DrayTek

# VigorAP 1060C

802.11ax Ceiling-mount AP

# USER'S GUIDE

V1.2

# VigorAP 1060C

11ax Ceiling AP

User's Guide

Version: 1.2

Firmware Version: V1.4.4

Date: December 6, 2021

# 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 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 two (2) years 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 router via https://myvigor.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.

https://www.draytek.com

# Table of Contents


**Chapter I Installation ..... VII**

I-1 Introduction ..... 1

I-1-1 LED Indicators and Connectors ..... 2

I-2 Hardware Installation ..... 3

I-2-1 Ceiling-mount Installation (Wooden Ceiling) ..... 3
I-2-2 Ceiling-mount Installation (Plasterboard Ceiling) ..... 4
I-2-3 Suspended Ceiling (Lightweight Steel Frame) Installation ..... 5
I-2-4 Wall-Mounted Installation ..... 6
I-2-5 Connect to a Vigor Router using AP Management ..... 7

I-3 Network IP Configuration ..... 8

I-3-1 Windows 10 IP Address Setup ..... 8

I-4 Accessing to Web User Interface ..... 11

I-5 Changing Password ..... 14

I-6 Dashboard ..... 15

I-7 Quick Start Wizard ..... 16

I-7-1 Settings for Access Point ..... 17
I-7-2 Settings for Mesh Root ..... 20
I-7-3 Settings for Mesh Node ..... 25
I-7-4 Settings for Range Extender ..... 26

**Chapter II Connectivity ..... 31**

II-1 Operation Mode ..... 32

II-2 General Concepts for Wireless LAN ..... 34

II-3 Wireless LAN (2.4GHz/5GHz) Settings for AP Mode ..... 37

II-3-1 General Setup ..... 38
II-3-2 Security ..... 41
II-3-3 Access Control ..... 44
II-3-4 WPS ..... 46
II-3-5 Advanced Setting ..... 47
II-3-6 AP Discovery ..... 49
II-3-7 WDS AP Status ..... 50
II-3-8 Airtime Fairness ..... 50
II-3-9 Station Control ..... 52
II-3-10 Roaming ..... 54
II-3-11 Band Steering (for Wireless LAN (2.4GHz)) ..... 56
II-3-12 Station List ..... 61

II-4 Mesh Settings for Mesh Mode ..... 67

II-4-1 Mesh Setup ..... 69
II-4-2 Mesh Status ..... 74
II-4-3 Mesh Discovery ..... 76
II-4-4 Basic Configuration Sync ..... 77
II-4-5 Advanced Config Sync ..... 80
II-4-6 Support List ..... 80
II-4-7 Mesh Syslog ..... 81

II-5 Universal Repeater Settings for Range Extender Mode ..... 82

II-6 Monitor Radio ..... 86

II-6-1 Dashboard ..... 86
II-6-2 Monitor Setup ..... 89
II-6-3 Rogue AP White List ..... 91

II-6-4 Monitor Log ..... 92
II-7 LAN ..... 93
II-7-1 General Setup ..... 93
II-7-2 Hotspot Web Portal ..... 96
II-7-3 Port Control ..... 100

**Chapter III Management ..... 101**

III-1 System Maintenance ..... 102
III-1-1 System Status ..... 103
III-1-2 TR-069 ..... 104
III-1-3 Administrator Password ..... 106
III-1-4 User Password ..... 107
III-1-5 Configuration Backup ..... 108
III-1-6 Syslog/Mail Alert ..... 110
III-1-7 Time and Date ..... 111
III-1-8 SNMP ..... 113
III-1-9 Management ..... 114
III-1-10 Reboot System ..... 116
III-1-11 Firmware Upgrade ..... 117
III-2 Central AP Management ..... 118
III-2-1 General Setup ..... 118
III-2-2 APM Log ..... 119
III-2-3 Overload Management ..... 120
III-2-4 Status of Settings ..... 121
III-3 Mobile Device Management ..... 123
III-3-1 Station List ..... 123
III-3-2 Station Statistics ..... 129
III-3-3 Station Nearby ..... 130
III-3-4 Policies ..... 131
III-3-5 Station Control List ..... 132

**Chapter IV Others ..... 133**

IV-1 RADIUS Setting ..... 134
IV-1-1 RADIUS Server ..... 134
IV-1-2 Certificate Management ..... 135
IV-2 Applications ..... 138
IV-2-1 Schedule ..... 138
IV-2-2 Wi-Fi Auto On/Off ..... 141
IV-3 Objects Setting ..... 142
IV-3-1 Device Object ..... 142
IV-3-2 Device Group ..... 144

**Chapter V Mobile APP, DrayTek Wireless ..... 147**

V-1 Introduction of DrayTek Wireless ..... 148
V-2 Create a New Network ..... 149
V-3 Wizard - Mesh Root and Mesh Node ..... 151
V-4 Login ..... 155
V-4-1 Network ..... 156
V-4-2 Connect ..... 157
V-4-2-1 Dashboard of the Device ..... 158
V-4-2-2 Devices ..... 159
V-4-2-3 Clients / Groups ..... 161
V-4-2-4 Setup ..... 162

**Chapter VI Troubleshooting ..... 163**

VI-1 Diagnostics ..... 164

VI-1-1 System Log ..... 165
VI-1-2 Speed Test ..... 165
VI-1-3 Traffic Graph ..... 166
VI-1-4 WLAN (2.4GHz) Statistics ..... 166
VI-1-6 WLAN (5GHz) Statistics ..... 168
VI-1-7 Support Area ..... 169

VI-2 Checking the Hardware Status ..... 170

VI-3 Checking the Network Connection Settings ..... 171

VI-3-1 For Windows ..... 171
VI-3-2 For Mac Os ..... 173

VI-4 Pinging the Device ..... 174

VI-4-1 For Windows ..... 174
VI-4-2 For Mac Os (Terminal) ..... 174

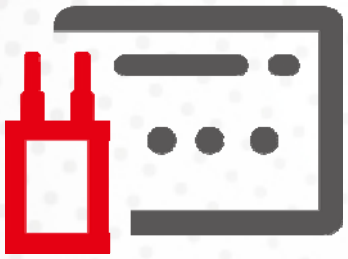
VI-5 Backing to Factory Default Setting ..... 176

VI-5-1 Software Reset ..... 176
VI-5-2 Hardware Reset ..... 176

VI-6 Contacting DrayTek ..... 177

Index ..... 178

# 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 this VigorAP 1060C!

As a tri-band AP, it provides an extra 5GHz Wireless band which increases the supported number of wireless devices. In Mesh mode or Range Extender mode, this extra band can also be dedicated as the Uplink band to the Internet. VigorAP 1060C is suitable to construct a small Wireless network.

VigorAP 1060C can operate in standalone mode for your office network or a classroom; connected to your LAN and offering you wireless access.

It makes high density with quality-performance be feasible for users as it is going to be implemented with DrayTek VigorACS 2 supports configuration, firmware upgrade, status, and monitoring.

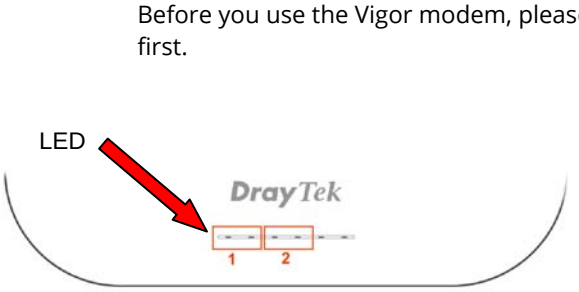
The Power of Ethernet (PoE) on VigorAP 1060C relieves the installation of the power plug. The massive deployment of VigorAP 1060CC for hospitalities and school environment will be much easier.

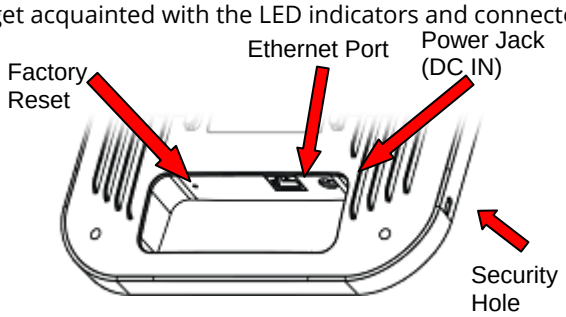
With the optimized antennas built-in, DrayTek VigorAP 1060C ceiling-mount wireless access point is ideal for hospitalities, small offices, and small campus.

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!

# 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 |
|---|---|---|
| 1 | On (Blue) | The system is in boot-loader mode. |
| | Off | The system is not ready or fails. |
| | Blinking(Blue) | The system is in TFTP mode. |
| 2 | Off | The system is not ready or fails. |
| | Blinking(Blue) | The system is ready and can work normally. |

| Interface | Explanation |
|---|---|
| Ethernet Port | Connects to LAN or router.<br>Supports PoE power & Gigabit (2.5Gpbs). |
| Power Jack (12V ⎓ 2.5A) | Connecter for a power adapter. |

| Hole | Explanation |
|---|---|
| Factory Reset | Restores the unit back to factory default settings.<br>To use, insert a small item such as an unbent paperclip into the hole. You will feel the button inside depress gently. Hold it for 5 seconds.<br>The VigorAP will restart with the factory default configuration and the LED will blink blue. |
| Security Hole | A security hole for installing the anti-theft lock. |

**Note:**

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

# I-2 Hardware Installation

This section will guide you through installing the VigorAP.

VigorAP can be installed under certain locations: wooden ceiling, plasterboard ceilings, light-weighted steel frame and wall.

---

**Note:**

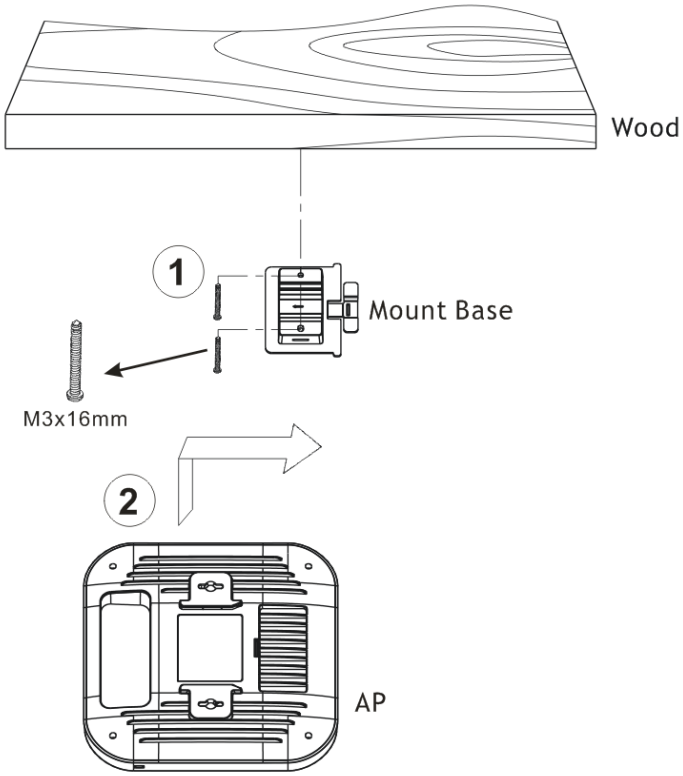
For the sake of personal safety, only trained and qualified personnel should install this access point.

---

## I-2-1 Ceiling-mount Installation (Wooden Ceiling)

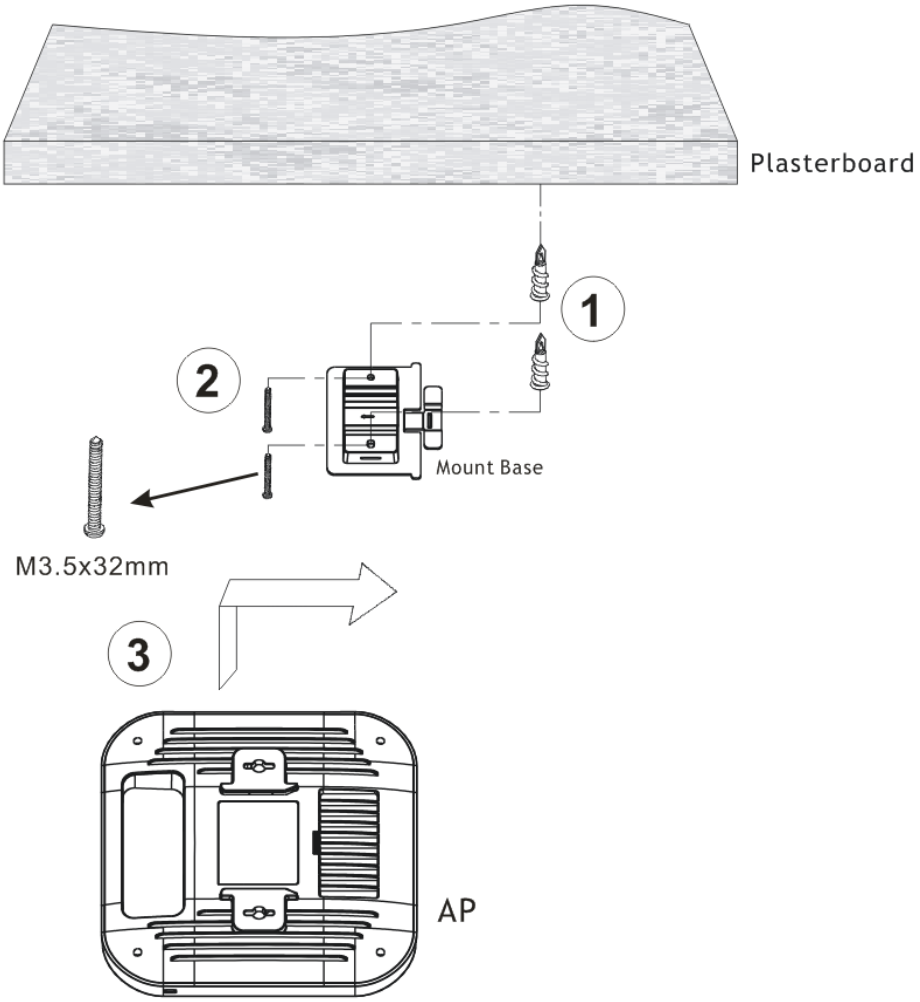
Determine where the Access Point to be placed and mark location on the surface for the two mounting holes. Use the appropriate drill bit to drill two holes in the markings and hammer the bolts into the openings.

1. Place the mount base under the wooden ceiling and fasten it on the ceiling with two screws firmly.
2. Place the mount base under the wooden ceiling and fasten it on the ceiling with two screws firmly.



## I-2-2 Ceiling-mount Installation (Plasterboard Ceiling)

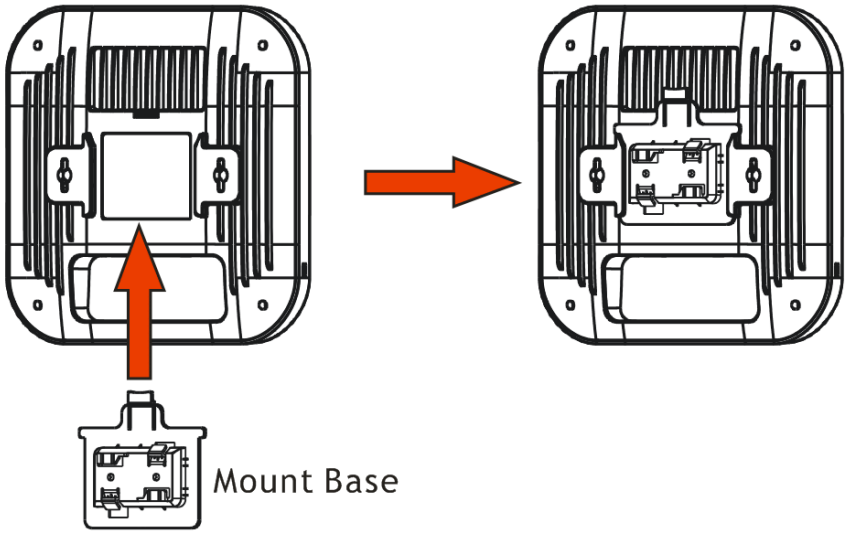
1. Place the Mount Base under the plasterboard ceiling and fasten two turnbuckles firmly.
2. Make the screws pass through the Mount Base and insert into the turnbuckles. Fasten them to offer more powerful supporting force.
3. When the Mount Base is in place, slide the mount base into the slot of the AP.



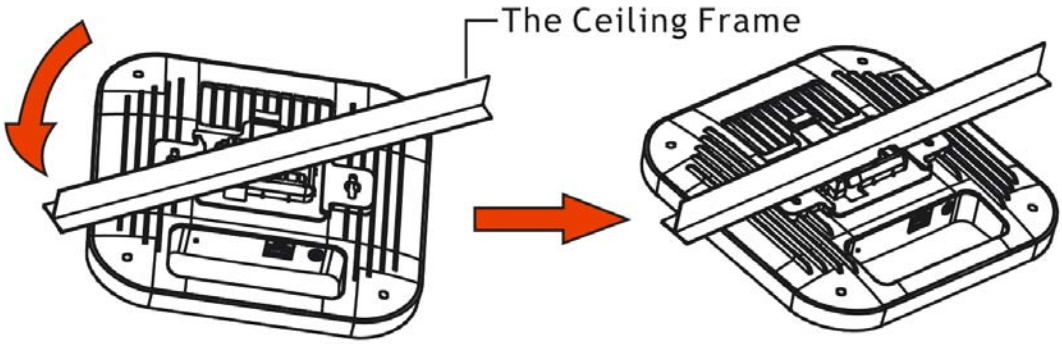
## I-2-3 Suspended Ceiling (Lightweight Steel Frame) Installation

You cannot screw into ceiling tiles as they are weak and not suitable for bearing loads. Your VigorAP is supplied with mounts (Mount Base) which will be used to attach directly to the ceiling frame of your suspended ceiling.

1. Slide the mount base into the slot of the AP.




2. Hold the Access Point with one hand to reach the other hand over the T-Rail sides of the bracket.




3. Rotate and hook the stationary end of the ceiling mount base onto the T-Rail ceiling frame.

---

**Note:**

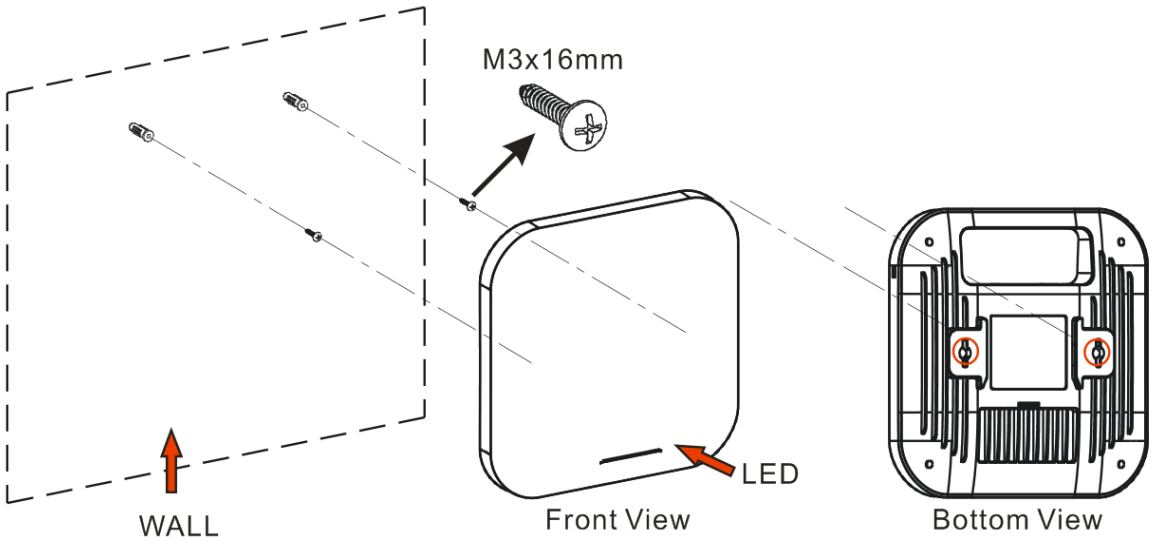
Warning: The screw set shown below is for wall mounting only. Do not use such set for ceiling mounting due to the danger of falling.

---

## I-2-4 Wall-Mounted Installation

For wall-mounting, the VigorAP has keyhole type mounting slots on the underside.

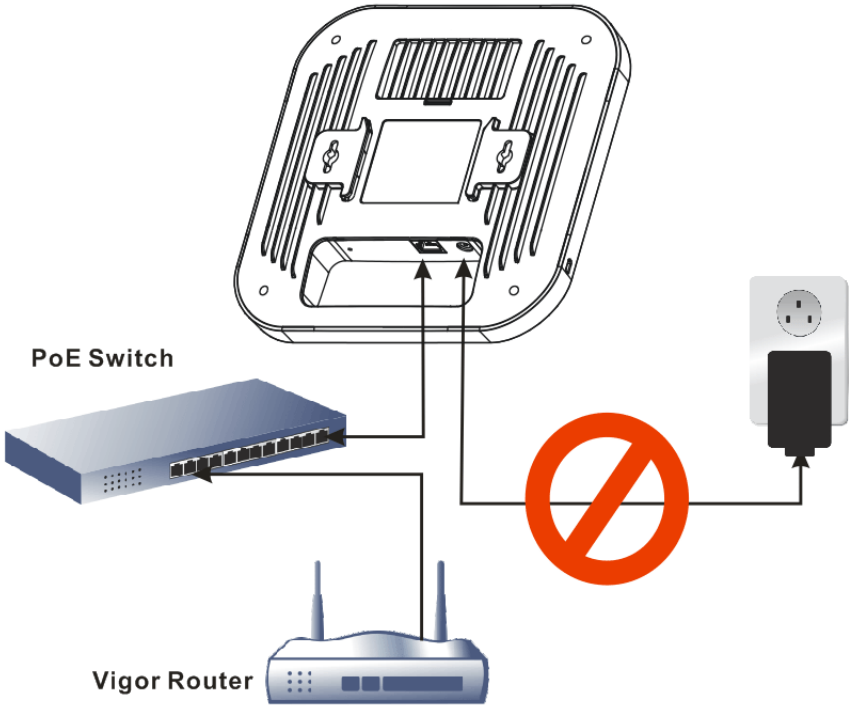
1. Use the appropriate drill bit to drill two 8.1mm diagram and 26mm depth holes in the markings and hammer the bolts into the openings.
2. Screw the anchors unto the holes until they are flush with the wall; screw the included screws into the anchors.
3. Place the Access Point against wall with the mounting screw heads.



# I-2-5 Connect to a Vigor Router using AP Management

Your VigorAP can be used with Vigor routers which support AP management (such as the Vigor2865 or Vigor2927 series). AP Management enables you to monitor and manage multiple DrayTek APs from a single interface.

1. Connect VigorAP to PoE switch (via LAN port) with Ethernet cable. VigorAP will get the power from the switch directly. Then, connect the VigorSwitch to a Vigor router.




2. Access into the web user interface of Vigor router. Here we take Vigor2865 as an example. Open **Central Management>>AP>>Status**.

3. Locate VigorAP 1060C. Click the IP address assigned by Vigor router to access into web user interface of VigorAP 1060C.

4. After entering the username and password (admin/admin), the main screen will be displayed.

# I-3 Network IP Configuration

After the network connection is built, the next step you should do is setup VigorAP 1060C with proper network parameters, so it can work properly in your network environment.

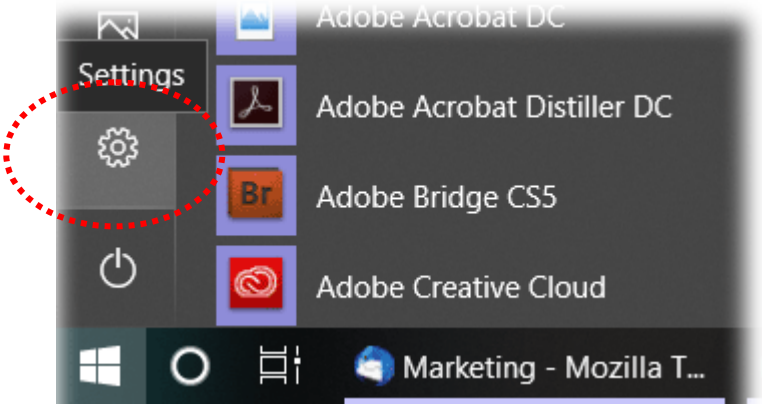
Before you can connect to the access point and start configuration procedures, your computer must be able to get an IP address in the same subnet as this AP. If it's not connected to the same DHCP Server with the AP or you're unsure, please follow the following instructions to configure your computer to use the static IP address in the same subnet as default IP address of this AP.

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...***

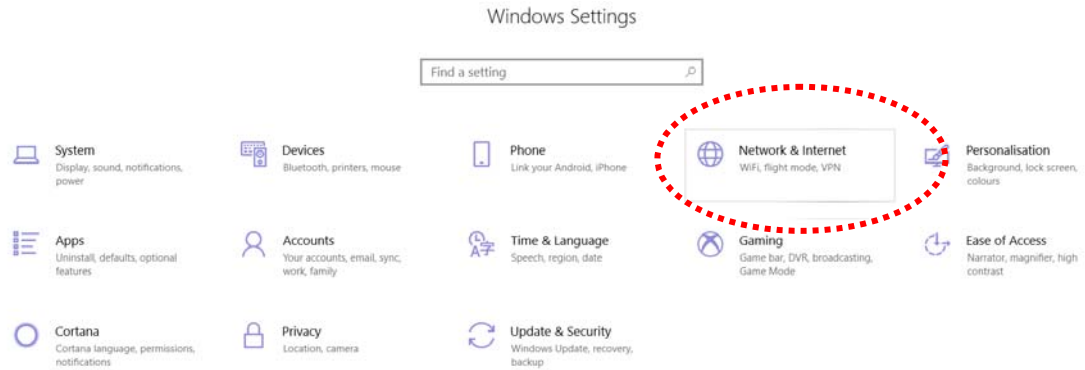
**Windows 10** **- please go to section I-3-1**

## I-3-1 Windows 10 IP Address Setup

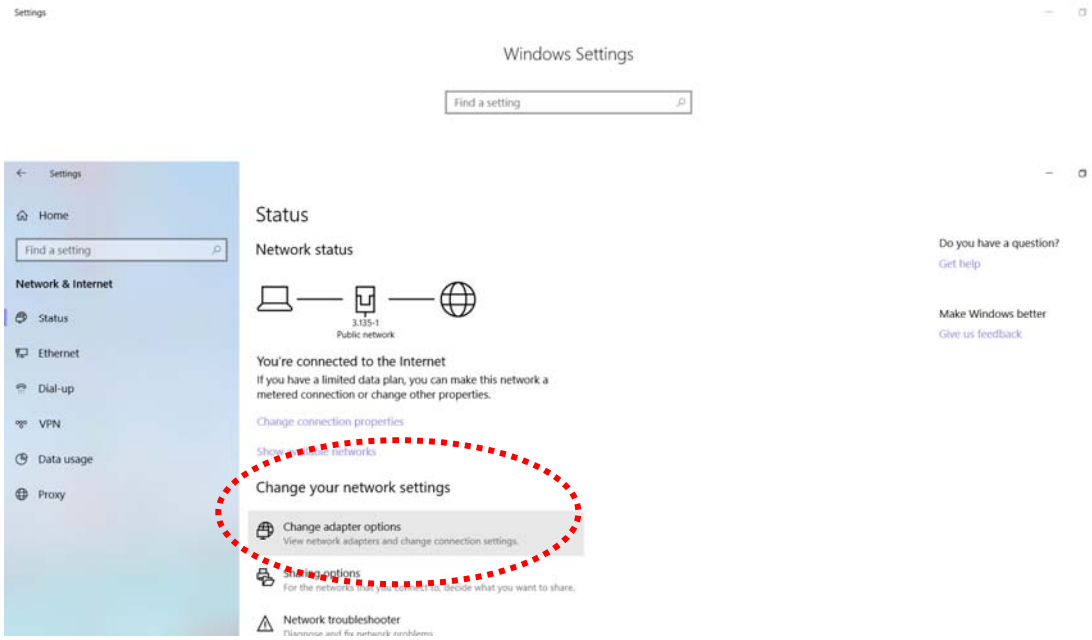
Click the **Start** button (it should be located at lower-left corner of your computer), then click the **Settings** icon.



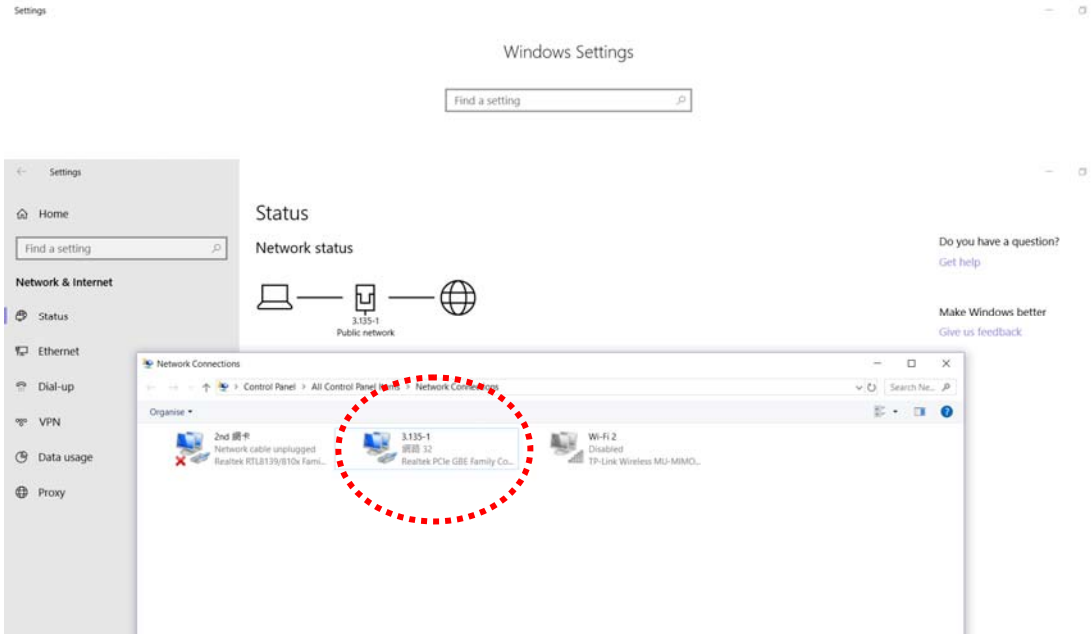

Double-click **Network & Internet**.



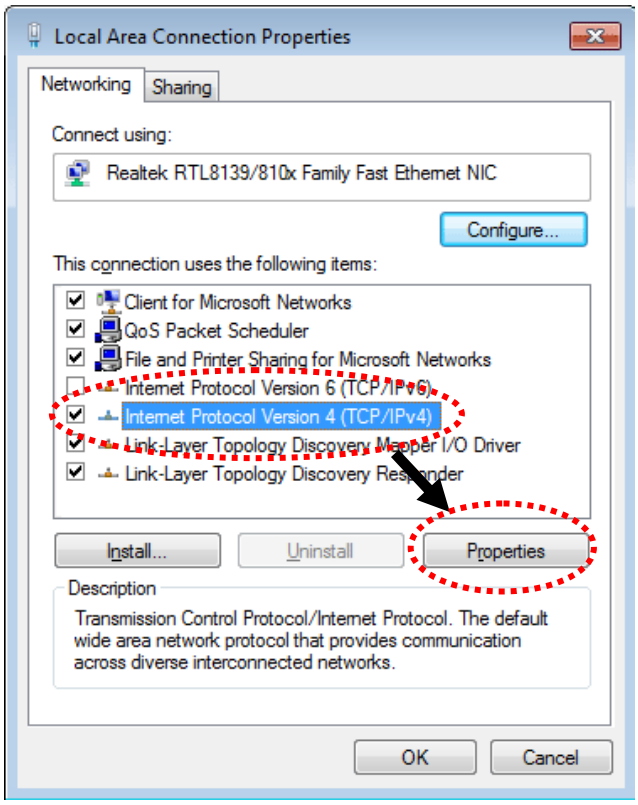
Next, click **Change adapter options**.




Click the local area connection.



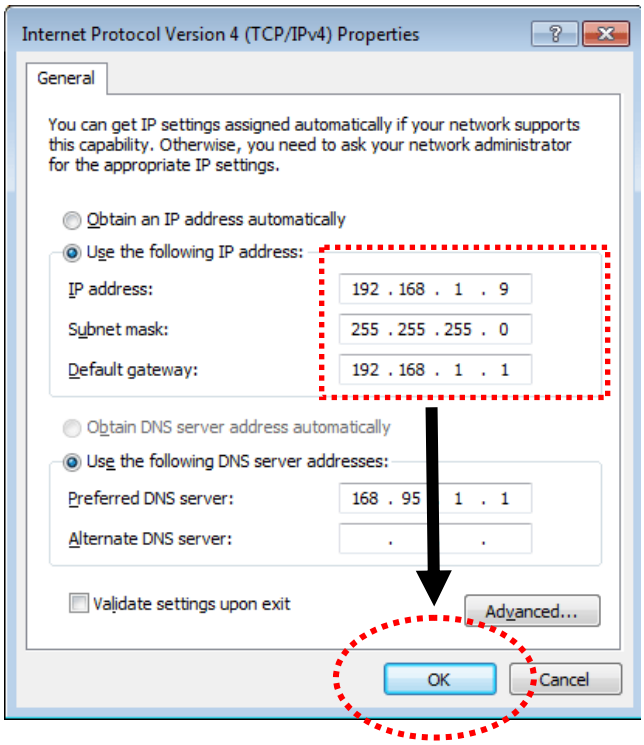
Then, select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.




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**

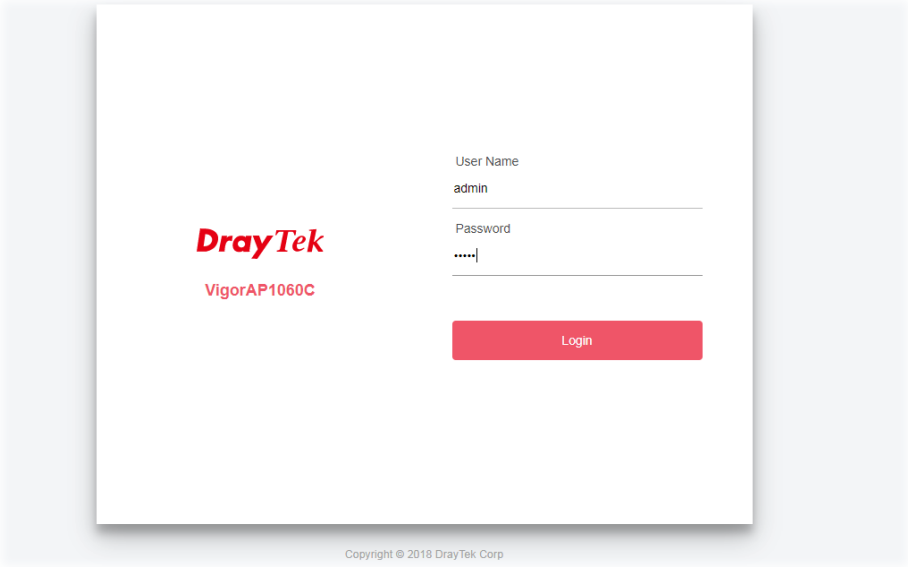
Subnet Mask: **255.255.255.0**



# I-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 1060C 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**.

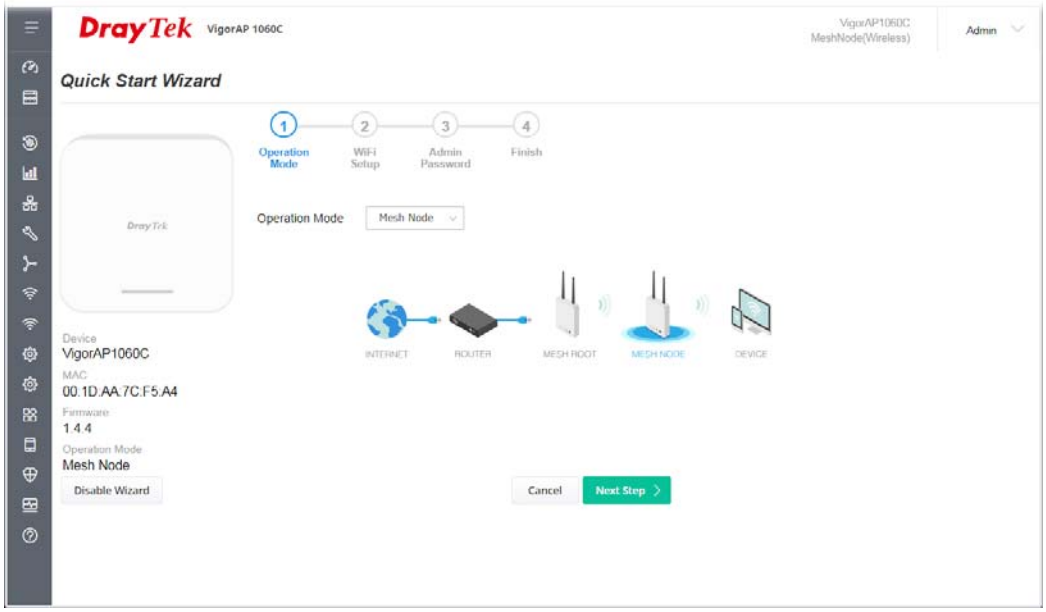



**Note:**

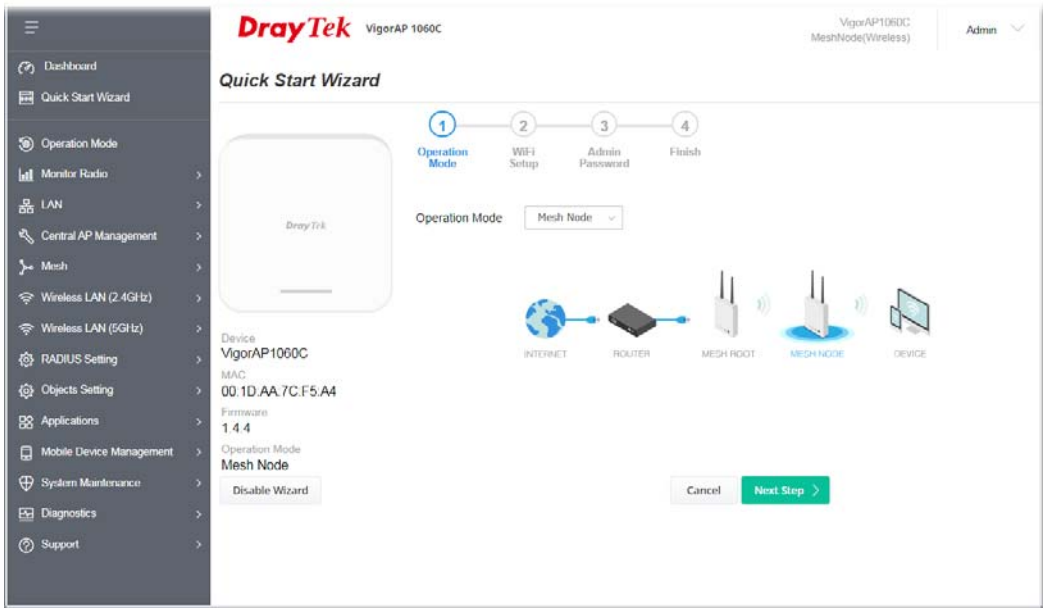
You may either simply set up your computer to get IP dynamically from the router or set up the IP address of the computer to be in the same subnet as **the IP address of VigorAP 1060C.**

- If there is no DHCP server on the network, then VigorAP 1060C will have an IP address of 192.168.1.2.
- If there is DHCP available on the network, then VigorAP 1060C 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.

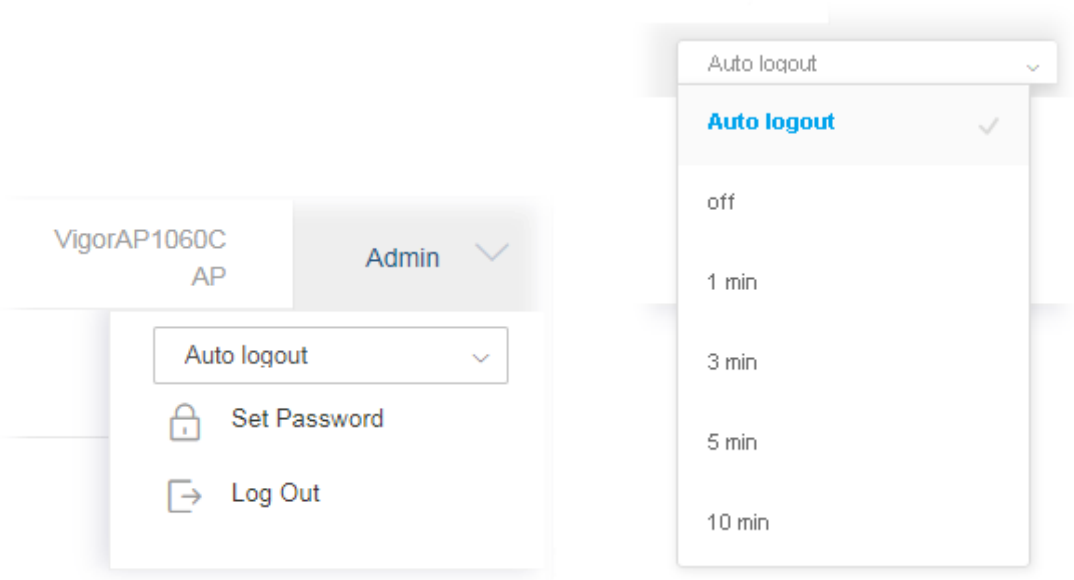
3. For the first time accessing VigorAP, the **Quick Start Wizard** for configuring wireless settings will appear as follows. Refer to *Section I-7 Quick Start Wizard for detailed information*.




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:**

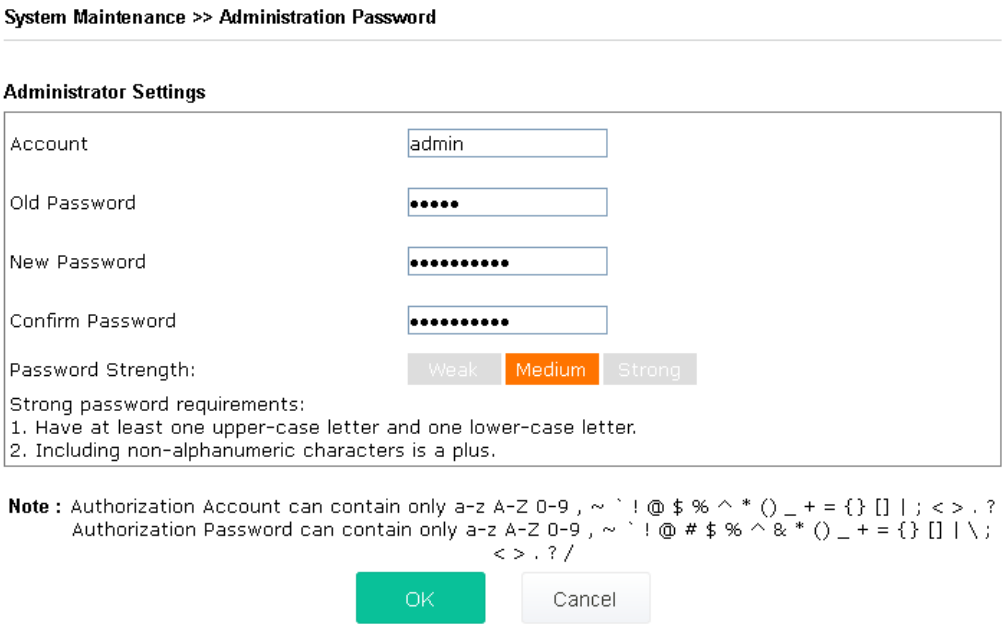
If you fail to access the web configuration, please go to the section “Trouble Shooting” for detecting and solving your problem.

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

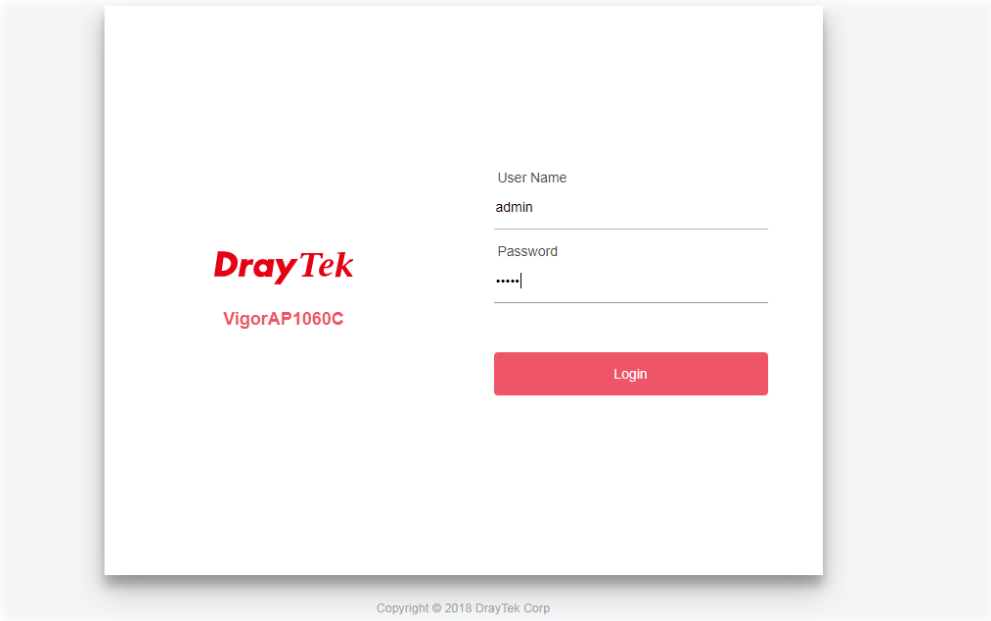
---

# 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.**



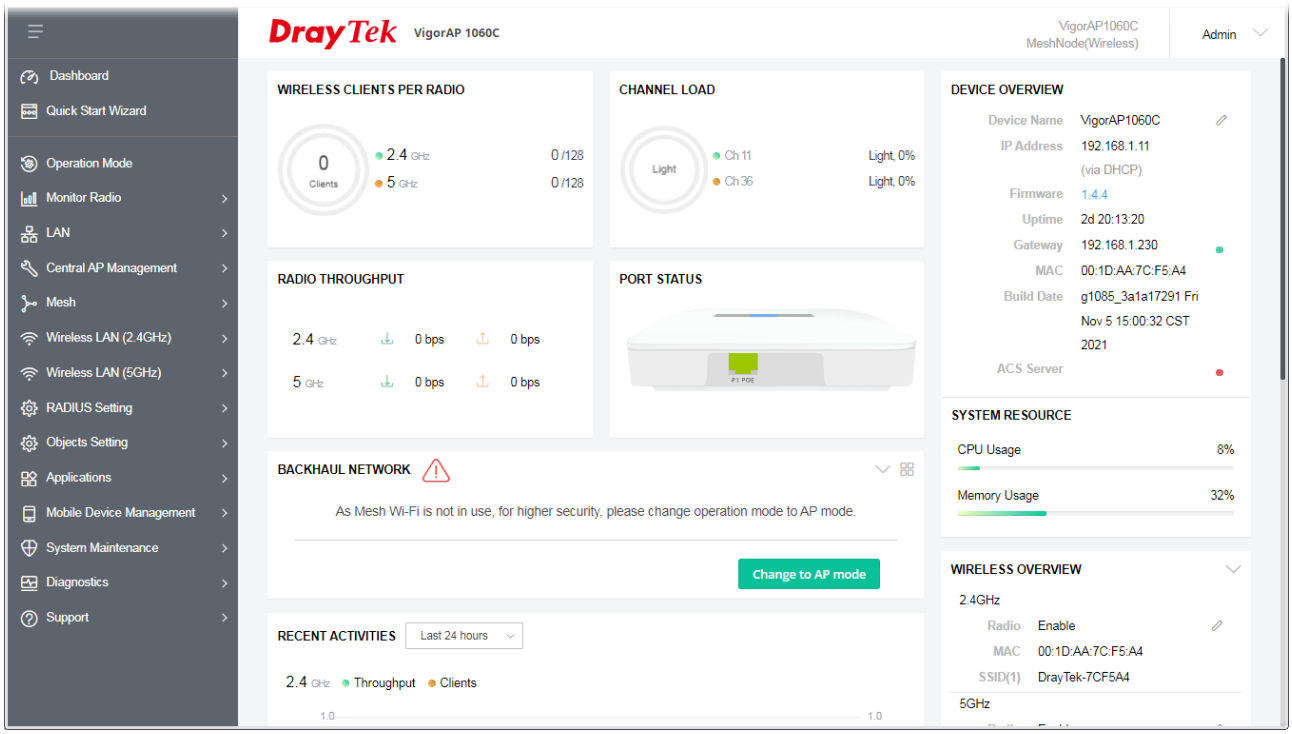

3. Enter the new login password on the field of **Password**. Then click **OK** to continue.
4. Now, the password has been changed. Next time, use the new password to access the Web User Interface for this modem.



# I-6 Dashboard

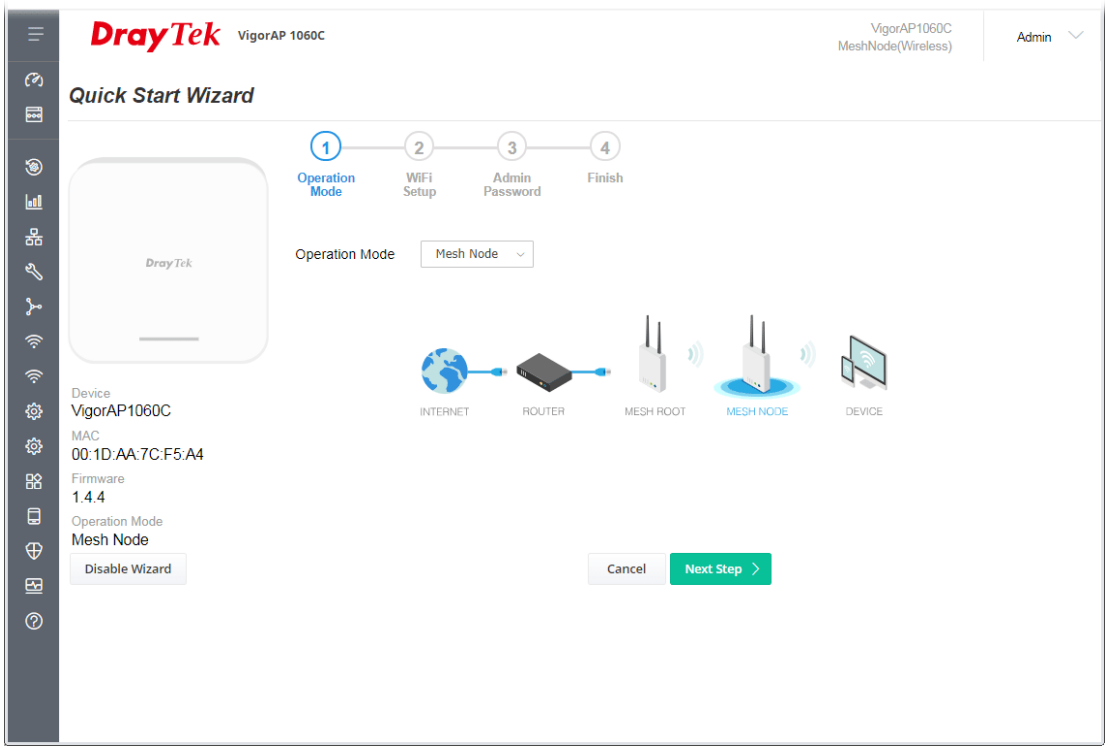
Dashboard shows system status including the number of client connected, throughput, gateway, physical connection status, radio (2.4GHz / 5GHz) status, backhaul network, recent activities, wireless network usage, and so on.

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 /5G wireless setting and other corresponding settings for Vigor Access Point step by step.



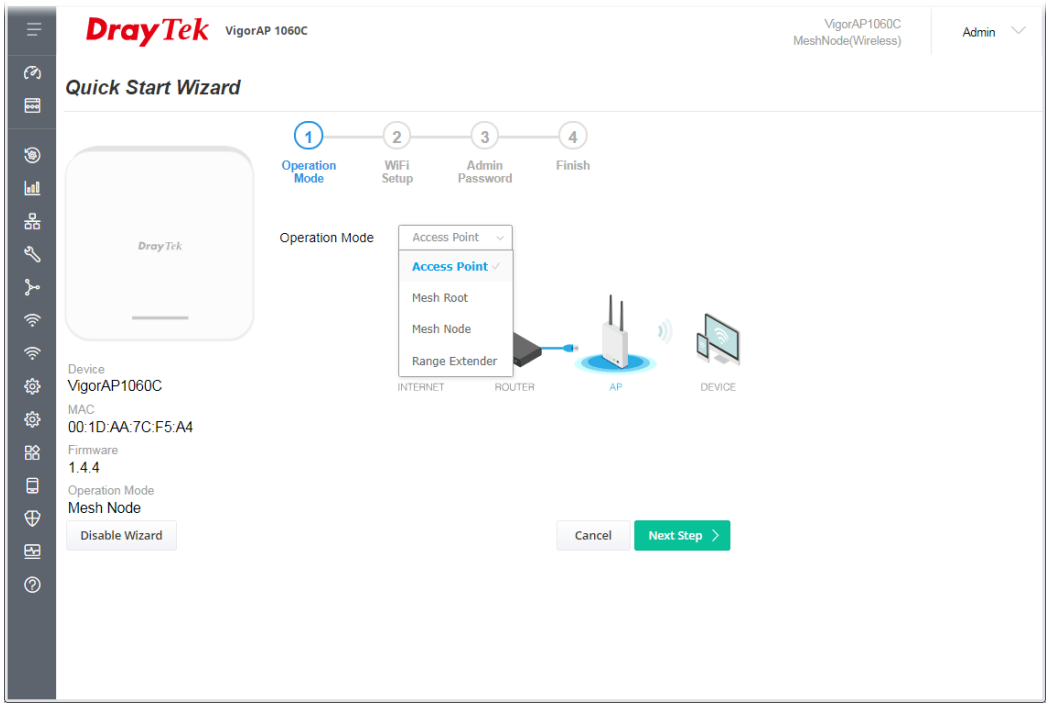

Available operation mode includes:

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

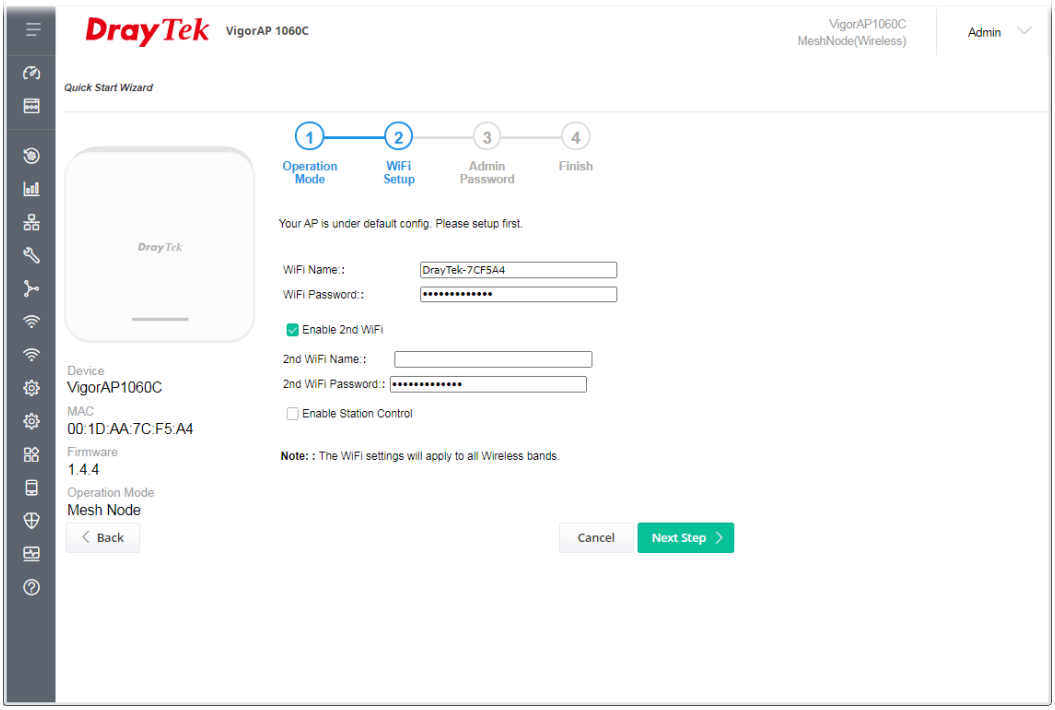
In this page, the advanced settings pages will vary according to the operation mode specified.

# 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 2.4GHz, and 5GHz) and click **Next Step**.

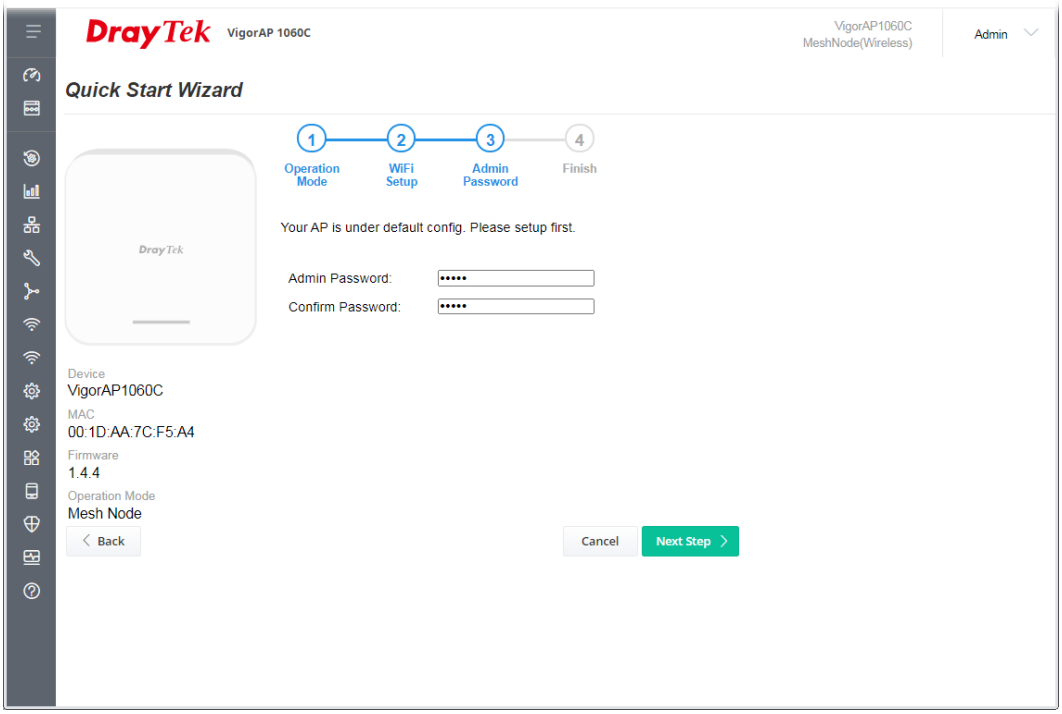



Available settings are explained as follows:

| Item | Description |
|---|---|
| **WiFi Name** | Set a name for VigorAP 1060C 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 WiFi** | Check the box to enable the **guest** wireless setting.<br><br>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.<br><br>**2nd WiFi Name** - Set a name for VigorAP device which can be identified and connected by wireless guest.<br><br>**2nd WiFi Password -** Set **8~63** ASCII characters or **64** Hexadecimal digits leading by 0x which can be used for logging into VigorAP device by wireless guest. |
| **Enable Station Control** | Check the box to set the duration for the guest connecting /reconnecting to Vigor device.<br><br>**Connection Time** –Scroll the radio button to choose the value you want.<br><br>**Reconnection Time** –Scroll the radio button to choose the value you want. |

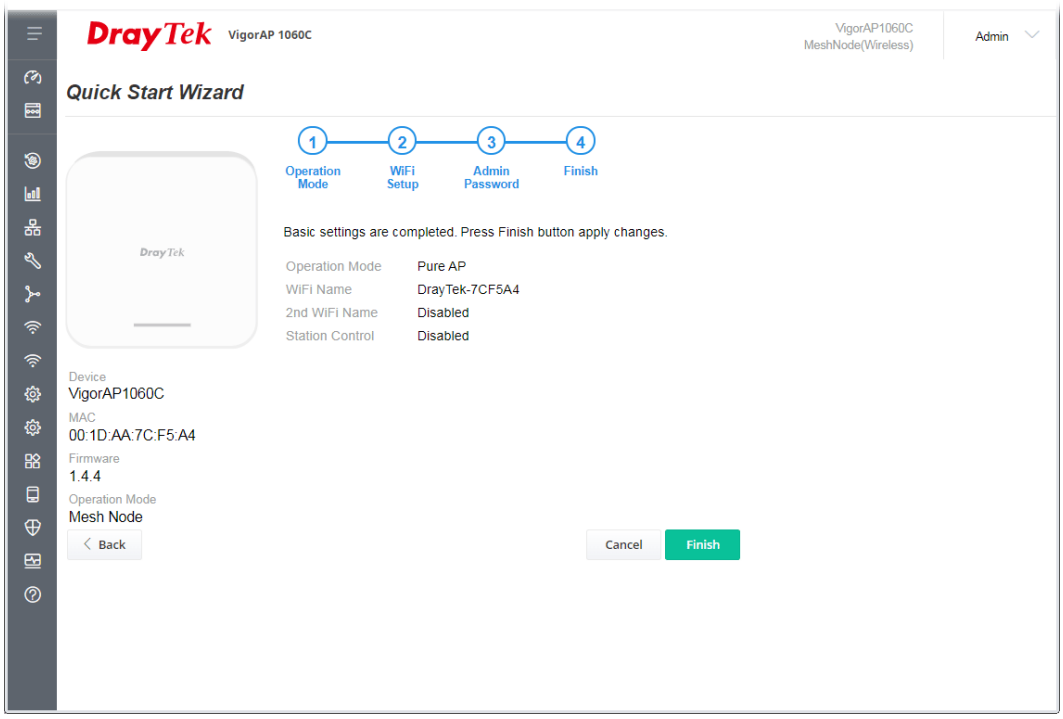
3. Change the default password for such device with new value. Then click **Next Step**.




Available settings are explained as follows:

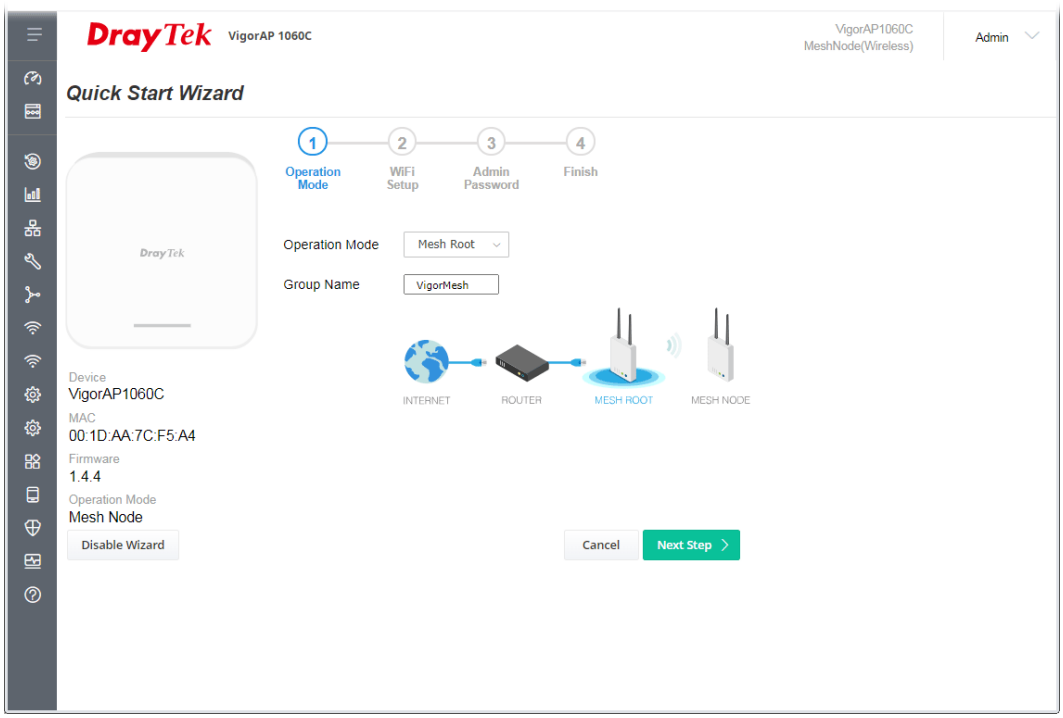
| Item | Description |
|---|---|
| **Admin Password** | Enter a new password. |
| **Confirm Password** | Enter the new password again for confirmation. |

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

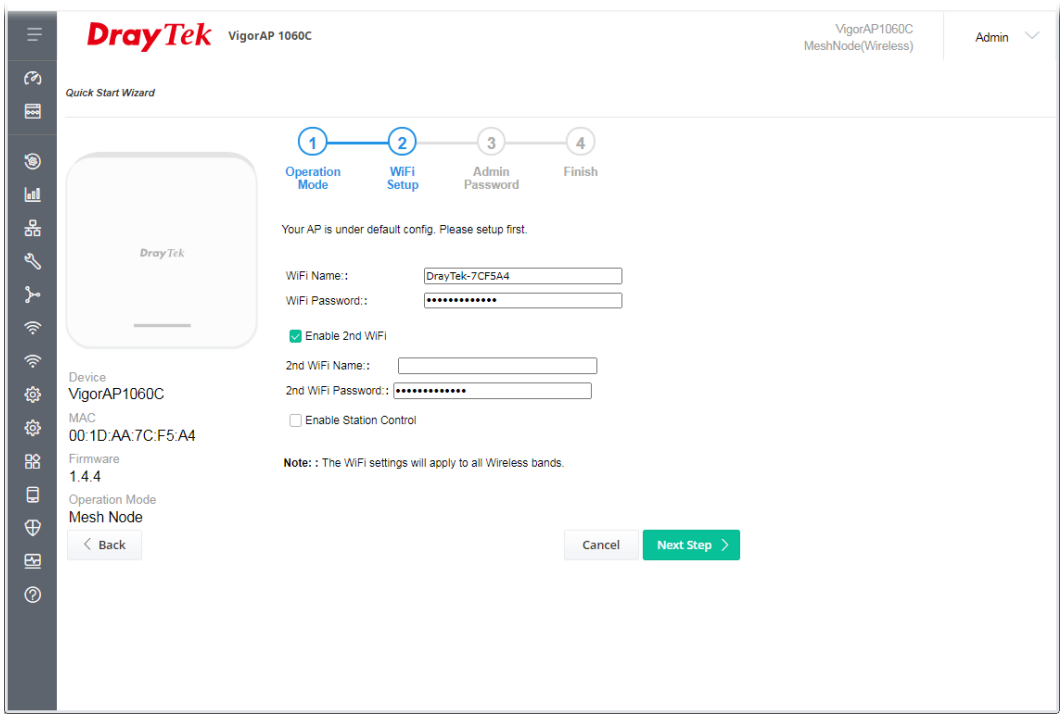


# I-7-2 Settings for Mesh Root

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




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

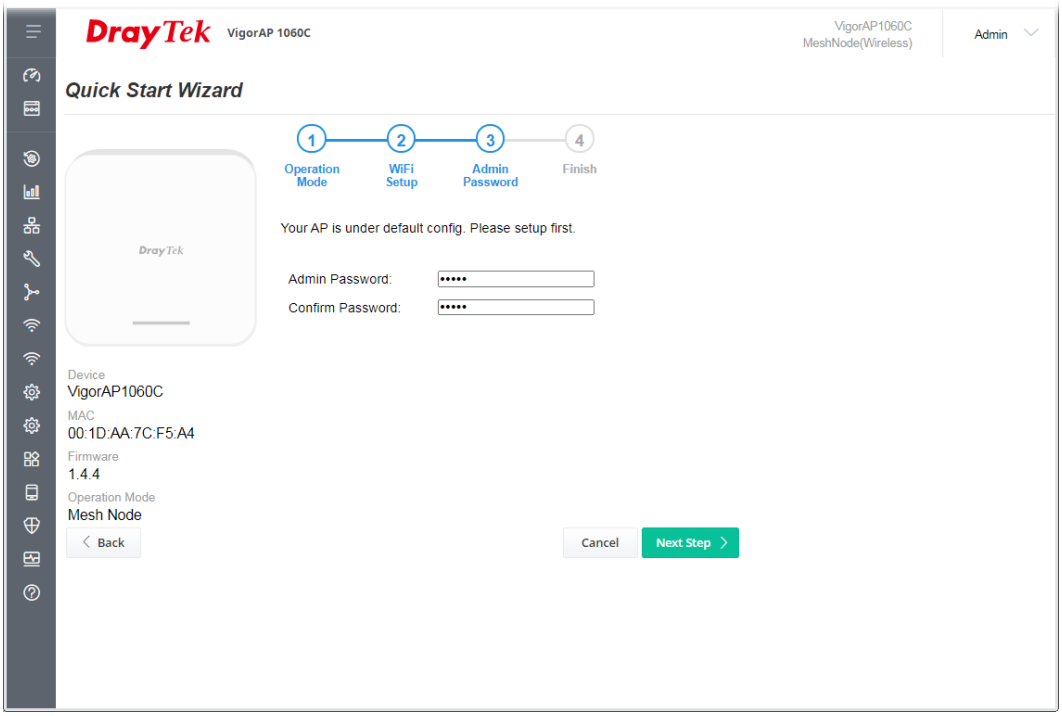



Available settings are explained as follows:

| Item | Description |
|---|---|
| **WiFi Name** | Set a name for VigorAP 1060C 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 WiFi** | Check the box to enable the second wireless setting.<br><br>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.<br><br>**2nd WiFi Name** - Set a name for VigorAP 1060C which can be identified and connected by wireless guest.<br><br>**2nd WiFi Password -** Set **8~63** ASCII characters or **64** Hexadecimal digits leading by 0x which can be used for logging into VigorAP 1060C by wireless guest. |
| **Enable Station Control** | Check the box to set the duration for the guest connecting /reconnecting to Vigor device.<br><br>**Connection Time** –Scroll the radio button to choose the value you want.<br><br>**Reconnection Time** –Scroll the radio button to choose the value you want. |

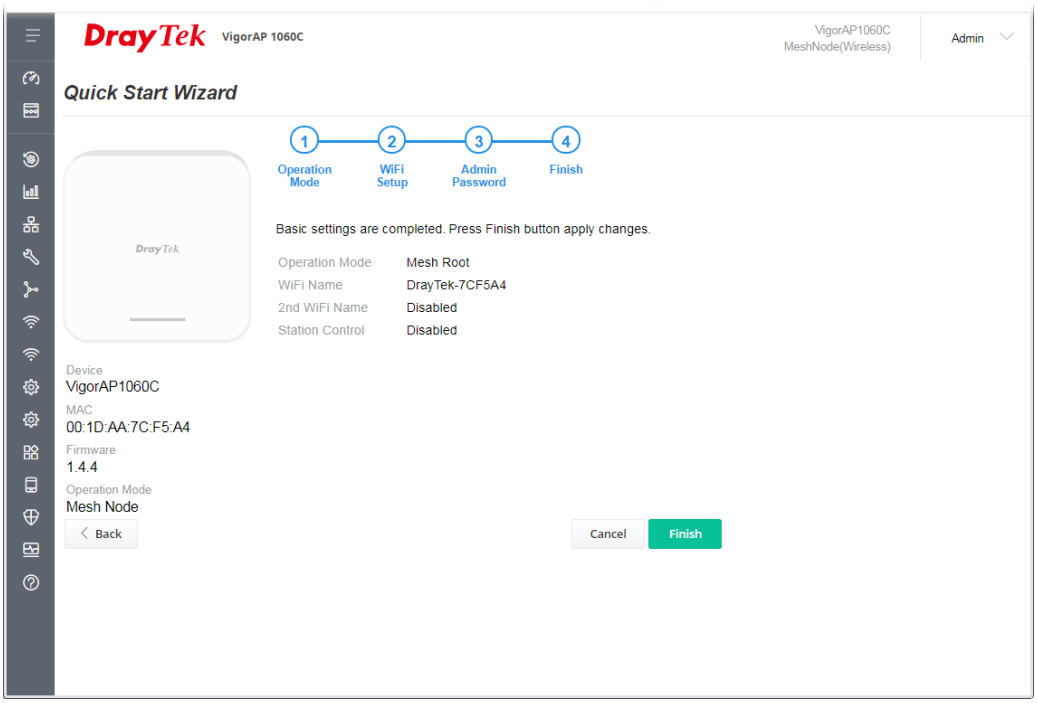
3. Change the default password for such device with new value. Then click **Next Step**.



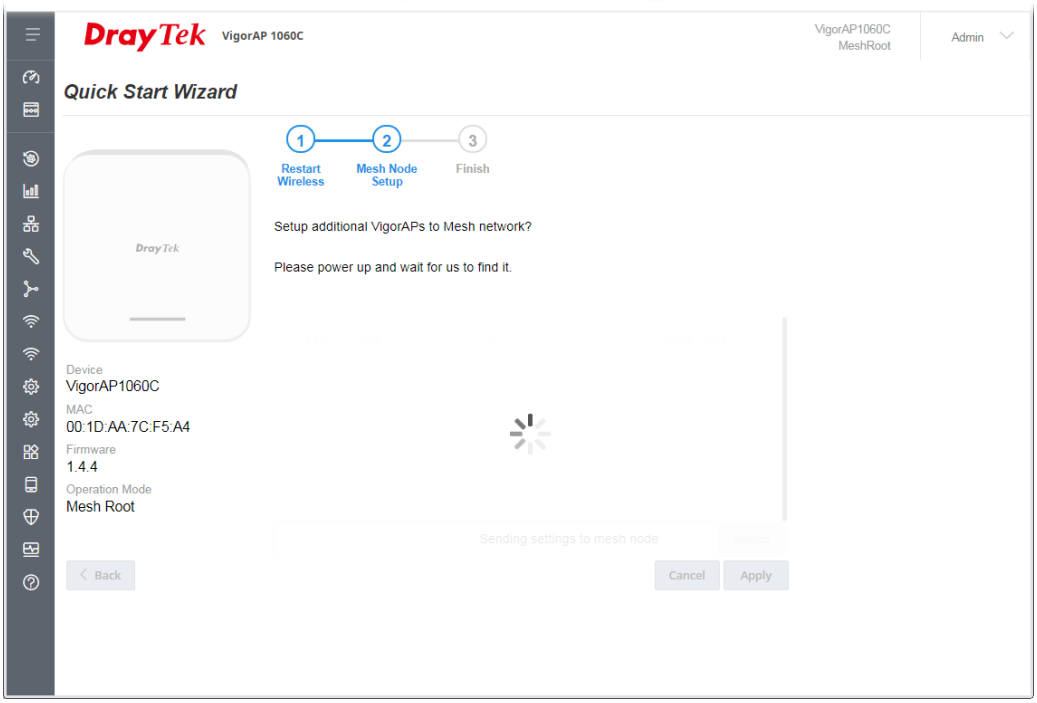

Available settings are explained as follows:

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

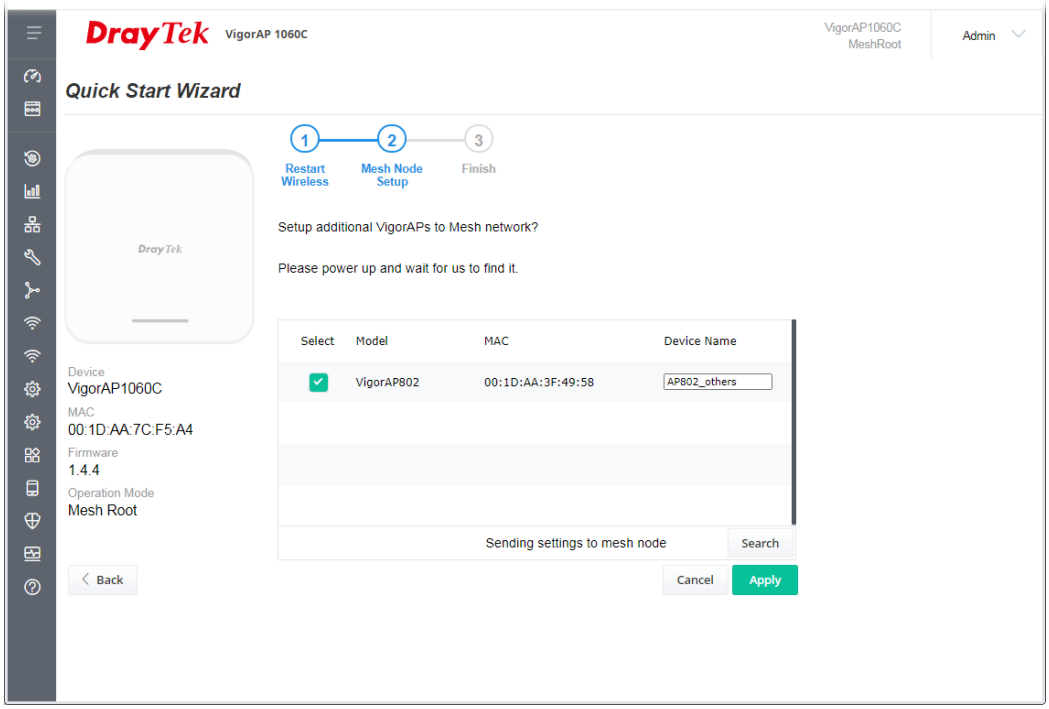
4. A summary of settings configuration will be shown on screen. Click **Finish**.



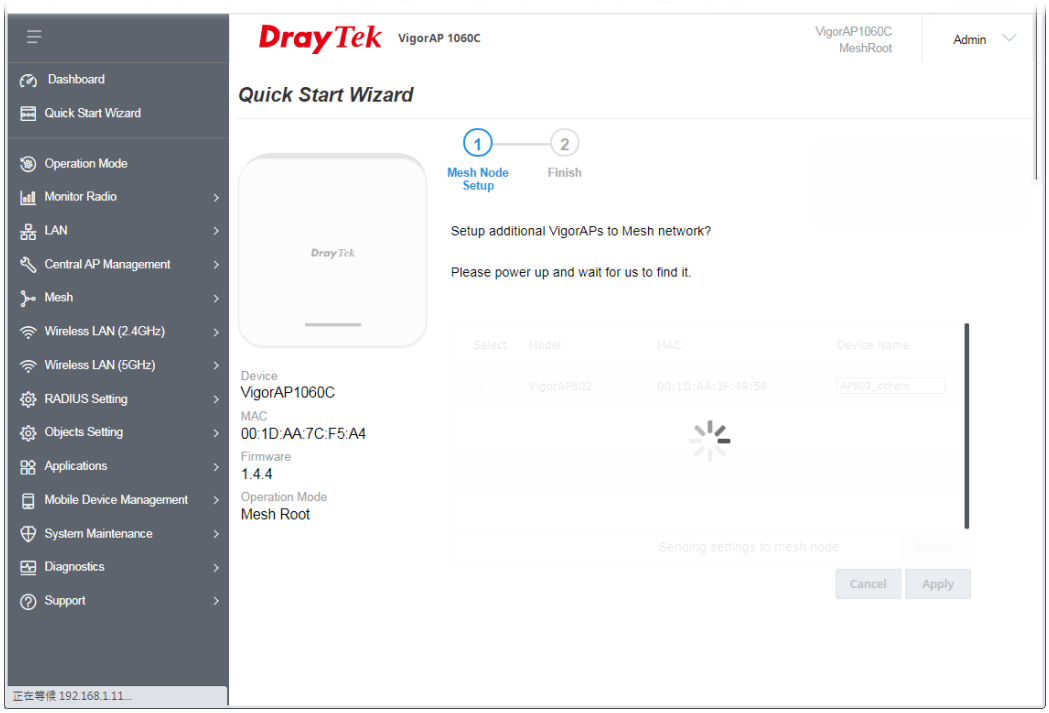

5. After clicking **Finish**, the following web page appears. VigorAP will search for mesh node around the network.



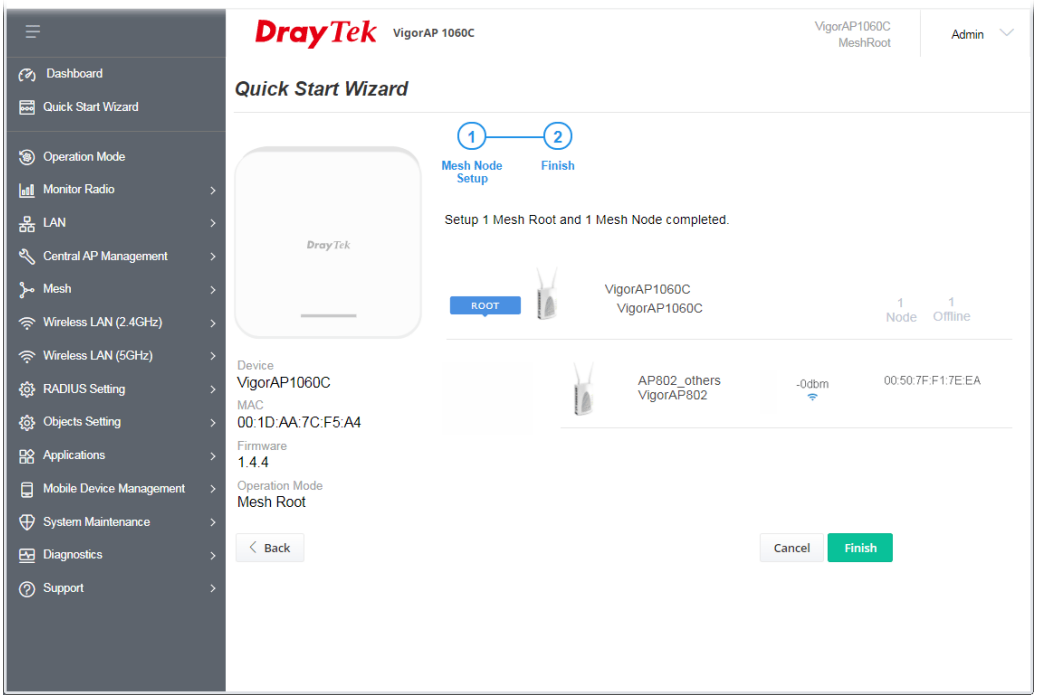
6. Available VigorAP devices will be shown on the screen. Select the device (as a mesh node) for grouping under such mesh group and enter a device name for identification.




7. Click **Apply** and wait for a while.

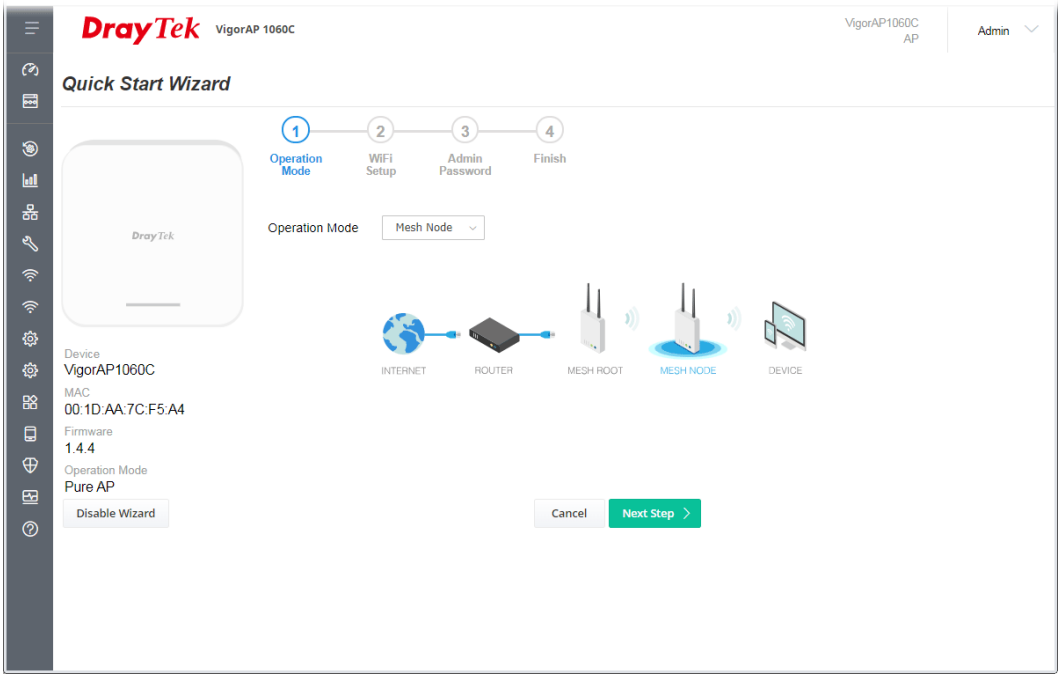


8. Later, a summary page of mesh root with mesh node will be shown on the screen.

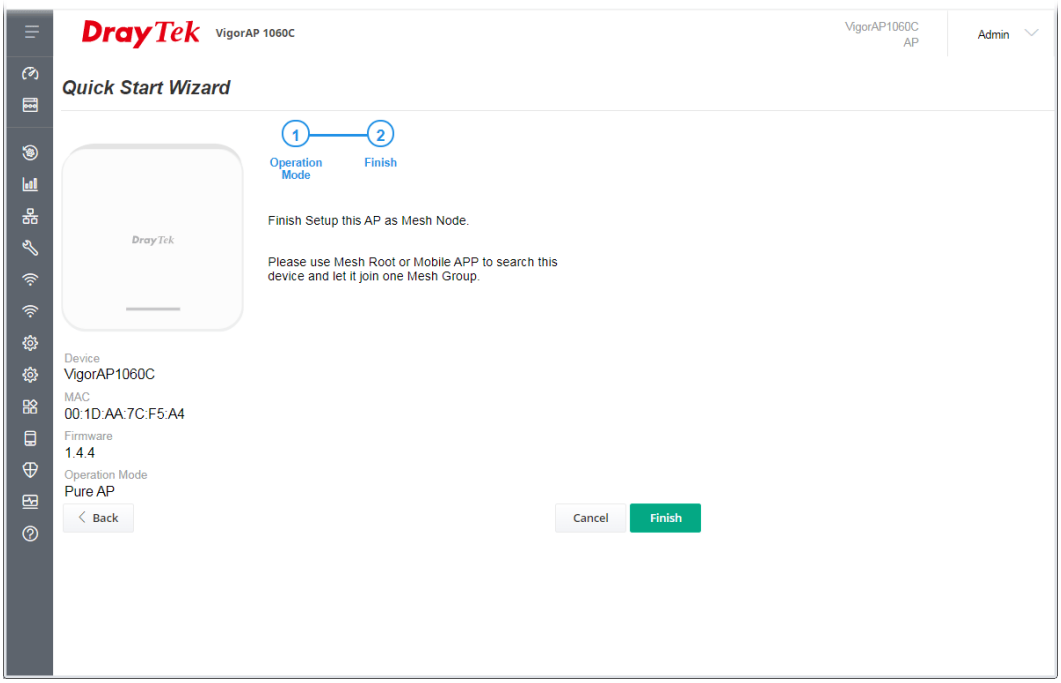


# I-7-3 Settings for Mesh Node

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

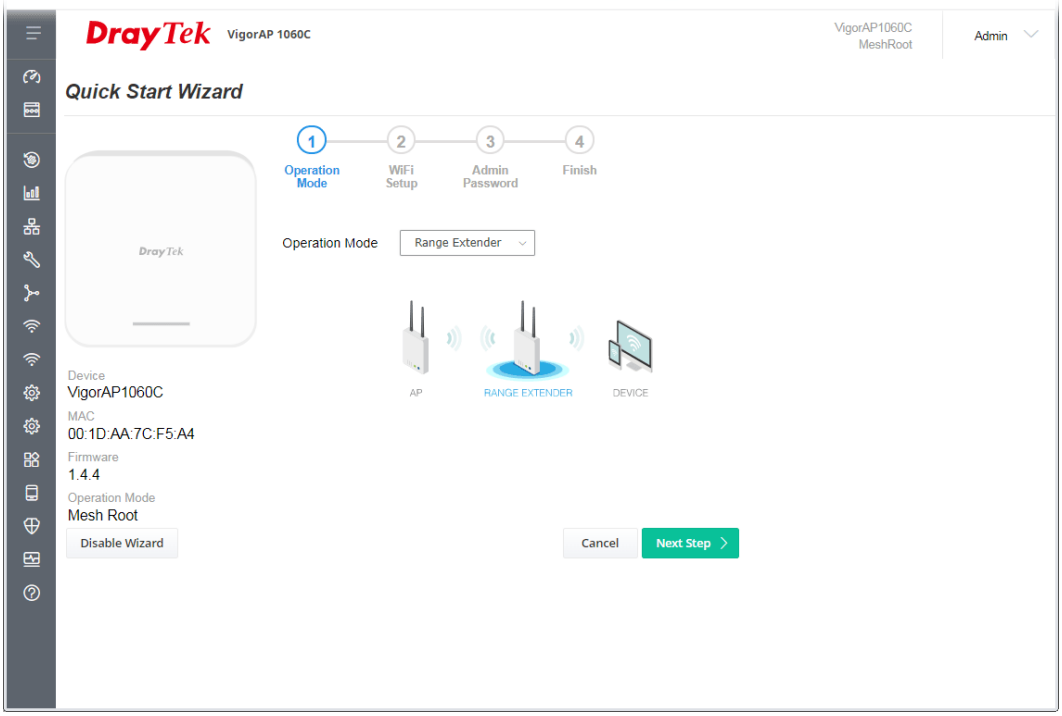



2. A summary of settings configuration will be shown on screen. Click **Finish**.

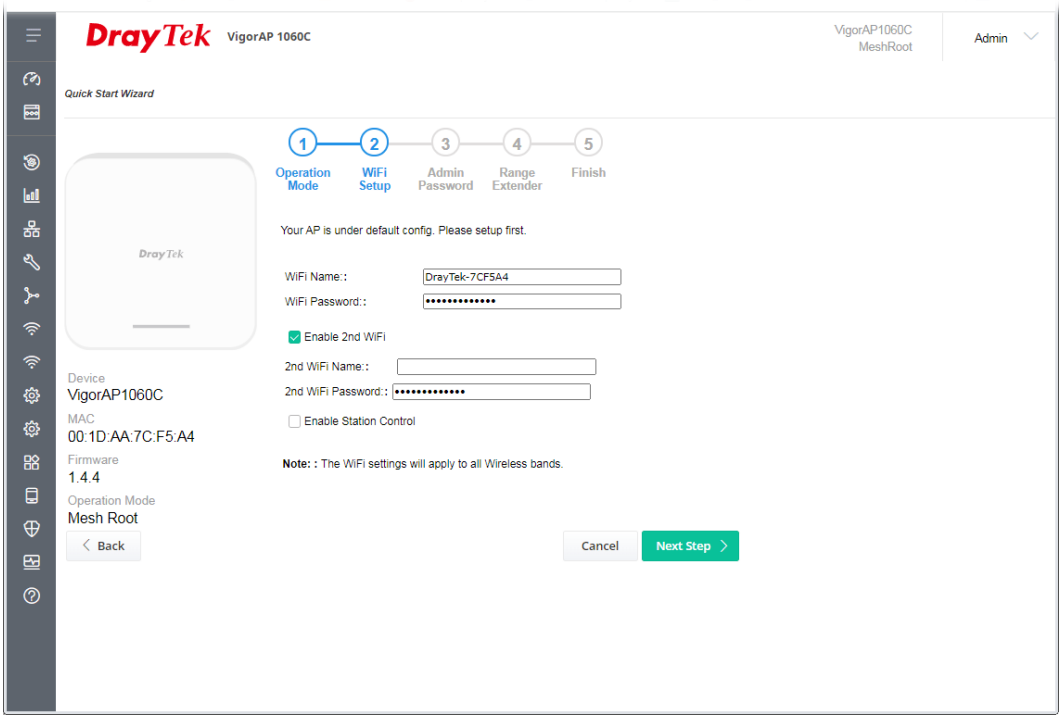


# I-7-4 Settings for Range Extender

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




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

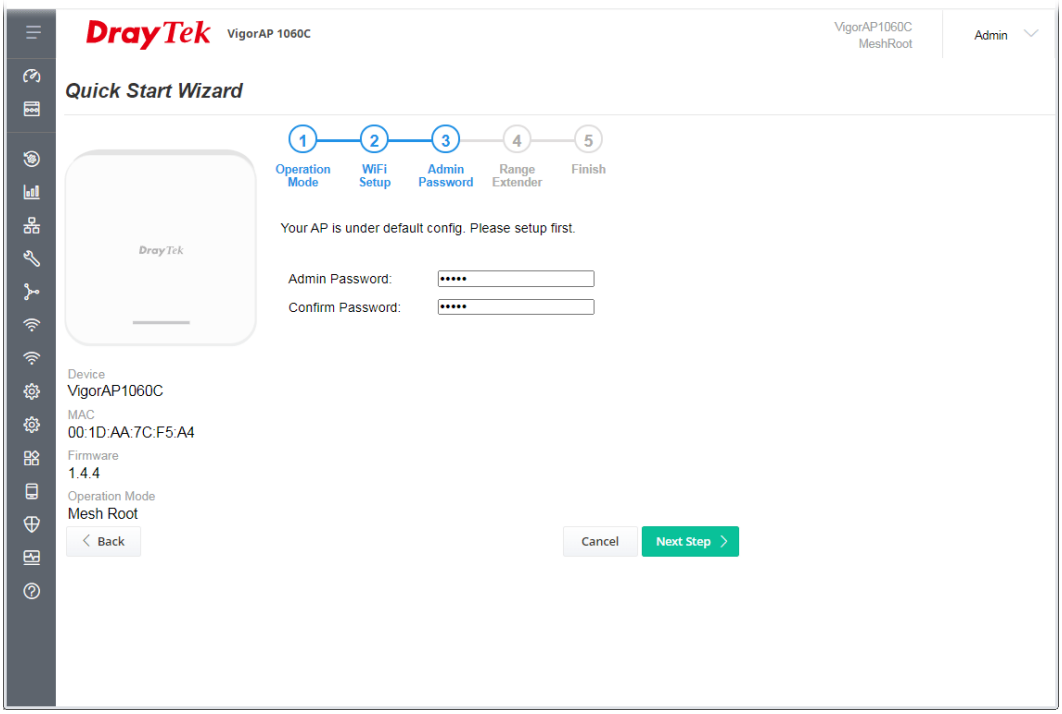



Available settings are explained as follows:

| Item | Description |
|---|---|
| **WiFi Name** | Set a name for VigorAP 1060C 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 WiFi** | Check the box to enable the second wireless setting.<br><br>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.<br><br>**2nd WiFi Name** - Set a name for VigorAP 1060C which can be identified and connected by wireless guest.<br><br>**2nd WiFi Password -** Set **8~63** ASCII characters or **64** Hexadecimal digits leading by 0x which can be used for logging into VigorAP 1060C by wireless guest. |
| **Enable Station Control** | Check the box to set the duration for the guest connecting /reconnecting to Vigor device.<br><br>**Connection Time** –Scroll the radio button to choose the value you want.<br><br>**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**.

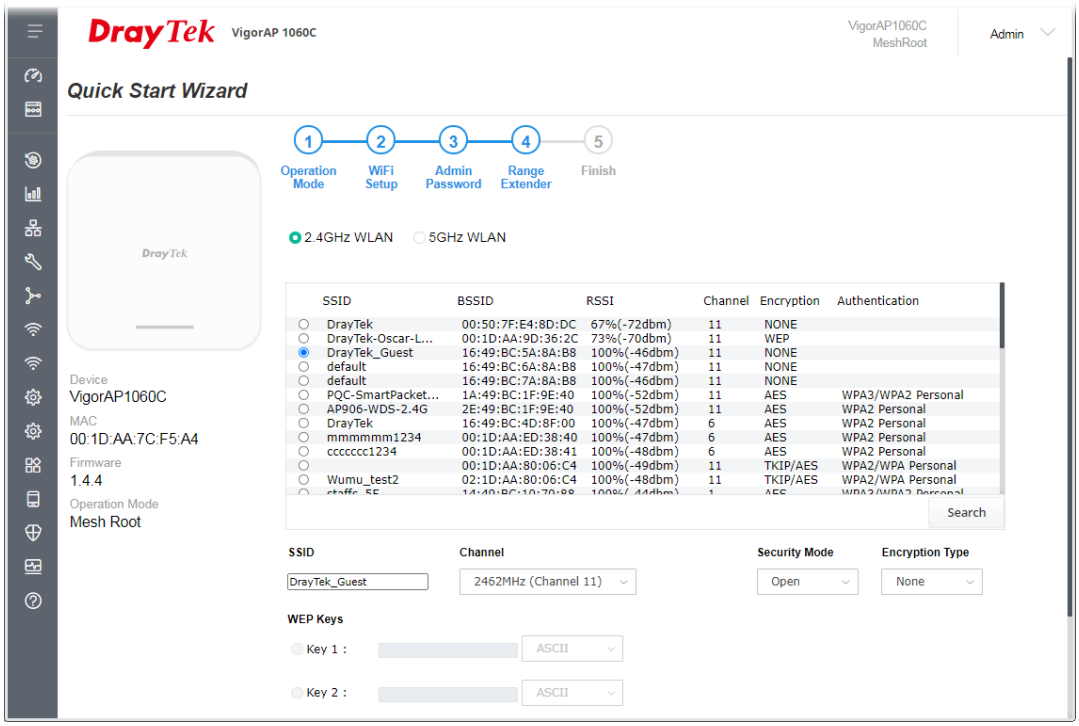



Available settings are explained as follows:

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

4. In the following page, click **Search** to find out neighboring access point. When all the available access points appear on the page, click the one you want to connect. Corresponding settings

(e.g., SSID, Security Mode) of the selected device will be shown below. Enter the Security Key. Then click **Next Step**.

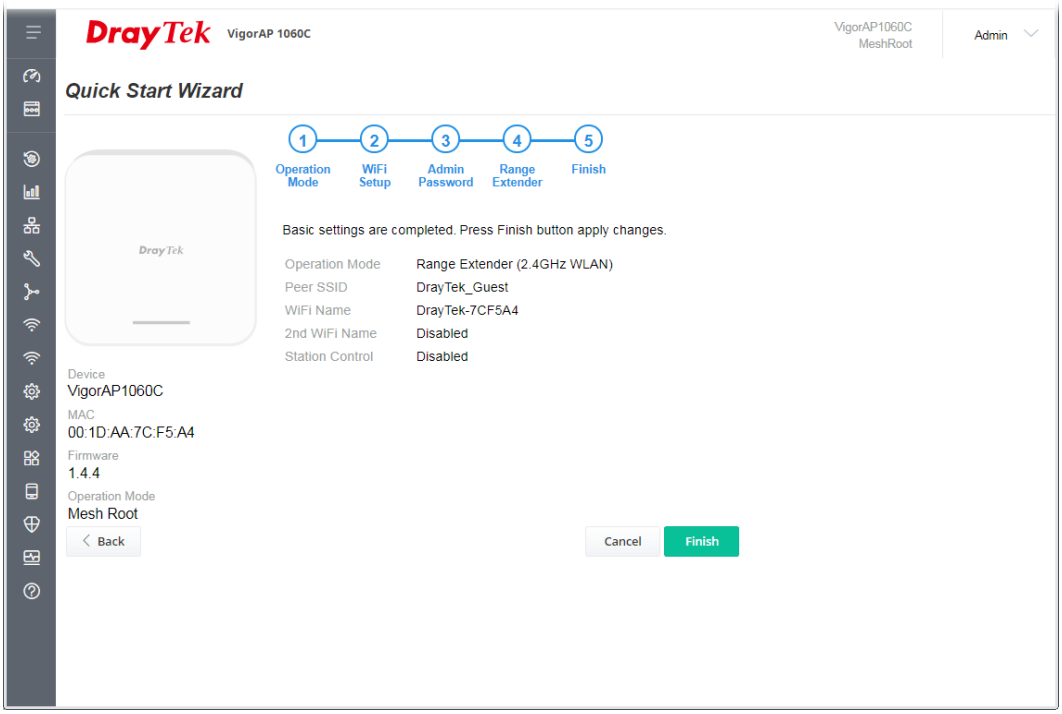



Available settings are explained as follows:

| Item | Description |
|---|---|
| **SSID** | Displays the SSID of the selected access point. |
| **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**.<br>**When Open is selected**:<br>● Choose **None** to disable the WEP Encryption. Data sent to the AP will not be encrypted.<br>● **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 ','.<br>**When Shared is selected**:<br>● **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 |

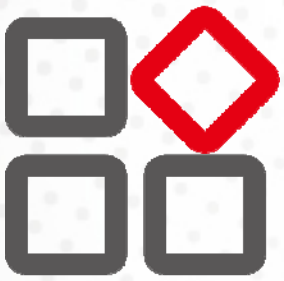
| | |
|---|---|
| | ';'.<br>**When WPA/PSK or WPA2/PSK is selected**:<br>● Select **TKIP** or **AES** as the algorithm for WPA.<br>**Security Key** - Enter **8~63** ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). |

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



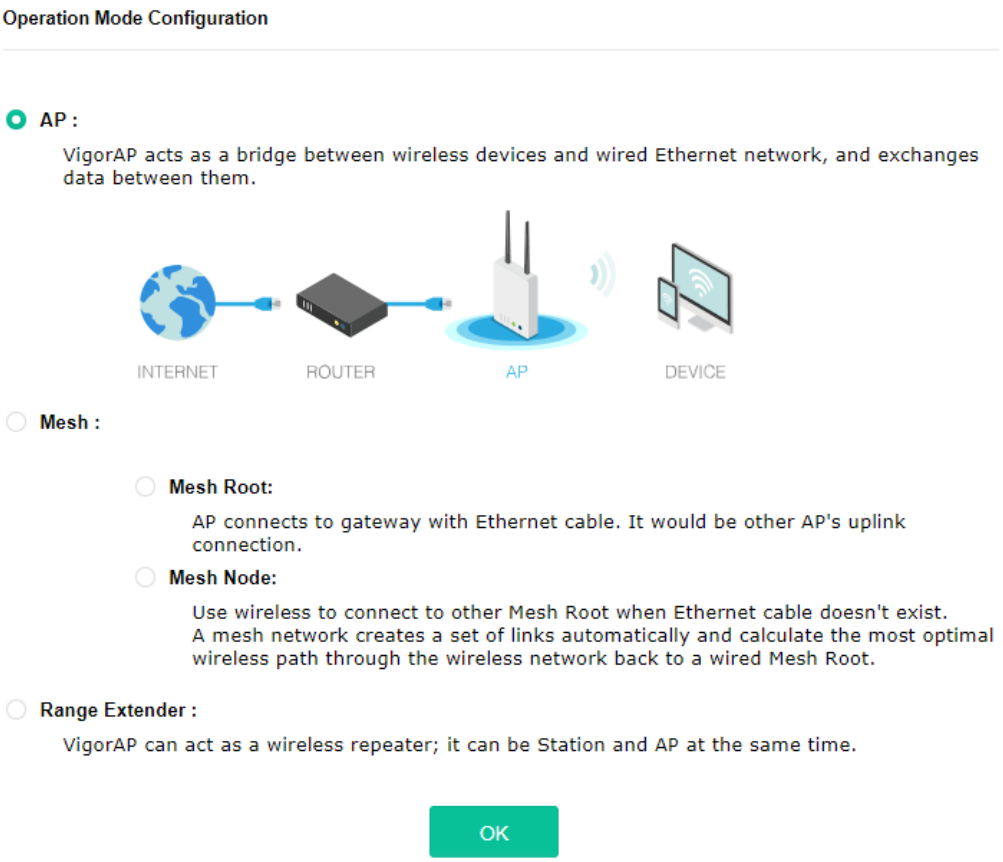
This page is left blank.

# 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.<br>**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

VigorAP 1060C is a highly integrated wireless local area network (WLAN) for 2.4/5 GHz 802.11b/g/n/ax WLAN applications. It supports channel operations of 20/40 MHz at 2.4 GHz and 20/40/80/160 MHz at 5 GHz. VigorAP 1060C can support data rates up to 2.4 GBps in 802.11ax 80/160 MHz bandwidth.

**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 1060C 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 1060C. 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.

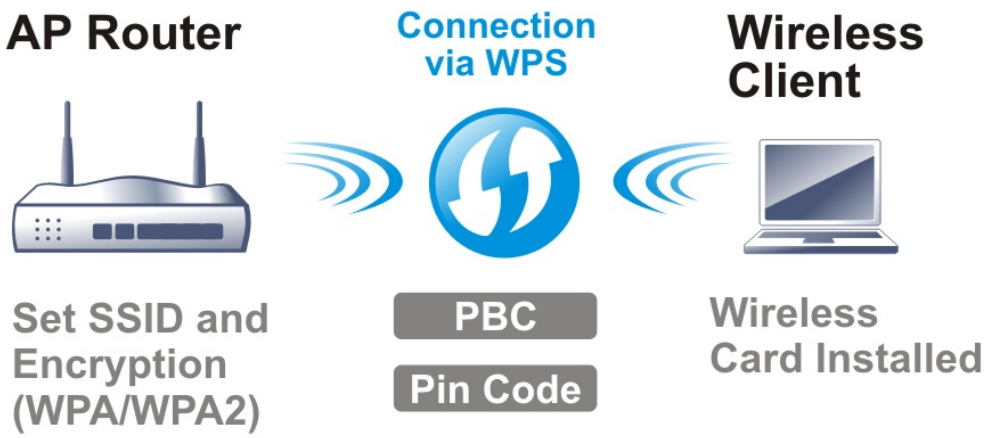
WPA (Wi-Fi Protected Access), the most dominating security mechanism in industry, is separated into two categories: WPA-personal or called WPA Pre-Share Key (WPA/PSK), and WPA-Enterprise or called WPA/802.1x.

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 1060C 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 1060C) with the encryption of WPA and WPA2.




It is the simplest way to build connection between wireless network clients and VigorAP 1060C. 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 1060C automatically.

---

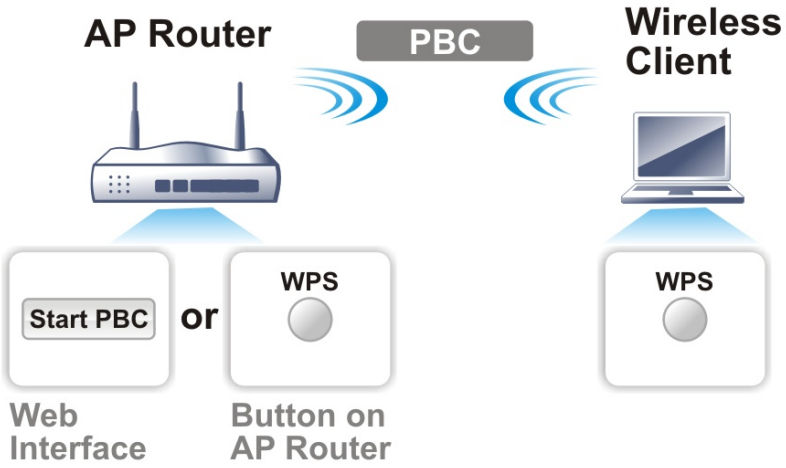
**Note:**

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

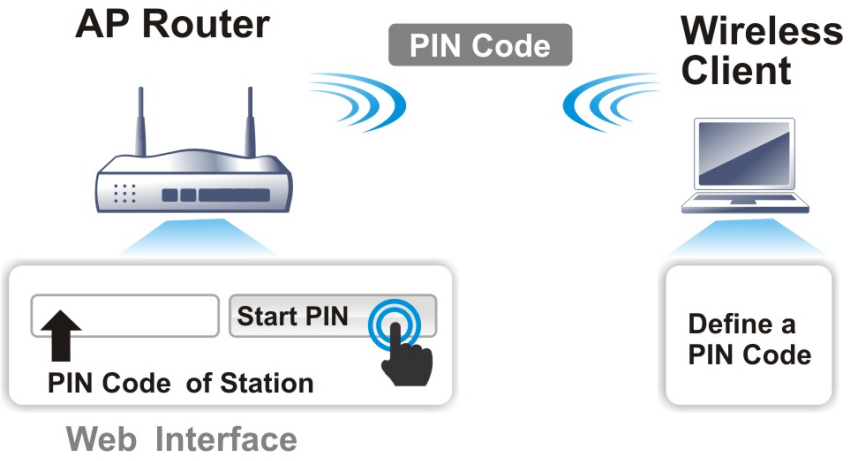
---

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 1060C series which served as an AP, press **WPS** button once on the front panel of VigorAP 1060C 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.

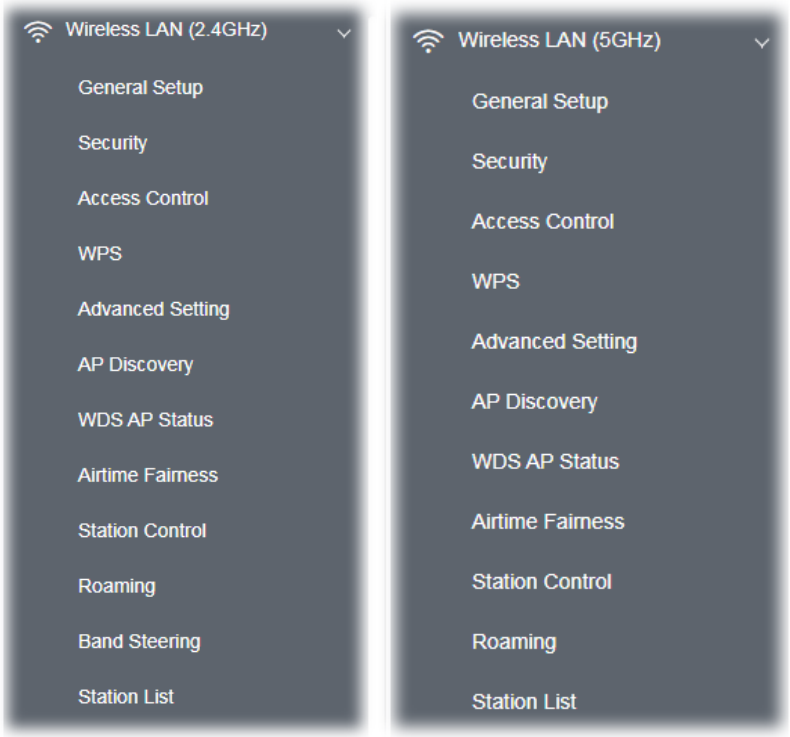



If you want to use PIN code, you have to know the PIN code specified in wireless client. Then provide the PIN code of the wireless client you wish to connect to the VigorAP 1060C.


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

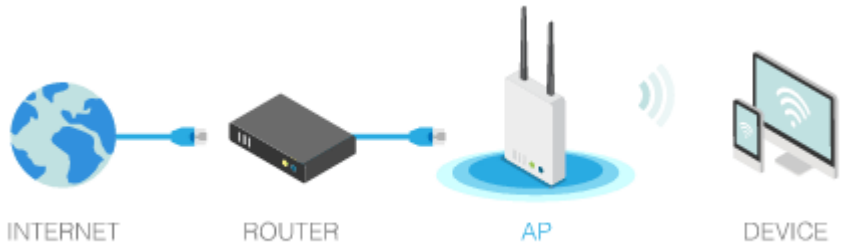
When you choose **AP** as the operation mode, the Wireless LAN menu items will include General Setup, Security, Access Control, WPS, Advanced Setting, AP Discovery, WDS AP Status, Bandwidth Management, Airtime Fairness, Station Control, Roaming, Band Steering (for 2.4GHz) and Station List.




**Note:**

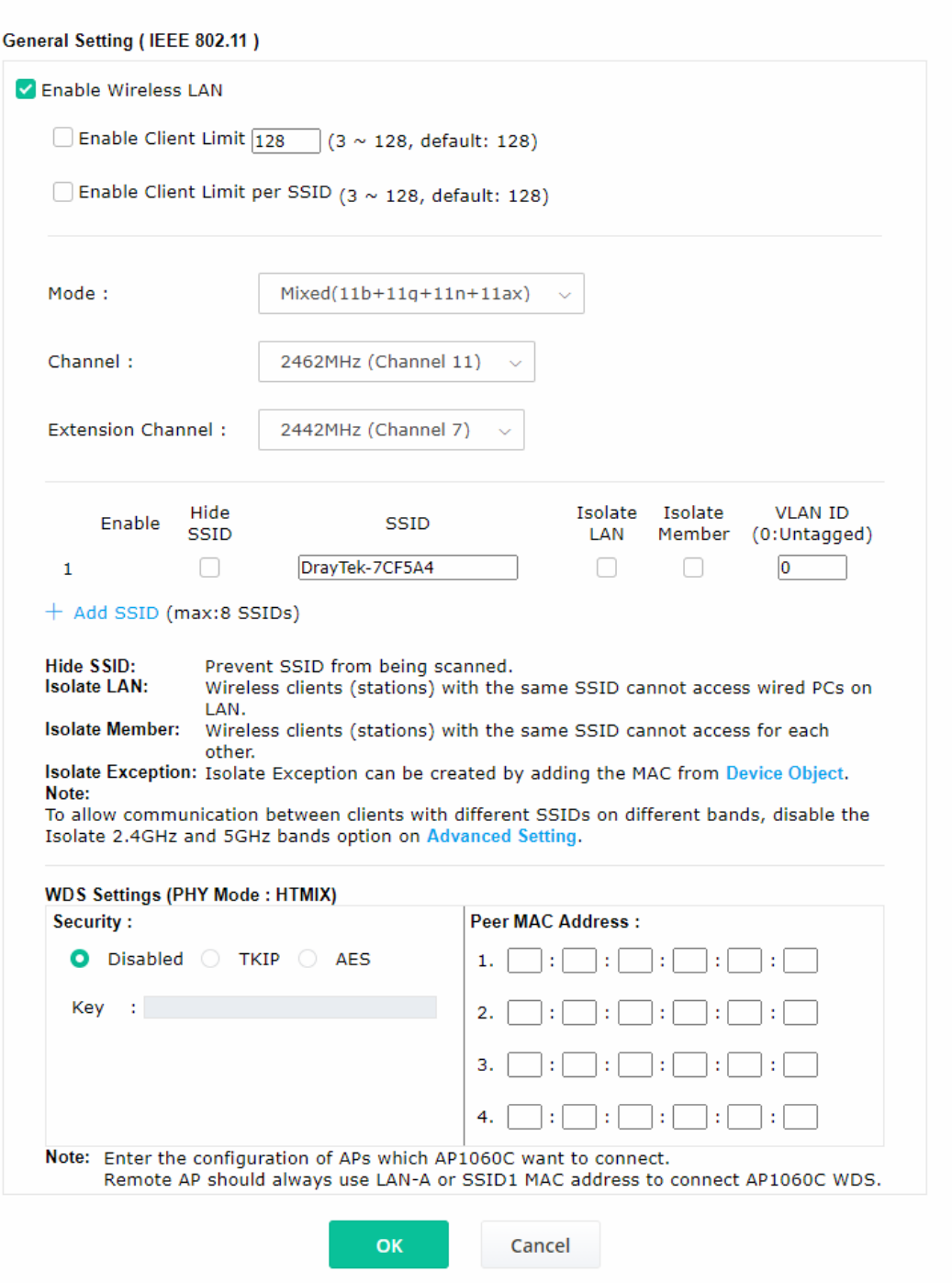
Available settings for **Wireless LAN (2.4GHz)** and **Wireless LAN (5GHz)** are almost the same, except for Band Steering.

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



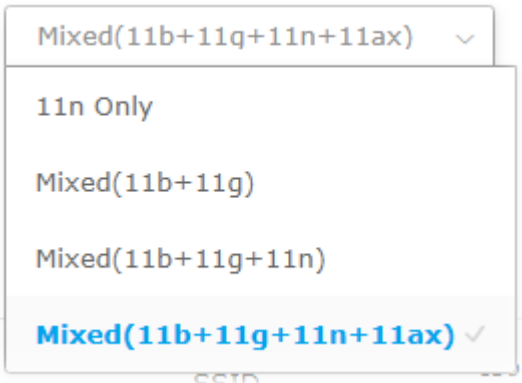
## II-3-1 General Setup

By clicking the **General Setup**, a new web page will appear so that you could select mode, channel, the SSID, the wireless channel, 2nd subnet and WDS. 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 128. |
| **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 128. |
| **Mode** | At present, VigorAP 1060C can connect to 11n only, Mixed (11b+11g), Mixed (11b+11g+11n), Mixed (11b+11g+11n+11ax), 11a Only, 11n Only(5G), Mixed (11a+11n), Mixed (11a+11n+11ac) and Mixed (11a+11n+11ac+11ax) stations simultaneously. Simply choose the default mode.<br>  <br>(for 2.4GHz)<br> <br>(for 5GHz ) |
| **Channel** | Means the channel of frequency of the wireless LAN.<br>VigorAP offers different channels for WLAN 2.4GHz and 5GHz respectively.<br>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.<br>**Filtered Out List** - It will be shown if **AutoSelect** is selected as **Channel**. Click such link to access into **Wireless LAN >> Advanced Settings** page. |
| **Extension Channel**<br>**(for 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. |
| **Enable Bridge VLAN to** | Check it to support VLAN feature within the Mesh network. |

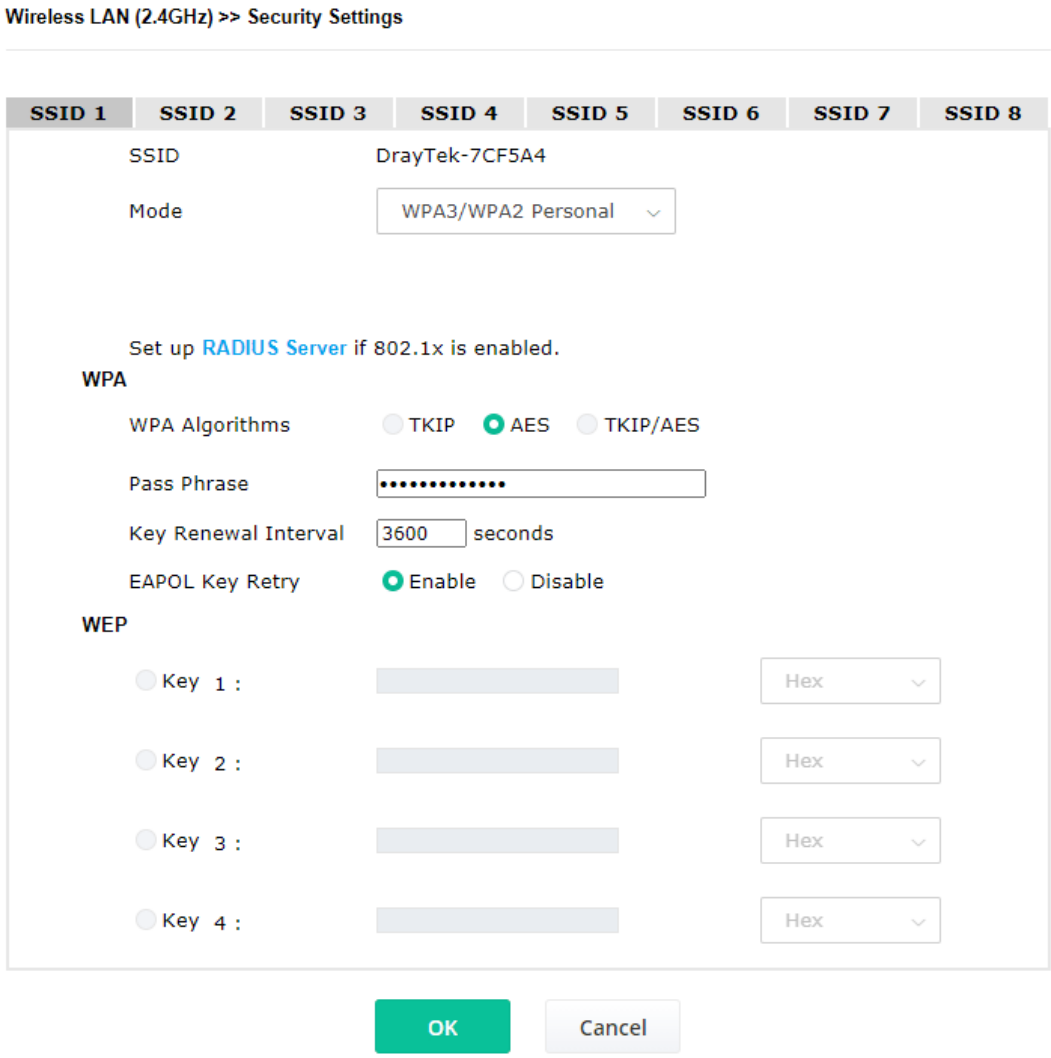
| | |
|---|---|
| **Mesh** | |
| **Enable** | Check it to enable the SSID setting. |
| **Hide SSID** | Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about VigorAP 1060C while site surveying. The system allows you to set four sets of SSID for different usage. |
| **SSID** | Set a name for VigorAP 1060C to be identified. Default settings are DrayTek-XXXXXX (the last six bytes of the MAC address). |
| **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.<br>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. |
| **+ Add SSID** | Click it to add a new SSID (up to 8 SSIDs). |
| **Security** | Select WEP, TKIP or AES as the encryption algorithm.<br>Type **8~63** ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). |
| **Peer MAC Address** | Type the peer MAC address for the access point that VigorAP 1060C 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 to 8 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.

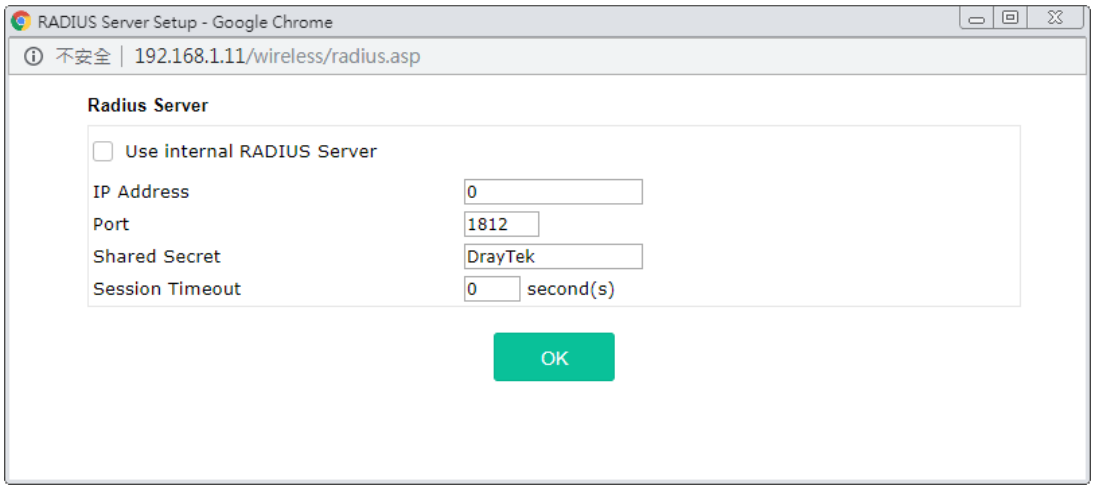



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Mode** | There are several modes provided for you to choose.<br>Below shows the modes with higher security:<br>● **WPA3 Personal, WPA3/WPA2 Personal, WPA2 Personal, WPA2/WPA Personal -** 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.<br>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. |

| | |
|---|---|
| | • **WPA3 Enterprise, WPA3/WPA2 Enterprise, WPA2 Enterprise, WPA2/WPA Enterprise -** 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.<br>• **OWE** - WPA3 also introduces a new open and secure connection mode; "Opportunistic Wireless Encryption" (OWE). It allows the clients to connect without a password, ideal for hotspot networks, but the connection between each individual client is uniquely encrypted behind the scenes.<br>Below shows the modes with basic security:<br>• **WPA Personal** - 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.<br>• **WPA Enterprise** - 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.<br>• **WEP Personal** - Accepts only WEP clients and the encryption key should be entered in WEP Key.<br>• **WEP Enterprise -** The built-in RADIUS client feature enables VigorAP 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.<br>• **None** - The encryption mechanism is turned off. |
| **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.<br>Click **Enable** to make sure that the key will be installed and used once in order to prevent key reinstallation attack. |
| **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.



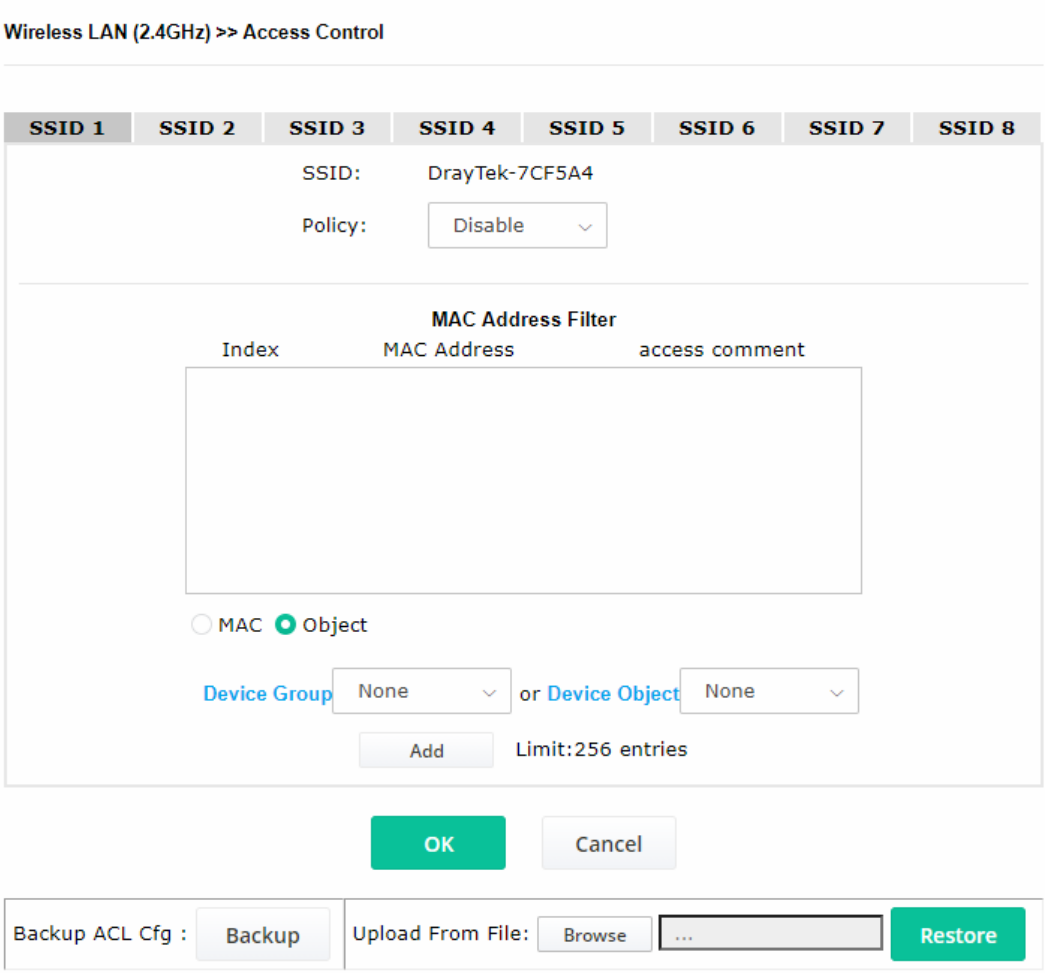

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Use internal RADIUS Server** | There is a RADIUS server built in VigorAP 1060C 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.<br>Besides, if you want to use the external RADIUS server for authentication, do not check this box.<br>Please refer to the section, **IV-1-1 RADIUS Server** to configure settings for internal server of VigorAP 1060C. |
| **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.

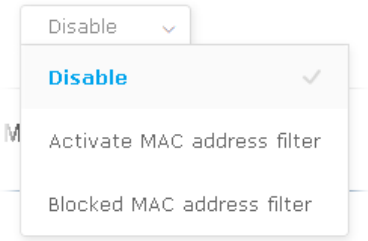
## II-3-3 Access Control

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:

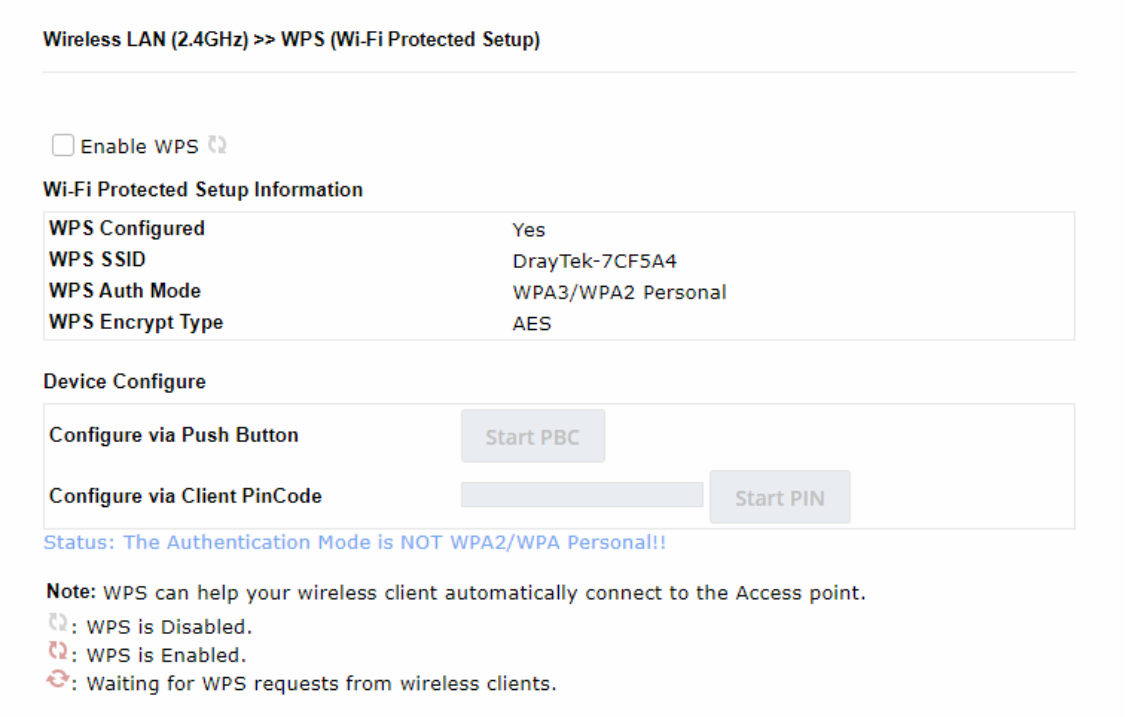
| Item | Description |
|---|---|
| **Policy** | Select to enable any one of the following policy or disable the policy. Choose **Activate MAC address filter** to type in the MAC addresses for other clients in the network manually. Choose **Blocked MAC address filter,** so that all of the devices with the MAC addresses listed on the MAC Address Filter table will be blocked and cannot access into VigorAP 1060C. |

| | |
|---|---|
| |  |
| **MAC Address Filter** | Display all MAC addresses that are edited before. |
| **MAC** | **Client's MAC Address -** Manually enter the MAC address of wireless client.<br>**Add -** Add a new MAC address into the list.<br>**Delete -** Delete the selected MAC address in the list.<br>**Edit -** Edit the selected MAC address in the list. |
| **Object** | In addition to enter the MAC address of the device manually, you can<br>**Device Group** - Select one of the existed device groups and click **Add**. All the devices belonging to the selected group will be shown on the MAC Address Filter table.<br>**Device Object** - Select one of the existed device object and click **Add**. The MAC address of the device will be shown on the MAC Address Filter table. |
| **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.

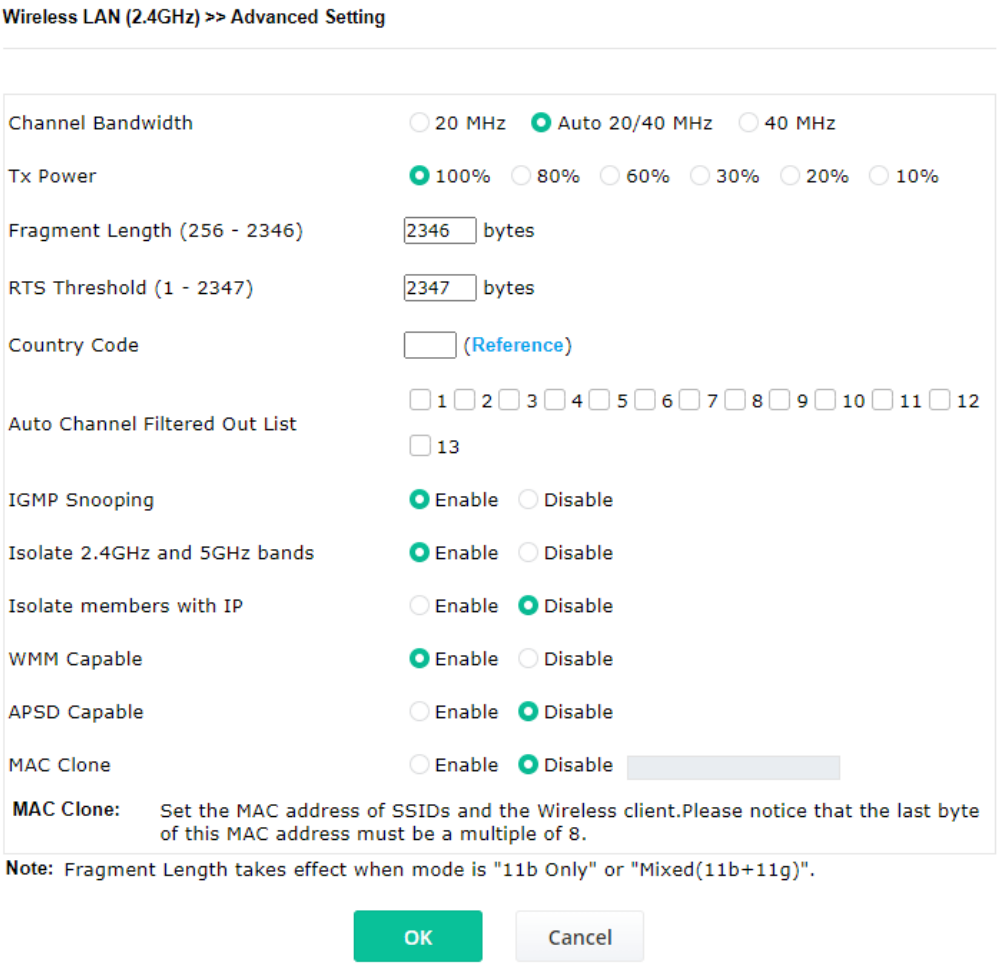



Available settings are explained as follows:

| 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 1060C 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 1060C. Only WPA2/PSK and WPA/PSK support WPS. |
| **WPS Encrypt Type** | Display encryption mode (None, WEP, TKIP, AES, etc.) of VigorAP 1060C. |
| **Configure via Push Button** | Click **Start PBC** to invoke Push-Button style WPS setup procedure. VigorAP 1060C will wait for WPS requests from wireless clients about two minutes. Both ACT and 2.4G WLAN LEDs on VigorAP 1060C 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 1060C 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 Bandwidth** | **20 MHz-** The device will use 20MHz for data transmission and receiving between the AP and the stations.<br><br>**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.<br><br>**40 MHz-** The device will use 40MHz for data transmission and receiving between the AP and the stations. It is for wireless LAN 2.4GHz only.<br><br>**Auto 20/40 /80 MHz -** The device will use 20/40/80 MHz channel bandwidth for data transmission and receiving between the AP and the stations.<br><br>**Auto 20/40 /80/160 MHz -** The device will use 20/40/80/160 MHz channel bandwidth for data transmission and receiving between the AP and the stations. |
| **Tx Power** | The default setting is the maximum (100%). Lowering down the value may degrade range and throughput of wireless. |

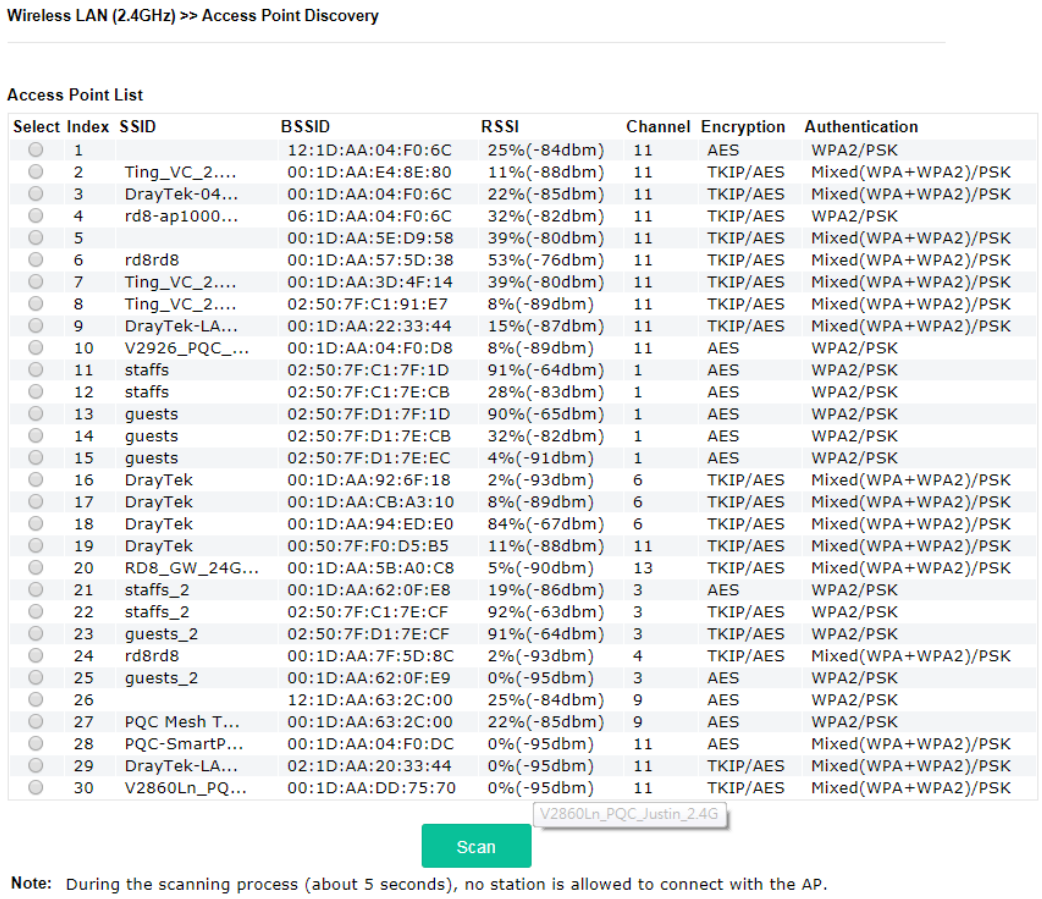
| | |
|---|---|
| **Fragment Length** | Set the Fragment threshold of wireless radio. Do not modify default value if you don't know what it is, default value is 2346. |
| **RTS Threshold** | Minimize the collision (unit is bytes) between hidden stations to improve wireless performance.<br>Set the RTS 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** | Click **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.<br>For WLAN 2.4GHz and 5GHz set with the same SSID name:<br>● 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.<br>● 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".<br>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.<br>The default setting is **Disable**. |
| **MAC Clone**<br>**(for 2.4GHz only)** | 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. |

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

## II-3-6 AP Discovery

VigorAP 1060C 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 VigorAP.

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 | | 12:1D:AA:04:F0:6C | 25%(-84dbm) | 11 | AES | WPA2/PSK |
| ○ | 2 | Ting_VC_2.... | 00:1D:AA:E4:8E:80 | 11%(-88dbm) | 11 | TKIP/AES | Mixed(WPA+WPA2)/PSK |
| ○ | 3 | DrayTek-04... | 00:1D:AA:04:F0:6C | 22%(-85dbm) | 11 | TKIP/AES | Mixed(WPA+WPA2)/PSK |
| ○ | 4 | rd8-ap1000... | 06:1D:AA:04:F0:6C | 32%(-82dbm) | 11 | TKIP/AES | WPA2/PSK |
| ○ | 5 | | 00:1D:AA:5E:D9:58 | 39%(-80dbm) | 11 | TKIP/AES | Mixed(WPA+WPA2)/PSK |
| ○ | 6 | rd8rd8 | 00:1D:AA:57:5D:38 | 53%(-76dbm) | 11 | TKIP/AES | Mixed(WPA+WPA2)/PSK |
| ○ | 7 | Ting_VC_2.... | 00:1D:AA:3D:4F:14 | 39%(-80dbm) | 11 | TKIP/AES | Mixed(WPA+WPA2)/PSK |
| ○ | 8 | Ting_VC_2.... | 02:50:7F:C1:91:E7 | 8%(-89dbm) | 11 | TKIP/AES | Mixed(WPA+WPA2)/PSK |
| ○ | 9 | DrayTek-LA... | 00:1D:AA:22:33:44 | 15%(-87dbm) | 11 | TKIP/AES | Mixed(WPA+WPA2)/PSK |
| ○ | 10 | V2926_PQC_... | 00:1D:AA:04:F0:D8 | 8%(-89dbm) | 11 | AES | WPA2/PSK |
| ○ | 11 | staffs | 02:50:7F:C1:7F:1D | 91%(-64dbm) | 1 | AES | WPA2/PSK |
| ○ | 12 | staffs | 02:50:7F:C1:7E:CB | 28%(-83dbm) | 1 | AES | WPA2/PSK |
| ○ | 13 | guests | 02:50:7F:D1:7F:1D | 90%(-65dbm) | 1 | AES | WPA2/PSK |
| ○ | 14 | guests | 02:50:7F:D1:7E:CB | 32%(-82dbm) | 1 | AES | WPA2/PSK |
| ○ | 15 | guests | 02:50:7F:D1:7E:EC | 4%(-91dbm) | 1 | AES | WPA2/PSK |
| ○ | 16 | DrayTek | 00:1D:AA:92:6F:18 | 2%(-93dbm) | 6 | TKIP/AES | Mixed(WPA+WPA2)/PSK |
| ○ | 17 | DrayTek | 00:1D:AA:CB:A3:10 | 8%(-89dbm) | 6 | TKIP/AES | Mixed(WPA+WPA2)/PSK |
| ○ | 18 | DrayTek | 00:1D:AA:94:ED:E0 | 84%(-67dbm) | 6 | TKIP/AES | Mixed(WPA+WPA2)/PSK |
| ○ | 19 | DrayTek | 00:50:7F:F0:D5:B5 | 11%(-88dbm) | 11 | TKIP/AES | Mixed(WPA+WPA2)/PSK |
| ○ | 20 | RD8_GW_24G... | 00:1D:AA:5B:A0:C8 | 5%(-90dbm) | 13 | TKIP/AES | Mixed(WPA+WPA2)/PSK |
| ○ | 21 | staffs_2 | 00:1D:AA:62:0F:E8 | 19%(-86dbm) | 3 | AES | WPA2/PSK |
| ○ | 22 | staffs_2 | 02:50:7F:C1:7E:CF | 92%(-63dbm) | 3 | TKIP/AES | WPA2/PSK |
| ○ | 23 | guests_2 | 02:50:7F:D1:7E:CF | 91%(-64dbm) | 3 | TKIP/AES | WPA2/PSK |
| ○ | 24 | rd8rd8 | 00:1D:AA:7F:5D:8C | 2%(-93dbm) | 4 | TKIP/AES | Mixed(WPA+WPA2)/PSK |
| ○ | 25 | guests_2 | 00:1D:AA:62:0F:E9 | 0%(-95dbm) | 3 | AES | WPA2/PSK |
| ○ | 26 | | 12:1D:AA:63:2C:00 | 25%(-84dbm) | 9 | AES | WPA2/PSK |
| ○ | 27 | PQC Mesh T... | 00:1D:AA:63:2C:00 | 22%(-85dbm) | 9 | AES | WPA2/PSK |
| ○ | 28 | PQC-SmartP... | 00:1D:AA:04:F0:DC | 0%(-95dbm) | 11 | AES | Mixed(WPA+WPA2)/PSK |
| ○ | 29 | DrayTek-LA... | 02:1D:AA:20:33:44 | 0%(-95dbm) | 11 | TKIP/AES | Mixed(WPA+WPA2)/PSK |
| ○ | 30 | V2860Ln_PQ... | 00:1D:AA:DD:75:70 | 0%(-95dbm) | 11 | TKIP/AES | Mixed(WPA+WPA2)/PSK |

V2860Ln_PQC_Justin_2.4G

Scan

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

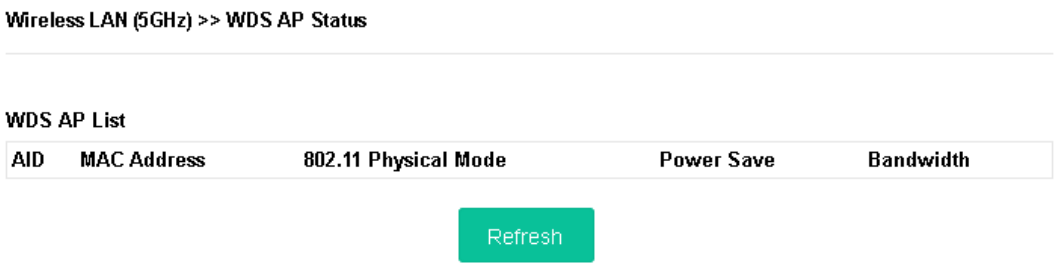
Each item is explained as follows:

| Item | Description |
|---|---|
| **SSID** | Display the SSID of the AP scanned by VigorAP 1060C. |
| **BSSID** | Display the MAC address of the AP scanned by VigorAP 1060C. |
| **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 1060C. |
| **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 |
| **AP's MAC Address / AP's SSID** | Display the MAC address and SSID of the AP selected from the Access Point. |

| | |
|---|---|
| **Add** | Click it to add the AP selected from the Access Point List (with the same channel width) to the WDS Settings as peer' s setting. |

## II-3-7 WDS AP Status

VigorAP 1060C 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.




It is available for wireless LAN (5GHz) only.

## II-3-8 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.

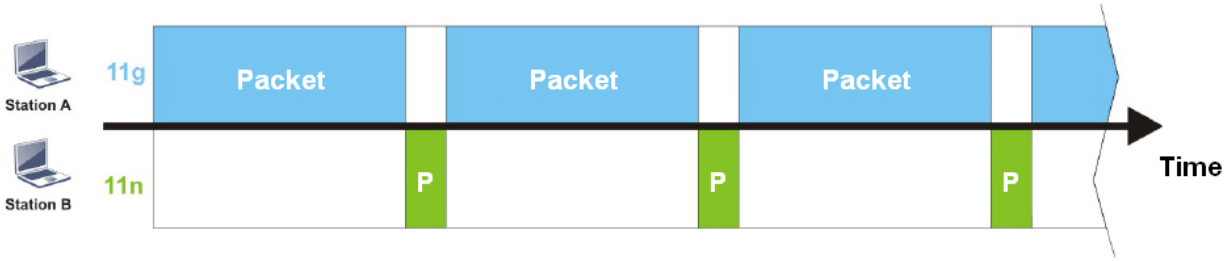
With airtime fairness, every client at a given quality-of-service level has equal access to the network's airtime.

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

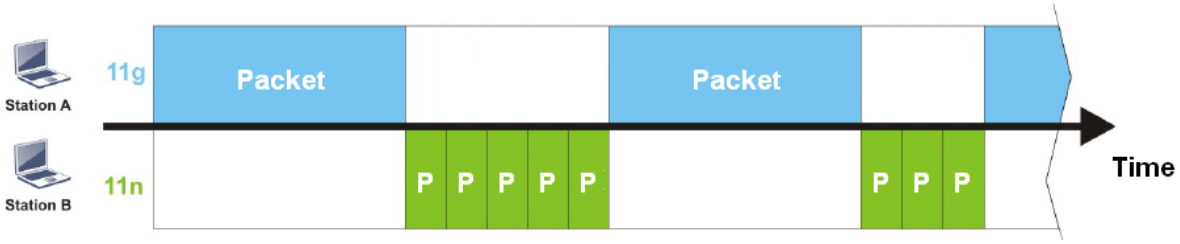
The principle behind the IEEE802.11 channel access mechanisms is that each station has ***equal probability*** to access the channel. When wireless stations have similar data rate, this principle leads to a fair result. In this case, stations get similar channel access time which is called airtime.

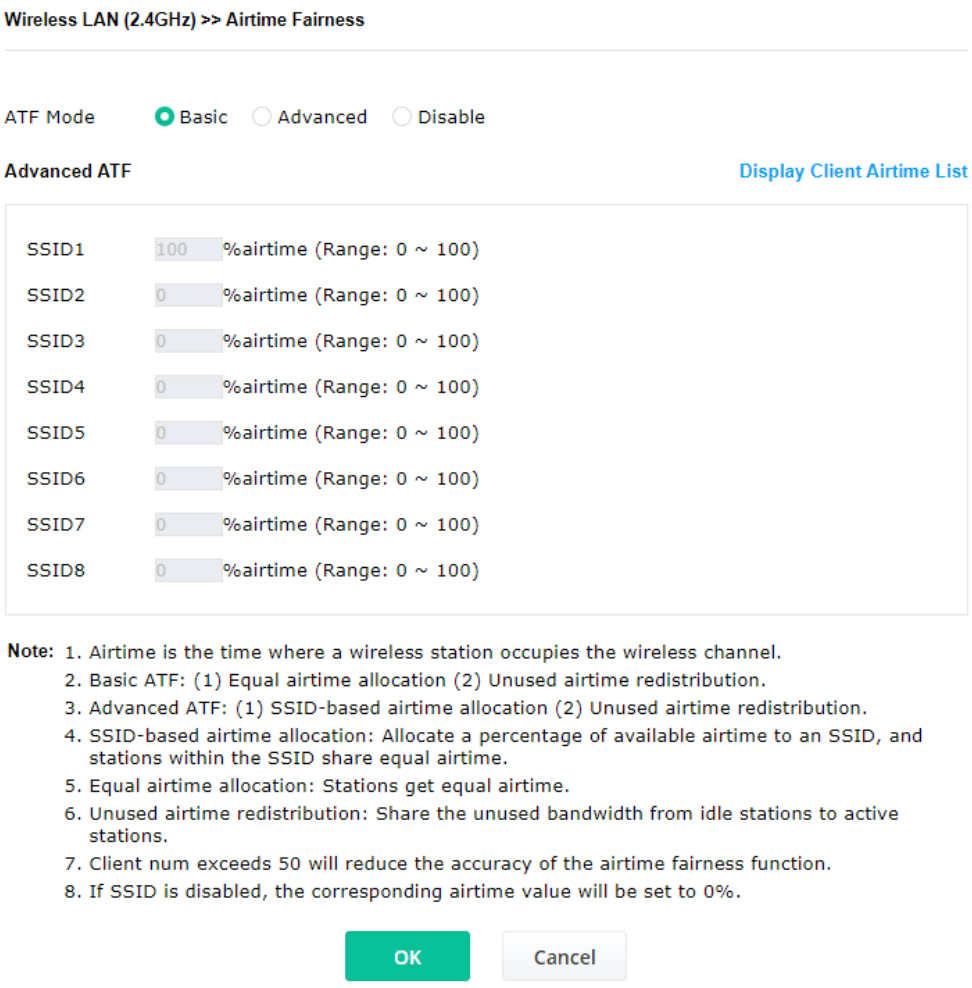
However, when stations have various data rate (e.g., 11g, 11n), the result is not fair. The slow stations (11g) work in their slow data rate and occupy too much airtime, whereas the fast stations (11n) become much slower.

Take the following figure as an example, both Station A(11g) and Station B(11n) transmit data packets through VigorAP 1060C. 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, Hardware-Based Airtime Fairness (ATF) is added for VigorAP 1060C. Basic Mode of ATF tries to assign equal airtime to each station (A/B). In the following figure, Station B (11n) has a higher probability to send data packets than Station A(11g). In this way, Station B (fast rate) gets fair airtime and its speed is not limited by Station A(slow rate).




Available settings are explained as follows:

| Item | Description |
|---|---|
| **ATF Mode** | **Basic -** Select to enable the basic airtime fairness settings.<br>**Advanced -** Select to enable the advanced airtime fairness settings.<br>**Disable -** Select to disable the ATF function. |
| **Advanced ATF** | It is SSID-based airtime allocation.<br>The downstream or upstream from FTP, HTTP or some P2P applications will occupy large of bandwidth and affect the applications for other programs. Adjust the value (0 ~ 100) of airtime bandwidth for each SSID. |
| **Display Client Airtime List** | Click to get a table of current clients which share the bandwidth via airtime fairness. |

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

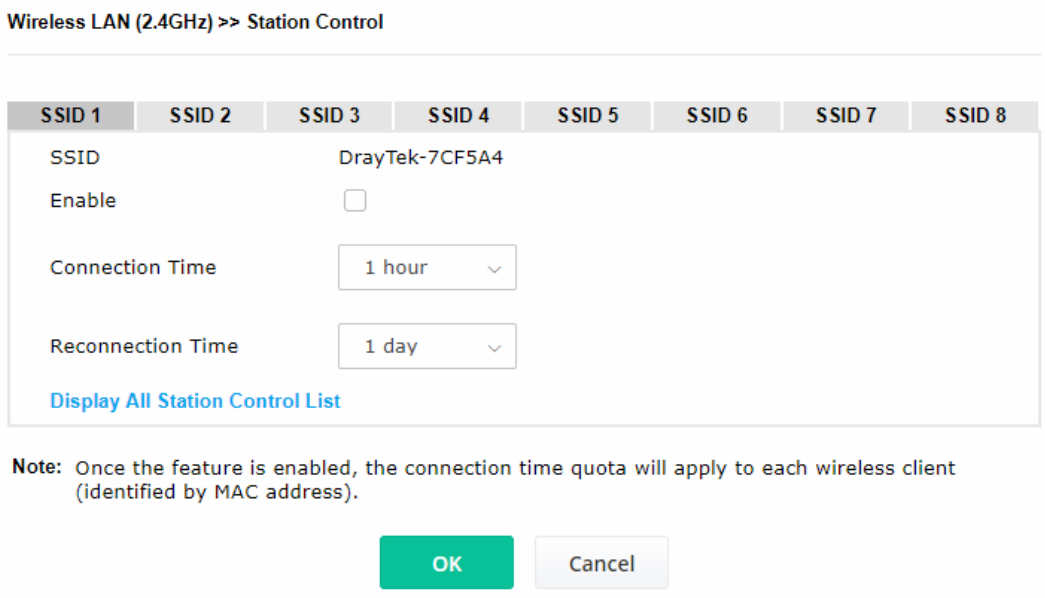
## II-3-9 Station Control

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:

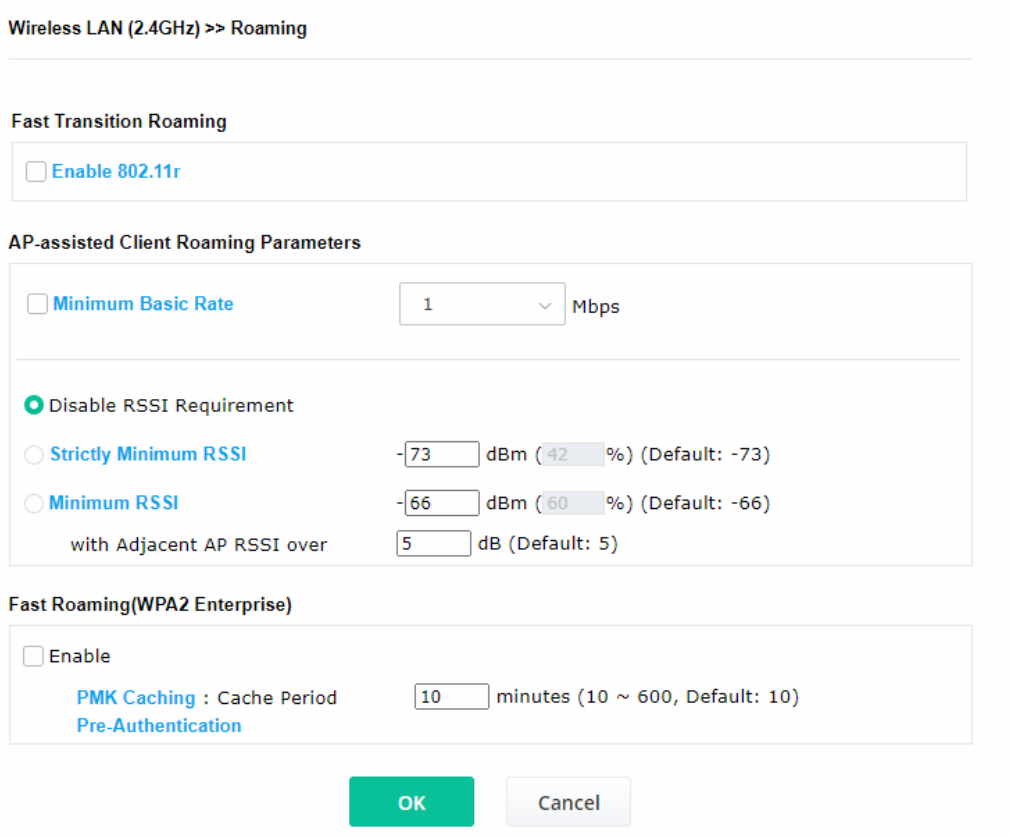
| Item | Description |
| --- | --- |
| **SSID** | Display the SSID that the wireless station will use it to connect with Vigor router. |
| **Enable** | Check the box to enable the station control function. |
| **Connection Time / Reconnection Time** | Use the drop down list to choose the duration for 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-3-10 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:

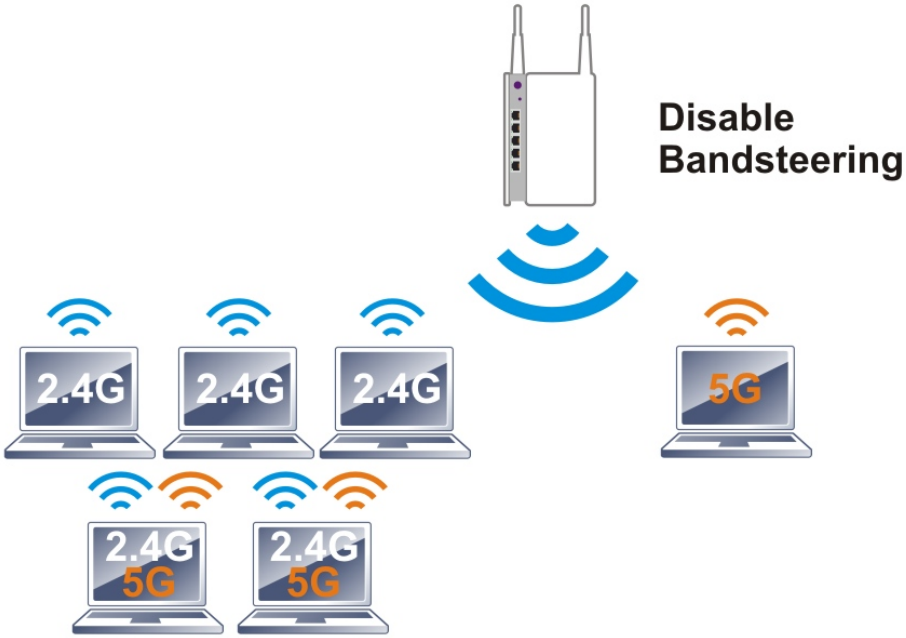
| Item | Description |
|---|---|
| **Fast Transition Roaming** | Fast Transition Roaming can save reconnect time with the way (following the 802.11r standard) of data exchange in advance between two VigorAP devices.<br>**Enable 802.11r** - Check the box to perform pre-authentication based on 802.11r standard. This feature is available for WPA2 Enterprise, WPA2 Personal, WPA3/WPA2 Enterprise or WPA3/WPA2 Personal. |
| **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 1060C 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.<br>**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 1060C 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.<br>**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 1060C will terminate the network connection for that wireless station.<br>**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 1060C, VigorAP 1060C will terminate the network connection for that wireless station. Later, the wireless station can connect to the adjacent AP (with better RSSI).<br>• **With Adjacent AP RSSI over –** Specify a value as a threshold. |
| **Fast Roaming (WPA2 Enterprise)** | **Enable –** Check the box to enable fast roaming configuration.<br>**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 Enterprise** mode.<br>**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)<br>**Enable** - Enable IEEE 802.1X Pre-Authentication.<br>**Disable** - Disable IEEE 802.1X Pre-Authentication. |

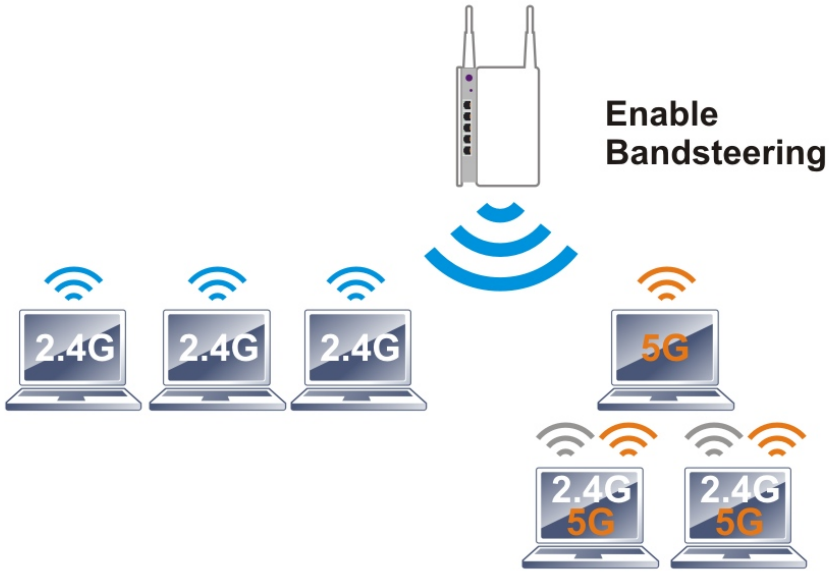
After finishing this web page configuration, please click **OK** to save the settings.

## II-3-11 Band Steering (for Wireless LAN (2.4GHz))

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.



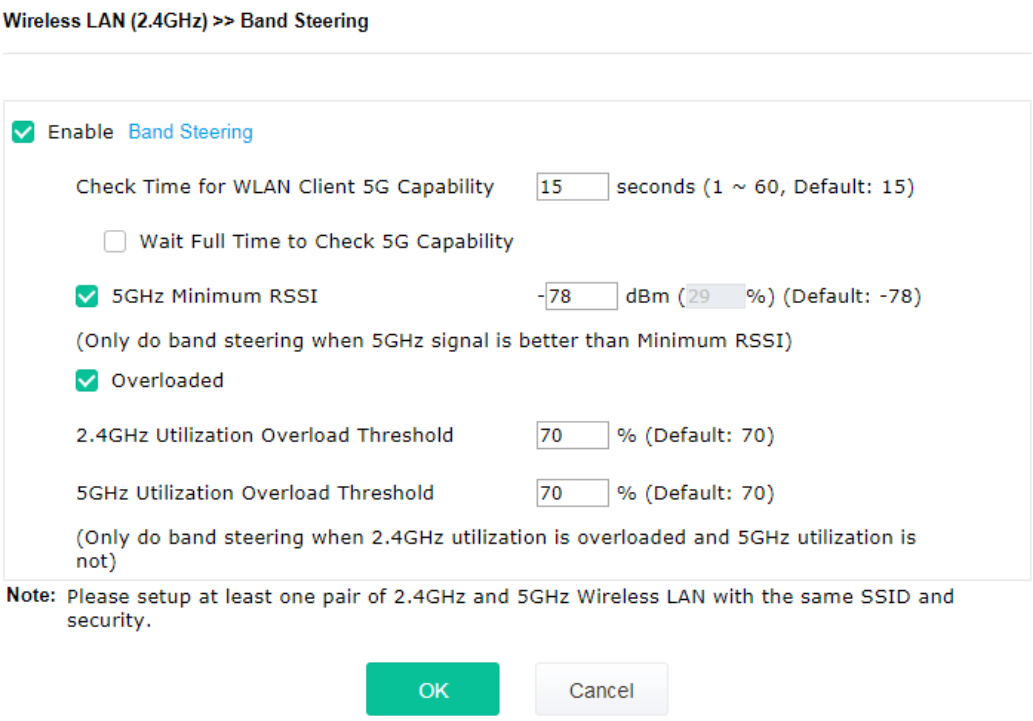

If dual-band is detected, the AP will let the wireless client connect to less congested wireless LAN, such as 5GHz to prevent from network congestion.



**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:



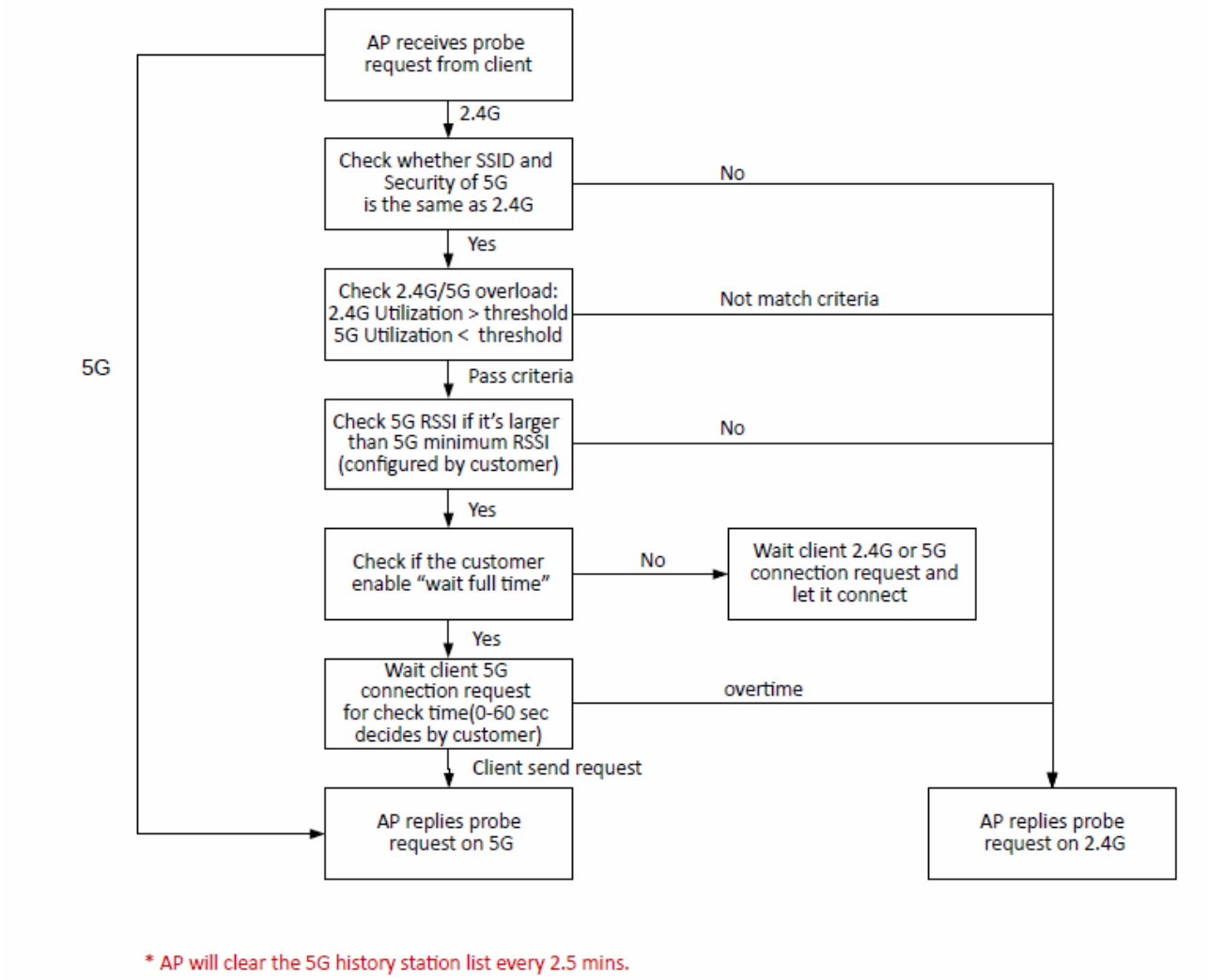

Available settings are explained as follows:

| 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.<br>**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.<br>**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.<br>**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.<br>**Overloaded** – If it is enabled, VigorAP will activate the band steering |

| | |
|---|---|
| | according to the conditions set below.<br>• **2.4GHz Utilization Overload Threshold** – The default setting is 70%. It can define the network congestion for 2.4GHz.<br>• **5GHz Utilization Overload Threshold** – The default setting is 70%. It can define the network congestion for 5GHz.<br>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.

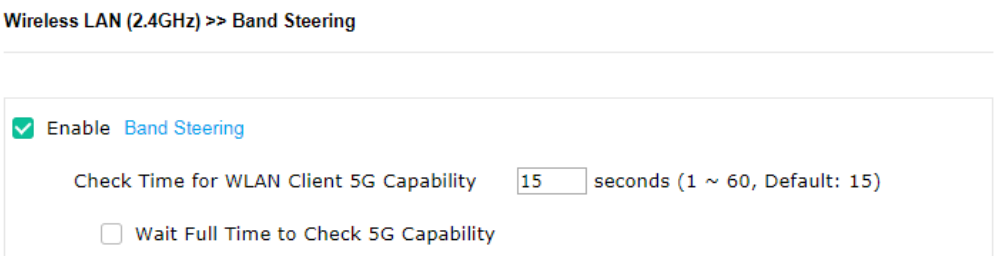
Below shows how Band Steering works.



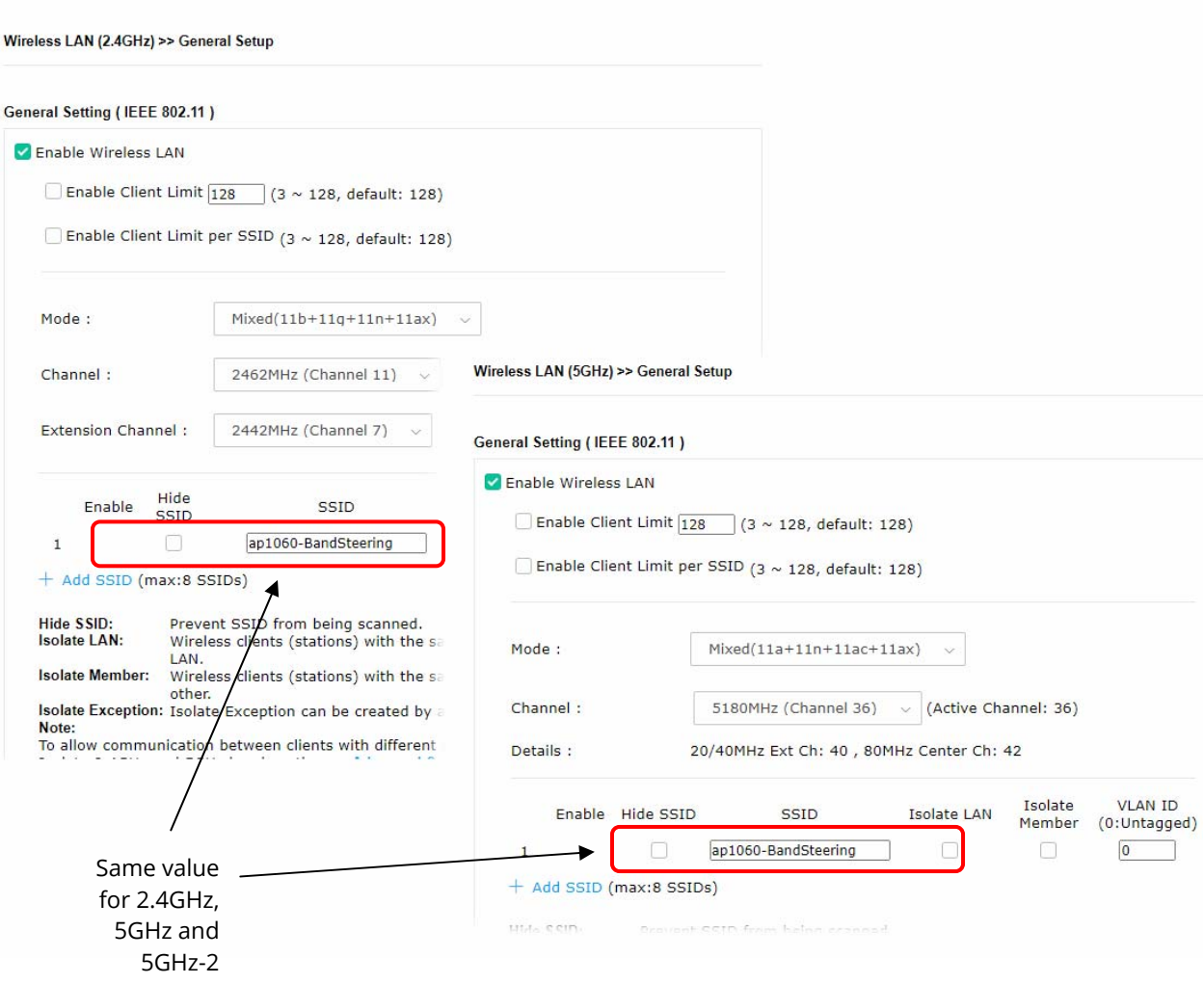

* AP will clear the 5G history station list every 2.5 mins.

**How to Use Band Steering?**

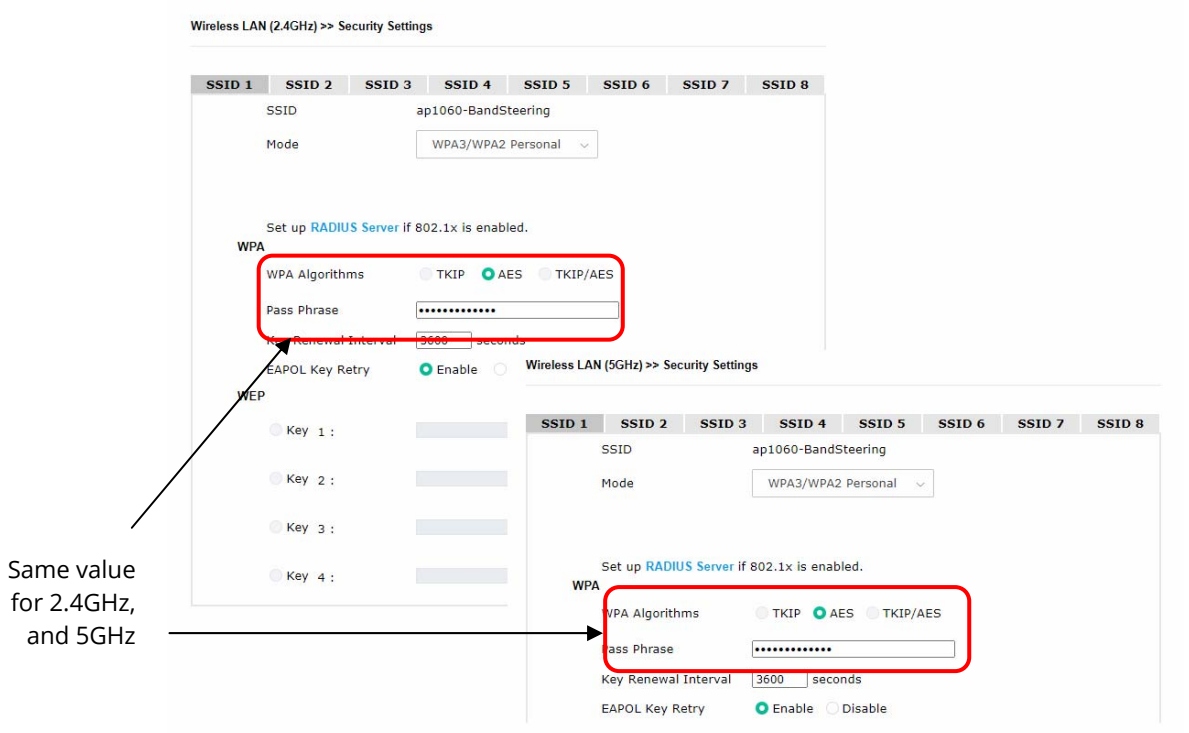
1. Open **Wireless LAN(2.4GHz)>>Band Steering**.
2. Check the box of **Enable Band Steering** and use the default value (15) for check time setting.




3. Click **OK** to save the settings.
4. Open **Wireless LAN (2.4GHz)>>General Setup** and **Wireless LAN (5GHz)>>General Setup**. Configure SSID as *ap1060-BandSteering* for these pages. Click **OK** to save the settings.



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



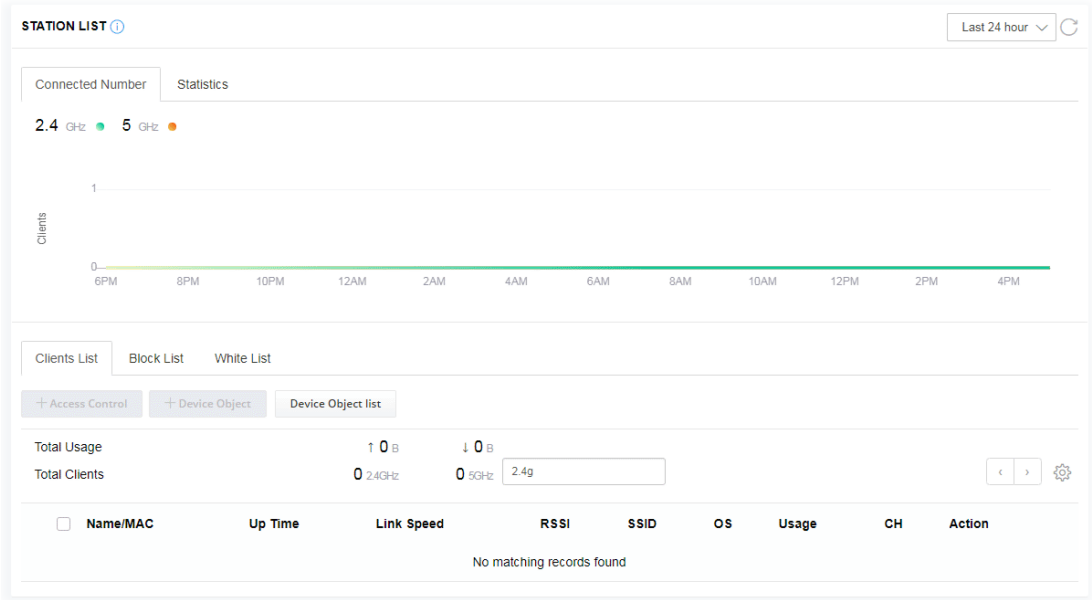

6. Now, VigorAP 1060C will let the wireless clients connect to less congested wireless LAN, such as 5GHz to prevent from network congestion.

# II-3-12 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

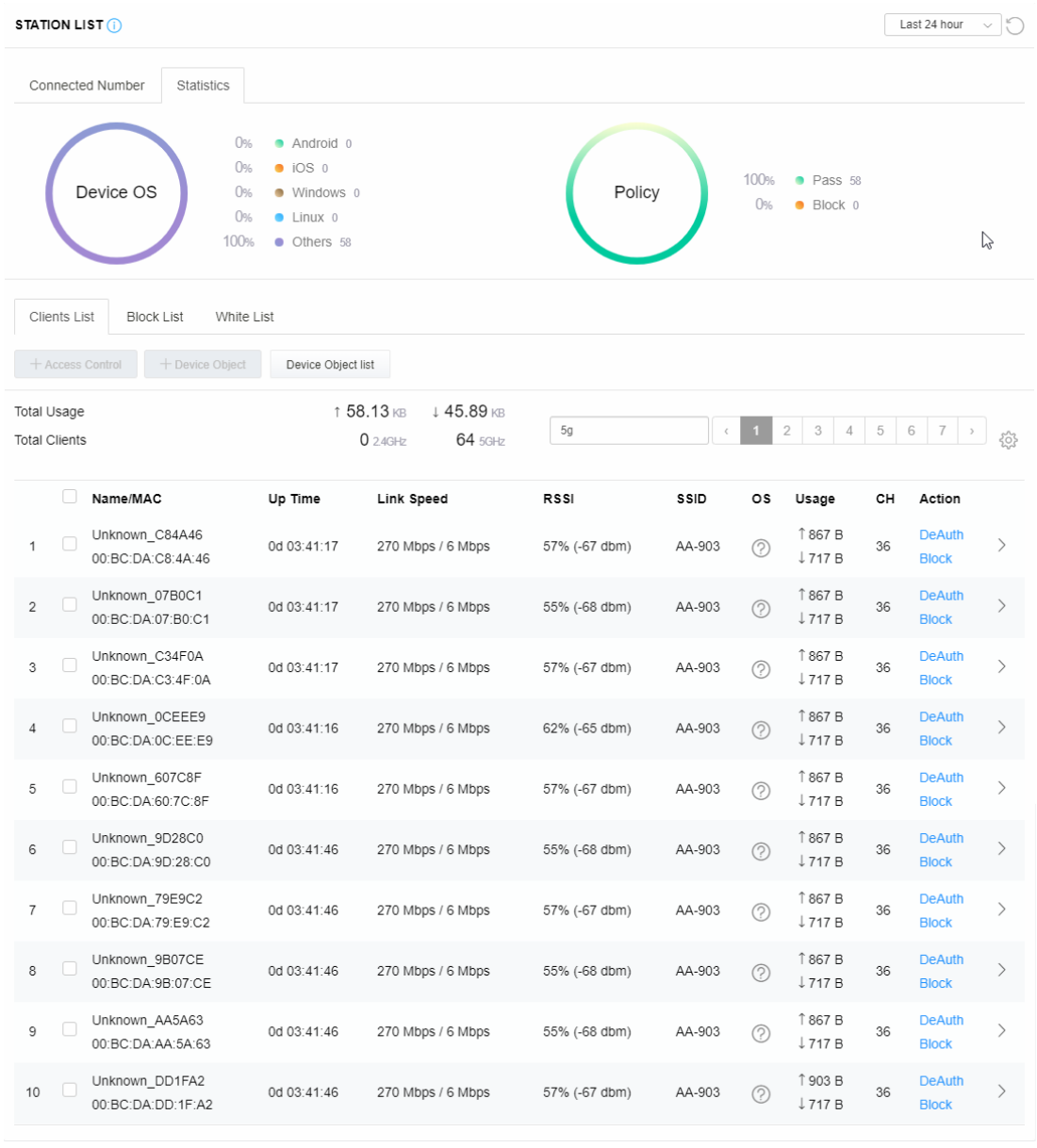
### II-3-12-1 Connected Number

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



### II-3-12-2 Statistics

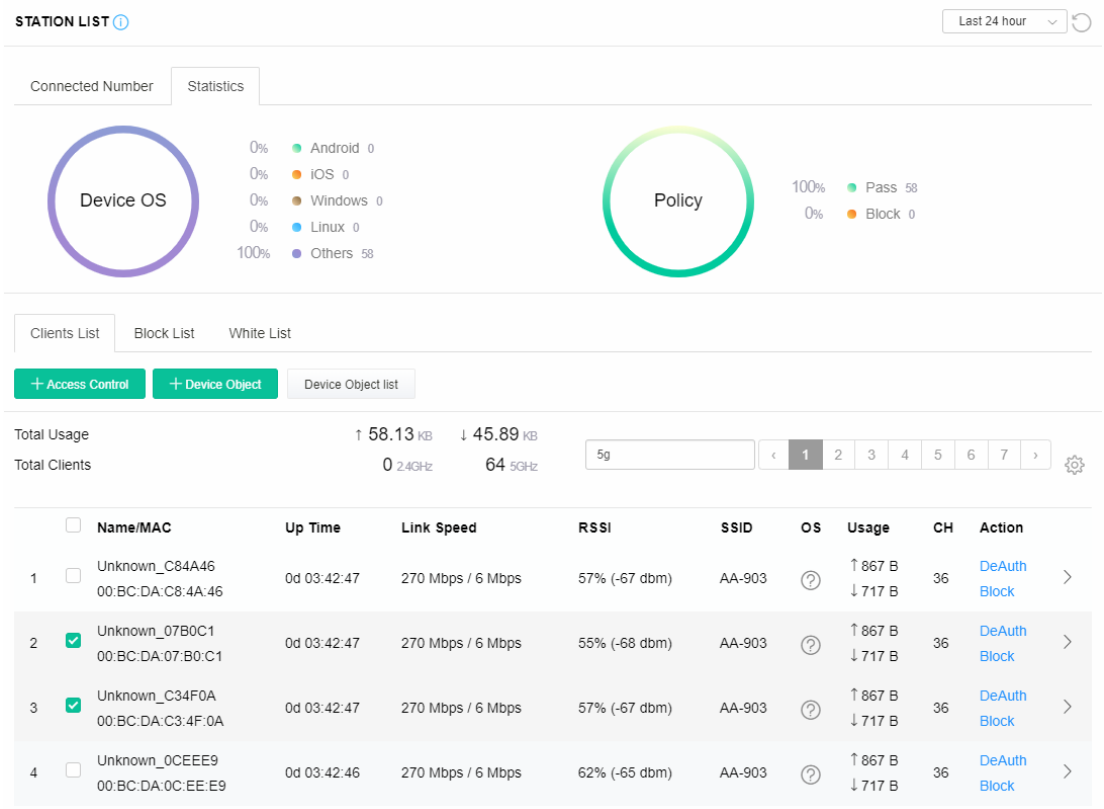
The number of detected devices and the number of device(s) passed/blocked according to the policy specified in **Mobile Device Management>>Policy** can be illustrated as doughnut chart.



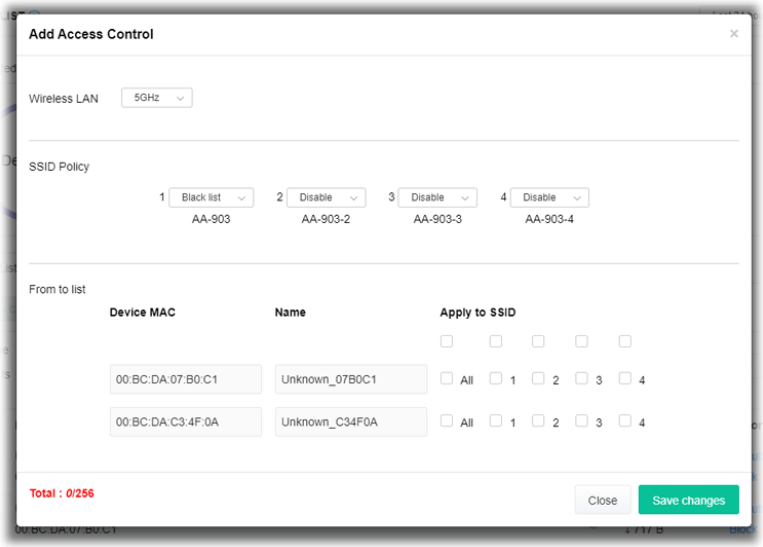

| | | Name/MAC | Up Time | Link Speed | RSSI | SSID | OS | Usage | CH | Action |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | | Unknown_C84A46<br>00:BC:DA:C8:4A:46 | 0d 03:41:17 | 270 Mbps / 6 Mbps | 57% (-67 dbm) | AA-903 | | ↑867 B<br>↓717 B | 36 | DeAuth<br>Block |
| 2 | | Unknown_07B0C1<br>00:BC:DA:07:B0:C1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

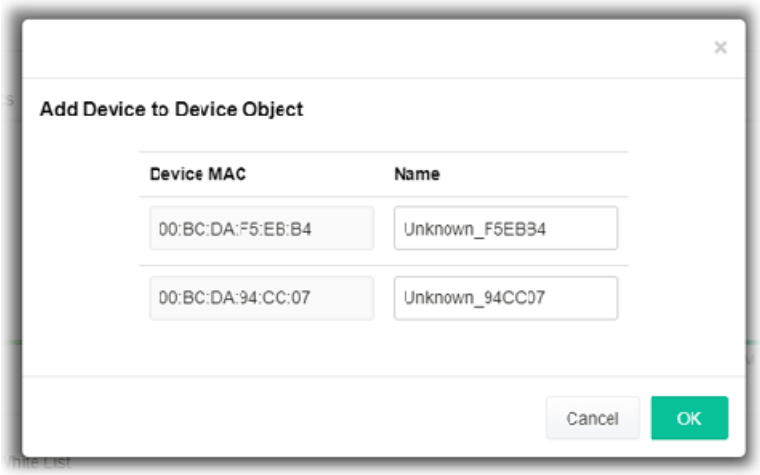
### II-3-12-3 Clients List

The client list displays all the stations connecting to VigorAP.



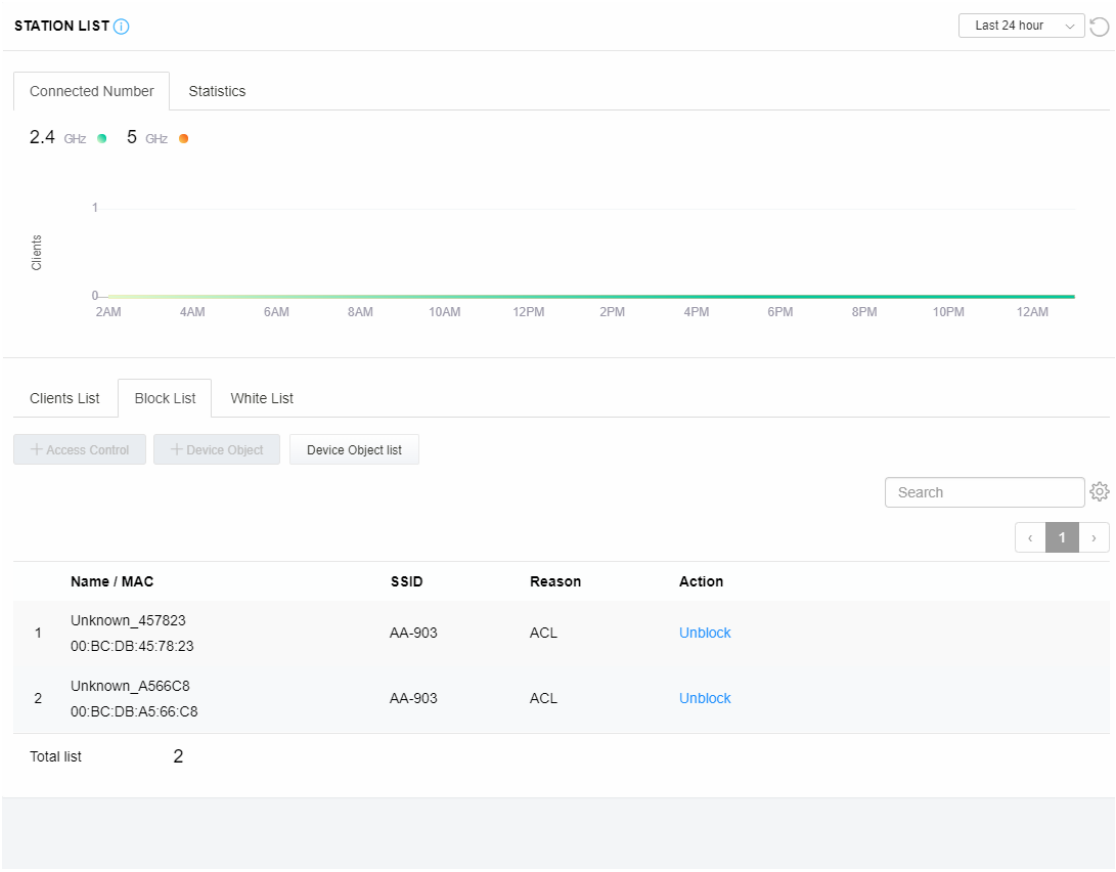

Available settings are explained as follows:

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

| | |
|---|---|
| | control.<br>**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.<br>**Close** - Exit this page without saving any changes.<br>**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.<br>  <br>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.<br> |
| **Clients List** | Display the stations connecting to this Vigor device.<br>**Total Usage -** Display<br>**Total Clients -** Display the number of the clients using 2.4GHz<br>**Name / MAC -** Display the host name / MAC address of the connecting client.<br>**Up Time** - Display the connection time.<br>**Link Speed**- Display the link speed.<br>**RSSI** - Display the RSSI value.<br>**SSID** - Display the SSID the client used for connecting VigorAP.<br>**OS** - Display the OS of the client.<br>**Usage** - Display the bandwidth usage (up and down) of the client.<br>**CH** - Display the channel used by the client.<br>**Action** - Display the authentication method used by the client, and if it is on block list or white list. |

### II-3-12-4 Block List

This page displays information of the stations under block list.

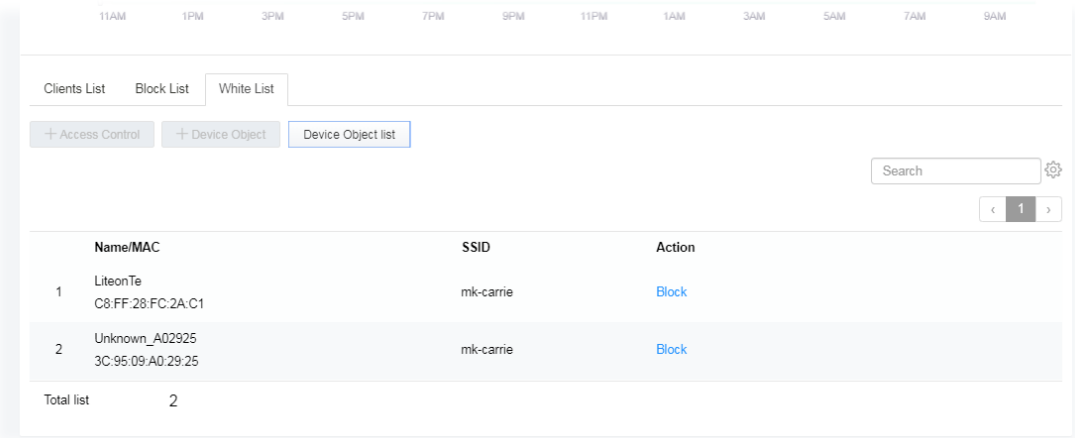



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Device Object list** | Click it to open the Device Object List dialog for reference.<br> |
| **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.<br>**Unblock** - Click to unblock the entry. |

### II-3-12-5 White List

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

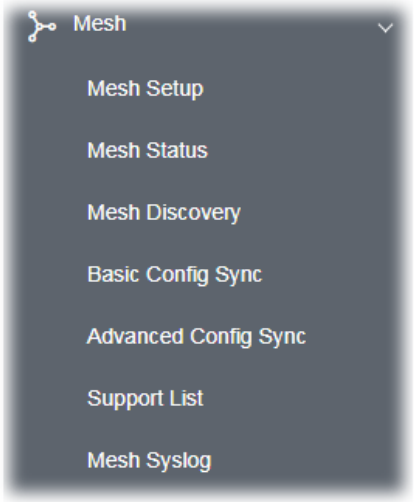



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Device Object list** | Click it to open the Device Object List dialog for reference.<br> |
| **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.<br>**Block** - Click to block the entry. |

# II-4 Mesh Settings for Mesh Mode

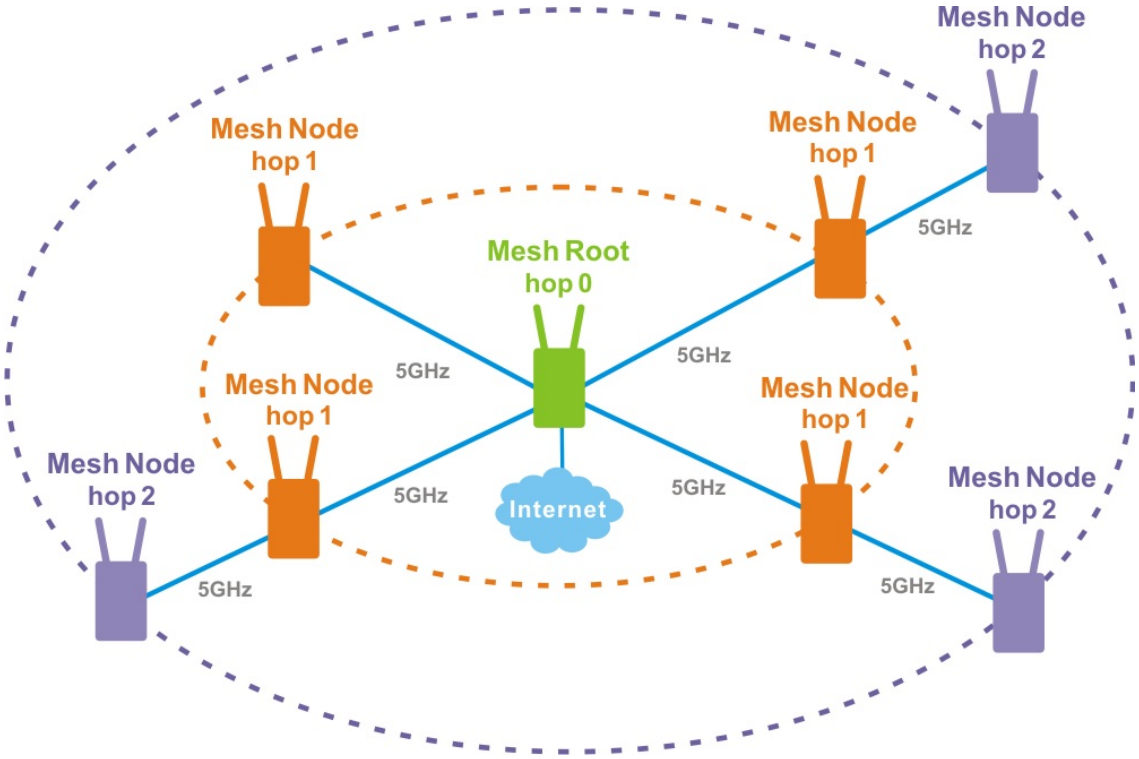
When you choose **Mesh** as the operation mode, the Mesh menu with the settings of Mesh Setup, Mesh Status, Mesh Discovery and Configuration Sync will be shown on the screen.




Please note that, within VigorMesh network,

- the total number allowed for mesh nodes is 8 (including the mesh root)
- the maximum number of hop is 3

Refer to the following figure:




For the mesh group set within VigorMesh network,

- It must be composed by “1” Mesh Root and “0~7” mesh nodes
- (Roaming) Normally members in a mesh group use the same Wireless SSID/security

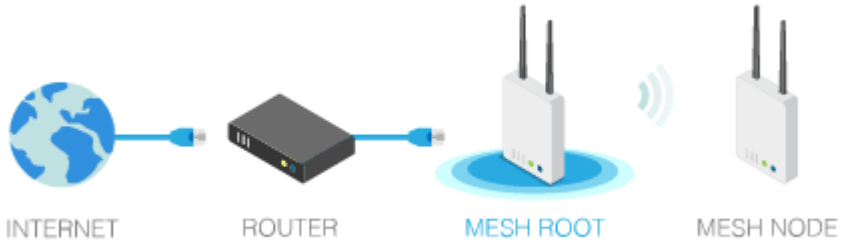
- (Add) Only the mesh root can add a new mesh node into the mesh group
- (Recover) A disconnected mesh node will automatically try to connect to another connected mesh node of the same group

**Mesh Root and 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 the mesh root or mesh node within the same mesh group via wireless network or physical connection with an Ethernet cable.

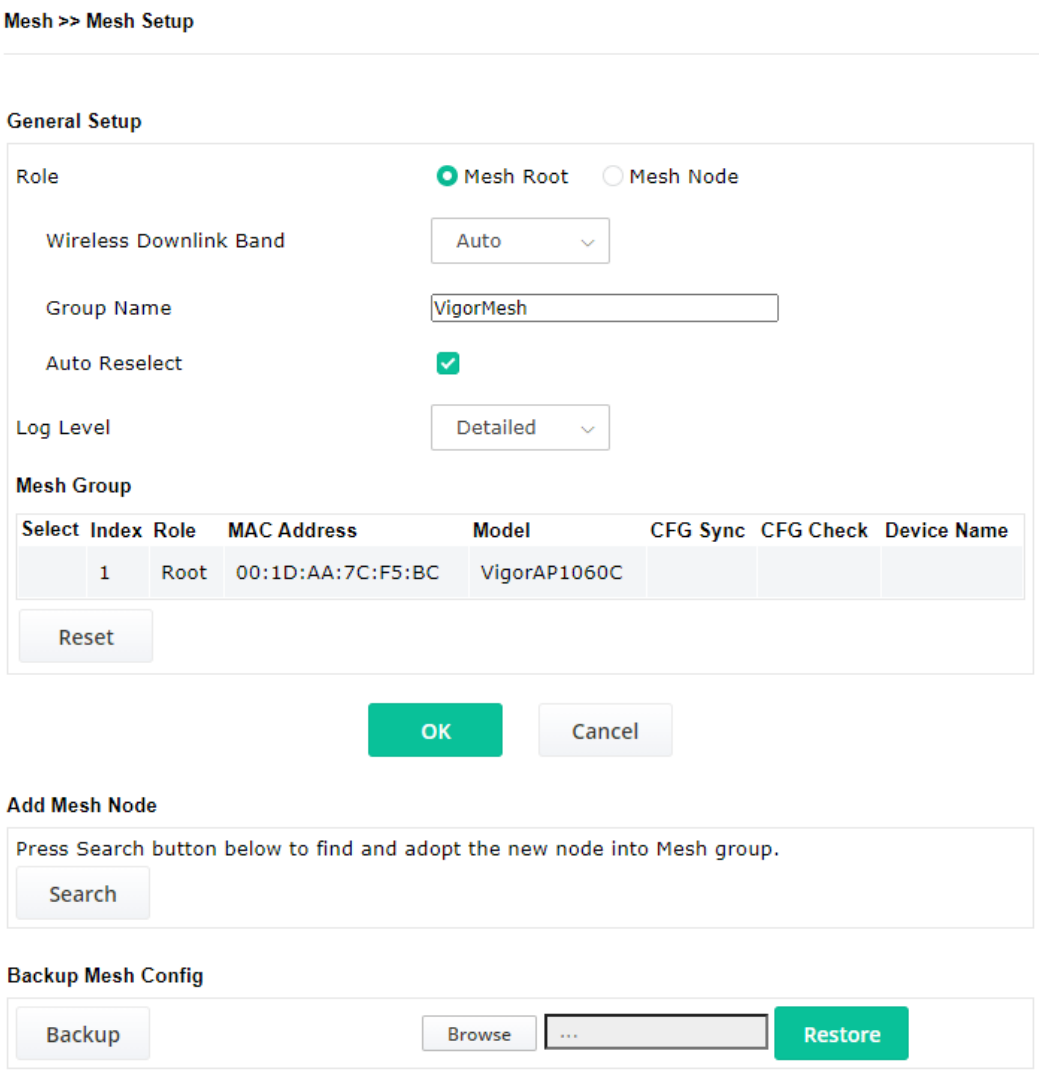
The following figure shows how VigorAP runs as MESH ROOT:




The following figure shows how VigorAP runs as MESH NODE:

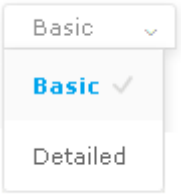
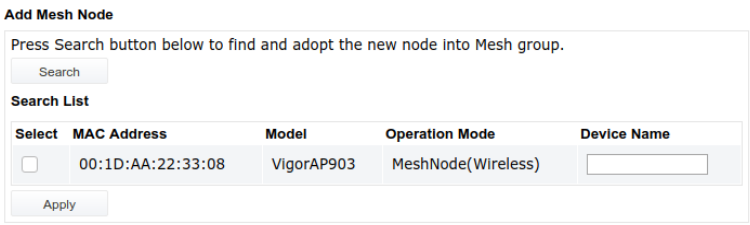
# II-4-1 Mesh Setup

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:

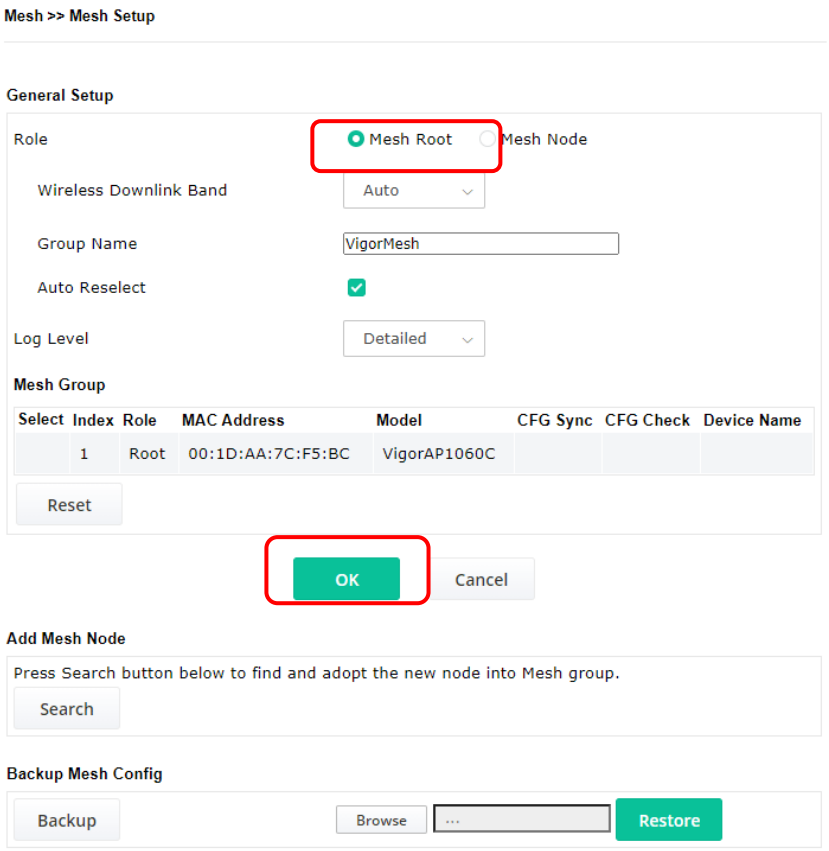
| Item | Description |
|---|---|
| **Role** | **Mesh Root –** When VigorAP is connected to a Vigor router with a physical Ethernet cable, it can be set as mesh root to deliver the wireless signals to a mesh node AP.<br>**Mesh Node –** As a mesh node, such VigorAP can pass the wireless connection signal to other mesh node or a remote device (PC, CPE, mobile phone).<br>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.<br>**Log Level –** Choose **Basic** or **Detailed**. Related information will be shown on the **Diagnostics>>System Log.** |

| | |
|---|---|
| |  |
| **When Mesh Root is selected** | **Wireless Downlink Band** – Choose a wireless band for connecting with a downlink mesh root or a downlink mesh node.<br>**Group Name** - Display the name of the current mesh group.<br>**Auto Reselect** - It is selected in default. To perform the auto reselect, make sure the process for CFG Sync and CFG Check for mesh nodes are successful. If enabled, after changing the environment of mesh network (e.g., offline, disconnection), the root device will perform auto reselect to reconstruct the mesh network. |
| **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.<br>**Wireless Uplink Band** – Choose a wireless band for connecting with an uplinked mesh root or an uplinked mesh node.<br>**Log Level –** Choose **Basic** or **Detailed**. Related information will be shown on the **Diagnostics>>System Log.** |
| **Mesh Group** | When the 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.<br>Up to 8 entries (one mesh root and seven mesh nodes) will be shown on this field.<br>**Reset -** Click it to clear the Mesh Group information.<br>**Delete** - Click it to remove the selected entry. |
| **Add Mesh Node** | Click **Search** to find out available mesh node on the network.<br>  <br>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.<br>**Upload/Restore** – Click the Upload button to specify a configuration file. Then click Restore to apply the configuration.<br>When the MAC address of such VigorAP does not appear under the mesh group, the restore operation will not succeed and the error message, ”Device MAC is not in mesh group list”, will be shown instead. |

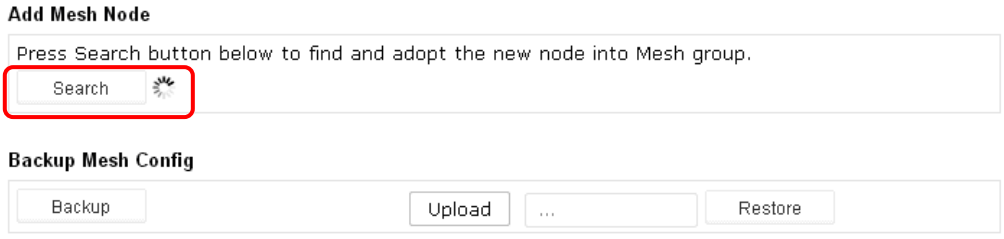
**How to set up a mesh group?**

The following steps will guide you how to setup a Mesh Group (with mesh root and mesh node) from **Mesh >> Mesh Setup**.

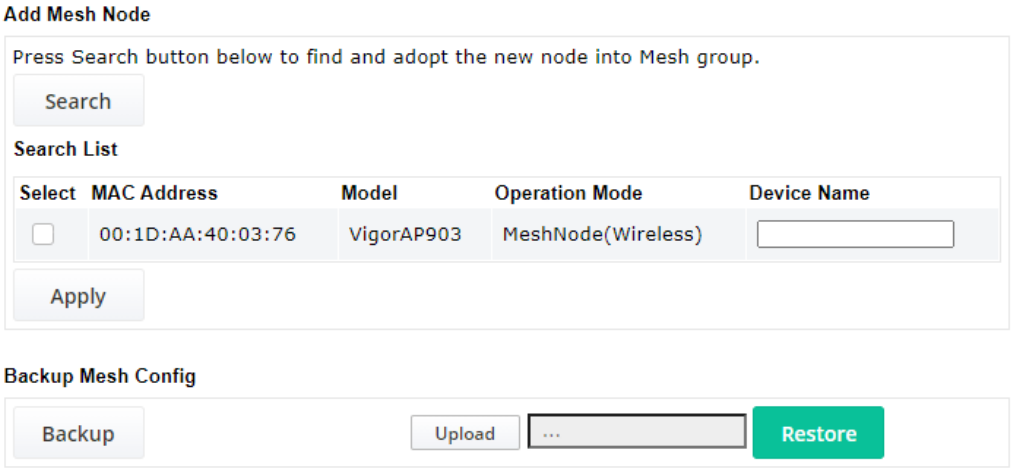
1. Open **Mesh>>Mesh Setup**. Click **Mesh Root** and click **OK** for the VigorAP connected to PC with Ethernet cable. At first, a Mesh Group is with only Mesh Root.



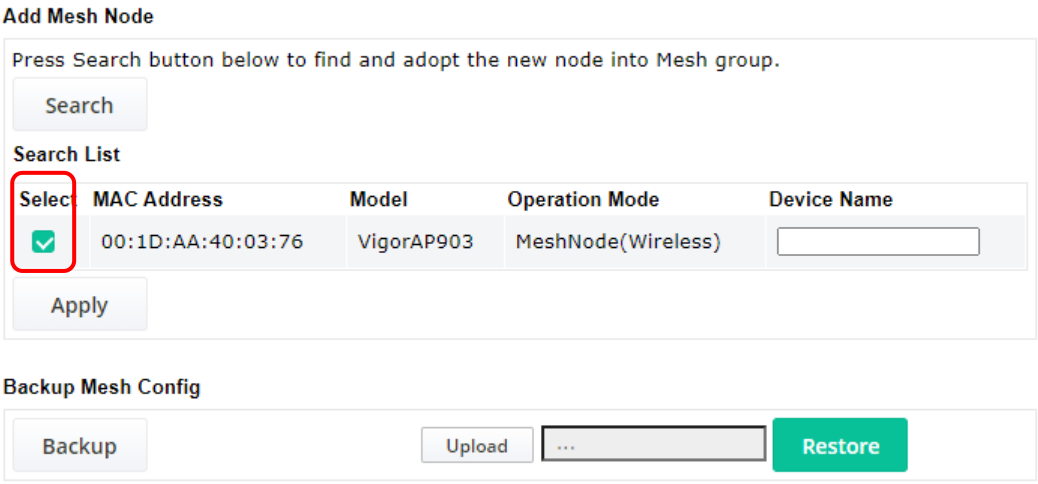

2. Click the **Search** button in the field of **Add Mesh Node**.



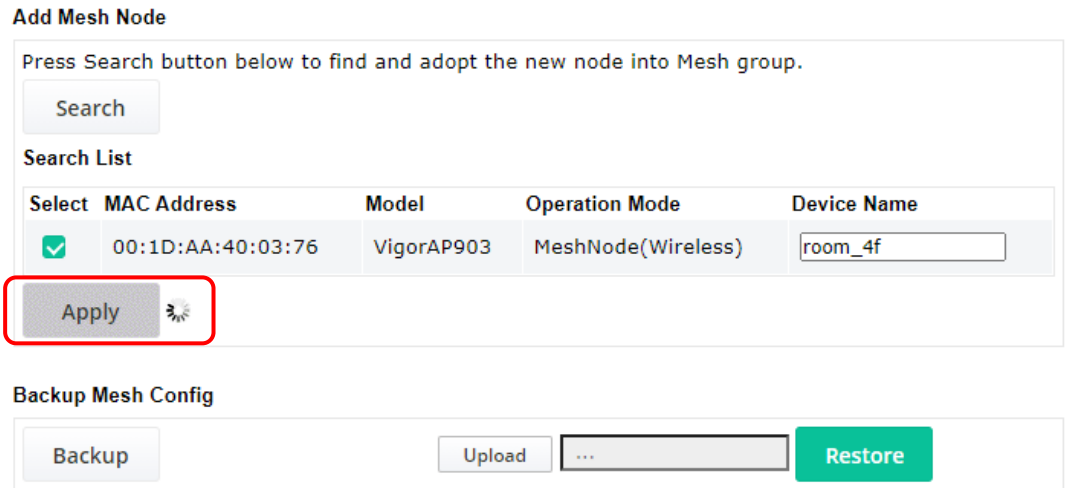
3. Wait until the searching result appears.



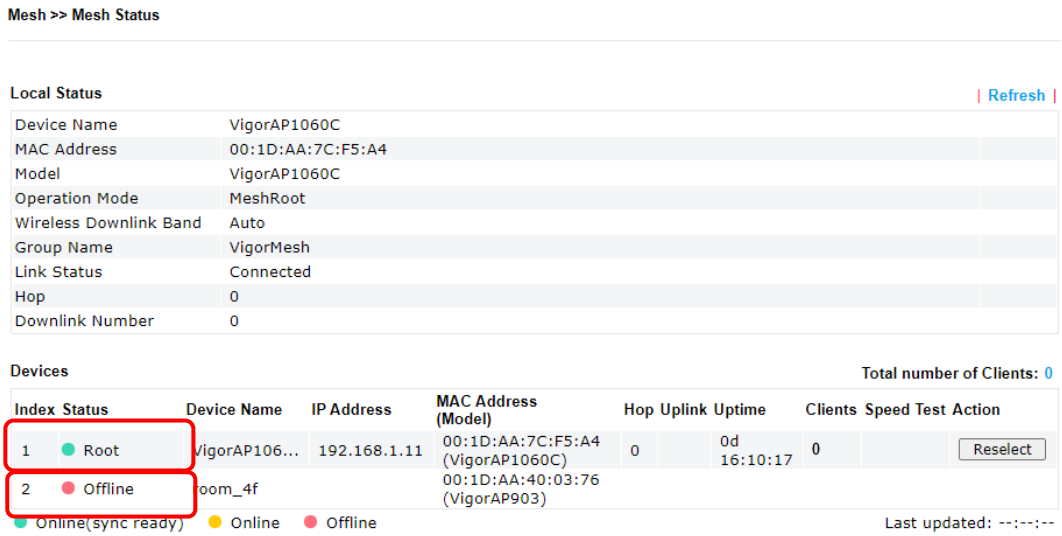

4. Choose the device(s) you want to add to the Mesh Group as mesh node(s) and define the **Device Name** for each node. In this example, five devices are specified as mesh nodes.




5. Click the **Apply** button and wait for it to finish the procedure.



6. After finishing the mesh network configuration, refer to **Mesh>>Mesh Status** for viewing the result.



**Mesh >> Mesh Status**

**Local Status** | Refresh |

| | |
|---|---|
| Device Name | VigorAP1060C |
| MAC Address | 00:1D:AA:7C:F5:A4 |
| Model | VigorAP1060C |
| Operation Mode | MeshRoot |
| Wireless Downlink Band | Auto |
| Group Name | VigorMesh |
| Link Status | Connected |
| Hop | 0 |
| Downlink Number | 0 |

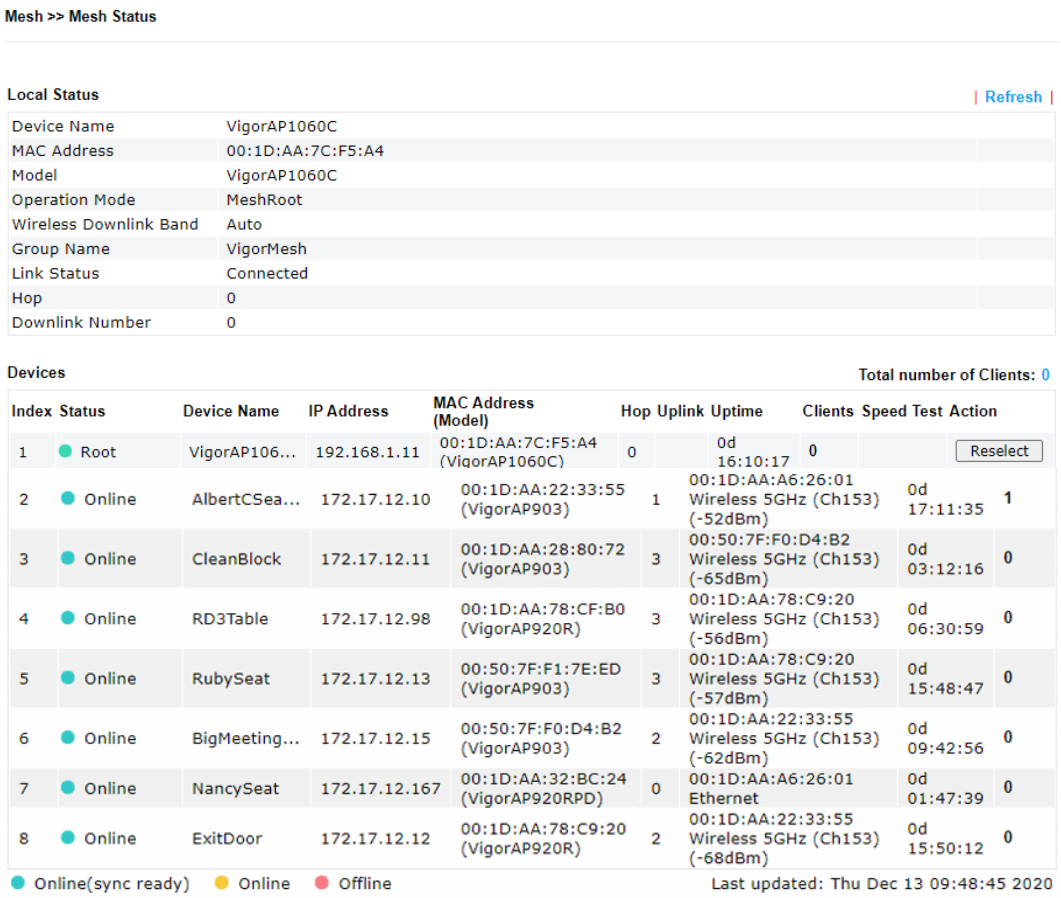
**Devices** Total number of Clients: 0

| Index | Status | Device Name | IP Address | MAC Address (Model) | Hop | Uplink | Uptime | Clients | Speed Test | Action |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Root | VigorAP106... | 192.168.1.11 | 00:1D:AA:7C:F5:A4 (VigorAP1060C) | 0 | | 0d 16:10:17 | 0 | | Reselect |
| 2 | Offline | oom_4f | | 00:1D:AA:40:03:76 (VigorAP903) | | | | | | |

Online(sync ready) Online Offline Last updated: --:--:--

## II-4-2 Mesh Status

This page shows that one Mesh Group can contain up to 8 devices. In the following figure, the Device with hop 0 is one special Ethernet Backhaul. It means this node will use Ethernet cable to join the mesh group while others use the wireless link.



**Mesh >> Mesh Status**

**Local Status** | Refresh |

| | |
|---|---|
| Device Name | VigorAP1060C |
| MAC Address | 00:1D:AA:7C:F5:A4 |
| Model | VigorAP1060C |
| Operation Mode | MeshRoot |
| Wireless Downlink Band | Auto |
| Group Name | VigorMesh |
| Link Status | Connected |
| Hop | 0 |
| Downlink Number | 0 |

**Devices** Total number of Clients: 0

| Index | Status | Device Name | IP Address | MAC Address (Model) | Hop | Uplink | Uptime | Clients | Speed Test | Action |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Root | VigorAP106... | 192.168.1.11 | 00:1D:AA:7C:F5:A4 (VigorAP1060C) | 0 | | 0d 16:10:17 | 0 | | Reselect |
| 2 | Online | AlbertCSea... | 172.17.12.10 | 00:1D:AA:22:33:55 (VigorAP903) | 1 | 00:1D:AA:A6:26:01 Wireless 5GHz (Ch153) (-52dBm) | 0d 17:11:35 | 1 | | |
| 3 | Online | CleanBlock | 172.17.12.11 | 00:1D:AA:28:80:72 (VigorAP903) | 3 | 00:50:7F:F0:D4:B2 Wireless 5GHz (Ch153) (-65dBm) | 0d 03:12:16 | 0 | | |
| 4 | Online | RD3Table | 172.17.12.98 | 00:1D:AA:78:CF:B0 (VigorAP920R) | 3 | 00:1D:AA:78:C9:20 Wireless 5GHz (Ch153) (-56dBm) | 0d 06:30:59 | 0 | | |
| 5 | Online | RubySeat | 172.17.12.13 | 00:50:7F:F1:7E:ED (VigorAP903) | 3 | 00:1D:AA:78:C9:20 Wireless 5GHz (Ch153) (-57dBm) | 0d 15:48:47 | 0 | | |
| 6 | Online | BigMeeting... | 172.17.12.15 | 00:50:7F:F0:D4:B2 (VigorAP903) | 2 | 00:1D:AA:22:33:55 Wireless 5GHz (Ch153) (-62dBm) | 0d 09:42:56 | 0 | | |
| 7 | Online | NancySeat | 172.17.12.167 | 00:1D:AA:32:BC:24 (VigorAP920RPD) | 0 | 00:1D:AA:A6:26:01 Ethernet | 0d 01:47:39 | 0 | | |
| 8 | Online | ExitDoor | 172.17.12.12 | 00:1D:AA:78:C9:20 (VigorAP920R) | 2 | 00:1D:AA:22:33:55 Wireless 5GHz (Ch153) (-68dBm) | 0d 15:50:12 | 0 | | |

Online(sync ready) Online Offline Last updated: Thu Dec 13 09:48:45 2020

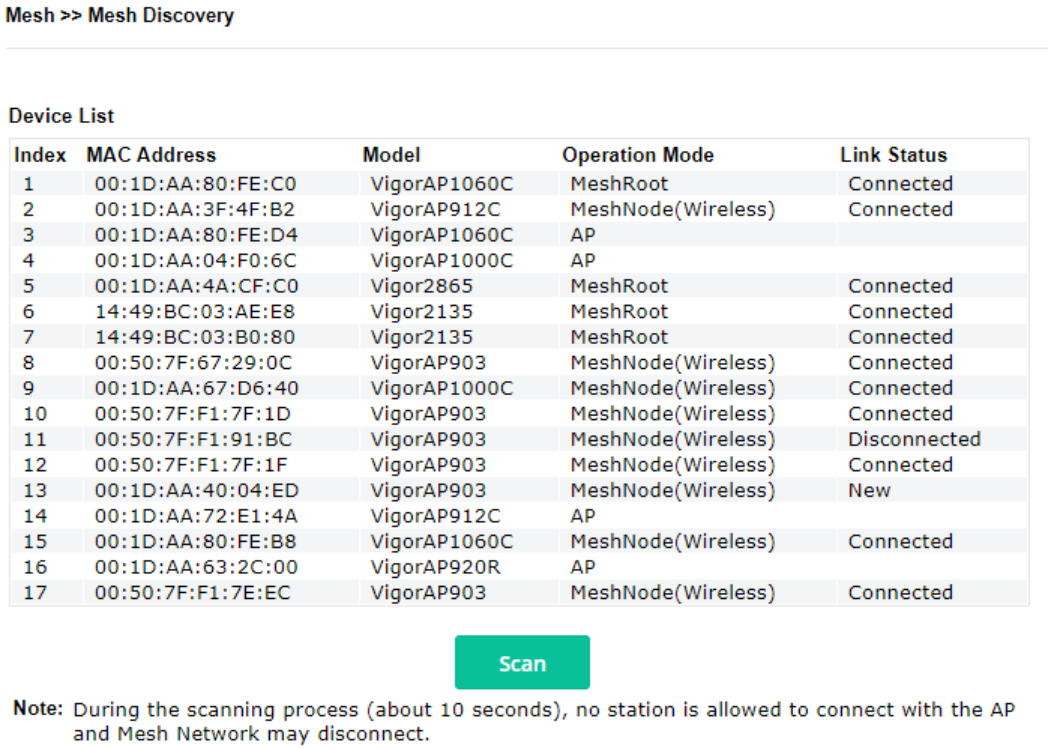
| Item | Description |
|---|---|
| **Local Status** | Display general information for such VigorAP. |
| **Devices** | Display detailed information for this VigorAP (as mesh root) and mesh node(s) in the group.<br>**Index** – Display the number of the device within a mesh group.<br>**Status** – Display the role of the device within a mesh group.<br>**Device Name** – Display the name of the device (for identification).<br>**IP Address** – Display the IP address of the device.<br>**MAC Address** – Display the MAC address of the device.<br>**Hop** – Display the level of the devices within a mesh group. “0” means the access point is connected to a device by using Ethernet cable (wired). “1” to “3” means the level of the access point within a mesh group and it connects to other access point via wireless link.<br>**Uplink** – Display the MAC address of the device that the AP connects to. |
| **Total number of Clients** | Display the station list of all mesh devices. |

**Station List of All Devices**

| Index | MAC Address | Hostname | Vendor | SSID | Channel | RSSI | TxRate(Kbps) | RxRate(Kbps) |
|---|---|---|---|---|---|---|---|---|
| 1 | 00:50:7F:F0:C9:72 | TA001029 | DrayTek | staffs_4F | 6 | 68%(-63dBm) | 0 | 0 |
| 2 | 00:50:7F:F0:D1:1D | ta002171 | DrayTek | staffs_4F | 6 | 41%(-73dBm) | 0 | 0 |
| 3 | 5C:97:F3:D3:D5:F7 | Tze-Pingde... | Apple | staffs_4F | 6 | 100% (-49dBm) | 0 | 0 |
| 4 | 40:98:AD:5B:F2:52 | Tyronetkii... | Apple | staffs | 6 | 55%(-68dBm) | 0 | 0 |
| 5 | 00:50:7F:37:6D:E5 | N/A | DrayTek | staffs_4F | 6 | 52%(-69dBm) | 0 | 0 |
| 6 | 00:50:7F:37:67:BE | N/A | DrayTek | staffs_4F | 6 | 55%(-68dBm) | 0 | 0 |
| 7 | 30:F7:C5:1D:3D:11 | N/A | Apple | guests | 6 | 83%(-57dBm) | 30 | 12 |
| 8 | 40:F0:2F:22:EB:A0 | N/A | LiteonTe | staffs | 6 | 34%(-76dBm) | 22 | 4 |
| 9 | 18:65:90:DE:D4:E5 | N/A | Apple | staffs_4F | 6 | 100% (-44dBm) | 0 | 0 |
| 10 | 60:45:CB:57:1F:36 | N/A | N/A | staffs_4F | 6 | 15%(-84dBm) | 0 | 0 |
| 11 | AC:5F:3E:62:E6:0D | N/A | Samsung | staffs_4F | 6 | 81%(-58dBm) | 0 | 0 |
| 12 | 50:BC:96:E0:00:11 | N/A | Apple | staffs | 6 | 71%(-62dBm) | 0 | 0 |
| 13 | 04:B1:67:52:48:90 | Redmi5-mys... | N/A | staffs_4F | 6 | 45%(-72dBm) | 0 | 0 |
| 14 | 04:C2:3E:3F:CB:F8 | android-ac... | HTC | staffs_4F | 6 | 55%(-68dBm) | 0 | 0 |
| 15 | 0C:8B:FD:31:0B:78 | N/A | Intel | staffs_4F | 6 | 89%(-55dBm) | 2 | 2 |
| 16 | 58:48:22:EB:F8:62 | android-5f... | Sony | staffs | 6 | 55%(-68dBm) | 0 | 0 |
| 17 | CC:9F:7A:63:11:27 | N/A | N/A | staffs_4F5... | 36 | 52%(-69dBm) | 0 | 0 |
| 18 | 20:47:DA:58:17:79 | RedmiNote5... | N/A | staffs_4F5... | 36 | 50%(-70dBm) | 0 | 0 |
| 19 | 70:81:EB:65:80:E5 | cheng | Apple | staffs_4F5... | 36 | 87%(-56dBm) | 0 | 0 |
| 20 | 8C:85:90:64:FE:A4 | N/A | Apple | staffs_4F5... | 36 | 36%(-75dBm) | 0 | 0 |

# II-4-3 Mesh Discovery

Before a Mesh Node is connected, it is unable to check the device status from Mesh Root. This page can help to discover all Mesh devices around and offer the Link Status and Operation Mode of each Mesh device.



**Mesh >> Mesh Discovery**

**Device List**

| Index | MAC Address | Model | Operation Mode | Link Status |
|---|---|---|---|---|
| 1 | 00:1D:AA:80:FE:C0 | VigorAP1060C | MeshRoot | Connected |
| 2 | 00:1D:AA:3F:4F:B2 | VigorAP912C | MeshNode(Wireless) | Connected |
| 3 | 00:1D:AA:80:FE:D4 | VigorAP1060C | AP | |
| 4 | 00:1D:AA:04:F0:6C | VigorAP1000C | AP | |
| 5 | 00:1D:AA:4A:CF:C0 | Vigor2865 | MeshRoot | Connected |
| 6 | 14:49:BC:03:AE:E8 | Vigor2135 | MeshRoot | Connected |
| 7 | 14:49:BC:03:B0:80 | Vigor2135 | MeshRoot | Connected |
| 8 | 00:50:7F:67:29:0C | VigorAP903 | MeshNode(Wireless) | Connected |
| 9 | 00:1D:AA:67:D6:40 | VigorAP1000C | MeshNode(Wireless) | Connected |
| 10 | 00:50:7F:F1:7F:1D | VigorAP903 | MeshNode(Wireless) | Connected |
| 11 | 00:50:7F:F1:91:BC | VigorAP903 | MeshNode(Wireless) | Disconnected |
| 12 | 00:50:7F:F1:7F:1F | VigorAP903 | MeshNode(Wireless) | Connected |
| 13 | 00:1D:AA:40:04:ED | VigorAP903 | MeshNode(Wireless) | New |
| 14 | 00:1D:AA:72:E1:4A | VigorAP912C | AP | |
| 15 | 00:1D:AA:80:FE:B8 | VigorAP1060C | MeshNode(Wireless) | Connected |
| 16 | 00:1D:AA:63:2C:00 | VigorAP920R | AP | |
| 17 | 00:50:7F:F1:7E:EC | VigorAP903 | MeshNode(Wireless) | Connected |

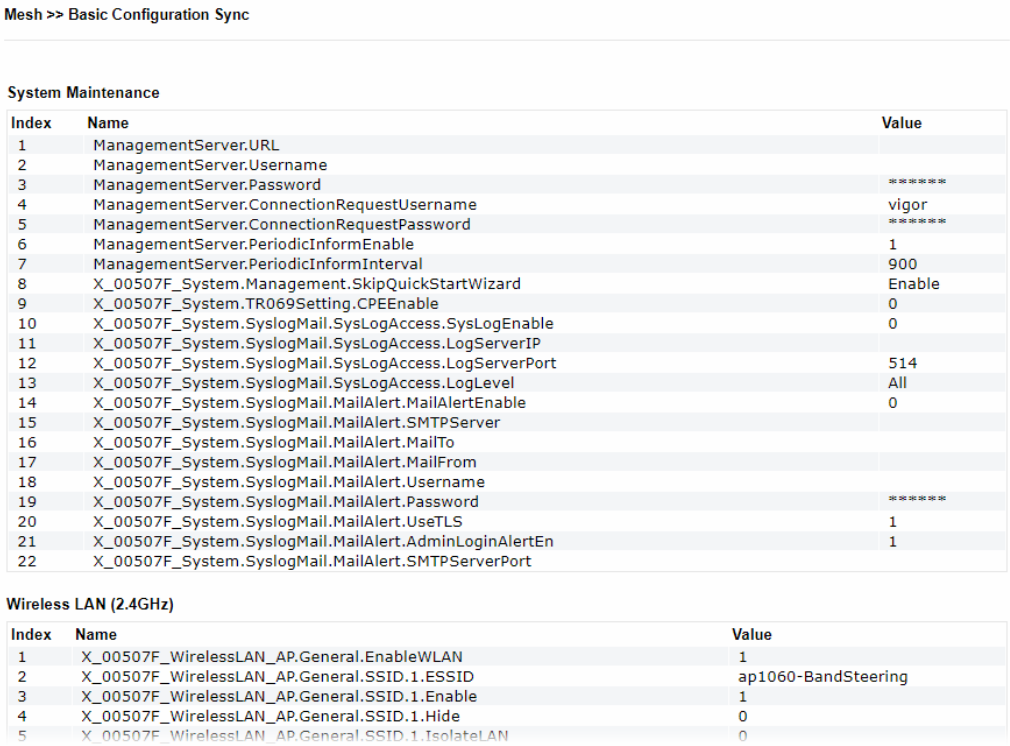
Scan

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

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

# 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.



**Mesh >> Basic Configuration Sync**

**System Maintenance**

| Index | Name | Value |
|---|---|---|
| 1 | ManagementServer.URL | |
| 2 | ManagementServer.Username | |
| 3 | ManagementServer.Password | ****** |
| 4 | ManagementServer.ConnectionRequestUsername | vigor |
| 5 | ManagementServer.ConnectionRequestPassword | ****** |
| 6 | ManagementServer.PeriodicInformEnable | 1 |
| 7 | ManagementServer.PeriodicInformInterval | 900 |
| 8 | X_00507F_System.Management.SkipQuickStartWizard | Enable |
| 9 | X_00507F_System.TR069Setting.CPEEnable | 0 |
| 10 | X_00507F_System.SyslogMail.SysLogAccess.SysLogEnable | 0 |
| 11 | X_00507F_System.SyslogMail.SysLogAccess.LogServerIP | |
| 12 | X_00507F_System.SyslogMail.SysLogAccess.LogServerPort | 514 |
| 13 | X_00507F_System.SyslogMail.SysLogAccess.LogLevel | All |
| 14 | X_00507F_System.SyslogMail.MailAlert.MailAlertEnable | 0 |
| 15 | X_00507F_System.SyslogMail.MailAlert.SMTPServer | |
| 16 | X_00507F_System.SyslogMail.MailAlert.MailTo | |
| 17 | X_00507F_System.SyslogMail.MailAlert.MailFrom | |
| 18 | X_00507F_System.SyslogMail.MailAlert.Username | |
| 19 | X_00507F_System.SyslogMail.MailAlert.Password | ****** |
| 20 | X_00507F_System.SyslogMail.MailAlert.UseTLS | 1 |
| 21 | X_00507F_System.SyslogMail.MailAlert.AdminLoginAlertEn | 1 |
| 22 | X_00507F_System.SyslogMail.MailAlert.SMTPServerPort | |

**Wireless LAN (2.4GHz)**

| Index | Name | Value |
|---|---|---|
| 1 | X_00507F_WirelessLAN_AP.General.EnableWLAN | 1 |
| 2 | X_00507F_WirelessLAN_AP.General.SSID.1.ESSID | ap1060-BandSteering |
| 3 | X_00507F_WirelessLAN_AP.General.SSID.1.Enable | 1 |
| 4 | X_00507F_WirelessLAN_AP.General.SSID.1.Hide | 0 |
| 5 | X_00507F_WirelessLAN_AP.General.SSID.1.IsolateLAN | 0 |

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.<br>**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):

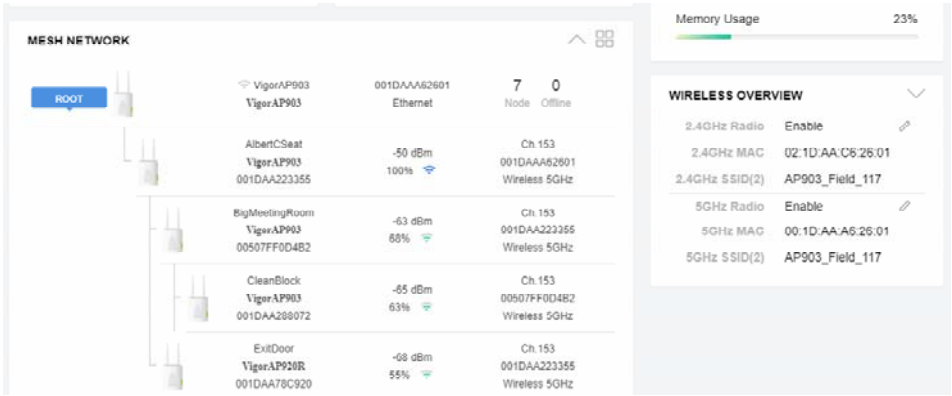
  iPad connects to Root : 80Mbps

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

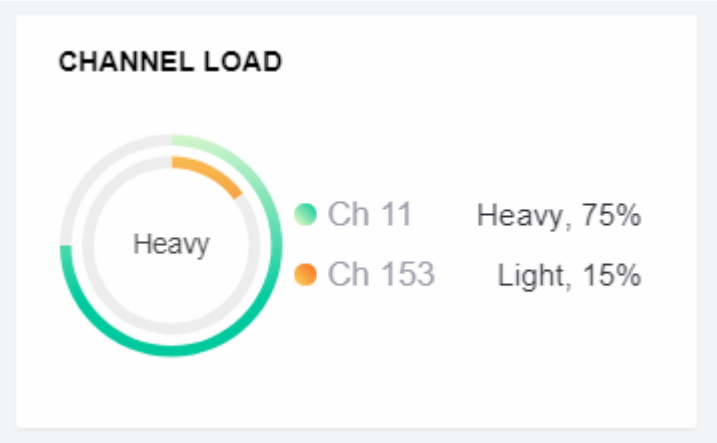
  iPad connects to hop2 Node : 41Mbps (Uplink RSSI : hop2 -64dBm / hop1 -55dBm)

iPad connects to hop3 Node : 26Mbps (Uplink RSSI : hop3 -62dBm / hop2 -68dBm / hop1 -55dBm)

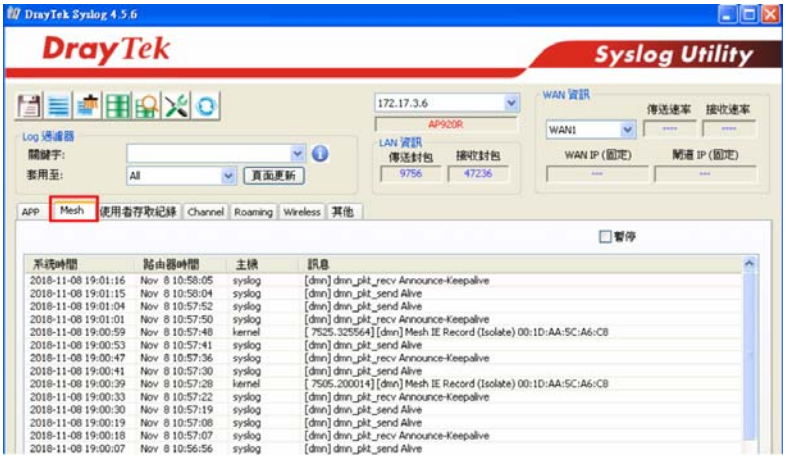
- It is not suggested to use a wireless Mesh Node with Ethernet cable connected to a Mesh Root.
- If resetting a Mesh Root,
  - All "connected" Mesh Nodes will be informed to reset.
  - Group List and Group Key will be reset, too.
  - For those Mesh Nodes unable to reset, reset them manually. Reset the 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 1060C 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%.

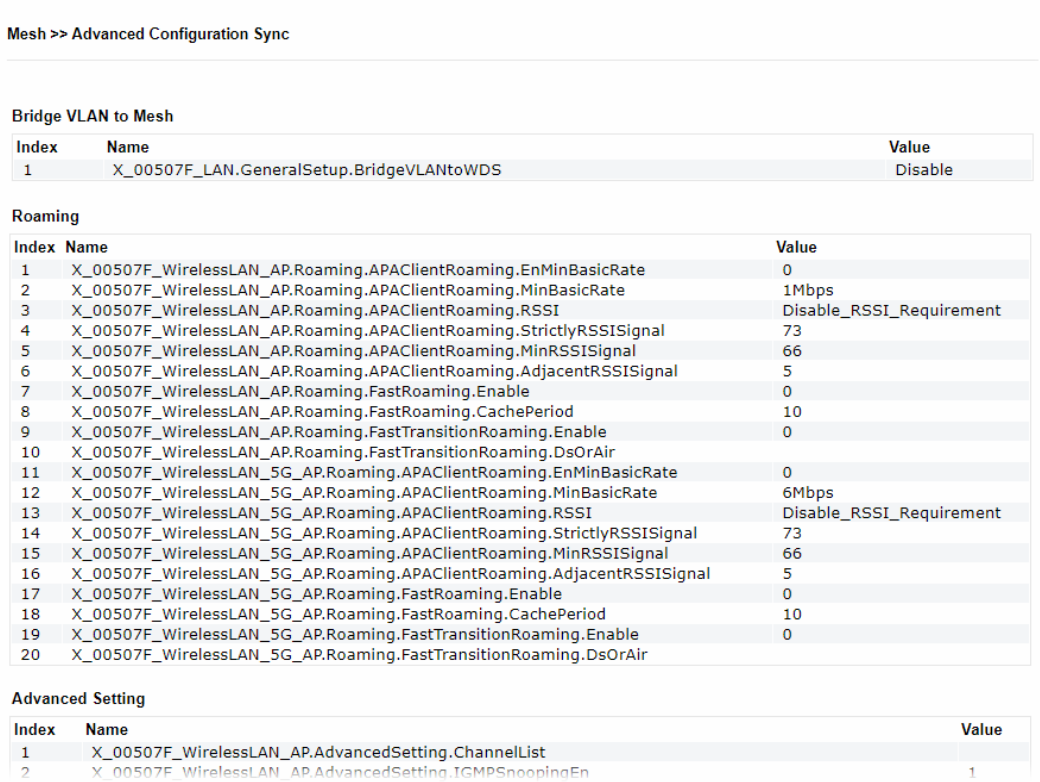



- Collect some Mesh logs and send the result to DrayTek for analyzing.



## 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**

**Bridge VLAN to Mesh**

| Index | Name | Value |
|---|---|---|
| 1 | X_00507F_LAN.GeneralSetup.BridgeVLANtoWDS | Disable |

**Roaming**

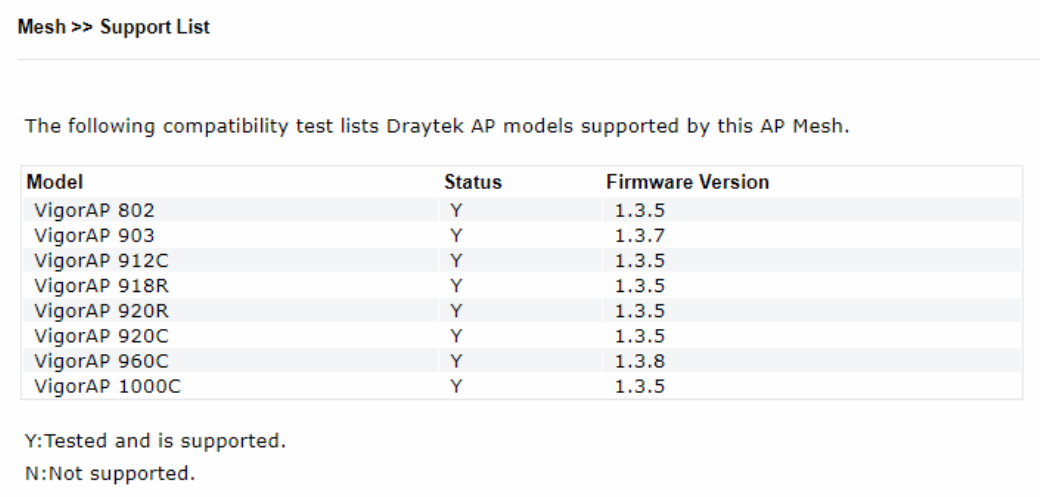
| Index | Name | Value |
|---|---|---|
| 1 | X_00507F_WirelessLAN_AP.Roaming.APAClientRoaming.EnMinBasicRate | 0 |
| 2 | X_00507F_WirelessLAN_AP.Roaming.APAClientRoaming.MinBasicRate | 1Mbps |
| 3 | X_00507F_WirelessLAN_AP.Roaming.APAClientRoaming.RSSI | Disable_RSSI_Requirement |
| 4 | X_00507F_WirelessLAN_AP.Roaming.APAClientRoaming.StrictlyRSSISignal | 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 | |
| 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 |
| 19 | X_00507F_WirelessLAN_5G_AP.Roaming.FastTransitionRoaming.Enable | 0 |
| 20 | X_00507F_WirelessLAN_5G_AP.Roaming.FastTransitionRoaming.DsOrAir | |

**Advanced Setting**

| Index | Name | Value |
|---|---|---|
| 1 | X_00507F_WirelessLAN_AP.AdvancedSetting.ChannelList | |
| 2 | X_00507F_WirelessLAN_AP.AdvancedSetting.IGMPSnoopingEn | 1 |

## II-4-6 Support List

This page shows a list of AP models supported by this AP (Mesh network).



**Mesh >> Support List**

The following compatibility test lists Draytek AP models supported by this AP Mesh.

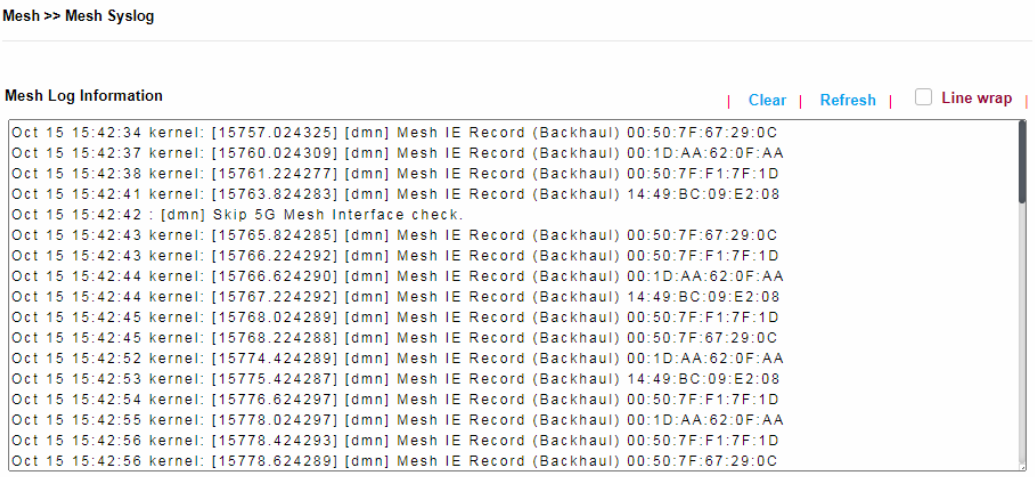
| Model | Status | Firmware Version |
|---|---|---|
| VigorAP 802 | Y | 1.3.5 |
| VigorAP 903 | Y | 1.3.7 |
| VigorAP 912C | Y | 1.3.5 |
| VigorAP 918R | Y | 1.3.5 |
| VigorAP 920R | Y | 1.3.5 |
| VigorAP 920C | Y | 1.3.5 |
| VigorAP 960C | Y | 1.3.8 |
| VigorAP 1000C | Y | 1.3.5 |

Y:Tested and is supported.

N:Not supported.

# II-4-7 Mesh Syslog

This page shows the log information of mesh sync.

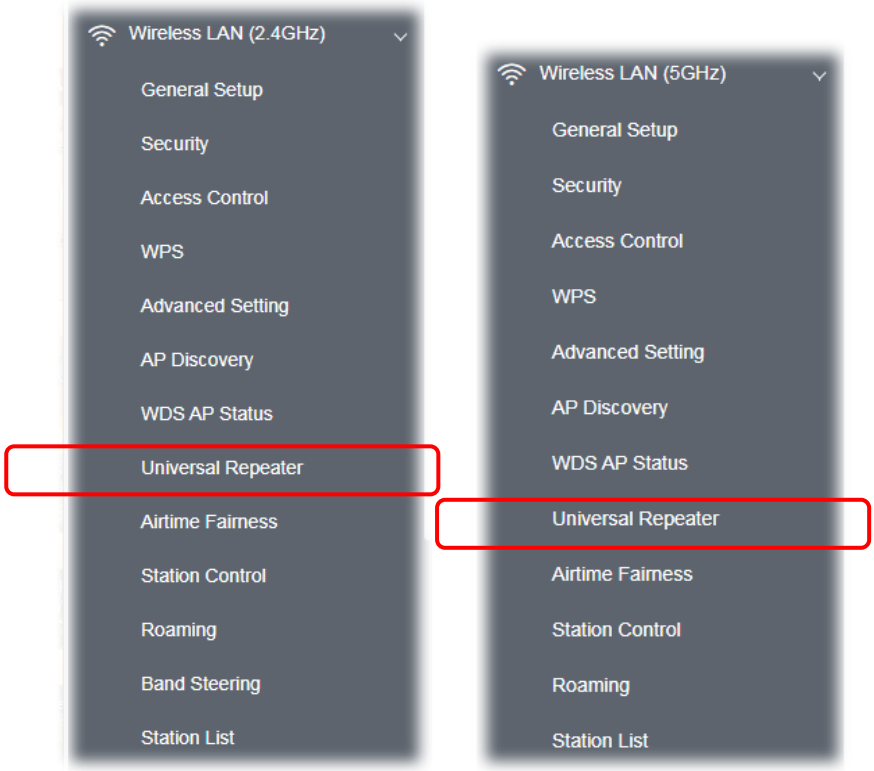


# II-5 Universal Repeater Settings for Range Extender Mode

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, 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.

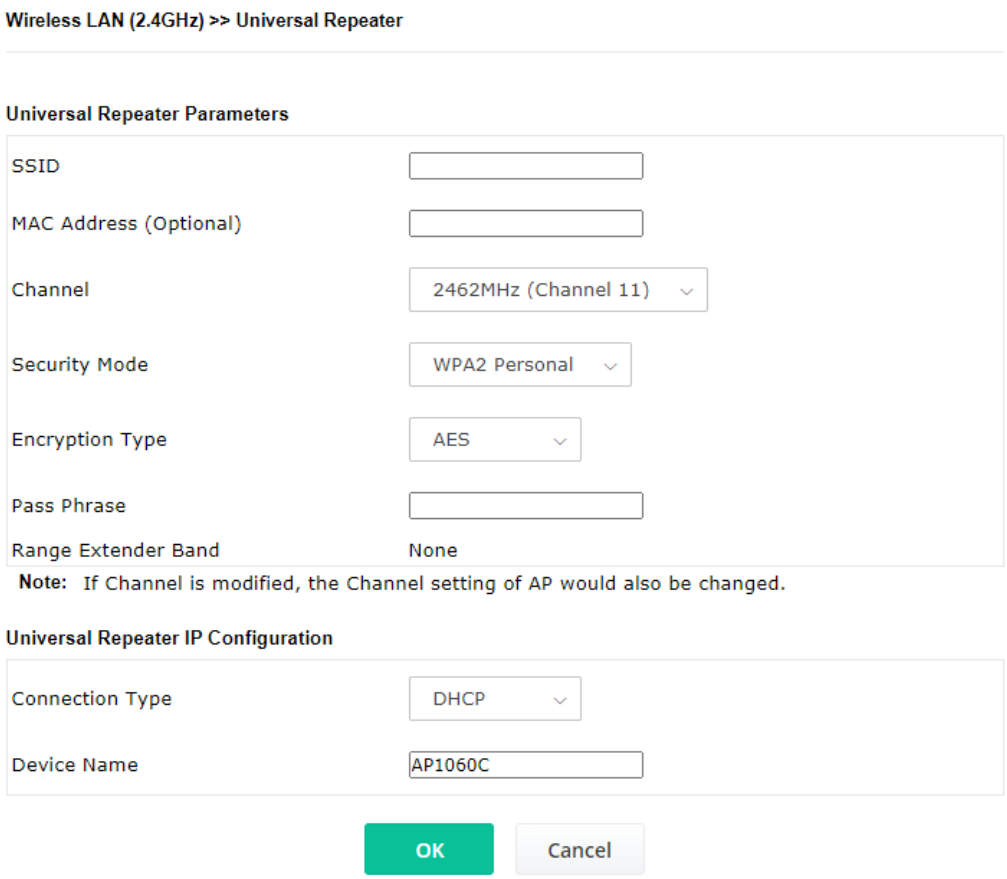



The following figure shows how VigorAP runs as Range Extender:

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.

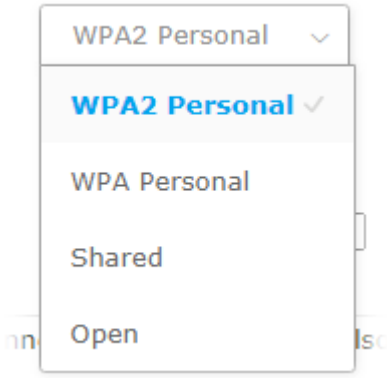
**Note:**

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 |
|---|---|
| **Universal Repeater Parameters** | |
| **SSID** | Display the SSID defined for Range Extender operation mode in Quick Start Wizard.<br>Change the name of SSID whenever you want. |
| **MAC Address (Optional)** | Type the MAC address of access point that VigorAP 1060C wants to connect to. |
| **Channel** | Means the channel of frequency of the wireless LAN.<br>VigorAP offers different channels for WLAN 2.4GHz and 5GHZ respectively.<br>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. |
| **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.<br>  |
| **Encryption Type for Open/Shared** | This option is available when Open/Shared is selected as Security Mode.<br>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**.<br>**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 Personal and WPA2 Personal** | This option is available when WPA Personal or WPA2 Personal is selected as **Security Mode**.<br>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..."). |
| **Range Extender Band** | Display which wireless band (2.4G/5G) is currently used for Universal Repeater.<br>**None** - No network connection. |
| **Universal Repeater IP Configuration** | |
| **Connection Type** | Choose DHCP or Static IP as the connection mode.<br>**DHCP** – The wireless station will be assigned with an IP from VigorAP.<br>**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**.<br>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**.<br>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**.<br>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**.<br>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.

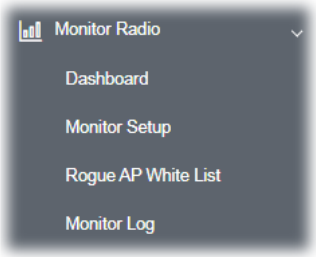
# II-6 Monitor Radio

VigorAP allows wireless clients to connect to the Internet with 2.4G and 5G bands via the built-in radios. In addition, VigorAP is equipped with a third radio which functions as a monitor.

The function of Monitor Radio contains the following points:

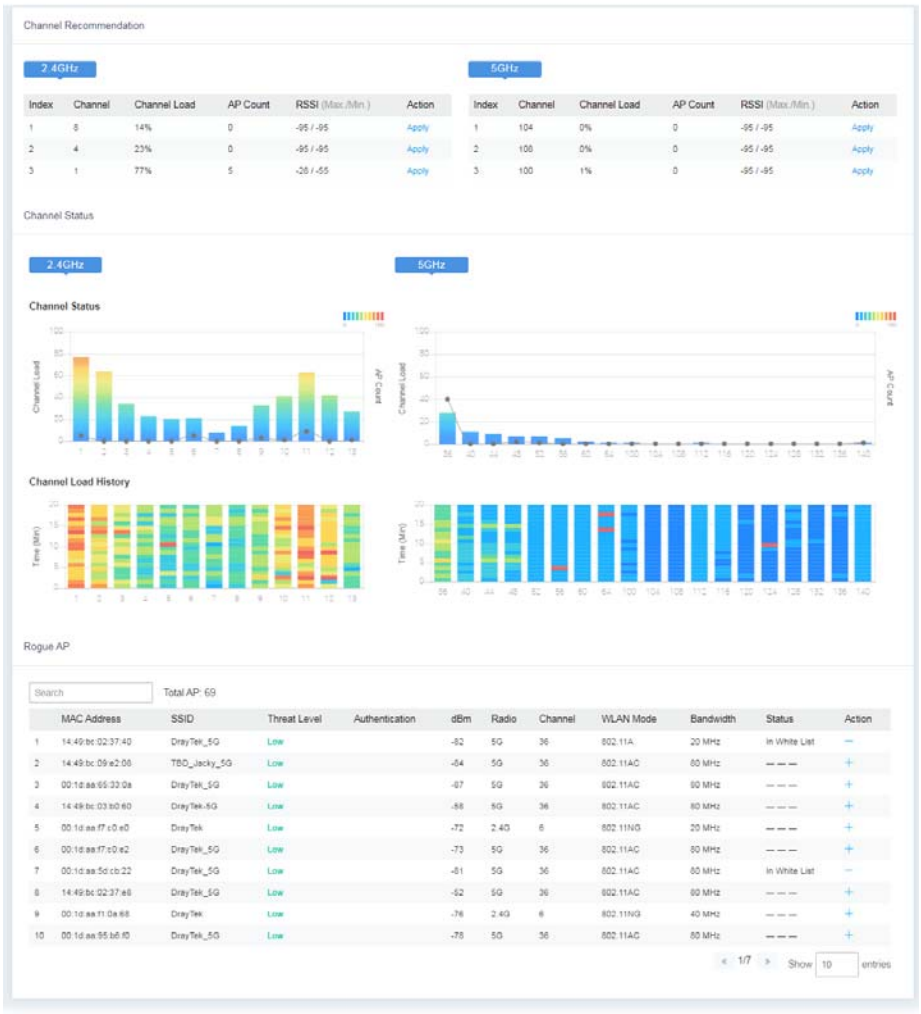
1. Offer RF analytics and the best channel suggestion.

2. Offer wireless intrusion detection (rogue AP detection with mail alert and white list).



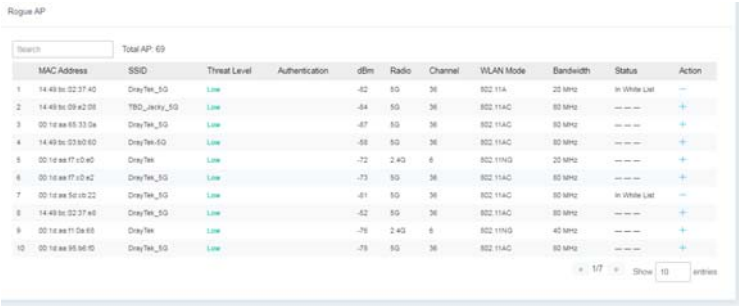

## II-6-1 Dashboard

Click **Monitor Radio** to open the monitor menu. Choose **Dashboard**.



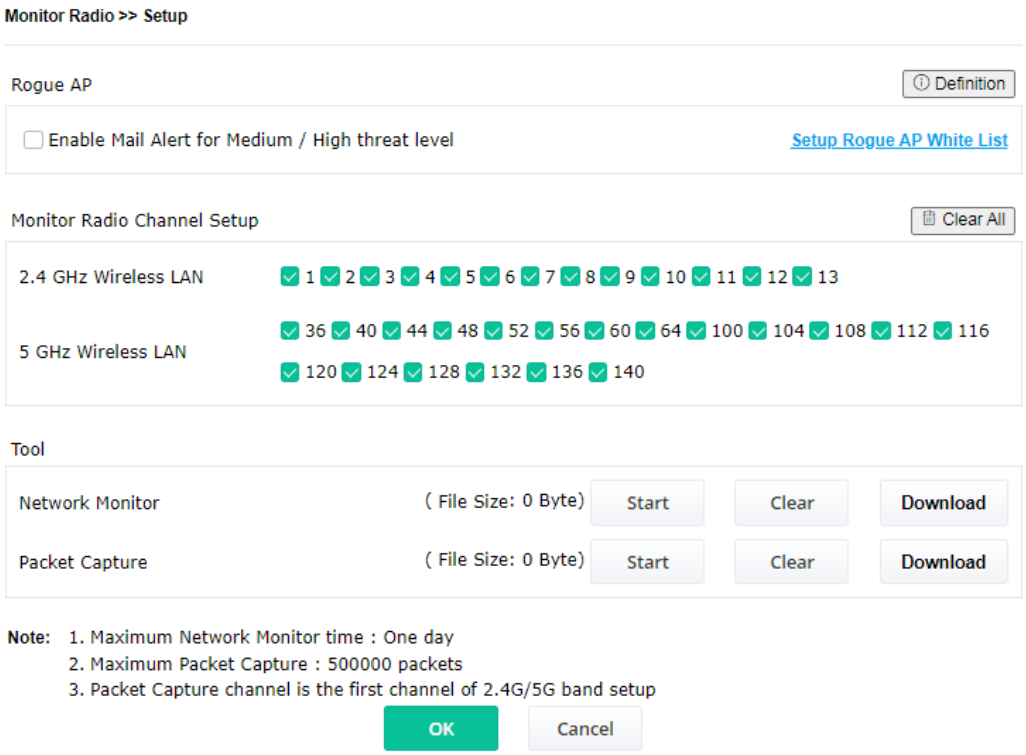

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Channel Recommendation** | Up to three best channels with related information (e.g., channel loading, number of AP scanned, RSSI value) will be recommended and displayed on this page.<br>**Index** - Displays the index number of the top-three best channels.<br>**Channel** - Displays the number of channel frequency of the wireless LAN.<br>**Channel Load** - Displays the percentage of the channel loading for each channel.<br>**AP Count** - Displays the total quantity of AP detected by this Vigor device.<br>**RSSI** - Displays the maximum/minimum RSSI value of the AP detected by this device.<br>**Action** - Click to activate the settings above. |
| **Channel Status** | The high and low histograms represent the channel load for each channel frequency. However, the channel frequency will vary depending on the country that the AP located. For example, in Taiwan,1 to 13 will be used by 2.4GHz; and 36 to 140 used by 5GHz for the wireless stations.<br>**Dots (AP Count)** - It represents the AP Count for each channel frequency. |

| | |
|---|---|
| **Channel Load History** | Records the channel load status within 20 minutes. |
| **Rogue AP** | Displays general information for rogue AP detected by this AP device.<br>  <br>**Threat** - Displays the risk of the AP. If rogue AP with High or Medium threat has been detected, VigorAP would send out an alert mail to the recipient specified in **System Maintenance >> Syslog / Mail Alert Setup>>Mail To**.<br>Low - Means harmless.<br>Medium - The AP is under the LAN of the host and has the same SSID as the host.<br>High - The AP is not under the LAN of the host but has the same SSID as the host.<br>**Action** - Click the "+" to move the selected AP onto the white list. |

## II-6-2 Monitor Setup

This page allows you to configure settings for detecting/monitoring the rogue AP around current AP device.



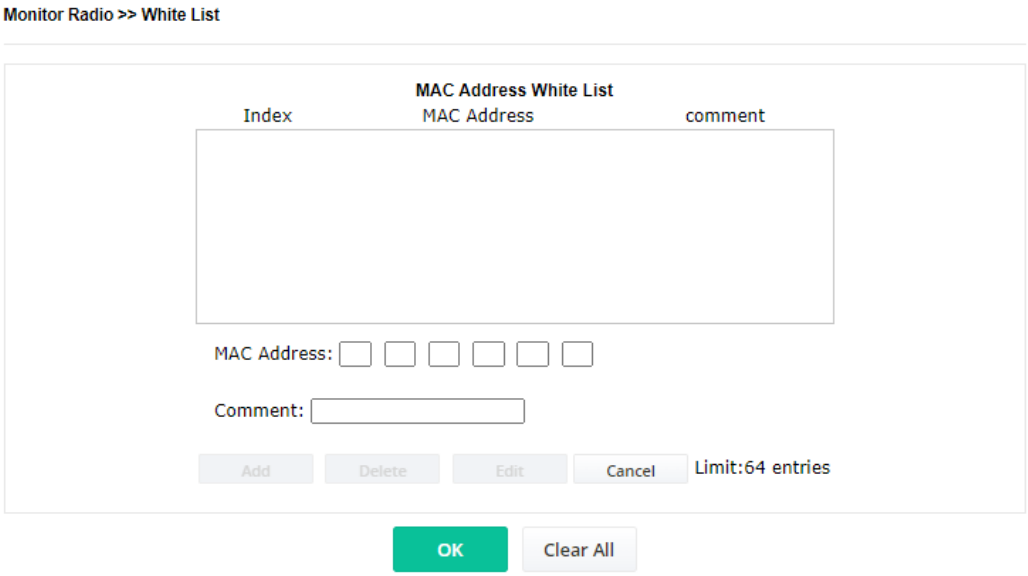

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Rogue AP** | |
| **Enable Mail Alert for Medium / High threat level** | If enabled, Vigor system will send an e-mail to the recipient when detecting a rogue AP around.<br>Setup Rogue AP White List - Click the link to open Rogue AP White List page. Any IP listed on the white list will not be treated as rogue AP. |
| **Monitor Radio Channel Setup** | |
| **2.4/5 GHz Wireless LAN** | Available channels for 2.4/5 wireless LAN are listed in this area. Select the one(s) to be monitored.<br>In default, all channels will be selected. |
| **Clear All** | Click this button to remove all of the channel selections. |
| **Tool** | |
| **Network Monitor** | **Start** - Start to record the network information around the AP for a period of time.<br>**Clear** - Delete the file with monitored information.<br>**Download** - Click to download the record. |
| **Packet Capture** | **Start** - Start to record the packet captured passing through the selected channel.<br>**Clear** - Delete the file with packets information. |

| | |
|---|---|
| | **Download** - Click to download the wireless packets. |
| **OK** | Click to save the changes. |
| **Cancel** | Clear the contents of all the above fields. |

## II-6-3 Rogue AP White List

Configure detailed settings for the AP moved from rogue AP to the white list.




Available settings are explained as follows:

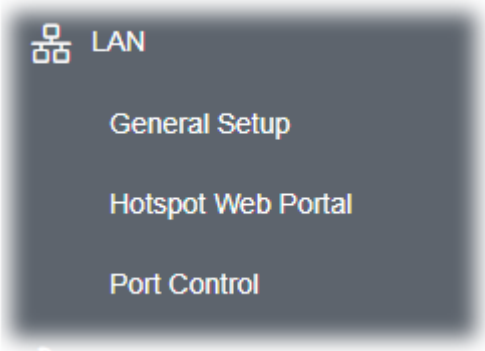
| Item | Description |
|---|---|
| **MAC Address White List** | Displays all MAC addresses in the white list. |
| **MAC Address** | Manually enter the MAC address of the rogue AP. |
| **Comment** | Enter a brief description for the rogue AP. |
| **Add** | After entering the MAC address for a rogue AP, click this button to add the new entry onto MAC Address White List. |
| **Delete** | Delete the selected MAC address from the white list. |
| **Edit** | Update the selected MAC address in the white list using the information entered above. |
| **Cancel** | Clear the contents of all the above fields. This will discard all changes without saving to the MAC Address White List. |
| **OK** | Click to save the changes. |
| **Clear All** | Remove all entries from the MAC Address White List. |

# II-6-4 Monitor Log

This page shows the monitor information for rogue AP device(s).

# II-7 LAN

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

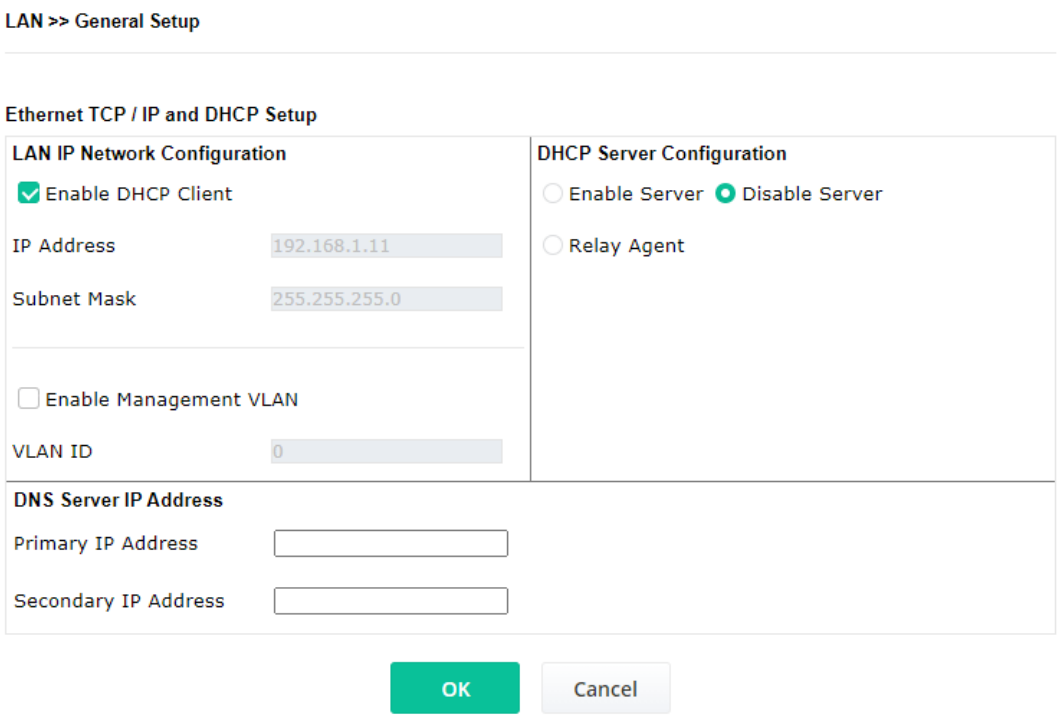



## II-7-1 General Setup

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

**Note:**

This 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 1060C will be treated as a client and can be managed / controlled by AP Management server offered by Vigor router (e.g., Vigor2860).<br>• **IP Address** – Type in private IP address for connecting to a local private network (Default: 192.168.1.2).<br>• **Subnet Mask** – Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)<br>**Enable Management VLAN** – VigorAP 1060C supports tag-based VLAN for wireless clients accessing Vigor device. Only the clients with the specified VLAN ID can access into VigorAP 1060C.<br>• **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.<br>**Enable Server -** Enable Server lets the modem assign IP address to every host in the LAN.<br>• **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.<br>• **End IP Address -** Enter a value of the IP address pool for the DHCP server to end with when issuing IP addresses.<br>• **Subnet Mask -** Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)<br>• **Default Gateway -** Enter a value of the gateway IP address for the DHCP server.<br>• **Lease Time** - It allows you to set the leased time for the specified PC.<br>• **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.<br>• **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.<br>**Relay Agent -** Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to.<br>• **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.<br>**Disable Server -** Disable Server lets you manually or use other DHCP server to assign IP address to every host in the LAN. |

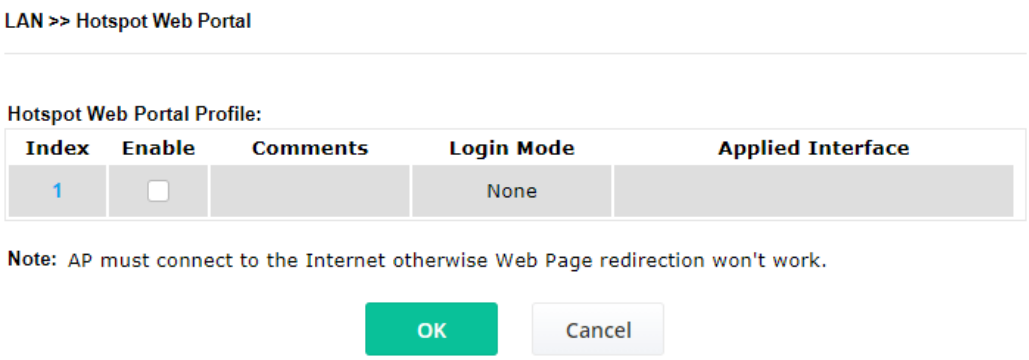
| | |
|---|---|
| **DNS Server IP Address** | **Primary DNS Server -** You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the modem will automatically apply default DNS Server IP address: 194.109.6.66 to this field.<br><br>**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-7-2 Hotspot Web Portal

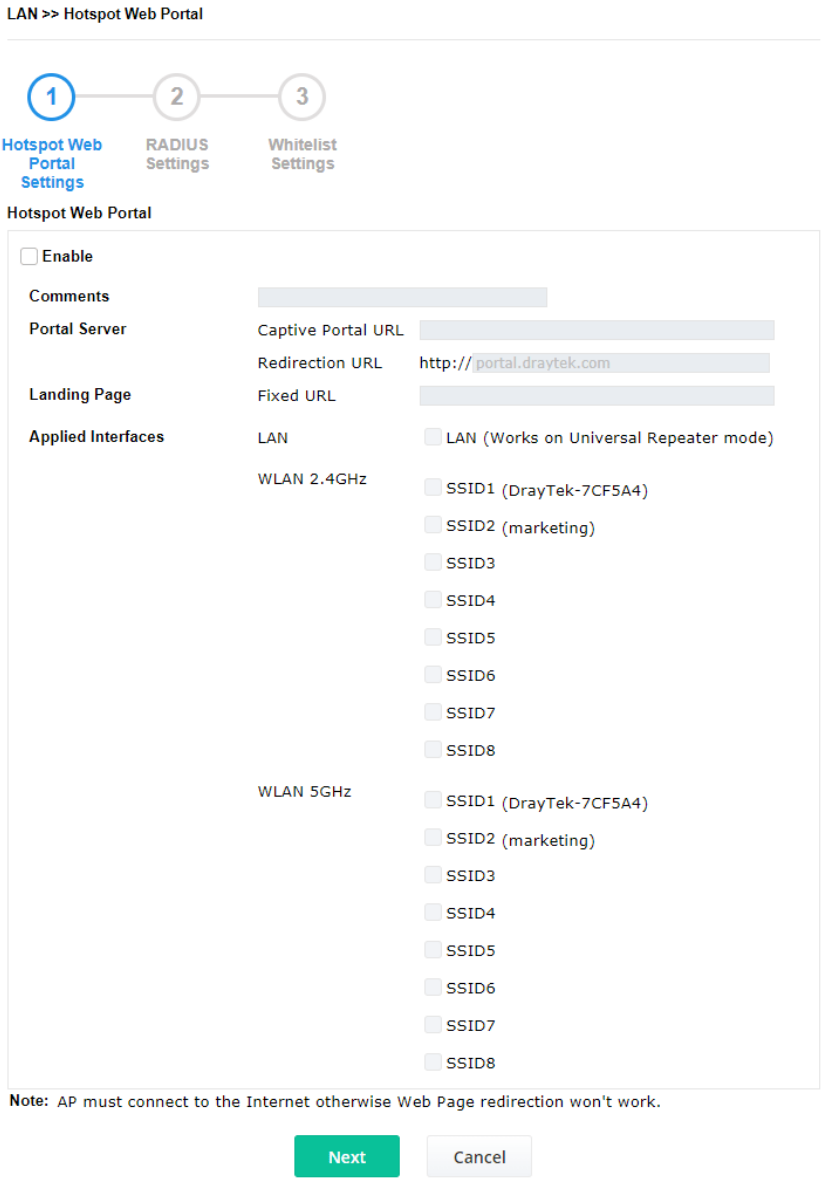
The Hotspot Web Portal feature allows you to set up profiles so that LAN users could either be redirected to specific URLs, or be shown messages when they first connect to the Internet through the router. Users could be required to read and agree to terms and conditions, or authenticate themselves, prior to gaining access to the Internet. Other potential uses include the serving of advertisements and promotional materials, and broadcast of public service announcements.

Click **LAN** to open the LAN settings page and choose **Hotspot Web Portal**. Follow the on-screen steps to configure settings.




Click the index number (e.g., #1 in this case) to open the setting pages.

**(1) Hotspot Web Portal Settings**



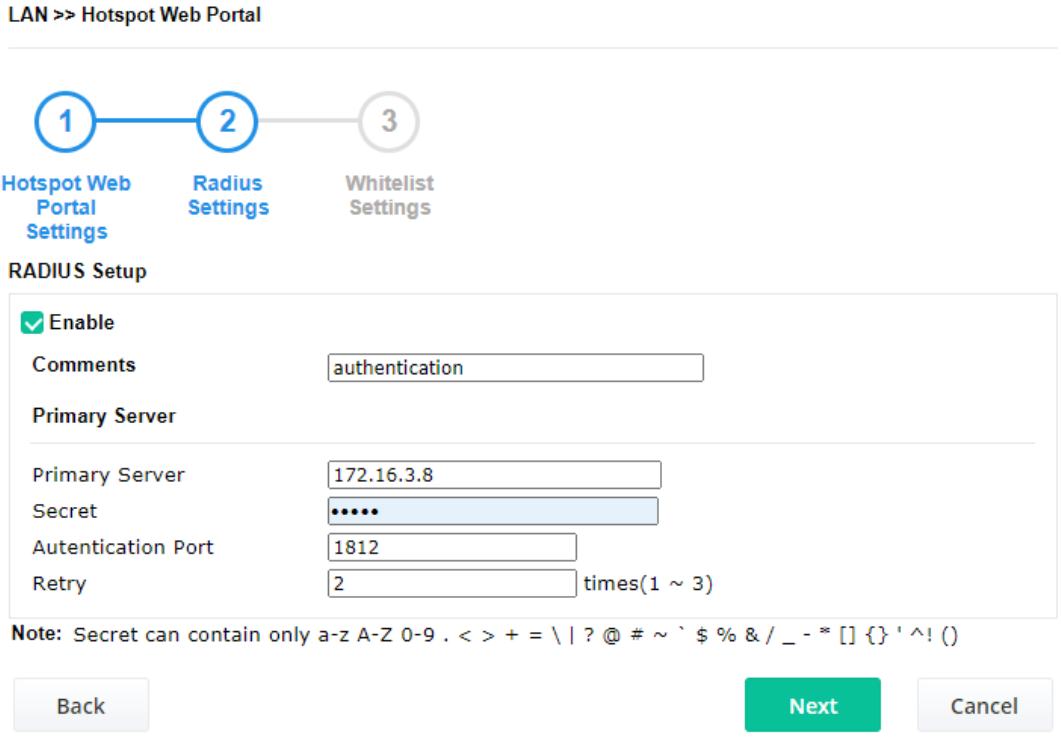

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Check it to enable the hotspot web portal settings. |
| **Comments** | Enter a brief description for this profile. |
| **Portal Server** | **Captive Portal URL -** Enter the captive portal URL.<br>**Redirection URL -** Enter the URL to which the client will be redirected. |
| **Landing page** | **Fixed URL** - Enter the URL as the landing page for wireless clients. |
| **Applied Interfaces** | **LAN -** The current Hotspot Web Portal profile will be in effect for the selected LAN.<br>**SSID1 to SSID8** - The current Hotspot Web Portal profile will be in effect for the selected WLAN SSIDs. |
| **Next** | Click to access into next page. |

After finishing this web page configuration, please click **Next** for next setting page.

**(2) RADIUS Settings**

Configure the external RADIUS server for mutual authentication.



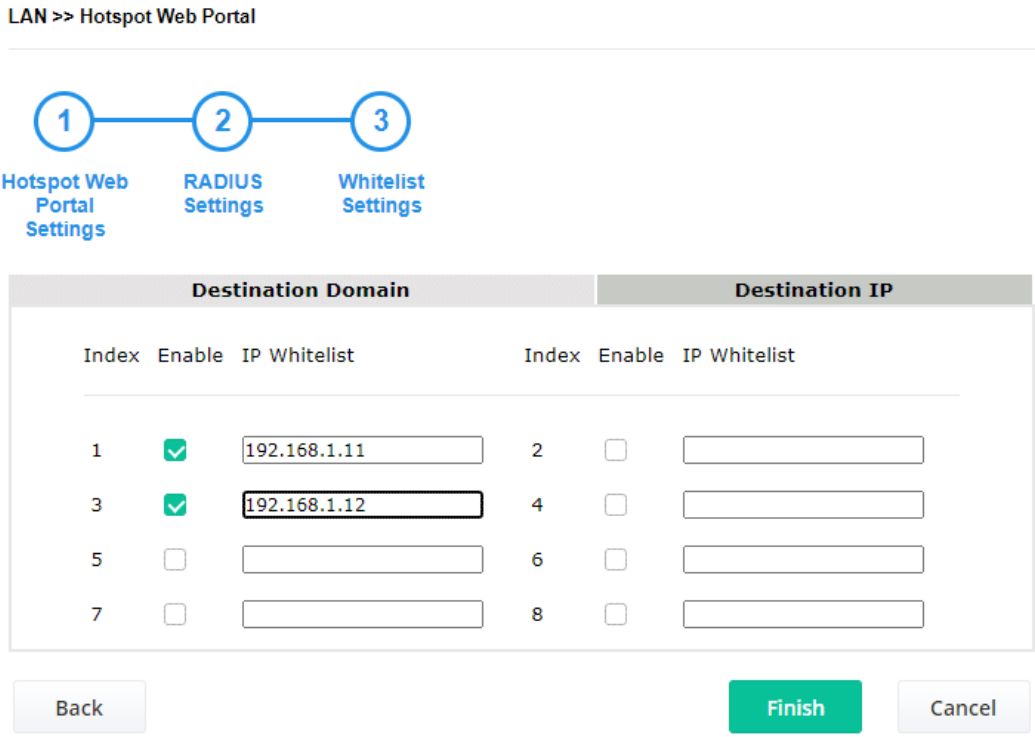

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Check it to enable the RADIUS server settings. |
| **Comments** | Enter a brief description for this profile. |
| **Primary Server** | Enter the IP address of RADIUS server. |
| **Secret** | The 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. The maximum length of the shared secret you can set is 36 characters. |
| **Authentication Port** | The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138. |
| **Retry** | Set the number of attempts to perform reconnection with RADIUS server. |
| **Next** | Click to access into next page. |

After finishing this web page configuration, please click **Next** for next setting page.

### (3) Whitelist Settings

Users are allowed to send and receive the traffic that satisfies whitelist settings. IPs under whitelist will not be redirected to other website (URL).



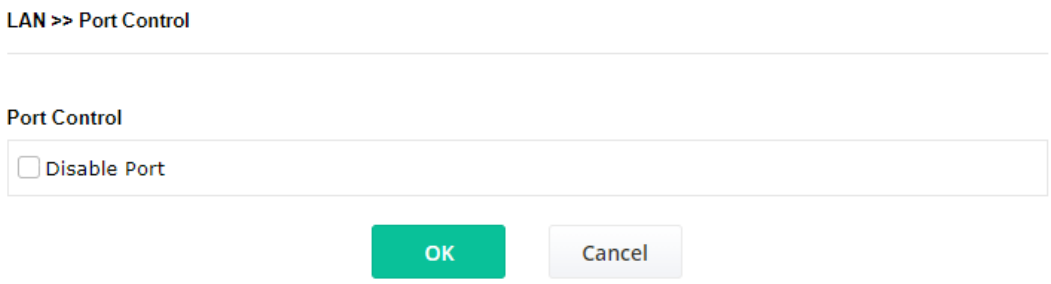

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Destination Domain** | |
| **Enable** | Check to enable the setting. |
| **Domain Whitelist** | Enter a domain (URL) / an IP address. |
| **Destination IP** | |
| **Enable** | Check to enable the setting. |
| **IP Whitelist** | LAN users with the IPs set in this page are able to access into Internet without entering other portal. |
| **Finish** | Click to save the settings. |

After finishing this web page configuration, please click **Finish** to complete the configuration.

## II-7-3 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 |
|---|---|
| **Port Control** | |
| **Disable Port** | Check to disable the function of physical LAN port. |

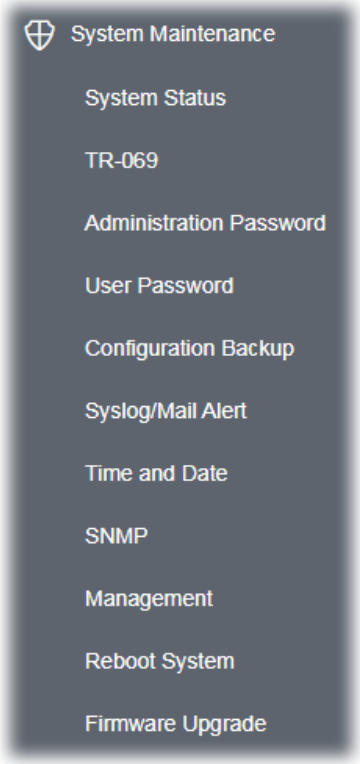
After finishing this web page configuration, please click **OK** to save the settings.

# Chapter III Management

# III-1 System Maintenance

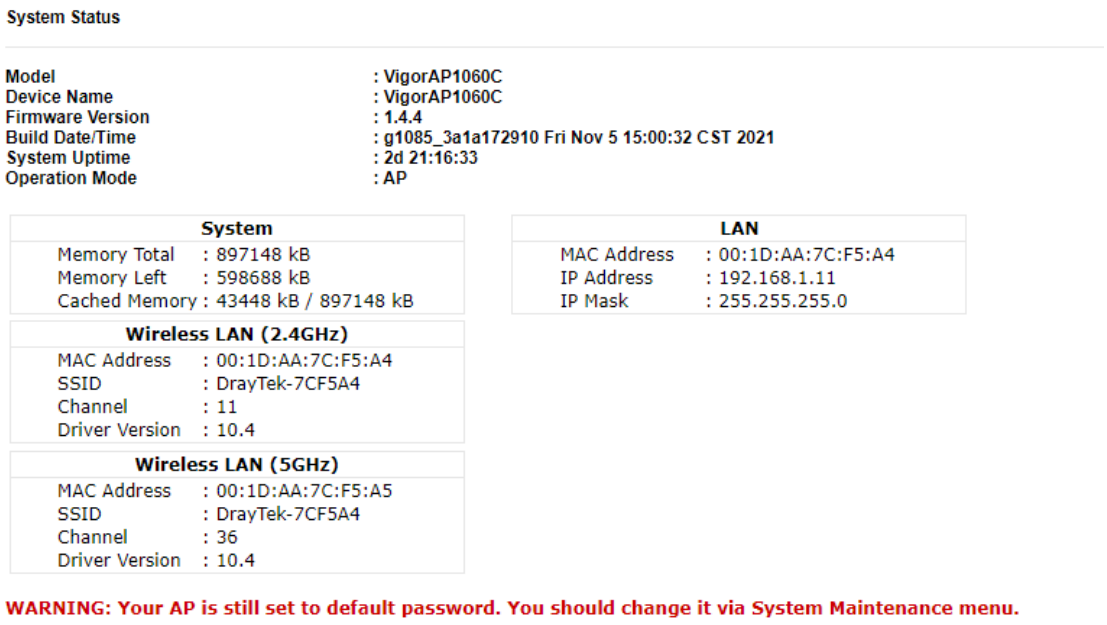
For the system setup, there are several items that you have to know the way of configuration: Status, TR-069, Administrator Password, User Password, Configuration Backup, Syslog/Mail Alert, Time and Date, SNMP, Management, Reboot System, and Firmware Upgrade.

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.

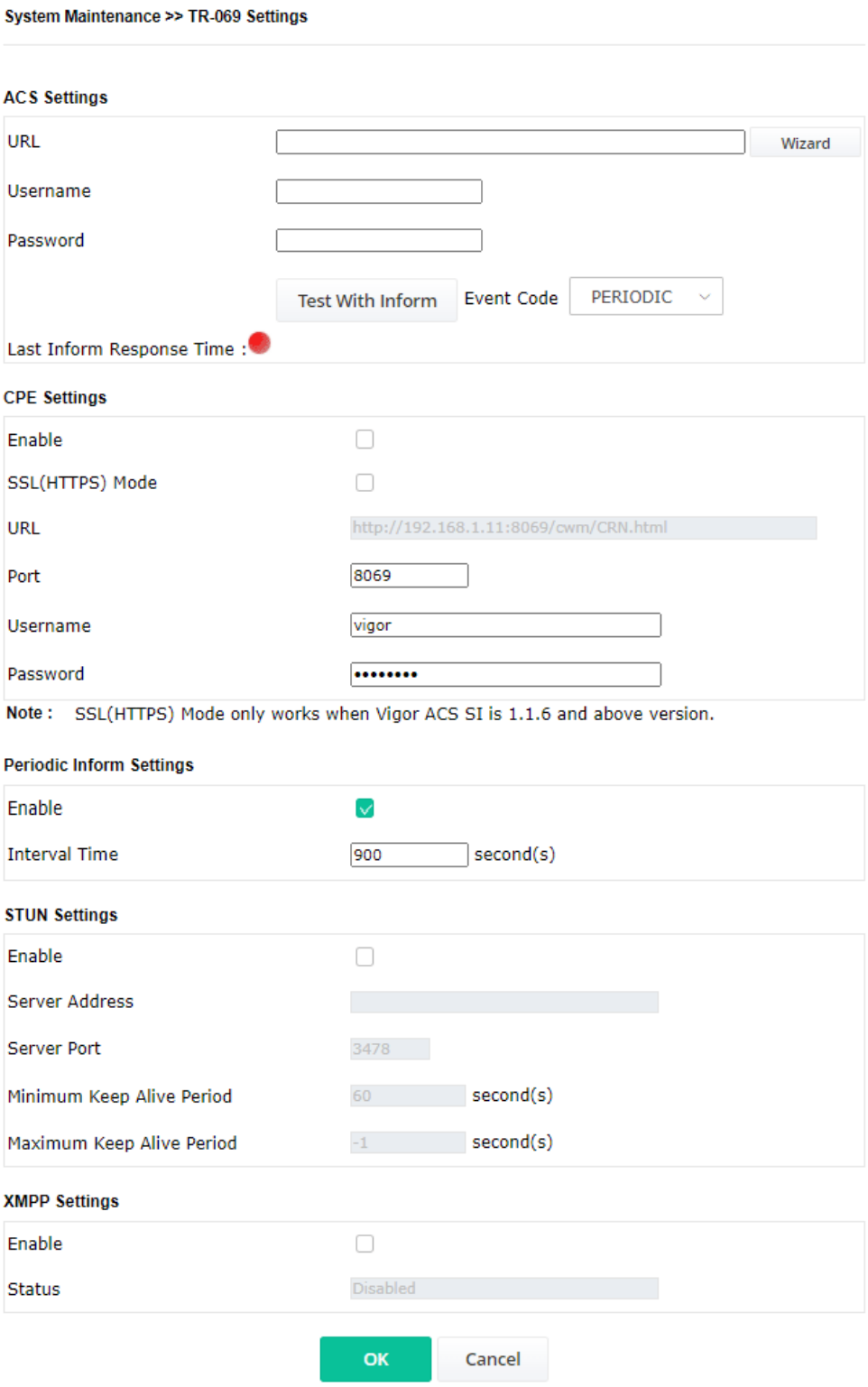



Each item is explained as follows:

| 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:

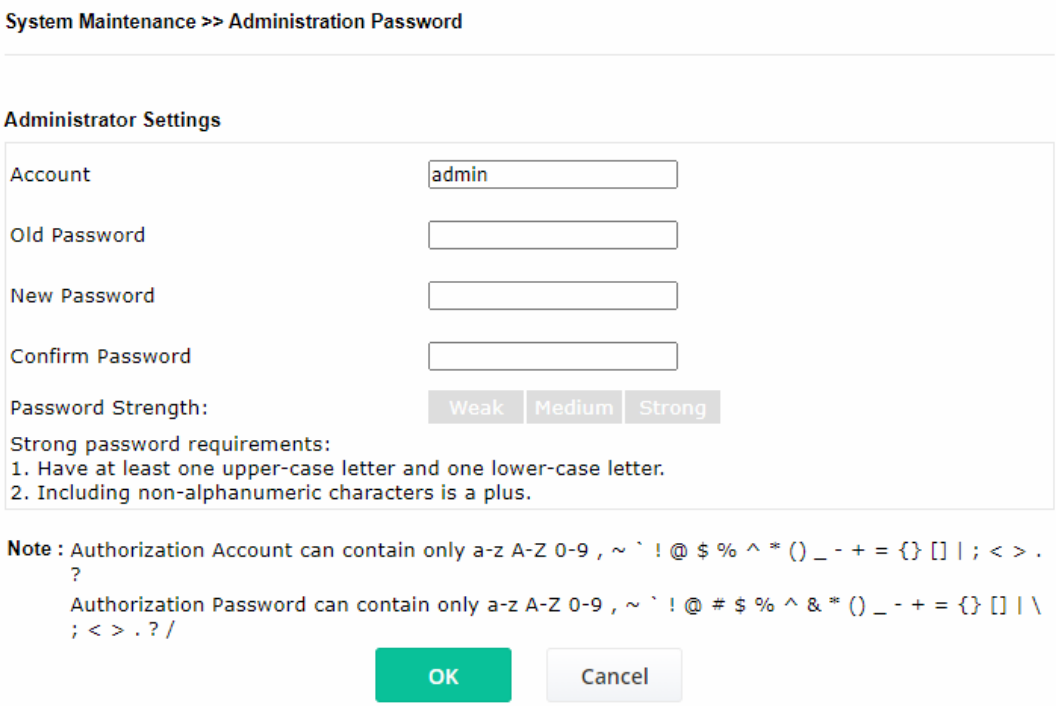
| Item | Description |
|---|---|
| **ACS Settings** | **Wizard** – Click it to enter the IP address of VigorACS server host, port |

| | |
|---|---|
| | number and the handler.<br>**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.<br>**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.<br>**Event Cod**e – Use the drop down menu to specify an event to perform the test.<br>**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).<br>**Enable**– Check the box to allow the CPE Client to connect with Auto Configuration Server.<br>**SSL(HTTPS) Mode** - Check the box to allow the CPE client to connect with ACS through SSL.<br>**Port** – Sometimes, port conflict might be occurred. To solve such problem, you might change port number for CPE.<br>**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.<br>**Interval Time** – Type the value for the interval time setting. The unit is "second". |
| **STUN Settings** | The default is **Disable**.<br>Check the box to enable the service and type the relational settings listed below:<br>**Server Address –** Type the IP address of the STUN server.<br>**Server Port –** Type the port number of the STUN server.<br>**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".<br>**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. |
| **XMPP Settings** | XMPP is an abbreviation of Extensible Messaging and Presence Protocol. If your AP register to XMPP server, it could help VigorACS to manage the AP **under the NAT** at any time, without obstruction. |

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.



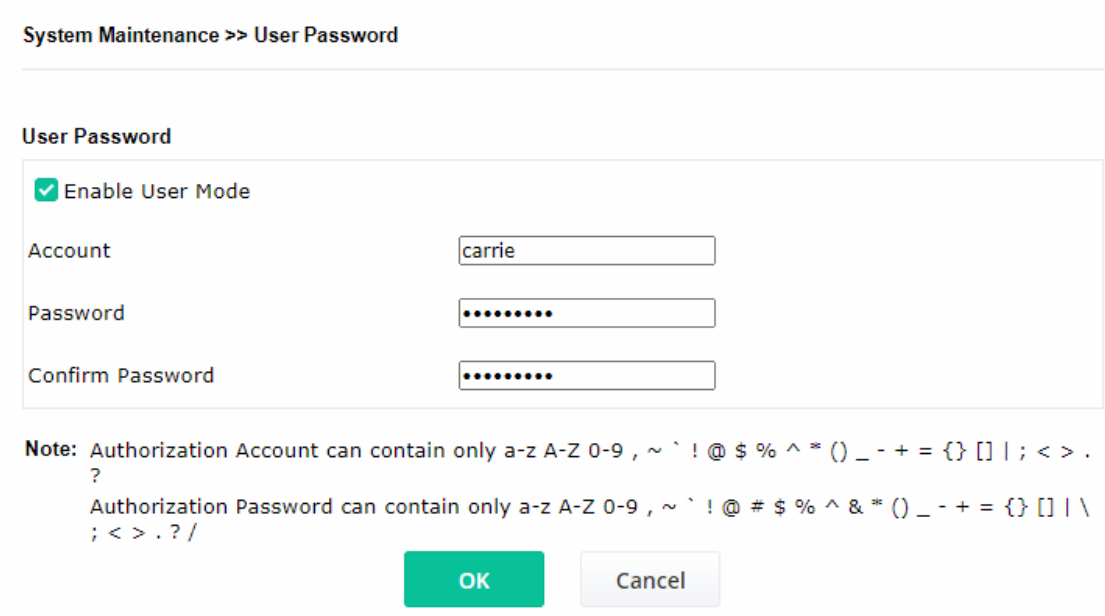

Available settings are explained as follows:

| 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:

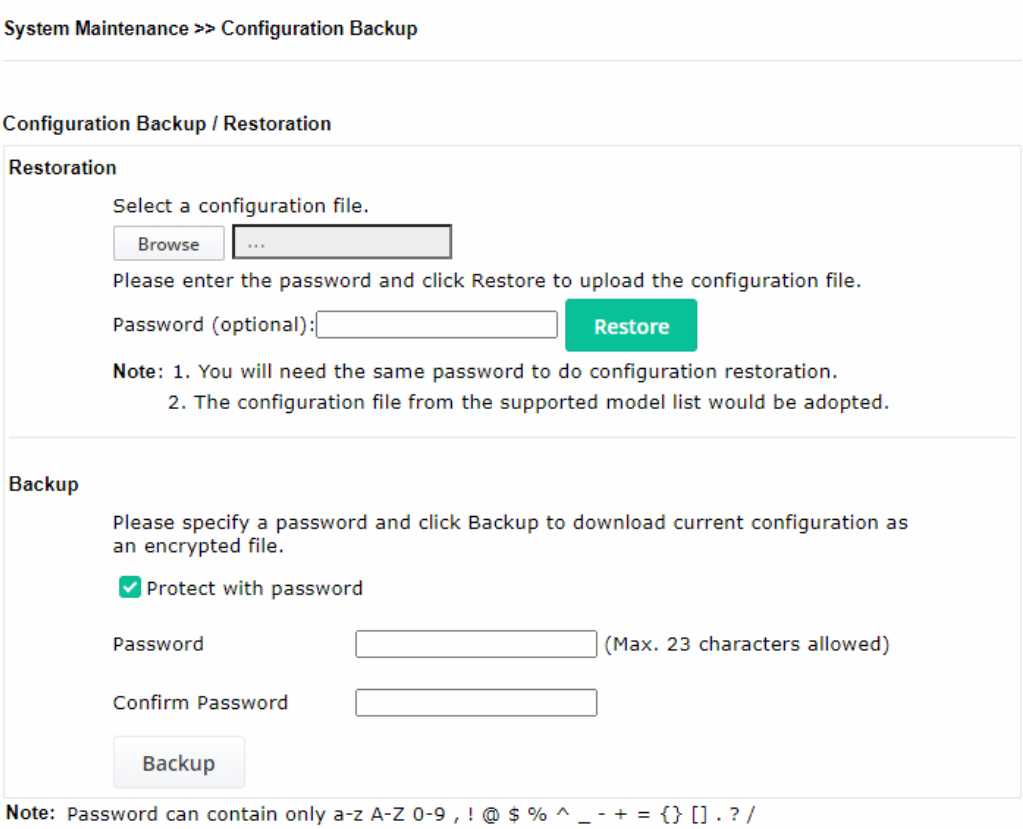
| Item | Description |
|---|---|
| **Enable User Mode** | After checking this box, you can access into the web user interface with the password typed here for simple web configuration.<br>The settings on simple web user interface will be different with full web user interface accessed by using the administrator 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. |

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 1060C settings.




Available settings are explained as follows:

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

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. 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.

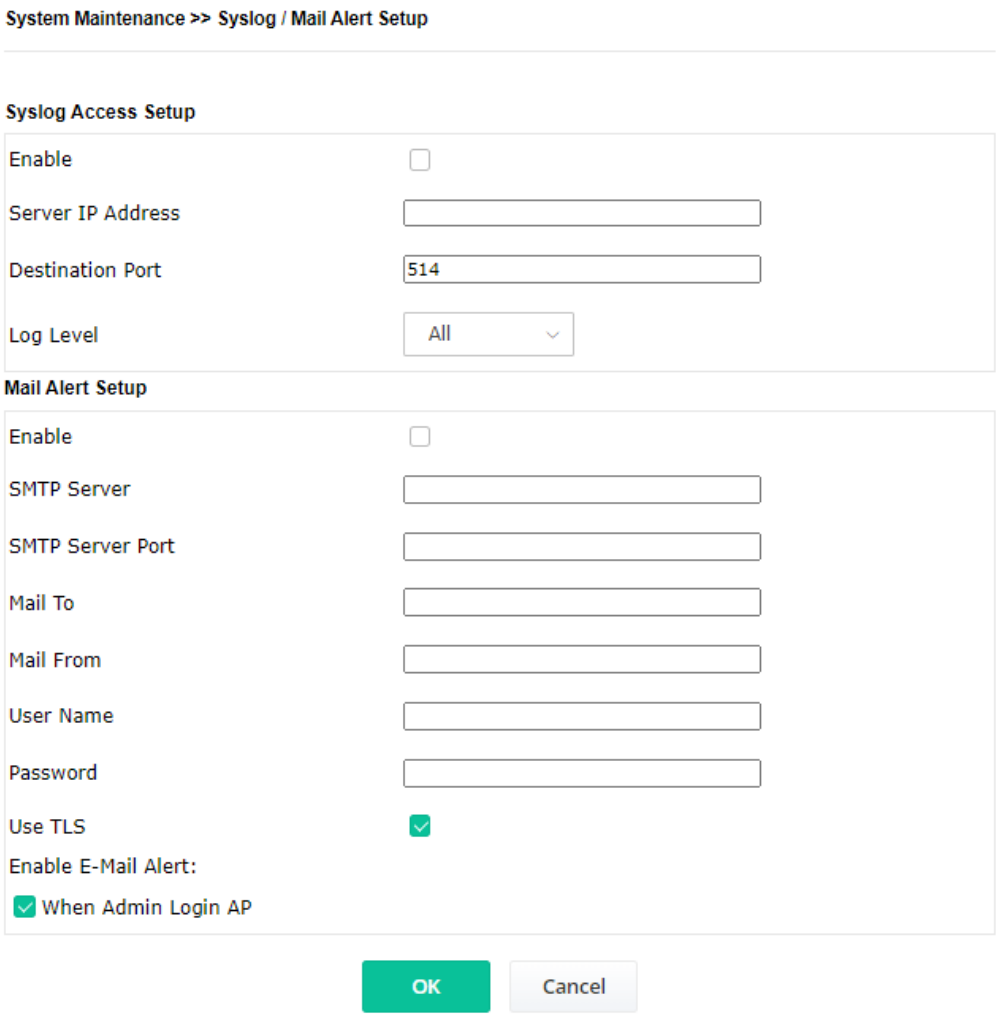
---

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.

## 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:

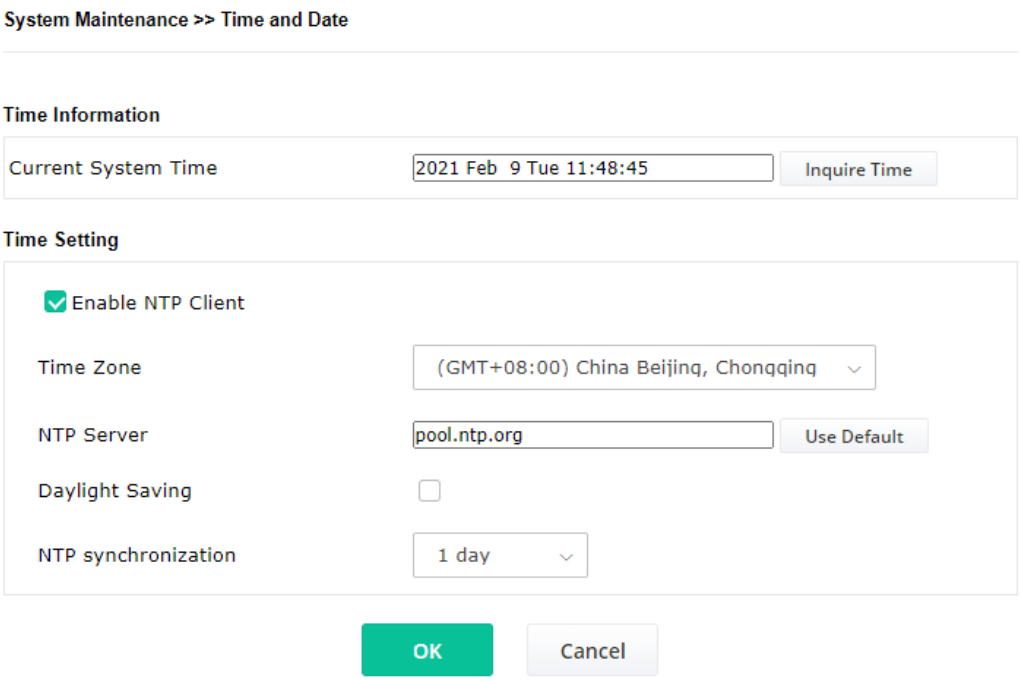
| Item | Description |
|---|---|
| **Syslog Access Setup** | **Enable** - Check **Enable** to activate function of Syslog.<br>**Server IP Address** -The IP address of the Syslog server.<br>**Destination Port** - Assign a port for the Syslog protocol. The default setting is 514.<br>**Log Level** - Specify 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.<br>**SMTP Server -** The IP address of the SMTP server.<br>**SMTP Server Port** - Assign a port for the SMTP server.<br>**Mail To -** Assign a mail address for sending mails out.<br>**Mail From -** Assign a path for receiving the mail from outside. |

| | |
|---|---|
| | **User Name -** Type the user name for authentication.<br>**Password -** Type the password for authentication.<br>**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.<br>**Enable E-Mail Alert** - VigorAP will send an e-mail out when a user accesses into the user interface by using web or telnet.<br>**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. |
| **Enable NTP Client** | Select to inquire time information from Time Server on the Internet using assigned protocol.<br>● **Time Zone** - Select a time protocol.<br>● **NTP Server** - Type the IP address of the time server.<br>**Use Default** – Click it to choose the default NTP server.<br>● **Daylight Saving** - Check the box to enable the daylight saving. Such feature is available for certain area.<br>● **NTP synchronization -** Select a time interval for updating from |

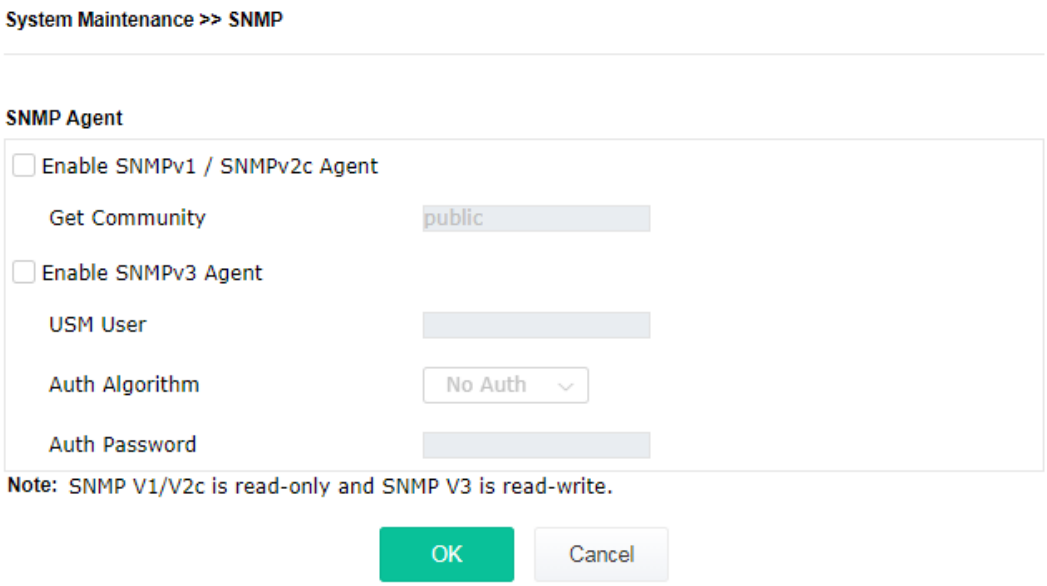
| | |
|---|---|
| | the NTP server. |
| **OK** | Save the settings. |

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.



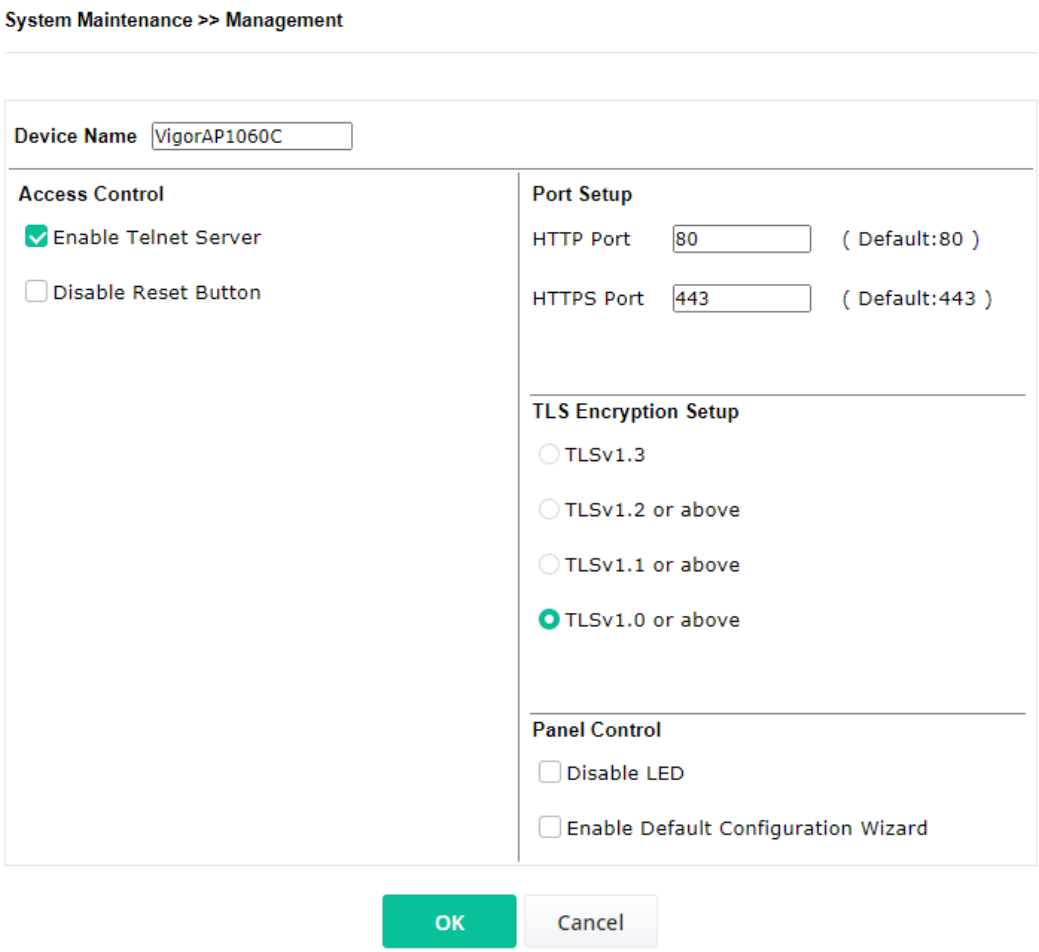

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable SNMPv1 / SNMPv2 Agent** | Check it to enable this function. |
| **Enable SNMPV3 Agent** | Check it to enable this function. |
| **USM User** | USM means user-based security mode.<br>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:

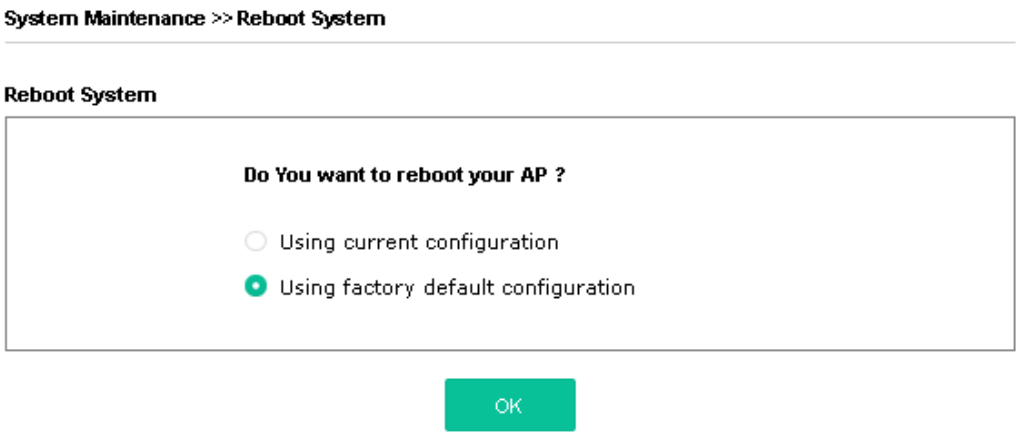
| Item | Description |
|---|---|
| **Device Name** | The default setting is VigorAP 1060C. Change the name if required. |
| **Access Control** | **Enable Telnet Server**– The administrator / user can access into the command line interface of VigorAP remotely for configuring settings.<br>**Disable Reset Button** - If enabled, the function of the **Reset** button will be invalid. |
| **Port Setup** | **HTTP port/HTTPS port** -Specify user-defined port numbers for the HTTP and HTTPS servers. |
| **TLS Encryption Setup** | Select to enable the function of TLS 1.0/1.1/1.2/1.3 if required.<br>Due to security consideration, the built-in HTTPS server had upgraded to TLS1.x protocol. |
| **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.<br>**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.<br><br>Such function will be disabled 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:**

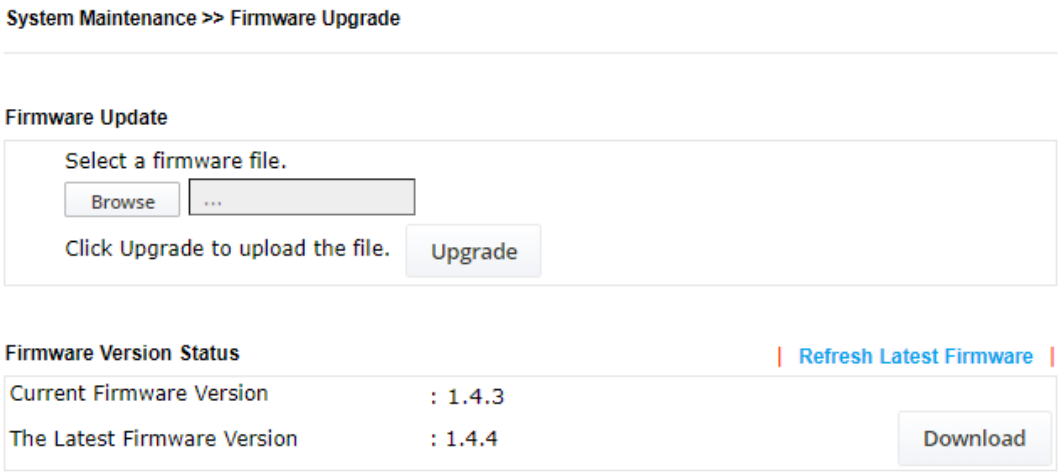
When the system pops up Reboot System web page after configuring the web settings, please click **OK** to reboot your device for ensuring normal operation and preventing unexpected errors of the modem in the future.

# III-1-11 Firmware Upgrade

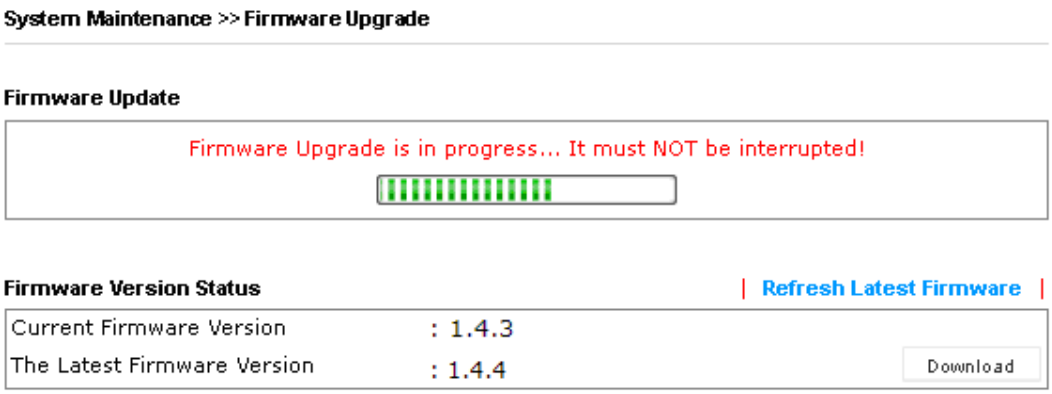
Before upgrading your modem firmware, you need to install the Modem Tools. The **Firmware Upgrade Utility** is included in the tools. The following web page will guide you to upgrade firmware by using an example. Note that this example is running over Windows OS (Operating System).

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.

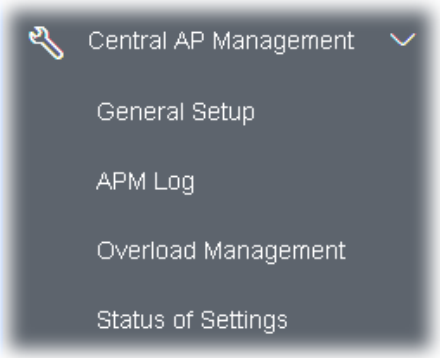



Click **Download** to locate the newest firmware from your hard disk and click **Upgrade**.

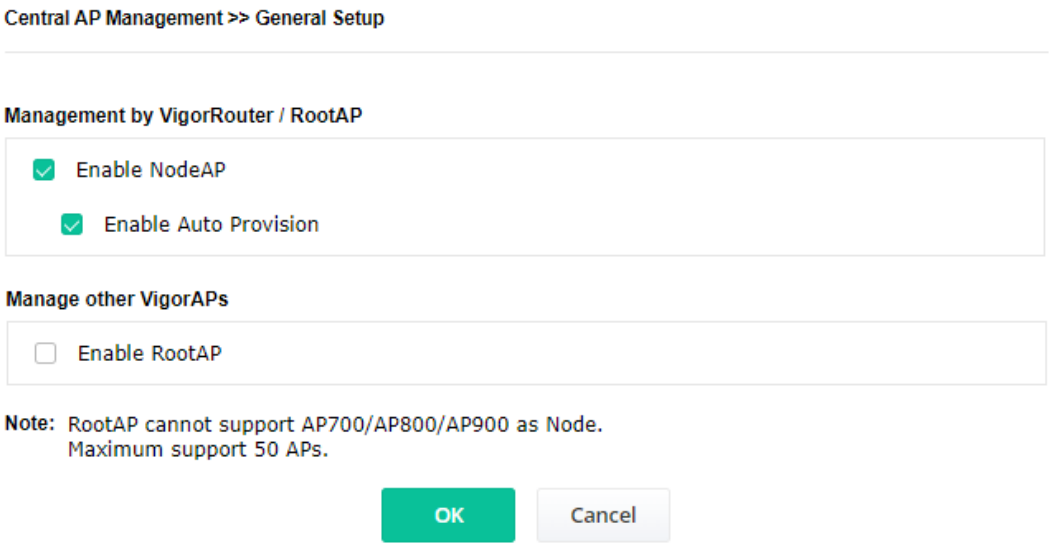


# III-2 Central AP Management

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:

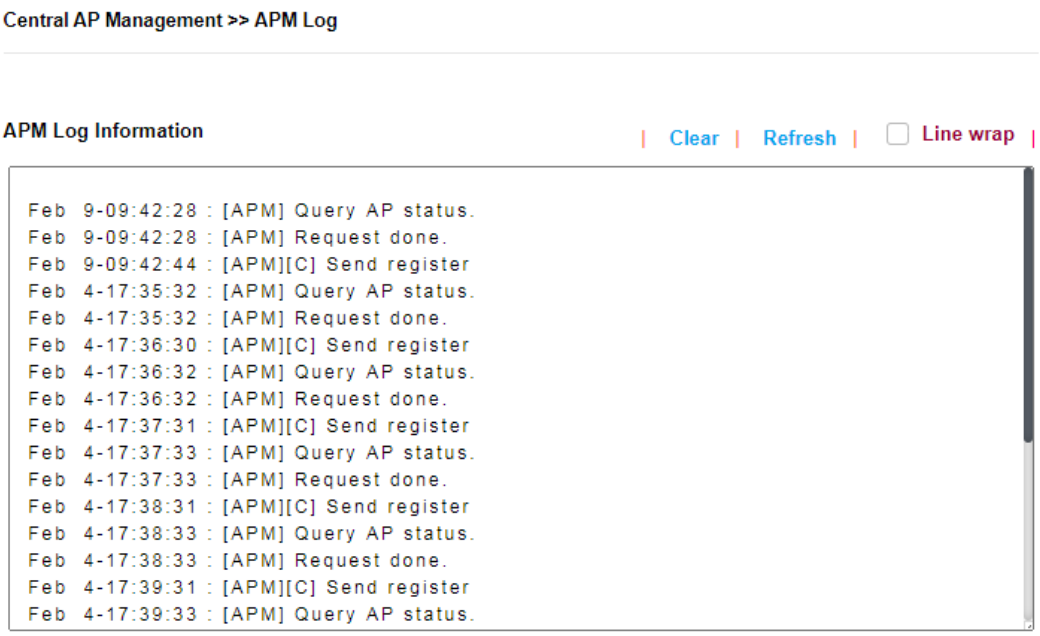
| Item | Description |
|---|---|
| **Enable NodeAP** | Check the box to enable the function of AP Management (APM). |
| **Enable Auto Provision** | VigorAP 1060C can be controlled under Central AP Management in Vigor2862 series. When both Vigor2862 series and VigorAP 1060C have such feature enabled, once VigorAP 1060C is registered to Vigor2862 series, the **WLAN profile** pre-configured on Vigor2862 series will be applied to VigorAP 1060C immediately. Thus, it is not necessary to configure VigorAP 1060C separately. |
| **Enable RootAP** | Check this box to enable AP management. The role of this AP is "Root". |

Click **OK** to save these settings.

# III-2-2 APM Log

This page will display log information related to wireless stations connected to VigorAP 1060C and central AP management.

Such information also will be delivered to Vigor router (e.g., Vigor2862 or Vigor2926 series) and be shown on **Central AP Management>>Event Log** of Vigor router.

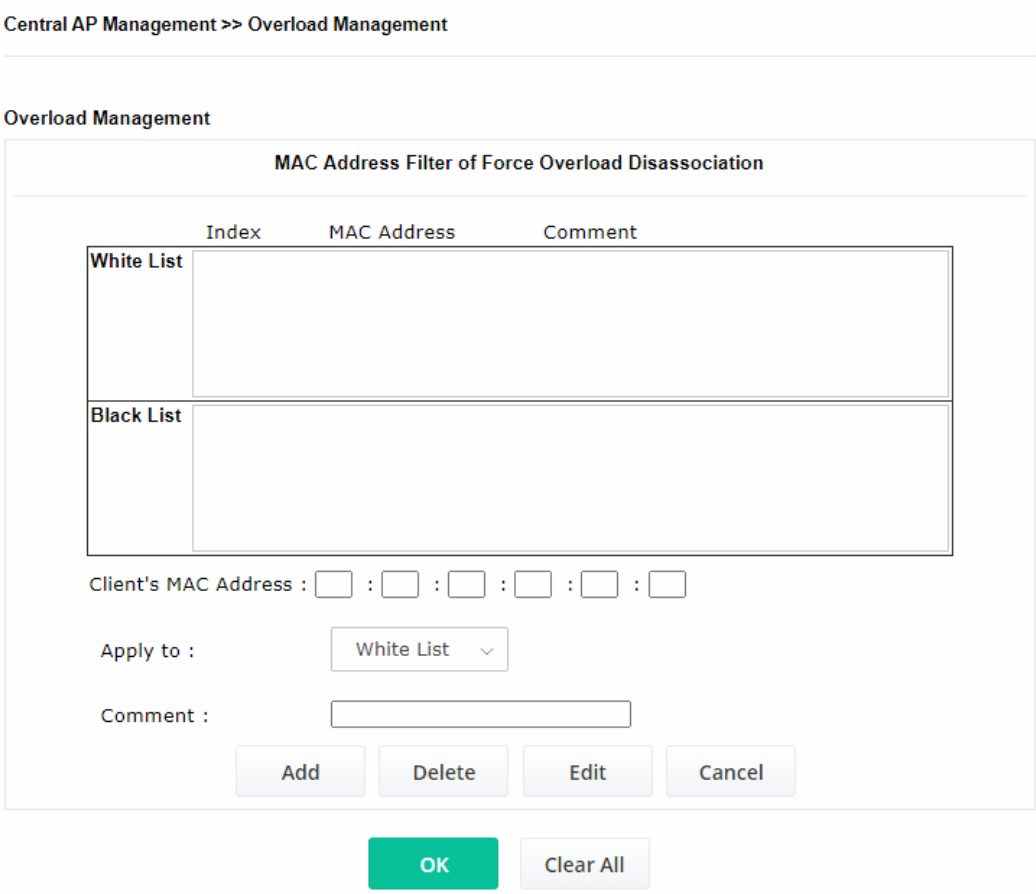


# III-2-3 Overload Management

Load Balance can help to distribute the traffic for all of the access points (e.g., VigorAP 1060C) 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 1060C 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., Vigor2860 or Vigor2925 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.<br><br>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.<br><br>**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 1060C) registered to Vigor 2862 or Vigor2926 series. This web page displays the settings related to Load Balance for VigorAP 1060C. In which, By Station Number, By Traffic and Force Overload Disassociation indicate settings configured in Vigor2862 or Vigor2926 series.

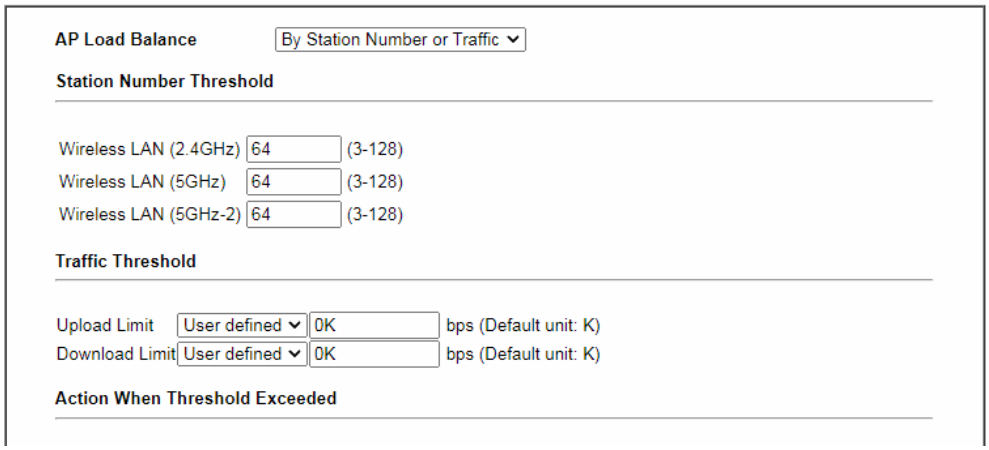
**Central AP Management >> Status of Settings**

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

"X" means the function is not enabled or VigorAP 1060C has not registered to any Vigor router yet.

Below shows a setting example for Load Balance settings configured in Vigor2927 series.

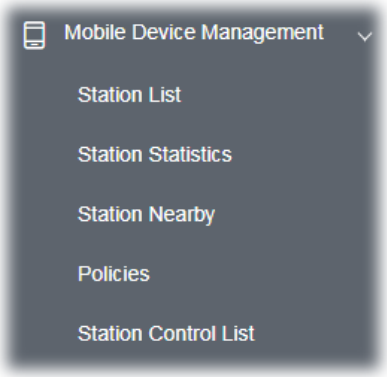
Central Management >> AP >> Load Balance



# 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).

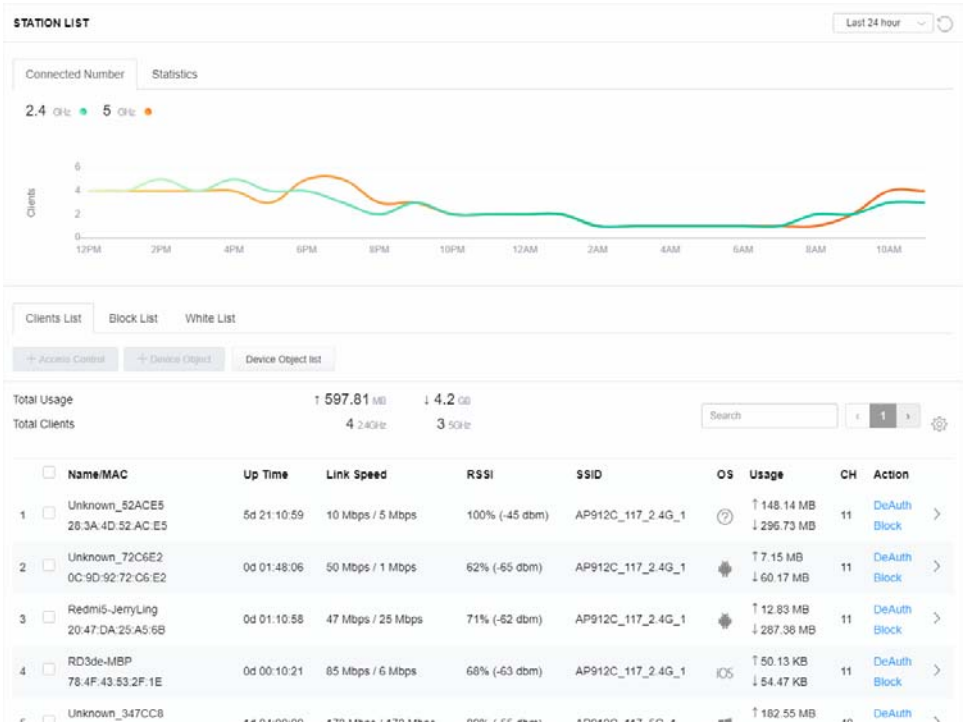



## III-3-1 Station List

**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

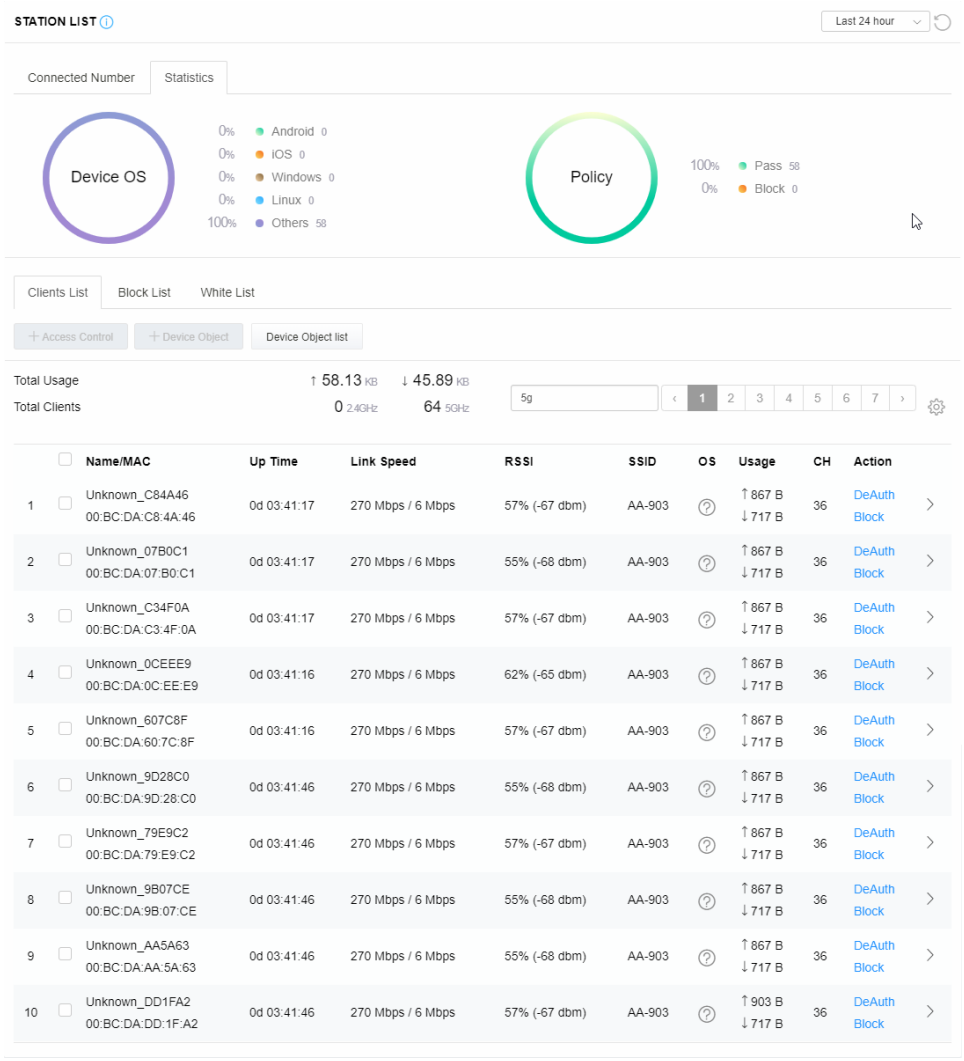
### III-3-1-1 Connected Number

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

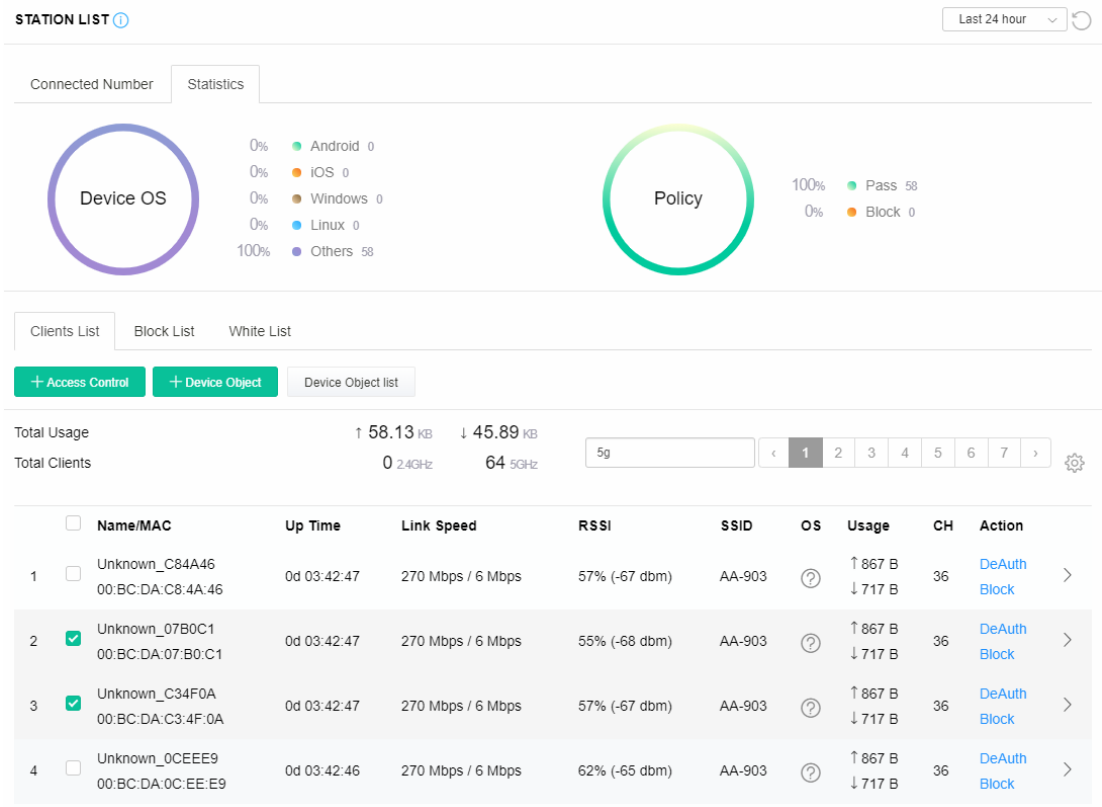
The number of detected devices and the number of device(s) passed/blocked according to the policy specified in **Mobile Device Management>>Policies** can be illustrated as doughnut chart.



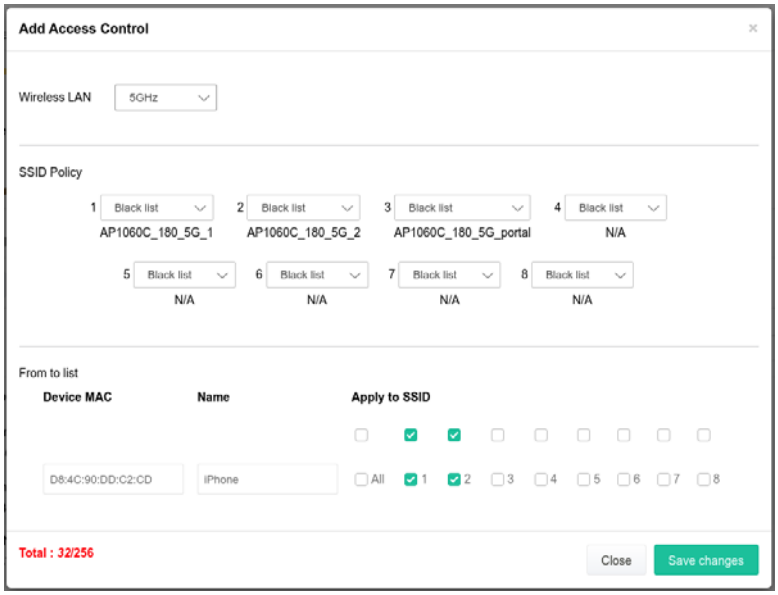

| | Name/MAC | Up Time | Link Speed | RSSI | SSID | OS | Usage | CH | Action |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Unknown_C84A46<br>00:BC:DA:C8:4A:46 | 0d 03:41:17 | 270 Mbps / 6 Mbps | 57% (-67 dbm) | AA-903 | | ↑867 B<br>↓717 B | 36 | DeAuth<br>Block |
| 2 | Unknown_07B0C1<br>00:BC:DA:07:B0:C1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

### III-3-1-3 Clients List

The client list displays all the stations connecting to VigorAP.




Available settings are explained as follows:

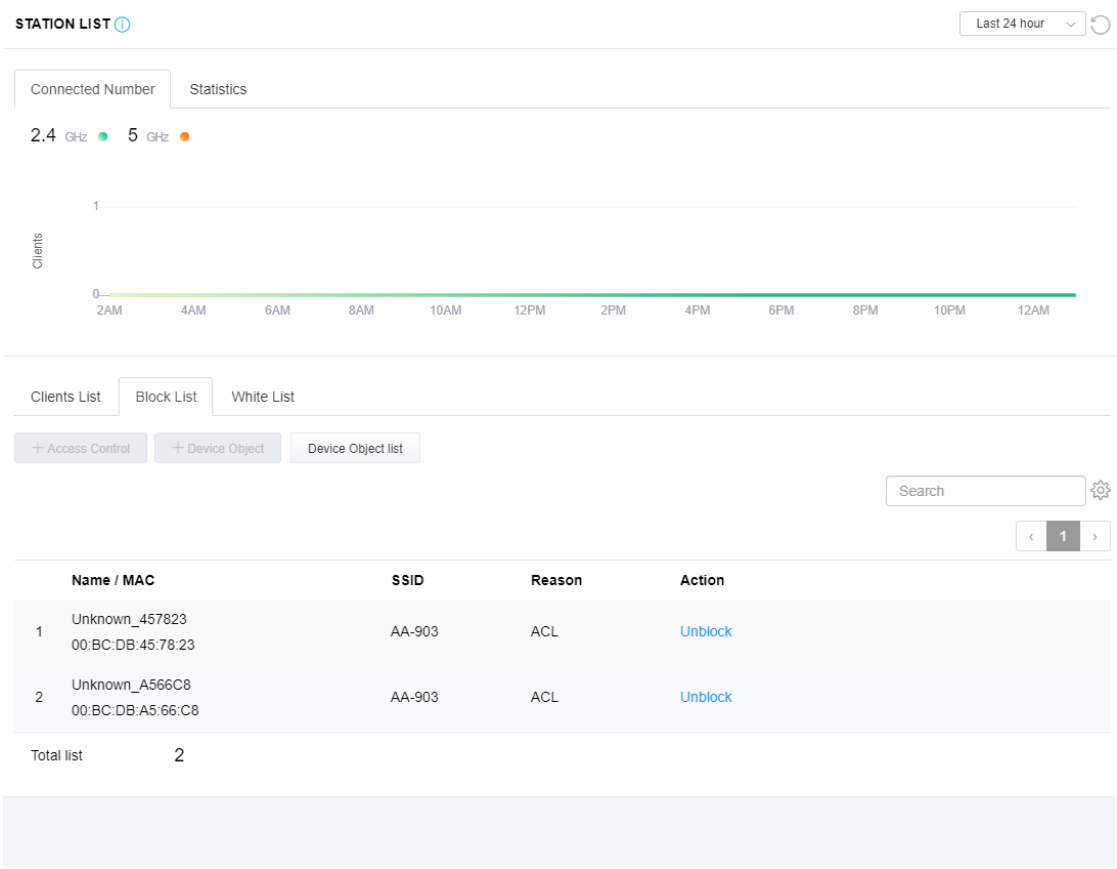
| Item | Description |
|---|---|
| **+Access Control** | It is available after choosing one of the entries (clients) on Clients List.<br>  <br>**Wireless LAN** - Specify the bandwidth for the access control list.<br>**SSID Policy** - Set the policy for each SSID as black list or white list or disable.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

| | |
|---|---|
| | **From to list** - Display the clients available for applying this access control.<br>**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.<br>**Close** - Exit this page without saving any changes.<br>**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.<br> <br>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.<br> |
| **Clients List** | Display the stations connecting to this Vigor device.<br>**Total Usage -** Display the summary of transmission and receiving packets for each device under the client list.<br>**Total Clients -** Display the number of the clients using 2.4GHz.<br>**Name / MAC -** Display the host name / MAC address of the connecting client.<br>**Up Time** - Display the connection time.<br>**Link Speed**- Display the link speed.<br>**RSSI** - Display the RSSI value.<br>**SSID** - Display the SSID the client used for connecting VigorAP.<br>**OS** - Display the OS of the client.<br>**Usage** - Display the bandwidth usage (up and down) of the client.<br>**CH** - Display the channel used by the client.<br>**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.

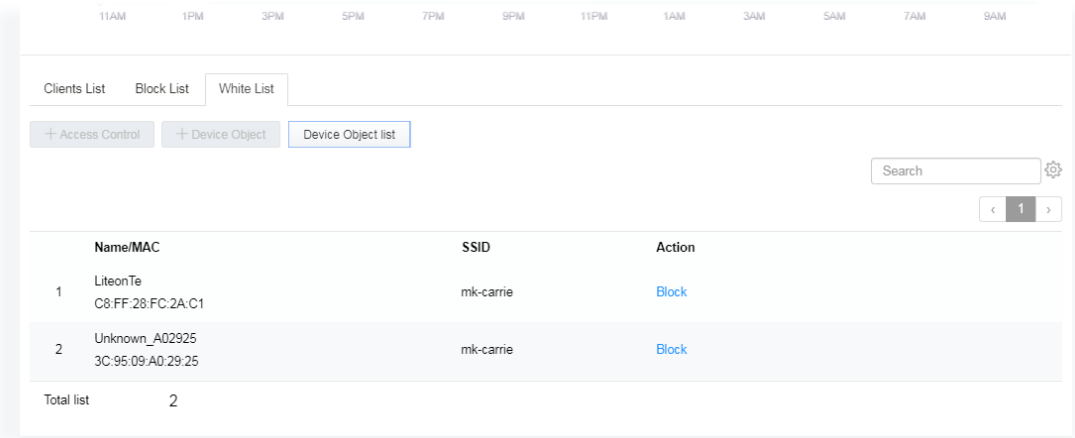



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Device Object list** | Click it to open the Device Object List dialog for reference.<br> |
| **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.<br>**Unblock** - Click to unblock the entry. |

### III-3-1-5 White List

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

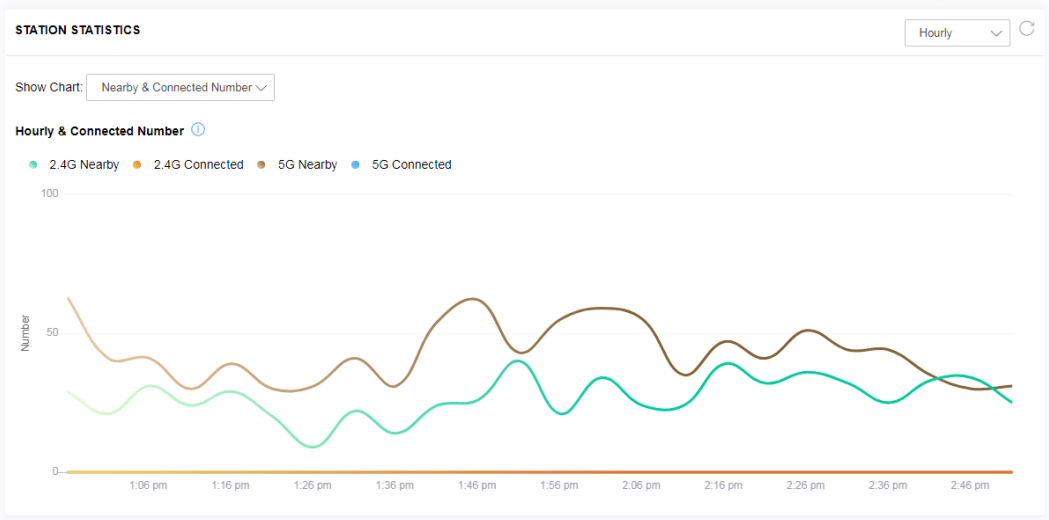



Available settings are explained as follows:

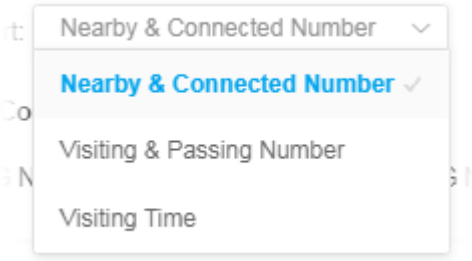
| Item | Description |
|---|---|
| **Device Object list** | Click it to open the Device Object List dialog for reference.<br> |
| **Name / MAC** | Display the host name / MAC Address for the connecting client. |
| **SSID** | Display the SSID that the wireless client connects to. |
| **Action** | Display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

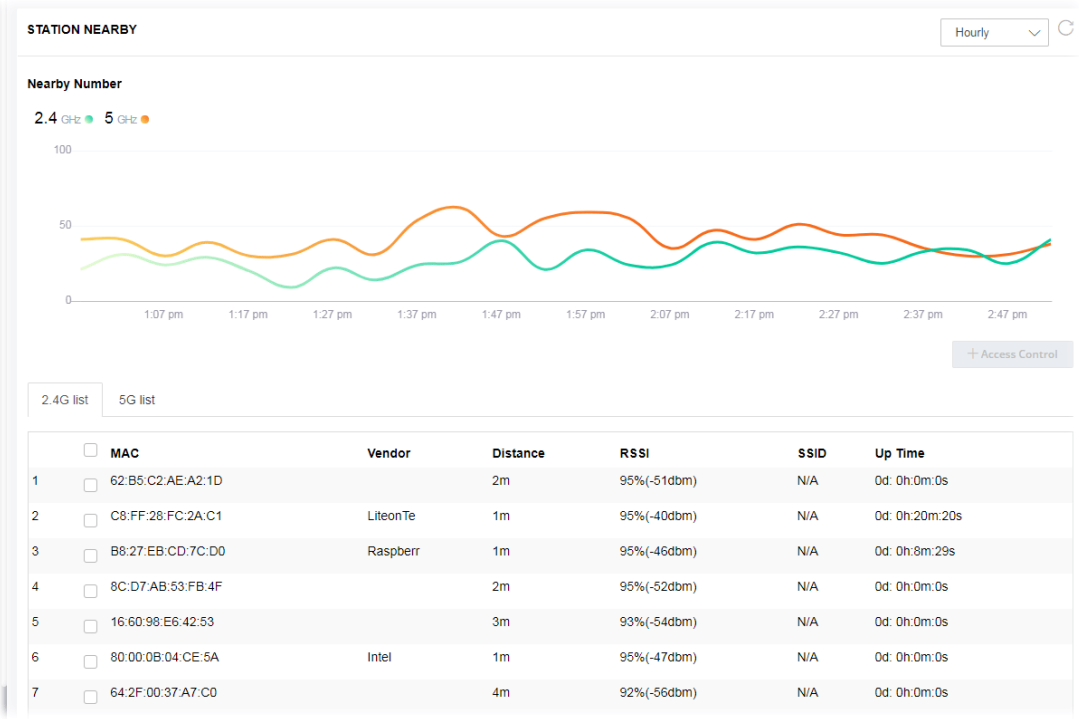



Available parameters are explained as follows:

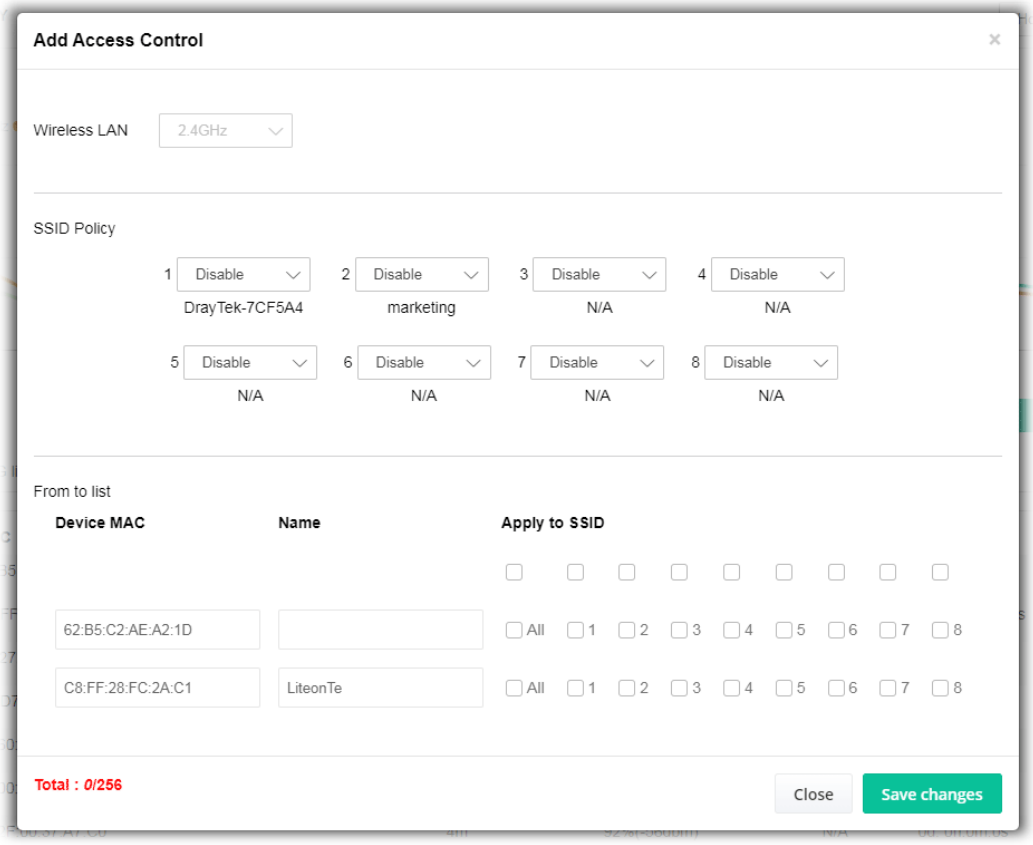
| Item | Description |
|---|---|
| **Show Chart** | Choose one of the items to display the statistics chart for wireless stations.<br>  <br>**Nearby & Connected Number** – Choose it to have the statistics of the wireless stations which is nearby and connected to VigorAP 1060C.<br>**Visiting & Passing Number** – Choose it to have the statistics of the wireless stations which is visiting and passing to VigorAP 1060C.<br>**Visiting Time** - Choose it to have the statistics of the wireless stations which is visiting VigorAP 1060C. |

# 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.

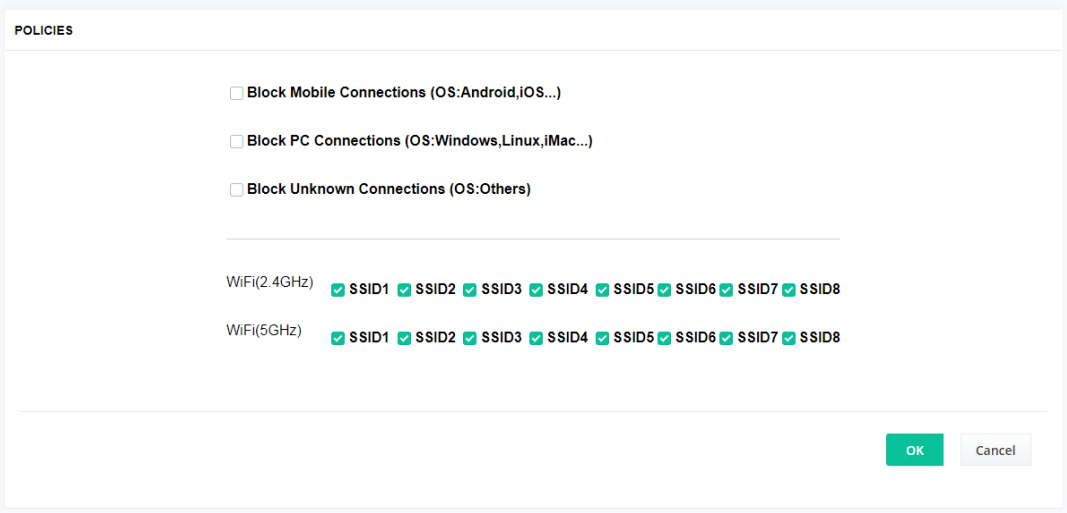


Available parameters are explained as follows:

| Item | Description |
|---|---|
| **SSID Policy** | Determine the policy (disable, white list or black list) applied for the SSID (1 to 8). |
| **From to list** | **Device MAC** - Display the MAC address of the selected station.<br>**Name** - Display the name of the selected station.<br>**Apply to SSID** - Check the box(es) to apply the SSID to the selected station.<br>**Close** - Exit the dialog without saving the changes.<br>**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.



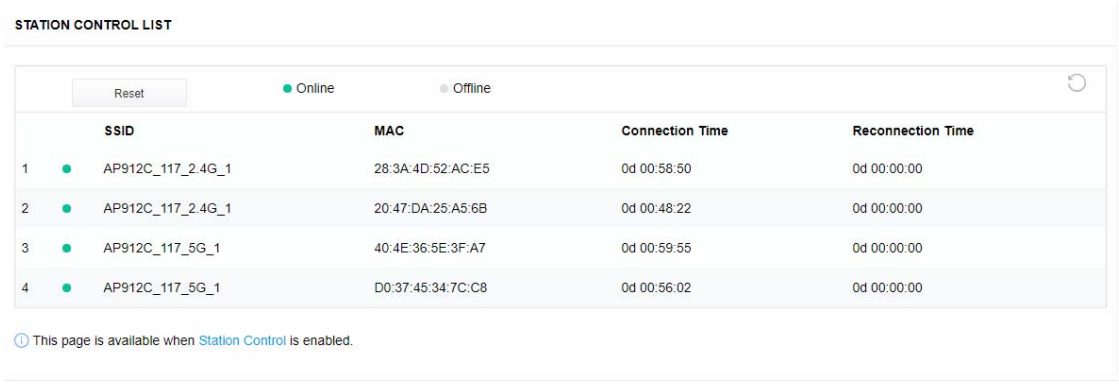

Each item is explained as follows:

| 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.

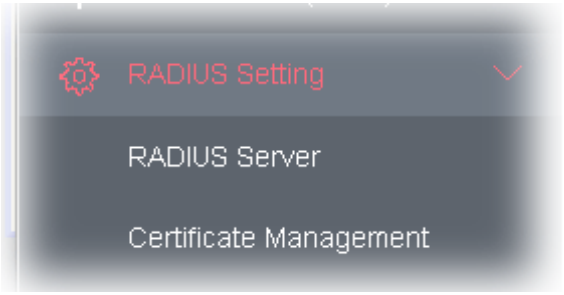
# III-3-5 Station Control List

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



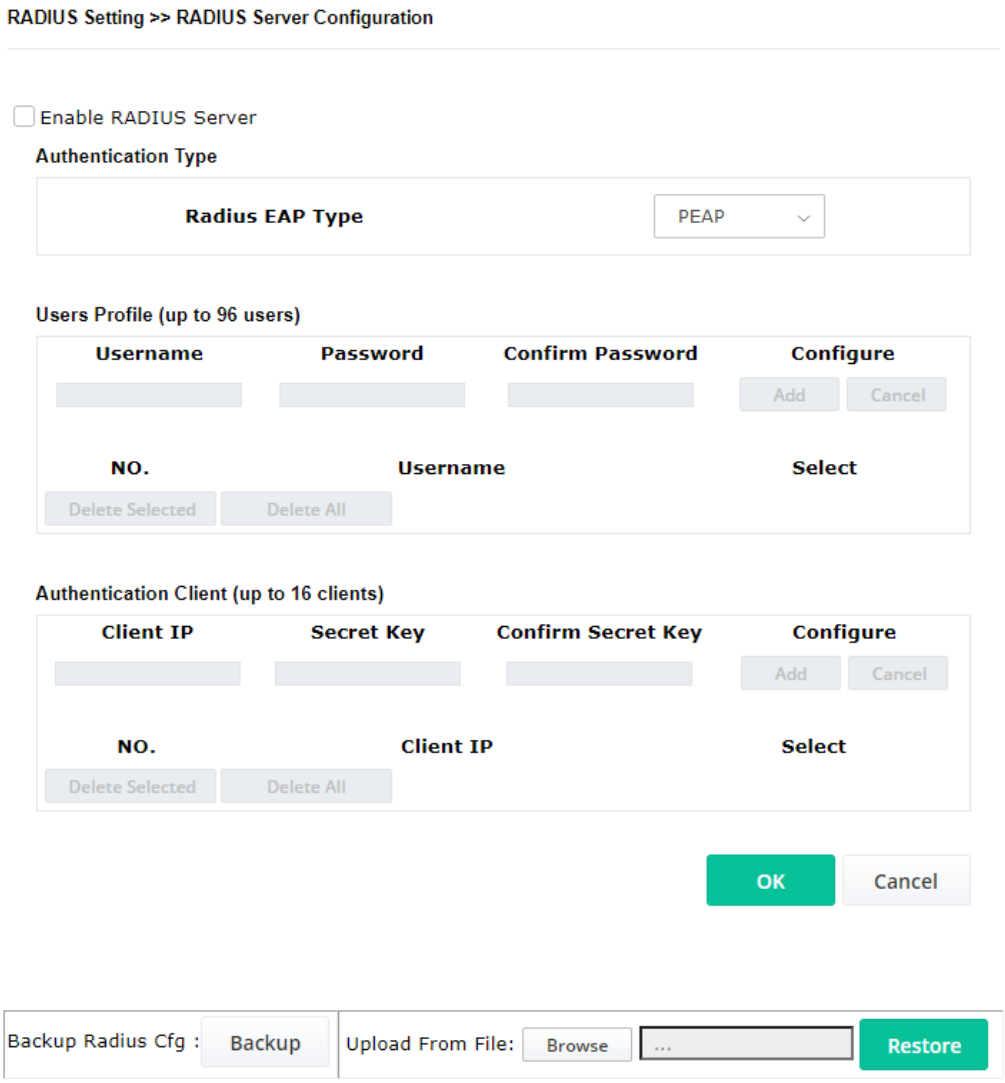
# Chapter IV Others

# IV-1 RADIUS Setting




## IV-1-1 RADIUS Server

VigorAP 1060C offers a built-in RADIUS server to authenticate the wireless client that tries to connect to VigorAP 1060C. 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.<br>**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.<br>**Password** – Type a new password for such new user profile.<br>**Confirm Password** – Retype the password to confirm it.<br>**Configure**<br>• **Add** – Make a new user profile with the name and password specified on the left boxes.<br>• **Cancel** – Clear current settings for user profile.<br>**Delete Selected** – Delete the selected user profile (s).<br>**Delete All** – Delete all of the user profiles. |
| **Authentication Client** | This internal RADIUS server of VigorAP 1060C 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 1060C as its external RADUIS server.<br>**Client IP** – Type the IP address for the user to be authenticated by VigorAP 1060C when the user tries to use VigorAP 1060C as the external RADIUS server.<br>**Secret Key** – Type the password for the user to be authenticated by VigorAP 1060C while the user tries to use VigorAP 1060C as the external RADIUS server.<br>**Confirm Secret Key** – Type the password again for confirmation.<br>**Configure**<br>• **Add** – Make a new client with IP and secret key specified on the left boxes.<br>• **Cancel** – Clear current settings for the client.<br>**Delete Selected** – Delete the selected client(s).<br>**Delete All** – Delete all of the clients. |
| **Backup Radius Cfg** | **Backup** - Click to store the configuration set on this page as a file. |
| **Upload From File** | **Upload** - Click to upload the RADIUS configuration file from the host to VigorAP.<br>**Restore** - Click to restore the RADIUS configuration file to VigorAP. |

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

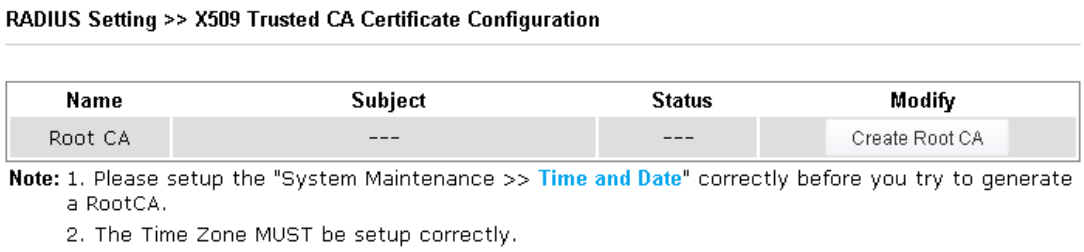
## IV-1-2 Certificate Management

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.

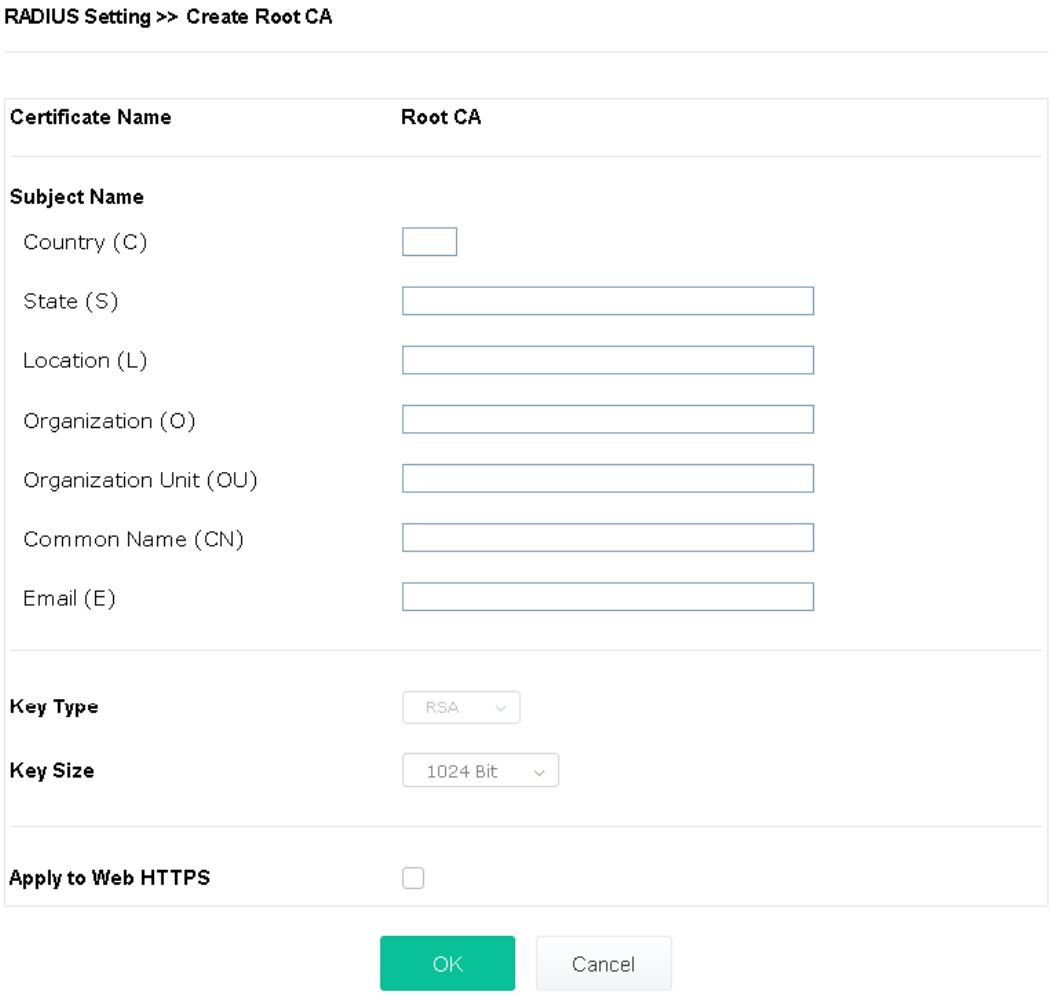
However, the procedure of applying digital certificate from a trusted root certificate authority is complicated and time-consuming. Therefore, Vigor AP offers a mechanism which allows you to

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.<br>Country (C) – Type the country code (two characters) in this box.<br>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.<br>Check this box to use the user-defined root CA certificate which will substitute for the original certificate applied by web HTTPS. |

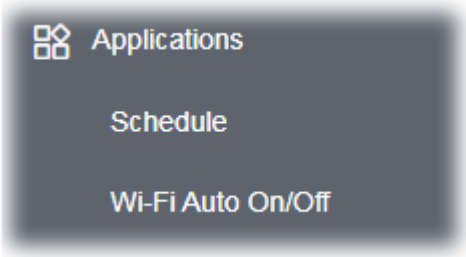
**Note:**

"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

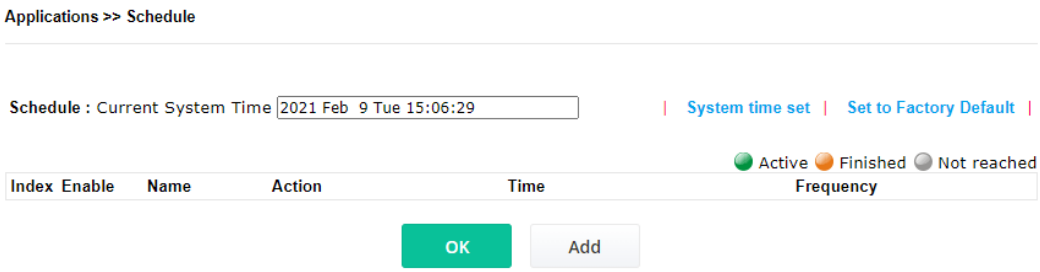
Below shows the menu items for Applications.




## 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.



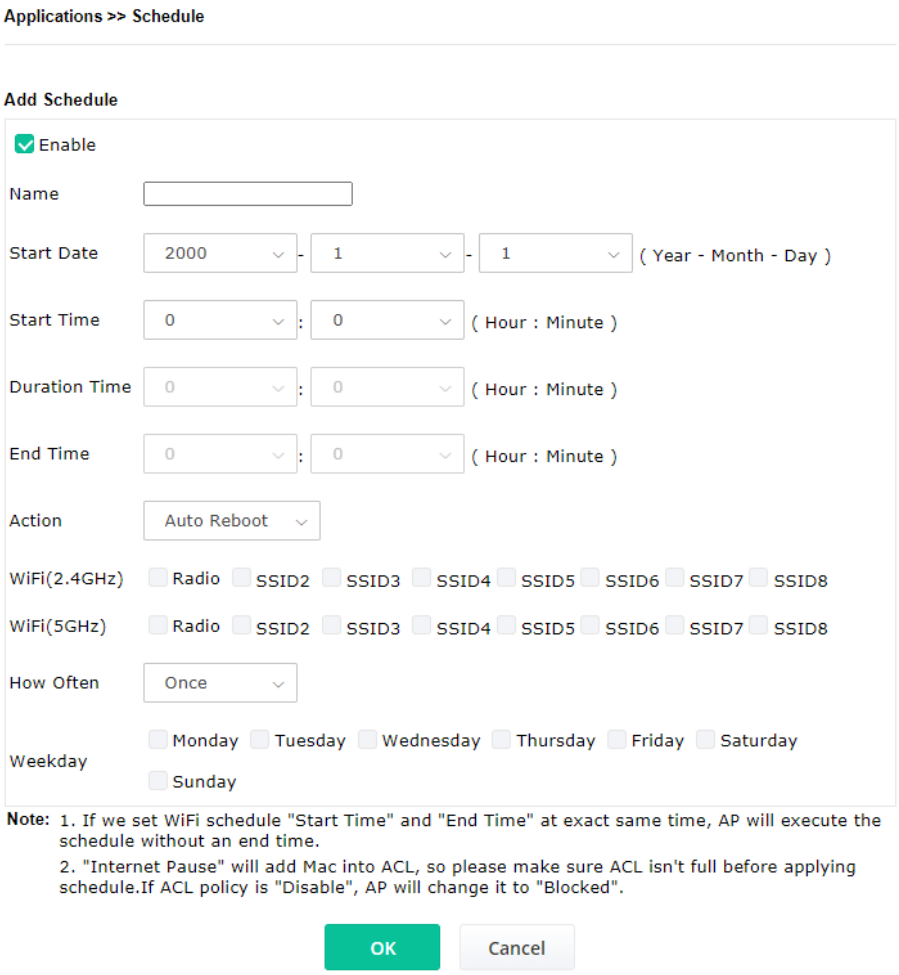

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Current System Time** | Display current system time. |
| **System time set** | Click it to open Time and Date page for configuring the time setting. |
| **Set to Factory Default** | Click it to return to the factory default setting and remove all the schedule profiles. |
| **Index** | Display the sort number of the schedule profile. |
| **Enable** | Check it to enable the function of schedule configuration. |
| **Name** | Display the name of the schedule. |
| **Action** | Display the action adopted by the schedule profile. |
| **Time** | Display the time setting of the schedule. |

| | |
|---|---|
| **Frequency** | Display the frequency of the time schedule. |

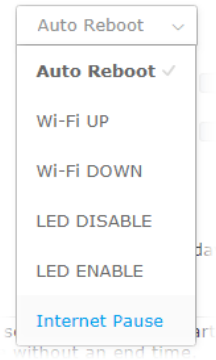
You can set up to **15** schedules. To add a schedule:

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

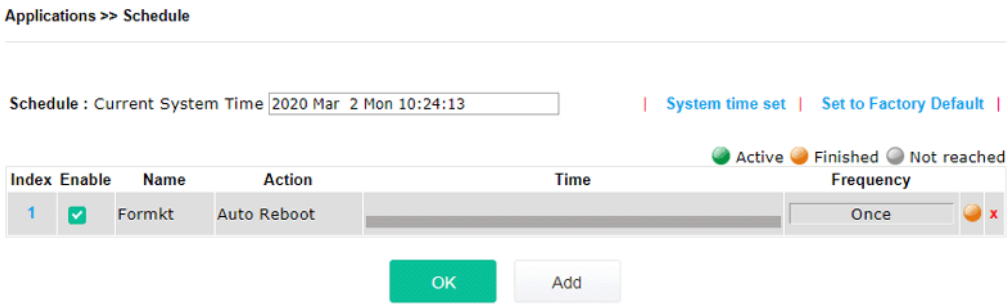



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Check to enable such schedule profile. |
| **Name** | Enter the name of the 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.<br>It is available only for the action set with WIFI UP, WIFI Down, or Internet Pause. |
| **End Time** | Display the ending time (sum of start time and duration time) of the schedule. |
| **Action** | Specify which action should apply the schedule. |

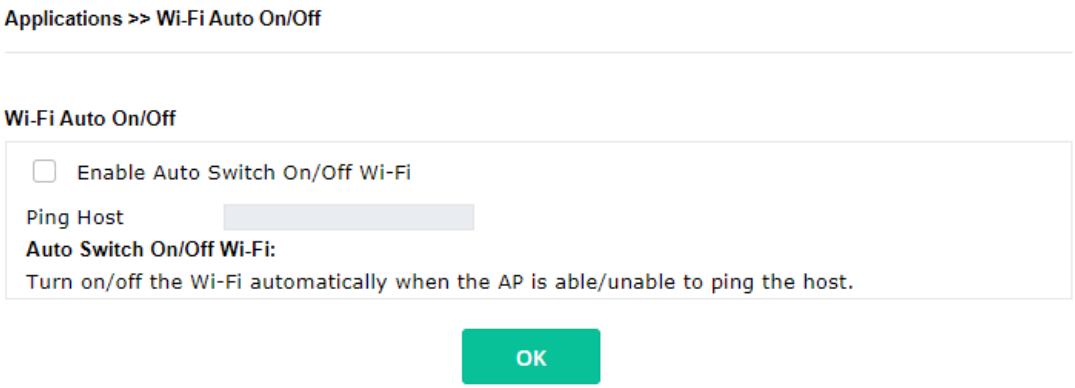
| | |
|---|---|
| |  <br>In which, you have to specify the device object/device group profile for blocking certain wireless clients when Internet Pause is selected as the Action. |
| **WiFi(2.4GHz)/ WiFi(5GHz)** | When **Wi-Fi UP** or **Wi-Fi DOWN** is selected as **Action**, you can check the Radio or SSID 2~4 boxes (2.4GHz and 5GHz respectively) to setup the network based on the schedule profile.<br>**Note**: When Radio is selected, SSID2 to SSID8 are not available for choosing, vice versa. Moreover, SSID2 to SSID8 are not available for choosing if they are not enabled. |
| **How Often** | Specify how often the schedule will be applied.<br>**Once -**The schedule will be applied just once<br>**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 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.



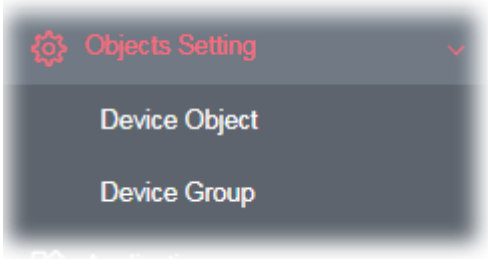

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable Connection Detection** | 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. |

Click **OK** to save the settings.

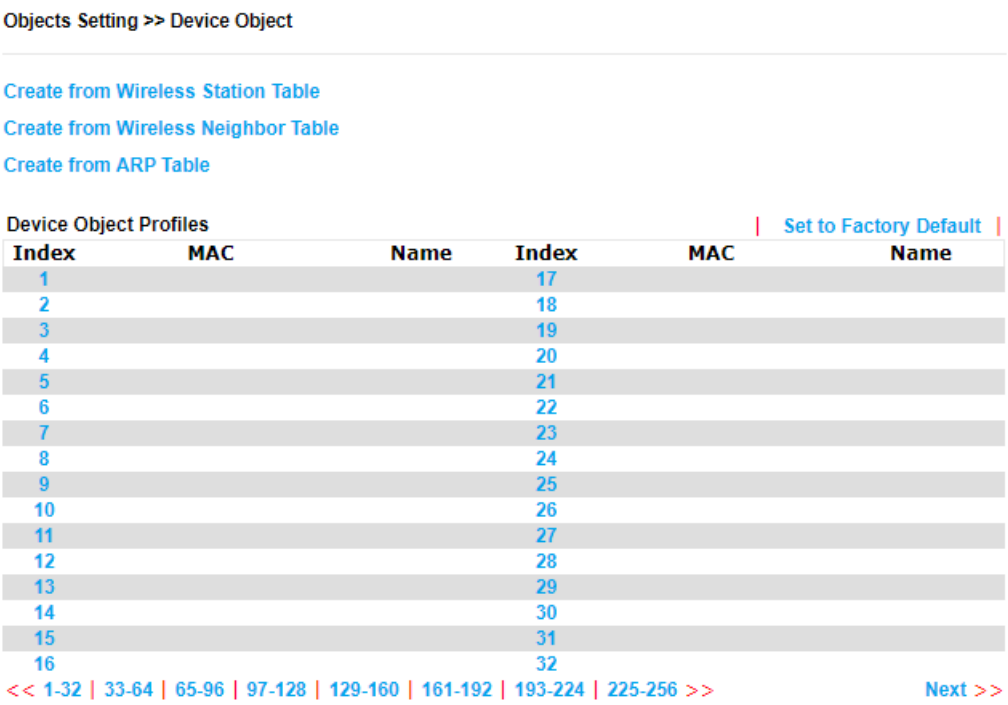
# IV-3 Objects Setting

Below shows the menu items for Objects Setting.



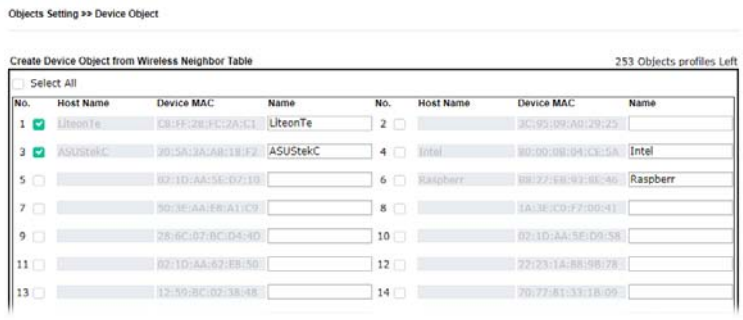
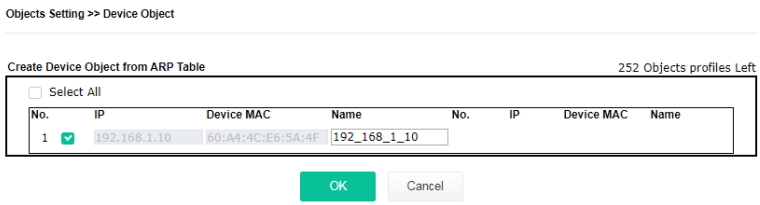

## IV-3-1 Device Object

VigorAP can specify a client as a device object to be used by other applications.

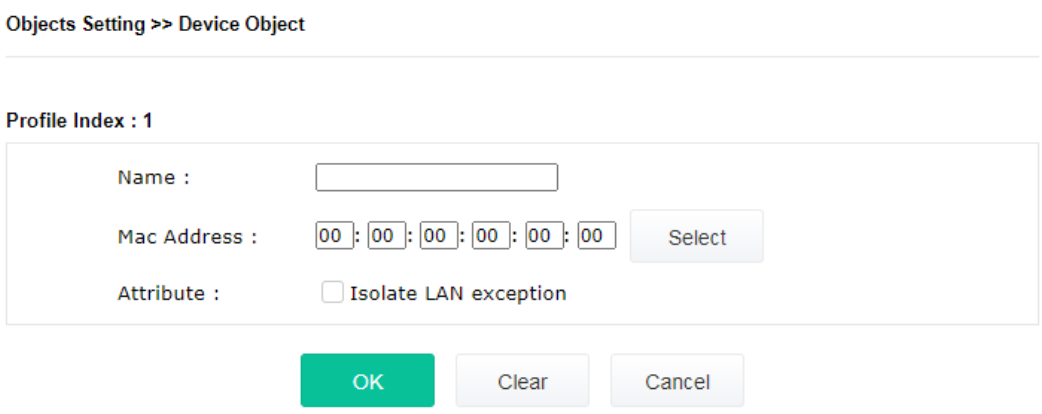



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Create from Wireless Station Table** | Click the link to open the following page.<br> <br>Choose the one(s) you want and click **OK**. The selected entries will be |

| | |
|---|---|
| | listed on the Device Object Profiles. |
| **Create from Wireless Neighbor Table** | Click the link to open the following page.<br>  <br><br>Choose the one(s) you want and click **OK**. The selected entries will be listed on the Device Object Profiles. |
| **Create from ARP Table** | Click the link to open the following page.<br>  <br><br>Choose the one(s) you want and click **OK**. The selected entries will be listed on the Device Object Profiles. |
| **Set to Factory Default** | Click it to return to the factory default setting and remove all the device object profiles. |
| **Index** | Display the index number of device object profile. |
| **MAC** | Display the MAC address specified by the device object profile. |
| **Name** | Display the name of the device object profile. |
| **Back Device Object Cfg** | **Backup** - Click to backup current configuration. |
| **Upload From File** | **Upload** - Click to upload the selected file onto Vigor device. |

In addition to choosing from the wireless station table, neighbor table or ARP table, you can click any index number link to create a new device object profile by entering the name and MAC address manually.

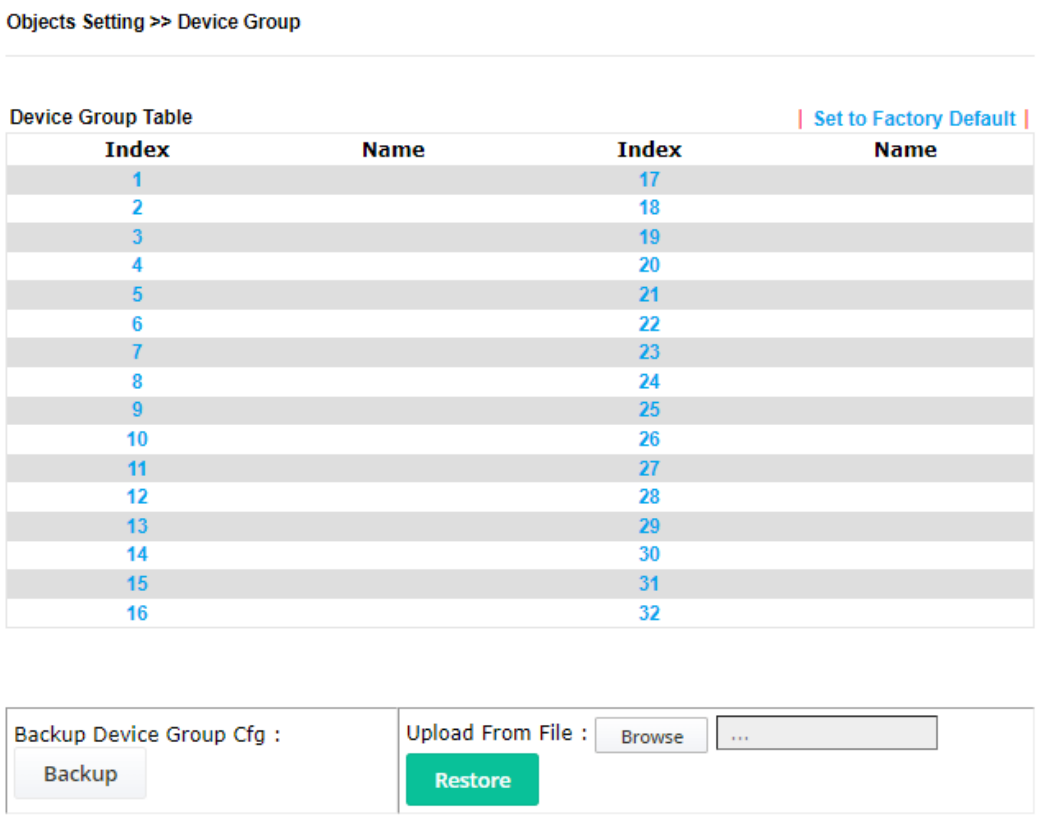



| Item | Description |
|---|---|
| **Name** | Enter the name of the profile. |

| | |
|---|---|
| **Mac Address** | Enter the MAC address of the client. |
| **Attribute** | Check the box to ignore the function of Isolate LAN. |
| **OK** | Save the settings. |
| **Clear** | Remove the settings. |
| **Cancel** | Discard the settings and return to previous page. |

## IV-3-2 Device Group

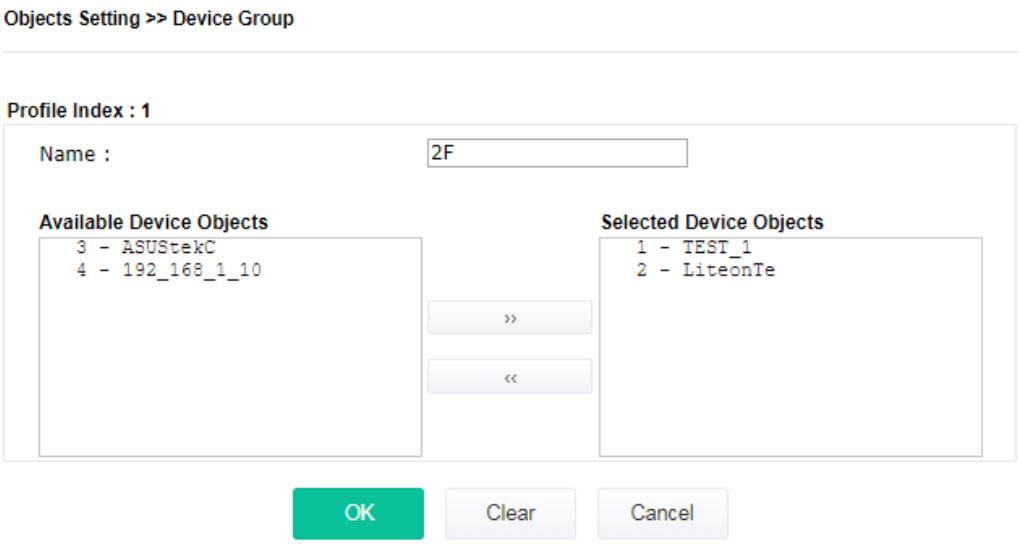
Clients can be integrated as a group and be used by other applications.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Set to Factory Default** | Click it to return to the factory default setting and remove all the device group profiles. |
| **Index** | Display the index number of the device group profile. |
| **Name** | Display the name of the device group profile. |
| **Backup Device Group Cfg** | **Backup** - Click to backup current configuration. |
| **Upload From File** | **Restore** - Click to upload the selected file onto Vigor device. |

Click any index number link to create a new device group profile.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Name** | Enter the name of the new group profile. |
| **Available Device Objects** | Display current available device objects.<br>Choose the one(s) and click the >> button to move them under the Selected IP Objects. |
| **Selected Device Objects** | Display the selected device objects.<br>Choose the one(s) and click the << button to discard the selections. |
| **OK** | Save the settings. |
| **Clear** | Remove the settings. |
| **Cancel** | Discard the settings and return to previous page. |

This page is left blank.

# Chapter V Mobile APP, DrayTek Wireless

# V-1 Introduction of DrayTek Wireless

VigorAP 1060C supports Android/iOS APP : DrayTek Wireless. The mobile user can find the APP through Apple App Store / Google Play Store.

After downloading the APP, a mobile user is able to access and login the configuration page of VigorAP.

---

**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.

---

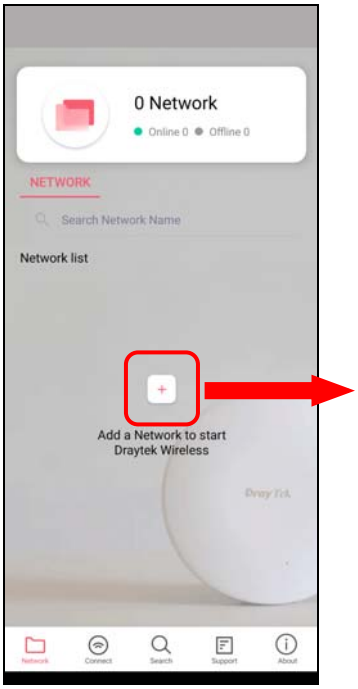
It is not necessary to connect to VigorAP physically. The mobile user must connect to one network with the same subnet as the VigorAP.

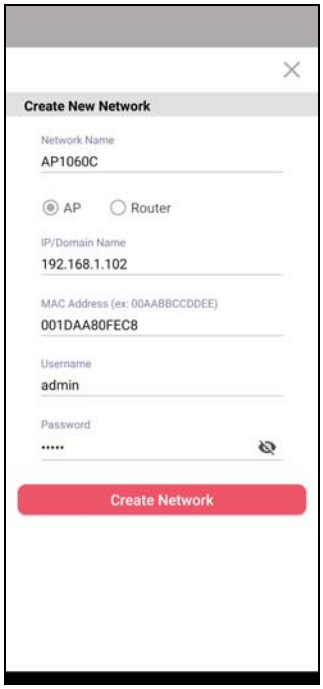
# V-2 Create a New Network

1. Run DrayTek Wireless APP.

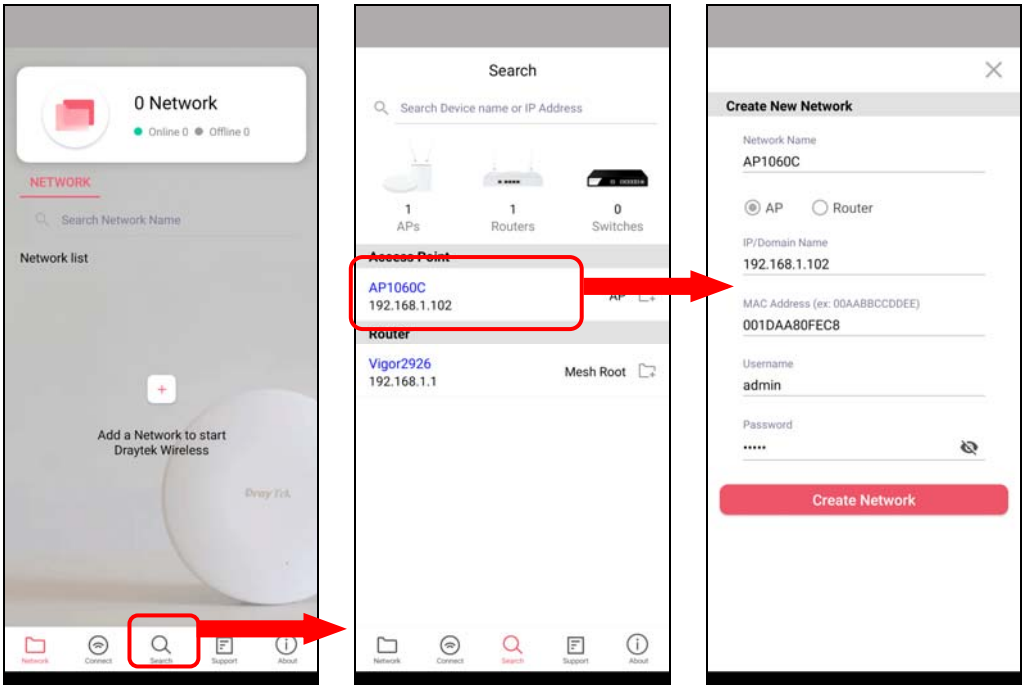
2. The system will open the NETWORK page to ask you create a new network first.
3. There are two methods for creating a new network. Click "+" or press the search button

A: Click "+" to enter the next page. Enter the required information for the device that you want to create a network.

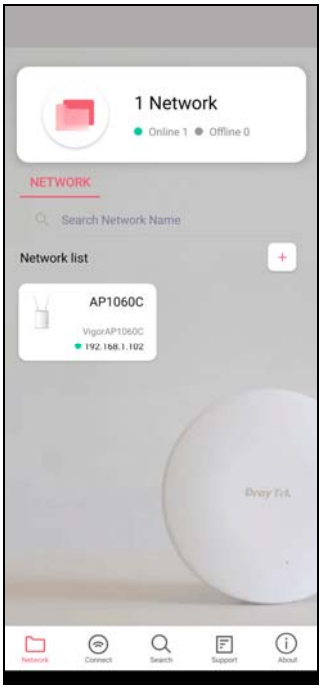


B: Press the search button. Later, the system will show the device searched. Select the one you want and click the name to get the detailed information.



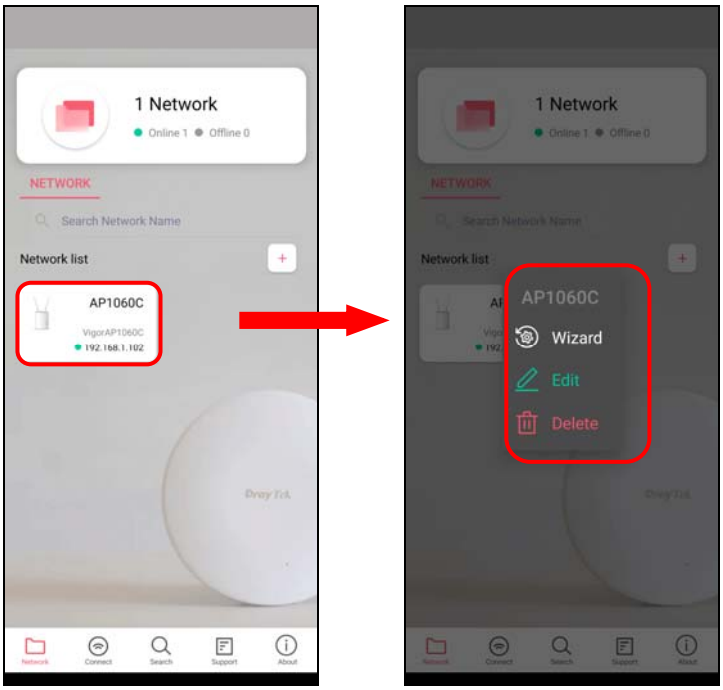

4. After clicking **Create Network**, a new network will be shown on the screen.



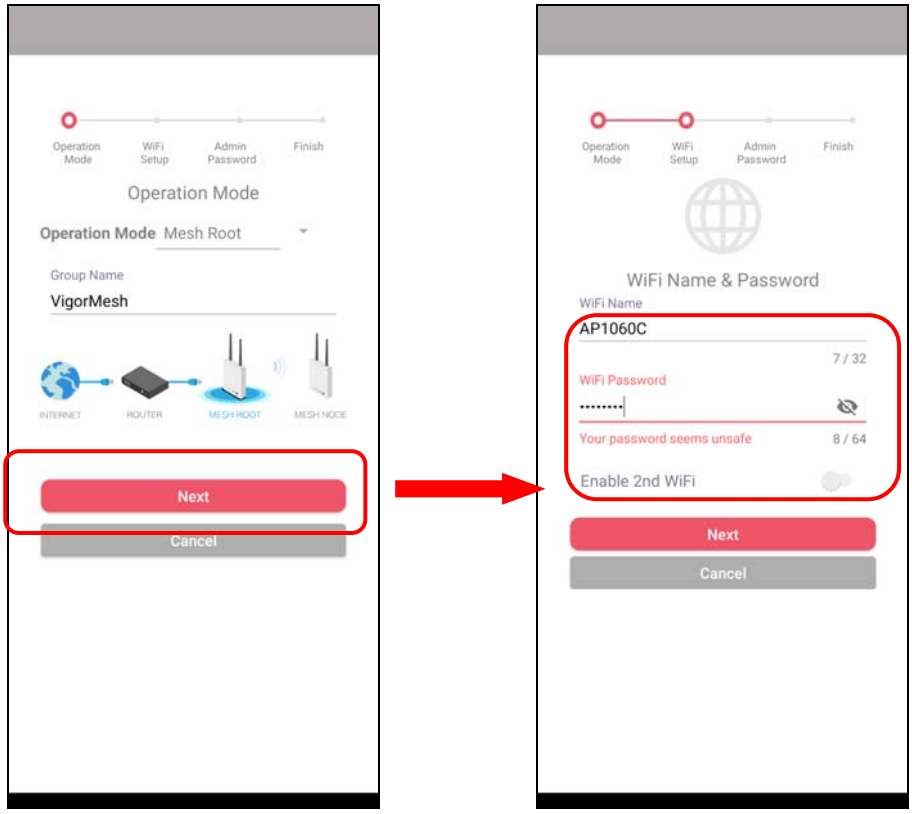
# V-3 Wizard - Mesh Root and Mesh Node

The wizard can assist to configure mesh root and mesh node(s).

1. Click and hold the network item till available actions (**Wizard, Edit** and **Delete)** shown on the screen. Select and click **Wizard**.

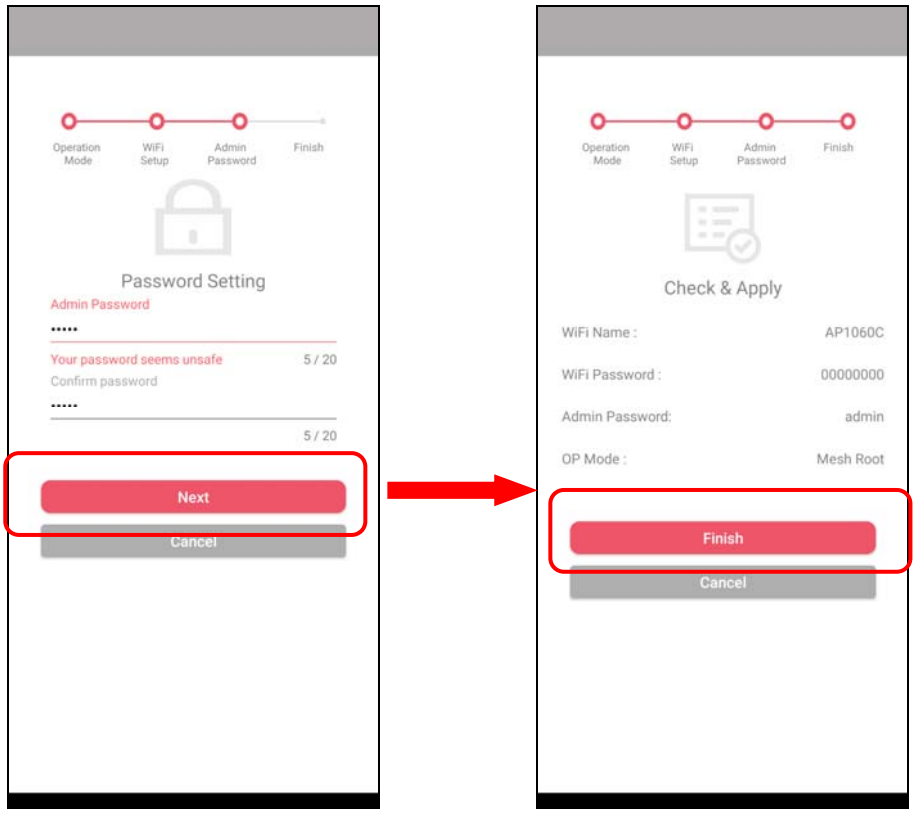


2. After clicking **Wizard**, select **Mesh Root** as the Operation Mode. The default Group Name is VigorMesh. Change the name if required. Click **Next** to enter the next page.

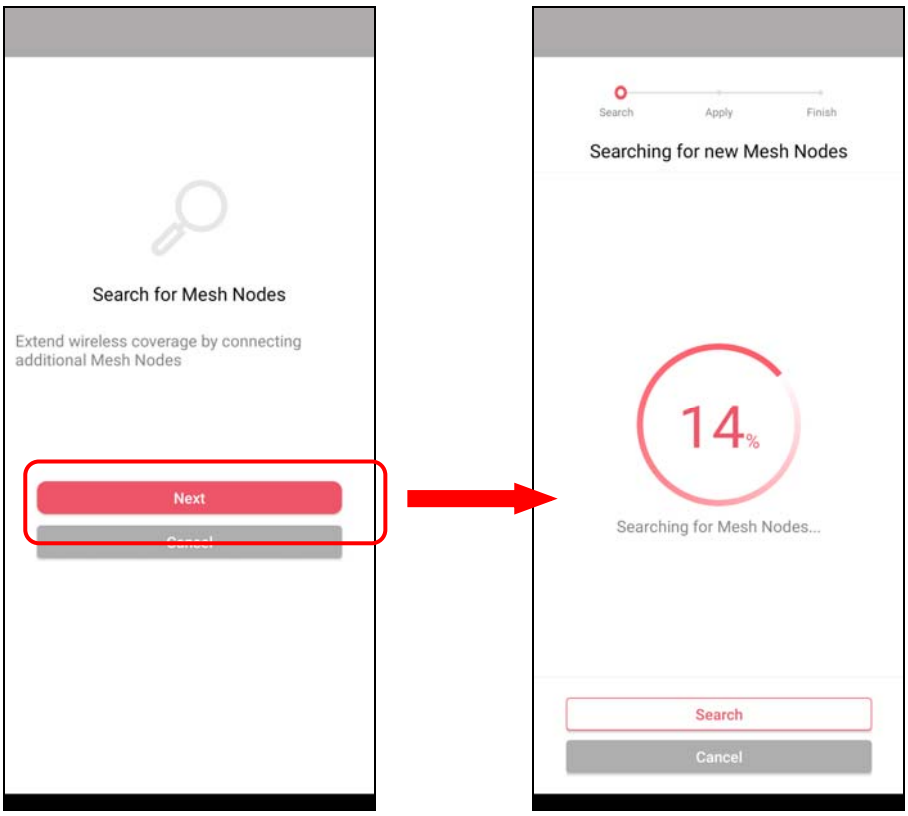



On the WiFi Name & Password page, enter the WiFi Name and the password (should be the same as the security settings set on the device's WUI). You can also enable 2nd SSID by enabling the function of 2nd WiFi. Then click the **Next** button.

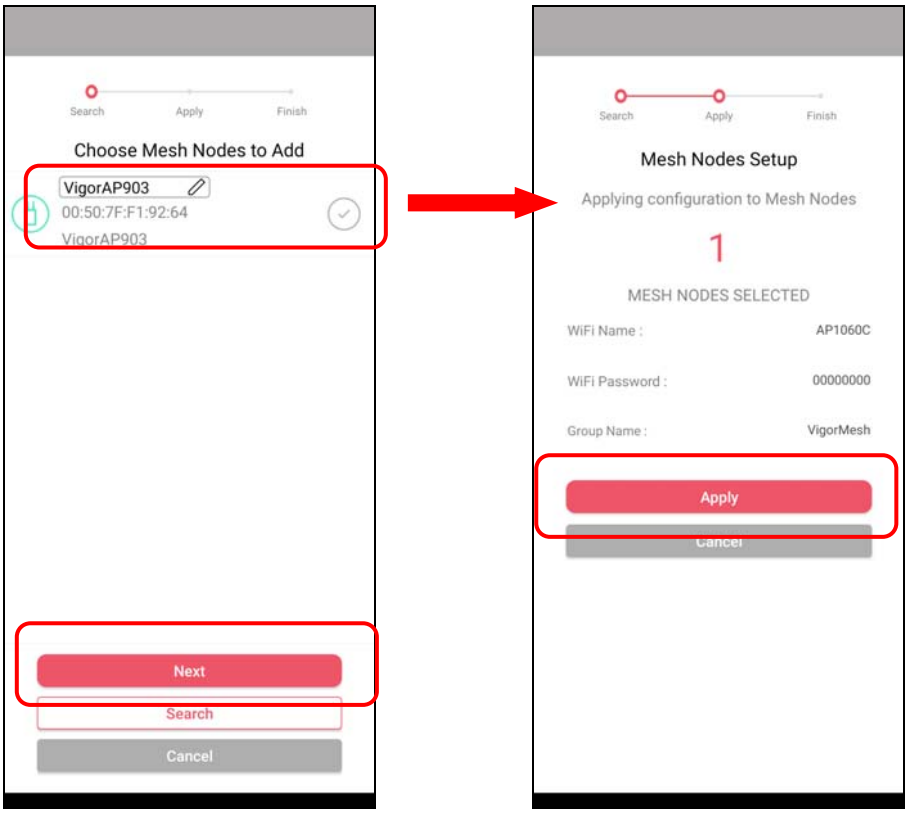
3. On the **Password Setting** page, enter the admin password and confirm the password. Then click **Next** for the APP to verify the password. If successful, the **Finish** button will appear.



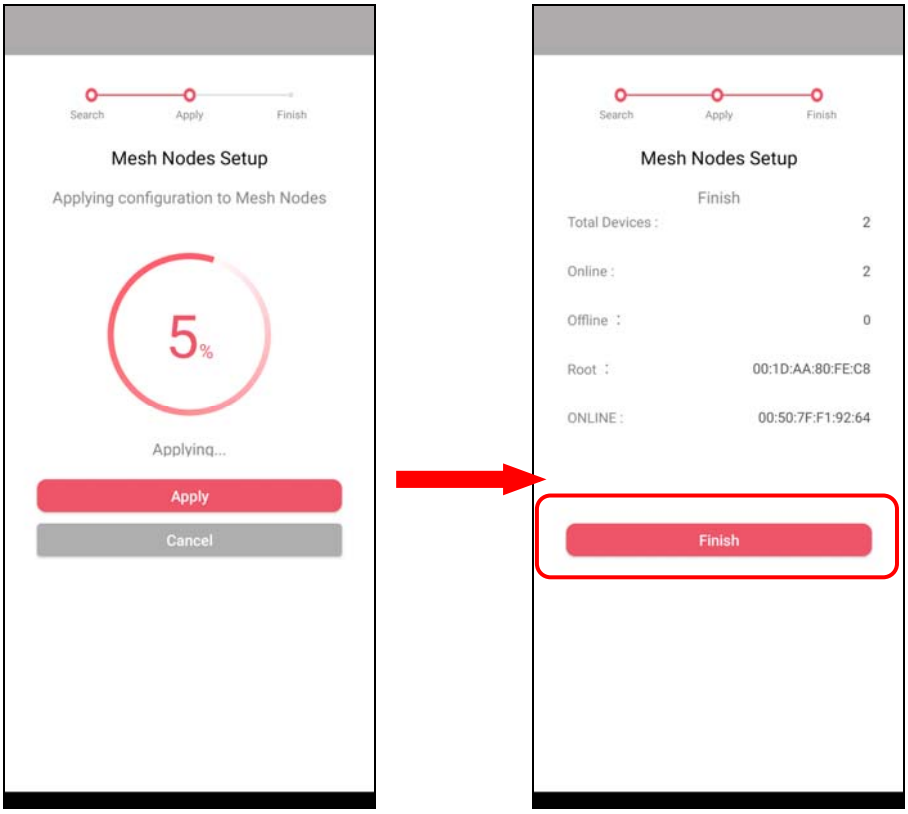
4. After sending configuration to VigorAP, it will take some time to take effect. Now, the VigorAP has been set as Mesh Root. You can search several Mesh Nodes which do not belong to any other mesh group by clicking **Next**.




5. Later, available VigorAP devices will be shown as the left figure below. Choose the Mesh Node you want to add and give a device name (e.g., VigorAP903) for it. The selected mesh node(s) will be grouped under such mesh root. Click **Next**. After checking the quantity of mesh node and mesh information and click **Apply**.



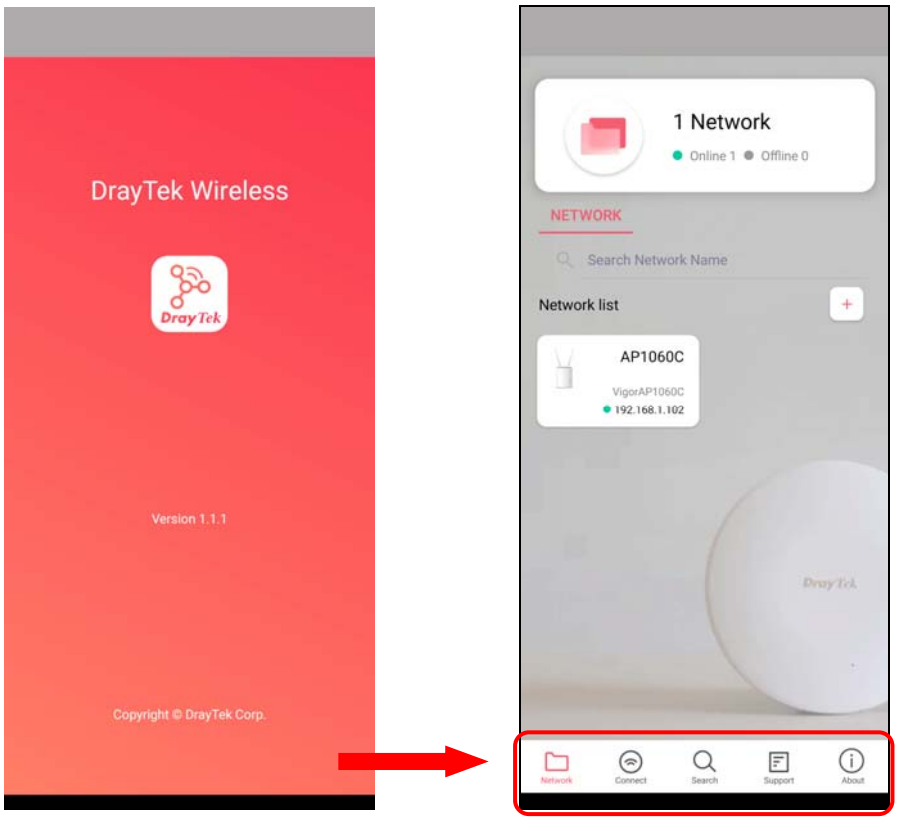
6. Wait until the mesh root applies general configuration to the mesh nodes. Later, current status of the mesh node(s) will be shown on the following page. Click **Finish**.




7. A network with mesh root and mesh node has been set up successfully.

# V-4 Login

Run DrayTek Wireless APP.

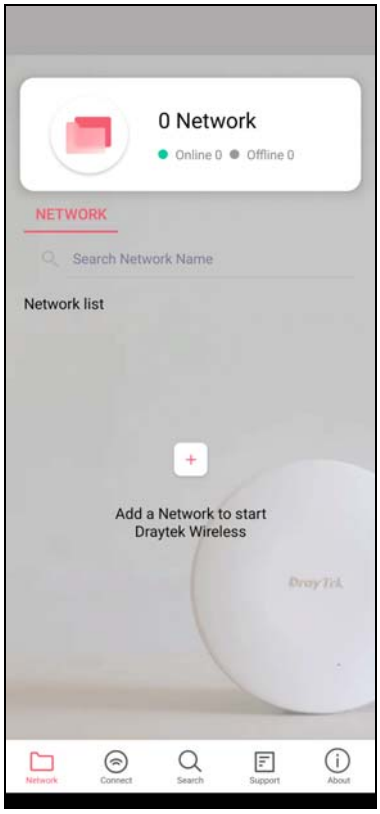



Available settings are explained as follows:

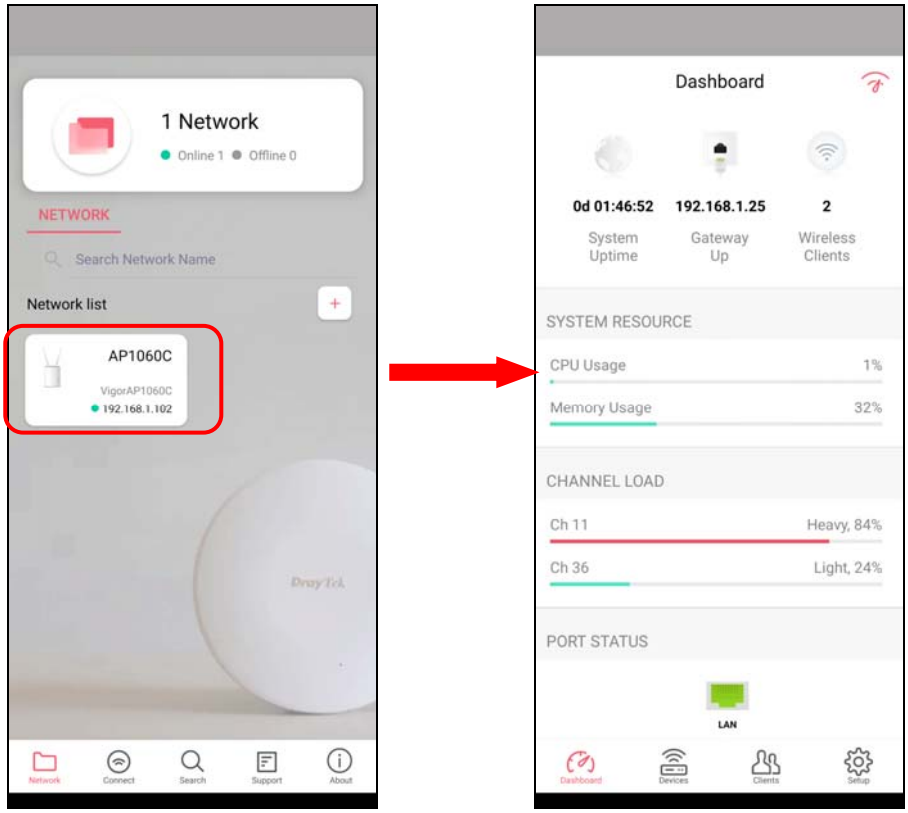
| Item | Description |
|---|---|
| **Network** | Create a new network. |
| **Connect** | Connect to a device (AP/CPE). |
| **Search** | Search available devices for connection. |
| **Support** | Display a list of models supported by this APP. |
| **About** | Display the version information of this APP. |

## V-4-1 Network

The Network page allows you to search devices (CPE/AP) for creating a network or editing an existing network (refer to V-2 for detailed information).



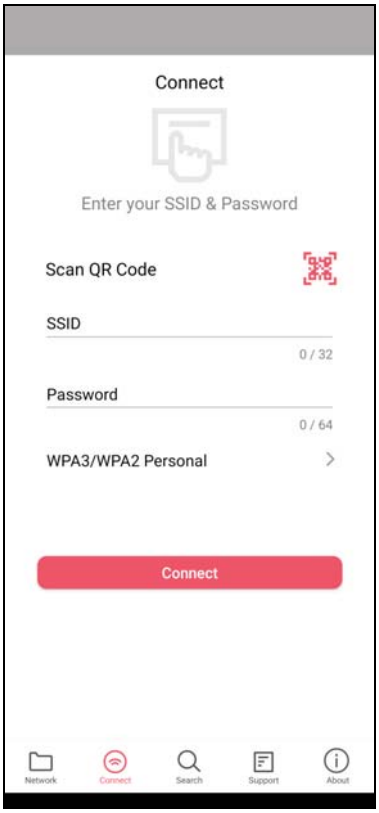

For checking the general information of certain device, click the existing item under the Network list to open the **Dashboard** of the selected device.

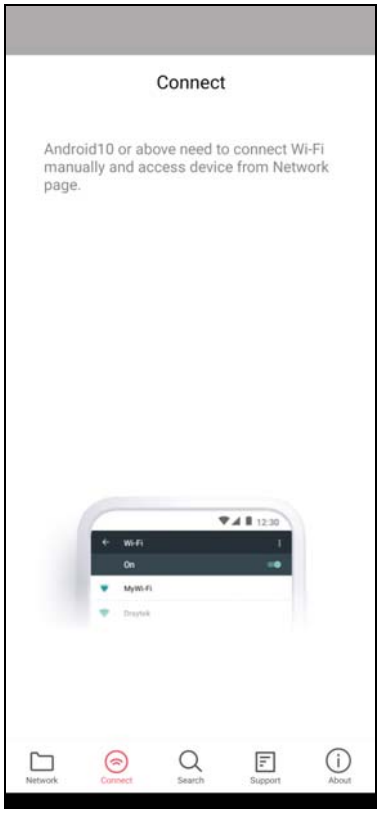


## V-4-2 Connect

For viewing the detailed information of a selected CPE/AP, click the **Connect** icon ( Connect ) to open the following left figure. Enter the SSID, password and select an encryption mode of the device.

Then click the **Connect** button ( Connect ) for accessing into the dashboard of the device.



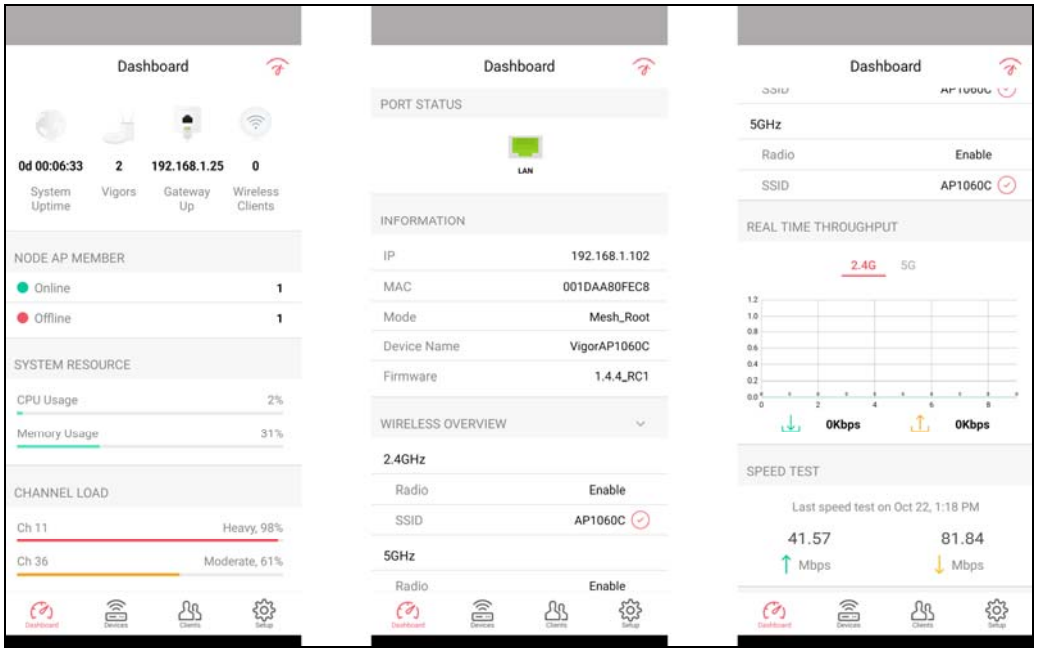




Or, click **Scan (** **)** to scan the QR code printed on VigorAP packaging box to connect the designated VigorAP.

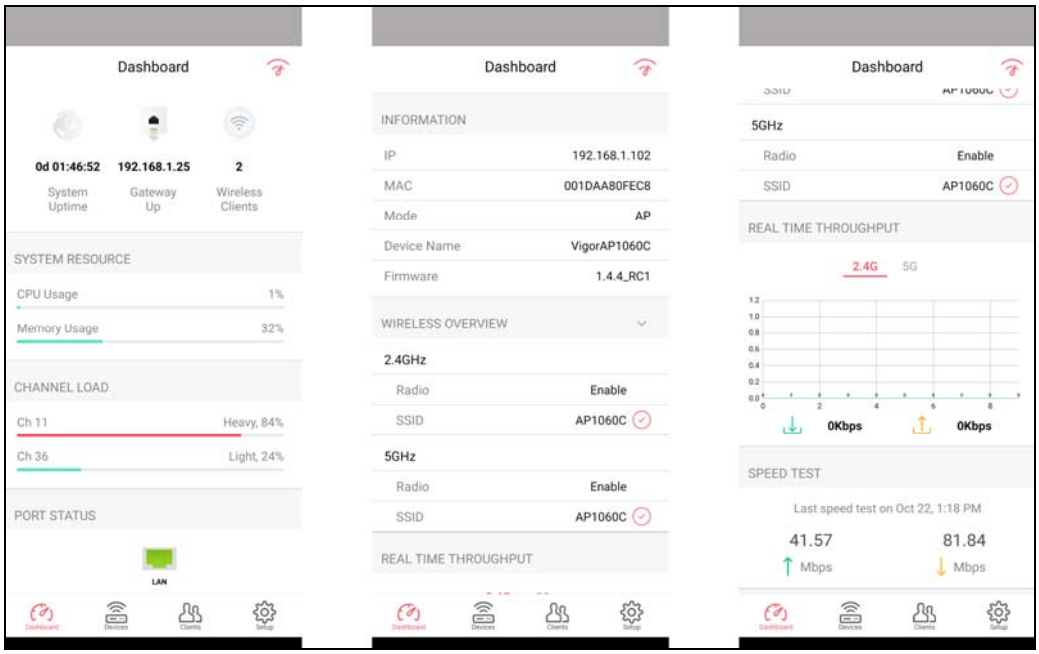
## V-4-2-1 Dashboard of the Device

Below shows the dashboard of the device. Use the scroll bar up and down for viewing other information.

Information for **Mesh Root** Mode




Information for **AP** Mode




Available settings are explained as follows:

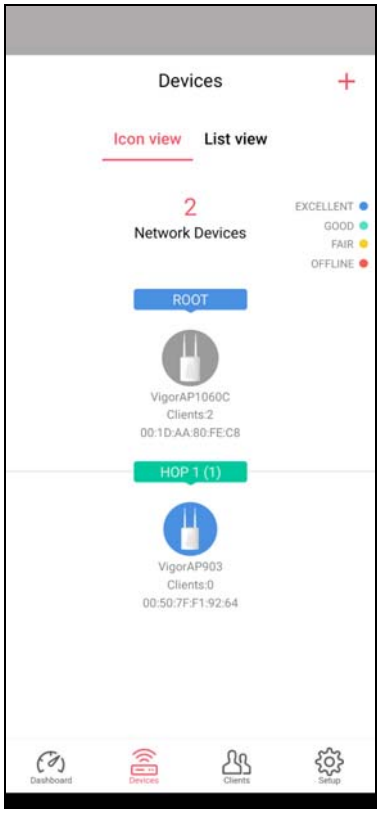
| Item | Description |
|---|---|
| **Dashboard** | The dashboard is designed with Responsive Web Design. You can click **Dashboard** to connect to the selected VigorAP WUI. |
| **Devices** | All of the devices (mesh root and mesh nodes) controlled by the mesh group will be shown on this page. One mesh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

| | |
|---|---|
| **Clients** | Displays general information for all clients / groups in Mesh Group. |
| **Setup** | Configures TR-069, Manage and WLAN settings for the connected VigorAP. |

## V-4-2-2 Devices

Below shows the icon view and list view of the device. One mesh group contains up to eight devices.

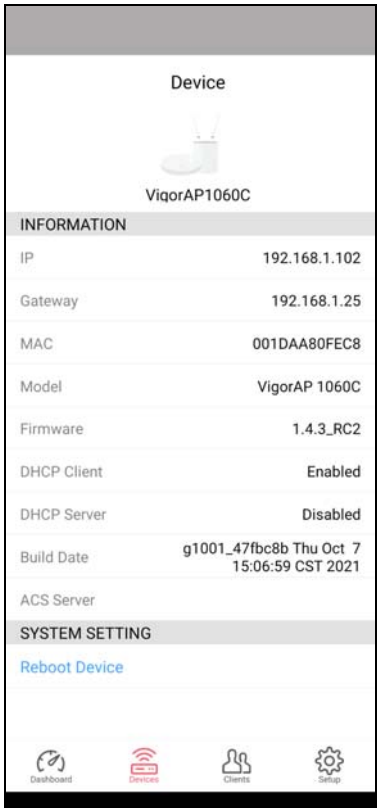
Icon view and List view for **Mesh Root** Mode



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Icon view / List view** | Switch to display the network devices in icons or a list. |
| **"+"** | To add more mesh node, click the "+" link. |

Device for **AP** Mode



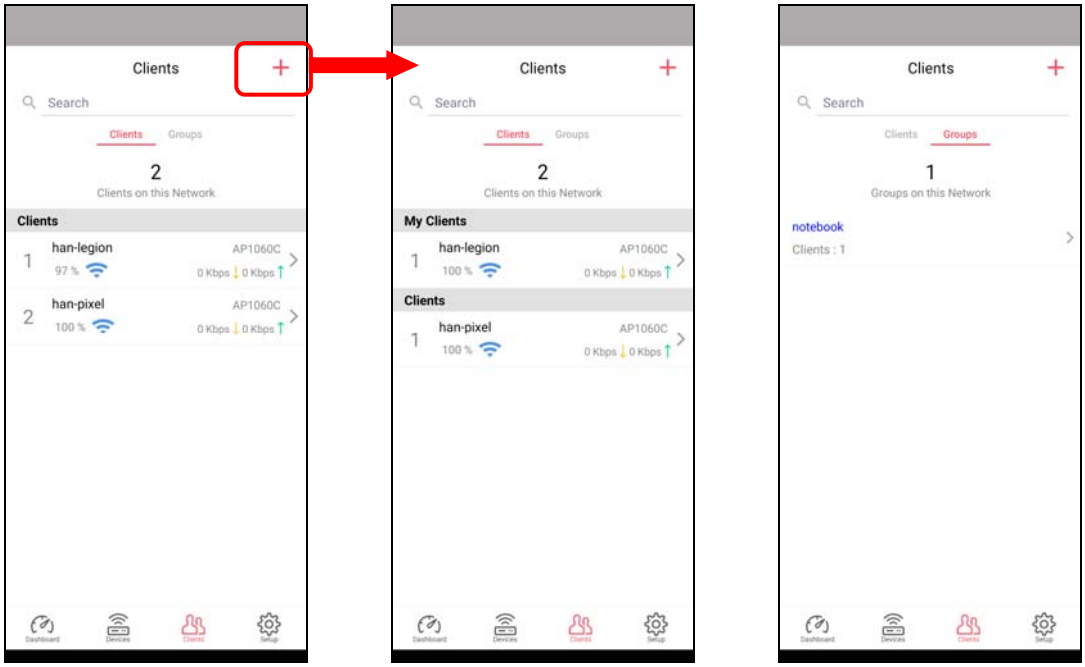

Available settings are explained as follows:

| Item | Description |
|---|---|
| **INFORMATION** | Display general information of the device (e.g., IP address, Gateway, MAC and etc.) |
| **SYSTEM SETTINGS** | **Reboot Device** - Click to reboot the device immediately. |

## V-4-2-3 Clients / Groups

This page shows relationship between devices and groups.

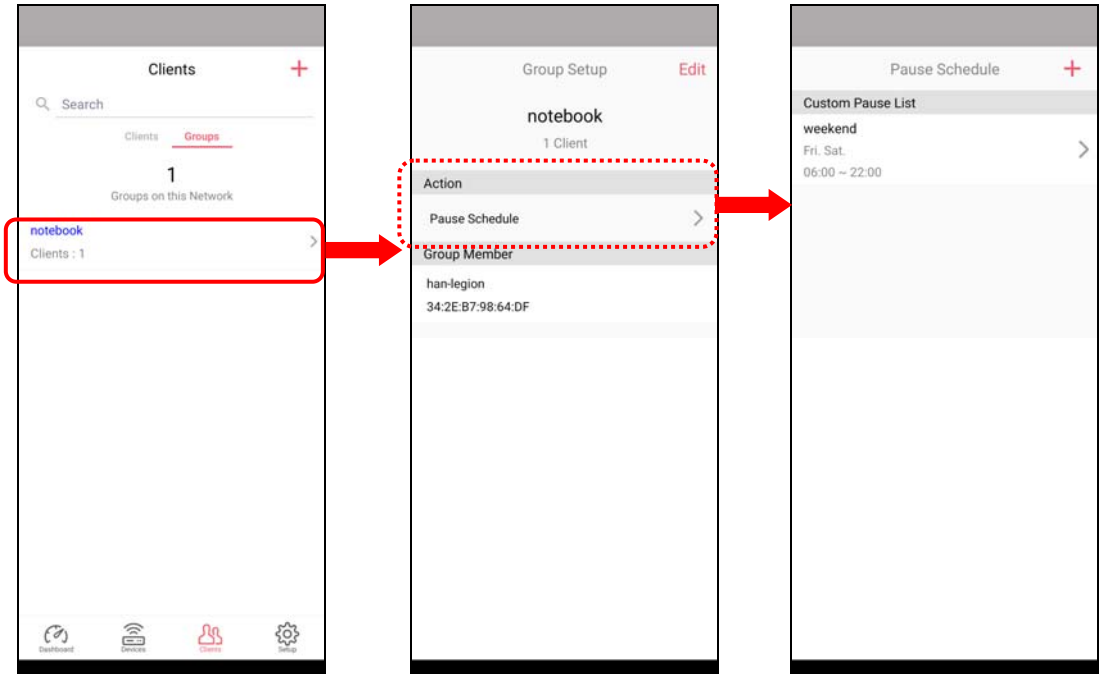
All client members can be classified (into groups). Additionally, the network connection time of the device group can be adjusted.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Search** | Search available CPE/AP around. |
| **Clients** | **+** - Click it to open the page containing My Clients for adding new clients under My Clients.<br>**My Clients** - Devices under this area can be classified under a group.<br>**Clients** - Displays devices which have not been classified under any network group. |
| **Groups** | Displays the group member and action.<br>**+** - Click it to display the items listed under My Clients. Select the one you want to add it under current group. |

Click the group to access the group setup page. If required, click **Edit** to add or remove the group member. Or click **Pause Schedule** to modify the schedule of the group.




## V-4-2-4 Setup

Setup page is used for configuring TR-069, Admin Password, Wireless LAN and Wi-Fi Blocklist settings of the Vigor device.

# Chapter VI Troubleshooting

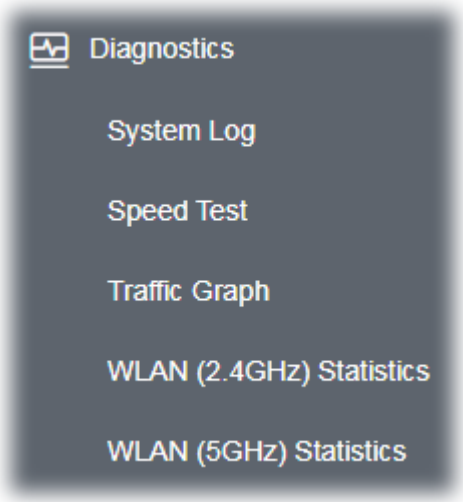
# VI-1 Diagnostics

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.

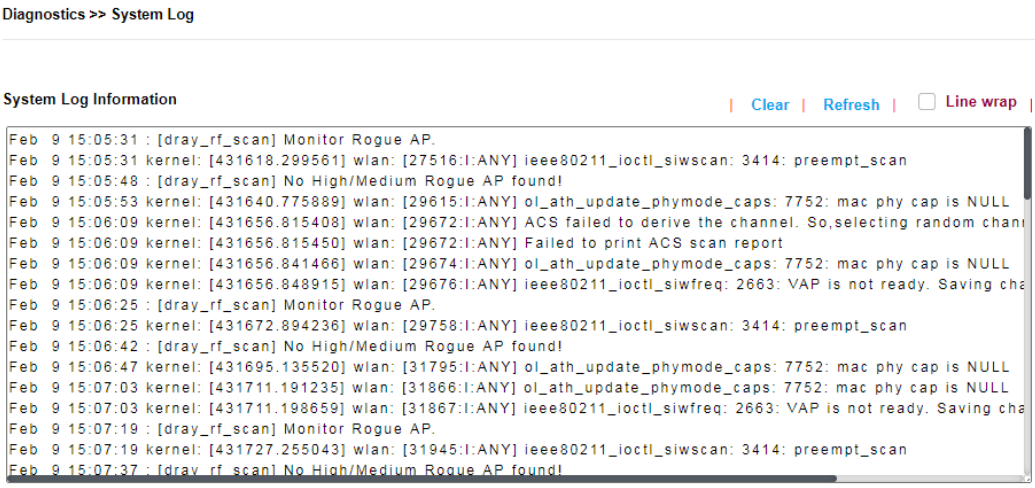
If all above stages are done and the router still cannot run normally, it is the time for you to contact your dealer or DrayTek technical support for advanced help.

Diagnostic tools provide a useful way to **view** or **diagnose** the status of your VigorAP 1060C.



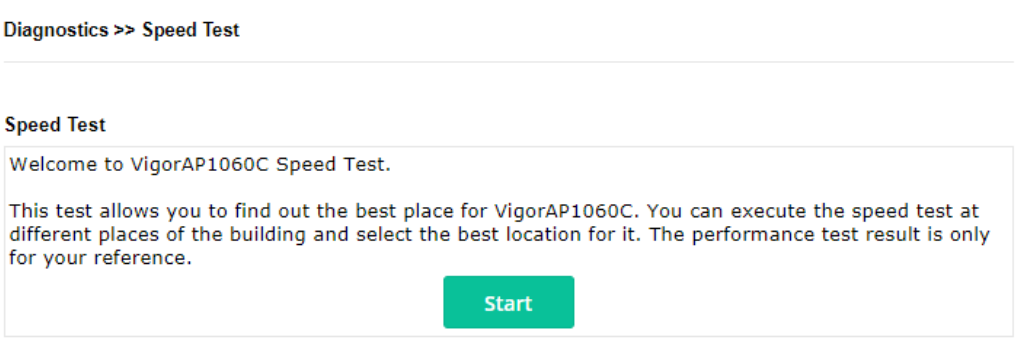
## VI-1-1 System Log

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



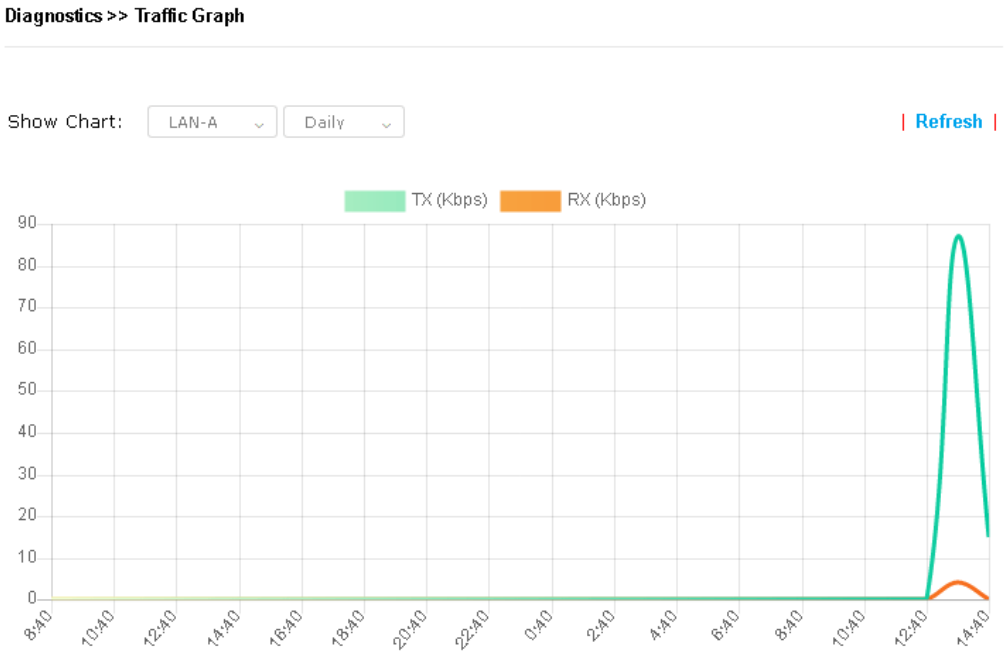

## VI-1-2 Speed Test

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 or LAN-B, 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 | 13073208 |
| Tx Multi/Broadcast Data Packets | 0 | Rx CRC errors | 0 |
| Tx failures | 0 | Rx MIC errors | 0 |
| | | Rx Decryption errors | 0 |
| | | Rx errors | 0 |

| | SSID1 (DrayTek-7CF5A4) | SSID2 (marketing) | SSID3 (N/A) | SSID4 (N/A) |
|---|---|---|---|---|
| Tx Data Packets | 0 | 0 | N/A | N/A |
| Tx Data Bytes | 0 | 0 | N/A | N/A |
| Tx Data BytesTx Data Payload Bytes | 0 | 0 | N/A | N/A |
| Rx Data Packets | 0 | 0 | N/A | N/A |
| Rx Data Bytes | 0 | 0 | N/A | N/A |
| Rx Data Payload Bytes | 0 | 0 | N/A | N/A |
| Tx Unicast Data Packets | 0 | 0 | N/A | N/A |
| Tx Multi/Broadcast Data Packets | 0 | 0 | N/A | N/A |
| Average Tx Rate (kbps) | No Station | No Station | N/A | N/A |
| Average Rx Rate (kbps) | No Station | No Station | N/A | N/A |
| Rx errors | 0 | 0 | N/A | N/A |
| Tx failures | 0 | 0 | N/A | N/A |

| | SSID5 (N/A) | SSID6 (N/A) | SSID7 (N/A) | SSID8 (N/A) |
|---|---|---|---|---|
| Tx Data Packets | N/A | N/A | N/A | N/A |
| Tx Data Bytes | N/A | N/A | N/A | N/A |

# VI-1-6 WLAN (5GHz) Statistics

Such page is used for debug by RD only.

**Diagnostics >> WLAN (5GHz) Statistics**

Auto-Refresh | Refresh

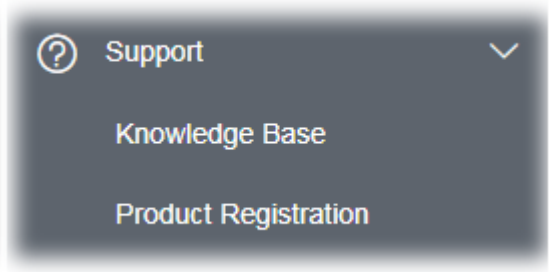
| | | | |
|---|---|---|---|
| Tx Data Packets | 0 | Rx Data Packets | 0 |
| Tx Data Bytes | 0 | Rx Data Bytes | 0 |
| Average Tx Rate (kbps) | No Station | Average Rx Rate (kbps) | No Station |
| Tx Unicast Data Packets | 0 | Rx PHY errors | 4790855 |
| Tx Multi/Broadcast Data Packets | 0 | Rx CRC errors | 0 |
| Tx failures | 0 | Rx MIC errors | 0 |
| | | Rx Decryption errors | 0 |
| | | Rx errors | 0 |

| | SSID1 (DrayTek-7CF5A4) | SSID2 (marketing) | SSID3 (N/A) | SSID4 (N/A) |
|---|---|---|---|---|
| Tx Data Packets | 0 | 0 | N/A | N/A |
| Tx Data Bytes | 0 | 0 | N/A | N/A |
| Tx Data BytesTx Data Payload Bytes | 0 | 0 | N/A | N/A |
| Rx Data Packets | 0 | 0 | N/A | N/A |
| Rx Data Bytes | 0 | 0 | N/A | N/A |
| Rx Data Payload Bytes | 0 | 0 | N/A | N/A |
| Tx Unicast Data Packets | 0 | 0 | N/A | N/A |
| Tx Multi/Broadcast Data Packets | 0 | 0 | N/A | N/A |
| Average Tx Rate (kbps) | No Station | No Station | N/A | N/A |
| Average Rx Rate (kbps) | No Station | No Station | N/A | N/A |
| Rx errors | 0 | 0 | N/A | N/A |
| Tx failures | 0 | 0 | N/A | N/A |

| | SSID5 (N/A) | SSID6 (N/A) | SSID7 (N/A) | SSID8 (N/A) |
|---|---|---|---|---|
| Tx Data Packets | N/A | N/A | N/A | N/A |
| Tx Data Bytes | N/A | N/A | N/A | N/A |
| Tx Data BytesTx Data Payload | | | | |

## 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 Hardware Installation"** for details.
2. Power on the modem. Make sure the **POWER** LED**, 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 Hardware Installation"** 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.

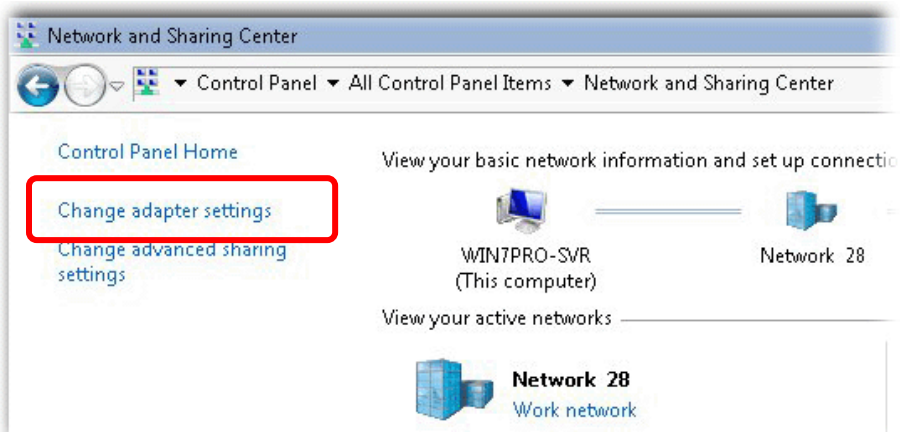
## VI-3-1 For Windows

**Note:**

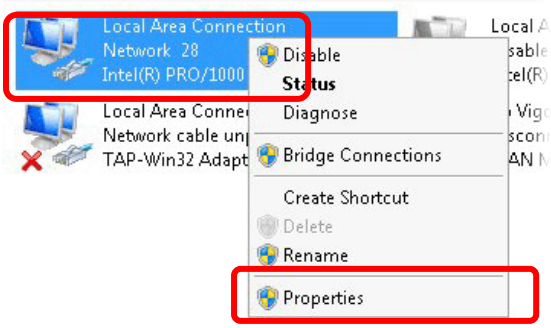
The example is based on Windows 7 (Professional Edition). As to the examples for other operation systems, please refer to the similar steps or find support notes in **www.draytek.com**.

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

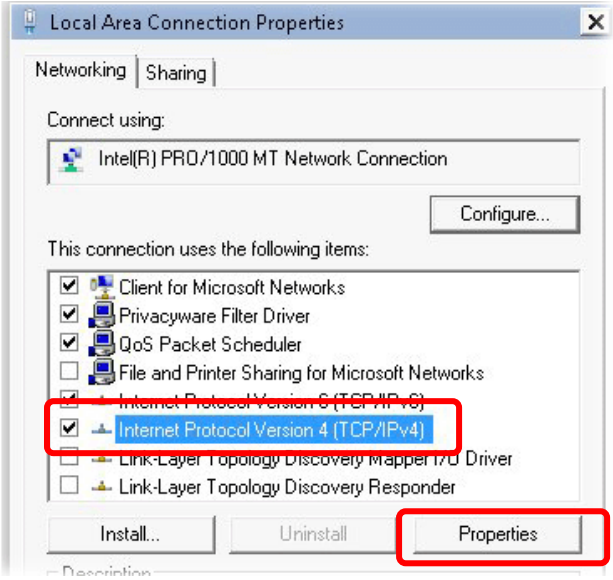
2. In the following window, click **Change adapter settings**.



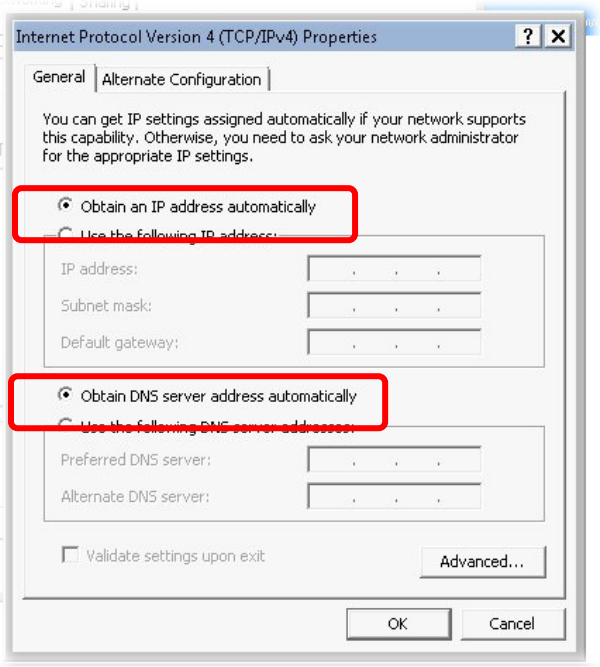
3. Icons of network connection will be shown on the window. Right-click on **Local Area Connection** and click on **Properties**.




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

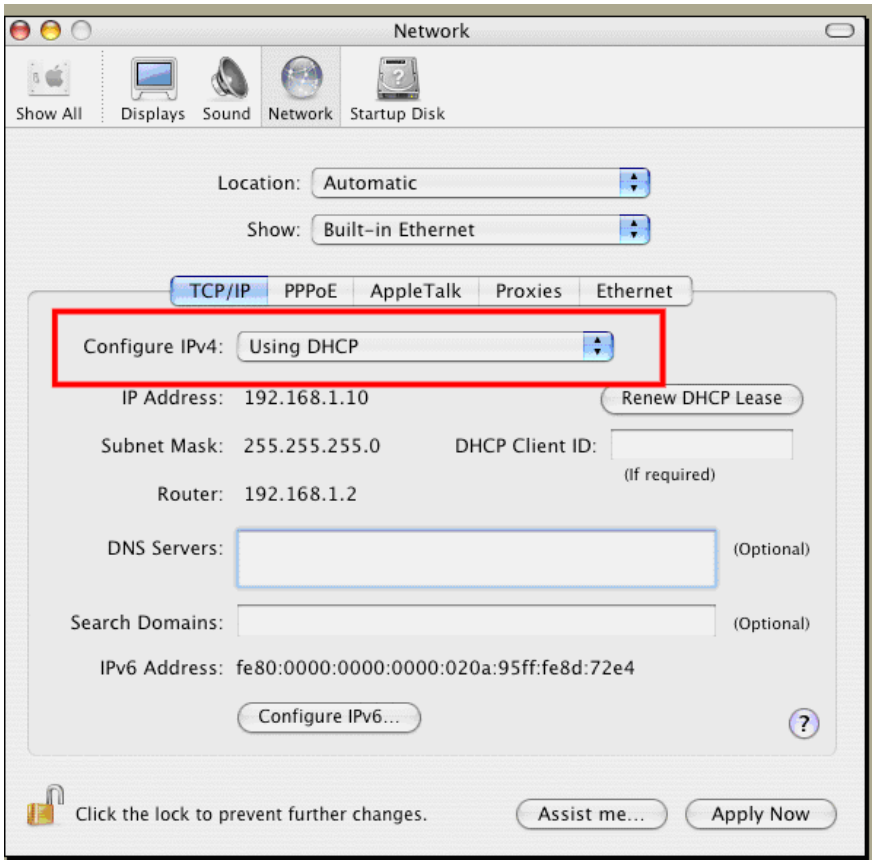



5. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Finally, click **OK**.



## 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.



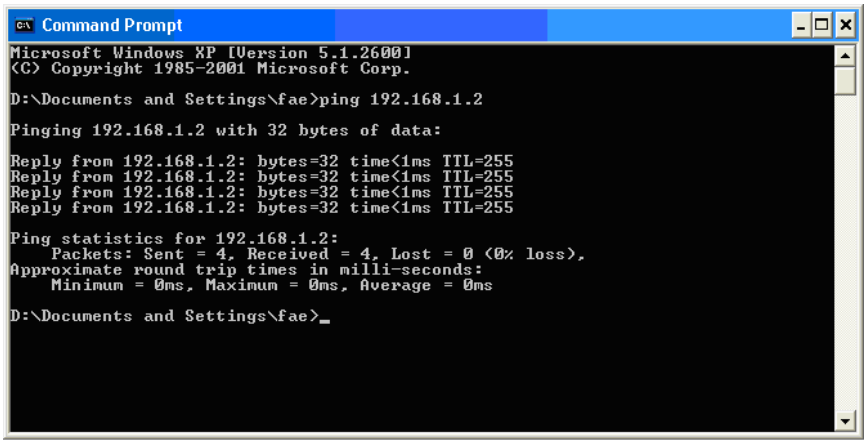
# VI-4 Pinging the Device

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

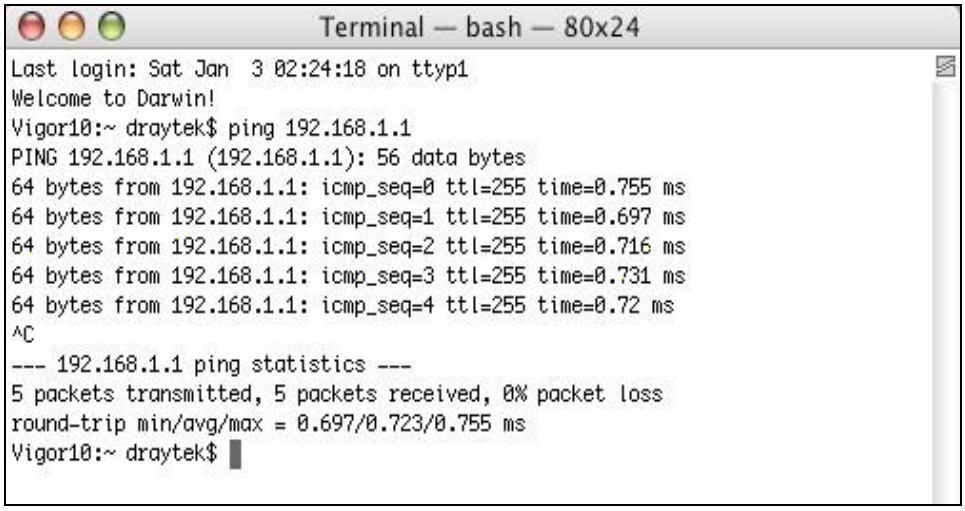
1. Open the **Command** Prompt window (from **Start menu> Run**).
2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/2000/XP/Vista/7). The DOS command dialog will appear.




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.

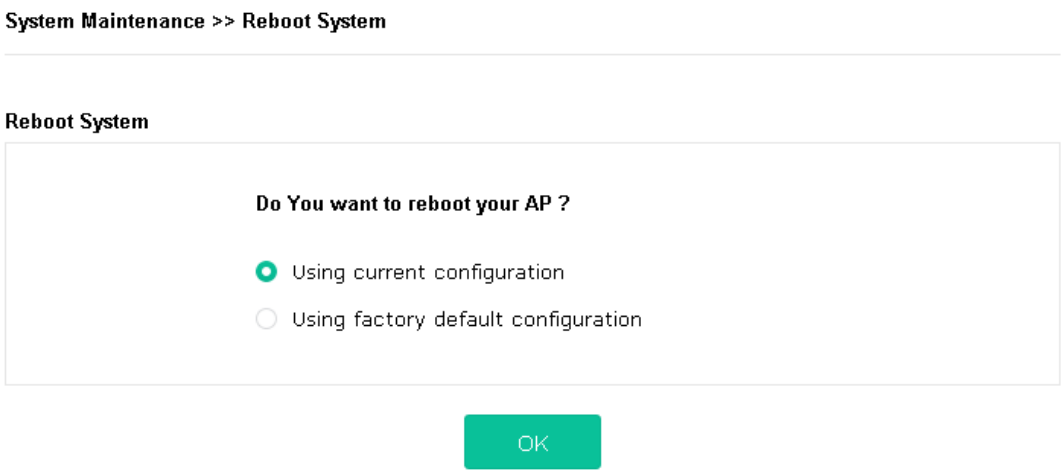
**Warning:**

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

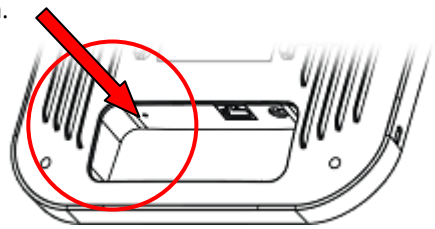
You can reset the modem to factory default via Web page.

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, 39

## A

Access Control, 44
Action, 139
Advanced Setting, 47
AES, 28
Airtime Fairness, 50
AP Discovery, 49
AP Management, 118
AP Mode, 37, 67, 82
AP Operation Mode, 17
APM Log, 119
Applications, 138, 142
Auth Mode, 46
Authentication Client, 135
Authentication Type, 135
Auto Channel Filtered Out List, 48
Auto Logout, 13
Auto Provision, 118

## B

Band Steering, 56
Bandwidth Limit, 18, 21, 27
Black List, 120

## C

Central AP Management, 118
Certificate Management, 135
Changing Password, 14
Channel, 39, 83
Channel Width, 47
Client IP, 135
Client PinCode, 46
Client's MAC Address, 120
Configuration Backup, 107, 108
Connect to a Vigor Router, 7
Connection Time, 53
Connection Type, 84
Country Code, 48

## D

Default Gateway, 85
Detection, 123, 129, 130
DHCP Client, 94
DHCP server, 11

## E

EAP Type, 135
Encryp Type, 46
End Time, 139
Extension Channel, 39

## F

Factory Default Setting, 176
Fast Roaming, 55
Firmware Upgrade, 117
Force Overload Disassociation, 120
Fragment Length, 48

## G

General Setup, LAN, 86, 89, 91, 92, 93

## H

Hardware Reset, 176
Hide SSID, 40
HTTP port, 114
HTTPS, 137
HTTPS port, 114

## I

IP Address, 84, 94
Isolate Member, 40

## K

Keep Alive Period, 105
Key Renewal Interval, 42
Key Size, 137
Key Type, 137

## L

LAN, 93
LAN port, 100
Lease Time, 94
LED Indicators and Connectors, 2
Limit Client, 38
Limit Client per SSID, 39
Load Balance, 120

## M

MAC Address, 83
MAC Address Filter, 45
MAC Clone, 48
Main SSID, 17, 20, 26
Management, 114
Management VLAN, 94
Mobile Device Management, 123
Mode, 39, 41

## N

NTP, 138
NTP Client, 111
NTP synchronization, 112

## O

Once, 140
Open/Shared, 28, 84
Operation Mode, 32
Overload Management, 120

## P

Pass Phrase, 42, 84
Password, 14
Password Strength, 106
Periodic Inform Settings, 105
PIN Code, 35
PMK Cache Period, 55
Policy, 44, 131, 132
Port, 43
Port Control, 96, 100
Pre-Authentication, 55
Primary DNS Server, 94
PSK, 34
Push Button, 46

## Q

Quick Start Wizard, 16

## R

RADIUS Server, 43, 134
RADIUS Setting, 134
Reboot System, 116
Reconnection Time, 53
Relay Agent, 94
Restore, 45
Roaming, 54
Router Name, 84
Routine, 140
RSSI, 54
RTS Threshold, 48

## S

Schedule, 138, 142, 144
Secondary DNS Server, 94
Secret Key, 135
Security, 41
Security Mode, 83
Security Overview, 34
Security Settings, 41
Session Timeout, 43
Shared Secret, 43
Show Chart, 129
Software Reset, 176
Speed Test, 165
SSL(HTTPS), 105
Start Date, 139
Start PBC, 35
Start Time, 139
Station Control, 18, 21, 27, 52
Station List, 61
Status of Settings, 121
STUN, 105
Subject Name, 136
Subnet, 40
Subnet Mask, 84, 94
Support Area, 169

Syslog/Mail Alert, 110
System Log, 165
System Maintenance, 102
System Status, 103

## T

Temperature Sensor, 141
Time and Date, 111
TKIP, 28, 34
TR-069, 104
Traffic Graph, 166
traffic overload, 120
Tx Power, 47

## U

Users Profile, 135

## V

VLAN ID, 40, 94

## W

WEP, 28
WEP (Wired Equivalent Privacy), 34
White List, 120
Wi-Fi DOWN, 140
Wi-Fi UP, 140
Wired Connection, 7
WLAN (2.4GHz) Statistics, 166
WLAN (5GHz) Statistics, 168
WPA (Wi-Fi Protected Access), 34
WPA Algorithms, 42
WPS, 46
WPS (Wi-Fi Protected Setup), 34