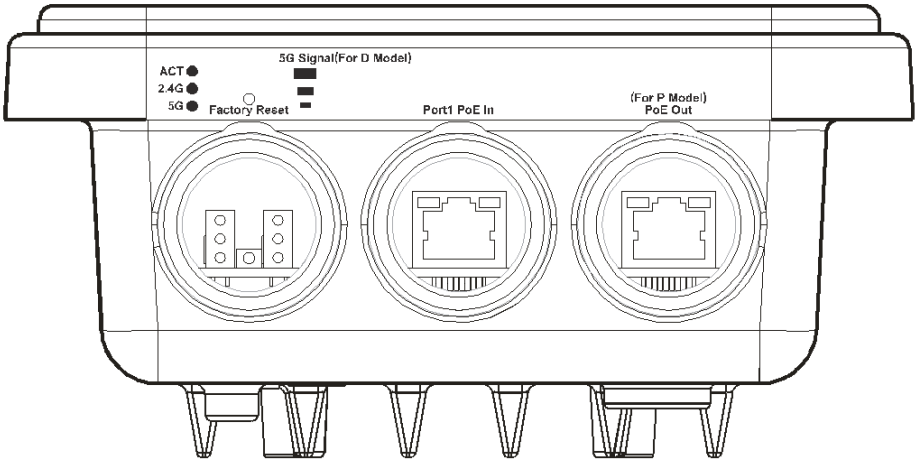
Easy install procedures allows any computer users to setup a network environment in very short time - within minutes, even inexperienced users. Just follow the instructions given in this user manual, you can complete the setup procedure and release the power of this access point all by yourself!

VigorAP 920RP also is a Power over Ethernet Powered Device which adopts the technology of PoE for offering power supply and transmitting data through the Ethernet cable.



I-1-1 LED Indicators and Connectors

Before you use the Vigor modem, please get acquainted with the LED indicators and connectors first.



LED	Status	Explanation
ACT	Off	The system is not ready or has failed.
	Blinking	The system is ready.
2.4G / 5G	On	Wireless function is ready.
	Off	Wireless function is not ready.
	Blinking	Data is being transmitted (sending/receiving).
5G Signal (For D Model)		The signal strength (excellent) > -50dBm.
5G Signal (For D Model)		The signal strength (good) is between -66dBm ~ -51dBm.
5G Signal (For D Model)		The signal strength (fair) is between -73dBm~ -67dBm.
5G Signal (For D Model)		No signal or the signal strength is <-73dBm.

Interface	Description
Factory Reset	Restore the default settings. Usage: Switch on the access point. Press and hold reset button for at least 10 seconds. The router will restart with the factory default configuration. Before pressing the button, the cover should first be removed by rotating it with a torque of 13 kgf-cm. After the access point has been reset, replace the cover and lock it with the same amount of torque.
Port 1 PoE In	Connector for receiving power from another device.
PoE Out (for P Model)	Connector for supplying power to another device.

Note:

For the sake of security, make the accessory kit away from children.

I-2 Mounting the Access Point

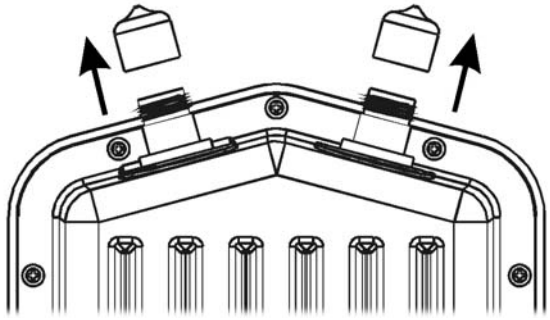
The VigorAP can be pole mounted depending on the installation environment. This section will guide you through installing the VigorAP.

Note:

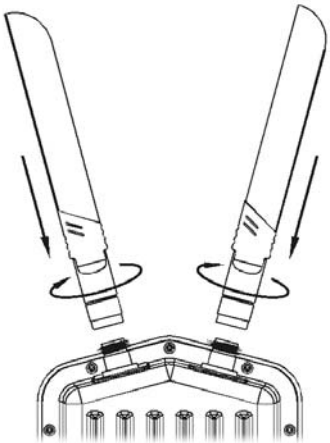
For the sake of personal safety, only trained and qualified personnel should install this device.

I-2-1 Antennas Installation

1. Remove the protective cap.



2. Insert the antennas and fasten them by rotating clockwise.



Warning:

Do not open the top cover of the device.

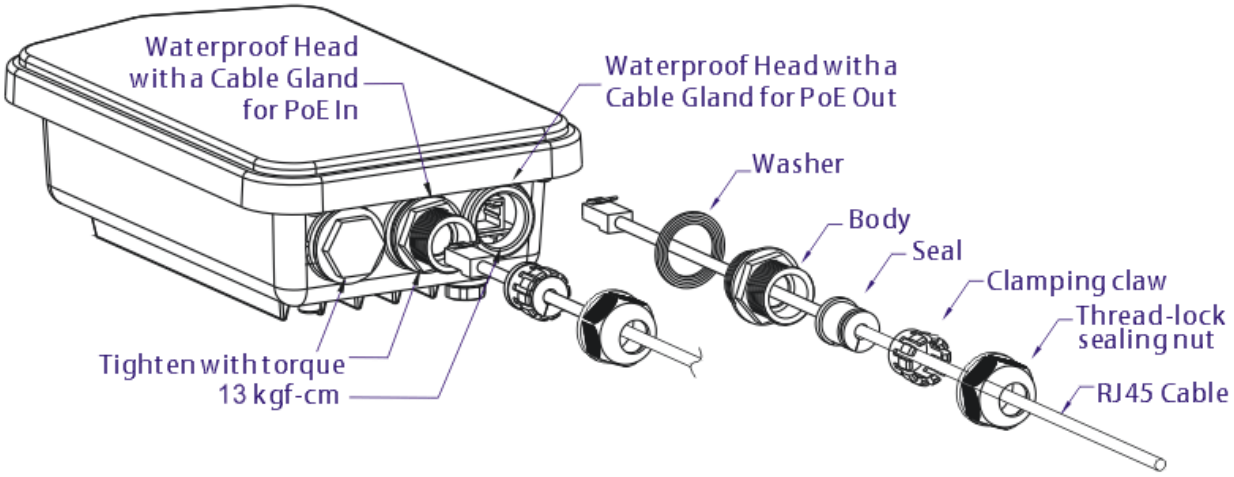
Installation during thunderstorms could be dangerous.

I-2-2 Connecting Ethernet Cable(s)

Refer to the following steps to attach the Ethernet cable and waterproof head. (Take VigorAP 920RP as an example.)

1. Remove the cable cover for Ethernet Port (e.g., **Port 1 PoE In)**.
2. Before connecting, verify that the cable has a rubber seal and that it is not damaged.

   To prevent the enclosure from water leakage, make sure the Ethernet cable gland and the rubber gasket are present and installed properly.
3. Inserting RJ-45 connector into the port.



4. Use an adjustable wrench and tighten the thread-lock sealing nut with torque 10 kgf-cm.

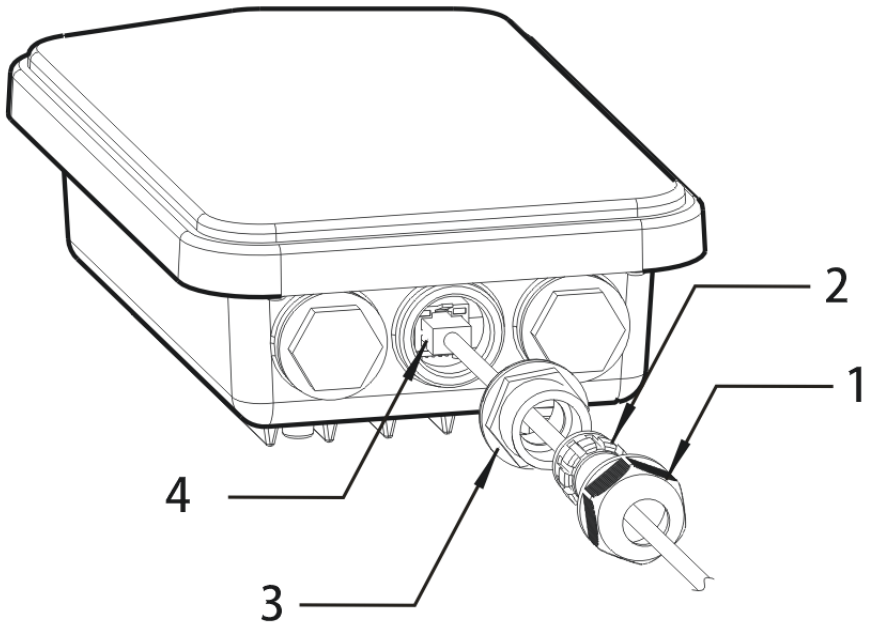
Warning:

Do not open the top cover of the device.

Installation during thunderstorms could be dangerous.

Reconnecting Ethernet Cable

1. Loosen the thread-lock sealing nut.
2. Loosen the clamping claw and seal.
3. Loosen the body and washer.
4. Remove the cable.



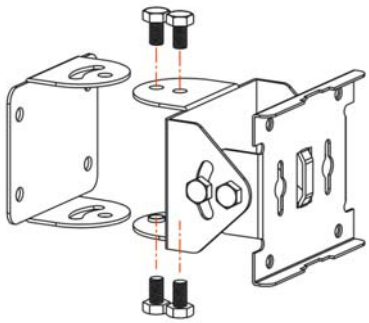
5. To reattach the cable, follow the above steps in reverse.

Note:

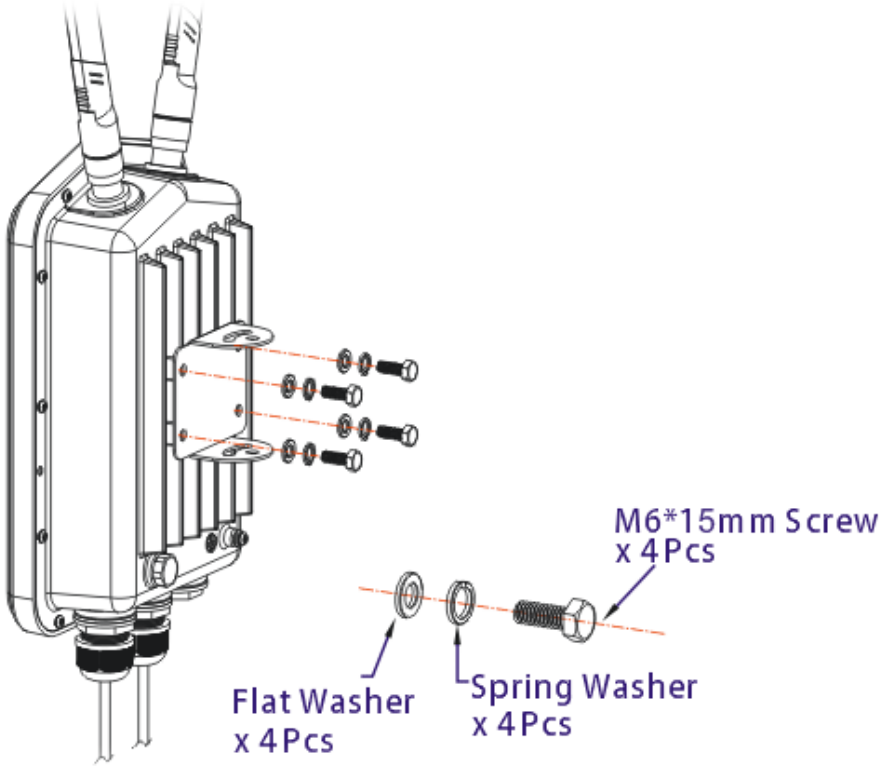
The diameter for the Ethernet cable shall be limited between 4.3mm to 5.9mm.

I-2-3 Access Point Installation – Pole Mount

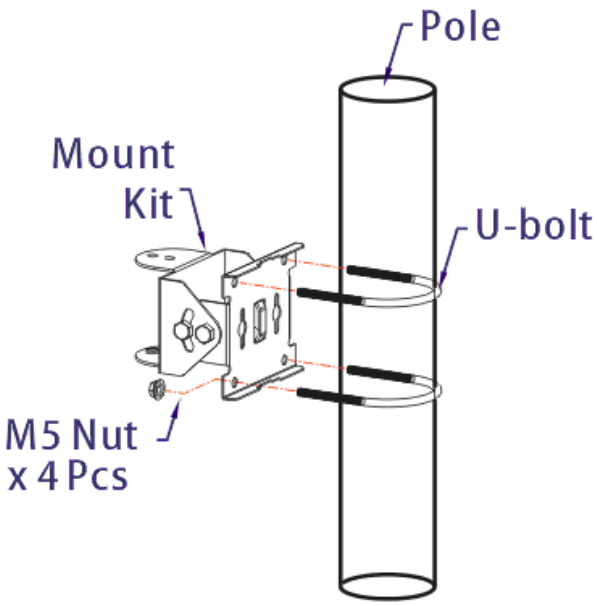
1. Find a suitable location for installing the access point.
2. Select a mounting point on a pole.
3. Remove the mounting plate from the mount kit by removing the four mounting screws.



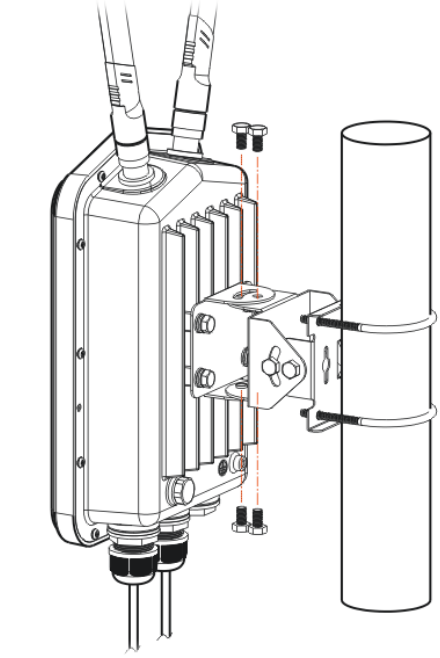
4. Attach the VigorAP920R series to the mounting plate. Lock the screws with torque of 20 kgf-cm.



5. Fasten the mount kit on the pole with nut screws and with torque of 20 kgf-cm.



6. Fasten the access point to the mount kit with screws (torque of 20 kgf-cm) as shown in the following figure.



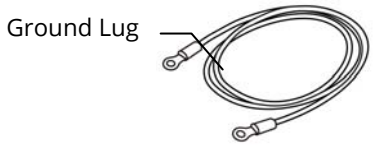
Note:

Before connecting the access point to the mount kit, make sure it is oriented with the LED indicators pointing downwards.

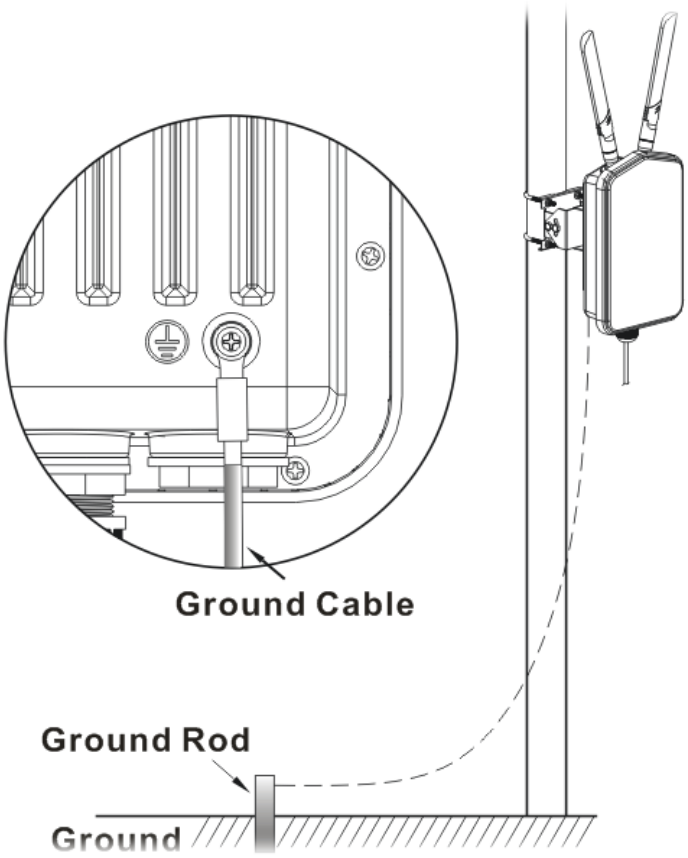
I-2-4 Grounding Access Point

In outdoor installations and before powering the access point with AC power, VigorAP must be grounded prior to wire installation.

1. Take out the ground cable from the mount kit.



2. Insert a ground rod on the ground.
3. Strip the insulation for the ground lug.
4. Use the appropriate crimping tool to crimp the ground cable to the grounding lug.
5. Connect the ground rod and the VigorAP using the ground cable.



Note:

Please consult an electrician if you are uncertain about the type of grounding that is required.

I-2-5 Powering Access Point

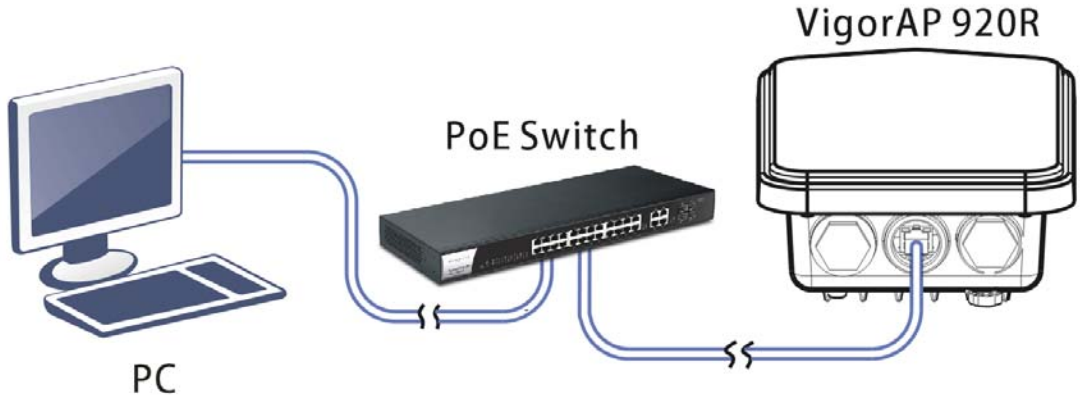
VigorAP 920R/PR can be powered via the PoE input from an in-line power injector or a suitably powered switch port.

Before powering VigorAP, you should:

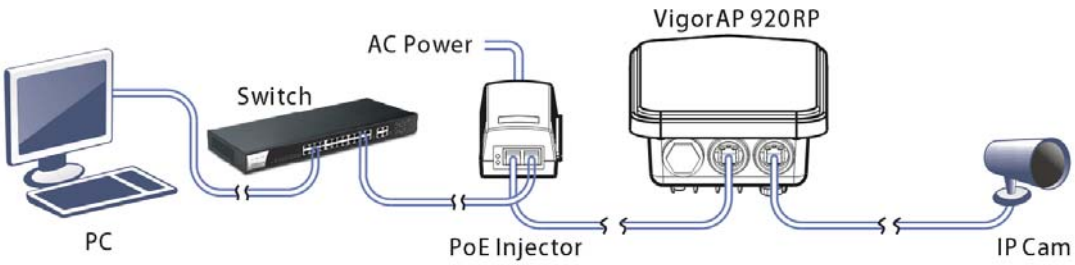
- Pay attention to local and national electrical codes.
- Not place the power injector / VigorSwitch in outdoor environment without any protection. Moisture might get into the power injector and cause a short circuit or possible fire.
- Not work on the system during periods of lighting activity to avoid the risk of electric shock, and do not connect or disconnect the Ethernet cables under bad weather.

Below shows two examples of connecting power for VigorAP 920R and VigorAP 920RP.

Example 1: AP920R



Example 2: AP920RP



I-3 Network IP Configuration

After the network connection is built, the next step you should do is setup VigorAP 920R with proper network parameters, so it can work properly in your network environment.

Before you can connect to the access point and start configuration procedures, your computer must be able to get an IP address automatically (use dynamic IP address). If it's set to use static IP address, or you're unsure, please follow the following instructions to configure your computer to use dynamic IP address:

For the default IP address of this AP is set "192.168.1.2", we recommend you to use "192.168.1.X (except 2)" in the field of IP address on this section for your computer.
If the operating system of your computer is...

Windows 7 **- please go to section I-3-1**

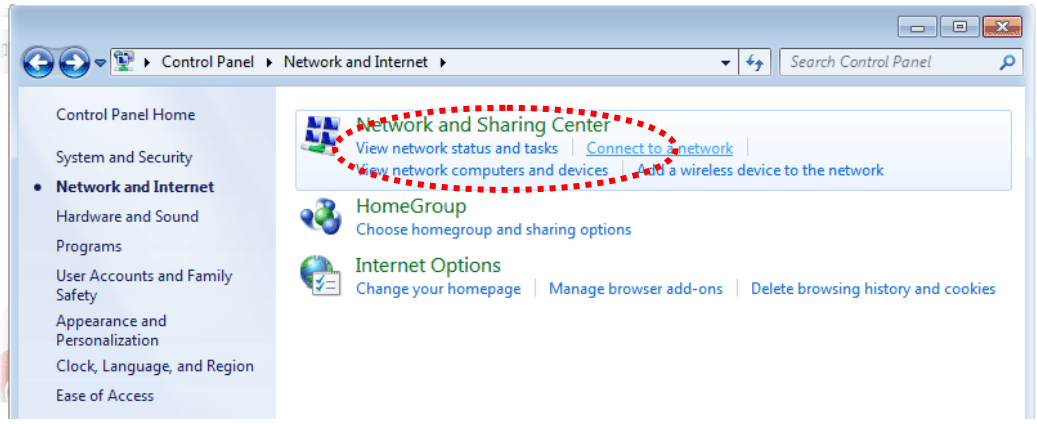
Windows 2000 **- please go to section I-3-2**

Windows XP **- please go to section I-3-3**

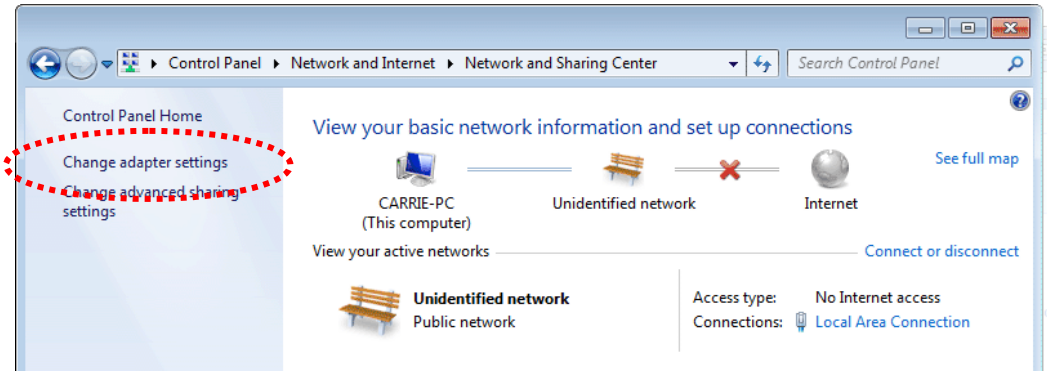
Windows Vista **- please go to section I-3-4**

I-3-1 Windows 7 IP Address Setup

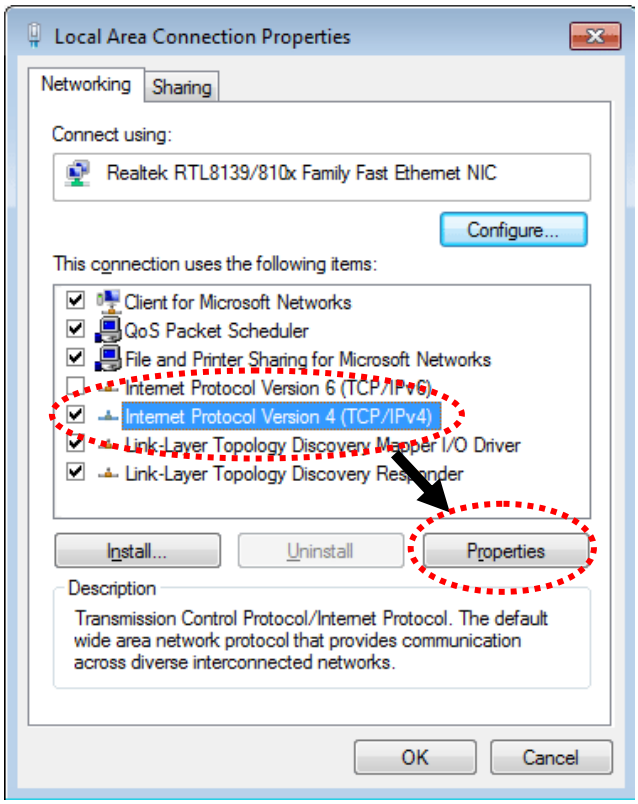
Click **Start** button (it should be located at lower-left corner of your computer), then click Control Panel. Double-click **Network and Internet**, and the following window will appear. Click **Network and Sharing Center**.



Next, click **Change adapter settings** and click **Local Area Connection**.



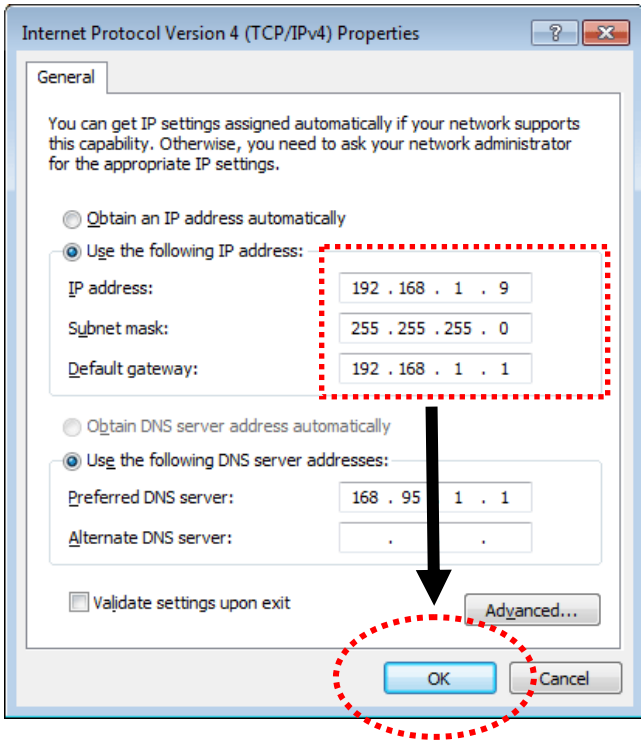
Then, select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



Under the General tab, click **Use the following IP address.** Then input the following settings in respective field and click **OK** when finish.

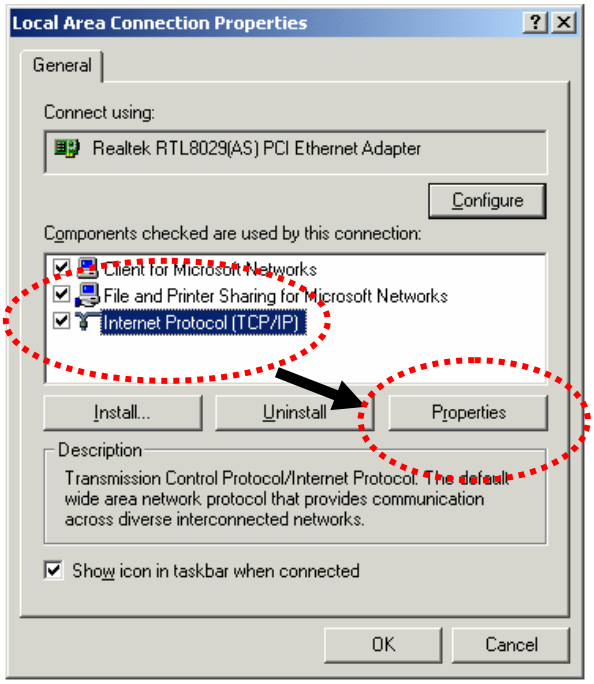
IP address: **192.168.1.9**

Subnet Mask: **255.255.255.0**



I-3-2 Windows 2000 IP Address Setup

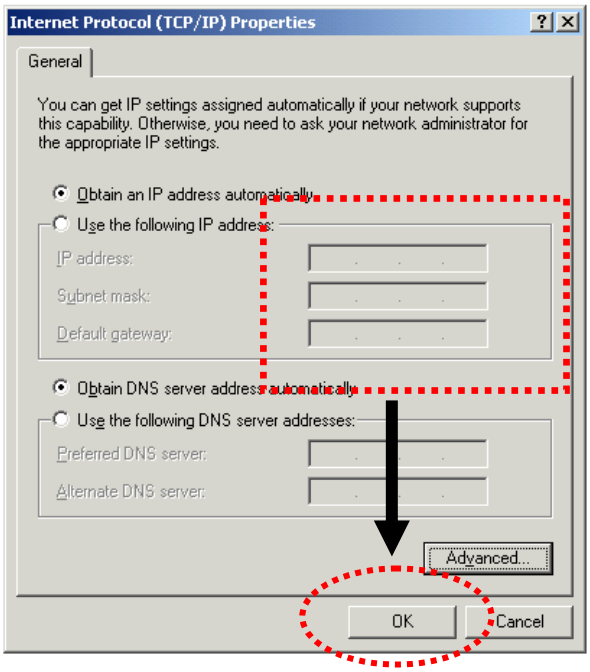
Click **Start** button (it should be located at lower-left corner of your computer), then click control panel. Double-click **Network and Dial-up Connections** icon, double click **Local Area Connection,** and **Local Area Connection Properties** window will appear. Select **Internet Protocol (TCP/IP)**, then click **Properties**.



Select **Use the following IP address**, then input the following settings in respective field and click **OK** when finish.

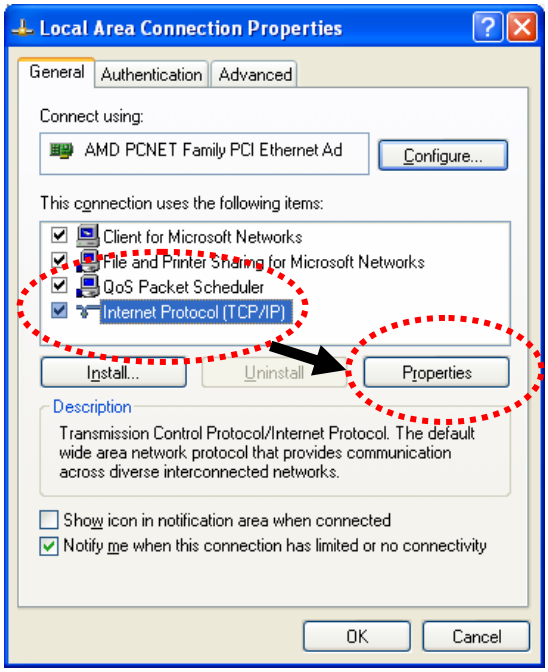
IP address: **192.168.1.9**

Subnet Mask: **255.255.255.0**



I-3-3 Windows XP IP Address Setup

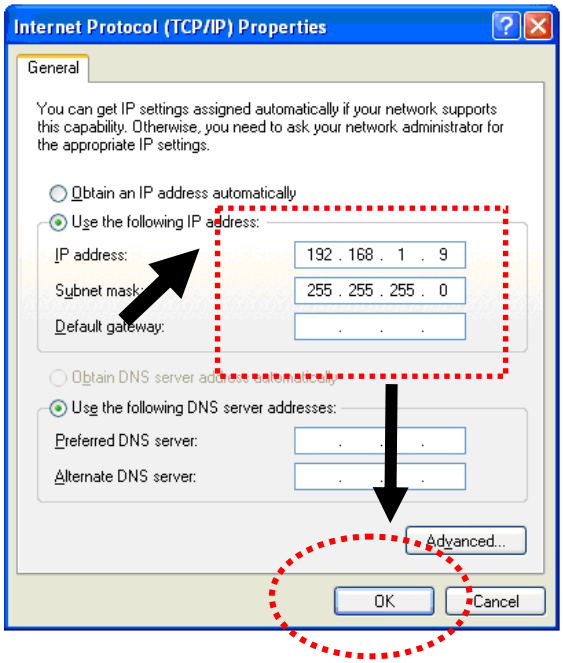
Click **Start** button (it should be located at lower-left corner of your computer), then click control panel. Double-click **Network and Internet Connections** icon, click **Network Connections,** and then double-click **Local Area Connection, Local Area Connection Status** window will appear, and then click **Properties**.



Select **Use the following IP address**, then input the following settings in respective field and click **OK** when finish:

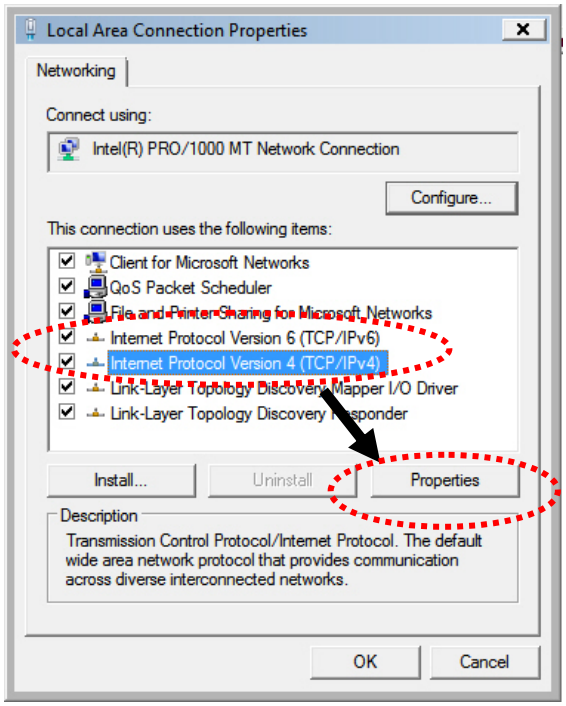
IP address: **192.168.1.9**

Subnet Mask: **255.255.255.0**.



I-3-4 Windows Vista IP Address Setup

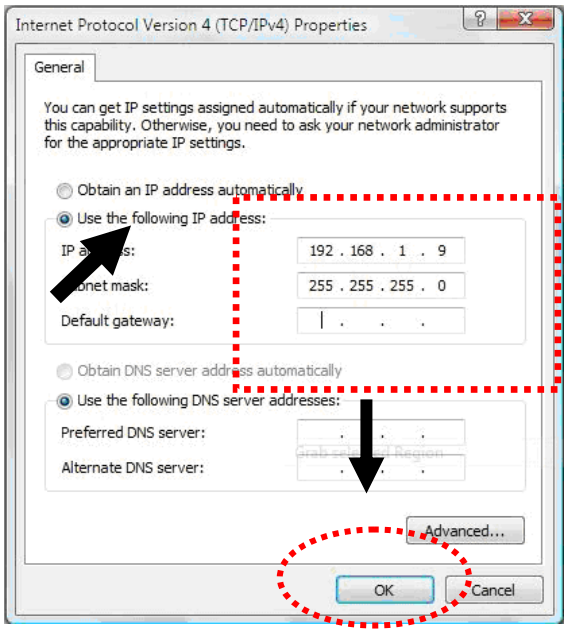
Click **Start** button (it should be located at lower-left corner of your computer), then click control panel. Click **View Network Status and Tasks**, then click **Manage Network Connections.** Right-click **Local Area Netwrok, then select 'Properties'. Local Area Connection Properties** window will appear, select I**nternet Protocol Version 4 (TCP / IPv4)**, and then click **Properties**.



Select **Use the following IP address**, then input the following settings in respective field and click **OK** when finish:

IP address: **192.168.1.9**

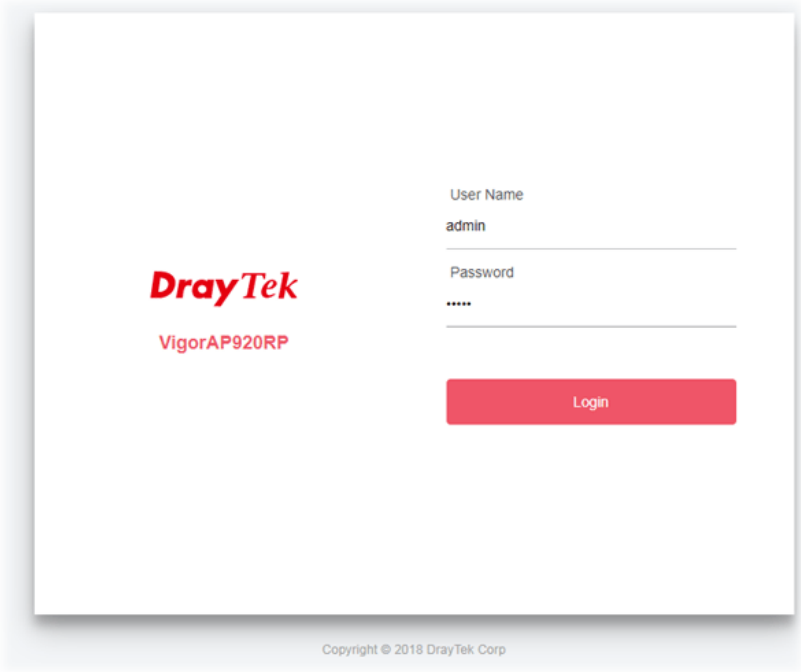
Subnet Mask: **255.255.255.0**.



I-4 Accessing to Web User Interface

All functions and settings of this access point must be configured via web user interface. Please start your web browser (e.g., Firefox).

1. Make sure your PC connects to the VigorAP 920R correctly.
2. Open a web browser on your PC and type **http://192.168.1.2.** A pop-up window will open to ask for username and password. Pease type “admin/admin” on Username/Password and click **OK**.

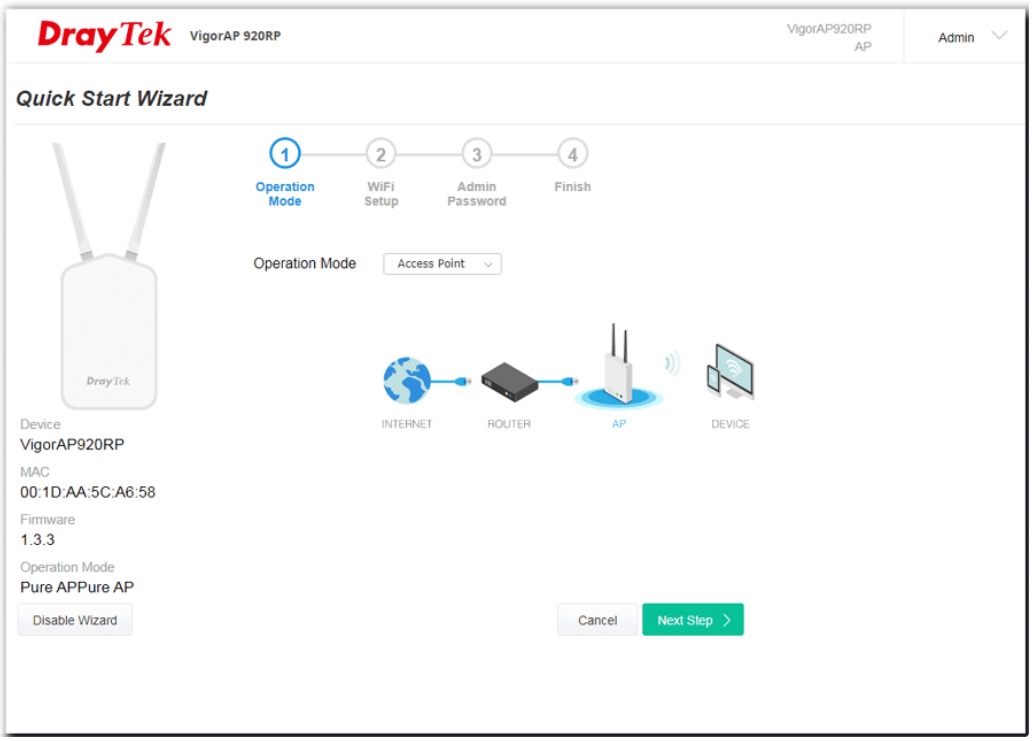


Note:

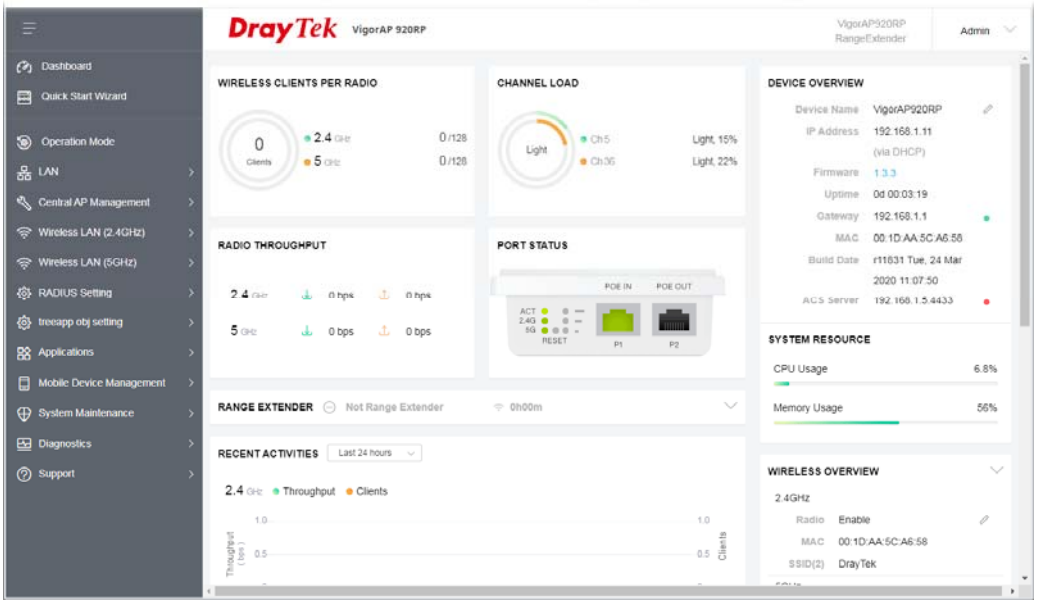
You may either simply set up your computer to get IP dynamically from the router or set up the IP address of the computer to be in the same subnet as **the IP address of VigorAP 920R.**

- If there is no DHCP server on the network, then VigorAP 920R will have an IP address of 192.168.1.2.
- If there is DHCP available on the network, then VigorAP 920R will receive it’s IP address via the DHCP server.
- If you connect to VigorAP by wireless LAN, you could try to access the web user interface through http://vigorap.com.

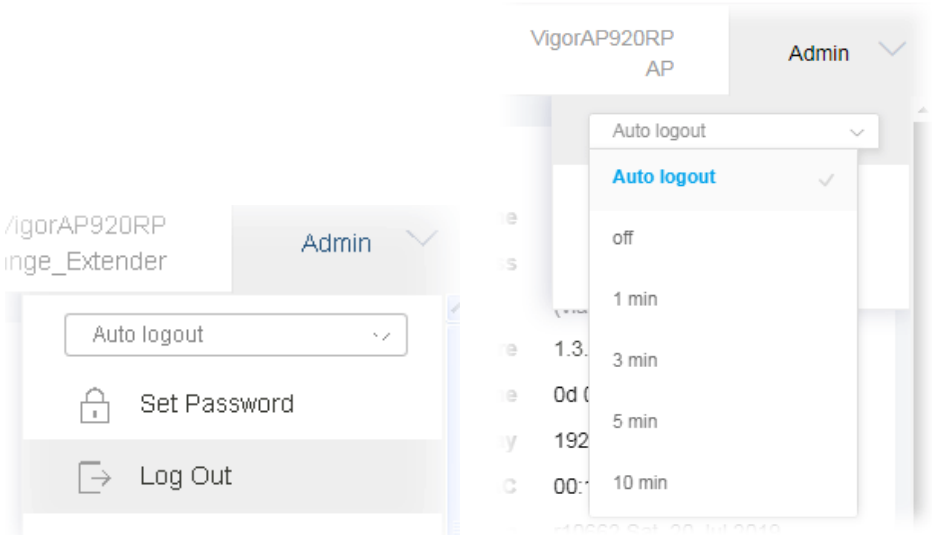
3. For the first time accessing VigorAP, the **Quick Start Wizard** for configuring wireless settings will appear as follows. Refer to *Section I-7 Quick Start Wizard for detailed information*.



4. If VigorAP has been configured previously, the Dashboard of VigorAP will appear as follows:



5. The web page can be logged out by clicking **Log Out** on the top right of the web page. Or, logout the web user interface according to the chosen condition. The default setting is **Auto Logout**, which means the web configuration system will logout after 5 minutes without any operation. Change the setting of auto logout if you want.



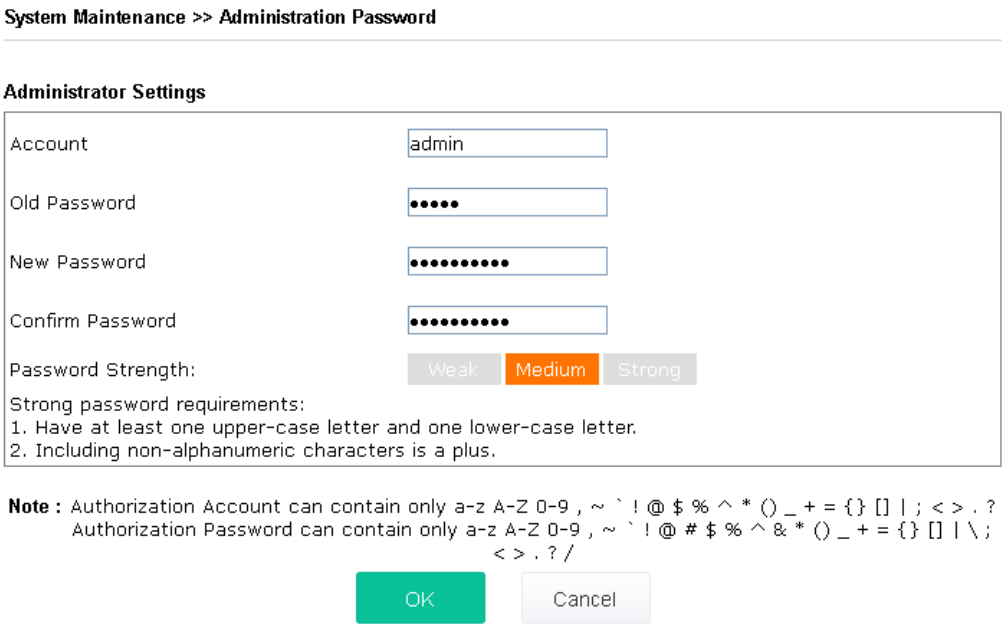
Note:

If you fail to access the web configuration, please go to the section “Trouble Shooting” for detecting and solving your problem.

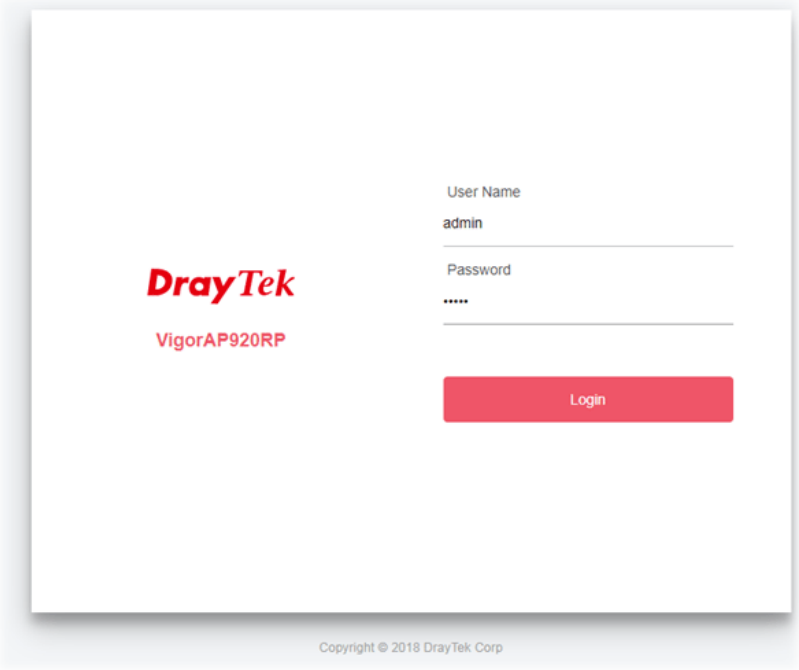
For using the device properly, it is necessary for you to change the password of web configuration for security and adjust primary basic settings.

I-5 Changing Password

1. Please change the password for the original security of the modem.
2. Go to **System Maintenance** page and choose **Administration Password.**



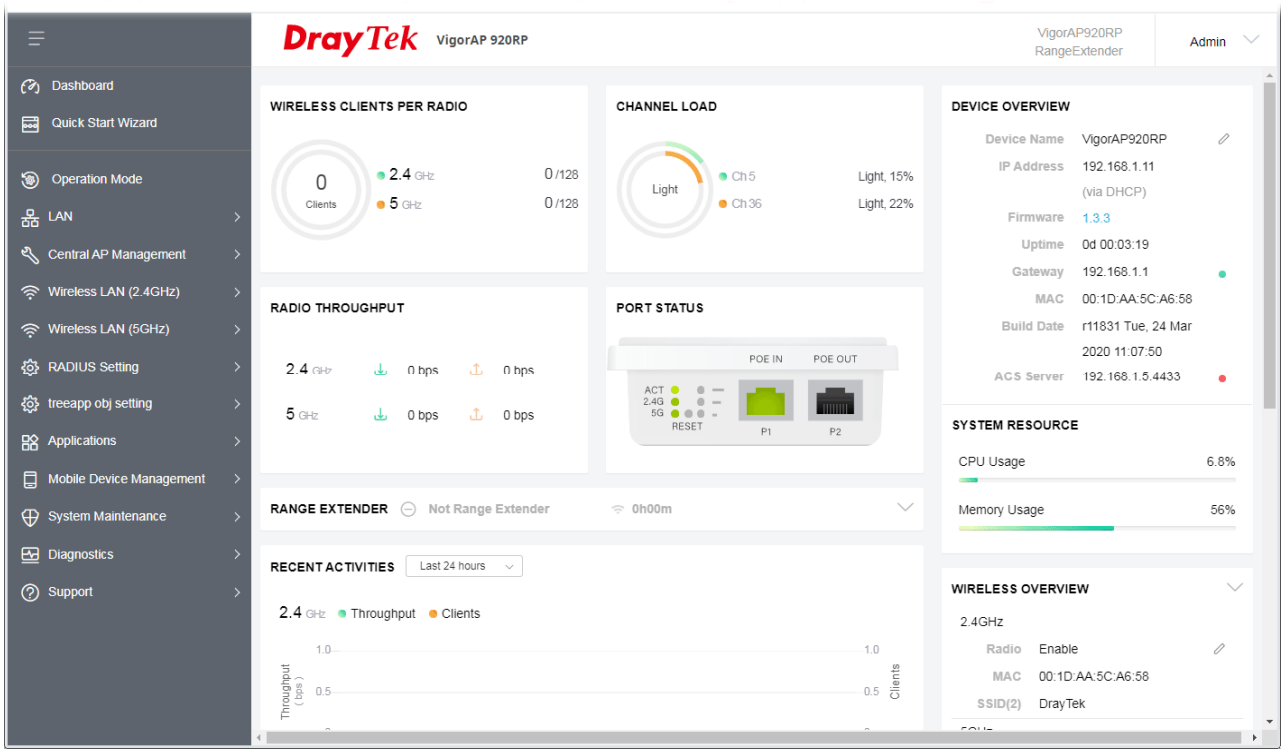
3. Enter the new login password on the field of **Password**. Then click **OK** to continue.
4. Now, the password has been changed. Next time, use the new password to access the Web User Interface for this modem.



I-6 Dashboard

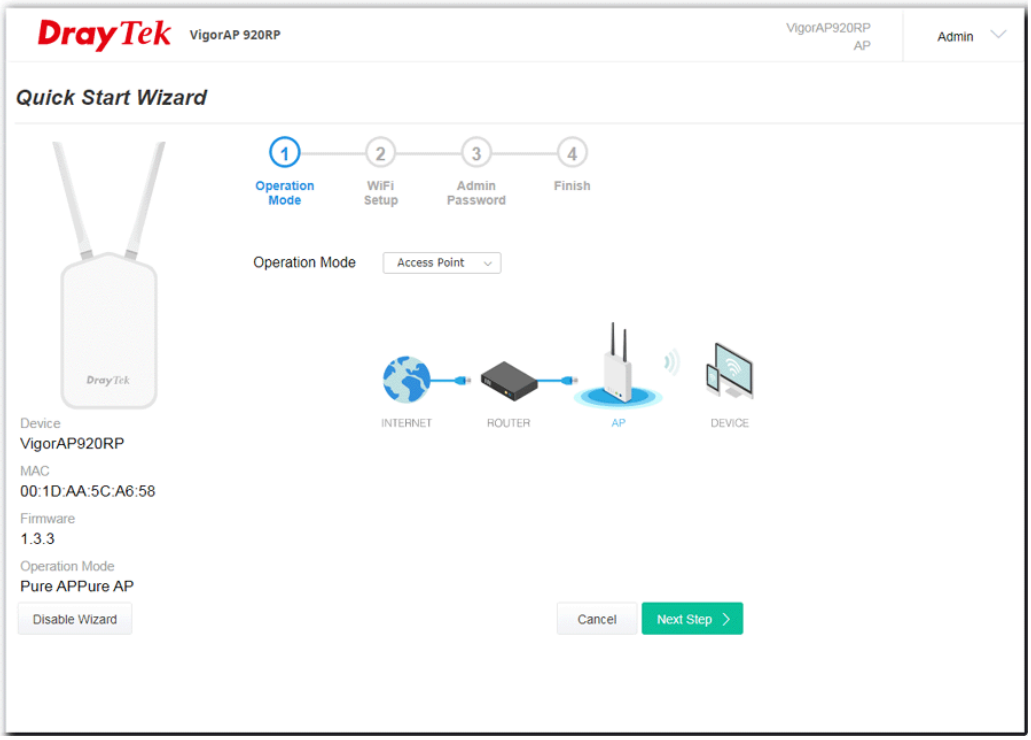
Dashboard shows system status including the number of client connected, throughput, gateway, physical connection status, radio (2.4GHz / 5GHz) status, backhaul network, recent activities, wireless network usage, and so on.

Click **Dashboard** from the main menu on the left side of the main page.



I-7 Quick Start Wizard

Quick Start Wizard will guide you to configure 2.4G wireless setting, 5G wireless setting and other corresponding settings for Vigor Access Point step by step. Here, we take VigorAP920RPD as an example.



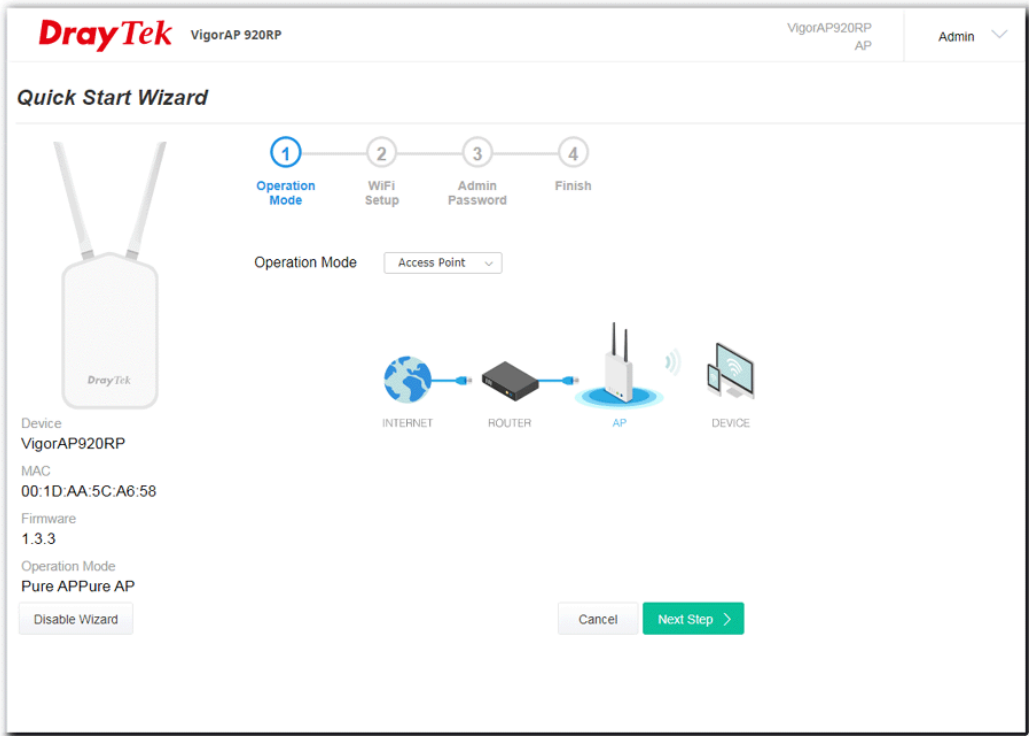
Available operation mode includes:

- Access Point
- Mesh Root
- Mesh Node
- Range Extender

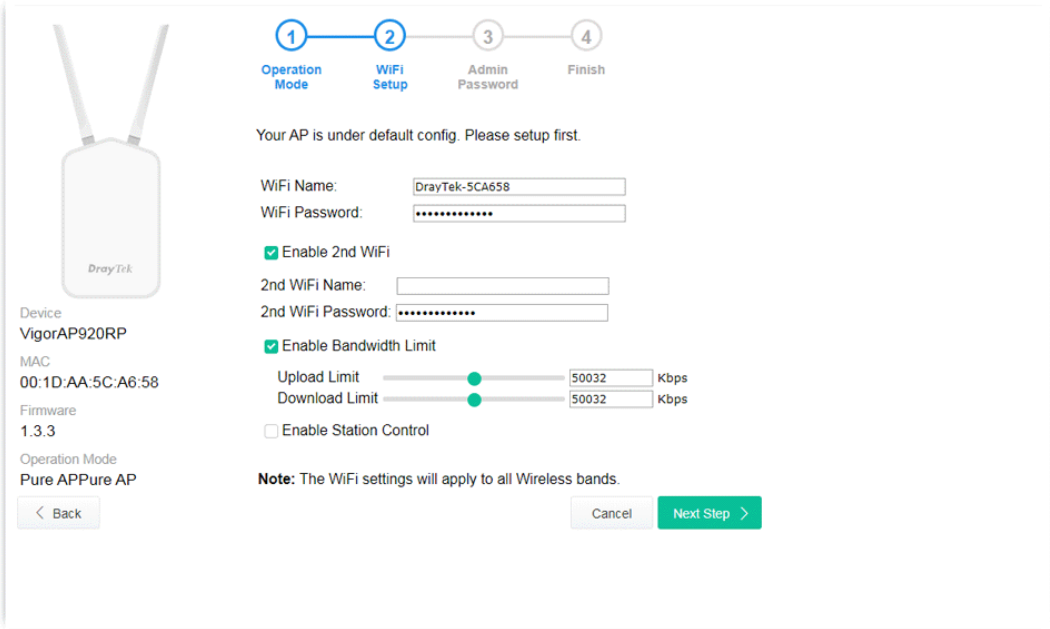
In this page, the advanced settings pages will vary according to the operation mode specified.

I-7-1 Settings for Access Point

1. Choose **Access Point** as the operation mode and click **Next Step**.



2. In the following page, configure the settings for wireless LAN (for both 2.4GHz and 5GHz) and click **Next Step**.

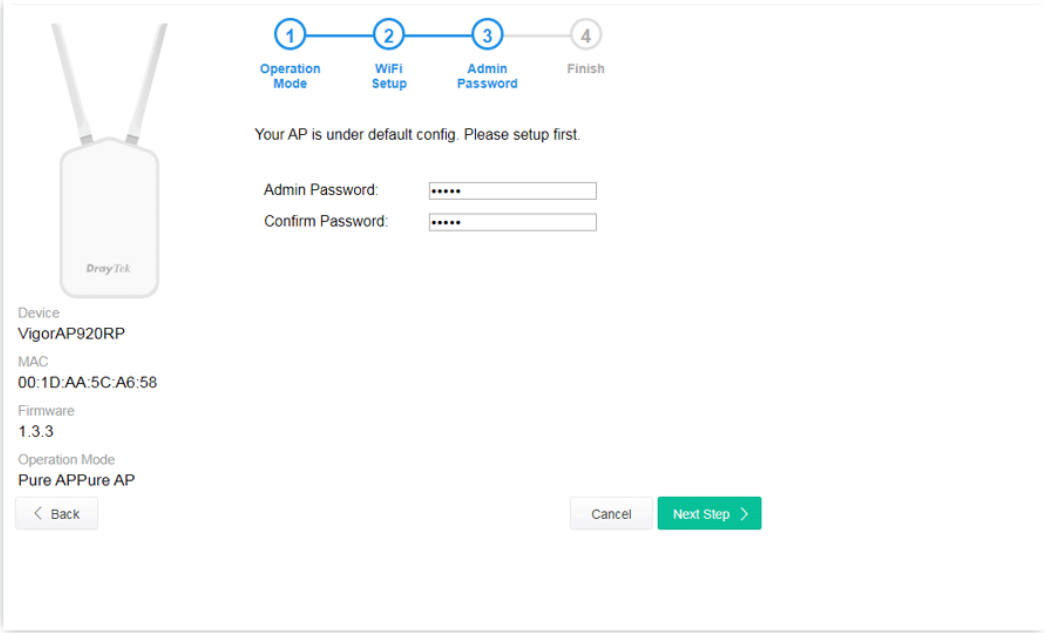


Available settings are explained as follows:

Item	Description
WiFi Name	Set a name for VigorAP 920R to be identified.
WiFi Password	Type **8~63** ASCII characters, such as 012345678..(or 64 Hexadecimal

	digits leading by 0x, such as "0x321253abcde...").
Enable 2nd Wireless	Check the box to enable the **guest** wireless setting. Such feature is especially useful for free Wi-Fi service. For example, a coffee shop offers free Wi-Fi service for its guests for one hour every day. **2nd WiFi Name** - Set a name for VigorAP device which can be identified and connected by wireless guest. **2nd WiFi Password -** Set **8~63** ASCII characters or **8~63** ASCII characters which can be used for logging into VigorAP device by wireless guest.
Enable Bandwidth Limit	Check the box to define the maximum speed of the data uploading/downloading which will be used for the guest connecting to Vigor device with the same SSID. **Upload Limit** – Scroll the radio button to choose the value you want. **Download Limit** –Scroll the radio button to choose the value you want.
Enable Station Control	Check the box to set the duration for the guest connecting /reconnecting to Vigor device. **Connection Time** –Scroll the radio button to choose the value you want. **Reconnection Time** –Scroll the radio button to choose the value you want.

3. Change the default password for such device with new value. Then click **Next Step**.

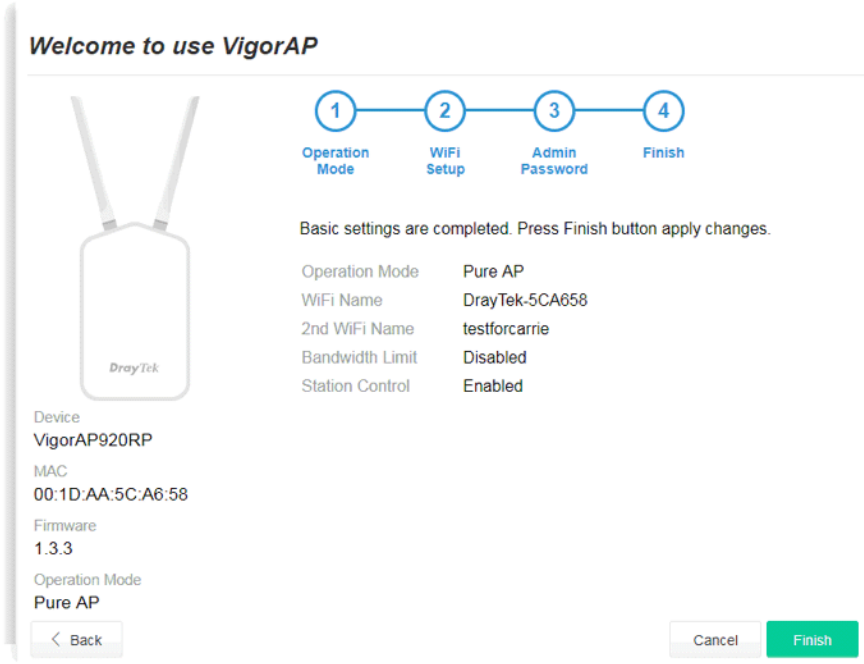


Available settings are explained as follows:

Item	Description
Admin Password	Enter a new password.
Confirm	Enter the new password again for confirmation.

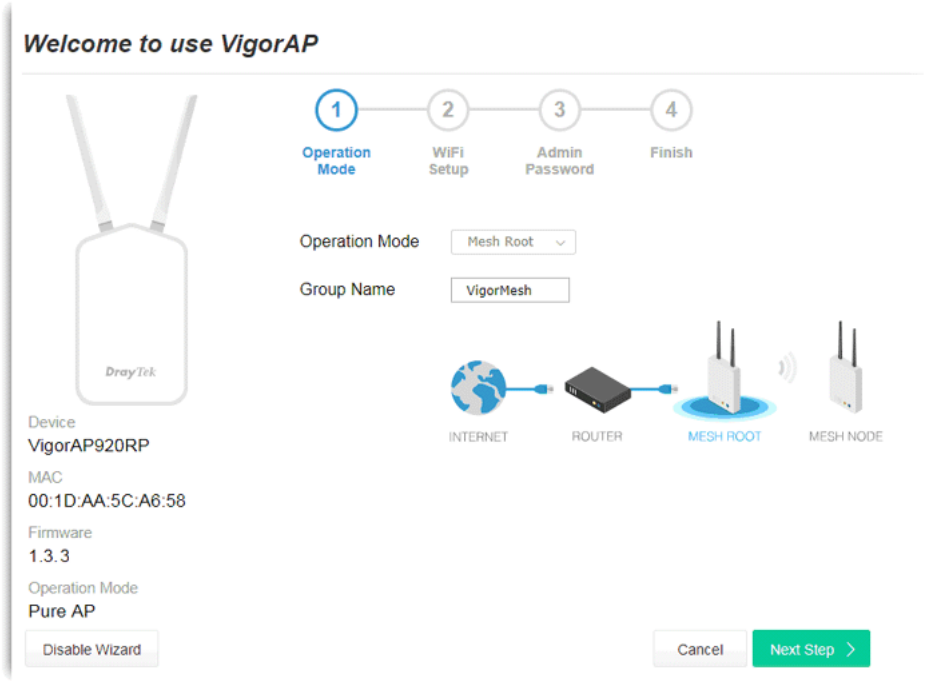
Password	

4. A summary of settings configuration will be shown on screen. Click **Finish**.

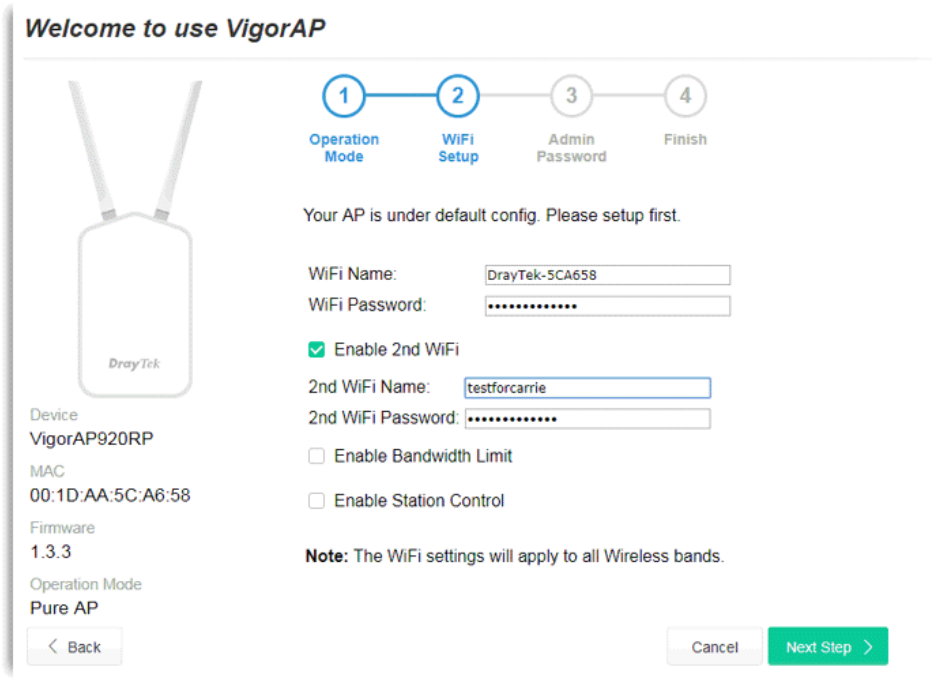


I-7-2 Settings for Mesh Root

1. Choose **Mesh Root** as the operation mode and click **Next Step**.



2. Configure the settings for wireless LAN (for both 2.4GHz and 5GHz) and click **Next Step**.

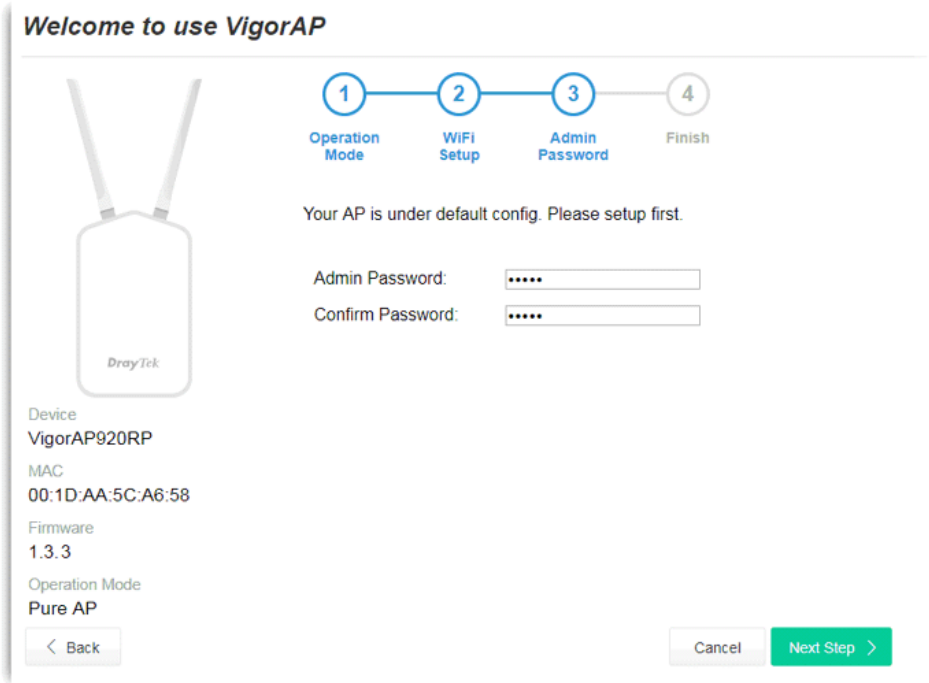


Available settings are explained as follows:

Item	Description
WiFi Name	Set a name for VigorAP 920R to be identified.
WiFi Password	Type **8~63** ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

Enable 2nd Wireless	Check the box to enable the **guest** wireless setting. Such feature is especially useful for free Wi-Fi service. For example, a coffee shop offers free Wi-Fi service for its guests for one hour every day. **2nd WiFi Name** - Set a name for VigorAP 920R which can be identified and connected by wireless guest. **2nd WiFi Password -** Set **8~63** ASCII characters or **8~63** ASCII characters which can be used for logging into VigorAP 920R by wireless guest.
Enable Bandwidth Limit	Check the box to define the maximum speed of the data uploading/downloading which will be used for the guest connecting to Vigor device with the same SSID. **Upload Limit** – Scroll the radio button to choose the value you want. **Download Limit** –Scroll the radio button to choose the value you want.
Enable Station Control	Check the box to set the duration for the guest connecting /reconnecting to Vigor device. **Connection Time** –Scroll the radio button to choose the value you want. **Reconnection Time** –Scroll the radio button to choose the value you want.

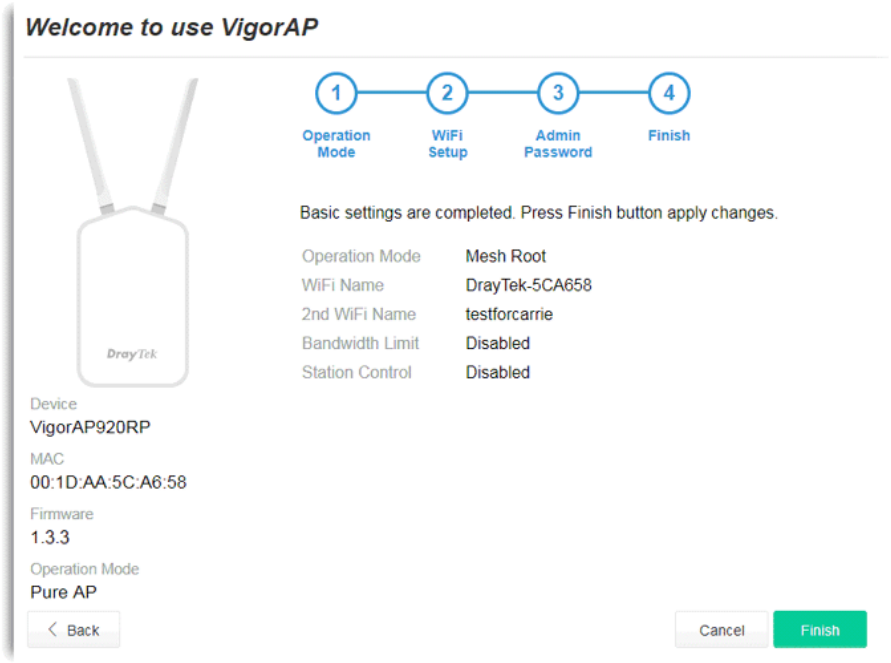
3. Change the default password for such device with new value. Then click **Next Step**.



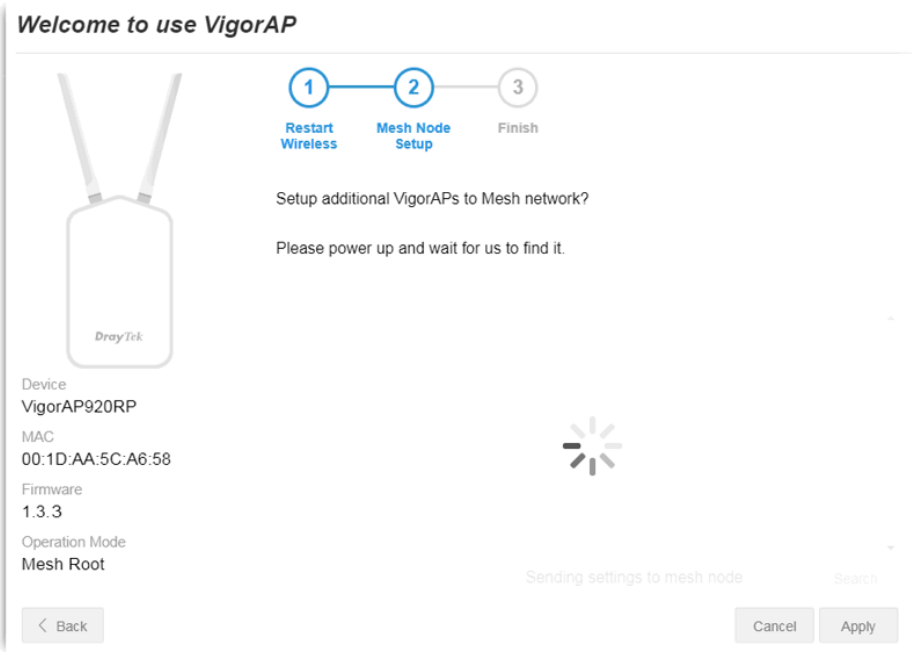
Available settings are explained as follows:

Item	Description
Admin Password	Enter a new password.
Confirm Password	Enter the new password again for confirmation.

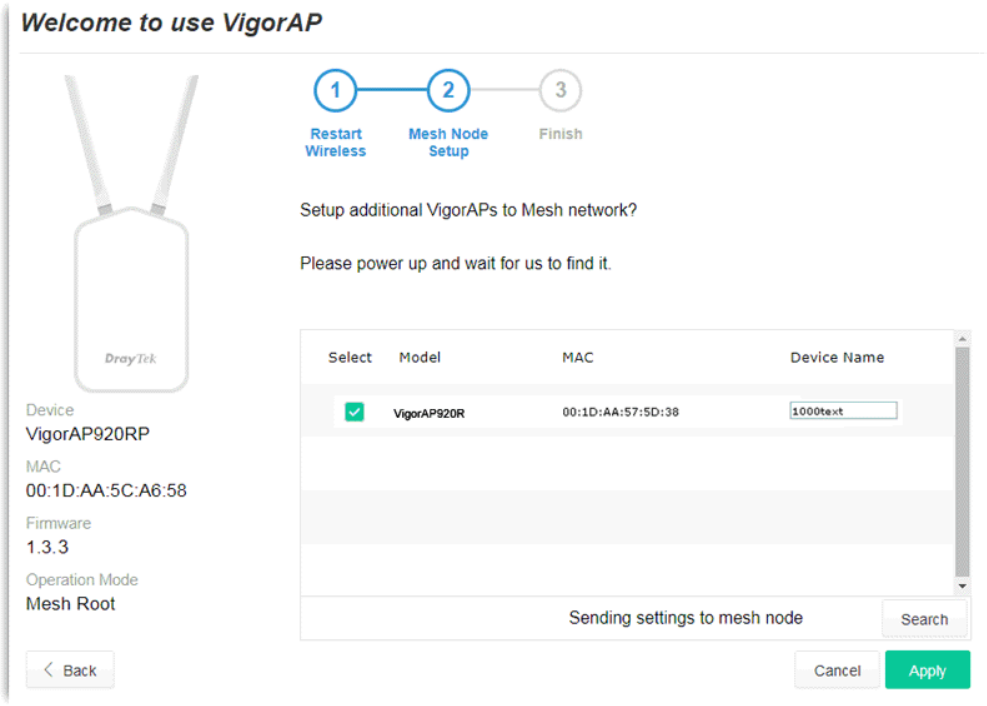
4. A summary of settings configuration will be shown on screen. Click **Finish**.



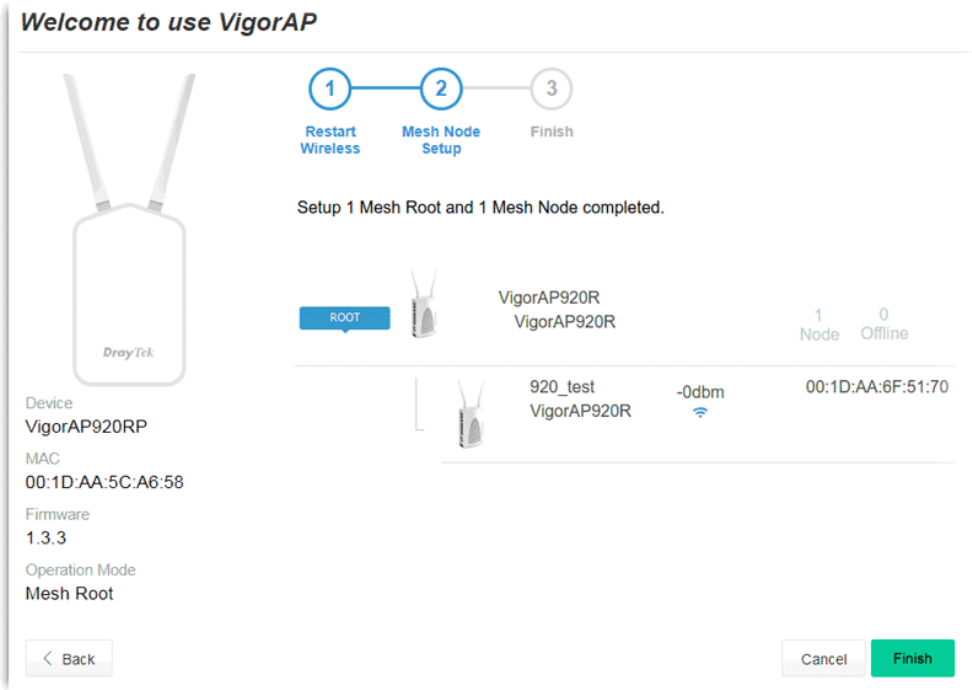
5. After clicking **Finish**, the following web page appears. VigorAP will search for mesh node around the network.



6. Available VigorAP devices will be shown on the screen. Select the device (as a mesh node) for grouping under such mesh group and enter a device name for identification.

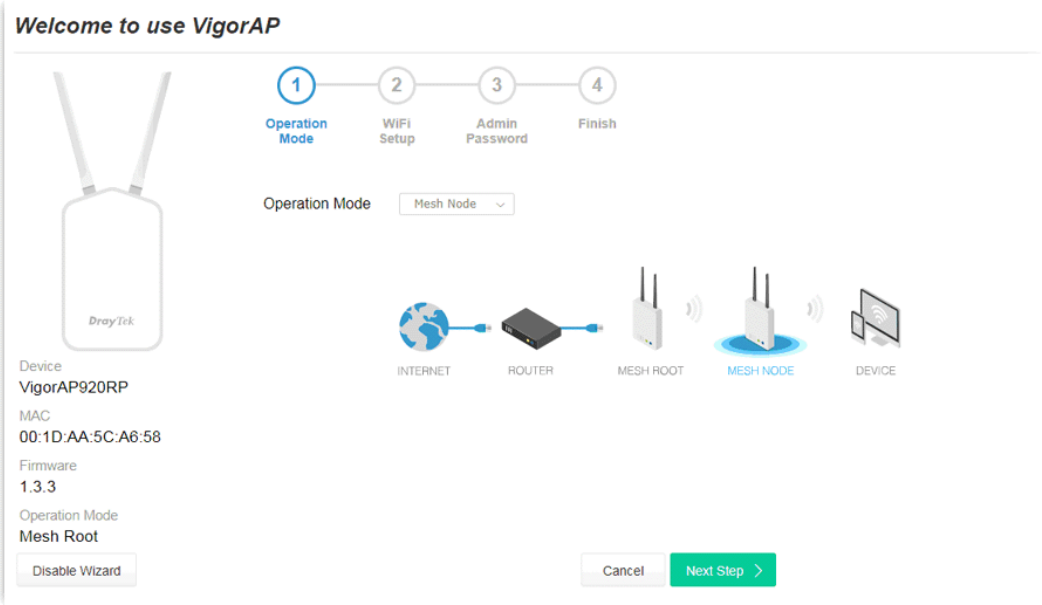


7. Click **Apply** and wait for a while. Later, a summary page of mesh root with mesh node will be shown on the screen.

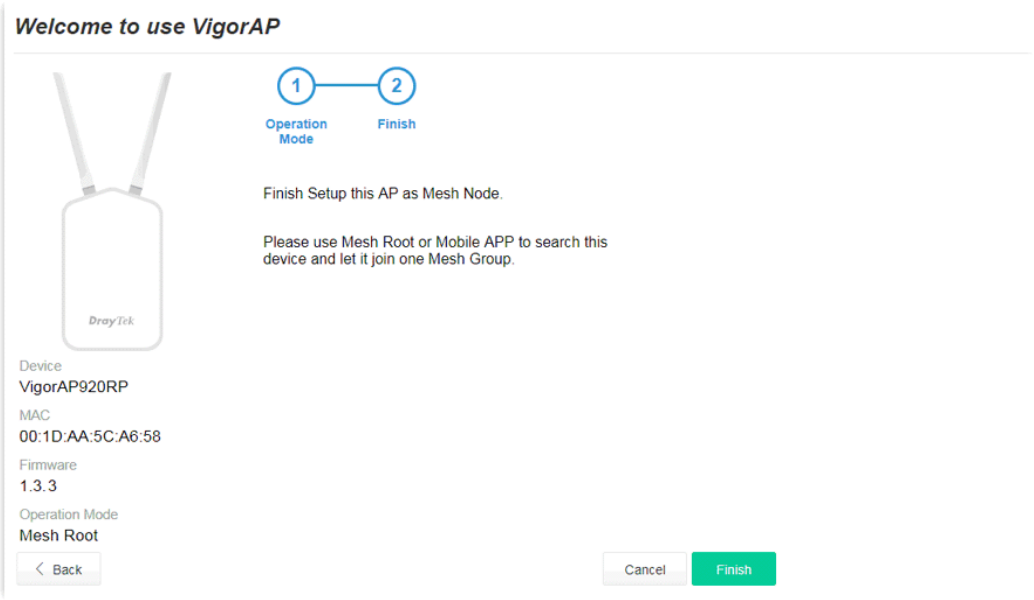


I-7-3 Settings for Mesh Node

1. Choose **Mesh Node** as the operation mode and click **Next Step**.

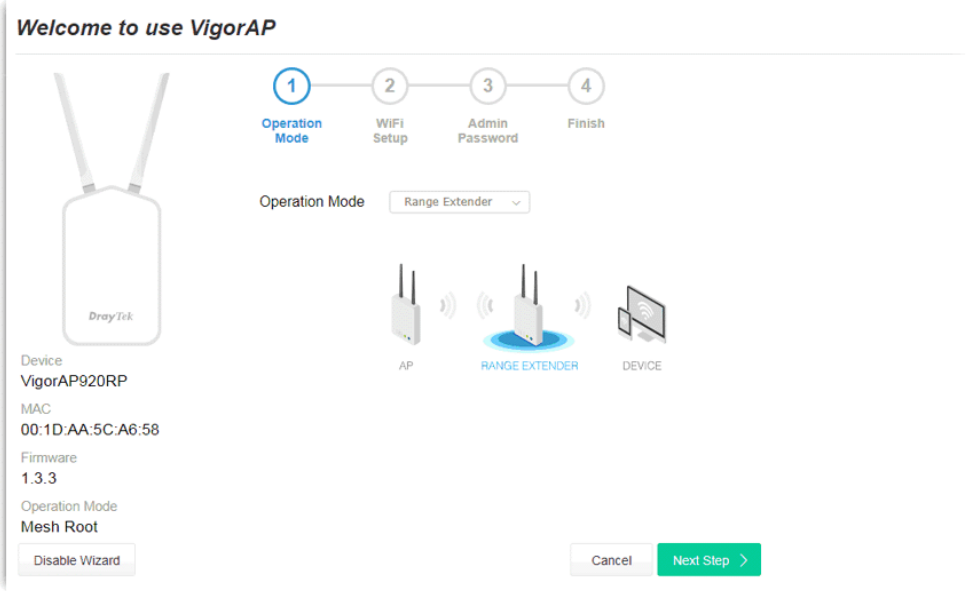


2. A summary of settings configuration will be shown on screen. Click **Finish**.

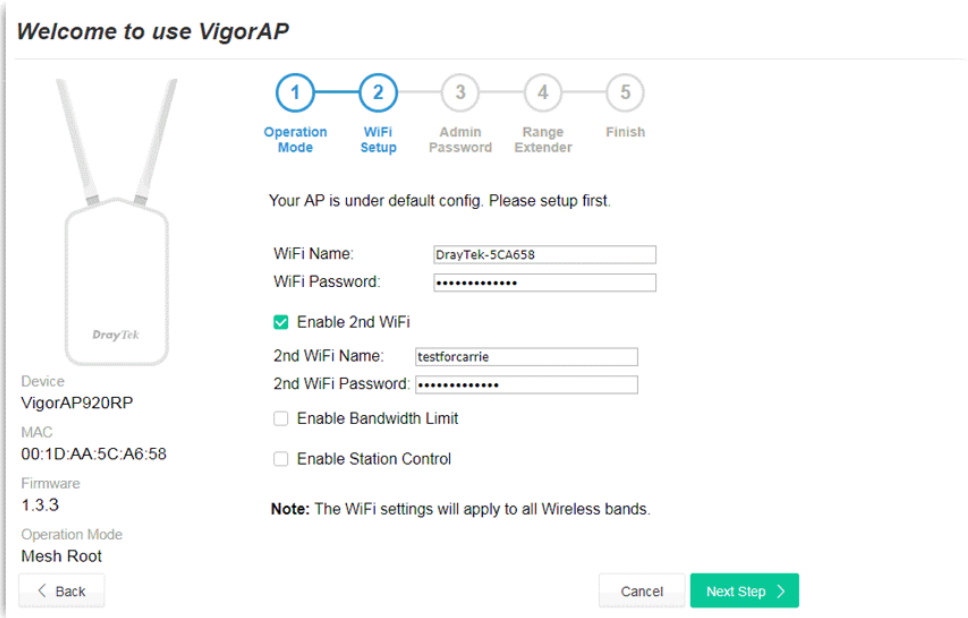


I-7-4 Settings for Range Extender

1. Choose **Range Extender** as the operation mode and click **Next Step**.



2. Configure the settings for wireless LAN (for both 2.4GHz and 5GHz) and click **Next Step**.

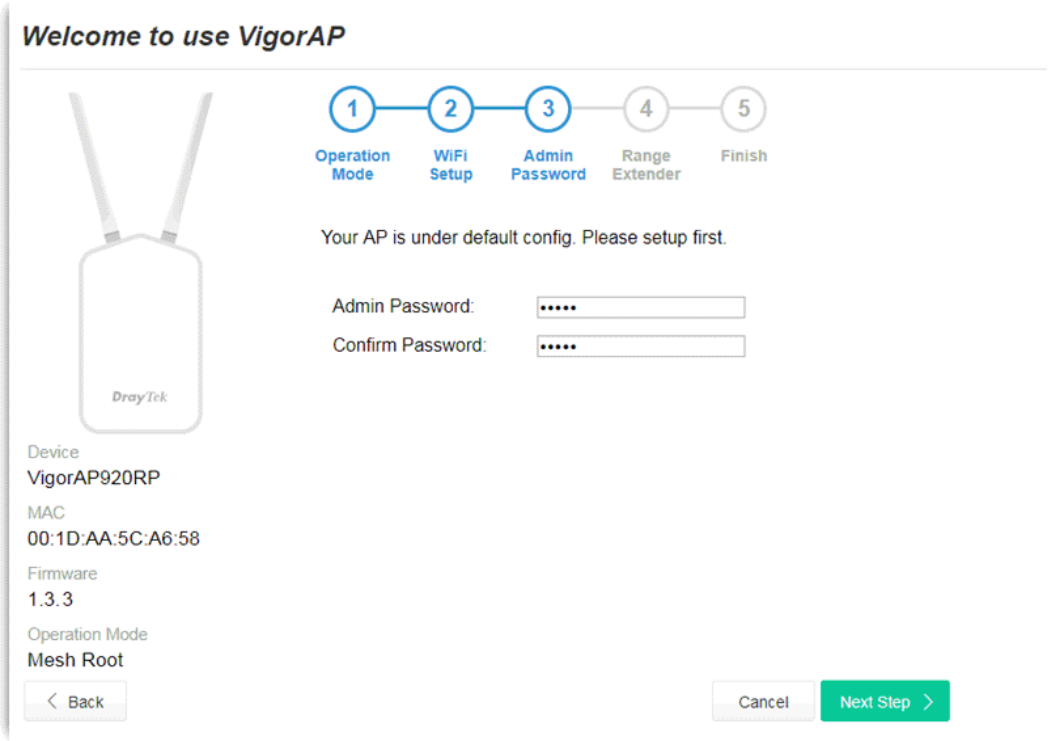


Available settings are explained as follows:

Item	Description
WiFi Name	Set a name for VigorAP 920R to be identified.
WiFi Password	Type **8~63** ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").
Enable 2nd Wireless	Check the box to enable the **guest** wireless setting. Such feature is especially useful for free Wi-Fi service. For example, a coffee shop offers free Wi-Fi service for its guests for one hour every day.

	2nd WiFi Name - Set a name for VigorAP 920R which can be identified and connected by wireless guest. **2nd WiFi Password -** Set **8~63** ASCII characters or **8~63** ASCII characters which can be used for logging into VigorAP 920R by wireless guest.
Enable Bandwidth Limit	Check the box to define the maximum speed of the data uploading/downloading which will be used for the guest connecting to Vigor device with the same SSID. **Upload Limit** – Scroll the radio button to choose the value you want. **Download Limit** –Scroll the radio button to choose the value you want.
Enable Station Control	Check the box to set the duration for the guest connecting /reconnecting to Vigor device. **Connection Time** –Scroll the radio button to choose the value you want. **Reconnection Time** –Scroll the radio button to choose the value you want.

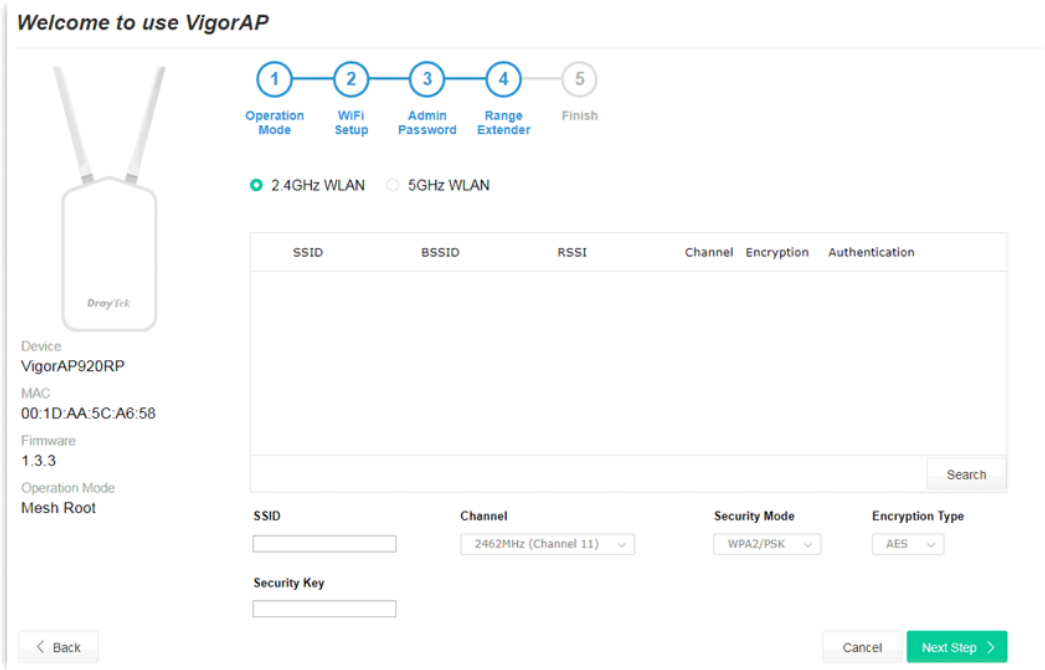
3. Change the default password for such device with new value. Then click **Next Step**.



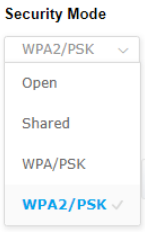
Available settings are explained as follows:

Item	Description
Admin Password	Enter a new password.
Confirm Password	Enter the new password again for confirmation.

4. A summary of settings configuration will be shown on screen. Click **Finish**.

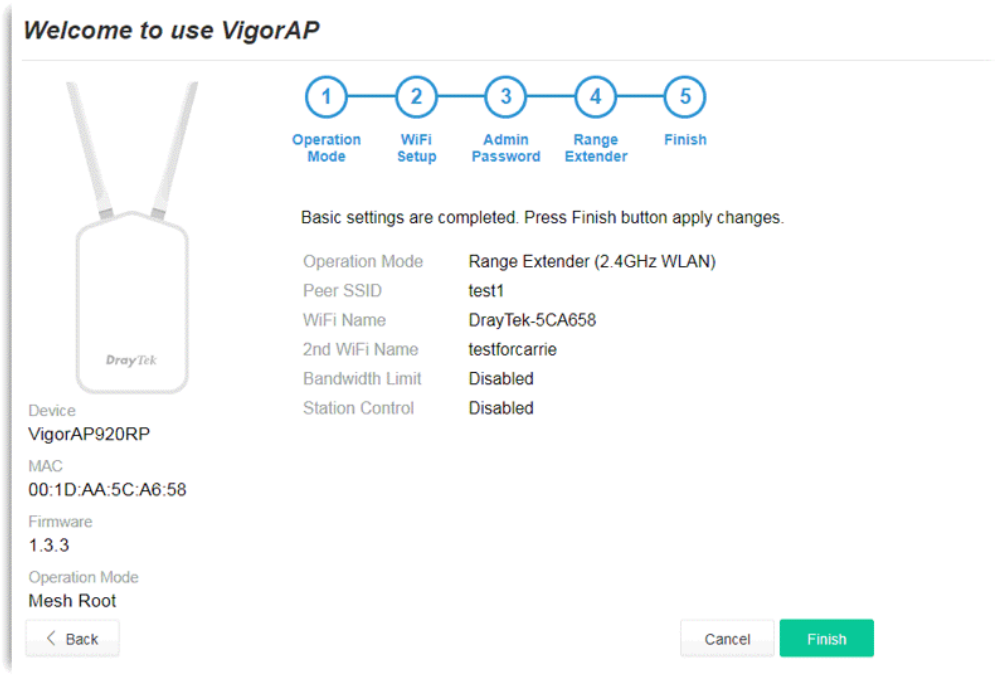


Available settings are explained as follows:

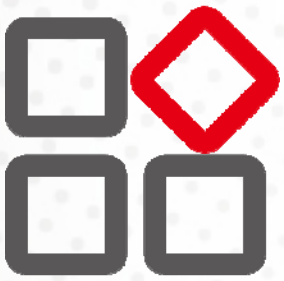
Item	Description
SSID	Set a name for VigorAP 920R to be identified.
Channel	Means the channel frequency of the wireless LAN. You may switch channel if the selected channel is under serious interference.
Security Mode	There are several modes provided for you to choose. Each mode will bring up different parameters (e.g., WEP keys, Pass Phrase) for you to configure. 
Encryption Type	Available options will vary according to the selected **Security Mode**. When **Open** is selected: ● Choose **None** to disable the WEP Encryption. Data sent to the AP will not be encrypted. ● **WEP Keys** –To enable WEP encryption for data transmission, please choose **WEP**. Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ','. When **Shared** is selected: ● **WEP Keys** - To enable WEP encryption for data transmission, please choose **WEP**. Four keys can be entered here, but only one

	key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ','. When **WPA/PSK** or **WPA2/PSK** is selected: ● Select **TKIP** or **AES** as the algorithm for WPA. ● **Security Key** - Select WEP, TKIP or AES as the encryption algorithm. Type **8~63** ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

5. A summary of settings configuration will be shown on screen. Click **Finish**.

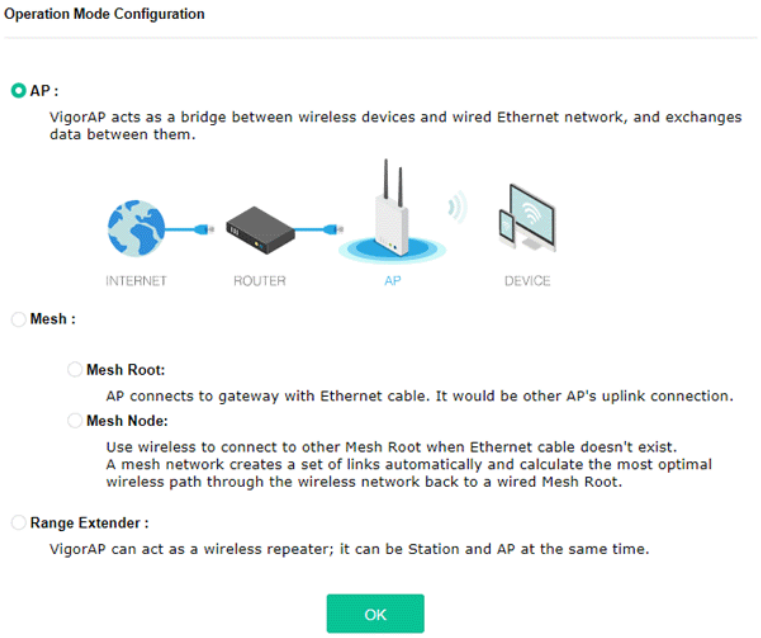


Chapter II Connectivity



II-1 Operation Mode

This page provides several available modes for you to choose for different conditions. Click any one of them and click **OK**. The system will configure the required settings automatically.



Available settings are explained as follows:

Item	Description
AP	This mode allows wireless clients to connect to access point and exchange data with the devices connected to the wired network.
Mesh	**Mesh Root –** VigorAP must connect to a gateway with an Ethernet cable. **Mesh Node –** VigorAP can connect to other mesh root via wireless connection. A mesh network creates one set of links automatically and calculates the most optimal wireless path through the wireless network back to a wired mesh root.
Range Extender	VigorAP can act as a wireless repeater which will help you to extend the networking wirelessly. The access point can act as Station and AP at the same time. It can use Station function to connect to a Root AP and use AP function to service all wireless clients within its coverage.

Note:

The Wireless LAN settings will be changed according to the Operation Mode selected here. For the detailed information, please refer to the section of Wireless LAN.

II-2 General Concepts for Wireless LAN (2.4GHz/5GHz)

VigorAP 920R is a highly integrated wireless local area network (WLAN) for 5 GHz 802.11ac or 2.4/5 GHz 802.11n WLAN applications. It supports channel operations of 20/40 MHz at 2.4 GHz and 20/40/80 MHz at 5 GHz. VigorAP 920R can support data rates up to 867 MBps in 802.11ac 80 MHz channels.

Note:

* The actual data throughput will vary according to the network conditions and environmental factors, including volume of network traffic, network overhead and building materials.

VigorAP 920R plays a role as an Access Point (AP) connecting to lots of wireless clients or Stations (STA). All the STAs will share the same Internet connection via VigorAP 920R. The **General Setup** will set up the information of this wireless network, including its SSID as identification, located channel etc.

Security Overview

WEP (Wired Equivalent Privacy) is a legacy method to encrypt each frame transmitted via radio using either a 64-bit or 128-bit key. Usually access point will preset a set of four keys and it will communicate with each station using only one out of the four keys.

WPA (Wi-Fi Protected Access), the most dominating security mechanism in industry, is separated into two categories: WPA-personal or called WPA Pre-Share Key (WPA/PSK), and WPA-Enterprise or called WPA/802.1x.

In WPA-Personal, a pre-defined key is used for encryption during data transmission. WPA applies Temporal Key Integrity Protocol (TKIP) for data encryption while WPA2 applies AES. The WPA-Enterprise combines not only encryption but also authentication.

Since WEP has been proved vulnerable, you may consider using WPA for the most secure connection. You should select the appropriate security mechanism according to your needs. No matter which security suite you select, they all will enhance the over-the-air data protection and /or privacy on your wireless network. The VigorAP 920R is very flexible and can support multiple secure connections with both WEP and WPA at the same time.

WPS Introduction

WPS (Wi-Fi Protected Setup) provides easy procedure to make network connection between wireless station and wireless access point (VigorAP 920R) with the encryption of WPA and WPA2.

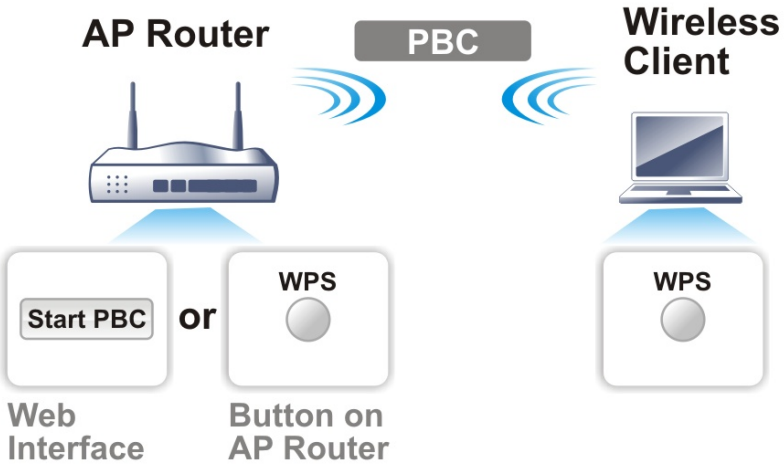
It is the simplest way to build connection between wireless network clients and VigorAP 920R. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for client and VigorAP 920R automatically.

Note:

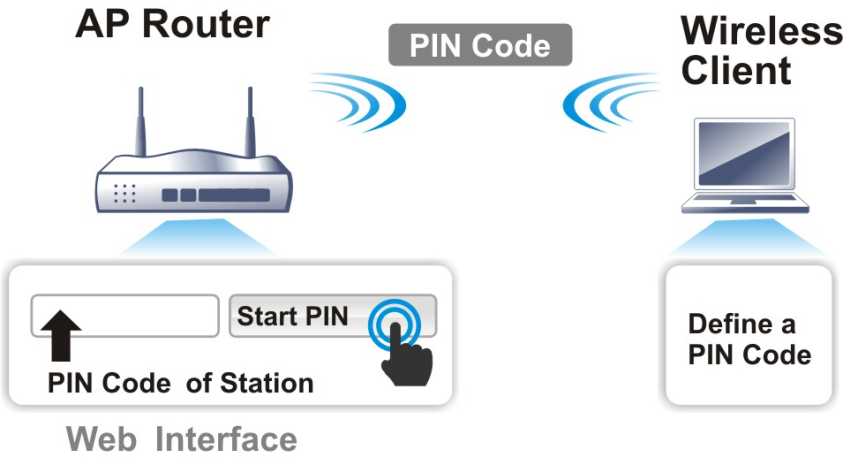
Such function is available for the wireless station with WPS supported.

There are two methods to do network connection through WPS between AP and Stations: pressing the ***Start PBC*** button or using ***PIN Code***.

On the side of VigorAP 920R series which served as an AP, press **WPS** button once on the front panel of VigorAP 920R or click **Start PBC** on web configuration interface. On the side of a station with network card installed, press **Start PBC** button of network card.

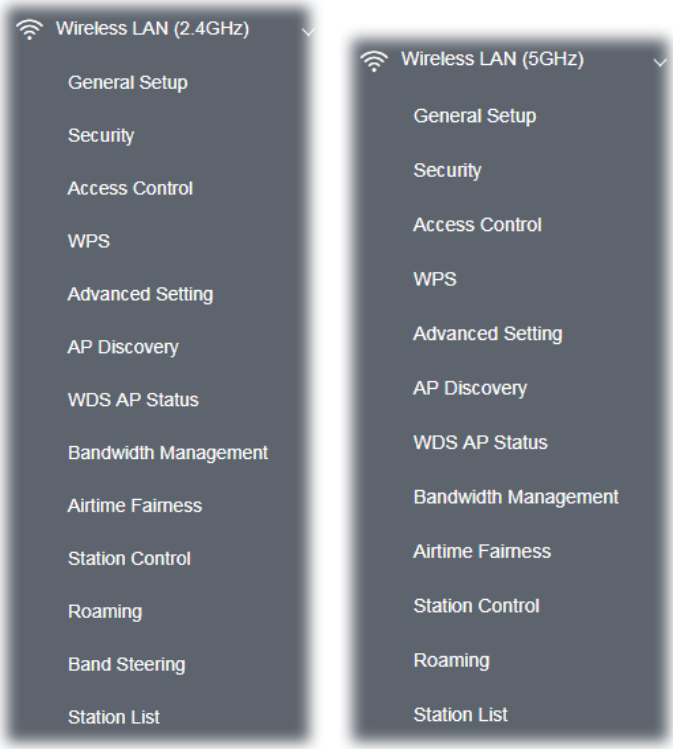


If you want to use PIN code, you have to know the PIN code specified in wireless client. Then provide the PIN code of the wireless client you wish to connect to the VigorAP 920R.


AP Router
PIN Code
Wireless Client
Start PIN
PIN Code of Station
Define a PIN Code
Web Interface

II-3 Wireless LAN (2.4GHz/5GHz) Settings for AP Mode

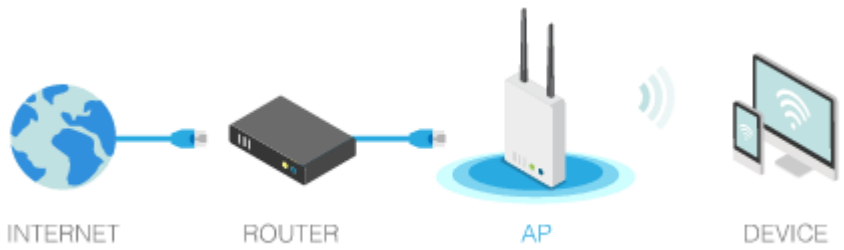
When you choose **AP** as the operation mode, the Wireless LAN menu items will include General Setup, Security, Access Control, WPS, Advanced Setting, AP Discovery, WDS AP Status, WMM Configuration, Bandwidth Management, Airtime Fairness, Station Control, Roaming, Band Steering and Station List.



Note:

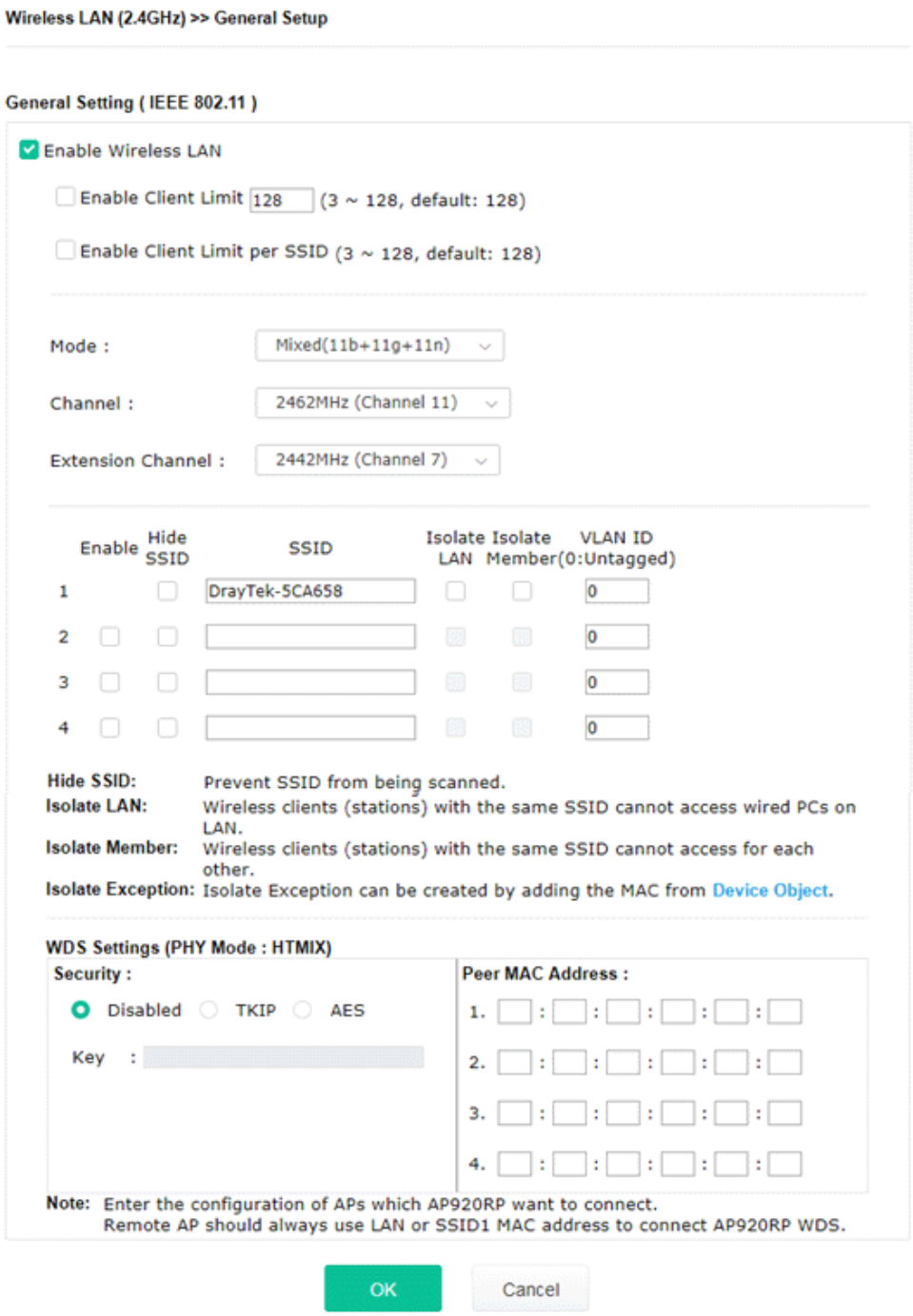
Available settings for **Wireless LAN (2.4GHz) and Wireless LAN (5Ghz)** are almost the same, except for Band Steering.

The following figure shows how VigorAP runs as AP (Access Point)



II-3-1 General Setup

By clicking the **General Setup**, a new web page will appear so that you could configure the SSID and the wireless channel. Please refer to the following figure for more information.



Available settings are explained as follows:

Item	Description
Enable Wireless LAN	Check the box to enable wireless function.
Enable Client Limit	Check the box to set the maximum number of wireless stations which try to connect Internet through Vigor device. The number you can set is from 3 to 64.

Enable Client Limit per SSID	Define the maximum number of wireless stations per SSID which try to connect to Internet through Vigor device. The number you can set is from 3 to 64.
Mode	At present, VigorAP 920R can connect to 11a Only, 11n Only, 11n Only (5G), Mixed (11b+11g), Mixed (11a+11n), Mixed (11b+11g+11n) and Mixed (11a+11n+11ac) stations simultaneously. Simply use the default one.
Channel	Means the channel of frequency of the wireless LAN. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select **AutoSelect** to let system determine for you. **Filtered Out List –** Such link will be shown if **AutoSelect** is selected as **Channel**. Click such link to access into **Wireless LAN >> Advanced Settings** page.
Extension Channel	It is available for wireless LAN (2.4GHz) With 802.11n, there is one option to double the bandwidth per channel. The available extension channel options will be varied according to the **Channel** selected above. Configure the extension channel you want.
Hide SSID	Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about VigorAP 920R while site surveying. The system allows you to set four sets of SSID for different usage.
SSID	Set a name for VigorAP 920R to be identified. Default settings are DrayTek-LAN-A and DrayTek-LAN-B. When **Enable 2 Subnet** is enabled, you can specify subnet interface (LAN-A or LAN-B) for each SSID by using the drop down menu.
Isolate LAN	Check this box to isolate the wireless connection from LAN. It can make the wireless clients (stations) with remote-dial and LAN to LAN users not accessing for each other.
Isolate Member	Check this box to make the wireless clients (stations) with the same SSID not access for each other.
VLAN ID	Type the value for such SSID. Packets transferred from such SSID to LAN will be tagged with the number. If your network uses VLANs, you can assign the SSID to a VLAN on your network. Client devices that associate using the SSID are grouped into this VLAN. The VLAN ID range is from 3 to 4095. The VLAN ID is 0 by default, it means disabling the VLAN function for the SSID.
PHY Mode	Data will be transmitted via HTMIX mode. Each access point should be setup to the same **PHY Mode** for

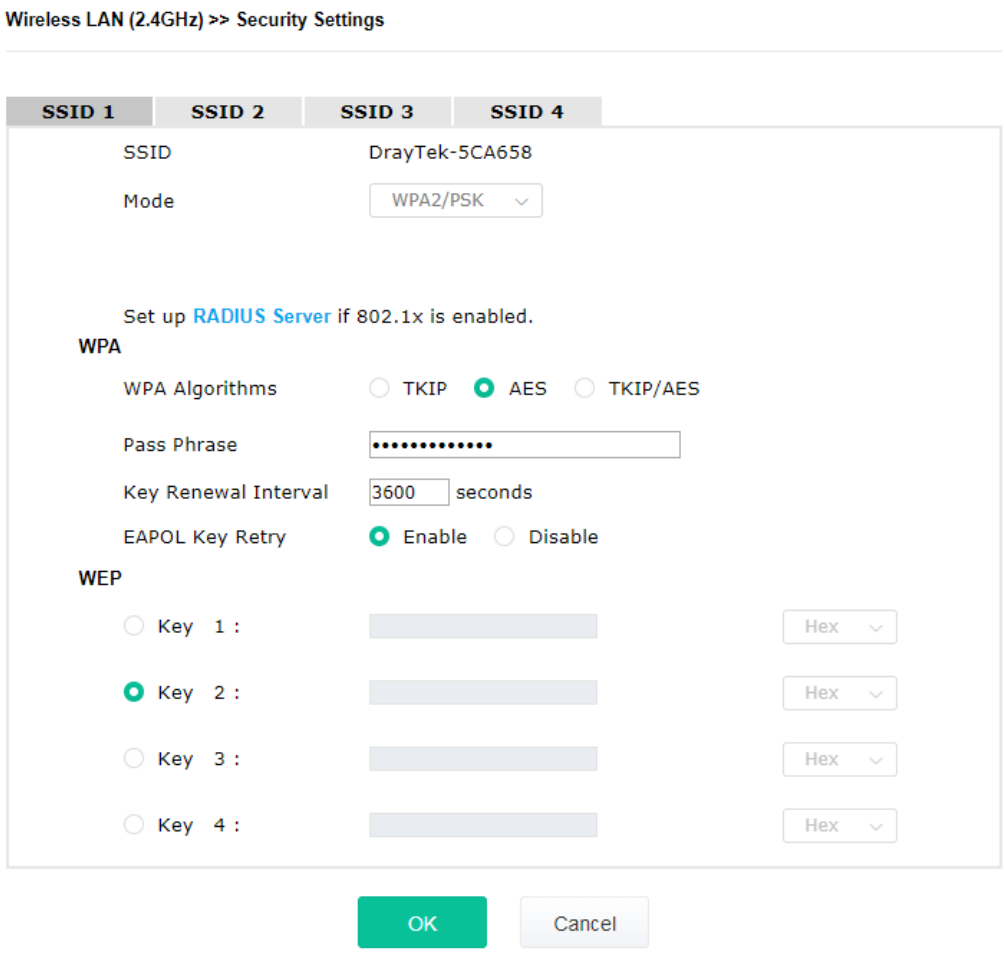
	connecting with each other.
Security	Select TKIP or AES as the encryption algorithm. Type the key number if required.
Peer MAC Address	Type the peer MAC address for the access point that VigorAP 920RP connects to.

After finishing this web page configuration, please click **OK** to save the settings.

II-3-2 Security

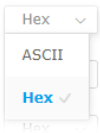
This page allows you to set security with different modes for SSID 1, 2, 3 and 4 respectively. After configuring the correct settings, please click **OK** to save and invoke it.

By clicking the **Security Settings**, a new web page will appear so that you could configure the settings.

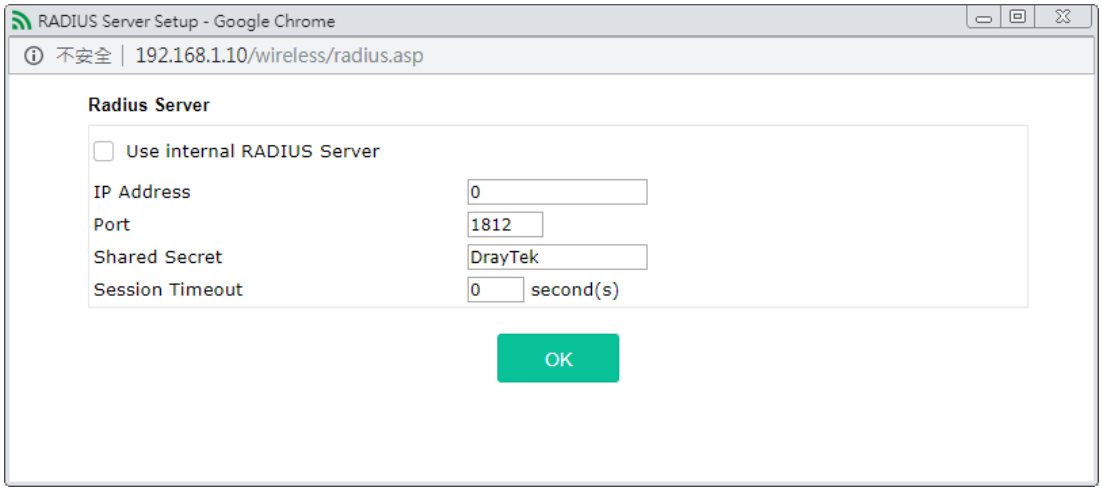


Available settings are explained as follows:

Item	Description
Mode	There are several modes provided for you to choose. **Disable** - The encryption mechanism is turned off. **WEP** - Accepts only WEP clients and the encryption key should be entered in WEP Key. **WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK -** Accepts only WPA clients and the encryption key should be entered in PSK. The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. **WEP/802.1x -** The built-in RADIUS client feature enables VigorAP 920R to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access authentication for network management. The WPA encrypts each frame transmitted from the radio using the

	key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Select WPA, WPA2 or Auto as WPA mode. **WPA/802.1x -** The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. **WPA2/802.1x -** The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication.
WPA Algorithms	Select TKIP, AES or TKIP/AES as the algorithm for WPA. Such feature is available for **WPA2/802.1x, WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK** mode.
Pass Phrase	Type **8~63** ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). Such feature is available for **WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK** mode.
Key Renewal Interval	WPA uses shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key that is periodically replaced. Enter the renewal security time (seconds) in the column. Smaller interval leads to greater security but lower performance. Default is 3600 seconds. Set 0 to disable re-key. Such feature is available for **WPA2/802.1,WPA/802.1x, WPA/PSK or WPA2/PSK or Mixed (WPA+WPA2)/PSK** mode.
EAPOL Key Retry	EAPOL means Extensible Authentication Protocol over LAN. Click **Enable** to make sure that the key will be installed and used once in order to prevent key reinstallation attack.
WEP	**Disable** - Disable the WEP Encryption. Data sent to the AP will not be encrypted. **Enable** - Enable the WEP Encryption. Such feature is available for **WEP/802.1x** mode.
Key 1 – Key 4	Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ','. Such feature is available for **WEP** mode. 

Click the link of **RADIUS Server** to access into the following page for more settings.



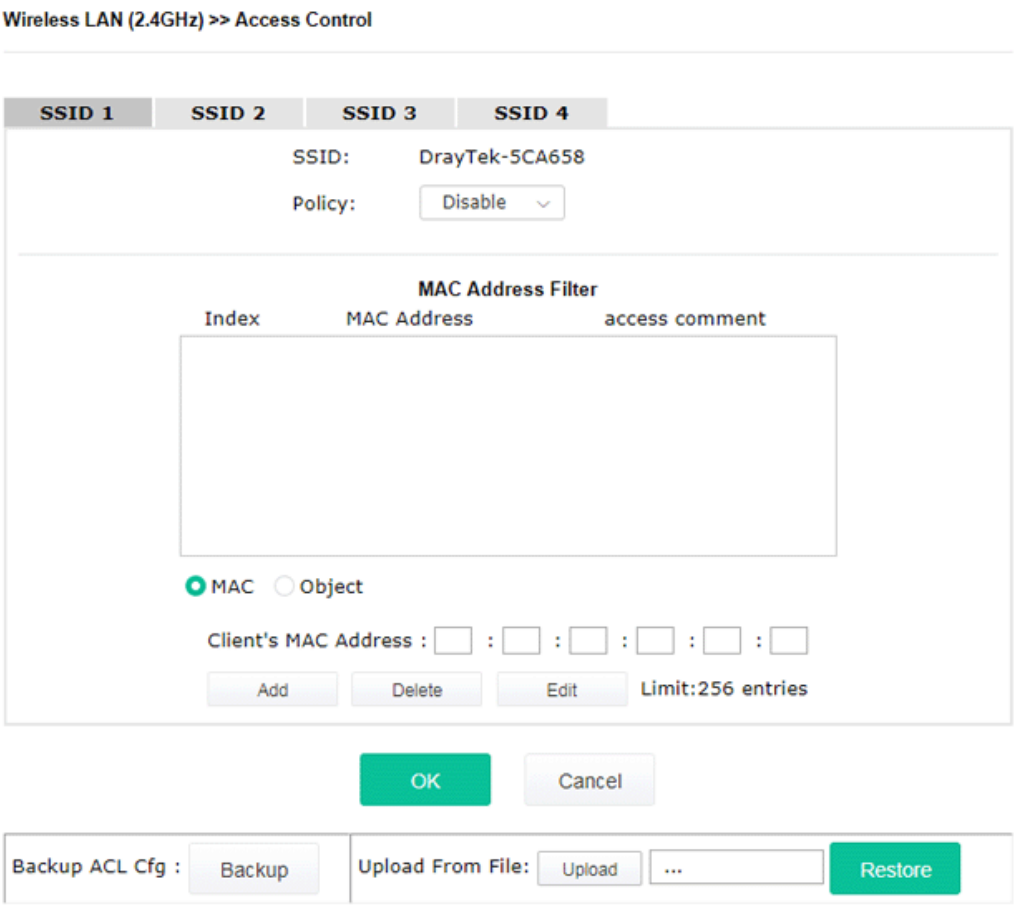
Available settings are explained as follows:

Item	Description
Use internal RADIUS Server	There is a RADIUS server built in VigorAP 920R which is used to authenticate the wireless client connecting to the access point. Check this box to use the internal RADIUS server for wireless security. Besides, if you want to use the external RADIUS server for authentication, do not check this box. Please refer to the section, **IV-1-1 RADIUS Server** to configure settings for internal server of VigorAP 920R.
IP Address	Enter the IP address of external RADIUS server.
Port	The UDP port number that the external RADIUS server is using. The default value is 1812, based on RFC 2138.
Shared Secret	The external RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.
Session Timeout	Set the maximum time of service provided before re-authentication. Set to zero to perform another authentication immediately after the first authentication has successfully completed. (The unit is second.)

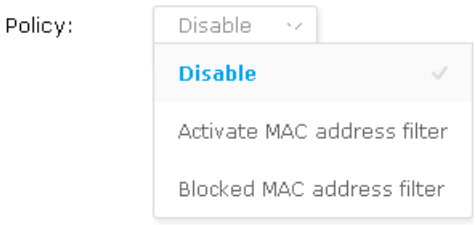
After finishing this web page configuration, please click **OK** to save the settings.

II-3-3 Access Control

For additional security of wireless access, the **Access Control** facility allows you to restrict the network access right by controlling the wireless LAN MAC address of client. Only the valid MAC address that has been configured can access the wireless LAN interface. By clicking the **Access Control**, a new web page will appear, as depicted below, so that you could edit the clients' MAC addresses to control their access rights (deny or allow).



Available settings are explained as follows:

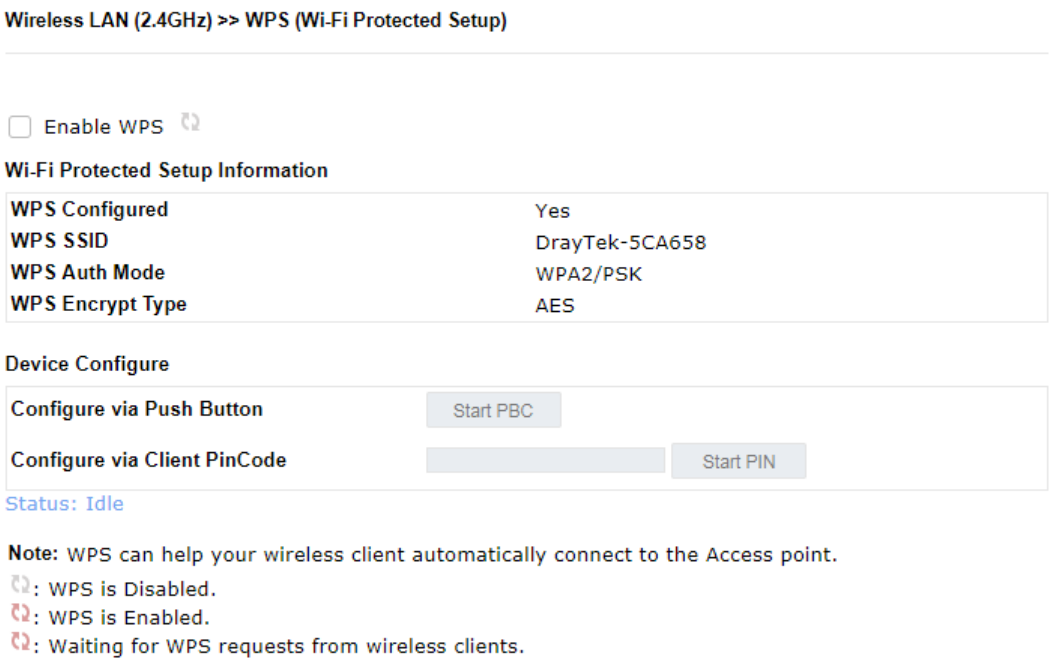
Item	Description
Policy	Select to enable any one of the following policy or disable the policy. Choose **Activate MAC address filter** to type in the MAC addresses for other clients in the network manually. Choose **Blocked MAC address filter,** so that all of the devices with the MAC addresses listed on the MAC Address Filter table will be blocked and cannot access into VigorAP 920R. 
MAC Address Filter	Display all MAC addresses that are edited before.
Client's MAC Address	Manually enter the MAC address of wireless client.

Add	Add a new MAC address into the list.
Delete	Delete the selected MAC address in the list.
Edit	Edit the selected MAC address in the list.
Cancel	Give up the access control set up.
Backup	Click it to store the settings (MAC addresses on MAC Address Filter table) on this page as a file.
Restore	Click it to restore the settings (MAC addresses on MAC Address Filter table) from an existed file.

After finishing this web page configuration, please click **OK** to save the settings.

II-3-4 WPS

Open **Wireless LAN>>WPS** to configure the corresponding settings.



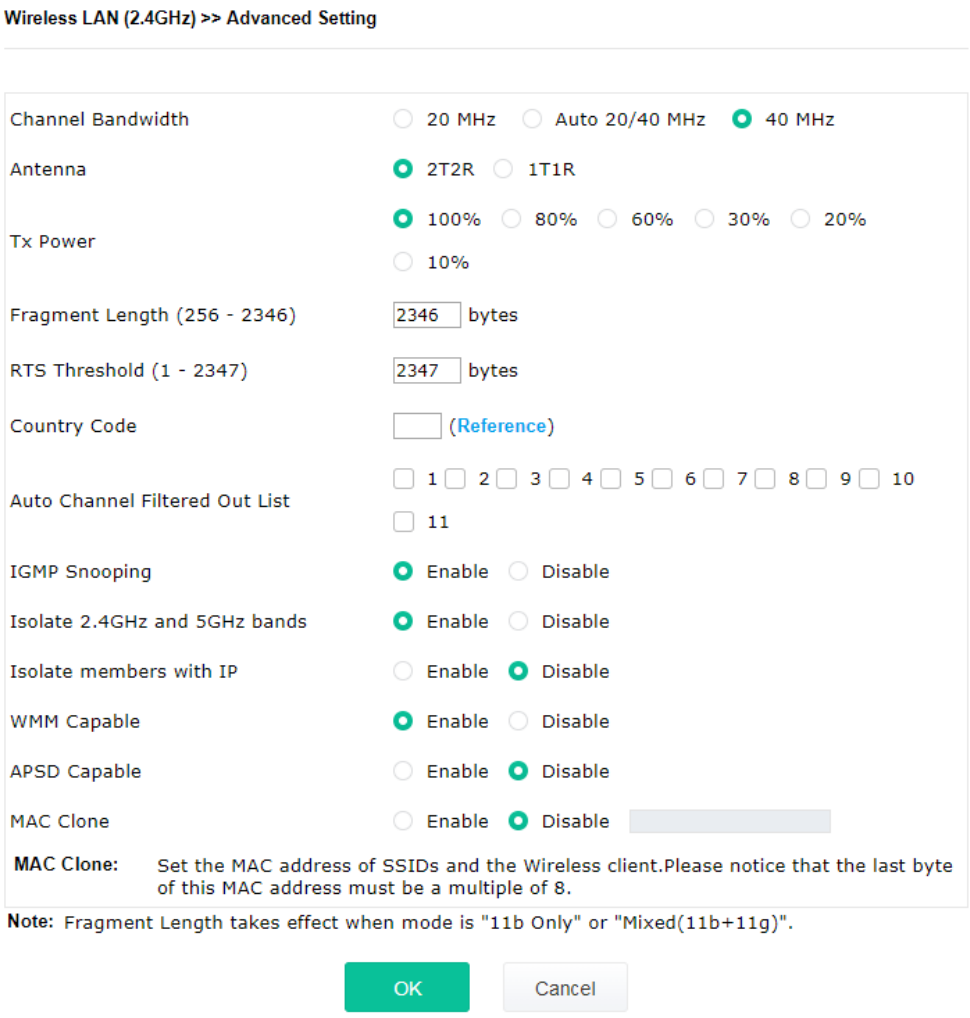
Available settings are explained as follows:

Item	Description
Enable WPS	Check this box to enable WPS setting.
WPS Configured	Display related system information for WPS. If the wireless security (encryption) function of VigorAP 920R is properly configured, you can see 'Yes' message here.
WPS SSID	Display current selected SSID.
WPS Auth Mode	Display current authentication mode of the VigorAP 920R. Only WPA2/PSK and WPA/PSK support WPS.
WPS Encrypt Type	Display encryption mode (None, WEP, TKIP, AES, etc.) of VigorAP 920R.
Configure via Push Button	Click **Start PBC** to invoke Push-Button style WPS setup procedure. VigorAP 920R will wait for WPS requests from wireless clients about two minutes. Both ACT and 2.4G WLAN LEDs on VigorAP 920R will blink quickly when WPS is in progress. It will return to normal

	condition after two minutes. (You need to setup WPS within two minutes)
Configure via Client PinCode	Type the PIN code specified in wireless client you wish to connect, and click **Start PIN** button. Both ACT and 2.4G WLAN LEDs on VigorAP 920R will blink quickly when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes).

II-3-5 Advanced Setting

This page is to determine which algorithm will be selected for wireless transmission rate.



Available settings are explained as follows:

Item	Description
Channel Width	**20 MHz-** the device will use 20MHz for data transmission and receiving between the AP and the stations. **Auto 20/40 MHz–** the AP will scan for nearby wireless AP, and then use 20MHz if the number of AP is more than 10, or use 40MHz if it's not. **40 MHz-** the device will use 40MHz for data transmission and receiving between the AP and the stations.

Antenna	VigorAP can be attached with two antennas to have good data transmission via wireless connection. However, if you have only one antenna attached, please choose 1T1R. Such feature is available for wireless LAN (2.4GHz).
Tx Power	The default setting is the maximum (100%). Lowering down the value may degrade range and throughput of wireless.
Fragment Length	Set the Fragment threshold of wireless radio. Do not modify default value if you don't know what it is, default value is 2346.
RTS Threshold	Minimize the collision (unit is bytes) between hidden stations to improve wireless performance. Set the RTS threshold of wireless radio. Do not modify default value if you don't know what it is, default value is 2347.
Country Code	VigorAP broadcasts country codes by following the 802.11d standard. However, some wireless stations will detect / scan the country code to prevent conflict occurred. If conflict is detected, wireless station will be warned and is unable to make network connection. Therefore, changing the country code to ensure successful network connection will be necessary for some clients.
Auto Channel Filtered Out List	The selected wireless channels will be discarded if **AutoSelect** is selected as **Channel** selection mode in **Wireless LAN>>General Setup**.
IGMP Snooping	Check **Enable** to enable IGMP Snooping. Multicast traffic will be forwarded to ports that have members of that group. Disabling IGMP snooping will make multicast traffic treated in the same manner as broadcast traffic.
Isolate 2.4GHz and 5GHz bands	The default setting is "Enable". It means that the wireless client using 2.4GHz band is unable to connect to the wireless client with 5GHz band, and vice versa. For WLAN 2.4GHz and 5GHz set with the same SSID name: ● No matter such function is enabled or disabled, clients using WLAN 2.4GHz and 5GHz can communicate for each other if **Isolate Member** (in **Wireless LAN>>General Setup**) is NOT enabled for such SSID. ● Yet, if the function of **Isolate Member** (in **Wireless LAN>>General Setup**) is enabled for such SSID, clients using WLAN 2.4GHz and 5GHz will be unable to communicate with each other.
Isolate members with IP	The default setting is "Disable". If it is enabled, VigorAP will isolate different wireless clients according to their IP address(es).
WMM Capable	To apply WMM parameters for wireless data transmission, please click the **Enable** radio button.
APSD Capable	APSD (automatic power-save delivery) is an enhancement over the power-save mechanisms supported by Wi-Fi networks. It allows devices to take more time in sleeping state and consume less power to improve the performance by minimizing transmission latency. The default setting is **Disable**.
MAC Clone	Click **Enable** and manually enter the MAC address of the device with SSID 1. The MAC address of other SSIDs will change based on this

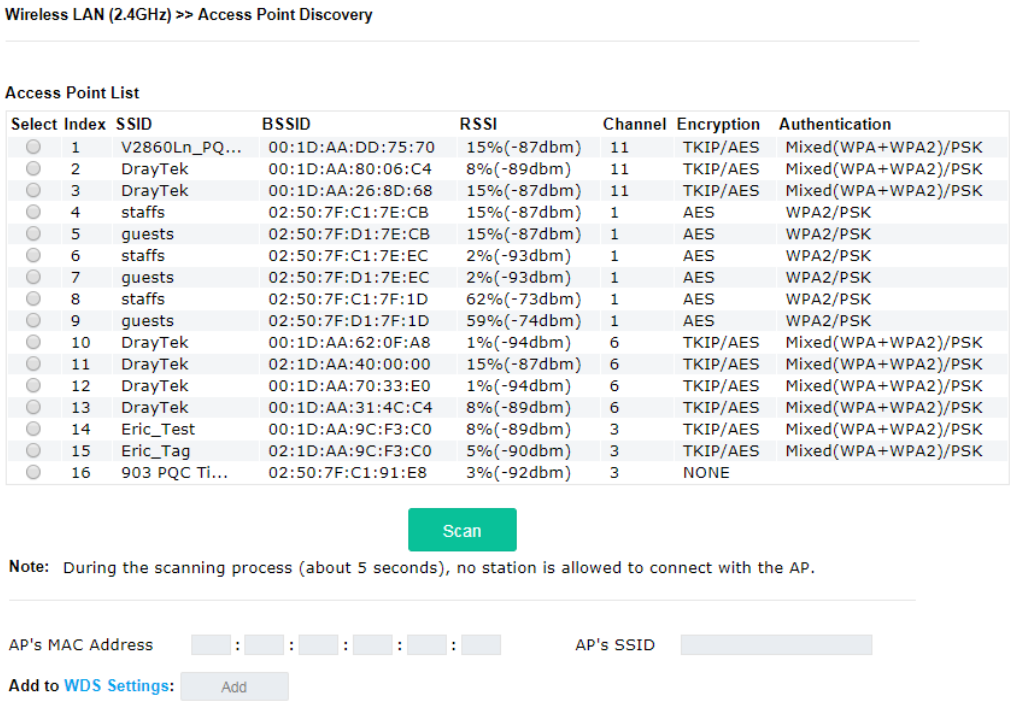
	MAC address. Such feature is available for wireless LAN (2.4GHz).

After finishing this web page configuration, please click **OK** to save the settings.

II-3-6 AP Discovery

VigorAP 920R can scan all regulatory channels and find working APs in the neighborhood. Based on the scanning result, users will know which channel is clean for usage. Also, it can be used to facilitate finding an AP for a WDS link. Notice that during the scanning process (about 5 seconds), no client is allowed to connect to Vigor.

This page is used to scan the existence of the APs on the wireless LAN. Please click **Scan** to discover all the connected APs.



Wireless LAN (2.4GHz) >> Access Point Discovery

Access Point List

Select	Index	SSID	BSSID	RSSI	Channel	Encryption	Authentication
○	1	V2860Ln_PQ...	00:1D:AA:DD:75:70	15%(-87dbm)	11	TKIP/AES	Mixed(WPA+WPA2)/PSK
○	2	DrayTek	00:1D:AA:80:06:C4	8%(-89dbm)	11	TKIP/AES	Mixed(WPA+WPA2)/PSK
○	3	DrayTek	00:1D:AA:26:8D:68	15%(-87dbm)	11	TKIP/AES	Mixed(WPA+WPA2)/PSK
○	4	staffs	02:50:7F:C1:7E:CB	15%(-87dbm)	1	AES	WPA2/PSK
○	5	guests	02:50:7F:D1:7E:CB	15%(-87dbm)	1	AES	WPA2/PSK
○	6	staffs	02:50:7F:C1:7E:EC	2%(-93dbm)	1	AES	WPA2/PSK
○	7	guests	02:50:7F:D1:7E:EC	2%(-93dbm)	1	AES	WPA2/PSK
○	8	staffs	02:50:7F:C1:7F:1D	62%(-73dbm)	1	AES	WPA2/PSK
○	9	guests	02:50:7F:D1:7F:1D	59%(-74dbm)	1	AES	WPA2/PSK
○	10	DrayTek	00:1D:AA:62:0F:A8	1%(-94dbm)	6	TKIP/AES	Mixed(WPA+WPA2)/PSK
○	11	DrayTek	02:1D:AA:40:00:00	15%(-87dbm)	6	TKIP/AES	Mixed(WPA+WPA2)/PSK
○	12	DrayTek	00:1D:AA:70:33:E0	1%(-94dbm)	6	TKIP/AES	Mixed(WPA+WPA2)/PSK
○	13	DrayTek	00:1D:AA:31:4C:C4	8%(-89dbm)	6	TKIP/AES	Mixed(WPA+WPA2)/PSK
○	14	Eric_Test	00:1D:AA:9C:F3:C0	8%(-89dbm)	3	TKIP/AES	Mixed(WPA+WPA2)/PSK
○	15	Eric_Tag	02:1D:AA:9C:F3:C0	5%(-90dbm)	3	TKIP/AES	Mixed(WPA+WPA2)/PSK
○	16	903 PQC Ti...	02:50:7F:C1:91:E8	3%(-92dbm)	3	NONE	

Scan

Note: During the scanning process (about 5 seconds), no station is allowed to connect with the AP.

AP's MAC Address : : : : : : AP's SSID

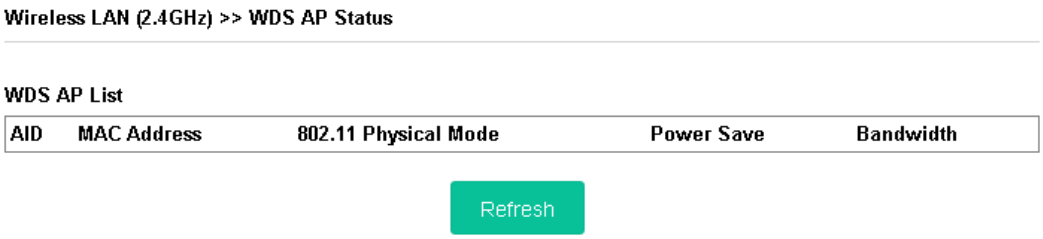
Add to WDS Settings: Add

Each item is explained as follows:

Item	Description
SSID	Display the SSID of the AP scanned by VigorAP 920R.
BSSID	Display the MAC address of the AP scanned by VigorAP 920R.
RSSI	Display the signal strength of the access point. RSSI is the abbreviation of Received Signal Strength Indication.
Channel	Display the wireless channel used for the AP that is scanned by VigorAP 920R.
Encryption	Display the encryption mode for the scanned AP.
Authentication	Display the authentication type that the scanned AP applied.
Scan	It is used to discover all the connected AP. The results will be shown on the box above this button
Add	If you want the found AP applying the WDS settings, please type in the AP's MAC address on the bottom of the page. Next, click **Add**. Later, the MAC address of the AP will be added to WDS settings page.

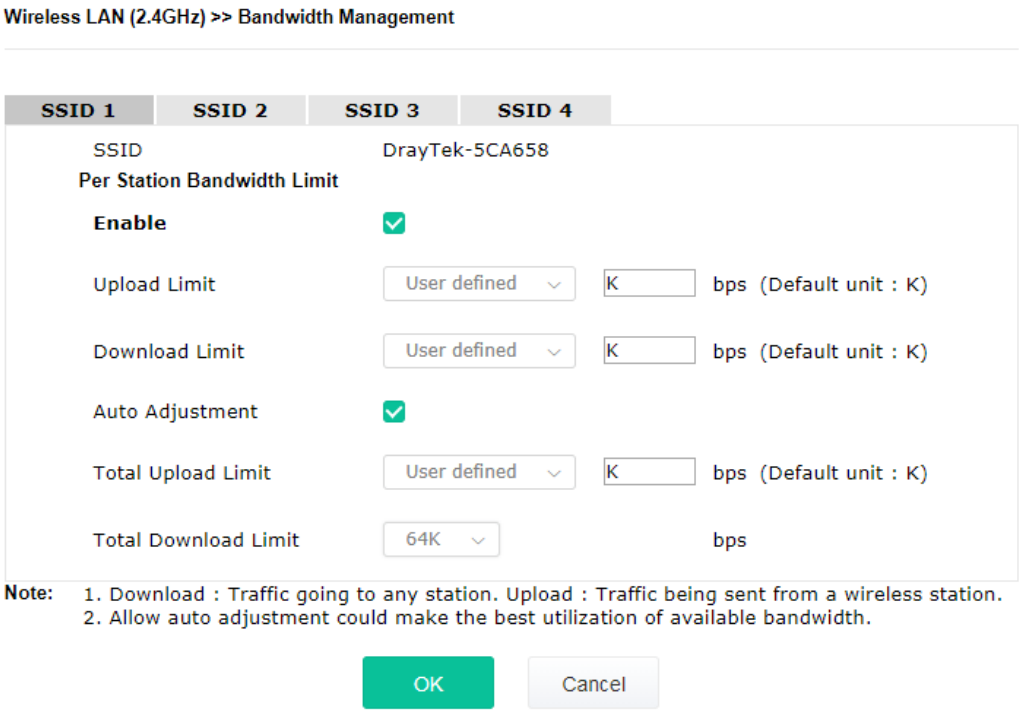
II-3-7 WDS AP Status

VigorAP 920RP can display the status such as MAC address, physical mode, power save and bandwidth for the working AP connected with WDS. Click **Refresh** to get the newest information.



II-3-8 Bandwidth Management

The downstream or upstream from FTP, HTTP or some P2P applications will occupy large of bandwidth and affect the applications for other programs. Please use Bandwidth Management to make the bandwidth usage more efficient.



Available settings are explained as follows:

Item	Description
SSID	Display the specific SSID name.
Enable	Check this box to enable the bandwidth management for clients.
Upload Limit	Define the maximum speed of the data uploading which will be used for the wireless stations connecting to Vigor device with the same SSID. Use the drop down list to choose the rate. If you choose **User defined**, you have to specify the rate manually.
Download Limit	Define the maximum speed of the data downloading which will be used for the wireless station connecting to Vigor device with the same

	SSID. Use the drop down list to choose the rate. If you choose **User defined**, you have to specify the rate manually.
Auto Adjustment	Check this box to have the bandwidth limit determined by the system automatically.
Total Upload Limit	When Auto Adjustment is checked, the value defined here will be treated as the total bandwidth shared by all of the wireless stations with the same SSID for data uploading.
Total Download Limit	When Auto Adjustment is checked, the value defined here will be treated as the total bandwidth shared by all of the wireless stations with the same SSID for data downloading.

After finishing this web page configuration, please click **OK** to save the settings.

II-3-9 Airtime Fairness

Airtime fairness is essential in wireless networks that must support critical enterprise applications.

Most of the applications are either symmetric or require more downlink than uplink capacity; telephony and email send the same amount of data in each direction, while video streaming and web surfing involve more traffic sent from access points to clients than the other way around. This is essential for ensuring predictable performance and quality-of-service, as well as allowing 802.11n and legacy clients to coexist on the same network. Without airtime fairness, offices using mixed mode networks risk having legacy clients slow down the entire network or letting the fastest client(s) crowd out other users.

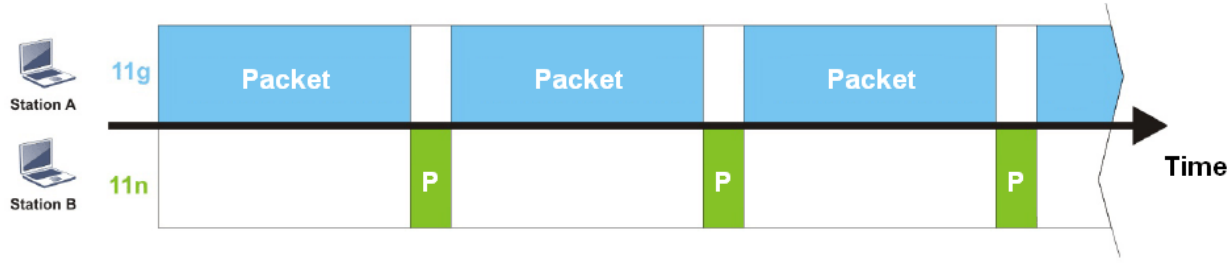
With airtime fairness, every client at a given quality-of-service level has equal access to the network's airtime.

The wireless channel can be accessed by only one wireless station at the same time.

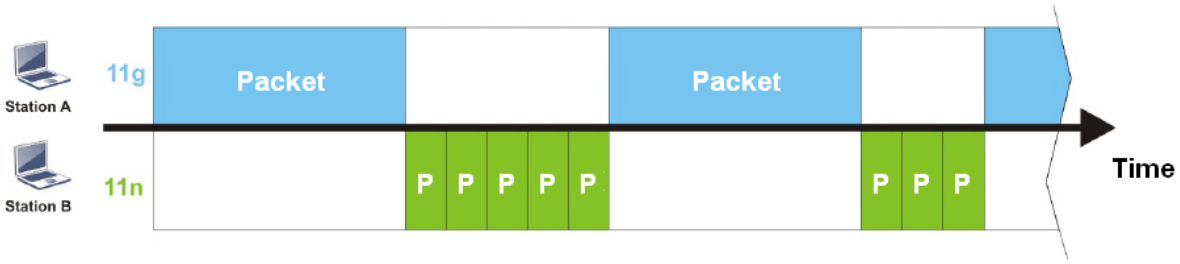
The principle behind the IEEE802.11 channel access mechanisms is that each station has ***equal probability*** to access the channel. When wireless stations have similar data rate, this principle leads to a fair result. In this case, stations get similar channel access time which is called airtime.

However, when stations have various data rate (e.g., 11g, 11n), the result is not fair. The slow stations (11g) work in their slow data rate and occupy too much airtime, whereas the fast stations (11n) become much slower.

Take the following figure as an example, both Station A(11g) and Station B(11n) transmit data packets through VigorAP 920R. Although they have equal probability to access the wireless channel, Station B(11n) gets only a little airtime and waits too much because Station A(11g) spends longer time to send one packet. In other words, Station B(fast rate) is obstructed by Station A(slow rate).



To improve this problem, Airtime Fairness is added for VigorAP 920R. Airtime Fairness function tries to assign *similar airtime* to each station (A/B) by controlling TX traffic. In the following figure, Station B(11n) has higher probability to send data packets than Station A(11g). By this way, Station B(fast rate) gets fair airtime and it's speed is not limited by Station A(slow rate).



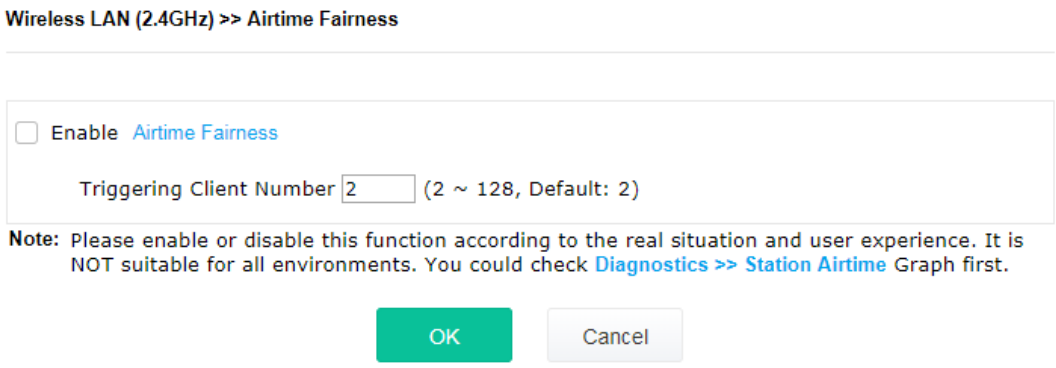
It is similar to automatic Bandwidth Limit. The dynamic bandwidth limit of each station depends on instant active station number and airtime assignment. Please note that Airtime Fairness of 2.4GHz and 5GHz are independent. But stations of different SSIDs function together, because they all use the same wireless channel. IN SPECIFIC ENVIRONMENTS, this function can reduce the bad influence of slow wireless devices and improve the overall wireless performance.

Suitable environment:

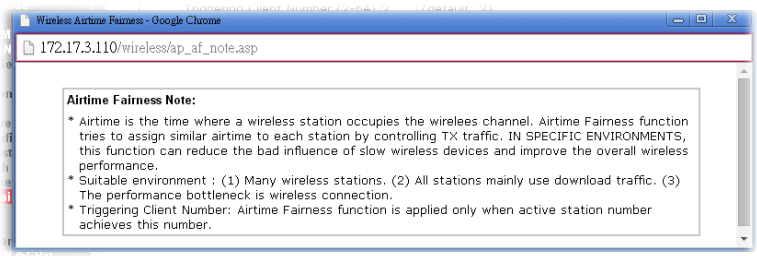
(1) Many wireless stations.

(2) All stations mainly use download traffic.

(3) The performance bottleneck is wireless connection.



Available settings are explained as follows:

Item	Description
Enable Airtime Fairness	Try to assign similar airtime to each wireless station by controlling TX traffic. **Airtime Fairness** – Click the link to display the following screen of airtime fairness note.  **Triggering Client Number –**Airtime Fairness function is applied only

	when active station number achieves this number.

After finishing this web page configuration, please click **OK** to save the settings.

Note:

Airtime Fairness function and Bandwidth Limit function should be mutually exclusive. So their webs have extra actions to ensure these two functions are not enabled simultaneously.

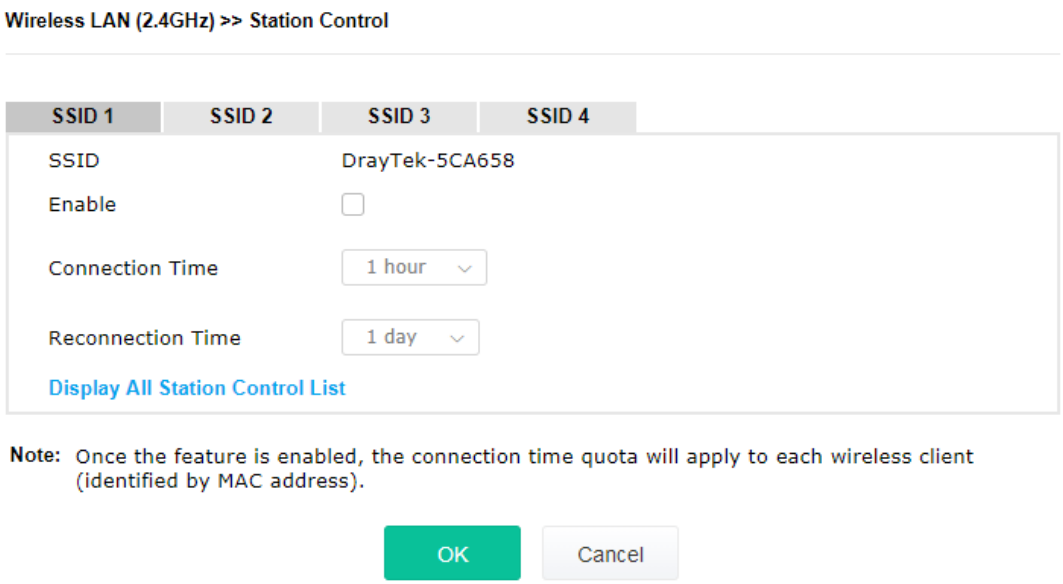
II-3-10 Station Control

Station Control is used to specify the duration for the wireless client to connect and reconnect VigorAP. If such function is not enabled, the wireless client can connect VigorAP until it shuts down.

Such feature is especially useful for free Wi-Fi service. For example, a coffee shop offers free Wi-Fi service for its guests for one hour every day. Then, the connection time can be set as “1 hour” and reconnection time can be set as “1 day”. Thus, the guest can finish his job within one hour and will not occupy the wireless network for a long time.

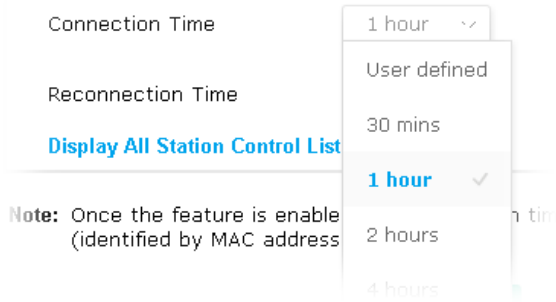
Note:

Up to 300 Wireless Station records are supported by VigorAP.



Available settings are explained as follows:

Item	Description
SSID	Display the SSID that the wireless station will use it to connect with Vigor router.
Enable	Check the box to enable the station control function.
Connection Time / Reconnection Time	Use the drop down list to choose the duration for the wireless client connecting /reconnecting to Vigor device. Or, type the duration manually when you choose **User defined**.

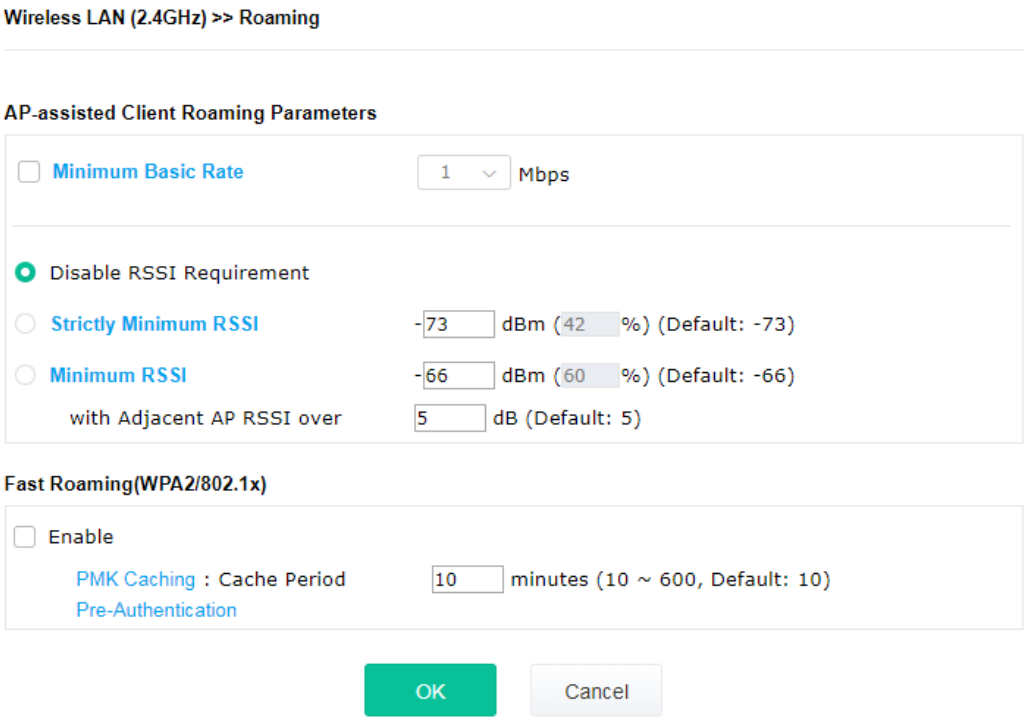
	
Display All Station Control List	All the wireless stations connecting to Vigor router by using such SSID will be listed on Station Control List.

After finishing all the settings here, please click **OK** to save the configuration.

II-3-11 Roaming

The network signal for a single wireless access point might be limited by its coverage range. Therefore, if you want to expand the wireless network in a large exhibition with a quick method, you can install multiple access points with enabling the Roaming feature for each AP to reach the purpose of expanding wireless signals seamlessly.

These access points connecting for each other shall be verified by pre-authentication. This page allows you to enable the roaming feature and the pre-authentication.



Available settings are explained as follows:

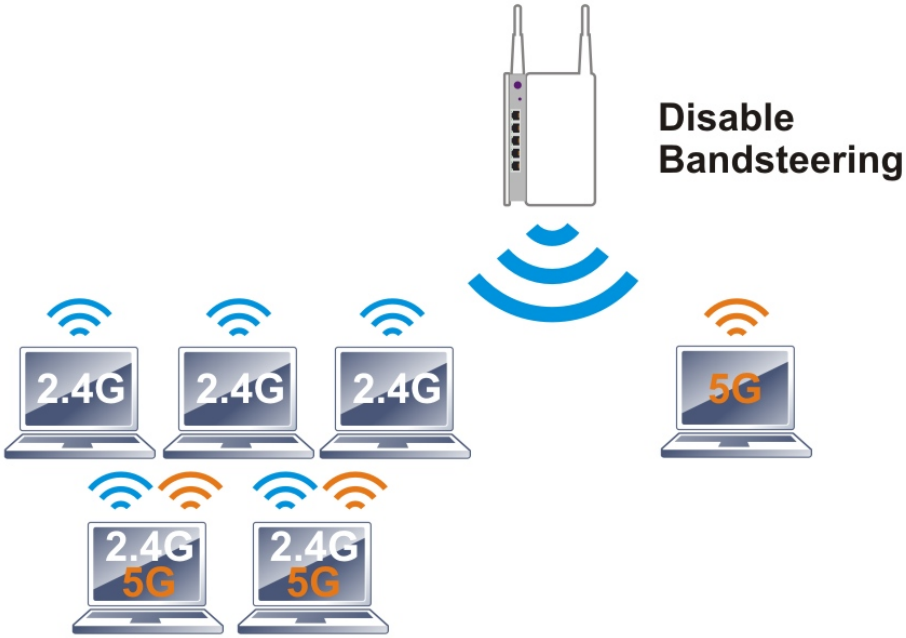
Item	Description
AP-assisted Client Roaming Parameters	When the link rate of wireless station is too low or the signal received by the wireless station is too worse, VigorAP 920R will automatically detect (based on the link rate and RSSI requirement) and cut off the

	network connection for that wireless station to assist it to connect another Wireless AP to get better signal. **Minimum Basic Rate –** Check the box to use the drop down list to specify a basic rate (**Mbps**). When the link rate of the wireless station is below such value, VigorAP 920R will terminate the network connection for that wireless station. **Disable RSSI Requirement -** If it is selected, VigorAP will not terminate the network connection based on RSSI. **Strictly Minimum RSSI -** VigorAP uses RSSI (received signal strength indicator) to decide to terminate the network connection of wireless station. When the signal strength is below the value (**dBm**) set here, VigorAP 920R will terminate the network connection for that wireless station. **Minimum RSSI -** When the signal strength of the wireless station is below the value (**dBm**) set here and adjacent AP (must be DrayTek AP and support such feature too) with higher signal strength value (defined in the field of **With Adjacent AP RSSI over**) is detected by VigorAP 920R, VigorAP 920R will terminate the network connection for that wireless station. Later, the wireless station can connect to the adjacent AP (with better RSSI). • **With Adjacent AP RSSI over –** Specify a value as a threshold.
Fast Roaming (WPA2/802.1x)	**Enable –** Check the box to enable fast roaming configuration. **PMK Caching -** Set the expire time of WPA2 PMK (Pairwise master key) cache. PMK Cache manages the list from the BSSIDs in the associated SSID with which it has pre-authenticated. Such feature is available for **WPA2/802.1** mode. **Pre-Authentication -** Enables a station to authenticate to multiple APs for roaming securer and faster. With the pre-authentication procedure defined in IEEE 802.11i specification, the pre-four-way-handshake can reduce handoff delay perceivable by a mobile node. It makes roaming faster and more secure. (Only valid in WPA2) **Enable** - Enable IEEE 802.1X Pre-Authentication. **Disable** - Disable IEEE 802.1X Pre-Authentication.

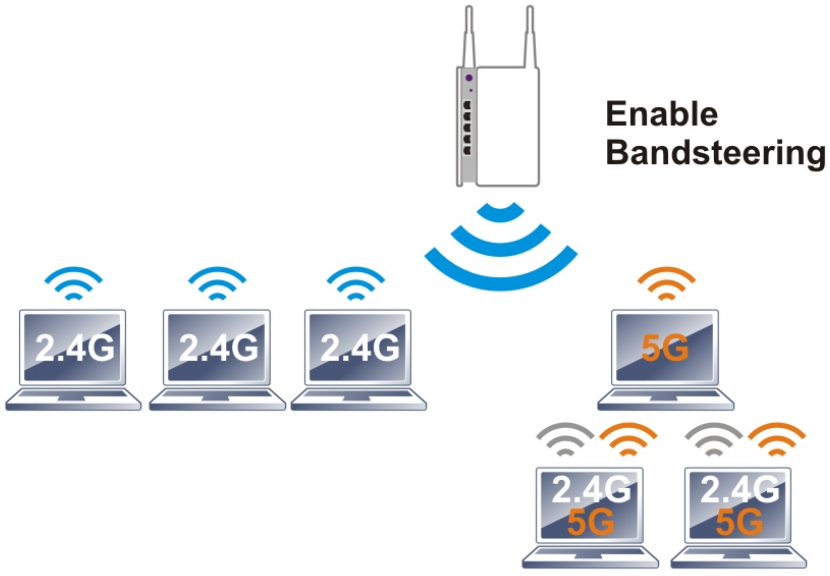
After finishing this web page configuration, please click **OK** to save the settings.

II-3-12 Band Steering

Band Steering detects if the wireless clients are capable of 5GHz operation, and steers them to that frequency. It helps to leave 2.4GHz band available for legacy clients, and improves users experience by reducing channel utilization.



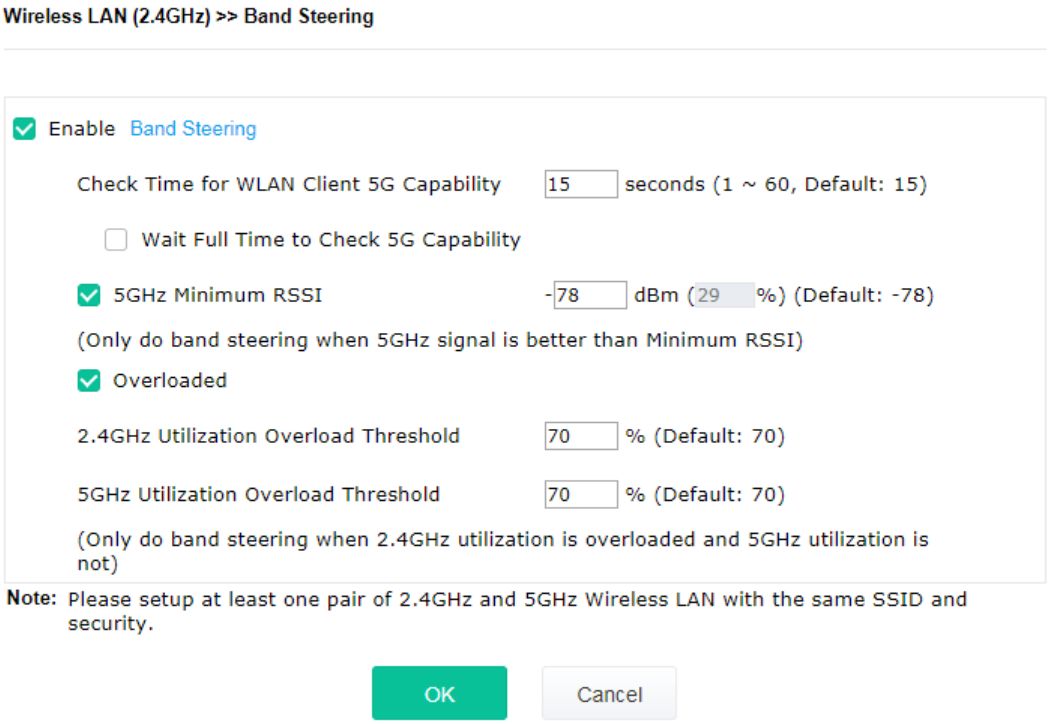
If dual-band is detected, the AP will let the wireless client connect to less congested wireless LAN, such as 5GHz to prevent from network congestion.



Note:

To make Band Steering work successfully, SSID and security on 2.4GHz also MUST be broadcasted on 5GHz.

Open **Wireless LAN (2.4GHz)>>Band Steering** to get the following web page:

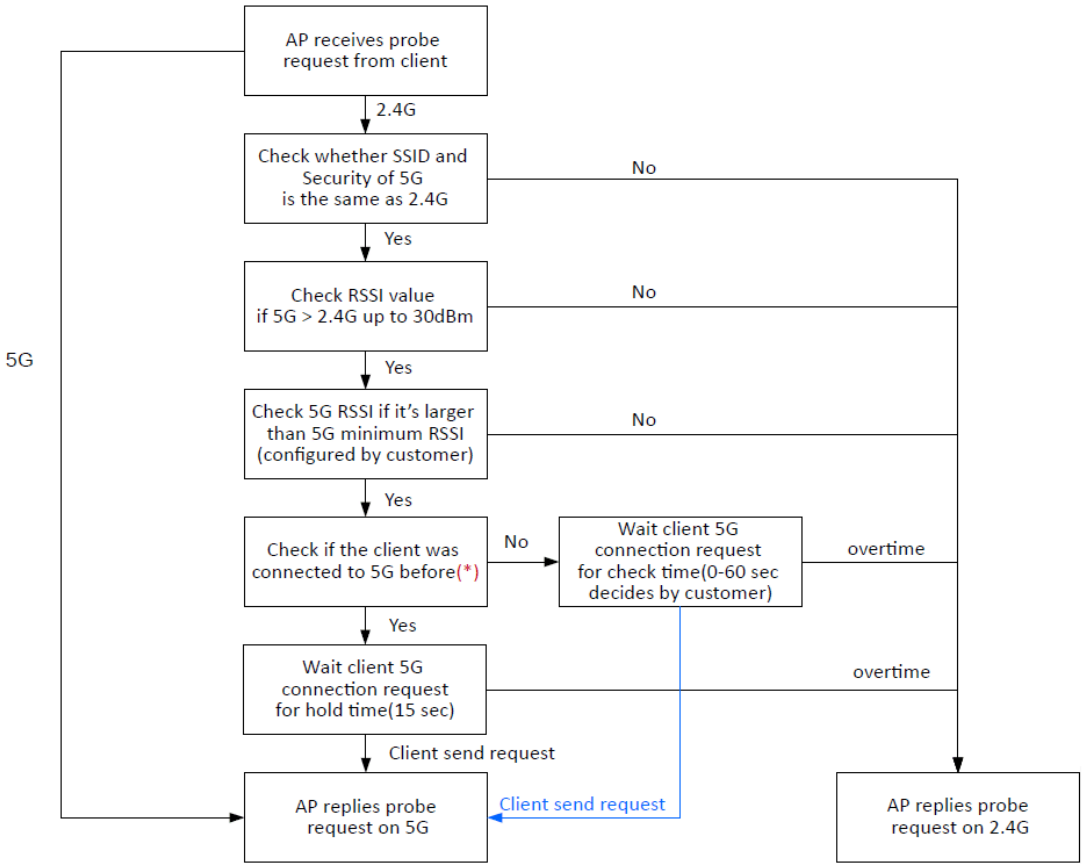


Available settings are explained as follows:

Item	Description
Enable Band Steering	If it is enabled, VigorAP will detect if the wireless client is capable of dual-band or not within the time limit. **Check Time**.... – If the wireless station does not have the capability of 5GHz network connection, the system shall wait and check for several seconds (15 seconds, in default) to make the 2.4GHz network connection. Specify the time limit for VigorAP to detect the wireless client. **Wait Full Time to Check 5G Capability** – If enabled, the client trying to connect to wireless network 2.4G has to wait for a few seconds (defined in **Check Time...** above) to check if the connecting device has the 5G capability. If no 5G capability, the client will be directed to the wireless 2.4G network. **5GHz Minimum RSSI** – The wireless station has the capability of 5GHz network connection, yet the signal performance might not be satisfied. Therefore, when the signal strength is below the value set here while the wireless station connecting to VigorAP 920RP, VigorAP will allow the client to connect to 2.4GHz network. **Overloaded** – If it is enabled, VigorAP will activate the band steering according to the conditions set below. • **2.4GHz Utilization Overload Threshold** – The default setting is 70%. It can define the network congestion for 2.4GHz. • **5GHz Utilization Overload Threshold** – The default setting is 70%. It can define the network congestion for 5GHz. When the utilization of 2.4GHz is higher than the specified threshold and the utilization of 5GHz is lower than the specified threshold, VigorAP will steer the client to connect to 5GHz network.

After finishing this web page configuration, please click **OK** to save the settings.

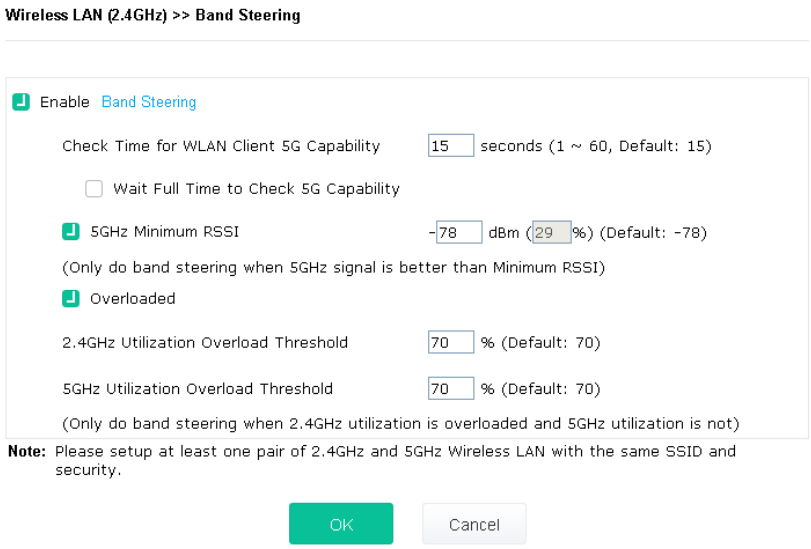
Below shows how Band Steering works.



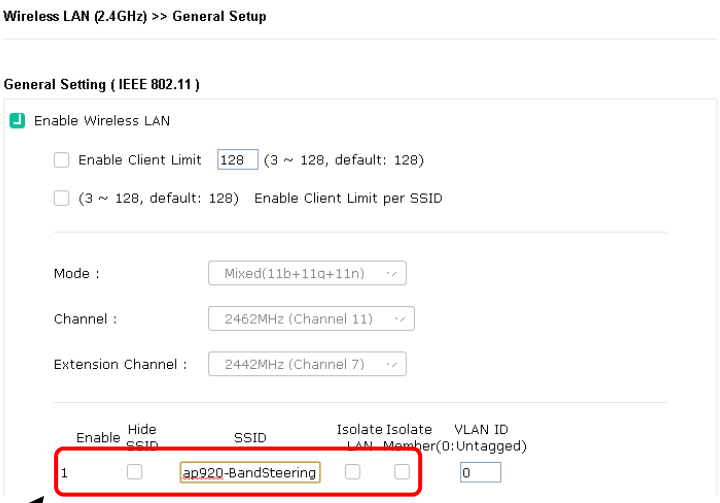
* AP will clear the 5G history station list every 2.5 mins.

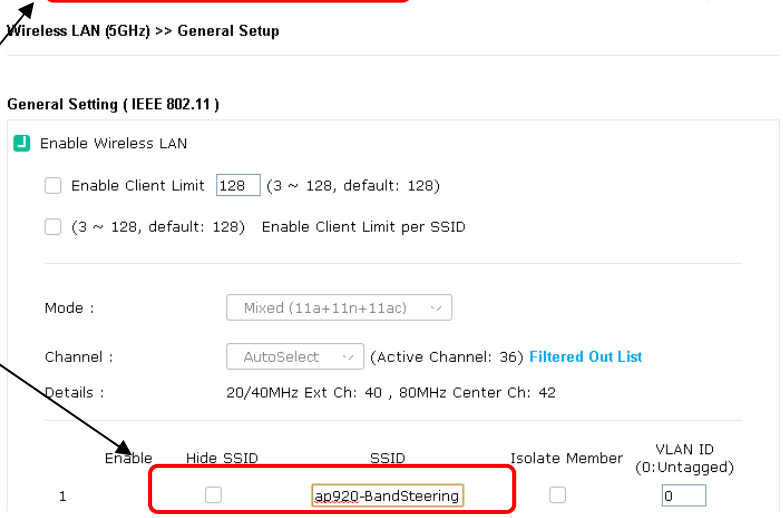
How to Use Band Steering?

1. Open **Wireless LAN(2.4GHz)>>Band Steering**.
2. Check the box of **Enable Band Steering** and use the default value (15) for check time setting.



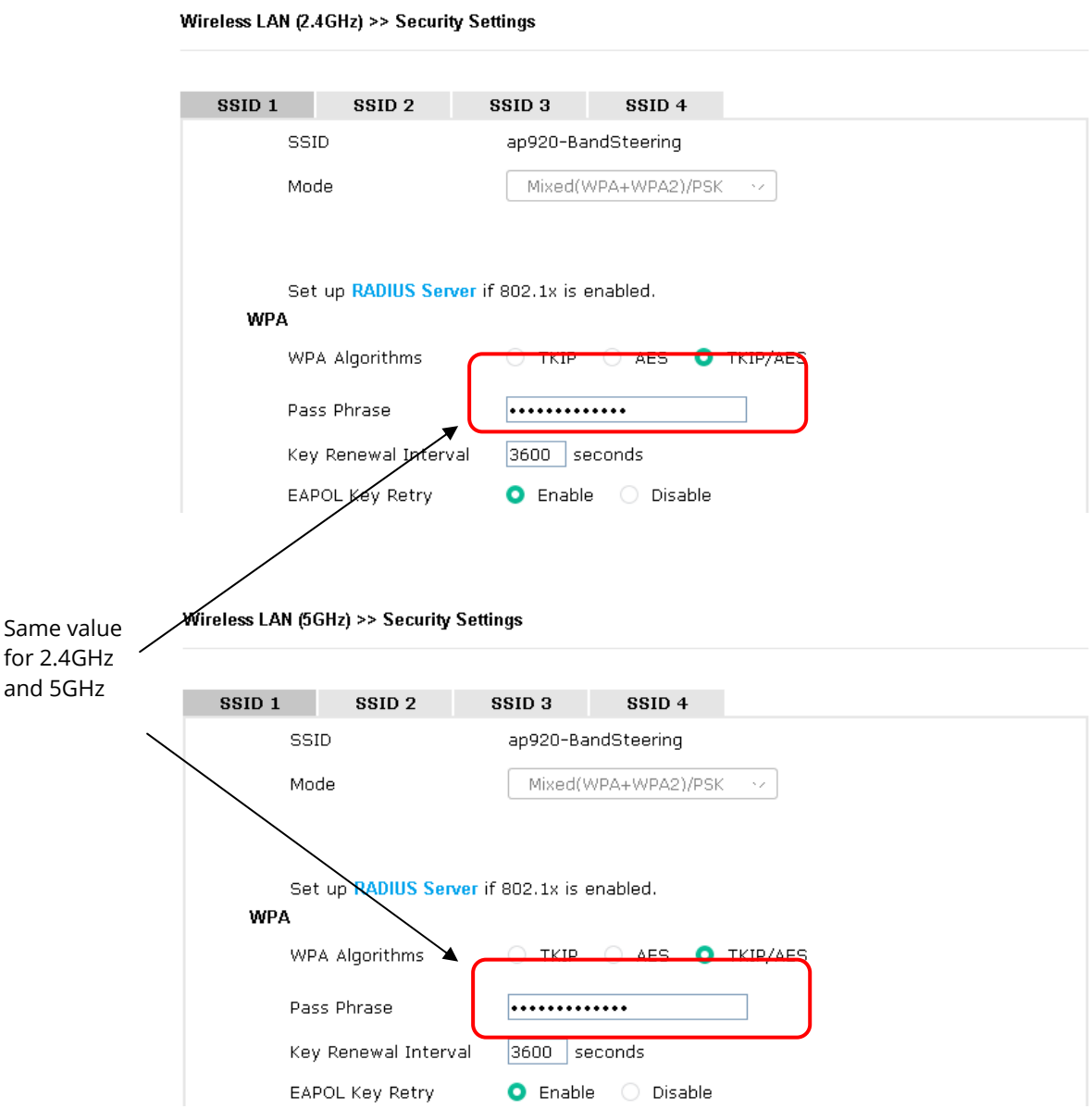
3. Click **OK** to save the settings.
4. Open **Wireless LAN (2.4GHz)>>General Setup** and **Wireless LAN (5GHz)>> General Setup**. Configure SSID as *ap920-BandSteering* for both pages. Click **OK** to save the settings.





Same value for 2.4GHz and 5GHz

5. Open **Wireless LAN (2.4GHz)>>Security** and **Wireless LAN (5GHz)>>Security.** Configure Security as *12345678* for both pages. Click **OK** to save the settings.



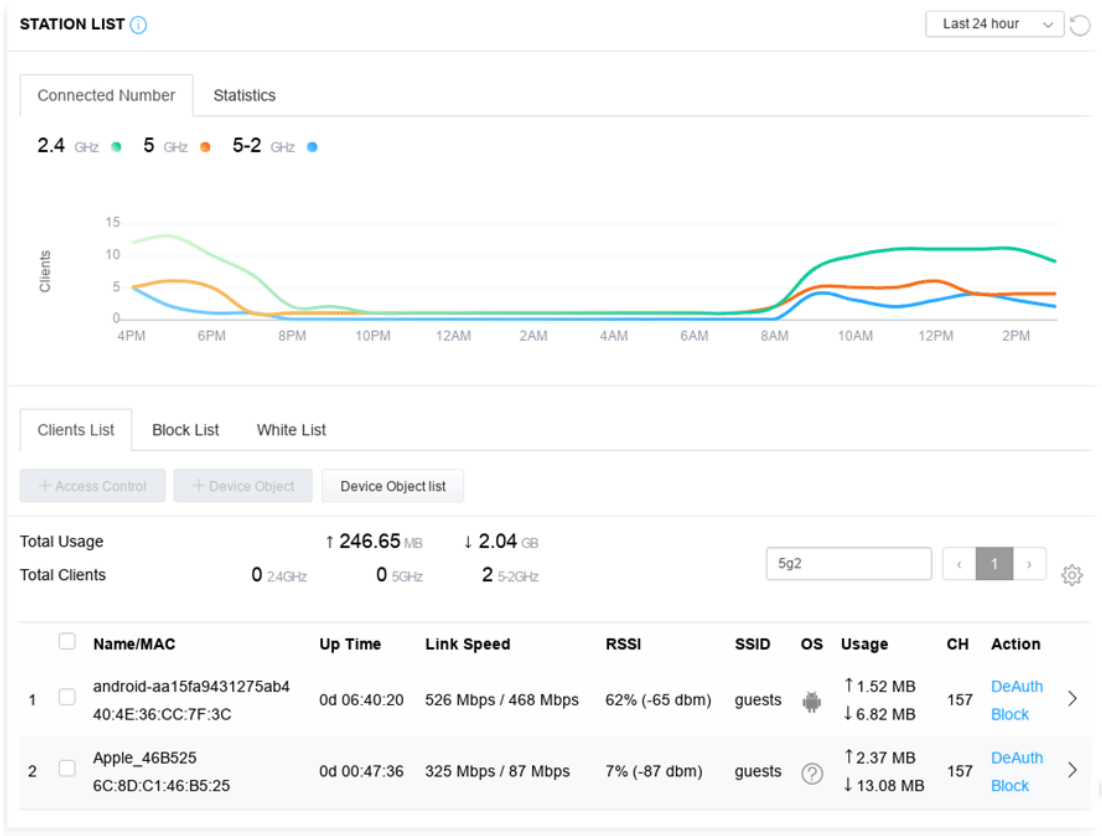
6. Now, VigorAP 920R will let the wireless clients connect to less congested wireless LAN, such as 5GHz to prevent from network congestion.

II-3-13 Station List

Station List provides the information related to the number of clients connecting to VigorAP, used bandwidth and the statistics of the AP device OS. Besides, users can create access control policies, device objects and set black & white list for

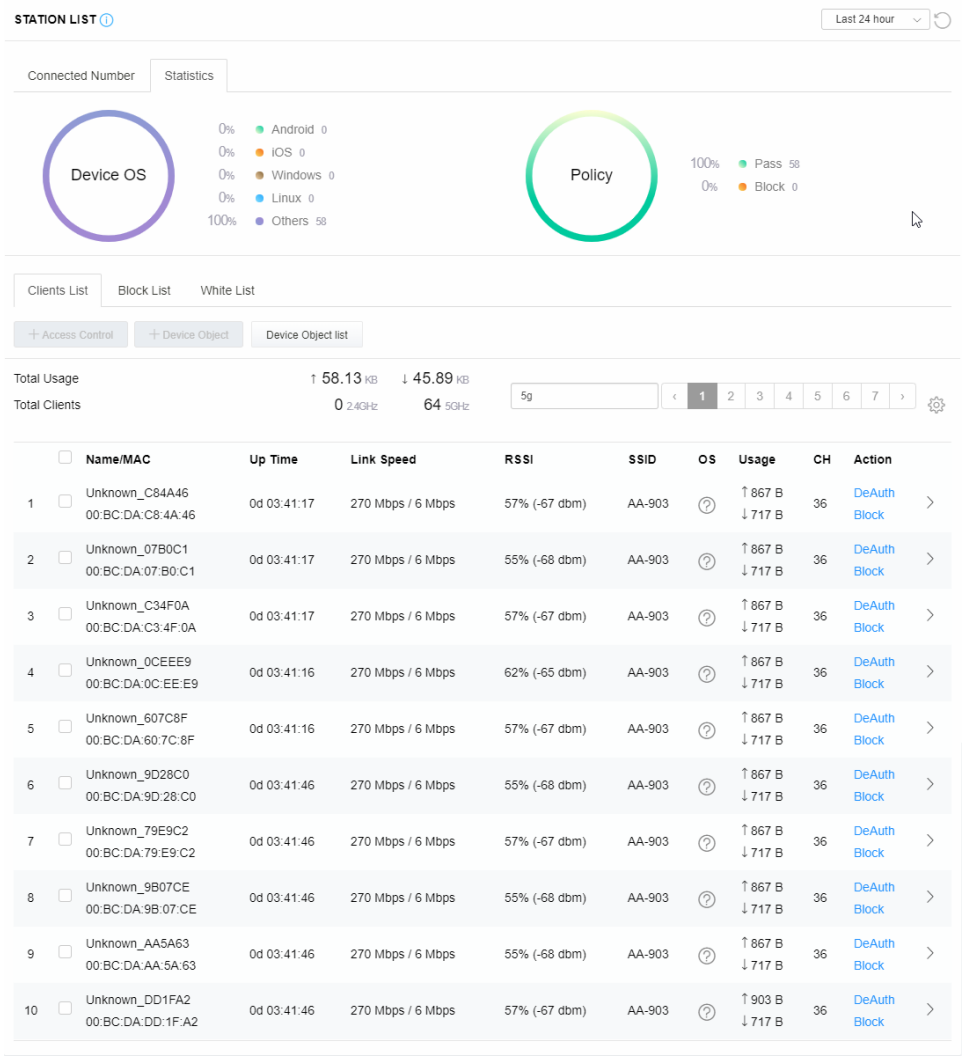
II-3-13-1 Connected Number

This page lists the graph for the number of wireless stations connected to this Access Point with different time phases.



II-3-13-2 Statistics

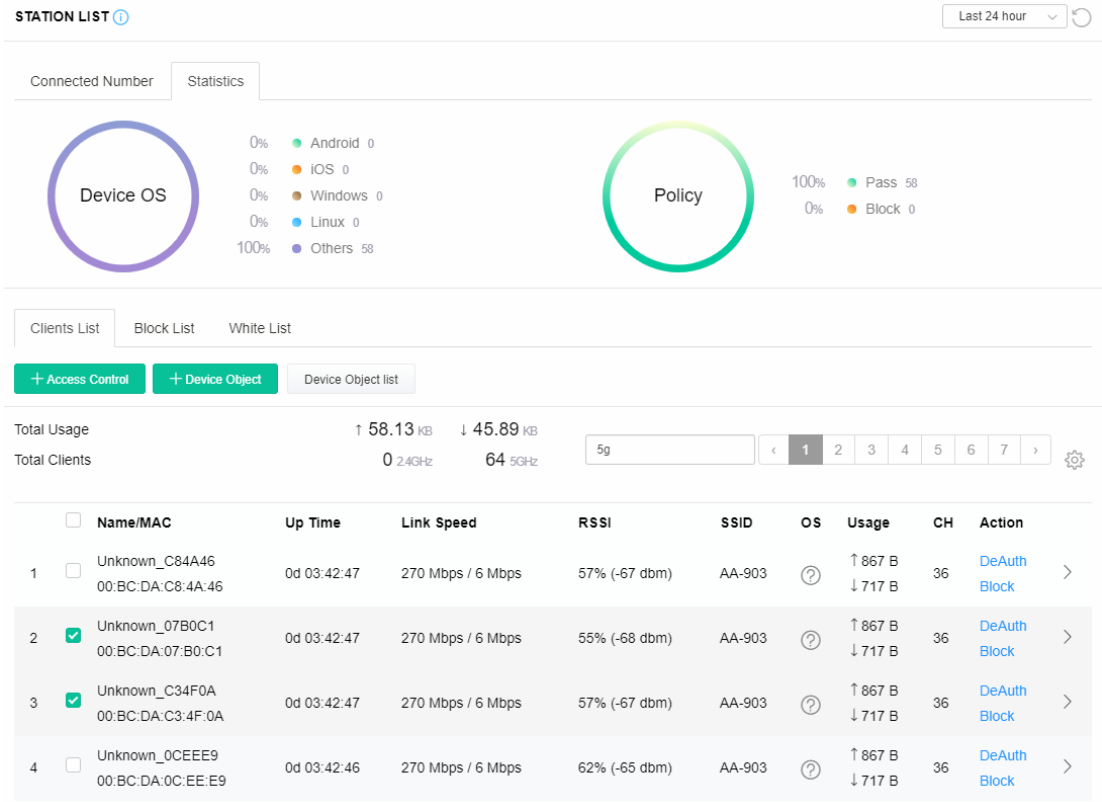
The number of detected devices and the number of device(s) passed/blocked according to the policy specified in **Mobile Device Management>>Policy** can be illustrated as doughnut chart.



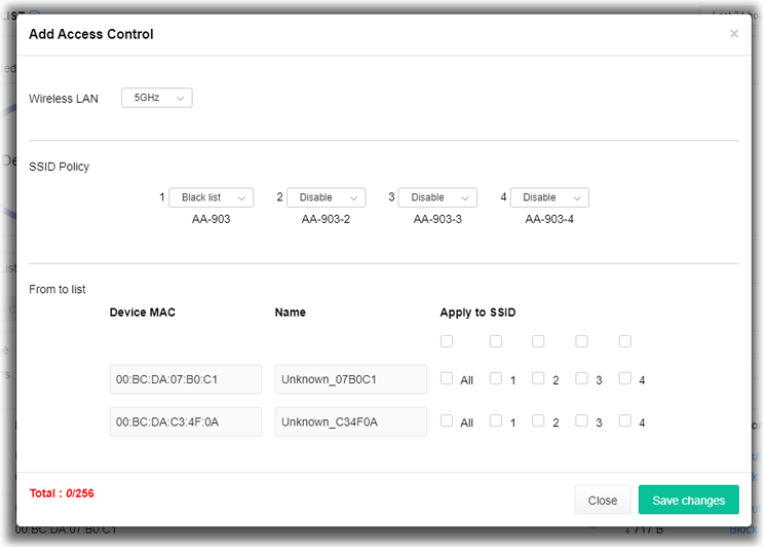
	Name/MAC	Up Time	Link Speed	RSSI	SSID	OS	Usage	CH	Action
1	Unknown_C84A46 00:BC:DA:C8:4A:46	0d 03:41:17	270 Mbps / 6 Mbps	57% (-67 dbm)	AA-903		↑ 867 B ↓ 717 B	36	DeAuth Block
2	Unknown_07B0C1 00:BC:DA:07:B0:C1	0d 03:41:17	270 Mbps / 6 Mbps	55% (-68 dbm)	AA-903		↑ 867 B ↓ 717 B	36	DeAuth Block
3	Unknown_C34F0A 00:BC:DA:C3:4F:0A	0d 03:41:17	270 Mbps / 6 Mbps	57% (-67 dbm)	AA-903		↑ 867 B ↓ 717 B	36	DeAuth Block
4	Unknown_0CEEE9 00:BC:DA:0C:EE:E9	0d 03:41:16	270 Mbps / 6 Mbps	62% (-65 dbm)	AA-903		↑ 867 B ↓ 717 B	36	DeAuth Block
5	Unknown_607C8F 00:BC:DA:60:7C:8F	0d 03:41:16	270 Mbps / 6 Mbps	57% (-67 dbm)	AA-903		↑ 867 B ↓ 717 B	36	DeAuth Block
6	Unknown_9D28C0 00:BC:DA:9D:28:C0	0d 03:41:46	270 Mbps / 6 Mbps	55% (-68 dbm)	AA-903		↑ 867 B ↓ 717 B	36	DeAuth Block
7	Unknown_79E9C2 00:BC:DA:79:E9:C2	0d 03:41:46	270 Mbps / 6 Mbps	57% (-67 dbm)	AA-903		↑ 867 B ↓ 717 B	36	DeAuth Block
8	Unknown_9B07CE 00:BC:DA:9B:07:CE	0d 03:41:46	270 Mbps / 6 Mbps	55% (-68 dbm)	AA-903		↑ 867 B ↓ 717 B	36	DeAuth Block
9	Unknown_AA5A63 00:BC:DA:AA:5A:63	0d 03:41:46	270 Mbps / 6 Mbps	55% (-68 dbm)	AA-903		↑ 867 B ↓ 717 B	36	DeAuth Block
10	Unknown_DD1FA2 00:BC:DA:DD:1F:A2	0d 03:41:46	270 Mbps / 6 Mbps	57% (-67 dbm)	AA-903		↑ 903 B ↓ 717 B	36	DeAuth Block

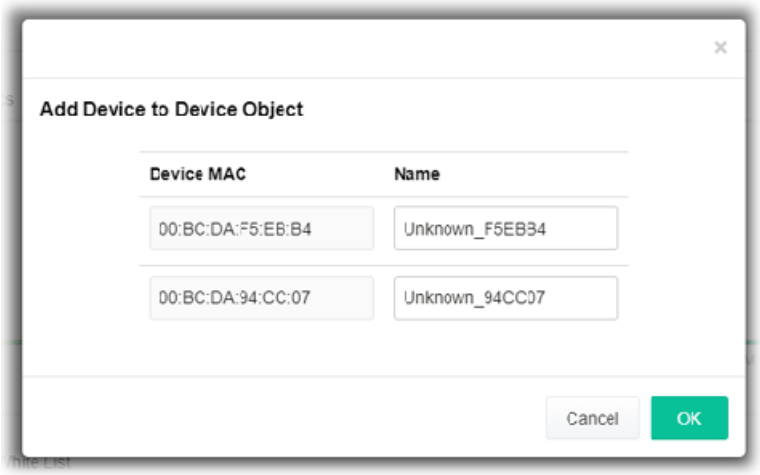
II-3-13-3 Clients List

The client list displays all the stations connecting to VigorAP.



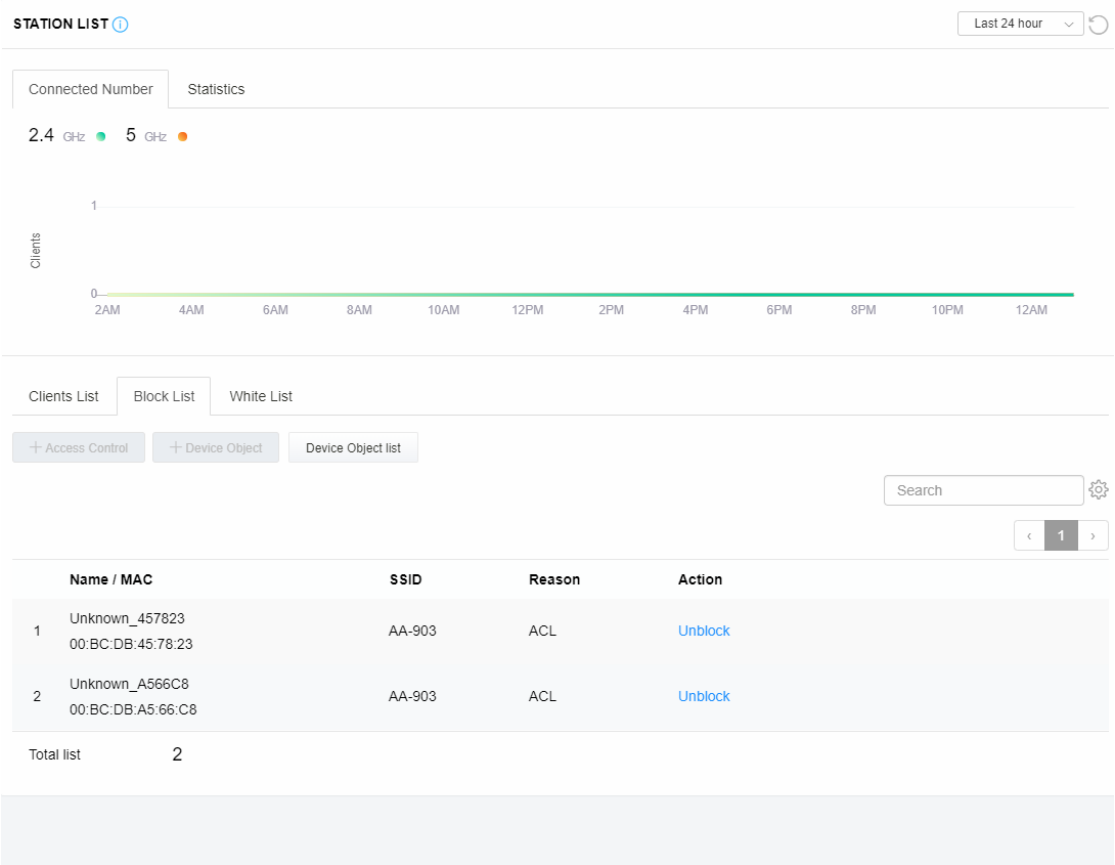
Available settings are explained as follows:

Item	Description
+Access Control	It is available after choosing one of the entries (clients) on Clients List.  **Wireless LAN** - Specify the bandwidth for the access control list. **SSID Policy** - Set the policy for each SSID as black list or white list or disable. **From to list** - Display the clients available for applying this access

	control. **Apply to SSID** - Check **All** to make the device apply the policies to all SSIDs. Or select the one(s) to make the device apply the policies to the selected SSIDs. **Close** - Exit this page without saving any changes. **Save changes** - Save the changes and exit this page.
+Device Object	To add a device to device object list, choose one of the entries (clients) on Clients List to enable the Device Object button. Click the button to open the following page.  Check the information listed on the page. Change the MAC address or name of the selected entry if required. Then click **OK** and exit the page.
Device Object list	The existed device object profiles will be shown on the following page.
Clients List	Display the stations connecting to this Vigor device. **Total Usage -** Display **Total Clients -** Display the number of the clients using 2.4GHz **Name / MAC -** Display the host name / MAC address of the connecting client. **Up Time** - Display the connection time. **Link Speed**- Display the link speed. **RSSI** - Display the RSSI value. **SSID** - Display the SSID the client used for connecting VigorAP. **OS** - Display the OS of the client. **Usage** - Display the bandwidth usage (up and down) of the client. **CH** - Display the channel used by the client. **Action** - Display the authentication method used by the client, and if it is on block list or white list.

II-3-13-4 Block List

This page displays information of the stations under block list.

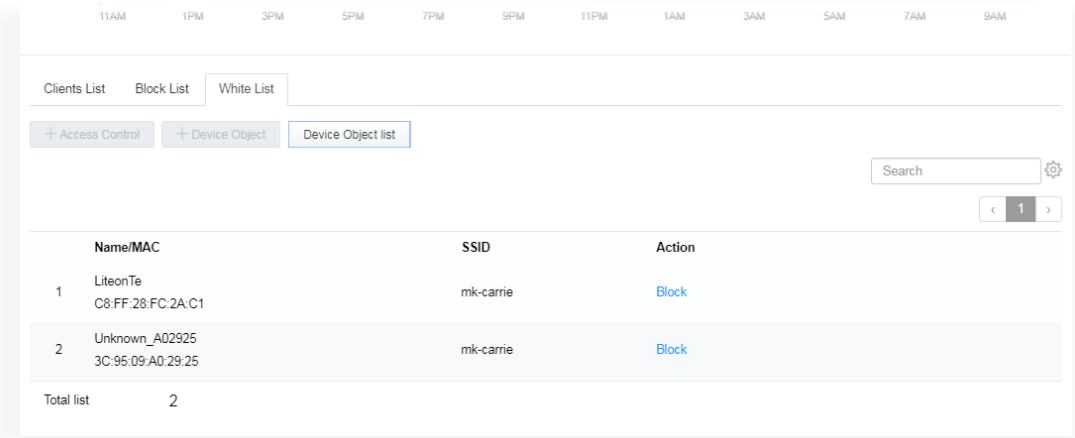


Available settings are explained as follows:

Item	Description
Device Object list	Click it to open the Device Object List dialog for reference.
Name / MAC	Display the host name / MAC Address for the connecting client.
SSID	Display the SSID that the wireless client connects to.
Reason	Display the reference information.
Action	Display the action that you can execute for the station. **Unblock** - Click to unblock the entry.

II-3-13-5 White List

This page displays general information of the stations under white list.

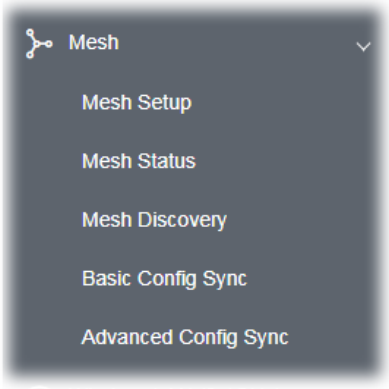


Available settings are explained as follows:

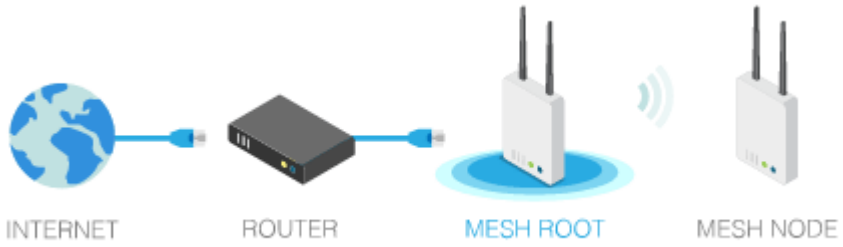
Item	Description
Device Object list	Click it to open the Device Object List dialog for reference.
Name / MAC	Display the host name / MAC Address for the connecting client.
SSID	Display the SSID that the wireless client connects to.
Action	Display the action that you can execute for the station. **Block** - Click to block the entry.

II-4 Mesh Settings for Mesh Mode

When you choose **Mesh** as the operation mode, the Mesh menu with the settings of Mesh Setup, Mesh Status, Mesh Discovery and Configuration Sync will be shown on the screen.



The following figure shows how VigorAP runs as MESH ROOT:



The following figure shows how VigorAP runs as MESH NODE:

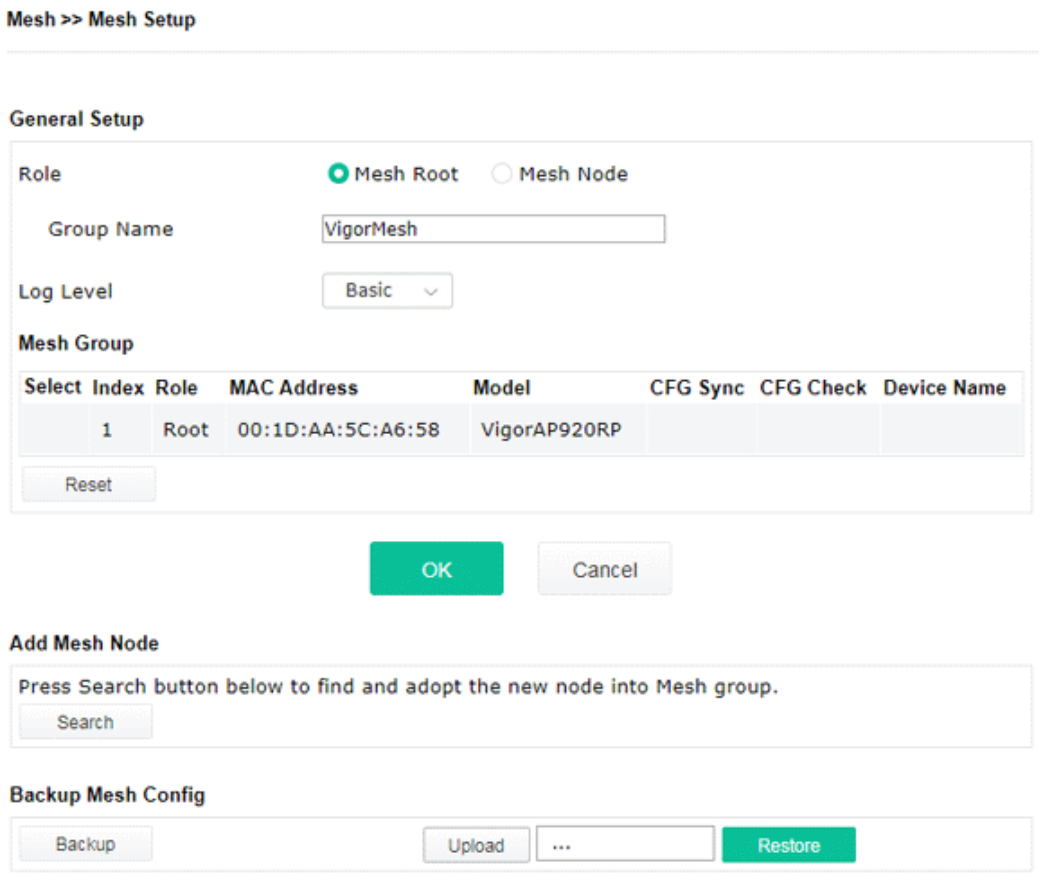
Mesh Root indicates that VigorAP would be other AP's uplink connection. As a Mesh Root, VigorAP must connect to a gateway with Ethernet cable first to have an internet connection.

As a Mesh Node, VigorAP can connect to other Mesh Root or Mesh Node via wireless network or physical connection with an Ethernet cable.

Mesh Root can contain many mesh nodes and form as a mesh group.

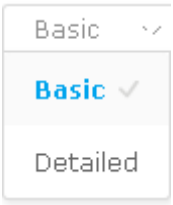
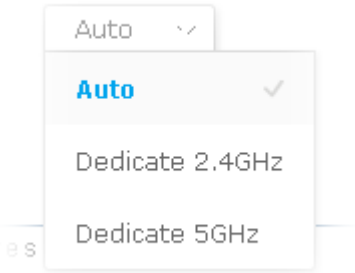
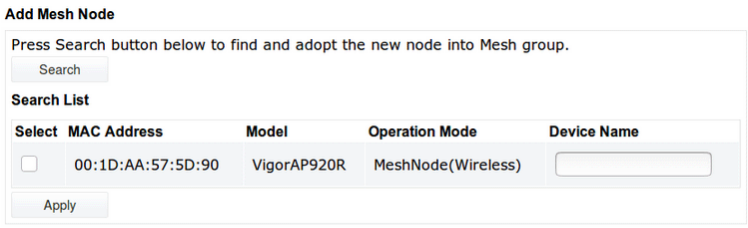
II-4-1 Mesh Setup

Such page can determine the role of the VigorAP connecting to the computer physically. For a mesh root, you can search and specify mesh nodes as members under current mesh group.



Available settings are explained as follows:

Item	Description
Role	**Mesh Root –** When VigorAP is connected to a Vigor router with a physical Ethernet cable, it can be set as mesh root to deliver the wireless signals to a mesh node AP. When VigorAP is set as mesh root, it is necessary to configure wireless connection settings for mesh root and mesh node. **Mesh Node –** As a mesh node, such VigorAP can pass the wireless connection signal to other mesh node or a remote device (PC, CPE, mobile phone). In addition, VigorAP can be searched by mesh root AP and join the mesh group of the root AP. The configuration set for mesh root can be applied to mesh node.
When Mesh Root is selected	**Group Name** - When such VigorAP is set as mesh root or is added to a mesh group, the basic information including role, MAC address, and model name of the AP will be shown in this area. Up to 8 entries (one mesh root and seven mesh nodes) will be shown on this field. **Log Level –** Choose **Basic** or **Detailed**. Related information will be shown on the **Diagnostics>>System Log.**

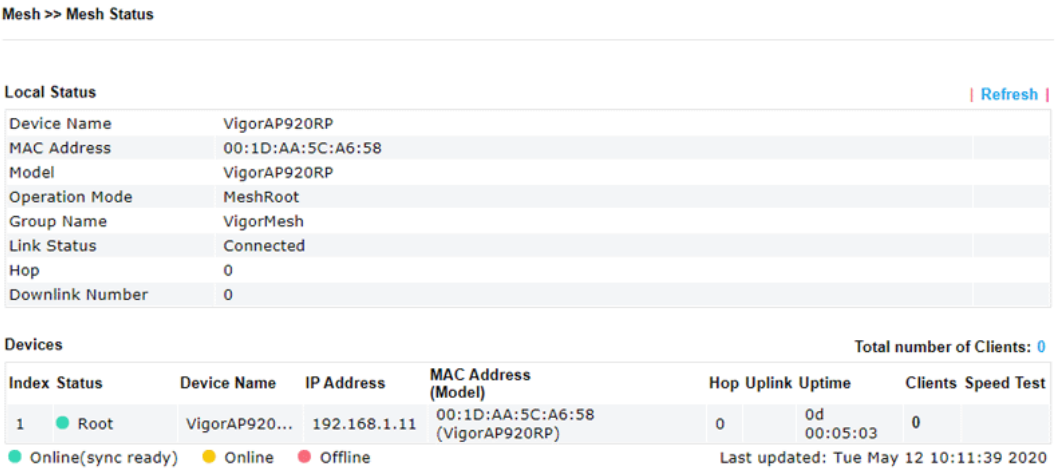
	
When Mesh Node is selected	**Wired Uplink –** Check the box if such VigorAP connects to an uplinked mesh root or an uplinked mesh node with an ethernet cable. **Wireless Uplink Band** – Choose a wireless band for connecting with an uplinked mesh root or an uplinked mesh node.  **Log Level –** Choose **Basic** or **Detailed**. Related information will be shown on the **Diagnostics>>System Log.**
Reset	Click it to clear the Mesh Group information.
Add Mesh Node	Click **Search** to find out available mesh node on the network.  Check the one you want and click **Apply**. The selected AP will be added onto current mesh root.
Backup Mesh Config	**Backup** – Click the button to save the configuration as a file. **Upload/Restore** – Click the Upload button to specify a configuration file. Then click Restore to apply the configuration. When the MAC address of such VigorAP does not appear under the mesh group, the restore operation will not succeed and error message, ”Device MAC is not in mesh group list”, will be shown instead.

II-4-2 Mesh Status

This page shows current status for such Vigor AP (as a mesh root or mesh node). Meanwhile, information for the AP(s) within the mesh group such as connection status, IP address, MAC address, hop, uplink, uptime and number of clients also will be shown on this page.

When VigorAP is set as mesh node, the status page will be shown as follow:

When VigorAP is set as mesh root, the status page will be shown as follow:

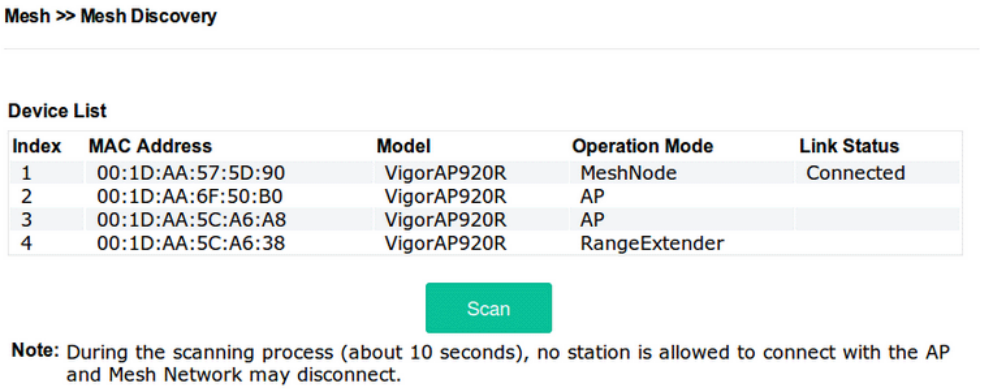


Item	Description
Local Status	Displays general information for such VigorAP.
Devices	Displays detailed information for this VigorAP (as mesh root) and mesh node(s) connected to such mesh root.

II-4-3 Mesh Discovery

For obtaining the list of devices around this VigorAP, click **Scan** and wait for a minute. Later, surrounding VigorAP device(s) will be displayed on this page.

Information under Device List will include MAC address, model name, operation mode and link status.



Mesh >> Mesh Discovery

Device List

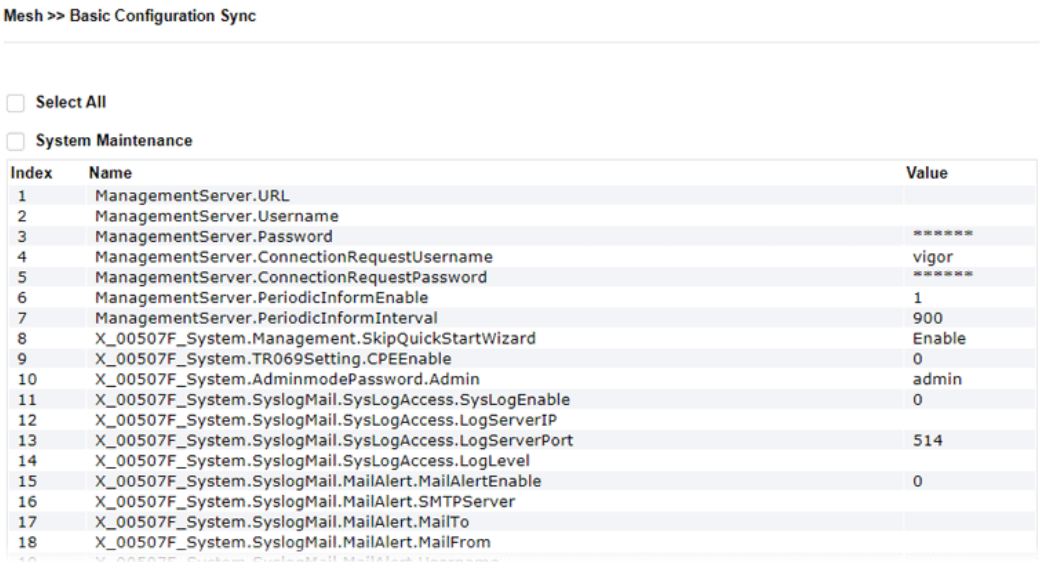
Index	MAC Address	Model	Operation Mode	Link Status
1	00:1D:AA:57:5D:90	VigorAP920R	MeshNode	Connected
2	00:1D:AA:6F:50:B0	VigorAP920R	AP	
3	00:1D:AA:5C:A6:A8	VigorAP920R	AP	
4	00:1D:AA:5C:A6:38	VigorAP920R	RangeExtender	

Scan

Note: During the scanning process (about 10 seconds), no station is allowed to connect with the AP and Mesh Network may disconnect.

II-4-4 Basic Configuration Sync

If you add one Mesh Node in a mesh group, the Mesh Root will send the basic configuration to the device. This page could help you to change the Mesh Root settings and deliver the new configuration of the Mesh Root to all "connected" Mesh Nodes.



Available settings are explained as follows:

Item	Description
System Maintenance / Wireless LAN (2.4Hz) / Wireless LAN (5GHz)	Check the item(s) you want to make configuration sync. **Apply** – Click it to apply the settings configured by such AP to all connected mesh node. **Note that this button is available only when such AP is in mesh root mode.**

Tips for Mesh Network Setup

- Set up TWO mesh devices with uplink RSSI larger than -65dBm.
- Upgrade the firmware version of Mesh devices through Mesh link, starting from the mesh device with less hop number. For example, upgrade the firmware from the root, hop1 Mesh Node then hop2 Mesh Node, and so on.
- VigorMesh network supports up to 3 hops of mesh devices. However, it is suggested to connect the mesh group with less than or equals to 2 hops.

  For your reference, we make a real mesh environment test and get the following record. (Use VigorAP APP to do internet speed test with different hops mesh node.)

  Internet Download Speed (for root and hop1 ~ hop3):

  iPad connects to Root : 80Mbps

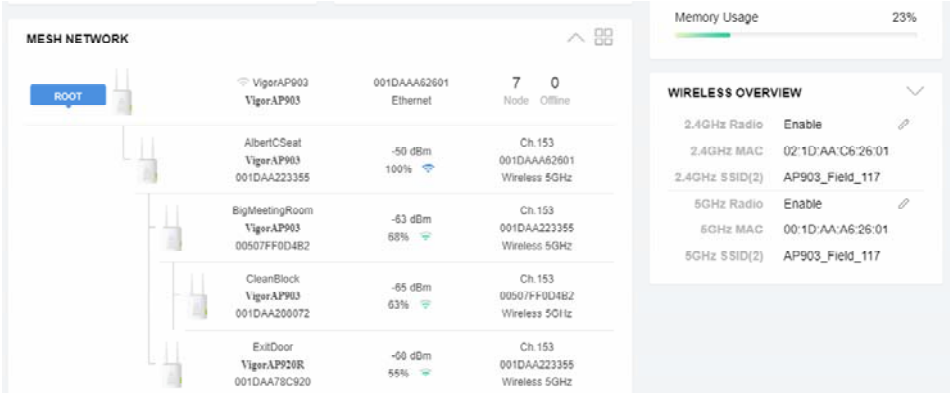
  iPad connects to hop1 Node : 49Mbps (Uplink RSSI : -55dBm)

  iPad connects to hop2 Node : 41Mbps (Uplink RSSI : hop2 -64dBm / hop1 -55dBm)

  iPad connects to hop3 Node : 26Mbps (Uplink RSSI : hop3 -62dBm / hop2 -68dBm / hop1 -55dBm)
- It is not suggested to use a wireless Mesh Node with Ethernet cable connected to a Mesh Root.
- If resetting a Mesh Root,

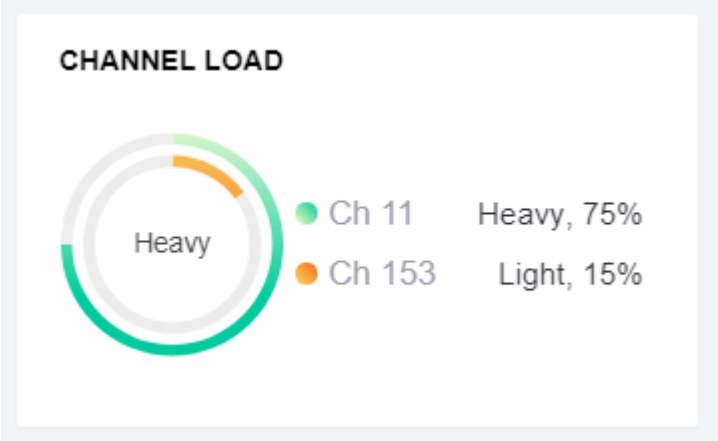
- All "connected" Mesh Nodes will be informed to reset.
- Group List and Group Key will be reset, too.
- For those Mesh Nodes unable to reset, reset them manually. Reset the Group List by web or factory default.

- If resetting a Mesh Node,
  - Group List and Group Key will be cleared.
  - Link Status will become "New".
- Mesh network status also can be viewed and checked through the dashboard by clicking MESH NETWORK.

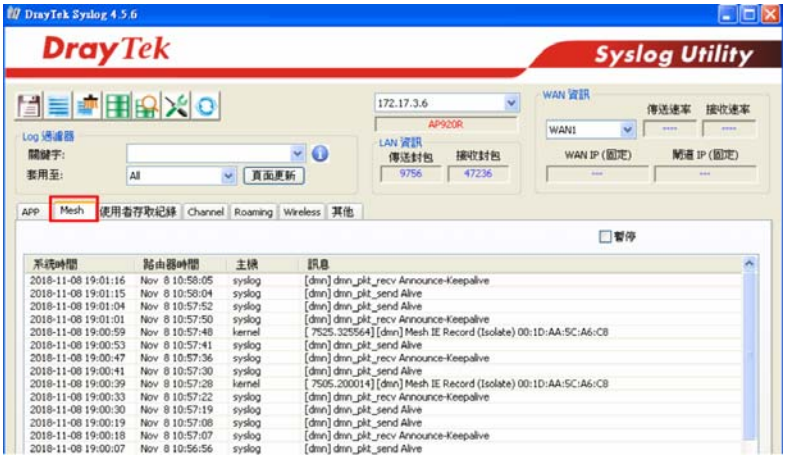


- If Mesh Search / Apply / Discover is worked too fast or is done with empty result, your request may be rejected. Please try again.

- Troubleshooting:
  - Check the firmware version. Please make sure all APs within the mesh group are in the newest firmware version.
  - Check the OP (operation) Mode. Make sure new Mesh Node doesn't accidentally get DHCP IP and becomes AP mode.
  - Check the country code and channels. For example, it is impossible for connecting a VigorAP 1000C Mesh Root with 5G channel 36 to VigorAP920R Wireless Mesh Node in EU country code.
  - Check the channel load. Make sure it is not over 70%.

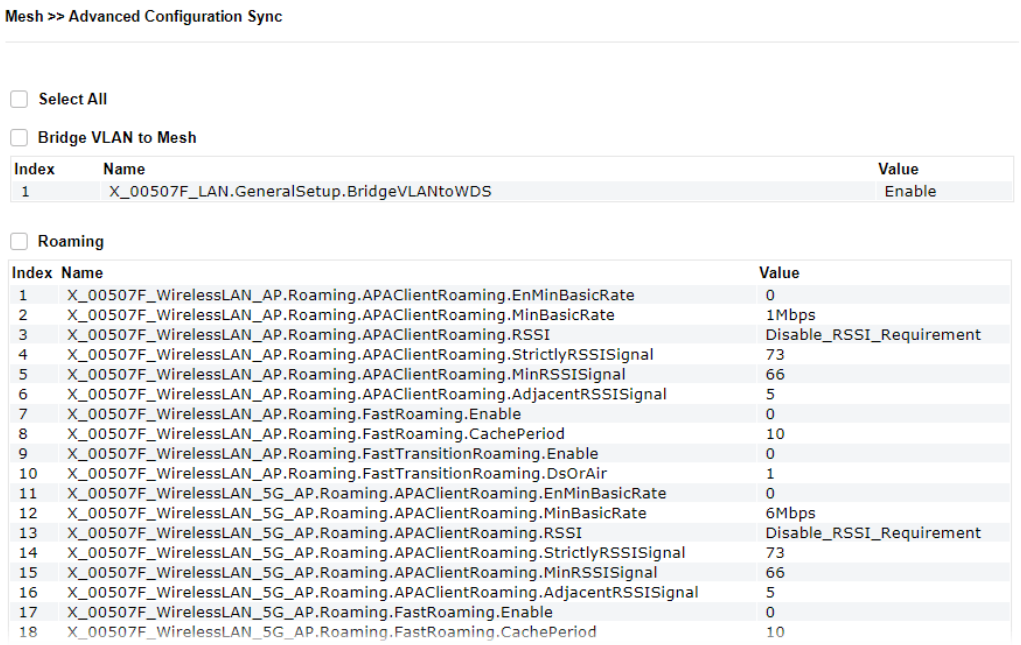


  - Collect some Mesh logs and send the result to DrayTek for analyzing.


DrayTek Syslog 4.5.6
DrayTek
Syslog Utility
172.17.3.6
AP920R
WAN 資訊
傳送速率
接收速率
WAN1
WAN IP (固定)
閘道 IP (固定)
Log 過濾器
關鍵字:
套用至:
All
頁面更新
LAN 資訊
傳送封包
接收封包
9756
47236
APP
Mesh
使用者存取紀錄
Channel
Roaming
Wireless
其他
暫停
系統時間
路由器時間
主機
訊息
2018-11-08 19:01:16 Nov 8 10:58:05 syslog [dmn] dmn_pkt_recv Announce-Keepalive
2018-11-08 19:01:15 Nov 8 10:58:04 syslog [dmn] dmn_pkt_send Alive
2018-11-08 19:01:04 Nov 8 10:57:52 syslog [dmn] dmn_pkt_send Alive
2018-11-08 19:01:01 Nov 8 10:57:50 syslog [dmn] dmn_pkt_recv Announce-Keepalive
2018-11-08 19:00:59 Nov 8 10:57:48 kernel [7525.325564] [dmn] Mesh IE Record (Isolate) 00:1D:AA:5C:A6:C8
2018-11-08 19:00:53 Nov 8 10:57:41 syslog [dmn] dmn_pkt_send Alive
2018-11-08 19:00:47 Nov 8 10:57:36 syslog [dmn] dmn_pkt_recv Announce-Keepalive
2018-11-08 19:00:41 Nov 8 10:57:30 syslog [dmn] dmn_pkt_send Alive
2018-11-08 19:00:39 Nov 8 10:57:28 kernel [7505.200014] [dmn] Mesh IE Record (Isolate) 00:1D:AA:5C:A6:C8
2018-11-08 19:00:33 Nov 8 10:57:22 syslog [dmn] dmn_pkt_recv Announce-Keepalive
2018-11-08 19:00:30 Nov 8 10:57:19 syslog [dmn] dmn_pkt_send Alive
2018-11-08 19:00:19 Nov 8 10:57:08 syslog [dmn] dmn_pkt_send Alive
2018-11-08 19:00:18 Nov 8 10:57:07 syslog [dmn] dmn_pkt_recv Announce-Keepalive
2018-11-08 19:00:07 Nov 8 10:56:56 syslog [dmn] dmn_pkt_send Alive

II-4-5 Advanced Config Sync

If you add one Mesh Node in a mesh group, the Mesh Root will synchronize the advanced configuration to the device based on the setting results on this page.



Mesh >> Advanced Configuration Sync

Select All

Bridge VLAN to Mesh

Index	Name	Value
1	X_00507F_LAN.GeneralSetup.BridgeVLANtoWDS	Enable

Roaming

Index	Name	Value
1	X_00507F_WirelessLAN_AP.Roaming.APAClientRoaming.EnMinBasicRate	0
2	X_00507F_WirelessLAN_AP.Roaming.APAClientRoaming.MinBasicRate	1Mbps
3	X_00507F_WirelessLAN_AP.Roaming.APAClientRoaming.RSSI	Disable_RSSI_Requirement
4	X_00507F_WirelessLAN_AP.Roaming.APAClientRoaming.StrictlyRSSISignal	73
5	X_00507F_WirelessLAN_AP.Roaming.APAClientRoaming.MinRSSISignal	66
6	X_00507F_WirelessLAN_AP.Roaming.APAClientRoaming.AdjacentRSSISignal	5
7	X_00507F_WirelessLAN_AP.Roaming.FastRoaming.Enable	0
8	X_00507F_WirelessLAN_AP.Roaming.FastRoaming.CachePeriod	10
9	X_00507F_WirelessLAN_AP.Roaming.FastTransitionRoaming.Enable	0
10	X_00507F_WirelessLAN_AP.Roaming.FastTransitionRoaming.DsOrAir	1
11	X_00507F_WirelessLAN_5G_AP.Roaming.APAClientRoaming.EnMinBasicRate	0
12	X_00507F_WirelessLAN_5G_AP.Roaming.APAClientRoaming.MinBasicRate	6Mbps
13	X_00507F_WirelessLAN_5G_AP.Roaming.APAClientRoaming.RSSI	Disable_RSSI_Requirement
14	X_00507F_WirelessLAN_5G_AP.Roaming.APAClientRoaming.StrictlyRSSISignal	73
15	X_00507F_WirelessLAN_5G_AP.Roaming.APAClientRoaming.MinRSSISignal	66
16	X_00507F_WirelessLAN_5G_AP.Roaming.APAClientRoaming.AdjacentRSSISignal	5
17	X_00507F_WirelessLAN_5G_AP.Roaming.FastRoaming.Enable	0
18	X_00507F_WirelessLAN_5G_AP.Roaming.FastRoaming.CachePeriod	10

Available settings are explained as follows:

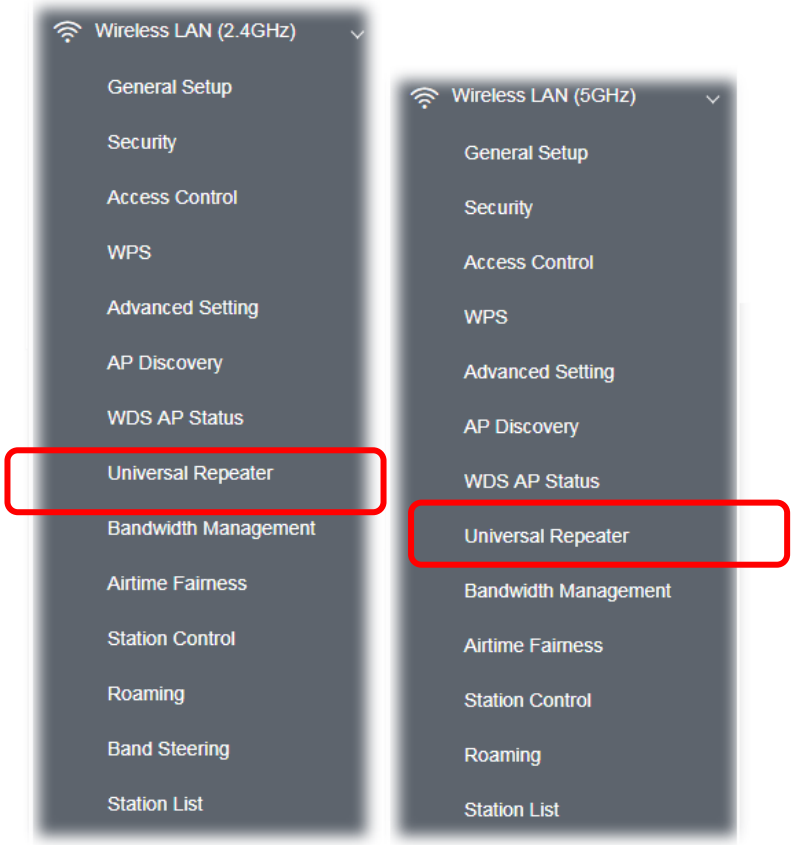
Item	Description
Select All	All item(s) will be selected for making configuration sync.
Bridge VLAN to Mesh	Check to transmit the packets with VLAN tag to mesh nodes.

II-5 Universal Repeater Settings for Range Extender Mode

When you choose **Range Extender** as the operation mode, the Wireless LAN menu items (for 2.4GHz and 5GHz) will include General Setup, Security, Access Control, WPS, Advanced Setting, AP Discovery, WDS AP Status, Universal Repeater, WMM Configuration, Bandwidth Management, Airtime Fairness, Station Control, Roaming, Band Steering and Station List.

This section will introduce settings for Universal Repeater only.

For other wireless setting items (e.g., General Setup, Security, WPS, and etc.), please refer to II-3.

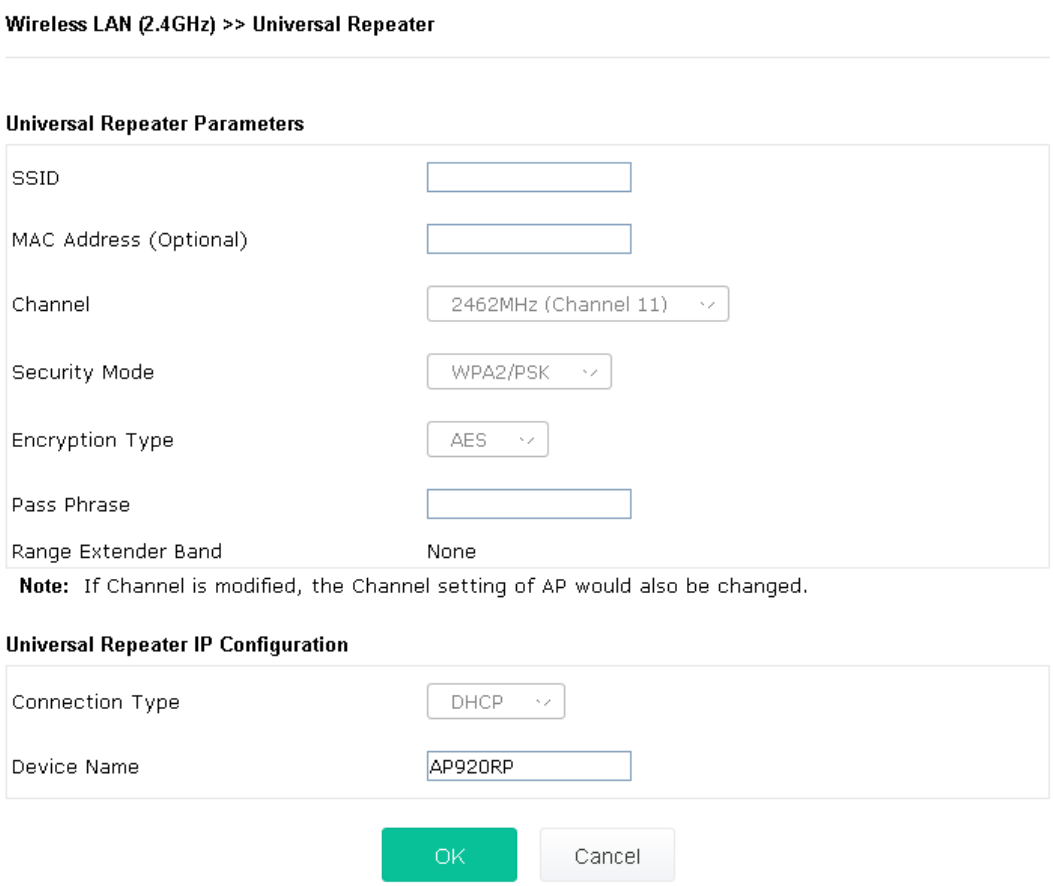


The following figure shows how VigorAP runs as Range Extender:

The access point can act as a wireless repeater; it can be Station and AP at the same time. It can use Station function to connect to a root AP and use AP function to serve all wireless stations within its coverage.

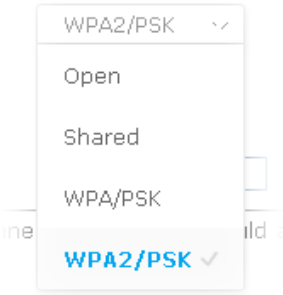
Note:

While using **Universal Repeater** mode, the access point will demodulate the received signal. Please check if this signal is noise for the operating network, then have the signal modulated and amplified again. The output power of this mode is the same as that of AP mode.



Available settings are explained as follows:

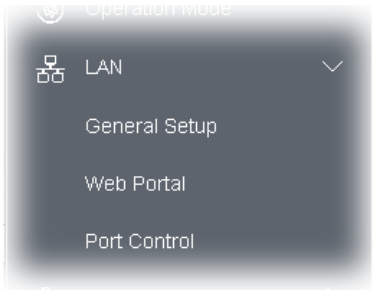
Item	Description
SSID	Set the name of access point that VigorAP 920R wants to connect to.
MAC Address (Optional)	Type the MAC address of access point that VigorAP 920R wants to connect to.
Channel	Means the channel of frequency of the wireless LAN. You may switch channel if the selected channel is under serious interference.
Security Mode	There are several modes provided for you to choose. Each mode will bring up different parameters (e.g., WEP keys, Pass Phrase) for you to configure.

	
Encryption Type for Open/Shared	This option is available when Open/Shared is selected as Security Mode. Choose **None** to disable the WEP Encryption. Data sent to the AP will not be encrypted. To enable WEP encryption for data transmission, please choose **WEP**. **WEP Keys** - Four keys can be entered here, but only one key can be selected at a time. The format of WEP Key is restricted to 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or restricted to 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. The allowed content is the ASCII characters from 33(!) to 126(~) except '#' and ','.
Encryption Type for WPA/PSK and WPA2/PSK	This option is available when WPA/PSK or WPA2/PSK is selected as **Security Mode**. Select **TKIP** or **AES** as the algorithm for WPA.
Pass Phrase	Type **8~63** ASCII characters, such as 012345678 (or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").
Connection Type	Choose DHCP or Static IP as the connection mode. **DHCP** – The wireless station will be assigned with an IP from VigorAP. **Static IP** – The wireless station shall specify a static IP for connecting to Internet via VigorAP.
Device Name	This setting is available when **DHCP** is selected as **Connection Type**. Type a name for the VigorAP as identification. Simply use the default name.
IP Address	This setting is available when **Static IP** is selected as **Connection Type**. Type an IP address with the same network segment of the LAN IP setting of VigorAP. Such IP shall be different with any IP address in LAN.
Subnet Mask	This setting is available when **Static IP** is selected as **Connection Type**. Type the subnet mask setting which shall be the same as the one configured in LAN for VigorAP.
Default Gateway	This setting is available when **Static IP** is selected as **Connection Type**. Type the gateway setting which shall be the same as the default gateway configured in LAN for VigorAP.

After finishing this web page configuration, please click **OK** to save the settings.

II-6 LAN

Local Area Network (LAN) is a group of subnets regulated and ruled by modem.

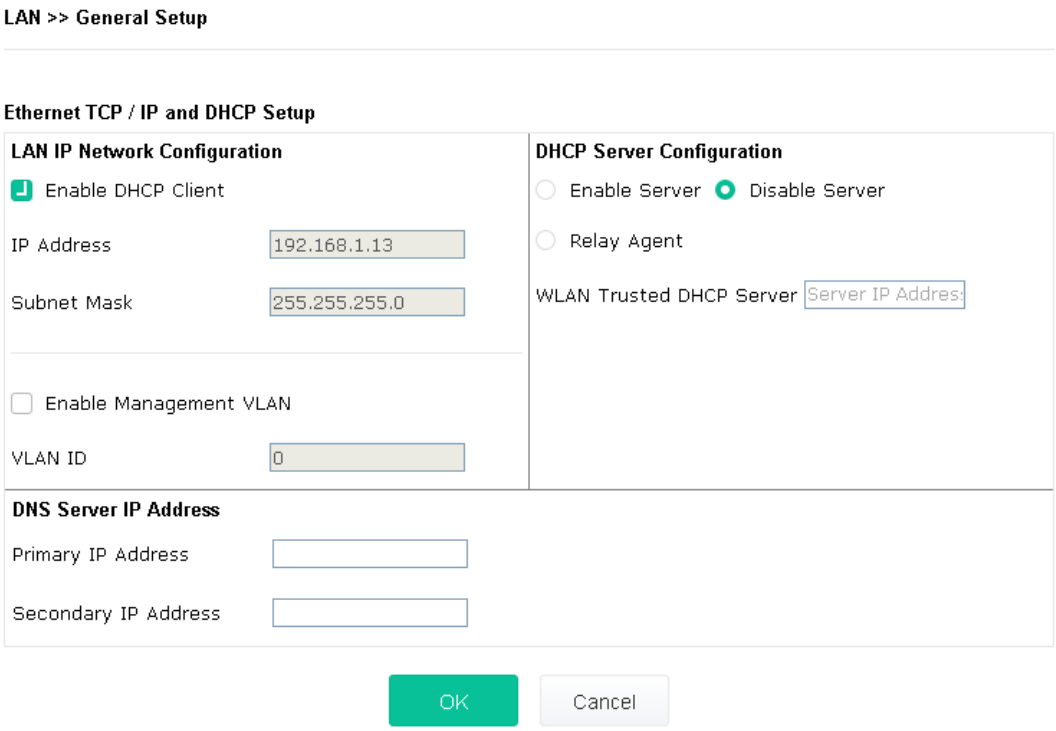


II-6-1 General Setup

Click **LAN** to open the LAN settings page and choose **General Setup**.

Note:

Such page will be changed according to the Operation Mode selected. The following screen is obtained by choosing AP as the operation mode.



Available settings are explained as follows:

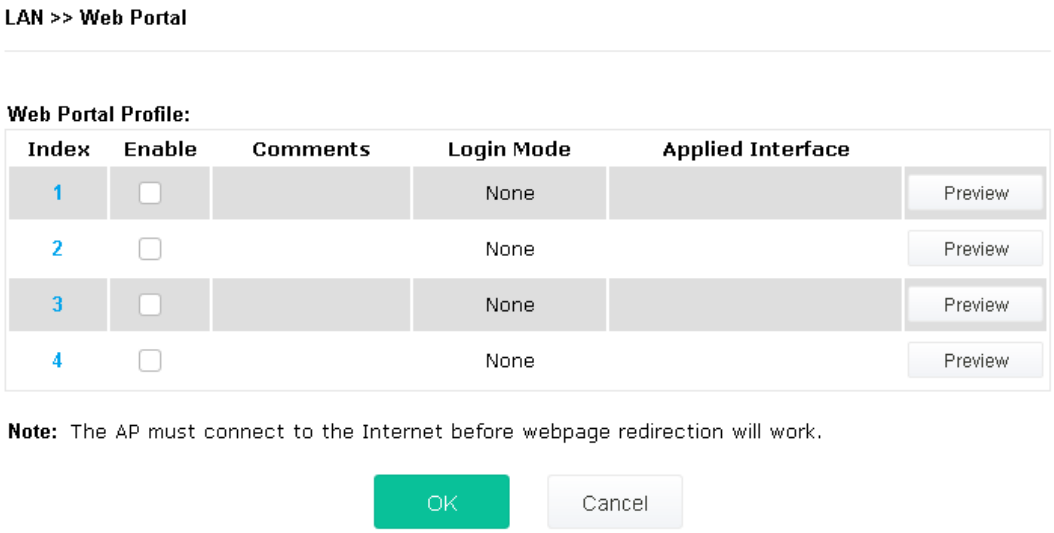
Item	Description
LAN IP Network Configuration	**Enable DHCP Client** – When it is enabled, VigorAP 920R will be treated as a client and can be managed / controlled by AP Management server offered by Vigor router (e.g., Vigor2860). **IP Address** – Type in private IP address for connecting to a local private network (Default: 192.168.1.2). **Subnet Mask** – Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24) **Enable Management VLAN** – VigorAP 920R supports tag-based VLAN for wireless clients accessing Vigor device. Only the clients with the specified VLAN ID can access into VigorAP 920R. • **VLAN ID** – Type the number as VLAN ID tagged on the transmitted packet. "0" means no VALN tag.
DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. DHCP server can automatically dispatch related IP settings to any local user configured as a DHCP client. **Enable Server -** Enable Server lets the modem assign IP address to every host in the LAN. • **Start IP Address -** Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your modem is 192.168.1.2, the starting IP address must be 192.168.1.3 or greater, but smaller than 192.168.1.254. • **End IP Address -** Enter a value of the IP address pool for the DHCP server to end with when issuing IP addresses. • **Subnet Mask -** Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24) • **Default Gateway -** Enter a value of the gateway IP address for the DHCP server. • **Lease Time** - It allows you to set the leased time for the specified PC. • **Primary DNS Server -** You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the modem will automatically apply default DNS Server IP address: 194.109.6.66 to this field. • **Secondary DNS Server -** You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the modem will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field. **Relay Agent -** Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to. • **DHCP Relay Agent -** It is available when Enable Relay Agent is selected. Set the IP address of the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server. **Disable Server -** Disable Server lets you manually or use other DHCP server to assign IP address to every host in the LAN.

	• **WLAN Trusted DHCP Server –**There is no right for such VigorAP to assign IP address for wireless LAN user. However, you can specify another valid DHCP server on other VigorAP to make the wireless LAN client obtaining the IP address from the designated DHCP server. Specify a DHCP server in such field. All the IP addresses of the devices on LAN of VigorAP will be assigned via such specified server. It is used to avoid IP assignment interference due to multiple DHCP servers in one LAN.
DNS Server IP Address	**Primary DNS Server -** You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the modem will automatically apply default DNS Server IP address: 194.109.6.66 to this field. **Secondary DNS Server -** You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the modem will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field.

After finishing this web page configuration, please click **OK** to save the settings.

II-6-2 Web Portal

This page allows you to configure a profile with specified URL for accessing into or display a message when a wireless/LAN user connects to Internet through this router. No matter what the purpose of the wireless/LAN client is, he/she will be forced into the URL configured here while trying to access into the Internet or the desired web page through this router. That is, a company which wants to have an advertisement for its products to users can specify the URL in this page to reach its goal.

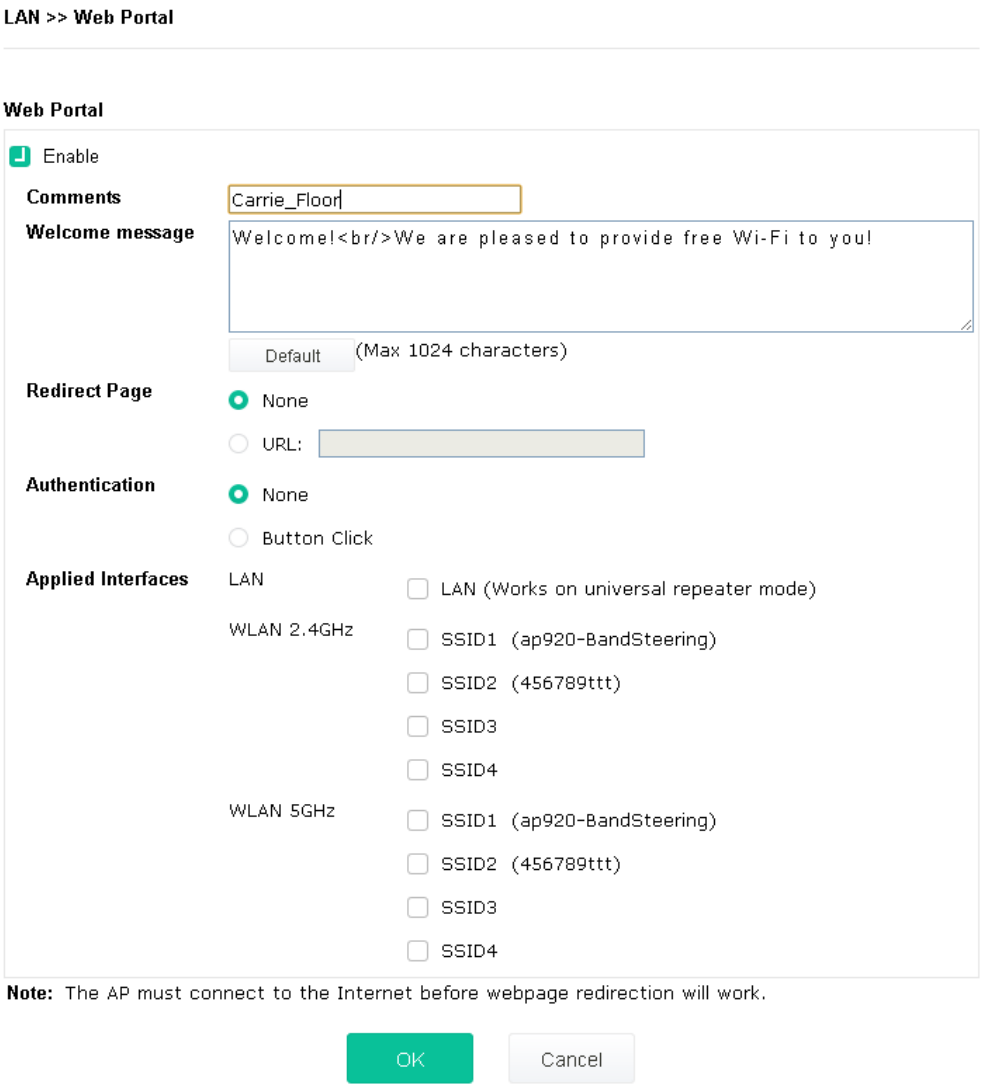


Available settings are explained as follows:

Item	Description
Index	Display the number link which allows you to configure the profile.
Enable	Check the box to enable such profile.
Comments	Display the content (Disable, URL Redirect or Message) of the profile.
Login Mode	Display the login mode that a client uses to access into Internet.
Applied Interface	Display the applied interfaces of the profile.
Preview	Open a preview window according to the configured settings.

After finishing this web page configuration, please click **OK** to save the settings.

To configure the profile, click any index number link to open the following page.



Available settings are explained as follows:

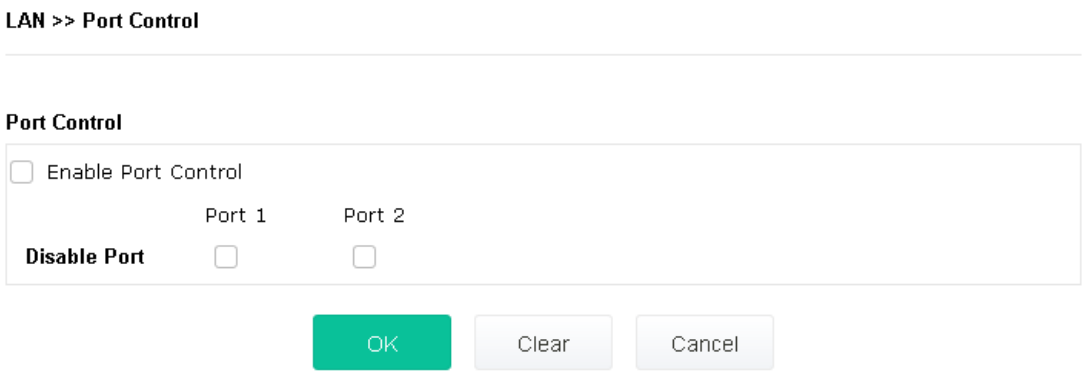
Item	Description
Enable	Check the box to enable this function.
Comments	Enter a brief comment to explain such web portal profile.
Welcome message	Enter words or sentences here. The message will be displayed on the screen for several seconds when the wireless users access into the web page through the router. • **Default** – Click it to restore the default content.
Redirect Page	**None** - User can access into Internet directly. **URL -** Any user who wants to access into Internet through this router will be redirected to the URL specified here first. It is a useful method for the purpose of advertisement. For example, force the wireless user(s) in hotel to access into the web page that the hotel wants the user(s) to visit.
Authentication	**None** – User can access into Internet directly without authentication. **Button Click** – When a client tries to access into Internet, a welcome message page with a button named "Accept" will appear on the screen first. The client must click that button (Accept) and then he/she is

	allowed to access Internet.
Applied Interfaces	Check the box(es) representing different interfaces to be applied by such profile. • **LAN** – If it is selected and Universal Repeater is specified as connection mode for such AP, both LAN client and WLAN client can access into Internet via web portal. Yet, if AP mode is selected, only wireless LAN client shall access into Internet via web portal. • **WLAN 2.4GHz/5GHz** - The advantage is that each SSID (1/2/3/4) for wireless network can be applied with different web portal separately.

After finishing this web page configuration, please click **OK** to save the settings.

II-6-3 Port Control

To avoid wrong connection due to the insertion of unsuitable Ethernet cable, the function of physical LAN ports can be disabled via web configuration.



Available settings are explained as follows:

Item	Description
Enable Port Control	Check it to enable the port control. If it is enabled, you are allowed to disable the function of physical LAN port by checking the corresponding check box.
Disable Port	Choose and check the LAN port.

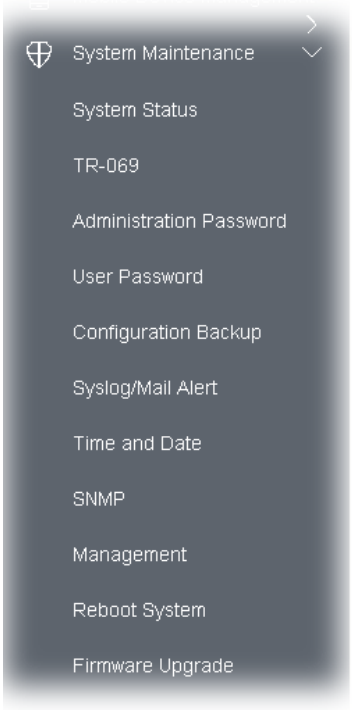
After finishing this web page configuration, please click **OK** to save the settings.

Chapter III Management

III-1 System Maintenance

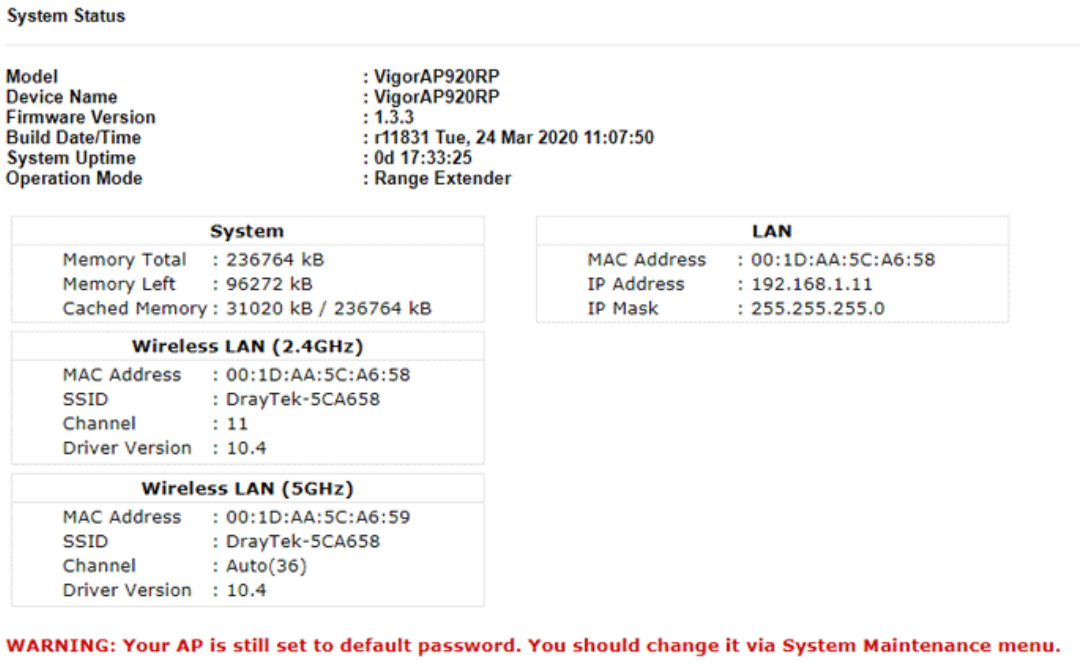
For the system setup, there are several items that you have to know the way of configuration: System Status, TR-069, Administrator Password, User Password, Configuration Backup, Syslog/Mail Alert, Time and Date, SNMP, Management, Reboot System, and Firmware Upgrade.

Below shows the menu items for System Maintenance.



III-1-1 System Status

The **System Status** provides basic network settings of Vigor modem. It includes LAN and WAN interface information. Also, you could get the current running firmware version or firmware related information from this presentation.

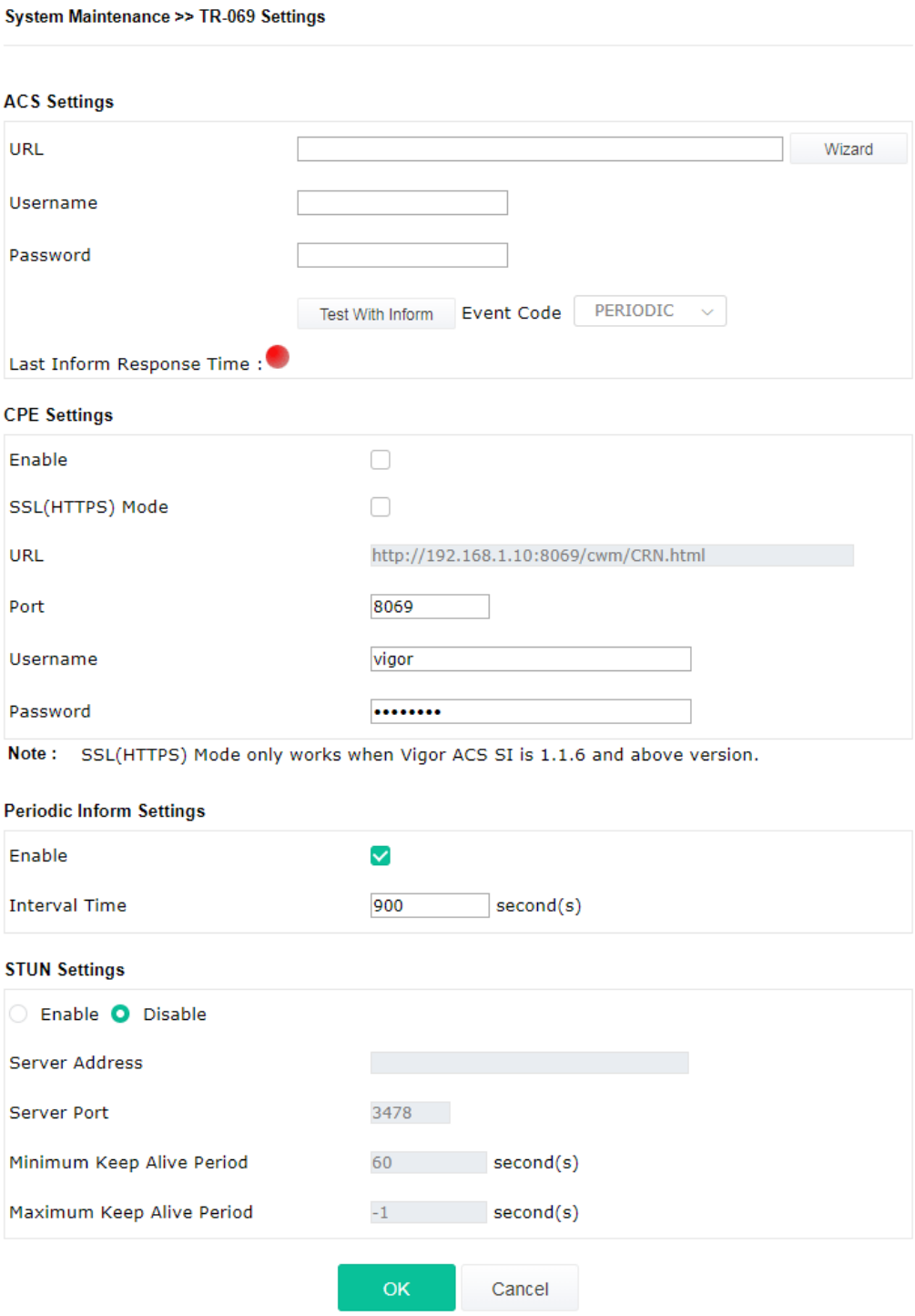


Each item is explained as follows:

Item	Description
Model /Device Name	Display the model name of the modem.
Firmware Version	Display the firmware version of the modem.
Build Date/Time	Display the date and time of the current firmware build.
System Uptime	Display the period that such device connects to Internet.
Operation Mode	Display the operation mode that the device used.
System	
Memory total	Display the total memory of your system.
Memory left	Display the remaining memory of your system.
LAN	
MAC Address	Display the MAC address of the LAN Interface.
IP Address	Display the IP address of the LAN interface.
IP Mask	Display the subnet mask address of the LAN interface.
Wireless LAN (2.4GHz/5GHz)	
MAC Address	Display the MAC address of the WAN Interface.
SSID	Display the SSID of the device.
Channel	Display the channel that the station used for connecting with such device.

III-1-2 TR-069

This device supports TR-069 standard. It is very convenient for an administrator to manage a TR-069 device (Vigor router, AP and etc.) through VigorACS (Auto Configuration Server).



Available settings are explained as follows:

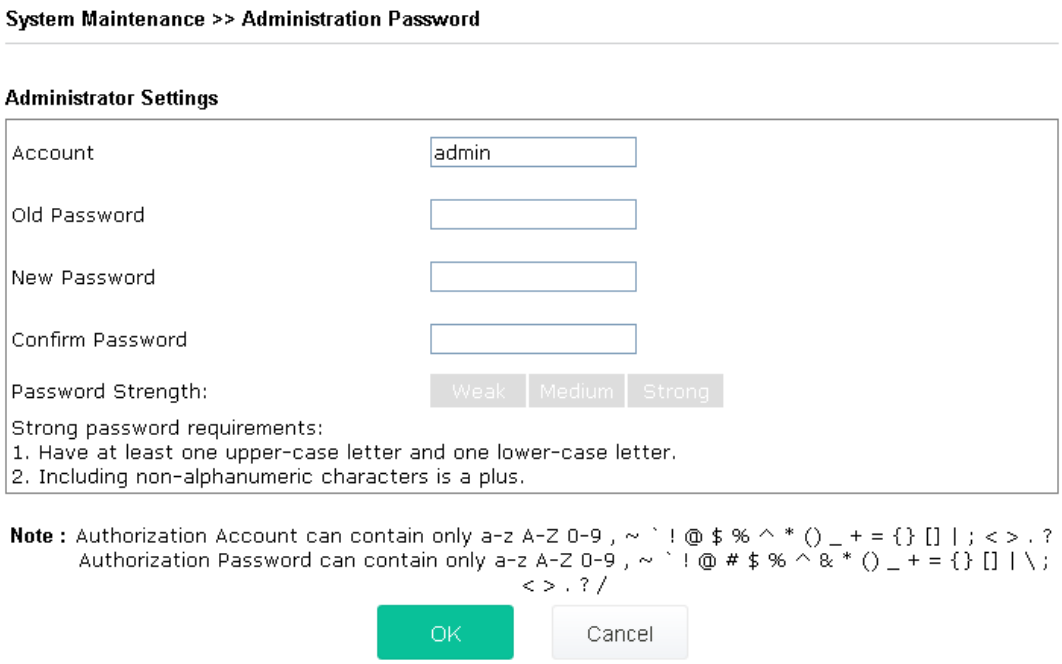
Item	Description
ACS Settings	**Wizard** – Click it to enter the IP address of VigorACS server host, port number and the handler. **URL/Username/Password –** Such data must be typed according to

	the ACS (Auto Configuration Server) you want to link. Please refer to Auto Configuration Server user's manual for detailed information. **Test With Inform** – Click it to send a message based on the event code selection to test if such CPE is able to communicate with VigorACS SI server. **Event Cod**e – Use the drop down menu to specify an event to perform the test. **Last Inform Response Time** – Display the time that VigorACS server made a response while receiving Inform message from CPE last time.
CPE Settings	Such information is useful for Auto Configuration Server (ACS). **Enable**– Check the box to allow the CPE Client to connect with Auto Configuration Server. **SSL(HTTPS) Mode** - Check the box to allow the CPE client to connect with ACS through SSL. **Port** – Sometimes, port conflict might be occurred. To solve such problem, you might change port number for CPE. **Username/Password –** Type the username and password that VigorACS can use to access into such CPE.
Periodic Inform Settings	The default setting is **Enable**. Please set interval time or schedule time for the AP to send notification to VigorACS server. **Interval Time** – Type the value for the interval time setting. The unit is "second".
STUN Settings	The default is **Disable**. If you click **Enable**, please type the relational settings listed below: **Server Address –** Type the IP address of the STUN server. **Server Port –** Type the port number of the STUN server. **Minimum Keep Alive Period –** If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the minimum period. The default setting is "60 seconds". **Maximum Keep Alive Period –** If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the maximum period. A value of "-1" indicates that no maximum period is specified.

After finishing this web page configuration, please click **OK** to save the settings.

III-1-3 Administrator Password

This page allows you to set new password for accessing into web user interface of VigorAP.



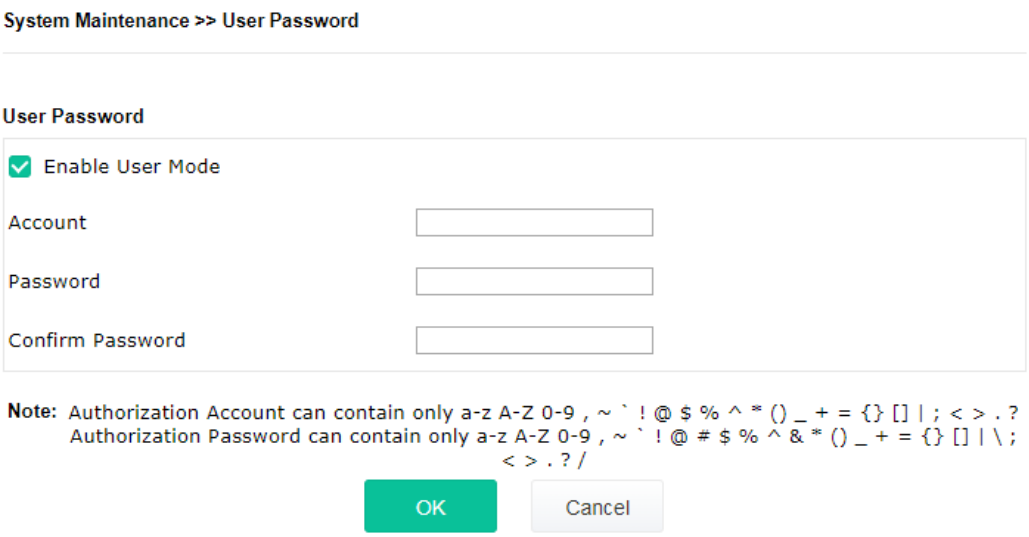
Available settings are explained as follows:

Item	Description
Account	Enter the name for accessing into web user Interface.
Old Password	Enter the old password for accessing into the web user interface.
New Password	Enter in new password in this filed.
Confirm Password	Enter the new password again for confirmation.
Password Strength	The system will display the password strength (represented with the word of weak, medium or strong) of the password specified above.

When you click **OK**, the login window will appear. Please use the new password to access into the web user interface again.

III-1-4 User Password

This page allows you to set new account and password for accessing the web pages under User Mode.



Available settings are explained as follows:

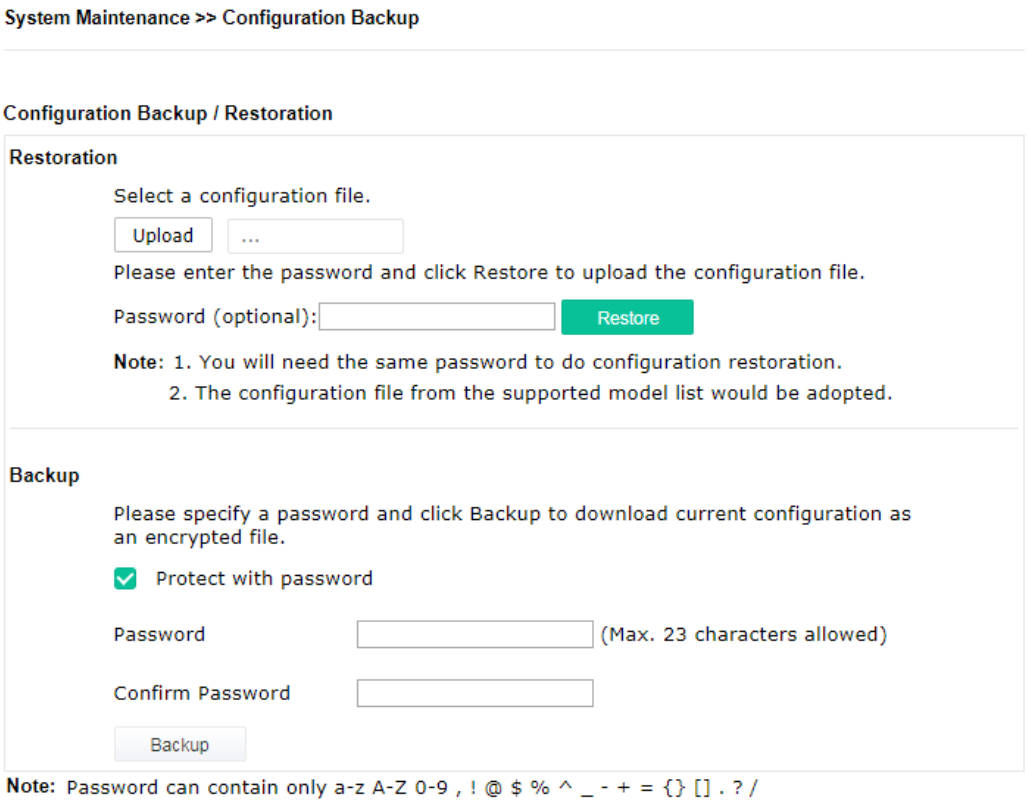
Item	Description
Enable User Mode	After checking this box, you can access into the web user interface with the password typed here for simple web configuration. The settings on simple web user interface will be different with full web user interface accessed by using the administrator password.
Account	Enter a user name.
Password	Enter in new password in this field. The length of the password is limited to 31 characters.
Confirm Password	Enter the new password again.
Password Strength	Display the security strength of the password specified above.

Click **OK** to save the settings**.**

Settings to be configured in User Mode will be less than settings in Admin Mode. Only basic configuration settings will be available in User Mode.

III-1-5 Configuration Backup

Such function can be used to backup/restore the VigorAP 920R settings.

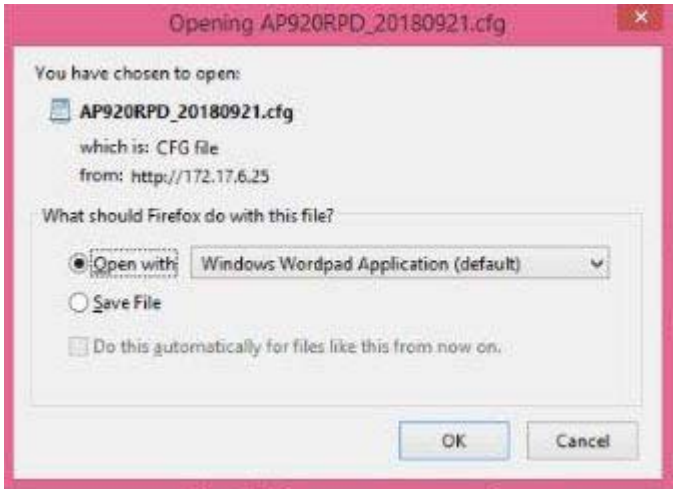


Available settings are explained as follows:

Item	Description
Restoration	**Upload** - Click it to specify a file to be restored. **Password (optional)** – Enter a password for configuration restoration.
Backup	Perform the configuration backup of this device. **Protect with password-** For the sake of security, the configuration file for the access point can be encrypted. **Password** – Type several characters as the password for encrypting the configuration file. **Confirm Password** – Type the password again for confirmation.

Follow the steps below to backup your configuration.

1. Go to **System Maintenance** >> **Configuration Backup**.
2. If required, check the box of **Protect with password** and enter the password.
3. Click **Backup** to get into the following dialog.



Or

4. Click **Save**, the configuration will download automatically to your computer as a file named **config.cfg**.

The above example is using **Windows** platform for demonstrating examples. The **Mac** or **Linux** platform will appear different windows, but the backup function is still available.

Note:

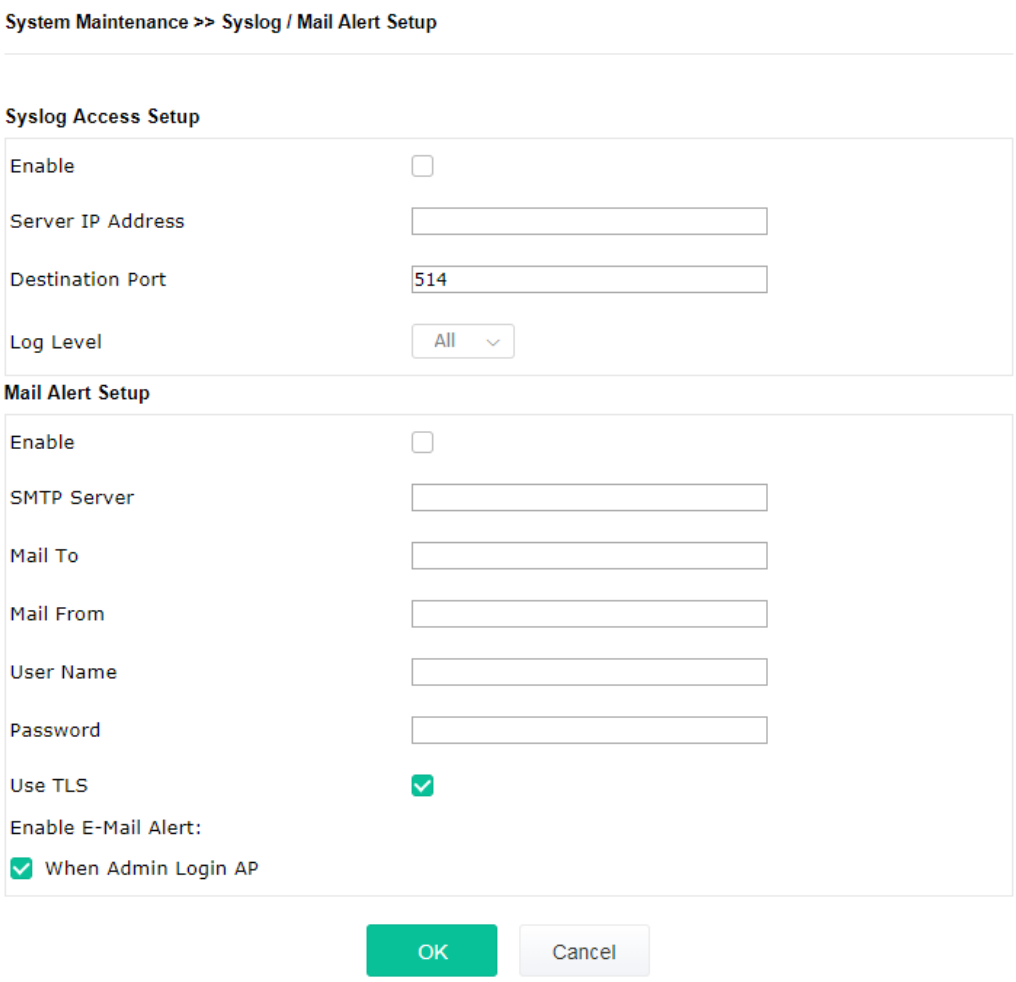
Backup for Certification must be done independently. The Configuration Backup does not include information of Certificate.

Follow the steps below to restore your configuration.

1. Go to **System Maintenance** >> **Configuration Backup**.
2. Click **Upload** to choose the correct configuration file for uploading to the AP.
3. Click **Restore** and wait for few seconds, the following picture will tell you that the restoration procedure is successful.

III-1-6 Syslog/Mail Alert

SysLog function is provided for users to monitor AP. There is no bother to directly get into the Web user interface of the AP or borrow debug equipments.



Available settings are explained as follows:

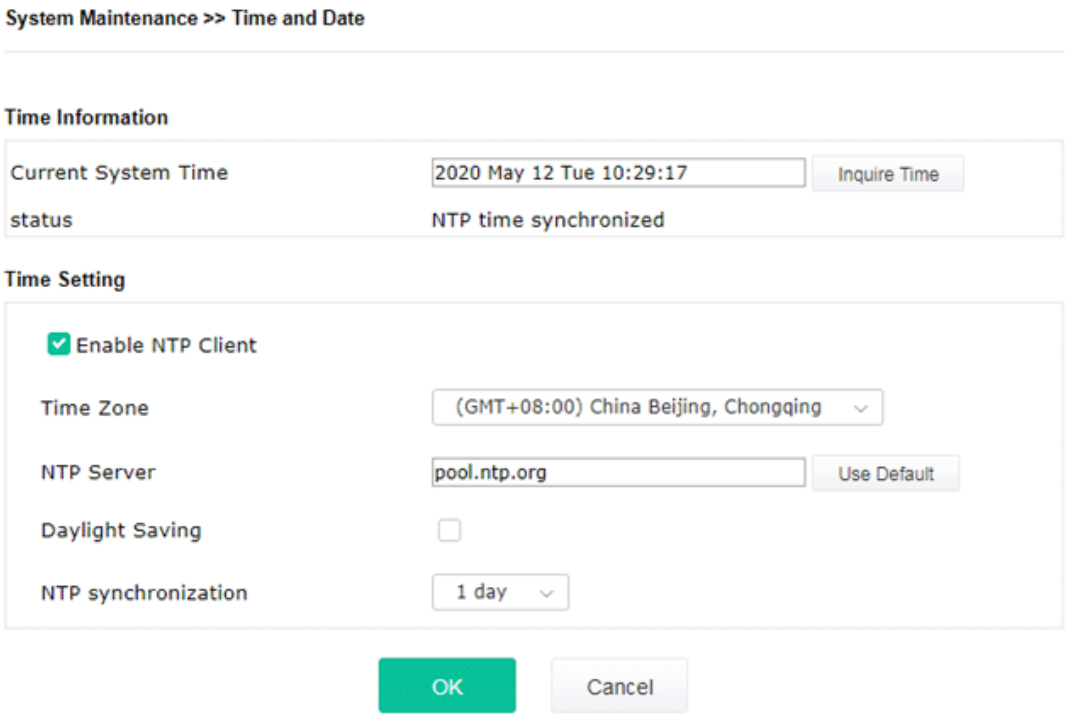
Item	Description
Syslog Access Setup	**Enable** - Check **Enable** to activate function of Syslog. **Server IP Address** -The IP address of the Syslog server. **Destination Port** -Assign a port for the Syslog protocol. The default setting is 514. **Log Level** - Specify which level of the severity of the event will be recorded by Syslog.
Mail Alert Setup	**Enable** - Check **Enable** to activate function of mail alert. **SMTP Server -** The IP address of the SMTP server. **Mail To -** Assign a mail address for sending mails out. **Mail From -** Assign a path for receiving the mail from outside. **User Name -** Type the user name for authentication. **Password -** Type the password for authentication.

	Use TLS – Check this box to encrypt alert mail. However, if the SMTP server specified here does not support TLS protocol, the alert mail with encrypted data will not be received by the receiver. **Enable E-Mail Alert** - VigorAP will send an e-mail out when a user accesses into the user interface by using web or telnet. **When Admin Login AP** – Enable/disable the function. When it is enabled, VigorAP will send out an e-mail to the recipient defined above when a user tries to access into VigorAP by entering login username and password.

Click **OK** to save the settings**.**

III-1-7 Time and Date

It allows you to specify where the time of VigorAP should be inquired from.



Available parameters are explained as follows:

Item	Description
Current System Time	Click **Inquire Time** to get the current time.
Use NTP Client	**Enabled** - Select to inquire time information from Time Server on the Internet using assigned protocol. **Disabled** - Use the browser time from the remote administrator PC host as router's system time.
Time Zone	Select a time protocol.
NTP Server	Type the IP address of the time server. **Use Default** – Click it to choose the default NTP server.
Daylight Saving	Check the box to enable the daylight saving. Such feature is available for certain area.

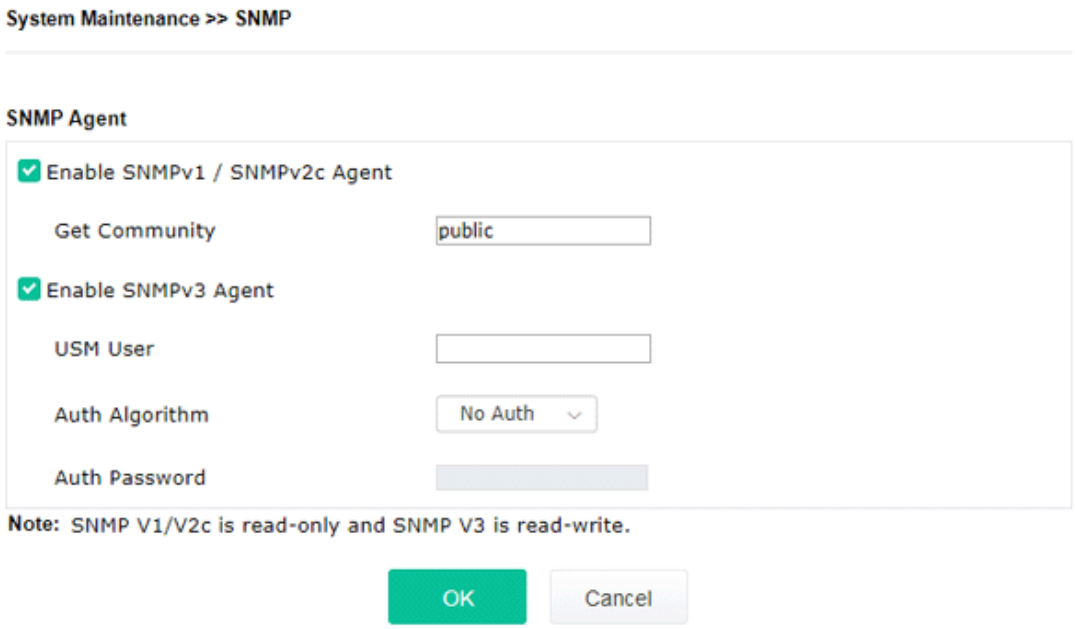
NTP synchronization	Select a time interval for updating from the NTP server.

Click **OK** to save these settings.

III-1-8 SNMP

This page allows you to configure settings for SNMP and SNMPV3 services.

The SNMPv3 is **more secure than** SNMP through the authentication method (support e.g., MD5) for the management needs.



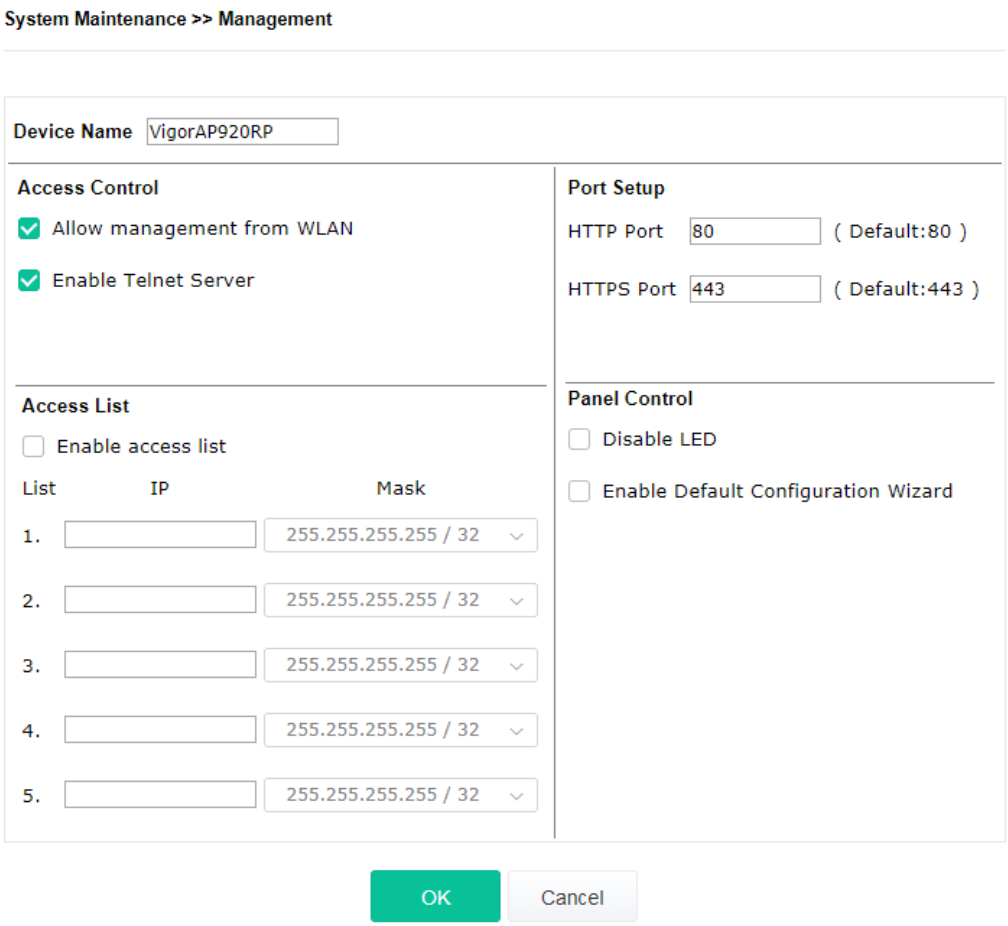
Available settings are explained as follows:

Item	Description
Enable SNMPv1/SNMPv2c Agent	Check it to enable this function.
Enable SNMPV3 Agent	Check it to enable this function.
USM User	USM means user-based security mode. Type a username which will be used for authentication. The maximum length of the text is limited to 23 characters.
Auth Algorithm	Choose one of the encryption methods listed below as the authentication algorithm.
Auth Password	Type a password for authentication. The maximum length of the text is limited to 23 characters.

Click **OK** to save these settings.

III-1-9 Management

This page allows you to specify the port number for HTTP and HTTPS server.



Available parameters are explained as follows:

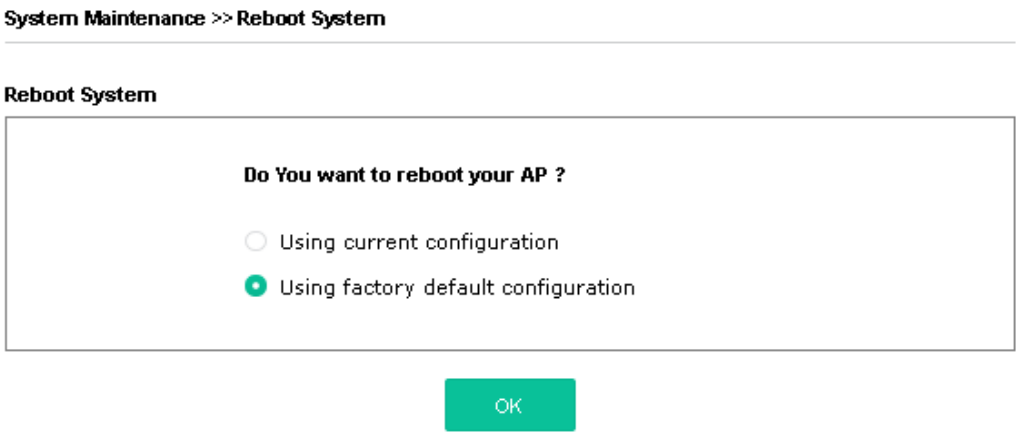
Item	Description
Device Name	The default setting is VigorAP 920R. Change the name if required.
Access Control	**Allow management from WLAN** - Enable the checkbox to allow system administrators to login from wireless LAN. **Enable Telnet Server**– The administrator / user can access into the command line interface of VigorAP remotely for configuring settings.
Access List	**Enable access list** – Check the box to specify that the system administrator can only login from a specific host or network defined in the list. A maximum of five IPs/subnet masks is allowed.
Port Setup	**HTTP port/HTTPS port** -Specify user-defined port numbers for the HTTP and HTTPS servers.
Panel Control	**Disable LED** - The LEDs blink always since VigorAP is powered on. Some people might not like that. Therefore the function of LED is allowed to be disabled to make people feeling comfortable and undisturbed. After checking it, all the LEDs on VigorAP will light off immediately after clicking OK. **Enable Default Configuration Wizard** – Default setting is enabled. When it is enabled, you will be guided into **Quick Start Wizard**

	whenever clicking the DrayTek logo on the top of the web user interface. Such function will be disabled temporary if you have configured Operation Mode, WLAN>>General Setup, WLAN>>Bandwidth Management, WLAN>>Station Control or System Maintenance>>Administration Password.

Click **OK** to save these settings.

III-1-10 Reboot System

The web user interface may be used to restart your modem. Click **Reboot System** from **System Maintenance** to open the following page.



If you want to reboot the modem using the current configuration, check **Using current configuration** and click **OK**. To reset the modem settings to default values, check **Using factory default configuration** and click **OK**. The modem will take 5 seconds to reboot the system.

Note:

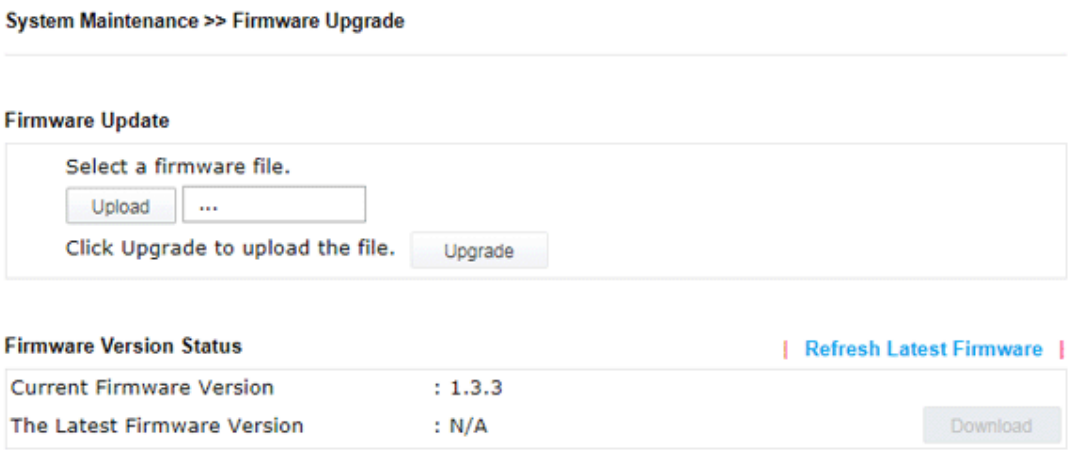
When the system pops up Reboot System web page after configuring the web settings, please click **OK** to reboot your device for ensuring normal operation and preventing unexpected errors of the modem in the future.

III-1-11 Firmware Upgrade

Before upgrading your modem firmware, you need to install the Modem Tools. The **Firmware Upgrade Utility** is included in the tools. The following web page will guide you to upgrade firmware by using an example. Note that this example is running over Windows OS (Operating System).

Download the newest firmware from DrayTek's web site or FTP site. The DrayTek web site is www.draytek.com (or local DrayTek's web site) and FTP site is ftp.draytek.com.

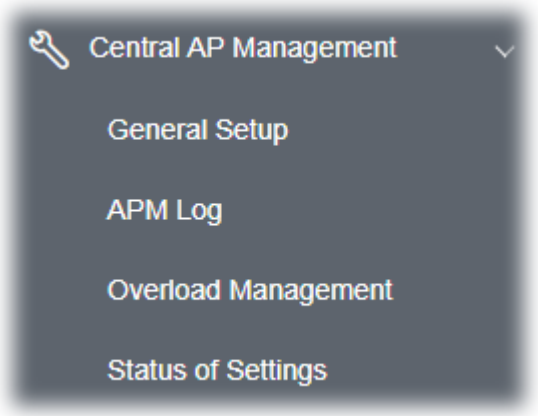
Click **System Maintenance>> Firmware Upgrade** to launch the Firmware Upgrade Utility.



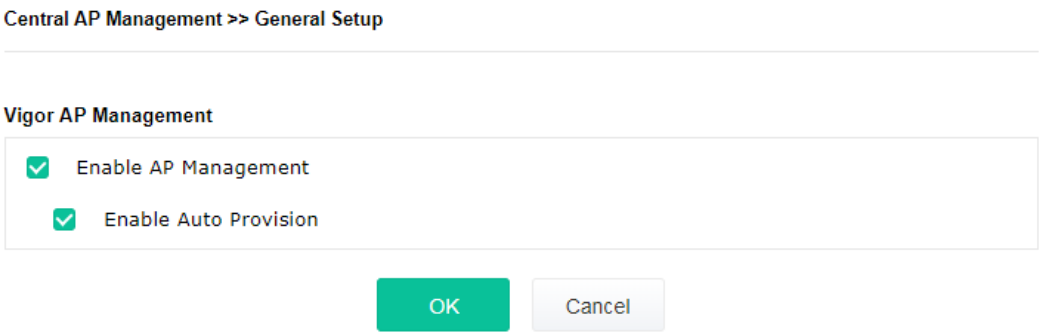
Click **Upload** to locate the newest firmware from your hard disk and click **Upgrade**.

III-2 Central AP Management

Such menu allows you to configure VigorAP device to be managed by Vigor router.



III-2-1 General Setup



Available settings are explained as follows:

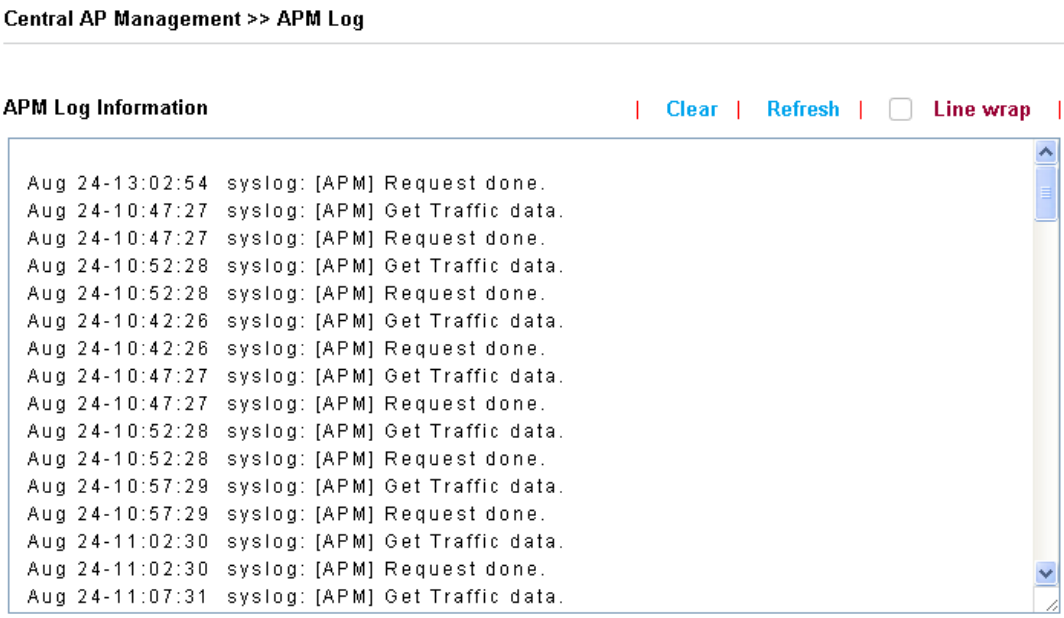
Item	Description
Enable AP Management	Check the box to enable the function of AP Management (APM).
Enable Auto Provision	VigorAP 920R can be controlled under Central AP Management in Vigor2860 series. When both Vigor2860 series and VigorAP 920R have such feature enabled, once VigorAP 920R is registered to Vigor2860 series, the **WLAN profile** pre-configured on Vigor2860 series will be applied to VigorAP 920R immediately. Thus, it is not necessary to configure VigorAP 920R separately.

Click **OK** to save these settings.

III-2-2 APM Log

This page will display log information related to wireless stations connected to VigorAP 920R and central AP management.

Such information also will be delivered to Vigor router (e.g., Vigor2860 or Vigor2925 series) and be shown on **Central AP Management>>Event Log** of Vigor router.

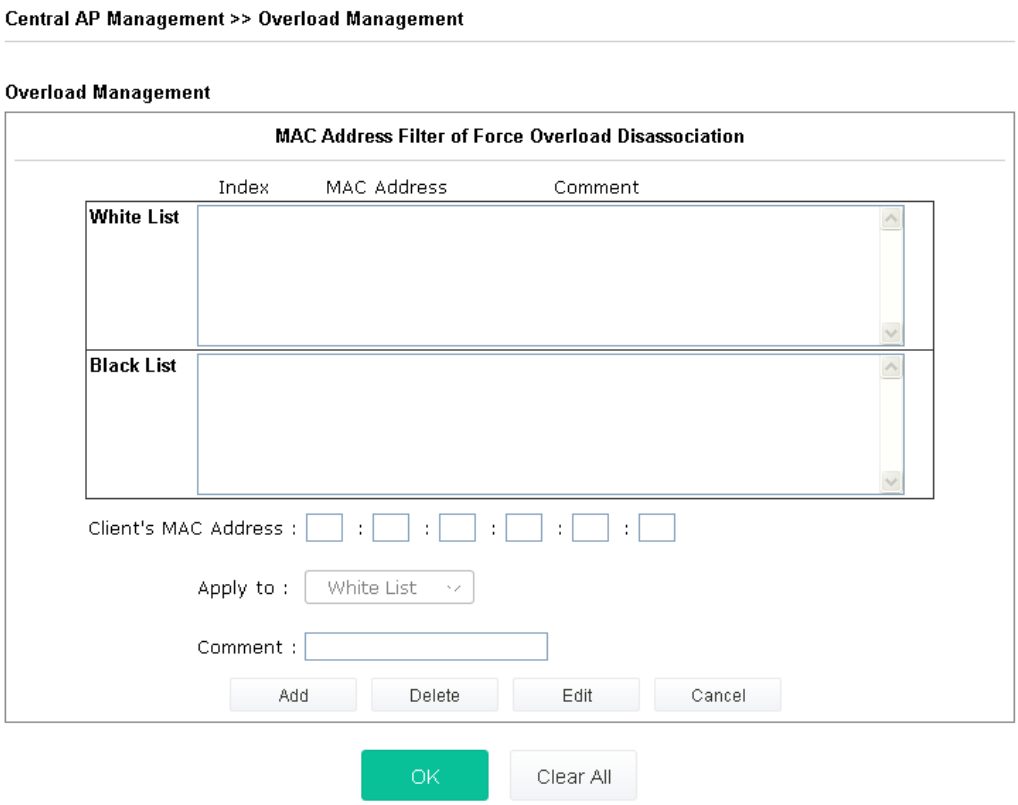


III-2-3 Overload Management

Load Balance can help to distribute the traffic for all of the access points (e.g., VigorAP 920R) registered to Vigor router. Thus, the bandwidth will not be occupied by certain access points.

However, traffic overload might be occurred if too many wireless stations connected to VigorAP 920R for data incoming and outgoing. Therefore, "Force Overload Disassociation" is required to terminate the network connection of the client's station to release network traffic. When the function of "Force Overload Disassociation" in web user interface of Vigor router (e.g., Vigor2862 or Vigor2926 series) is enabled, wireless clients specified in **black list** of such web page will be disassociated to solve the problem of traffic overload.

The following web page is used to configure white list and black list for wireless stations.



Available settings are explained as follows:

Item	Description
White List/Black List	Display the information (such as index number, MAC address and comment) for all of the members in White List/Black List. Wireless stations listed in Black List will be forcefully disconnected first when traffic overload occurs and "Force Overload Disassociation" is enabled.
Client's MAC Address	Specify the MAC Address of the remote/local client.
Apply to	**White List** – MAC address listed inside Client's MAC Address will be categorized as one of members in White List. **Black List** - MAC address listed inside Client's MAC Address will be categorized as one of members in Black List.

Comment	Type a brief description for the specified client's MAC address.
Add	Add a new MAC address into the White List/Black List.
Delete	Delete the selected MAC address in the White List/Black List.
Edit	Edit the selected MAC address in the White List/Black List.
Cancel	Give up the configuration.

Click **OK** to save these settings.

III-2-4 Status of Settings

Load Balance can help to distribute the traffic for all of the access points (e.g., VigorAP 920Rs) registered to Vigor 2862 or Vigor2926 series. This web page displays the settings related to Load Balance for VigorAP 920R. In which, By Station Number, By Traffic and Force Overload Disassociation indicate settings configured in Vigor 2862 or Vigor2926 series.

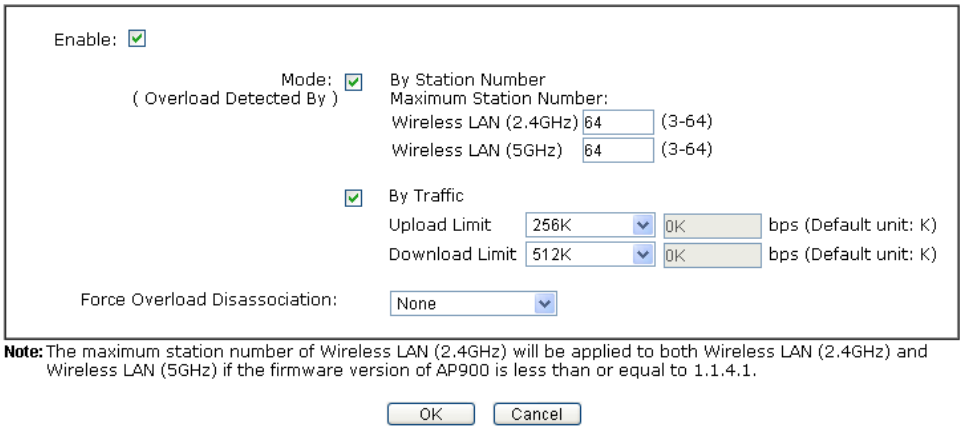
Central AP Management >> Status of Settings

Function Name	Status	Value
Load Balance		
Station Number Threshold	✗	
Max WLAN(5GHz) Station Number		128
Max WLAN(2.4GHz) Station Number		128
Traffic Threshold	✗	
Download Limit		None bps
Upload Limit		None bps
Force Overload Disassociation	✗	
RSSI Threshold		-50 dBm
Disassociate By		None
Rogue AP Detection		
Rogue AP Detection	✗	

"X" means the function is not enabled or VigorAP 920R has not registered to any Vigor router yet.

Below shows a setting example for Load Balance settings configured in Vigor 2862 or Vigor2926 series.

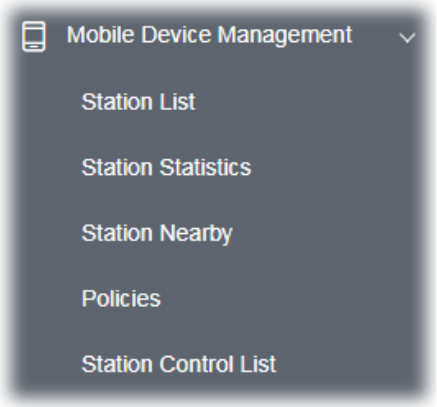
Central AP Management >> Load Balance



III-3 Mobile Device Management

Such feature can control / manage the mobile devices accessing the wireless network of VigorAP. VigorAP offers wireless LAN service for mobile device(s), PC users, MAC users or other users according to the policy selected.

Below shows the menu items for Mobile Device Management (MDM).

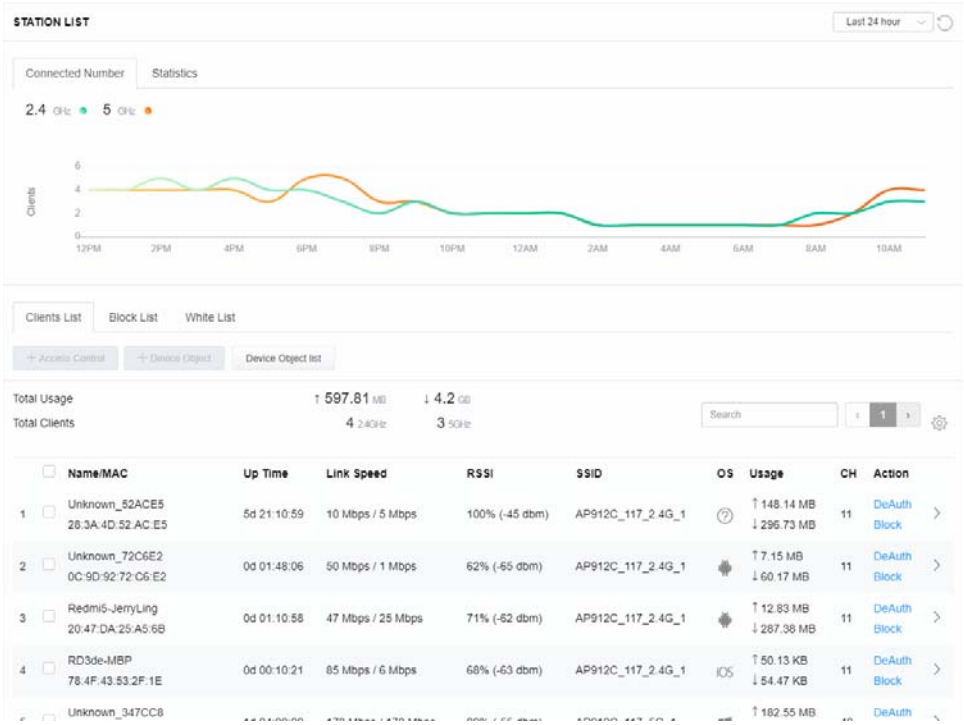


III-3-1 Station List

Station List provides the information related to the number of clients connecting to VigorAP, used bandwidth and the statistics of the AP device OS. Besides, users can create access control policies, device objects and set black & white list for

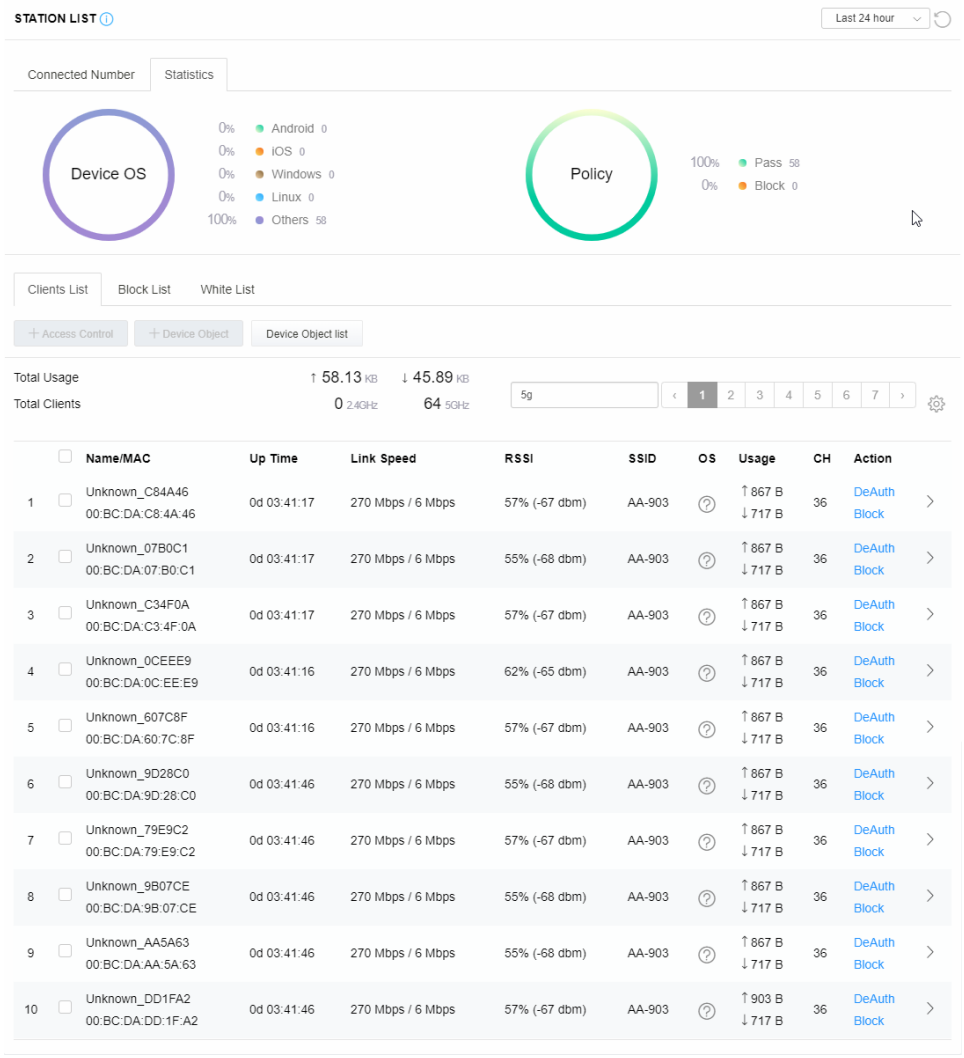
III-3-1-1 Connected Number

This page lists the graph for the number of wireless stations connected to this Access Point with different time phases.



III-3-1-2 Statistics

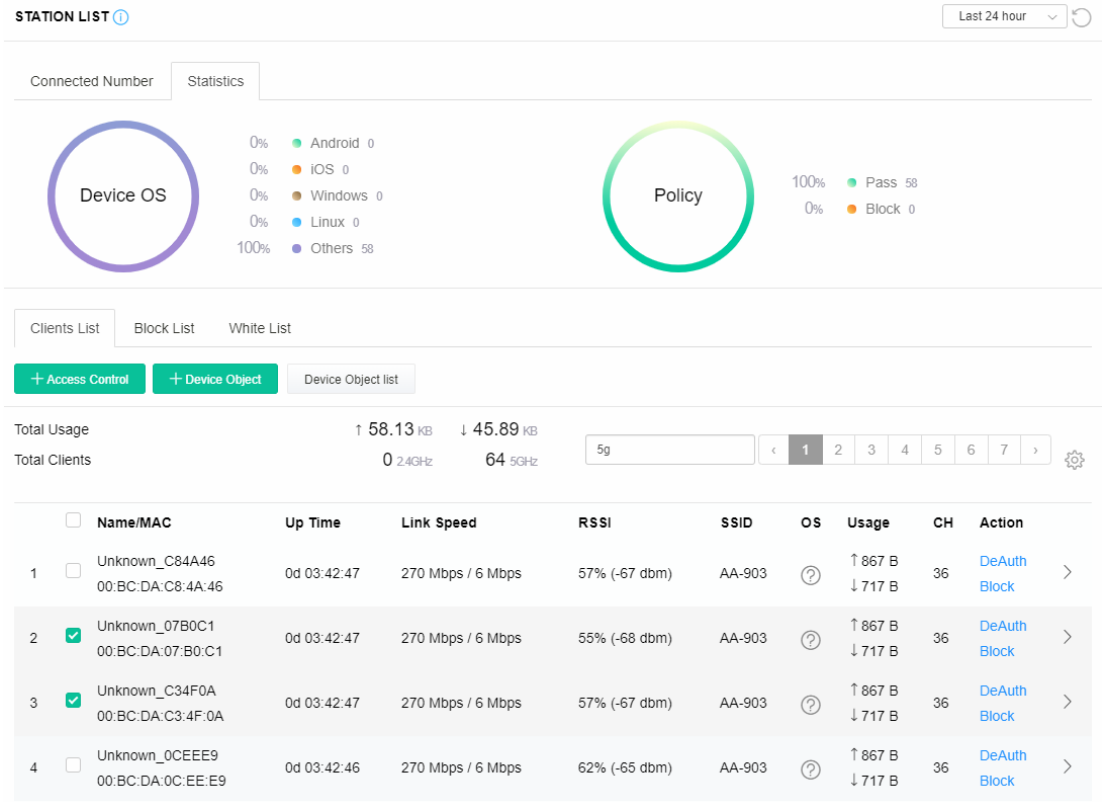
The number of detected devices and the number of device(s) passed/blocked according to the policy specified in **Mobile Device Management>>Policies** can be illustrated as doughnut chart.



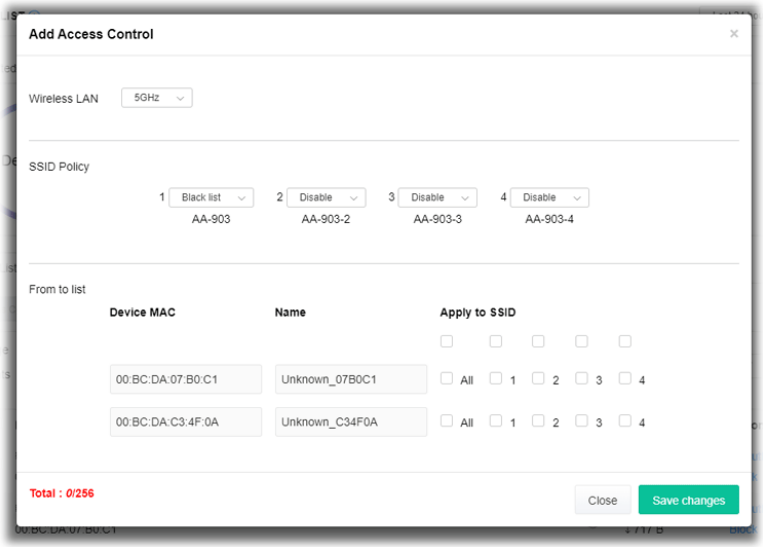
	Name/MAC	Up Time	Link Speed	RSSI	SSID	OS	Usage	CH	Action
1	Unknown_C84A46 00:BC:DA:C8:4A:46	0d 03:41:17	270 Mbps / 6 Mbps	57% (-67 dbm)	AA-903		↑867 B ↓717 B	36	DeAuth Block
2	Unknown_07B0C1 00:BC:DA:07:B0:C1	0d 03:41:17	270 Mbps / 6 Mbps	55% (-68 dbm)	AA-903		↑867 B ↓717 B	36	DeAuth Block
3	Unknown_C34F0A 00:BC:DA:C3:4F:0A	0d 03:41:17	270 Mbps / 6 Mbps	57% (-67 dbm)	AA-903		↑867 B ↓717 B	36	DeAuth Block
4	Unknown_0CEEE9 00:BC:DA:0C:EE:E9	0d 03:41:16	270 Mbps / 6 Mbps	62% (-65 dbm)	AA-903		↑867 B ↓717 B	36	DeAuth Block
5	Unknown_607C8F 00:BC:DA:60:7C:8F	0d 03:41:16	270 Mbps / 6 Mbps	57% (-67 dbm)	AA-903		↑867 B ↓717 B	36	DeAuth Block
6	Unknown_9D28C0 00:BC:DA:9D:28:C0	0d 03:41:46	270 Mbps / 6 Mbps	55% (-68 dbm)	AA-903		↑867 B ↓717 B	36	DeAuth Block
7	Unknown_79E9C2 00:BC:DA:79:E9:C2	0d 03:41:46	270 Mbps / 6 Mbps	57% (-67 dbm)	AA-903		↑867 B ↓717 B	36	DeAuth Block
8	Unknown_9B07CE 00:BC:DA:9B:07:CE	0d 03:41:46	270 Mbps / 6 Mbps	55% (-68 dbm)	AA-903		↑867 B ↓717 B	36	DeAuth Block
9	Unknown_AA5A63 00:BC:DA:AA:5A:63	0d 03:41:46	270 Mbps / 6 Mbps	55% (-68 dbm)	AA-903		↑867 B ↓717 B	36	DeAuth Block
10	Unknown_DD1FA2 00:BC:DA:DD:1F:A2	0d 03:41:46	270 Mbps / 6 Mbps	57% (-67 dbm)	AA-903		↑903 B ↓717 B	36	DeAuth Block

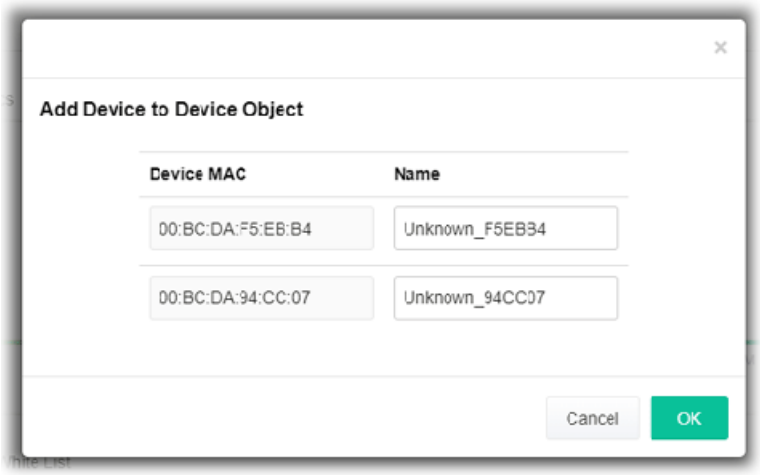
III-3-1-3 Clients List

The client list displays all the stations connecting to VigorAP.



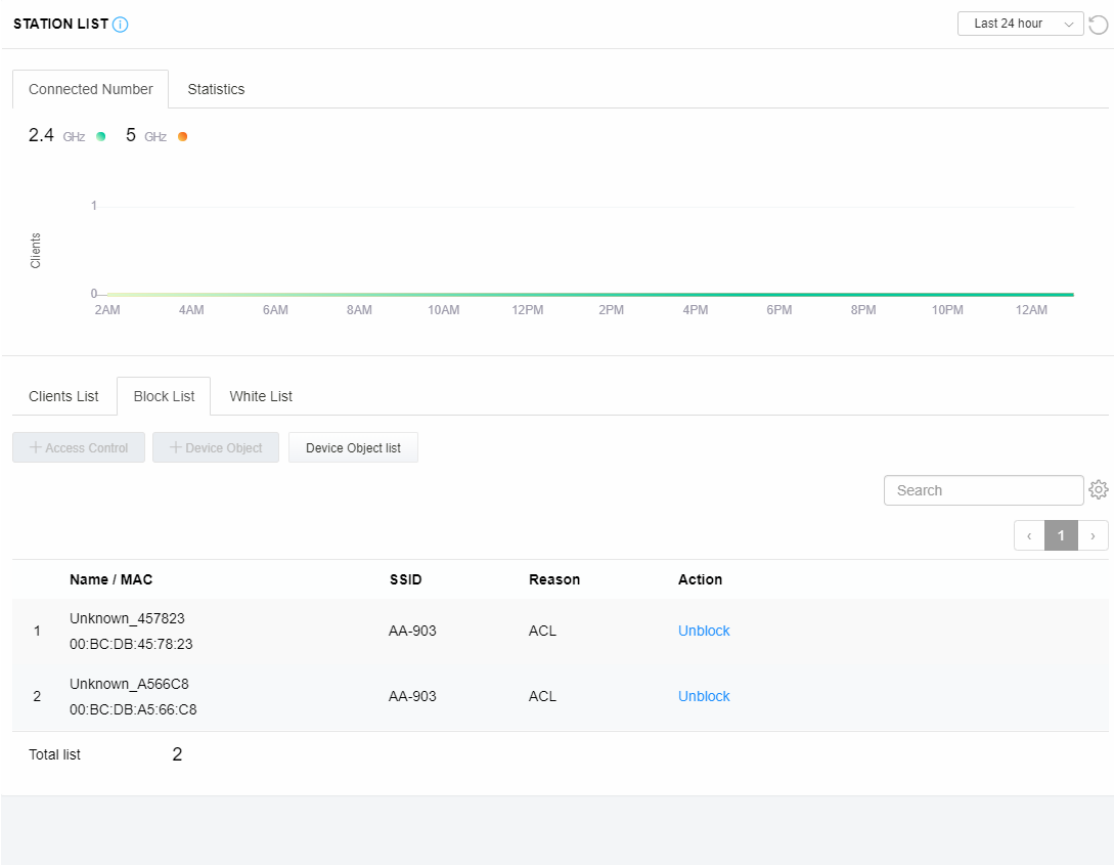
Available settings are explained as follows:

Item	Description
+Access Control	It is available after choosing one of the entries (clients) on Clients List.  **Wireless LAN** - Specify the bandwidth for the access control list. **SSID Policy** - Set the policy for each SSID as black list or white list or disable. **From to list** - Display the clients available for applying this access

	control. **Apply to SSID** - Check **All** to make the device apply the policies to all SSIDs. Or select the one(s) to make the device apply the policies to the selected SSIDs. **Close** - Exit this page without saving any changes. **Save changes** - Save the changes and exit this page.
+Device Object	To add a device to device object list, choose one of the entries (clients) on Clients List to enable the Device Object button. Click the button to open the following page.  Check the information listed on the page. Change the MAC address or name of the selected entry if required. Then click **OK** and exit the page.
Device Object list	The existed device object profiles will be shown on the following page.
Clients List	Display the stations connecting to this Vigor device. **Total Usage -** Display **Total Clients -** Display the number of the clients using 2.4GHz **Name / MAC -** Display the host name / MAC address of the connecting client. **Up Time** - Display the connection time. **Link Speed**- Display the link speed. **RSSI** - Display the RSSI value. **SSID** - Display the SSID the client used for connecting VigorAP. **OS** - Display the OS of the client. **Usage** - Display the bandwidth usage (up and down) of the client. **CH** - Display the channel used by the client. **Action** - Display the authentication method used by the client, and if it is on block list or white list.

II-3-13-4 Block List

This page displays information of the stations under block list.

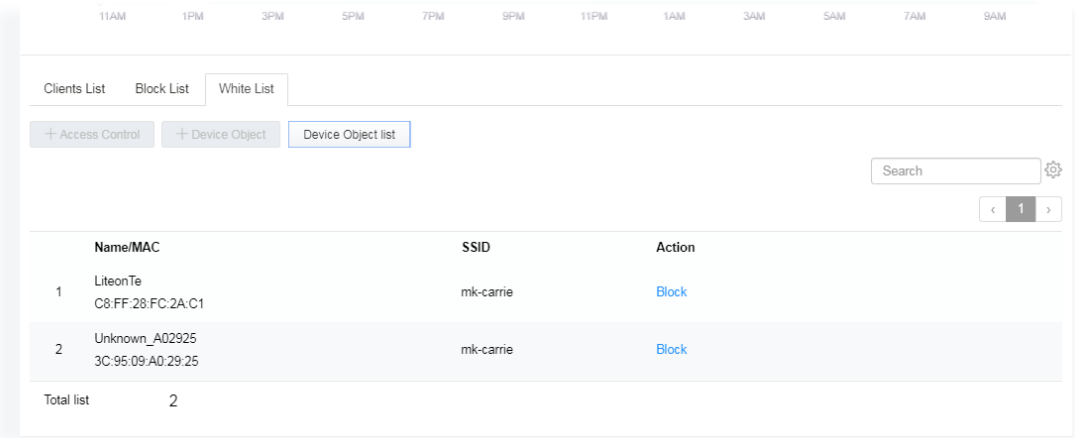


Available settings are explained as follows:

Item	Description
Device Object list	Click it to open the Device Object List dialog for reference.
Name / MAC	Display the host name / MAC Address for the connecting client.
SSID	Display the SSID that the wireless client connects to.
Reason	Display the reference information.
Action	Display the action that you can execute for the station. **Unblock** - Click to unblock the entry.

III-3-1-5 White List

This page displays general information of the stations under white list.

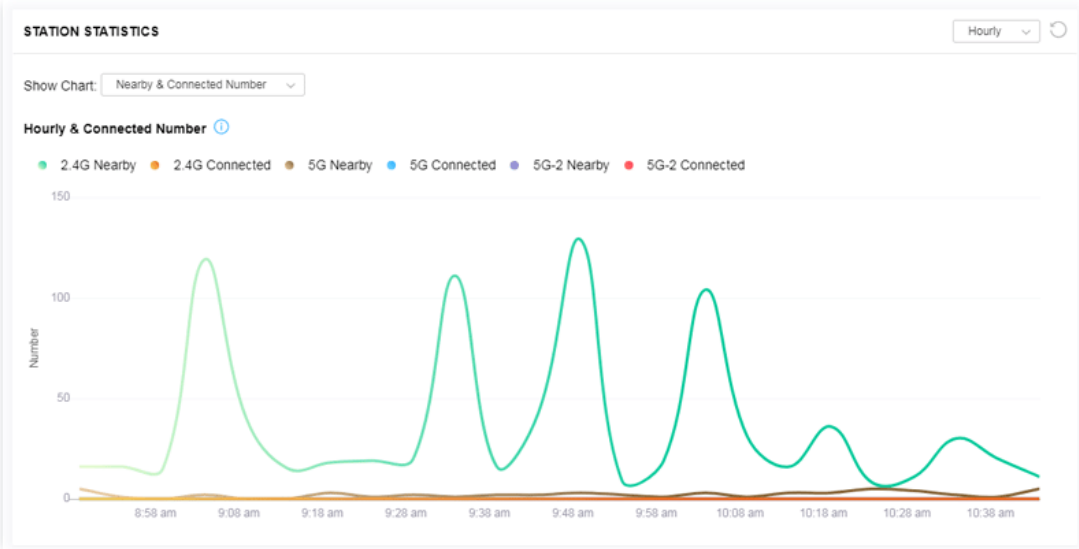


Available settings are explained as follows:

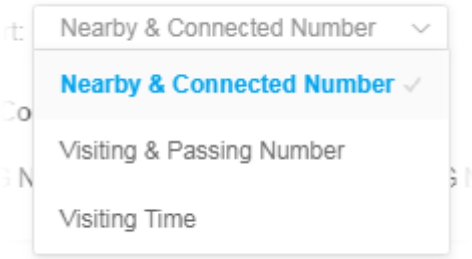
Item	Description
Device Object list	Click it to open the Device Object List dialog for reference.
Name / MAC	Display the host name / MAC Address for the connecting client.
SSID	Display the SSID that the wireless client connects to.
Action	Display the action that you can execute for the station. **Block** - Click to block the entry.

III-3-2 Station Statistics

This page is used for debug or for the user to observe network traffic and network quality.

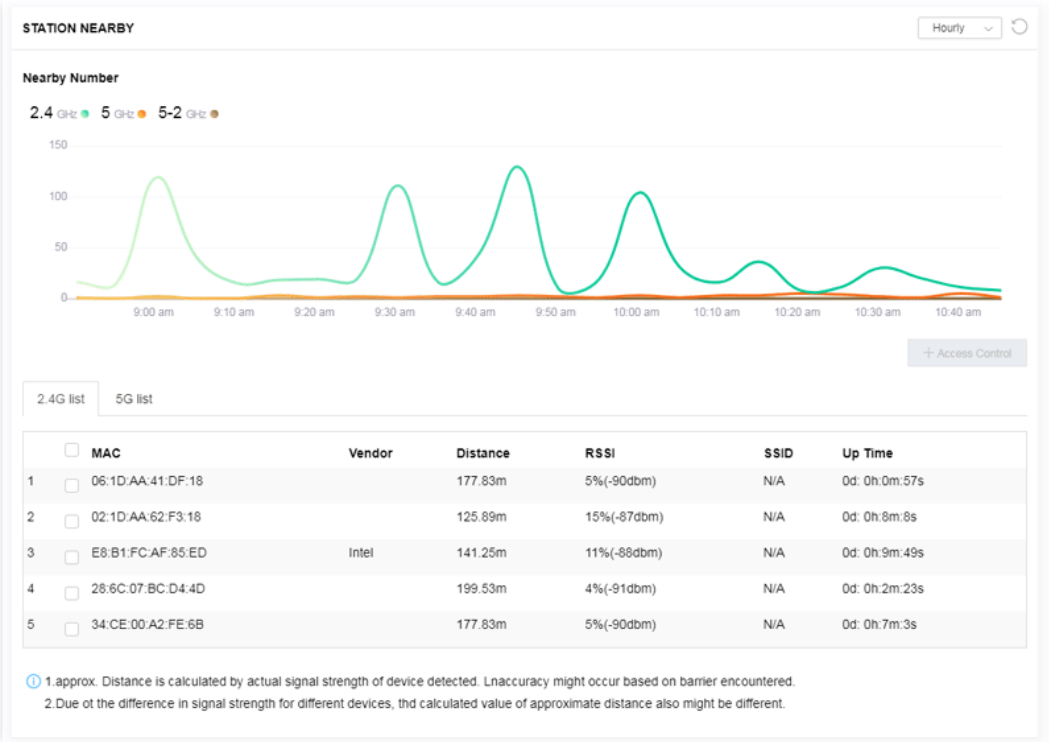


Available parameters are explained as follows:

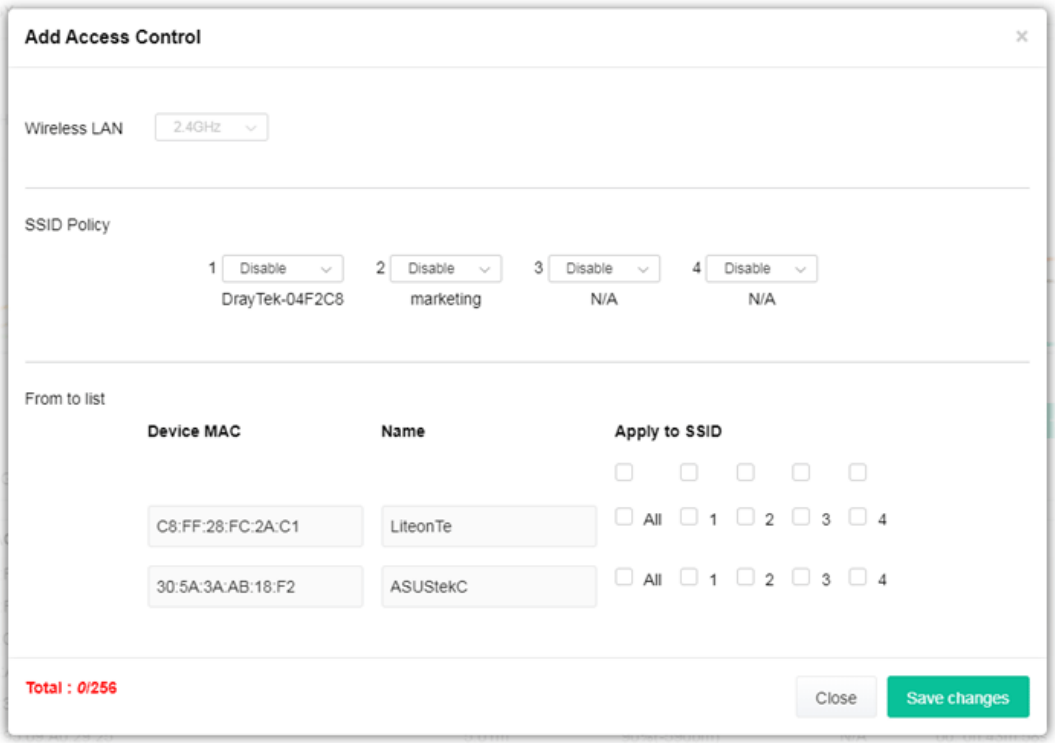
Item	Description
Show Chart	Choose one of the items to display the statistics chart for wireless stations.  **Nearby & Connected Number** – Choose it to have the statistics of the wireless stations which is nearby and connected to VigorAP 920R. **Visiting & Passing Number** – Choose it to have the statistics of the wireless stations which is visiting and passing to VigorAP 920R. **Visiting Time** - Choose it to have the statistics of the wireless stations which is visiting VigorAP 920R.

III-3-3 Station Nearby

This page displays the general information for the nearby stations.



You can select the station(s) and click **+Access Control** to configure the nearby stations as the one(s) to pass through VigorAP or to be blocked by VigorAP.

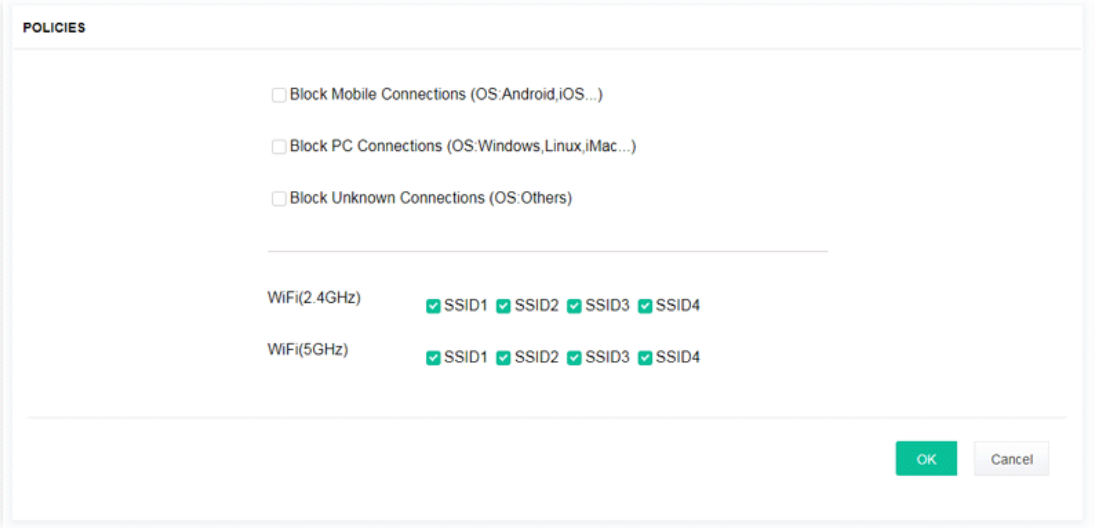


Available parameters are explained as follows:

Item	Description
SSID Policy	Determine the policy (disable, white list or black list) applied for the SSID (1 to 4).
From to list	**Device MAC** - Display the MAC address of the selected station. **Name** - Display the name of the selected station. **Apply to SSID** - Check the box(es) to apply the SSID to the selected station. **Close** - Exit the dialog without saving the changes. **Save changes** - Save the changes and exit the dialog.

III-3-4 Policies

Such page determines which devices (mobile, PC, MAC or others) allowed to make network connections via VigorAP or blocked by VigorAP.



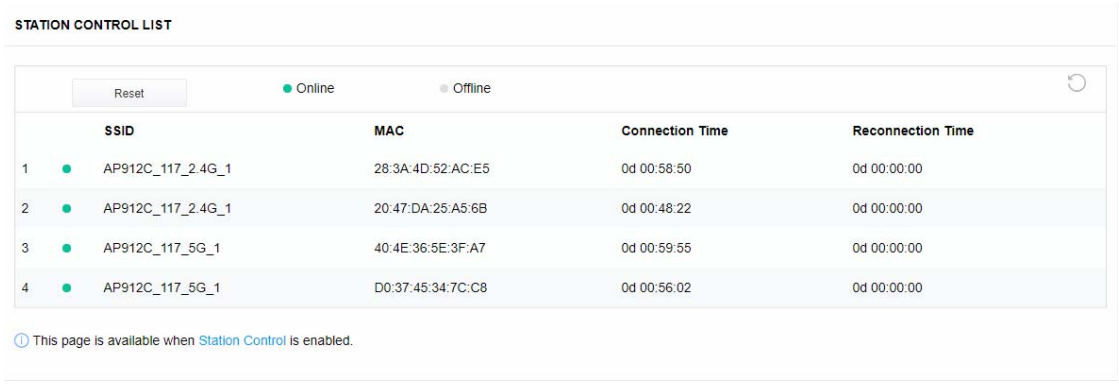
Each item is explained as follows:

Item	Description
Block Mobile Connections	All of mobile devices will be blocked and not allowed to access into Internet via VigorAP.
Block PC Connections	All of network connections based on PC, MAC or Linux platform will be blocked and terminated.
Block Unknown Connections	Only the unknown network connections (unable to be recognized by Vigor router) will be blocked and terminated.
WiFi(2.4GHz)	Specify the SSID(s) to apply such policy.
WiFi(5GHz)	Specify the SSID(s) to apply such policy.

After finished the policy selection, click **OK**. VigorAP will *reboot* to activate the new policy automatically.

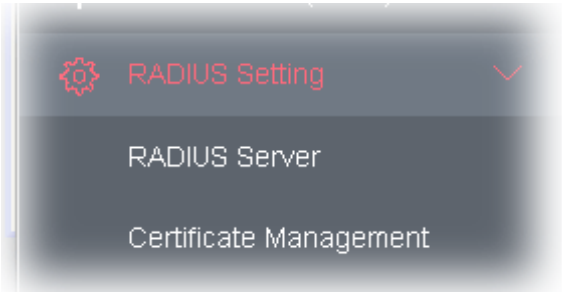
III-3-5 Station Control List

This page displays information related to the wireless stations connecting to the Vigor AP.



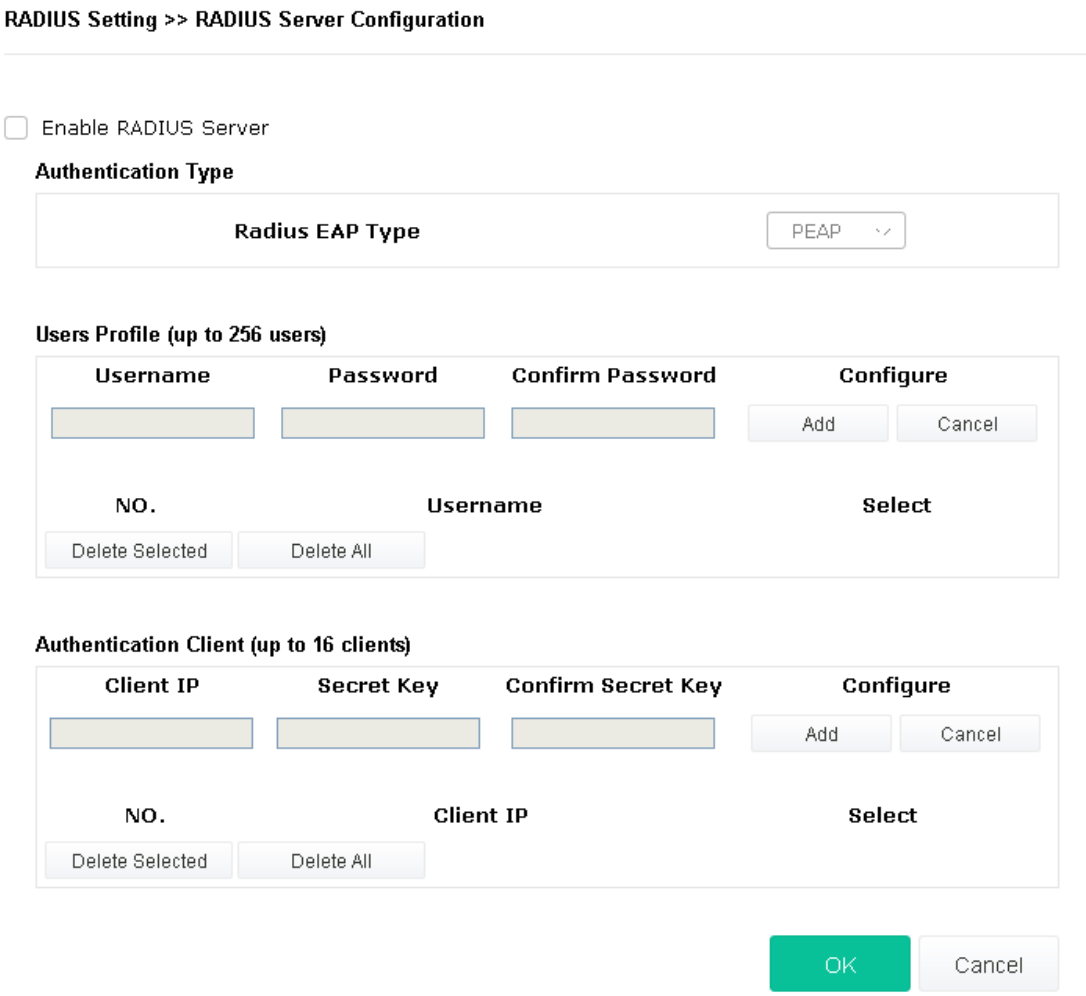
Chapter IV Others

IV-1 RADIUS Setting



IV-1-1 RADIUS Server

VigorAP 920R offers a built-in RADIUS server to authenticate the wireless client that tries to connect to VigorAP 920R. The AP can accept the wireless connection authentication requested by wireless clients.



Available settings are explained as follows:

Item	Description
Enable RADIUS Server	Check it to enable the internal RADIUS server.

Authentication Type	Let the user to choose the authentication method for RADIUS server. **Radius EAP Type** – There are two types, PEAP and EAP TLS, offered for selection. If EAP TLS is selected, a certificate must be installed or must be ensured to be trusted.
Users Profile	**Username** – Type a new name for the user profile. **Password** – Type a new password for such new user profile. **Confirm Password** – Retype the password to confirm it. **Configure** • **Add** – Make a new user profile with the name and password specified on the left boxes. • **Cancel** – Clear current settings for user profile. **Delete Selected** – Delete the selected user profile (s). **Delete All** – Delete all of the user profiles.
Authentication Client	This internal RADIUS server of VigorAP 920R can be treated as the external RADIUS server for other users. Specify the client IP and secret key to make the wireless client choosing VigorAP 920R as its external RADUIS server. **Client IP** – Type the IP address for the user to be authenticated by VigorAP 920R when the user tries to use VigorAP 920R as the external RADIUS server. **Secret Key** – Type the password for the user to be authenticated by VigorAP 920R while the user tries to use VigorAP 920R as the external RADIUS server. **Confirm Secret Key** – Type the password again for confirmation. **Configure** • **Add** – Make a new client with IP and secret key specified on the left boxes. • **Cancel** – Clear current settings for the client. **Delete Selected** – Delete the selected client(s). **Delete All** – Delete all of the clients.
Backup	Click it to store the settings (RADIUS configuration) on this page as a file.
Restore	Click it to restore the settings (RADIUS configuration) from an existed file.

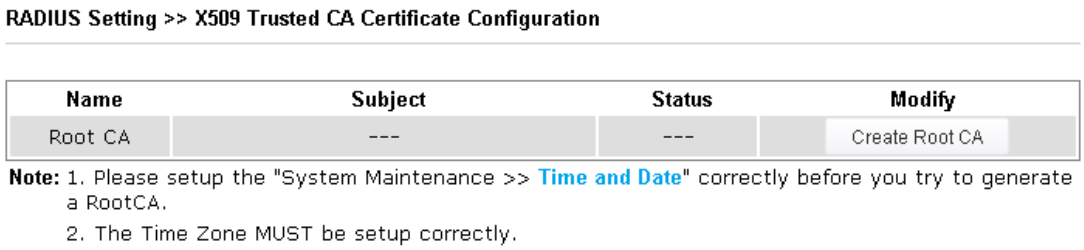
After finishing this web page configuration, please click **OK** to save the settings.

IV-1-2 Certificate Management

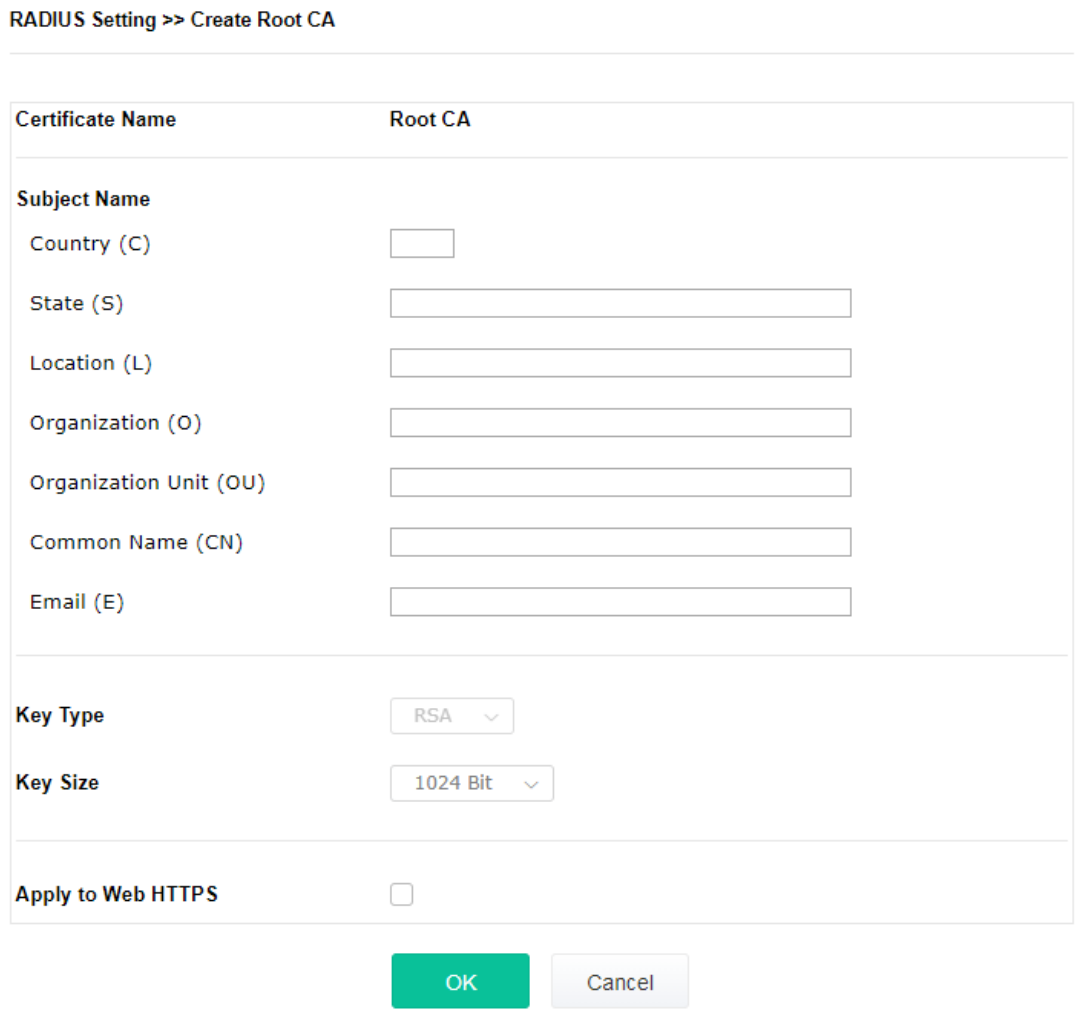
When the local client and remote server are required to make certificate authentication (e.g., Radius EAP-TLS authentication) for wireless connection and avoiding the attack of MITM, a trusted root certificate authority (Root CA) will be used to authenticate the digital certificates offered by both ends.

However, the procedure of applying digital certificate from a trusted root certificate authority is complicated and time-consuming. Therefore, Vigor AP offers a mechanism which allows you to generate root CA to save time and provide convenience for general user. Later, such root CA generated by DrayTek server can perform the issuing of local certificate.

Root CA can be deleted but not edited. If you want to modify the settings for a Root CA, please delete the one and create another one by clicking Create Root CA.



Click **Create Root CA** to open the following page. Type or choose all the information that the window request such as subject name, key type, key size and so on.



Available settings are explained as follows:

Item	Description
Subject Name	Type the required information for creating a root CA. Country (C) – Type the country code (two characters) in this box. State (S)/ Location (L)/ Organization (O)/ Organization Unit (OU) /Common Name (CN) - Type the name or information for the root CA with length less than 32 characters. Email (E) – Type the email address for the root CA with length less than 32 characters.
Key Type	At present, only RSA (an encryption algorithm) is supported by such

	device.
Key Size	To determine the size of a key to be authenticated, use the drop down list to specify the one you need.
Apply to Web HTTPS	VigorAP needs a certificate to access into Internet via Web HTTPS. Check this box to use the user-defined root CA certificate which will substitute for the original certificate applied by web HTTPS.

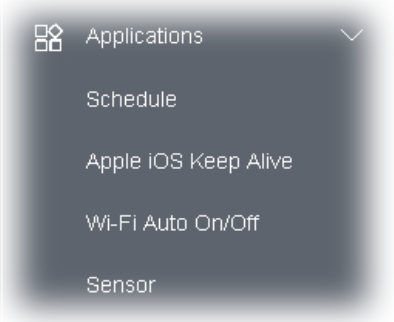
Note:

"Common Name" must be configured with rotuer's WAN IP or domain name.

After finishing this web page configuration, please click **OK** to save the settings. A new root CA will be generated.

IV-2 Applications

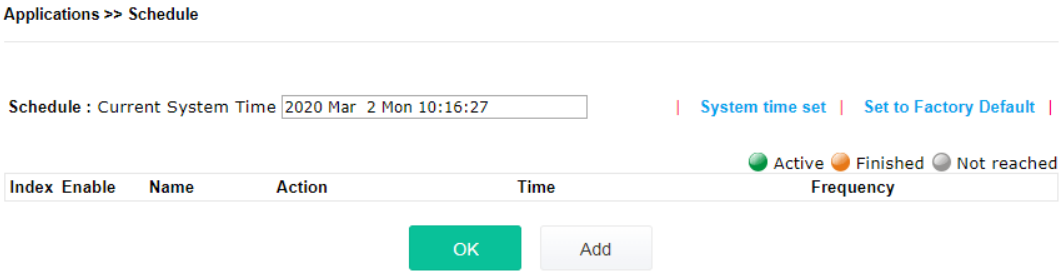
Below shows the menu items for Applications.



IV-2-1 Schedule

The VigorAP has a built-in clock which can update itself manually or automatically by means of Network Time Protocols (NTP). As a result, you can not only schedule the AP to dialup to the Internet at a specified time, but also restrict Internet access to certain hours so that users can connect to the Internet only during certain hours, say, business hours. The schedule is also applicable to other functions.

You have to set your time before set schedule. In **System Maintenance>> Time and Date** menu, press **Inquire Time** button to set the VigorAP's clock to current time of your PC. The clock will reset once if you power down or reset the AP. There is another way to set up time. You can inquiry an NTP server (a time server) on the Internet to synchronize the AP's clock. This method can only be applied when the WAN connection has been built up.



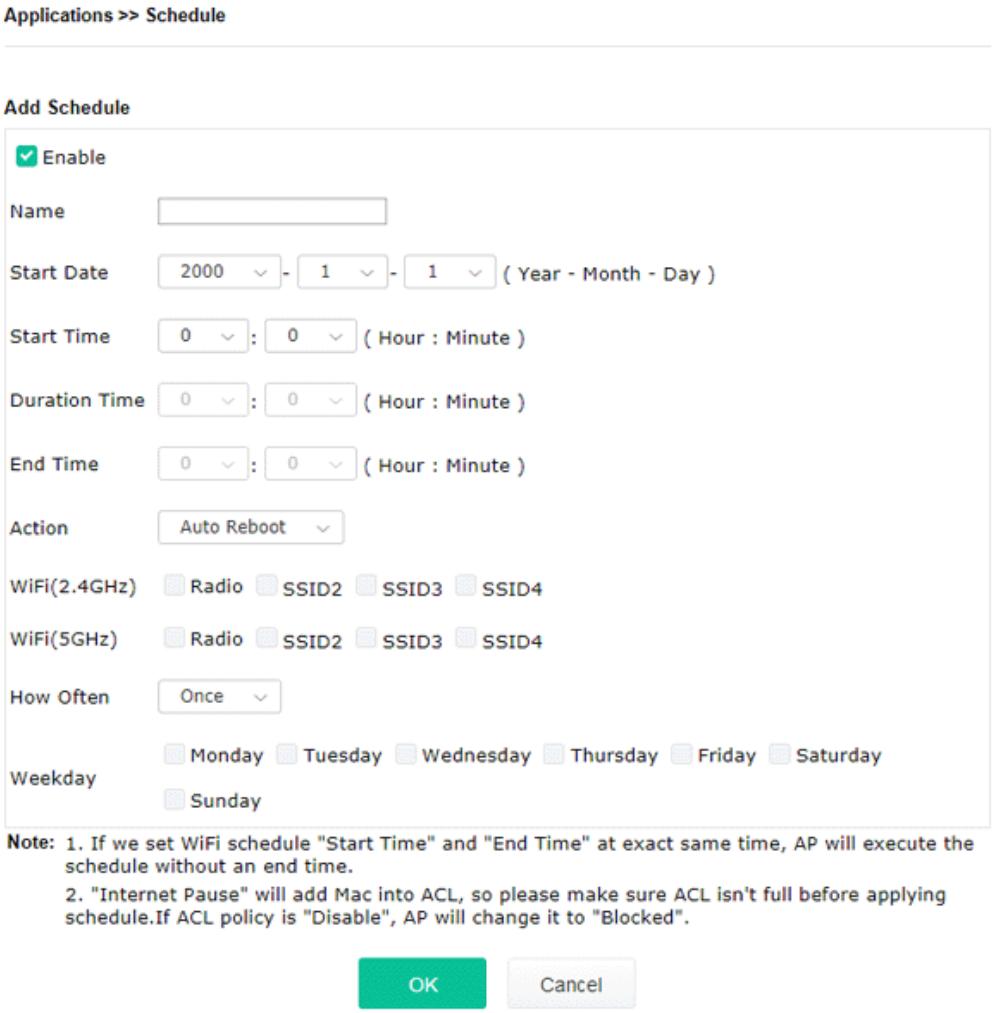
Available settings are explained as follows:

Item	Description
Schedule	**Enable Schedule** - Check it to enable the function of schedule configuration.
Schedule Configuration	**Index** – Display the sort number of the schedule profile. **Setting** – Display the summary of the schedule profile. **Action** – Display the action adopted by the schedule profile. **Status** – Display if the profile is enabled (V) or not (X). **Add** – Such button is available when **Enable Schedule** is checked. It allows to add a new schedule profile.

	Delete – Check the index box of the schedule profile and click such button to remove the profile.

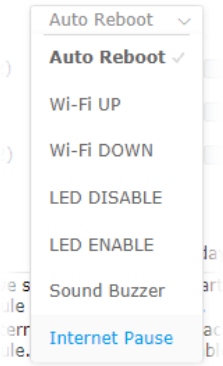
You can set up to **15** schedules. To add a schedule:

1. Check the box of **Enable Schedule**.
2. Click the **Add** button to open the following web page.

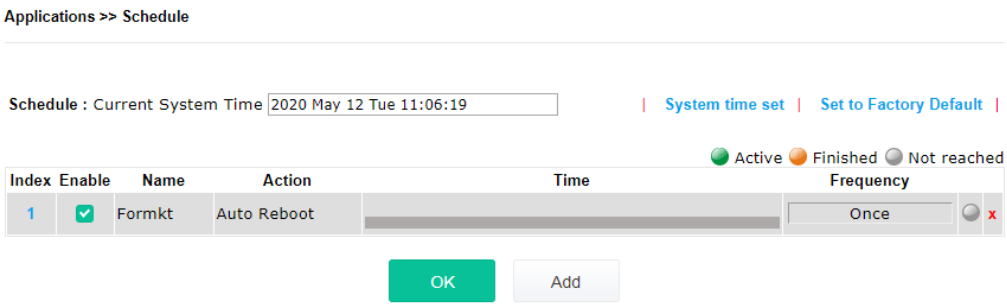


Available settings are explained as follows:

Item	Description
Enable	Check to enable such schedule profile.
Start Date	Specify the starting date of the schedule.
Start Time	Specify the starting time of the schedule.
Duration Time	Specify the duration (or period) for the schedule.
End Time	Specify the ending time of the schedule.
Action	Specify which action should apply the schedule.

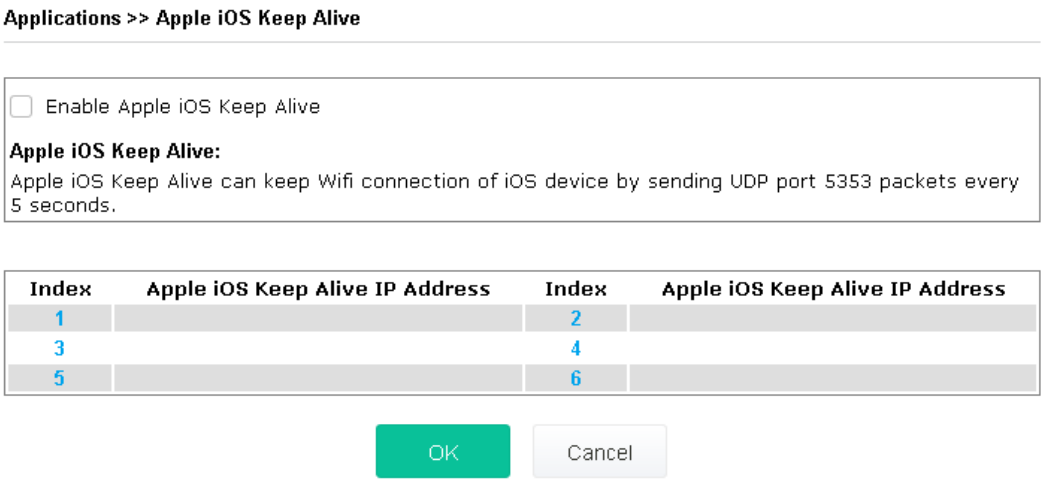
	 In which, you have to specify the device object/device group profile for blocking certain wireless clients when Internet Pause is selected as the Action.
WiFi(2.4GHz)/ WiFi(5GHz)	When **Wi-Fi UP** or **Wi-Fi DOWN** is selected as **Action**, you can check the Radio or SSID 2~4 boxes (2.4GHz and 5GHz respectively) to setup the network based on the schedule profile. **Note**: When Radio is selected, SSID2, SSID3 and SSID4 are not available for choosing, vice versa. Moreover, SSID2, SSID3, and SSID4 are not available for choosing if they are not enabled.
How Often	Specify how often the schedule will be applied. **Once** - The schedule will be applied just once **Weekdays** - Specify which days in one week should perform the schedule.
Weekday	Choose and check the day to perform the schedule. It is available when **Weekdays** is selected as **How Often**.

3. After finishing this web page configuration, please click **OK** to save the settings. A new schedule profile has been created and displayed on the screen.



IV-2-2 Apple iOS Keep Alive

To keep the wireless connection (via Wi-Fi) on iOS device in alive, VigorAP 920R will send the UDP packets with 5353 port to the specific IP every five seconds.



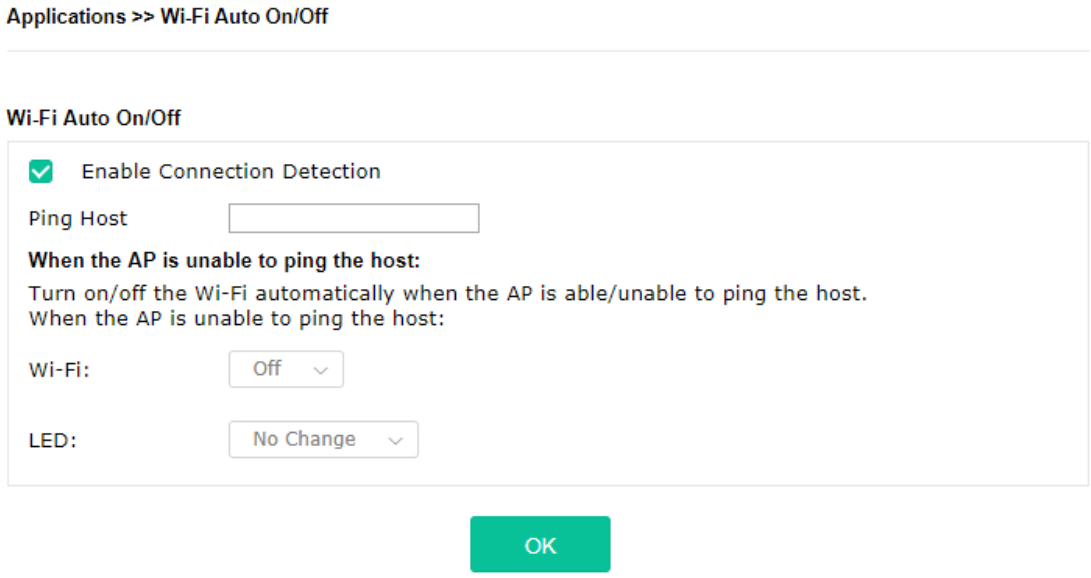
Available settings are explained as follows:

Item	Description
Enable Apple iOS Keep Alive	Check to enable the function.
Index	Display the setting link. Click the index link to open the configuration page for setting the IP address.
Apple iOS Keep Alive IP Address	Display the IP address.

Click **OK** to save the settings.

IV-2-3 Wi-Fi Auto On/Off

When VigorAP is able or unable to ping the specified host, the Wi-Fi function will be turned on or off automatically. The purpose of such function is to avoid wireless station roaming to an AP which is unable to access Internet.



Available settings are explained as follows:

Item	Description
Enable Auto Switch On/Off Wi-Fi	Check the box to enable such function.
Ping Host	Type an IP address (e.g., 8.8.8.8) or a domain name (e.g., google.com) for testing if the access point is stable or not.
When the AP is unable to ping the host	
Wi-Fi	**Off** - When the AP is unable to ping the host, the Wi-Fi connection will be turned off. **No Change** - When the AP is unable to ping the host, the Wi-Fi connection will be on still.
LED	**Off** - When the AP is unable to ping the host, the LED indicator will be turned off. **No Change** - When the AP is unable to ping the host, the LED indicator will not be turned off.

Click **OK** to save the settings.

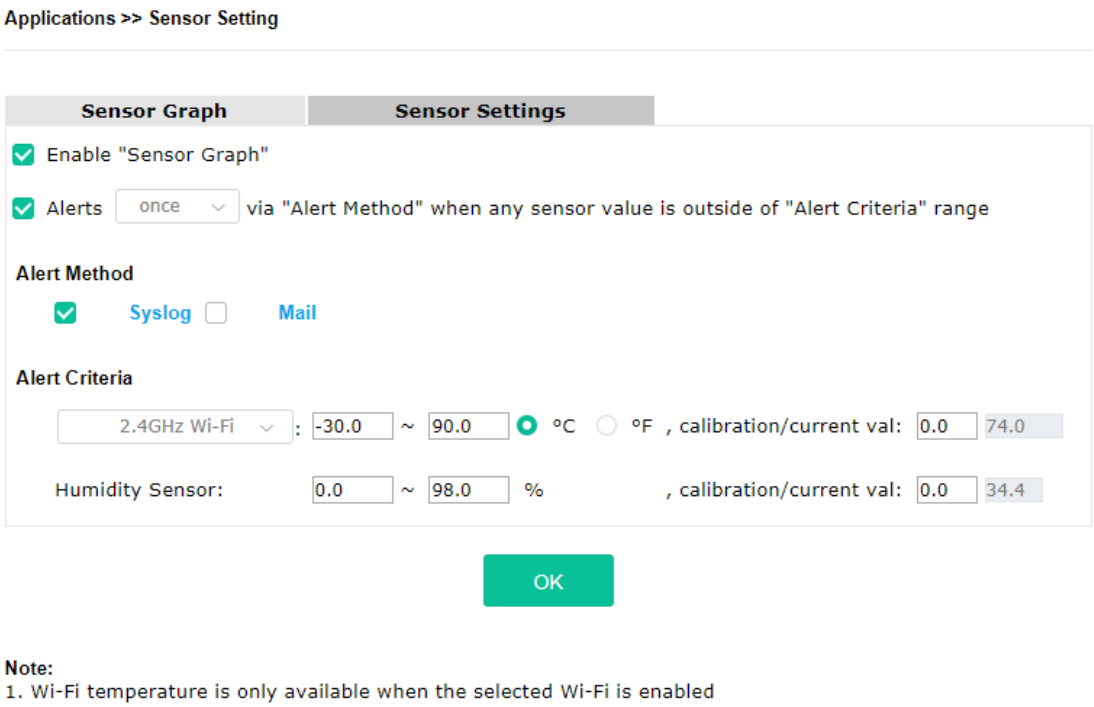
IV-2-4 Sensor

A USB Thermometer is now available that complements your installed DrayTek AP installations that will help you monitor the server or data communications room environment and notify you if the server room or data communications room is overheating.

During summer in particular, it is important to ensure that your server or data communications equipment are not overheating due to cooling system failures.

The inclusion of a USB thermometer in compatible VigorAP will continuously monitor the temperature of its environment. When a pre-determined threshold is reached you will be alerted via Syslog.

Sensor Settings



Note:
1. Wi-Fi temperature is only available when the selected Wi-Fi is enabled

Available settings are explained as follows:

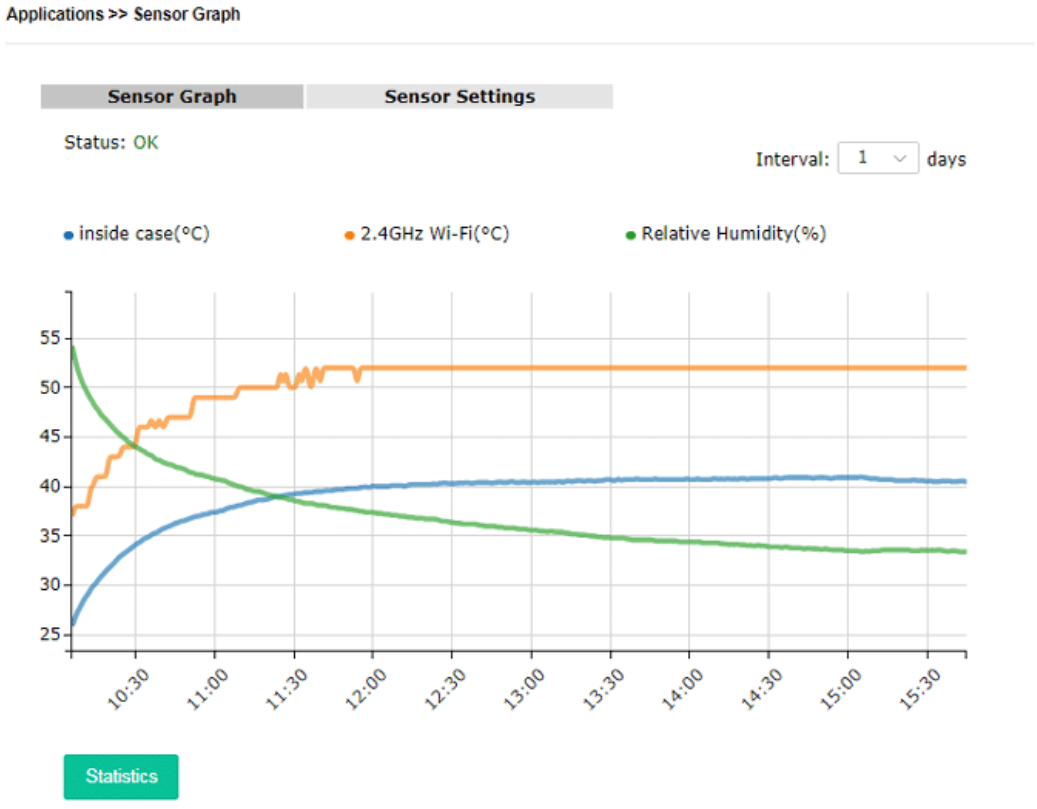
Item	Description
Enable Sensor Graph	To display a graph for the connected sensor, check the box.

Alerts once/per min via	It can determine the time/interval to send an alert message. **Once** – An alert will be sent out once when the sensor value is outside the range defined in Alert Criteria. **Per min.** – Alert message will be sent out per minute when the sensor value is outside the range defined in Alert Criteria.
Alert Method	**Syslog** - The log containing the alarm message will be recorded on Syslog if it is enabled. **Mail** - The log containing the alarm message will be sent by mail.
Alert Criteria	Alert message will be sent out according to the rules specified in this field. **Inside case –** The temperature reading is obtained just from the data recorded inside the chip of VigorAP. **2.4GHz Wi-Fi –** The temperature reading for 2.4G Wi-Fi network operation is estimated by using 2.4GHz CPU Wi-Fi module. The built-in sensor of VigorAP contains temperature sensor and humidity sensor. Please type the upper limit and lower limit for VigorAP system to send out temperature alert / humidity alert. **Calibration / current val-** Type values used for correcting the temperature error and humidity error. **C°/F° -** Choose the display unit of the temperature. There are two types for you to choose.

Sensor Graph

Below shows an example of temperature graph.

Click the circles (blue, orange, and green) on the screen to display / close the wave charts related to “inside case”, “2.4GHz Wi-Fi”, and “Relative Humidity”.



Chapter V Mobile APP, DrayTek Wireless

V-1 Introduction of DrayTek Wireless

VigorAP AP20R supports Android/iOS APP : DrayTek Wireless. The mobile user can find the APP through Apple Store / Android APP.

After downloading the APP, a mobile user is able to access and login the configuration page of VigorAP. It can be used to set up or check status of VigorAP device in different Operation Mode.

- To access into the VigorAP configured previously, please refer to ***V-2 Select a VigorAP***
- To access into a new installed VigorAP, please refer to ***V-3 Quick Start Wizard***

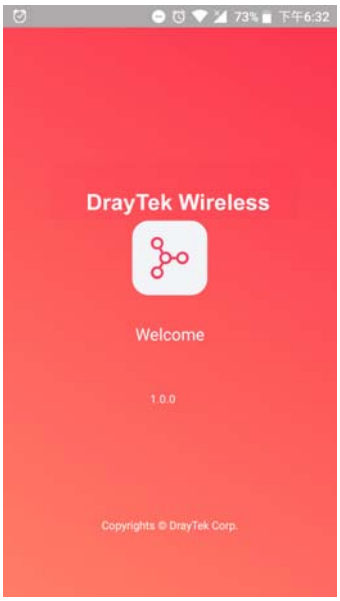
Note:

Before using the DrayTek Wireless APP, please **ENABLE** your Wi-Fi feature first. Then, select the Wi-Fi network with Vigor access point(s) connected physically.

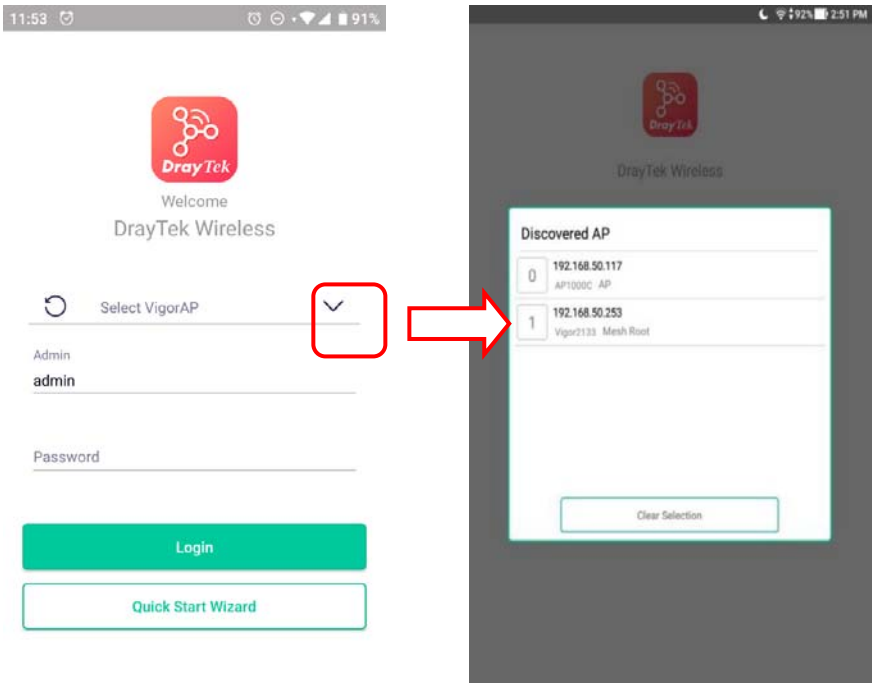
It is not necessary to connect to VigorAP physically. The mobile user must connect to one network with the same subnet as the VigorAP.

V-2 Select a VigorAP

1. Run DrayTek Wireless APP.



2. Choose one AP in the network by clicking the inverted triangle icon to open a drop down list.



Available VigorAP devices with Model Name, IP and Operation mode of VigorAP found by DrayTek Wireless APP will be listed under **Discovered VigorAP**. Choose one of the devices to login (or use Quick Start Wizard function).

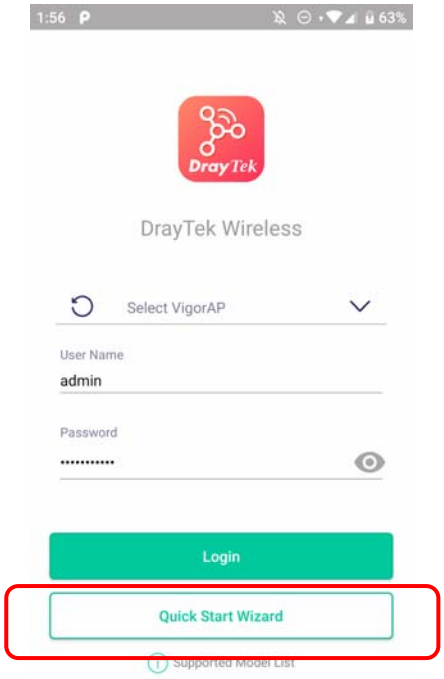
If no AP is found, Quick Start Wizard will start with Wi-Fi connection or start with wizard procedure directly.

V-3 Quick Start Wizard

Quick Start Wizard in Wireless APP is useful for connecting an new installed AP and configuring with different Operation Mode.

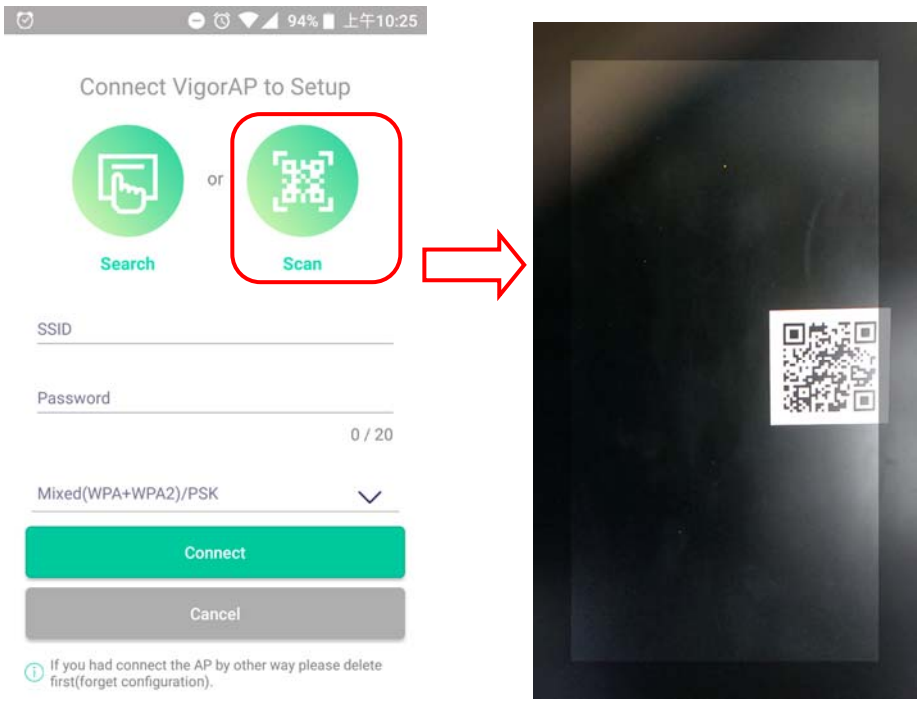
How to create a Mesh Group?

1. Click **Quick Start Wizard**.

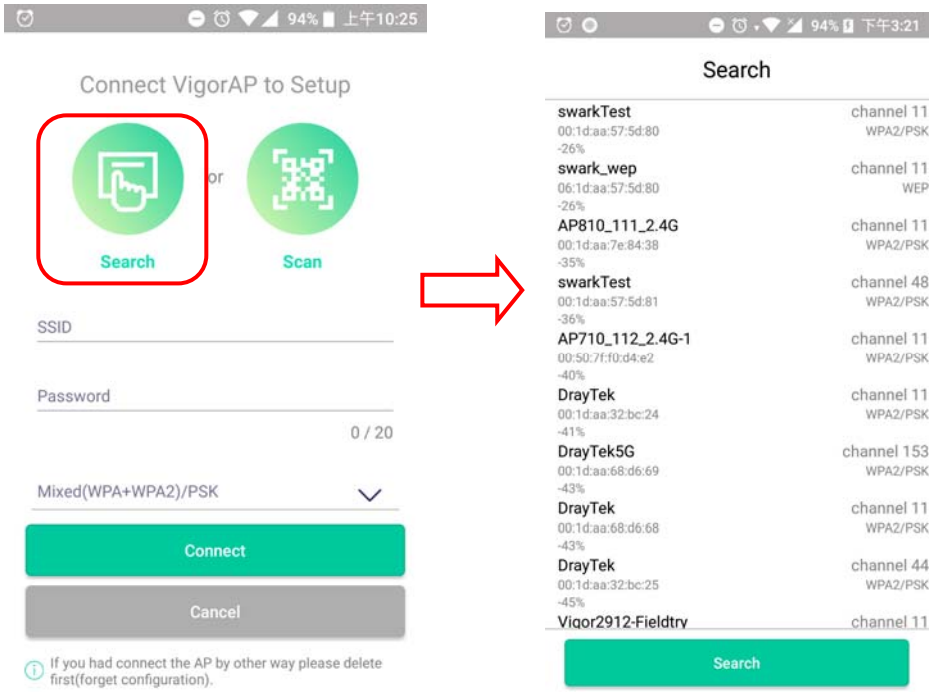


2. Under Quick Start Wizard, there are two methods to locate a mesh root, Search and Scan,

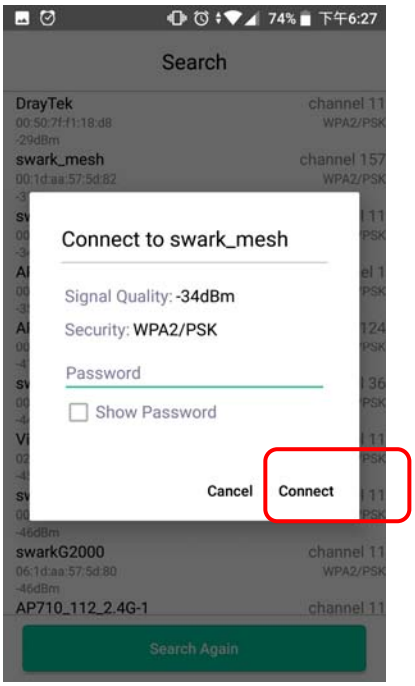
- Click **Scan** to scan the QR code printed on VigorAP packaging box to connect the designated VigorAP.



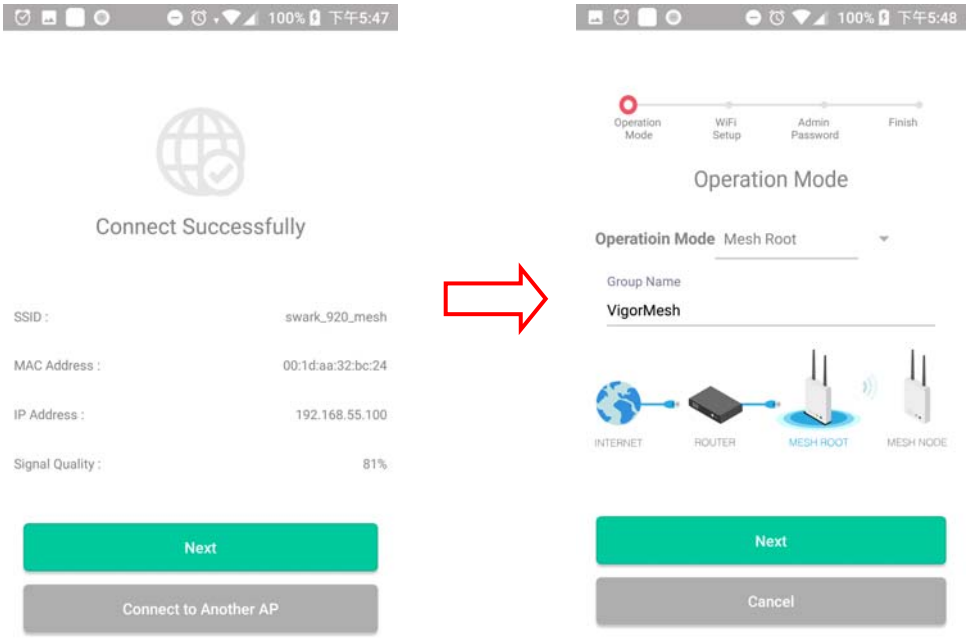
- Or, click **Search**. When the searching result appears, choose one of the AP devices to connect.



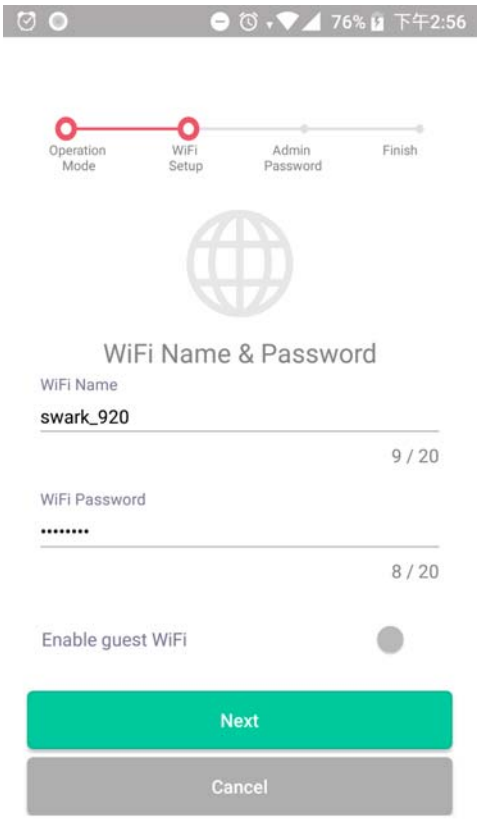
3. When the following page appears, enter the password for the VigorAP device. Then, click **Connect.**



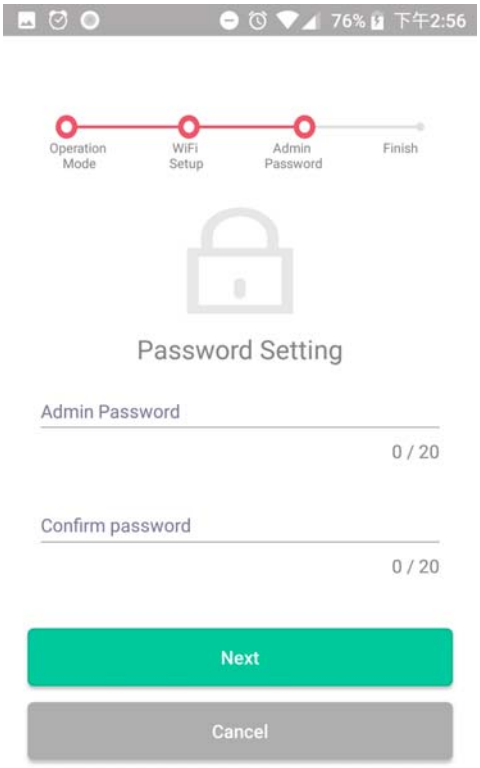
4. When the connection is successful, click **Next**. Then, set Operation Mode of VigorAP as **Mesh Root** and click **Next**.



5. In the following page, set the WiFi Name (SSID) and WiFi Password for your network. You can also enable 2nd SSID by enabling the function of 2nd WiFi. Then, click **Next.**

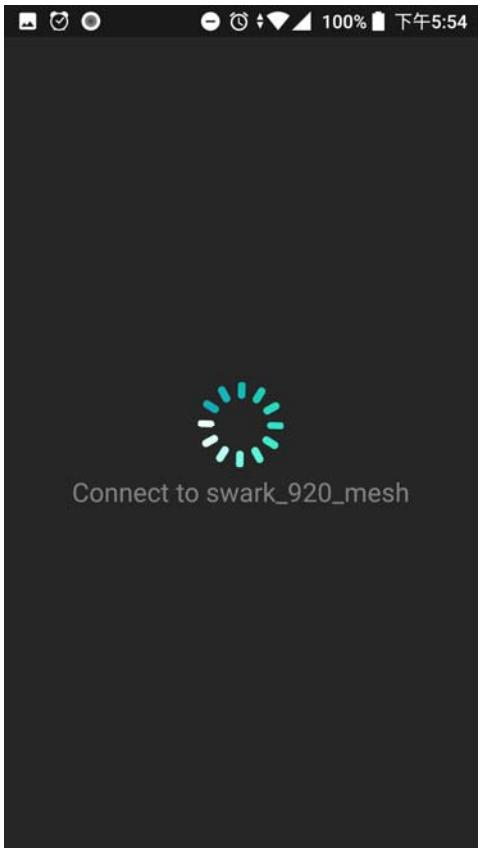


6. Change the default admin password for the network security and click **Next**.

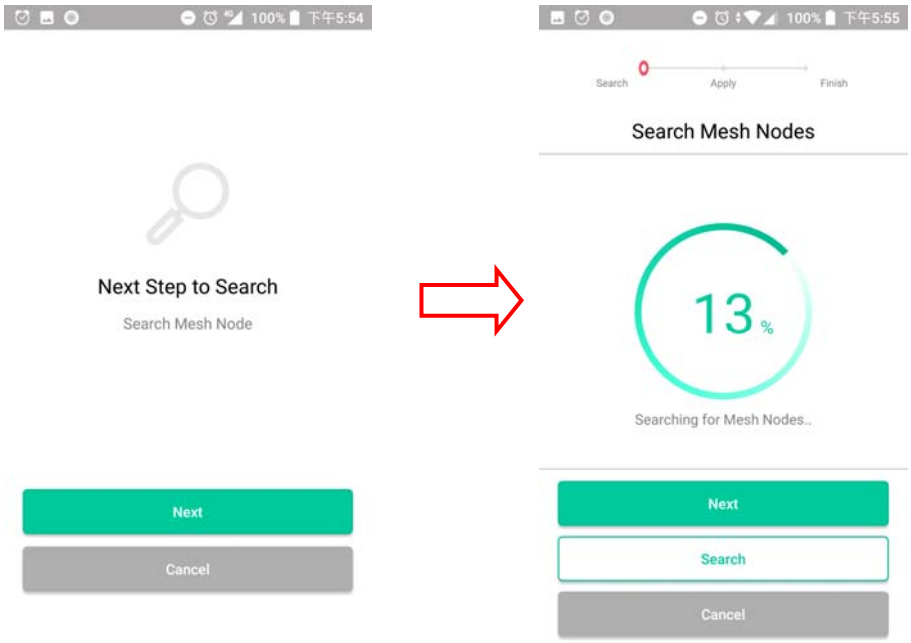


7. In the page of **Check and Apply**, click **Finish** to apply the settings to the specified VigorAP.

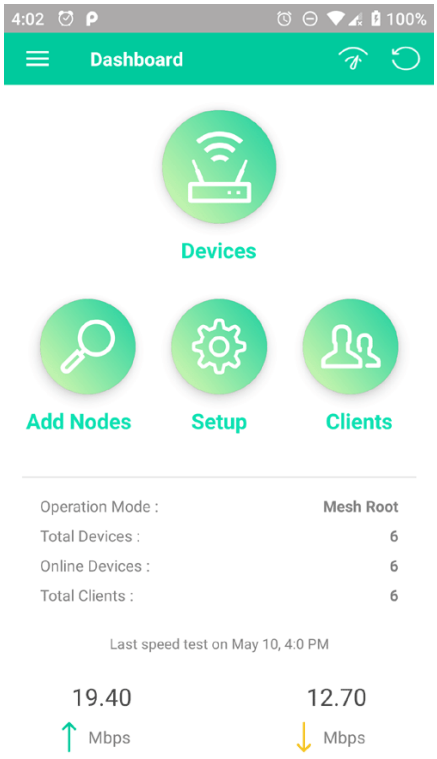
8. After sending configuration to VigorAP, it will take some time to take effect. DrayTek Wireless APP will try to reconnect to wireless network again. Please wait for a while here.



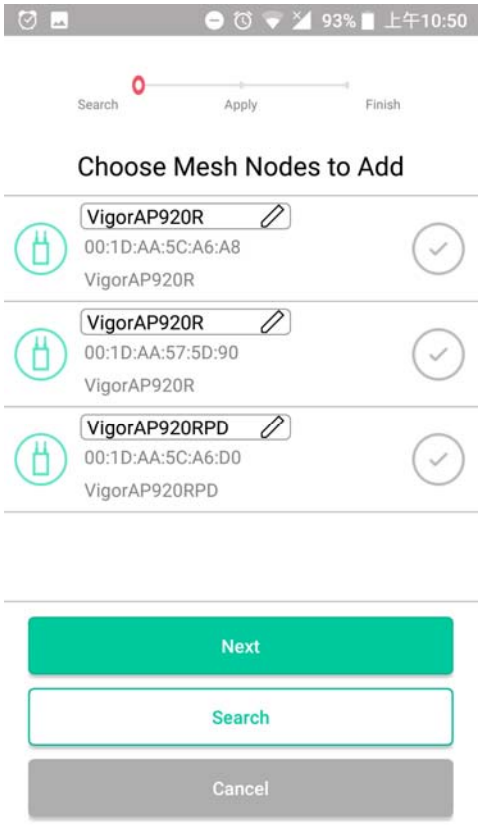
9. Now, the VigorAP has been set as Mesh Root. You can search several Mesh Nodes which do not belong to any other mesh group by clicking **Next**.



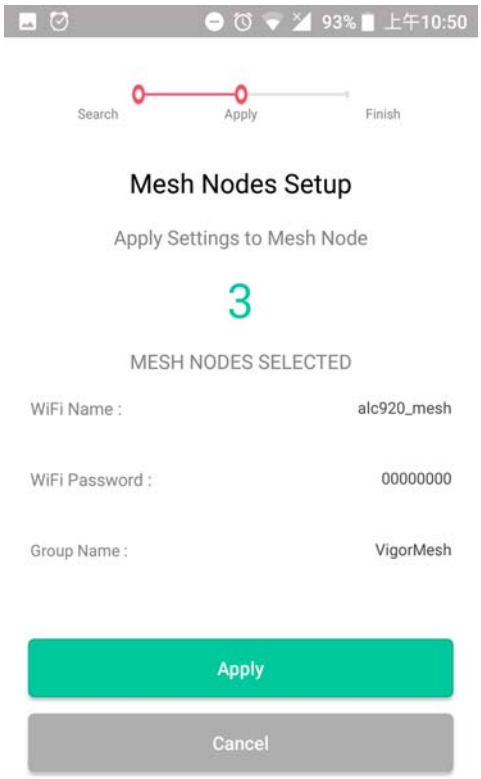
Or, click **Cancel** to return to the home page. Then, click **Add Nodes** to search several Mesh Nodes which do not belong to any other mesh group.



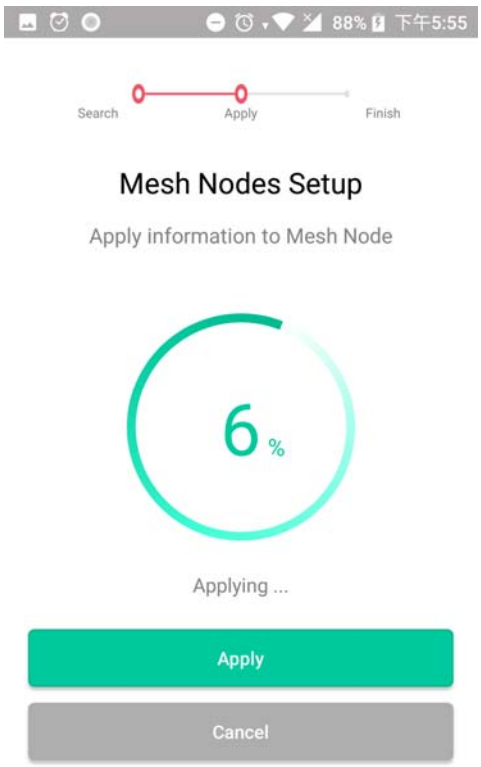
10. Later, available VigorAP devices will be shown on the page. Choose the Mesh Node you want to add and give a device name (e.g,, VigorAP920R) for it. The selected mash node(s) will be grouped under such mesh root. Click **Next**.



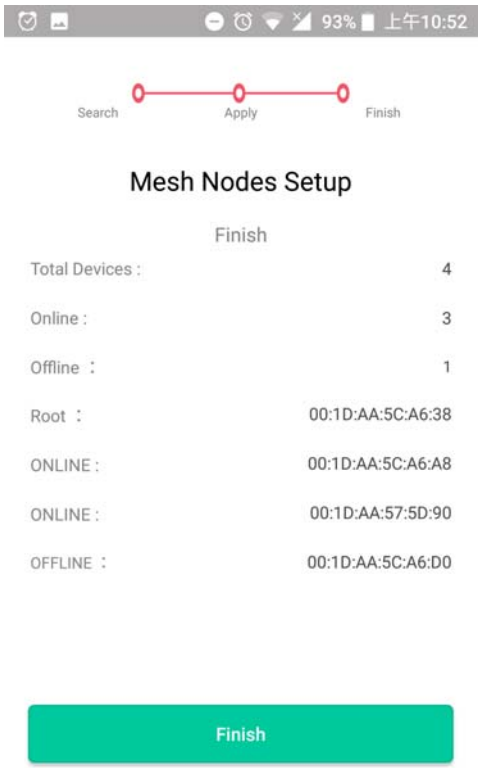
11. The following page displays the total number of mesh nodes selected. Click **Apply**.



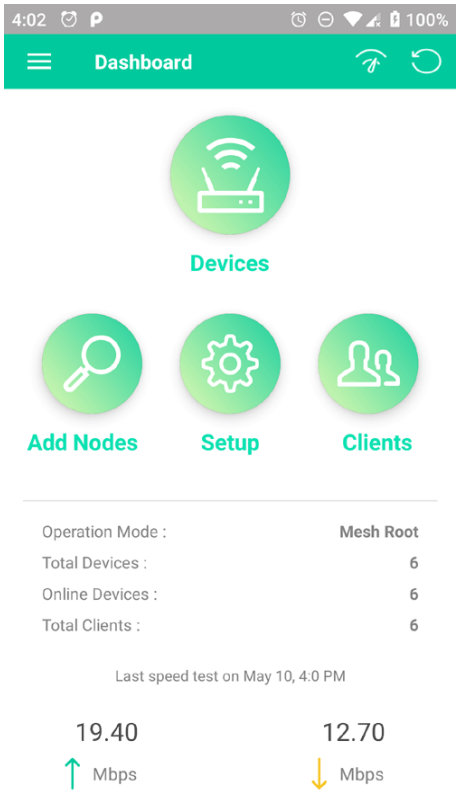
12. Wait until the mesh root applies general configuration to the mesh nodes.



13. Later, current status of the mesh node(s) will be shown on the following page. Click **Finish**.

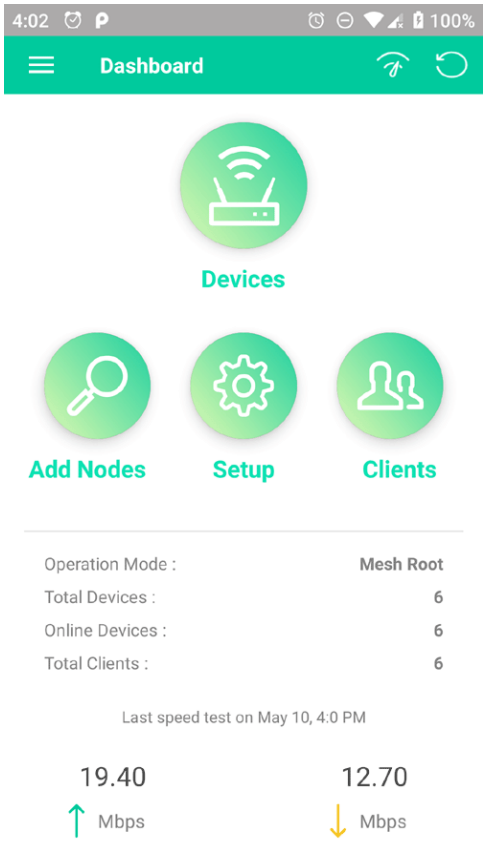
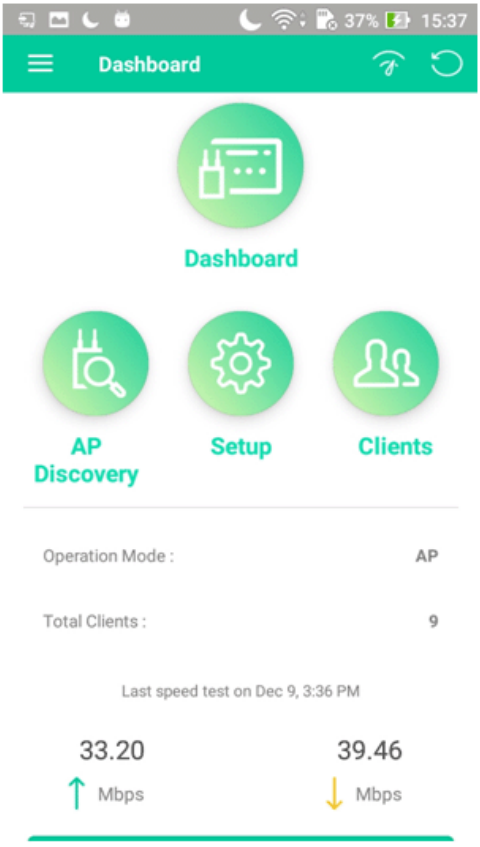


14. Now, the main page of VigorAP APP will be displayed as follows.



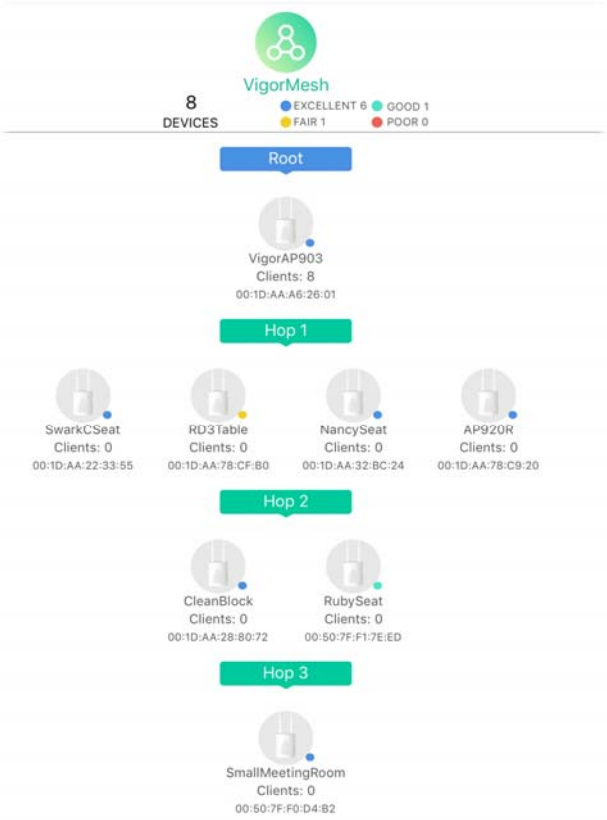
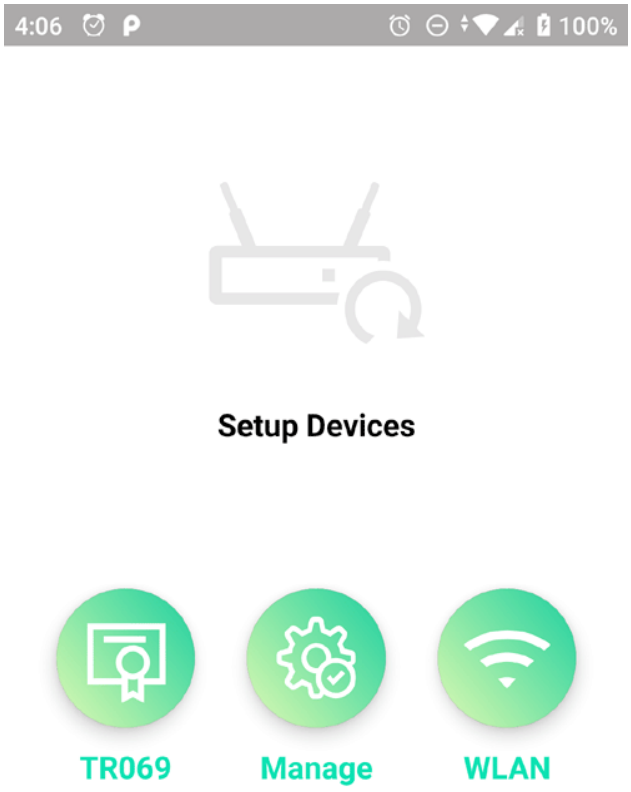
V-4 Login

The main page of VigorAP APP will be different slightly according to the operation mode of VigorAP.

After login to one AP with **Mesh Root**, the major information will be shown as follows:	After login to one AP with **AP mode**, the major information will be shown as follows:
	

Available settings are explained as follows:

Item	Description
Devices / Dashboard	**Dashboard -** The dashboard is designed with Responsive Web Design. You can click **Dashboard** to connect to the selected VigorAP WUI. **Devices –** All of the devices (mesh root and mesh nodes) controlled by the mesh group will be shown on this page with hop number. One mesh group contains up to eight devices.

	
Add Nodes / AP Discovery	**Add Nodes –** Click it to add a new mesh node to this mesh group. **AP Discovery** – Click it to search another access point.
Setup	Click it to configure TR-069, Manage and WLAN settings for the connected VigorAP. 

Clients	Displays general information for all clients in Mesh Group or all clients connected to the selected AP (non-mesh device).
Operation Mode	Display the operation mode (e.g., Mesh Root, AP, Mesh Node) of this AP.
Total Devices	Display the number of the total devices grouped under this mesh group.
Online Devices	Display current online devices grouped under this mesh group.
Total Clients	Display the number of the total clients connected to the mesh group or the selected AP (non-mesh device).
(Speed test)	Click it to make a speed test for the mesh group / AP.
Logout	Exit this APP.

This page is left blank.

Chapter VI Troubleshooting

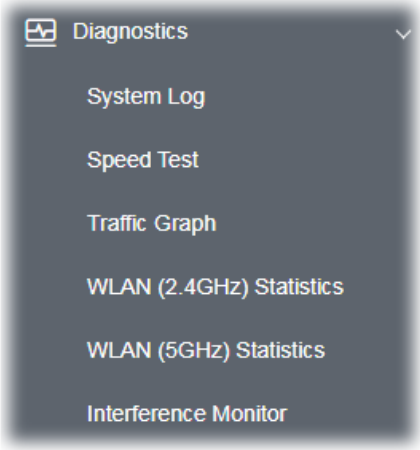
VI-1 Diagnostics

This section will guide you to solve abnormal situations if you cannot access into the Internet after installing the router and finishing the web configuration. Please follow sections below to check your basic installation status stage by stage.

- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

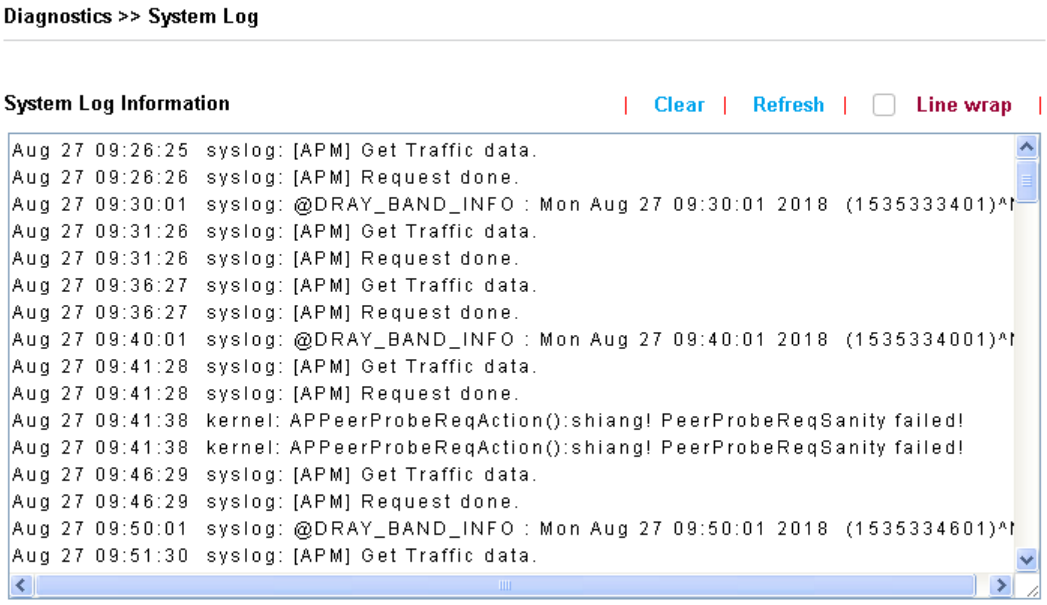
If all above stages are done and the router still cannot run normally, it is the time for you to contact your dealer or DrayTek technical support for advanced help.

Diagnostic tools provide a useful way to **view** or **diagnose** the status of your VigorAP 920R series.



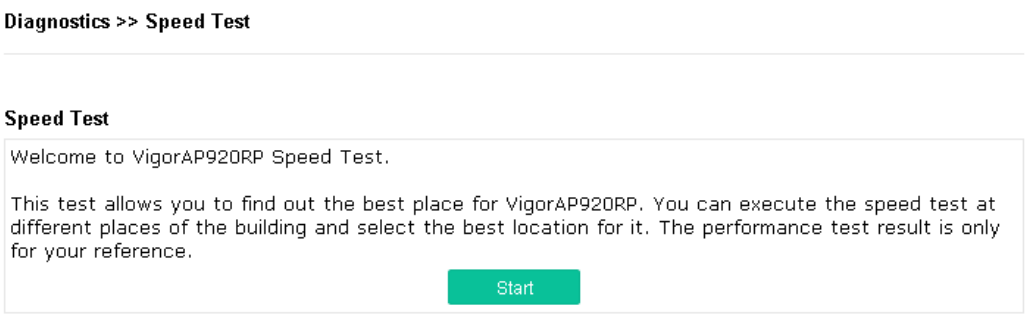
VI-1-1 System Log

At present, only **System Log** is offered.



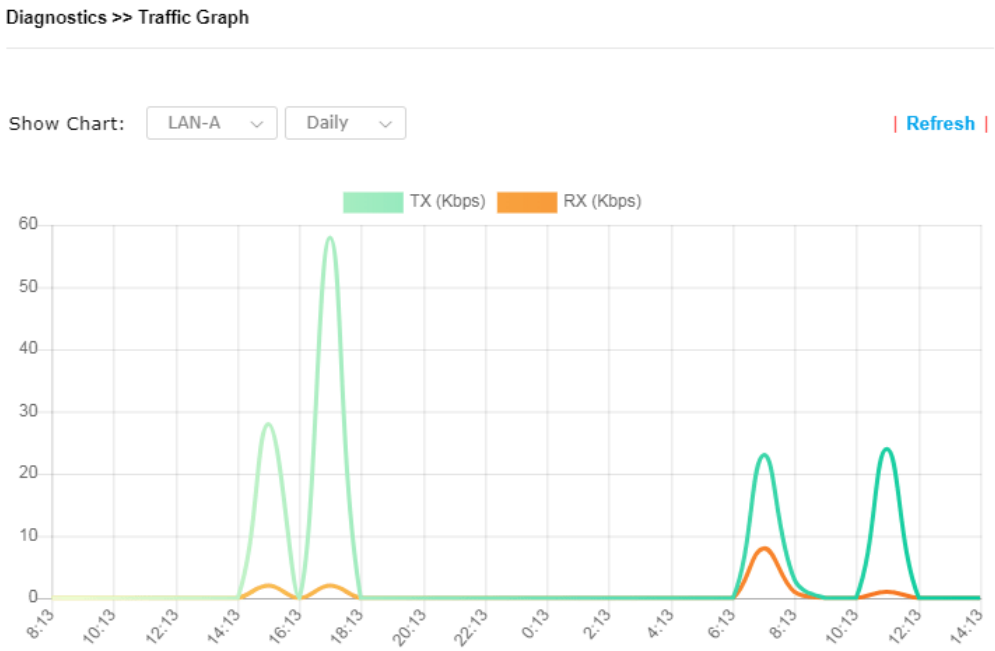
VI-1-2 Speed Test

Click the **Start** button on the page to test the speed. Such feature can help you to find the best installation place for Vigor AP.



VI-1-3 Traffic Graph

Click **Traffic Graph** to open the web page. Choose one of the managed Access Points, LAN-A, daily or weekly for viewing data transmission chart. Click **Refresh** to renew the graph at any time.



The horizontal axis represents time; the vertical axis represents the transmission rate (in Kbps).

VI-1-4 WLAN (2.4GHz) Statistics

Such page is used for debug by RD only.

Diagnostics >> WLAN (2.4GHz) Statistics

Auto-Refresh | Refresh

Tx Data Packets	0	Rx Data Packets	0
Tx Data Bytes	0	Rx Data Bytes	0
Average Tx Rate (kbps)	No Station	Average Rx Rate (kbps)	No Station
Tx Unicast Data Packets	0	Rx PHY errors	0
Tx Multi/Broadcast Data Packets	0	Rx CRC errors	1799
Tx failures	0	Rx MIC errors	0
		Rx Decryption errors	0
		Rx errors	0

	SSID1 (DrayTek-5CA658)	SSID2 (N/A)	SSID3 (N/A)	SSID4 (N/A)
Tx Data Packets	0	N/A	N/A	N/A
Tx Data Bytes	0	N/A	N/A	N/A
Tx Data BytesTx Data Payload Bytes	0	N/A	N/A	N/A
Rx Data Packets	0	N/A	N/A	N/A
Rx Data Bytes	0	N/A	N/A	N/A
Rx Data Payload Bytes	0	N/A	N/A	N/A
Tx Unicast Data Packets	0	N/A	N/A	N/A
Tx Multi/Broadcast Data Packets	0	N/A	N/A	N/A
Average Tx Rate (kbps)	No Station	N/A	N/A	N/A
Average Rx Rate (kbps)	No Station	N/A	N/A	N/A
Rx errors	0	N/A	N/A	N/A
Tx failures	0	N/A	N/A	N/A

VI-1-5 WLAN (5GHz) Statistics

Such page is used for debug by RD only.

Diagnostics >> WLAN (5GHz) Statistics

Auto-Refresh | Refresh

Tx Data Packets	0	Rx Data Packets	0
Tx Data Bytes	0	Rx Data Bytes	0
Average Tx Rate (kbps)	No Station	Average Rx Rate (kbps)	No Station
Tx Unicast Data Packets	0	Rx PHY errors	0
Tx Multi/Broadcast Data Packets	0	Rx CRC errors	21860
Tx failures	0	Rx MIC errors	0
		Rx Decryption errors	0
		Rx errors	0

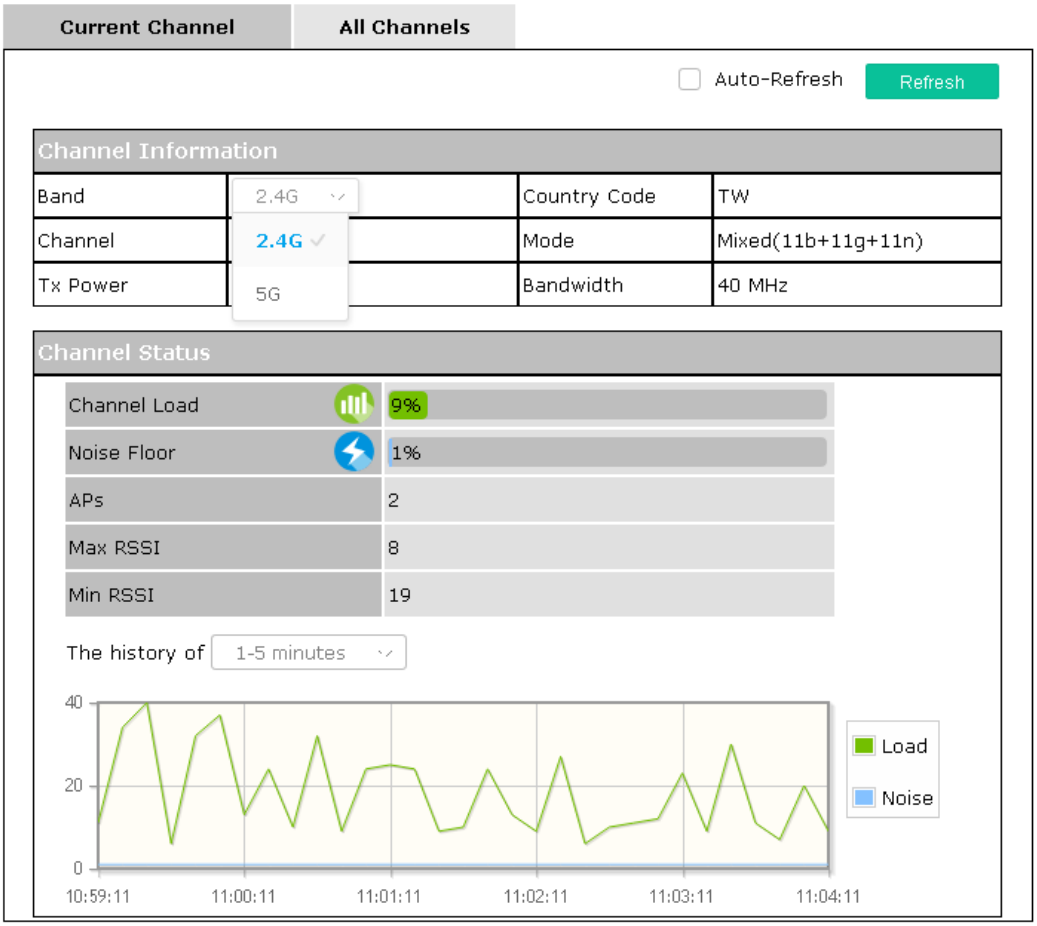
	SSID1 (DrayTek-5CA658)	SSID2 (N/A)	SSID3 (N/A)	SSID4 (N/A)
Tx Data Packets	0	N/A	N/A	N/A
Tx Data Bytes	0	N/A	N/A	N/A
Tx Data BytesTx Data Payload Bytes	0	N/A	N/A	N/A
Rx Data Packets	0	N/A	N/A	N/A
Rx Data Bytes	0	N/A	N/A	N/A
Rx Data Payload Bytes	0	N/A	N/A	N/A
Tx Unicast Data Packets	0	N/A	N/A	N/A
Tx Multi/Broadcast Data Packets	0	N/A	N/A	N/A
Average Tx Rate (kbps)	No Station	N/A	N/A	N/A
Average Rx Rate (kbps)	No Station	N/A	N/A	N/A
Rx errors	0	N/A	N/A	N/A
Tx failures	0	N/A	N/A	N/A

VI-1-6 Interference Monitor

As an interference detector, VigorAP can detect all of the environmental interference factors for certain channel used or for all of the wireless channels.

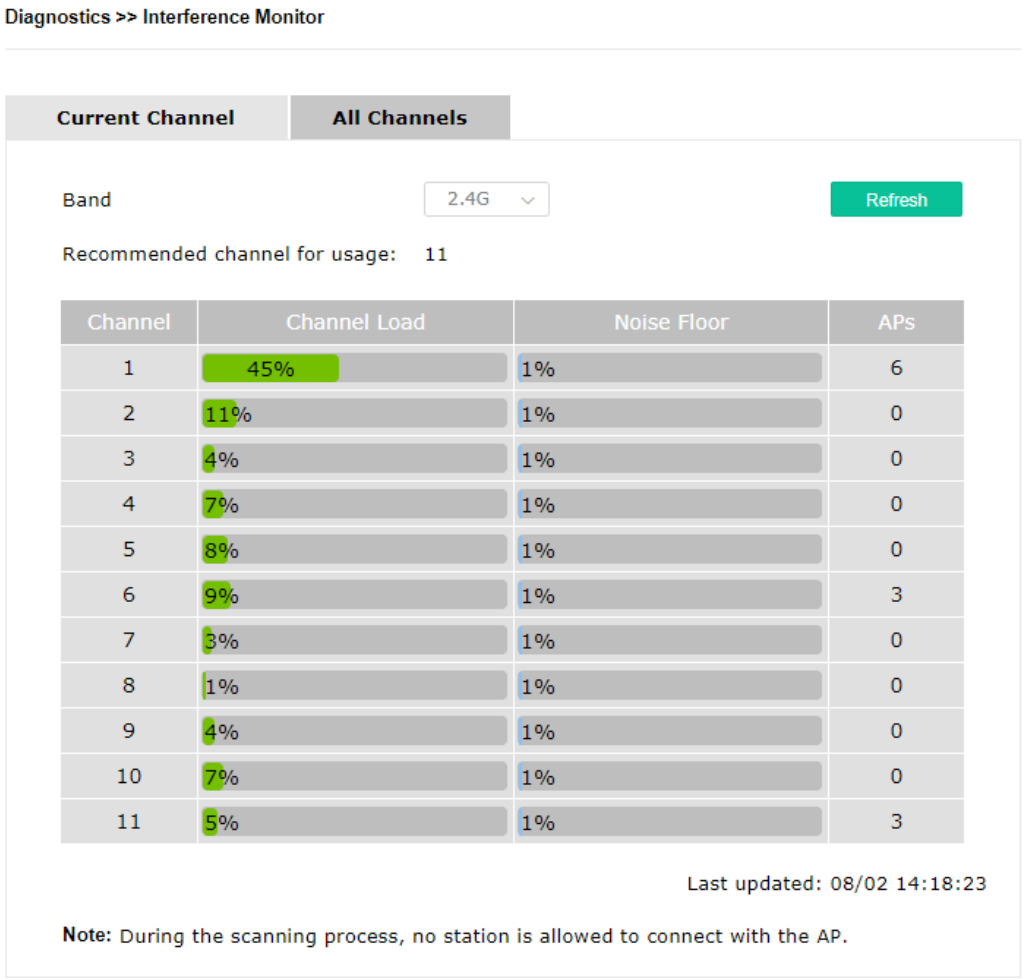
Current Channel

The analysis page with information about wireless band, channel, transmission power, bandwidth, wireless mode, and country code chosen will be displayed on this page completely based on the wireless band (2.4G or 5G) selected. Also, channel status can be seen easily from this page.



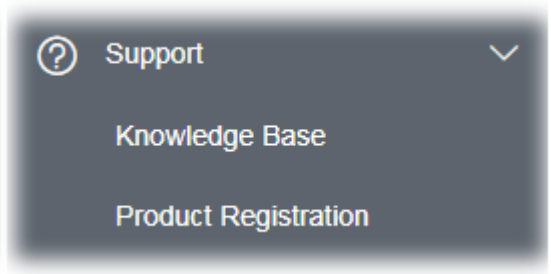
All Channels

This page displays the utilization and energy result for all channels based on 2.4G/5G. Click **Refresh** to get the newly update interference situation.



VI-1-7 Support Area

When you click **Support Area**, you will be guided to visit www.draytek.com and open the corresponding pages directly.



VI-2 Checking the Hardware Status

Follow the steps below to verify the hardware status.

1. Check the power line and cable connections.

   Refer to “**I-2 Mounting the Access Point”** for details.

2. Power on the modem. Make sure the **ACT** LED and **LAN** LED are bright.

3. If not, it means that there is something wrong with the hardware status. Simply back to **“I-2 Mounting the Access Point”** to execute the hardware installation again. And then, try again.

VI-3 Checking the Network Connection Settings

Sometimes the link failure occurs due to the wrong network connection settings. After trying the above section, if the link is stilled failed, please do the steps listed below to make sure the network connection settings is OK.

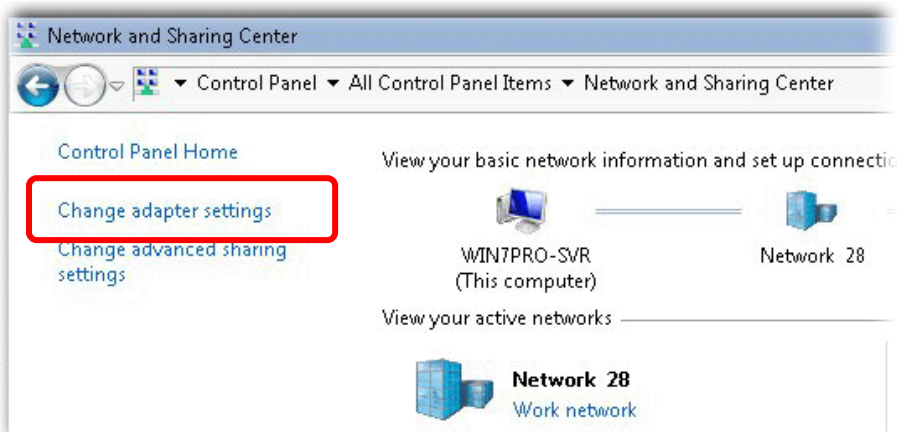
VI-3-1 For Windows

Note:

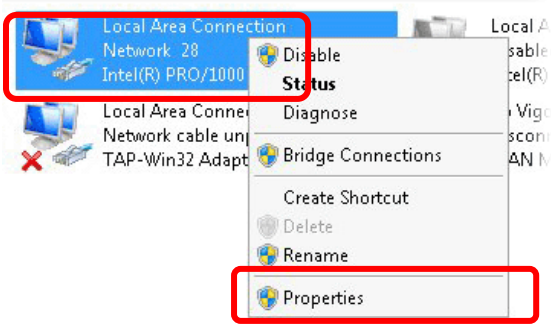
The example is based on Windows 7 (Professional Edition). As to the examples for other operation systems, please refer to the similar steps or find support notes in **www.draytek.com**.

1. Open **All Programs>>Getting Started>>Control Panel.** Click **Network and Sharing Center.**

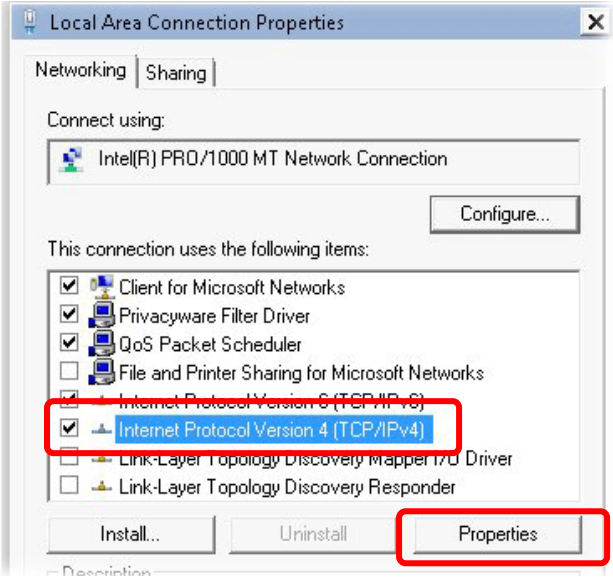
2. In the following window, click **Change adapter settings**.



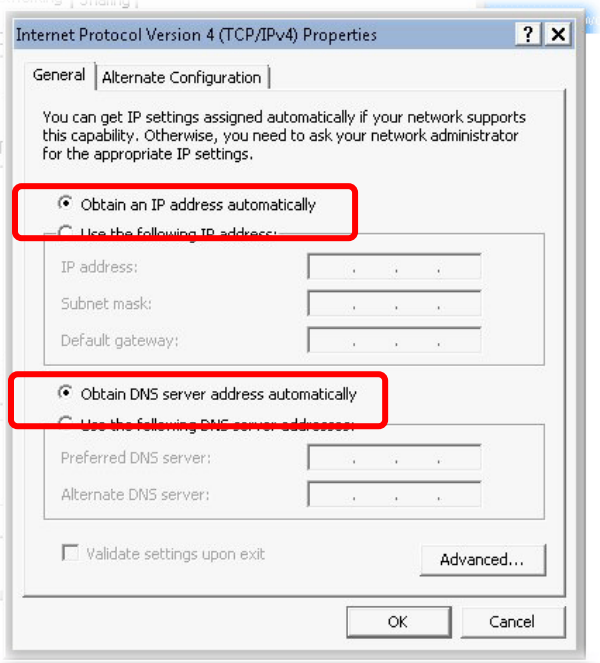
3. Icons of network connection will be shown on the window. Right-click on **Local Area Connection** and click on **Properties**.



4. Select **Internet Protocol Version 4 (TCP/IP)** and then click **Properties**.

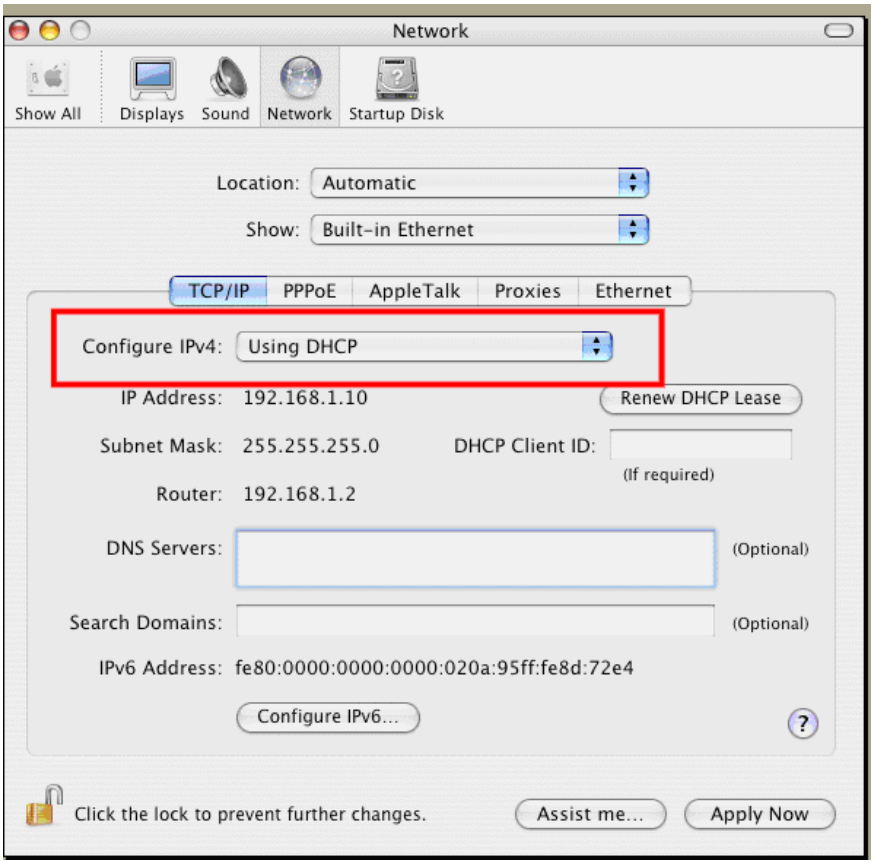


5. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Finally, click **OK**.



VI-3-2 For Mac Os

1. Double click on the current used Mac Os on the desktop.
2. Open the **Application** folder and get into **Network**.
3. On the **Network** screen, select **Using DHCP** from the drop down list of Configure IPv4.



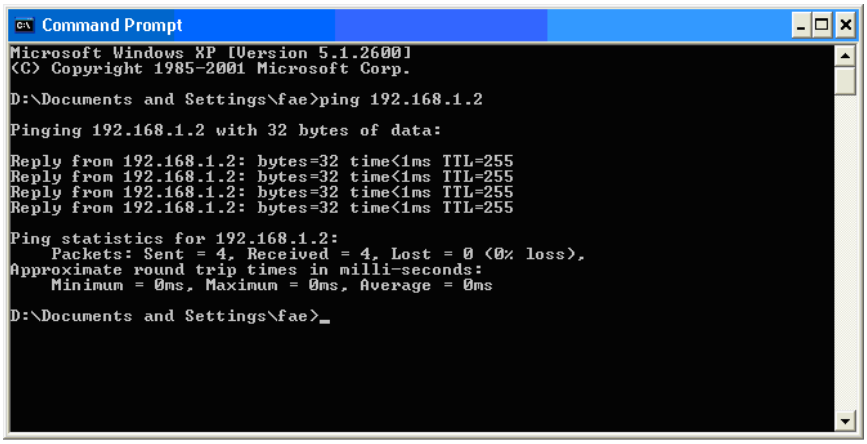
IV-4 Pinging the Device

The default gateway IP address of the modem is 192.168.1.2. For some reason, you might need to use “ping” command to check the link status of the modem. **The most important thing is that the computer will receive a reply from 192.168.1.2.** If not, please check the IP address of your computer. We suggest you setting the network connection as **get IP automatically**. (Please refer to the section V-2)

Please follow the steps below to ping the modem correctly.

VI-4-1 For Windows

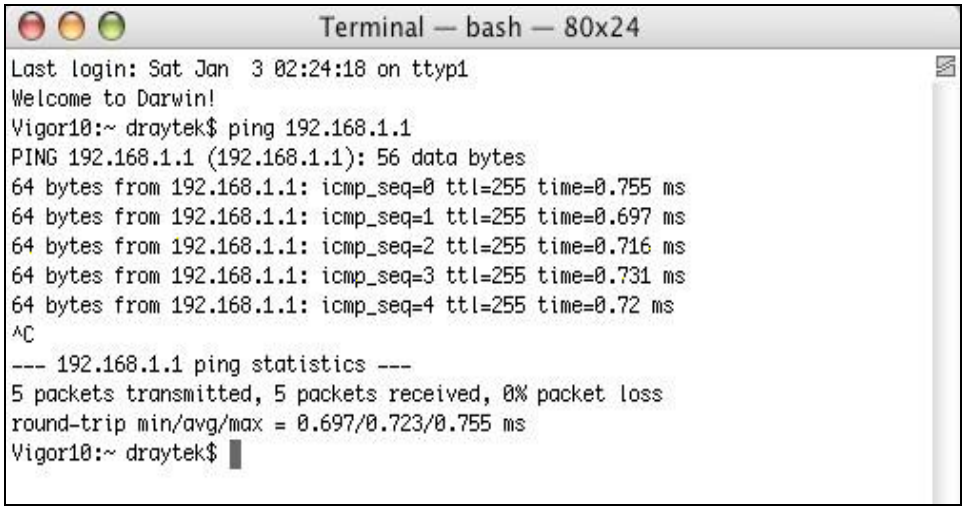
1. Open the **Command** Prompt window (from **Start menu> Run**).
2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/2000/XP/Vista/7). The DOS command dialog will appear.



3. Type ping 192.168.1.2 and press [Enter]. If the link is OK, the line of **“Reply from 192.168.1.2:bytes=32 time<1ms TTL=255”** will appear.
4. If the line does not appear, please check the IP address setting of your computer.

VI-4-2 For Mac Os (Terminal)

1. Double click on the current used Mac Os on the desktop.
2. Open the **Application** folder and get into **Utilities**.
3. Double click **Terminal**. The Terminal window will appear.
4. Type **ping 192.168.1.2** and press [Enter]. If the link is OK, the line of **“64 bytes from 192.168.1.2: icmp_seq=0 ttl=255 time=xxxx ms**” will appear.


Terminal — bash — 80x24
Last login: Sat Jan 3 02:24:18 on ttyp1
Welcome to Darwin!
Vigor10:~ draytek$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.697/0.723/0.755 ms
Vigor10:~ draytek$

VI-5 Backing to Factory Default Setting

Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the modem by software or hardware.

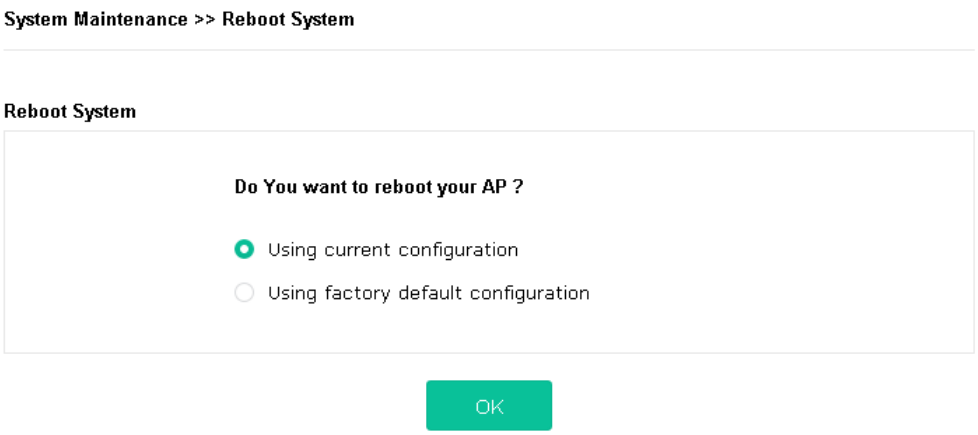
Warning:

After pressing **factory default setting**, you will loose all settings you did before. Make sure you have recorded all useful settings before you pressing. The password of factory default is null.

VI-5-1 Software Reset

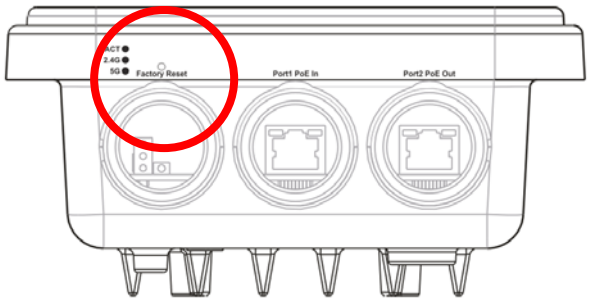
You can reset the modem to factory default via Web page.

Go to **System Maintenance** and choose **Reboot System** on the web page. The following screen will appear. Choose **Using factory default configuration** and click **OK**. After few seconds, the modem will return all the settings to the factory settings.



VI-5-2 Hardware Reset

While the modem is running, press the **Factory Reset** button and hold for more than 5 seconds. When you see the **ACT** LED blinks rapidly, please release the button. Then, the modem will restart with the default configuration.



After restore the factory default setting, you can configure the settings for the modem again to fit your personal request.

VI-6 Contacting DrayTek

If the modem still cannot work correctly after trying many efforts, please contact your dealer for further help right away. For any questions, please feel free to send e-mail to support@draytek.com.

Index

8

802.11n, 40

802.1x, 43

A

Access Control, 45

Action, 123

Advanced Setting, 47

AES, 31

Airtime Fairness, 52

Antenna, 48

AP Discovery, 50

AP Management, 103

AP Mode, 38, 69, 78

AP Operation Mode, 21

APM Log, 104

Apple iOS Keep Alive, 125

Applications, 122

Auth Mode, 46

Authentication Client, 119

Authentication Type, 119

Auto Adjustment, 52

Auto Channel Filtered Out List, 48

Auto Logout, 17

Auto Provision, 103

AutoSelect, 79

B

Backup, 119

Band Steering, 58

Bandwidth Limit, 22, 25, 30

Bandwidth Management, 51

Black List, 105

C

Central AP Management, 103

Certificate Management, 119

Changing Password, 18

Channel, 40, 79

Channel Width, 47

Client IP, 119

Client PinCode, 47

Client's MAC Address, 105

Configuration Backup, 93, 94

Connection Time, 55

Connection Type, 80

Country Code, 48

D

Daylight Saving, 97

Default Gateway, 80

Detection, 107, 113, 114

DHCP Client, 82

DHCP server, 15

Download Limit, 51

E

EAP Type, 119

Encryp Type, 46

End Time, 123

Extension Channel, 40

F

Factory Default Setting, 159

Fast Roaming, 57

Firmware Upgrade, 102

Force Overload Disassociation, 105

Fragment Length, 48

G

General Setup, LAN, 81

H

Hardware Installation, 3

Hardware Reset, 159

Hide SSID, 40

HTMIX, 40

HTTP port, 99

HTTPS, 121

HTTPS port, 99

I

Interference Monitor, 151
IP Address, 80, 82
Isolate Member, 40

K

Keep Alive Period, 91
Key Renewal Interval, 43
Key Size, 121
Key Type, 120

L

LAN, 81
LAN port, 86
Lease Time, 82
LED Indicators and Connectors, 2
Limit Client, 39
Limit Client per SSID, 40
Load Balance, 105

M

MAC Address, 79
MAC Address Filter, 45
MAC Clone, 48
Main SSID, 21, 24, 29
Management, 99
Management VLAN, 82
Mobile Device Management, 107
Mode, 40, 42

N

NTP, 122
NTP Client, 97
NTP Server, 97
NTP synchronization, 98

O

Once, 124
Open/Shared, 31, 80
Operation Mode, 34
Overload Management, 105

P

Pass Phrase, 43, 80
Password, 18
Password Strength, 92, 93
Periodic Inform Settings, 91
PIN Code, 36
PMK Cache Period, 57
PoE Connection, 9
Policy, 45, 115, 116
Port, 44
Port Control, 84, 86
Pre-Authentication, 57
Primary DNS Server, 82
PSK, 35
Push Button, 46

Q

Quick Start Wizard, 20

R

RADIUS Server, 43, 118
RADIUS Setting, 118
Reboot System, 101
Reconnection Time, 55
Relay Agent, 82
Restore, 46, 119
Roaming, 56
Router Name, 80
Routine, 124
RSSI, 56
RTS Threshold, 48

S

Schedule, 122
Secondary DNS Server, 82
Secret Key, 119
Security, 41, 42
Security Mode, 79
Security Overview, 35
Security Settings, 42
Session Timeout, 44
Shared Secret, 44
Show Chart, 113

Software Reset, 159
Speed Test, 147
SSL(HTTPS), 91
Start Date, 123
Start PBC, 36
Start Time, 123
Station Control, 22, 25, 30, 55
Station List, 63
Status of Settings, 106
STUN, 91
Subject Name, 120
Subnet, 40
Subnet Mask, 80, 82
Support Area, 152
Syslog/Mail Alert, 96
System Log, 147
System Maintenance, 88
System Status, 89

T

Temperature Sensor, 126, 127
Temperature Sensor Graph, 128
Time and Date, 97
Time Zone, 97
TKIP, 31, 35
Total Download Limit, 52
Total Upload Limit, 52
TR-069, 90
Traffic Graph, 148
traffic overload, 105
Triggering Client Number, 53
Trust DHCP Server, 82
Tx Power, 48

U

Upload Limit, 51
Users Profile, 119

V

VLAN ID, 40, 82

W

WEP, 31
WEP (Wired Equivalent Privacy), 35
White List, 105
Wi-Fi DOWN, 124
Wi-Fi UP, 124
Wired Connection, 3, 4, 6
Wireless Connection, 8
Wireless LAN (2.4GHz/5GHz), 35
WLAN (2.4GHz) Statistics, 149
WLAN (5GHz) Statistics, 150
WPA (Wi-Fi Protected Access), 35
WPA Algorithms, 43
WPS, 46
WPS (Wi-Fi Protected Setup), 35