# Vigor2136 Series

Gigabit Broadband Router

User's Guide

Version: 1.4

Firmware Version: V5.4.4.1

Date: 30 October 2026

# Intellectual Property Rights (IPR) Information

**Copyrights**

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

**Trademarks**

The following trademarks are used in this document:

- Microsoft is a registered trademark of Microsoft Corp.
- Windows 8, 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 modem.
- The modem is a complicated electronic unit that may be repaired only be authorized and qualified personnel. Do not try to open or repair the modem yourself.
- Do not place the modem in a damp or humid place, e.g. a bathroom.
- The modem should be used in a sheltered area, within a temperature range of 0 to +40 Celsius.
- Do not expose the modem to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources.
- Do not deploy the cable for LAN connection outdoor to prevent electronic shock hazards.
- 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 router before powering it off when a TR-069/ ACS server manages the router.
- Keep the package out of reach of children.
- When you want to dispose of the modem, please follow local regulations on conservation of the environment.

**Warranty**

We warrant to the original end user (purchaser) that the modem will be free from any defects in workmanship or materials for a period of two (2) years from the date of purchase from the dealer. Please keep your purchase receipt in a safe place as it serves as proof of date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, we will, at our discretion, repair or replace the defective products or components, without charge for either parts or labor, to whatever extent we deem necessary tore-store the product to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be offered solely at our discretion. This warranty will not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions. The warranty does not cover the bundled or licensed software of other vendors. Defects which do not significantly affect the usability of the product will not be covered by the warranty. We reserve the right to revise the manual and online documentation and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

**Be a Registered Owner**

Web registration is preferred. You can register your Vigor router via https://myvigor.draytek.com.

**Firmware & Tools Updates**

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

# Table of Contents


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

I-1 Introduction ..... 2
I-1-1 LED Indicators and Connectors for Vigor2136 ..... 2
I-1-2 LED Indicators and Connectors for Vigor2136ax ..... 4
I-1-3 LED Indicators and Connectors for Vigor2136ax-4G ..... 6
I-1-4 LED Indicators and Connectors for Vigor2136F ..... 8
I-1-5 LED Indicators and Connectors for Vigor2136Fax ..... 10
I-2 Hardware Installation ..... 12
I-2-1 Network Connection ..... 12
I-2-2 Wall-Mounted Installation ..... 13
I-2-3 Antenna Installation (for 4G model) ..... 14
I-3 Accessing to Web User Interface ..... 16
I-4 Dashboard ..... 19

**Chapter II Connectivity ..... 21**

II-1 Configuration ..... 22
II-1-1 Physical Interface ..... 22
II-1-2 WAN ..... 25
II-1-2-1 WAN Connections ..... 25
II-1-2-2 WAN AutoHunt ..... 41
II-1-2-3 Virtual WAN ..... 47
II-1-2-4 Dynamic DNS ..... 51
II-1-2-5 WAN Budget ..... 55
II-1-2-6 DHCP Options ..... 58
II-1-2-7 LB & Failover ..... 60
II-1-2-8 Link Health Check ..... 62
II-1-2-9 Performance SLA ..... 64
II-1-2-10 PPPoE Pass Through ..... 66
II-1-3 LAN ..... 67
II-1-3-1 LANs ..... 68
II-1-3-2 Bind IP to MAC ..... 73
II-1-3-3 DHCP Options ..... 75
II-1-3-4 Inter-LAN Routing ..... 77
II-1-3-5 VLAN List ..... 78
II-1-3-6 Interface VLAN ..... 80
II-1-3-7 LAN Port 802.1x ..... 81
II-1-3-8 LAN Port Mirror ..... 82
II-1-3-9 Backup & Restore ..... 83
II-1-4 DNS ..... 84
II-1-4-1 DNS Security ..... 84
II-1-4-2 LAN DNS/Forwarding ..... 86
II-1-5 Wireless LAN ..... 88
II-1-5-1 SSID ..... 90
II-1-5-2 Radio Settings ..... 94
II-1-5-3 Roaming ..... 97
II-1-5-4 AP Discovery ..... 99
II-1-5-5 WPS ..... 100
II-1-5-6 WDS ..... 103
II-1-6 Routing ..... 105
II-1-6-1 Route Policy ..... 105
II-1-6-2 IPv4 Static Route ..... 109
II-1-6-3 IPv6 Static Route ..... 111
II-1-7 RIP ..... 112

II-1-7-1 General Setup ..... 112
II-1-7-2 RIP Network (IPv4) ..... 115
II-1-7-3 RIPng Network (IPv6) ..... 116
II-1-8 BGP ..... 118
II-1-8-1 General Setup ..... 118
II-1-8-2 IPv4 Neighbors ..... 120
II-1-8-3 IPv4 Networks ..... 122
II-1-8-4 IPv6 Neighbors ..... 123
II-1-8-5 IPv6 Networks ..... 125
II-1-9 OSPF ..... 127
II-1-9-1 General Setup ..... 127
II-1-9-2 OSPFv2 Networks ..... 129
II-1-9-3 OSPFv3 Networks ..... 131
II-1-10 Bandwidth Management ..... 133
II-1-10-1 Traffic Shaping Policy ..... 133
II-1-10-2 Bandwidth Limit ..... 136
II-1-10-3 QoS Setup ..... 138
II-1-10-4 APP QoS ..... 140
II-1-10-5 Default Policy ..... 141
II-1-11 NAT ..... 142
II-1-11-1 Port Forwarding ..... 142
II-1-11-2 DMZ Host ..... 145
II-1-11-3 Port Triggering ..... 146
II-1-11-4 ALG ..... 149
II-1-11-5 UPnP ..... 150
II-1-12 IGMP ..... 150
II-1-12-1 General Setup ..... 151
II-1-12-2 IGMP Status ..... 152
II-1-13 Objects ..... 153
II-1-13-1 IP Object ..... 153
II-1-13-2 IP Group ..... 155
II-1-13-3 MAC Object ..... 157
II-1-13-4 MAC Group ..... 158
II-1-13-5 Schedule ..... 159
II-1-13-6 Service Type Object ..... 161
II-1-13-7 Country Object ..... 162
II-1-13-8 Keyword Object ..... 164
II-1-13-9 Backup & Restore ..... 166
II-1-14 USB Application ..... 167
II-1-14-1 General Setup ..... 167
II-1-14-2 USB User Management ..... 168
II-1-14-3 USB Device Status ..... 169
II-1-14-4 Temperature Sensor Settings ..... 171
II-1-14-5 Modem Support List ..... 172
II-1-14-6 SMB Client Support List ..... 173
II-1-15 Wake on LAN ..... 174
II-1-16 Notification Services ..... 176
II-1-16-1 Services & Providers ..... 176
II-1-16-2 SMTP Server ..... 177
II-1-16-3 SMS Provider ..... 179
II-1-16-4 Webhook ..... 181
II-1-16-5 Notification ..... 182
II-1-16-6 Backup & Restore ..... 184
II-1-17 RADIUS/TACACS+ ..... 185
II-1-17-1 External RADIUS ..... 185
II-1-17-2 Internal RADIUS ..... 187
II-1-17-3 External TACACS+ ..... 190
II-1-18 Certificates ..... 191
II-1-18-1 Local Certificates ..... 191

II-1-18-2 Trusted CA ..... 195
II-1-18-3 Local Services ..... 198
II-1-18-4 Backup & Restore ..... 199
II-2 Security ..... 200
II-2-1 Firewall Filters ..... 200
II-2-1-1 URL/IP Reputation Filters ..... 201
II-2-1-2 IP Filters ..... 203
II-2-1-3 Content Filters ..... 207
II-2-1-4 Default Filters ..... 209
II-2-1-5 Backup & Restore ..... 212
II-2-2 Defense Setup ..... 213
II-2-2-1 DoS Defense ..... 213
II-2-2-2 Brute Force Protection ..... 216
II-2-2-3 Allow/Block List ..... 218
II-2-2-4 Defense Syslog ..... 220
II-2-3 MAC Filtering Profile ..... 220
II-2-3-1 MAC Filtering Profile ..... 220
II-2-3-2 Backup & Restore ..... 222
II-2-4 IPv6 Address Security ..... 223
II-2-5 Security Defense Status ..... 224
II-2-5-1 Brute Force Protection Status ..... 224
II-2-5-2 URL/IP Reputation ..... 225
II-2-6 URL/IP Lookup ..... 225
II-3 IAM ..... 228
II-3-1 Users & Groups ..... 229
II-3-1-1 Users ..... 229
II-3-1-2 User Groups ..... 238
II-3-1-3 Authentication Server ..... 240
II-3-2 IAM Policies ..... 241
II-3-2-1 Apply Policies to LAN ..... 241
II-3-2-2 Access Policies ..... 243
II-3-2-3 Group Policies ..... 245
II-3-2-4 Conditional Access Policy ..... 249
II-3-3 Resources ..... 250
II-3-4 Hotspot Web Portal ..... 253
II-3-4-1 Profile Setup ..... 253
II-3-4-2 Quota Policy Profile ..... 260
II-3-4-3 Users Information ..... 262
II-3-5 Account Status ..... 263
II-3-5 Backup & Restore ..... 264
II-4 VPN ..... 265
II-4-1 General Setup ..... 265
II-4-1-1 Access Control ..... 265
II-4-1-2 EasyVPN ..... 268
II-4-1-3 IPsec ..... 269
II-4-1-4 WireGuard ..... 271
II-4-1-5 OpenVPN ..... 273
II-4-1-6 L2TP ..... 274
II-4-1-7 VPN MSS ..... 275
II-4-2 Site-to-Site VPN ..... 277
II-4-2-1 VPN Type - IPsec ..... 277
II-4-2-2 VPN Type - WireGuard ..... 284
II-4-2-3 VPN Type - OpenVPN ..... 287
II-4-2-4 VPN Type – L2TP ..... 291
II-4-3 Teleworker VPN ..... 295
II-4-4 VPN Connection Status ..... 304
II-4-5 Backup & Restore ..... 305
II-5 Virtual Controller - Wireless ..... 306

II-5-1 Role Setup ..... 307
II-5-2 Device ..... 310
II-5-2-1 Device List ..... 310
II-5-2-2 Mesh Status ..... 314
II-5-2-3 AP Adoption ..... 315
II-5-3 AP Profile ..... 319
II-5-3-1 SSID ..... 319
II-5-3-2 Radio Settings ..... 323
II-5-3-3 Roaming ..... 326
II-6 Virtual Controller - Switch ..... 328
II-6-1 General Setup ..... 328
II-6-2 Device ..... 330
II-6-3 Port Profile ..... 337
II-6-4 Maintenance ..... 346

**Chapter III Management ..... 349**

III-1 System Maintenance ..... 350
III-1-1 Device Settings ..... 350
III-1-1-1 Time ..... 350
III-1-1-2 Device Name ..... 352
III-1-1-3 Syslog ..... 352
III-1-1-4 SNMP ..... 353
III-1-1-5 System ..... 356
III-1-2 Management ..... 357
III-1-2-1 Service Control ..... 357
III-1-2-2 TR-069 ..... 360
III-1-2-3 XMPP ..... 361
III-1-2-4 TR-369 ..... 362
III-1-3 System Upgrade ..... 365
III-1-3-1 Firmware ..... 365
III-1-3-2 GeoIP Database ..... 367
III-1-4 Backup & Restore ..... 369
III-1-5 Accounts & Permission ..... 370
III-1-5-1 Local Admin Account ..... 370
III-1-5-2 Role & Permission ..... 373
III-1-6 System Reboot ..... 375

**Chapter IV Others ..... 377**

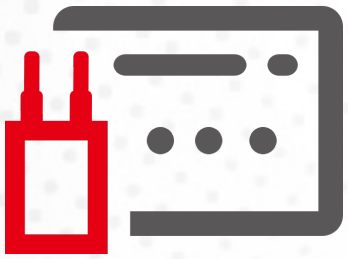
IV-1 Monitoring ..... 378
IV-1-1 Clients List ..... 378
IV-1-2 Log Center ..... 380
IV-1-2-1 Log Center ..... 380
IV-1-2-2 DDNS Log ..... 381
IV-1-2-3 Notification ..... 381
IV-1-3 Wireless Information ..... 382
IV-1-3-1 Wireless Information ..... 382
IV-1-3-2 Recent Activities ..... 382
IV-1-3-3 Real Time Throughput 2.4G ..... 383
IV-1-3-4 Real Time Throughput 5G ..... 383
IV-1-4 WAN ..... 384
IV-1-4-1 WAN Utilization ..... 384
IV-1-4-2 WAN Status ..... 384
IV-1-5 ARP Table ..... 386
IV-1-5-1 LAN ..... 386
IV-1-5-2 WAN ..... 386
IV-1-6 Route Table ..... 387
IV-1-6-1 IPv4 ..... 387
IV-1-6-2 IPv6 ..... 388

IV-1-7 DHCP Table ..... 389
IV-1-7-1 IPv4 DHCP Subnet ..... 389
IV-1-7-2 IPv4 DHCP Lease ..... 389
IV-1-7-3 IPv6 Assignment ..... 390
IV-1-8 IPv6 TSPC Status ..... 390
IV-1-9 IPv6 Neighbor Table ..... 391
IV-1-10 LLDP Neighbors ..... 391
IV-1-11 DNS Cache Table ..... 392
IV-1-11-1 IPv4 ..... 392
IV-1-11-2 IPv6 ..... 392
IV-1-12 Remote DSL Status ..... 393
IV-1-13 PPPoE Pass-Through ..... 394
IV-1-14 Sessions ..... 395
IV-1-14-1 Session Status ..... 395
IV-1-14-2 NAT Session Table ..... 395
IV-1-15 Running Services ..... 396
IV-1-16 Port Knocking Status ..... 396
IV-2 Utility ..... 397
IV-2-1 Network Tools ..... 397
IV-2-1-1 Ping ..... 397
IV-2-1-2 Traceroute ..... 398
IV-2-1-3 DNS ..... 399
IV-2-1-4 iPerf Connectivity Test ..... 400
IV-2-2 Packet Capture ..... 401
IV-2-3 Debug Logs ..... 402
IV-2-4 Web CLI ..... 403

**Chapter V Troubleshooting ..... 405**

V-1 Checking the Hardware Status ..... 406
V-2 Checking the Network Connection Settings ..... 407
V-2-1 For Windows ..... 407
V-2-2 For Mac Os ..... 409
V-3 Pinging the Device ..... 410
V-3-1 For Windows ..... 410
V-3-2 For Mac Os (Terminal) ..... 410
V-4 Backing to Factory Default Setting ..... 412
V-4-1 Software Reset ..... 412
V-4-2 Hardware Reset ..... 413
V-5 Contacting DrayTek ..... 414

# 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.

## I-1-1 LED Indicators and Connectors for Vigor2136

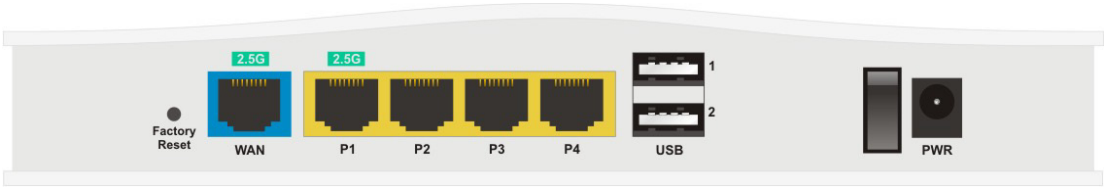
Before you use the Vigor modem, please get acquainted with the LED indicators and connectors first.

### LED



| LED | Status | Explanation |
|---|---|---|
| (Activity) | Blinking | The router is powered on and running normally. |
| | Off | The router is powered off. |
| WAN | On | Internet connection is ready. |
| | Blinking | The data is transmitting. |
| | Off | Internet connection is not ready. |
| LAN1/2/3/4 | On | The LAN port is connected. |
| | Blinking | The data is transmitting. |
| | Off | The LAN port is disconnected. |
| USB | On | A USB device is connected and active. |
| | Blinking | The data is transmitting. |

## Connectors



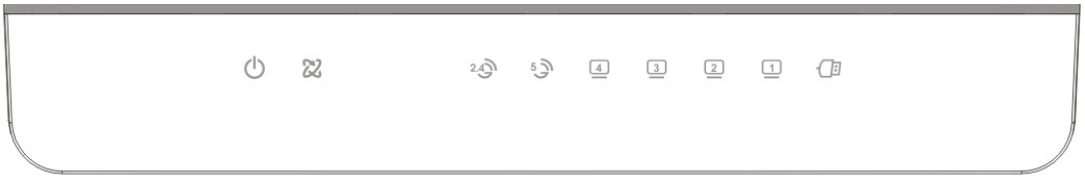

| Interface | Explanation |
|---|---|
| Factory Reset | Restore the default settings.<br>Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration. |
| 2.5G WAN | Connector for remote networked devices (by Ethernet cable). |
| P1~P4 | Connectors for local networked devices.<br>In which the transmission rate for P1(only) can reach 2.5G. |
| USB1~USB2 | Connector for a USB device (USB Modem or printer). |
| ON/OFF | Power switch. |
| PWR | Connector for a power adapter. |

**Note**

Remove the protective film from the router before use to ensure ventilation.

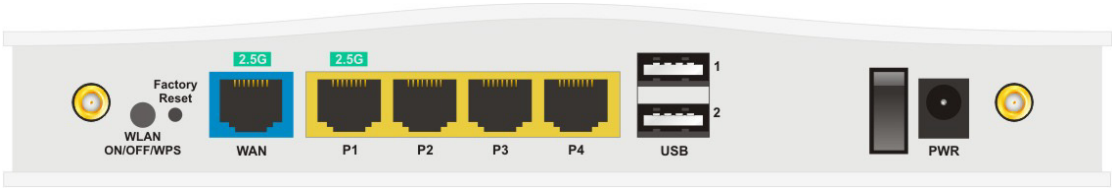
# I-1-2 LED Indicators and Connectors for Vigor2136ax

## LED



| LED | Status | Explanation |
|---|---|---|
| (Activity) | Blinking | The router is powered on and running normally. |
| | Blinking (quickly) | When both ACT and WLAN LEDs blink quickly, it means the WPS function is enabled and active. The system is waiting for a wireless station of connection. |
| | Off | The router is powered off. |
| WAN | On | Internet connection is ready. |
| | Blinking | The data is transmitting. |
| | Off | Internet connection is not ready. |
| WLAN | On | Wireless access point is ready. |
| | Blinking | Ethernet packets are transmitting over wireless LAN. |
| | Blinking (quickly) | When both ACT and WLAN LEDs blink quickly, it means the WPS function is enabled and active. The system is waiting for a wireless station of connection. |
| | Off | The WLAN function is inactive. |
| LAN1/2/3/4 | On | The LAN port is connected. |
| | Blinking | The data is transmitting. |
| | Off | The LAN port is disconnected. |
| USB | On | A USB device is connected and active. |
| | Blinking | The data is transmitting. |

## Connectors




| Interface | Explanation |
|---|---|
| Wireless LAN ON/OFF/WPS | WLAN On - Press the button and release it within 2 seconds. When the wireless function is ready, the green LED will be on.<br>WLAN Off - Press the button and release it within 2 seconds to turn off the WLAN function. When the wireless function is not ready, the LED will be off.<br>WPS - When WPS function is enabled by web user interface, press this button for more than 2 seconds to wait for client's device making network connection through WPS. |
| Factory Reset | Restore the default settings.<br>Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration. |
| 2.5G WAN | Connector for remote networked devices (by Ethernet cable). |
| P1~P4 | Connectors for local networked devices.<br>In which the transmission rate for P1(only) can reach 2.5G. |
| USB1~USB2 | Connector for a USB device (USB Modem or printer). |
| ON/OFF | Power switch. |
| PWR | Connector for a power adapter. |

**Note**

Remove the protective film from the router before use to ensure ventilation.

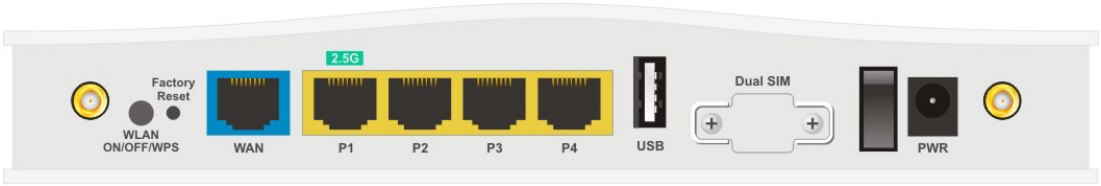
# I-1-3 LED Indicators and Connectors for Vigor2136ax-4G

## LED



| LED | Status | Explanation |
|---|---|---|
| (Activity) | Blinking | The router is powered on and running normally. |
| | Blinking (quickly) | When both ACT and WLAN LEDs blink quickly, it means the WPS function is enabled and active. The system is waiting for a wireless station of connection. |
| | Off | The router is powered off. |
| WAN | On | Internet connection is ready. |
| | Blinking | The data is transmitting. |
| | Off | Internet connection is not ready. |
| 2 1 | On | SIM card is inserted into the slot and detected by Vigor device. |
| | Blinking | No SIM card in detected. |
| 2.4 ~ 5 WLAN | On | Wireless access point is ready. |
| | Blinking | Ethernet packets are transmitting over wireless LAN. |
| | Blinking (quickly) | When both ACT and WLAN LEDs blink quickly, it means the WPS function is enabled and active. The system is waiting for a wireless station of connection. |
| | Off | The WLAN function is inactive. |
| 1 ~ 4 LAN1/2/3/4 | On | The LAN port is connected. |
| | Blinking | The data is transmitting. |
| | Off | The LAN port is disconnected. |
| USB | On | A USB device is connected and active. |
| | Blinking | The data is transmitting. |

## Connectors




| Interface | Explanation |
|---|---|
| | Connecter for installing WLAN antennas. (For ax model). |
| WLAN ON/OFF/WPS | WLAN On - Press the button and release it within 2 seconds. When the wireless function is ready, the green LED will be on.<br>WLAN Off - Press the button and release it within 2 seconds to turn off the WLAN function. When the wireless function is not ready, the LED will be off.<br>WPS - When WPS function is enabled by web user interface, press this button for more than 2 seconds to wait for client's device making network connection through WPS. |
| Factory Reset | Restore the default settings.<br>Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration. |
| WAN | Connector for remote networked devices (by Ethernet cable). |
| P1~P4 | Connectors for local networked devices.<br>In which the transmission rate for P1(only) can reach 2.5G. |
| USB | Connector for a USB device (USB Modem or printer). |
| Dual SIM | Slots for installing SIM card(s). |
| ON/OFF | Power switch. |
| PWR | Connector for a power adapter. |

**Note**

Remove the protective film from the router before use to ensure ventilation.

# I-1-4 LED Indicators and Connectors for Vigor2136F

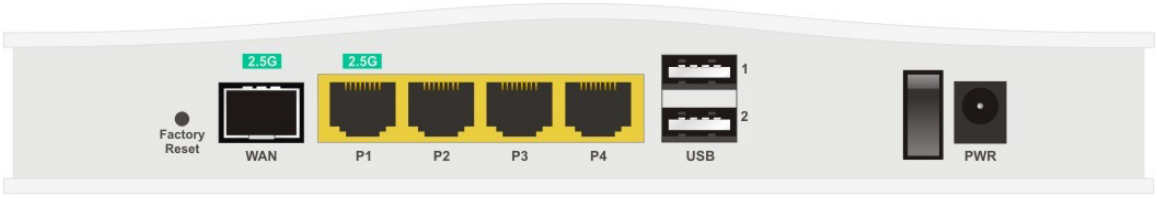
Before you use the Vigor modem, please get acquainted with the LED indicators and connectors first.

## LED



| LED | Status | Explanation |
|---|---|---|
| (Activity) | Blinking | The router is powered on and running normally. |
| | Off | The router is powered off. |
| WAN | On | Internet connection is ready. |
| | Blinking | The data is transmitting. |
| | Off | Internet connection is not ready. |
| ~ LAN1/2/3/4 | On | The LAN port is connected. |
| | Blinking | The data is transmitting. |
| | Off | The LAN port is disconnected. |
| USB | On | A USB device is connected and active. |
| | Blinking | The data is transmitting. |

## Connectors



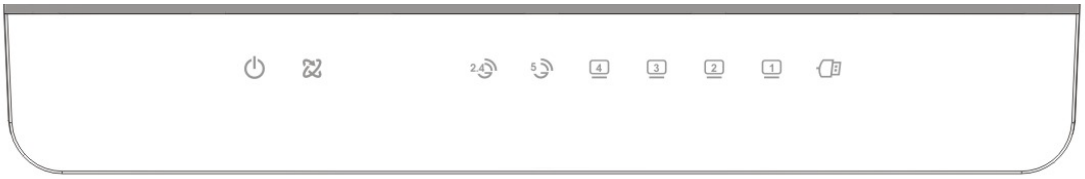

| Interface | Explanation |
|---|---|
| Factory Reset | Restore the default settings.<br>Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration. |
| WAN | Connector for fiber connection for accessing the Internet. |
| P1~P4 | Connectors for local networked devices.<br>In which the transmission rate for P1(only) can reach 2.5G. |
| USB1~USB2 | Connector for a USB device (USB Modem or printer). |
| ON/OFF | Power switch. |
| PWR | Connector for a power adapter. |

**Note**

Remove the protective film from the router before use to ensure ventilation.

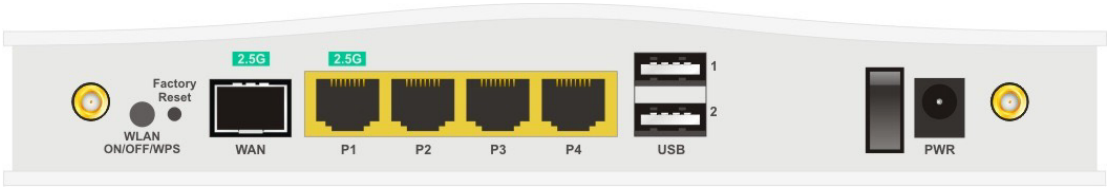
# I-1-5 LED Indicators and Connectors for Vigor2136Fax

## LED



| LED | Status | Explanation |
|---|---|---|
| (Activity) | Blinking | The router is powered on and running normally. |
| | Blinking (quickly) | When both ACT and WLAN LEDs blink quickly, it means the WPS function is enabled and active. The system is waiting for a wireless station of connection. |
| | Off | The router is powered off. |
| WAN | On | Internet connection is ready. |
| | Blinking | The data is transmitting. |
| | Off | Internet connection is not ready. |
| WLAN | On | Wireless access point is ready. |
| | Blinking | Ethernet packets are transmitting over wireless LAN. |
| | Blinking (quickly) | When both ACT and WLAN LEDs blink quickly, it means the WPS function is enabled and active. The system is waiting for a wireless station of connection. |
| | Off | The WLAN function is inactive. |
| LAN1/2/3/4 | On | The LAN port is connected. |
| | Blinking | The data is transmitting. |
| | Off | The LAN port is disconnected. |
| USB | On | A USB device is connected and active. |
| | Blinking | The data is transmitting. |

## Connectors




| Interface | Explanation |
|---|---|
| | Connecter for installing WLAN antennas. (For ax model). |
| WLAN ON/OFF/WPS | WLAN On - Press the button and release it within 2 seconds. When the wireless function is ready, the green LED will be on.<br>WLAN Off - Press the button and release it within 2 seconds to turn off the WLAN function. When the wireless function is not ready, the LED will be off.<br>WPS - When WPS function is enabled by web user interface, press this button for more than 2 seconds to wait for client's device making network connection through WPS. |
| Factory Reset | Restore the default settings.<br>Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration. |
| WAN | Connector for fiber connection for accessing the Internet. |
| P1~P4 | Connectors for local networked devices.<br>In which the transmission rate for P1(only) can reach 2.5G. |
| USB | Connector for a USB device (USB Modem or printer). |
| ON/OFF | Power switch. |
| PWR | Connector for a power adapter. |

**Note**

Remove the protective film from the router before use to ensure ventilation.

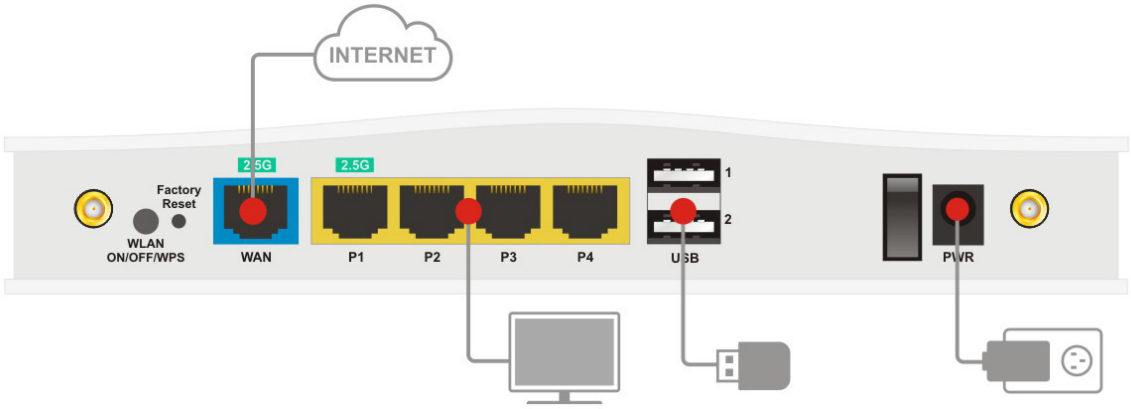
# I-2 Hardware Installation

This section will guide you to install the Vigor2136 through a hardware connection and configure the device's settings through the web browser.

## I-2-1 Network Connection

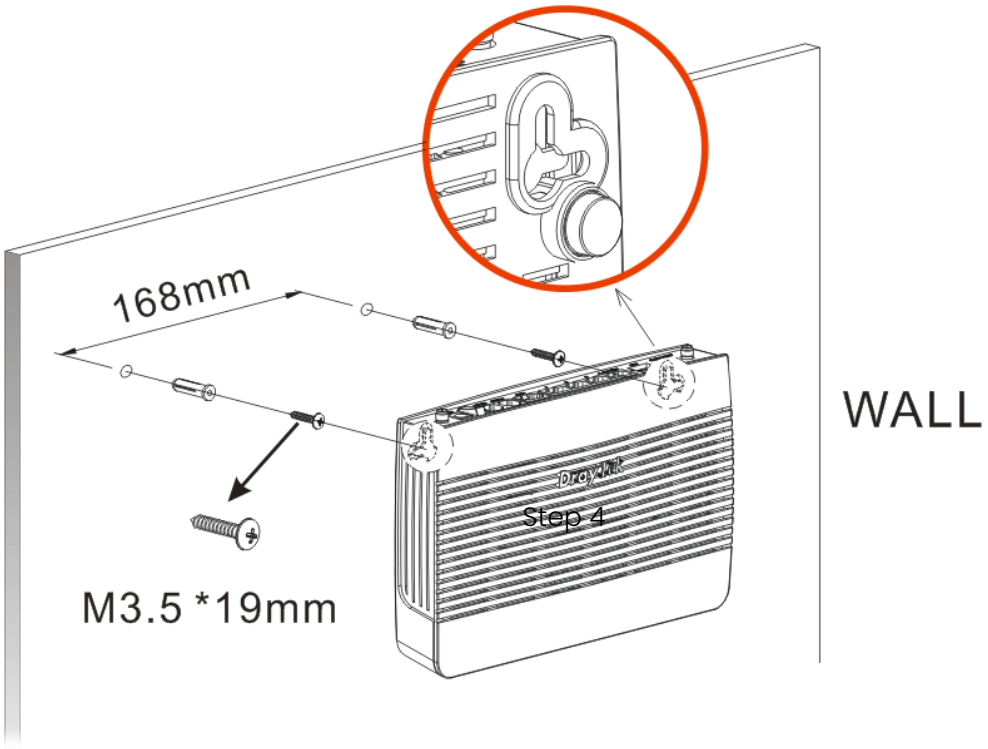
1. Connect the cable Modem/DSL Modem/Media Converter to any WAN port of router with Ethernet cable (RJ-45).
2. Connect one end of an Ethernet cable (RJ-45) to one of the **LAN** ports of the router and the other end of the cable (RJ-45) into the Ethernet port on your computer.
3. Connect one end of the power cord to the power port of this device. Connect the other end to the wall outlet of electricity.
4. For ac series, connect detachable antennas to the router.
5. Power on the router. Check the **ACT** and **WAN**, **LAN** LEDs to assure network connection.

   (For the detailed information of LED status, please refer to section 2. Panel Explanation)



## I-2-2 Wall-Mounted Installation

1. Drill the holes on the wall according to the recommended instruction.
2. Fit screws into the wall using the appropriate type of wall plug.
3. With the screws installed, the router can be slotted into place.




---

**Note**

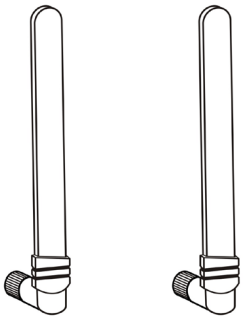
The recommended drill diameter shall be 6.5mm (1/4").

---

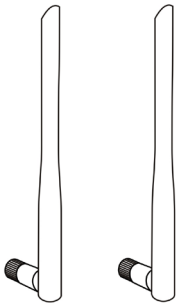
4. When you finished the above procedure, the modem has been mounted on the wall firmly.

## I-2-3 Antenna Installation (for 4G model)

Antenna must be installed on Vigor router correctly to obtain the transmission signal.

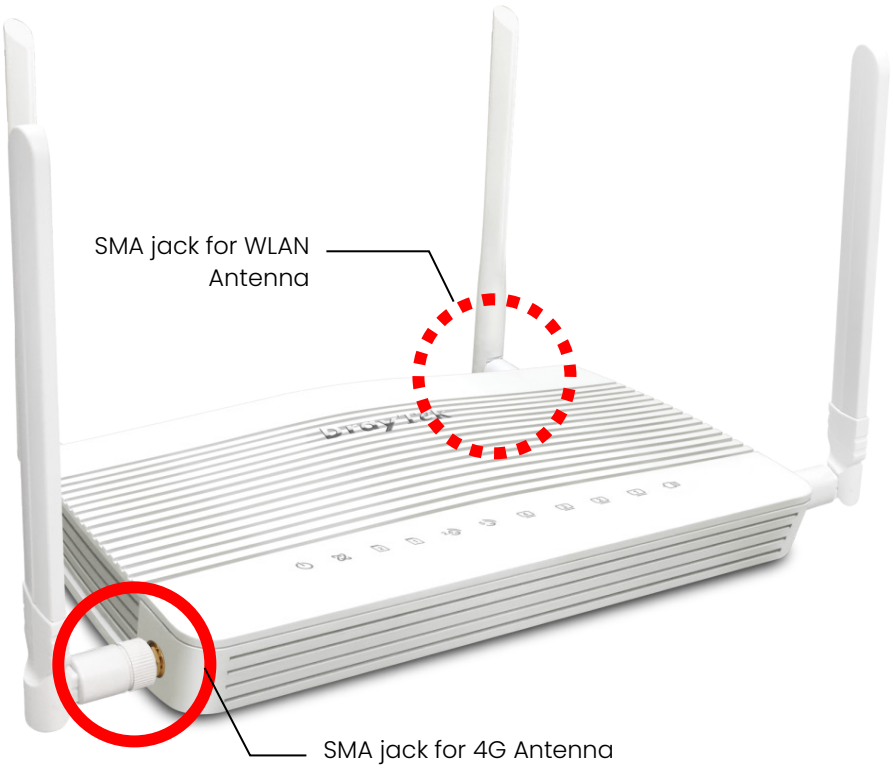


For model with SIM installed



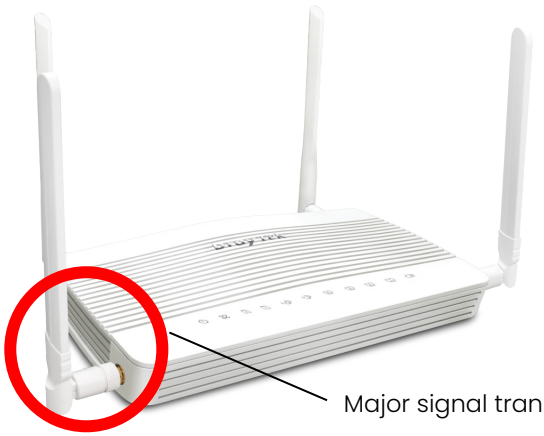
For ax models

There are two types of antennas provided for Vigor2136ax-4G, which must be installed in different locations carefully and correctly. Wrong installation might cause bad signal of wireless connection. Therefore, pay attention to the installation of antennas by referring to the following illustration.



Note

The antennas for Vigor2136ax-4G must be installed on both sides of the device. If only one antenna will be used, please install on the left side of Vigor router.

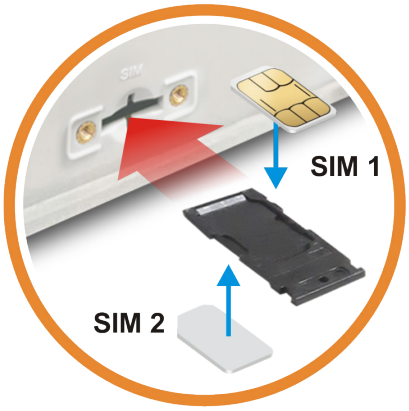



For installing the SIM card into the card slot,

(1) While installing the SIM card into the card slot, note that the back plate of the SIM card slot must be removed first.

(2) Assemble the SIM1 and SIM2 with the SIM tray. Then insert the SIM tray into the SIM card slot of the router.






Note

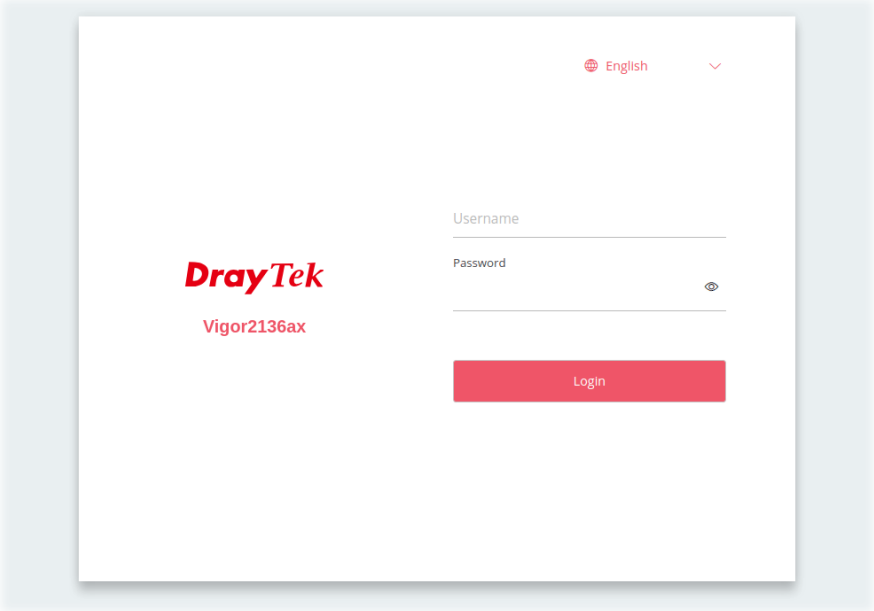
If you need to remove SIM1 or SIM2, carefully take them out of the card slot without bending the SIM tray.



# I-3 Accessing to Web User Interface

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

1. Make sure your PC connects to the Vigor router correctly.
2. Open a web browser on your PC and type **http://192.168.1.1.** A pop-up window will open to ask for a username and password. Pease type "admin/admin" on Username/Password and click **Login.**

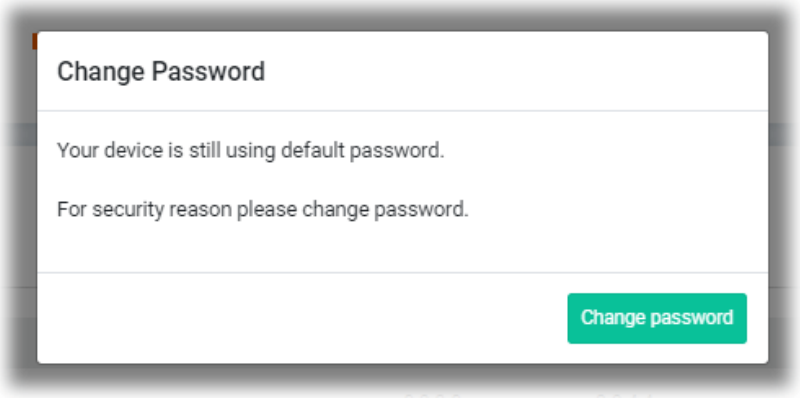



**Note:**

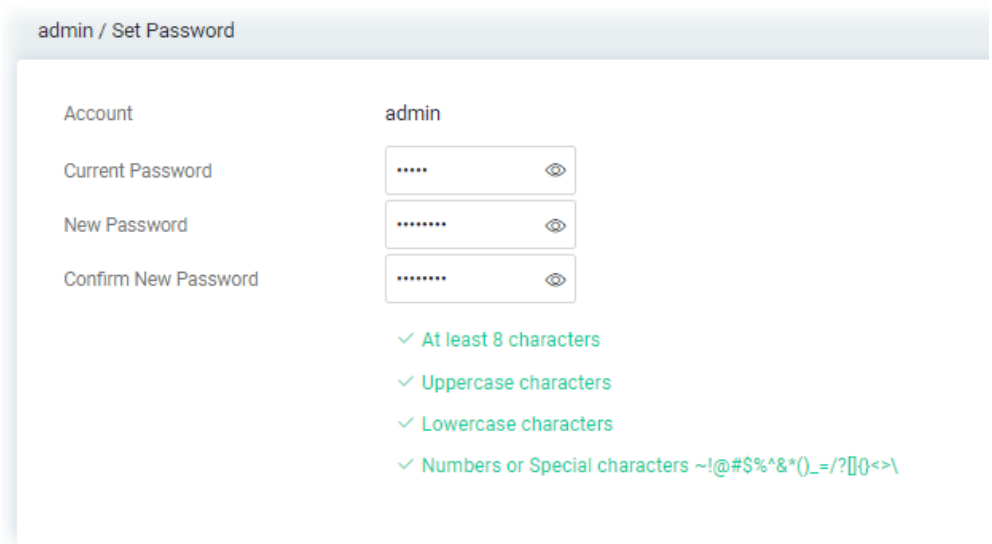
You may either simply set up your computer to get IP dynamically from the router or set up the IP address of the computer to be the same subnet as **the default IP address of Vigor router 192.168.1.1**.

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

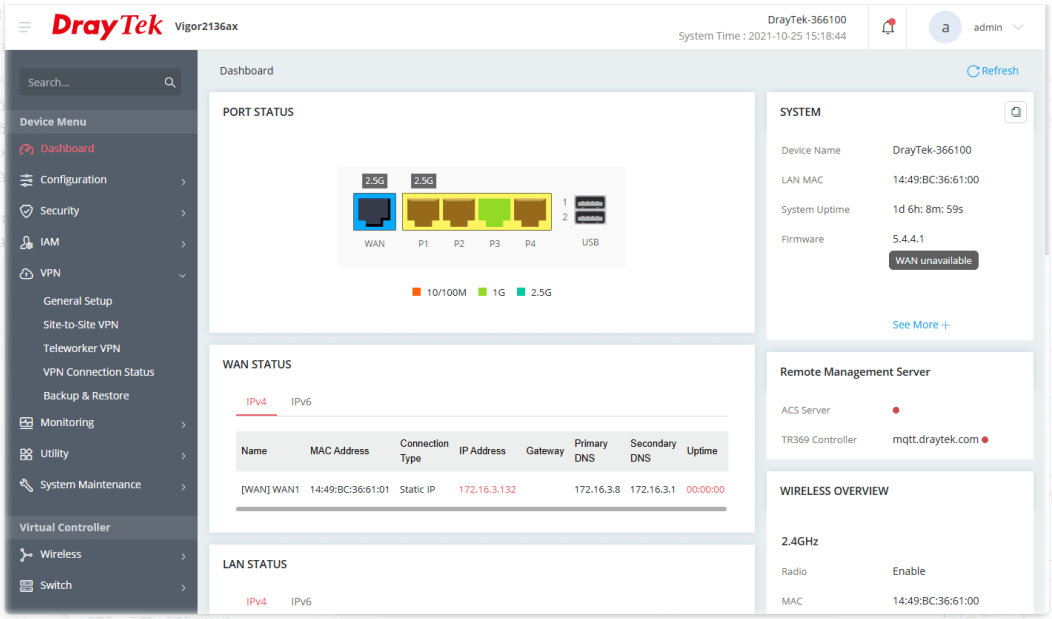
3. Next, the page will appear to guide you change the login password.



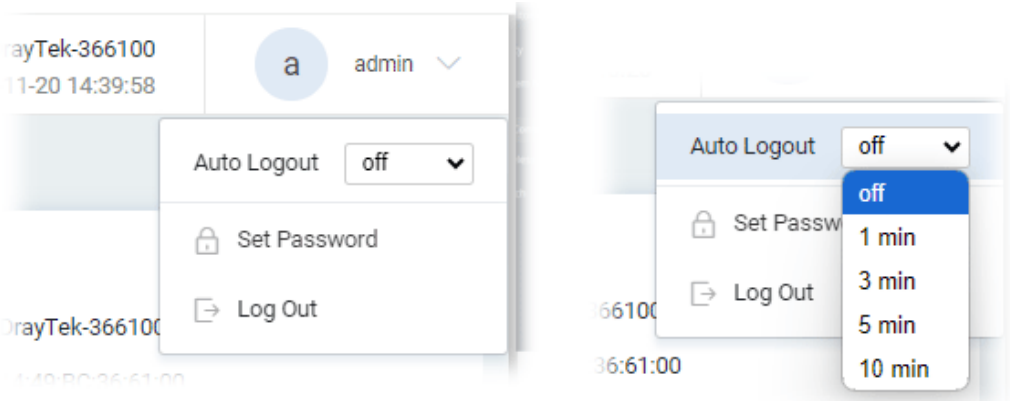

4. You **MUST** change the login password before accessing the web user interface. Please set a new password for network security.




5. After clicking **Apply**, the Main Screen will pop up.



6. 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 log out after 5 minutes without any operation. Change the setting of auto-logout if you want.




---

**Note:**

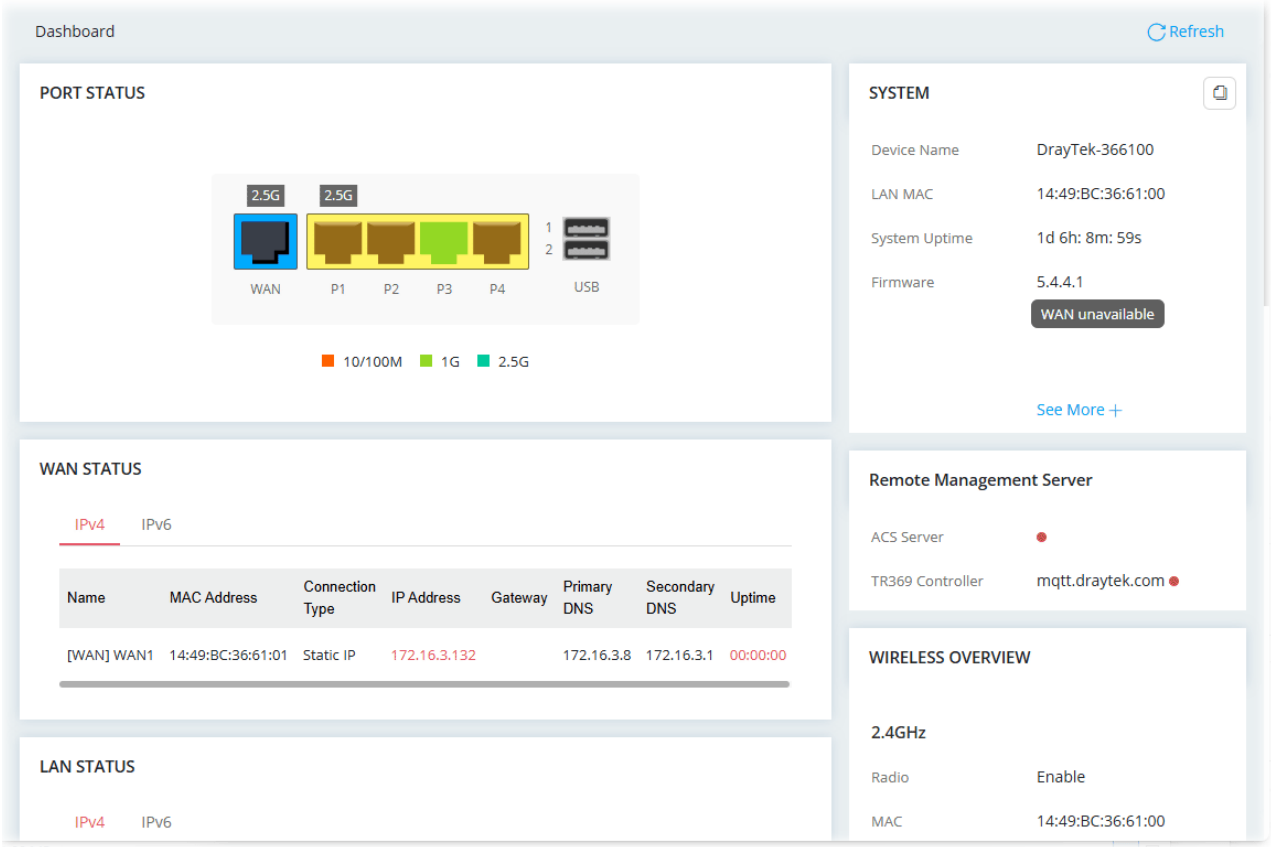
For using the device properly, it is necessary for you to change the password of web configuration for security and adjust primary basic settings.

---

# I-4 Dashboard

Dashboard shows port status, LAN status, system status, LAN/WAN Usage and DSL information.

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




---

**Note:**

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

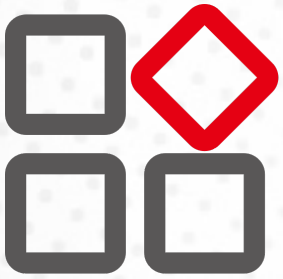
 - means “Enable”.

 - means “Disable”.

---

This page is left blank.

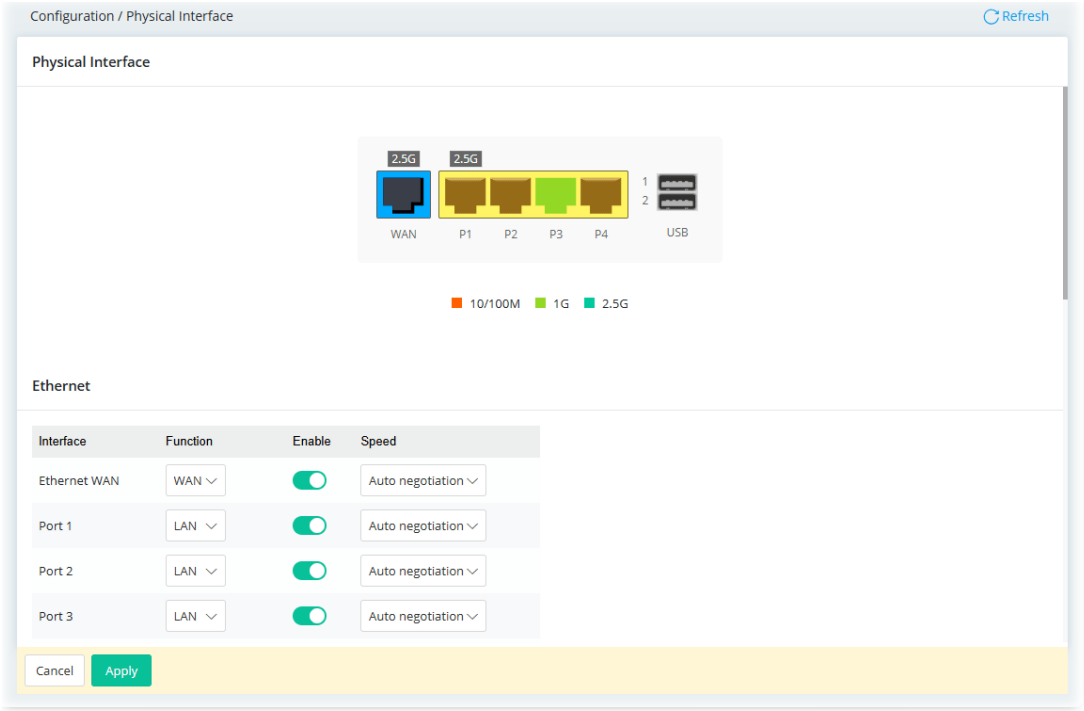
# Chapter II Connectivity



# II-1 Configuration

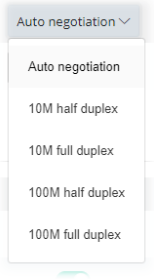
## II-1-1 Physical Interface

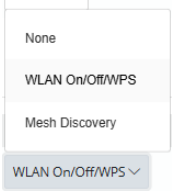
Configure the general settings for available interfaces. Open **Configuration >> Physical Interface**.




Available settings are explained as follows:

| Item | Description |
|---|---|
| | **Ethernet** |
| **Interface** | Displays the available interfaces of this device. |
| **Function** | Displays the type (WAN or LAN) of the interface.<br>Except Ethernet WAN is fixed to WAN, Port 1 can be set as WAN or LAN to meet different requirements. Use the drop-down menu to set the specified interface as LAN or WAN. |
| **Enable** | Switch the toggle to enable or disable the interface. |
| **Speed** | Set the port speed capabilities for each interface. |

| | |
|---|---|
| |  For Ethernet WAN / Port 1<br> For Port 2 to Port 4<br>Port speed capabilities:<br>**Auto negotiation** - Auto speed with all capabilities.<br>**2.5G** - Force speed with 2.5G ability.<br>**1G** - Force speed with 1G ability.<br>**10M half duplex** - Force speed with 10M ability.<br>**10M full duplex** - Force speed with 10M ability.<br>**100M half duplex** - Force speed with 100M ability.<br>**100M full duplex** - Force speed with 100M ability.<br>Selecting Auto (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect. |
| **Wireless** | |
| **Interface** | Displays the available wireless interfaces (2.4GHz/5GHz) of this device. |
| **Function** | Displays the type (WAN or LAN) of the interface.<br>The interface can be set as WAN or LAN to meet different requirements. Use the drop-down menu to set the specified interface as LAN or WAN. |
| **Enable** | Switch the toggle to enable or disable the interface. |
| **USB** | |
| **Interface** | Displays the available USB interface of this device. |
| **Enable** | Switch the toggle to enable or disable the interface. |

| LED | |
|---|---|
| **Interface** | Indicate all LEDs on the front panel. |
| **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.<br>When LED is slept, it can be woken up by pressing one of the following buttons:<br>• Factory Reset on the front panel<br>• Wake up LED on this configuration page<br>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. |
| **Enable** | In default, the LED on the device will be always on.<br>However, the LED can be turned on or off after a specified number of minutes has elapsed to meet certain requirements.<br>For this, switch the toggle to enable this setting. |
| **Button** | |
| **Interface** | Displays the available buttons (Wireless, Reset) of this device. |
| **Usage** | **WLAN On/Off/WPS** – The default is enabled. If it is not, the Wireless button will lose control over WLAN and WPS functions.<br>**Mesh Discovery** – Click it to find the available mesh node(s). The scanned result can be seen on Syslog.<br> |
| **Configuration Reset Button** | Switch the toggle to enable or disable the function of the factory reset button. |
| **Enable** | Switch the toggle to enable or disable the function of the buttons. |
| **Cancel** | Discard current settings. |
| **Apply** | Save the current settings. |

**Note:**

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

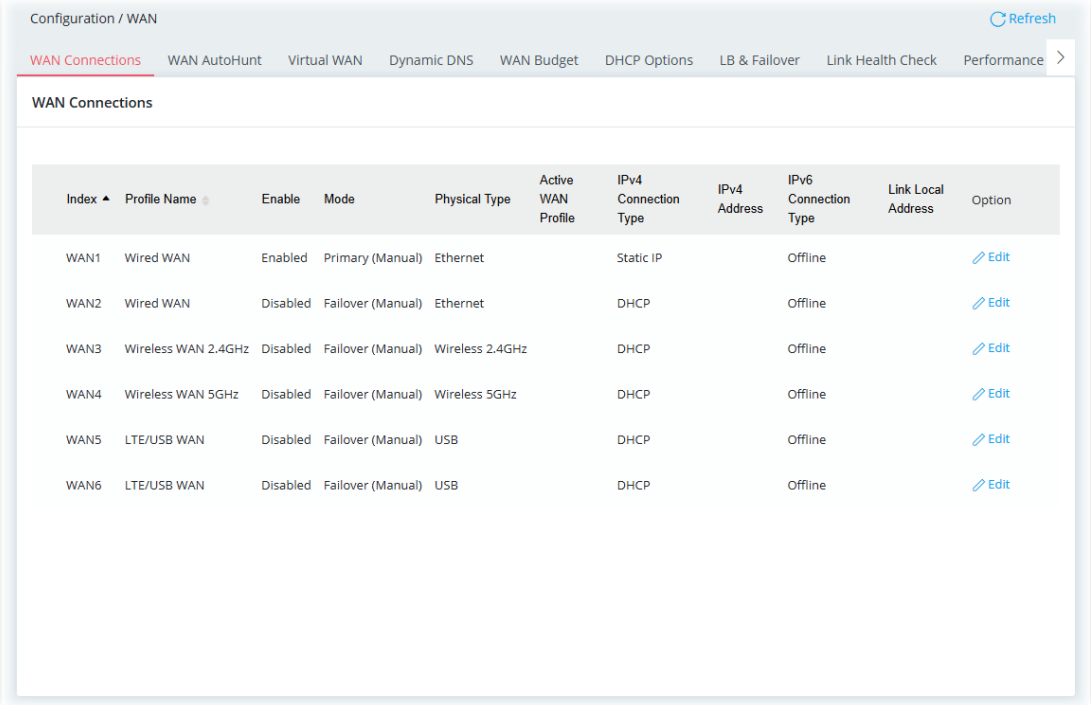
 - means “Enable”.

 - means “Disable”.

# II-1-2 WAN

## II-1-2-1 WAN Connections

This page is to configure the general settings for WAN connection.




Available settings are explained as follows:

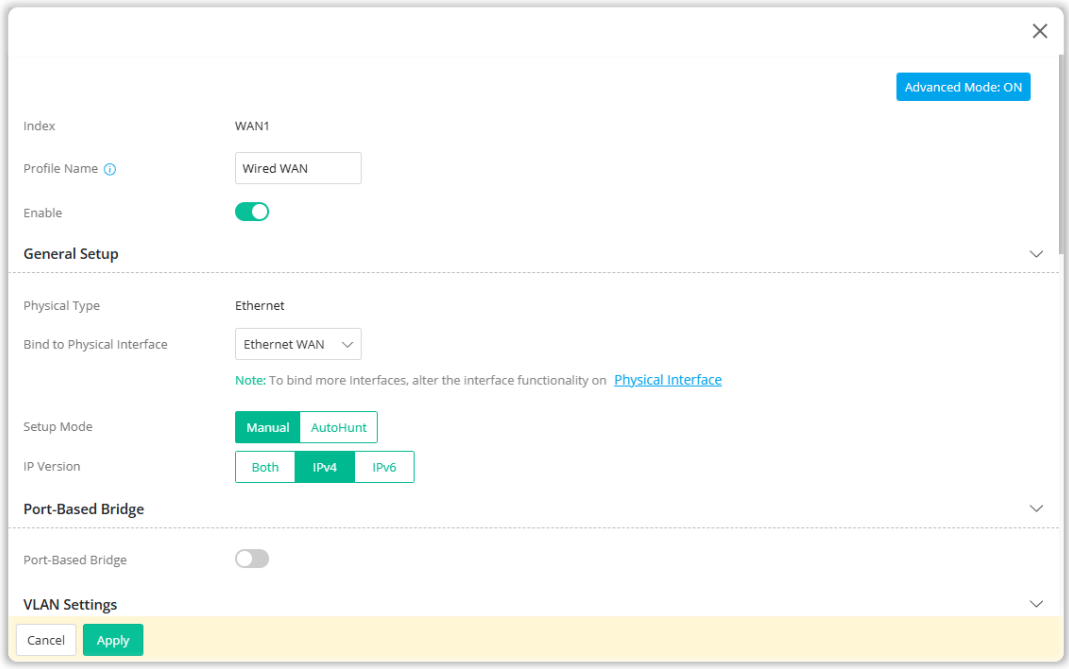
| Item | Description |
|---|---|
| **Profile Name** | Displays the name of the interface. |
| **Enable** | Displays if the WAN interface is enabled or disabled. |
| **Mode** | Displays if the WAN interface is primary or failover interface. |
| **Physical Type** | Displays the physical type (e.g., Ethernet, Wireless 2.4GHz, Wireless 5GHz or USB) of the WAN interface. |
| **Active WAN Profile** | Displays the active Autohunt profile applied for this WAN interface. |
| **IPv4 Connection Type** | Displays the IPv4 connection type (e.g, Static IP, DHCP and etc.) used by the WAN interface. |
| **IPv4 Address** | Displays the IP address assigned by the DHCP server or the static IP address specified manually. |
| **IPv6 Connection Type** | Displays the IPv6 connection type used by the WAN interface. |
| **Link Local Address** | Displays the IPv6 address for the IPv6 connection type – Static. |
| **Option** | **Edit** - Click to modify the interface name and physical mode. |

To configure the detailed settings (varied by physical type) for the selected WAN interface, click the **Edit** link to the right side of the WAN interface.

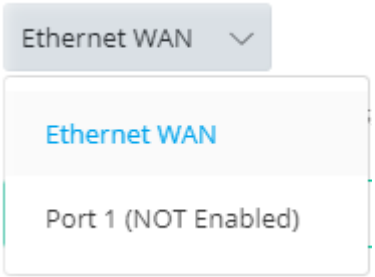
For Physical Type with Ethernet

Ethernet WAN and Port 1 can be configured as the WAN interfaces. WAN connections for these two ports can be configured separately.

Click the **Edit** link for WAN1 or WAN2 (LAN port 1) to open the following page.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Advanced Mode:ON/OFF** | Click to show or hide the advanced settings (IP Alias and WAN MAC Address) for the WAN interface. |
| **Index** | Displays current WAN interface. |
| **Profile Name** | Displays the name of the profile. |
| **Enable** | Switch the toggle to enable or disable the function. |
| **General Setup** | |
| **Physical Type** | Displays the physical type used by this interface. |
| **Bind to Physical Interface** | Select a physical interface (Ethernet). If LAN port 1 has been set as WAN port, it will be shown as Port 1 (Enabled) available for chosen as the WAN interface.<br> |
| **Setup Mode** | Determine the WAN connection established on the settings page |

| | |
|---|---|
| | or automatically based on the AutoHunt profiles, processed one by one.<br>**Manual** – If selected, the WAN connection will be performed according to the settings configured in this page.<br>**AutoHunt** – The Vigor router will automatically connect to Ethernet WAN connection. Once connected and powered on, the router will run through a list of network connection settings (based on the autohunt profiles) to determine if it can establish a connection. If it is unable to connect, the mechanism will proceed to the next ISP setting until it receives an IP address.<br>If Auto Hunt is selected, configure the following:<br>• **AutoHunt Profile** – Select the AutoHunt profile(s).<br>• **+Add** – Click to specify the autohunt profile(s). |
| **IP Version** | Set the protocol (IPv4 or IPv6 or both) that this WAN interface used. |
| | **Port-Based Bridge** |
| **Port Based Bridge** | Switch the toggle to enable or disable the function. |
| **Binding Interface** | Select the interfaces for binding. |
| **Bridge VLAN** | This function can bridge VLAN-tagged frames between the selected interfaces. |
| **+Add** | Click to create a bridge VLAN tag. |
| **VLAN Tag** | Enter the value as the VLAN ID number. The range is from 0 to 4094. |
| **Keep VLAN** | Check this box to forward (bridge) VLAN-tagged frames without removing the VLAN tag. |
| **Option** | **Delete** – Click to remove the selected item. |
| | **VLAN Settings** |
| **Customer VLAN** | Switch the toggle to enable or disable the function of VLAN with tag. If enabled, enter the values for the tag and priority.<br>**Tag** - Enter the value as the VLAN ID number. The range is from 0 to 4094.<br>**Priority** - Enter the packet priority number for such VLAN. The range is from 0 to 7. |
| **Service VLAN** | Switch the toggle to enable or disable the function of VLAN with tag. If enabled, enter the values for the tag and priority.<br>**Tag** - Enter the value as the VLAN ID number. The range is from 0 to 4094.<br>**Priority** - Enter the packet priority number for such VLAN. The range is from 0 to 7. |
| | **IPv4** |
| **IPv4 Connection Type** | It is available when Both or IPv4 is selected as IP Version and the Port Based Bridge is inactive.<br>**PPPoE** – Set the access mode as PPPoE.<br>• **Username** – Username provided by the ISP for PPPoE authentication.<br>• **Password** – Password provided by the ISP for PPPoE authentication.<br>• **Service Name (Optional) –** PPP service name tag. Required |

| | |
|---|---|
| | by some ISPs. Leave blank unless instructed otherwise by your ISP. This feature is available only when Advanced Mode is activated.<br>• **PPP Authentication –** The protocol used for PPP authentication. **PAP or CHAP**- Both PAP and CHAP (Challenge-Handshake Authentication Protocol) can be used for PPP authentication. Router negotiates with the PPTP or L2TP server to determine which protocol to use. This feature is available only when Advanced Mode is activated.<br>• **IP Assignment –**This feature is available only when Advanced Mode is activated. It is available when PPPoE is selected as IPv4 Connection Type.<br>**DHCP** - WAN IP address is dynamically allocated.<br>**Static IP** - ISP has assigned a fixed WAN IP address. Enter an IP address.<br>**DHCP** – The router receives IP configuration information from a DHCP server.<br>• **WAN DNS** – Select **Auto** or **Manual**.<br>If Manual is selected, specify the primary and secondary DNS servers.<br>**IPv4 Primary DNS** –IP address of primary DNS server.<br>**IPv4 Secondary DNS** - IP address of secondary DNS server.<br>**Static IP** – Set the access mode as Static IP.<br>• **IP Address** – WAN IP address assigned by the ISP.<br>• **Subnet Mask** – WAN subnet mask.<br>• **Gateway IP** – IP address of the WAN Gateway.<br>• **IPv4 Primary DNS** –IP address of primary DNS server.<br>• **IPv4 Secondary DNS** - IP address of secondary DNS server.<br>**Outbound DNS Query IP -** This feature is available only when Advanced Mode is activated and PPPoE/DHCP/Static IP is selected as the IPv4 Connection Type. Specify the source IP address which will be used by the router to send out the DNS query.<br>• **Default IP –** The query IP is set by Vigor router automatically.<br>• **Alias IP –** Enter a user-defined IP for DNS query. |
| **WAN Connection Detection** | |
| **Mode** | Configures how the WAN connection is monitored.<br>**Always On -** The router assumes the WAN connection is always active.<br>**ARP Detect** - The router broadcasts an ARP request every 5 seconds. If no response is received within 30 seconds, the WAN connection is deemed to have failed.<br>**Ping Detect** - The router sends an ICMP (Internet Control Message Protocol) echo request every second to the host, whose address is specified in the Ping IP field, to verify the WAN connection. If the remote host does not respond within 30 seconds, the WAN connection is deemed to have failed.<br>If you choose **Ping Detect** as the detection mode, you have to enter required settings for the following items.<br>• **Ping Gateway IP** - Switch the toggle to enable/ use the current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off. |

| | |
|---|---|
| | • **TTL** –Time To Live, the maximum allowed number of hops to the ping destination. Valid values range from 1 to 255.<br>• **Ping Interval (Sec, 10-3600)** – Enter the interval for the system to execute the PING operation.<br>• **Ping Retry** - Enter the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged. |
| IP Alias | **IPv4 Alias** - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using.<br>**+Add** – Click to add an IPv4 address as the IPv4 alias. |
| | IPv6 |
| IPv6 Connection Type | It is available when Both or IPv6 is selected as IP Version.<br>**Offline** – When Offline is selected, the IPv6 connection will be disabled.<br>• **WAN DNS** – Select **Auto** or **Manual**.<br>If Manual is selected, specify the primary and secondary DNS servers.<br>- **IPv6 Primary DNS** –IP address of primary DNS server.<br>- **IPv6 Secondary DNS** - IP address of secondary DNS server.<br>**PPP** – IPv6 WAN address is assigned along with the IPv4 WAN address during PPPoE negotiation. This IPv6 access mode requires that the IPv4 uses PPPoE.<br>• **WAN DNS** – Select **Auto** or **Manual**.<br>If Manual is selected, specify the primary and secondary DNS servers.<br>- **IPv6 Primary DNS** –IP address of primary DNS server.<br>- **IPv6 Secondary DNS** - IP address of secondary DNS server.<br>**Static** – Configure an ISP-assigned static IPv6 setup.<br>• **+Add** –Click this button to add the values in the IPv6 Address and Prefix Length fields to the **Global Address Table**.<br>• **IPv6 Global Address** – WAN IPv6 address assigned by the ISP.<br>• **Prefix Length –** Length of the IPv6 prefix.<br>• **Gateway Address -** IPv6 address of the ISP gateway.<br>• **IPv6 Primary DNS** –IPv6 address of primary DNS server.<br>• **IPv6 Secondary DNS** – IPv6 address of secondary DNS server.<br>**DHCPv6** – Use DHCPv6 protocol to obtain IPv6 address from server.<br>• **DUID** – Displays the DHCP unique ID used by this WAN interface.<br>• **IAID** – Unique integer that identifies this WAN interface.<br>• **Authentication Protocol** - This protocol will be used for the client to be authenticated by DHCPv6 server before accessing into Internet. There are three types can be specified, **Reconfigure Key**, **Delayed** and **None**. In general, the default setting is None.<br>- **Reconfigure Key** – During the connection process, DHCPv6 server will authenticate the client automatically.<br>- **Delayed** - During the connection process, DHCPv6 server will authenticate and identify the client based on the key |

ID, realm and secret information specified in these fields.
**Key ID** – Type a value (range from 1 to 65535) which will be used to generate HMAC-MD5 value.
**Realm** – The name (1 to 31 characters) typed here will identify the key which generates HMAC-MD5 value.
**Secret** – Type a text (1 to 31 characters) as s a unique identifier for each client on each DHCP server.

- **WAN DNS** – Select **Auto** or **Manual**.

  If Manual is selected, specify the primary and secondary DNS servers.

  - **IPv6 Primary DNS** –IP address of primary DNS server.
  - **IPv6 Secondary DNS** - IP address of secondary DNS server.

**TSPC** - Tunnel setup protocol client (TSPC) is an application which could help you to connect to IPv6 network easily.

Please make sure your IPv4 WAN connection is OK and apply one free account from hexago (http://gogonet.gogo6.com/page/freenet6-account ) before you try to use TSPC for network connection. TSPC would connect to tunnel broker and requests a tunnel according to the specifications inside the configuration file. It gets a public IPv6 IP address and an IPv6 prefix from the tunnel broker and then monitors the state of the tunnel in background.

After getting the IPv6 prefix and starting router advertisement daemon (RADVD), the PC behind this router can directly connect to IPv6 the Internet.

- **Tunnel Broker Address** – Enter the address for the tunnel broker IP, FQDN or an optional port number.
- **Username** – It is suggested for you to apply another username and password for http://gogonet.gogo6.com/page/freenet6-account.
- **Password** - Enter the password assigned with the user name.
- **WAN DNS** – Select **Auto** or **Manual**.

  If Manual is selected, specify the primary and secondary DNS servers.

  - **IPv6 Primary DNS** –IP address of primary DNS server.
  - **IPv6 Secondary DNS** - IP address of secondary DNS server.

**6in4** – Setup 6in4 Static Tunnel for WAN interface.

However, 6in4 offers a prefix outside of 2002::0/16. So, you can use a fixed endpoint rather than any cast endpoint. The mode has more reliability.

- **Enable IPv4 WAN Ping Access for 6in4/6rd Tunnel** – To use this 6in4 connection type, IPv4 WAN access must be allowed, and the firewall must allow the Tunnel Broker IP address to pass through.
- **Remote Endpoint IPv4 Address** – WAN IPv6 address assigned by the tunnel provider.
- **6in4 IPv6 Address** – WAN IPv6 address assigned by the tunnel provider.
- **6in4 IPv6 Prefix Length –** WAN IPv6 prefix length assigned by the tunnel provider.
- **LAN Routed Prefix –** LAN IPv6 address prefix.
- **LAN Routed Prefix Length –** LAN IPv6 address prefix length.
- **Tunnel TTL –** Time to live value, which is the maximum

| | |
|---|---|
| | number of hops allowed to the endpoint.<br>• **WAN DNS** – Select **Auto** or **Manual**.<br>If Manual is selected, specify the primary and secondary DNS servers.<br>- **IPv6 Primary DNS** –IP address of primary DNS server.<br>- **IPv6 Secondary DNS** - IP address of secondary DNS server.<br>**6rd** - Setup 6rd for WAN interface.<br>• **Enable IPv4 WAN Ping Access for 6in4/6rd Tunnel** – To use this 6rd connection type, IPv4 WAN access must be allowed, and the firewall must allow the Tunnel Broker IP address to pass through.<br>• **Mode** – Two options, Auto and Static. **Auto** - Used in conjunction with DHCPv4, the router automatically provisions IPv6 using option 212. **Static** - IPv6 configuration information is manually entered.<br>• **IPv4 Border Relay** – Enter the IPv4 addresses of the 6rd Border Relay for a given 6rd domain.<br>• **6rd Prefix** – Enter the 6rd IPv6 address.<br>• **6rd Prefix Length** - Enter the IPv6 prefix length for the 6rd IPv6 prefix in number of bits.<br>• **WAN DNS** – Select **Auto** or **Manual**.<br>If Manual is selected, specify the primary and secondary DNS servers.<br>- **IPv6 Primary DNS** –IP address of primary DNS server.<br>- **IPv6 Secondary DNS** - IP address of secondary DNS server. |
| IPv6 WAN Connection Detection | |
| Mode | Configures how the WAN connection is monitored. Available modes will vary based on the selected IPv6 Connection Type.<br>**Always On -** The router assumes the WAN connection is always active.<br>**NS Detect** - The router verifies connectivity by issuing Neighbor Solicitation packets.<br>**Ping Detect** - The router sends an ICMP (Internet Control Message Protocol) echo request every second to the host, whose address is specified in the Ping IP field, to verify the WAN connection. If the remote host does not respond within 30 seconds, the WAN connection is deemed to have failed.<br>If you choose **Ping Detect** as the detection mode, you have to enter required settings for the following items.<br>• **Primary Ping IP** – Enter an IP address in this field for pinging.<br>• **Secondary Ping IP** - Enter an IP address in this field for pinging.<br>• **TTL** –Time To Live, the maximum allowed number of hops to the ping destination. Valid values range from 1 to 255.<br>• **Ping Interval (Sec, 10-3600)** – Enter the interval for the system to execute the PING operation.<br>• **Ping Retry** - Enter the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged. |
| MTU | |

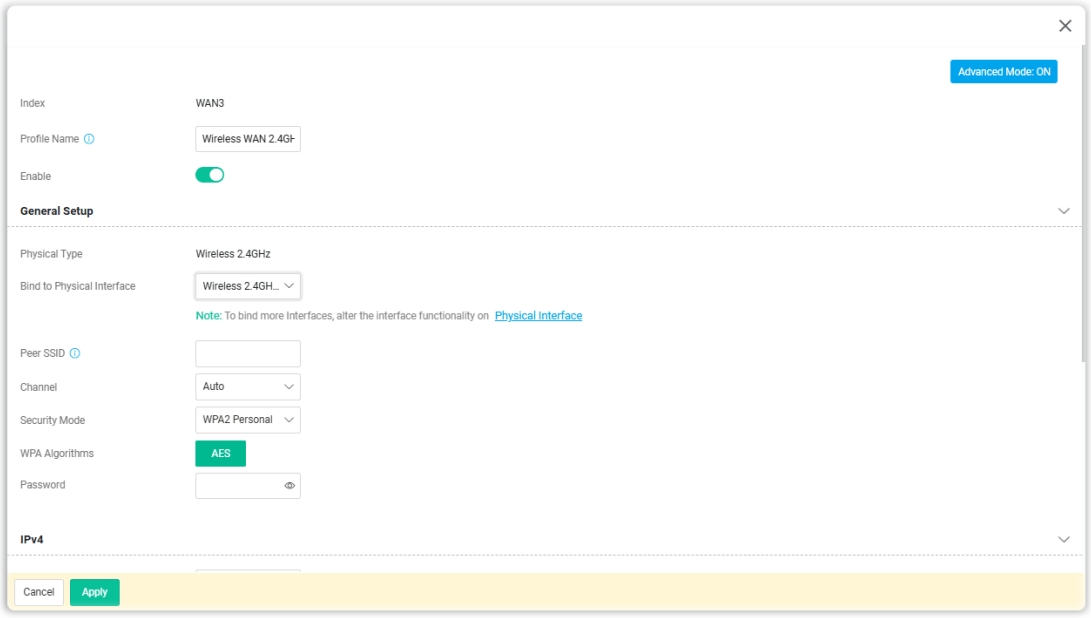
| | |
|---|---|
| MTU | Maximum Transmission Unit, the size of the largest packet, in bytes, that can be transmitted to the WAN. The maximum value is 1500. For PPPoE connections, there is always an 8-byte overhead, so the maximum valid MTU value for PPPoE is 1492. |
| WAN MAC Address | |
| Mode | **Default** – Use the default MAC address for the WAN port.<br>• **MAC -** Displays the MAC address of this device.<br>**Customized** - Select this option if your ISP authenticates by MAC addresses.<br>• **MAC** - Specify a MAC address for the WAN Ethernet port. |
| Cancel | Discard current settings and return to previous page. |
| Apply | Save the current settings and exit the page. |

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

For Physical Type with Wireless 2.4GHz

When Wireless 2.4G is selected as Physical Type, WAN interface uses wireless station mode to access Internet. The Router acts as a 2.4GHz wireless station and connects to the specific Wireless AP.

Click the **Edit** link for WAN3 or WAN4 to open the following page.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Advanced Mode:ON/OFF** | Click to show or hide the advanced settings (WAN MAC Address) for the WAN interface. |
| **Index** | Displays current WAN interface. |
| **Profile Name** | Displays the name of the profile. |
| **Enable** | Switch the toggle to enable or disable the function. |
| **General Setup** | |
| **Physical Type** | Displays the physical type used by this interface. |
| **Bind to Physical Interface** | At present, only Wireless 2.4GHz is available for WAN3 and Wireless 5GHz for WAN4.<br> |
| **Peer SSID** | Enter the identification of the wireless device. |
| **Channel** | Select the channel of frequency of the device. |
| **Security Mode** | There are several modes provided for you to choose from. Each mode will bring up different parameters (e.g., Pass Phrase) for you |

| | |
|---|---|
| | to configure.<br>**WPA3 Personal** – The Router connects to the wireless AP as a WPA3 client and the encryption key should be entered in PSK.<br>**WPA2 Personal** – The Router connects to the wireless AP as a WPA2 client and the encryption key should be entered in PSK.<br>**OPEN** – The encryption mechanism is turned off. |
| **WPA Algorithms** | Select AES as the algorithm for WPA. |
| **Password** | Enter **8~64** ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). |
| | **IPv4** |
| **IPv4 Connection Type** | It is available when Both or IPv4 is selected as IP Version.<br>**DHCP** – The router receives IP configuration information from a DHCP server.<br>● **WAN DNS** - Select **Auto** or **Manual**.<br>If Manual is selected, specify the primary and secondary DNS servers.<br>**IPv4 Primary DNS** - IP address of primary DNS server.<br>**IPv4 Secondary DNS** - IP address of secondary DNS server.<br>**Static IP** – Set the access mode as Static IP.<br>● **IP Address** – WAN IP address assigned by the ISP.<br>● **Subnet Mask** – WAN subnet mask.<br>● **Gateway IP** – IP address of the WAN Gateway.<br>● **IPv4 Primary DNS** – IP address of primary DNS server.<br>● **IPv4 Secondary DNS** - IP address of secondary DNS server. |
| | **WAN Connection Detection** |
| **Mode** | Configures how the WAN connection is monitored.<br>**Always On -** The router assumes the WAN connection is always active.<br>**ARP Detect** - The router broadcasts an ARP request every 5 seconds. If no response is received within 30 seconds, the WAN connection is deemed to have failed.<br>**Ping Detect** - The router sends an ICMP (Internet Control Message Protocol) echo request every second to the host, whose address is specified in the Ping IP field, to verify the WAN connection. If the remote host does not respond within 30 seconds, the WAN connection is deemed to have failed.<br>If you choose **Ping Detect** as the detection mode, you have to enter required settings for the following items.<br>● **Ping Gateway IP** - Switch the toggle to enable/ use the current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off.<br>● **TTL** –Time To Live, the maximum allowed number of hops to the ping destination. Valid values range from 1 to 255.<br>● **Ping Interval (Sec, 5-3600)** – Enter the interval for the system to execute the PING operation.<br>● **Ping Retry** - Enter the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged. |

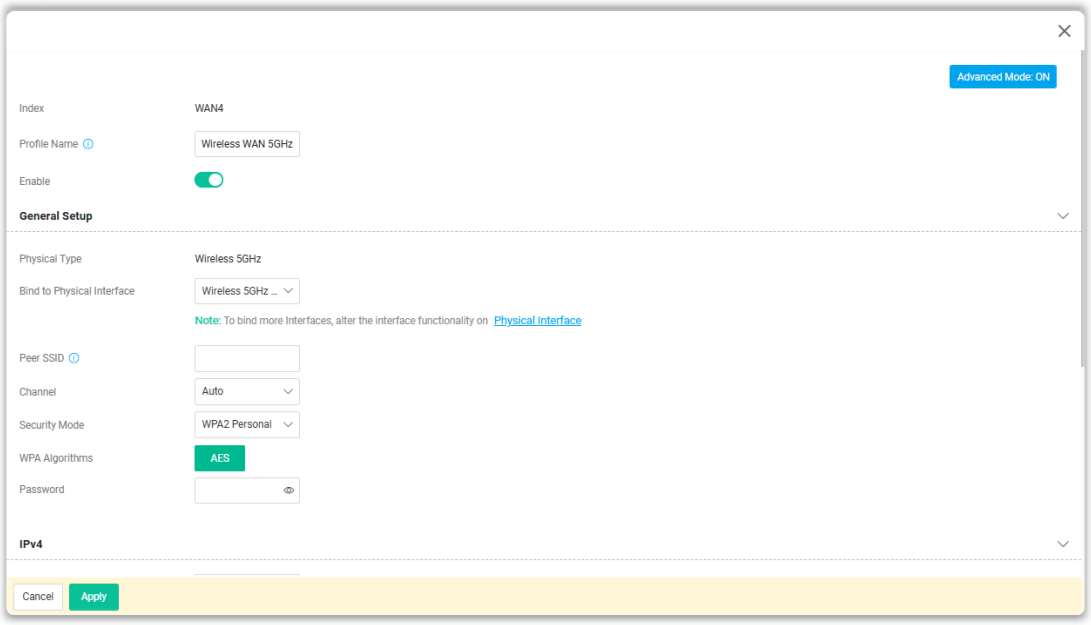
| MTU | |
|---|---|
| MTU | Maximum Transmission Unit, the size of the largest packet, in bytes, that can be transmitted to the WAN. The maximum value is 1500. For PPPoE connections, there is always an 8-byte overhead, so the maximum valid MTU value for PPPoE is 1492. |
| **WAN MAC Address** | |
| Mode | **Default** – Use the default MAC address for the wireless WAN.<br>• **MAC -** Displays the MAC address of this device.<br>**Customized** - Select this option to use customized MAC addresses.<br>• **MAC** - Specify a MAC address for the wireless WAN. |
| Cancel | Discard current settings and return to previous page. |
| Apply | Save the current settings and exit the page. |

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

For Physical Type with Wireless 5GHz

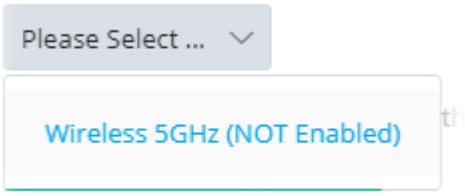
When Wireless 5G is selected as Physical Type, WAN interface uses wireless station mode to access Internet. The Router acts as a 5GHz wireless station and connects to the specific Wireless AP.

Click the **Edit** link for WAN4 to open the following page.




Available settings are explained as follows:

| Item | Description |
|---|---|
| Advanced Mode:ON/OFF | Click to show or hide the advanced settings (WAN MAC Address) for the WAN interface. |
| Index | Displays current WAN interface. |
| Profile Name | Displays the name of the profile. |

| | |
|---|---|
| **Enable** | Switch the toggle to enable or disable the function. |
| | **General Setup** |
| **Physical Type** | Displays the physical type used by this interface. |
| **Bind to Physical Interface** | At present, only Wireless 2.4GHz is available for WAN3 and Wireless 5GHz for WAN4.<br> |
| **Peer SSID** | Enter the identification of the wireless device. |
| **Channel** | Select the channel of frequency of the device. |
| **Security Mode** | There are several modes provided for you to choose from. Each mode will bring up different parameters (e.g., Pass Phrase) for you to configure.<br>**WPA3 Personal** – The Router connects to the wireless AP as a WPA3 client and the encryption key should be entered in PSK.<br>**WPA2 Personal** – The Router connects to the wireless AP as a WPA2 client and the encryption key should be entered in PSK.<br>**OPEN** – The encryption mechanism is turned off. |
| **WPA Algorithm** | Select AES as the algorithm for WPA. |
| **Password** | Enter **8~64** ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde..."). |
| | **IPv4** |
| **IPv4 Connection Type** | It is available when Both or IPv4 is selected as IP Version.<br>**DHCP** – The router receives IP configuration information from a DHCP server.<br>• **WAN DNS** - Select **Auto** or **Manual**.<br>If Manual is selected, specify the primary and secondary DNS servers.<br>**IPv4 Primary DNS** - IP address of primary DNS server.<br>**IPv4 Secondary DNS** - IP address of secondary DNS server.<br>**Static IP** – Set the access mode as Static IP.<br>• **IP Address** – WAN IP address assigned by the ISP.<br>• **Subnet Mask** – WAN subnet mask.<br>• **Gateway IP** – IP address of the WAN Gateway.<br>• **IPv4 Primary DNS** – IP address of primary DNS server.<br>• **IPv4 Secondary DNS** - IP address of secondary DNS server. |
| | **WAN Connection Detection** |
| **Mode** | Configures how the WAN connection is monitored.<br>**Always On -** The router assumes the WAN connection is always active.<br>**ARP Detect** - The router broadcasts an ARP request every 5 |

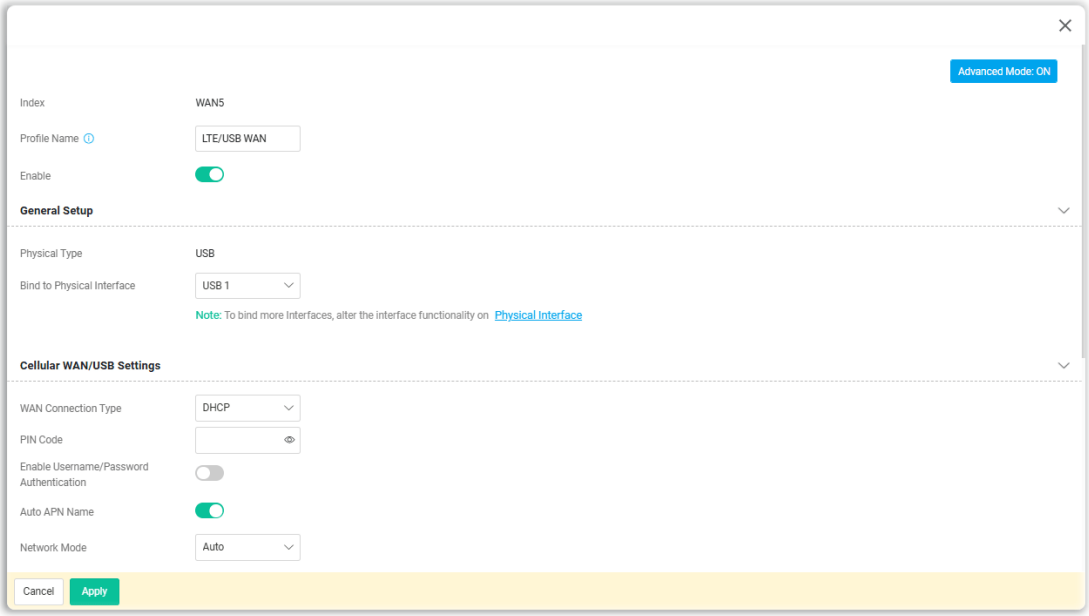
| | |
|---|---|
| | seconds. If no response is received within 30 seconds, the WAN connection is deemed to have failed.<br>**Ping Detect** - The router sends an ICMP (Internet Control Message Protocol) echo request based on the ping interval setting to the host, whose address is specified in the Ping Gateway IP field, to verify the WAN connection. If the remote host does not respond within certain seconds (defined in the ping interval), the WAN connection is deemed to have failed.<br>If you choose **Ping Detect** as the detection mode, you have to enter required settings for the following items.<br>• **Ping Gateway IP** - Switch the toggle to enable/ use the current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off.<br>• **TTL** –Time To Live, the maximum allowed number of hops to the ping destination. Valid values range from 1 to 255.<br>• **Ping Interval (Sec, 5-3600)** – Enter the interval for the system to execute the PING operation.<br>• **Ping Retry** - Enter the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged. |
| **MTU** | |
| **MTU** | Maximum Transmission Unit, the size of the largest packet, in bytes, that can be transmitted to the WAN. The maximum value is 1500. For PPPoE connections, there is always an 8-byte overhead, so the maximum valid MTU value for PPPoE is 1492. |
| **WAN MAC Address** | |
| **Mode** | **Default** – Use the default MAC address for the wireless WAN.<br>• **MAC -** Displays the MAC address of this device.<br>**Customized** - Select this option to use customized MAC addresses.<br>• **MAC** - Specify a MAC address for the wireless WAN. |
| **Cancel** | Discard current settings and return to previous page. |
| **Apply** | Save the current settings and exit the page. |

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

For Physical Type with LTE/USB

It is available for USB modem only. USB WAN uses the embedded module to access internet.

Click the **Edit** link for WAN5 or WAN6 to open the following page.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Advanced Mode:ON/OFF** | Click to show or hide the advanced settings (WAN MAC Address) for the WAN interface. |
| **Name** | Displays current WAN interface. |
| **Enable** | Switch the toggle to enable or disable the access mode. |
| **General Setup** | |
| **Physical Type** | Displays the physical type used by this interface. |
| **Bind to Physical Interface** | When an external USB modem has been connected to USB port, select USB1 or USB2 as the physical WAN interface according to the location of the modem connected.<br> |
| **Cellular WAN/USB Settings** | |
| **WAN Connection Type** | **DHCP** – Dynamic Host Configuration Protocol is used to establish a connection.<br>**PPP** - Point-to-Point Protocol is used to establish a connection. |
| **PIN Code** | PIN code of the SIM card in the modem. The maximum length of the PIN is 15 characters. |
| **Enable Username/Password Authentication** | Switch the toggle to enable or disable the function.<br>**Authentication** – Select the protocol used for PPP authentication.<br>• **PAP only** - Only PAP (Password Authentication Protocol) is |

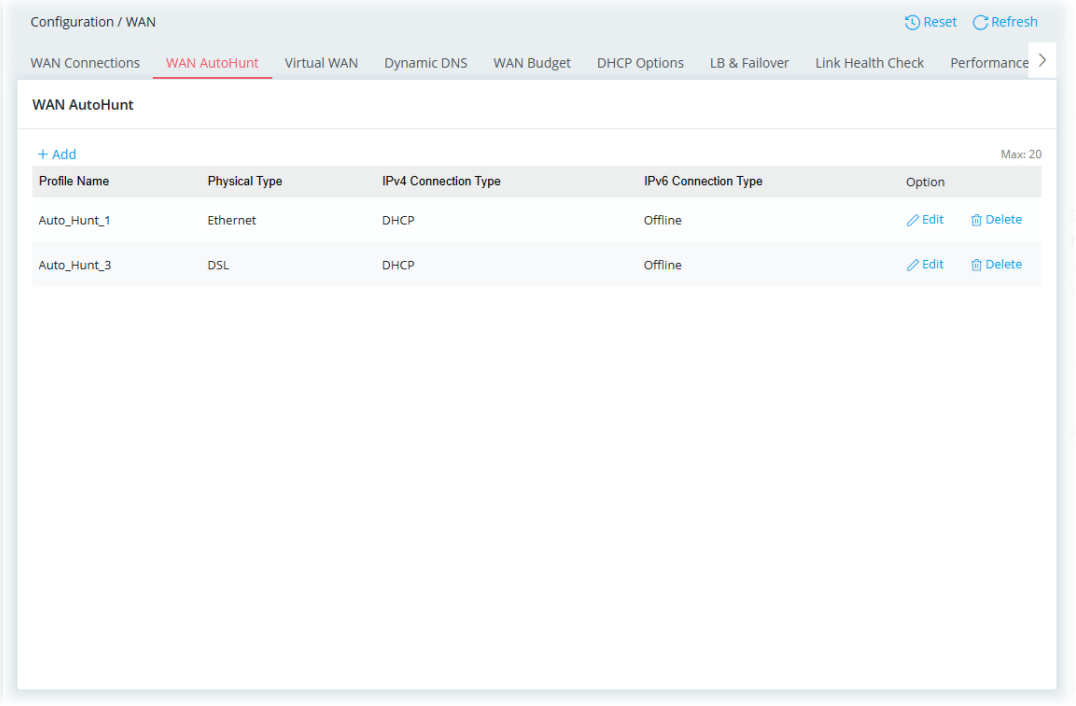
| | |
|---|---|
| | used.<br>• **PAP or CHAP** - Both PAP and CHAP (Challenge-Handshake Authentication Protocol) can be used for PPP authentication. Router negotiates with the PPTP or L2TP server to determine which protocol to use.<br>**Username** – Username provided by the ISP for authentication (optional).<br>**Password** - Password provided by the ISP for authentication (optional). |
| **Generate Modem Initial String by** | Configure this setting if PPP is selected as the **WAN Connection Type.**<br>**Following APN Name** – Use the APN name as the modem initial string.<br>• **Modem Initial String2 (Optional)** –The initial string 1 is shared with APN. In some cases, user may need another initial AT command to restrict 3G band or do any special settings.<br>• **Modem Dial String (Optional)** - It is used to dial through USB mode. Please use the default value. If you have any question, please contact to your ISP.<br>**Customized String** – Set a string as the modem initial string.<br>• **Modem Initial String (Optional)** – It is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP.<br>• **Modem Initial String2 (Optional)** – The initial string 1 is shared with APN. In some cases, user may need another initial AT command to restrict 3G band or do any special settings.<br>• **Modem Dial String (Optional)** – It is used to dial through USB mode. Please use the default value. If you have any question, please contact to your ISP. |
| **Auto APN Name** | Access Point Name to be used for the connection. Please contact your ISP or carrier for the appropriate value.<br>If disabling this feature, enter the APN name. |
| **Service Name (Optional)** | Configure this setting if PPP is selected as the **WAN Connection Type.**<br>Enter the description of the specific network service. |
| **Network Mode** | Configure this setting if DHCP is selected as the **WAN Connection Type.**<br>Force Vigor router to connect Internet with the mode specified here. If you choose 4G Only/3G Only/Auto as network mode, the router will choose a suitable one according to the actual wireless signal automatically. |
| **IPv4 - WAN Connection Detection** | |
| **WAN DNS** | Select **Auto** or **Manual**.<br>If Manual is selected, specify the primary and secondary DNS servers.<br>• **IPv4 Primary DNS** –IP address of primary DNS server.<br>• **IPv4 Secondary DNS** - IP address of secondary DNS server. |
| **Mode** | Configures how the WAN connection is monitored. The options available are based on the selected WAN connection type.<br>**Always On -** The router assumes the WAN connection is always |

| | |
|---|---|
| | active.<br>**PPP Detect** – A method which detects if PPP connection between the router and the ISP is successful or not.<br>**Ping Detect** - The router sends an ICMP (Internet Control Message Protocol) echo request every second to the host, whose address is specified in the Ping IP field, to verify the WAN connection. If the remote host does not respond within 30 seconds, the WAN connection is deemed to have failed.<br>If you choose **Ping Detect** as the detection mode, you have to enter required settings for the following items.<br>• **Ping Gateway IP** - Switch the toggle to enable/ use the current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off.<br>• **TTL** –Time To Live, the maximum allowed number of hops to the ping destination. Valid values range from 1 to 255.<br>• **Ping Interval (Sec, 5-3600)** – Enter the interval for the system to execute the PING operation.<br>• **Ping Retry** - Enter the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged. |
| MTU | |
| **MTU** | Maximum Transmission Unit, the size of the largest packet, in bytes, that can be transmitted to the WAN. The maximum value is 1500. For PPPoE connections, there is always an 8-byte overhead, so the maximum valid MTU value for PPPoE is 1492. |
| WAN MAC Address | |
| **Mode** | It is available when **Advanced Mode** is **ON.**<br>**Default** – Use the default MAC address for the WAN port.<br>**Customized** - Select this option if your ISP authenticates by MAC addresses.<br>• **MAC** - Specify a MAC address for the WAN Ethernet port. |
| **Cancel** | Discard current settings and return to previous page. |
| **Apply** | Save the current settings and exit the page. |

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

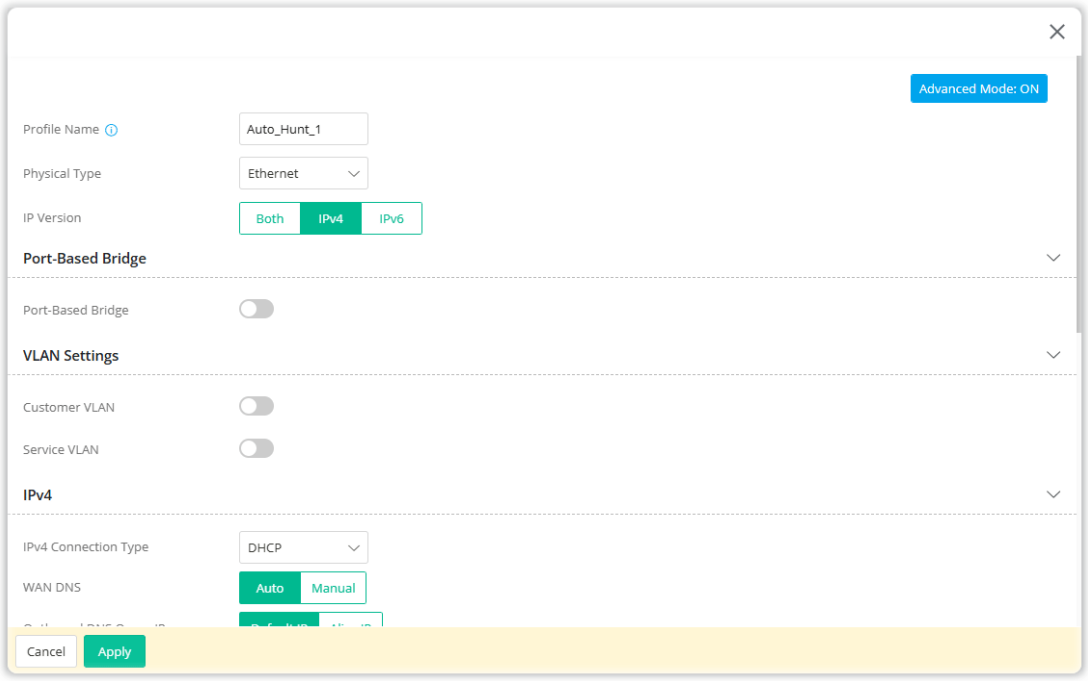
## II-1-2-2 WAN AutoHunt

The Vigor router will automatically connect to Ethernet WAN connection. Once connected and powered on, the router will run through a list of network connection settings (based on the autohunt profiles) to determine if it can establish a connection. If it is unable to connect, the mechanism will proceed to the next ISP setting until it receives an IP address.




| Item | Description |
|---|---|
| **Reset** | Click to clear all profiles to factory settings. |
| **+Add** | Click to bring up the configuration page of the virtual WAN profile (max. 20). |

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




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Advanced Mode:ON/OFF** | Click to show or hide the advanced settings (IP Alias and WAN MAC Address) for the WAN interface. |
| **Physical Type** | Displays the physical type used by this interface. |
| **IP Version** | Set the protocol (IPv4 or IPv6 or both) that this WAN interface used. |
| **Port-Based Bridge** | |
| **Port-Based Bridge** | Switch the toggle to enable or disable the function. |
| **Binding Interface** | Select the interfaces for binding. |
| **Bridge VLAN** | This function can bridge VLAN-tagged frames between the selected interfaces. |
| **+Add** | Click to create a bridge VLAN tag. |
| **VLAN Tag** | Enter the value as the VLAN ID number. The range is from 0 to 4094. |
| **Keep VLAN** | Check this box to forward (bridge) VLAN-tagged frames without removing the VLAN tag. |
| **Option** | **Delete** – Click to remove the selected item. |
| **VLAN Settings** | |
| **Customer VLAN** | Switch the toggle to enable or disable the function of VLAN with tag. If enabled, enter the values for the tag and priority.<br>**Tag** - Enter the value as the VLAN ID number. The range is from 0 to 4094.<br>**Priority** - Enter the packet priority number for such VLAN. The range is from 0 to 7. |
| **Service VLAN** | Switch the toggle to enable or disable the function of VLAN with tag. If enabled, enter the values for the tag and priority.<br>**Tag** - Enter the value as the VLAN ID number. The range is from 0 to |

| | |
|---|---|
| | 4094.<br>**Priority** - Enter the packet priority number for such VLAN. The range is from 0 to 7. |
| **IPv4** | |
| **IPv4 Connection Type** | It is available when Both or IPv4 is selected as IP Version.<br>**PPPoE** – Set the access mode as PPPoE.<br>• **Username** – Username provided by the ISP for PPPoE authentication.<br>• **Password** – Password provided by the ISP for PPPoE authentication.<br>• **Service Name (Optional)** – PPP service name tag. Required by some ISPs. Leave blank unless instructed otherwise by your ISP.<br>• **PPP Authentication** – The protocol used for PPP authentication.<br>**PAP or CHAP** - Both PAP and CHAP (Challenge-Handshake Authentication Protocol) can be used for PPP authentication. Router negotiates with the PPTP or L2TP server to determine which protocol to use.<br>• **IP Assignment** – It is available when PPPoE is selected as IPv4 Connection Type.<br>**DHCP** - WAN IP address is dynamically allocated.<br>**Static IP** - ISP has assigned a fixed WAN IP address. Enter an IP address.<br>• **WAN DNS** – Select **Auto** or **Manual**.<br>If Manual is selected, specify the primary and secondary DNS servers.<br>**IPv4 Primary DNS** –IP address of primary DNS server.<br>**IPv4 Secondary DNS** - IP address of secondary DNS server.<br>**DHCP** – The router receives IP configuration information from a DHCP server.<br>• **WAN DNS** – Select **Auto** or **Manual**.<br>If Manual is selected, specify the primary and secondary DNS servers.<br>**IPv4 Primary DNS** –IP address of primary DNS server.<br>**IPv4 Secondary DNS** - IP address of secondary DNS server.<br>**Static IP** – Set the access mode as Static IP.<br>• **IP Address** – WAN IP address assigned by the ISP.<br>• **Subnet Mask** – WAN subnet mask.<br>• **Gateway IP** – IP address of the WAN Gateway.<br>• **IPv4 Primary DNS** –IP address of primary DNS server.<br>• **IPv4 Secondary DNS** - IP address of secondary DNS server.<br>**Outbound DNS Query IP -** This feature is available only when Advanced Mode is activated. Specify the source IP address which will be used by the router to send out the DNS query.<br>• **Default IP –** The query IP is set by Vigor router automatically.<br>• **Alias IP –** Enter a user-defined IP for DNS query. |
| **WAN Connection Detection** | |
| **Mode** | Configures how the WAN connection is monitored. Select **PPP** |

| | |
|---|---|
| | **Detect, ARP Detect** or **Ping Detect** or **Always On**.<br>**PPP Detect –** A method which detects if PPP connection between the router and the ISP is successful or not.<br>**ARP Detect –** The router broadcasts an ARP request every 5 seconds. If no response is received within 30 seconds, the WAN connection is deemed to have failed.<br>**Always On -** The router assumes the WAN connection is always active.<br>**Ping Detect** - The router sends an ICMP (Internet Control Message Protocol) echo request every second to the host, whose address is specified in the Ping IP field, to verify the WAN connection. If the remote host does not respond within 30 seconds, the WAN connection is deemed to have failed.<br>If you choose **Ping Detect** as the detection mode, you have to enter required settings for the following items.<br>● **Ping Gateway IP** - Switch the toggle to enable/ use the current WAN gateway IP address for pinging. With the IP address(es) pinging, Vigor router can check if the WAN connection is on or off.<br>● **TTL** –Time To Live, the maximum allowed number of hops to the ping destination. Valid values range from 1 to 255.<br>● **Ping Interval (Sec, 10-3600)** – Enter the interval for the system to execute the PING operation.<br>● **Ping Retry** - Enter the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged. |
| IP Alias | **IPv4 Alias** - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using.<br>**+Add** – Click to add an IPv4 address as the IPv4 alias. |
| | IPv6 |
| IPv6 Connection Type | It is available when Both or IPv6 is selected as IP Version.<br>**Offline** – When Offline is selected, the IPv6 connection will be disabled.<br>● **WAN DNS** – Select **Auto** or **Manual**.<br>If Manual is selected, specify the primary and secondary DNS servers.<br>- **IPv6 Primary DNS** –IP address of primary DNS server.<br>- **IPv6 Secondary DNS** - IP address of secondary DNS server.<br>**PPP** – IPv6 WAN address is assigned along with the IPv4 WAN address during PPPoE negotiation. This IPv6 access mode requires that the IPv4 uses PPPoE.<br>● **WAN DNS** – Select **Auto** or **Manual**.<br>If Manual is selected, specify the primary and secondary DNS servers.<br>- **IPv6 Primary DNS** –IP address of primary DNS server.<br>- **IPv6 Secondary DNS** - IP address of secondary DNS server.<br>**Static** – Configure an ISP-assigned static IPv6 setup.<br>● **+Add** –Click this button to add the values in the IPv6 Address and Prefix Length fields to the **Global Address Table**. |

- **IPv6 Global Address** – WAN IPv6 address assigned by the ISP.
- **Prefix Length –** Length of the IPv6 prefix.
- **Gateway Address -** IPv6 address of the ISP gateway.
- **IPv6 Primary DNS** –IP address of primary DNS server.
- **IPv6 Secondary DNS** - IP address of secondary DNS server.

**DHCPv6** – Use DHCPv6 protocol to obtain IPv6 address from server.

- **IAID** – Unique integer that identifies this WAN interface.
- **Authentication Protocol** - This protocol will be used for the client to be authenticated by DHCPv6 server before accessing into Internet. There are three types can be specified, **Reconfigure Key**, **Delayed** and **None**. In general, the default setting is None.
  - **Reconfigure Key** – During the connection process, DHCPv6 server will authenticate the client automatically.
  - **Delayed** - During the connection process, DHCPv6 server will authenticate and identify the client based on the key ID, realm and secret information specified in these fields.
    **Key ID** – Type a value (range from 1 to 65535) which will be used to generate HMAC-MD5 value.
    **Realm** – The name (1 to 31 characters) typed here will identify the key which generates HMAC-MD5 value.
    **Secret** – Type a text (1 to 31 characters) as s a unique identifier for each client on each DHCP server.
- **WAN DNS** – Select **Auto** or **Manual**.

  If Manual is selected, specify the primary and secondary DNS servers.
  - **IPv6 Primary DNS** –IP address of primary DNS server.
  - **IPv6 Secondary DNS** - IP address of secondary DNS server.

**TSPC** - Tunnel setup protocol client (TSPC) is an application which could help you to connect to IPv6 network easily.

Please make sure your IPv4 WAN connection is OK and apply one free account from hexago (http://gogonet.gogo6.com/page/freenet6-account ) before you try to use TSPC for network connection. TSPC would connect to tunnel broker and requests a tunnel according to the specifications inside the configuration file. It gets a public IPv6 IP address and an IPv6 prefix from the tunnel broker and then monitors the state of the tunnel in background.

After getting the IPv6 prefix and starting router advertisement daemon (RADVD), the PC behind this router can directly connect to IPv6 the Internet.

- **Tunnel Broker Address** – Enter the address for the tunnel broker IP, FQDN or an optional port number.
- **Username** – It is suggested for you to apply another username and password for http://gogonet.gogo6.com/page/freenet6-account.
- **Password** - Enter the password assigned with the user name.
- **WAN DNS** – Select **Auto** or **Manual**.

  If Manual is selected, specify the primary and secondary DNS servers.
  - **IPv6 Primary DNS** –IP address of primary DNS server.
  - **IPv6 Secondary DNS** - IP address of secondary DNS server.

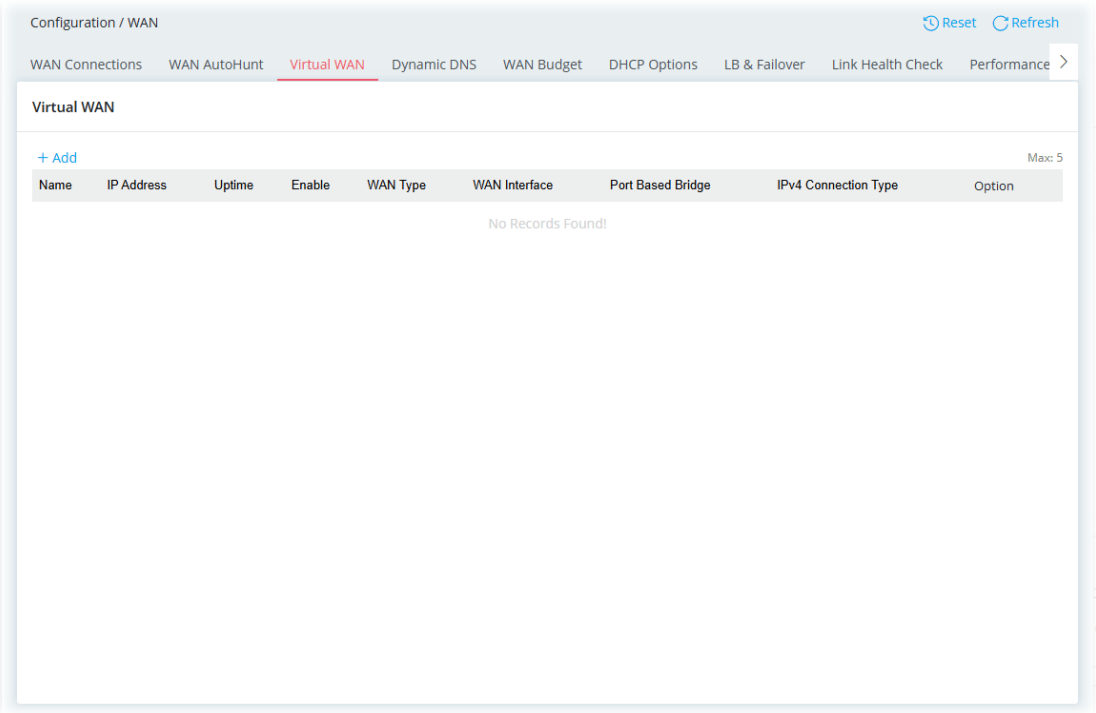
| | |
|---|---|
| | **6in4** – Setup 6in4 Static Tunnel for WAN interface.<br>However, 6in4 offers a prefix outside of 2002::0/16. So, you can use a fixed endpoint rather than any cast endpoint. The mode has more reliability.<br>• **Enable IPv4 WAN Ping Access for 6in4/6rd Tunnel** – To use this 6in4 connection type, IPv4 WAN access must be allowed, and the firewall must allow the Tunnel Broker IP address to pass through.<br>• **Remote Endpoint IPv4 Address** – WAN IPv6 address assigned by the tunnel provider.<br>• **6in4 IPv6 Address** – WAN IPv6 address assigned by the tunnel provider.<br>• **6in4 IPv6 Prefix Length –** WAN IPv6 prefix length assigned by the tunnel provider.<br>• **LAN Routed Prefix –** LAN IPv6 address prefix.<br>• **LAN Routed Prefix Length –** LAN IPv6 address prefix length.<br>• **Tunnel TTL –** Time to live value, which is the maximum number of hops allowed to the endpoint.<br>• **WAN DNS** – Select **Auto** or **Manual**.<br>If Manual is selected, specify the primary and secondary DNS servers.<br>- **IPv6 Primary DNS** –IP address of primary DNS server.<br>- **IPv6 Secondary DNS** - IP address of secondary DNS server.<br>**6rd** - Setup 6rd for WAN interface.<br>• **Enable IPv4 WAN Ping Access for 6in4/6rd Tunnel** – To use this 6rd connection type, IPv4 WAN access must be allowed, and the firewall must allow the Tunnel Broker IP address to pass through.<br>• **Mode** – Two options, Auto and Static. **Auto** - Used in conjunction with DHCPv4, the router automatically provisions IPv6 using option 212. **Static** - IPv6 configuration information is manually entered.<br>• **IPv4 Border Relay** – Enter the IPv4 addresses of the 6rd Border Relay for a given 6rd domain.<br>• **6rd Prefix** – Enter the 6rd IPv6 address.<br>• **6rd Prefix Length** - Enter the IPv6 prefix length for the 6rd IPv6 prefix in number of bits.<br>• **WAN DNS** – Select **Auto** or **Manual**.<br>If Manual is selected, specify the primary and secondary DNS servers.<br>- **IPv6 Primary DNS** –IP address of primary DNS server.<br>- **IPv6 Secondary DNS** - IP address of secondary DNS server. |
| **IPv6 WAN Connection Detection** | |
| **Mode** | Configures how the WAN connection is monitored.<br>**Always On -** The router assumes the WAN connection is always active.<br>**NS Detect** - The router verifies connectivity by issuing Neighbor Solicitation packets.<br>**Ping Detect** - The router sends an ICMP (Internet Control Message Protocol) echo request every second to the host, whose address is specified in the Ping IP field, to verify the WAN connection. If the |

| | |
|---|---|
| | remote host does not respond within 30 seconds, the WAN connection is deemed to have failed.<br>If you choose **Ping Detect** as the detection mode, you have to enter required settings for the following items.<br>• **Primary Ping IP** – Enter an IP address in this field for pinging.<br>• **Secondary Ping IP** - Enter an IP address in this field for pinging.<br>• **TTL** –Time To Live, the maximum allowed number of hops to the ping destination. Valid values range from 1 to 255.<br>• **Ping Interval (Sec, 10-3600)** – Enter the interval for the system to execute the PING operation.<br>• **Ping Retry** - Enter the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged. |
| **MTU** | |
| **MTU** | Maximum Transmission Unit, the size of the largest packet, in bytes, that can be transmitted to the WAN. The maximum value is 1500. For PPPoE connections, there is always an 8-byte overhead, so the maximum valid MTU value for PPPoE is 1492. |
| **WAN MAC Address** | |
| **Mode** | This feature is available only when Advanced Mode is activated.<br>**Default** – Use the default MAC address for the WAN port.<br>• **MAC -** Displays the MAC address of this device.<br>**Customized** - Select this option if your ISP authenticates by MAC addresses.<br>• **MAC** - Specify a MAC address for the WAN Ethernet port. |
| **Cancel** | Discard current settings and return to previous page. |
| **Apply** | Save the current settings and exit the page. |

## II-1-2-3 Virtual WAN

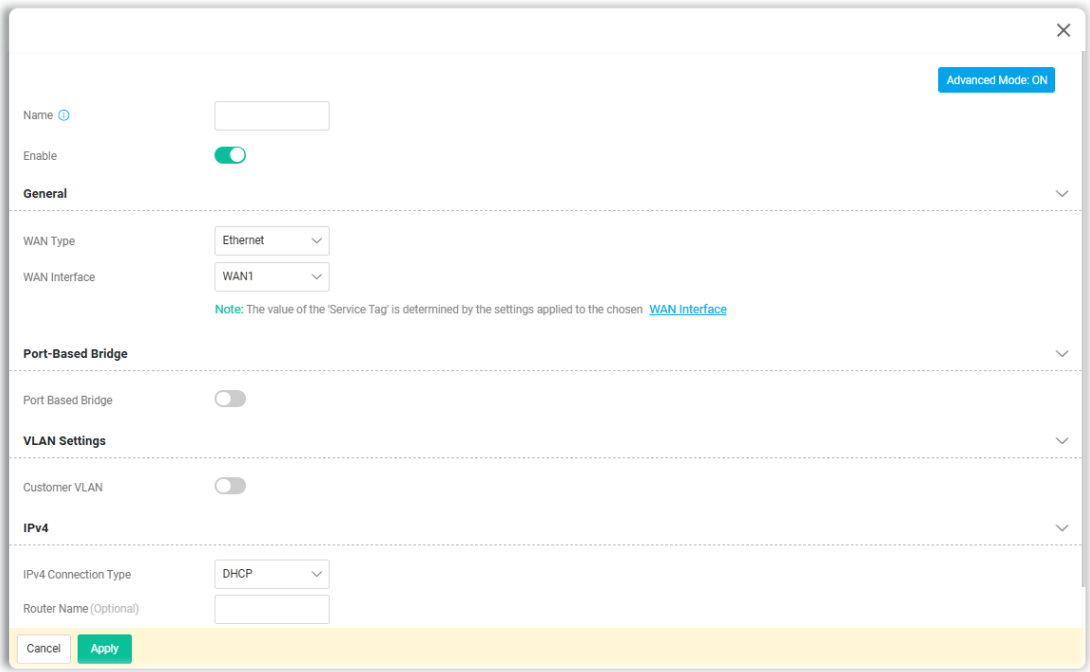
Up to five virtual WAN profiles can be set for applying to different applications.

Each profile can be specified with VLAN and binding interfaces according to the requirements of the practical network environment.




| Item | Description |
|---|---|
| **Reset** | Click to clear all profiles to factory settings. |
| **+Add** | Click to bring up the configuration page of the virtual WAN profile (max. 5). |

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




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Advanced Mode: ON/OFF** | Click to show or hide the advanced settings for virtual WAN. |

| | |
|---|---|
| Name | Enter a name as the profile name. |
| Enable | Switch the toggle to enable or disable the function. |
| General | |
| WAN Type | Displays the type (e.g., Ethernet) of the physical interface. |
| WAN Interface | Select one of the available WAN interfaces (enabled on WAN>>WAN Connections). |
| Port-Based Bridge | |
| Port Based Bridge | Switch the toggle to enable or disable the function.<br>Binding Interface - Select an interface for binding. |
| Multicast Stream VLAN Trans | Switch the toggle to enable or disable the function.<br>In some areas, the multicast VLAN tag value might be different from the IGMP VLAN tag. That might cause data transfer issues for IPTV packets flooding to other VLAN ports while watching the IPTV program.<br>Configure the IGMP VLAN tag and the multicast VLAN tag with the same value if required.<br>Downstream Multicast VLAN Tag – Enter the value for tagging the multicast packet. The range is from 0 to 4094.<br>Upstream IGMP VLAN Tag – Enter the value for tagging the IGMP packet. The range is from 0 to 4094. |
| VLAN Settings | |
| Customer VLAN | It is available when a WAN Type is selected.<br>Switch the toggle to enable or disable the function of VLAN with tag.<br>Tag - Enter the value as the VLAN ID number. The range is from 0 to 4094.<br>Priority - Enter the packet priority number for such VLAN. The range is from 0 to 7.<br>Note if Multicast Stream VLAN Trans is enabled, the VLAN Settings will be ignored and disabled. |
| Options under the Advanced Mode | |
| IPv4 | |
| IPv4 Connection Type | There are several types for network connection:<br>• PPPoE<br>• DHCP<br>• Static IP |
| Username/Password | It is available when PPPoE is selected as IPv4 Connection Type. |
| PPP Authentication | It means the protocol used for PPP authentication.<br>Both PAP and CHAP (Challenge-Handshake Authentication Protocol) can be used for PPP authentication. Router negotiates with the PPTP or L2TP server to determine which protocol to use. |
| IP Assignment | It is available when PPPoE is selected as IPv4 Connection Type.<br>DHCP - WAN IP address is dynamically allocated. |

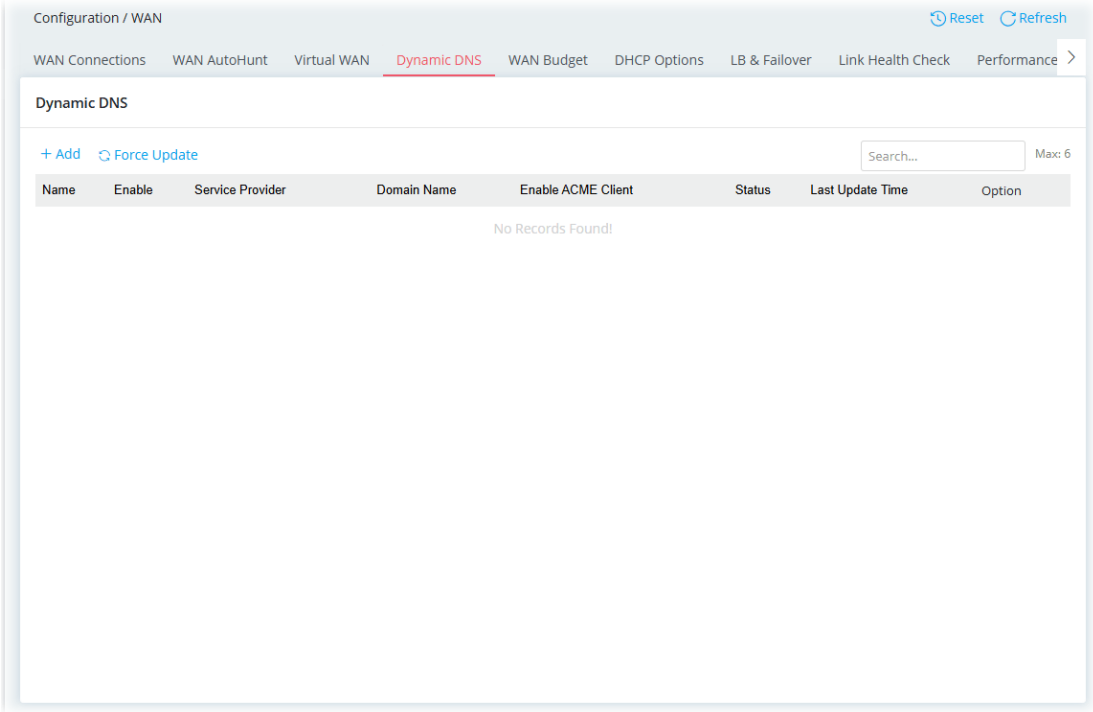
| | |
|---|---|
| | **Static IP** - ISP has assigned a fixed WAN IP address. Enter an IP address. |
| **IP Address** | It means the WAN IP address assigned by the ISP.<br>It is available when Static IP is selected as IPv4 Connection Type. |
| **Subnet Mask** | It means the WAN subnet mask.<br>It is available when Static IP is selected as IPv4 Connection Type. |
| **Gateway IP** | It means the IP address of the WAN Gateway.<br>It is available when Static IP is selected as IPv4 Connection Type. |
| **Router Name** | Set a name for the router.<br>It is available when DHCP is selected as IPv4 Connection Type. |
| **Domain Name** | Enter the domain name used for the router.<br>It is available when DHCP is selected as IPv4 Connection Type. |
| **Cancel** | Discard current settings and return to 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-1-2-4 Dynamic DNS

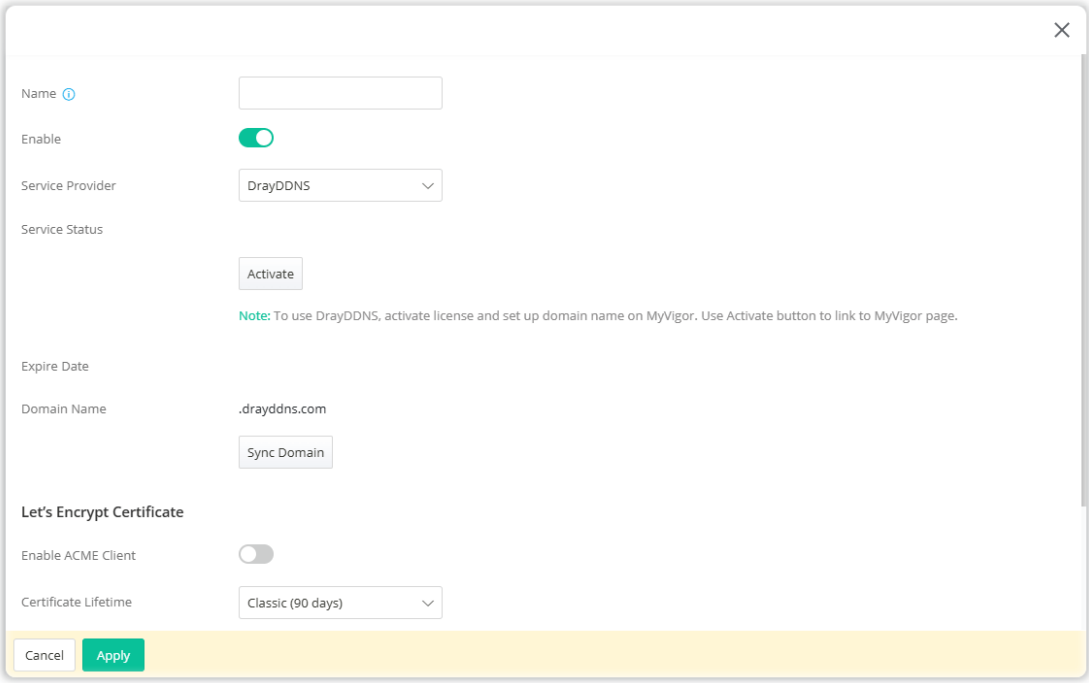
Most ISPs assigns dynamic WAN IP addresses to their customers. Dynamic IP addresses presents challenges to users who would like to accept remote connections to their LANs from the Internet, as service could be disrupted due to the IP address changing without notice. By setting up service with a Dynamic DNS (DDNS) provider, and configuring Dynamic DNS updates on the Vigor router, you can have reliable access to your network by means of an easy-to-remember domain address that resolves to the most current WAN IP address.

The Vigor router supports a wide range of DDNS providers. Please contact the DDNS provider of your choice to set up service before configuring DDNS on the router.




| Item | Description |
|---|---|
| **Reset** | Click to clear all profiles to factory settings. |
| **+Add** | Click to bring up the configuration page of the DDNS profile (max. 6). |
| **Force Update** | Click to connect immediately to DDNS servers to update IP address information. |

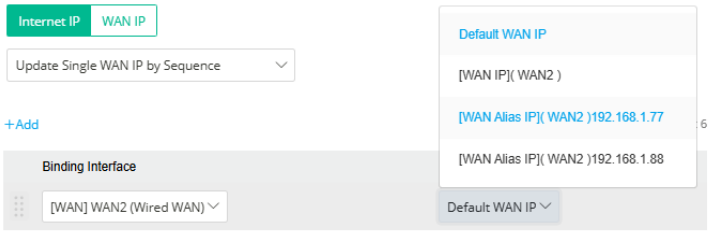
To add a new DDNS profile, click the **+Add** link to get the following page.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Name** | Enter a name as the profile name. |
| **Enable** | Switch the toggle to enable or disable the function. |
| **Service Provider** | Select the DDNS provider. If your DDNS provider is not listed, select **User-Defined** and manually configure the profile.<br>● **DrayDDNS**<br>● **NO-IP**<br>● **Dyn.com**<br>● **58DDNS**<br>● **UBDDNS**<br>● **Cloudflare**<br>● **User-Defined**<br>● **Let's Encrypt ACME**<br>● **Let's Encrypt ACME(IP)** |
| **If DrayDDNS is selected as Service Provider** | **Service Status** - Click **Activate** to activate the service.<br>**Expire Date** - Display the expired date of the service.<br>**Domain Name** - Display the domain and sub-domain to be updated.<br>**Sync Domain** – The domain name for DrayDDNS is set on the MyVigor server. Click this button to load and obtain the domain name if it is available. |
| **If NO-IP, Dyn.com, 58DDNS, UBDDNS is selected as Service Provider** | **Domain Name** - The domain and sub-domain to be updated.<br>**Account Name** - Enter the login name of the DDNS account.<br>**Password** - Enter the password of the DDNS account. |
| **If Cloudflare is selected as Service Provider** | **Domain Name** - The domain and sub-domain to be updated.<br>**API Token –** Enter the Cloudflare API authorization token. |

| | |
|---|---|
| | **Zone ID –** Enter the Cloudflare Zone ID associated with the domain. |
| **If User-Defined is selected as Service Provider** | **Provider Host URL** - Enter the IP address or the domain name of the host which provides related service.<br>**Service API** - Enter the IP address or the domain name of the host which provides related service.<br>**Server Response** - Enter any text that you want to receive from the DDNS server.<br>**Account Name** - Enter the login name of the DDNS account.<br>**Password** - Enter the password of the DDNS account.<br>**Auth Type** –Two types can be used for authentication.<br>● **Basic** – Username and password defined later can be shown from the packets captured.<br>● **URL** - Username and password defined later can be shown in URL.<br>**Enable ACME Client** – Switch the toggle to generate a certificate issued by Let's Encrypt for applying to such DDNS account. |
| **Let's Encrypt Certificate** | **Enable ACME Client** – Switch the toggle to generate a certificate issued by Let's Encrypt for applying to such DDNS account.<br>**Certificate Lifetime** – Select the validity period of the certificate.<br>**Domain Name** – Enter the domain name of the server (available if Let's Encrypt ACME / User-Defined is selected as the Service Provider).<br>**IP Address** – Enter the IP address for the certificate (available if Let's Encrypt ACME (IP) is selected as the Service Provider).<br>**Status** – Display the information related to Let's Encrypt certificate. |
| **More settings** | |
| **Update DDNS with** | If a Vigor router is installed behind any NAT router, you can enable this function to locate the real WAN IP.<br>When the WAN IP used by Vigor router is private IP, this function can detect the public IP used by the NAT router and use the detected IP address for DDNS update.<br>There are two methods offered for you to choose:<br>**Internet IP** –The real public IP address will be used. Select this option if the IP address assigned to the router's WAN interface is not the actual external IP address.<br>**WAN IP** – The IP address of the router's WAN interface will be used.<br>**+Add** – Click to create a new group of Binding Interface and Interface IP. Up to 6 sets can be created.<br>**Binding Interface** – Select the WAN interface associated with the DDNS profile.<br>**Interface IP** – Select a WAN IP. If not, the default WAN IP will be used instead. |
| **Update WAN IP Mode** | It is available when **DrayDDNS** is set as the Service Provider.<br>**Update All Selected WAN IPs** – The Vigor router system will update all selected WAN IPs.<br>**Update Single WAN IP by Sequence** – The Vigor router system will update the WAN IP in sequence.<br>**+Add** – Click to add IP address (up to six).<br>● **Binding Interface** – Select an interface (WAN1 to WAN6) for |

| | |
|---|---|
| | traffic passing through. Up to six interfaces can be defined.<br>• **Interface IP** – If there is any IP alias configured before, available item(s) will be shown in this field. The first IP listed in the Binding Interface is the default IP. Select one of the items to match the binding interface.<br> |
| **Protocol** | It is available when **DrayDDNS or 58DDNS** is set as the Service Provider.<br>Select the IP type (IPv4 or IPv6, or Any) of the IP address that would be used for answering to the DDNS service provider. |
| **Auto Update Interval** | The frequency, in minutes, at which the router connects to DDNS servers to update IP address information.<br>The default is 14400. |
| **Cancel** | Discard current settings and return to previous page. |
| **Apply** | Save the current settings and exit the page. |

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

## DrayDDNS Settings

DrayDDNS, a DDNS service developed by DrayTek, can record multiple WAN IP (IPv4/IPv6) on single domain name. It is convenient for users to use and easily to set up with MyVigor. Each Vigor Router is available to register one domain name to MyVigor for one year license.

## DDNS updates take place when:

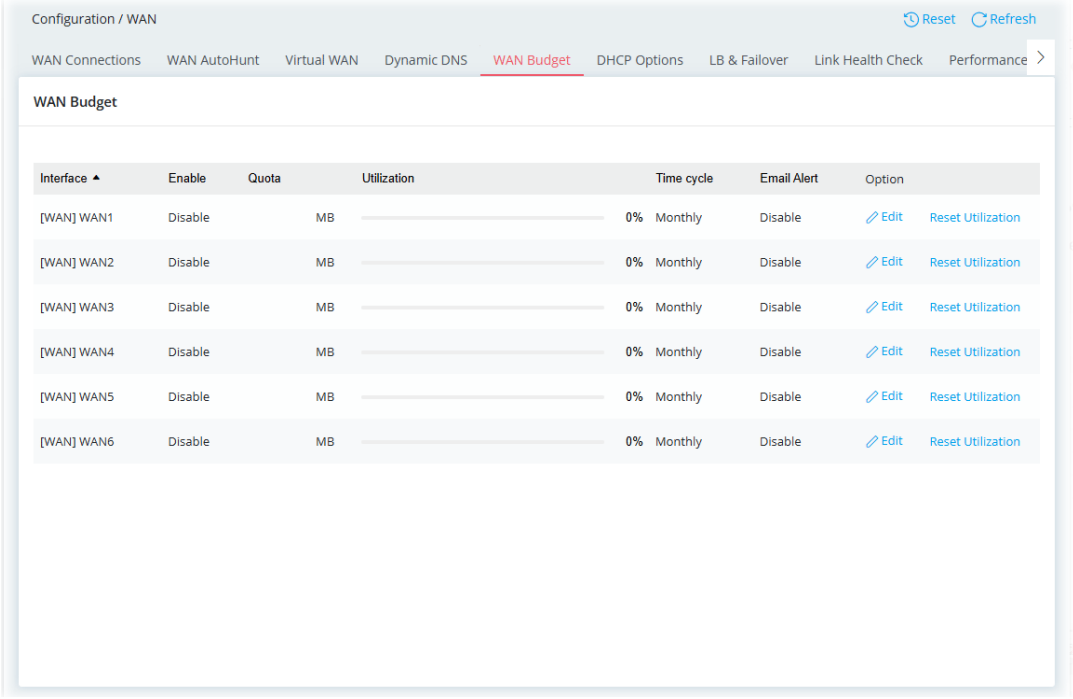
- The router is powered on or rebooted.
- The public IP address of any WAN interface changes.
- The online status of a WAN interface changes (going from online to offline or vice versa).
- The DDNS function is changed from “disabled” to “enabled”.
- A DDNS entry is modified and enabled.
- The Auto Update Interval has elapsed.
- Pressing the Force Update.

## II-1-2-5 WAN Budget

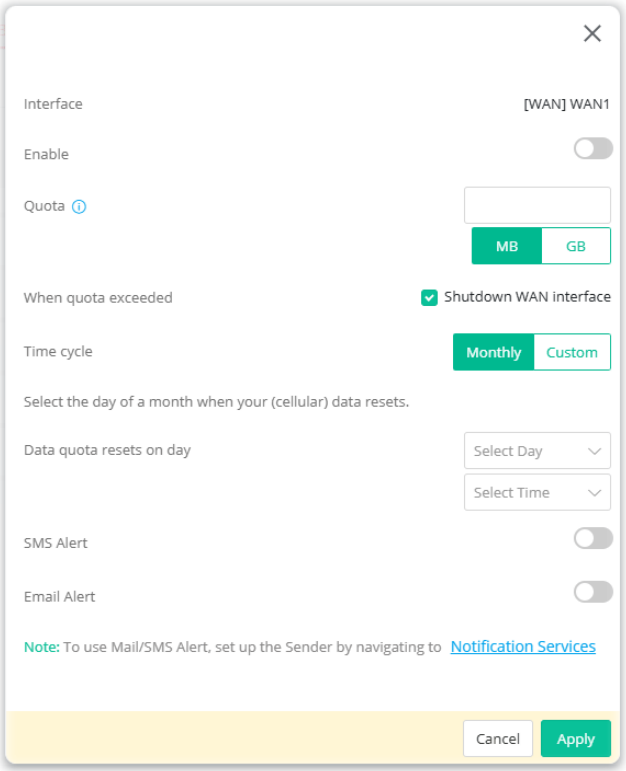
This function is used to determine the data *traffic volume* for each WAN interface respectively to prevent overcharges for data transmission by the ISP. Please note that the Quota Limit and Billing cycle day of month settings will need to be configured correctly first in order for some period calculations to be performed correctly.

The WAN Budget feature allows you to conveniently keep track of Internet traffic volume. You can:

- set up calendar cycles to monitor;
- limit your Internet usage according to your ISP's quota;
- set up action(s) to take when the quota is exceeded.




To edit a profile, click the **Edit** link to get the following page.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Switch the toggle to enable or disable the profile.<br>When enabled, the WAN Budget is enabled for this WAN. |
| **Quota** | Enter the data traffic quota allowed for such WAN interface. There are two unit (MB and GB) offered for you to specify. |
| **When quota exceed** | **Shutdown WAN interface** - All the outgoing traffic through such WAN interface will be halted when the traffic has exceeded the budget limit. |
| **Time Cycle** | **Monthly** – Some ISP might apply for the network limitation based on the traffic limit per month. This setting is to offer a mechanism of resetting the traffic record every month.<br>**Custom** - This setting allows the user to define the billing cycle according to his request. The WAN budget will be reset with an interval of billing cycle. |
| **When Monthly is selected as the Time Cycle** | **Data quota resets on day** - You can determine the starting day in one month. |
| **When Custom is selected as the Time Cycle** | Monthly is default. If long period or a short period is required, use **Custom**. The period of cycle duration is between 1 day and 30 days. You can determine the cycle duration by specifying the days and the hours. In addition, you can specify which day of today is in a cycle.<br>**Cycle duration (Days)** – Specify the days (1~31) to reset the traffic record.<br>**Cycle duration (Hours)** – Specify the hours (0~23) to reset the traffic record.<br>**Start Date** – Specify the day in the cycle as the starting point |

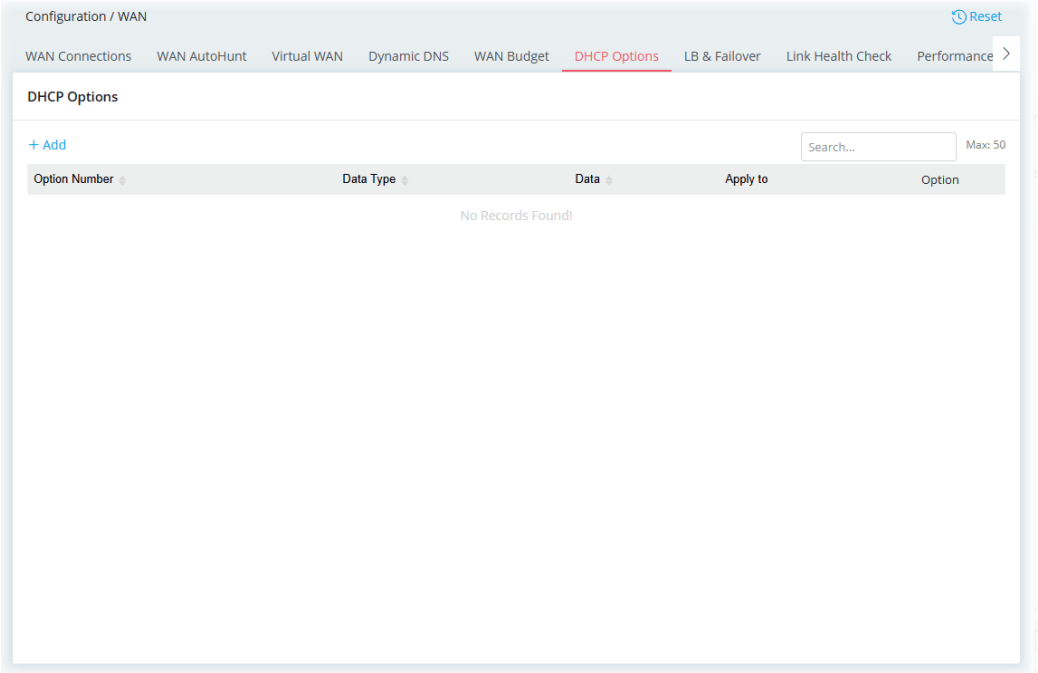
| | |
|---|---|
| | which Vigor router will reset the traffic record.<br>**Start Time (Hr:Min.)** - Specify the time for data quota rest in the cycle as the starting point which Vigor router will reset the traffic record. |
| **SMS Alert** | Switch the toggle to enable or disable the function.<br>**Send Alert SMS to** – The system will send out SMS message to the user specified here when the quota is running out (less than 10%). |
| **Email Alert** | Switch the toggle to enable or disable the function.<br>**Send Alert Email to** – The system will send out a warning message to the user specified here when the quota is running out (less than 10%). |
| **Cancel** | Discard current settings and return to previous page. |
| **Apply** | Save the current settings and exit the page. |

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

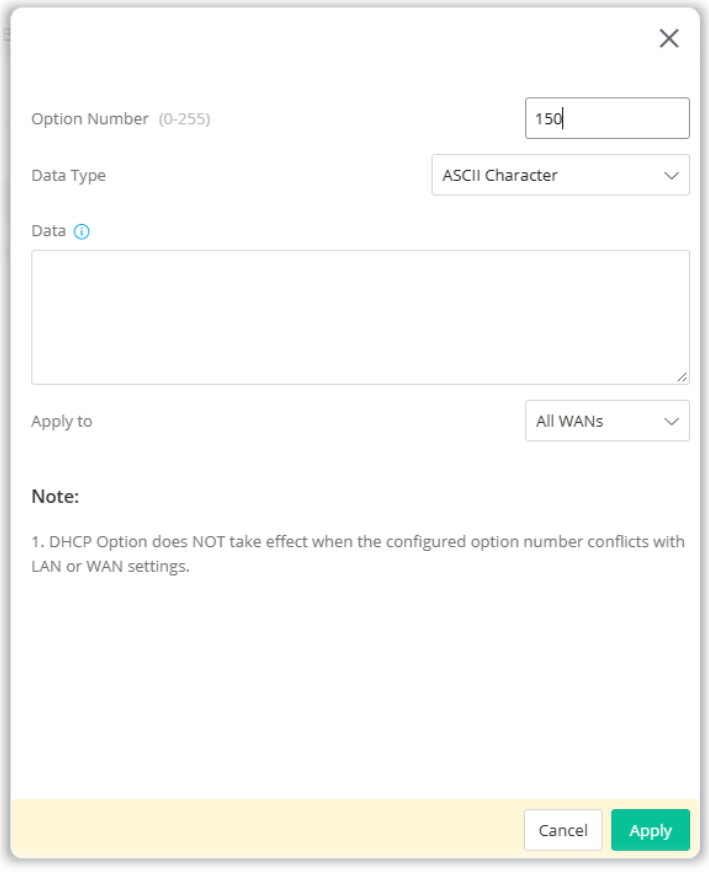
## II-1-2-6 DHCP Options

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

This page allows to configure additional DHCP client options.




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



Available settings are explained as follows:

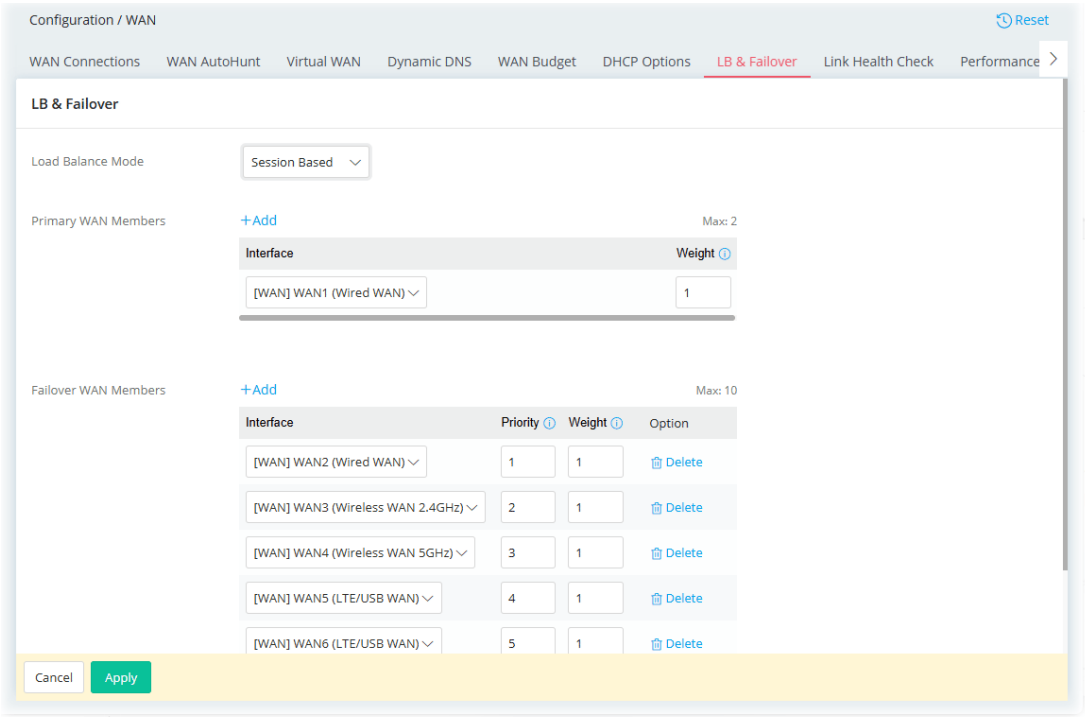
| Item | Description |
| --- | --- |
| **Option Number** | Each DHCP option is composed by an option number with data.<br>Enter a number. |
| **Data Type** | Choose the type (ASCII or Hex or Address List) for the data to be stored. Type of data in the Data field:<br>• **ASCII Character**: A text string. Example: /path.<br>• **Hexadecimal Digit**: A hexadecimal string. Valid characters are from 0 to 9 and from a to f. Example: 2f70617468.<br>• **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. |
| **Apply to** | Select WAN interface(s) to which this entry is applicable. |
| **Cancel** | Discard current settings and return to previous page. |
| **Apply** | Save the current settings and exit the page. |

## II-1-2-7 LB & Failover

This page allows to configure settings for load balance and failover WAN.

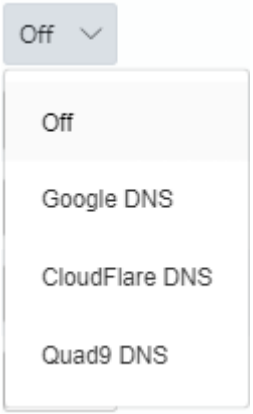
Failover allows the traffic to be forwarded to an alternate interface if the specified interface loses connection.

LB (load balance) can avoid excessive load on a single server by distributing the load, optimizing resource usage, and preventing a single server failure. The Vigor router can distribute the inbound NAT sessions among the servers with the configured load balance weight.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Load Balance Mode** | **IP Based** – For ensuring the consistency of user sessions, this function will lead the requests from a specific client (listed on Interface/Weight) to the same server. However, it may not distribute traffic evenly once many requests come from the same client.<br>**Session Based** – This option offers more evenly and effectively distributed traffic by considering IP address, full session details and current load conditions. The primary WAN interface will be used (as out-going WAN) for passing through new sessions to get better transmission speed. Though good speed test result for throughput might be reached; however, some web site may not open smoothly, especially the site need authentication, e.g., FTP. |
| **Primary WAN Members** | **+Add** – Click to create a new entry.<br>**Interface** – Select a WAN interface. This WAN will be used for network connection in default. However, if all the primary WAN interfaces lose connection, the failover WAN members will take over the network connection based on priority.<br>**Weight** - Select the weight value (1 to 255) for this entry.<br>**Option (Delete)** – Click to remove the selected entry. |

| | |
|---|---|
| **Failover WAN Members** | Display all the active WAN interfaces which will run as failover WAN. If the interface specified in this field loses connection or is detected unsuccessfully, traffic can be forwarded to an alternate interface.<br>**+Add** – Click to create a new entry.<br>**Interface** – Select a Failover WAN interface. This WAN is intended to serve as a backup when other WAN ports specified have lost connection.<br>**Priority** – Determine the priority of the failover WAN. The less the number is, the more it is used first as a backup WAN. All failover WANs can have the same priority value. When the primary WAN loses connection, all failover WAN members will activate the network connection.<br>**Weight** - Select the weight value (1 to 255) for this entry.<br>**Option (Delete)** – Click to remove the selected entry. |
| Advanced Settings | |
| **Failback** | Packets will be sent through another Interface or follow another policy when the original interface goes down (**Failover to**). Once the original interface resumes service (**Failback**), the packets will be returned to it immediately.<br>Switch the toggle to enable / disable the function. |
| **Restore Link Checks** | It is available if **Failback** is enabled.<br>Enter a value that will enable the system to determine the number of checks required for the link. Once the link is successfully checked, the connection will be restored. |
| **Link Health Check and Performance SLA** | Switch the toggle to enable the function.<br>If disabled, the active WAN interface will be determined based on WAN connection detection mode defined in the WAN Connections Profile.<br>If enabled, the WAN connection detection defined in the WAN Connections Profile will be ignored. The router will measure the performance of interface members, and active interfaces will be determined using Link Health Check and Performance SLA.<br>**Interface Link Health & Performance SLA** – List the available WAN interfaces for setting different health check methods.<br>• **Interface** – Display the WAN interfaces.<br>• **Link Health Check Profile** – Select one of the available check profiles (defined on Configuration>>WAN>>Link Health Check) for the interface.<br> |

| | |
|---|---|
| | • **Performance SLA** – Select one of the available check profiles (defined on Configuration>>WAN>>Performance SLA) for the interface.<br>• **Failure Retry Checks -** Specify how many times for the system to check the connections. If all attempts fail, the system will determine that the connection is unstable. |
| **Load Balance Exception List** | Establish an exception list that will utilize a fixed WAN instead of Multiple WAN Load Balancing.<br>**+Add** – Click to create a new entry (up to 10).<br>**Enable** – Switch the toggle to enable the entry.<br>**Comment** – Enter a brief description for identification.<br>**Service Type** –S elect the service type to which this entry applies. Service is a predefined or user-defined type of traffic that uses certain protocols or ports. To set up a custom service, select **Customized** to set the service name, the protocol, and port number.<br>**Protocol** – Select TCP, UDP or TCP/UDP for the service type.<br>**Source Port** – Enter a port number for the source IP address.<br>**Destination** – Enter the destination IP address.<br>**Destination Port** – Enter a port number for the destination IP address.<br>**Option (Delete)** – Click to remove the selected entry. |
| **Cancel** | Discard current settings and return to previous page. |
| **Apply** | Save the current settings and exit the page. |

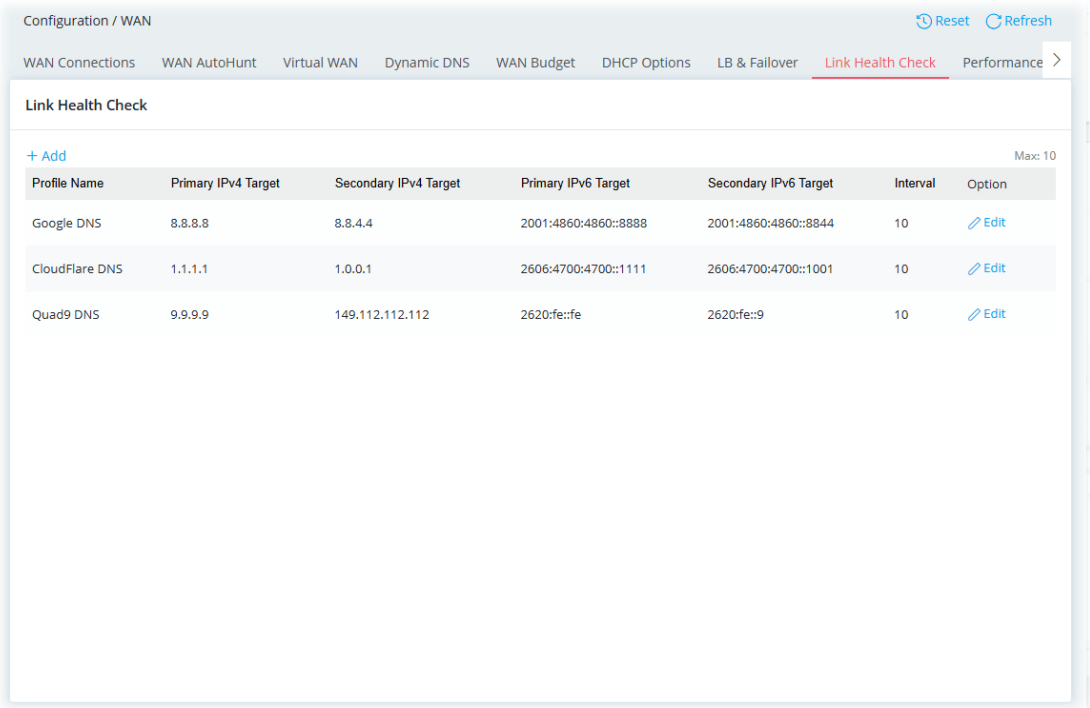
## II-1-2-8 Link Health Check

Link Health Check is used for specifying the IPs (IPv4 and IPv6) that need to be verified to ensure network connectivity via ping/httping.

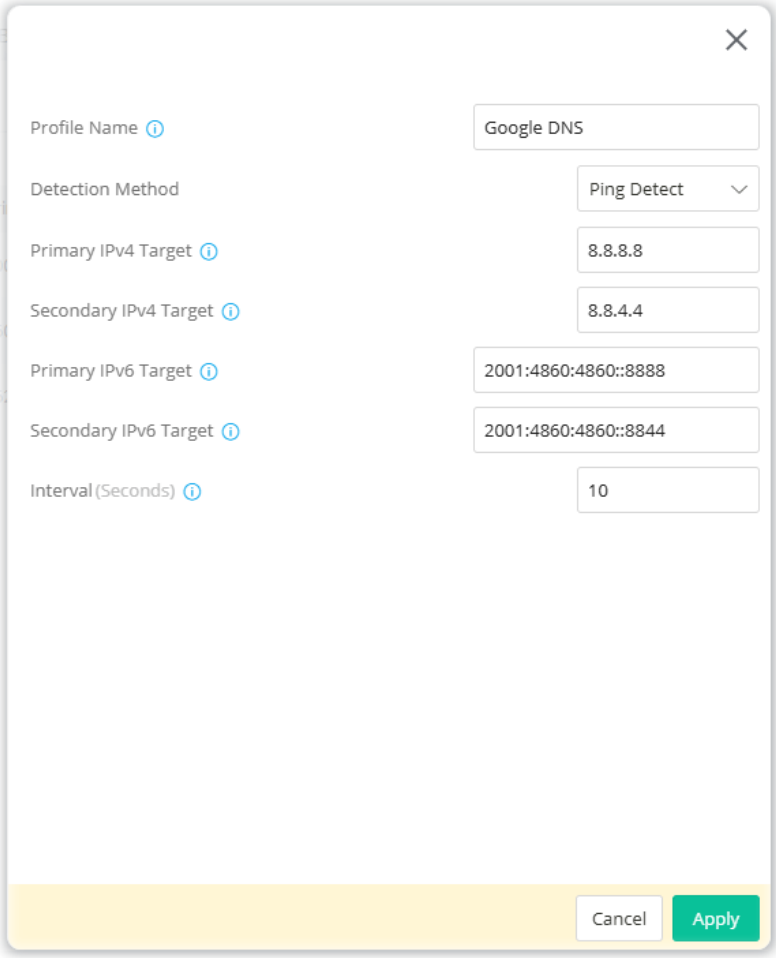
This page allows you to create profiles for executing the link health of the WAN interface.

By default, the system offers standard health check options such as Google DNS, CloudFlare DNS, and Quad9 DNS.

Take Google DNS as an example. This profile indicates that primary/secondary IPv4 target (8.8.8.8/8.8.4.4) is used for checking IPv4 network connection, while primary/secondary IPv6 target (2001:4860:4860::8888, 2001:4860:4860::8844) is used for checking IPv6 network connection. Network connection detection is performed per 10 seconds. If one of the IPv4 and IPv6 addresses is detected connection unsuccessfully, it will be judged as checking network connection failure.




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



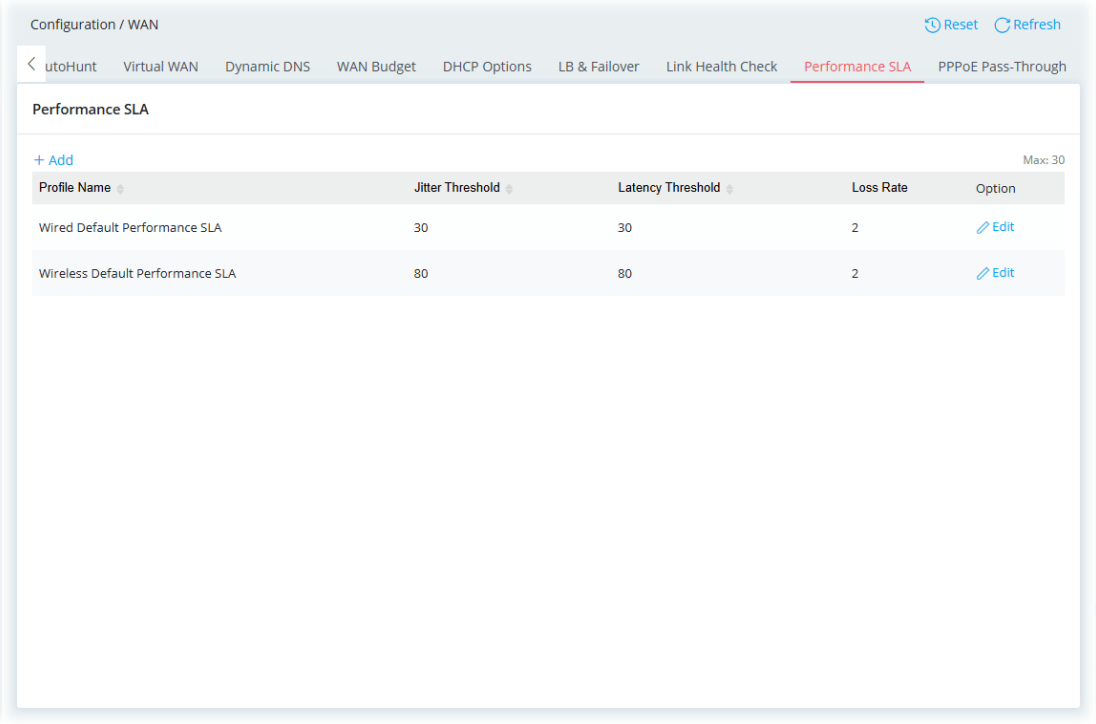

Available settings are explained as follows:

| Item | Description |
|---|---|

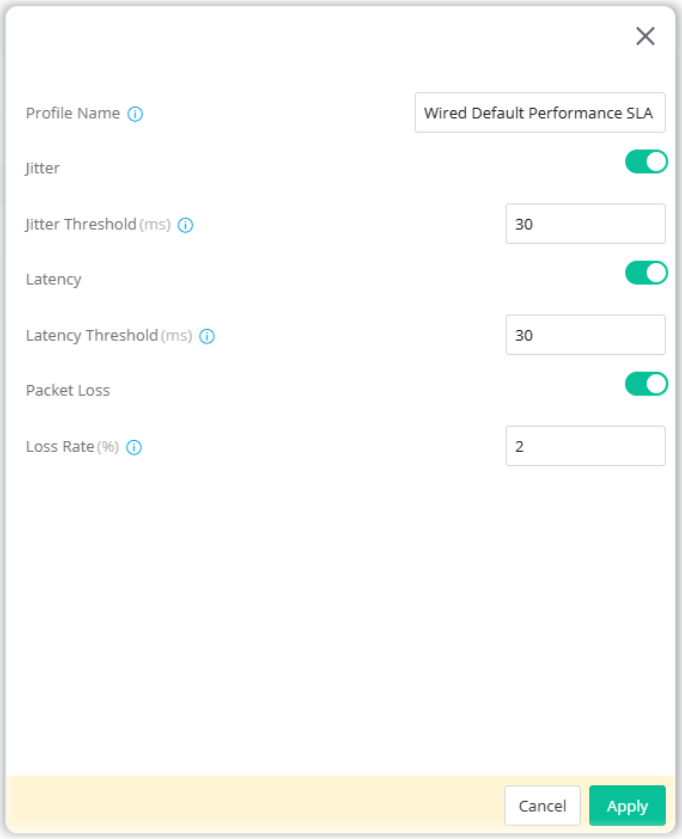
| | |
|---|---|
| **Profile Name** | Enter a name as the Link Health Check profile. |
| **Detection Method** | Select the protocol for ping detection.<br>• **HTTP Detect**<br>• **Ping Detect** |
| **Primary IPv4 Target** | Enter the first IPv4 address as the primary target for health check. |
| **Secondary IPv4 Target** | Enter the second IPv4 address as the secondary target for health check. |
| **Primary IPv6 Target** | Enter the first IPv6 address as the primary target for health check. |
| **Secondary IPv6 Target** | Enter the second IPv6 address as the secondary target for health check. |
| **Interval** | Set the time interval (unit is second) for network detection or checking. |
| **Cancel** | Discard current settings and return to previous page. |
| **Apply** | Save the current settings and exit the page. |

## II-1-2-9 Performance SLA

This page allows you to set the thresholds for jitter, latency, and loss for Performance SLA (Service Level Agreement), which will be used for detecting the health status of the WAN connection.




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



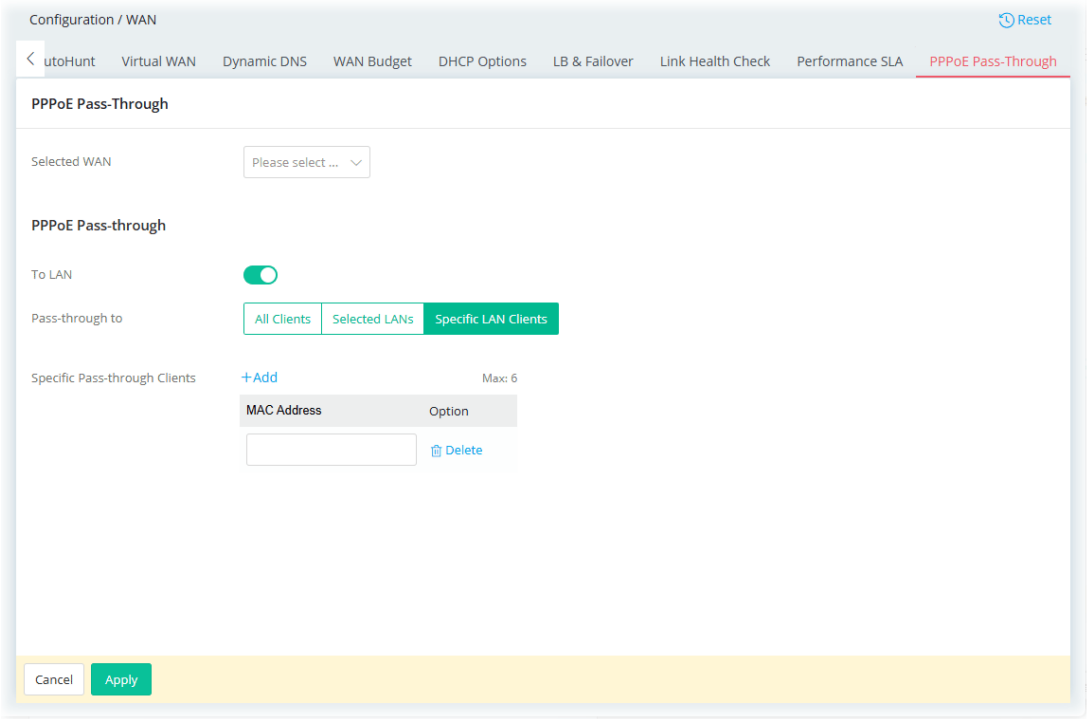

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Profile Name** | Enter a name as the Link Health Check profile. |
| **Jitter** | Switch the toggle to enable or disable the jitter function.<br>**Jitter Threshold** - It defines the change rate of latency. For stable session, small jitter value will be better.<br>When the detected value is greater than the value set here, the connection will be regarded as unstable and connection failure. |
| **Latency** | Switch the toggle to enable or disable the latency function.<br>**Latency Threshold** - It defines the time taken by Vigor router when sending the packets to the IP set in Link Condition Detection.<br>When the detected value is greater than the value set here, the connection will be regarded as unstable and connection failure. |
| **Packet Loss** | Switch the toggle to enable or disable the packet loss function.<br>**Loss Rate** - It defines the proportion that packets will be discarded before arriving at the IP set in Link Condition Detection.<br>When the detected value is greater than the value set here, the connection will be regarded as unstable and connection failure. |
| **Cancel** | Discard current settings and return to previous page. |
| **Apply** | Save the current settings and exit the page. |

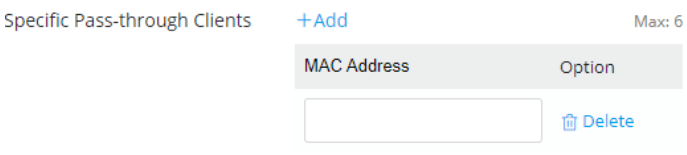
## II-1-2-10 PPPoE Pass Through

The router offers PPPoE dial-up connection. Besides, you also can establish the PPPoE connection directly from local clients to your ISP via the Vigor router. According to the WAN Connection Type, this feature will encapsulate the PPPoE package of local clients and send it to the WAN Server.

Thus, the PC can access Internet through such direction.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Selected WAN** | Select a WAN interface for applying the PPPoE pass-through. |
| **To LAN** | Switch the toggle to enable or disable the function. If enabled, wired LAN clients can initiate PPPoE dial-up connections to the selected WAN. |
| **Pass-through to** | **All Clients** – All the wired LAN clients can initiate PPPoE dial-up connections to the selected WAN.<br>**Selected LANs** – One or more LAN clients can initiate PPPoE dial-up connections to the selected WAN.<br>**Specific LAN Clients** – Up to six specific LAN clients can initiate PPPoE dial-up connections to the selected WAN.<br>• **+Add** –Click to add a new client.<br> |
| **Cancel** | Discard current settings. |
| **Apply** | Save the current settings. |

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

## II-1-3 LAN

A LAN(Local Area Network) comprises a collection of LAN clients, which are networked devices on your premises. A LAN client can be a computer, a printer, a Voice-over-IP (VoIP) phone, a mobile phone, a gaming console, an Internet Protocol Television (IPTV), etc, and can have either a wired (using Ethernet cabling) or wireless (using WiFi) network connection.

LAN clients within the same LAN are normally able to communicate with one another directly, as they are peers to one another, unless measures, such as firewalls or VLANs, have been put in place to restrict such access. Nowadays the most common LAN firewalls are implemented on the LAN client itself. For example, Microsoft Windows since Windows XP and Apple OS X have built-in firewalls that can be configured to restrict traffic coming in and going out of the computer. VLANs, on the other hand, are usually set up using network switches or routers.

To communicate with the hosts outside of the LAN, LAN clients have to go through a network gateway, which in most cases is a router that sits between the LAN and the ISP network, which is the WAN. The router acts as a director to ensure traffic between the LAN and the WAN reach their intended destinations.

### IP Address

On most broadband networks, the ISP assigns a single WAN IP address to the subscriber. All LAN clients have to share this WAN IP address when accessing the Internet. To achieve this, a technique called Network Address Translation (NAT) is used. Under NAT, a private block of IP addresses is assigned to the LAN clients, which communicate with WAN hosts through the router, also known as the gateway.

On outgoing traffic to the WAN, the router makes note that a LAN client has attempted to reach a WAN host, and forwards the request to the intended WAN recipient.

On traffic incoming to the LAN from a WAN host, the router checks its records to see if a matching outstanding request from a LAN client to this WAN host exists, and if so, forwards it to the LAN client. Otherwise, the traffic is dropped.

There are 3 distinct blocks of IPv4 address that are reserved for use as private IP addresses on a LAN.

| Name | IP Address Range | Number of Available Addresses | Largest Subnet Mask |
|---|---|---|---|
| 24-bit Block | 10.0.0.0 to 10.255.255.255 | 16,777,216 | 255.0.0.0 |
| 20-bit Block | 172.16.0.0 to 172.31.255.255 | 1,048,576 | 255.240.0.0 |
| 16-bit Block | 192.168.0.0 to 192.168.255.255 | 65,536 | 255.255.0.0 |

The default beginning IP Address of LAN 1 is 192.168.1.1, and the Subnet Mask is 255.255.255.0, for a total of 254 assignable IP addresses, from 192.168.1.1 to 192.168.1.254. The final IP address of the selected range is reserved for routing and cannot be assigned to a LAN client.

In most cases, the default IP address block should work satisfactorily. However, there are situations where you need to select a different address block, such as when you need to communicate with other LANs that already use the same address block.

Private IP addresses can be assigned automatically to LAN clients using Dynamic Host Configuration Protocol (DHCP), or manually assigned. The DHCP server can either be the router (the most common case), or a separate server, that hands out IP addresses to DHCP clients.

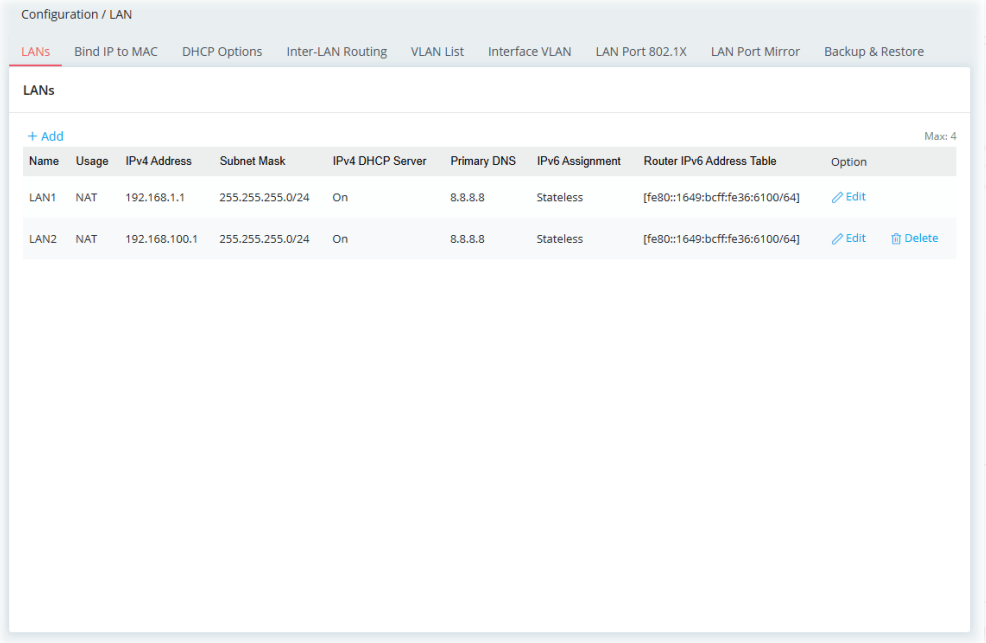
Alternatively, static IP addresses can be manually configured on LAN clients as part of their network settings. No matter how IP addresses are configured, it is important that no two devices get the same IP address. If both DHCP and static assignment are used on a network, it is important to exclude the static IP addresses from the DHCP IP pool. For example, if your LAN uses the 192.168.1.x subnet and you have 20 DHCP clients and 20 static IP clients, you could

configure 192.168.1.10 as the Start IP Address, 50 as the IP Pool Counts (enough for the current number of DHCP clients, plus room for future expansion), and use addresses greater than 192.168.1.100 for static assignment.

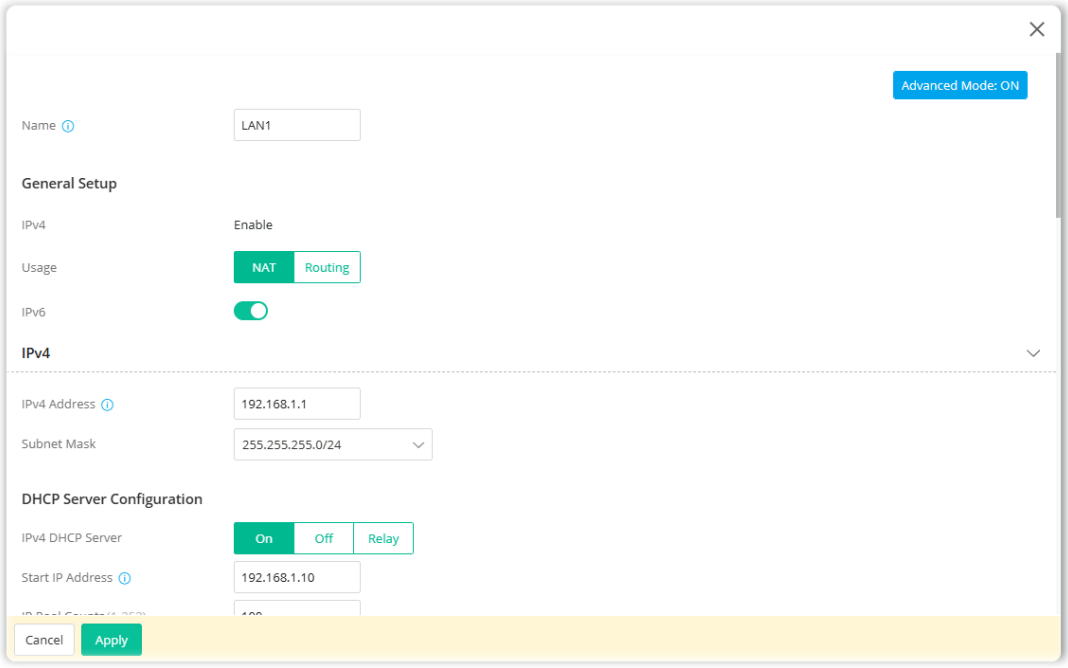
## II-1-3-1 LANs

This page provides you the general settings for LAN.

Open **Configuration>>LAN** and click the **LANs** tab to open the following page.




To add/edit a profile, click the **+Add/Edit** link to get the following page. Here, we take LAN1 as an example.




Available settings are explained as follows:

| Item | Description |
|---|---|

| | |
|---|---|
| **Advanced Mode: ON/OFF** | Click to show or hide the advanced settings for LAN. |
| **Name** | Display the name for identification. Change the name if required. |
| | **General Setup** |
| **IPv4** | Display the status (enable/disable) of the profile. |
| **Usage** | Specify the IP forwarding method.<br>• **NAT**<br>• **Routing** |
| **IPv6** | Switch the toggle to configure / ignore the IPv6 settings. |
| | **IPv4** |
| **IPv4 Address** | This is the IP address of the LAN interface (default: 192.168.1.1). |
| **Subnet Mask** | Select a subnet mask of the LAN interface. |
| | **DHCP Server Configuration** |
| **IPv4 DHCP Server** | LAN1 is configured with DHCP in default.<br>DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatches related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network.<br>If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.<br>**On** - Enables the built-in DHCP server on the router.<br>**Off** - Disables the built-in DHCP server on the router.<br>**Relay** - When selected, all DHCP requests are forwarded to a DHCP server outside of the LAN subnet, and whose address is specified in the DHCP Server IP Address field. |
| **If On is selected as DHCP Server** | **Start IP Address** - The beginning LAN IP address that is given out to LAN DHCP clients.<br>**IP Pool Counts** - The maximum number of IP addresses to be handed out by DHCP. The default value is 100. Valid range is between 1 and 253.<br>**Gateway IP Address** - The IP address of the gateway, which is the host on the LAN that relays all traffic coming into and going out of the LAN. The gateway is normally the router.<br>**Lease Time** - The maximum duration DHCP-issued IP addresses can be used before they have to be renewed.<br>**Primary DNS** - DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address.<br>**Secondary DNS** - You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. |
| **If Relay is selected as** | When selected, all DHCP requests are forwarded to a DHCP server |

| | |
|---|---|
| DHCP Server | outside of the LAN subnet, and whose address is specified in the DHCP Server IP Address field.<br>**Primary DNS** - DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address.<br>You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server.<br>**Secondary DNS** - You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server.<br>**DHCP Relay over WAN (Primary)** – Switch the toggle to enable this function. Then, specify a WAN interface for the first DHCP Server.<br>• **Primary DHCP Server Interface** – Use the drop-down list to choose a WAN interface for the first DHCP Server.<br>**Primary DHCP Server IP Address** - Enter the IP Address of the DHCP server to which DHCP requests from LAN clients are forwarded.<br>**DHCP Relay over WAN (Secondary)** - The secondary DHCP server is an optional setting. If required, specify a WAN interface for the second DHCP Server as a backup server.<br>• **Secondary DHCP Server Interface** – Use the drop-down list to choose a WAN interface for the second DHCP Server.<br>**Secondary DHCP Server IP Address** - Enter the IP Address of the DHCP server to which DHCP requests from LAN clients are forwarded. |
| IP Assignment for Teleworkers | The VPN client will receive an IP address from the DHCP pool or IP address range (defined below) for Teleworkers.<br>**Assignment Start IP** – Enter an IP address that serves as the starting point of a range of IP addresses.<br>**Assignment End IP** – Enter an IP address that serves as the end point of a range of IP addresses. |
| IPv6 | |
| IPv6 Assignment | Configures the Managed Address Configuration flag (M-bit) in Route Advertisements.<br>**Stateless** – M-bit is unset.<br>**DHCPv6(Stateful)** – M-bit is set, which indicates to LAN clients that they should acquire all IPv6 configuration information from a DHCPv6 server. The DHCPv6 server can either be the one built into the Vigor router, or a separate DHCPv6 server.<br>**Manual** – No configuration information is sent. |
| Router Advertisement Configuration | It is available when Stateless is selected as the IPv6 Assignment.<br>The router advertisement daemon sends Router Advertisement messages, specified by RFC 2461, to a local Ethernet LAN periodically and when requested by a node sending a Router Solicitation message. These messages are required for IPv6 stateless auto-configuration.<br>**Generate Prefix From** – Select the primary WAN interface which is capable to generate the prefix for IPv6 address. Use the drop down list to specify a WAN interface for IPv6. |

| | |
|---|---|
| |  |
| DNS Configuration | It is available when Stateless is selected as the IPv6 Assignment.<br>**DNS Assign Methods**<br>• **RA(RDNSS)** – The DNS server used for hosts (e.g., PC) will be configured via the Router Advertisement Configuration.<br>• **Bit(DHCPv6)** – The DNS server used for hosts will be configured via DHCPv6 server.<br>• **Manual** – Vigor router system will not send DNS sever configuration to the hosts.<br>**Primary DNS Address** - Enter the IPv6 address for Primary DNS server.<br>**Secondary DNS Address** - Enter another IPv6 address for DNS server if required. |
| DHCPv6 Server Configuration | It is available when DHCPv6 (Stateful) is selected as the IPv6 Assignment.<br>**On** - Enables the built-in DHCPv6 server on the router.<br>• **Generate Prefix From** – Select the primary WAN interface which is capable to generate the prefix for IPv6 address. Use the drop down list to specify a WAN interface for IPv6.<br>• **Auto IPv6 Address Range**<br>• **Random IPv6 Address Allocation**<br>**Off** - Disables the built-in DHCPv6 server on the router.<br>**Relay** - When selected, all DHCP requests are forwarded to a DHCP server outside of the LAN subnet, and whose address is specified in the DHCP Server IP Address field.<br>• **DHCPv6 Server Interface** – Use the drop down list to specify a WAN interface for IPv6.<br>• **DHCPv6 Server Address** - Enter the IPv6 address of the DHCPv6 server. |
| DNS Configuration | It is available when DHCPv6 (Stateful) is selected as the IPv6 Assignment.<br>**Primary DNS Address** - Enter the IPv6 address for Primary DNS server.<br>**Secondary DNS Address** - Enter another IPv6 address for DNS server if required. |
| More Settings - Force DNS Redirection | **Enable** – Switch the toggle to enable or disable the function. This function allows all outgoing DNS queries to be intercepted and redirected to the router built-in DNS server, improving the domain lookup performance by caching DNS queries and results. |
| Options under the Advanced Mode | |

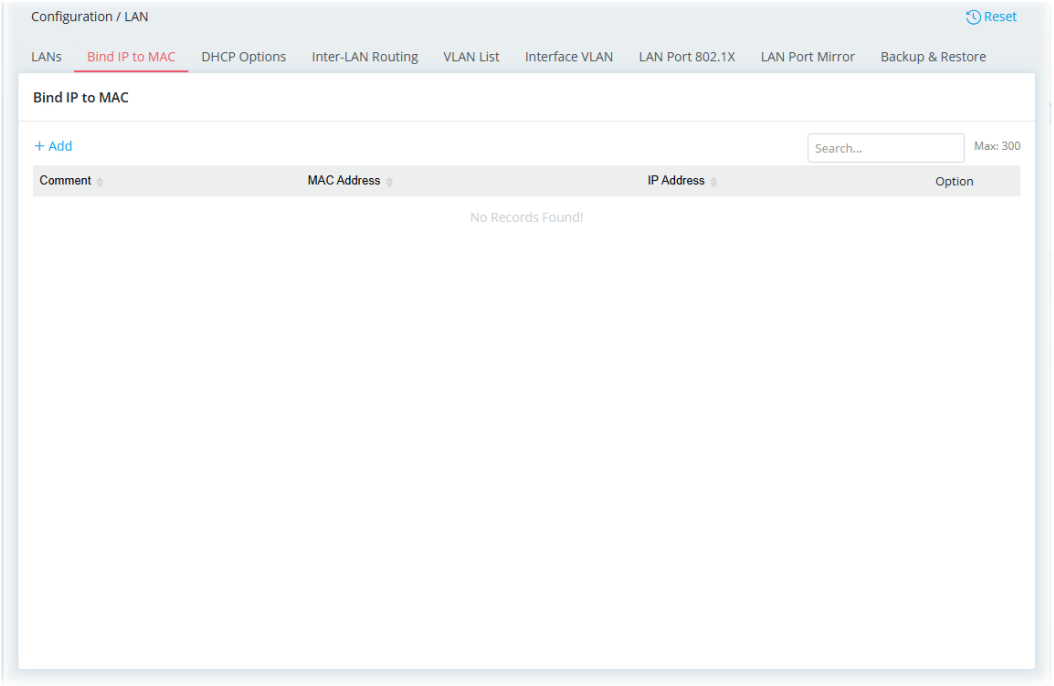
| | |
|---|---|
| Router IPv6 Address Table | Enter IPv6 Address and Prefix length to be added, or click an existing IPv6 address to be deleted in the Current IPv6 Address Table below and the values will be automatically copied over.<br>**+Add** – Click it to add a new entry. Max is 5.<br>**Static IP Address** – Enter the static IPv6 address for LAN.<br>**Prefix Length** - Enter the IPv6 prefix length for the IPv6 address. |
| Unique Local Address Configuration | Unique Local Addresses (ULAs) are private IPv6 addresses assigned to LAN clients.<br>**ULA Prefix** – LAN clients will be assigned ULAs generated based on the prefix manually entered.<br>• **Off** – ULA is disabled.<br>• **Auto** – LAN clients will be assigned ULAs using an automatically-determined prefix.<br>• **Manual** – Enter an IPv6 address. |
| Router Advertisement Configuration | The Advanced Settings page has additional settings for Router Advertisement and enabling multiple WANs for IPv6 traffic.<br>The following options are available when Stateless is selected as the IPv6 Assignment.<br>**RA Priority** – Select the default preference value (Low, Medium, High) of the router sent in route advertisement messages.<br>**Min / Max Interval Time** – Minimum/ Maximum time, in seconds, between unsolicited multicast route advertisement messages sent by the RA server.<br>**Valid Lifetime** – Enter one number (unit is second) to specify the valid lifetime for the DHCPv6 server. The device (connected via the LAN interface) is to be used as the default router.<br>This device (connected via the LAN interface) will be treated as the default router within the valid lifetime.<br>**Preferred Lifetime** – Enter one number (unit is second) to specify the preferred lifetime for the DHCPv6 server. It must be lower or equal to the valid lifetime. This device (Vigor router) will be treated as the default router within the preferred lifetime. When there are multiple routers, priority is necessary. In general, the router within the preferred lifetime has higher priority than the router within the valid lifetime.<br>**Hop Limit** - The value is required for the device behind the router when IPv6 is in use. Default value of hop limit field in Route Advertisement messages. |
| DHCPv6 Server Configuration | It is available when **DHCPv6 (Stateful)** is selected as the IPv6 Assignment.<br>**Authentication Protocol - Authentication Protocol** - This protocol will be used for the client to be authenticated by DHCPv6 server before accessing into Internet. There are three types can be specified, **Reconfigure Key**, **Delayed** and **None**. In general, the default setting is None.<br>• **Reconfigure Key** – During the connection process, DHCPv6 server will authenticate the client automatically.<br>• **Delayed** - During the connection process, DHCPv6 server will authenticate and identify the client based on the key ID, realm and secret information specified in these fields.<br>**Key ID** – Type a value (range from 1 to 65535) which will be used to generate HMAC-MD5 value.<br>**Realm** – The name (1 to 31 characters) typed here will identify |

| | |
|---|---|
| | the key which generates HMAC-MD5 value.<br>**Secret** – Type a text (1 to 31 characters) as s a unique identifier for each client on each DHCP server.<br>**Valid Lifetime** – Enter one number (unit is second) to specify the valid lifetime for the DHCPv6 server. The device (connected via the LAN interface) is to be used as the default router.<br>This device (connected via the LAN interface) will be treated as the default router within the valid lifetime.<br>**Preferred Lifetime** – Enter one number (unit is second) to specify the preferred lifetime for the DHCPv6 server. It must be lower or equal to the valid lifetime. This device (Vigor router) will be treated as the default router within the preferred lifetime. When there are multiple routers, priority is necessary. In general, the router within the preferred lifetime has higher priority than the router within the valid lifetime.<br>**Prefix Delegation** – Switch the toggle to enable/disable this function. If enabled, the router can dispatch the sub-prefix from the WAN side to the LAN client. |
| **Prefix Delegation Table** | It is available when **Prefix Delegation** is enabled. Up to 5 prefix delegation profiles can be configured.<br>**+Add** – Click to have a new entry.<br>**Prefix** – Enter an IPv6 address offered by the ISP.<br>**Prefix Length** – Enter the IPv6 prefix length for the IPv6 address.<br>**Client Link Local Address** – Enter an IPv6 address of the remote client.<br>**Client DUID** – Enter the DHCP Unique Identifier (DUID) of the remote client.<br>**Option** – Click Delete to remove the selected entry. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings and exit the page. |

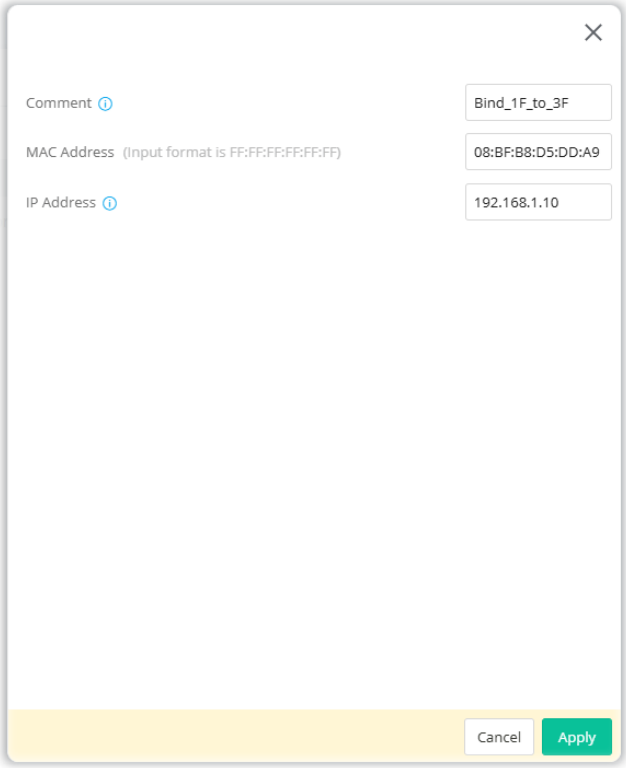
After finishing this web page configuration, please click **Apply** to save the settings.

## II-1-3-2 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.




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



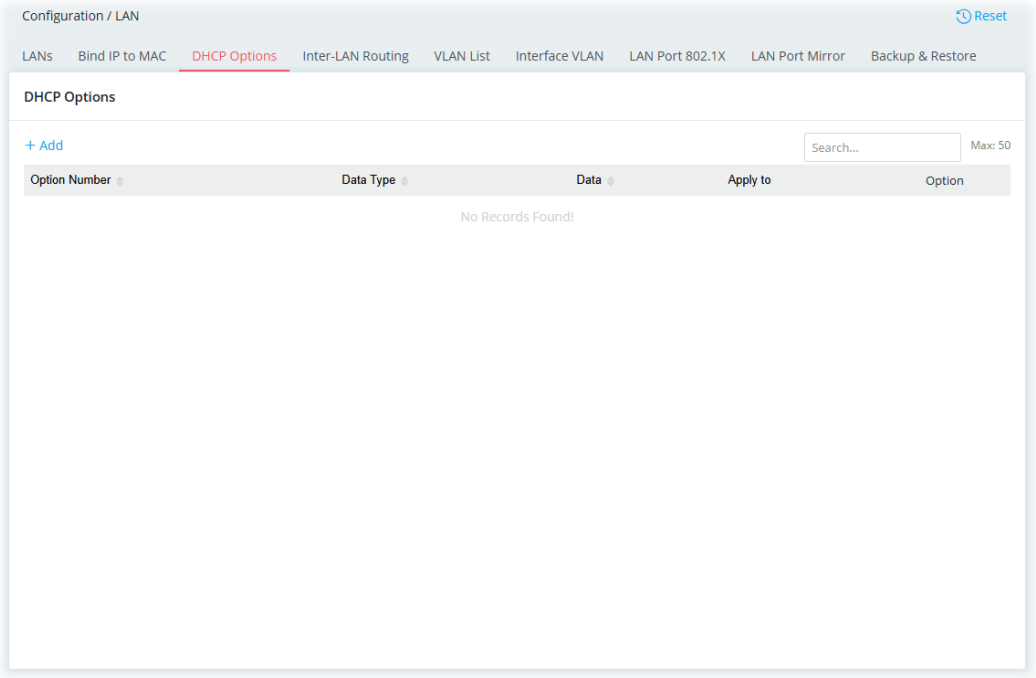

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Comments** | Enter a brief comment to identify this IP Address - MAC Address pair. |
| **MAC Address** | Enter the MAC address of the LAN client's network interface. |
| **IP Address** | Enter the IP address to be associated with a MAC address. |

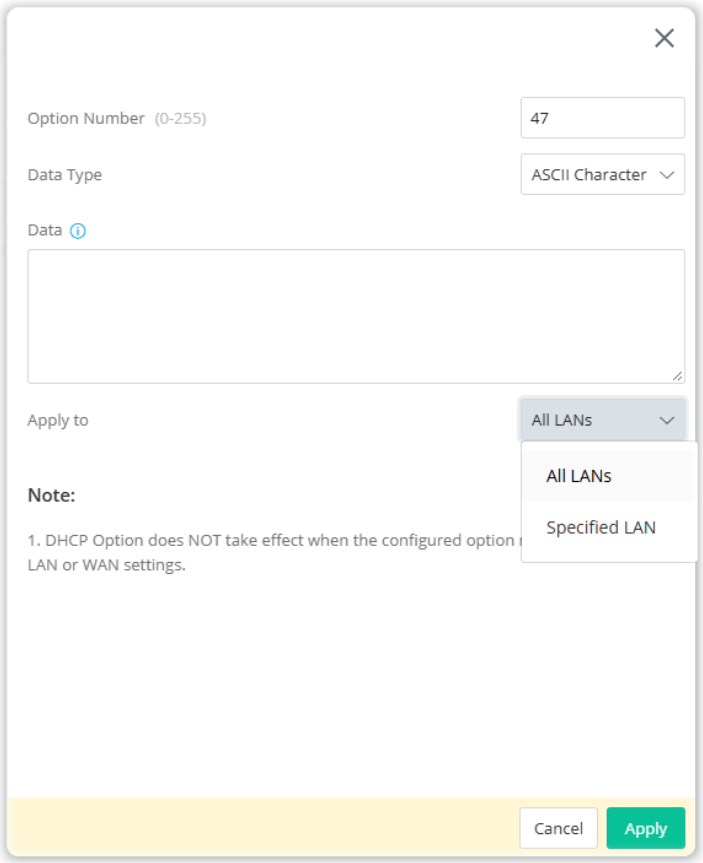
| | |
|---|---|
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings and exit the page. |

## II-1-3-3 DHCP Options

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




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

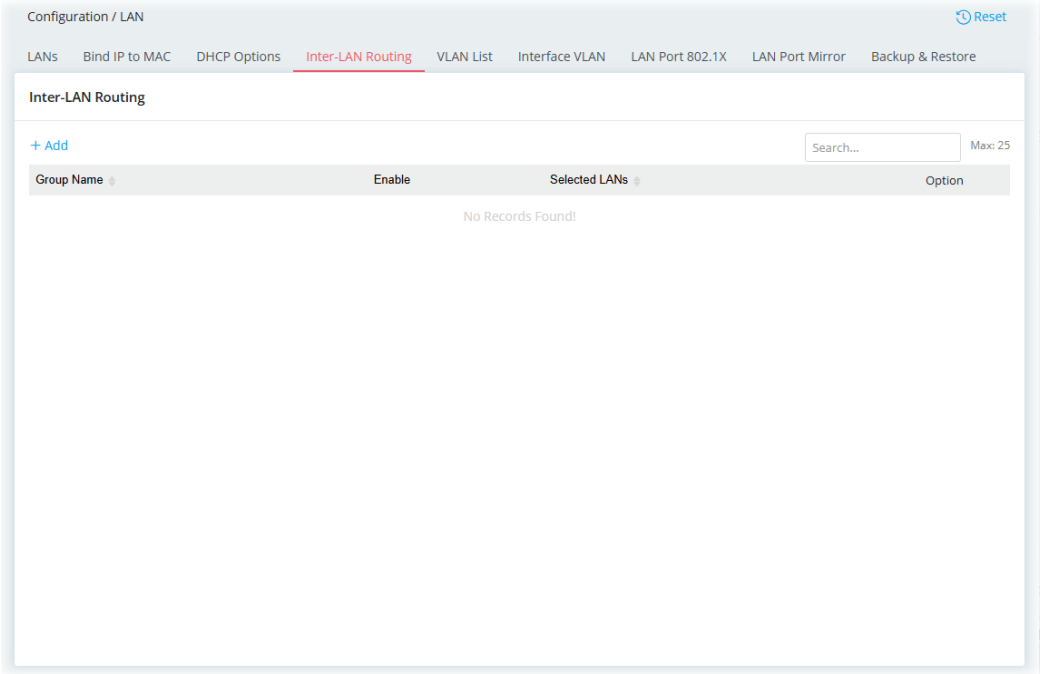



Available settings are explained as follows:

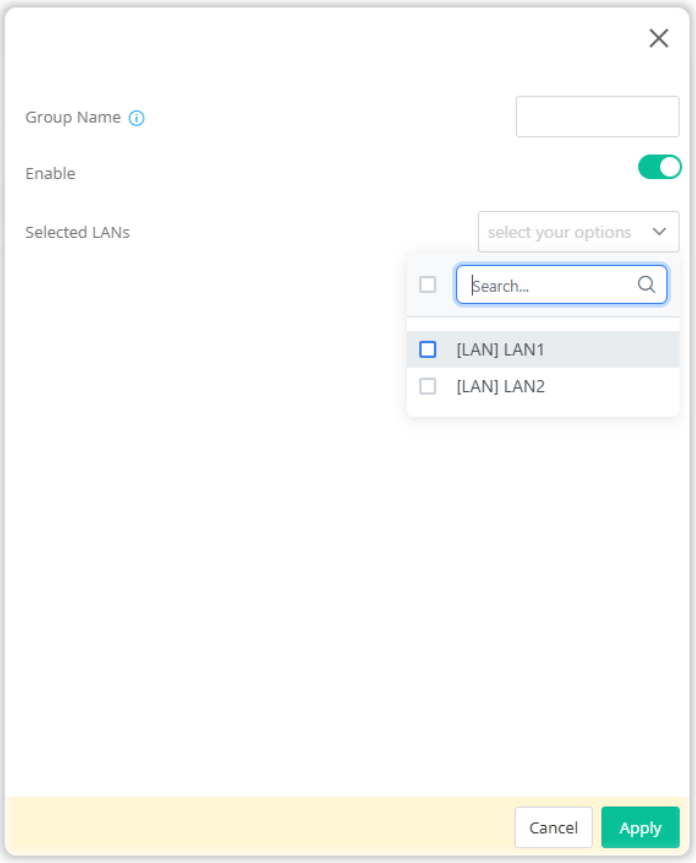
| Item | Description |
|---|---|
| **Option Number** | Enter a DHCP option number for this function. |
| **Data Type** | Choose the type (ASCII or Hex or Address List) for the data to be stored. |
| **Data** | Enter the data in the Data field based on the data type selected.<br>**ASCII Character** - A text string. Example: /path.<br>**Hexadecimal Digital** - A hexadecimal string. Valid characters are from 0 to 9 and from a to f. Example: 2f70617468.<br>**Address List** - One or more IPv4 addresses, delimited by commas. |
| **Apply to** | Select LAN interface(s) to which this entry is applicable. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings and exit the page. |

## II-1-3-4 Inter-LAN Routing

Up to 25 routing profiles provided by the router allow the users to divide groups into different subnets. In addition, different subnets can link for each other by configuring **Inter-LAN Routing**.




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



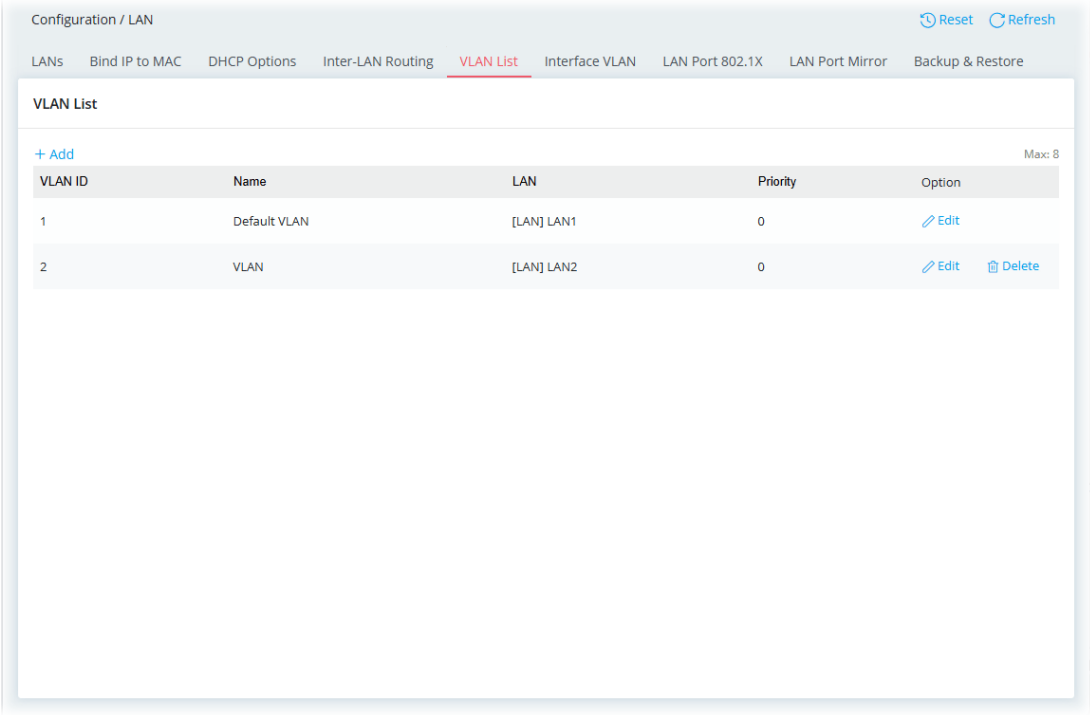

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Group Name** | Display the name for identification. Change the name if required. |
| **Enable** | Switch the toggle to enable the settings. |
| **Selected LANs** | Select the box to link two or more different subnets (LAN and LAN). |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings and exit the page. |

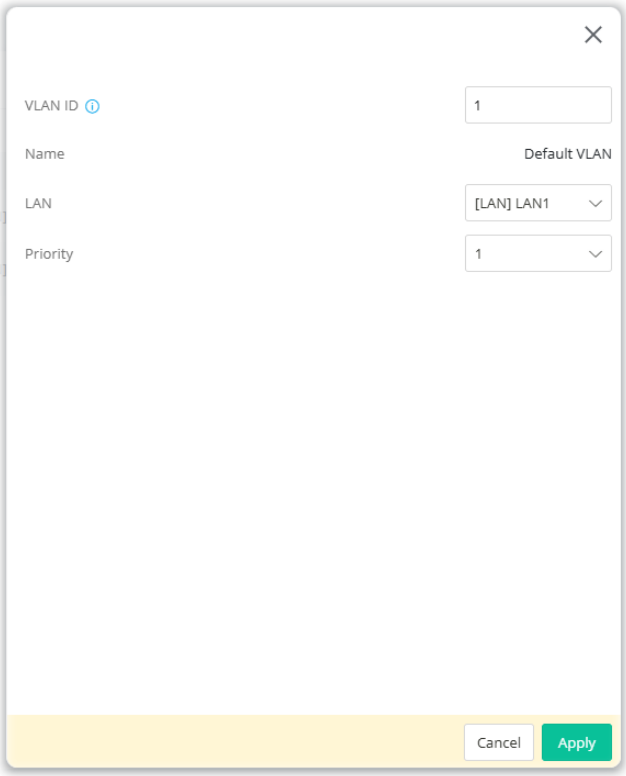
## II-1-3-5 VLAN List

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

This page allows you to create up to 8 VLAN profiles.




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



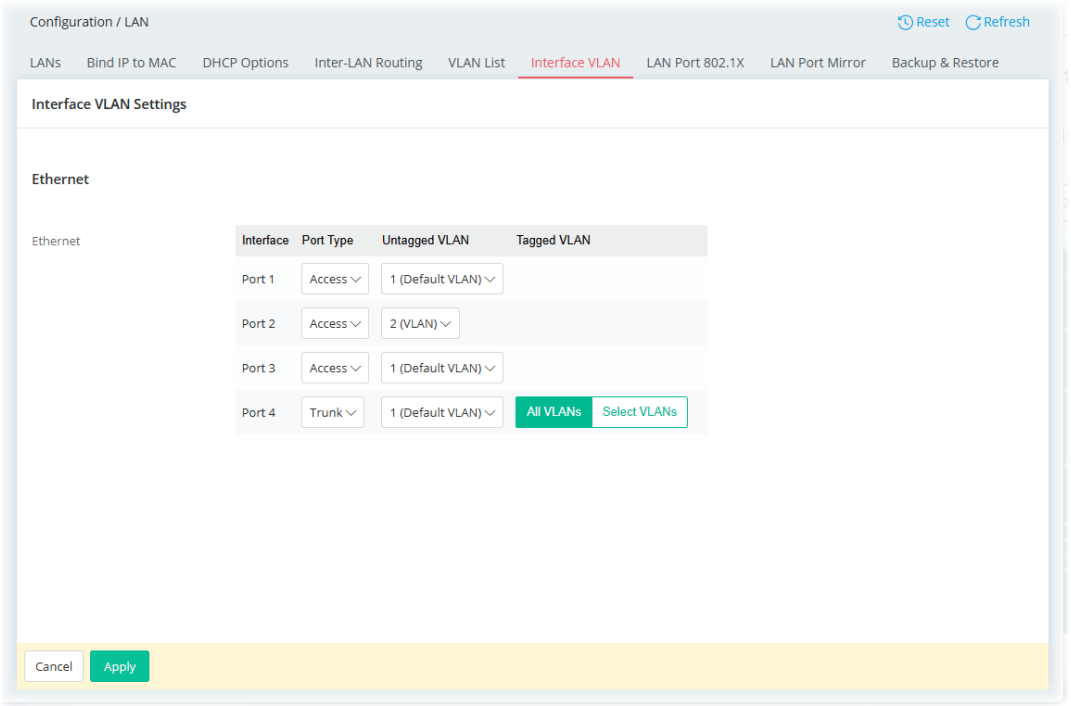

Available settings are explained as follows:

| Item | Description |
|---|---|
| VLAN ID | Enter a number as the VLAN Identifier. Valid values are form 1 to 4094. VIDs must be unique. |
| Name | Enter a name of the VLAN profile. |
| LAN | Display the physical LAN subnet on the router. Select the LAN subnet(s) to bind them under the selected VLAN. |
| Priority | Select the priority of this LAN profile. |
| Cancel | Discard current settings and return to the previous page. |
| Apply | Save the current settings and exit the page. |

## II-1-3-6 Interface VLAN

Port-based VLAN uses physical ports (P1 ~ P4) to separate the clients into different VLAN group.

Virtual LAN function provides you a very convenient way to manage hosts by grouping them based on the physical port. The multi-subnet can let a small businesses have much better isolation for multi-occupancy applications.

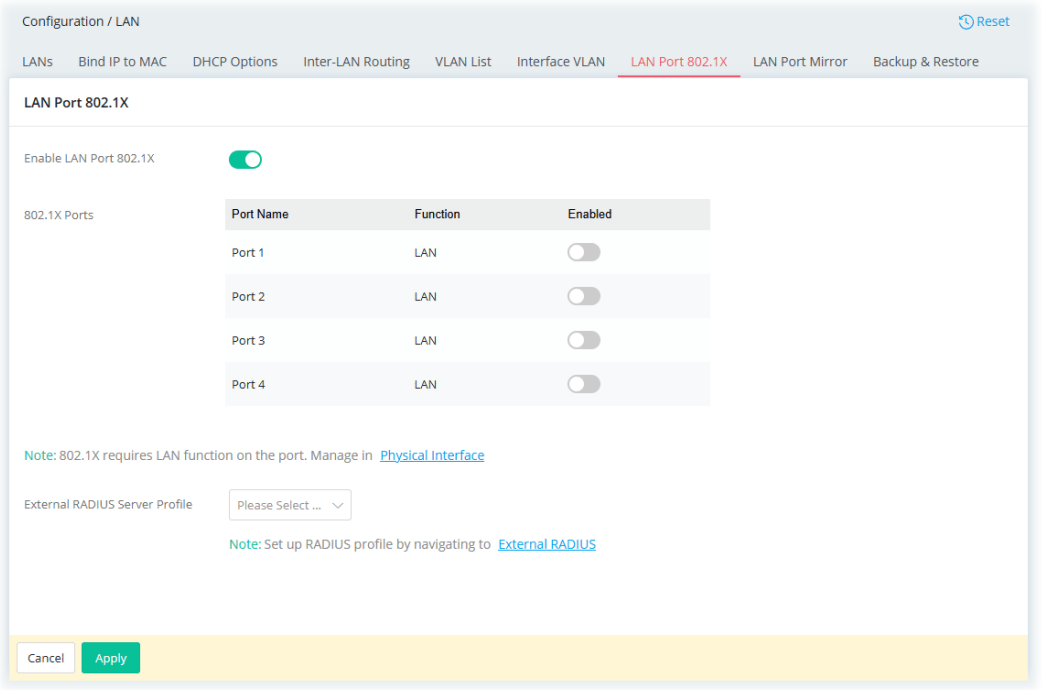



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Port Type** | Select the VLAN type that the interface (Port 1 to 4) will be applied.<br>**Trunk** – The selected Ethernet port can be used or applied to Multiple VLAN profiles.<br>**Access** – The selected Ethernet port can be used or applied to single VLAN profile. |
| **Untagged VLAN** | Select the VLAN profile(s) which will not be tagged.<br>Leave one VLAN untagged at least to prevent from not connecting to Vigor router due to unexpected error. |
| **Tagged VLAN** | Enable 802.1Q tagging for the selected VLAN.<br>The router will add specific VLAN number to all packets on the LAN while sending them out.<br>**All VLANs** – All VLAN profiles will be tagged.<br>**Selected VLANs** – Only the selected VLAN profiles will be tagged. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings and exit the page. |

## II-1-3-7 LAN Port 802.1x

**Wired 802.1X** provides authentication for clients wishing to connect to the LAN by Ethernet. Only one client can be authenticated on each LAN port.

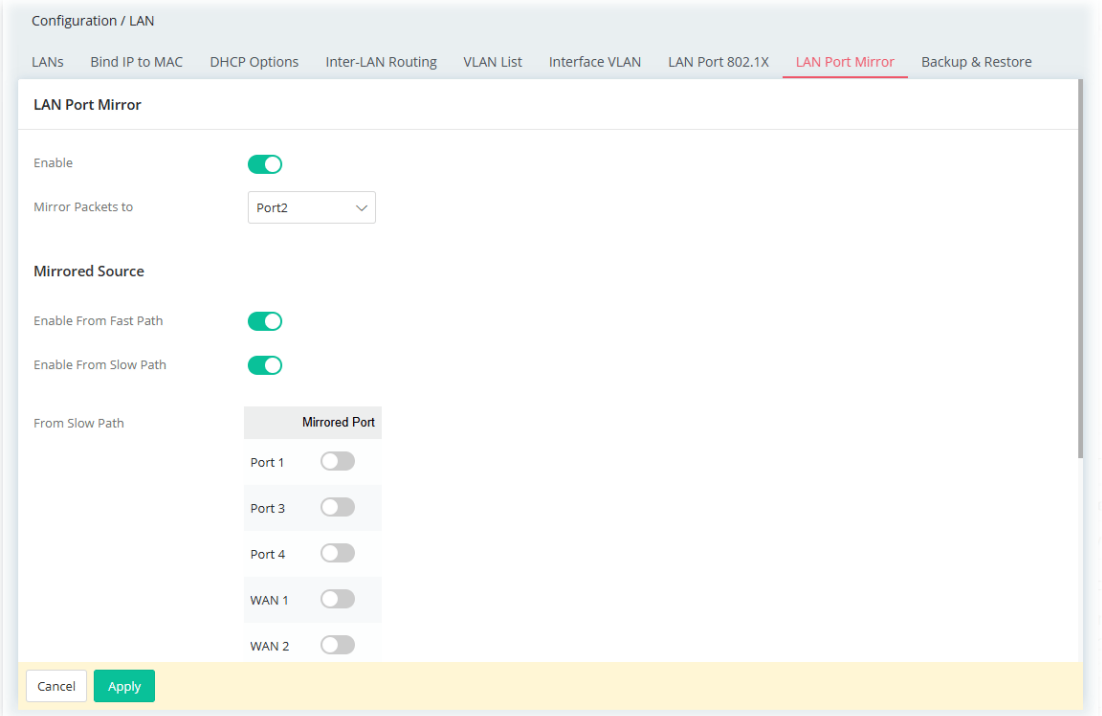



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable LAN Port 802.1X** | Switch the toggle to enable or disable LAN 802.1x function. |
| **802.1X Ports** | **Port Name** - Display the name of the physical LAN port.<br>**Enabled** - Switch the toggle to enable or disable the function. If enabled, the 802.1X authentication will be available for the selected LAN ports. |
| **External RADIUS Sever Profile** | Select one RADIUS server for authenticating the LAN clients. |
| **Cancel** | Discard current settings. |
| **Apply** | Save the current settings. |

## II-1-3-8 LAN Port Mirror

The **LAN Port Mirror** function allows network traffic of select LAN ports to be forwarded to another LAN port for analysis. This is useful for enforcing policies, detecting unauthorized access, monitoring network performance, etc.

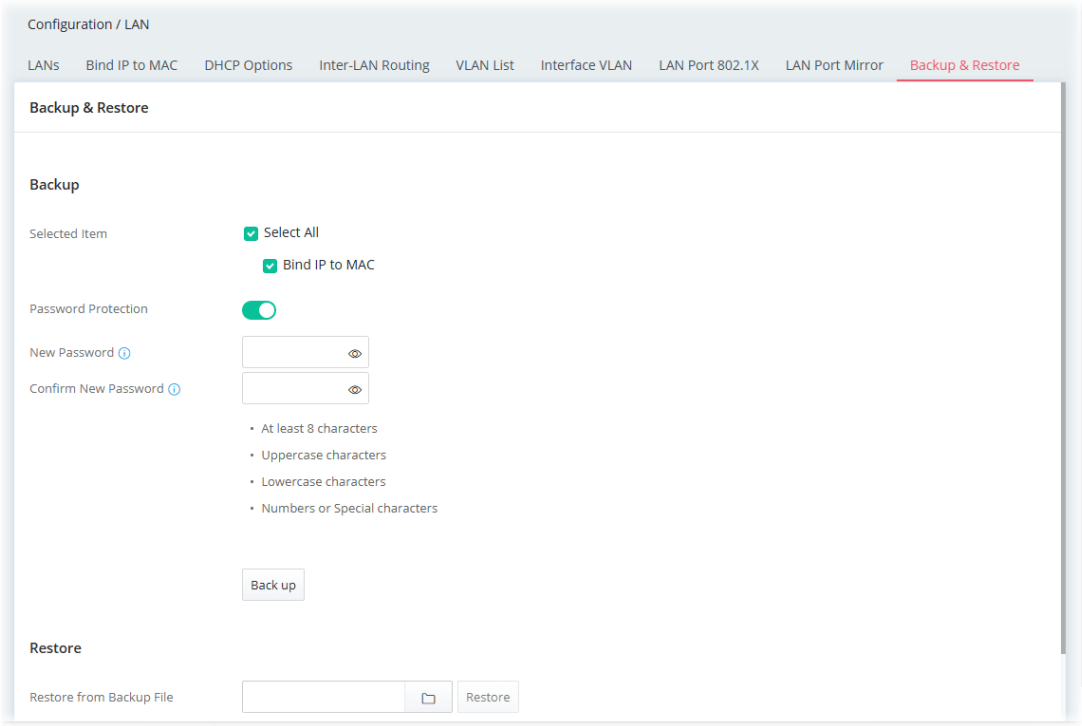



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Switch the toggle to enable or disable LAN port mirror function. |
| **Mirror Packets to** | Specify the mirror port.<br>One and only one port is selected as the mirror port, to which traffic is to be forwarded. |
| | **Mirror Source** |
| **Enable From Fast Path** | Switch the toggle to enable or disable the function. If enabled, all transmitted (TX) and received (RX) packets processed by Hardware Accelerator will be copied and sent to the mirror port. |
| **Enable From Slow Path** | Switch the toggle to enable or disable the function. If enabled, all transmitted (TX) and received (RX) packets passing through the selected Mirrored Port will be copied and sent to the mirror port. |
| **From Slow Path** | **Mirrored Port** – Switch the toggle to select the interface as the mirrored port. |
| **Cancel** | Discard current settings. |
| **Apply** | Save the current settings. |

## II-1-3-9 Backup & Restore

You can save or restore the LAN settings on the router to a file.




Available settings are explained as follows:

| Item | Description |
|---|---|
| | **Backup** |
| **Selected Item** | Select the item to be saved. |
| **Password Protection** | Switch the toggle to enable or disable the function.<br>If enabled, set the following items:<br>● **New Password** - Enter the password with which you wish to encrypt the certificate.<br>● **Confirm New Password** - Enter the password again.<br>**Back up** - Click to download the certificate. |
| | **Restore** |
| **Restore from Backup file** | Click to select the backup file you wish to restore.<br>- Click to locate the file for restoring.<br>**Restore** - Click to retrieve the certificate. |
| **File has Password Protection** | Switch the toggle to enable or disable the function.<br>If enabled, set the following item:<br>● **Password** - Enter the password that was used to encrypt the certificates. |

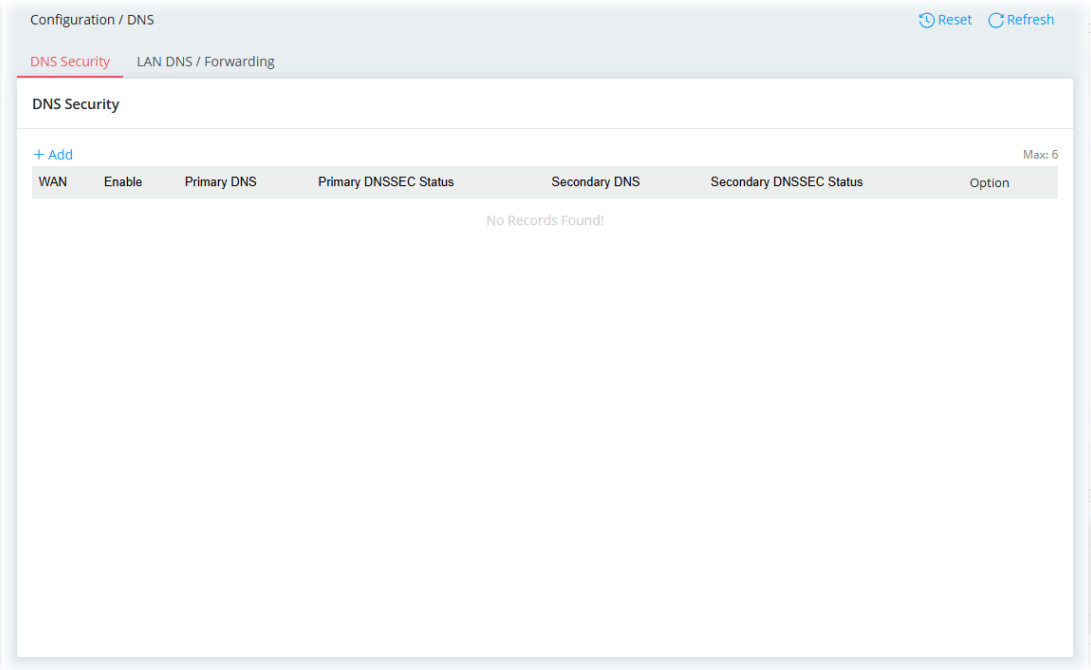
## II-1-4 DNS

DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address.

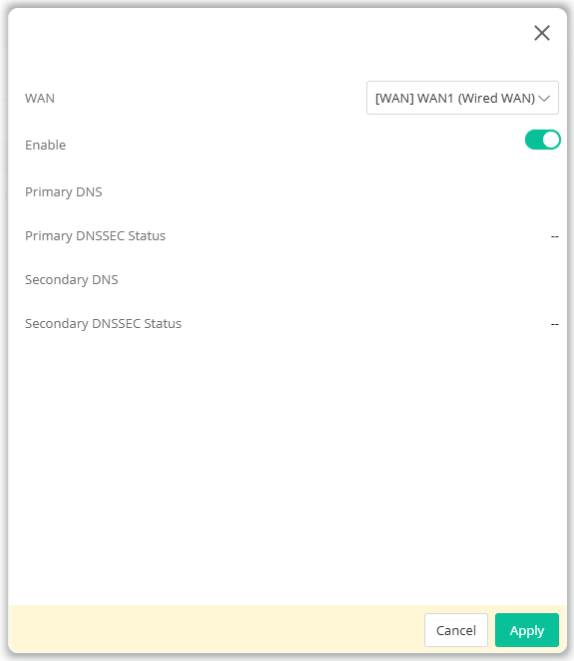
This section offers settings for DNS security and LAN DNS/Forwarding.

### II-1-4-1 DNS Security

The DNS servers must support DNS security validation for the feature to function properly.




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



Available settings are explained as follows:

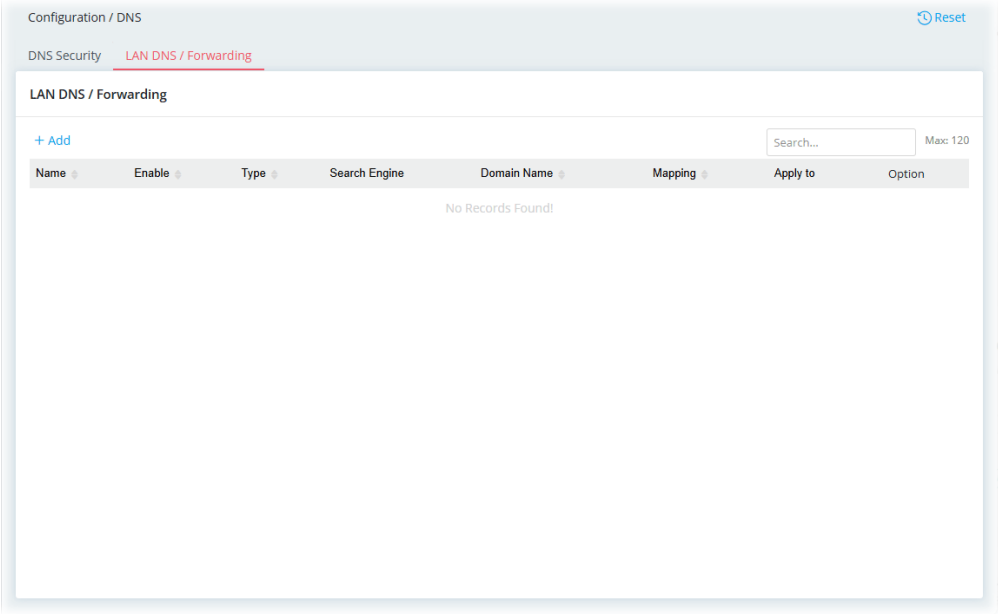
| Item | Description |
|---|---|
| WAN | Select the WAN interface for which DNS security is to be configured. |
| Enable | Switch the toggle to enable or disable DNS security for this WAN Interface. Bogus DNS Reply will be dropped when DNS security enabled. |
| Primary DNS | Shows the primary DNS server used by this WAN.<br>If "--" appears, it means that no WAN is up or no DNS server is configured. |
| Primary DNSSE Status | Shows the inspection results if the DNS server supports the DNS security. The result might be:<br>• [Supported] means the DNS server supporting DNS security.<br>• [Unsupported] means the DNS server does not support DNS security,<br>• "--" means the WAN interface is not up or no DNS server detected.<br>• [Check Failed - WAN Issue] means failure to inspect due to no Internet connection.<br>• [DNSSEC Disabled] means the DNS security is disabled.<br>**Note**: Domain Name System Security Extensions (DNSSEC) protects against DNS-based attacks by authenticating DNS responses from DNS resolvers. |
| Secondary DNS | Shows the secondary DNS server used by this WAN.<br>If "--" appears, it means that this WAN is not up or no DNS server is configured.<br>it means that this WAN is not up or no DNS server is configured. |
| Secondary DNSSE Status | Shows the inspection results if the DNS server supports the DNS security. The result might be:<br>• [Supported] means the DNS server supporting DNS security.<br>• [Unsupported] means the DNS server does not support DNS security,<br>• "--" means the WAN interface is not up or no DNS server detected.<br>• [Check Failed - WAN Issue] means failure to inspect due to no Internet connection.<br>• [DNSSEC Disabled] means the DNS security is disabled.<br>**Note**: Domain Name System Security Extensions (DNSSEC) protects against DNS-based attacks by authenticating DNS responses from DNS resolvers. |
| Cancel | Discard current settings and return to the previous page. |
| Apply | Save the current settings and exit the page. |

## II-1-4-2 LAN DNS/Forwarding

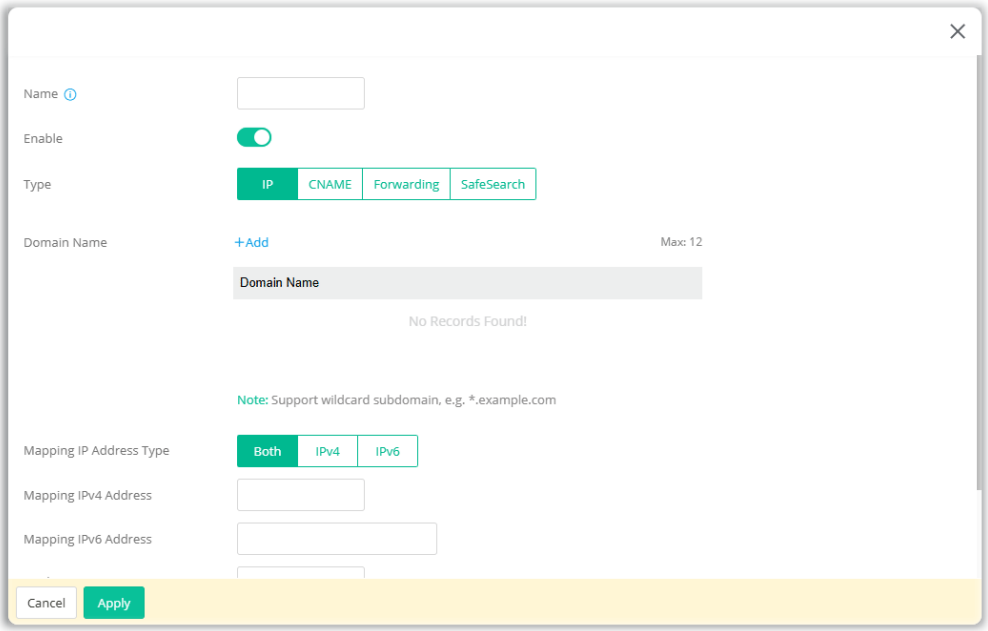
LAN DNS is a simple version of DNS server. LAN DNS allows the network administrator to override standard DNS resolutions for selecting domain addresses. The router will respond to queries on matched domain addresses with custom IP addresses. It is not necessary for the user to build another DNS server in LAN. With such feature, the user can configure some services (such as ftp, www or database) with domain name which is easy to be accessed.

DNS Forwarding allows the network administrator to forward DNS queries to different DNS servers based on the domain name.

LAN DNS and DNS Forwarding only affect DNS queries that are sent to the WAN through the router. DNS queries that are directed to a DNS server on the LAN will not be intercepted by the router.




To add/edit a profile (up to 120), click the **+Add/Edit** link to get the following page.




Available settings are explained as follows:

| Item | Description |
| --- | --- |
| Name | Enter a string as the profile name. |
| Enable | Switch the toggle to enable/disable this profile. |
| Type | Select **IP**, **CNAME, Forwarding** or **SafeSearch**. |
| Domain Name | **+Add** – Enter the domain name for the router to look for in DNS queries to intercept and reply to. Wildcards in the form of asterisks (*) can be used to match a domain level. For example, *.draytek.com will match domain names such as www.draytek.com and ftp.draytek.com.<br>Up to 12 domain names can be created. |
| If IP is selected as the Type | The IP address listed here will be used for mapping with the domain name specified above.<br>**Mapping IP Address Type** – Select Both, IPv4, or IPv6.<br>**Mapping IPv4 Address** – If Both/IPv4 is selected, enter an IPv4 address in this field.<br>**Mapping IPv6 Address** – If Both/IPv6 is selected, enter an IPv6 address in this field.<br>**Apply to** – Select all LANs or specified LAN interfaces for applying this DNS server profile. |
| If CNAME is selected as the Type | **CNAME** – Enter a domain name alias for the domain name.<br>**Apply to** - Select all LANs or specified LAN interfaces for applying this DNS server profile. |
| If Forwarding is selected as the Type | **DNS Server Type** – Both, IPv4, IPv6<br>**Primary IPv4 DNS Server** – Enter the primary IPv4 address of the DNS server you want to use for DNS forwarding.<br>**Secondary IPv4 DNS Server** – Enter the secondary IPv4 address of the DNS server you want to use for DNS forwarding.<br>**Primary IPv6 DNS Server** –Enter the primary IPv6 address of the DNS server you want to use for DNS forwarding.<br>**Secondary IPv6 DNS Server** – Enter the secondary IPv6 address of the DNS server you want to use for DNS forwarding.<br>**Apply to** - Select all LANs or specified LAN interfaces for applying this DNS server profile. |
| If SafeSearch is selected as the Type | Some search engines, such as Bing, Google, and Yandex, can enforce security measures to filter out pornographic and potentially offensive content. These engines are classified as SafeSearch type.<br>**Search Engine** – Select one or more of the commonly used search engines.<br>**Apply to** - Select all LANs or specified LAN interfaces for applying this DNS server profile. |
| Cancel | Discard current settings and return to the previous page. |
| Apply | Save the current settings and exit the page. |

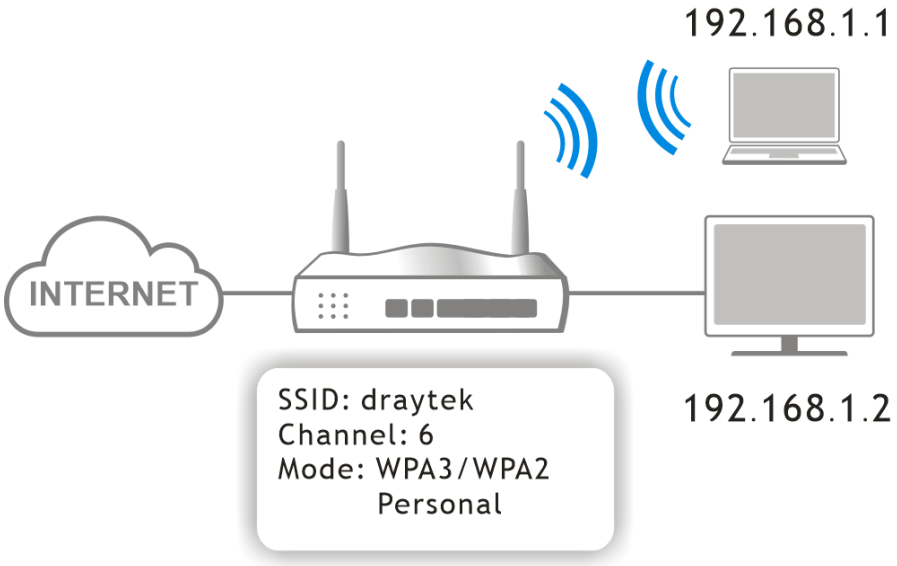
## II-1-5 Wireless LAN

Wireless LAN enables high mobility so WLAN users can simultaneously access all LAN facilities just like on a wired LAN as well as Internet access.

In recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches virtually every location on earth. Billions of people exchange information daily with wireless communication products. The Vigor2136 series of wireless routers (with "ax" in the model name), designed with maximum flexibility and efficiency in mind, is ideal for use in a small office or home. In a business environment, any authorized personnel can bring a WLAN-equipped tablet, PDA or notebook into a meeting room and connect to the network without drilling holes through walls or tearing up flooring to lay a clot of LAN cabling. Wireless networking enables high mobility so WLAN users can access all LAN resources in the same manner just as they would on a wired LAN, but without the cables.

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

In an Infrastructure Mode of wireless network, Vigor wireless router 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 Vigor wireless router. The wireless network settings, such as SSID, channels, encryption protocol, can be configured in this section.




### Multiple SSIDs

Vigor wireless routers support up to four SSIDs (Service Set Identifiers) per band for wireless connections. A service set is a group of wireless network clients that have the same networking parameters. Each service set can be configured to have a unique name (SSID) and specific VLAN or MAC Filtering List, and can be used by different categories of users.

### Real-time Hardware Encryption

Vigor wireless routers are equipped with a hardware AES encryption engine to provide the most effective and efficient protection of wireless traffic, without sacrificing user experience.

### Complete Security Standard Selection

To ensure the security and privacy of your wireless communication, we provide several prevailing standards on market.

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.

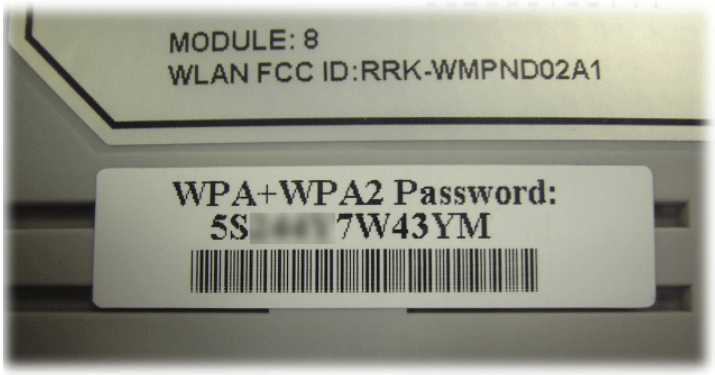
WPA (WiFi Protected Access), the most dominating security mechanism in industry, is separated into two categories: WPA-personal or called WPA Pre-Share Key (WPA/PSK), and WPA-Enterprise or called WPA/802.1x.

In WPA-Personal, a pre-defined key (PSK) is used to encrypt traffic during data transmission. WPA uses the Temporal Key Integrity Protocol (TKIP) for data encryption whereas WPA2/WPA3 applies AES (Advanced Encryption Standard). A major advantage of WPA-Enterprise is that it supports not only encryption but also authentication.

You should select the appropriate security mechanism according to your needs. Because WEP has proven to be vulnerable to attacks, you should consider using WPA instead for the most secure connection. 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 Vigor wireless router is very flexible and can support multiple secure connections with both WEP and WPA at the same time.

**Info**

The default password (PSK) is listed on a label attached to the bottom of the router. Since anyone who has physical access to the router can discover the default password, you are strongly advised to change it.




## Manage Wireless Stations – Monitoring - Clients List

All stations on the wireless network and their connection status will be shown here.

## WPS

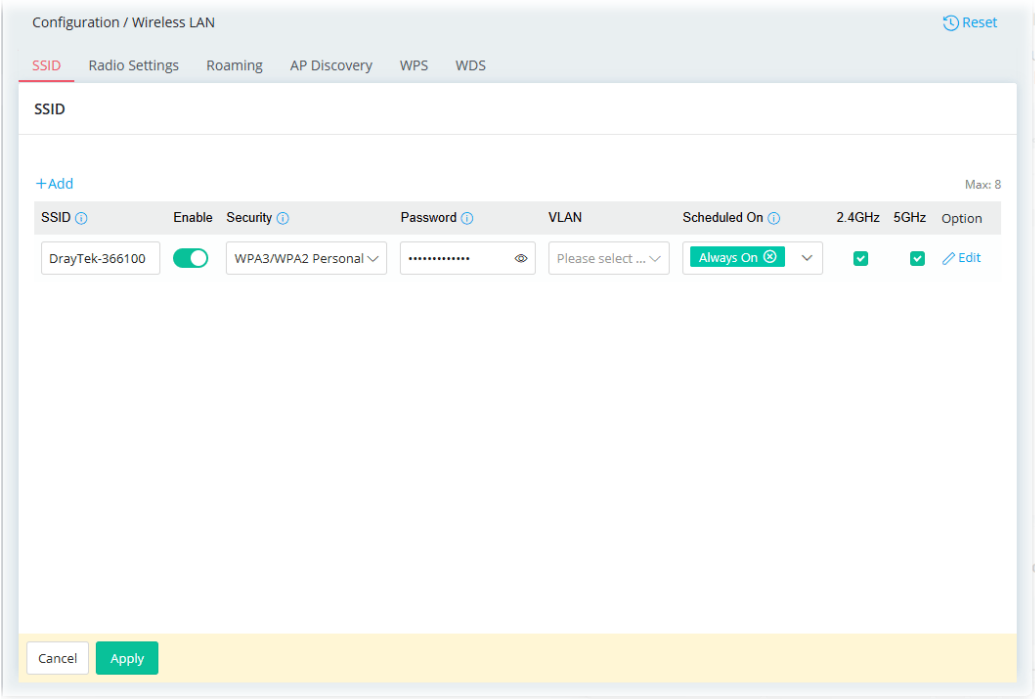
**WPS (WiFi Protected Setup)** makes connecting wireless clients to wireless access points and routers a simple process.



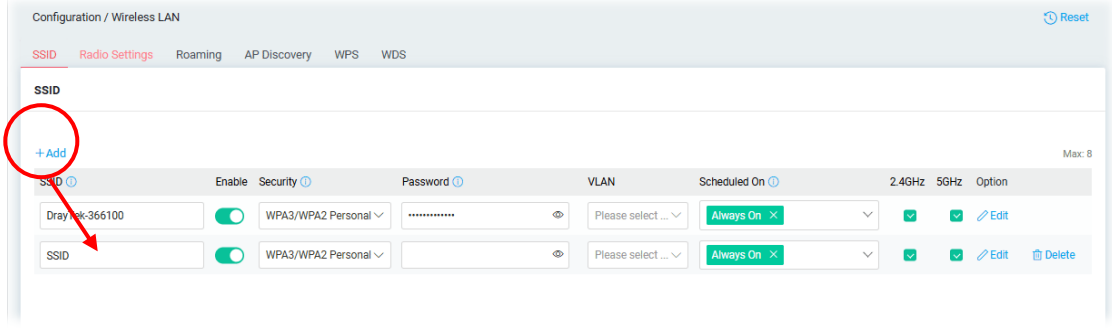

## II-1-5-1 SSID

On WiFi-equipped models, you can set up SSID for use by internal users, who are allowed to access both the LAN and the WAN (Internet).

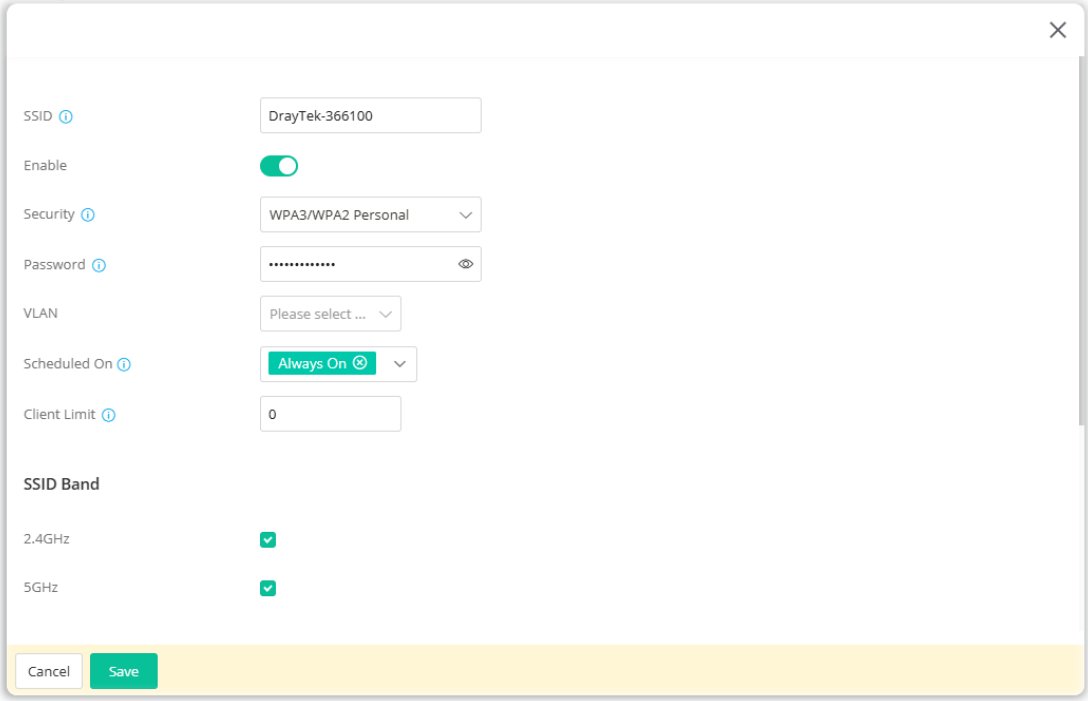
This page also allows you to configure a guest SSID (for wireless clients that are restricted to Internet access only, typically used by visitors) with LAN VLAN settings.



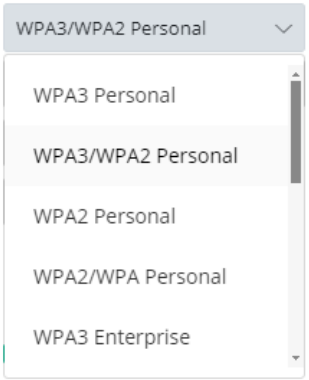

To add a new SSID profile, click **+Add** to create new entry boxes.

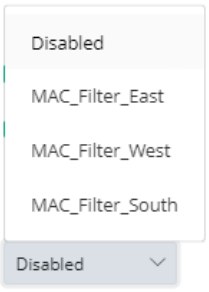


To edit a profile, click the **Edit** link on the right side to get the following page.




Available settings are explained as follows:

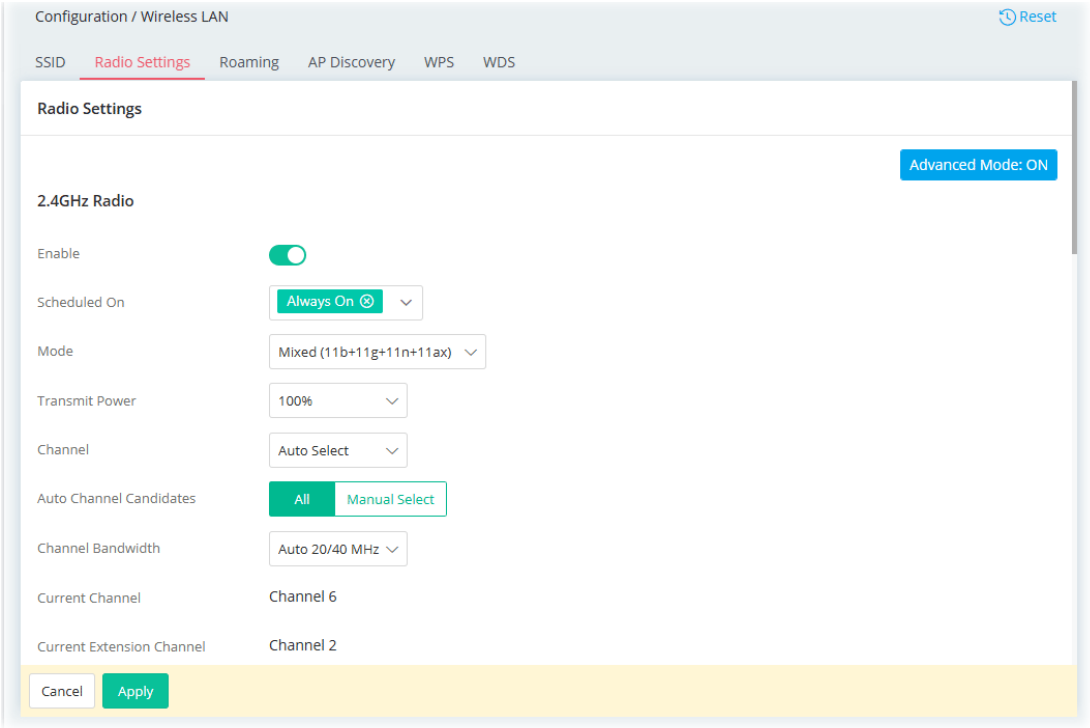
| Item | Description |
|---|---|
| **SSID** | Service Set Identification (SSID), which shows up as the AP identifier. Maximum length is 32 characters. Modify the name if required. |
| **Enable** | Switch the toggle to enable/disable the SSID profile. |
| **Security**<br> | There are several modes provided for you to choose from.<br>Below shows the modes with higher security;<br>**WPA3 Personal, WPA3/WPA2 Personal, WPA2 Personal, WPA2/WPA Personal** – Accepts only WPA clients and the encryption key should be entered in Password. The WPA encrypts each frame transmitted from the radio using the PSK (Pre-Shared Key) entered manually in Password."<br>● **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 key which automatically negotiated via 802.1x authentication.<br>● **OWE** - WPA3 also introduces a new open and secure connection mode; "Opportunistic Wireless Encryption" (OWE). It allows the clients to connect without a password, ideal for hotspot networks, but the connection between each individual client is uniquely encrypted behind the scenes.<br>Below shows the modes with basic security;<br>● **WPA Personal** - Accepts only WPA clients and the encryption key should be entered in Password. The WPA |

| | |
|---|---|
| | encrypts each frame transmitted from the radio using the PSK (Pre-Shared Key) entered manually in Password.<br>• **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.<br>• **WEP Personal** - Accepts only WEP clients and the encryption key should be entered in WEP Settings.<br>• **None** - The encryption mechanism is turned off. |
| **Password** | Enter 8~63 ASCII characters, such as "012345678". This feature is available for WPA Personal, WPA2/WPA Personal, WPA2 Personal, WPA3/WPA2 Personal, and WPA3 Personal mode. |
| **RADIUS Server** | This feature is available for **WPA3 Enterprise, WPA2 Enterprise, WPA2/WPA Enterprise,** and **WPA Enterprise** mode.<br>Use the drop-down list to select a RADIUS server setting.<br>**Note**: Before configuring the RADIUS server, go to **Configuration>>RADIUS/TACACS+** to create external RADIUS profiles (at least one) first. |
| **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).<br>The default is **Always On**. |
| **Client Limit** | Enter the limit number of the client(s) connecting to this AP via this SSID (0 means no limit). |
| **SSID Band** | |
| **2.4GHz/5GHz** | Select the band(s) for the SSID. |
| **SSID Settings** | |
| **MAC Filtering List** | The default is **Disabled**.<br>Select one of the MAC filter profiles (created via Security>>MAC Filtering Profile) for this SSID setting.<br>Only the valid MAC address that has been configured allow or deny to access the wireless LAN interface.<br> |
| **Isolate Client from Wireless** | Switch the toggle to enable/disable the function.<br>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.<br>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** | |
| **WPA Algorithm** | This feature is available for **WPA3 Enterprise, WPA2 Enterprise, WPA Enterprise, WPA3 Personal, WPA2 Personal, WPA Personal, WPA3/WPA2 Personal, or WPA2/WPA Personal** mode.<br>Select TKIP, AES, or TKIP/AES as the algorithm for WPA.<br>Note that not all modes of Vigor router support WPA3 mode. However, if the Vigor router supports WPA3 Personal/Enterprise security mode, the WPA algorithms will be set as AES. |
| **Key Renewal Interval** | It is available when WPA # is selected as Security.<br>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.<br>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. |

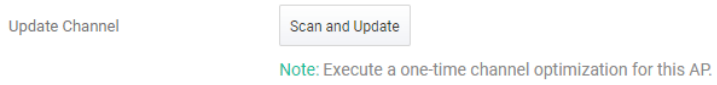
## II-1-5-2 Radio Settings

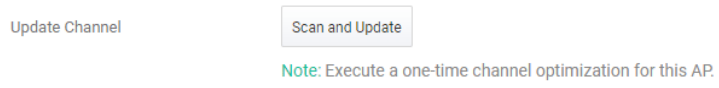
This page lets you configure the most basic settings of your wireless network, including mode, WLAN channels and channel bandwidth.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Advanced Mode:ON/OFF** | Click to show or hide the advanced settings for the Radio settings. |
| **2.4GHz Radio** | |
| **Enable** | Switch the toggle to enable/disable the RADIO settings. |
| **Scheduled On** | This SSID profile will be forced up /down based on the schedule profile used (profiles created via Configuration>>Objects>>Schedule).<br>The default is **Always On**. |
| **Mode** | Select the 802.11 mode allowed on the band.<br>On the 2.4GHz band on **ax** models (2136ax), the following wireless mode options are available:<br>• 11b Only<br>• 11g Only<br>• 11n Only (2.4 GHz)<br>• Mixed (11b+11g)<br>• Mixed (11g+11n)<br>• Mixed (11b+11g+11n)<br>• Mixed (11b+11g+11n+11ax) |
| **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. |
| **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.<br>**All** – The Vigor system can choose the optimal channel from all channels.<br>**Manual Select** – Select one channel or multiple channels for the Vigor system to choose the optimal channel. |
| **Channel Bandwidth** | **20 MHz** –Vigor Router will utilize 20 MHz channels for data transmission and reception between the router and wireless stations.<br>**40 MHz** – Vigor Router will utilize 40 MHz for data transmission and reception between the router and wireless stations.<br>**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. |
| **Current Channel** | Displays current used channel number. |
| **Current Extension Channel** | Displays current used extension channel number. |
| **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.<br> |
| | **5GHz Radio** |
| **Enable** | Switch the toggle to enable/disable the RADIO settings. |
| **Scheduled On** | This SSID profile will be forced up /down based on the schedule profile used (profiles created via Configuration>>Objects>>Schedule).<br>The default is **Always On**. |
| **Mode** | Select the 802.11 mode allowed on the band.<br>On the 5GHz band on ax models (2136ax), the following options are available:<br>• 11a Only<br>• 11n Only (5 GHz)<br>• Mixed (11a+11n)<br>• Mixed (11a+11n+11ac)<br>• Mixed (11a+11n+11ac+11ax) |

| | |
|---|---|
| **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. |
| **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.<br>**All** – The Vigor system can choose the optimal channel from all channels.<br>**Exclude DFS Channels** - The Vigor system can choose the optimal channel from all channels except DFS channels.<br>**Manual Select** – Select one channel or multiple channels for the Vigor system to choose the optimal channel. |
| **Channel Bandwidth** | **20 MHz** –Vigor Router will utilize 20 MHz for data transmission and reception between the router and wireless stations.<br>**40 MHz** – Vigor Router will utilize 40 MHz for data transmission and reception between the router and wireless stations.<br>**80 MHz** –Vigor Router will utilize 80 MHz for data transmission and reception between the router and wireless stations.<br>**160 MHz** – Vigor Router will utilize 160 MHz for data transmission and reception between the router and wireless stations. |
| **Current Channel** | Displays current used channel number. |
| **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.<br> |
| **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.<br>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. |
| **Options under the Advanced Mode** | |
| **TX/RX Stream** | Vigor router can be attached with two antennas to have good data transmission via wireless connection. However, if you have only one antenna attached, please choose 1T1R. |
| **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. |

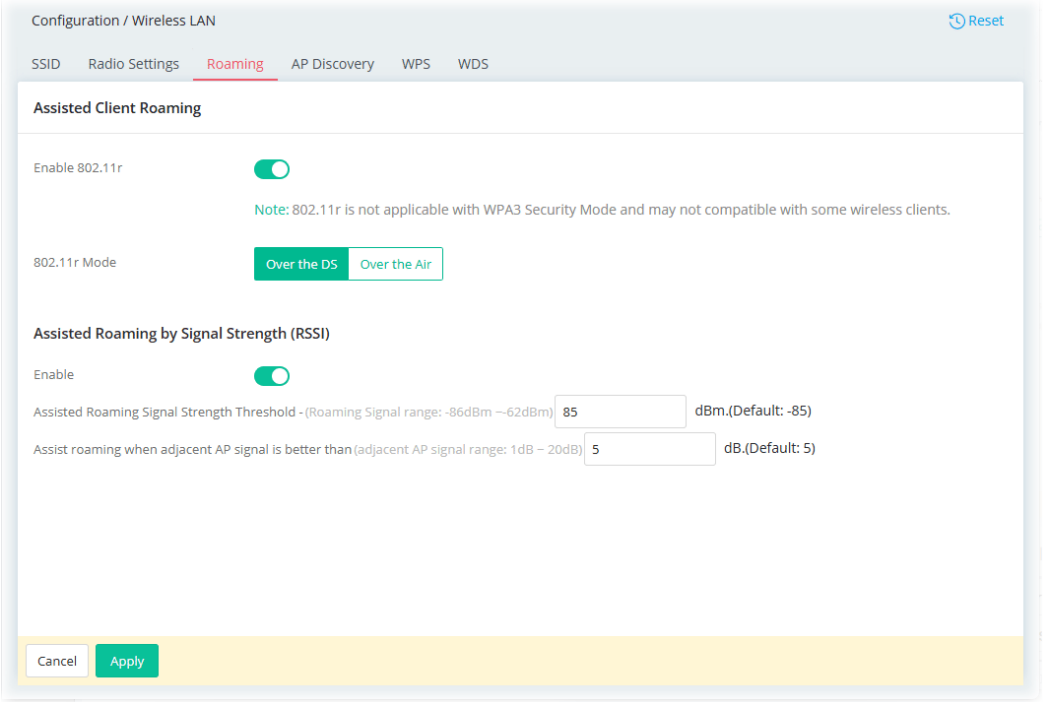
| | |
|---|---|
| | Set the RTS threshold of wireless radio. Do not modify the default value if you don't know what it is. The default value is 2347. |
| **Country Code** | Available for 2.4GHz Radio only.<br>Vigor router broadcasts country codes according to the 802.11d standard. However, some wireless 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 WiFi 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.<br>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 WiFi 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.<br>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.<br>Environments that can benefit by applying airtime fairness:<br>(1) Many wireless stations.<br>(2) All stations mainly use download traffic.<br>(3) The performance bottleneck is wireless connection. |
| **Cancel** | Discard current settings. |
| **Apply** | Save the current settings. |

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

## II-1-5-3 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.

This page allows you to enable the roaming feature.




Available settings are explained as follows:

| Item | Description |
|---|---|
| | **Assisted Client Roaming** |
| **Enable 802.11r** | Switch the toggle to enable/disable the function of fast roaming to make Wireless clients switch between the hotspots fast and securely.<br>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).<br>**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). |
| | **Assisted Roaming by Signal Strength (RSSI)** |
| **Enable** | Switch the toggle to enable/disable the function.<br>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** | Specify a value as a threshold. |

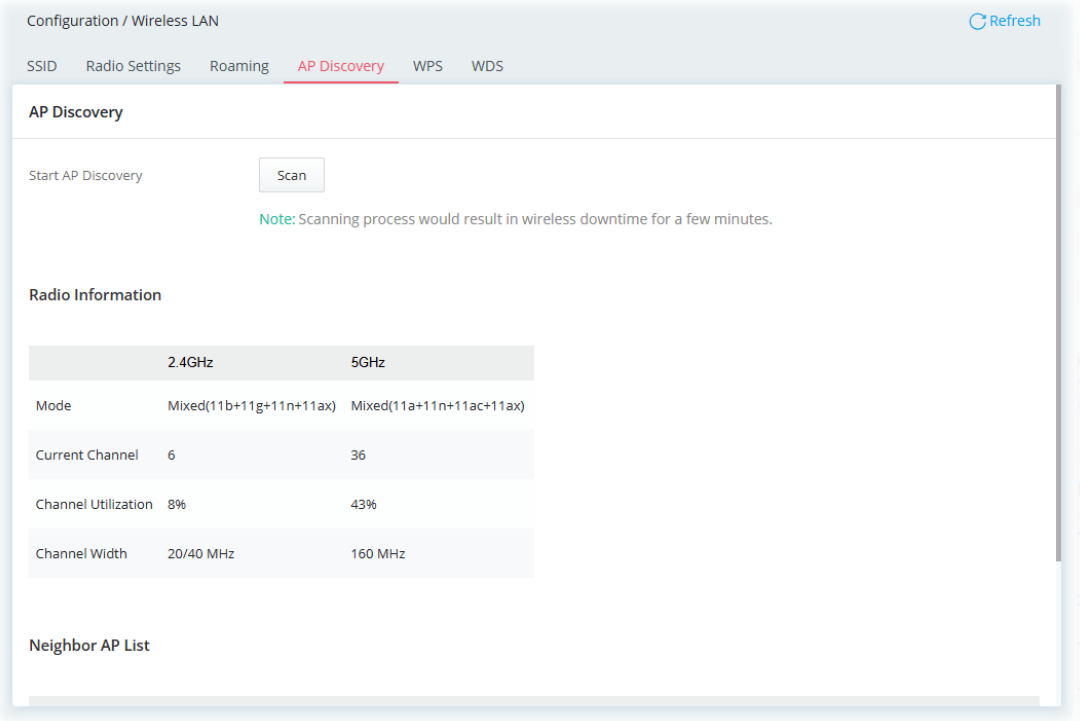
| | |
|---|---|
| better than | |
| Cancel | Discard current settings. |
| Apply | Save the current settings. |

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

## II-1-5-4 AP Discovery

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

This page is used to scan the existence of the APs around. Please click **Scan** to discover all the nearby APs.

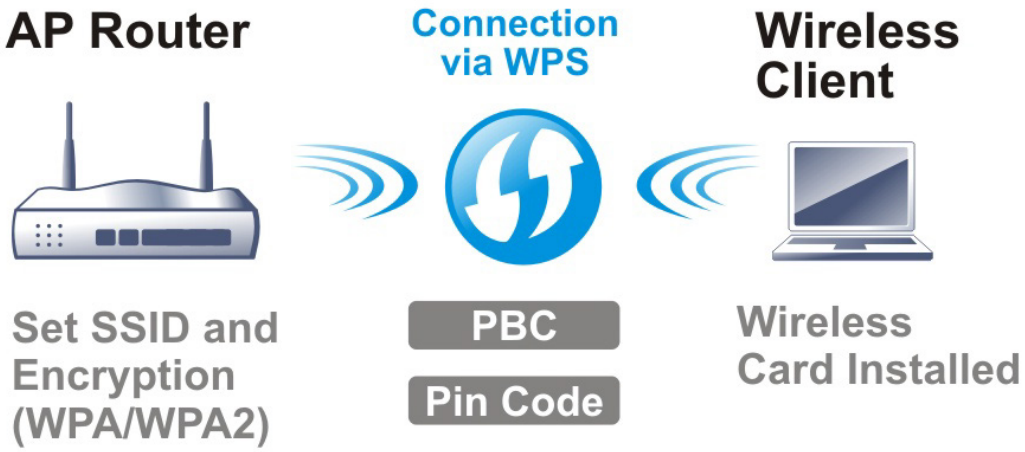



Available settings are explained as follows:

| Item | Description |
|---|---|
| Start AP Discovery | **Scan** - It is used to discover all the nearby AP. The results will be shown on the box below this button. |
| Radio Information | Displays current information for 2.4GHz and 5GHz used by Vigor router. |
| Neighbor AP List | Displays all the nearby APs scanned by Vigor router. |

## II-1-5-5 WPS

**WPS (WiFi Protected Setup)** provides an easy way to connect wireless to wireless access points and routers with WPA or WPA2 encryption.



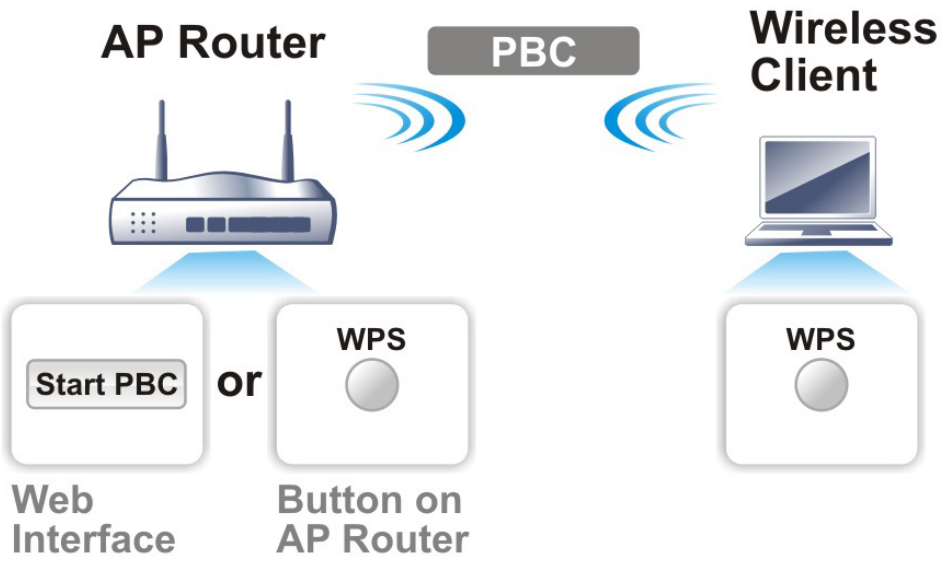

WPS works with wireless stations with WPA or WPA2 support. It does not work with WEP.

It is the simplest way to build connection between wireless network clients and vigor router. 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 router automatically.

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

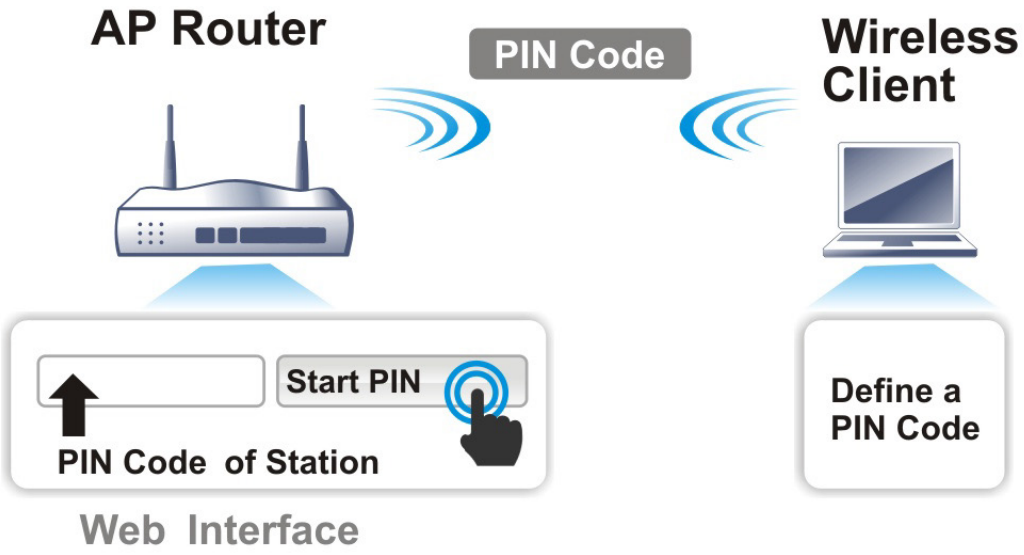
### Using the PBC button

On the Vigor router, press and hold the WPS button on the front panel for 2 seconds, or click the **Start PBC** button on the **Configuration>>Wireless LAN>>WPS** page in the Web User Interface. On the wireless station (for example, a laptop computer), press the **WPS/Start PBC** button on the network card.

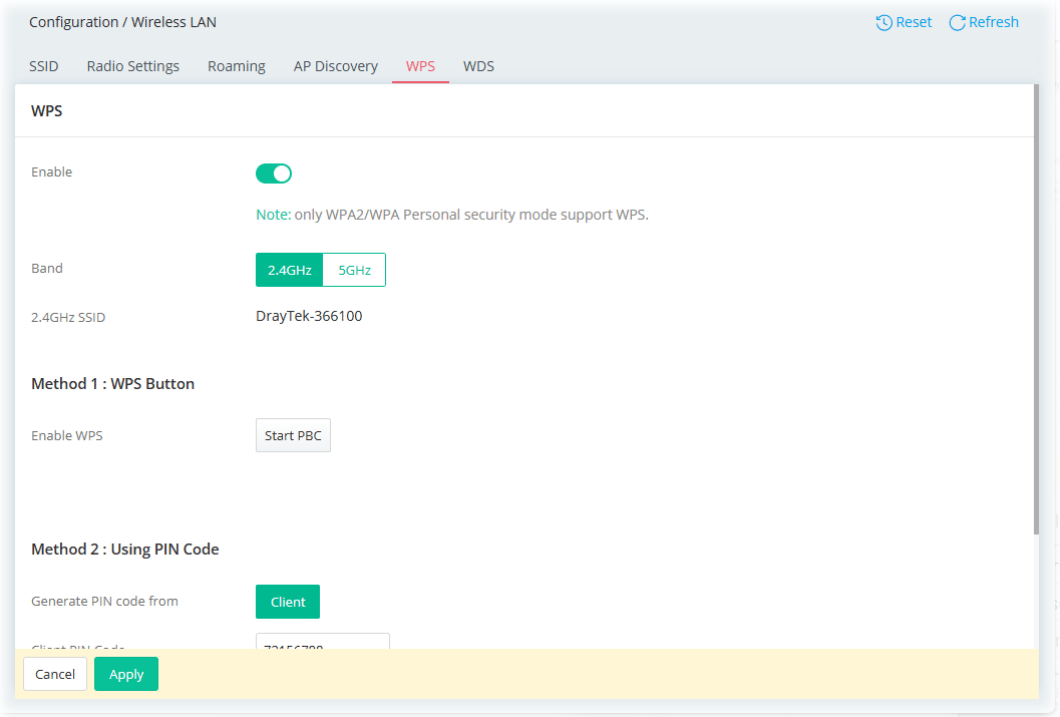


## Using a PIN code

You may establish a wireless connection by entering a PIN code generated by a wireless client that supports WPS.




Below shows **Configuration>>Wireless LAN>>WPS** web page:




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Reset** | Click to reset WPS with the default value. |
| **Refresh** | Click to refresh current page. |
| **Enable** | Switch the toggle to enable/disable the function. |
| **Band** | Select the band (2.4GHz/5GHz) for this function. |

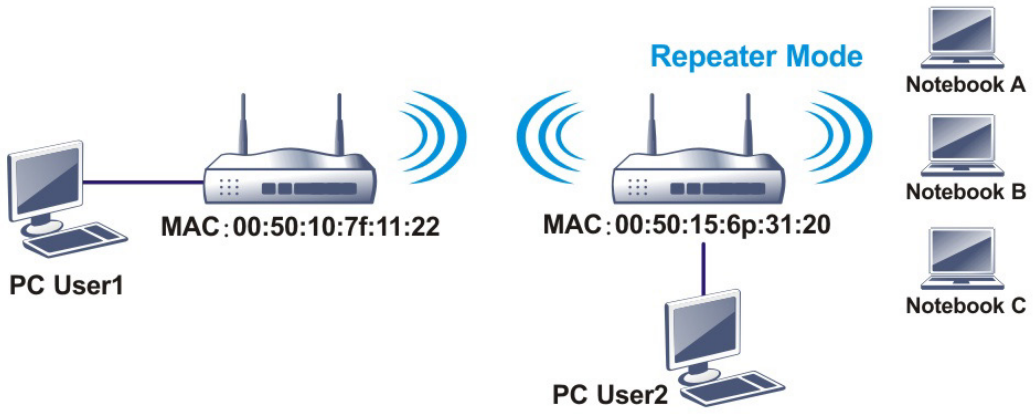
| | |
|---|---|
| 2.4GHz SSID / 5GHz SSID | Displays the SSID used for 2.4GHz/5GHz. |
| Method 1: WPS Button | **Start PBC** –Click it to invoke the Push-Button style WPS setup procedure. The router will wait for about 2 minutes for WPS connection requests from wireless clients. The ACT LED and WLAN LED on the router will blink fast simultaneously when WPS is in progress and will return to normal condition after two minutes. |
| Method 2: Using PIN Code | Enter a PIN code, and click the **Connect** button.<br>**Generate PIN code from** – At present, only **Client** is available.<br>**Client PIN Code** – Enter a PIN code.<br>**Connect** – Click it to make a connection. The ACT LED and WLAN LED on the router will blink fast simultaneously when WPS is in progress, for up to 2 minutes or until a successful WPS connection from a wireless client has been established. |
| Connection Status | Displays the connection status after clicking **Connect** or **Start PBC**. |
| Cancel | Discard current settings. |
| Apply | Save the current settings. |

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

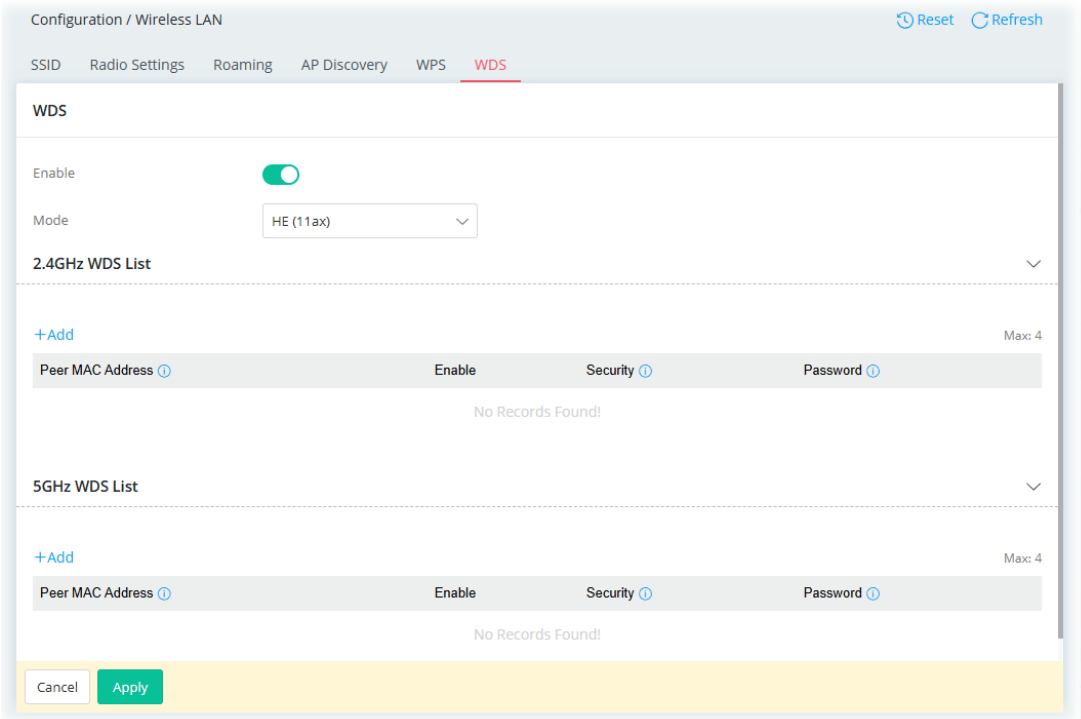
## II-1-5-6 WDS

Wireless Distribution System (WDS) is a protocol for linking access points (AP) wirelessly. Vigor2136ax WDS only supports Repeater mode.

- **Repeater mode**, which extends the coverage range of a WLAN.




Below shows **Configuration>>Wireless LAN>>WDS** web page:




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Reset** | Click to reset WPS with the default value. |
| **Refresh** | Click to refresh current page. |
| **Enable** | Switch the toggle to enable/disable the WDS function. |
| **Mode** | Select the physical mode for this WDS setting.<br>• **HE(11ax)**<br>• **VHT(11ac)**<br>• **HTMIX(11n)** |

| | |
|---|---|
| 2.4GHz/5GHz WDS List | **+Add** – Click to create WDS list (up to 4).<br>**Peer MAC Address** – Enter the MAC address of the WDS peer.<br>**Enable** – Switch the toggle to enable/disable this WDS link.<br>**Security** – Select the encryption method of this WDS link.<br>• **Open** - Security is disabled.<br>• **TKIP** – Enter a string.<br>• **AES** - Enter a string.<br>**Password** – Enter the key of the WDS link when Security is TKIP or AES. It should be a string with 8 ~ 63 ASCII characters.<br>**Delete** – Remove current entry. |
| Cancel | Discard current settings. |
| Apply | Save the current settings. |

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

# II-1-6 Routing

Through the IP address and interface configuration, a route policy can be used to configure any routing rules to fit actual requests.

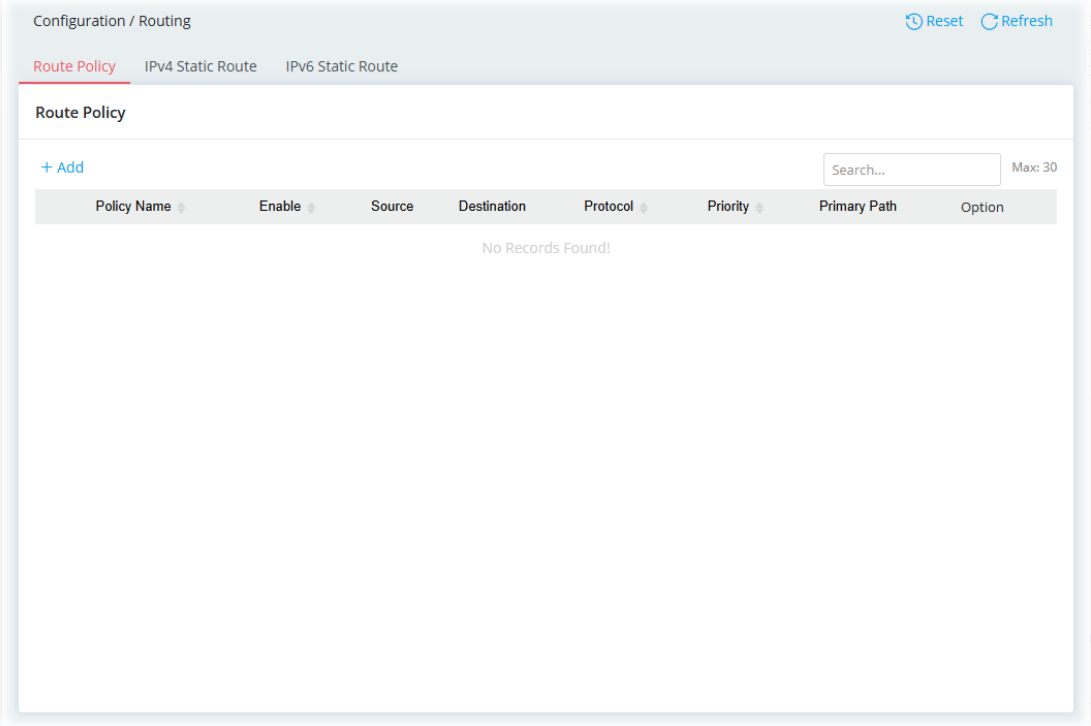
The packets will be directed to the specified interface if they match one of the routing policies.

The router offers IPv4 and IPv6 for you to configure the static route. Both protocols bring different web pages.

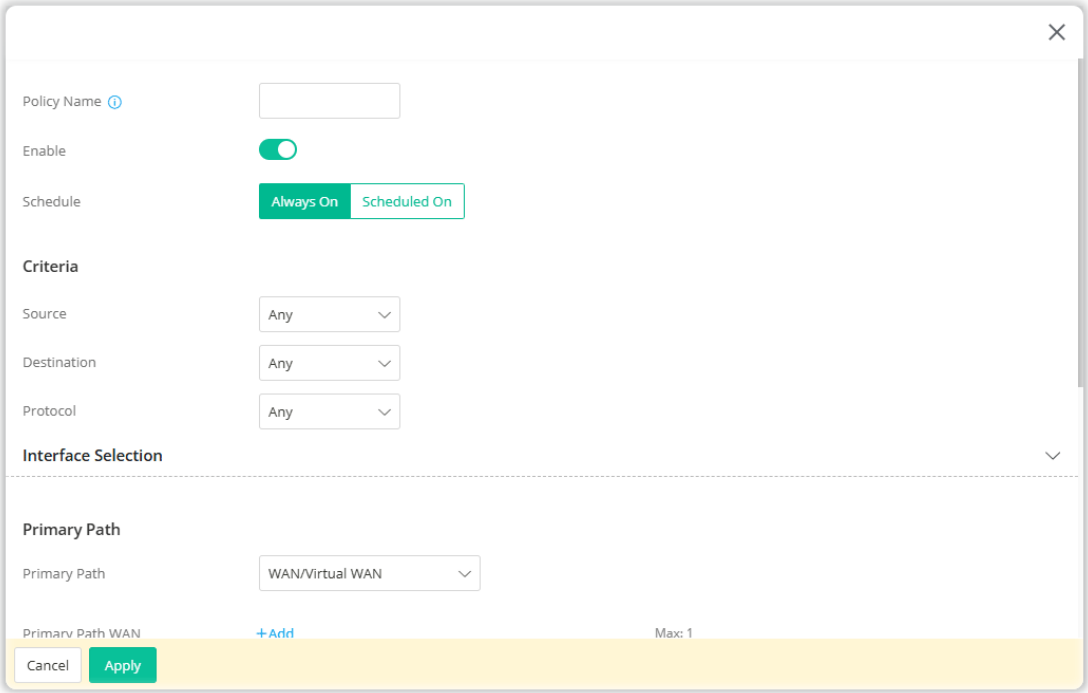
## II-1-6-1 Route Policy

**Route Policy** (also well known as PBR, policy-based routing) is a feature where you may need to get a strategy for routing. The packets will be directed to the specified interface if they match one of the policies. You can setup route policies in various reasons such as load balance, security, routing decision, and etc.

Through protocol, IP address, port number and interface configuration, Route Policy can be used to configure any routing rules to fit actual request.

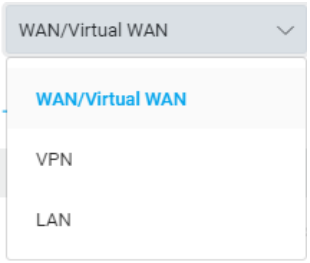


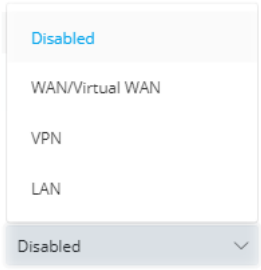
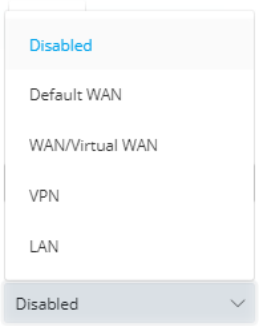

To add a new IPv4 route policy, click the **+Add** link to get the following page.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Policy Name** | Enter a name as the routing profile name. |
| **Enable** | Switch the toggle to enable/disable the profile. |
| **Schedule** | Determine the valid time for the routing profile.<br>**Always On** – The routing profile will be valid all the time if it is enabled.<br>**Scheduled On** – The routing profile will be valid based on the time schedule specified here. |
| **Criteria** | |
| **Source / Destination** | Select the type of IP addresses to which this rule is to be applied.<br>• **Any** - This policy applies to all source/destination IP addresses.<br>• **IPv4 Address** - This policy applies to the specified range of source IP addresses.<br>• **IPv4 Subnet** - This policy applies to source IP addresses defined by the specified network IP address and subnet mask.<br>• **IP Object** - This policy applies to a preconfigured IP object.<br>• **IP Group** - This policy applies to a preconfigured IP group. |
| **Source / Destination IPv4 Address** | It is available when **Source / Destination** is set as **IPv4 Address**.<br>**+Add** – Click to have new entries for setting IPv4 Address Start and End.<br>**IPv4 Address Start / End** – Enter two IPv4 address(s), one for start and one for end.<br>**Delete** – Click to remove current entries. |
| **Source / Destination IPv4 Subnet Address** | It is available when **Source / Destination** is set as **IPv4 Subnet**.<br>**+Add** – Click to have new entries for setting IPv4 subnet.<br>**IPv4 Address** – Enter an IP address. |

| | |
|---|---|
| | **Subnet Mask** - Use the drop down list to choose a suitable mask for the network. |
| **Source / Destination IP Object** | It is available when **Source / Destination** is set as **IP Object**.<br>**+Add** – Click it to create a new object (containing different IP addresses). Up to 12 objects can be created.<br>**Select Object** – Check to select an object or objects. |
| **Source / Destination IP Group** | It is available when **Source / Destination** is set as **IP Group**.<br>**+Add** –Click it to create a new group (containing different IP objects). Up to 12 groups can be specified here.<br>**Select Group** - Check to select a group or groups. |
| **Protocol** | Choose a proper protocol for the WAN interface.<br>**Any** – Any kind of protocol will be used for the WAN interface.<br>**Service Object** – The protocol used will be determined by the service object.<br>• **Service Type Object** – Click **+Add** to create a new object (containing different protocols). Up to 12 objects can be created.<br>**TCP/UDP** – Select TCP/UDP for the WAN interface.<br>• **Specify Source Port** – Switch the toggle to enable the setting of Source Port.<br>• **Source Port / Destination Port** – Set the range (1 to 65535).<br>**TCP** – Same as TCP/UDP.<br>**UDP** – Same as TCP/UDP.<br>**ICMP** – Select ICMP for the WAN interface. |
| | **Interface Selection** |
| **Primary Path** | Specify the interface that the traffic described by this rule is to be directed.<br>If the packet traffic is matched with the criteria set above, it will be sent to the designated interface and gateway.<br>**Primary Path** – Packets will be transferred to the interface chosen here. Select an interface from the list (WAN/LAN: A WAN or LAN interface; VPN: A Virtual Private Network).<br><br>**Primary Path WAN** – It is available when the WAN/Virtual WAN is selected.<br>**+Add** – Click **+Add** to create the primary path. Select WAN interface and the corresponding IP address. Packets match with the criteria will be transferred to the interface chosen here. Select an interface from the list. Specify the gateway (using the default device or customized a gateway IP). Then determine which mechanism (Force NAT/Routing) that the router will use to forward the packet to WAN.<br>**Primary Path VPN** - It is available when the VPN is selected.<br>**+Add** – Click **+Add** to create a new VPN path. Use the drop-down |

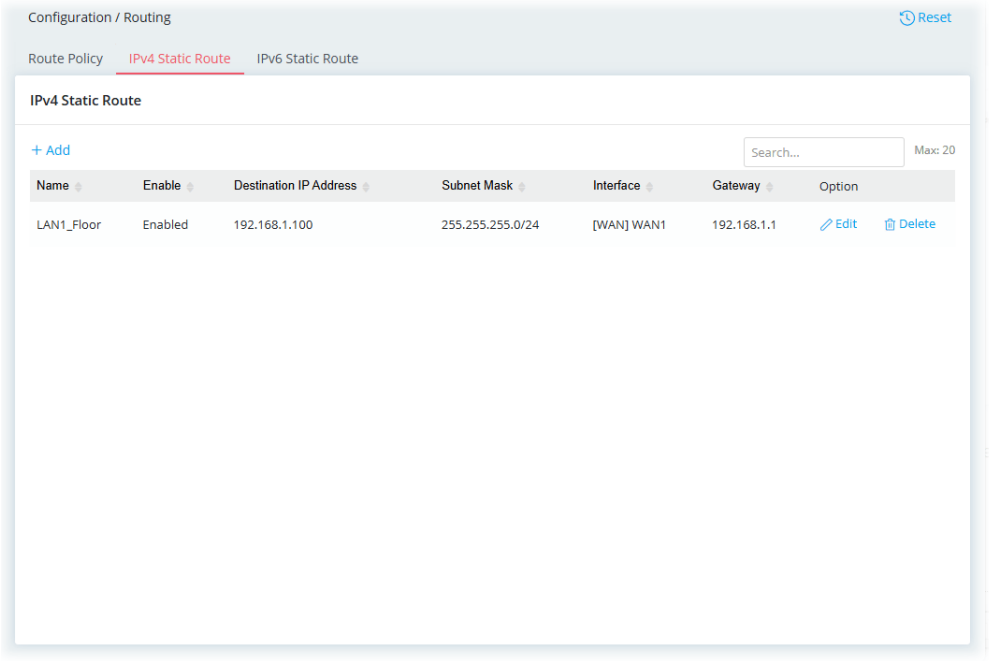
| | |
|---|---|
| | list to select a VPN profile.<br>**Primary Path LAN** - It is available when the LAN is selected.<br>**+Add** – Click +**Add** to create a new VPN path. Use the drop-down list to select a VPN profile. |
| Secondary Path | **Disabled** – Disable the function settings for the secondary path.<br><br>**Secondary Path WAN** – It is available when the WAN/Virtual WAN is set for Secondary Path.<br>**+Add** – Click +**Add** to create the secondary path by specifying WAN settings.<br>**Secondary Path VPN** - It is available when the VPN is set for Secondary Path.<br>**+Add** – Click +**Add** to create a new VPN path.<br>**Secondary Path LAN** - It is available when the LAN is set for Secondary Path.<br>**+Add** – Click +**Add** to create a new LAN path. |
| Last Resort Path | The last resort path (setting) will be adopted instead once the Primary Path or the Secondary Path could not be used for directing the traffic.<br>**Disabled** –Disable the function settings for the Last Resort Path.<br><br>Any packet matching with the rule (source/destination/protocol) specified in Criteria above, will be forwarded to the interface defined on Last Resort Path.<br>**Default WAN** – The default WAN interface will be used for the last resort path.<br>• **Gateway** – Select Default or Customize.<br>• **Gateway IP Address** – Enter the IP address of the gateway if Customize is selected.<br>• **Force NAT/Routing** – Determine which mechanism (Force NAT/Routing) that the router will use to forward the packet to WAN.<br>**WAN/Virtual WAN** – Specify a WAN interface or a virtual WAN interface for the last resort path.<br>• **Last Resort Path WAN** – Click +Add. Then select a WAN interface, the IP address (WAN), the gateway IP address(LAN) |

| | |
|---|---|
| | and the packet forwarding mechanism.<br>**VPN** –Specify a VPN profile for the last resort path.<br>• **Last Resort Path VPN** – Click +Add. Select one of the VPN profiles.<br>**LAN** – Specify a LAN interface for the last resort path.<br>• **Last Resort Path LAN** – Click **+Add**. Then select a LAN interface with an IP address (gateway) and the packet forwarding mechanism. |
| **More settings** | |
| **Enable Syslog** | Switch the toggle to enable/disable the function of saving corresponding log to Syslog. |
| **Priority** | Specifies the priority of the rule about other rules.<br>**Normal** – The routing profile does not affect other routes on the routing table.<br>**High** – The routing profile will override the VPN routes only. However, it will not affect LAN/Static route.<br>**Top** – The routing profile will override VPN and LAN/Static route. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings and exit the page. |

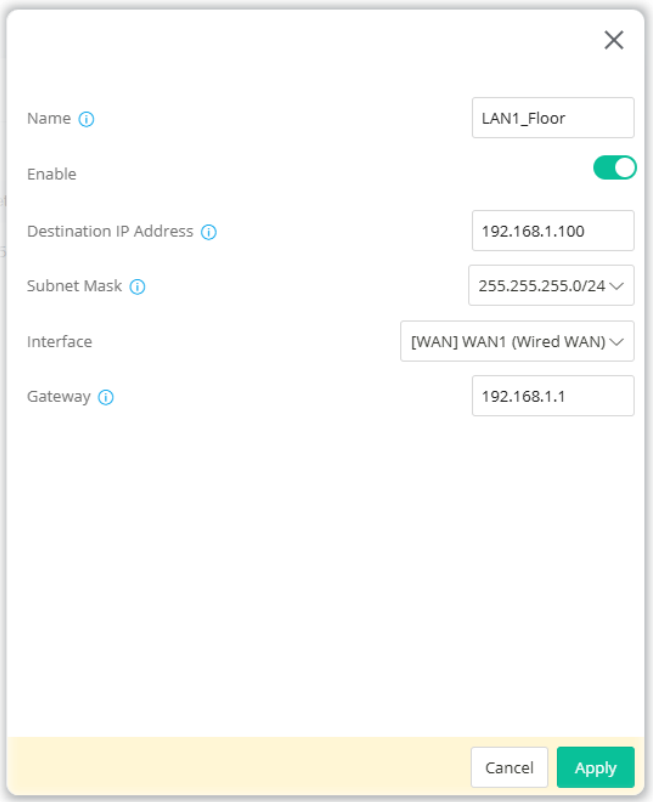
After finishing this web page configuration, please click **Apply** to save the settings.

## II-1-6-2 IPv4 Static Route

Static routing is an alternative to dynamic routing. It is a process that the system network administrator can configure network routers with all the required information for packet forwarding.




To add a new IPv4 static route, click the **+Add** link to get the following page.



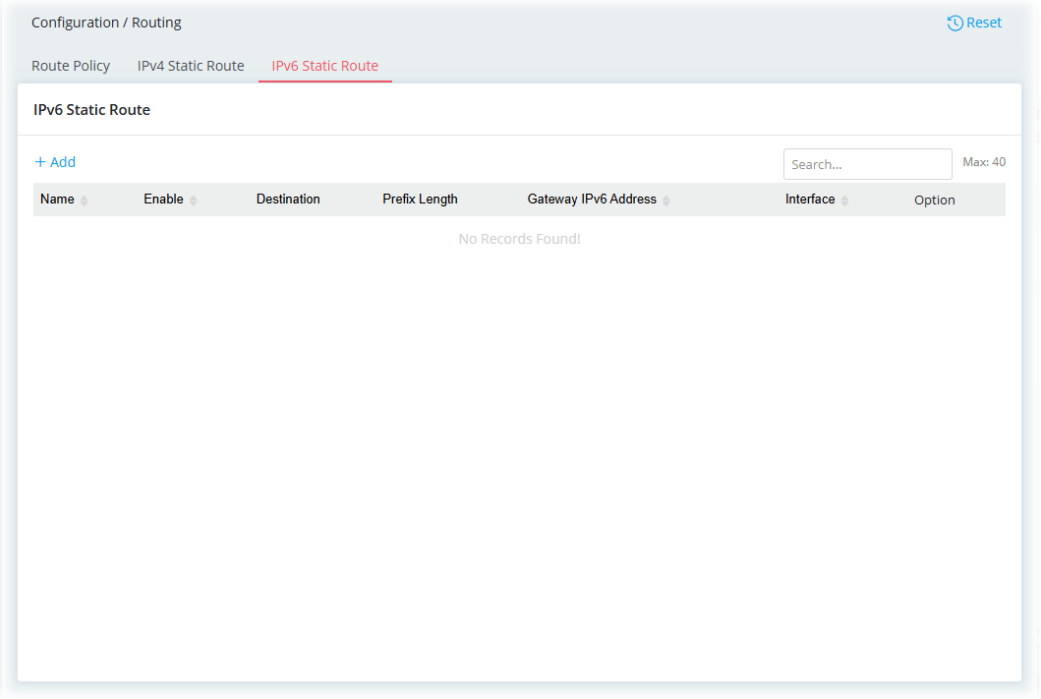

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Name** | Enter a name as the profile name. |
| **Enable** | Switch the toggle to enable or disable the function. |
| **Destination IP Address** | Enter the IP address as the destination IP address. |
| **Subnet Mask** | Select a subnet mask of this static route. |
| **Interface** | Use the drop-down list to specify an interface for this static route. |
| **Gateway** | Enter an IP address as the gateway. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings and exit the page. |

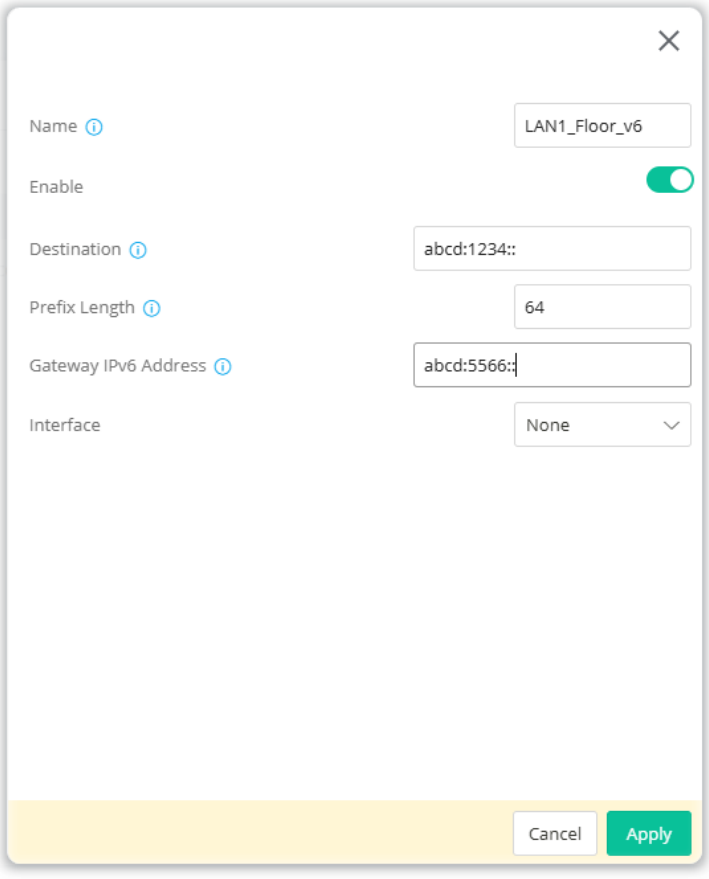
After finishing this web page configuration, please click **Apply** to save the settings.

## II-1-6-3 IPv6 Static Route

Static routing is an alternative to dynamic routing. It is a process that the system network administrator can configure network routers with all the required information for packet forwarding.




To add a new IPv6 static route, click the **+Add** link to get the following page.



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Name** | Enter a name as the profile name. |
| **Enable** | Switch the toggle to enable or disable the function. |
| **Destination** | Enter the IPv6 address as the destination IP address. |
| **Prefix Length** | Enter the fixed value for prefix length. |
| **Gateway IPv6 Address** | Enter an IPv6 address as the gateway. |
| **Interface** | Use the drop-down list to specify an interface for this static route. |
| **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.

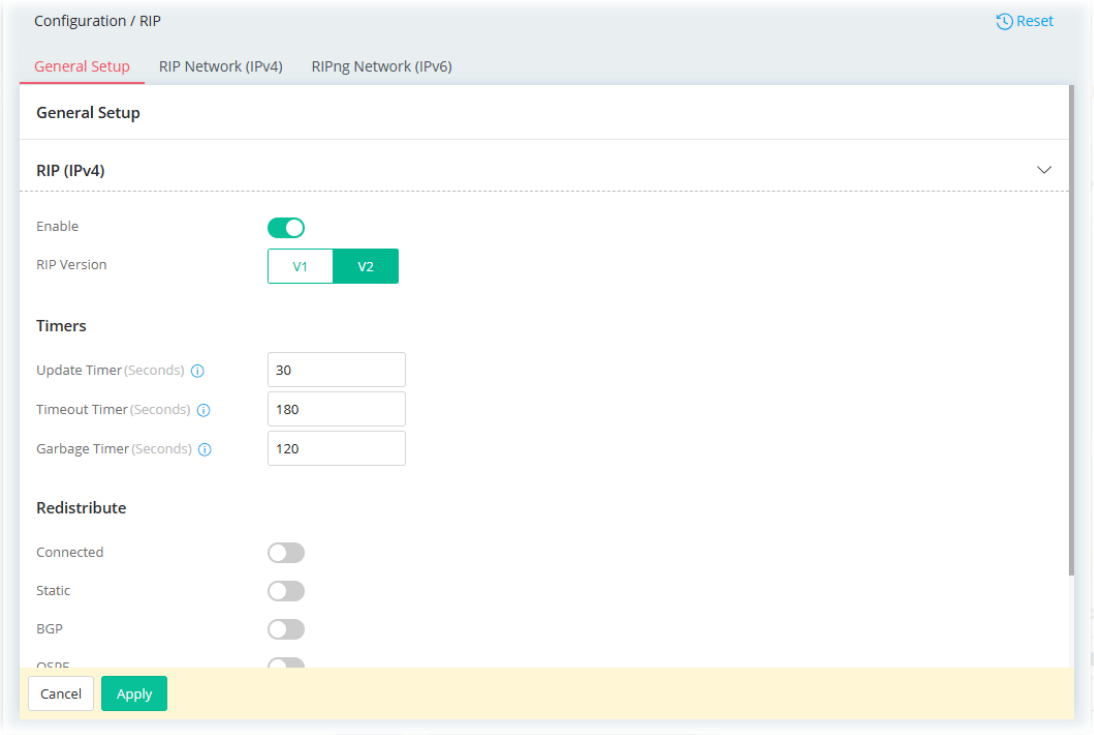
## II-1-7 RIP

The Routing Information Protocol (RIP) and the RIPng (RIP next generation) are the most popular interior routing protocols. The difference is that the RIPng (RIP next generation) is based on the IPv6 address, but offers the same functions and benefits as IPv4 RIP v2.

If enabling the RIP feature, the router will attempt to exchange routing information with neighboring routers using the Routing Information Protocol.

### II-1-7-1 General Setup

There are two versions of RIP available. This page offers comprehensive settings for each of these versions.



Available settings are explained as follows:

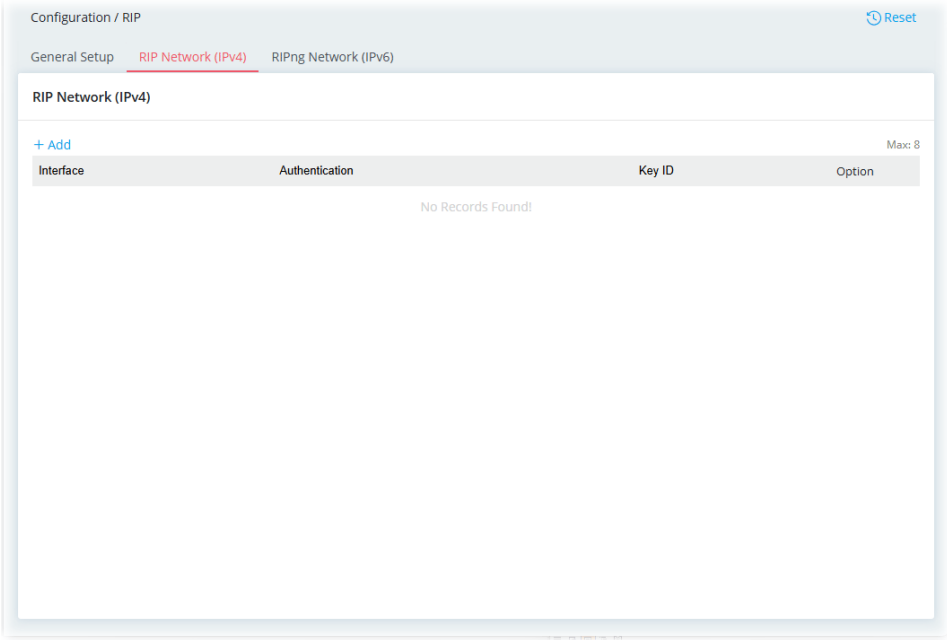
| Item | Description |
|---|---|
| | **RIP (IPv4)** |
| **Enable** | When Enabled, the router will attempt to exchange routing information with neighbouring routers using the Routing Information Protocol. |
| **RIP Version** | Specify the version number (V1/V2) for RIP protocol. |
| **Update Timer** | Enter a value as the update timer.<br>When the time is up, the Vigor router will send a message containing the complete routing table to all neighboring routers for exchanging the routing information. |
| **Timeout Timer** | The routing information will be valid (but not removed) till the time expiration set in this field.<br>The information will be kept in the routing table temporarily. At the same time, the neighbors will be notified that the route has been dropped. |
| **Garbage Timer** | The route will be removed from the routing table upon the expiration set in Garbage Timer. |
| **Connected** | Switch the toggle to enable/disable the function.<br>**All Networks** – Apply the RIP profile to all the LAN interfaces.<br>**Exclude NAT Networks** - Apply the RIP profile to all the LAN interfaces except for NAT network. |
| **Static** | Switch the toggle to enable (apply the static route to the RIP profile) or disable the function. |
| **BGP** | Switch the toggle to enable (allow dynamically route traffic based on information learned from the BGP protocol) or disable the function. |
| **OSPF** | Switch the toggle to enable (allow dynamically route traffic based on information learned from the OSPF protocol) or disable the function. |
| | **RIPng (IPv6)** |
| **Enable** | Switch the toggle to enable/disable the function of Routing Information Protocol next generation (RIPng).<br>By default, inbound IPv6 traffic is blocked. Please ensure that IPv6 traffic is allowed in Firewall Filters >> Default Filters for proper operation. |
| **Update Timer** | Enter a value as the update timer.<br>When the time is up, the Vigor router will send a message containing the complete routing table to all neighboring routers for exchanging the routing information. |
| **Timeout Timer** | The routing information will be valid (but not removed) till the time expiration set in this field.<br>The information will be kept in the routing table temporarily. At the same time, the neighbors will be notified that the route has been dropped. |
| **Garbage Timer** | The route will be removed from the routing table upon the expiration set in Garbage Timer. |

| | |
|---|---|
| Connected | Switch the toggle to enable (apply the RIPng settings to all the LAN interfaces) or disable the function. |
| Static | Switch the toggle to enable (apply the static route to the RIP profile) or disable the function. |
| BGP | Switch the toggle to enable (allow dynamically route traffic based on information learned from the BGP protocol) or disable the function. |
| OSPF | Switch the toggle to enable (allow dynamically route traffic based on information learned from the OSPF protocol) or disable the function. |
| Cancel | Discard current settings. |
| Apply | Save the current settings. |

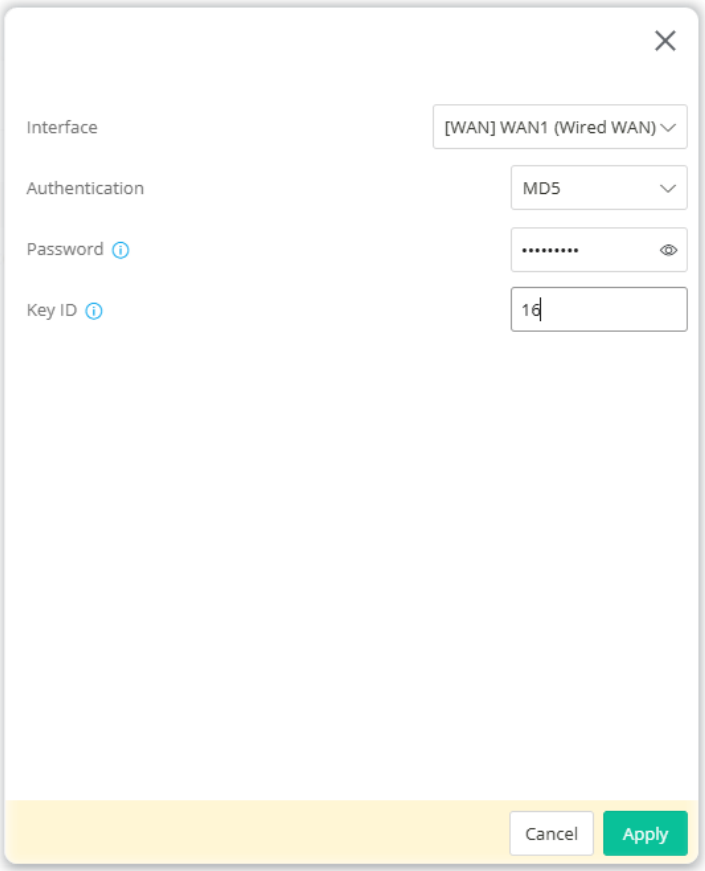
After finishing this web page configuration, please click **Apply** to save the settings.

## II-1-7-2 RIP Network (IPv4)

This page allows you to configure up to eight neighboring routers for exchanging the routing information with the local router (Vigor2136).




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



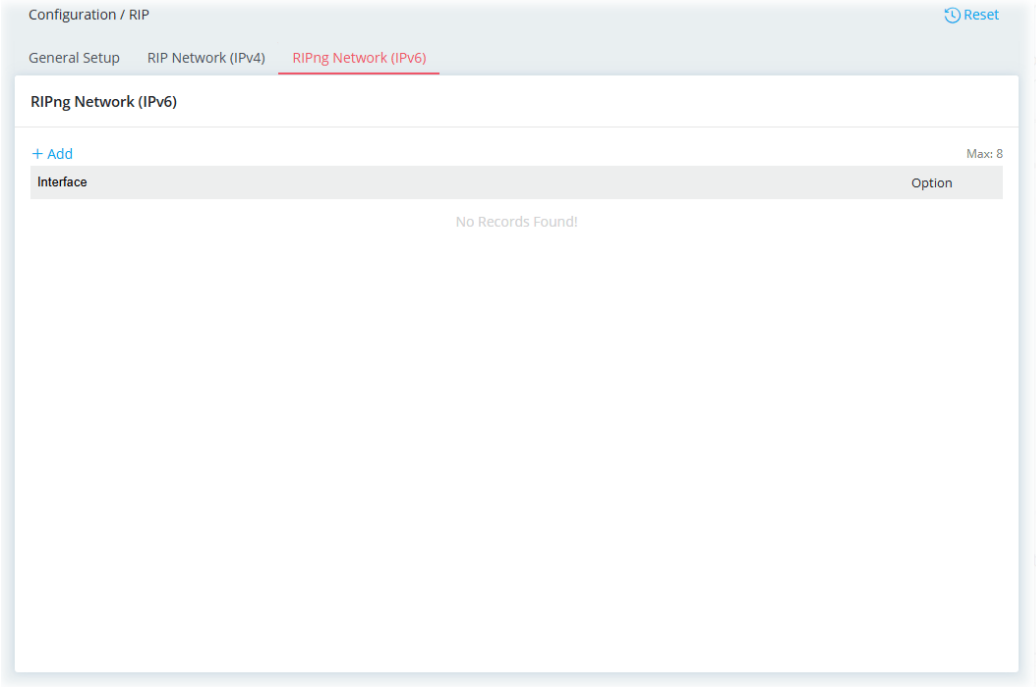

Available settings are explained as follows:

| Item | Description |
|---|---|
| Interface | Select a LAN / WAN interface to apply the settings configured for this profile. |
| Authentication | Select the authentication mechanism for this profile.<br>**Disabled** – No authentication mechanism will be used.<br>**Plain-Text** – Only password will be used for authentication.<br>• **Password** –Enter characters as the password for MD5 authentication.<br>**MD5** – Use MD5 authentication.<br>• **Password** – Enter characters as the password for MD5 authentication.<br>• **Key ID** – Enter a number (0~255). The ID will help Vigor router to be identified in an autonomous system. |
| 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-1-7-3 RIPng Network (IPv6)

This page allows you to configure up to eight interfaces (WAN or LAN) for exchanging the routing information with the local router (Vigor2136) based on IPv6 address(es).




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




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Interface** | Select a LAN / WAN interface to apply the settings configured for this profile. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings and exit the page. |

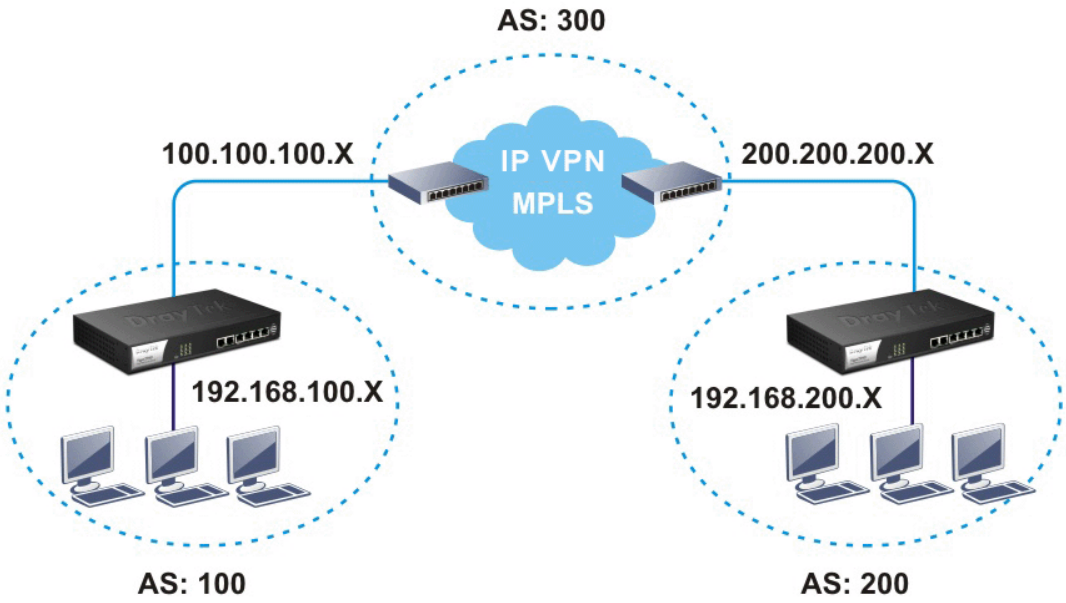
After finishing this web page configuration, please click **Apply** to save the settings.

## II-1-8 BGP

Border Gateway Protocol (BGP) is a standardized protocol designed to exchange routing and reachability information among autonomous systems (AS) on the Internet.

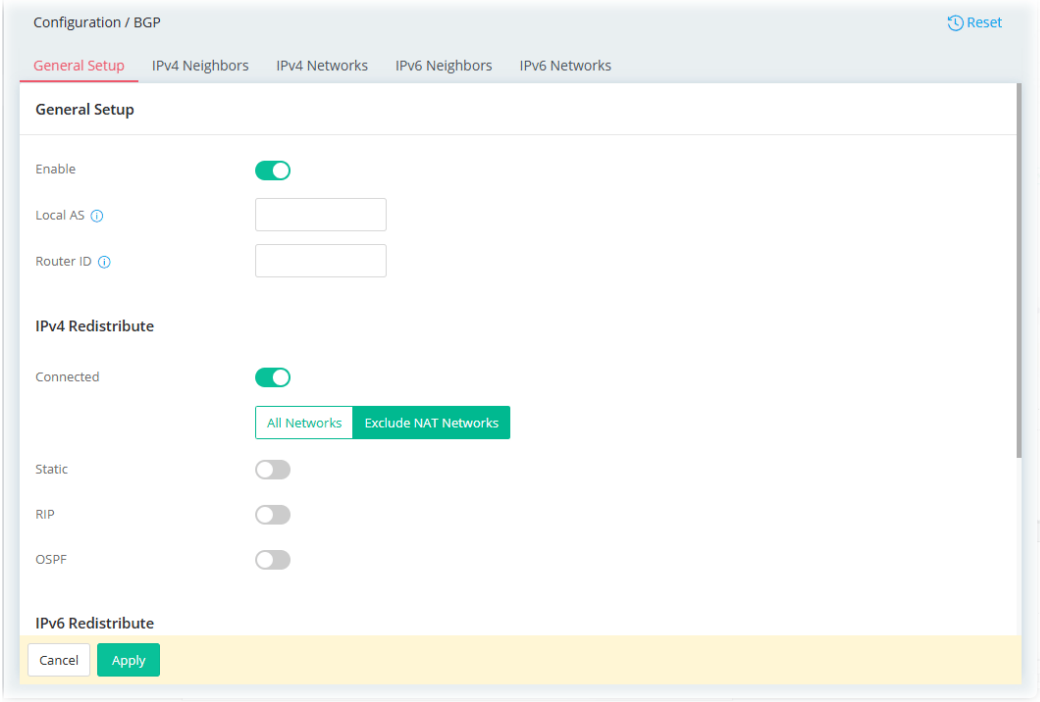
The protocol TCP is used by two routers supporting BGP for data transmission. They can exchange the BGP routing information for each other. A BGP router is the "neighbor" of other BGP routers. Define the IPv4/IPv6 address, AS number for the router is essential for TCP connection of BGP routing information exchange.

AS, the abbreviation of Autonomous System, is a group interconnected with multiple IPv4/IPv6 addresses. Each AS shall be assigned with one AS number (ASN). The ASN is a unique identifier for AS to distinguish each network group in the whole interconnected network. It can be operated by one or several ISPs and follows the routing policies made by ISP.




### II-1-8-1 General Setup

Set general settings for for local router and neighboring routers.



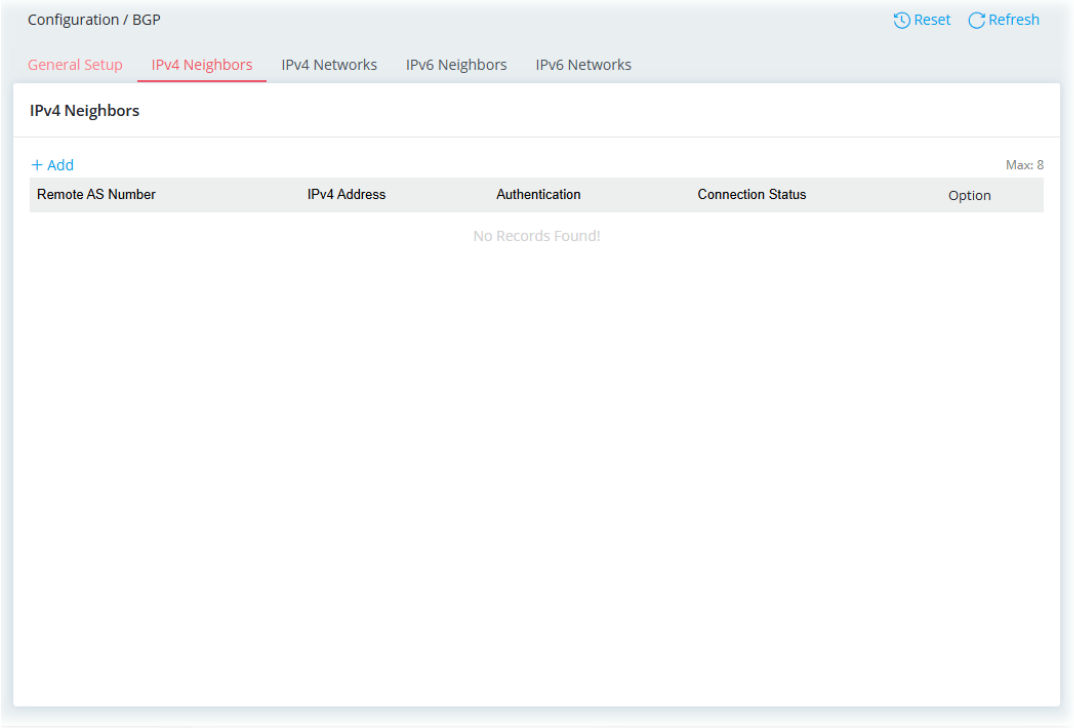

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Switch the toggle to enable/disable the basic BGP function for local router. |
| **Local AS** | Set the AS number for local router. |
| **Router ID** | Specify the LAN subnet for the router. |
| | **IPv4 Redistribute** |
| **Connected** | **All Networks** – Apply the BGP profile to all the LAN interfaces.<br>**Exclude NAT Networks** - Apply the BGP profile to all the LAN interfaces except for NAT network. |
| **Static** | Switch the toggle to enable or disable the function (apply the static route to the BGP profile). |
| **RIP** | Switch the toggle to enable or disable the function (apply the RIP function to the BGP profile). |
| **OSPF** | Switch the toggle to enable or disable the function (apply the OSPF function to the BGP profile). |
| | **IPv6 Redistribute** |
| **Connected** | Switch the toggle to enable (apply the BGP profile to all the LAN interfaces) or disable the function. |
| **Static** | Switch the toggle to enable or disable the function (apply the static route to the BGP profile). |
| **RIP** | Switch the toggle to enable or disable the function (allow dynamically route traffic based on information learned from the RIP protocol). |
| **OSPF** | Switch the toggle to enable or disable the function (allow dynamically route traffic based on information learned from the OSPF protocol). |

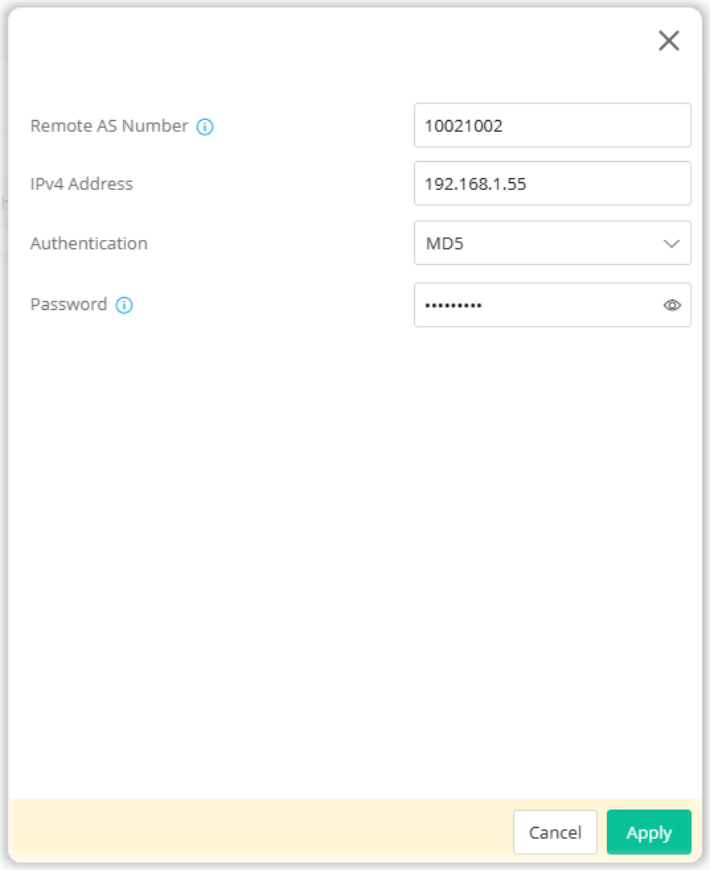
| | |
|---|---|
| Cancel | Discard current settings and return to the previous page. |
| Apply | Save the current settings and exit the page. |

## II-1-8-2 IPv4 Neighbors

Set general settings for the neighboring routers (based on IPv4 address).




To add a new IPv4 neighbors profile (up to 8), click the **+Add** link to get the following page.



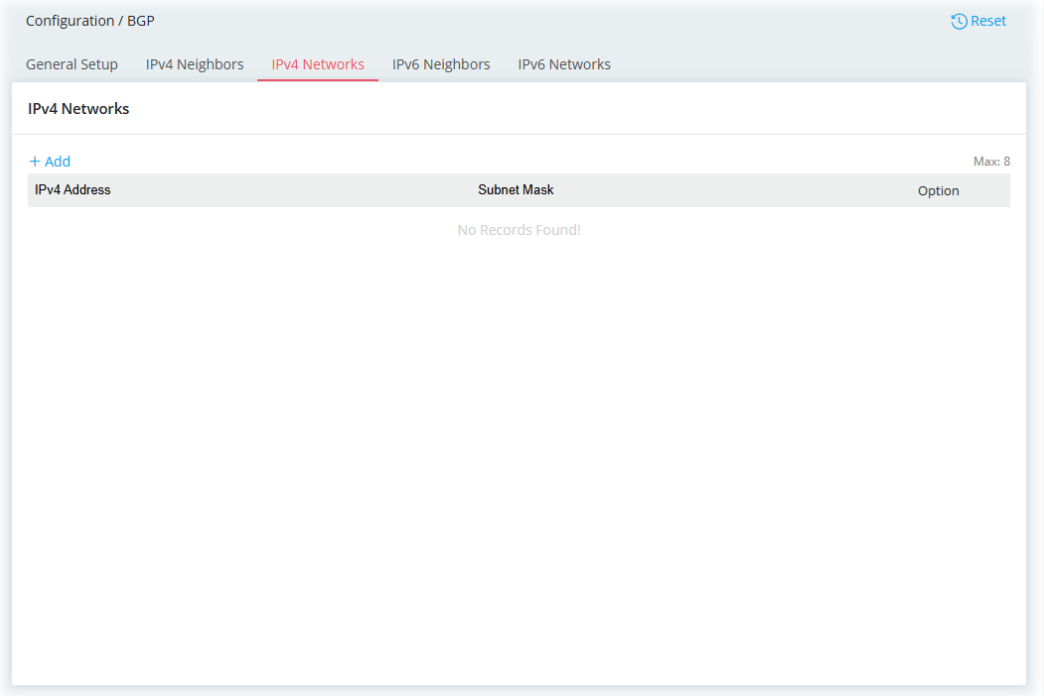

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Remote AS Number** | Specify the AS Number for neighboring router. |
| **IPv4 Address** | Enter the IP address specified for the neighboring profile. |
| **Authentication** | Select the authentication mechanism for this profile.<br>**Disabled** – No authentication mechanism will be used.<br>**MD5** – Use MD5 authentication.<br>• **Password** – Enter characters as the password for MD5 authentication. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings and exit the page. |

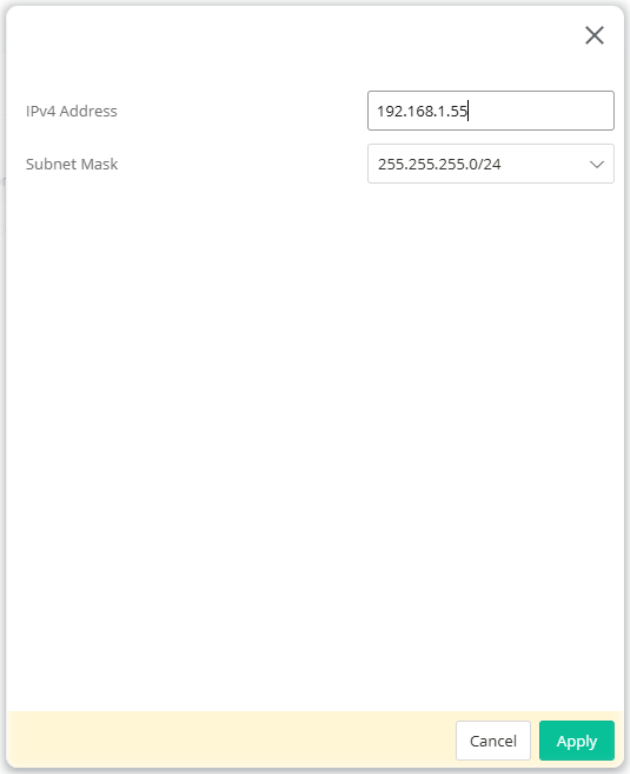
After finishing this web page configuration, please click **Apply** to save the settings.

## II-1-8-3 IPv4 Networks

This page allows you to configure up to eight neighboring networks for exchanging the routing information with the local router (Vigor2136). The IP address defined on this page will be used to declare which network will participate in the RIP protocol.




To add a new IPv4 networks profile (up to 8), click the **+Add** link to get the following page.



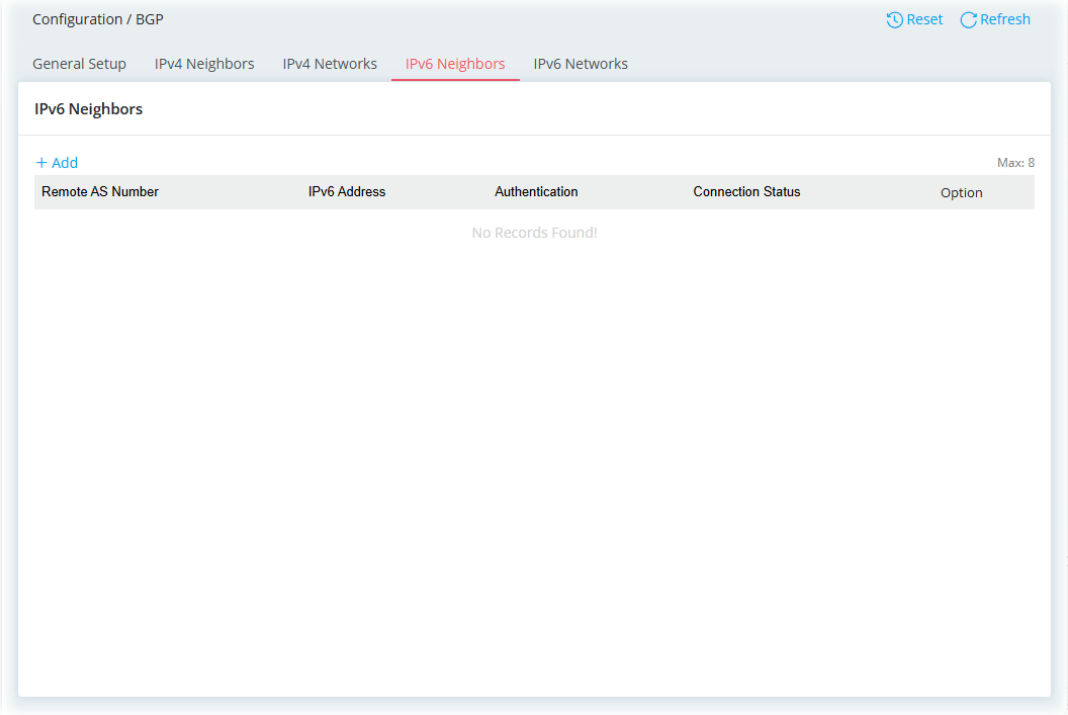

Available settings are explained as follows:

| Item | Description |
| --- | --- |
| **IPv4 Address** | Enter the IPv4 address of a neighboring network (following CIDR format).<br>Vigor router (e.g., 2136 series) will exchange routing information (RIP info) with the specified network. |
| **Subnet Mask** | Select the mask value for the IPv4 address specified above. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings and exit the page. |

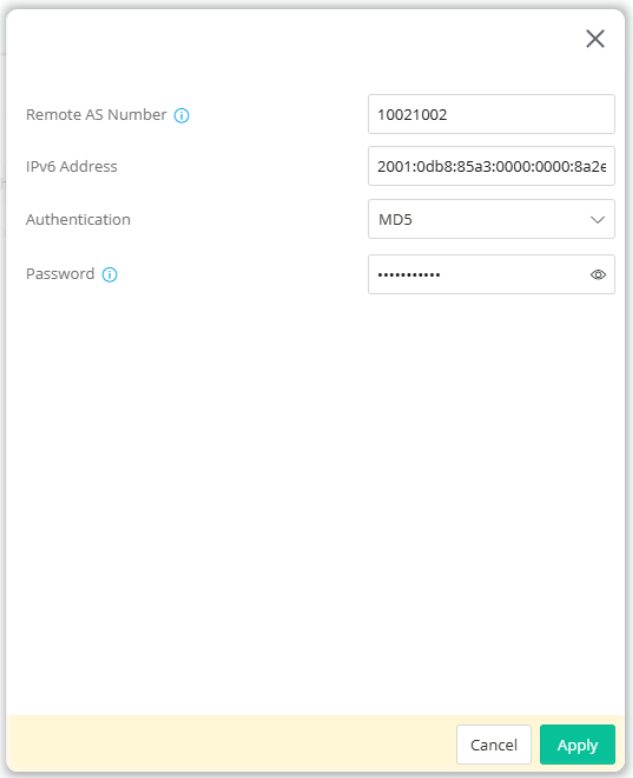
After finishing this web page configuration, please click **Apply** to save the settings.

## II-1-8-4 IPv6 Neighbors

Set general settings for local router and neighboring routers (based on IPv6 address).




To add a new IPv6 neighbors profile, click the **+Add** link to get the following page.



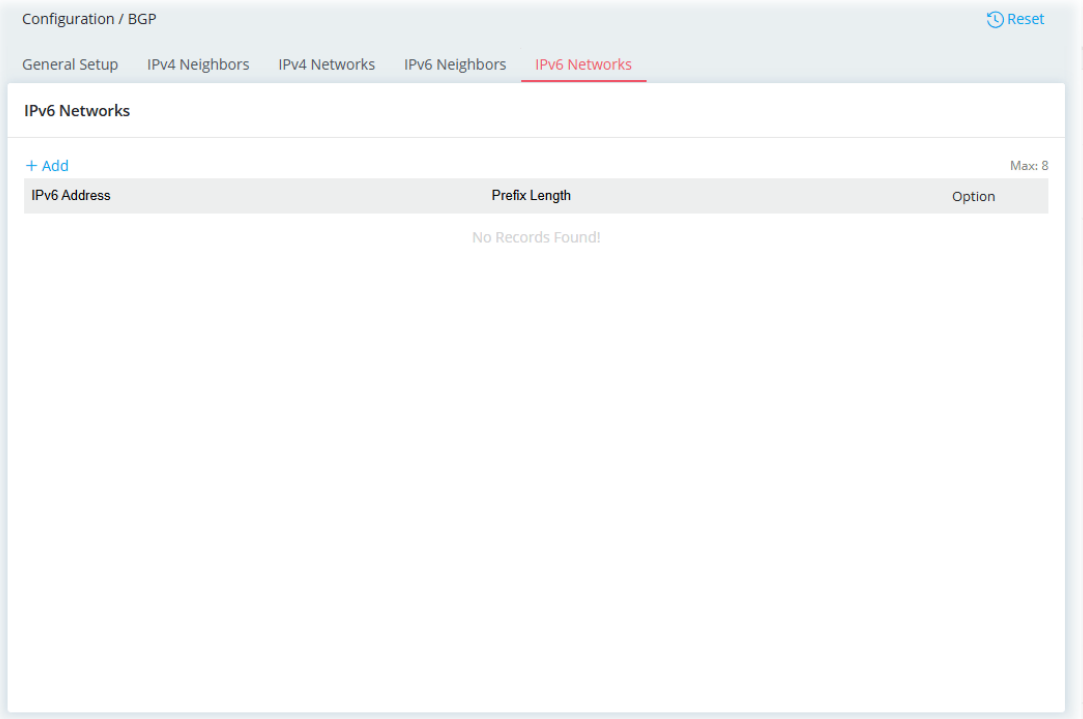

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Remote AS Number** | Specify the AS Number for neighboring router. |
| **IPv6 Address** | Enter the IPv6 address of a neighboring router. |
| **Authentication** | Select the authentication mechanism for this profile.<br>**Disabled** – No authentication mechanism will be used.<br>**MD5** – Use MD5 authentication.<br>• **Password** – Enter characters as the password for MD5 authentication. |
| **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-1-8-5 IPv6 Networks

This page allows you to configure up to eight neighboring networks for exchanging the routing information with the local router (Vigor2136). The IPv6 address defined on this page will be used to declare which network will participate in the RIPng protocol.




To add a new IPv6 networks profile, click the **+Add** link to get the following page.



Available settings are explained as follows:

| Item | Description |
| --- | --- |
| **IPv6 Address** | Enter the IPv6 address of a neighboring network (following CIDR format).<br>Vigor router (e.g., 2136 series) will exchange routing information (RIPng info) with the specified network. |
| **Prefix Length** | Enter the IPv6 prefix length for the IPv6 address. |
| **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-1-9 OSPF

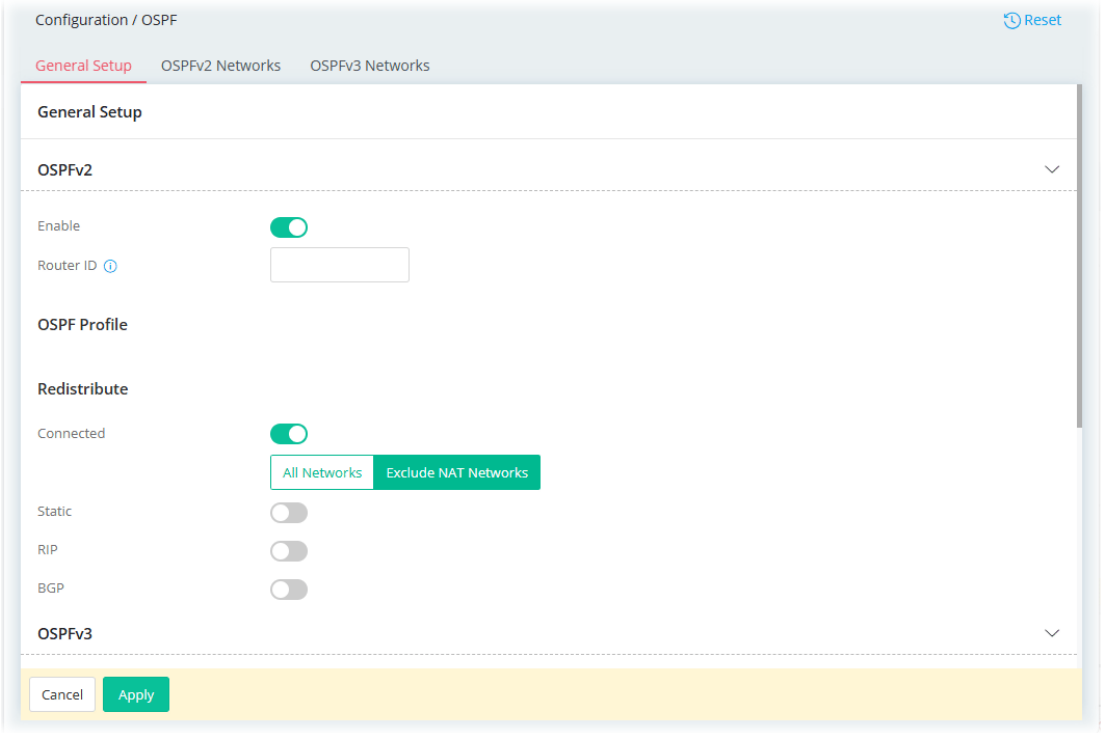
OSPF(Open Shortest Path First), running within the AS, is a routing protocol based on IP protocol. It uses the algorithm of SPF (Shortest Path First) to calculate the route metric. It is suitable for large network and complicated data exchange. Vigor router supports up to OSPF version 2(for IPv4) and OSPF version 3(for IPv6).

The Autonomous System (AS) used in OSPF can be divided into several **areas**. Usually, Area 0 will be used as OSPF backbone which distributing the routing information among areas.

When you need faster convergence than distance vector, want to support much larger networks or want to have less susceptible to bad routing information, you can enable OSPF feature to fit your request. Note that both routers must support OSPF function at the same time to build the OSPF connection.

## II-1-9-1 General Setup

This page allows you to configure general settings for OSPFv2 (IPv4) and/or OSPFv3 (Ipv6) profile.




Available settings are explained as follows:

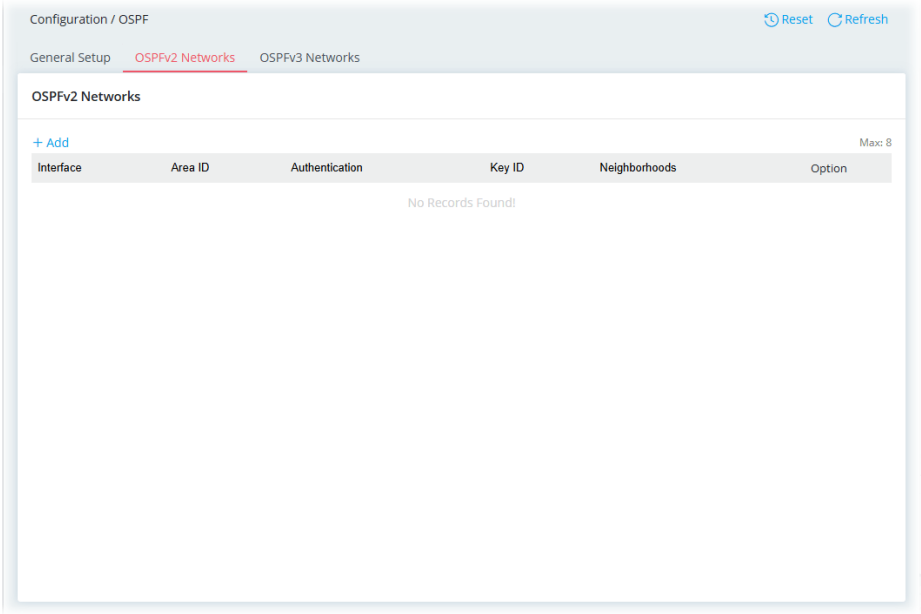
| Item | Description |
|---|---|
| | **General Setup** |
| **Enable** | Switch the toggle to enable/disable the OSPFv2 function. |
| **Router ID** | Specify the IPv4 address of the Vigor router for routing and neighbor discovery.<br>Such ID will help Vigor router to be identified in an autonomous system. However, if no address is specified, then an IP address of the active interface will be used by system automatically. |
| **Connected** | **All Networks** – Apply the OSPF profile to all the LAN interfaces.<br>**Exclude NAT Networks** - Apply the OSPF profile to all the LAN |

| | |
|---|---|
| | interfaces except for NAT network. |
| **Static** | Switch the toggle to apply the static route to the OSPF profile. |
| **RIP** | Switch the toggle to enable (allow dynamically route traffic based on information learned from the RIP protocol) or disable the function. |
| **BGP** | Switch the toggle to enable (allow dynamically route traffic based on information learned from the BGP protocol) or disable the function. |
| | **OSPFv3** |
| **Enable** | Switch the toggle to enable/disable the OSPFv3 function. |
| **Router ID** | Specify the IPv6 address of the Vigor router for routing and neighbor discovery.<br>Such ID will help Vigor router to be identified in an autonomous system. However, if no address is specified, then an IP address of the active interface will be used by system automatically. |
| **Connected** | Switch the toggle to enable (apply the OSPFv3 settings to all the LAN interfaces) or disable the function. |
| **Static** | Switch the toggle to enable (apply the static route to the OSPFv3 profile) or disable the function. |
| **RIP** | Switch the toggle to enable (allow dynamically route traffic based on information learned from the RIP protocol) or disable the function. |
| **BGP** | Switch the toggle to enable (allow dynamically route traffic based on information learned from the BGP protocol) or disable the function. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings and exit the page. |

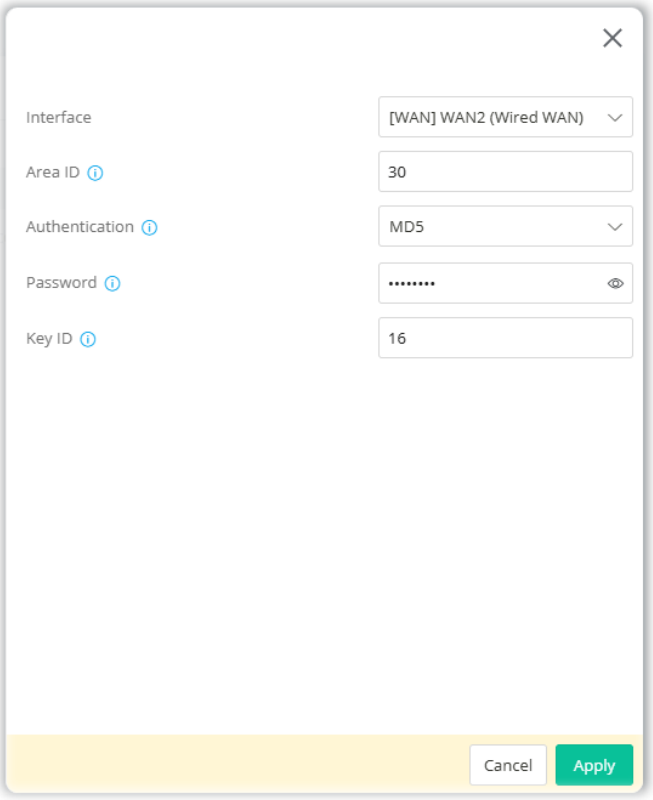
After finishing this web page configuration, please click **Apply** to save the settings.

## II-1-9-2 OSPFv2 Networks

This page allows you to set neighbors (by Area ID) for OSPFv2 profile.




To add a new OSPFv2 networks profile, click the **+Add** link to get the following page.




Available settings are explained as follows:

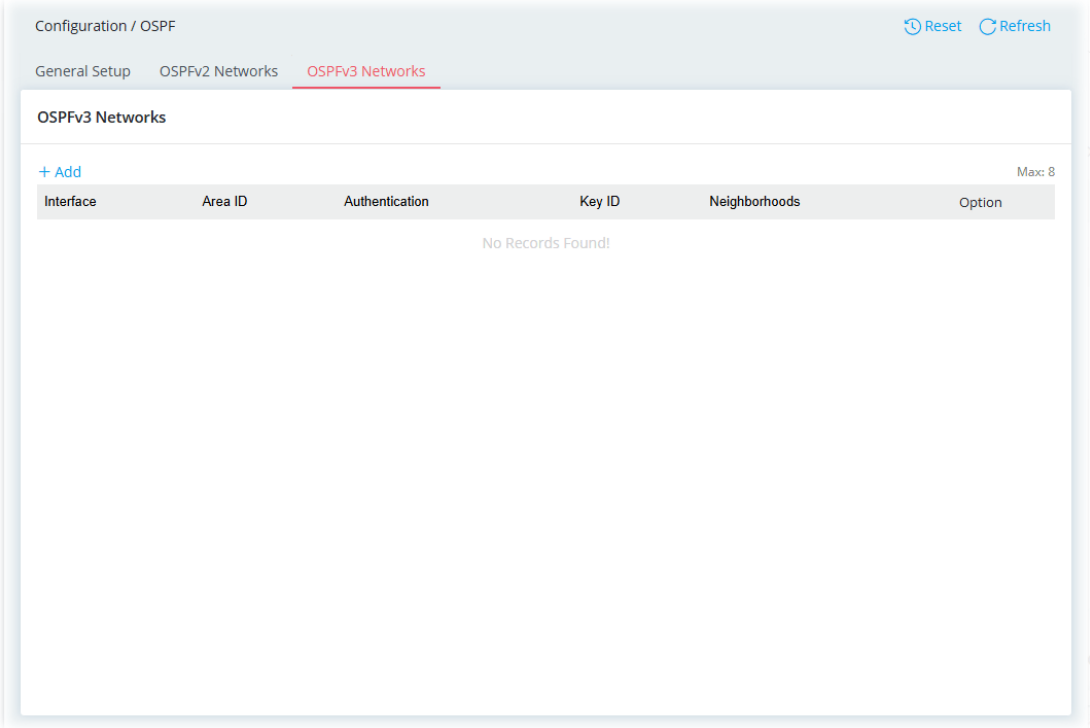
| Item | Description |
|---|---|
| **Interface** | Select a LAN / WAN interface to apply the settings configured for this profile. |

| | |
|---|---|
| Area ID | An AS will be divided into several areas. Each area must be assigned with a dedicated number.<br>Please enter a number or IPv4 address as the area ID. |
| Authentication | Select the authentication mechanism for this profile.<br>**Disabled** – No authentication mechanism will be used.<br>**Plain-Text** – Only password will be used for authentication.<br>• **Password** –Enter characters as the password for MD5 authentication.<br>**MD5** – Use MD5 authentication.<br>• **Password** – Enter characters as the password for MD5 authentication.<br>• **Key ID** – Enter a number (0~255). The ID will help Vigor router to be identified in an autonomous system. |
| Cancel | Discard current settings and return to the previous page. |
| Apply | Save the current settings and exit the page. |

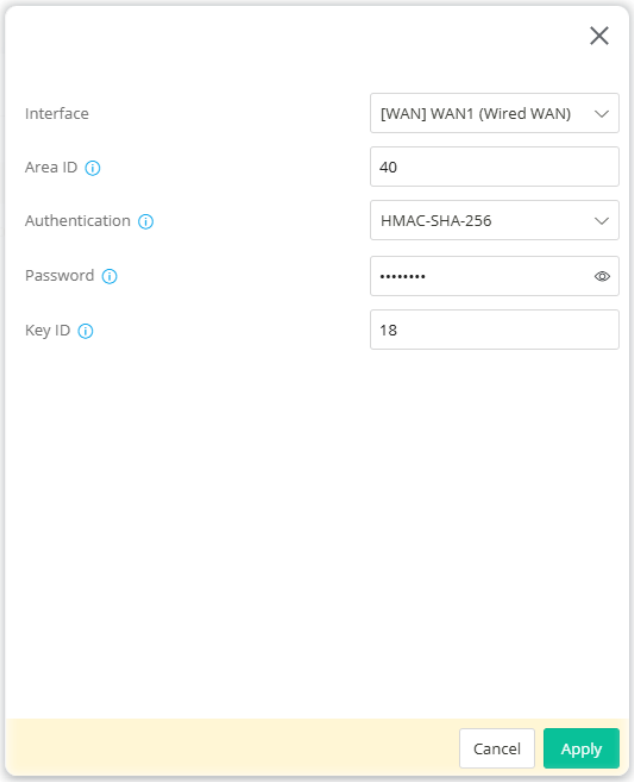
After finishing this web page configuration, please click **Apply** to save the settings.

## II-1-9-3 OSPFv3 Networks

This page allows you to set neighbors for OSPFv3 profile.




To add a new OSPFv3 networks profile, click the **+Add** link to get the following page.




Available settings are explained as follows:

| Item | Description |
|---|---|

| | |
|---|---|
| Interface | Select a LAN / WAN interface to apply the settings configured for this profile. |
| Area ID | An AS will be divided into several areas. Each area must be assigned with a dedicated number.<br>Please enter a number or IPv6 address as the area ID. |
| Authentication | Select the authentication mechanism for this profile.<br>Disabled – No authentication mechanism will be used.<br>Plain-Text – Only password will be used for authentication.<br>• Password –Enter characters as the password for MD5 authentication.<br>MD5 – Use MD5 authentication.<br>• Password – Enter characters as the password for MD5 authentication.<br>• Key ID – Enter a number (0~255). The ID will help Vigor router to be identified in an autonomous system. |
| Cancel | Discard current settings and return to the previous page. |
| Apply | Save the current settings and exit the page. |

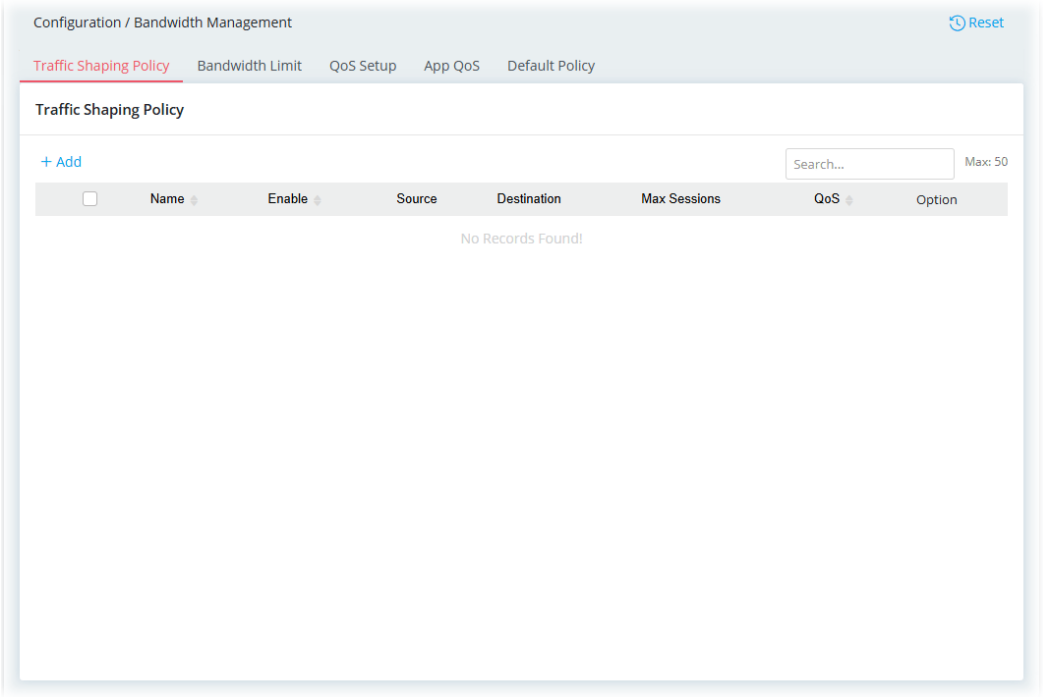
After finishing this web page configuration, please click **Apply** to save the settings.

# II-1-10 Bandwidth Management

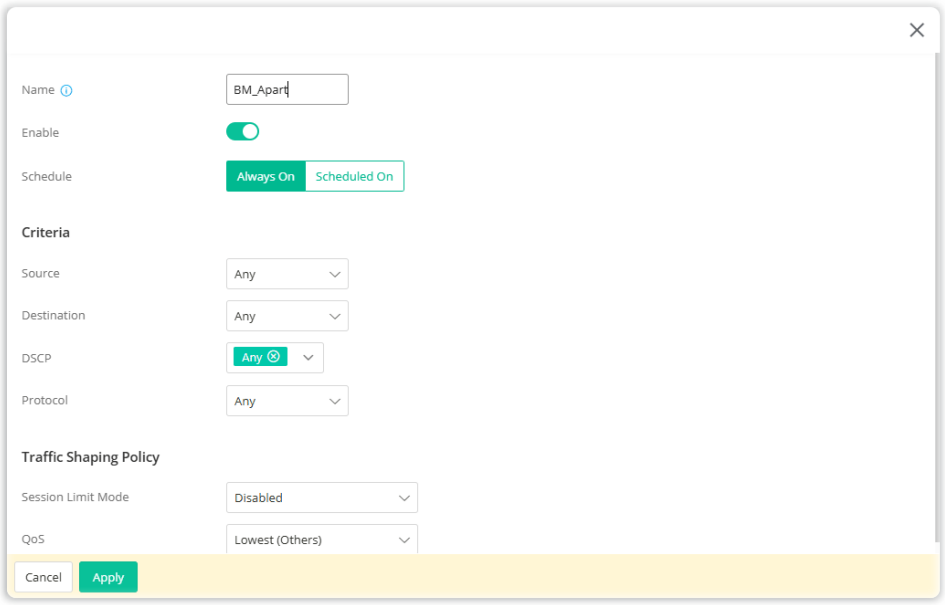
When LAN clients share a common public IP address by means of Network Address Translation (NAT), the router must track NAT sessions so that traffic to and from the WAN can reach the intended destinations. There is an finite number of sessions that can be tracked by the router, and by setting session limits will ensure that the router does not run out of resources. This is especially important when P2P applications are used. P2P applications, such as BitTorrent, that attempt to simultaneously establish connections to as many WAN hosts as possible.

## II-1-10-1 Traffic Shaping Policy

This page allows you to configure the session limits and QoS settings.

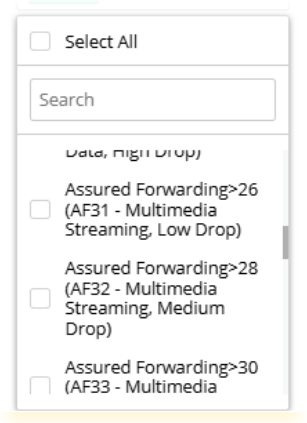


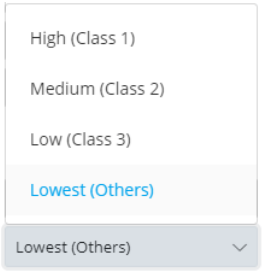

To add a new policy, click the **+Add** link to get the following page.



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Name** | Enter a name for identification. |
| **Enable** | Switch the toggle to enable/disable the traffic shaping policy profile. |
| **Schedule** | Vigor router can perform the traffic shaping policy profile all the time or on a certain date and time.<br>**Always On -** The function of traffic shaping policy profile is running all the time.<br>**Scheduled On -** The function of traffic shaping policy profile is activated based on the schedule profile. |
| **Criteria** | |
| **Source / Destination** | Specify the IP type.<br>Vigor router will restrict the sessions for the IPs by the default policy.<br>• **Any** – If Any is selected, the limitation will applied to any IP.<br>• **IPv4 Address**<br>• **IPv4 Subnet**<br>• **IPv6 Address**<br>• **IPv6 Subnet**<br>• **IP Object**<br>• **IP Group** |
| **Source / Destination IPv4 Address** | It is available when **Source / Destination** is set as **IPv4 Address**.<br>**+Add** – Click to create a new entry.<br>**IPv4 Address Start / End** - Enter an IPv4 address as the starting point. And, enter another IPv4 address as the ending point. |
| **Source / Destination IPv4 Subnet Address** | It is available when **Source / Destination** is set as **IPv4 Subnet**.<br>**+Add** – Click to create a new entry.<br>**IPv4 Address** – Enter an IPv4 address.<br>**Subnet Mask** – Specify the subnet mask for the IPv4 address. |
| **Source / Destination IPv6 Address** | It is available when **Source / Destination** is set as **IPv6 Address**.<br>**+Add** – Click to create a new entry.<br>**IPv6 Address Start / End** - Enter an IPv6 address as the starting point. And, enter another IPv6 address as the ending point. |
| **Source / Destination IPv6 Subnet Address** | It is available when **Source / Destination** is set as **IPv6 Subnet**.<br>**+Add** – Click to create a new entry.<br>**IPv6 Address** – Enter an IPv6 address.<br>**Prefix Length** – Set the prefix length for the IPv6 address. |
| **Source / Destination IP Object** | It is available when **Source / Destination** is set as **IP Object**.<br>**+Add** – Up to 12 objects can be specified here.<br>**Select Object** – Select the object(s) from the available object list on the right side. |
| **Source / Destination IP Group** | It is available when **Source / Destination** is set as **IP Group**.<br>**+Add** – Up to 12 groups can be specified here.<br>**Select Group** - Select the object(s) from the available group list on |

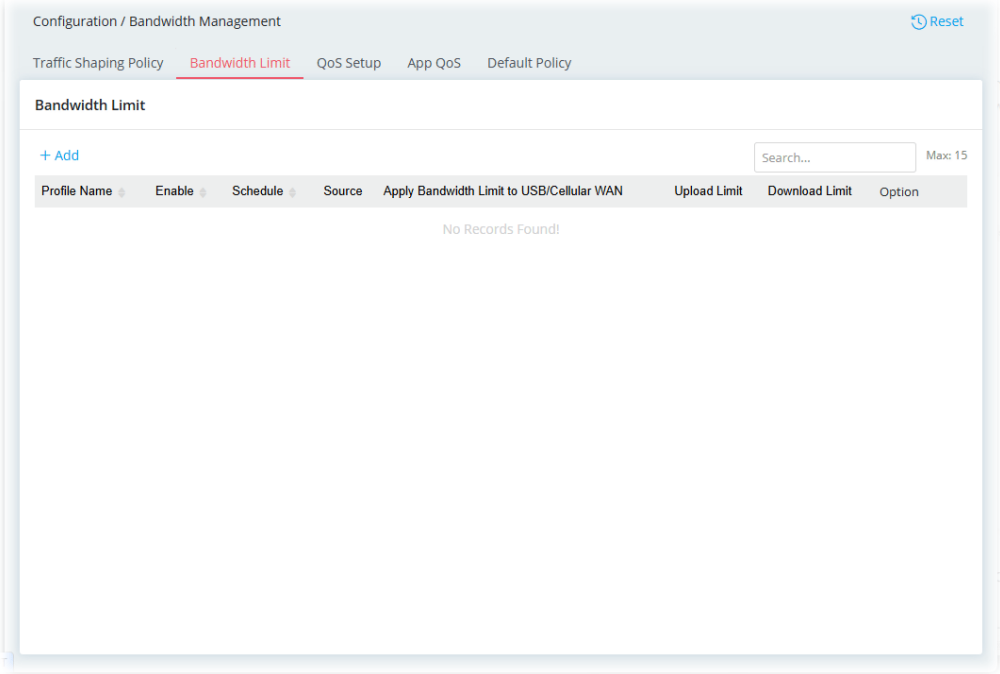
| | |
|---|---|
| | the right side. |
| DSCP | It displays the levels of the data for processing with QoS control.<br>Select DSCP or ToS precedence of packets to which this rule applies.<br> |
| Protocol | Only the traffic passing through the selected protocol will be limited.<br>Select one of the protocols from the drop-down menu.<br>**Any** – All traffic will be limited.<br>**Service Type Object** – Vigor system offers several service types set with different protocols.<br>• **Service Type Object** – Click +**Add** to create a new object. Up to 12 objects can be created.<br>**TCP/UDP** – Select Transmission Control Protocol/User Datagram Protocol.<br>• **Specify Source Port** – Switch the toggle to enable the setting of Source Port.<br>• **Source Port / Destination Port** – Set the port range (1 to 65535).<br>**TCP** – Transmission Control Protocol. Setting method is the same as TCP/UDP.<br>**UDP** – User Datagram Protocol. Setting method is the same as TCP/UDP. |
| | Traffic Shaping Policy |
| Session Limit Mode | **Disabled** – Select to deactivate session limit function.<br>**Per Source IP Limit** – Apply the session limit to the traffic.<br>• **Max Sessions** - The default maximum number of sessions allowed per LAN client, unless overridden by specifying a different number in the Limitation List. |
| QoS | Select the class level (Class 1, Class 2, Class 3 and others) of bandwidth which will be applied to this profile. |

| | |
|---|---|
| |  |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings and exit the page. |

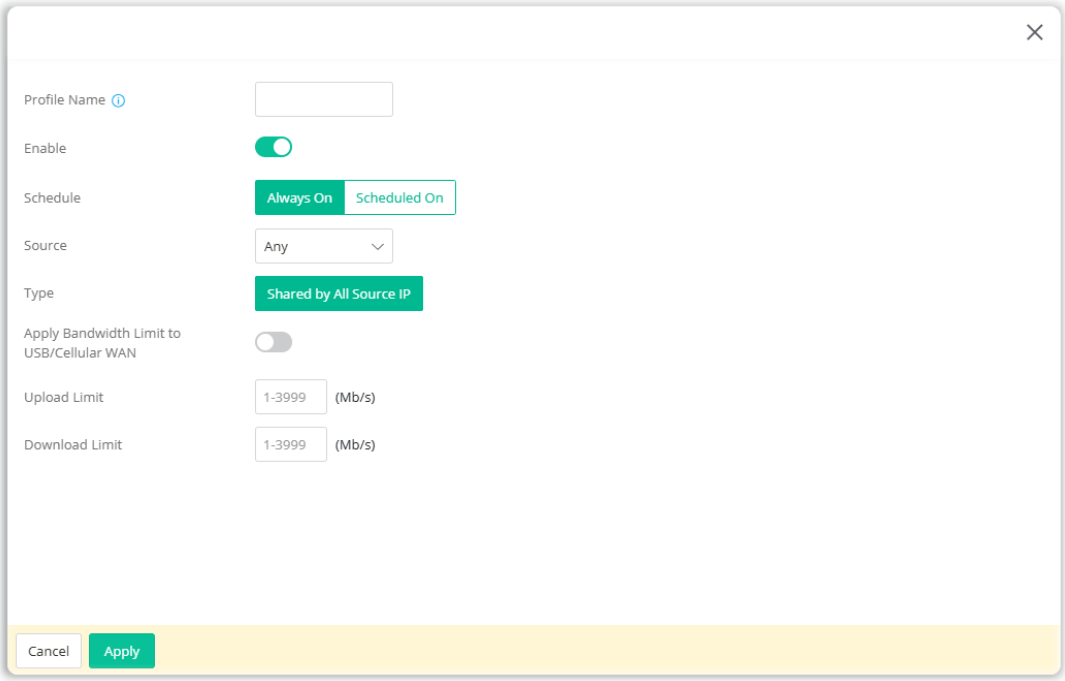
After finishing this web page configuration, please click **Apply** to save the settings.

## II-1-10-2 Bandwidth Limit

Bandwidth Limit ensures LAN clients get their fair share of network bandwidth by placing restrictions on upstream and downstream network speeds.




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




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Profile Name** | Enter a string as the profile name. |
| **Enable** | Switch the toggle to enable/disable this profile of bandwidth limit. |
| **Schedule** | Vigor router can perform the bandwidth limit all the time or on a certain date and time.<br>**Always On -** The function of bandwidth limit is running all the time.<br>**Scheduled On -** The function of bandwidth limit is activated based on the schedule profile. |
| **Source** | Identify the object to which the bandwidth limit will be applied.<br>● **Any -** All the IPs within the range defined will be restricted by bandwidth limit defined by TX Limit and RX Limit below.<br>● **IPv4 Address**<br>● **IPv4 Subnet**<br>● **IP Object**<br>● **IP Group** |
| **Source IPv4 Address** | It is available when IPv4 Address is selected as the Source.<br>Click **+Add** to add a new entry.<br>● **IPv4 Address Start -** The beginning IP address for this limit entry.<br>● **IPv4 Address End -** The ending IP address for limit entry. |
| **Source IPv4 Subnet Address** | It is available when IPv4 Subnet is selected as the Source.<br>Click **+Add** to add a new entry.<br>● **IPv4 Address -** Specify Start IP Address.<br>● **Subnet Mask -** Select a Subnet Mask. |
| **Source IP Object** | It is available when IP Object is selected as the Source.<br>All the IPs specified by the selected IP object will be restricted by bandwidth limit defined by TX Limit and RX Limit below.<br>Click on **+Add** to open the IP object table. Select the IP object(s) |

| | |
|---|---|
| | and click Close. A new entry will be added immediately. |
| **Source IP Group** | It is available when IP Group is selected as the Source.<br>All the IPs specified by the selected IP group will be restricted by bandwidth limit defined by TX Limit and RX Limit below.<br>Click on **+Add** to open the IP Group table. Select the IP group(s) and click Close. A new entry will be added immediately. |
| **Type** | **Shared by All Source IP** - The upload and download limits will be distributed evenly among all selected source IPv4 addresses, source IPv4 subnet addresses, source IP objects, or source groups. |
| **Apply Bandwidth Limit to USB/Cellular WAN** | Switch the toggle to enable/disable the feature.<br>The upload limit and the download limit will be applied to the USB WAN/Cellular WAN interface. |
| **Upload Limit – USB Mode** | It is available if **Apply Bandwidth Limit to USB/Cellular WAN** is enabled.<br>Set the upstream speed limit for USB WAN/Cellular WAN interface.<br>Value must be between 1 and 50 (Mb). |
| **Download Limit - USB Mode** | It is available if **Apply Bandwidth Limit to USB/Cellular WAN** is enabled.<br>Set the downstream speed limit for USB WAN/ Cellular WAN interface.<br>Value must be between 1 and 50 (Mb). |
| **Upload Limit** | Upstream speed limit for each LAN client. Value must be between 1 and 3999 (Mbps). |
| **Download Limit** | Downstream speed limit for each LAN client. Value must be between 1 and 3999 (Mbps). |
| **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.

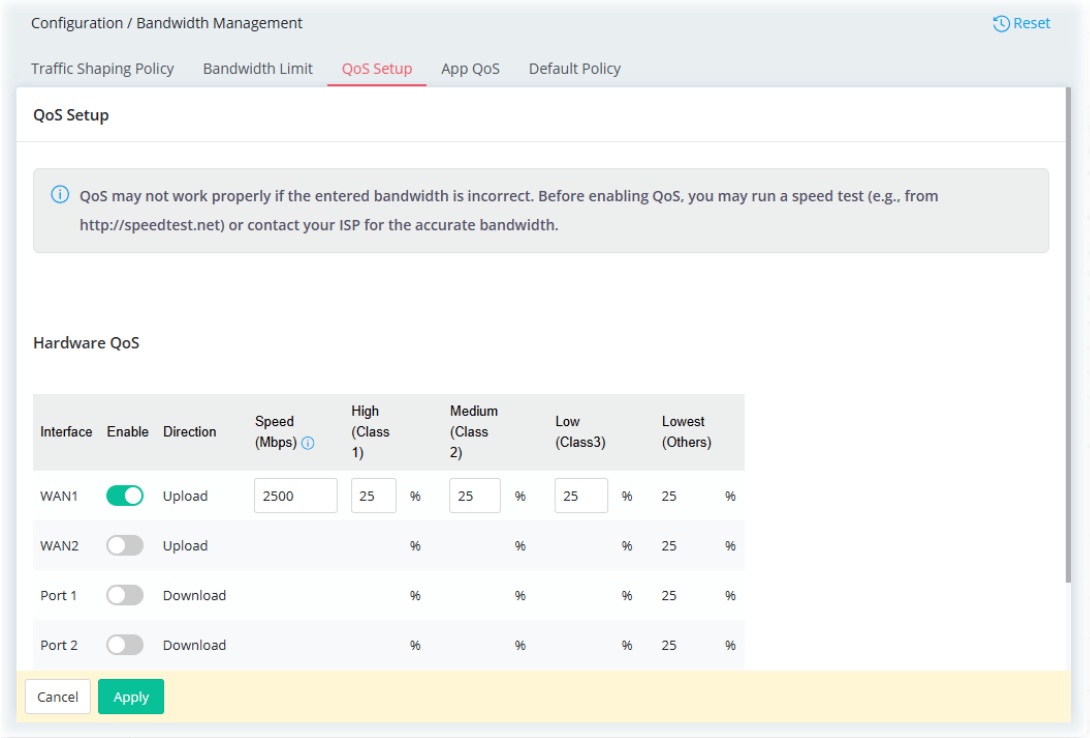
## II-1-10-3 QoS Setup

QoS (Quality of Service) ensures that all LAN clients receive their fair share of bandwidth that is required for applications to function properly and efficiently.

Without QoS, it is possible that certain applications may consume excessive network resources that they degrade performance of more important applications, especially ones that are less tolerant of jitter (delay variation) or lost or delayed packets. Additionally, at times of network congestion, QoS is able to prioritize different types of traffic according to their predefined priority, thus ensuring traffic of higher importance gets processed first.

A typical QoS deployment consists of two components:

- Classification: Identifying low-latency or crucial applications and marking them for high-priority service level enforcement throughout the network.
- Scheduling: Prioritizing packets by assigning them to different queues and service types according to service levels.



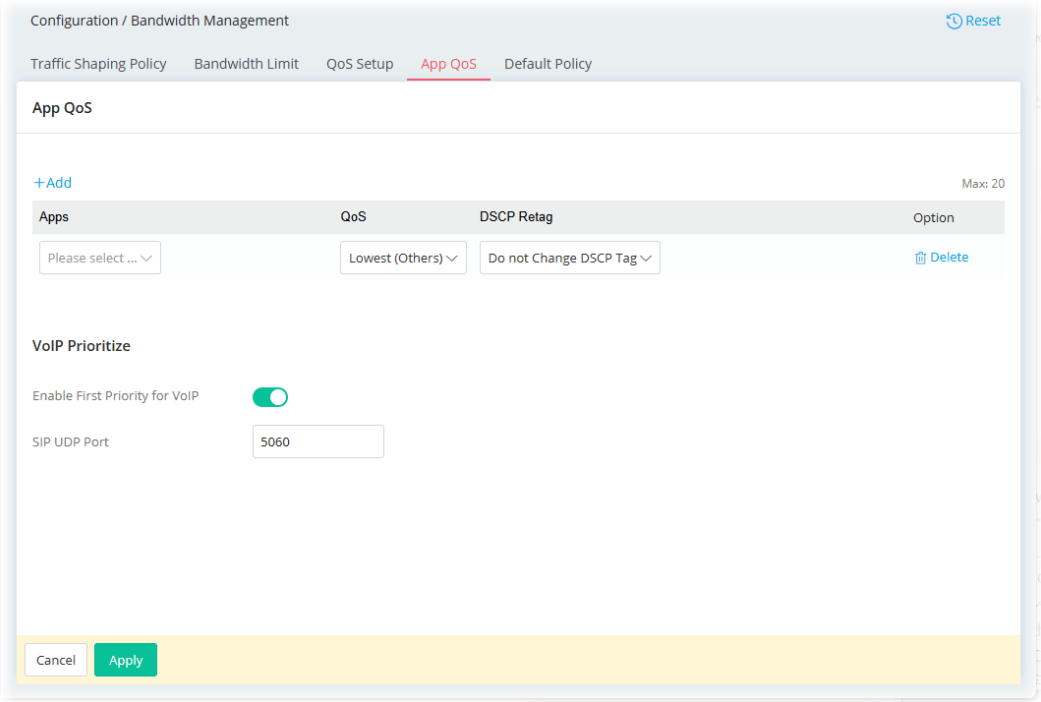

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Switch the toggle to enable/disable the WAN interface settings. |
| **Direction** | At present, only Upload (for outgoing traffic) is available. |
| **Speed(Mbps)** | Set the outbound bandwidth (default is 2500) of the WAN/LAN. |
| **High(Class 1)** | Set the percentage of bandwidth (upload speed) reserved for class 1. |
| **Medium(Class 2)** | Set the percentage of bandwidth (upload speed) reserved for class 2. |
| **Low(Class 3)** | Set the percentage of bandwidth (upload speed) reserved for class 3. |
| **Lowest(Others)** | Set the percentage of bandwidth (upload speed) reserved for others. |
| **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-1-10-4 APP QoS

APP QoS allows QoS to be applied to select protocols and applications.



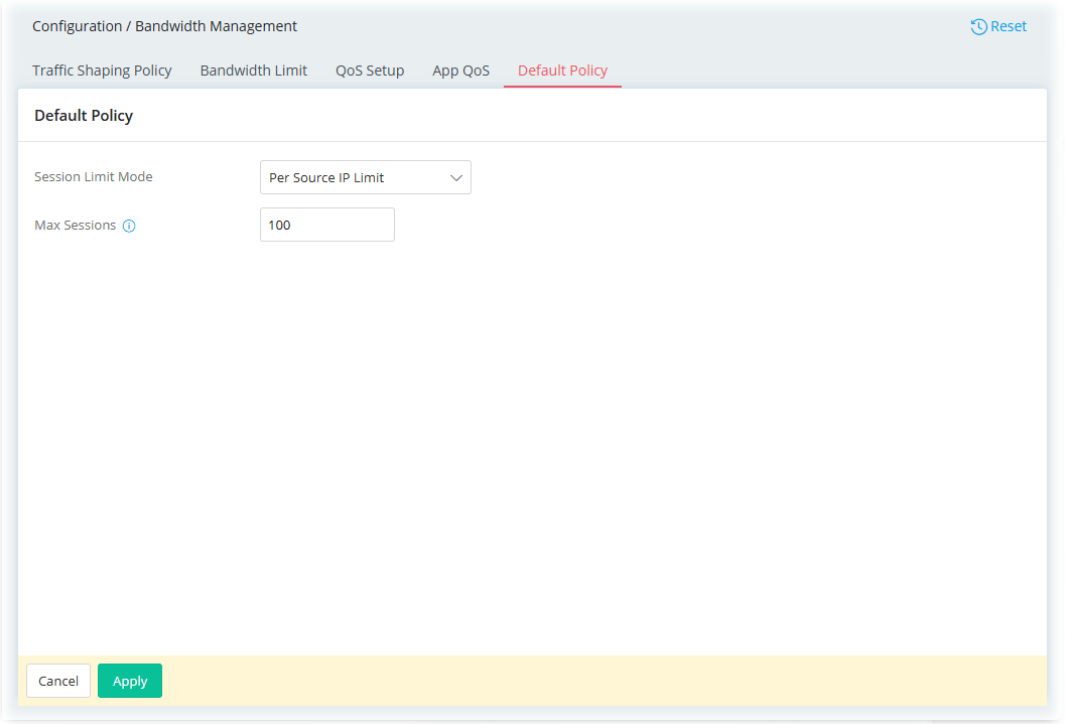

Available settings are explained as follows:

| Item | Description |
|---|---|
| +Add | **Apps** – The drop-down menu displays various APPEs. Select the one you want.<br>**QoS** – Select the class level (Class 1, Class 2, Class 3 and others) of bandwidth reserved for the Apps.<br>**DSCP Retag** – Select the level of the data for processing with QoS control.<br>**Delete** – Click to remove the selected entry. |
| VoIP Prioritize | |
| Enable First Priority for VoIP | Switch the toggle to enable/disable the function.<br>If enabled, it allows VoIP traffic to receive the highest priority. |
| SIP UDP Port | Enter a port number to be monitored for SIP traffic. |
| 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-1-10-5 Default Policy

Default policy defines the bandwidth limit and the session limit for all traffic in default.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Session Limit Mode** | **Disabled** – Select to deactivate session limit function.<br>**Per Source IP Limit** –Apply the session limit to the traffic.<br>• **Max Sessions** - The default maximum number of sessions allowed per LAN client, unless overridden by specifying a different number in the Limitation List. |
| **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-1-11 NAT

Most ISPs allocate one WAN IP address to each subscriber. In order to simultaneously connect multiple devices to the Internet, a technique called Network Address Translation is employed.

Usually, the router serves as an NAT (Network Address Translation) router. NAT is a mechanism that one or more private IP addresses can be mapped into a single public one. Public IP address is usually assigned by your ISP, for which you may get charged. Private IP addresses are recognized only among internal hosts.

When the outgoing packets destined to some public server on the Internet reach the NAT router, the router will change its source address into the public IP address of the router, select the available public port, and then forward it. At the same time, the router shall list an entry in a table to memorize this address/port-mapping relationship. When the public server response, the incoming traffic, of course, is destined to the router's public IP address and the router will do the inversion based on its table. Therefore, the internal host can communicate with external host smoothly.

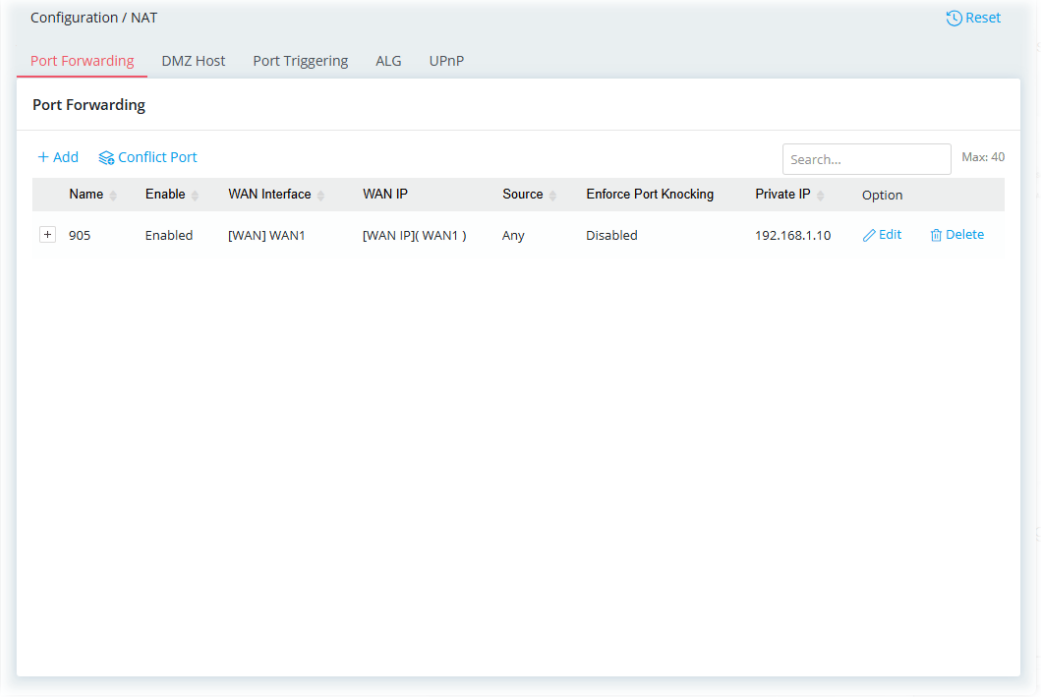
The benefit of the NAT includes:

- **Save cost on applying public IP address and apply efficient usage of IP address.** NAT allows the internal IP addresses of local hosts to be translated into one public IP address, thus you can have only one IP address on behalf of the entire internal hosts.
- **Enhance security of the internal network by obscuring the IP address.** There are many attacks aiming victims based on the IP address. Since the attacker cannot be aware of any private IP addresses, the NAT function can protect the internal network.

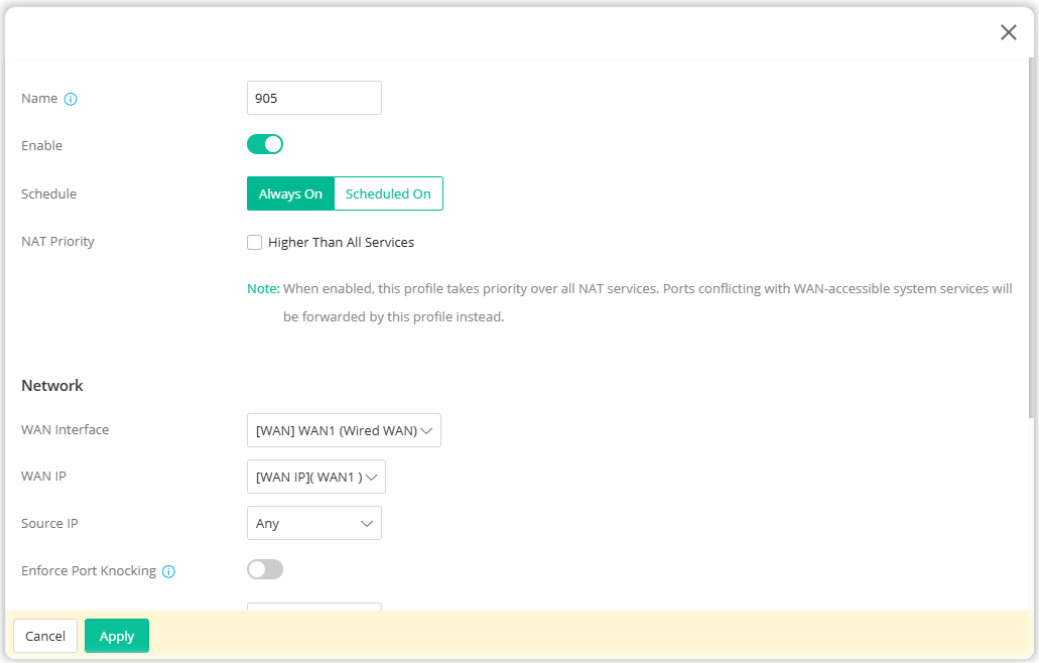
### II-1-11-1 Port Forwarding

This function allows inbound traffic from specific ports on WAN interfaces to be forwarded to LAN clients.

It allows you to open a range of ports for the traffic of special applications.

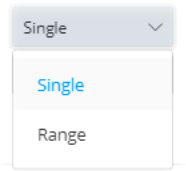



To add a new forwarding policy, click the **+Add** link to get the following page.

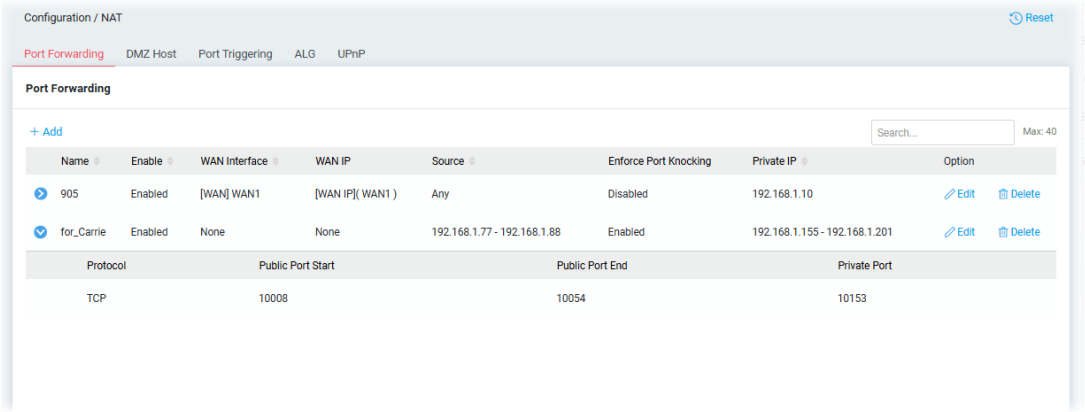



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Name** | Enter a name that identifies the rule. |
| **Enable** | Switch the toggle to enable or disable the function. |
| **Schedule** | Vigor router can perform the port forwarding all the time or on a certain date and time.<br>**Always On -** The function of port triggering is running all the time.<br>**Scheduled On -** The function of port triggering is activated based on the schedule profile. |
| **NAT Priority** | **Higher Than All Services** –By default, local services take priority over port forwarding rules. If both use the same port (e.g., port 443), port forwarding may not work.<br>Enable this option to prioritize this profile over all NAT services, including WAN-accessible system services that use the same port. |
| **Network** | |
| **WAN Interface** | The WAN port(s) whose incoming traffic will be forwarded to a LAN client. Select from a specific WAN interface WAN# to apply the rule to the WAN interface. |
| **WAN IP** | Select a WAN IP to match WAN interface. |
| **Source IP** | **Any** – Any data traffic coming from the source IP will be forwarded to a LAN.<br>• **Enforce Port Knocking** - Switch the toggle to enable/disable the Port Knocking function.<br>**IP Address** – Set a range of IP addresses. Any data traffic coming from the IP addresses within the range will be forwarded to a LAN.<br>**IP Object** – The data traffic coming from IPs within the IP objects will be forwarded to a LAN client.<br>• **+Add** – Click to specify an IP object profile. |

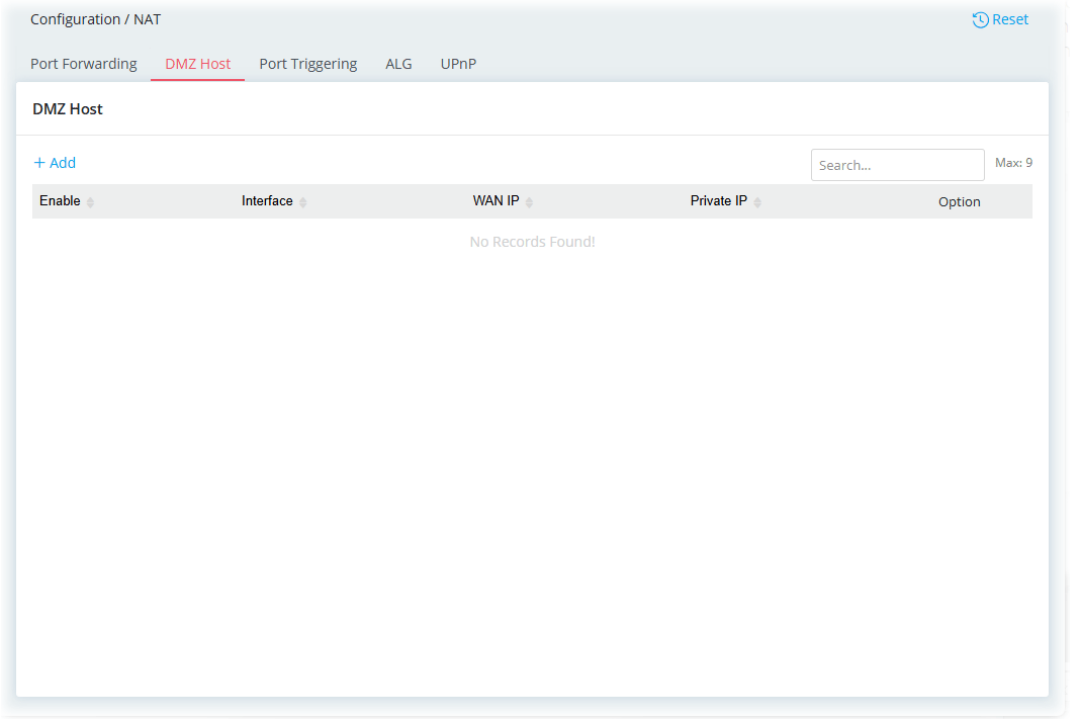
| | |
|---|---|
| | **IP Group** – The data traffic coming from IP objects within the IP groups will be forwarded to a LAN client.<br>• **+Add** – Click to specify an IP group profile.<br>**Host Name** – The data traffic coming from the host will be forwarded to a LAN client.<br>• **Hostname** – Enter the name of the host. |
| **Private IP** | Specify a LAN IP address or a range of LAN IP addresses to which the traffic will be forwarded.<br><br>**Single** – Specify a destination LAN IP address that will receive the forwarded traffic.<br>**Range** – Specify a range of destination LAN IP addresses that will receive the forwarded traffic. |
| | **Port Forwarding** |
| **+Add** | Click to set port numbers for the specified protocol (TCP, UDP, or TCP/UDP) for a port forwarding profile. |
| **Protocol** | The protocol to which this rule applies, TCP, UDP or TCP/UDP. |
| **Public Port Start** | Specify which port can be redirected to the specified **Private IP** and **Port** of the internal host. Enter the required number as the starting port. |
| **Public Port End** | Enter the required number as the ending port. |
| **Private Port Start** | The port on each LAN client to which the traffic will be directed to. Enter the required number as the starting port. |
| **Private Port End** | Enter the required number as the ending port. |
| **Option** | Click **Delete** to remove the selected entry. |
| **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.

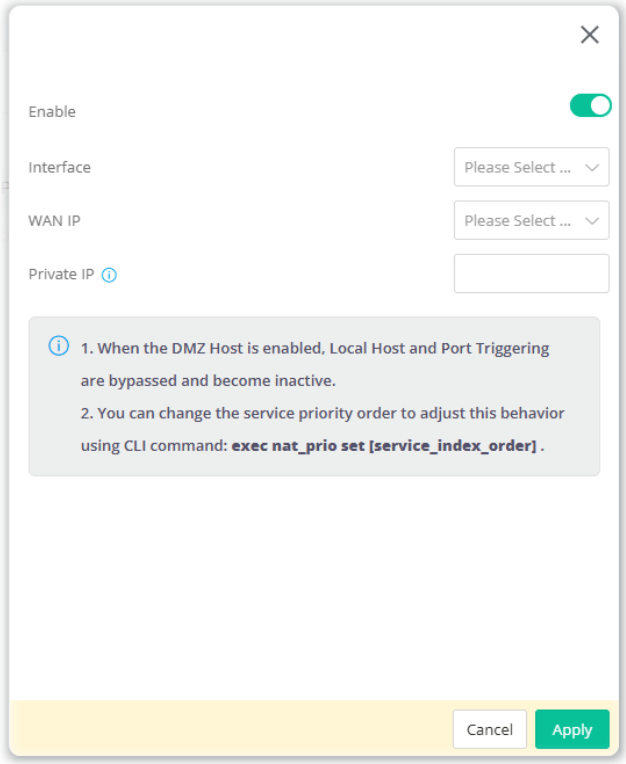


## II-1-11-2 DMZ Host

Vigor router provides a facility **DMZ Host** that maps ALL unsolicited data on any protocol to a single host in the LAN. Regular web surfing and other such Internet activities from other clients will continue to work without inappropriate interruption. **DMZ Host** allows a defined internal user to be totally exposed to the Internet, which usually helps some special applications such as Netmeeting or Internet Games etc.




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



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Switch the toggle to enable or disable the function. |
| **Interface** | Allows WAN traffic to be sent to a specific LAN IP address. |
| **WAN IP** | Enable the function of applying WAN alias IP. Then, select a WAN alias IP from the available IPv4 alias settings set on Configuration >> WAN >> WAN Connections. |
| **Private IP** | Enter an IP address to be the DMZ host. |
| **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-1-11-3 Port Triggering

If you run programs that function as server applications where they expect to receive unsolicited traffic from the WAN, you can set up rules in Port Triggering to detect LAN-to-WAN traffic initiated by those programs, and automatically open up WAN ports to accept incoming traffic and forward it to the LAN client running the server applications.

The duration that these ports are opened depends on the type of protocol used. The "default" values are shown below and these duration values can be modified via telnet commands.

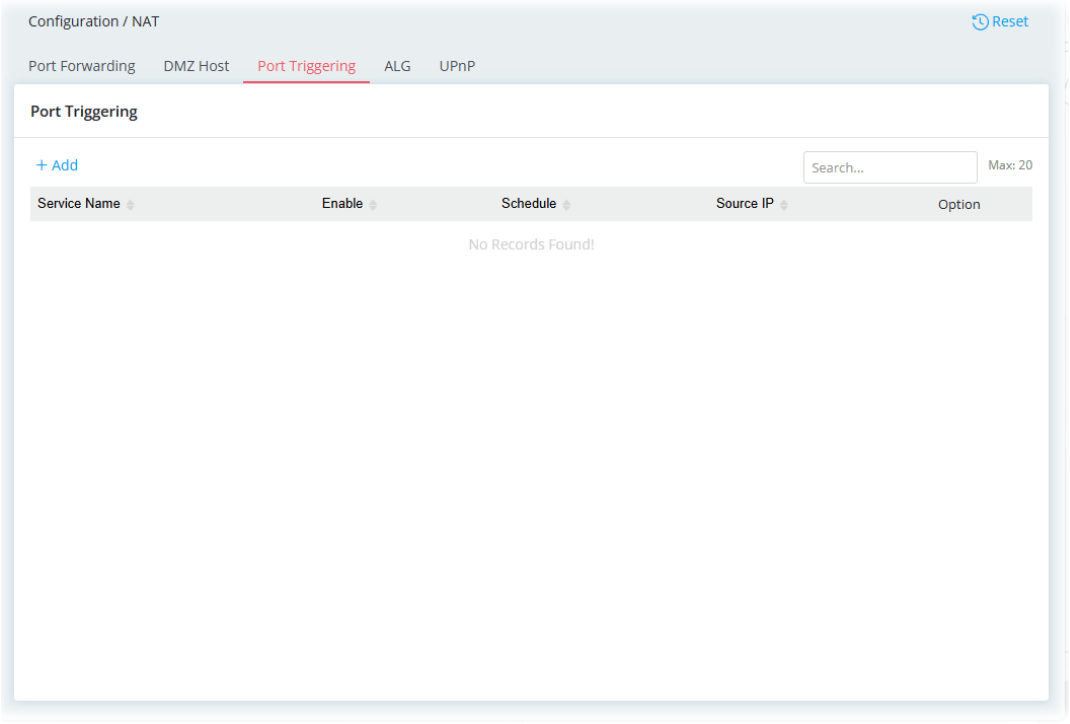
TCP: 86400 sec.

UDP: 180 sec.

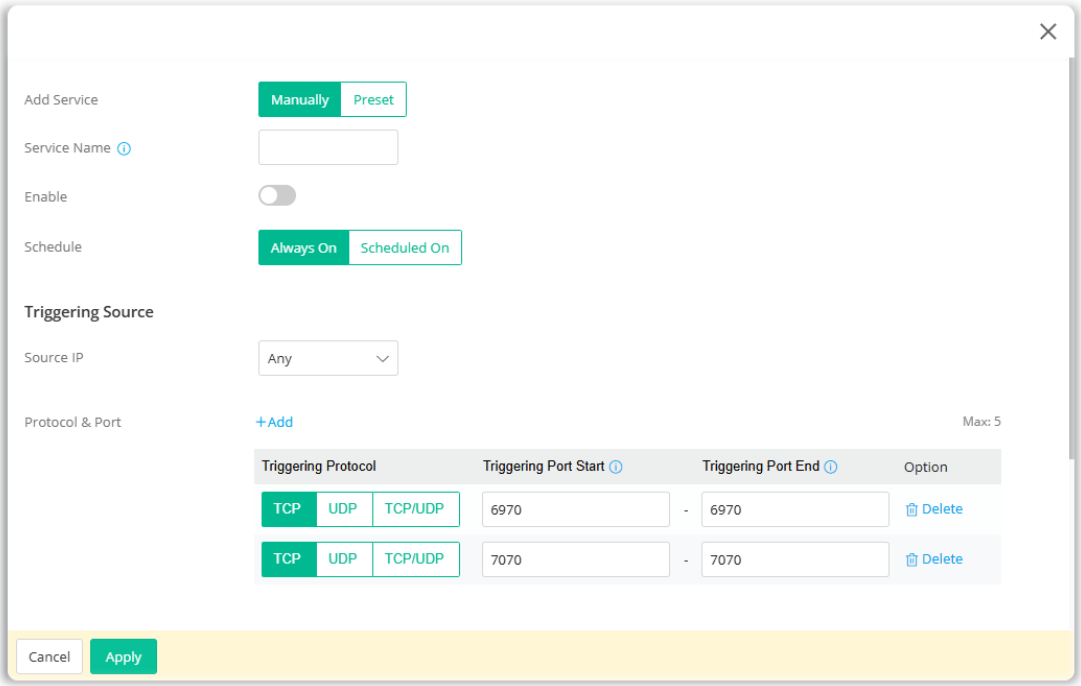
IGMP: 10 sec.

TCP WWW: 60 sec.

TCP SYN: 60 sec.



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




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Add Service** | Select from list of predefined service, or manually configure triggering and incoming protocols and ports.<br>**Manually -** If selected, self-define the service name.<br>• **Service Name** – Enter the name of the service.<br>**Preset -** If selected, various services will be offered for you to choose as the service name.<br>• **Service Name** – Use the drop-down list to specify one service. |
| **Enable** | Switch the toggle to enable or disable the function of port triggering. |
| **Schedule** | Vigor router can perform the port triggering all the time or on a certain date and time.<br>**Always On -** The function of port triggering is running all the time.<br>**Scheduled On -** The function of port triggering is activated based on the selected schedule profile. |
| **Triggering Source** | |
| **Source IP** | **Any -** Any source IP will be forwarded to a LAN.<br>**IP Address** - Set a range of IP addresses forwarded to a LAN.<br>• **IP Address** – Enter the IP address and the subnet mask.<br>**IP Object** – Click **+Add** to specify the IP object profile (up to 12 profiles).<br>**IP Group** - Click **+Add** to specify the IP group profile (up to 12 profiles). |
| **Protocol & Port** | **+Add** - Click to set the port numbers (start and end) for the specified protocol (TCP, UDP or TCP/UDP) for the outgoing data (that this rule monitors).<br>**Triggering Protocol -** The protocol(s) of the outgoing traffic. |

| | |
|---|---|
| | • **TCP** - open port(s) to TCP traffic.<br>• **UDP** - open port(s) to UDP traffic.<br>• **TCP/UDP** - open port(s) to both TCP and UDP traffic.<br>Select the protocol (TCP, UDP or TCP/UDP) for the outgoing data of such triggering profile.<br>**Triggering Port Start / Triggering Port End** - Outgoing traffic from the WAN destined for these port numbers be forwarded to the LAN client that triggered the rule.<br>Enter the port or port range for the outgoing packets. |
| Incoming Services | |
| **Protocol & Port** | **+Add -** Click to set port numbers (start and end) for the specified protocol (TCP, UDP or TCP/UDP) for the incoming data.<br>**Incoming Protocol -** The protocol(s) of the incoming traffic.<br>• **TCP** - open port(s) to TCP traffic.<br>• **UDP** - open port(s) to UDP traffic.<br>• **TCP/UDP** - open port(s) to both TCP and UDP traffic.<br>Select the protocol (TCP, UDP or TCP/UDP) for the incoming data of such triggering profile.<br>**Incoming Port Start / Incoming Port End** - Incoming traffic from the WAN destined for these port numbers be forwarded to the LAN client that triggered the rule.<br>Enter the port or port range for the incoming packets. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings and exit the page. |

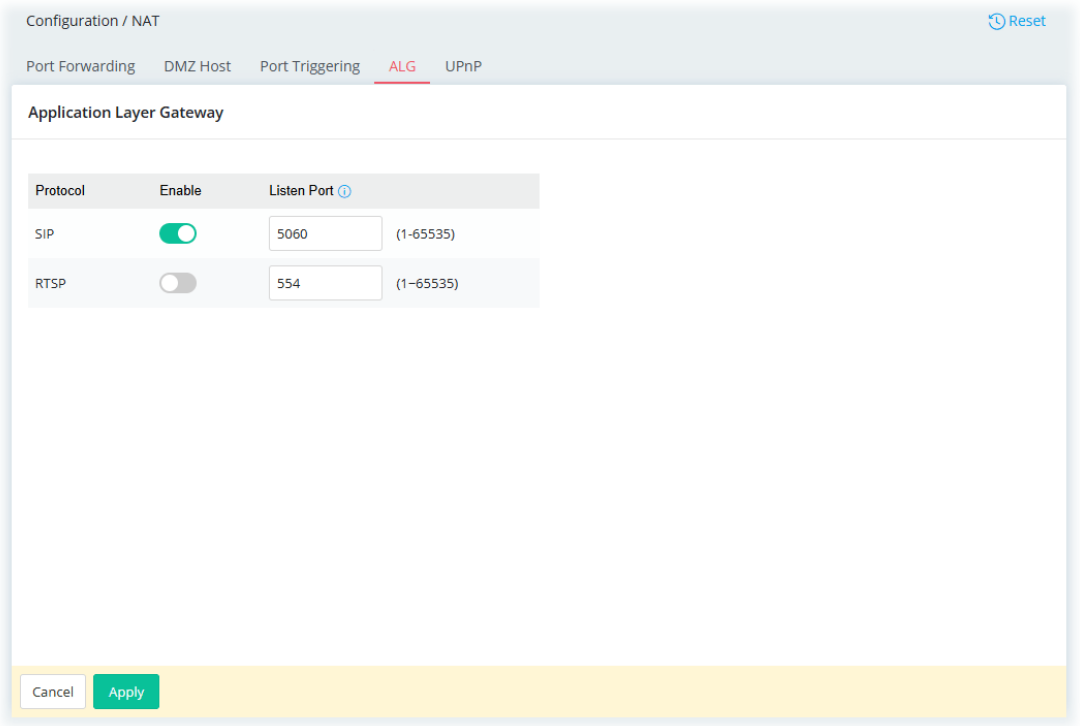
After finishing this web page configuration, please click **Apply** to save the settings.

## II-1-11-4 ALG

ALG means **Application Layer Gateway**. There are two methods provided by Vigor router, RTSP (Real Time Streaming Protocol) ALG and SIP (Session Initiation Protocol) ALG, for processing the packets of the voice and the video.

RTSP ALG makes RTSP message, RTCP message, and RTP packets of voice and video be transmitted and received correctly via NAT by Vigor router.

However, SIP ALG makes SIP message and RTP packets of voice be transmitted and received correctly via NAT by Vigor router.




Available settings are explained as follows:

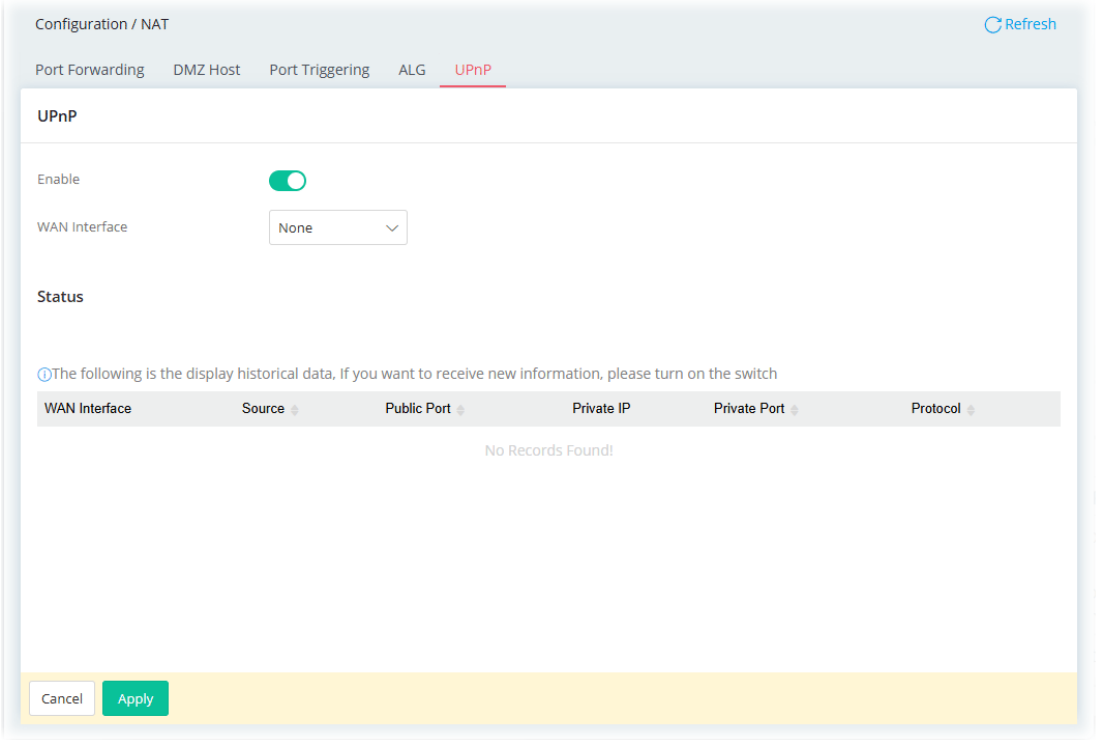
| Item | Description |
|---|---|
| **Enable** | Switch the toggle to enable or disable the function. |
| **Listen Port** | Enter a port number for SIP or RTSP protocol. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings and exit the page. |

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

## II-1-11-5 UPnP

The Vigor supports UPnP (Universal Plug and Play), which is a suite of network protocols that simplifies network configuration. Applications and network devices on the LAN, that support UPnP, may request the router to modify its settings to allow NAT Traversal, so that WAN hosts can connect to them directly.

Examples of applications and devices that support UPnP include file-sharing applications such as uTorrent, Vuze and eMule, gaming consoles such as the Sony PlayStations 3 and 4 Xbox 360 and Xbox One, media streaming applications such as Plex and XBMC, and messaging and calling applications such as Skype. To find out if a certain application or network device supports or requires UPnP, please consult its user manual or check with its vendor.




Available settings are explained as follows:

| Item | Description |
|---|---|
| | **UPnP** |
| **Enable** | Switch the toggle to enable or disable the function.<br>UPnP is required for some applications such as PPS, Skype, eMule...and etc. If you are not familiar with UPnP, it is suggested to turn off this function for security. |
| **WAN Interface** | Select the WAN port on which ports will be opened in response to UPnP commands. |
| **Status** | Displays the historical data. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings and exit the page. |

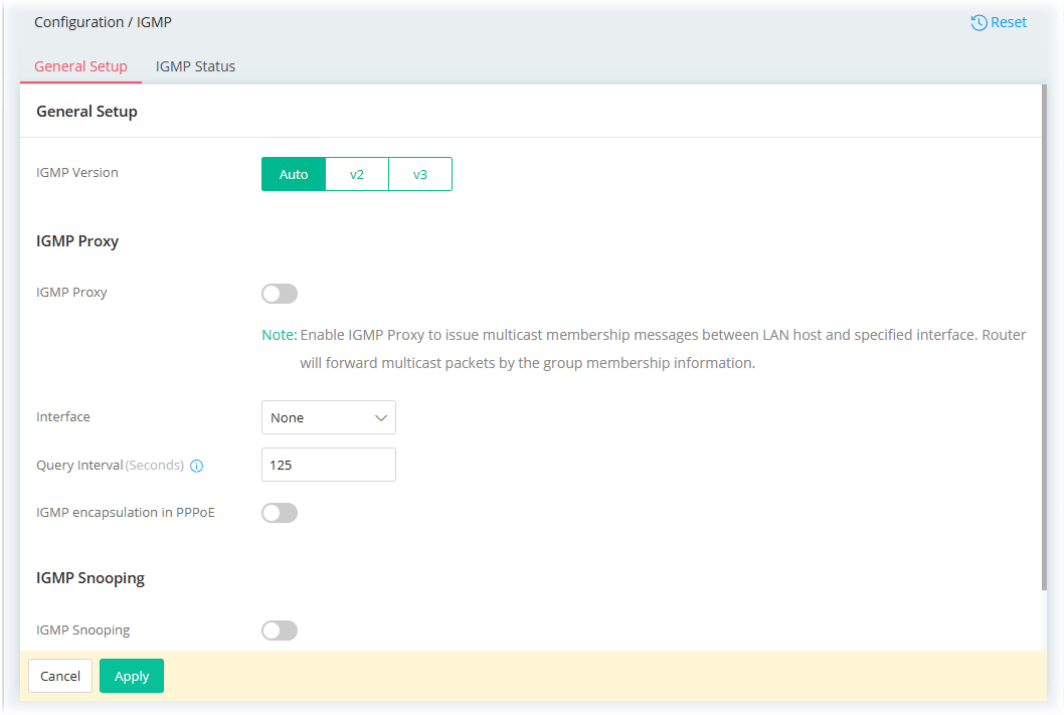
After finishing this web page configuration, please click **Apply** to save the settings.

## II-1-12 IGMP

Internet Group Management Protocol (IGMP) is an IPv4 communication protocol for establishing multicast group memberships.

## II-1-12-1 General Setup

This page offers the general setting for configuring the IGMP function.




Available settings are explained as follows:

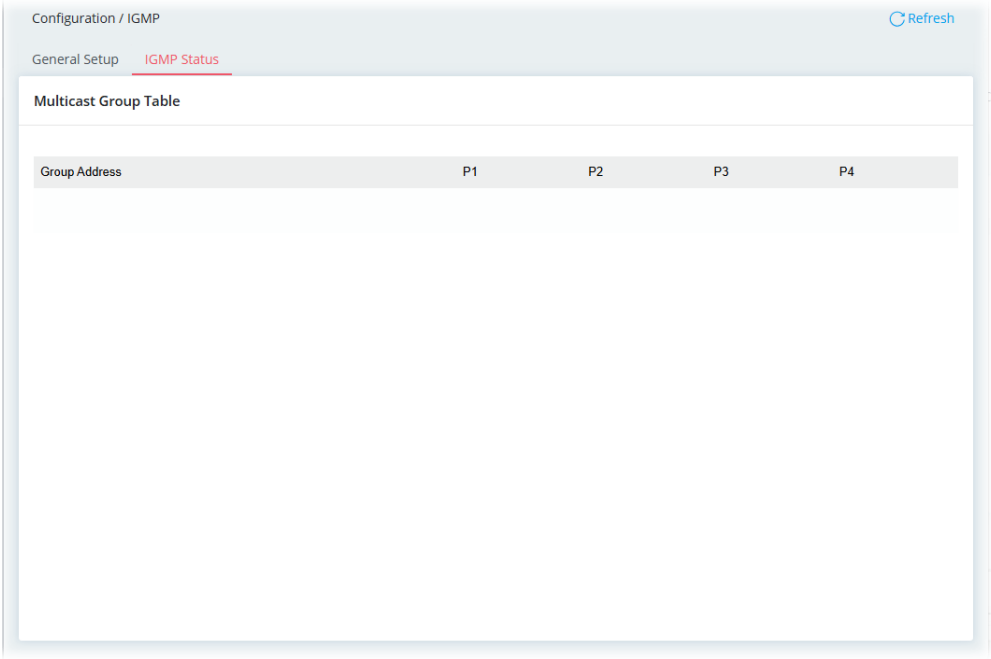
| Item | Description |
|---|---|
| **IGMP Version** | Select v2 or v3 or Auto. At present, two versions (v2 and v3) are supported by Vigor router. Choose the correct version based on the IPTV service you subscribe. |
| **IGMP Proxy** | |
| **IGMP Proxy** | Switch the toggle to enable or disable the function.<br>The application of multicast will be executed through WAN /PVC/VLAN port. In addition, such function is available in NAT mode. |
| **Interface** | Specify an interface for packets passing through. |
| **Query Interval** | Vigor router will periodically check which IP obtaining IPTV service by sending query. It might cause inconvenience for client. Therefore, set a suitable time (unit: second) as the query interval to limit the frequency of query sent by Vigor router. |
| **IGMP encapsulation in PPPoE** | It depends on the specifications regulated by each ISP. If you have no idea to enable or disable, simply contact your ISP providers. |
| **IGMP Snooping** | |
| **IGMP Snooping** | Select to enable IGMP Snooping so that multicast traffic will be forwarded to IGMP clients that have joined a multicast group. |
| **IGMP Fast Leave** | This option is shown only when IGMP Snooping is enabled. Select to enable IGMP Fast Leave. |

| | |
|---|---|
| | Normally when the router receives a "leave" message from an IGMP host, it will send a last member query message to see if there are still members within the multicast group. When Fast Leave is enabled, multicast for a group is immediately terminated when the last host in that group sends a "leave" message. |
| **IGMP Accept List** | Only the device with the IP address specified here is able to process the multicast traffic through the IGMP proxy.<br>**Any** – All IP addresses are allowed for using the IGMP proxy.<br>**IP Object** – Select the IP object(s). The data traffic through those IPs within the object will be processed through the IGMP proxy.<br>**IP Group** - Select the IP group(s). The data traffic through those objects within the group will be processed through the IGMP proxy. |
| **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-1-12-2 IGMP Status

This page displays a list of active multicast groups.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Group Address** | Address of the multicast group, which is within the IP range reserved for IGMP, 224.0.0.0 through 239.255.255.254. |
| **P1 to P4** | LAN ports that have IGMP hosts joined to this multicast group. |

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

# II-1-13 Objects

Vigor router system provides the object functions.

Users can define various types of objects and groups, and then apply them at various scenarios, like Configuration>>NAT>> Port Forwarding, Security>>Firewall Filters.

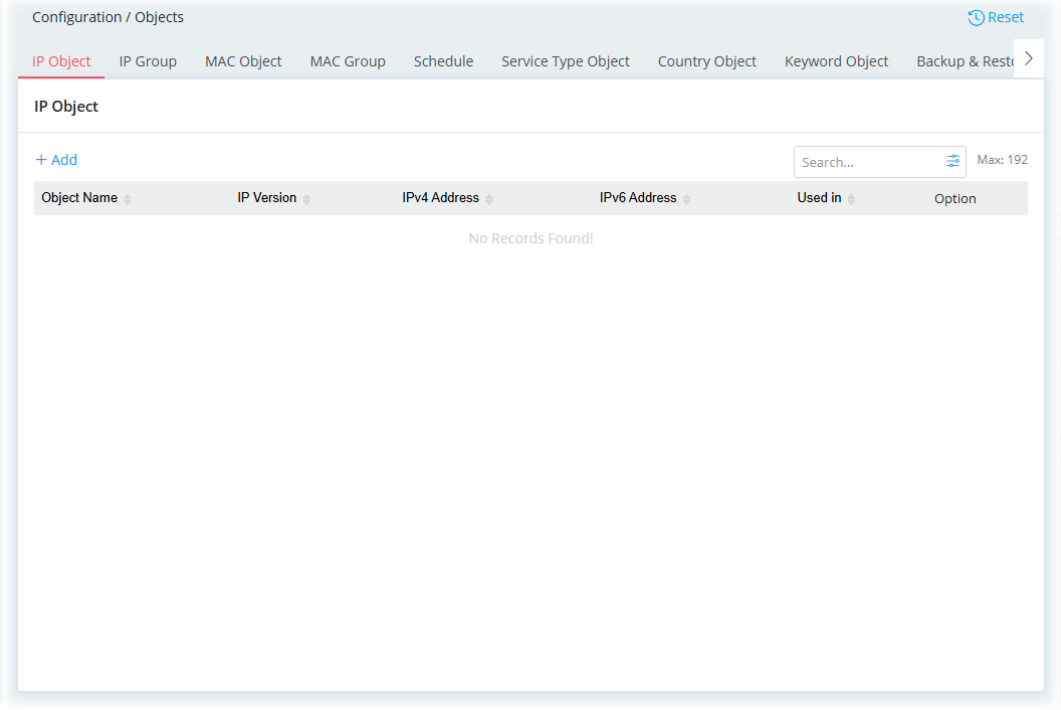
The advantage is that the user doesn't have to set data repetitively and it significantly enhances efficiency.

Currently, the objects that can be preset include IP, MAC, Schedule, Service Type, Keyword, and groups that include IP, MAC, etc.

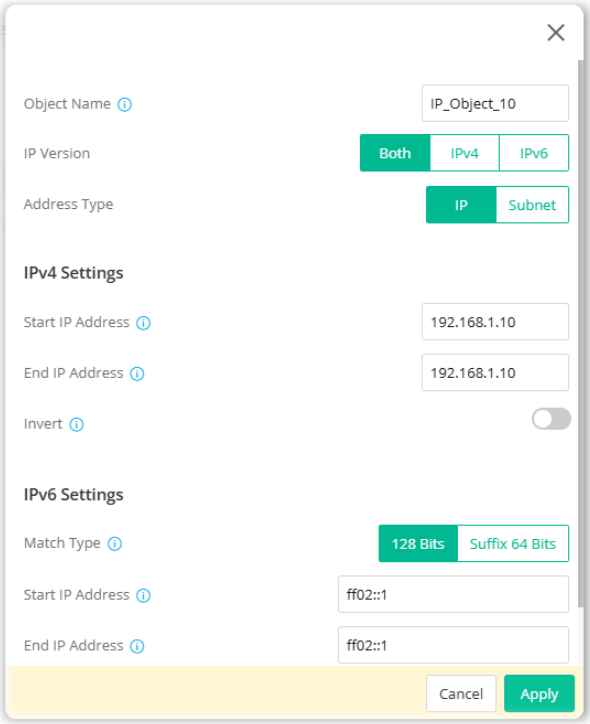
## II-1-13-1 IP Object

For IPs in a range and service ports in a limited range usually will be applied in configuring router's settings, therefore we can define them with ***objects*** and bind the objects with ***groups*** for using conveniently. Later, we can select that object/group for applying it.

For example, a range of IP address in the same department can be defined with an IP object.




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




Available settings are explained as follows:

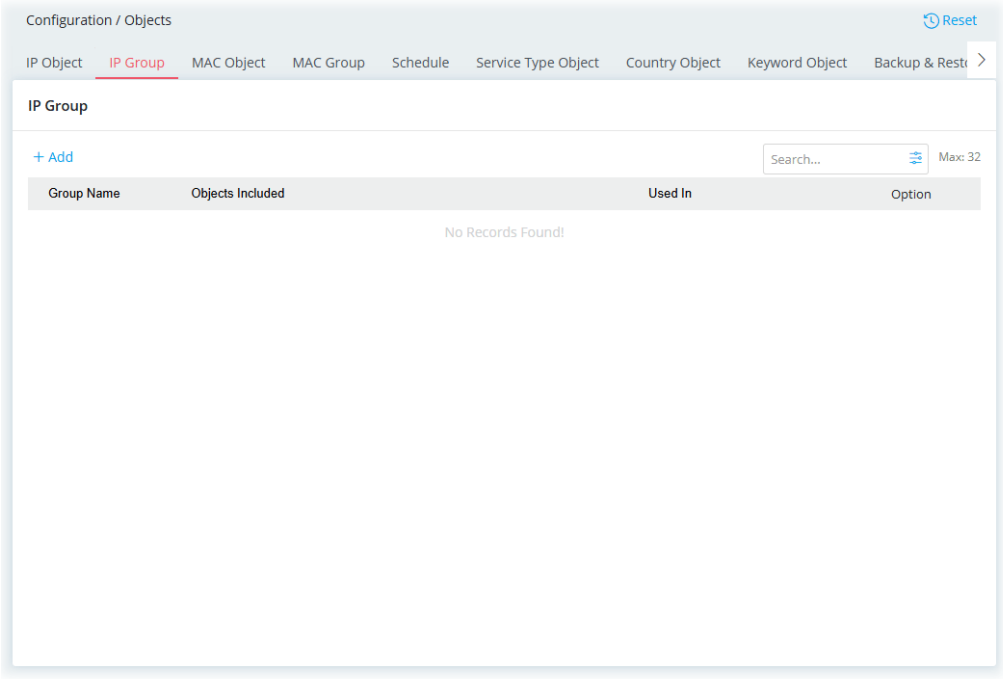
| Item | Description |
|---|---|
| **Object Name** | Enter the name that identifies this profile. |
| **IP Version** | Select the IP version (IPv4, IPv6 or Both) for entering correct IP address. |
| **Address Type** | Select the type (IP or Subnet) of address. |
| | **IPv4 Settings** |
| **Start IP Address** | Enter the beginning IP address, if the Address Type is IP.<br>To set a range of IP addresses, enter the different IP addresses as start IP address and end IP address. |
| **End IP Address** | Enter the ending IP address, if Address Type is IP. |
| **IP Address** | Enter an IP address if Address Type is Subnet. |
| **Subnet Mask** | Enter subnet mask, if Address Type is Subnet. |
| **Invert** | If enabled, all addresses except the ones entered above will be used. |
| | **IPv6 Settings** |
| **Match Type** | Specify the match type (128 Bits or Suffix 64 Bits) for the IPv6 address. |
| **Start IP Address** | Enter the beginning IPv6 address, if the Address Type is IP. To set a range of IP addresses, enter the different IP addresses as start IP address and end IPv6 address. |
| **End IP Address** | Enter the ending IPv6 address, if Address Type is IP. |
| **IP Address** | Enter an IPv6 address if Address Type is Subnet. |
| **Prefix Length** | Enter IPv6 prefix length, if Address type is Subnet. |
| **Invert** | If enabled, all addresses except the ones entered above will be |

| | |
|---|---|
| | used. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings and exit the page. |

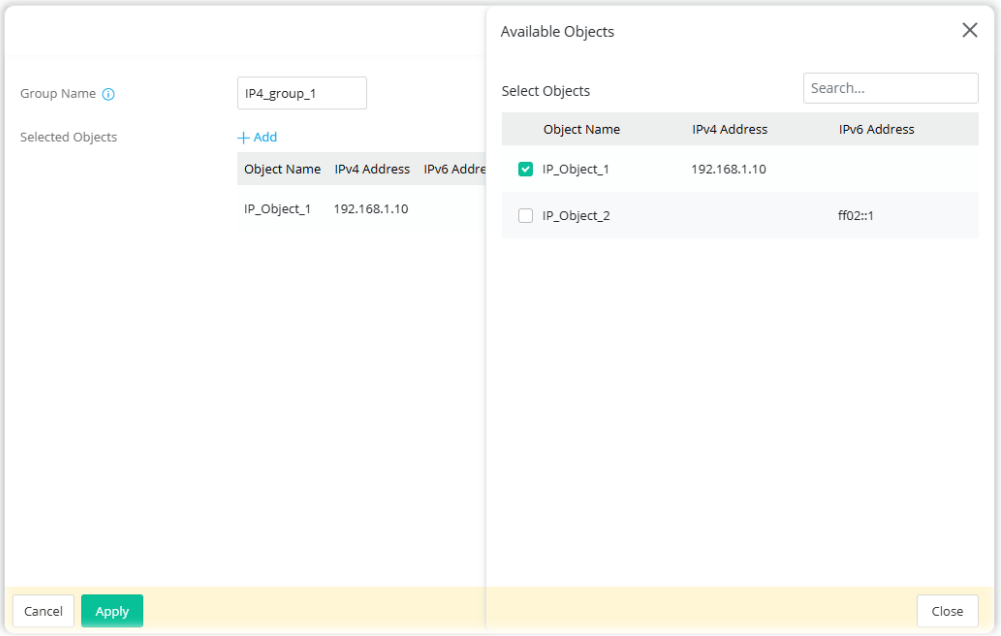
After finishing this web page configuration, please click **Apply** to save the settings.

## II-1-13-2 IP Group

Multiple **IPv4 Objects /IPv6 Objects** can be placed into an **IPv4 Group / IPv6 Group**.




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




Available settings are explained as follows:

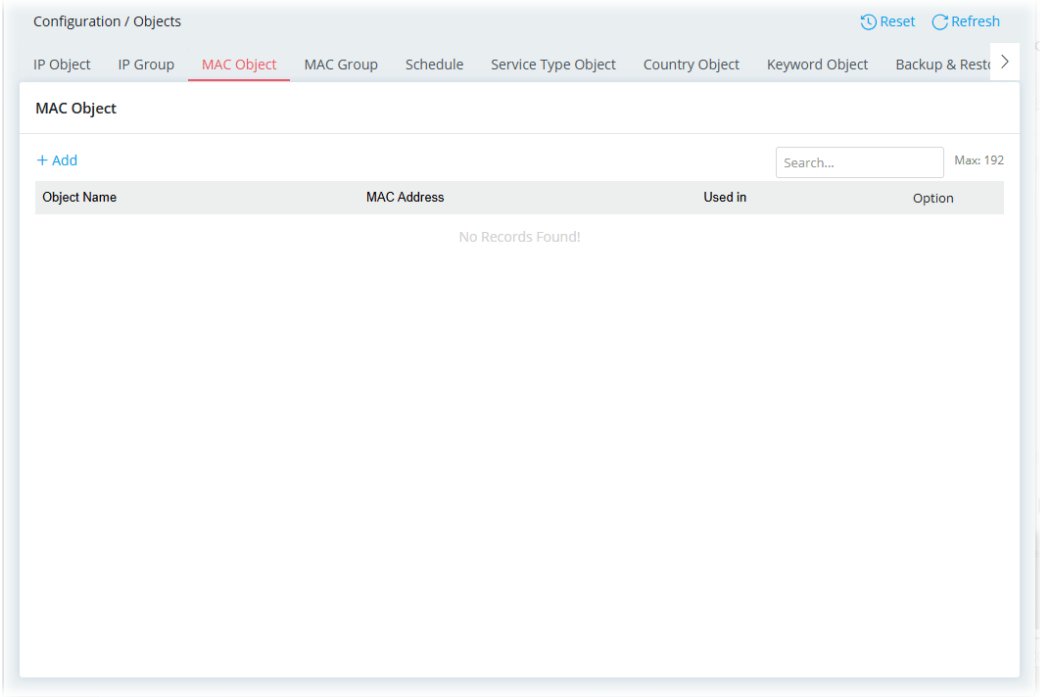
| Item | Description |
|---|---|

| | |
|---|---|
| **Group Name** | Enter a name that identifies this profile. |
| **Selected Objects** | **+Add -** Click to open the page with available objects. |
| **Available Object** | |
| **Search** | Enter the IP object name or the IPv4/IPv6 Address to search related IP object(s). |
| **Selected Objects** | Objects available for grouping will be displayed here. Select one or more objects to group under the current IP group. |
| **Object Name** | Display current existed IPv4/IPv6 object(s).<br>To add an IP object to the current IP group, simply select the object(s) you want. The selected items will then appear under the Selected Objects section on the left side. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings and exit the page. |

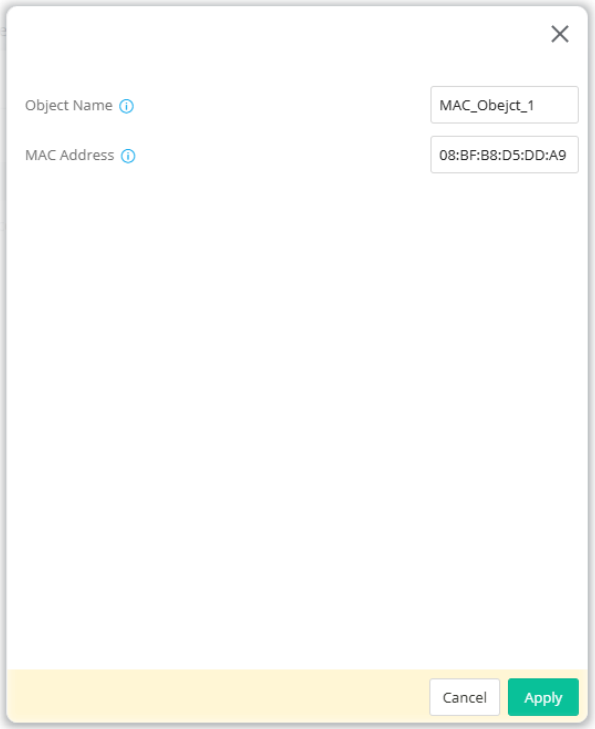
After finishing this web page configuration, please click **Apply** to save the settings.

## II-1-13-3 MAC Object

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




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




Available settings are explained as follows:

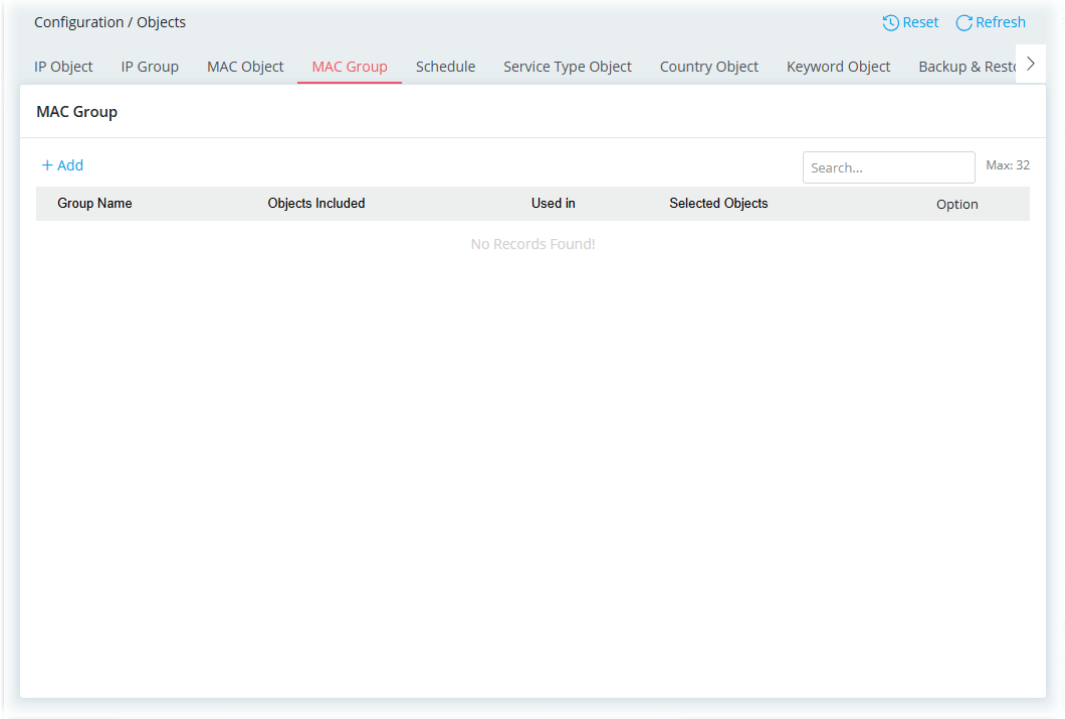
| Item | Description |
|---|---|
| **Object Name** | Enter a name that identifies this object. |
| **MAC Address** | Enter the MAC address of the client. |

| | |
|---|---|
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings and exit the page. |

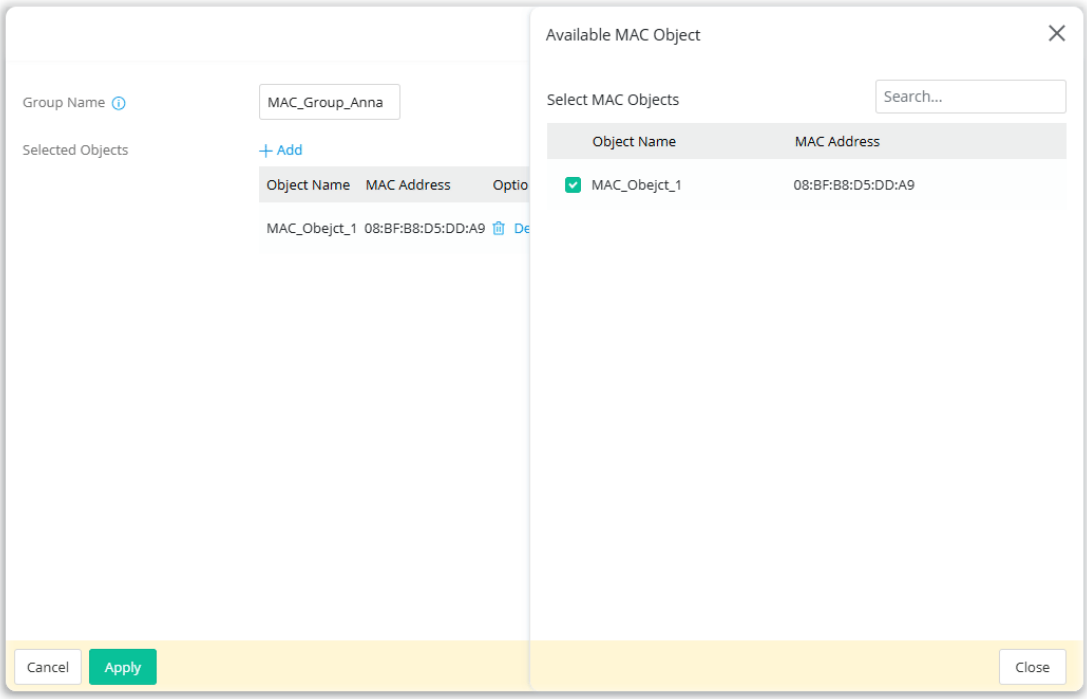
After finishing this web page configuration, please click **Apply** to save the settings.

## II-1-13-4 MAC Group

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




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



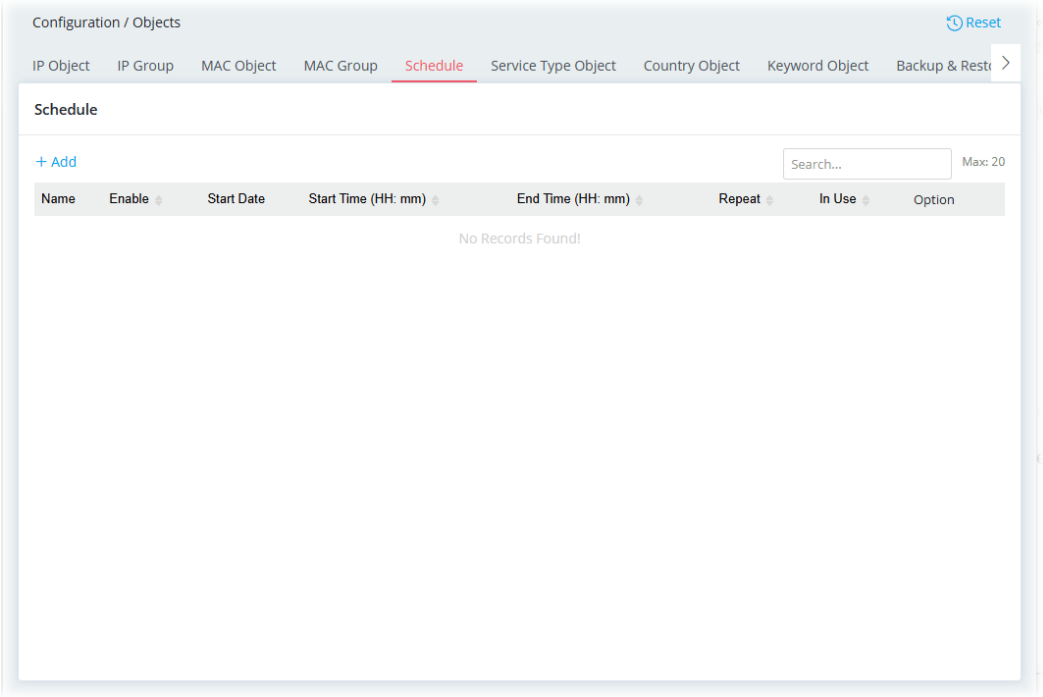

Available settings are explained as follows:

| 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** |
| Select MAC 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.<br>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. |

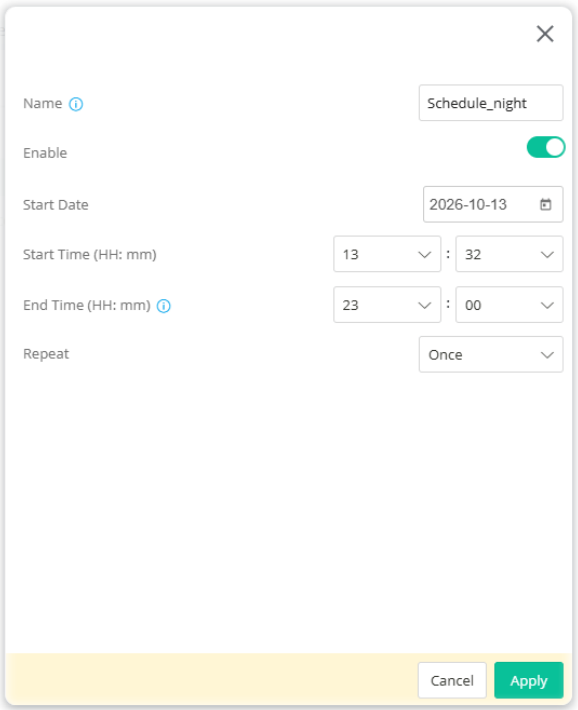
After finishing this web page configuration, please click **Apply** to save the settings.

## II-1-13-5 Schedule

Time schedules can be created and used with router features that support them, so that those features can be turned on and off automatically at preconfigured times.




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




Available settings are explained as follows:

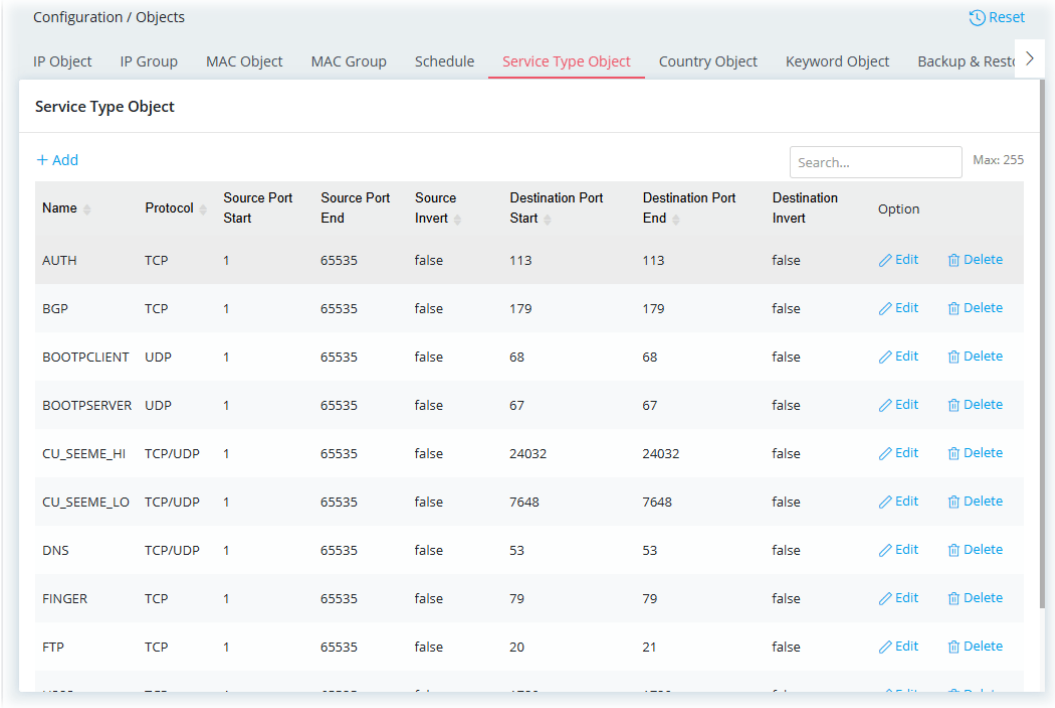
| Item | Description |
|---|---|
| **Name** | Enter the name of the schedule profile. |
| **Enable** | Switch the toggle to enable or disable this schedule profile. |
| **Start Date** | Select the date when the entry comes into effect. |
| **Start Time** | Set the time when the schedule is triggered. |
| **End Time** | Set the time for the schedule to be ended. |
| **Repeat** | **Once** - The schedule is triggered once based on **Date**, **Start Time** and **End Time**.<br>**Daily** - The schedule is triggered everyday based on **Start Time** and **End Time**.<br>● **End Repeat** - If enabled, the schedule will be triggered every day till the date defined in the End Repeat Date.<br>● **End Repeat Date** - The schedule will be ended on the specified date.<br>**Weekly** - The schedule will be triggered, starting at the Start Time and ending at the End Time, on the selected days of the week.<br>● **Every** - Select the day for triggering the schedule.<br>● **End Repeat** - If enabled, the schedule will be triggered every week till the date defined in the End Repeat Date..<br>● **End Repeat Date** - The schedule will be ended on the specified date.<br>**Monthly** - The schedule will be triggered monthly based on the Date setting. For example, choose 2022-04-27 as the date set. Later, this schedule will be triggered on the 27th of every month.<br>● **End Repeat** - If enabled, the schedule will be triggered every month till the date defined in the End Repeat Date.<br>● **End Repeat Date** - The schedule will be ended on the specified date. |

| | |
|---|---|
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings and exit the page. |

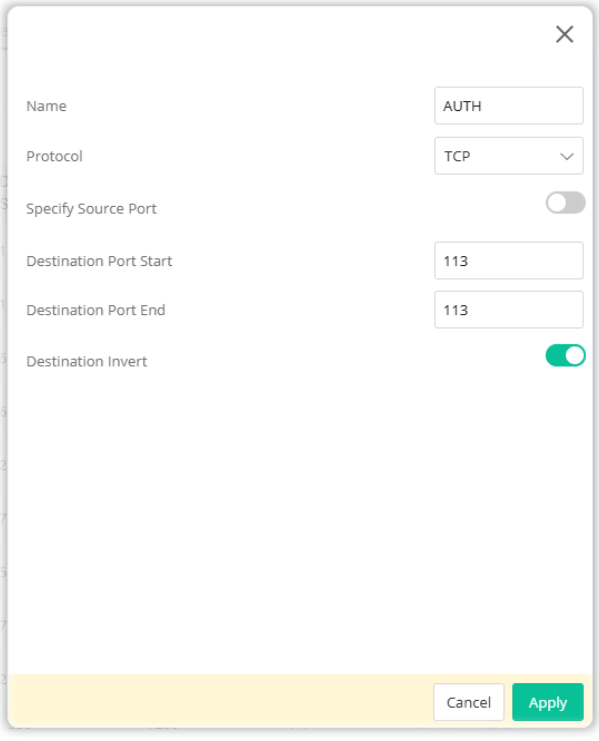
After finishing this web page configuration, please click **Apply** to save the settings.

## II-1-13-6 Service Type Object

Up to 255 Service Type Objects can be created.




To add/edit a service type profile, click the **+Add / Edit** link to get the following page.



Available settings are explained as follows:

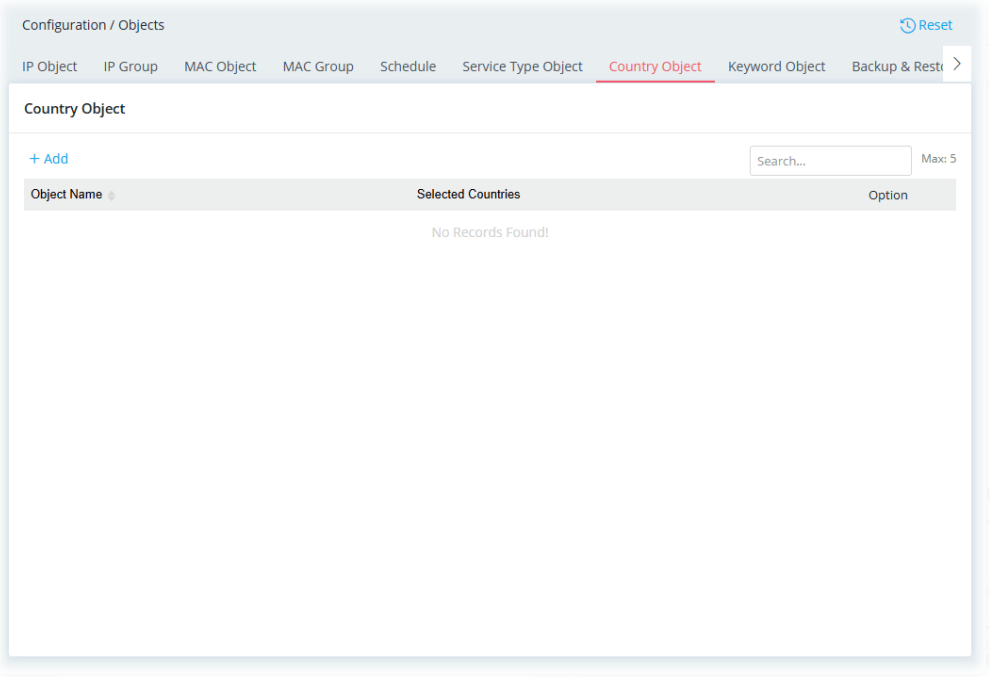
| Item | Description |
|---|---|
| Name | Name that identifies this profile. Maximum length is 15 characters. |
| Protocol | Protocol(s) to which this profile applies.<br>Any – All protocols.<br>ICMP / ICMPv6 – Internet Control Message Protocol<br>IGMP – Internet Group Management Protocol<br>TCP – Transmission Control Protocol<br>UDP – User Datagram Protocol<br>TCP/UDP – Transmission Control Protocol and User Datagram Protocol<br>Others – Other protocols not listed above. Enter protocol number in the textbox. |
| Specify Source Port | When protocol selected includes TCP or UDP, the source and destination ports can be specified.<br>Switch the toggle to enable/disable the source port settings.<br>Source Port Start / Source Port End – Enter two values to define the port range of source port.<br>Source Invert - If enabled, all port values except the ones entered above (Source Port Start/End) will be used. |
| Destination Port Start / Destination Port End | When protocol selected includes TCP or UDP, the source and destination ports can be specified. |
| Destination Invert | If enabled, all port values except the ones entered above (Destination Port Start/End) will be used. |
| 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.

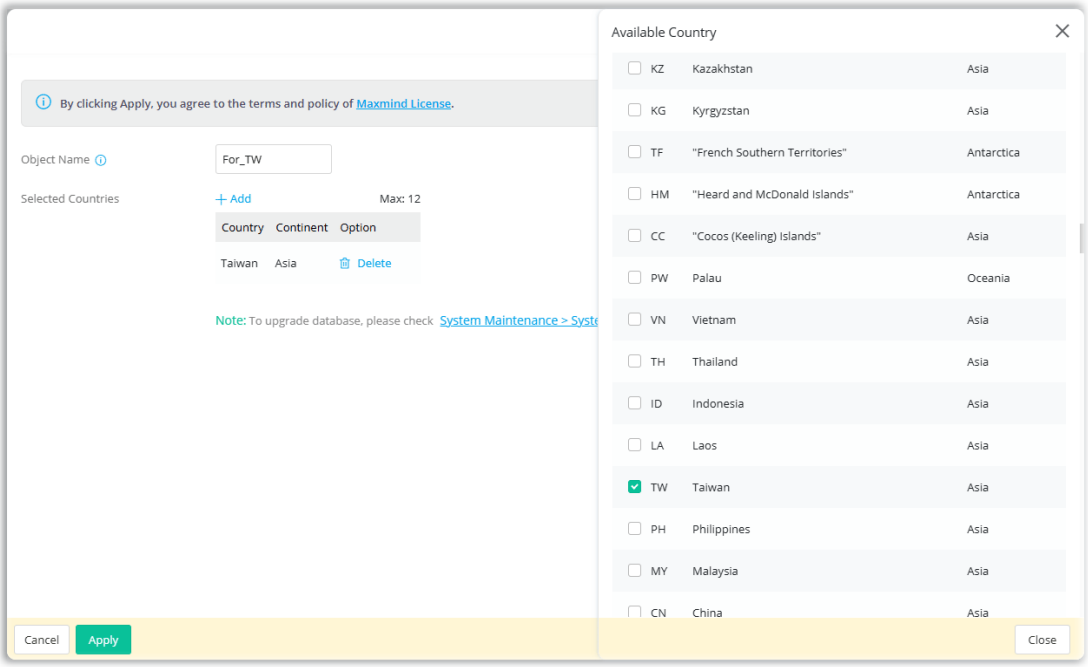
## II-1-13-7 Country Object

The country object profile can determine which country/countries shall be blocked by the Vigor router's Firewall.

Up to 5 country object profiles can be created for use as blacklists or white lists.




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



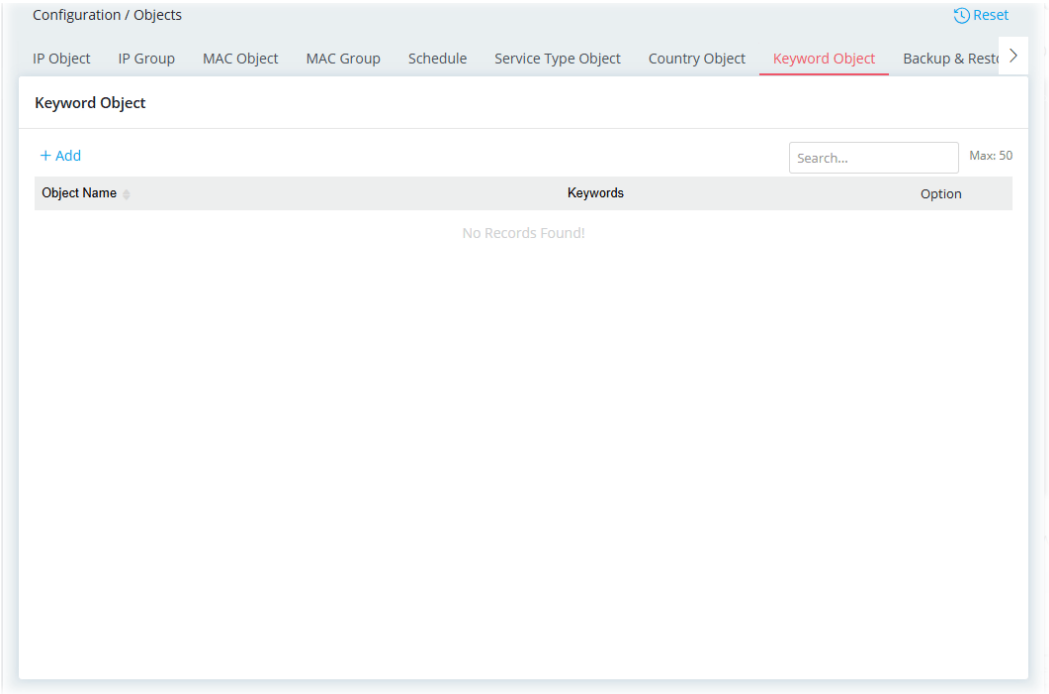

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Object Name** | Name that identifies this profile. Maximum length is 63 characters. |
| **Selected Countries** | **+Add** - Click to create an entry. A list of country codes will appear on the right side. Select up to 12 required codes for the new object. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings and exit the page. |

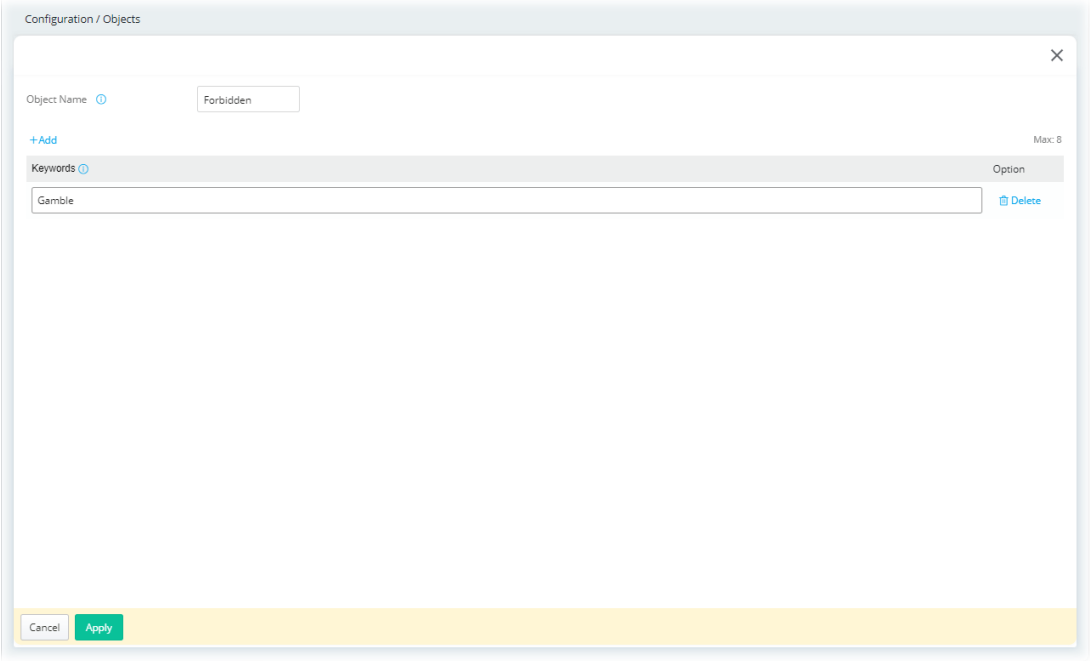
After finishing this web page configuration, please click **Apply** to save the settings.

## II-1-13-8 Keyword Object

50 Keyword Object Profiles can be created for use as blacklists or white lists.




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




Available settings are explained as follows:

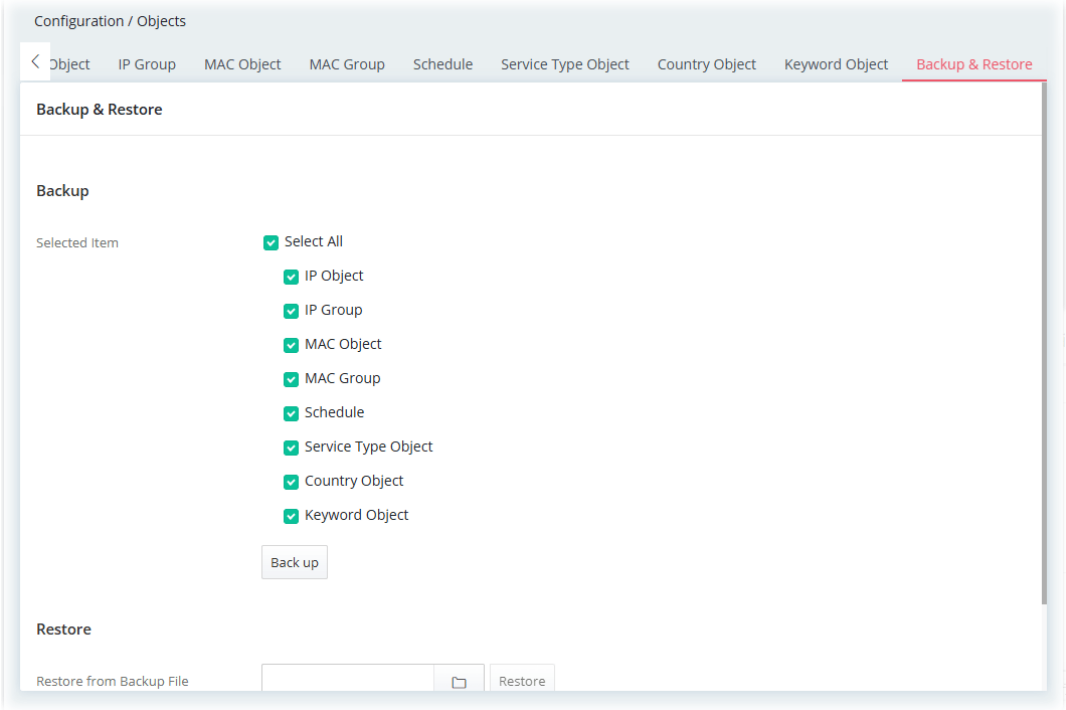
| Item | Description |
|---|---|
| **Object Name** | Name that identifies this profile. Maximum length is 16 characters. |
| **Keywords** | Keywords to be matched. Enter the content for this profile. For example, type *gambling* as Contents. When you browse the webpage, the page with gambling information will be watched out and be passed/blocked based on the configuration on |

| | |
|---|---|
| | Firewall settings.<br>In addition, up to 3 key phrases, separated by spaces, for a total length of 63 characters can be entered. For key phrases that contain spaces, replace spaces with the sequence %20. For example, the phrase “keep out” is to be entered as “keep%20out”. |
| **Delete** | Click to remove the selected entry. |
| **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-1-13-9 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.




Available settings are explained as follows:

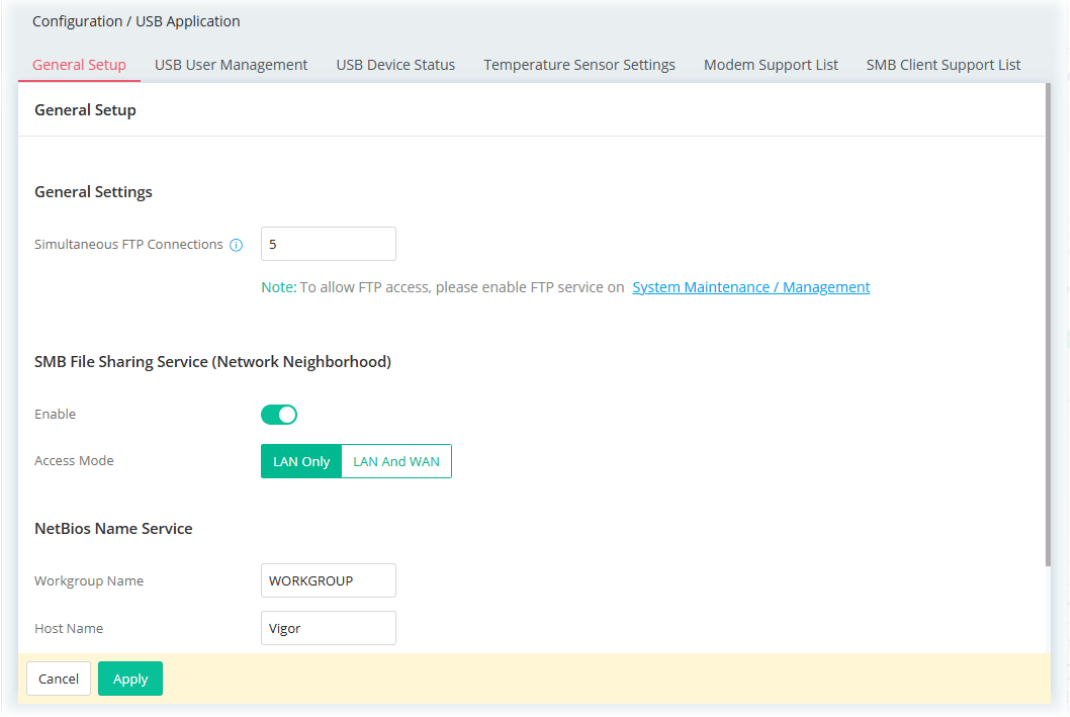
| Item | Description |
|---|---|
| **Backup** | Usually, a user can create the objects through the web page under Objects.<br>All the objects (or the template) can be saved and exported as a file by clicking Download.<br>**Back up** – Click it to backup current objects to a file. Such file can be restored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

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

# II-1-14 USB Application

## II-1-14-1 General Setup

This page allows you to configure the file sharing feature of the Vigor router, where USB mass storage devices such as thumb drives and hard drives can be made accessible to LAN clients.




Available settings are explained as follows:

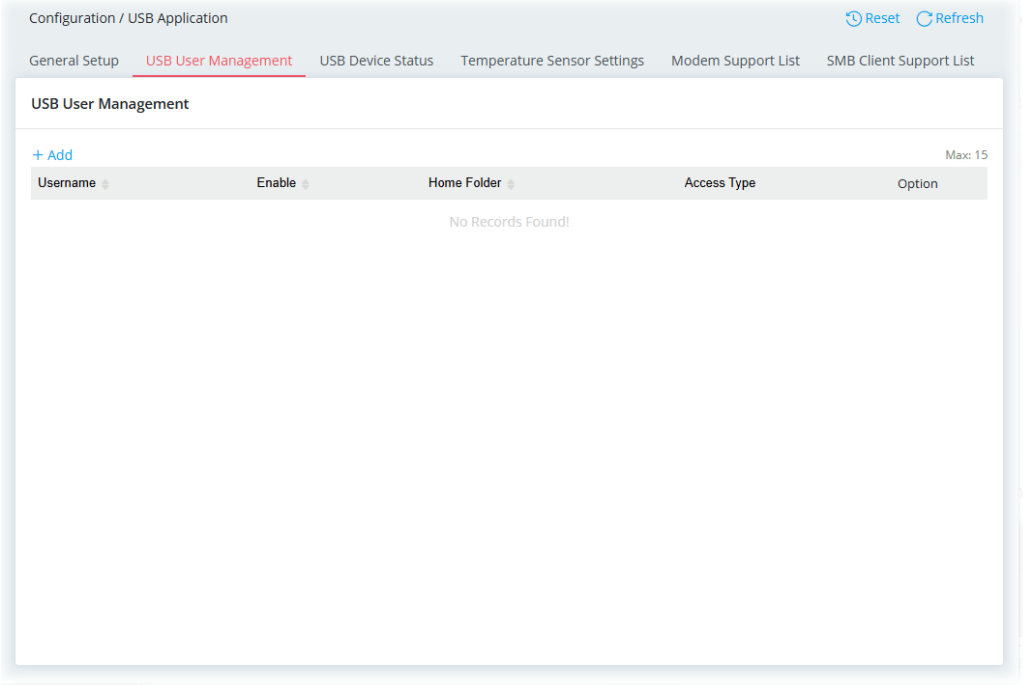
| Item | Description |
|---|---|
| **Simultaneous FTP Connections** | Enter the maximum number of simultaneous FTP sessions allowed. The router allows up to 6 simultaneous sessions. |
| **SMB File Sharing Service (Network Neighborhood)** | Click **Enable** to invoke SMB file sharing service via the router.<br>**Access Mode –** Select the access mode for file sharing service.<br>• **LAN Only** – Users coming from internet cannot connect to the SMB server of the router.<br>• **LAN And WAN** - Both LAN and WAN users can access SMB server of the router. |
| **NetBios Name Service** | For the NetBios service of USB storage disk, you have to specify a workgroup name and a host name. A workgroup name must not be the same as the host name. The workgroup name can have as many as 15 characters and the host name can have as many as 23 characters. Both them cannot contain any of the following--- ; : " < > * + = \ \| ?.<br>**Workgroup Name –** Type a name for the workgroup.<br>**Host Name –** Type the host name for the router. |
| **Printer Server** | Switch the toggle to enable/disable the printer server.<br>If enabled, the Vigor router will act as a print server for printers connected the USB. |

| | |
|---|---|
| **Cancel** | Discard current settings. |
| **Apply** | Save the current settings. |

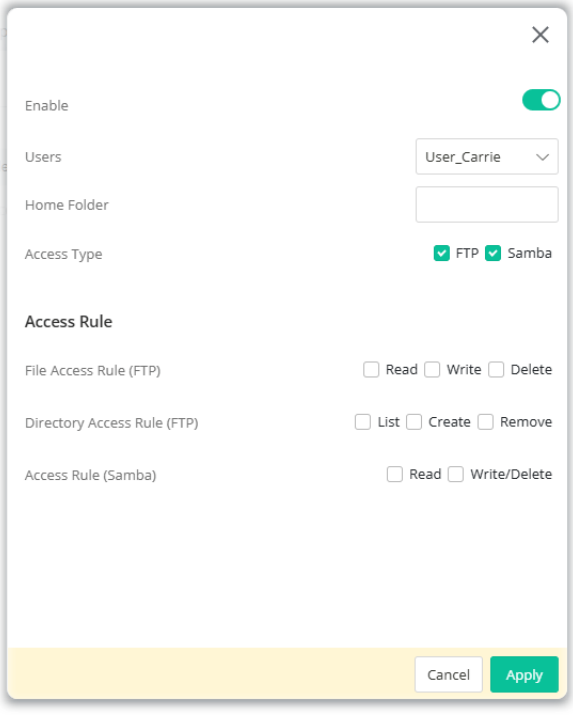
After finishing this web page configuration, please click **Apply** to save the settings.

## II-1-14-2 USB User Management

This page allows you to set up profiles for FTP/SMB users. Any user who wants to access the USB storage disk must authenticate using a username and password that have been configured on this page.




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



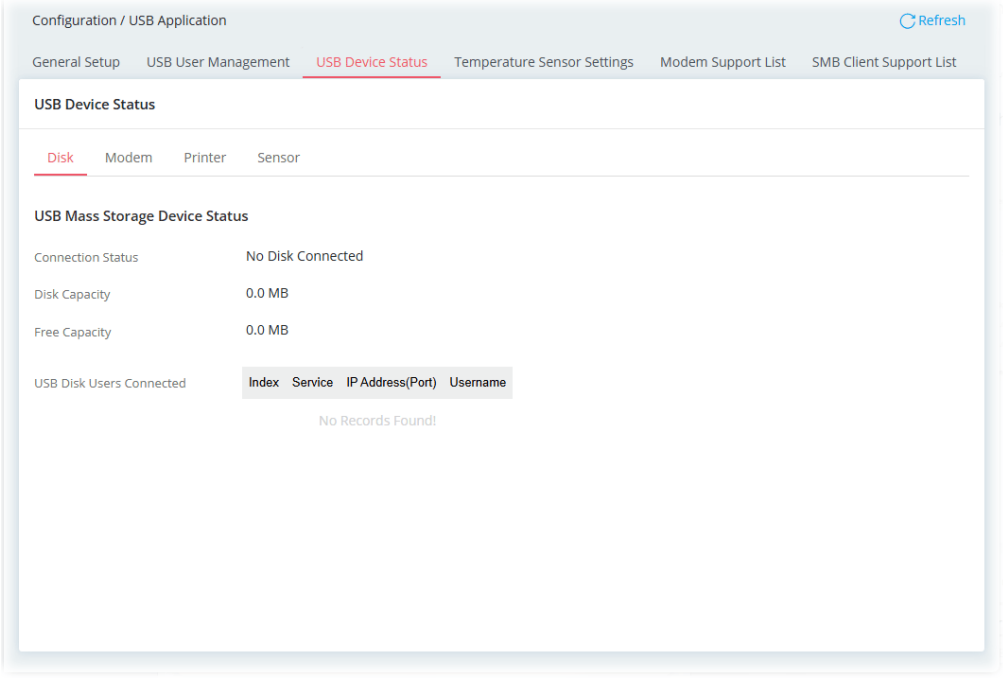
Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Switch the toggle to enable / disable this profile. |
| **Users** | Use the drop-down list to select an existed user account. |
| **Home Folder** | Enter the folder name which will be the root folder for FTP and SMB sessions established using the credentials of this user profile. Only folders and files inside this selected root folder are accessible to the user. |
| **Access Type** | **FTP** - It allows you to access and control a remote PC through FTP service.<br>**Samba** - It allows you to access and control a remote PC through Samba service. |
| **Access Rule** | It determines the authority for such profile. Any user, who uses such profile for accessing into USB storage disk, must follow the rule specified here.<br>**File Access Rule (FTP)** – Check the items (Read, Write and Delete) for such profile.<br>**Directory Access Rule (FTP)** – Check the items (List, Create and Remove) for such profile.<br>**Access Rule (Samba)** – Check the items (Read, Write/Delete) for such profile. |
| **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-1-14-3 USB Device Status

This page allows monitoring of the status of USB devices (disk, modem, printer, and sensor) connected to the Vigor router.



Available settings are explained as follows:

| Item | Description |
|---|---|
| Connection Status | Shows whether a USB disk is connected or not. If there is no USB device connected to the Vigor router, "No Disk Connected" will be displayed. |
| Disk Capacity | Shows the total capacity of the USB storage disk. |
| Free Capacity | Shows the free space on the USB storage disk. Click **Refresh** at any time to get the most up-to-date free capacity. |
| USB Disk Users Connected | Shows the clients that are connected to the SMB/FTP server.<br>**Index** – The profile index used by the client to establish the connection.<br>**Service** – Shows whether the connection is using FTP or SMB.<br>**IP Address** – Shows the client's IP address.<br>**Username** – Shows the username used to establish the connection. |

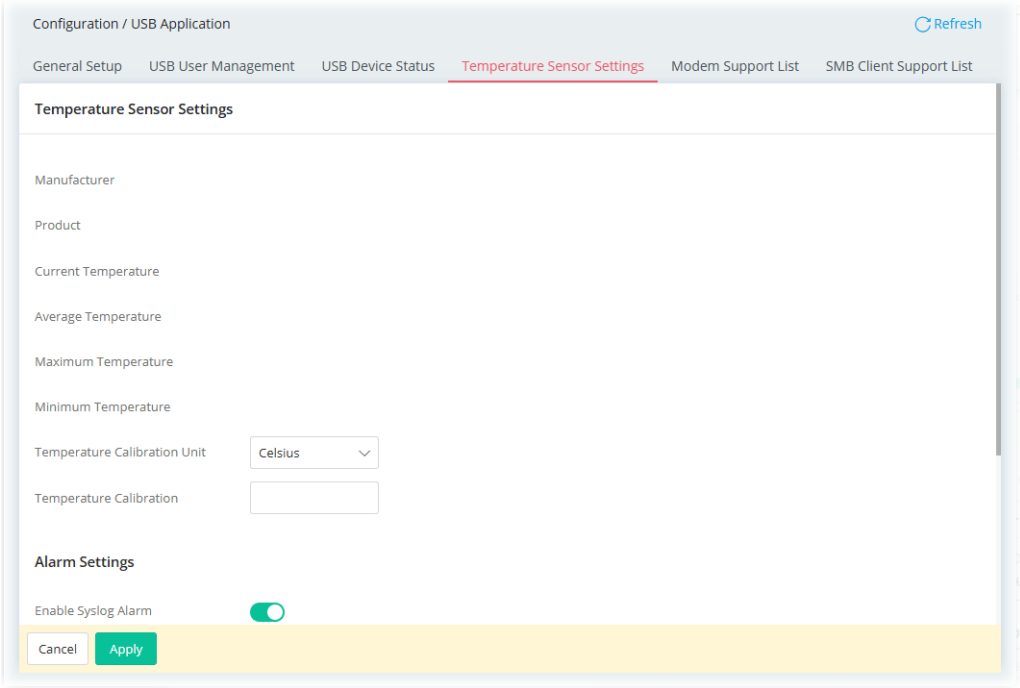
## II-1-14-4 Temperature Sensor Settings

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

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

The inclusion of a USB thermometer in compatible Vigor routers will continuously monitor the temperature of its environment. When a pre-determined threshold is reached you will be alerted by either an email or SMS so you can undertake appropriate action.

For a list of supported USB thermometers, visit our website at https://www.draytek.com/en/products/usb-thermometer/ or contact your local DrayTek partner.




Available settings are explained as follows:

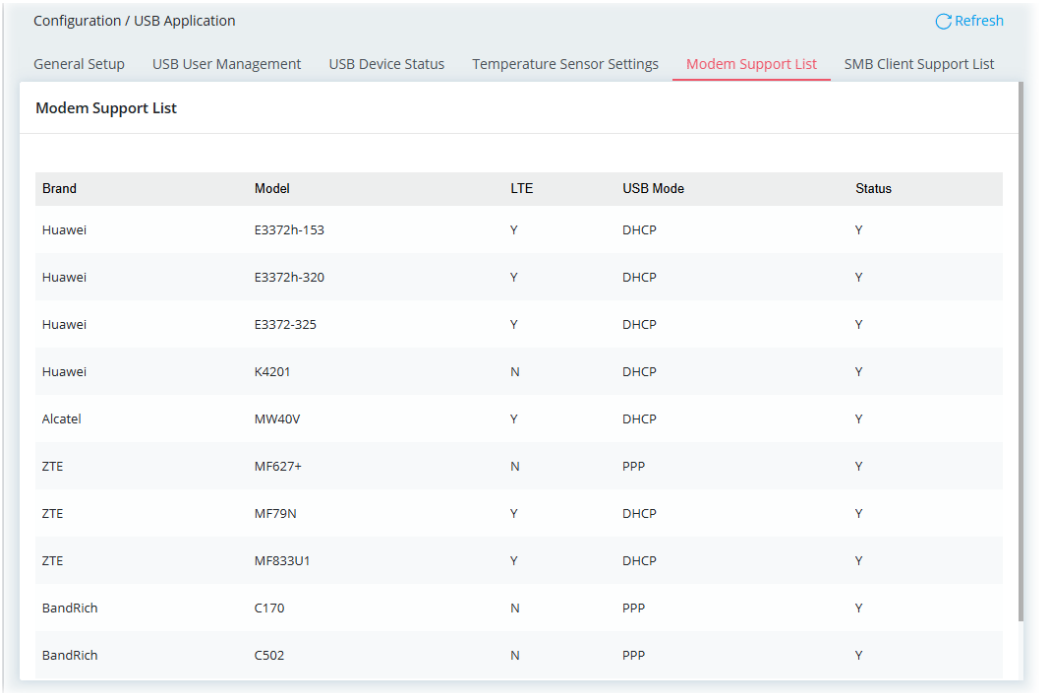
| Item | Description |
|---|---|
| **Temperature Sensor Settings** | Display information related to manufacturer, product, current temperature, average temperature, maximum temperature, and minimum temperature.<br>**Temperature Calibration Unit** - Select the temperature scale to be used.<br>**Temperature Calibration –** Enter the difference between the actual temperature and the temperature as reported by the thermometer. |
| **Alarm Settings** | **Enable Syslog Alarm** – Select to enable recording of the temperature in Syslog.<br>**SMS Alert** – Switch the toggle to enable/disable the SMS alert.<br>• **Send Alert SMS to** – Select the SMS sender profile (created on IAM>>Users & Groups>>Users, System Maintenance>>Account & Permission>>Local Admin Account).<br>**Email Alert** –Switch the toggle to enable/disable the email alert. |

| | |
|---|---|
| | • **Send Alert Email to** –Select the email sender profile (created on IAM>>Users & Groups>>Users, System Maintenance>>Account & Permission>>Local Admin Account).<br>**Lower temperature limit / Upper temperature limit**– Enter the upper and lower temperature limits. If the temperature falls outside of this range, an alert will be sent. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings and exit the page. |

## II-1-14-5 Modem Support List

This page lists the brands and models of USB modems that are supported by the Vigor router.

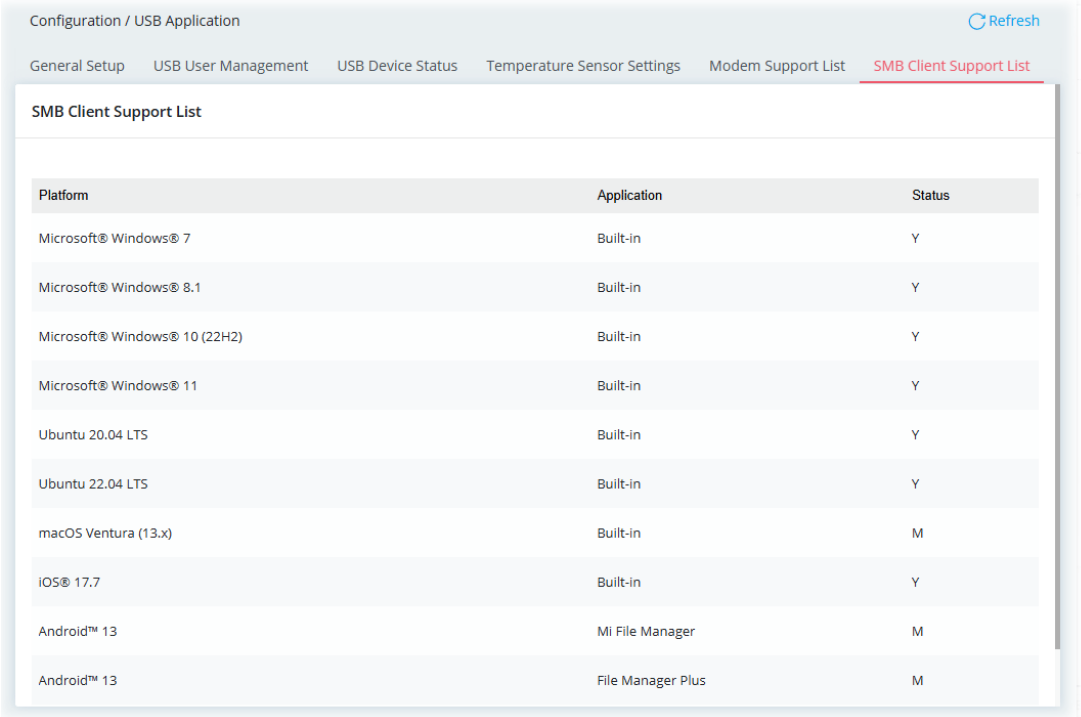
It is subject to change between different versions of firmware as support for new modems are added.




| Brand | Model | LTE | USB Mode | Status |
|---|---|---|---|---|
| Huawei | E3372h-153 | Y | DHCP | Y |
| Huawei | E3372h-320 | Y | DHCP | Y |
| Huawei | E3372-325 | Y | DHCP | Y |
| Huawei | K4201 | N | DHCP | Y |
| Alcatel | MW40V | Y | DHCP | Y |
| ZTE | MF627+ | N | PPP | Y |
| ZTE | MF79N | Y | DHCP | Y |
| ZTE | MF833U1 | Y | DHCP | Y |
| BandRich | C170 | N | PPP | Y |
| BandRich | C502 | N | PPP | Y |

## II-1-14-6 SMB Client Support List

The SMB Client Support List provides the test status information for applications with file sharing operated under different platforms.

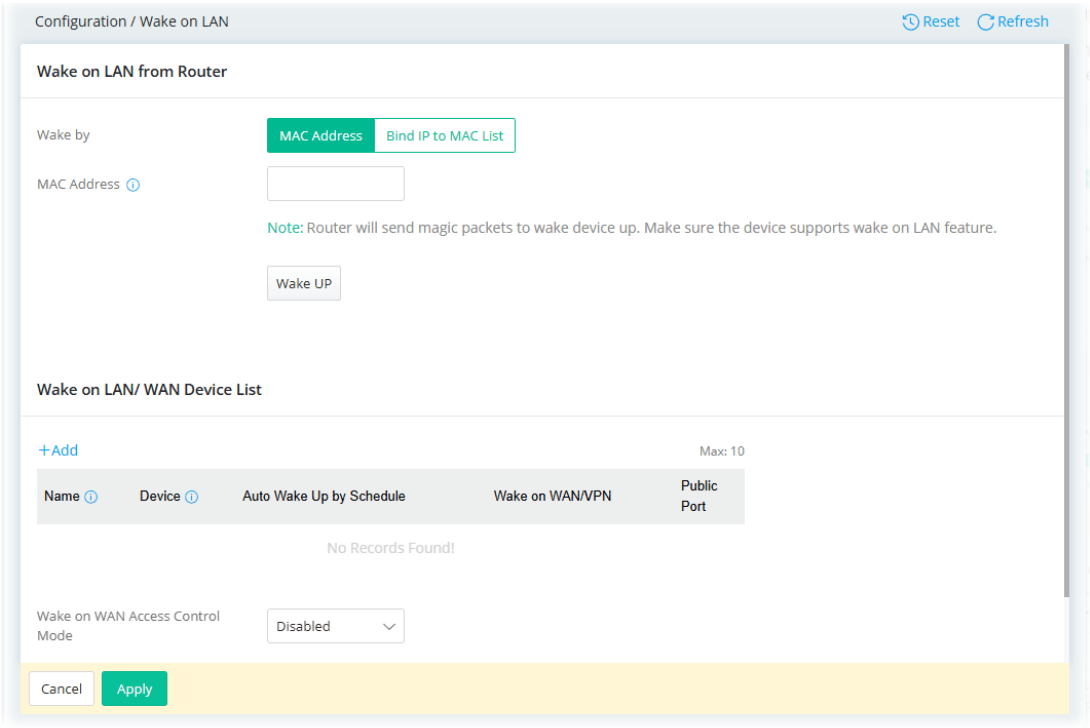


# II-1-15 Wake on LAN

Using the Wake on LAN (WoL) feature, LAN clients that support WoL can be powered on or resume from sleep over the network, without the need for physical access to the device.

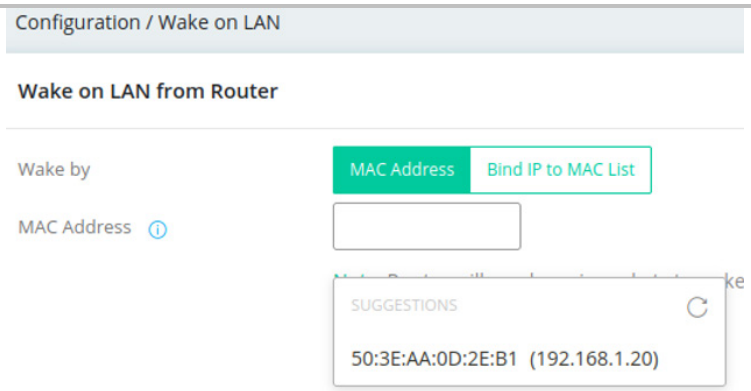
In order for LAN clients to be able to wake from sleep or off states, the network interface card must be configured to monitor Wake-on-LAN messages. Consult the documentation of the LAN client for details on setting up its network interface for Wake on LAN.

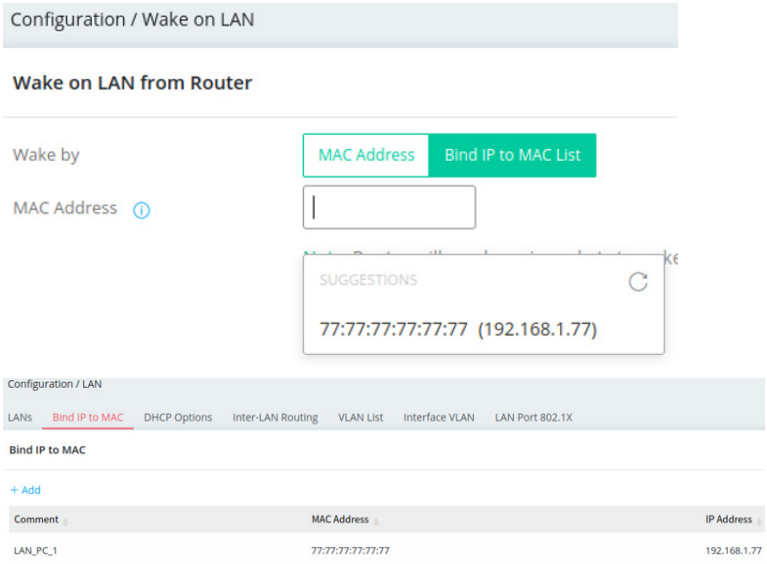
If you wish to be able to select the IP address of the Wake-on-LAN client, its MAC address must first be bound to a static IP address using the Bind IP to MAC function.




Available settings are explained as follows:

| Item | Description |
|---|---|
| | **Wake on LAN from Router** |
| **Wake by** | The type of address of the LAN client to be woken up.<br>• **MAC Address**<br>• **Bind IP to MAC List** |
| **MAC Address** | The MAC address provided here will be the device that the Vigor router will wake up.<br>If **MAC Address** is selected in Wake by, the content listed on ARP Table will be shown for you to choose. |

<table>
<tr><td></td><td>

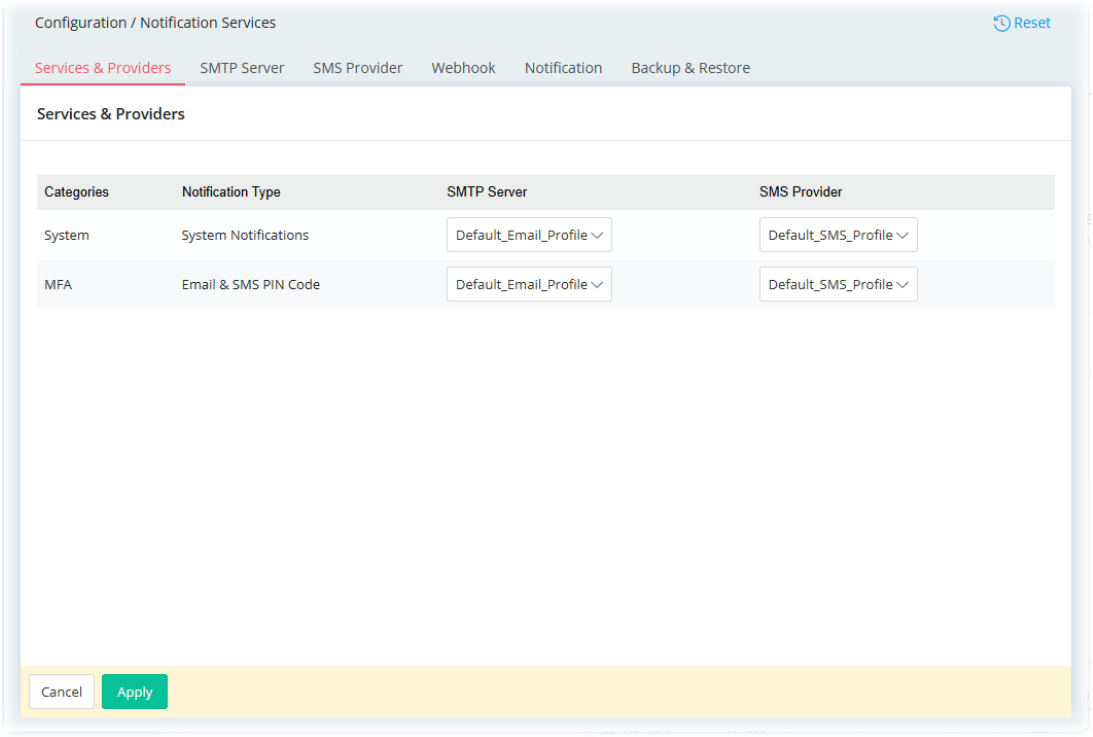
If Bind IP to MAC List is selected in Wake by, the profile content listed on Configuration>>LAN>>Bind IP to MAC will be shown for you to choose one.

</td></tr>
<tr><td>Wake Up</td><td>Click to send Wake-on-LAN message to the specified LAN client.</td></tr>
<tr><td colspan="2">Wake on LAN/WAN Device List</td></tr>
<tr><td>+Add</td><td>Click to specify a new device which will be awakened.<br>Name – Enter the name of the device.<br>Device – Enter the MAC address of the device.<br>Auto Wake Up by Schedule – The device can be awakened based on the schedule automatically.<br>Wake on WAN/VPN – Switch the toggle to enable / disable this function. The device can be awakened by the IPs selected on the Allow List.<br>Public Port – Enter the port value if Wake on WAN/VPN is enabled.<br>Option (Delete) – Remove the selected device.</td></tr>
<tr><td>Wake on WAN Access Control Mode</td><td>Set the path for the boot packet (sent by a mobile phone) to deliver to the remote device.<br>Allow List – Select the IP group. The boot packets will be transferred to the remote device via any WAN IP or the IP listed on the IP group.</td></tr>
<tr><td>Cancel</td><td>Discard current settings.</td></tr>
<tr><td>Apply</td><td>Save the current settings.</td></tr>
</table>

# II-1-16 Notification Services

Generally, the notification service refers to notifying users via email or SMS.

## II-1-16-1 Services & Providers

Before notifying the clients, the router's system administrator needs to configure the server and provider used to send letters or SMS messages.



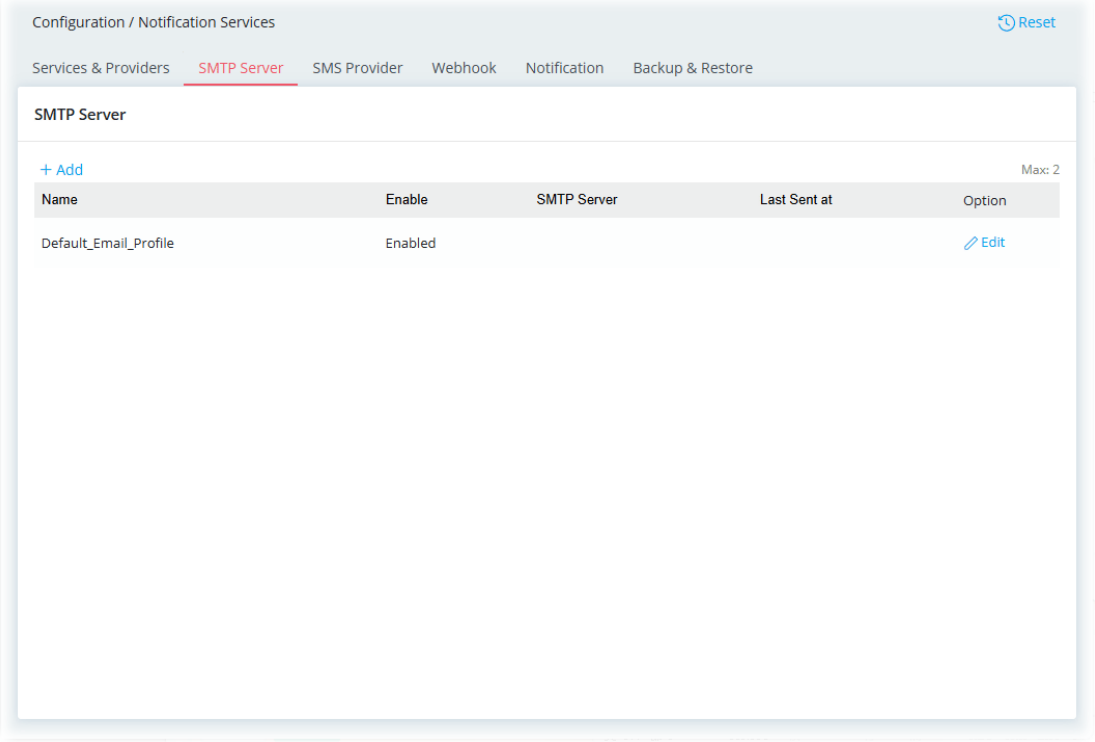

Available settings are explained as follows:

| Item | Description |
|---|---|
| **SMTP Server** | Use the drop-down menu to select the SMTP server for sending the e-mail. |
| **SMS Provider** | Use the drop-down menu to select the SMS Provider for sending the SMS. |
| **Cancel** | Discard current settings. |
| **Apply** | Save the current settings. |

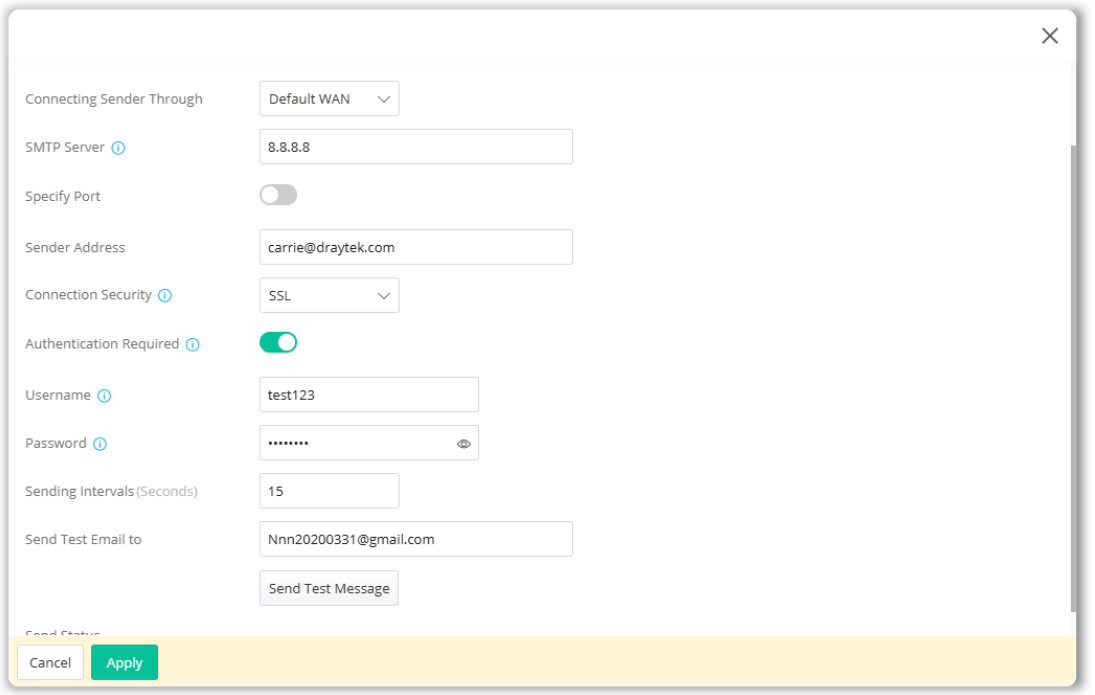
After finishing this web page configuration, please click **Apply** to save the settings.

## II-1-16-2 SMTP Server

Up to 2 SMTP server profiles can be set up for chosen by Services & Providers.




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




Available settings are explained as follows:

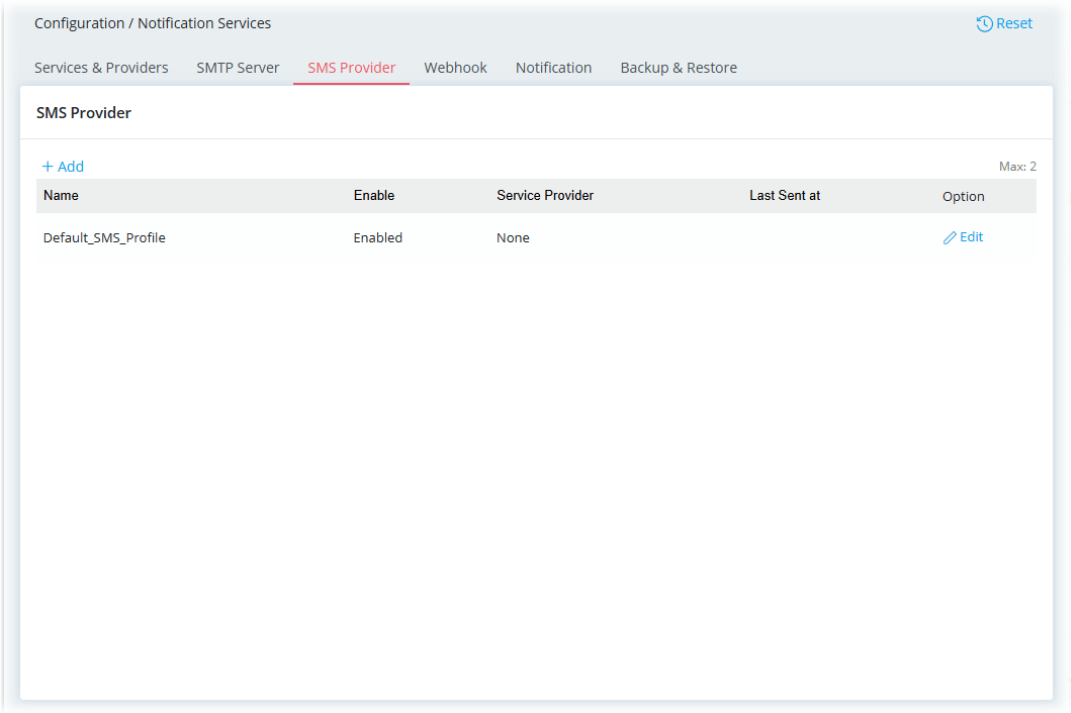
| Item | Description |
|---|---|
| **Name** | Enter the name of the profile. |
| **Enabled** | Switch the toggle to enable/disable this profile. |

| | |
|---|---|
| Connecting Sender Through | Specify the WAN interface for connecting the sender. |
| SMTP Server | Enter the IP address of the SMTP server. |
| Specify Port | Switch the toggle to enable the port setting.<br>**Specify SMTP Port** – Enter the port number of the SMTP server. |
| Sender Address | Enter the E-mail address of the sender. |
| Connection Security | There are three methods to enhance the connection security of SMTP server.<br>**None** - No SSL. Packets will be transferred without encryption.<br>**SSL** - Packets will be transferred with encrypted connection. Select to use SMTPS (SMTP over SSL) to communicate with the SMTP server. Note that the port number used for SMTPS server is 465.<br>**StartTLS** - It is a protocol used in communication to initiate a transition from an insecure one to a secure channel. |
| Authentication Required | Select to send username and password to SMTP server for authentication.<br>**Username** – Username for authentication. Maximum length is 31 characters.<br>**Password** – Password for authentication. Maximum length is 31 characters. |
| Sending Intervals | Minimum amount of time, in seconds, to wait between sending e-mail messages. |
| Send Test Email to | Specify an email address.<br>**Send Test Message** - Click it to send a test e-mail according to above configuration. |
| Cancel | Discard current settings and return to the previous page. |
| Apply | Save the current settings and exit the page. |

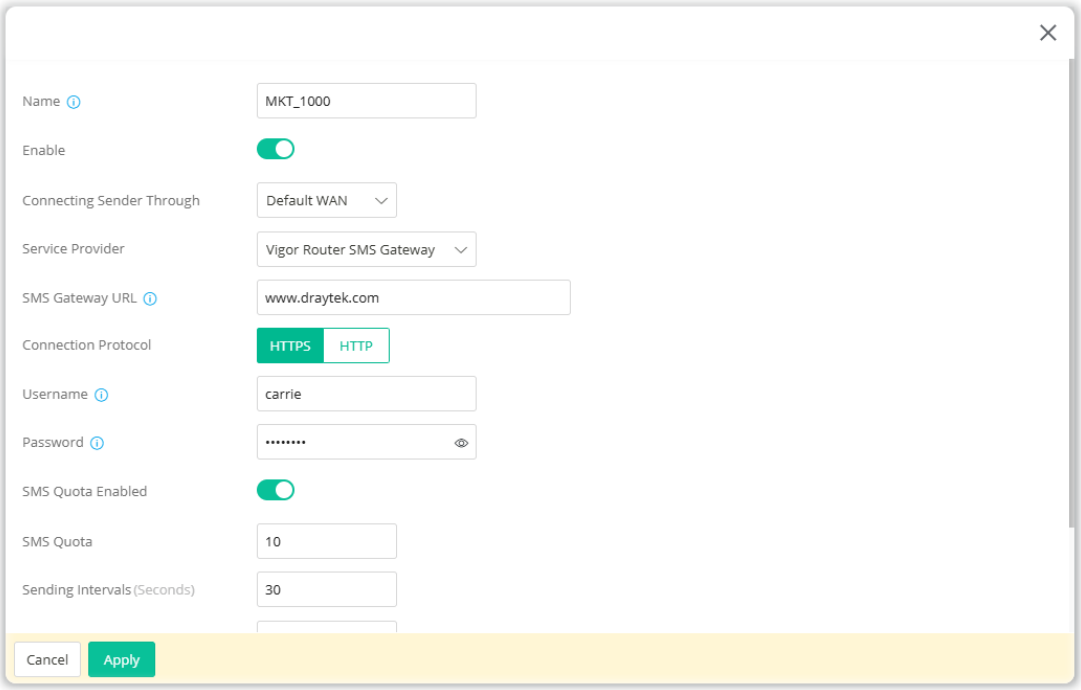
After finishing this web page configuration, please click **Apply** to save the settings.

## II-1-16-3 SMS Provider

Up to 2 SMS profiles can be set up as the SMS Providers.




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




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Name** | Enter the name of the profile. |
| **Enabled** | Switch the toggle to enable/disable this profile. |

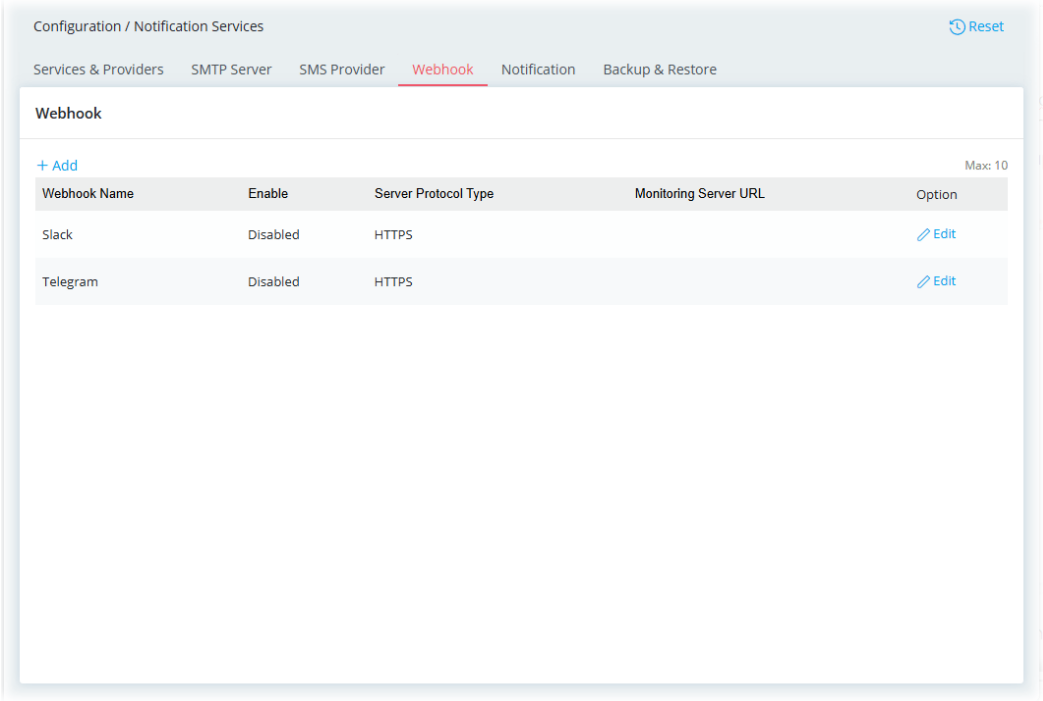
| | |
|---|---|
| Connecting Sender Through | Specify the WAN interface for connecting the sender. |
| Service Provider | **Vigor Router SMS Gateway** – Not all Vigor routers support the SMS function. This option allows you to set the IP address of the router which can be treated as a SMS gateway.<br>**Customized** – Set the IP address or URL provided by the SMS provider. |
| When Vigor Router SMS Gateway is selected as the Service Provider | **SMS Gateway URL** – Enter an identifier (domain name or IP address) for the service provider.<br>**Connection Protocol** – Specify HTTP or HTTPS.<br>**Username** - Used for being authenticated by the Service Provider. Maximum length is 31 characters.<br>**Password** - Used for being authenticated by the Service Provider. Maximum length is 31 characters. |
| When Customized is selected as the Service Provider | **SMS Provider API URL** – Enter the URL for the SMS service. Maximum length is 255 characters. Contact the service provider for the appropriate URL to use.<br>**SMS API Parameter** - For each API (Application Programming Interface) with an independent Text Message and Recipient Number (Send to), please enter the strings represented by each API.<br>**HTTP Method** – Two request methods offered here.<br>• **GET** - Used to request data from a specified resource.<br>• **POST** - Used to send data to a server to create/update a resource. |
| SMS Quota Enabled | Switch the toggle to enable/disable the quota setting. |
| SMS Quota | Remaining number of text messages allowed to be sent. The quota value reduces by 1 every time the router sends an SMS message. When the quota reaches 0, no SMS will be sent until it is reset to greater than 0. |
| Sending Intervals | Minimum amount of time, in seconds, to wait between sending SMS messages. |
| Send Test SMS to | Specify an email address.<br>**Send Test Message** - Click it to send a test e-mail according to above configuration. |
| 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.

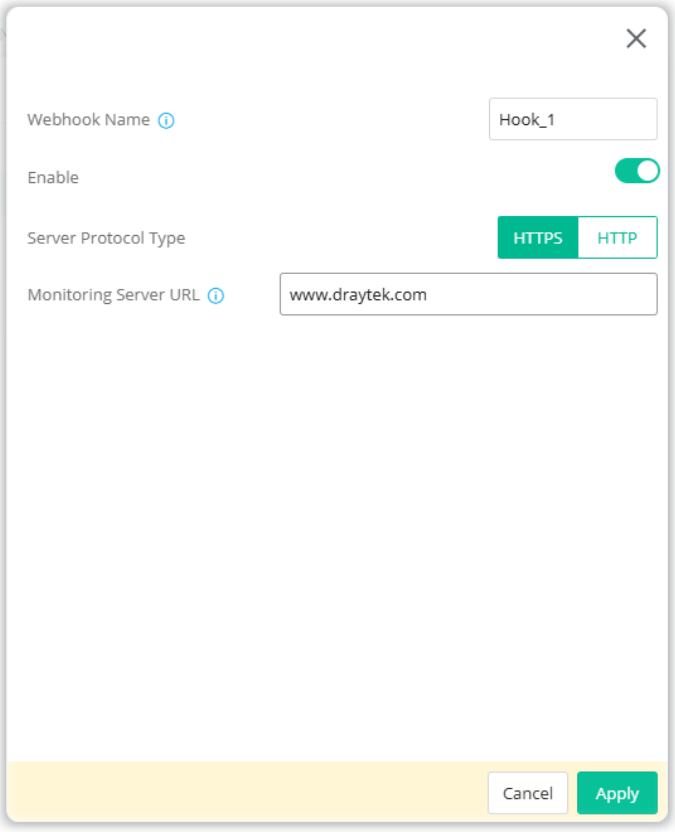
## II-1-16-4 Webhook

Vigor router will send a report (webhook message) including WAN up, down, CPU usage, memory usage and etc. to a monitoring server periodically.

Up to 10 webhook profiles can be set up.




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



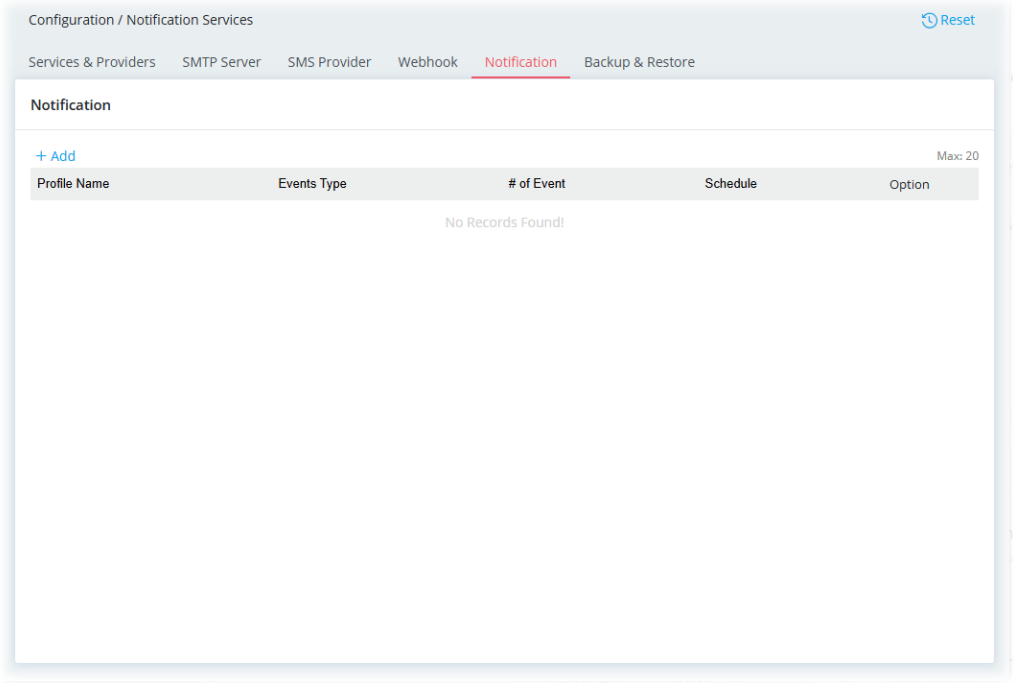
Available settings are explained as follows:

| Item | Description |
|---|---|
| **Webhook Name** | Enter the name of the profile. |
| **Enable** | Switch the toggle to enable/disable this profile. |
| **Server Protocol Type** | Select the protocol (HTTPS or HTTP) used for the server. |
| **Monitoring Server URL** | Enter the URL of a server. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings and exit the page. |

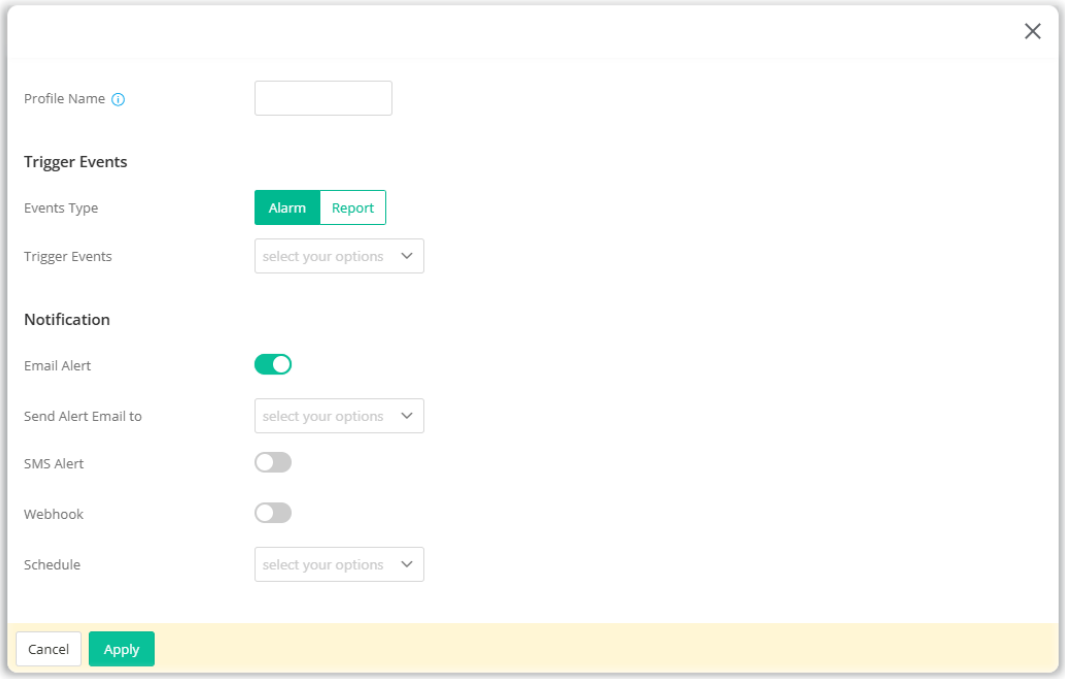
After finishing this web page configuration, please click **Apply** to save the settings.

## II-1-16-5 Notification

Up to 20 notification profiles can be created and applied with the provider notification services.




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



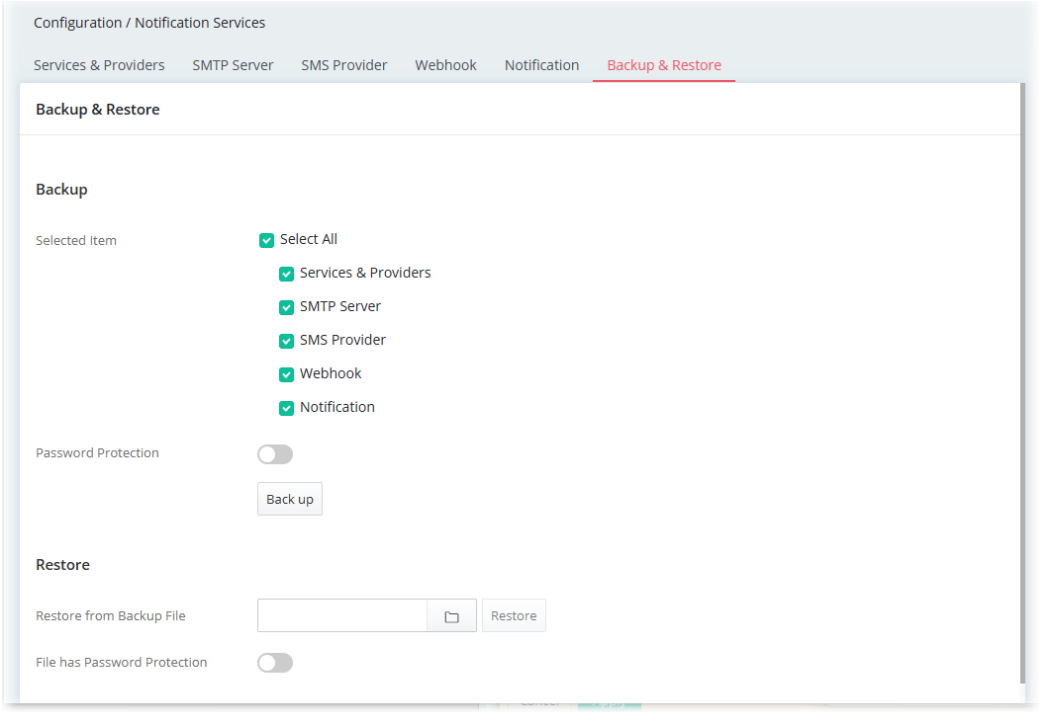

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Name** | Enter the name of the service profile. |
| **Events Type** | **Alarm** – The Vigor system will send alert messages to recipients if an alert event occurs.<br>**Report –** The Vigor system will periodically send reports to recipients when an alert event occurs.<br>• **Report Period** – Set the period (60-360 minutes) for Vigor system to send out the report by email, SMS and etc. |
| **Trigger Events** | Select the events that allow the Vigor system to send reports or alerts via email, SMS, and more using the drop-down list. |
| **Email Alert** | Switch the toggle to enable / disable the email alert function.<br>**Send Alert Email to** - Select the email profile(s) for sending out the notification by email. |
| **SMS Alert** | Switch the toggle to enable / disable the SMS alert function.<br>**Send Alert SMS to** - Select the SMS profile(s) for sending out the notification by SMS. |
| **Webhook** | Switch the toggle to enable / disable the webhook notification.<br>**Webhook Profile** - Select the webhook profile(s) for sending out the notification. |
| **Schedule** | Select the schedule profile(s) to send the notification (SMS, Email). |
| **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-1-16-6 Backup & Restore

Backup and restore the configuration settings for notification services.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Selected Item** | Select the items for which settings will be backed up or restored. |
| **Password Protection** | Switch the toggle to enable or disable the function.<br>If enabled, set a password.<br>**New Password** – Enter a string as the password.<br>**Confirm New Password** – Enter the string again.<br>**Back up** – Click to perform the backup job. |
| **Restore from Backup File** | Select the backup file you wish to restore. |
| **File has Password Protection** | Switch the toggle to enable or disable the function.<br>If enabled, set a password.<br>**Password** – Please enter a string to use as the password for restoring the configuration. |
| **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-1-17 RADIUS/TACACS+

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.

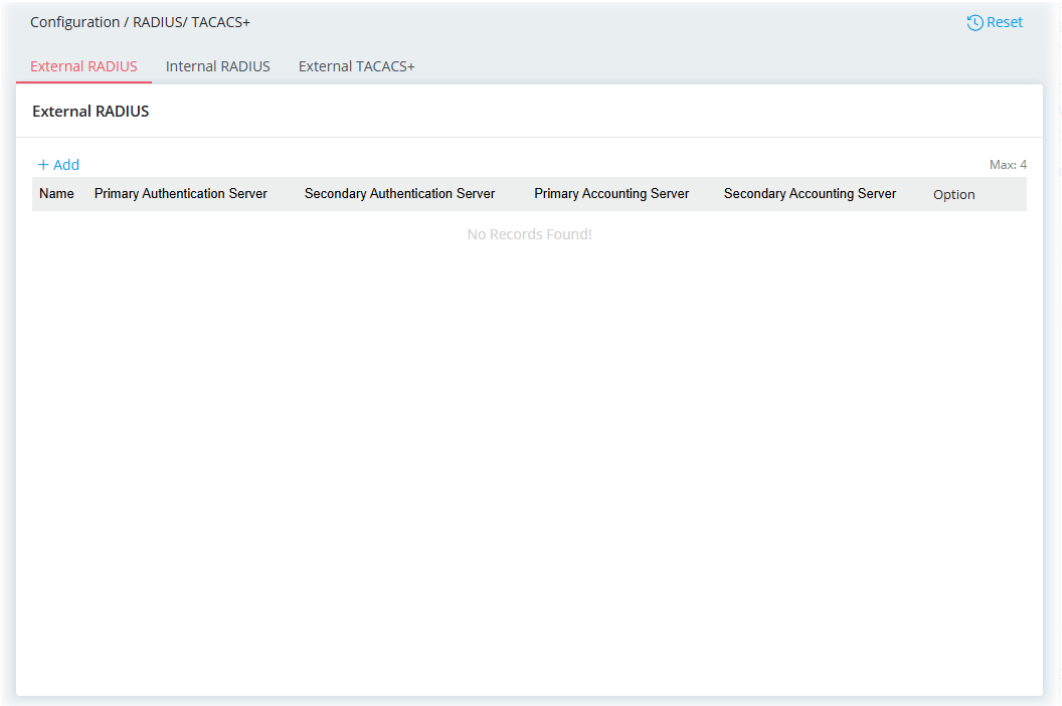
The router supports external TACACS+ and internal and external RADIUS servers for user authentication. Services that require user authentication include WLAN and VPN.

## II-1-17-1 External RADIUS

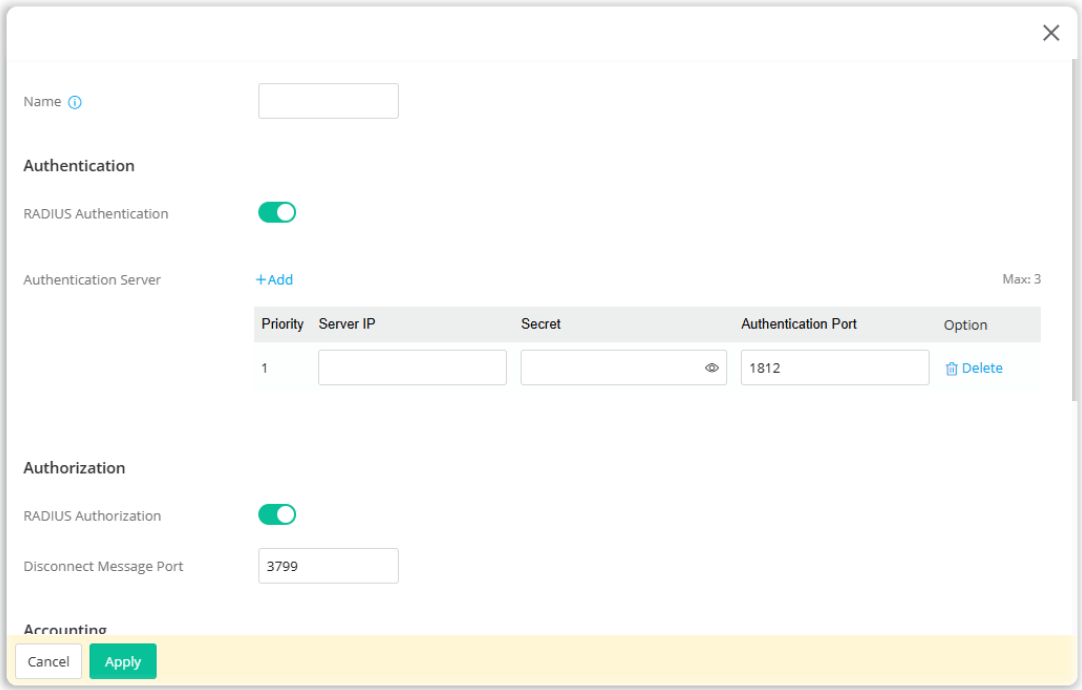
The built-in RADIUS client feature enables the router to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access authentication for network management.

Vigor router can be operated as a RADIUS client. This web page is used to configure settings for external RADIUS server. Then LAN users of Vigor router will be authenticated and accounted by such server for network application.

Select External RADIUS to configure the router to use an external RADIUS server for user authentication.




To add a new profile, click the **+Add** link (up to 4) to get the following page.

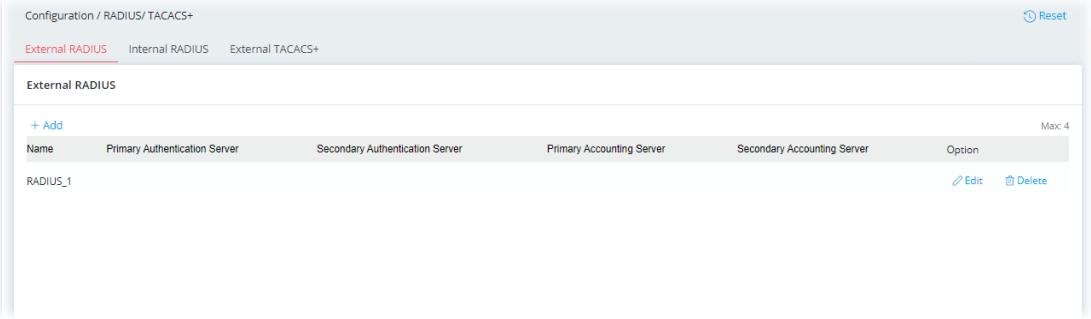



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Name** | Enter the name of the profile. |
| | **Authentication** |
| **RADIUS Authentication** | Switch the toggle to enable/disable this profile. |
| **Authentication Server** | **+Add** – Click to add a server (up to 3).<br>**Server IP** –Enter the IP address of RADIUS server.<br>**Secret** – The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret. The maximum length of the shared secret you can set is 36 characters.<br>**Authentication Port** – The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.<br>**Option (Delete)** - Remove the selected server. |
| | **Authorization** |
| **RADIUS Authorization** | Switch the toggle to enable/disable this profile.<br>**Disconnect Message Port** - Set a UDP port number (3799 in default) for receiving the disconnected-request packets from the AAA server. Note that these packets have been accepted by the RADIUS server before being disconnected by the AAA server. |
| | **Accounting** |
| **RADIUS Accounting** | RADIUS Accounting is a network customer billing mechanism for RADIUS server.<br>If enabled, Vigor router will deliver accounting request (e.g., IP address, traffic from the client) to the specified RADIUS server periodically.<br>Switch the toggle to enable/disable this profile. |
| **Accounting Server** | **+Add** - Click to add a server (up to 3). |

| | |
|---|---|
| | **Server IP** - Enter the IP address of RADIUS server.<br>**Secret** - The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret. The maximum length of the shared secret you can set is 36 characters.<br>**Authentication Port** - Set the UDP port number (1813 in default) as the accounting port.<br>**Option (Delete)** - Remove the selected server. |
| **Interim Update Interval** | Set an interval time from 10 minutes to 1440 minutes (1 day) for the router to deliver the accounting request to the RADIUS server. |
| | **RADIUS Server Failover Policy** |
| **Retry** | Set the number of attempts to perform reconnection with RADIUS server. If the connection (with the Primary Server) still fails, stop the connection attempt and begin to make connection with the secondary server. |
| **Timeout** | Set a timeout value for the router waiting for a response from the RADIUS server. If no response, Vigor router will send the authentication request again. |
| | **Connection Test** |
| **Connection Test** | **Test with Status Server** – Click to make a test of authentication server and accounting server. |
| **Server Status** | Display the test result of the connection test. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings and exit the page. |

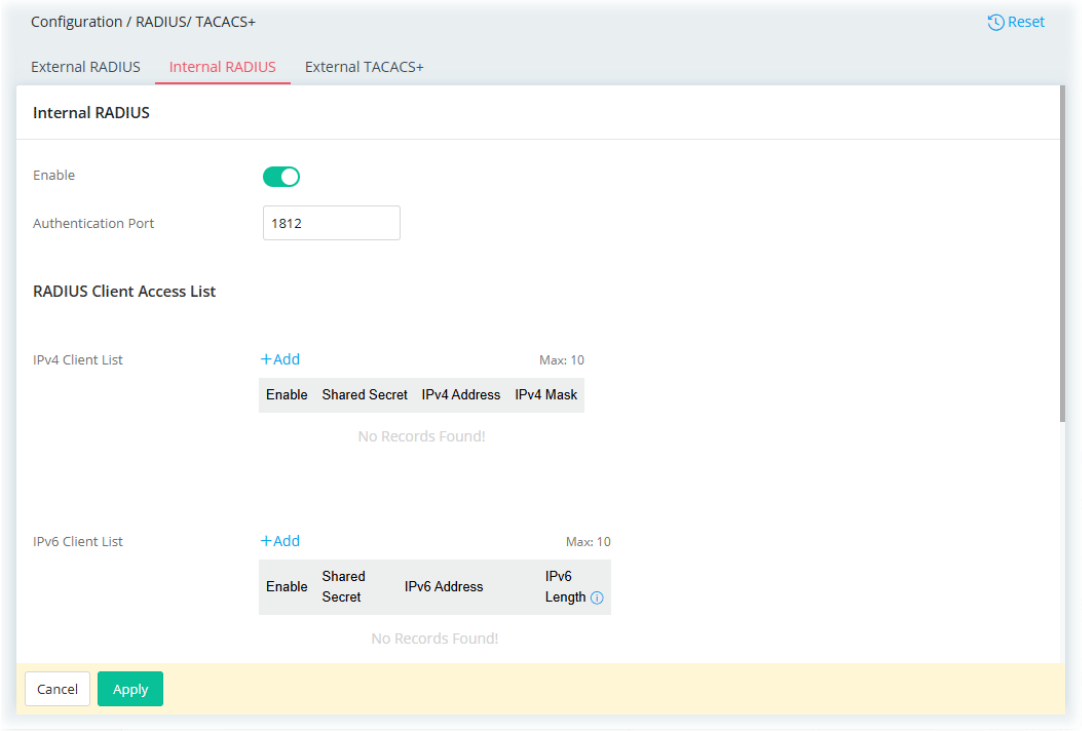
After finishing this web page configuration, please click **Apply** to save the settings.




## II-1-17-2 Internal RADIUS

Except for being a built-in RADIUS client, Vigor router also can be operated as a RADIUS server which performs security authentication by itself. This page is used to configure settings for internal RADIUS server. Then LAN user of Vigor router will be authenticated by Vigor router directly.

Select Internal RADIUS to configure the router's built-in RADIUS server.




Available settings are explained as follows:

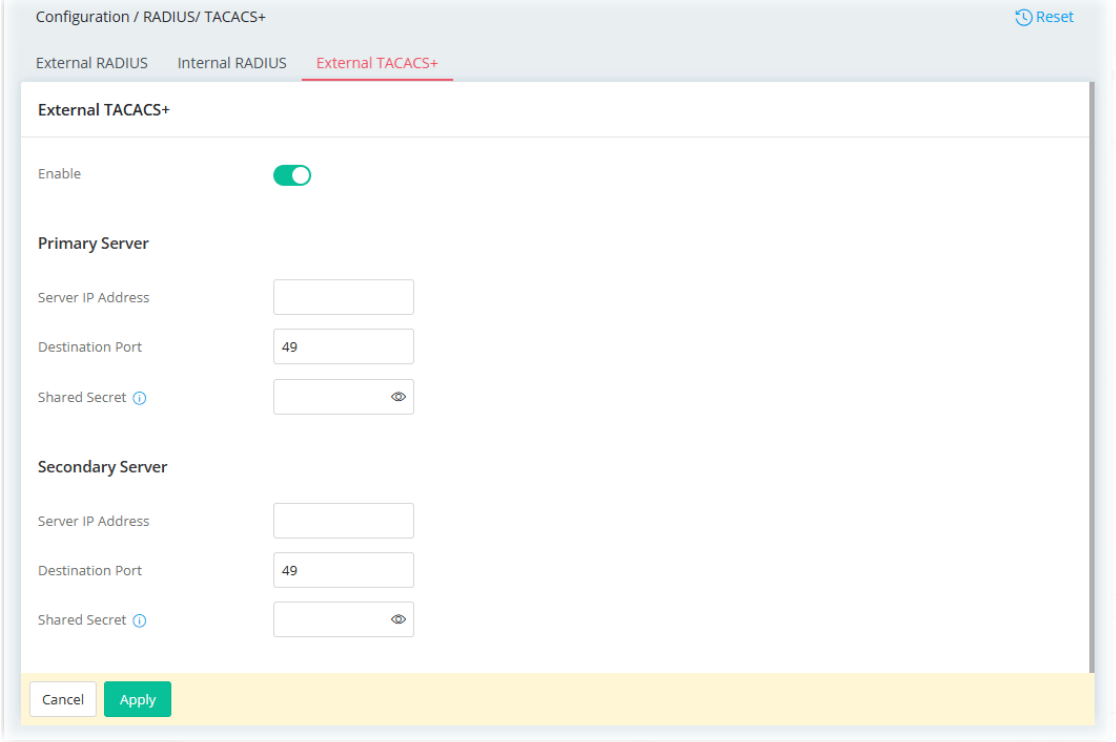
| Item | Description |
|---|---|
| **Enable** | Switch the toggle to enable/disable settings for this RADIUS server. |
| **Authentication Port** | The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138. |
| | **RADIUS Client Access List** |
| **IPv4 Client List** | Only clients that meet the criteria configured in the access list are allowed to access the RADIUS server.<br>**+Add** – Click to add a client (up to 10).<br>**Enabled** –Switch the toggle to enable/disable this entry.<br>**Shared Secret** – A text string that is known to both the router's RADIUS server and the RADIUS client that is used to authenticate messages sent between them. Maximum length is 36 characters.<br>**IPv4 Address** – Enter the IPv4 address of the client.<br>**IPv4 Mask** – Select the IP mask to configure the size of the IP block.<br>**Option (Delete)** - Remove the selected client. |
| **IPv6 Client List** | Only clients that meet the criteria configured in the access list are allowed to access the RADIUS server.<br>**+Add** – Click to add a client (up to 10).<br>**Enabled** –Switch the toggle to enable/disable this entry.<br>**Shared Secret** – A text string that is known to both the router's RADIUS server and the RADIUS client that is used to authenticate messages sent between them. Maximum length is 36 characters.<br>**IPv6 Address** –Enter the IPv6 address of the client.<br>**IPv6 Length** – Enter the prefix length of the IPv6 block.<br>**Option (Delete)** - Remove the selected client. |
| | **Authentication** |

| | |
|---|---|
| **Method** | Specify the way to authenticate the wireless client.<br>**PAP Only** – Only the Password Authentication Protocol will be used to validate users.<br>**PAP/CHAP/MS-CHAP/MS-CHAP2** - PAP, CHAP (Challenge-Handshake Authentication Protocol), and Microsoft versions of CHAP can be used to validate users. |
| **802.1X Method** | **Support 802.1X Method** – The built in RADIUS server offered by Vigor router can act as the AAA server. Select to enable 802.1X support. |
| **Certificate** | Select the certificate (created by Configuration>>Certificates>>Local Certificates) for applying to Internal RADIUS. |
| **User Profile** | |
| **User** | During the process of security authentication, user account and user password will be required for identity authentication. Before configuring such page, create at least one user profile in **IAM>>Users & Groups** first.<br>**All Users** – Click to make all user profiles for security authentication.<br>**Select Users** – Click to select the user profile(s) for security authentication. |
| **User Group** | **All Groups** – Click to make all user groups for security authentication.<br>**Select Groups** – Click to select the user groups for security authentication. |
| **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-1-17-3 External TACACS+

It means Terminal Access Controller Access-Control System Plus. It works like RADIUS does. Click the **External TACACS+** to open the following page:




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Switch the toggle to enable/disable this profile. |
| | **Primary Server/Secondary Server** |
| **Server IP Address** | Enter the IP address of the TACACS+ server.<br>Two external TACACS+ servers are allowed to set in this page.<br>The secondary TACACS+ server will be used as a backup server when the primary TACACS+ server is down. |
| **Destination Port** | Enter the port used by the TACACS+ server. Port 49 is most common. |
| **Shared Secret** | A text string that is known to both the TACACS+ server and client (the router) that is used to authenticate messages sent between them. Maximum length is 36 characters. |
| **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.

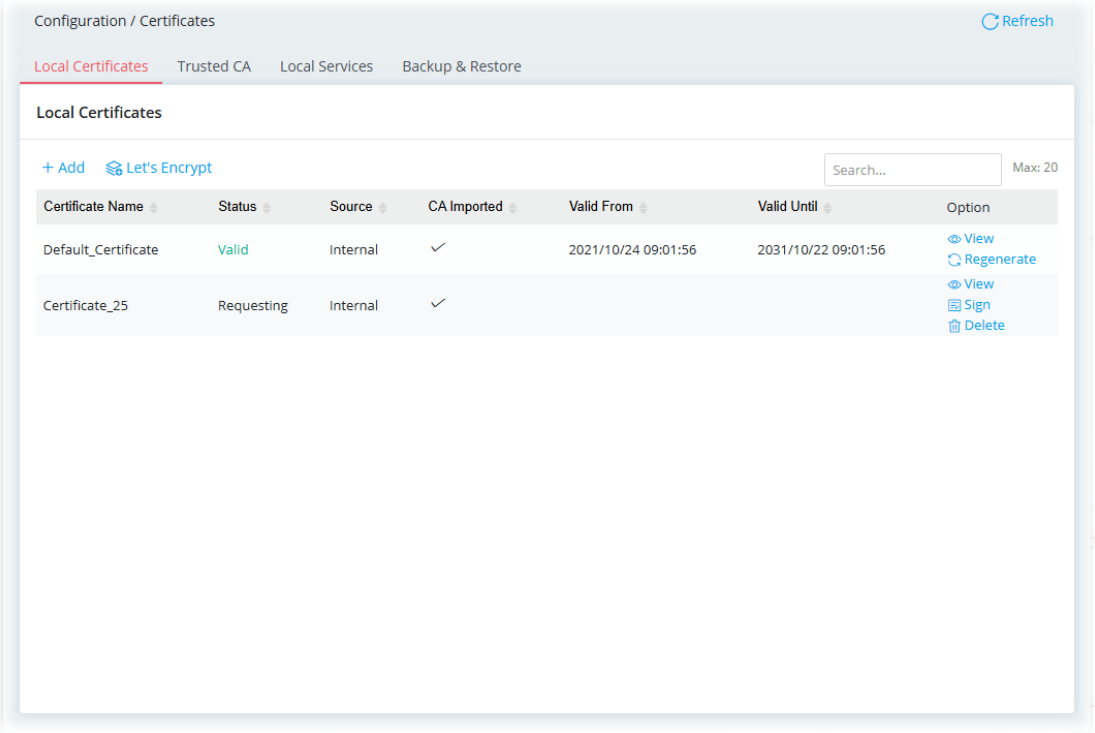
# II-1-18 Certificates

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 router supports digital certificates that conform to the X.509 standard.

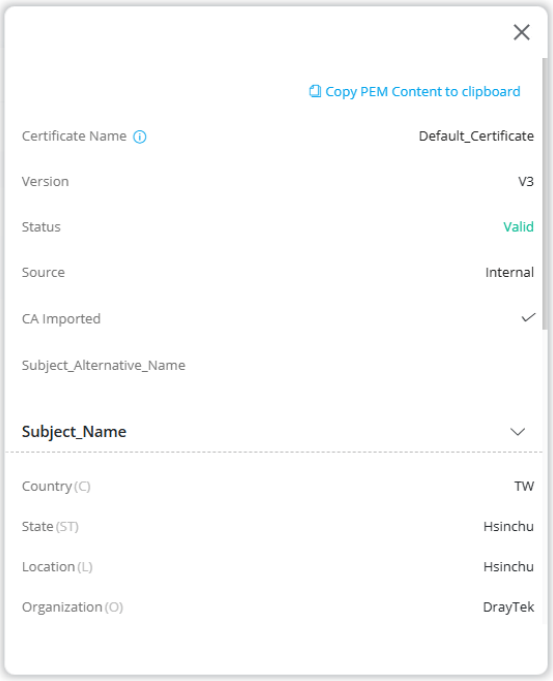
In this section, you can generate and manage local digital certificates, and import trusted CA certificates. Be sure that the system time is correct on the router so that certificates will not be erroneously considered to be invalid because of an incorrect system time falling outside of the certificate's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

## II-1-18-1 Local Certificates

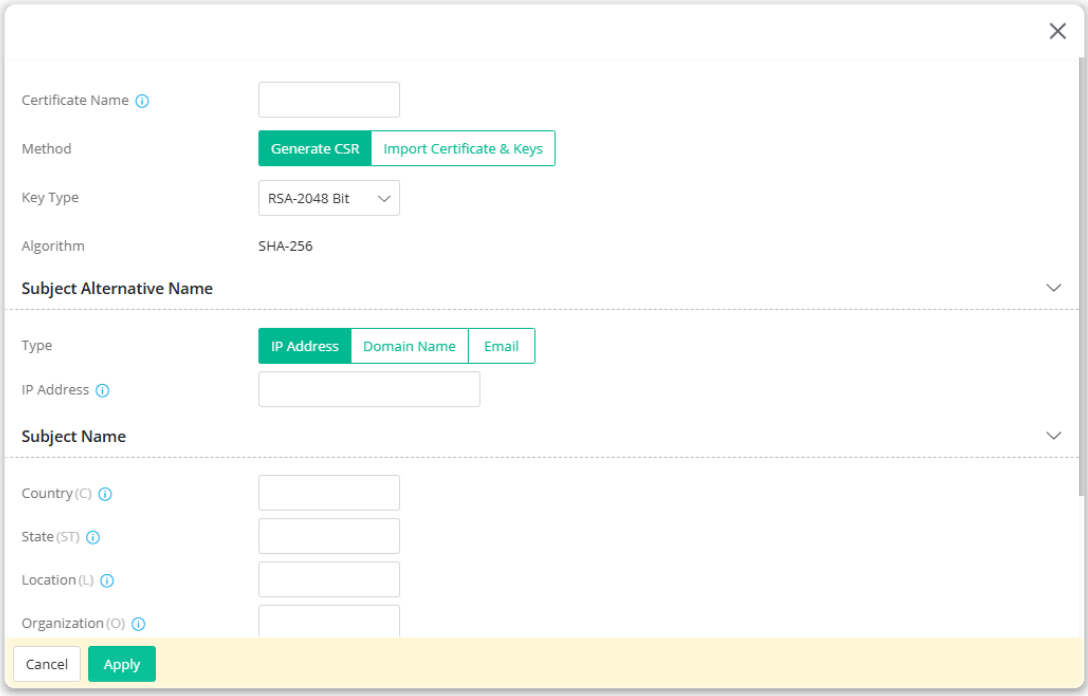
You can generate, import or view local certificates on this page.




To check detailed information of the selected certificate, click **View**.




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



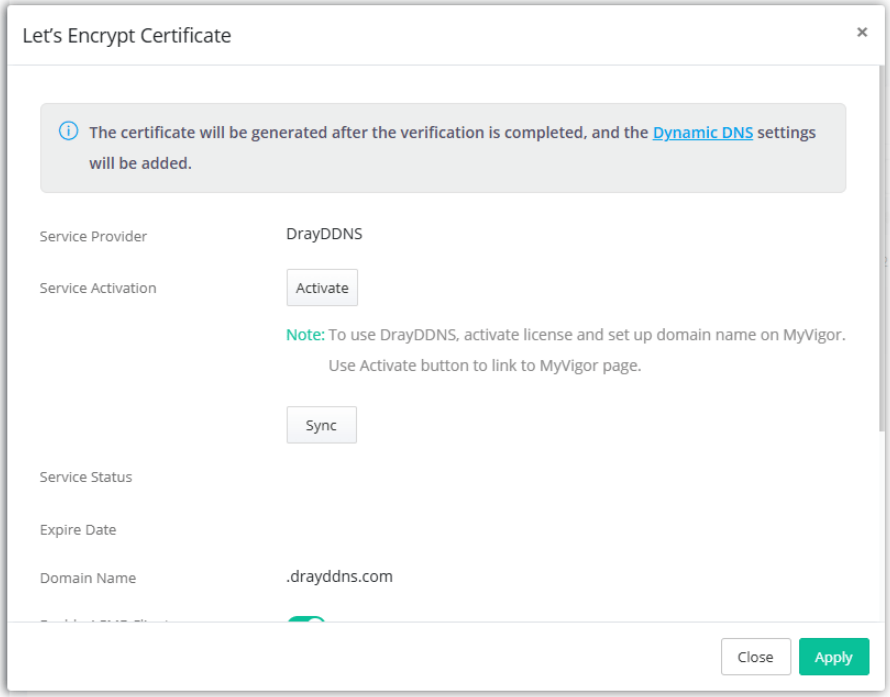

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Certificate Name** | Enter the name that identifies the certificate. |
| **Method** | **Generate CSR -** Generate a new local certificate.<br>**Import Certificate & Keys -** Vigor router 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.<br>● IP Address<br>● Domain Name<br>● 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 router 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.<br>**Certificate Only** - Local certificate.<br>● **Upload Certificate** - Click **Choose a file** to select a local certificate file.<br>**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.<br>● **Upload PKCS12 File** - Click **Choose a file** to select a PKCS12 certificate file.<br>● **Password** - Enter the password associated with the certificate and key files.<br>**Certificate & Keys** - It is useful when users have separated certificates and private keys. And the password is needed if the private key is encrypted.<br>● **Upload File** - Click **Choose a file** to select a local certificate file.<br>● **Upload Key** - Click **Choose a file** to select a key file.<br>● **Password** - Enter the password associated with the certificate and key files. |
| 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.

In addition to manually creating local certificates, you can use Let's Encrypt to generate certificates. Click the Let's Encrypt link in Configuration>>Certificates>>Local Certificates to get the following page. Here, you can use the DrayDDNS service to generate Let's Encrypt certificates. You can also view other options in Configuration>>WAN>>Dynamic DNS.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Service Provider** | Display the service provider of the Let's Encrypt Certificate. |
| **Service Activation** | **Activate** – Click to link to MyVigor web site to activate the Let's Encrypt Certificate.<br>**Sync** - The domain name for DrayDDNS is set on the MyVigor server. Click this button to load and obtain the domain name if it is available. |
| **Enable ACME Client** | Switch the toggle to generate a certificate issued by Let's Encrypt for applying to such DDNS account. |
| **More Settings** | |
| **Update DDNS with** | If a Vigor router is installed behind any NAT router, you can enable this function to locate the real WAN IP.<br>When the WAN IP used by Vigor router is private IP, this function can detect the public IP used by the NAT router and use the detected IP address for DDNS update.<br>There are two methods offered for you to choose:<br>**Internet IP** –The real public IP address will be used. Select this option if the IP address assigned to the router's WAN interface is not the actual external IP address.<br>**WAN IP** – The IP address of the router's WAN interface will be used. |
| **Update WAN IP Mode** | **Update All Selected WAN IPs** – Vigor router system will obtain the multiple WAN IPs based on the following table and upload to the service provider. |

| | |
|---|---|
| | **Update Single WAN IP by Sequence** – Vigor system will use the first selected WAN IP from the following table and upload to the service provider.<br>**+Add** – Click to create a new group of Binding Interface and Interface IP. Up to 6 sets can be created.<br>**Binding Interface** – Select the WAN interface associated with the DDNS profile.<br>**Interface IP** – Select a WAN IP. If not, the default WAN IP will be used instead. |
| **Auto Update Interval** | The frequency, in minutes, at which the router connects to DDNS servers to update IP address information.<br>The default is 14400. |
| **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.

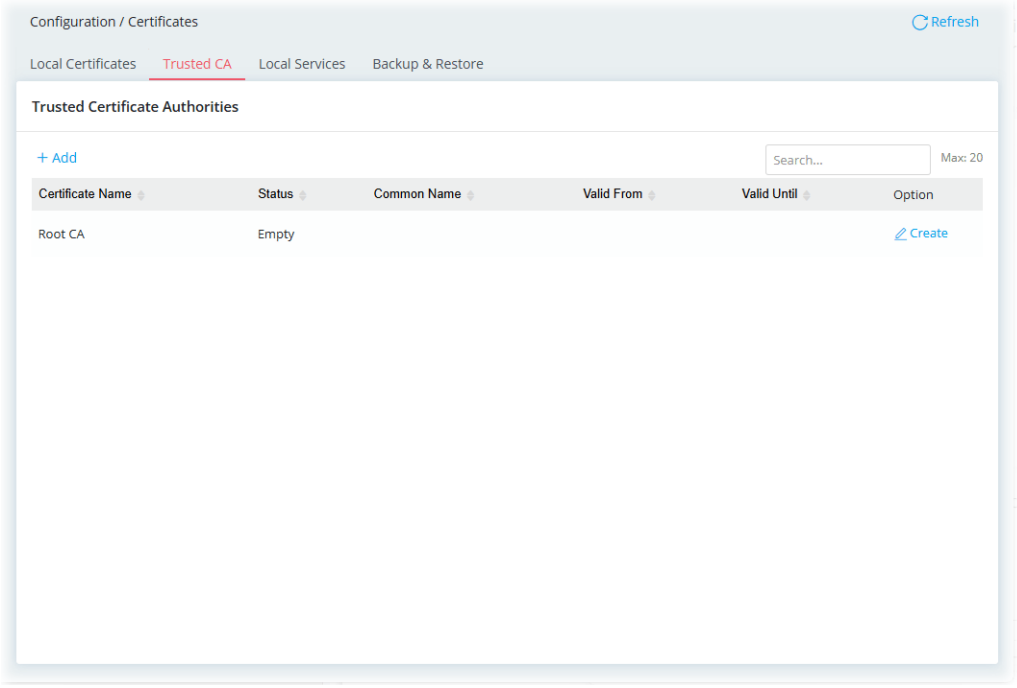
## II-1-18-2 Trusted CA

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

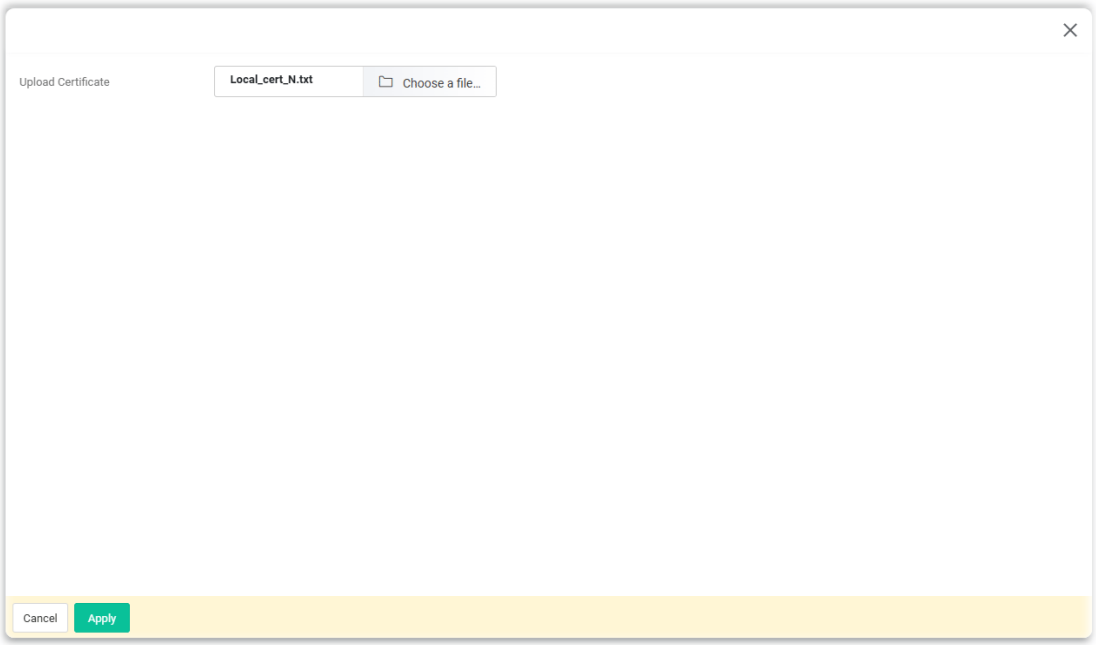
Trusted CA certificate lists three sets of trusted CA certificate. In addition, you can build a RootCA certificate if required.

When the local client and remote client are required to make certificate authentication (e.g., IPsec X.509) for data passing through SSL tunnel and avoiding the attack of MITM, a trusted root certificate authority (Root CA) will be used to authenticate the digital certificates offered by both ends.

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



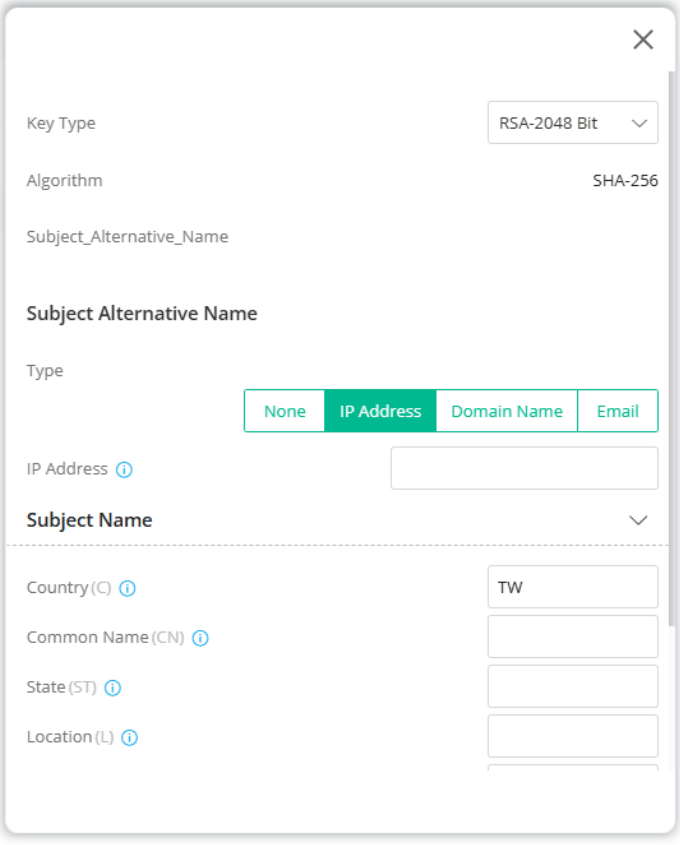

To import a RootCA to the Vigor router, click **+Add** to upload one certificate.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Upload Certificate** | **Choose a file** - Select a local certificate file. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Click to import selected certificate file to the router. |

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



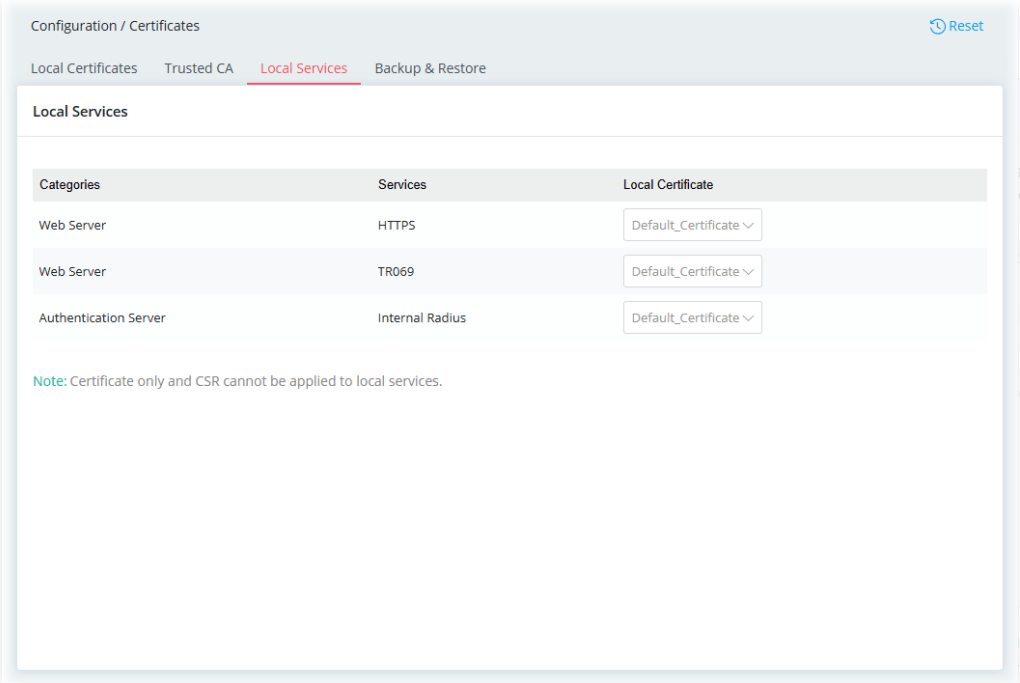
Available settings are explained as follows:

| Item | Description |
|---|---|
| **Key Type** | Displays the key type (set to RSA). |
| **Algorithm** | Displays the algorithm. |
| **Subject Alternative Name** | |
| **Type** | Vigor router accepts the type and value of the specified subject alternative name as valid authentication. Supported subject alternative types are **IP Address**, **Domain Name** and **E-Mail**.<br>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.

## II-1-18-3 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.



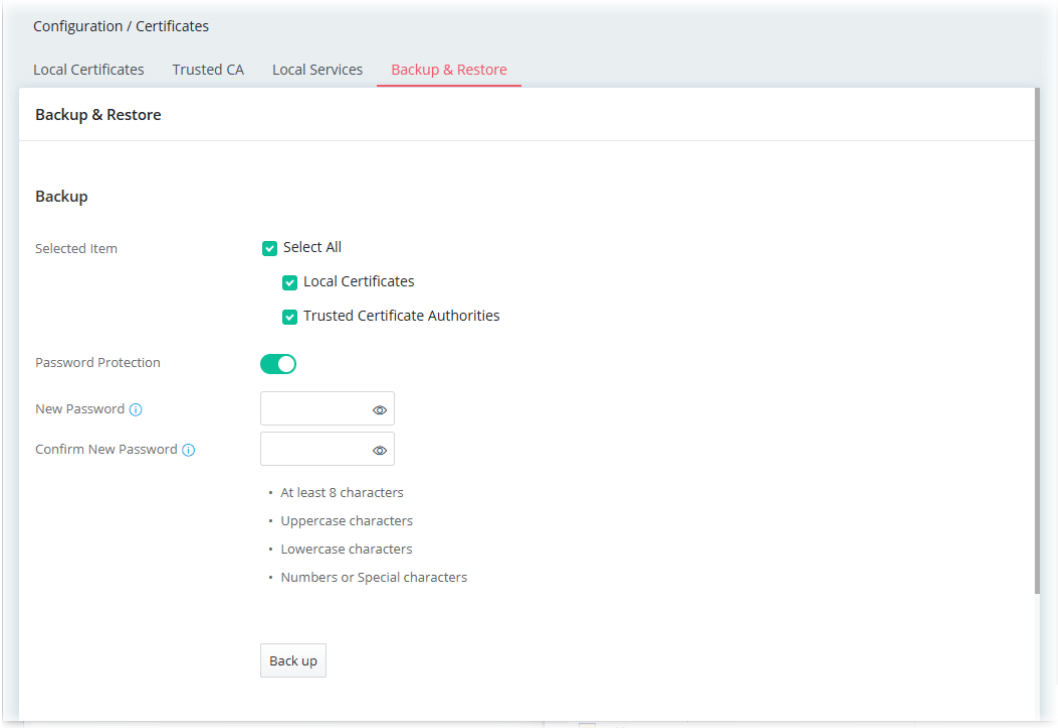

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Local Certificate** | Select a local certificate (has been imported to Vigor device) with full key and authentication information.<br>Certificate without key phrase or CSR (certificate signing request) file cannot be selected as local certificate. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings. |

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

## II-1-18-4 Backup & Restore

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




Available settings are explained as follows:

| Item | Description |
|---|---|
| | **Backup** |
| **Selected Item** | Select the certification type (local, trusted or all certificates). |
| **Password Protection** | Switch the toggle to enable or disable the function. If enabled, configure the following options.<br>● **New Password** - Enter the password with which you wish to encrypt the certificate.<br>● **Confirm New Password** - Enter the password again.<br>**Back up** - Click to download the certificate. |
| | **Restore** |
| **Restore from Backup file** | Click to select the backup file you wish to restore.<br>🗀 - Click to locate the file for restoring.<br>**Restore** - Click to retrieve the certificate. |
| **File has Password Protection** | Switch the toggle to enable or disable the function. If enabled, configure the following option.<br>● **Password** - Enter the password that was used to encrypt the certificates. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings. |

# II-2 Security

## II-2-1 Firewall Filters

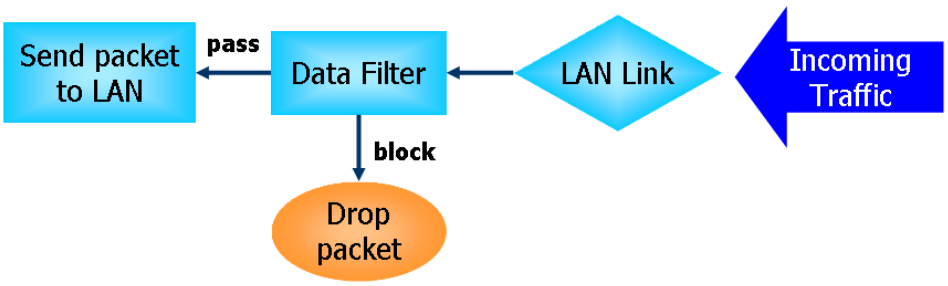
A network firewall monitors traffic travelling between networks, with the ability to selectively allow or block traffic using a predefined set of security rules. This helps to maintain the integrity of networks by stopping unauthorized access and the exchange of sensitive information.

LAN users are provided with secured protection by the following firewall facilities:

- User-configurable IP filter (Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

### Data Filter

All traffic, both incoming and outgoing, that does not trigger a PPP connection attempt (either because a PPP connection is not necessary, or the required PPP connection has already been established) is checked against the Data Filter, and will be allowed or blocked according to the rules configured within.




### Stateful Packet Inspection (SPI)

Stateful inspection is a firewall architecture that works at the network layer. Unlike legacy static packet filtering, which examines a packet based on the information in its header, stateful inspection builds up a state machine to track each connection traversing all interfaces of the firewall and makes sure they are valid. The stateful firewall of Vigor router not only examines the header information also monitors the state of the connection.

### Denial of Service (DoS) Defense

DoS attacks are categorized into two types: flooding-type attacks and vulnerability attacks. Flooding-type attacks attempts to exhaust system resources while vulnerability attacks attempts to paralyze the system by exploiting vulnerabilities of protocols or operation systems.

Vigor's DoS Defense functionality detects DoS attacks and mitigates their damage by inspecting every incoming packet, and malicious packets will be blocked. If Syslog is enabled, alert messages will also be sent. Abnormal traffic flow such as flood and port scan attacks that exceed allowable thresholds are also blocked.

The below shows the attack types that DoS/DDoS defense function can detect:

1. SYN flood attack
2. UDP flood attack
3. ICMP flood attack
4. Port Scan attack
5. IP options
6. Land attack
7. Smurf attack
8. Trace route
9. SYN fragment
10. Fraggle attack
11. TCP flag scan
12. Tear drop attack
13. Ping of Death attack
14. ICMP fragment
15. Unassigned Numbers

## II-2-1-1 URL/IP Reputation Filters

An IP Reputation Filter is a security tool that evaluates the trustworthiness of an IP address based on its historical behavior and various factors. This filter helps detect and prevent malicious activities, such as spam, hacking attempts, and other forms of cyberattacks.

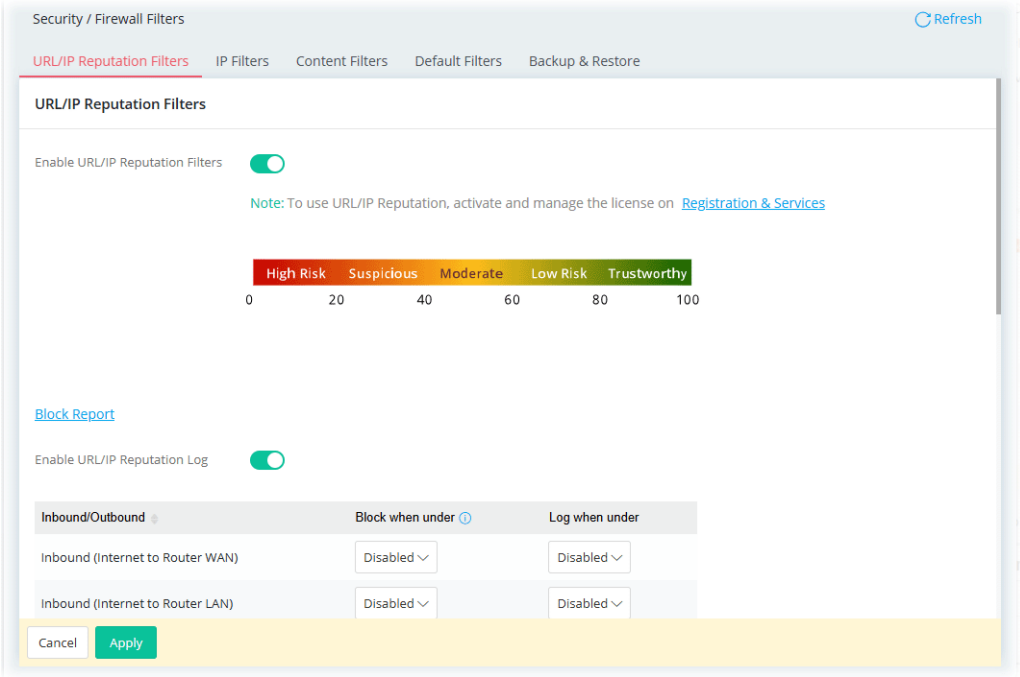
The IP Reputation Filter used by the Vigor router is designed to filter and block dangerous IP addresses. To effectively implement this filtering, three directions need to be considered as filtering conditions:

1. Inbound (from the Internet to the router's WAN)

2. Inbound (from the Internet to the router's LAN)

3. Outbound (from the LAN to the Internet)

This approach ensures comprehensive protection against harmful IP addresses.



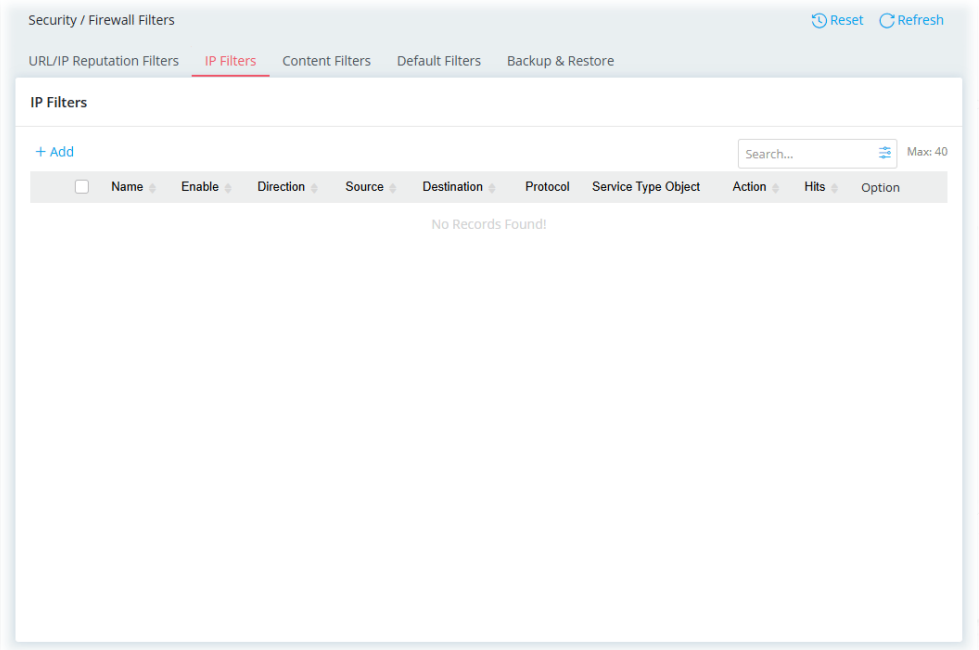

Available settings are explained as follows:

| Item | Description |
|---|---|
| IP Reputation Filters | |
| **Enable URL/IP Reputation Filters** | Switch the toggle to enable/disable this feature. |
| **Block Report** | Click to show the IP Reputation blocked report. |
| **Enable URL/IP** | Switch the toggle to enable or disable the logging function. |

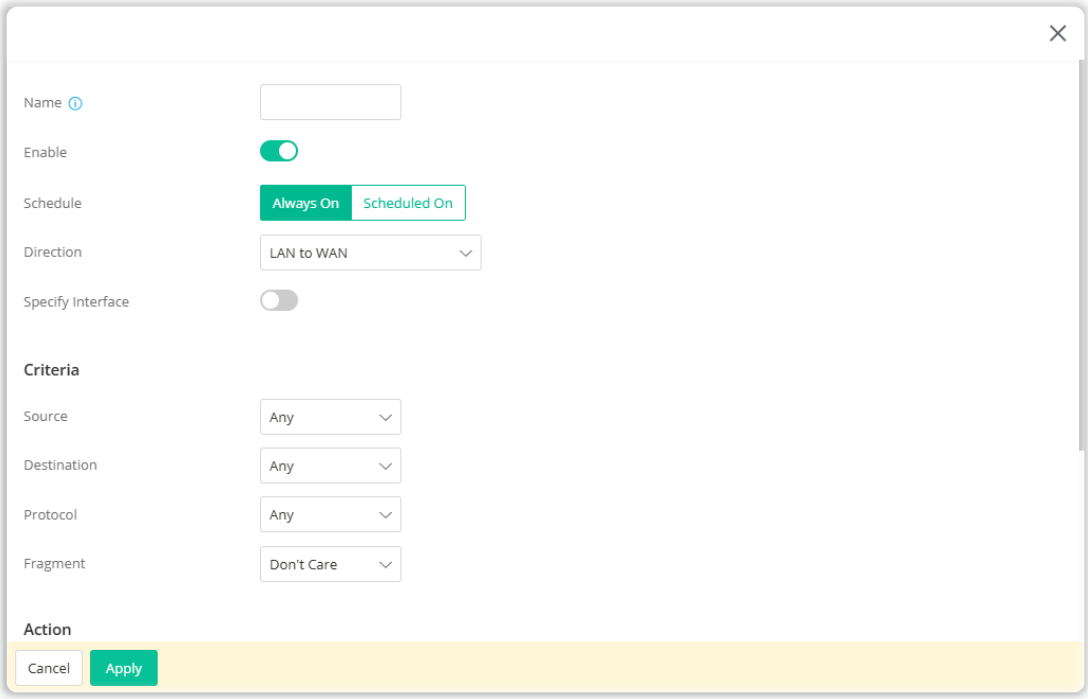
| | |
|---|---|
| Reputation Log | |
| Block when under | Select the risk level. Once the risk for the packets (incoming/outgoing) reaches the threshold (20/40/60/80) defined here, Vigor system will block the IP immediately. The default setting is "Disabled," which means that no filtering will be performed. |
| Log when under | Select the risk level. Once the risk for the packets (incoming/outgoing) reaches the percentage defined here, Vigor system will record corresponding information to the SysLog server. The default is Disabled. |
| Allow List | |
| Inbound (Internet to Router WAN) /<br>Inbound (Internet to LAN) /<br>Outbound (LAN to Internet) | IP address(es) of the clients within the allow list will not be filtered via IP Reputation Filter.<br>The direction of packet transmission includes:<br>• Inbound (Internet to Router WAN)<br>• Inbound (Internet to LAN)<br>• Outbound (LAN to Internet)<br>Click on each tab to create the allow list separately.<br>IP +Add – Click to add a new IP address as the member within the allow list.<br>• IP Address – Enter the IP address.<br>Object +Add – Click to add a new object / group as the member within the allow list.<br>• Object & Group – Use the drop-down list to specify the object & group profile.<br>Port +Add – Click to select a new service type. |
| Cancel | Discard current settings and return to the previous page. |
| Apply | Save the current settings. |

## II-2-1-2 IP Filters

Users can create access control policies and set black & white lists.



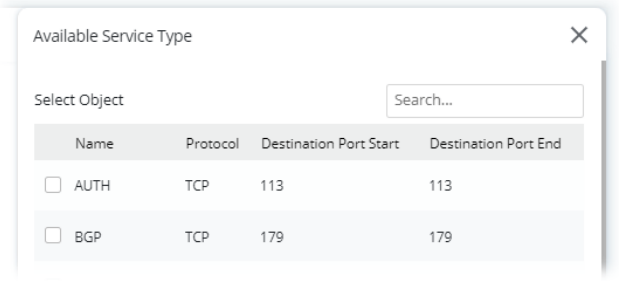

To add a new IP filter profile, click the **+Add** link to get the following page.




Available settings are explained as follows:

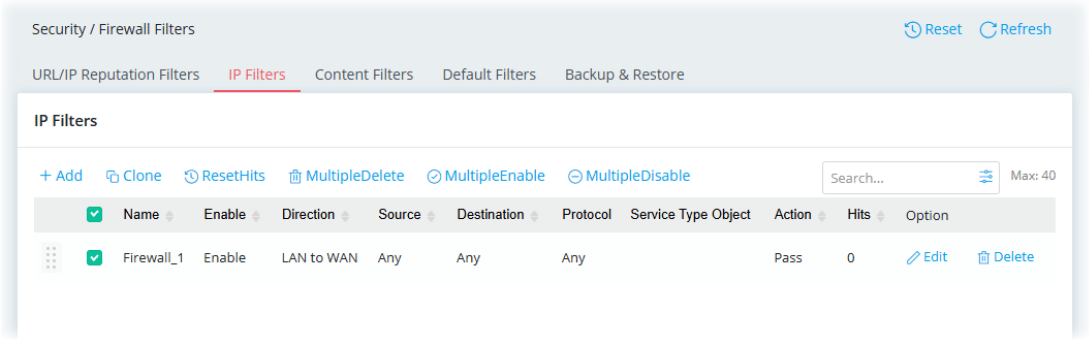
| Item | Description |
|---|---|
| **Name** | Enter a name to identify the rule. |
| **Enable** | Switch the toggle to enable/disable this profile. |
| **Schedule** | **Always On** – This rule is enabled and active for always.<br>**Scheduled On** - Select Schedule indexes to allow the rule to be |

| | |
|---|---|
| | enabled at specific times. You may choose up to 4 out of the 15 schedules in Configurations>>Objects>>Schedule. The rule is always enabled when no indexes have been selected.<br>• Clear Session when Schedule is On - Select this option to clear existing sessions when the rule is changes is enabled by a schedule profile. All connections will be reset. |
| Direction | Specify the direction of traffic flow to which this filter rule applies.<br>• LAN to WAN<br>• WAN to LAN<br>• LAN/VPN to LAN/VPN |
| Specify Interface | Switch the toggle to enable/disable the function.<br>If enabled, specify the interfaces for the traffic flow.<br>**Source Interface** – Select the LAN/VPN interface(s).<br>**Destination Interface** – Select the WAN interface(s). |
| Criteria | |
| Source | Configure the source IP addresses.<br>To set the IP address manually, please choose **Any / IPv4 Address / IPv4 Subnet / IPv6 Address / IPv6 Subnet / IP Object / IP Group / MAC Object / MAC Group** as the source and enter required information.<br>**Any** – All IP addresses<br>**IPv4 Address**–Enter the IP address.<br>• Source IPv4 Address – Click +Add to enter the IP address.<br>**IPv4 Subnet**–Enter the IP Address and the Subnet Mask.<br>• Source IPv4 Subnet Address - Click +Add to enter the IPv4 address with a subnet mask.<br>**IPv6 Address**–Enter the IPv6 address.<br>• Source IPv6 Address – Click +Add to enter the IPv6 address.<br>**IPv6 Subnet**–Enter the IPv6 Address and the prefix length.<br>• Source IPv6 Subnet Address - Click +Add to enter the IPv6 address with a subnet mask.<br>**IP Object**–Allows selection of predefined IP Objects.<br>• Source IP Object – Click +Add to select an IP object.<br>**IP Group** –Allows selection of predefined IP Groups.<br>• Source IP Group - Click +Add to select an IP group.<br>**MAC Object**–Allows selection of predefined MAC Objects.<br>• Source MAC Object – Click +Add to select an MAC object.<br>**MAC Group** –Allows selection of predefined MAC Groups.<br>Source MAC Group - Click +Add to select an MAC group. |
| Destination | Configure the destination IP addresses.<br>To set the IP address manually, please choose **Any / IPv4 Address / IPv4 Subnet / IPv6 Address / IPv6 Subnet / IP Object / IP Group** as the destination and enter required information.<br>**Any** – All IP addresses<br>**IPv4 Address**–Enter one IPv4 address.<br>• Destination IPv4 Address – Click +Add to enter the IP address.<br>**IPv4 Subnet**–Enter the IPv4 Address and the Subnet Mask.<br>• Destination IPv4 Subnet Address - Click +Add to enter the IPv4 |

| | |
|---|---|
| | address with a subnet mask.<br>**IPv6 Address**–Enter the IPv6 address.<br>• Destination IPv6 Address – Click +Add to enter the IPv6 address.<br>**IPv6 Subnet**–Enter the IPv6 Address and the prefix length.<br>• Destination IPv6 Subnet Address - Click +Add to enter the IPv6 address with a subnet mask.<br>**IP Object**–Allows selection of predefined IP Objects.<br>• Destination IP Object – Click +Add to select an IP object.<br>**IP Group** –Allows selection of predefined IP Groups.<br>• Destination IP Group - Click +Add to select an IP group.<br>**Country Object** –Allows selection of predefined Country Objects.<br>• Destination Country Object – Select the object. |
| **Protocol** | Specify the protocol(s) which this filter rule will apply to.<br>• Any<br>• Service Object<br>• TCP/UDP<br>• TCP<br>• UDP<br>• ICMP<br>• ICMPv6<br>• IGMP<br>• Others |
| **Service Type Object** | It is available when Service Object is set as the Protocol.<br>Click +Add to select the service type objects (up to 12) you want.<br> |
| **Specify Source Port** | It is available when TCP or UDP or TCP/UDP is set as the Protocol.<br>Switch the toggle to enable / disable the port settings.<br>**Source Port** – If enabled, please provide the starting and ending port values. |
| **Destination Port** | It is available when TCP or UDP or TCP/UDP is set as the Protocol.<br>To define a port range, please provide the starting and ending port values. |
| **Protocol Number** | It is available when Others is set as the Protocol.<br>Enter a value as the protocol number. |
| **Fragment** | Action to be taken for fragmented packets.<br>• **Don't care** –No action will be taken towards fragmented packets.<br>• **Unfragmented** –Apply the rule to unfragmented packets.<br>• **Fragmented** – Apply the rule to fragmented packets. |

| | |
|---|---|
| | • **Too Short** – Apply the rule only to packets that are too short to contain a complete header. |
| **Action** | |
| **Action** | Action to be taken when packets match the rule.<br>**Pass** - Packets matching the rule will be passed immediately.<br>**Block** - Packets matching the rule will be dropped immediately. |
| **Bypass Content Filter** | Switch the toggle to enable the function.<br>If enabled, Vigor router will perform the data transmission bypassing the content filter rules. |
| **Enable Syslog** | Switch the toggle to enable the recording the filter log onto SysLog. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings. |

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




Select one of the existed IP filter profile, more options will appear.

Available settings are explained as follows:

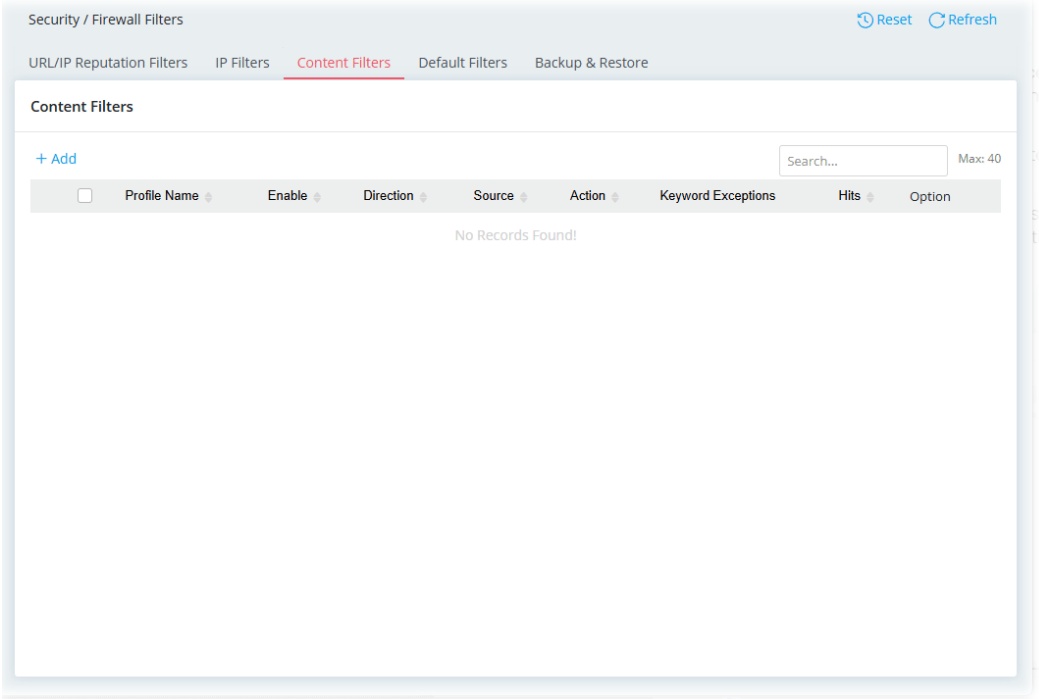
| Item | Description |
|---|---|
| **Clone** | Duplicate the selected IP filter profile with a new name. |
| **ResetHits** | Reset the number of times that each IP rule has been matched when comparing packets to the default value. |
| **MultipleDelete** | When more than one item is selected, click it to remove the items at one time. |
| **MultipleEnable** | When more than one IP filter profile is selected, click it to enable the profiles at one time. |
| **MultipleDisable** | When more than one IP filter profile is selected, click it to disable the profiles at one time. |
| **Edit** | Modify the selected IP filter profile. |
| **Delete** | Remove the selected IP filter profile. |

## II-2-1-3 Content Filters

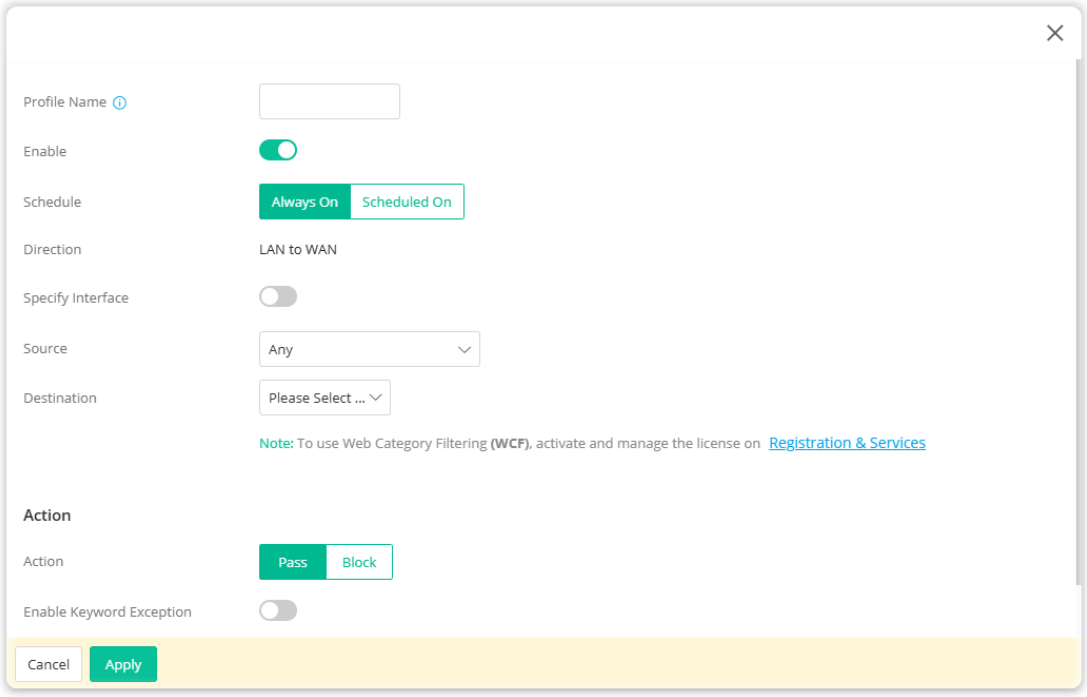
Content Filter includes APPE, URL Filter, and WCF services. APPE is filtered by defined pattern. URL and WCF filters filter the servers to connect to by examining the server name in DNS request packets or TLS client hello packets.

This page allows you to configure up to 40 content filters profiles (including APPE, URL, and WCF) previously.

Vigor router will perform the payload (content) analysis for the packets in each session (LAN to WAN) based on the filter profiles defined in this page till to find out which content filter meeting the traffic.




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



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Profile Name** | Enter a name to identify the filter profile. |
| **Enable** | Switch the toggle to enable/disable this profile. |
| **Schedule** | **Always On** – This rule is enabled and active for always.<br>**Scheduled On** - Select Schedule indexes to allow the rule to be enabled at specific times. You may choose up to 4 out of the 20 schedules in Configurations>>Objects>>Schedule.<br>• **Clear Session when Schedule is On** - Select this option to clear existing sessions when the rule is changes is enabled by a schedule profile. All connections will be reset. |
| **Direction** | Display the direction of traffic flow to which this filter rule applies. |
| **Specify Interface** | Switch the toggle to enable/disable the function.<br>If enabled, specify the interfaces for the traffic flow.<br>**Specified LAN** – Select the LAN interface(s). |
| **Source** | Configure the source IP addresses.<br>To set the IP address manually, please choose **Any / IPv4 Address / IPv4 Subnet / IPv6 Address / IPv6 Subnet / IP Object / IP Group / MAC Object / MAC Group** as the source and enter required information.<br>**Any** – All IP addresses<br>**IPv4 Address**–Enter the IP address.<br>• Source IPv4 Address – Click +Add to enter the IP address.<br>**IPv4 Subnet**–Enter the IP Address and the Subnet Mask.<br>• Source IPv4 Subnet Address - Click +Add to enter the IPv4 address with a subnet mask.<br>**IPv6 Address**–Enter the IPv6 address.<br>• Source IPv6 Address – Click +Add to enter the IPv6 address.<br>**IPv6 Subnet**–Enter the IPv6 Address and the prefix length.<br>• Source IPv6 Subnet Address - Click +Add to enter the IPv6 address with a prefix length.<br>**IP Object**–Allows selection of predefined IP Objects.<br>• Source IP Object – Click +Add to select an IP object.<br>**IP Group** –Allows selection of predefined IP Groups.<br>• Source IP Group - Click +Add to select an IP group.<br>**MAC Object**–Allows selection of predefined MAC Objects.<br>• Source MAC Object – Click +Add to select an MAC object.<br>**MAC Group** –Allows selection of predefined MAC Groups.<br>• Source MAC Group - Click +Add to select an MAC group. |
| **Destination** | Select specific WCF and/or APPE and/or UCF (keyword object) profile to be included in the filter. |
| | **Action** |
| **Action** | Action to be taken when packets match the rule.<br>**Pass** - Packets matching the rule will be passed immediately.<br>**Block** - Packets matching the rule will be dropped immediately. |
| **Enable Keyword** | Switch the toggle to enable/disable the function. |

| | |
|---|---|
| **Exception** | **Keyword Exceptions** - Displays selected keyword objects.<br>The system will check the sessions additionally with the selected keyword profile(s). If the session meets the keyword filter profile, the system will perform the action reversely. |
| **Enable Syslog** | Switch the toggle to enable the recording the filter log onto SysLog. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings. |

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

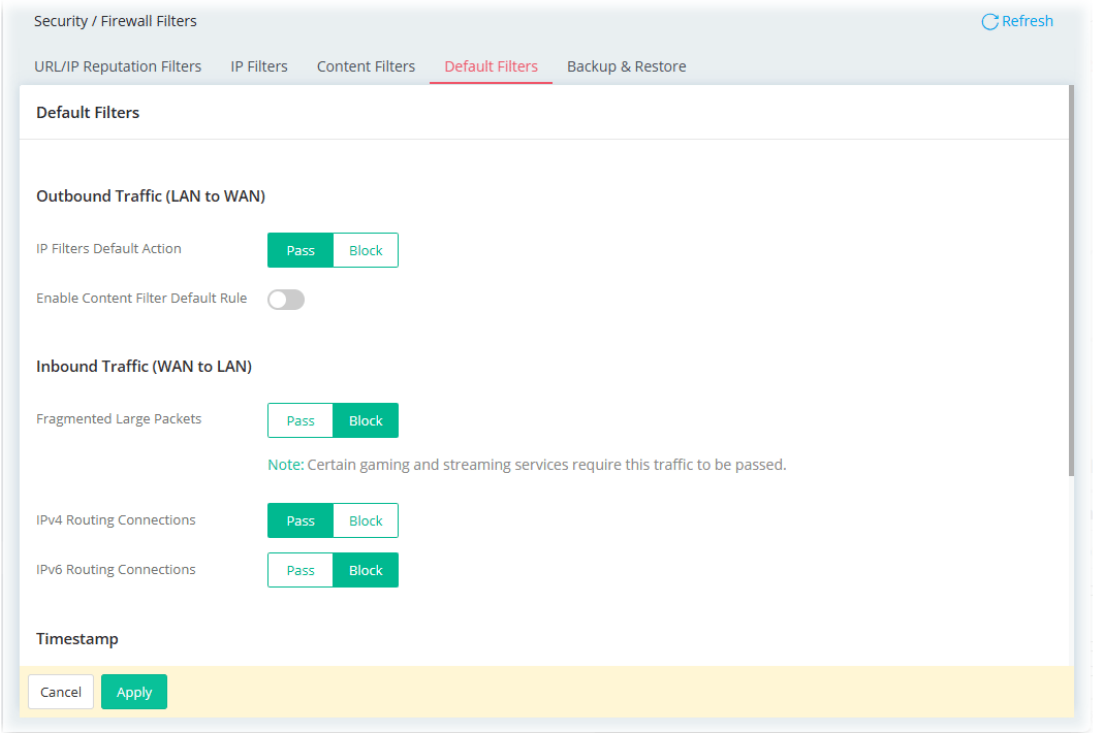
## II-2-1-4 Default Filters

Traffic is filtered by firewall functions in the following order:

1. Data Filter Sets and Rules
2. Block connections initiated from WAN
3. Default Rule

This page allows you to choose filtering profiles including QoS, Load-Balance policy, WCF, APP Enforcement, URL Content Filter, for data transmission via Vigor router.

The default rule applies to all traffic that is not constrained by other filters or rules.




Available settings are explained as follows:

| Item | Description |
|---|---|
| | **Outbound Traffic (LAN to WAN)** |
| **IP Filters Default Action** | Define the default action for the outgoing packets that do not match any IP filter rule.<br>**Pass** –The packets that do not match any IP filter rule will be passed and next wait for the content filter. |

| | |
|---|---|
| | **Block** – The packets that do not match any IP filter rule will be blocked by Vigor system. |
| **Enable Content Filter Default Rule** | Switch the toggle to enable or disable the function. |
| **Content Filters Default Rule** | Define the default action for the outgoing traffic that match the following Content Destination rule.<br>If the outgoing traffic doesn't match any IP/content filter rule and the **IP Filters Default Action** is PASS, it will be checked with this rule additionally.<br>If the outgoing traffic meets the above conditions but still doesn't meet the following Content Destination rules, the system will perform the action reversely.<br>**Pass** –The outgoing traffic that matches the following Content Destination rule will be passed. Otherwise, it will be blocked.<br>**Block** – The outgoing traffic that matches the following Content Destination rule will be blocked. Otherwise, it will be allowed to pass through. |
| **Content Destination** | Select specific WCF and/or APPE and/or UCF(keyword object) profile to be included in the filter. |
| **Inbound Traffic (WAN to LAN)** | |
| **Fragmented Large Packets** | Certain games and video streaming service use fragmented UDP packets to transfer data.<br>**Pass** - The router always passes fragmented packets without reassembling them, regardless of the size of the packet.<br>**Block** - The router will attempt to reassemble fragmented packets up to a certain value (e.g., 15xx~2102) kilobytes long. Packets larger than the certain value will be discarded. |
| **IPv4 Routing Connections** | **Pass** – For LAN hosts receiving WAN IPv4 addresses using the IP routed subnet, select this option to prevent WAN hosts from connecting to LAN hosts. This option has no effect on LAN hosts on private LAN subnets.<br>**Block** - Block the LAN hosts from connecting to WAN hosts using IPv4. |
| **IPv6 Routing Connections** | **Pass** – IPv6 does not make use of Network Address Translation (NAT), so all LAN hosts receive public IPv6 IP addresses that are exposed to the WAN.<br>**Block** - Block the WAN hosts from connecting to LAN hosts using IPv6. |
| **Timestamp** | |
| **ICMP Timestamp** | Protocols that expose system time information may unintentionally reveal predictable external information.<br>To minimize this risk, it is recommended to block ICMP Timestamp message types if required.<br>**Pass** – Allow the ICMP Timestamp messages packets to pass through the interface.<br>**Block** – Drop the ICMP Timestamp messages packets to prevent potential information disclosure. |
| **TCP Timestamp** | The TCP Timestamp may expose system uptime, which could assist attackers inferring timing information.<br>To minimize this risk, it is recommended to block TCP Timestamp |

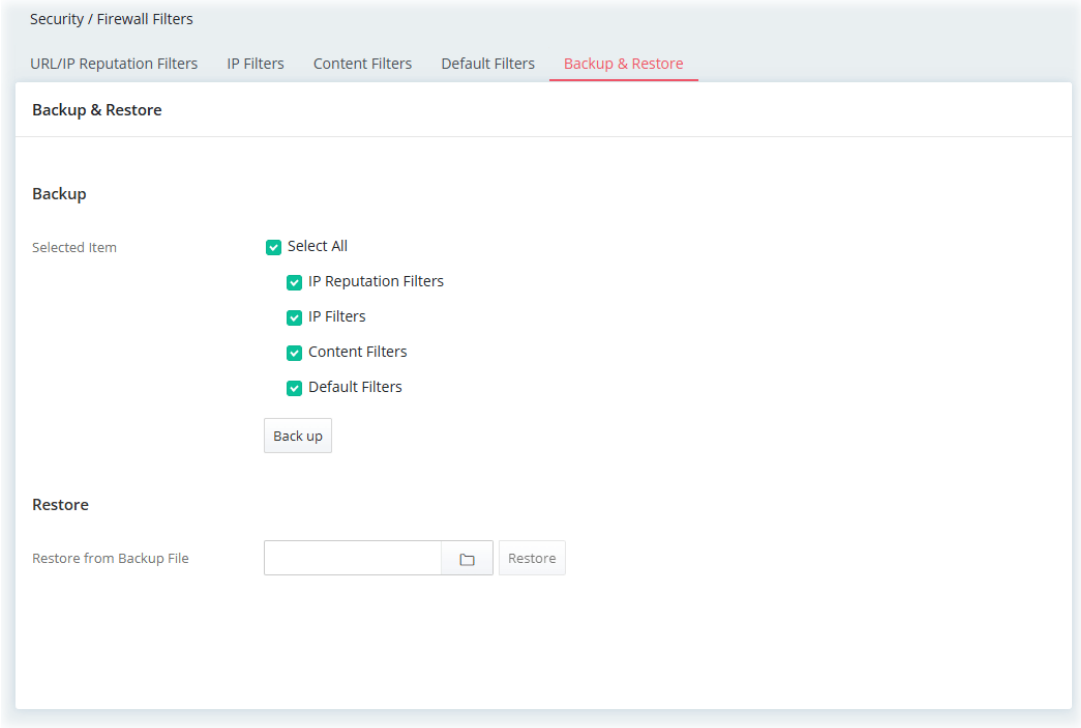
| | |
|---|---|
| | options if required.<br>**Pass** – Allow the TCP Timestamp message packet types passing through the interface.<br>**Block** - Block the TCP Timestamp message to prevent potential information disclosure. |
| **Syslog** | **Enable Syslog** – If enabled, the log related to default filter will be recorded to Syslog. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings. |

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

## II-2-1-5 Backup & Restore

This page allows the backup and restoration of router settings.

In addition to restoring Vigor2136's own configuration backup, it is possible to restore backups from certain DrayTek routers on Vigor2136.



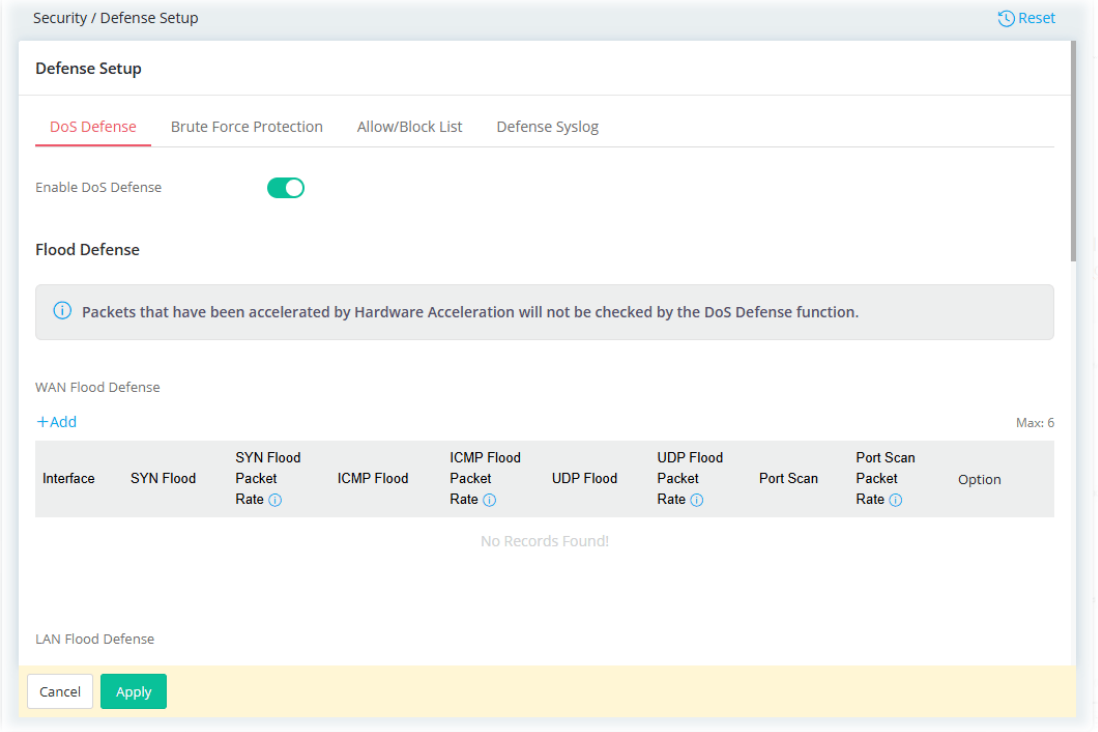

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Backup** | **Selected Items** – Select the item(s).<br>**Backup** - Perform the configuration backup of this router based on the item (Selected All, IP Filters, Content Filters and Default Filters) selected above. |
| **Restore** | **Restore from Backup File** – Click the button to specify a file to be restored<br>**Restore** - Click to initiate restoration of configuration. If the backup file is encrypted, you will be asked to enter the password. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings. |

# II-2-2 Defense Setup

## II-2-2-1 DoS Defense

As a sub-functionality of IP Filter/Firewall, there are several types of detect / defense function in the **DoS Defense** setup. In default, the DoS Defense is disabled.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable DoS Defense** | Switch the toggle to enable/disable the DoS Defense. |
| | **Defense Setup** |
| **Flood Defense** | **+Add** – Click it set profiles for flood defense. Up to 6 profiles can be created.<br>**Interface** – Select a WAN interface. Set the packet rate values for WAN to meet your request.<br>**SYN Flood** – Switch the toggle to enable/disable SYN flood defense. When the arrival rate of SYN packets exceeds the Threshold value, the router will start to randomly discard TCP SYN packets for a period of time as defined in Timeout. This is to prevent TCP SYN packets from exhausting router resources.<br>• **SYN Flood Packet Rate** – The default values of threshold and timeout are 2000 packets per second and 10 seconds, respectively.<br>**ICMP Flood** – Switch the toggle to enable/disable the ICMP flood defense. When the arrival rate of ICMP packets exceeds the Threshold value, the router will start to randomly discard TCP SYN packets for a period of time as defined in Timeout.<br>• **ICMP Flood Packet Rate** – The default values of threshold and timeout are 250 packets per second and 10 seconds, |

| | |
|---|---|
| | respectively.<br>**UDP Flood** – Switch the toggle to enable/disable UDP flood defense. When the arrival rate of UDP packets exceeds the Threshold value, the router will start to randomly discard TCP SYN packets for a period of time as defined in Timeout.<br>• **UDP Flood Packet Rate** – The default values of threshold and timeout are 5000 packets per second and 10 seconds, respectively.<br>**Port Scan** – Switch the toggle to enable/disable the Port Scan detection. Port Scans attack your network by sending packets to a range of ports in an attempt to find services that would respond. When Port Scan detection is enabled, the router sends warning messages when it detects port scanning activities that exceed the Threshold rate.<br>• **Port Scan Packet Rate** – The default threshold is 2000 packets per second.<br>**Option (Edit/Delete)** – Click **Edit** to open the setting page to modify in detail (packet rate and burst rate). Click **Delete** to remove the selected entry. |
| LAN Flood Defense | **Interface** – It contains LAN/VLAN and VPN. In which the default packet rate values for LAN/VLAN are the same as WAN flood defense, and will take effect for all LAN interfaces within a VLAN. The packet rate values for VPNs will be effective for LAN interfaces used for VPN. Set the packet rate values for LAN/VLAN and VPN accordingly.<br>**SYN Flood** – Switch the toggle to enable/disable SYN flood defense. When the arrival rate of SYN packets exceeds the Threshold value, the router will start to randomly discard TCP SYN packets for a period of time as defined in Timeout. This is to prevent TCP SYN packets from exhausting router resources.<br>• **SYN Flood Packet Rate** – The default values of threshold and timeout are 2000 packets per second and 10 seconds, respectively.<br>**ICMP Flood** – Switch the toggle to enable/disable the ICMP flood defense. When the arrival rate of ICMP packets exceeds the Threshold value, the router will start to randomly discard TCP SYN packets for a period of time as defined in Timeout.<br>• **ICMP Flood Packet Rate** – The default values of threshold and timeout are 250 packets per second and 10 seconds, respectively.<br>**UDP Flood** – Switch the toggle to enable/disable UDP flood defense. When the arrival rate of UDP packets exceeds the Threshold value, the router will start to randomly discard TCP SYN packets for a period of time as defined in Timeout.<br>• **UDP Flood Packet Rate** – The default values of threshold and timeout are 5000 packets per second and 10 seconds, respectively.<br>**Port Scan** – Switch the toggle to enable/disable the Port Scan detection. Port Scans attack your network by sending packets to a range of ports in an attempt to find services that would respond. When Port Scan detection is enabled, the router sends warning messages when it detects port scanning activities that exceed the Threshold rate.<br>• **Port Scan Packet Rate** – The default threshold is 2000 packets per second. |

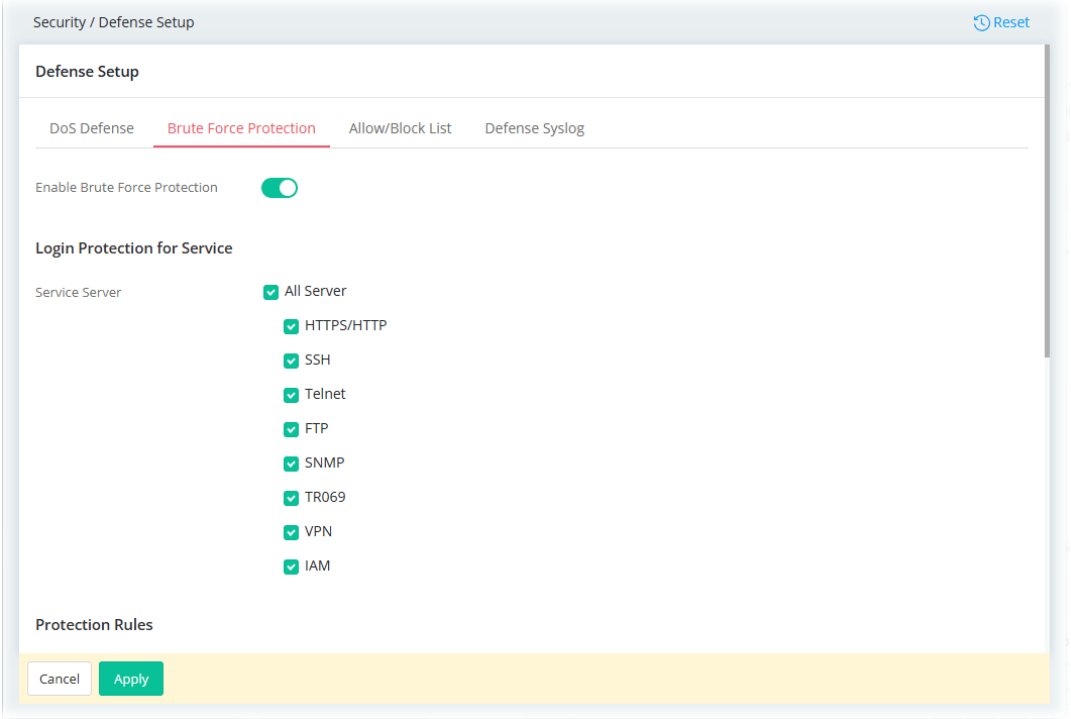
| | |
|---|---|
| | **Option (Edit/Delete)** – Click **Edit** to open the setting page to modify in detail (packet rate and burst rate). Click **Delete** to remove the selected entry. |
| General | Switch the toggle to enable/disable the function listed below.<br>**Block IP Options** – If enabled, the Vigor router will ignore IP packets with IP option field set in the datagram header. IP options are rarely used and could be abused by attackers as they carry information about the private network otherwise not available to the external network, such as security, TCC (closed user group) parameters, a series of Internet addresses, routing messages, etc, which external eavesdroppers can use to discover details about the private network.<br>**Block Land** – Enable to block LAND attacks. LAND attacks happen when an attacker sends spoofed SYN packets with both source and destination addresses set to that of the target system, which causes the target to reply to itself continuously.<br>**Block SMURF** – Enable to block Smurf attacks. The router will ignore any broadcasting ICMP echo request.<br>**Block Trace Route** – Enable to block traceroutes. The router will not forward traceroute packets.<br>**Block SYN Fragment** – Enable to block SYN packet fragments. The router will drop any packets having both the SYN and more-fragments bits set.<br>**Block Fraggle** – Enable to block Fraggle Attacks. Broadcast UDP packets received from the Internet are blocked.<br>Activating this feature might block some legitimate packets. Since all broadcast UDP packets coming from the Internet are blocked, RIP packets from the Internet could also be dropped.<br>**Block Tear Drop** – Enable to block Tear Drop attacks. Some clients may crash when they receive ICMP datagrams (packets) that exceed the maximum length. The router discards any fragmented ICMP packets having lengths greater than 1024 octets.<br>**Block Ping of Death** – Enable to block Ping of Death, where fragmented ping packets are sent to target hosts so that those hosts could crash as they reassemble the malformed ping packets.<br>**Block ICMP Fragment** – Enable to block ICMP Fragments. ICMP packets with the more-fragments bit set are dropped.<br>**Block Unknown Protocol** – Enable to block Unassigned Protocol Numbers, and the router will block packets having unassigned protocol numbers. Individual IP packet has a protocol field in the datagram header to indicate the protocol type running over the upper layer. However, the protocol types greater than 100 are reserved and undefined at this time. Therefore, the router should have ability to detect and reject this kind of packets. |
| ARP Spoofing Defense | |
| Block ARP replies with | This feature can protect a network from ARP (Address Resolution Protocol) spoofing attacks.<br>**Inconsistent Source MAC addresses** – If the sender's MAC address in the ARP packets does not match the source MAC address from ARP packet's ethernet header, the Vigor system will block the packets immediately.<br>**Inconsistent Destination MAC addresses** - If the target MAC address in the ARP packets does not match the destination MAC |

| | |
|---|---|
| | address from ARP packet's ethernet header, the Vigor system will block the packets immediately. |
| **Virtual MAC Address in ARP Table (VRRP)** | **Accept** – The virtual MAC address can be recorded in the ARP table.<br>**Decline** –The virtual MAC address cannot be recorded in the ARP table. |
| **IP Spoofing Defense** | |
| **Block IP Packets with** | IP spoofing defense can prevent unauthorized access and then protect the data integrity to make sure the security of network.<br>**Inconsistent Source IP addresses from WAN** – Blocks the fake IP from WAN. For example, if the source IP address from the WAN interface is LAN subnet IP packets, the Vigor system will block the packets immediately.<br>**Inconsistent Source IP addresses from LAN** – Blocks the fake IP from LAN. For example, if the source IP address from the LAN interface is WAN subnet IP packets, the Vigor system will block the packets immediately. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings. |

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

## II-2-2-2 Brute Force Protection

Any client trying to access into Internet via Vigor router will be asked for passing through user authentication. Such feature can prevent Vigor router from attacks when a hacker tries every possible combination of letters, numbers and symbols until find out the correct combination of password.




Available settings are explained as follows:

| Item | Description |
|---|---|

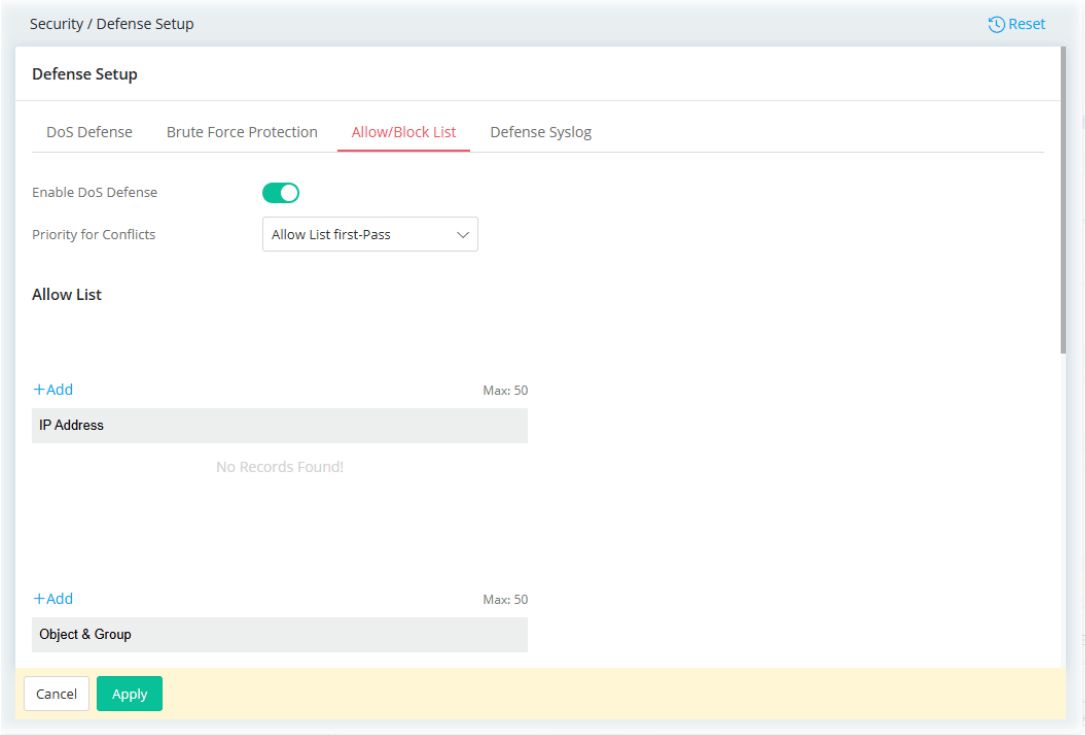
| | |
|---|---|
| Enable Brute Force Protection | Switch the toggle to enable or disable the detection of brute force login attempts. |
| Login Protection for Service | |
| Service Server | BFP can protect the Vigor router's login feature from hacker attacks attempting to crack accounts and passwords through protocols such as HTTPS/HTTP, SSH, Telnet, FTP, SNMP, TR-069, VPN, IAM, and more.<br>The default setting is **All Server**. |
| Protection Rules | |
| IAM Users | Define the protection rules for IAM users (e.g., using FTP and IAM service.<br>**Enable** –Switch the toggle to enable or disable the defense setup settings for the IAM users.<br>**Maximum Login Attempts** – Specify the maximum number of failed login attempts before further login is blocked.<br>The users who fail to log in multiple times by reaching the maximum login attempts will be penalized a period not to login Vigor system (e.g., using FTP and IAM Service).<br>**Penalty Period** – Set the period for penalty delay.<br>During this period, the user cannot log in. This setting aims to prevent outside automated attacks that attempt to guess passwords, authentication codes, or other credentials through repeated trials.<br>**Enable User Account Lockout** – Switch the toggle to enable or disable the IAM users account lockout function.<br>**Login Attempts** – Set a maximum number of failed login attempts for all user accounts. After reaching this limit, the IAM user account will be locked if login fails (e.g., through FTP or IAM Service).<br>**Unlock User Account After** – Set a time period to unlock specific IAM user accounts.<br>**Email Notification** – Send a notification to the account via an e-mail when lockout event happened to the user. |
| VPN | Define the protection rules for VPN connection.<br>**Enable** –Switch the toggle to enable or disable the defense setup settings for the VPN connection.<br>**Maximum Login Attempts** – Specify the maximum number of failed login attempts before further login is blocked.<br>The users who fail to log in multiple times by reaching the maximum login attempts will be penalized a period not to login Vigor system.<br>**Penalty Period** – Set the period for penalty delay.<br>During this period, the user is unable to log in or access Vigor's system. This setting aims to prevent outside automated attacks that attempt to guess passwords, authentication codes, or other credentials through repeated trials.<br>**Email Notification** - Send a notification to the account via an e-mail when lockout event happened to the user. |
| System Account | Define the protection rules for the system account (User and Administrator).<br>**Enable** – Switch the toggle to enable or disable the defense setup settings for the system account. |

| | |
|---|---|
| | **Maximum Login Attempts** – The System Accounts who fail to log in multiple times by reaching the maximum login attempts will be penalized a period not to login Vigor system (e.g., using HTTPS/HTTP, SSH, Telnet, SNMP, and TR069 Service).<br>**Penalty Period** – Set the period for penalty delay.<br>During this period, the user is unable to log in or access Vigor's system. This setting aims to prevent outside automated attacks that attempt to guess passwords, authentication codes, or other credentials through repeated trials.<br>**Enable User Account Lockout** –Switch the toggle to enable or disable the System Account lockout function.<br>**Login Attempts** – Specify the maximum number of failed login attempts for all System Accounts. After that, the System Accounts will be locked if login failed (e.g., logging into HTTPS/HTTP, SSH, Telnet, SNMP, and TR-069 Service).<br>**Unlock User Account After** – Specify a time period to unlock specific system account.<br>**Email Notification** - Send a notification to the account via an e-mail when lockout event happened to the user. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings. |

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

## II-2-2-3 Allow/Block List

Define the white list and the black list for the clients.




Available settings are explained as follows:

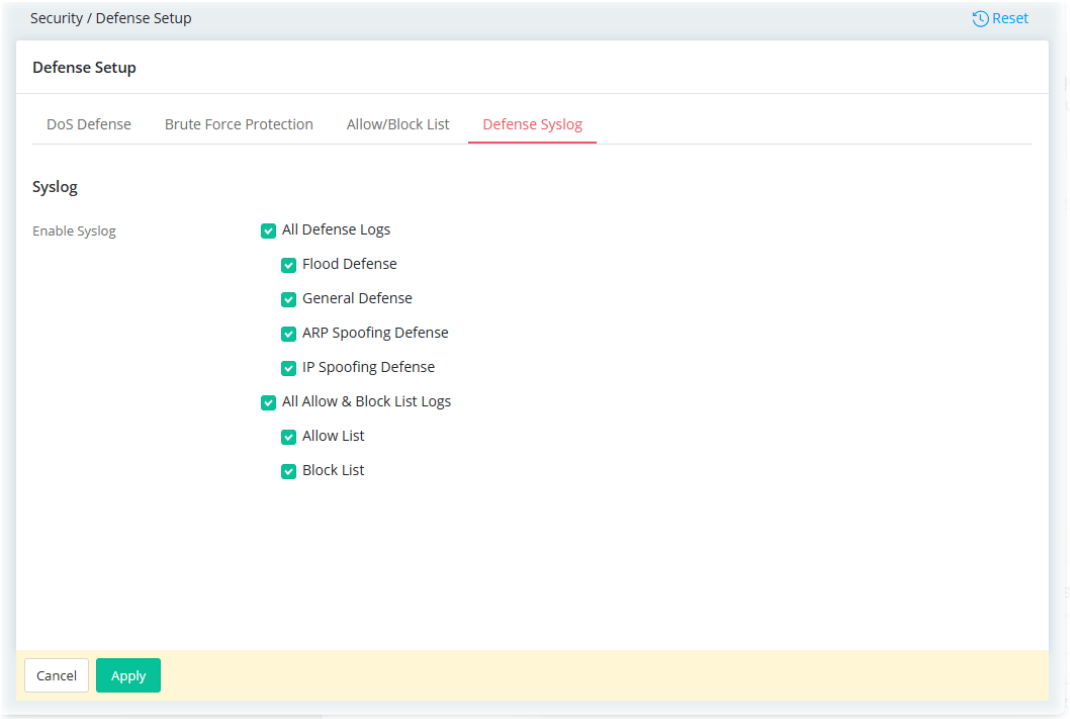
| Item | Description |
|---|---|
| **Enable DoS Defense** | Switch the toggle to enable or disable the DoS Defense function. |

| | |
|---|---|
| **Priority for Conflicts** | Define the processing order/priority for the conflicts.<br>• **Allow List first-Pass** – Let the IP address listed on the Allow List pass through first.<br>• **Block List first-Block** – Block the IP address listed on the Block List pass through first. |
| **Allow List** | Define the IP address(es) of the clients that the packets can be received / delivered via Vigor router.<br>**+Add** – Click to add a new IP address as the member within the allow list.<br>• **IP Address** – Enter the IP address.<br>**+Add** – Click to add a new object / group as the member within the allow list.<br>• **Object & Group** – Use the drop-down list to specify the object & group profile. |
| **Block List** | Define the IP address(es) of the clients that will be blocked by Vigor router.<br>**+Add** – Click to add a new IP address as the member within the allow list.<br>• **IP Address** – Enter the IP address.<br>**+Add** – Click to add a new object / group as the member within the allow list.<br>• **Object & Group** – Use the drop-down list to specify the object & group profile. |
| **Apply** | Save the current settings. |

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

## II-2-2-4 Defense Syslog

Display the type of Syslog provided by Vigor router. Corresponding information related to operation, status, and defense to Vigor router will be recorded to the Syslog server.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable Syslog** | Select the feature(s). Operation procedure, result or any information related to the feature will be recorded to the Syslog server. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings. |

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

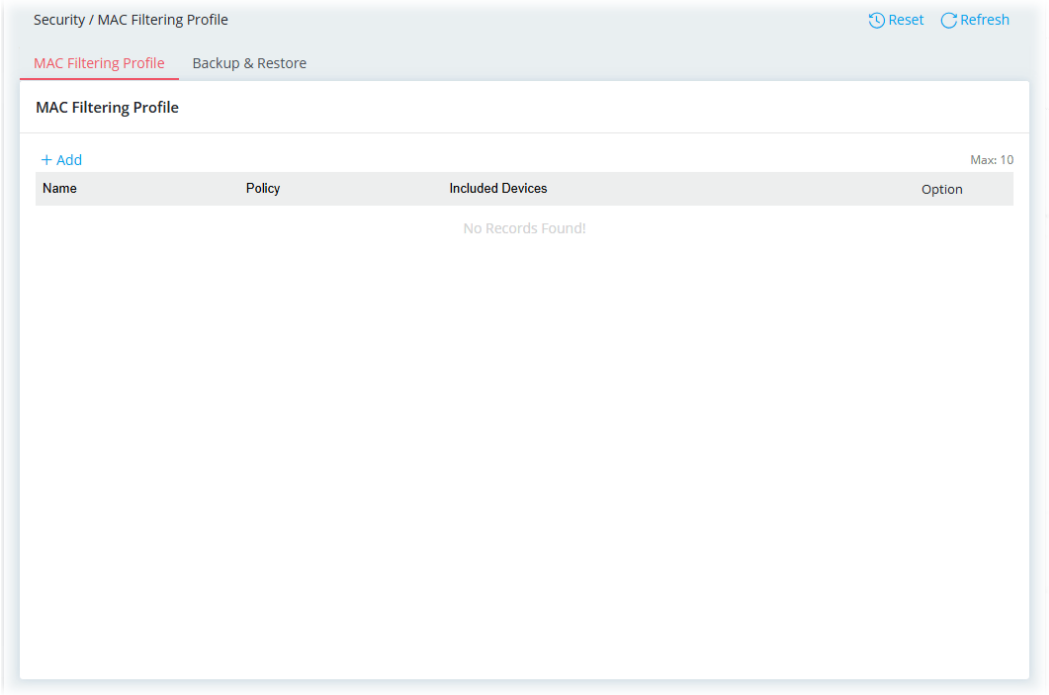
# II-2-3 MAC Filtering Profile

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

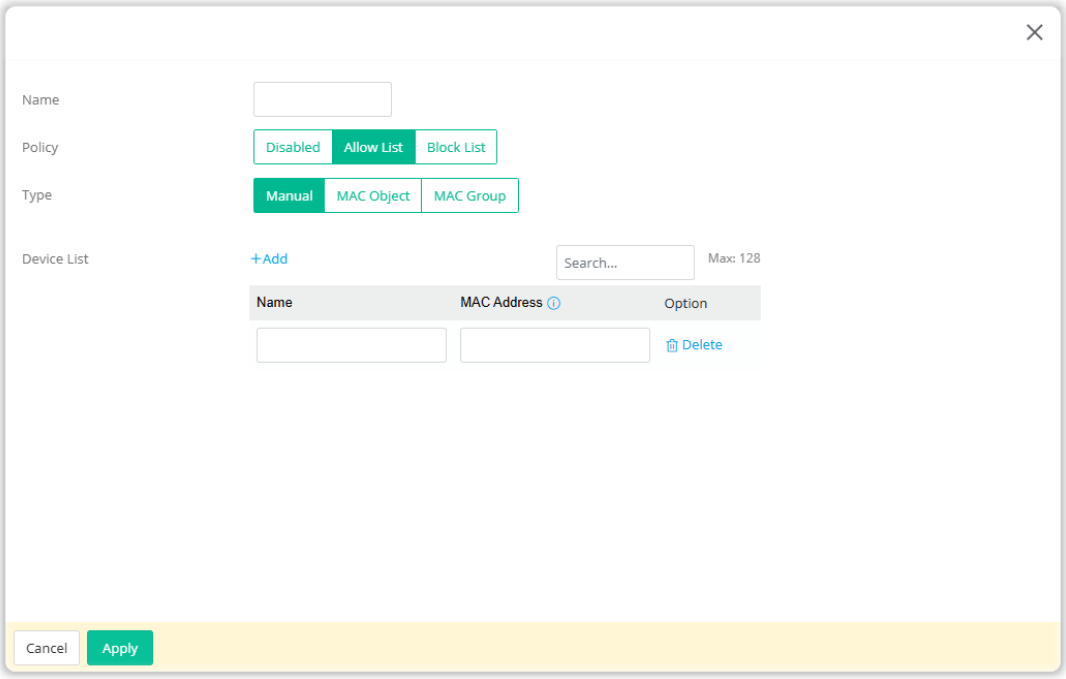
The router's administrator may block wireless clients by inserting their MAC addresses into a black list, or only allow some wireless clients to connect by inserting their MAC addresses into a white list.

## II-2-3-1 MAC Filtering Profile

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.




To add a new profile, click +Add.




Available settings are explained as follows:

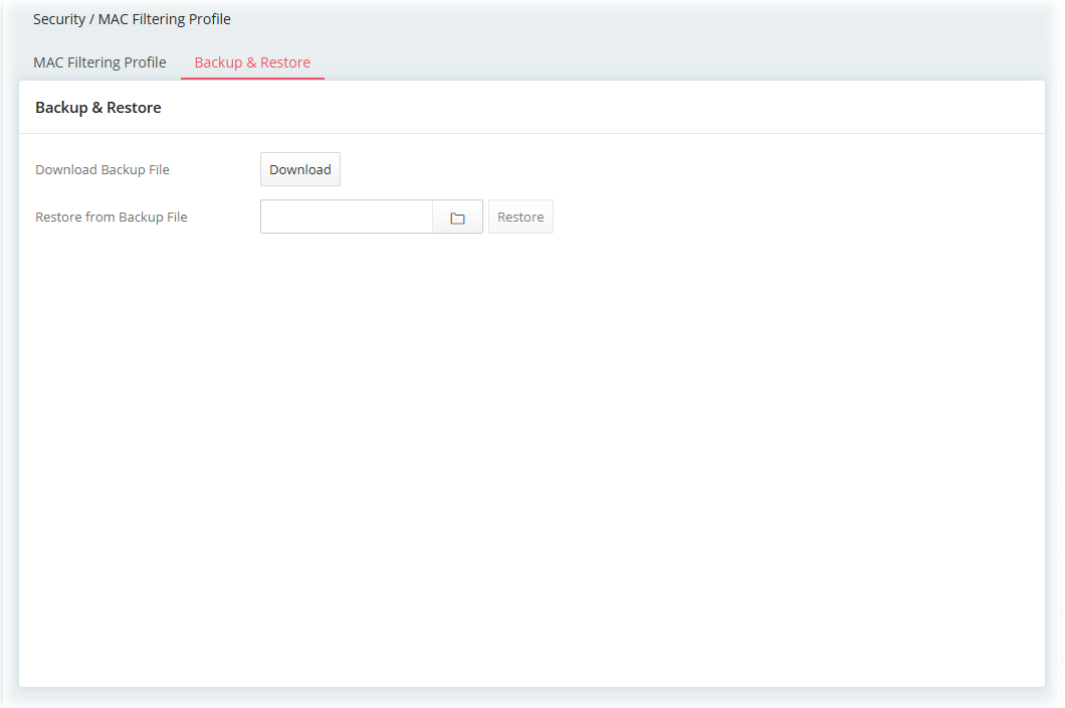
| Item | Description |
|---|---|
| **Name** | Enter a string as the profile name. |
| **Policy** | **Disabled** – Disable this policy.<br>**Allow List** – Only allow wireless clients whose MAC addresses are listed in the Device list.<br>**Block List** - Only allow wireless clients whose MAC addresses 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.<br>**MAC Object –** Select the MAC object(s). All the MAC address under the MAC object will be allowed or blocked.<br>**MAC Group –** Select the MAC group(s). All the MAC objects under the MAC group will be allowed or blocked. |
| **Device List** | **+Add** – Click to add a new device by entering the device name and the MAC address. |
| **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-2-3-2 Backup & Restore

This page allows the backup and restoration of MAC filtering profile settings.

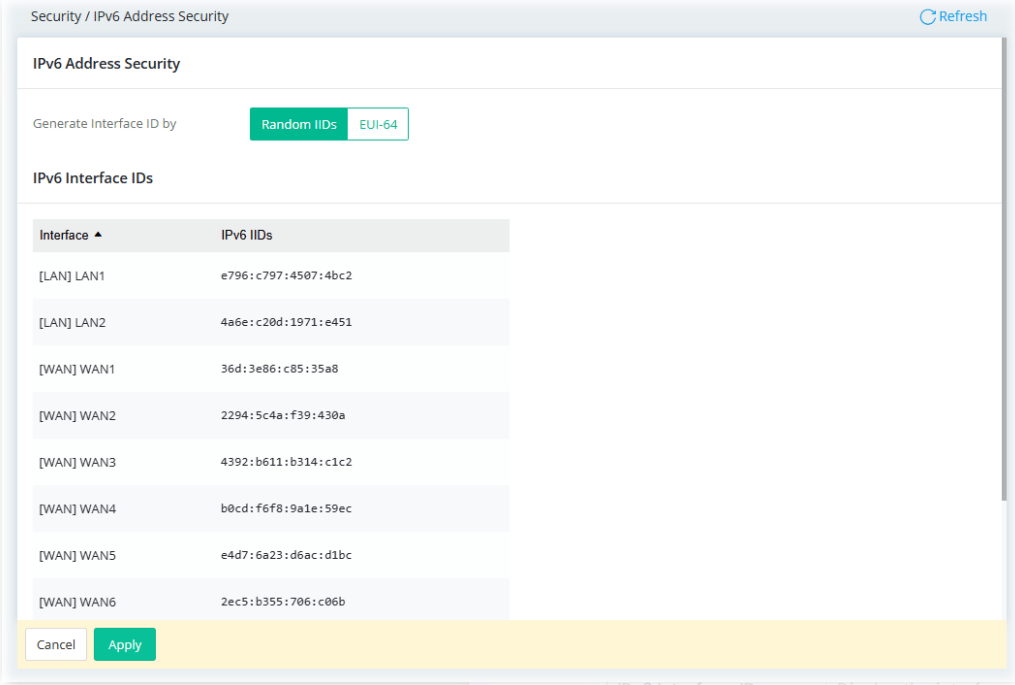



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Download Backup File** | Click to save current configurations for MAC Filtering Profile. |
| **Restore from Backup File** | - Click to locate the file for restoring.<br>**Restore** – Click to execute the restoration. |

# II-2-4 IPv6 Address Security

This page allows you to configure the IPv6 interface ID.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Generate Interface ID by** | Select to use Random IIDs or EUI-64 IIDs as the interface ID.<br>• **Random IIDs**<br>• **EUI-64** |
| **IPv6 Interface ID** | Display the interface and corresponding IPv6 IIDs. |
| **Regenerate Random Interface IDs** | **Regenerate** - Re-generate the random IIDs for all interfaces. |
| **Cancel** | Discard current settings. |
| **Apply** | Save the current settings. |

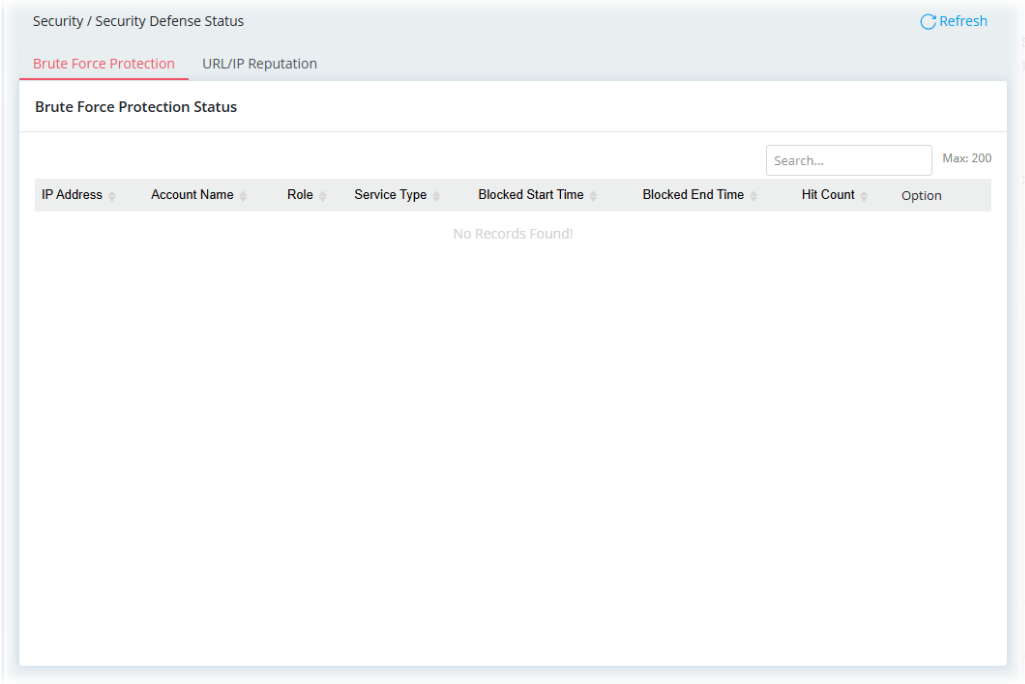
After finishing this web page configuration, please click **Apply** to save the settings.

# II-2-5 Security Defense Status

The router's current security protection mechanisms include Brute Force Protection and IP Reputation. This page provides details on the status of these protection mechanisms.

## II-2-5-1 Brute Force Protection Status

This page shows the status of Brute Force Protection.

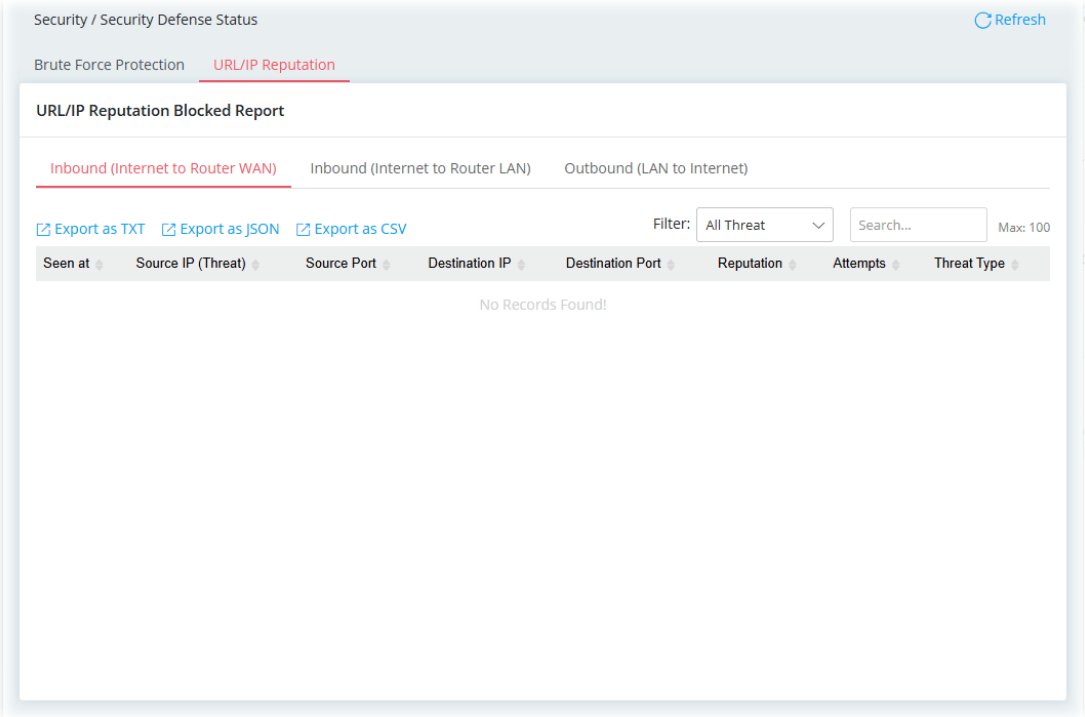



Available settings are explained as follows:

| Item | Description |
|---|---|
| IP Address | Displays the IP addresses that have been blocked due to triggering the Penalty or User Account Lockout function when using a System Account (e.g., logging into HTTPS/HTTP, SSH, Telnet, SNMP, and TR-069 Service |
| Account Name | Displays the account names that have been blocked due to triggering the Penalty or User Account Lockout function when using a System Account (e.g., logging into HTTPS/HTTP, SSH, Telnet, SNMP, and TR-069 Service. |
| Role | Displays the role of the account. |
| Service Type | Displays the service type set for the user account. |
| Blocked Start Time / Blocked End Time | Displays both the start and end times for blocking the IP address. |
| Hit Count | Displays the number of times a System Account has triggered the Penalty or User Account Lockout. |
| Option | **Unblock** – Click to remove the blocked IPs.<br>**Add to Block List** - Add IPs to the Defense Setup's Allow/Block List. |

## II-2-5-2 URL/IP Reputation

This page displays the IP Reputation status for the Vigor router regarding both inbound and outbound traffic.

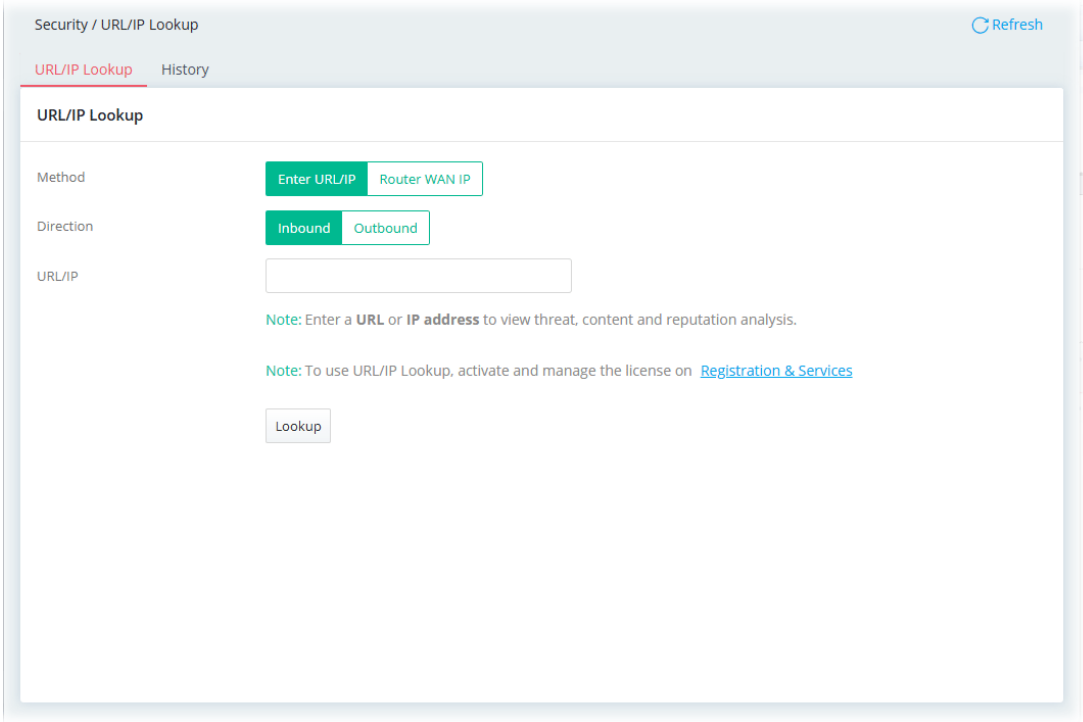



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Export as TXT/JSON/CSV** | Export the IP reputation settings with the file format of TXT, JSON, or CSV. |
| **Seen at** | Displays the time when the packet matches the specified rule. |
| **Source IP (Threat)** | Displays the IP address of the source of the threat. |
| **Source Port** | Displays the port number of the source IP. |
| **Destination IP** | Displays the IP address of the destination to which the threat is directed. |
| **Destination Port** | Displays the port number of the destination IP. |
| **Reputation** | Displays the score of the IP address. |
| **Attempts** | Displays the times of attempts made by the threat towards the target destination. |
| **Threat Type** | Displays the type of the threat. |

# II-2-6 URL/IP Lookup

This page allows you to view various score of specified IP or URL, click the **Look Up** button to see the relevant information. After analysis, the Vigor system will provide relevant information about the IP/URL, including risk level, reputation score, category, and more.

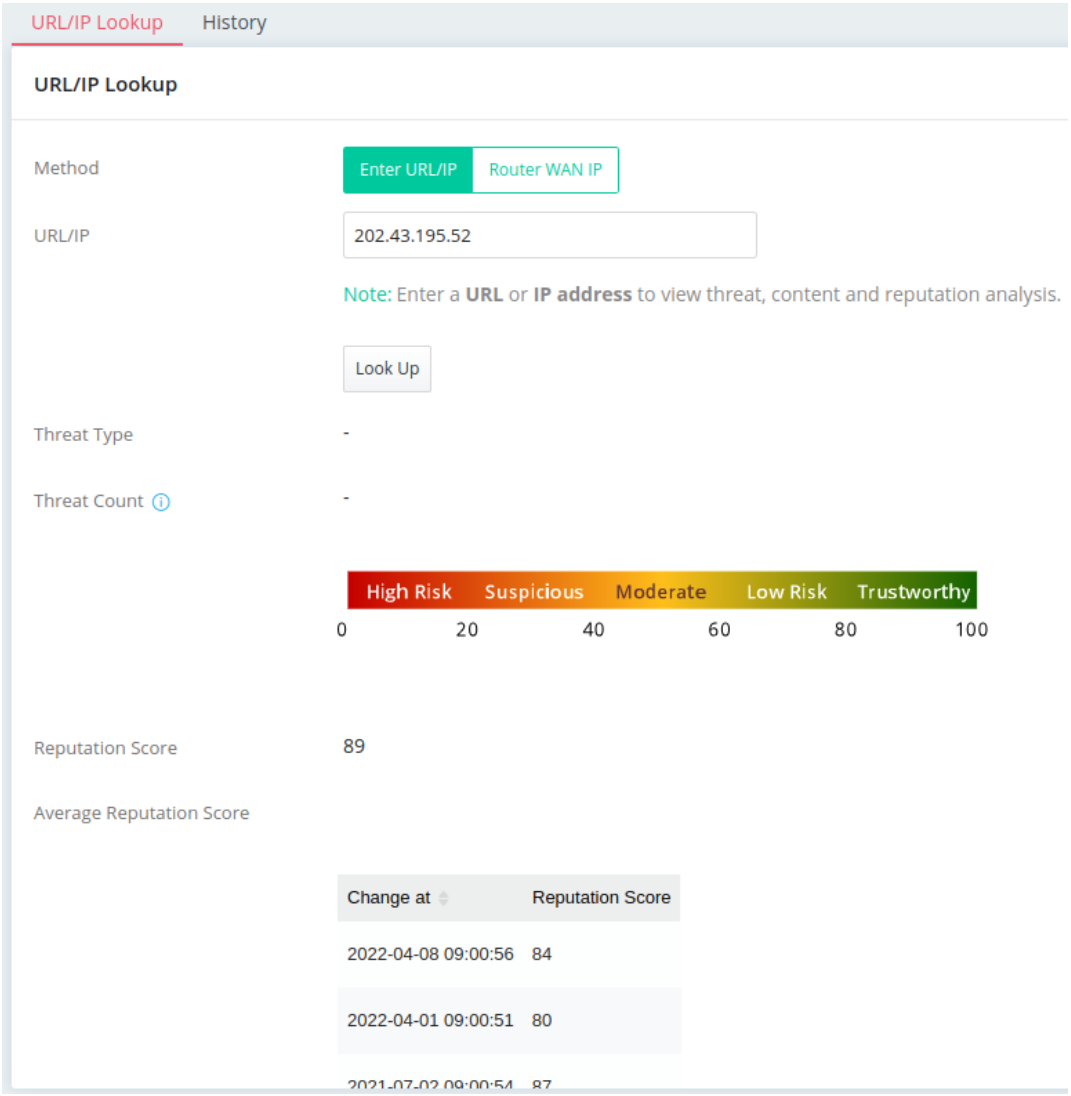



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Method** | **Enter URL/IP –** Select this method to look up using URL or IP address.<br>• **URL/IP -** Enter the URL or the IP address of the subject you want to look up.<br>**Router WAN IP** – Select this method to look up through WAN interface. |
| **Look Up** | Click to display information related to the IP/URL you look up.<br>In which, the relevant information associated, see below, with the IP address will be shown on the page.<br>• Threat Type<br>• Threat Count<br>• Reputation Score<br>• Average Reputation Score<br>• Organization<br>• Location<br>• Latitude<br>• Longitude<br>Or, enter the name of the URL. The relevant information associated with the URL will be shown on the page.<br>• Reputation Score<br>• Category<br>• Category Confidence<br>• Popularity<br>• Name Servers<br>• Registrar Name<br>• Created Date<br>• Expired Date |

| | |
|---|---|
| | • Organization<br>• Location |

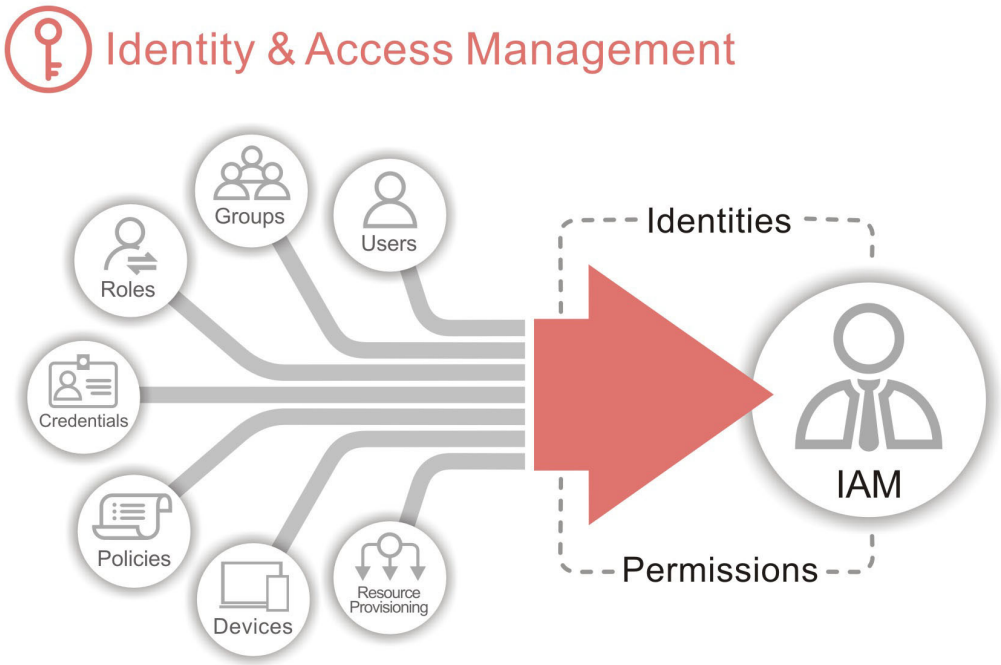
Below shows an example of look up IP/URL:



# II-3 IAM

Identity and Access Management (IAM) allows the network administrator to manage Internet access at the user level. After a user has been authenticated using a username and password, the user will be granted Internet access and additionally, optional firewall rules and LAN access policies can be applied.

In addition to being used for identification (via user account/VLAN), IAM can also set access policies to control users accessing network, and can be used as a firewall through group policy (group policy) to perform network management.



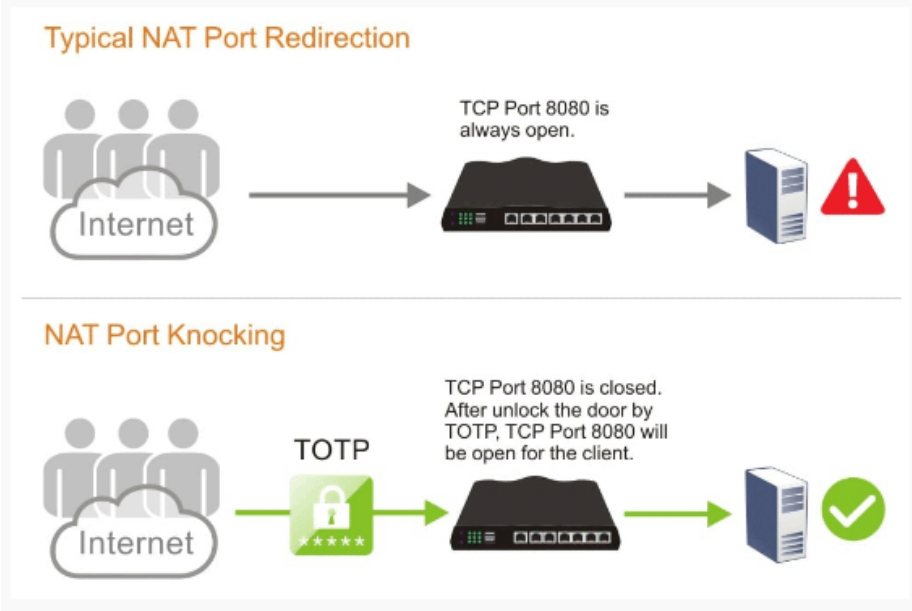

## Port Knocking

Port Redirection is one of the typical ways to allow the internal servers to be accessible from the Internet. However, the port may be exposed to the Internet and may be scanned by malware if it is open.

Therefore, a technology that can add an extra layer of protection to the internal servers and protect network services from unauthorized access is Port Knocking.

Port Knocking is a security technique that provides an additional layer of access protection by initially keeping all service ports closed and invisible to the public.

Only when a remote client performs a predefined sequence of connection attempts (known as knock ports), the system verifies the sequence. If the sequence is correct, the system temporarily opens the target service port for that client, allowing it to establish the actual connection.



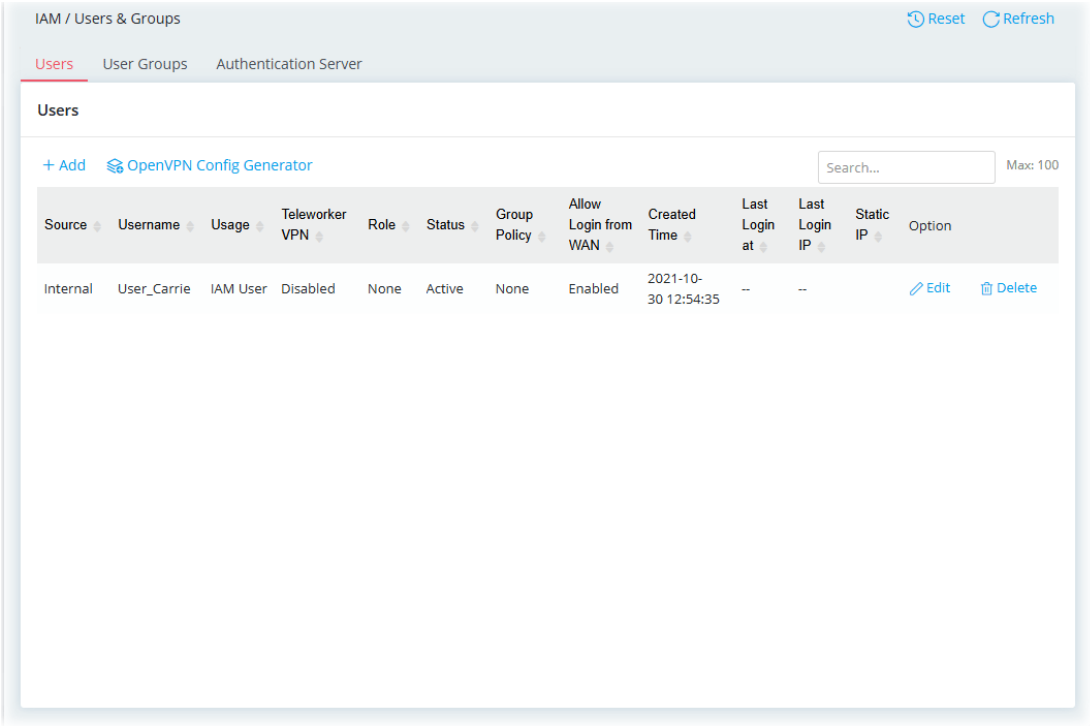

# II-3-1 Users & Groups

Before accessing the Internet through the device, any user must be authenticated by the Vigor system to ensure system security.

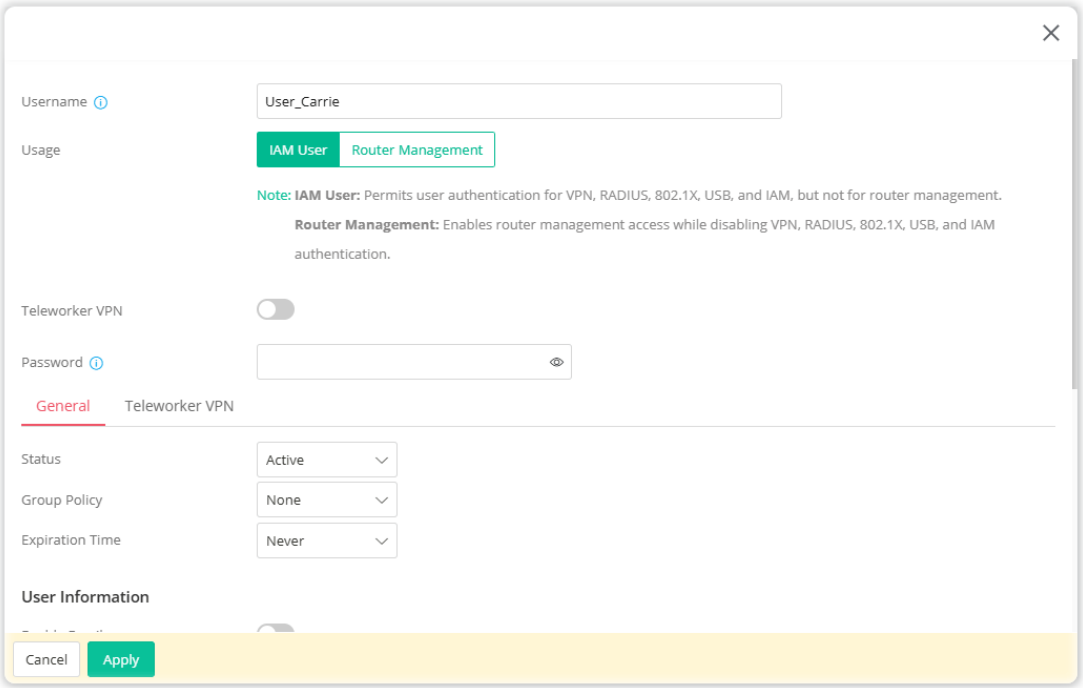
This section helps the system administrator create different users and groups profiles as the verification basis.

## II-3-1-1 Users

Up to 100 user profiles can be configured in this section.




To add a new user account profile, click **+Add**.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Username** | Enter the Login name (e.g., *LAN_User_Group_1, WLAN_User_Group_A, WLAN_User_Group_B,* etc.) for this user profile. |
| **Usage** | Define the type of this user profile.<br>**IAM User** – This profile can be used for VPN, RADIUS, 802.1X, USB and IAM (Identity and Access Management) authentication.<br>**Router Management** – This profile is only for router management access and cannot be used for VPN, RADIUS, 802.1X, USB, and IAM authentication. |
| **Teleworker VPN** | It is available if IAM User is selected as the Usage.<br>Switch the toggle to enable or disable the Teleworker VPN function. |
| **Password** | It is available if IAM User is selected as the Usage.<br>Password (e.g., *lug123, wug123,wug456,* etc.) for this user profile.<br>When a user tries to access the Internet, he or she must supply a valid user name and password combination for authentication. The profile with matching user name and password will be applied to the session. |
| **Password/**<br>**New Password/**<br>**Confirm New Password** | It is available if Router Management is selected as the Usage.<br>Password (e.g., *lug123, wug123,wug456,* etc.) for this user profile.<br>When a user tries to access the Internet, he or she must supply a valid user name and password combination for authentication. The profile with matching user name and password will be applied to the session. |
| **General**<br>**(if IAM User is selected as the Usage)** | |
| **Status** | **Active** – Enable the general settings in this page.<br>**Inactive** – Disable the general settings in this page. |

| | |
|---|---|
| **Group Policy** | It is available if "IAM User" is selected as the usage.<br>Select a group policy profile to be applied by this user profile. |
| **Expiration Time** | It is available if "IAM User" is selected as the usage.<br>Set the network connection to work at certain time interval only. All user accounts will apply the time configuration automatically by default.<br>**Never** – The network connection is always on.<br>**Expire in** –The network connection will expire and terminate the connection after specified minutes, hours, days, or weeks once built.<br>**Expire at** – The network connection will expire and terminate the connection on the date and time specified below once built.<br>• **Date**<br>• **Time** |
| **User Information** | **Enable Email** – Switch the toggle to enable or disable the email setting.<br>• **Email** – Enter the email address for receiving the MFA PIN code.<br>• **Send Email Notification to the newly created User** – Send a notification email to this user account.<br>**Enable SMS** – Switch the toggle to enable or disable the SMS setting.<br>• **SMS** - Enter the destination SMS number for receiving the MFA PIN code. |
| **MFA & Port Knocking** | Multi-factor authentication (MFA) can offer a more secure network connection.<br>**Enable MFA** – Switch the toggle to enable/disable the MFA function.<br>• **Allowed MFA Method** - Select to require TOTP, SMS or email authentication when logging in from the WAN.<br>**TOTP** – For the Time-based One-time Password (TOTP) mechanism, please make sure the time zone of your router is correct. Then, install Google Authenticator APP on your cell phone. Open the APP to scan the QR code on this page. A one-time password will be shown on your phone. Select TOTP and click **Apply.** A pop-up dialog will appear as follows:<br><br><br>In the filed of Validation Code, enter the one-time password and click Verify.<br>Now, the configuration is finished. You will be asked to enter |

| | |
|---|---|
| | the 2FA code on the after passing the username and password authentication.<br>**SMS/Email** –The password will be sent via SMS or email as selected in the User Information above.<br>• **Enforce Port Knocking** – Switch the toggle to enable/disable the Port Knocking function.<br>**1st Knock Port -** Enter a value (3001~59999). Click the (!) mark to have more information.<br>**TOTP Secret –** Display the secret used for TOTP. |
| **Account Info** | Displays general information (created time, last login at and last login IP) for the user account. |
| **Teleworker VPN**<br>**(available if IAM User is selected as the Usage)** | |
| **General** | **Idle Timeout** – If the user is idle over the limitation of the timer, the network connection will be stopped for this user. By default, the Idle Timeout is set to 300 seconds.<br>**VPN Schedule** – Select Always On (Telework VPN is running all the time). Or choose **Scheduled On** to make the VPN connection based on the schedule.<br>Before configuring VPN Schedule, add the required time intervals in Configuration>>Objects >>Schedule.<br>**Netbios Naming over VPN** – Switch the toggle to allow/ deny NetBIOS naming packets to traverse through the VPN tunnel.<br>**Multicast over VPN** – Switch the toggle to allow/ deny multicast packets to traverse through the VPN tunnel.<br>**mDNS over VPN** – Switch the toggle to allow/ deny mDNS packets to traverse through the VPN tunnel.<br>**Download SmartVPN Client** - Click to download the utility of DrayTeck SmartVPN client for building VPN connection. |
| **Allowed VPN Protocols** | Select IPsec, WireGuard or OpenVPN as the protocol for the teleworker VPN connection.<br>**IPsec** – Switch the toggle to enable the IPsec protocol.<br>If enabled, select IKEv1/v2, EAP and/or XAuth as the IPsec protocol.<br>**OpenVPN** - Switch the toggle to enable OpenVPN protocol.<br>**WireGuard** – Switch the toggle to enable WireGuard protocol.<br>**L2TP** - Switch the toggle to enable L2TP protocol. If enabled, configure **L2TP with IPsec Policy.** L2TP with IPsec encryption is mandatory for this connection type to ensure data integrity and confidentiality.<br>• **Must** - Specify the IPsec policy to be definitely applied on the L2TP connection. |
| **Security** | **Specify VPN Peer** – Switch the toggle to enable/disable the security mechanism for the remote client.<br>• **Remote Client IP** – Enter the IP address of the remote peer if Specify VPN Peer is enabled.<br>**Pre-Shared Key** – It is available when the IPsec is selected as the Allowed VPN Protocols. "Specify VPN Peer" can restrict the IPsec to be initiated only by the specified peer IP address or domain name, and specify the private key to be used.<br>**X.509 Digital Signature** - It is available when the IPsec is selected as the Allowed VPN Protocols. Accept the certificates |

| | |
|---|---|
| | authentication. To use an X.509 digital signature, select one of the authentication methods and enter the required information for each method.<br>• **Disabled** – Select to disable the certificate application for VPN connection.<br>• **Accept Subject Alternative Name** –The following three formats of Peer ID are acceptable, including IP Address, Domain Name, and Email.<br>• **Select from Existing Certificates** –Select a peer certificate that has been pre-obtained and stored in Configuration>>Certificates Local Certificates.<br>• **Accept Subject Name** – Enter the complete certificate subject name.<br>• **Accept Any** – Any certificate signed by a trusted CA in Configuration>>Certificates Trusted CA will be considered valid.<br>Click **IPsec Advanced Settings** to get the following options. Local ID and Peer ID are provided for certain connections that require specifying an ID, such as IKEv1 using Aggressive mode and IKEv2 (optional).<br>• **Peer ID** – Specify a local ID to be used when establishing a VPN connection using IPsec VPN type. Enter the ID name for the remote client.<br>• **Local ID (optional)** - If the values are specified, only connections coming from the specified IP address and/or having the specified Peer ID will be accepted. |
| WireGuard Settings | It is available when the **WireGuard** is selected as the Allowed VPN Protocols.<br>**Generate Key Mode** – Select Auto or Customized.<br>**Generate Key Pair** – Click to generate the client private key and the client public key automatically.<br>**Client Public Key** – Enter the string offered by the remote WireGuard VPN client.<br>**Pre-Shared Key** – Displays the private key generated by clicking Generate PSK.<br>**Generate PSK** – Click the Generate PSK button to generate a pre-shared key.<br>**Persistent Keepalive** – Default is 60 seconds. If the peer is behind a NAT or a firewall, use the default setting. |
| Local IP Assignment | **Assign IP By –** Select **LAN DHCP** or **Static IP.** This option will be unavailable if the WireGuard VPN protocol is enabled.<br>**Assign IP from** – Select a LAN interface for IP assignment.<br>**Assign DNS By** – Choose **LAN DHCP** (the DNS IP will be assigned by Vigor router automatically) or **Static DNS**. If Static DNS is selected, configure Primary DNS and Secondary DNS.<br>• **Primary DNS** – Enter the IPv4 address for Primary DNS server.<br>• **Secondary DNS** – Enter another IPv4 address for DNS server if required.<br>If **Static IP** is selected,<br>• Static IP – Specify an IPv4 address. |
| WireGuard Client Config Generator | This option will be unavailable if the WireGuard VPN protocol is enabled. |

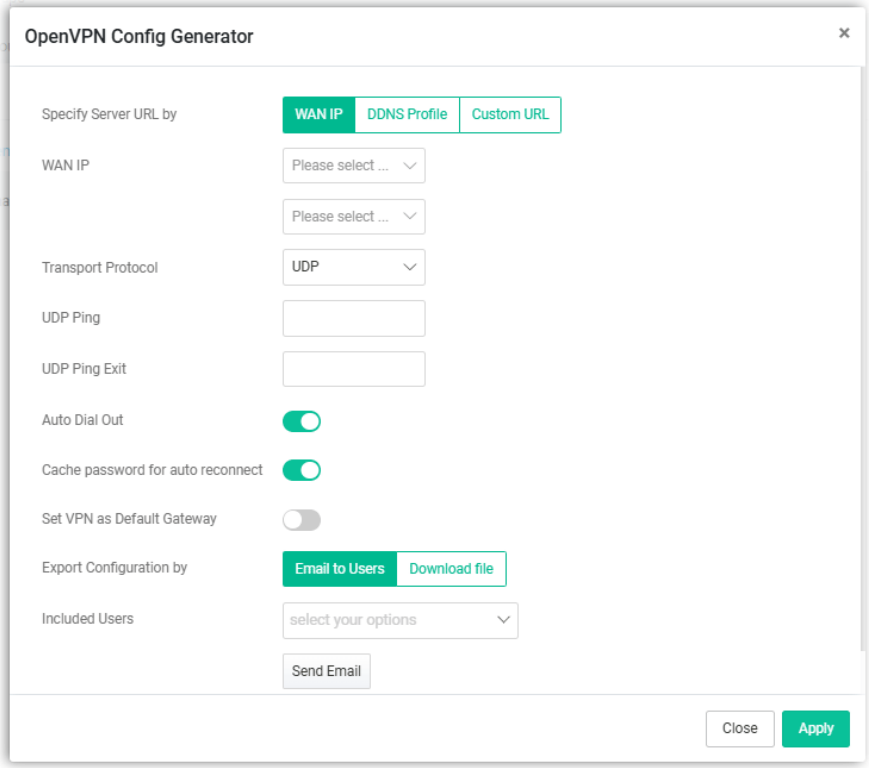
| | |
|---|---|
| | **VPN Server –** Enter WAN IP or domain name of this router.<br>**Set VPN as Default Gateway –** Switch the toggle to enable/disable the function.<br>• **Enable** - The Vigor router will be treated as a "default" gateway for WireGuard VPN clients. The WireGuard VPN client will redirect all the traffic to the Vigor router via the WireGuard VPN tunnel.<br>• **Disable** - Disable the function.<br>• **Replace the Default Route –** Switch the toggle to enable/disable the feature. After clicking **Apply**, the client's default route will be replaced by the VPN route.<br>**config –** The default text in this field is displayed automatically. It will be changed according to the QR-Code variation. Modify the text if required.<br>**Download Configuration -** Click this button to download the config on this page as a file, which can be imported into a VPN client to establish WireGuard VPN connections. |
| **General**<br>**(if Router Management is selected as the Usage)** | |
| **Role** | It is available if "Router Management" is selected as the usage.<br>• **Administrator**<br>• **Guest**<br>• **Users** |
| **Status** | **Active** – Enable the general settings in this page.<br>**Inactive** – Disable the general settings in this page. |
| **Allow Login from WAN** | It is available if "Router Management" is selected as the usage.<br>If enabled, the user can login from WAN by using this user account. |
| **User Information** | **Enable Email** – Switch the toggle to enable or disable the email setting.<br>• **Email** – Enter the email address for receiving the MFA PIN code.<br>• **Send Email Notification to the newly created User** – Send a notification email to this user account.<br>**Enable SMS** – Switch the toggle to enable or disable the SMS setting.<br>• **SMS** - Enter the destination SMS number for receiving the MFA PIN code. |
| **MFA & Port Knocking** | Multi-factor authentication (MFA) can offer a more secure network connection.<br>**Enable MFA** – Switch the toggle to enable/disable the MFA function.<br>• **Allowed MFA Method** - Select to require TOTP, SMS or email authentication when logging in from the WAN.<br>**TOTP** –For the Time-based One-time Password (TOTP) mechanism, please make sure the time zone of your router is correct. Then, install Google Authenticator APP on your cell phone. Open the APP to scan the QR code on this page. A one-time password will be shown on your phone. Select TOTP and click **Apply.** A pop-up dialog will appear as follows: |

| | |
|---|---|
| | <br>In the filed of Validation Code, enter the one-time password and click Verify.<br>Now, the configuration is finished. You will be asked to enter the 2FA code on the after passing the username and password authentication.<br>**SMS/Email** –The password will be sent via SMS or email as selected in the User Information above.<br>• **Enforce Port Knocking** – Switch the toggle to enable/disable the Port Knocking function.<br>**1st Knock Port –** Enter a value (3001~59999). Click the (!) mark to have more information.<br>**TOTP Secret –** Display the secret used for TOTP. |
| **Account Info** | Displays general information (created time, last login at and last login IP) for the user account. |
| **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.

To add a new OpenVPN profile, click **OpenVPN Config Generator**.

On this page, you can create configuration required for a remote OpenVPN client to connect to the router and then download it directly or send it to the user via email.



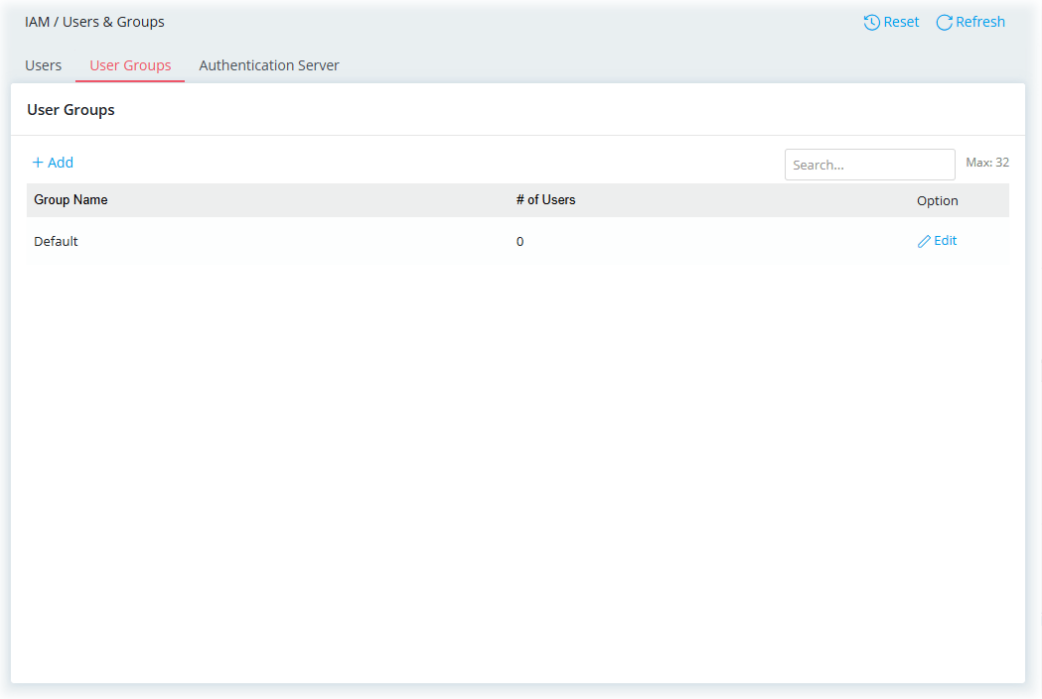

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Specify Server URL by** | The OpenVPN client will use the IP address or domain name to connect to the router.<br>**WAN IP** – The OpenVPN configuration file will use the numeric IP address as the server address.<br>• **WAN IP** – Select the WAN interface.<br>**DDNS Profile** – The OpenVPN configuration file will use the domain name from the DDNS Profile.<br>• **DDNS Profile** – Select a DDNS profile.<br>**Custom URL** – The OpenVPN configuration file will use the user-defined server IP or domain name.<br>• **Custom URL** – Specify a user-defined URL. |
| **Transport Protocol** | **TCP/UDP** - Select UDP or TCP for the protocol to be used by the OpenVPN client to connect to the router. |
| **UDP Ping** | Ping remote device over the UDP control channel, if no packets have been sent for the number of seconds configured here. |
| **UDP Ping Exit** | Let OpenVPN exit after the seconds set here if no reception of a ping or other packet from the remote device. |
| **Auto Dial Out** | Switch the toggle to enable/disable the function.<br>**Enable** - The remote client can auto-dial to this Vigor router to build an OpenVPN tunnel.<br>**Disable** - Disable the function. |

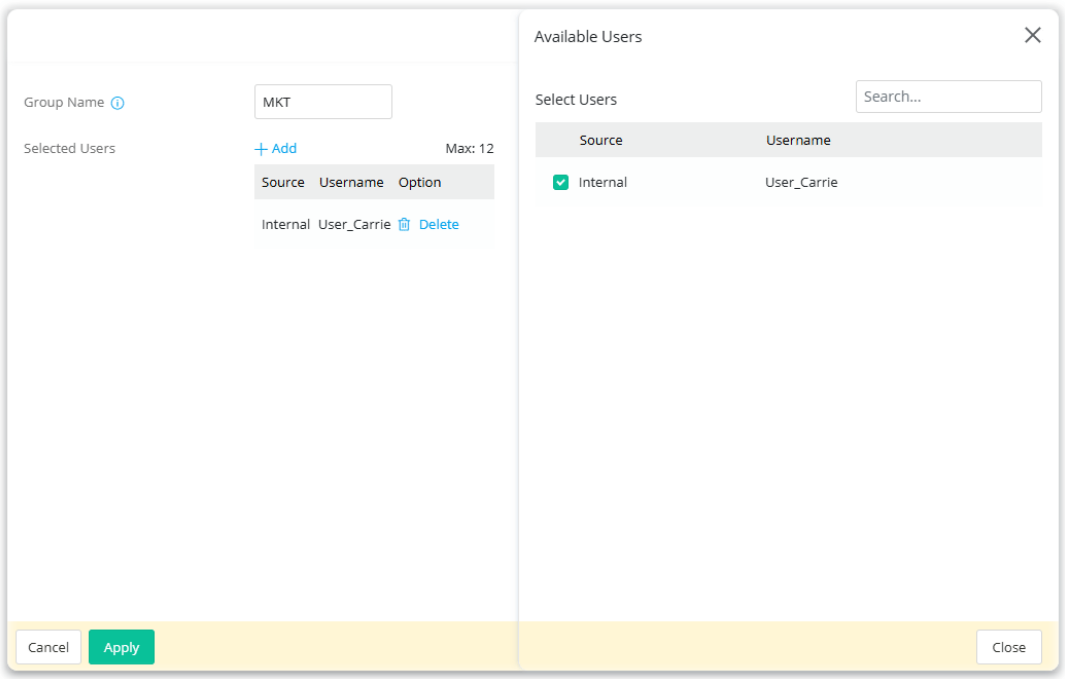
| | |
|---|---|
| Cache password for auto reconnect | Switch the toggle to enable/disable the function.<br>**Enable** - OpenVPN will reconnect per hour. While reconnecting, the password is required. If the function is enabled, the password for OpenVPN connection will be kept and used by the Vigor system for reconnection every time.<br>**Disable** - Disable the function. |
| Set VPN as Default Gateway | Switch the toggle to enable/disable the function.<br>**Enable** - The Vigor router will be treated as a "default" gateway for OpenVPN clients. The OpenVPN client will redirect all the traffic to the Vigor router via the OpenVPN tunnel.<br>**Disable** - Disable the function. |
| Export Configuration by | **Email to Users** – If selected, the Included Users field below will be displayed. The OpenVPN configuration file will be sent to users listed on Included Users.<br>• **Included Users** – Select teleworker users that will receive the configuration from Vigor router.<br>• **Send Email** – Click to email the settings on this page as a file, which can be imported into a VPN client to establish OpenVPN connections to teleworker users.<br>**Download zip file** – The configuration file for OpenVPN will be stored on the database. If selected, the Download Configuration button below will be displayed.<br>• **Download Configuration** - Click this button to download the settings on this page as a file, which can be imported into a VPN client to establish OpenVPN connections. |
| Included Users | Select teleworker users that will receive the configuration from Vigor router.<br>**Send Email –** Click to email the settings on this page as a file, which can be imported into a VPN client to establish OpenVPN connections to teleworker users. |
| Close | Discard current settings and return to the previous page. |
| Apply | Save the current settings and exit the page. |

## II-3-1-2 User Groups

This page allows you to place multiple user profiles into groups.




To add a new user group profile, click **+Add**.




Available settings are explained as follows:

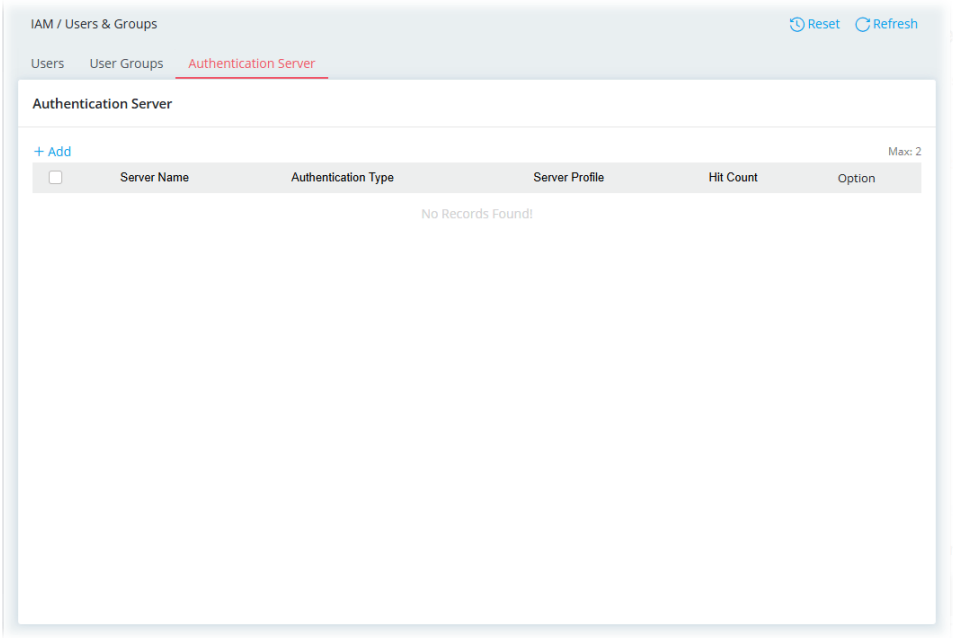
| Item | Description |
|---|---|
| **Group Name** | Enter a name for identification. |
| **Selected Users** | **+Add** – Click to select user profiles to be grouped under the current group profile. |

| | |
|---|---|
| Available Users | It appears after clicking **+Add**.<br>**Selected Users** – Select the member from available user profiles. |
| Cancel | Discard current settings and return to the previous page. |
| Apply | Save the current settings and exit the page. |

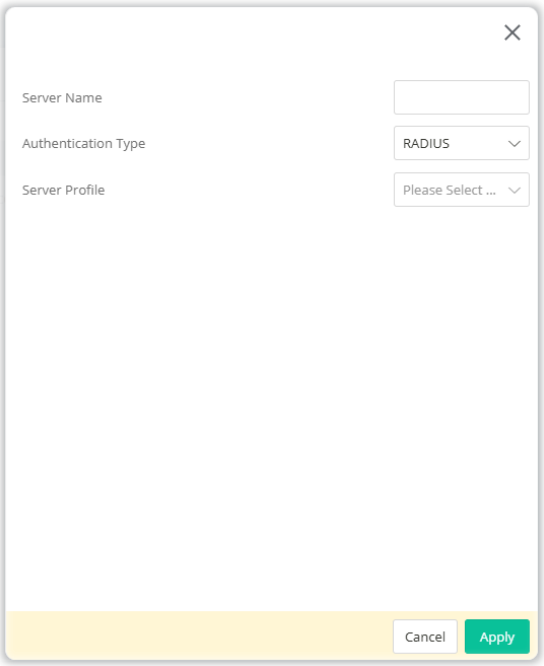
After finishing this web page configuration, please click **Apply** to save the settings.

## II-3-1-3 Authentication Server

Vigor router can authenticate users using either a built-in (None) or external service (Radius or TACACS+) server.




To create a new authentication server profile, click **+Add**.

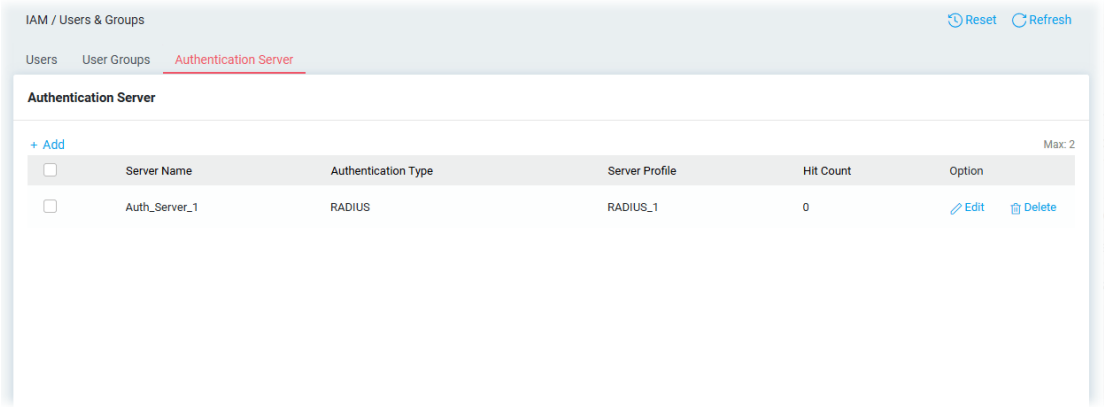



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Server Name** | Enter a name for identification. |
| **Authentication Type** | Select the authentication type (RADIUS or TACACS+). |
| **Server Profile** | If RADIUS is selected as Authentication Type, the available RADIUS server profiles (created on Configuration>>RADIUS/TACACS+) will |

| | |
|---|---|
| | be shown in this area. Select the one you need. |
| **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.

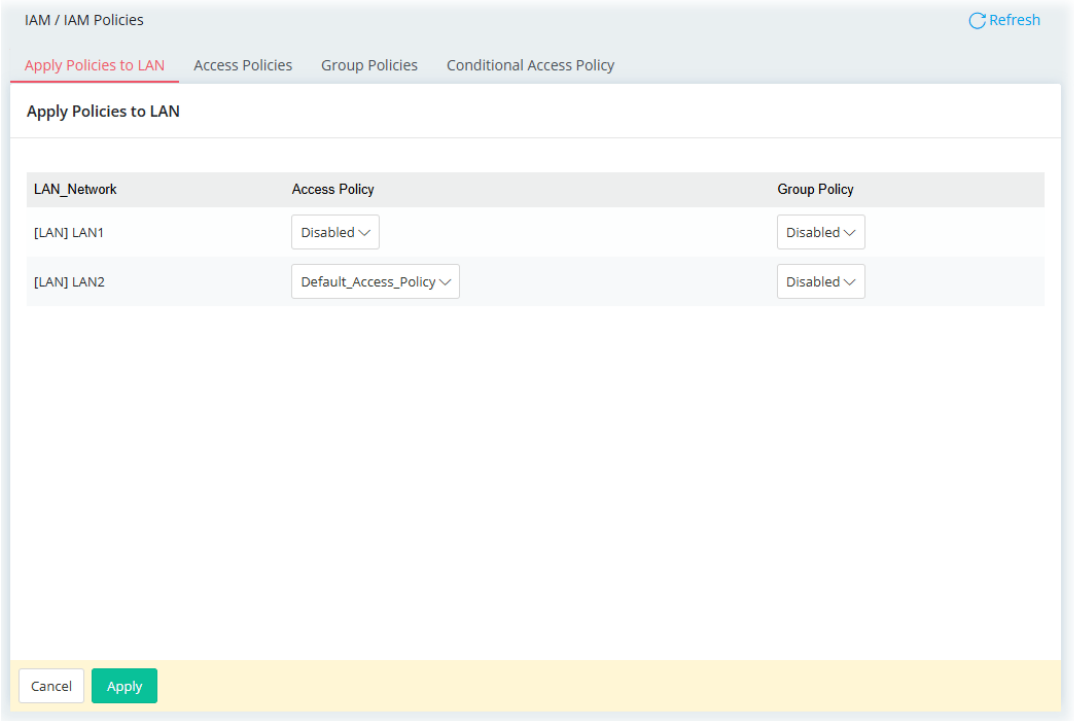



# II-3-2 IAM Policies

IAM Policy contains access policy, group policy and conditional access policy.

## II-3-2-1 Apply Policies to LAN

This page is used for selecting access policy and group policy which will be applied to the LAN profile.




Available settings are explained as follows:

| Item | Description |
|---|---|

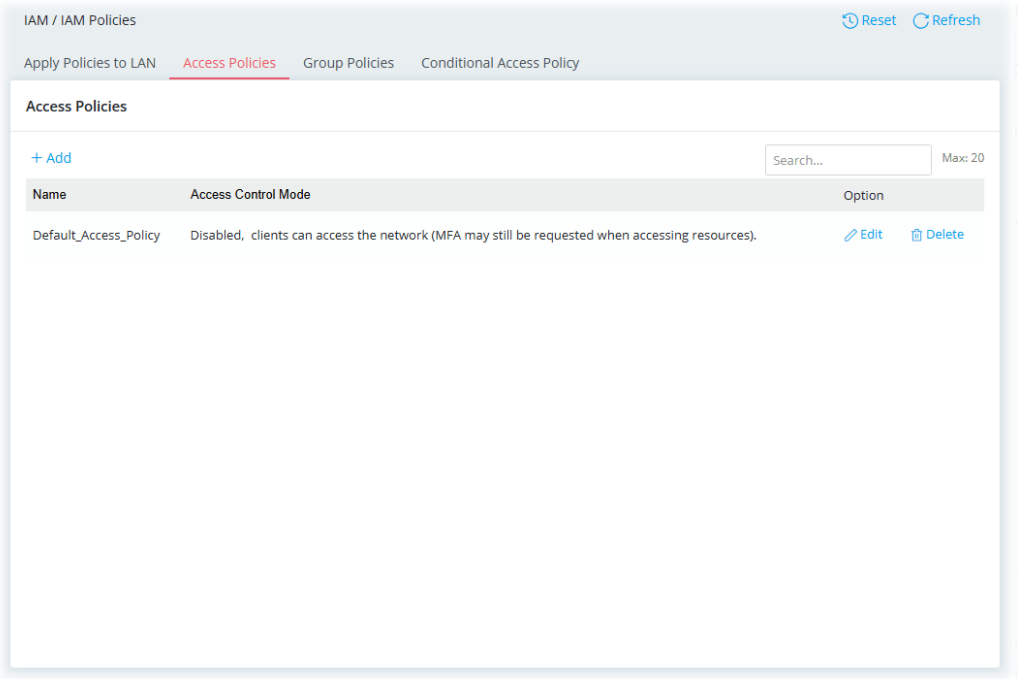
| | |
|---|---|
| LAN Network | Display the interface that the IAM policy will apply to. |
| Access Policy | Select an access policy for this interface. Or select Disabled to ignore the setting. |
| Group Policy | Select a group policy for this interface. Or select Disabled to ignore the setting. |
| Cancel | Discard current settings. |
| Apply | Save the current settings. |

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

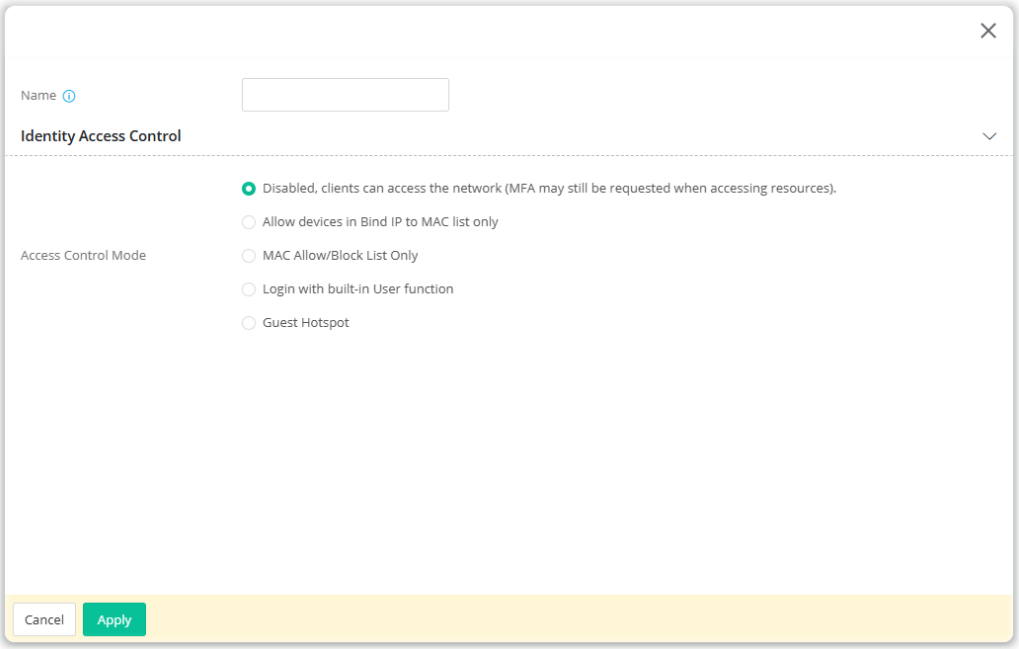
## II-3-2-2 Access Policies

Access Policies can be applied to LAN interface to determine how the users/clients access the Internet via identification authentication.

This page is used for define different access policies for IAM application.




To add a new access policy profile, click **+Add**.



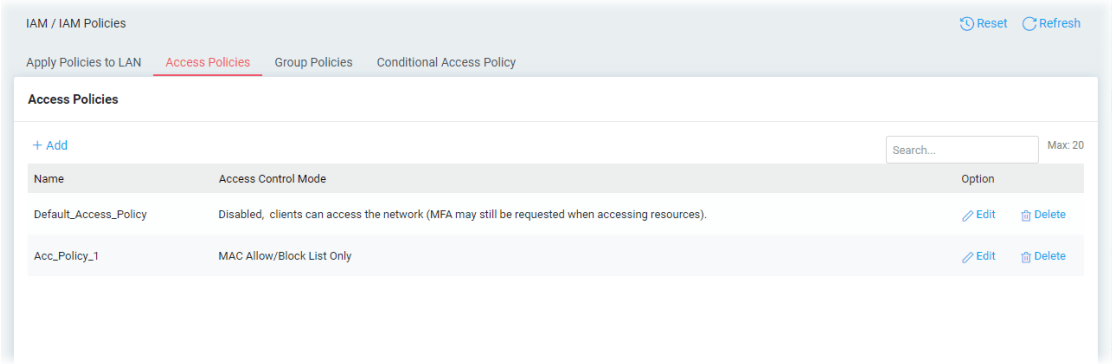

Available settings are explained as follows:

| Item | Description |
|---|---|
| Name | Enter a name for identification. |
| Identity Access Control | |

| | |
|---|---|
| Access Control Mode | **Disabled** – All clients/user accounts can access the network.<br>**Allow devices in Bind IP to MAC list** – Allow the clients/user accounts access to the network based on the Bind IP to MAC list.<br>**MAC Allow/Block List Only** – Allow or deny the clients/user accounts access to the network by the MAC address filter profile.<br>**Login with built-in User function** – The clients will be authenticated before accessing the network.<br>**Guest Hotspot** - Allow or deny the clients/user accounts access to the network based on the hotspot profile selected. |
| If **MAC Allow/Block List Only** is selected as the **Access Control Mode**. | |
| **MAC Address Filter** | |
| Set up MAC Address Filter by | **Selecting from Profile** – Use pre-defined MAC Filtering profiles as the filtering basis.<br>• **MAC Filtering Profile** - Select one of the MAC filtering profiles (Security>>MAC Filtering Profile) as the filtering basis.<br>**Manually** – Define the MAC addresses and separate them as Allow List or Block List.<br>• **MAC Address Filter Mode** – Select **Allow List** (allow the clients to access) or **Block List** (deny the clients access). Then, enter the MAC address of the clients separately on the MAC Address Filter Table.<br>• **MAC Address Filter Table** – Click **+Add** to enter the MAC address of the client. |
| If **Login with built-in User function** is selected as the **Access Control Mode** | |
| Authentication Mode | **Single-Factor** - Only identification authentication is required.<br>**Multi-Factor** - Multi-Factor authentication adds an extra layer of security, ensuring that only those users or devices within the Users or VLAN that apply specified Group Policy can access the specified resource. |
| **MAC Address Filter** | |
| Set up MAC Address Filter by | **Selecting from Profile** – Use pre-defined MAC Filtering profiles as the filtering basis.<br>• **MAC Filtering Profile** - Select one of the MAC filtering profiles (Security>>MAC Filtering Profile) as the filtering basis.<br>**Manually** – Define the MAC addresses and separate them as Allow List or Block List.<br>• **MAC Address Filter Mode** – Select **Allow List** (allow the clients to access) or **Block List** (deny the clients access). Then, enter the MAC address of the clients separately on the MAC Address Filter Table.<br>• **MAC Address Filter Table** – Click **+Add** to enter the MAC address of the client. |
| **Allowed User List** | |
| User | Configure the whitelist settings. Users are allowed to send and receive traffic that satisfies whitelist settings.<br>**All Users** – All user accounts will be considered part of the whitelist.<br>**Selected Users** – The whitelist will only consider the user accounts that have been selected.<br>**None** - There will be no user account applied. |

| | |
|---|---|
| **User Groups** | Configure the whitelist settings. Groups are allowed to send and receive traffic that satisfies whitelist settings.<br>**All Groups** – All user groups will be considered part of the whitelist.<br>**Selected Groups** – The whitelist will only consider the user groups that have been selected.<br>**None** – There will be no user group applied. |
| **Login Session Lifetime** | |
| **Login Session Lifetime** | Control the session time for users/clients. After the session's lifetime, the users/clients must log in to access the network, again.<br>Specify the number of days, hours, and minutes. |
| If **Guest Hotspot** is selected as the **Access Control Mode** | |
| **Login Session Lifetime** | |
| **Hotspot Profile** | Select one of the hotspot profiles. |
| **Login Session Lifetime** | Control the session time for users/clients. After the session's lifetime, the users/clients must log in to access the network, again.<br>Specify the number of days, hours, and minutes. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings and exit the page. |

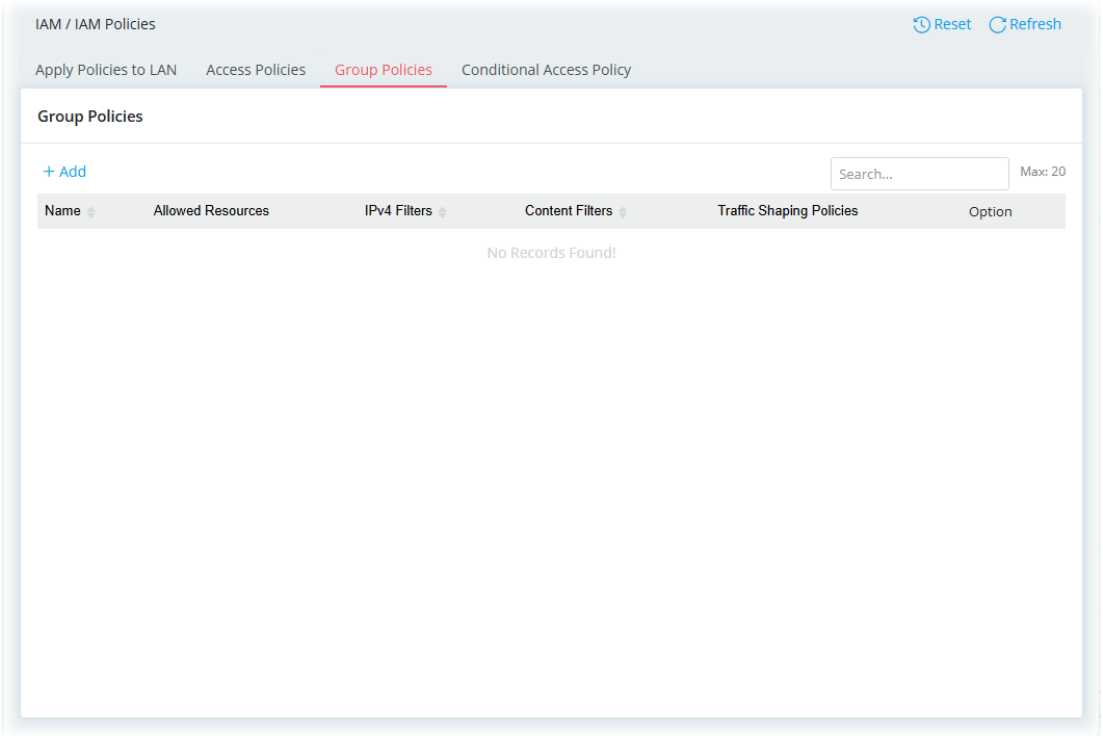
After finishing this web page configuration, please click **Apply** to save the settings.




## II-3-2-3 Group Policies

The traditional firewall generally provides a blocking mechanism with IP-based rules to permit or block traffic on designated ports. To more securely manage access privilege, Group Policies provide a better way to help administrators decide permission for specific users, which define limitations and configuration based on role behavior to authorize corresponding restrictions, such as Time and Date Limit, Resources, Firewall Policies, and Traffic Shaping Policies.

This page is used for configuring group policies for IAM application.



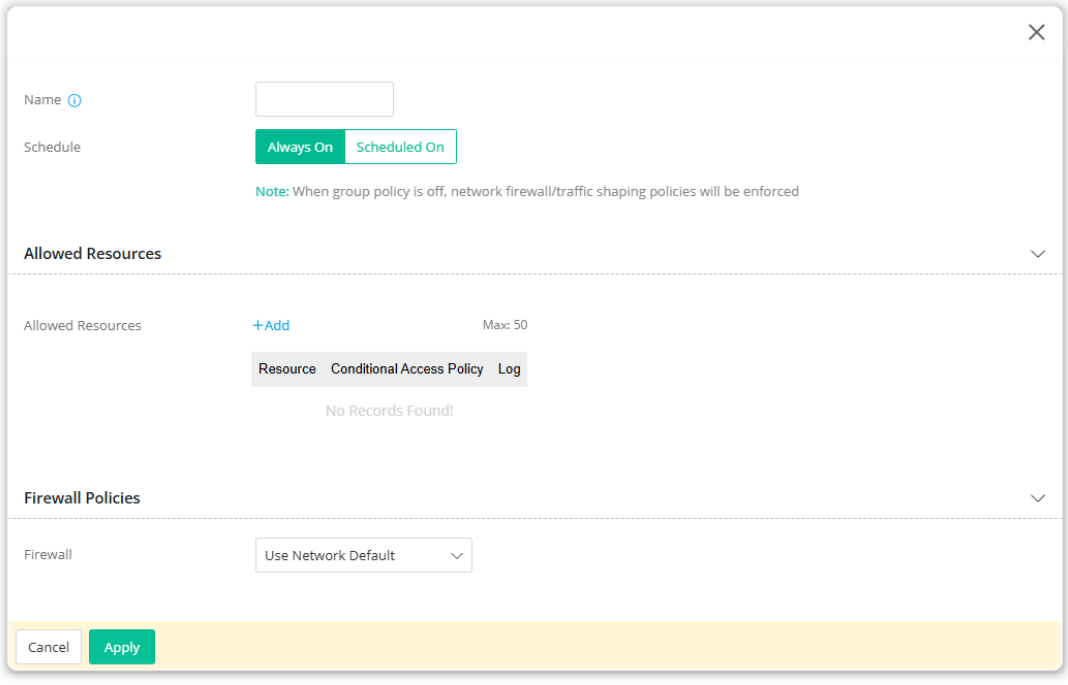

---

**Note:**

Once Group Policies are applied to user account/VLAN profile, even if the firewall filter setting has been setup, Group Policies will override rules set at the firewall filter.

---

To add a new group policy profile, click **+Add**.



Available settings are explained as follows:

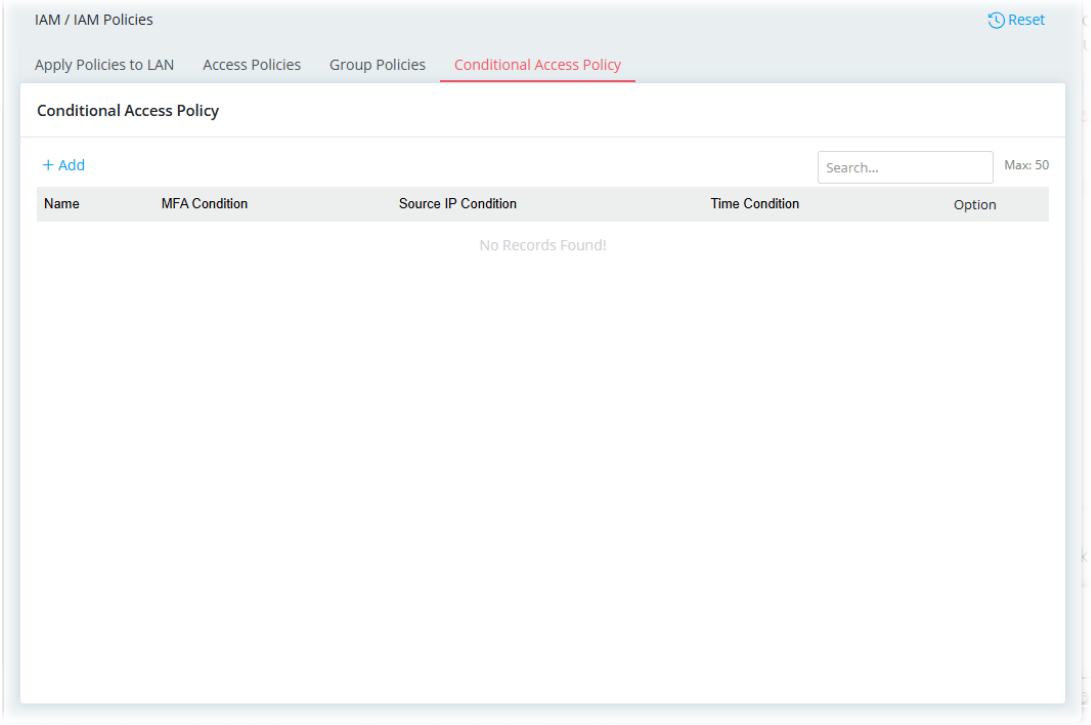
| Item | Description |
|---|---|
| Name | Enter a name for identification. |
| Schedule | **Always On -** The function of group policy is running all the time.<br>**Scheduled On -** The function of group policy is activated based on the schedule profile. |
| Allowed Resources | |
| Allowed Resources | Select resources profile(s) and apply to this policy profile.<br>**+Add** – Click to add a new resource profile.<br>**Resource** – Use the drop-down menu to select IP or MAC resource profile.<br>**Conditional Access Policy** – Use the drop-down menu to select access condition profile.<br>**Log** – Select Pass or Block or Both. Corresponding records (related to passing or blocking packets) will be stored as a log.<br>**Option (Delete)** – Click to remove the entry. |
| Firewall Policies | |
| Firewall | **Use Network Default** – Select this item to use the default group firewall filter settings.<br>**Customize Group firewall filters** – Select this item to customize the group firewall filter settings. The firewall policy will be applied to allowed resources defined above. |
| If **Customize Group firewall filters** is selected as the **Firewall** | |
| Outbound IPv4 Filters | **+Add** – Click to add new IPv4 filter profiles (up to 10) for outgoing traffic.<br>**Name** – Set a name that identifies the IP filter profile. The maximum length of the Profile Name is 15 characters.<br>**Scheduled On** - The filter profile will be valid based on the time schedule specified here.<br>**Destination IP Start** – Enter an IP address as the starting IP address.<br>**Destination IP End** – Enter an IP address as the ending IP address. If only one static IP address will be filtered by this profile, enter the same IP address as the value in Destination IP Start.<br>**Protocol** – Specify the protocol(s) which this filter rule will apply to.<br>**Dest Port Start** – Specify the target port range (starting point) if the protocol is TCP or UDP.<br>**Dest Port End** – Specify the target port range (ending point) if the protocol is TCP or UDP.<br>**Action** –Select Pass to allow access to the IP address; select Block to disallow access to the IP address.<br>**Option(Delete)** - Click to remove the selected entry. |
| Content Filters | The system will check the outgoing sessions additionally with the selected content filters profile(s).<br>**+Add** – Click to add a new content filter profile (up to 10).<br>**Profile Name** – Set a name that identifies the content filter profile. The maximum length of the Profile Name is 15 characters.<br>**Scheduled On** - The filter profile will be valid based on the time schedule specified here. |

| | |
|---|---|
| | **Destination** – Select specific WCF and/or APPE and/or UCF (keyword object) profile to be included in the filter.<br>**Action** – Select Pass to allow access to the Destination; select Block to disallow access to the Destination.<br>**Enable Keyword Exception** – Switch the toggle to enable/disable the function.<br>**Keyword Exceptions** - Display selected keyword objects.<br>The system will check the sessions additionally with the selected keyword profile(s). If the session meets the keyword filter profile, the system will perform the action reversely.<br>**Option (Delete)** - Click to remove the selected entry. |
| **IP Filters Default Action** | Any packet that does not comply with the rules set in Outbound IPv4 Filters and Content Filters will be processed according to the default action.<br>• **Pass** - Allow access to the IP address.<br>• **Block** - Disallow access to the IP address. |
| **Enable Content Filter Default Rule** | If enabled,<br>**Content Filters Default Action** - Any session that does not comply with the above firewall filters rules but matches the content destination rule will be processed according to the default action.<br>• **Pass** - Allow the session pass which is matched Content Destination rule. The outgoing traffic that matches the following Content Destination rule will be passed. Otherwise, it will be blocked.<br>• **Block** - Disallow the session pass which is matched Content Destination rule. The outgoing traffic that matches the following Content Destination rule will be blocked. Otherwise, it will be allowed to pass through.<br>**Content Destination** – Select the WCF and/or APPE and/or UCF (keyword object) profile to be included in the filter. It is treated as an additional content filter rule to determine whether the packets/sessions will be passed or blocked. |
| **Enable Syslog** | The filtering result can be recorded according to the setting selected for Syslog. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings and exit the page. |

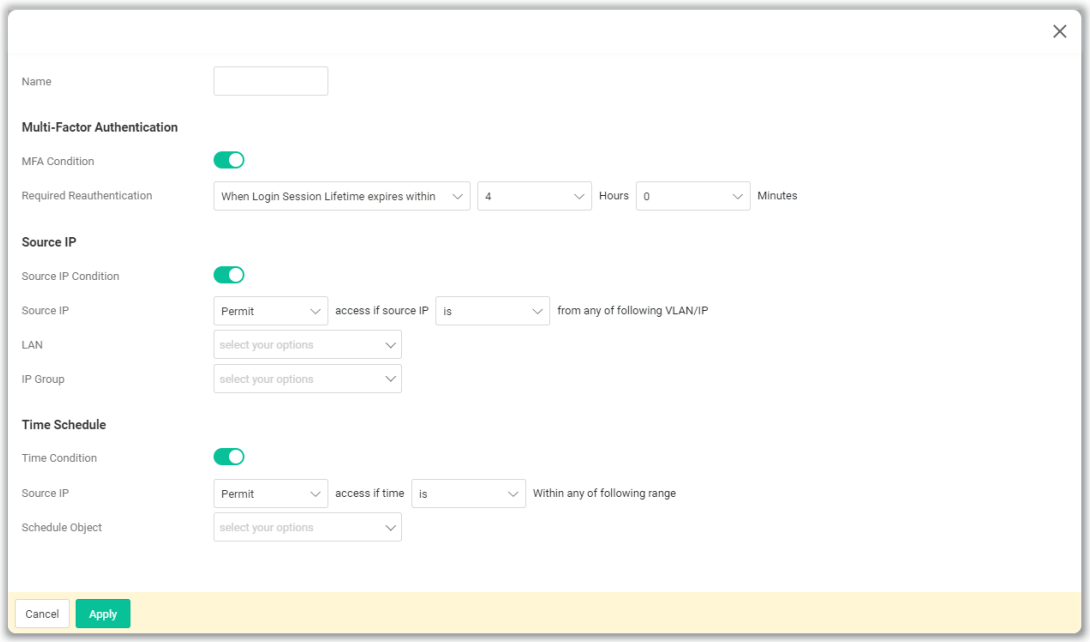
After finishing this web page configuration, please click **Apply** to save the settings.

## II-3-2-4 Conditional Access Policy

Different from the Access Policies designed for setting Access Control Mode, this page provides a policy combination of time schedule, source IP, and multi-factor authentication (MFA). It can be used together with the resources.




To add a new conditional policy profile, click **+Add**.




Available settings are explained as follows:

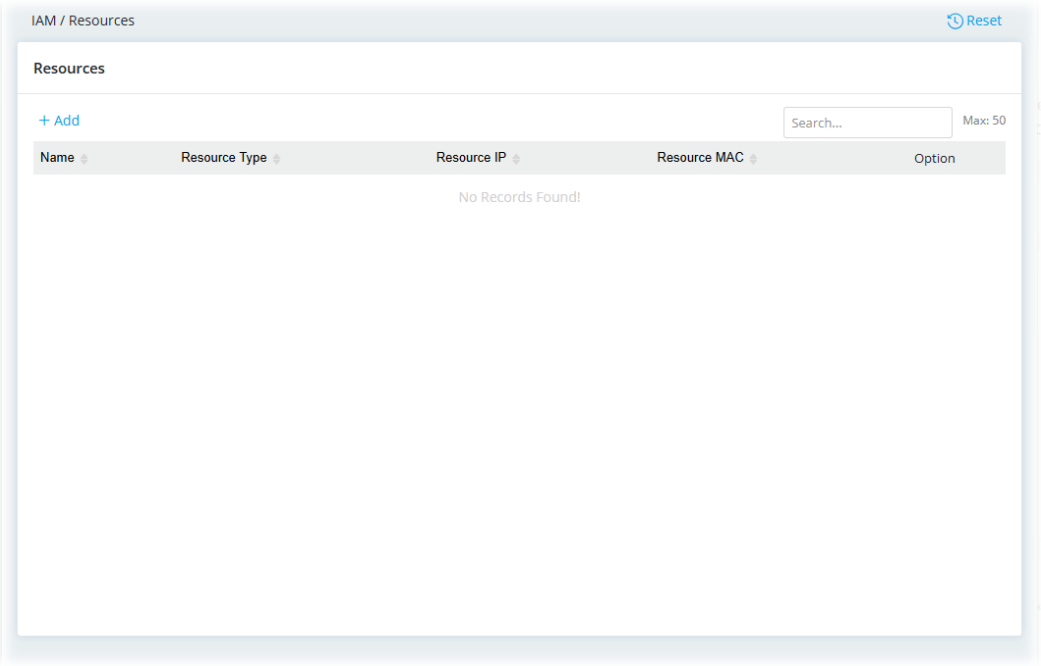
| Item | Description |
|---|---|
| Name | Enter a name for identification. |
| Multi-Factor Authentication | |

| | |
|---|---|
| **MFA Condition** | Switch the toggle to enable/disable the function. |
| **Required Reauthentication** | Set the time period for re-authenticating the user when the user wants to access the other IP address (defined in IAM>>Resources).<br>Select **Everytime** or **When Login Session Lifetime expires within.**<br>Vigor system will perform the reauthentication job for users (clients). |
| **Source IP** | |
| **Source IP Condition** | To Permit or Deny Access if the source IP is from the designated VLAN/IP. |
| **Source IP** | Specify the action (Permit or Deny) for the source IP. |
| **LAN** | Select an interface. |
| **IP Group** | Select an appropriate IP group or multiple IP groups that you would like to include in this policy. |
| **Time Schedule** | |
| **Time Condition** | Switch the toggle to enable/disable the time schedule. |
| **Source IP** | Determine whether you would like to Permit or Deny the source IP. |
| **Schedule Object** | Select an appropriate schedule profile or multiple profiles that you would like to apply to this policy. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings and exit the page. |

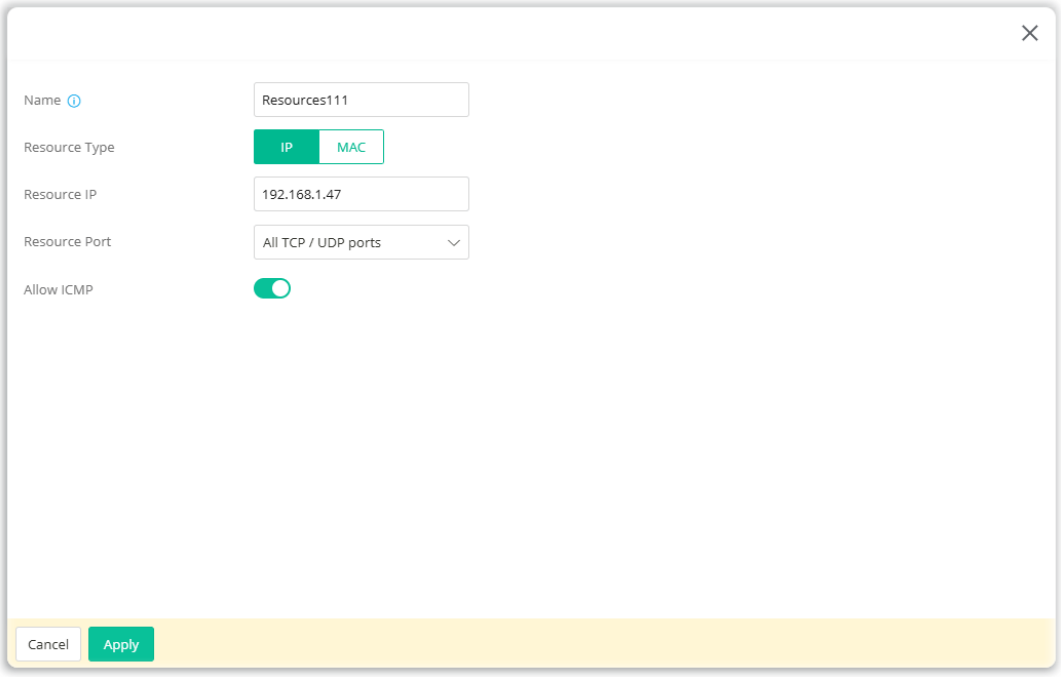
After finishing this web page configuration, please click **Apply** to save the settings.

## II-3-3 Resources

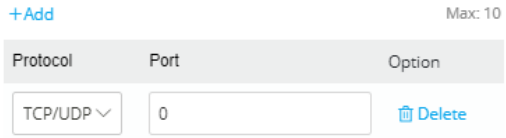
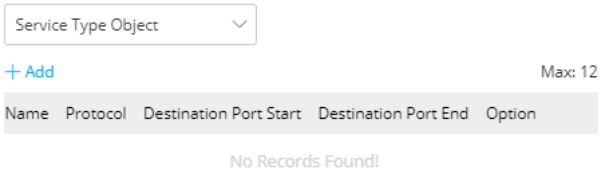
This page assists to lock down source objects under IAM control by specifying their **IP**, corresponding **MAC** addresses and the port type.




To add a new resources profile (up to 50), click **+Add**.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Name** | Enter a name for identification. |
| **Resource Type** | Select **IP** or **MAC** as the resource type. |
| **Resource IP / MAC** | Enter the IP address or MAC address according to the resource type selected for this profile. |
| **Resource Port** | Select the resource port type.<br>• **All TCP/UDP ports** - Transmission Control Protocol and User Datagram Protocol<br>• **All TCP ports** - Transmission Control Protocol<br>• **All UDP ports** - User Datagram Protocol<br>• **Specify ports** – Select this port type and set the port number for TCP/UDP, TCP, or UDP respectively.<br><br>• **Service Type Object** – Up to 12 service-type object profiles can be set in this field.<br><br>Click **+Add** to display the available service type list to the right side. Select the one(s) you want. |
| **Allow ICMP** | It's for diagnostic and control purposes, to send error messages about IP operations, messages about requested services, or messages about the reachability of a host or router. |

| | |
|---|---|
| Cancel | Discard current settings and return to the previous page. |
| Apply | Save the current settings and exit the page. |

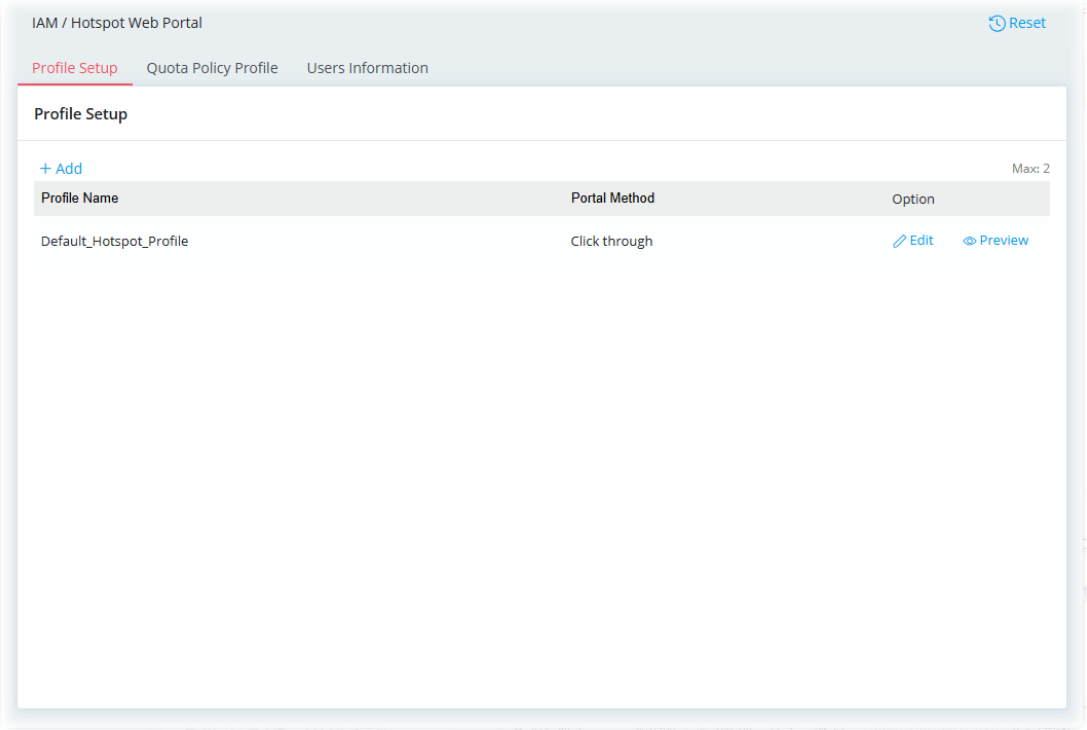
After finishing this web page configuration, please click **Apply** to save the settings.

# II-3-4 Hotspot Web Portal

The Hotspot Web Portal, or the so-called captive portal allows you to control and manage access from LAN users.

## II-3-4-1 Profile Setup

It is also a manner of IAM to identify, authenticate, and authorize any Access from the LAN or redirect to your appointed landing page.

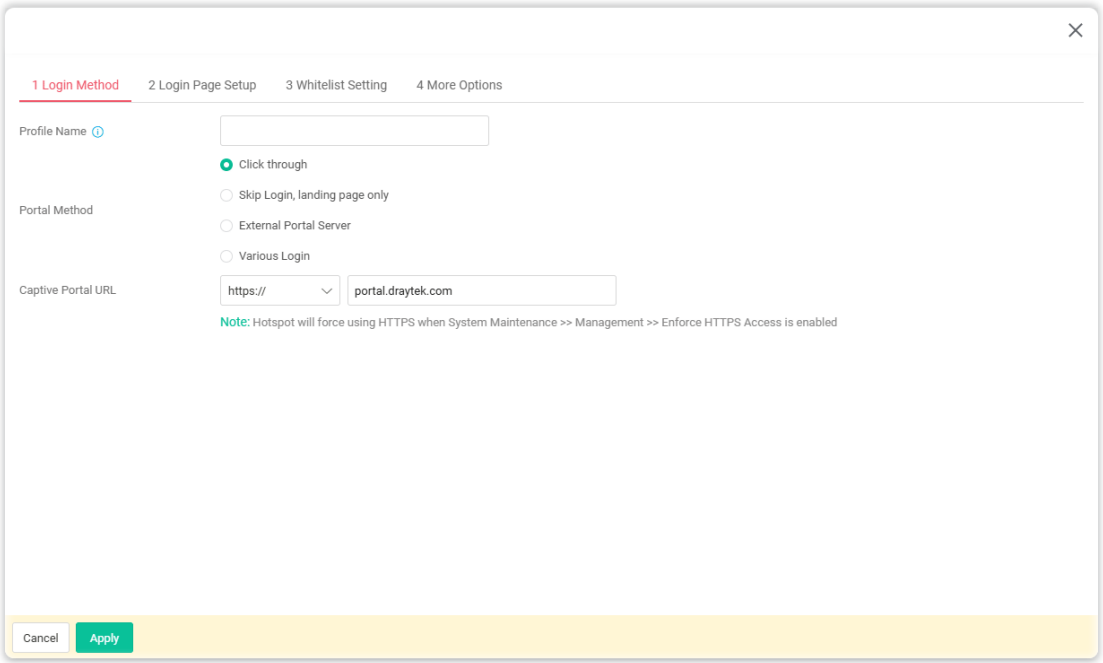



To add a new hotspot profile (up to 2), click **+Add**.

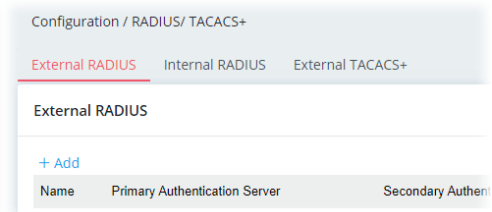
Click Login Method, Login Page Setup, Whitelist Setting, and/or More Options for detailed configuration.

### 1 Login Method

At present, there are three login methods to choose from for authenticating network clients: **Click Through**, **Skip Login, landing page only**, **External Portal Server** and **Various Login**. Each login mode will present a different web page to users when they connect to the network.



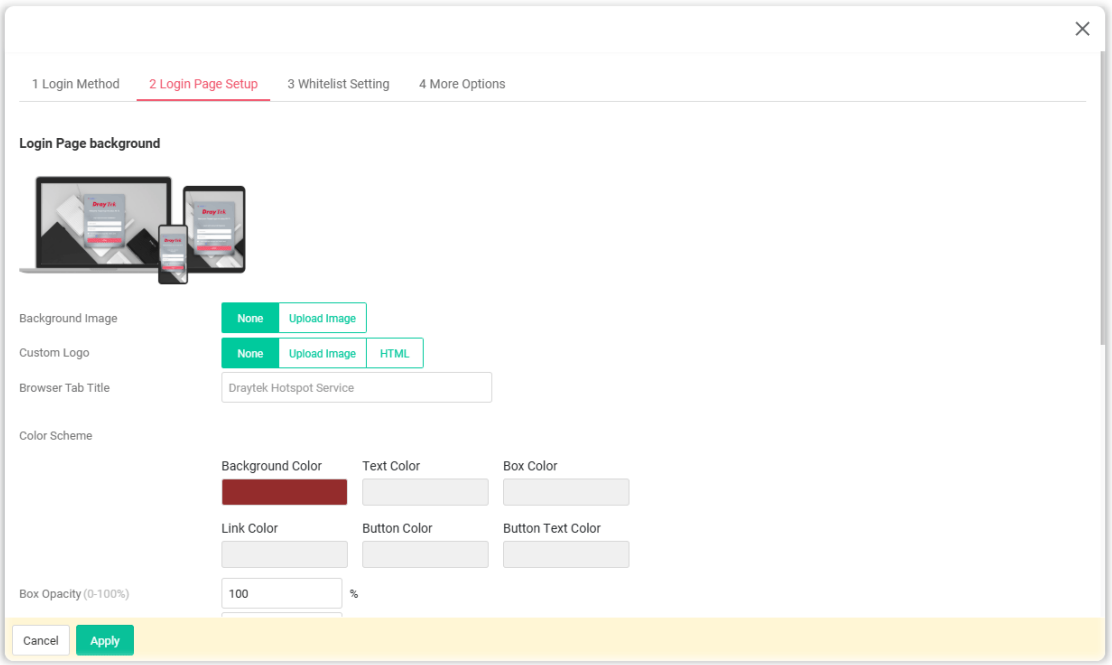

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Profile Name** | Enter a name for identification. |
| **Portal Method** | **Click through** – The user will be redirected to the landing page (defined in Captive Portal URL) and be granted access to the Internet.<br>**Skip Login, landing page only** – This mode does not perform any authentication. The user will be redirected to the landing page. The user can then leave the landing page to visit other websites.<br>**External Portal Server** - External RADIUS server will authenticate the users when they attempt to access the Internet for the first time via the router.<br>**Various Login** - An authentication page will appear when users attempt to access the Internet for the first time via the router. After authenticating themselves using a Facebook account, Google account, PIN code, password for RADIUS sever, they will be redirected to the landing page and be granted access to the Internet. |
| **Captive Portal URL** | Enter the captive portal URL. |
| **Redirection URL** | It is available when the External Portal Server is selected as the Portal Method.<br>Enter the URL to which the client will be redirected. |
| **RADIUS Server** | **External RADIUS Server Profile** - To configure the RADIUS server, click the External RADIUS link and you will be presented with the configuration page.<br> |

| | |
|---|---|
| | **RADIUS MAC Authentication** – Switch the toggle to enable/disable the function. If the RADIUS server supports authentication by MAC address, enable **RADIUS MAC Authentication** and select the MAC address format that is used by the RADIUS server.<br>**MAC Address Format** - Select the MAC address format.<br>**RADIUS NAS-Identifier** - Enter an ID. |
| **Login Method** | This setting is available when **Various Login** is selected as the portal method.<br>Select one or more desired login methods. Switch the toggle to enable the desired item.<br>• **Facebook**<br>• **Google**<br>• **PIN via SMS**<br>• **PIN via Mail**<br>• **RADIUS**<br>• **Leave Info**<br>**Facebook -** This setting is available when **Facebook** is selected as the login method.<br>• **Facebook APP ID** - Enter a valid Facebook developer app ID.<br>• **Facebook APP Secret** - Enter the secret configured for the APP ID entered above.<br>**Google -** This setting is available when **Login with Google** is selected as the login method.<br>• **Google App ID** - Enter a valid Google app ID.<br>• **Google App Secret** - Enter the secret configured for the APP ID entered above.<br>**PIN via SMS -** This setting is available when **Receive PIN via SMS** is selected as the login method.<br>• **SMS Provider** - Select the SMS Provider to send PIN notifications.<br>• **SMS Content** – Enter a message.<br>**PIN via Mail -** This setting is available when **Receive PIN via Mail** is selected as the login method.<br>• **Mail Server** - Select the mail server to send PIN notifications.<br>• **Mail Content** – Enter a message.<br>**Table (for Leave Info) –** This setting is available when **Leave Info** is selected as the login method.<br>• **+Add** – Click to add a new entry (up to 10) of leave info.<br>• **Info Type** – Select the information (e.g., General Info, Phone, Email or Checkbox) that the client needs to offer for connection.<br>• **Required** – If enabled, items on the login page will ask for entering required information for further connection.<br>• **Title** – Enter the heading of the Leave Info.<br>• **Content** – Enter the placeholder for the Leave Info.<br>• **Option (Delete)** – Click to remove the selected entry. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings and exit the page. |

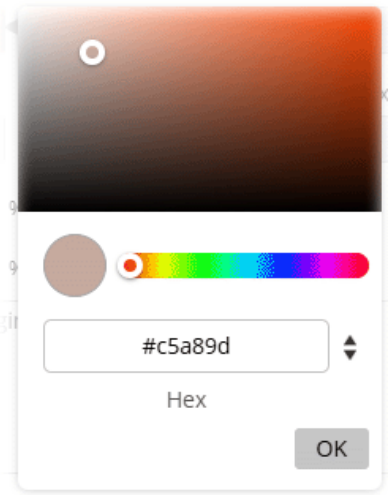
## 2 Login Page Setup

If you have selected a Login Mode that requires authentication, click **Login Page Setup** to select a background for the login page.



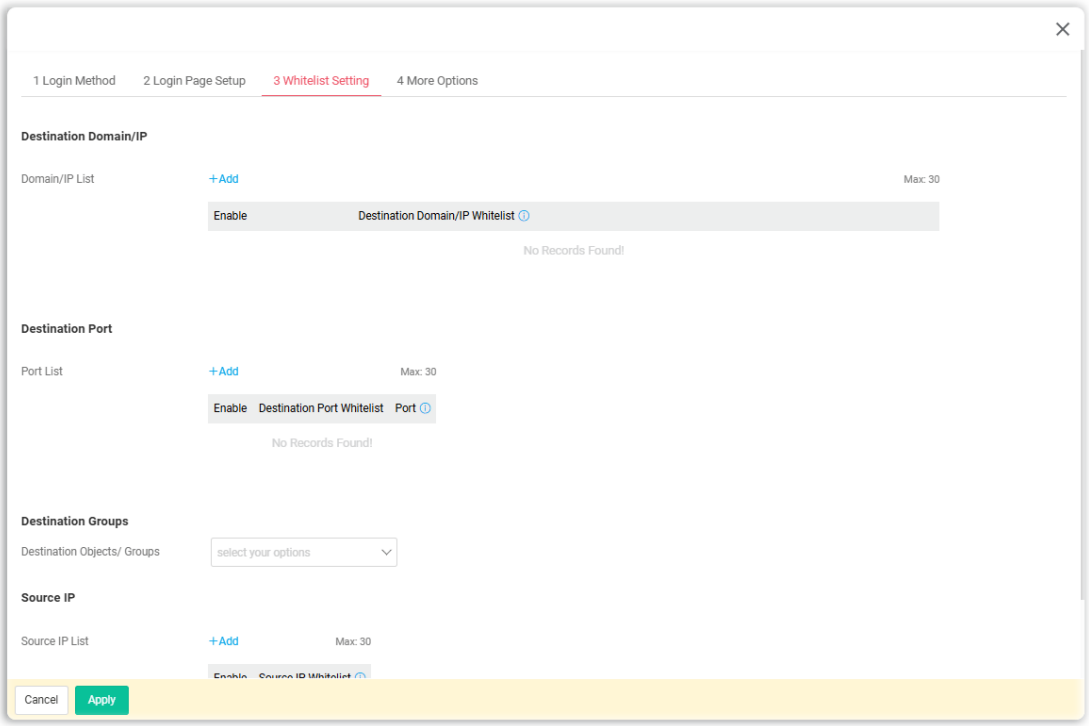

Available settings are explained as follows:

| Item | Description |
|---|---|
| | **Login Page background** |
| **Background Image** | Set the login page background scheme.<br>**None** – No image will be used.<br>**Upload Image** – Click to select an image file (.JPG or .PNG format) as the background image. The file size must be less than 5MB.<br>• **Current Background Image** – Click **Upload** to upload the selected file to Vigor router system. |
| **Custom Logo** | Set a logo displayed on the portal.<br>**None** – DrayTek default logo will be used.<br>**Upload Image** – Click to use another image as the logo. The file size must be less than 1MB.<br>• **Current Logo Image** – Click **Upload** to store the selected file to Vigor router system. |
| **Browser Tab Title** | Enter the text to be shown as the webpage title in the browser. |
| **Color Scheme** | Set the color used for the background, text, box, link, button and button text. A color box will appear for you to drag your mouse cursor on it to choose the color you want. |

| | |
|---|---|
| |  |
| **Box Opacity** | Set the opacity of the background image. |
| **Box Shadow** | Set the transparency (0 – 100%) of login column. |
| **Welcome Message** | Enter the text to be displayed as the welcome message. |
| **Privacy Policy & Terms and Condition** | |
| **Terms and Conditions** | Switch the toggle to enable the function.<br>**User must tick to get the internet access** – If selected, any user wishing to access the Internet must agree to the terms and conditions by ticking the box. Otherwise, the Vigor system will deny the Internet access. |
| **Terms and Conditions Content** | Select **Internal Content** or **External Content**.<br>**Internal Content** - Enter the text to be displayed in the Terms and Conditions pop-up window.<br>**External Content** - Enter a URL. After clicking the link of Terms and Conditions on the hotspot login page, the client will be redirected to access the web page of the URL specified here. |
| **Data Collection for Marketing** | Switch the toggle to enable the function.<br>**User must tick to get the internet access** – If selected, any user wishing to access the Internet must agree to the terms and conditions by ticking the box. Otherwise, the Vigor system will deny the Internet access.<br>**Marketing Content -** Enter the text to inform the user. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings and exit the page. |

## 3 Whitelist Setting

In this page you can configure the whitelist settings. Users are allowed to send and receive traffic that satisfies whitelist settings.



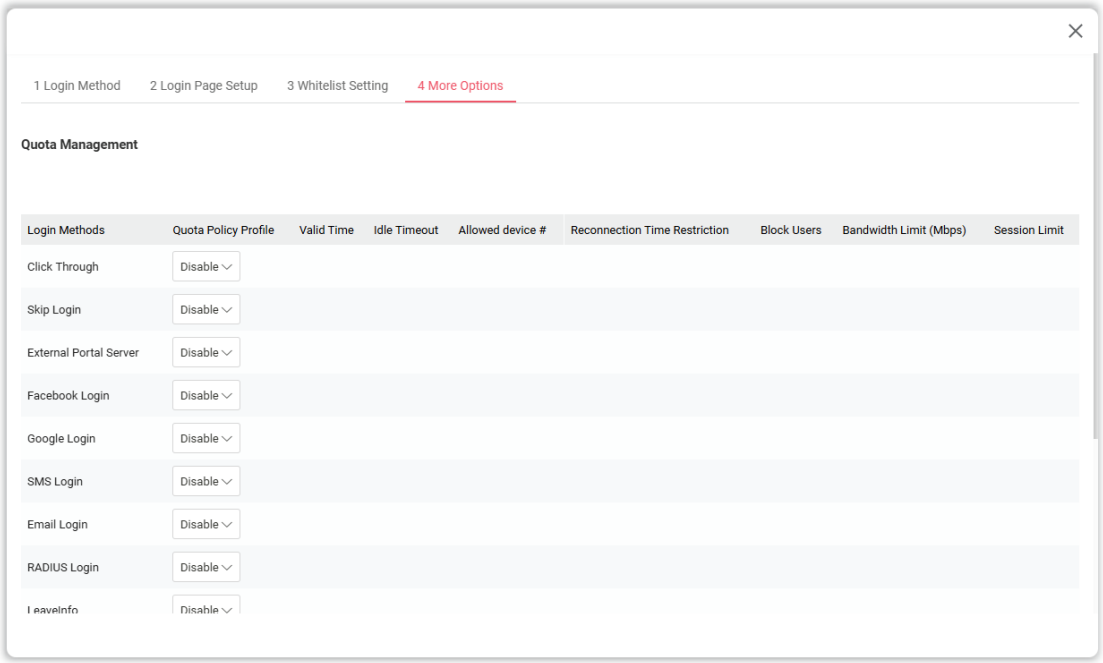

Available settings are explained as follows:

| Item | Description |
|---|---|
| | **Destination Domain/IP** |
| **Domain/IP List** | **+Add –** Click to add a new entry.<br>**Enable** – Switch the toggle to enable/disable the setting.<br>**Destination Domain/IP Whitelist** – Please enter IP address or domain name without the 'http://' or 'https://' prefix.<br>**Option (Delete)** – Remove current entry. |
| | **Destination Port** |
| **Port List** | **+Add –** Click to add a new entry.<br>**Enable** – Switch the toggle to enable/disable the setting.<br>**Destination Port Whitelist** – Select TCP, UDP, or TCP/UDP. The, enter the port number.<br>**Port** – Enter a number.<br>**Option (Delete)** – Remove current entry. |
| | **Destination Groups** |
| **Destination Objects/ Groups** | Select one IP object/group or multiple IP objects/groups as the destination.<br>The selected groups are allowed to be accessed. |
| | **Source IP** |
| **Source IP List** | The selected IPs are allowed through the router.<br>**+Add –** Click to add a new entry.<br>**Enable** – Switch the toggle to enable/disable the setting.<br>**Source IP Whitelist** – Enter the IP address.<br>**Option (Delete)** – Remove current entry. |
| **Cancel** | Discard current settings and return to the previous page. |

| | |
|---|---|
| **Apply** | Save the current settings and exit the page. |

## 4 More Options

In this step you can configure **advanced** options for the Hotspot Web Portal.



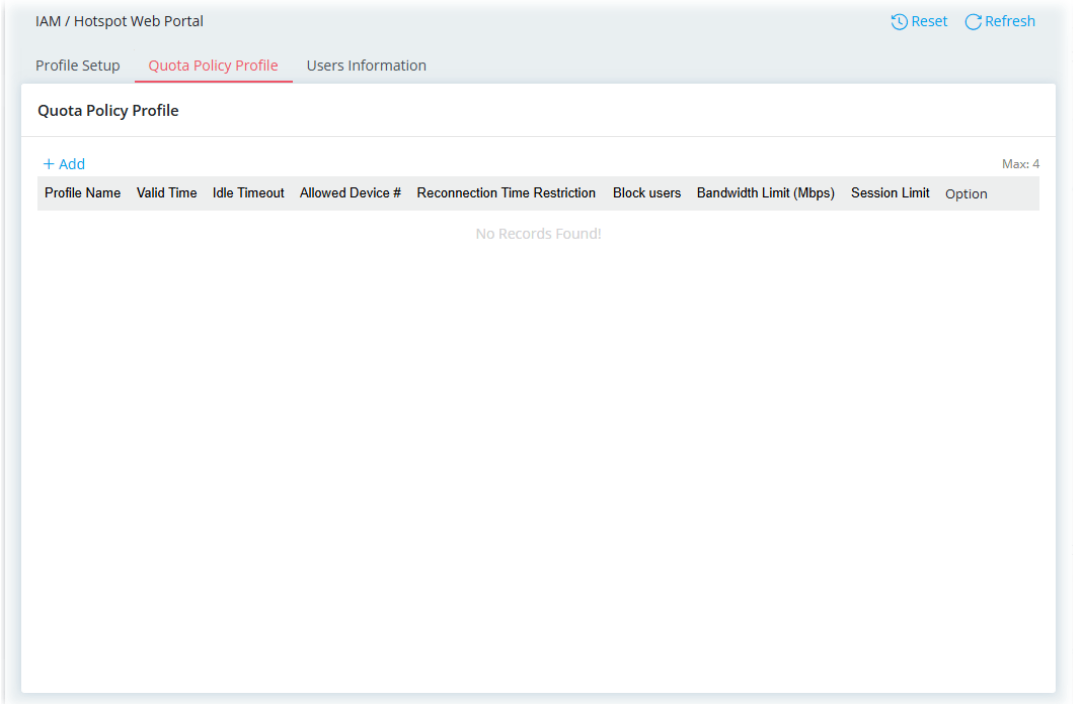

Available settings are explained as follows:

| Item | Description |
|---|---|
| | **Quota Management** |
| **Login Methods** | Show different login methods. Set individual quota policy profiles for each method. |
| **Quota Policy Profile** | Specify a quota policy profile for each login method.<br>The default is **Disable**.<br>Go to **IAM>>Hotspot Web Portal>>Quota Policy Profile** to configure several profiles, if required. |
| | **Landing Page After Authentication** |
| **Landing Page After Auth** | **Fixed URL** – Specifies the webpage that will be displayed after the user has successfully authenticated.<br>The user will be redirected to the specified URL. This could be used for displaying advertisements to users, such as guests requesting wireless Internet access in a hotel.<br>**User Requested URL** - The user will be redirected to the URL they initially requested. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings and exit the page. |

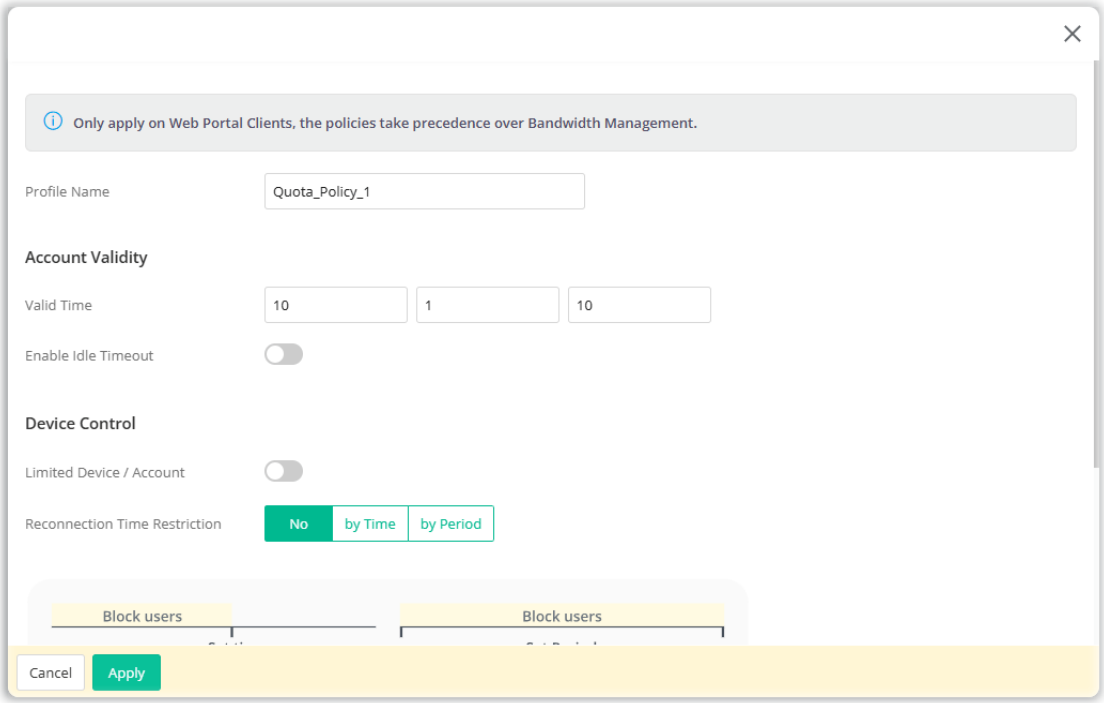
After finishing this web page configuration, please click **Apply** to save the settings.

## II-3-4-2 Quota Policy Profile

The system administrator can set restrictions on valid time, idle time, reconnection time, bandwidth, and session quotas that apply only to the web portal clients.




To add a new quota policy profile, click **+Add**.




Available settings are explained as follows:

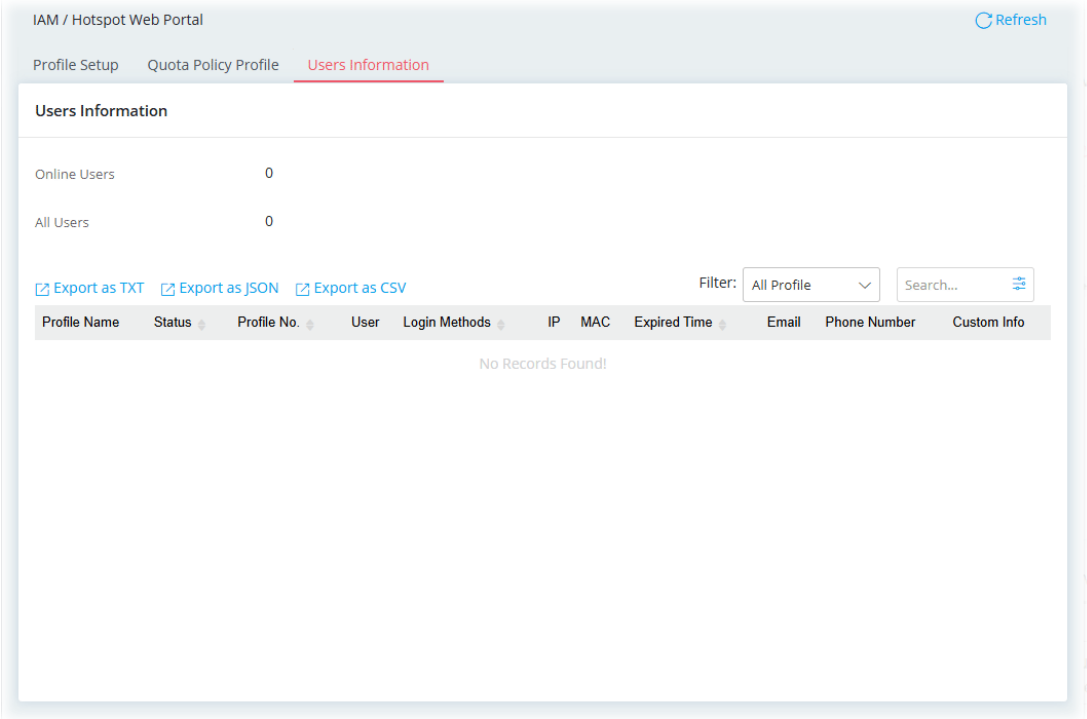
| Item | Description |
|---|---|
| **Profile Name** | Enter a name as the profile name. |

| | |
|---|---|
| **Account Validity** | |
| **Valid Time** | Configure the validity duration for login by setting days (0-180), hours (0-23), and minutes (0-59).<br>Once the login period expires, the Vigor router will disconnect the client from accessing the network or the Internet. If the client wishes to log in again, they will need to be verified or authenticated by the Vigor router. |
| **Enable Idle Timeout** | When this option is enabled, Vigor router will terminate the network connection if the is no activity from the user after the specified idle time has passed.<br>**Idle Timeout** – Enter a number (1-480, minutes). |
| **Device Control** | |
| **Limited Device / Account** | Set the maximum number of devices that can be connected for each account, and the time restriction for the client accessing Internet via the web portal.<br>Switch the toggle to enable or disable the function.<br>If enabled, set the number of Allowed device.<br>**Allowed device #** – Set the maximum number of devices that can be connected for each account, and the time restriction for the client accessing Internet via the web portal. The maximum is 100. |
| **Reconnection Time Restriction** | Blocks the account from being used to connect devices to the network in one of three ways:<br>**No** – No block.<br>**by Time** – After the login expires, the account cannot be used to connect devices to the network until the set time of day.<br>• **Block users before** – Choose the deadline (hour and minute) from the drop-down menu. When the time expires, the user's access will be disconnected and blocked.<br>**by Period** – After the login expires, the account cannot be used to connect devices to the network for a set period of time.<br>• **Block users for** – Enter the number of hours and minutes to specify the user block period. |
| **Bandwidth & Session Limit** | |
| **Bandwidth Limit** | Set the maximum upload and download speeds.<br>Switch the toggle to enable or disable the function.<br>If enabled, configure the following settings:<br>**Upload Limit / Download Limit** –Enter a number (1 to 9999). |
| **Session Limit** | Configure a maximum session limit for web portal clients.<br>Switch the toggle to enable or disable the function.<br>If enabled, configure the following setting:<br>**Sessions** – Enter a number (1 to 50000). |
| **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-3-4-3 Users Information

This page provides details about users (web portal clients) connected to this router.

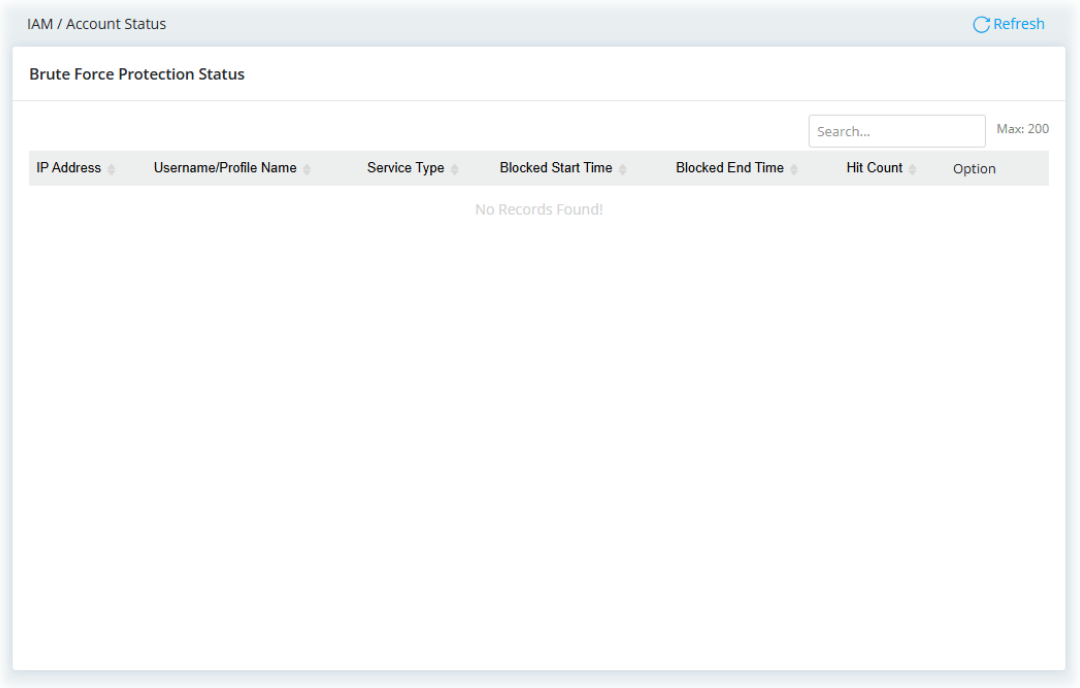



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Online Users** | Display the number of online users connected to the Internet via the Vigor router. |
| **All Users** | Display the total number of users (both online and offline) connecting to the Internet through the Vigor router. |
| **Export as TXT** | Click to export the user information as a TXT file. |
| **Export as JSON** | Click to export the user information as a JSON file. |
| **Export as CSV** | Click to export the user information as a CSV file. |
| **Filter** | Display the hotspot web portal profiles. |

# II-3-5 Account Status

This page displays the status of Brute Force Protection for the IAM user account (e.g., using FTP and IAM Service).

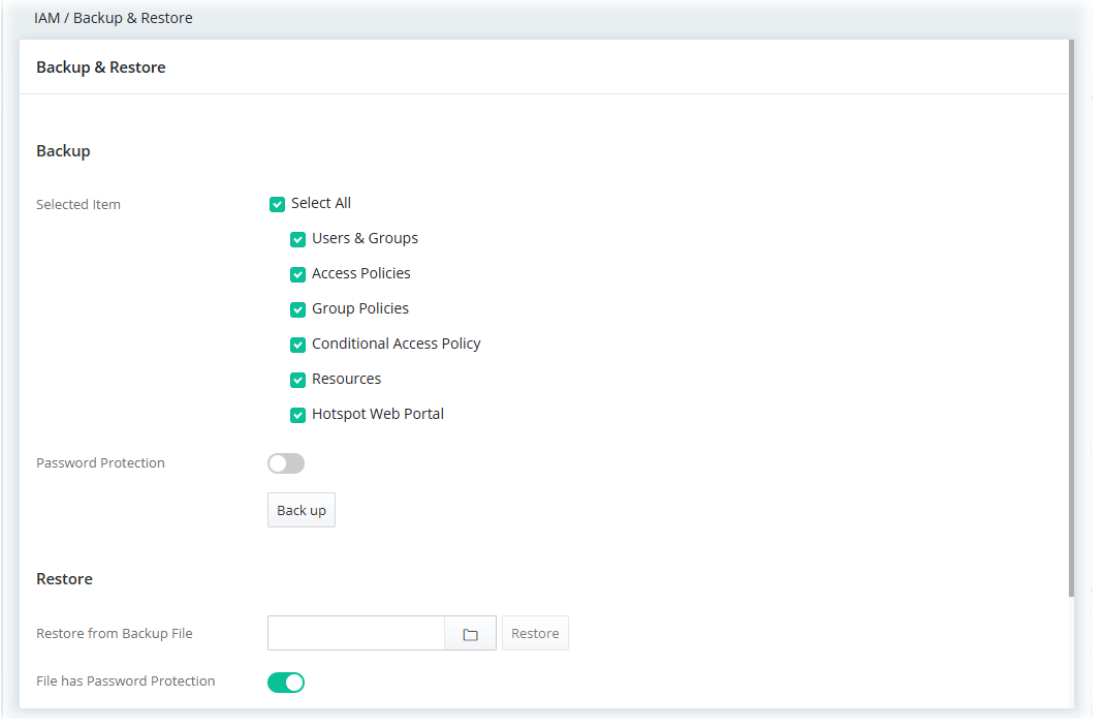



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Hit Count** | Displays the number of times an IAM user has triggered the Penalty or User Account Lockout. |
| **Option** | **Unblock** – Click to remove the blocked IPs.<br>**Add to Block List** - Add IPs to the Defense Setup's Allow/Block List. |

# II-3-5 Backup & Restore

This page can be used to backup/restore the IAM configuration.




Available settings are explained as follows:

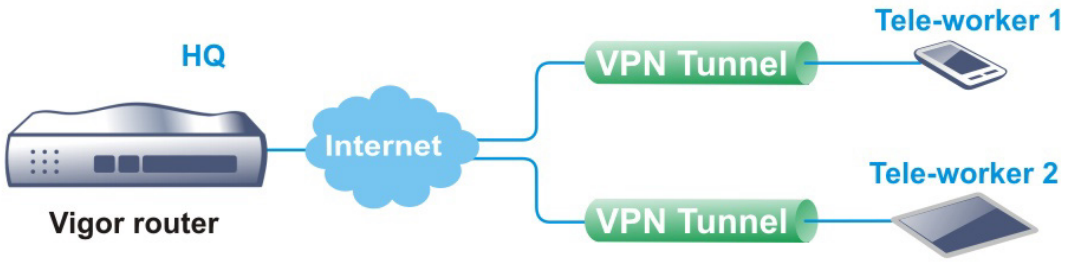
| Item | Description |
|---|---|
| | **Backup** |
| **Selected Item** | Select the policy or policies for the configuration backup. |
| **Password Protection** | For the sake of security, the configuration file for the access point can be encrypted.<br>Switch the toggle to enable/disable the function.<br>**New Password** – Enter a string as the new password.<br>**Confirm New Password** – Enter the string again for confirmation.<br>**Back up** – Click to save the settings. |
| | **Restore** |
| **Restore from Backup File** | - Click to locate the file for restoring.<br>**Restore** - Click to execute the restoration. |
| **File has Password Protection** | Switch the toggle to enable/disable the function. If enabled, a password will be required for restoring the configuration.<br>**Password** – Enter a string used for configuration restoration. |

# II-4 VPN

A Virtual Private Network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. In short, by VPN technology, you can send data between two computers across a shared or public network in a manner that emulates the properties of a point-to-point private link.

Here are some uses of VPNs:

- Communication between home office and customer.
- Secure connection between Teleworker, staff on business trip and main office.
- Exchange data between remote office and main office.
- POS between chain store and headquarters.
- Circumvention of Internet censorship that filters websites or contents.
- Circumvention of geolocation techniques employed by service providers or vendors to block or restrict services to users.
- Secure communications over public access points

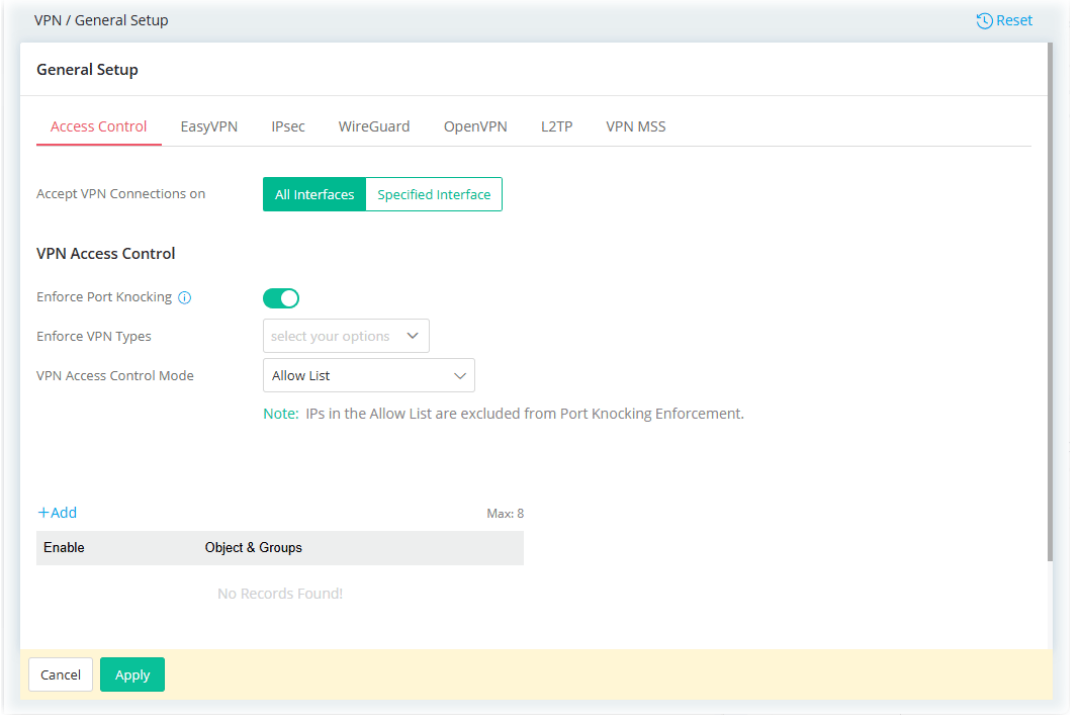



## II-4-1 General Setup

This section offers general settings for the VPN server with different types (e.g., EasyVPN, IPsec, WireGuard, OpenVPN, and L2TP).

### II-4-1-1 Access Control

Administrators can establish a secure VPN connection by configuring the interfaces allowed for VPN dial-in and pairing them with a whitelist or blacklist of VPN source IP addresses.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Accept VPN Connections on** | It can filter trusted VPN connections by setting up IP object/group allow lists or block lists.<br>Select the WAN interfaces to accept VPN connections.<br>**All Interfaces –** Accept the VPN connections on all WAN interfaces.<br>**Specified Interface –** Customize the WAN interface, IP address, and VPN protocols which allow the VPN connections.<br>**+Add –** Click to add up to 8 settings.<br>• **WAN** – Select the WAN interface.<br>• **IPv4 Address** – Select the WAN IP address (Default WAN IP) or disable this option.<br>• **Allowed VPN Protocols** – There are four protocols (IPsec, WireGuard, OpenVPN, L2TP and EasyVPN). Select the one(s) allowed for VPN connection.<br>• **Option** – Click **Delete** to remove the selected interface. |
| **VPN Access Control** | |
| **Enforce Port Knocking** | Switch the toggle to enable/disable the Port Knocking function.<br>**Enforce VPN Type** – Select the service protocol(s). Only the source IP addresses that complete Port Knocking successfully will be permitted to access these selected services (from the WAN interface); all others will be denied. |
| **VPN Access Control Mode** | It can filter trusted VPN connections by setting up IP object/IP group/country object allow lists or block lists.<br>**Allow All Connections** – Accept the VPN connections from all clients.<br>**Allow List** – Accept VPN connections from users within the IP object/IP group/country object settings selected below.<br>• **+Add** - Click to have a new entry setting. |

| | |
|---|---|
| | **Block List** – Deny VPN connections from users within the IP object/IP group/country object settings selected below.<br>• **+Add** - Click to have a new entry setting. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings and exit the page. |

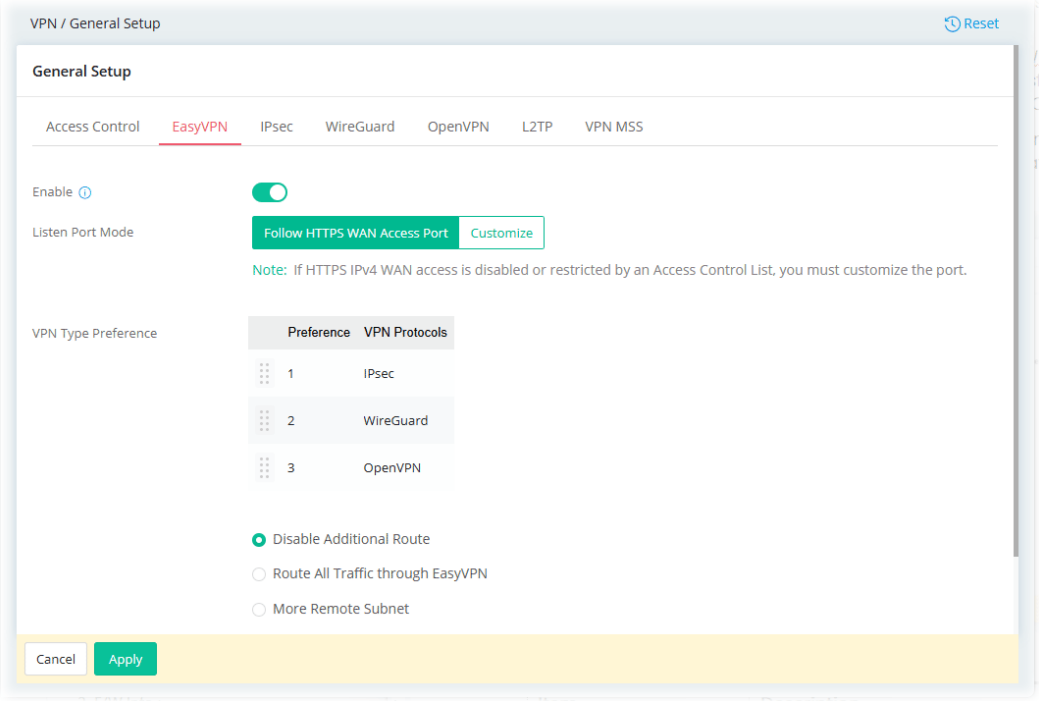
After finishing this web page configuration, please click **Apply** to save the settings.

## II-4-1-2 EasyVPN

The Vigor router supports multiple VPN protocols, including IPsec, WireGuard, and OpenVPN. However, general users may find it challenging to choose the right protocol or may face difficulties during the VPN setup. Additionally, environmental factors can sometimes prevent a successful VPN connection. To address these issues, the Vigor router introduces a new protocol called EasyVPN, designed to simplify the process.

With EasyVPN, users no longer need to generate keys for WireGuard, import configuration files for OpenVPN, or upload certificates. To establish a successful VPN connection, users simply need to enter their username and password or obtain an OTP code via email.

Moreover, if a VPN connection cannot be established for any reason, the Vigor system will automatically switch the EasyVPN connection to the next available protocol and attempt to reconnect.




Available settings are explained as follows:

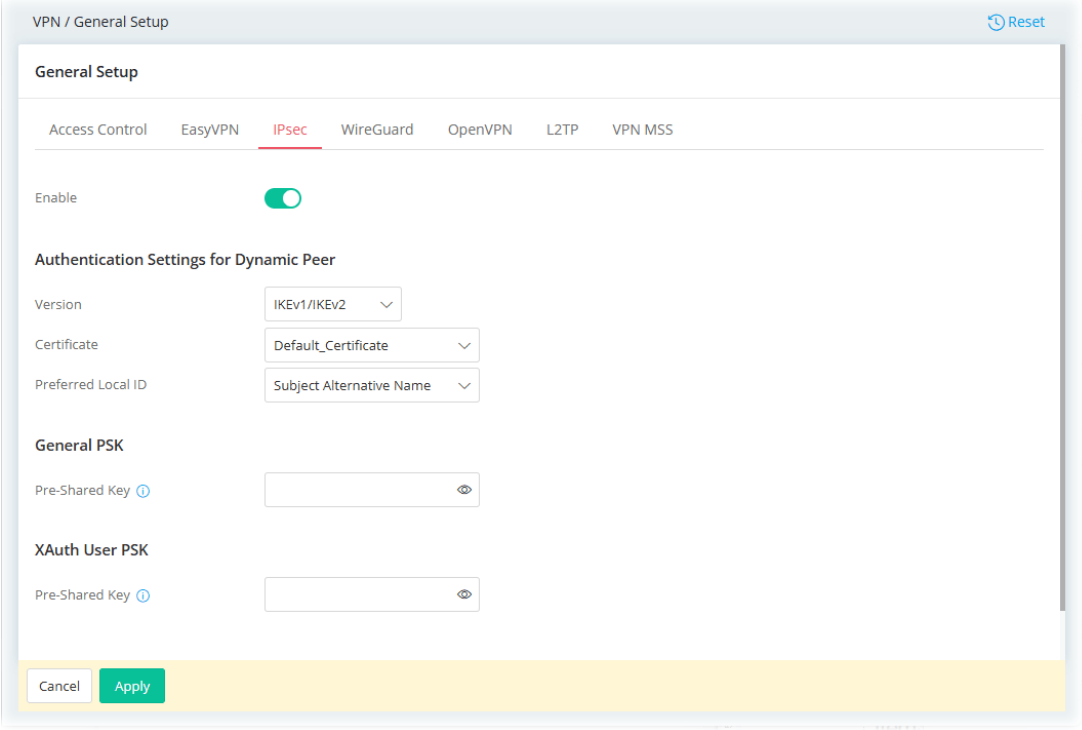
| Item | Description |
|---|---|
| **Enable** | Switch the toggle to enable/disable this service. |
| **Listen Port Mode** | Configure the ports that the EasyVPN service listens to.<br>**Follow HTTPS WAN Access Port –** For the EasyVPN service, use the same port as the HTTPS management port. Ensure that HTTPS management from the WAN is enabled to allow communication between the EasyVPN client and the EasyVPN server.<br>**Customize –** Select to define the listening port number manually.<br>• **Listen Port –** Enter a port value (1-65535). |
| **VPN Type Preference** | This feature enables users to customize the priority of their Dial-In VPN connections. By default, the order is based on VPN performance, arranged as follows: IPsec VPN > WireGuard VPN > OpenVPN.<br>To change the order, simply drag and rearrange the items in the provided interface.<br>**Preference –** Display the order of the VPN protocols. |

| | |
|---|---|
| | **VPN Protocols –** Display the name of the VPN protocols. |
| **Disable Additional Route** | If this feature is selected (enabled), the additional routes (created in More Remote Subnets) will not be used for VPN connection. |
| **Route All Traffic through EasyVPN** | If this feature is selected (enabled), **all traffics** will be routed through EasyVPN. |
| **More Remote Subnet** | Select this feature to create more subnets for Vigor router offering VPN service to remote clients.<br>**+Add** - Click to have a new entry setting. Up to 8 profiles can be created for VPN connection.<br>**Remote Network** – Enter the IPv4 address of the remote client.<br>**Subnet Mask** – Use the drop-down list to specify the subnet mask for the remote client.<br>**Option** – Click Delete to remove the selected interface. |
| **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-4-1-3 IPsec

IPsec (Internet Protocol Security) encrypts and authenticates network traffic, ensuring secure data transmission over VPNs. It protects against unauthorized access, data tampering, and eavesdropping, making it ideal for remote work, site-to-site and teleworker connections, while safeguarding sensitive information across untrusted networks.




Available settings are explained as follows:

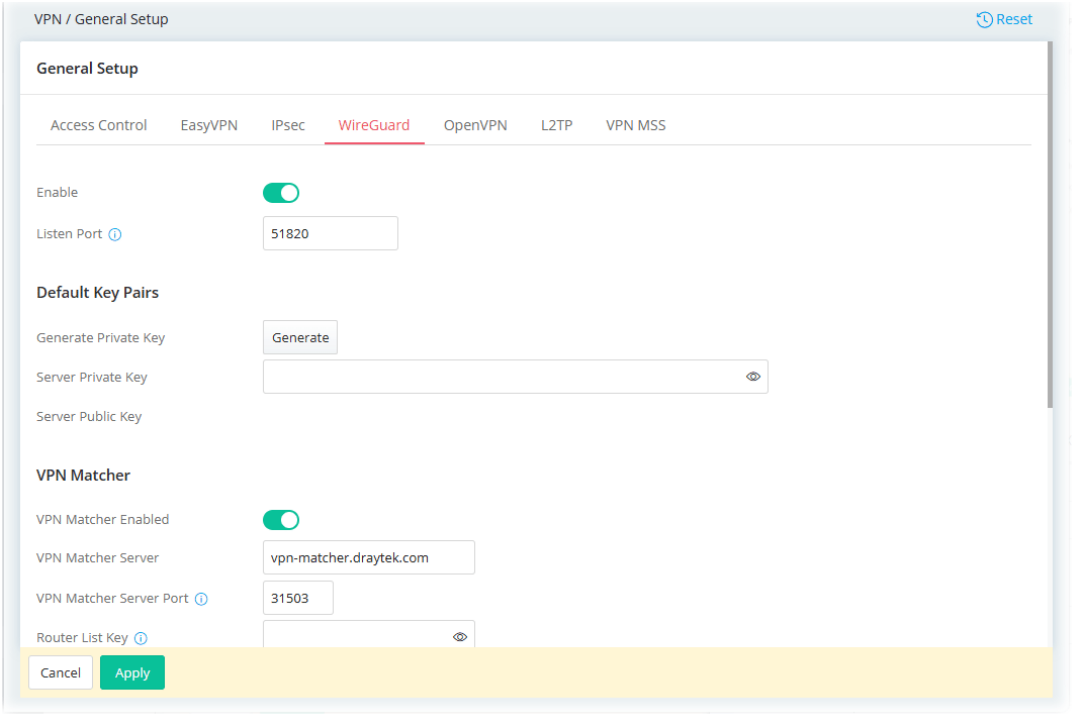
| Item | Description |
|---|---|
| **Enable** | Switch the toggle to enable/disable the settings. |
| | **Authentication Settings for Dynamic Peer** |

| | |
|---|---|
| Version | Select the protocol - IKEv1, IKEv2 or IKEv1/IKEv2. |
| Certificate | Select a router VPN server certificate. It will be used for X.509 authentication in the IPsec connection.<br>To set up certificates on the router, go to the Configuration>>Certificates section. |
| Preferred Local ID | Select Alternative Subject Name or Subject Name.<br>Specify the preferred local ID information (Alternative Subject Name or Subject Name) for IPsec authentication. |
| General PSK | Pre-Shared key - Define the PSK key for general authentication. |
| XAuth User PSK | Pre-Shared Key - Define the PSK key for IPsec XAuth authentication. |
| 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-4-1-4 WireGuard

WireGuard is a secure, fast, and modern open-source VPN Protocol. This VPN connection can build a VPN by exchanging private and public keys between VPN servers (e.g., Vigor router) and VPN clients (e.g., WireGuard VPN Client).




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Switch the toggle to enable/disable the settings. |
| **Listen Port** | Enter a port number for WireGuard VPN server.<br>The default number is 51820. |
| | **Default Key Pairs** |
| **Generate Private Key** | **Generate** – Click to generate keys (private and public) for the VPN server. |
| **Server Private Key** | Displays the private key generated. |
| **Server Public Key** | It is required to be configured in the WireGuard VPN client router.<br>After clicking **Generate**, the public key will be shown on this page. |
| | **VPN Matcher** |
| **VPN Matcher Enabled** | This VPN matching technology is built on the standard WireGuard VPN protocol.<br>Normally, to establish VPN connection, at least one peer must have a public IP address. The VPN Matcher server can help two Draytek routers behind NAT establish a secure VPN tunnel for data transmission between each other.<br>Switch the toggle to enable/disable the VPN Matcher function.<br>Note that only the drayos4 model, which supports WireGuard, can establish a VPN connection with VigorC410/C510 via the matcher. |
| **VPN Matcher Server** | The IP address of the DrayTek VPN Matcher server is defined as |

| | |
|---|---|
| | "vpn-matcher.draytek.com". |
| **VPN Matcher Server Port** | The IP address of the DrayTek VPN Matcher server is defined as "vpn-matcher.draytek.com" with the port number "31503". |
| **Router List Key** | Enter the authentication key for finding a Vigor router with the same group of this device from the VPN matcher server. Then set a VPN link between Vigor routers on both ends via VPN wizard. |
| **STUN Server** | **Detect** - Click to check if the NAT used by Vigor router is core NAT or not. If not, no VPN can be established. |
| **Detect Status** | **Get Device List -** After entering the Authkey above, click to get available Vigor router which is within the same group as this device. |
| **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-4-1-5 OpenVPN

The OpenVPN protocol utilizes public keys, certificates, and usernames and passwords to authenticate the client. Traffic is carried over secure channels built upon industry-standard SSL/TLS encryption protocols.

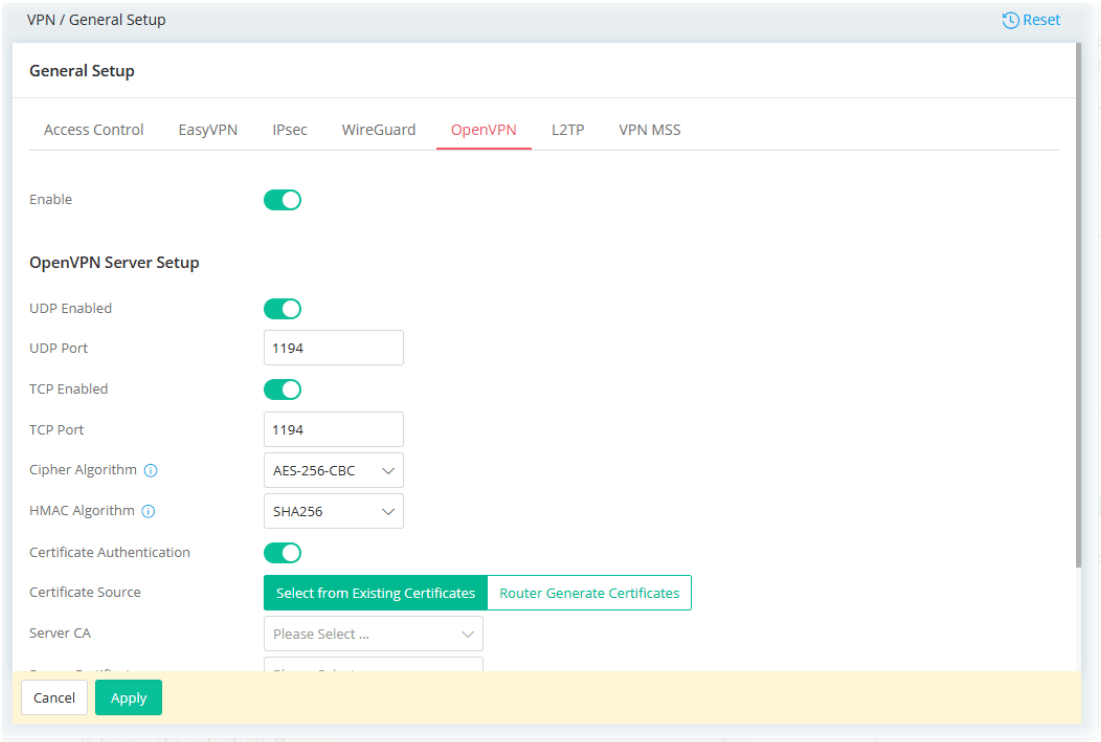
With integrating of OpenVPN, Vigor router can help users to achieve more robust, reliable and secure private connections for business needs.

OpenVPN offers a convenient way for users to build a VPN between the local end and the remote end. There are two advantages of OpenVPN:

- It can be operated on different systems such as Windows, Linux, and MacOS.
- Based on the standard protocol of SSL encryption, OpenVPN can provide you with a scalable client/server mode, permitting multi-client to connect to a single OpenVPN Server process over a single TCP or UDP port.

In terms of credentials, the administrator can choose to let the router generate the certificates, or import certificates issued by third-party certificate authorities (CAs). When the router generates the certificates, it acts as the root CA to issue the trusted CA certificates. If, however, a certificate issued by a third-party CA is used, both the CA's certificate and the issued certificate need to be imported to the router in the Trusted CA Certificate and Local Certificate sections, respectively.

OpenVPN requires the use of certificates. Before establishing OpenVPN connection, general settings for OpenVPN service shall be configured first.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Switch the toggle to enable/disable the settings. |
| **OpenVPN Server Setup** | |
| **UPD Enabled** | Switch the toggle to enable/disable the UDP protocol for OpenVPN |

| | |
|---|---|
| | connections.<br>**UDP Port** - Enter the UDP port number. |
| **TCP Enabled** | Switch the toggle to enable/disable the TCP protocol for OpenVPN connections.<br>**TCP Port** - Enter the TCP port number. |
| **Cipher Algorithm** | Select the desired cipher algorithm. Two encryption algorithms are supported: AES128, AES192 and AES256. AES256 is more secure than AES128 but may result in lower performance because it incurs higher computational overhead. |
| **HMAC Algorithm** | HMAC stands for Hash-based Message Authentication Code. It is used to validate the data integrity and authenticity of the VPN data.<br>Select the desired HMAC hash algorithm. Two hash algorithms, SHA1 and SHA256, are supported. SHA256 is preferred as it is more robust and reliable than SHA1. |
| **Certificate Authentication** | Switch the toggle to enable if you would like to validate that the client certificate was issued by a trusted CA. |
| **Certificate Source** | Select a source for the certificate to be used for OpenVPN.<br>**Select from Existing Certificates** – Third-party certificates will be used for OpenVPN.<br>**Router Generate Certificates** – Router-generated certificates that will be used for OpenVPN. |
| **Server CA** | Use the dropdown list to select the trust CA certificate that has already been uploaded to the router.<br>To upload more Trusted CA certificates to the router, go to Certificate Configuration>>Certificates page and click the Trusted CA tab for obtaining more certificates. |
| **Server Certificate** | Use the dropdown list to select a server certificate that has already been uploaded to the router.<br>To upload more local certificates to the router, go to Certificate Configuration>>Certificates page and click Local Certificate tab for obtaining more certificates. |
| **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-4-1-6 L2TP

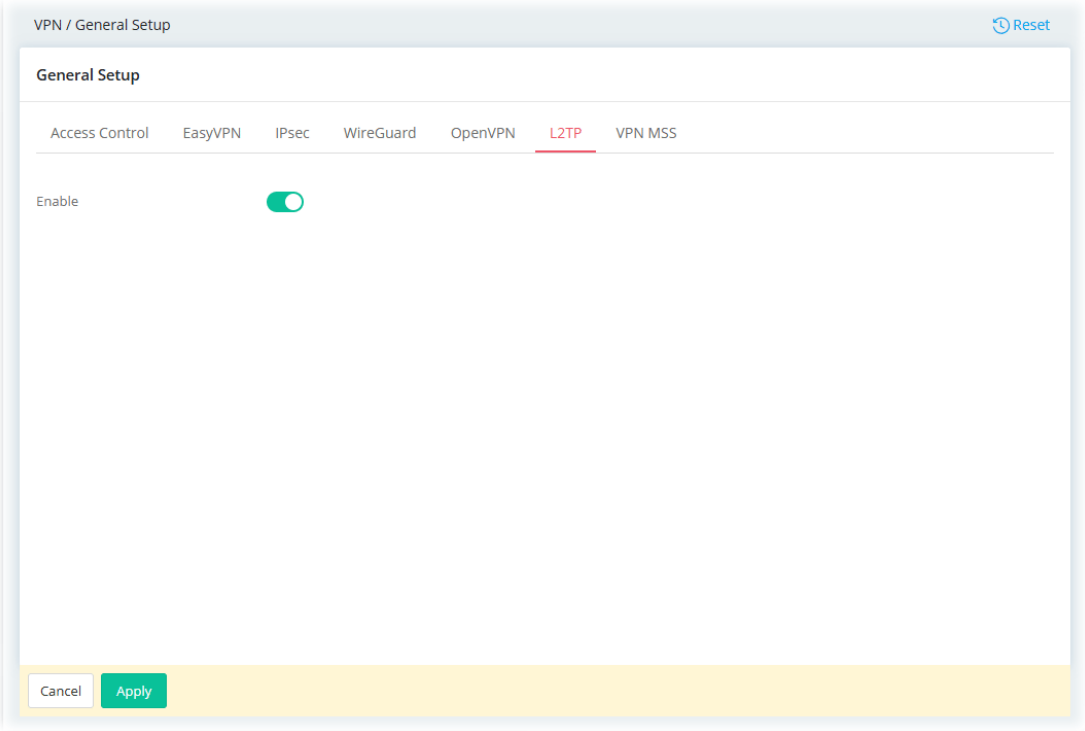
To establish a secure and encrypted tunnel for data transmission, this option will utilize the L2TP in conjunction with the IPsec encryption.

When this option is enabled, the device supports:

- VPN Site Dial-in connections using L2TP over IPsec
- Teleworker VPN connections using L2TP over IPsec

This allows remote users or branch sites to securely connect to the VPN gateway using a standard L2TP/IPsec connection.

To use the L2TP server as the protocol for VPN tunnel, switch the toggle to enable the L2TP server.

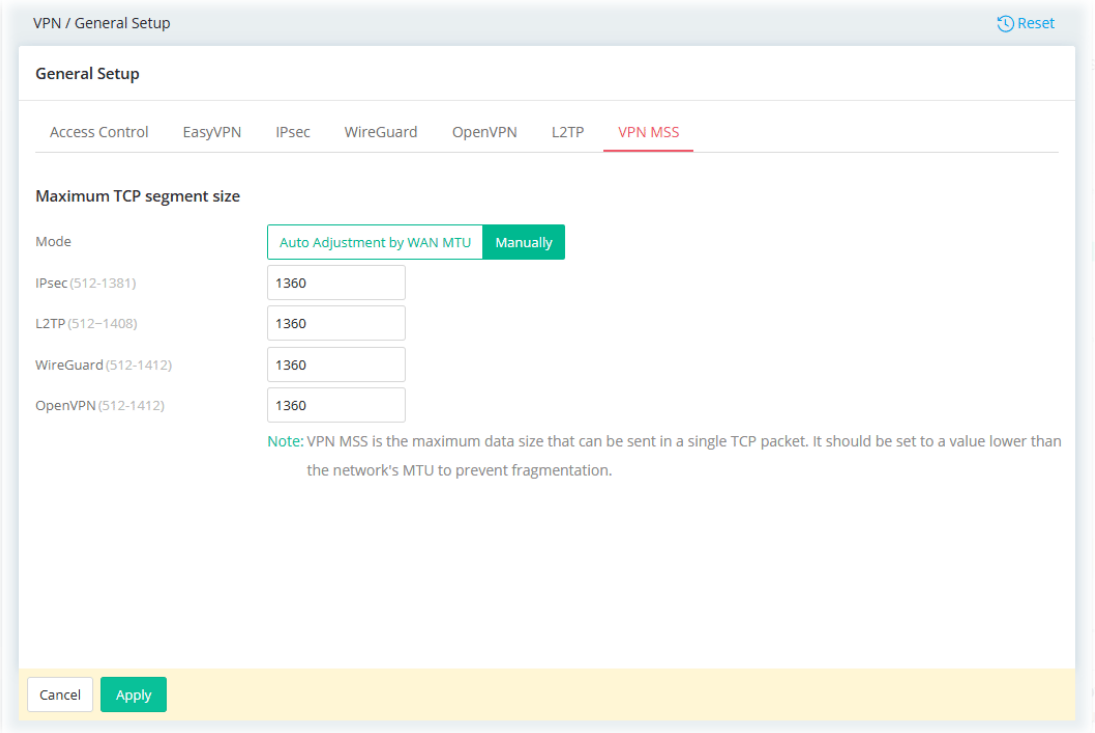



Switch the toggle to enable/disable the L2TP VPN connection. Click **Apply** to save the settings.

## II-4-1-7 VPN MSS

MSS is the abbreviation of Maximum TCP segment size.

This page is used to automatically adjust the TCP MSS value within a VPN tunnel. It optimizes packet size to prevent fragmentation and ensure the efficient data transmission over the network.



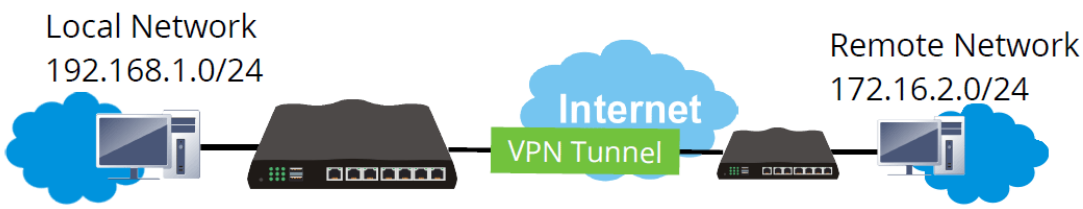

Available settings are explained as follows:

| Item | Description |
| --- | --- |
| Mode | **Auto Adjustment by WAN MTU** – Obtain the MSS value by automatically adjusting it according to the WAN MTU.<br>**Manually** - Please specify the MSS values for each type to avoid packets cut by MTU during the data transmission period via the VPN connection.<br>• IPsec<br>• L2TP<br>• WireGuard<br>• OpenVPN |
| Cancel | Discard current settings and return to the previous page. |
| Apply | Save the current settings and exit the page. |

## II-4-2 Site-to-Site VPN

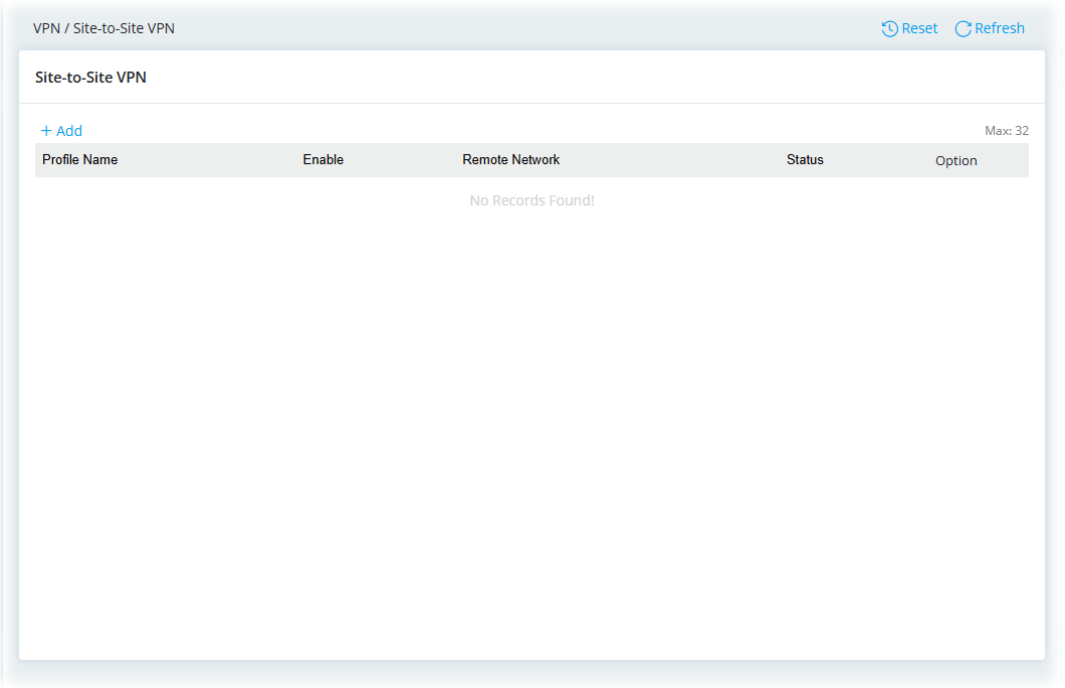
The VPN means a connection between two router's LAN networks, which

- Allows employees in branch offices and head office to share the same network resources.




- Configures the VPN server for inbound connections from other routers.

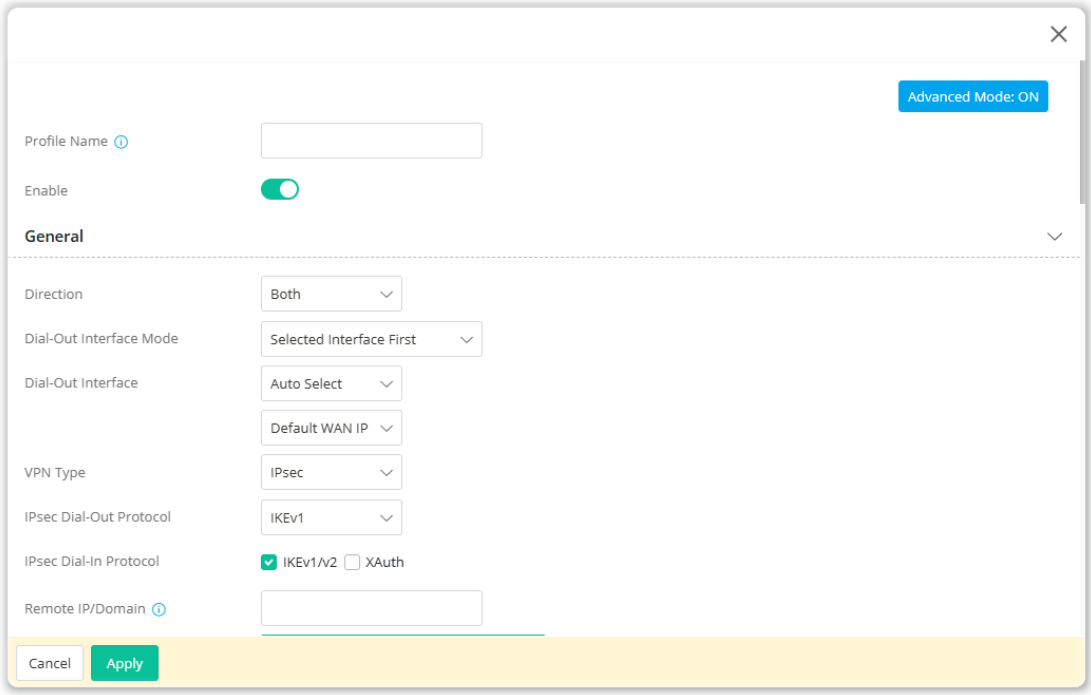
This page allows to configure the VPN server for inbound connections from other routers.




### II-4-2-1 VPN Type - IPsec

IPsec (Internet Protocol Security) encrypts and authenticates network traffic, ensuring secure data transmission over VPNs. It protects against unauthorized access, data tampering, and eavesdropping, making it ideal for remote work, site-to-site and teleworker connections, while safeguarding sensitive information across untrusted networks.

To add a new resources profile (IPsec VPN type), open VPN>>Site-to-Site VPN and click **+Add**.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Advanced Mode:ON/OFF** | Click to show or hide the advanced settings for the site-to-site VPN. |
| **Profile Name** | Enter the name of the profile. |
| **Enable** | Switch the toggle to enable/disable the settings. |
| | **General** |
| **Direction** | Specify the allowed call direction of this VPN profile.<br>**Both** – Profile is to be used to initiate (dial out) or accept (dial in) connections.<br>**Dial-Out** – Profile is to be used to initiate outgoing connections.<br>**Dial-In** – Profile is to be used to accept incoming connections.<br>**VPN Matcher** – This VPN matching technology is built on the standard WireGuard VPN protocol. The VPN Matcher server can help two Draytek routers behind NAT establish a secure VPN tunnel for data transmission between each other. Note that only the drayos4 model, which supports WireGuard, can establish a VPN connection with Vigor device via the matcher. |
| **VPN Type** | Select a VPN type for building the VPN connection.<br>**Direction on Dial-out** – Available VPN type includes:<br>• **IPsec**<br>• **OpenVPN**<br>• **WireGuard**<br>**Direction on Dial-In** – Available VPN type includes:<br>• **IPsec**<br>• **OpenVPN**<br>• **WireGuard**<br>**Direction on Both** – Available VPN type includes: |

| | |
|---|---|
| | • IPsec<br>• OpenVPN<br>**Direction on VPN Matcher** – Available VPN type includes:<br>• WireGuard<br>Other options related to the IPsec VPN type will be changed according to the Direction used.<br>**IPsec (with the direction on Both, Dial-In)** -<br>• IPsec Dial-In Protocol<br>• Dial-in Allowed Schedule<br>**IPsec (with the direction on Both, Dial-Out)**-<br>• IPsec Dial-Out Protocol<br>• Remote IP/ Domain<br>• Dial-Out Mode |
| **IPsec Dial-In Protocol** | Select a protocol to trigger an IPsec VPN connection through the Internet.<br>• IKEv1/v2<br>• XAuth. |
| **IPsec Dial-Out Protocol** | Select a protocol to trigger an IPsec VPN connection through the Internet.<br>• IKEv1<br>• IKEv2<br>• IKEv2 EAP<br>• XAuth. |
| **Dial-In Allowed Schedule** | **Always Allow** – Select this option to maintain an always on dial-out connection.<br>**Scheduled** – Select this option to make the VPN connection based on the schedule.<br>• **Drop the Active Tunnel when Schedule is Enforced** – Switch the toggle to enable/disable the function.<br>• **VPN Schedule** – Use the drop-down menu to specify one VPN profile. Before configuring the VPN Schedule, add the required time intervals in Configuration>> Objects>> Schedule. |
| **Remote IP/ Domain** | Enter IPv4 or hostname for the remote VPN server. |
| **Dial-Out Mode** | **On Demand** – The VPN connection will be triggered when detecting traffic going to the remote network.<br>**Always On** – Select this option to maintain an always on dial-out connection.<br>**Scheduled** –Select this option to make the VPN connection based on the schedule.<br>• **Drop the Active Tunnel when Schedule is Enforced** – Switch the toggle to enable/disable the function.<br>• **VPN Schedule** – Use the drop-down menu to specify one VPN profile. Before configuring the VPN Schedule, add the required time intervals in Configuration>> Objects>> Schedule. |
| **Username and Password** | |
| **Username** | It is available when XAuth is selected as IPsec Dial-In/Dial-Out Protocol.<br>Used by the remote LAN to establish a VPN connection. |

| | |
|---|---|
| **Password** | It is available when XAuth is selected as IPsec Dial-In/Dial-Out Protocol.<br>Used by the remote LAN to establish a VPN connection. |
| **IKE Authentication for Dial-Out/Both** | |
| **Dial-Out Settings** | It is available when **Dial-Out** is selected as the Direction and **IPsec** is selected as VPN Type. |
| **Negotiation** | It is available when IKEv1 is selected as IPsec Dial-Out Protocol.<br>Select **Main** mode or **Aggressive** mode. The ultimate outcome is to exchange security proposals to create a protected secure channel. The default value in Vigor router is Main mode.<br>**Main Mode** – **Main** mode is more secure than **Aggressive** mode since more exchanges are done in a secure channel to set up the IPsec session. However, the **Aggressive** mode is faster.<br>**Aggressive Mode** – **Main** mode is more secure than **Aggressive** mode since more exchanges are done in a secure channel to set up the IPsec session. However, the **Aggressive** mode is faster. |
| **Authentication** | It is available when using **IKEv1 (under Main Mode)** or **IKEv2** is selected.<br>**Pre-Shared Key** – Select as the authentication method.<br>• **Pre-Shared Key** – Input the characters as pre-shared key.<br>**Certificate** –Select as the authentication method.<br>• **Local Certificate** – Select one of the profiles set in Configuration>>Certificates Local Certificates.<br>• **Local ID** – Select Subject Name or Subject Alternative Name.<br>• **Peer ID** – Select Accept Subject Alternative Name, Peer Certificate, Accept Subject Name, Accept Any.<br>**Select Accept Subject Alternative Name** - The following three formats of Peer ID are acceptable, including IP Address, Domain Name, and Email.<br>**Peer Certificate** - Select a peer certificate that has been pre-obtained and stored in Configuration>>Certificates Local Certificates.<br>**Accept Subject Name** – Enter the complete certificate subject name.<br>**Accept Any** - Any certificate signed by a trusted CA in Configuration>>Certificates Trusted CA will be considered valid. |
| **IKE Identifier** | Set the local ID and Peer ID for identification.<br>Local ID and Peer ID are provided for certain connections that require specifying an ID, such as IKEv1 using Aggressive mode and IKEv2 (optional). |
| **Local ID** | Specify a local ID to be used when establishing a VPN connection using IPsec VPN type. |
| **Peer ID** | Enter the ID name for the remote client.<br>If the values are specified, only connections coming from the specified IP address and/or having the specified Peer ID will be accepted. |
| **IKE Authentication for Dial-In/Both** | |
| **Dial-In Settings** | It is available when **Dial-In** is selected as the Direction and **IPsec** is |

| | |
|---|---|
| | selected as VPN Type. |
| Negotiation | Select **Main** mode or **Aggressive** mode. The ultimate outcome is to exchange security proposals to create a protected secure channel. The default value in Vigor router is Main mode.<br>**Main Mode** – **Main** mode is more secure than **Aggressive** mode since more exchanges are done in a secure channel to set up the IPsec session. However, the **Aggressive** mode is faster.<br>**Aggressive Mode** – **Main** mode is more secure than **Aggressive** mode since more exchanges are done in a secure channel to set up the IPsec session. However, the **Aggressive** mode is faster. |
| Specify VPN Peer | It is available when IKEv1/v2 is selected as IPsec Dial-In Protocol.<br>This feature can restrict this IPsec to be initiated only by the specified peer IP address or domain name, and specify the private key to be used.<br>If enabled,<br>**Remote IP/Domain** – Enter the IP address of the remote peer.<br>**Pre-Shared Key** – Input characters as pre-shared key for authentication. |
| X.509 Digital Signature | It is available when IKEv1/v2 is selected as IPsec Dial-In Protocol.<br>To use an X.509 digital signature, select one of the authentication methods and enter the required information for each method.<br>**Select Accept Subject Alternative Name** - The following three formats of Peer ID are acceptable, including IP Address, Domain Name, and Email.<br>**Peer Certificate** - Select a peer certificate that has been pre-obtained and stored in Configuration>>Certificates Local Certificates.<br>**Accept Subject Name** – Enter the complete certificate subject name.<br>**Accept Any** - Any certificate signed by a trusted CA in Configuration>>Certificates Trusted CA will be considered valid. |
| IKE Identifier | Set the local ID and Peer ID for identification.<br>Local ID and Peer ID are provided for certain connections that require specifying an ID, such as IKEv1 using Aggressive mode and IKEv2 (optional). |
| Local ID | Specify a local ID to be used when establishing a VPN connection using IPsec VPN type. |
| Peer ID | Enter the ID name for the remote client.<br>If the values are specified, only connections coming from the specified IP address and/or having the specified Peer ID will be accepted. |
| More settings for IKE Authentication | |
| IKE Phase 1 | **Encryption** – Use Auto/AES/3DES/DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.<br>**Group** – Specify a key exchange proposal.<br>**Authentication** – Select SHA256 or SHA1 for packet authentication.<br>**Lifetime** - For security reason, the lifetime of key should be defined. The default value is 28800 seconds. You may specify a value in between 900 and 86400 seconds. |
| Force UDP | Switch the toggle to enable/disable the function. |

| | |
|---|---|
| Encapsulation | All IPsec packets will be encapsulated with UDP header if enabled. |
| Force Reauthentication | Switch the toggle to enable/disable the function.<br>If this option is enabled, it will reauthenticate identities for both sides when renewing the IPsec session. |
| IKE Phase 2 | Specify the security protocol, proposal encryption and proposal authentication.<br>**Security Protocol** – AH (Medium) means data will be authenticated, but not be encrypted. By default, this option is active. ESP (High) means payload (data) will be encrypted and authenticated.<br>**Encryption** – Use AES/3DES/DES encryption algorithm.<br>**Authentication** – Select All, SHA256 or SHA1 for packet authentication.<br>**Lifetime** – For security reason, the lifetime of key should be defined. The default value is 3600 seconds. You may specify a value in between 600 and 28800 seconds.<br>**Perfect Forward Secret** – Switch the toggle to enable/disable this function. PFS forces key exchange during Phase-2 periodic Rekey. |
| Phase 2 Network ID | Change the source IP address of VPN traffic to the specified IP address for the NAT mode selected in the Network field. |
| Dead Peer Detection | Dead Peer Detection (DPD) is the method to detect an IPsec connection.<br>**DPD Delay** – It is a keep-alive timer. A Hello message will be emitted periodically when a tunnel is idle. Use the value 0 to disable this function. The recommended value is 30 seconds if enabled.<br>**DPD Timeout** - It is the timeout timer. The peer will be declared dead once no acknowledge message is received after timeout value. Use the value 0 to disable this function. The recommended value is 120 seconds if enabled. |
| Network | |
| Network | Specify that traffic from the local subnet and remote subnet can pass through the VPN connection.<br>**Local Network** – The default value is 0.0.0.0, which means the Vigor router will get a PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP or L2TP.<br>**Subnet Mask** – Display the local network IP and mask for TCP / IP configuration. Select the one to meet the local network value.<br>**Remote Network** – The default value is 0.0.0.0, which means the Vigor router will get a remote Gateway PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP or L2TP.<br>**Subnet Mask** - Select the one to meet the local network value. It is used to add a static route to direct all traffic destined to this Remote Network IP Address/Remote Network Mask through the VPN connection. For IPsec, this is the destination clients IDs of phase 2 quick mode. |
| Routing/NAT Mode | **Routing Mode** – It enables a standard site-to-site VPN, where the traffic is directly routed between two networks without altering the |

| | |
|---|---|
| | source IP address.<br>**NAT Mode** – It modifies VPN traffic to the remote site by translating the source IP into a virtual IP address before sending it to the destination. |
| **More Remote Subnets** | It is used to add more static routes for subnets destined for the remote network.<br>**Disabled** – Disable this function.<br>**Multiple SAs** – Multiple SAs will establish different Phase 2 SAs based on the local network and remote network to provide additional security for data transmission. Select for adding new route.<br>• **+Add** – Click to add new static route. Enter required information for local network, subnet mask, remote network and subnet mask.<br>**More Subnets** – Add new static routes based on remote network to provide additional security for data transmission. Select for adding new route.<br>• **+Add** – Click to add new static route. Enter required information for remote network and subnet mask. |
| **Options under the Advanced Mode** | |
| **Dial-Out Interface Mode** | It is available when the call direction of this VPN profile is set to Dial-Out the Advanced Mode is ON.<br>Select the WAN connection for connections made using this profile. This setting is useful for dial-out only.<br>**Selected Interface First** – While connecting, the router will use the selected WAN interface first for VPN connection. If selected WAN fails, the router will try to use other WAN(s).<br>**Selected Interface Only** – While connecting, the router will use selected WAN as the only interface for VPN connection.<br>**Manual** – Customize VPN settings. Specify which WANs can be used as outgoing interfaces. |
| **Dial-Out Interface** | It is available when the call direction of this VPN profile is set to Dial-Out the Advanced Mode is ON.<br>**Auto Select** – Decide which interface to dial out based on the default route.<br>**Default WAN IP / IP Address** – Use the drop-down list to specify one WAN IP address for this VPN profile. |
| **Idle Timeout** | The tunnel will be disconnected when no traffic is detected within Idle Timeout. Disable this feature by setting the value to 0. |
| **GRE Over IPsec** | Switch the toggle to enable/disable the function.<br>It will verify data and transmit data in encryption with GRE over IPsec packet after configuring IPsec Dial-Out setting. Both ends must match for each other by setting same virtual IP address for communication.<br>**GRE Local IP** – Enter the virtual IP for router itself for verified by peer.<br>**GRE Remote IP** - Enter the virtual IP of peer host for verified by router. |
| **Netbios Naming over VPN** | Switch the toggle to allow/ deny NetBIOS naming packets to traverse through the VPN tunnel. |
| **Multicast over VPN** | Switch the toggle to allow/ deny multicast packets to traverse |

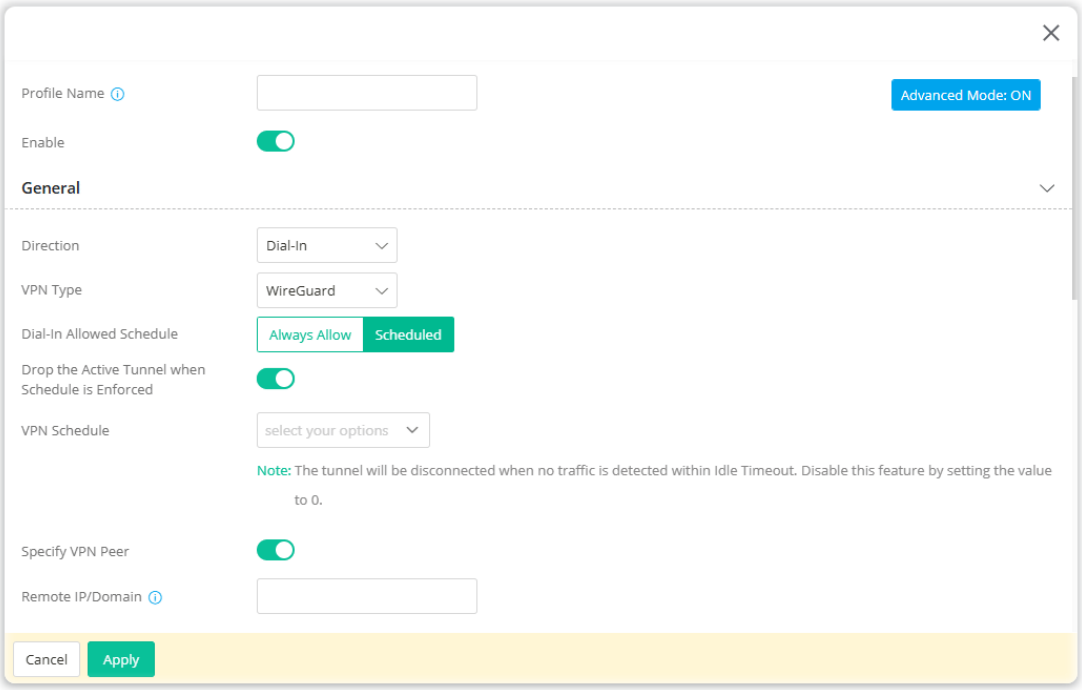
| | |
|---|---|
| | through the VPN tunnel. |
| **mDNS over VPN** | Switch the toggle to allow/ deny mDNS packets to traverse through the VPN tunnel. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings and exit the page. |

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

## II-4-2-2 VPN Type - WireGuard

WireGuard is a secure, fast, and modern open-source VPN Protocol. This VPN connection can build a VPN by exchanging private and public keys between VPN servers (e.g., Vigor router) and VPN clients (e.g., WireGuard VPN Client).

To add a new resources profile (WireGuard VPN type), open VPN>>Site-to-Site VPN and click **+Add**.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Advanced Mode:ON/OFF** | Click to show or hide the advanced settings for the site-to-site VPN. |
| **Profile Name** | Enter the name of the profile. |
| **Enable** | Switch the toggle to enable/disable the settings. |
| | **General** |
| **Direction** | Specify the allowed call direction of this WireGuard VPN profile.<br>**Dial-Out** – Profile is to be used to initiate outgoing connections.<br>**Dial-In** – Profile is to be used to accept incoming connections.<br>**VPN Matcher** - This VPN matching technology is built on the standard WireGuard VPN protocol. The VPN Matcher server can help two Draytek routers behind NAT establish a secure VPN tunnel |

| | |
|---|---|
| | for data transmission between each other. Note that only the drayos4 model, which supports WireGuard, can establish a VPN connection with Vigor device via the matcher. |
| VPN Type | Select a VPN type for building the VPN connection. Options related to WireGuard VPN type will be changed according to the Direction used.<br>**WireGuard (with the direction on Dial-In)** - Available options are:<br>• **Dial-in Allowed Schedule**<br>• **Specify VPN Peer**<br>**WireGuard (with the direction on Dial-Out)** –Available options are:<br>• **Remote IP/Domain**<br>• **Server Port**<br>• **Dial-Out Mode**<br>**WireGuard (with the direction on VPN Matcher)** – Available options are:<br>• **Device**<br>• **Remote IP/Domain**<br>• **Server Port**<br>• **Dial-Out Mode** |
| Dial-In Allowed Schedule | Connect and disconnect according to schedule profiles.<br>**Always Allow** – Select this option to maintain an always on dial-in connection.<br>**Scheduled** –Select this option to make the VPN connection based on the schedule.<br>• **Drop the Active Tunnel when Schedule is Enforced** – Switch the toggle to enable/disable the function.<br>• **VPN Schedule** – Use the drop-down menu to specify one VPN profile. Before configuring the VPN Schedule, add the required time intervals in Configuration>> Objects>> Schedule. |
| Specify VPN Peer | Switch the toggle to enable/disable the security mechanism for the remote client.<br>• **Remote IP/Domain** – Enter the IP address/domain name of the remote peer if Specify VPN Peer is enabled. |
| Server Port | Set a port number for the VPN server. |
| Dial-Out Mode | **On Demand** – The VPN connection will be triggered when detecting traffic going to the remote network.<br>**Always On** – Select this option to maintain an always on dial-out connection.<br>**Scheduled** –Select this option to make the VPN connection based on the schedule.<br>• **Drop the Active Tunnel when Schedule is Enforced** – Switch the toggle to enable/disable the function.<br>• **VPN Schedule** – Use the drop-down menu to specify one VPN profile. Before configuring the VPN Schedule, add the required time intervals in Configuration>> Objects>> Schedule. |
| Device | DrayTek VPN routers are registered with the same DrayTek VPN Matcher account, they can locate each other. Allowing them to establish a secure, end-to-end encrypted VPN tunnel between the two routers.<br>Only the device(s) registered to DrayTek VPN Matcher server will |

| | |
|---|---|
| | be displayed in this field. Select the one to make the VPN connection with this Vigor router. |
| | **WireGuard** |
| **Interface** | It is available when **Dial-Out** is selected as the Direction and **Wireguard** is selected as VPN Type.<br>**Private Key** – Displays the private key generated by clicking **Generate**.<br>**Generate Private Key** – Click the **Generate** button to generate a key pair (including private key and public key).<br>**Public Key** - Displays the public key generated by clicking **Generate**. |
| **Peer** | It is available when **Dial-Out/Dial-In** is selected as the Direction and **Wireguard** is selected as VPN Type.<br>Configure the settings for the client (peer).<br>**Public Key** - Enter the Public key of the Peer VPN server.<br>**Pre-Shared Key** - Displays the private key generated by clicking **Generate PSK**.<br>**Generate PSK** - Click Generate to generate the pre-shared key.<br>**For NAT Client Address (Optional)** – It is for Dial-In only. Enter the IP address of the remote peer.<br>**Keepalive** - Default is 60 seconds. |
| | **Network** |
| **Network** | It is crucial for defining the traffic routing. Traffic from both the local and remote subnets can pass through the **WireGuard** VPN connection.<br>**Local Network** – Defines the range of IP addresses that belong to your local network, which will be used when routing traffic through the VPN.<br>**Subnet Mask** – The subnet mask helps define the size of your local network and tells the VPN how to interpret the network portion of the IP address. A subnet mask of 255.255.255.0 (or /24 in CIDR notation) means that the first 24 bits of the IP address are for the network, and the remaining 8 bits are for hosts (devices) within the local network.<br>**Remote Network** – Defines the IP address range of the remote network that you are connecting to. For instance, if the remote network is 10.0.0.0/24, you are telling the VPN that the remote network's IP range is 10.0.0.1 through 10.0.0.254.<br>**Subnet Mask** - Similar to the local network, the subnet mask for the remote network determines how the remote network's IP range is divided. If the remote network has a subnet mask of 255.255.255.0 (or /24), it means that the remote network has 254 possible addresses for devices. |
| **Routing/NAT Mode** | When **Dial-In** is selected as the **Direction,** only **Routing** will be used. The remote network only allows one IP address for the local network.<br>When **Dial-Out/VPN Matcher** is selected as the **Direction**:<br>If the remote network only allows one IP address for the local network, select **NAT**; otherwise, select **Routing**.<br>**Routing** – It enables a standard site-to-site VPN, where the traffic is directly routed between two networks without altering the |

| | |
|---|---|
| | source IP address.<br>• **Translate Local Network** –To establish a bilateral VPN connection, the Local and Remote subnet cannot be the same. If they are accidentally the same, IP address translation is required (e.g., if both sides use 192.168.1.10, one of them needs to be translated to 192.168.2.10 to enable a bilateral VPN connection).<br>• **Translated Network** - Specify an IPv4 address.<br>**NAT** – It modifies VPN traffic to the remote site by translating the source IP into a virtual IP address before sending it to the destination. |
| **More Subnets** | It is used to add more static routes for subnets destined for the remote network.<br>**Disabled** – Disable this function.<br>• **+Add** – Click to add new static route. Enter required information for the remote network and subnet mask. |
| **Options under the Advanced Mode** | |
| **Dial-Out Interface Mode** | Select the WAN connection for connections made using this profile. This setting is useful for dial-out only.<br>**Selected Interface First** – While connecting, the router will use the selected WAN interface first for VPN connection. If selected WAN fails, the router will try to use other WAN(s).<br>**Selected Interface Only** – While connecting, the router will use selected WAN as the only interface for VPN connection.<br>**Manual** – Customize VPN settings. Specify which WANs can be used as outgoing interfaces. |
| **Dial-Out Interface** | It is available when the call direction of this VPN profile is set to Dial-Out.<br>**Auto Select** – Decide which interface to dial out based on the default route.<br>**Default WAN IP / IP Address** – Use the drop-down list to specify one WAN IP address for this VPN profile. |
| **Idle Timeout** | The tunnel will be disconnected when no traffic is detected within Idle Timeout. Disable this feature by setting the value to 0. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings and exit the page. |

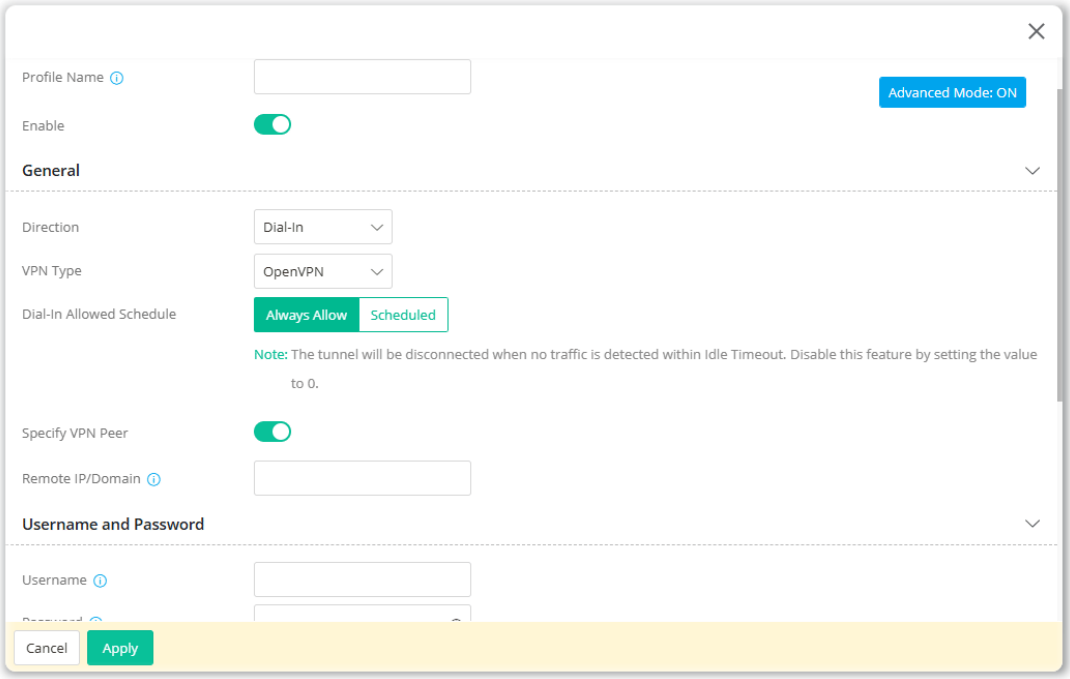
After finishing this web page configuration, please click **Apply** to save the settings.

## II-4-2-3 VPN Type - OpenVPN

The OpenVPN protocol utilizes public keys, certificates, and usernames and passwords to authenticate the client. Traffic is carried over secure channels built upon industry-standard SSL/TLS encryption protocols.

OpenVPN requires the use of certificates. Before establishing OpenVPN connection, general settings for OpenVPN service shall be configured first.

To add a new resources profile (OpenVPN VPN type), open VPN>>Site-to-Site VPN and click **+Add**.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Advanced Mode:ON/OFF** | Click to show or hide the advanced settings for the site-to-site VPN. |
| **Profile Name** | Enter the name of the profile. |
| **Enable** | Switch the toggle to enable/disable the settings. |
| | **General** |
| **Direction** | Specify the allowed call direction of this VPN profile.<br>**Dial-Out** – Profile is to be used to initiate outgoing connections.<br>**Dial-In** – Profile is to be used to accept incoming connections.<br>**Both** - Profile is to be used to initiate (dial out) or accept (dial in) connections. |
| **VPN Type** | Select a VPN type for building the VPN connection. Options related to OpenVPN type will be changed according to the Direction used.<br>**OpenVPN (with the direction on Both, Dial-In)** – Available options are:<br>• **Dial-in Allowed Schedule**<br>• **Specify VPN Peer**<br>**OpenVPN (with the direction on Both, Dial-Out)** – Available options are:<br>• **Remote IP/Domain**<br>• **Server Port**<br>• **Dial-Out Mode** |
| **Dial-In Allowed Schedule** | Connect and disconnect according to schedule profiles.<br>**Always Allow** – Select this option to maintain an always on dial-in connection.<br>**Scheduled** –Select this option to make the VPN connection based on the schedule.<br>• **Drop the Active Tunnel when Schedule is Enforced** – Switch |

| | |
|---|---|
| | the toggle to enable/disable the function.<br>• **VPN Schedule** – Use the drop-down menu to specify one VPN profile. Before configuring the VPN Schedule, add the required time intervals in Configuration>> Objects>> Schedule. |
| **Remote IP/Domain** | Enter IPv4 or hostname for the remote VPN server. |
| **Server Port** | Set a port number for the VPN server. |
| **Dial-Out Mode** | **On Demand** – The VPN connection will be triggered when detecting traffic going to the remote network.<br>**Always On** – Select this option to maintain an always on dial-out connection.<br>**Scheduled** – Connect and disconnect according to schedule profiles. The default setting of this field is blank and the function will always work.<br>• **Drop the Active Tunnel when Schedule is Enforced** – Switch the toggle to enable/disable the function.<br>• **VPN Schedule** – Use the drop-down menu to specify one VPN profile. Before configuring the VPN Schedule, add the required time intervals in Configuration>> Objects>> Schedule. |
| **Specify VPN Peer** | It is available if **Both/Dial-In** is selected as the **Direction**.<br>Switch the toggle to enable/disable the security mechanism for the remote client.<br>• **Remote IP/Domain** – Enter the IP address/domain name of the remote peer if Specify VPN Peer is enabled. |
| **Username and Password** | |
| **Username and Password** | It is available when **Dial-Out/Dial-In** is selected as the Direction and **OpenVPN** is selected as VPN Type.<br>**Username -**Used by the remote LAN to establish a VPN connection.<br>**Password -** Used by the remote LAN to establish a VPN connection. |
| **OpenVPN Settings** | |
| **OpenVPN Settings** | It is available when **Dial-Out** is selected as the Direction and **OpenVPN** is selected as VPN Type.<br>**Dial-Out Protocol** – Select TCP or UDP as VPN server protocol.<br>**Import OpenVPN Config** - An OpenVPN config file from other Vigor router can be imported and apply to this router.<br>Select to import an OpenVPN configuration file from a specified OpenVPN server (e.g., Vigor router, PC, other VPN provider, etc.) onto to Vigor router. Later, as a VPN client, this router can access into VPN server via the username and password. If the configuration file contains certificates, they will be automatically imported. |
| **Network** | |
| **Network** | It is crucial for defining the traffic routing. Traffic from both the local and remote subnets can pass through the VPN connection.<br>**Local Network** – Defines the range of IP addresses that belong to your local network, which can be accessed through the VPN tunnel.<br>**Subnet Mask** – The subnet mask helps define the size of your local network and tells the VPN how to interpret the network portion of the IP address. A subnet mask of 255.255.255.0 (or /24 in CIDR notation) means that the first 24 bits of the IP address are for the |

| | |
|---|---|
| | network, and the remaining 8 bits are for hosts (devices) within the local network.<br>**Remote Network** –Defines the IP address range of the remote network that you are connecting to. For instance, if the remote network is 10.0.0.0/24, you are telling the VPN that the remote network's IP range is 10.0.0.1 through 10.0.0.254.<br>**Subnet Mask** - Similar to the local network, the subnet mask for the remote network determines how the remote network's IP range is divided. If the remote network has a subnet mask of 255.255.255.0 (or /24), it means that the remote network has 254 possible addresses for devices. |
| **Routing/NAT Mode** | When **Dial-In** is selected as the **Direction,** only **Routing** will be used. The remote network only allows one IP address for the local network.<br>When **Dial-Out/Both** is selected as the **Direction**:<br>If the remote network only allows one IP address for the local network, select **NAT**; otherwise, select **Routing**.<br>**Routing** – It enables a standard site-to-site VPN, where the traffic is directly routed between two networks without altering the source IP address.<br>• **Translate Local Network** –To establish a bilateral VPN connection, the Local and Remote subnet cannot be the same. If they are accidentally the same, IP address translation is required (e.g., if both sides use 192.168.1.10, one of them needs to be translated to 192.168.2.10 to enable a bilateral VPN connection).<br>• **Translated Network** - Specify an IPv4 address.<br>**NAT** – It modifies VPN traffic to the remote site by translating the source IP into a virtual IP address before sending it to the destination. |
| **More Subnets** | It is used to add more static routes for subnets destined for the remote network.<br>Switch the toggle to enable/disable this function.<br>• **+Add** – If the function is enabled, click **Add** to add new static route. Enter required information for remote network and subnet mask. |
| **Options under the Advanced Mode** | |
| **Dial-Out Interface Mode** | Select the WAN connection for connections made using this profile. This setting is useful for dial-out only.<br>**Selected Interface First** – While connecting, the router will use the selected WAN interface first for VPN connection. If selected WAN fails, the router will try to use other WAN(s).<br>**Selected Interface Only** – While connecting, the router will use selected WAN as the only interface for VPN connection.<br>**Manual** – Customize VPN settings. Specify which WANs can be used as outgoing interfaces. |
| **Dial-Out Interface** | **Auto Select** – Decide which interface to dial out based on the default route.<br>**Default WAN IP / IP Address** – Use the drop-down list to specify one WAN IP address for this VPN profile. |
| **Dial Out Advanced** | **Cipher Algorithm** – Select the desired cipher algorithm. Two encryption algorithms are supported: AES128, AES192 and AES256. |

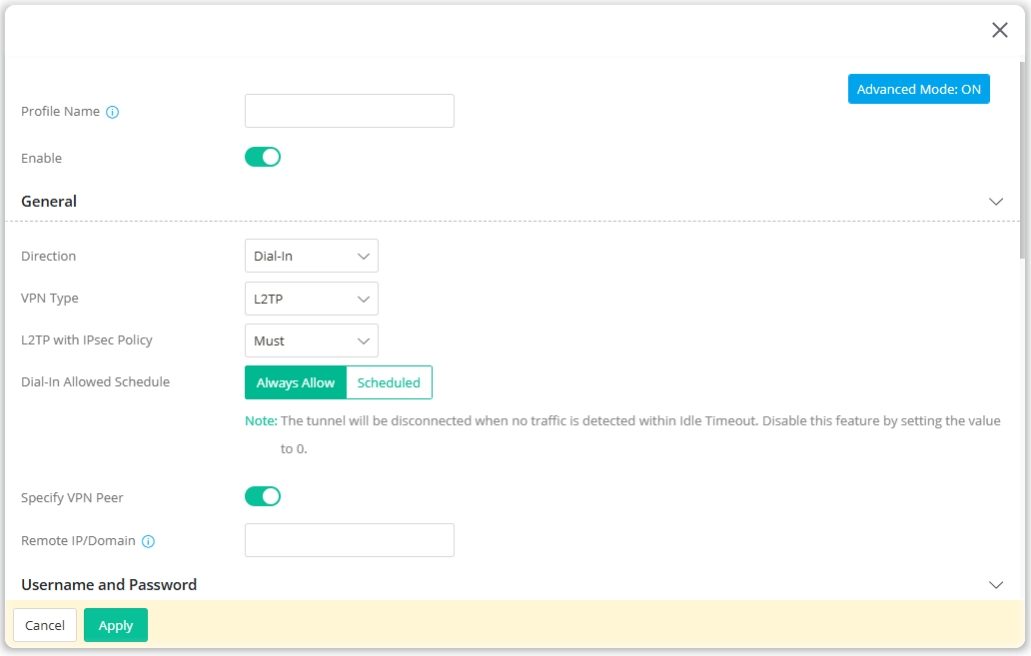
| | |
|---|---|
| **Settings** | AES256 is more secure than AES128 but may result in lower performance because it incurs higher computational overhead.<br>**HMAC Algorithm** – HMAC stands for Hash-based Message Authentication Code. It is used to validate the data integrity and authenticity of the VPN data.<br>Select the desired HMAC hash algorithm. Two hash algorithms, SHA1 and SHA256, are supported. SHA256 is preferred as it is more robust and reliable than SHA1.<br>**Client Certificate** – Use the dropdown list to select a client certificate that has already been uploaded to the router. Default (Use CERT from OpenVPN Config) will be selected automatically after import OpenVPN Config file.<br>**Trusted CA** – Use the dropdown list to select a trust CA certificate that has already been uploaded to the router. Default (Use CA from OpenVPN Config) will be selected automatically after import OpenVPN Config file.<br>**Compress** – Select a method to compress the packets to reduce the bandwidth usage while transferring the compressed packets.<br>**TLS Auth** – Switch the toggle to use/close the TLS authentication method. If the OpenVPN configuration file contains TLS Key, they will be automatically imported. |
| **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-4-2-4 VPN Type – L2TP

L2TP utilizes mandatory IPsec encryption to establish a secure VPN tunnel. To ensure data integrity and confidentiality, this connection type does not support L2TP without IPsec encryption.

To add a new resources profile (L2TP VPN type), open VPN>>Site-to-Site VPN and click **+Add**.



Available settings are explained as follows:

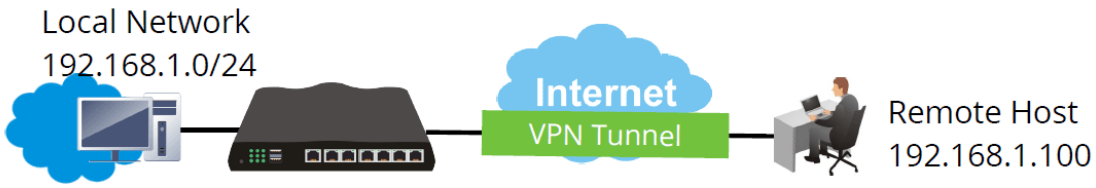
| Item | Description |
|---|---|
| **Advanced Mode:ON/OFF** | Click to show or hide the advanced settings for the site-to-site VPN. |
| **Profile Name** | Enter the name of the profile. |
| **Enable** | Switch the toggle to enable/disable the settings. |
| | **General** |
| **Direction** | Specify the allowed call direction of this VPN profile.<br>**Dial-In** – Profile is to be used to accept incoming connections. |
| **VPN Type** | Select a VPN type (L2TP) for building the VPN connection. |
| **L2TP with IPsec Policy** | L2TP with IPsec encryption is mandatory for this connection type to ensure data integrity and confidentiality.<br>**Must** - Specify the IPsec policy to be definitely applied on the L2TP connection. |
| **Dial-In Allowed Schedule** | Connect and disconnect according to schedule profiles.<br>**Always Allow** – Select this option to maintain an always on dial-in connection.<br>**Scheduled** –Select this option to make the VPN connection based on the schedule.<br>• **Drop the Active Tunnel when Schedule is Enforced** – Switch the toggle to enable/disable the function.<br>• **VPN Schedule** – Use the drop-down menu to specify one VPN profile. Before configuring the VPN Schedule, add the required time intervals in Configuration>> Objects>> Schedule. |
| **Specify VPN Peer** | Switch the toggle to enable/disable the security mechanism for the remote client.<br>• **Remote IP/Domain** – Enter the IP address/domain name of the remote peer if Specify VPN Peer is enabled. |
| | **Username and Password** |
| **Username and Password** | **Username -**Used by the remote LAN to establish a VPN connection.<br>**Password -** Used by the remote LAN to establish a VPN connection. |
| | **IKE Authentication** |
| **Dial-In Settings** | It is available when **Dial-In** is selected as the Direction and **IPsec** is selected as VPN Type. |
| **Negotiation** | Select **Main Mode** or **Aggressive Mode**. The ultimate outcome is to exchange security proposals to create a protected secure channel. The default value in Vigor router is Main mode.<br>**Main Mode** – **Main** mode is more secure than **Aggressive** mode since more exchanges are done in a secure channel to set up the IPsec session. However, the **Aggressive** mode is faster.<br>**Aggressive Mode** – **Main** mode is more secure than **Aggressive** mode since more exchanges are done in a secure channel to set up the IPsec session. However, the **Aggressive** mode is faster. |
| **Pre-Shared Key** | Input characters as pre-shared key for authentication. |
| **X.509 Digital Signature** | It is available when IKEv1/v2 is selected as IPsec Dial-In Protocol.<br>To use an X.509 digital signature, select one of the authentication |

| | |
|---|---|
| | methods and enter the required information for each method.<br>**Select Accept Subject Alternative Name** - The following three formats of Peer ID are acceptable, including IP Address, Domain Name, and Email.<br>**Peer Certificate** - Select a peer certificate that has been pre-obtained and stored in Configuration>>Certificates Local Certificates.<br>**Accept Subject Name** – Enter the complete certificate subject name.<br>**Accept Any** - Any certificate signed by a trusted CA in Configuration>>Certificates Trusted CA will be considered valid. |
| **IKE Identifier** | Set the local ID and Peer ID for identification.<br>Local ID and Peer ID are provided for certain connections that require specifying an ID, such as IKEv1 using Aggressive mode and IKEv2 (optional). |
| **Local ID** | Specify a local ID to be used when establishing a VPN connection using IPsec VPN type. |
| **Peer ID** | Enter the ID name for the remote client.<br>If the values are specified, only connections coming from the specified IP address and/or having the specified Peer ID will be accepted. |
| **More settings for IKE Authentication** | |
| **IKE Phase 1** | **Encryption** – Use Auto/AES/3DES/DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.<br>**Group** – Specify a key exchange proposal.<br>**Authentication** – Select SHA256 or SHA1 for packet authentication.<br>**Lifetime** - For security reason, the lifetime of key should be defined. The default value is 28800 seconds. You may specify a value in between 900 and 86400 seconds. |
| **IKE Phase 2** | Specify the security protocol, proposal encryption and proposal authentication.<br>**Security Protocol** – AH (Medium) means data will be authenticated, but not be encrypted. By default, this option is active. ESP (High) means payload (data) will be encrypted and authenticated.<br>**Encryption** – Use AES/3DES/DES encryption algorithm.<br>**Authentication** – Select All, SHA256 or SHA1 for packet authentication.<br>**Lifetime** – For security reason, the lifetime of key should be defined. The default value is 3600 seconds. You may specify a value in between 600 and 28800 seconds.<br>**Perfect Forward Secret** – Switch the toggle to enable/disable this function. PFS forces key exchange during Phase-2 periodic Rekey. |
| **Dead Peer Detection** | Dead Peer Detection (DPD) is the method to detect an IPsec connection.<br>**DPD Delay** – It is a keep-alive timer. A Hello message will be emitted periodically when a tunnel is idle. Use the value 0 to disable this function. The recommended value is 30 seconds if enabled.<br>**DPD Timeout** - It is the timeout timer. The peer will be declared dead once no acknowledge message is received after timeout |

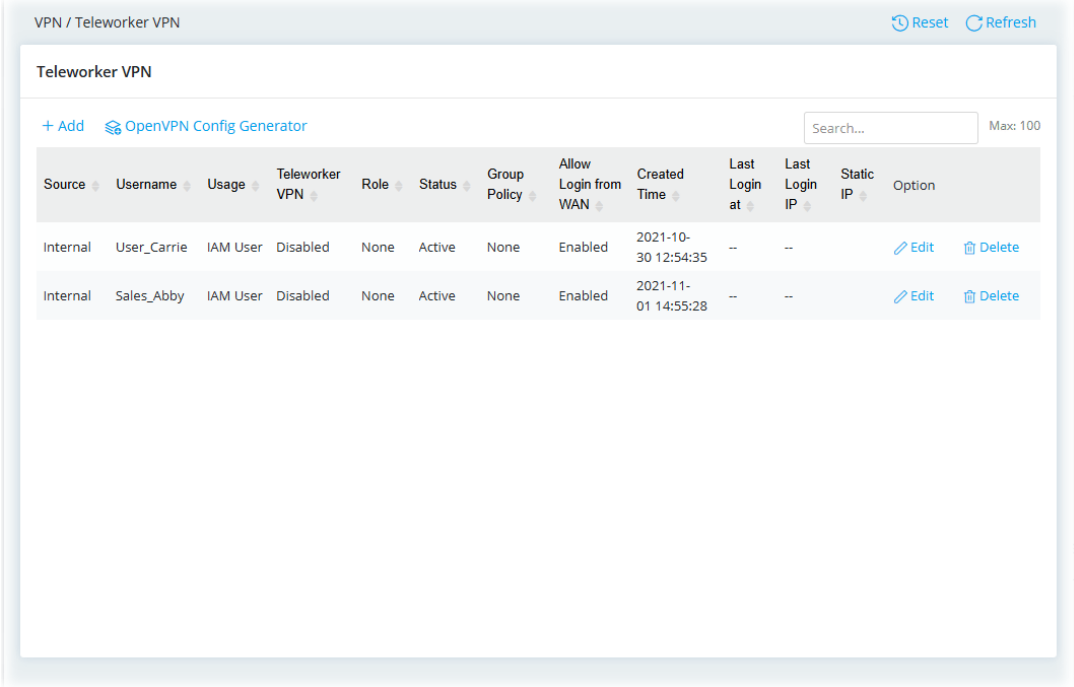
| | |
|---|---|
| | value. Use the value 0 to disable this function. The recommended value is 120 seconds if enabled. |
| Network | |
| Network | It is crucial for defining the traffic routing. Traffic from both the local and remote subnets can pass through the VPN connection.<br>**Local Network** – Defines the range of IP addresses that belong to your local network, which can be accessed through the VPN tunnel.<br>**Subnet Mask** – The subnet mask helps define the size of your local network and tells the VPN how to interpret the network portion of the IP address. A subnet mask of 255.255.255.0 (or /24 in CIDR notation) means that the first 24 bits of the IP address are for the network, and the remaining 8 bits are for hosts (devices) within the local network.<br>**Remote Network** –Defines the IP address range of the remote network that you are connecting to. For instance, if the remote network is 10.0.0.0/24, you are telling the VPN that the remote network's IP range is 10.0.0.1 through 10.0.0.254.<br>**Subnet Mask** - Similar to the local network, the subnet mask for the remote network determines how the remote network's IP range is divided. If the remote network has a subnet mask of 255.255.255.0 (or /24), it means that the remote network has 254 possible addresses for devices. |
| Routing/NAT Mode | If the remote network only allows one IP address for the local network, **NAT** will be shown in this field. Otherwise, **Routing** will be shown in this field. |
| More Subnets | It is used to add more static routes for subnets destined for the remote network.<br>Switch the toggle to enable/disable this function.<br>• **+Add** – If the function is enabled, click **Add** to add new static route. Enter required information for remote network and subnet mask. |
| Cancel | Discard current settings and return to the previous page. |
| Apply | Save the current settings and exit the page. |

## II-4-3 Teleworker VPN

The VPN means a connection between the remote host and router's LAN network. The host will use an IP address in the local subnet. It allows employees to access the company's internal resources when they are traveling.

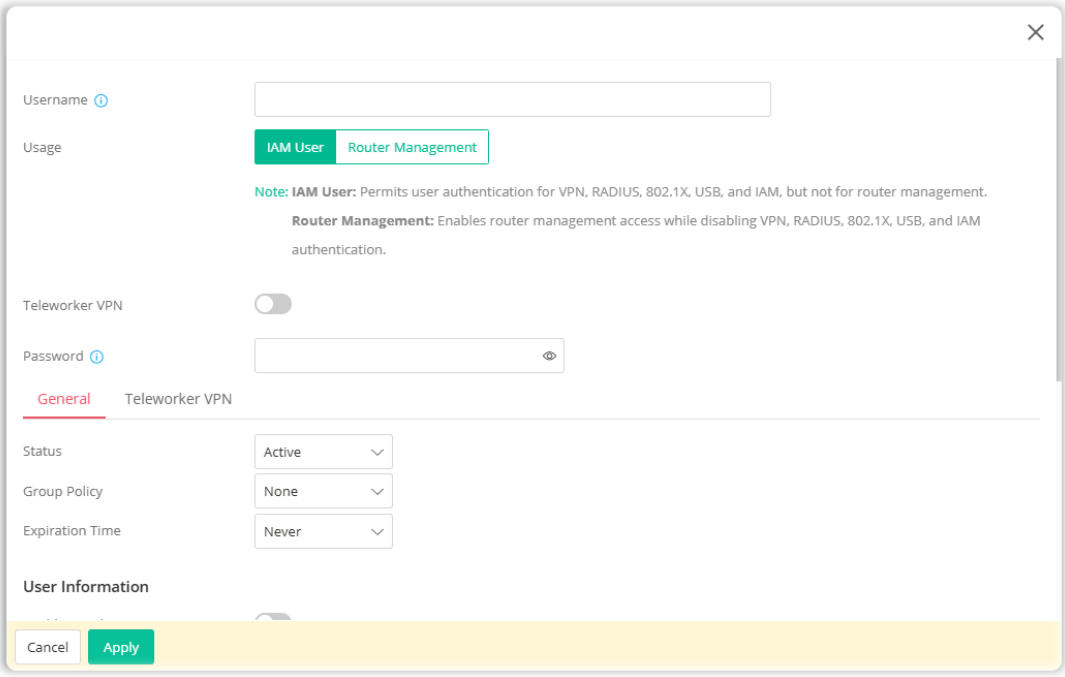



Open VPN>>Teleworker VPN to get the following page.




To add a new VPN profile, click **+Add**.

Note that the settings modification related to the user profile (no matter add or edit) here will rewrite the settings on IAM>>Users & Groups>>Users synchronically, and vice versa.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Username** | Enter the Login name (e.g., *LAN_User_Group_1, WLAN_User_Group_A, WLAN_User_Group_B,* etc.) for this user profile. |
| **Usage** | Define the type of this user profile.<br>**IAM User** – This profile can be used for VPN, RADIUS, 802.1X, USB and IAM (AWS Identity and Access Management) authentication.<br>**Router Management** – This profile is only for router management access and cannot be used for VPN, RADIUS, 802.1X, USB, and IAM authentication. |
| **Teleworker VPN** | It is available if IAM User is selected as the Usage.<br>Switch the toggle to enable or disable the Teleworker VPN function. |
| **Password** | It is available if IAM User is selected as the Usage.<br>Password (e.g., *lug123, wug123,wug456,* etc.) for this user profile.<br>When a user tries to access the Internet, he or she must supply a valid user name and password combination for authentication. The profile with matching user name and password will be applied to the session. |
| **New Password/**<br>**Confirm New Password** | It is available if Router Management is selected as the Usage.<br>Password (e.g., *lug123, wug123,wug456,* etc.) for this user profile.<br>When a user tries to access the Internet, he or she must supply a valid user name and password combination for authentication. The profile with matching user name and password will be applied to the session. |
| **General**<br>**(if IAM User is selected as the Usage)** | |
| **Status** | **Active** – Enable the general settings in this page.<br>**Inactive** – Disable the general settings in this page. |

| | |
|---|---|
| **Group Policy** | It is available if "IAM User" is selected as the usage.<br>Select a group policy profile to be applied by this user profile. |
| **Expiration Time** | It is available if "IAM User" is selected as the usage.<br>It means that the user account will be automatically disconnected after the time is up.<br>Set the network connection to work at certain time interval only. All user accounts will apply the time configuration automatically by default.<br>**Never** – The network connection is always on.<br>**Expire in** – The network connection will expire and terminate the connection after specified minutes, hours, days, or weeks once built.<br>**Expire at** – The network connection will expire and terminate the connection on the date and time specified below once built.<br>• **Date**<br>• **Time**<br>• **Expiration Time** |
| **User Information** | **Enable Email** – Switch the toggle to enable or disable the email setting.<br>• **Email** – Enter the email address for receiving the MFA PIN code.<br>• **Send Email Notification to the newly created User** – Send a notification email to this user account.<br>**Enable SMS** – Switch the toggle to enable or disable the SMS setting.<br>• **SMS** - Enter the destination SMS number for receiving the MFA PIN code. |
| **MFA & Port Knocking** | Multi-factor authentication (MFA) can offer a more secure network connection.<br>**Enable MFA** – Switch the toggle to enable/disable the MFA function.<br>• **Allowed MFA Method** - Select to require TOTP, SMS or email authentication when logging in from the WAN.<br>**TOTP** –For the Time-based One-time Password (TOTP) mechanism, please make sure the time zone of your router is correct. Then, install Google Authenticator APP on your cell phone. Open the APP to scan the QR code on this page. A one-time password will be shown on your phone. Select TOTP and click **Apply.** A pop-up dialog will appear as follows:<br> |

| | |
|---|---|
| | In the filed of Validation Code, enter the one-time password and click Verify.<br>Now, the configuration is finished. You will be asked to enter the 2FA code on the after passing the username and password authentication.<br>**SMS/Email** –The password will be sent via SMS or email as selected in the User Information above.<br>• **Enforce Port Knocking** – Switch the toggle to enable/disable the Port Knocking function.<br>**1st Knock Port –** Enter a value (3001~59999). Click the (!) mark to have more information.<br>**TOTP Secret –** Display the secret used for TOTP. |
| **Account Info** | Displays general information (created time, last login at and last login IP) for the VPN user account. |
| **Teleworker VPN**<br>**(available if IAM User is selected as the Usage)** | |
| **General** | **Idle Timeout** – If the user is idle over the limitation of the timer, the **network connection will be stopped for such user.** By default, the Idle Timeout is set to 300 seconds.<br>**VPN Schedule** – Select **Always On**. Or choose **Scheduled On** to make the VPN connection based on the schedule.<br>Before configuring VPN Schedule, add the required time intervals in Configuration>>Objects >>Schedule.<br>**Netbios Naming over VPN** – Switch the toggle to allow/ deny NetBIOS naming packets to traverse through the VPN tunnel.<br>**Multicast over VPN** - Switch the toggle to allow/ deny multicast packets to traverse through the VPN tunnel.<br>**mDNS over VPN** - Switch the toggle to allow/ deny mDNS packets to traverse through the VPN tunnel.<br>**Download SmartVPN Client** – Click to download the utility of DrayTeck SmartVPN client for building VPN connection. |
| **Allowed VPN Protocols** | Select IPsec, WireGuard or OpenVPN as the protocol for the teleworker VPN connection.<br>**IPsec** – Switch the toggle to enable the IPsec protocol. If enabled, select IKEv1/v2, EAP and/or XAuth as the IPsec authentication.<br>**OpenVPN** - Switch the toggle to enable OpenVPN protocol.<br>**WireGuard** –Switch the toggle to enable WireGuard protocol.<br>• **General Key Mode** – Select Auto or Customized.<br>Select **Auto** and click **Generate Key Pair** to generate the key pair of the private key and the public key of the peer.<br>Select **Customized** to enter the public key of the peer side.<br>• **Client Public Key** – Enter the string offered by the remote WireGuard VPN client.<br>• **Pre-Shared Key** – Displays the private key generated by clicking Generate PSK.<br>• **Generate PSK** – Click the Generate PSK button to generate a pre-shared key.<br>• **Persistent Keepalive** – Default is 60 seconds. If the peer is behind a NAT or a firewall, use the default setting.<br>**L2TP** – Switch the toggle to enable L2TP protocol. If enabled, configure the following settings: |

| | |
|---|---|
| | • **L2TP with IPsec Policy -** L2TP with IPsec encryption is mandatory for this connection type to ensure data integrity and confidentiality.<br>**Must** - Specify the IPsec policy to be definitely applied on the L2TP connection. |
| Security | **Specify VPN Peer** – Switch the toggle to enable/disable the security mechanism for the remote client.<br>• **Remote Client IP** – Enter the IP address of the remote peer if Specify VPN Peer is enabled.<br>• **Pre-Shared Key** – It is available when the IPsec is selected as the Allowed VPN Protocols. "Specify VPN Peer" can restrict the IPsec to be initiated only by the specified peer IP address or domain name, and specify the private key to be used.<br>**X.509 Digital Signature** - It is available when the IPsec/L2TP is selected as the Allowed VPN Protocols. Accept the certificates authentication. To use an X.509 digital signature, select one of the authentication methods and enter the required information for each method.<br>• **Disabled** – Select to disable the certificate application for VPN connection.<br>• **Accept Subject Alternative Name** –The following three formats of Peer ID are acceptable, including IP Address, Domain Name, and Email.<br>• **Select from Existing Certificates** –Select a peer certificate that has been pre-obtained and stored in Configuration>>Certificates Local Certificates.<br>• **Accept Subject Name** – Enter the complete certificate subject name.<br>• **Accept Any** – Any certificate signed by a trusted CA in Configuration>>Certificates Trusted CA will be considered valid. |
| Local IP Assignment | **Assign IP by** – It is available if WireGuard protocol is disabled.<br>Select **LAN DHCP** for getting an IP from the router automatically. Or, select **Static IP** to specify an IPv4 address.<br>**Assign IP from** - Select a LAN interface for IP assignment. And specify an IPv4 address as the static IP.<br>**Assign DNS By** – Select **LAN DHCP** or **Static DNS**.<br>If LAN DHCP is selected, the DNS IP will be assigned by Vigor router automatically.<br>If Static DNS is selected,<br>• **Primary DNS** – Enter the IPv4 address for Primary DNS server.<br>• **Secondary DNS** – Enter another IPv4 address for DNS server if required. |
| WireGuard Client Config Generator | Configure the settings for VPN client (peer) if WireGuard is enabled as the **Allowed VPN Protocols**.<br>**VPN Server –** Enter the public IP address or domain name of Vigor router.<br>**Set VPN as Default Gateway –** Switch the toggle to enable/disable the function.<br>• **Enable** - The Vigor router will be treated as a "default" gateway for WireGuard VPN clients. The WireGuard VPN client will redirect all the traffic to the Vigor router via the WireGuard |

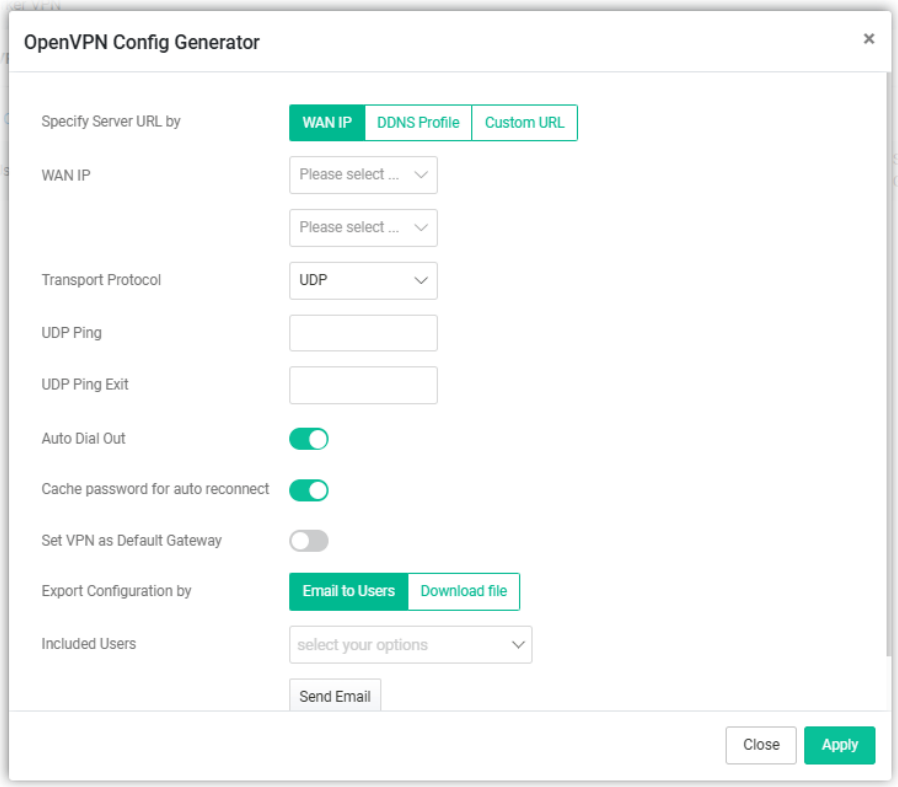
| | |
|---|---|
| | VPN tunnel.<br>• **Disable** - Disable the function.<br>• **Replace the Default Route –** Switch the toggle to enable/disable the feature. After clicking **Apply**, the client's default route will be replaced by the VPN route.<br>**config –** The default text in this field is displayed automatically. It will be changed according to the QR-Code variation. Modify the text if required.<br>**Download Configuration -** Click this button to download the config on this page as a file, which can be imported into a VPN client to establish WireGuard VPN connections. |
| General<br>(if Router Management is selected as the Usage) | |
| **Role** | It is available if "Router Management" is selected as the usage.<br>• **Administrator**<br>• **Guest**<br>• **Users** |
| **Status** | **Active** – Enable the general settings in this page.<br>**Inactive** – Disable the general settings in this page. |
| **Allow Login from WAN** | It is available if "Router Management" is selected as the usage.<br>If enabled, the user can login from WAN by using this user account. |
| **User Information** | **Enable Email** – Switch the toggle to enable or disable the email setting.<br>• **Email** – Enter the email address for receiving the MFA PIN code.<br>• **Send Email Notification to the newly created User** – Send a notification email to this user account.<br>**Enable SMS** – Switch the toggle to enable or disable the SMS setting.<br>• **SMS** - Enter the destination SMS number for receiving the MFA PIN code. |
| **MFA & Port Knocking** | Multi-factor authentication (MFA) can offer a more secure network connection.<br>**Enable MFA** – Switch the toggle to enable/disable the MFA function.<br>• **Allowed MFA Method** - Select to require TOTP, SMS or email authentication when logging in from the WAN.<br>**TOTP** –For the Time-based One-time Password (TOTP) mechanism, please make sure the time zone of your router is correct. Then, install Google Authenticator APP on your cell phone. Open the APP to scan the QR code on this page. A one-time password will be shown on your phone. Select TOTP and click **Apply.** A pop-up dialog will appear as follows: |

| | |
|---|---|
| | <br>In the filed of Validation Code, enter the one-time password and click Verify.<br>Now, the configuration is finished. You will be asked to enter the 2FA code on the after passing the username and password authentication.<br>**SMS/Email** –The password will be sent via SMS or email as selected in the User Information above.<br>• **Enforce Port Knocking** – Switch the toggle to enable/disable the Port Knocking function.<br>**1st Knock Port -** Enter a value (3001~59999). Click the (!) mark to have more information.<br>**TOTP Secret –** Display the secret used for TOTP. |
| **Account Info** | Displays general information (created time, last login at and last login IP) for the user account. |
| **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.

### OpenVPN Config Generator

On this page, you can create configuration required for a remote OpenVPN client to connect to the router and then download it directly or send it to the user via email.




Available settings are explained as follows:

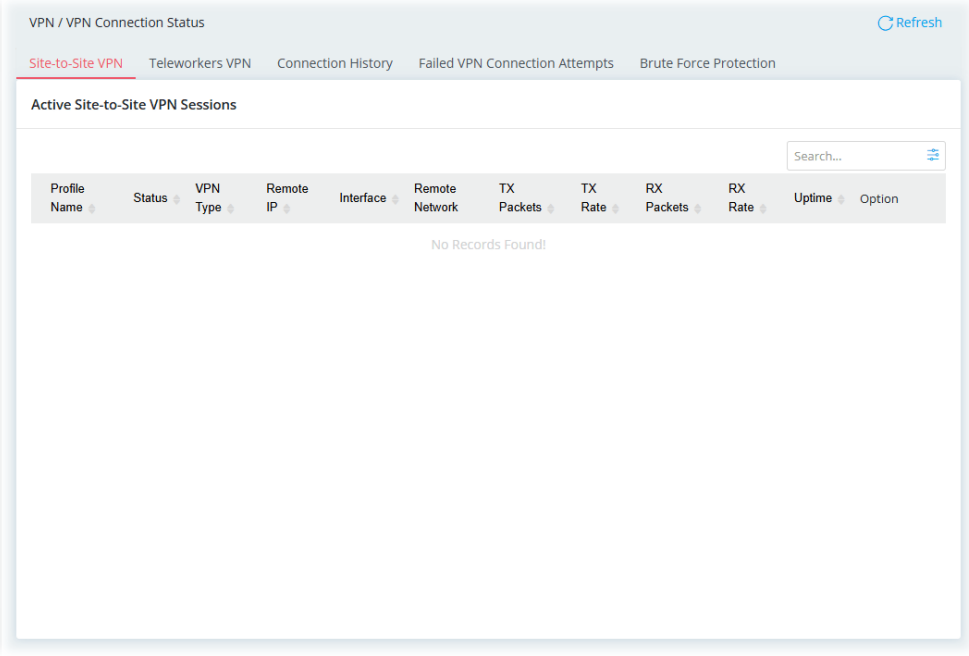
| Item | Description |
|---|---|
| **Specify Server URL by** | The OpenVPN client will use the IP address or domain name to connect to the router.<br>**WAN IP** – The OpenVPN configuration file will use the numeric IP address as the server address.<br>• **WAN IP** – Select the WAN interface.<br>**DDNS Profile** – The OpenVPN configuration file will use the domain name from the DDNS Profile.<br>• **DDNS Profile** – Select a DDNS profile.<br>**Custom URL** – The OpenVPN configuration file will use the user-defined server IP or domain name.<br>• **Custom URL** – Specify a user-defined URL. |
| **Transport Protocol** | **TCP/UDP** - Select UDP or TCP for the protocol to be used by the OpenVPN client to connect to the router. |
| **UDP Ping** | Ping remote device over the UDP control channel, if no packets have been sent for the number of seconds configured here. |
| **UDP Ping Exit** | Let OpenVPN exit after the seconds set here if no reception of a ping or other packet from the remote device. |
| **Auto Dial Out** | Switch the toggle to enable/disable the function.<br>**Enable** - The remote client can auto-dial to this Vigor router to build an OpenVPN tunnel.<br>**Disable** - Disable the function. |
| **Cache password for auto reconnect** | Switch the toggle to enable/disable the function.<br>**Enable** - OpenVPN will reconnect per hour. While reconnecting, the password is required. If the function is enabled, the password for OpenVPN connection will be kept and used by the Vigor system for |

| | |
|---|---|
| | reconnection every time.<br>**Disable** - Disable the function. |
| **Set VPN as Default Gateway** | Switch the toggle to enable/disable the function.<br>**Enable** - The Vigor router will be treated as a "default" gateway for OpenVPN clients. The OpenVPN client will redirect all the traffic to the Vigor router via the OpenVPN tunnel.<br>**Disable** -Disable the function. |
| **Export Configuration by** | **Email to Users** – If selected, the Included Users field below will be displayed. The OpenVPN configuration file will be sent to users listed on Included Users.<br>• **Included Users** – Select teleworker users that will receive the configuration from Vigor router.<br>• **Send Email** – Click to email the settings on this page as a file, which can be imported into a VPN client to establish OpenVPN connections to teleworker users.<br>**Download file** – The configuration file for OpenVPN will be stored on the database. If selected, the Download Configuration button below will be displayed.<br>• **Download Configuration** - Click this button to download the settings on this page as a file, which can be imported into a VPN client to establish OpenVPN connections. |
| **Close** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings and exit the page. |

# II-4-4 VPN Connection Status

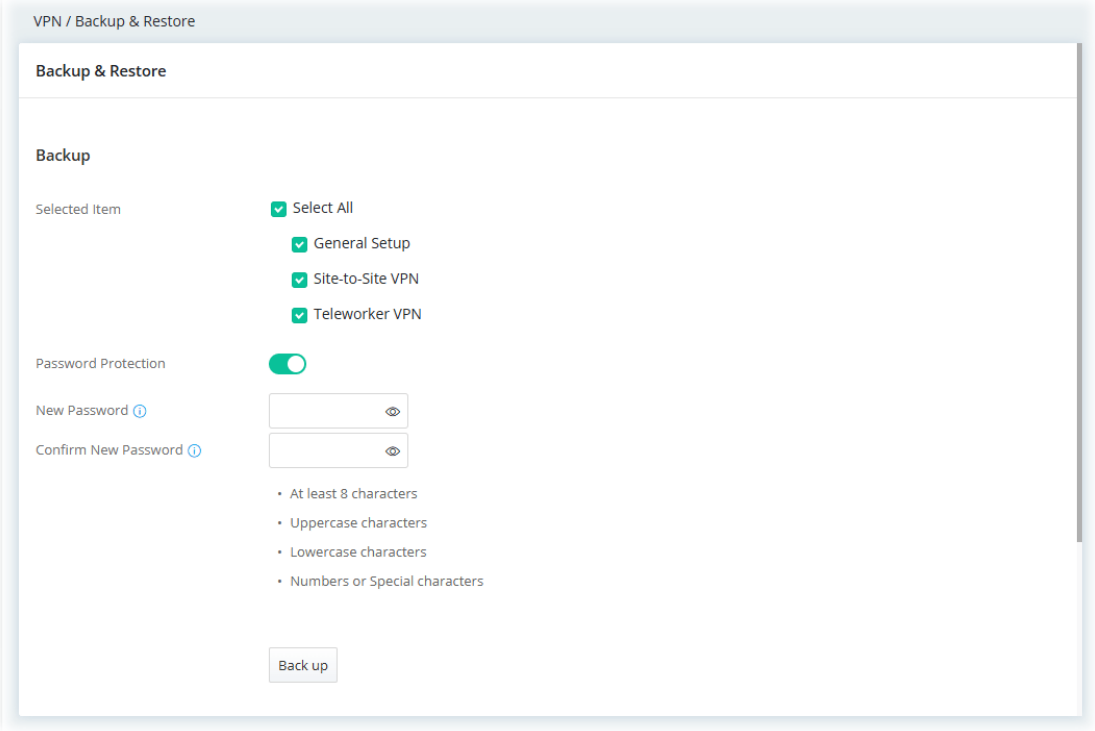
This section displays various VPN connection status, including

- Site-to-Site VPN
- Teleworker VPN
- Connection History
- Failed VPN Connection Attempts
- Brute Force Protection



# II-4-5 Backup & Restore

This page can be used to backup/restore the VPN configuration.




Available settings are explained as follows:

| Item | Description |
|---|---|
| | **Backup** |
| **Selected Item** | Select the VPN type for the configuration backup. |
| **Password Protection** | For the sake of security, the configuration file for the access point can be encrypted.<br>Switch the toggle to enable or disable the function. |
| **New Password/ Confirm New Password** | Enter several characters as the password for encrypting the configuration file. |
| **Back up** | Click it to backup the configuration file. |
| | **Restore** |
| **Restore from Backup File** | - Click to locate the file for restoring.<br>**Restore** - Click to execute the restoration. |
| **File has Password Protection** | Switch the toggle to enable or disable the function. If enabled, a password will be required for restoring the configuration.<br>**Password -** Enter a password for configuration restoration. |

# II-5 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.

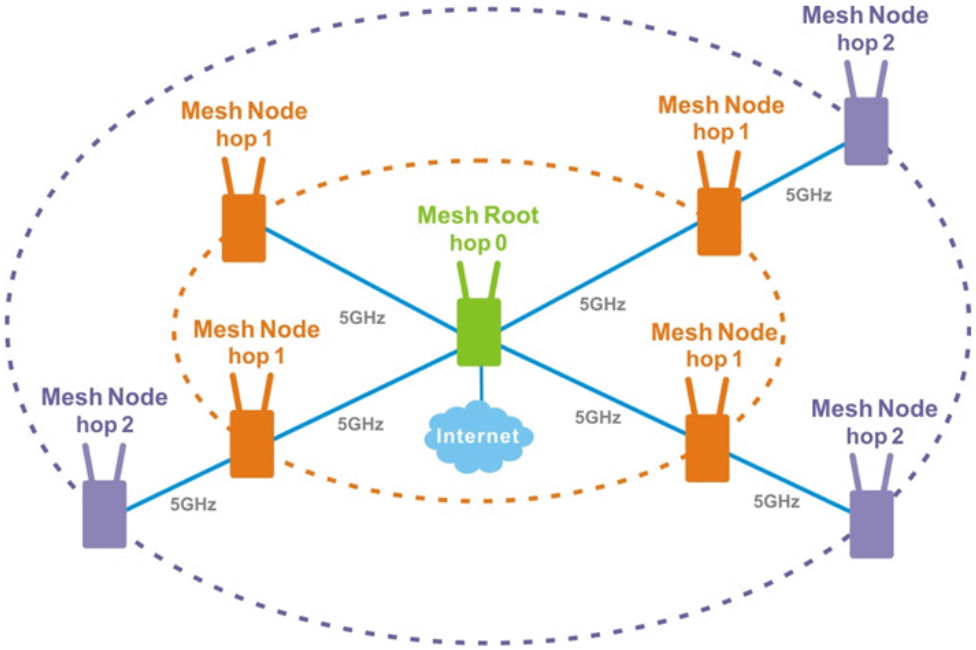
For Mesh networks, Root is also the outlet to the Internet. All devices of a network are in the same Group. The root can add a new Node to its Group or delete members from its Group. Users can choose VigorMesh or EasyMesh to establish the Mesh network. If Mesh is disabled, a network with wired links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

Vigor router plays a role of Mesh root in a VigorMesh network.

Please note that, within VigorMesh network,

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

Refer to the following figure:



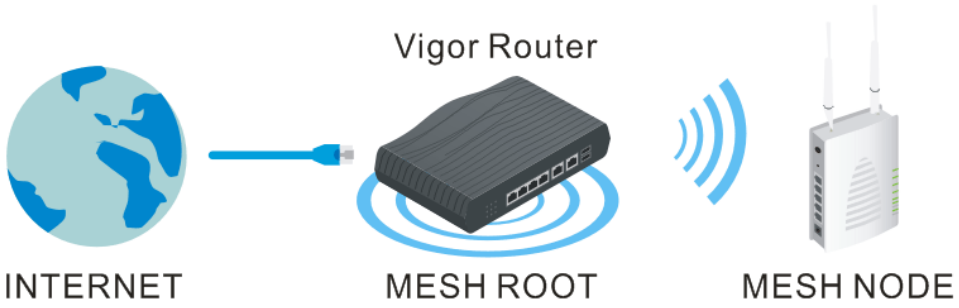

For the mesh group set within VigorMesh network,

- It must be composed by "1" Mesh Root and "0~7" mesh nodes
- (Roaming) Normally members in a mesh group use the same Wireless SSID/security
- (Add) Only the mesh root can add a new mesh node into the mesh group
- (Recover) A disconnected mesh node will automatically try to connect to another connected mesh node of the same group

## Mesh Root

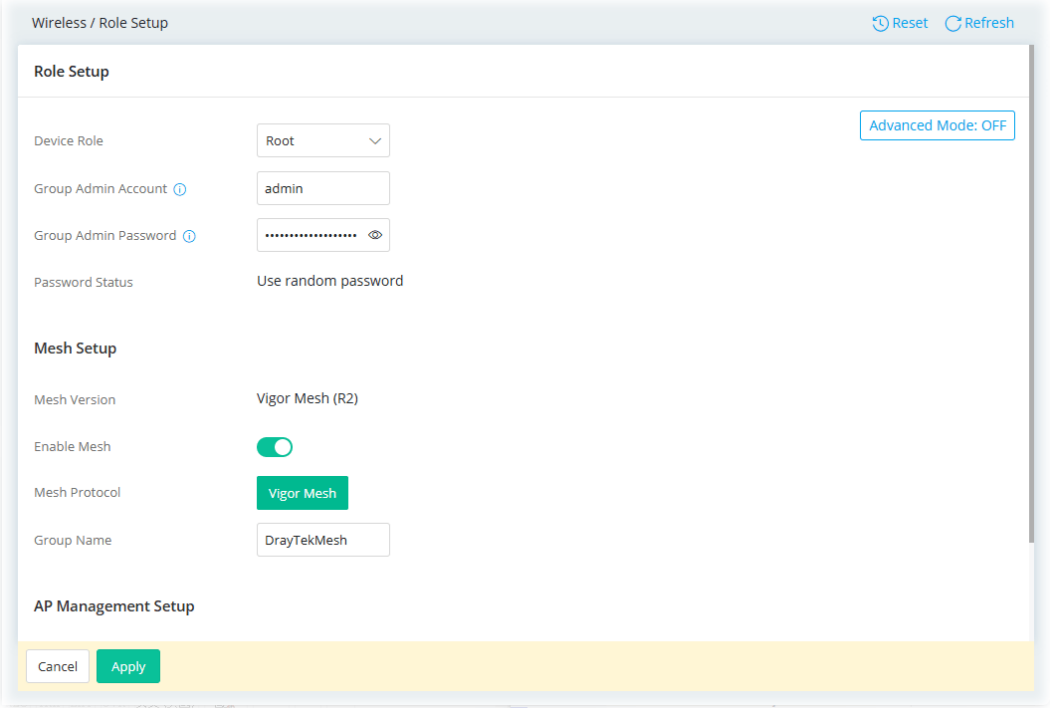
Mesh Root indicates that Vigor router would be other AP's uplink connection. As a Mesh Root, Vigor router must connect to internet through WANs to have an internet connection.

The following figure shows how Vigor router runs as MESH ROOT:



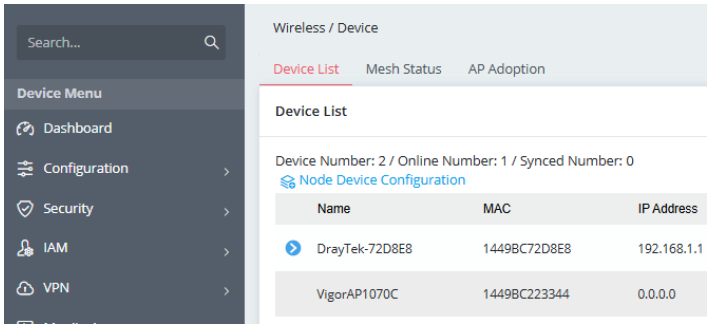
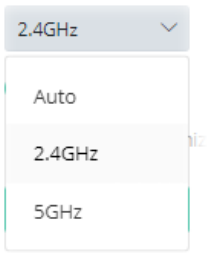

## II-5-1 Role Setup

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




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Advanced Mode:ON/OFF** | Click to show or hide the advanced settings (**Wireless Download Band, Auto Wireless Uplinks Optimization** and **Log Level**). |
| **Device Role** | **Root –** The device is a Root. It controls the network and syncs configurations to the Nodes of its Group. |
| **Group Admin Account** | Set an account for the system administrator to manage the mesh nodes.<br>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. |

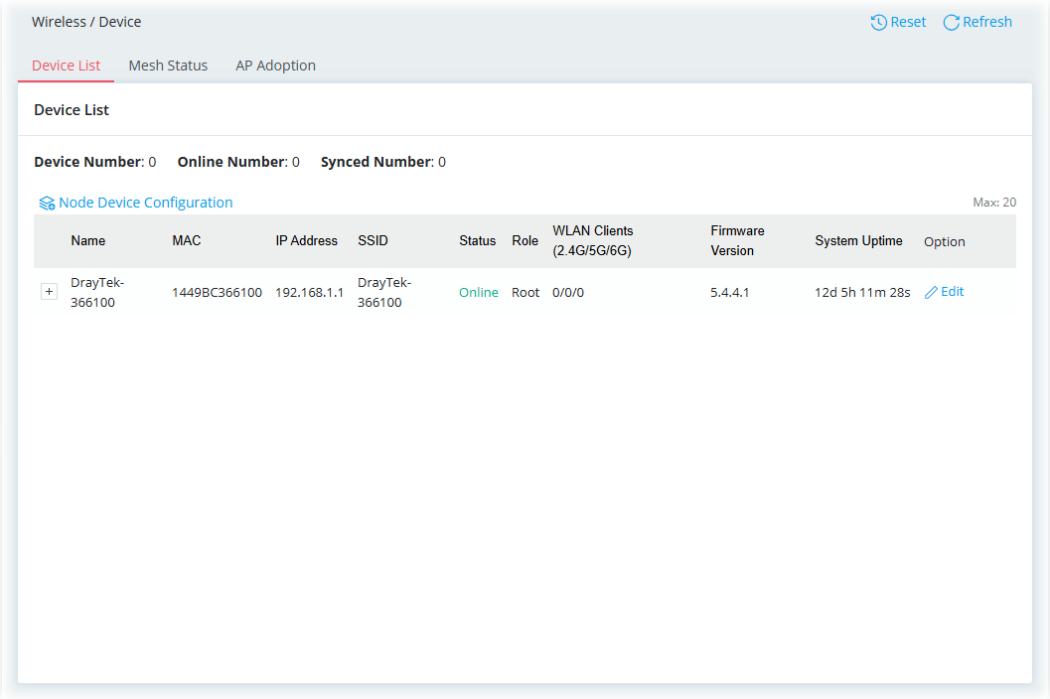
| | |
|---|---|
| | The password configured here will replace the password defined for each node to ensure the mesh node's account security. |
| **Password Status** | **User random password** – The default display state. By default, the mesh group password will be generated randomly by the Vigor system.<br>**Ready** – If the password is set or changed manually, after finishing the configuration, the word "Ready" will be shown instead. |
| **Initial Config Sync** | |
| **Set Configuration by** | **Follow Root -** Follow the root settings to apply the configuration - Full Config or Select Scope. |
| **Config Sync to** | **Full Config –** Sync the full configuration to all nodes.<br>**Select Scope -** Sync the selected configuration to all nodes. |
| **Mesh Setup** | |
| **Enable Mesh** | Switch the toggle to enable or disable the mesh function. |
| **Mesh Protocol** | Select the mesh protocol to manage the mesh network.<br>**Vigor Mesh** – A protocol developed by DrayTek. |
| **Group Name** | Displays the name of the current mesh group. Change the name if required. |
| **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.<br>Default is Disabled. If this feature is enabled, when a new Wired AP is detected by VigorMesh packets through Ethernet, the Root (e.g., Vigor2136) will add it to the **Device>>Device List** and start to register. Then the Node will be adopted automatically.<br>Note that both sides (the root and the node) must support and enable the Auto Wired Adoption.<br> |
| **Wireless Download Band** | It is available only when **Advanced Mode** is set to **On.**<br>Select a wireless band (Auto, 2.4GHz or 5GHz) for connecting with a downlink mesh root or a downlink mesh node.<br> |
| **Auto Wireless Uplinks** | It is available only when **Advanced Mode** is set to **On.** |

| | |
|---|---|
| Optimization | It is enabled in default. To perform the auto reselect, make sure the process for CFG Sync and CFG Check for mesh nodes (members) are successful. If enabled, after changing the environment of mesh network (e.g., offline, disconnection), the root device will perform auto reselect to reconstruct the mesh network. |
| Log Level | It is available only when **Advanced Mode** is set to **On.**<br>Choose **Basic** or **Detailed**. Related information will be shown on Syslog. |
| AP Management Setup | |
| Enable AP Management | Switch the toggle to enable/disable the AP Management. |
| Cancel | Discard current settings and return to the previous page. |
| Apply | Save the current settings and exit the page. |

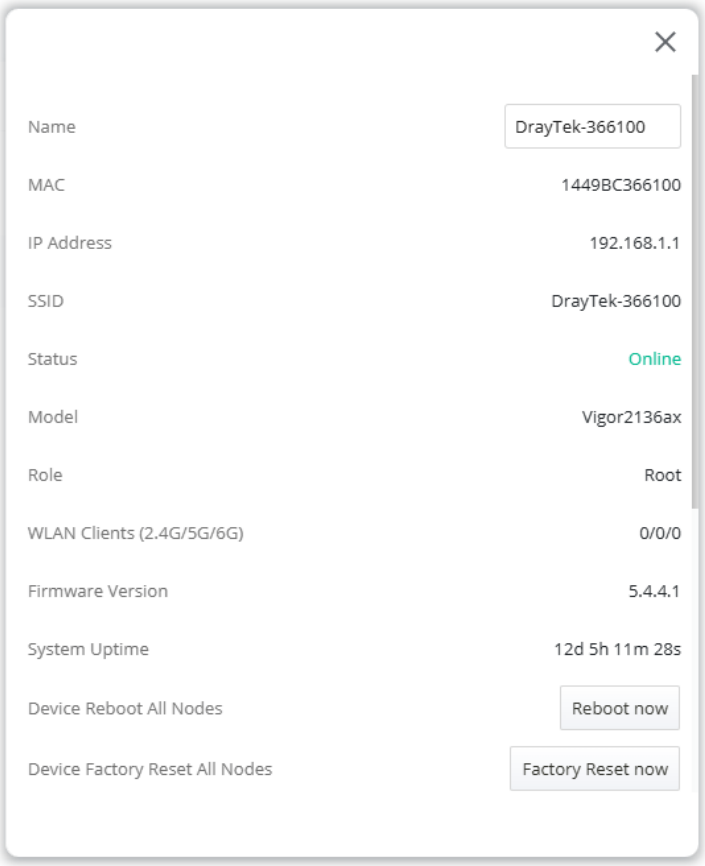
# II-5-2 Device

## II-5-2-1 Device List

General information about Vigor AP devices detected by this router or managed by the Vigor router's AP management system will be displayed on this page.




Click **Edit** 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.




Available settings are explained as follows:

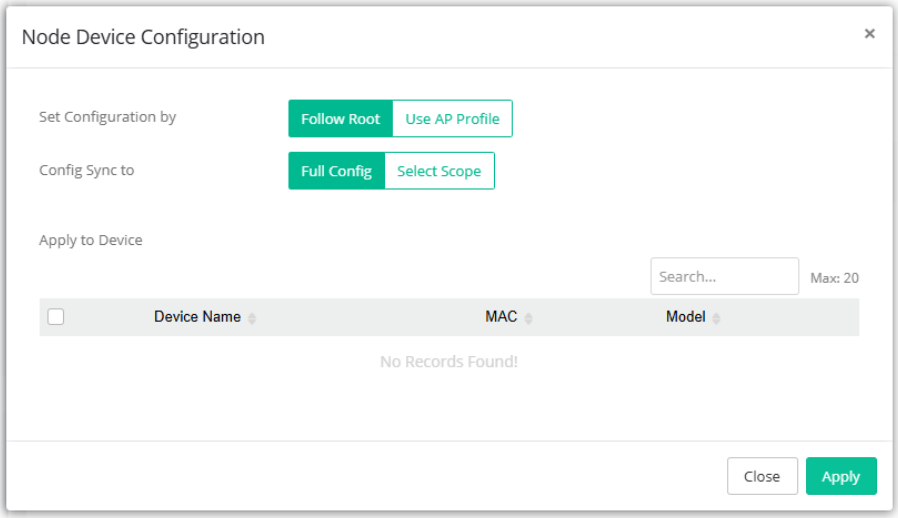
| Item | Description |
|---|---|
| **Device Reboot All Nodes** | **Reboot Now** – Click to reboot all nodes immediately. |
| **Device Factory Reset All Nodes** | **Factory Reset Now** - Click to reset all nodes with factory settings immediately. |
| **Config Sync to All Nodes** | **Full Config** – Sync the full configuration to all nodes.<br>**Select Scope** - Sync the selected configuration to all nodes. |
| **Sync Config** | **Sync now** –Click to execute the sync configuration. |
| **Device Maintenance** | |
| **Admin Account** | The Root uses the settings to manage its AP node.<br>Select the type you need.<br>**Default –** Use the **Group Admin Account / Group Admin Password** configured in **Wireless>>Role Setup** to access the AP node.<br>**Customize –** Use the **Node Account / Node Password** configured in this page to access the AP node.<br>Before being managed by the Root, if the node's account and password have been changed from their default values, make sure to configure the node's account and password here with the same values used by the AP node. Otherwise, the Root will not have permission to manage the selected AP node. |
| **Node Account** | Enter the specific user account name for the selected device if the Admin Account is set to **Customize**.<br>After clicking **Apply**, enter the new account name the next time to |

| | |
|---|---|
| | access the device. |
| **Node Password** | Enter the specific user password for this selected device if the Admin Account is set as **Customize**.<br>After clicking **Apply**, enter the new password the next time to access the device. |
| **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.

## Node Device Configuration

The Vigor router, functioning as a mesh root, can manage up to 49 mesh nodes simultaneously. These nodes can be configured with the settings defined by the Vigor router. A convenient way to apply pre-set configurations to all access points at once is through the "Node Device Configuration" feature.




Available settings are explained as follows:

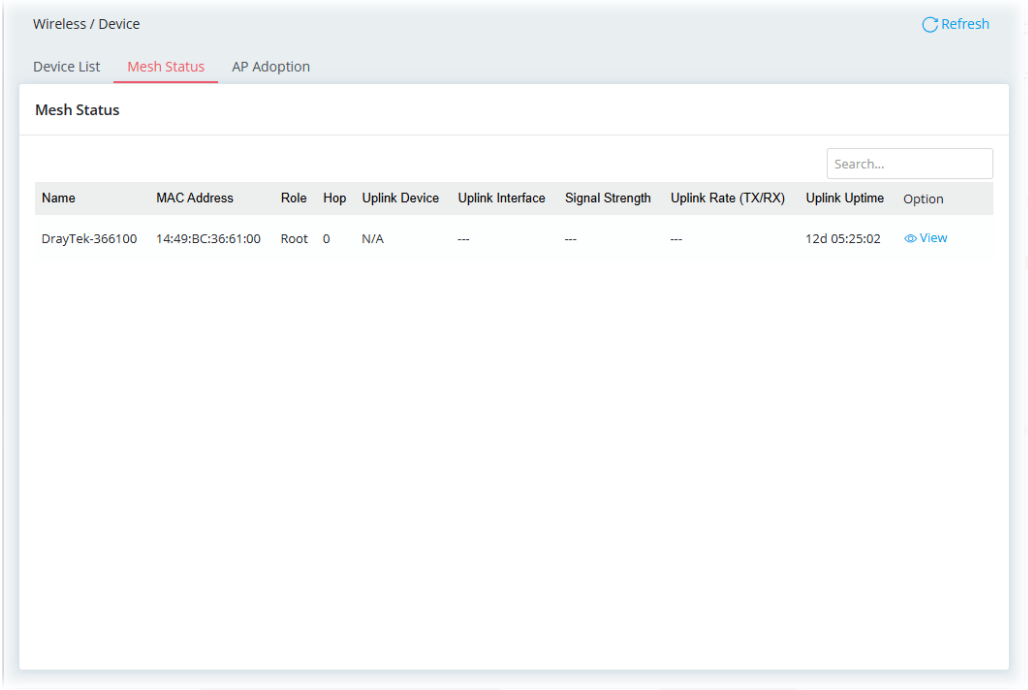
| Item | Description |
|---|---|
| **Set Configuration by** | There are two modes for applying the configuration.<br>**Follow Root –** Follow the root settings to apply the configuration - Full Config or Select Scope.<br>● **Full Config –** Sync the full configuration to all nodes.<br>● **Select Scope -** Sync the selected configuration to all nodes.<br>**Use AP Profile –** Apply the configuration by selecting an AP profile.<br>● **AP Profile -** Select an AP profile from the drop-down list. |
| **Apply to Device** | Display a table of AP device(s) that can be applied with the settings configured by this access point. |
| **Device Name** | Display the device name of the AP node. |
| **MAC** | Display the MAC address of the AP node. |
| **Model** | Display the model name of the AP node. |
| **Close** | Discard current settings and return to the previous page. |
| **Apply** | Save settings to the selected AP nodes and exit the page. |

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

## II-5-2-2 Mesh Status

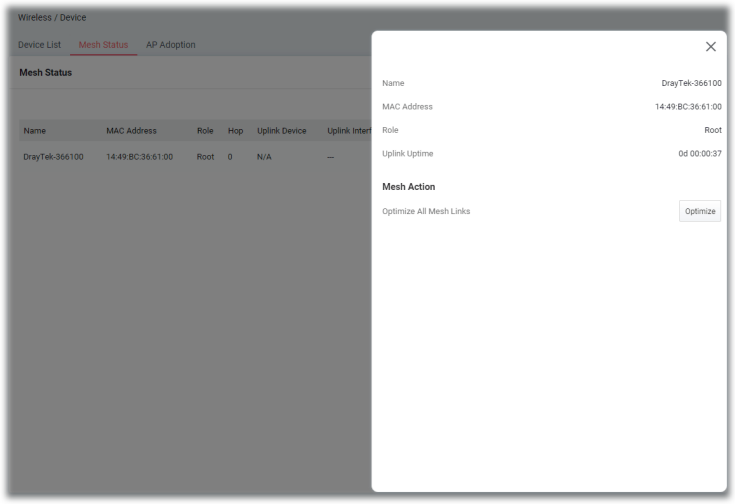
Display general information of the Mesh network, including the mesh root and the mesh nodes.

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




Available settings are explained as follows:

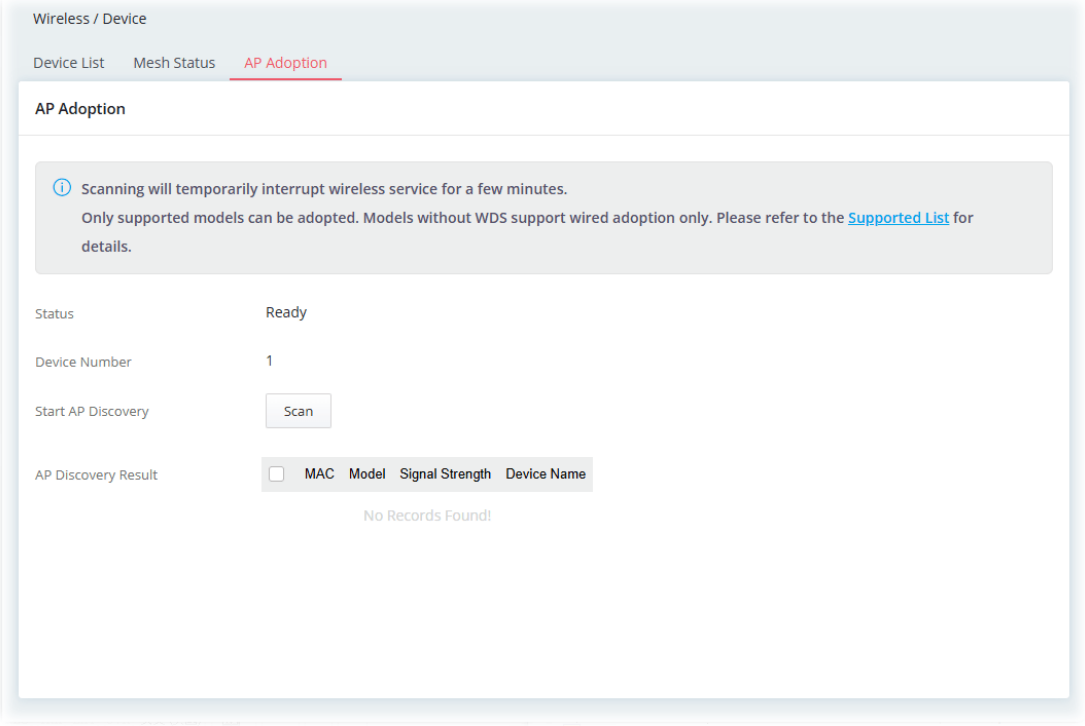
| Item | Description |
|---|---|
| **Name** | Displays the name of the device (for identification). |
| **MAC Address** | Displays the MAC address of the device. |
| **Role** | Displays the role of the device. |
| **Hop** | Displays the number of Wireless links from the device to Root. "0" means the 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.<br>Displays the link rate of the device to its uplink. |
| **Uplink Uptime** | It is available only when **VigorMesh** is selected as Mesh Protocol.<br>Displays how long the device is online. |
| **Option** | Click **View** to modify the selected mesh device. |

| | |
|---|---|
| | <br>**Optimize All Mesh Links -** It is available only when **VigorMesh** is selected as Mesh Protocol and the device is a Root.<br>Press the **Optimize** button to perform reselect to reconstruct the Mesh network. |

## II-5-2-3 AP Adoption

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

This page is available when current device role is Root.




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<br>☐ - Select the checkbox if you want to add the device into a Group.<br>**MAC** - Displays the MAC address of the device.<br>**Model** - Displays the model of the device.<br>**Signal Strength** - Displays the signal strength of the device if it was found through the Wireless.<br>**Device Name** - Insert the name of the device for identification. |

## 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 a Mesh Group through Wireless or Wired connection.
  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

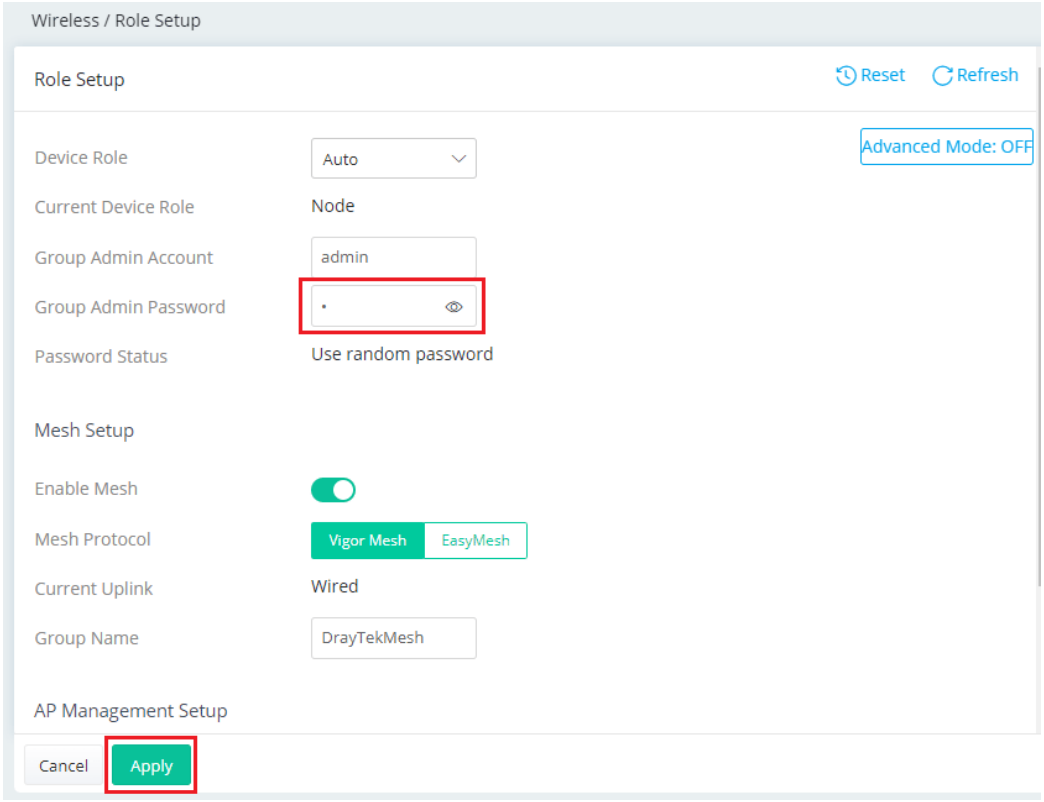
## How to set up a VigorMesh group?

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

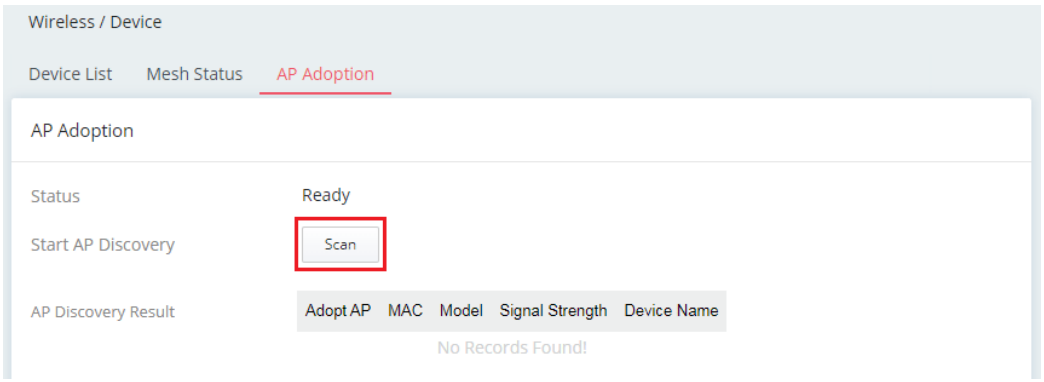
Please access the web of the device which you want to use it as the Root.

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.



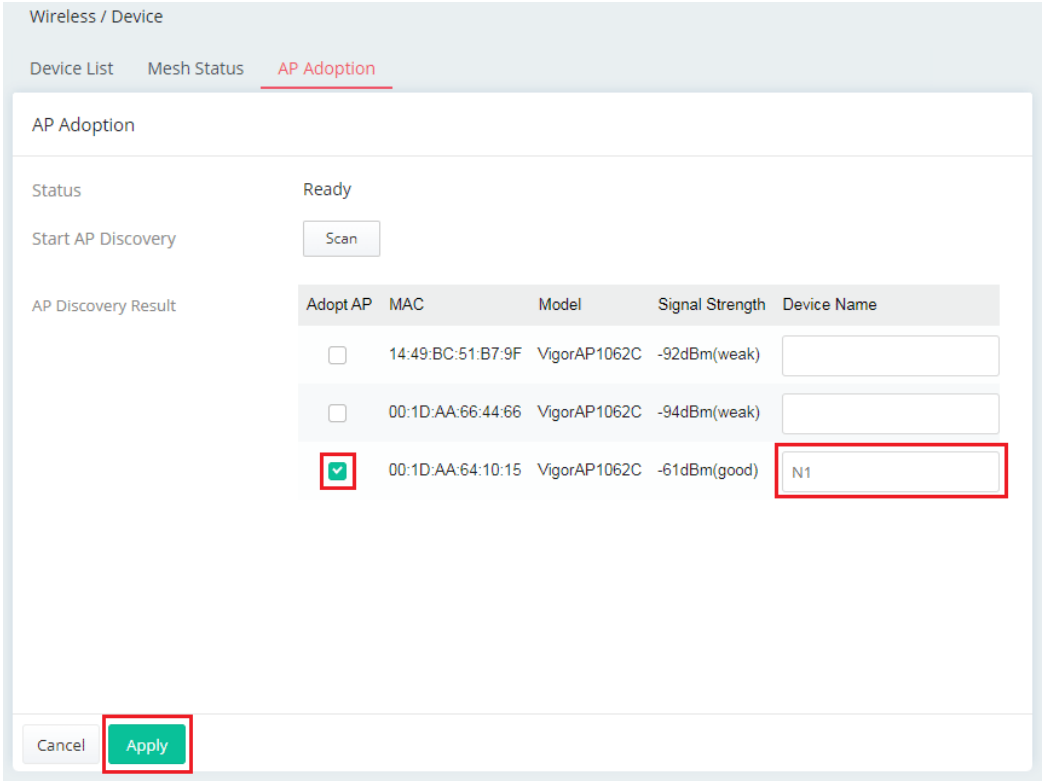

2. Open **Virtual Controller>>Wireless>>Device>>AP Adoption**. Click the **Scan** button.



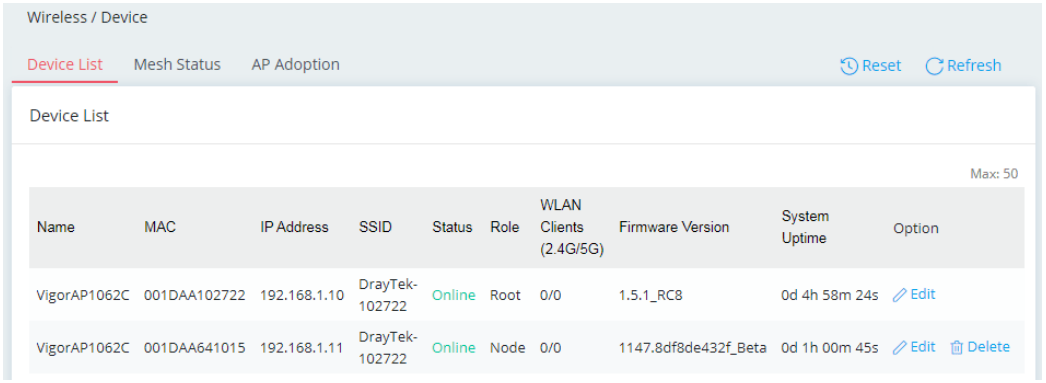

3. Wait until the searching result appears.

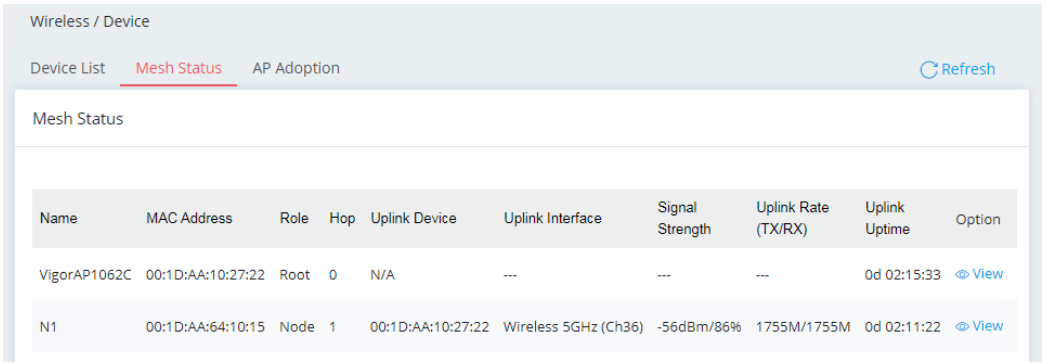
   Choose the device(s) you want to add to the Group and set the names for identification.

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



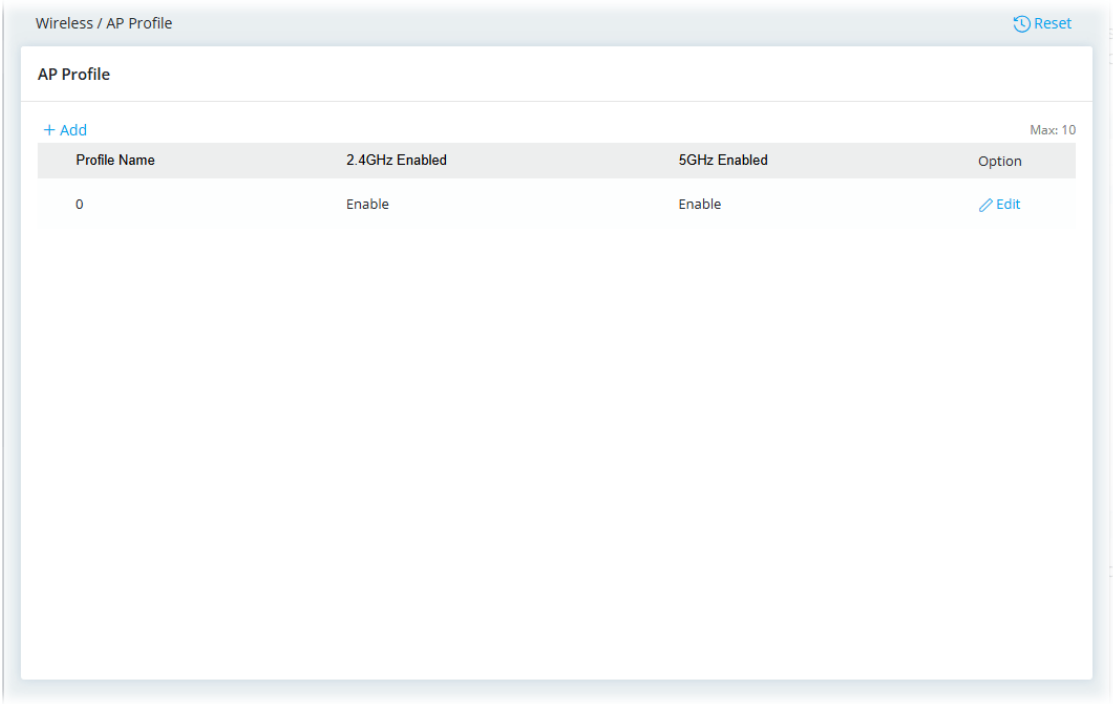

4. Refer to **Virtual Controller>>Wireless>>Device>>Device List** and **Virtual Controller >> Wireless >> Device >>Mesh Status** for viewing the result.



## II-5-3 AP Profile

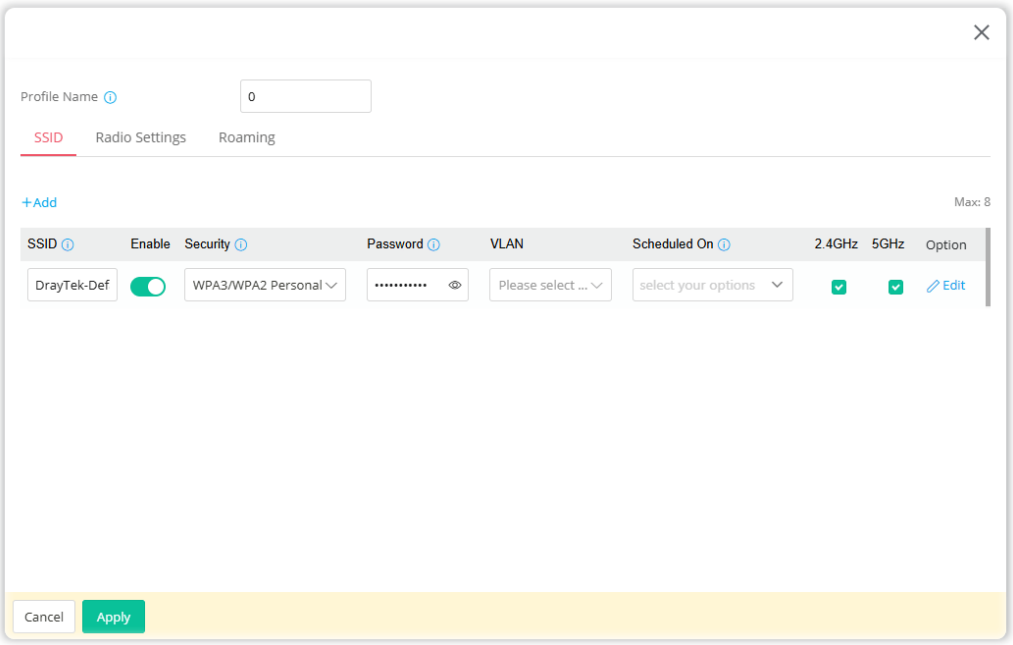
AP profile is used to apply to a selected access point. It is very convenient for the administrator to configure the setting for access point without opening the web user interface of the access point.




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

### II-5-3-1 SSID

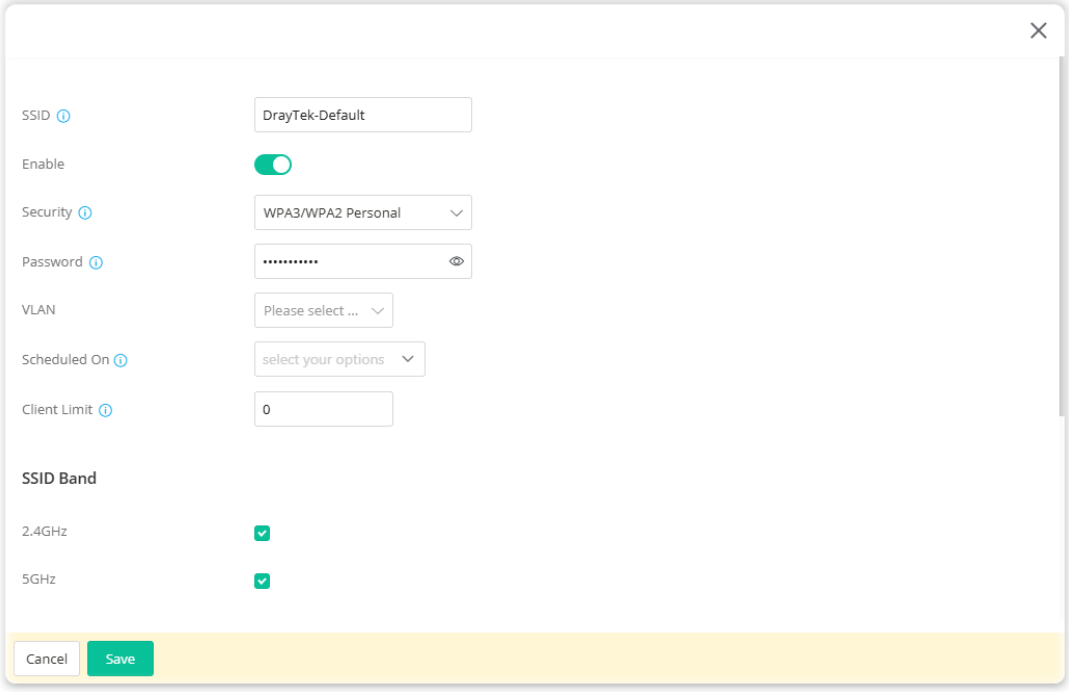
An AP profile can be configured to support up to 8 SSIDs.




Available settings are explained as follows:

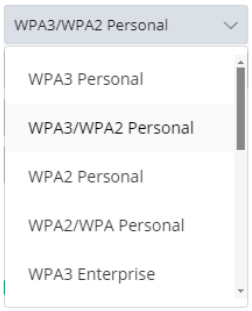
| Item | Description |
| --- | --- |
| +Add | Click to create a new entry. |
| SSID | Enter a name as the AP identifier. |
| Enable | Switch the toggle to enable or disable the SSID. |
| Security | Select the security mode. |
| Password | Enter 8~64 ASCII characters. |
| VLAN | Select a VLAN to which 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. |

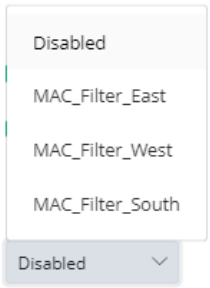
Click **Edit** to configure detailed settings for the SSID profile.




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.<br>Below shows the modes with higher security:<br>● **WPA3 Personal, WPA3/WPA2 Personal, WPA2 Personal, WPA2/WPA Personal -** Accepts only WPA clients and the encryption key should be entered in Password. The WPA encrypts each frame transmitted from the radio using the PSK (Pre-Shared Key) entered manually in Password."<br>● **WPA3 Enterprise, WPA2 Enterprise, WPA2/WPA Enterprise -** Accepts only WPA clients and the Authentication Server |

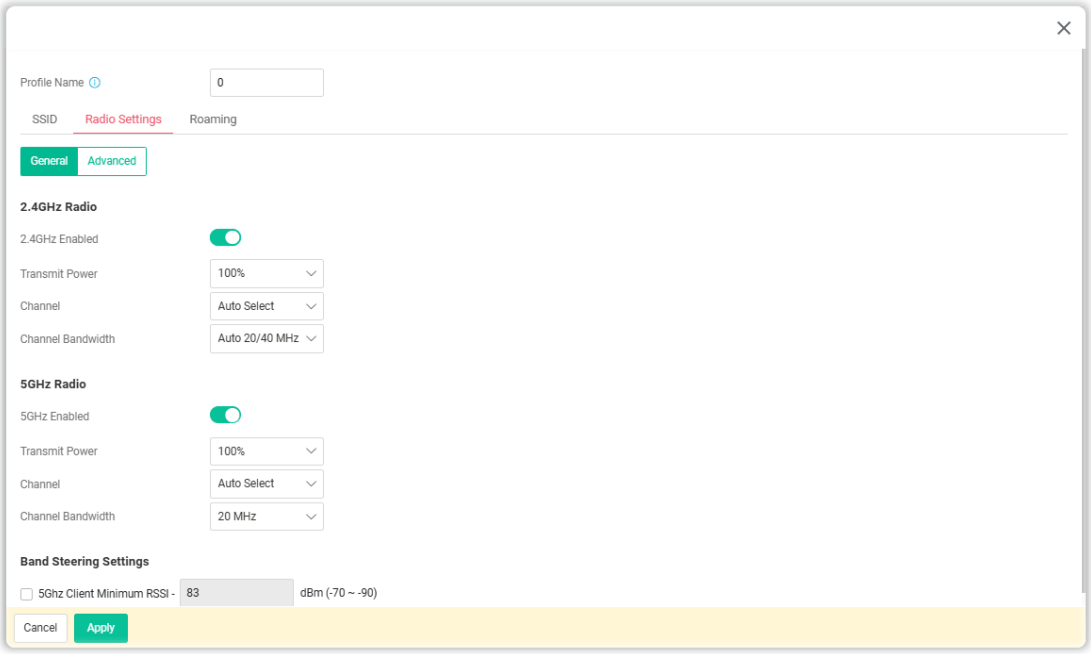
| | |
|---|---|
|  | should be set in Configuration >> RADIUS/ TACACS+ >> External RADIUS and be selected in RADIUS Server. The WPA encrypts each frame transmitted from the radio using the key which automatically negotiated via 802.1x authentication.<br>• **OWE** - WPA3 also introduces a new open and secure connection mode; "Opportunistic Wireless Encryption" (OWE). It allows the clients to connect without a password, ideal for hotspot networks, but the connection between each individual client is uniquely encrypted behind the scenes.<br>Below shows the modes with basic security:<br>• **WPA Personal** - Accepts only WPA clients and the encryption key should be entered in Password. The WPA encrypts each frame transmitted from the radio using the PSK (Pre-Shared Key) entered manually in Password.<br>• **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.<br>• **WEP Personal** - Accepts only WEP clients and the encryption key should be entered in WEP Settings.<br>• **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).<br>The default is **Always On**. |
| **Client Limit** | Enter the limit number of the client(s) connecting to this AP via this SSID (0 means no limit). |
| **SSID Band** | |
| **2.4GHz/5GHz** | Select the band(s) for the SSID. |
| **SSID Settings** | |
| **MAC Filtering List** | The default is **Disabled**.<br>Select one of the MAC filter profiles (created via Security>>MAC Filtering Profile) for this SSID setting.<br>Only the valid MAC address that has been configured allow or deny to access the wireless LAN interface. |

| | |
|---|---|
| |  |
| **Isolate Client from Wireless** | Switch the toggle to enable/disable the function.<br>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.<br>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.<br>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.<br>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-5-3-2 Radio Settings

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




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.<br>**40 MHz** – Vigor Router will utilize 40 MHz for data transmission and reception between the router and wireless stations.<br>**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 |

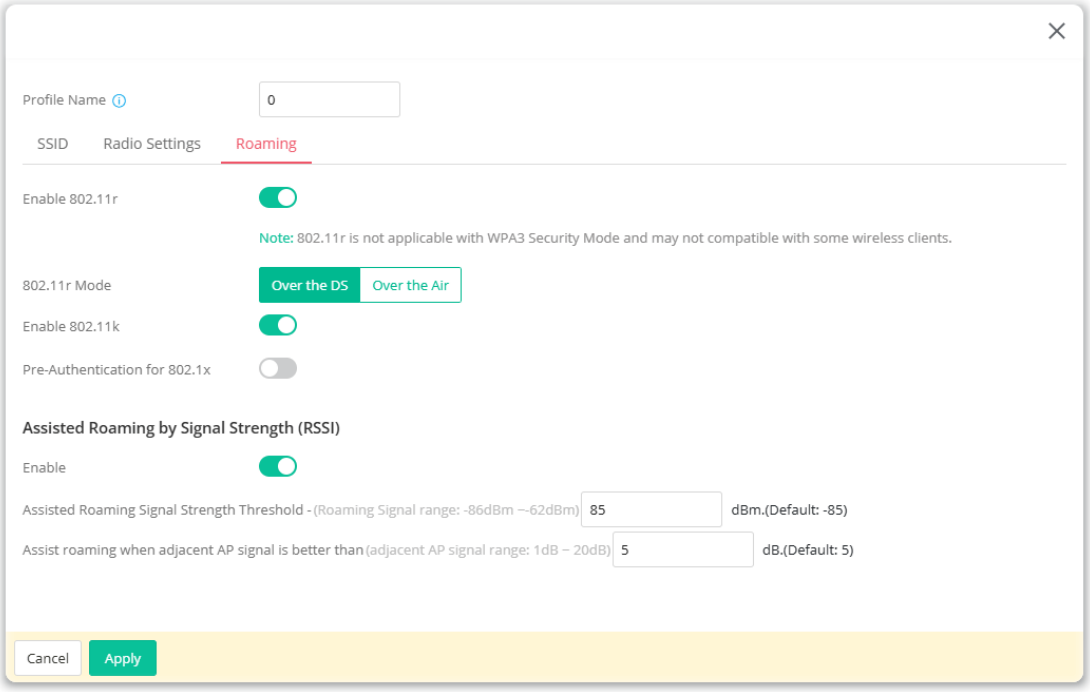
| | |
|---|---|
| | signal will be. |
| Channel | Allows you to specify a particular wireless channel to use, or let the system determine the optimal channel by selecting "**Auto Select**". The list of available channels varies depending on the local for which the router is intended. |
| Channel Bandwidth | **20 MHz** –Vigor Router will utilize 20 MHz for data transmission and reception between the router and wireless stations.<br>**40 MHz** – Vigor Router will utilize 40 MHz for data transmission and reception between the router and wireless stations.<br>**80 MHz** –Vigor Router will utilize 80 MHz for data transmission and reception between the router and wireless stations.<br>**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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>Environments that can benefit by applying airtime fairness:<br>(1) Many wireless stations.<br>(2) All stations mainly use download traffic.<br>(3) The performance bottleneck is wireless connection. |
| **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-5-3-3 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.




Available settings are explained as follows:

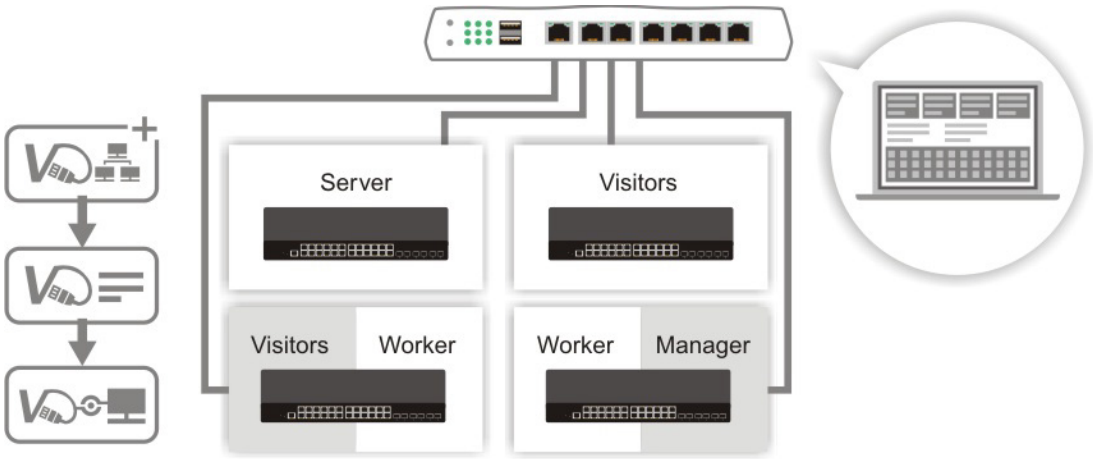
| Item | Description |
|---|---|
| **Enabled 802.11r** | Switch the toggle to enable/disable the function of fast roaming to make Wireless clients switch between the hotspots fast and securely.<br>There are two methods to run fast roaming. |
| **802.11r Mode** | **Over the DS** - In response to the needs of signal strength change, the client can communicate with the other AP through the original AP with Action Frames (FT Request and FT Response).<br>**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)<br>Switch the toggle to enable/disable 802.11x Pre-Authentication.<br>**Enable** - Enable IEEE 802.1X Pre-Authentication.<br>**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.<br>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.

# II-6 Virtual Controller - Switch

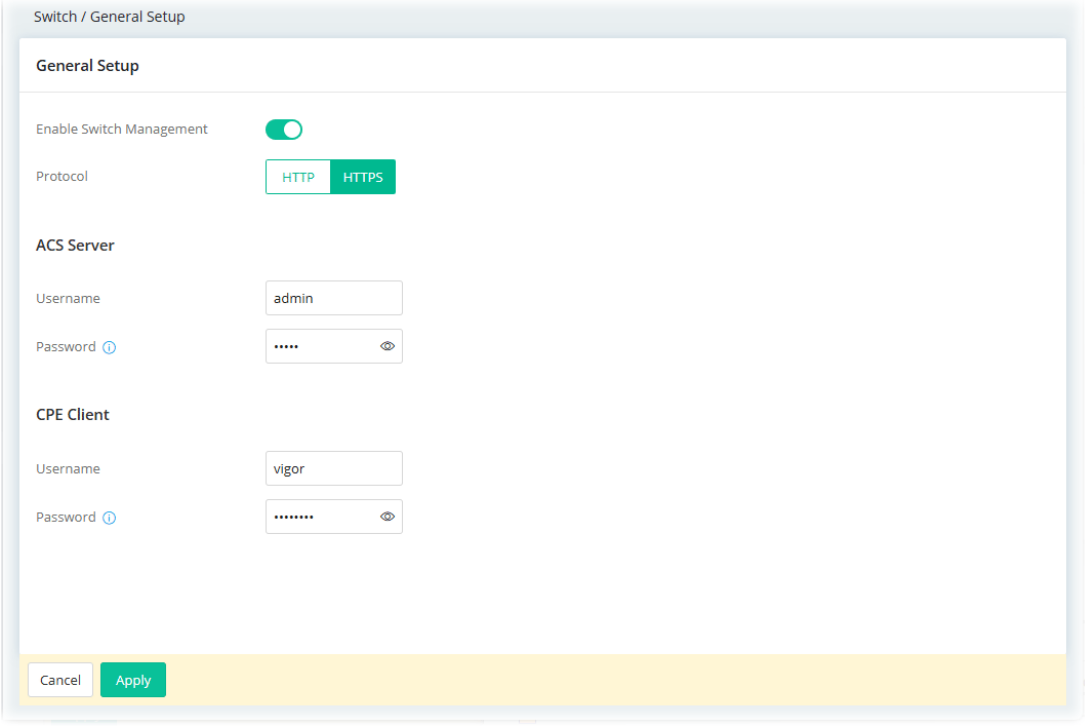
Vigor router can manage lots of VigorSwitch devices connected to it. Through profile and group settings, the administrator can execute firmware/configuration backup, restore for VigorSwitch device, reboot the device or return to factory default settings of VigorSwitch at one time.




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

## II-6-1 General Setup

In this page, switch the toggle to enable / disable the switch management function.

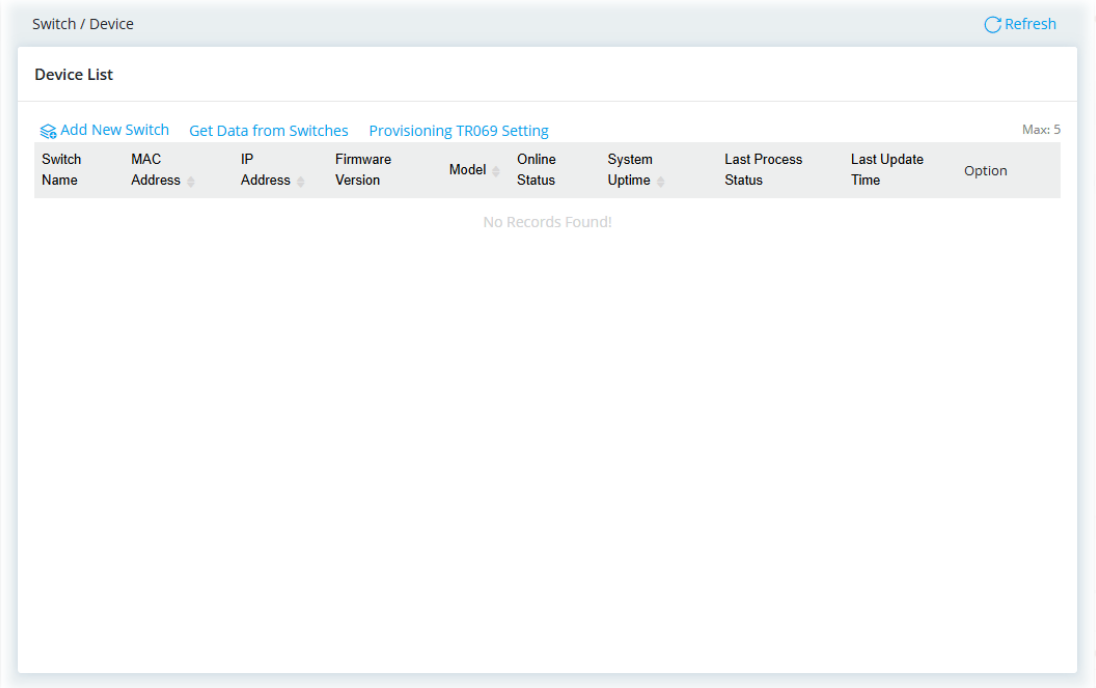



Available settings are explained as follows:

| Item | Description |
| --- | --- |
| Enable Switch Management | Switch the toggle to enable or disable the switch management function. |
| Protocol | Select HTTP or HTTPS as the protocol to connect to this router. |
| ACS Server | |
| Username | Enter the username required for the Vigor switch to connect to the ACS server.<br>The username configured here will be synchronized with the switch managed by this router. (The username should match what is set in the ACS server under System Maintenance >> Access Management >> TR-069 of the VigorSwitch.) |
| Password | Enter the password required for the Vigor switch to connect to the ACS server.<br>The password configured here will be synchronized with the switch managed by this router. (The password should match what is set in the ACS server under System Maintenance >> Access Management >> TR-069 of the VigorSwitch.) |
| CPE Client | |
| Username | Enter the username required for the Vigor router to connect to this switch. (The username should match what is set in the CPE Settings under System Maintenance >> Access Management >> TR-069 of the VigorSwitch.) |
| Password | Enter the password required for the Vigor router to connect to this switch. (The password should match what is set in the CPE Settings under System Maintenance >> Access Management >> TR-069 of the VigorSwitch.) |
| Cancel | Discard current settings. |
| Apply | Save the current settings. |

# II-6-2 Device

This page displays information, including Switch name, MAC address, IP address, Firmware Version, Model, Online Status, System Uptime, Port in Use, Clients, Last Process Status and Option of a VigorSwitch connected to the Vigor router.

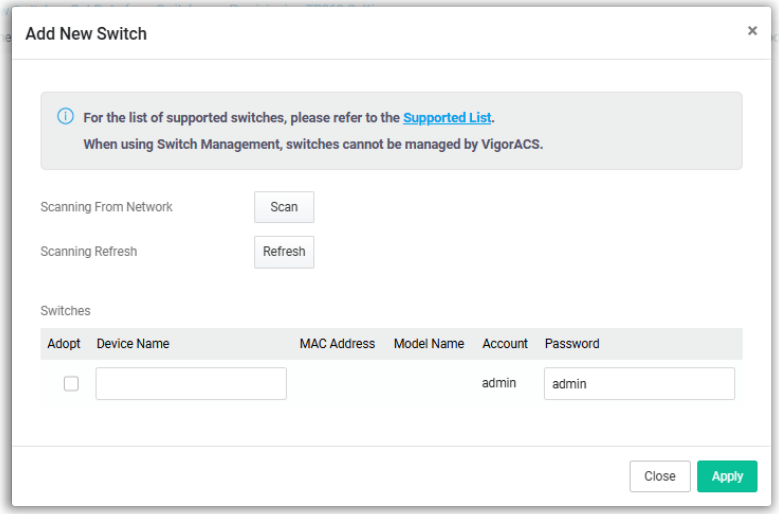



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Add New Switch** | Click to add a new switch to be managed by the Vigor router. |
| **Get Data from Switches** | Click to get the new information (e.g., switch name, MAC address, IP address, and so on) related to all switches managed by the Vigor router. |
| **Provisioning TR069 Setting** | Click to send TR-069 provisioning settings (including protocol type, ACS username, ACS password, CPE username and CPE password) to all switches managed by the Vigor router. |
| **Option** | **Edit** – Click to modify settings of the selected Vigor switch.<br>**Delete** – Click to remove the selected Vigor switch item.<br>**Get** – Click to assign IP address to the selected Vigor switch item. |

## Add New Switch

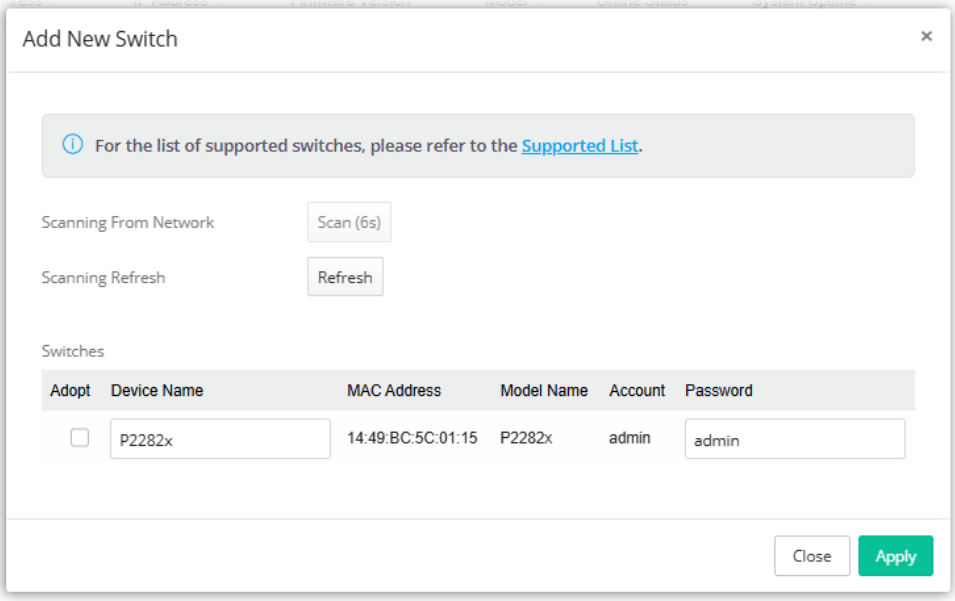
1. To add a new switch, click the **Add New Switch** link to open the following page.




Available settings are explained as follows:

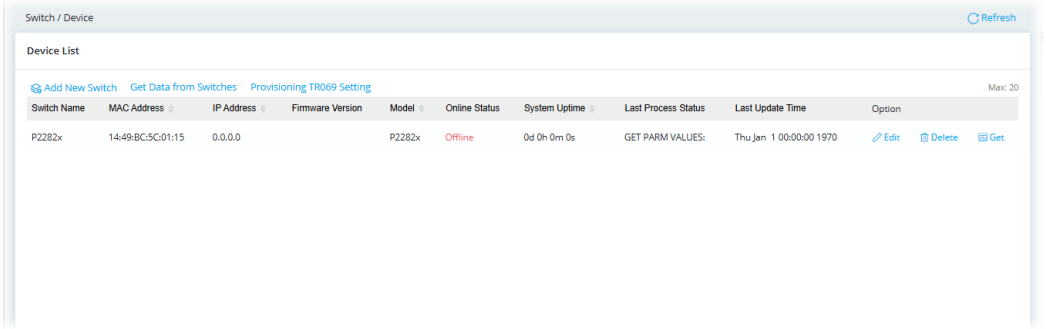
| Item | Description |
|---|---|
| **Scan** | Search the switch around the Vigor router. The searched switch(es) will be displayed under Switches table. |
| **Refresh** | Refresh the Switches table. |
| **Adopt** | Select the Vigor switch to be managed by Vigor router. |
| **Device Name** | Display the name of the Vigor switch. |
| **Password** | Display the password for login this Vigor switch. |
| **Close** | Exit the dialog without saving the settings. |
| **Apply** | Save the settings. |

2. Click **Scan** and wait for a while Vigor router will scan and list the switch connecting to Vigor router.

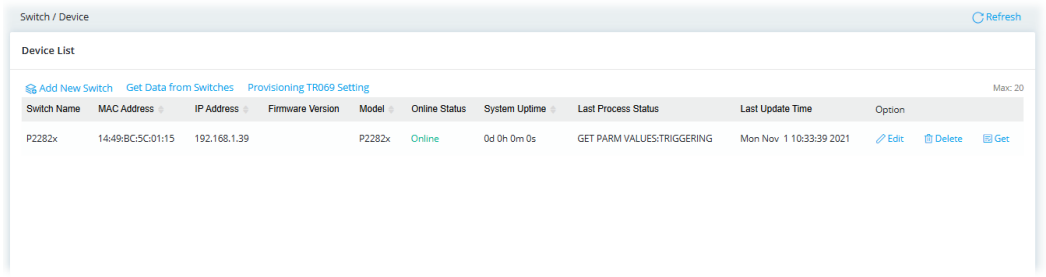



3. Check the box below **Adopt** to select the device and click **Apply**.

   The selected switch(es) will be displayed on the Device List as shown below.



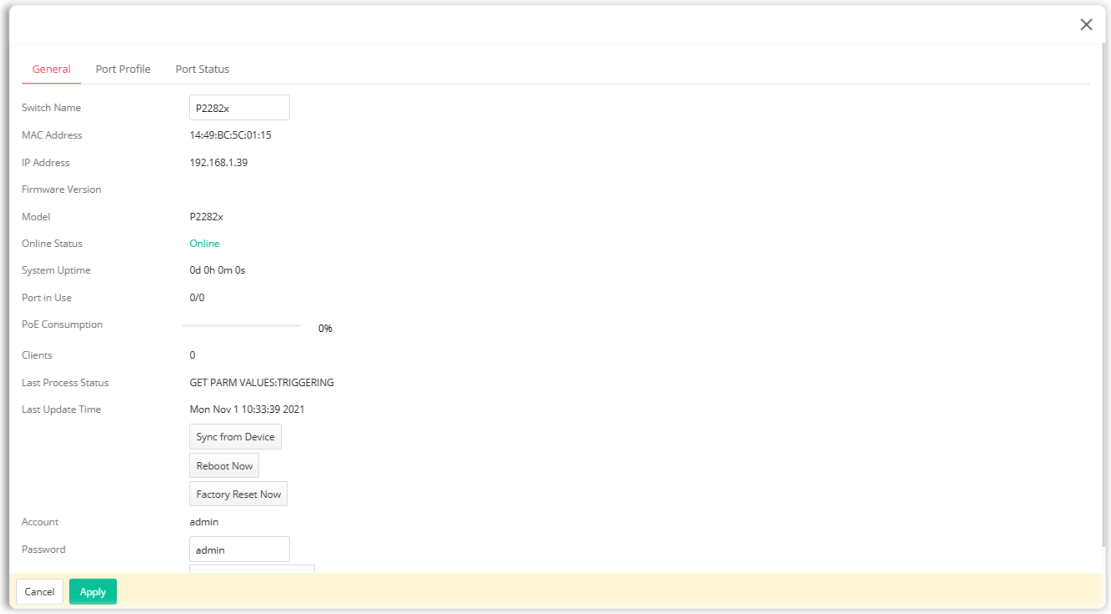

Note: If the **Online Status** shows as **Offline**, click **Get** to obtain the IP address assigned by the Vigor router.




4. When the **Online Status** shows as **Online**, the selected switch is managed by the Vigor router.

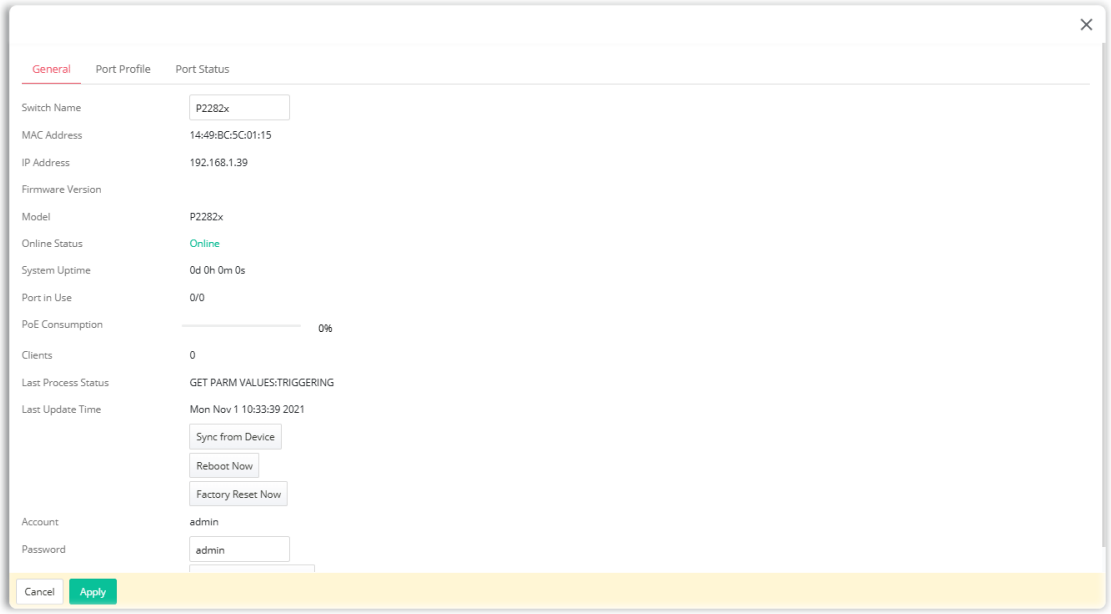
## Edit Switch Settings

To edit the device information, set port profile or view the port status of the switch, click **Edit.**




## General

This page shows a summary related to the VigorSwitch. Also, it offers Reboot Now and Factory Reset Now buttons to assist users in updating the switch.



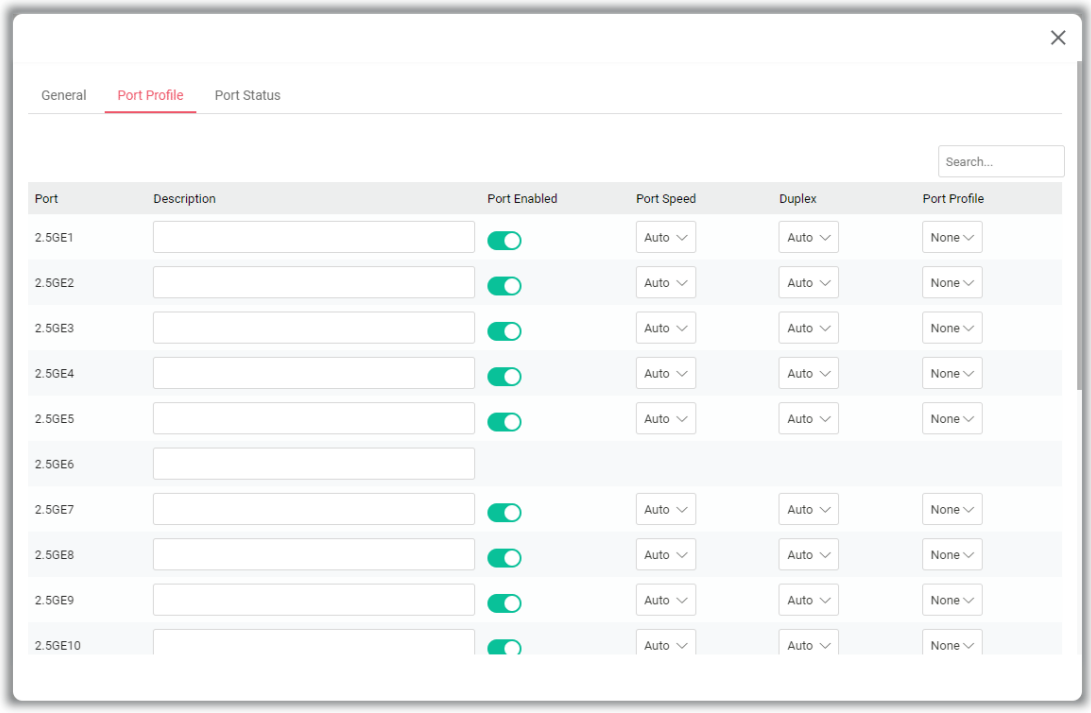

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Switch Name** | Display the name of the switch. Change the name if required. |
| **Sync from Device** | Click to get the new information (e.g., switch name, MAC address, IP address, and so on) related to this switch. |
| **Reboot Now** | Click to reboot the switch immediately with current configuration. |
| **Factory Reset Now** | Click to reset the switch with factory default setting. |
| **Password** | The password displayed here must match the login password for the Vigor Switch. Otherwise, the selected switch will not be managed by the Vigor router, and the Port Profile and Port status may not display accurately.<br>**Provisioning CWMP Conf** – Click to send TR-069 provisioning settings from the Vigor router to the switch, ensuring it is managed by the Vigor router. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings and exit the page. |

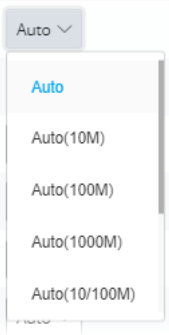
After finishing this web page configuration, please click **Apply** to save the settings.

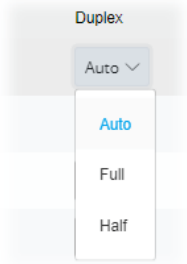
## Port Profile

This page configures the speed, duplex mode, and port profile for each GE port of the VigorSwitch.




Available settings are explained as follows:

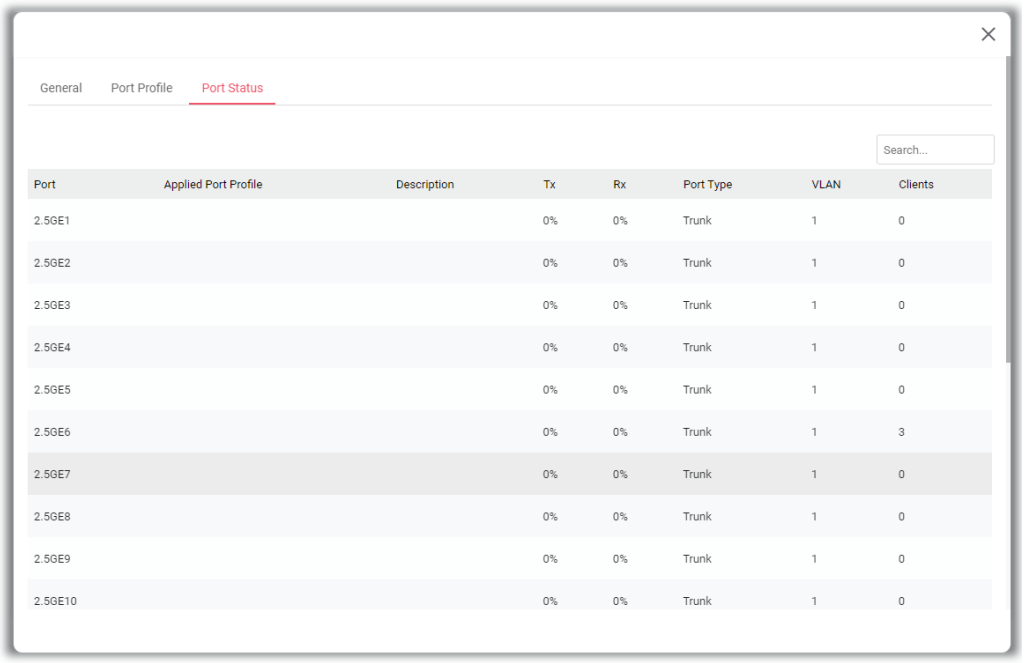
| Item | Description |
|---|---|
| **Port** | Display the number of the GE port. |
| **Description** | If required, enter a brief description to explain the device connected to VigorSwitch via the LAN port. |
| **Port Enabled** | The port (e.g., GE2 in this case) which is used to connect VigorSwitch and Vigor router will not be shutdown by Vigor router.<br>Other LAN ports of VigorSwitch allow to connect to any LAN device. When it is checked, after clicking **Apply**, the network connection between that device and VigorSwitch will be terminated. |
| **Port Speed** | Ethernet speed is set automatically by router system or manually set to 10M/100M/1000M/2G bit/s.<br><br><br>Port speed capabilities:<br>• **Auto:** Auto speed with all capabilities.<br>• **Auto(10M):** Auto speed with 10M ability only. |

| | |
|---|---|
| | • **Auto(100M):** Auto speed with 100M ability only.<br>• **Auto(1000M):** Auto speed with 1000M ability only.<br>• **Auto(10/100M):** Auto speed with 10/100M ability.<br>• **10M:** Force speed with 10M ability.<br>• **100M:** Force speed with 100M ability.<br>• **1000M:** Force speed with 1000M ability.<br>Selecting Auto (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.<br>For SFP fiber module, you might need to manually configure the speed to match fiber module speed. |
| **Duplex** | Select the duplex mode for the LAN port.<br>**Auto** – Auto duplex with all capabilities.<br>**Full** – Auto speed with 10/100/1000M ability only. Allows data transmission in both directions.<br>**Half** - Auto speed with 10/100M ability only. Allows data transmission in both directions. However, only one device (router or peer's device) is allowed to transmit data at the same time.<br> |
| **Port Profile** | Select a port profile to which the LAN port of VigorSwitch will apply. |
| **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.

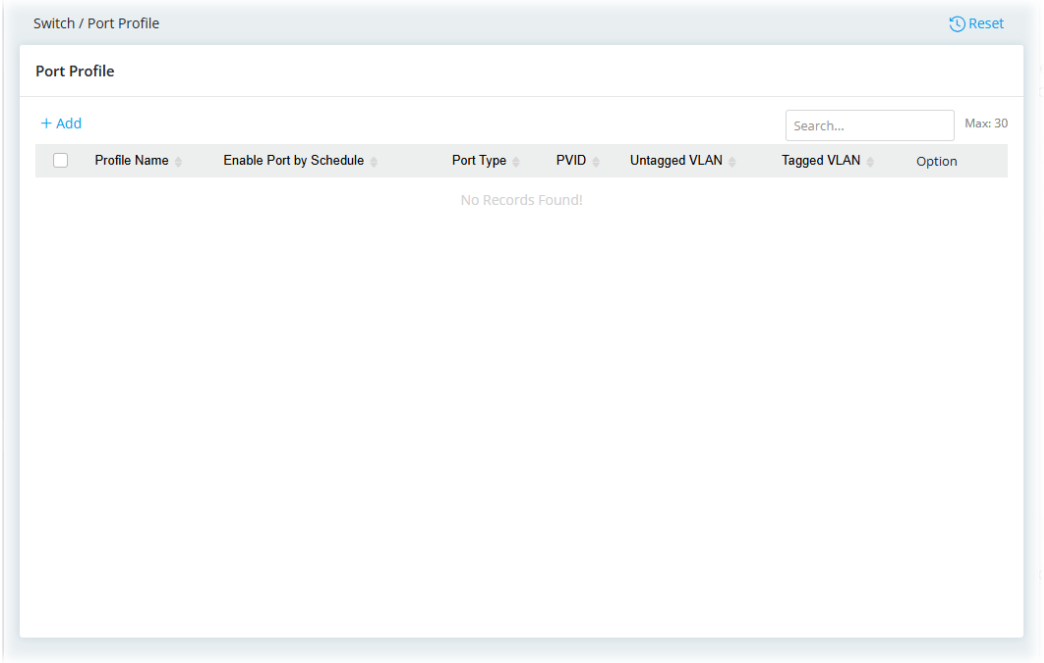
## Port Status

This page will display the current status of each GE port of the Vigor switch such as the transmission rate (TX/RX), port type, VLAN ID, applied port profile, etc.



# II-6-3 Port Profile

This page allows you to configure profiles with general settings such as name, group, IP address, MAC address, model, and password required by VigorSwitch when it connects to this Vigor router.

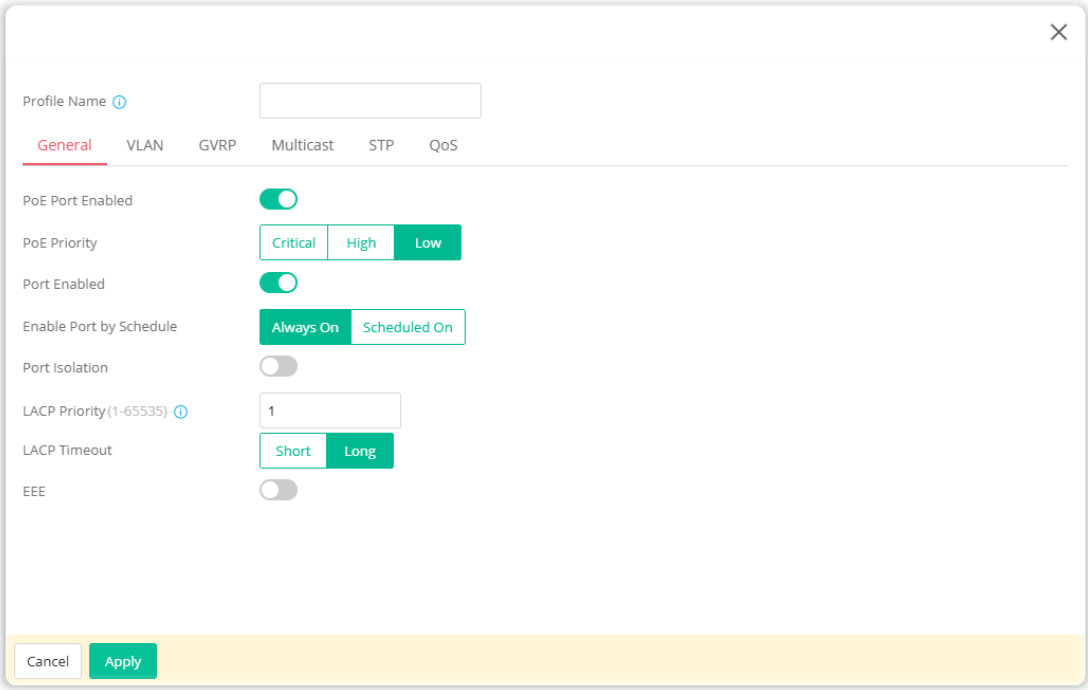



To add a new profile, click **+Add**. To modify an existing profile, select the one and click the **+Edit** link to open the setting page.

## General

Available settings displayed here will vary according to the VigorSwitch managed by Vigor router.

Below is the settings page after clicking **+Add**.




Available settings are explained as follows:

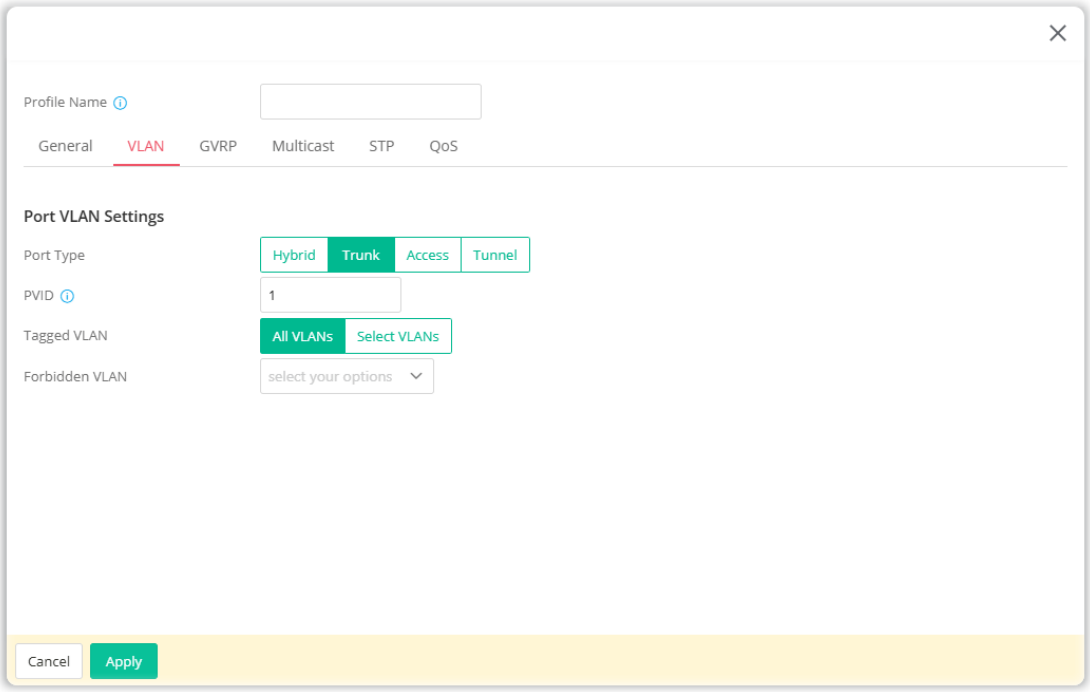
| Item | Description |
|---|---|
| **Profile Name** | Enter a name for the Switch. The purpose of name is used for identification.<br>It is useful when there are many VigorSwitch (same modes) devices connecting to Vigor router. |
| **PoE Port Enabled** | Enable/disable the PoE feature of the selected port. If enabled, this port can be used for connecting the PoE device. |
| **PoE Priority** | Select Priority for PoE device.<br>**Critical** - Set PoE device to highest priority connection.<br>**High** –Set PoE device to high priority connection.<br>**Low** –Set PoE device to low priority connection. |
| **Port Enabled** | Switch the toggle to enable/disable the function of **Enable Port by Schedule**. |
| **Enable Port by Schedule** | Set the valid time for the "port profile" when it is applied to specific GE port.<br>**Always On** – The port profile will be valid all the time if it is enabled.<br>**Scheduled On** – The port profile will be valid based on the time schedule specified here. |
| **Port Isolation** | It allows the network administrator to configure protected port setting to prevent the selected ports from communication with each other. Port isolation is only allowed to communicate with unprotected port.<br>For example, GE1 and GE3 are selected in Port List and Enable is clicked as port isolation, then users behind GE1 and GE3 are separated and can not communicate with each other.<br>Switch the toggle to enable / disable this function. |
| **LACP Priority** | Enter a port priority number (1 to 65535) for the port. |
| **LACP Timeout** | The timeout option decides how local switch of LAG connection determines connection to be lost. Switch would also notify the |

| | |
|---|---|
| | remote switch about this setting value, so that remote switch can send LACP PDU in correct timing.<br>**Short -** LACP PDU will be sent per second. If port member is not seen over 3 seconds, it will cause port member timeout.<br>**Long -** LACP PDU will be sent every 30 seconds. If port member is not seen over 90 seconds, it will cause port member timeout. |
| **EEE** | Switch the toggle to enable or disable port EEE (Energy Efficient Ethernet) function for the selected port. |
| **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.

## VLAN

This page allows a user to configure interface (GE) settings related to VLAN.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Profile Name** | Enter a name for the Switch. The purpose of name is used for identification.<br>It is useful when there are many VigorSwitch (same modes) devices connecting to Vigor router. |
| **Port Type** | Select the VLAN mode of the interface.<br>**Hybrid** – Support all functions as defined in IEEE 802.1Qspecification.<br>**Trunk** - An untagged member of one VLAN at most, and is a tagged member of zero or more VLANs.<br>**Access** – Accepts only untagged frames and join an untagged VLAN.<br>**Tunnel** - Accepts only untagged frames and join an untagged VLAN. |
| **PVID** | A PVID (Port VLAN ID) is a tag that adds to incoming untagged frames received on a port so that the frames are forwarded to the VLAN group that the tag defines.<br>For port under **Access/Tunnel** Mode, VLAN ID provided as PVID would automatically be selected as the untagged VLAN. |
| **Accepted Type** | It is available when Hybrid is selected as the port type.<br>Specify the acceptable-frame-type of the specified interfaces. It's only available with Hybrid mode.<br>**All** - Accept frames regardless it's tagged with 802.1q or not.<br>**Tag Only** - Accept frames only with 802.1q tagged.<br>**Untag Only** - Accept frames untagged. |

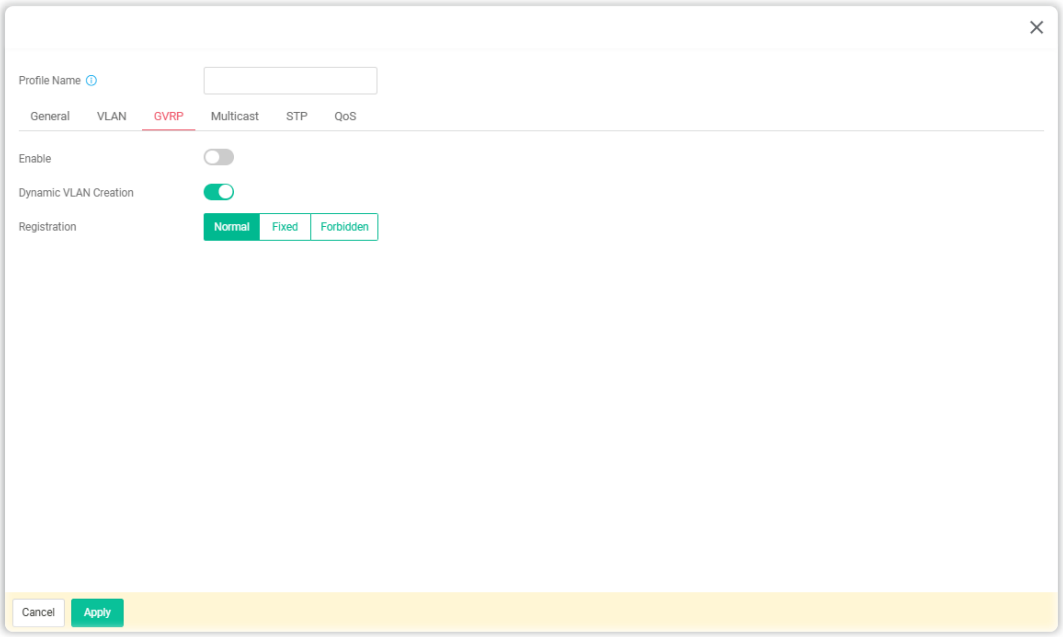
| | |
|---|---|
| **Untagged VLAN** | It is available when Hybrid is selected as the port type.<br>Specify the VLAN profile to be untagged in the VLAN. |
| **Tagged VLAN** | Select all VLAN profiles or independent VLAN profiles to be tagged in the VLAN. |
| **Forbidden VLAN** | The GE port set in a VLAN profile allows default VLAN packet to pass through.<br>Select the VLAN profile as forbidden VLAN. |
| **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.

## GVRP

This page allows the network administrator to configure registration mode (e.g., Normal, Fixed or Forbidden) of GVRP (GARP VLAN Registration Protocol) for each GE port.

Such function can eliminate unnecessary network traffic and prevent any attempt to transmit information to unregistered users.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Profile Name** | Enter a name for the Switch. The purpose of name is used for identification.<br>It is useful when there are many VigorSwitch (same modes) devices connecting to Vigor router. |
| **Enabled** | Switch the toggle to enable / disable the GVRP port setting. |
| **Dynamic VLAN Creation** | Switch the toggle to enable / disable the VLAN creation. |
| **Registration** | There are three modes to be specified.<br>**Normal** – Default setting. All packets can pass through the selected GE port.<br>**Fixed** – The selected GE port only sends static VLAN information to |

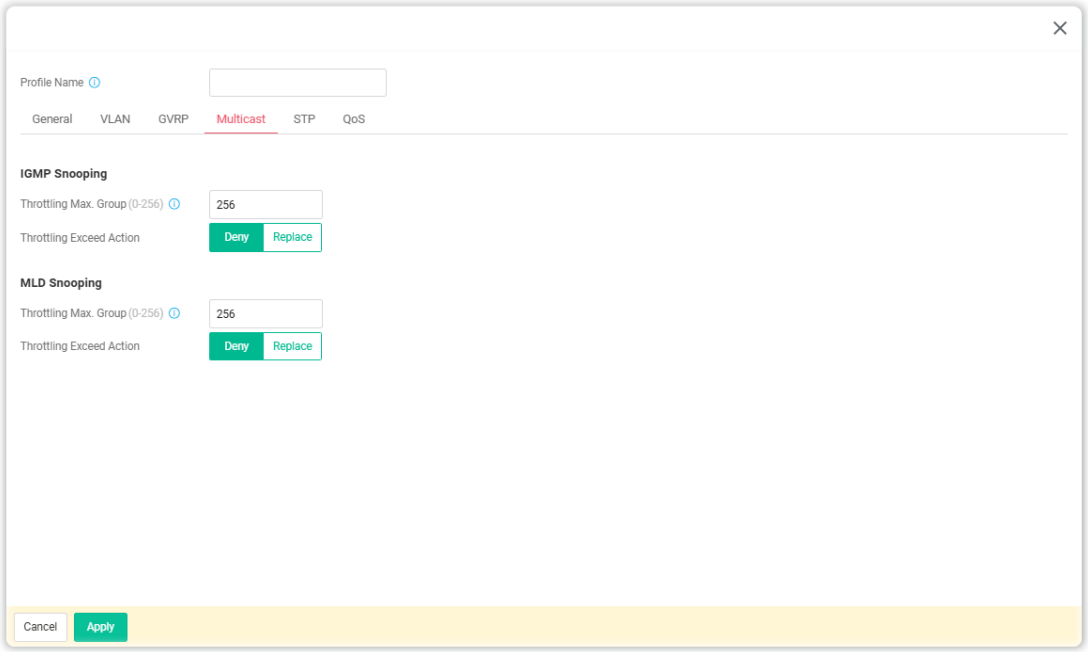
| | |
|---|---|
| | neighboring device and allows static VLAN packet to pass through.<br>**Forbidden** – The selected GE port only allows default VLAN packet to pass through. |
| **Cancel** | Discard current settings and return to the previous page. |
| **Apply** | Save the current settings and exit the page. |

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

## Multicast

**IGMP snooping** is the process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations the switch maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them and thus controls which ports receive specific multicast traffic.

**MLD snooping** does the same thing as IGMP snooping. The difference is that IGMP snooping acts on IPv4 packets; MLD snooping acts on IPv6 packets. MLD snooping is the process of listening to Multicast Listener Discovery network traffic. It can examine IPv6 packets and forward these packets to designate location via VLAN port members.




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Profile Name** | Enter a name for the Switch. The purpose of name is used for identification.<br>It is useful when there are many VigorSwitch (same modes) devices connecting to Vigor router. |
| | **IGMP Snooping** |
| **Throttling Max. Group** | Define the maximum number of IGMP group profile that a user on the switch can join. If "0" is selected, then such interface (port) can join all of the IGMP group profiles (defined in Filtering Profile). |
| **Throttling Exceed Action** | VigorSwitch will perform the action defined below when the number of IGMP join reports for the specified interface exceeds |

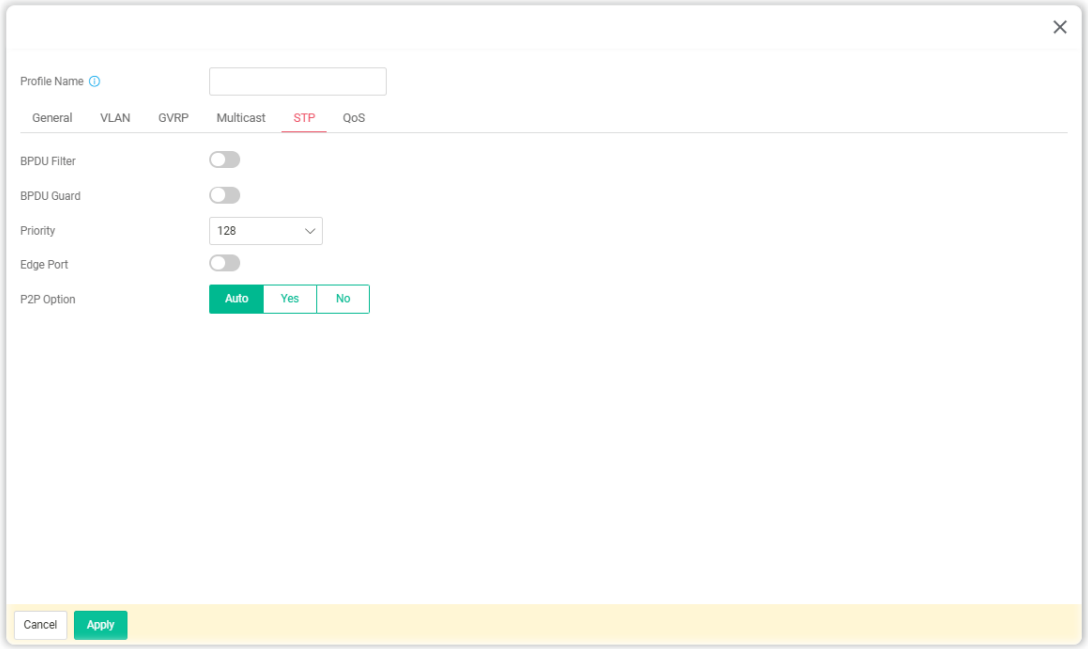
| | |
|---|---|
| | the value defined in Max Group.<br>**Deny** – It is default setting. The IGMP join report (for multicast service) received by such interface will be discarded.<br>**Replace** – When it is selected, a new group with IGMP report received will replace the existing group. |
| | **MLD Snooping** |
| **Throttling Max. Group** | Define the maximum number of MLD group profile that a user on the switch can join. If "0" is selected, then such interface (port) can join all of the MLD group profiles (defined in Filtering Profile). |
| **Throttling Exceed Action** | VigorSwitch will perform the action defined below when the number of MLD join reports for the specified interface exceeds the value defined in Max Group.<br>**Deny** – It is default setting. The MLD join report (for multicast service) received by such interface will be discarded.<br>**Replace** – When it is selected, a new group with MLD report received will replace the existing group. |
| **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.

## STP

The Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology for any bridged Ethernet local area network.

Bridge Protocol Data Units (BPDUs) are frames that contain information about the Spanning Tree Protocol (STP). Switches send BPDUs using a unique MAC address from its origin port and a multicast address as destination MAC (01:80:C2:00:00:00, or 01:00:0C:CC:CC:CD for Per VLAN Spanning Tree).




Available settings are explained as follows:

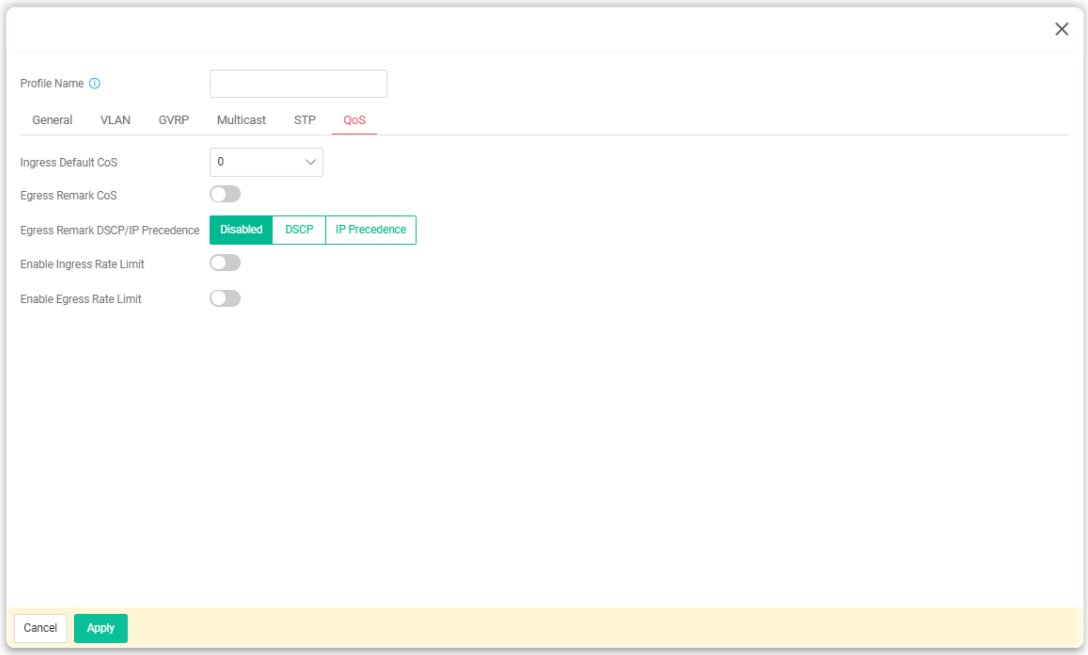
| Item | Description |
|---|---|
| **Profile Name** | Enter a name for the Switch. The purpose of name is used for |

| | |
|---|---|
| | identification.<br>It is useful when there are many VigorSwitch (same modes) devices connecting to Vigor router. |
| **BPDU Filter** | Switch the toggle to enable / disable the function of dropping all BPDU packets and no BPDU will be sent. |
| **BPDU Guard** | BPDU Guard further protects your switch by turning this port into error state and shutdown if any BPDU received from this port. Check it to enable such function.<br>Switch the toggle to enable/disable the BPDU Guard function. |
| **Priority** | Specify a priority value for the switch. The smaller the priority value, the higher the priority and greater chance of becoming the root. |
| **Edge Port** | In the Edge mode, the interface would be put into the Forwarding state immediately upon link up. If the edge mode is enabled for the interface and there are BPDUs received on the interface, the loop might be occurred in the short time before the STP state change.<br>Switch the toggle to enable / disable the function. |
| **P2P Option** | **Auto** – VigorSwitch determines the STP of link type for this port automatically.<br>**Yes** – It means the STP of link type on this port is full-duplex and directly connect to another switch or host.<br>**No** - It means the STP of link type on this port is “not” full-duplex and “does not” directly connect to another switch or host. |
| **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.

## QoS

This page is used to configure port settings for QoS. The configuration result for each port will be displayed on the table listed on the lower side of this web page.




Available settings are explained as follows:

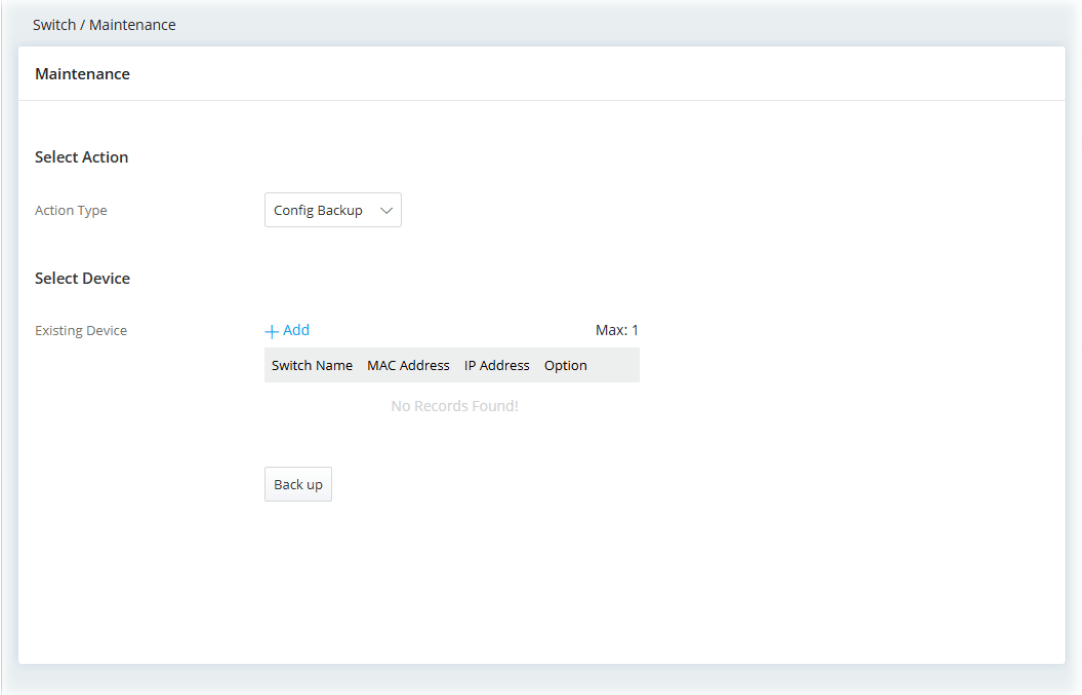
| Item | Description |
|---|---|
| **Profile Name** | Enter a name for the Switch. The purpose of name is used for identification.<br>It is useful when there are many VigorSwitch (same modes) devices connecting to Vigor router. |
| **Ingress Default CoS** | Specify the default CoS priority value for those ingress frames without given trust QoS tag (802.1q/DSCP/IP Precedence, depending on configuration). |
| **Egress Remark CoS** | Switch the toggle to enable/disable the function. |
| **Egress Remark DSCP/IP Precedence** | **Disabled** - Select to disable this function.<br>**DSCP** - Egress traffic will be marked with DSCP value according to the Queue to DSCP mapping table.<br>**IP Precedence** - Egress traffic will be marked with IP Precedence value according to the Queue to IP Precedence mapping table. |
| **Enable Ingress Rate Limit** | This page is used to configure port settings for QoS. The configuration result for each port will be displayed on the table listed on the lower side of this web page.<br>Switch the toggle to enable/disable the function.<br>**Ingress Rate Limit** - Enter the rate value (16-1000000), unit:16 Kbps. |
| **Enable Egress Rate Limit** | This page is used to configure port settings for QoS. The configuration result for each port will be displayed on the table listed on the lower side of this web page.<br>Switch the toggle to enable/disable the function.<br>**Egress Rate Limit** - Enter the rate value (16-1000000), unit:16 Kbps. |
| **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-6-4 Maintenance

Vigor router can backup, restore, reboot, or reset the managed Vigor switch devices.



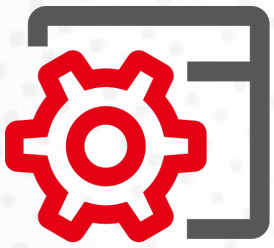

Available settings are explained as follows:

| Item | Description |
|---|---|
| | **Selection Action** |
| **Action Type** | There are four types of action that can be performed on Vigor switch by Vigor router.<br>**Config Backup** – Backup current configuration of Vigor switch.<br>**Config Restore** – Restore the configuration of Vigor switch with backup file.<br>**Remote Reboot** – Reboot the Vigor switch remotely by Vigor router.<br>**Factory Reset** – Reset the Vigor switch remotely by Vigor router. |
| | **Select Device** |
| **Existing Device** | **+Add** – Click to add a new device that will be applied with the settings configured above.<br>At present, only one device can be added in this field.<br>For the Action Type set as **Config Backup**:<br>• **Backup** – Click to make a backup copy for the current configurations of the selected device(s) (listed on Existing Device list).<br>For the Action Type set as **Config Restore**:<br>•  - Click to locate the backup file for restoring. |

| | |
|---|---|
| | • **Restore** - Click to restore the configuration of the selected device(s) (listed on Existing Device list) with the backup file.<br>For the Action Type set as **Remote Reboot**:<br>• **Reboot** – Click to reboot the remote switch (managed by Vigor router) with current configuration.<br>For the Action Type set as **Factory Rest**:<br>• **Reset** – Click to reset the selected device(s) (listed on Existing Device list) with the factory default switch settings. |

This page is left blank.

# 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 and Reboot System, and Firmware Upgrade.

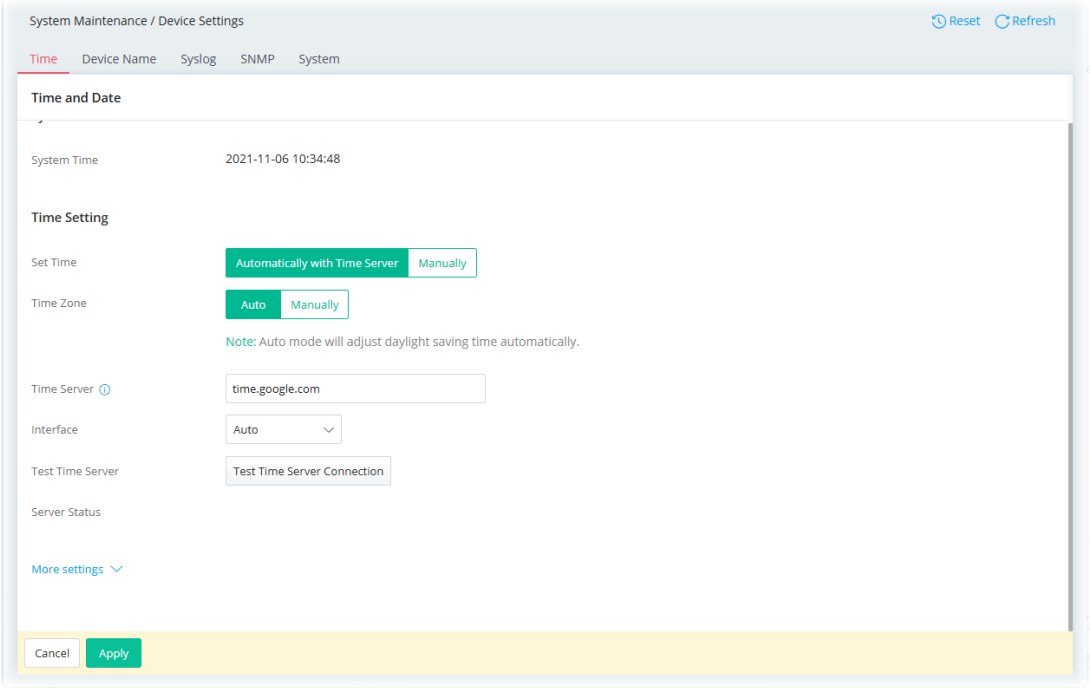
## III-1-1 Device Settings

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

### III-1-1-1 Time

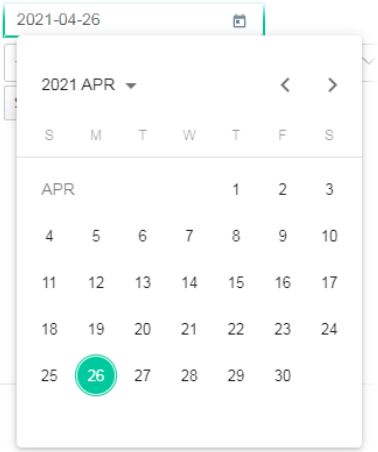
Open **System Maintenance>>Device Settings** and click the **Time** tab.

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




Available parameters are explained as follows:

| Item | Description |
|---|---|
| | **Time Setting** |
| **Set Time** | Determine the method (automatically or manually) to set the time.<br>**Automatically with Time Server** - Set the system time by retrieving time information from the specified network time server using the Network Time Protocol (NTP).<br>**Manually** - Set the system time using the time reported by the web browser. |
| **When Automatically with Time Server is** | **Time Zone** - Select the time zone (Auto or Manually) where the router is located. |

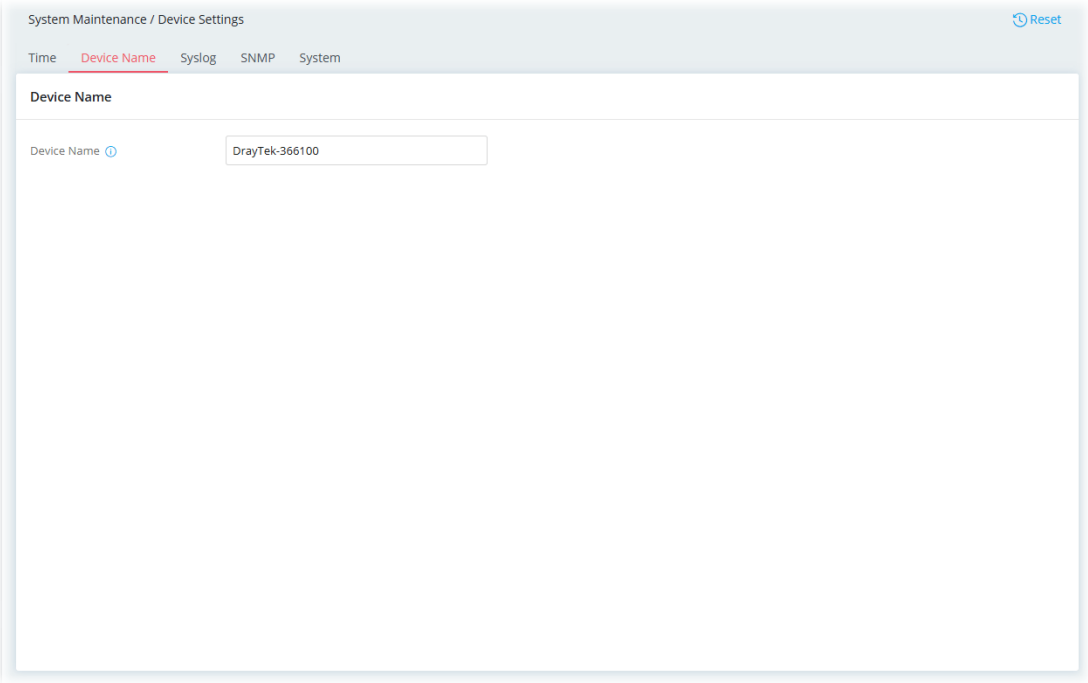
| | |
|---|---|
| selected as Set Time | **Time Server** - Enter the web site of the primary time server.<br>**Interface** - Renew the time through the selected WAN/LAN interface. If Auto is selected, the Vigor system will renew the time through WAN or LAN.<br>**Test Time Server** – Click the **Test Time Server Connection** button to test if the time server works well.<br>**Server Status** - Displays last update time status.<br>**More Settings** - Click to open advanced settings for the time server.<br>● **Auto Update Interval** - Select the time interval (e.g., 30min or 60min) at which the router updates the system time periodically.<br>● **Secondary Server** - For having a backup time server, please enter the URL/IP address in the field of Secondary Server.<br>● **Secondary Interface** - Renew the time through the selected WAN/LAN interface. If Auto is selected, the Vigor system will renew the time through WAN or LAN. This is an optional setting and is used as the interface for the backup time server. If the primary time server fails to renew the time setting, the Vigor system will use the secondary time server instead.<br>● **Daylight Saving** – It is available when **Manually** is selected as Time Zone. Switch the toggle to enable or disable the function. Enable Daylight Saving Time (DST) if it is applicable to your location if Manually) is selected as Time Zone.<br>● **Daylight Saving Period** - It is available when Daylight Saving is enabled. Specify the starting time and the ending time if "by Week" or "by Date" is selected. |
| When Manually is selected as Set Time | **Date -** Use the drop-down calendar to specify correct date.<br><br>**Time -** Set the time by specifying hours, minutes, and seconds.<br>**Synchronize with Browser** - 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 router name. Change the name if you want.

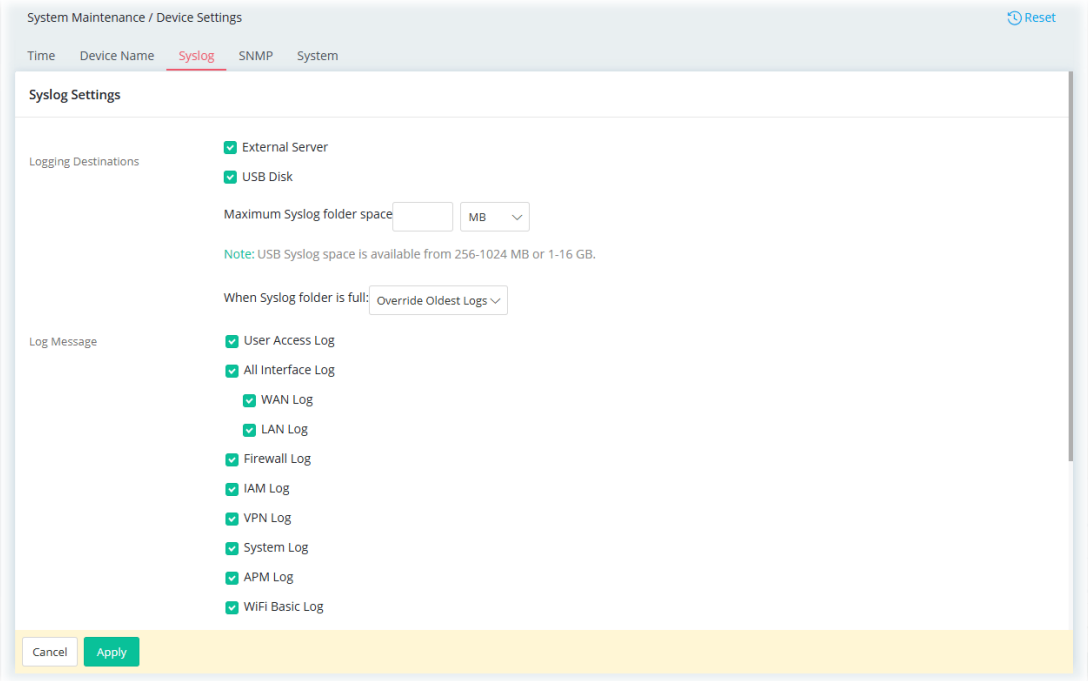
Open **System Maintenance>>Device Settings** and click the **Device Name** tab.




## III-1-1-3 Syslog

SysLog function is provided for users to monitor the router.

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




Available parameters are explained as follows:

| Item | Description |
| --- | --- |
| | Syslog Settings |
| Logging Destinations | **External Server** - Select to set Log Message item(s) and configure Syslog Servers.<br>**USB Disk** - Select to configure settings related to USB Disk.<br>**Maximum Syslog folder space** - Enter the number for the folder space.<br>In which, set the number ranges from 256 – 1024 for MB, and 1 – 16 for GB.<br>**When Syslog folder is full -** Select the action performed if the Syslog folder is full.<br>• Override Oldest Logs<br>• Stop when Full |
| 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.<br>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 (1-65535) of the Syslog Server. |
| Option | **Delete** - Click it to remove the selected server profile. |
| Apply | Save the current settings and exit the page. |
| Cancel | Discard current settings and return to the previous page. |

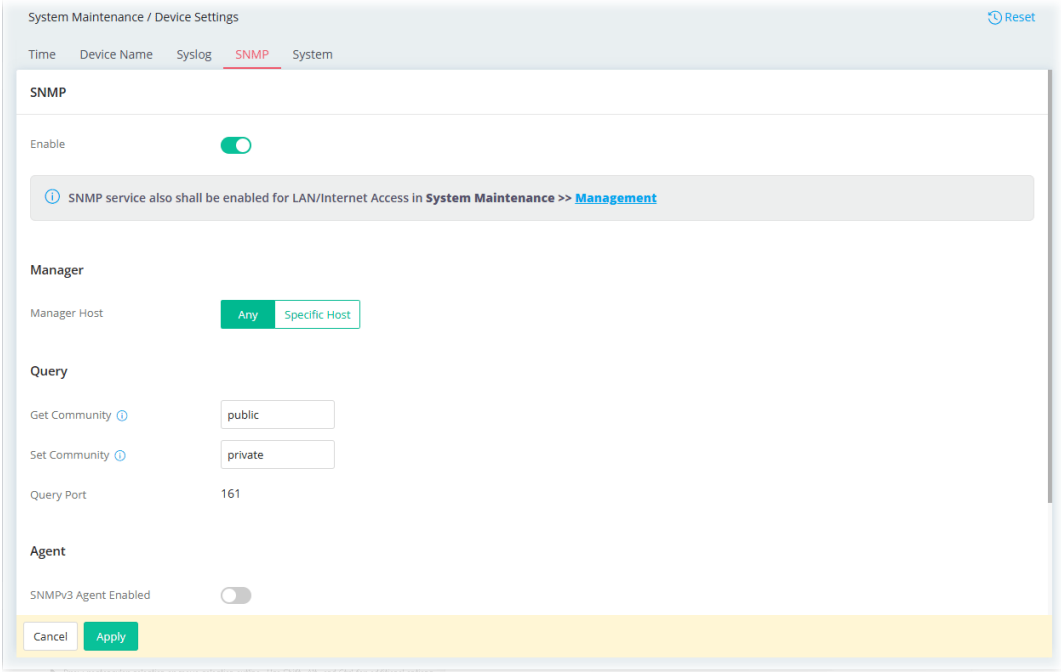
After finishing this web page configuration, please click **Apply** to save the settings.

## III-1-1-4 SNMP

This section allows you to configure settings for SNMP services.

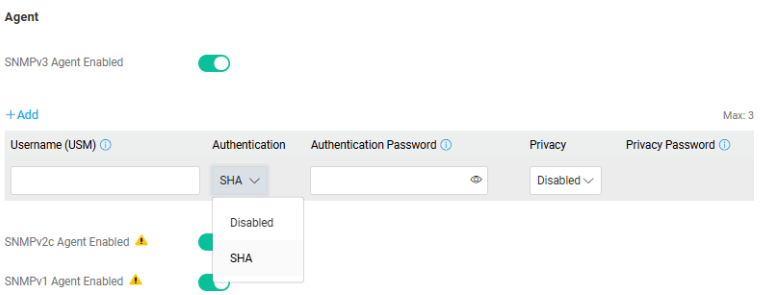
The SNMPv3 is more secure than SNMP through the use of encryption (supports AES and DES) and authentication (supports MD5 and SHA) for the management needs.

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



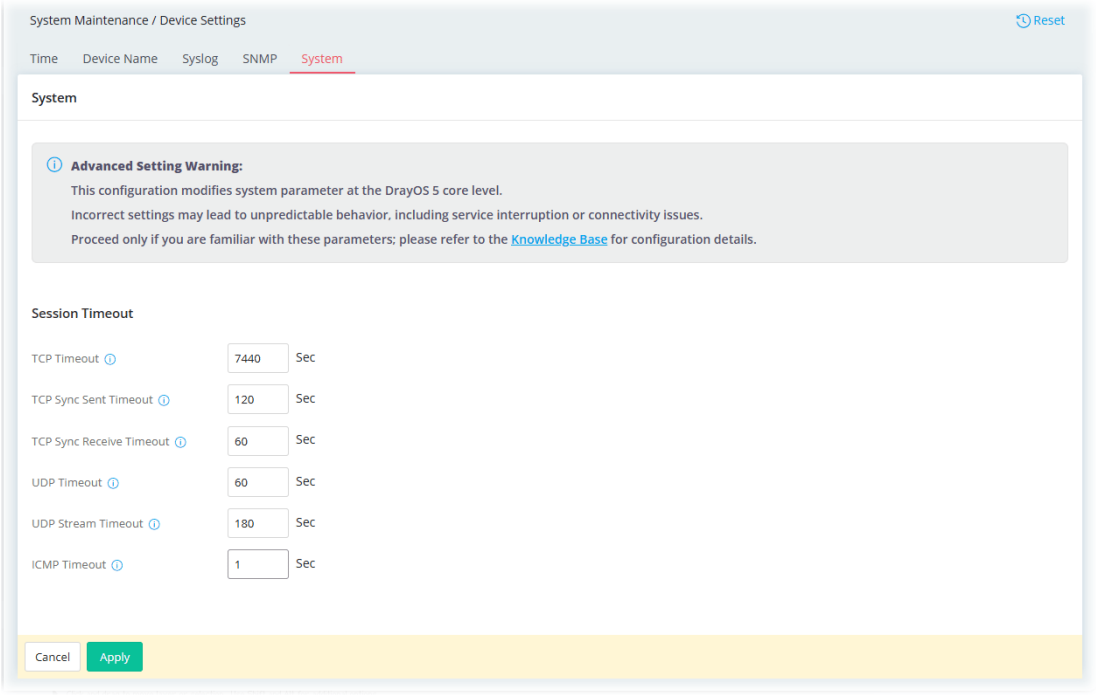

Available parameters are explained as follows:

| Item | Description |
|---|---|
| | **SNMP** |
| **Enable** | Switch the toggle to enable/disable the SNMP function.<br>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.<br>**Specific Host** - Specify a host (IPv4 or IPv6) or hosts (both IPv4 and IPv6).<br>• **IP Type** – Select Both, IPv4 or IPv6.<br>• **Specific Manager Host (IPv4/IPv6)** is available when IPv4/IPv6 is selected as the IP Type. Click **+Add** to have a new entry.<br>Enter the IPv4 address with subnet mask / IPv6 address with specified prefix length of hosts that are allowed to issue SNMP commands. If these fields 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. |
| **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. |
| **Query Port** | Displays the port number used by the query server. |
| | **Agent** |
| **SNMPv3 Agent Enabled** | Switch the toggle to enable/disable the SNMPv3 function.<br>If enabled, specify corresponding settings. Click **+Add** to have a new entry. |

| | |
|---|---|
| | <br>**Username(USM)** - USM means user-based security mode.<br>Enter the username to be used for authentication.<br>**Authentication** - Select one of the hashing methods to be used with the authentication algorithm.<br>**Authentication Password** - Enter a password for authentication.<br>**Privacy** - Select an encryption method as the privacy algorithm.<br>**Privacy Password** - Enter a password for privacy. |
| **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.<br>• **V1**<br>• **V2c**<br>• **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.<br>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.<br>• **Both**<br>• **IPv4**<br>• **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. |

## III-1-1-5 System

This section allows you to configure settings related to session timeout.



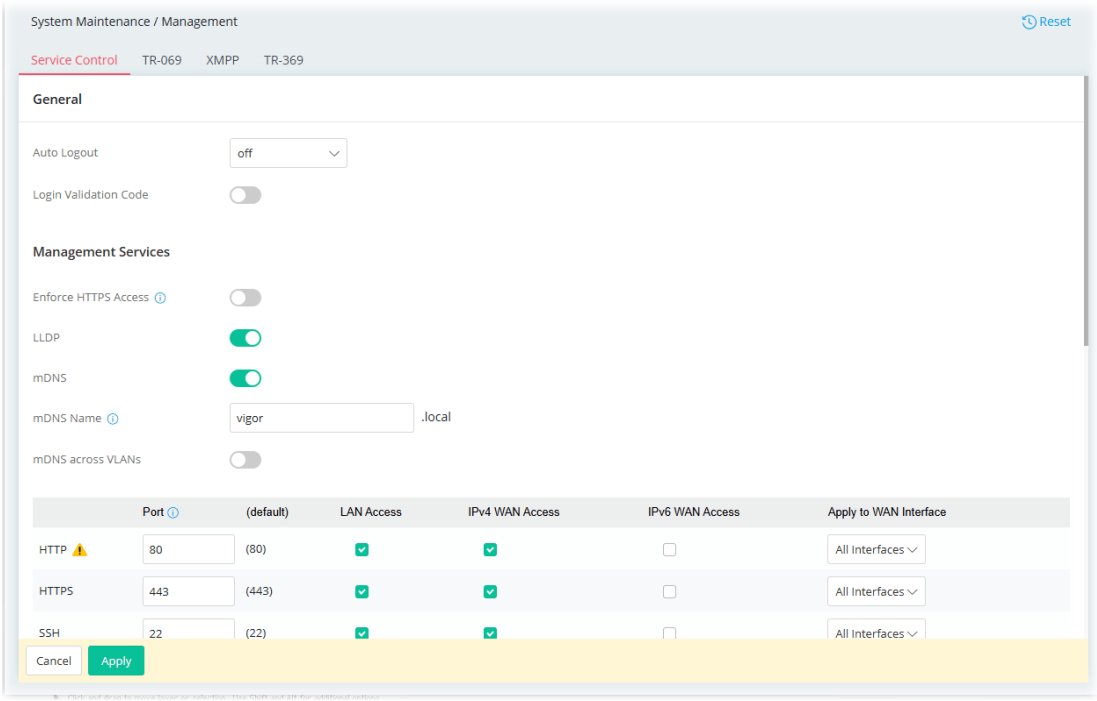

Available settings are explained as follows:

| Item | Description |
|---|---|
| TCP Timeout | Set the session retention time.<br>After the TCP completes the three-way handshake and the bidirectional data transmission, if no new packet comes in or out, the connection will be terminated when the time is up. |
| TCP Sync Sent Timeout | Set the TCP SYN Send Timeout.<br>Specifies how long the client waits for a SYN/ACK response after sending a SYN request. |
| TCP Sync Receive Timeout | Set the TCP SYN Receive Timeout.<br>Specifies the time the router waits for the client's ACK after replying with a SYN/ACK. |
| UDP Timeout | Set the UDP Timeout.<br>Specifies the duration for which the UDP packet remains valid while waiting for a response from the peer. |
| UDP Stream Timeout | Specifies the timeout applied to a UDP stream after bidirectional traffic is detected. |
| ICMP Timeout | Set the ICMP Timeout.<br>Specifies the session timeout for ICMP packets, such as ping and traceroute. |
| Cancel | Discard current settings. |
| Apply | Save the current settings and exit the page. |

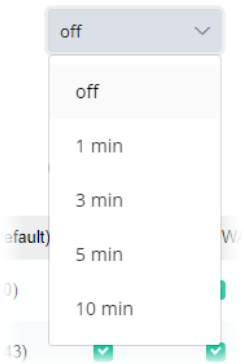
# III-1-2 Management

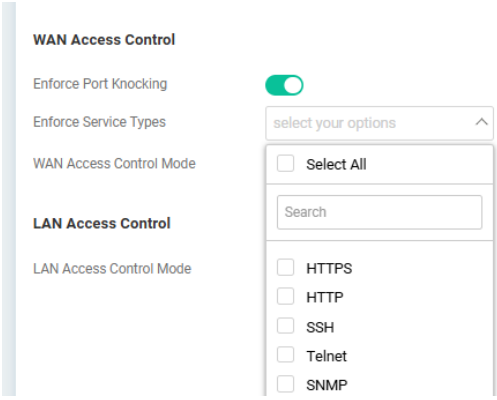
## III-1-2-1 Service Control

This page allows you to manage the general settings, management services, and TLS/SSL Encryption setup. After a user has been authenticated by means of a username and password, he or she can be granted Internet access, and optional firewall rules and WAN access policies can be applied.




Available settings are explained as follows:

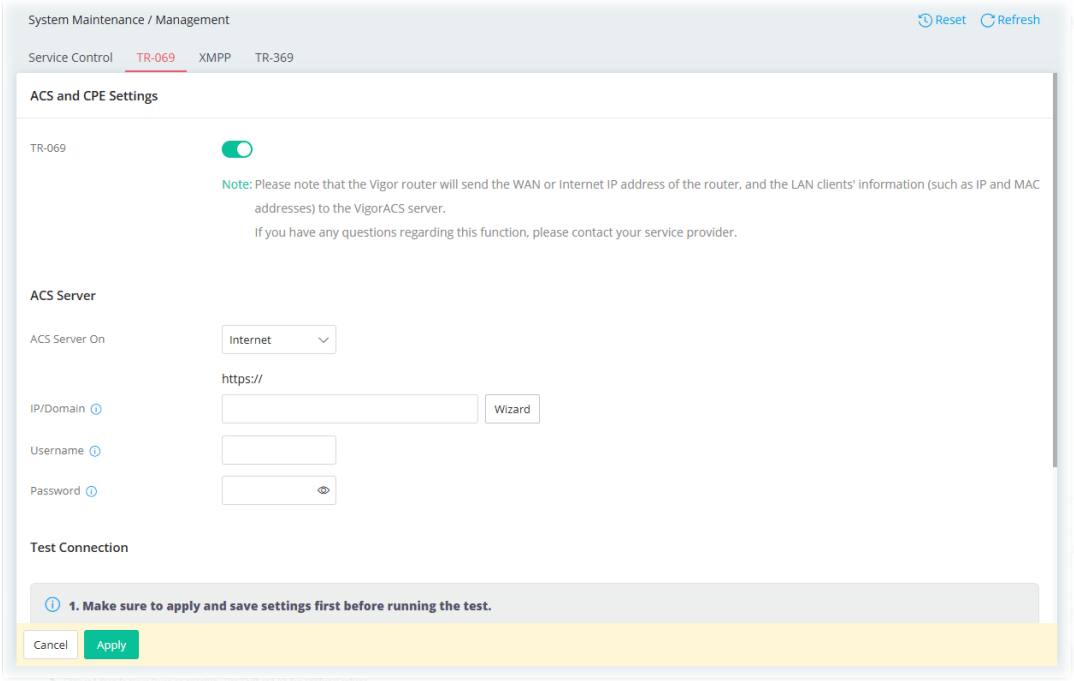
| Item | Description |
|---|---|
| | **General** |
| **Auto Logout** | If "off" is selected, the function of auto-logout for the web user interface will be disabled.<br>The web user interface will be open until you click the Logout icon manually.<br><br>The web page can be logged out according to the chosen condition. The default setting is off. Change the setting for your necessity. |
| **Login Validation Code** | Switch the toggle to enable/disable the feature of login validation |

| | |
|---|---|
| | code. |
| | **Management Services** |
| Enforce HTTPS Access | Switch the toggle to enable/disable the feature of allowing system administrators to login Vigor router via HTTPS. |
| LLDP | Switch the toggle to enable/disable the LLDP service. |
| 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. |
| mDNS across VLANs | Switch the toggle to enable/disable the function. |
| Port | Specify user-defined port numbers for the HTTP, HTTPS, SSH, Telnet and SNMP servers. |
| LAN Access | Select the checkbox to allow the system administrators to login from LAN interface. Later, configure the **LAN Access Control** below to determine who (the client) is able to access the LAN management services (HTTP, HTTPS, SSH, Telnet and SNMP). |
| IPv4/IPv6 WAN Access | Select the checkbox to allow the system administrators to login from IPv4/IPv6 WAN interface. Later, configure the **WAN Access Control** below to determine who (the client) is able to access the IPv4 WAN management services (HTTP, HTTPS, SSH, Telnet and SNMP). |
| | **TLS Encryption** |
| TLS 1.3/TLS 1.2 | Switch the toggle to enable or disable the function. |
| | **Access Control List** |
| WAN Access Control | In general, all the clients via WAN interface can access the IPv4 WAN management services (based on the HTTP, HTTPS, SSH, Telnet and SNMP checkboxes selected).<br>**Enforce Port Knocking** - Switch the toggle to enable/disable the Port Knocking function.<br>• **Enforce Service Types –** Select the service protocol(s). Only the source IP addresses that complete Port Knocking successfully will be permitted to access these selected services (from the WAN interface); all others will be denied.<br><br>**WAN Access Control Mode –** Select Allow All Connections or Allow List. Only the chosen IP objects/ IP groups / Keyword objects / country objects can access the services listed on this page via the WAN interface.<br>• **Allow All Connections** - The default is **Allow All Connections**.<br>• **Allow List** – Click **+Add** to have a new entry. The maximum number you can add is up to 6. |
| LAN Access Control | In general, all the clients via LAN interface can access the LAN |

| | |
|---|---|
| | management services (based on the HTTP, HTTPS, SSH, Telnet and SNMP checkboxes selected).<br>**LAN Access Control Mode** - Select **Allow All Connections** or Allow List. Only the chosen IP objects/ IP groups / Keyword objects / country objects can access the services listed on this page via the LAN interface.<br>• **Allow All Connections** - The default is **Allow All Connections**.<br>• **Allow List** - Click **+Add** to have a new entry. The maximum number you can add is up to 6. |
| Cancel | Discard current settings and return to the previous page. |
| Apply | Save the current settings and exit the page. |

## 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.




Available settings are explained as follows:

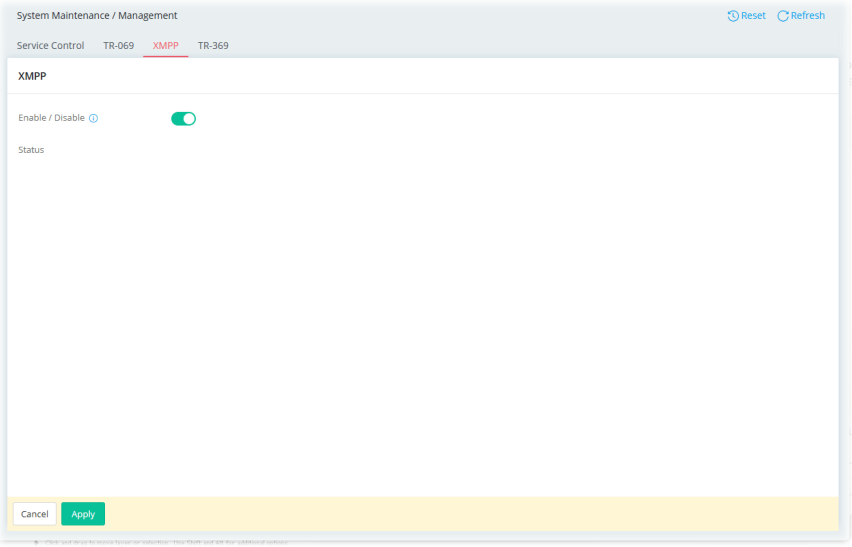
| Item | Description |
|---|---|
| TR-069 | Switch the toggle to enable or disable the function. |
| ACS Server | |
| ACS Server On | Choose the interface for connecting the router to the Auto Configuration Server. |
| IP/Domain | Enter the IP/domain for connecting to the ACS.<br>**Wizard** - Click it 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.<br>**Test With Inform** - Click it to send a message based on the event code selection to test if such CPE is able to communicate with VigorACS server. |
| More settings | |
| CPE Client | This section specifies the settings of the CPE Client.<br>**Protocol** - Select HTTPS if the connection is encrypted; otherwise select HTTP.<br>**Port** - In the event of port conflicts, change the port number of the CPE.<br>**Password** - Enter the password that the VigorACS will use to connect to the CPE. |
| Periodic Inform | **Enable / Disable** - Switch the toggle to enable or disable the |

| | |
|---|---|
| **Settings** | 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.<br>**Time Interval** - Set interval time or schedule time for the router to send notification to CPE. |
| **STUN Settings** | **Mode** - The default is **Auto**. If select **Enabled**, please enter the relational settings listed below:<br>• **Server Address** - Enter the IP address of the STUN server.<br>• **Server STUN Port** - Enter the port number (1-65535) of the STUN server.<br>• **Minimum Keep Alive Period** - If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the minimum period. The default setting is "60 seconds".<br>• **Maximum Keep Alive Period** - If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the maximum period. A value of "-1" indicates that no maximum period is specified. |
| **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 XMPP

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

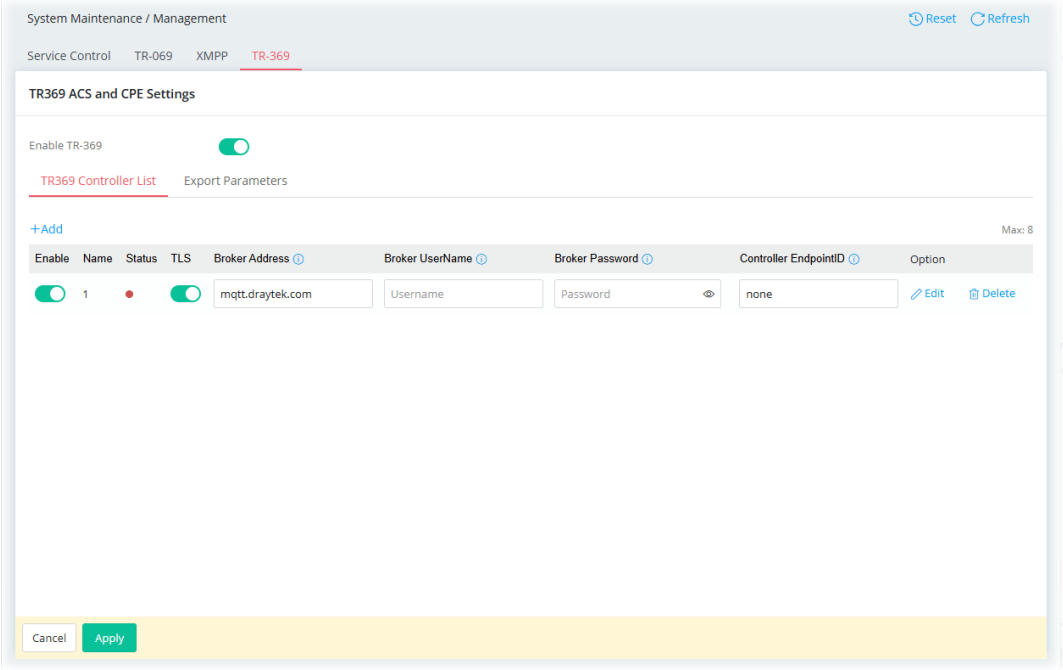



Switch the toggle of Enable/Disable to enable or disable the XMPP feature.

## III-1-2-4 TR-369

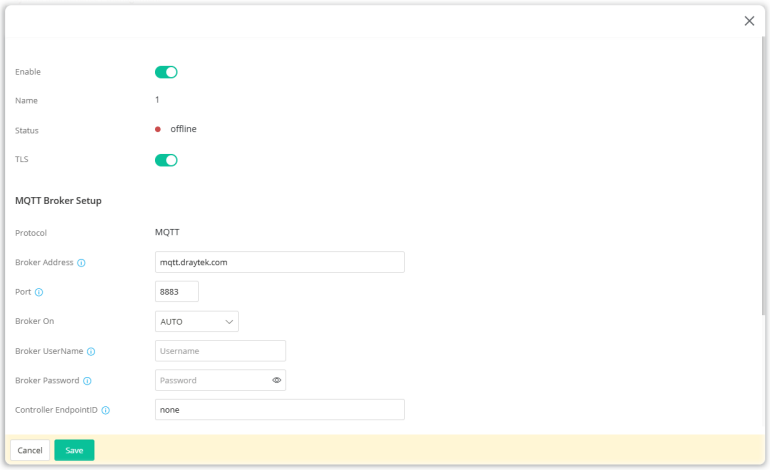
TR-369 is a management protocol that enables ISPs to remotely manage the router and its network services.

### TR369 Controller List




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Switch the toggle to enable or disable the TR-369 (USP) protocol settings. |
| **TLS** | Switch the toggle to enable or disable the TLS encryption mechanism. Ensure this remote management channel is secure. |
| **Broker Address** | Enter the IP address or hostname of the MQTT Broker provided by your ISP.<br>MQTT is the abbreviation of Message Queuing Telemetry Transport. |
| **Broker UserName** | Enter the broker's username from your ISP for MQTT connection authentication. |
| **Broker Password** | Enter the broker's password from your ISP for MQTT connection authentication. |
| **Controller EndpointID** | Enter the Endpoint ID of the USP Controller provided by your ISP.<br>The format is typically proto::identifier (e.g., proto::my-controller).<br>USP is the abbreviation of User Services Platform. |
| **Option** | **Edit** – Click to modify the detailed settings of the controller list. |




**Broker Address** – Display the IP address or hostname of the MQTT Broker. Change it if required.

**Port** – Enter a port number for the server.

**Broker On** – Specify an interface (LAN/WAN/AUTO) on your router to accept the MQTT Broker service.

**Broker UserName** – Display the broker's username from your ISP. Change it if required.

**Broker Password** – Display the broker's password from your ISP. Change it if required.

**Controller EndpointID** – Display the Endpoint ID of the USP Controller provided by your ISP. Change it if required.

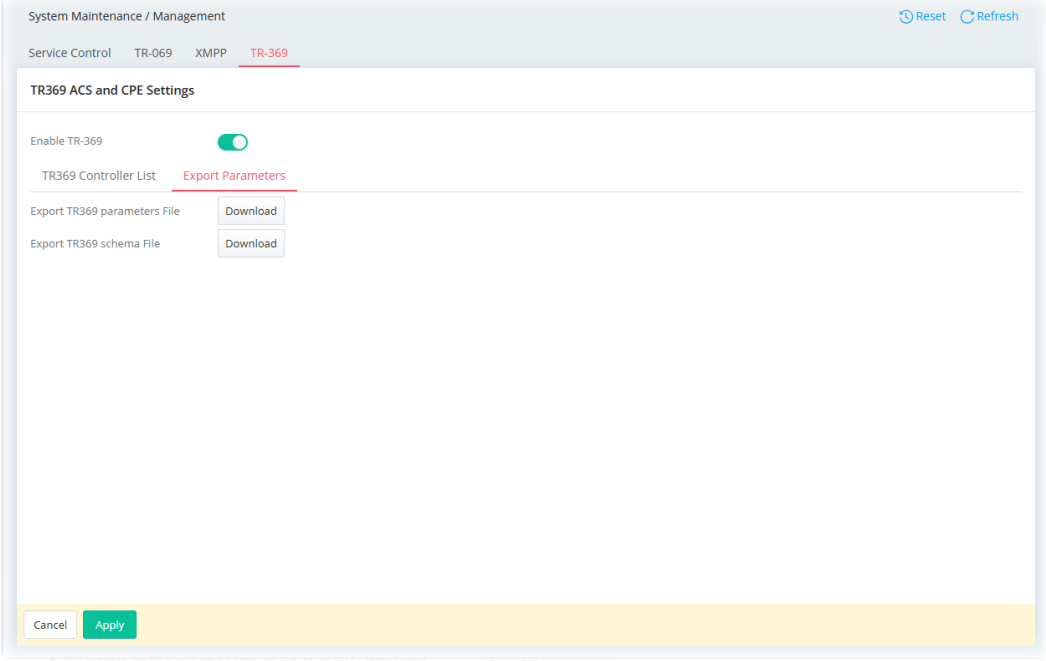
**Response Topic** – MQTT topic on which the USP Agent publishes response messages to the Controller. This value is defined by your ISP's deployment. Contact your ISP for the correct topic string.

**Controller Topic –** The MQTT topic the USP Agent subscribes to for receiving commands from the Controller. This value is defined by your ISP's deployment. Contact your ISP for the correct topic string.

**ACS UserName** – Optional. Most ACS servers do not require these credentials. If you are using VigorACS and credentials are required, contact your ISP or VigorACS administrator for the correct values.

**ACS Password** - Optional. Most ACS servers do not require these credentials. If you are using VigorACS and credentials are required, contact your ISP or VigorACS administrator for the correct values.

## Export Parameters




Available settings are explained as follows:

| Item | Description |
|---|---|
| **Export TR369 parameters File** | **Download –** Click to download current TR-369 parameters configuration as a file for storage, development or analysis by technicians. |
| **Export TR369 schema File** | **Download –**Click to download the TR-369 data model schema supported by the device. |

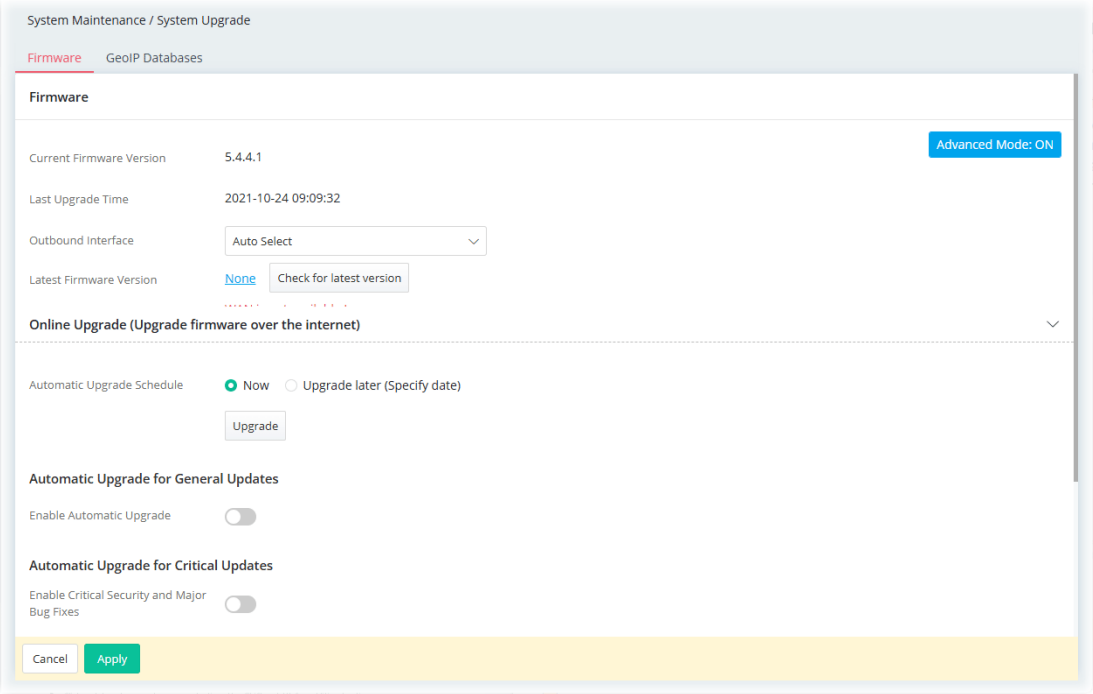
# III-1-3 System Upgrade

## III-1-3-1 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 router 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 router. This option is particularly beneficial for addressing critical security issues and fixing major bugs.



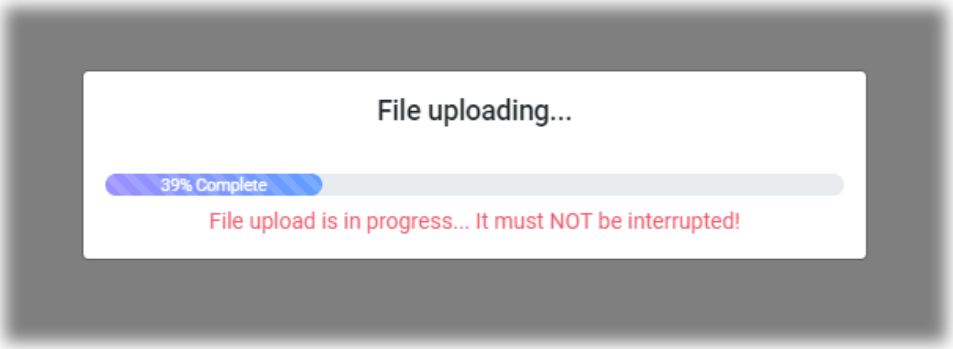

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Advanced Mode:ON/OFF** | Click to show or hide the advanced settings . |
| **Current Firmware Version** | Display the firmware version currently used. |
| **Outbound Interface** | It is available when the Advanced Mode is ON.<br>Select the WAN interface that will be used to download the firmware from the DrayTek website for automatic upgrade. Then select an IP or IP alias for the chosen WAN.<br>The default is **Auto Select.** |

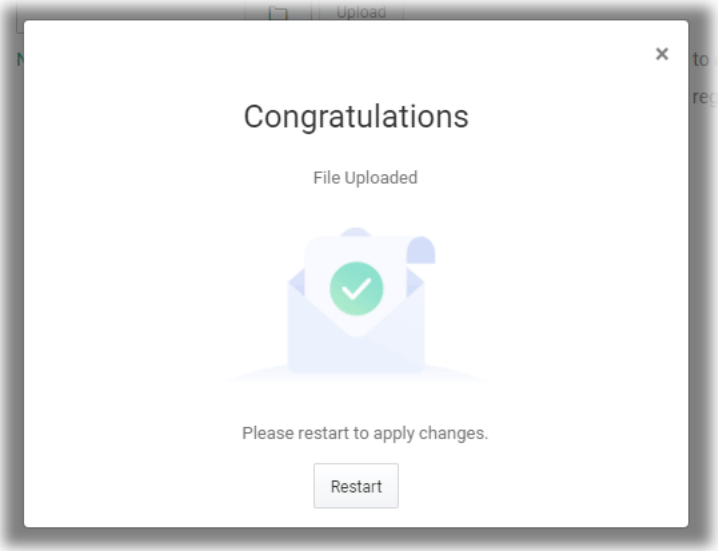
| | |
|---|---|
| Latest Firmware Version | **Check for latest version** – Click to find out if there is the latest firmware version from the DrayTek website. |
| Online Upgrade (Upgrade firmware over the Internet) | |
| Automatic Upgrade Schedule | Upgrade the firmware at a specified time and date.<br>**Now** – Select and click Upgrade to upgrade the firmware immediately.<br>**Upgrade later** – Specify a date and time to upgrade the firmware. |
| Automatic Upgrade for General Updates | |
| Enable Automatically Upgrade | Default is disabled.<br>Switch the toggle to enable/disable automatic firmware upgrade within a designated time. |
| Upgrade Schedule | Set the timing for the firmware upgrade.<br>**In the middle of the night** – The firmware upgrade will take place at midnight.<br>**Schedule Update** - The firmware upgrade will occur on a specific day and time each week. |
| Automatic Upgrade for Critical Updates | |
| Enable 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.<br>Default is disabled. Switch the toggle to enable/disable this feature. |
| Upgrade Schedule | Set the timing for the firmware upgrade.<br>**In the middle of the night** – The firmware upgrade will take place at midnight.<br>**Schedule Update** - The firmware upgrade will take place on a specified on one day and time in a week. |
| Local Upgrade (Upgrade firmware from a local life) | |
| Firmware for upload |  - Click to locate the firmware file for upgrade.<br>**Upload** – Click to upload the selected file onto Vigor system. |
| 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.

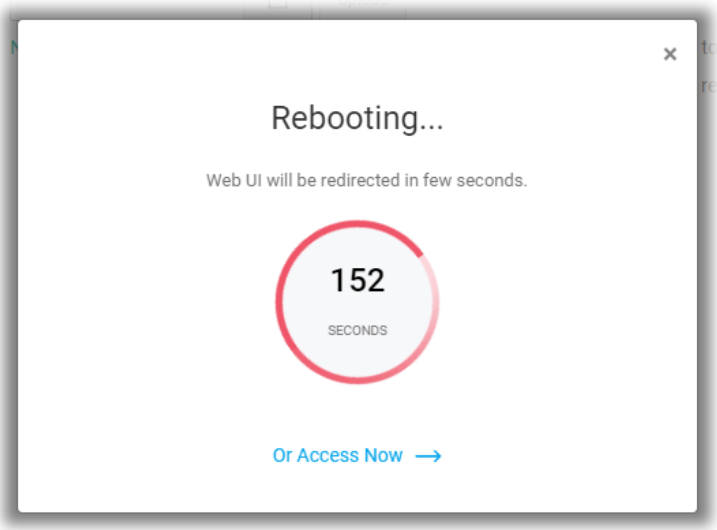
Then click **Upload** and wait for a few seconds.




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



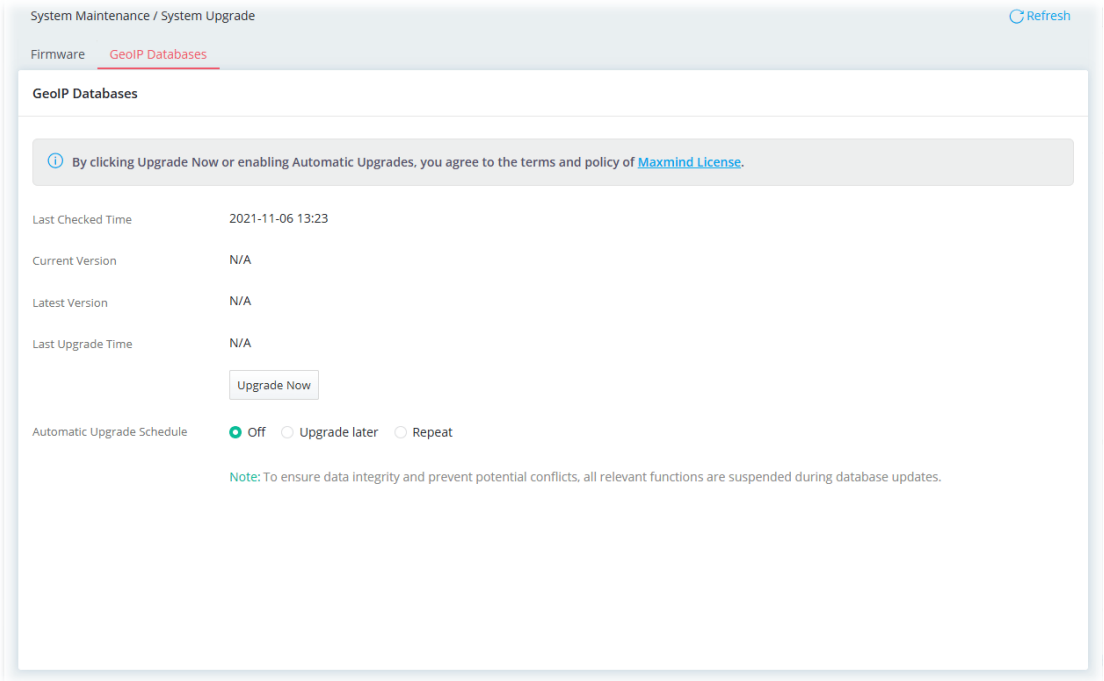

Wait for a while until the system finishes the rebooting.



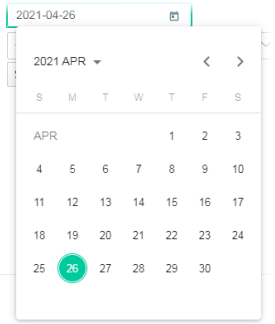

## III-1-3-2 GeoIP Database

GeoIP database provides information for Classless Inter-Domain Routing (CIDR) and location. Vigor router adopts the geographical distribution based on the GeoIP database offered by MaxMind.

If required, update the GeoIP database.

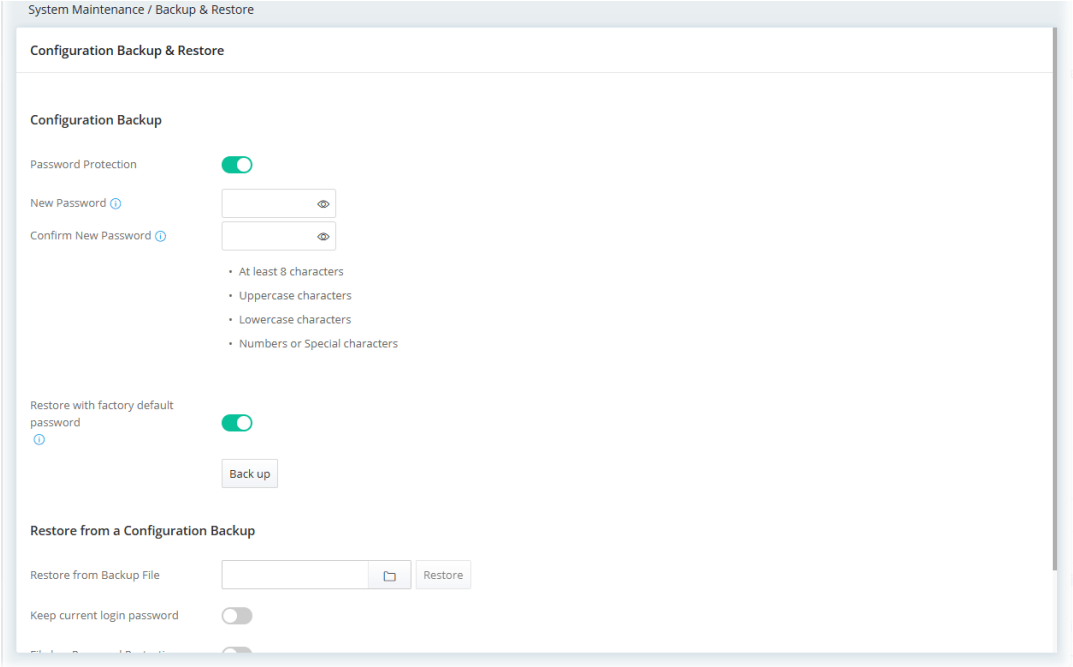



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Upgrade Now** | Click to upgrade the GeoIP database. |
| **Automatic Upgrade Schedule** | **Off –** There is no need to upgrade the database, even when a new version is available.<br>**Upgrade Later –** Allow to specify a time to upgrade the database.<br>● Start Date – Use the drop-down calendar to specify correct date.<br><br>● Start Time - Use the drop-down list to select the time.<br>**Repeat –** The system will check for any new version updates on the first day of every month.<br>● 1st of each month at - Use the drop-down list to select the time. |

# III-1-4 Backup & Restore

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



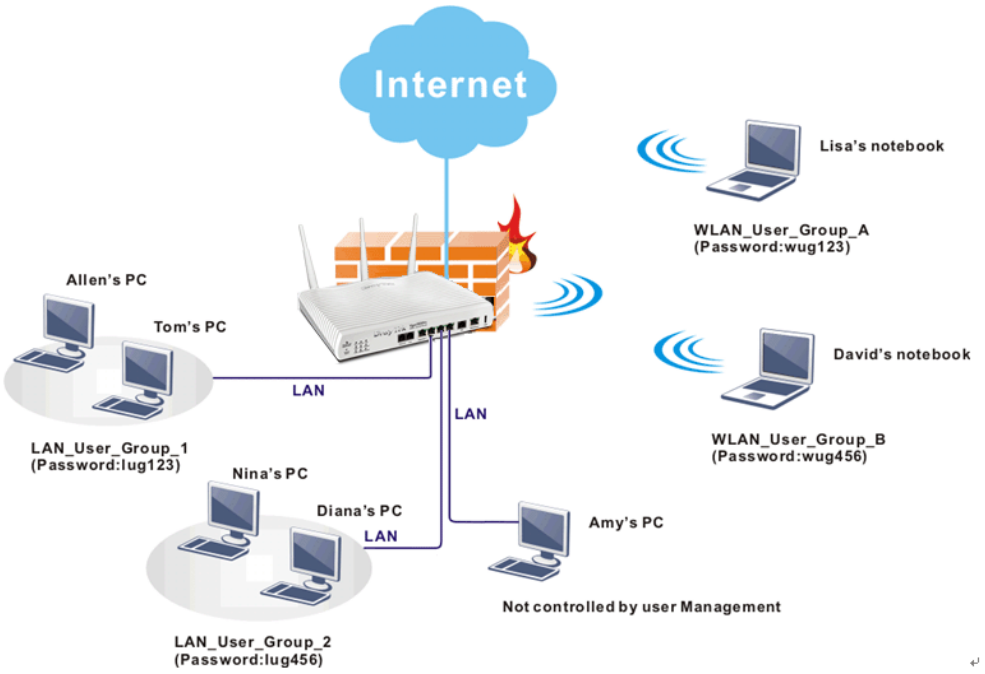

Available settings are explained as follows:

| Item | Description |
|---|---|
| | **Configuration Backup** |
| **Password Protection** | For the sake of security, the configuration file for the access point can be encrypted.<br>Switch the toggle to enable or disable the function. |
| **New Password/ Confirm New Password** | Enter several characters as the password for encrypting the configuration file. |
| **Restore with factory default password** | Switch the toggle to enable or disable the function.<br>After the restoration is complete, you can log in using the factory-default username and password. |
| **Back up** | Click it to backup the configuration file. |
| | **Restore from a Configuration Backup** |
| **Restore from Backup File** | - Click to locate the file for restoring.<br>**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.<br>**Restore Password -** Enter a password for configuration restoration. |

# III-1-5 Accounts & Permission

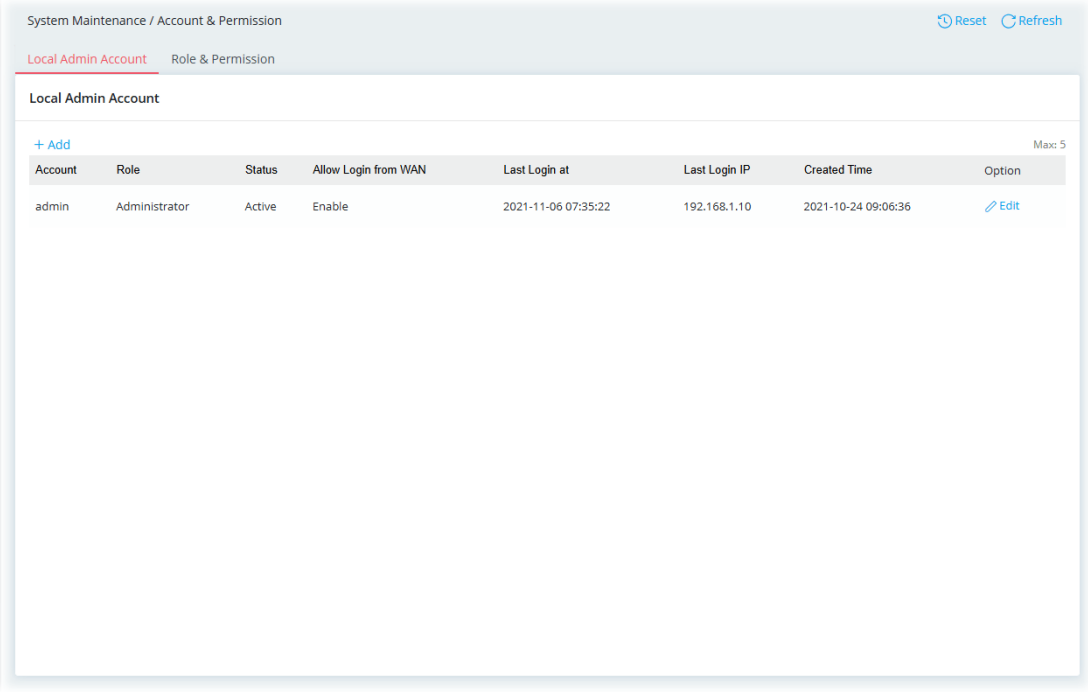
This page allows you to modify your current administration account and password.

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.



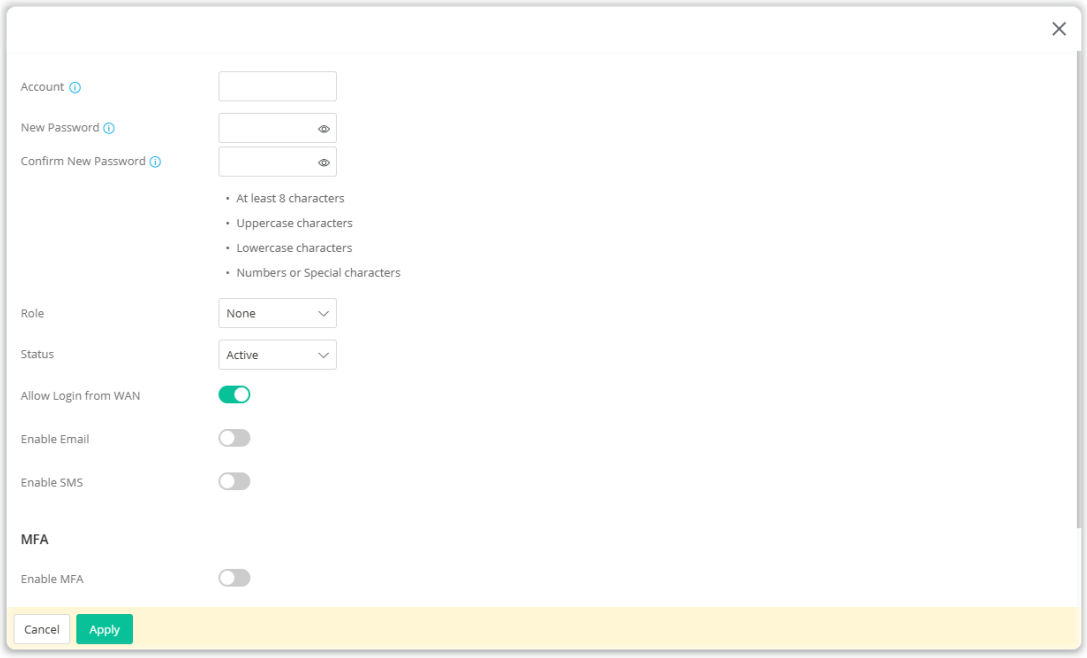

Available settings are explained as follows:

| 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**.




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. |
| **Confirm New Password** | Enter the new password again. |
| **Role** | Specify the role of the account.<br>• **Administrator**<br>• **Guest**<br>• **Users (created on the Role & Permission page)** |
| **Status** | **Active** - Enable the selected account profile.<br>**Inactive** - Disable the selected account profile. |
| **Allow Login from WAN** | It is available if "Router Management" is selected as the usage.<br>If enabled, the user can login from WAN by using this user account. |
| **Enable Email** | Switch the toggle to enable or disable the email setting.<br>**Email** – Enter the email address for receiving the MFA PIN code. |
| **Enable SMS** | Switch the toggle to enable or disable the SMS setting.<br>**SMS** - Enter the destination SMS number for receiving the MFA PIN code. |

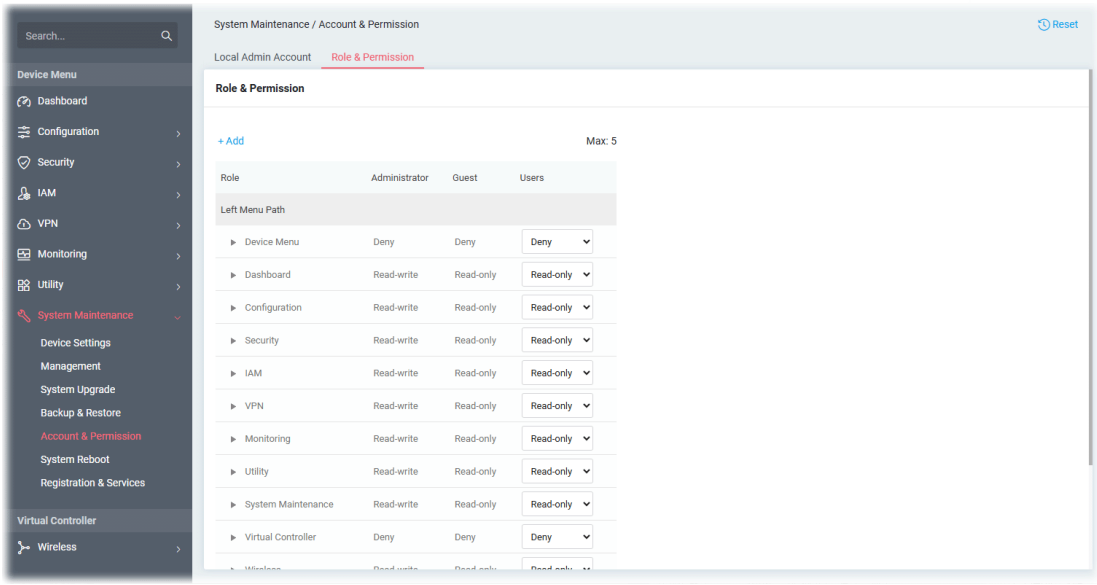
| MFA | |
|---|---|
| **Enable MFA** | Switch the toggle to enable/disable the function of Multi-Factor Authentication (MFA).<br>**Allowed MFA Method** - Select to require TOTP, Email, or SMS authentication when logging in to Vigor router.<br>**TOTP** – For the Time-based One-time Password (TOTP) mechanism, please make sure the time zone of your router is correct. Then, install Google Authenticator APP on your cell phone. Open the APP to scan the QR code on this page. A one-time password will be shown on your phone.<br><br>In the filed of Validation Code, enter the one-time password and click Verify.<br>Now, the configuration is finished. You will be asked to enter the 2FA code on the after passing the username and password authentication.<br>**SMS/Email** – The password will be transferred via the SMS and/or Mail profiles selected from User Information above. |
| **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.

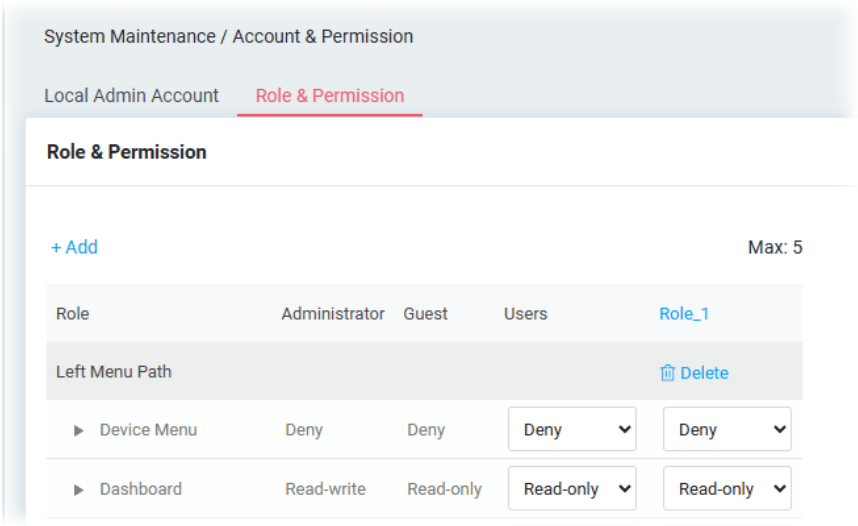
## III-1-5-2 Role & Permission

This page allows the creation of up to five roles which can be applied to the local admin account.

The default roles are Administrator, Guest and Users.

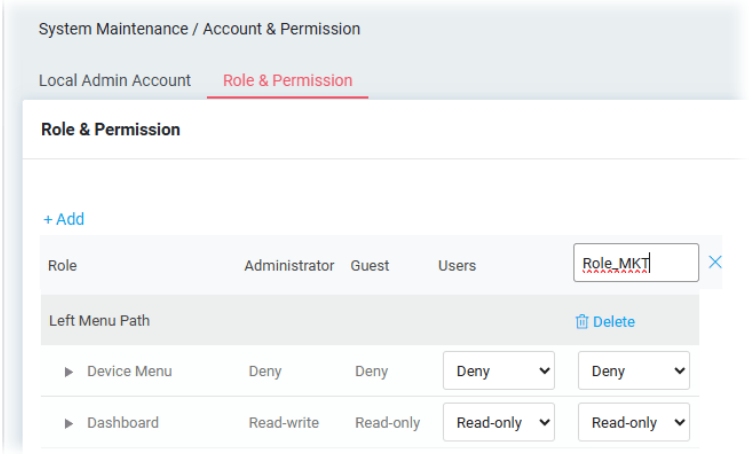
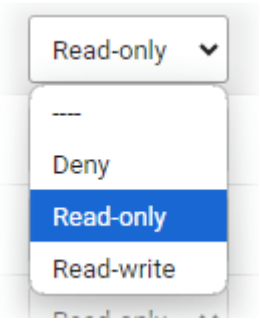



To create a new role profile, click **+Add**. A new role will be added on to the page.

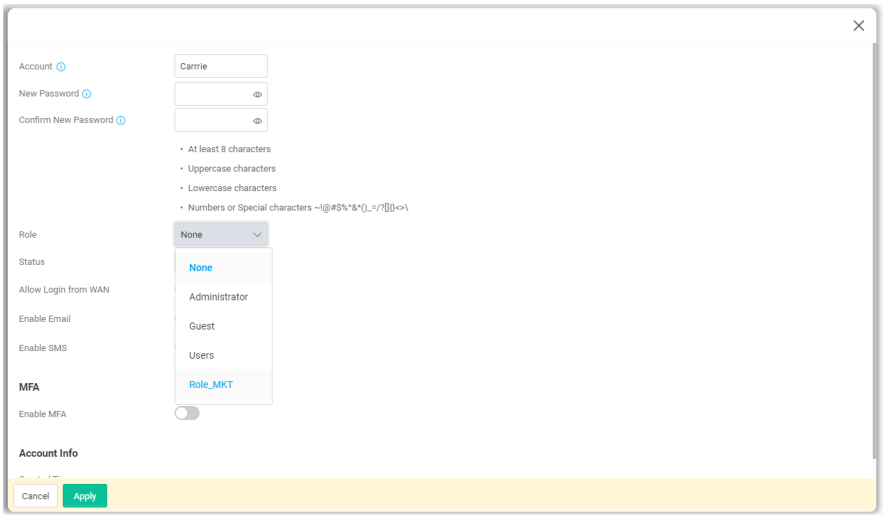



Available settings are explained as follows:

| 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). |

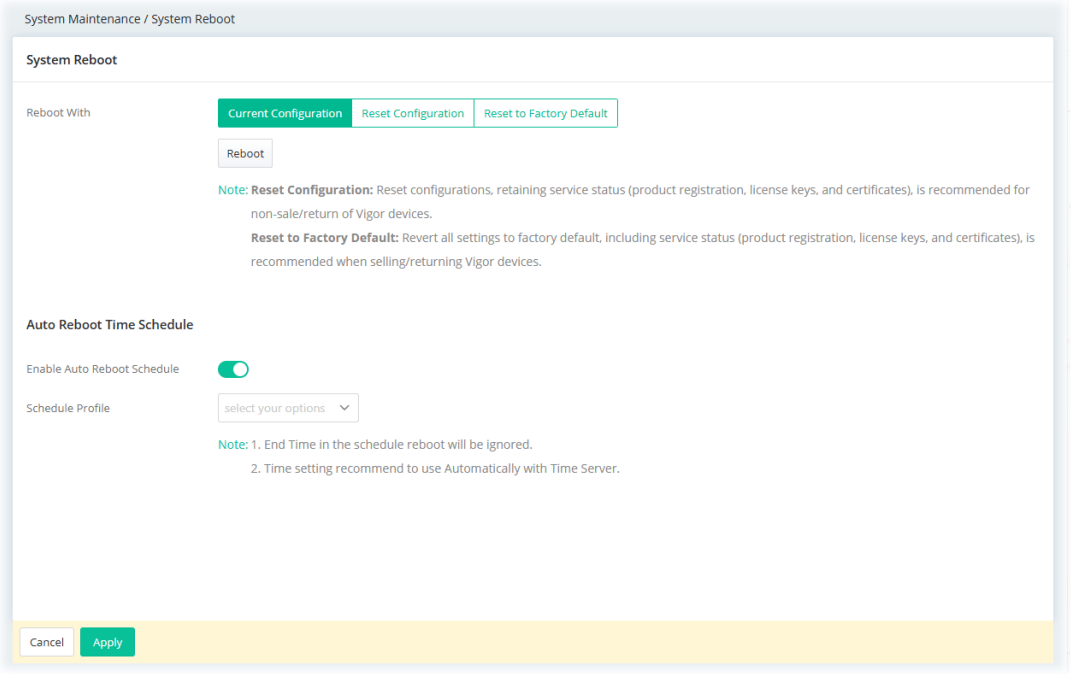
| | |
|---|---|
| |  |
| **Left Menu Path** | Lists all of the features that a role can have.<br>The role of **Administrator** has the highest authority for accessing Vigor router.<br>The role of **Guest/Users** has the lowest authority for accessing Vigor router.<br>The permissions for user-defined roles are based on read-only or read-write access granted to each menu path (such as dashboard, configuration, device menu, etc.) individually.. |
| **Delete** | Remove the selected user-defined role profile. |
|  | Specify the permission for each menu item for the user-defined role.<br>**Deny** - The permission for the menu item on the left side is not allowed for the user-defined role profile.<br>**Read-only** - The permission for the menu item on the left side allowed for the user-defined role profile to be read-only.<br>**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**.



# III-1-6 System Reboot

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

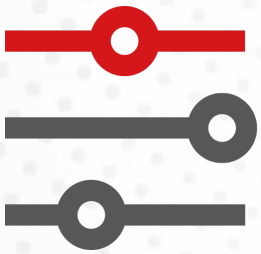



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Reboot With** | Select one of the following options, and press the **Reboot** button to reboot the router.<br>**Current Configuration** – Select this option to reboot the router using the current configuration.<br>**Reset Configuration** – Select this option to reset the router while retaining service status (product registration, license keys, and certificates).<br>**Reset to Factory Default** – Select this option to reset the router's configuration to the factory defaults before rebooting. |
| **Auto Reboot Time Schedule** | **Enable Auto Reboot Schedule** – Switch the toggle to enable or disable the function. If enabled, Vigor router will reboot automatically based on the schedule profile.<br>**Schedule Profile** – Use the drop-down list to select the profile(s). |

This page is left blank.

# Chapter IV Others

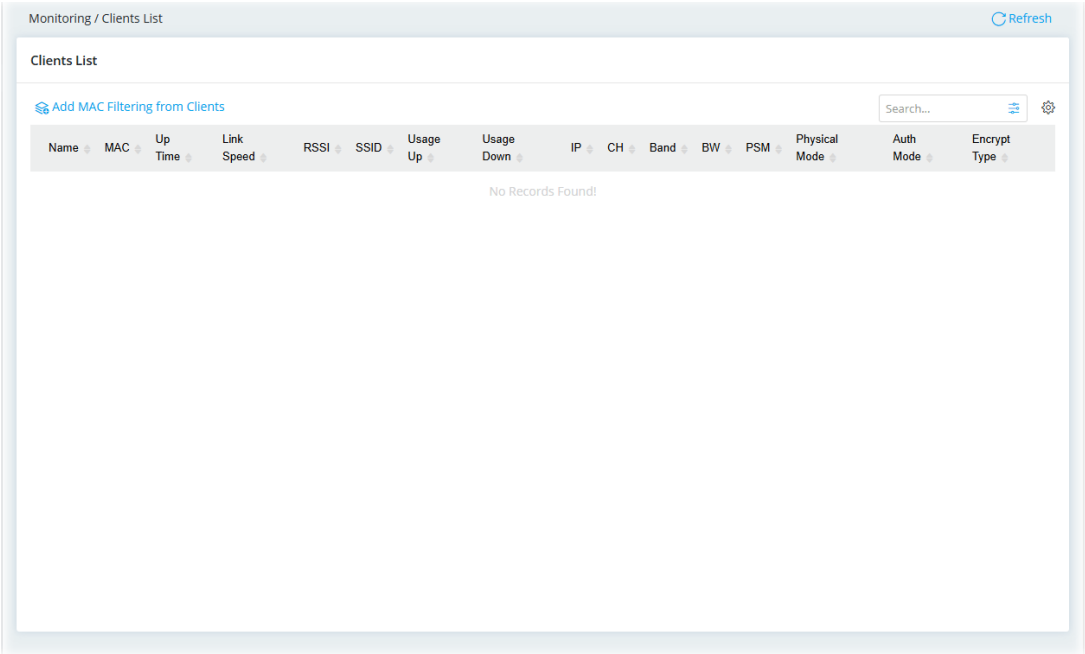


# IV-1 Monitoring

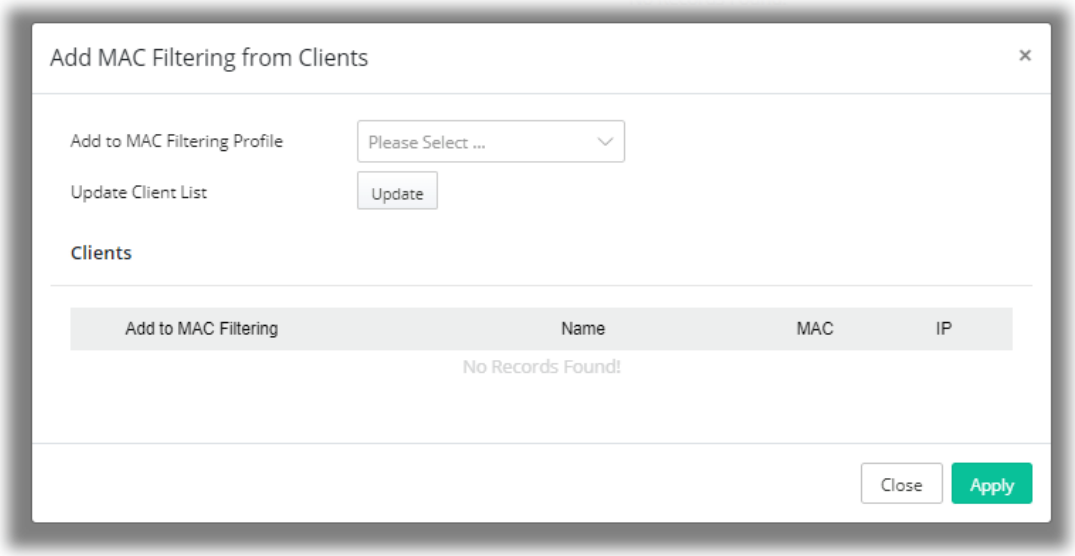
## IV-1-1 Clients List

Clients List displays the configuration status of the wireless clients that connect to the Vigor router via WiFi connection.

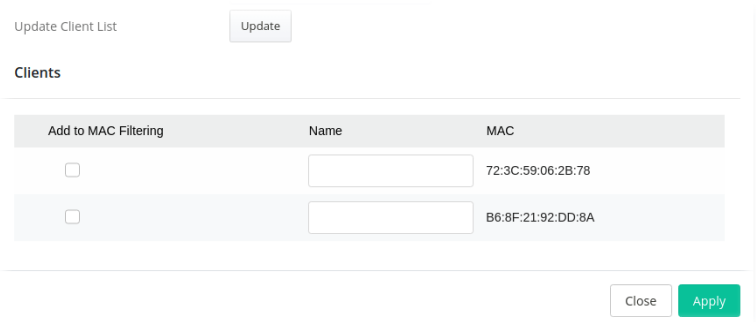
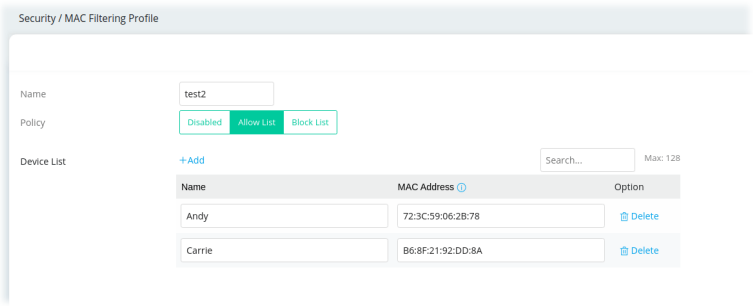
Besides, this page offers a quick method to add the wireless client to any existing MAC Filtering Profile.




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




Available settings are explained as follows:

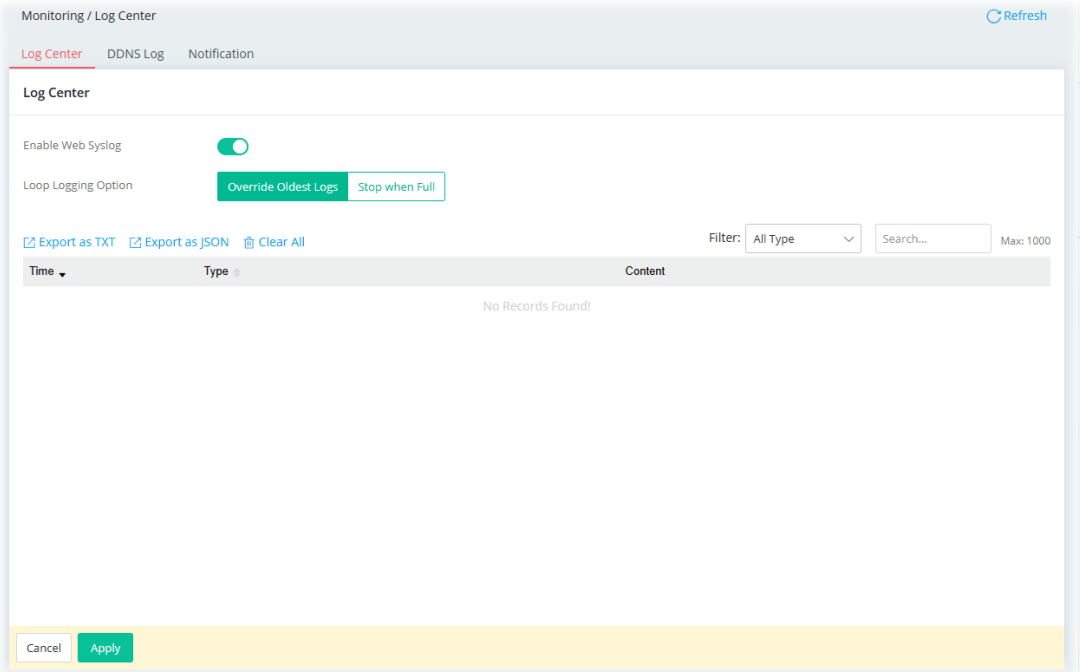
| Item | Description |
| --- | --- |
| **Add to MAC Filtering Profile** | Select one of the MAC filtering profiles (Security>>MAC Filtering Profile) as the filtering basis. |
| **Update Client List** | **Update** – Click to renew the client list based on the actual wireless connection.<br> |
| **Clients** | Displays the SSID name, MAC address, and IP address of the wireless clients.<br>**Add to MAC Filtering** – Select to make the wireless client join the MAC Filtering Profile set above.<br>**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.<br>To check if the new added wireless clients on the MAC Filtering profile or not, refer to Security>>MAC Filtering Profile.<br> |

Click **Apply** to save the settings.

# IV-1-2 Log Center

## IV-1-2-1 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.



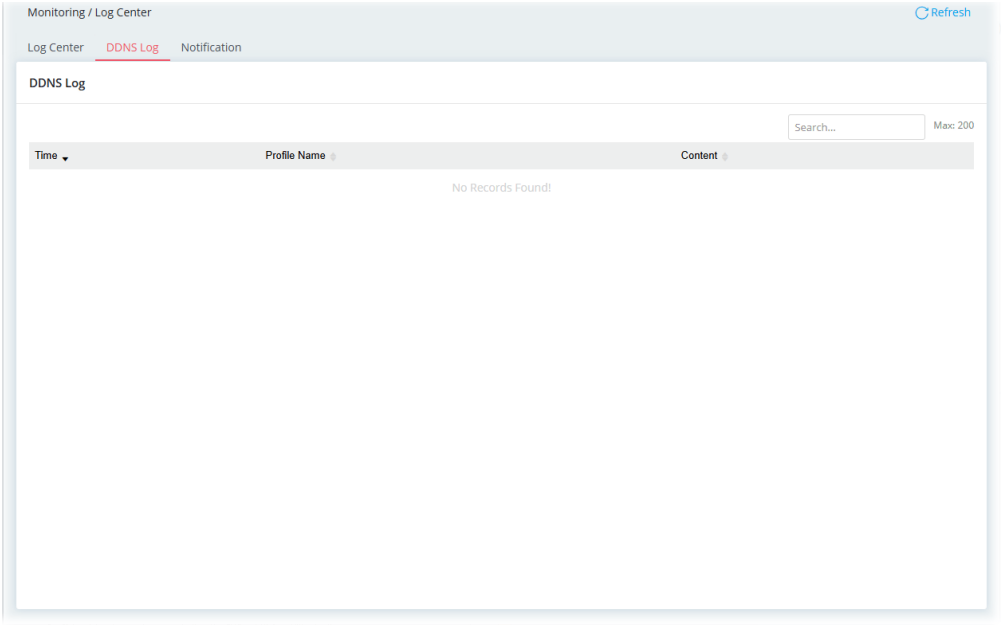

Available settings are explained as follows:

| Item | Description |
|---|---|
| **Enable Web Syslog** | Switch the toggle to enable or disable the function.<br>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.<br>**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-1-2-2 DDNS Log

This page displays the log (time, profile name and content) related to Dynamic DNS actions performed by this device.

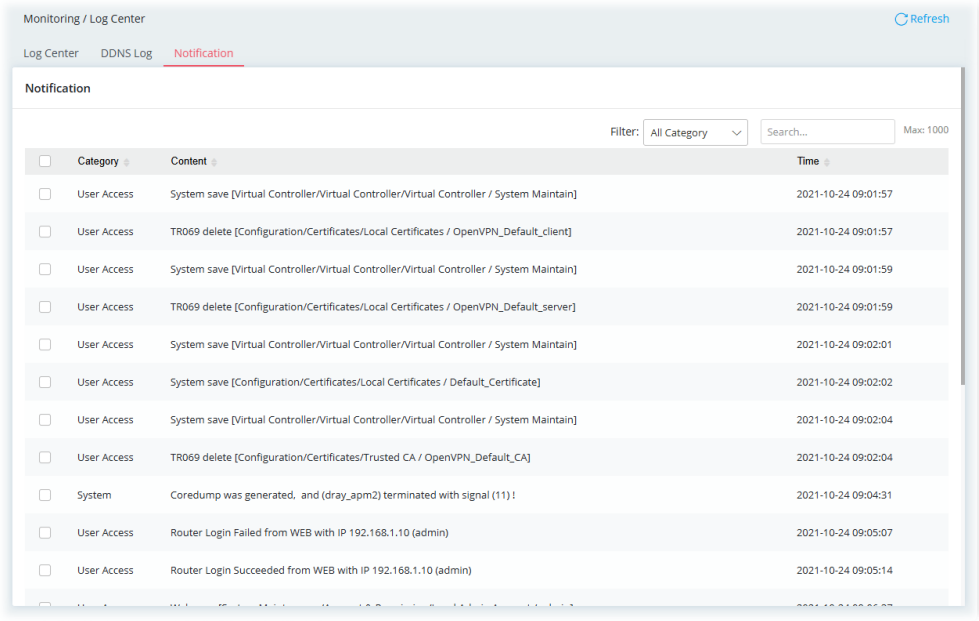



Click **Refresh** to reload this page with the most up-to-date information.

## IV-1-2-3 Notification

This page displays important log information, including:

- important message
- the notification of SSH/Telnet Login, Web Login
- the notification of the firmware upgrade status
- the notification of configuration convert (restoration or update)

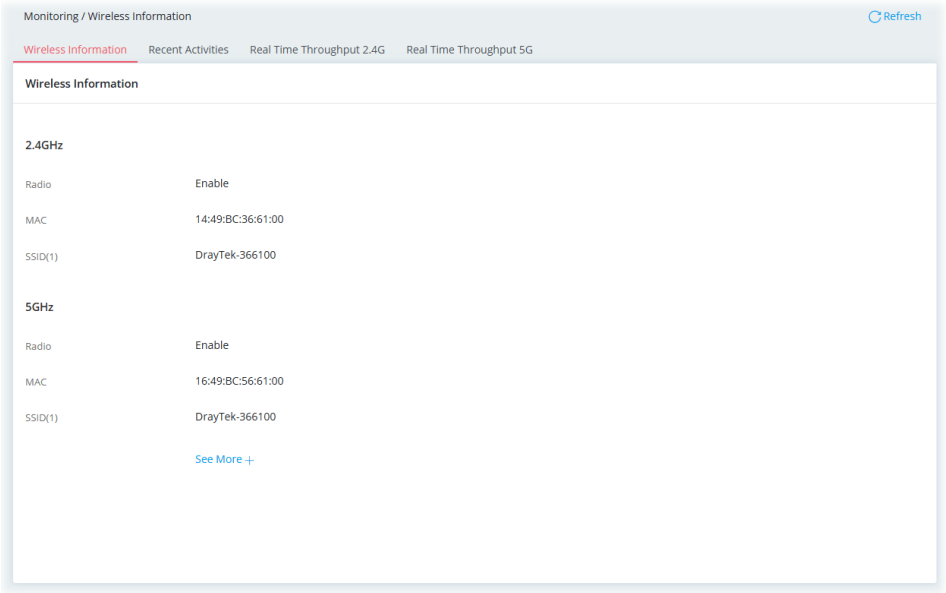


# IV-1-3 Wireless Information

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.

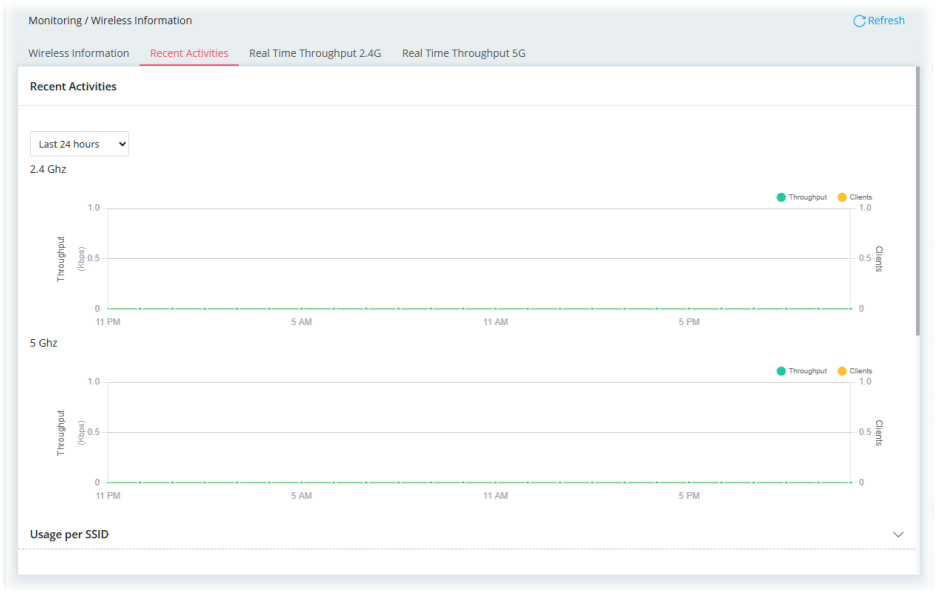



Click **Refresh** to reload this page with the most up-to-date information.

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

## IV-1-3-2 Recent Activities

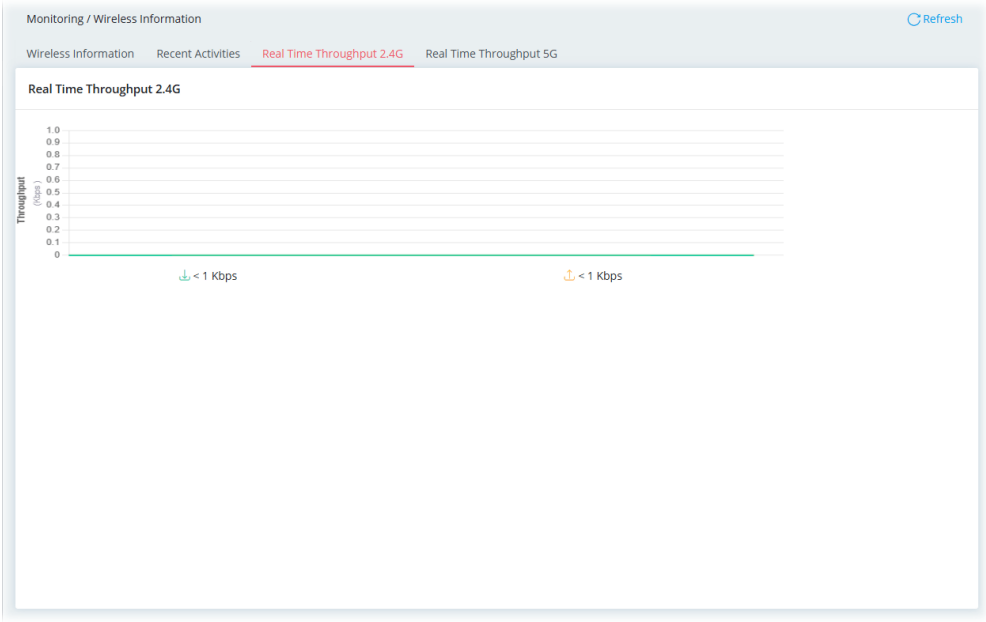
The activities regarding to wireless network can be shown with line graphs.




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

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

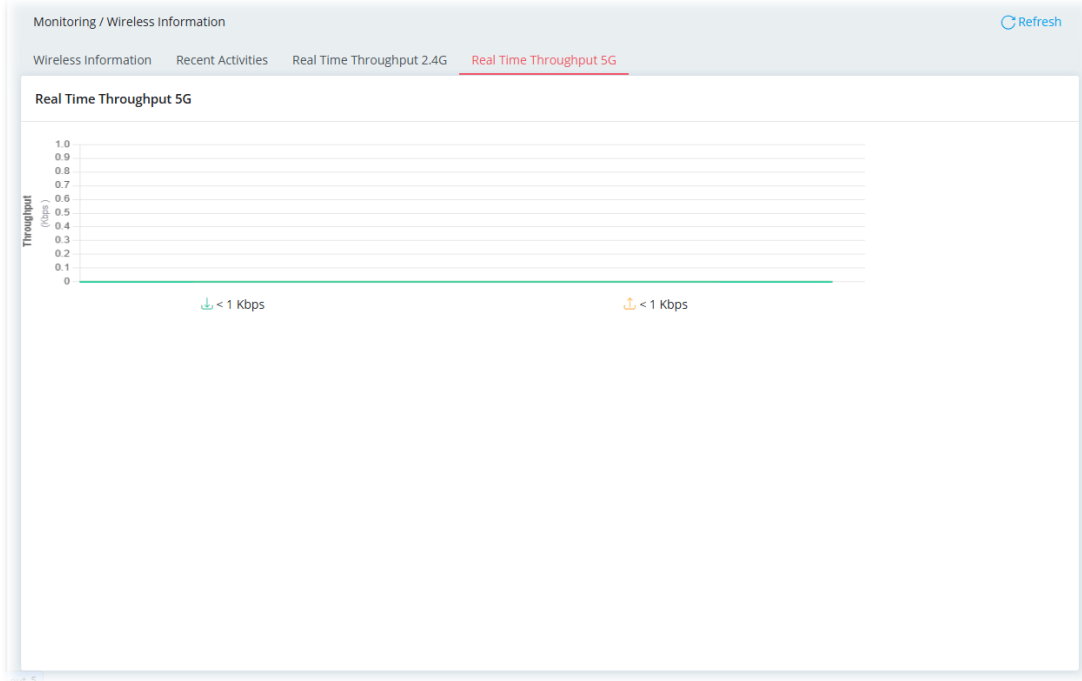
The real-time throughput (2.4G) can be shown with line graphs.




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

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

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



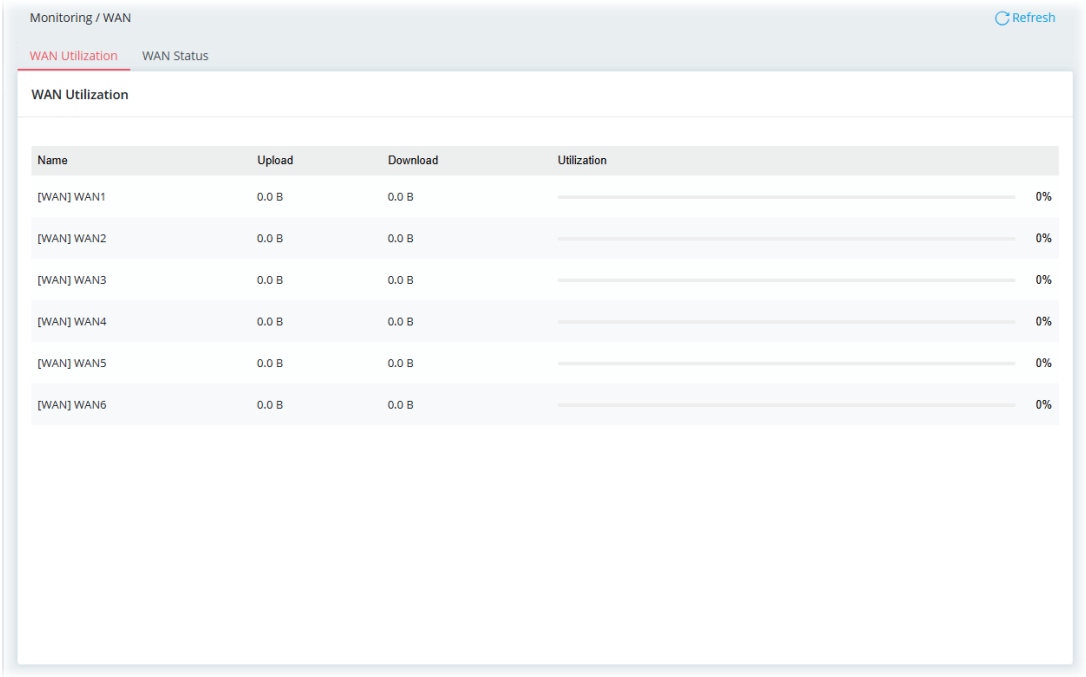

Click **Refresh** to reload this page with the most up-to-date information.

# IV-1-4 WAN

This page can display the WAN connection status, including the connection interface, MAC address, connection type, connection IP address, connection gateway, primary DNS and secondary DNS server addresses, online Time, and so on.

## IV-1-4-1 WAN Utilization

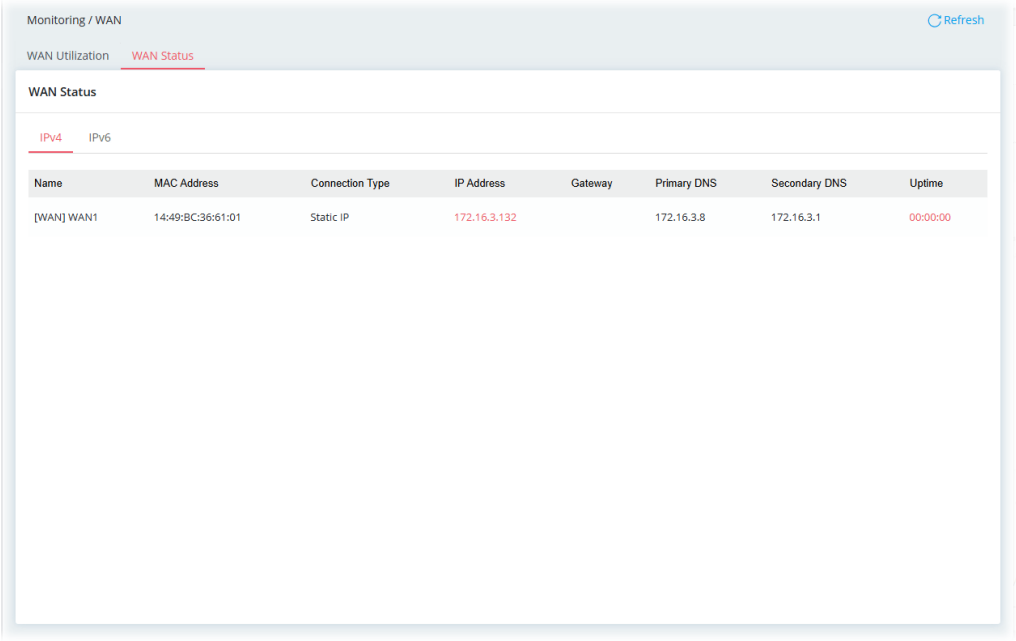
This page displays the utilization, including upload, download, and percentage of data transmission for each WAN interface.




## IV-1-4-2 WAN Status

### IPv4

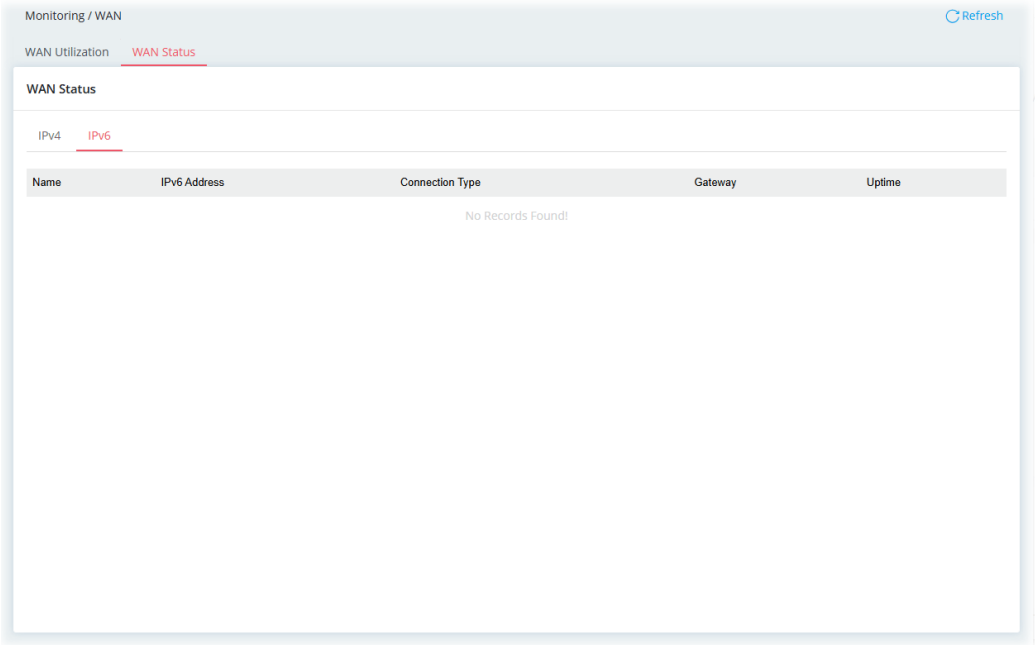
Select the IPv4 tab to display the IPv4 WAN connection status.




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

## IPv6

Select the IPv6 tab to get the WAN connection information (e.g., name, IPv6 address, connection type, gateway and the uptime).



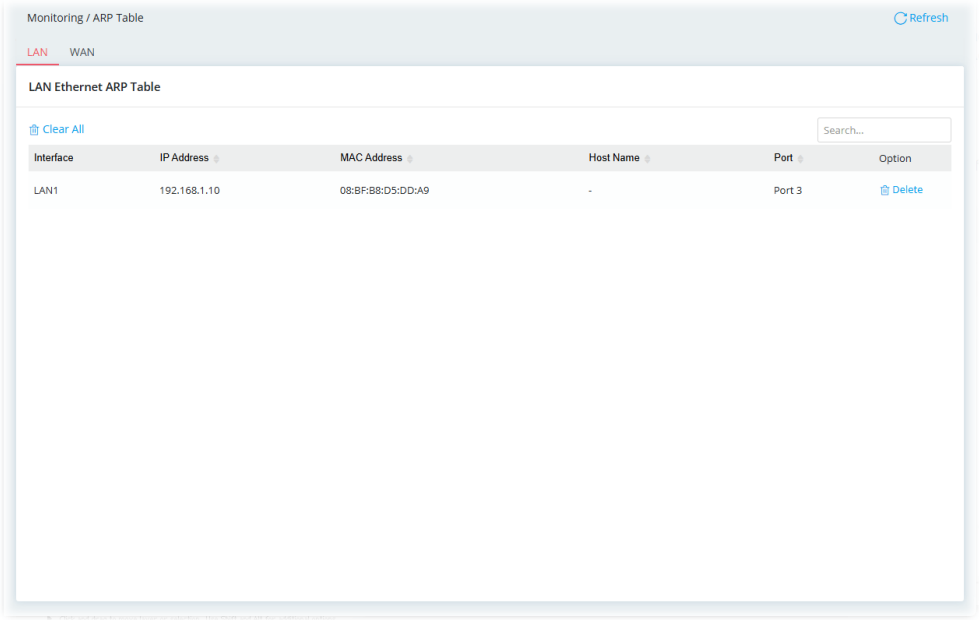

Click **Refresh** to reload this page with the most up-to-date information.

# IV-1-5 ARP Table

The table shows the contents of the ARP (Address Resolution Protocol) cache held in the router and shows the mappings between Ethernet hardware addresses (MAC Addresses) and IP addresses.

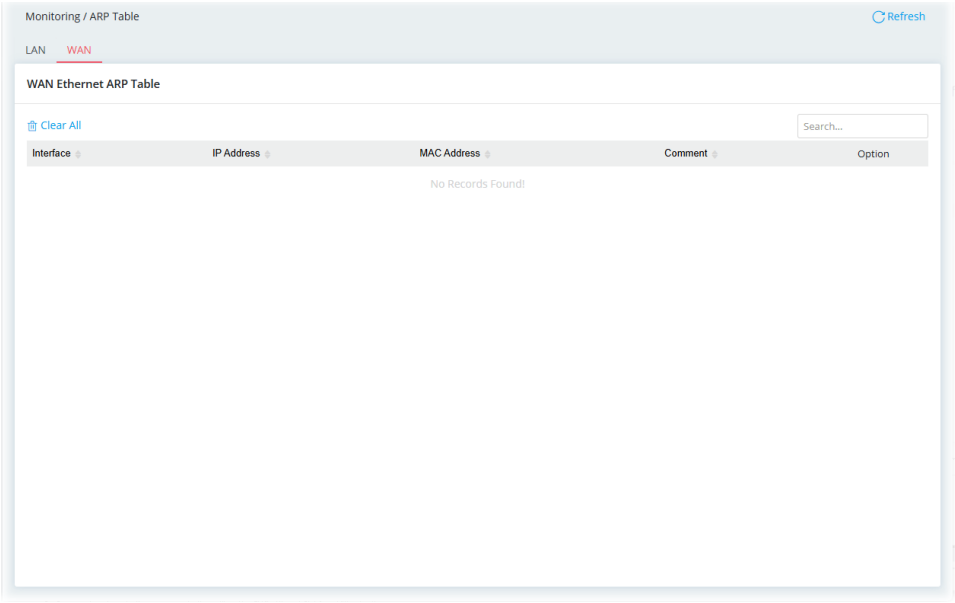
## IV-1-5-1 LAN

Click **Refresh** to reload this page with the most up-to-date information of LAN Ethernet ARP table.




## IV-1-5-2 WAN

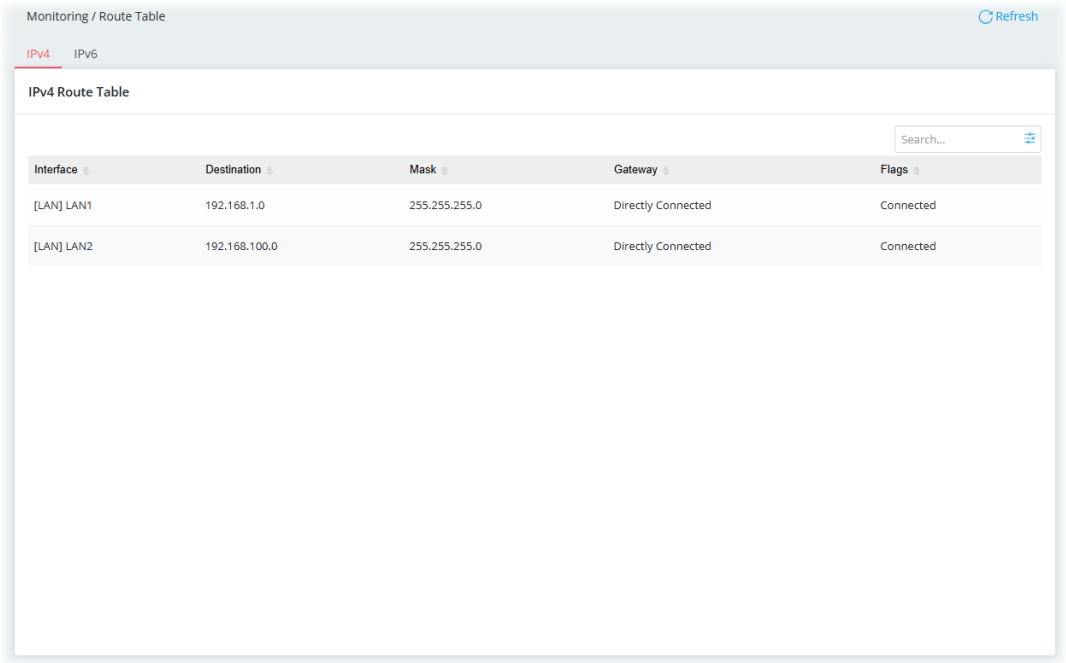
Click **Refresh** to reload this page with the most up-to-date information of WAN Ethernet ARP table.



# IV-1-6 Route Table

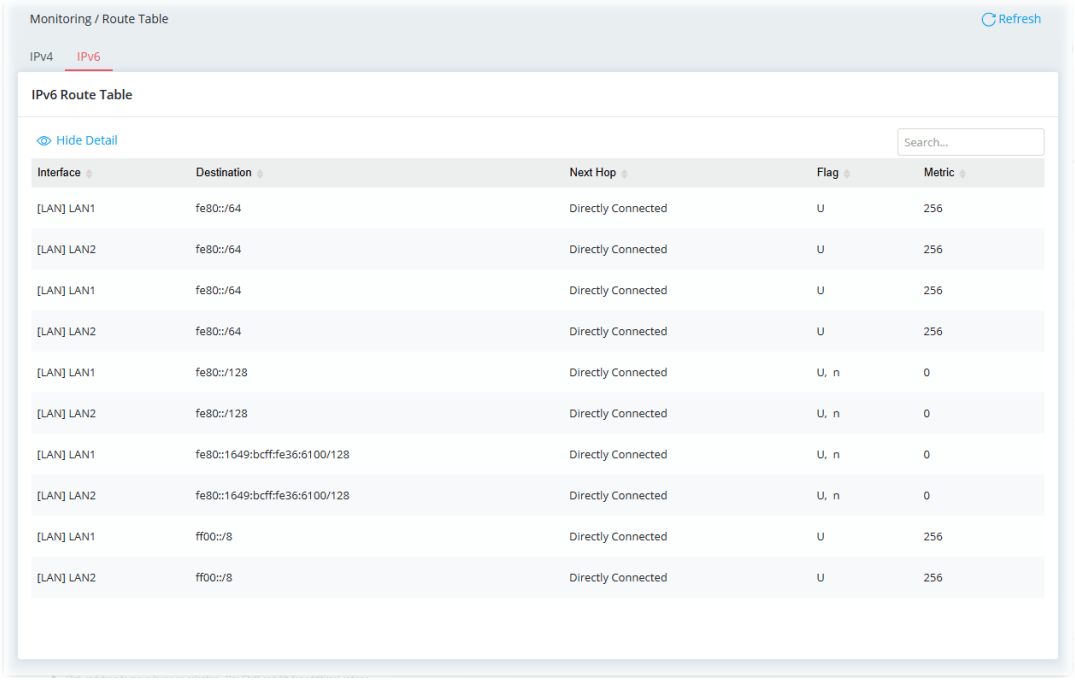
## IV-1-6-1 IPv4

Click **Refresh** to reload this page with the most up-to-date IPv4 routing information.



## IV-1-6-2 IPv6

Click **Refresh** to reload this page with the most up-to-date IPv6 routing information.



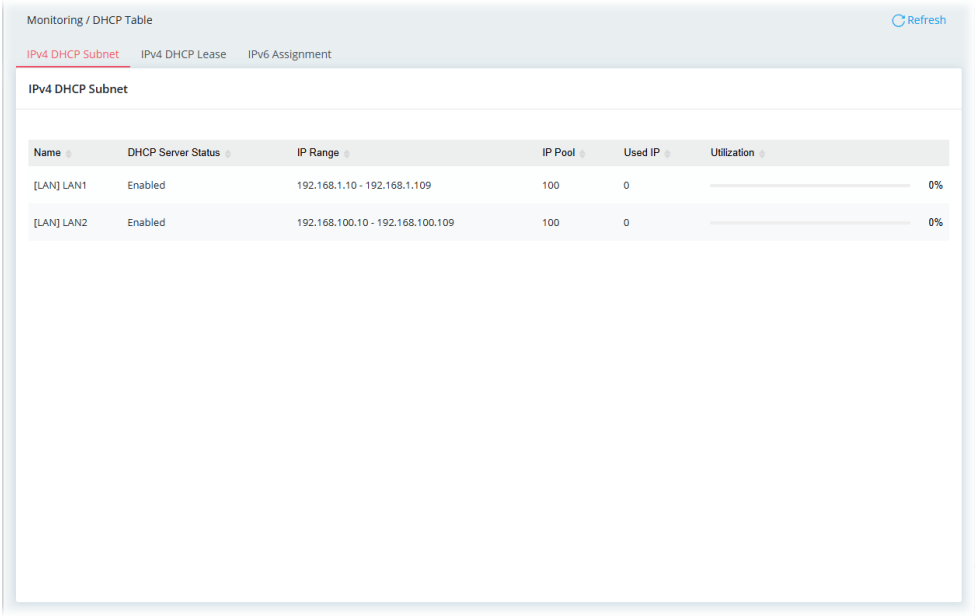
# IV-1-7 DHCP Table

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.

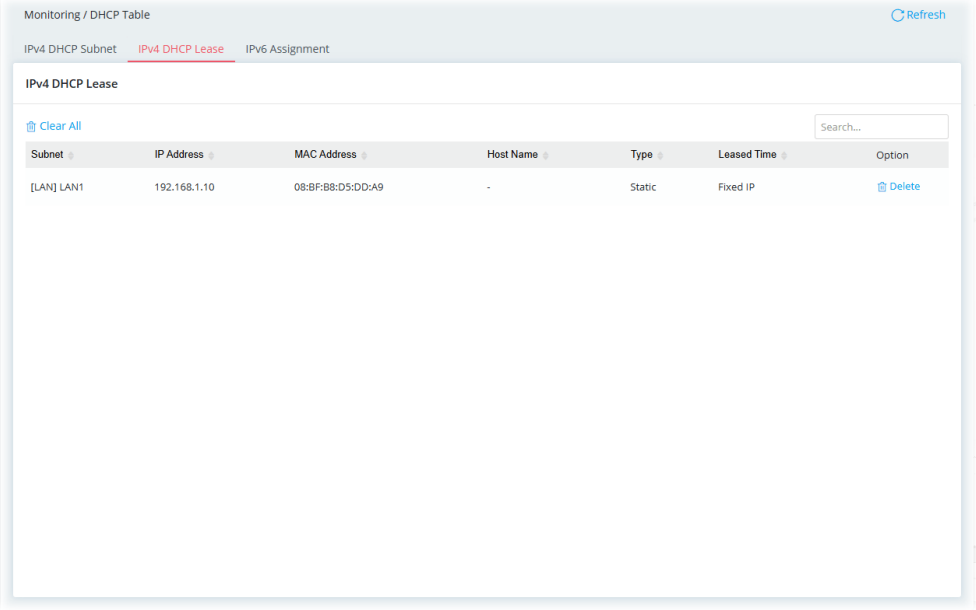
## IV-1-7-1 IPv4 DHCP Subnet

This page shows the DHCP server status, IP range, IP pool, Used IP, and percentage of utilization for each LAN interface.



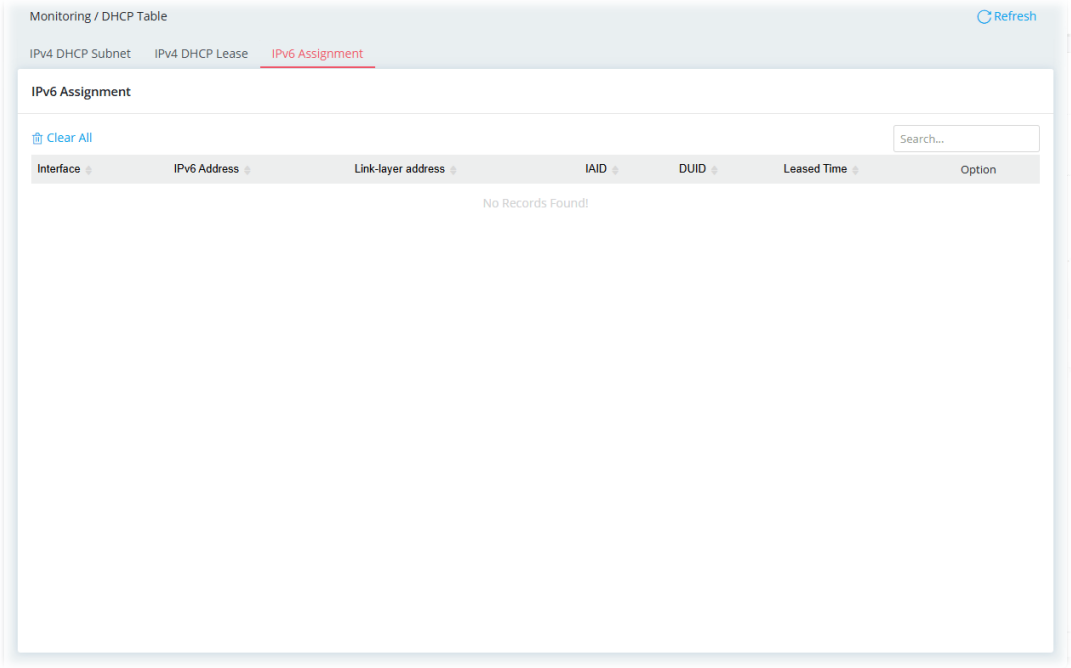

## IV-1-7-2 IPv4 DHCP Lease

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



### IV-1-7-3 IPv6 Assignment

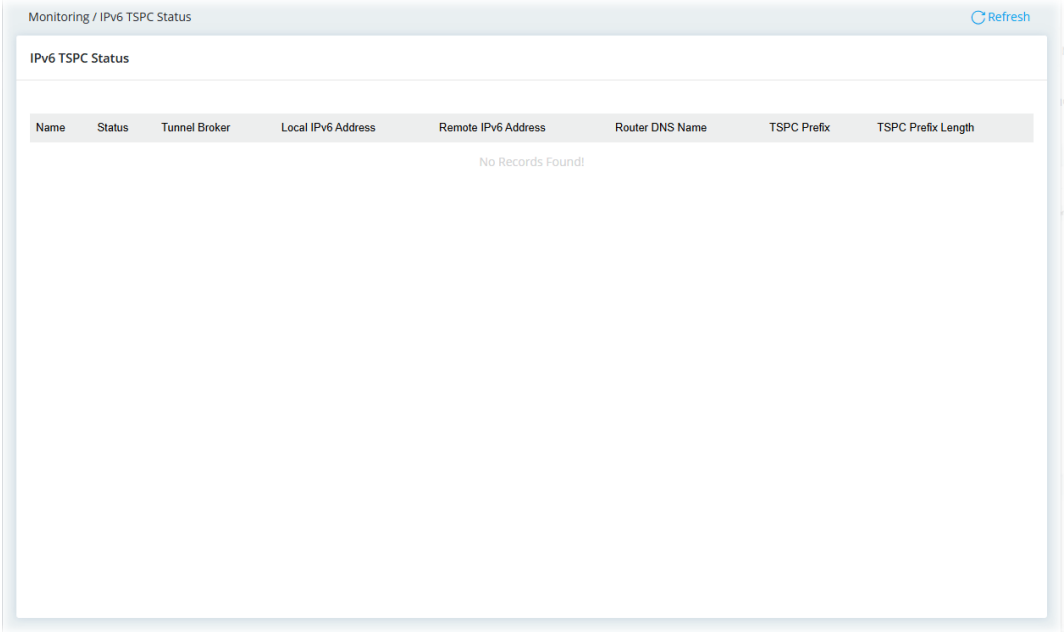
This page shows the remaining time of the IPv6 DHCP lease of the device.




## IV-1-8 IPv6 TSPC Status

IPv6 TSPC (Tunnel Setup Protocol Client) status page could help you diagnose issues with IPv6 connections that utilize TSP.

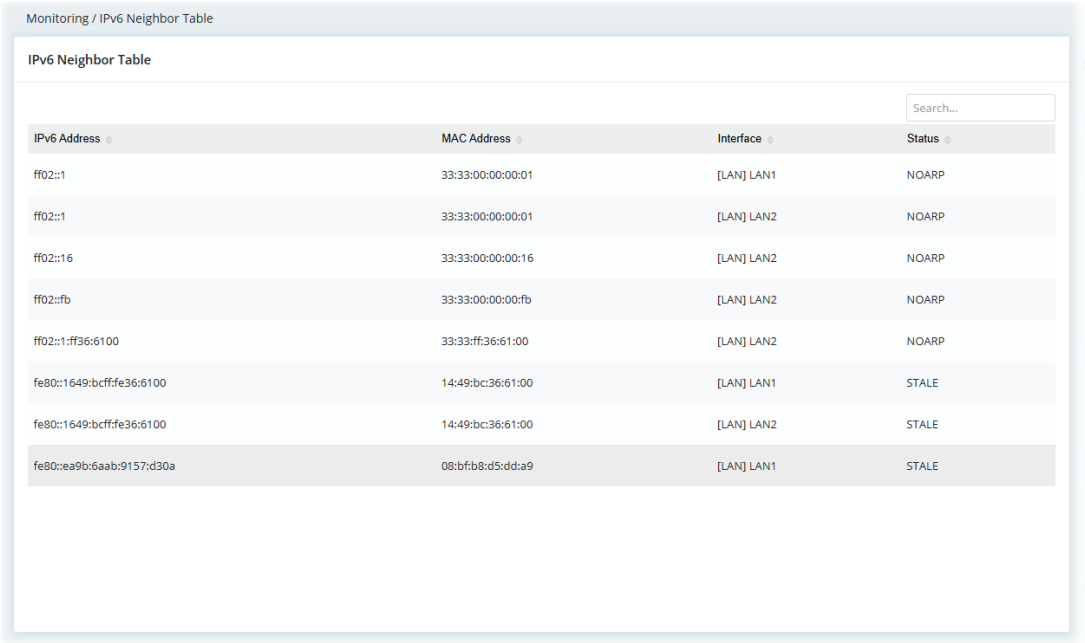
If TSPC is configured properly, the router will display the following when the router has connected to the tunnel broker successfully.




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

## IV-1-9 IPv6 Neighbor Table

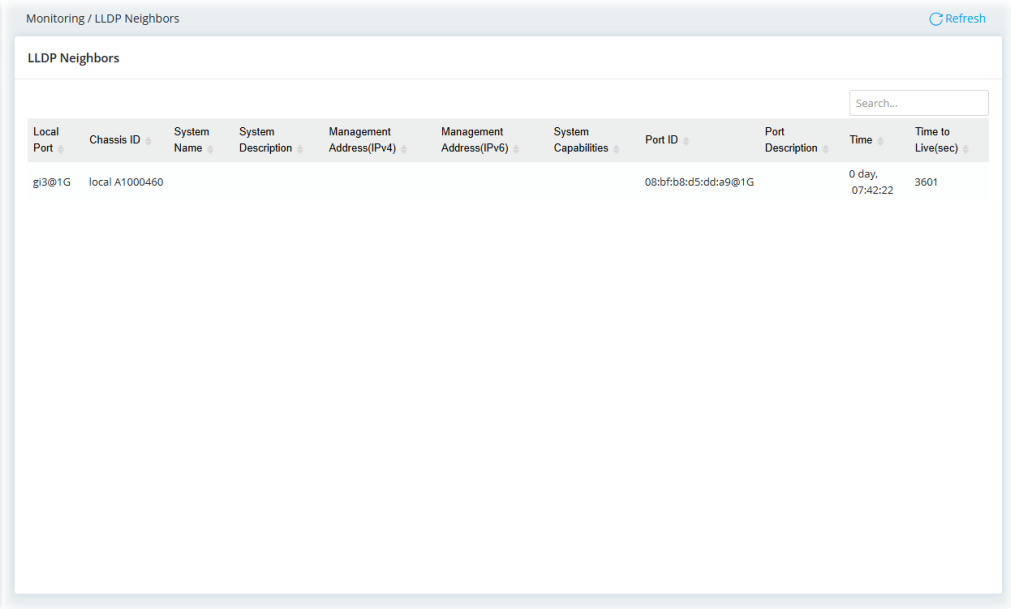
This page displays the mapping between Ethernet hardware addresses (MAC addresses) and the IPv6 addresses. This information is helpful in diagnosing network problems, such as IP address conflicts.




## IV-1-10 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

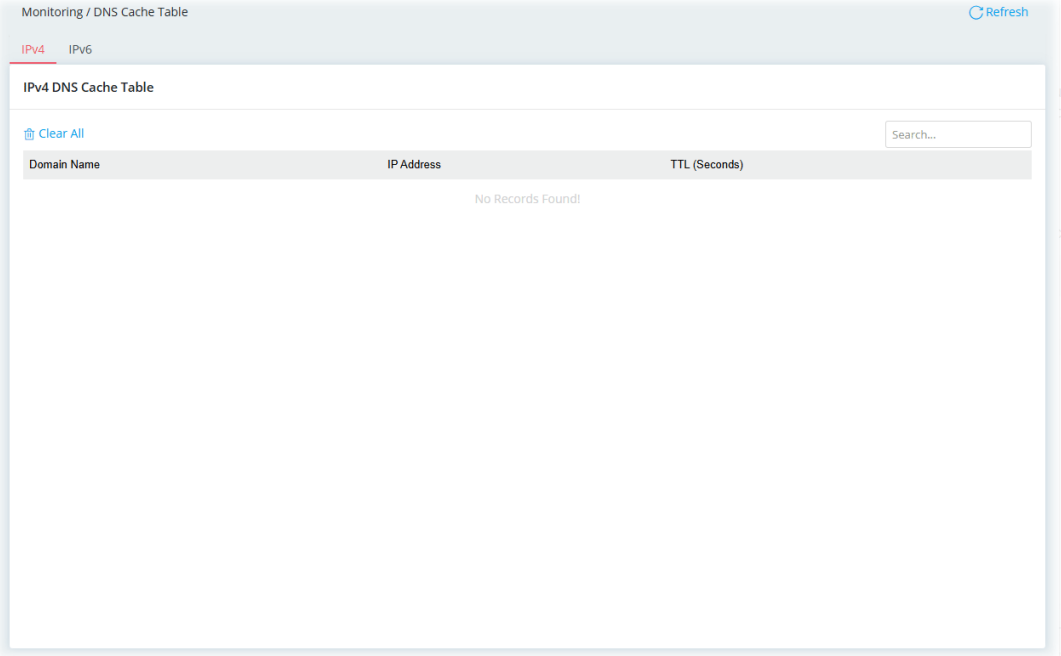



# IV-1-11 DNS Cache Table

The router can function as a DNS server which allows LAN clients to look up DNS information by sending DNS requests to the router. The DNS information is temporarily cached on the router and can be viewed on this page.

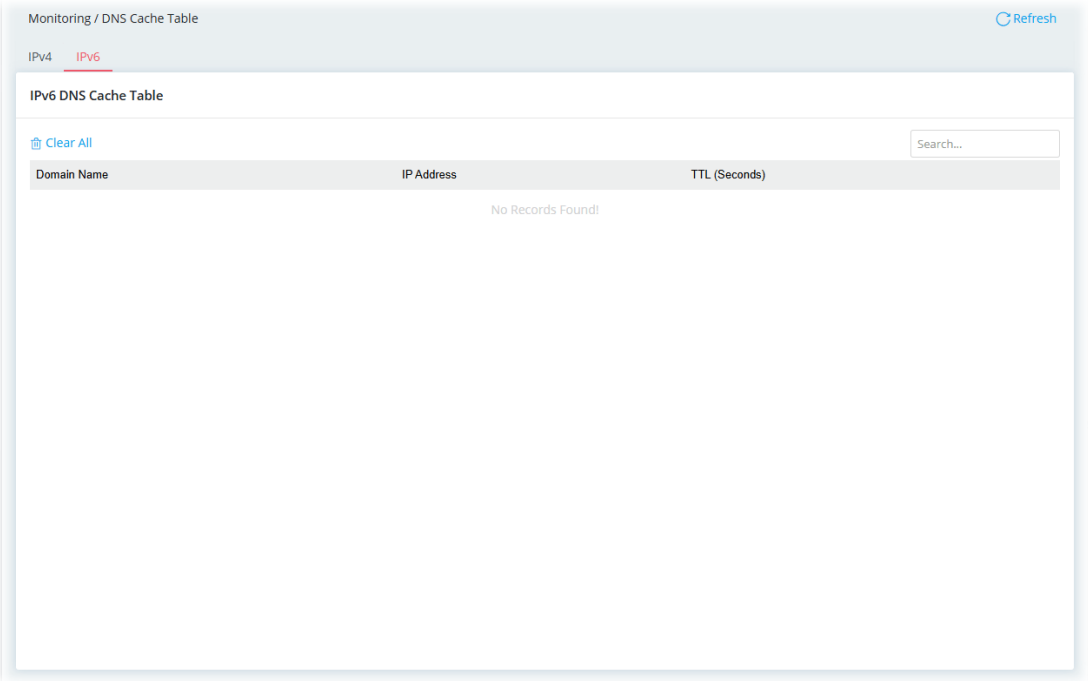
## IV-1-11-1 IPv4

Click **Refresh** to reload the most up-to-date information of the IPv4 DNS cache data.




## IV-1-11-2 IPv6

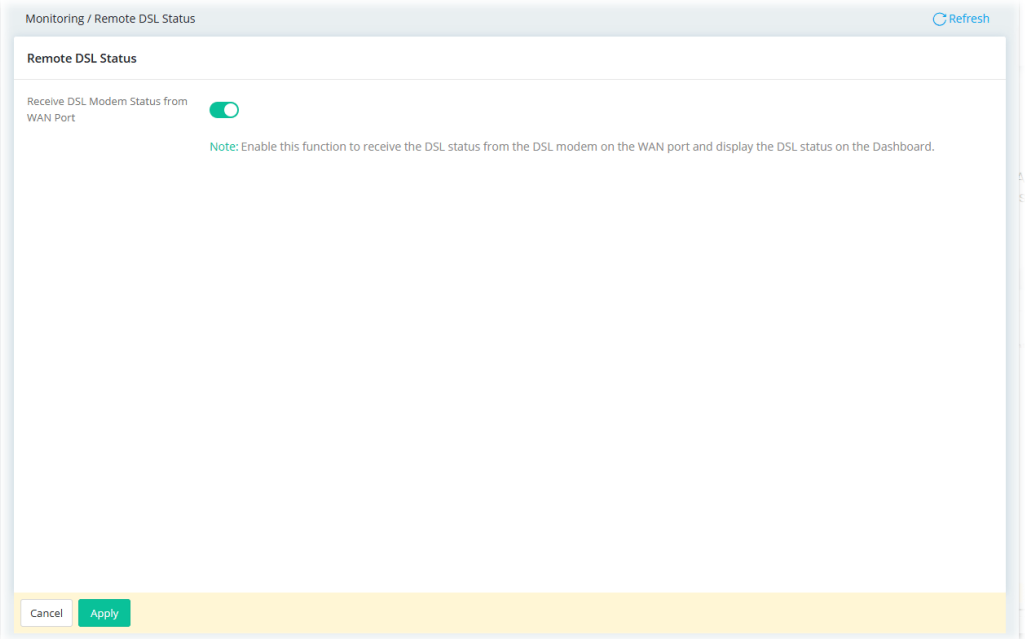
Click **Refresh** to reload the most up-to-date information of the IPv6 DNS cache data.




## IV-1-12 Remote DSL Status

To receive the remote DSL status from the DrayTek DSL modem on the WAN port and display the status on the Dashboard, switch the toggle to enable the function of showing the remote DSL status.

The default is disabled.



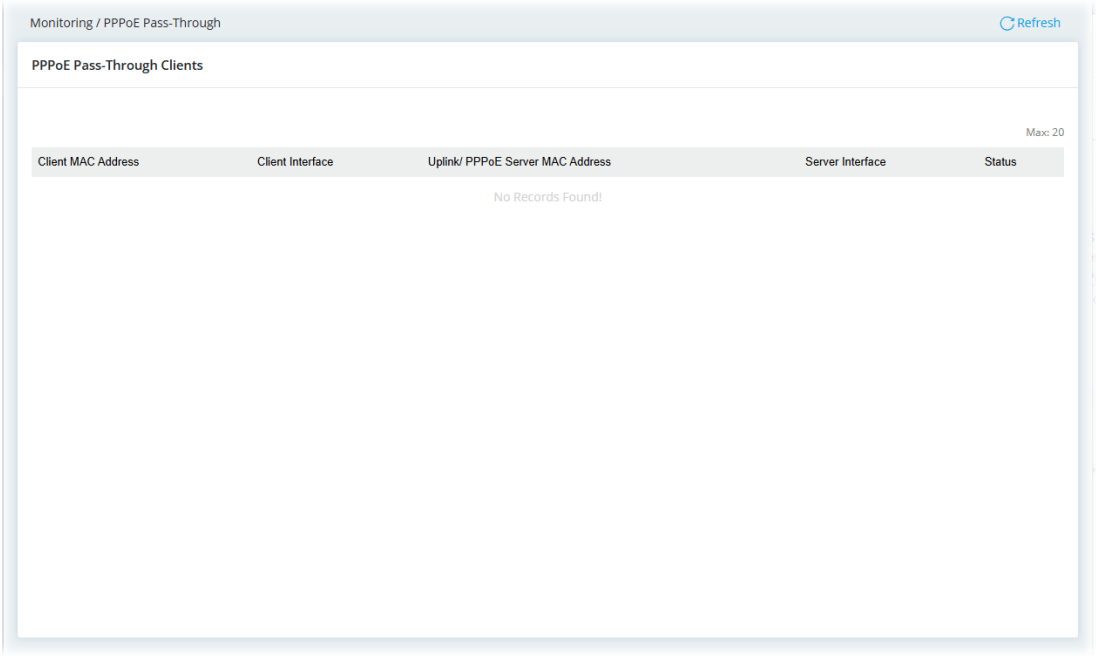

Click **Apply** to save the settings.

# IV-1-13 PPPoE Pass-Through

The router offers PPPoE dial-up connection. Besides, you also can establish the PPPoE connection directly from local clients to your ISP via the Vigor router. When PPPoA protocol is selected, the PPPoE package transmitted by PC will be transformed into PPPoA package and sent to WAN server. Thus, the PC can access Internet through such direction.

This page displays the results of performing PPPoE Pass-Through.

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

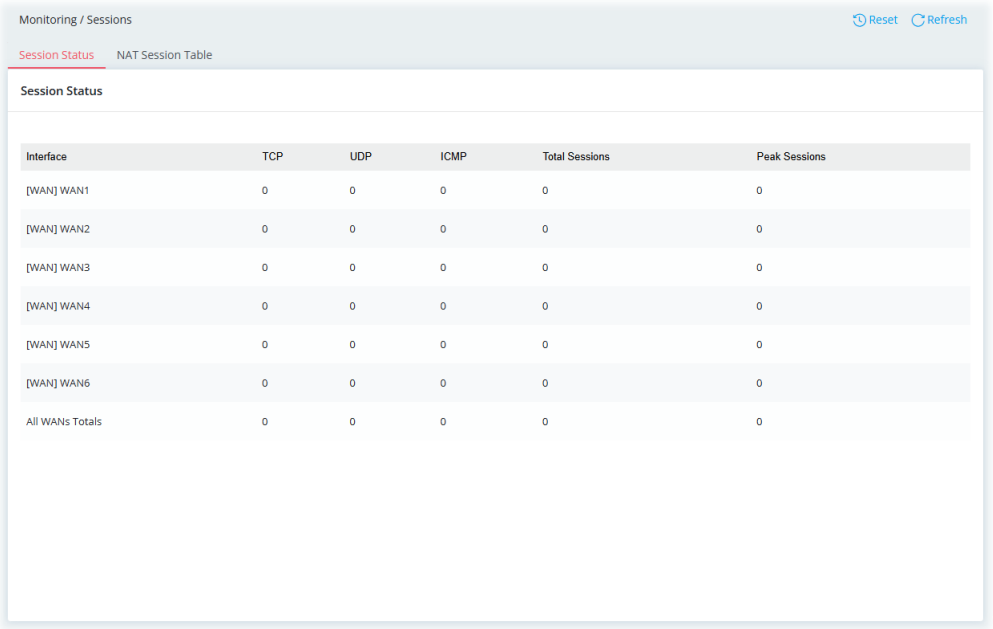


# IV-1-14 Sessions

## IV-1-14-1 Session Status

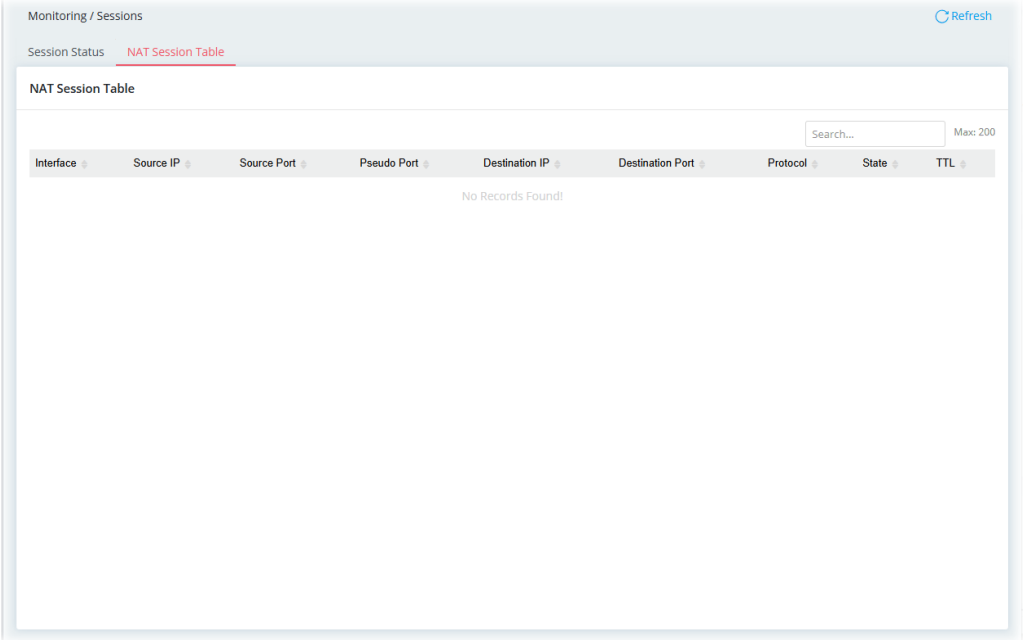
This page displays the number of sessions (TCP/UDP/ICMP/Total/Peak) for each WAN interface.

The last column, "Peak Sessions," indicates the highest number of connections since the router was activated.



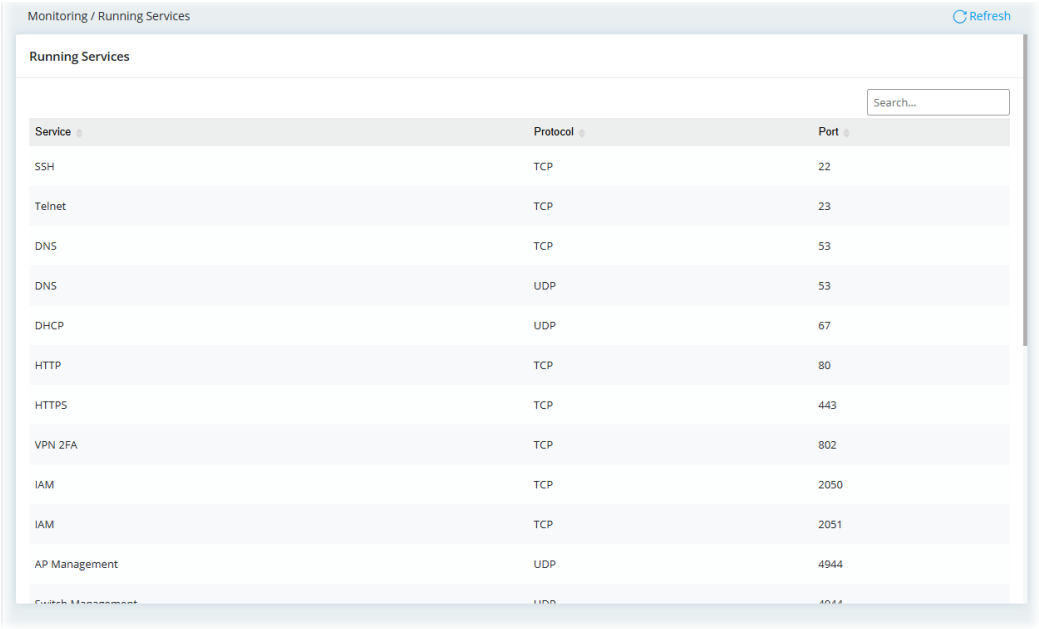

## IV-1-14-2 NAT Session Table

This screen shows the 200 newest entries in the NAT sessions table. Click **Refresh** to reload this page with the most up-to-date information.



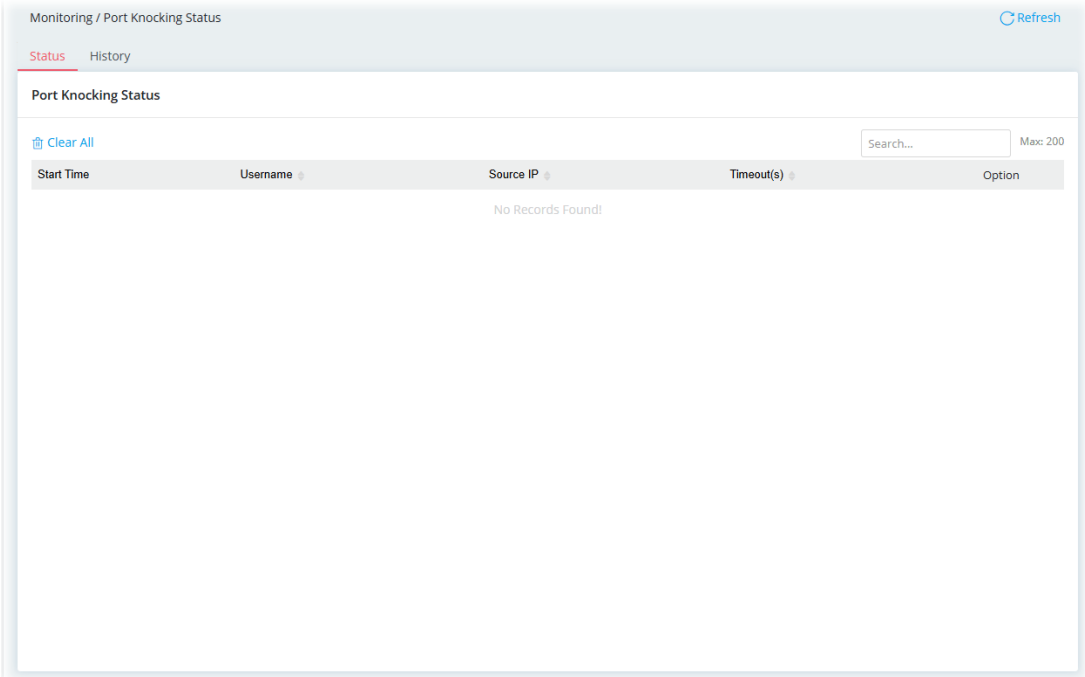
## IV-1-15 Running Services

This screen shows current running services (service name, protocol and the port number) for Vigor router.




## IV-1-16 Port Knocking Status

This page displays the users and IP addresses that have successfully passed Port Knocking authentication.



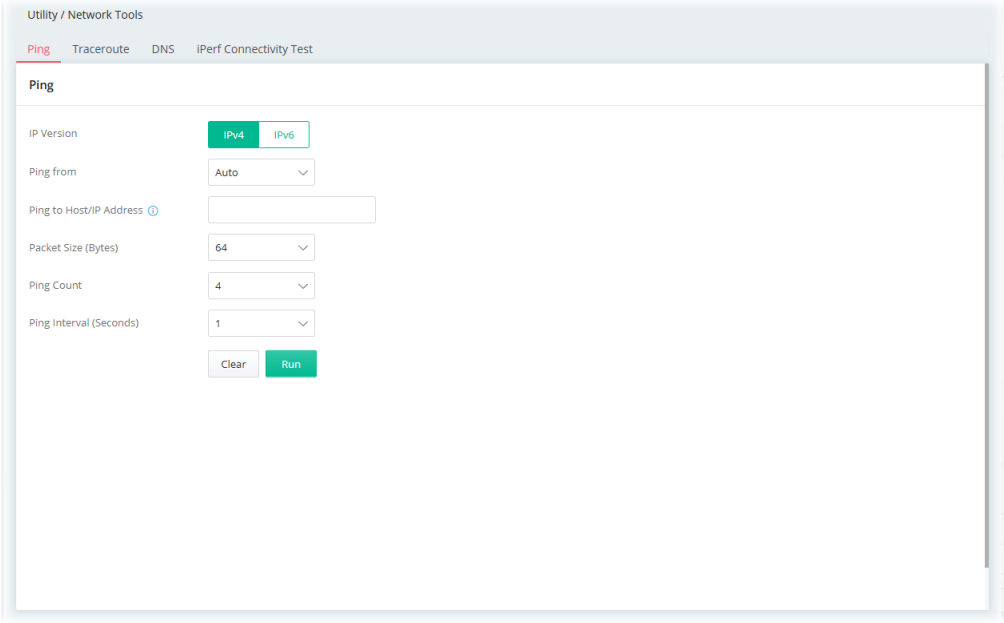
# IV-2 Utility

This section contains utilities (e.g., ping tool, traceroute, DNS and etc.) that can assist you in analyzing issues and failures during the setup and operation of the router.

## IV-2-1 Network Tools

### IV-2-1-1 Ping

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.

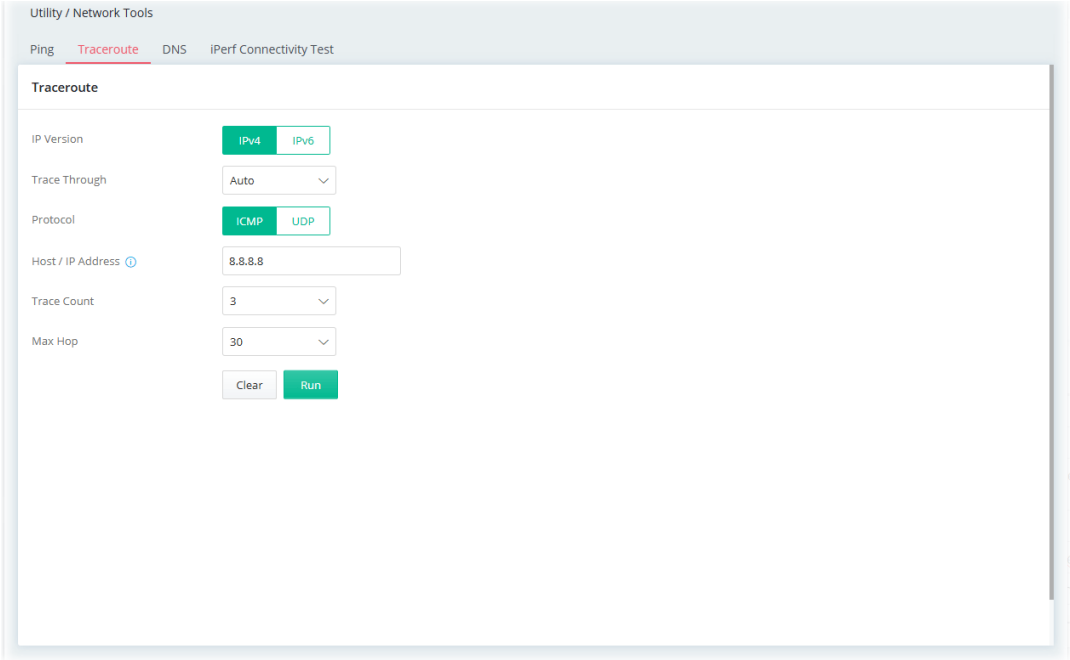



Available settings are explained as follows:

| Item | Description |
|---|---|
| **IP Version** | Select the IP version for entering correct IP address. |
| **Ping from** | Select an interface (LAN or WAN) from drop down list to through which you want to perform the ping operation, or choose **Auto** to be let the router select the WAN interface. |
| **Ping to Host/IP Address** | Enter the IP address of the Host/IP that you want to ping. |
| **Packet Size (byte)** | Determine the packet size for the ping job. |
| **Ping Count** | Determine the quantity of the packet being pinged. |
| **Ping Interval (Seconds)** | Set 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-2-1-2 Traceroute

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.

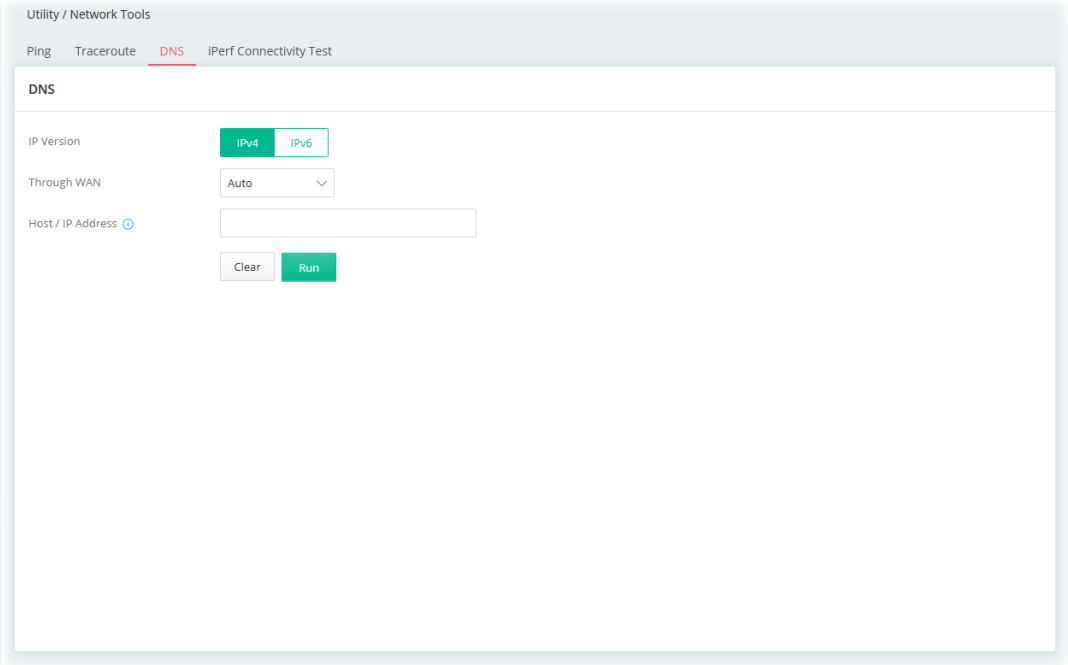



Available settings are explained as follows:

| Item | Description |
|---|---|
| IP Version | Select the IP version for entering correct IP address. |
| 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 job. |

## IV-2-1-3 DNS

The user can diagnose the router by query Domain Name System (DNS) servers to obtain domain name or IP address information.

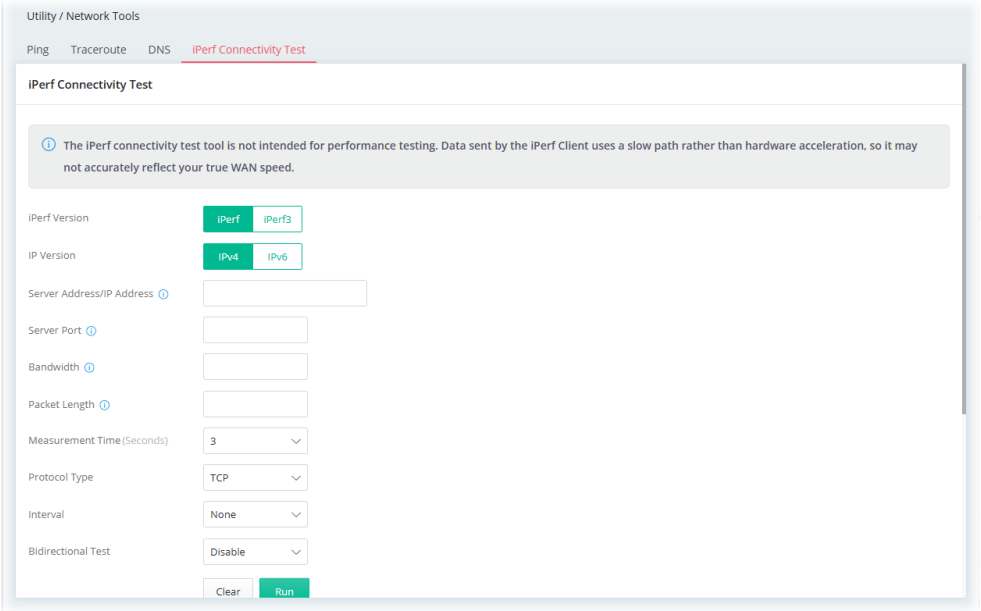



Available settings are explained as follows:

| Item | Description |
|---|---|
| **IP Version** | Select the IP version for entering correct IP address. |
| **Through WAN** | Trace through specific interface. |
| **Host/IP Address** | Enter the domain name or IP address (IPv4 or IPv6) for DNS query to get corresponding information. |
| **Clear** | Remove the settings and return to the factory settings. |
| **Run** | Perform the job. |

## IV-2-1-4 iPerf Connectivity Test

iPerf is a tool used to test network connection between the Vigor router and any other device, such as a notebook or a mobile phone.



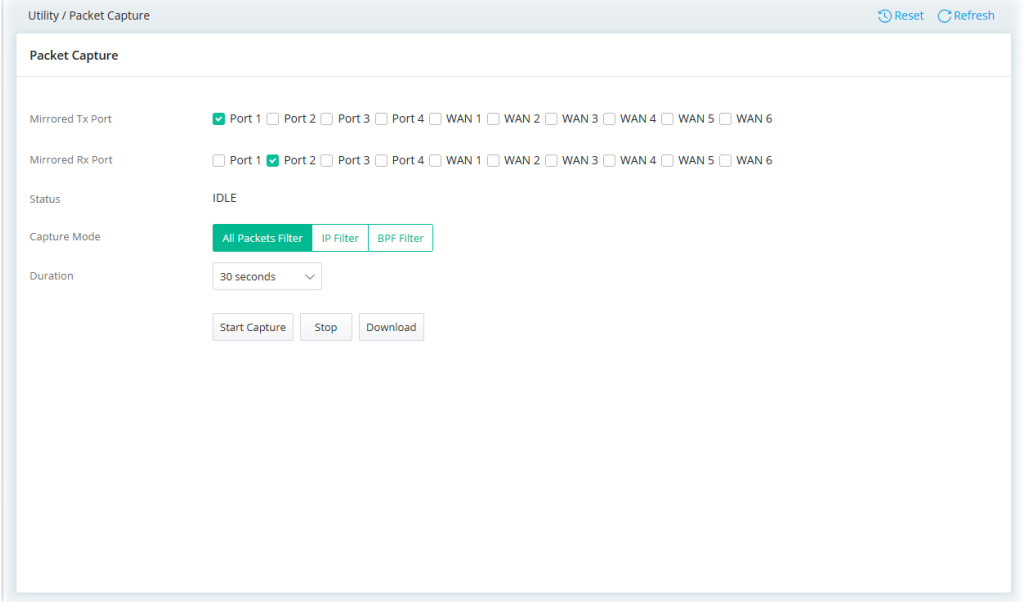

Available settings are explained as follows:

| Item | Description |
|---|---|
| **iPerf Version** | Select the iPerf Version based on the iPerf server used. |
| **IP Version** | Select the IP version (IPv4 or IPv6). |
| **Server Address/IP Address** | Enter an IPv4/IPv6 address or the hostname of the iPerf server. |
| **Server Port** | Enter a port number for the iPerf server. |
| **Bandwidth** | Set the bandwidth (1-1000MB) for every performance test. |
| **Packet Length** | Specify the packet length (8-64000 Bytes) for the test. |
| **Measurement Time** | Select the duration time (3, 5, 10, 20, and 50) for every performance test.<br>Unit is second. |
| **Protocol Type** | Select TCP or UDP for the iPerf server to test the transmission quality.<br>For Bidirectional Test, select UDP. |
| **Interval** | Specify the time interval (1, 2, 3, 5, 10 and None) for the test.<br>Unit is second. |
| **Bidirectional Test** | Each test includes both upload (TX) and download (RX) packets. Note that the test might result in significant CPU usage.<br>**Disable** – Disable the test.<br>**Tradeoff** – Test upload traffic first, then download traffic.<br>**Dualtest** – Test upload and download traffic simultaneously. |
| **Clear** | Remove the settings and return to the factory settings. |
| **Run** | Perform the job. |

# IV-2-2 Packet Capture

Packet capture records packets passing through the network interface intact, which can then be viewed and analyzed using various tools (such as Wireshark and tcpdump).

This technique is mainly used for debugging, protocol analysis, troubleshooting, and cybersecurity investigations.

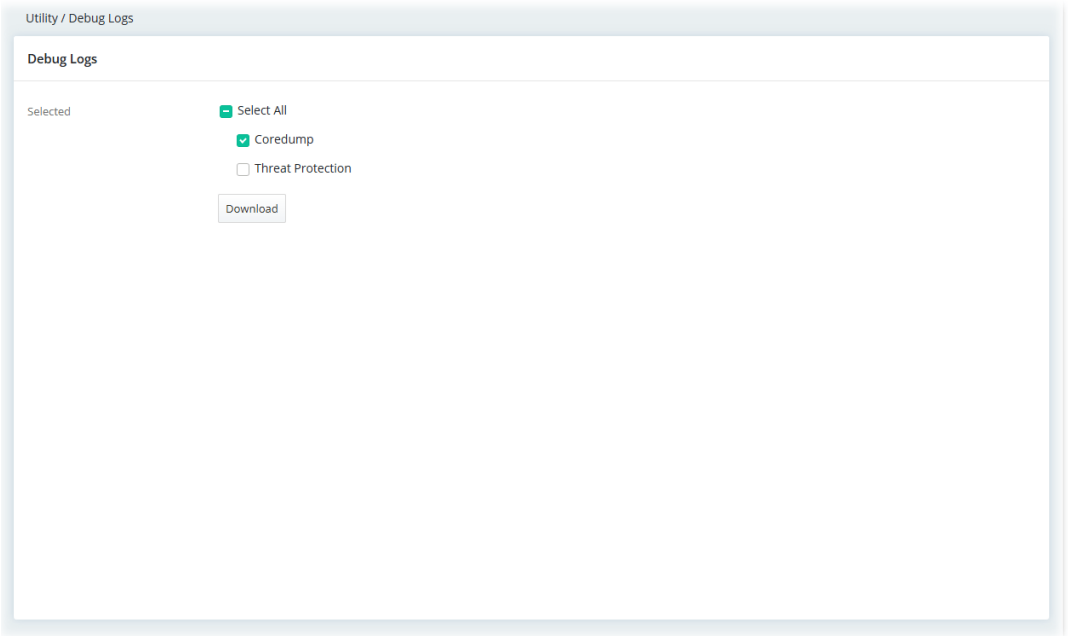



Available settings are explained as follows:

| Item | Description |
|---|---|
| **Mirrored Tx Port** | Select the interface(s) to capture the packets passing through. |
| **Mirrored Rx Port** | Select the interface(s) as the packet reception. |
| **Status** | Displays the current status of packet capture. |
| **Capture Mode** | Select a method to capture the packet.<br>**All Packets Filter** – All packets will be captured.<br>**IP Filter** – Only the packets passing through the specified IP addresses will be captured.<br>• **Protocol** – Select a protocol (any, ICMP, TCP, UDP or TCP/UDP).<br>• **Port** – When TCP, UDP, or TCP/UDP is selected as the protocol, specify a port number. You can choose any number or select the Customized Port option to enter a specific port number.<br>• **IP Address** – Select Any or select Customize IP to enter a specified IP address.<br>**BPF Filter** - Packets matching the BPF filter (with standard tcpdump/libpcap BPF syntax, libpcap 1.9.1) will be captured. |
| **Duration** | The packet capturing will be automatically stopped when the time is up. |
| **Start Capture** | Perform the packet capturing job. |
| **Stop** | Click to stop the packet capturing. |
| **Download** | Save the records as a file that will be used for analysis with the specified tool. |

# IV-2-3 Debug Logs

This page is for technical use only. To help technicians identify issues with this device, please select the box(es) on this page and click 'Download' to save the logs.

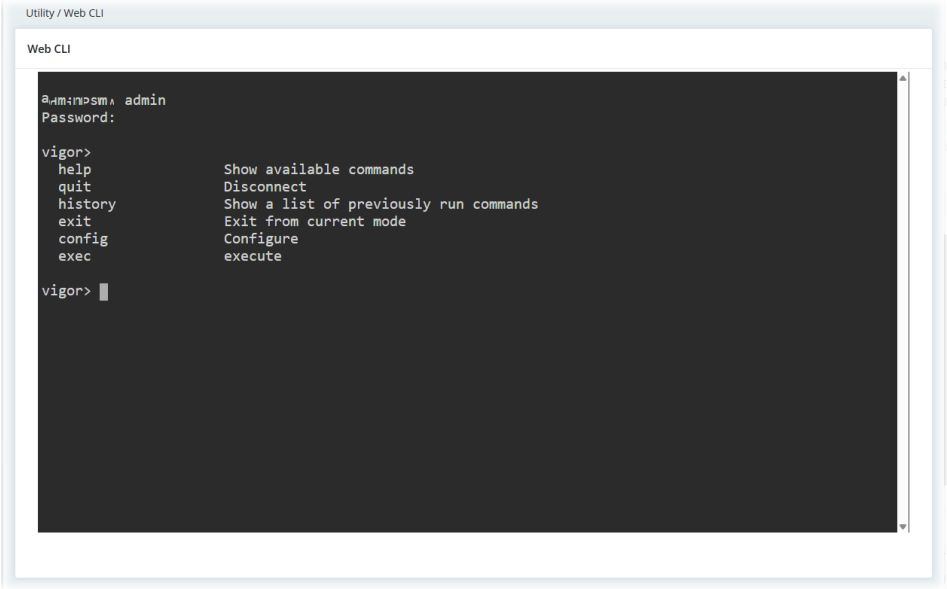


# IV-2-4 Web CLI

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**.



This page is left blank.

# Chapter V Troubleshooting



# V-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-2 Hardware Installation"** for details.
2. Power on the modem. Make sure the **POWER** LED**, ACT** LED and **LAN** LED are bright.
3. If not, it means that there is something wrong with the hardware status. Simply back to **"I-2 Hardware Installation"** to execute the hardware installation again. And then, try again.

# V-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.

## V-2-1 For Windows

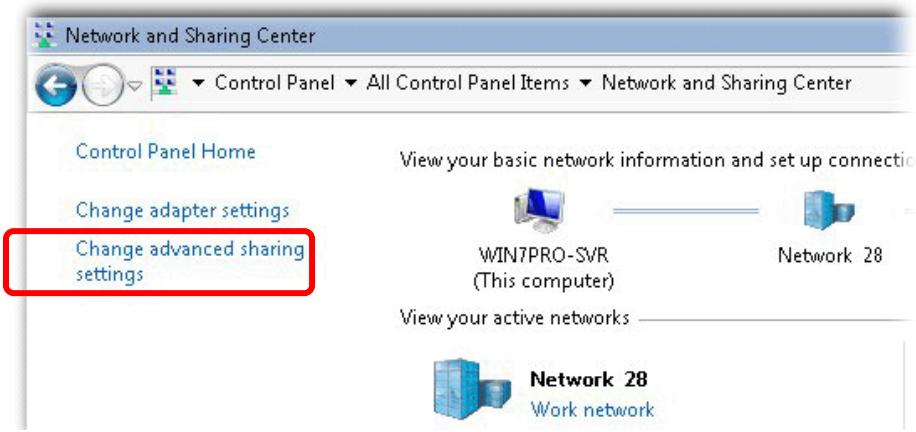
**Note:**

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**.

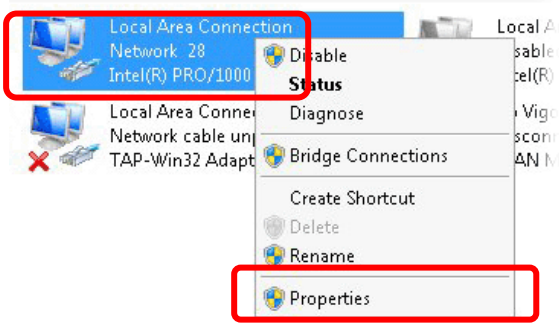
1. Open **All Programs>>Getting Started>>Control Panel.** Click **Network and Sharing Center.**



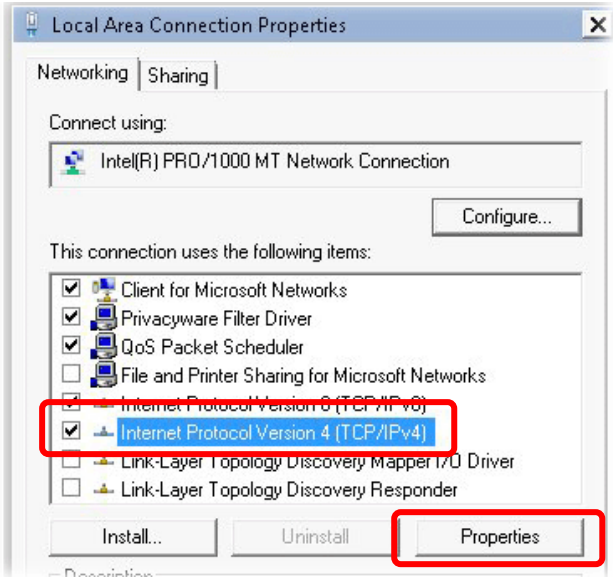

2. In the following window, click **Change adapter settings**.



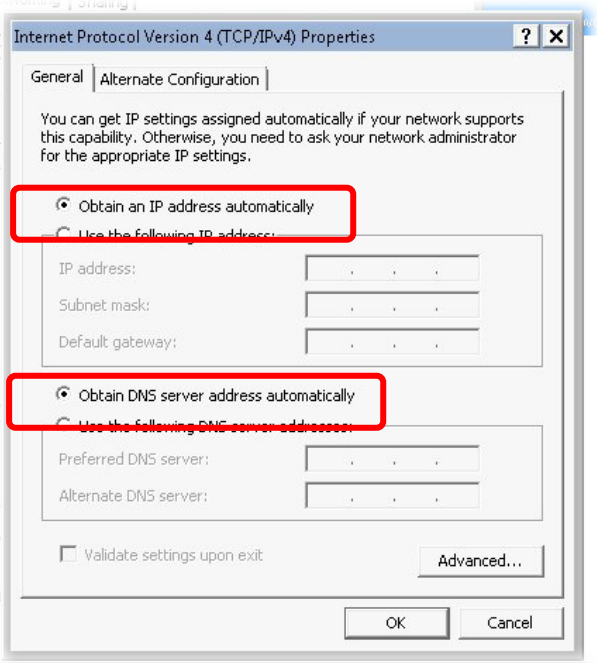
3. Icons of the network connection will be shown on the window. Right-click on **Local Area Connection** and click on **Properties**.




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

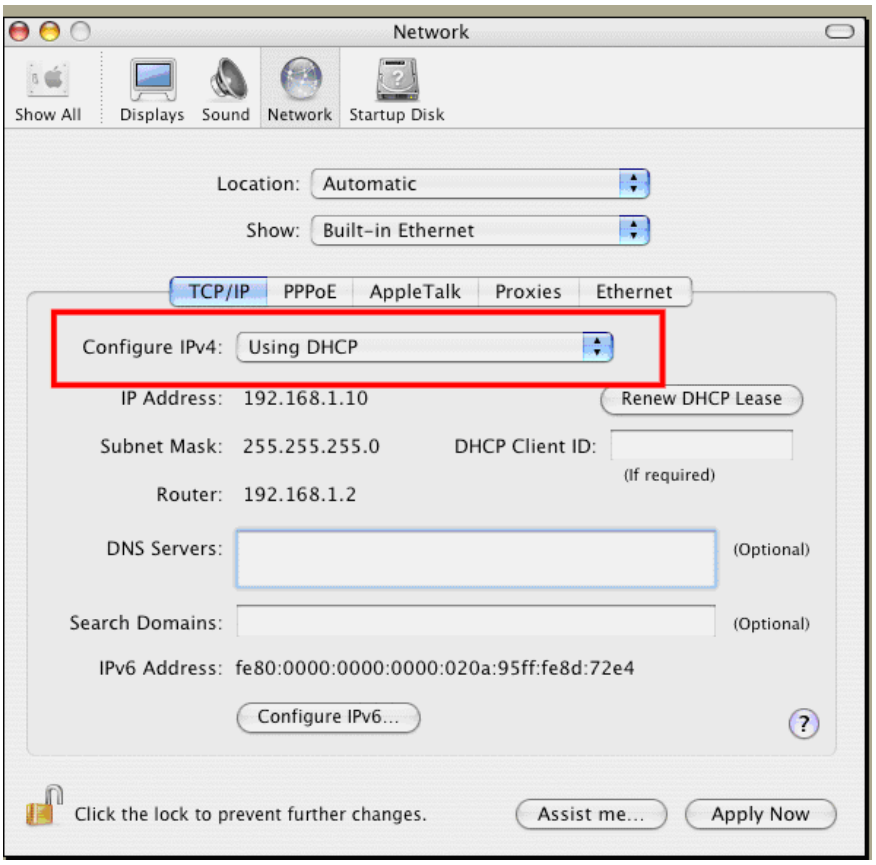



5. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Finally, click **OK**.



## V-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.



# V-3 Pinging the Device

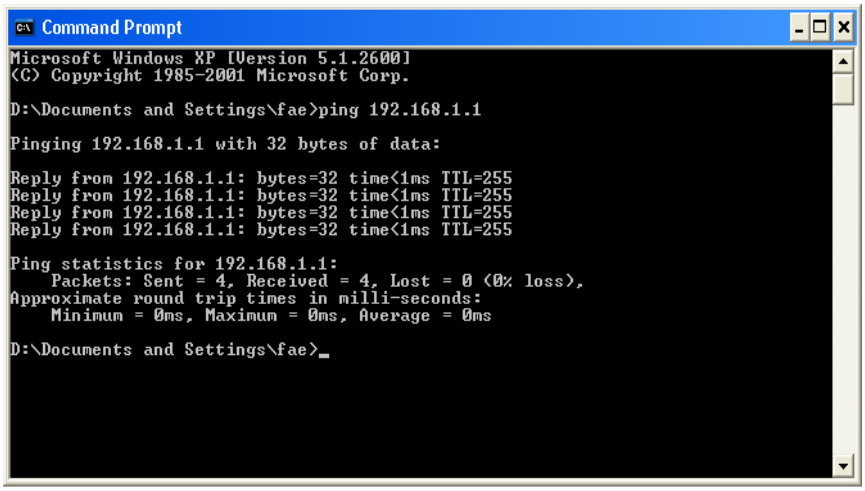
The default gateway IP address of the modem is 192.168.1.1. For some reason, you might need to use "ping" command to check the link status of the modem. **The most important thing is that the computer will receive a reply from 192.168.1.1.** If not, please check the IP address of your computer. We suggest you setting the network connection as **get IP automatically**. (Please refer to the section V-2)

Please follow the steps below to ping the modem correctly.

## V-3-1 For Windows

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

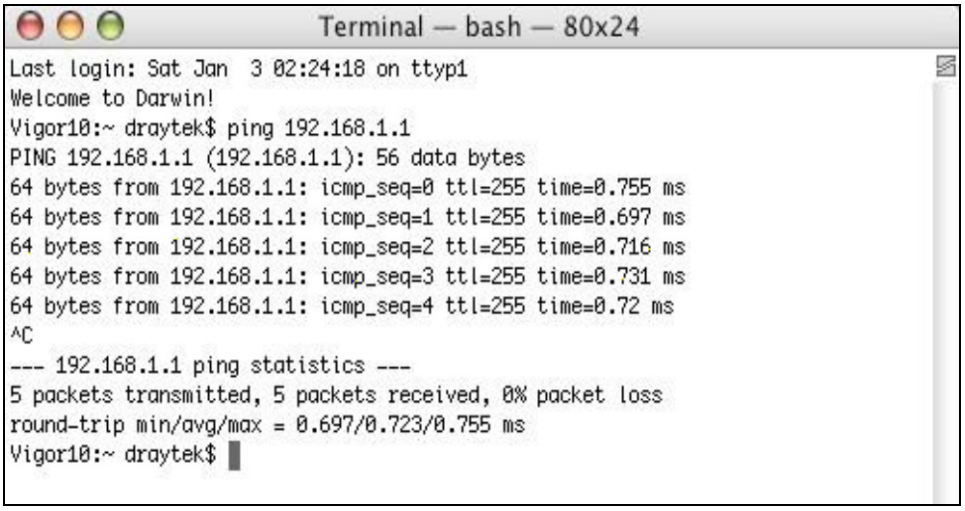
   Type **cmd**. The DOS command dialog will appear.




2. Type ping 192.168.1.1 and press [Enter]. If the link is OK, the line of **"Reply from 192.168.1.1:bytes=32 time<1ms TTL=255"** will appear.
3. If the line does not appear, please check the IP address setting of your computer.

## V-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 192.168.1.1** and press [Enter]. If the link is OK, the line of **"64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms**" will appear.


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

# V-4 Backing to Factory Default Setting

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

---

**Warning:**

After using the factory default settings, you will lose all settings you did before. Make sure you have recorded all useful settings before you pressing.

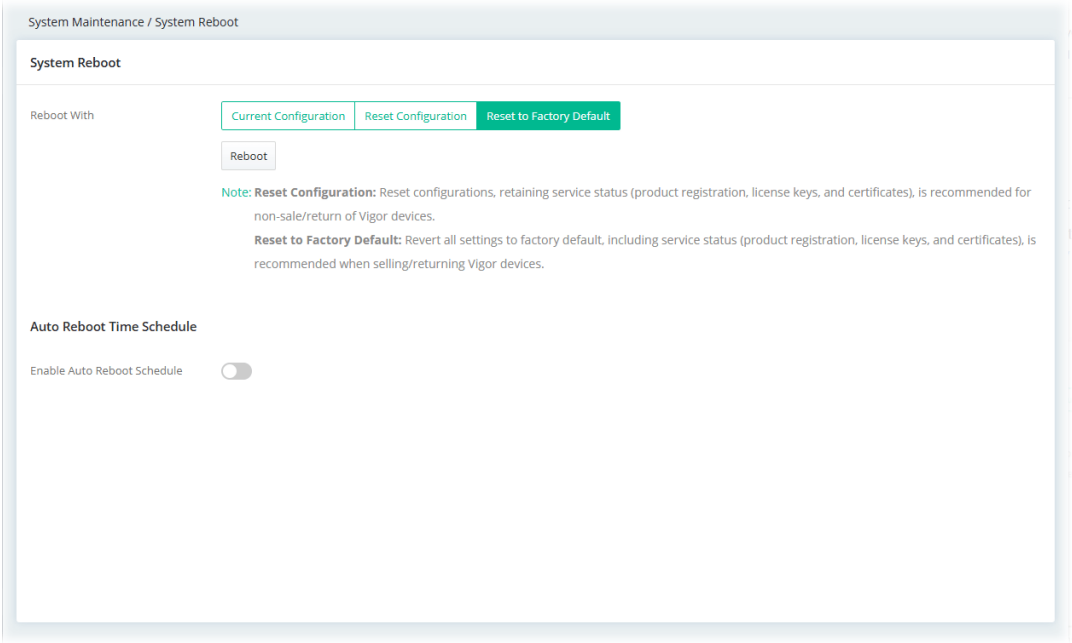
---

## V-4-1 Software Reset

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

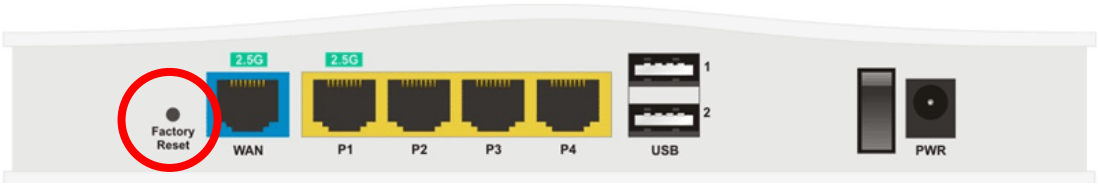
Go to **System Maintenance** and choose **System Reboot** on the web page. The following screen will appear. Choose **Reset to Factory Default** and click **Reboot**.

After few seconds, the modem will return all the settings to the factory settings.



## V-4-2 Hardware Reset

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




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

# V-5 Contacting DrayTek

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