VigorAP 805

802.11ax Access Point

User's Guide

Version: 1.2

Firmware Version: V5.1.0

Date: 4 February 2026

Intellectual Property Rights (IPR) Information

Copyrights

Trademarks

The following trademarks are used in this document:

- Microsoft is a registered trademark of Microsoft Corp.
- Windows, Windows 10, 11 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 device.
- The device is a complicated electronic unit that may be repaired only be authorized and qualified personnel. Do not try to open or repair the device yourself.
- Do not place the device in a damp or humid place, e.g. a bathroom.
- The device should be used in a sheltered area, within a temperature range of 0 to +40 Celsius.
- Do not expose the device 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.
- Do not power off the device when saving configurations or firmware upgrades. It may damage the data in a flash. Please disconnect the Internet connection on the device before powering it off when a TR-069/ ACS server manages the device.
- Keep the package out of reach of children.
- When you want to dispose of the device, please follow local regulations on conservation of the environment.

Warranty

We warrant to the original end user (purchaser) that the device 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 devices 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

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 805, the concurrent dual-band wireless (2.4G/5G) access point offering high-speed data transmission. With this high cost-efficient VigorAP 805, computers and wireless devices which are compatible with 802.11n/802.11a can connect to the existing wired Ethernet network via this VigorAP 805, at the speed of 300Mbps.

Easy install procedures allow any computer users to set up a network environment in a 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!

AP Management

The VigorAP 805 can operate in standalone mode for your office network or a classroom or a waiting room of some transportation terminals (e.g. ferry terminal, bus station, train station) or a clinic's waiting room; connected to your LAN and offering you with wireless access. If your network requires several VigorAP 805 units, centrally manage and monitor them individually as a group will be expected. DrayTek central wireless management (AP Management) lets control, efficiency, monitoring, and security of your company-wide wireless access easier be managed. Inside the web user interface, we name the "central wireless management" as Central AP Management which supports mobility, client monitoring/reporting, and load-balancing to multiple APs. For central wireless management, you will need a Vigor2865 or Vigor2927 series router; there is no per-node licensing or subscription required. For multiple wireless clients to apply the AP Load Balancing to the multiple APs, AP management will manage wireless traffic with smooth flow and enhanced efficiency.

Support Mesh Network

The message, information, and data can be transferred via wireless connection among VigorAP 805 devices without using Ethernet cables. It can reduce the construction cost and eliminate the trouble of wiring. Therefore, mesh AP is suitable for outdoor activities, or meetings.

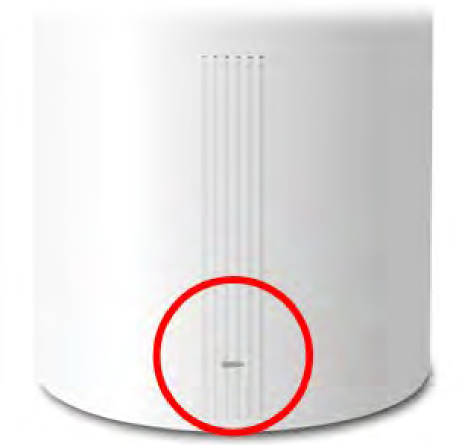
In short, VigorAP with mesh function has the following benefits:

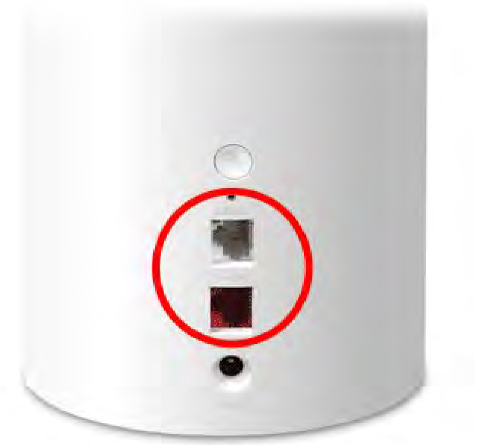
- In the traditional wireless network, users must choose the best signal source manually from various SSIDs. The mesh AP can find out the best route automatically.
  Besides, if any one of the mesh AP devices disconnects due to an unknown reason, the mesh system will determine another accessible AP and transfer the packets to that AP.
- Maintain a certain degree of normal operation for it is not easily affected by connection interference or terrain blocking of walls or floors.

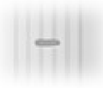
- For the mesh network system to adopt the mesh topology, each node in the network not only has a single connection but also interweaves to other nodes like a net. Because of such characteristics, the mesh network can set up stronger network architecture.
- Each node (mesh AP) in the mesh network can be operated as an independent wireless AP; therefore, the whole mesh network can offer a more stable and faster wireless connection.
- The mesh network is suitable for large spaces and large numbers of people for the configuration for each AP is easy and simple.

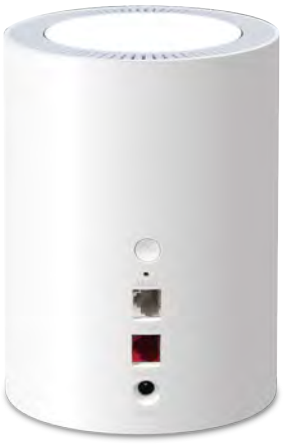
I-1-1 LED Indicators and Connectors

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





LED	Status	Explanation
	On (Red)	The system is in Loader mode.
	Blinking Slowly (Red)	The system is in TFTP mode.
	Blinking (Red), just like an SOS signal	The system failed due to some reason.
	Blinking Slowly(white)	The system is ready and can work normally.
	Blinking Quickly(white)	The system is booting up or reset to the factory default.
	Off	The system is not ready or is failed.
LED on Connector		
LAN 2.5G Port	On (Green)	LAN is connected.
	Blinking (Green)	Data is transmitting (sending/receiving).
	Off	LAN is disconnected.
LAN 1G Port	On (Green)	LAN is connected.
	Blinking (Green)	Data is transmitting (sending/receiving).
	Off	LAN is disconnected.



Interface	Description
🔗	Mesh button. Press it and release within 2 seconds. The LED will turn to blink in red, and the access point will start to connect to the Mesh network.
Reset	Restore the default settings. Usage: Turn on the router. Press the button and keep for more than 10 seconds. Then the router will restart with the factory default configuration.
LAN 1/2	Connecter for xDSL / Cable modem (Giga level) or router.
	Connecter for a power adapter.

I-2 Hardware Installation

This section will guide you through installing the VigorAP.

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

ⓘ Note:

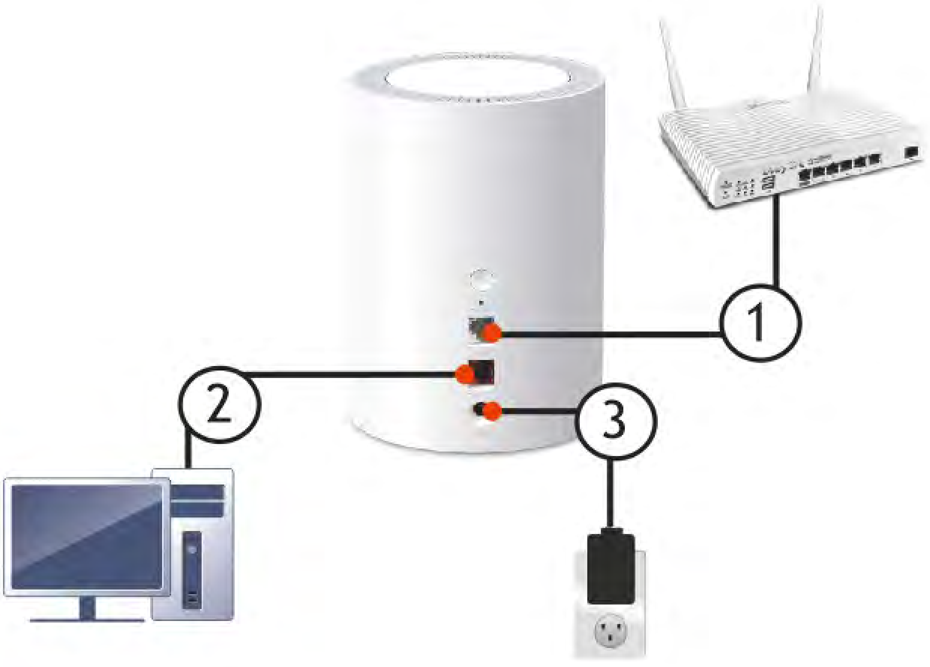
For the sake of personal safety, only trained and qualified personnel should install this access point.

1. Connect VigorAP 805 to xDSL modem, router, or switch/hub in your network through the LAN 1 or LAN2 port of the access point by Ethernet cable.

   You can also connect VigorAP 805 to a Vigor router via wireless connection. For detailed information, refer to VigorAP 805 User's Guide.

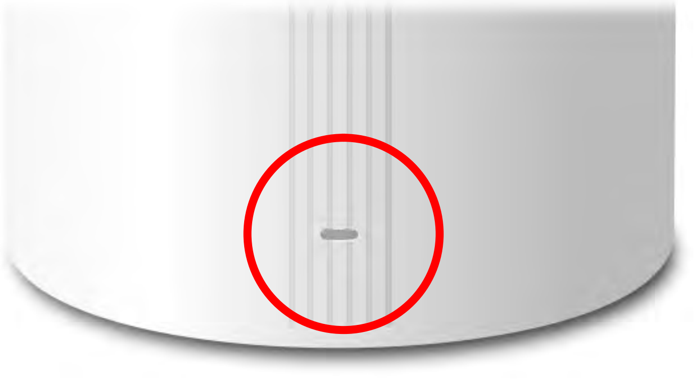
2. Connect a computer to other available LAN port. Make sure the subnet IP address of the PC is the same as VigorAP 805 management IP, e.g., 192.168.1.X.

3. Connect the A/C power adapter to the wall socket, and then connect it to the PWR connector of the access point.



4. Power on VigorAP.

5. Check and make sure the LED on the front panel is solid on (red or white).



I-3 Network IP Configuration

After the network connection is built, the next step you should do is setup VigorAP 805 with proper network parameters, so it can work properly in your network environment.

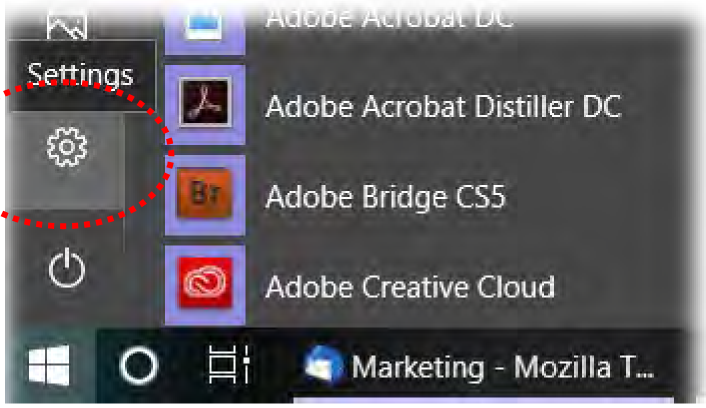
Before you can connect to the access point and start configuration procedures, your computer must be able to get an IP address in the same subnet as this AP. If it's not connected to the same DHCP Server with the AP or you're unsure, please follow the following instructions to configure your computer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

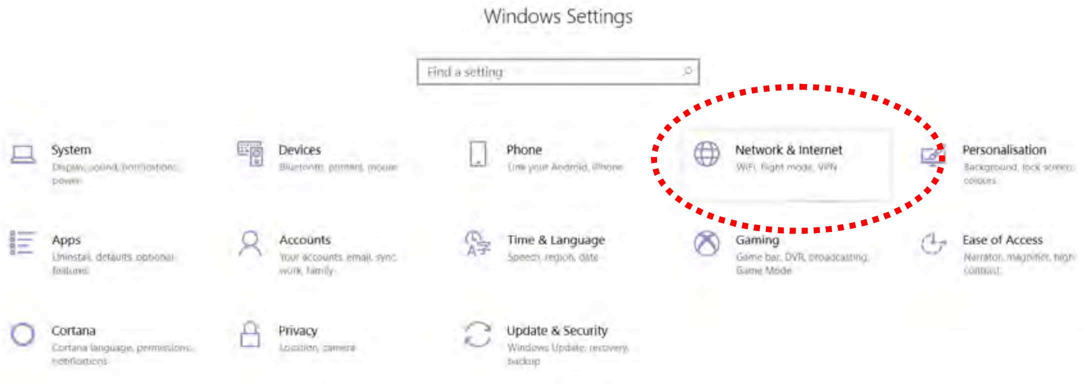
Windows 10 - please go to section I-3-1

I-3-1 Windows 10 IP Address Setup

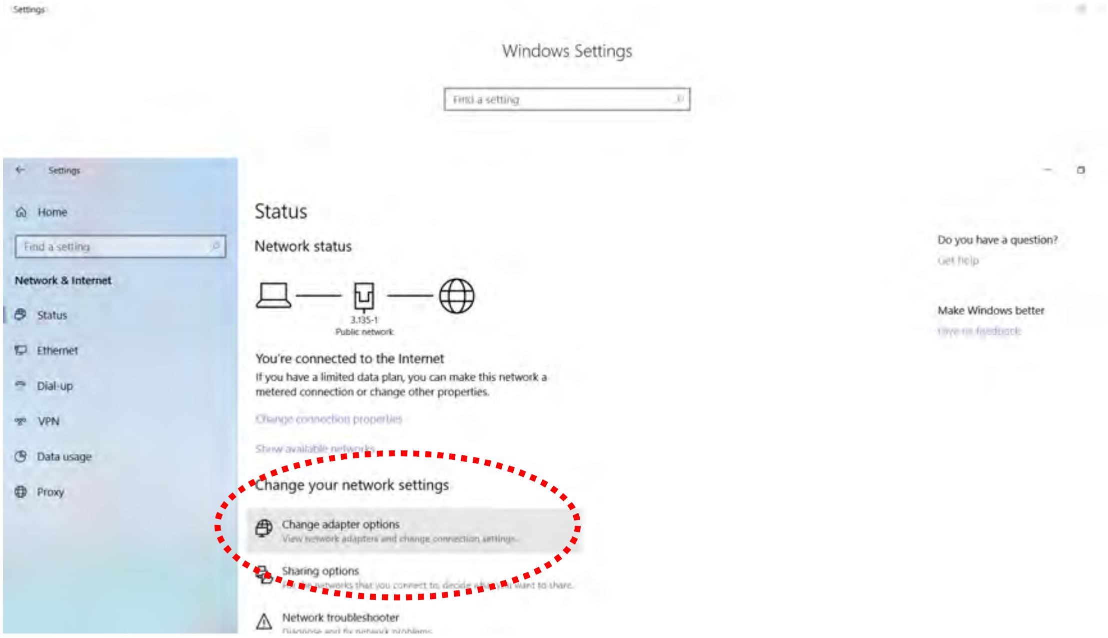
Click the **Start** button (it should be located at lower-left corner of your computer), then click the **Settings** icon.



Double-click **Network & Internet**.


Windows Settings
Find a setting
System
Display, sound, notifications, power
Devices
Bluetooth, printers, mouse
Phone
Link your Android, iPhone
Network & Internet
WiFi, flight mode, VPN
Personalisation
Background, lock screen, colours
Apps
Uninstall, defaults, optional features
Accounts
Your accounts, email, sync, work, family
Time & Language
Speech, region, date
Gaming
Game bar, DVR, broadcasting, Game Mode
Ease of Access
Narrator, magnifier, high contrast
Cortana
Cortana language, permissions, notifications
Privacy
Location, camera
Update & Security
Windows Update, recovery, backup

Next, click **Change adapter options.**

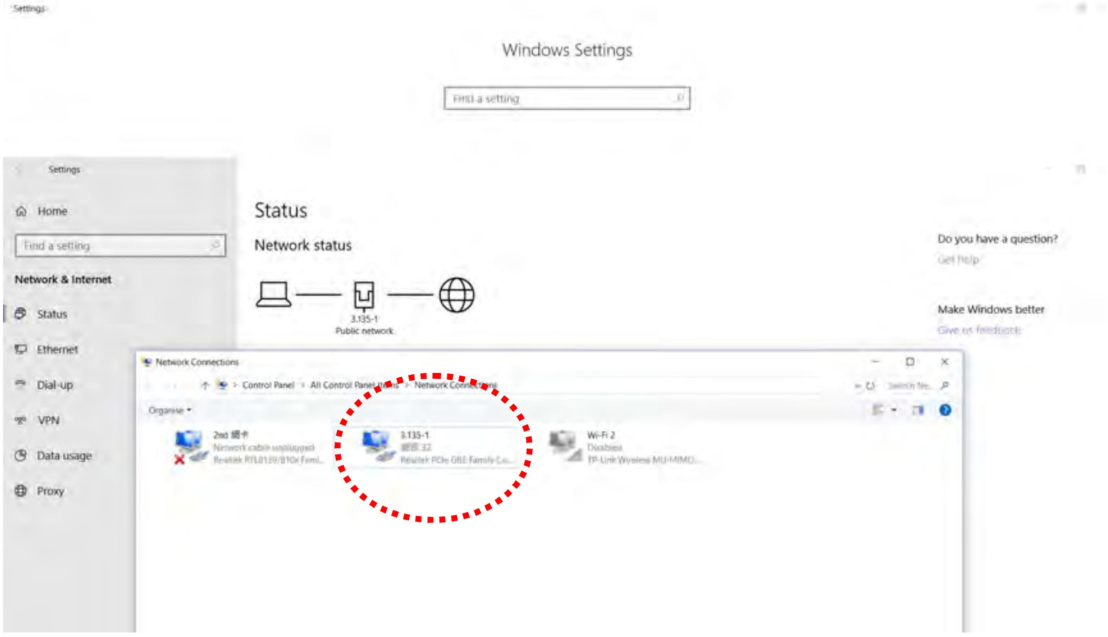


You're connected to the Internet

If you have a limited data plan, you can make this network a metered connection or change other properties.

Change connection properties
Show available networks
Change your network settings
Change adapter options
View network adapters and change connection settings.
Sharing options
For the networks that you connect to, decide what you want to share.
Network troubleshooter
Diagnose and fix network problems.
Do you have a question?
Get help
Make Windows better
Give us feedback

Click the local area connection.

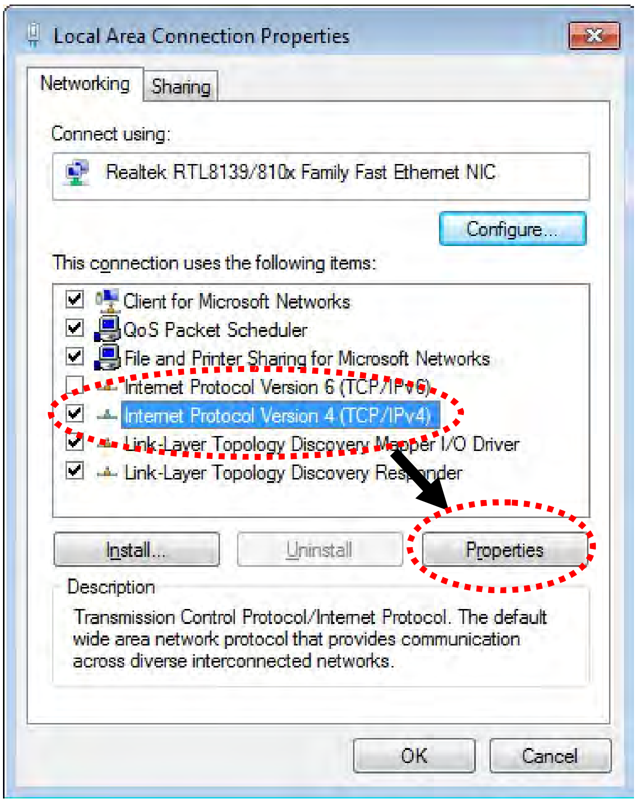


2nd 網卡
Network cable unplugged
Realtek RTL8139/810x Fami...

3.135-1
網路 32
Realtek PCIe GBE Family Co...

Wi-Fi 2
Disabled
TP-Link Wireless MU-MIMO...

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



Local Area Connection Properties

Connect using:

Realtek RTL8139/810x Family Fast Ethernet NIC

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- □ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

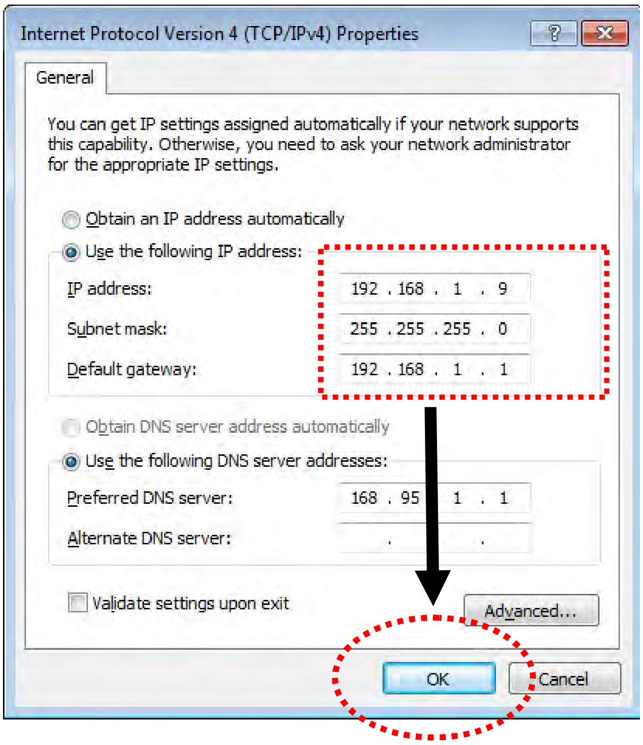
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

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**



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 9

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 168 . 95 . 1 . 1

Alternate DNS server: . . .

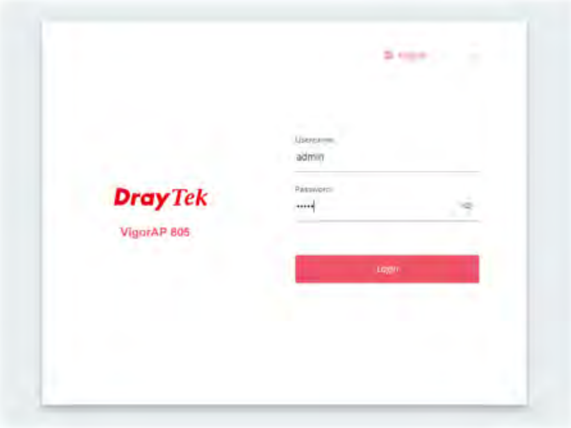
□ Validate settings upon exit

I-4 Accessing to Web User Interface

107

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 805 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. Please type "admin/admin" on Username/Password and click **OK**.



ⓘ Note:

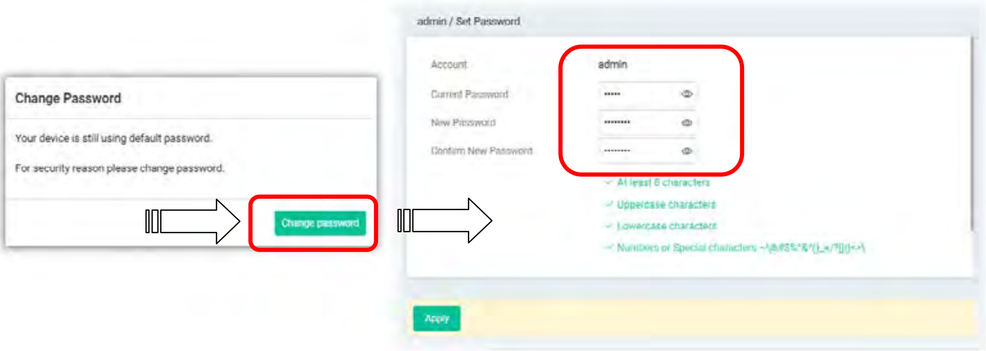
You may either simply set up your computer to get IP dynamically from the router or set up the IP address of the computer to be in the same subnet as **the IP address of VigorAP 805.**

- If there is no DHCP server on the network, then VigorAP 805 will have an IP address of 192.168.1.2.
- If there is DHCP available on the network, then VigorAP 805 will receive it's IP address via the DHCP server.

---

3. Next, the page will appear to guide you change the login password.

You **MUST** change the login password before accessing the web user interface. Please set a new password for network security.



Change Password

Your device is still using default password.

For security reason please change password.

admin / Set Password

Account: admin

Current Password: •••••

New Password: ••••••••

Confirm New Password: ••••••••

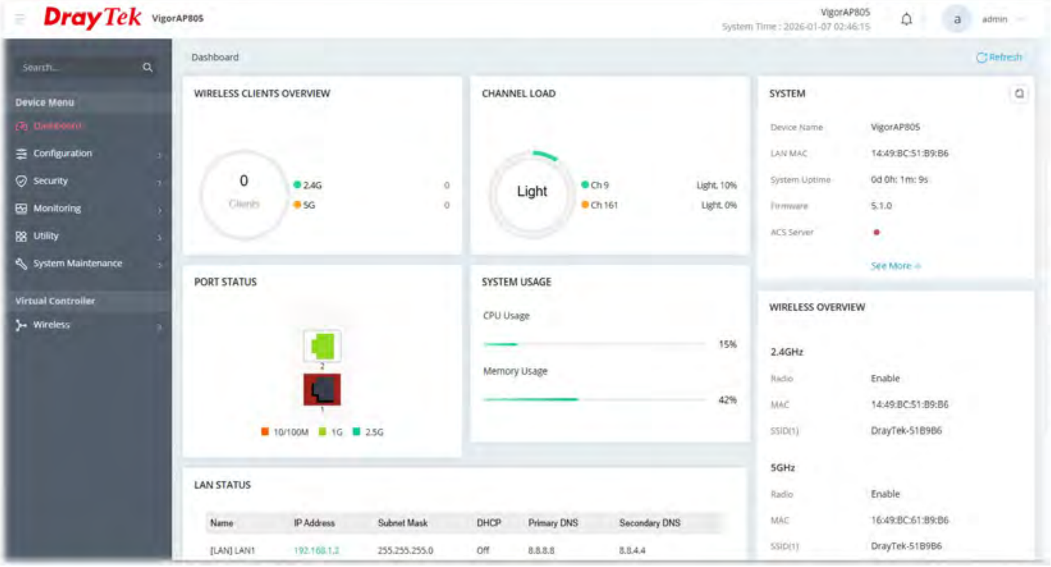
✓ At least 8 characters

✓ Uppercase characters

✓ Lowercase characters

✓ Numbers or Special characters ~!@#$%^&*()_=/?[]{}<>\

4. After clicking **Apply**, the Main Screen will pop up. When the homepage appears, view the configuration and modify the settings if you want.



SYSTEM

Device Name: VigorAP805
LAN MAC: 14:49:BC:51:B9:B6
System Uptime: 0d 0h: 1m: 9s
Firmware: 5.1.0
ACS Server: ●

WIRELESS OVERVIEW

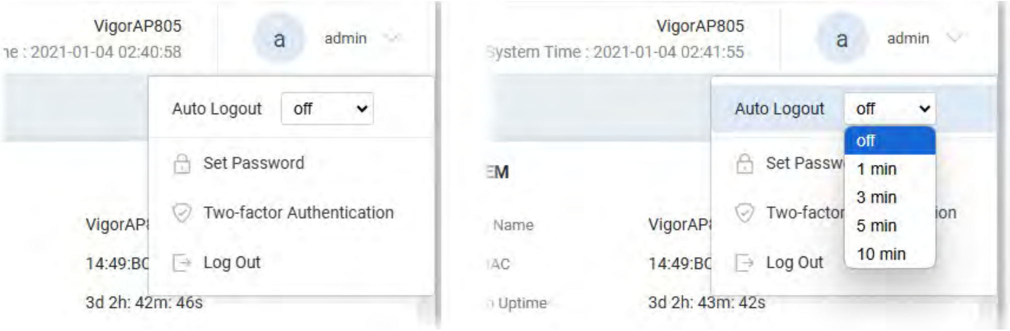
2.4GHz
Radio: Enable
MAC: 14:49:BC:51:B9:B6
SSID(1): DrayTek-51B9B6

5GHz
Radio: Enable
MAC: 16:49:BC:61:B9:B6
SSID(1): DrayTek-51B9B6

LAN STATUS

Name	IP Address	Subnet Mask	DHCP	Primary DNS	Secondary DNS
[LAN] LAN1	192.168.1.2	255.255.255.0	Off	8.8.8.8	8.8.4.4

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.



Auto Logout: off

Note:

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

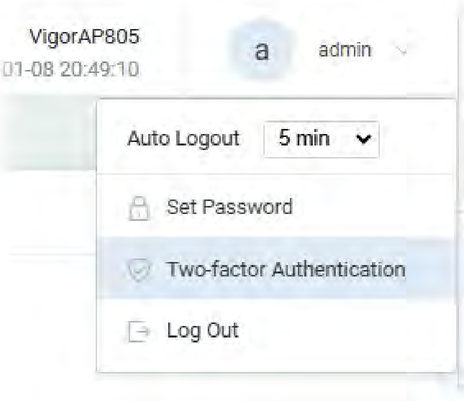
For using the device properly, it is necessary for you to change the password of web configuration for security and adjust primary basic settings.

I-5 Two-Factor Authentication

If network security is highly concerned, two-factor authentication will be strongly recommended.

For using two-factor authentication for accessing VigorAP;

1. Get and install **Google Authenticator** (iOS/Android) first.
2. Login VigorAP by using the user account and password.
3. Select **Two-factor Authentication.**

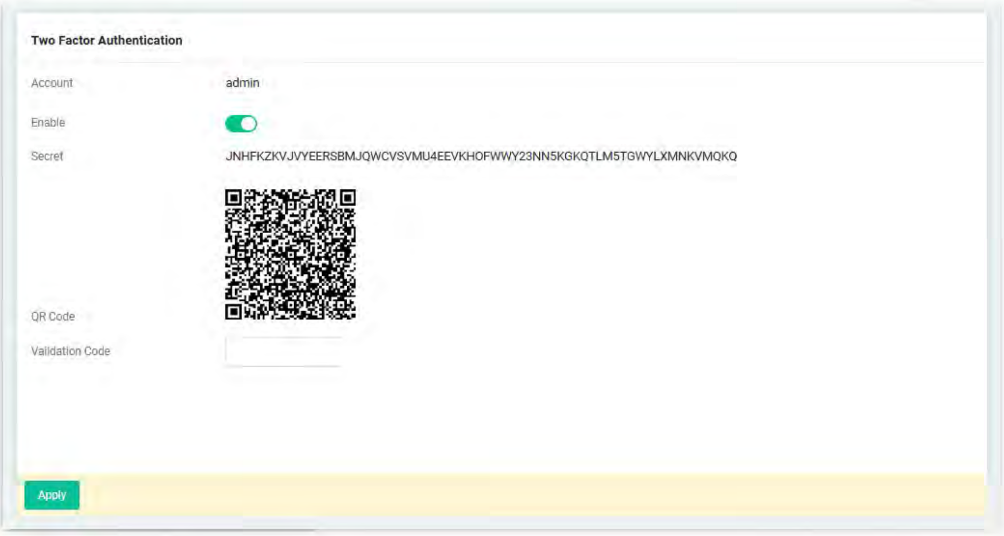


VigorAP805
01-08 20:49:10

admin

Auto Logout: 5 min

4. On the following page, switch the toggle of **Enable** to enable the function.



Two Factor Authentication

Account: admin

Enable: ●

Secret: JNHFKZKVJVYEERSBMJQWCVSVMU4EEVKHOFWWY23NN5KGKQTLM5TGWYLXMNKVMQKQ

QR Code

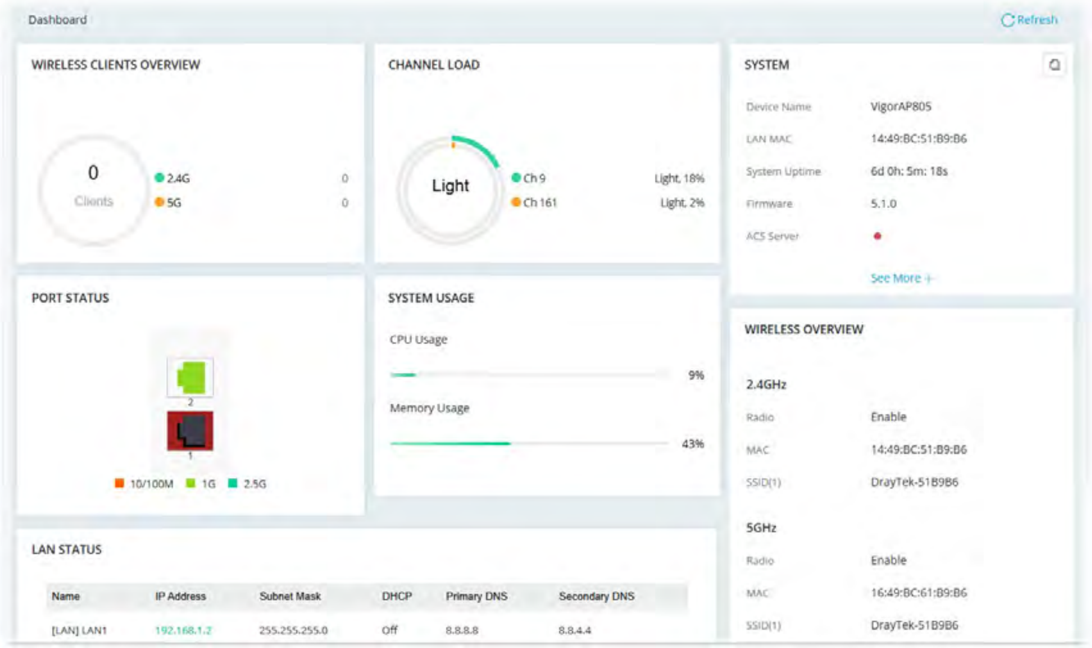
Validation Code

5. Use your cell phone to scan the QR-Code shown on the page. A key will be created randomly on the cell phone. Enter that key on the box of Verification Code and click the **Apply** button.
6. Logout VigorAP.
7. Re-login VigorAP. The first login web page requires you to enter the original user account and password. After clicking the Login button, the ***second*** login web page appears. Please enter the authentication code (created randomly) obtained from the APP (Google Authenticator) on your cell phone and click the Verify button.

I-6 Dashboard

Dashboard shows port status, LAN status, LAN usage, system status, and wireless overview information.

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



WIRELESS CLIENTS OVERVIEW

● 2.4G	0
● 5G	0

CHANNEL LOAD

● Ch 9	Light, 18%
● Ch 161	Light, 2%

SYSTEM USAGE

CPU Usage	9%
Memory Usage	43%

SYSTEM

Device Name	VigorAP805
LAN MAC	14:49:BC:51:B9:B6
System Uptime	6d 0h: 5m: 18s
Firmware	5.1.0
ACS Server	●

WIRELESS OVERVIEW

2.4GHz

Radio	Enable
MAC	14:49:BC:51:B9:B6
SSID(1)	DrayTek-51B9B6

5GHz

Radio	Enable
MAC	16:49:BC:61:B9:B6
SSID(1)	DrayTek-51B9B6

LAN STATUS

Name	IP Address	Subnet Mask	DHCP	Primary DNS	Secondary DNS
[LAN] LAN1	192.168.1.2	255.255.255.0	Off	8.8.8.8	8.8.4.4

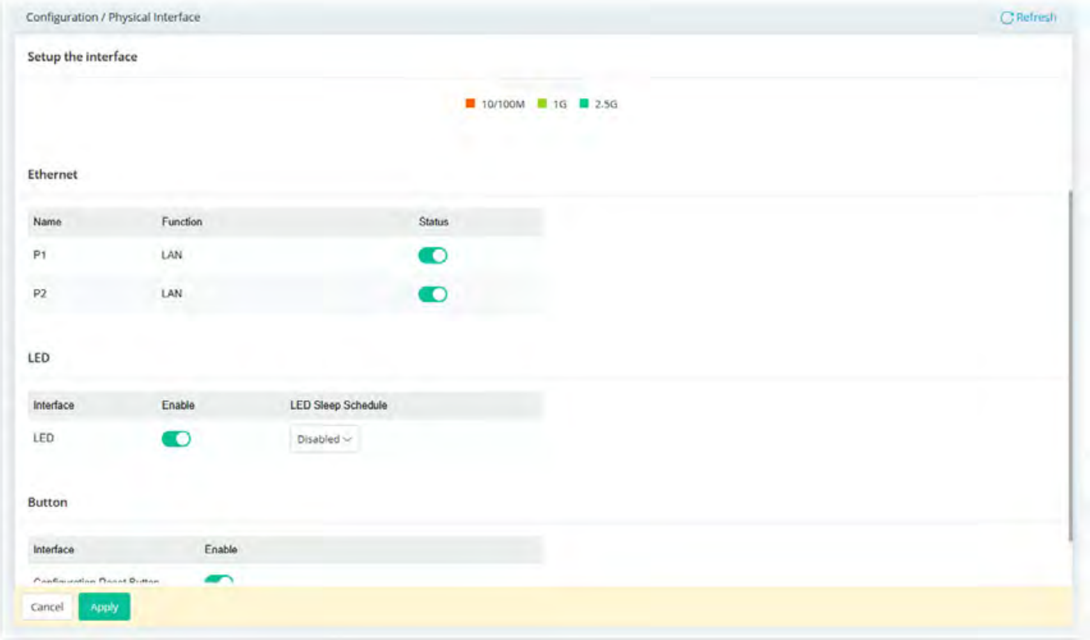
This page is left blank.

Chapter II Connectivity

II-1 Configuration

II-1-1 Physical Interface

Configure the general settings for LAN interface. Open **Configuration >> Physical Interface**.



Configuration / Physical Interface

Setup the interface

Ethernet

Name	Function	Status
P1	LAN	●
P2	LAN	●

LED

Interface	Enable	LED Sleep Schedule
LED	●	Disabled

Button

Interface	Enable
Configuration Reset Button	●

Available settings are explained as follows:

Item	Description
Ethernet	
Name	Displays the name of the Ethernet port.
Function	Displays current function of the Ethernet port.
Status	Switch the toggle to enable or disable the Ethernet port.
LED	
Interface	Displays the name of the LED.
Enable	In default, the LED on the device will be always on. However, the LED can be turned on or off after a specified number of minutes has elapsed to meet certain requirements. For this, switch the toggle to enable this setting.
LED Sleep Schedule	The LED can be turned on or off based on the settings configured in the selected schedule (defined under Configuration>>Objects) profile to fulfill specific requirements. When LED is slept, it can be woken up by pressing one of the following buttons:

	● Factory Reset on the front panel ● Wake up LED on this configuration page Note that if the schedule is set with repeat type and applied here, the LED on the device will be turned on and turned off at specified time periodically and automatically.
Button	
Configuration Reset Button	The default value is **Enable**. Switch the toggle to disable the reset function of the factory reset button. Disabling the Factory Reset button only prevents it from being used to reboot Vigor router with default settings.
Cancel	Click to discard the modification
Apply	Click to save the settings.

ⓘ Note:

Switch these two icons by click the mouse cursor on them.

◉ - means “Enable”.

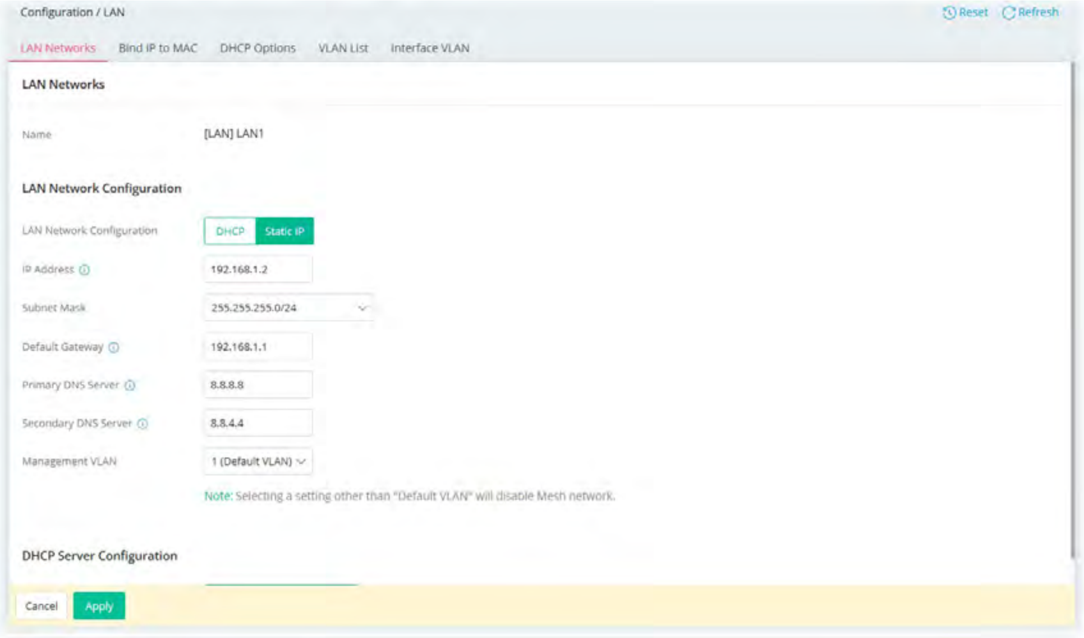
○ - means “Disable”.

II-1-2 LAN

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

II-1-2-1 LAN Networks

Open **Configuration>>LAN** and select the **LAN Networks** tab to open the following page.



LAN Networks

Name: [LAN] LAN1

LAN Network Configuration

LAN Network Configuration: DHCP [✓ Static IP]

IP Address: 192.168.1.2

Subnet Mask: 255.255.255.0/24

Default Gateway: 192.168.1.1

Primary DNS Server: 8.8.8.8

Secondary DNS Server: 8.8.4.4

Management VLAN: 1 (Default VLAN)

Note: Selecting a setting other than "Default VLAN" will disable Mesh network.

DHCP Server Configuration

Available settings are explained as follows:

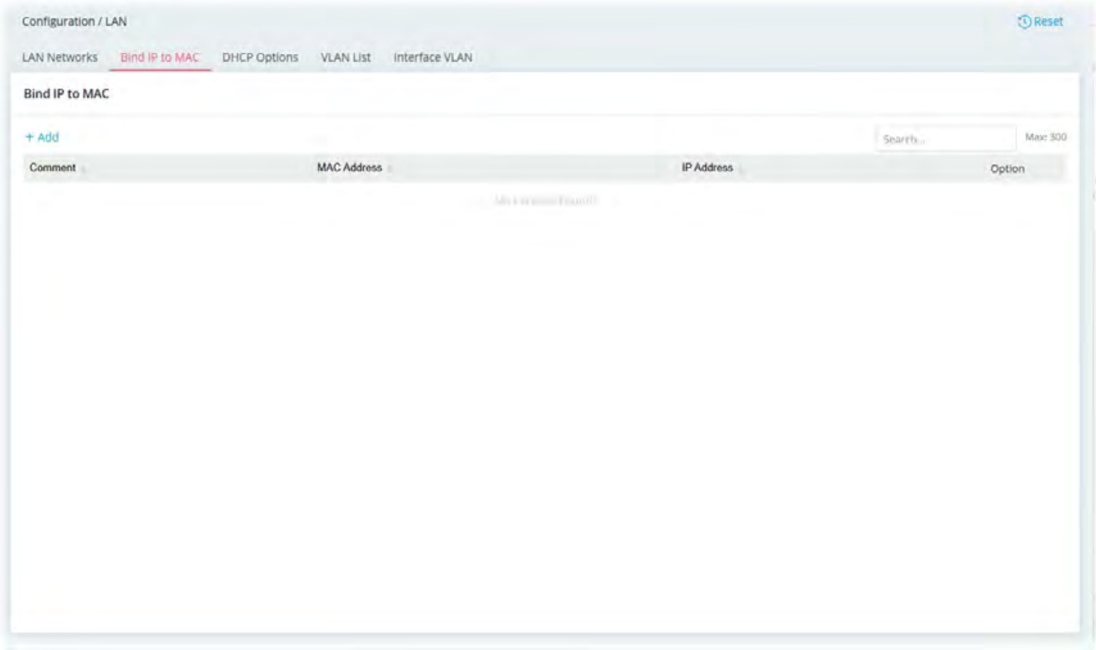
Item	Description
LAN Network Configuration	
LAN Network Configuration	Select the connection type for the LAN network. ● **DHCP** - DHCP stands for Dynamic Host Configuration Protocol. DHCP server can automatically dispatch related IP settings to any local user configured as a DHCP client. ● **Static IP**
When DHCP is selected	
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 device will automatically apply default DNS Server IP address: 194.109.6.66 to this field.
Secondary DNS Server	You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the device will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field.
Management VLAN	VigorAP 805 supports tag-based VLAN for wireless clients accessing Vigor device. Only the clients with the specified VLAN ID can access into VigorAP 805. Select a number as VLAN ID tagged on the transmitted packet. "None" means no VALN tag.

When Static IP is selected	
IP Address	Enter a private IP address for connecting to a local private network (Default: 192.168.1.2).
Subnet Mask	Enter an address code that determines the size of the network. (Default: 255.255.255.0/ 24)
Default Gateway	Enter a value of the gateway IP address for the DHCP server.
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 device will automatically apply default DNS Server IP address: 194.109.6.66 to this field.
Secondary DNS Server	You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the device will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field.
Management VLAN	VigorAP 805 supports tag-based VLAN for wireless clients accessing Vigor device. Only the clients with the specified VLAN ID can access into VigorAP 805. Select a number as VLAN ID tagged on the transmitted packet. "None" means no VALN tag.
DHCP Server Configuration - Available when Static IP is selected	
DHCP Server	● On - Lets the device assign IP address to every host in the LAN. ● Off - Lets you manually or use other DHCP server to assign IP address to every host in the LAN. ● Relay - Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to.
Start IP Address	It is available when On is selected as the DHCP Server. 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 device is 192.168.1.2, the starting IP address must be 192.168.1.3 or greater, but smaller than 192.168.1.254.
IP Pool Counts	It is available when On is selected as the DHCP Server. Enter a value of the IP address pool for the DHCP server to end with when issuing IP addresses.
Gateway IP Address	It is available when On is selected as the DHCP Server. Enter a value of the gateway IP address for the DHCP server.
Lease Time	It is available when On is selected as the DHCP Server. It allows you to set the leased time for the specified PC.
Primary DNS	It is available when On is selected as the DHCP 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 device will automatically apply default DNS Server IP address: 194.109.6.66 to this field.
Secondary DNS	It is available when On is selected as the DHCP 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 device will automatically apply default DNS Server IP address: 194.109.6.66 to this field.

DHCP Server IP Address	It is available when **Relay** is selected as the DHCP Server.
Cancel	Click to discard the modification and return to the previous page.
Apply	Click to save the settings.

II-1-2-2 Bind IP to MAC

This function is used to bind the IP and MAC address in LAN to have a strengthening control in network. With the Bind IP to MAC feature you can reserve LAN IP addresses for LAN clients. Each reserved IP address is associated with a Media Access Control (MAC) address.



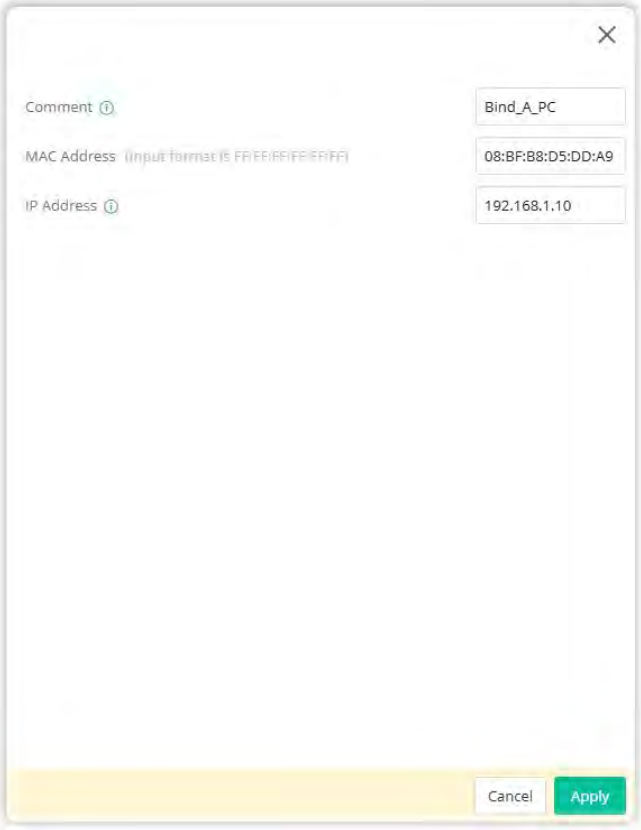
Comment	MAC Address	IP Address	Option

Available settings are explained as follows:

Item	Description
+Add	Click to create a new profile.
Comment	Displays a brief description for the entry.
MAC Address	Displays the MAC address used by the entry.
IP Address	Displays the IP address used by the entry.
Option	**Edit** - Click to modify the selected profile. **Delete** - Click to delete the selected entry.

To modify an existing profile, select a file and click **Edit.**

To add a new profile, click the +Add link to get the following page.



Comment ⓘ Bind_A_PC

MAC Address (Input format is FF:FF:FF:FF:FF:FF) 08:BF:B8:D5:DD:A9

IP Address ⓘ 192.168.1.10

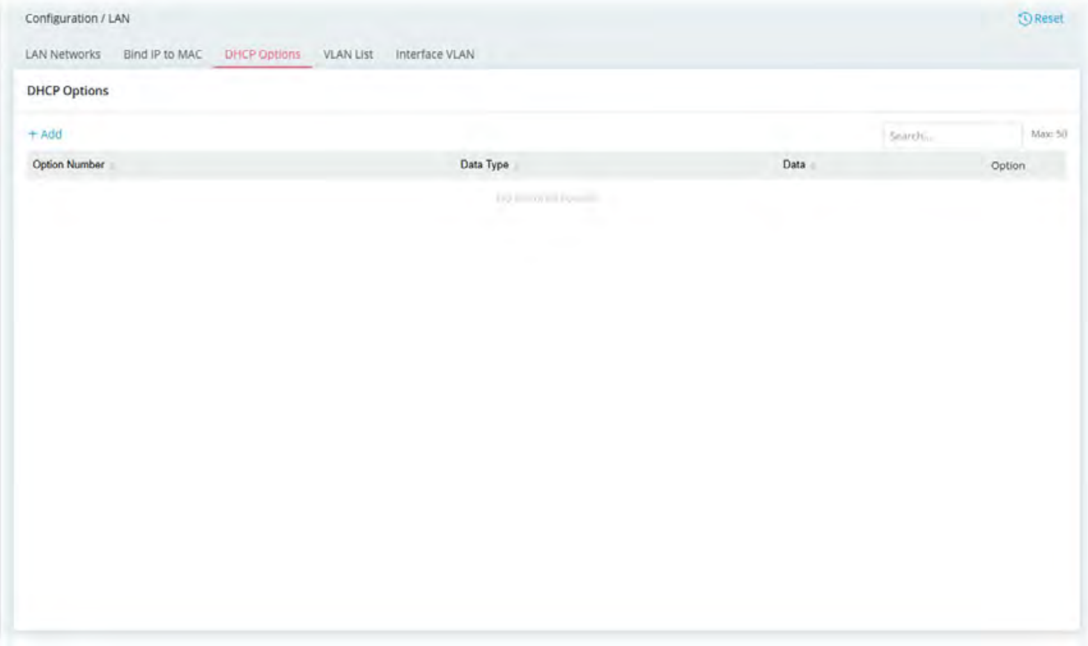
Available settings are explained as follows:

Item	Description
Comment	This is an optional field to identify this IP Address - MAC Address pair.
MAC Address	Use the drop-down menu to select a MAC address
IP Address	Use the drop-down menu to select an IP address.
Cancel	Discard the settings and return to the previous page.
Apply	Click it to save the settings and return to the previous page.

II-1-2-3 DHCP Options

DHCP packets can be processed by adding option number and data information when such function is enabled and configured.

This page allows you to configure additional DHCP client options.

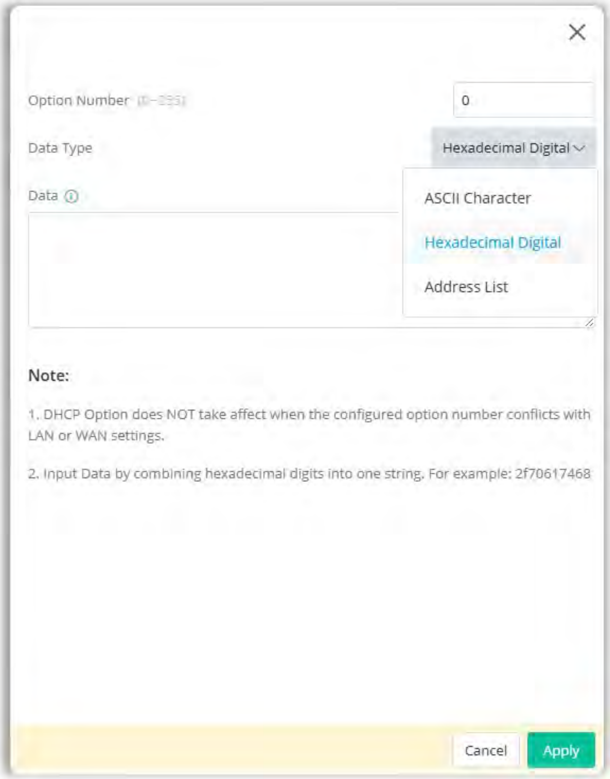


Available settings are explained as follows:

Item	Description
+Add	Click to create a new profile.
Option Number	Displays the number used by this profile.
Data Type	Displays the data type.
Option	**Edit** - Click to modify the selected profile. **Delete** - Click to delete the selected entry.

To modify an existing profile, select a file and click **Edit.**

To add a new profile, click the **+Add** link to get the following page.



Option Number (0 ~ 255) 0

Data Type: Hexadecimal Digital

Note:

1. DHCP Option does NOT take affect when the configured option number conflicts with LAN or WAN settings.

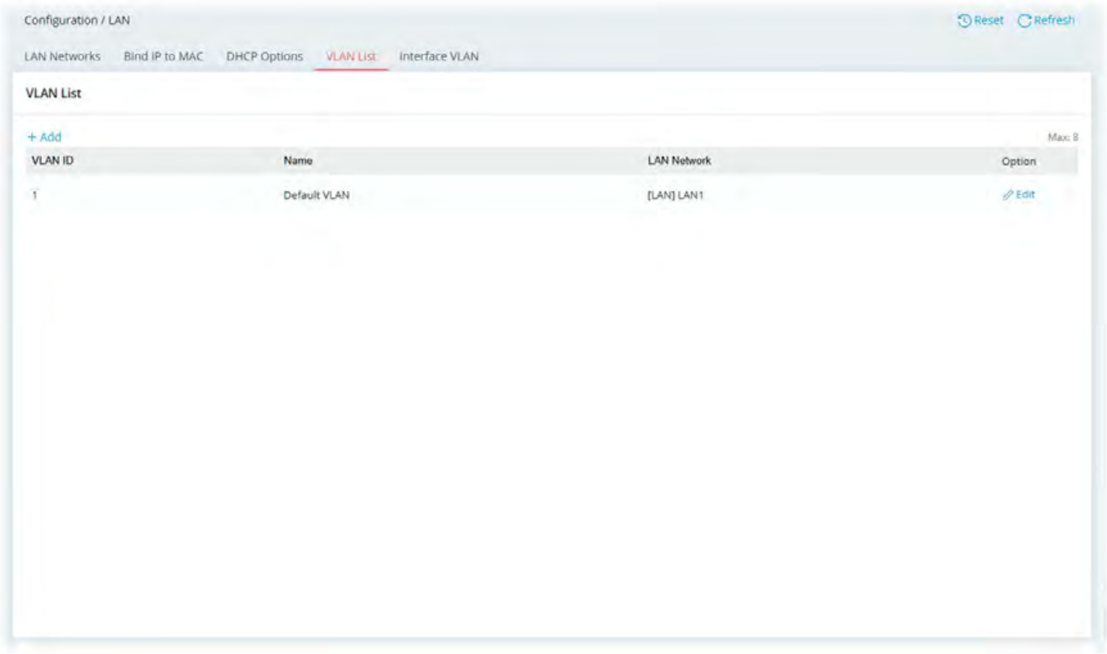
2. Input Data by combining hexadecimal digits into one string. For example: 2f70617468

Available settings are explained as follows:

Item	Description
Option Number	Enter a number (0 to 255) for this function.
Data Type	Choose the type (ASCII or Hex or Address List) for the data to be stored. Type of data in the Data field: ● ASCII Character - A text string. Example: /path. ● Hexadecimal Digit - A hexadecimal string. Valid characters are from 0 to 9 and from a to f. Example: 2f70617468. ● Address List - One or more IPv4 addresses, delimited by commas.
Data	Enter the content of the data to be processed by the function of DHCP option.
Cancel	Discard the settings and return to the previous page.
Apply	Click it to save the settings and return to the previous page..

II-1-2-4 VLAN List

Virtual Local Area Networks (VLANs) allow you to subdivide your LAN to facilitate management or to improve network security.



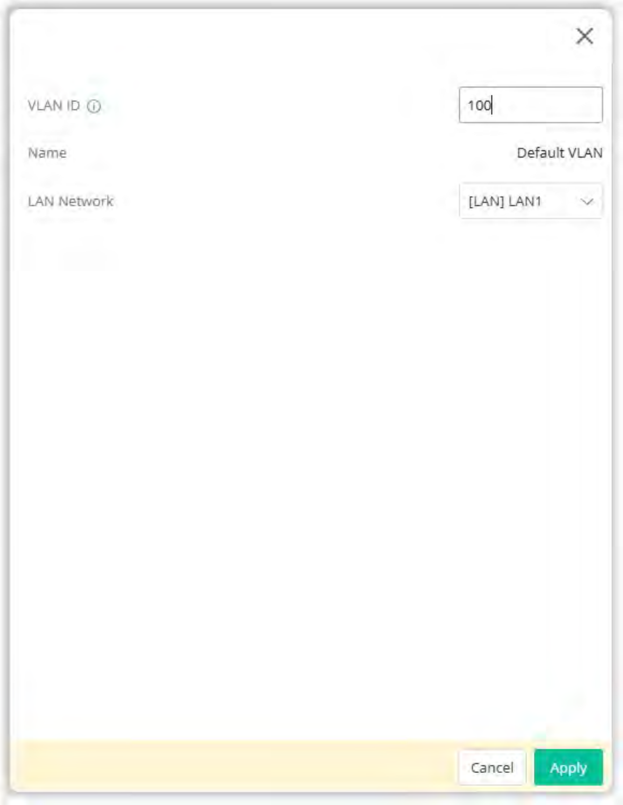
VLAN ID	Name	LAN Network	Option
1	Default VLAN	[LAN] LAN1	Edit

Available settings are explained as follows:

Item	Description
+Add	Click to create a new profile.
VLAN ID	Displays the number used by this profile.
Name	Displays the name of the VLAN profile.
LAN Network	Displays the LAN network used by the VLAN profile.
Option	**Edit** - Click to modify the selected profile. **Delete** - Click to delete the selected entry.

To modify an existing profile, select a file and click **Edit.**

To add a new profile, click the **+Add** link to get the following page.



VLAN ID: 100

Name: Default VLAN

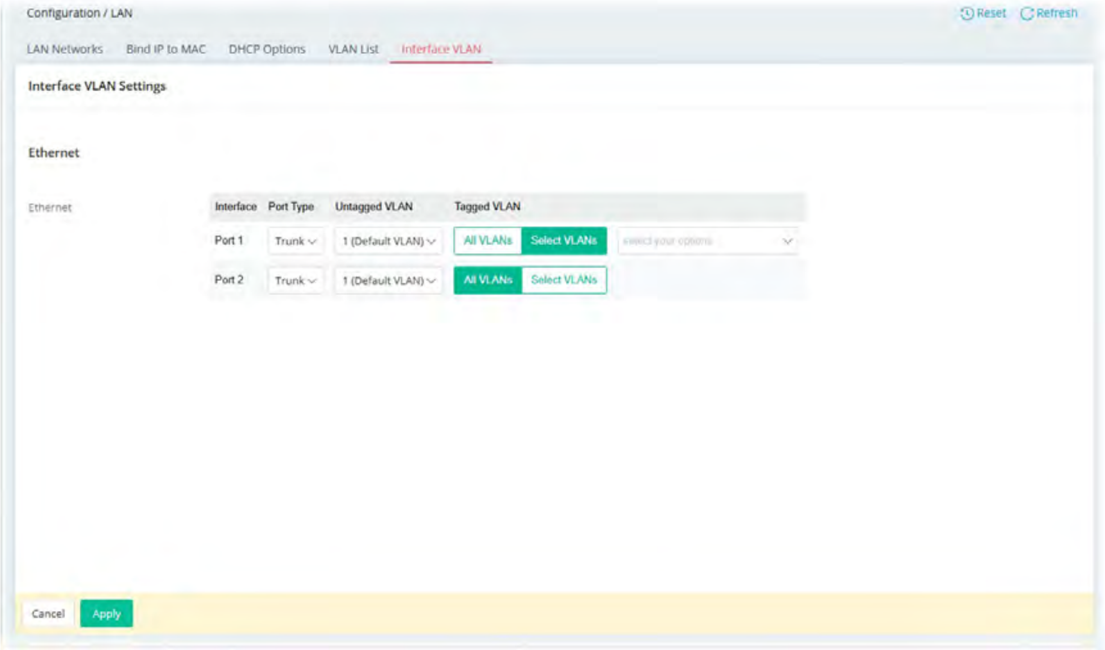
LAN Network: [LAN] LAN1

Available settings are explained as follows:

Item	Description
VLAN ID	Enter the value as the VLAN ID number.
Name	Enter a name to represent the VLAN profile.
LAN Network	Select the LAN network used by the VLAN profile.
Cancel	Discard the settings and return to the previous page.
Apply	Click it to save and apply the settings.

II-1-2-5 Interface VLAN

This page allows you to configure the LAN port settings to assure the VLAN profile can work normally.



Interface VLAN Settings

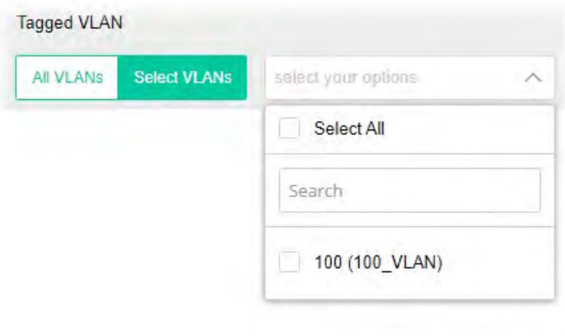
Ethernet

Ethernet

Interface	Port Type	Untagged VLAN	Tagged VLAN	
Port 1	Trunk	1 (Default VLAN)	All VLANs [✓ Select VLANs]	select your options
Port 2	Trunk	1 (Default VLAN)	[✓ All VLANs] Select VLANs	

Available settings are explained as follows:

Item	Description
Interface	Displays the Ethernet port number.
Port Type	Trunk - A trunk port can transmit data from multiple VLANs. Access - Transmits the data to and from a specific VLAN. An access port is only assigned to a single VLAN, it sends and receives frames that aren't tagged and only have the access VLAN value.
Untagged VLAN	Use the drop-down list to select a VLAN ID as the untagged VLAN. The connected host sends its traffic without any VLAN tag on the frames. However, when the frame reaches this interface (LAN port), It will be added with the VLAN tag.
Tagged VLAN	Select to enable 802.1Q tagging on this VLAN. The device will add specific VLAN number to all packets on the LAN while sending them out. All VLANs - All VLAN will be tagged. Select VLANs - Only the selected VLAN will be tagged.

	 Tagged VLAN All VLANs Select VLANs select your options Select All Search 100 (100_VLAN)
Cancel	Discard the settings and return to the previous page.
Apply	Save and apply the settings.

II-1-3 Wireless LAN

VigorAP 805 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 805 can support data rates up to 2.4 Gbps/4.8Gbps 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 805 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 805.

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.

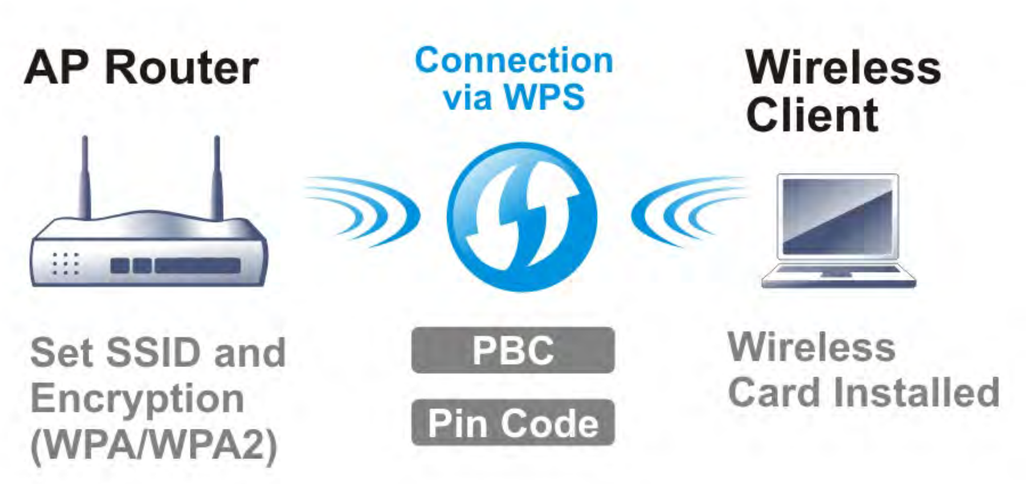
WPA (Wi-Fi Protected Access), the most dominating security mechanism in industry, is separated into two categories: WPA-personal or called WPA Pre-Share Key (WPA/PSK), and WPA-Enterprise or called WPA/802.1x.

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 805 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 805) with the encryption of WPA and WPA2.



It is the simplest way to build connection between wireless network clients and VigorAP 805. 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 805 automatically.

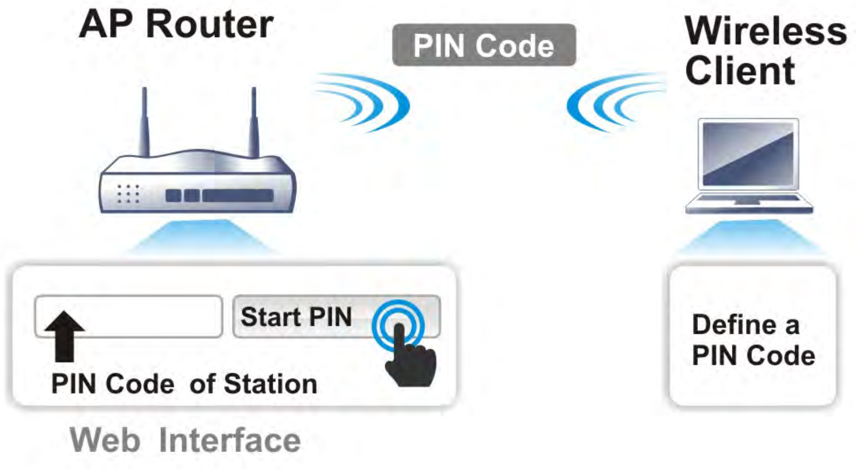
Note:

This 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*.

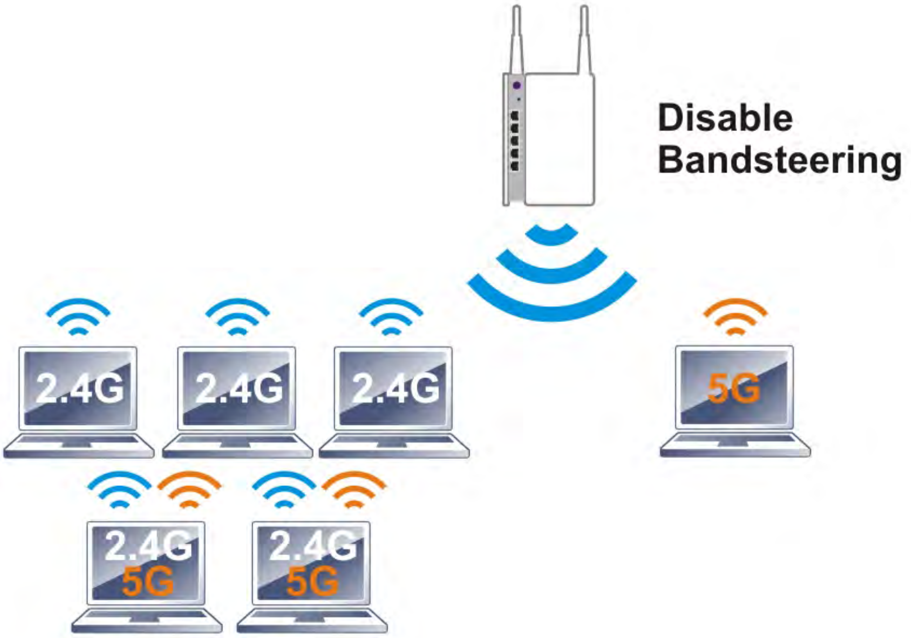
On the side of VigorAP 805 series which served as an AP, click Start PBC on web configuration interface. On the side of a station with network card installed, press Start PBC button of network card.

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 805.

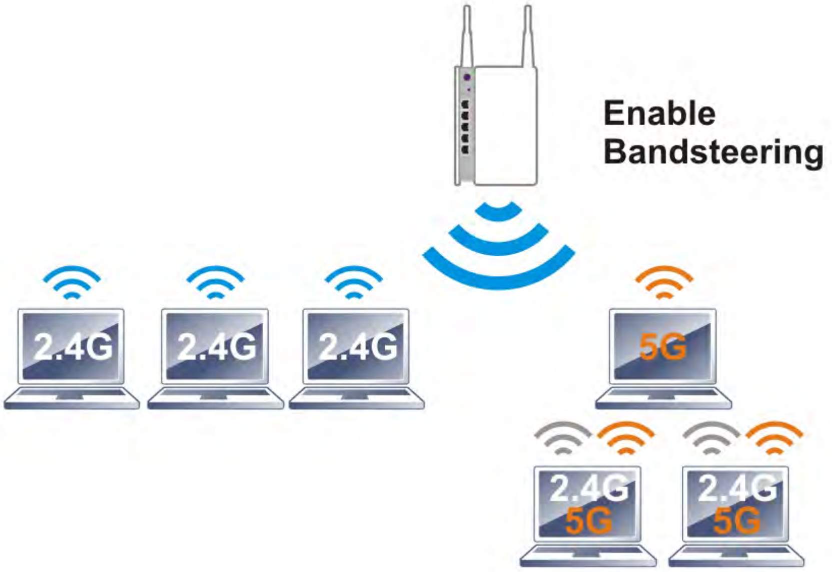


Band Steering

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



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



ⓘ Note:

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

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.

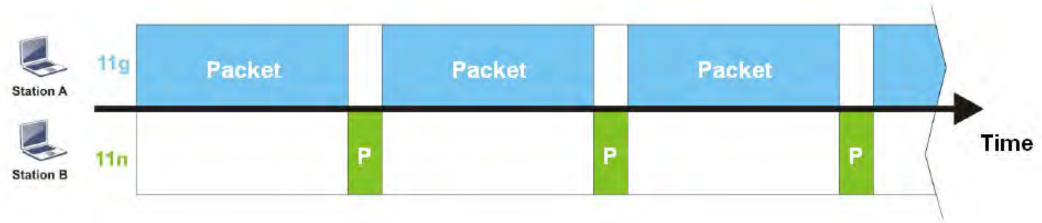
With airtime fairness, every client at a given quality-of-service level has equal access to the network's airtime.

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

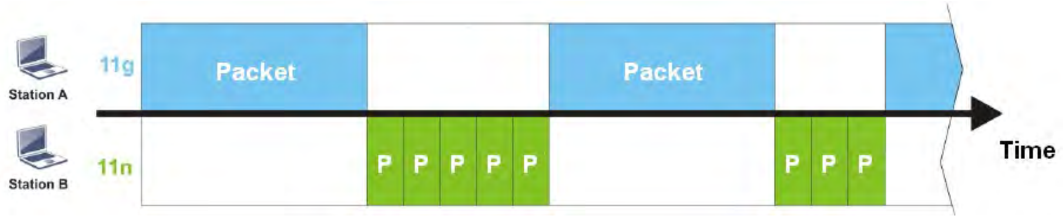
The principle behind the IEEE802.11 channel access mechanisms is that each station has ***an equal probability*** to access the channel. When wireless stations have similar data rates, this principle leads to a fair result. In this case, stations get a similar channel access time which is called airtime.

However, when stations have various data rates (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. Although they have an equal probability to access the wireless channel, Station B(11n) gets only a little airtime and waits too much because Station A(11g) spends a longer time to send one packet. In other words, Station B(fast rate) is obstructed by Station A(slow rate).



To improve this problem, Airtime Fairness is added for VigorAP. Airtime Fairness function tries to assign similar airtime to each station (A/B) by controlling TX traffic. In the following figure, Station B(11n) has 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).



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

Suitable environment:

(1) Many wireless stations.

(2) All stations mainly use download traffic.

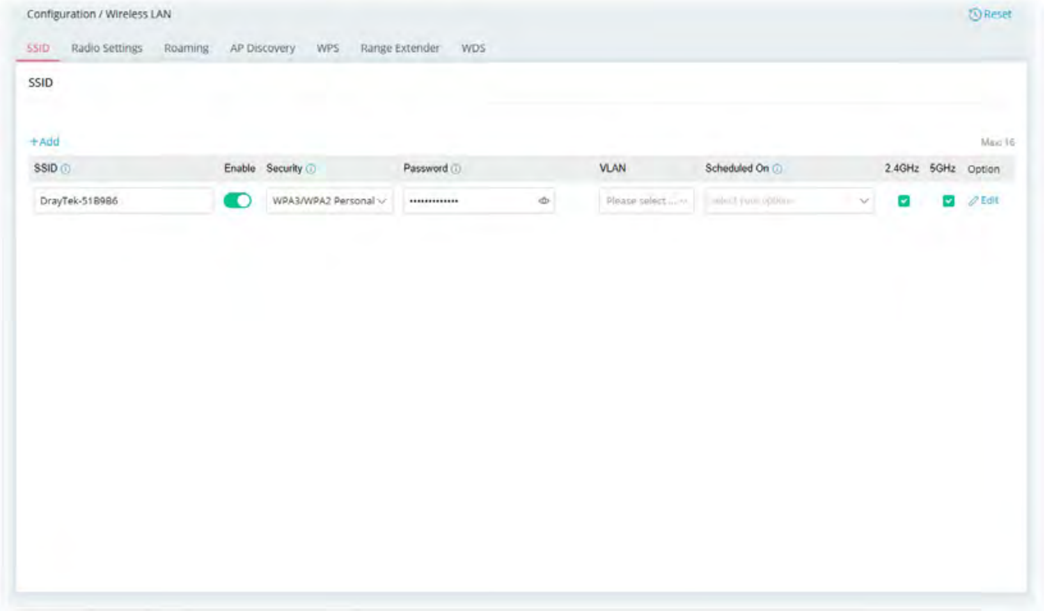
(3) The performance bottleneck is the wireless connection.

ⓘ Note:

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

II-1-3-1 SSID

By clicking the SSID tab, a web page will appear so that you could set the SSID, the security mode, and the password.



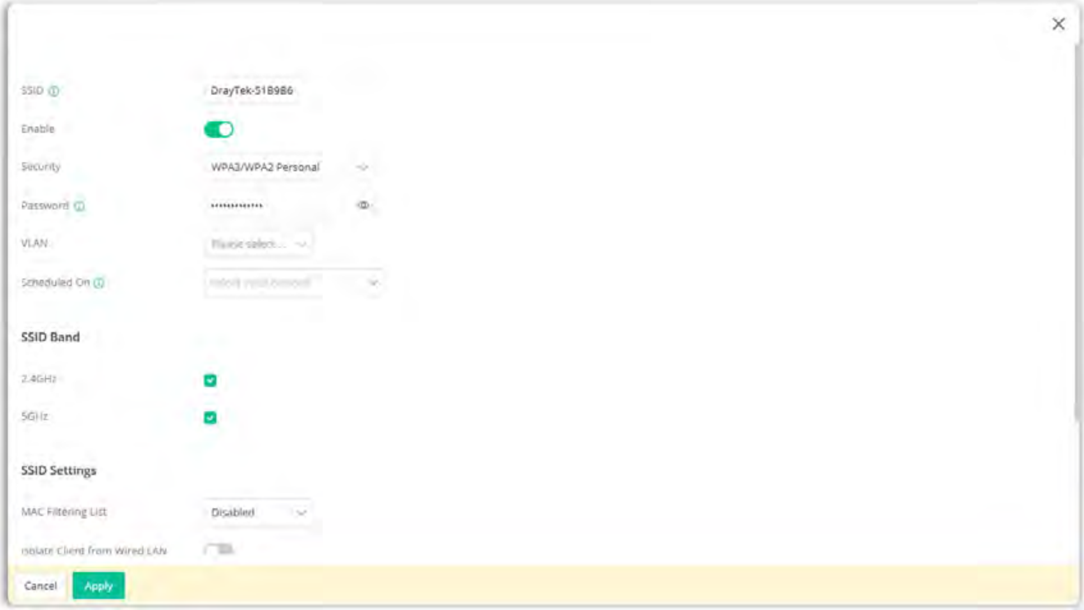
SSID	Enable	Security	Password	VLAN	Scheduled On	2.4GHz	5GHz	Option
DrayTek-51B986	●	WPA3/WPA2 Personal	••••••••••••••	Please select ...	select your options	☑	☑	Edit

Available settings are explained as follows:

Item	Description
+Add	Click to set a new SSID.
SSID Name	Displays the name of the SSID.
Enable	Switch the toggle to enable or disable this entry.
Security	Displays the security mode used by this entry. If required, use the drop-down list to select another mode.
Password	Displays the password used by this entry.

VLAN	Select VLAN ID # for this SSID. Packets transferred from this SSID to LAN will be tagged with the number.
Scheduled On	Select either the "Always On" option or set a specific schedule for the SSID.
2.4GHz	Switch the toggle to enable or disable this entry. If enabled, this entry will be applied to 2.4GHz wireless network.
5GHz	Switch the toggle to enable or disable this entry. If enabled, this entry will be applied to 5GHz wireless network.
Option	**Edit** - Click to modify the selected profile. **Delete** - Click the selected entry. The default SSID can not be deleted.
Cancel	Discard the settings and return to the previous page.
Apply	Save and apply the settings.

To edit an existing SSID, click the **Edit** link to get to the following page.



SSID: DrayTek-518986

Enable: on

Security: WPA3/WPA2 Personal

Password: ••••••••••••••

VLAN: Please select...

Scheduled On: [illegible]

SSID Band

2.4GHz: ☑

5GHz: ☑

SSID Settings

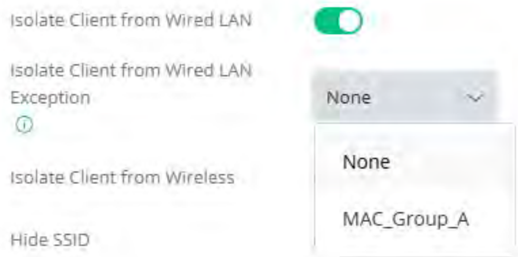
MAC Filtering List: Disabled

Isolate Client from Wired LAN: off

Available settings are explained as follows:

Item	Description
SSID	Set a name for VigorAP to be identified.
Enable	Switch the toggle to enable or disable the function.
Security	There are several modes provided for you to choose from. Below shows the modes with higher security; ● **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. 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, 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. ● **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. Below shows the modes with basic security; ● **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. ● **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. ● **WEP Personal** - Accepts only WEP clients and the encryption key should be entered in WEP Key. ● **None** - The encryption mechanism is turned off.
Password	Enter **8~63** ASCII characters, such as "012345678". This feature is available for **WPA Personal or WPA2 Personal or WPA2 / WPA Personal** mode, **WPA3 Personal** or **WPA3/WPA2 Personal**.
RADIUS Server	This feature is available for **WPA3 Enterprise, WPA2 Enterprise, WPA2/WPA Enterprise,** and **WPA Enterprise** mode. Use the drop-down list to select a RADIUS server setting. **Note**: Before configuring the RADIUS server, go to **Configuration>>RADIUS** to create external RADIUS profiles (at least one) first.
VLAN	Select VLAN ID # for this SSID. Packets transferred from this SSID to LAN will be tagged with the number. If your network uses VLANs, you can assign the SSID to a VLAN on your network. Client devices that associate using the SSID are grouped into this VLAN. The VLAN ID range is from 3 to 4095. The VLAN ID is None by default, it means disabling the VLAN function for the SSID.
Scheduled On	Select Always or any other schedule profile. **Always** - This WLAN profile will be active all the time. Or, use the drop-down list to select a preset schedule profile. Before choosing, please go to **Configuration>>Object** to create schedule profiles (at least one).
SSID Band	
2.4GHz/5GHz	Select 2.4GHz and/or 5GHz for applying to this wireless LAN setting.

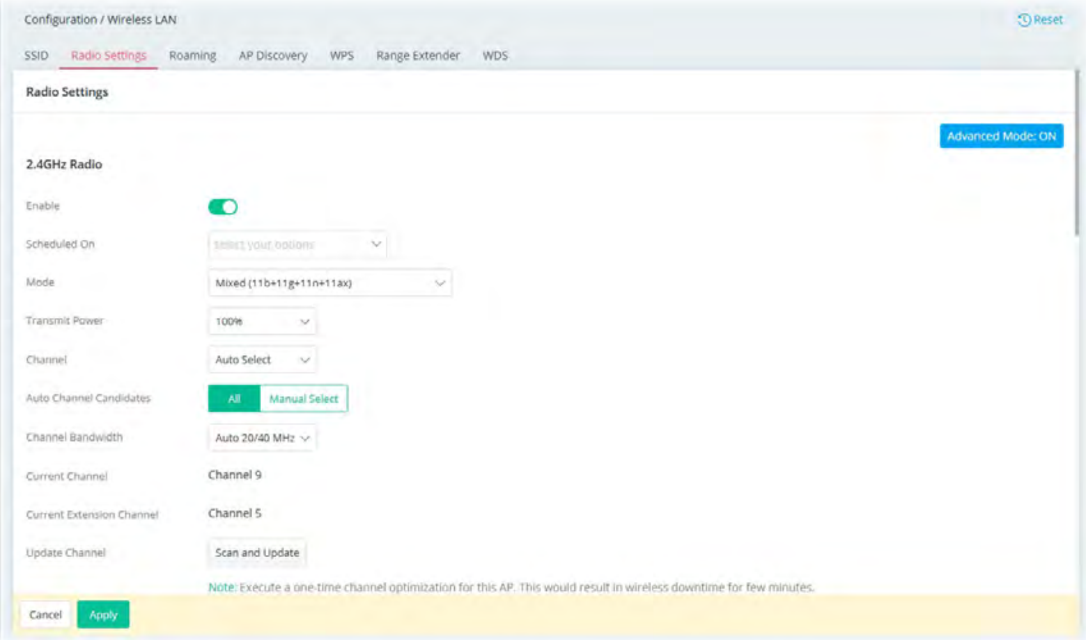
SSID Settings	
MAC Filtering List	**Disabled** - Disable the function of using MAC Filtering List. Or, use the drop-down list to select a preset profile. Before choosing, please go to **Security>>MAC Filtering** to create MAC filtering profiles (at least one).
Isolate Client from Wired LAN	Switch the toggle to enable or disable the function. Makes the Wireless clients with this SSID not access to Wired devices. **Isolate Client from Wired LAN Exception** - Select the MAC group object (created in Configuration>>Object>>MAC Group). Wireless clients with this SSID are allowed to access the Wired devices specified in the MAC group object.  Isolate Client from Wired LAN Isolate Client from Wired LAN Exception: None Isolate Client from Wireless Hide SSID
Isolate Client from Wireless LAN	Switch the toggle to enable or disable the function. Makes the wireless clients (stations) with the same SSID not access for each other.
Hide SSID	Switch the toggle to enable or disable the function. Prevents 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 805 while site surveying. The system allows you to set four sets of SSID for different usage.
WPA Settings	
WPA Algorithm	This feature is available for **WPA2 Personal, WPA2/WPA Personal, WPA2 Enterprise, WPA2/WPA Enterprise, WPA Personal, or WPA Enterprise mode.** Select TKIP, AES, or TKIP/AES as the algorithm for WPA.
Key Renewal Interval	WPA uses a shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key 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. This feature is available for **WPA3 Personal, WPA3/WPA2 Personal, WPA2 Personal, WPA2/WPA Personal, WPA3 Enterprise, WPA2 Enterprise, WPA2/WPA Enterprise, WPA Personal, WPA Enterprise** mode.
WEP Settings	
Default Key	This feature is available for **WEP Personal** mode. 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 ','.
Key # Type	Hex/ASCII - 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 ','. This feature is available for WEP Personal mode.
Key #	Enter 5 ASCII characters or 10 hexadecimal values in 64-bit encryption level, or 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level. This feature is available for WEP Personal mode.
Cancel	Discard the settings and return to the previous page.
Apply	Save and apply the settings.

Click Apply to save the settings and return to the previous page.

II-1-3-2 Radio Settings

This page is to determine the wireless radio setting, like channel, physical mode, channel bandwidth, transmit power and etc.



Radio Settings

2.4GHz Radio

Enable: ON

Scheduled On: select your options

Mode: Mixed (11b+11g+11n+11ax)

Transmit Power: 100%

Channel: Auto Select

Auto Channel Candidates: All / Manual Select

Channel Bandwidth: Auto 20/40 MHz

Current Channel: Channel 9

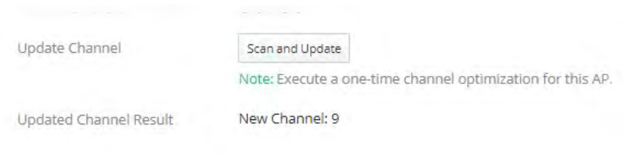
Current Extension Channel: Channel 5

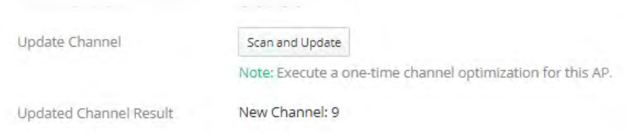
Update Channel: Scan and Update

Note: Execute a one-time channel optimization for this AP. This would result in wireless downtime for few minutes.

Available settings are explained as follows:

Item	Description
Advanced Mode	**ON/OFF** - Click the button to show or hide more settings.
2.4GHz Radio	
Enable	Switch the toggle to enable or disable the function.
Scheduled On	Select Always or any other schedule profile. **Always** - This WLAN profile will be active all the time. Or, use the drop-down list to select a preset schedule profile. Before choosing, please go to **Configuration>>Object** to create schedule profiles (at least one).
Mode	At present, VigorAP can connect to 11b only, 11g only, 11n only, Mixed (11b+11g), Mixed (11g+11n), Mixed (11b+11g+11n) and Mixed (11b+11g+11n+11ax) stations simultaneously. Simply choose Mixed (11b+11g+11n+11ax) mode.
Transmit Power	The default setting is the maximum (100%). Lowering down the value may degrade the range and throughput of wireless.
Channel	Means the channel of frequency of the wireless LAN. You may switch the channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select **Auto Select** to let the system determine for you.
Auto Channel Candidates	Let the system determine the optimal channel by selecting “Auto Select”. The list of available channels varies depending on the settings configured here. **All** – The Vigor system can choose the optimal channel from all

	channels. **Manual Select** – Select one channel or multiple channels for the Vigor system to choose the optimal channel.
Channel Bandwidth	**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. **20 MHz**- The device will use 20MHz for data transmission and receiving between the AP and the stations. **40 MHz**- The device will use 40MHz for data transmission and receiving between the AP and the stations.
Current Channel	Displays current channel number.
Current Extension Channel	Displays current extension channel.
Update Channel	**Scan and Update** - Click to select the best channel again when **Auto Select** is selected as the Channel setting.
Updated Channel Result	Displays the best channel after pressing the **Scan and Update** button.  Update Channel: Scan and Update Note: Execute a one-time channel optimization for this AP. Updated Channel Result: New Channel: 9
5GHz Radio	
Enable	Switch the toggle to enable or disable the function.
Scheduled On	Select Always or any other schedule profile. **Always** - This WLAN profile will be active all the time. Or, use the drop-down list to select a preset schedule profile. Before choosing, please go to **Configuration>>Object** to create schedule profiles (at least one).
Mode	At present, VigorAP can connect to 11a only, 11n only (5G), Mixed (11a+11n), Mixed (11a+11n+11ac), and Mixed (11a+11n+11ac+11ax) stations simultaneously. Simply choose Mixed (11b+11g+11n+11ax) mode.
Transmit Power	The default setting is the maximum (100%). Lowering down the value may degrade the range and throughput of wireless.
Channel	Means the channel of frequency of the wireless LAN. You may switch the channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select **Auto Select** to let the system determine for you.
Auto Channel Candidates	Let the system determine the optimal channel by selecting "Auto Select". The list of available channels varies depending on the settings configured here. **All** – The Vigor system can choose the optimal channel from all channels. **Exclude DFS Channels** - The Vigor system can choose the optimal channel from all channels except DFS channels. **Manual Select** – Select one channel or multiple channels for the Vigor system to choose the optimal channel.

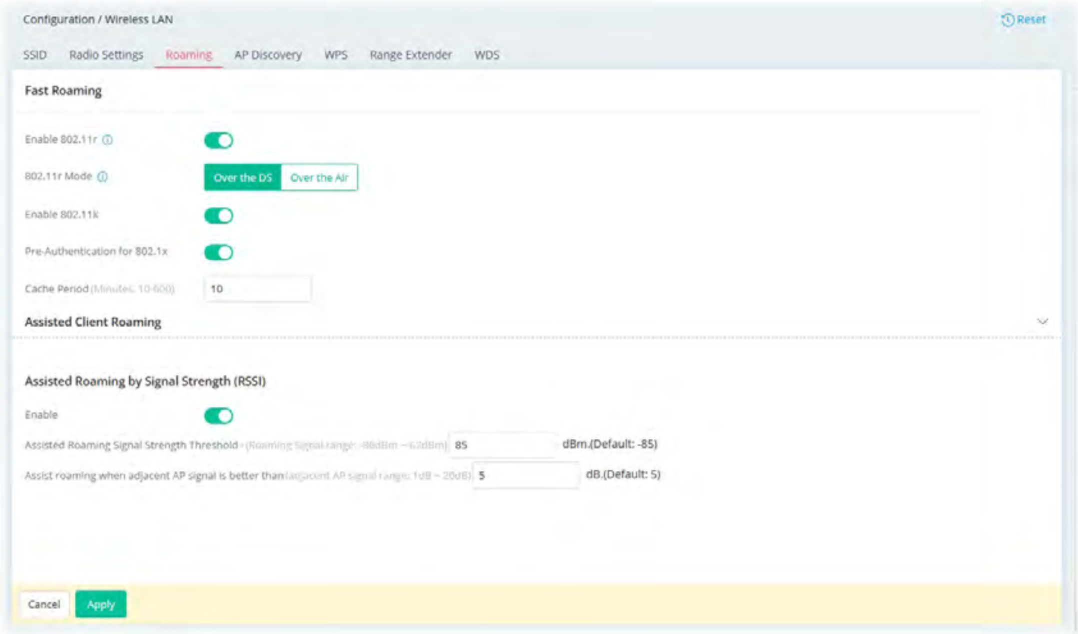
Channel Bandwidth	20 MHz- The device will use 20MHz for data transmission and receiving between the AP and the stations. 40 MHz- The device will use 40MHz for data transmission and receiving between the AP and the stations. It is for wireless LAN 2.4GHz only. 80 MHz- The device will use 80MHz for data transmission and receiving between the AP and the stations. 160 MHz- The device will use 160MHz for data transmission and receiving between the AP and the stations.
Current Channel	Displays current channel number.
Update Channel	Scan and Update - Click to scan current channel used.
Updated Channel Result	Displays current channel used.  Update Channel: Scan and Update Note: Execute a one-time channel optimization for this AP. Updated Channel Result: New Channel: 9
Band Steering Settings	
5Ghz Client Minimum RSSI	If it is enabled, VigorAP will detect if the wireless client is capable of dual-band or not within the time limit. The wireless station has the capability of a 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, VigorAP will allow the client to connect to the 2.4GHz network.
Below shows more settings if the Advance Mode is ON	
TX/RX Stream	Configure the number of antenna for transmission and reception.
Fragment Length	Sets the Fragment threshold of wireless radio. Do not modify the default value if you don’t know what it is. The default value is 2346.
RTS Threshold	Minimize the collision (unit is bytes) between hidden stations to improve wireless performance. Set the RTS threshold of wireless radio. Do not modify the default value if you don’t know what it is. The 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, the wireless station will be warned and is unable to make a network connection. Therefore, changing the country code to ensure a successful network connection will be necessary for some clients.
WMM Capable	To apply WMM parameters for wireless data transmission, switch the toggle to enable the function.
APSD Capable	APSD (Automatic Power-Save Delivery) is an enhancement over the power-saving mechanisms supported by Wi-Fi networks. It allows access points to buffer traffic before transmitting it to wireless devices, thus allowing wireless devices to enter into power saving mode which reduces power consumption. Not all wireless clients support APSD properly, and the only way to find out

	if APSD is appropriate for your network is to experiment.
Airtime Fairness	Try to assign similar airtime to each wireless station by controlling TX traffic. Switch the toggle to enable the function.
WiFi HW Acceleration	Disable this option to turn off WiFi HW NAT and IGMP Snooping. (Recommended if some websites or images fail to load)
Cancel	Discard the settings and return to the previous page.
Apply	Click it to save and apply the settings.

II-1-3-3 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.



Fast Roaming

Enable 802.11r: on

802.11r Mode: Over the DS | Over the Air

Enable 802.11k: on

Pre-Authentication for 802.1x: on

Cache Period (Minutes: 10-600): 10

Assisted Client Roaming

Assisted Roaming by Signal Strength (RSSI)

Enable: on

Assisted Roaming Signal Strength Threshold - (Roaming Signal range: -88dBm ~ -62dBm): 85 dBm.(Default: -85)

Assist roaming when adjacent AP signal is better than(adjacent AP signal range: 1dB ~ 20dB): 5 dB.(Default: 5)

Available settings are explained as follows:

Item	Description
	Fast Roaming
Enable 802.11r	Enable 802.11r - Switch the toggle to enable the 802.11r protocol(also known as Fast Basic Service Set (BSS) Transition. If enabled, the access point will improve the roaming experience for the wireless clients.
802.11r Mode	Over the DS - Transmit the handshake messages between the client and the new AP using the distribution system. In response to signal strength change, the client can communicate with the other AP through the original AP with Action Frames (FT Request and FT Response).

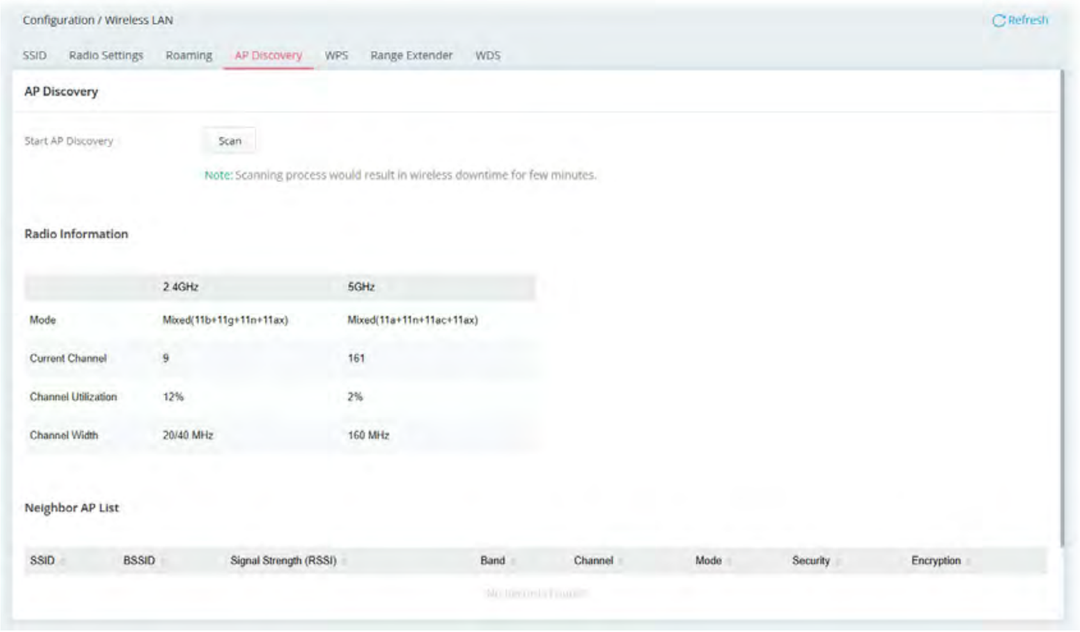
	Over the Air - Transmits the messages directly over the wireless network. In response to the needs of signal strength change, the client can communicate directly with the other AP using a fast roaming authentication algorithm (without requiring reauthentication at every AP). Note that both APs must ping each other via DS (Distribution System) / WDS.
Enable 802.11k	Switch the toggle to enable the 802.11k protocol (also know as Radio Resource Management (RRM)). If enabled, the access point will optimize the performance of wireless networks.
Pre-Authentication for 802.1x	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) Switch the toggle to enable/disable 802.11x Pre-Authentication. Enable - Enable IEEE 802.1X Pre-Authentication. Disable - Disable IEEE 802.1X Pre-Authentication.
Cache Period	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.
Assisted Client Roaming	
Assisted Roaming by Signal Strength	When the link rate of wireless station is too low or the signal received by the wireless station is too worse, VigorAP 805 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. Enable – Enable the function. Assisted Roaming Signal Strength Threshold – 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 Assist roaming when adjacent AP signal is better than) is detected by VigorAP 805, VigorAP 805 will terminate the network connection for that wireless station. Later, the wireless station can connect to the adjacent AP (with better RSSI). Assist roaming when adjacent AP signal is better than - Specify a value as a threshold.
Cancel	Discard the settings and return to the previous page.
Apply	Click it to save and apply the settings.

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

II-1-3-4 AP Discovery

VigorAP 805 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.



AP Discovery

Start AP Discovery

Note: Scanning process would result in wireless downtime for few minutes.

Radio Information

	2.4GHz	5GHz
Mode	Mixed(11b+11g+11n+11ax)	Mixed(11a+11n+11ac+11ax)
Current Channel	9	161
Channel Utilization	12%	2%
Channel Width	20/40 MHz	160 MHz

Neighbor AP List

SSID	BSSID	Signal Strength (RSSI)	Band	Channel	Mode	Security	Encryption

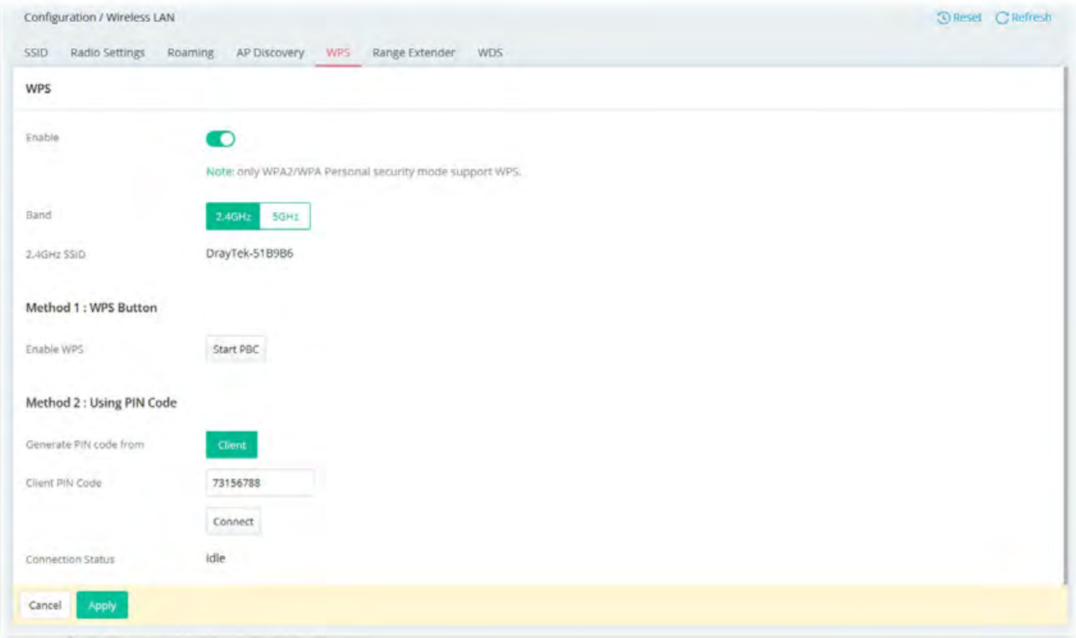
No item(s) Found

Each item is explained as follows:

Item	Description
Start AP Discovery	**Scan** - Discover all the connected AP. The results will be shown on the box above this button
	Radio Information
Mode, Current Channel, Channel Utilization, Channel Width	A table lists the radio information for this VigorAP 805.
	Neighbor AP List
SSID	Displays the SSID of the AP scanned by VigorAP 805.
BSSID	Displays the MAC address of the AP scanned by VigorAP 805.
Signal Strength (RSSI)	Displays the signal strength of the access point. RSSI is the abbreviation of Received Signal Strength Indication.
Band	Displays the wireless band(2.4GHz/5GHz) used by the AP.
Channel	Displays the wireless channel used for the AP that is scanned by VigorAP 805.
Mode	Displays the physical mode used by the scanned AP.
Security	Displays the security mode used by the scanned AP.
Encryption	Displays encryption mode (None, WEP, TKIP, AES, etc.) of AP.

II-1-3-5 WPS

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



WPS

Enable: ●

Note: only WPA2/WPA Personal security mode support WPS.

Band: [✓ 2.4GHz] 5GHz

2.4GHz SSID: DrayTek-51B9B6

Method 1 : WPS Button

Enable WPS: Start PBC

Method 2 : Using PIN Code

Generate PIN code from: [✓ Client]

Client PIN Code: 73156788

Connection Status: idle

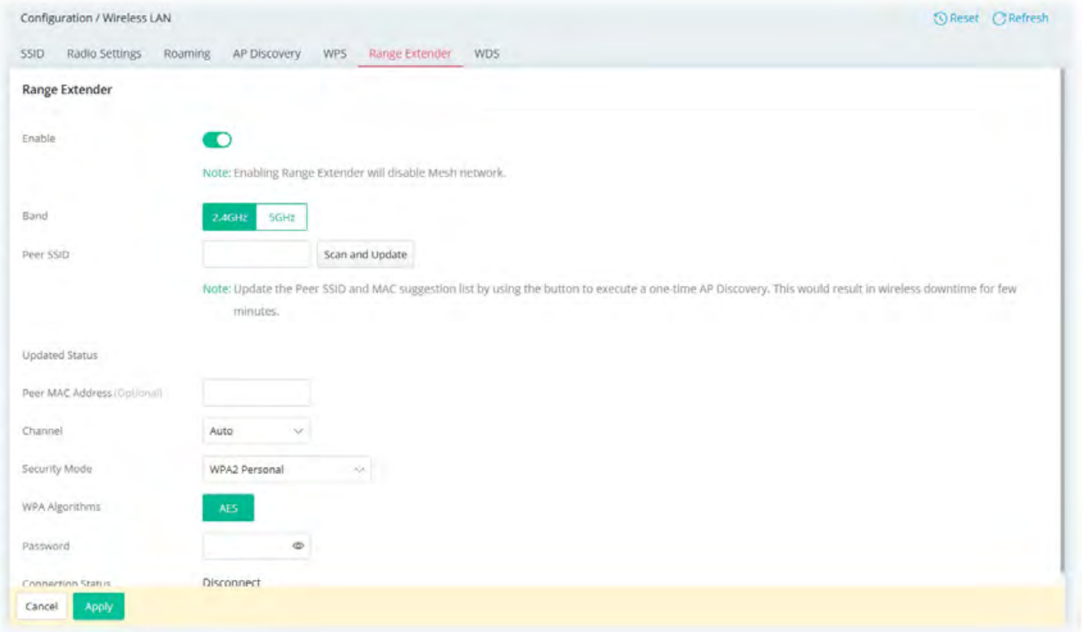
Available settings are explained as follows:

Item	Description
Enable	Switch the toggle to enable/disable the WPS setting.
Band	Specify which wireless band (2.4G/5G) will be used for this connection mode. ● 2.4GHz ● 5GHz
2.4GHz/5GHz SSID	Displays the SSID setting for 2.4GHz/5GHz.
Method 1: WPS Button	
Enable WPS	Click **Start PBC** to invoke Push-Button style WPS setup procedure. VigorAP 805 will wait for WPS requests from wireless clients about two minutes.
Method 2: Using PIN Code	
Generate PIN code from	**Client** - Use wireless client's PIN code to securely connect it to the Wi-Fi network.
Client PIN Code	Enter a number as the PIN code from the wireless client.
Connect	Click to build WPS connection between this AP and another station.
Apply	Click it to save and apply the settings.
Cancel	Discard the settings.

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

II-1-3-6 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 the Station function to connect to a Root AP and use the AP function to service all wireless clients within its coverage.



Range Extender

Enable: on

Note: Enabling Range Extender will disable Mesh network.

Band: 2.4GHz | 5GHz

Peer SSID

Note: Update the Peer SSID and MAC suggestion list by using the button to execute a one-time AP Discovery. This would result in wireless downtime for few minutes.

Updated Status

Peer MAC Address (Optional)

Channel: Auto

Security Mode: WPA2 Personal

WPA Algorithms: AES

Password

Connection Status: Disconnect

Available settings are explained as follows:

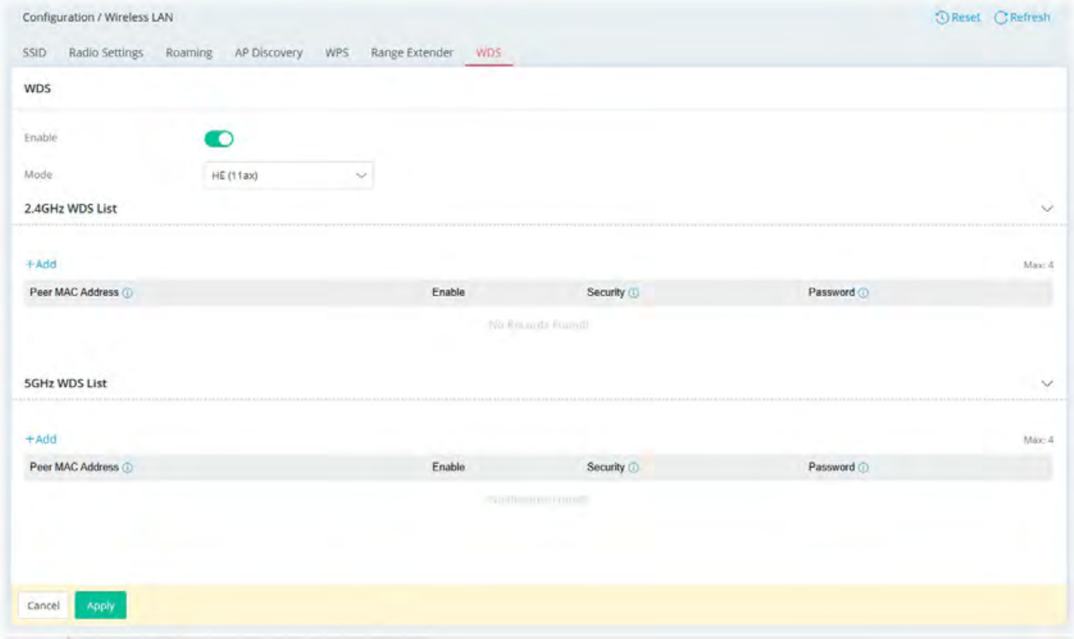
Item	Description
Enable	Switch the toggle to enable/disable the Range Extender setting.
Band	Specify which wireless band (2.4G/5G) will be used for this connection mode. ● 2.4GHz ● 5GHz
Peer SSID	Enter the SSID of the access point that VigorAP 805 wants to connect to. **Scan and Update** - Scan the peer SSID and connect to it again.
Update Status	
Peer MAC Address (Optional)	Enter the MAC address of the access point that VigorAP 805 wants to connect to.
Channel	Means the channel of frequency of the wireless LAN. You may switch the channel if the selected channel is under serious interference. At present, only **Auto** is available for selection which lets the system determine for you.
Security Mode	There are several modes provided for you to choose from. Each mode will bring up different parameters for you to configure. ● WPA3 Personal ● WPA2 Personal ● OPEN
WPA Algorithm	This option is available when WPA3 Personal or WPA2 Personal is

	selected as **Security Mode**. At present, only **AES** is available for selection.
Password	This option is available when WPA3 Personal or WPA2 Personal is selected as **Security Mode**. Enter **8~63** ASCII characters, such as "012345678".
Connection Status	Displays current connection status.
Cancel	Discard the settings.
Apply	Click it to save and apply the settings.

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

II-1-3-7 WDS

Wireless Distribution System (WDS) is a protocol for linking access points (AP) wirelessly.



Configuration / Wireless LAN

WDS

Enable: ●

Mode: HE (11ax)

2.4GHz WDS List

+Add Max: 4

Peer MAC Address ⓘ	Enable	Security ⓘ	Password ⓘ
No Records Found!			

5GHz WDS List

+Add Max: 4

Peer MAC Address ⓘ	Enable	Security ⓘ	Password ⓘ
No Records Found!			

Available settings are explained as follows:

Item	Description
Enable	Switch the toggle to enable/disable the WDS setting.
Mode	Select the physical mode for this WDS setting. ● HE(11ax) ● VHT(11ac) ● HTMIX(11n)
2.4GHz WDS List	
+Add	Creates a new WDS entry for wireless band 2.4GHz.
Peer MAC Address	Displays the peer MAC addresses Enter the peer MAC addresses in these fields. Up to four peer MAC addresses may be entered in this page. Select the checkbox in front of a MAC address to enable it.
Enable	Switch the toggle to enable/disable this setting.

Security	Displays the security type.
Password	Displays the password for TKIP/AES mode.
5GHz WDS List	
+Add	Creates a new WDS entry for wireless band 5GHz.
Peer MAC Address	Displays the peer MAC addresses Enter the peer MAC addresses in these fields. Up to four peer MAC addresses may be entered in this page.
Enable	Switch the toggle to enable/disable this setting.
Security	Displays the security type.
Password	Displays the password for TKIP/AES mode.
Cancel	Discard the settings.
Apply	Click it to save and apply the settings.

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

II-1-4 Objects

Vigor router system provides the object functions.

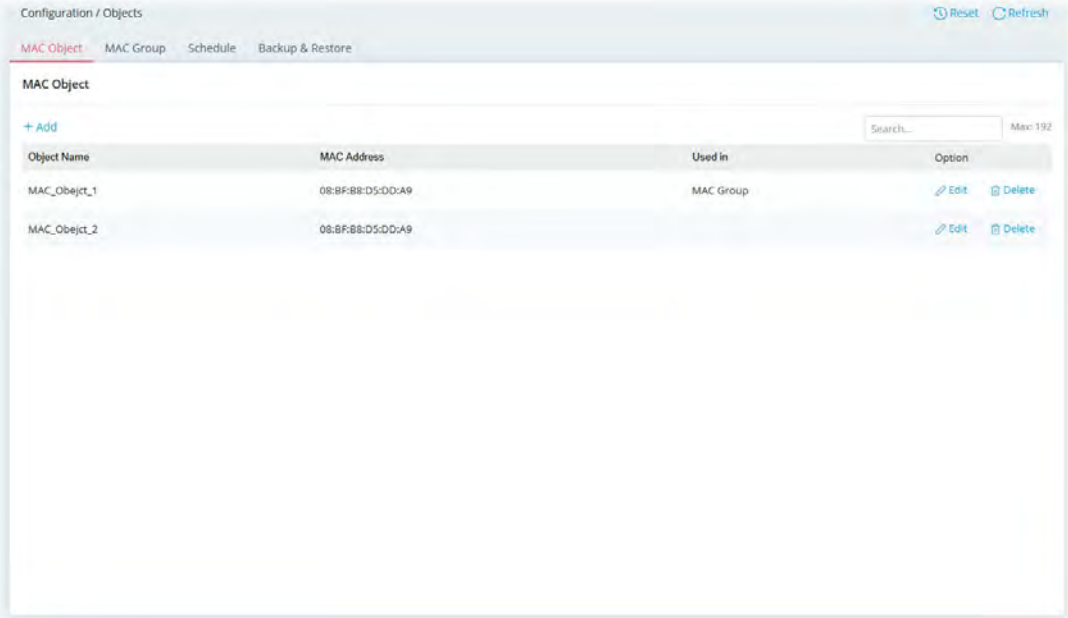
Users can define various types of objects and groups, and then apply them at various scenarios.

The advantage is that the user doesn't have to set data repetitively and it significantly enhances efficiency.

Currently, the objects that can be preset include MAC object, MAC group and Schedule.

II-1-4-1 MAC Object

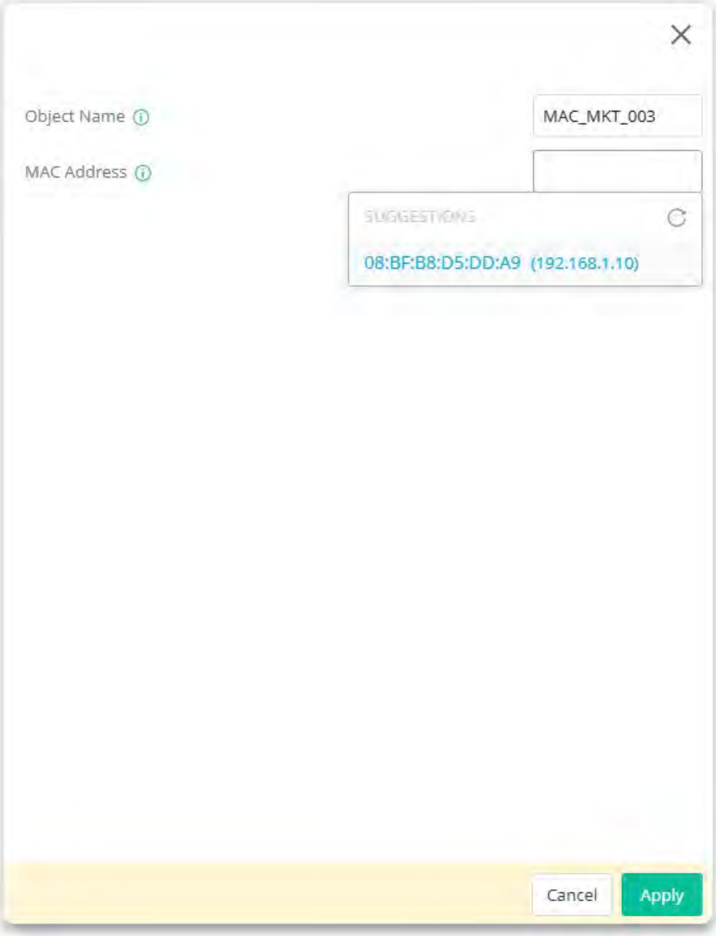
The MAC address of local or remote clients can be specified in the MAC Object page.



MAC Object

Object Name	MAC Address	Used in	Option
MAC_Obejct_1	08:BF:B8:D5:DD:A9	MAC Group	Edit Delete
MAC_Obejct_2	08:BF:B8:D5:DD:A9		Edit Delete

To add a new profile, click the **+Add** link to get the following page.



Object Name: MAC_MKT_003

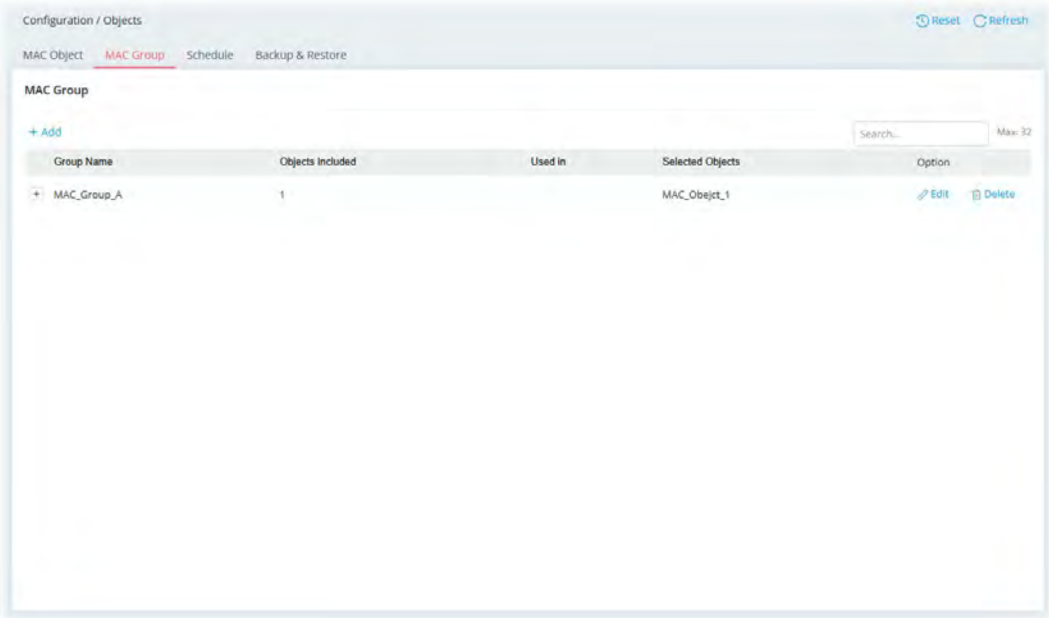
Available settings are explained as follows:

Item	Description
Object Name	Enter a name that identifies this object.
MAC Address	Enter the MAC address of the client.
Cancel	Discard the settings.
Apply	Click it to save the settings.

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

II-1-4-2 MAC Group

Multiple **MAC Objects** can be placed into a **MAC Group**.



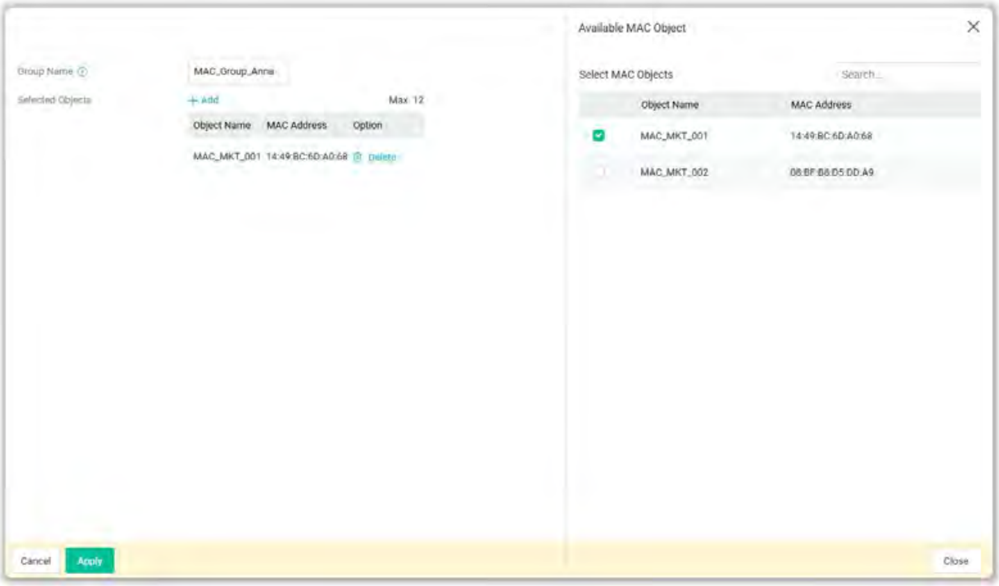
Configuration / Objects

MAC Group

Max: 32

	Group Name	Objects Included	Used in	Selected Objects	Option
+	MAC_Group_A	1		MAC_Obejct_1	Edit Delete

To add a new profile, click the **+Add** link to get the following page.



Group Name: MAC_Group_Anna

Selected Objects: + Add Max 12

Object Name	MAC Address	Option
MAC_MKT_001	14:49:BC:6D:A0:68	Delete

Available MAC Object

Select MAC Objects

	Object Name	MAC Address
☑	MAC_MKT_001	14:49:BC:6D:A0:68
□	MAC_MKT_002	08:BF:B8:D5:DD:A9

Available settings are explained as follows:

Item	Description
Group Name	Enter a name that identifies this profile.
Selected Objects	**+Add** - Click to open the page with available objects.
	Available MAC Object
Selected Objects	**Search** - Enter the MAC object name to display existed MAC objects.
Object Name	Select the object(s) to be grouped under the current MAC group. The selected one will be shown under the Selected Objects on the

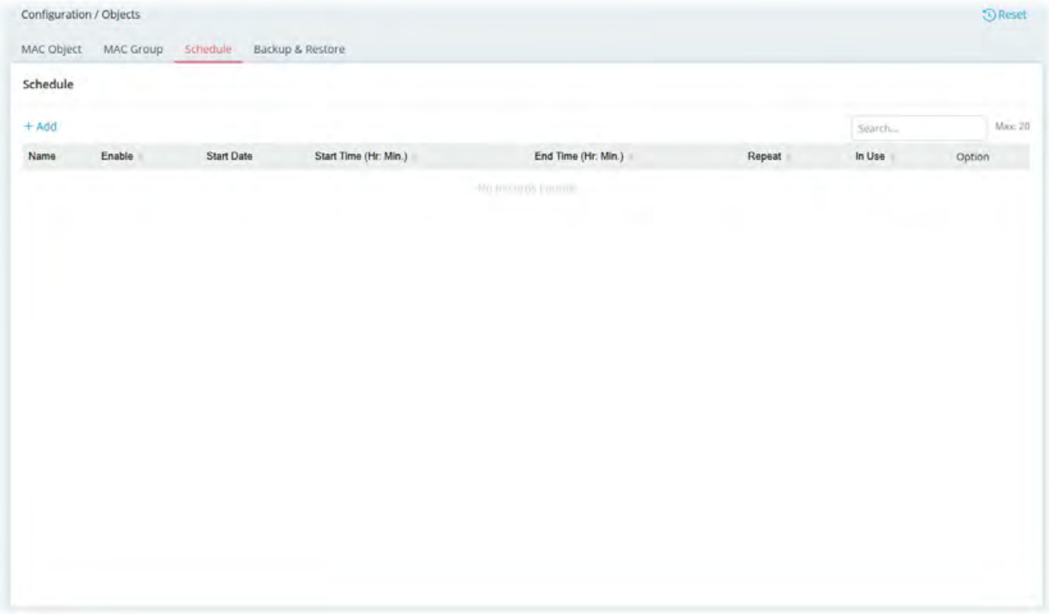
	left side.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

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

II-1-4-3 Schedule

This page allows you to set schedule profiles that can be used for the VigorAP to dial up to the Internet at a specified time. It is especially useful for each WLAN SSID to access the Internet network at different time periods by assigning different schedule profiles.

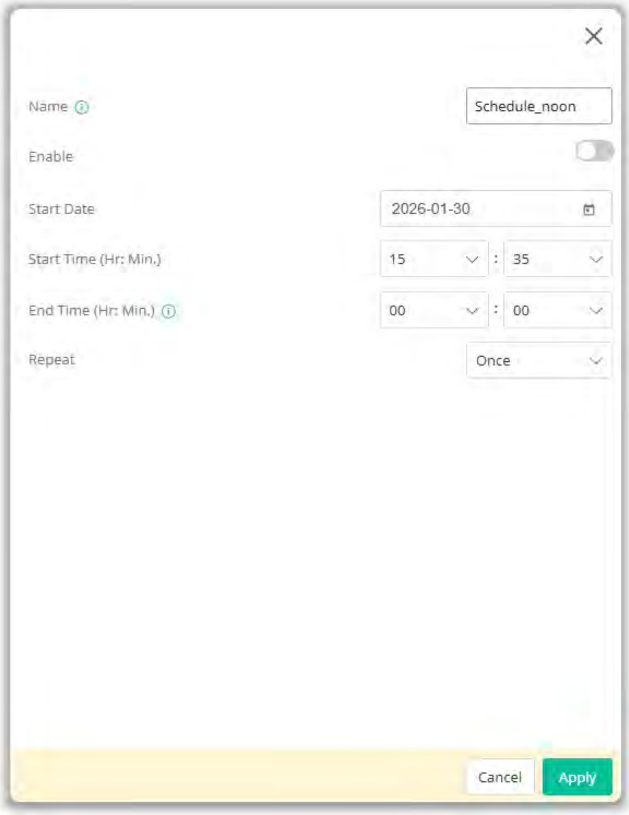
The schedule is also applicable to other functions.



Name	Enable	Start Date	Start Time (Hr: Min.)	End Time (Hr: Min.)	Repeat	In Use	Option

No records found

To add a new schedule profile, click the +Add link to get the following page.



Name ⓘ Schedule_noon

Enable

Start Date 2026-01-30

Start Time (Hr: Min.) 15 : 35

End Time (Hr: Min.) ⓘ 00 : 00

Repeat Once

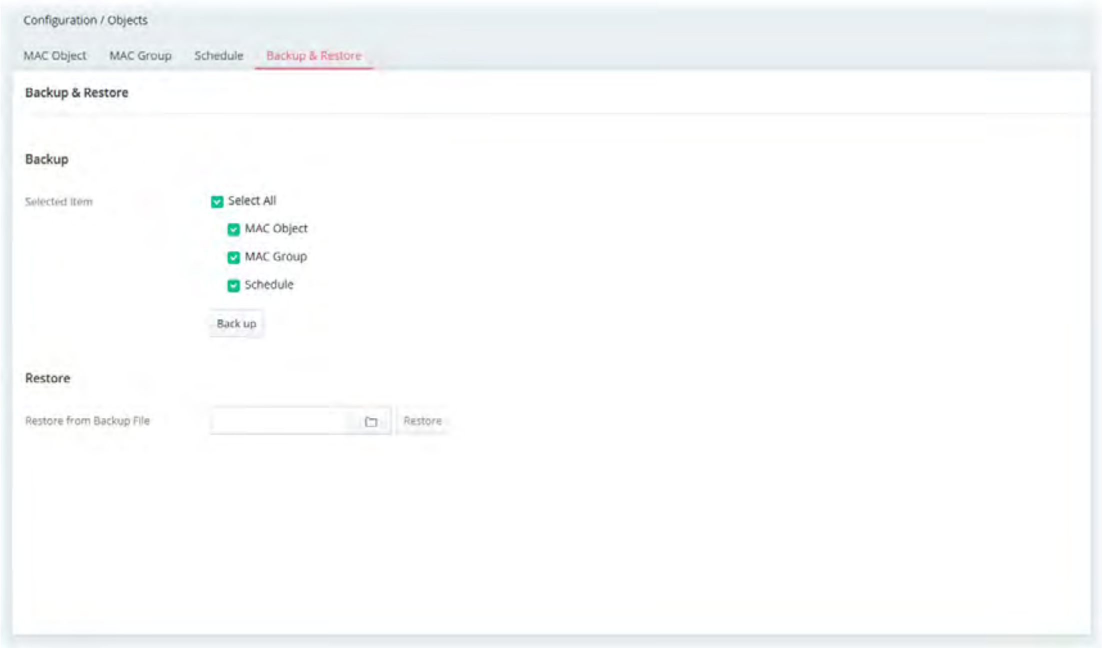
Available settings are explained as follows:

Item	Description
Name	Enter the name of the schedule profile.
Enable	Switch the toggle to enable/disable the schedule profile.
Start Date	Specify the starting date of the schedule.
Start Time (Hr:Min.)	Specify the starting time of the schedule.
End Time (Hr:Min.)	Specify the ending time of the schedule.
Repeat	Specify how often the schedule will be applied. Once - The schedule will be applied just once. Daily - The schedule will be applied every day based on the above settings. ● End Repeat - Switch the toggle to enable/disable the daily function. ● End Repeat Date - The schedule is valid until that day. Weekly - Specify which days in one week should perform the schedule. ● Every - Select the days in one week. ● End Repeat - Switch the toggle to enable/disable the daily function. ● End Repeat Date - The schedule is valid until that day. Monthly - The schedule will be applied every month. ● End Repeat - Switch the toggle to enable/disable the daily function.

	● **End Repeat Date** - The schedule is valid until that day.
Cancel	Discard the settings.
Apply	Click it to save the settings and exit the page.

II-1-4-4 Backup & Restore

The object settings can be backed up as a file. The backup file can be imported to the device to restore the configuration in the future if required.



Configuration / Objects

MAC Object MAC Group Schedule Backup & Restore

Backup & Restore

Backup

Selected Item
☑ Select All
☑ MAC Object
☑ MAC Group
☑ Schedule

Back up

Restore

Restore from Backup File 🗀 Restore

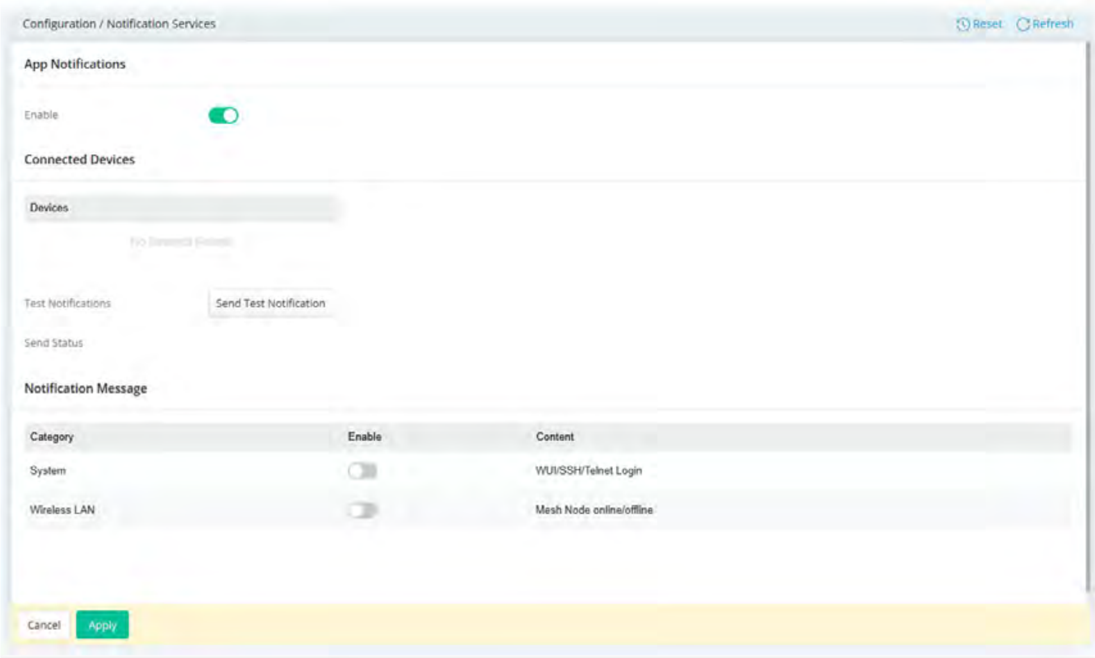
Available settings are explained as follows:

Item	Description
Backup	Usually, a user can create the objects through the web page under Objects. All the objects (or the template) can be saved and exported as a file by clicking Download. **Back up** – Click it to backup current objects to a file. Such file can be restored for future use.
Restore	**Restore from Backup File** 🗀 – Click it to specify a file backed up previously. **Restore** – Click to execute the restoration.

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

II-1-5 Notification Services

VigorAP can send messages related to the system and the wireless LAN to DrayTek Wireless APP.



Configuration / Notification Services

App Notifications

Enable ●

Connected Devices

Devices

Test Notifications: Send Test Notification

Send Status

Notification Message

Category	Enable	Content
System	○	WUI/SSH/Telnet Login
Wireless LAN	○	Mesh Node online/offline

Available settings are explained as follows:

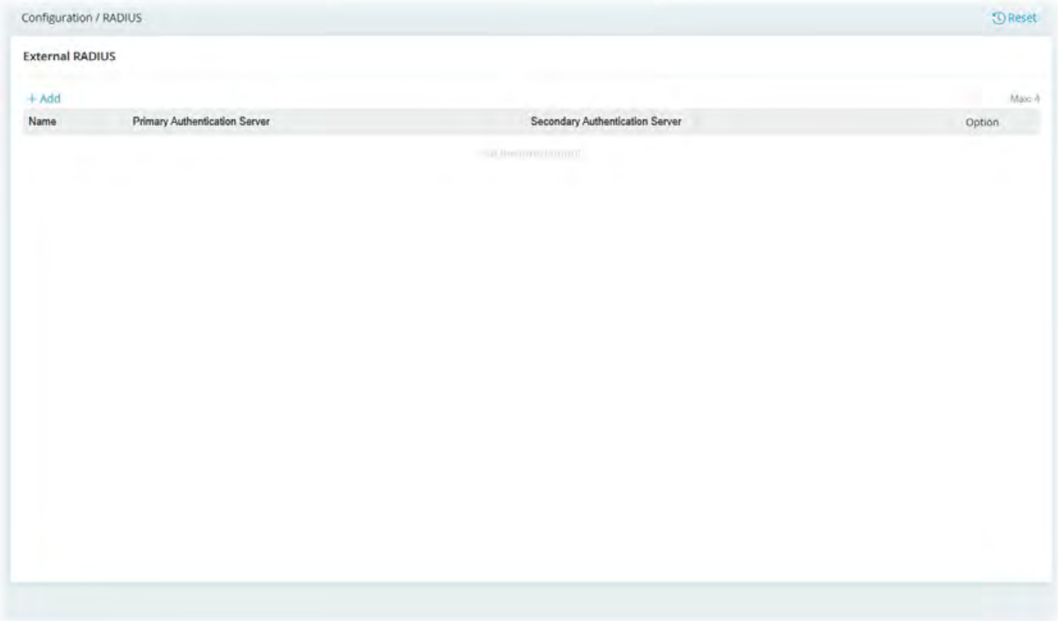
Item	Description
	App Notification
Enable	Switch the toggle to enable/disable the function of sending notification to the DrayTek Wireless APP.
	Connected Devices
Devices	Display the name (device ID) of the mobile phone(s) connected and submitted to DrayTek Wireless APP. Note that the little bell on the top-right corner of the APP must be turned on to receive the message from VigorAP 805.
Test Notifications	Send Test Notification – Press to send a message to DrayTek Wireless APP.
Send Status	Display the test result after pressing the Send Test Notification button.
	Notification Message
Category	At present, only two categories are available.
Enable	Switch the toggle to enable/disable the category.
Content	Display the detailed information for the selected category.

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

II-1-6 RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a security authentication client/server protocol that supports authentication, authorization and accounting, which is widely used by Internet service providers. It is the most common method of authenticating and authorizing dial-up and tunneled network users.

This web page is used to configure settings for external RADIUS server. Then WLAN users of VigorAP will be authenticated and accounted by such server for network application.



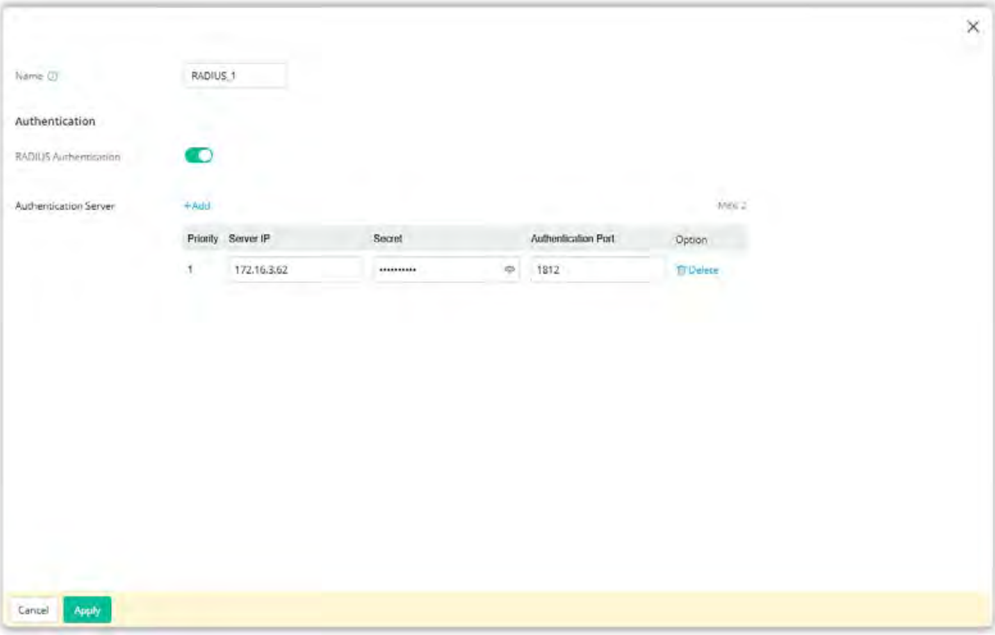
Configuration / RADIUS

External RADIUS

Name	Primary Authentication Server	Secondary Authentication Server	Option

To edit an existing profile, click the **Edit** link of the selected profile to make modifications.

To add a new profile, click the **+Add** link to get the following page.



Name: RADIUS_1

Authentication

RADIUS Authentication: ON

Authentication Server

Priority	Server IP	Secret	Authentication Port	Option
1	172.16.3.62	••••••••••	1812	Delete

Available settings are explained as follows:

Item	Description
Name	Enter the name of the server profile.
	Authentication
RADIUS Authentication	Switch the toggle to enable/disable the function.
Authentication Server	**+Add** - Click to create a new server profile. ● **Priority** - Only two external servers can be used. ● **Server IP** - Enter the IP address of the external RADIUS server. ● **Secret** - Enter the password for the user to be authenticated by VigorAP 805 while the user tries to use VigorAP 805 as the RADIUS server. ● **Authentication Port** - Enter a port number for the RADIUS server. ● **Option** - Click **Delete** to remove the selected entry.
Cancel	Discards the settings and exits the page.
Apply	Click it to save the settings and exit the page.

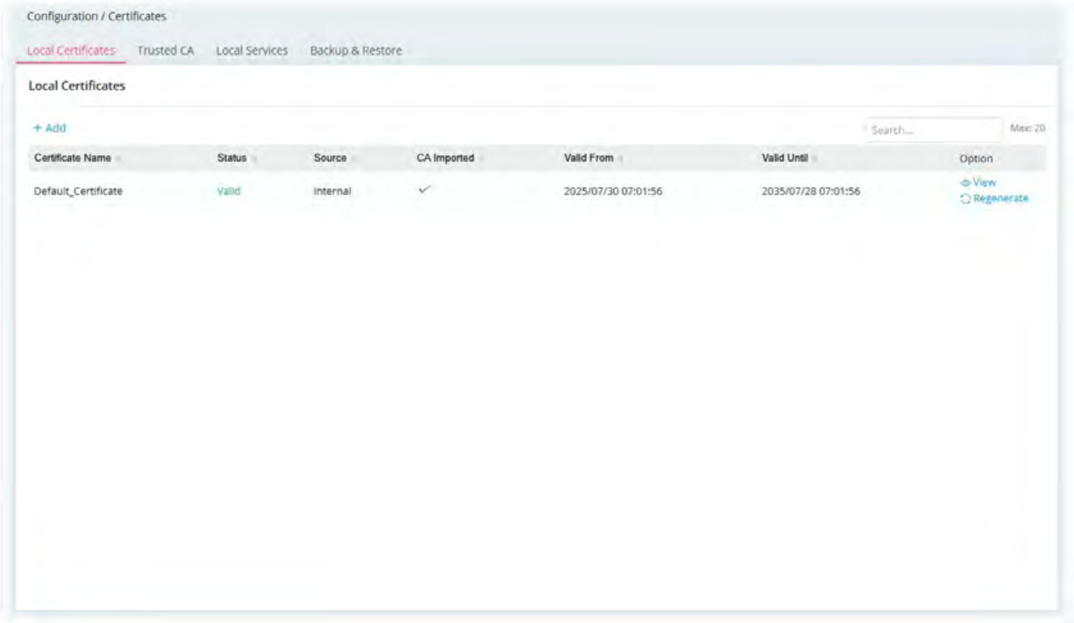
II-1-7 Certificates

A digital certificate is an electronic document issued by a certification authority (CA) to an entity to prove ownership of a public key. It contains identifying information including the issued-to party's name, a serial number, expiration dates etc., and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Vigor AP supports digital certificates that conform to the X.509 standard.

In this section, you can generate and manage local digital certificates, and import trusted CA certificates. Be sure that the system time is correct on the access point so that certificates will not be erroneously considered to be invalid because of an incorrect system time falling outside of the certificate's valid time period. The easiest way to accomplish this is by periodically synchronizing the system time to a Network Time Protocol (NTP) server.

II-1-7-1 Local Certificates

You can generate, import or view local certificates on this page.



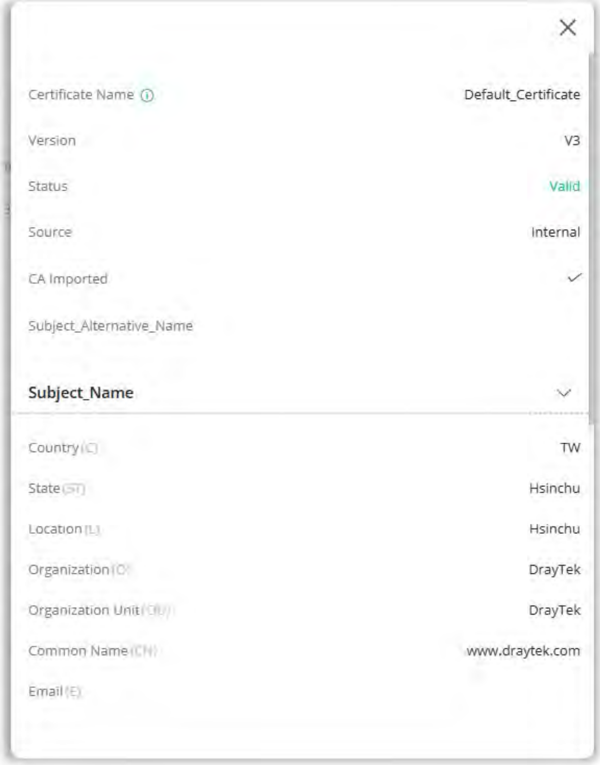
Configuration / Certificates

Local Certificates

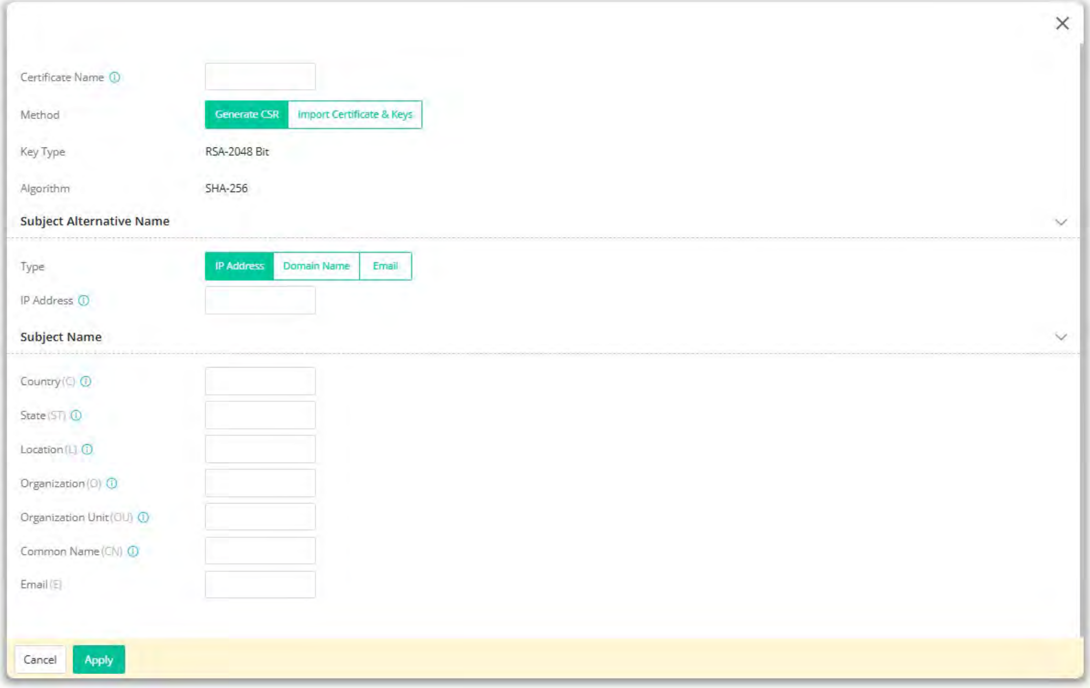
Certificate Name	Status	Source	CA Imported	Valid From	Valid Until	Option
Default_Certificate	Valid	Internal	✓	2025/07/30 07:01:56	2035/07/28 07:01:56	View Regenerate

Available settings are explained as follows:

Item	Description
+Add	Creates a new certificate.
View	Displays the content of the certificate.

	 Certificate Name: Default_Certificate Version: V3 Status: Valid Source: Internal CA Imported: ✓ Subject_Alternative_Name **Subject_Name** Country (C): TW State (ST): Hsinchu Location (L): Hsinchu Organization (O): DrayTek Organization Unit (OU): DrayTek Common Name (CN): www.draytek.com Email (E)
Regenerate	Regenerate the certificate.

To add a new local certificate profile, click the **+Add** link to get the following page.



Certificate Name ⓘ	
Method	Generate CSR / Import Certificate & Keys
Key Type	RSA-2048 Bit
Algorithm	SHA-256
Subject Alternative Name	
Type	IP Address / Domain Name / Email
IP Address ⓘ	
Subject Name	
Country (C) ⓘ	
State (ST) ⓘ	
Location (L) ⓘ	
Organization (O) ⓘ	
Organization Unit (OU) ⓘ	
Common Name (CN) ⓘ	
Email (E)	

Available settings are explained as follows:

Item	Description
Certificate Name	Enter the name that identifies the certificate.
Method	**Generate CSR -** Generate a new local certificate. **Import Certificate & Keys -** Vigor access point allows you to

	generate a certificate request and submit it the CA server, then import it as "Local Certificate". If you have already gotten a certificate from a third party, you may import it directly. The supported types are PKCS12 Certificate and Certificate with a private key.
Method - Generate CSR	
Key Type	Displays the key type used by the certificate.
Algorithm	Displays the algorithm for generating the certificate.
Type	Select the type of Subject Alternative Name and enter its value. ● IP Address ● Domain Name ● Email
Country (C)	Enter the country name (code) in which your organization is located.
State (ST)	Enter the state or province where your organization is located.
Location (L)	Enter the city where you're your organization is located.
Organization (O)	Enter the legal name of your organization.
Organization Unit (OU)	Enter the department within your organization that you wish to be associated with this certificate.
Common Name (CN)	Enter the fully-qualified domain name / WAN IP that will be used to reach your server.
Email (E)	Enter the email address of the entry.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.
Method - Import Certificate & Keys	
File Type	Vigor AP allows you to generate a certificate request and submit it the CA server, then import it as "Local Certificate". If you have already gotten a certificate from a third party, you may import it directly. The supported types are PKCS12 Certificate and Certificate with a private key. Certificate Only - Local certificate. ● Upload Certificate - Click **Choose a file** to select a local certificate file. PKCS12 - Users can import the certificate whose extensions are usually .pfx or .p12. And these certificates usually need passwords. PKCS12 is a standard for storing private keys and certificates securely. It is used in (among other things) Netscape and Microsoft Internet Explorer with their import and export options. ● Upload PKCS12 File - Click **Choose a file** to select a PKCS12 certificate file. ● Password - Enter the password associated with the certificate and key files. Certificate & Keys - It is useful when users have separated certificates and private keys. And the password is needed if the private key is encrypted. ● Upload File - Click **Choose a file** to select a local certificate file.

	- Upload Key - Click **Choose a file** to select a key file. - Password - Enter the password associated with the certificate and key files.
Cancel	Discards current settings and return to the previous page.
Apply	Save the current settings and exit the page.

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

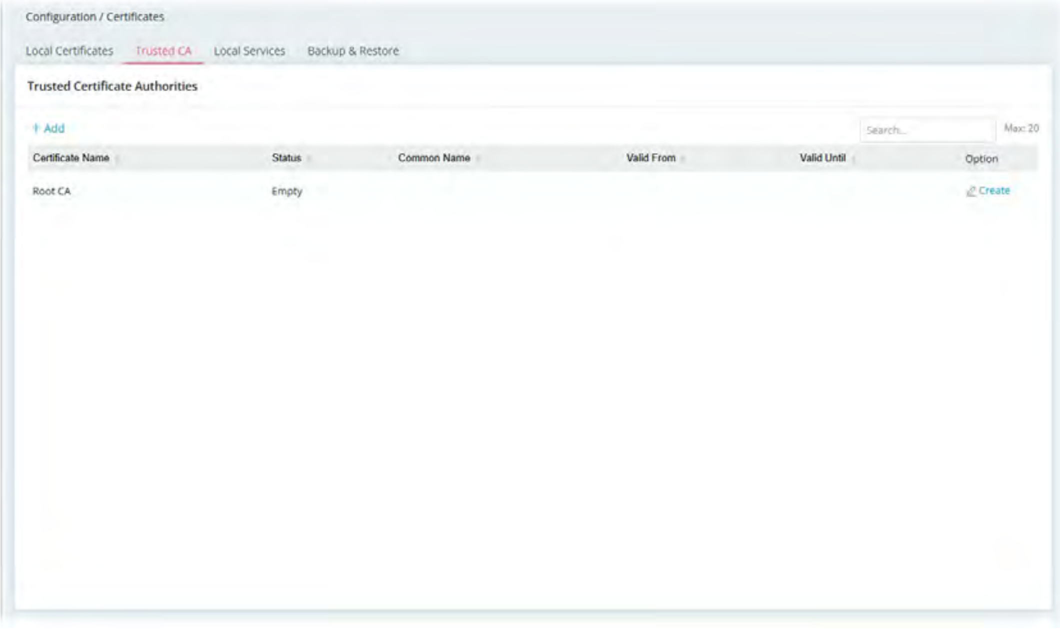
II-1-7-2 Trusted CA

The user can build RootCA certificates (up to three) if required.

When the local client and remote server are required to make certificate authentication (e.g., Radius EAP-TLS authentication) for wireless connection and avoid 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 for digital certificates from a trusted root certificate authority is complicated and time-consuming. Therefore, Vigor AP offers a mechanism that allows you to generate root CA to save time and provide convenience for general users. Later, such root CA generated by the DrayTek server can perform the issuing of the 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.



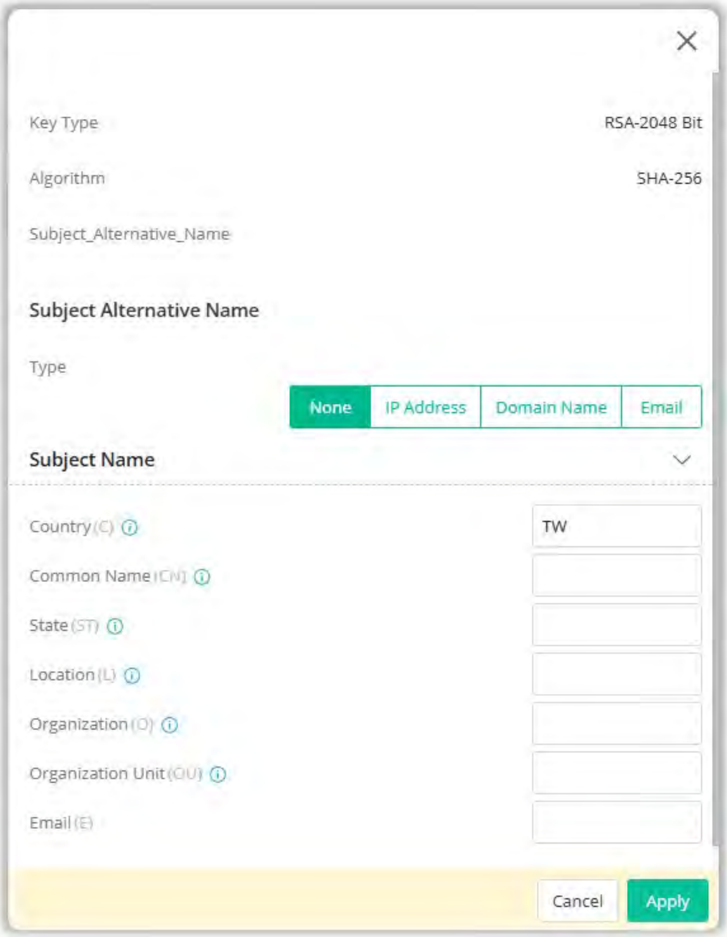
Trusted Certificate Authorities

Certificate Name	Status	Common Name	Valid From	Valid Until	Option
Root CA	Empty				Create

Available settings are explained as follows:

Item	Description
+Add	Creates a new trusted certificate.
Option	**Create** - Click to open the configuration page.

To create a new RootCA, click **Create** to get the following page.



Key Type RSA-2048 Bit

Algorithm SHA-256

Subject_Alternative_Name

Subject Alternative Name

Type

Subject Name

Country (C) TW

Common Name (CN)

State (ST)

Location (L)

Organization (O)

Organization Unit (OU)

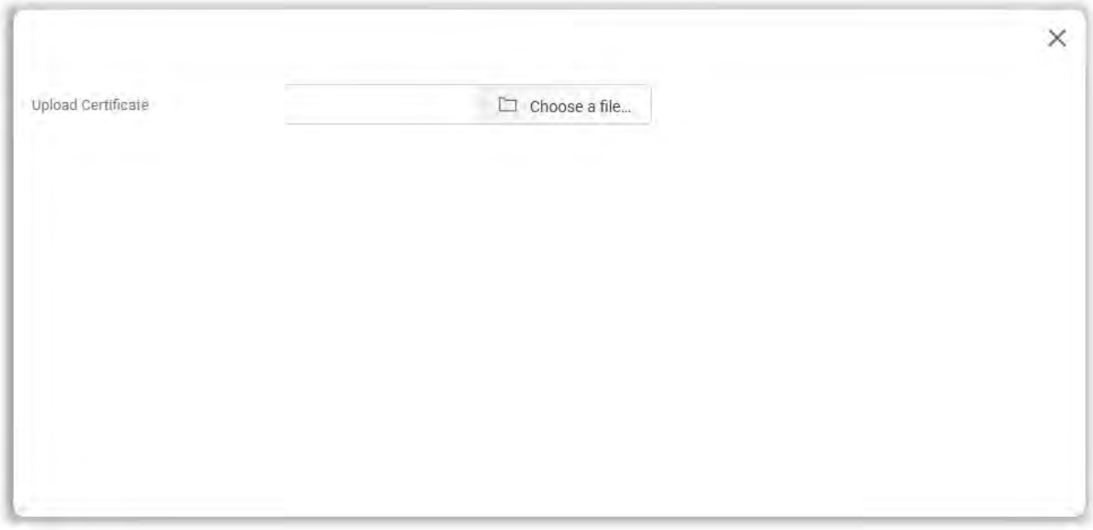
Email (E)

Available settings are explained as follows:

Item	Description
Key Type	Displays the key type (set to RSA).
Algorithm	Displays the algorithm.
	Subject Alternative Name
Type	Select the type of Subject Alternative Name and enter its value.
	Subject Name
Country (C)	Enter the country name (code) in which your organization is located.
Common Name (CN)	Enter the fully-qualified domain name / WAN IP that will be used to reach your server.
State (ST)	Enter the state or province where your organization is located.
Location (L)	Enter the city where you're your organization is located.
Organization (O)	Enter the legal name of your organization.
Organization Unit (OU)	Enter the department within your organization that you wish to be associated with this certificate.
Email (E)	Enter the email address of the entry.
Cancel	Discard current settings and return to the previous page.
Apply	Click to submit generate request to the CA server.

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

To upload a certificate, click the **+Add** link to get the following page.



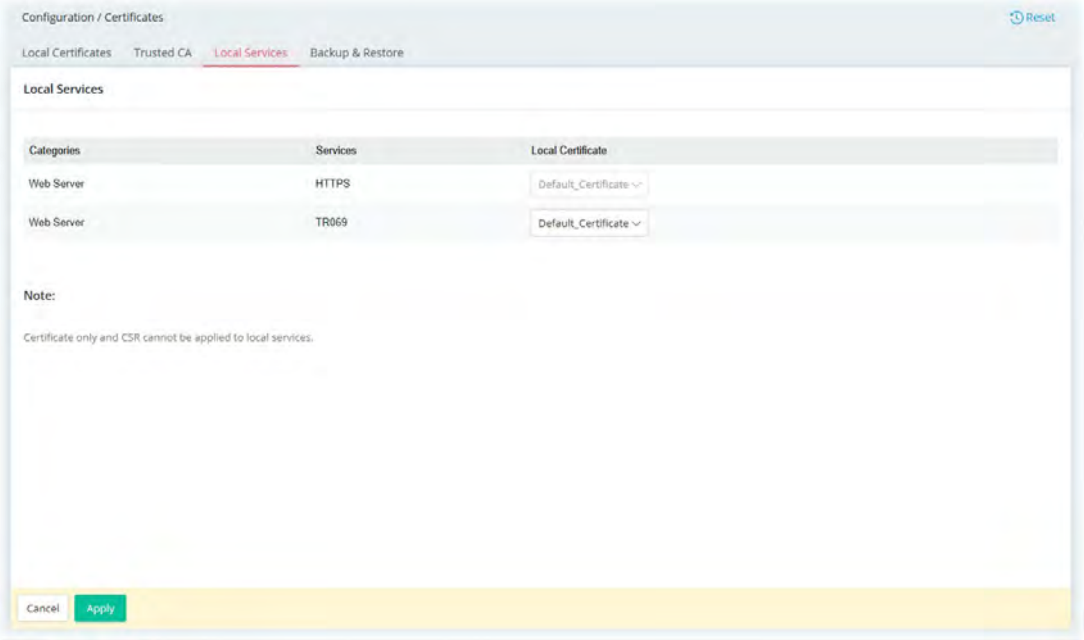
Available settings are explained as follows:

Item	Description
Upload Certificate	**Choose a file** - Select an existing certificate.
Cancel	Discards the settings and exits the page.
Apply	Click it to save the settings and exit the page.

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

II-1-7-3 Local Services

This page allows you to set different categories and services for the local certificate(s) to prevent security warning messages popped up due to using different browsers.



Local Services

Categories	Services	Local Certificate
Web Server	HTTPS	Default_Certificate
Web Server	TR069	Default_Certificate

Note:

Certificate only and CSR cannot be applied to local services.

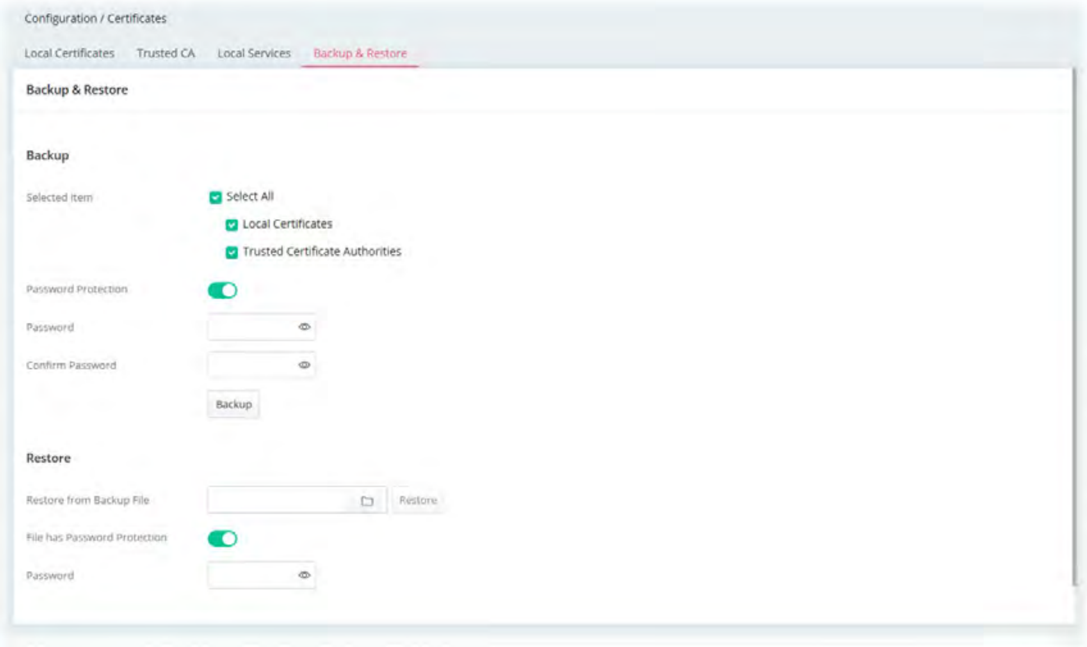
Available settings are explained as follows:

Item	Description
Local Certificate	Select a local certificate (has been imported to Vigor device) with full key and authentication information. Certificate without key phrase or CSR (certificate signing request) file cannot be selected as local certificate.
Cancel	Discards the settings and exits the page.
Apply	Click it to save the settings and exit the page.

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

II-1-7-4 Backup & Restore

You can back up or restore the Local and Trusted CA certificates on the access point to a file.



Configuration / Certificates

Local Certificates | Trusted CA | Local Services | Backup & Restore

Backup & Restore

Backup

Selected Item: ☑ Select All
☑ Local Certificates
☑ Trusted Certificate Authorities

Password Protection: ●

Password:

Confirm Password:

Backup

Restore

Restore from Backup File: Restore

File has Password Protection: ●

Password:

Available settings are explained as follows:

Item	Description
Backup	
Selected Item	● Select All ● Local Certificates ● Trusted Certificate Authorities
Password Protection	Switch the toggle to enable or disable the function. ● **Password** - Enter the password with which you wish to encrypt the certificate. ● **Confirm Password** - Enter the password again. **Backup** - Click to download the certificate.
Restore	
Restore from Backup File	Click to select the backup file you wish to restore. **Restore** - Click to retrieve the certificate.
File has Password Protection	Switch the toggle to enable or disable the function. If enabled, set the password. **Password** - Enter the password that was used to encrypt the certificates.

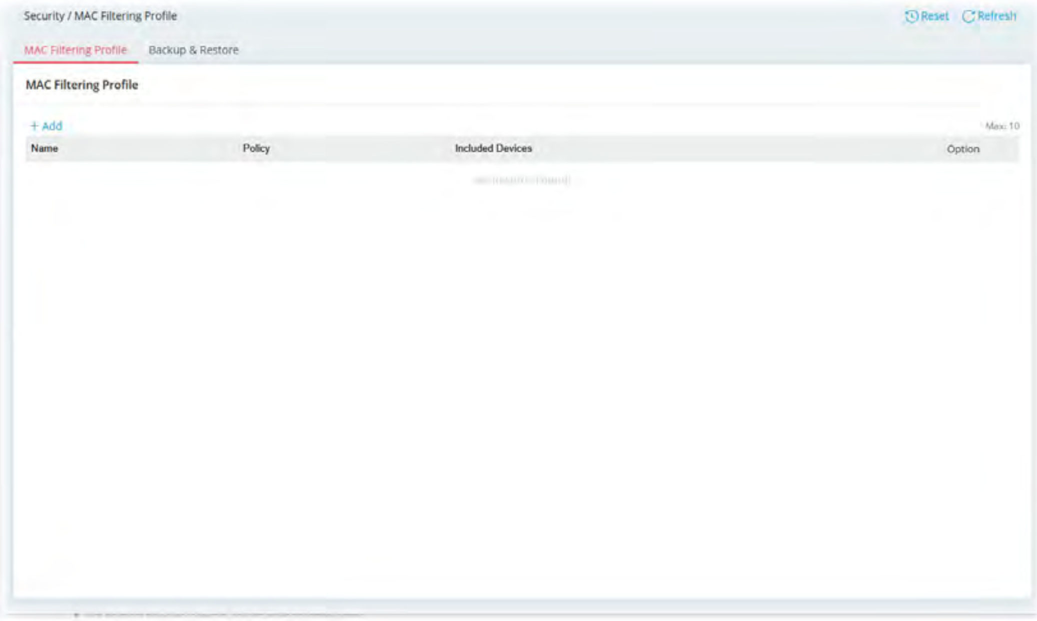
II-2 Security

II-2-1 MAC Filtering Profile

Vigor router may restrict wireless access to specified wireless clients only by referencing a MAC address black/white list.

The router's administrator may block wireless clients by inserting their MAC addresses into a black list, or only allow some wireless clients to connect by inserting their MAC addresses into a white list.

This page allows to set the MAC Filtering Profiles (up to 10) that will be applied to SSID (configured on Configuration>>Wireless LAN>>SSID) to meet different needs.



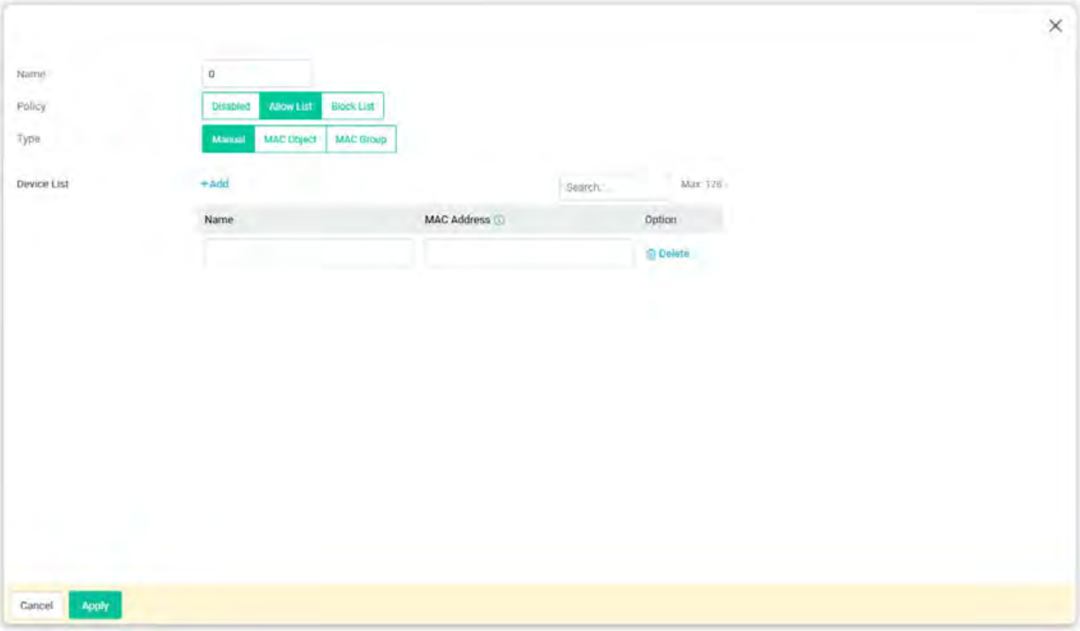
MAC Filtering Profile

Name	Policy	Included Devices	Option

Available settings are explained as follows:

Item	Description
+Add	Click to create a new entry.
Edit	Click to modify the selected entry.
Delete	Click to remove the selected entry.

To add a new MAC filtering profile, click the **+Add** link to get the following page.



Name 0

Policy Disabled [✓ Allow List] Block List

Type [✓ Manual] MAC Object MAC Group

Device List +Add Search... Max: 128

Name	MAC Address	Option
		Delete

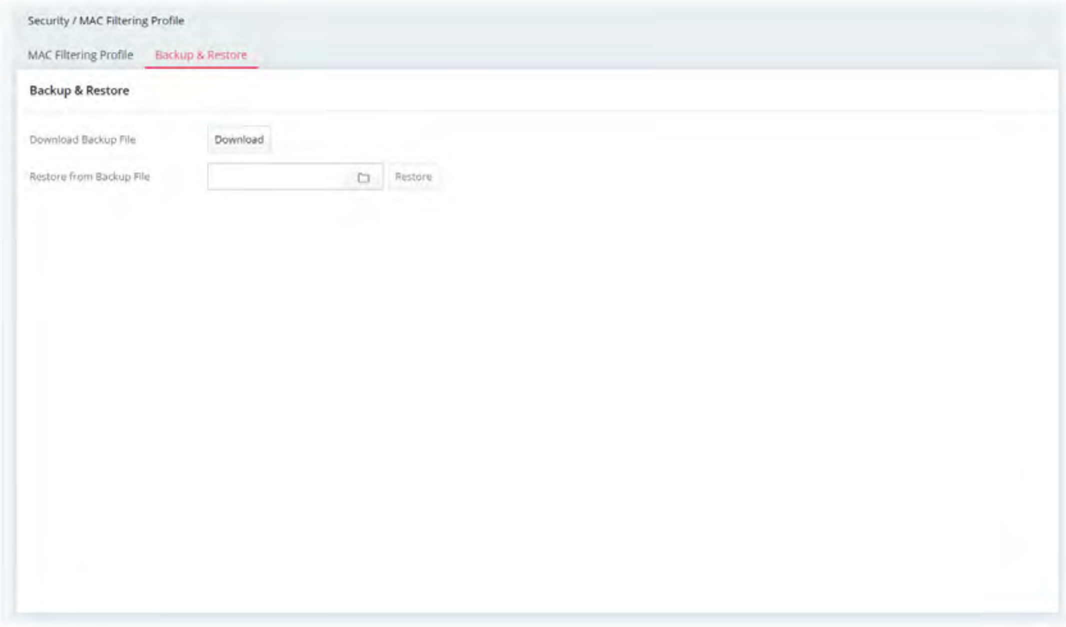
Available settings are explained as follows:

Item	Description
Name	Enter the name of the profile.
Policy	**Disabled** – Disable this policy. **Allow List** – Only allow wireless clients whose MAC addresses are listed in the Device list. **Block List** - Only allow wireless clients whose MAC addresses are not listed in the Device list.
Type	Determine which wireless clients can be applied to SSID. **Manual** – Enter the MAC address of certain device one by one. **MAC Object** – Select the MAC object(s). All the MAC address under the MAC object will be allowed or blocked. **MAC Group** – Select the MAC group(s).
Device List	**+Add** – Click to add a new device by entering the device name and the MAC address.
Cancel	Discard the settings.
Apply	Click it to save the settings and exit the page.

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

II-2-2 Backup & Restore

This page allows you to save the access control policies and black & white lists as a profile, which can be used for restoration purposes.



Available settings are explained as follows:

Item	Description
Download Backup File	Download - Click to save the MAC filtering profile.
Restore from Backup File	🗀 - Click to locate the file for restoring. Restore – Click to execute the restoration.

II-3 Virtual Controller - Wireless

This feature allows users to establish and manage a network of DrayTek devices connected by Wireless or Wired links.

The network consists of one Root and multiple Nodes. Root controls this network and syncs configurations to Nodes. Normally Root and Nodes use the same Wireless SSID/security, and Wireless clients can connect to any of them.

For Mesh networks, Root is also the outlet to the Internet. All devices of a network are in the same Group. The root can add a new Node to its Group or delete members from its Group. Users can choose VigorMesh or EasyMesh to establish the Mesh network. If Mesh is disabled, a network with wired links alone could still be established as long as AP Management is enabled.

Mesh Root and Mesh Node

Mesh Root indicates that this device would be another device's uplink connection.

As a Mesh Root, the device must connect to a gateway with an Ethernet cable first to have an Internet connection.

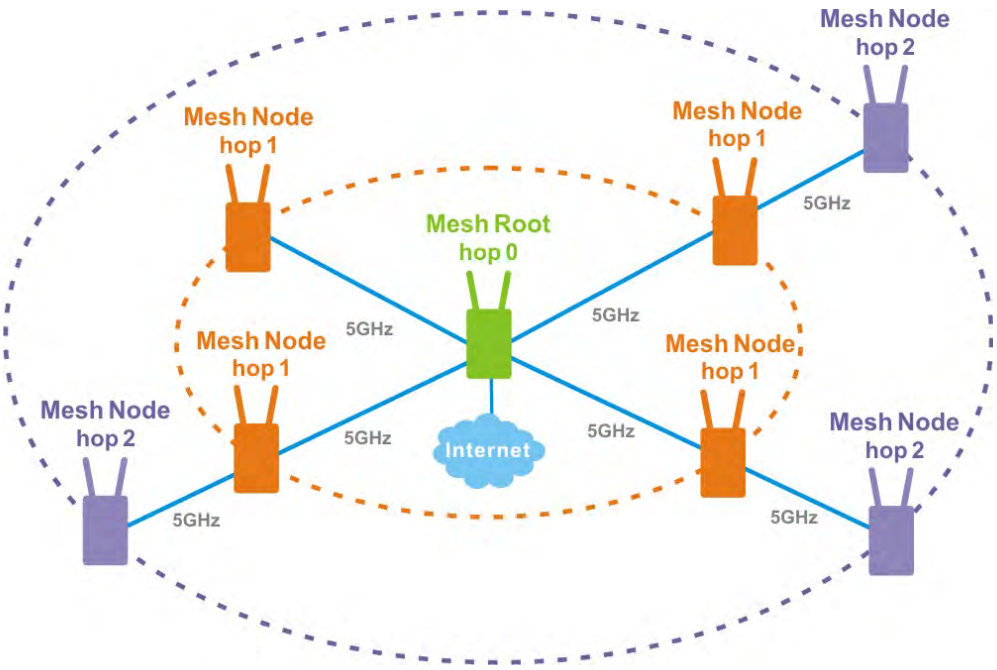
As a Mesh Node, the device can connect to the Mesh Root or Mesh Node within the same Mesh Group via Wireless or Wired links.

VigorMesh

VigorMesh is a DrayTek proprietary Mesh function.
Pleae note that, within VigorMesh network,

- The total number allowed for Group members is 8 (including the Mesh Root).
- The maximum number of hop is 3.

Refer to the following figure:

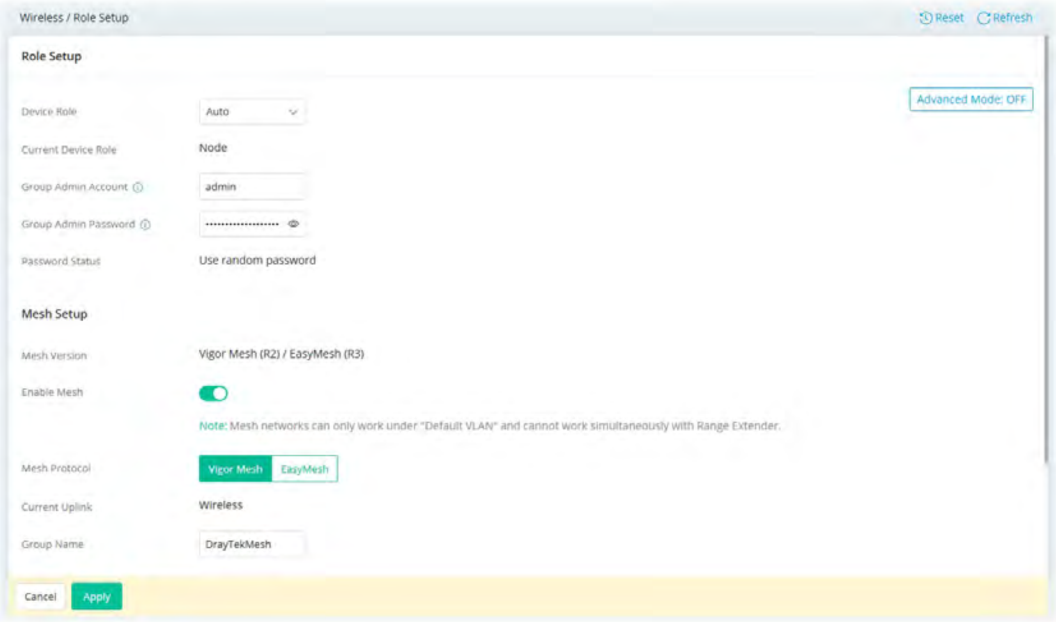


EasyMesh

EasyMesh is a standard Mesh protocol of Wi-Fi Alliance.

II-3-1 Role Setup

This page can determine the role of the VigorAP connecting to the computer physically. And set up its Mesh function and AP Management function.



Wireless / Role Setup

Reset Refresh

Role Setup

Advanced Mode: OFF

Device Role: Auto

Current Device Role: Node

Group Admin Account: admin

Group Admin Password: ••••••••••••••••••••

Password Status: Use random password

Mesh Setup

Mesh Version: Vigor Mesh (R2) / EasyMesh (R3)

Enable Mesh: ●

Note: Mesh networks can only work under "Default VLAN" and cannot work simultaneously with Range Extender.

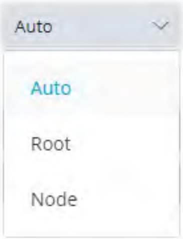
Mesh Protocol: Vigor Mesh | EasyMesh

Current Uplink: Wireless

Group Name: DrayTekMesh

Cancel Apply

Available settings are explained as follows:

Item	Description
	Role Setup
Device Role	**Auto** - The device can switch between a Root and a Node based on the actual situation. **Root** – The device is a Root. It controls the network and syncs configurations to the Nodes of its Group. If Mesh is enabled, the device must connect to a gateway with an Ethernet cable to have an Internet connection. **Node** – The device is a Node. It is managed by a Root if it has joined a Group. If Mesh is enabled, the device can connect to the network through wireless. 
Current Device Role	Displays the current role of the device.
Group Admin Account	Set an account for the system administrator to manage the mesh nodes. The account configured here will replace the account name

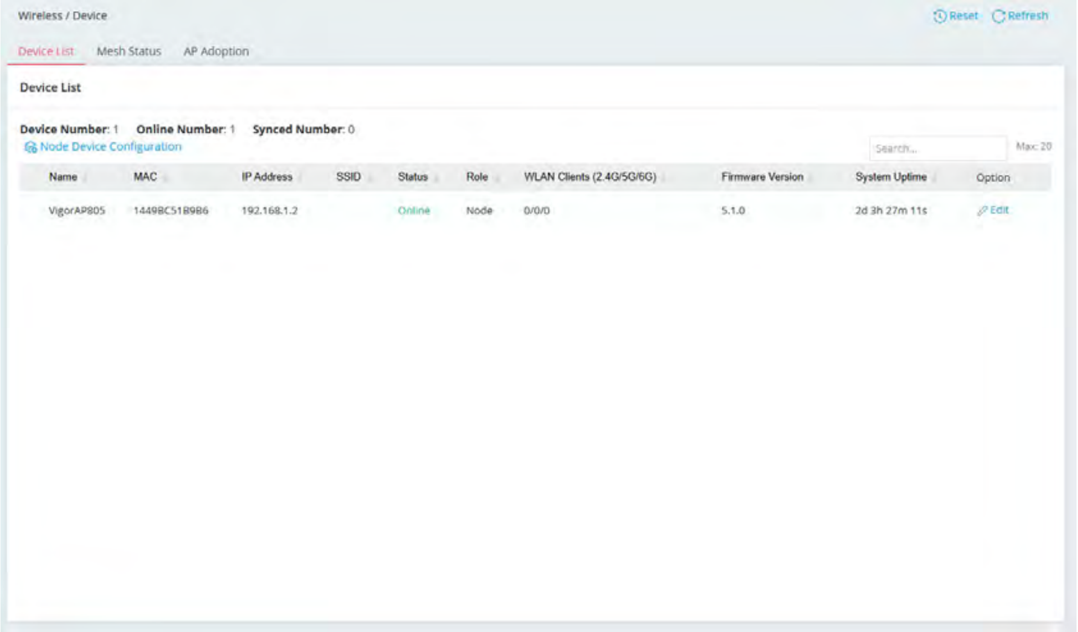
	defined for each node to ensure the mesh node's account security.
Group Admin Password	Set a password for the system administrator to manage the mesh nodes. The password configured here will replace the password defined for each node to ensure the mesh node's account security.
Mesh Setup	
Enable Mesh	Switch the toggle to enable/disable the mesh function.
Mesh Protocol	Select the mesh protocol to manage the mesh network. ● **Vigor Mesh** - A protocol developed by DrayTek. ● **EasyMesh** - A protocol defined by WiFi alliance.
Uplink	It is available only when **Node / VigorMesh** is selected as Device Role / Mesh Protocol. Set the uplink of the device. ● **Auto** - If the Ethernet port is connected and the device can access its gateway, use Wired uplink. Otherwise, use the Wireless uplink. ● **Wired** - Fixed on the Wired uplink. ● **Wireless** - Fixed on the Wireless uplink.
Current Uplink	Displays the current uplink. It is available only when **Auto or Node / VigorMesh** is selected as Device Role / Mesh Protocol.
Group Name	Displays the name of the current Mesh Group. It is available only when Auto or **Root / VigorMesh** is selected as Device Role / Mesh Protocol. If required, change the name.
Mesh Onboarding Mode	It is available only when **EasyMesh** is selected as Mesh Protocol. ● **PBC** - Means the push-button configuration.
Start PBC Onboarding	It is available only when **EasyMesh** is selected as Mesh Protocol and **PBC** is selected as Mesh Onboarding Mode. ● **Start PBC** - Triggers the WPS connection to build network between node backhaul and the root fronthaul.
AP Management Setup	
Enable AP Management	Switch the toggle to enable/disable the AP Management.
Advanced Mode: On	
Auto Wired Adoption	This feature allows users to skip Search/Selection in web AP Adoption and establish VigorMesh group by simply connect the APs to the Root's LAN ports. Default is Disabled. If this feature is enabled, when a new Wired AP is detected by VigorMesh packets through Ethernet, the Root will add it to the **Device>>Device List** and start to register. Then the Node will be adopted automatically. Note that both sides (the root and the node) must support and enable the Auto Wired Adoption.
Wireless Uplink Band	It is available only when **Auto** or **Node / VigorMesh** is selected as Device Role / Mesh Protocol.

	Select available Wireless bands for connecting with uplink
Wireless Downlink Band	It is available only when VigorMesh is selected as Mesh Protocol. Select available Wireless bands for connecting with downlink.
Preferred Wireless Uplink Device	It is available only when Auto or Node / VigorMesh is selected as Device Role / Mesh Protocol. Select a Mesh member as the first priority when choosing Wireless uplink.
Preferred Wireless Uplink Timeout(min)	It is available only when Auto or Node / VigorMesh is selected as Device Role / Mesh Protocol. Set the time period (1 to 10 minutes) to wait for the Preferred Wireless Uplink Device.
Auto Wireless Uplinks Optimization	It is available only when Auto or Root / VigorMesh is selected as Device Role / Mesh Protocol. It is selected in default. If enabled, after changing the environment of the Mesh network, Root will perform reselect to reconstruct the Mesh network.
Log Level	It is available only when VigorMesh is selected as Mesh Protocol. Select Basic or Detailed. Related information will be shown on Syslog.
Cancel	Discard the settings.
Apply	Click it to save the settings.

II-3-2 Device

II-3-2-1 Device List

This page displays general information about the belonging group.



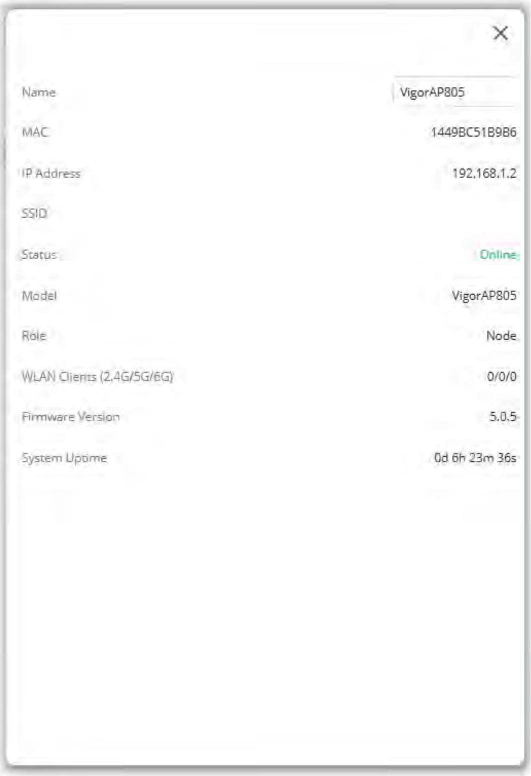
Device List

Device Number: 1 **Online Number:** 1 **Synced Number:** 0

Name	MAC	IP Address	SSID	Status	Role	WLAN Clients (2.4G/5G/6G)	Firmware Version	System Uptime	Option
VigorAP805	1449BC51B9B6	192.168.1.2		Online	Node	0/0/0	5.1.0	2d 3h 27m 11s	Edit

Available settings are explained as follows:

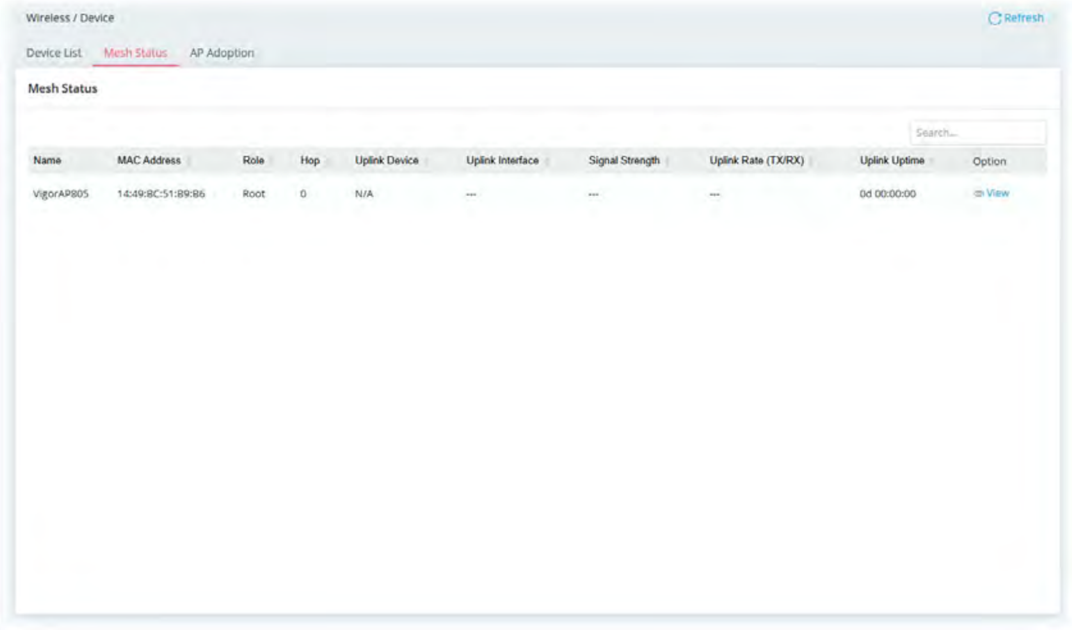
Item	Description
Edit	Click to modify the settings of the selected device. The settings for the APs are slightly different based on the role of the Root and Node. Settings for the AP (as the Node):

	 Name VigorAP805 MAC 1449BC51B9B6 IP Address 192.168.1.2 SSID Status Online Model VigorAP805 Role Node WLAN Clients (2.4G/5G/6G) 0/0/0 Firmware Version 5.0.5 System Uptime 0d 6h 23m 36s

II-3-2-2 Mesh Status

Displays general information of the Mesh network.

This page is available only when **Mesh** is enabled (**Virtual Controller>>Role Setup**).

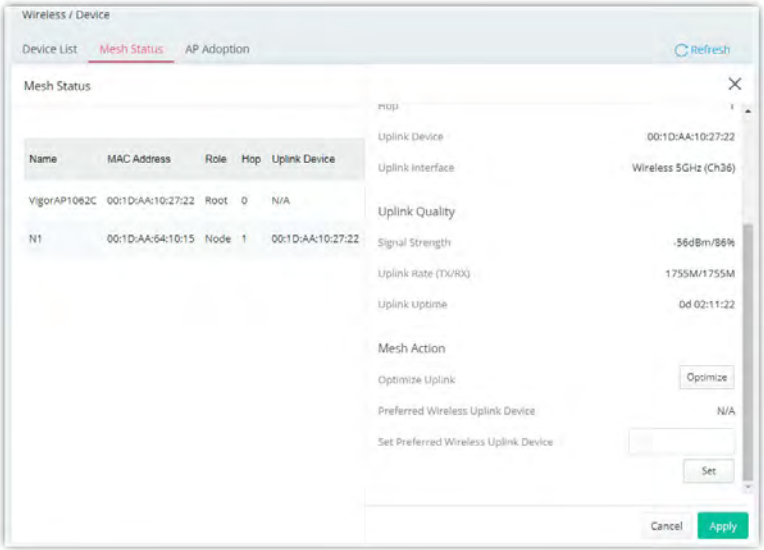


Mesh Status

Name	MAC Address	Role	Hop	Uplink Device	Uplink Interface	Signal Strength	Uplink Rate (TX/RX)	Uplink Uptime	Option
VigorAP805	14:49:BC:51:B9:B6	Root	0	N/A	---	---	---	0d 00:00:00	View

Available settings are explained as follows:

Item	Description
Name	Displays the name of the device (for identification).
MAC Address	Displays the MAC address of the device.
Role	Displays the role of the device.
Hop	Displays the number of Wireless links from the device to Root. "0" means the device is using a Wired uplink.
Uplink Device	Displays the MAC address of the device that this device connects to.
Uplink Interface	Displays the interface which the device is using to connect to uplink.
Signal Strength	Displays the signal strength of the device to its uplink.
Uplink Rate(Tx/RX)	It is available only when **VigorMesh** is selected as Mesh Protocol. Displays the link rate of the device to its uplink.
Uplink Uptime	It is available only when **VigorMesh** is selected as Mesh Protocol. Displays how long the device is online.
Option	Click **View** to modify the selected mesh device.



Name	MAC Address	Role	Hop	Uplink Device
VigorAP1062C	00:1D:AA:10:27:22	Root	0	N/A
N1	00:1D:AA:64:10:15	Node	1	00:1D:AA:10:27:22

Hop	1
Uplink Device	00:1D:AA:10:27:22
Uplink Interface	Wireless 5GHz (Ch36)
Uplink Quality	
Signal Strength	-56dBm/86%
Uplink Rate (TX/RX)	1755M/1755M
Uplink Uptime	0d 02:11:22
Mesh Action	
Optimize Uplink	Optimize
Preferred Wireless Uplink Device	N/A
Set Preferred Wireless Uplink Device	

Optimize All Mesh Links - It is available only when **VigorMesh** is selected as Mesh Protocol and the device is a Root.

Press the **Optimize** button to perform reselect to reconstruct the Mesh network.

Optimize Uplink - It is available only when **VigorMesh** is selected as Mesh Protocol and the device is a Wireless Node.

Press the **Optimize** button to disconnect the device from Mesh network. The device might connect to a better uplink later.

Preferred Wireless Uplink Device - It is available only when **VigorMesh** is selected as Mesh Protocol and the device is a Node.

Displays the Preferred Wireless Uplink of the device.

Set Preferred Wireless Uplink Device - It is available only when **VigorMesh** is selected as Mesh Protocol and the device is a Node.

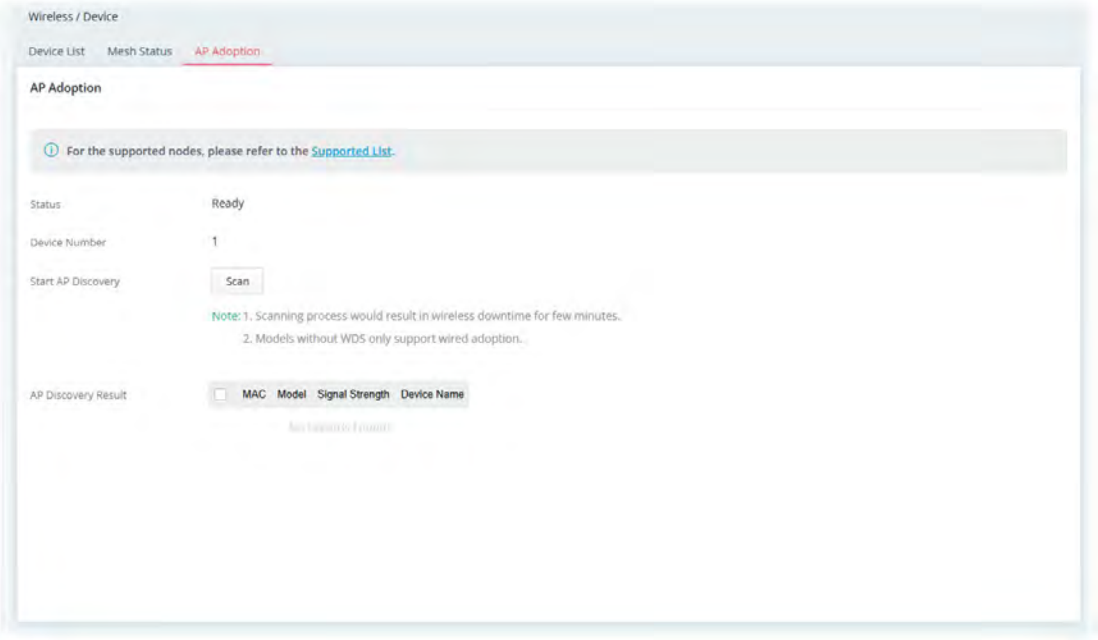
Select a Mesh member and press the **Set** button to set the Preferred Wireless Uplink Device of the device.

II-3-2-3 AP Adoption

Search and add new Nodes to the device's Group.

This page is available when Current Device Role is Root.

It is also available when Device Role is Auto and Device List contains only the device itself.



Wireless / Device

AP Adoption

For the supported nodes, please refer to the Supported List.

Status: Ready

Device Number: 1

Start AP Discovery: Scan

Note: 1. Scanning process would result in wireless downtime for few minutes.
2. Models without WDS only support wired adoption.

AP Discovery Result

☐	MAC	Model	Signal Strength	Device Name

No results found

Available settings are explained as follows:

Item	Description
Status	Displays whether the Scan button is available now.
Start AP Discovery	Press the Scan button to search new Nodes.
AP Discovery Result	Displays the scanned result. ☐ - Select the checkbox if you want to add the device into a Group. MAC - Displays the MAC address of the device. Model - Displays the model of the device. Signal Strength - Displays the signal strength of the device if it was found through the Wireless. Device Name - Insert the name of the device for identification.
Cancel	Discard current settings.
Apply	Click to add the selected device(s) into the Group.

Tips for VigorMesh Network Setup

- VigorMesh supports auto uplink. If a device could not access its gateway, it becomes a Wireless Node automatically.

  A Mesh Root or a Wired Mesh Node should be able to ping its gateway through Ethernet.

- VigorMesh can add new Mesh Nodes into Mesh Group through both Wireless and Wired. However, we recommend to connect new Nodes to the Root by Ethernet cables and add them into Mesh Group first.

  Wait until the configuration sync finishes. And then move the Nodes to their destinations.
- VigorMesh supports up to 3 hops. However, it is suggested to connect the Mesh network with less than or equal to 2 hops.
- It is suggested to make the Uplink Signal Strengths of all Wireless Mesh Nodes be larger than -65 dBm.
- A Wireless Mesh Node with an Ethernet cable should not loop to another Node.
- If the Mesh Root disappears and there are online Wired Mesh Nodes with Device Role Auto, one of the Wired Mesh Nodes will become a Mesh Root automatically.
- A VigorMesh Group can be reset by the "Reset" button on Virtual Controller >> Wireless >> Device >> Device List.
  - If resetting a Mesh Root,
    - All online Mesh Nodes will be informed to reset.
    - For those Mesh Nodes unable to reset, reset them manually.
  - If resetting a Mesh Node,
    - The device will become a New Node again.
    - The Wireless SSID settings of the device will be reset, too.

Troubleshooting:

- Check the country code and Wireless channels.
- Check the firmware version. Please make sure all Mesh members are in the newest firmware version.
- Check the Current Device Role and Current Uplink of the device.
- Please make sure that the device is not in DFS CAC detection.
- Check the channel load. Make sure it is not over 70%.

Tips for EasyMesh Network Setup

- Set up multiple mesh devices with uplink RSSI larger than -65dBm.
- Setup is recommended to use wired connection and device list to add devices.
- EasyMesh network supports up to 3 hops of devices. However, it is suggested to connect with less than or equal to 2 hops.
- EasyMesh is not suggested to join existing VigorMesh Environment.
- The maximum of devices number is (ssid_num * device_num <= 56) -> device_num is the max device number.

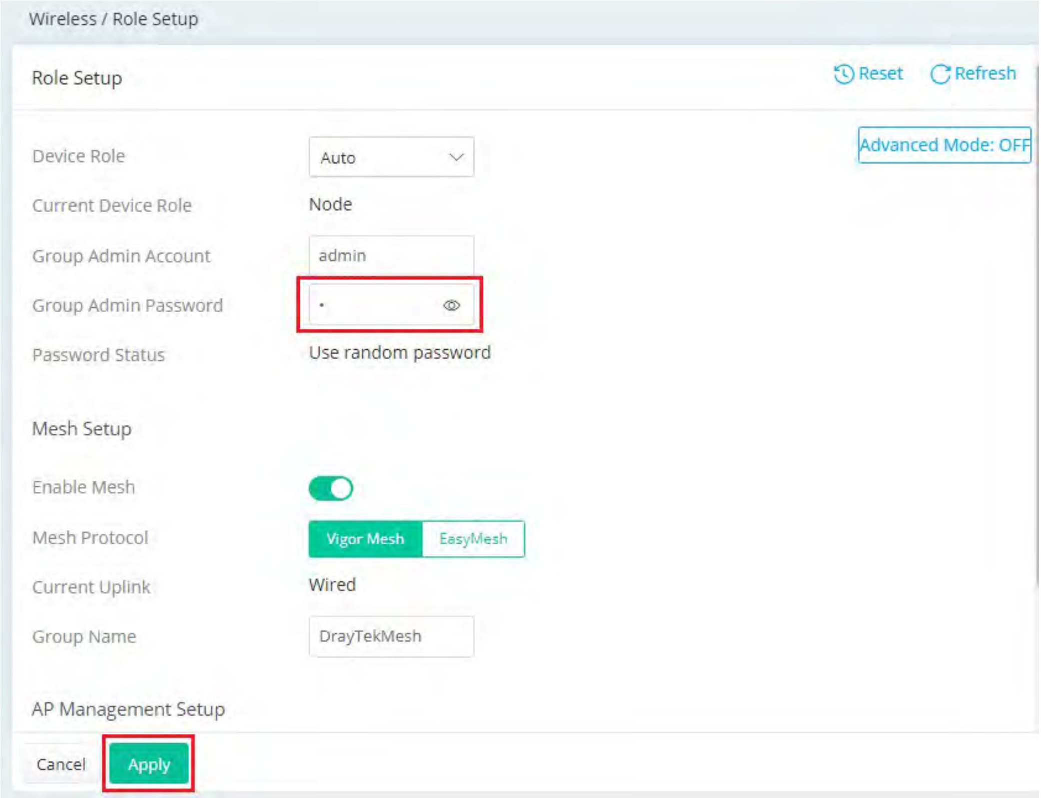
How to set up a VigorMesh group?

The following steps will guide you how to setup a VigorMesh Group.

Please access the web of the device which you want to use it as the Root.

1. (Optional) Open Virtual Controller>>Wireless>>Role Setup.

   Set Group Admin Password. This value will be the Administrator Password of the Nodes after they join the Mesh Group and complete configuration sync.



Wireless / Role Setup

Role Setup

Device Role: Auto

Current Device Role: Node

Group Admin Account: admin

Group Admin Password: •

Password Status: Use random password

Mesh Setup

Enable Mesh: ON

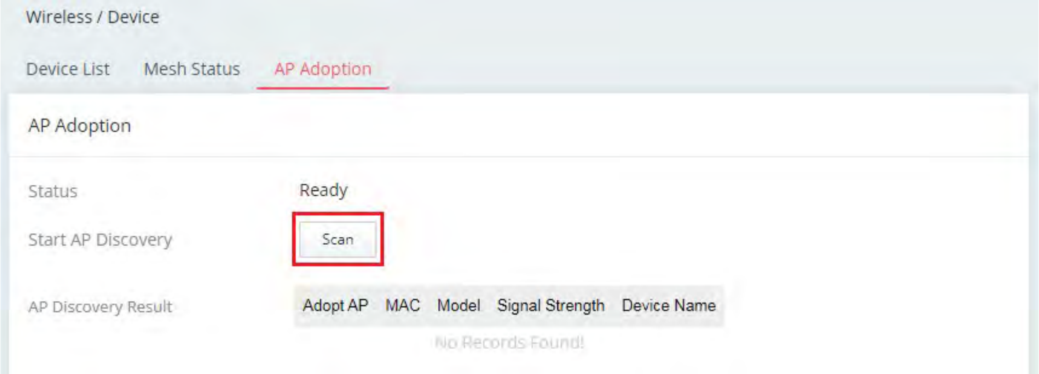
Mesh Protocol: Vigor Mesh

Current Uplink: Wired

Group Name: DrayTekMesh

AP Management Setup

2. Open **Virtual Controller>>Wireless>>Device>>AP Adoption**. Click the **Scan** button.



Wireless / Device

AP Adoption

Status: Ready

Start AP Discovery: Scan

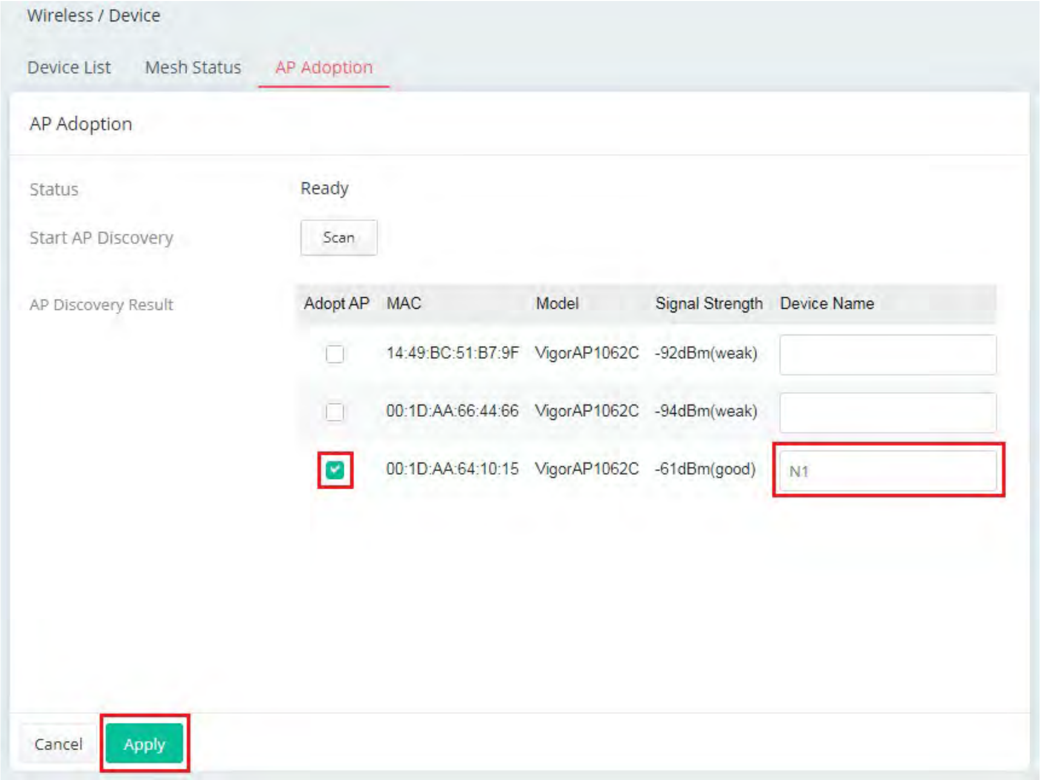
AP Discovery Result:

Adopt AP	MAC	Model	Signal Strength	Device Name
No Records Found!				

3. Wait until the searching result appears.

   Choose the device(s) you want to add to the Group and set the names for identification.

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



Wireless / Device

AP Adoption

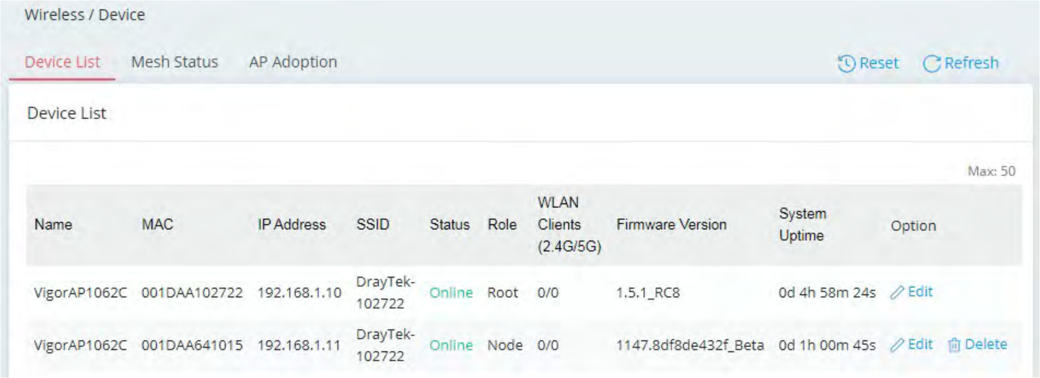
Status: Ready

Start AP Discovery: Scan

AP Discovery Result

Adopt AP	MAC	Model	Signal Strength	Device Name
□	14:49:BC:51:B7:9F	VigorAP1062C	-92dBm(weak)	
□	00:1D:AA:66:44:66	VigorAP1062C	-94dBm(weak)	
☑	00:1D:AA:64:10:15	VigorAP1062C	-61dBm(good)	N1

4. Refer to **Virtual Controller>>Wireless>>Device>>Device List** and **Virtual Controller >> Wireless >> Device >>Mesh Status** for viewing the result.

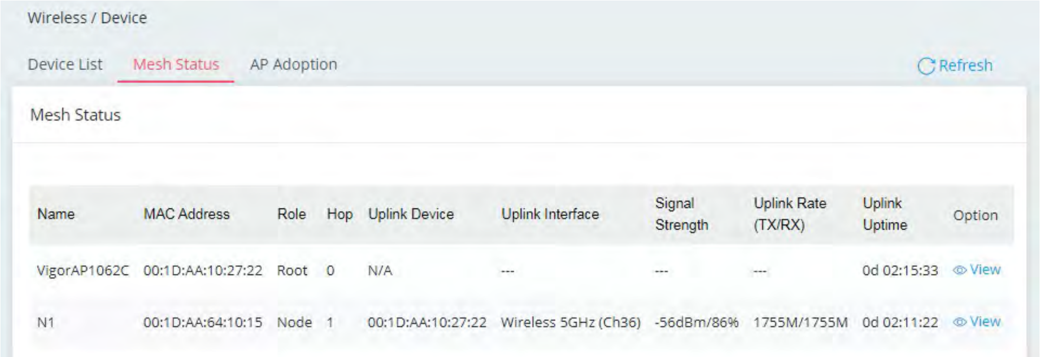


Wireless / Device

Device List

Max: 50

Name	MAC	IP Address	SSID	Status	Role	WLAN Clients (2.4G/5G)	Firmware Version	System Uptime	Option
VigorAP1062C	001DAA102722	192.168.1.10	DrayTek-102722	Online	Root	0/0	1.5.1_RC8	0d 4h 58m 24s	Edit
VigorAP1062C	001DAA641015	192.168.1.11	DrayTek-102722	Online	Node	0/0	1147.8df8de432f_Beta	0d 1h 00m 45s	Edit Delete



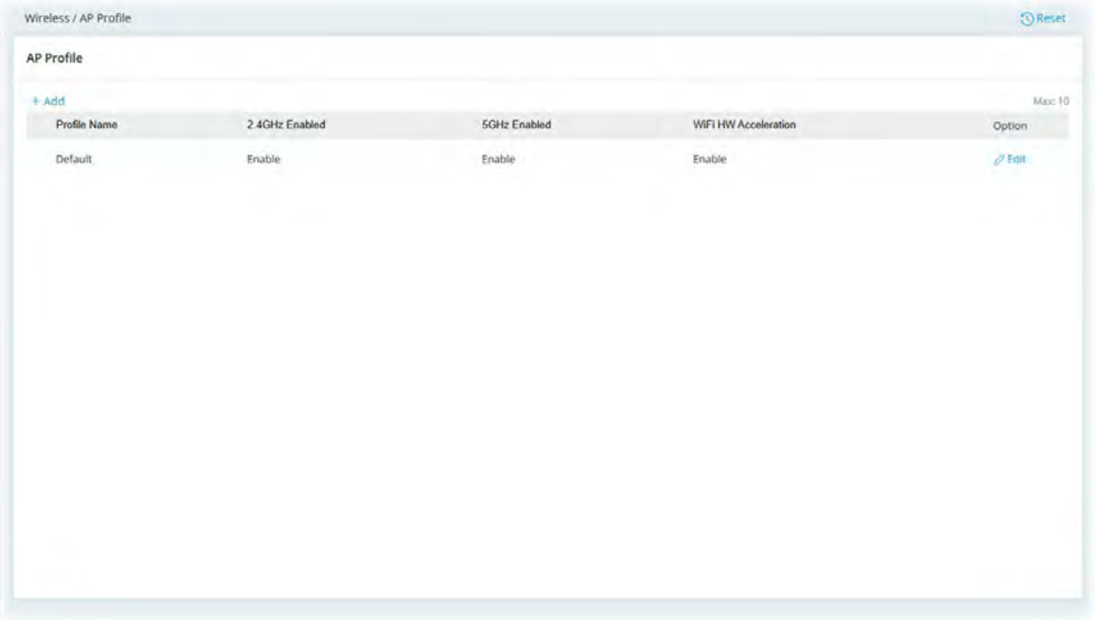
Wireless / Device

Mesh Status

Name	MAC Address	Role	Hop	Uplink Device	Uplink Interface	Signal Strength	Uplink Rate (TX/RX)	Uplink Uptime	Option
VigorAP1062C	00:1D:AA:10:27:22	Root	0	N/A	---	---	---	0d 02:15:33	View
N1	00:1D:AA:64:10:15	Node	1	00:1D:AA:10:27:22	Wireless 5GHz (Ch36)	-56dBm/86%	1755M/1755M	0d 02:11:22	View

II-3-3 AP Profile

AP profile is used to apply to a selected access point. It is very convenient for the administrator to configure the setting for access point without opening the web user interface of the access point.



Wireless / AP Profile

Reset

AP Profile

+ Add

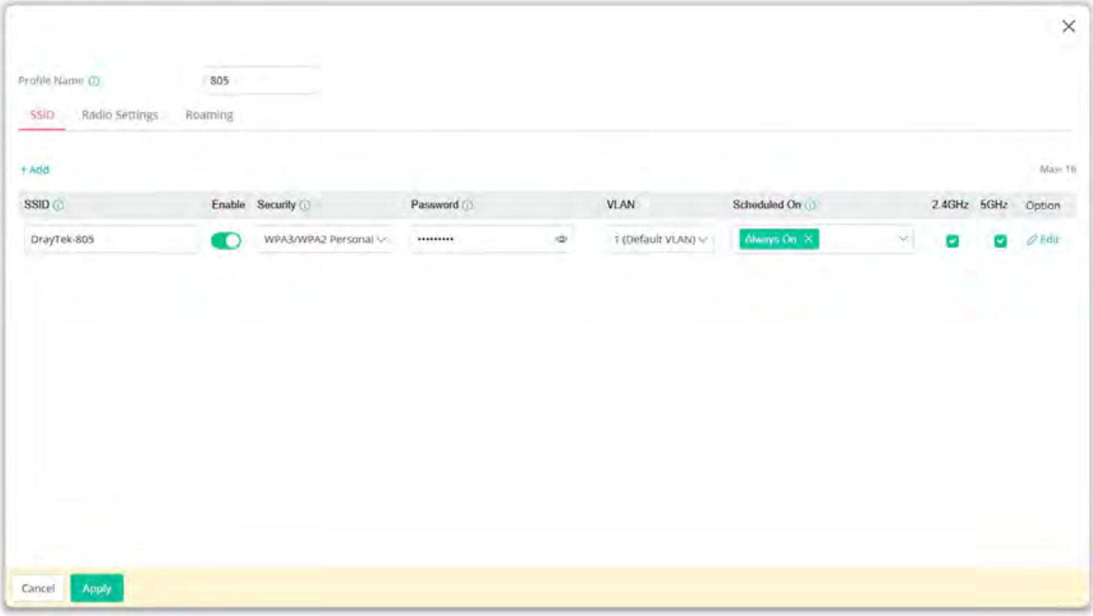
Max: 10

Profile Name	2.4GHz Enabled	5GHz Enabled	WiFi HW Acceleration	Option
Default	Enable	Enable	Enable	Edit

To add a new profile, click the **Add** link to create AP profiles with various SSIDs, Radio Settings, and Roaming settings.

II-3-3-1 SSID

An AP profile can be configured to support up to 8 SSIDs.



Profile Name: 805

SSID | Radio Settings | Roaming

+ Add

Max: 16

SSID	Enable	Security	Password	VLAN	Scheduled On	2.4GHz	5GHz	Option
DrayTek-805	●	WPA3/WPA2 Personal	••••••••••	1 (Default VLAN)	Always On	☑	☑	Edit

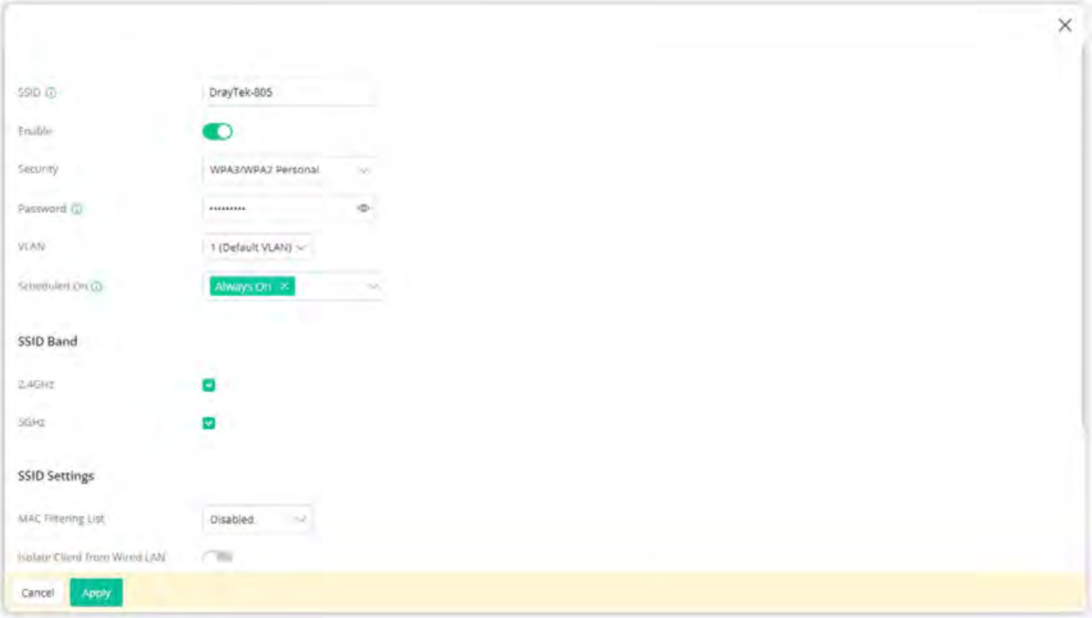
Cancel | Apply

Available settings are explained as follows:

Item	Description

+Add	Click to create a new entry of SSID.
SSID	Enter a name as the AP identifier.
Enable	Switch the toggle to enable or disable the SSID.
Security	Select the security mode.
Password	Enter 8~64 ASCII characters.
VLAN	Select a VLAN to which this SSID belongs.
Scheduled On	This SSID profile will be forced up /down based on the schedule profile selected.
2.4GHz/5GHz	Select the band(s) for the SSID.
Option	**Edit** – Configure the detailed settings for the SSID.

Click **Edit** to configure detailed settings for the SSID profile.



SSID: DrayTek-805

Enable: ●

Security: WPA3/WPA2 Personal

Password: •••••••••

VLAN: 1 (Default VLAN)

Scheduled On: Always On

SSID Band

2.4GHz: ☑

5GHz: ☑

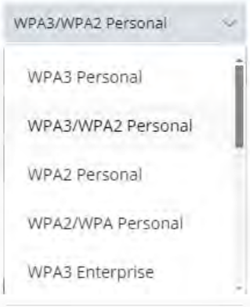
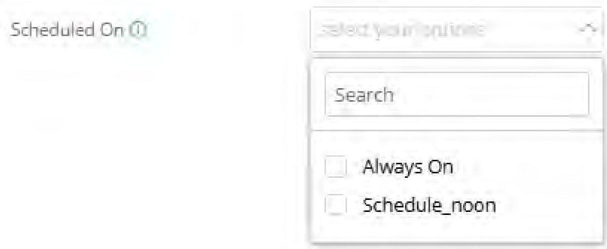
SSID Settings

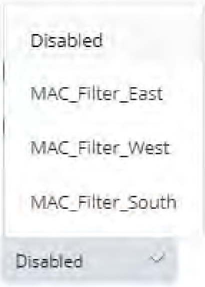
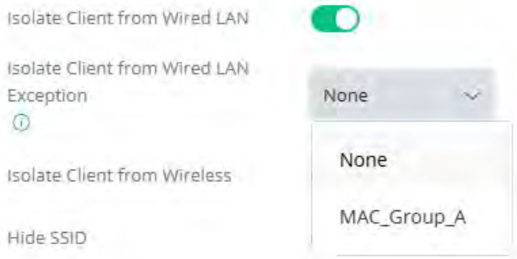
MAC Filtering List: Disabled

Isolate Client from Wired LAN: ○

Available settings are explained as follows:

Item	Description
SSID	Service Set Identification (SSID), which shows up as the AP identifier. Maximum length is 32 characters. Modify the name if required.
Enable	Switch the toggle to enable/disable the SSID profile.
Security	There are several modes provided for you to choose from. Below shows the modes with higher security; **WPA3 Personal, WPA3/WPA2 Personal, WPA2 Personal, WPA2/WPA Personal** - Accepts only WPA clients and the encryption key should be entered in Password. The WPA encrypts each frame transmitted from the radio using the PSK (Pre-Shared Key) entered manually in Password." ● **WPA3 Enterprise, WPA2 Enterprise, WPA2/WPA Enterprise** - Accepts only WPA clients and the Authentication Server should be set in Configuration >> RADIUS/ TACACS+ >> External RADIUS and be selected in RADIUS Server. The WPA encrypts each frame transmitted from the radio using the

 WPA3/WPA2 Personal WPA3 Personal WPA3/WPA2 Personal WPA2 Personal WPA2/WPA Personal WPA3 Enterprise	key which automatically negotiated via 802.1x authentication. ● 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. Below shows the modes with basic security; ● WPA Personal - Accepts only WPA clients and the encryption key should be entered in Password. The WPA encrypts each frame transmitted from the radio using the PSK (Pre-Shared Key) entered manually in Password. ● WPA Enterprise - Accepts only WPA clients and the Authentication Server should be set in Configuration >> RADIUS/ TACACS+ >> External RADIUS and be selected in RADIUS Server. The WPA encrypts each frame transmitted from the radio using the key which automatically negotiated via 802.1x authentication. ● WEP Personal - Accepts only WEP clients and the encryption key should be entered in WEP Settings. ● None - The encryption mechanism is turned off.
Password	Enter 8~64 ASCII characters, such as "012345678". This feature is available for WPA Personal, WPA2/WPA Personal, WPA2 Personal, WPA3/WPA2 Personal, and WPA3 Personal mode.
VLAN	Select a VLAN to which this SSID belongs.
Scheduled On	This SSID profile will be forced up /down based on the schedule profile used (profiles created via Configuration>>Objects>>Schedule).  Scheduled On ⓘ Select your options Search □ Always On □ Schedule_noon The default is Always On.
	SSID Band
2.4GHz/5GHz	Select the band(s) for the SSID.
	SSID Settings
MAC Filtering List	The default is Disabled. Select one of the MAC filter profiles (created via Security>>MAC Filtering Profile) for this SSID setting. Only the valid MAC address that has been configured allow or deny to access the wireless LAN interface.

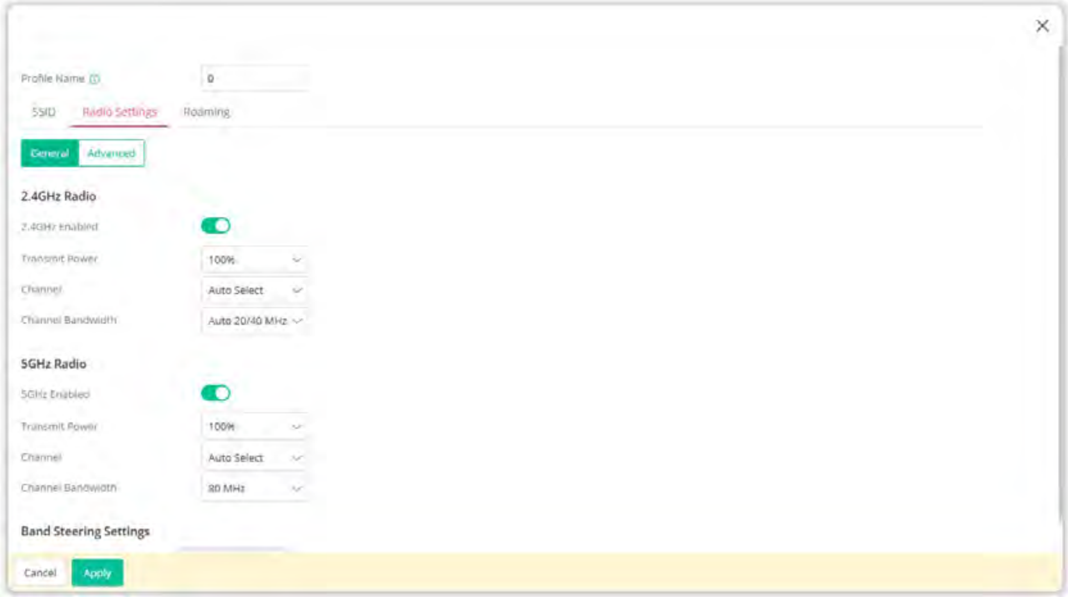
	 Disabled MAC_Filter_East MAC_Filter_West MAC_Filter_South Disabled
Isolate Client from Wired LAN	Switch the toggle to enable or disable the function. Makes the Wireless clients with this SSID not access to Wired devices. **Isolate Client from Wired LAN Exception** - Select the MAC group object (created in Configuration>>Object>>MAC Group). Wireless clients with this SSID are allowed to access the Wired devices specified in the MAC group object.  Isolate Client from Wired LAN Isolate Client from Wired LAN Exception: None None MAC_Group_A Isolate Client from Wireless Hide SSID
Isolate Client from Wireless	Switch the toggle to enable/disable the function. If enabled, it disallows communication between wireless clients (stations) on the same SSID.
Hide SSID	Switch the toggle to enable(hide) /disable (show) the SSID. Select to keep SSIDs from showing up when scans are performed by wireless clients, which makes it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless client and software used, the user may see only an AP listed without the SSID, or the AP might not even show up.
WPA Settings	
Key Renewal Interval	It is available when WPA # is selected as Security. WPA uses a shared key for authentication to the network. However, normal network operations use a different encryption key that is randomly generated. This randomly generated key 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.
WEP Settings	
Default Key	This feature is available for **WEP Personal** mode. 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 ','.
Key # Type	**Hex/ASCII** - 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 ','.
Key #	Enter 5 **ASCII** characters or 10 **hexadecimal** values in 64-bit encryption level, or 13 ASCII characters or 26 hexadecimal values in 128-bit encryption level.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

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

II-3-3-2 Radio Settings

This page lets you configure the most basic settings of your wireless network, including mode, WLAN channels and channel bandwidth.



Profile Name: 0

2.4GHz Radio

2.4GHz Enabled: on
Transmit Power: 100%
Channel: Auto Select
Channel Bandwidth: Auto 20/40 MHz

5GHz Radio

5GHz Enabled: on
Transmit Power: 100%
Channel: Auto Select
Channel Bandwidth: 80 MHz

Band Steering Settings

Available settings are explained as follows:

Item	Description
General for 2.4GHz	
2.4GHz Enabled	Switch the toggle to enable/disable the 2.4GHz Radio settings.
Transmit Power	Sets the power percentage of the access point's transmission signal. The greater the TX Power value, the higher intensity of the signal will be.
Channel	Allows you to specify a particular wireless channel to use, or let the system determine the optimal channel by selecting "Auto Select". The list of available channels varies depending on the locale for which the router is intended.
Channel Bandwidth	20 MHz –Vigor Router will utilize 20 MHz channels for data transmission and reception between the router and wireless stations. 40 MHz – Vigor Router will utilize 40 MHz for data transmission and reception between the router and wireless stations. Auto 20/40 MHz – Vigor Router will utilize either 20 MHz or 40 MHz for data transmission and reception depending on the number of AP nearby the router. 20MHz will be used when there are more than 10 wireless APs; otherwise 40MHz will be used. Selecting this setting ensures the best performance for data transit on networks with both 20 MHz and 40 MHz clients.
General for 5GHz	
5GHz Enabled	Switch the toggle to enable/disable the 5GHz Radio settings.
Transmit Power	Sets the power percentage of the access point's transmission signal. The greater the TX Power value, the higher intensity of the signal will be.

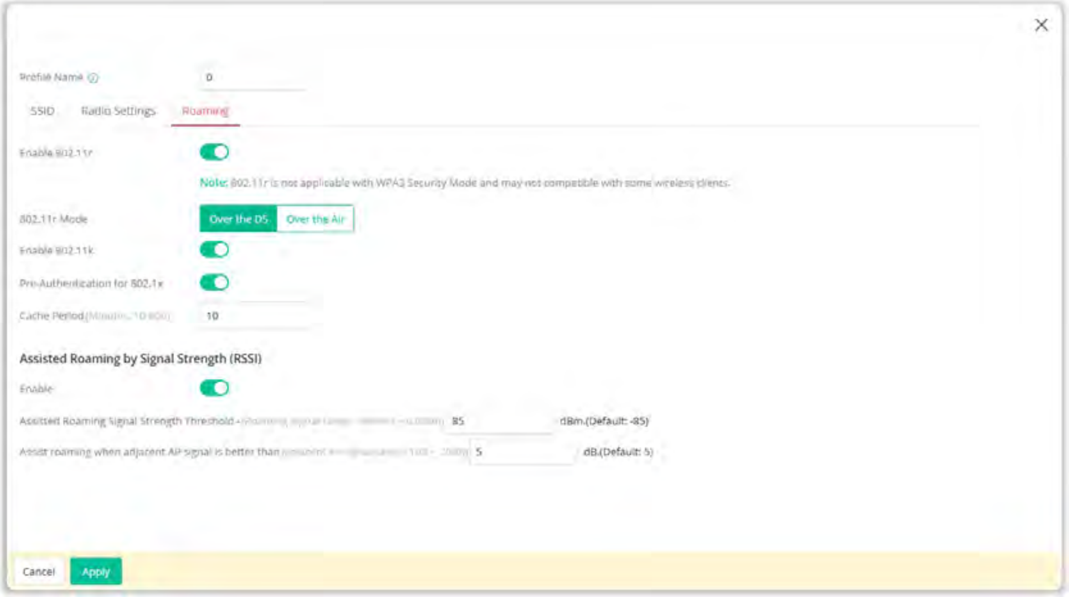
Channel	Allows you to specify a particular wireless channel to use, or let the system determine the optimal channel by selecting "**Auto Select**". The list of available channels varies depending on the local for which the router is intended.
Channel Bandwidth	**20 MHz** –Vigor Router will utilize 20 MHz for data transmission and reception between the router and wireless stations. **40 MHz** – Vigor Router will utilize 40 MHz for data transmission and reception between the router and wireless stations. **80 MHz** –Vigor Router will utilize 80 MHz for data transmission and reception between the router and wireless stations. **160 MHz** – Vigor Router will utilize 160 MHz for data transmission and reception between the router and wireless stations.
Band Steering Settings	
5Ghz Client Minimum RSSI	If it is enabled, Vigor router will detect if the wireless client is capable of dual-band or not within the time limit. The wireless station has the capability of a 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 Vigor router, Vigor router will allow the client to connect to the 2.4GHz network.
Advanced	
Fragment Length	Set the Fragment threshold of wireless radio. Do not modify the default value if you don't know what it is. The default value is 2346.
RTS Threshold	Minimize the collision (unit is bytes) between hidden stations to improve wireless performance. Set the RTS threshold of wireless radio. Do not modify the default value if you don't know what it is. The default value is 2347.
Country Code	Available for 2.4GHz Radio only. Vigor router broadcasts country codes according to the 802.11d standard. However, some wireless stations will detect/scan access points looking for country codes to determine which country it is in, and utilize channels appropriate to the country. The wireless client might get confused if there are multiple access points in the vicinity broadcasting different country codes. In such cases, it might be necessary to change the country code of the access point to ensure these clients can successfully establish a wireless connection.
WMM Capable	WMM stands for Wi-Fi Multimedia. It provides basic Quality of Service (QoS) by prioritizing traffic based on four access categories defined in the IEEE 802.11e standard. The access categories are AC_VO, AC_VI, AC_BE and AC_BK, which corresponds to traffic types of voice, video, best effort and low priority (background) data, respectively. To apply WMM parameters for wireless data transmission, please switch the toggle to enable the function.
APSD Capable	APSD (Automatic Power-Save Delivery) is an enhancement over the power-saving mechanisms supported by Wi-Fi networks. It allows access points to buffer traffic before transmitting it to wireless devices, thus allowing wireless devices to enter into power saving mode which reduces power consumption. Not all wireless clients support APSD properly, and the only way to find out if APSD is appropriate for your network is to experiment.

	The default setting is **Disable**.
Airtime Fairness	Switch the toggle to enable/disable the function. With airtime fairness, every client at a given quality-of-service level has equal access to the network's airtime. Environments that can benefit by applying airtime fairness: (1) Many wireless stations. (2) All stations mainly use download traffic. (3) The performance bottleneck is wireless connection.
WiFi HW Acceleration	Disable this option to turn off WiFi HW NAT and IGMP Snooping. (Recommended if some websites or images fail to load)
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

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

II-3-3-3 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 by enabling the Roaming feature for each AP to reach the purpose of expanding wireless signals seamlessly.



Profile Name: 0

Enable 802.11r: ●

Note: 802.11r is not applicable with WPA3 Security Mode and may not compatible with some wireless clients.

802.11r Mode: [✓ Over the DS] Over the Air

Enable 802.11k: ●

Pre-Authentication for 802.1x: ●

Cache Period (Minutes, 10-800) [illegible]: 10

Assisted Roaming by Signal Strength (RSSI)

Enable: ●

Assitted Roaming Signal Strength Threshold [illegible]: 85 dBm.(Default: -85)

Assist roaming when adjacent AP signal is better than [illegible]: 5 dB.(Default: 5)

Available settings are explained as follows:

Item	Description
Enabled 802.11r	Switch the toggle to enable/disable the function of fast roaming to make Wireless clients switch between the hotspots fast and securely. There are two methods to run fast roaming.
802.11r Mode	**Over the DS** - In response to the needs of signal strength change, the client can communicate with the other AP through the original AP with Action Frames (FT Request and FT Response). **Over the Air** - In response to the needs of signal strength change,

	the client can communicate directly with the other AP using a fast roaming authentication algorithm (without requiring reauthentication at every AP).
Enable 802.11k	Switch the toggle to enable the 802.11k protocol (also know as Radio Resource Management (RRM)). If enabled, the access point will optimize the performance of wireless networks.
Pre-Authentication for 802.1x	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) Switch the toggle to enable/disable 802.11x Pre-Authentication. Enable - Enable IEEE 802.1X Pre-Authentication. Disable - Disable IEEE 802.1X Pre-Authentication.
Cache Period	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.
	Assisted Roaming by Signal Strength (RSSI)
Enable	Switch the toggle to enable/disable the function. When the link rate of the wireless station is too low or the signal received by the wireless station is too worse, Vigor router 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.
Assisted Roaming Signal Strength Threshold	When the signal strength of the wireless station is below the value (dBm) set here and adjacent AP (must be DrayTek Router/AP and support such feature too) with higher signal strength value (defined in the field of Assist roaming when adjacent AP signal is better than) is detected by Vigor router, Vigor router will terminate the network connection for that wireless station. Later, the wireless station can connect to the adjacent AP (with better RSSI).
Assist roaming when adjacent AP signal is better than	Specify a value as a threshold.
Cancel	Discard current settings.
Apply	Save the current settings.

After finishing this web page configuration, please click Apply 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: Device Settings, Management, Firmware, Backup & Restore, Accounts & Permission, System Reboot, and Registration & Services.

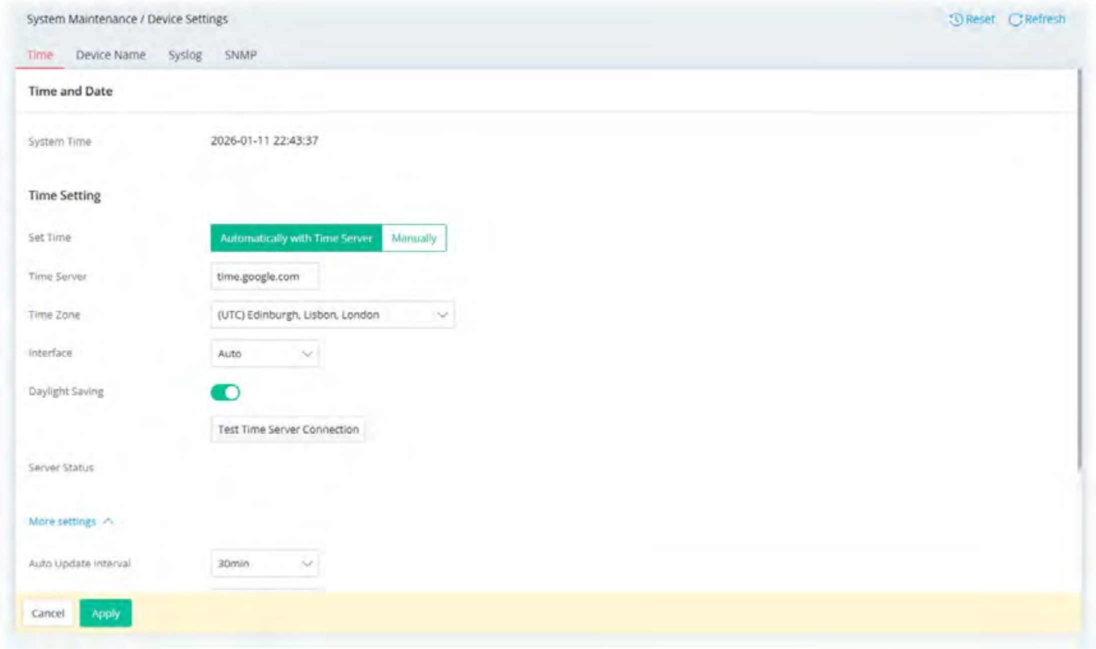
III-1-1 Device Settings

The user can modify the time, device name, and Syslog for the device.

III-1-1-1 Time

Open **System Maintenance>>Device Settings** and click the **Time** tab.

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


System Maintenance / Device Settings
Reset
Refresh
Time
Device Name
Syslog
SNMP
More settings
Test Time Server Connection
Cancel
Apply

Time and Date

System Time: 2026-01-11 22:43:37

Time Setting

Set Time: Automatically with Time Server | Manually

Time Server: time.google.com

Time Zone: (UTC) Edinburgh, Lisbon, London

Interface: Auto

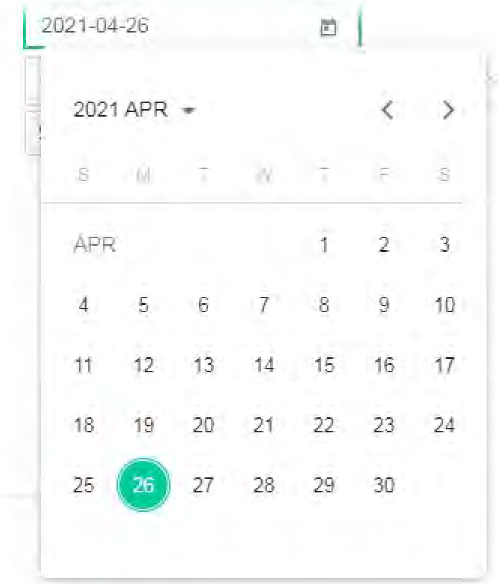
Daylight Saving: ●

Server Status

Auto Update Interval: 30min

Available parameters are explained as follows:

Item	Description
	Time and Date
System Time	Display current time.
	Time Setting
Set Time	Determine the method (automatically or manually) to set the time. **Automatically with Time Server** - Set the system time by retrieving time information from the specified network time server using the Network Time Protocol (NTP). **Manually** - Set the system time using the time reported by the

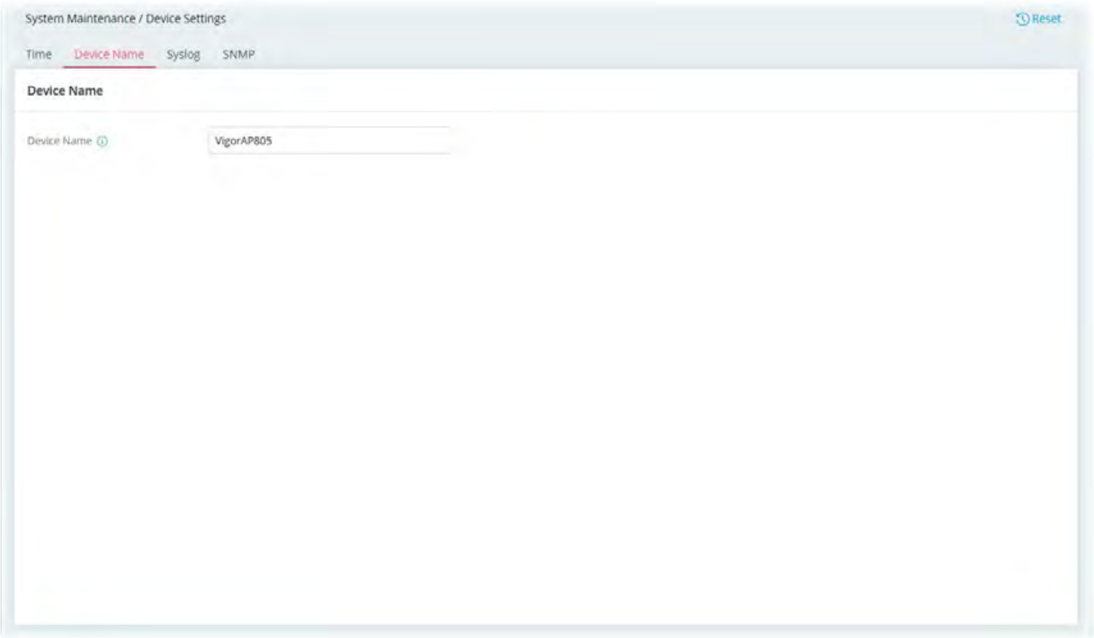
	web browser.
When Automatically with Time Server is selected as Set Time	**Time Server** - Enter the web site of the primary time server. **Time Zone** - Select the time zone where the access point is located. **Interface** - Renew the time through the interface selected by VigorAP automatically. **Daylight Saving** - Enable Daylight Saving Time (DST) if it is applicable to your location. **Test Time Server Connection** – Click to make a test if the selected time server workable for the network. **Server Status** - Displays the status (success/failure) of time server connection. **More Settings** - Click to open advanced settings for the time server. ● **Auto Update Interval** - Select the time interval (30min or 60min) at which the AP updates the system time periodically. ● **Secondary Server** - For having a backup time server, please enter the URL/IP address in the field of Secondary Server. ● **Secondary Interface** - Backup interface for renewing the time automatically. ● **Daylight Saving Period** - It is available when **Daylight Saving** is enabled. Enter a custom schedule to enable the Daylight Saving Time (DST) - Default, by Week and by Date.
When Manually is selected as Set Time	**Time Zone** - Select the time zone where the AP is located. **Date** - Use the drop-down calendar to specify correct date.  2021-04-26 2021 APR S M T W T F S APR 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 **Time** - Set the time by specifying hours, minutes, and seconds. **Synchronize with Browse** - Click **Sync now** to sync the time setting with the browser.
Apply	Save the current settings and renew the system time.
Cancel	Discard current settings and return to the previous page.

After finishing this web page configuration, please click **Apply** to renew the system time.

III-1-1-2 Device Name

Display the device name. Change the name if you want.

Open **System Maintenance>>Device Settings** and click the **Device Name** tab.



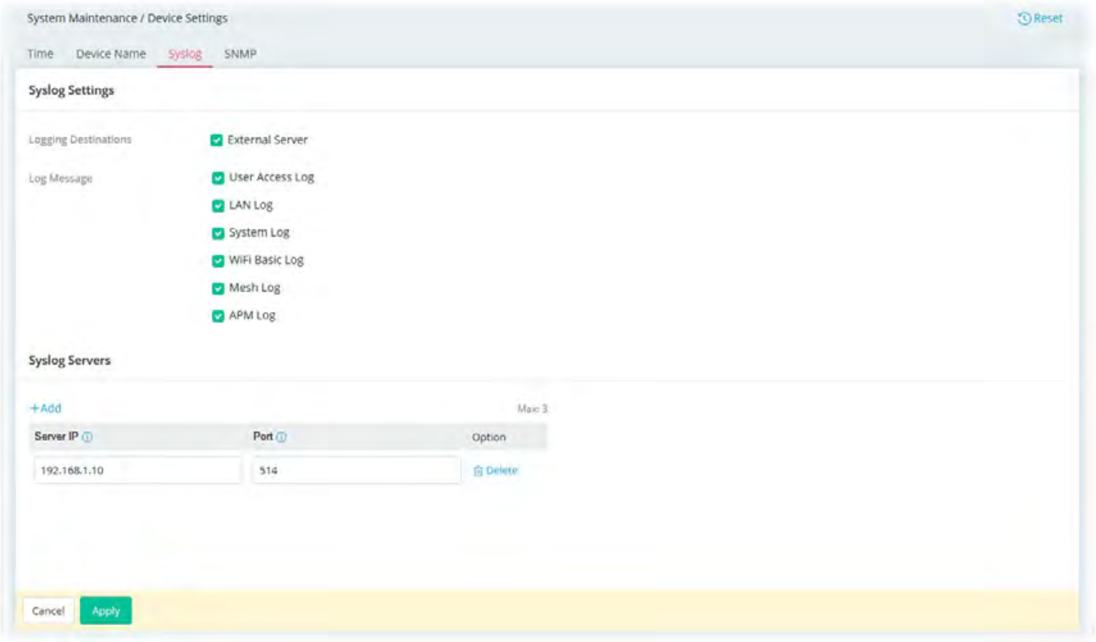
Device Name

Device Name: VigorAP805

III-1-1-3 Syslog

SysLog function is provided for users to monitor the device.

Open **System Maintenance>>Device Settings** and click the **Syslog** tab.



Syslog Settings

Logging Destinations: ☑ External Server

Log Message: ☑ User Access Log ☑ LAN Log ☑ System Log ☑ WiFi Basic Log ☑ Mesh Log ☑ APM Log

Syslog Servers

Server IP	Port	Option
192.168.1.10	514	Delete

Available parameters are explained as follows:

Item	Description

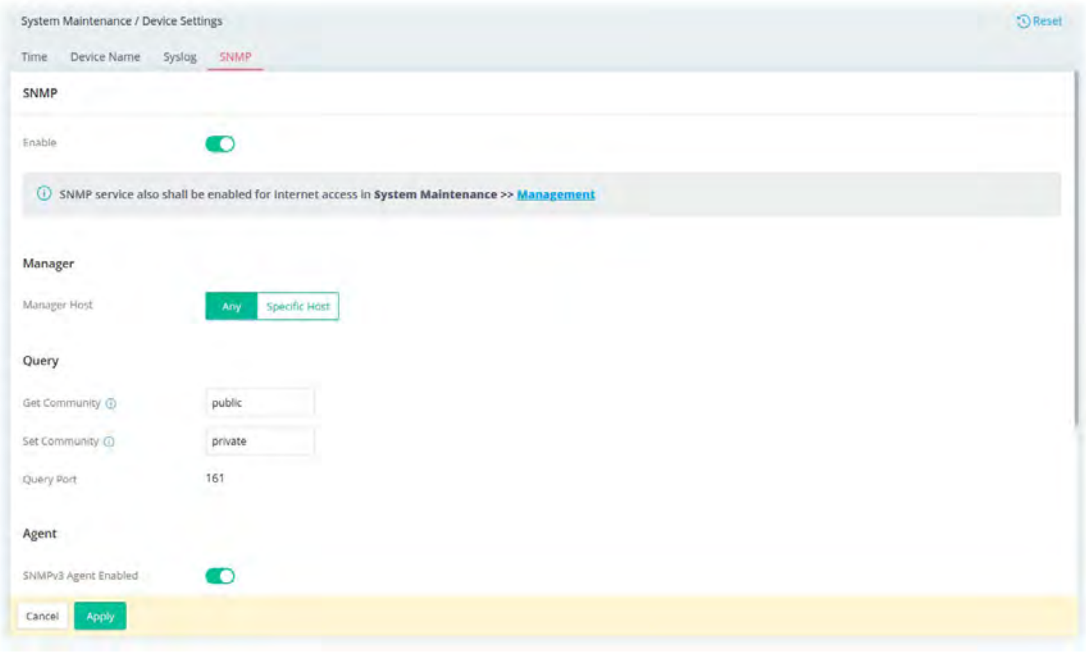
Syslog Settings	
Logging Destinations	Select External Server to display Log Message and Syslog Servers for detailed configuration.
Log Message	Select to send the corresponding message of user access, interface, and system information to Syslog.
Syslog Servers	
+Add	Click to display new entry boxes for creating a new Syslog server profile. The maximum number of Syslog servers to be added is "3".
Server IP	Enter the IP address of the Syslog Server.
Port	Enter the port number of the Syslog Server.
Option	**Delete** - Click it to remove the selected server profile.
Apply	Save the current settings and exit the page.

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

III-1-1-4 SNMP

This section allows you to configure settings for SNMP services.

The SNMPv3 is more secure than SNMP through the use of encryption (supports AES and DES) and authentication (supports MD5 and SHA) for the management needs.



System Maintenance / Device Settings

SNMP

Enable: enabled

SNMP service also shall be enabled for Internet access in **System Maintenance** >> Management

Manager

Manager Host: Any

Query

Get Community: public

Set Community: private

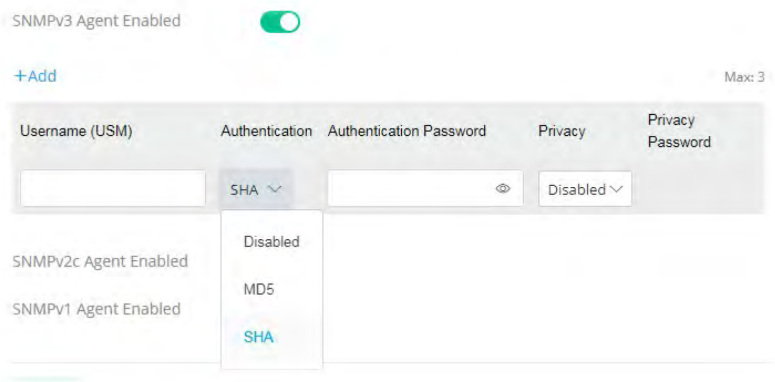
Query Port: 161

Agent

SNMPv3 Agent Enabled: enabled

Available parameters are explained as follows:

Item	Description
SNMP	
Enable	Switch the toggle to enable/disable the SNMP function. If enabled, Manager, Query, Agent and Trap settings will be valid for you to configure.
Manager	

Manager Host	**Any** - Any IP can be set as the manager host. **Specific Host** - Specify a host (IPv4 or IPv6) or hosts (both IPv4 and IPv6). Enter the IPv4 address with subnet mask / IPv6 address with specified prefix length of hosts that are allowed to issue SNMP commands. If these field are left blank, any IPv4/IPv6 LAN host is allowed to issue SNMP commands.
Query	
Get Community	Enter the Get Community string. The default setting is **public**. Devices that send requests to retrieve information using get commands must pass the correct Get Community string. The maximum allowed length is 23 characters.
Set Community	Enter the Set Community string. The default setting is **private**. Devices that send requests to change settings using set commands must pass the correct Set Community string. The maximum length of the text is 23 characters.
Query Port	Displays the port number used by the query server.
Agent	
SNMPv3 Agent Enabled	Switch the toggle to enable/disable the SNMPv3 function. If enabled, specify corresponding settings.  SNMPv3 Agent Enabled +Add Max: 3 Username (USM) Authentication Authentication Password Privacy Privacy Password SHA Disabled Disabled MD5 SHA SNMPv2c Agent Enabled SNMPv1 Agent Enabled **Username(USM)** - USM means user-based security mode. Enter the username to be used for authentication. The maximum allowed length is 23 characters. **Authentication** - Select one of the hashing methods to be used with the authentication algorithm. **Authentication Password** - Enter a password for authentication. The maximum allowed length is 23 characters. **Privacy** - Select an encryption method as the privacy algorithm. **Privacy Password** - Enter a password for privacy. The maximum allowed length is 23 characters.
SNMPv2c Agent Enabled	Switch the toggle to enable/disable the SNMPv2 function.
SNMPv1 Agent Enabled	Switch the toggle to enable/disable the SNMPv1 function.
Trap	
Enable	Switch the toggle to enable/disable the Trap function.
Trap Version	Select the trap version.

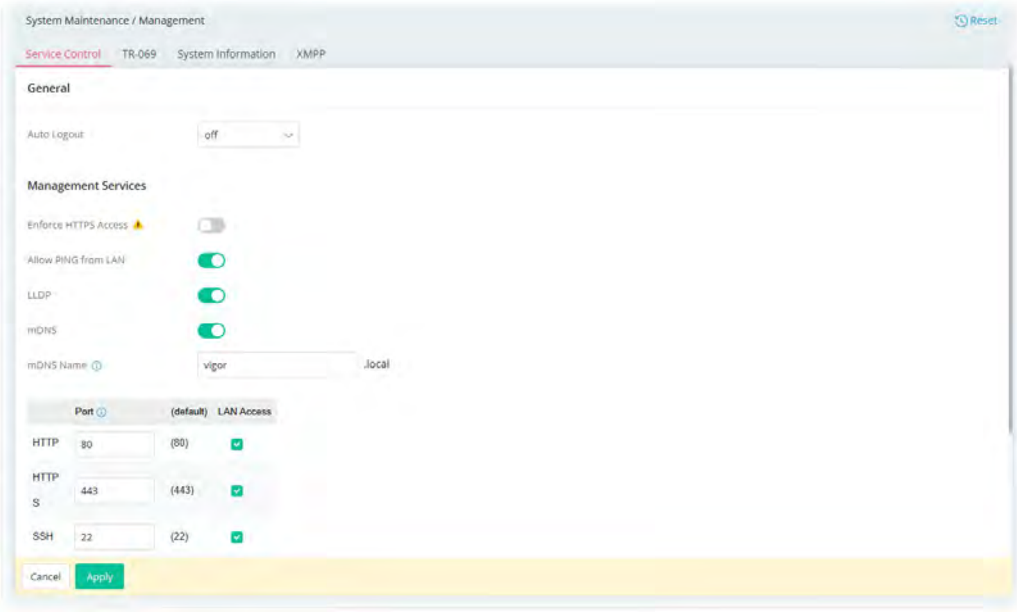
	● V1 ● V2c ● V3
Trap Community	Enter the Trap Community string. The default setting is public. Devices that send unsolicited messages to the SNMP console must pass the correct Trap Community string. The maximum length of the text is 23 characters.
Trap Port	Enter the port number used for the Trap server.
Notification Host IP Type	Select the type of the notification host. ● Both ● IPv4 ● IPv6
Notification Host(IPv4)	+Add - Enter the IPv4 address of hosts that are allowed to be sent SNMP traps.
Notification Host(IPv6)	+Add - Enter the IPv6 address of hosts that are allowed to be sent SNMP traps.
Trap Events	Select the event(s) to apply the settings configured in this page.
Apply	Save the current settings and exit the page.

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

III-1-2 Management

III-1-2-1 Service Control

This page allows you to manage the general settings, management services, and TLS/SSL Encryption setup.



General

Auto Logout: off

Management Services

Enforce HTTPS Access: off

Allow PING from LAN: on

LLDP: on

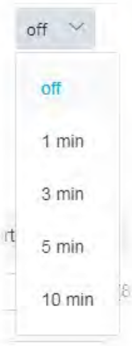
mDNS: on

mDNS Name: vigor .local

	Port	(default)	LAN Access
HTTP	80	(80)	☑
HTTPS	443	(443)	☑
SSH	22	(22)	☑

Available settings are explained as follows:

Item	Description

General	
Auto Logout	If "off" is selected, the function of auto-logout for the web user interface will be disabled. The web user interface will be open until you click the Logout icon manually.  off off 1 min 3 min 5 min 10 min
Management Services	
Enforce HTTPS Access	Switch the toggle to allow system administrators to login Vigor device via HTTPS.
Allow PING from LAN	Allow all PING packets from LAN.
LLDP	Switch the toggle to transmit the information (related to the model name, IP address, and connecting port) via LLDP to answer the inquiry from another device (e.g., the neighbor router, access point, etc.).
mDNS	Switch the toggle to enable/disable the mDNS (Multicast Domain Name System) service.
mDNS Name	Enter a name as the identity in a local network that allows communication with other devices.
Port	Specify user-defined port numbers for the HTTP, HTTPS, SSH, Telnet and SNMP servers.
LAN Access	Select the checkbox to allow system administrators to login from LAN interface.
TLS/SSL Encryption	
TLS 1.3/TLS 1.2	Switch the toggle to enable the function of TLS 1.3/1.2 if required.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

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

Note:

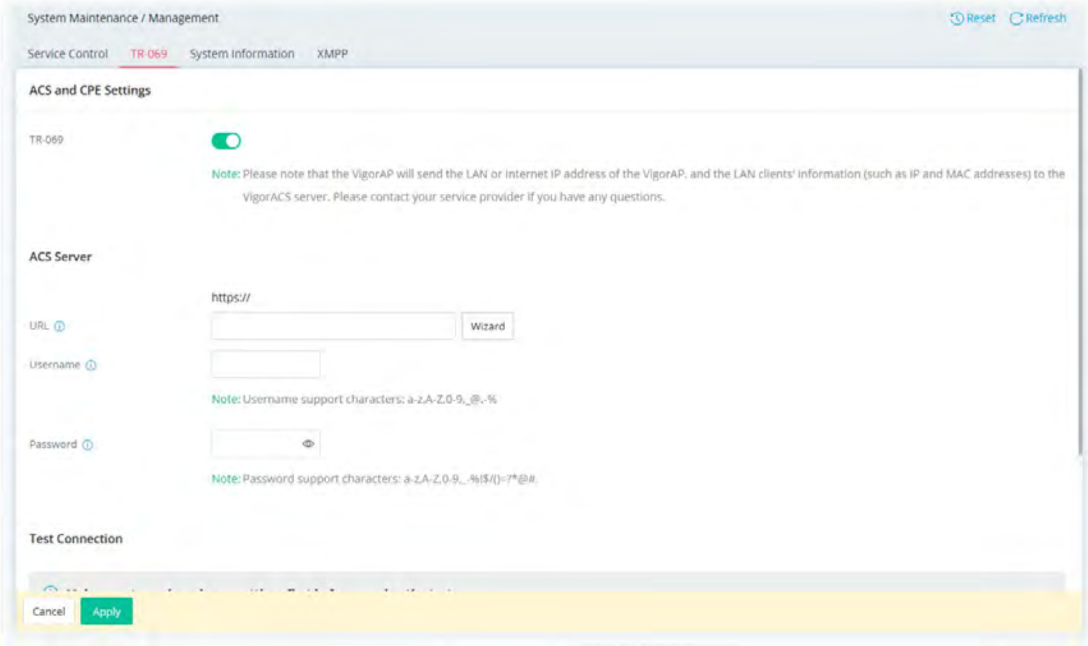
Switch these two icons by click the mouse cursor on them.

● - means “Enable”.

○ - means “Disable”.

III-1-2-2 TR-069

Vigor device supports the TR-069 standard for remote management of customer-premises equipment (CPE) through an Auto Configuration Server, such as VigorACS.



System Maintenance / Management

Reset | Refresh

Service Control | TR-069 | System Information | XMPP

ACS and CPE Settings

TR-069

Note: Please note that the VigorAP will send the LAN or Internet IP address of the VigorAP, and the LAN clients' information (such as IP and MAC addresses) to the VigorACS server. Please contact your service provider if you have any questions.

ACS Server

URL: https:// | Wizard

Username

Note: Username support characters: a-z,A-Z,0-9,_@.-%

Password

Note: Password support characters: a-z,A-Z,0-9,_-%!$/()=?*@#

Test Connection

Cancel | Apply

Available settings are explained as follows:

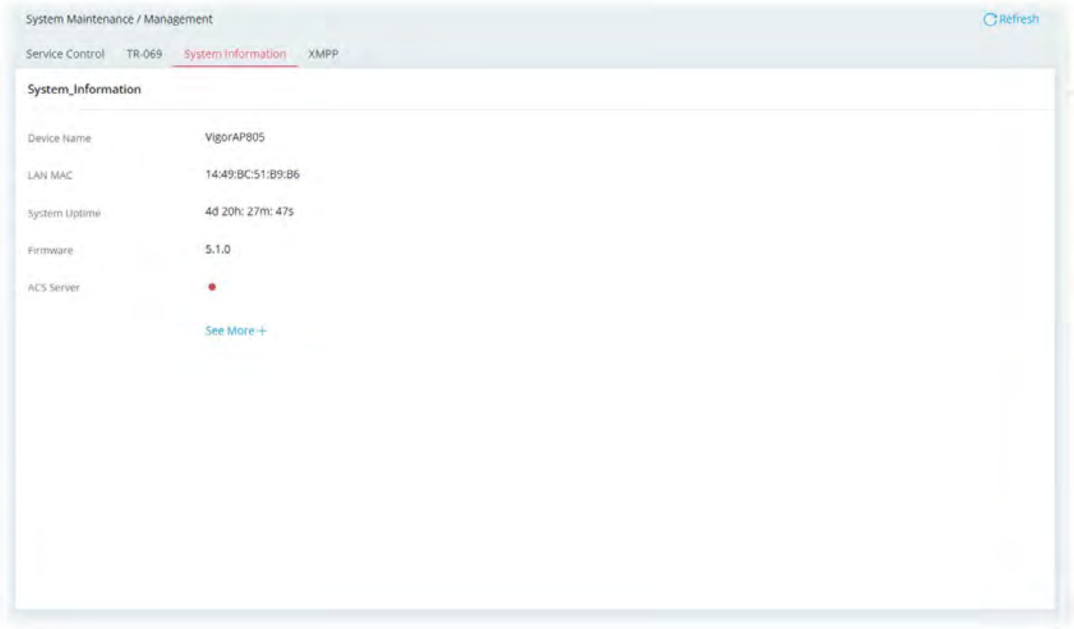
Item	Description
TR-069	Switch the toggle to enable or disable the function. If enabled, settings available for TR-069 will be shown below.
	ACS Server
URL	Enter the URL for connecting to the ACS. **Wizard** - Click it to enter the IP address of VigorACS server, port number and the handler.
Username/Password	Enter the credentials required to connect to the ACS server.
	Test Connection
Event Code	Use the drop down menu to specify an event to perform the test. **Test Connection** - Click it to send a message based on the event code selection to test if such CPE is able to communicate with VigorACS server.
	More settings
CPE Client	This section specifies the settings of the CPE Client. **Protocol** - Select Https if the connection is encrypted; otherwise select Http. **Port** - In the event of port conflicts, change the port number of the CPE. **Username / Password** - Enter the password that the VigorACS will use to connect to the CPE.
Periodic Inform Settings	**Enable / Disable** - Switch the toggle to enable or disable the function. The default setting is Enable, which means the CPE Client

	will periodically connect to the ACS Server to update its connection parameters at intervals specified in the Interval Time field. Time Interval - Set interval time or schedule time for the device to send notification to CPE.
STUN Settings	Auto / Enabled / Disabled - If you select Enabled, please enter the relational settings listed below: Server Address - Enter the IP address of the STUN server. Server STUN Port - Enter the port number of the STUN server. Minimum Keep Alive Period - If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the minimum period. The default setting is “60 seconds”. Maximum Keep Alive Period - If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the maximum period. A value of “-1” indicates that no maximum period is specified.
Apply	Save the current settings and exit the page.
Cancel	Discard current settings and return to the previous page.

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

III-1-2-3 System Information

The System Information displays basic information (e.g., device name, LAN MAC, system uptime, firmware, ACS server and etc.) of Vigor device.



System_Information

Device Name VigorAP805

LAN MAC 14:49:BC:51:B9:B6

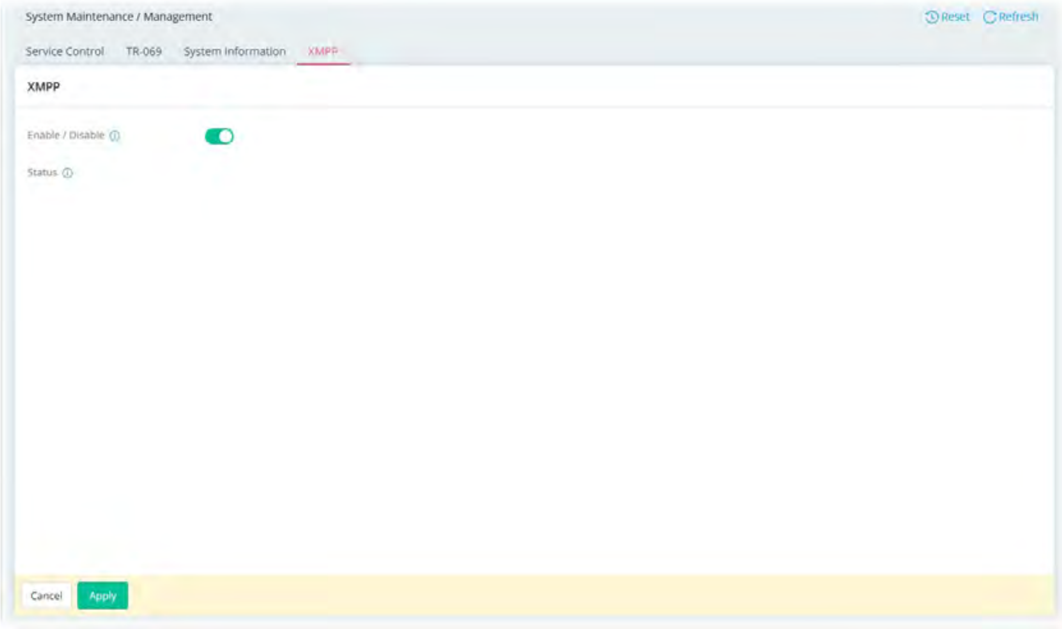
System Uptime 4d 20h: 27m: 47s

Firmware 5.1.0

ACS Server ●

III-1-2-4 XMPP

XMPP is an abbreviation of Extensible Messaging and Presence Protocol. If your access point is registered with the XMPP server, it can help VigorACS manage the access point under NAT at any time without obstruction.



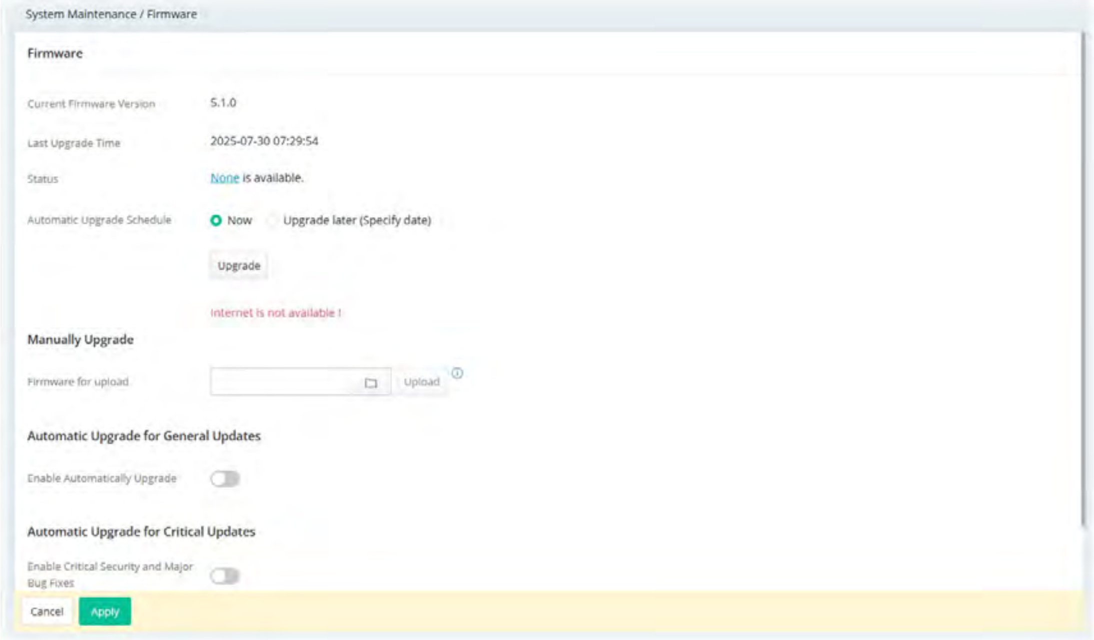
Switch the toggle of Enable/Disable to enable or disable the XMPP feature.

III-1-3 Firmware

Open System Maintenance>> System Upgrade. 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).

There are two methods to execute the firmware upgrade.

- Manual Upgrade - Before firmware upgrade, please download the newest firmware from the DrayTeks website or FTP site first. The DrayTek website is www.draytek.com (or local DrayTeks website) and the FTP site is ftp.draytek.com.
- Automatic Upgrade – The Vigor system now offers automatic firmware upgrade feature (optionally, default is disabled), making it convenient for users to stay updated on crucial firmware changes, security issues, and significant bugs that necessitate immediate firmware update. With this feature, there is no need to download the latest firmware version yourself. The Vigor system will automatically detect the latest release, download it, and upgrade the device. This option is particularly beneficial for addressing critical security issues and fixing major bugs.



System Maintenance / Firmware

Firmware

Current Firmware Version 5.1.0

Last Upgrade Time 2025-07-30 07:29:54

Status None is available.

Automatic Upgrade Schedule ● Now ○ Upgrade later (Specify date)

Upgrade

Internet is not available !

Manually Upgrade

Firmware for upload Upload

Automatic Upgrade for General Updates

Enable Automatically Upgrade

Automatic Upgrade for Critical Updates

Enable Critical Security and Major Bug Fixes

Cancel Apply

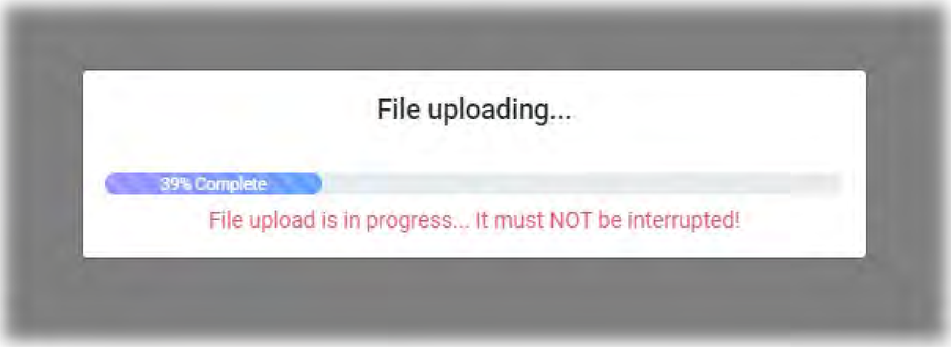
Available settings are explained as follows:

Item	Description
Current Firmware Version	Display the firmware version currently used.
Status	Upgrade Now – Click to upgrade the firmware immediately.
Automatic Upgrade Schedule	Upgrade the firmware at a specified time and date. Now – Select and click Upgrade to upgrade the firmware immediately. Upgrade later – Specify a date and time to upgrade the firmware.
Manually Upgrade	
Firmware for upload	□ - Click to locate the firmware file for upgrade.

	Upload – Click to upload the selected file onto Vigor system.
	Automatic Upgrade for General Updates
Enable Automatically Upgrade	Default is disabled. Switch the toggle to enable/disable automatic firmware upgrade within a designated time.
Upgrade Timing	Set the timing for the firmware upgrade. **In the middle of the night** – The firmware upgrade will take place at midnight. **Schedule Update** - The firmware upgrade will take place on a specified on one day and time in a week.
	Automatic Upgrade for Critical Updates
Enabled Critical Security and Major Bug Fixes	Vigor router will perform the system upgrade automatically once receiving the newly firmware with critical security and major bugs fixed information. Default is disabled. Switch the toggle to enable/disable this feature.
Upgrade Timing	Set the timing for the firmware upgrade. **In the middle of the night** – The firmware upgrade will take place at midnight. **Schedule Update** - The firmware upgrade will take place on a specified on one day and time in a week.
	Notifications
Allow Notifications	Switch the toggle to enable / disable the notification mechanism.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

Click 📁 to locate the firmware from your host.

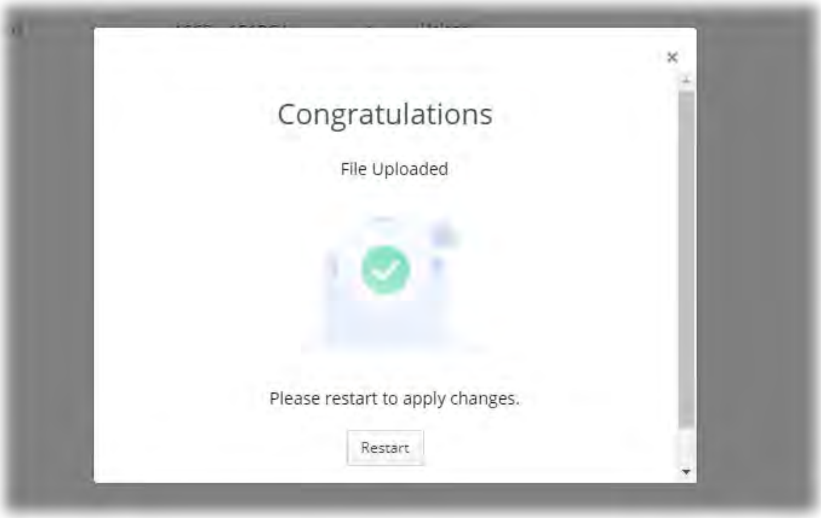
Then click **Upload** and wait for a few seconds.



File uploading...

File upload is in progress... It must NOT be interrupted!

When the upload is finished, please click the **Restart** button.

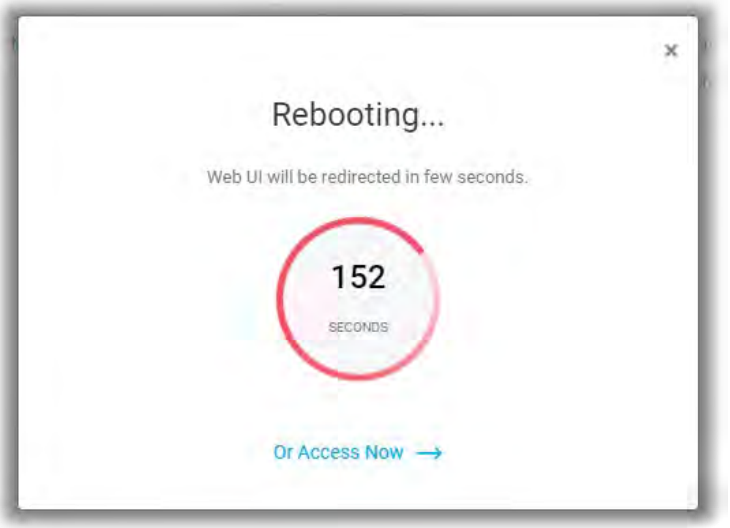


Congratulations

File Uploaded

Please restart to apply changes.

Wait for a while until the system finishes the rebooting.

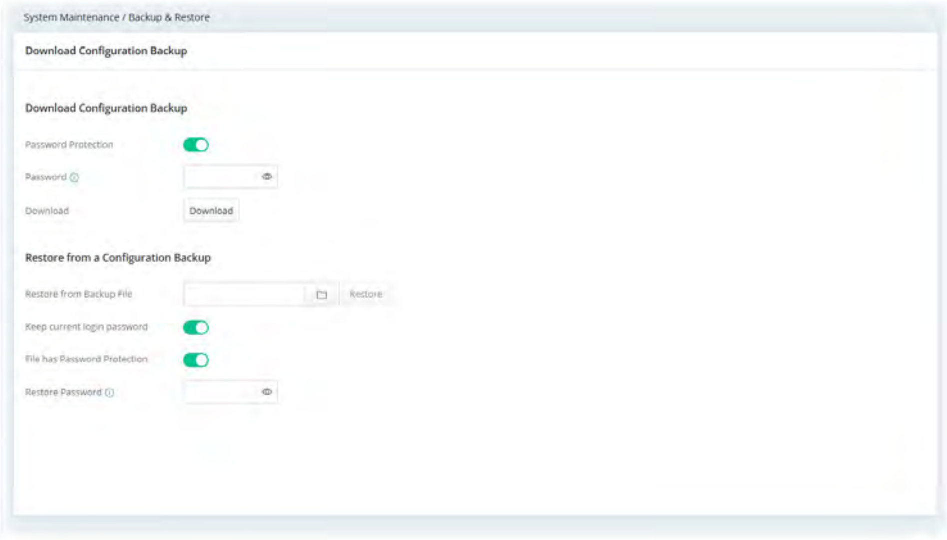


Rebooting...

Web UI will be redirected in few seconds.

III-1-4 Backup and Restore

This function can be used to backup/restore the VigorAP settings.


System Maintenance / Backup & Restore
Download Configuration Backup
Download Configuration Backup
Password Protection
Password
Download
Download
Restore from a Configuration Backup
Restore from Backup File
Restore
Keep current login password
File has Password Protection
Restore Password

Available settings are explained as follows:

Item	Description
	Download Configuration Backup
Password Protection	For the sake of security, the configuration file for the access point can be encrypted. Switch the toggle to enable or disable the function.
Password	Enter several characters as the password for encrypting the configuration file.
Download	Click it to backup the configuration file.
	Restore from a Configuration Backup
Restore from Backup File	🗀 - Click to locate the file for restoring. Restore - Click to execute the restoration.
Keep current login password	Switch the toggle to enable or disable the function.
File has Password Protection	Switch the toggle to enable or disable the function. If enabled, a password will be required for restoring the configuration.
Restore Password	Enter a password for configuration restoration.

ⓘ Note:

Switch these two icons by click the mouse cursor on them.

● - means “Enable”.

○ - means “Disable”.

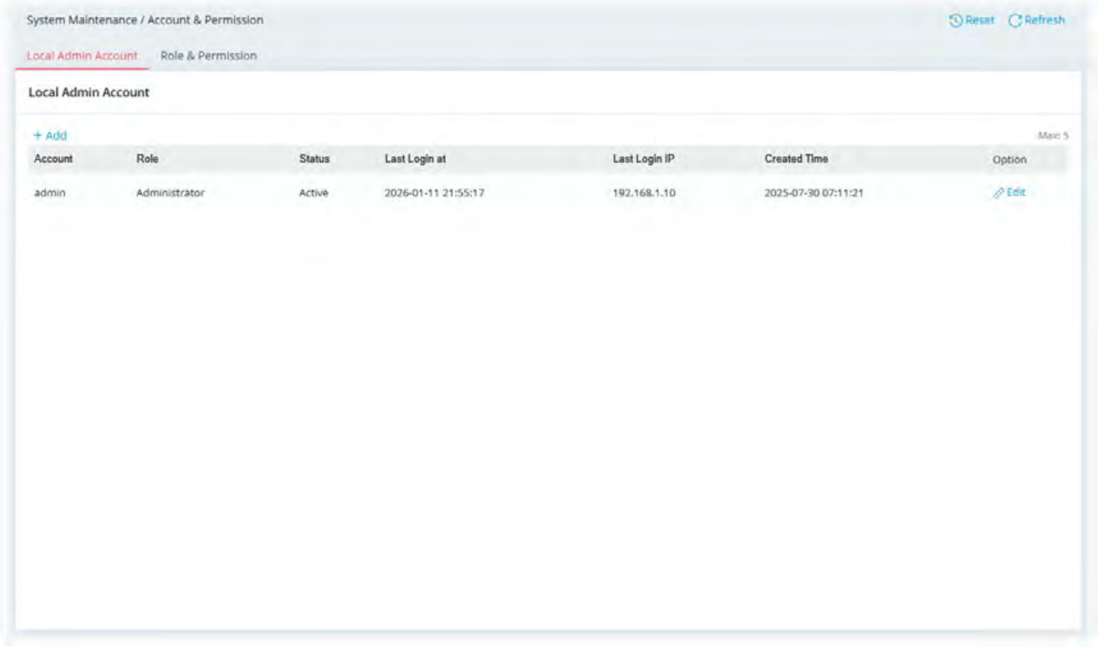
III-1-5 Accounts & Permission

This page allows you to modify current administration account and password.

It allows the network administrator to manage Internet access at the user level.

III-1-5-1 Local Admin Account

This page allows you to create up to five local admin account profiles.



Local Admin Account

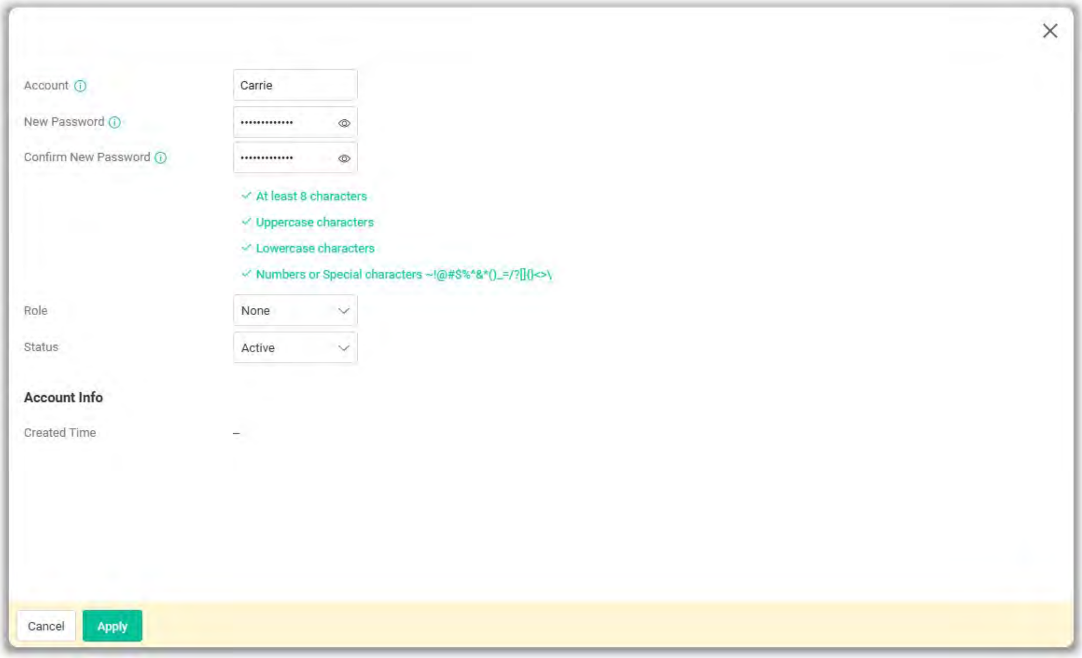
Account	Role	Status	Last Login at	Last Login IP	Created Time	Option
admin	Administrator	Active	2026-01-11 21:55:17	192.168.1.10	2025-07-30 07:11:21	Edit

Available settings are explained as follows:

Item	Description
+Add	Create a new account profile.
Edit	Modify the selected account profile.
Delete	Remove the selected account profile.

To modify an existing profile, select the one and click the **+Edit** link to open the setting page.

To add a new profile, Click **+Add**.



Account: Carrie

New Password: ••••••••••••••

Confirm New Password: ••••••••••••••

✓ At least 8 characters

✓ Uppercase characters

✓ Lowercase characters

✓ Numbers or Special characters ~!@#$%^&*()_=/?[]{}<>\

Role: None

Status: Active

Account Info

Created Time: –

Available settings are explained as follows:

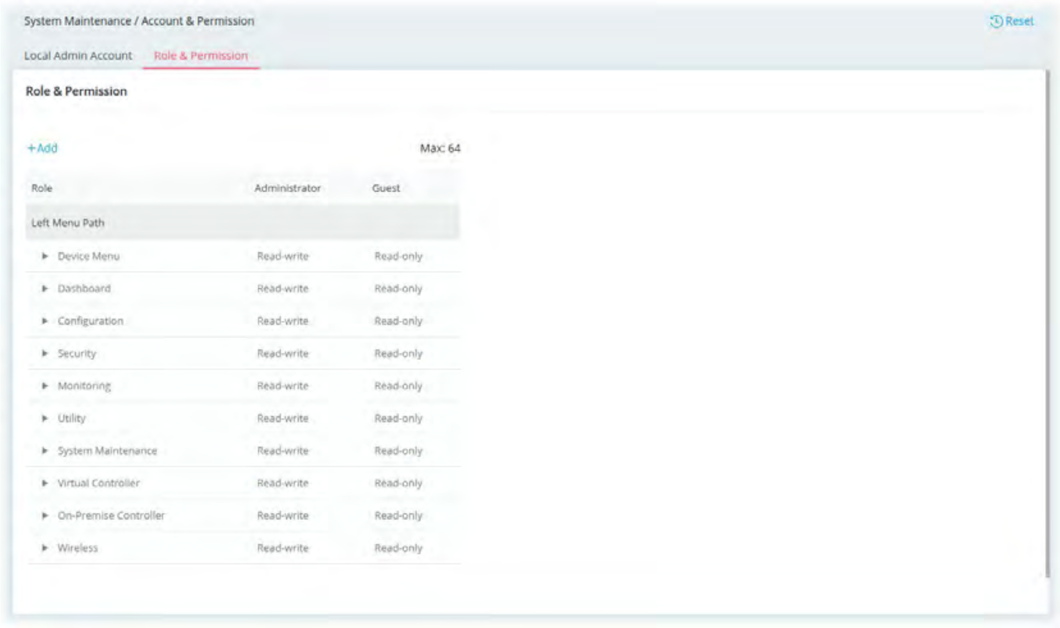
Item	Description
	Local Admin Account
Account	Display the name of the account.
New Password	Enter a new password in this field. The length of the password is limited to 83 characters.
Confirm New Password	Enter the new password again.
Role	Specify the role of the account. ● Administrator ● Guest ● User-defined role (created on the Role & Permission page)
Status	Active - Enable the selected account profile. Inactive - Disable the selected account profile.
	Account Info
Created Time	Display the created time of the user account.
Cancel	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page.

Click Apply to save the settings.

III-1-5-2 Role & Permission

This page allows to create new roles which can be applied to local admin account.

The default roles are Administrator and Guest.



Role & Permission

+Add

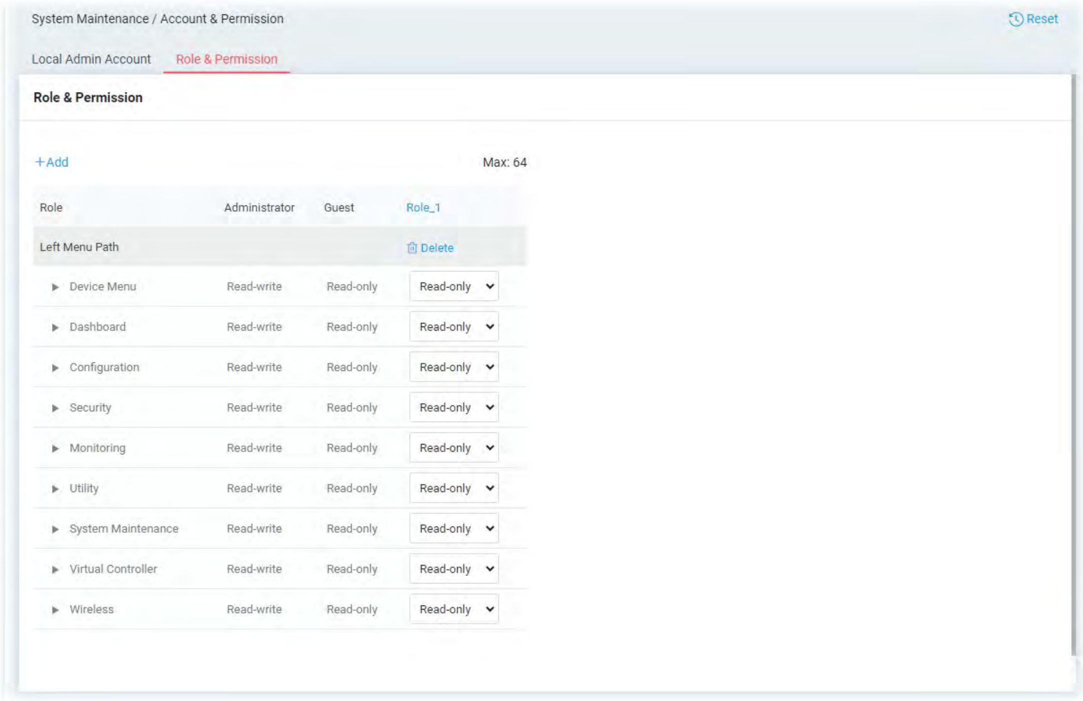
Max: 64

Role	Administrator	Guest
Left Menu Path		
▸ Device Menu	Read-write	Read-only
▸ Dashboard	Read-write	Read-only
▸ Configuration	Read-write	Read-only
▸ Security	Read-write	Read-only
▸ Monitoring	Read-write	Read-only
▸ Utility	Read-write	Read-only
▸ System Maintenance	Read-write	Read-only
▸ Virtual Controller	Read-write	Read-only
▸ On-Premise Controller	Read-write	Read-only
▸ Wireless	Read-write	Read-only

Available settings are explained as follows:

Item	Description
+Add	Create a new role profile.
Role	Lists all of the features that a role can have.

To create a new role profile, click **+Add**. A new role (named with Role_1, in this case) will be added on to the page.



System Maintenance / Account & Permission

Reset

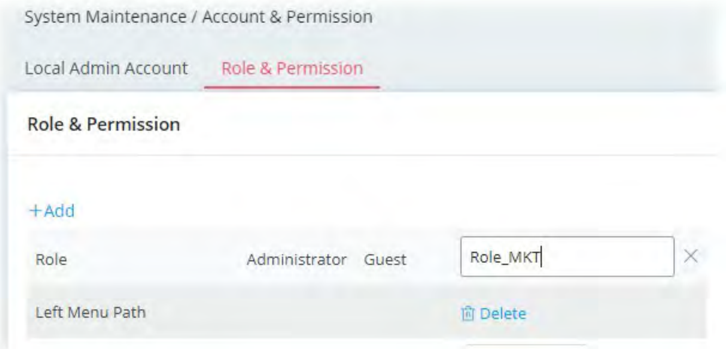
Local Admin Account | Role & Permission

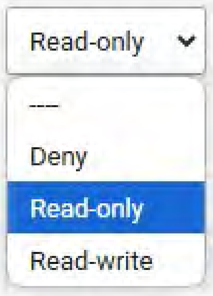
Role & Permission

+Add Max: 64

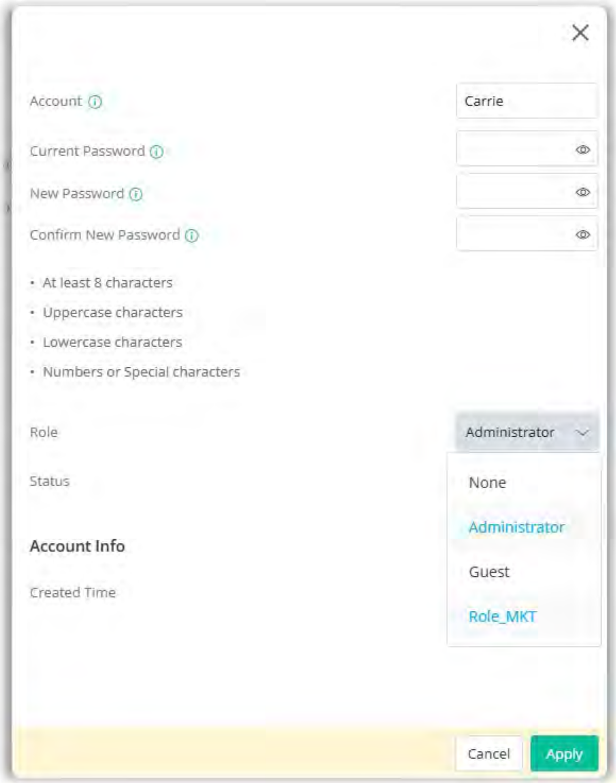
Role	Administrator	Guest	Role_1
Left Menu Path			Delete
▸ Device Menu	Read-write	Read-only	Read-only
▸ Dashboard	Read-write	Read-only	Read-only
▸ Configuration	Read-write	Read-only	Read-only
▸ Security	Read-write	Read-only	Read-only
▸ Monitoring	Read-write	Read-only	Read-only
▸ Utility	Read-write	Read-only	Read-only
▸ System Maintenance	Read-write	Read-only	Read-only
▸ Virtual Controller	Read-write	Read-only	Read-only
▸ Wireless	Read-write	Read-only	Read-only

Available settings are explained as follows:

Item	Description
+Add	Create a new role profile.
Role_1	The field of profile name. New added profile will be named as Role_#. To modify the name, simply click the name and enter a new string (e.g., Role_MKT).  System Maintenance / Account & Permission Local Admin Account | Role & Permission Role & Permission +Add Role | Administrator | Guest | Role_MKT Left Menu Path | Delete
Left Menu Path	Lists all of the features that a role can have. The role of Administrator have the highest authority for accessing VigorAP. The role of Guest have the lowest authority for accessing VigorAP. The authority of the user-defined roles must be based on the conditions selected respectively.
Delete	Remove the selected user-defined role profile.

	Specify the permission for each menu item for the user-defined role. **Deny** - The permission for the menu item on the left side is not allowed for the user-defined role profile. **Read-only** - The permission for the menu item on the left side allowed for the user-defined role profile to be read-only. **Read-write** - The permission for the menu item on the left side allowed for the user-defined role profile to be both read-only and written.
Apply	Save the current settings and exit the page.

After finished the settings, click **Apply.** The new role can be seen and selected on **System Maintenance>>Account & Permission>>Local Admin Account**.



Account ⓘ Carrie

Current Password ⓘ

New Password ⓘ

Confirm New Password ⓘ

- At least 8 characters
- Uppercase characters
- Lowercase characters
- Numbers or Special characters

Role Administrator

Status

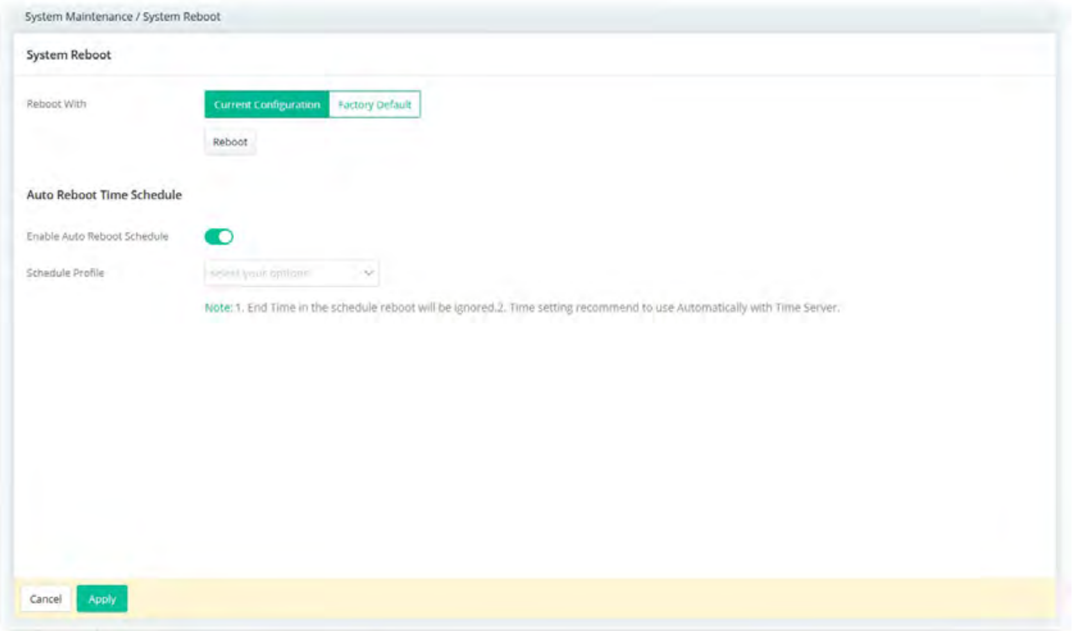
Account Info

Created Time

New role

III-1-6 System Reboot

The Web user interface may be used to restart your VigorAP. Open **System Maintenance >> System Reboot** to get the following page.



System Maintenance / System Reboot

System Reboot

Reboot With: Current Configuration | Factory Default

Reboot

Auto Reboot Time Schedule

Enable Auto Reboot Schedule: ●

Schedule Profile: select your options

Note: 1. End Time in the schedule reboot will be ignored.2. Time setting recommend to use Automatically with Time Server.

Available settings are explained as follows:

Item	Description
Reboot With	Select one of the following options, and press the **Reboot** button to reboot the VigorAP. **Current Configuration** – Select this option to reboot the VigorAP. using the current configuration. **Factory Default** – Select this option to reset the VigorAP's configuration to the factory defaults before rebooting.
Reboot	Reboot the device immediately.
Auto Reboot Time Schedule	
Enable Auto Reboot Schedule	Switch the toggle to enable/disable the auto reboot schedule.
Schedule Profile	Vigor device can perform the system reboot on a certain date and time based on the selected schedule profile.

After finished the settings, click **Apply**.

This page is left blank.

Chapter IV Others

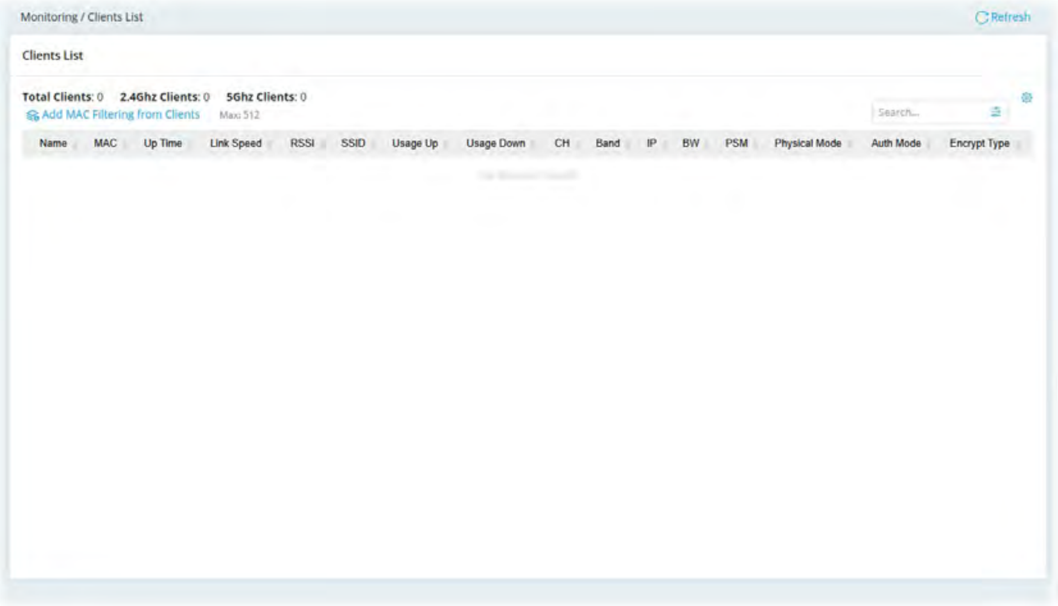
IV-1 Monitoring

IV-1-1 Clients List

It provides the information related to the wireless clients connecting to the VigorAP 805.

Clients List displays the configuration status of the wireless clients that connect to the Vigor device via Wi-Fi connection.

Besides, this page offers a quick method to add the wireless client to any existing MAC Filtering Profile.

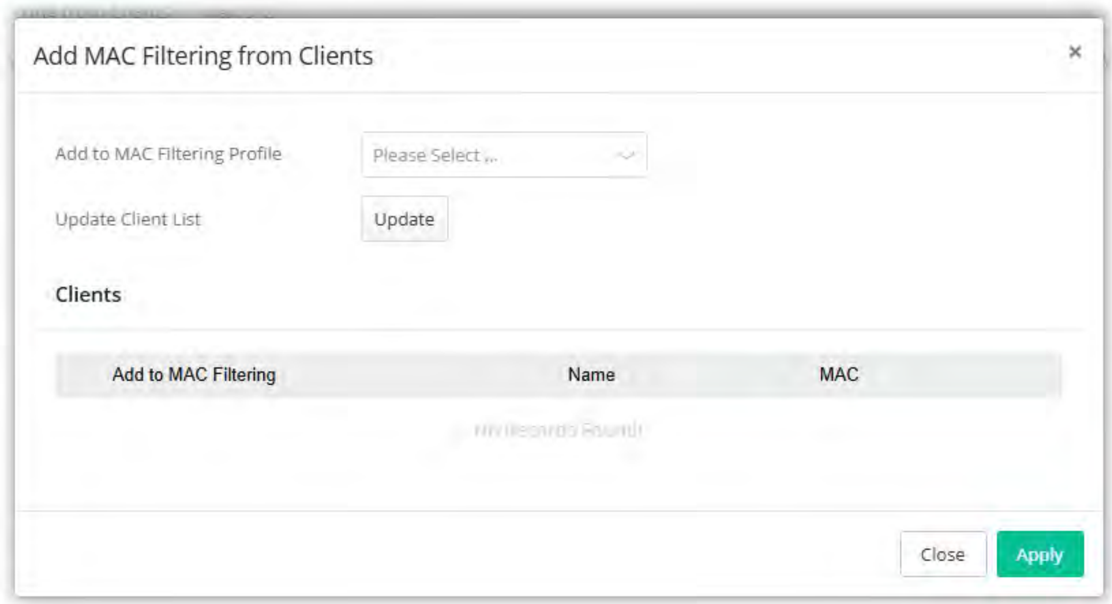


Total Clients: 0 2.4Ghz Clients: 0 5Ghz Clients: 0

Max: 512

Name	MAC	Up Time	Link Speed	RSSI	SSID	Usage Up	Usage Down	CH	Band	IP	BW	PSM	Physical Mode	Auth Mode	Encrypt Type

To add the wireless client(s) onto an existing MAC Filtering Profile, click **Add MAC Filtering from Clients** to open the following page.



Add MAC Filtering from Clients

Add to MAC Filtering Profile: Please Select ...

Update Client List: Update

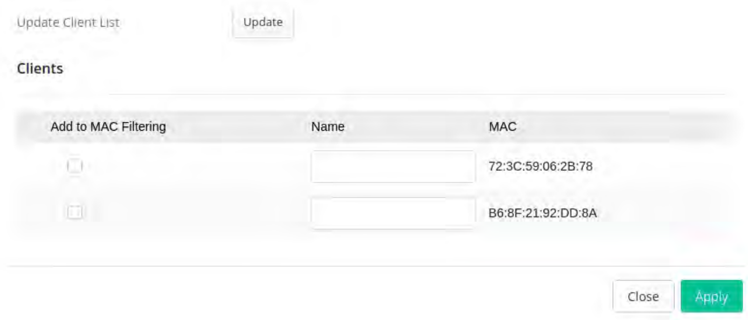
Clients

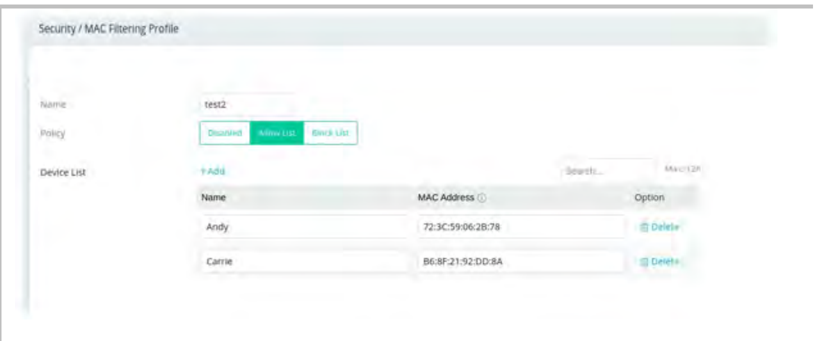
Add to MAC Filtering	Name	MAC

No Records Found!

Available settings are explained as follows:

Available settings are explained as follows:

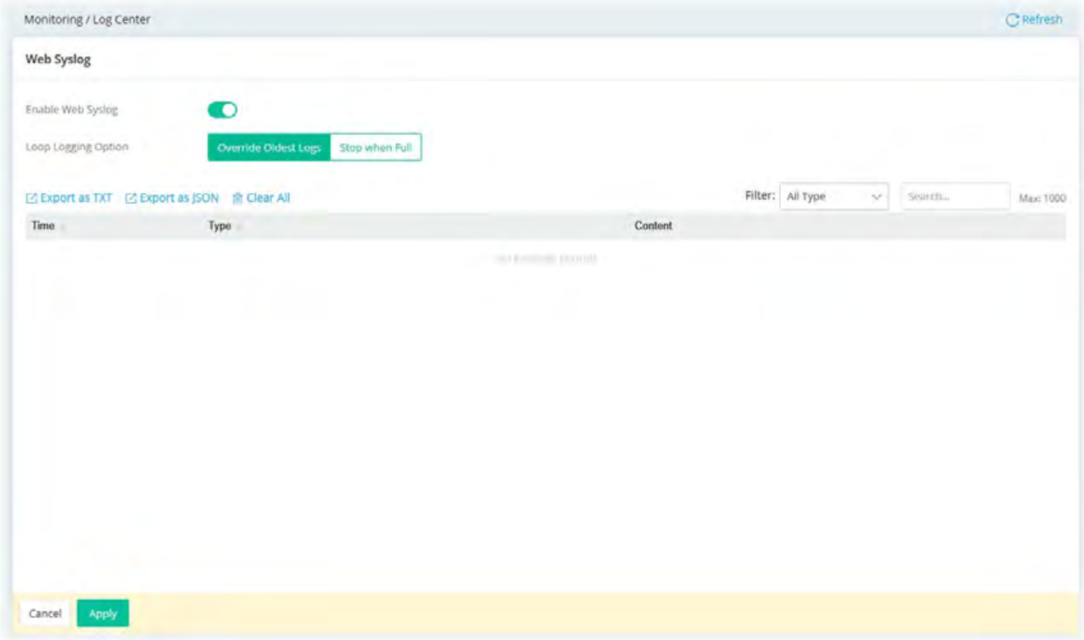
Item	Description
Add to MAC Filtering Profile	Select one of the MAC filtering profiles (Security>>MAC Filtering Profile) as the filtering basis.
Update Client List	**Update** – Click to renew the client list based on the actual wireless connection.  Update Client List: Update Clients Add to MAC Filtering / Name / MAC □ / 72:3C:59:06:2B:78 □ / B6:8F:21:92:DD:8A Close / Apply
Clients	Displays the SSID name, MAC address, and IP address of the wireless clients. **Add to MAC Filtering** – Select to make the wireless client join the MAC Filtering Profile set above. **Name** – Enter a name for identification.
Close	Discard current settings and return to the previous page.
Apply	Save the current settings and exit the page. To check if the new added wireless clients on the MAC Filtering profile or not, refer to Security>>MAC Filtering Profile.

	 Security / MAC Filtering Profile Name: test2 Policy: Disabled / [✓ Allow List] / Block List Device List: + Add — Search... — Max:128 Name / MAC Address / Option Andy / 72:3C:59:06:2B:78 / Delete Carrie / B6:8F:21:92:DD:8A / Delete

Click **Apply** to save the settings.

IV-1-2 Log Center

Log related to setting configuration and/or actions performed by this device can be stored on web Syslog. Click **Refresh** to reload this page with the most up-to-date information.



Monitoring / Log Center

Refresh

Web Syslog

Enable Web Syslog: ●

Loop Logging Option: [✓ Override Oldest Logs] Stop when Full

Export as TXT | Export as JSON | Clear All

Filter: All Type | Search... | Max: 1000

Time	Type	Content

Cancel | Apply

Available settings are explained as follows:

Item	Description
Enabled Web Syslog	Switch the toggle to enable or disable the function. If enabled, **Loop Logging Option** will be shown as follows.
Loop Logging Option	**Override Oldest Logs** - Vigor router system will backup all existed information on the flash onto the host and clean up the information from the flash. Later, it will start a new record. **Stop when Full** - Vigor router system will stop to record the user information onto the flash.
Export	Click it to export the log records as a file (.txt, .json).
Clear All	Click it to clear all log records on this page.
Filter	Select the type of log to display on this page.
Cancel	Discard current settings and return to the previous page.

Apply	Save the current settings and exit the page.

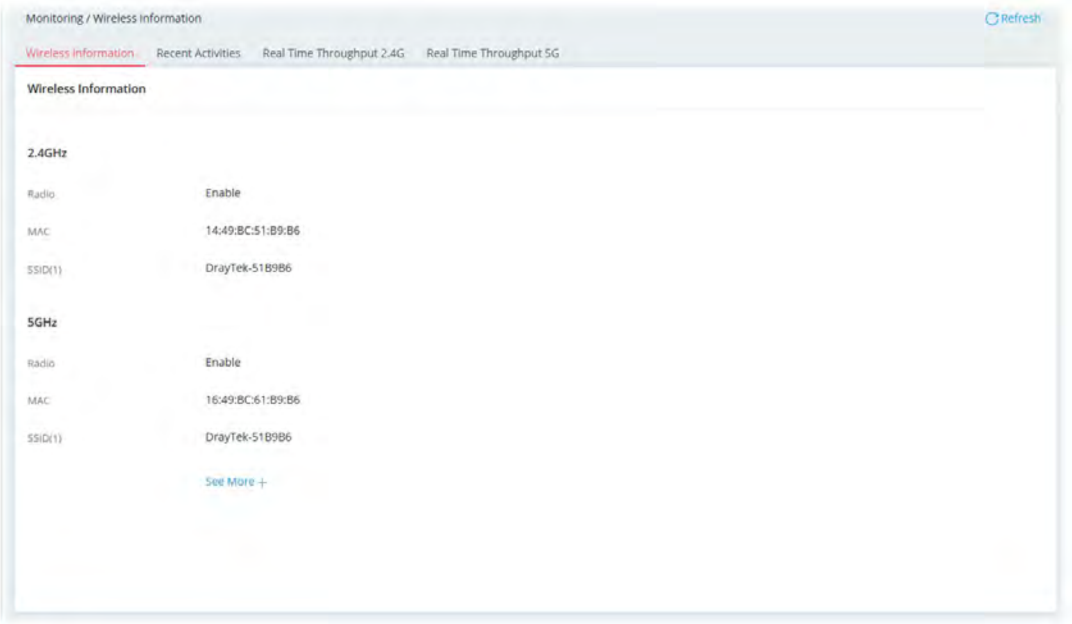
Click Apply to save the settings.

IV-1-3 Wireless Information

For viewing the SSIDs used by 2.4GHz/5GHz or real time throughput for 2.4GHz/5GHz, open Monitoring>>Wireless Information for detailed.

IV-1-3-1 Wireless Information

This page shows general information (e.g., 2.4GHz/5GHz enabled or not, MAC address, SSID name and etc.) for wireless connection.



Wireless Information

2.4GHz

Radio	Enable
MAC	14:49:BC:51:B9:B6
SSID(1)	DrayTek-51B9B6

5GHz

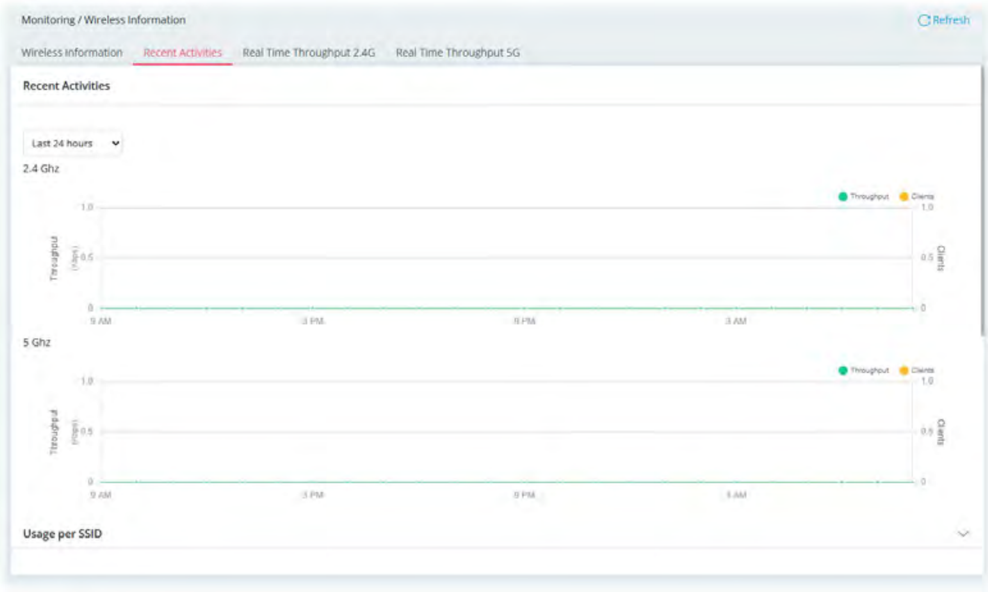
Radio	Enable
MAC	16:49:BC:61:B9:B6
SSID(1)	DrayTek-51B9B6

Click **Refresh** to reload this page with the most up-to-date information.

Click **See More+** to view more information.

IV-1-3-2 Recent Activities

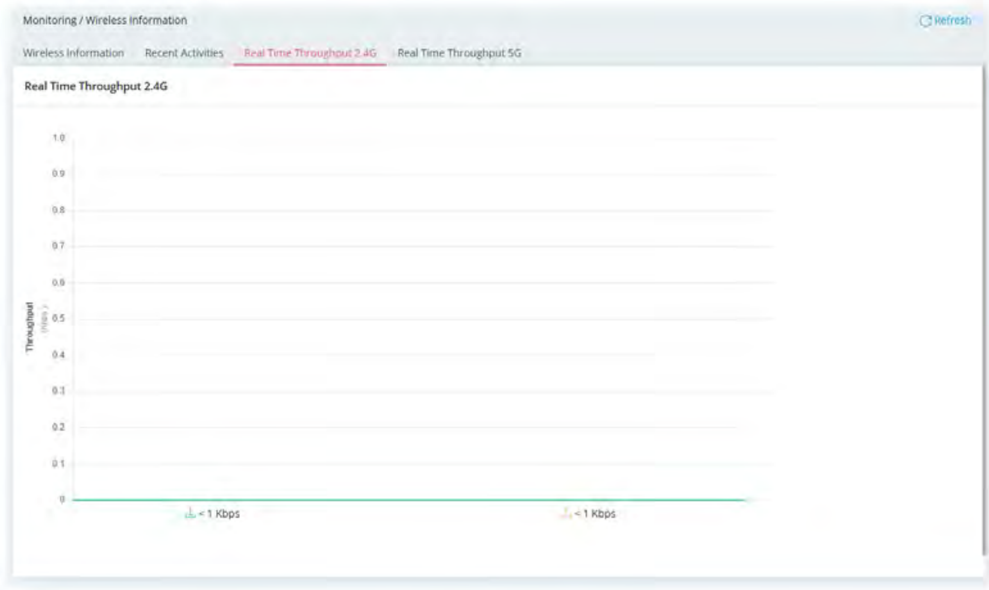
The activities regarding to wireless network can be shown with line graphs.



Click **Refresh** to reload this page with the most up-to-date information.

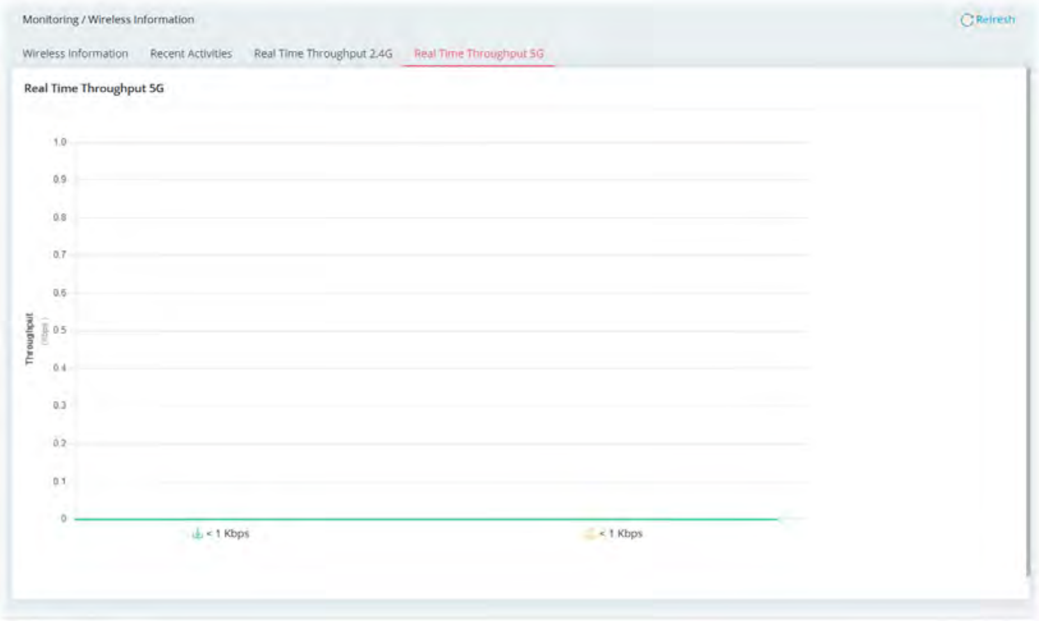
IV-1-3-3 Real Time Throughput 2.4G

The real-time throughput (2.4G) can be shown with line graphs.



IV-1-3-4 Real Time Throughput 5G

The real-time throughput (5G) can be shown with line graphs.

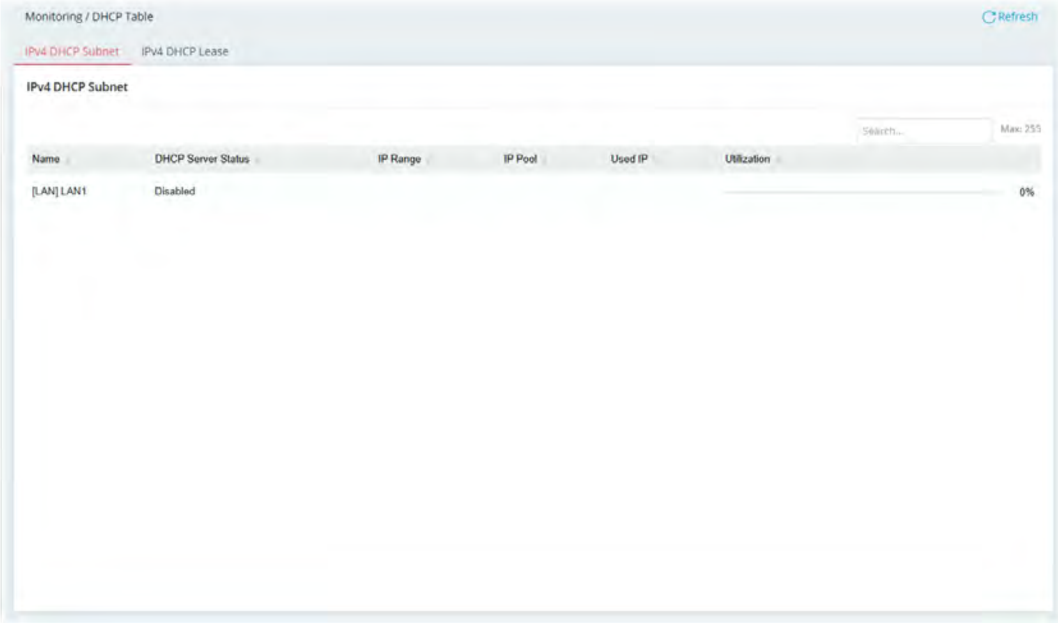


IV-1-4 DHCP Table

This page provides information on IP address assignments. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.

Click **Refresh** to reload this page with the most up-to-date information.

IV-1-4-1 IPv4 DHCP Subnet

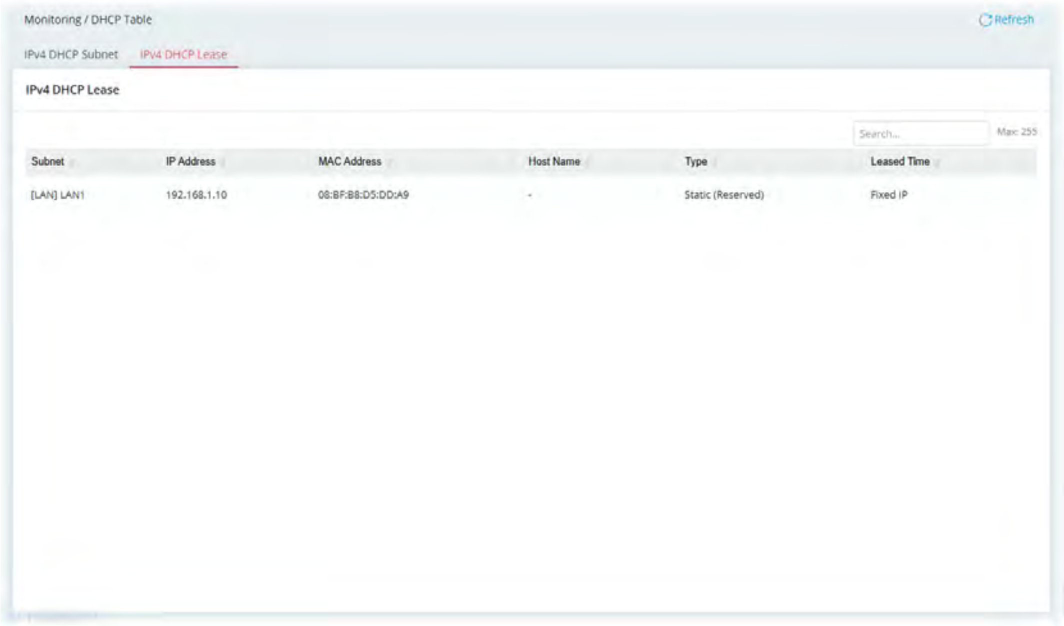


IPv4 DHCP Subnet

Name	DHCP Server Status	IP Range	IP Pool	Used IP	Utilization
[LAN] LAN1	Disabled				0%

IV-1-4-2 IPv4 DHCP Lease

This page shows the remaining time of the IPv4 DHCP lease of the device.



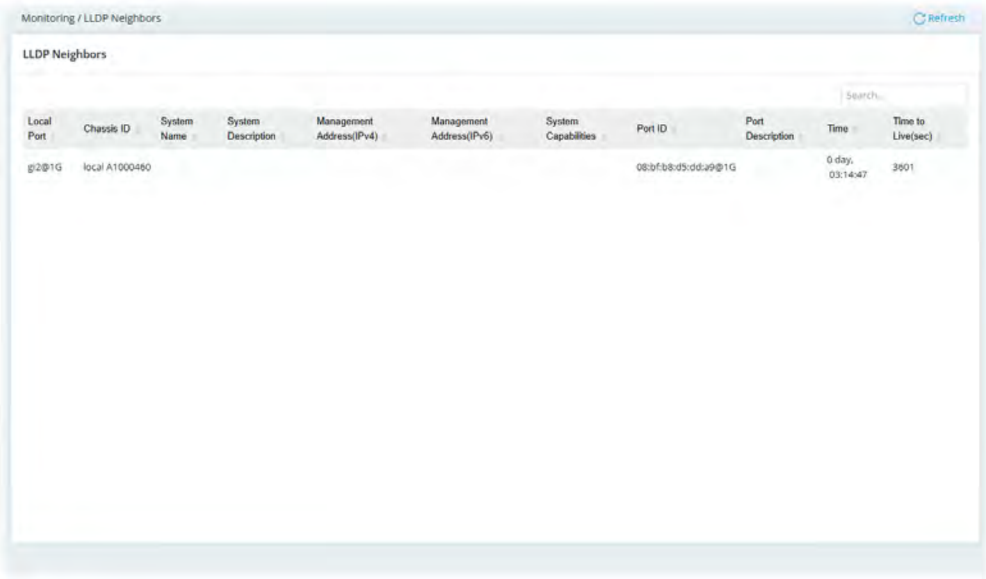
IPv4 DHCP Lease

Subnet	IP Address	MAC Address	Host Name	Type	Leased Time
[LAN] LAN1	192.168.1.10	08:BF:B8:D5:DD:A9	-	Static (Reserved)	Fixed IP

IV-1-5 LLDP Neighbors

This page allows the system administrator to understand the topology of network devices and the relationships between devices. Usually, information includes:

- System name
- System Description
- IPv4/IPv6 address (optional)
- Port ID
- Port Description
- Time
- Time to Live

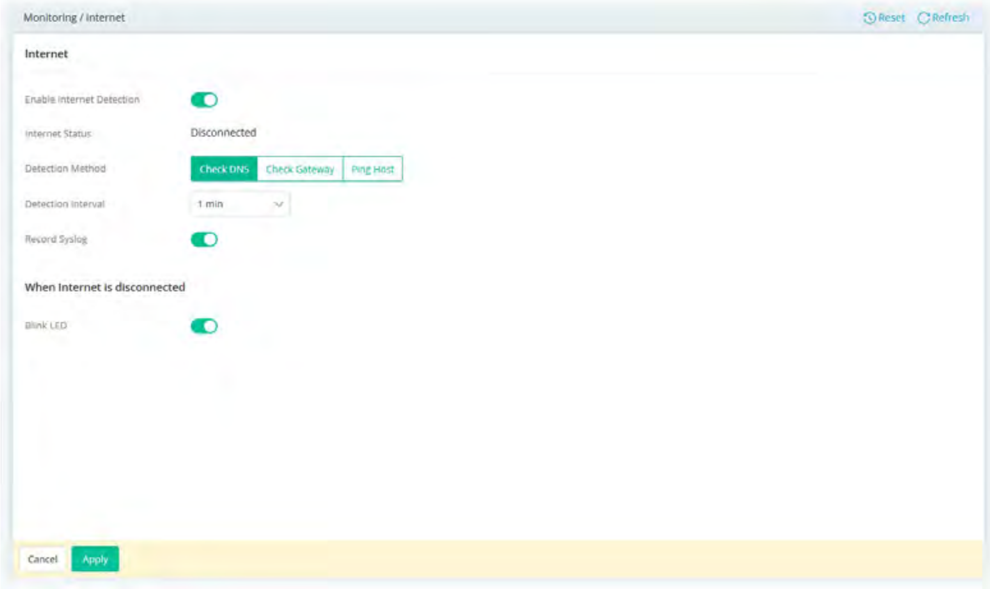


LLDP Neighbors

Local Port	Chassis ID	System Name	System Description	Management Address(IPv4)	Management Address(IPv6)	System Capabilities	Port ID	Port Description	Time	Time to Live(sec)
gi2@1G	local A1000460						08:bf:b8:d5:dd:a9@1G		0 day, 03:14:47	3601

IV-1-6 Internet

This feature can help users realize whether the internet is disconnected.



Internet

Enable Internet Detection: on

Internet Status: Disconnected

Detection Method: Check DNS | Check Gateway | Ping Host

Detection Interval: 1 min

Record Syslog: on

When Internet is disconnected

Blink LED: on

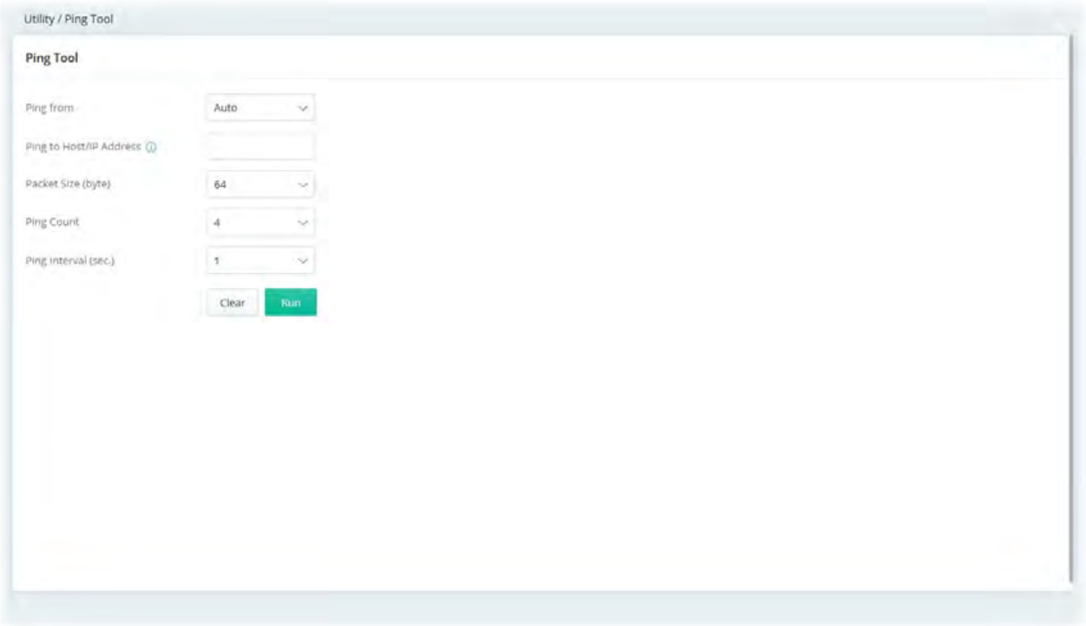
Available settings are explained as follows:

Item	Description
Enable Internet Detection	Switch the toggle to enable or disable the feature of Internet detection.
Internet Status	Display current Internet status (e.g., N/A, Connected, Connected [WAN IP=xxx.xxx.xxx.xxx] and Disconnected).
Detection Method	Vigor system provides three types of detection method. ● Check DNS ● Check Gateway ● Ping Host If Ping Host is selected, enter the Vigor system's Host IP address to perform the detection work.
Detection Interval	VigorAP device will detect the Internet connection with the interval (10 sec, 1 min, 10 min and 30 min) selected here.
Record Syslog	Switch the toggle to enable or disable the feature. If this feature is enabled, information about Internet disconnections will be recorded in the SysLog.
Blink LED	Switch the toggle to enable or disable the feature. When the ACT LED blinks twice and then pauses for one second repeatedly, it indicates that the Internet connection is disconnected.
Cancel	Discard current settings.
Apply	Save the current settings.

IV-2 Utility

IV-2-1 Ping Tool

The user can perform the ping job for specified IP (host) to diagnose if the data transmission via the Vigor system is well or not.



Utility / Ping Tool

Ping Tool

Ping from: Auto

Ping to Host/IP Address ⓘ:

Packet Size (byte): 64

Ping Count: 4

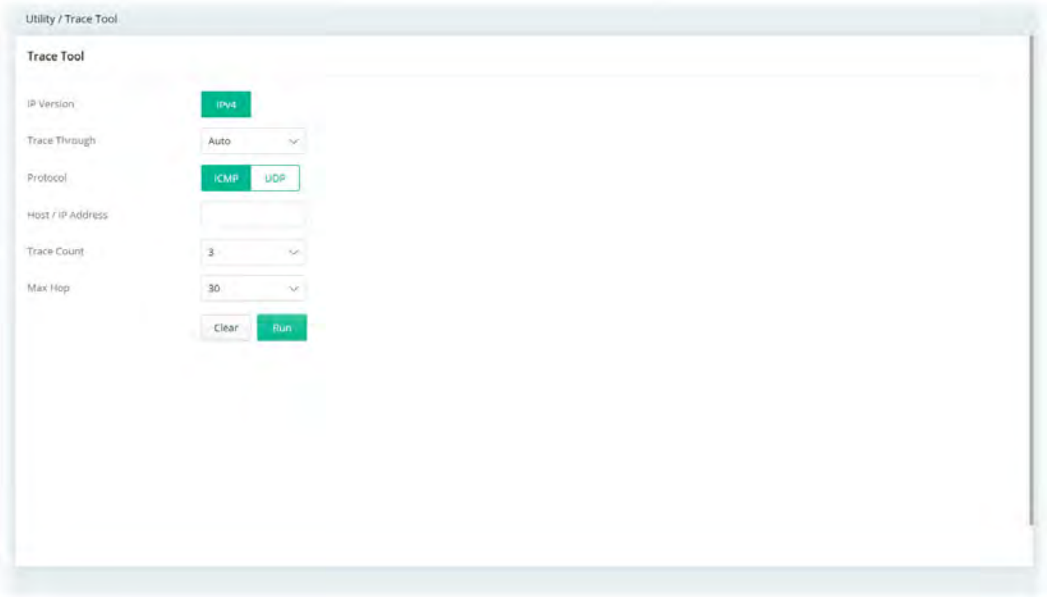
Ping Interval (sec.): 1

Available settings are explained as follows:

Item	Description
Ping from	Choose **Auto** for the router to select the WAN interface.
Ping to Host/IP Address	Enter the host / IP address that you want to ping.
Packet Size (byte)	Select the packet size for the ping job.
Ping Count	Select the quantity of the packet being pinged.
Ping Interval (sec.)	Select a time interval (unit:second) for the system to ping the IP address specified above.
Clear	Remove the settings and return to the factory settings.
Run	Perform the ping job.

IV-2-2 Trace Tool

The user can perform the traceroute job for specified IP (host) to diagnose if the data transmission via the Vigor system is well or not.



Utility / Trace Tool

Trace Tool

IP Version	IPv4
Trace Through	Auto
Protocol	ICMP UDP
Host / IP Address	
Trace Count	3
Max Hop	30

Available settings are explained as follows:

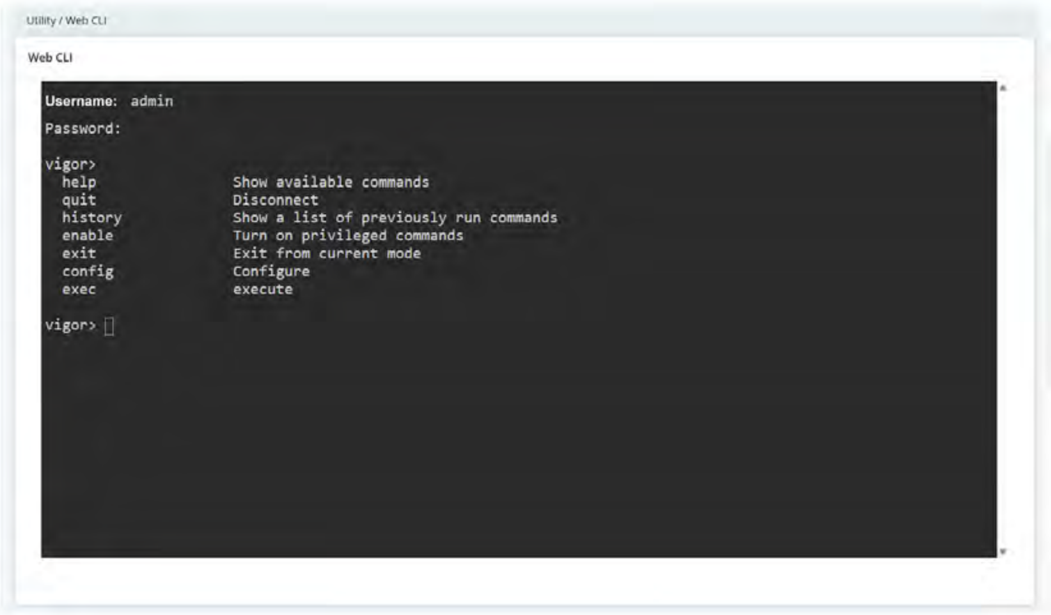
Item	Description
IP Version	Select the IP version. At present, only IPv4 is available for selection.
Trace Through	Trace through specific interface. Only Auto is available for selection.
Protocol	Select ICMP or UDP protocol.
Host/IP Address	Enter the host / IP address that you want to traceroute.
Trace Count	Select the max hops for traceroute, select none for unlimited.
Max Hop	Set the maximum number of hops to search for the target.
Clear	Remove the settings and return to the factory settings.
Run	Perform the ping job.

IV-2-3 Web CLI

It is not necessary to use the telnet command via DOS prompt. The changes made by using web console have the same effects as modified through web user interface. The functions/settings modified under Web Console also can be reviewed on the web user interface.

Click the Web Console icon on the top of the main screen to open the following screen.

Open the page of Utility>>Web CLI.



```
Username:  admin
Password:

vigor>
  help                 Show available commands
  quit                 Disconnect
  history              Show a list of previously run commands
  enable               Turn on privileged commands
  exit                 Exit from current mode
  config               Configure
  exec                 execute

vigor> 
```

Chapter V Mobile APP, DrayTek Wireless

V-1 Introduction of DrayTek Wireless

VigorAP 805 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.

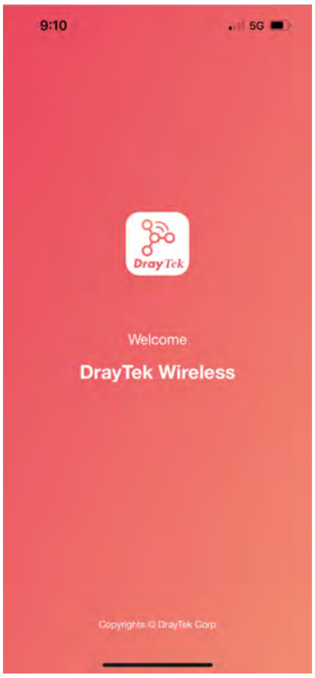
ⓘ Note:

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.



9:10

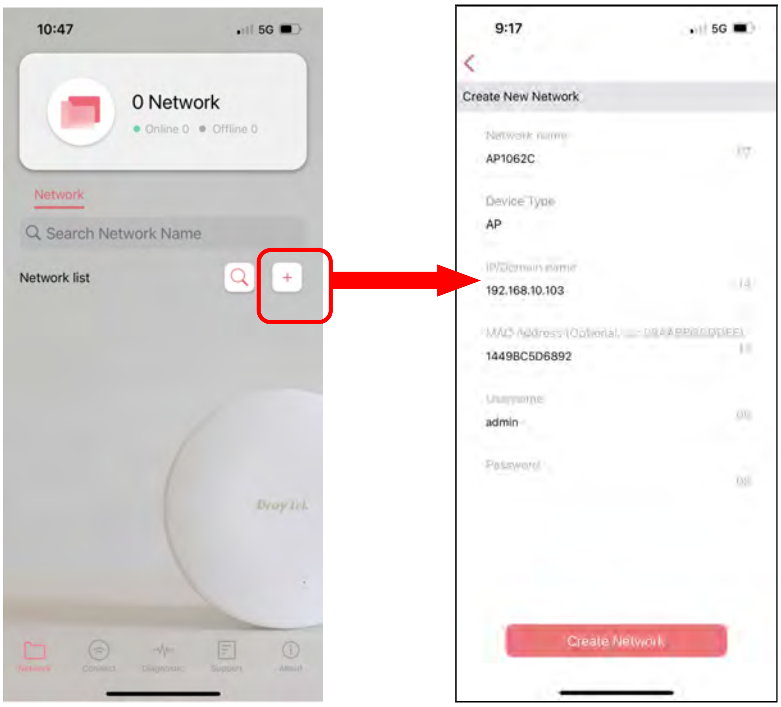
Welcome

DrayTek Wireless

Copyrights © DrayTek Corp

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.



10:47

0 Network

Online 0 · Offline 0

9:17

Create New Network

Network name
AP1062C

Device Type
AP

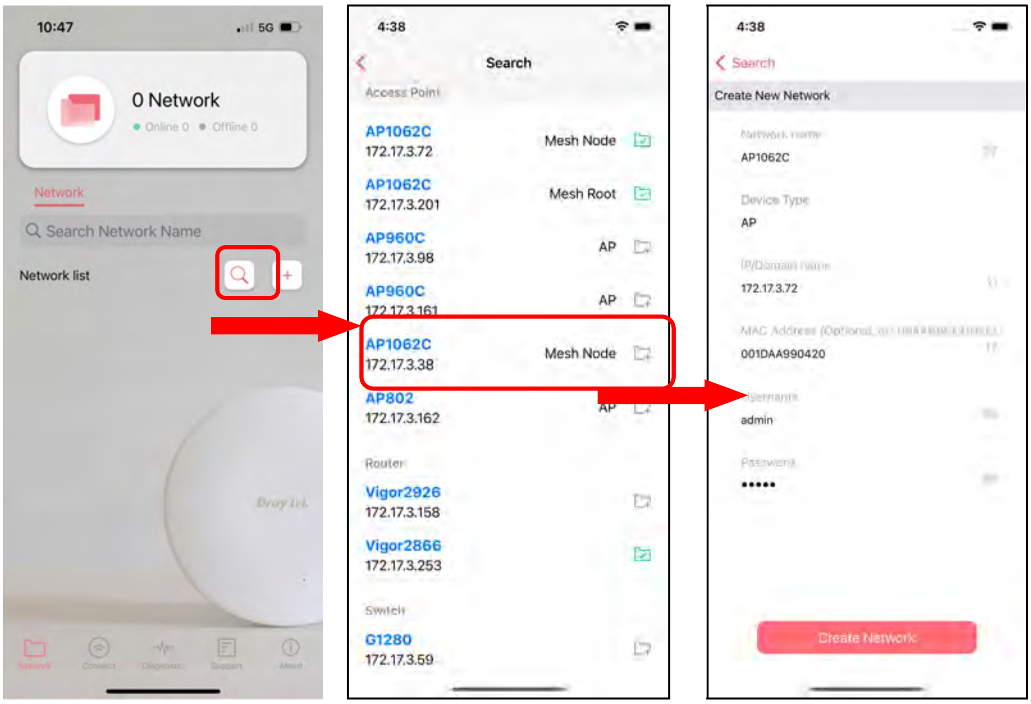
IP/Domain name
192.168.10.103

MAC Address (Optional, ... AABBCCDDEEFF)
1449BC5D6892

Username
admin

Password

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.



10:47

0 Network

Online 0 Offline 0

Network

Search Network Name

Network list

4:38

Search

Access Point

AP1062C 172.17.3.72 Mesh Node

AP1062C 172.17.3.201 Mesh Root

AP960C 172.17.3.98 AP

AP960C 172.17.3.161 AP

AP1062C 172.17.3.38 Mesh Node

AP802 172.17.3.162 AP

Router

Vigor2926 172.17.3.158

Vigor2866 172.17.3.253

Switch

G1280 172.17.3.59

4:38

Search

Create New Network

Network name: AP1062C

Device Type: AP

IP/Domain name: 172.17.3.72

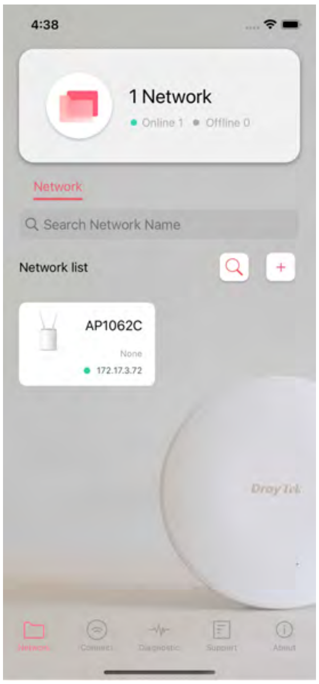
MAC Address (Optional): 001DAA990420

Username: admin

Password: •••••

Create Network

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



4:38

1 Network

Online 1 Offline 0

Network

Search Network Name

Network list

AP1062C

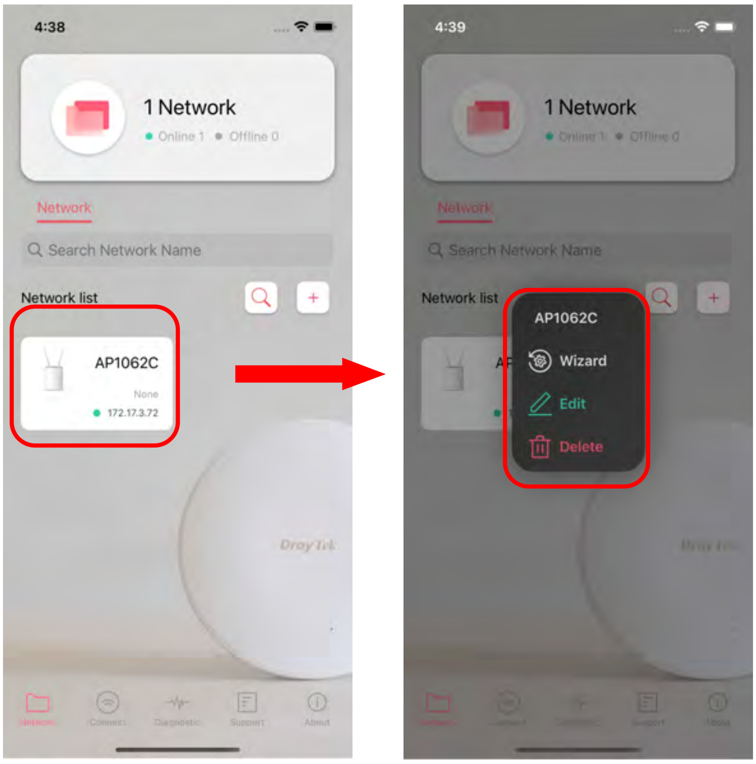
None

172.17.3.72

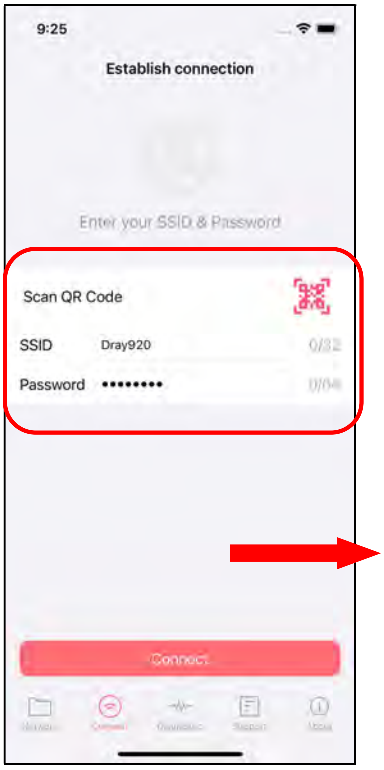
V-3 Wizard

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

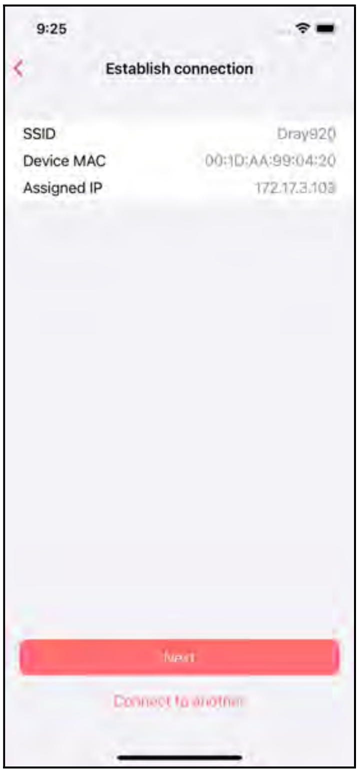
1. Click and hold the network item till available actions (**Wizard, Edit** and **Delete**) shown on the screen. Select and click **Wizard**.



2. On the next page, enter the SSID and the password for VigorAP and click **Connect.** When a summary page appears, click the **Next** button.

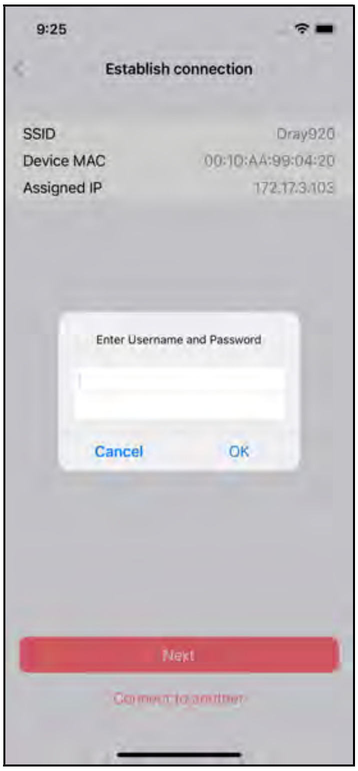


SSID Dray920 0/32
Password •••••••• 0/64

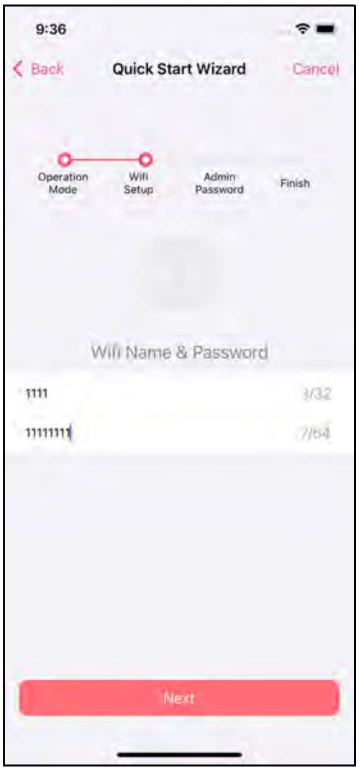


SSID Dray920
Device MAC 00:1D:AA:99:04:20
Assigned IP 172.17.3.103

3. Enter the username and the password of VigorAP, click **OK**. On the WiFi Name & Password page, define the WiFi Name and the Password. Then click the **Next** button.

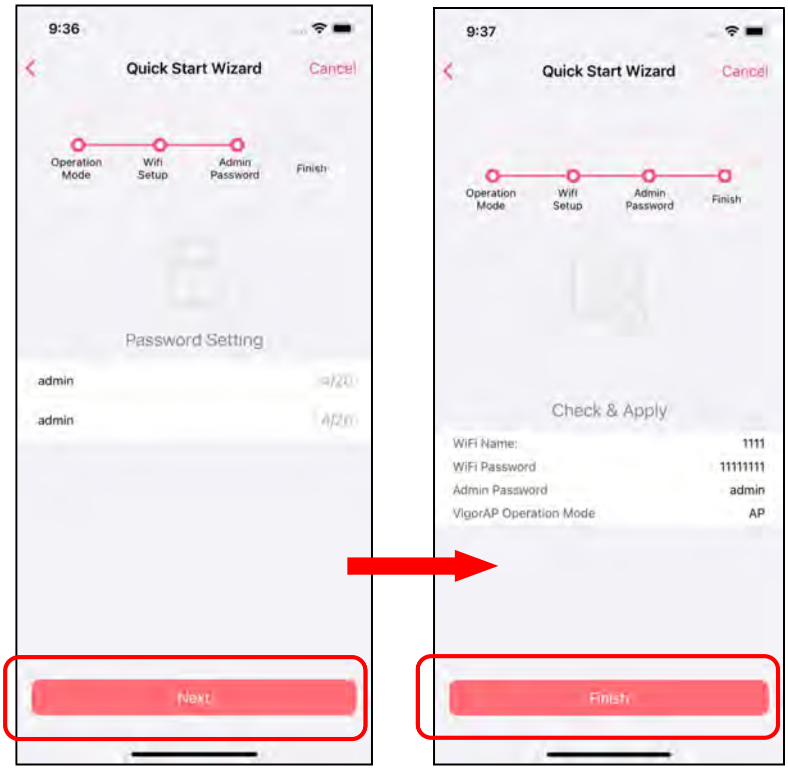


SSID Dray920
Device MAC 00:1D:AA:99:04:20
Assigned IP 172.17.3.103



1111 3/32
11111111 7/64

4. 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.



admin 4/20

admin 4/20

WiFi Name: 1111

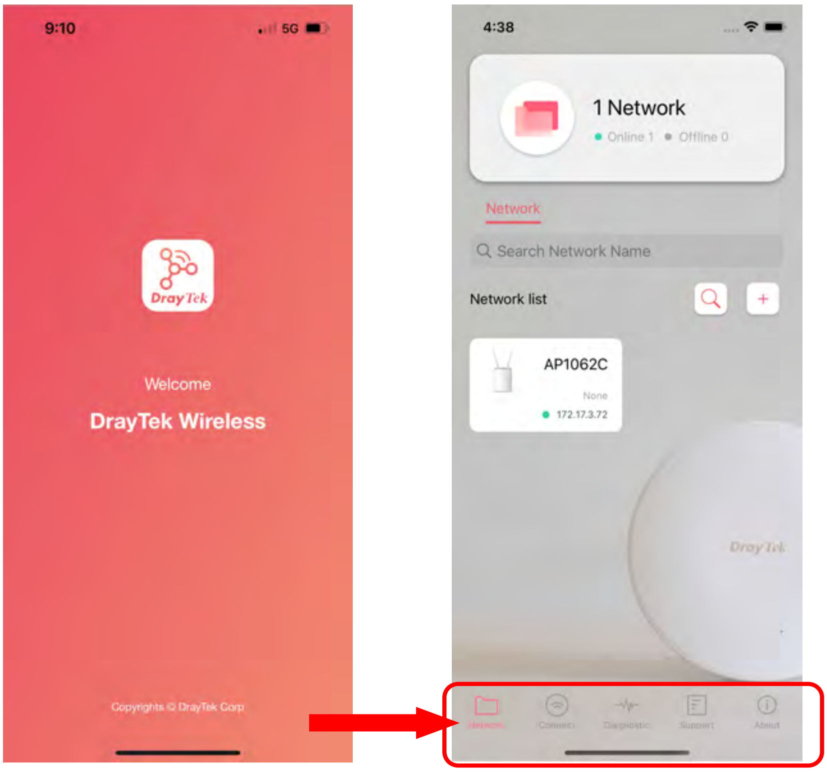
WiFi Password 11111111

Admin Password admin

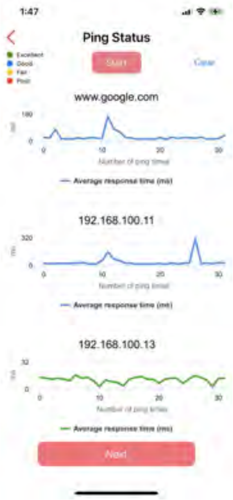
VigorAP Operation Mode AP

V-4 Login

Run DrayTek Wireless APP.



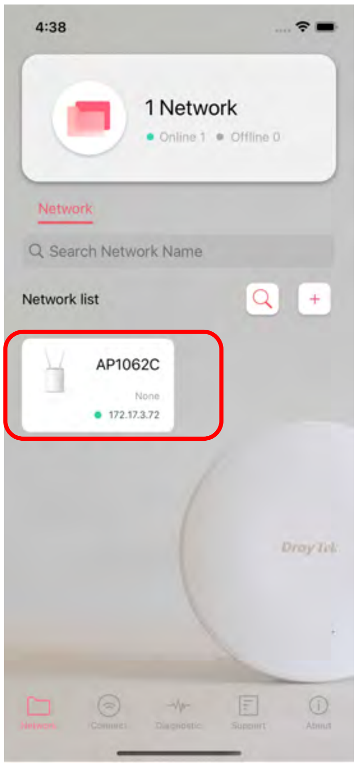
Available settings are explained as follows:

Item	Description
Network	Create a new network.
Connect	Connect to a device (AP/CPE).
Diagnostic	Analyze the current Wi-Fi network to check the network quality.  1:47 Ping Status Excellent Good Fair Poor Start Clear www.google.com 192.168.100.11 192.168.100.13 Next
Support	Display a list of models supported by this APP.

About	Display the version information of this APP.

V-4-1 Setup

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


4:38

1 Network

Online 1 · Offline 0

Network

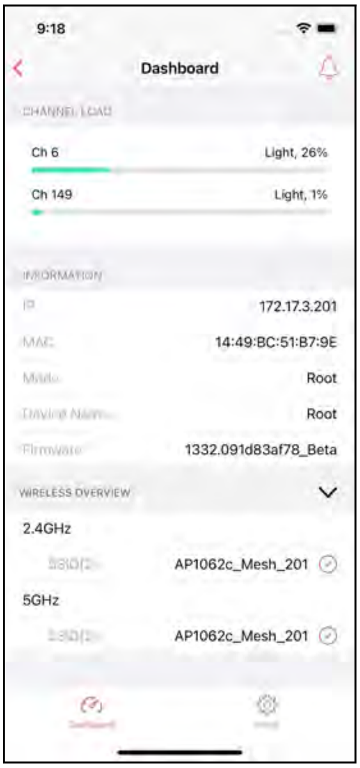
Search Network Name

Network list

AP1062C

None

172.17.3.72


9:18

Dashboard

CHANNEL LOAD

Ch 6 Light, 26%

Ch 149 Light, 1%

INFORMATION

IP 172.17.3.201

MAC 14:49:BC:51:B7:9E

Mode Root

Device Name Root

Firmware 1332.091d83af78_Beta

WIRELESS OVERVIEW

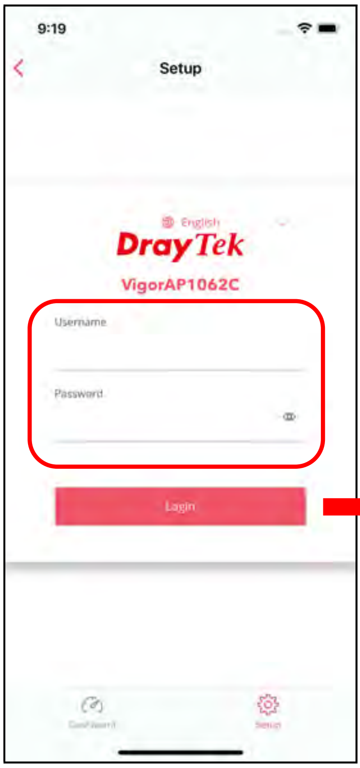
2.4GHz

SSID1 AP1062c_Mesh_201

5GHz

SSID1 AP1062c_Mesh_201

Click **Setup** to access into the web user interface of VigorAP 805. On the following page, enter the username and the password. Click **Login** to get the dashboard of the access point.


9:19

Setup

English

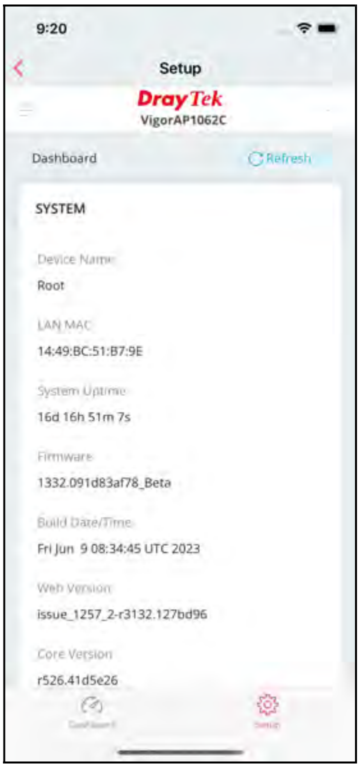
DrayTek

VigorAP1062C

Username

Password

Login


9:20

Setup

DrayTek

VigorAP1062C

Dashboard Refresh

SYSTEM

Device Name

Root

LAN MAC

14:49:BC:51:B7:9E

System Uptime

16d 16h 51m 7s

Firmware

1332.091d83af78_Beta

Build Date/Time

Fri Jun 9 08:34:45 UTC 2023

Web Version

issue_1257_2-r3132.127bd96

Core Version

r526.41d5e26

Chapter VI Troubleshooting

VI-1 Checking the Hardware Status

Follow the steps below to verify the hardware status.

1. Check the power line and cable connections.
   Refer to "I-1-1 LED Indicators and Connectors" for details.
2. Power on the device. Make sure the POWER 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-2 Checking the Network Connection Settings

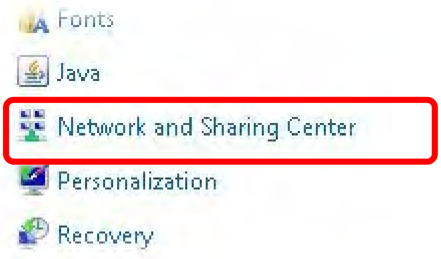
Sometimes the link failure occurs due to the wrong network connection settings. After trying the above section, if the link is stilled failed, please do the steps listed below to make sure the network connection settings is OK.

VI-2-1 For Windows

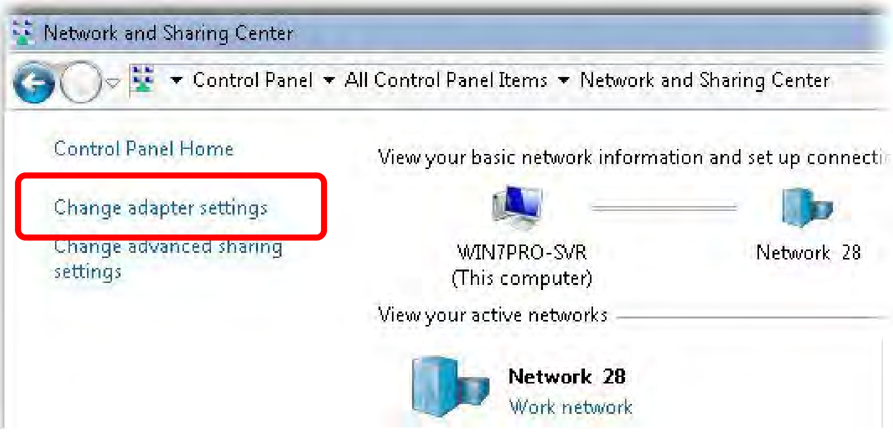
ⓘ Note:

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.

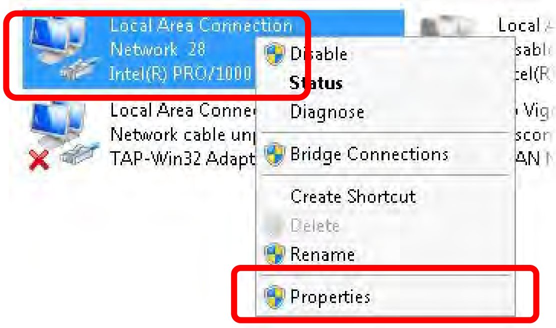
1. Open **All Programs>>Getting Started>>Control Panel.** Click **Network and Sharing Center.**



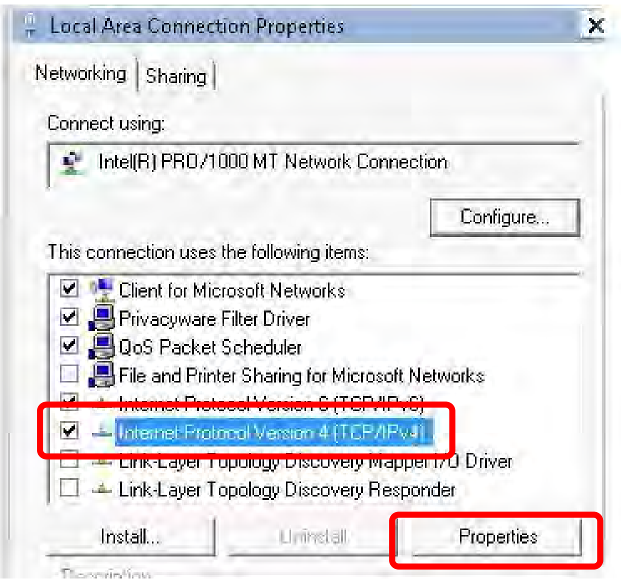
2. In the following window, click **Change adapter settings**.


Network and Sharing Center
Control Panel ▸ All Control Panel Items ▸ Network and Sharing Center
Control Panel Home
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connecti
WIN7PRO-SVR
(This computer)
Network 28
View your active networks
Network 28
Work network

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**.



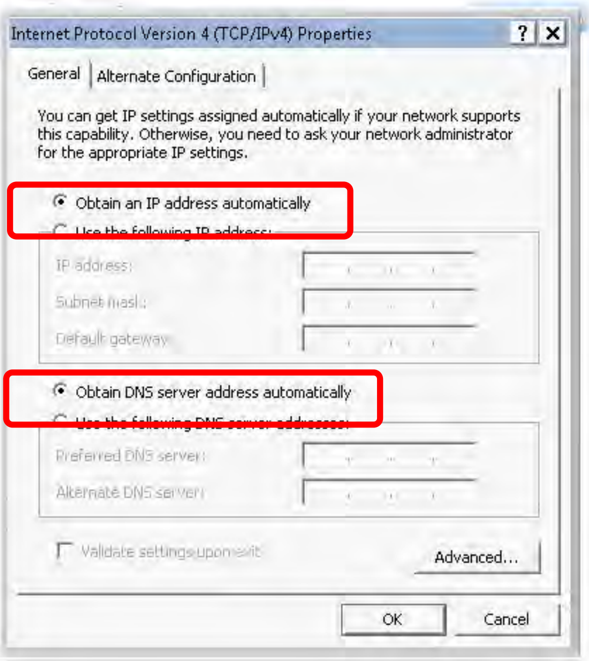
Connect using:

Intel(R) PRO/1000 MT Network Connection

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ Privacyware Filter Driver
- ☑ QoS Packet Scheduler
- □ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- □ Link-Layer Topology Discovery Mapper I/O Driver
- □ Link-Layer Topology Discovery Responder

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



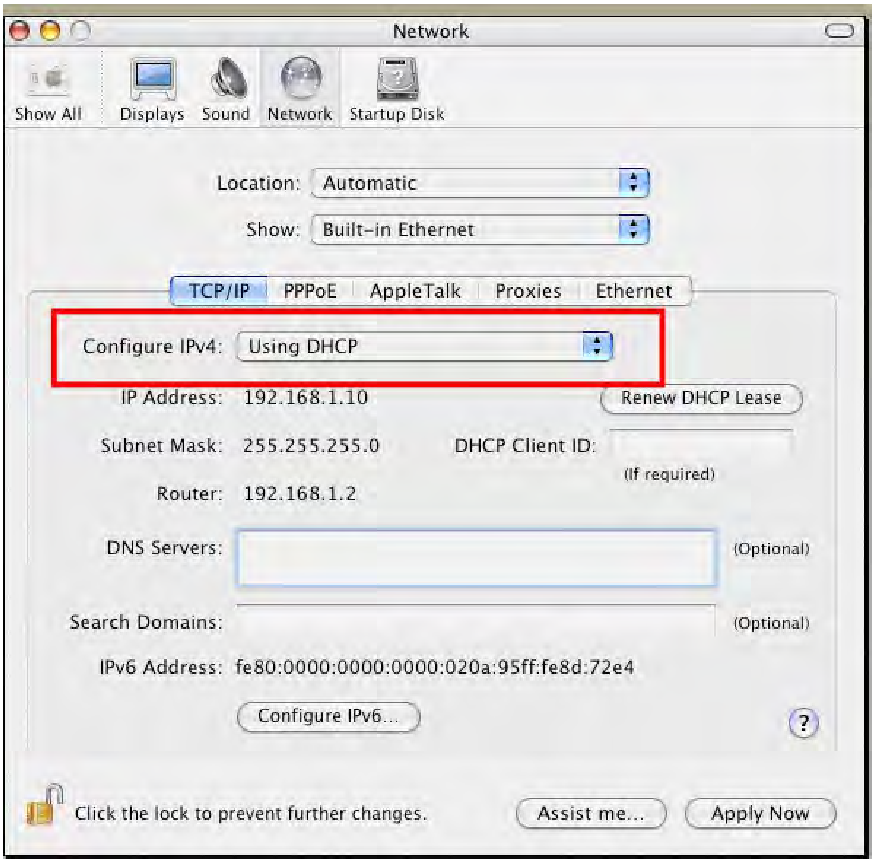
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

- ● Obtain an IP address automatically
- ○ Use the following IP address:
  - IP address:
  - Subnet mask:
  - Default gateway:
- ● Obtain DNS server address automatically
- ○ Use the following DNS server addresses:
  - Preferred DNS server:
  - Alternate DNS server:

□ Validate settings upon exit

VI-2-2 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.



Location: Automatic

Show: Built-in Ethernet

Configure IPv4: Using DHCP

IP Address: 192.168.1.10

Subnet Mask: 255.255.255.0

DHCP Client ID: (If required)

Router: 192.168.1.2

DNS Servers: (Optional)

Search Domains: (Optional)

IPv6 Address: fe80:0000:0000:0000:020a:95ff:fe8d:72e4

Click the lock to prevent further changes.

VI-3 Pinging the Device

The default gateway IP address of the device is 192.168.1.2. For some reason, you might need to use "ping" command to check the link status of the device. **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)

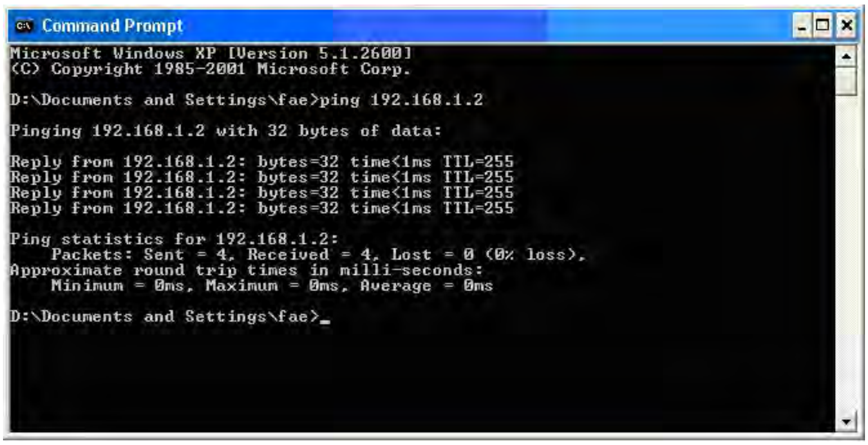
Please follow the steps below to ping the device correctly.

VI-3-1 For Windows

1. Open the **Command** Prompt window (from **Start menu> Run**).

   Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/2000/XP/Vista/7).

   The DOS command dialog will appear.

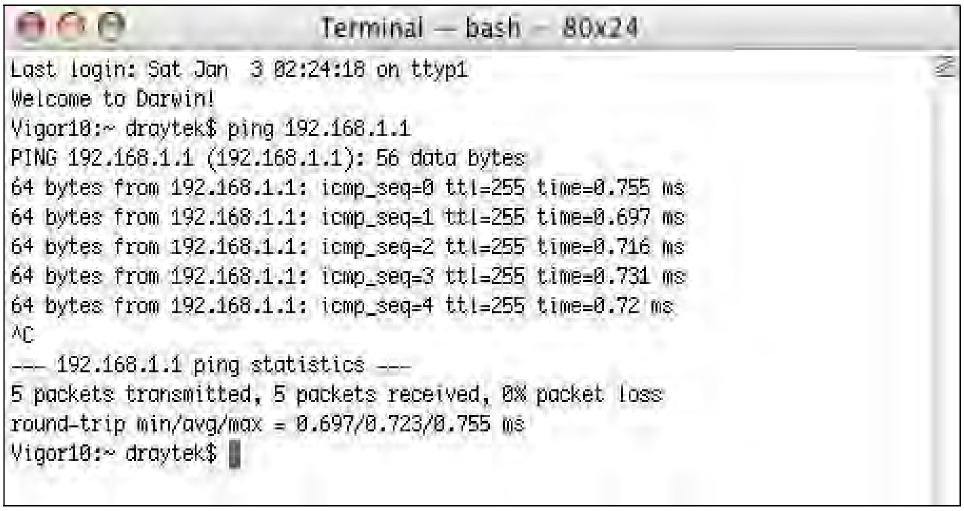


```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\Documents and Settings\fae>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=255
Reply from 192.168.1.2: bytes=32 time<1ms TTL=255
Reply from 192.168.1.2: bytes=32 time<1ms TTL=255
Reply from 192.168.1.2: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

D:\Documents and Settings\fae>_
```

2. 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.
3. If the line does not appear, please check the IP address setting of your computer.

VI-3-2 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.



```
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-4 Backing to Factory Default Setting

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

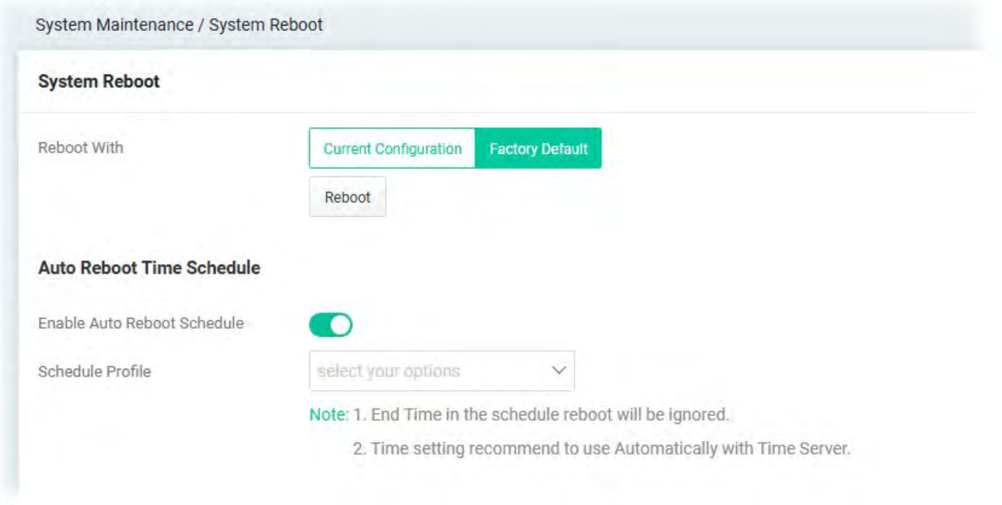
ⓘ Warning:

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-4-1 Software Reset

You can reset the device 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 device will return all the settings to the factory settings.



System Maintenance / System Reboot

System Reboot

Reboot With: Current Configuration / **Factory Default** (selected)

Reboot

Auto Reboot Time Schedule

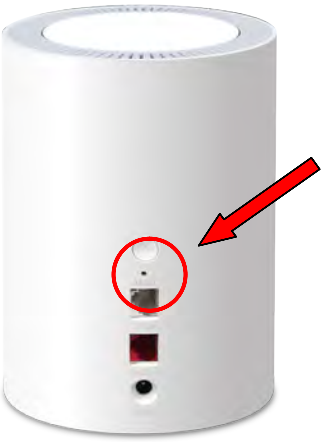
Enable Auto Reboot Schedule: ● (on)

Schedule Profile: select your options

Note: 1. End Time in the schedule reboot will be ignored.
2. Time setting recommend to use Automatically with Time Server.

VI-4-2 Hardware Reset

While the AP 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 AP will restart with the default configuration.



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

VI-5 Contacting DrayTek

If the AP 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.