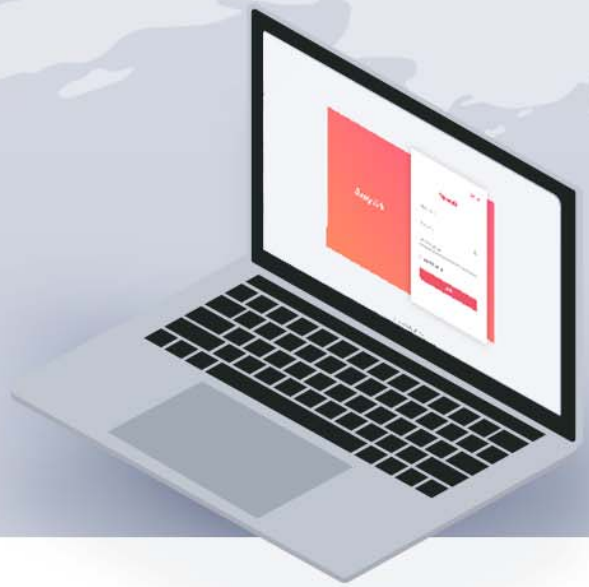
# VigorACS3

Unified Management System



## User's Guide

V1.0

# VigorACS 3

## Unified Management System User's Guide

Manual Version: V1.0

Date: March 3, 2021

Software Version: V3.0.3

© 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. The scope of delivery and other details are subject to change without prior notice.

Microsoft is a registered trademark of Microsoft Corp.

Windows 8, 10 and Explorer are trademarks of Microsoft Corp.

Apple and Mac OS are registered trademarks of Apple Inc.

DrayTek is a registered trademark of DrayTek Corp.

Other products may be trademarks or registered trademarks of their respective manufacturers.

# VigorACS 3 License

© All rights reserved.

No part of this distribution may be reproduced, transmitted, transcribed, stored in a system, or translated into any language without written permission from the copyright holders.

# Limited Warranty

DrayTek warrants that (a) the VigorACS 3 (henceforth called the SOFTWARE) will perform substantially in accordance with the accompanying written materials for a period of ninety (90) days from the date of receipt, and (b) any support service provided by DrayTek shall be substantially as described in applicable written materials provided to you by DrayTek, and DrayTek support engineers will make commercially reasonable efforts to solve any problems. To the extent allowed by applicable law, implied warranties on the SOFTWARE, if any, are limited to ninety (90) days.

**Customer Remedies**

DrayTek's and its suppliers entire liability and your exclusive remedy shall be, at DrayTek's option, either (a) return of the price paid, if any, or (b) repair or replacement of the SOFTWARE that des not meet DrayTek's Limited Warranty and which is returned to DrayTek with a copy of your receipt. This Limited Warranty is void if failure of the SOFTWARE has resulted from accident, abuse, or misapplication. Any replacement SOFTWARE will be warranted for the remainder of the original warranty period of thirty (30) days, whichever is longer. Outside Taiwan, neither these remedies nor any product support services offered by DrayTek are available without proof of purchase from an authorized international source.

**No Other Warranties**

To the maximum extent permitted by applicable law, DrayTek and its suppliers disclaim all other warranties and conditions, either express or implied, including, but not limited to, implied warranties of merchantability, fitness for a particular purpose, title, and non-infringement, with regard to the SOFTWARE, and the provision of or failure to provide support services. This limited warranty gives you specific legal rights. You may have others, which vary from state/jurisdiction to state/jurisdiction.

Please read the license screen in the installation wizard. You must accept the terms of the license in order to install VigorACS 3.

# Table of Contents

**Part I** ..... **1**

Chapter 1 Introduction ..... 2

1.1 Main Features and Benefit ..... 2
1.2 System Architecture ..... 2
1.3 Web Service ..... 3

Chapter 2 Install & Startup ..... 5

2.1 Platform for Windows 10 ..... 5
2.1.1 Installation for Java ..... 5
2.1.2 Installation for MariaDB ..... 9
2.1.3 Installation for VigorACS 3 ..... 14
2.1.4 StartMySQL/MariaDB Database ..... 23
2.1.5 Start VigorACS ..... 23
2.2 Platform for Linux ..... 25
2.2.1 Installation for MariaDB, Java and VigorACS ..... 25
2.2.2 StartMySQL/MariaDB Databse ..... 30
2.2.3 Start InfluxDB ..... 30
2.2.4 Start VigorACS ..... 31
2.2.5 Edit VigorACS IP ..... 31
2.3 Registering VigorACS ..... 32
2.3.1 Registration for VigorACS via Windows Platform ..... 32
2.3.2 Troubleshooting for Unstable CPE Status ..... 37

Chapter 3 Getting Started ..... 41

3.1 Accessing Web Page of VigorACS ..... 41
3.2 Dashboard ..... 42
3.2.1 Dashboard for Root Network ..... 42
3.2.2 Dashboard for a Network Group ..... 43
3.2.3 Dashboard for a Device ..... 44
3.2.4 Menu Bar ..... 45
3.2.5 Root Network, Group Network, and Selected CPE ..... 46
3.2.6 Capture Packets ..... 47
3.2.7 Set Password, Two-factor Authentication, Change and Log Out ..... 50
3.2.8 Auto Refresh, Manual Refresh, and Widget ..... 55
3.2.9 Overviews ..... 56
3.2.10 Icons Used in VigorACS 3 ..... 62
3.3 Operation Procedure ..... 62
Applications ..... 63
A.1 How to Register a CPE onto VigorACS 3? ..... 63
A.2 How to Create a New Network? ..... 65
A.3 How to Assign a New Added CPE to a Network? ..... 67
A.4 How to Create a New User Group? ..... 68

**Part II** ..... **71**

Chapter 4 SD-WAN Solution ..... 72

4.1 Topology of SD-WAN, Edge Router and ACS Server ..... 72
4.1.1 Enabling SD-WAN on VigorACS ..... 73
4.1.2 Auto VPN ..... 74
4.1.3 VoIP WAN ..... 75
4.1.4 Full Traffic Control with the Route Policy ..... 76
4.2 Dashboard for SD-WAN Network Group ..... 77
4.3 Statistics for SD-WAN Network Group ..... 79
4.4 Monitoring for SD-WAN Network Group ..... 79
4.4.1 WAN (SD-WAN) ..... 80
4.4.2 VPN (SD-WAN) ..... 81
4.4.3 VoIP (SD-WAN) ..... 87
4.4.4 Data Usage (SD-WAN) ..... 88

Chapter 5 SD-WAN CPE ..... 90

5.1 Dashboard for SD-WAN CPE ..... 90

5.2 Statistics for SD-WAN CPE ..... 92
5.3 Monitoring for SD-WAN CPE ..... 92
5.3.1 Alarm ..... 93
5.3.2 Logs ..... 94
5.3.3 Diagnostics ..... 95
5.3.4 GPS ..... 99
5.3.5 WAN (SD-WAN) ..... 99
5.3.6 VPN (SD-WAN) ..... 100
5.3.7 VoIP (SD-WAN) ..... 101
5.3.8 Data Usage (SD-WAN) ..... 102
5.4 Configuration Menu for SD-WAN CPE ..... 104

**Part III ..... 105**

Chapter 6 System Menu ..... 106

6.1 Maintenance ..... 106
6.1.1 Scheduled Backup ..... 107
6.1.2 Configuration Restore ..... 110
6.1.3 Firmware Upgrade ..... 114
6.1.4 Device Reboot ..... 117
6.1.5 System Password Reset ..... 120
6.1.6 Schedule Profile ..... 121
6.1.7 File Manager ..... 122
6.1.8 Batch Activation ..... 124
6.2 Reports ..... 128
6.2.1 Report Tasks ..... 128
6.2.2 Reports ..... 132
6.3 Provisioning ..... 134
6.3.1 Global Parameters ..... 134
6.3.2 CPE Set Parameters ..... 139
6.3.3 CPE Keep Parameters ..... 142
6.3.4 Firmware Upgrade ..... 143
6.4 Network Management ..... 146
6.4.1 Setting ..... 147
6.4.2 Map ..... 153
6.5 System ..... 154
6.5.1 System Parameter ..... 154
6.5.2 Language ..... 162
6.5.3 External Monitoring Server ..... 163
6.5.4 Access Control ..... 164
6.5.5 Clear Logs ..... 168
6.5.6 Upload Serial Number ..... 169
6.5.7 Google API Key ..... 170
6.5.8 Certificate ..... 170
6.5.9 Backup Database ..... 174
6.5.10 Login Bulletin ..... 179
6.5.11 Adverts Carousel ..... 183
6.5.12 Logs ..... 188
6.5.13 Delete Logs Actions ..... 189
6.6 User ..... 191
6.6.1 User Management ..... 191
6.6.2 Group Management ..... 194
6.6.3 Network Group ..... 197
6.6.4 External Authentication Server ..... 197
6.6.5 Mail Server ..... 200
6.6.6 Function Management ..... 201
6.6.7 Wholesale Wizard ..... 201
6.6.8 SMS Server ..... 204
6.6.9 SNMP Server ..... 205
6.7 About VigorACS ..... 206
6.7.1 License Information ..... 207
6.7.2 License Mail Notify ..... 208
6.7.3 License Agreements ..... 209
Applications ..... 210
A.1 How to Create a Provision Profile with Global Parameters? ..... 210

A.2 How to Modify Provision Profile with Global Parameters? ... 211
A.3 How to Create a Network for Managing Devices? ... 213
A.4 How to Change the Network of a Device? ... 214
A.5 How to Add a User? ... 217
A.6 How to Add a Group? ... 218

**Part IV ... 221**

Chapter 7 Root Network Menu ... 222

7.1 Dashboard for the Root Network ... 222
7.2 Monitoring ... 223
7.2.1 Alarm ... 224
7.2.2 Logs ... 225
7.2.3 Devices ... 226
7.2.4 Cellular Data Usage ... 227
7.2.5 Floor Plan ... 228
7.2.6 Rogue AP Detection ... 233
7.3 Configuration ... 236
7.3.1 VPN ... 236
7.3.2 AP Profile ... 236

Chapter 8 Network Group Menu ... 242

8.1 Dashboard for the Network Group ... 242
8.2 Statistics for Network Group ... 244
8.3 Monitoring for Network Group ... 245
8.3.1 Alarm ... 246
8.3.2 Logs ... 247
8.3.3 Devices ... 247
8.3.4 Clients ... 249
8.3.5 Cellular Data Usage ... 250
8.3.6 Floor Plan ... 251
8.3.7 Rouge AP Detection ... 256
8.3.8 WAN (SD-WAN), VPN (SD-WAN), VoIP (SD-WAN), Data Usage (SD-WAN) ... 258
8.4 Configuration Menu for Network Group, ... 259
8.4.1 VPN ... 259
8.4.2 AP Profile ... 260
8.4.3 Load Balance ... 264
8.4.4 Route Policy (SD-WAN) ... 265
8.4.5 VoIP WAN (SD-WAN) ... 269
8.5 Hotspot Web Portal for SD-WAN Network Group ... 271
8.5.1 Profile ... 271
8.5.2 Quota Management ... 280
8.5.3 Network & Devices ... 282
8.5.4 Analytics ... 283
Applications ... 284
A.1 How to apply an AP profile to AP device(s)? ... 284

**Part V ... 285**

Chapter 9 Device Menu ... 286

9.1 Dashboard for CPE ... 286
9.2 Statistics for CPE ... 287
9.3 Monitoring ... 288
9.3.1 Alarm ... 288
9.3.2 Logs ... 289
9.3.3 Diagnostics ... 290
9.4 Configuration ... 293
9.4.1 WAN ... 295
9.4.2 LAN ... 312
9.4.3 Hotspot Web Portal ... 323
9.4.4 Routing ... 337
9.4.5 NAT ... 344
9.4.6 Hardware Acceleration ... 350
9.4.7 Firewall ... 351

9.4.8 User Management ..... 365
9.4.9 Object Setting ..... 368
9.4.10 QoS ..... 385
9.4.11 Applications ..... 389
9.4.12 VPN ..... 407
9.4.13 Mesh ..... 419
9.4.14 Wireless LAN ..... 422
9.4.14 Bandwidth Management ..... 435
9.4.15 USB Applications ..... 440
9.4.16 System ..... 444
9.4.17 Switch ..... 458
9.4.18 Advanced ..... 470

# Part I

Introduction

# Chapter 1 Introduction

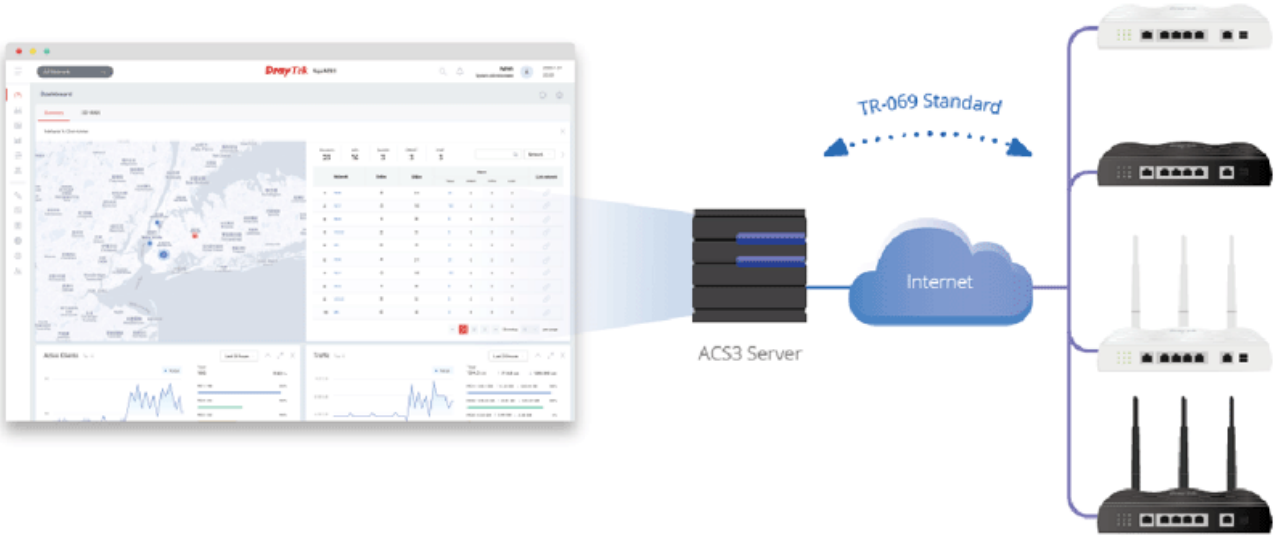
VigorACS 3 is a software which provides centralized device management for TR-069 based CPEs such as broadband gateway, XDSL router, VoIP gateway, wireless AP **and switch**. VigorACS 3 has device status, monitor status of devices, or perform scheduling tasks such as firmware upgrade, configuration backup/restore and parameter profile for mass deployment of CPE devices. It is easy to use through intuitive Web-based GUI with security management. VigorACS 3 can be installed on different kinds of platform e.g., **Windows, Linux** and so on.

## 1.1 Main Features and Benefit

- Manage all kinds of devices complied with TR-069 specification.
- VigorACS 3 server can be installed in Windows and Linux.
- Intuitive Web-based GUI can be executed on all browsers like Edge, Firefox, Chrome and so on.
- Support scheduling firmware upgrade, configuration backup/restore and parameter profile deployment.
- Support auto-discovery to survey all TR-069 devices.
- Provide device inform management.
- Support security management.

## 1.2 System Architecture

The following figure shows an overview for the application between VigorACS 3 and CPE devices. With TR-069 protocol, VigorACS 3 can communicate and manage devices with ease.



## 1.3 Web Service

Web service is a software system identified by a URI, whose public interfaces and bindings are defined and described using XML. Its definition can be discovered by other software systems. These systems may then interact with the Web service in a manner prescribed by its definition, using XML based messages conveyed by internet protocols.

The basis for Web Services contains: XML, WSDL (Web Services Description Language), SOAP (Simple Object Access Protocol), UDDI(Universal Description, Discovery and Integration). The procedure for the structure of bottom layer: transform Web Service information into XML file format, use WSDL statement to describe the objects for service. The remote end can get required information through such description. It carries out transformation job to search or register from UDDI by means of SOAP communication bottom layer.

- For the designers of Java program: you can write java program to control VigorACS. Also, VigorACS will offer some API for you to write and call it. For example, you can get all the connected CPE devices controlled VigorACS through web service.

  Corresponding files are placed in -
  WebServices_TR069API.zip

  The documentation for web services api is placed in -
  WebServices_TR069API/doc/

  Sample program is placed in -
  WebServices_TR069API/example/src/tw/com/draytek/acs/test/TestMain.java

- For the designers with other program language: you can define WSDL to control VigorACS through SOAP(Simple Object Access Protocol)

This page is left blank.

# Chapter 2 Install & Startup

Please follow the procedure listed below to install VigorACS completely. The installation for different platforms might be different.

VigorACS 3 can be operated only by a host with 64-bit operation system.

## 2.1 Platform for Windows 10

To start up the VigorACS, the normal procedure is listed as follows:

(I) Installation for Java,

(II) Installation for MariaDB

(III) Installation for VigorACS 3

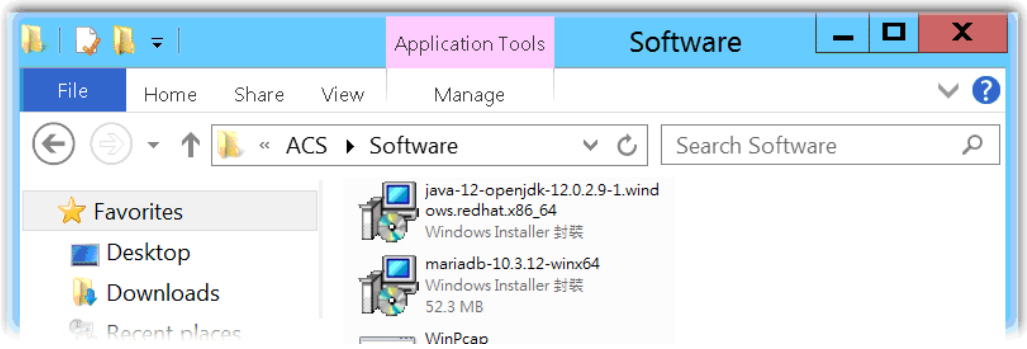
(IV) Start MySQL/MariaDB Database.

(V) Edit VigorACS ip.

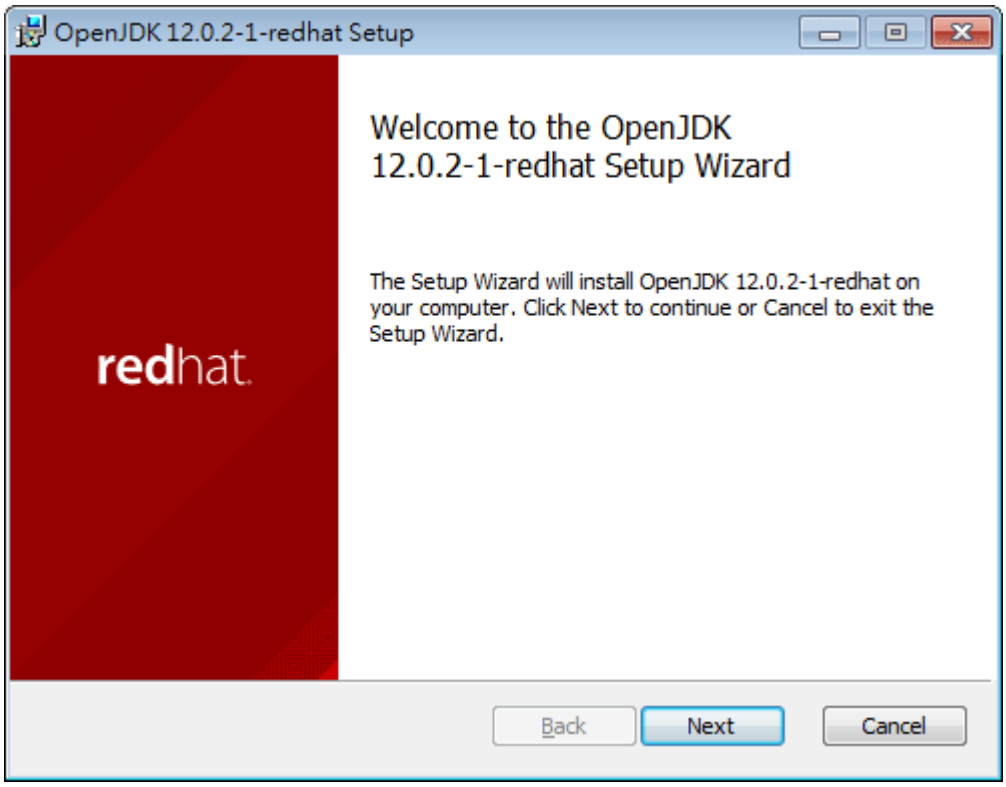
(VI) Start VigorACS.

### 2.1.1 Installation for Java

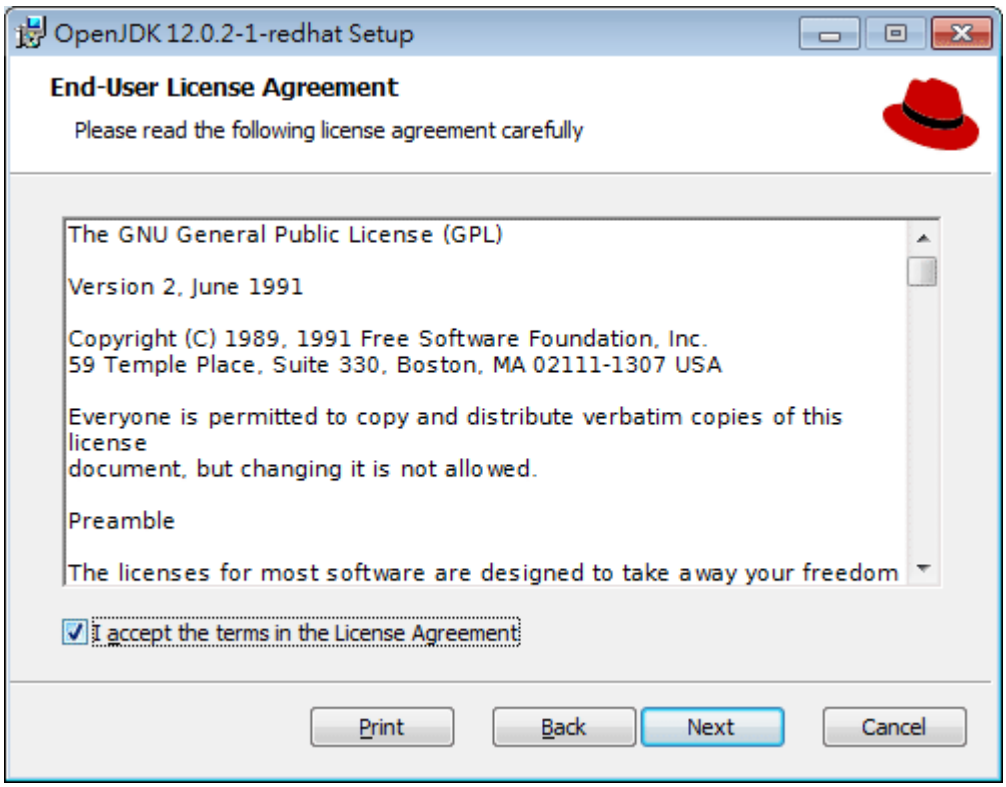
1. Install Java by clicking “java-12-openjdk-12.0.2.9-1.windows.redhat.x86_64” (or later) to execute the installation.



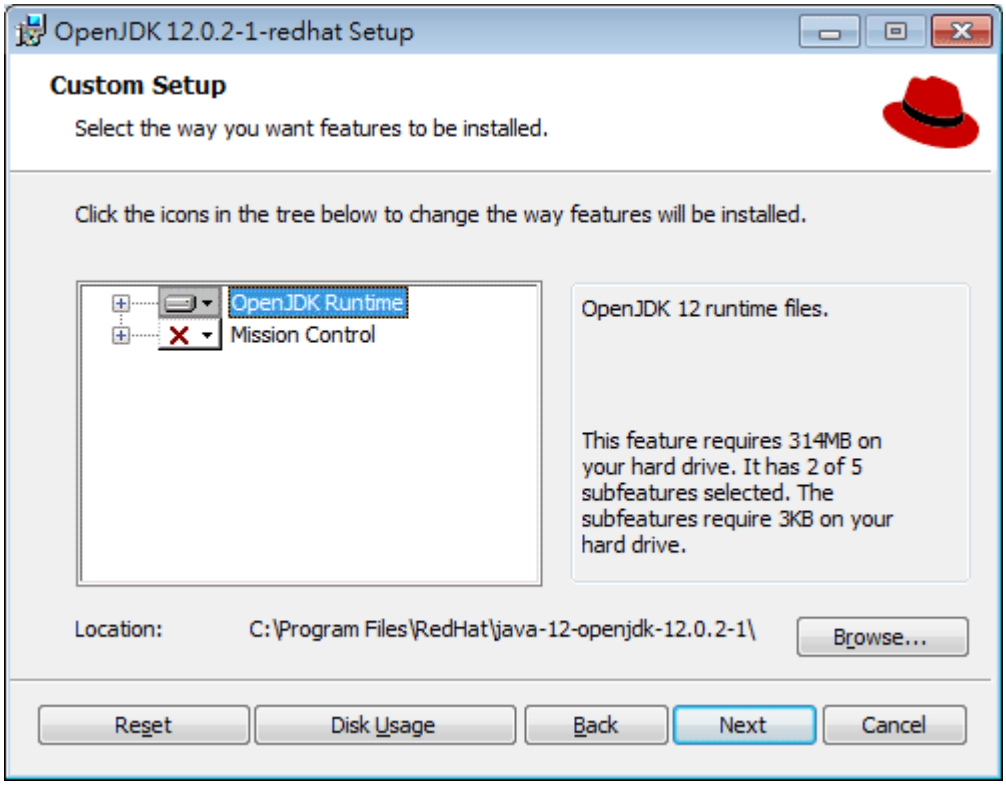
2. The first page will be shown as follows. Click **Next** to get into next page.



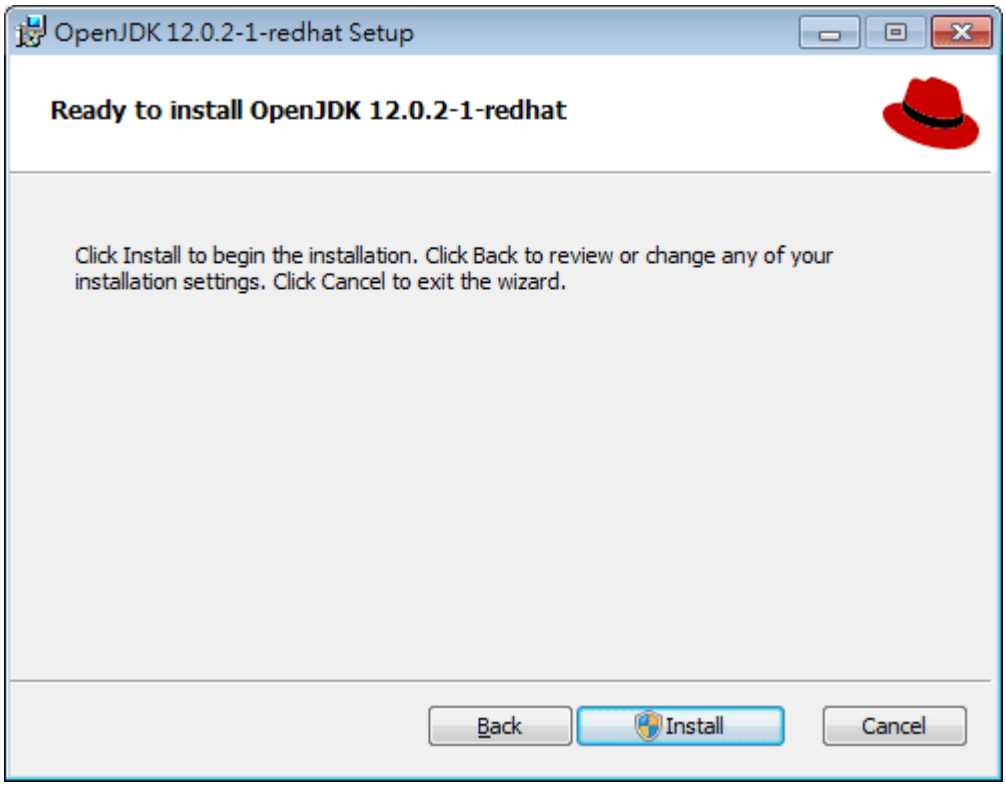

3. Then, check "I accept the terms..." and click the **Next** button.



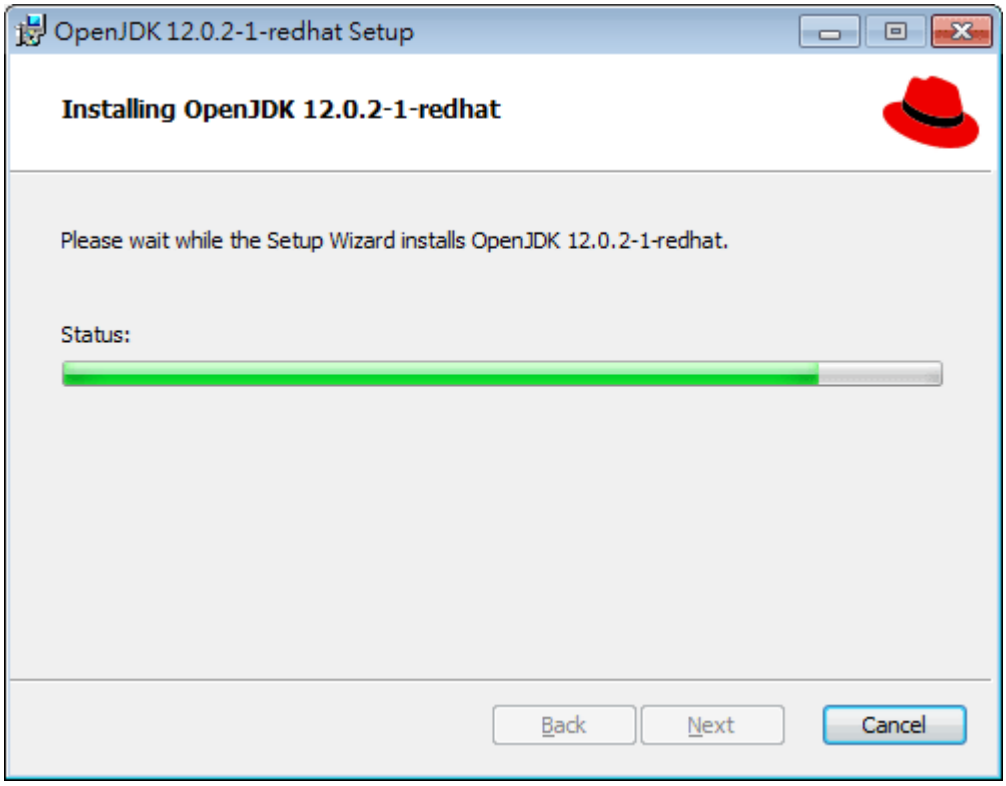
4. In this page, optional features will be listed for you to specify the destination folder for JAVA driver installation. Choose the one you need and click **Next**.



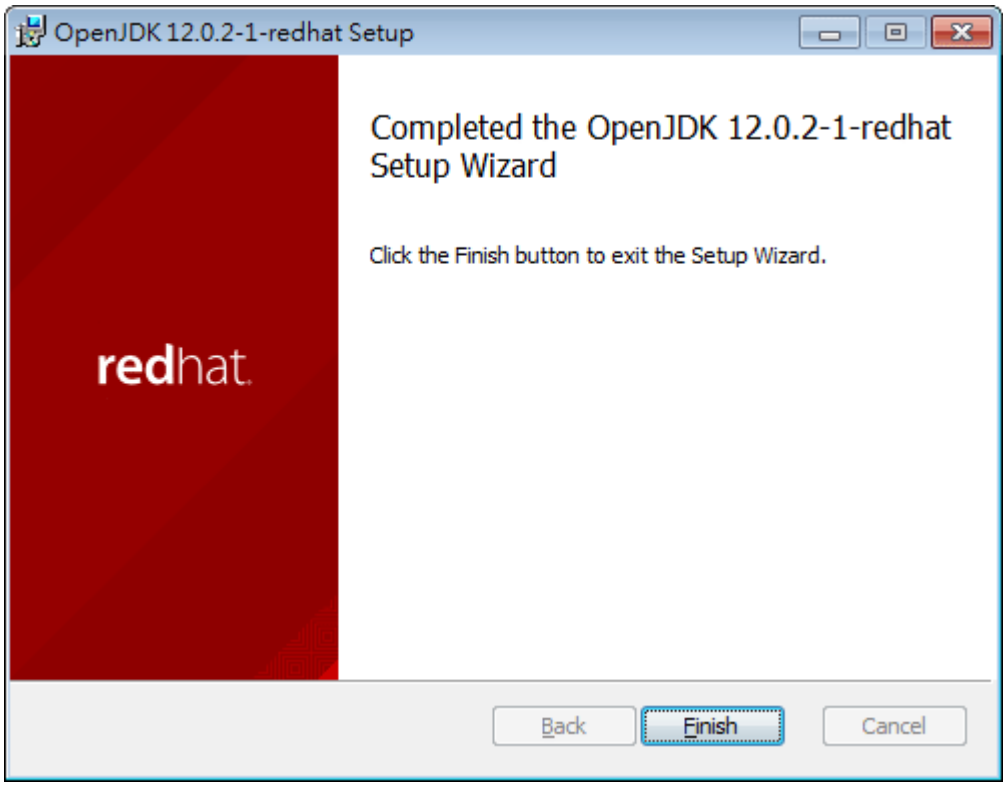

5. In the following page, just click **Install.**



6. Wait for a while to install the required features.

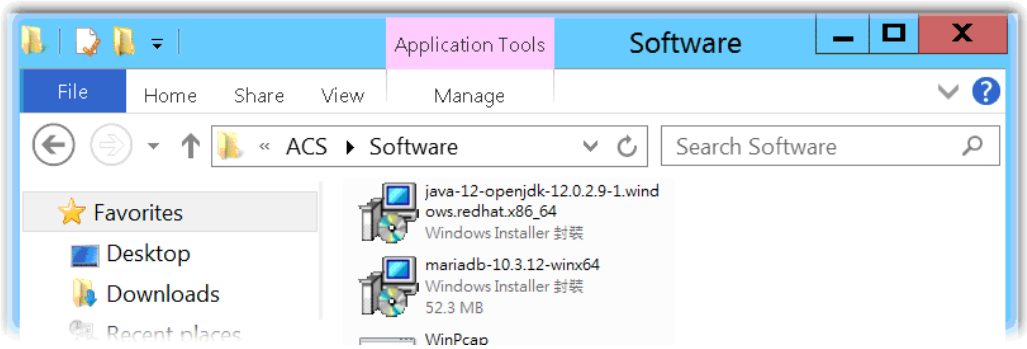



7. When the following page appears, the installation is completed. Click **Finish** to exit the installing program.



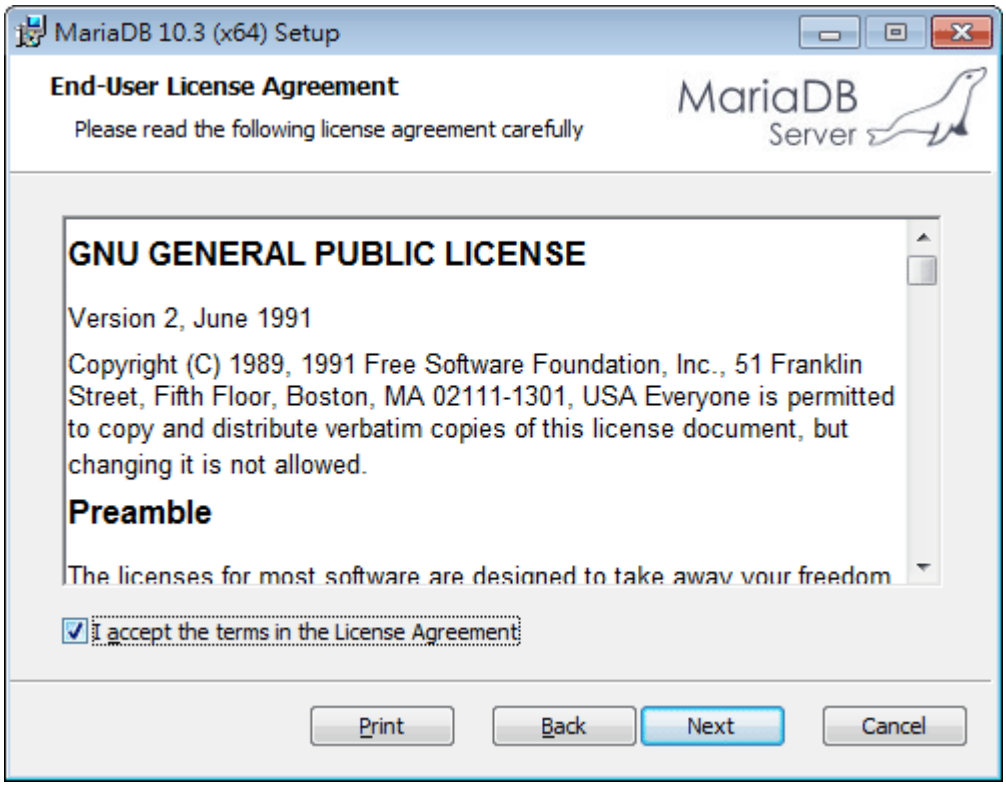
### 2.1.2 Installation for MariaDB

1. Install MariaDB by clicking “mariadb-10.3.12-winx64” (based on your PC condition) it to execute the installation.

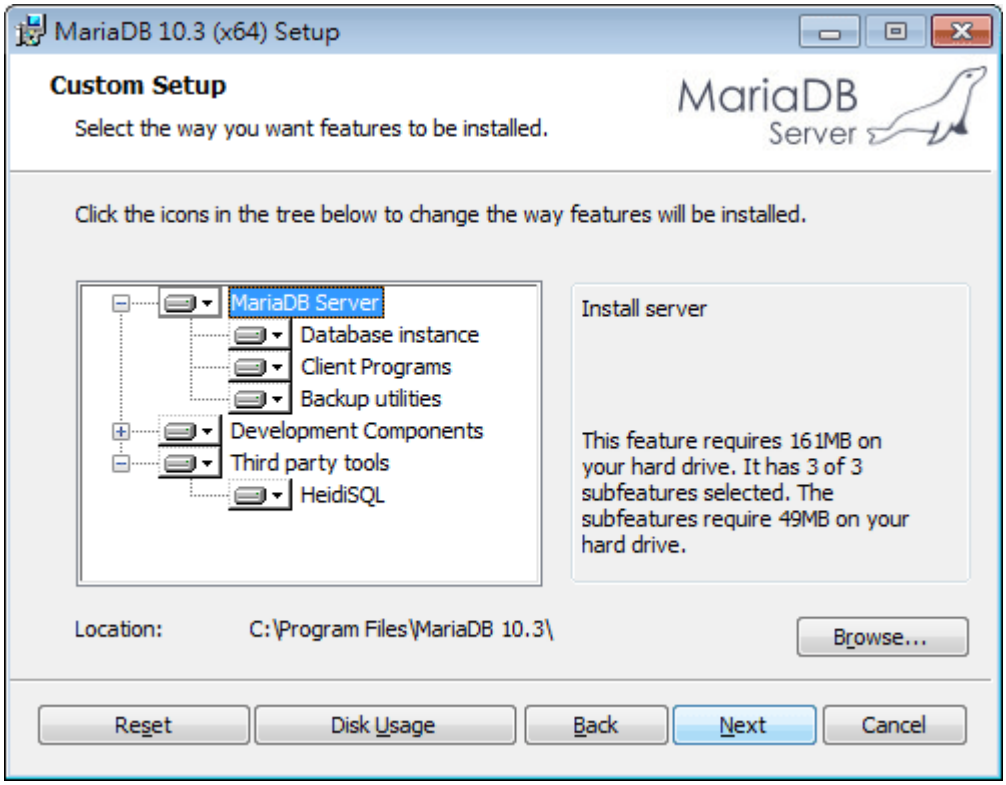



2. When the welcome screen appears, please click **Next** for next step.

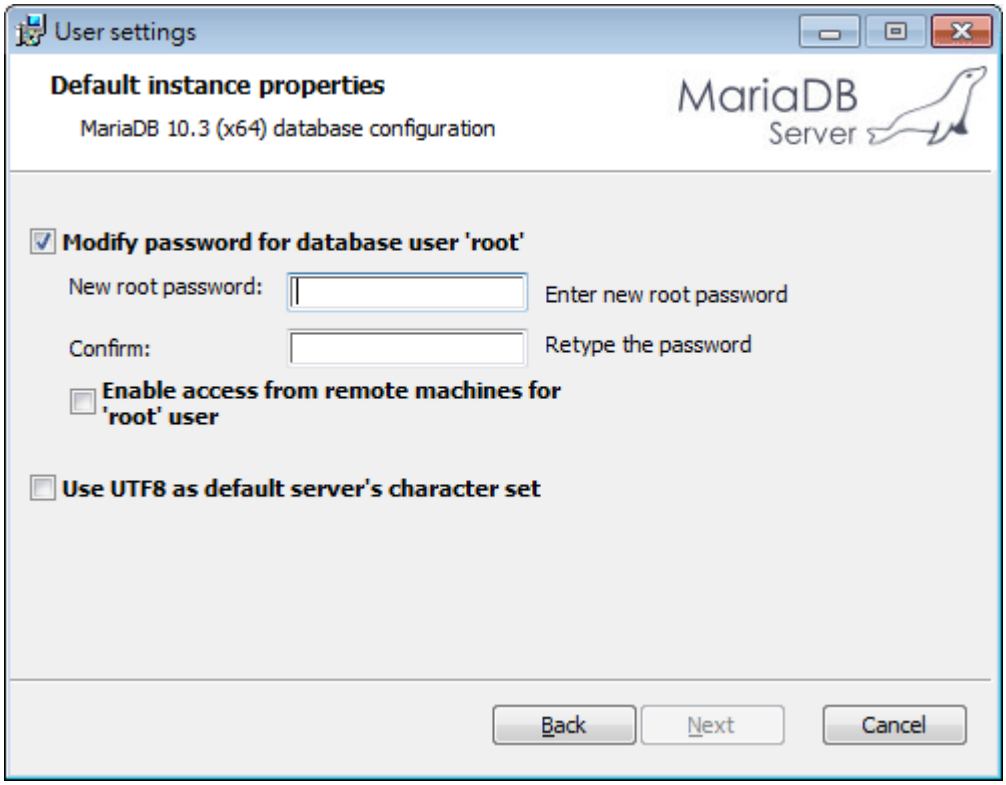
3. On this dialog box, check the box of “I accept the terms….” and click **Next**.



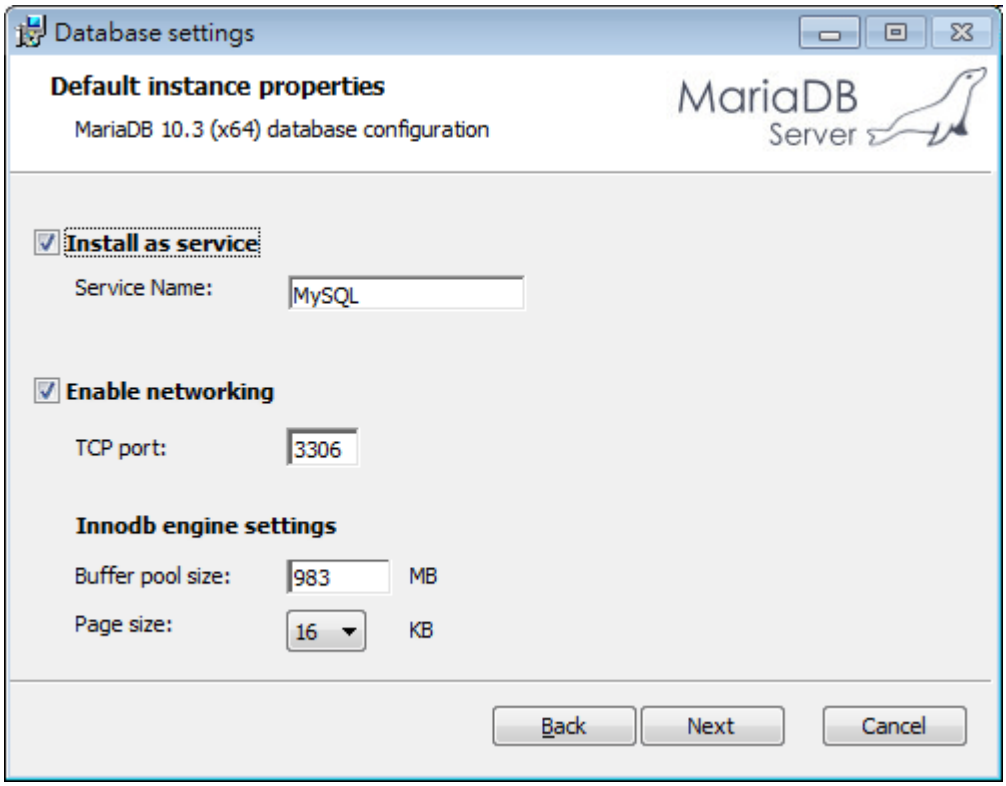

4. Select the way for the features to be installed. Then click **Next**.



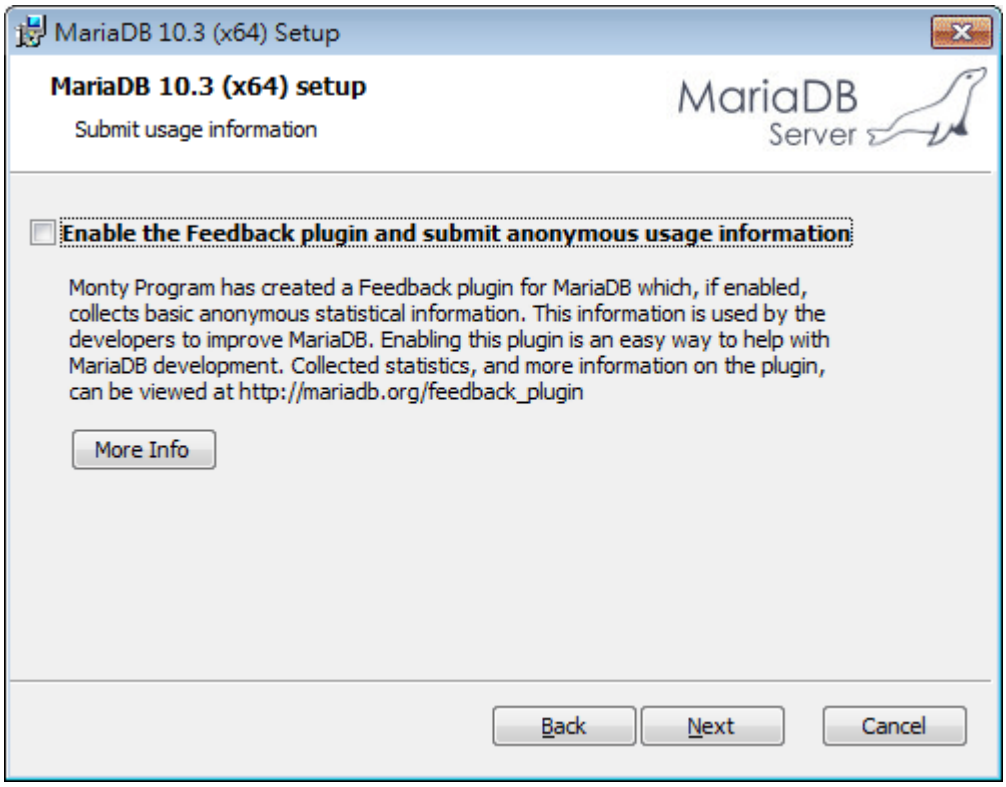
5. If you want to configure password for MariaDB server, please check **Modify password...** and enter the password. It depends on your request. Otherwise, simply click **Next**.



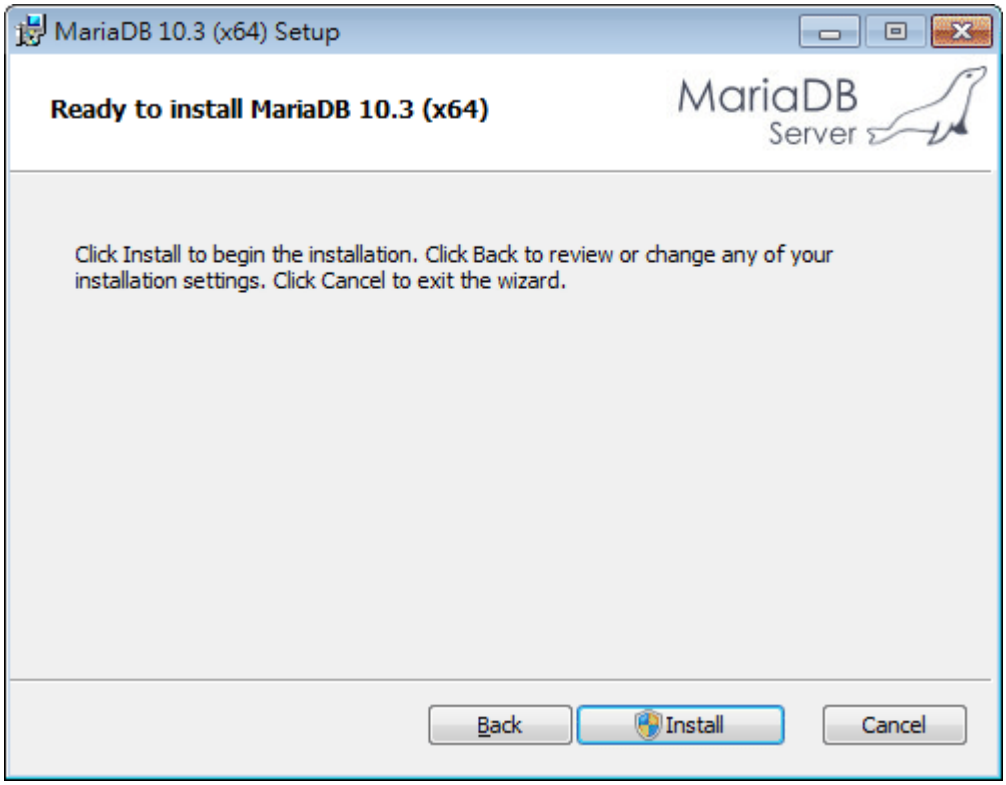

6. Modify the default instance properties if required. Then click **Next.**



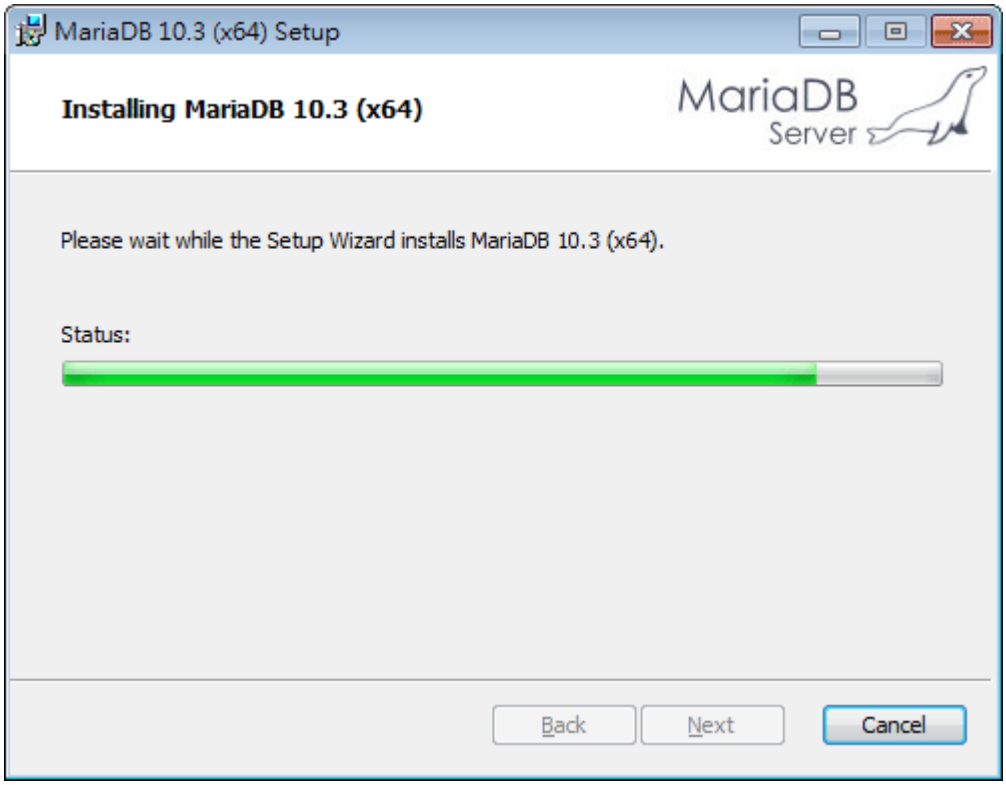
7. On this dialog box, click **Next**.



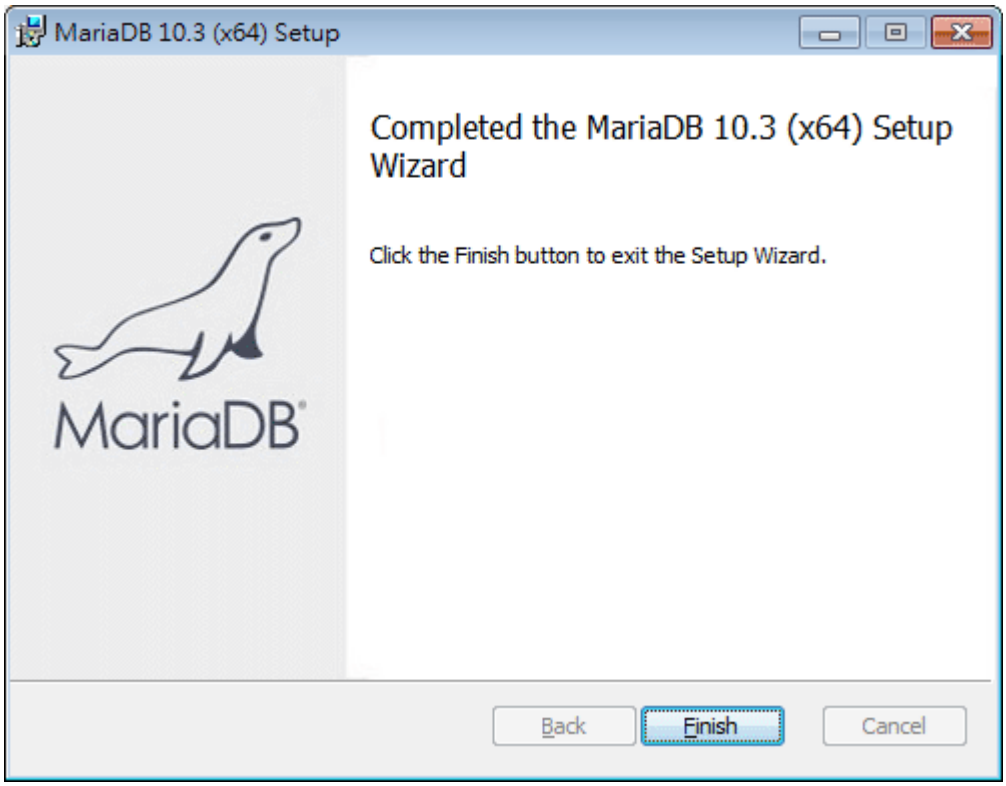

8. On this dialog box, click **Install**.



9. The installation program starts to install required files for MariaDB to your computer. Wait for several seconds.



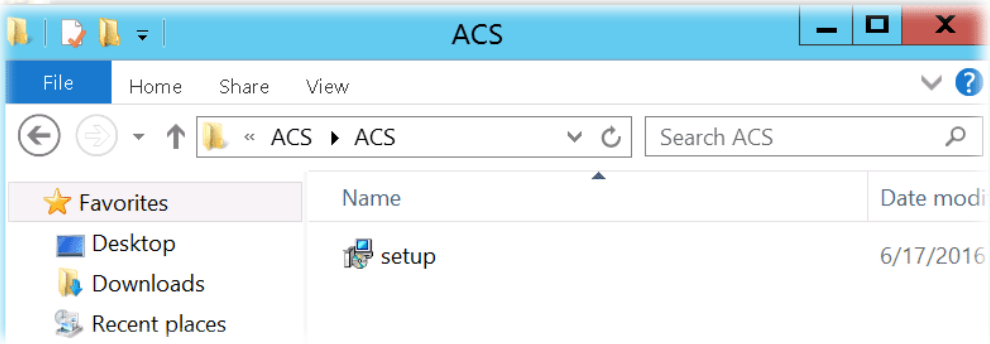

10. After finishing the configuration, please click **Finish** to exit the wizard.



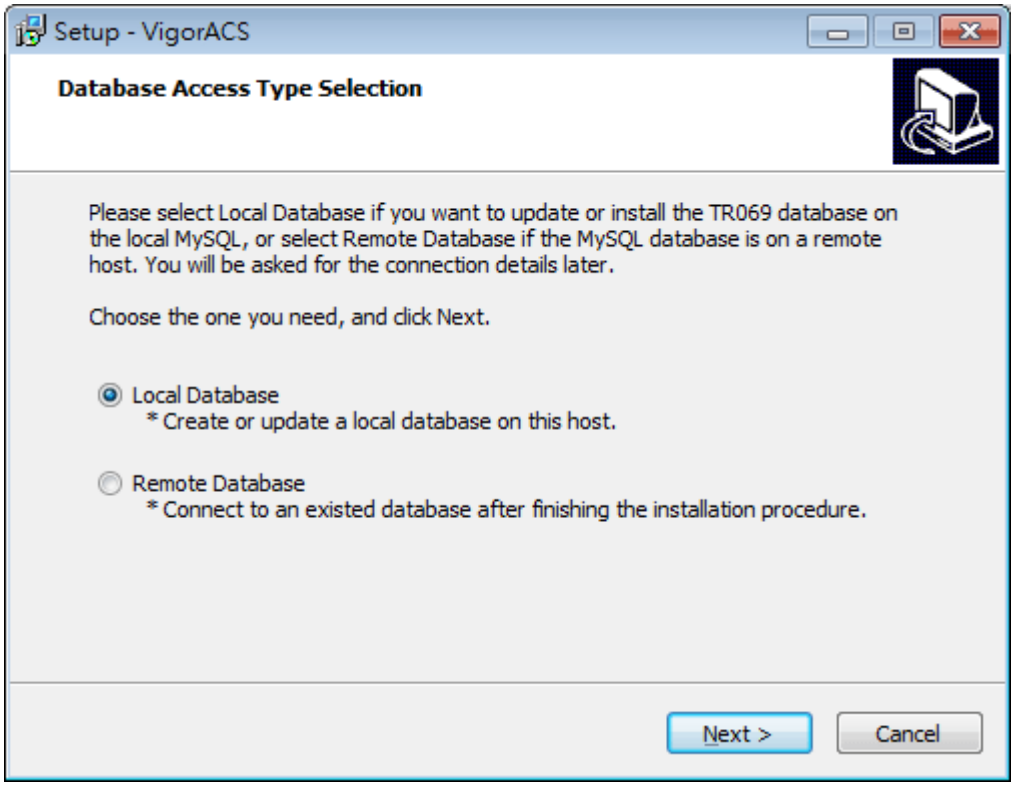
### 2.1.3 Installation for VigorACS 3

It is time to install VigorACS main program. Follow the steps below.

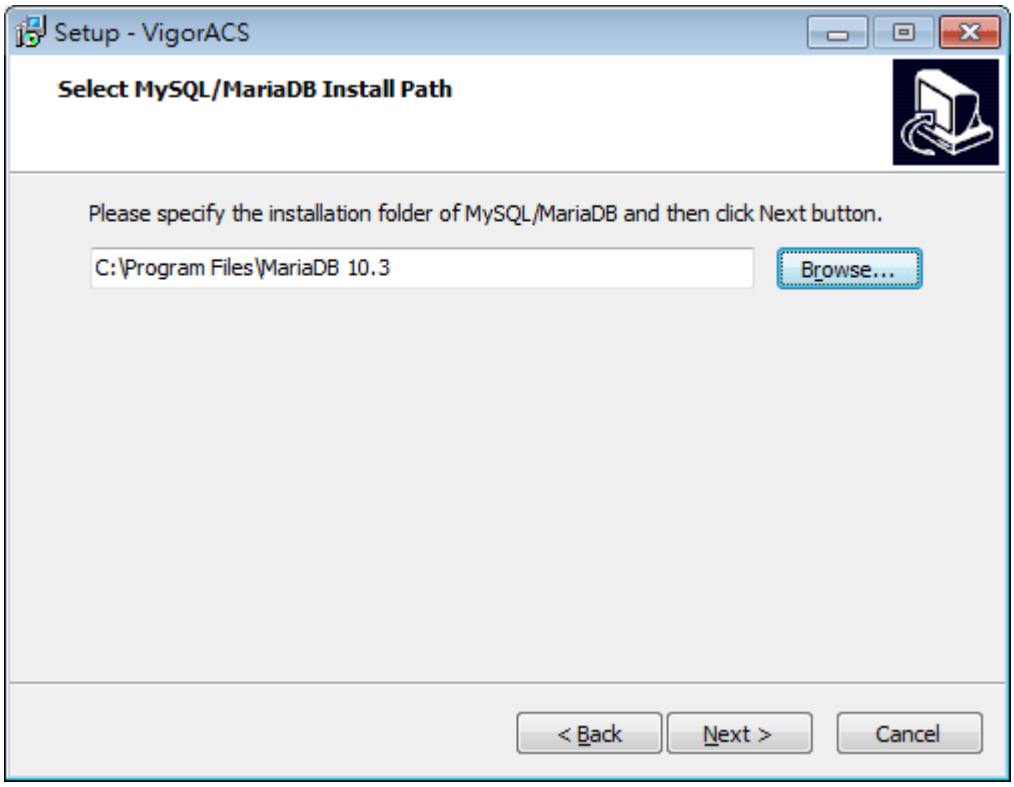
1. Click **Setup** to run VigorACS 3 setup wizard.



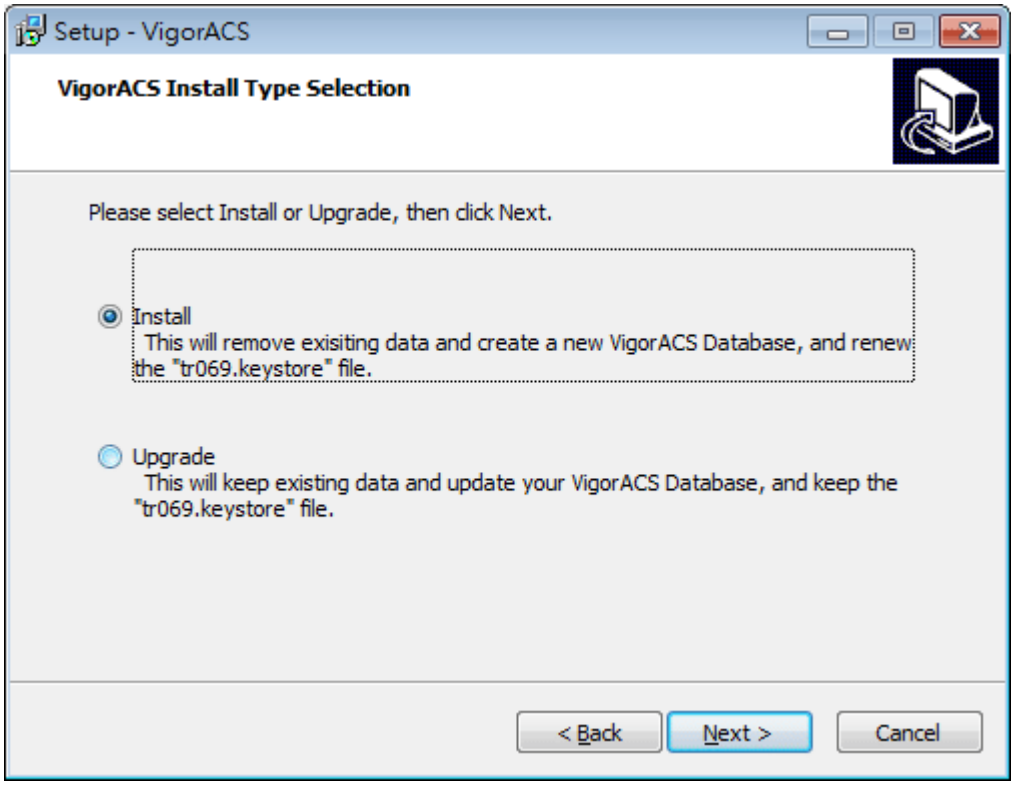

2. When the following dialog appears, choose **Local Database / Remote Database** and click **Next**.



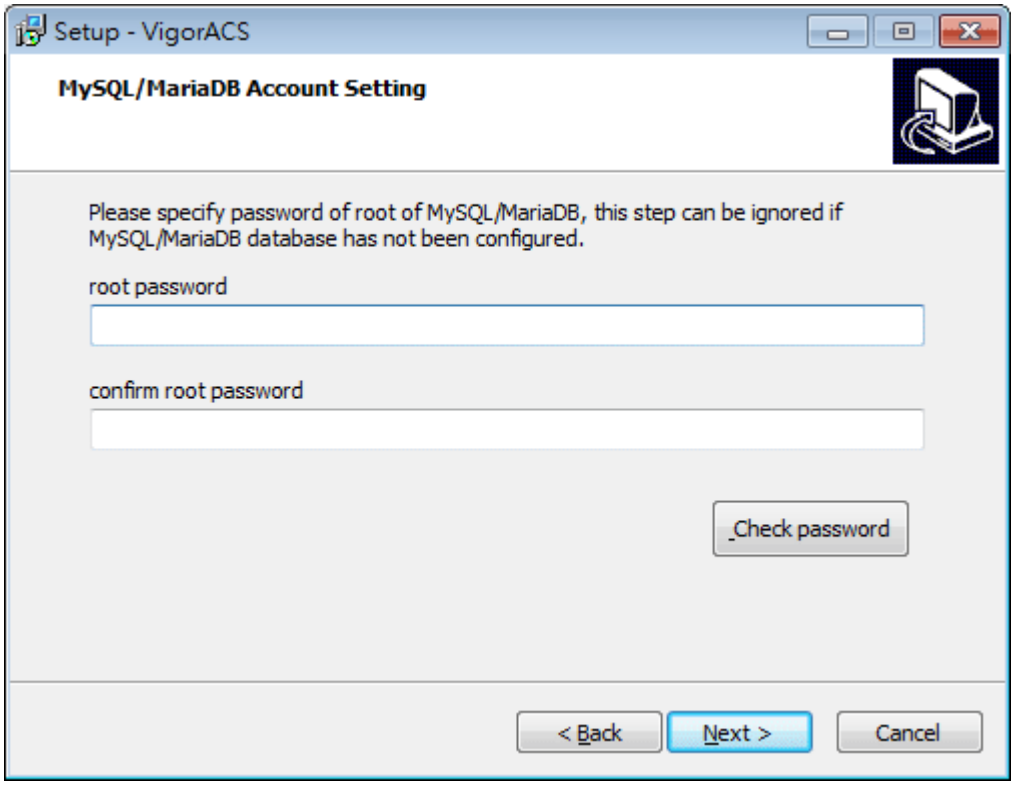
3. Select the directory that MariaDB being installed (done in 2.1.2) and click **Next.**

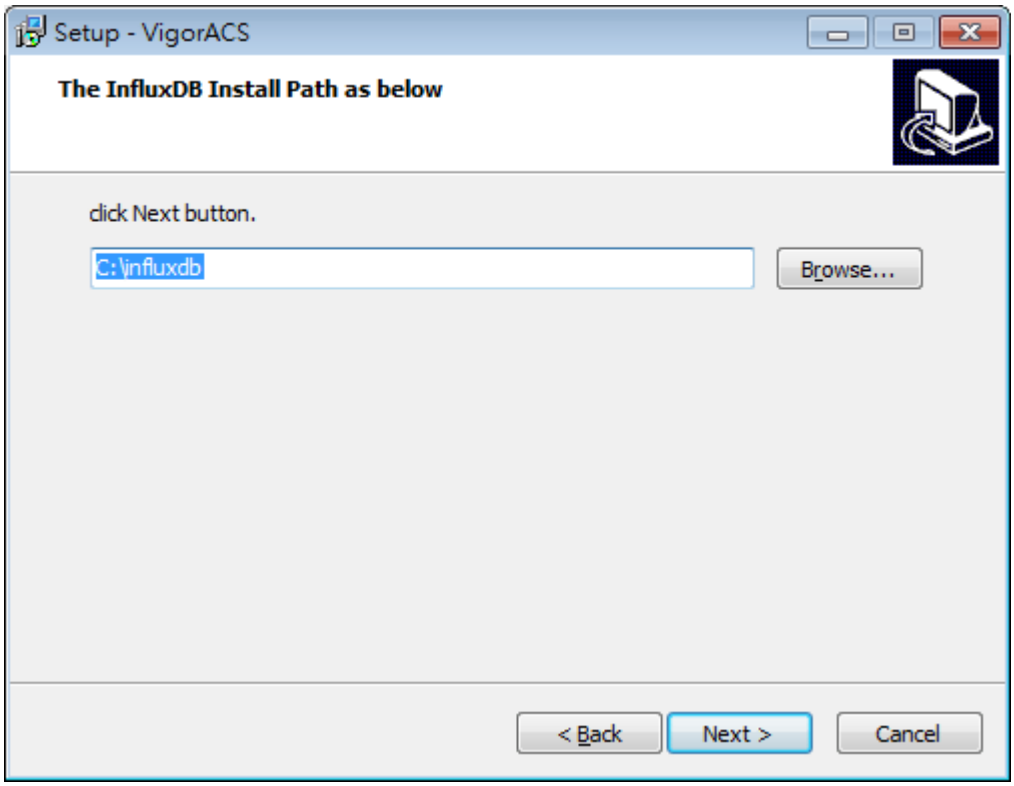



4. In this dialog box, choose **Rebuild Database** (for rebuilding the VigorACS database) or **Upgrade Database** (for upgrading the database). For the first time using, please choose **Rebuild Database**. Then click **Next**.

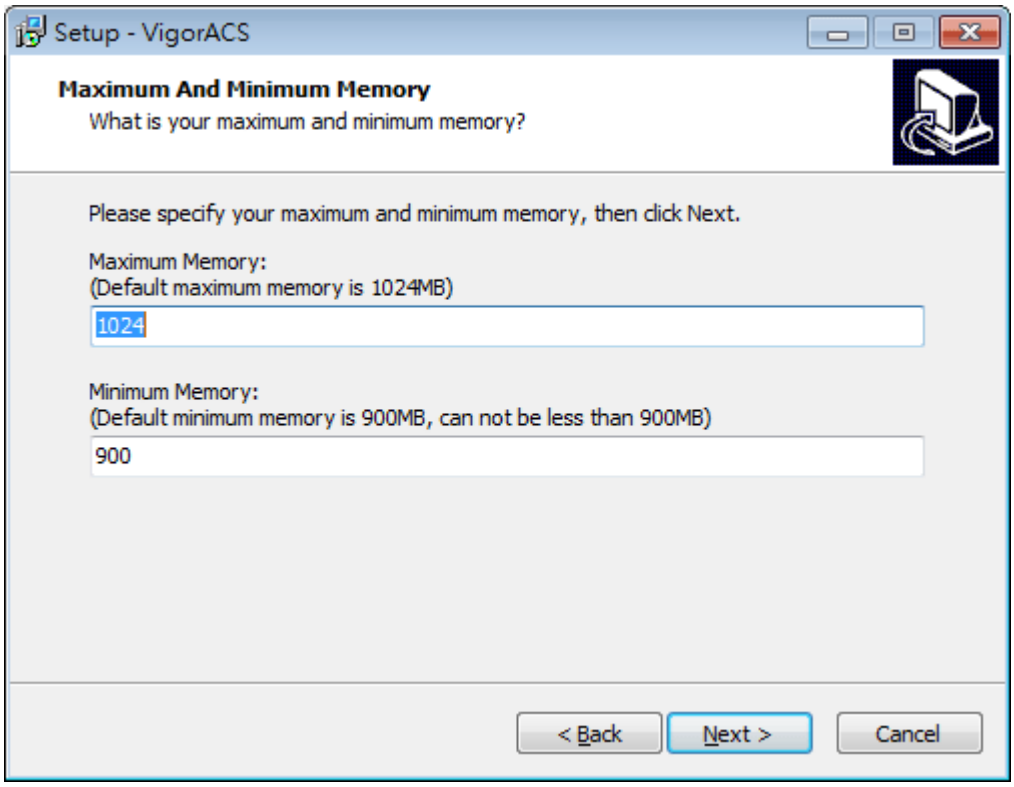


5. Click **Next**. If you have configured MySQL/MariaDB previously and specified password for it, you have to enter the password in this page and then click **Next**.

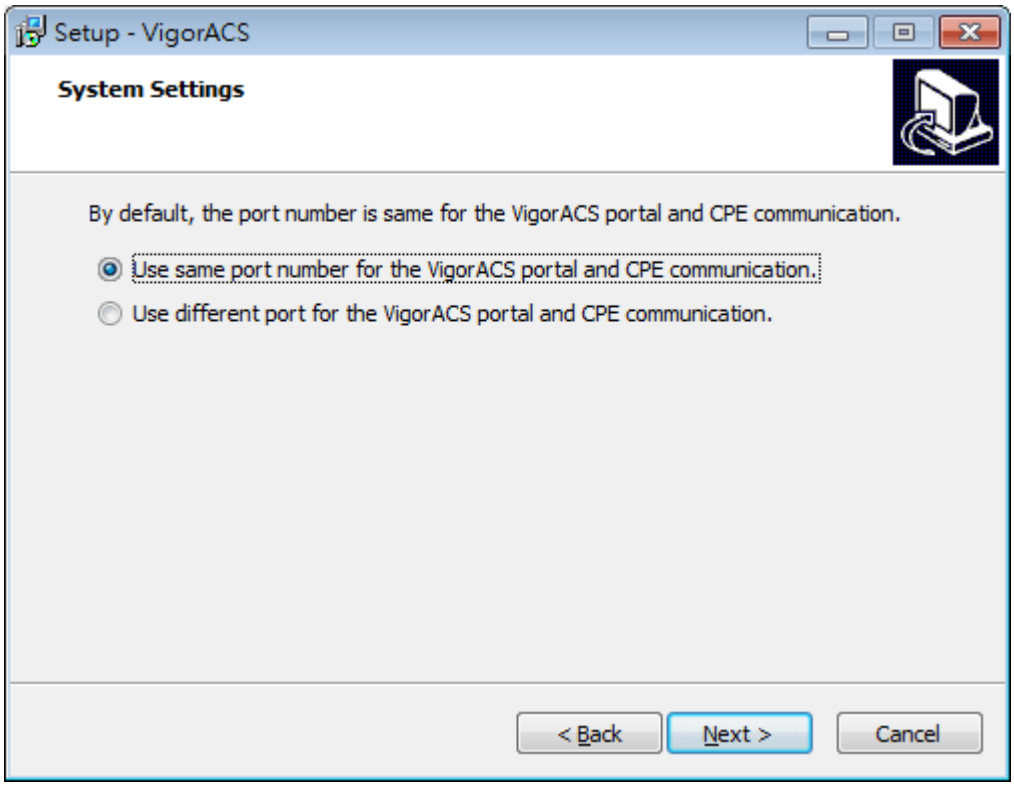


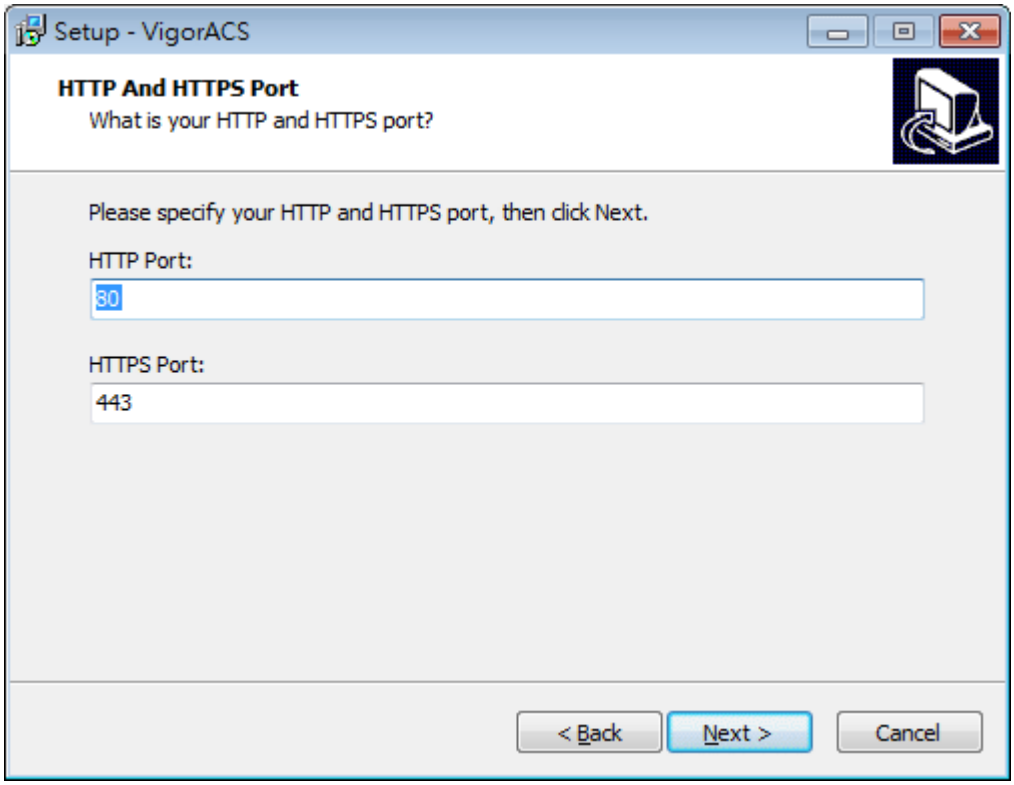
6. Set the maximum memory and minimum memory. Click **Next**.

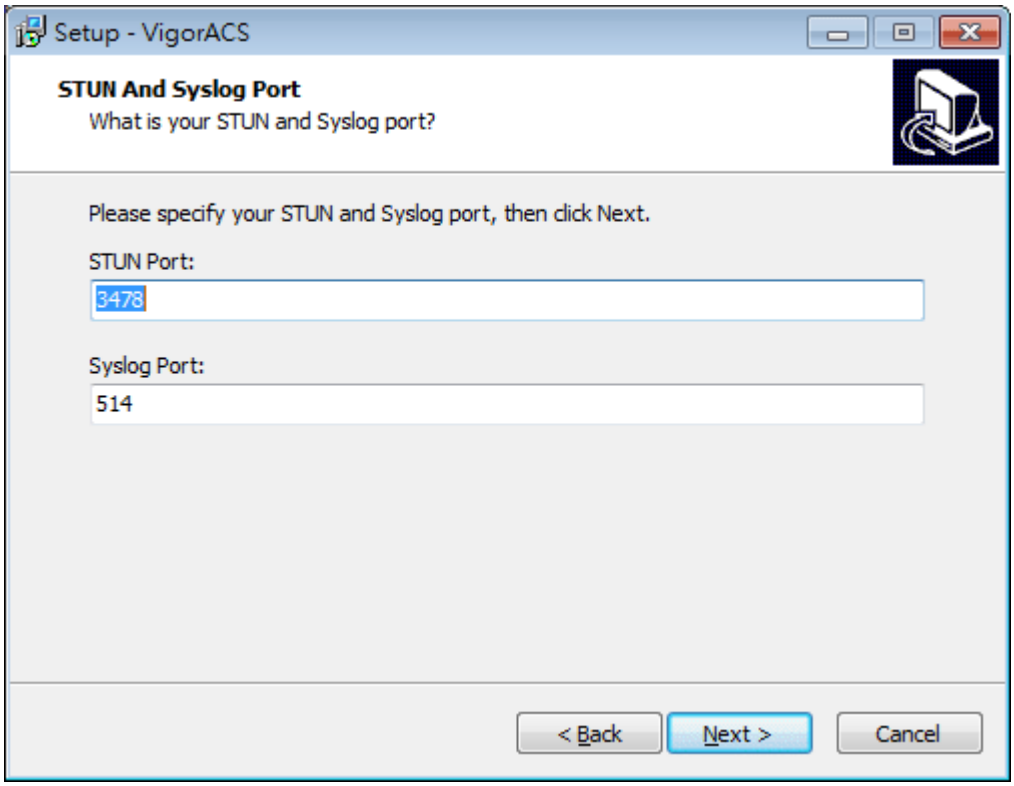



7. Setup the system settings by clicking one of the options. Here, click "Use same port number..." and click **Next**.



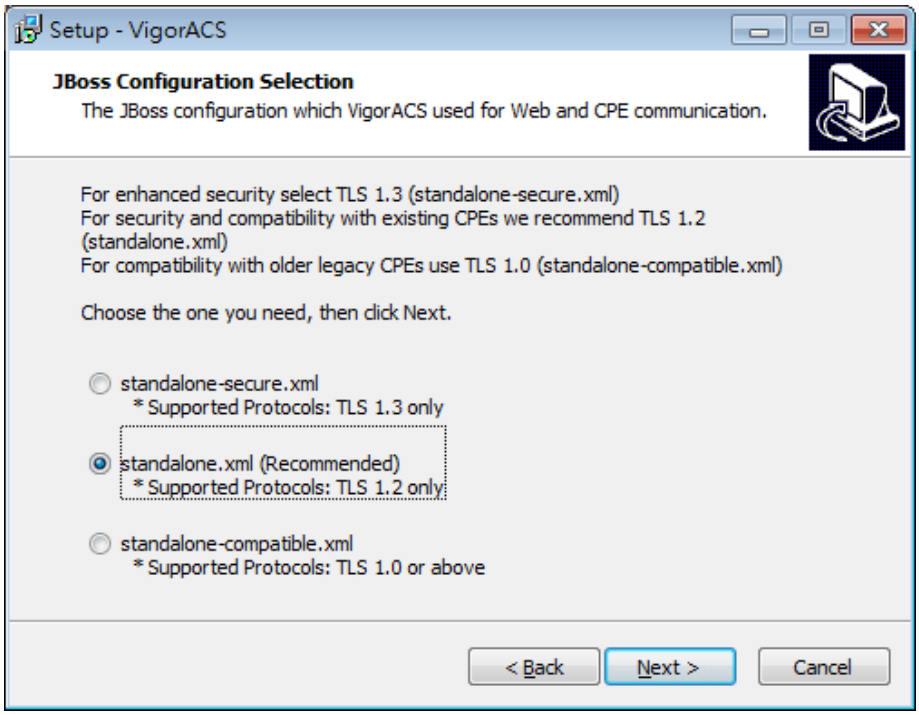
8. Setup ACS HTTP and HTTPS port. It is suggested using other port instead of default 80 and 443 port to prevent conflict.



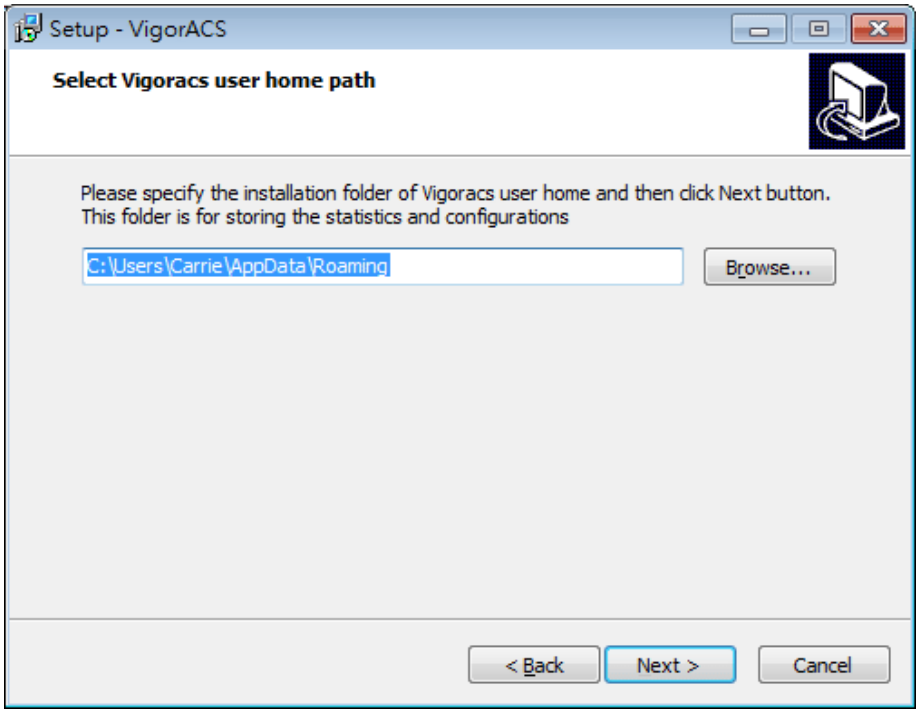




The port number defined here will be used for opening VigorACS later.

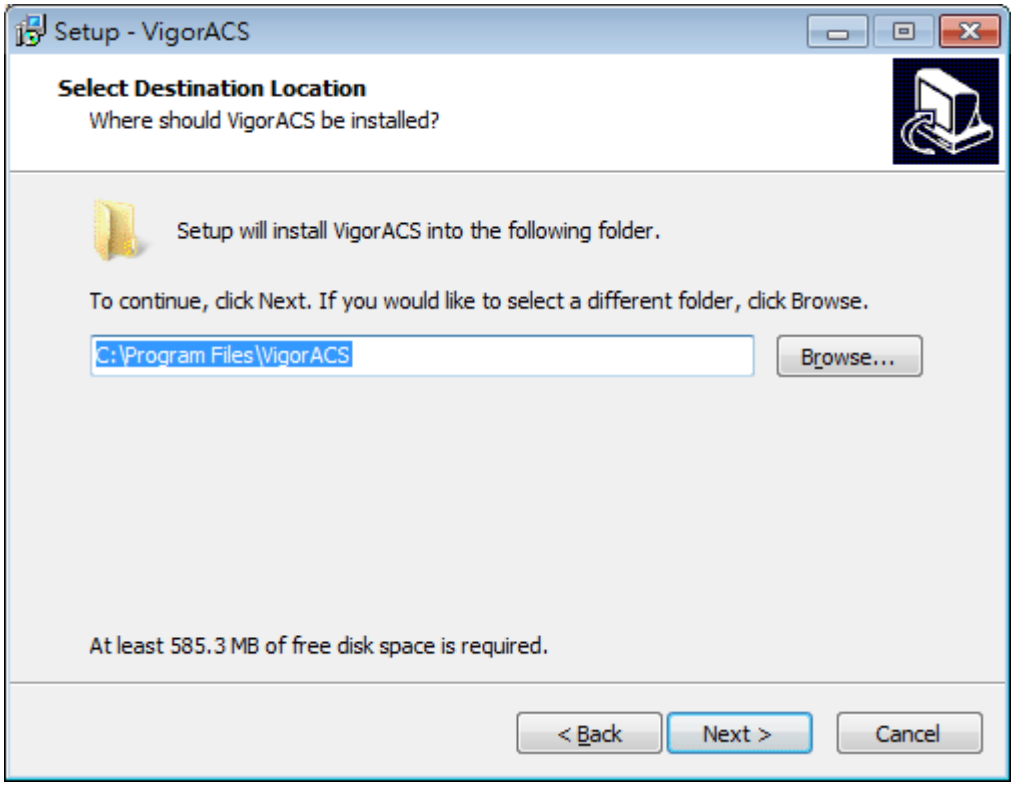
9. Use the default item (standalone.xml) and click **Next**.



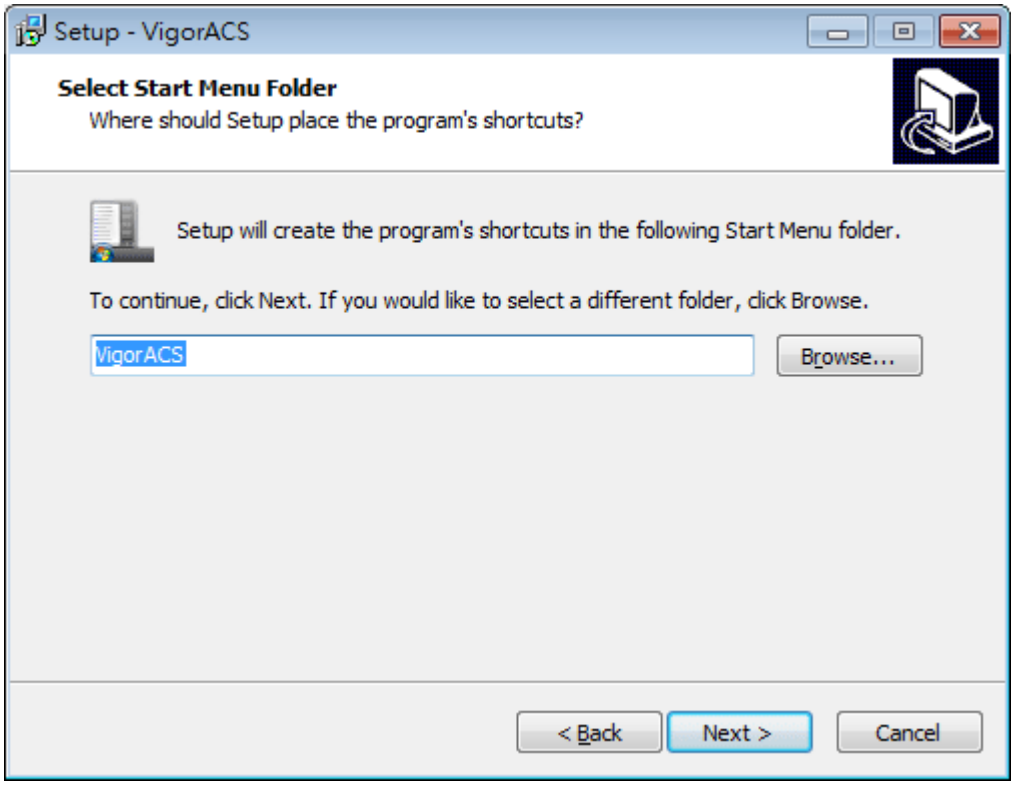

10. Determine the home path and click **Next**. The default directory used by this program is *C:\Users.* You can modify it if you want and please make sure the length of directory is not over 100 characters, otherwise you might encounter problem of VigorACS in installation.



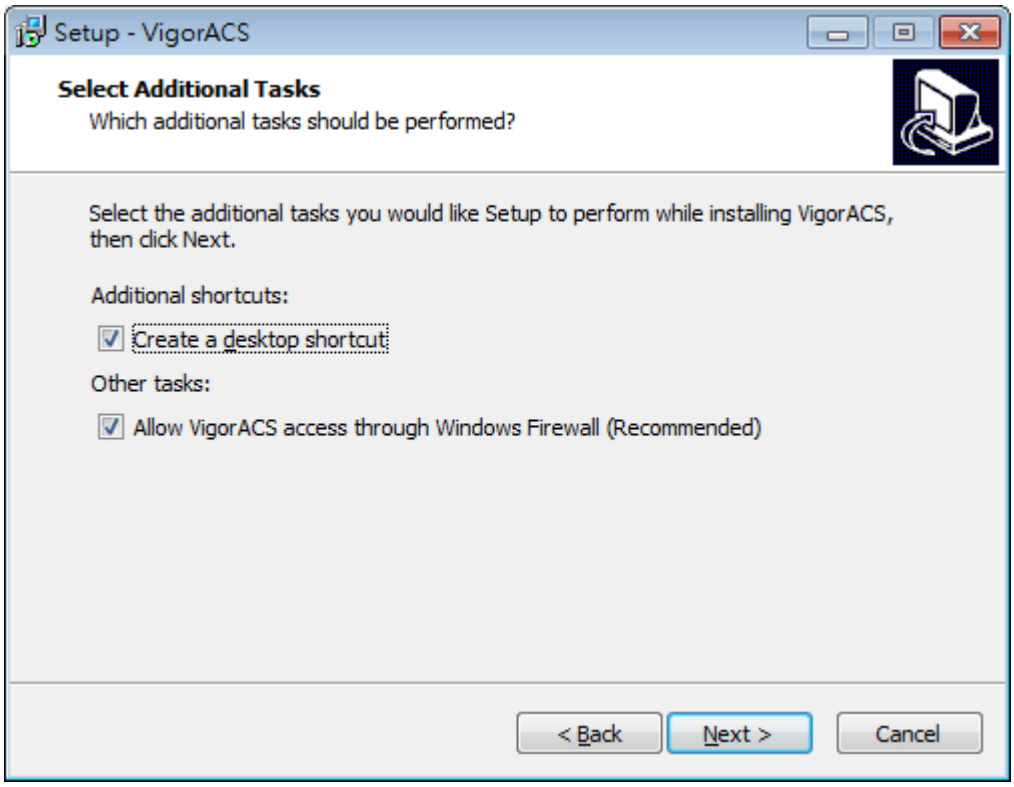
11. Determine the destination folder and click **Next**. The default directory used by this program is *C:\Program Files\VigorACS.* You can modify it if you want and please make sure the length of directory is not over 100 characters, otherwise you might encounter problem of VigorACS in installation.



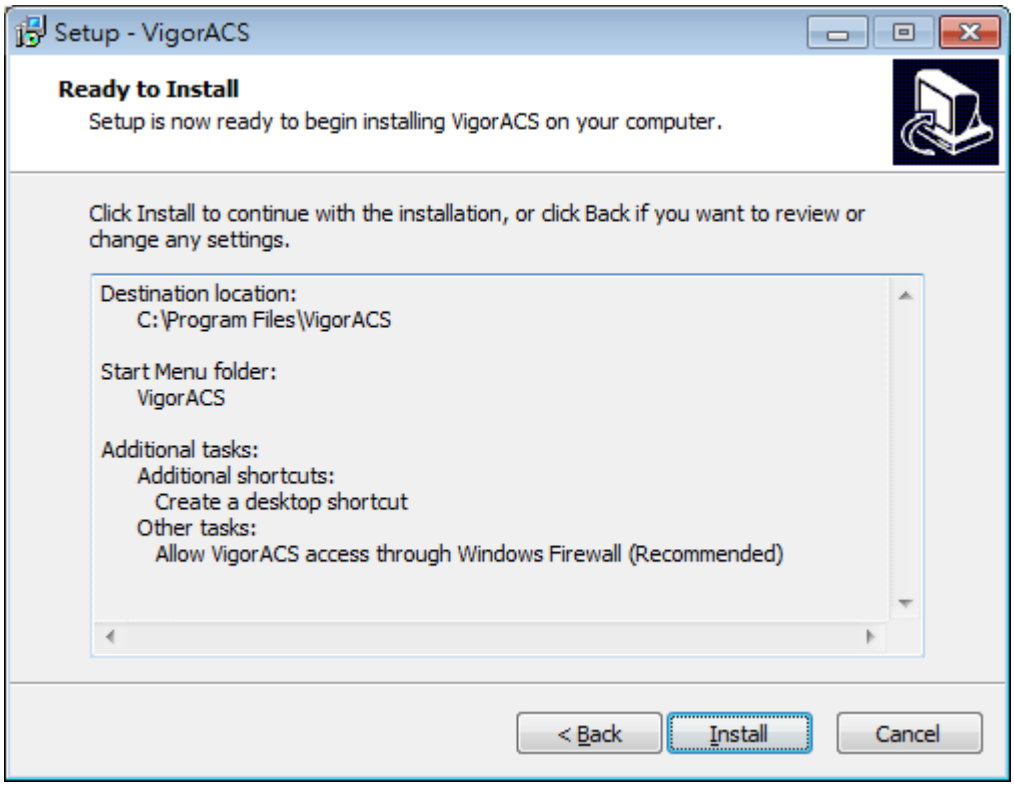

12. Determine the start menu folder and click **Next**. The default directory used by this program is *VigorACS.* You can modify it if you want and please make sure the length of directory is not over 100 characters, otherwise you might encounter problem of VigorACS in installation.



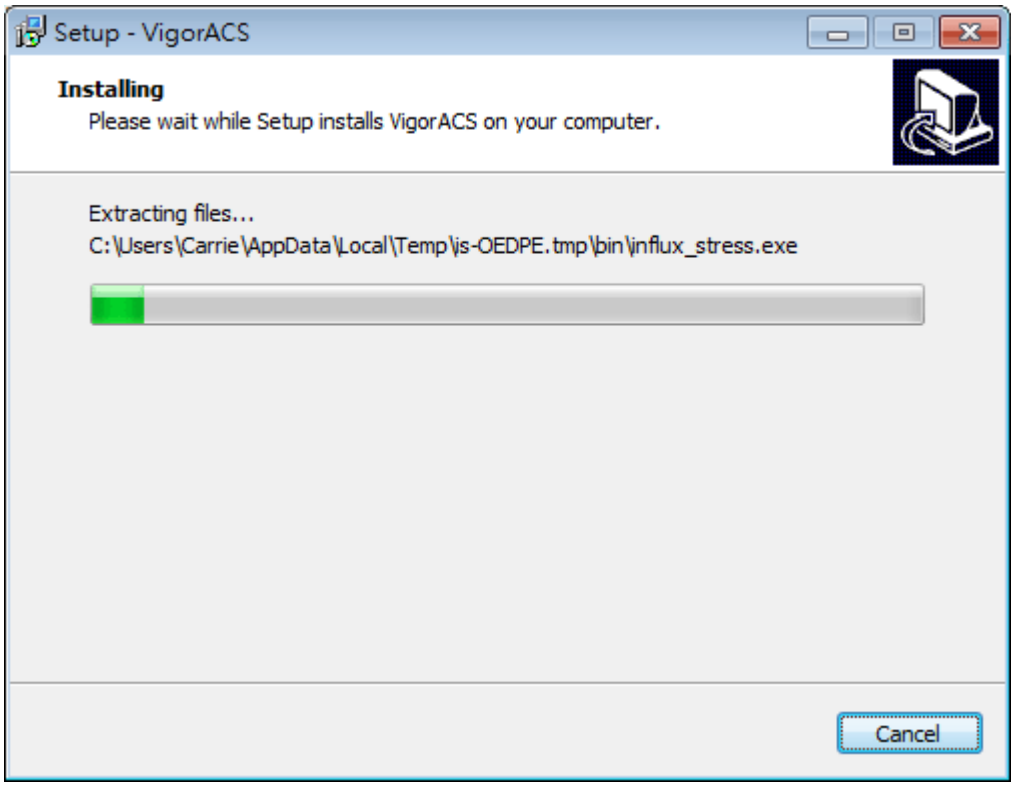
13. In this dialog, check the box of "**Create a desktop shortcut**" for your necessity. Click **Next**.



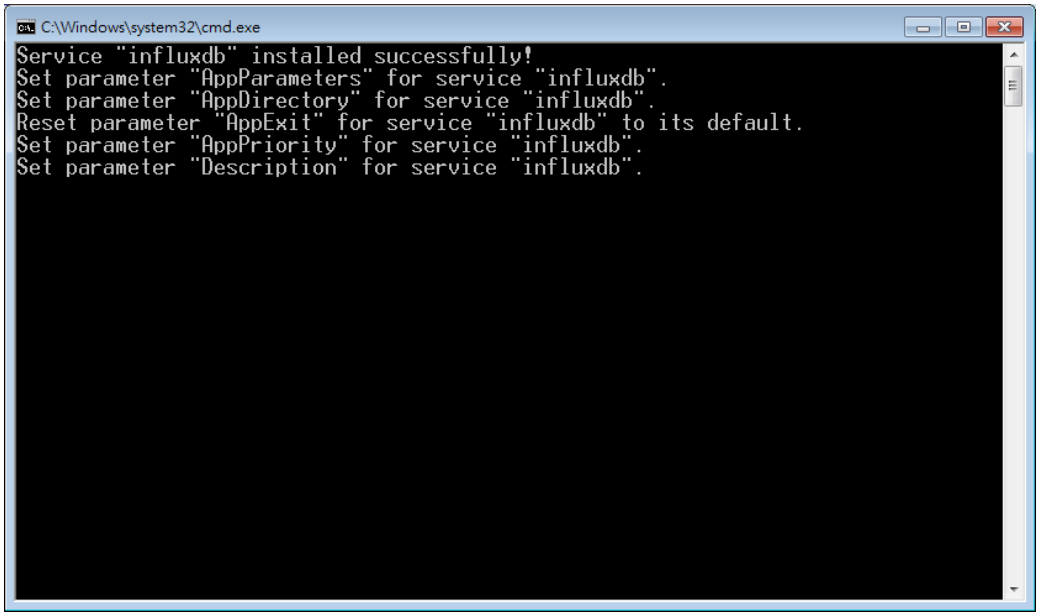

14. Now, the program is ready to install necessary features and files to your computer. Please click **Install** to start.



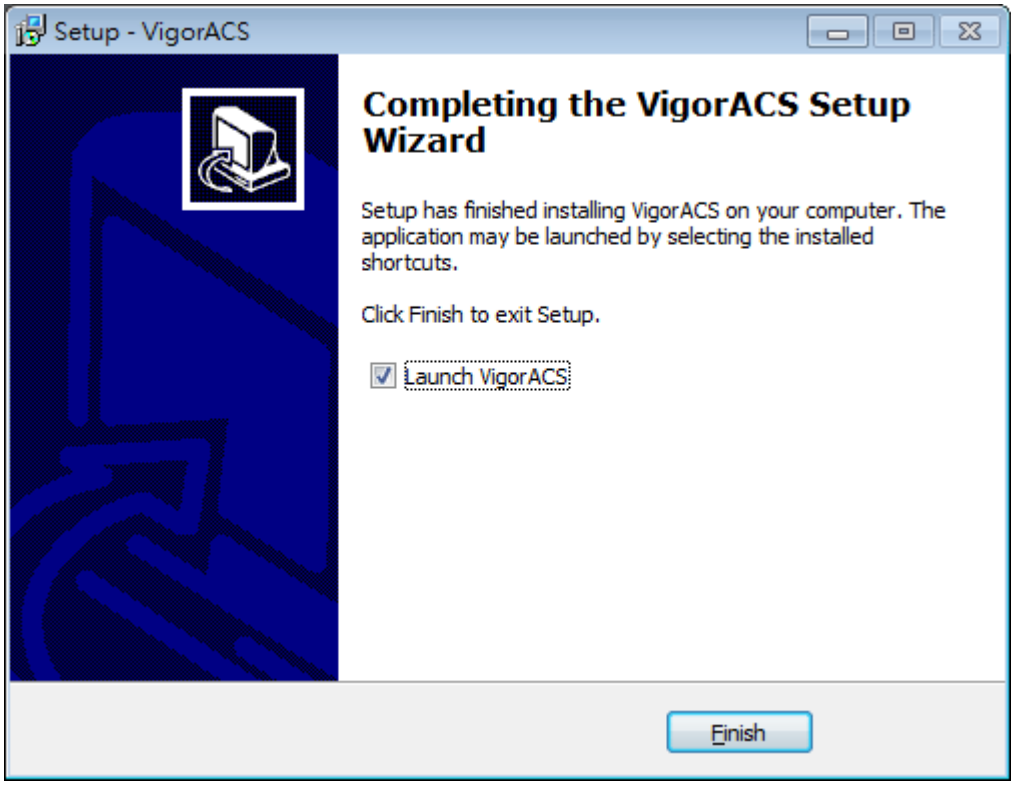
15. Please wait for a while to complete the installation.




16. While installing, the following screen will appear to show the procedure of database generation.



17. When the following screen appears, it means the program has completed the installation. Click **Finish** to exit it.



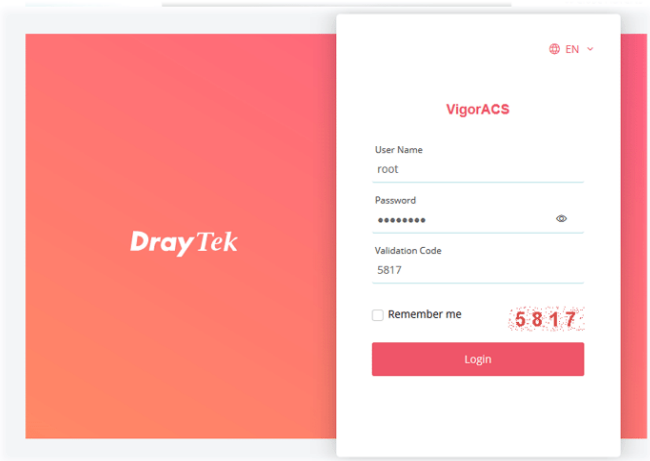

### 2.1.4 StartMySQL/MariaDB Database

After installing VigorACS, install program will register MySQL/MariaDB to Windows Service. MySQL /MariaDB will startup automatically after installing VigorACS or rebooting system.

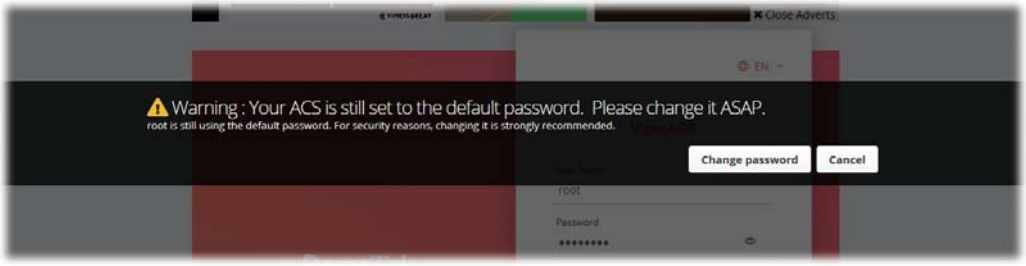
Normally, you don't need to worry about this step on Windows. But if you find any problems on VigorACS, you should check mysql/mariadb first. Please go to Windows Service check the MySQL/MariaDB Service starts or not.

### 2.1.5 Start VigorACS

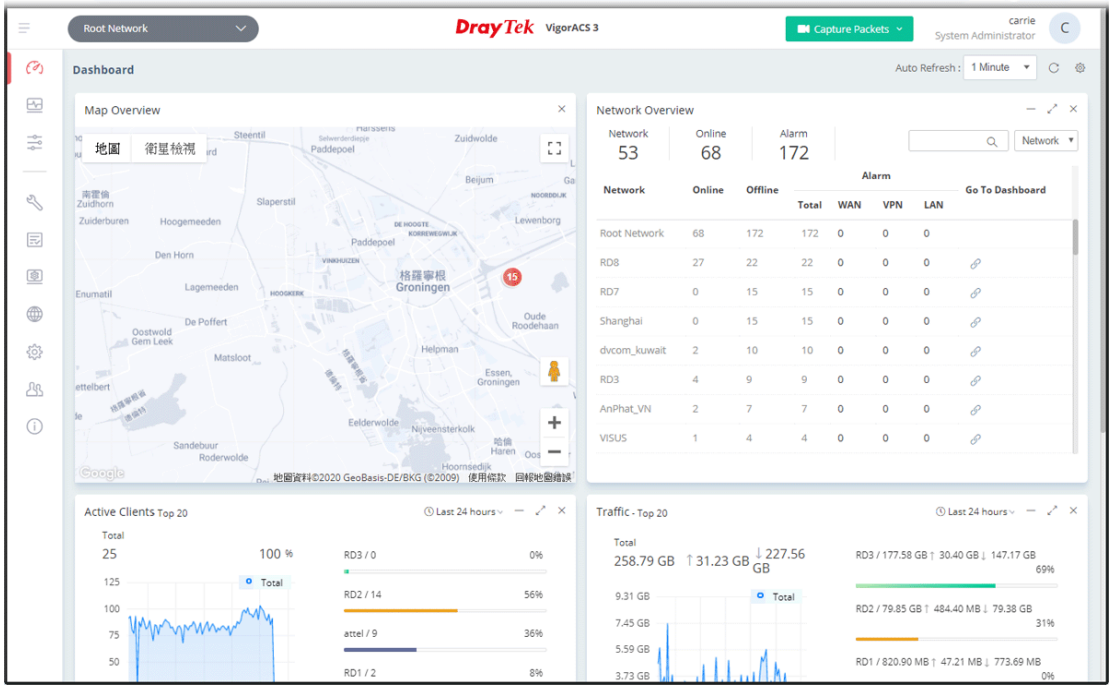
1. Login VigorACS. Use a web browser and enter “localhost:portnumber”. Note that the port number must be the one defined for HTTP and HTTPS port while installing VigorACS. For example, if HTTPS is defined as 8011, then the URL will be “localhost:8011”.
2. The login page of VigorACS will be shown as the following. Please type “root” as user name and “admin123” as password and type the authentication code. Then click Login.




3. For the first time to access into the web user interface, a warning message appears first. Please click the Change password button to change the default password for network security. If not, click Cancel to access into the web user interface of VigorACS and change the password later.




4. After clicking Login, main screen of VigorACS 3 will be shown as below.




If you start it first time, VigorACS will ask you to input the server bind IP. Refer to 2.1.5.

## 2.2 Platform for Linux

VigorACS is compatible with all of the Linux distribution, including Ubuntu, OpenSUSE, CentOS, Debian and RedHat.

To start up the VigorACS, please execute "/usr/local/vigoracs/VigorACS/bin/vigoracs.sh" instruction. A list of menu items will be shown as follows.

1. Start Mysql/MariaDB.
2. Shutdown Mysql/MariaDB.
3. Start InfluxDB.
4. Shutdown InfluxDB.
5. Start VigorACS.
6. Shutdown VigorACS.
7. Edit bind IP of VigorACS Server (please keyin IP or servername).
8. Memory Configuration.
9. Port Configuration.
10. Exit.

### 2.2.1 Installation for MariaDB, Java and VigorACS

Follow the steps listed below to install VigorACS under Linux:

1. Login Linux with root or the root privilege.
2. Download the ACS installation tar.bz2 package and extract it via below command:

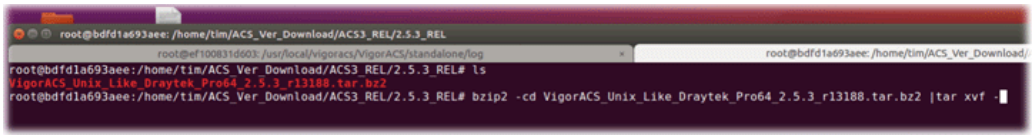
   #bzip2 -cd VigorACS_Unix_Like_xxxxxx_xxxxx.tar.bz2 | tar xvf -

   or

   #tar -jxv -f VigorACS_Unix_Like_xxxxxx_xxxxx.tar.bz2

3. Decompress the setup packages

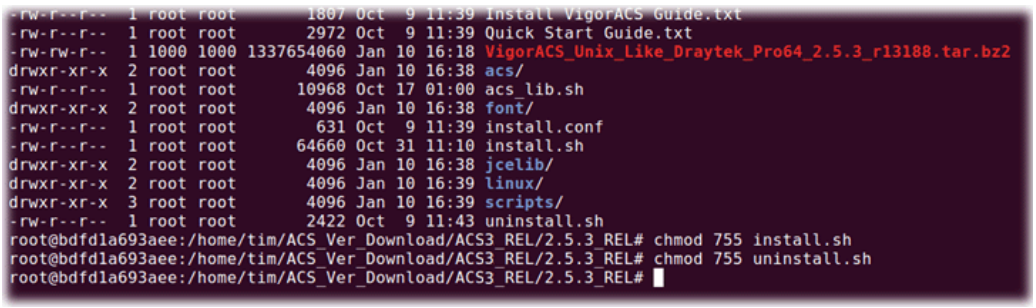
   bzip2 -cd VigorACS_Unix_Like_xxxxxx_xxxxx.tar.bz2 |tar xvf –



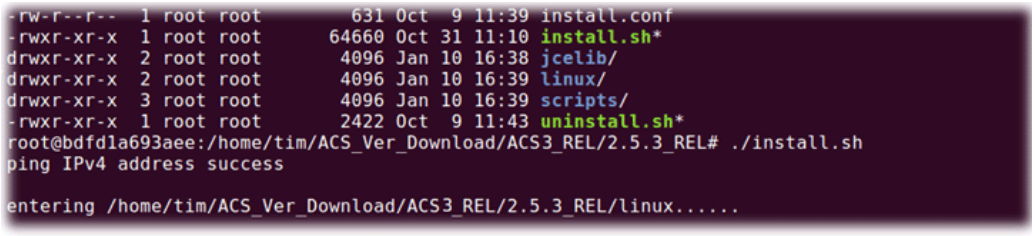

4. Change the permissions mode of install.sh and uninstall.sh.

   chmod 755 ./install.sh

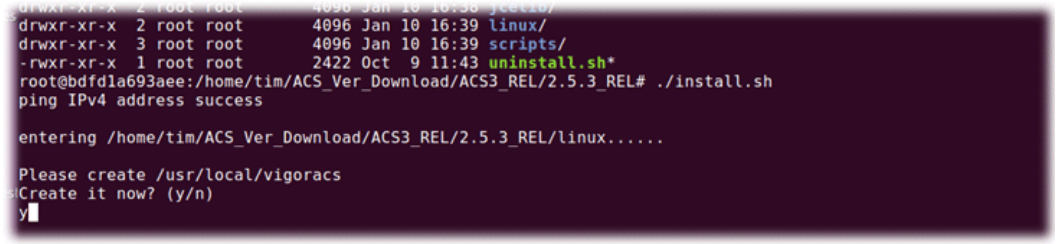
   chmod 755 ./uninstall.sh



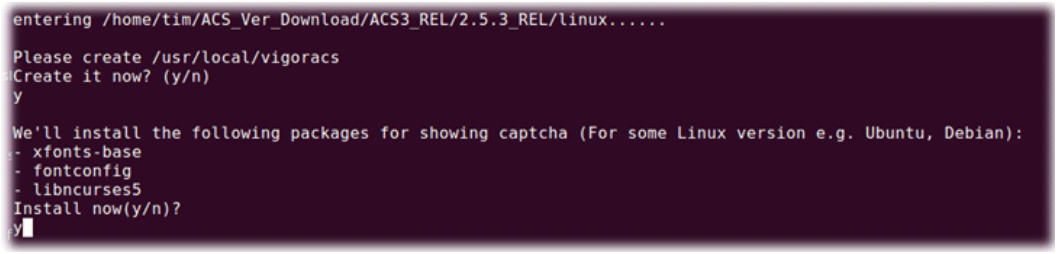
5. Execute ./install.sh installation file.




6. The system will ask to create vigoracs, enter “y” to proceed.




7. Next, the system will ask you to install xfonts-base, fontconfig and libncurses5, just enter “y” to proceed.




8. Next, please select the item number which you want to execute. Note that VigorACS supports Linux OS. The program will detect the system you have in your computer.

(1) Install MySQLl/MariaDB

(2) Change root password and security configuration of MySQLl/MariaDB

(3) Install InfluxDB

(4) Install or Upgrade java

(5) Install VigorACS

(6) Upgrade VigorACS

(7) Redirect the database path of VigorACS to remote host

(8) Exit

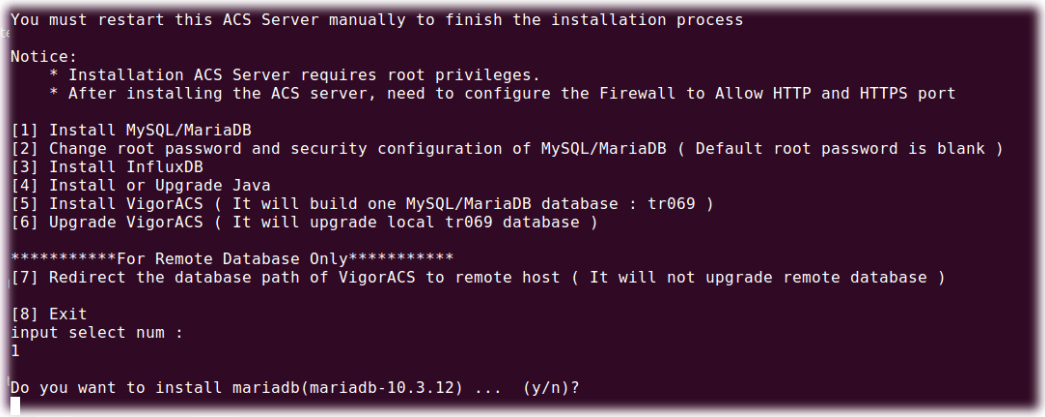
input select num :

If your computer has installed MariaDB and java previously, ignore the installation of them. Otherwise, install all the required items (MariaDB, Java and VigorACS) for your system. Item number 6 is used to upgrade VigorACS, so it is not necessary for you to execute for the first time of installation.

9. Input 1 to install MariaDB first. Notice that it will setup blank as default password. You can change the password by using the following command.

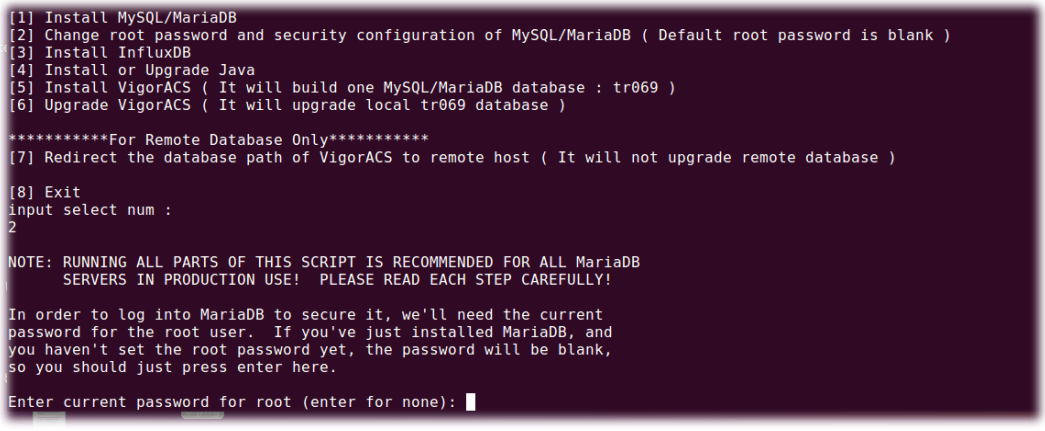
   #/usr/local/mysql/bin/mysqladmin --defaults-file=/usr/local/mysql/my.cnf -u root password 'new password'

The password set in this step is used for VigorACS 3 to login database.



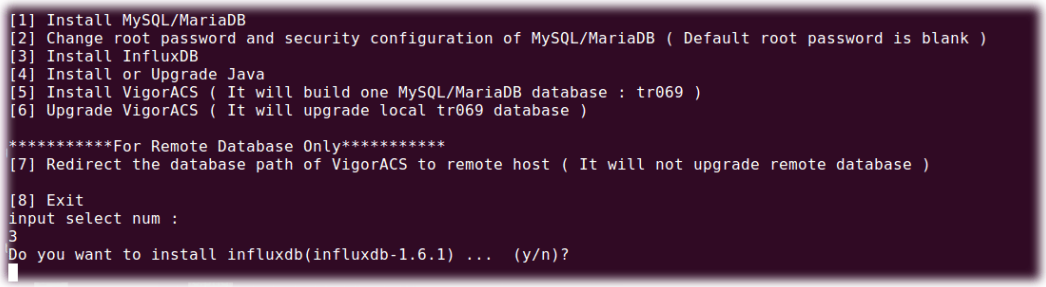

Follow the instructions on the screen to finish the MariaDB installation.

10. Later, input 2 to change root password and security configuration of mysql/mariadb.



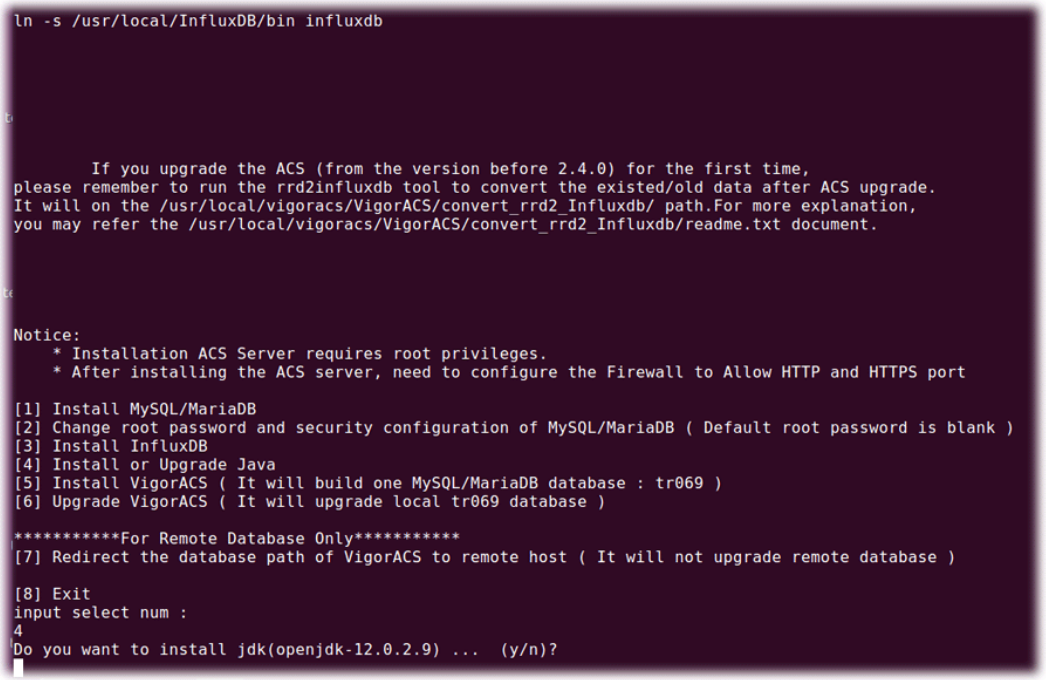

The password set in this step is used for VigorACS 3 to login database.

11. Input 3 to install InfluxDB.



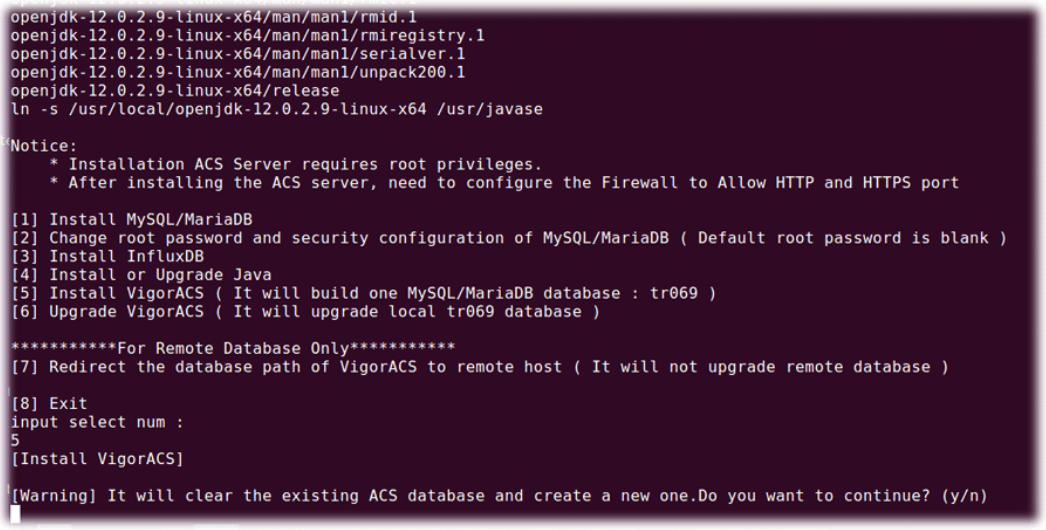

Follow the instructions on the screen to finish the InfluxDB installation.

12. Input 4 to install Java.

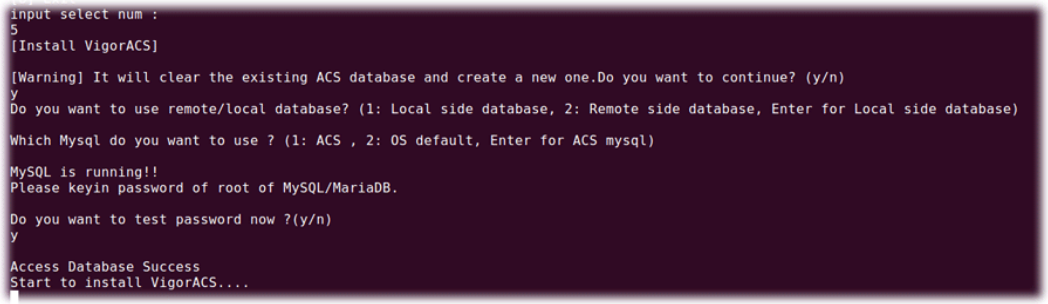



Follow the instructions on the screen to finish the Java installation.

13. Input 5 to install VigorACS. It is suggested to use ACS customized MariaDB database. When asked to enter MariaDB password, press “Enter” if you haven’t changed the password via the command. Then, confirm that TR-069 database has been installed successfully.



Wait and follow the instructions on the screen to finish the installation.



14. Now, input 7 to redirect the database path of VigorACS to remote host. For remote database, please execute such step on remote host.

15. Input 7 to finish and exit the installation.

---

Step 14 is required for establishing remote database only. You can ignore it while building local database.

To prevent port conflicts, we'll suggest that using other ports for HTTP and HTTPS instead of default 80 and 443.

---

### 2.2.2 StartMySQL/MariaDB Databse

After installing VigorACS, mysql/mariadb daemon has started. You can check it using "ps -ef|grep mysql" instruction. Use the menu item 1 / 2 to start / shutdown mysql/mariadb.

### 2.2.3 Start InfluxDB

After installing InfluxDB, access “/usr/local/vigoracs/VigorACS/bin” and execute “./vigoracs.sh”. Next, it is necessary to start InfluxDB for VigorACS.

Select item 3 to start InfluxDB.

### 2.2.4 Start VigorACS

After installing VigorACS, access “/usr/local/vigoracs/VigorACS/bin” and execute “./vigoracs.sh”.

Select item 5 to start VigorACS.

If you ever reboot the machine after installing VigorACS, just select item 1 to start mysql/mariadb first. Then, select item 5 to start VigorACS.

### 2.2.5 Edit VigorACS IP

When starting the VigorACS at first time on Solaris or Linux, startup program will ask you input Server IP or input Enter key by using the IP address of the host. Once you input the IP address, VigorACS will keep it on startway.txt. Next time, if you want to change it, you can select item 7 to edit startway.txt using vi editor.

## 2.3 Registering VigorACS

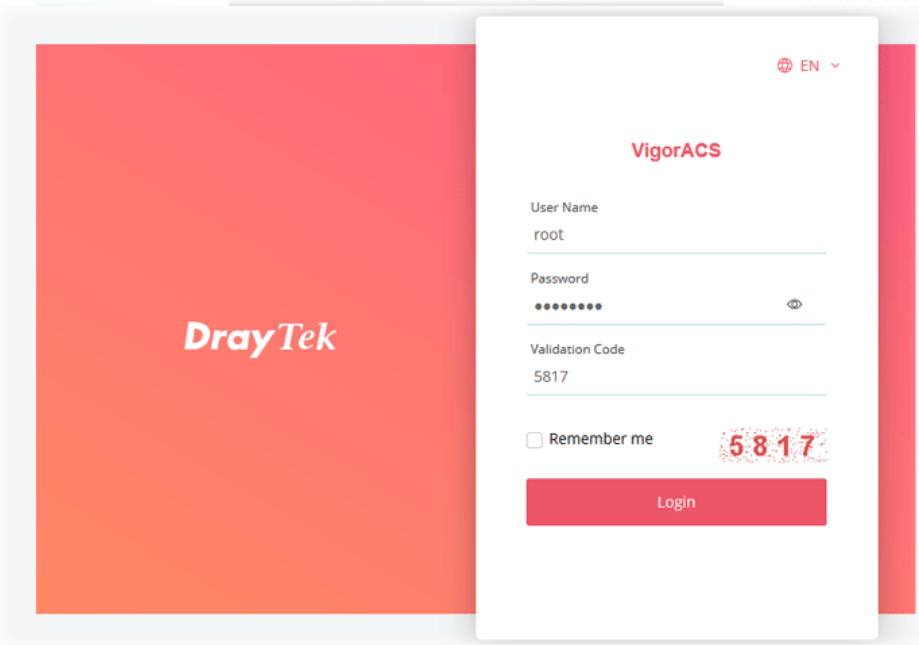
For the first time to activate VigorACS, the system will ask you to register VigorACS onto DrayTek MyVigor server. Refer to the following sections to register VigorACS on different platforms.

> While installing VigorACS, install program will register MySQL/MariaDB to Windows Service. MySQL/MariaDB will startup automatically after installing VigorACS or rebooting system. Normally, you don't need to worry about this step on Windows. But if you find any problems on VigorACS, you should check mysql/mariadb first. Please go to Windows Service check the MySQL/MariaDB Service starts or not.
>
> After installing VigorACS, the software will startup automatically. Normally, you don't need to worry about this step on Windows. But, if you find any problem on VigorACS, you could shut down VigorACS and start VigorACS again.

### 2.3.1 Registration for VigorACS via Windows Platform

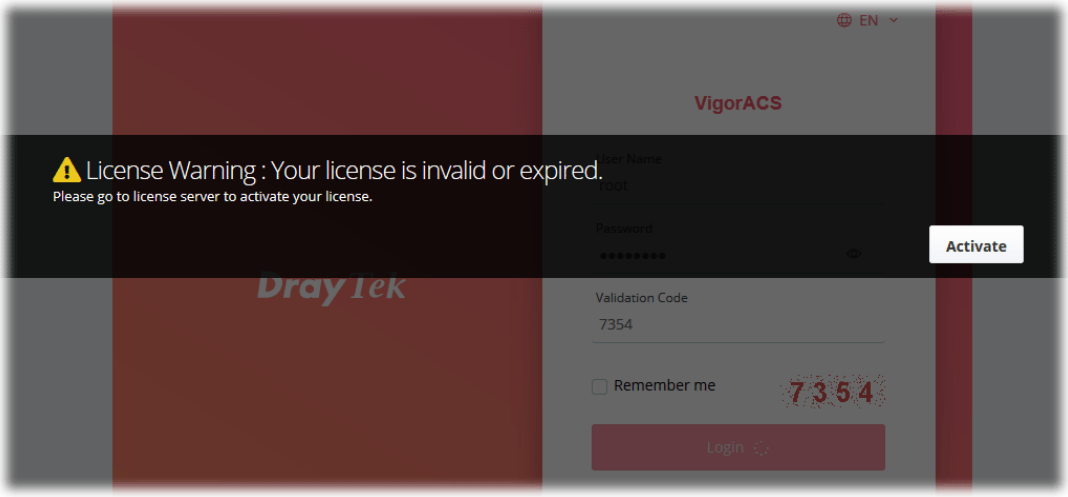
Below shows the steps to register VigorACS:

1. Login VigorACS. Use a web browser and enter "*localhost:portnumber*". Note that the port number must be the one defined for HTTP and HTTPS port while installing VigorACS. For example, if HTTPS is defined as 8011, then the URL will be "*localhost:8011*".
2. The login page of VigorACS will be shown as the following. Please enter "**root**" as user name and "**admin123**" as password and enter the authentication code. Then click **Login**.

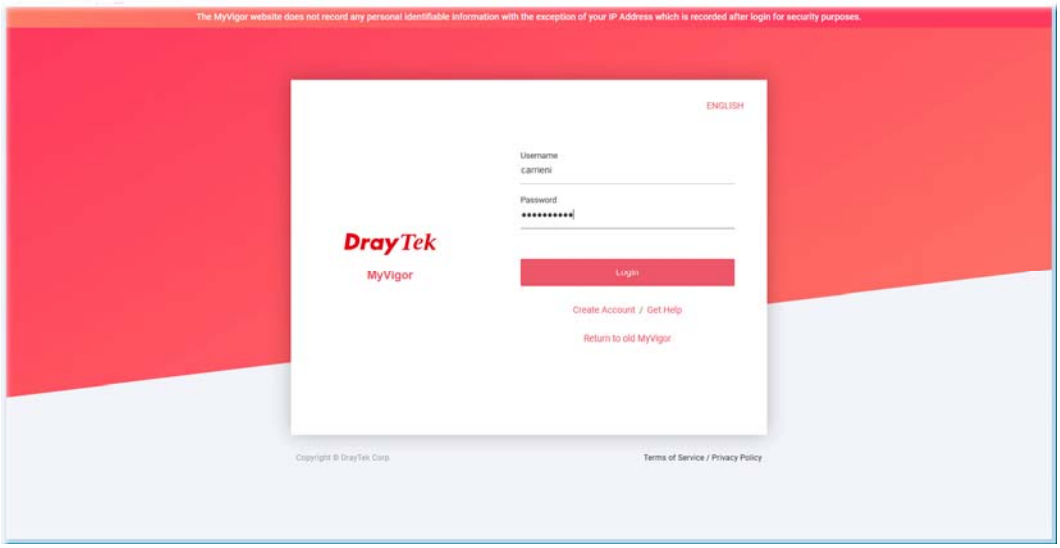


“root” and “admin123” are default settings.

3. A License Error dialog appears as follows. Simply click **Active**.

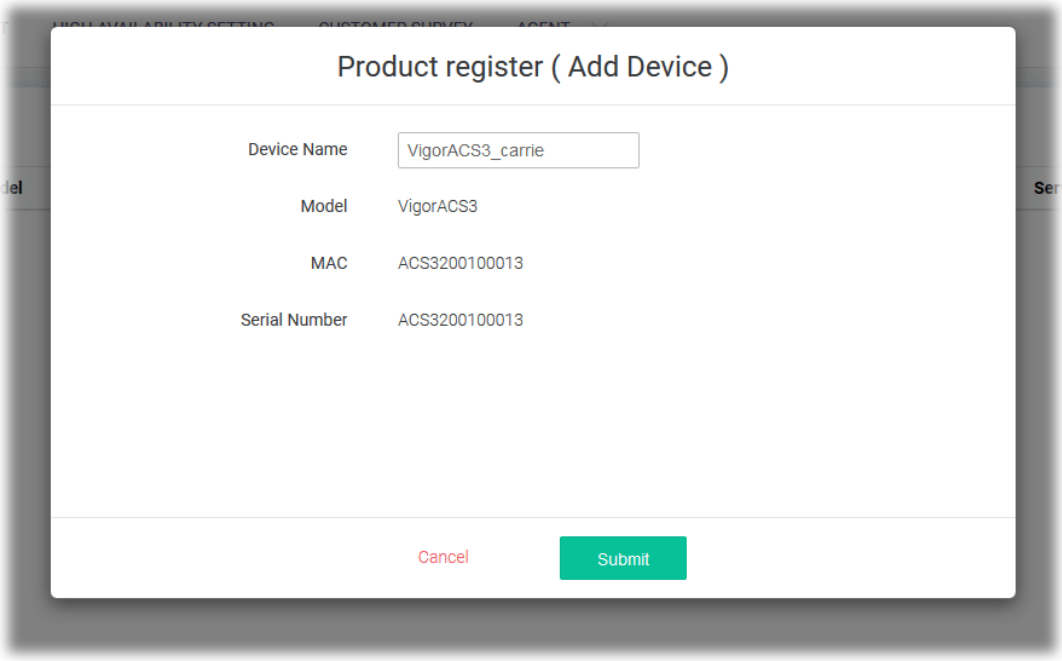



4. A login page for MyVigor web site will be popped up automatically. Type your account (user name) and password in this page. Check the box of “I’m not a robot”. Then, click **Login.**

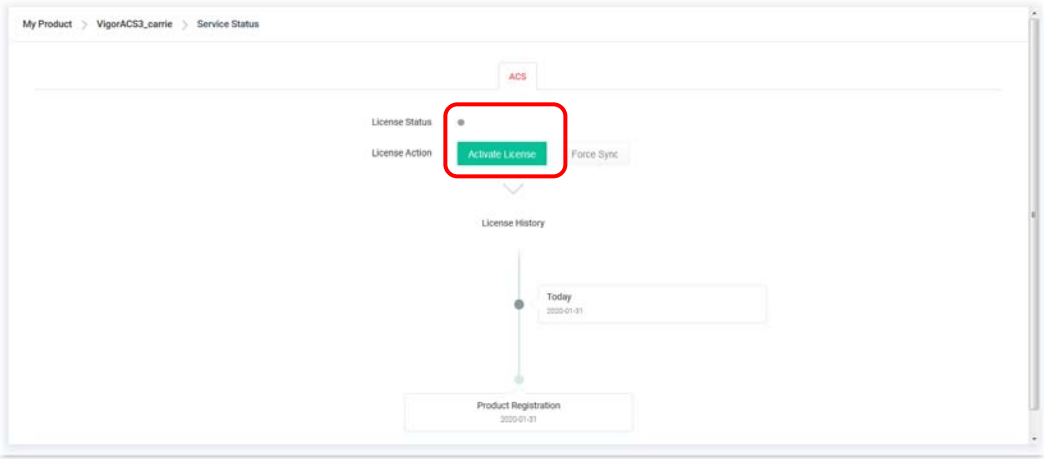



If you do not have any account, simply click **Create Account** to create a new one for using the service provided by MyVigor web site.

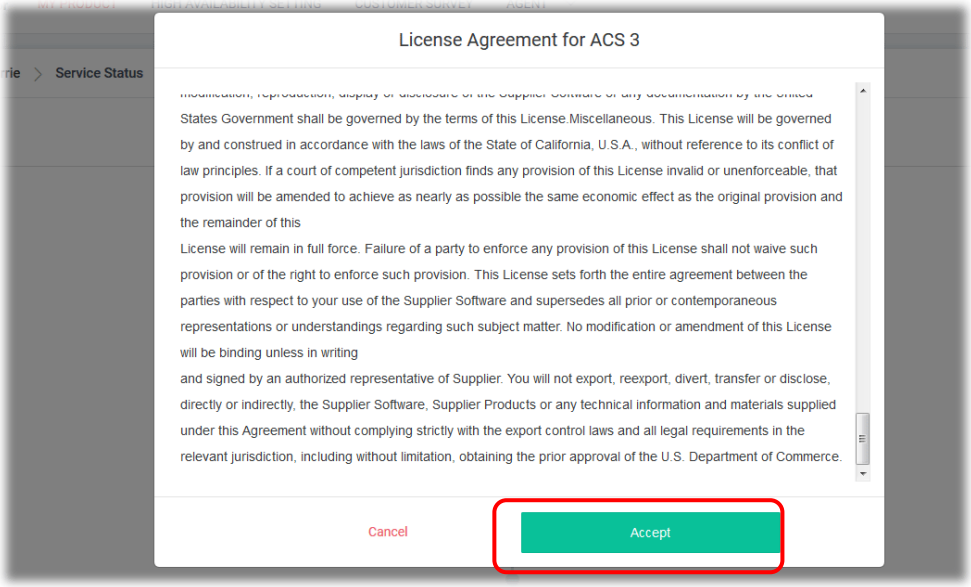
5. MyVigor will verify and authenticate if the user account you typed is allowed to access into the web site. If yes, the following screen will appear. Enter a nickname for VigorACS and click **Submit**.



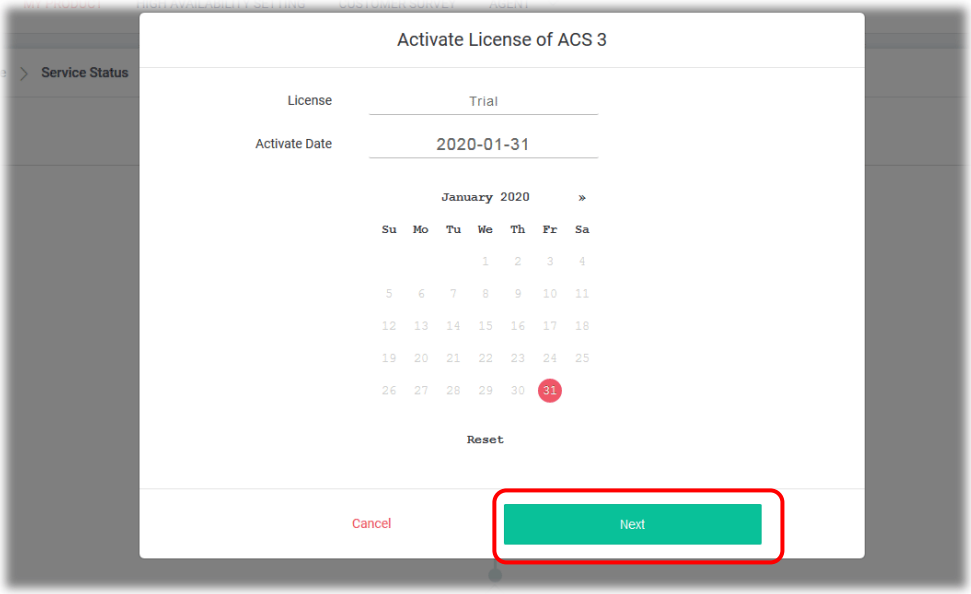

6. The information related to VigorACS has been added to the database and has been registered to *myvigor* website successfully. Clilck **Activate License**.



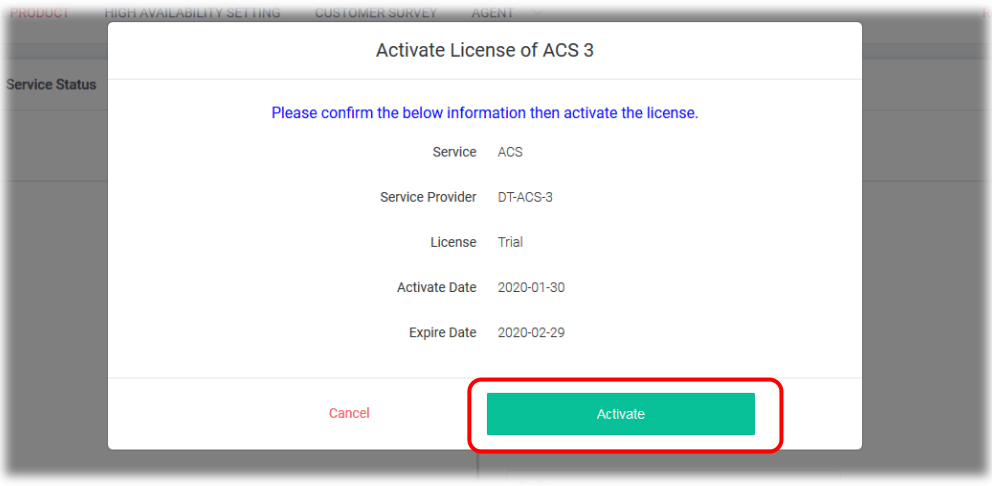
7. When the following page appears, click **Accept**.



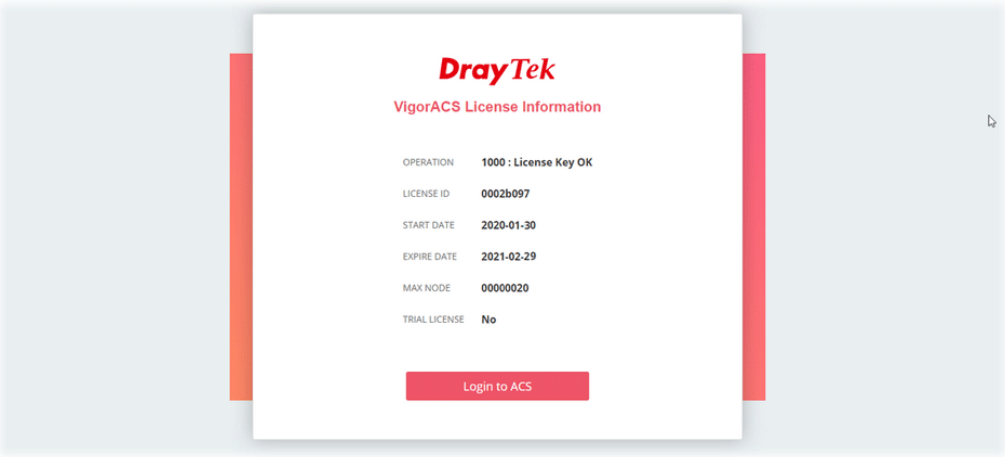

8. Make sure the registration date of VigorACS. Click **Next**.



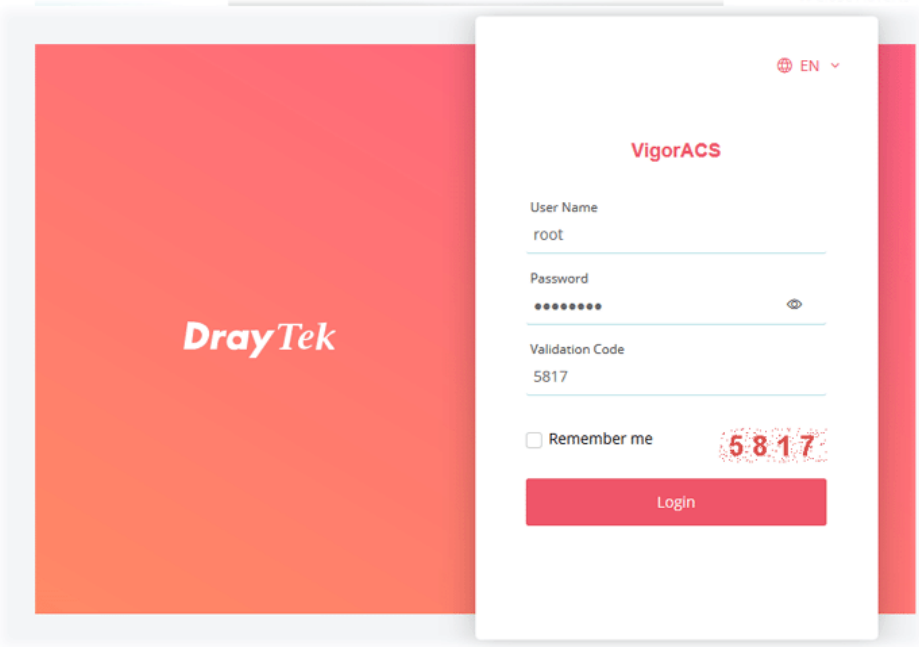

9. Confirm the content and click **Activate**.



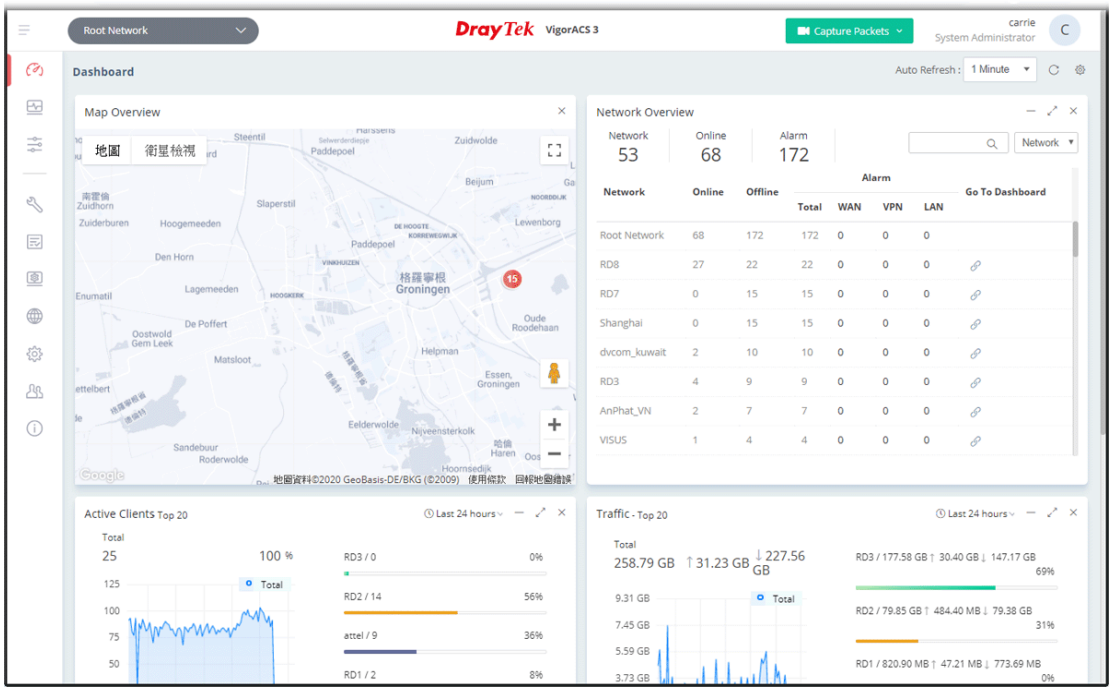
10. When the License Information page appears, the service is ready for you to use. Click **Login to ACS** to use VigorACS service.




11. The login page will appear as follows. Type the default settings of User Name (root) and Password (admin123) and type the authentication code. Then, click **Login**.

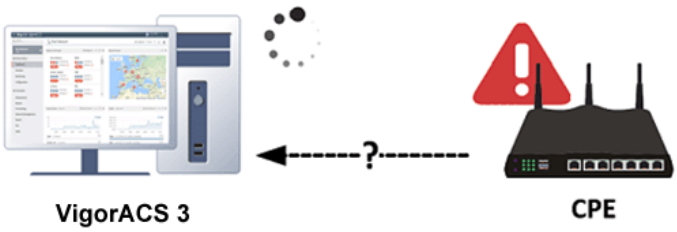


12. Now, the main screen of VigorACS will be shown as follows.



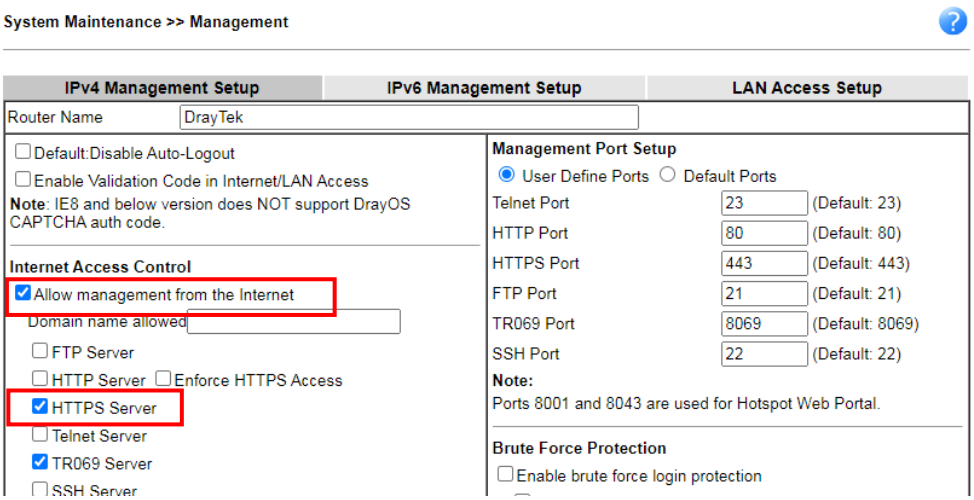

## 2.3.2 Troubleshooting for Unstable CPE Status

In some cases, the online status of CPE is unstable, which displayed offline when it is online. Check the following if you meet such kind of problem.



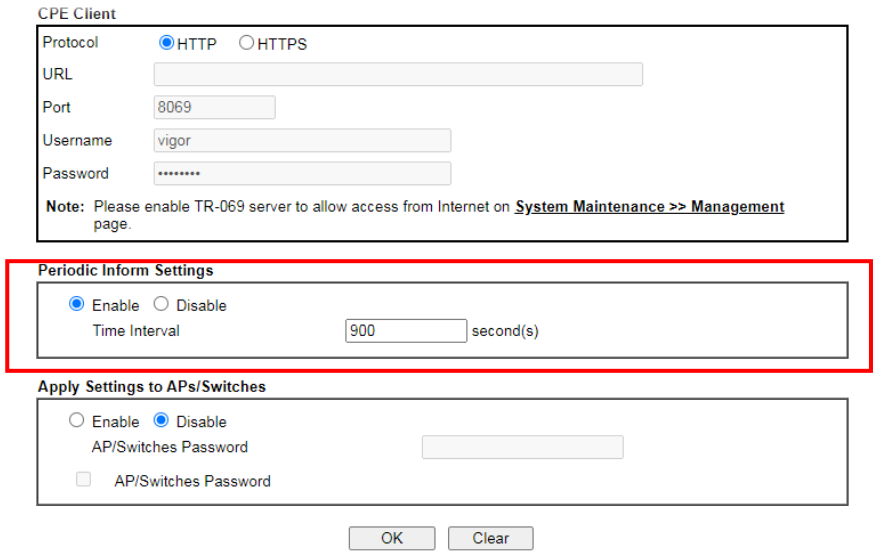

- **Allow TR-069 server access from the Internet**

  Please make sure you have enabled the TR-069 server remote access from System Maintenance >> Management of CPE WebUI if your ACS server is on the Internet/WAN side.



### Enable Periodic Inform

The periodic inform option should be enabled from System Maintenance >> TR-069 of CPE WebUI. It is recommended to configure the 900 seconds as the inform interval. Sending inform too frequently may increase the loading of the ACS server.

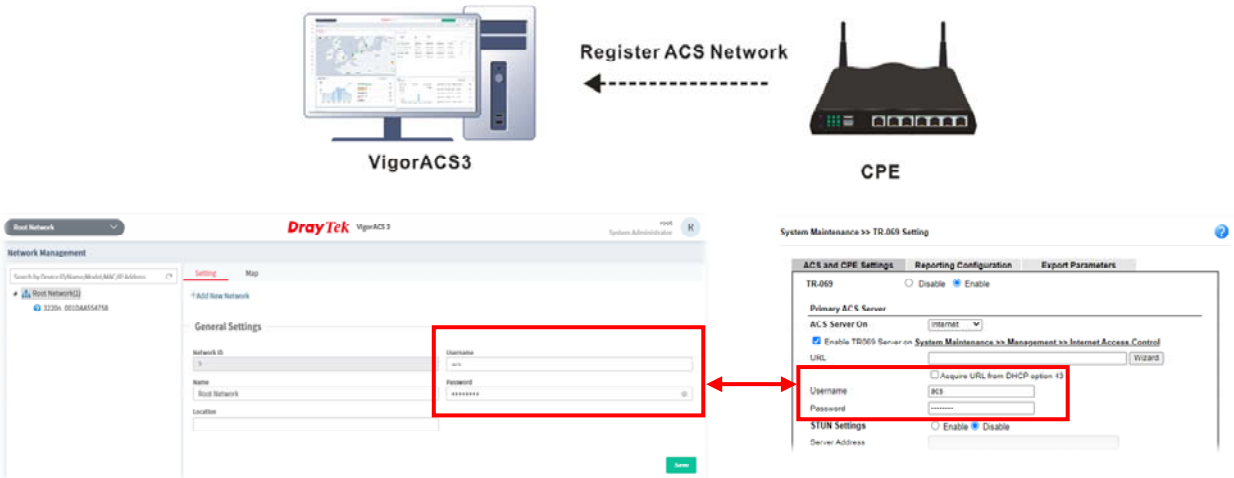



### Check TR-069 authentication

There are two sets of authentication info displayed on the CPE TR-069 setting page, which have different meanings.

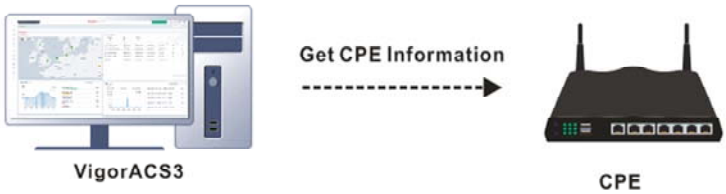
- Register to the network of VigorACS 3

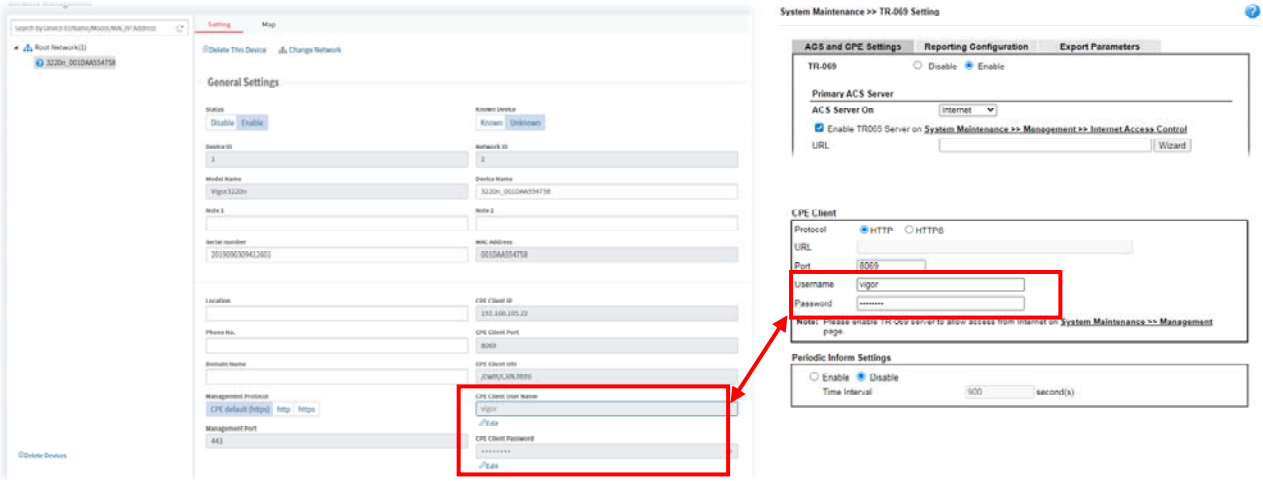
ACS will check the username and password fields from the TR-069 setting and assign to the corresponding network group.



- Get CPE information

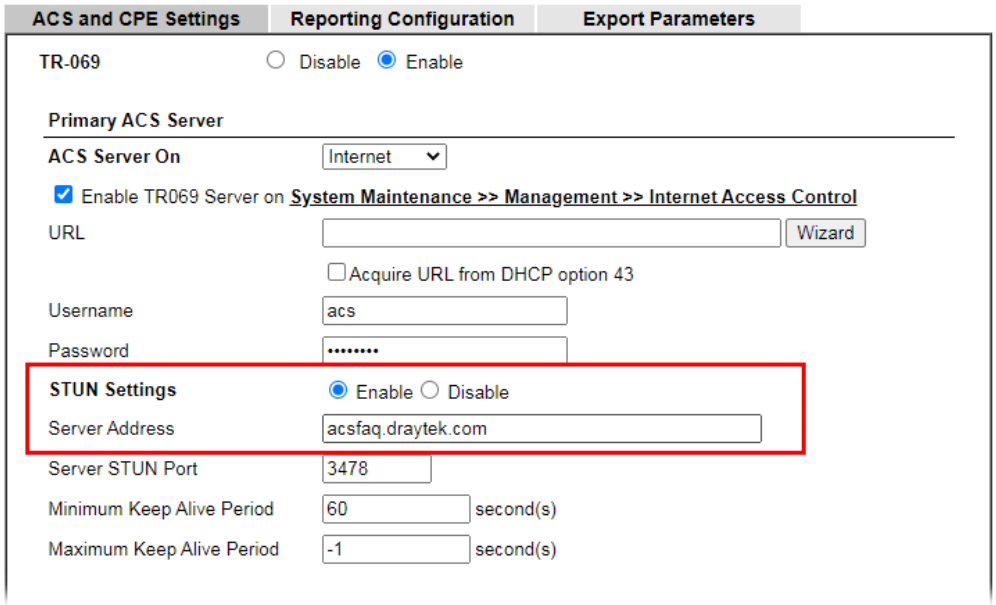
The authentication is required while ACS initiates the connection to CPE for information requested. The username and password between System Maintenance >> TR-069 >> CPE client (within CPE's GUI) and Network Management >> Device (on ACS) should be the same.



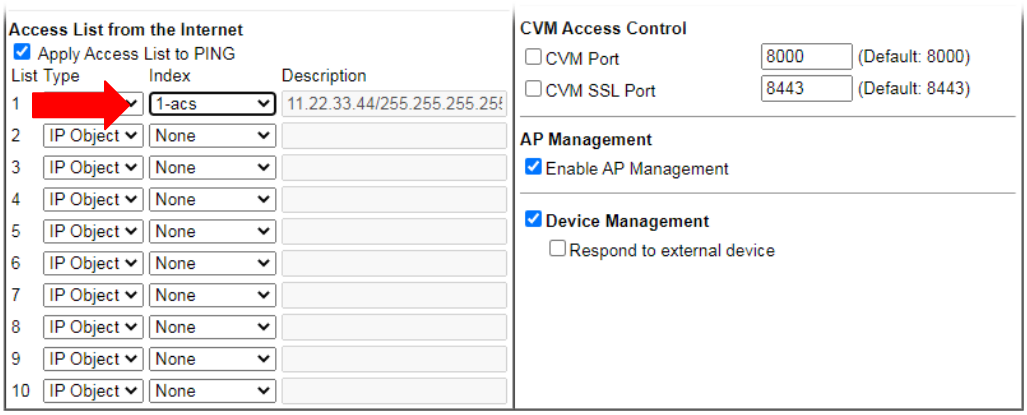

- **Check STUN setting**

If the CPE is behind NAT, do not forget to enable the STUN setting. Also, the STUN server is only allowed to use our ACS server. Please DO NOT use the 3rd party STUN server.




- **Check the ACL setting**

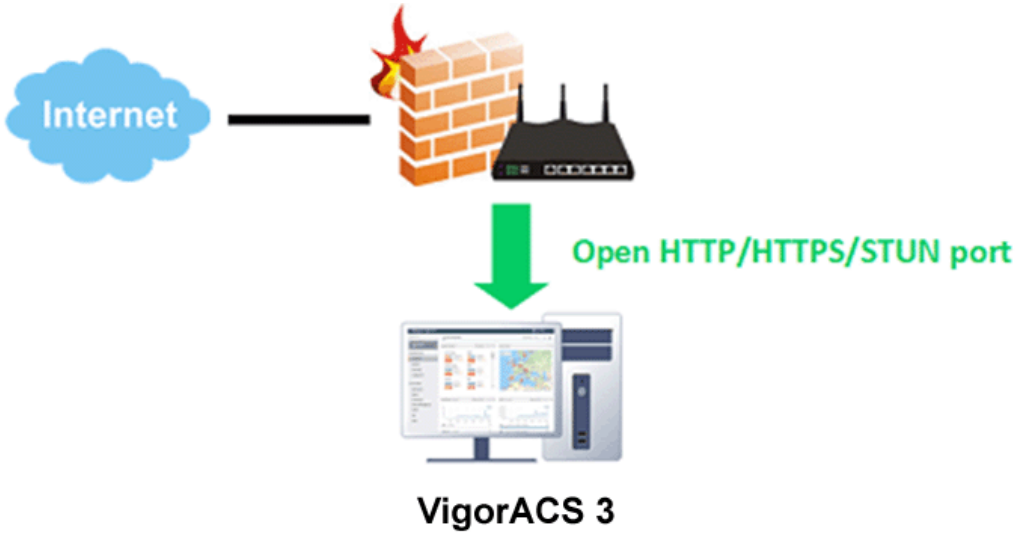
Make sure the IP of ACS server is also added into your access list once you enable it.




- **Check the firewall on ACS server**

  Make sure your ACS server has correct firewall setting which allows those incoming traffic:

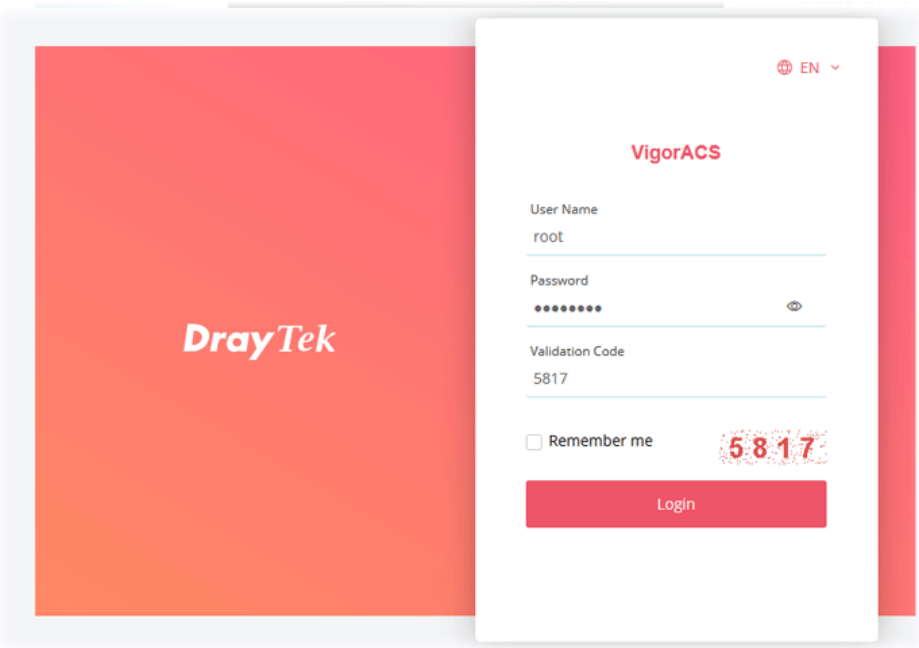
  - HTTP port (Default tcp port 80)
  - HTTPS port (Default tcp port 443)
  - STUN port (Default udp port 3478)



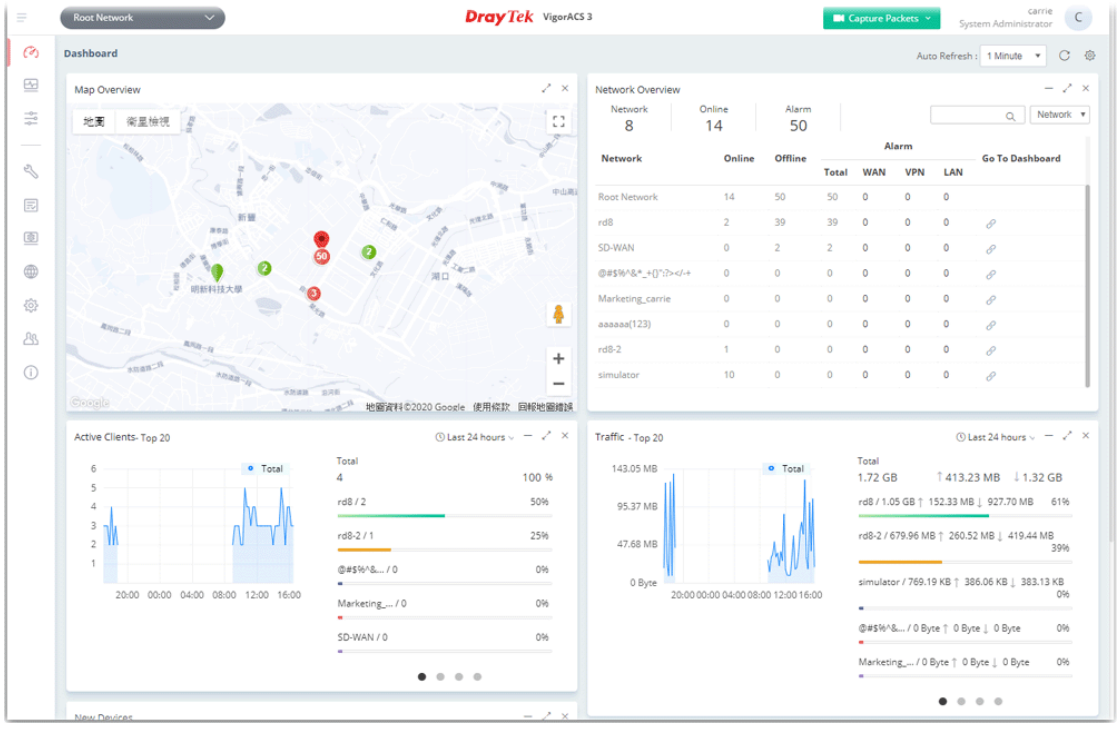
# Chapter 3 Getting Started

## 3.1 Accessing Web Page of VigorACS

1. Login VigorACS. Use a web browser and type *"localhost:portnumber"*. Note that the port number must be the one defined for HTTP and HTTPS port while installing VigorACS. For example, if HTTPS is defined as 8011, then the URL will be *"localhost:8011".*



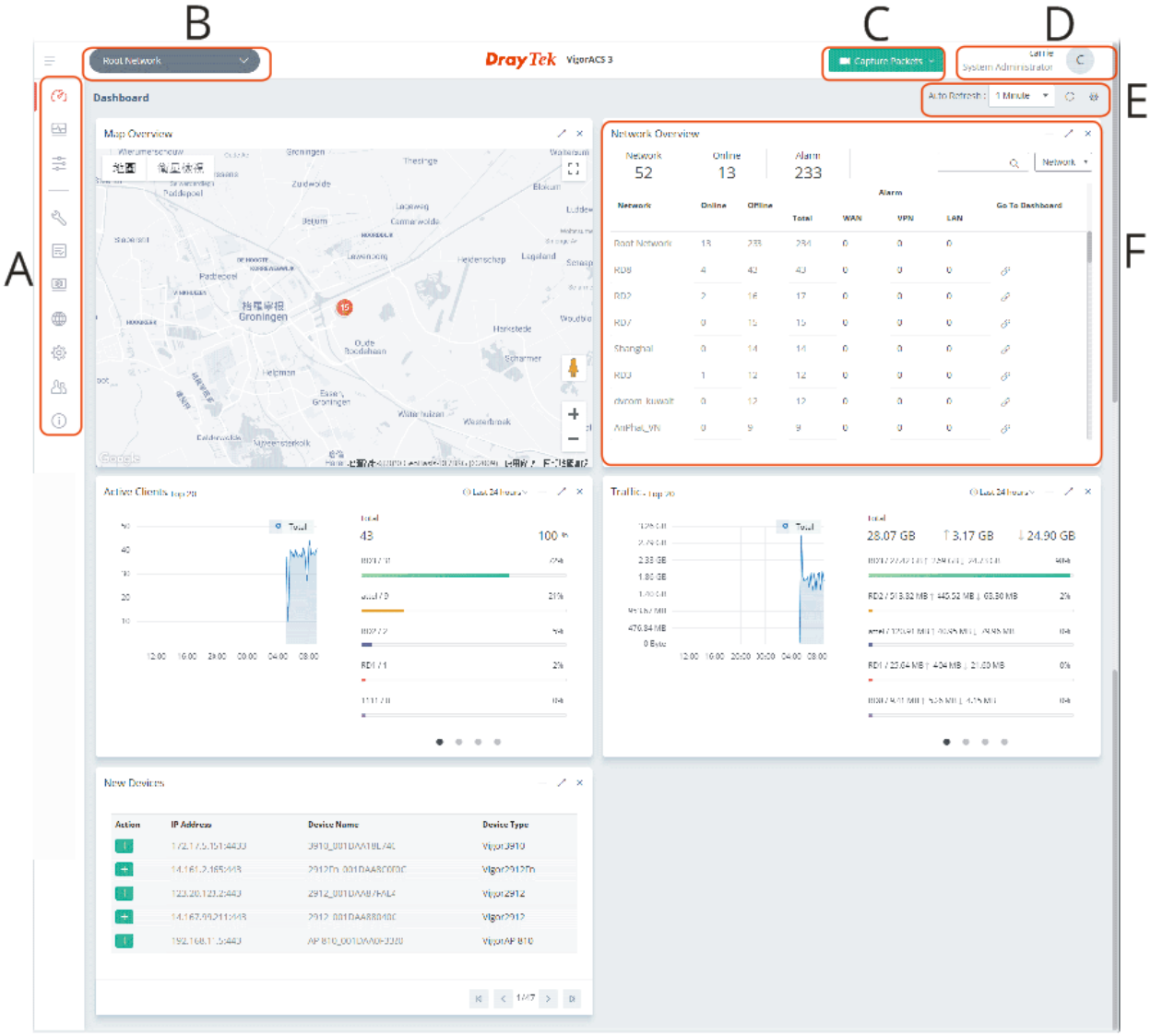

2. After clicking **Login**, main screen of VigorACS 3 will be shown as below.



## 3.2 Dashboard

### 3.2.1 Dashboard for Root Network

The Dashboard displays general information and quick overview for all the devices (CPE, Access Point) managed by VigorACS.




**A: Menu Bar** - Displays the menu items related to the network.

**B: Display Tab** - Displays current selected item, e.g., root network, group network and CPE model. In this page, the Root Network is selected.

**C: Capture Packets** - Offer options to view what packets that VigorACS server transmits or receives. To enable the function, open System>>System Parameter and choose True for ID number 81: PacketCaptureTool.

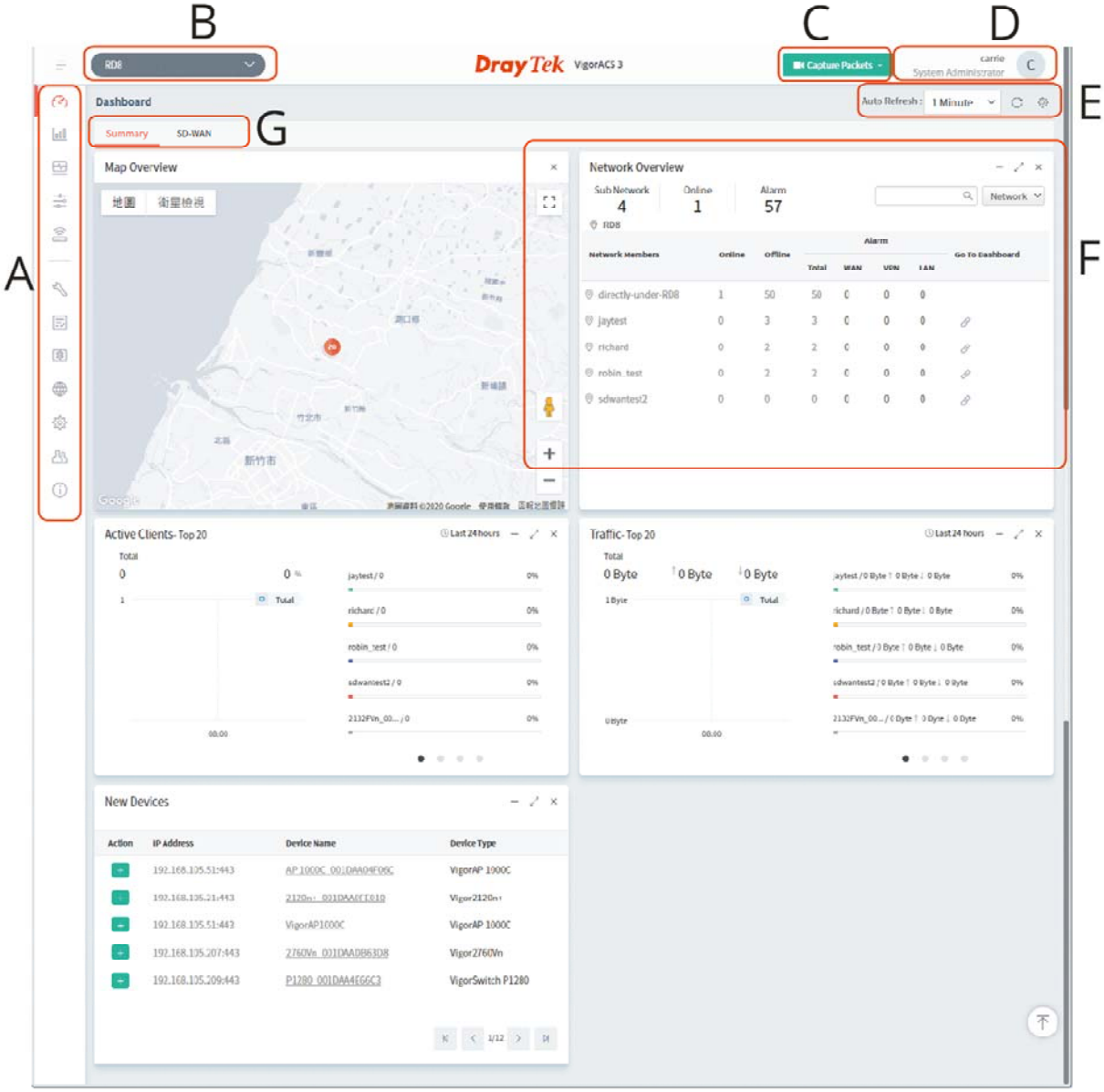
**D: Selections** - Display current used account and offer selections for setting password, two-factor authentication, theme change and logout.

**E: Auto Refresh, Manual Refresh, and Widget** - For the widget, there are six display views to select, including Network Overview, Map Overview, Clients, Traffic, New Devices and Reset to default. Only the selected one(s) will be displayed on the dashboard.

**F: Overview** - There are five types (Network Overview, Map Overview, Clients, Traffic, New Devices) of overview under the Root Network.

### 3.2.2 Dashboard for a Network Group

Under the selected network group (e.g., RD8 in this case), there are two tabs to choose. One is Summary; the other is SD-WAN.




**A: Menu Bar** - Displays the menu items related to the network.

**B: Display Tab** - Displays current selected item, e.g., root network, group network and CPE model. In this page, the group network (e.g., RD8) is selected.

**C: Capture Packets** - Offer options to view what packets that VigorACS server transmits or receives. To enable the function, open System>>System Parameter and choose True for ID number 81: PacketCaptureTool.

**D: Selections** - Display current used account and offer selections for setting password, two-factor authentication, theme change and logout.

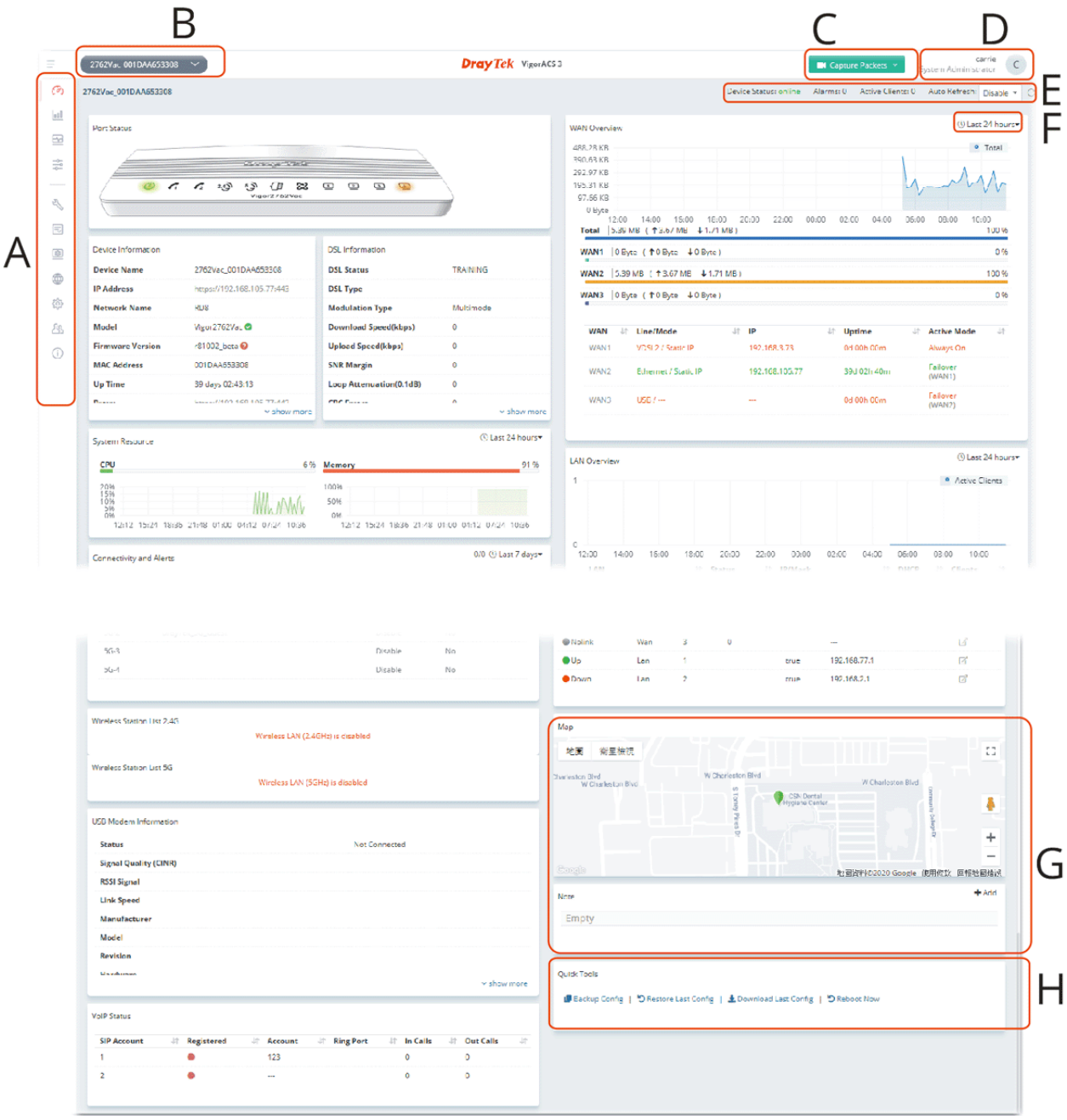
**E: Auto Refresh, Manual Refresh, and Widget** - For the widget, there are six display views to select, including Network Overview, Map Overview, Clients, Traffic, New Devices and Reset to default. Only the selected one(s) will be displayed on the dashboard.

**F: Overview** - There are five types (Network Overview, Map Overview, Clients, Traffic, New Devices) of overview under the Root Network.

**G: Summary and SD-WAN** - There are two tabs bringing different page contents.

### 3.2.3 Dashboard for a Device

This page offers device information such as system resource, connectivity and alerts for such device, wireless LAN configuration, wireless station overview, WAN overview, LAN overview, VPN overview, Port Status, Network Status, LTE Information, USB Modem Information, Map, VoIP Status, and Quick Tools for the selected device.




**A: Menu Bar** - Displays the menu items related to the selected device (CPE).

**B: Display Tab** - Displays current selected item, e.g., root network, group network and CPE model. In this page, a CPE device (e.g., Vigor2927 series) is selected.

**C: Capture Packets** - Offer options to view what packets that VigorACS server transmits or receives. To enable the function, open System>>System Parameter and choose True for ID number 81: PacketCaptureTool.

**D: Selections** - Display current used account and offer selections for setting password, two-factor authentication, theme change and logout.

**E: Status** - Display current status (online/offline) of the CPE and allow to refresh current page.

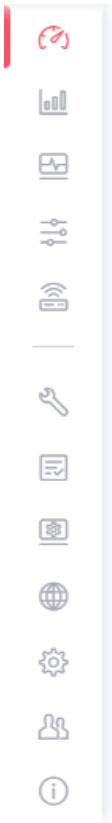
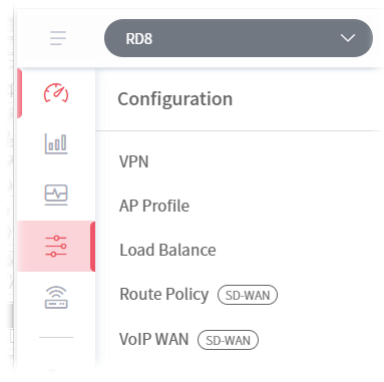
**F: Time Setting** - Display the clients detected within 24 hours, 7 days or 30 days.

**G: Overview** - There are several types (Network Overview, Map Overview, Clients, Traffic, New Devices) of overview under the selected device (CPE).

**H: Quick Tools** - Offer a quick method to backup configuration, restore last configuration, download last configuration and perform immediate reboot.

### 3.2.4 Menu Bar

Displays the menu items available for the network or network group or selected device (CPE).

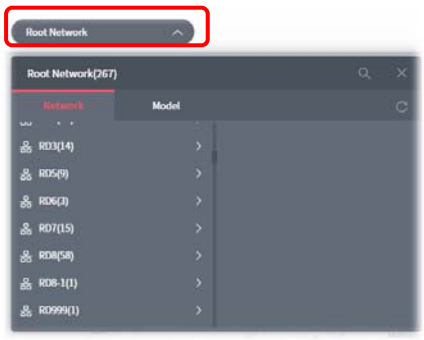
| | Menu Bar for Root Network. | | Menu Bar for Network Group. | | Menu Bar for Selected CPE. |
|---|---|---|---|---|---|
| | • Dashboard<br>• Monitoring<br>• Configuration<br>----------<br>• Maintenance<br>• Reports<br>• Provisioning<br>• Network Management<br>• System<br>• User<br>• About |  | • Dashboard<br>• Statistics<br>• Monitoring<br>• Configuration<br>• Hotspot Web Portal<br>----------<br>• Maintenance<br>• Reports<br>• Provisioning<br>• Network Management<br>• System<br>• User<br>• About | | • Dashboard<br>• Statistics<br>• Monitoring<br>• Configuration<br>----------<br>• Maintenance<br>• Reports<br>• Provisioning<br>• Network Management<br>• System<br>• User<br>• About |
|  | Move the mouse cursor to each icon to open the drop down menu list.<br><br>Select the menu item and access into the configuration web page. | | | | |

### 3.2.5 Root Network, Group Network, and Selected CPE

The information on the dashboard will be shown according to the root network, the network group or a CPE selected.

#### 3.2.5.1 The Display Tab, Root Network

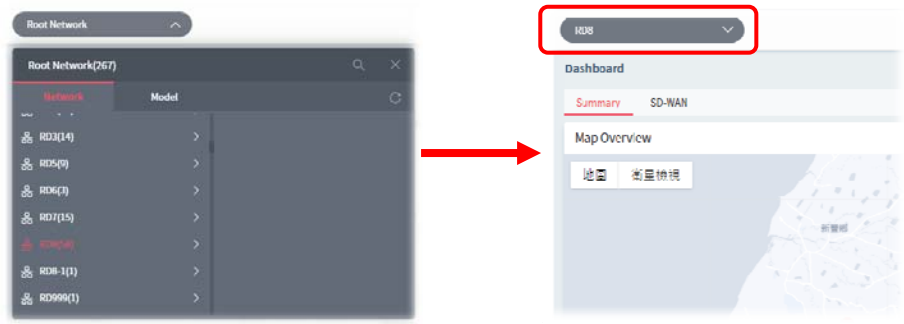
Click the **Display Tab** to display a drop-down list. This tab will display the name of the network group or the name of the selected CPE based on your selection. In default, Root Network will be shown on the Display Tab.




When the **Display Tab** shows a network group / CPE, and you want to return to Root Network, please move the mouse cursor on the Display Tab. Click to display the drop-down list and select the Root Network.

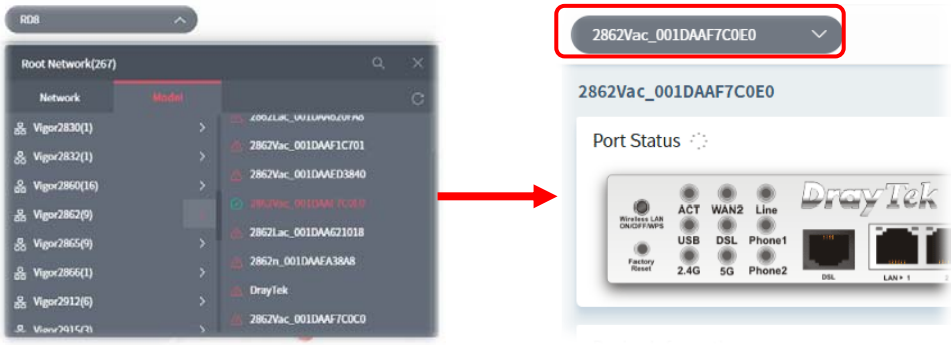
#### 3.2.5.2 The Display Tab, Network Group

Click the **Network Tab**. Move the mouse cursor on the network groups. Scroll and click the one (e.g., RD8) you want. Later, the selected network group will be shown on the Display Tab.




#### 3.2.5.3 The Display Tab, CPE Device

Click the **Model Tab**. Next, click the **>** button to list other CPE devices with the same model as the selected device. Select the device you want, then the selected CPE will be shown on the Display Tab.



### 3.2.6 Capture Packets

Offer options to view what packets that VigorACS server transmits or receives.

The system administrator might want to inspect what packets that VigorACS server transmits or receives. He/she can perform the packet capturing by using Wireshark or use the Capture Packets icon on the top-right of VigorACS web page. The captured packets information between VigorACS server and CPE client will be the basis of debugging.

This function can be enabled or disabled on **System>>System Parameter**, ID 81 PacketCaptureTool. In default, it is disabled.

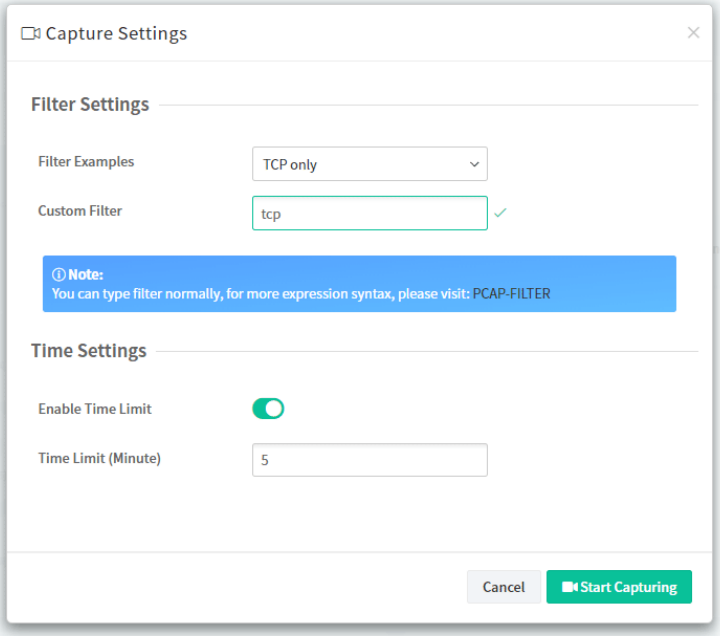
---

If no WinPcap or Libpcap installed on VigorACS server, the following message will be shown on the screen instead of Capture Packets icon.

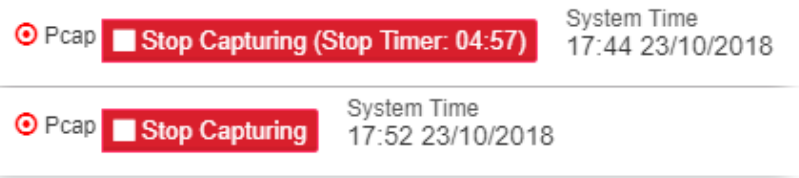
---

After clicking the Capture Packets icon, all of the network interfaces possessed by VigorACS server will be shown on a drop-down list. Under the network interface, corresponding IP address and MAC address also will be listed.

Click one of the network interfaces to configure settings for and perform the packet capturing.

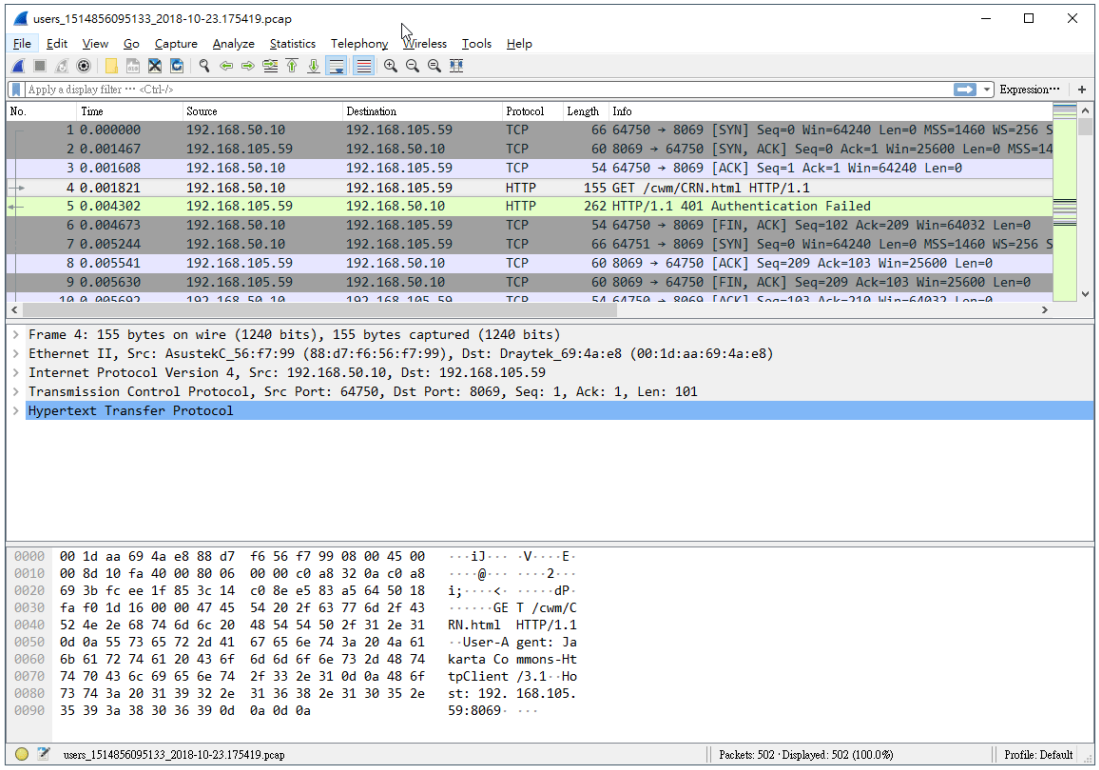



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Filter Settings** | **Filter Examples** – Choose a filter for filtering the packet corresponding to the type selected.<br>For example, when TCP Only is selected, only TCP packets will be captured and recorded. When IPv4 address 127.0.0.1 is selected, then only the packets coming from/sending to that IP address will be captured and recorded.<br>**Custom Filter** – Variation of Filter Examples will change the setting in Custom Filter. However, the system administrator can define the filter by entering correct syntax (e.g., host 172.16.2.222) if required. Packet capturing will be executed according to Custom Filter setting. |
| **Time Settings** | **Enable Time Limit** – If enabled, VigorACS server will capture the packets within the time limit defined below.<br>**Time Limit (Minute)** – Enter a value as a time limit. |
| **Start Capturing** | Click to start packets capturing.<br>● After clicking it, VigorACS server will continuously capture the packets until time up or manual stop. While capturing, the system administrator can perform any job on VigorACS still. The status of Pcap will be shown as the following figure. If **Time Limit** is disabled, the status bar will not show the timer information.<br>  <br><br>● When the time is up or stop the job manually, the status of Pcap will display the icons of Download and Delete and create a new capture. Click Download to store the file on the hard disk. Later, use the tool |

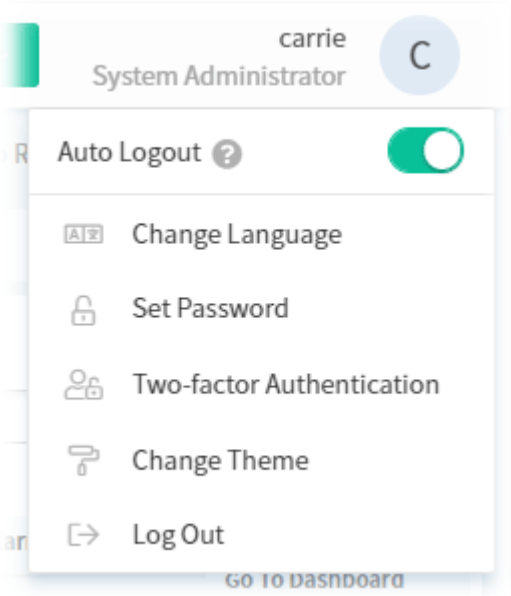
| | |
|---|---|
| | of Wireshark to check the content of the file.<br> <br>• After clicking **Delete and create a new capture**, VigorACS server will delete the packets just captured and restore the **Capture Packets** icon for next time using.<br>• In considering the network security, when someone performs the packet capturing on VigorACS server, other users are not permitted to use **Capture Packets** until the one finishes or stops the job. Only the one who performs the packets capturing can download the Pcap file.<br> <br>Click the **Refresh** button on the right side of Pcap status bar to check if someone else uses Pcap or not. |

The default file format of **Pcap** file: user ID_date (YYYY-MM-DD.hhmmss). The following example figure shows the content of pcap file by using Wireshark.



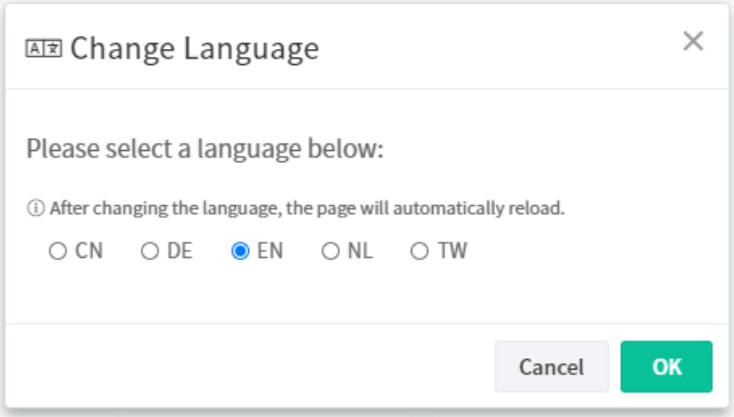
### 3.2.7 Set Password, Two-factor Authentication, Change and Log Out

Display current used account and offer selections for setting password, two-factor authentication, theme change and logout.




#### 3.2.7.1 Change Language

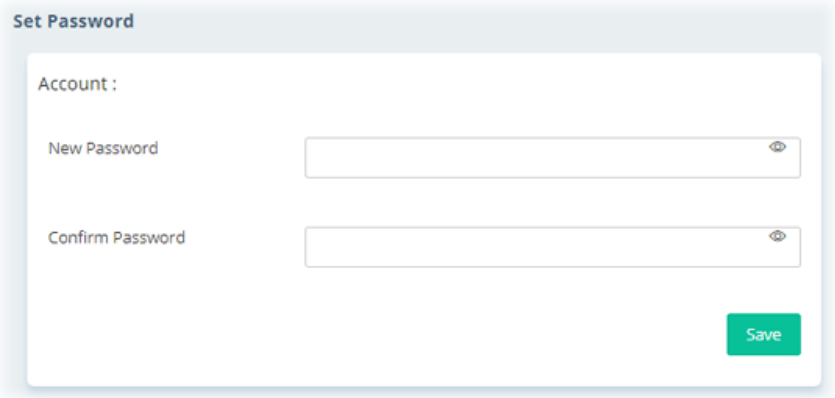
The web pages of VigorACS can be expressed with different languages,




CN means Simplified Chinese; DE means German; EN means English; NL means Dutch; and TW means Taiwan's Traditional Chinese.

#### 3.2.7.2 Set Password

The login password for current user account can be changed simply and easily by using Set Password from the drop down menu on the top-right corner.

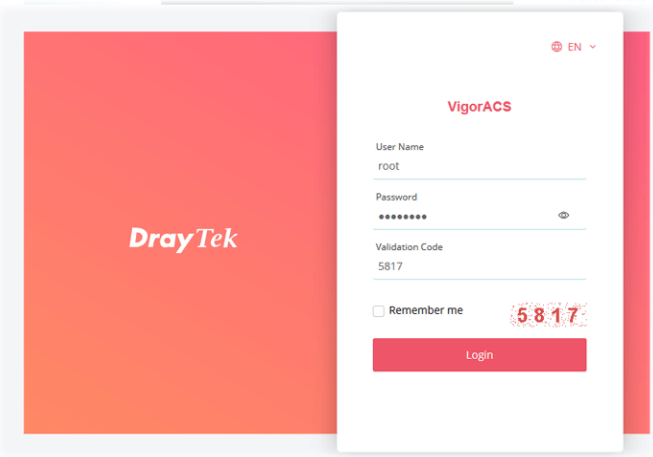



### 3.2.7.3 Two-factor Authentication

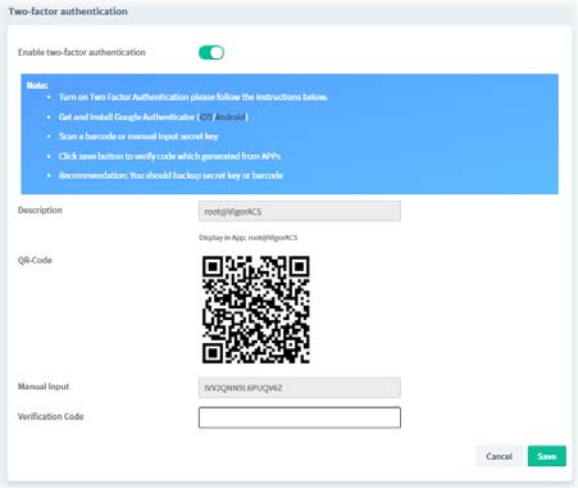
Usually, the system administrator can access into VigorACS by using user account and password. If network security is highly concerned, two-factor authentication will be strongly recommended.

For using two-factor authentication for accessing VigorACS;

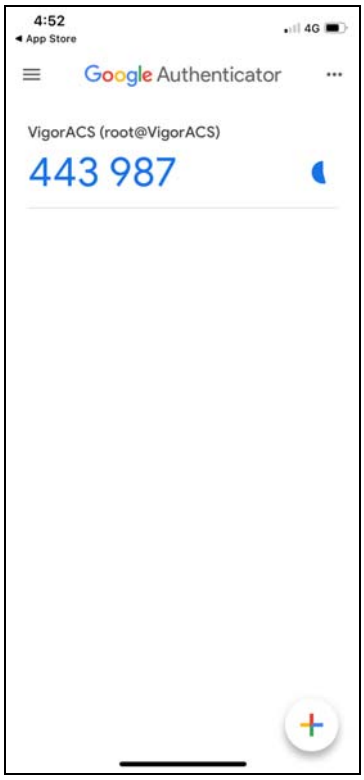
1. Get and install **Google Authenticator** (iOS/Android) first.
2. Login VigorACS 3 by using the user account and password.



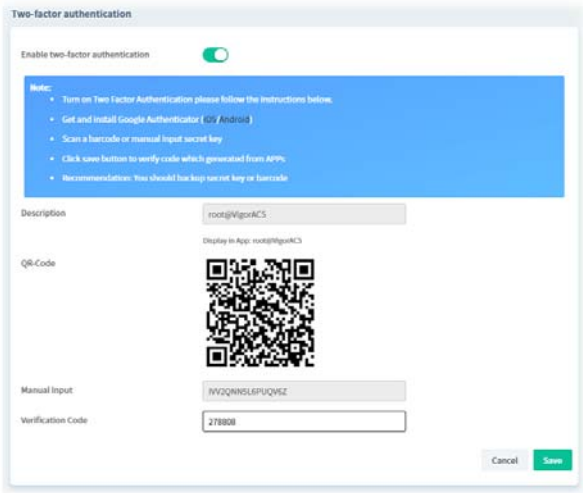

3. Open Root>>Two-factor Authentication and enable the button of Enable two-factor authentication.



4. Use your cell phone to scan the QR-Code shown on the Two-factor Authentication page.

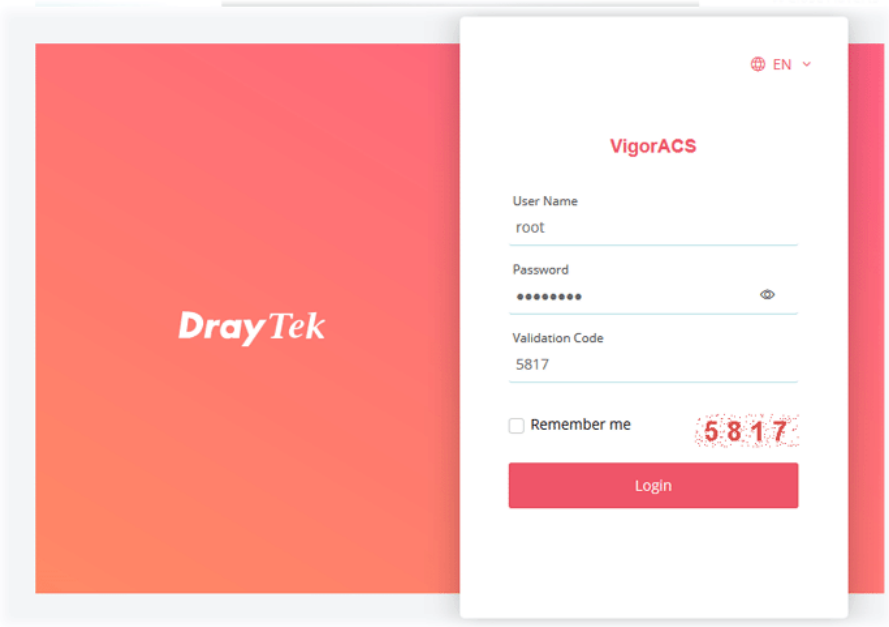



5. A key will be created randomly on the cell phone. Enter that key on the box of **Verification Code** and click the **Save** button.

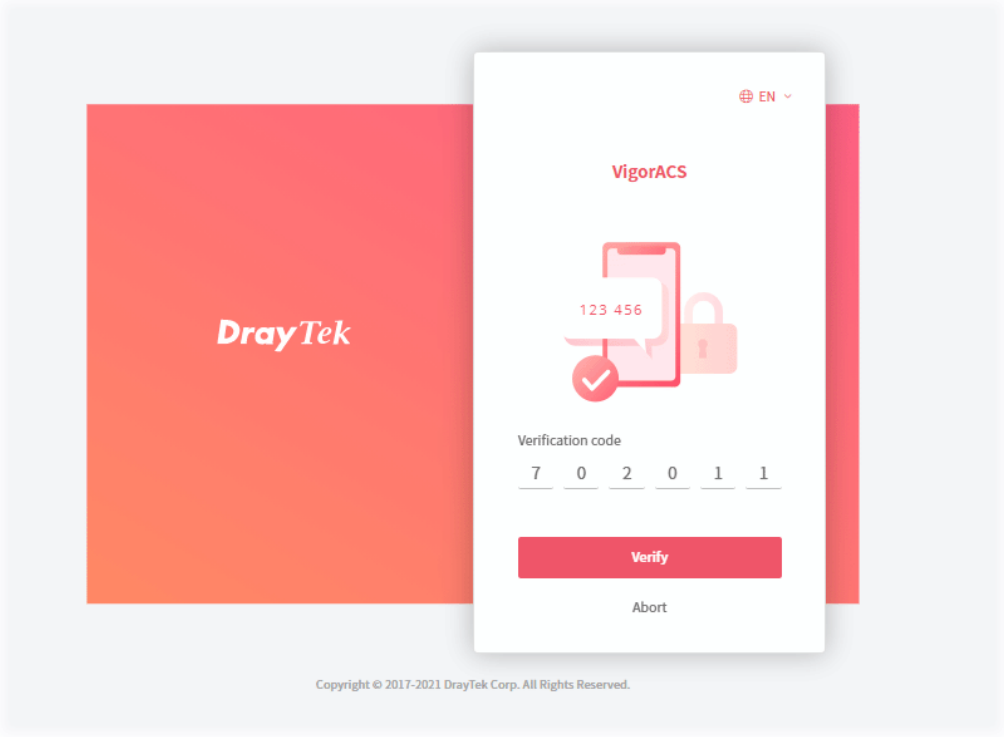



6. Logout VigorACS 3.

7. Re-login VigorACS 3. The first login web page requires you to enter the original user account and password.

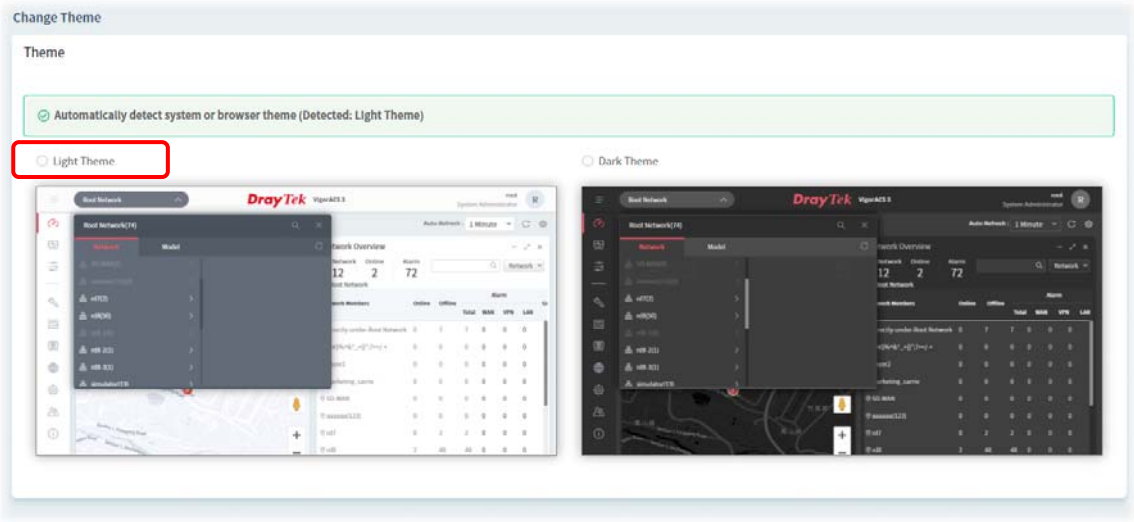



After clicking the Login button, the ***second*** login web page appears. Please enter the verification code (created randomly) obtained from the APP (Google Authenticator) on your cell phone and click the Verify button.



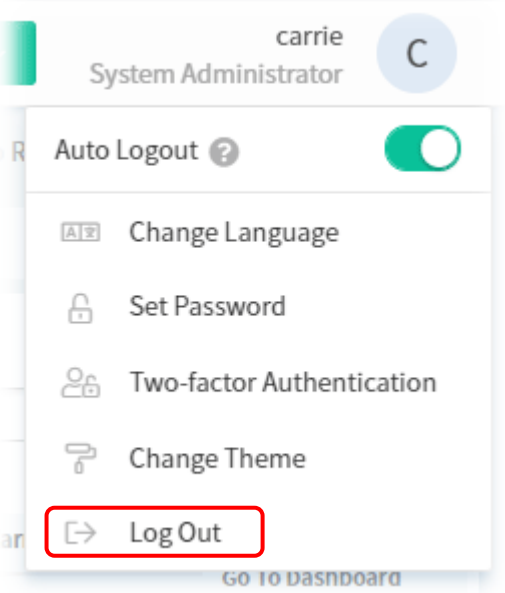
### 3.2.7.4 Change Theme

Click **Change Theme** icon to choose light theme or dark theme for screen display.

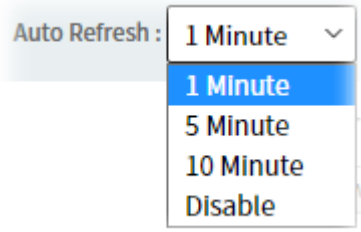
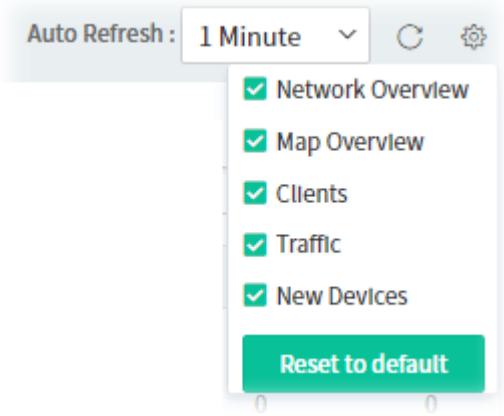



### 3.2.7.5 Logout VigorACS

Click **Logout** icon to logout VigorACS.

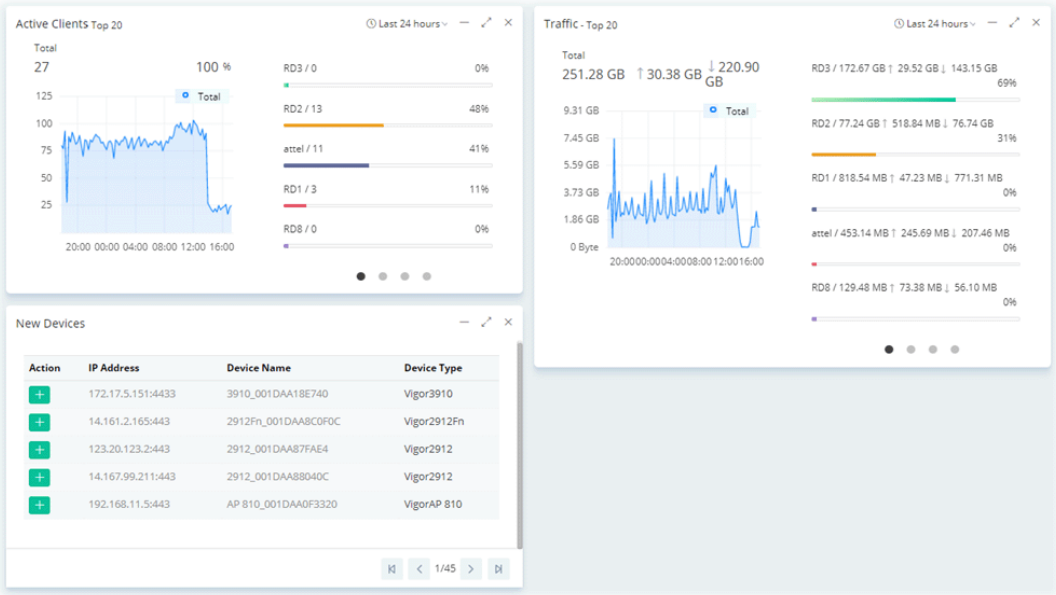


### 3.2.8 Auto Refresh, Manual Refresh, and Widget

| Item | Description |
|---|---|
| Auto Refresh | Select the time interval for refresh the web page automatically.<br>  |
| Manual Refresh | Click to refresh the web page immediately. |
| Widget | There are six display views to select, including Network Overview, Map Overview, Clients, Traffic, New Devices and Reset to default. Only the selected one(s) will be displayed on the dashboard.<br>  |

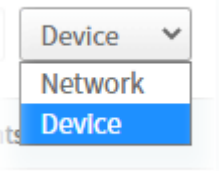
### 3.2.9 Overviews

There are five types (Network Overview, Map Overview, Clients, Traffic, New Devices) of overview under the Root Network. Use the Widget drop menu to select or deselect the type of the overview.

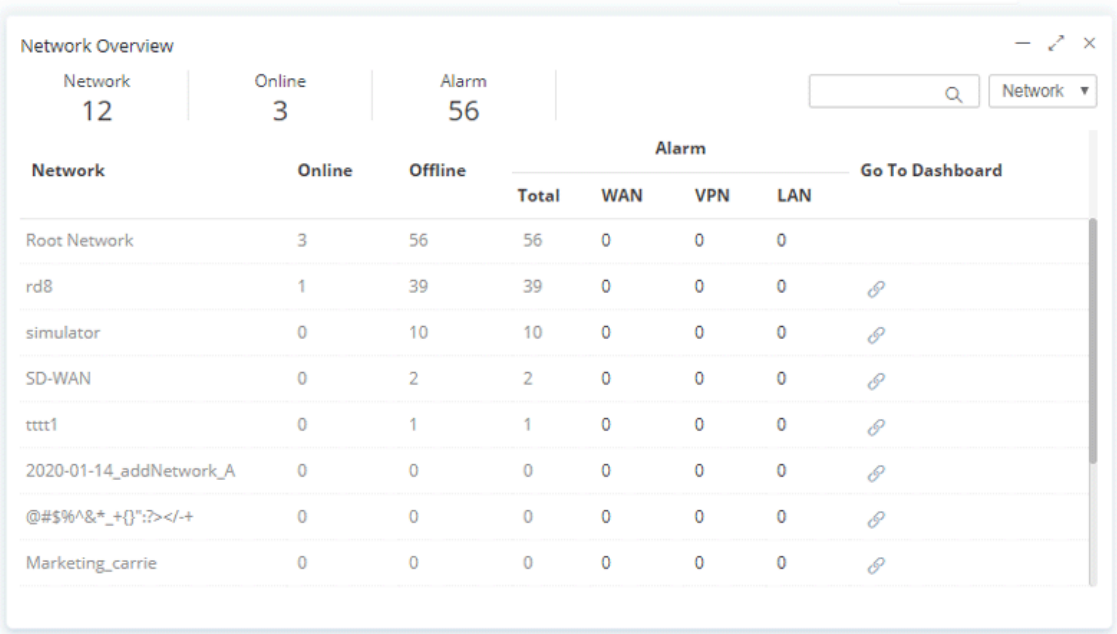



#### 3.2.9.1 Network Overview / Device Overview

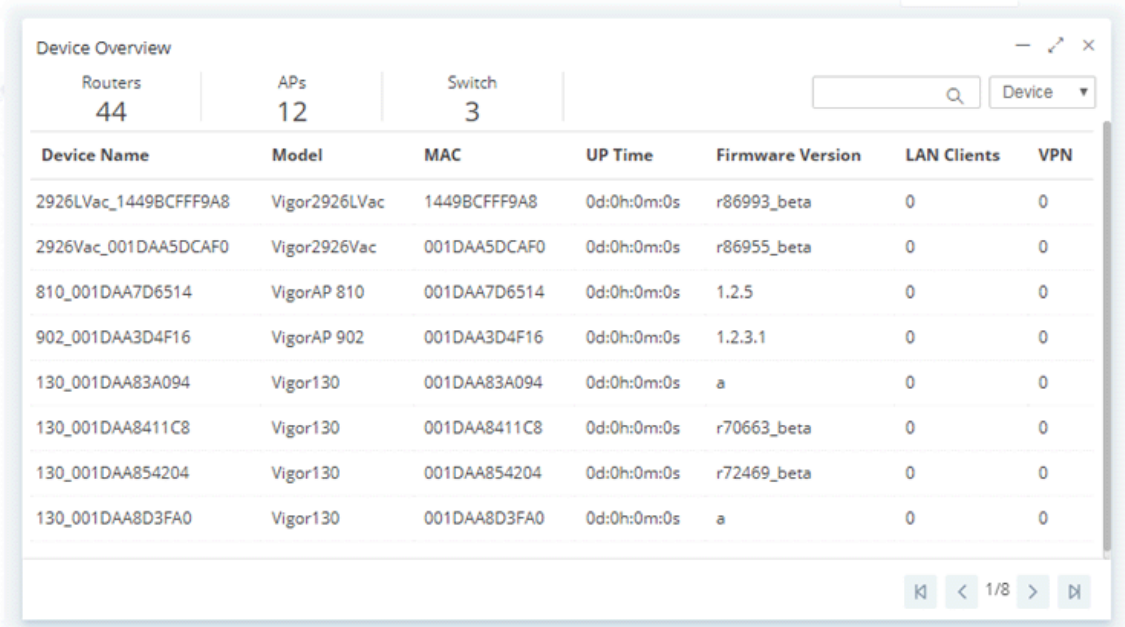
This area displays the Network Overview or the Device Overview.

| Item | Description |
|---|---|
| Category | Switch between **Network** or **Device**.<br>  |
| / | -(Collapse) - Hide the page.<br>(Fullscreen) - Display the page in fullscreen. |
| | x (Delete) - Delete this widget. |

Under **Network Overview**, all of the networks with names can be seen on this area. Use the scroll bar to view others networks. Icons of W, V and L represent WAN Alarm, VPN Alarm and LAN Alarm. The digit next to the word, Alarm, indicates the number of warning message received by that network. The number next to ONLINE indicates how many devices are active; the number next to OFFLINE indicates how many devices are inactive.



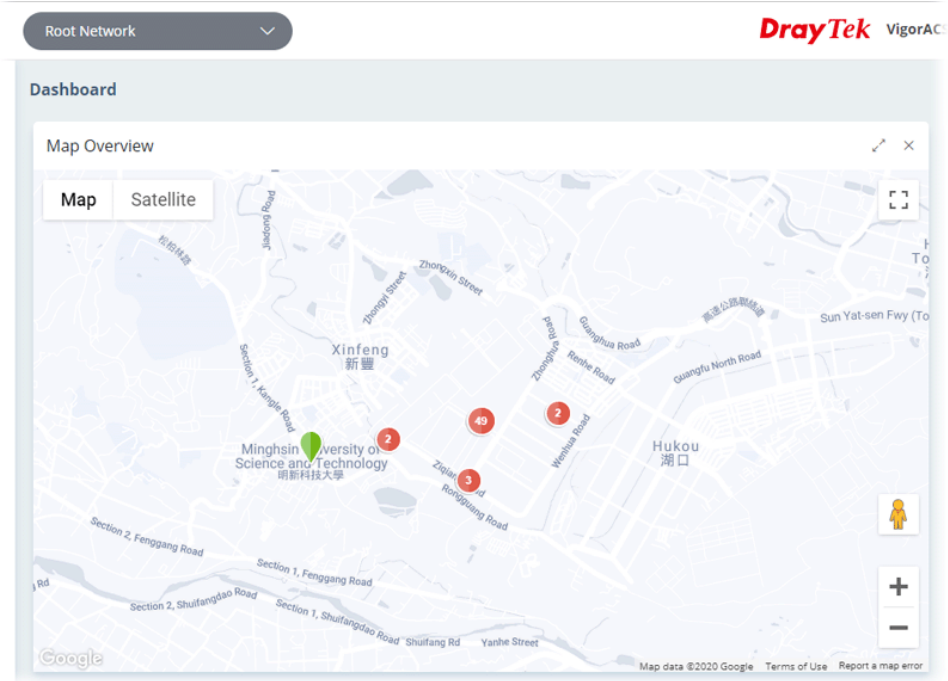

Under **Device Overview**, move the scroll bar left and right to check basic information for each device. Click **>>** (Next) or **<<** (Previous) arrow to display next page for checking information for other devices.

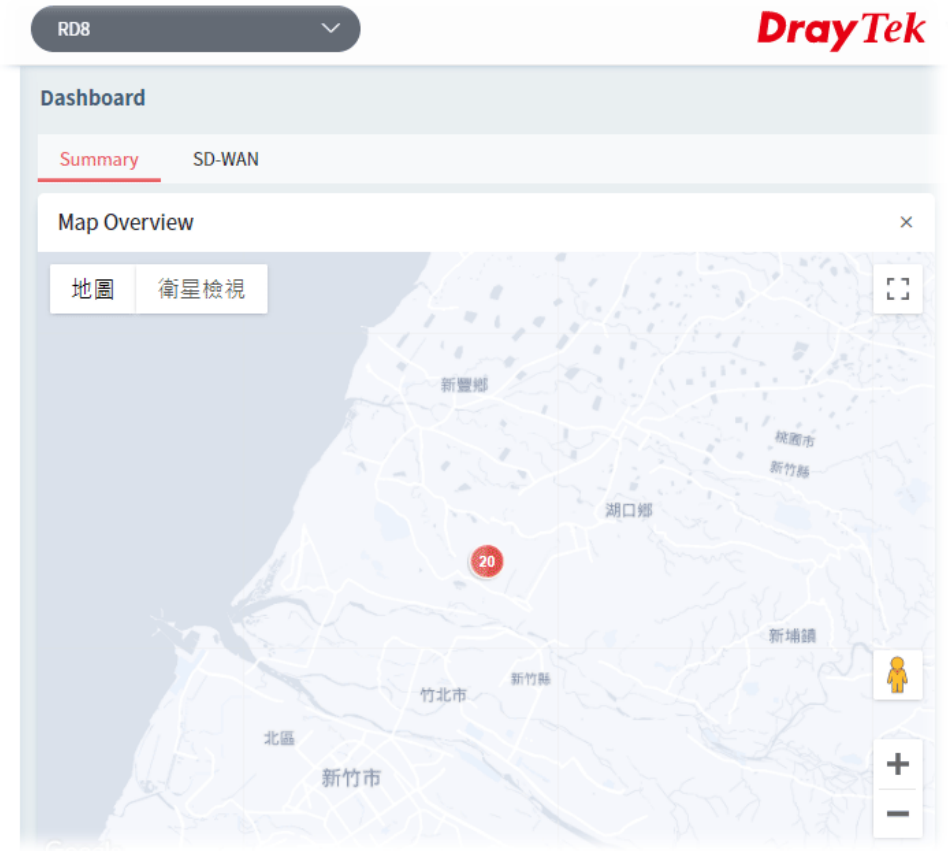


### 3.2.9.2 Map Overview

This map displays the location of the devices managed by VigorACS. The number on the map points the quantity of the devices classified under the root network or network group. Move your mouse on the number and click it. The map will be zoomed in with more detailed information.

Map Overview will vary according to the root network or the network group selected.



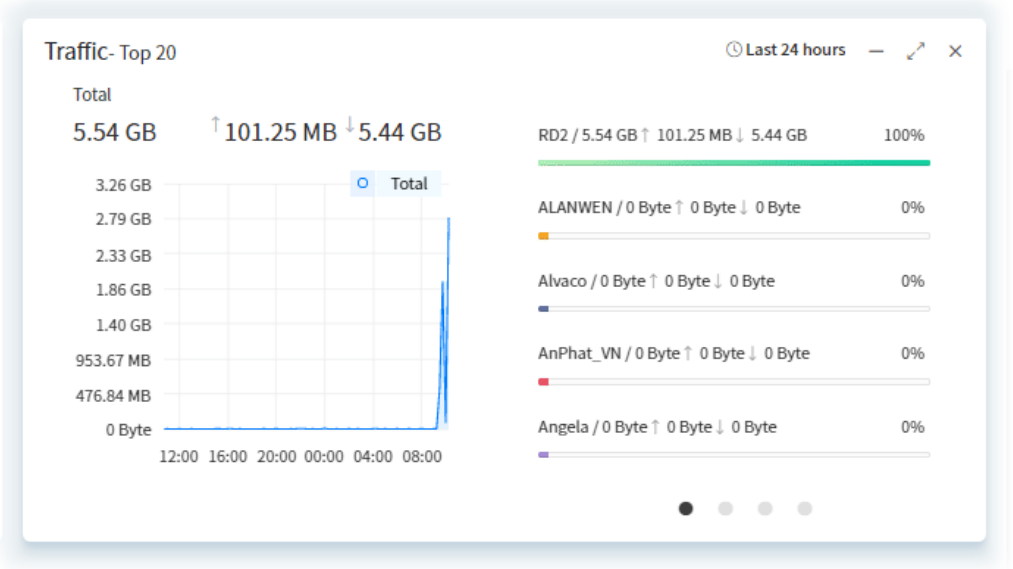
### 3.2.9.3 Clients

This area displays the top 10 clients or top 20 clients accessing into VigorACS during the last 24 hours, 7 days or 30 days.

| Item | Description |
|---|---|
| Last 24 hours | Use the drop down list to specify the time period, last 24 hours, 7 days or 30 days. |
| − / ⤢ | - (Collapse) - Hide the page.<br>⤢ (Fullscreen) - Display the page in fullscreen. |
| ✖ | x (Delete) - Delete this widget. |

### 3.2.9.4 Traffic

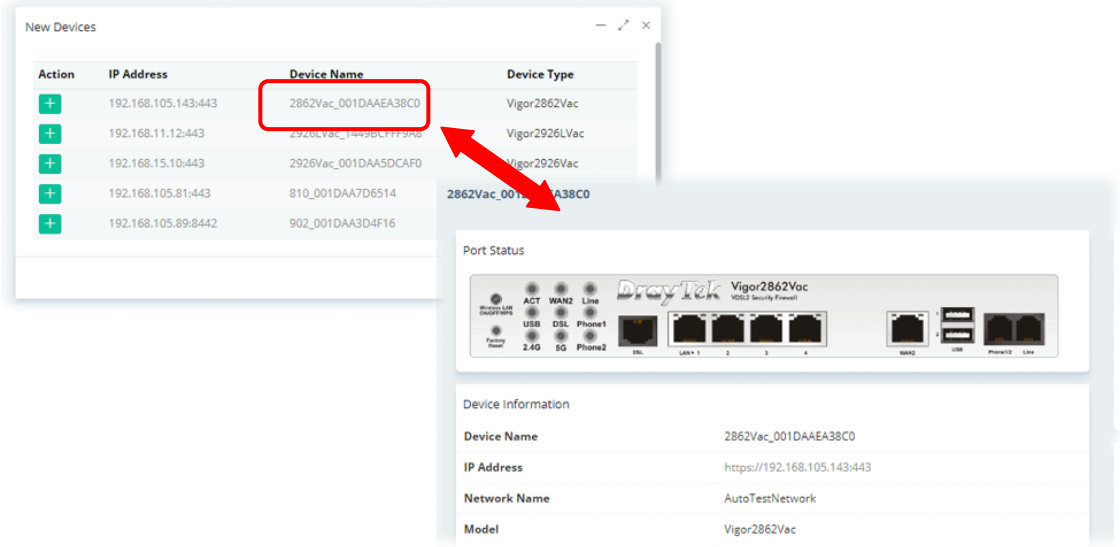
The figure displays the traffic for top 10 or 20 groups/devices during the last 24 hours, 7 days or 30 days.




| Item | Description |
|---|---|
| Last 24 hours | Use the drop down list to specify the time period, last 24 hours, 7 days or 30 days. |
| / | - (Collapse) - Hide the page.<br>(Fullscreen) - Display the page in fullscreen. |
| | x (Delete) - Delete this widget. |

### 3.2.9.5 New Devices

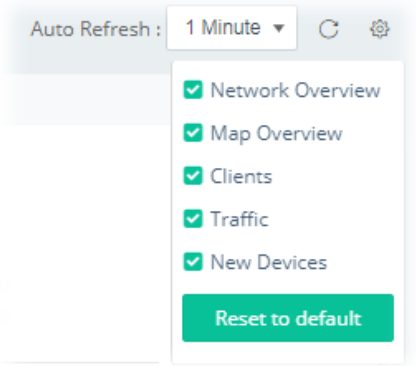
New added device(s) can be found on the field of **New Devices**. When you move your mouse on the device name of the device and click it, a detailed information page for that device will be displayed on the screen.




| Item | Description |
|---|---|
| − / ⤢ | - (Collapse) - Hide the page.<br>⤢ (Fullscreen) - Display the page in fullscreen. |
| ✖ | x (Delete) - Delete this widget. |
| + | Click the button to add a new device onto the network.<br>Refer to "Applications, A.3 How to Assign a New Added CPE to a Network?" for detailed information. |

### 3.2.9.6 Reset to Default

Use the Widget drop menu to select or deselect the type of the overview. Or, click Reset to default to restore the factory default overviews on the dashboard.



### 3.2.10 Icons Used in VigorACS 3

| Item | Description |
|---|---|
| + | Add a new device. |
| − / ⤢ | Hide the page / Display the page in fullscreen. |
| ✖ | Delete the selected widget. |
| / | Switch these two icons by click the mouse cursor on it.<br>- means “Enable”.<br>- means “Disable”. |

## 3.3 Operation Procedure

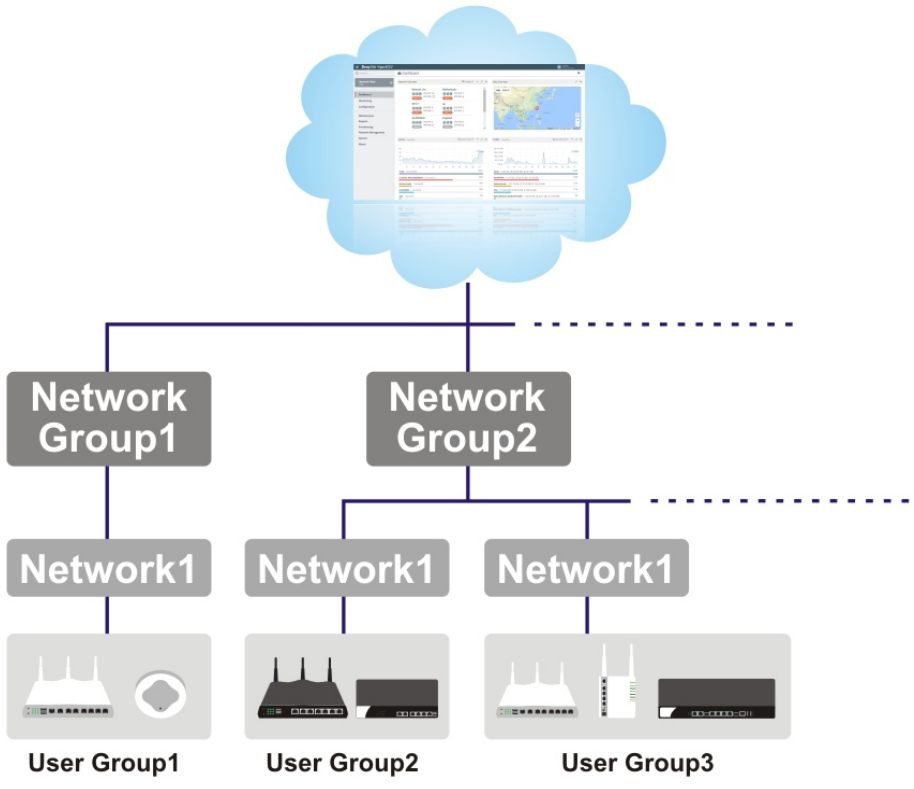
Follow the instruction listed below to operate VigorACS 3:

- Create networks.
- Create users and user groups.

  A user can own several CPE devices; however, each CPE device can be assigned to one “user group” only.

  User shall be assigned under different user groups. RootGroup is the default user group.
- Edit and modify the settings for the TR-069 devices.

Below shows a brief illustration to describe the relationships among CPE, user group, network and network group.



# Applications

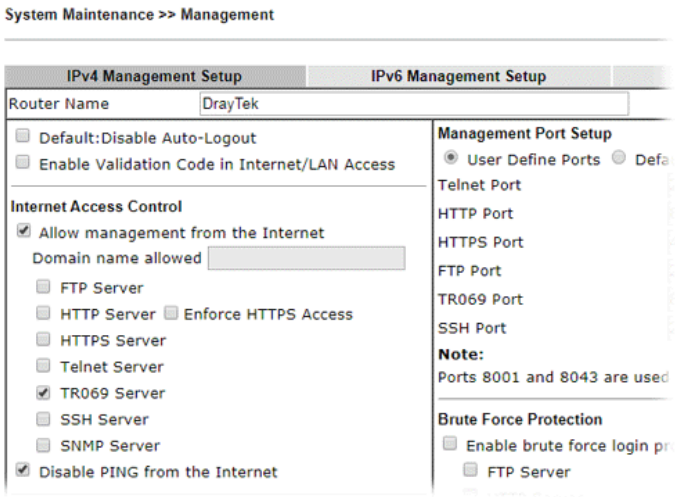
## A.1 How to Register a CPE onto VigorACS 3?

This section briefly shows a simple way to register a CPE onto VigorACS 3 with few steps. For detailed information, refer to **Chapter 4**.

The CPE to be managed by VigorACS 3 must be configured and restarted. Here we take Vigor2926Vac as an example.

Note that STUN setting is required if CPE is behind a NAT device, for the purpose of keeping the connection between VigorACS 3 and Vigor device up.

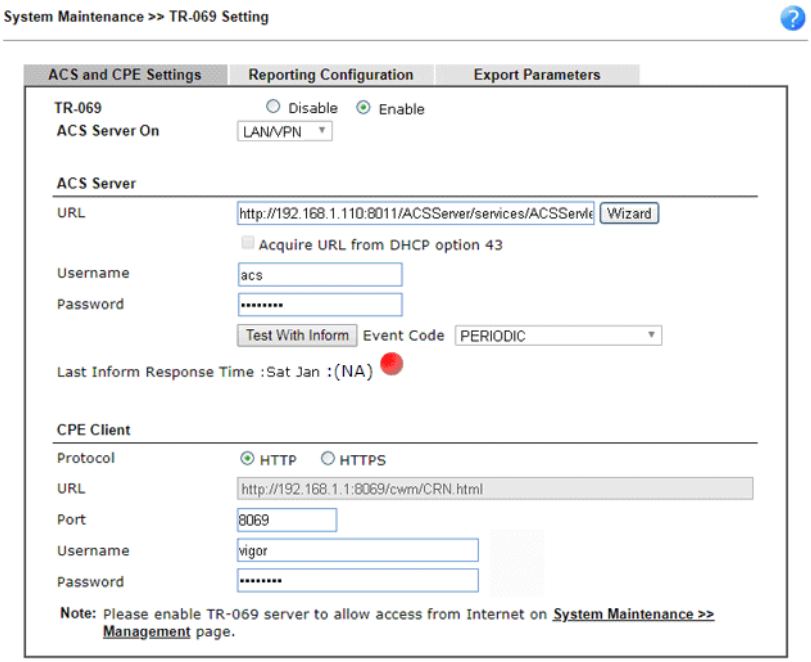
1. Access into the web user interface of Vigor router.
2. Open **System Maintenance>>Management.**




- Allow management from the Internet – Enabled.

- TR-069 Server – Enabled.

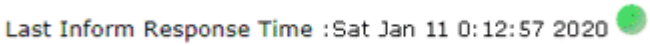
3. Open **System Maintenance>>TR-069**.



- Specify the interface for ACS Server On.

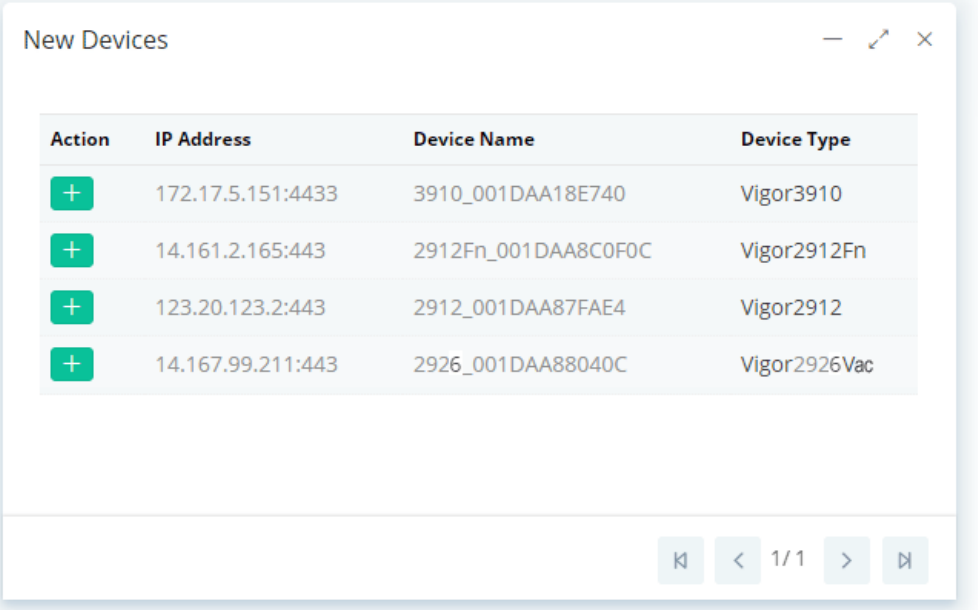
- Set URL, username, password for network group.

4. Click **OK** and click **Test With Inform**. When the green light appears (on the Last Inform Response Time), the settings on CPE have been configured well.




5. Open the homepage of VigorACS 3.

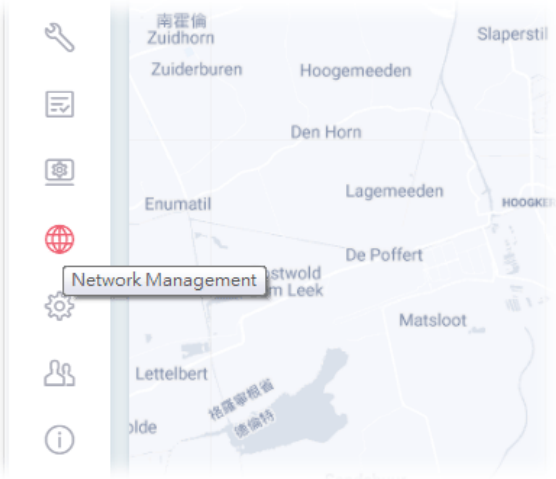
6. Now, Vigor2926Vac has been registered onto VigorACS 3 and displayed on the homepage.



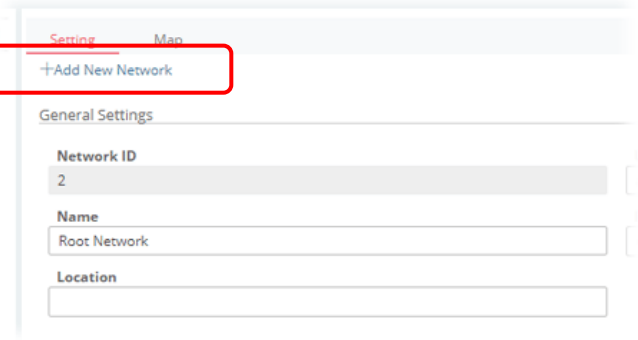
## A.2 How to Create a New Network?

VigorACS allows the administrator to build several networks (and sub-network) for different CPE devices under the root network.

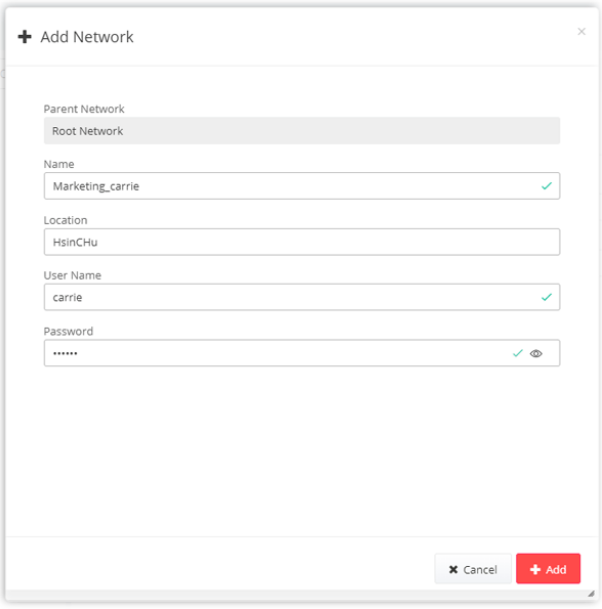
1. Only the administrator has the right to create a new user group.
2. From the MENU bar, click **Network Management**.




3. When the following page appears, click the link of **+Add New Network**.




4. A pop-up window appears. Type the required information.



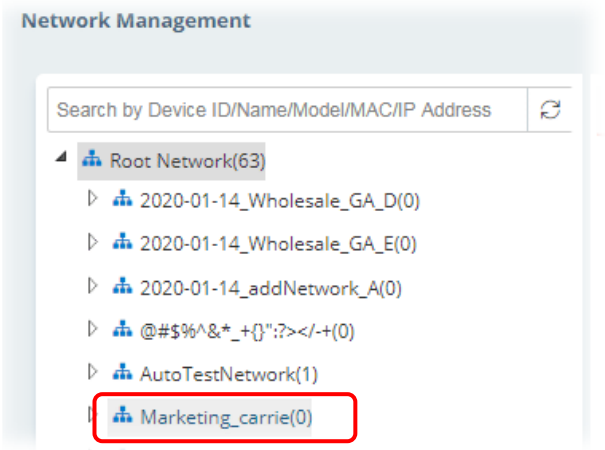
- Name - Enter a new name of the network.

- Location – Define the location of such network.

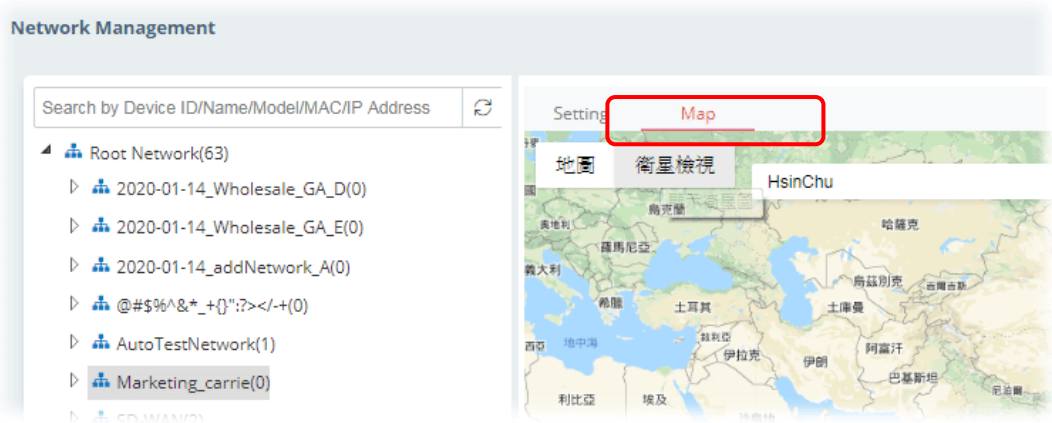
- User Name – Enter a user name for such network.

- Password – Enter a password for such network.

5. Click **+Add** to save the settings. The new created network will be seen under the **Root Network**.



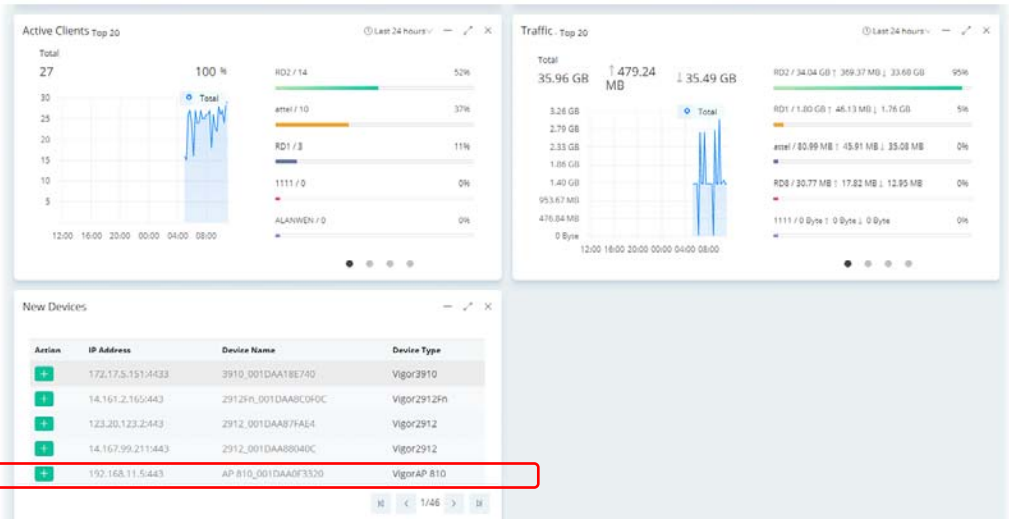

6. Click the **Map** tab. Manually input specific location of the device on the input box; GoogleMap will show the location for the new created network.



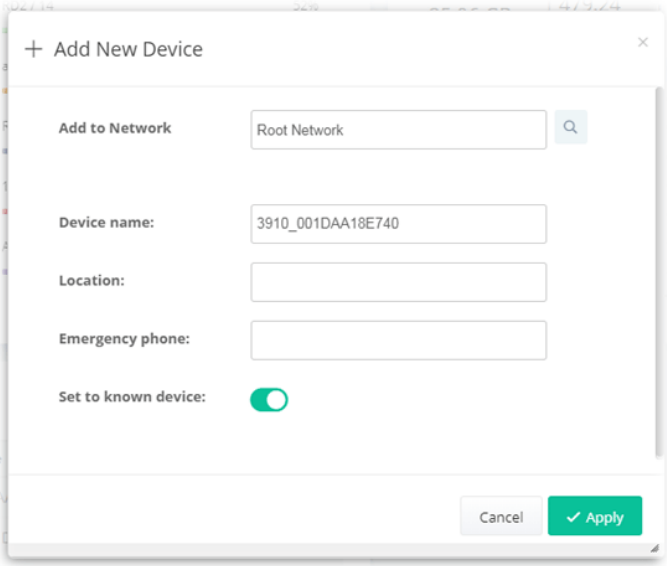
## A.3 How to Assign a New Added CPE to a Network?

New added device can be grouped under Network. If no assignment, the new device will be grouped under Root Network in default.

1. On the Dashboard, locate the device from **New Devices**. Here, we take Vigor3910 as an example.




2. Click the add icon (+). The following dialog will appear.



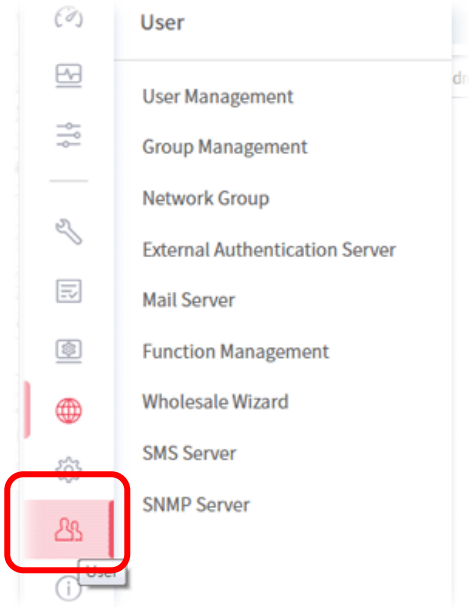

- Add to network – Choose the network from the drop down list.
- Location – Enter the location of the selected device.
- Emergency phone – Enter the mobile phone for communication.
- Set to known device – Click to make the device visibly or invisibly.

3. Click **Apply** to save the changes.

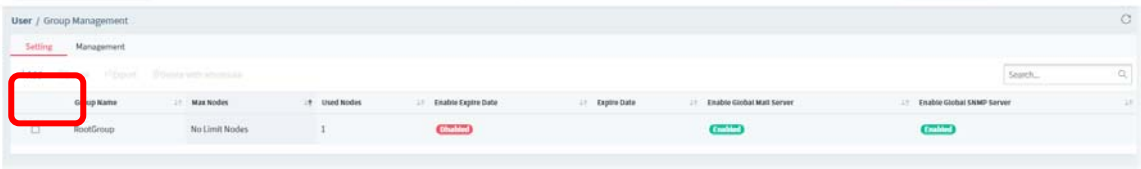
## A.4 How to Create a New User Group?

Only the administrator can create a new user group.

1. From MENU bar, open the **User** menu.

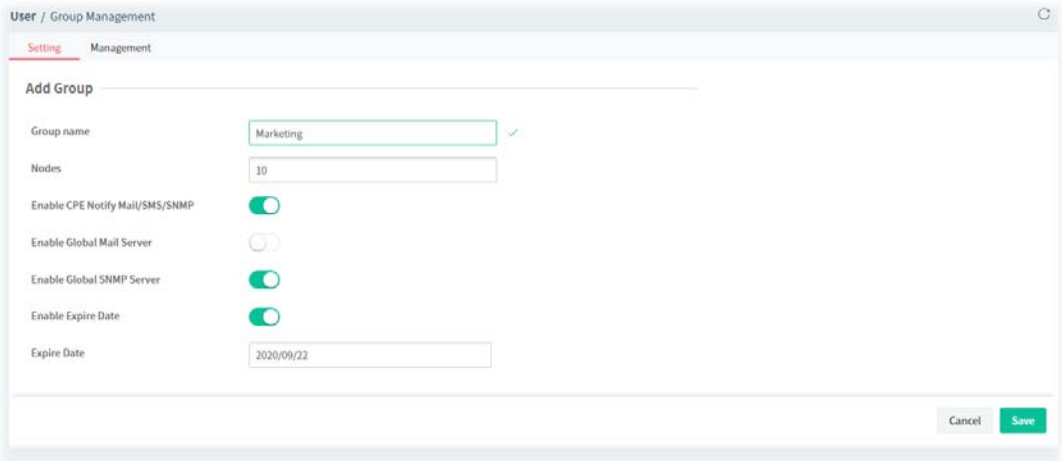



2. Click **Group Management**. The following page will appear.




RootGroup is a default setting.

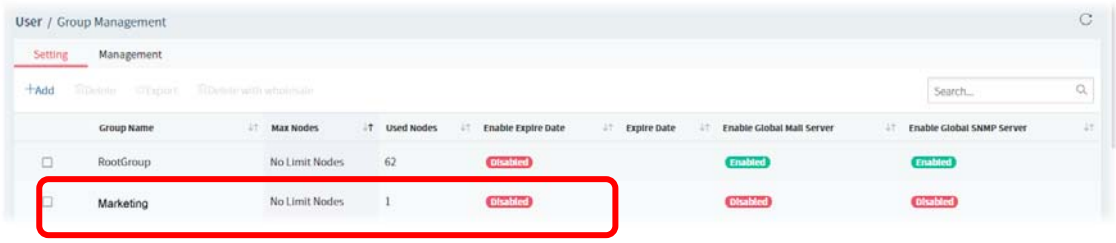
3. Click **+Add** to open the following page for creating a new one.




- Group name – Enter a new name.
- Nodes – Use ▲ or ▼ to add or decrease the number of nodes.
- Enable Global Mail Server – Click to enable or disable the service.
- Enable Global SNMP Server - Click to enable or disable the service.
- Enable Expire Date - Click to enable the Expire Date mechanism.

- Expire Date – If it is enabled, click the entry box to choose the date.

4. Click **Save** to save the settings and exit the dialog. The new network group has been created and displayed on the screen.



This page is left blank.

# Part II

SD-WAN

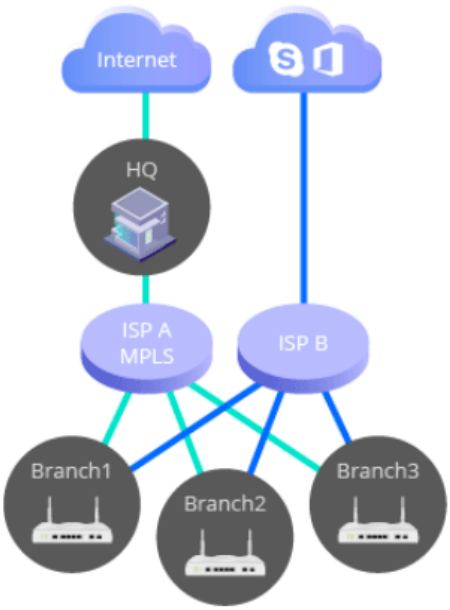
# Chapter 4 SD-WAN Solution

Traditionally most business applications were running on the private servers in the HQ, and MPLS that routes all traffics to the center site made this model quite efficient.

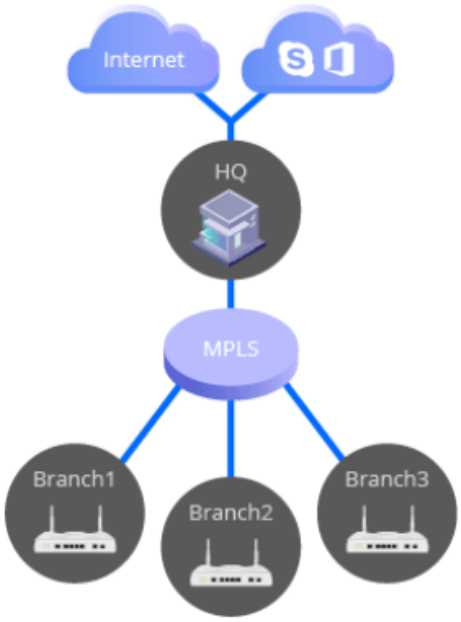
However, with adopting more and more SaaS and private/public cloud applications, we need new technologies that can efficiently and dynamically route different traffics either to the central site or to the cloud directly.

SD-WAN is the solution to make the complex routing scheme simple and intuitive. Based on traditional load balancing and failover functions, SD-WAN further improves user experience by focusing on interface and application quality.

Take a look at the following two figures. The right one expresses a traditional network connection which is tunneled via the central site at a higher cost. However, the left one shows the direct Internet access with lower cost with the feature of SD-WAN.



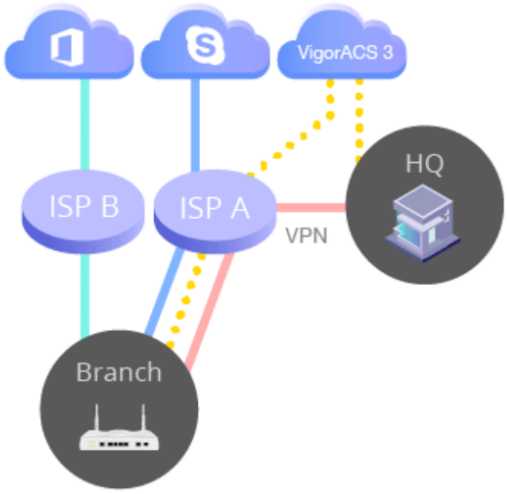

Direct Internet Access with lower cost




Tunneled via Central Site with higher cost

## 4.1 Topology of SD-WAN, Edge Router and ACS Server

VigorACS is the central software where network administrators perform the configurations, provisioning, and monitoring the activity. The multitenant capability makes xSP services easy.



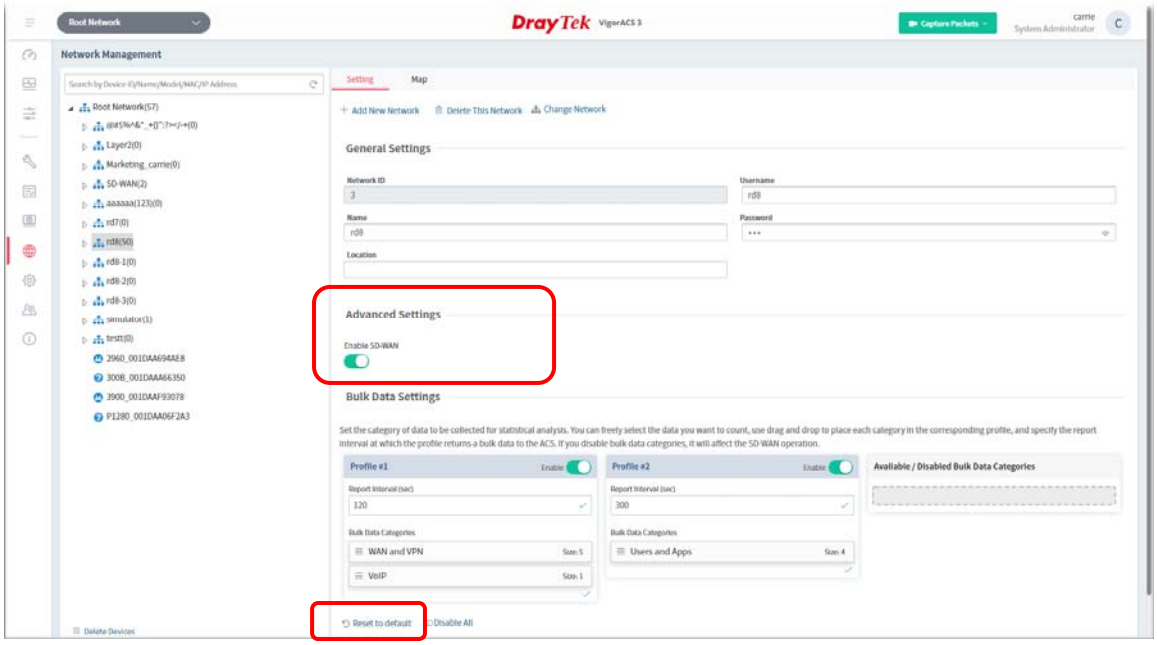

The physical routers installed in HQ and branches are named **edge router**.

The network administrators can establish VPN tunnels (IPsec by default) from the branches to the HQ to form a Hub-and-Spoke topology. These routers can receive SD-WAN configurations from the VigorACS server, perform the edge computing according to SD-WAN policies, and upload the data to the **VigorACS server** for monitoring.

At present, the edge router (supporting SD-WAN) includes Vigor2927 series and Vigor2865 series.

### 4.1.1 Enabling SD-WAN on VigorACS

To enable SD-WAN function on VigorACS, simply open **Network Management** under **Root Network**. Specify a network group (e.g., RD8) which contains the CPEs supporting SD-WAN features. On the Setting page, turn on the toggle button of **Enable SD-WAN**. Then click **Reset to Default** to use the bulk data with the default values. At last, click **Save**.




The main features for SD-WAN are manifested in three aspects:

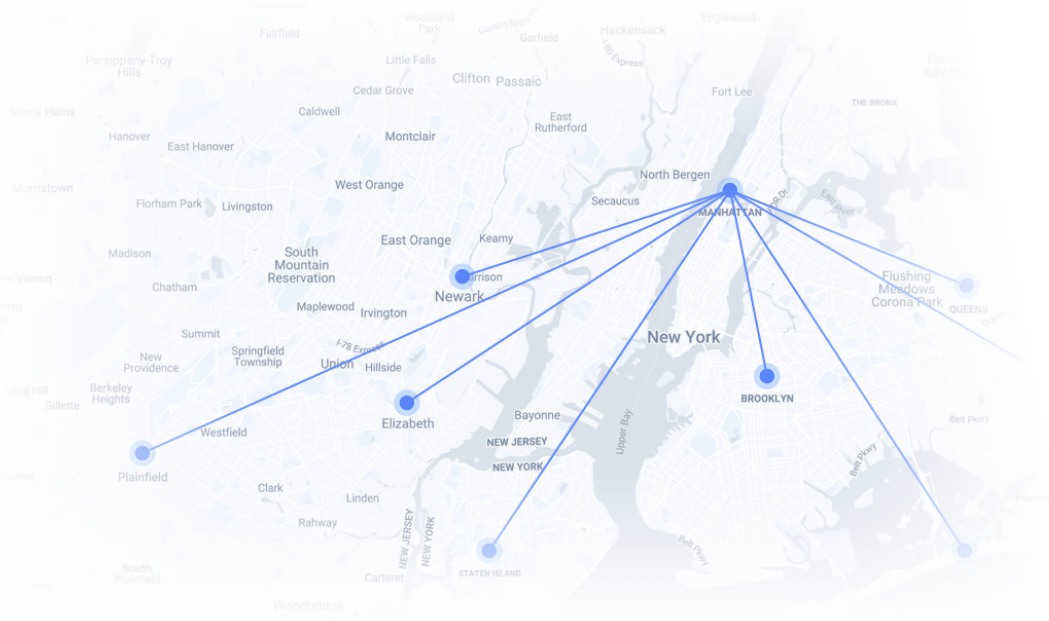
- Auto VPN
- VoIP WAN, and
- Full Traffic Control with SD-WAN Route Policy

### 4.1.2 Auto VPN

There are two types of Auto VPN, Hub and Spoke and Full Mesh.

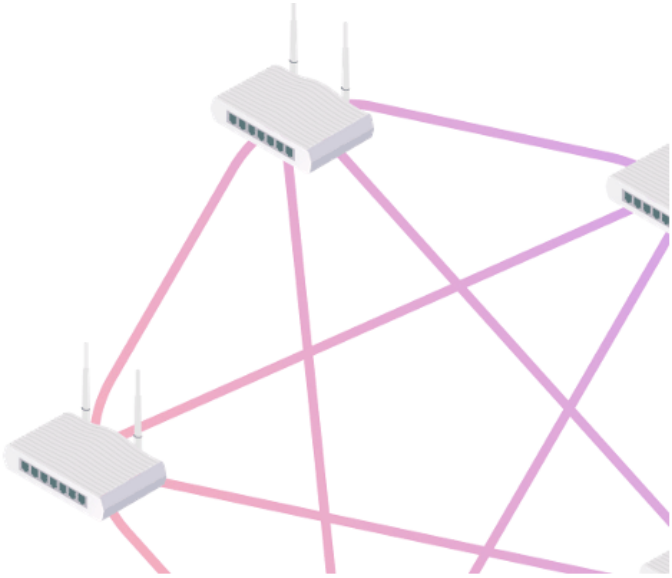
- For Hub and Spoke(s)

  Select one of the devices as a hub router; other devices will be regarded as "spokes". VigorACS server will automatically create one IPsec tunnel, with AES256 encryption method, from each spoke to the hub router. If a subnet conflict occurs, VigorACS server is capable to design and suggest LAN subnets for all devices.




- For Full Mesh

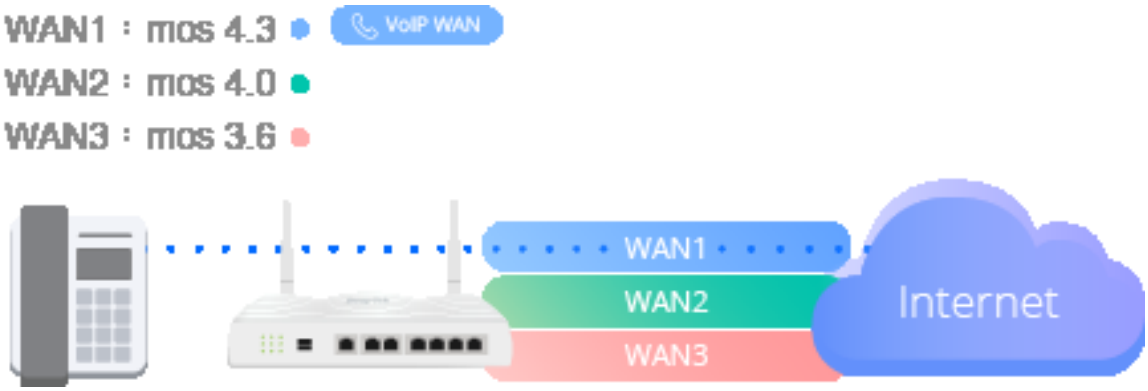
  VigorACS server will create tunnels between each router automatically. If a subnet conflict occurs, VigorACS server is capable to design and suggest LAN subnets for all devices.



### 4.1.3 VoIP WAN

The router can automatically detect the best quality interface, named with VoIP WAN, from existed WAN interfaces to optimize VoIP performance.

SIP registrations will follow the VoIP WAN to make sure the upcoming inbound & outbound VoIP Call will be sent via VoIP WAN.




In a Route Policy, the Administrator can select VoIP WAN as the Interface for VoIP. So VoIP will always been sent via best quality WAN.

Real-time Call Quality Monitoring

- Every single call is continuously monitored with MOS (mean opinion score), from the beginning till the end.
- Supported interface including WAN and VPN.

Live Failover when Having Poor Call Quality

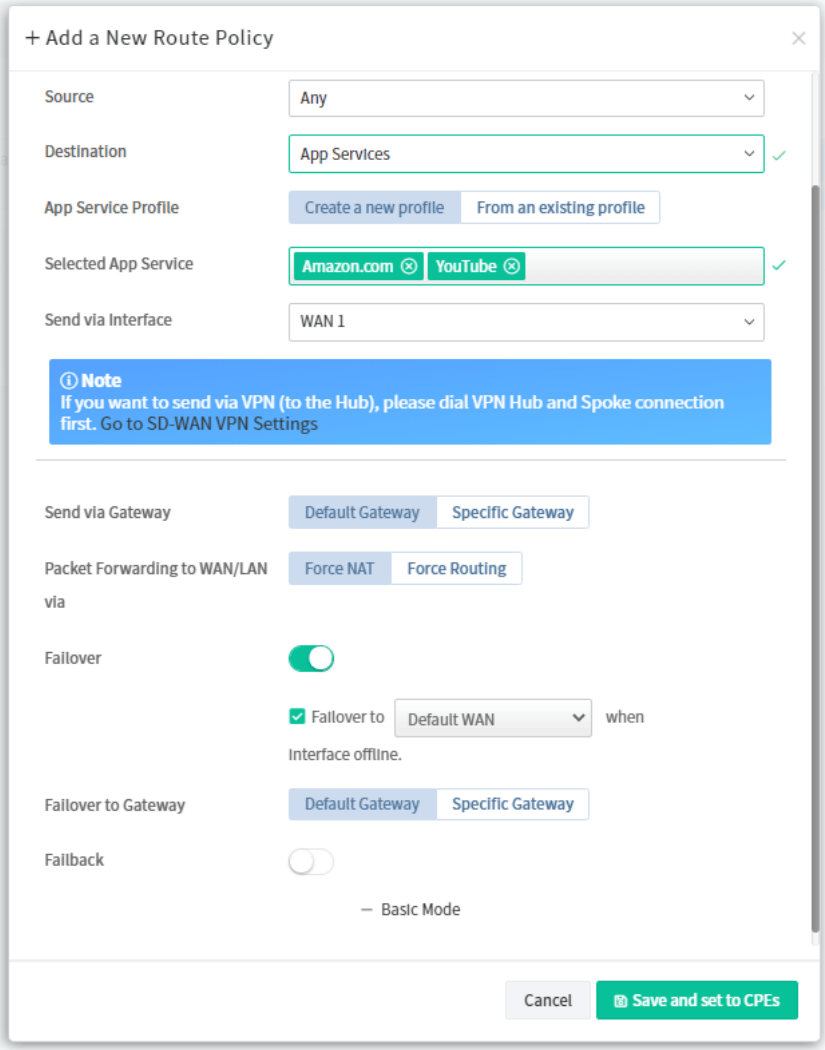
- Even being sent via best-quality WAN, sometimes call quality could still be poor due to some hops along the path.
- If enable this function, router will failover the RTP sessions for the poor quality calls (while good quality calls remain with VoIP WAN).

Live Failover Scenarios

- Interface is selected as VoIP WAN => failover to 2nd VoIP WAN.
- Interface is selected as VPN to Hub=> manually select your failover interface.

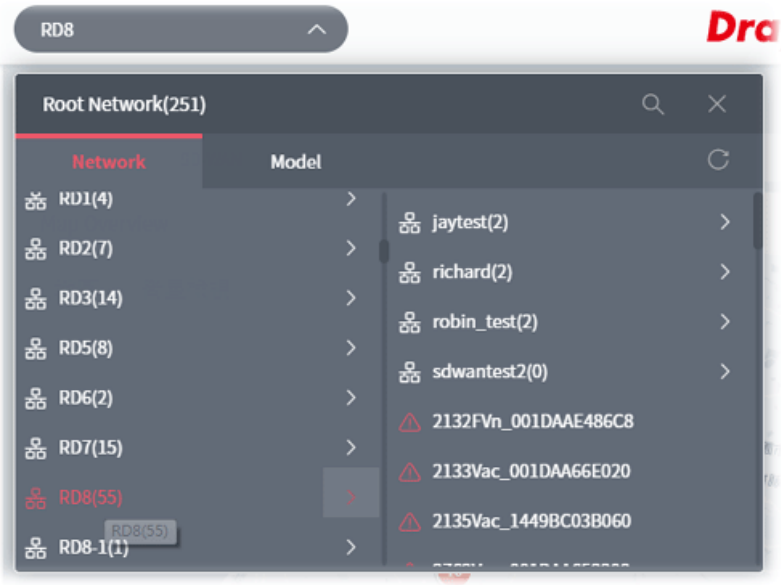
### 4.1.4 Full Traffic Control with the Route Policy

SD-WAN provides complete routing control by allowing Network Admin to specify the desired route for selected applications/domains to make sure the specific routing scenarios can be accomplished.

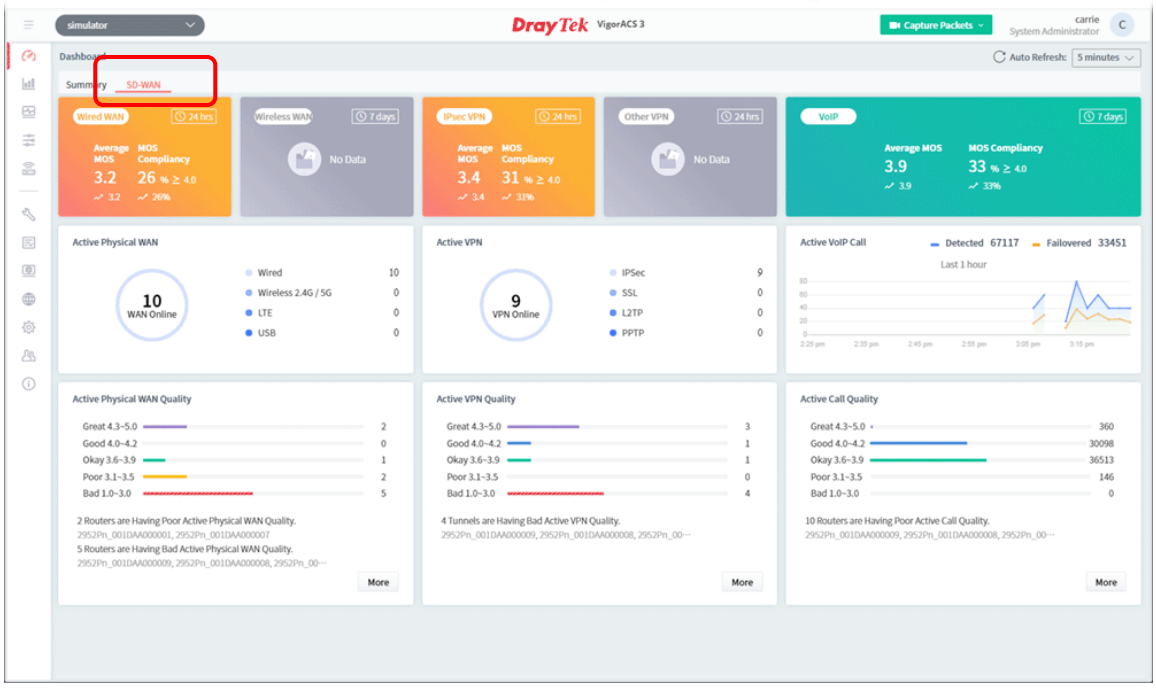


## 4.2 Dashboard for SD-WAN Network Group

To display the SD-WAN dashboard, select a network group first. Find the one you want from the Network list under the Root Network. In this case, we choose RD8 as an example.




Click the **SD-WAN** tab to display the page of dashboard (for monitoring).

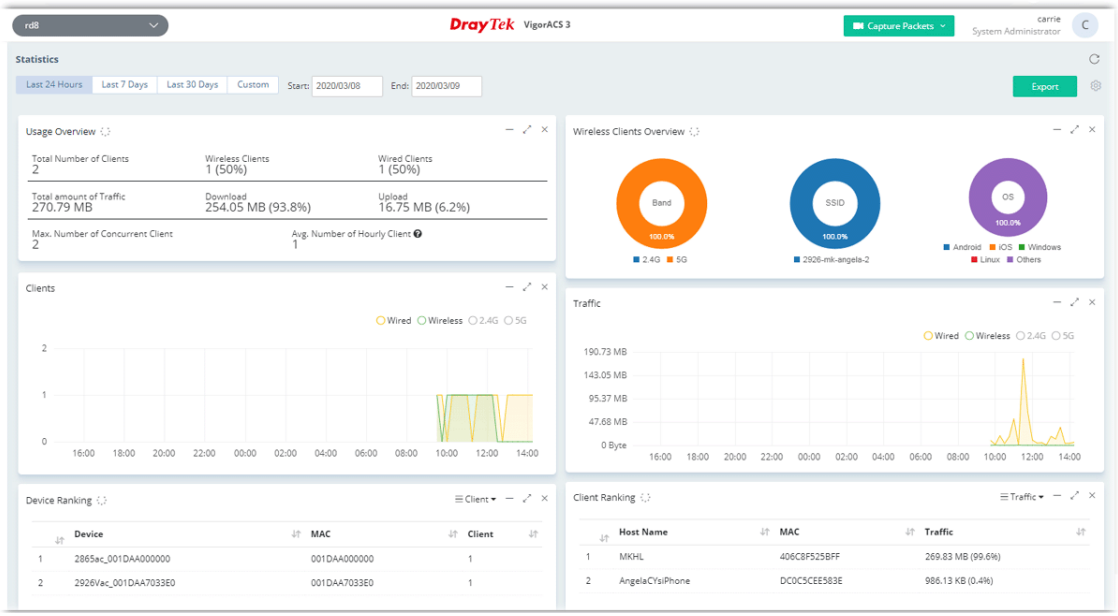



| Item | Description |
|---|---|
| **Wired WAN / Wireless WAN** | Wired and Wireless WAN (including wireless 2.4G/5G WAN, LTE WAN, and USB WAN) quality monitoring are separated as wired WAN usually provides better quality. Only VPN tunnels that are established by the SD-WAN VPN tool are counted for VPN MOS. |
| **IPsec VPN / Other** | Displays the quality levels (Great, Good, Okay, Poor and Bad) for active |

| | |
|---|---|
| **VPN** | VPN. |
| **VoIP** | Every NATed VoIP call is monitored with MOS (routed calls or VoIP via VPN are not counted at the moment).<br>VigorACS only captures the signals from the SD-WAN CPE with VoIP feature. |
| **More** | Click to access into the **Monitoring>>WAN**, **VPN**, or **VoIP** web page for get more detailed information. |

## 4.3 Statistics for SD-WAN Network Group

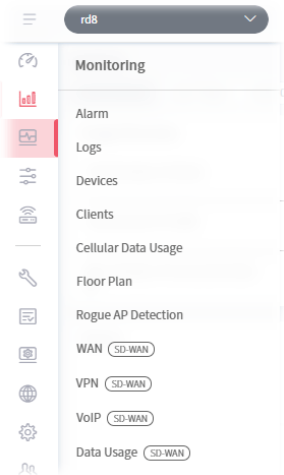
The page offers statistics for all the devices listed under root networks, including usage overview, wireless clients Overview, data traffic, device ranking, and client ranking. By clicking Last 24 Hours, Last 7 Days, Last 30 Days or Custom setting (define the period), the administrator can obtain various statistics within the time period.




In addition, the statistics can be exported as ".XLS" file if you click the **Export** button on the top side.

## 4.4 Monitoring for SD-WAN Network Group

Monitoring menu offers options for monitoring the normal and abnormal actions for network group and CPE. Here, we choose RD8 as an example.

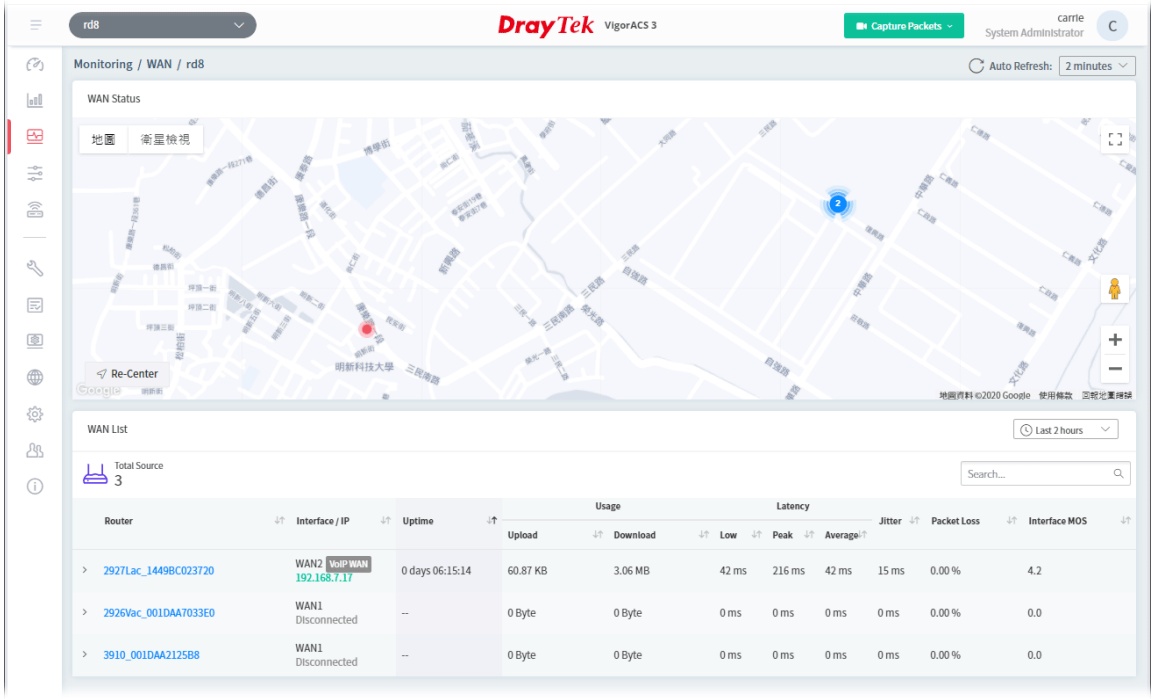



In which, the usage and settings for Alarm, Logs, Devices, Clients, Cellular Data Usage, Floor Plan and Rogue AP Detection are totally the same as the network group without SD-WAN enabled. For detailed information, refer to **Chapter 8 Network Group Menu**.

This section will describe configuration pages for WAN (SD-WAN), VPN (SD_WAN), VoIP (SD-WAN) and Data Usage (SD-WAN).

### 4.4.1 WAN (SD-WAN)

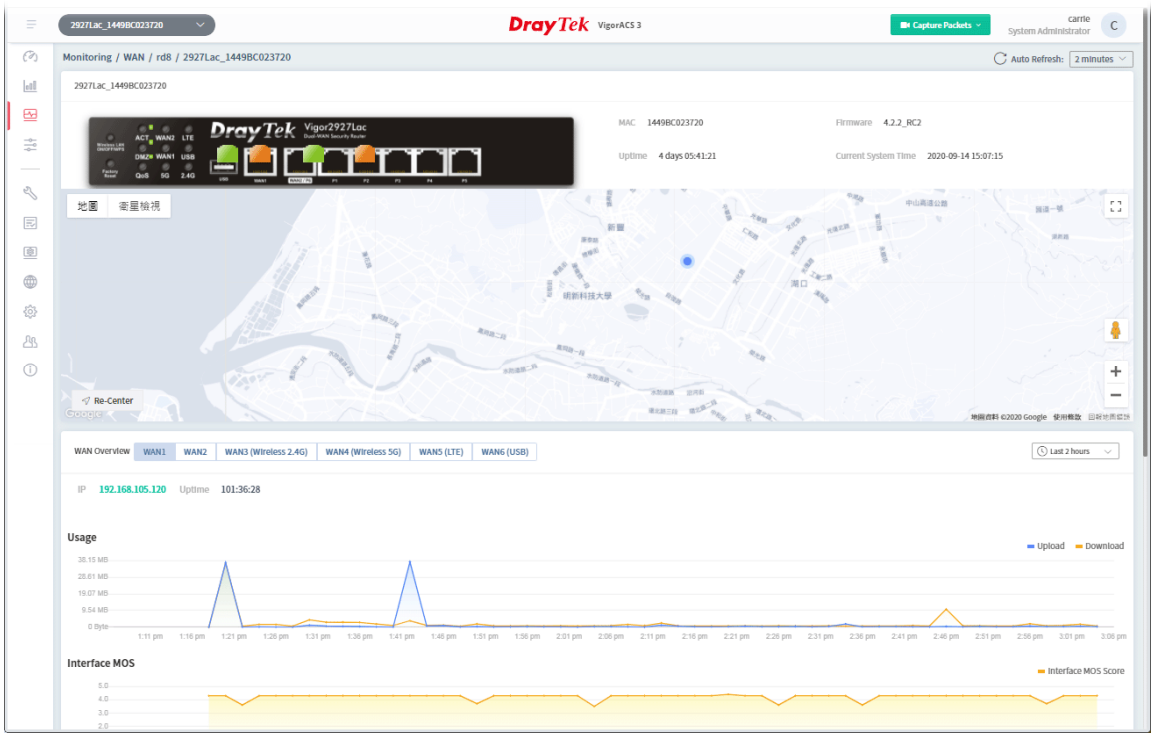
This page displays the location, name, interface/IP, uptime, usage, latency, jitter, packet loss and interface MOS of the routers within the group.




These parameters are explained as follows:

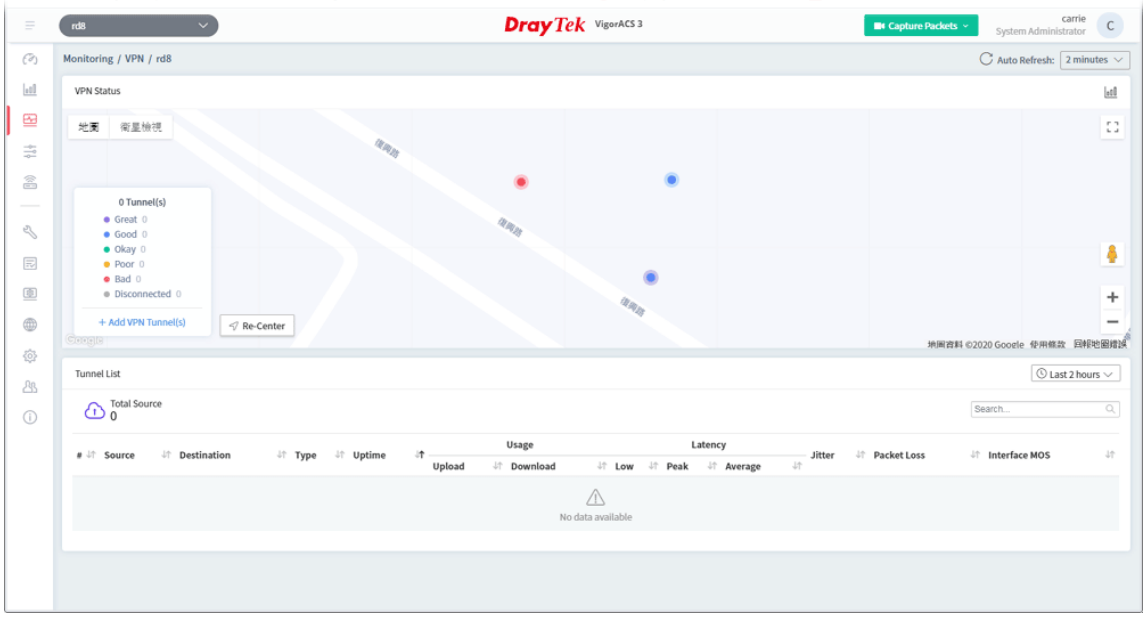
| Item | Description |
|---|---|
| **WAN Status** | Displays the location of the network group. |
| **WAN List** | Displays the total number of CPEs within the selected group. |

Click the name link of the router to get the following page.



### 4.4.2 VPN (SD-WAN)

The monitoring page will vary based on VPN established or not. Before establishing VPN, the page will be shown as follows:



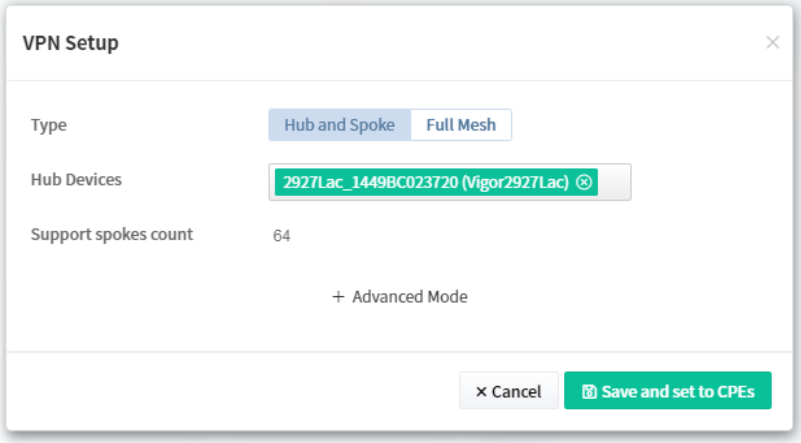

#### 4.4.2.1 AutoVPN Establishment

As a Hub-and-Spoke network,

- VigorACS will create 1 IPsec tunnel from each spoke to the hub.
- VigorACS can auto create tunnels among the Routers.
- Vigor ACS is capable to design and suggest LAN subnets for all CPEs if meeting subnet conflicts.

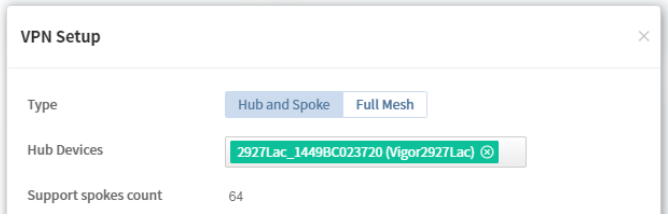
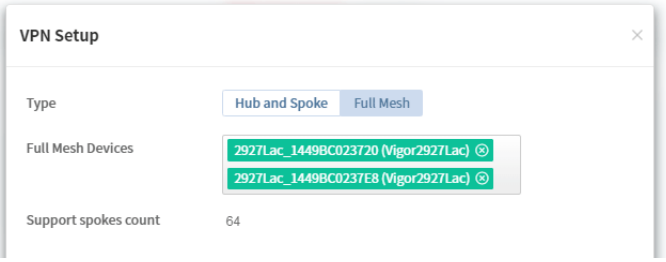
#### 4.4.2.2 Creating VPN with Basic Mode

1. Click **+Add VPN Tunnel**. In default, the settings based on Basic Mode will be shown as follows.

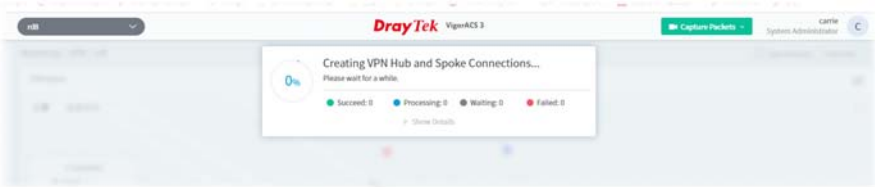



These parameters for Basic Mode are explained as follows:

| Item | Description |
|---|---|
| **Type** | **Hub and Spoke** - Simply select a router as the hub router, the rests would be spokes automatically. |

| | |
|---|---|
| |  <br>**Full Mesh** - It is effective only when there are more than three CPEs on the group.<br>  |
| **Hub Devices / Full Mesh Devices** | Lists the name of the hub device or full mesh device. Select one device as the hub device. |
| **Support spokes count** | Displays the total number of devices, excluding the main device. |
| **+Advanced Mode** | Click to open the configuration page with more options. |
| **Save and Set to CPEs** | Save the above configuration and set to CPE devices. |

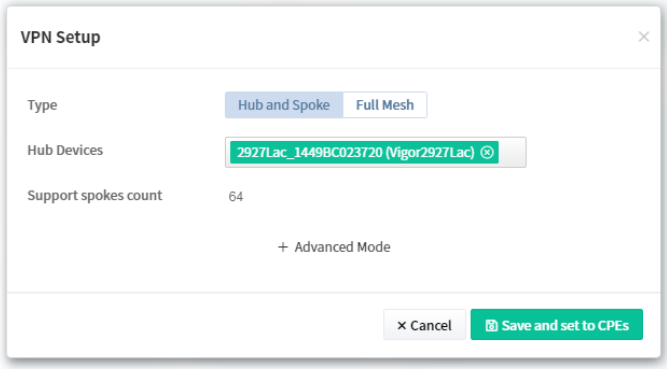
2. Click **Save and set to CPEs**.



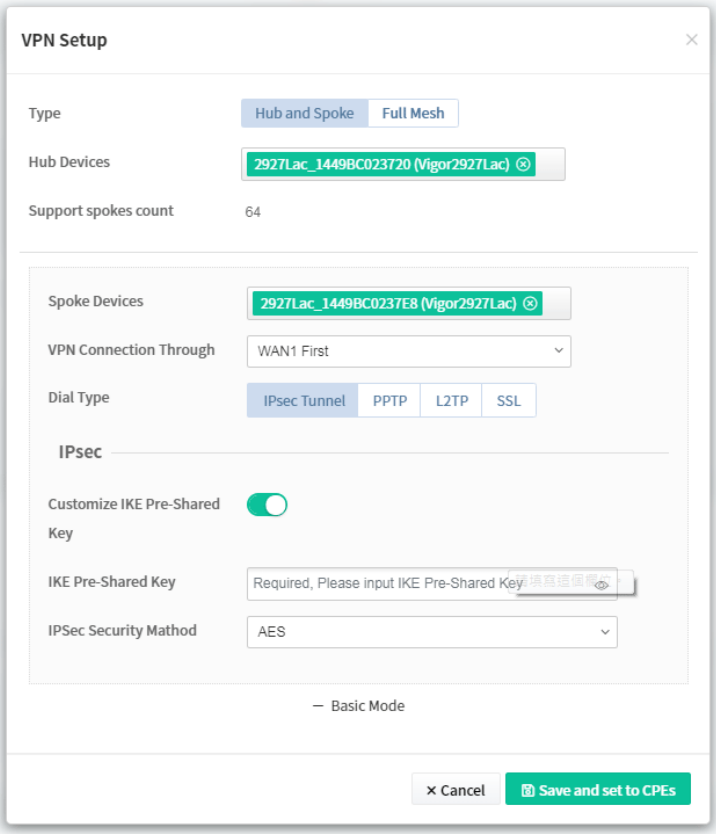

3. The VPN tunnel has been set successfully.

### 4.4.2.3 Creating VPN with Advanced Mode

1. Click **+Add VPN Tunnel** to get the following page.

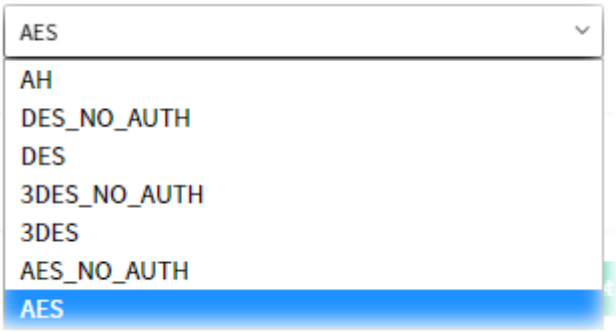
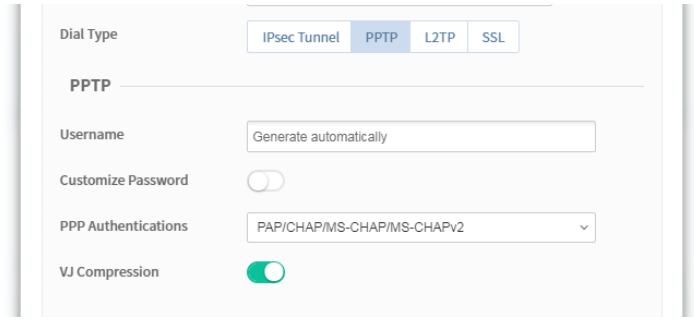


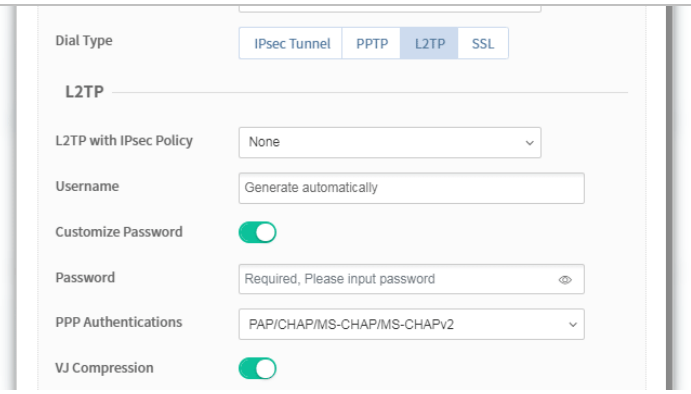
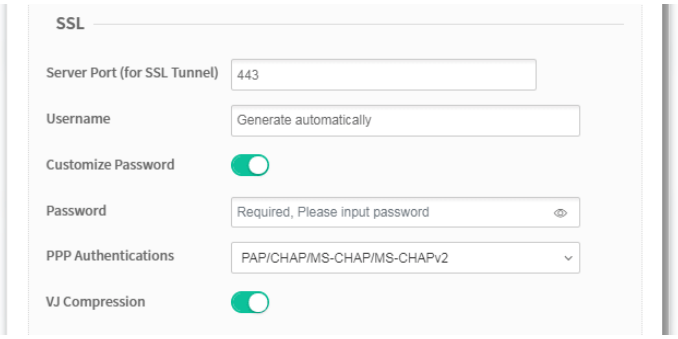

2. Click **+Advanced Mode** to get the following page.



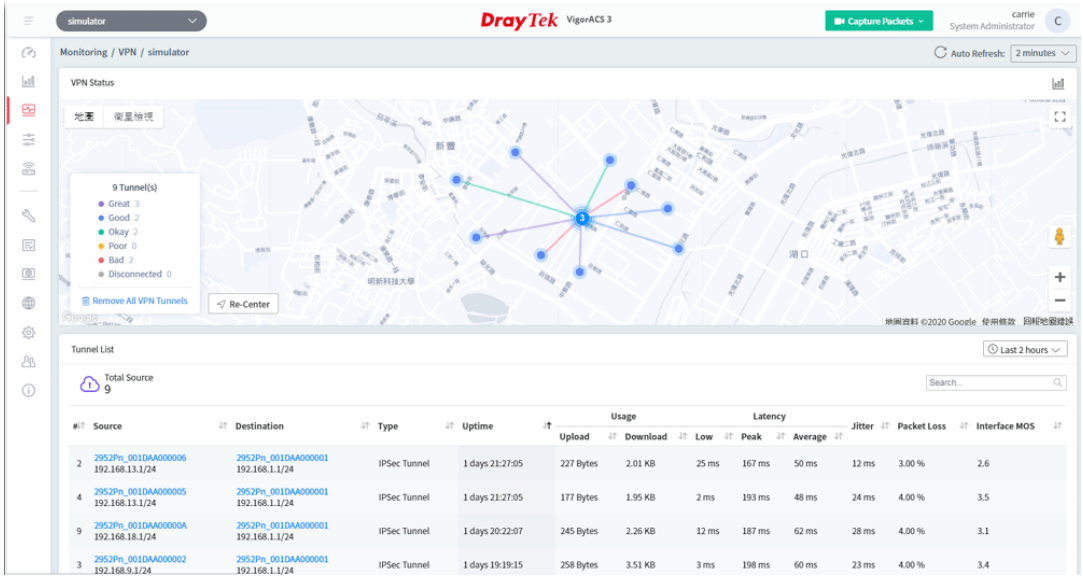

These parameters for Advanced Mode are explained as follows:

| Item | Description |
|---|---|
| **Spoke Devices** | Lists the name of the devices. Select one device as the spoke device. |
| **VPN Connection Through** | Select a WAN interface.<br>**WANx First** - While connecting, the router will use WANx or LTE as the first channel for VPN connection. If WANx or LTE fails, the router will use another WAN interface instead.<br>**WANx Only** - While connecting, the router will use WANx or LTE as the first channel for VPN connection. If WANx or LTE fails, the connection will be off. |
| **Dial Type** | Select one of the tunnels for this VPN profile.<br>● IPsec Tunnel<br>● PPTP<br>● L2TP<br>● SSL |
| **IPsec -** IPsec Tunnel is selected as Dial Type | |
| **IPsec** | **Customize IKE Pre-Shared Key** - Click to enable or disable the IKE PSK setting.<br>**IKE Pre-Shared Key -** Enter a string as PSK.<br>**IPsec Security Method** - Authentication Header (AH) means data will be authenticated, but not be encrypted. The Encapsulating Security Payload (ESP) protocol can be used to provide authentication and encryption to IPsec traffic. Three encryption standards are supported for ESP: DES, 3DES and AES, in ascending order of security. DES_NO_AUTH, 3DES_NO_AUTH and AES_NO_AUTH means the packets will be encrypted |

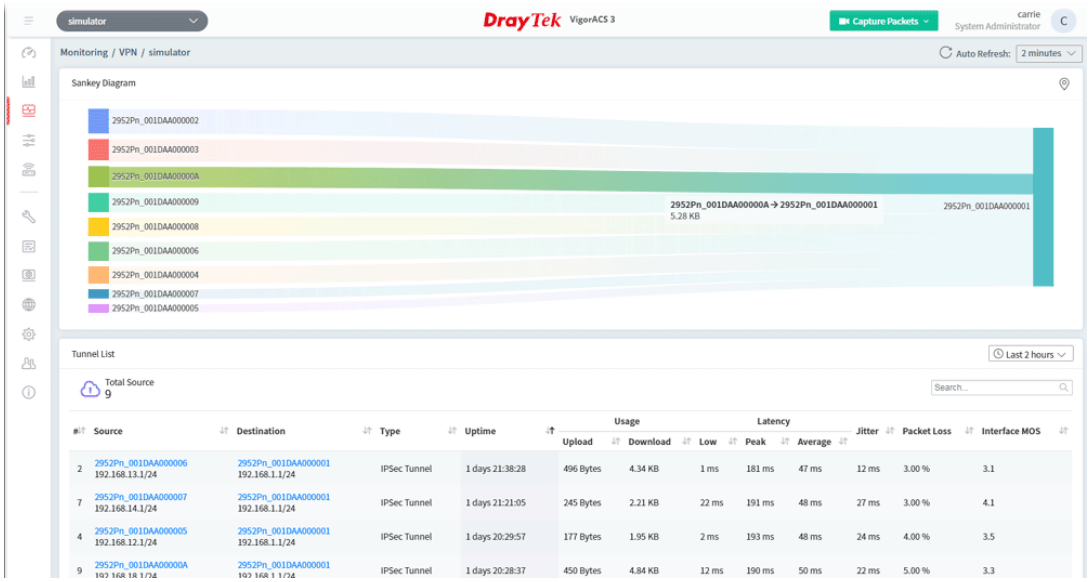
| | |
|---|---|
| | with no authentication.<br>  |
| **PPTP -** PPTP is selected as Dial Type | |
| **PPTP** | **Username -** Enter a username for establishing VPN connection.<br>**Customize Password -** Click to enable the password configuration.<br>● **Password -** Enter a username for establishing VPN connection.<br>**PPP Authentications -** Authenticate dial-in users using the PAP protocol only or PAP/CHAP/MS-CHAP/MS-CHAPv2.<br>**VJ Compression -** Click to enable Van Jacobson (VJ) header compression to improve throughput on slow connections.<br>  |
| **L2TP -** L2TP is selected as Dial Type | |
| **L2TP** | **L2TP with IPsec Policy -** Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPsec. Select from below:<br>● **None -** Do not apply the IPsec policy. Accordingly, the VPN connection employed the L2TP without IPsec policy can be viewed as one pure L2TP connection.<br>● **Nice to Have** - Apply the IPsec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection.<br>● **Must -** Specify the IPsec policy to be definitely applied on the L2TP connection.<br>**Username -** Enter a username for establishing VPN connection.<br>**Customize Password -** Click to enable the password configuration.<br>● **Password -** Enter a username for establishing VPN connection.<br>**PPP Authentications -** Authenticate dial-in users using the PAP protocol only or PAP/CHAP/MS-CHAP/MS-CHAPv2.<br>**VJ Compression -** Click to enable Van Jacobson (VJ) header compression to improve throughput on slow connections. |

| | |
|---|---|
| |  |
| **SSL** | **Server Port (for SSL Tunnel) -** Enter a port number for SSL Tunnel. The default is 443.<br>**Username -** Enter a username for establishing VPN connection.<br>**Customize Password -** Click to enable the password configuration.<br>● **Password -** Enter a username for establishing VPN connection.<br>**PPP Authentications -** Authenticate dial-in users using the PAP protocol only or PAP/CHAP/MS-CHAP/MS-CHAPv2.<br>**VJ Compression -** Click to enable Van Jacobson (VJ) header compression to improve throughput on slow connections.<br>  |
| **-Basic Mode** | Click to return to configuration page with less options. |
| **Save and Set to CPEs** | Save the above configuration and set to CPE devices. |

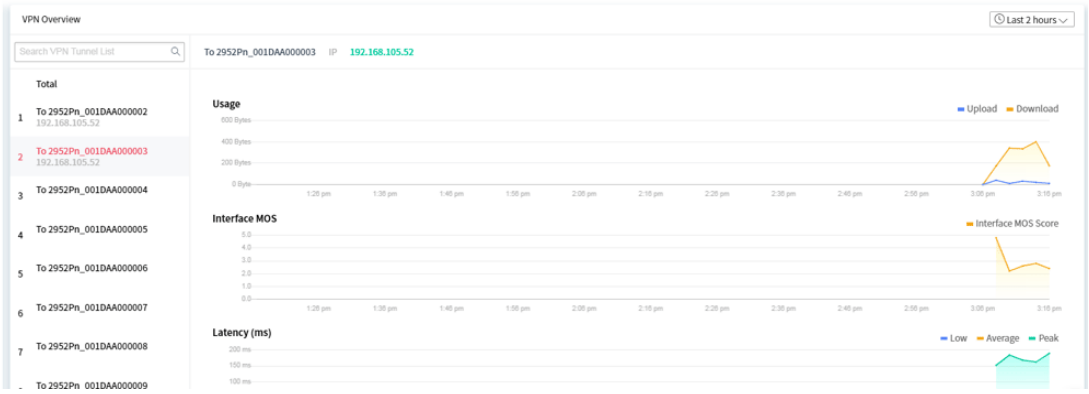
3. After finished and save the above settings, the VPN tunnel has been set successfully.

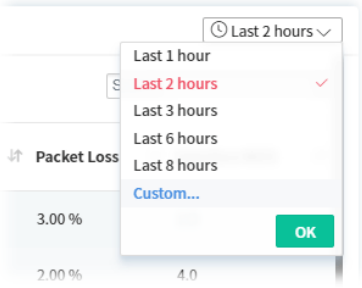



To have a sankey diagram, please click the right-top icon to display the following page.



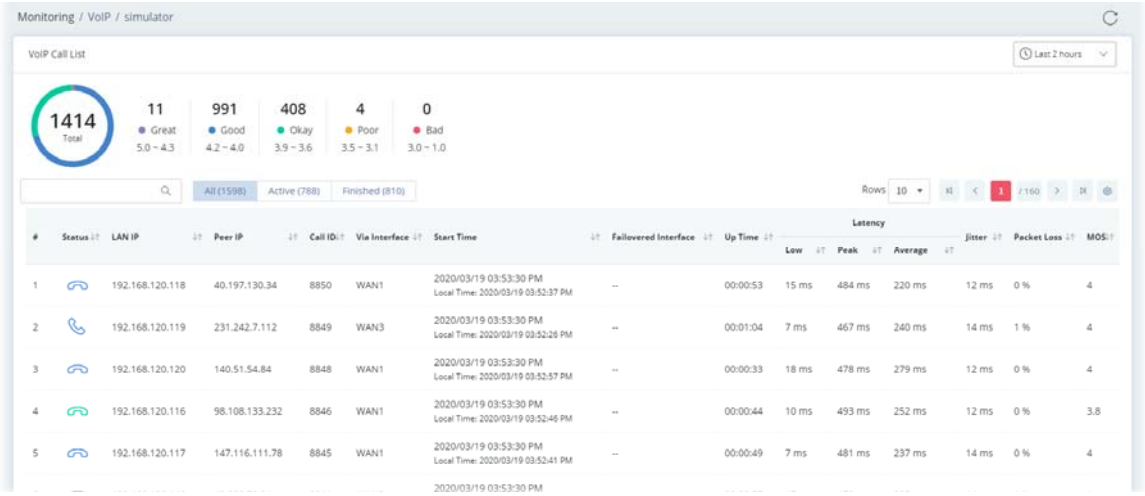

From the **Tunnel List**, click any CPE link to display the detailed information (e.g., Usage, Interface MOS, Latency and etc.) of the CPE. Here we take Vigor2952Pn as an example.






### 4.4.3 VoIP (SD-WAN)

VoIP call list displays the communication status related to incoming and outgoing calls via VoIP WAN.

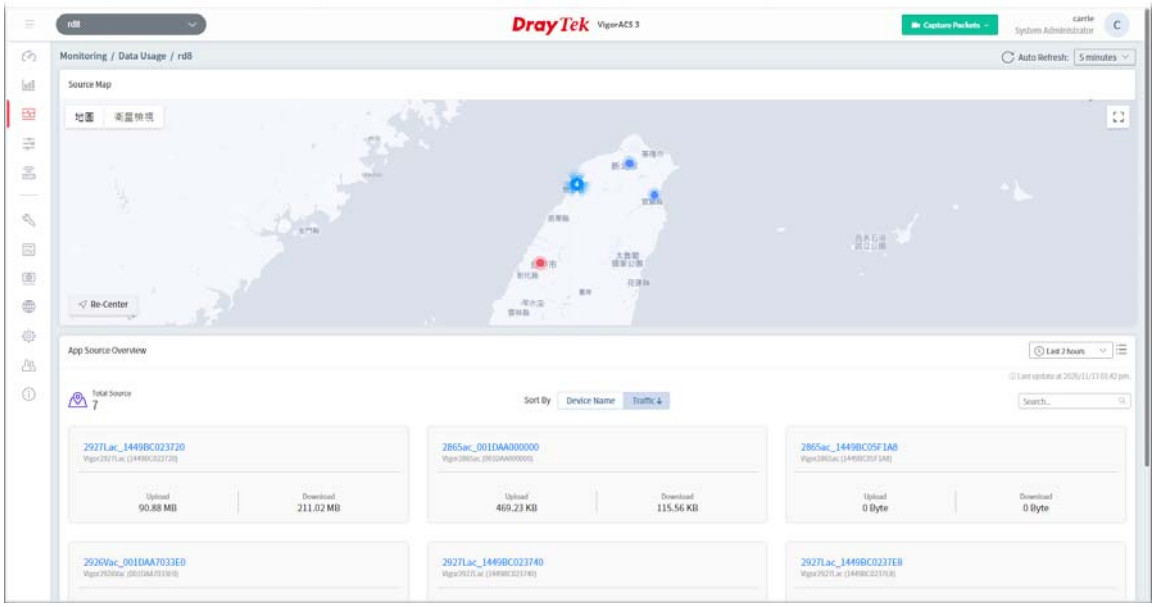



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Great, Good, Okay, Poor, Bad** | All the VoIP calls will be separated with different levels according to its quality. |
| | Enter the IP address (LAN IP/ Peer IP) as a condition to search the VoIP call. |
| **Status** | Displays the status of the phone call.<br>- Active call. Quality level is Good.<br>- Finished call. Quality level is Good.<br>- Finished call. Quality level is Okay. |
| **LAN IP** | Displays the IP address of the local side. |
| **Peer IP** | Displays the IP address of the peer side. |
| **Call ID** | Displays the ID number of the caller. |
| **Via Interface** | Displays the interface that VoIP call passing through. |
| **Start Time** | Displays the start time of the VoIP call. |
| **Failovered Interface** | Displays the failover interface for VoIP calls passing through. |
| **Up Time** | Displays the time length of the VoIP call. |
| **Latency** | Displays the transmission latency data (low, peak and average values) of |

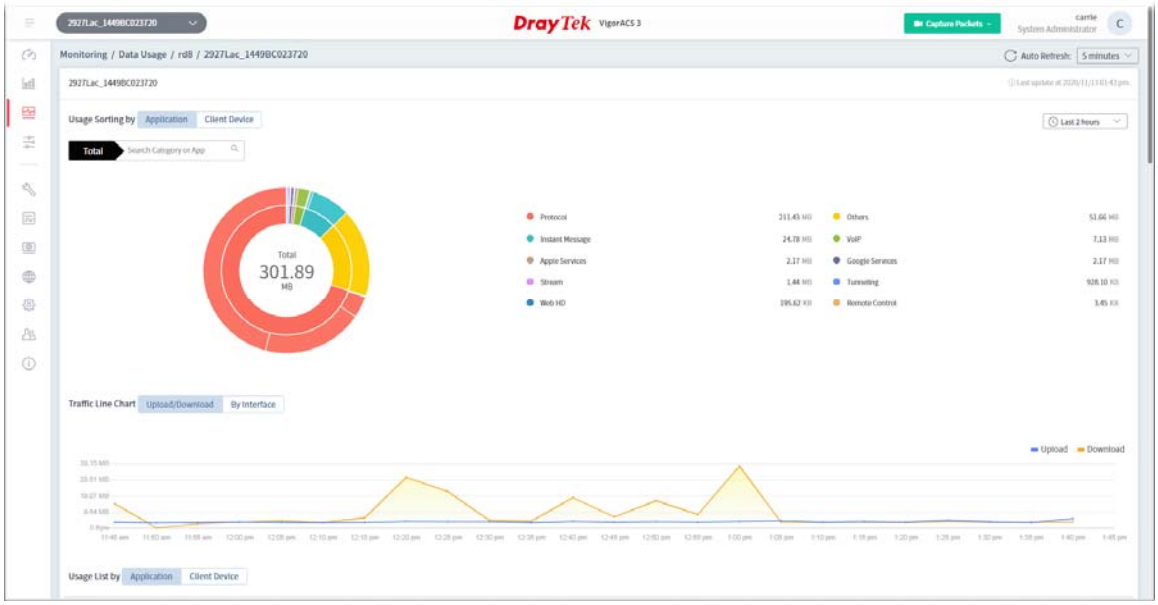
| | |
|---|---|
| | the VoIP call. |
| **Jitter** | Displays the packet jitter value of the VoIP call. |
| **Packet Loss** | Displays the packet loss of the VoIP call. |
| **MOS** | Displays the mean opinion score of the VoIP call. 1 means the worst; 5 means the best. |

### 4.4.4 Data Usage (SD-WAN)



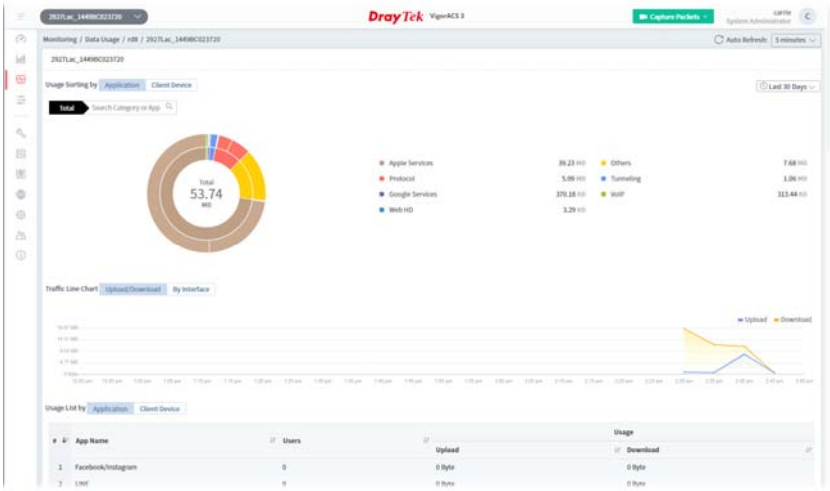
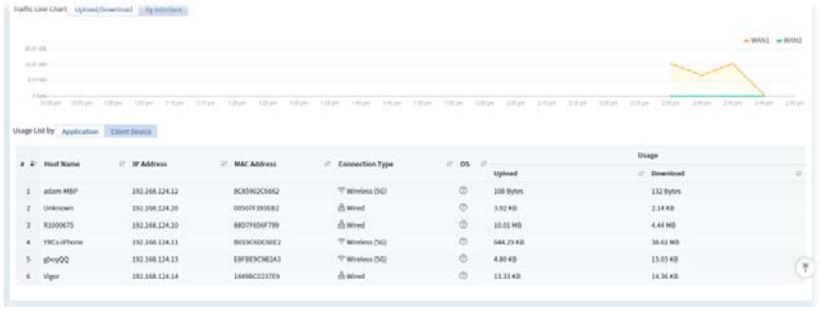

#### 4.4.4.1 Data Usage of Selected CPE

Click a device link (e.g., Vigor2927Lac in this case) under **App Source Overview**.




These parameters are explained as follows:

| Item | Description |
|---|---|
| **Usage Sorting by** | Displays a pie chart related to various application usage. |

| | |
|---|---|
| | **Application** - Click to display a pie chart for various application usage.<br>**Client Device** - Click to display a pie chart for the selected CPE. |
| **Traffic Line Chart** | Displays a line chart related to data upload/download, or traffic via the WAN interface.<br>**Upload/Download** - Click to display data upload/download.<br>**By Interface** - Click to display a line chart related to traffic via the WAN interface. |
| **Usage List by** | Displays the data usage for common Apps or for connected client.<br>**Application** - Click to display the data information related to various applications, including name of application, number of users, upload and download usage.<br>  <br>**Client Device** - Click to display data information for the selected CPE, including host name, IP address, MAC address, connection type, operation system, upload and download usage.<br>  |

# Chapter 5 SD-WAN CPE

The menu items related to a CPE:

Dashboard

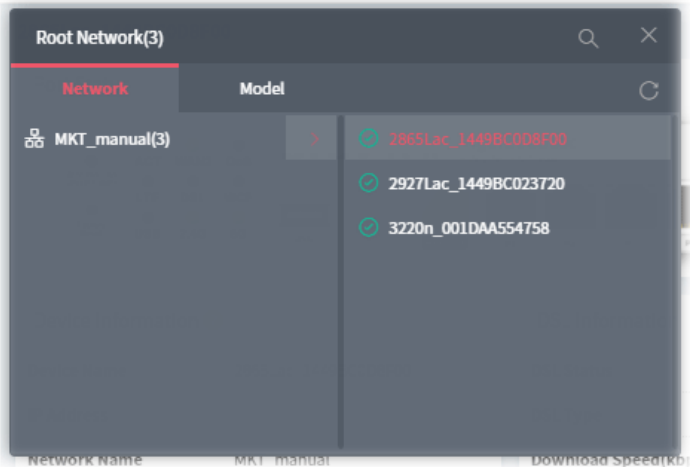
Statistics

Monitoring

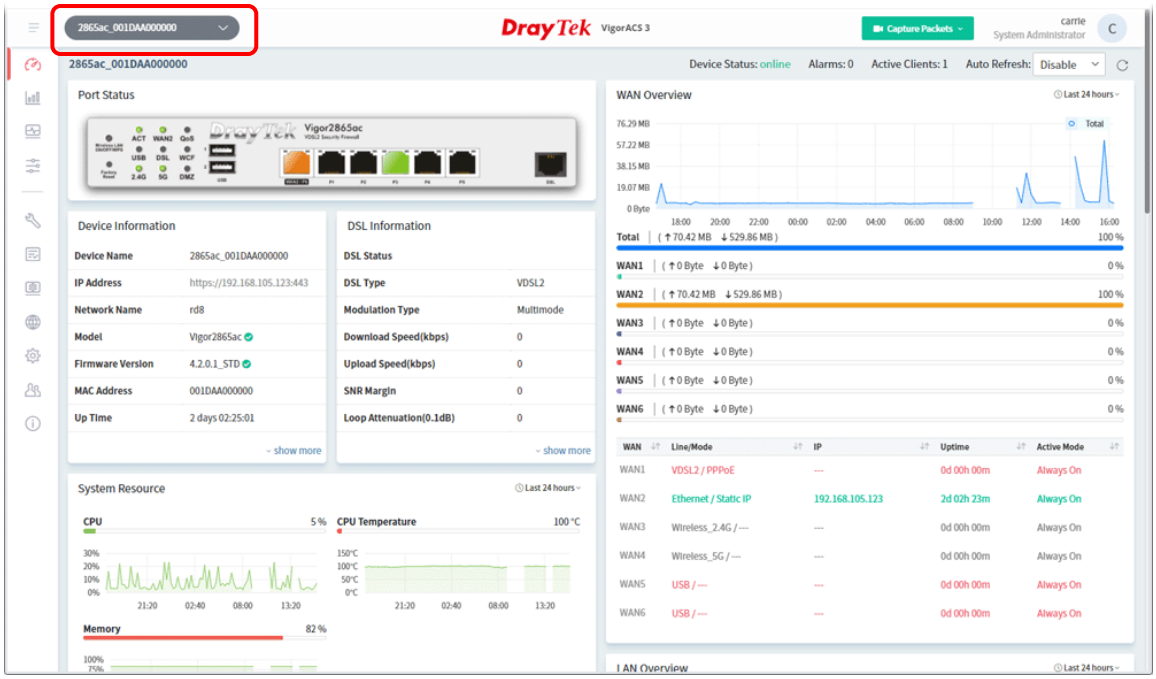
Configuration

## 5.1 Dashboard for SD-WAN CPE

To display the SD-WAN CPE dashboard, find the one (a CPE with SD-WAN feature) you want from the list under the Model tab.

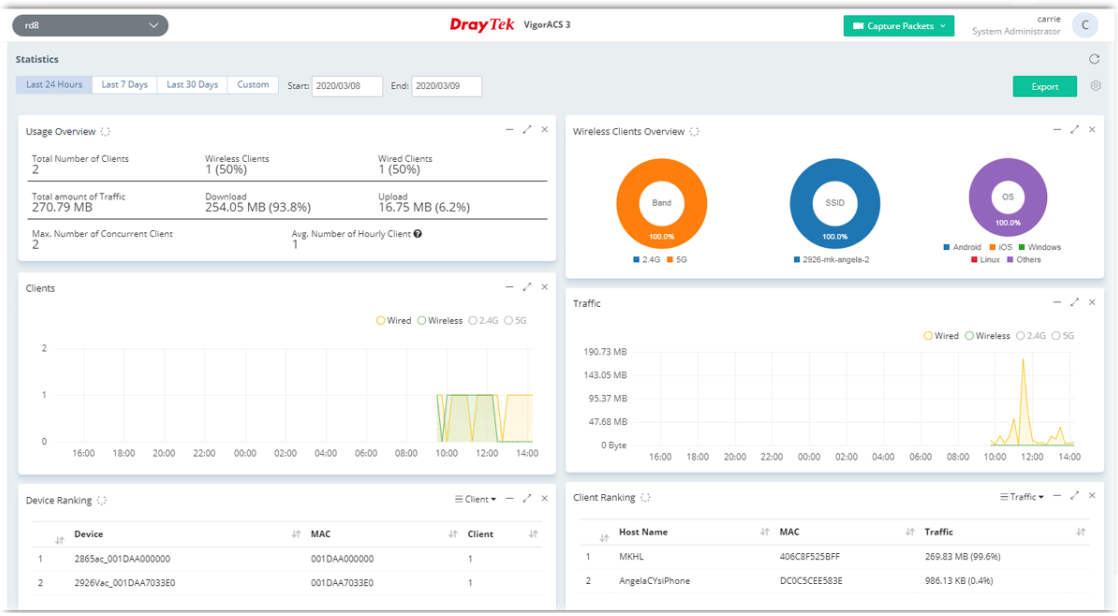


In this case, we choose Vigor2865 series (e.g., Vigor2865ac) as an example.



## 5.2 Statistics for SD-WAN CPE

The page offers statistics for all the devices listed under root networks, including usage overview, wireless clients Overview, data traffic, device ranking, and client ranking. By clicking Last 24 Hours, Last 7 Days, Last 30 Days or Custom setting (define the period), the administrator can obtain various statistics within the time period.

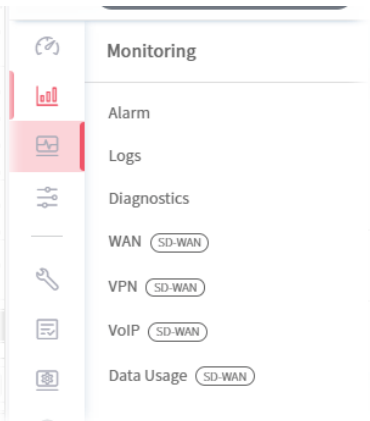



In addition, the statistics can be exported as ".XLS" file if you click the **Export** button on the top side.

## 5.3 Monitoring for SD-WAN CPE

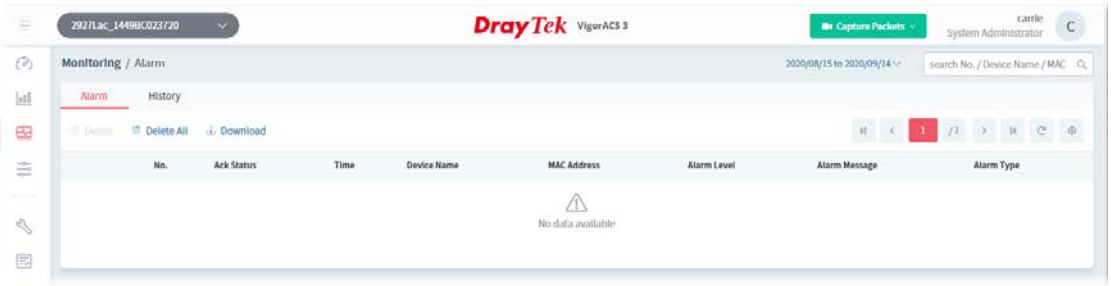
Monitoring menu offers options for monitoring the normal and abnormal actions for network, group and CPE. This section offers Monitoring menu items for a selected SD-WAN CPE.

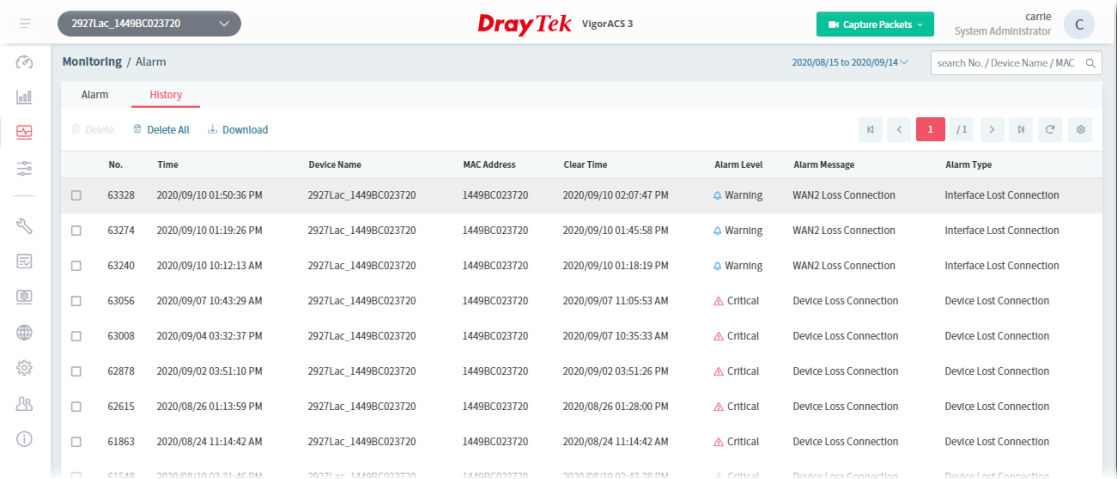
In this section, we choose Vigor2927Lac / Vigor2865ac series as an example.



### 5.3.1 Alarm

Alarm message will be recorded on VigorACS 3 server when there is a trouble happened to the selected device (CPE).



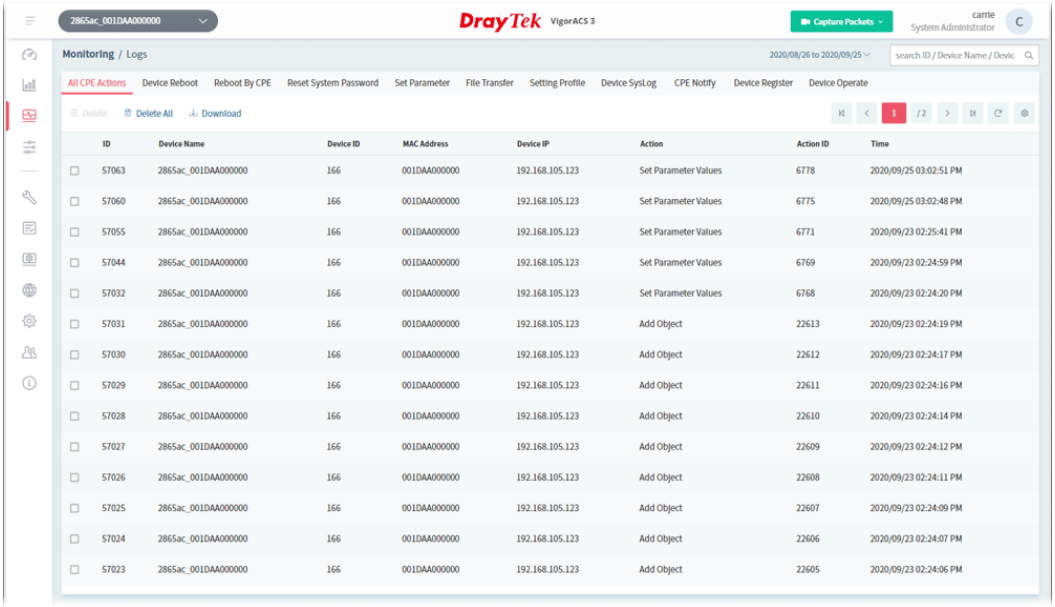

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Alarm / History** | **Alarm –** Displays the alarm records recently.<br>**History –** Displays all the alarm records that have been solved and cleared. |
| **Delete** | Clear the alarm record which has been solved by VigorACS 3. |
| **Delete All** | Clear all of the alarm records which have been solved by VigorACS 3. |
| **Download** | Click to save alarm log as a XLS file. |
| **No.** | Display the index number of the alarm. It is offered by VigorACS 3 automatically. |
| **Ack Status** | Display the status of the records with the type specified here (Not Ack or Acked). |
| **Time** | Displays the time of the device to be monitored. |
| **Device Name** | Displays the name of the monitored device. |
| **MAC Address** | Displays the MAC address of the monitored device. |
| **Alarm Level** | Displays the alarm message with the severity (e.g., Critical) specified. |
| **Alarm Message** | Displays a brief explanation for the alarm sent by VigorACS 3 automatically. |
| **Alarm Type** | Displays the alarm message with the type specified. |

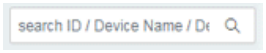
### 5.3.2 Logs

Log provides administrator records for all CPE Actions, Device Reboot, Reboot by CPE, Reset System Password, Set Parameter, File Transfer, Setting Profile, Device SysLog, CPE Notify, Device Register and Device Operate. Click each tab to get more detailed information.

The following page shows the log for all CPE actions executed, device name, MAC address, Device IP, and Current Time for CPE device managed and monitored by VigorACS.



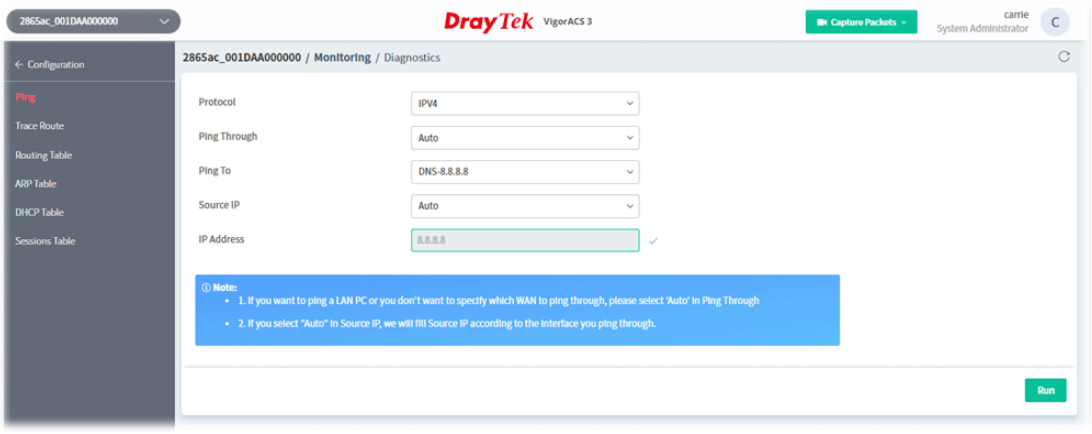

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Log Type** | Click one of the tabs (e.g., All CPE Actions, Device Reboot, Reboot By CPE, Reset System Password, Set Parameter, File Transfer, Setting Profile, Device SysLog, CPE Notify, Device Register, Device Operate and etc.) to display related log on this page. |
|  | Enter the condition for VigorACS to search and display relational information. |
| **Delete** | Clear the alarm record which has been solved by VigorACS. |
| **Delete All** | Clear all of the alarm records which have been solved by VigorACS. |
| **Download** | Click this button to save log as a XLS file. |

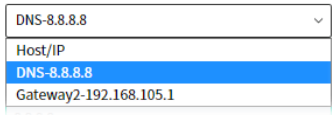
### 5.3.3 Diagnostics

The menu items for Diagnostics will vary based on the CPE model. In this case, we take Vigor2865 series as an example.

#### 5.3.3.1 Ping

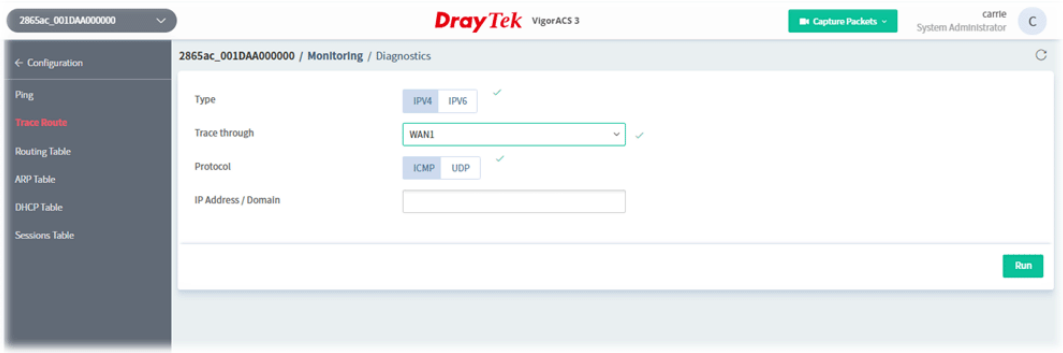



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Protocol** | Select the protocol (IPv4 or IPv6) to perform the ping operation. |
| **Ping Though** | Select a WAN interface 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** | Select the type of target (Host/IP, DNS, Gateway) to which you wish to ping.<br>  |
| **Source IP** | Select a WAN IP as the source IP.<br>If Auto is selected, the source IP will be specified according to the interface chosen for ping through. |
| **IP Address** | Enter the IP address of the Host/IP that you want to ping. |
| **Run** | Click to perform the job. |

#### 5.3.3.2 Trace Route

This page allows you to trace the routes from router to the host. Simply Enter the IP address of the host in the box and click **Run**. The result of route trace will be shown on the screen.

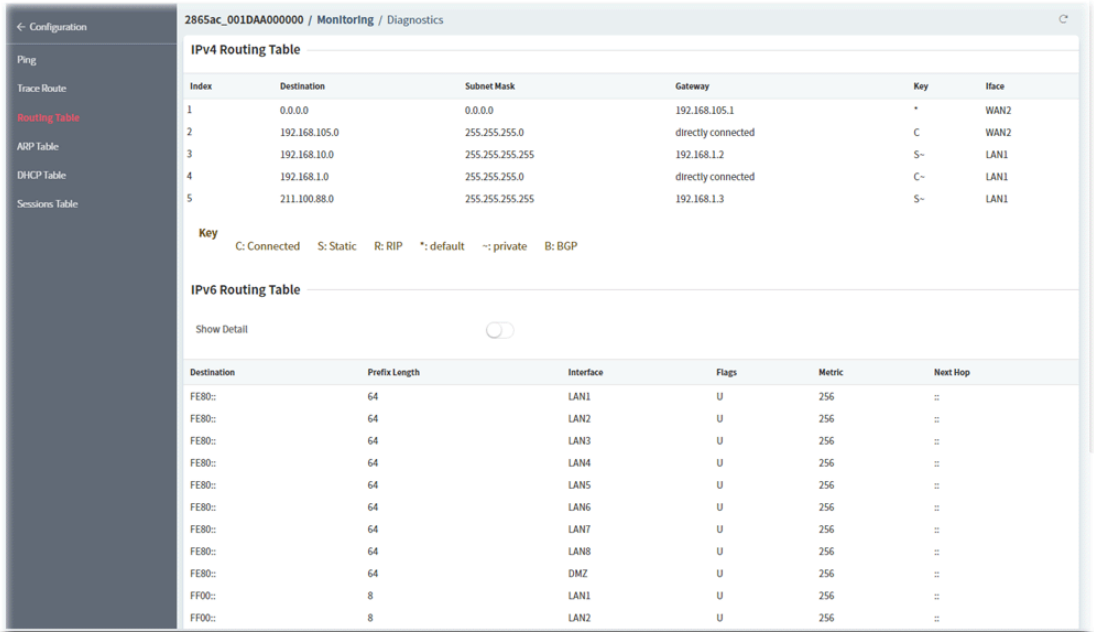



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Type** | Select the IP version (IPv4/IPv6) used to perform the trace route. |
| **Trace through** | Select the WAN interface used to perform the trace route. |
| **Protocol** | Select either UDP or ICMP used to perform the trace route. |
| **IP Address / Domain** | Enter the hostname or the IP address of trace route destination. |
| **Run** | Click to perform the job. |

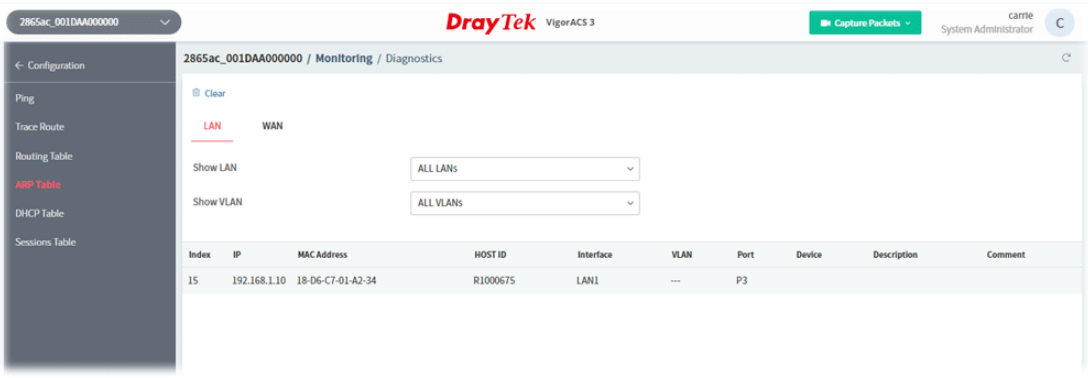
### 5.3.3.3 Routing Table

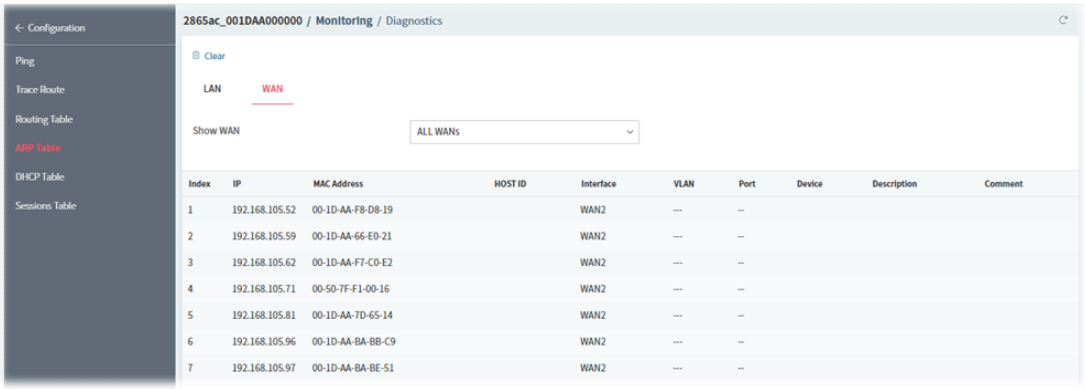
This page displays the IPv4/IPv6 routing information.



### 5.3.3.4 ARP Table

This page displays the contents of the ARP (Address Resolution Protocol) cache held in the router. The table shows the mappings between Ethernet hardware addresses (MAC Addresses) and IP addresses.



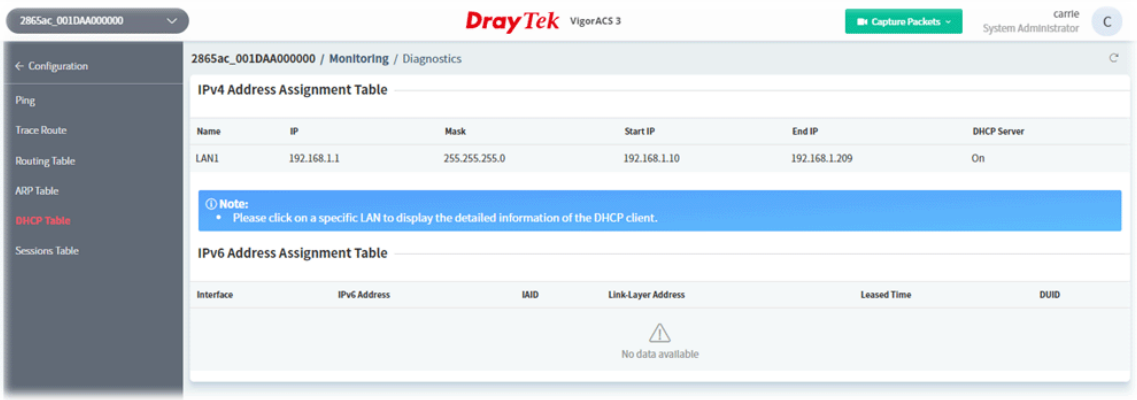




These parameters are explained as follows:

| Item | Description |
|---|---|
| **Show LAN / VLAN / WAN** | Select the LAN(s), VLAN(s) and WAN(s) to display ARP table information.<br>By default, information on all LANs, VLANs and WANs is displayed. |

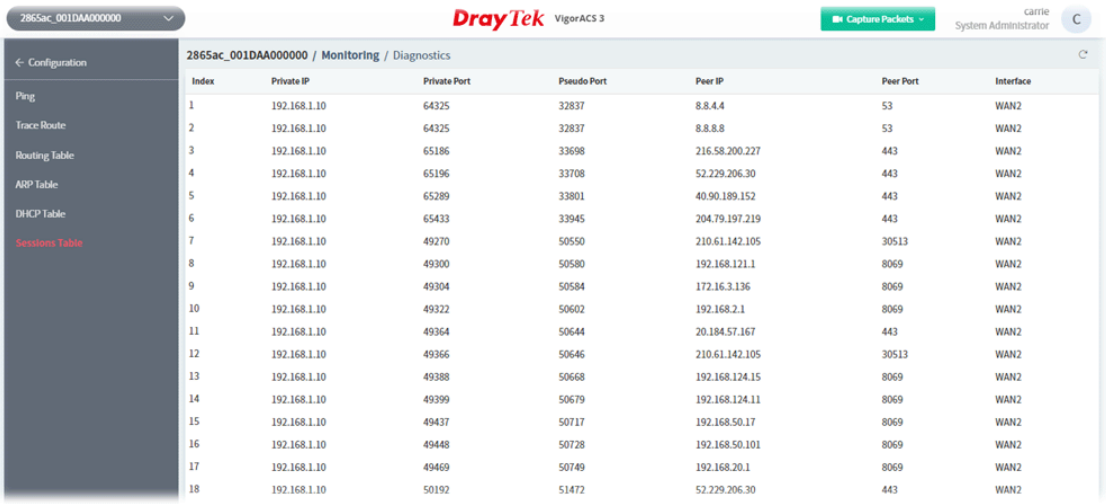
### 5.3.3.5 DHCP Table

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



### 5.3.3.6 Sessions Table

This screen shows the 128 newest entries in the NAT sessions table.

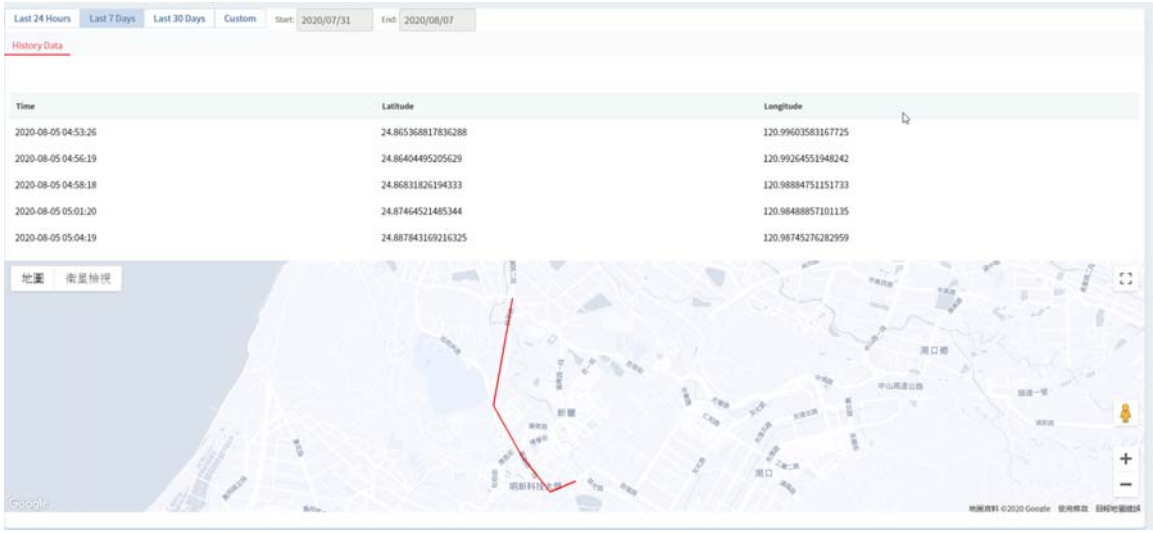



| Index | Private IP | Private Port | Pseudo Port | Peer IP | Peer Port | Interface |
|---|---|---|---|---|---|---|
| 1 | 192.168.1.10 | 64325 | 32837 | 8.8.4.4 | 53 | WAN2 |
| 2 | 192.168.1.10 | 64325 | 32837 | 8.8.8.8 | 53 | WAN2 |
| 3 | 192.168.1.10 | 65186 | 33698 | 216.58.200.227 | 443 | WAN2 |
| 4 | 192.168.1.10 | 65196 | 33708 | 52.229.206.30 | 443 | WAN2 |
| 5 | 192.168.1.10 | 65289 | 33801 | 40.90.189.152 | 443 | WAN2 |
| 6 | 192.168.1.10 | 65433 | 33945 | 204.79.197.219 | 443 | WAN2 |
| 7 | 192.168.1.10 | 49270 | 50550 | 210.61.142.105 | 30513 | WAN2 |
| 8 | 192.168.1.10 | 49300 | 50580 | 192.168.121.1 | 8069 | WAN2 |
| 9 | 192.168.1.10 | 49304 | 50584 | 172.16.3.136 | 8069 | WAN2 |
| 10 | 192.168.1.10 | 49322 | 50602 | 192.168.2.1 | 8069 | WAN2 |
| 11 | 192.168.1.10 | 49364 | 50644 | 20.184.57.167 | 443 | WAN2 |
| 12 | 192.168.1.10 | 49366 | 50646 | 210.61.142.105 | 30513 | WAN2 |
| 13 | 192.168.1.10 | 49388 | 50668 | 192.168.124.15 | 8069 | WAN2 |
| 14 | 192.168.1.10 | 49399 | 50679 | 192.168.124.11 | 8069 | WAN2 |
| 15 | 192.168.1.10 | 49437 | 50717 | 192.168.50.17 | 8069 | WAN2 |
| 16 | 192.168.1.10 | 49448 | 50728 | 192.168.50.101 | 8069 | WAN2 |
| 17 | 192.168.1.10 | 49469 | 50749 | 192.168.20.1 | 8069 | WAN2 |
| 18 | 192.168.1.10 | 50192 | 51472 | 52.229.206.30 | 443 | WAN2 |

### 5.3.4 GPS

It is available when the selected CPE supports SD-WAN feature.

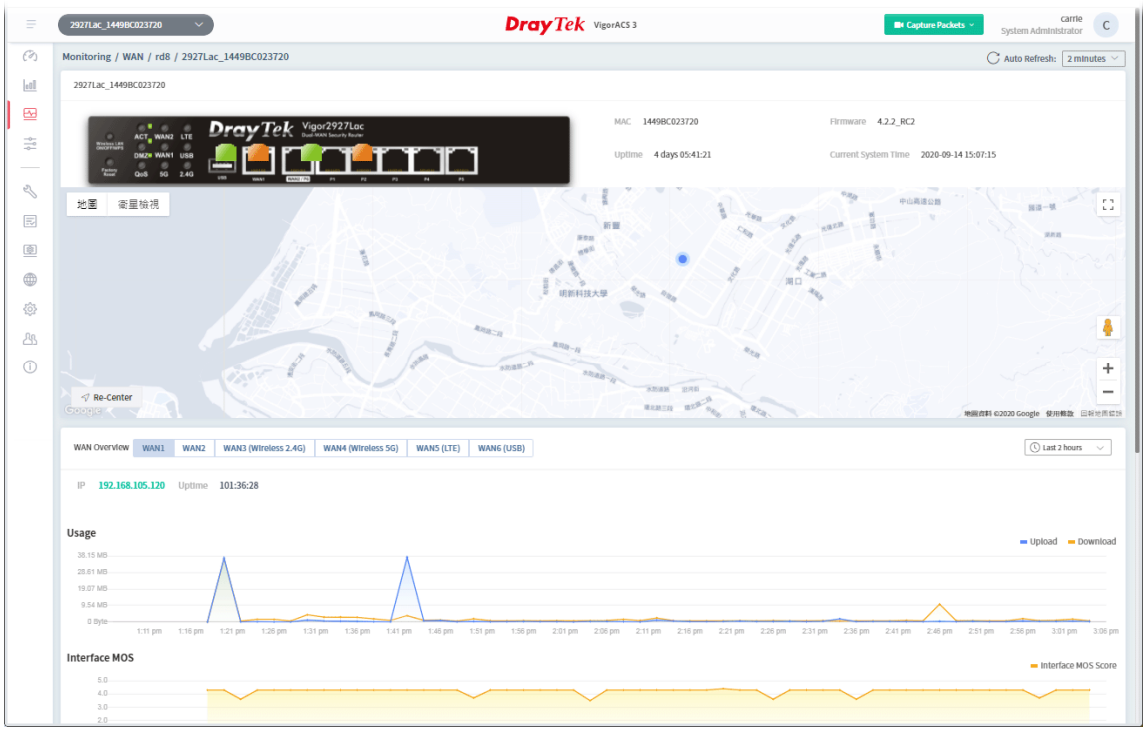
The GPS page will display the moving path (including time and coordinate position, latitude, and longitude) of the Vigor device.




### 5.3.5 WAN (SD-WAN)

It is available when the selected CPE supports SD-WAN feature.

This page displays the location, MAC address, firmware used, uptime of the selected CPE and WAN overview.




These parameters are explained as follows:

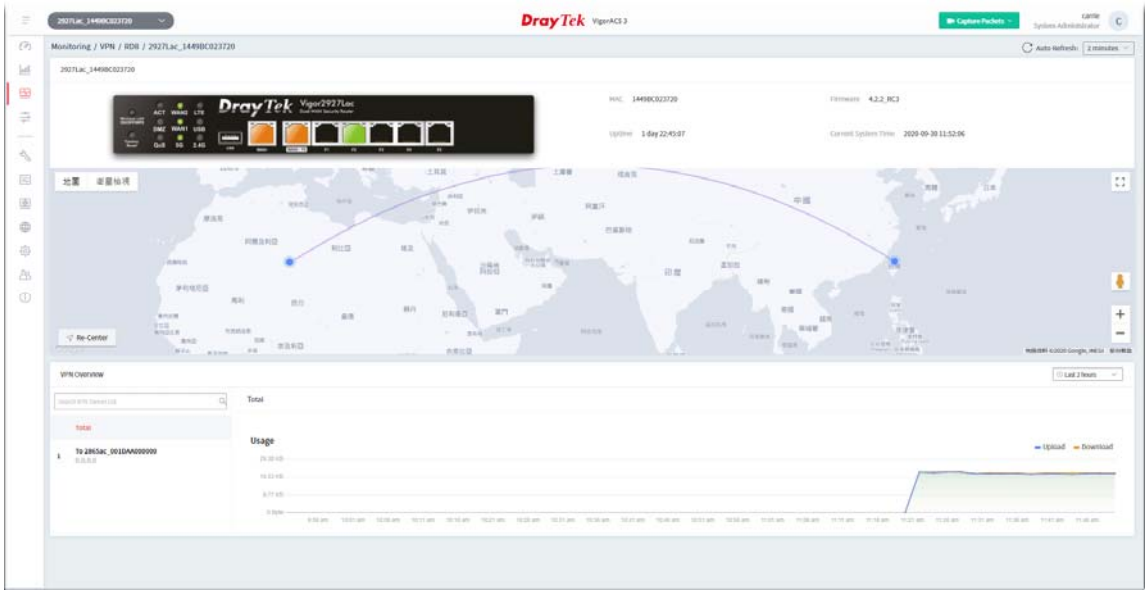
| Item | Description |
|---|---|

| | |
|---|---|
| **Google Map** | Displays the location of the selected CPE. |
| **WAN Overview** | Click the number of the WAN interface to display information related to traffic usage, estimated MOS score, latency, jitter, packet loss and so on. |

### 5.3.6 VPN (SD-WAN)

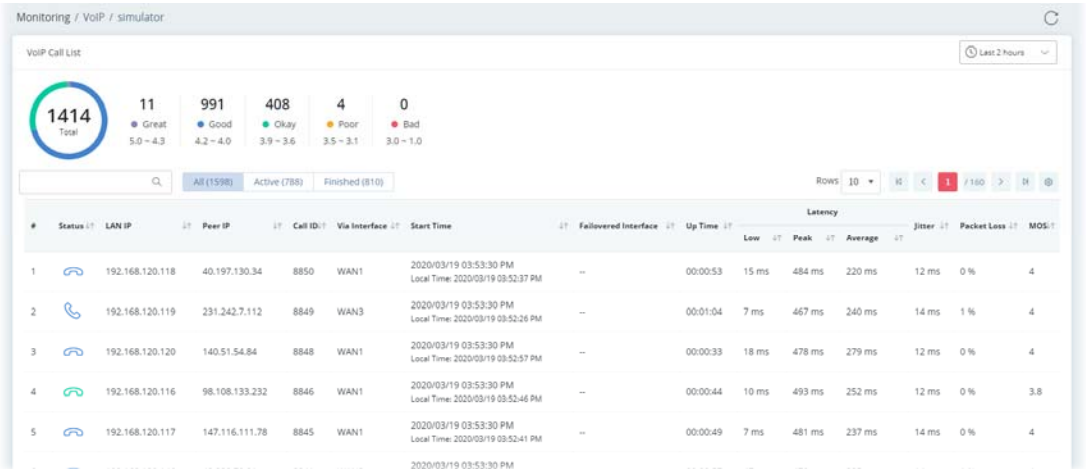
This page displays the location, MAC address, firmware used, uptime of the selected CPE and the traffic for data download/upload by VPN.

The monitoring page will vary based on VPN established or not. Before establishing VPN, the page will be shown as follows:



### 5.3.7 VoIP (SD-WAN)

VoIP call list displays the communication status related to incoming and outgoing calls via VoIP WAN.

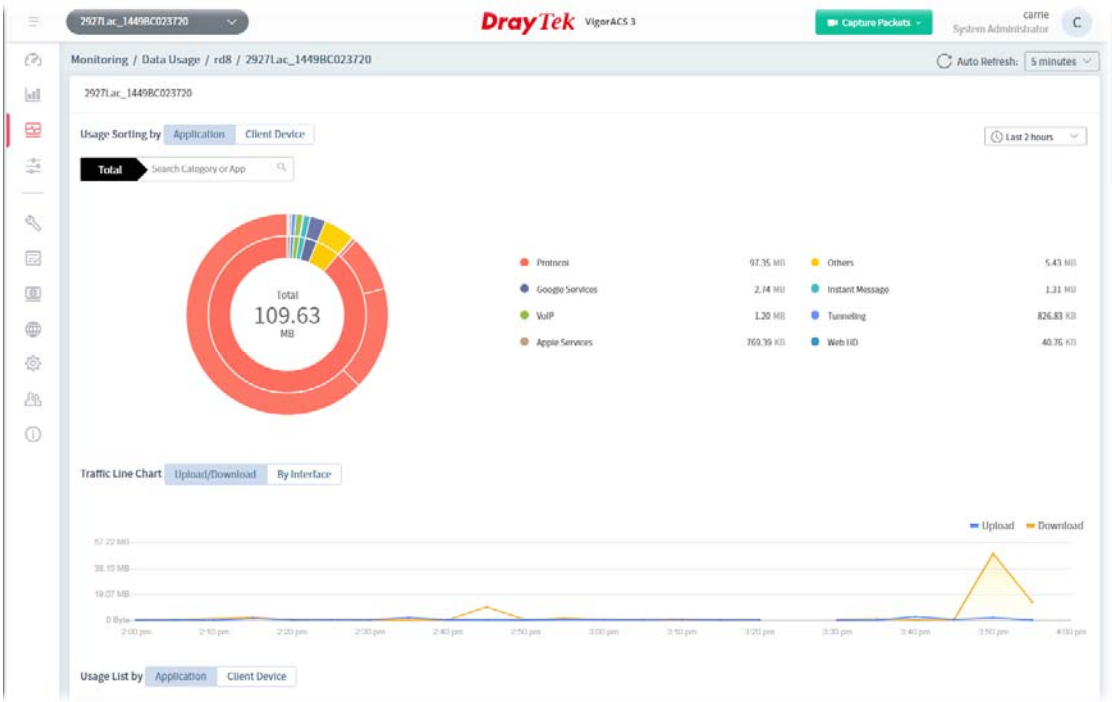



These parameters are explained as follows:

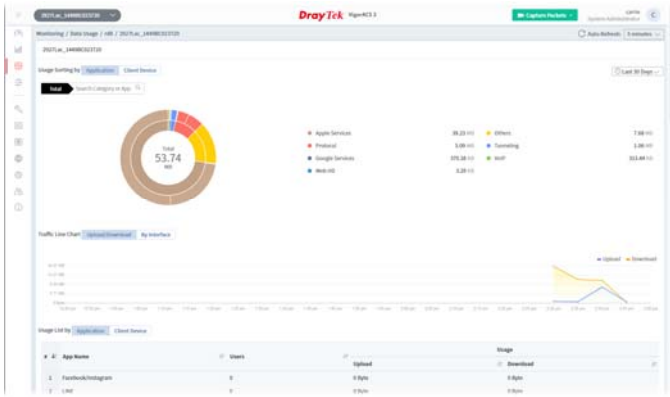
| Item | Description |
|---|---|
| **Great, Good, Okay, Poor, Bad** | All the VoIP calls will be separated with different levels according to its quality. |
| | Enter the IP address (LAN IP/ Peer IP) as a condition to search the VoIP call. |
| **Status** | Displays the status of the phone call.<br> - Active call. Quality level is Good.<br> - Finished call. Quality level is Good.<br> - Finished call. Quality level is Okay. |
| **LAN IP** | Displays the IP address of the local side. |
| **Peer IP** | Displays the IP address of the peer side. |
| **Call ID** | Displays the ID number of the caller. |
| **Via Interface** | Displays the interface that VoIP call passing through. |
| **Start Time** | Displays the start time of the VoIP call. |
| **Failovered Interface** | Displays the failover interface for VoIP calls passing through. |
| **Up Time** | Displays the time length of the VoIP call. |
| **Latency** | Displays the transmission latency data (low, peak and average values) of the VoIP call. |
| **Jitter** | Displays the packet jitter value of the VoIP call. |
| **Packet Loss** | Displays the packet loss of the VoIP call. |
| **MOS** | Displays the mean opinion score of the VoIP call. 1 means the worst; 5 means the best. |

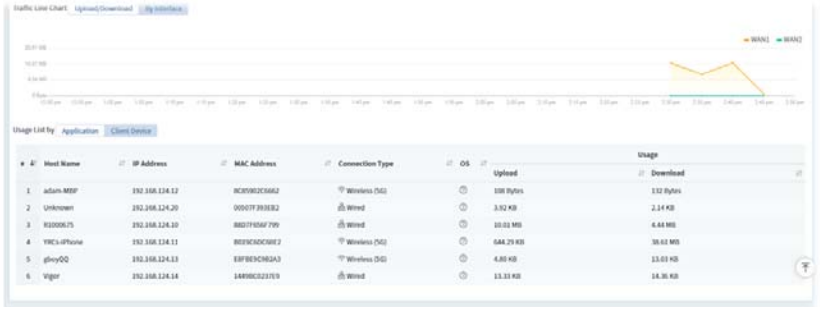
### 5.3.8 Data Usage (SD-WAN)

This page displays the data usage for a SD-WAN CPE.




These parameters are explained as follows:

| Item | Description |
|---|---|
| **Usage Sorting by** | Displays a pie chart related to various application usage.<br>**Application** - Click to display a pie chart for various application usage.<br>**Client Device** - Click to display a pie chart for the selected CPE. |
| **Traffic Line Chart** | Displays a line chart related to data upload/download, or traffic via the WAN interface.<br>**Upload/Download** - Click to display data upload/download.<br>**By Interface** - Click to display a line chart related to traffic via the WAN interface. |
| **Usage List by** | Displays the data usage for common Apps or for connected client.<br>**Application** - Click to display the data information related to various applications, including name of application, number of users, upload and download usage.<br>  <br>**Client Device** - Click to display data information for the selected CPE, |

| | |
|---|---|
| | including host name, IP address, MAC address, connection type, operation system, upload and download usage.<br>  |

## 5.4 Configuration Menu for SD-WAN CPE

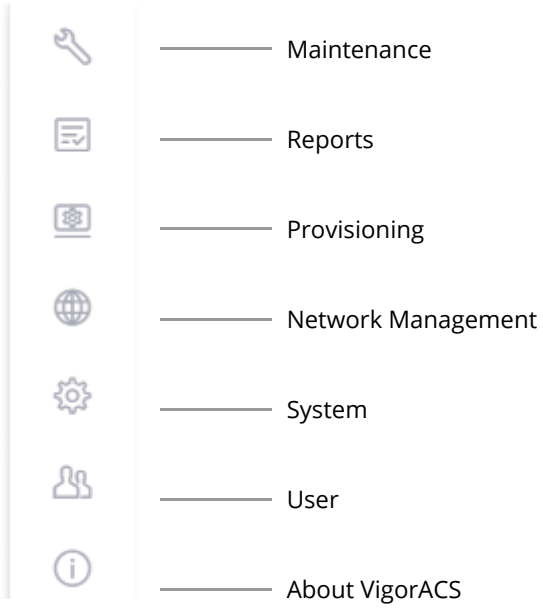
The configuration menu will vary in accordance with the CPE model. For more detailed information, refer to Part V, Chapter 9 Device Menu, Section 9.4 Configuration.

# Part III

System Menu

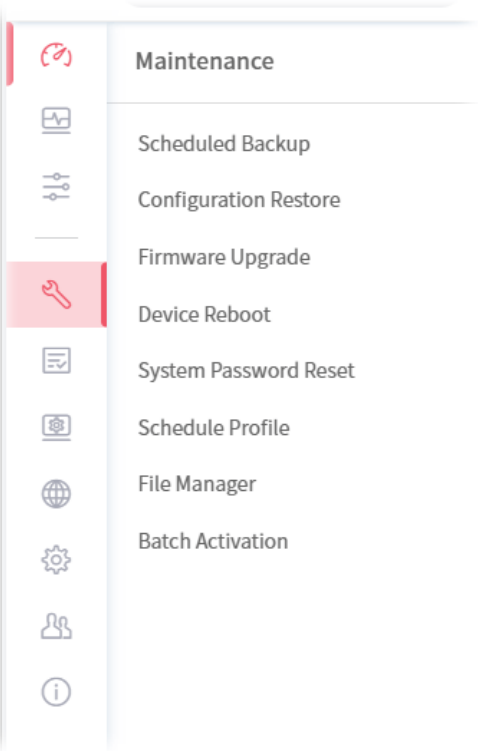
# Chapter 6 System Menu

System menu contains:




## 6.1 Maintenance

Settings in Maintenance can be applied onto numerous TR-069 CPEs instead of configuring settings for each CPE one by one.

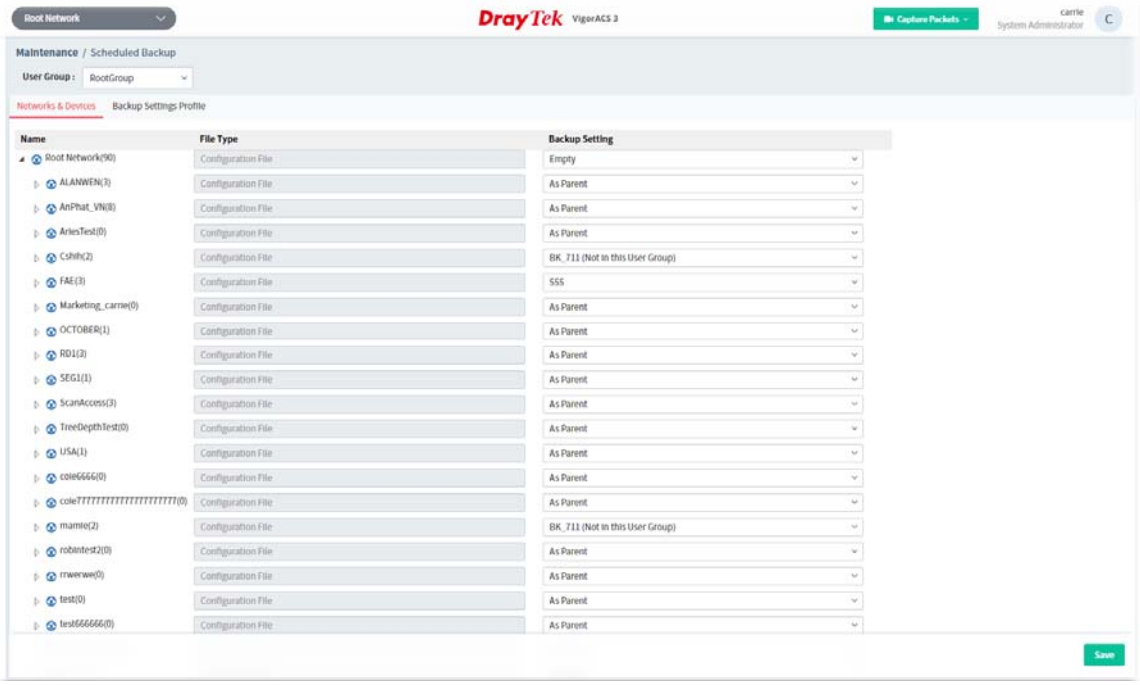


Maintenance menu is available only for the role of **System Administrator**, **Group Administrator**, **Administrator** and **Standard** (limited in VigorACS cloud version).

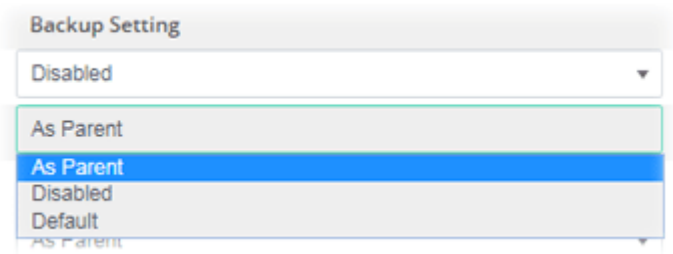
## 6.1.1 Scheduled Backup

### 6.1.1.1 Networks & Devices

This page is used to specify a backup profile for the device / network. Later, the configuration backup for the device/network will be executed automatically by VigorACS.



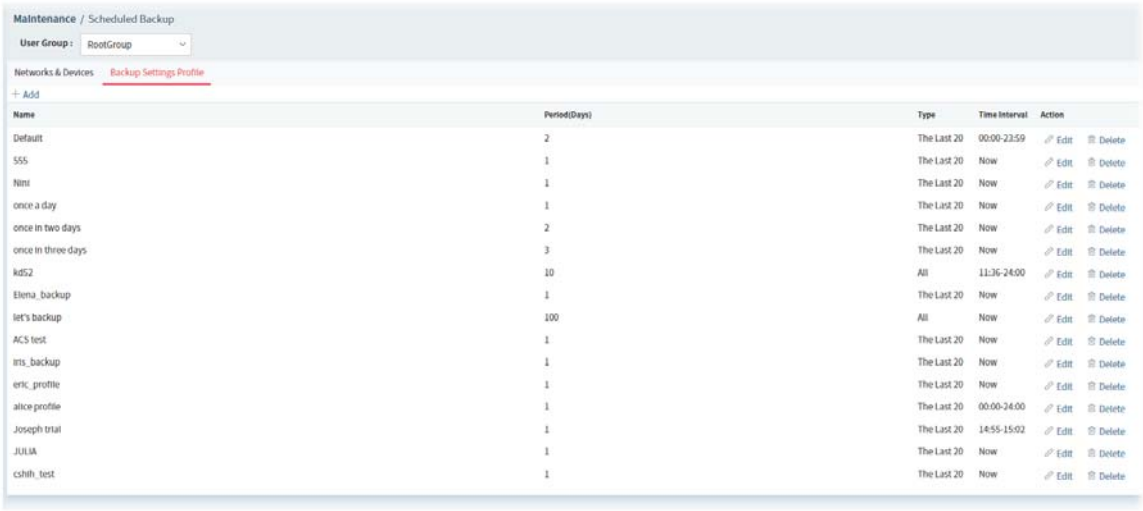

These parameters are explained as follows:

| Item | Description |
|---|---|
| **User Group** | Specify a user group for applying the backup settings profile.<br>Each user group can be configured with different backup settings profiles. |
| **File Type** | Display the file type used for the device. |
| **Backup Setting** | Choose a profile defined in **Backup Settings Profile** for applying onto the selected CPE.<br>  <br>**As Parent** - The backup setting for the selected network / device is the same as the top setting.<br>**Disable** - No backup setting for the selected network / device.<br>**Default** - Use the default backup setting for the selected network / device. |

| | |
|---|---|
| | **Others** - In addition to As Parent, Disable and Default, profiles defined in Backup Settings Profile also will be listed in this drop-down list. |
| **Save** | Save the current settings. |

### 6.1.1.2 Backup Settings Profile

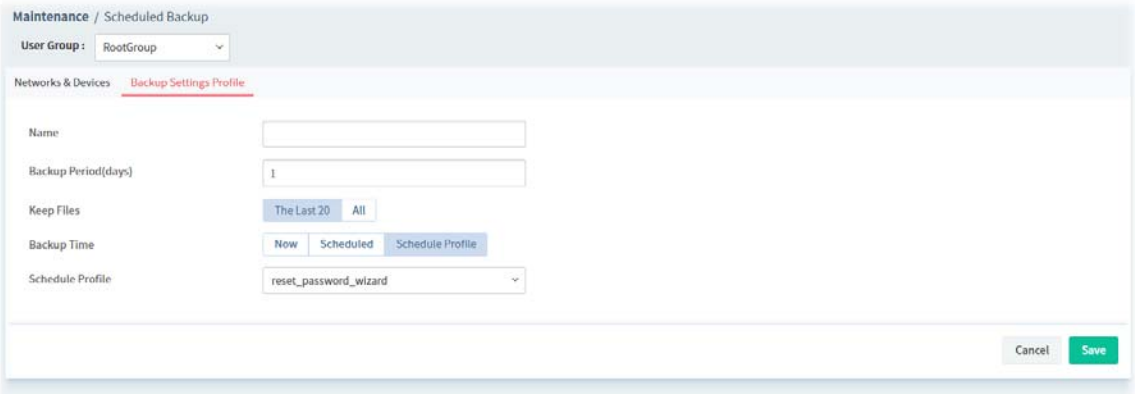
This page determines the trigger time and method for firmware backup.




These parameters are explained as follows:

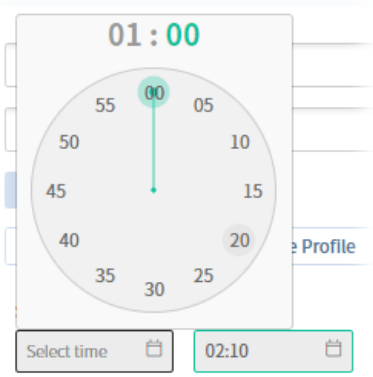
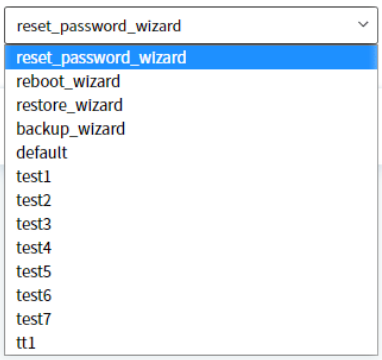
| Item | Description |
|---|---|
| **User Group** | Specify a user group for applying the backup settings profile.<br>Each user group can be configured with different backup settings profiles. |
| **+Add** | Click to create a new profile. |
| **Edit** | Click to modify, change the selected profile. |
| **Delete** | Click to delete the selected profile. |

The following setting page appears when **+Add** is clicked.




These parameters are explained as follows:

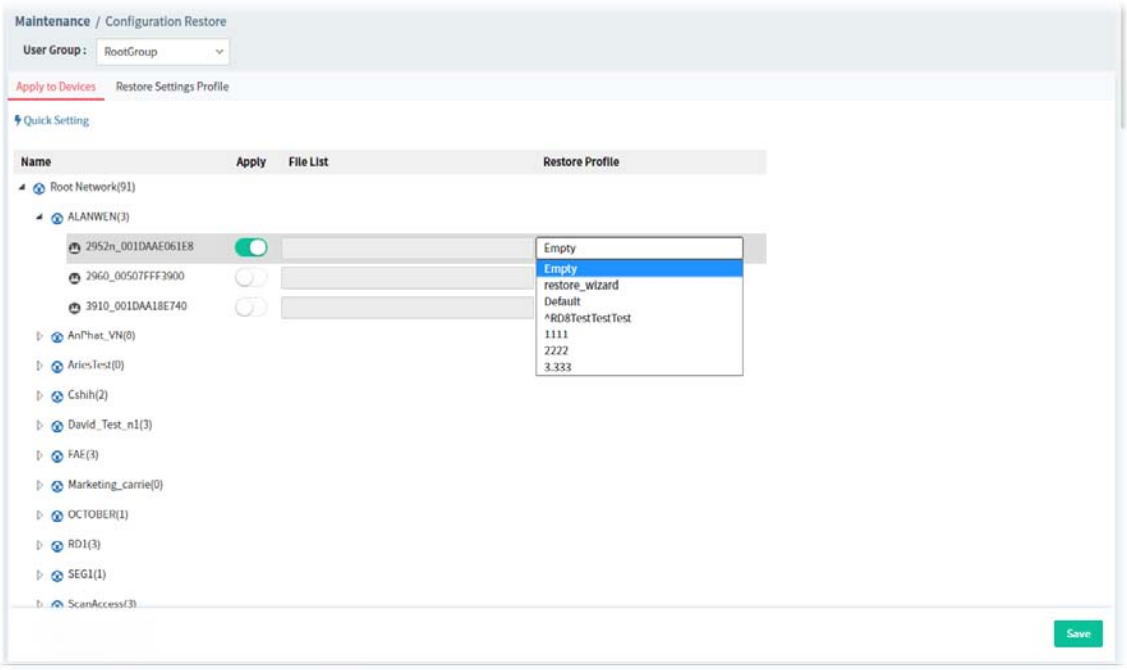
| Item | Description |
|---|---|
| **User Group** | Specify a user group for applying the backup settings profile.<br>Each user group can be configured with different backup settings profiles. |
| **Name** | Enter a name of the backup profile. |

| | |
|---|---|
| **Backup Period(days)** | The number typed here means the interval for the backup executed by VigorACS. The unit is “day”. If you type 1, that means the backup will be executed one time by one day. |
| **Keep Files** | Choose to keep all of the files (router’s configuration files) or the last 20 files. |
| **Backup Time** | Set a time interval for executing the backup work for networks and devices.<br>● **Now**<br>● **Scheduled**<br>● **Schedule Profile** |
| **Scheduled** | **Start Time / End Time –** Click **Select time** to display a clock. Set the hour and minutes by clicking the number on the clock.<br>  <br>**Specify Start Date** – Click to enable the time setting.<br>**Date** – Click to pop up a calendar to choose a date as the starting date. |
| **Schedule Profile** | Choose a trigger profile from the drop down list. In which, VigorACS offers default schedule profile.<br>  |

## 6.1.2 Configuration Restore

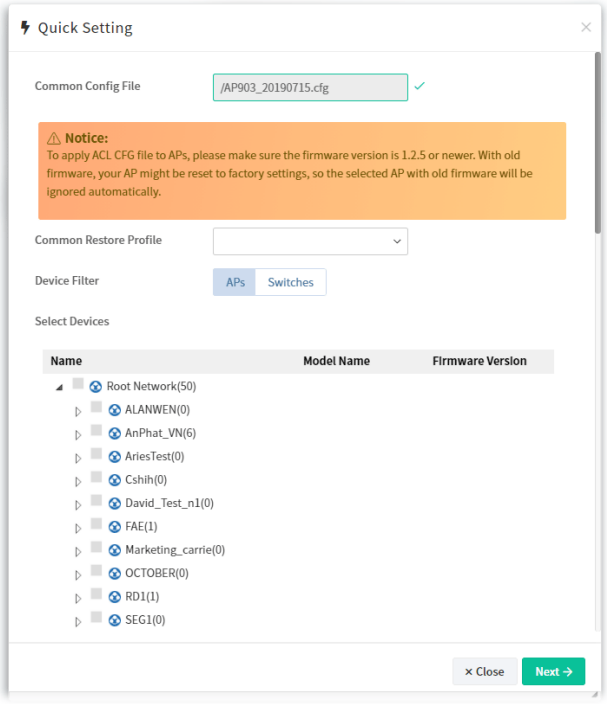
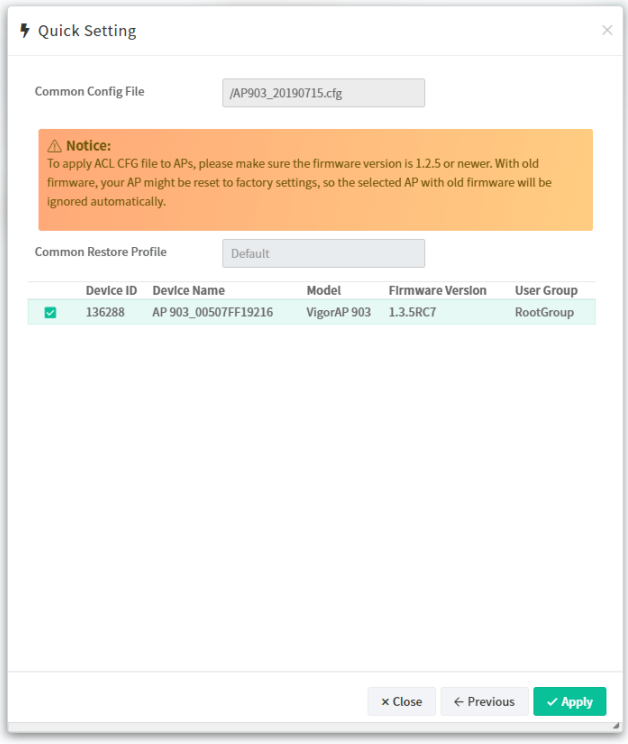
### 6.1.2.1 Apply to Devices

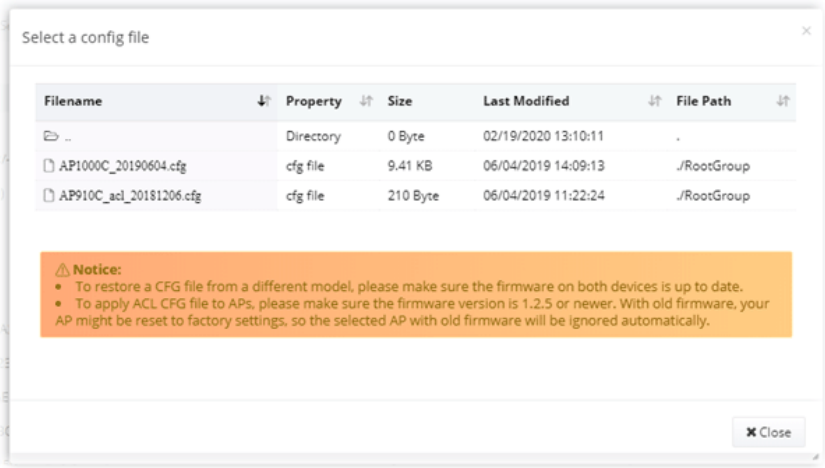
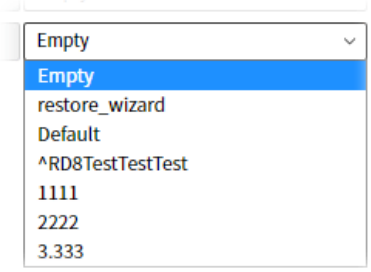
This page can determine which device or network will be applied with restore profiles. Later, the configuration restoration for the device/network will be executed automatically by VigorACS.




These parameters are explained as follows:

| Item | Description |
|---|---|
| **User Group** | Specify a user group for applying the restore settings profile.<br>Each user group can be configured with different restore settings profiles. |
| **Quick Setting** | This wizard offers a series of steps to specify configuration file which can be applied to multiple APs / Switches at one time. |

| | |
|---|---|
| |  <br>In which, click the Common Config File to select a "cfg" file. Then select a restore profile and specify the device filter (AP or switch). From the Select Devices list, select one or more APs/Switches required to apply the configuration file. Click **Next** to get the following page.<br>  <br>Check if the selected devices are correct or not. If yes, click **Apply**. The selected configuration file will apply to all of the selected devices. |
| **Apply** | Click the icon to enable configuration restoration for the selected CPE. |
| **File List** | Open a dialog to choose one of the files for the file restoration of the selected CPE. |

| | |
|---|---|
| |  |
| **Restore Profile** | Choose a profile defined in **Restore Settings Profile** for applying onto the selected CPE.<br>  <br>**Empty** - No restore setting for the selected network / device.<br>**Default** - Use the default restore setting for the selected network / device.<br>**Others** - In addition to Empty and Default, profiles defined in Restore Settings Profile also will be listed in this drop-down list. |
| **Save** | Save the current settings. |

### 6.1.2.2 Restore Settings Profile

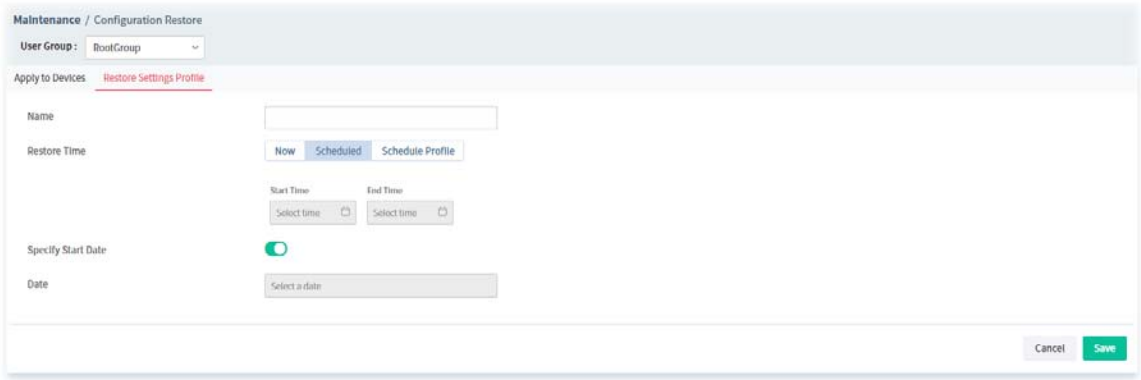
This page can determine the trigger time and method for firmware restoration.

These parameters are explained as follows:

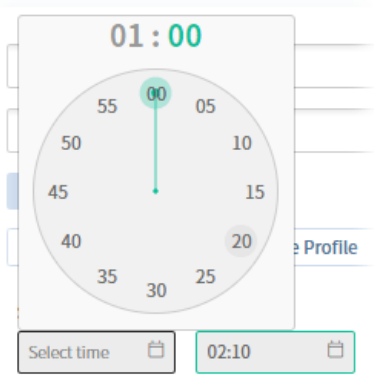
| Item | Description |
|---|---|
| **User Group** | Specify a user group for applying the configuration restore settings profile.<br>Each user group can be configured with different configuration restore settings profiles. |
| **+Add** | Click to create a new profile. |
| **Name** | Displays the name of the restore setting profile. |

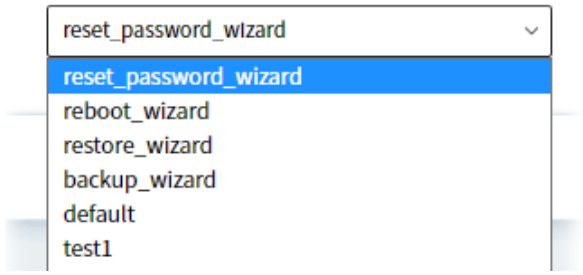
| | |
|---|---|
| **Trigger Profile** | Displays the time schedule selected for the restore setting profile. |
| **Time Interval** | Displays the time period to trigger the setting restoration. |
| **Edit** | Click to modify, change the selected profile. |
| **Delete** | Click to delete the selected profile. |

The following setting page appears when **+Add** is clicked.




These parameters are explained as follows:

| Item | Description |
|---|---|
| **User Group** | Specify a user group for applying the restore settings profile.<br>Each user group can be configured with different restore settings profiles. |
| **Name** | Enter a name of the restore setting profile. |
| **Restore Time** | Set a time interval for executing the backup work for networks and devices.<br>● **Now**<br>● **Scheduled**<br>● **Schedule Profile** |
| **Now** | The configuration restore will be executed after clicking **Save.** |
| **Scheduled** | **Start Time / End Time –** Click **Select time** to display a clock. Set the hour and minutes by clicking the number on the clock.<br>  <br>**Specify Start Date** – Click to enable the time setting.<br>**Date** – Click to pop up a calendar to choose a date as the starting date. |
| **Schedule Profile** | **Trigger Profile –** Choosing a trigger profile from the drop down list. In which, VigorACS offers default schedule profile. |




### 6.1.3 Firmware Upgrade

When VigorACS server receives information from CPE about firmware upgrade, it will check if the received model name, modem firmware version, and software version correspond to the information recorded in VigorACS server. If everything can match but software version not, VigorACS will judge that the remote CPE requiring firmware upgrade. Next, VigorACS server will execute firmware upgrade with the file listed in Job List automatically at specified time.

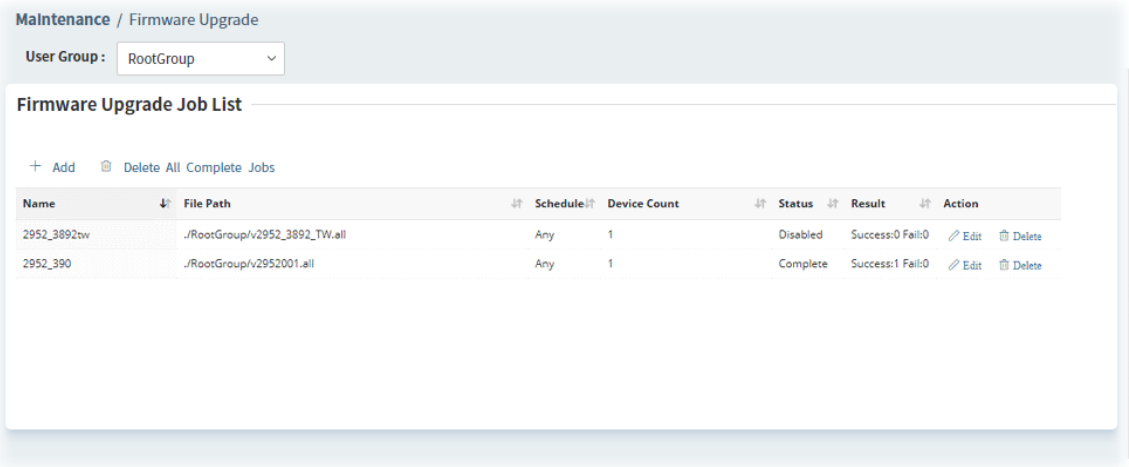
This web page allows you to **specify** required information for matching with the CPE device. The profiles created here will be regarded as a basis that VigorACS server uses to compare information coming from CPE router with the information stored in VigorACS server's database.

---

The firmware upgrade profile created in such page can be applied to single and selected devices (but not applied to the whole network).

For applying an upgrade provision profile to the whole network / group, please go to Provisioning>>Firmware Upgrade for more detailed information.

---

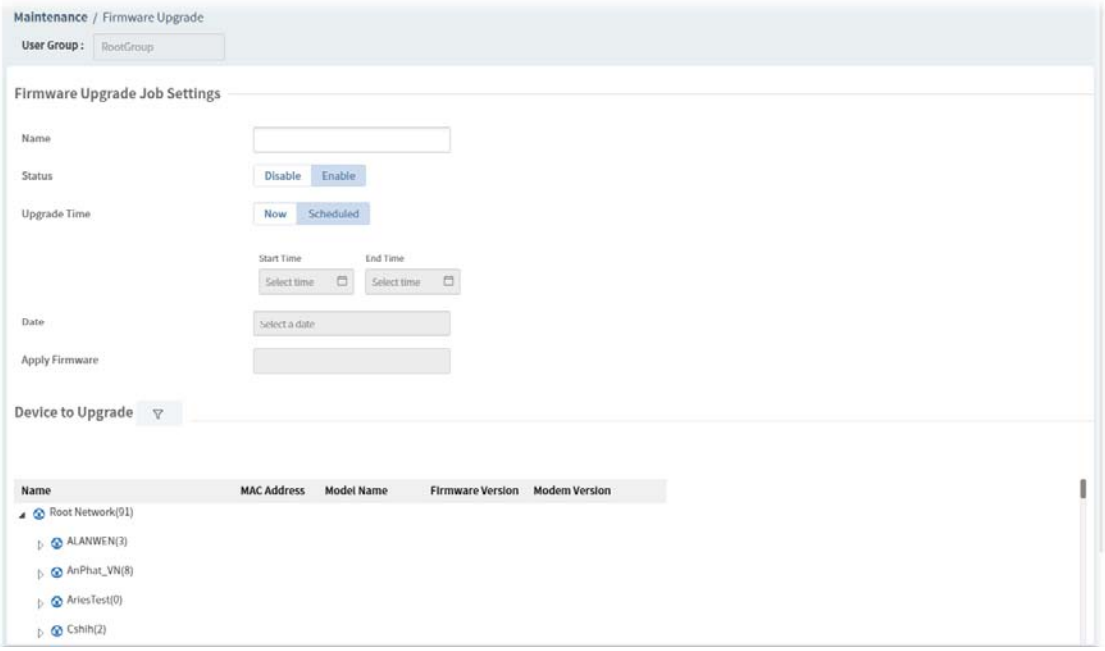



These parameters are explained as follows:

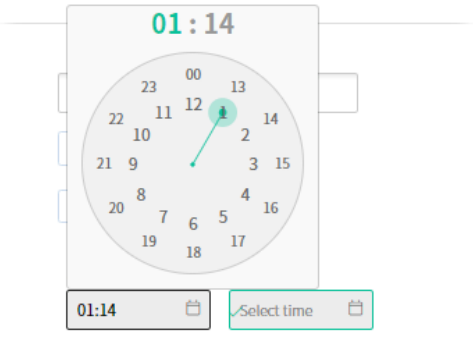
| Item | Description |
|---|---|
| **User Group** | Specify a user group. The job list under that group will be displayed on this page. |
| **+Add** | Click to create a new job profile. |
| **Delete All Complete Jobs** | Click to delete all profile. |
| **Edit** | Click to edit / modify the settings for the selected profile. |

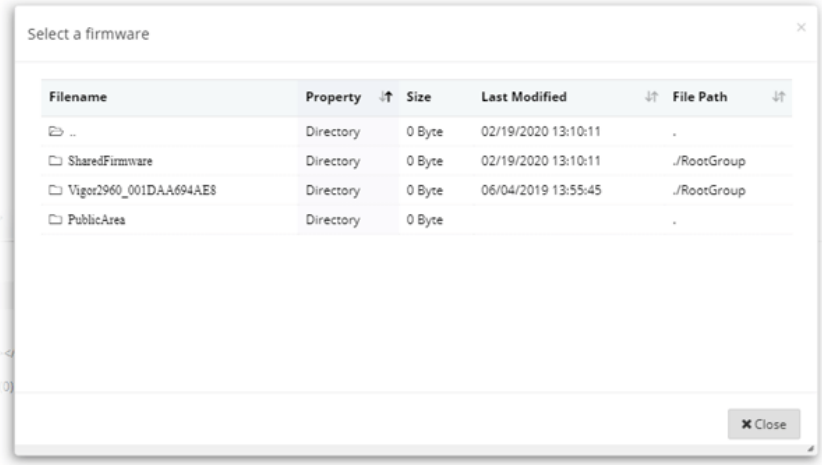
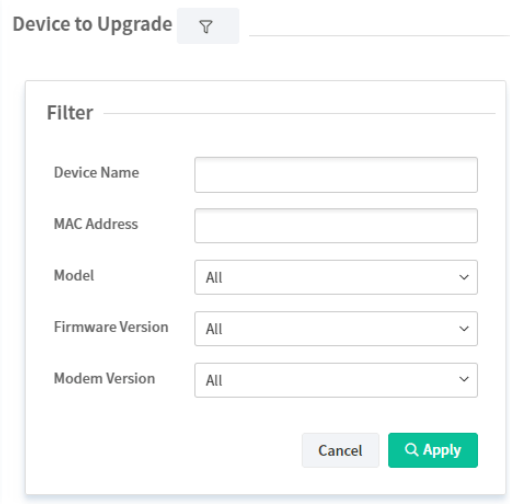
| | |
|---|---|
| **Delete** | Click to delete the selected profile. |

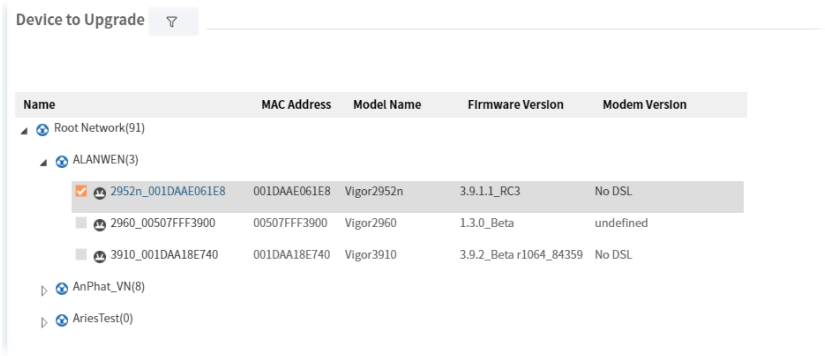
The following setting page appears when **+Add** is clicked.




These parameters are explained as follows:

| Item | Description |
|---|---|
| **Name** | Enter a name of the job profile. |
| **Status** | Click **Enable** to activate the firmware upgrade profile. |
| **Upgrade Time** | Set a time interval for executing the backup work for networks and devices.<br>● **Now**<br>● **Scheduled** |
| **Scheduled** | **Start Time / End Time –** Click **Select time** to display a clock. Set the hour and minutes by clicking the number on the clock.<br>  <br>**Date** – Click to pop up a calendar to choose a date as the starting date. |
| **Apply Firmware** | Click to open a dialog to select a firmware file. VigorACS will upgrade the selected CPE with the selected file. |

| | |
|---|---|
| |  |
| **Device to Upgrade** | Click the **Filter** icon to set the filtering conditions.<br>  <br>**Device Name -** Enter the name of the device to be shown on the table.<br>**MAC Address** - Enter the MAC address of the device to be shown on the table.<br>**Model** – Select a model of CPE.<br>**Firmware Version** – Select a firmware version. CPE with the selected firmware will be shown on the table.<br>**Modem Version** - Select a modem version. CPE with the selected modem will be shown on the table.<br>**Apply** - After clicking **Apply**, the table below will show the devices according to filter conditions. |
| **Table** | Select one device or more devices to apply the firmware upgrade provision. |

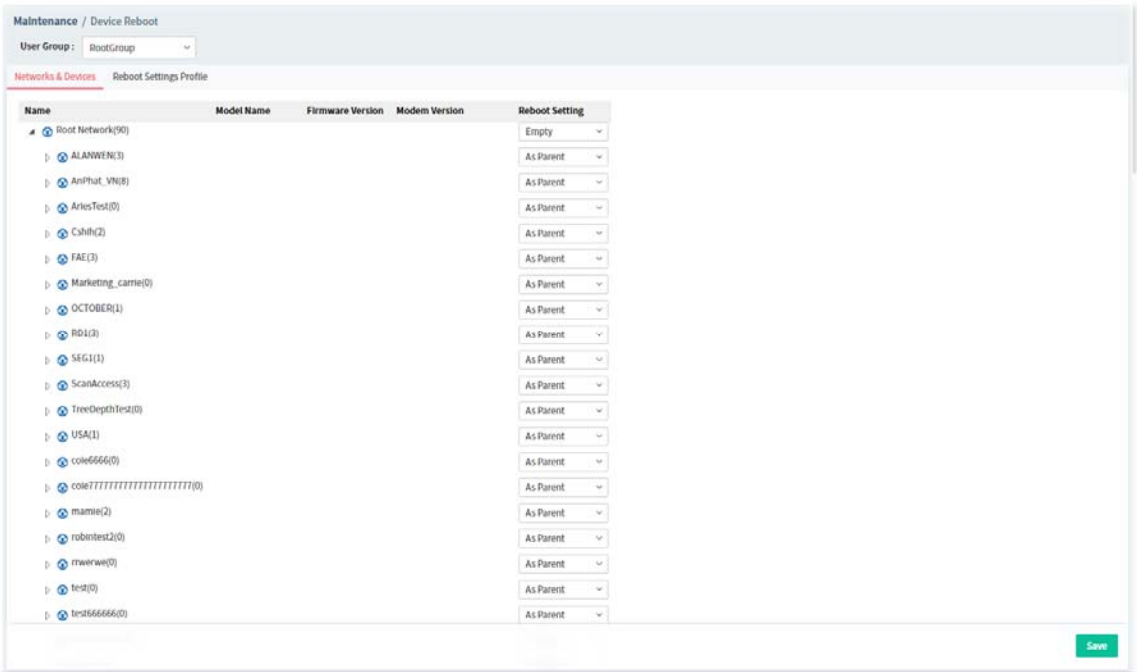
| | |
|---|---|
| |  <br>**Model Name** – Display the model name for identification.<br>**Firmware Version** – Display the firmware version that the model used currently. |
| **Cancel** | Discard current settings and return to previous page. |
| **Save** | Save the current settings and exit the page. |

## 6.1.4 Device Reboot

You can define the time schedule for rebooting the selected CPE(s) automatically by VigorACS. Open **Maintenance>>Device Reboot** to display the following page.

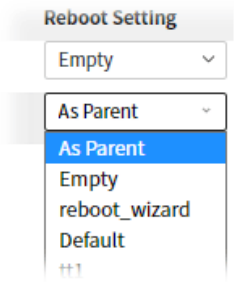
### 6.1.4.1 Networks & Devices

This page is used for configuring the reboot setting for network(s) & device(s)



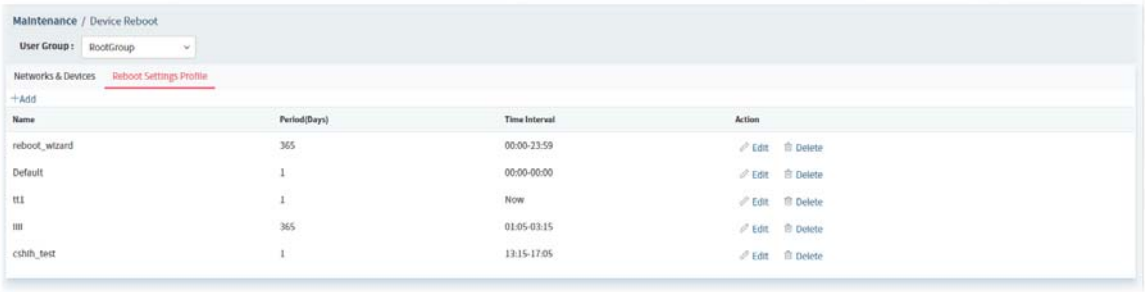

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Reboot Setting** | Choose a profile defined in **Reboot Settings Profile** for applying onto the selected CPE. |

| | |
|---|---|
| |  <br>**As Parent** - The reboot setting for the selected network / device is the same as the top setting.<br>**Empty** - No reboot setting for the selected network / device.<br>**Default** - Use the default reboot setting for the selected network / device.<br>**Others** - In addition to As Parent, Empty and Default, profiles defined in Reboot Settings Profile also will be listed in this drop-down list. |
| **Save** | Save the current settings. |

### 6.1.4.2 Reboot Settings Profile

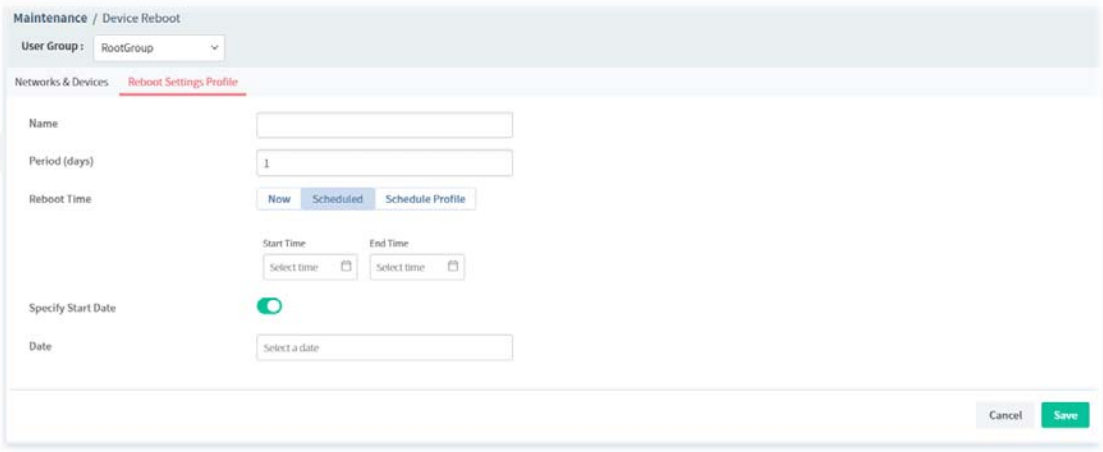
This page can determine the trigger time and method for device reboot.



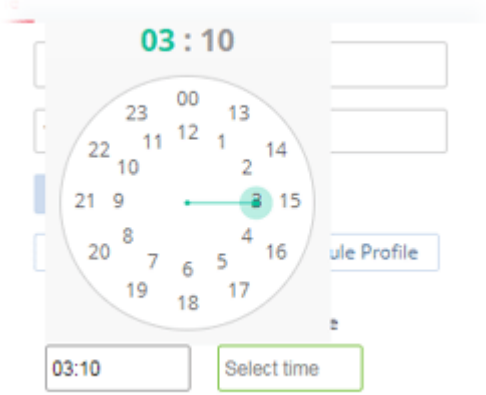
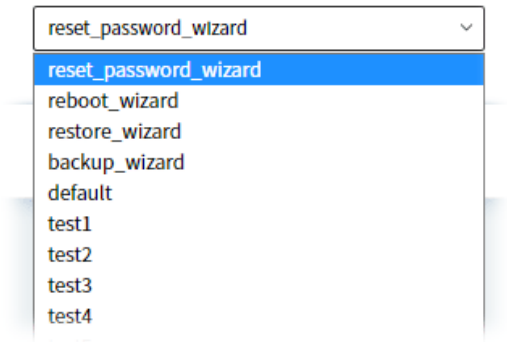

These parameters are explained as follows:

| Item | Description |
|---|---|
| **User Group** | Specify a user group. |
| **+Add** | Click to create a new device reboot profile. |
| **Edit** | Click to edit / modify the settings for the selected profile. |
| **Delete** | Click to delete the selected profile. |

The following setting page appears when **+Add** is clicked.

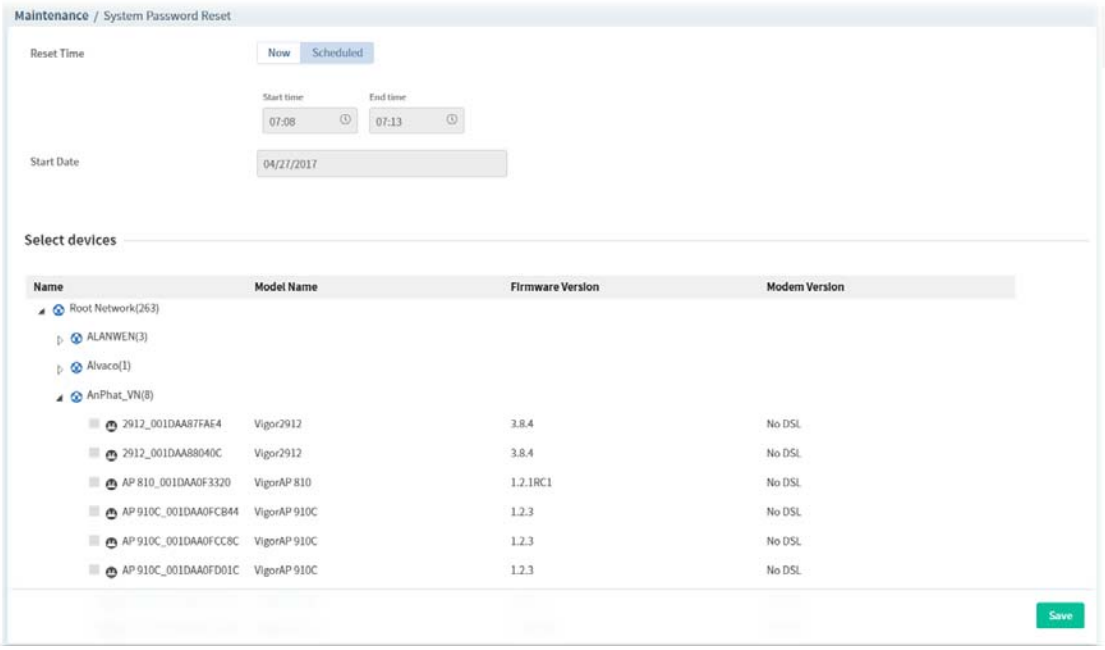



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Name** | Enter the name of the profile. |
| **Period(days)** | Determine the frequency for the CPE reboot by VigorACS. The default value is 1 day. |
| **Reboot Time** | Set a time interval for executing the device reboot.<br>● **Now**<br>● **Scheduled**<br>● **Schedule Profile** |
| **Scheduled** | **Start Time / End Time –** Click **Select time** to display a clock. Set the hour and minutes by clicking the number on the clock.<br>  <br>**Specify Start Date** – Click to enable the time setting.<br>**Date** – Click to pop up a calendar to choose a date as the starting date. |
| **Schedule Profile** | **Trigger Profile –** Choosing a trigger profile from the drop down list. In which, VigorACS offers default schedule profile.<br>  |
| **Cancel** | Discard current settings and return to previous page. |
| **Save** | Save the current settings. |

### 6.1.5 System Password Reset

This page is used to reset the default factory password for the administrator of CPE.

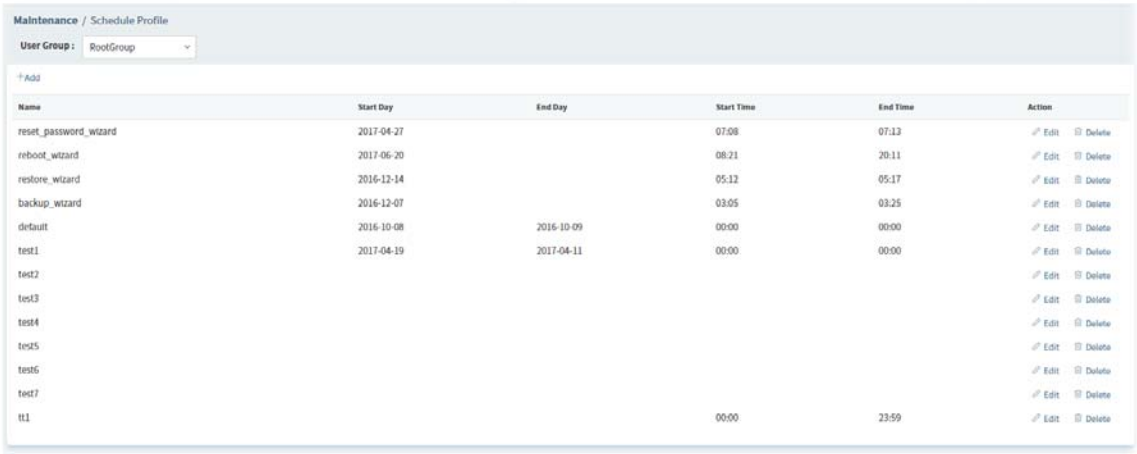



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Reset Time** | **Now** – Reset the password for the selected device(s) immediately.<br>**Scheduled** – To specify a certain time to perform the job, choose this one and specify start day, start time and end time respectively. VigorACS will perform the job for the selected CPE (s) according to the schedule set here.<br>● **Start time** - Use the drop down menu to specify the hour and minutes you want to start the operation.<br>● **End time** - Use the drop down menu to specify the hour and minutes you want to finish the operation.<br>● **Start day** – Use the drop down calendar to specify the day you want to start the operation. |
| **Select devices** | Choose the device that you want to do device password reset. |
| **Save** | Save the current settings. |

### 6.1.6 Schedule Profile

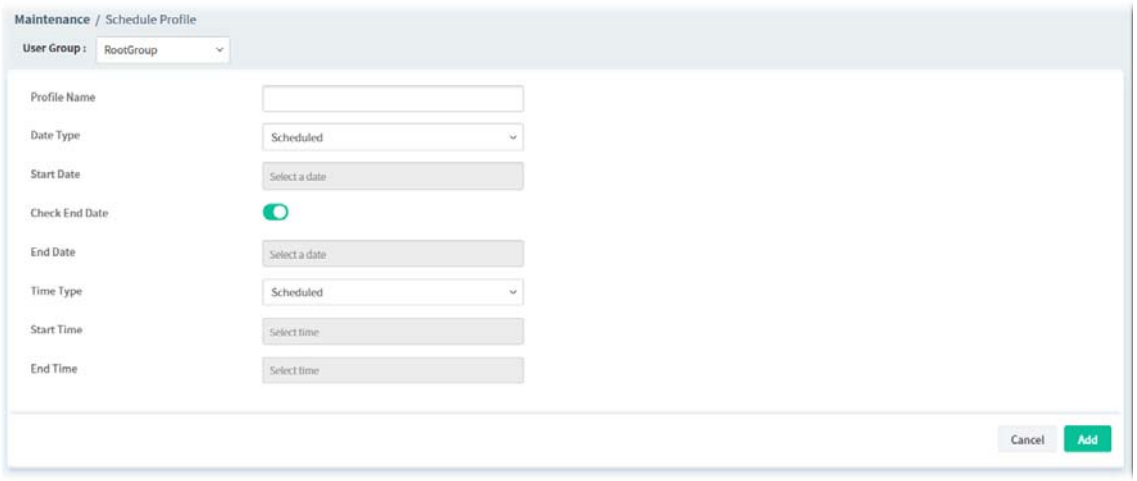
Schedule profiles can be set to apply to devices managed by VigorACS 3. Later, you can not only schedule the router to dialup to the Internet at a specified time, but also restrict Internet access to certain hours so that users can connect to the Internet only during certain hours, say, business hours. The schedule profile is applicable to several functions driven by VigorACS 3.




These parameters are explained as follows:

| Item | Description |
|---|---|
| **User Group** | Specify a user group. The schedule profiles under that group will be displayed on this page. |
| **+Add** | Click to create a new schedule profile. |
| **Edit** | Click to modify, change the selected profile. |
| **Delete** | Click to delete the selected profile. |

The following setting page appears when **+Add** is clicked.



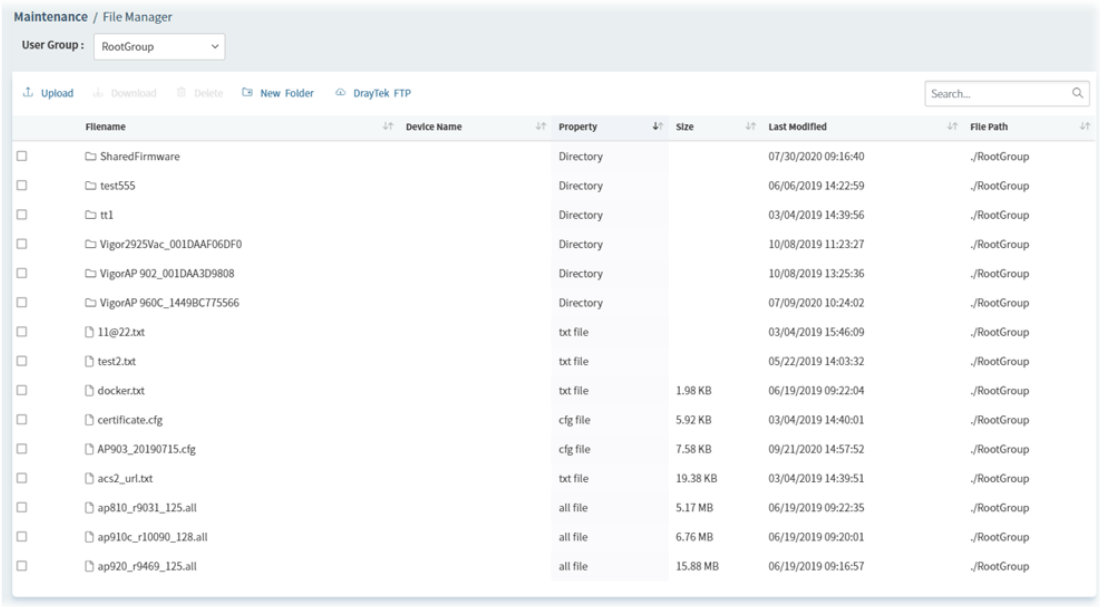

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Profile Name** | Enter a name of the schedule profile. |
| **Date Type** | VigorACS 3 will perform the job for the selected CPE (s) according to the schedule set here.<br>**Now** – When CPE meets settings configured in the profile, the job (e.g., |

| | |
|---|---|
| | upgrade) for the CPE will be performed immediately.<br>**Schedule** – To specify a certain day to perform the job, choose this one and specify start day and end day respectively. |
| **Start Day** | Use the drop down calendar to specify the day you want to start the operation. |
| **Check End Day** | Click to enable the end day to determine if the job is performed or not. For example, the end day for firmware upgrade is out of date, then the upgrade will not be executed for the selected CPE. |
| **End Day** | Use the drop down calendar to specify the day you want to end the operation. |
| **Time Type** | **Now** – When CPE meets settings configured in the profile, the job (e.g., upgrade) for the CPE will be performed immediately.<br>**Schedule** – To specify a certain time to perform the job, choose this one and specify start time and end time respectively. VigorACS will perform the job for the selected CPE (s) according to the schedule set here. |
| **Start Time** | Use the drop down menu to specify the hour and minutes you want to start the operation. |
| **End Time** | Use the drop down menu to specify the hour and minutes you want to finish the operation. |
| **Cancel** | Discard current settings and return to previous page. |
| **Add** | Save the current settings and create a new profile. |

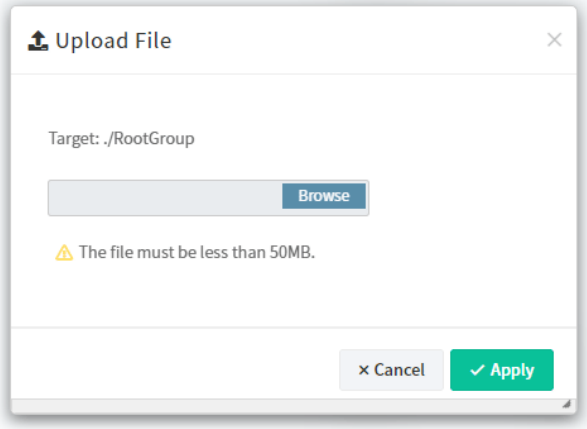
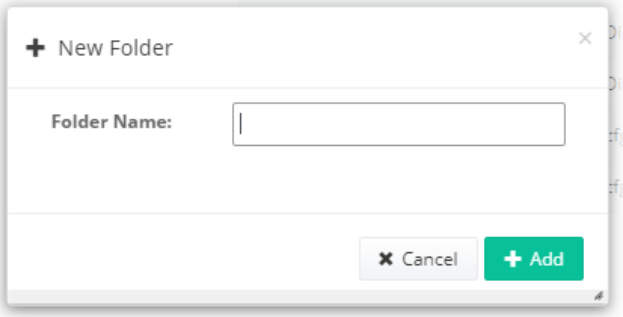
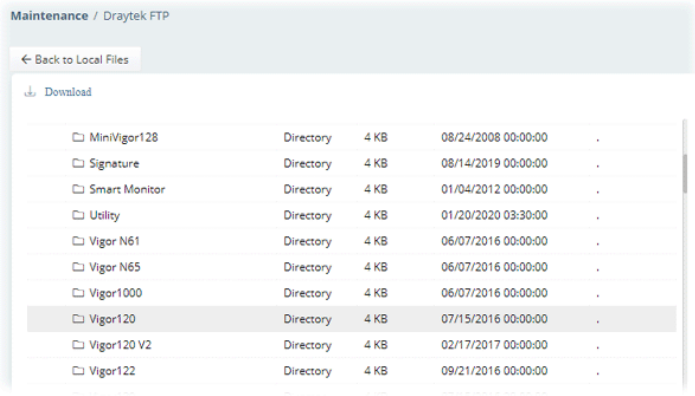
### 6.1.7 File Manager

Firmware driver, configuration file for devices (VigorAP, Vigor router or Vigor switches) can be managed or classified with different folders.



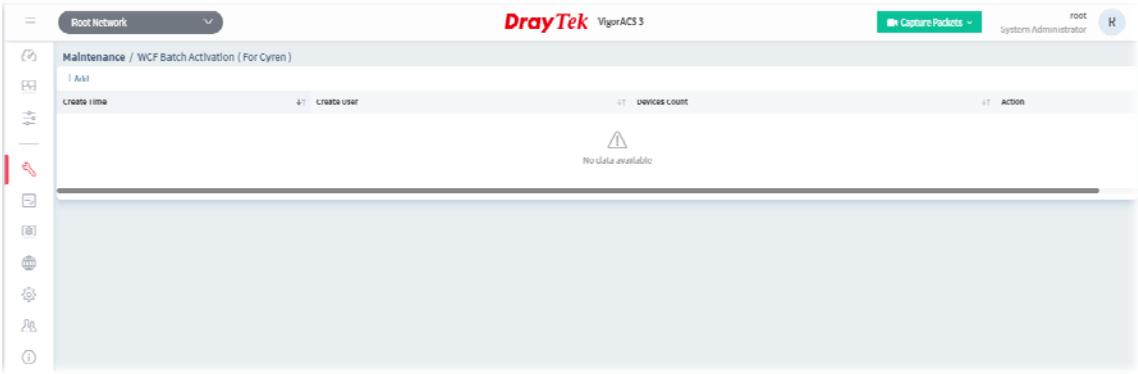

These parameters are explained as follows:

| Item | Description |
|---|---|
| **User Group** | Specify a user group. The devices (represented with MAC address) under that group will be displayed on this page. |

| | |
|---|---|
| **Upload** | Click to upload a file to VigorACS 3 server.<br>  |
| **Download** | Download a driver (*.all, *.rst and etc.) related to CPE device from VigorACS 3 server. |
| **Delete** | Click to delete the selected profile. |
| **New Folder** | Create folders for files classification/management.<br>  |
| **DrayTek FTP** | After clicking the link, the following page will appear for you to download file from DrayTek FTP directly.<br>  |

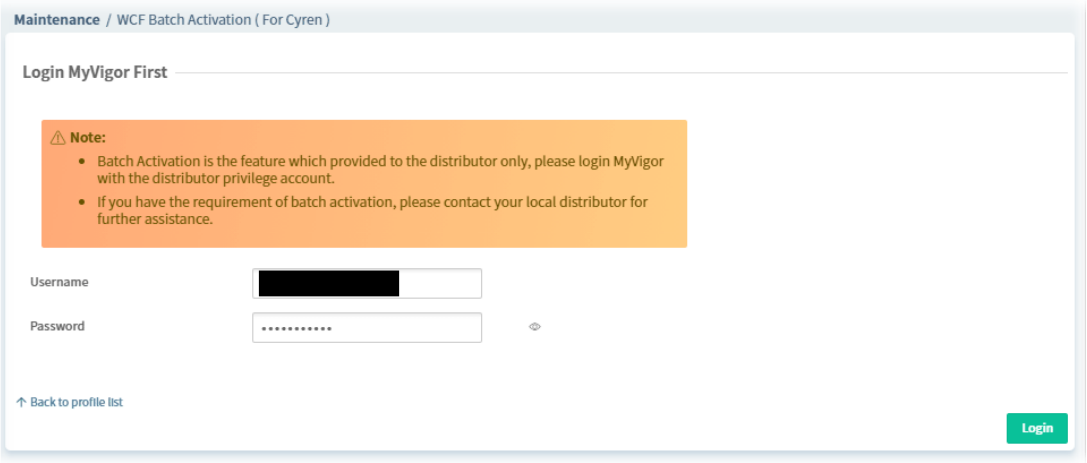
### 6.1.8 Batch Activation

Batch activation is convenient for a distributor to activate WCF filter service for multiple routers at one time. It is available only for Cyren web content filter service. In default, Batch Activation is disabled. To enable the feature, open **System >> System Parameter**. Locate the ID 48 and change the value as True. Then, open **Maintenance>>Batch Activation** to get the following page.



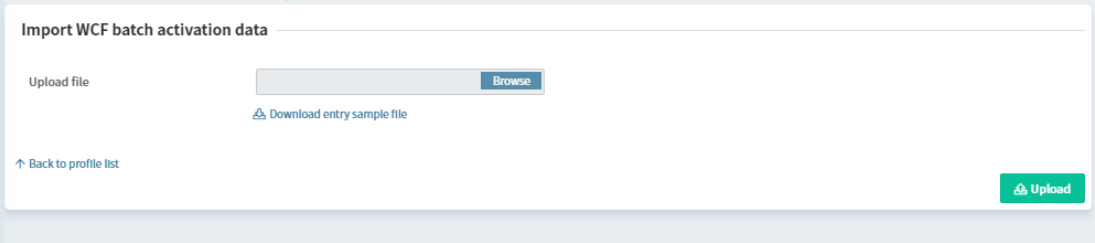

VigorACS will perform the job after creating a new profile. The execution result will be shown on the screen immediately.

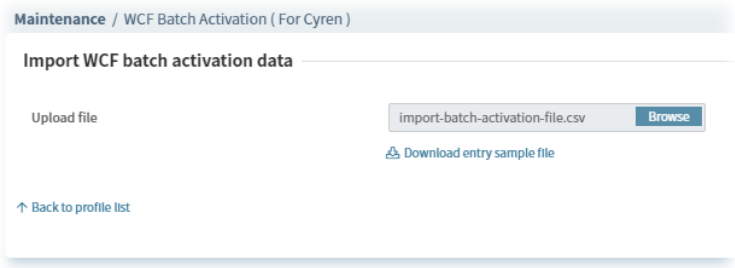
1. Click **+Add** to create a new batch activation profile.



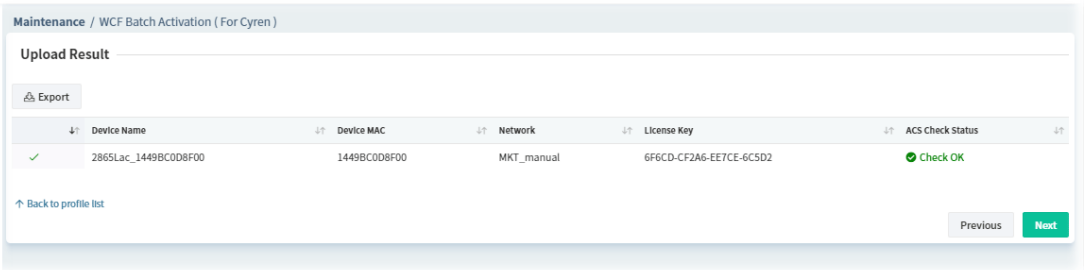

| Item | Description |
|---|---|
| **Username** | Enter a user account with the distributor privilege.<br>Once authenticated by MyVigor server successfully, the username will be brought out automatically next time. |
| **Password** | Enter the password.<br>Once authenticated by MyVigor server successfully, the password will be brought out automatically next time. |
| **Back to profile list** | Return to the previous profile list page. |
| **Login** | Access into next page. |

2. Enter the username and password and click **Login.** After authenticated by MyVigor server, the following page will be shown.

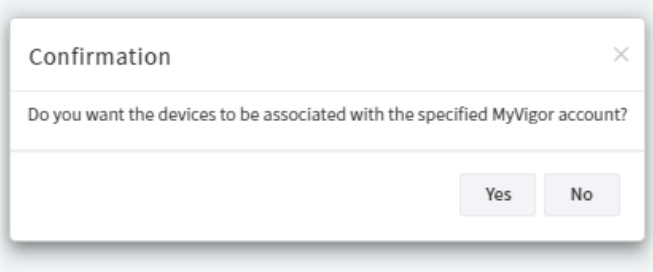



| Item | Description |
|---|---|
| **Upload file** | Click **Browse** to locate the CSV file with name of import-batch-activation-file.<br>  <br><br>If there is no file existed, click "Download entry sample file" link to download one file. |
| **Download entry sample file** | Click to download an entry sample file (import-batch-activation-file.csv).<br>Open the CSB file and enter the "MAC address" and "WCF KEY" for each device. |
| **Back to profile list** | Return to the previous profile list page. |
| **Login** | Access into next page. |

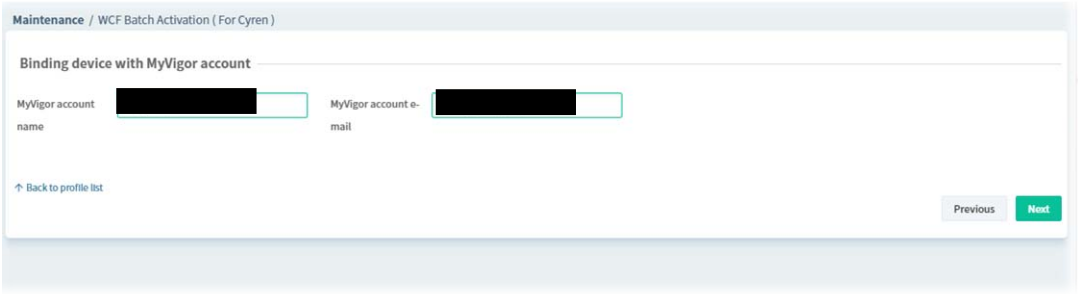
3. After locating the CSV file, click **Upload**. Later, the result will be shown as follows.



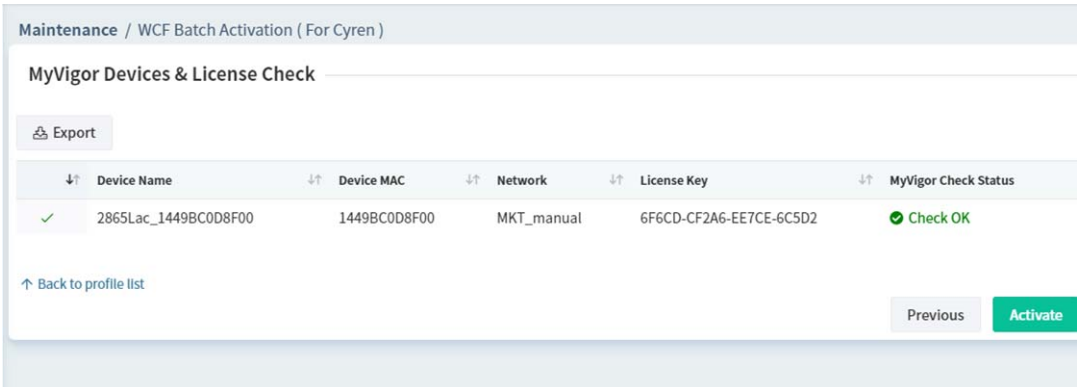

4. Click **Next**. If one of the CPE device not registered to the MyVigor server yet, a dialog will appear as follows.



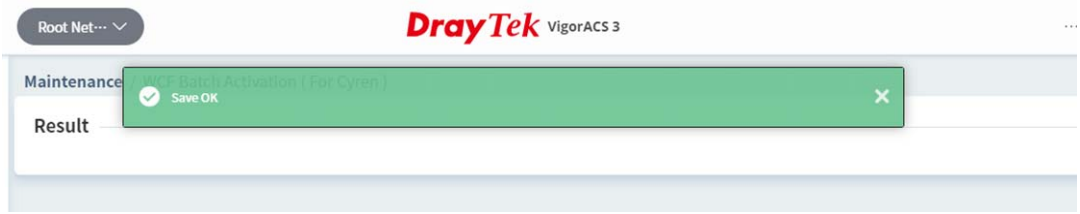
5. Click **Yes** to get the following page. Click **NO** and skip to step 6.




6. Enter an existed account name and account e-mail. The CPE device will be registered to the MyVigor server with this account.




7. Click **Activate**. Wait for a minute.

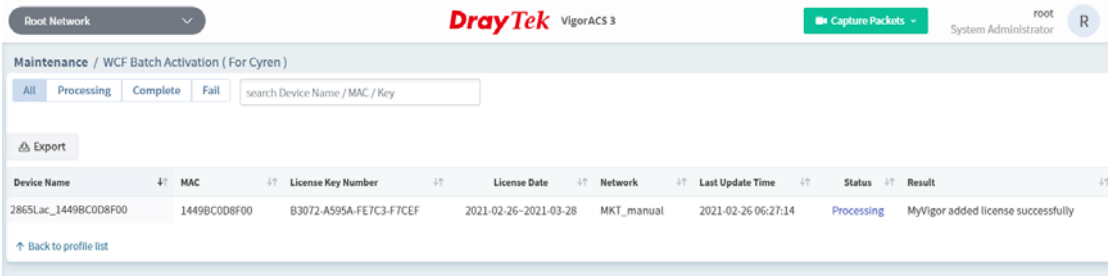



8. The batch activation profile has been created. The activation logs (time, user, device count and action) will be shown on this page.

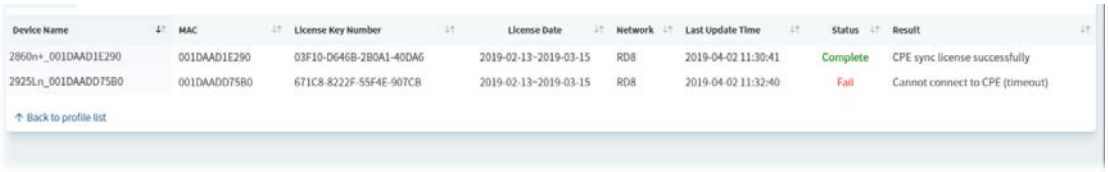
| Item | Description |
|---|---|
| **+Add** | Click to create a new batch activation profile. |
| **View Log** | Click to view the records of the WCF batch activation. |
| **Delete** | Click to remove the selected record. |

Click **View Log** to see current processing status.

example 1



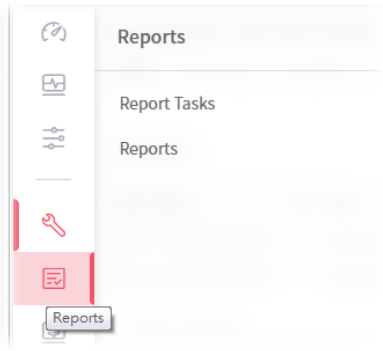

example 2




| Item | Description |
|---|---|
| **All, Processing, Complete, Fail** | Switch among these tabs to display the detailed information for the WCF application. |
| **Export** | Click to export current log to VigorACS server. |
| **Back to profile list** | Return to the previous profile list page. |

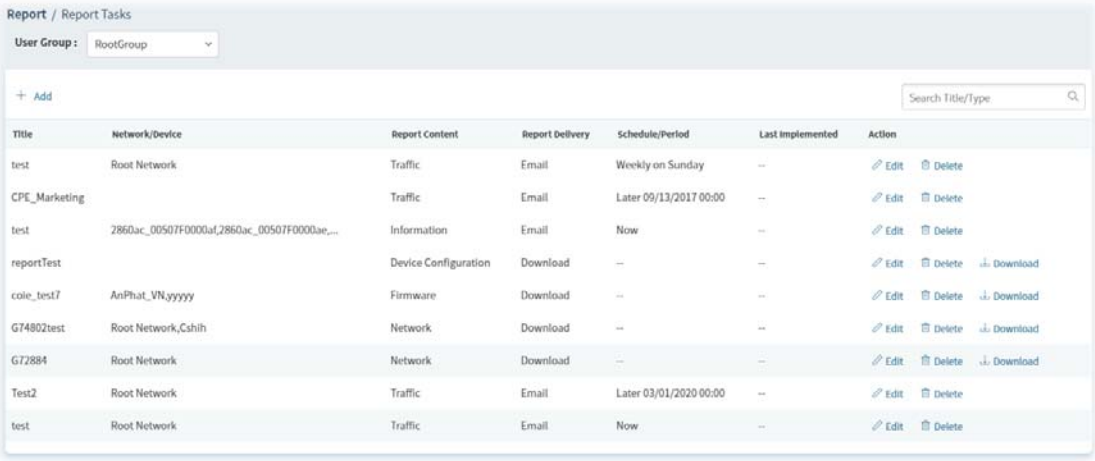
## 6.2 Reports

VigorACS will send reports to certain users periodically based on the report task profile defined in this page. The report task profile can be configured what kind of data (e.g., LAN statistics, traffic or firmware used) will be recorded, with different CPE, content of report, time, recipient, and so on.




### 6.2.1 Report Tasks

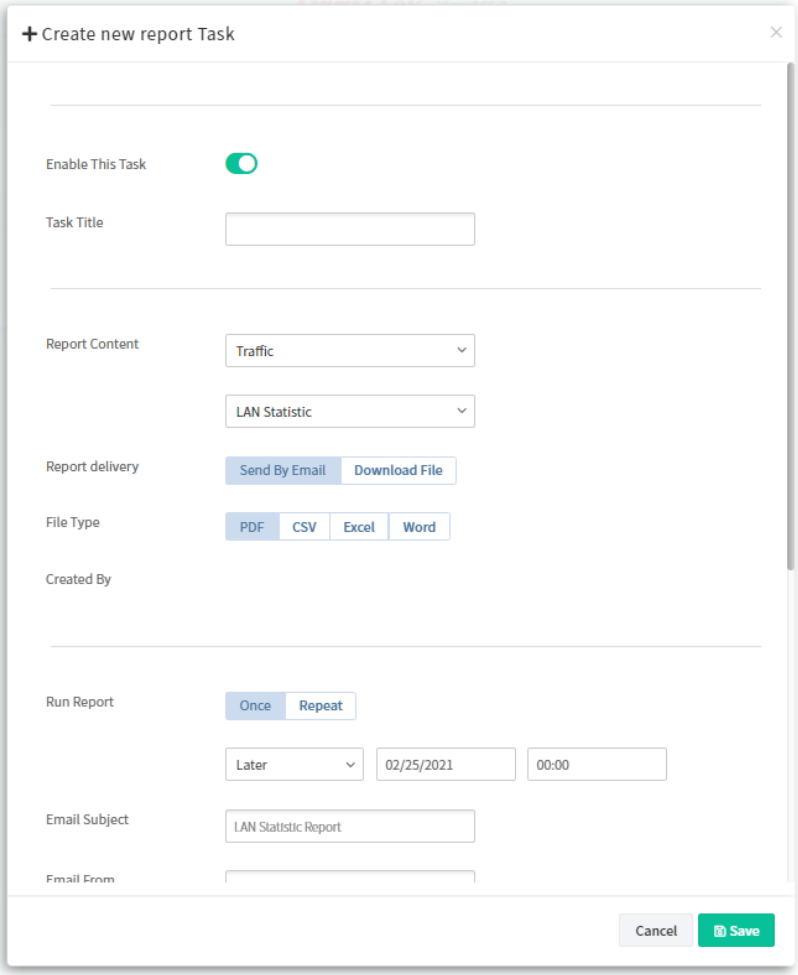
Open **Reports>Reports Tasks** to get the following page.



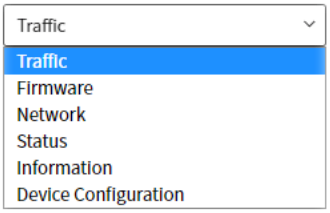

These parameters are explained as follows:

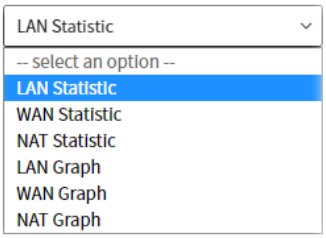
| Item | Description |
|---|---|
| **User Group** | Use the drop down list to choose a group (e.g., RootGroup).<br>Only the report task profiles defined for the selected user group will be shown on this page. If there is “no” profile displayed for the selected group, you may click the link of **+Add** to create a new one. |
| **+Add** | Click to create a new report task for specified CPE. |
| **Action** | **Edit** – Click to modify an existing report task.<br>**Delete** – Click to remove the selected report task.<br>**Download** - Click to download the report task as a "*.pdf" file for reference. |

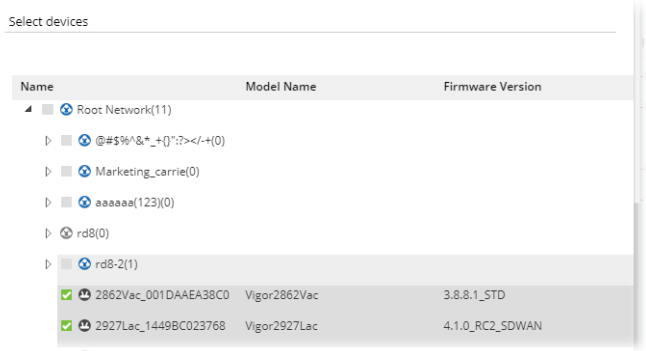
The following setting page appears when **+Add** is clicked.




These parameters are explained as follows:

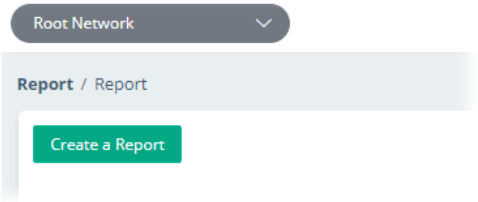
| Item | Description |
|---|---|
| **Enable This Task** | Enable this feature to make the system send report e-mail to the recipient on schedule. |
| **Task Title** | Enter a name for such report task profile. |
| **Report Content** | At present, VigorACS offers several types of report, including traffic, firmware, network, status, information and device configuration.<br>  <br>Use the scroll bar to choose the type you want and select an option for that type.<br>Next, select the way (statistic or graph) to show the report. |

| | |
|---|---|
| |  |
| **Report delivery** | Choose the method to process the report.<br>**Send By Email** - The report will be sent out based on the mail conditions set in this page.<br>**Download File** - The report can be downloaded to local host. |
| **File Type** | It is available when **Device Configuration** is selected as **Report Content**.<br>Choose PDF, CSV, Excel or Word as the file format for device configuration report. |
| **Parameter List** | It is available when **Device Configuration** is selected as **Report Content**.<br>Enter the TR-069 parameter on the entry box and click +Add. Later, the report will be created with the configuration of the specified parameters listed in Parameter List.<br> |
| **Run Report** | **Once** – The report will be made just for one time. Specify the date and time.<br>**Repeat** – The report will be made repeatedly. Click the **Edit** link to open a dialog. Set the day, starting date and starting time. |
| **Email Subject** | It is available when **Send By Email** is selected as **Report delivery.**<br>Specify the subject for the email. |
| **Email From** | It is available when **Send By Email** is selected as **Report delivery.**<br>Enter the email address of the sender. |
| **Email Content** | It is available when **Send By Email** is selected as **Report delivery.**<br>Enter the content of the email. |
| **Email To** | It is available when **Send By Email** is selected as **Report delivery.** Enter the email address of the recipient.<br>**+Add** – If there is more than one recipient for adding, click the link to have more entry box(es) for adding more recipients. |
| **Select devices** | Only the CPEs under the selected User Group (e.g., RootGroup in this case) will be shown in this field.<br>Check the box to the left of the network group to select the device(s) you want to make report. |

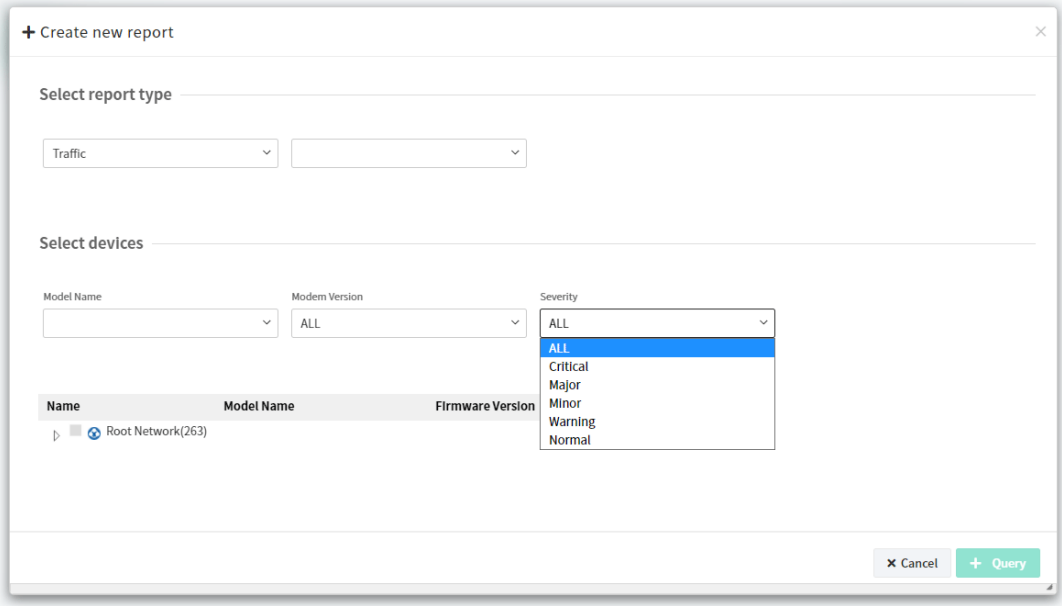
| | |
|---|---|
| |  |
| **Save** | Save the settings and return to previous page. |

### 6.2.2 Reports

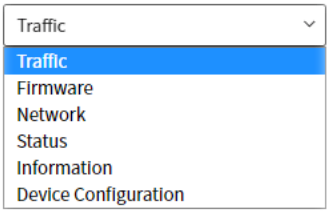
This function can print out VigorACS report based on the settings configured in this web page.

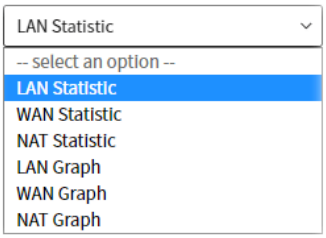
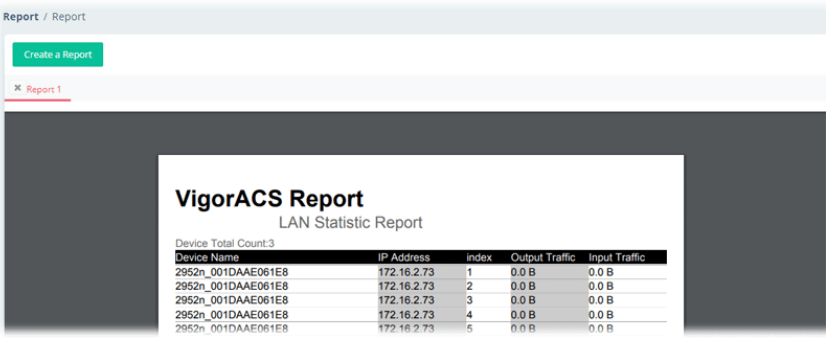



Click **Create a Report** to get the following page.



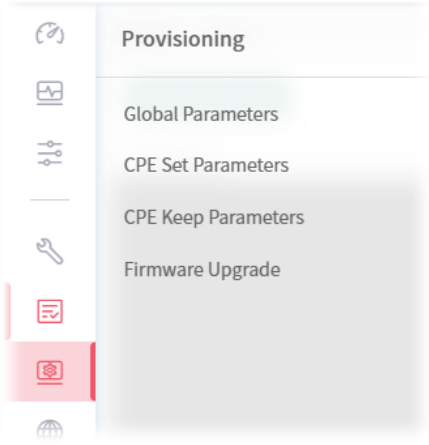

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Select report type** | At present, VigorACS offers five types of report, including traffic, firmware, network, status, information and device configuration.<br>  <br><br>Use the scroll bar to choose the type you want and select an option for that type.<br>Next, select the way (statistic or graph) to show the report. |

| | |
|---|---|
| |  |
| **Select devices** | **Model Name** – All of the model names will be displayed in this field. Select the one you want. The default is “All”. All of the model names will be seen on the bottom of this page.<br>**Modem Version** – The default is “All”. However, some models do not have modem version, choose “No DSL” instead.<br>**Severity** – Specify the severity of the selected device(s). |
| **Name** | The models displayed here depend on the conditions set in **Select devices.** |
| **Query** | After specifying the conditions (report type, device selection...), click **Query** to create a new report.<br>  <br>**Create a Report** – This button appears after the first report created. If required, Click to create more reports for reference.<br>**Report 1/ Report 2 ...** - Each tab represents different reports created. |

## 6.3 Provisioning

Provision functions allow users to set provision profiles for applying in numerous TR-069 CPEs instead of configuring settings for each CPE one by one.




Provisioning menu is available only for the role of **System Administrator**, **Group Administrator**, and **Administrator**.

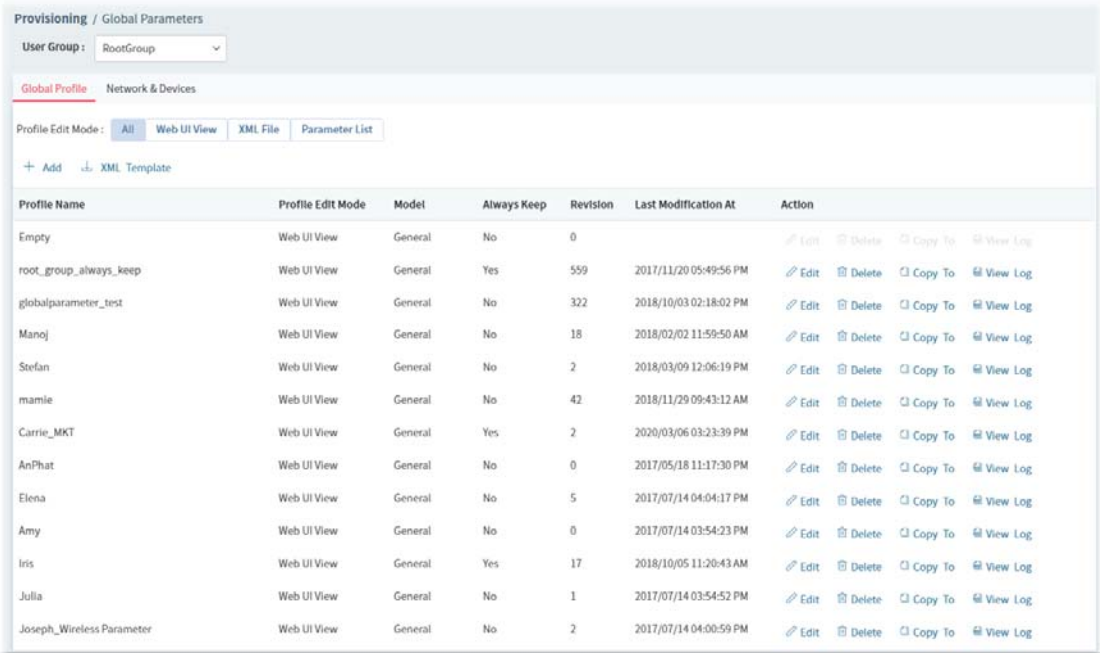
### 6.3.1 Global Parameters

Global Parameters configured in this page can be applied to all of the CPEs/APs at the same time by using VigorACS instead of configuring them one by one.

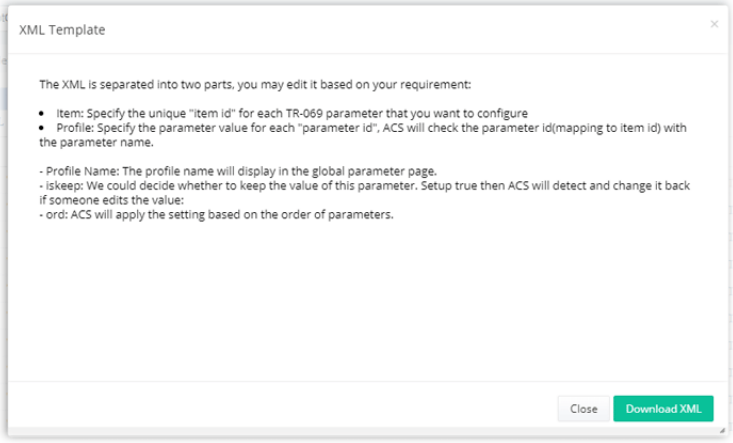
It is suitable and convenient when there are several CPE (with the same model) devices required to be configured with the same settings and values.

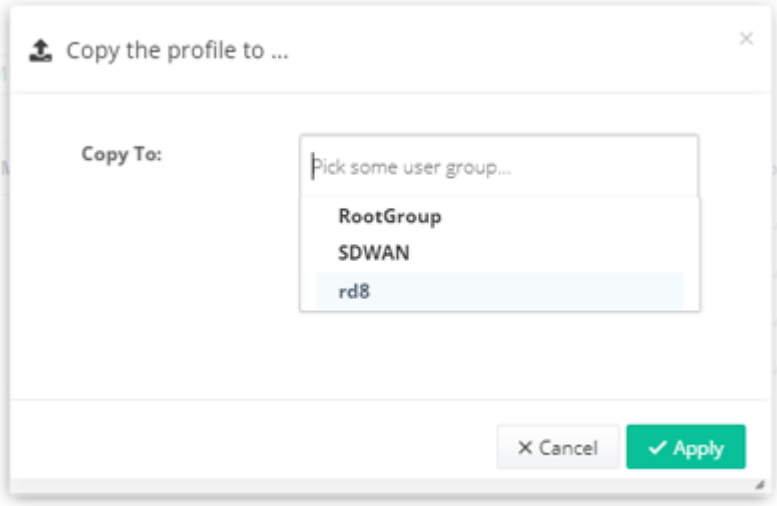
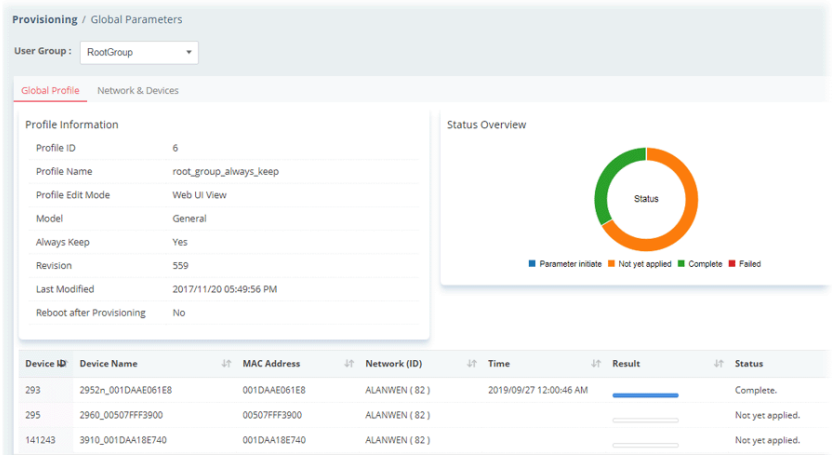
#### 6.3.1.1 Global Profile

This page listed the parameters profiles with profile names, model, and the status of the profile to be kept or not.

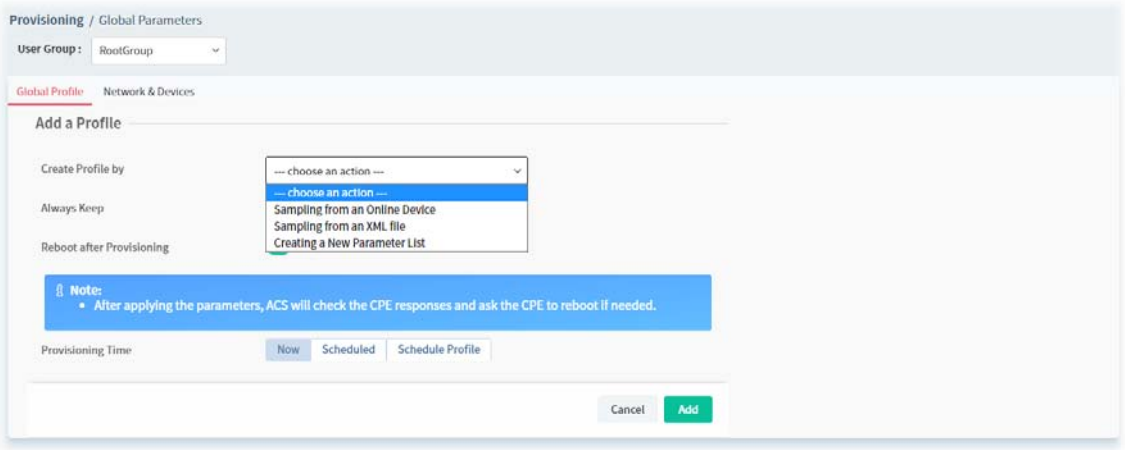



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Profile Edit Mode** | **All** - Displays all of the profiles.<br>**Web UI View** - Displays the profiles related to web UI view.<br>**XML File** - Displays the profiles with the file format of "XML".<br>**Parameter List** - Displays the profiles related to parameter settings for different CPEs. |
| **+Add** | Click to create a new provision profile. |
| **XML Template** | Click to store current global parameter configuration as a file (*.xml).<br>  |
| **Profile Name** | Displays the name of the profile. |
| **Profile Edit Mode** | Displays the edit mode. |
| **Model** | Display the model name of the device. |
| **Always Keep** | **Yes** – Such profile is kept always.<br>**No** – Such profile is not kept always. |
| **Revision** | Displays the time for last modification. |
| **Last Modification At** | Displays the time and date of the last modification of the provision. |

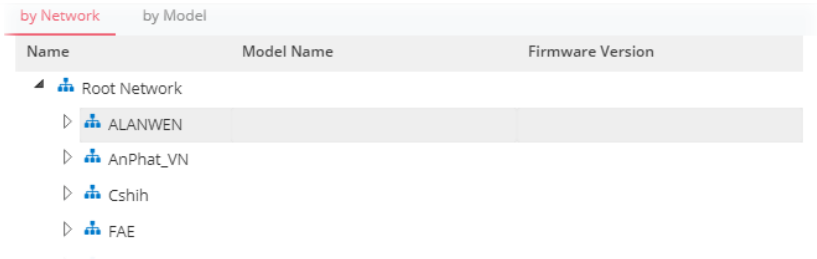
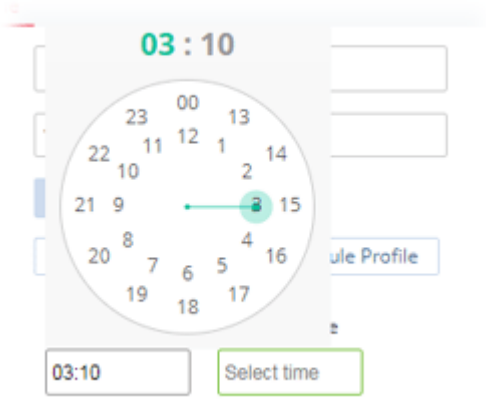
| Action | **Edit –** Click to configure settings for the selected profile.<br>**Delete –** Click to delete the profile.<br>**Copy To** – If the administrator wants to apply the provision to certain user group, such action shall be used.<br>  <br>**View Log –** Click to review detailed information for the selected profile.<br>  |
|---|---|

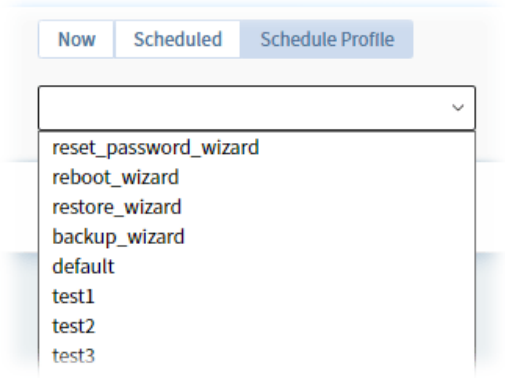
The following setting page appears when **+Add** is clicked.



These parameters are explained as follows:

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

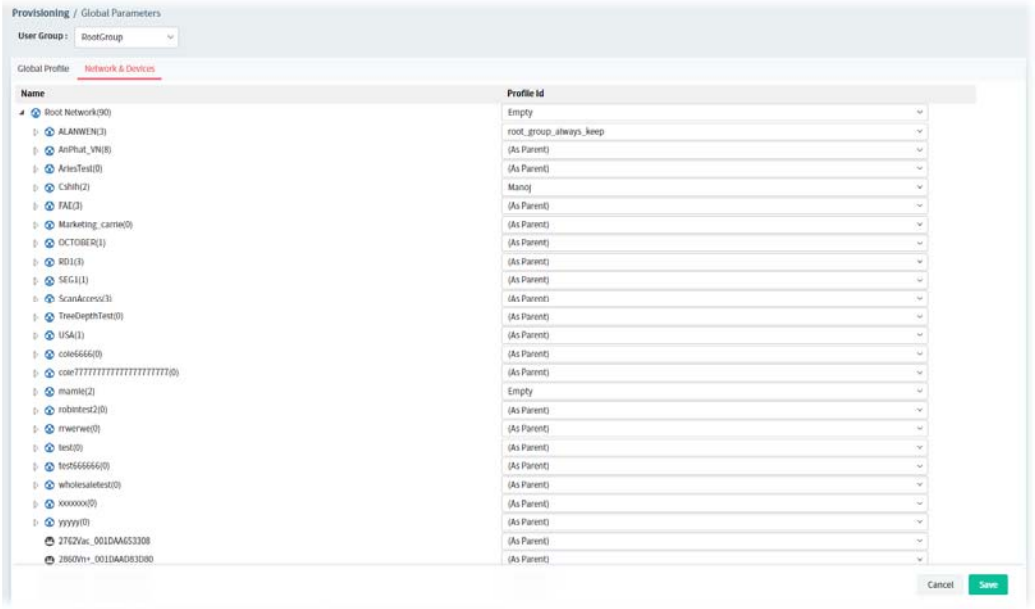
| | |
|---|---|
| **Create Profile by** | There are three methods (Sampling from an Online Device, Sampling from an XML file, Creating a New Parameter List) to create a profile. |
| For **Sampling from an Online Device**, | **Profile Name** - It is available when Sampling from an Online Device / Creating a New Parameter List is specified on "Create Profile by".<br>Enter a name for the parameter profile.<br>**Select Device** - Click **Edit** to choose the device.<br>  |
| For **Sampling from an XML file**, | **Select XML file** - Click Browse to choose a file. |
| For **Creating a New Parameter List**, | **Profile Name** - Enter a name to create a new profile. |
| **Always Keep** | Some ISPs do not wish CPE client changing the parameters of CPE device, therefore make the profile being kept is required. |
| **Reboot after Provisioning** | Enable it to reboot the CPE after the provisioning is applied by certain CPE. |
| **Provisioning Time** | Set a time interval for executing the backup work for networks and devices.<br>● **Now**<br>● **Scheduled**<br>● **Schedule Profile** |
| **Scheduled** | **Start Time / End Time –** Click **Select time** to display a clock. Set the hour and minutes by clicking the number on the clock.<br>  <br>**Specify Start Date** – Click to enable the time setting.<br>**Start date** – Click to pop up a calendar to choose a date as the starting date. |
| **Schedule Profile** | **Trigger Profile** - Choose a trigger profile from the drop down list. In which, VigorACS offers default schedule profile. |

| | |
|---|---|
| |  |
| **Cancel** | Discard current settings and restore the default settings. |
| **Add** | Save and create the new profile. |

### 6.3.1.2 Network & Devices

Specify certain profile (global parameter) to be applied in selected network, selected CPE/AP by clicking on the tree view structure.

Locate a CPE/AP by unfolding the tree view structure displayed under **Name**. Use the drop down list of **Profile Id** to specify the global parameter profile required for that CPE/AP.




These parameters are explained as follows:

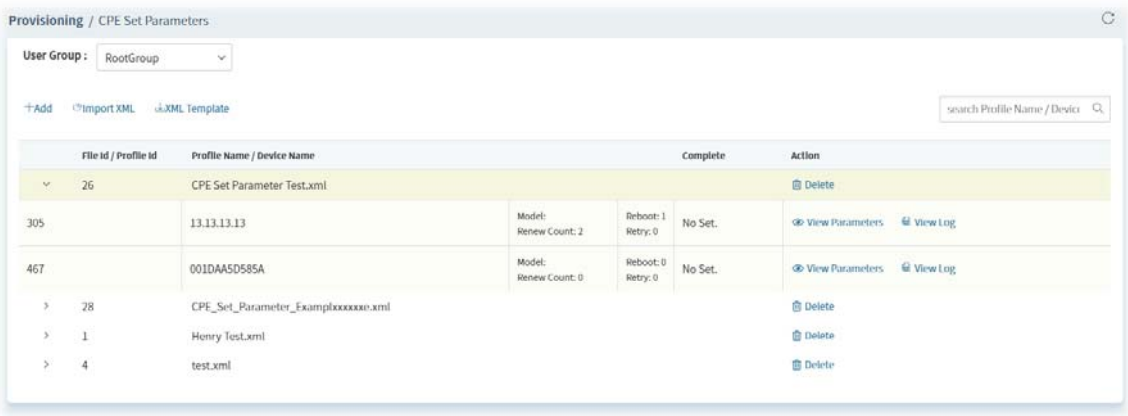
| Item | Description |
|---|---|
| **User Group** | Specify a user group. The devices under that group will be displayed on this page. |
| **Name** | Display the CPE/AP with the authority of the selected group. |
| **Profile Id** | Choose a profile (with global settings) defined in **Global Profiles** to be applied in such selected CPE/AP.<br>**(As Parent)**- Use the same setting as the previous layer. |
| **Cancel** | Discard current settings and restore the default settings. |
| **Save** | Save the settings. |

### 6.3.2 CPE Set Parameters

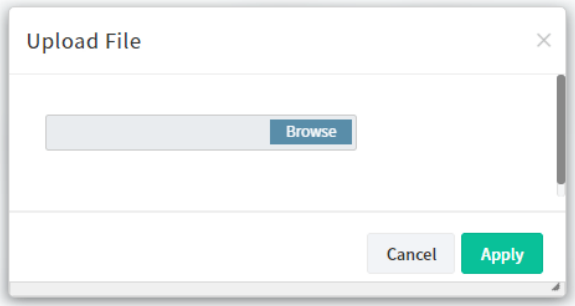
CPE parameters configured here can be applied to all of the CPEs at the same time by using VigorACS instead of configuring them one by one.

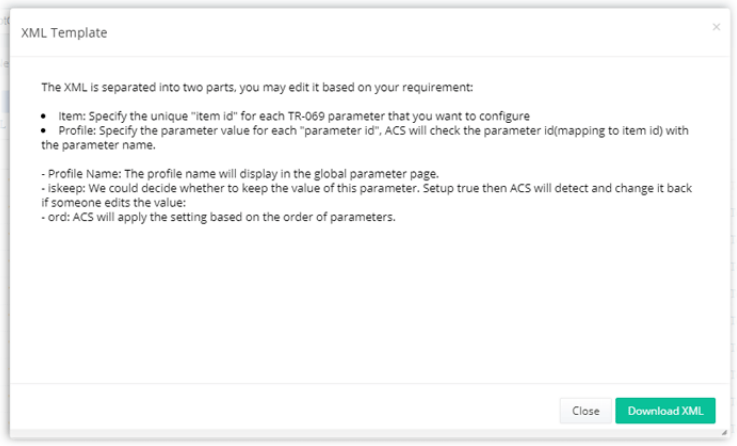
CPE Set Parameters is suitable and convenient when there are several CPE (with the same model) devices required to be configured with **different** settings and values.

However, Global Parameters is suitable and convenient when there are several CPE (with the same model) devices required to be configured with the **same** settings and values.

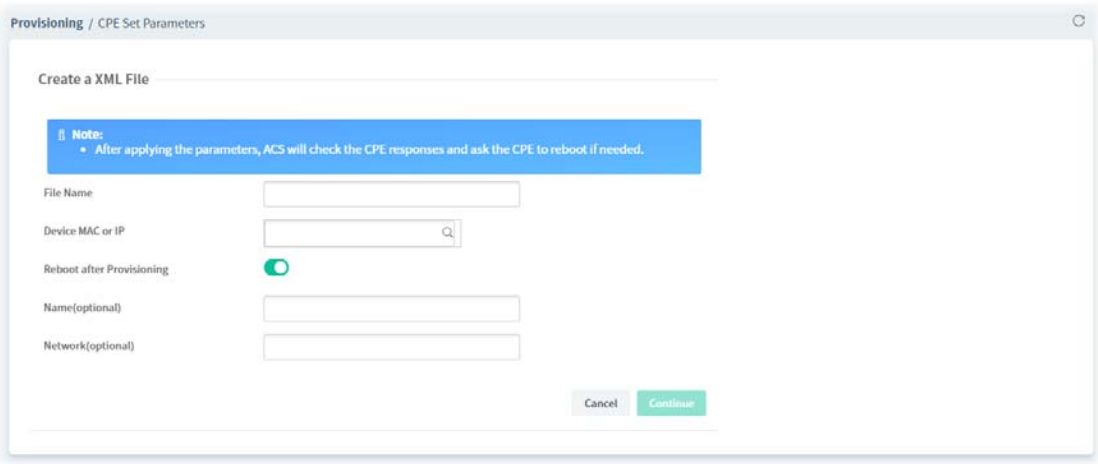



These parameters are explained as follows:

| Item | Description |
|---|---|
| **User Group** | Specify a user group. The devices under that group will be displayed on this page. |
| **+Add** | Click to create a file saved with the file format of XML. |
| **Import XML** | Click to upload a file to VigorACS 3 server.<br>  |
| **XML Template** | Click to store current global parameter configuration as a file (*.xml). |

| | |
|---|---|
| |  |
| **File Id / Profile Id** | Displays the number of parameter file or the ID number of the profile. |
| **Profile Name / Device Name** | Displays the profile name or the device name. |
| **Action** | **Delete –** Click to delete the profile.<br>**View Parameters –** Click to display parameter settings for the selected profile.<br>**View Log –** Click to review detailed information for the selected profile. |

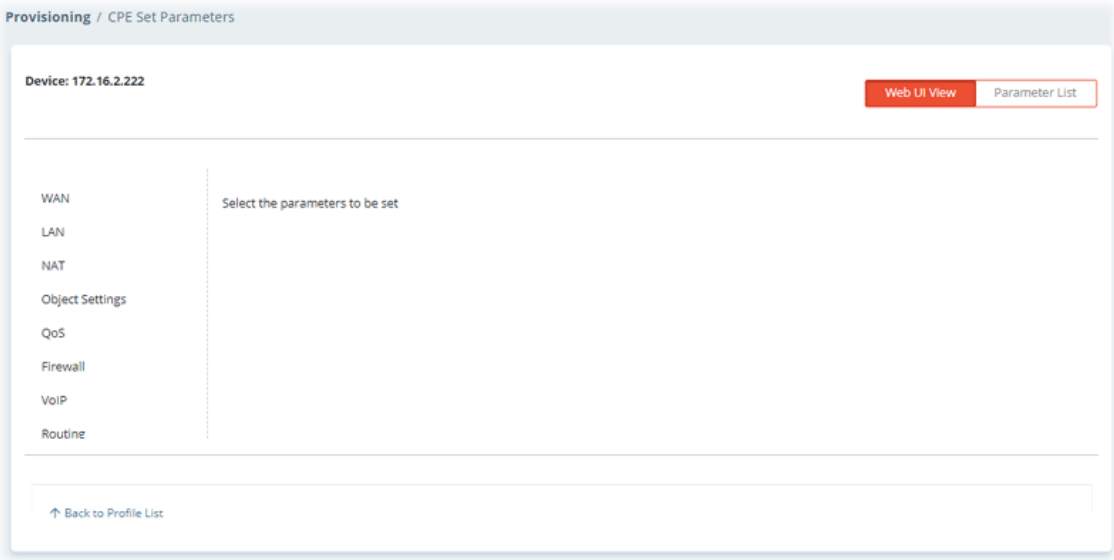
The following setting page appears when **+Add** is clicked.




These parameters are explained as follows:

| Item | Description |
|---|---|
| **File Name** | Enter a name for the parameter profile. |
| **Device MAC or IP** | Enter the MAC address or IP address.<br>After typing the address, VigorACS 3 will search from the database and locate the one you specify. |
| **Reboot after provisioning** | Enable it to reboot the CPE after the provisioning is applied by certain CPE. |
| **Cancel** | Discard current modification. |
| **Continue** | Click to get into next setting page. |

The following web page appears after clicking **Continue**.

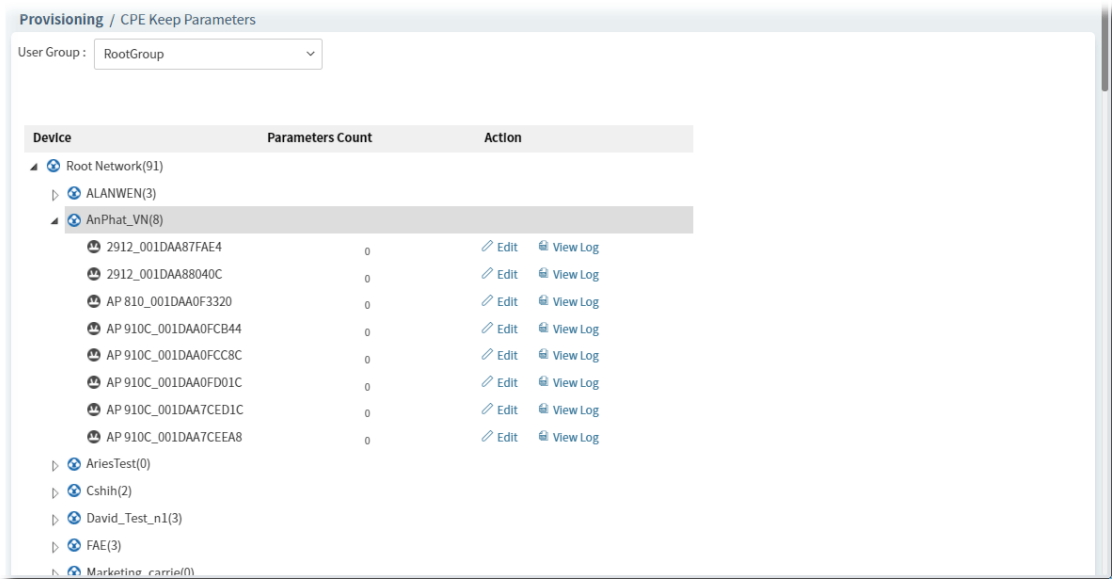



These parameters are explained as follows:

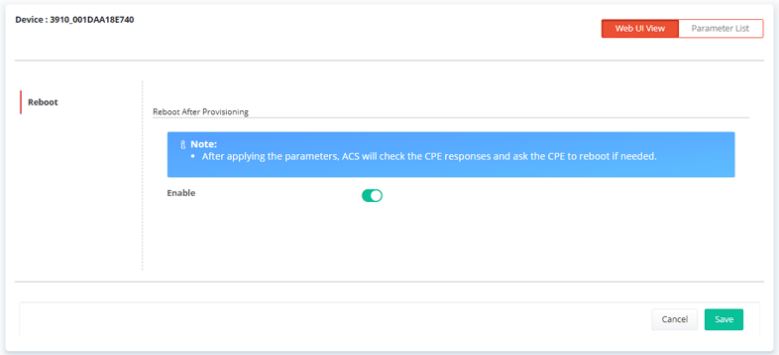
| Item | Description |
|---|---|
| **Device** | Display the name of the device which will be applied with the parameters configured in this page. |
| **Web UI View** | Parameters (including WAN, LAN, NAT, Object Settings, QoS, Firewall, System, Routing, Wireless, Applications and etc.) ready for each CPE provision profile can be seen and configured in this page.<br>The setting page for each parameter listed in left side will be displayed on the right side. Simply click the parameter to expand the sub-menu items. Then, choose a sub-menu item and click **+Add** to open setting page. After entering the required information for that menu item, click **Save**. |
| **Parameter List** | Display an overview of settings configured in Primary View. |
| **Back to Profile List** | Return to Profile List page. |

### 6.3.3 CPE Keep Parameters

This web page listed the parameters profiles with index number, profile names, and the status of the profile to be kept or not.




These parameters are explained as follows:

| Item | Description |
|---|---|
| **Edit** | Click to open the configuration page.<br>  |

### 6.3.4 Firmware Upgrade

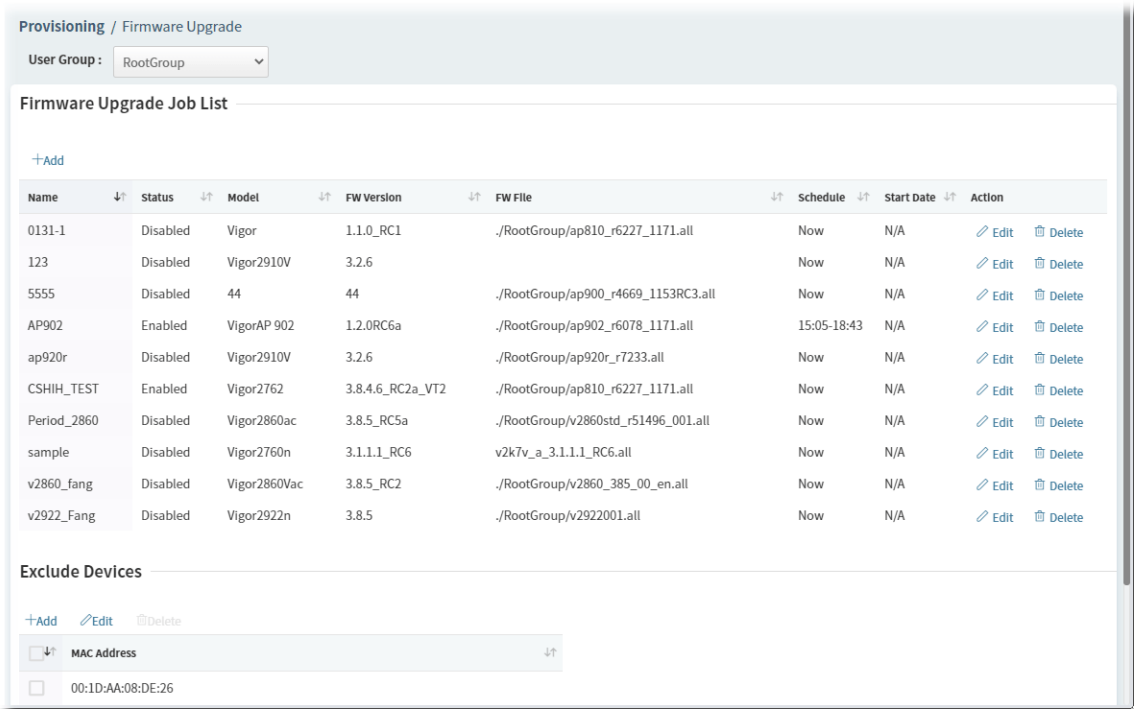
When VigorACS server receives information from CPE about firmware upgrade, it will check if the received model name, modem firmware version, and software version correspond to the information recorded in VigorACS server. If everything can match but software version not, VigorACS will judge that the remote CPE requiring firmware upgrade. Next, VigorACS server will execute firmware upgrade with the file listed in Job List automatically at specified time.

The firmware upgrade profile created in such page can be applied to the whole **network / group**.

For applying an upgrade provision profile to single and selected **devices** (but not applied to the whole network), please go to **Maintenance>>Firmware Upgrade** for more detailed information.

#### 6.3.4.1 Firmware Upgrade Job List

This web page allows you to **specify** required information for matching with the CPE device. The profiles created here will be regarded as a basis that VigorACS server uses to compare information coming from CPE router with the information stored in VigorACS server's database.

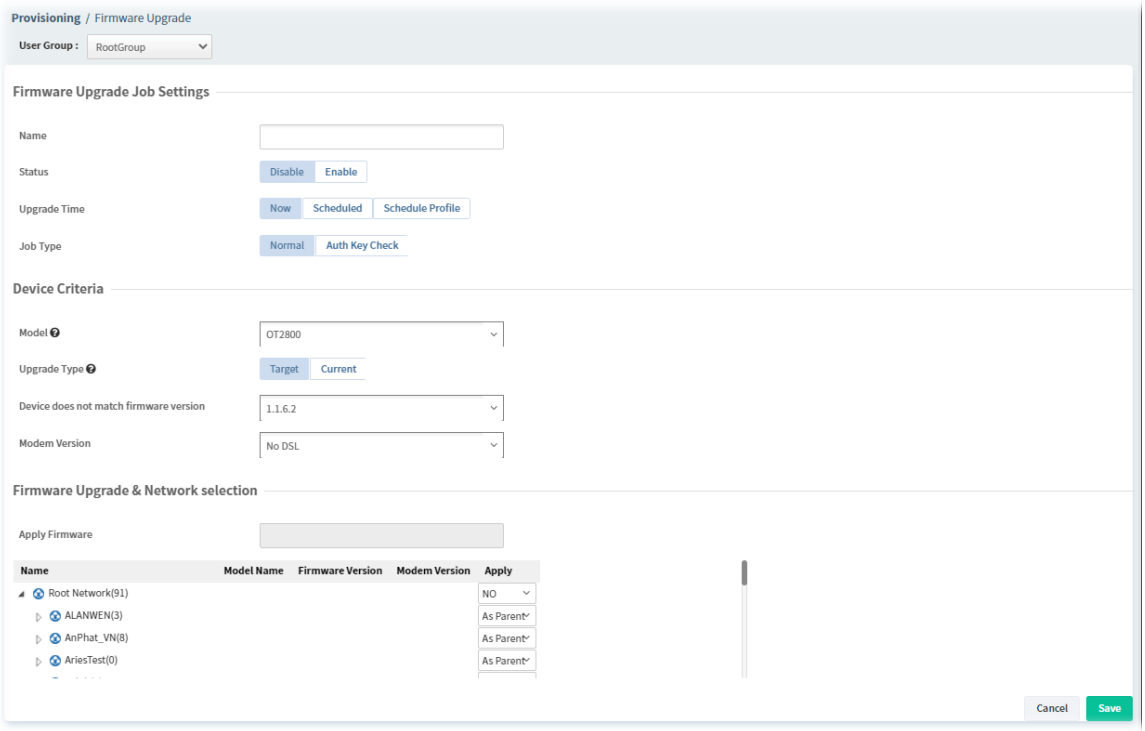



These parameters are explained as follows:

| Item | Description |
|---|---|
| **User Group** | Specify a user group. The job list under that group will be displayed on this page. |
| **Firmware Upgrade Job List** | |
| **+Add** | Click to create a new job profile. |
| **Edit** | Click to modify, change the selected profile. |
| **Delete** | Click to delete the selected profile. |

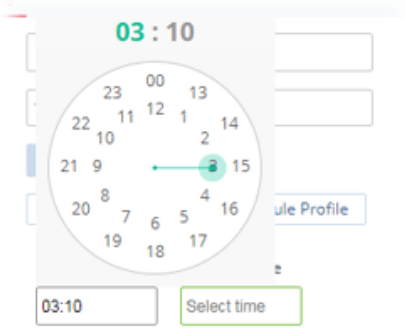
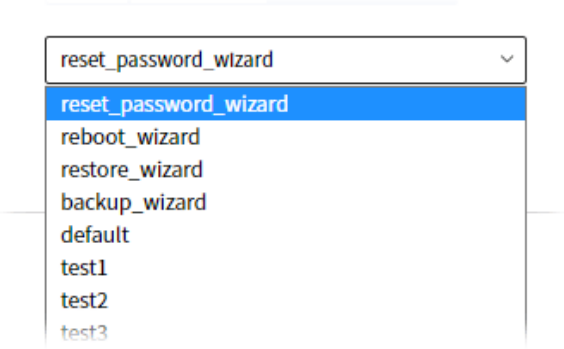
| Exclude Devices | |
|---|---|
| **+Add** | Specify the device that the firmware upgrade job configured and displayed on the job list will not perform for it.<br>Click to display an entry box. Enter the MAC address of the device. |
| **Edit** | Click to modify the MAC address of the devices one by one. |
| **Delete** | Click to delete the selected device. |
| **Check box** | Check the box to specify a device. Later, the selected one can be deleted if required. |
| **MAC Address** | Displays the MAC address of the device. |

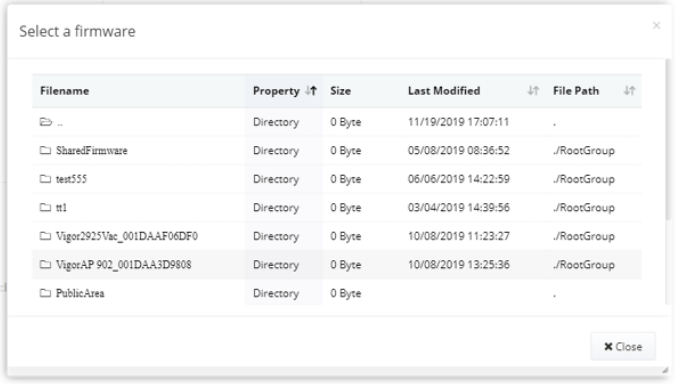
The following setting page appears when **+Add** is clicked.




These parameters are explained as follows:

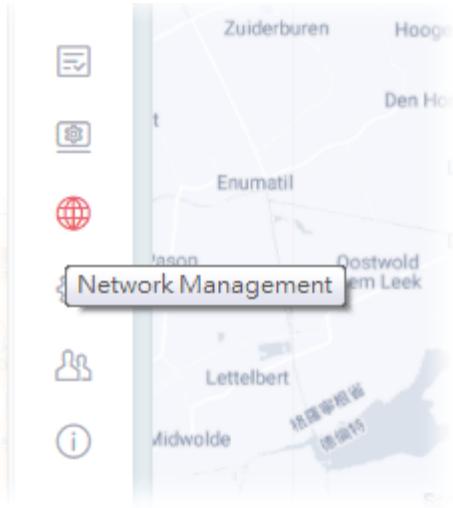
| Item | Description |
|---|---|
| **Firmware Upgrade Job Settings** | |
| **Name** | Enter a name of the job profile. |
| **Status** | **Disable** – Firmware upgrade is not allowed for such job profile.<br>**Enable** – Firmware upgrade is allowed for such job profile. |
| **Upgrade Time** | Set a time interval for executing the backup work for networks and devices.<br>● **Now**<br>● **Scheduled**<br>● **Schedule Profile** |
| **Scheduled** | **Start Time / End Time –** Click **Select time** to display a clock. Set the hour and minutes by clicking the number on the clock. |

| | |
|---|---|
| |  <br>**Specify Start Date** – Click to enable the time setting.<br>**Date** – Click to pop up a calendar to choose a date as the starting date. |
| **Schedule Profile** | **Trigger Profile –** Choosing a trigger profile from the drop down list. In which, VigorACS 3 offers default schedule profile.<br>  |
| **Job Type** | **Normal** – VigorACS 3 performs firmware upgrade without using any authentication key.<br>**Auth Key Check** – To avoid hacker's attack via Vigor device (router or AP), special authentication key is used for communication between Vigor device and VigorACS 3. That is, VigorACS 3 will verify all of the Vigor devices via authentication key issued by DrayTek to ensure the network security. |
| **Device Criteria** | |
| **Model** | Choose a model for firmware upgrade. |
| **Upgrade Type** | Select Target or Current.<br>**Target** - If the firmware version of the CPE is different from the one listed in "Device matches firmware version", the firmware upgrade job will be performed immediately.<br>• **Device does not match firmware version -** Displays current firmware version recorded on VigorACS server.<br>**Current** - If the firmware version of the CPE is the same as the one listed in "Device matches firmware version", the firmware upgrade job will be performed immediately.<br>• **Device matches firmware version -** Displays current firmware version recorded on VigorACS server. |
| **Modem Version** | Available versions from VigorACS 3 database will be displayed in this field.<br>Choose the correct modem version of the device, e.g., Annex A, Annex B and etc.<br>Before performing firmware upgrade for the CPE, VigorACS 3 will check if the received model name, modem firmware version, and software version match with the information recorded in VigorACS 3 server or not. If you type "*" in this filed, the modem version will not be regarded as a |

| | |
|---|---|
| | comparison condition in the process of firmware upgrade. It will be ignored. |
| **Firmware Upgrade & Network selection** | |
| **Apply Firmware** | Click to open a dialog.<br>  <br><br>Available versions from VigorACS 3 database will be displayed in this field.<br>Select the firmware version of the device and click **Close**. |
| **Apply** | **As Parent** - The setting for the selected network / device is the same as the top setting.<br>**NO** - No setting for the selected network / device.<br>**YES** - Use the firmware selected above for the network / device. |
| **Cancel** | Discard current settings and return to previous page. |
| **Save** | Save the current settings and exit the page. |

## 6.4 Network Management

Network Management allows you to modify the information for Networks and Devices.




It can

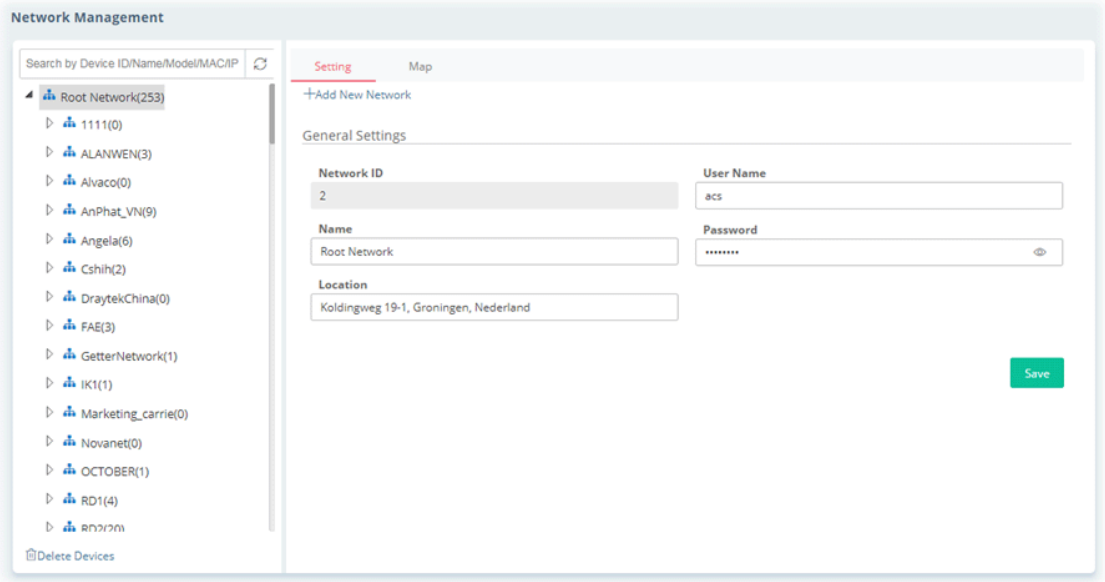
- Add new network (s) for new client which will be managed by VigorACS.
- Delete existed network if the client will not be managed by VigorACS.
- Modify the name and location of the network for management.

Network Management is available only for the role of **System Administrator**, **Group Administrator**, **Administrator** and **Standard** (limited in VigorACS cloud version).

## 6.4.1 Setting

To add, change or delete a network, please open **Network Management.**

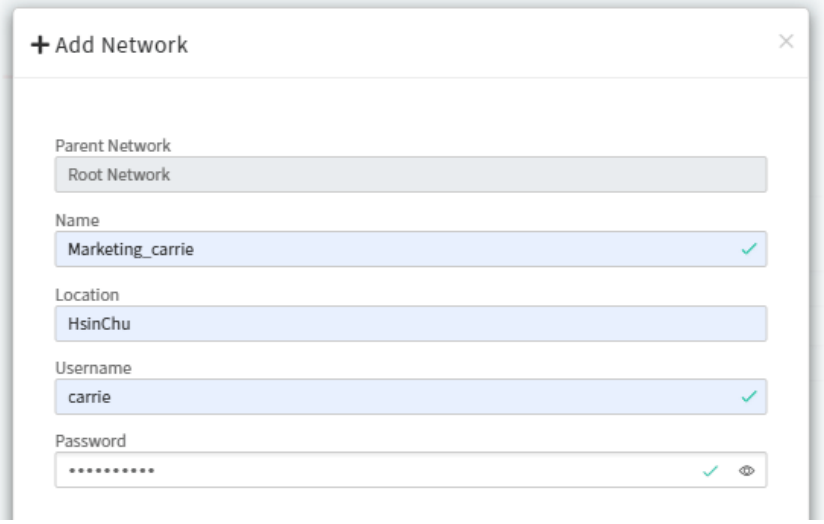
### 6.4.1.1 Settings for Root Network




These parameters are explained as follows:

| Item | Description |
|---|---|
| **Search device ID/name/model/MAC** | Enter the ID, name, model or MAC address of the device you want to locate. |
| **+Add New Network** | Click to add a new network. |
| **General Settings** | |
| **Network ID** | Display a number which is given by VigorACS randomly for the selected network. |
| **Name** | Display the name of the parent network. You can modify it if required. |
| **Location** | Type the location (e.g., HsinChu, New York) for such network. |
| **User Name** | Display the name of the selected network. Change it if required. |
| **Password** | Display the password of the selected network. Change it if required. |
| **Save** | Click to save the change. |

The following setting page appears when **+Add New Network** is clicked.

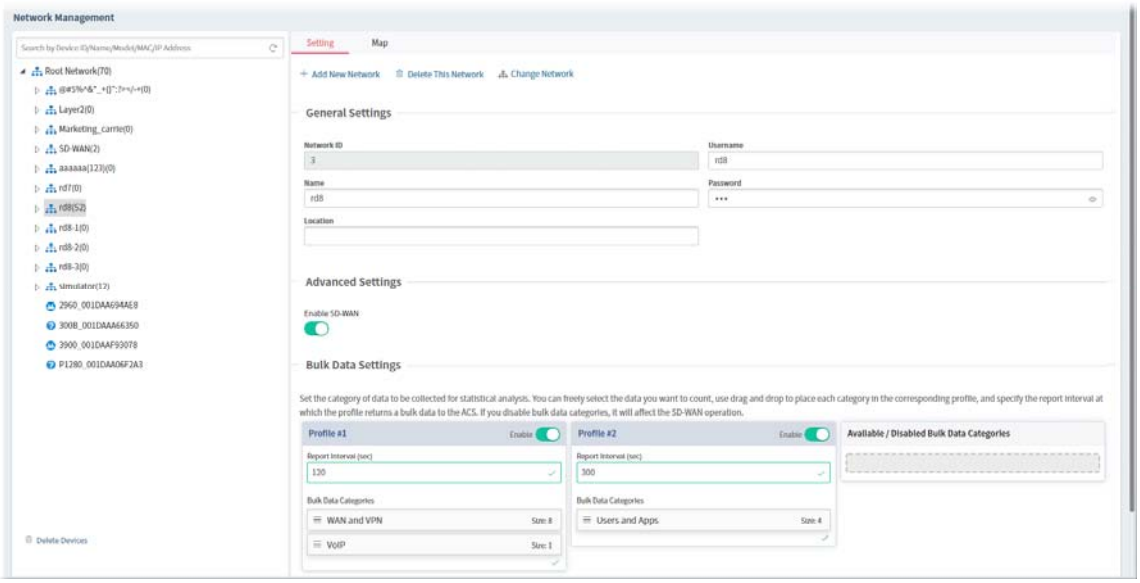



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Parent Network** | Display the name of the root network. New created network will be the sub-network of the parent network.<br>In default, **Root Network** is the parent network for any new created network. |
| **Name** | Enter a name for the new network. |
| **Location** | Enter the location for the new network. Later, you can locate such network on the web page of **Network Management>>Map.** |
| **Username** | Enter a login name (e.g., Marketing_carrie) for the new network which will be used for communication between Vigor device and VigorACS. |
| **Password** | Enter a password (e.g., admin123) for such new network. If you are going to group several devices under such network, please open **System Maintenance>>TR-069** in the web configuration page of CPE. Then, type the user name and password defined in this page (e.g., in this case, they are *Marketing_carrie* and *admin123*) in the corresponding fields. |
| **Cancel** | Discard current modification. |
| **+Add** | Save the current settings and exit the page. |

### 6.4.1.2 Settings for Network Group

To add, change or delete a network group, please open **Network Management.**

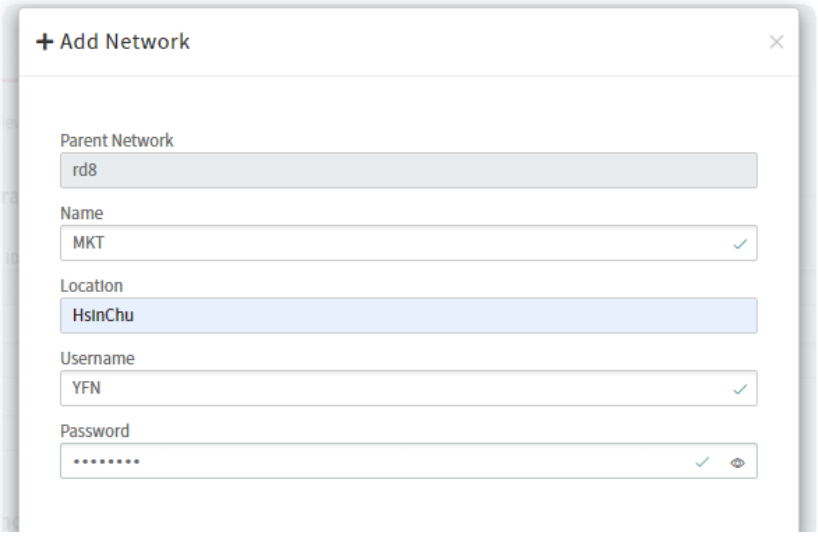



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Search device ID/name/model/MAC** | Enter the ID, name, model or MAC address of the device you want to locate. |
| **+Add New Network** | Click to add a new network. New created network will be the sub-network of current selected network. |
| **General Settings** | |
| **Network ID** | Display a number which is given by VigorACS randomly for the selected network. |
| **Name** | Display the name of the parent network. You can modify it if required. |
| **Location** | Type the location (e.g., HsinChu, New York) for this network. |
| **Username** | Display the name of the selected network (e.g., rd8, in this case). Change it if required. |
| **Password** | Display the password of the selected network. Change it if required. |
| **Advanced Settings** | |
| **Enable SD-WAN** | Enable or disable the SD-WAN function for current network group. |
| **Bulk Data Settings** | |
| **Profile #** | **Enable** - Click to enable or disable the profile.<br>If you disable bulk data categories, it will affect the SD-WAN operation. |
| **Report Interval (sec)** | Specify the report interval for the profile returning a bulk data to VigorACS server. |
| **Bulk Data Categories** | Set the category of data to be collected for statistical analysis. You can freely select the data you want to count.<br>Use drag and drop to place each category in the corresponding profile, and specify the report interval at which the profile returns a bulk data to VigorACS server. |
| **Available / Disabled** | At present, available categories include *VoIP, WAN and VPN, Users and Apps*. |

| | |
|---|---|
| **Bulk Data Categories** | Each category can be joined to the selected profile or be removed from the selected profile, by using drag-and-drop. |
| **Reset to default** | Click to reset to factory default settings of Bulk Data Settings.<br> |
| **Disable All** | After clicking the link, all data categories on Profile # will be removed. The data report for all CPEs under the selected network group will not be collected for VigorACS. Thus, no data, message can be collected by and displayed on the sub items based on SD-WAN feature under Monitoring menu.<br>However, the SD-WAN functions such as Hub and Spoke, Full Mesh VPN, Route Policy, and VoIP WAN for the selected network group are still active.<br> |
| **Save** | Click to save the change. |

The following setting page appears when **+Add New Network** is clicked.

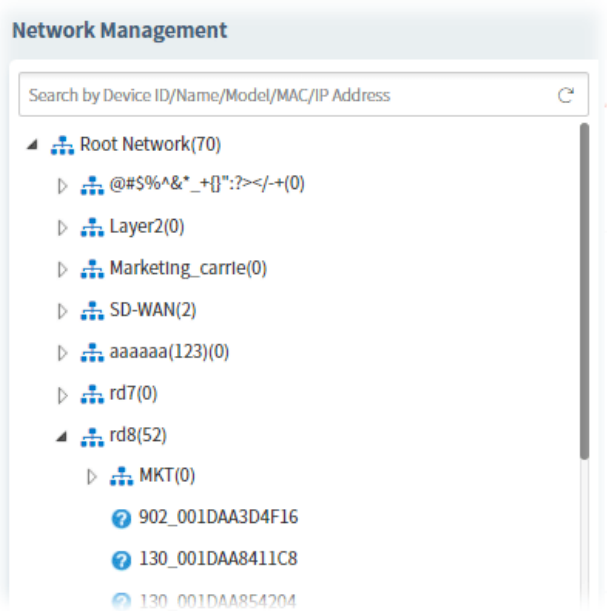



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Parent Network** | Display the name of the selected network group (e.g., rd8 in this case). New created network will be the sub-network of the parent network. |
| **Name** | Enter a name (e.g., MKT) for the new network. |
| **Location** | Enter the location for the new network. Later, you can locate such network on the web page of **Network Management>>Map.** |
| **Username** | Enter a login name (e.g., YFN) for the new network group which will be used for communication between Vigor device and VigorACS. |
| **Password** | Enter a password (e.g., admin123) for this new network group. |
| **Cancel** | Discard current modification. |

| | |
|---|---|
| **+Add** | Save the current settings and exit the page. |

After clicking +**Add**, the new network group (MKT) will be listed below its parent network, rd8.



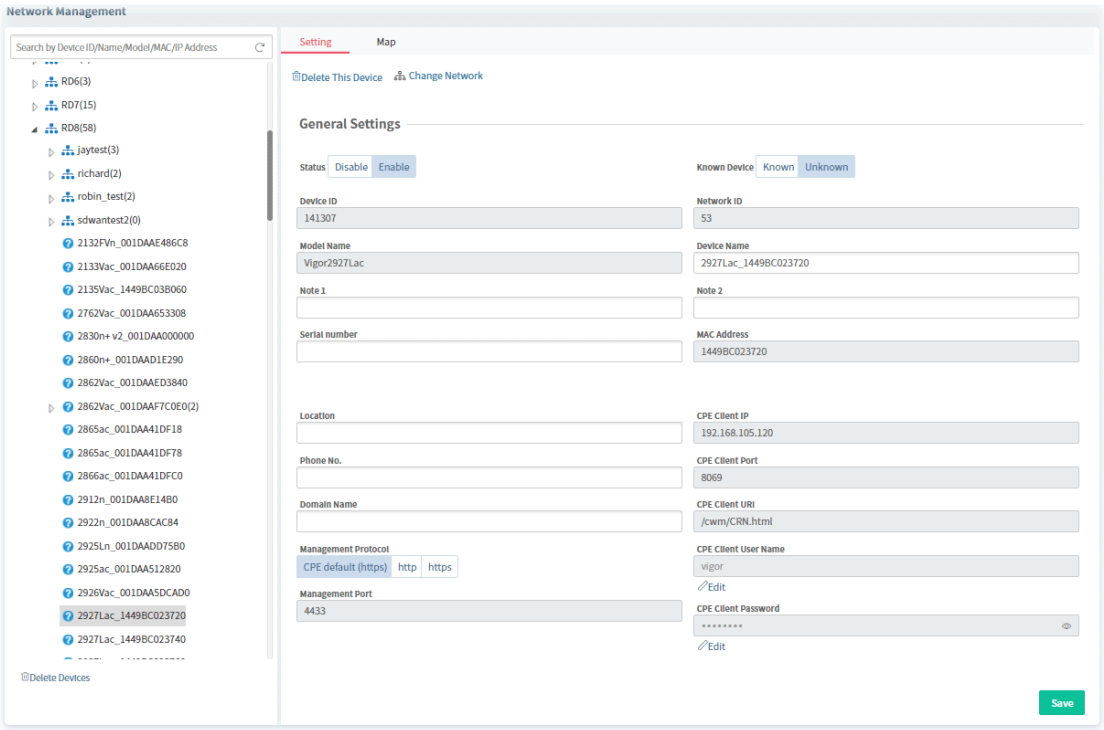

### 6.4.1.3 Settings for Device

The administrator can create several sub networks for different CPEs. Also, the administrator can change the network for the CPEs.

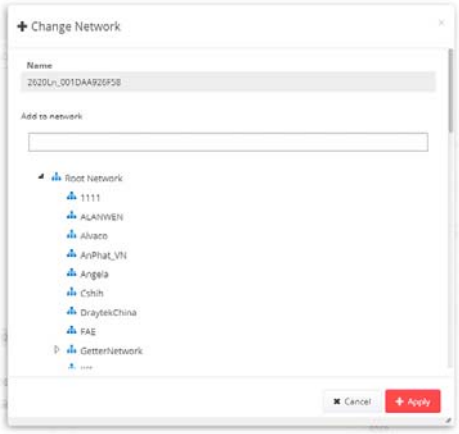
Open **Network Management.** This web page allows to:

- Modify the name of the device (CPE) for easy identification and management by VigorACS.
- Modify the location of the device (CPE) easily. It can be identified precisely while using GoogleMap to search it.
- Modify the user name/password of certain device (non-DrayTek CPE) to be managed by VigorACS.
- Enable or disable the management of the device (CPE) for VigorACS.
- Select certain protocol (e.g., TR-069) for the device (CPE) for management.

Choose and click any one of the CPE displayed on **Root Network** tree view to get the following web page.




These parameters are explained as follows:

| Item | Description |
|---|---|
| **Delete This Device** | Click to remove the selected CPE from current group. |
| **Change Network** | Click to change the network / group for the selected CPE.<br>  <br>Move the mouse cursor on the network you want and click **Apply.** |
| **General Settings** | |
| **Status** | **Disable** – The selected device will be hidden on the tree view.<br>**Enable** – The selected device can be displayed on the tree view. |
| **Known Device** | **Known** – The selected CPE is known() to VigorACS 3.<br>**Unknown** – If the selected CPE is new added device, it will be identified as Unknown (). |
| **Device ID / Network ID** | **Device ID** – Display the number of that device which is given by VigorACS 3 randomly.<br>**Network ID**- Display the ID number of the network that selected device is grouped under. |

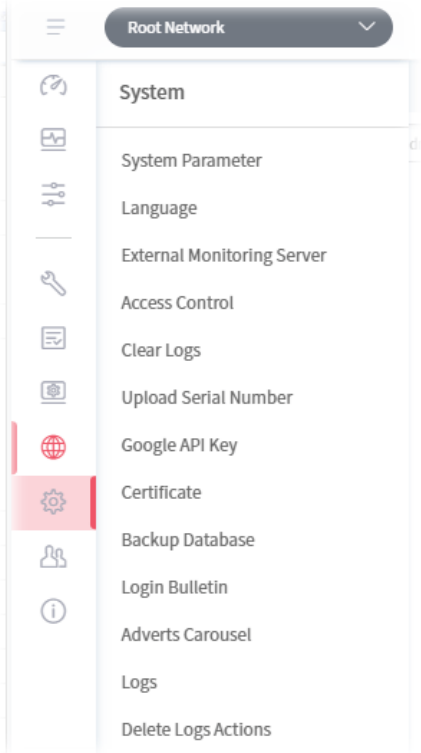
| | |
|---|---|
| **Model Name / Device Name** | **Model Name** – Display the model name of the selected device. Model name cannot be changed.<br>**Device Name** – Display the name of the device for identification. It can be changed if required. |
| **Note 1 / Note 2** | Note 1 – Display brief description for the selected device.<br>Note 2 – Display brief description for the network. |
| **Serial number / MAC Address** | **Serial number** – Enter a number for identification of the device.<br>**MAC Address** – Display the MAC address of the device. |
| **Location** | Display the position of the device. |
| **Phone No.** | It is optional and is used to offer additional information for reference. If required, Enter a phone number for such device. |
| **Domain Name** | Enter a domain name for a CPE. Later, simply click the domain name to access into the CPE. |
| **Management Port** | Enter a port number which will be used for accessing into web user interface of the CPE. |
| **Management Protocol** | Choose HTTPS or HTTP. |
| **CPE Client IP / Port / URI** | Display the IP address, port number and URI. |
| **CPE Client User Name / Password** | Display the username and password that VigorACS 3 can use to access into the CPE.<br>**Edit** - Click to change the username and password. |

### 6.4.2 Map

This page displays the location of the network / device on google map.

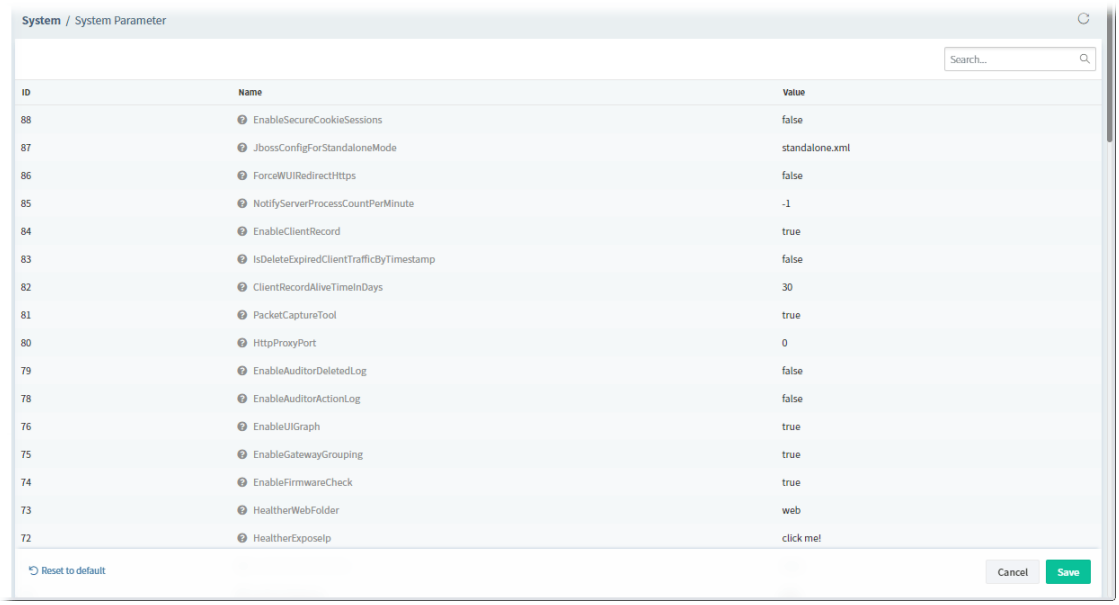
## 6.5 System

System menu varies according to the role (**System Administrator**, **Group Administrator**, **Administrator, Operator, View Only Operator, Auditor** and **Standard** (limited in VigorACS cloud version)) used for logging into VigorACS. Here we take System Administrator as an example.




### 6.5.1 System Parameter

Open **System** >> **System Parameter** to get the following web page:




These parameters are explained as follows:

| Item | Description |
| --- | --- |
| | **Reset to default**<br>Click the link to reset all of the system parameters with factory default values. |
| 1 | **ProvisionKeepParameter**<br>It can be set with true or false.<br>True – Enable the function of Keep Profile (profile or parameters in provision).<br>False - VigorACS will disable the function of **Keep Profile**. |
| 2 | **ProvisionWaitCount**<br>It means how many times VigorACS will compare the parameter values got from CPEs with the parameter values set within profiles. If these values are different from each other (from CPEs and from profiles), VigorACS will increase the count number by one. When the count increases to the value that users defined here, VigorACS will perform Keep Profile function. |
| 3 | **ProvisionFactoryResetEnable**<br>True – The function of keep profile will perform immediately for CPE without reaching the value of 'ProvisionWaitCount'. |
| 4 | **FirmwareUpgradeCount**<br>The value indicates how many CPEs can perform firmware upgrade at the same time. Set a proper value to prevent hardware from over loading and causing a crash. |
| 5 | **ProvisionDeviceAutoEnable**<br>False - The CPE would not be added in Homepage when a profile defines a CPE with different names but with the same serial number.<br>True – The CPE would be added in Homepage when a profile defines a CPE with different names but with the same serial number. |
| 6 | **ProvisionChangeDeviceNameEnable**<br>True - If it is set with true and a profile defines a CPE with different name but same MAC address, VigorACS would modify current CPE name with the pre-defined setting in profile. That is, if the device name in profile is not the same as the log recorded in VigorACS database, the system will modify the device name automatically. |
| 7 | **SettingProfileSpaceSetEnable**<br>True - Users can use space as character in parameter values. For example, users can use the space character as their password. |
| 8 | **ParameterListLongWaitCount**<br>It is a positive integer (ms). After upgrading firmware, VigorACS will scan and get all parameters to restore the parameter backup. The value determines how long the waiting time out is. Multiplying the value with 50 is the maximum waiting time in millisecond.<br>It will take effect after VigorACS restarts. Default is 1200. |
| 12 | **GetSetParameterCount**<br>When applying the provision onto CPEs, VigorACS tries to get or set parameter from or onto CPEs. This value determines how many parameter values can be obtained or set at the same time. For example, set the value as 20. That means there are 20 parameters which can be obtained at the same time.<br>Set this value properly to prevent CPEs from crashing or improve the efficiency. |
| 13 | **IsDownloadUsedHttps**<br>When a CPE connects to VigorACS with Https, users can enable this parameter (set with true) to let CPE download file from VigorACS via Https. |
| 14 | **ProvisionProfileFormat**<br>It can be set with 1, 2, 3 or 4. |

| | |
|---|---|
| | This value indicates the format of text configured profile.<br>If the value is set with 1, the format is defined as serial number, network_device name, isreboot, and [parameter1, parameter2,.. and so on].<br>If the value is set with 2 (as the default format), the format is defined as serial number, device name, isreboot, network, and [parameter1, parameter2,.. and so on].<br>If the value is set with 3, the format is defined as serial number, network_device name, isreboot, address and [parameter1, parameter2,.. and so on].<br>If the value is set with 4, the format is defined as serial number, network_device name, isreboot, network, address and [parameter1, parameter2,.. and so on]. |
| **15** | **IsRebootAfterDownload**<br>True- After downloading and upgrading the firmware, reboot the CPE.<br>False - Users must reboot the CPE manually. |
| **16** | **KeepProfileUpdateRule**<br>It can be set with is 1, 2 or 3.<br>The value 1 means after uploading profile, keep original Keep Profile settings and add extra parameter settings (if the profile contains more parameter settings).<br>The value 2 means after uploading profile, delete original Keep Profile setting if the device name changed.<br>The value 3 means after uploading profile, delete original Keep Profile settings every time. |
| **17** | **IsSetGlobalParameter**<br>False - Disable global parameter configuration function. When it is disabled, even users set global parameters, these parameters won't be applied. |
| **19** | **IsTurnOffPeriodicInform**<br>True - If **PeriodicInform interval** (configured in 59. CPEPeriodicInformInterval) is too short, CPE may send too much information to VigorACS and cause the server crash. Set this value true only if the case happened (server crashed). The default interval setting shall be 900 seconds.<br>False - After adjusting the PeriodicInform (configured in 59. CPEPeriodicInformInterval) of CPEs, remember to set this value false. |
| **20** | **PollingDeviceCount**<br>The value determines the maximum number of CPEs to poll at one time. If this value is set too small (e.g., 500), it might cause server overload. However, if it is set too big (e.g., 600000), it could make CPE status refresh very slowly.<br>Note: After changing this parameter value, restart VigorACS to apply the change. |
| **21** | **DeviceAutoEnable**<br>True - If it is set true, after obtaining the information from CPE, the newly added device would be added in the tree view of Homepage.<br>False – When VigorACS receives information from new added device, it will not display the CPE on the tree view of Homepage until make configuration in SYSTEM MENU>>Network Management. |
| **22** | **PollingInterval**<br>Set the polling interval for VigorACS to examine CPE. The unit is milliseconds. Default is 900000. |
| **23** | **CPEWebUiPort**<br>Set a port number for VigorACS system accesses into CPE's WUI. |
| **26** | **VPNIPSecDefaultSecurity**<br>Set the default security method for establishing VPN based on IPsec. |

| | |
|---|---|
| **27** | **CheckDeviceStatusCount**<br>Determine how many times shall VigorACS system check the device before the device becomes offline. |
| **28** | **VPNChangeEnable**<br>True – If one of the WAN IP addresses changes on both ends of VPN, VigorACS will change the setting automatically to rebuild the VPN tunnel.<br>False – Default value. |
| **29** | **WANSeverity**<br>Set the severity (critical, major, minor, warning and normal) for WAN connection. |
| **30** | **VPNSeverity**<br>Set the severity (critical, major, minor, warning and normal) for VPN connection. |
| **32** | **EnableHttpChunkedMode**<br>True - Use chunked mode (chunked transfer encoding) for HTTP.<br>False – Default value. |
| **33** | **CPEWebUiProtocol**<br>Set HTTP (default) or HTTPs as the protocol for accessing CPE's web user interface. |
| **34** | **EnableValidateCodeCheck**<br>True – Enable the function of validating code check on the login page.<br>False – Disable the function. It is the default value. |
| **35** | **VPNIPSecDefaultMode**<br>Set the default mode for IPsec VPN connection.<br>Main<br>Aggressive |
| **36** | **StatisticsStep**<br>Set the time interval (default is 900) for data collection for RRD traffic. |
| **38** | **EnableWebServices**<br>True – The third party software can get/set VigorACS functions through web services.<br>False – Default value. |
| **41** | **HidePassword**<br>True – Hide the password value on provision page.<br>False – Default value. |
| **43** | **VPNEnablePingKeepAlive**<br>True – Enable the function of Enable PING to keep VPN alive for CPE while creating VPN by using the VPN wizard.<br>False – Default value. |
| **44** | **CPEDetectMode**<br>Set the CPE detection mode. 0 means TR069; 1 means ping. |
| **46** | **EnableRRD**<br>True – Enable the function of data collection (StatisticsStep) for RRD traffic. |
| **47** | **AutoDetectRouteName**<br>True – Get CPE's router name.<br>False – Default value. |
| **48** | **EnableBatchActivation** |

| | |
|---|---|
| | True – Enable the batch activation license to MyVigor portal server function.<br>False – Default value. |
| **49** | **DefaultSetDeviceKnown**<br>True – Set the new added CPE as a known device.<br>False – Default value. |
| **50** | **KeepProfileRebootByBOOTSTRAP**<br>True – VigorACS will ask the CPE to reboot if receiving CPE request including BOOTSTRAP.<br>False – Default value. |
| **51** | **DisableAlarmMailByACSReboot**<br>True – VigorACS will not send alarm message within 15 minutes after turning on VigorACS.<br>False – Default value. |
| **52** | **DeleteOldDeviceBySameIP**<br>True – If a new CPE with an IP address which is the same as an old device recorded on VigorACS database, VigorACS will delete the information for the old device.<br>False – Default value. |
| **54** | **DisablePolling**<br>True – Disable VigorAP to poll CPE. Restart VigorACS after finished the configuration.<br>False – Default value. |
| **55** | **DisableAlarmMailByClear**<br>True – Disable the function of sending alarm e-mail when alarm status is clear. It is the default setting.<br>False – VigorACS will send alarm e-mail when alarm status is clear. |
| **56** | **UseStunAddressForVpn**<br>True – Remote IP address will use the STUN IP address for VPN connection.<br>False –Default value. |
| **57** | **EnableChangeNetworkByNetworkUser**<br>True – Default value. When VigorACS finds that the username and password sent from the CPE changed, it will move the CPE to the network group with the same username and password.<br>False – Disable such function. |
| **58** | **FWUpgradeFailInterval**<br>If the firmware upgrade failed, the next firmware upgrade will execute after the time interval configured here. Default value is 86400 seconds. |
| **59** | **CPEPeriodicInformInterval**<br>CPE will send general information to VigorACS periodically. The default value is 900 seconds. If required, enter the time interval for the CPE to send general information to VigorACS. |
| **60** | **EnableForceSetCPEPeriodicInformInterval**<br>True **–**Default value. Enable the function of CPEPeriodicInformInterval.<br>False – Disable the function of CPEPeriodicInformInterval. |
| **61** | **TimeFormat**<br>Display the time format. 0 means 24-hour clock; 1 means 12-hour clock. |
| **62** | **EnableRecordActionLog**<br>True **–** Enable the function of record action log. It is the default value.<br>False – Disable the function of record action log. |

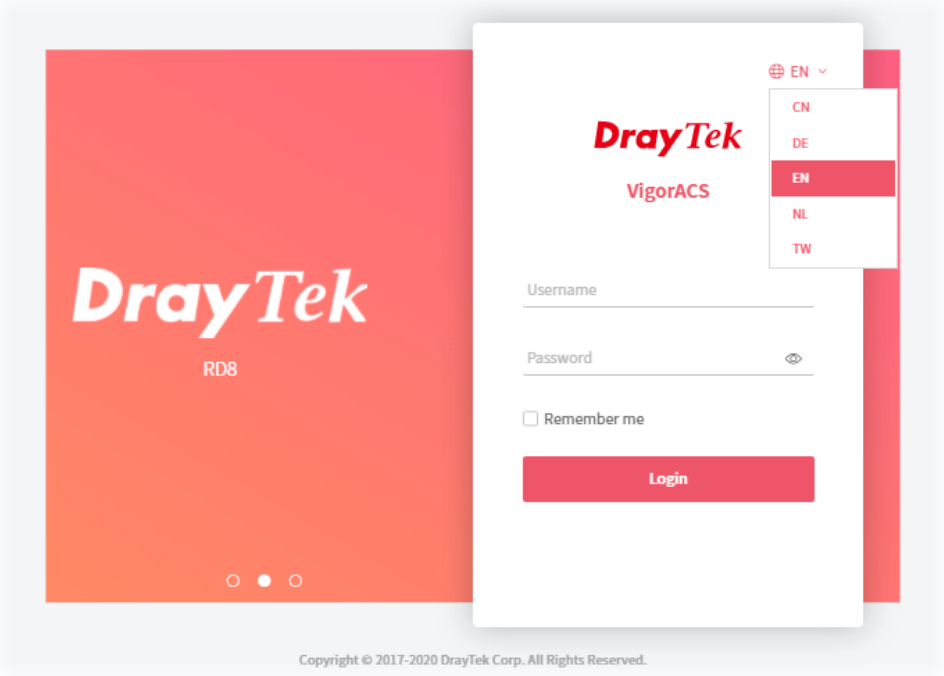
| | |
|---|---|
| **63** | **EnableBackupCheck**<br>True **–** VigorACS will check the parameter value of "InternetGatewayDevice.X_00507F_System.ConfigBak.ConfigChanged" and perform the configuration backup automatically if any change made for CPE's configuration.<br>False – Default value. |
| **64** | **CheckCPEValidByAuthKey**<br>True **–** VigorACS will check if the authentication key informed by CPE is valid or not.<br>False – Default value. |
| **65** | **New_DeleteOldDeviceBySameIP**<br>True **–** If a new CPE with an IP address which is the same as an old device recorded on VigorACS database, VigorACS will delete the information for the old device and write the configuration on the database related to the old CPE onto new CPE.<br>False – Default value. |
| **66** | **CheckCPEValidByNetworkUser**<br>True **–** Each network can be set with a group of username and password individually. All of the CPEs grouped under the network shall use such username and password for connecting to VigorACS. Such function let VigorACS check if the username and password sent from the CPE match with the settings on the network or not. If not, VigorACS will ignore the CPE request and change the group of the CPE into root network.<br>False – Default value. |
| **67** | **EnableAutoChangeWebPort**<br>True – Enable for changing web port automatically. It is the default setting.<br>False – Disable the function. |
| **68** | **DisableSaveInformLog**<br>True – Disable the function of Save Inform Log.<br>False – Default value. |
| **70** | **ShowTreeCount**<br>Set how many devices will be shown on the home device tree. Default value is 100. |
| **71** | **EnableSendCPENotify**<br>True - When the value of parameters for CPE is changed, a notification of 'IntenetGatewayDevice.X_00507F_Notify' will be sent to VigorACS. VigorACS will send the message to the specified user by e-mail, SMS or SNMP.<br>False - When the value of parameters for CPE is changed, a notification of 'IntenetGatewayDevice.X_00507F_Notify' will be sent to VigorACS. VigorACS will not send the message to the specified user. |
| **72** | **HealtherExposeIp**<br>It means the exposed IP in Monitoring Server message. Default is one of VigorACS host IP addresses. You can change to any IP without restarting ACS Server. |
| **73** | **HealtherWebFolder**<br>It means the folder name of VigorACS in JBoss deployment folder. It is used to create the URL for the device in Monitoring Server message.<br>Default folder name is set as "web". |
| **74** | **EnableFirmwareCheck**<br>True - VigorACS will compare current firmware of the device with the file version detected from DrayTek website. Therefore, while viewing the Firmware Version on the dashboard of the selected device, a pop-up window with current firmware version detected will appear if both firmware versions are different. |

| | |
|---|---|
| **75** | **EnableGatewayGrouping**<br>True – Enable the function of grouping VigorAP devices by using gateway addresses and displaying AP devices behind the gateway routers.<br>False – Default value. |
| **76** | **EnableUIGraph**<br>True – Enable the function of displaying graph of web user interface. It is the default value.<br>False – Disable the function. |
| **78** | **EnableAuditorActionLog**<br>True – The auditor action will be recorded and displayed on SYSTEM MENU >> System >> Delete Logs Actions.<br>False – Default value. When the auditor deletes logs or protects identity information on clients, the action will NOT be recorded. |
| **79** | **EnableAuditorDeletedLog**<br>True – The selected logs will be moved to another table which can be read by auditors. While protecting client identity information, the protected value can be recovered for auditors.<br>False – Default value. The selected logs will be deleted from database permanently. While protecting client identity information, the protected value cannot be recovered for auditors. |
| **80** | **HttpProxyPort**<br>It can be set with 0 to 65535, or a port range (e.g. 10000-10005). If the value set to 0, the proxy port number will be automatically allocated. If you start the proxy server before change this value, you have to restart VigorACS Server to apply this change on the current proxy. If the proxy port is only one number large than 0, you can only create one proxy server for each time. |
| **81** | **PacketCaptureTool**<br>True – VigorACS will capture the packets automatically and the result will be specified from the drop down list of Capture Packets on the top-right of the screen.<br>False – Default value. |
| **82** | **ClientRecordAliveTimeInDays**<br>Set the number of days for reserving the record (about client traffic). When exceeding the day limit, VigorACS will delete the record.<br>Default value is 30(days). |
| **83** | **IsDeleteExpiredClientTrafficByTimestamp**<br>True – Enable the function of ClientRecordAliveTimeInDays.<br>False – Default setting. |
| **84** | **EnableClientRecord**<br>True – Default value. Enable the function of recording client traffic and displaying related information on NETWORK MENU >> Monitoring >>Clients. |
| **85** | **NotifyServerProcessCountPerMinute**<br>It can be set with -1, 100 to 100000. This parameter determines how many Emails, SMS, and health parameters notification items the notification server can process per minute.<br>-1 means unlimited. |
| **86** | **ForceWUIRedirectHttps**<br>True - Force ACS WUI to HTTPS only. If you encounter login failed error after changing this parameter, please clear the browser's cache then try again. If the EnableSecureCookieSessions parameter is set to "true", this parameter will be automatically enabled and disallow set to false**.** |

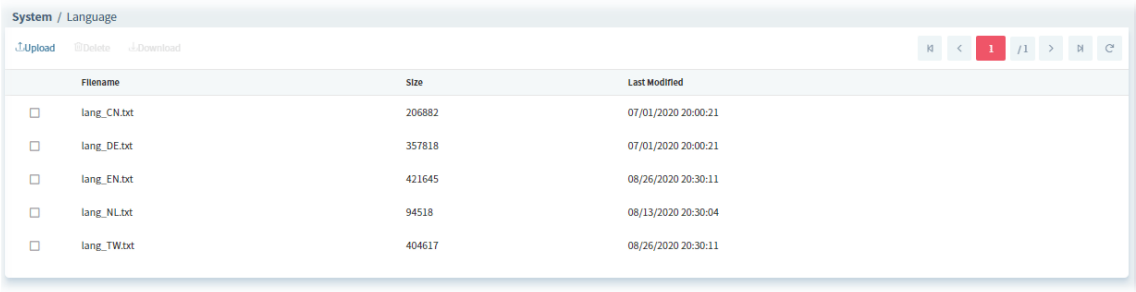
| | |
|---|---|
| **87** | **JbossConfigForStandaloneMode**<br>The Default Configuration for standalone Mode is "standalone.xml" (default). The standalone-secure.xml will enhance the security protections of your ACS website with plugins that prevent hacking. |
| **88** | **EnableSecureCookieSessions**<br>True - Secure flag is to prevent cookies from being observed by unauthorized parties due to the transmission of a the cookie in clear text. If the value set to true, the ForceWUIRedirectHttps parameter will be automatically enabled and the cookie will only be sent in a secure manner (i.e. Https).<br>False - Default setting. |
| **Save** | Save the current settings. |

### 6.5.2 Language

VigorACS 3 can be displayed and operated with different language texts. Choose the language system from the top-right of the login page. Later, VigorACS will be shown with the language you want.




In general, lang_EN.txt is the default language for VigorACS 3. If necessary, you can download a text file with VigorACS 3 settings; translate/edit the file with the language you want; and upload the edited file onto VigorACS.



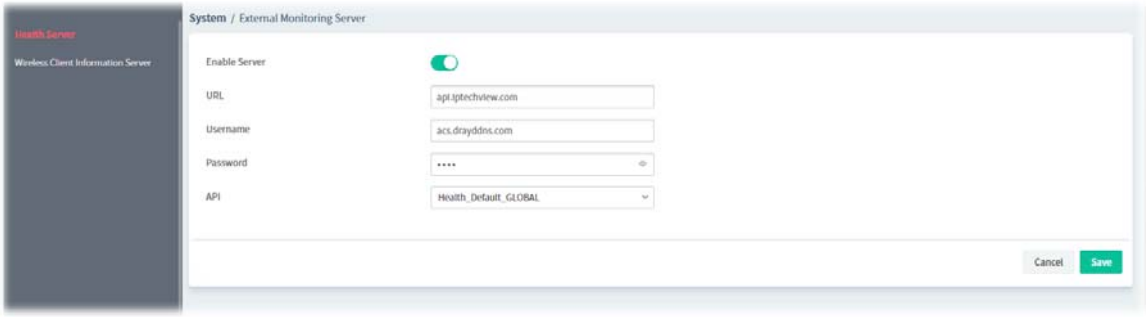

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Upload** | Click this button to upload a language file from your host to VigorACS. |
| **Delete** | Remove the selected language system. |
| **Download** | Click this button to download a txt file from VigorACS to your computer. User can edit such text file (containing all of the fields) if required. |

## 6.5.3 External Monitoring Server

### 6.5.3.1 Health Server

The health information for CPE can be transferred to the server of third party periodically.

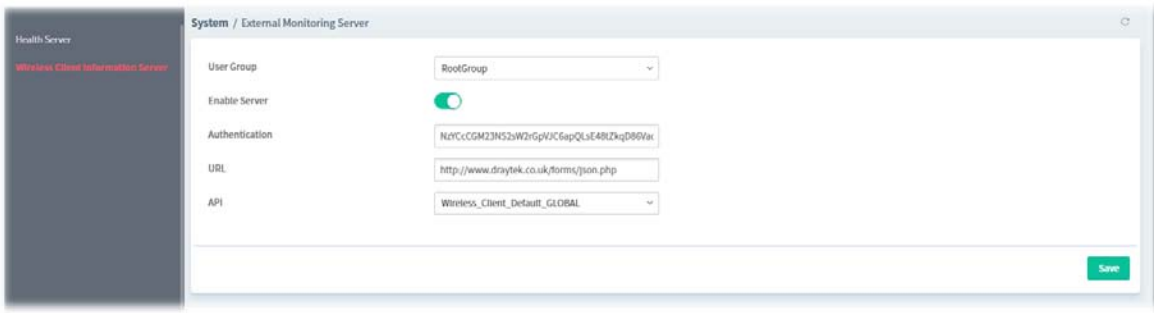



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Click the icon to enable / disable the server. |
| **URL** | Enter the URL or IP address of the third party's server. |
| **User Name** | Enter the user name for accessing into the third party's server. |
| **Password** | Enter the password for accessing into the third party's server. |
| **API** | Use the drop down menu to specify the third party's server. |
| **Cancel** | Discard current settings and restore the default settings. |
| **Save** | Save and activate the current settings. |

### 6.5.3.2 Wireless Client Information Server

The sever defined in such page is used to record information for wireless client information periodically.




These parameters are explained as follows:

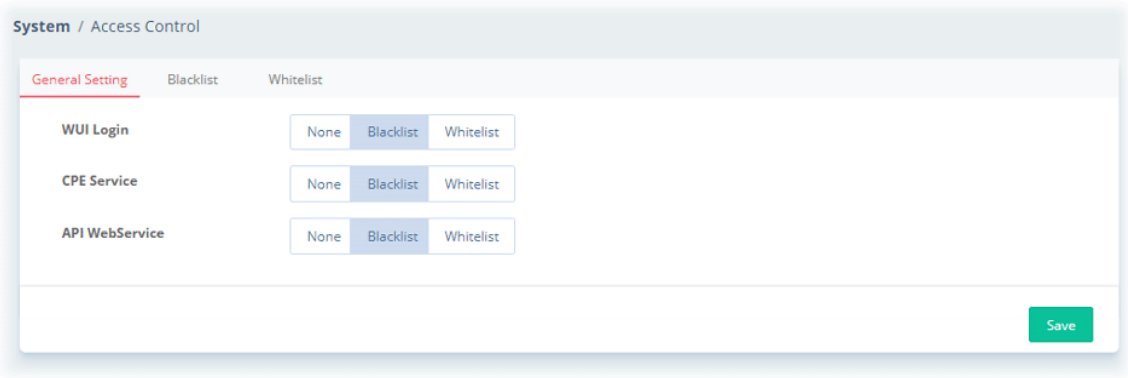
| Item | Description |
|---|---|
| **User Group** | Use the drop down list to specify a user group.<br>In which, RootGroup contains all of the users with the role of system administrator in default. |
| **Enable Server** | Click the icon to enable / disable the server. |
| **Authentication** | Enter a string for authentication. |
| **URL** | Enter the URL or IP address of the third party's server. |
| **API** | Use the drop down menu to specify the third party's server. |
| **Save** | Save and activate the current settings. |

## 6.5.4 Access Control

VigorACS can restrict network connection for clients by locking their IP address into a black or white list.

### 6.5.4.1 General Setting

Regardless of web login, CPE service or API web service, you can set a blacklist or whitelist to allow clients in the list to use or prohibit use.

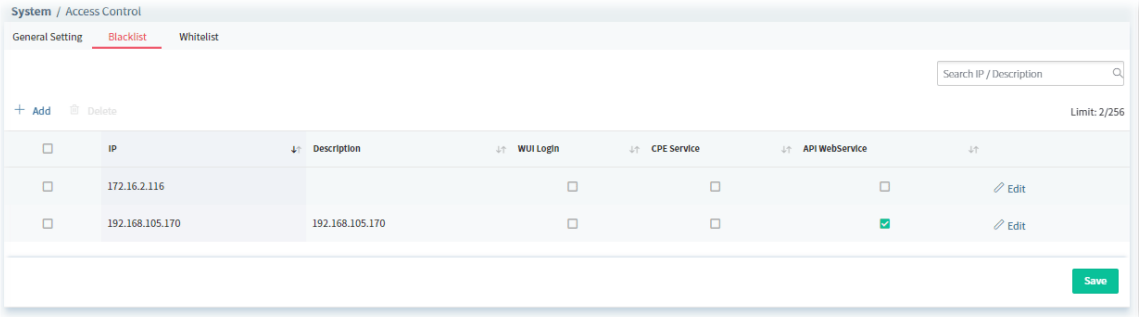



These parameters are explained as follows:

| Item | Description |
|---|---|
| **WUI Login** | **None** - It means no limitation for any client.<br>**Blacklist** - It means clients in the list are not allowed to login the WUI managed by VigorACS.<br>**Whitelist** - It means clients in the list are allowed to login the WUI managed by VigorACS. |
| **CPE Service** | **None** - It means no limitation for any client.<br>**Blacklist** - CPE clients in the list are not allowed to connect to VigorACS.<br>**Whitelist** - CPE clients in the list are allowed to connect to by VigorACS. |
| **API WebService** | **None** - It means no limitation for any client.<br>**Blacklist** - It means clients in the list are not allowed to use API web service managed by VigorACS.<br>**Whitelist** - It means clients in the list are allowed to use API web service managed by VigorACS. |

### 6.5.4.2 Blacklist

This page is used for creating blacklist profiles.

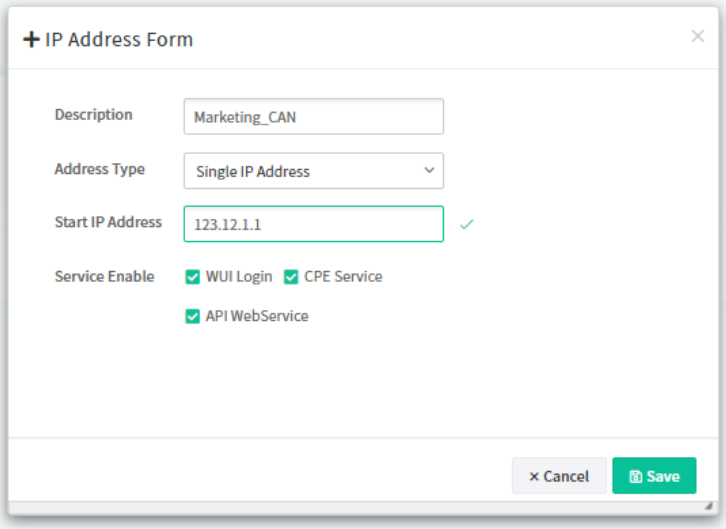



These parameters are explained as follows:

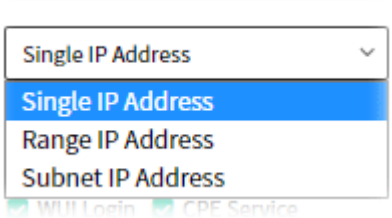
| Item | Description |
|---|---|

| | |
|---|---|
| **Search IP / Description** | Enter an IP or a brief description for searching the profile. |
| **+Add** | Click to create a new access control profile. |
| **Delete** | Click to delete the selected profile. |
| **Check box** | Check the box to specify a profile. Later, the selected one can be deleted if required. |
| **IP** | Displays the IP address, IP range, or subnet specified on the profile. |
| **Description** | Displays the comment of the profile. |
| **WUI Login, CPE Service, API WebService** | Displays the type(s) selected for the profile. |
| **Edit** | Click to modify, change the selected profile. |
| **Save** | Click to save the settings. |

The following setting page appears when **+Add** is clicked.



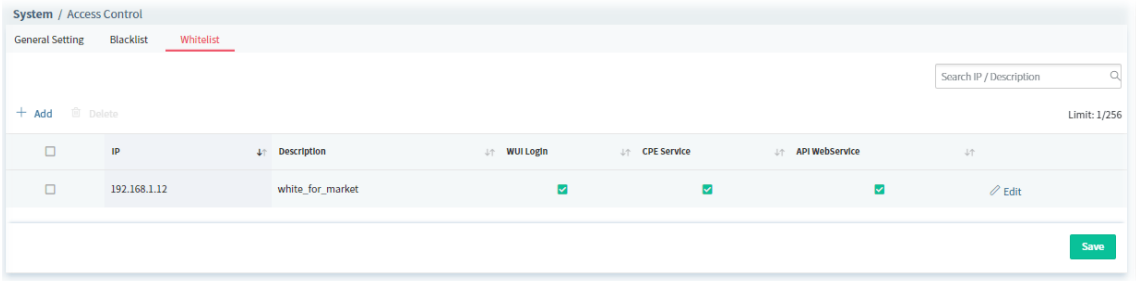

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Description** | Enter a name of the blacklist profile. |
| **Address Type** | Specify the address type to enter the IP address.<br>  <br><br>**Single IP Address** - Select it to specify one IP address.<br>**Range IP Address** - Specify a range of IP addresses.<br>**Subnet IP Address** - Specify a subnet IP address. |
| **Start IP Address** | It is available when Single IP Address or Range IP Address is selected.<br>Enter an IP address as a starting point. |

| | |
|---|---|
| **End IP Address** | It is available when Range IP Address is selected.<br>Enter an IP address as the ending point. |
| **Subnet Mask** | It is available when Subnet IP Address is selected.<br>Enter a mask address. |
| **Service Enable** | Select the service for this blacklist profile applying to. |
| **Cancel** | Discard current settings and restore the default settings. |
| **Save** | Click to save the settings. |

### 6.5.4.3 Whitelist

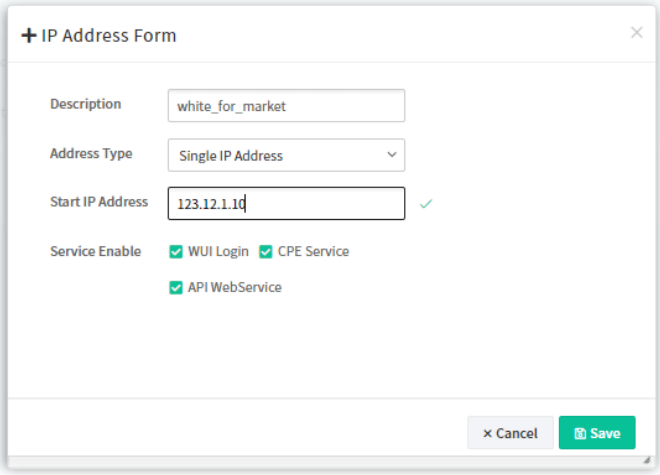
This page is used for creating whitelist profiles.



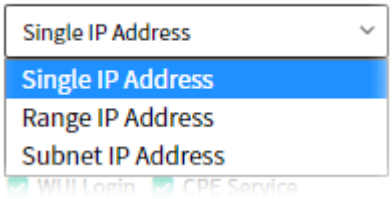

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Search IP / Description** | Enter an IP or a brief description for searching the profile. |
| **+Add** | Click to create a new access control profile. |
| **Delete** | Click to delete the selected profile. |
| **Check box** | Check the box to specify a profile. Later, the selected one can be deleted if required. |
| **IP** | Displays the IP address, IP range, or subnet specified on the profile. |
| **Description** | Displays the comment of the profile. |
| **WUI Login, CPE Service, API WebService** | Displays the type(s) selected for the profile. |
| **Edit** | Click to modify, change the selected profile. |
| **Save** | Click to save the settings. |

The following setting page appears when **+Add** is clicked.

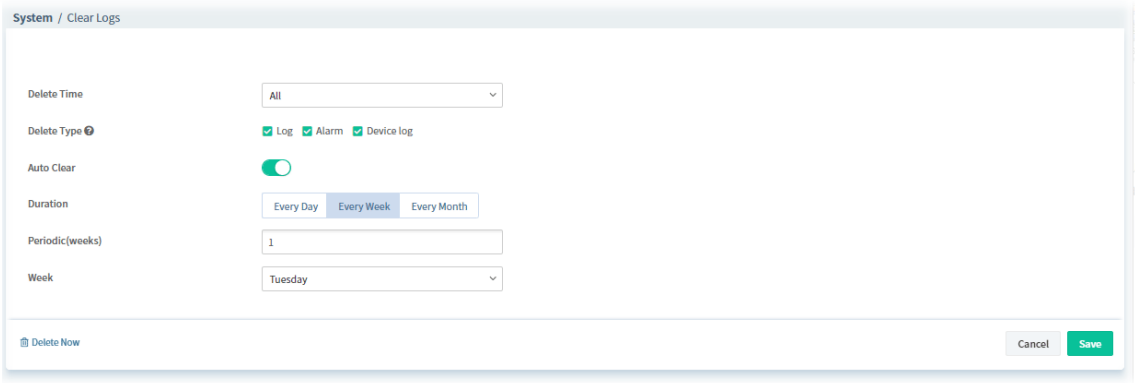



These parameters are explained as follows:

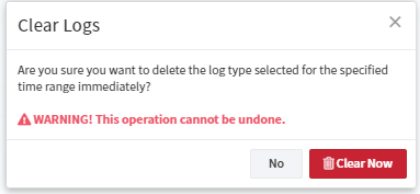
| Item | Description |
|---|---|
| **Description** | Enter a name of the whitelist profile. |
| **Address Type** | Specify the address type to enter the IP address.<br>  <br><br>**Single IP Address** - Select it to specify one IP address.<br>**Range IP Address** - Specify a range of IP addresses.<br>**Subnet IP Address** - Specify a subnet IP address. |
| **Start IP Address** | It is available when Single IP Address or Range IP Address is selected.<br>Enter an IP address as a starting point. |
| **End IP Address** | It is available when Range IP Address is selected.<br>Enter an IP address as the ending point. |
| **Subnet Mask** | It is available when Subnet IP Address is selected.<br>Enter a mask address. |
| **Service Enable** | Select the service for this blacklist profile applying to. |
| **Cancel** | Discard current settings and restore the default settings. |
| **Save** | Click to save the settings. |

### 6.5.5 Clear Logs

VigorACS will keep log until overload the capacity of hard disk. To avoid such trouble, use Clear Logs to delete the log periodically.



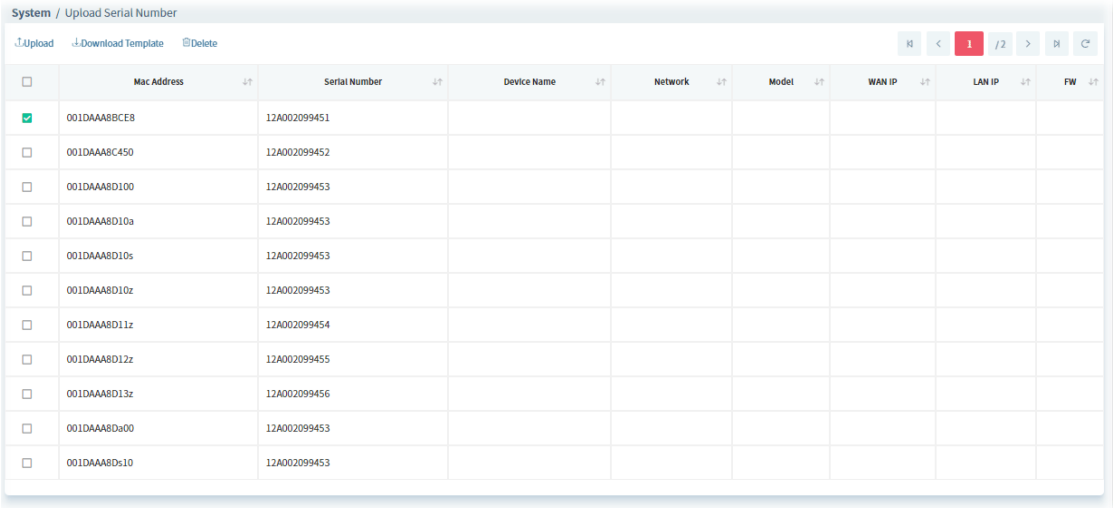

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Delete Time** | Use the drop down list to specify the timing to delete the log.<br>**All** – All of the logs recorded.<br>**Before 1, 3, 6 Month** – Log recorded before 1, 3 or 6 month ago.<br>**Before 1, 2 Years** – Log recorded before 1 or 2 years ago. |
| **Delete Type** | At present, there are three types (Log, Alarm, Device log) that corresponding log can be deleted through such feature. |
| **Auto Clear** | When it is enabled, VigorACS will periodically delete the logs based on the conditions configured below. |
| **Duration** | **Every Day** – VigorACS deletes the log every day.<br>**Every Week** – VigorACS deletes the log every week.<br>**Every Month** – VigorACS deleted the log every month. |
| **Periodic (days / weeks / months)** | Remove the log per days, per weeks or per months. For example, type “2” for Periodic (months). That means the system will clear the log every two months. |
| **Day** | It is available when **Every Month** is selected as the Duration. Specify the day within a month that VigorACS performs the log deletion. For example, choose 4 means VigoACS will delete the log on the fourth day of every month. |
| **Week** | It is available when **Every Week** is selected as the Duration. Specify Monday, Tuesday, Wednesday, Thursday, Friday, Saturday and Sunday. For example, choose Saturday means VigoACS will delete the log on Saturday every week. |
| **Delete Now** | Click to remove the log immediately. A pop-up window will appear for confirmation. If yes, click Clear Now; if not, click No to discard the action.<br>  |

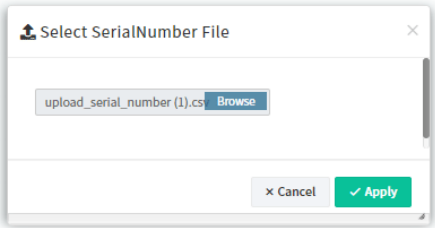
| | |
|---|---|
| **Cancel** | Discard current settings and restore the default settings. |
| **Save** | Save and activate the current settings. |

### 6.5.6 Upload Serial Number

The information for serial number on the rear side / bottom of the CPE or VigorAP can be uploaded onto VigorACS as a reference to be inspected by the administrator.

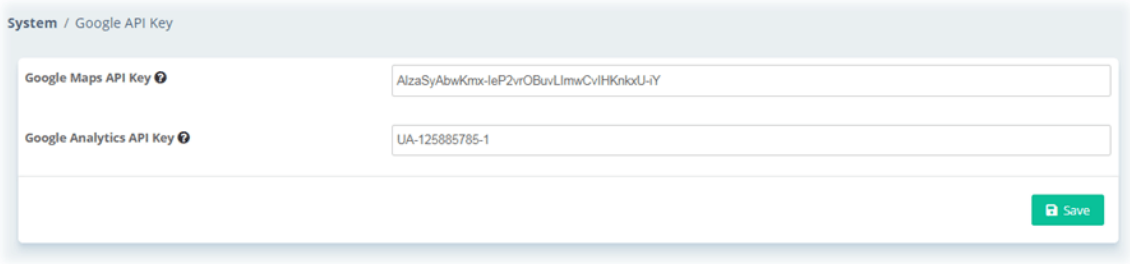



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Upload** | Click to upload a ".CSV" file (located on host) to VigorACS.<br>After comparing the MAC address listed on the file with the information of device(s) managed by VigorACS, the result (device name with serial number) will be shown on this page immediately.<br>  |
| **Download Template** | Click to download a template from the VigorACS server to your local host.<br>This template is convenient for the system administrator to enter the required information for lots of devices at one time. Later, the template can be uploaded to VigorACS server.<br>Please open the template with a software which can read and write ".CSV" file. Fill the MAC address and serial number (printed on the rear side / bottom) of a device. |
| **Delete** | Click to delete the selected entry. |
| **Check box** | Check the box to specify an entry. Later, the selected one can be deleted if required. |

### 6.5.7 Google API Key

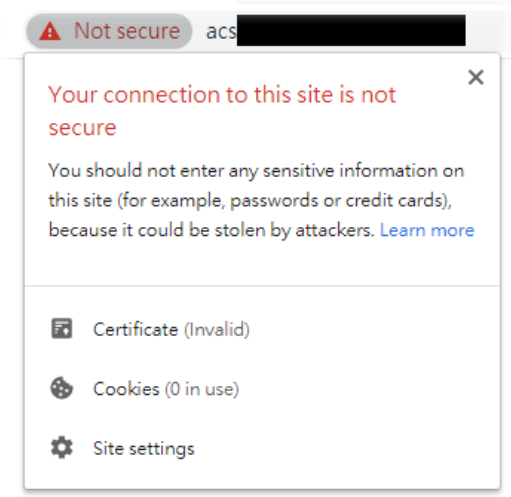
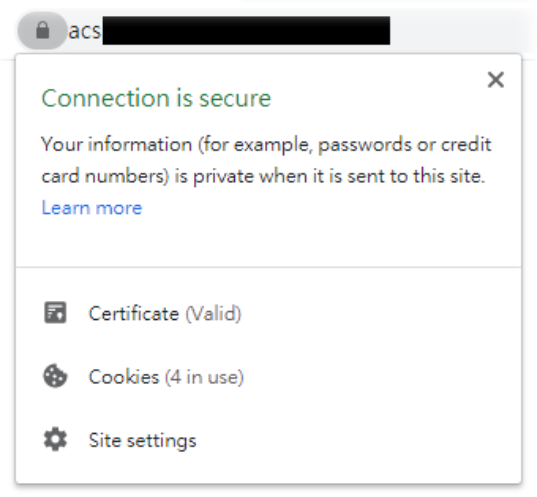
Before using the API of Google Map, it is necessary to apply and get a key from Google. Later, type the key in this page to activate the Google Map. After clicking **Save**, VigorACS will be granted to display the map on the dashboard.




### 6.5.8 Certificate

On website browsing, at present, the security offered by HTTP is less than HTTPS.

It is suggested to use HTTPS protocol for encrypting the connection between the browser and the web server for every website to prevent private information (such as account, password, personal data, credit number, and others) entered by users from leakage.

| Browsed by Google Chrome<br>A prompt for HTTPS web site encrypted with **INVALID** certificate | Browsed by Google Chrome<br>A prompt for HTTPS web site encrypted with **VALID** certificate |
|---|---|
|  |  |

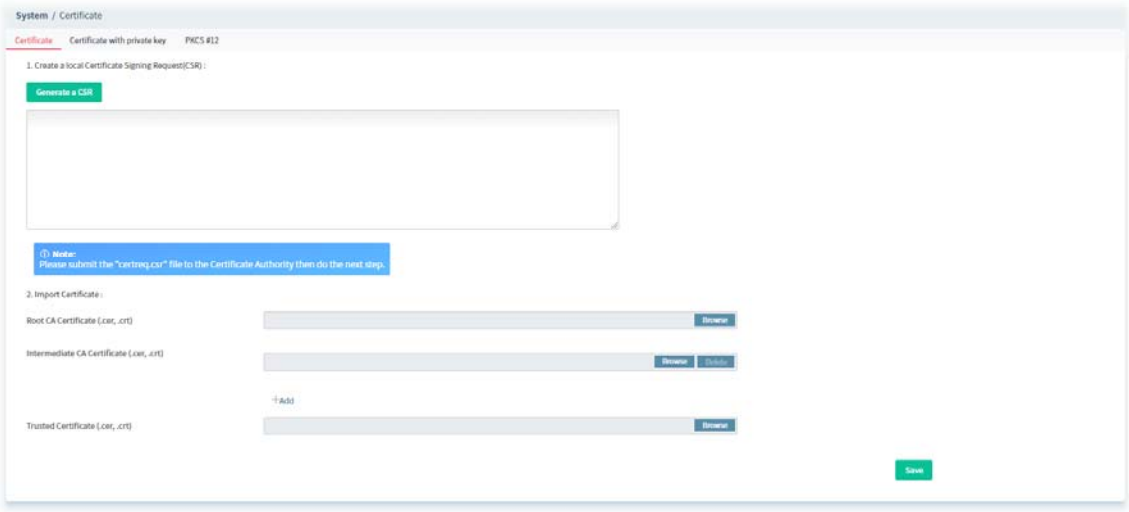




#### 6.5.8.1 Certificate

For using HTTPS, it is necessary to prepare a certificate issued by the third-party certificate authority.

This page can generate CSR (certificate signing request) file for certificate signing and import the HTTPS certificate file from third-party certificate authority to VigorACS server. Later, after restarting VigorACS server, Vigor system will apply such HTTPS certificate.

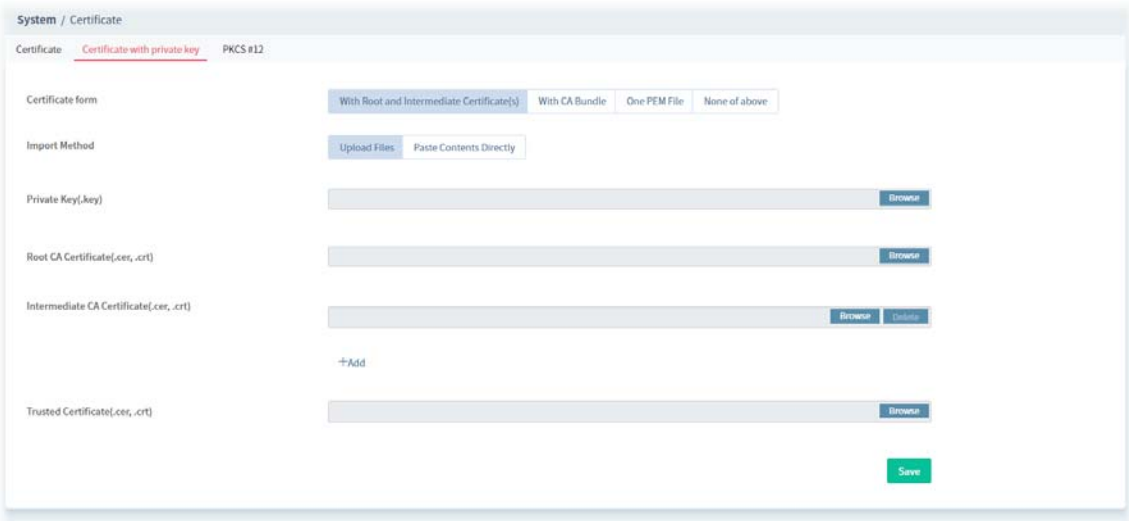



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Generate a CSR** | Click to generate a CSR certificate. |
| **Import Certificate** | Click the **Browse** button to specify a file to apply the HTTPS certificate.<br>● Root CA Certificate<br>● Intermediate CA Certificate<br>● Trusted Certificate |
| **Save** | Save current settings and uploading/pasting the certificate. |

### 6.5.8.2 Certificate with Private Key

Some of certificate authority (third-party) does not submit CSR file but generate a private key and sign a certificate (e.g., SSL for free, COMODO, and so on) to be applied by other web site. This page is used for uploading a certificate with private key from a certificate authority (third-party) to VigorACS server.



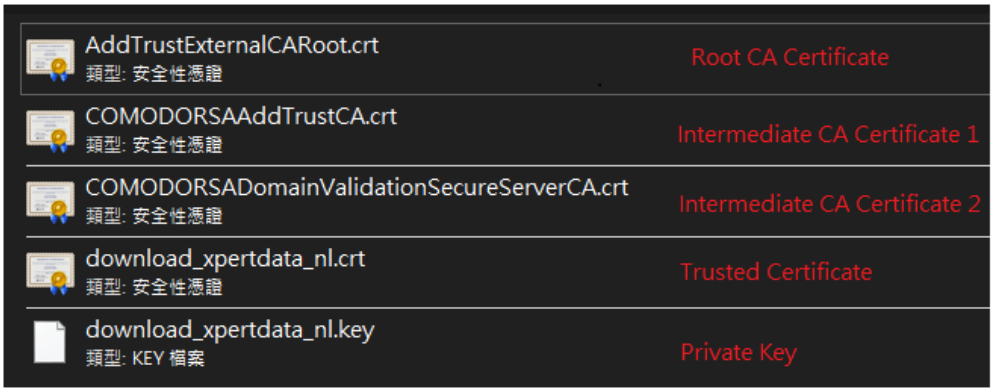

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Certificate form** | Confirm the file format of the certificate issued by the certificate authority and then select a file with corresponding file format for uploading or |

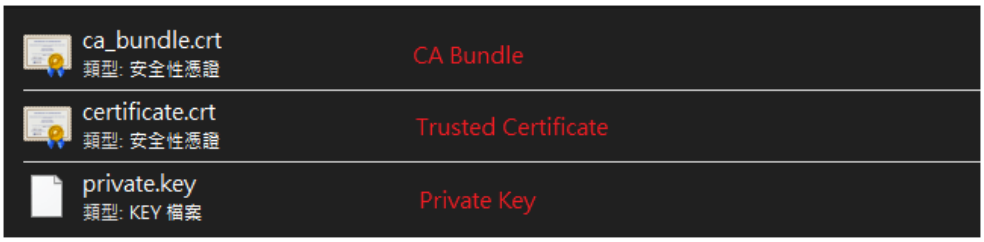
| | |
|---|---|
| | pasting on this page directly.<br>• **With Root and Intermediate Certificate(s)**<br>• **With CA Bundle**<br>• **One PEM File** – The certificate issued by the certificate authority contains only one PEM file.<br>• **None of above** - The certificate issued by the certificate authority contains only one certificate (CRT file) with a private key. |
| **Import Method** | **Upload Files** – The content of the certificate / key shall be obtained by uploading a file.<br>**Paste Contents Directly** – The content of the certificate / key shall be pasted from clipboard. |
| **Private Key (.key)** | Click the Browse button to select one key file or obtain the content of the key from the clipboard. |
| **Trusted Certificate (.cer, .crt)** | Click the Browse button to select one Trusted CA certificate or obtain the content of the certificate from the clipboard. |
| **When With Root and Intermediate Certificate(s) is selected** | |
| **Root CA Certificate (.cer, .crt)** | Click the Browse button to select one root CA certificate or obtain the content of the certificate from the clipboard. |
| **Intermediate CA Certificate (.cer, .crt)** | Enter the name of intermediate CA certificate or Click the Browse button to select one intermediate CA certificate or obtain the content of the certificate from the clipboard.<br>**Add** – If there is more than one intermediate CA certificate file, Click to import more. |
| **When With CA Bundle is selected** | |
| **CA Bundle (.cer, .crt)** | Click the Browse button to select one certificate or obtain the content of the certificate from the clipboard. |
| **When One PEM File is selected** | |
| **PEM File (.pem)** | Click the Browse button to select one PEM file. |
| **Save** | Save current settings and uploading/pasting the certificate. |

### Example

The following example shows the file formats of certificates issued by Comodo. It is suitable for “With Root and Intermediate Certificate(s)”.




The following example shows the file formats of certificates issued by SSL For Free. It is suitable for “With CA Bundle”.



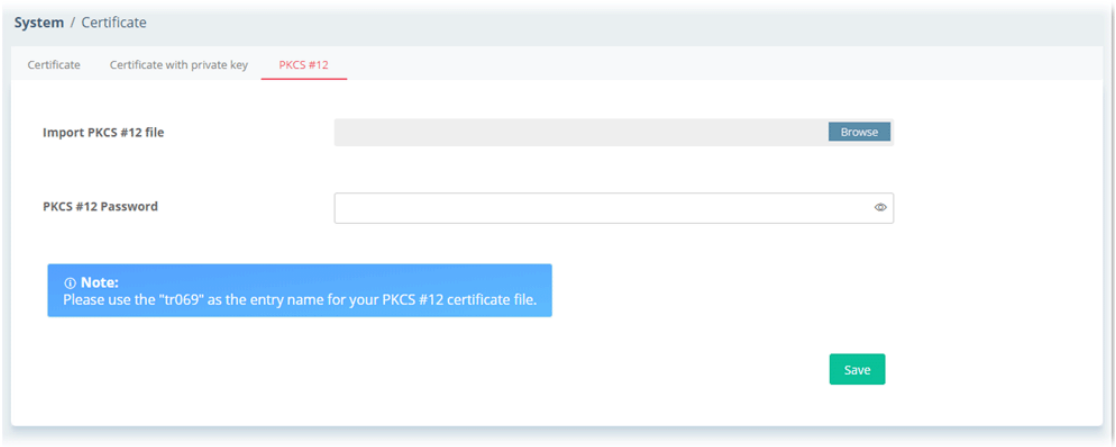

The content of PEM file shall contain at least one group of Private Key and Certificate or one Private Key with multiple certificates. See below:

```
-----BEGIN PRIVATE KEY-----
MIIEkjC....
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIGDjCCBPag....
-----END CERTIFICATE-----
```

#### 6.5.8.3 PKCS #12

PKCS #12 file indicates a valid certificate which can be output and protected with a password setting. Also, it means a file which merges the private key with signed certificate by using keytool and protected with a password setting.

This page is used for importing PKCS #12 file and applying to VigorACS server with specified password.




These parameters are explained as follows:

| Item | Description |
|---|---|
| **Import PKCS #12 file** | Click the Browse button to specify the file. |
| **PKCS #12 Password** | Enter a string as password for PKCS #12 certificate. |
| **Save** | Save and activate the current settings. |

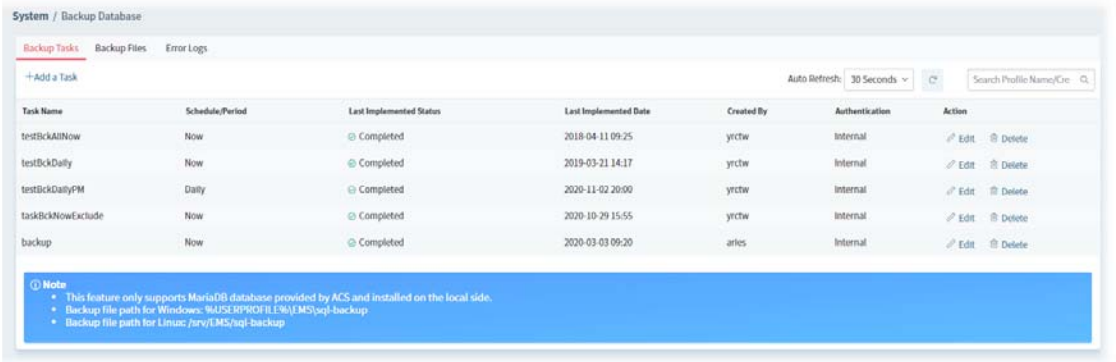
### 6.5.9 Backup Database

#### 6.5.9.1 Backup Tasks

VigorACS system will backup database periodically / immediately according to the selected task profile.

The purpose of task profile is to avoid failing to backup database in VigorACS server when transferring VigorACS server from one platform to another one due to damage on the database or hard disk.

The backup file will be stored on the hard disk of VigorACS Server located.

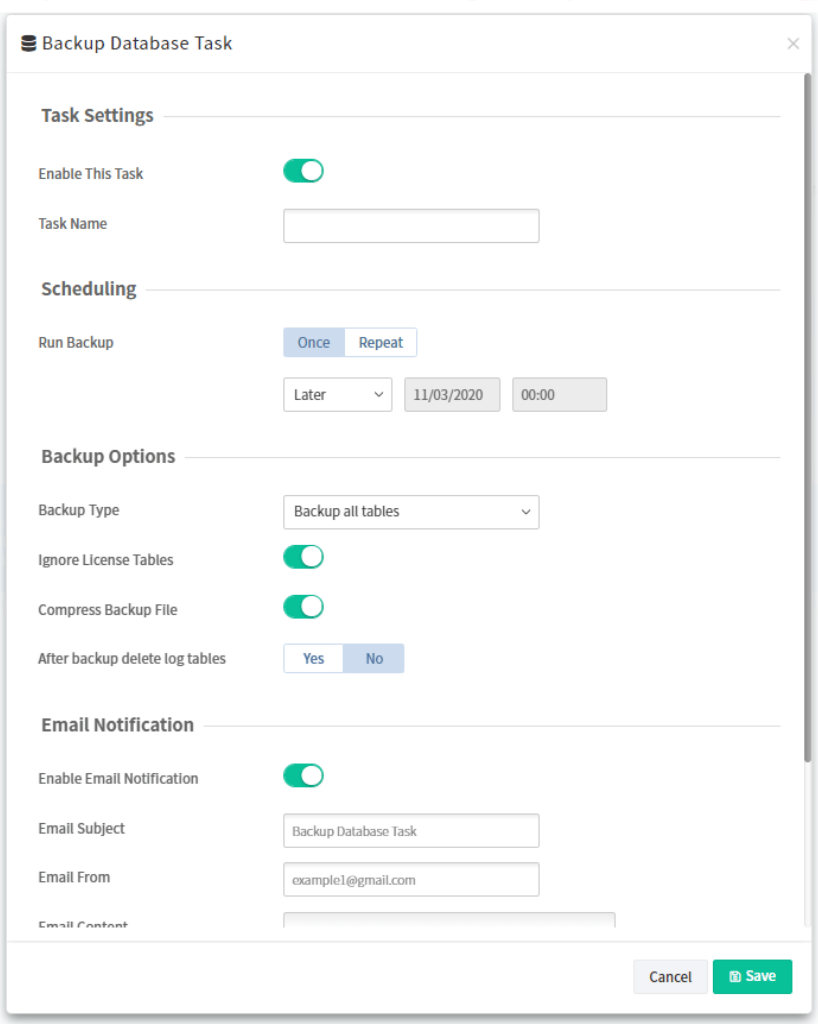



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Search Profile Name / Created by** | Specify the conditions (type the profile name, creator) for database task searching. |

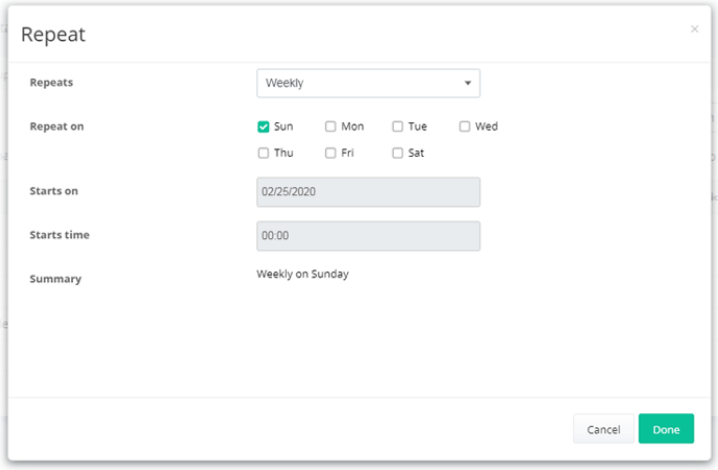
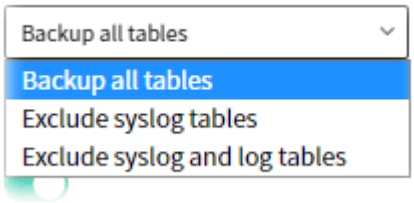
| | |
|---|---|
| **+Add Backup Database Task** | Click to add a backup database task. |
| **Task Name** | Display the name of the task. |
| **Schedule/Period** | Display the schedule profile or period of time of database backup. |
| **Last Implemented Status** | Display the status (completed or backup failed) of database backup. |
| **Last Implemented Date** | Display last implemented date of database backup. |
| **Created By** | Display the name of the creator of such task. |
| **Action** | **Edit** – Click to modify, change the selected profile.<br>**Delete** - Click to delete the selected profile. |

The following setting page appears when **+Add a Task** is clicked.



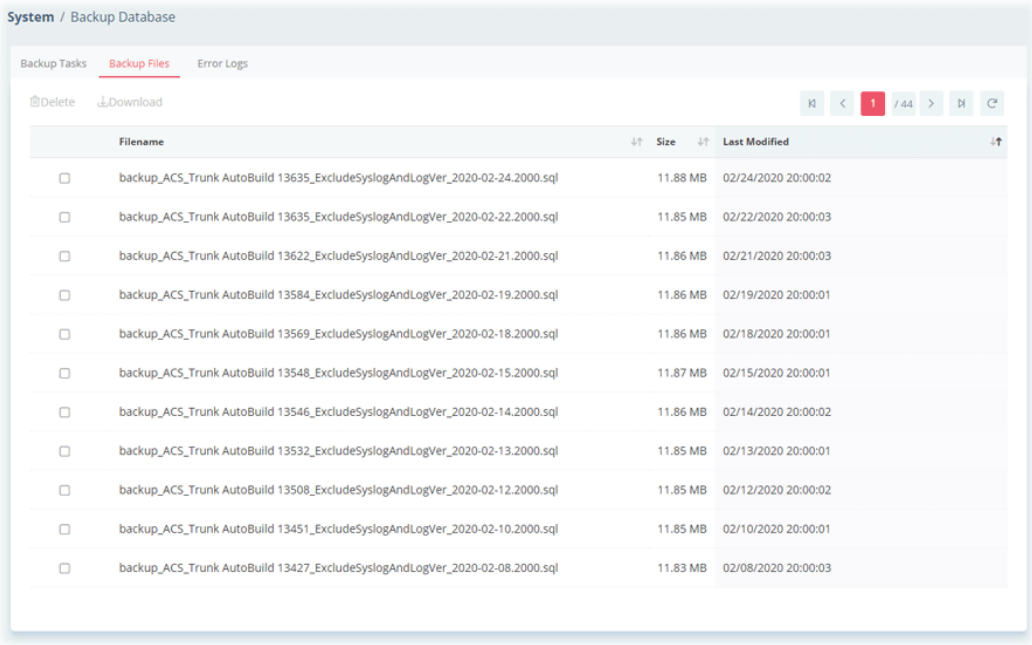

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Task Settings** | **Enable This Task** - Click to enable the task.<br>**Task Name** - Enter a name for the new task. |
| **Scheduling** | **Run Backup** – Choose **Once** to perform the backup immediately or at certain time. Choose **Repeat** to perform the backup periodically. |

| | |
|---|---|
| | • **Later / Now** – It is available when Once is selected as Run Backup.<br>• **Starts on xxxxx** – It is available when Repeat is selected as Run Backup. Click **Edit** to open the following web page for modifying the time setting.<br>  |
| **Backup Options** | **Backup Type** – Choose an option to perform the backup.<br>  <br>**Ignore License Tables** – VigorACS system performs the database backup by ignoring the tables concerning of backup and license (such as syscd, syssn, dslpmid, dslpmshow and etc.,) to prevent from license error while transferring VigorACS server. The default value is "Enabled".<br>**Compress Backup File** - The backup file will be compressed.<br>**After backup delete log tables** – Delete the log tables immediately when VigorACS server finishes the backup job |
| **Email Notification** | **Enable Email Notification** – If enabled, VigorACS server will send a notification email **about database backup** to the recipient.<br>• **Email Subject** – Enter the subject for the email.<br>• **Email From** – Enter the email address of the sender/agent/registrar.<br>• **Email Content** – Enter the content of the email.<br>• **Email To** – Enter the email address of the recipient.<br>• **+Add recipient** – Add more recipients to receive the email from VigorACS server. |
| **Cancel** | Discard current modification. |
| **Save** | Save the current settings and exit the page. |

### 6.5.9.2 Backup Files

This page shows a list of backup files generated by VigorACS server.

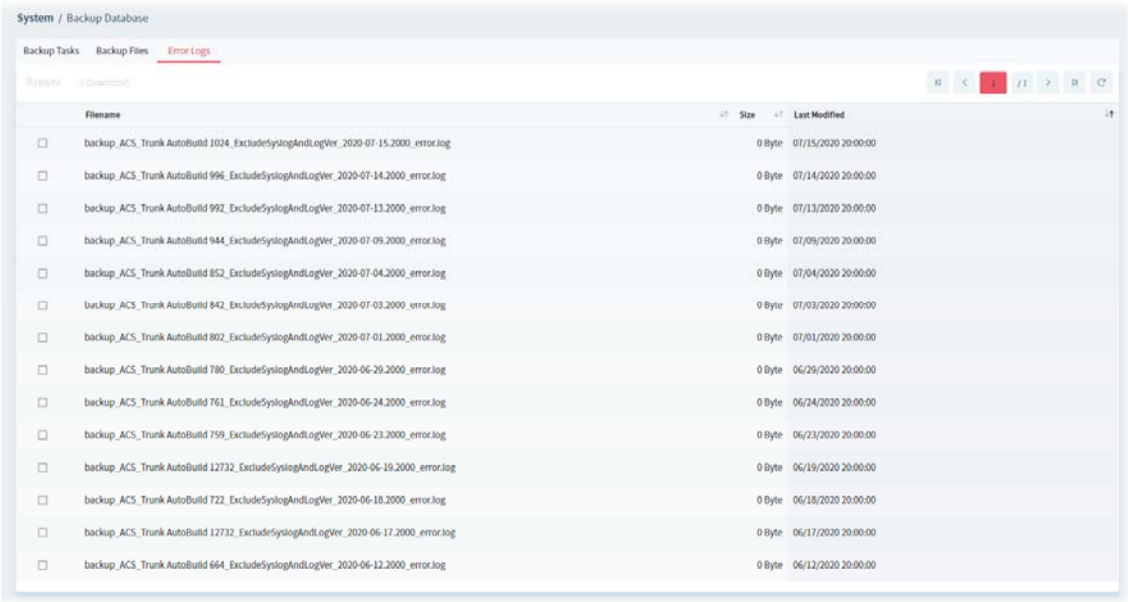



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Delete** | Click to remove the selected filename. |
| **Download** | Click to download the file from the hard disk of VigorACS server located for restoration or transferring.<br> |
| **Filename** | Display the name of the backup file. |
| **Size** | Display the size of the backup file. |
| **Last Modified** | Display the last modified time. |

### 6.5.9.3 Error Logs

This page will display logs of the task which failed to back up the database.




These parameters are explained as follows:

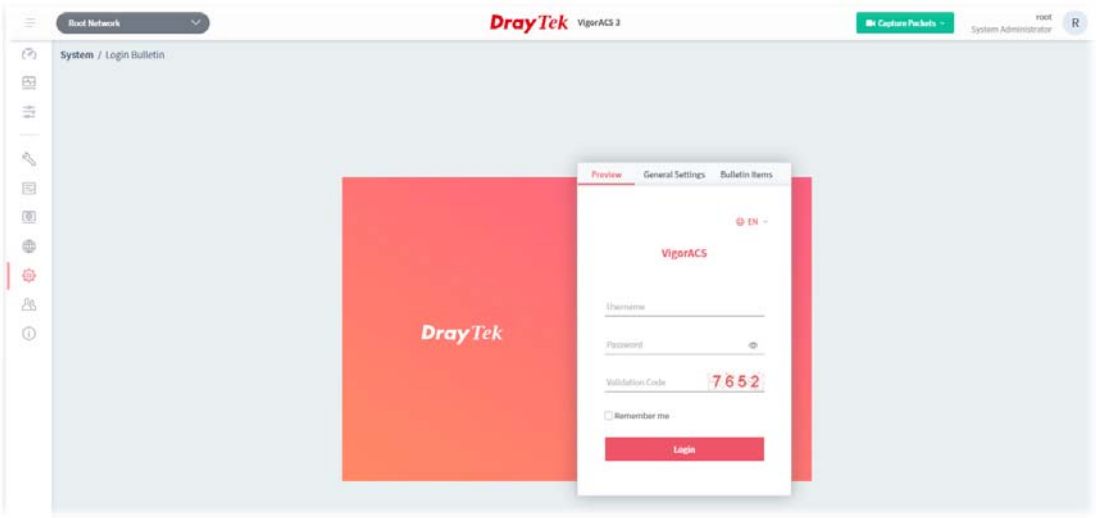
| Item | Description |
|---|---|
| **Delete** | Click to remove the selected error log. |
| **Download** | Click to download the selected error log from the hard disk of VigorACS server located.<br>The downloaded log file can be browsed by any text editor. If the content of the log contains the error message output by the program of “mysqldump”, the system administrator can get the reason for backup failure by analyzing the error message.<br>If **Email Notification** is enabled, the error log file will be sent by e-mail to the recipient(s) defined in **System>>Backup Database>>Backup Tasks**. |
| **Filename** | Display the name of the error log. |
| **Size** | Display the size of the backup file. |
| **Last Modified** | Display the time that such error occurred. |

### 6.5.10 Login Bulletin

VigorACS server operator can put several important messages on VigorACS login page.

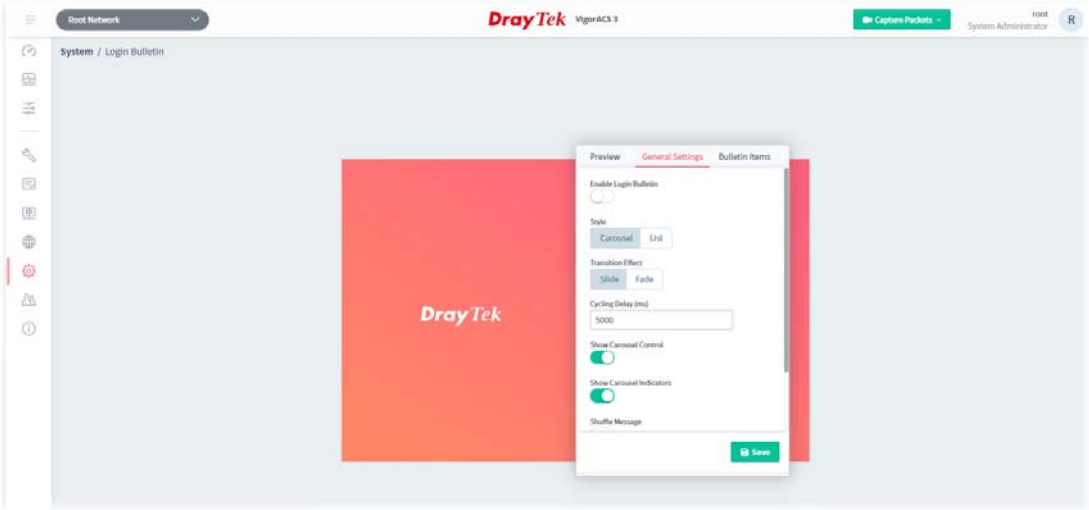
#### 6.5.10.1 Preview

This page displays a preview of bulletin with specified content on the login web page of VigorACS.



### 6.5.10.2 General Settings

It allows the user to enable and configure settings for login bulletin.

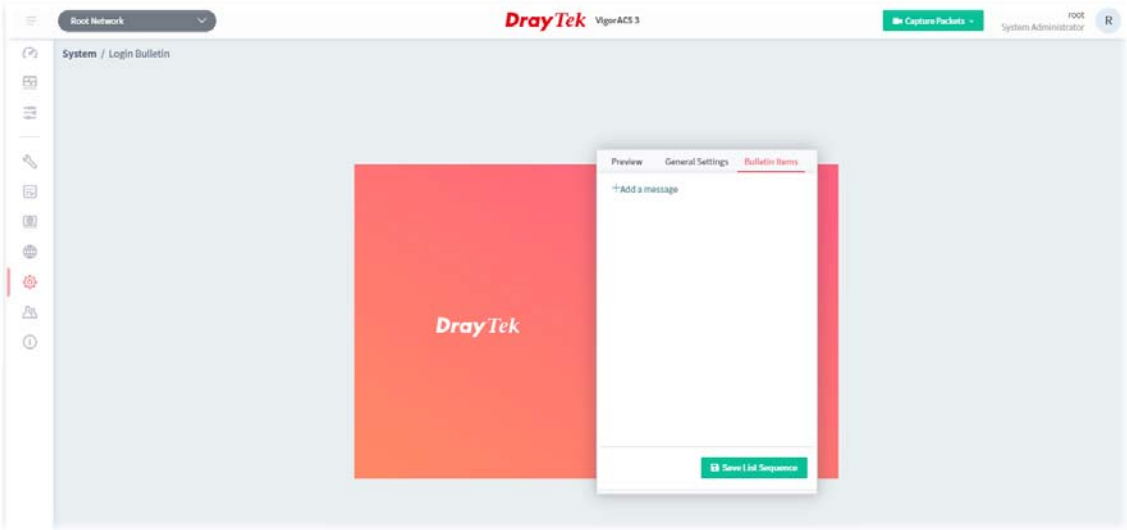



These parameters are explained as follows:

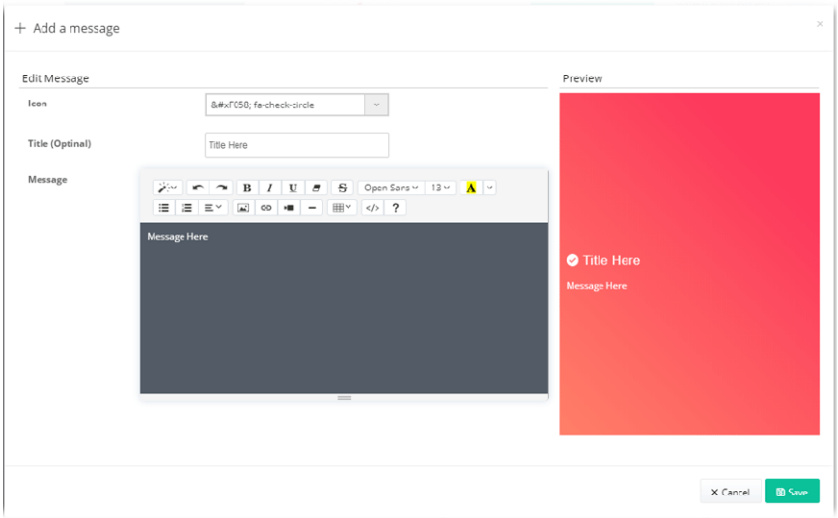
| Item | Description |
|---|---|
| **Enable Login Bulletin** | If it is enabled, a bulletin with specified content will be shown on the login web page of VigorACS. |
| **Style** | The message on the bulletin will be displayed with carousel animation or listed one by one.<br>**Carousel** – Messages in bulletin will be displayed with carousel animation.<br>**List** – All of the messages in bulletin will be listed at one time. |
| **Transition Effect** | **Slide** –The messages will appear automatically from left to right or right to left by sliding.<br>**Fade -** The message will appear one by one. |
| **Cycling Delay** | Set the time delay for every bulletin message item. The available range is 1000 to 60000 ms. |
| **Show Carousel Control** | Small arrows below the messages will be shown on the page if this function is enabled. |
| **Show Carousel Indicators** | Indicators of the slides below the message will be shown on the page if this function is enabled. |
| **Shuffle Message** | The messages will appear randomly if this function is enabled. |
| **Save** | Save the current settings. |

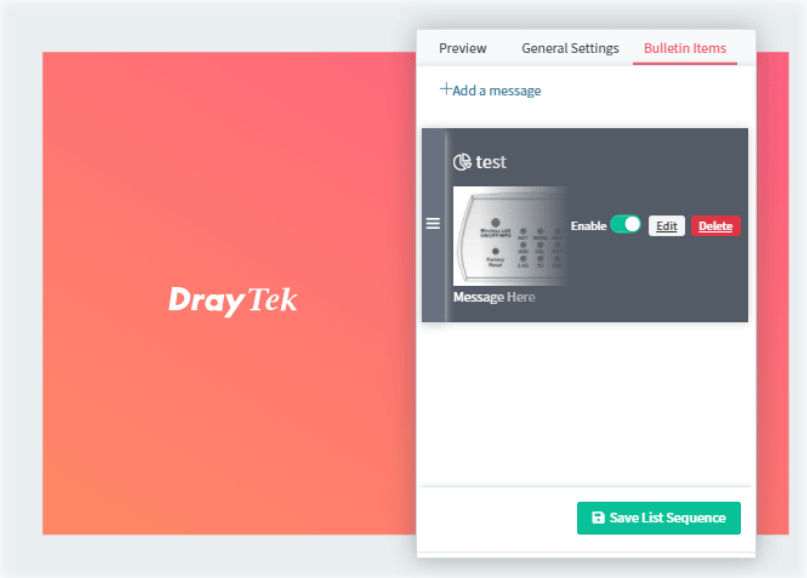
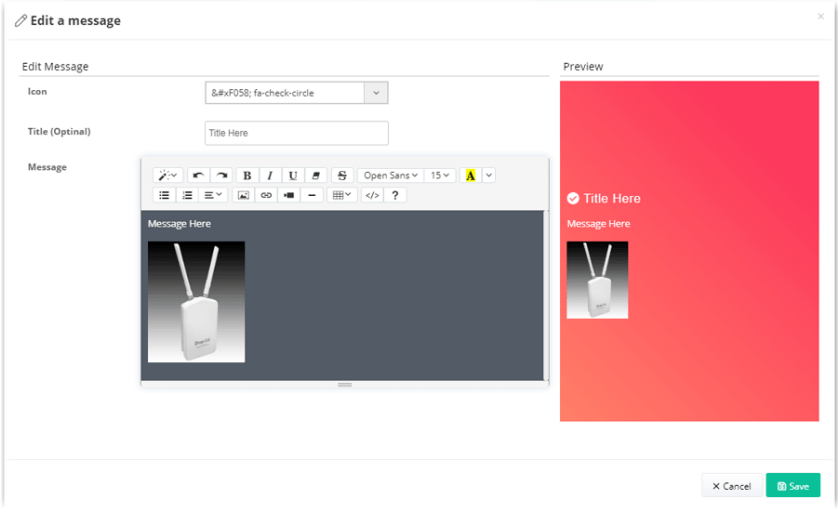
### 6.5.10.3 Bulletin Items

This page is used for creating new message or modifying existing message.




These parameters are explained as follows:

| Item | Description |
|---|---|
| **+Add a message** | Create a new message.<br>  <br>**Icon** – Specify one of the types as the icon in the front of the title.<br>**Title (Optional)** – Enter a string as the heading for the message.<br>**Message** – Enter the content of the message.<br>**Preview** – The changes made above will be shown in this area immediately.<br>**Save** – Save the message and exit the dialog. Refer to the following setting result. |

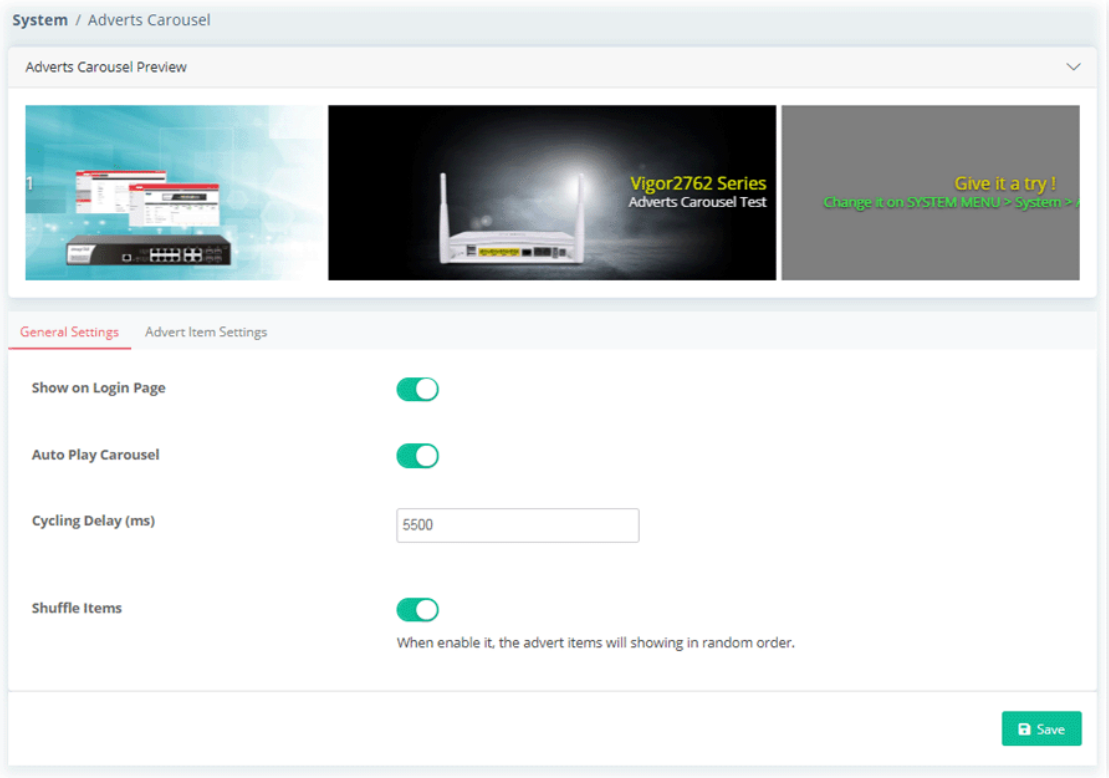
| | |
|---|---|
| |  |
| **Edit** | Modify the selected message.<br>  <br>**Icon** – Specify one of the types as the icon in the front of the title.<br>**Title (Optional)** – Enter a string as the heading for the message.<br>**Message** – Enter the content (including text and/or image) of the message.<br>**Preview** – The changes made above will be shown in this area immediately.<br>**Save** – Save the message and exit the dialog. |
| | Drag this control item to change the sequence of the selected message on the list. After changing, click **Save**.<br>If the option **Shuffle Message** in **Login Bulletin>>General Settings** is enabled, the messages will not be displayed in the order of the list, but will be displayed randomly. |
| **Enable** | If enabled, the message will be USED and shown in the login bulletin. If disabled, the message will NOT be used and shown in the login bulletin. |
| **Delete** | Remove the selected message. |
| **Save List Sequence** | Save the list sequence for all messages. |

### 6.5.11 Adverts Carousel

VigorACS server operator can add adverts which will be shown on the banner of VigorACS login page or the dashboard of VigorACS server.

#### 6.5.11.1 General Settings

This page determines if displaying the adverts on the login page or not, enabling the auto play carousel function, selecting cycling delay time and using the shuffle items.

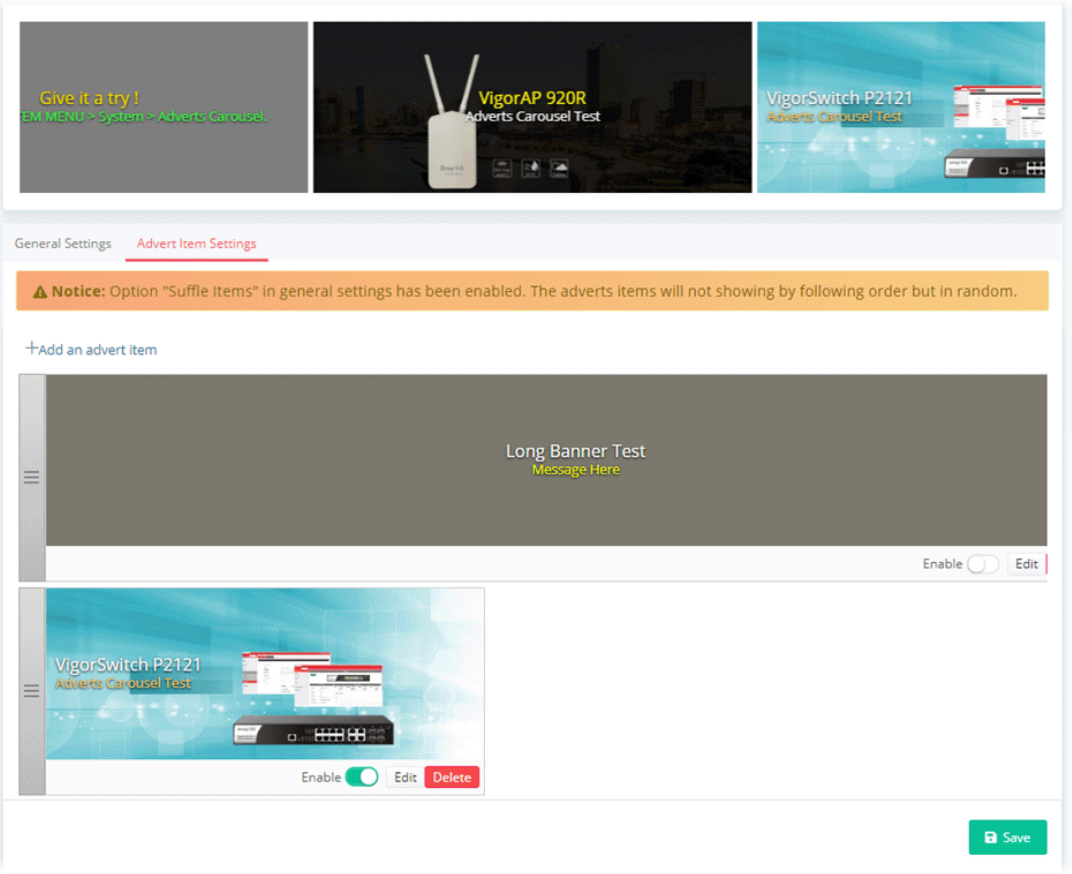



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Adverts Carousel Preview** | Display a preview of the adverts carousel with specified images. When adding, deleting, enabling or disabling any advert item, or changing any setting configuration, this field will display the content of the modification. |
| **Show on Login Page** | If enabled, the adverts carousel will be SEEN on the login page.<br>If disabled, the adverts carousel will NOT be seen on the login page. |
| **Auto Play Carousel** | If enabled, the adverts carousel will be PLAYED automatically.<br>If disabled, the adverts carousel will NOT be played automatically.<br>When the number of advert item is smaller than 1, the system will not perform the adverts carousel. |
| **Cycling Delay (ms)** | Set the time delay for every advert item. The available range is 1000 to 60000 ms. |
| **Shuffle Items** | If enabled, the advert items will be played randomly on the adverts carousel. |

### 6.5.11.2 Advert Item Settings

This page is used to upload a selected image onto VigorACS server and enter words (title, message of the image and color specified) on the image for advertisement.

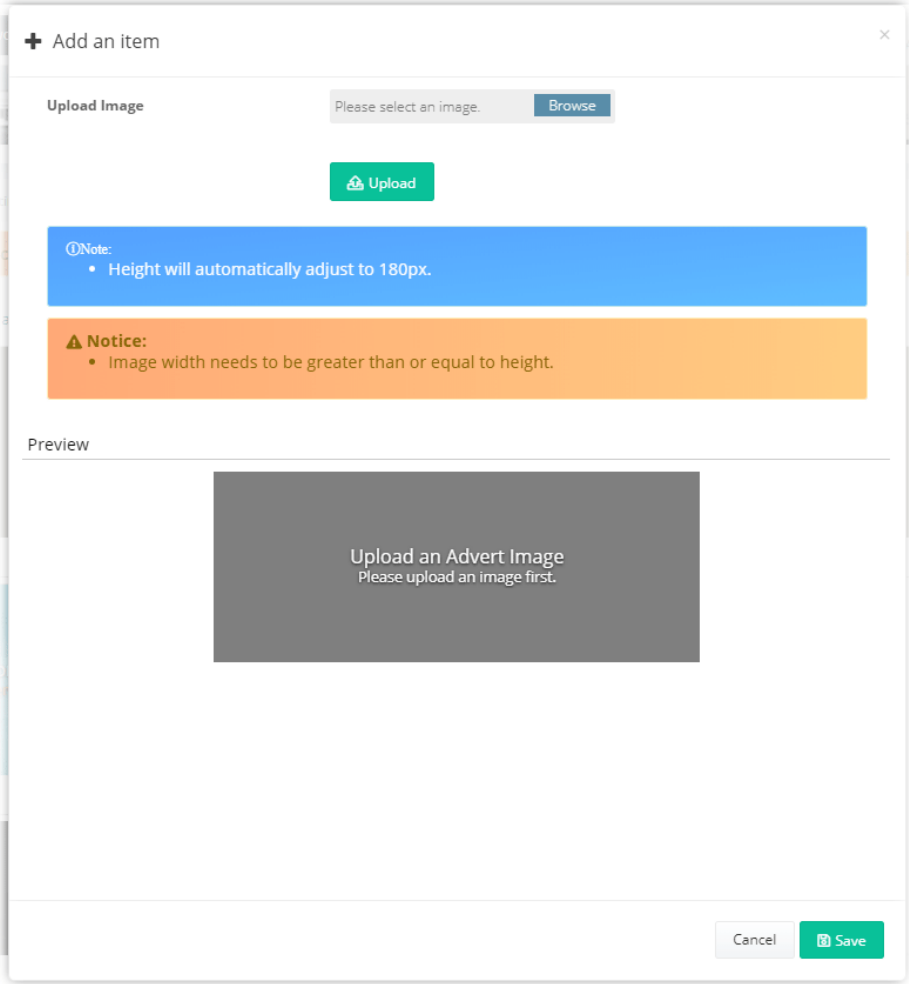



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Adverts Carousel Preview** | Display a preview of the adverts carousel with specified images. When adding, deleting, enabling or disabling any advert item, or changing any setting configuration, this field will display the content of the modification. |
| **+Add an advert item** | Create a new advert item to be used on adverts carousel. |

To add an advert item, do the following steps.

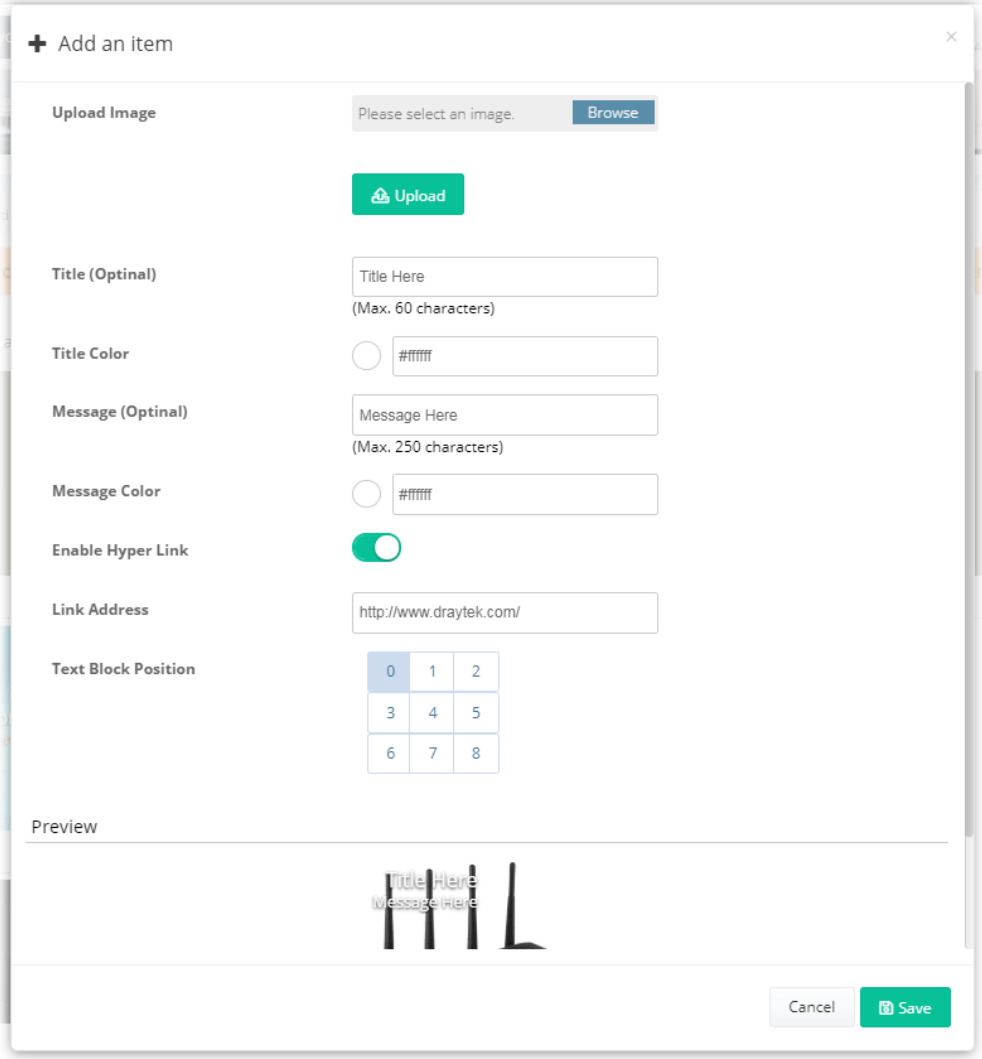
1. Click **+Add an advert item** to display the following setting page.




These parameters are explained as follows:

| Item | Description |
|---|---|
| **Upload Image** | Click Browse button to locate the image file (supporting .gif, .jpg, and .png format). After clicking Upload, the images will be stored to the ACS Server. Note that the height of the image will be automatically adjusted to 180 pixel. Image width needs to be greater than or equals to the height. Different adverts can use the same image which is uploaded to VigorACS 3 server. |
| **Upload** | Upload the selected image to ACS server as the advert image. |

2. After specifying an image file, click the **Upload** button. Later, a page with detailed settings will appear as follows:

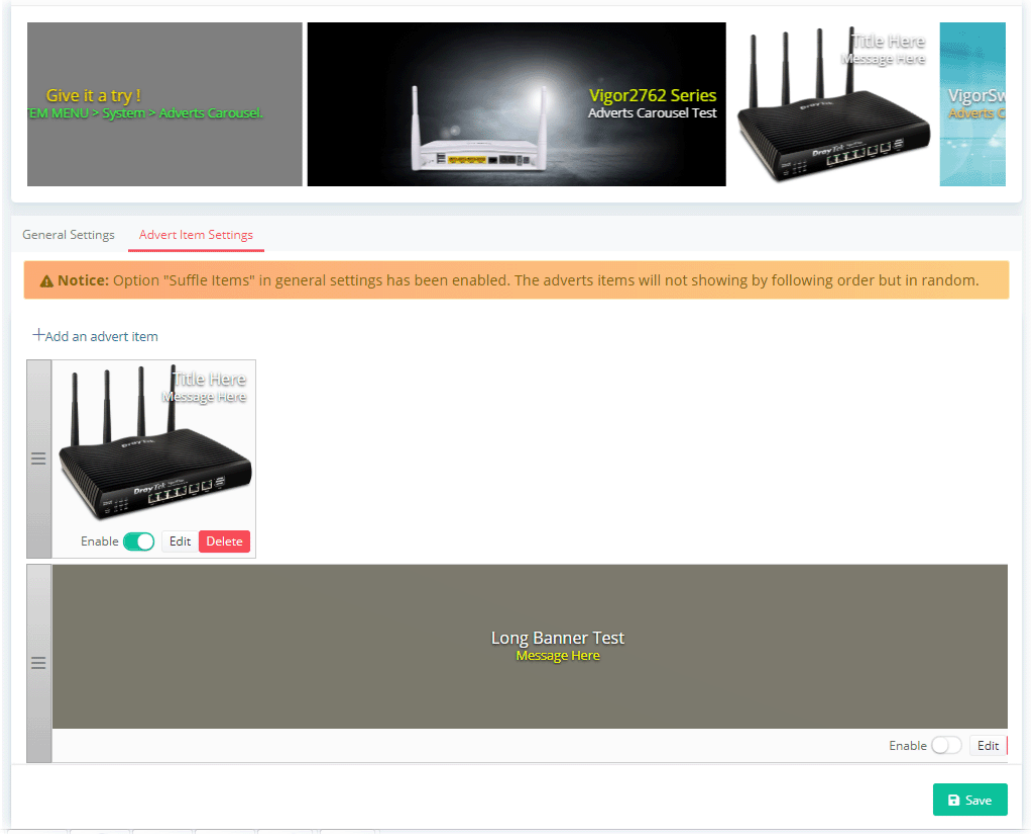



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Upload Image** | Click Browse button to locate the image file (supporting .gif, .jpg, and .png format). After clicking Upload, the images will be stored to the ACS Server. Note that the height of the image will be automatically adjusted to 180 pixel. Image width needs to be greater than or equals to the height. Different adverts can use the same image which is uploaded to VigorACS 3 server. |
| **Title (Optional)** | Enter a string as a title for this image. |
| **Title Color** | Assign a color to apply to the title. (Default color is #ffffff). |
| **Message (Optional)** | Enter a brief description for the advertisement. |
| **Message Color** | Assign a color to apply to the message. (Default color is #ffffff). |
| **Enable Hyper Link** | Choose Enable to activate hyper link for the advertisement. |
| **Link Address** | If Enable Hyper Link is enabled, enter the URL of the link. |
| **Text Block Position** | Determine the position of the title and message on the advert image. |
| **Preview** | Any changes on this setting page will be shown in this field. |

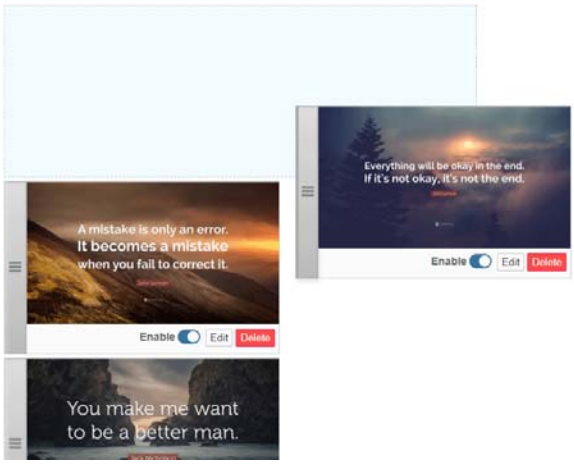
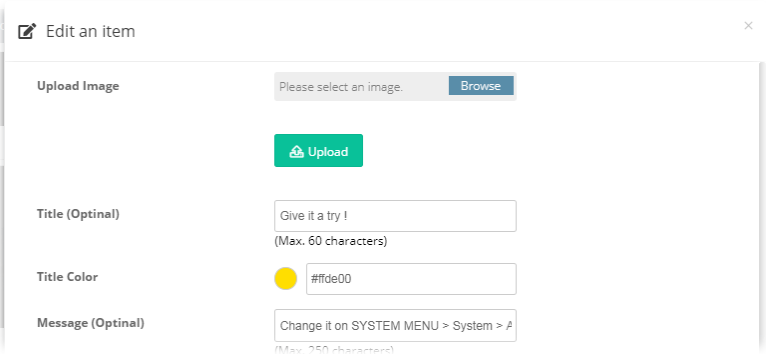
| | |
|---|---|
| | Preview<br> <br>If the width of the advert image uploaded to VigorACS server is smaller than the advertisement area, the blank space will be filled with repeated advert image. |
| **Cancel** | Discard current modification. |
| **Save** | Save the current settings and exit the page. |

3. Enter the value(s) required for the image, then click **Save**.
4. Now, the selected image has been added and shown on this setting page. If the image width is smaller than the banner width, the advert images will appear repeatedly.



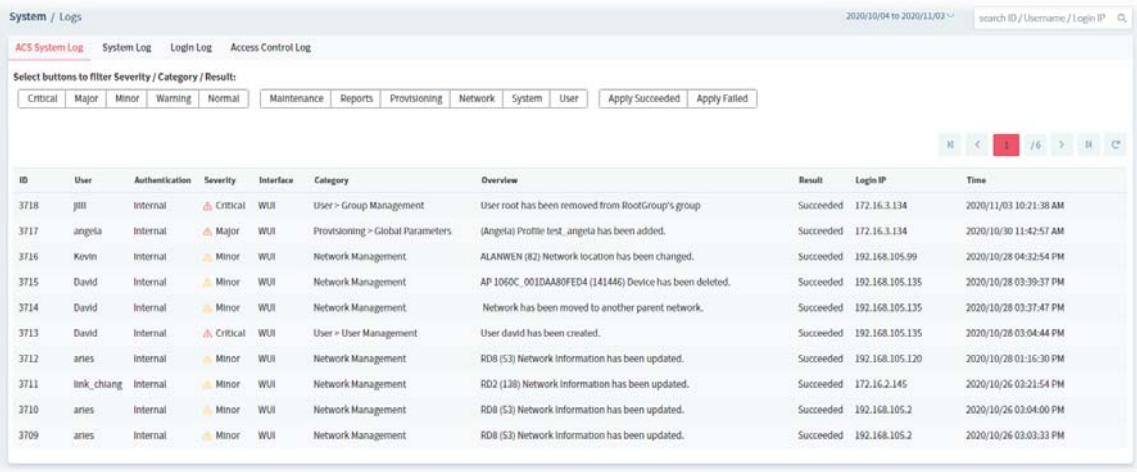

These parameters are explained as follows:

| Item | Description |
|---|---|
| | Drag this control item to change the sequence of the selected advert item on the list. After changing, click **Save**.<br>If the option **Shuffle Items** in **Adverts Carousel>>General Settings** is enabled, the adverts items will not be displayed in the order of the list, but will be displayed randomly. |

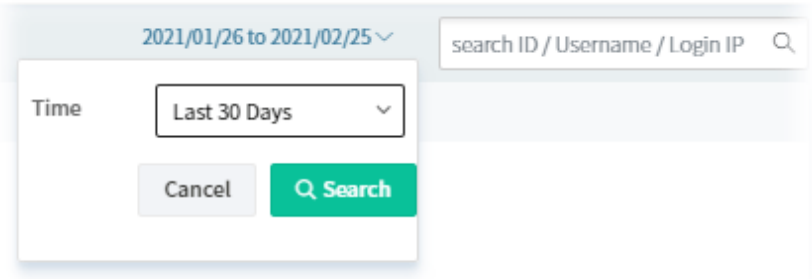
| | |
|---|---|
| |  |
| **Enable** | If enabled, the advert item will be USED and shown in the adverts carousel.<br>If disabled, the advert item will NOT be used and shown in the adverts carousel. |
| **Edit** | Click to modify settings for the selected image.<br>  |
| **Delete** | Delete the selected advert item. |
| **Save** | Save the current settings. |

### 6.5.12 Logs

Information displayed here shall be useful for the administration to viewing the status for user access.



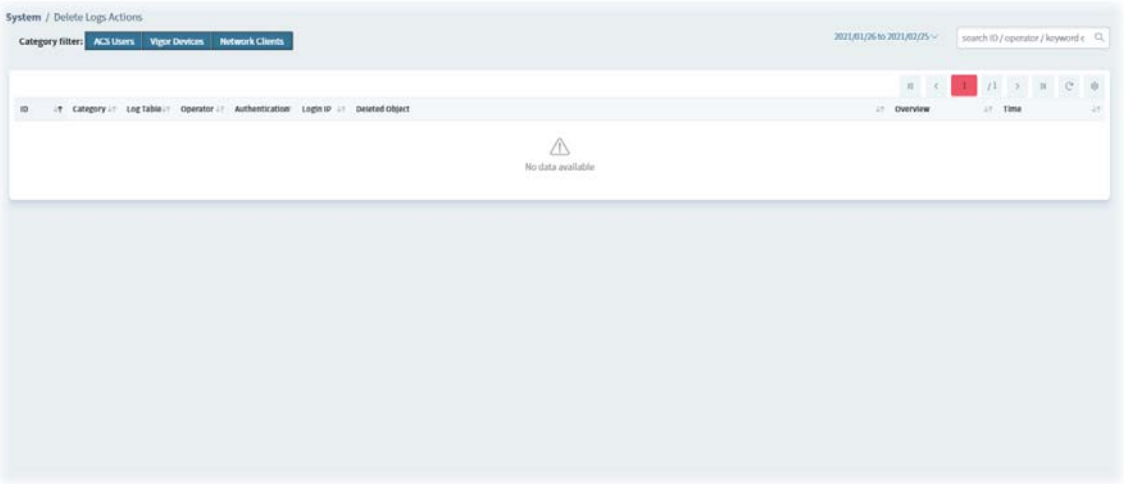

These parameters are explained as follows:

| Item | Description |
|---|---|
| **ACS System Log / System Log / Login Log / Access Control Log** | Click one of the types to display log of ACS System, System and Login. |
| **Search ID / Username / Login IP / Overview** | Specify the conditions (type the ID number, username, the IP address or overview) for log searching. |
| **Time Setting** |  |
| **ACS System Log** | Display the ID, username, login IP, category, overview, severity and time for clients accessing into VigorACS.<br>**Select buttons to filter Severity / Category / Result** - Click the one of the buttons (Critical, Major, Minor, Warning, Normal, Maintenance... and so on). The log related to the selected type will be displayed on the screen. |
| **System Log** | Display the ID number, model name with MAC address for the CPE, and the action executed in CPE.<br>**Export All** - Log information can be exported as a file. |
| **Login Log** | Display the log information, including status, username, login IP, login time and logout time for clients accessing into VigorACS.<br>**Export All** - Log information can be exported as a file. |
| **Access Control Log** | Display the log information, including ID, Source IP, Service Type, Access Control Policy, Overview and Time for clients based on ACL profile applied.<br>**Export All** - Log information can be exported as a file. |

### 6.5.13 Delete Logs Actions

Information displayed here shall be deleted.

Delete Logs Actions is available only for the **Root** user and the user with the role of **Auditor**.

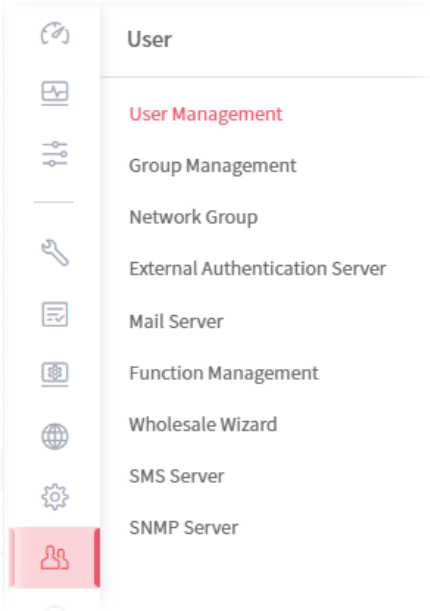



All logs with the Information including an ID number, category filter, log table, operator, authentication, login IP Deleted Object, Overview, and time will be displayed on this page. They will be kept forever until they are deleted from this page.

## 6.6 User

VigorACS allows a user to manage CPE/AP devices through VigorACS server. However, the user has to type specific name and password defined in this page. Different users must use different names and passwords for accessing VigorACS.

This chapter will guide you to define users. It can be set with different roles (such as System Administrator, Administrator, Group Administrator, Operator, and etc.); each role has different administration authority.

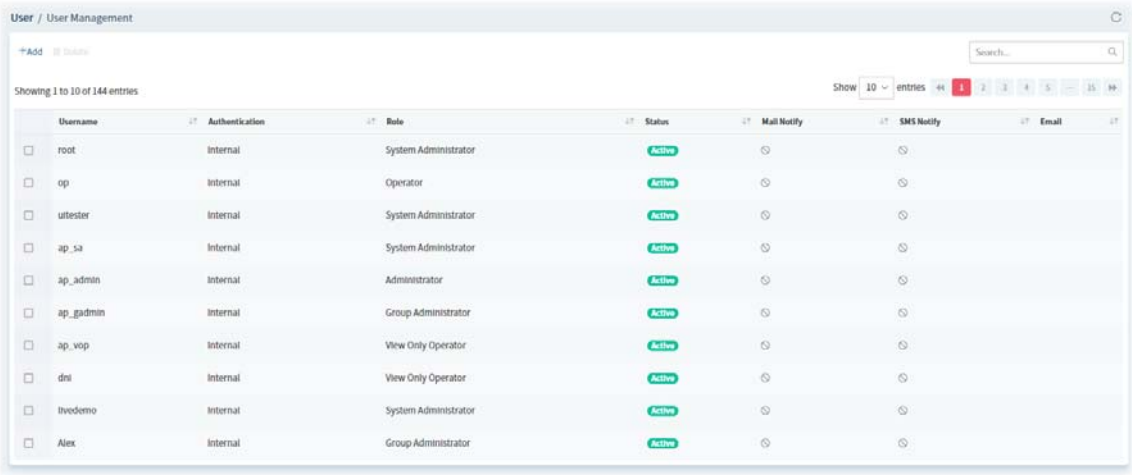



User menu is available only for the role of **System Administrator**, and **Group Administrator**.

### 6.6.1 User Management

The user management function allows a user to set name, password, and e-mail address as identification in VigorACS system.

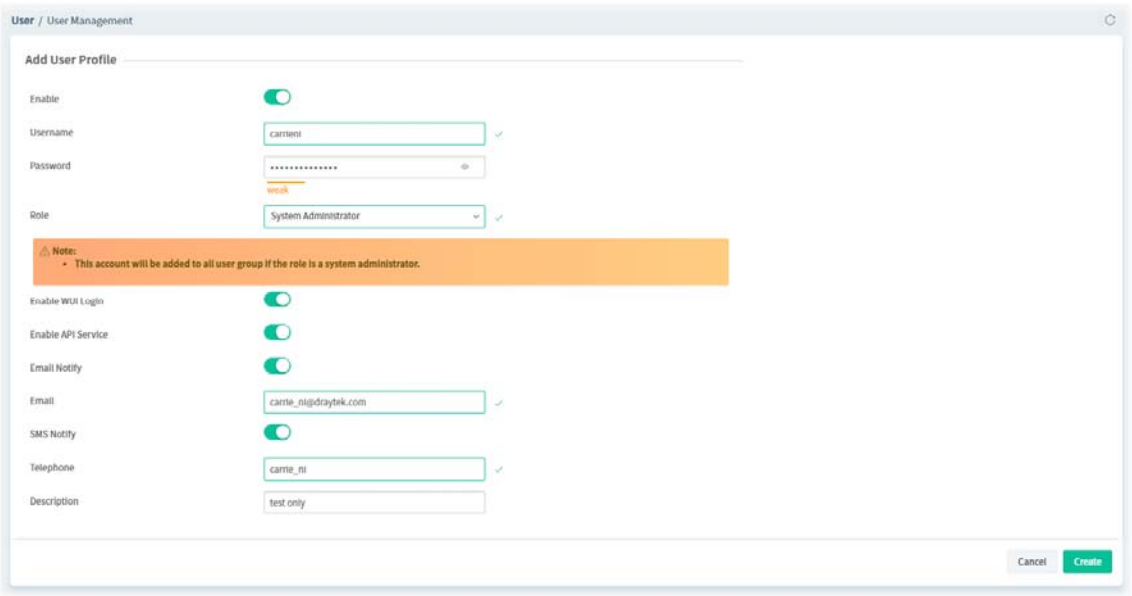
To add, delete a user or check information for a user, open **User** and choose **User Management.** This page displays basic information including username, role (system administrator, administrator, group administrator, operator, view only operator), status (active, inactive), mail notify (yes or no), SMS notify (yes or no), email address, telephone number, other description for the user.




These parameters are explained as follows:

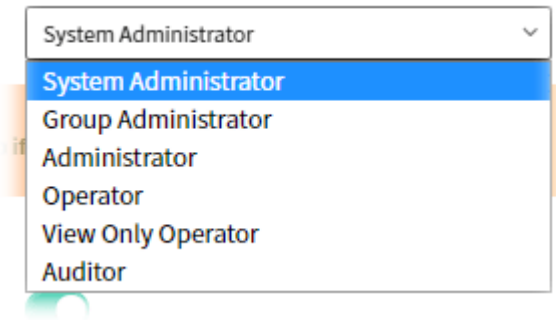
| Item | Description |
|---|---|
| **+Add** | Click to add a user. |
| **Delete** | Click to remove the selected user. |

The following setting page appears when **+Add** is clicked.




These parameters are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Click to enable the user profile. |
| **Username** | Enter a name for the new user. |
| **Password** | Enter the password for the user. |
| **Role** | Choose the role for the selected **user**. Different role represents different authority that the user group will have. The great the authority is, the more functions the user can have. |

| | |
|---|---|
| |  <br>• **System Administrator** – Have the highest authority.<br>• **Group Administrator –** Have the middle authority high than "Administrator".<br>• **Administrator** – Have the middle authority.<br>• **Operator** – Have the low authority higher than View Only Operator.<br>• **View Only Operator –** Have the lowest authority.<br>• **Auditor** - Have limited authority different from other roles. It is available for choosing only when the system administrator accesses into VigorACS with the role of Root (default account). The only action allowed is to view the deleted log information (on the page of System>>Delete Logs Action). |
| **Enable WUI Login** | Click to enable/disable the function.<br>When it is enabled, the user is allowed to access into the web user interface of VigorACS. |
| **Enable API Service** | Click to enable/disable the function.<br>When it is enabled, the user is allowed to use RESTful API service. |
| **Email Notify** | Click to enable/disable the function.<br>When it is enabled, an email will be sent to the user as a notification when the connected device gets alarms. |
| **Email** | Enter the email for communication between the user and VigorACS server. |
| **SMS Notify** | Click to enable/disable the function.<br>When it is enabled, an SMS will be sent to the one listed here as a notification when the device gets alarms. |
| **Telephone** | Enter the telephone number for receiving the SMS notification. |
| **Description** | Enter a brief description for the user. |
| **Cancel** | Discard current modification. |
| **Create** | Save the current settings and exit the page. |

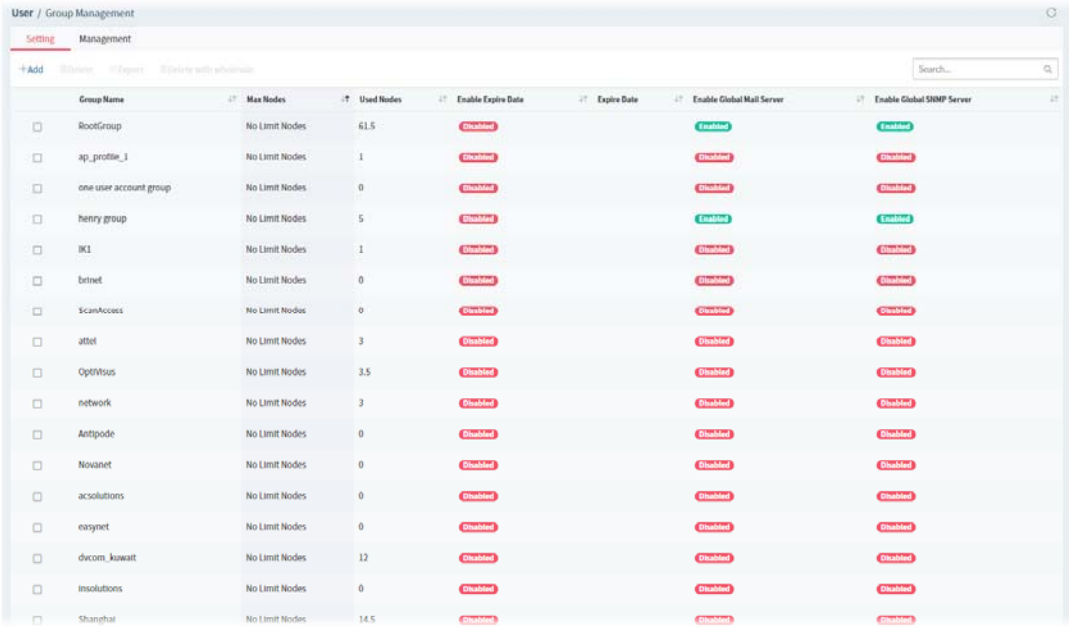
After finished the above settings, click **Create** to add a new user account.

## 6.6.2 Group Management

This page allows you to add a new user group containing with many users (with different roles or authorities). To add, delete a user group or check information for a user group, open **SYSTEM MENU>>User** and choose **Group Management.**

### 6.6.2.1 Setting

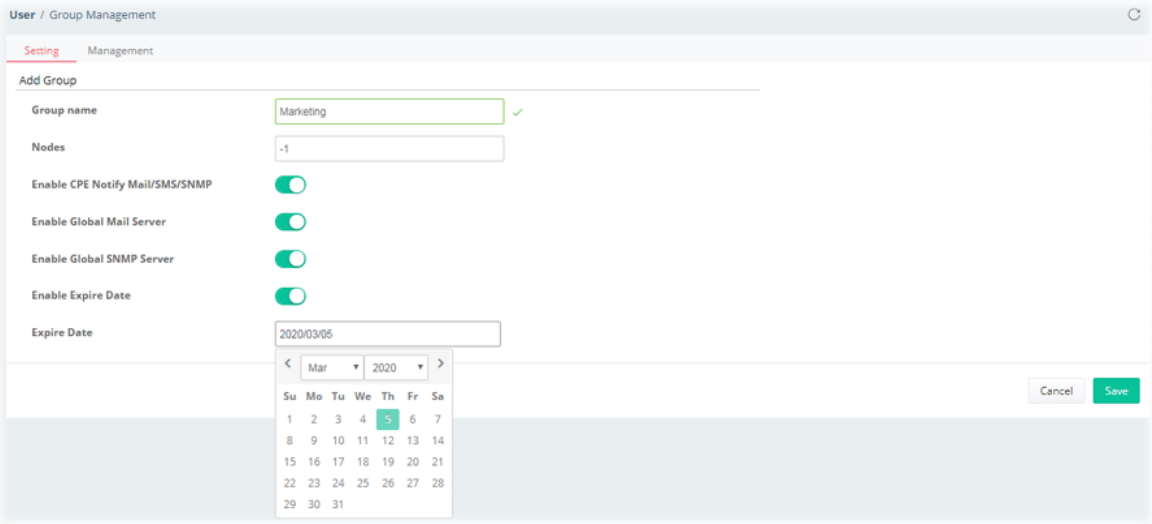
**RootGroup** is defined in factory and owns the highest authority. You can define new user group(s) to fit your requirement.




These parameters are explained as follows:

| Item | Description |
|---|---|
| **+Add** | Click to add a user group. |
| **Delete** | Click to clear the selected group. Before using such function, check if the group is blank or not by switching to the Management tab.<br>If the selected group still contains any user in it, such group is unable to be deleted. In this case, use Delete with Whole Sale instead. |
| **Export** | Click to open a dialog for typing SQL syntax to export the settings. |
| **Delete with Whole Sale** | Click to delete the selected user group. |

Click any one of the existed entries to access into the configuration page for making modifications. Or, click **+Add** to create a new group.

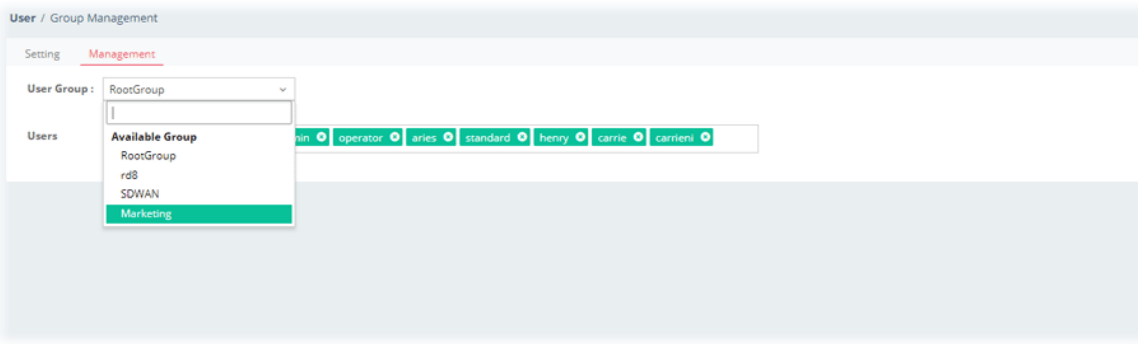



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Group Name** | Enter the name (e.g., Marketing) that can represent the user group. |
| **Nodes** | Display the number of license nodes for this group. Change the number by using the scroll box. |
| **Enable CPE Notify Mail/SMS/SNMP** | If it is enabled, this group will be allowed to use CPE's notify server / mail server / SNMP server. |
| **Enable Global Mail Server** | If it is enabled, this group will be allowed to use global mail server. |
| **Enable Global SNMP Server** | If it is enabled, this group will be allowed to use global SNMP server. |
| **Enable Expire Date** | Click to enable / disable the expire date setting. If enabled, set the expire date.<br>**Expire Date** - Display the valid date of the license for this group.<br>To change the date, move the mouse cursor on the box to display a calendar. Next click the date you want. |
| **Cancel** | Discard current modification. |
| **Save** | Save the current settings and exit the page. |

### 6.6.2.2 Management

This page allows you to specify users who want to access VigorACS into different user groups.

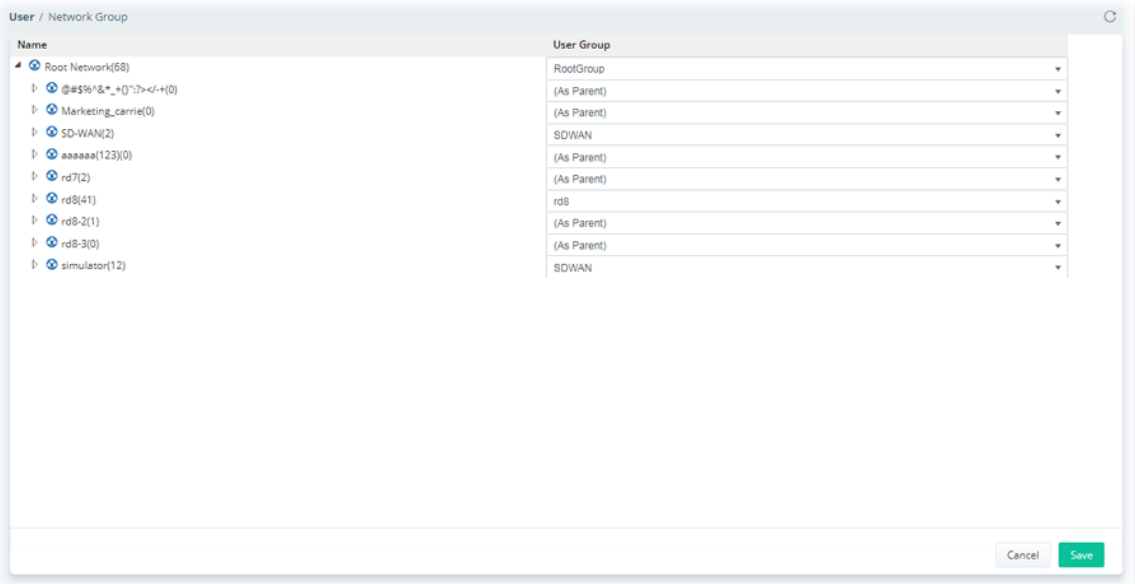



These parameters are explained as follows:

| Item | Description |
| --- | --- |
| **User Group** | Use the drop down list to specify a user group.<br>In which, RootGroup contains all of the users with the role of system administrator in default. |
| **Users** | Display all of the users belonging to the selected user group.<br>Basically, the user(s) with the highest authority (e.g., system administrator defined as user role) will be shown in this area automatically as selection items. To remove any selection item that you don't want to put in this group, simply click the "x" to delete it. |

### 6.6.3 Network Group

Though the VigorACS server allows the administrator to create several user groups in the database, yet each device can be assigned to one user group only. Therefore, if the device has been specified in certain user group, it will not be accessed by other users in different user group.

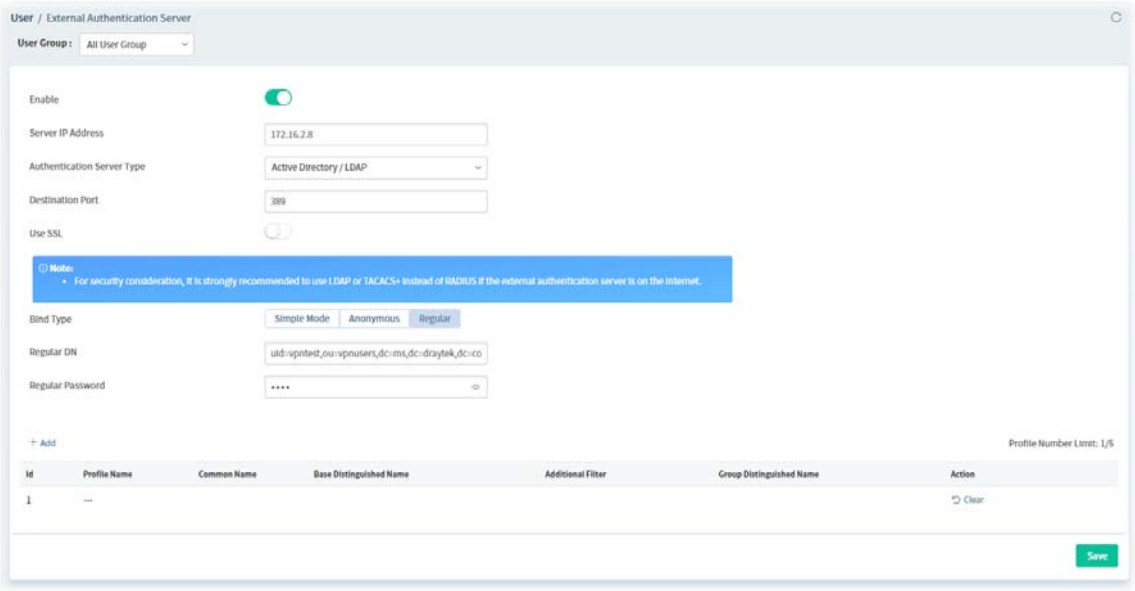



These parameters are explained as follows:

| Item | Description |
|---|---|
| **User Group** | **As Parent** – Choose the same setting as the previous layer. |
| **Cancel** | Discard current modification. |
| **Save** | Save the current settings and exit the page. |

### 6.6.4 External Authentication Server

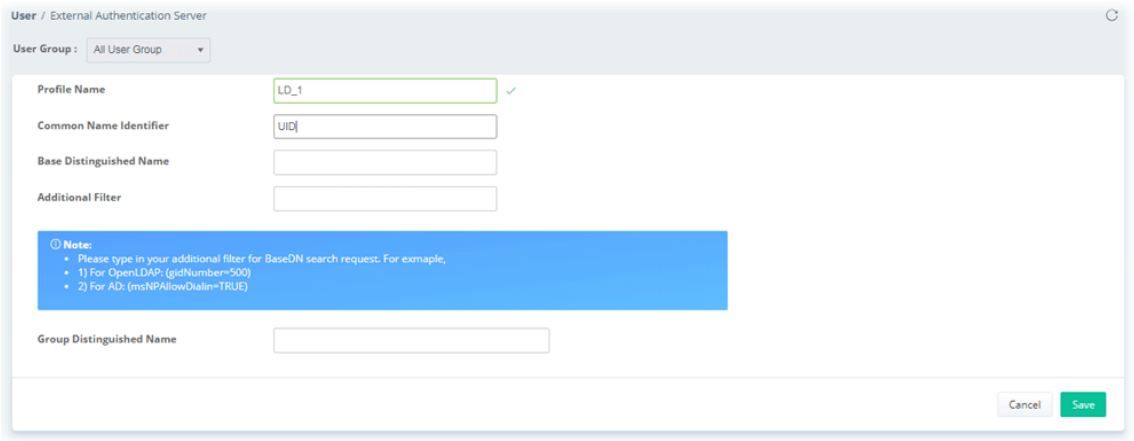
The external authentication server includes LDAP and RADIUS server. It is used to authentication the client whenever he/she wants to login VigorACS.



These parameters are explained as follows:

| Item | Description |
|---|---|
| **User Group** | Select a group to configure authentication settings. |
| **Enable** | Click to enable this function. |
| **Server IP Address** | Enter the IP address of LDAP server. |
| **Destination Port** | Enter a port number as the destination port for LDAP server. |
| **Authentication Server Type** | **Active Directory / LDAP** –<br>● **Use SSL –** Enable it to use the port number specified for SSL.<br>● **Bind Type –** There are three types of bind type supported:<br>- **Simple Mode** – Just simply do the bind authentication without any search action.<br>- **Anonymous** – Perform a search action first with Anonymous account then do the bind authentication.<br>- **Regular Mode**– Mostly it is the same with anonymous mode. The different is that, the server will firstly check if you have the search authority. For the regular mode, you'll need to type in the **Regular DN** and **Regular Password**.<br>● **Regular DN –**Type this setting if **Regular Mode** is selected as **Bind Type.**<br>● **Regular Password -** Specify a password if **Regular Mode** is selected as **Bind Type.**<br>**RADIUS** –<br>● **Shared 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>● **Confirm Shared Secret** - Re-type the Shared Secret for confirmation.<br>**TACACS+** –<br>● **Authentication Protocol** – Select PAP or CHAP.<br>● **Shared Secret** - Enter the Shared Secret for confirmation.<br>● **Confirmed Shared Secret** - Re-enter the Shared Secret for confirmation. |
| **+Add** | Click to create a profile related to LDAP. |
| **Save** | Save the current settings and exit the page. |

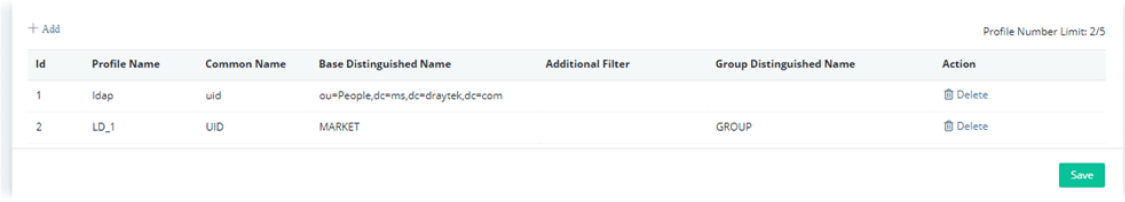
Click **+Add** to create an Active Directory / LDAP profile.



These parameters are explained as follows:

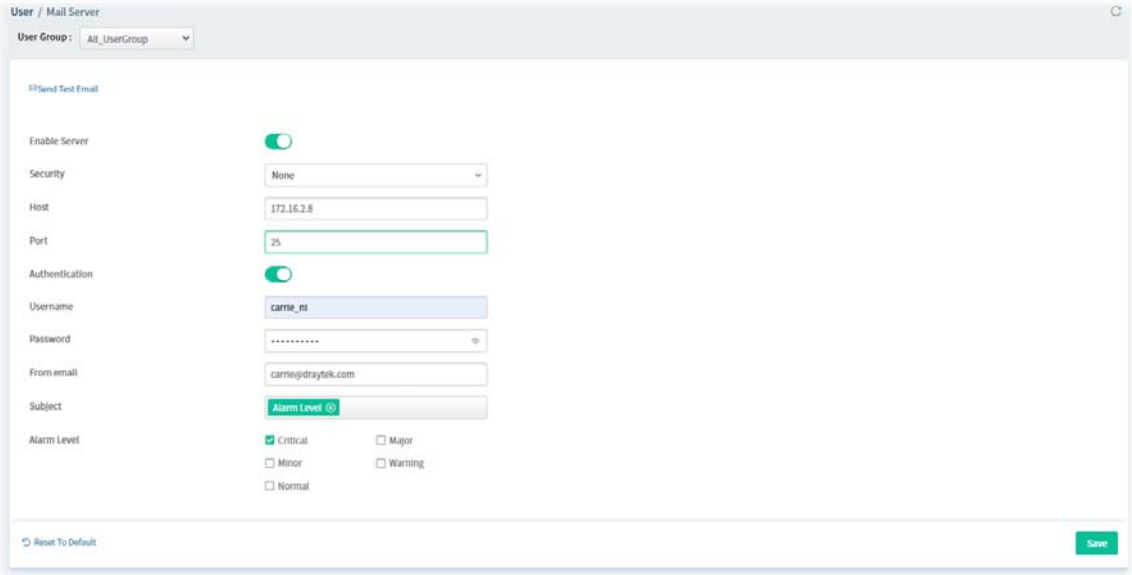
| Item | Description |
|---|---|
| **Profile Name** | Enter a name for such profile. |
| **Common Name Identifier** | Enter or edit the common name identifier for the LDAP server. The common name identifier for most LDAP server is “cn”. |
| **Additional Filter** | Enter the condition for additional filter. |
| **Base Distinguished Name / Group Distinguished Name** | Enter or edit the distinguished name used to look up entries on the LDAP server. |
| **Cancel** | Discard current modification. |
| **Save** | Save the current settings and exit the page. |

After finished the above settings, click **Save** to save the change and return to previous page. A new Active Directory / LDAP profile will be listed on the bottom of the web page as shown as below.



### 6.6.5 Mail Server

It is used to configure the mail server for sending e-mail. All of the user groups can apply the mail server settings configured in this page.

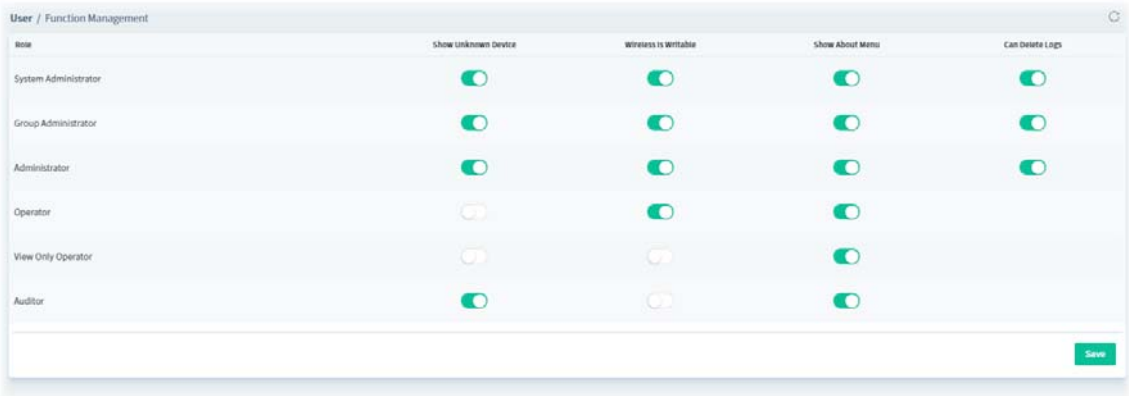



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Send Test Email** | Click to make a simple test if the user (receiver) can get the mail or not. Notification mail can be sent to multiple mail addresses after clicking Send Test Email. |
| **Enable Server** | Click to enable /disable the SMTP server. |
| **Security** | Choose None / SSL / TLS for the security of the mail transferring. |
| **Host** | Type the IP address of the SMTP server. |
| **Port** | Type the port number of the SMTP server. |
| **Authentication** | Click to activate/disable this function while using e-mail application. |
| **Username** | Type the user name for authentication. |
| **Password** | Type the password for authentication. |
| **From email** | Type the e-mail address as the sender. |
| **Subject** | At present, there are four objects to be selected for the subject of the email. |
| **Alarm Level** | There are five alarm levels (Critical, Major, Minor, Warning and Normal) which determine the timing that VigorACS mail server sends e-mail to the recipient. |
| **Save** | Save the current settings. |
| **Reset To Default** | Click to reset the mail server to default settings. |

### 6.6.6 Function Management

In addition to specifying the authority for the user, what functions that the user can have also can be specified.



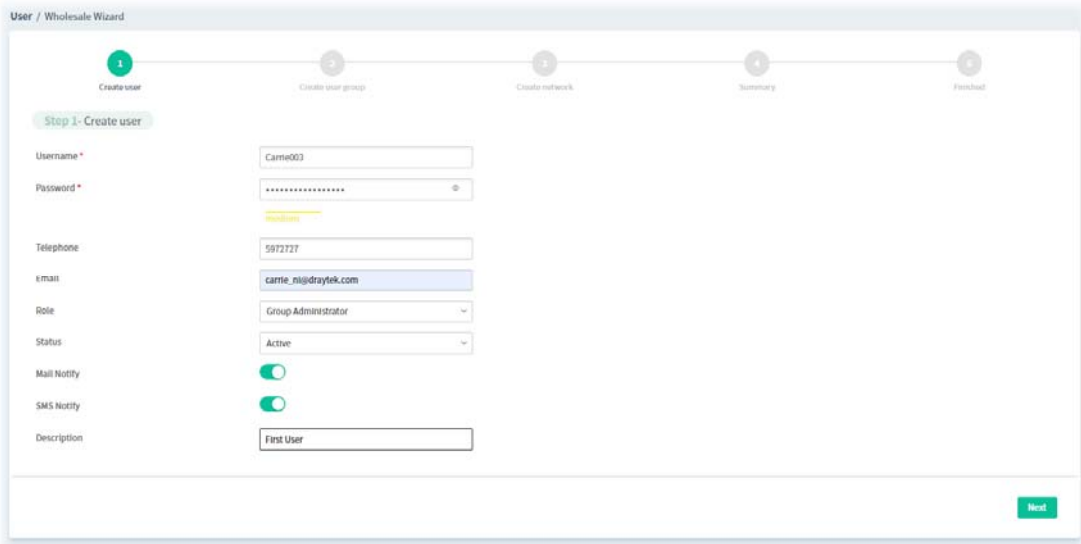

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Show Unknown Device** | Unknown device can be seen / hidden if it is enabled / disabled. |
| **Wireless is Writable** | When it is enabled, settings related to wireless connection are allowed to be configured. |
| **Show About Menu** | The About menu with information of VigorACS can be seen if it is enabled for the role. |
| **Can Delete Logs** | If enabled, logs can be deleted by the user with the role of System Administrator, Group Administrator and Administrator. |

### 6.6.7 Wholesale Wizard

This section can guide the administrator to a create user, user group and network profile via a wizard.

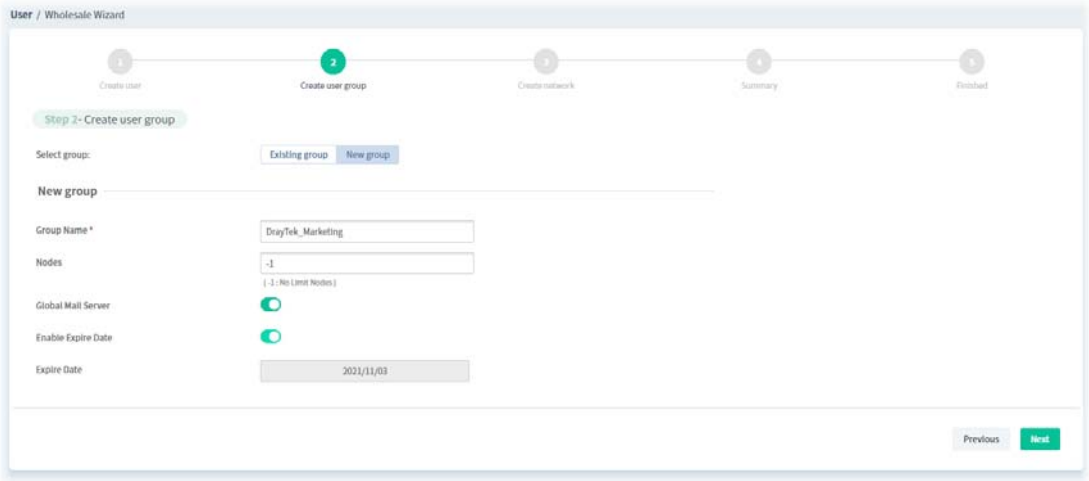
1. Open **User** >> **Wholesale Wizard.**




These parameters are explained as follows:

| Item | Description |
|---|---|
| **Username** | Enter a new name for a new user. |
| **Password** | Enter a new password. |
| **Telephone** | Enter the telephone number of such user for receiving the SMS notification. |
| **Email** | Enter the email address of such user for receiving the mail notification. |
| **Role** | Assign a Role for such user. |
| **Status** | Choose **Active** to make such user being seen on the network. |
| **Mail Notify** | When this function is enabled, an e-mail will be sent to the user as a notification when the device gets alarms. |
| **SMS Notify** | When this function is enabled, an SMS will be sent to the user as a notification when the device gets alarms. |
| **Description** | Give a brief introduction of such user. |
| **Next** | Go to next configuration page. |

2. When you finished tying the above settings, click **Next** to create a new group or specify an existing user group for such user.

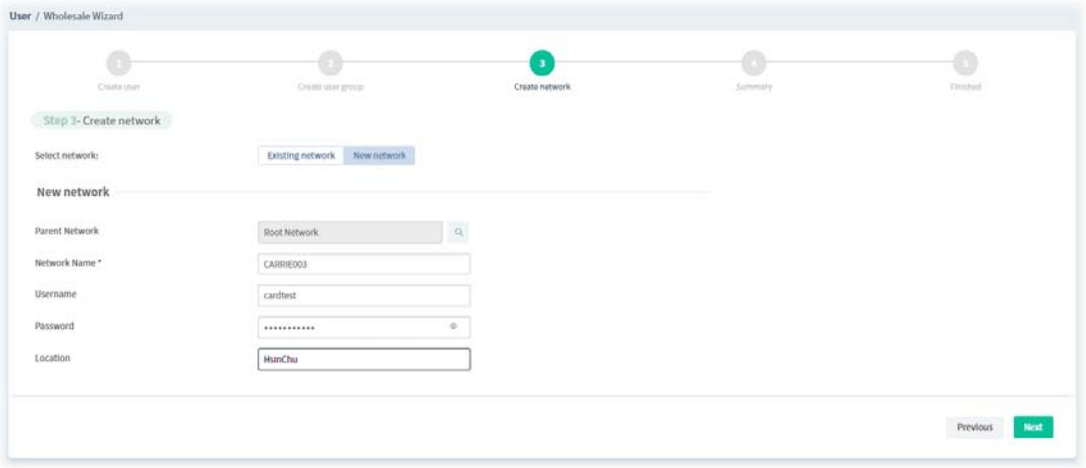



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Select group** | Determine the group source by choosing **Existing group** or New group. |
| **Existing group** | It is available when **Existing group** is selected as **Select group**.<br>**User group** – Use the drop down list to choose the group you want. |
| **New group** | It is available when **New group** is selected as **Select group**.<br>**Group Name** – Type the name (e.g., Marketing) that can represent the user group.<br>**Nodes** – Set the number of Nodes for such group. The default number "-1" means there is no limit of the number.<br>**Global Mail Server** –Click to enable /disable the global mail server.<br>**Enable Expire Data** – Click to enable /disable the expire date setting.<br>**Expire Date** - Use to pop-up calendar to specify the expire date. |
| **Previous** | Back to previous configuration page. |

| | |
|---|---|
| **Next** | Go to next configuration page. |

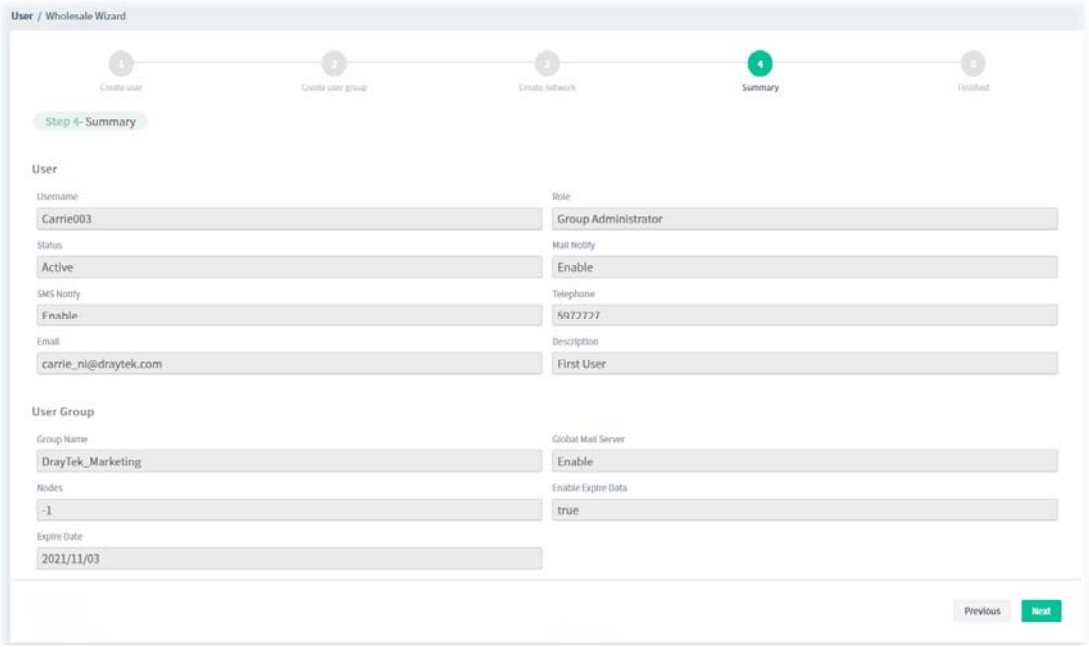
3. When you finished entering the above settings, click **Next** to create or specify an existing network for such user.



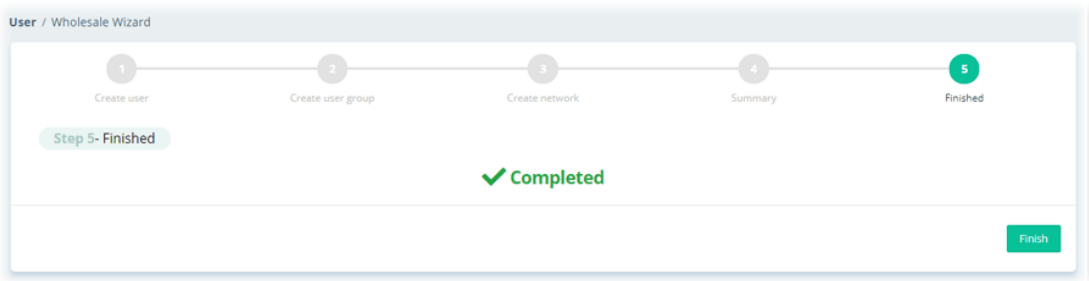

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Select network** | Determine the group source by choosing **Existing network** or New network. |
| **Existing network** | It is available when **Existing network** is selected as **Select network**.<br>**Network** – Use the drop down list to choose the network you want. |
| **New network** | It is available when **New network** is selected as **Select network**.<br>**Parent Network -** Choose one of the existing networks as the Parent Network.<br>**Network Name** – Enter a name for the new network.<br>**User Name** – Enter a name (e.g., market) for the new network.<br>**Password** – Enter a password (e.g., market) for such new network.<br>**Location** - Enter a brief description for the new network. |
| **Previous** | Back to previous configuration page. |
| **Next** | Go to next configuration page. |

4. When you finished tying the above settings, click **Next** to review the settings. A summary for the new user and network will be displayed as the following figure.



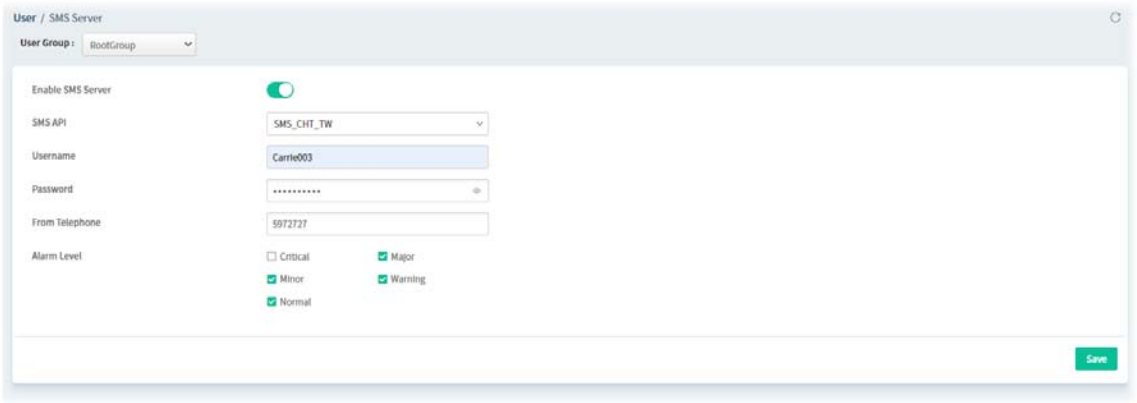

5. If nothing shall be modified, click **Next** to get the following page.




6. Click **Finish** to save the settings.

## 6.6.8 SMS Server

It is used to configure the SMS server for sending notification. When a CPE in a group encounters an event which can be classified as the level defined in this page, a SMS will be sent out for notification.



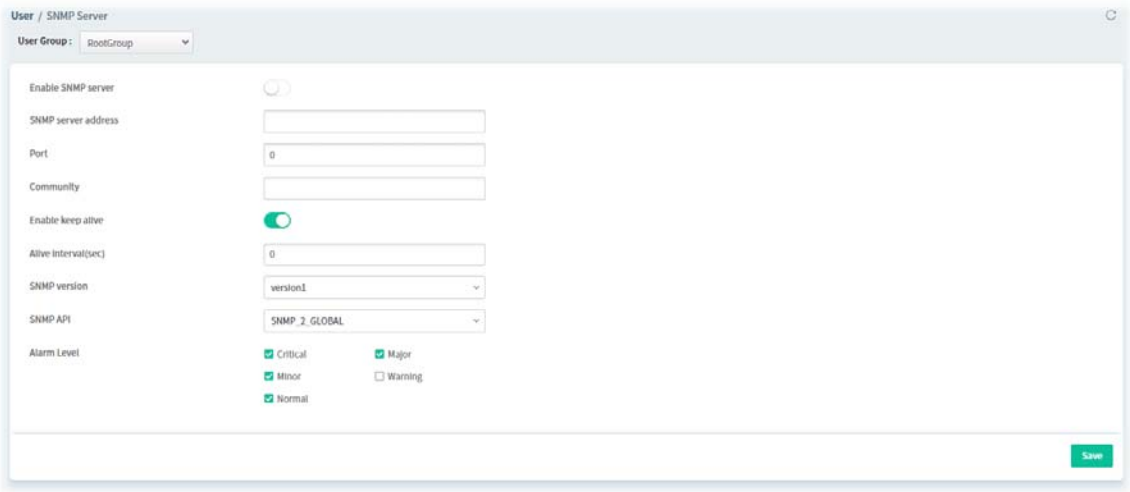

These parameters are explained as follows:

| Item | Description |
|---|---|
| **User Group** | Specify a user group to apply the SMS server settings. |
| **Enable SMS Server** | Click to enable /disable the SMS server. |

| | |
|---|---|
| **SMS API** | Use the drop down list to choose an ISP for sending SMS. |
| **User Name** | Type the user name for authentication. |
| **Password** | Type the password for authentication. |
| **From Telephone** | Type the phone number of the sender. |
| **Alarm Level** | There are five alarm levels (Critical, Major, Minor, Warning and Normal) which determine the timing that VigorACS SMS server sends SMS to the recipient.<br>For example, device loss connection will be treated as “Critical” event. |
| **Save** | Save the current settings. |

### 6.6.9 SNMP Server

It is used to configure the SNMP server for sending notification. All of the user groups can apply the SNMP server settings configured in this page.

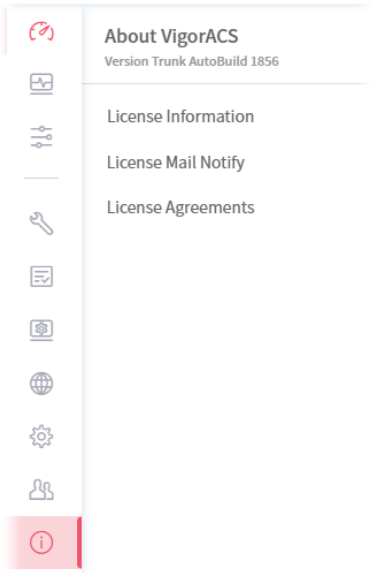



These parameters are explained as follows:

| Item | Description |
|---|---|
| **User Group** | Specify a user group to apply the SNMP server settings. |
| **Enable SNMP Server** | Click to enable /disable the SNMP server. |
| **SNMP server address** | Enter the IP address of SNMP server. |
| **Port** | Enter the port number of SNMP server. |
| **Community** | Set the name for getting community by typing a proper character. In general, it depends on the setting that SNMP service provider offers. The default setting is **public.** |
| **Enable keep alive** | It is available when RootGroup is selected as User Group.<br>Click to enable / disable keep alive function. VigorACS will notify SNMP server every period of time automatically to proof that it is still alive. |
| **Alive interval (sec)** | It is available when RootGroup is selected as User Group.<br>Enter an interval value for keeping alive. |
| **SNMP version** | Choose the version of the SNMP server that you apply to. |
| **SNMP API** | Choose SNMP API from the drop down list. |

| | |
|---|---|
| **Alarm Level** | There are five alarm levels (Critical, Major, Minor, Warning and Normal) which determine the timing that VigorACS mail server sends e-mail to the recipient. Specify the severity level of the mail. |
| **Save** | Save the current settings. |

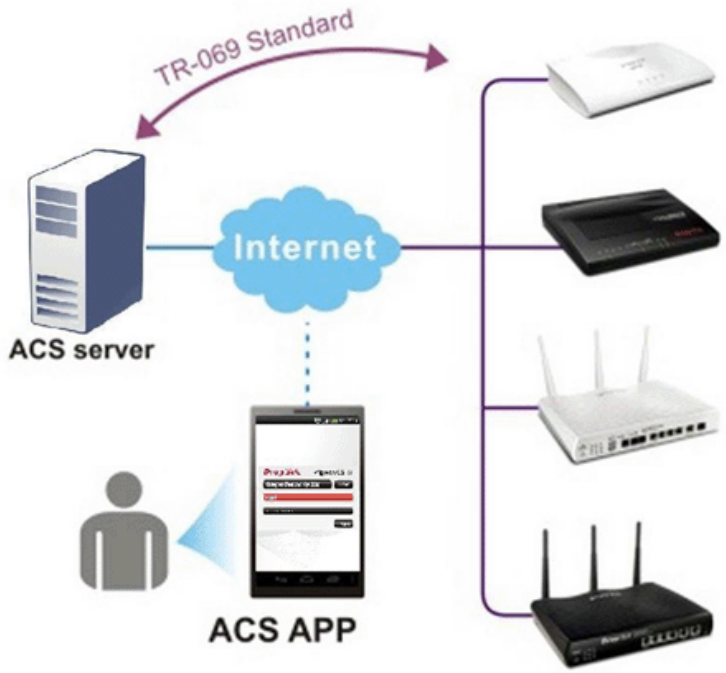
## 6.7 About VigorACS




About VigorACS menu varies according to the role (**System Administrator**, **Group Administrator**, **Administrator, Operator, View Only Operator, Auditor** and **Standard** (limited in VigorACS cloud version)) used for logging into VigorACS. Here we take System Administrator as an example.

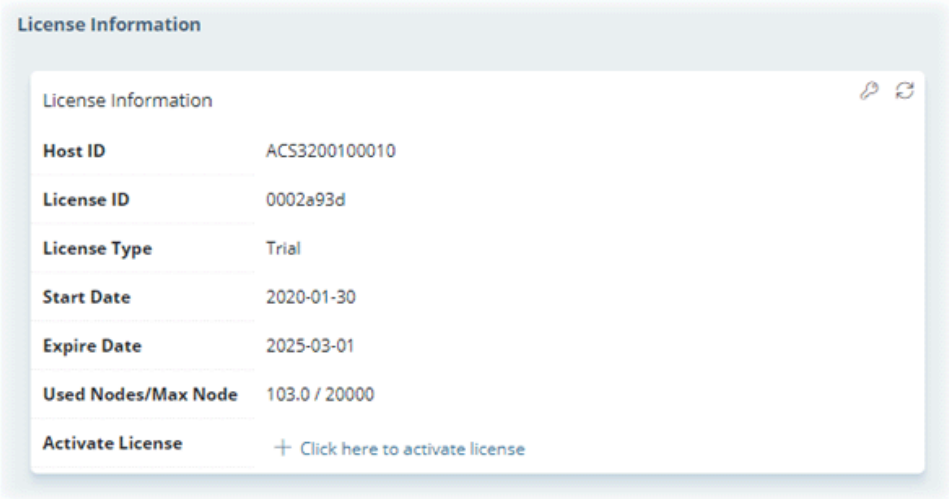
Android APP and software version information for VigorACS will be displayed as follows:

If your mobile phone is supported by Android system, you can use it to scan Android APP or Server Address QR code to connect to VigorACS system.



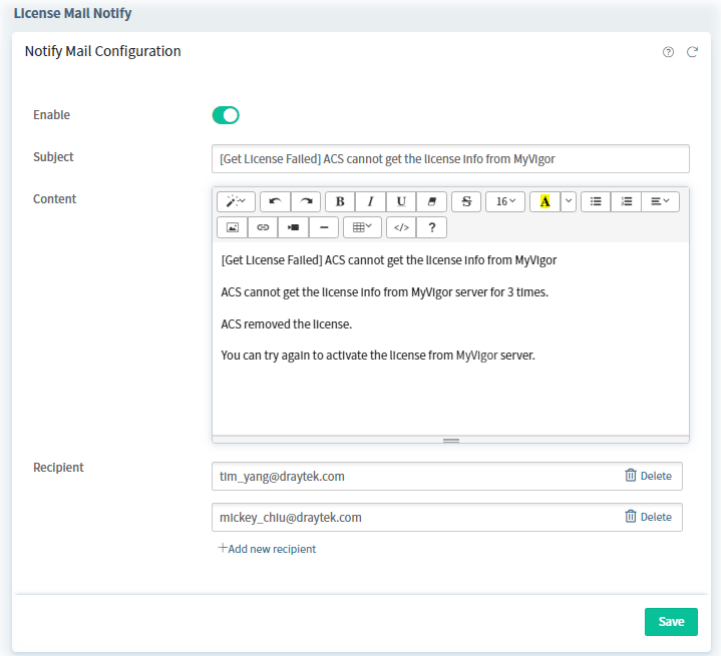

### 6.7.1 License Information

This page displays relational information for license key current used by VigorACS 3. In addition, it offers a channel to new the license key for VigorACS 3 when it is going to be expired.



### 6.7.2 License Mail Notify

When the ACS license synchronization fails and VigorACS cannot work, the VigorACS server system will send a email to the system administrator to notify the abnormal situation.

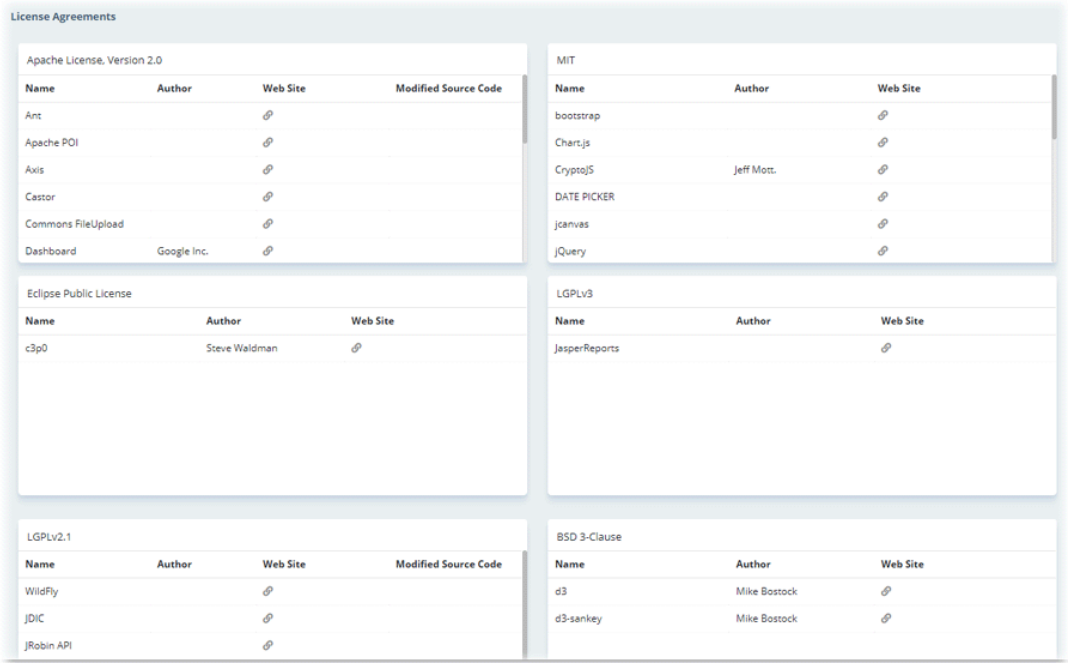



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Click to enable /disable the mail notification function. |
| **Subject** | Enter the subject of the mail. |
| **Content** | Enter the actual text for informing the recipient. |
| **Recipient** | Enter the e-mail address of the one to receive the mail. |
| **+Add new recipient** | Click to enter a new e-mail address. |
| **Delete** | Click to remove the selected e-mail address. |
| **Save** | Save the current settings. |

### 6.7.3 License Agreements

This page displays relational license information required by VigorACS 3.

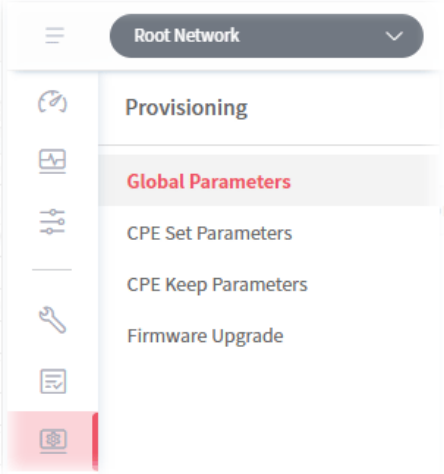


# Applications

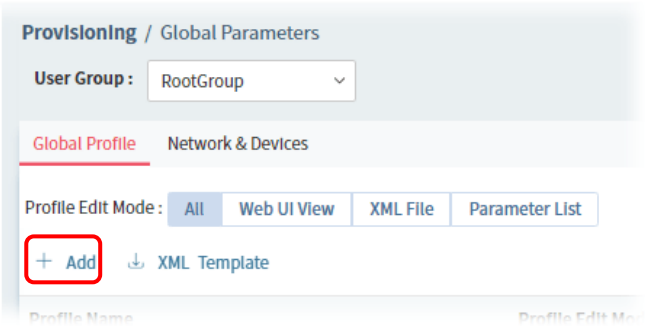
## A.1 How to Create a Provision Profile with Global Parameters?

This section briefly shows a simple way to register a CPE onto VigorACS 3 with few steps.

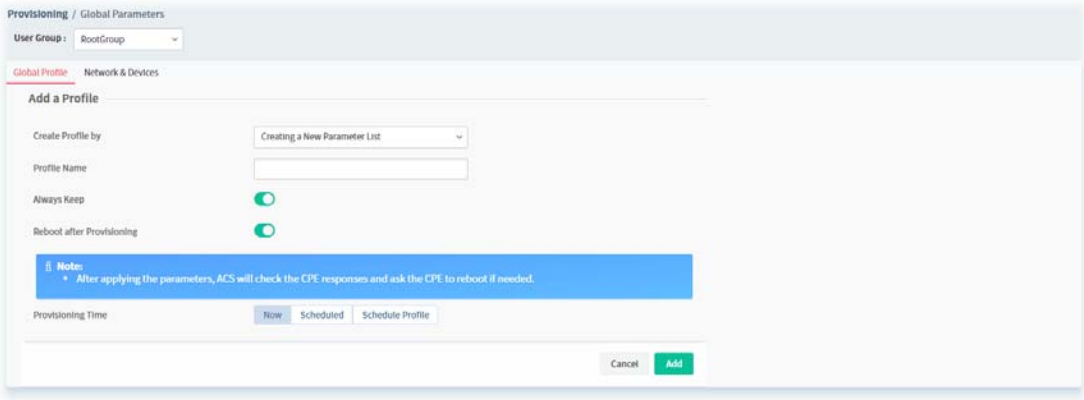
1. Open **Provisioning**>> **Global Parameters**.



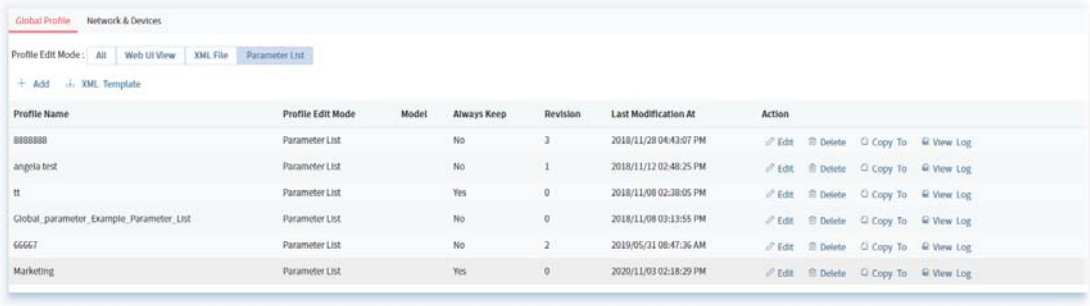

2. Select the **Global Profile** tab and click +**Add**.




3. From the following window, select Creating a New Parameter List, enter the Profile Name, enable the function of keeping the parameters and set the Provisioning Time.

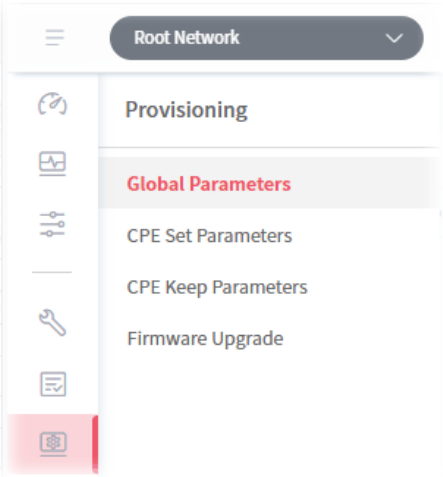


4. After finished the settings, click **Add**. The new profile will be displayed on the web page.

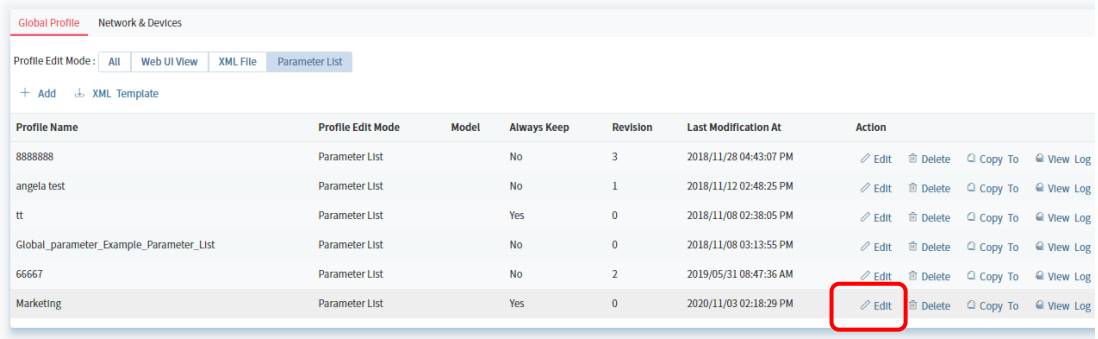



## A.2 How to Modify Provision Profile with Global Parameters?

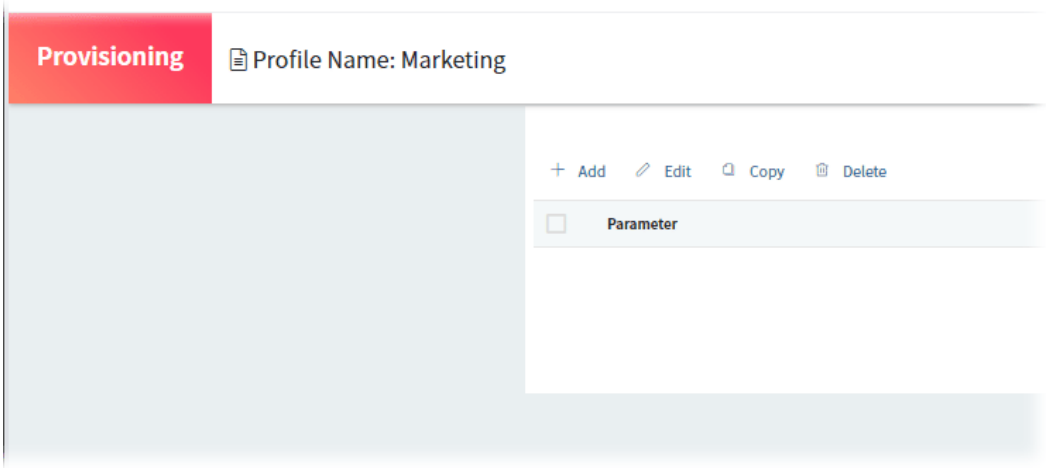
1. Open **Provisioning**>> **Global Parameters**.



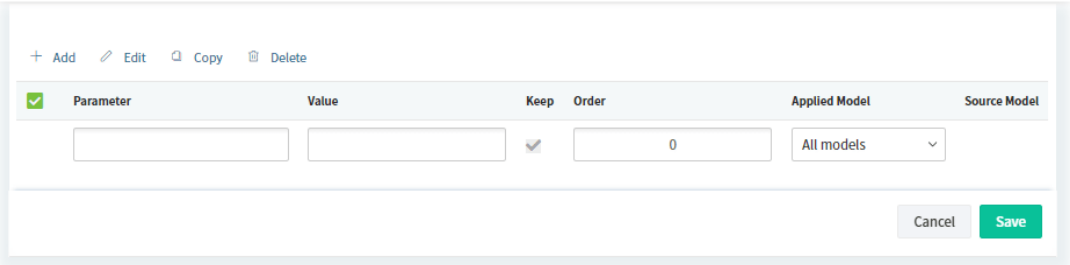

2. Choose the profile (e.g., Marketing) you want to modify and click **Edit.**



3. Click the **Edit** link in this page.



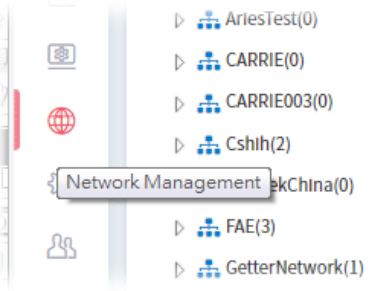

4. Modify the **Value, Keep, Order** and **Applied Model** if you are not satisfied with the configuration above and want to make change. After finished the changes, click **Save**.



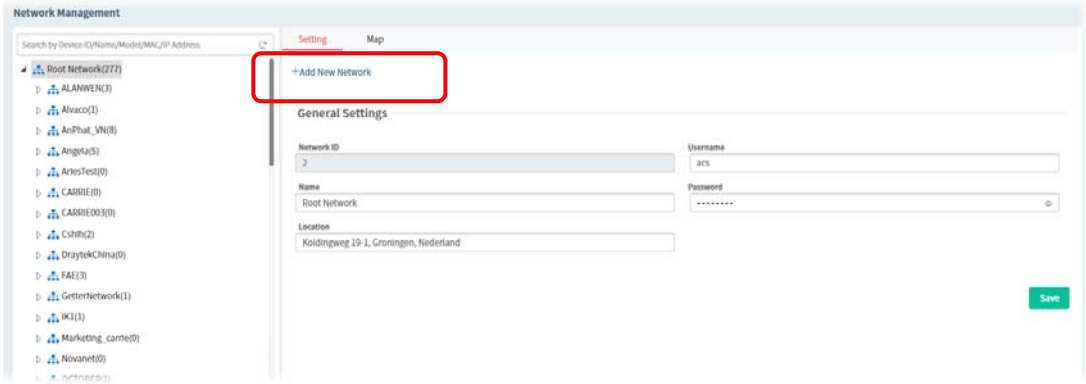

For the detailed information of parameters definition, refer to User's Guide of each device if required.

## A.3 How to Create a Network for Managing Devices?

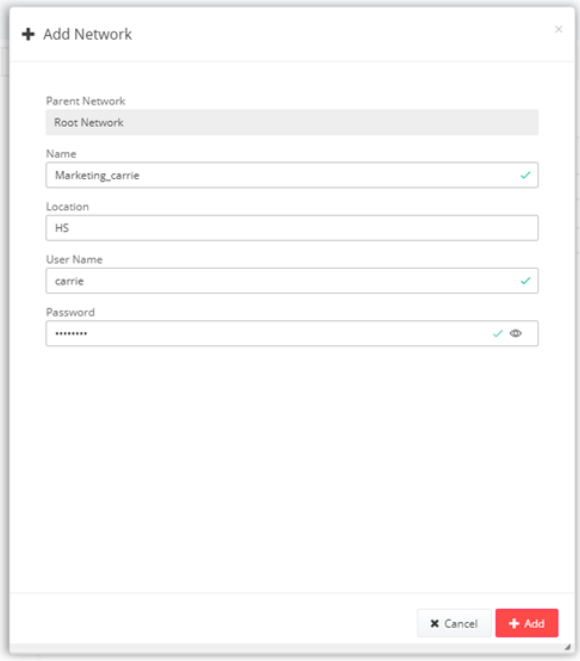
1. Open **Network Management.**



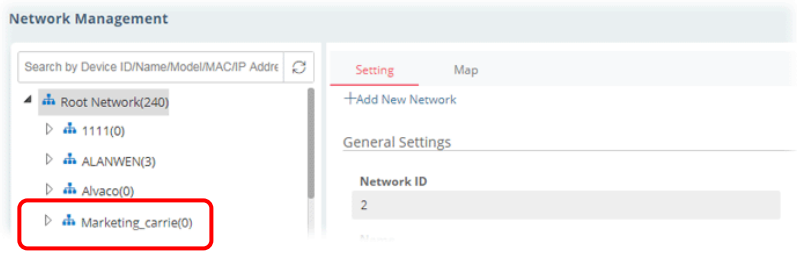

2. Click **+Add New Network** on the **Setting** page.




3. In the following page, type required information for the new network.

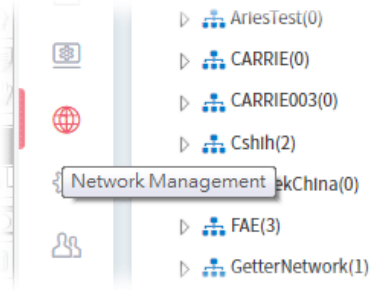



4. Click **Add**.
5. The new network has been created and displayed on the tree view.

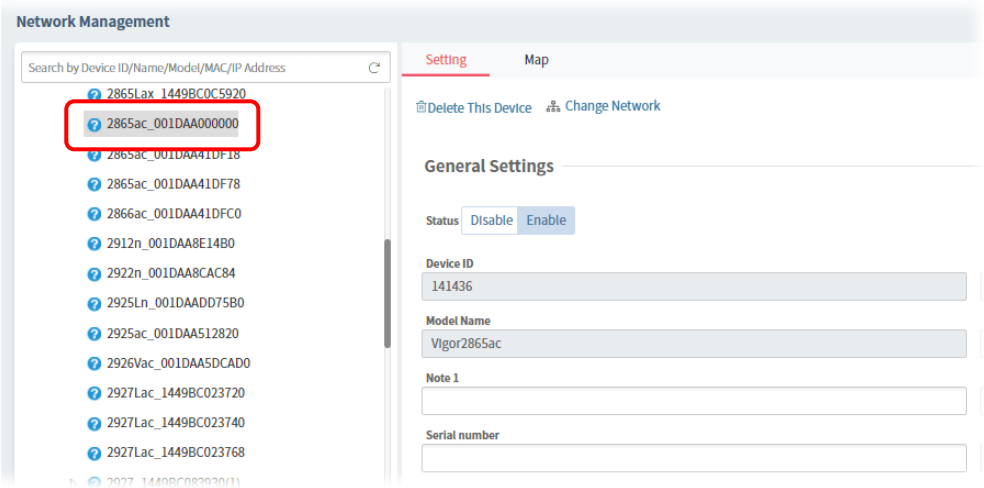



## A.4 How to Change the Network of a Device?

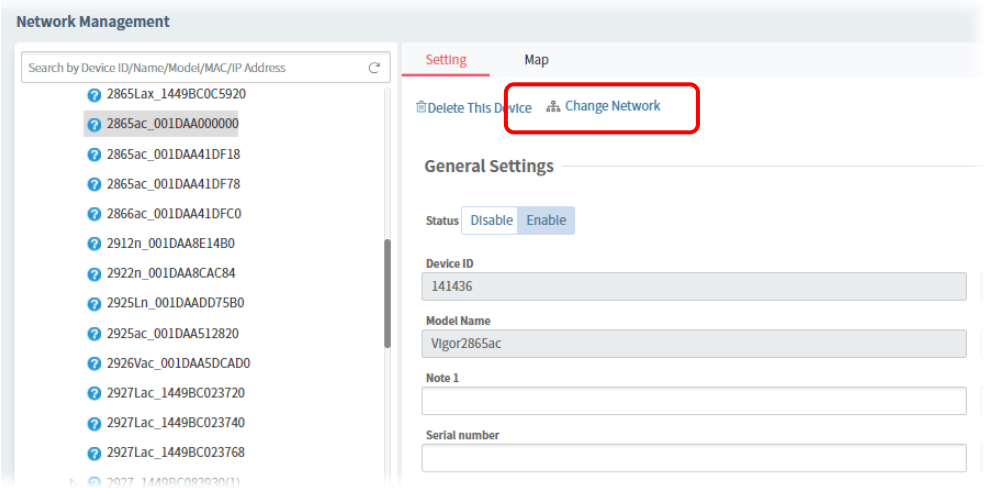
1. Open **Network Management.**



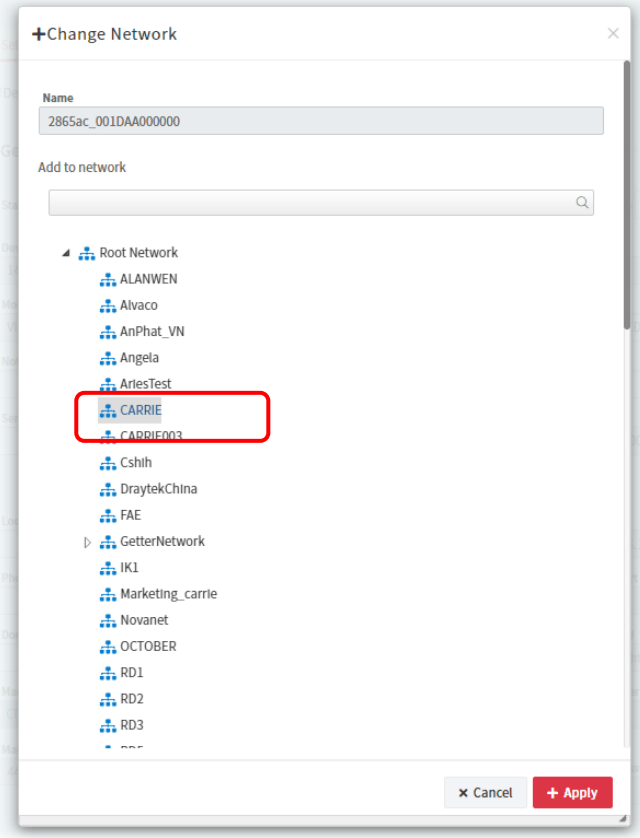

2. Choose and click a CPE displayed on **Root Network** tree view.

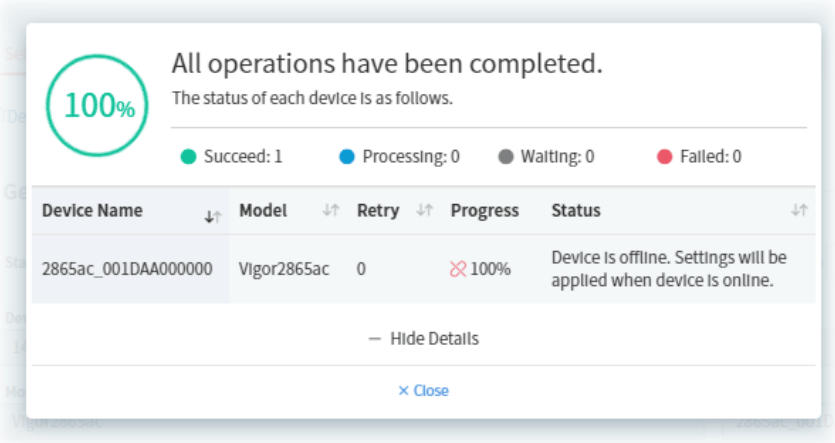



3. Click **Change Network.**

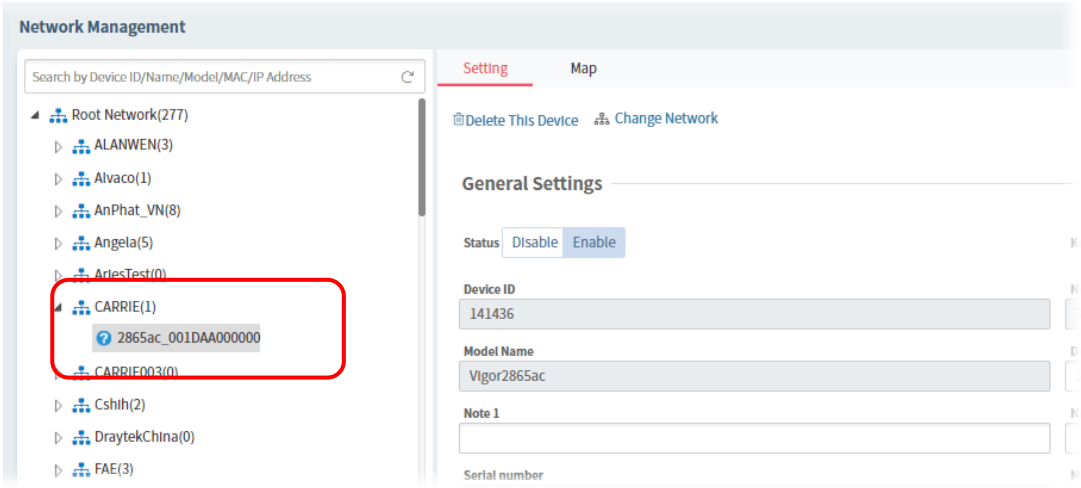


4. Click the network you want from **Root Network** and click **Apply**.



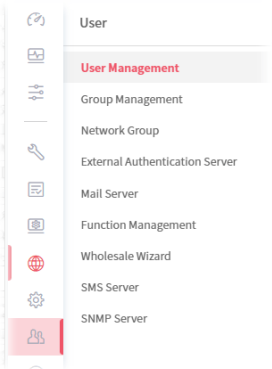



5. The selected device has been grouped under the specified network (CARRIE, in this case).

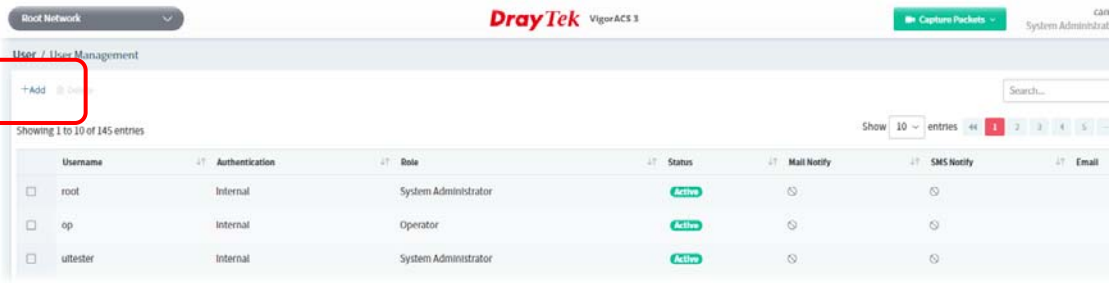


## A.5 How to Add a User?

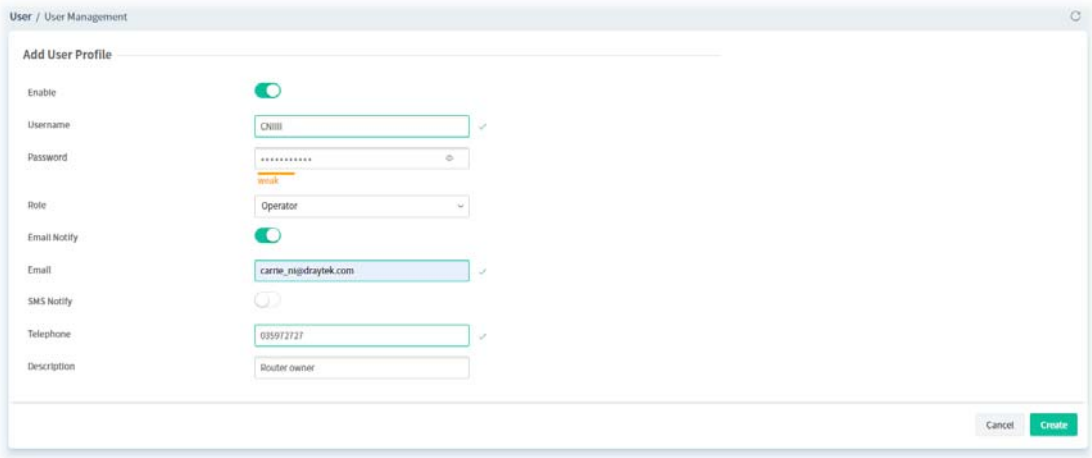
1. Open **User**>>**User Management.**



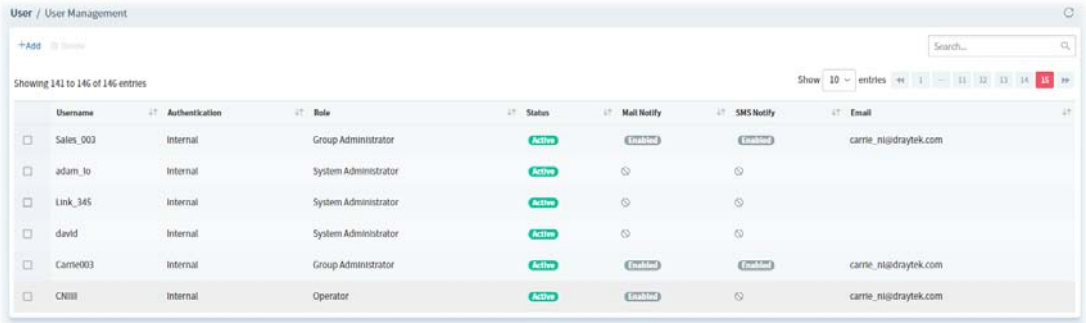

2. Click **+Add**.




3. In the following page, type required information for the new user.

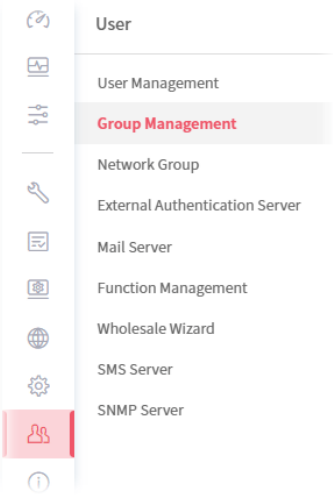



4. Click **Create**.

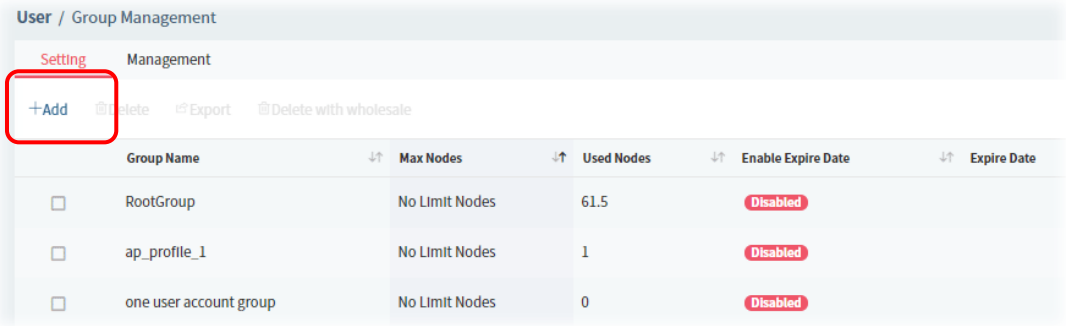


## A.6 How to Add a Group?

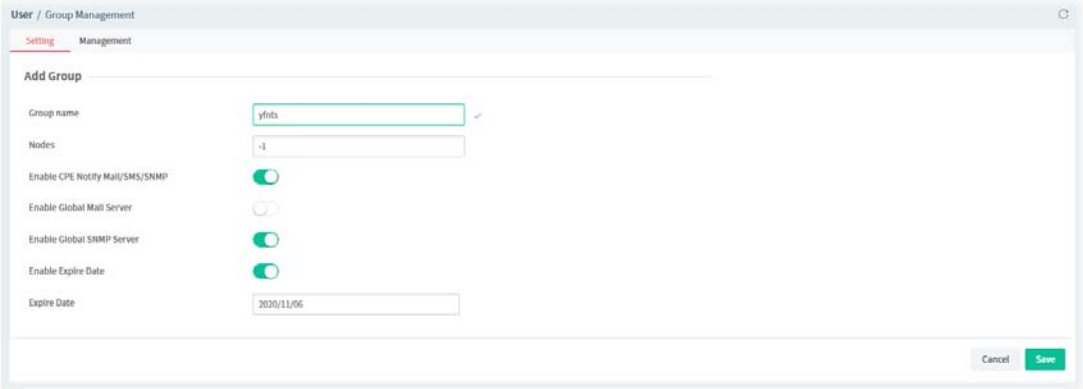
1. Open **User**>>**Group Management.**




2. Click **+Add**.

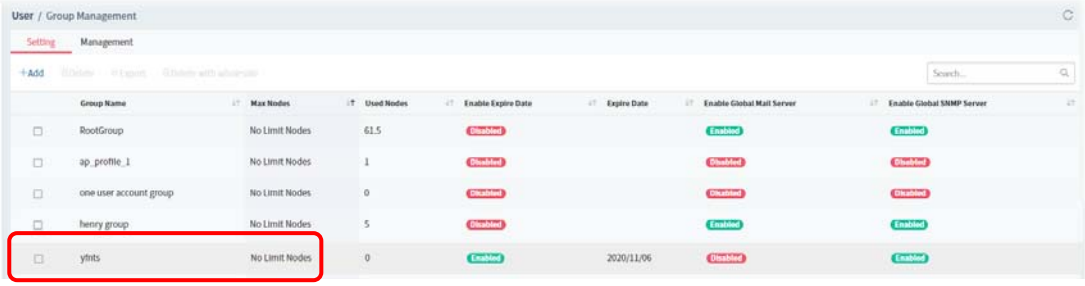



3. In the following page, type required information for the new user group.




- Group Name - Enter a new name of the user group.
- Nodes – Define number of node.
- Enable CPE Notify Mail/SMS/SNMP Server – Click to enable /disable global mail server.
- Enable Global Mail Server – Click to enable /disable global mail server.
- Enable Global SNMP Server – Click to enable /disable global SNMP server.
- Enable Expire Date – Click to enable/disable the expire date.
- Expire Date – Choose the expire date for such user group.

4. Click **Save**.


User / Group Management
Setting
Management
+Add
Search...
Group Name
Max Nodes
Used Nodes
Enable Expire Date
Expire Date
Enable Global Mail Server
Enable Global SNMP Server
RootGroup
No Limit Nodes
61.5
Disabled
Enabled
ap_profile_1
No Limit Nodes
1
Disabled
Disabled
Disabled
one user account group
No Limit Nodes
0
Disabled
Disabled
Disabled
henry group
No Limit Nodes
5
Disabled
Enabled
Enabled
yfnts
No Limit Nodes
0
Enabled
2020/11/06
Disabled
Enabled

This page is left blank.

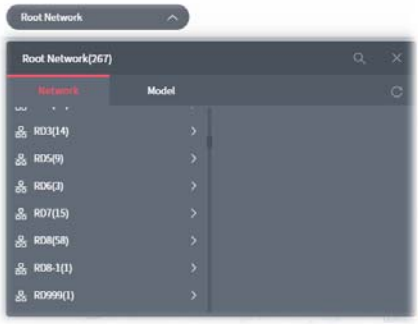
# Part IV

## Network Menu

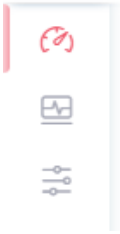
# Chapter 7 Root Network Menu

Network contains two types, Root Network and User-defined Network (e.g., RD8). For the user-defined network group, refer to Chapter 5.

Use the drop-down menu on the top of the left side to select a network group.




On the dashboard for root network, the Network menu contains:

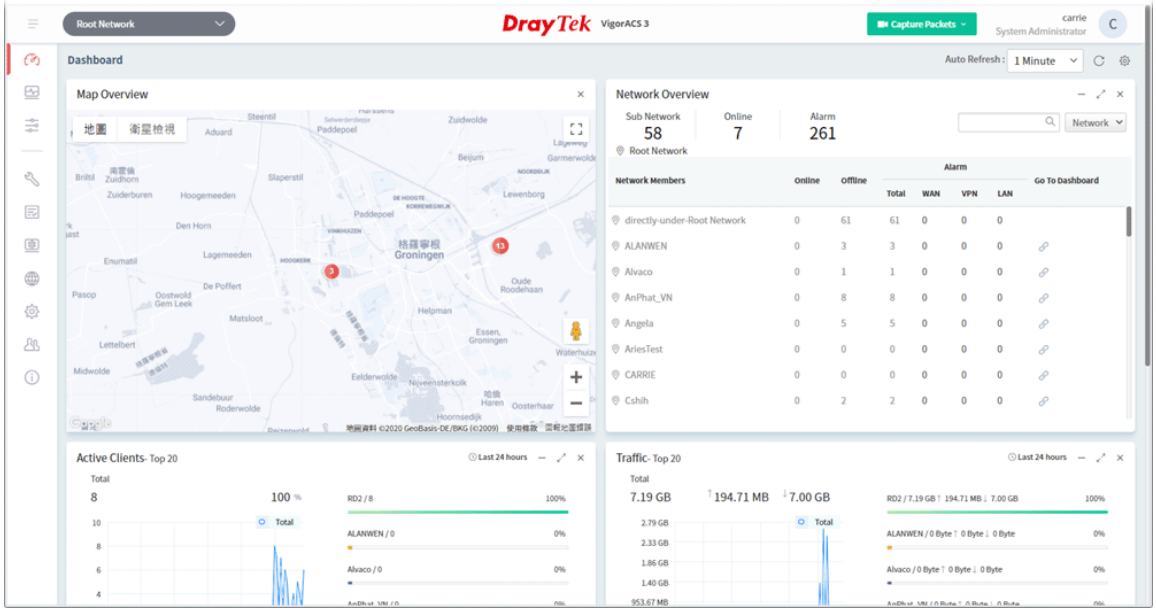


Dashboard

Monitoring

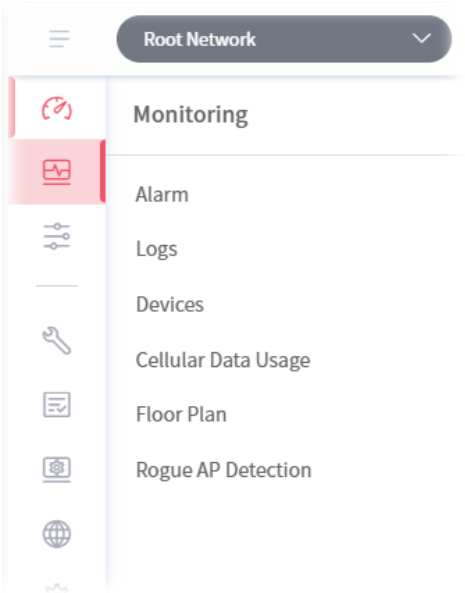
Configuration

## 7.1 Dashboard for the Root Network



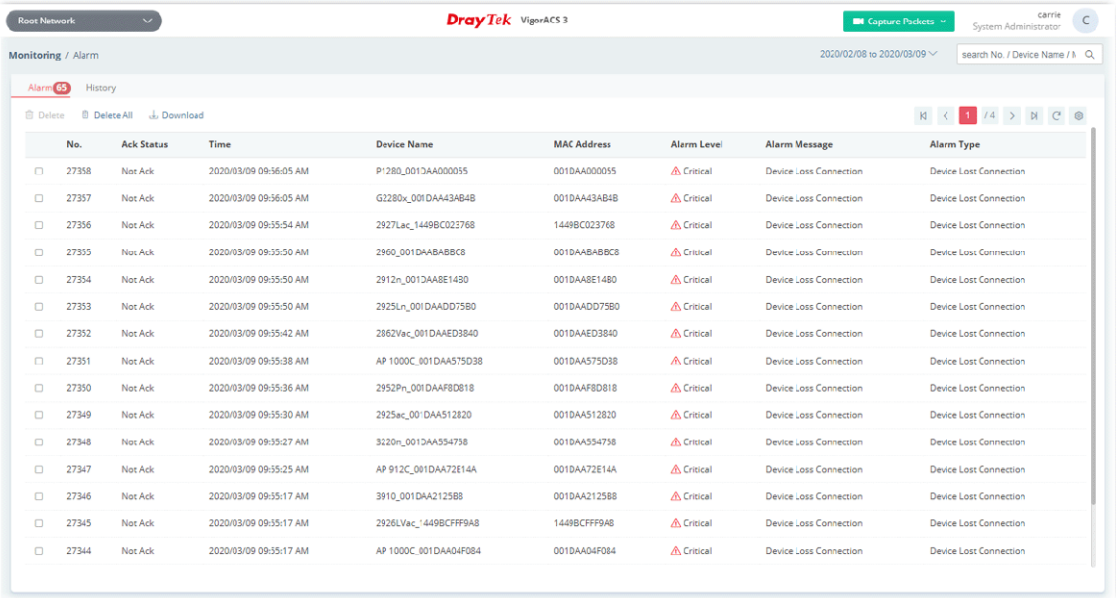
## 7.2 Monitoring

Monitoring menu offers options for monitoring the normal and abnormal actions for root network, network group and CPE. This section offers Monitoring menu items for the root network.



### 7.2.1 Alarm

Alarm message will be recorded on VigorACS 3 server when there is a trouble happened to the device (CPE). Only the users within the same user group will be notified for the message.

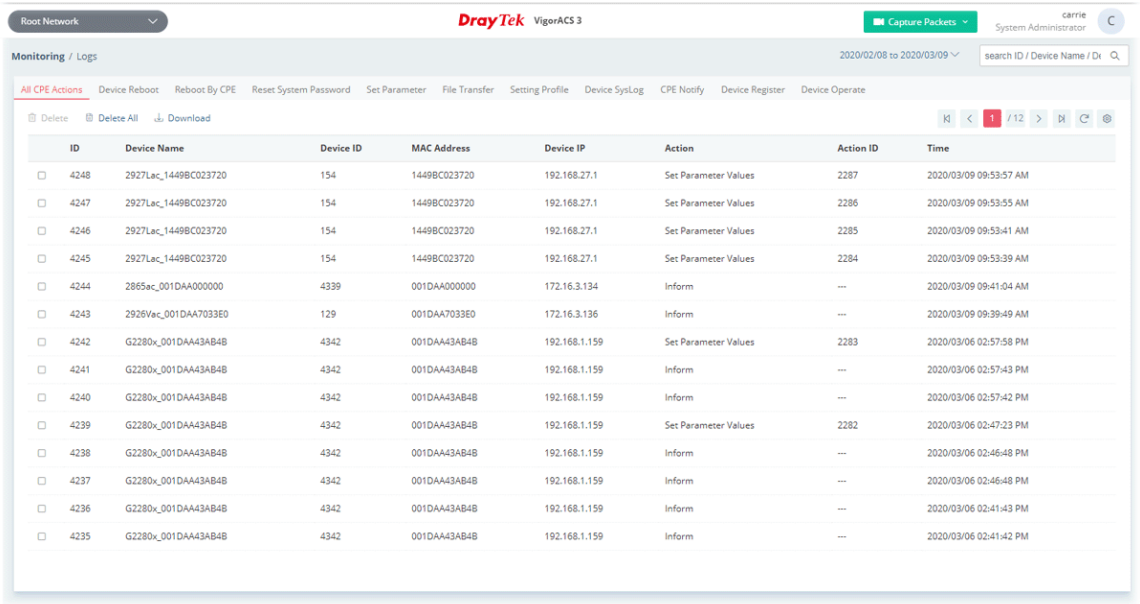



These parameters are explained as follows:

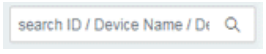
| Item | Description |
|---|---|
| **Alarm / History** | **Alarm –** Display the alarm records recently.<br>**History –** Display all the alarm records that have been solved and cleared. |
| **Delete** | Clear the alarm record which has been solved by VigorACS 3. |
| **Delete All** | Clear all of the alarm records which have been solved by VigorACS 3. |
| **Download** | Click this button to save alarm log as a XLS file. |
| **No.** | Display the index number of the alarm. It is offered by VigorACS 3 automatically. |
| **Ack Status** | Display the status of the records with the type specified here (Not Ack or Acked). |
| **Time** | Displays the time of the device to be monitored. |
| **Device Name** | Displays the name of the monitored device. |
| **MAC Address** | Displays the MAC address of the monitored device. |
| **Alarm Level** | Displays the alarm message with the severity (e.g., Critical) specified. |
| **Alarm Message** | Displays a brief explanation for the alarm sent by VigorACS 3 automatically. |
| **Alarm Type** | Displays the alarm message with the type specified. |

### 7.2.2 Logs

Log provides administrator records for action executed, device name, MAC address, Device IP, CommandKey, and Current Time for CPE device managed and monitored by VigorACS.



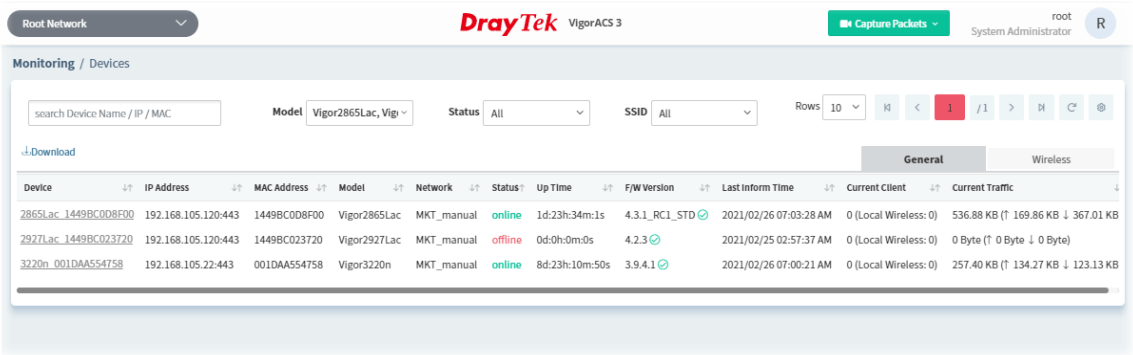

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Log Type** | Click one of the tabs (e.g., All CPE Actions, Device Reboot, Reboot By CPE, Reset System Password, Set Parameter, File Transfer, Setting Profile, Device SysLog, CPE Notify, Device Register, Device Operate and etc.) to display related log on this page. |
|  | Enter the condition for VigorACS to search and display relational information. |
| **Delete** | Clear the alarm record which has been solved by VigorACS. |
| **Delete All** | Clear all of the alarm records which have been solved by VigorACS. |
| **Download** | Click this button to save the log as an XLS file. |

### 7.2.3 Devices

The administrator (user) can check information (such as Device name, IP address, MAC address, model name, network, status, up time, firmware version, number of current connected client, data traffic, and so on) of CPE under the selected network group by this page. The network group (e.g., Root Network in this case) selected above is the group to be monitored and information related to this selected network group will be shown below.

Simply open **Monitoring>>Devices** to get the following page.

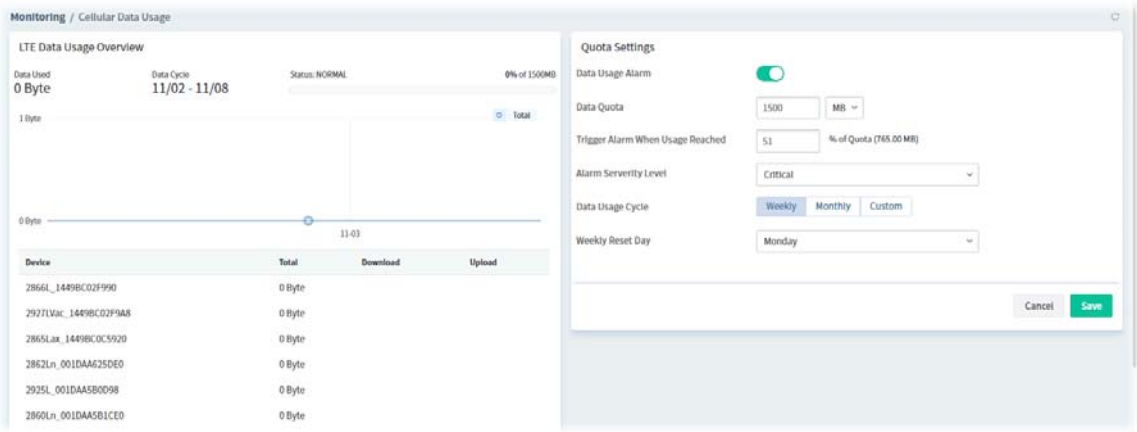



These parameters are explained as follows:

| Item | Description |
|---|---|
| search Device Name / IP / MAC | Enter the condition for VigorACS to search and display relational information. |
| **Model** | This area lists all of the devices that monitored by VigorACS.<br>Check **Select all** to display information for all of the devices; or check the name of the device to display the information related to the selected device. |
| **Status** | **Online** – This page displays information for the device which is online currently.<br>**Offline** – This page displays information for the device which is offline currently.<br>**All** – This page displays information for all of the devices no matter it is online or offline. |
| **SSID** | This area lists information for CPE with wireless features monitored by VigorACS.<br>Check **All** to display all of the devices; or check the name of the device to display the information related to the selected device.<br>**SSID** - SSIDs for CPE with wireless features will be displayed in this drop down list. Choose one of the SSIDs. Information related to the selected SSID will be displayed on this page. |
| **General / Wireless** | **General** – List the general information for the CPE under the selected group.<br>**Wireless** – List only the wireless information for the CPE under the selected group. |
| **Download** | Click this button to save information for monitored devices as an XLS file. |

### 7.2.4 Cellular Data Usage

This page displays traffic information including data used, data cycle, status, percentage, downloaded data, uploaded data for device equipped with LTE features (such as Vigor2925Ln, Vigor2860Ln and so on). The values defined in **Quota Settings** indicate total amount of quota for all LTE devices managed by VigorACS.



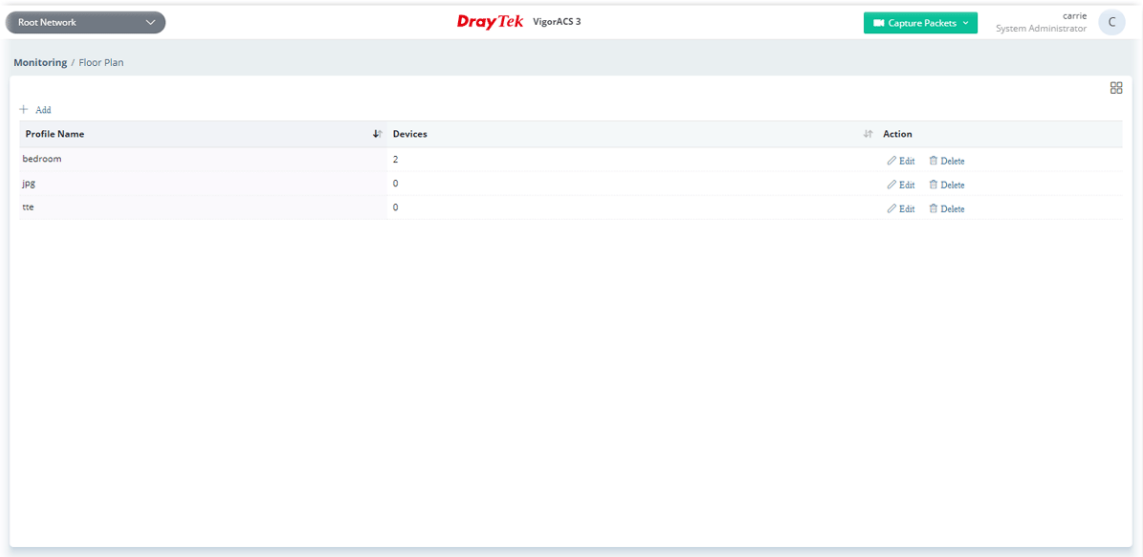

These parameters are explained as follows:

| Item | Description |
|---|---|
| **LTE Data Usage Overview** | **Status** - The bar chart displays the data usage in yellow, green and grey based on values defined in **Quota Settings**. If data usage for the LTE model exceeds the percentage of quota configured in the field of **Trigger Alarm When Usage Reached** in Q**uota Settings**, the amount of used data will be shown in Yellow; if not, it will be displayed in Green. The rest quota will be shown in gray.<br>In addition, device name, throughput, downloaded data and uploaded data for each LTE can be seen on the table below this page. |
| **Quota Settings** | |
| **Data Usage Alarm** | When it is enabled, a warning message will be shown in the page of **DEVICE MENU>>Monitoring>>Alarm** once the data usage reaches the threshold defined in **Trigger Alarm When Usage Reached**. |
| **Data Quota** | The value (unit is MB/GB) defined here means total amount of data quota available for all LTE devices managed by VigorACS. |
| **Trigger Alarm When Usage Reached** | Set a threshold for triggering alarm mechanism. |
| **Alarm Severity Level** | Set the alarm severity (critical, major, minor, warning and normal). Such severity will be shown on **DEVICE MENU>>Monitoring>>Alarm** when the data usage for LTE model(s) reaches the threshold. |
| **Data Usage Cycle** | Select one of the options (Weekly, Monthly, Custom) as data usage cycle.<br>**Cycle Duration(days) –** When **Custom** is selected, please specify the cycle duration. The data quota for LTE model will be reset after the days configured here.<br>**Cycle Starts On** –When **Custom** is selected, specify one date as a starting point to reset the data quota for LTE model.<br>**Weekly Reset Day** - When **Weekly** is selected as Data Usage Cycle, please use the drop down list to choose one day (Monday to Sunday) for VigorACS to reset the data quota for LTE model. |

| | |
|---|---|
| | **Monthly Reset Day** - When **Monthly** is selected as Data Usage Cycle, please use the drop down list to choose a date for VigorACS to reset the data quota for LTE model. |
| **Cancel** | Discard current modification. |
| **Save** | Save the current settings. |

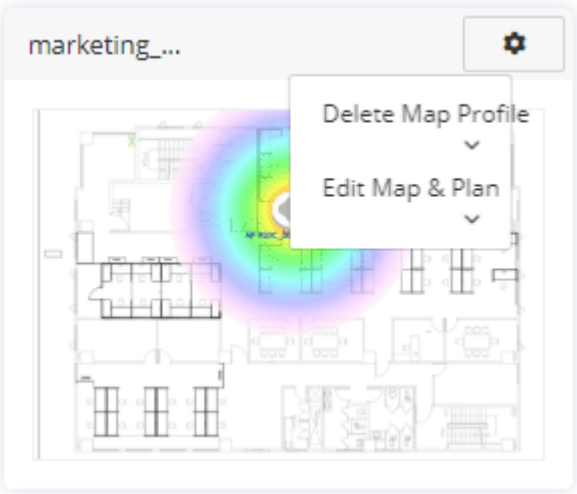
### 7.2.5 Floor Plan

This function is helpful to determine the best location for VigorAP in a room. A floor plan of a room is required to be uploaded first. By dragging and dropping available VigorAP icon from the list to the floor plan, the placement with the best wireless coverage will be clearly indicated through simulated signal strength.



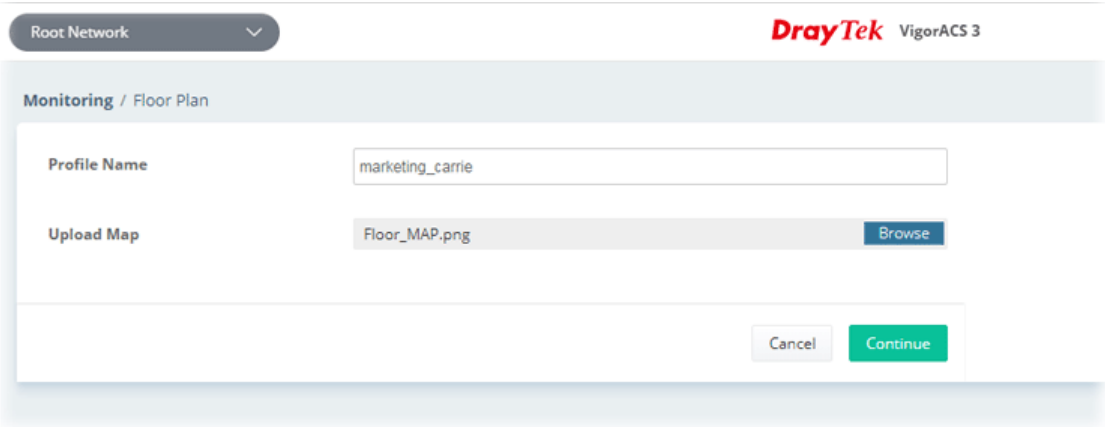

These parameters are explained as follows:

| Item | Description |
|---|---|
| **+Add** | Creates a new profile. |
| | Click to change to browse view.<br>It displays all of the floor plan profiles with the map used.<br> <br>You can click **Add** on this page to create a new profile. To modify the existed profile, click the icon on the right-top to display a drop down menu. Then click **Edit Map & Plan** to perform the modification, or click **Delete Map Profile** to remove the selected floor plan profile. |

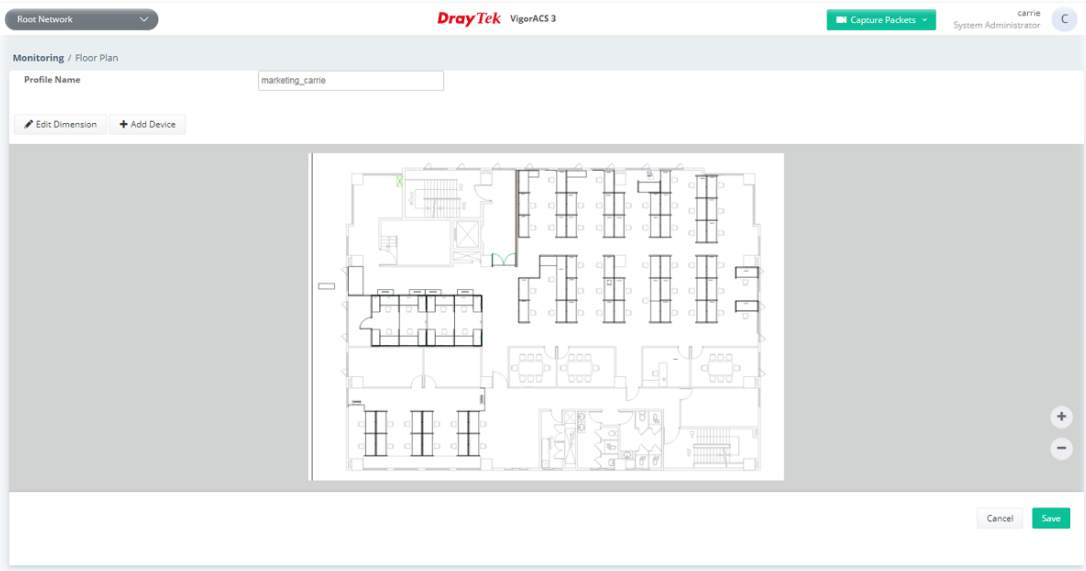
| | |
|---|---|
| |  |
| **Profile Name** | Displays the name of the floor plan profile. |
| **Device** | Displays the number of AP devices placed on the plan profile. |
| **Action** | **Edit** - Click to modify the profile.<br>**Delete** - Click to remove the selected profile. |

To create a new profile:

1. Click **+Add**.
2. From the following page, enter profile name (e.g., marketing_carrie) and click Browse to upload a map (e.g., Floor_MAP.png). Click **Continue**.



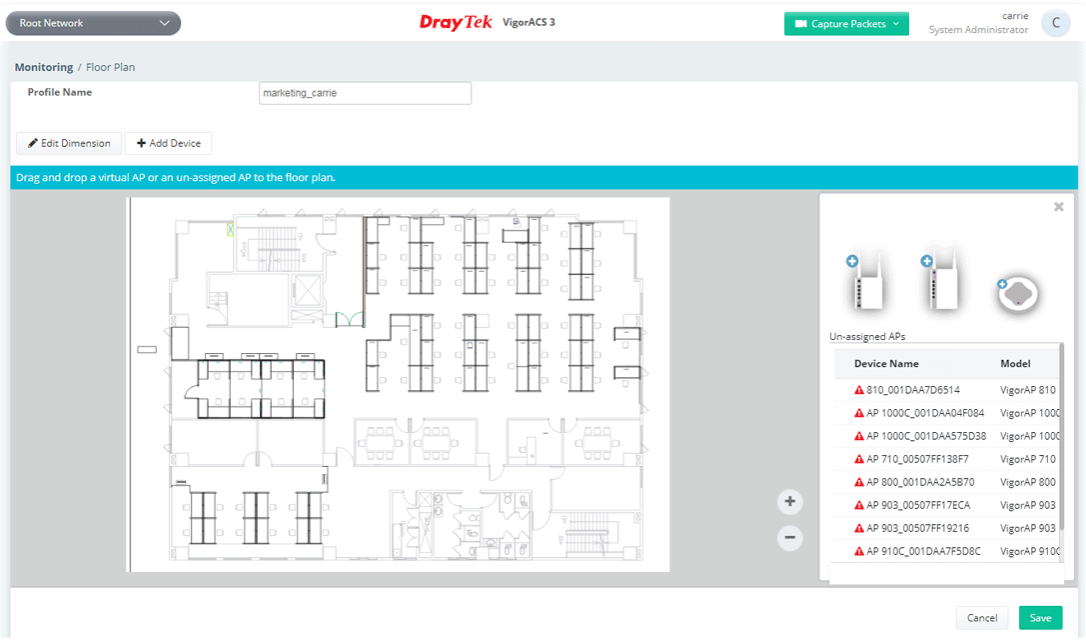
3. A floor map will be displayed on the screen.



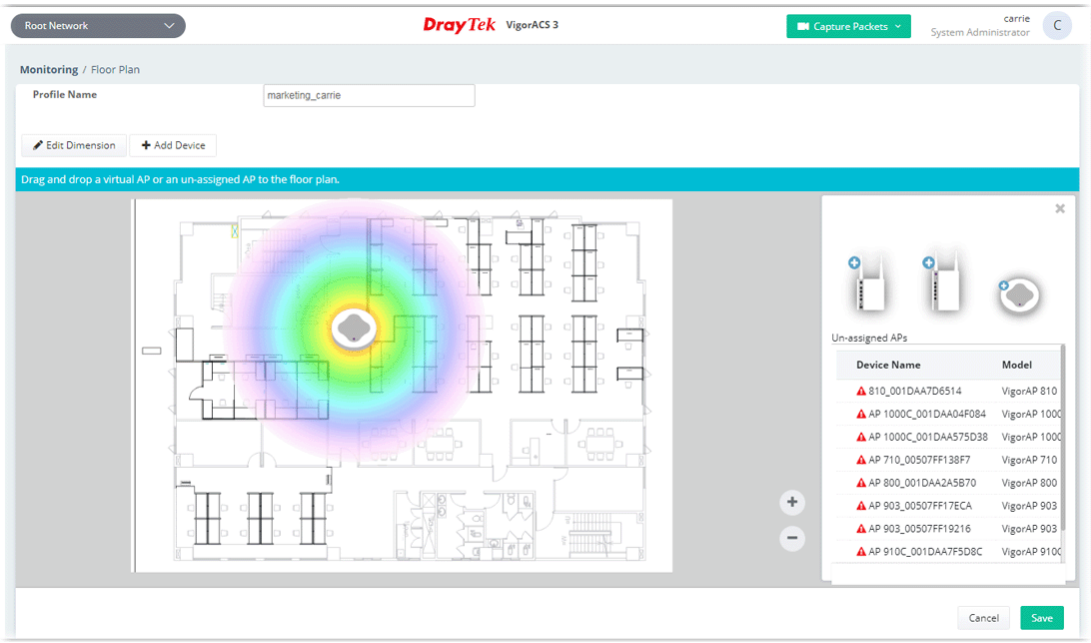

**Edit Dimension** – Draw a line and enter the distance of length / width of the map.

**Add Device** – Click to display available VigorAP to apply it on to the map.

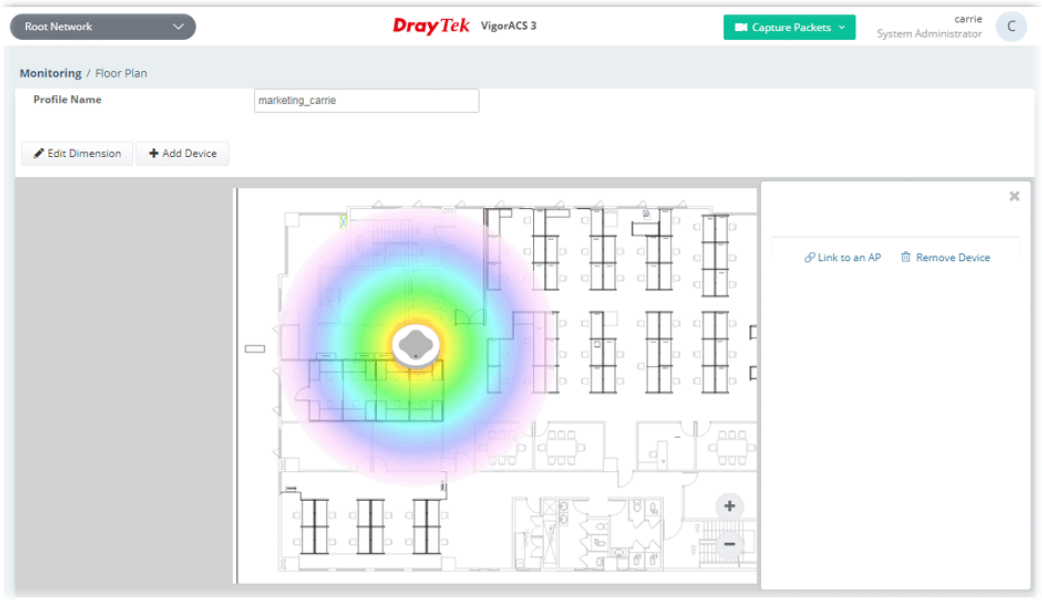
4. Click **+Add Device**. Available VigorAP icons and name list will be displayed on the right side of this page.



5. Select the AP you want (e.g., VigorAP910C icon, in this case) from right side of this page. Drag and drop the icon on the map. Later, an icon with effective signal range will be seen on the screen.



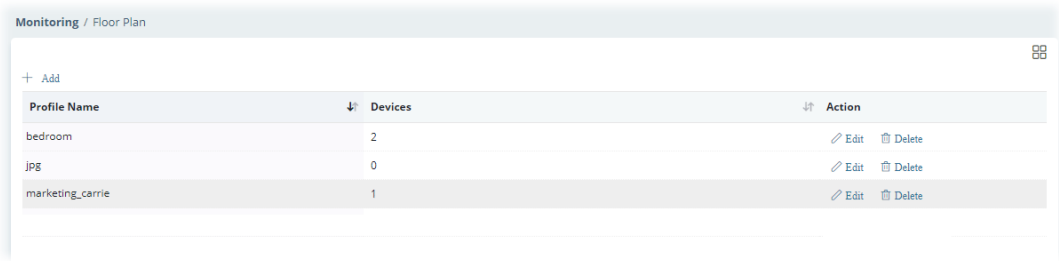

6. Slightly click the AP icon on the map. Two links of **Link to an AP** and **Remove Device** will be shown on the right side.




- **Remove Device** – If you do not satisfy the location of AP icon, click this link to remove the AP icon from the map.
- **Link to an AP** – If you satisfy the location of AP icon, click this link to select VigorAP. All of un-assigned AP names will be shown on the list. Choose the one you want and click Apply. Then such map has been connected with the specified AP.

7. Click **Link to an AP** to select the AP you want. After clicking **Apply**, the name of the VigorAP will be displayed below the icon on the map.

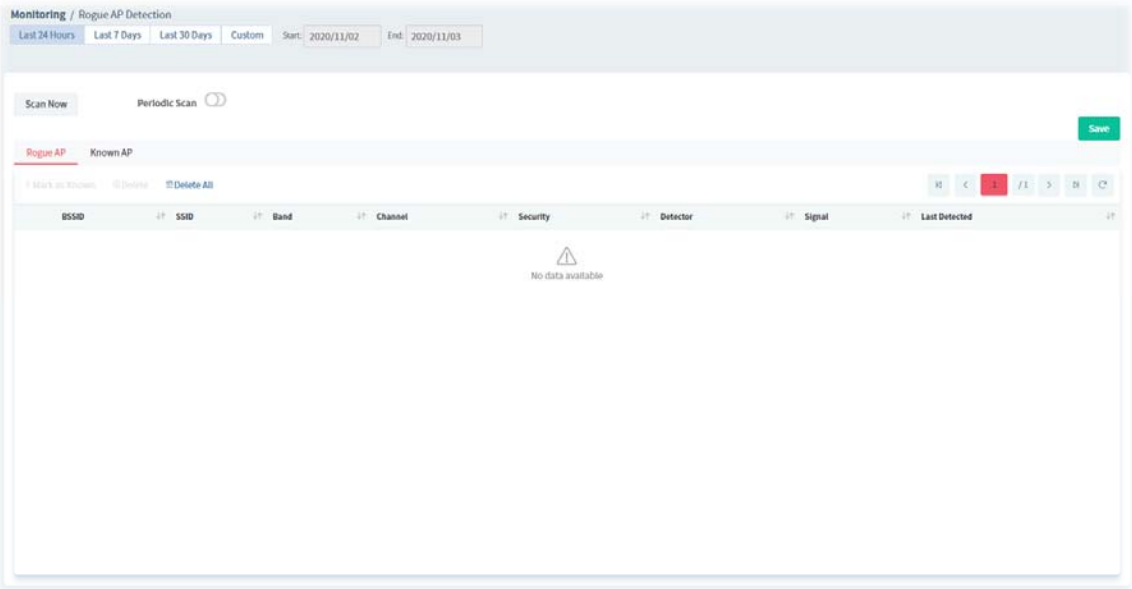
8. Click **Save**. The new created profile will be shown on the page.



### 7.2.6 Rogue AP Detection

Information detected by VigorAP can be displayed in this page. In which, the APs will be classified with rogue AP and known AP in different colors.

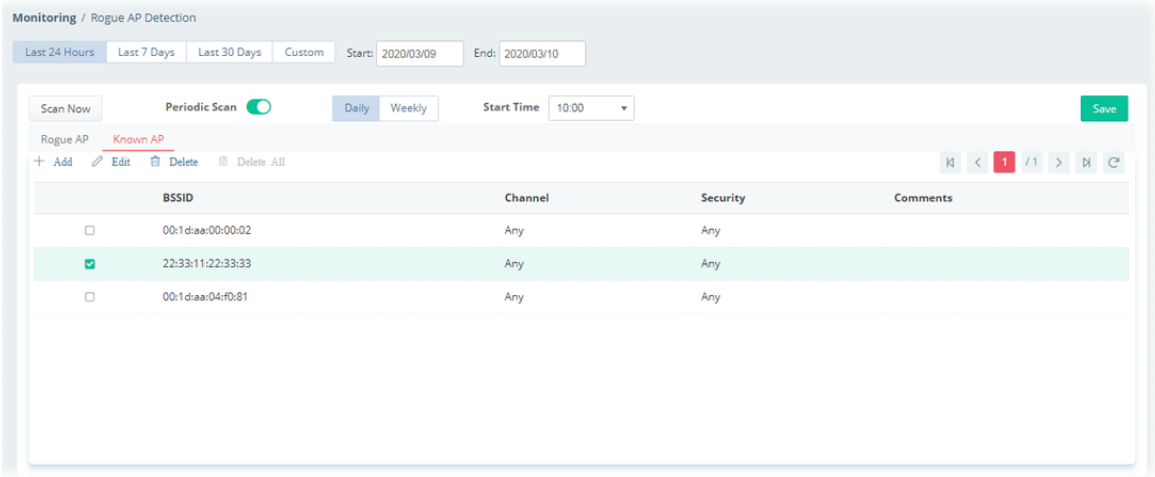
Click the **Rogue AP** tab to display the following page. All the APs detected will be treated as Rogue AP.



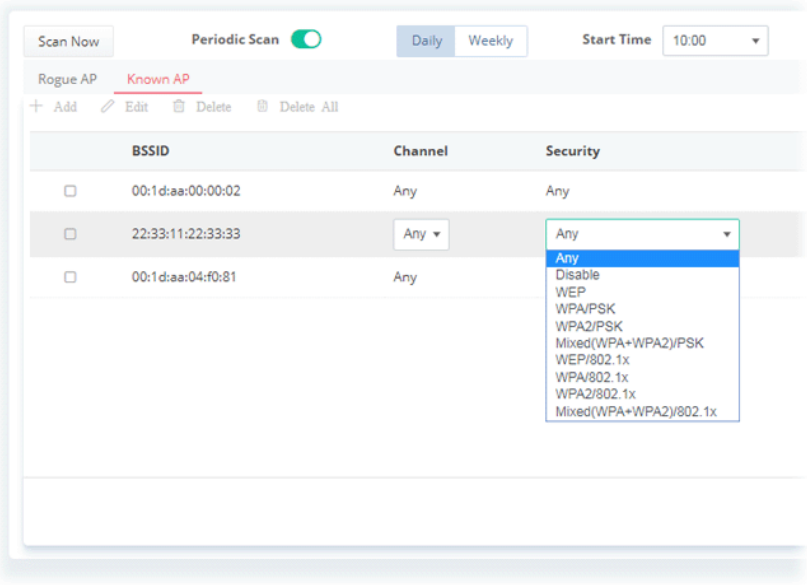

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Last 24 Hours / Last 7 Days / Last 30 Days / Custom** | Display the access point(s) detected within 24 hours, 7 days, 30 days or user defined days. |
| **Scan Now** | Perform device detection immediately. |
| **Periodic Scan** | After enabling this feature, access points will be detected periodically based on the setting configured here.<br>**Daily** – VigorACS will detect access point on certain time every day.<br>● **Start Time** – Specify a time point as starting time for device detection.<br>**Weekly –** VigorACS will detect access point on certain time every week.<br>● **On** – Choose the day to perform device detection.<br>● **Start Time** - Specify a time point as starting time for device detection. |
| **+Mark as Known** | Vigor access points can be detected and be shown in the table under Rogue AP. However, some of them might be known to you and should not be listed here. To solve this problem, simply click the access point and then click **Mark as Known**. The selected access point will be transferred and listed under Known AP. |
| **Delete** | Remove the selected access point from the list. |
| **Delete All** | Remove all of the access points from the list. |

Click **Known AP** to display the following page. All the access points listed under this page will be treated as friendly AP.



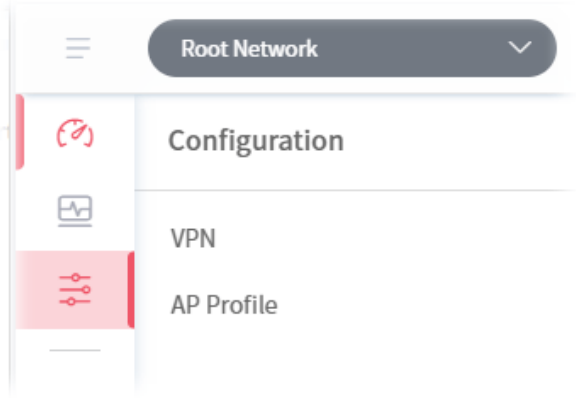

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Scan Now** | Perform device detection immediately. |
| **Add** | Click to create a new entry for entering information for access point. |
| **Edit** | Change the settings for a selected access point.<br>Select one of the access points. The Edit link will be available for clicking, then.<br>After clicking it, channel, security and comments will be allowed to be modified with different values.<br>  |
| **Delete** | Remove the selected access point from the list. |
| **Delete All** | Remove all of the access points from the list. |
| **BSSID** | Display the MAC address of the detected access point. |
| **Channel** | Display the channel used by the access point.<br>Check the box of the selected access point and click **Edit**. |
| **Security** | Display the security mode used by the access point. |

| | |
|---|---|
| | It can be changed. |
| **Comments** | Display a brief explanation for the access point.<br>It can be changed. |
| **Save** | Save the settings. |

## 7.3 Configuration

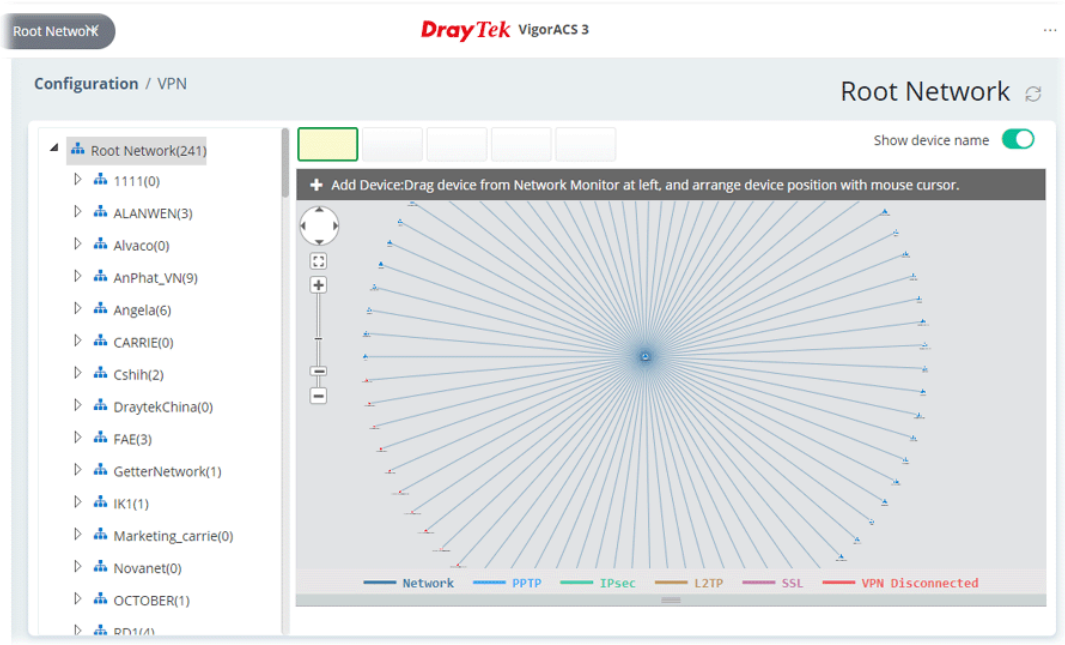
Configuration menu will vary for root network, group network and specified CPE.




### 7.3.1 VPN

VigorACS offers an easy method, VPN Wizard, to configure VPN settings for building VPN connection between two CPEs.

This page displays all the VPN connection status globally for Root Network or the VPN connection status for the network group selected.



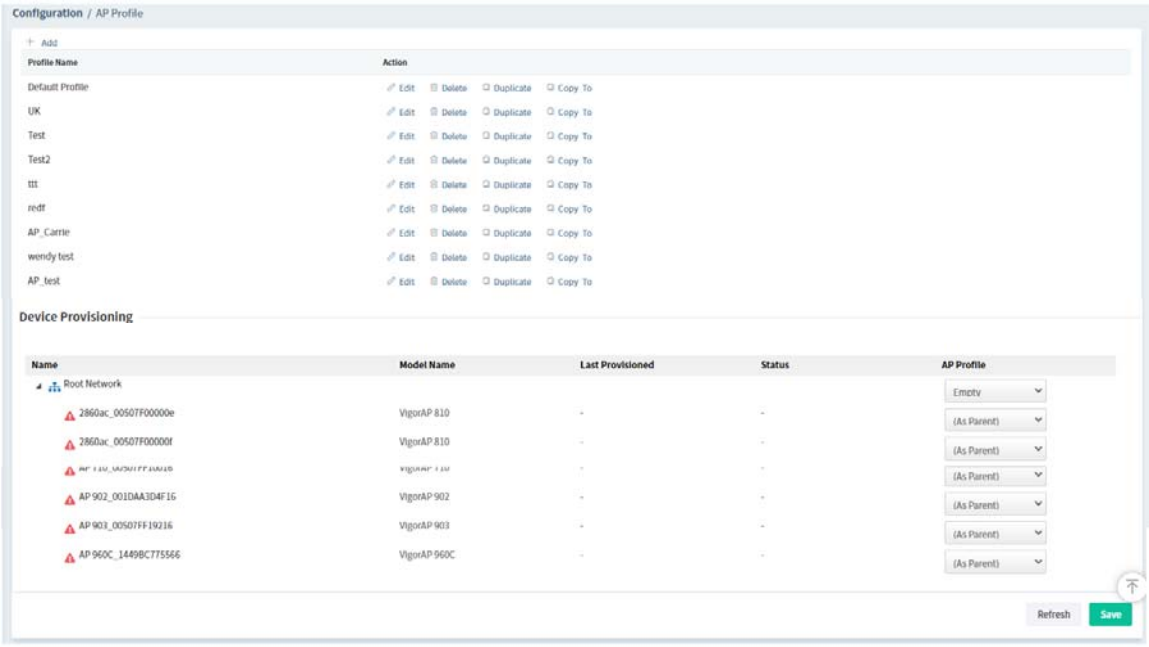

Different colors for arrows represent different protocols used in VPN connections. For example, Purple means Network Group; Green means PPTP mode; Blue means IPsec mode; and Red means the VPN connection is failed.

For detailed, refer to section 8.4.1.

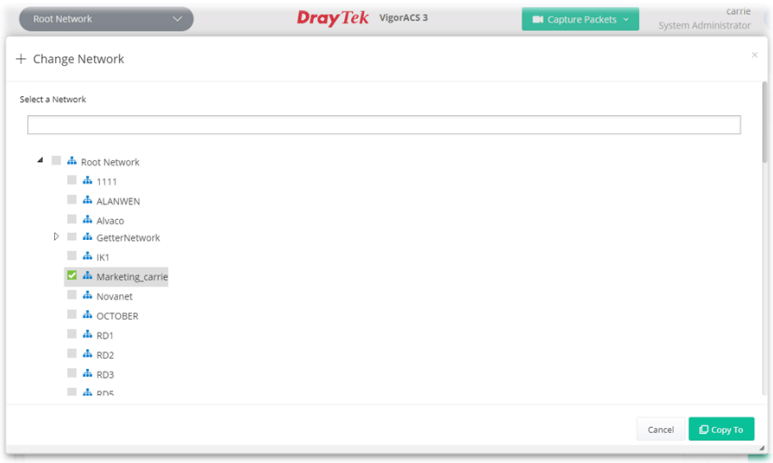
### 7.3.2 AP Profile

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.

The functions listed in the AP profile in VigorACS contain settings for all of models of VigorAP. When an AP profile is created, it can be used to apply onto any access point managed by VigorACS. If the access point does not have the functions defined in the AP profile, after being applied, only the functions that the selected access point supports will be overwritten by the selected AP profile.



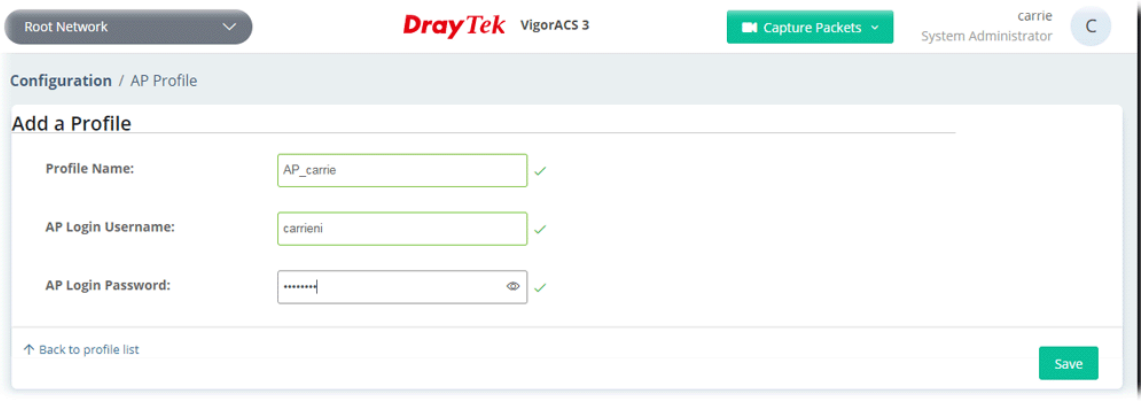

These parameters are explained as follows:

| Item | Description |
|---|---|
| **+Add** | Create a new AP profile with basic settings. |
| **Profile Name** | Display the name of AP profile. |
| **Action** | **Edit** - Configure detailed settings for the selected AP profile.<br>**Delete** –Delete the selected AP profile.<br>**Duplicate** – Click to duplicate a new profile (e.g., aaa(1)) based on the selected profile (e.g., aaa).<br>**Copy To** – Click to open the following page. Then select a network (e.g., Marketing_carrie in this case) from the tree view of Root Network. After clicking the Copy To button, the configuration of selected AP profile will be applied to the selected network (e.g., Marketing_carrie).<br>  |
| **Device Provisioning** | Locate the access points for applying suitable AP profile.<br>**Name** – Display a tree view for model managed by VigorACS. |

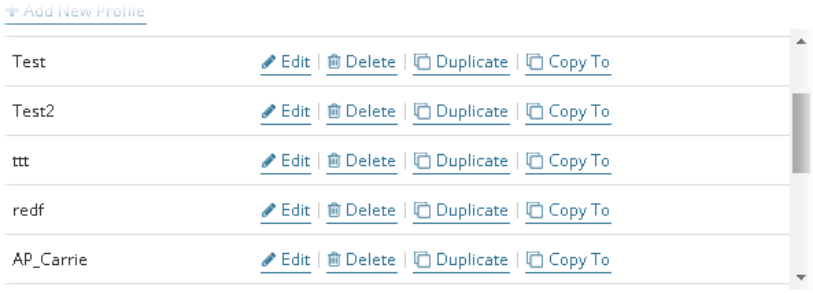
| | |
|---|---|
| | **Model Name** – Display the name of the model.<br>**Last Provisioned** – Display the time that AP profile was applied to the selected device.<br>**Status** – Display the status (updating, complete and "-") of the AP.<br>**AP Profile** – Choose an AP profile for applying to the selected AP**.** In which, **"As Parent"** means to apply the profile listed on the top to the selected AP. |
| **Refresh** | Click to refresh current page. |
| **Save** | Click to save the changes in this page. |

### 7.3.2.1 Add an AP Profile

Click **+Add** to create a new AP profile.

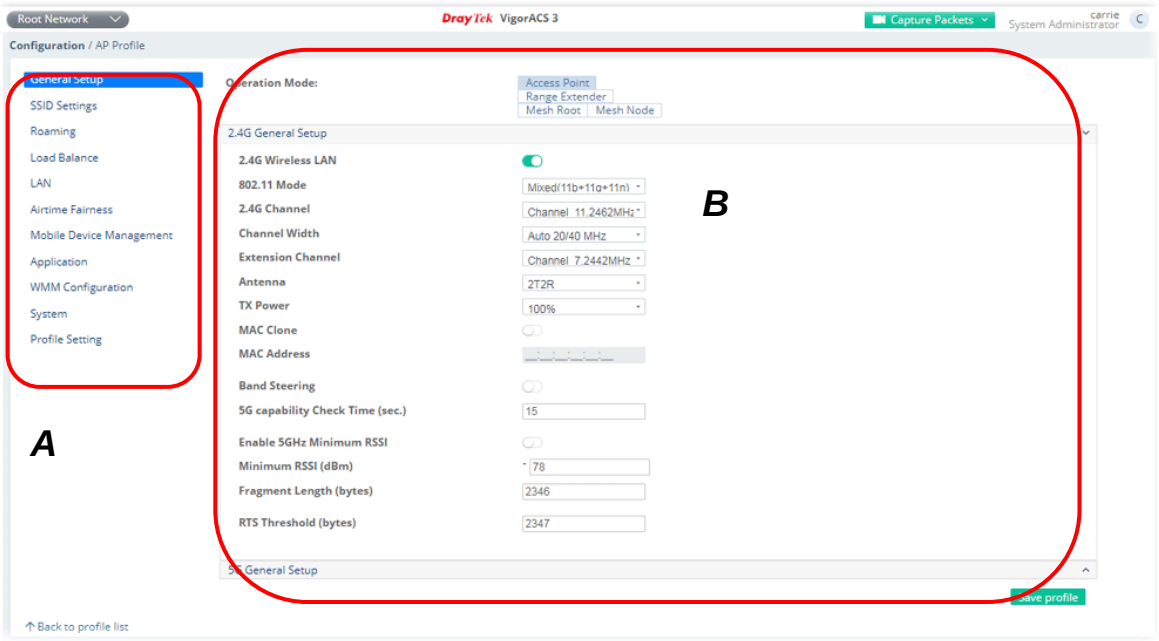



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Profile Name** | Enter a name of the profile. |
| **AP Login Username** | Enter a username for login the access point. |
| **AP Login Password** | Enter a password for login the access point. |
| **Back to profile list** | Return to previous page, AP profile list. |
| **Save** | Save the settings and display the new profile on the AP profile list.<br>  |

### 7.3.2.2 Edit an AP Profile

To configure detailed settings for each AP profile, click the **Edit** button for the selected profile. The setting page appears as follows:




These parameters are explained as follows:

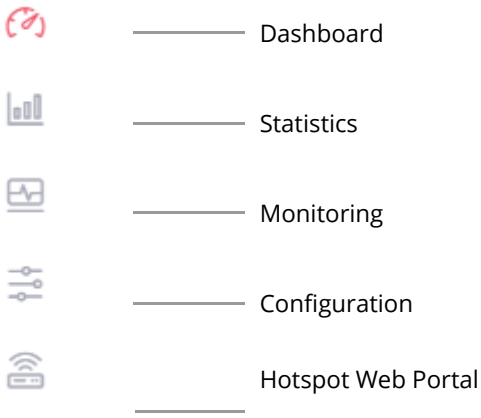
| Item | Description |
|---|---|
| **Area A - Menu Item** | At present, the available menu items contain,<br>● General Setup<br>● SSID Settings<br>● Roaming<br>● Load Balance<br>● LAN<br>● Airtime Fairness<br>● Mobile Device Management<br>● Application<br>● WMM Configuration<br>● System<br>● Profile Setting |
| **Area B - Settings** | This area will vary according to the item selected in Area A - Menu Item. |

Refer to User's Guide of VigorAP for the detailed information of settings definition.

This page is left blank.

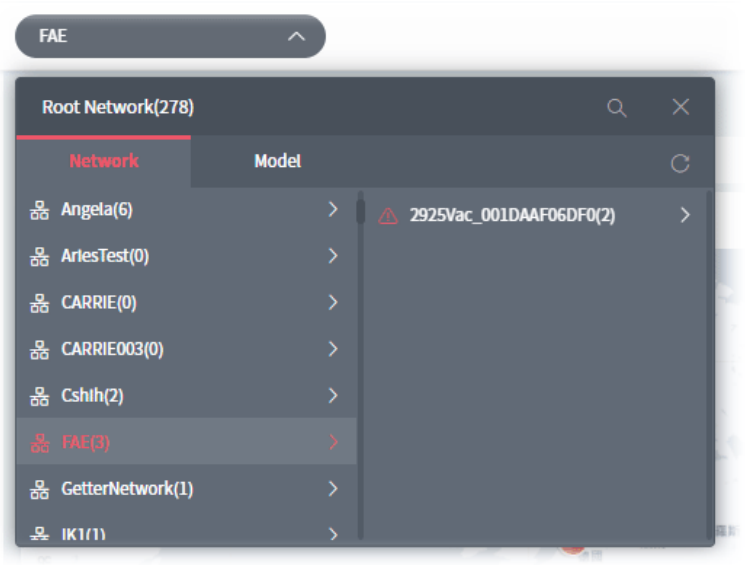
# Chapter 8 Network Group Menu

The menu items related to the network group:

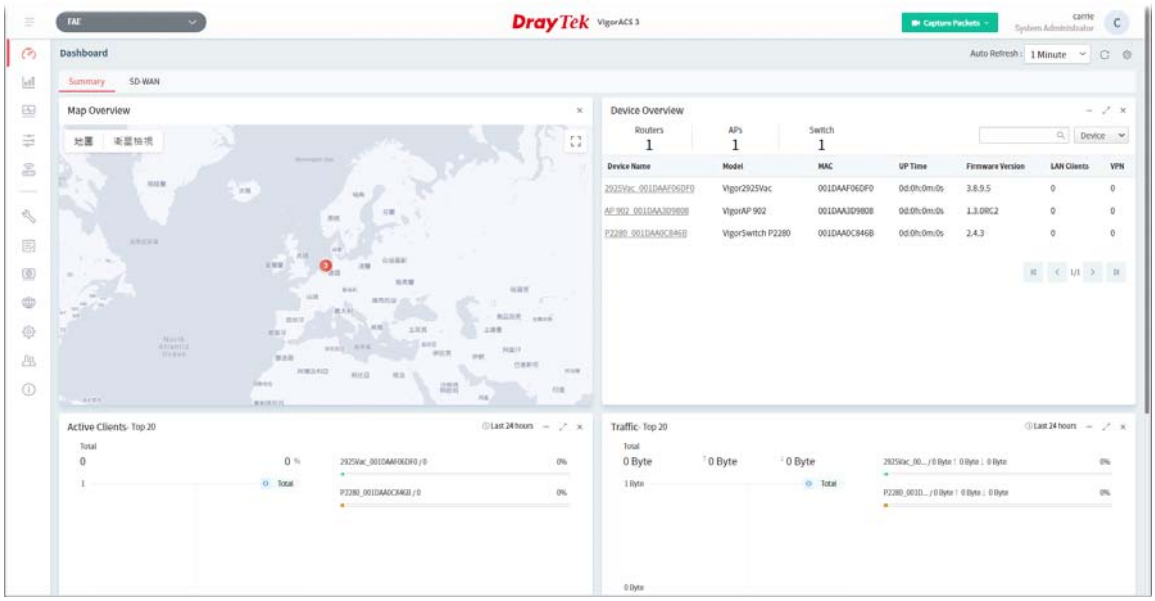



## 8.1 Dashboard for the Network Group

To display the network group dashboard, select a network group first. Find the one you want from the Network list under the Root Network. In this case, we choose FAE as an example.

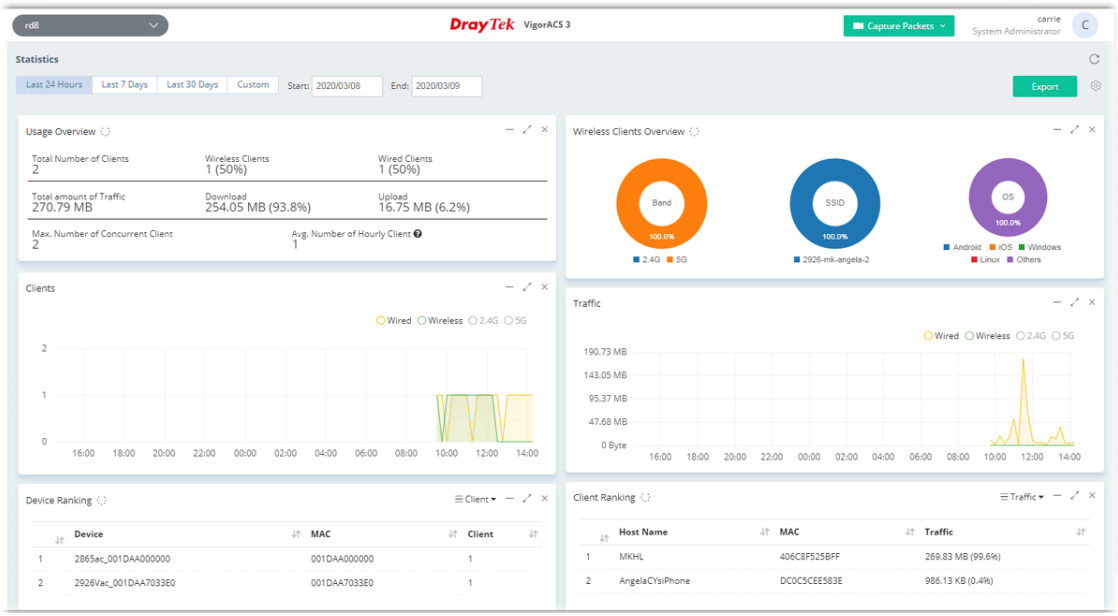


Click the **Summary** tab to display the page of dashboard (for monitoring).



## 8.2 Statistics for Network Group

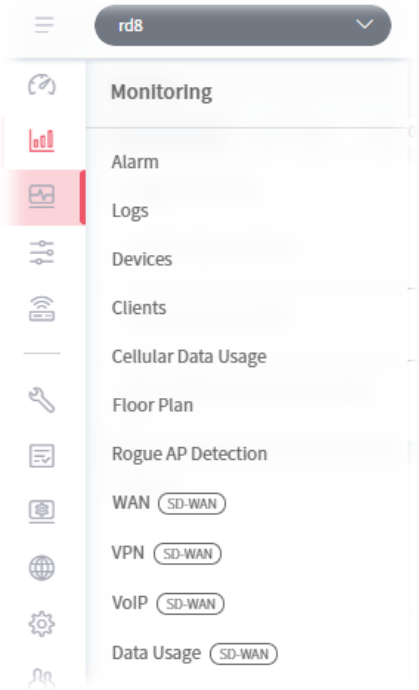
The page offers statistics for all the devices listed under root networks, including usage overview, wireless clients Overview, data traffic, device ranking, and client ranking. By clicking Last 24 Hours, Last 7 Days, Last 30 Days or Custom setting (define the period), the administrator can obtain various statistics within the time period.




In addition, the statistics can be exported as ".XLS" file if you click the **Export** button on the top side.

## 8.3 Monitoring for Network Group

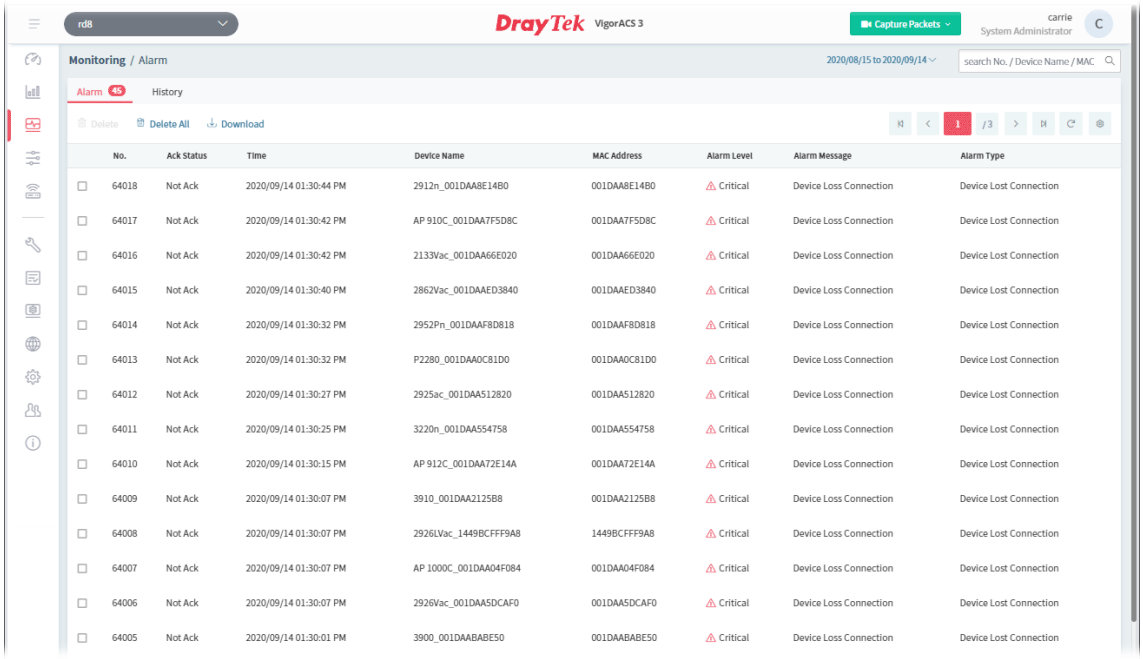
Monitoring menu offers options for monitoring the normal and abnormal actions for network group and CPE.




In this case, we choose RD8 as an example.

### 8.3.1 Alarm

Alarm message will be recorded on VigorACS 3 server when there is a trouble happened to the device (CPE). Only the users within the same user group will be notified for the message.

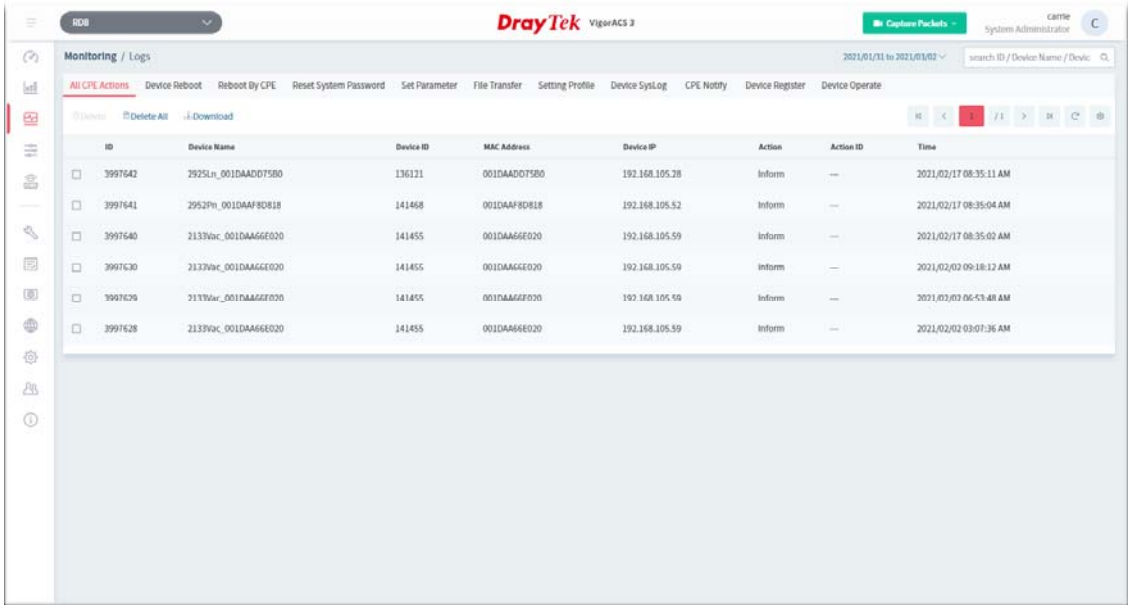



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Alarm / History** | **Alarm –** Displays the alarm records recently.<br>**History –** Displays all the alarm records that have been solved and cleared. |
| **Delete** | Clear the alarm record which has been solved by VigorACS 3. |
| **Delete All** | Clear all of the alarm records which have been solved by VigorACS 3. |
| **Download** | Click to save alarm log as a XLS file. |
| **No.** | Display the index number of the alarm. It is offered by VigorACS 3 automatically. |
| **Ack Status** | Display the status of the records with the type specified here (Not Ack or Acked). |
| **Time** | Displays the time of the device to be monitored. |
| **Device Name** | Displays the name of the monitored device. |
| **MAC Address** | Displays the MAC address of the monitored device. |
| **Alarm Level** | Displays the alarm message with the severity (e.g., Critical) specified. |
| **Alarm Message** | Displays a brief explanation for the alarm sent by VigorACS 3 automatically. |
| **Alarm Type** | Displays the alarm message with the type specified. |

### 8.3.2 Logs

Log provides administrator records for action executed, device name, MAC address, Device IP, CommandKey, and Current Time for CPE device managed and monitored by VigorACS.




These parameters are explained as follows:

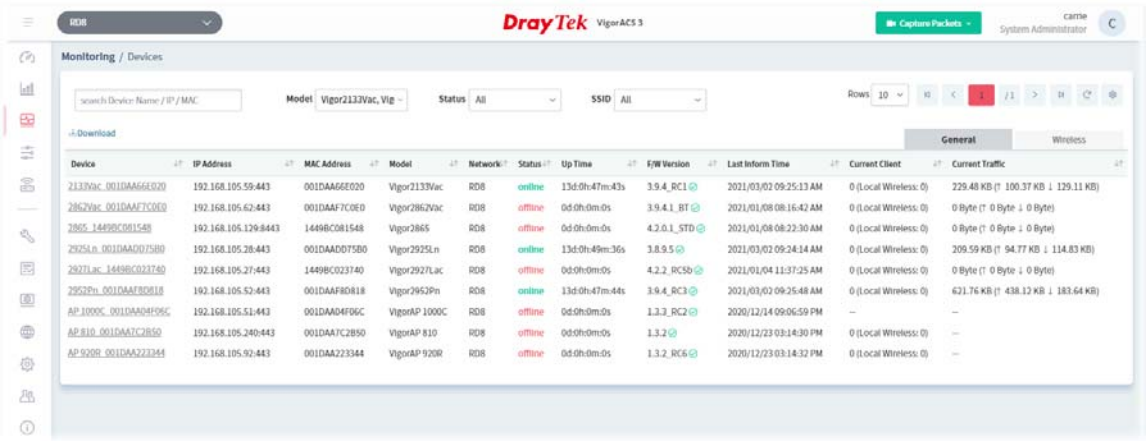
| Item | Description |
|---|---|
| **Log Type** | Click one of the tabs (e.g., All CPE Actions, Device Reboot, Reboot By CPE, Reset System Password, Set Parameter, File Transfer, Setting Profile, Device SysLog, CPE Notify, Device Register, Device Operate and etc.) to display related log on this page. |
| search ID / Device Name / De | Enter the condition for VigorACS to search and display relational information. |
| **Delete** | Clear the alarm record which has been solved by VigorACS. |
| **Delete All** | Clear all of the alarm records which have been solved by VigorACS. |
| **Download** | Click this button to save log as a XLS file. |

### 8.3.3 Devices

The administrator (user) can check information (such as Device name, IP address, MAC address, model name, network, status, up time, firmware version, number of current connected client, data traffic, and so on) of CPE under the selected network group by this page. The network group (e.g., Root Network in this case) selected above is the group to be monitored and information related to this selected network group will be shown below.

#### 8.3.3.1 Device Overview

This page shows all the devices (e.g., router, access points and switches) under the selected network group.

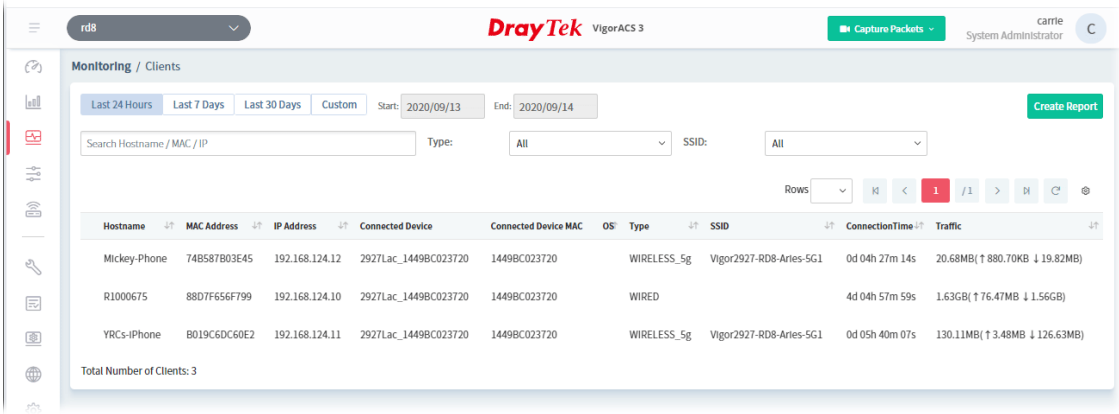



These parameters are explained as follows:

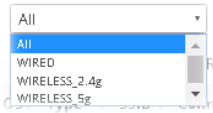
| Item | Description |
|---|---|
| search Device Name / IP / MAC | Enter the condition for VigorACS to search and display relational information. |
| **Model** | This area lists all of the devices that monitored by VigorACS.<br>Check **Select all** to display information for all of the devices; or check the name of the device to display the information related to the selected device. |
| **Status** | **Online** – This page displays information for the device which is online currently.<br>**Offline** – This page displays information for the device which is offline currently.<br>**All** – This page displays information for all of the devices no matter it is online or offline. |
| **SSID** | This area lists information for CPE with wireless features monitored by VigorACS.<br>Check **All** to display all of the devices; or check the name of the device to display the information related to the selected device.<br>**SSID** - SSIDs for CPE with wireless features will be displayed in this drop down list. Choose one of the SSIDs. Information related to the selected SSID will be displayed on this page. |
| **General / Wireless** | **General** – List the general information for the CPE under the selected group.<br>**Wireless** – List only the wireless information for the CPE under the selected group. |
| **Download** | Click this button to save information for monitored devices as a XLS file. |

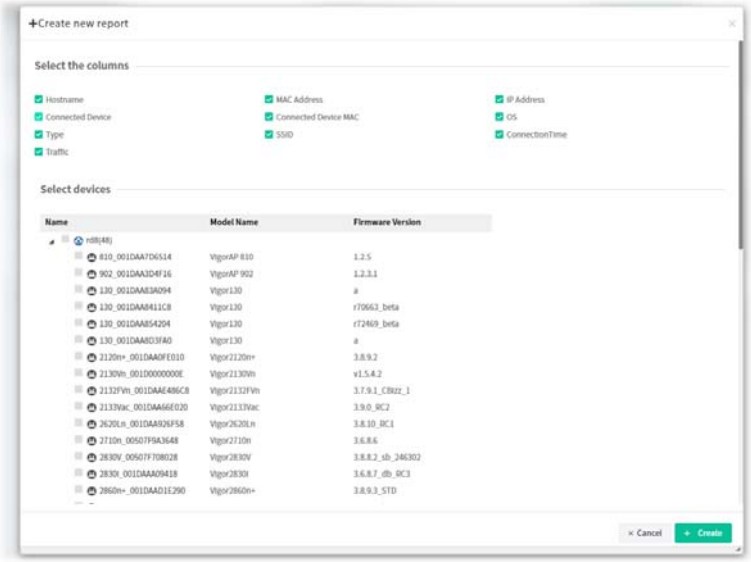
### 8.3.4 Clients

This page displays general information (such as hostname, MAC address, IP address, name of connected device, type, SSID, connection time, and etc.) for wireless / wired clients which connect to CPEs under the selected network group by this page. The network group (e.g., rd8 in this case) selected above is the group to be monitored and information related to this selected network group will be shown below.



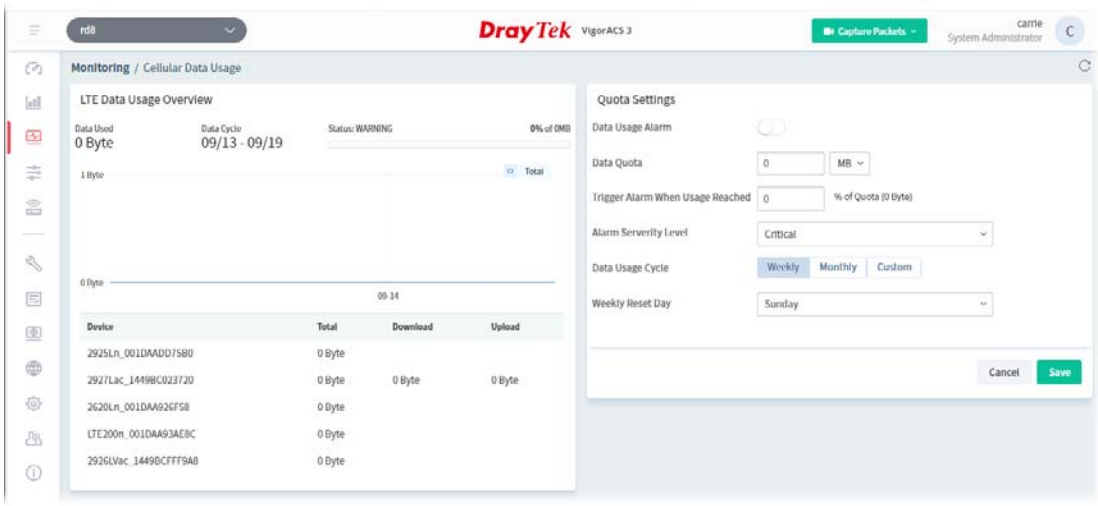

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Last 24 Hours / Last 7 Days / Last 30 Days / Custom** | Display the clients detected within 24 hours, 7 days, 30 days or user defined days. |
|   | Enter the condition for VigorACS to search and display relational information. |
| **Type**   | Check **All** to display information for all of the devices (including wired and wireless devices).<br>**Wired** – This page displays information for the device without wireless feature.<br>**Wireless_2.4g** – This page displays information for the device with 2.4GHz wireless feature.<br>**Wireless_5g** – This page displays information for the devices with 5GHz wireless feature. |
| **SSID** | This area lists information for CPE with wireless features monitored by VigorACS.<br>Check **All** to display all of the devices; or check the name of the device to display the information related to the selected device.<br>**SSID** - SSIDs for CPE with wireless features will be displayed in this drop down list. Choose one of the SSIDs. Information related to the selected SSID will be displayed on this page. |
| **Create Report** | Click this button to save client's information as a "XLS" file.<br>After clicking the button, the following page will appear. |

| | |
|---|---|
| |  <br>Set the conditions and choose the devices, then click **+Create**. |

## 8.3.5 Cellular Data Usage

This page displays traffic information including data used, data cycle, status, percentage, downloaded data, uploaded data for device equipped with LTE features (e.g., Vigor2927Lac). The values defined in **Quota Settings** indicate total amount of quota for all LTE devices managed by VigorACS.




These parameters are explained as follows:

| Item | Description |
|---|---|
| **LTE Data Usage Overview** | **Status** - The bar chart displays the data usage in yellow, green and grey based on values defined in **Quota Settings**. If data usage for the LTE model exceeds the percentage of quota configured in the field of **Trigger Alarm When Usage Reached** in Q**uota Settings**, the amount of used data will be shown in Yellow; if not, it will be displayed in Green. The rest quota will be shown in gray.<br>In addition, device name, throughput, downloaded data and uploaded data for each LTE can be seen on the table below this page. |
| **Quota Settings** | |

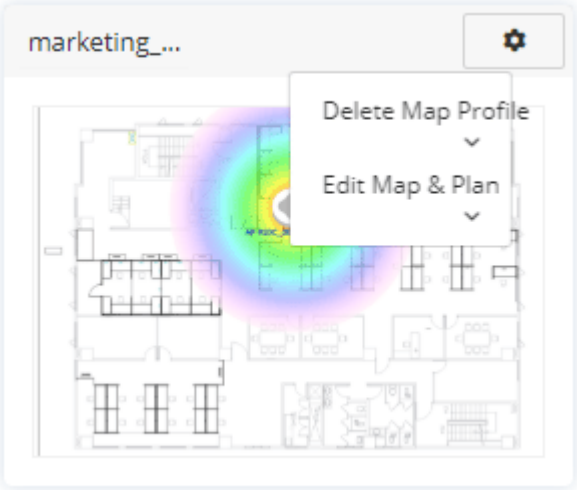
| | |
|---|---|
| **Data Usage Alarm** | When it is enabled, a warning message will be shown in the page of **DEVICE MENU>>Monitoring>>Alarm** once the data usage reaches the threshold defined in **Trigger Alarm When Usage Reached**. |
| **Data Quota** | The value (unit is MB/GB) defined here means total amount of data quota available for all LTE devices managed by VigorACS. |
| **Trigger Alarm When Usage Reached** | Set a threshold for triggering alarm mechanism. |
| **Alarm Severity Level** | Set the alarm severity (critical, major, minor, warning and normal). Such severity will be shown on **DEVICE MENU>>Monitoring>>Alarm** when the data usage for LTE model(s) reaches the threshold. |
| **Data Usage Cycle** | Select one of the options (Weekly, Monthly, Custom) as data usage cycle.<br>**Cycle Duration(days) –** When **Custom** is selected, please specify the cycle duration. The data quota for LTE model will be reset after the days configured here.<br>**Cycle Starts On** –When **Custom** is selected, specify one date as a starting point to reset the data quota for LTE model.<br>**Weekly Reset Day** - When **Weekly** is selected as Data Usage Cycle, please use the drop down list to choose one day (Monday to Sunday) for VigorACS to reset the data quota for LTE model.<br>**Monthly Reset Day** - When **Monthly** is selected as Data Usage Cycle, please use the drop down list to choose a date for VigorACS to reset the data quota for LTE model. |
| **Cancel** | Discard current modification. |
| **Save** | Save the current settings. |

### 8.3.6 Floor Plan

This function is helpful to determine the best location for VigorAP in a room. A floor plan of a room is required to be uploaded first. By dragging and dropping available VigorAP icon from the list to the floor plan, the placement with the best wireless coverage will be clearly indicated through simulated signal strength.

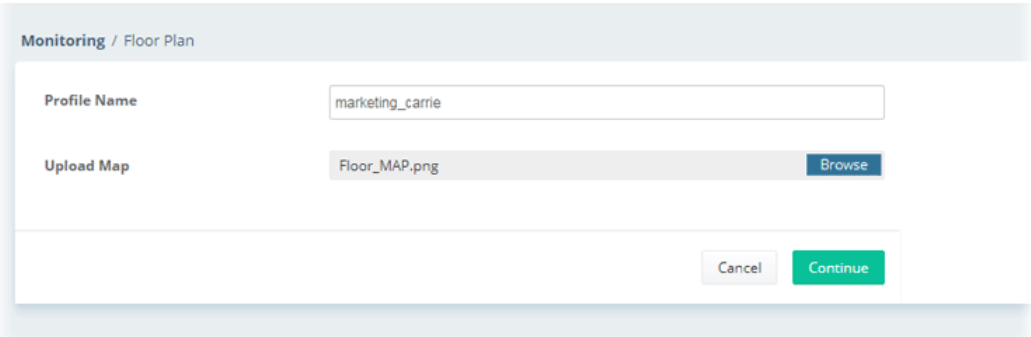
These parameters are explained as follows:

| Item | Description |
|---|---|
| **+Add** | Creates a new profile. |
| | Click to change to browse view.<br>It displays all of the floor plan profiles with the map used. |

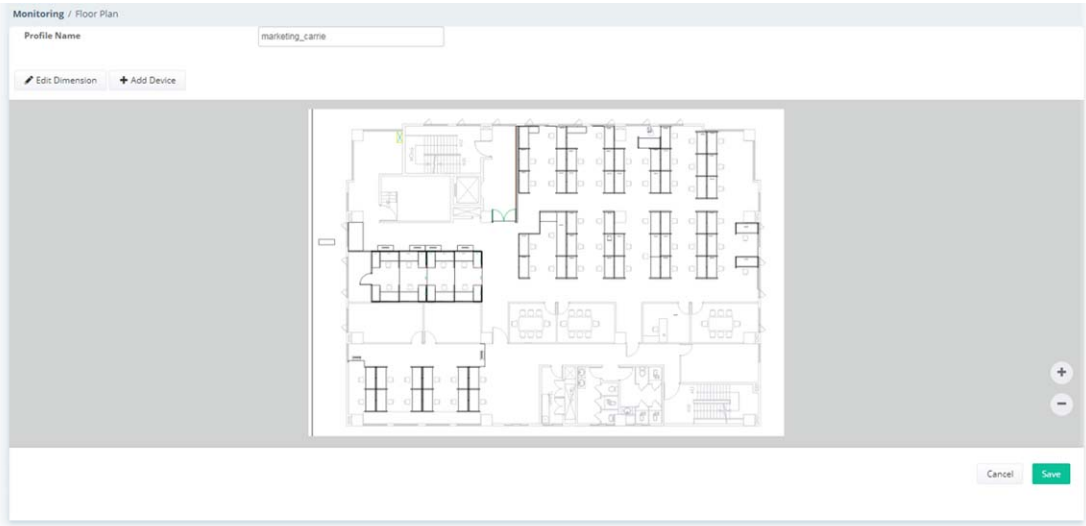
| | |
|---|---|
| | <br>You can click **Add** on this page to create a new profile. To modify the existed profile, click the icon on the right-top to display a drop down menu. Then click **Edit Map & Plan** to perform the modification, or click **Delete Map Profile** to remove the selected floor plan profile.<br>  |
| **Profile Name** | Displays the name of the floor plan profile. |
| **Device** | Displays the number of AP devices placed on the plan profile. |
| **Action** | **Edit** - Click to modify the profile.<br>**Delete** - Click to remove the selected profile. |

To create a new profile:

1. Click **+Add**.
2. From the following page, enter profile name (e.g., marketing_carrie) and click Browse to upload a map (e.g., Floor_MAP.png). Click **Continue**.



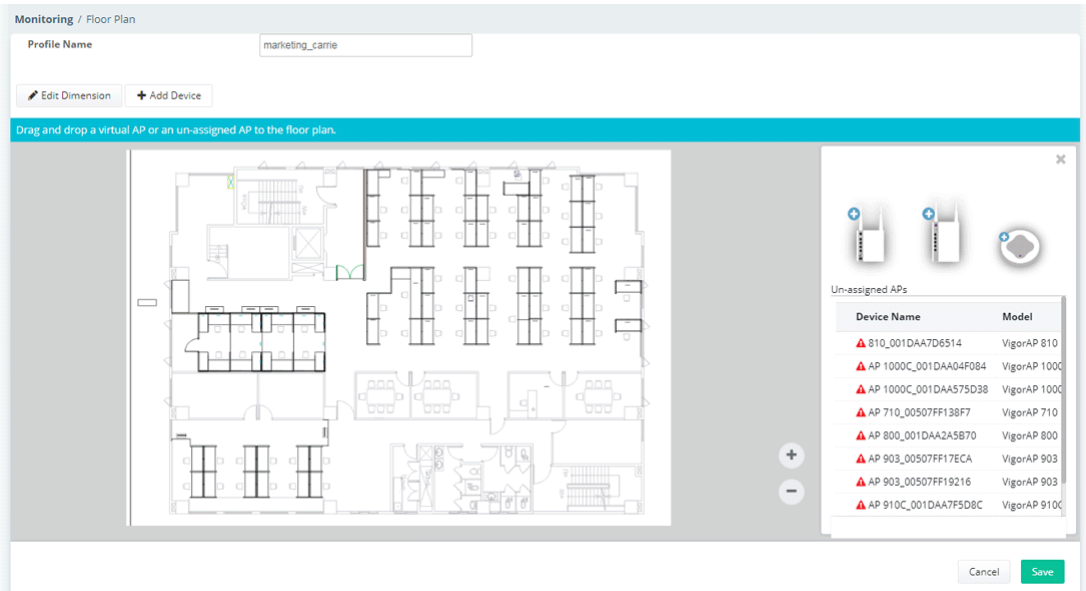
3. A floor map will be displayed on the screen.



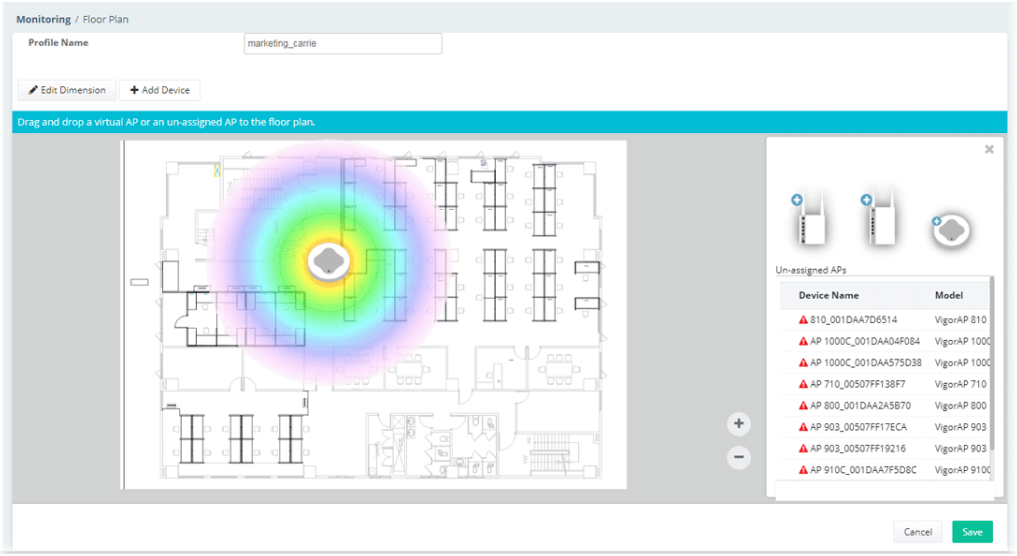

**Edit Dimension** – Draw a line and enter the distance of length / width of the map.

**Add Device** – Click to display available VigorAP to apply it on to the map.

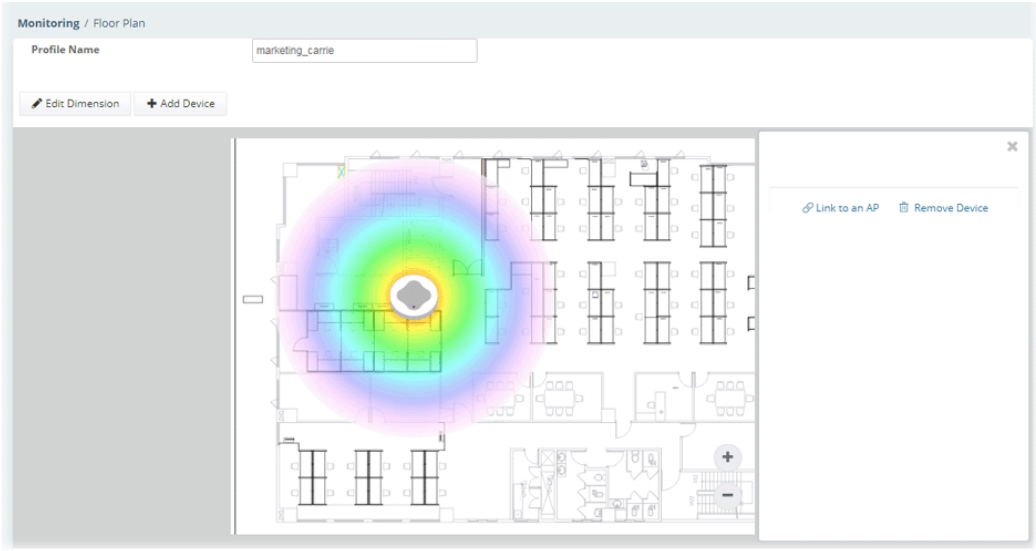
4. Click **+Add Device**. Available VigorAP icons and name list will be displayed on the right side of this page.



5. Select the AP you want (e.g., VigorAP910C icon, in this case) from right side of this page. Drag and drop the icon on the map. Later, an icon with effective signal range will be seen on the screen.



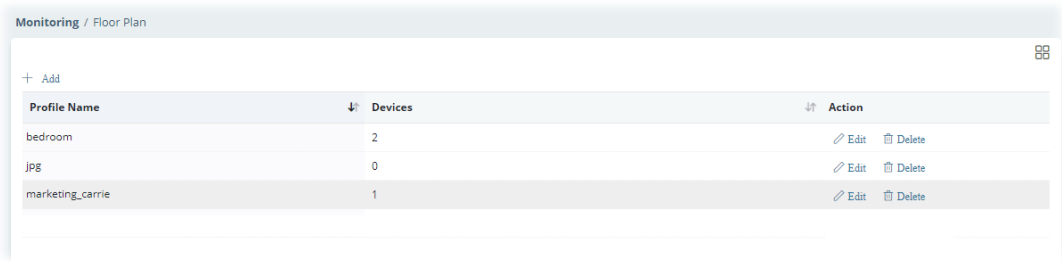

6. Slightly click the AP icon on the map. Two links of **Link to an AP** and **Remove Device** will be shown on the right side.




- **Remove Device** – If you do not satisfy the location of AP icon, click this link to remove the AP icon from the map.
- **Link to an AP** – If you satisfy the location of AP icon, click this link to select VigorAP. All of un-assigned AP names will be shown on the list. Choose the one you want and click Apply. Then such map has been connected with the specified AP.

7. Click **Link to an AP** to select the AP you want. After clicking **Apply**, the name of the VigorAP will be displayed below the icon on the map.

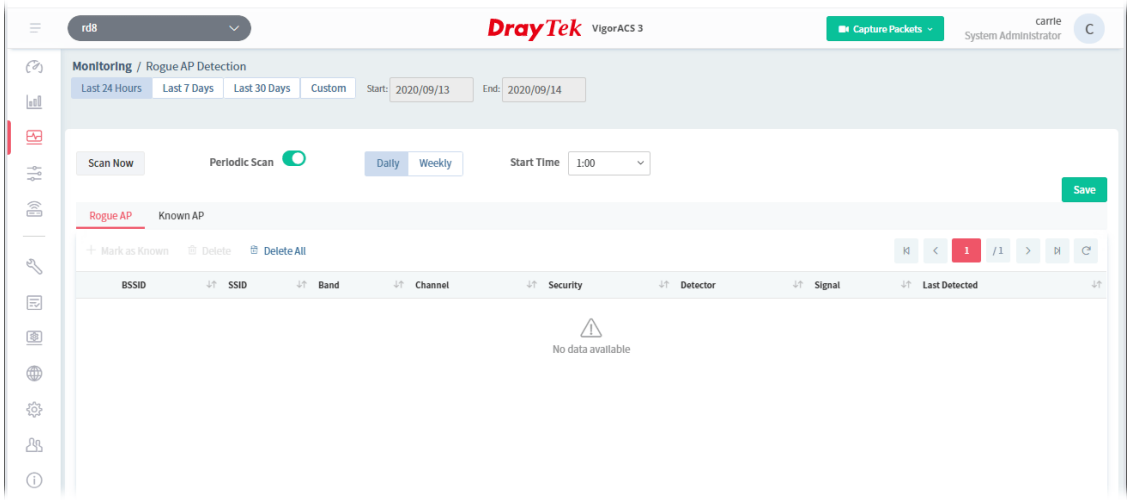
8. Click **Save**. The new created profile will be shown on the page.



### 8.3.7 Rouge AP Detection

Information detected by VigorAP can be displayed in this page. In which, the APs will be classified with rogue AP and known AP in different colors.

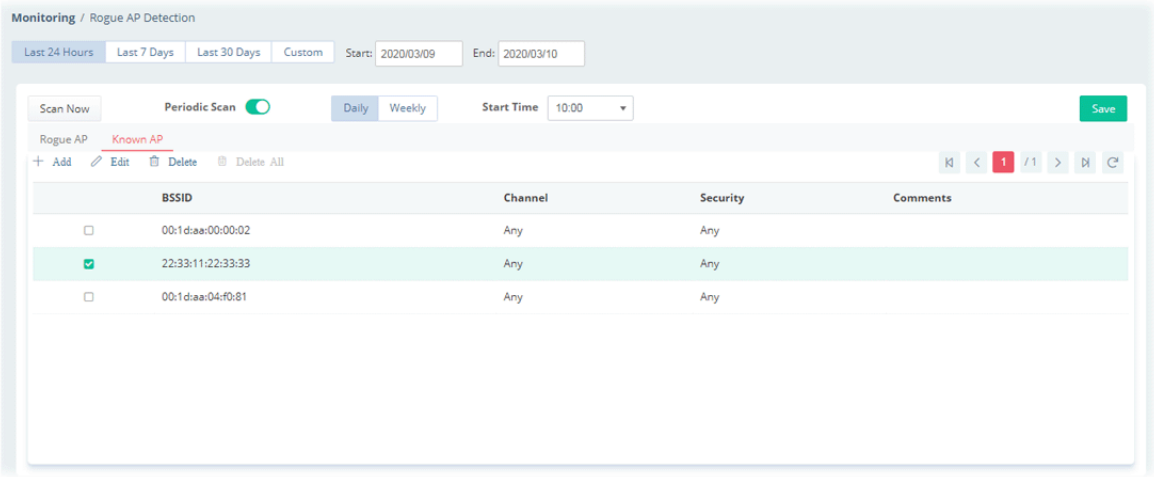
Click the **Rogue AP** tab to display the following page. All the APs detected will be treated as Rogue AP.



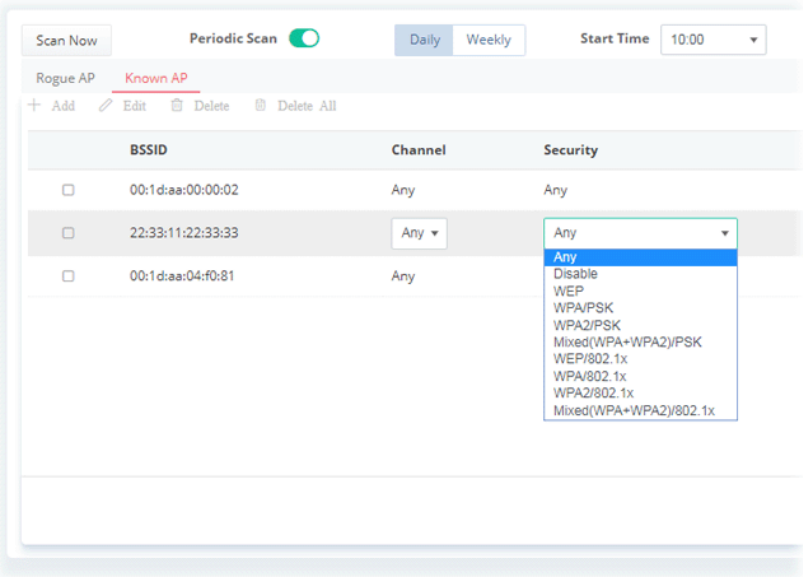

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Last 24 Hours / Last 7 Days / Last 30 Days / Custom** | Display the access point(s) detected within 24 hours, 7 days, 30 days or user defined days. |
| **Scan Now** | Perform device detection immediately. |
| **Periodic Scan** | After enabling this feature, access points will be detected periodically based on the setting configured here.<br>**Daily –**VigorACS will detect access point on certain time every day.<br>● **Start Time** – Specify a time point as starting time for device detection.<br>**Weekly –** VigorACS will detect access point on certain time every week.<br>● **On** – Choose the day to perform device detection.<br>● **Start Time** - Specify a time point as starting time for device detection. |
| **+Mark as Known** | Vigor access points can be detected and be shown in the table under Rogue AP. However, some of them might be known to you and should not be listed here. To solve this problem, simply click the access point and then click **Mark as Known**. The selected access point will be transferred and listed under Known AP. |
| **Delete** | Remove the selected access point from the list. |
| **Delete All** | Remove all of the access points from the list. |

Click **Known AP** to display the following page. All the access points listed under this page will be treated as friendly AP.



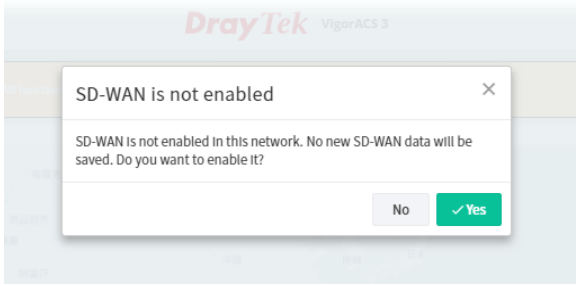

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Add** | Click to create a new entry for entering information for access point. |
| **Edit** | Change the settings for a selected access point.<br>Select one of the access points. The Edit link will be available for clicking, then.<br>After clicking it, channel, security and comments will be allowed to be modified with different values.<br>  |
| **Delete** | Remove the selected access point from the list. |
| **Delete All** | Remove all of the access points from the list. |
| **BSSID** | Display the MAC address of the detected access point. |
| **Channel** | Display the channel used by the access point.<br>Check the box of the selected access point and click **Edit**. |
| **Security** | Display the security mode used by the access point.<br>It can be changed. |

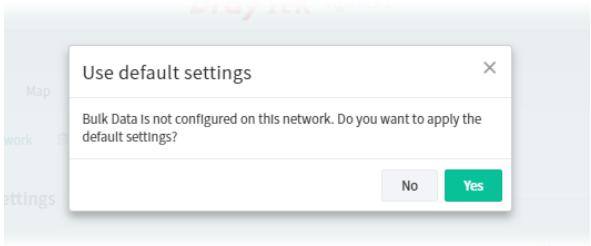
| | |
|---|---|
| **Comments** | Display a brief explanation for the access point.<br>It can be changed. |
| **Save** | Save the settings. |

### 8.3.8 WAN (SD-WAN), VPN (SD-WAN), VoIP (SD-WAN), Data Usage (SD-WAN)

These pages (WAN (SD-WAN), VPN (SD-WAN), VoIP (SD-WAN), Data Usage (SD-WAN)) are only available when SD-WAN feature for the selected network group has been enabled. If not, after accessing into these page, the following dialog will appear.

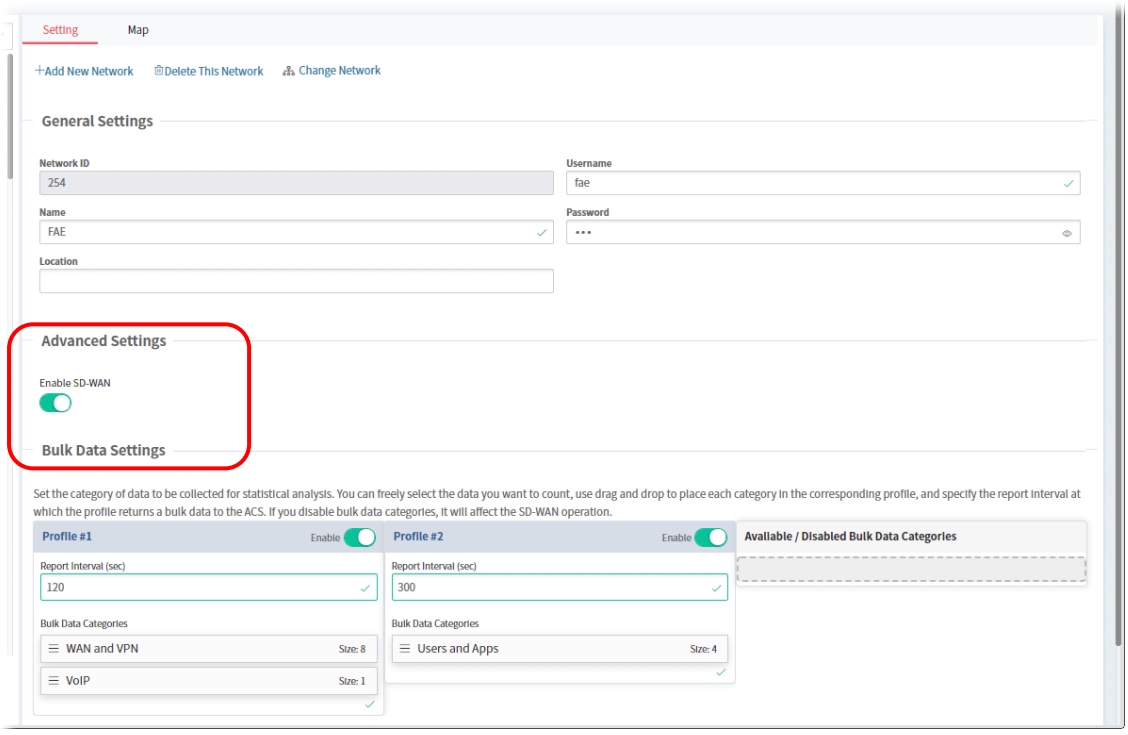



If you click **Yes**, the system will open the Network Management web page and pop-up the following dialog.




Click **Yes** to use the default settings.

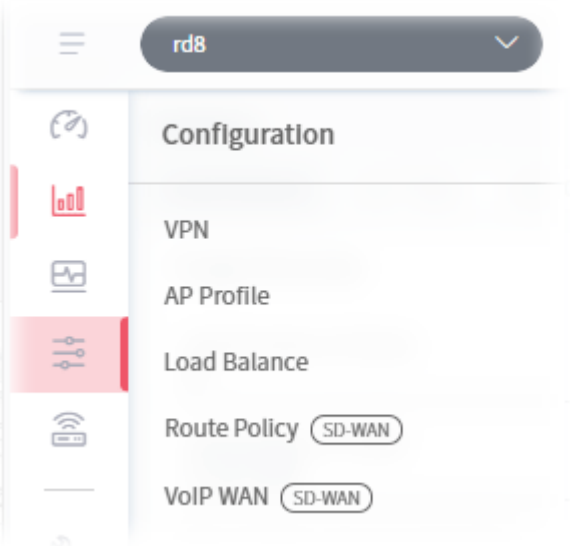
When the SD-WAN is enabled, refer to **4.4 Monitoring for SD-WAN Network Group** for detailed information of corresponding configuration pages.



## 8.4 Configuration Menu for Network Group,

Configuration settings will vary for root network, group network and specified CPE.

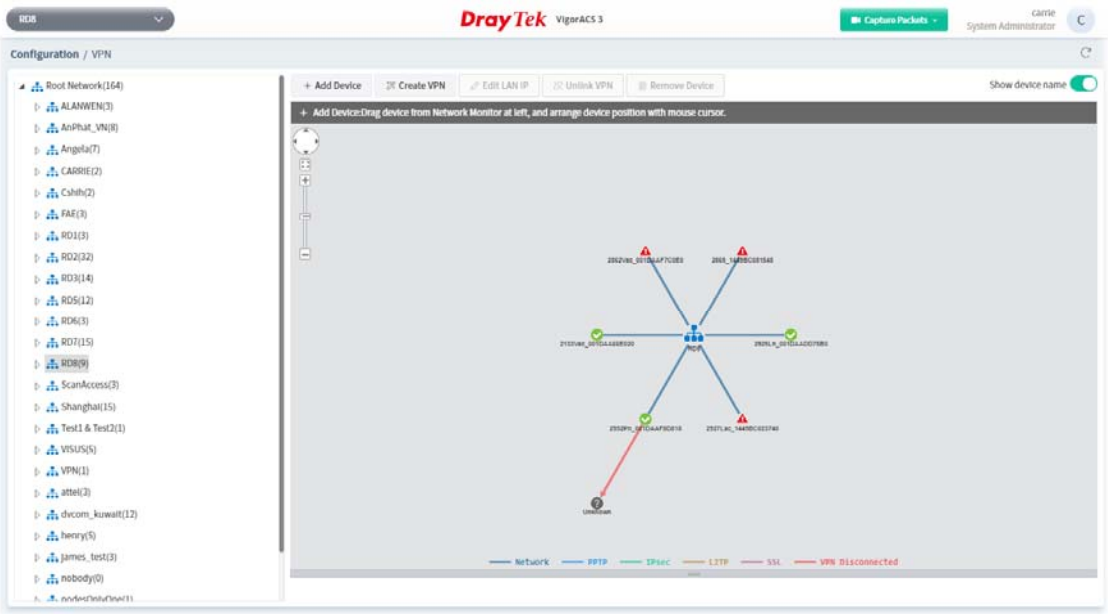
This section introduces the menu item used for the network group (e.g., RD8 in this case) with SD-WAN feature.




### 8.4.1 VPN

VigorACS offers an easy method, VPN Wizard, to configure VPN settings for building VPN connection between two CPEs.

This page displays all the VPN connection status globally for Root Network or the VPN connection status for the network group selected.

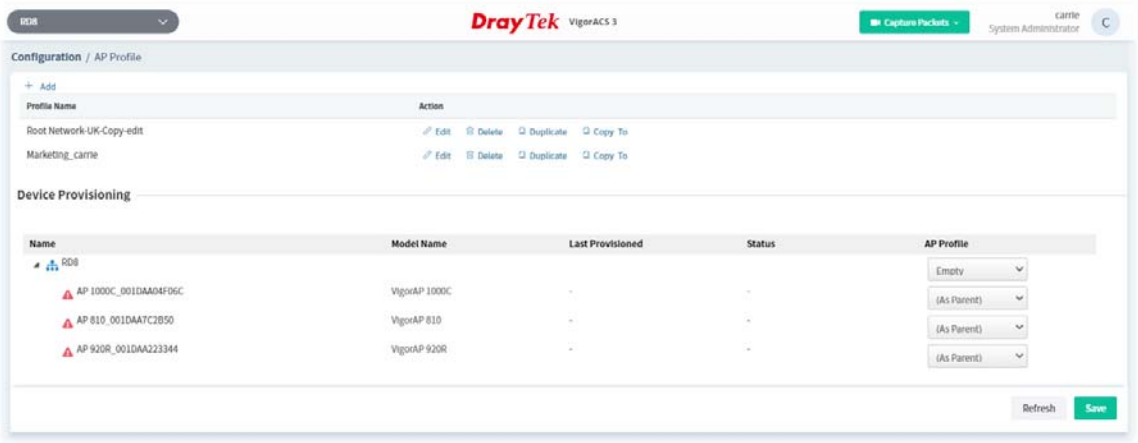



Different colors for arrows represent different protocols used in VPN connections. For example, Purple means Network Group; Green means PPTP mode; Blue means IPsec mode; and Red means the VPN connection is failed.

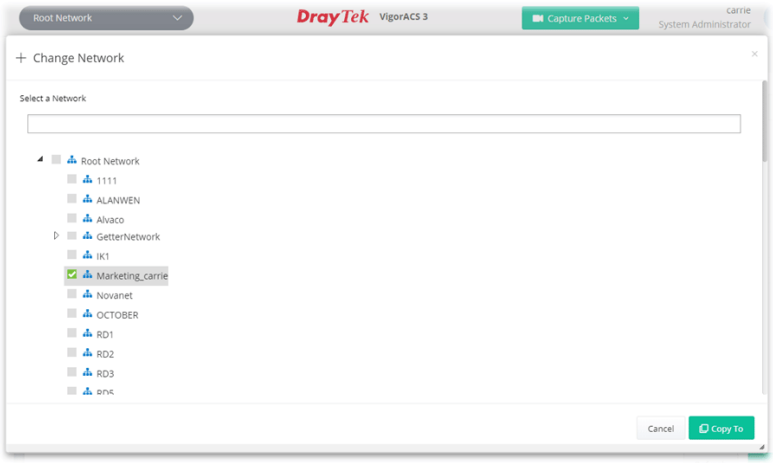
### 8.4.2 AP Profile

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.

The functions listed in the AP profile in VigorACS contain settings for all of models of VigorAP. When an AP profile is created, it can be used to apply onto any access point managed by VigorACS. If the access point does not have the functions defined in the AP profile, after being applied, only the functions that the selected access point supports will be overwritten by the selected AP profile.



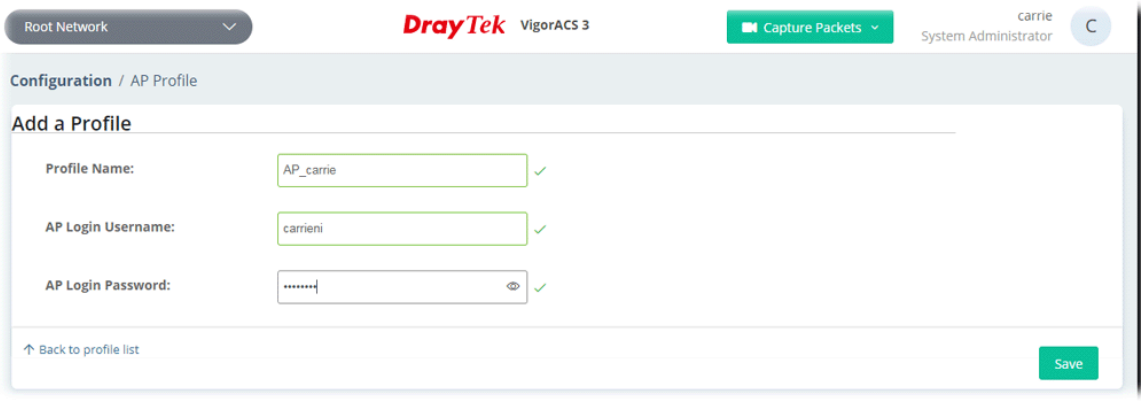

These parameters are explained as follows:

| Item | Description |
|---|---|
| **+Add** | Create a new AP profile with basic settings. |
| **Profile Name** | Display the name of AP profile. |
| **Action** | **Edit** - Configure detailed settings for the selected AP profile.<br>**Delete** –Delete the selected AP profile.<br>**Duplicate** – Click to duplicate a new profile (e.g., aaa(1)) based on the selected profile (e.g., aaa).<br>**Copy To** – Click to open the following page. Then select a network (e.g., Marketing_carrie in this case) from the tree view of Root Network. After clicking the Copy To button, the configuration of selected AP profile will be applied to the selected network (e.g., Marketing_carrie).<br>  |
| **Device Provisioning** | Locate the access points for applying suitable AP profile.<br>**Name** – Display a tree view for model managed by VigorACS. |

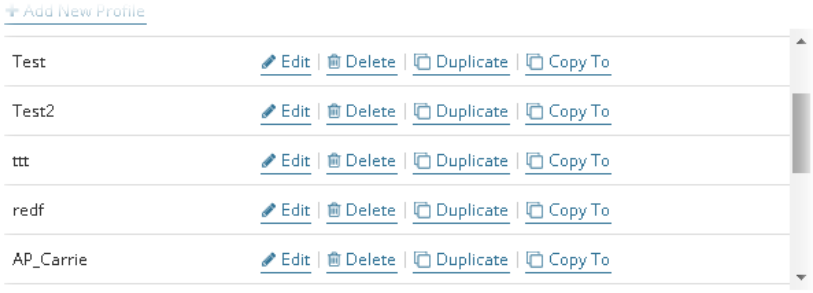
| | |
|---|---|
| | **Model Name** – Display the name of the model.<br>**Last Provisioned** – Display the time that AP profile was applied to the selected device.<br>**Status** – Display the status (updating, complete and "-") of the AP.<br>**AP Profile** – Choose an AP profile for applying to the selected AP**.** In which, **"As Parent"** means to apply the profile listed on the top to the selected AP. |
| **Refresh** | Click to refresh current page. |
| **Save** | Click to save the changes in this page. |

### 8.4.2.1 Add an AP Profile

Click **+Add** to create a new AP profile.

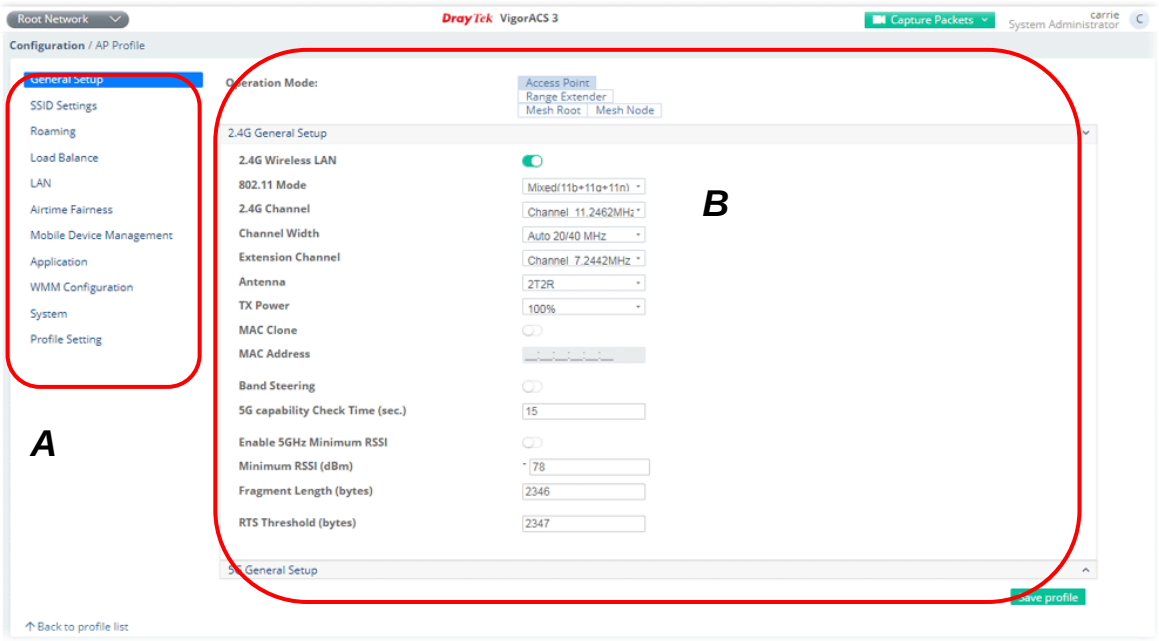



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Profile Name** | Enter a name of the profile. |
| **AP Login Username** | Enter a username for login the access point. |
| **AP Login Password** | Enter a password for login the access point. |
| **Back to profile list** | Return to previous page, AP profile list. |
| **Save** | Save the settings and display the new profile on the AP profile list.<br>  |

### 8.4.2.2 Edit an AP Profile

To configure detailed settings for each AP profile, click the **Edit** button for the selected profile. The setting page appears as follows:




These parameters are explained as follows:

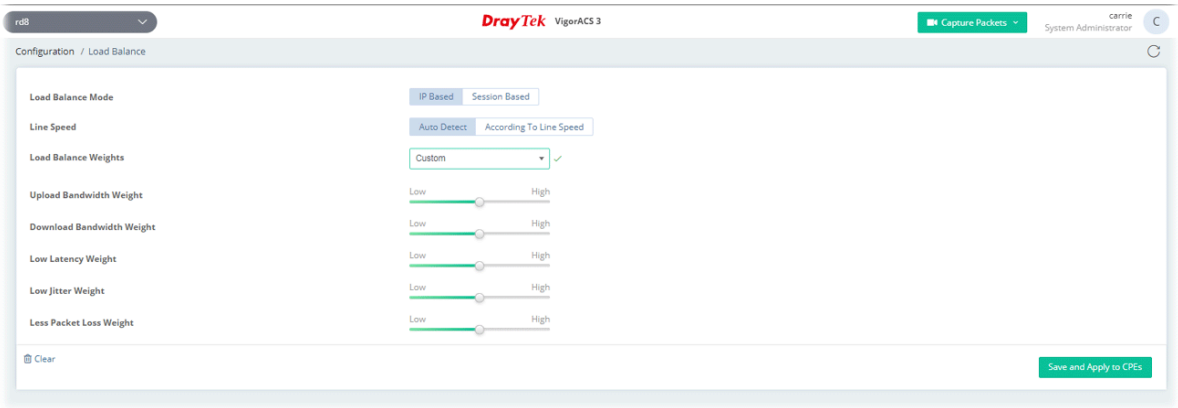
| Item | Description |
|---|---|
| **Area A - Menu Item** | At present, the available menu items contain,<br>● General Setup<br>● SSID Settings<br>● Roaming<br>● Load Balance<br>● LAN<br>● Airtime Fairness<br>● Mobile Device Management<br>● Application<br>● WMM Configuration<br>● System<br>● Profile Setting |
| **Area B - Settings** | This area will vary according to the item selected in Area A - Menu Item. |

If required, refer to User's Guide of VigorAP for the detailed information of settings definition.

### 8.4.3 Load Balance

While detecting the connection quality for the whole network group, the ACS server will consider the values of latency, loss, and jitter to get load balance for packets.

This page allows you to configure the weight for latency, jitter and packets loss.



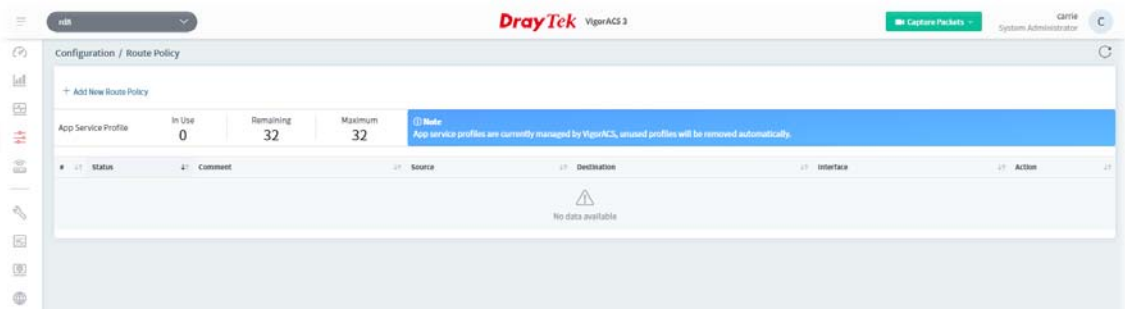

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Load Balance Mode** | **IP Based** - The same source / destination IP pair will select the same WAN interface as policy. It is the default setting.<br>**Session Based** - All of the WAN interfaces will be used (as out-going WAN) for passing through new sessions to get better transmission speed. |
| **Line Speed** | **Auto Detect** - Select to let the CPE reach the best load balance. It is the default setting.<br>**According to Line Speed** - Select it if you know the practical bandwidth for your WAN interface. |
| **Load Balance Weights** | There are four weight types for choosing to meet your request.<br>**Bandwidth-Based** - The load balance weight for each WAN will be executed according to line speed setting (DownLink/UpLink Rate).<br>**Quality-Based** - The load balance weight for each WAN will be executed according to the transmission rate, latency time and the jitter time.<br>**Reliability-Based** - The load balance weight for each WAN will be executed according to line speed and packet loss value. Usually, the WAN interface with low packet loss will have the higher ratio to be used.<br>**Custom** - You can distribute the usage ratio for each WAN interface by setting weights for bandwidth, latency, jitter, and packet loss respectively.<br>● **Upload /Download Bandwidth Weight -** The higher the weight is, the WAN interface with higher bandwidth will get higher usage.<br>● **Low Latency Weight -** It defines the time taken by Vigor router when sending the packets to the IP set in Link Condition Detection. The higher the weight is, the WAN interface with lower latency will get higher usage.<br>● **Low Jitter Weight** - It defines the change rate of latency. For stable session, small jitter value will be better. The higher the weight is, the WAN interface with lower jitter will get higher usage.<br>● **Less Packet Loss Weight -** It defines the proportion that packets will be discarded before arriving at the IP set in Link Condition Detection. The higher the weight is, the WAN interface with lower packet loss will get higher usage. |

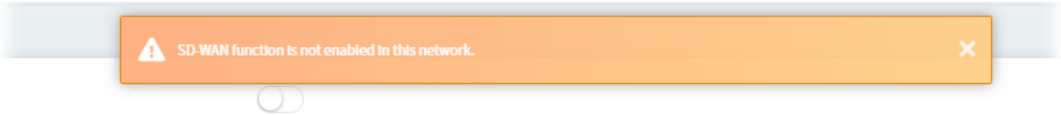
| | |
|---|---|
| **Clear** | Click to return to factory default setting. |
| **Save and Apply to CPE's** | Click to save the settings and apply them to all the CPE devices under the selected network group. |

### 8.4.4 Route Policy (SD-WAN)

The Route Policy feature gives you control over how different types of outbound traffic are routed, through any of the LANs, WANs or VPNs.

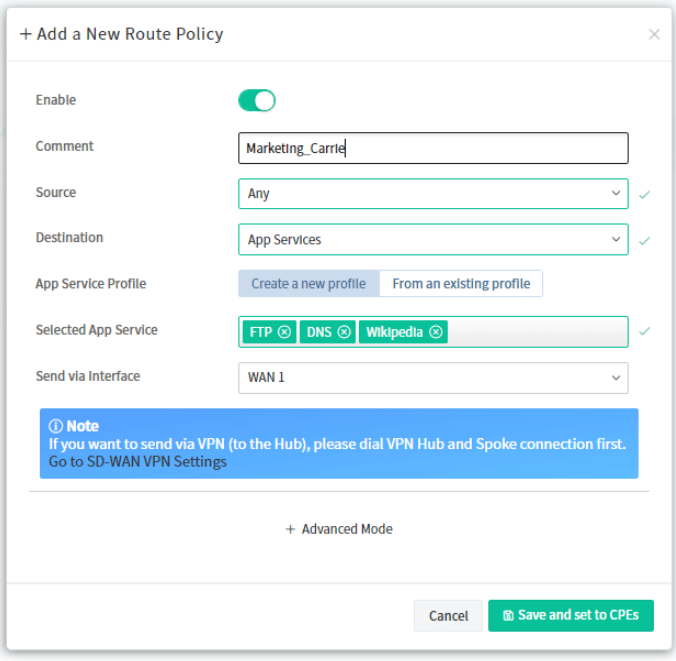



It is available only when SD-WAN feature is enabled for current used network group. If not enabled, a notification will appear to ask for SD-WAN activation.

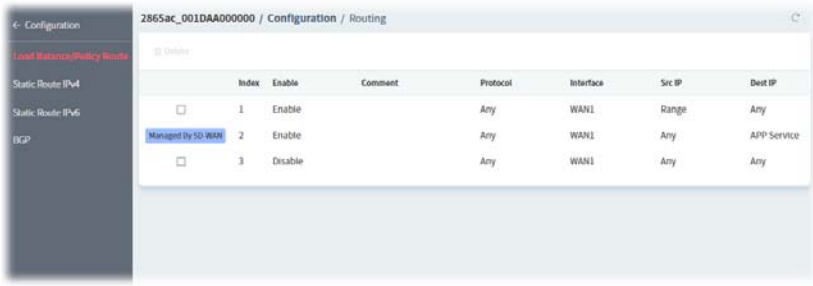



#### 8.4.4.1 Creating a Route Policy with Basic Mode

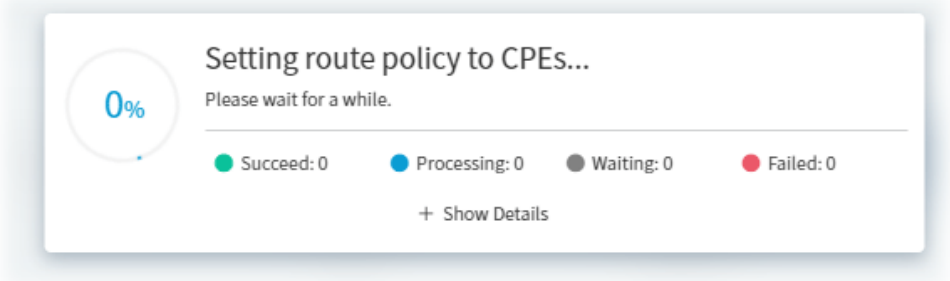
1. Click **+Add New Route Policy** to create a new profile. In default, the settings based on Basic Mode will be shown as follows.



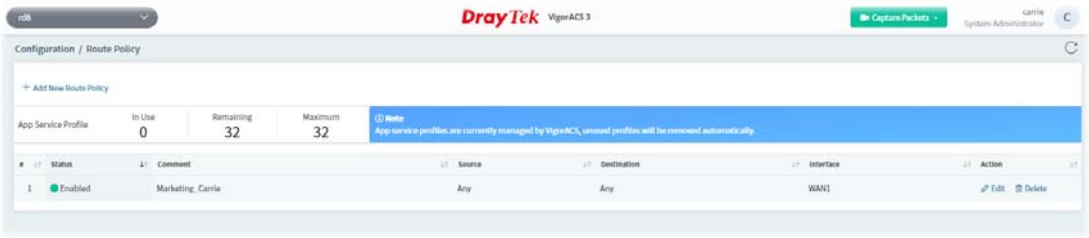
These parameters for Basic Mode are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Click the icon to enable / disable the policy profile. |
| **Comment** | Enter a name of the route policy profile. |
| **Source** | Set the source IP addresses to which this rule is to be applied.<br>**Any** - This rule applies to all source IP addresses.<br>**IP Range** - This rule applies to the specified range of source IP addresses. If there is only one source IP address, enter the address in both the Start and End fields. |
| **Destination** | Set the destination IP addresses to which this rule is to be applied.<br>**Any** - This rule applies to all destination IP addresses.<br>**IP Range** - This rule applies to the specified range of destination IP addresses. If there is only one destination IP address, enter the address in both the Start and End fields.<br>**VoIP** - This rule applies to VoIP packets.<br>**App Services** - This rule applies to App services.<br>● **Create a new profile** - Click this tab to create a new App Service Profile.<br>**Selected App Service** - Specify required App services (e.g., CNN, FTP, DNS, SMTP/SMTP STARTTLS, Wikipedia).<br>● **From an existing profile** - If an App service profile has been created previously, click this tab to choose an existing route policy profile.<br>**Selected an AP Service Profile** - From the drop-down list, choose the one you want.<br>Note that, when a route policy is set with App services, it will be applied to the router at the same time. Open Configuration>>Routing>>Load Balance / Policy Route. The routing rule with APP service will be highlighed and marked as "Managed By SD-WAN". It means the policy was created by ACS SD-WAN, and can be edited or deleted by ACS SD-WAN only.<br>  |
| **Send via Interface** | **WAN#/LAN#/DMZ/IP Routed Subnet** - Select an interface from the list. The traffic will be sent to the designated interface. |
| **+Advanced Mode** | Click to open the configuration page with more options. |
| **Save and Set to CPEs** | Save the above configuration and set to CPE devices. |

2. Click **Save and set to CPEs**.

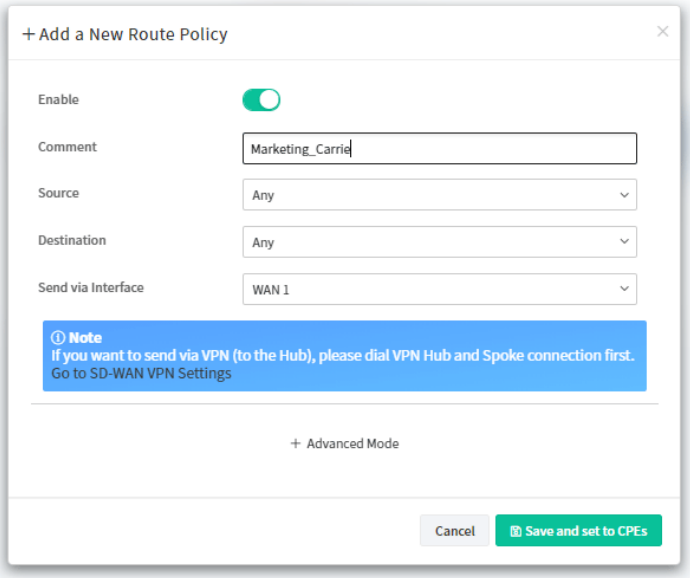



3. A route policy has been set successfully.

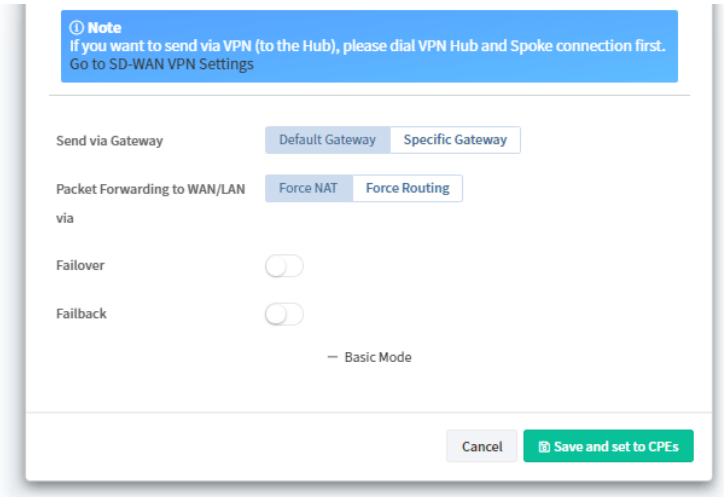


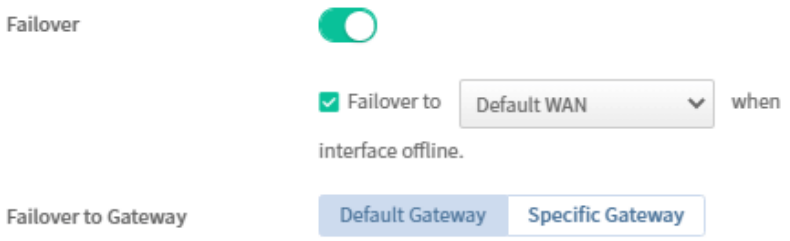

### 8.4.4.2 Creating a Route Policy with Advanced Mode

1. Click **+Add New Route Policy** to create a new profile. In default, the settings based on Basic Mode will be shown as follows.

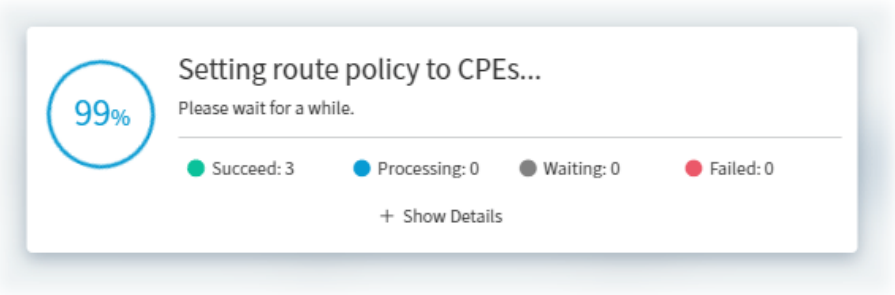



2. Click **+Advanced Mode** to get the following page.

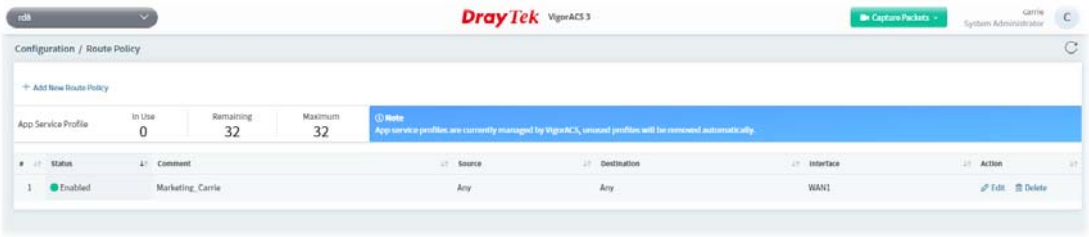



| Item | Description |
|---|---|
| **Send via Gateway** | **Default Gateway** - Traffic will be sent to the default gateway address of the specified interface.<br>**Specific Gateway** - Traffic will be sent to the specified gateway address instead of the default gateway address.<br>● **Specific Gateway** - Enter an IP address. |
| **Packet Forwarding to WAN/LAN** | **Force NAT** - The source IP address will not be used to connect to the remote destination. Network Address Translation (NAT) will be used, where a common IP address will be used.<br>**Force Routing** - The source IP address will be preserved when connecting to the remote destination. |
| **Failover** | Click the icon to enable / disable the failover function.<br>  <br><br>**Failover to** - If the interface specified above loses connection, traffic can be forwarded to an alternate interface or be scrutinized by an alternate route policy. Use the drop down list to choose an interface as an auto failover interface.<br>**Failover to Gateway** - The failed-over traffic can be sent to the gateway.<br>● **Default Gateway** - Click to use the default gateway.<br>● **Specific Gateway** - Click to use a specific gateway.<br>**Failover to Specify Gateway** - Enter an IP address.<br>**Failback** - Click the icon to enable / disable the failback function. |
| **Basic Mode** | Click to return to configuration page with less options. |
| **Save and set to CPEs** | Save the above configuration and set to CPE devices. |

4. Click **Save and set to CPEs**.

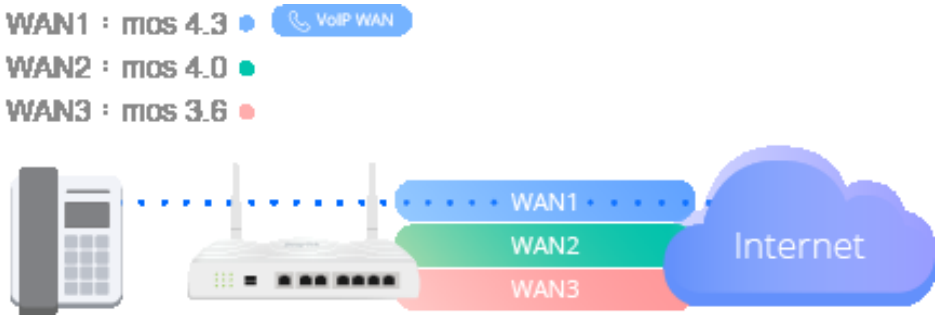



5. A route policy has been set successfully.

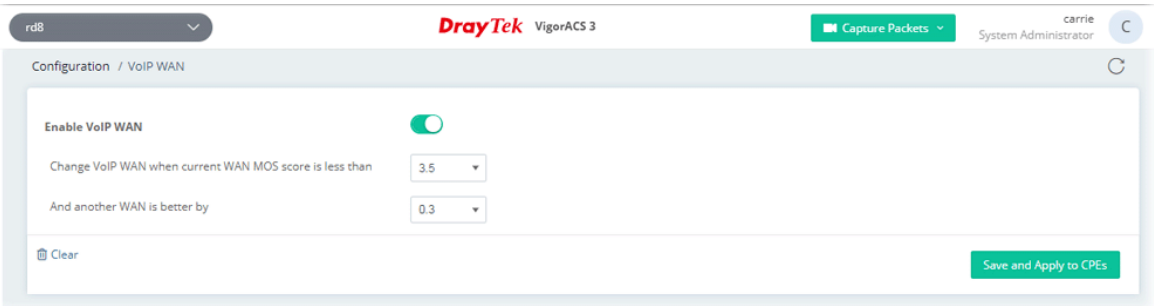



## 8.4.5 VoIP WAN (SD-WAN)

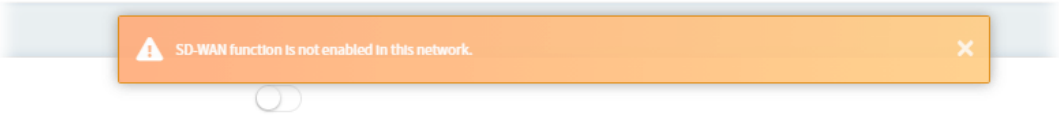
At present, the routers which support VoIP WAN (SD-WAN) are Vigor2927, Vigor2865 and Vigor2866.




Digital phones can be connected to any router via Ethernet interface (no need to support VoIP function). With the VoIP WAN function, we can set a range. As long as the signal strength falls within this range, you can use digital phones to communicate with the remote end.



It is available only when SD-WAN feature is enabled for current used network group. If not enabled, a notification will appear to ask for SD-WAN activation.

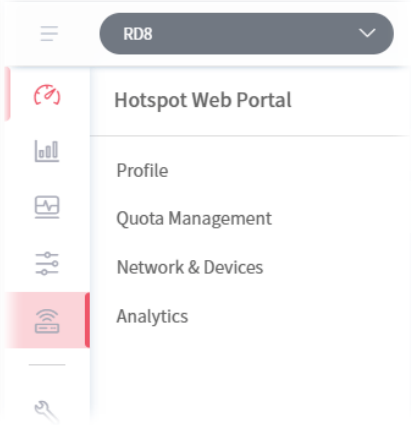



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Enable VoIP WAN** | Click to enable or disable the VoIP WAN connection.<br>If enabled, set a range for detecting the VoIP packets to pass through VigorACS server. |
| **Change VoIP WAN when current WAN MOS score is less than** | Specify a MOS number as the starting point.<br>MOS, the abbreviation of "Mean opinion score", represents overall quality of a system. The rating for MOS is from 1(bad) to 5 (excellent). |
| **And another WAN is better by** | Specify a MOS number as the ending point.<br>The rating for MOS is from 1(bad) to 5 (excellent). |
| **Clear** | Click to return to factory default setting. |
| **Save and Apply to CPE's** | Click to save the settings and apply to all of the CPE devices managed by VigorACS server. |

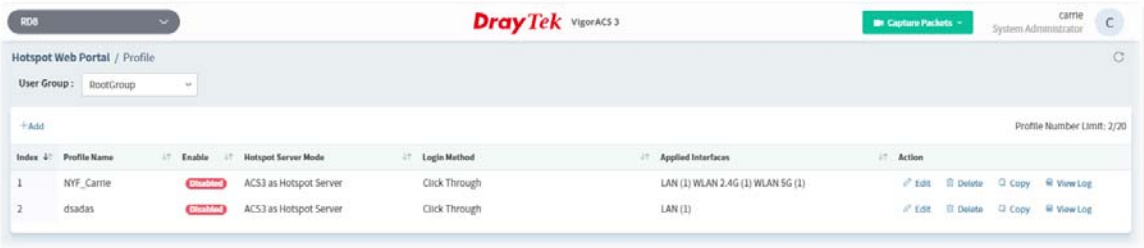
## 8.5 Hotspot Web Portal for SD-WAN Network Group

Configuration settings of Hotspot Web Portal will vary for group network and specified CPE.



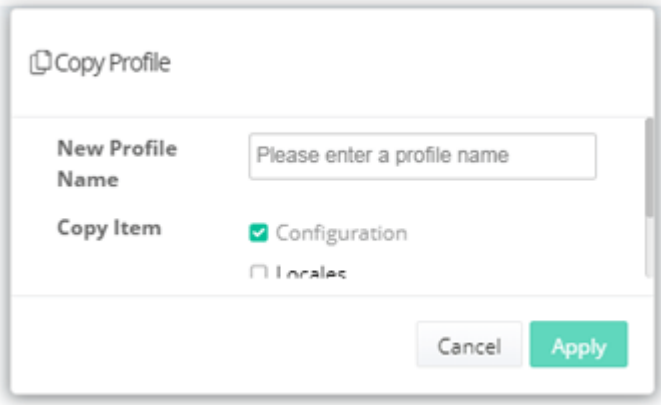

### 8.5.1 Profile

Profile is used to create or modify Hotspot Web Portal profiles. Up to 4 profiles can be created to meet different requirements according to LAN subnets, WLAN SSIDs, origin and destination IP addresses, etc.

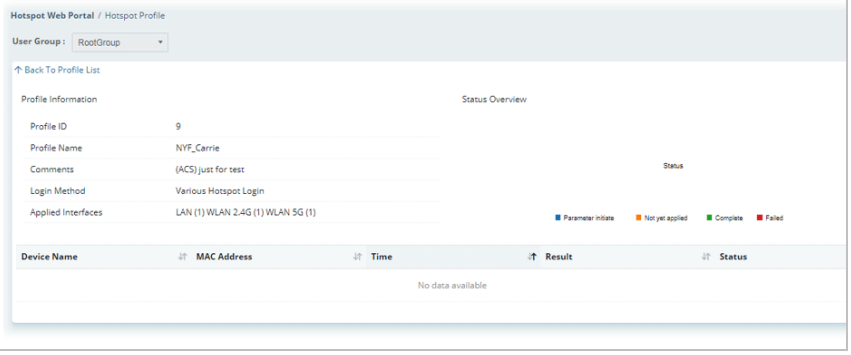



These parameters are explained as follows:

| Item | Description |
|---|---|
| **+Add** | Click to create a new hotspot web portal profile. |
| **Index** | Displays the index number of the profile. |
| **Profile Name** | Displays the name of the profile. |
| **Enable** | Displays if this profile is enabled or disabled. |
| **Hotspot Sever Mode** | Displays the hotspot server mode.<br>● ACS3 as Hotspot Server<br>● The 3rd Party Hotspot Server |
| **Login Method** | Displays the login method used by this profile. |
| **Applied Interfaces** | Displays the interfaces specified by this profile. |
| **Action** | **Edit –** Click to configure settings for the selected profile.<br>**Delete –** Click to delete the profile.<br>**Copy** – The hotspot profile can be copied to another hotspot profile. Enter the profile name and select items to be copied. Then click **Apply**. |

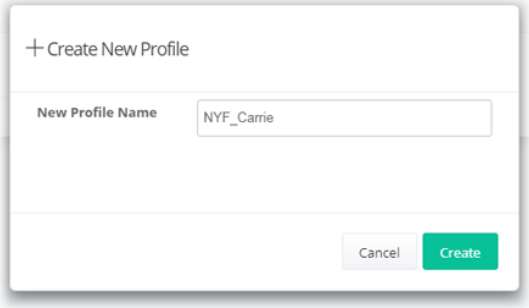



**View Log** – Click to review detailed information for the selected profile.

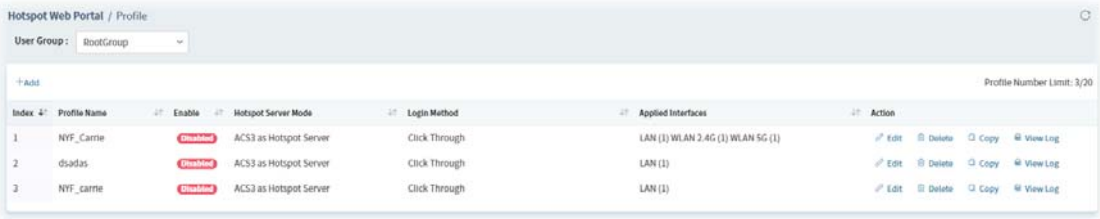



To create a new hotspot web portal profile:

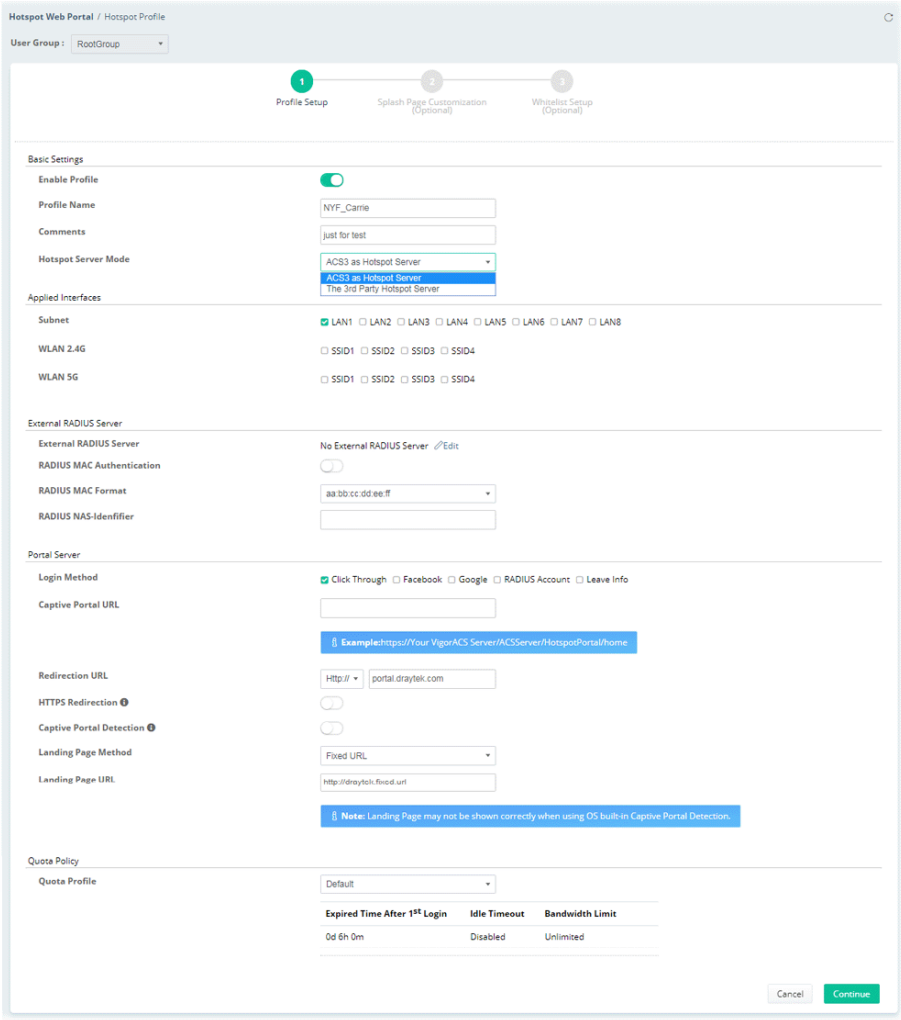
1. Click **+Add**.
2. From the following page, enter profile name (e.g., NYF_carrie) and click **Create**.




3. A new profile will be shown on the screen.

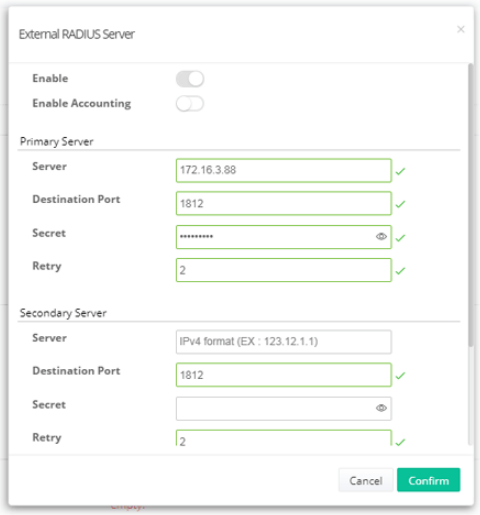


4. Click **Edit** for modifying the detailed settings.



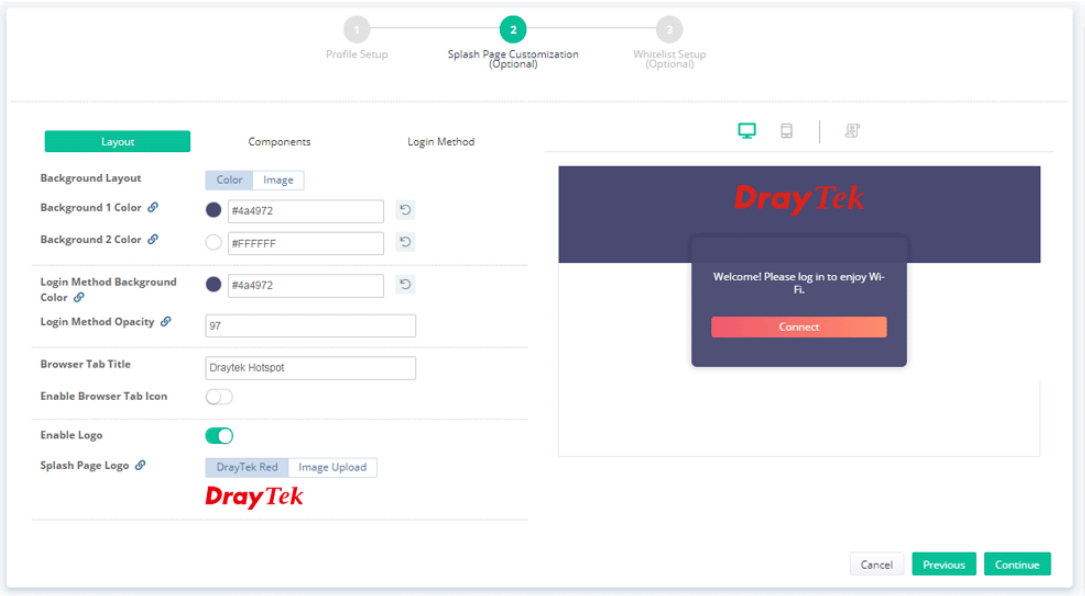

These parameters are explained as follows:

| Item | Description |
|---|---|
| | **Basic Settings** |
| **Enable Profile** | Check to enable this profile. |
| **Profile Name** | Enter a name for hotspot profile. |
| **Comments** | Enter a brief description to identify this profile. |
| **Hotspot Server Mode** | Specify the hotspot server.<br>● ACS3 as Hotspot Server - VigorACS server will be used as the server for authentication.<br>● The 3rd Party Hotspot Server - The third party server will be used as the server for authentication. |
| | **Applied Interfaces** |
| **Subnet** | The current Hotspot Web Portal profile will be in effect for the selected subnets. |
| **WLAN 2.4G/5G** | The current Hotspot Web Portal profile will be in effect for the selected WLAN SSIDs. |
| | **External RADIUS Server** |

| | |
|---|---|
| **External RADIUS Server** | Displays the IP address of the external RADIUS Server.<br>**Edit** - If required, Click to modify the RADIUS Server.<br>  |
| **RADIUS MAC Authentication** | 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. |
| **RADIUS MAC Format** | Select the MAC address format. |
| **RADIUS NAS-Identifier** | Enter the server's ID. |
| | **Portal Server** |
| **Login Method** | There are several methods to be selected as for portal server.<br>● Click Through -<br>● Facebook -<br>● Google -<br>● RADIUS Account -<br>● Leave Info - |
| **Captive Portal URL** | Enter the captive portal URL. |
| **Redirection URL** | Enter the URL to which the client will be redirected. |
| **HTTPS Redirection** | If this option is selected, unauthenticated clients accessing HTTPS websites will be redirected to the login page, but the browser may alert the user of certificate errors. If this option is not selected, attempts to access to HTTPS website will time out without redirection. |
| **Captive Portal Detection** | If this option is selected, the web portal page is triggered automatically when an unauthenticated client tries to access the Internet. |
| **Landing Page Method** | Specify the landing page for the client after passing the authentication.<br>● **Fixed URL** - Specify a landing page URL.<br>● **User Request** - The user will be redirected to the URL they initially requested.<br>● **Bulletin Message** - Show a message on Bulletin. |
| **Landing Page URL** | It is available when **Fixed URL** is selected as **Landing Page Method.**<br>Specifies the webpage that will be displayed after the user has successfully authenticated. |

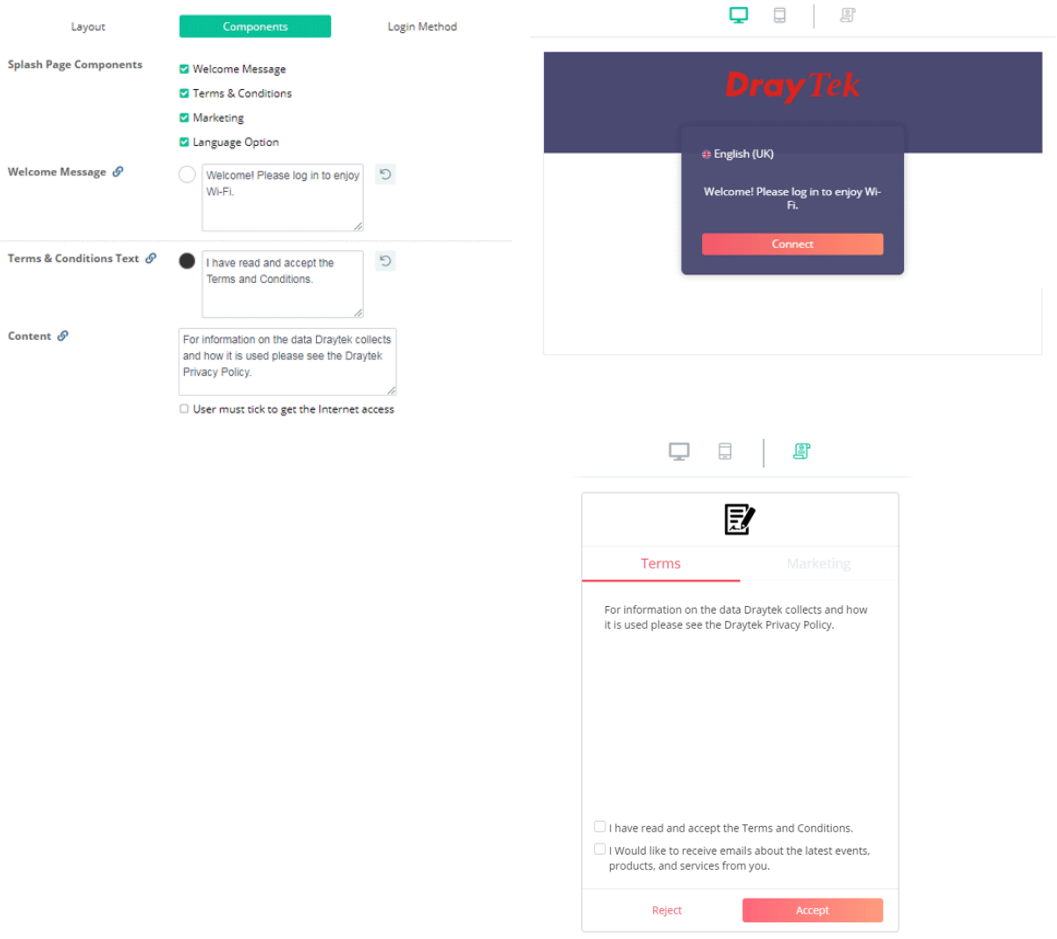
| | |
|---|---|
| | The user will be redirected to the specified URL. This could be used for displaying advertisements to users, such as guests requesting wireless Internet access in a hotel. |
| **HTML/Image for Bulletin Message** | **HTML/Image** is available when **Bulletin Message** is selected as **Landing Page Method.**<br>The message configured here will be briefly shown for a few seconds to the user. |
| **Facebook ID** | It is available when **Facebook** is selected as **Landing Page Method.**<br>Enter a valid Facebook developer app ID. |
| **Facebook Secret** | It is available when **Facebook** is selected as **Landing Page Method.**<br>Enter the secret configured for the APP ID entered above. |
| **Google ID** | It is available when **Google** is selected as **Landing Page Method.**<br>Enter a valid Google app ID. |
| **Google Secret** | It is available when **Google** is selected as **Landing Page Method.**<br>Enter the secret configured for the APP ID entered above. |
| | **Quota Policy** |
| **Quota Profile** | Choose a policy profile to apply to web portal clients.<br>Refer to **8.5.2 Quota Management** to define more profiles if required. |
| **Cancel** | Click to Discard current modification. |
| **Continue** | Click to get into next page. |

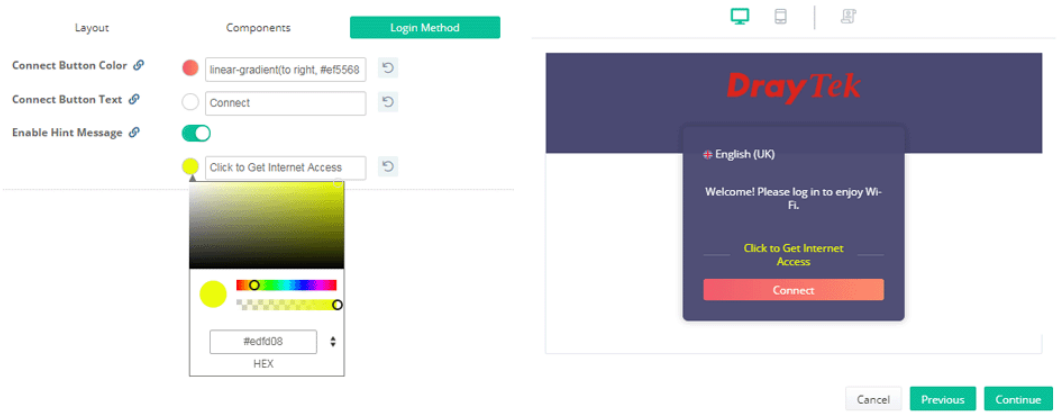
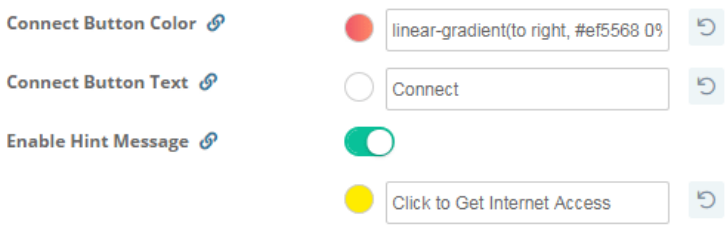
5. Choose **Click Through** as Login Method. Then, click **Continue** for Splash Page Customization. Splash Page Customization is available for **ACS3 as Hotspot Server** only.

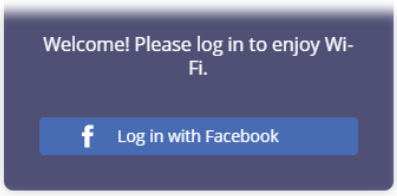
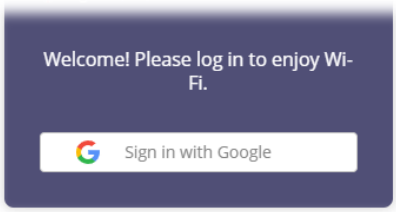
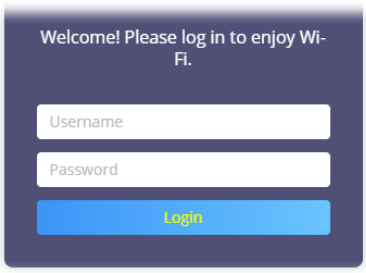


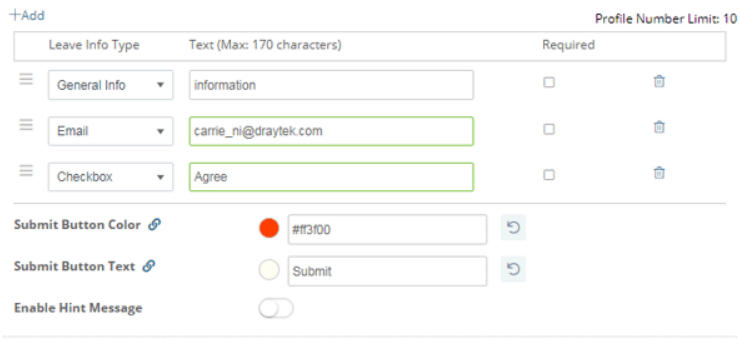

These parameters are explained as follows:

| Item | Description |
|---|---|
| | **Layout** |
| **Background Layout** | Select either **Color** or **Image** as the login page background scheme. |
| **Background 1 / 2** | Select the background color of the login window (up and down layer) from |

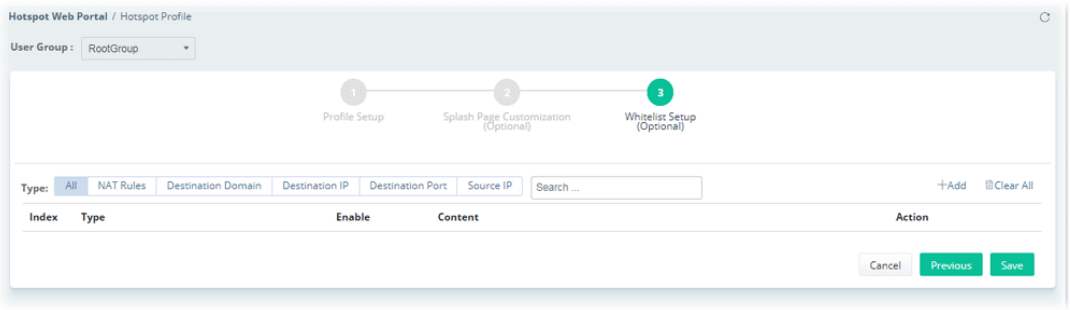
| | |
|---|---|
| **Color** | the predefined color list, or enter the RGB value (with the format of HEX). |
| **Login Method Background Color** | Select the background color of the login panel from the predefined color list, or enter the RGB value (with the format of HEX). |
| **Login Method Opacity** | Adjust the opacity (1-100) of the login panel. |
| **Browser Tab Title** | Enter the text to be shown as the webpage title in the browser. |
| **Enable Browser Tab Icon** | Click to enable / disable the browser tab icon for VigorACS WUI. |
| **Browser Tab Icon** | **DrayTek** - It is default setting.<br>**Image Upload** - Select an image by using Browse and upload to VigorACS. It will be used as the browser tab icon for VigorACS WUI. |
| **Enable Logo** | Click to enable / disable the logo display on the login window. |
| **Splash Page Logo** | **DrayTek Red** - It is default setting.<br>**Image Upload** - Select an image by using Browse and upload to VigorACS. It will be used as the logo display on the login window. |
| **Components**<br>  | |
| **Splash Page Components** | Defines the content of the splash page. Select the one(s) to show on the login page.<br>● Welcome Message<br>● Terms & Conditions<br>● Marketing |

| | |
|---|---|
| | • Language Option |
| **Welcome Message** | Enter the text to be displayed as the welcome message. |
| **Terms & Conditions Text** | If it is enabled, it will be shown on the second page after clicking the Connect / Submit button on the login page.<br>Enter the text which will be shown after the **checkbox** for Terms and Conditions. |
| **Content** | If it is enabled, it will be shown on the second page after clicking the Connect / Submit button on the login page.<br>Enter the text to be displayed in the Terms and Conditions window. |
| **Marketing Text** | If it is enabled, it will be shown on the second page after clicking the Connect / Submit button on the login page.<br>Enter the text which will be shown after the **checkbox** for marketing information. |
| **Marketing Content** | If it is enabled, it will be shown on the second page after clicking the Connect / Submit button on the login page.<br>Enter the text to be displayed in the Terms and Conditions window. |
| **Language** | Use the drop down menu to select a language.<br>**Browse** - Select a properties file from your host.<br>**Upload** - Click to upload a language file.<br>**Download** - Click to download a language file. |
| | **Login Method**<br>  |
| **Connect ...** | It is available when **Click Through** is selected as Landing Page Method.<br>**Connect Button Color -** Select the color of the connect button from the predefined color list, or using the RGB value (entered with the format of HEX).<br>**Connect Button Text -** Enter the text to be displayed on the connect button. The color of the text can be set from the predefined color list or using the RGB value (entered with the format of HEX).<br>  |
| **Facebook ...** | It is available when **Facebook** is selected as Landing Page Method. |

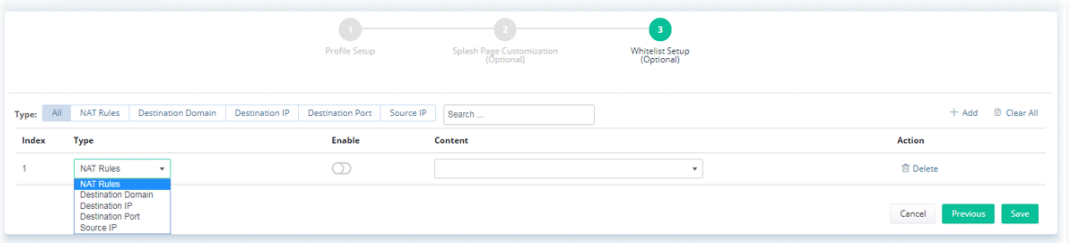
| | |
|---|---|
| |  <br>**Facebook Login (Login with Facebook) -** Enter the text to be displayed on the login button. The color of the text can be set from the predefined color list or using the RGB value (entered with the format of HEX). |
| **Google ...** | It is available when **Google** is selected as Landing Page Method.<br>  <br>**Google Login (Sign in with Google) -** Enter the text to be displayed on the login button. The color of the text can be set from the predefined color list or using the RGB value (entered with the format of HEX). |
| **RADIUS ...** | It is available when **RADIUS Account** is selected as Landing Page Method.<br>  <br>**RADIUS Username -** Enter the account name for passing the RADIUS authentication.<br>**RADIUS Password -** Enter the password for passing the RADIUS authentication.<br>**RADIUS Login Button Color -** Select the color of the login button from the predefined color list, or using the RGB value (entered with the format of HEX).<br>**RADIUS Login Button Text -** Enter the text to be displayed on the login button. The color of the text can be set from the predefined color list or using the RGB value (entered with the format of HEX). |
| **Submit ...** | It is available when **Leave Info** is selected as Landing Page Method.<br> |

| | |
|---|---|
| |  <br><br>**+Add** - Click to add general information, email or check box on the login panel which will be shown on the login panel as entry box or check box.<br>**Submit Button Color -** Select the color of the submit button from the predefined color list, or using the RGB value (entered with the format of HEX).<br>**Submit Button Text -** Enter the text to be displayed on the submit button. The color of the text can be set from the predefined color list or using the RGB value (entered with the format of HEX). |
| **Enable Hint Message** | Click to enable / disable the hint message.<br>If enabled, enter a sentence as a hint message. |
| **Cancel** | Click to Discard current modification. |
| **Previous** | Click to return to the previous page. |
| **Continue** | Click to get into the next page. |

6. After finished the settings, click **Continue** to open the following page. This page configuration is optional.




Click **+Add** to create a whitelist profile and apply to this hotspot profile.

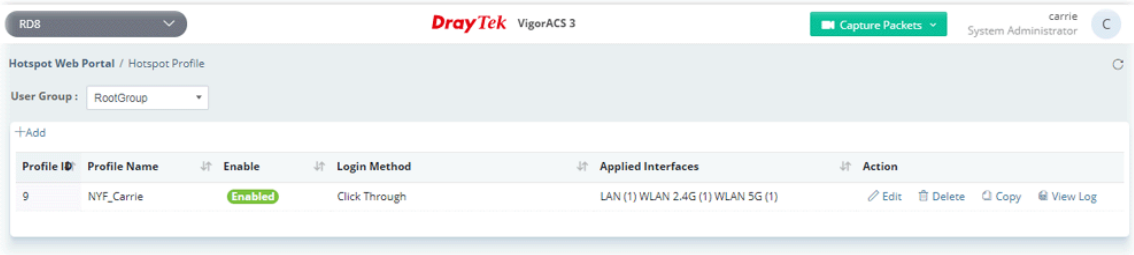



These parameters are explained as follows:

| Item | Description |
|---|---|
| **+Add** | Click to add a new whitelist profile. |
| **Clear All** | Click to remove all of the whitelist profiles. |

| | |
|---|---|
| **Type** | Use the drop-down list to specify the type of the whitelist profile.<br>● NAT Rules<br>● Destination Domain<br>● Destination IP<br>● Destination Port<br>● Source IP |
| **Enable** | Click to enable / disable the whitelist profile. |
| **Content** | Enter the value if required. It varies according to the type selected. |
| **Action** | **Delete** - Click to remove the selected whitelist profile. |
| **Cancel** | Click to Discard current modification. |
| **Previous** | Click to return to the previous page. |
| **Save** | Click to save the changes in this page. |

7. Click **Save** to finish and save the configuration.




## 8.5.2 Quota Management

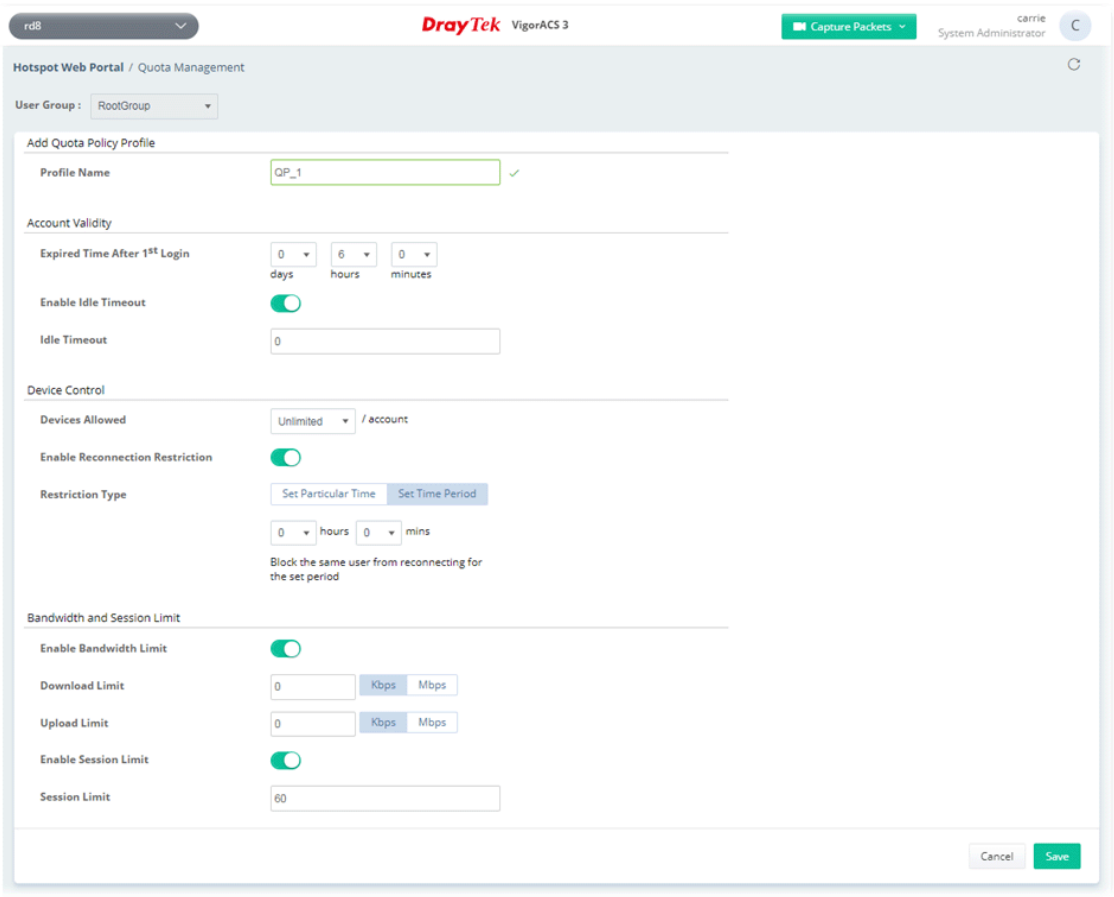
Quota management integrates bandwidth limit, session limit, applicable device number and validity period into one profile. This profile is prepared for a hotspot web portal profile.

These parameters are explained as follows:

| Item | Description |
|---|---|
| **User Group** | Specify a user group to display the quota management profiles under that group. |
| **+Add** | Create a new profile. |
| **Delete** | Click to delete the profile. |
| **Index** | Displays the index number of the profile. |
| **Profile Name** | Displays the name of the profile. |
| **Expired Time After 1st Login** | Displays the time remained for use after the first login. |
| **Idle Timeout** | Displays if the function is enabled or disabled. |

| | |
|---|---|
| **Bandwidth Limit** | Displays the number of bandwidth limit. |
| **Session Limit** | Displays the number of session limit. |

The following setting page appears when **+Add** is clicked.



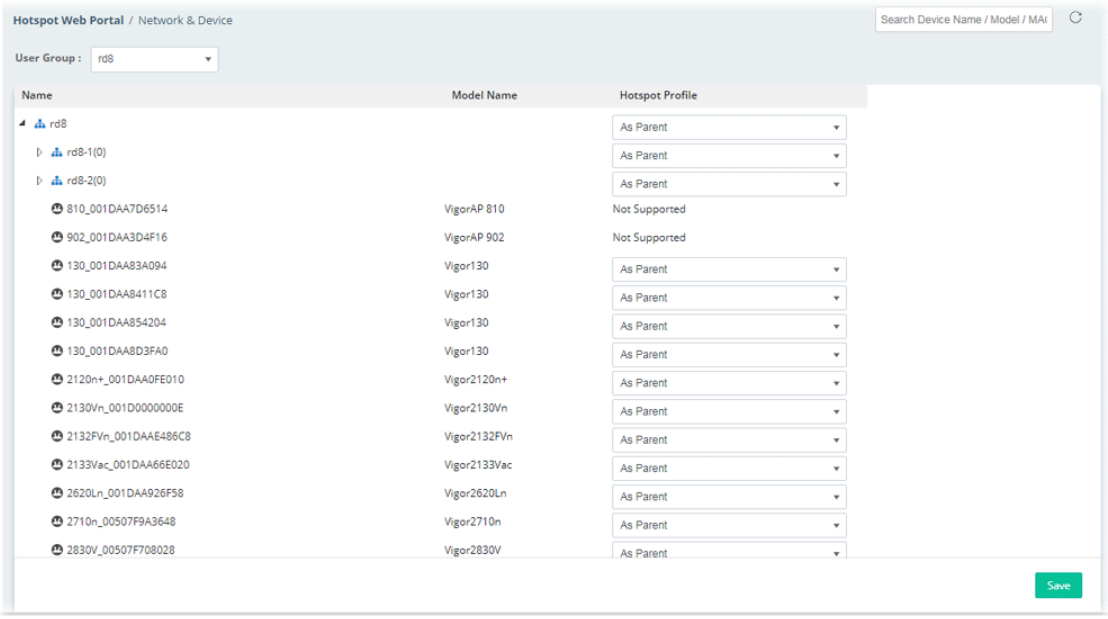

These parameters are explained as follows:

| Item | Description |
|---|---|
| | **Add Quota Policy Profile** |
| **Profile Name** | Enter a name for this profile. |
| **Account Validity** | |
| **Expired Time After 1st Login** | Enter the time (days, hours and minutes) remained for use after the first login. |
| **Enable Idle Timeout** | Click to enable the function of idle timeout.<br>**Idle Timeout** - Set the timeout for breaking down the Internet after passing through the time without any action. |
| | **Device Control** |
| **Devices Allowed** | Enter a number (1-100) of devices applied with this profile.<br>"Unlimited" means no number limitation. |
| **Enable Reconnection Restriction** | Click to block the same client reconnecting to Internet.<br>**Restriction Type** - There are two types to set the time period.<br>● **Set Particular Time** - The same user is unable to connect to Internet before the time setting. |

| | |
|---|---|
| | • **Set Time Period** - The same user is unable to connect to Internet before the time period. |
| | **Bandwidth and Session Limit** |
| **Enable Bandwidth Limit** | Click to enable the function of bandwidth limit.<br>**Download Limit** - Enter a value to define the maximum data traffic (downloading) for each client connecting to Vigor device.<br>**Upload Limit** - Enter a value to define the maximum data traffic (uploading) for each client connecting to Vigor device.<br>**Enable Session Limit** - Click to enable and set session limit.<br>• **Session Limit** - Enter a value to define the maximum sessions for each client connecting to Vigor device. |
| **Cancel** | Discard current modification. |
| **Save** | Save the current settings. |

### 8.5.3 Network & Devices

Each network group and / or device can be assigned with different hotspot profile.

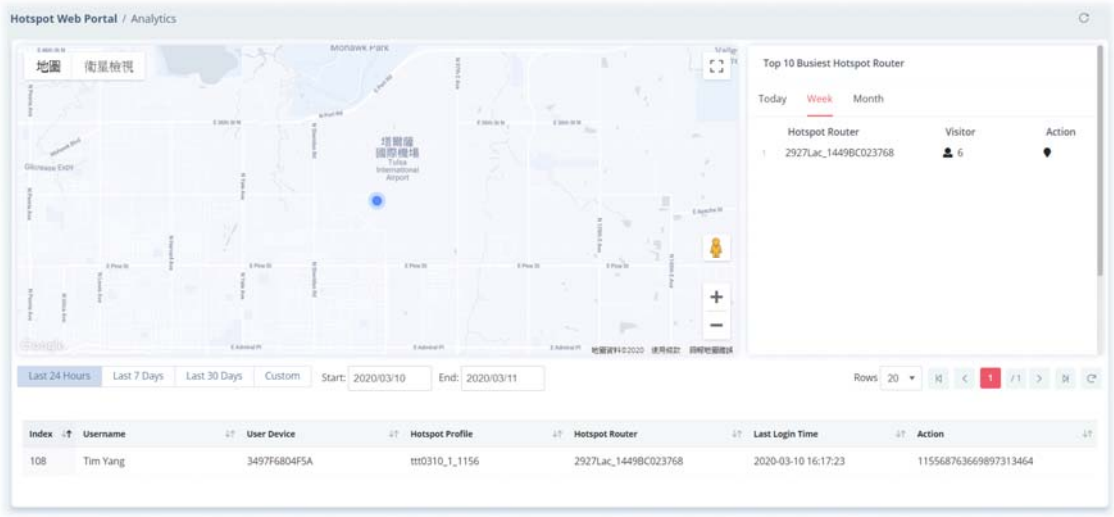



These parameters are explained as follows:

| Item | Description |
|---|---|
| **User Group** | Specify a network group. Specify the hotspot profile(s) for the device under the selected network group. |
| **Hotspot Profile** | Select a hotspot profile for the selected group / device.<br>**As Parent** - Use the same setting as the previous layer. |
| **Save** | Save the current settings. |

### 8.5.4 Analytics

This page displays the locations of the routers on the map, top 10 busiest hotspot routers and a list of clients accessing into the Internet via the hotspot web portal.



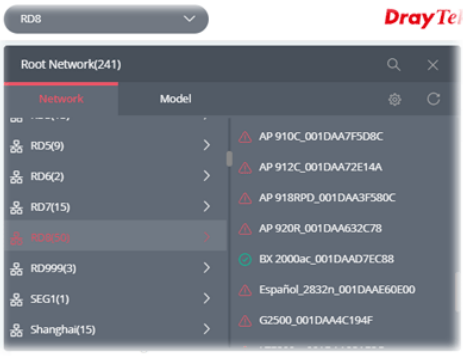

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Map** | Displays the location of the client. |
| **Top 10 Busiest Hotspot Router** | Displays the top 10 busiest routers.<br>**Today** - Display the name of the router, number of clients and performed action at the present day.<br>**Week** - Displays the name of the router, number of clients and performed action within one week.<br>**Month** - Displays the name of the router, number of clients and performed action within one month. |
| **Last 24 Hours, Last 7 Days, Last 30 Days, Custom** | Choose the time period, last 24 hours, 7 days or 30 days. Or click Custom to specify a certain period, for displaying the router location. |
| **Index** | Displays the index number of the router. |
| **Username** | Displays the username of the client. |
| **User Device** | Displays the MAC address of the router. |
| **Hotspot Profile** | Displays the name of the hotspot profile used. |
| **Hotspot Router** | Displays the name of the router used by the client to access into Internet. |
| **Last Login Time** | Displays the last login time. |

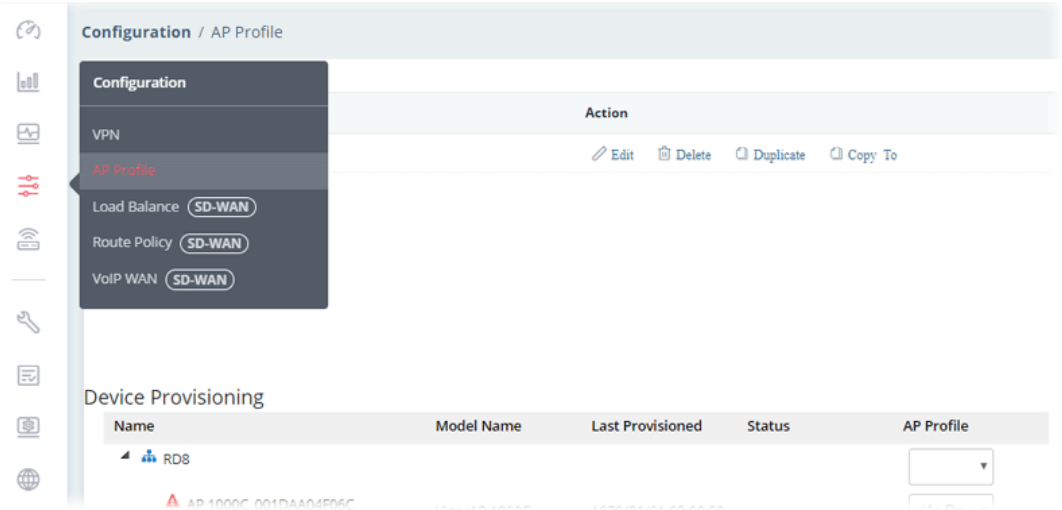
# Applications

## A.1 How to apply an AP profile to AP device(s)?

1. Choose a group containing with access points (e.g., “RD8” in this case) from Root Network.

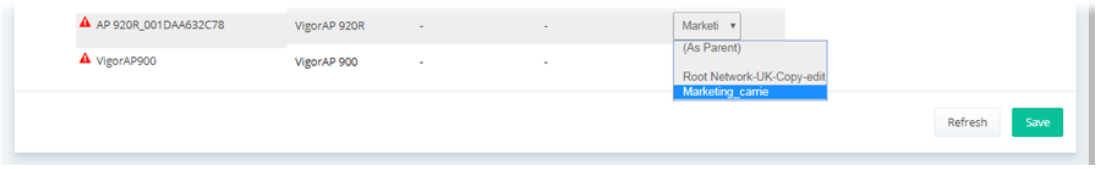



2. Open **Configuration>>AP Profile**.




In the **Device Provisioning**, all of the access points grouped under “RD8” are displayed under the field of Name.

3. Select the AP (e.g., AP 920R in this case) required to apply new AP profile; and use the drop down list of **AP Profile** to specify a profile (e.g., Marketing_carrie in this case).




---

You can click **+Add New Profile** to create a new AP profile if there is no AP profile to be chosen or the existed AP profile is not suitable for the AP model.

---

Click **Save**. The settings in web user interface of the selected VigorAP will be overwritten with the settings configured in AP profile immediately.

# Part V

## Device Menu

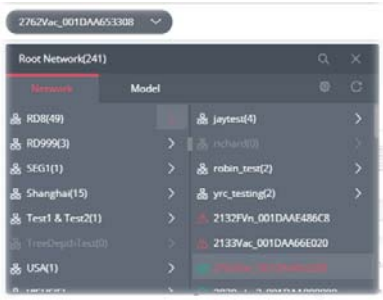
# Chapter 9 Device Menu

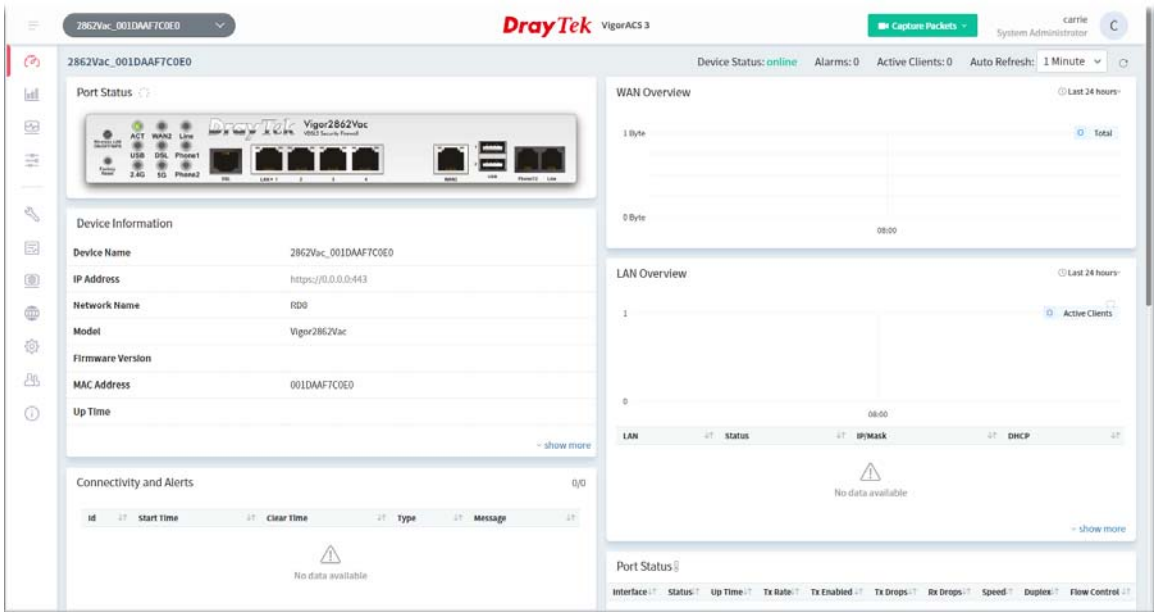
On the dashboard for CPE, the Device menu contains:

- Dashboard
- Statistics
- Monitoring
- Configuration

## 9.1 Dashboard for CPE

Use the drop-down menu on the top of the left side to select a CPE (e.g., Vigor2862 series).

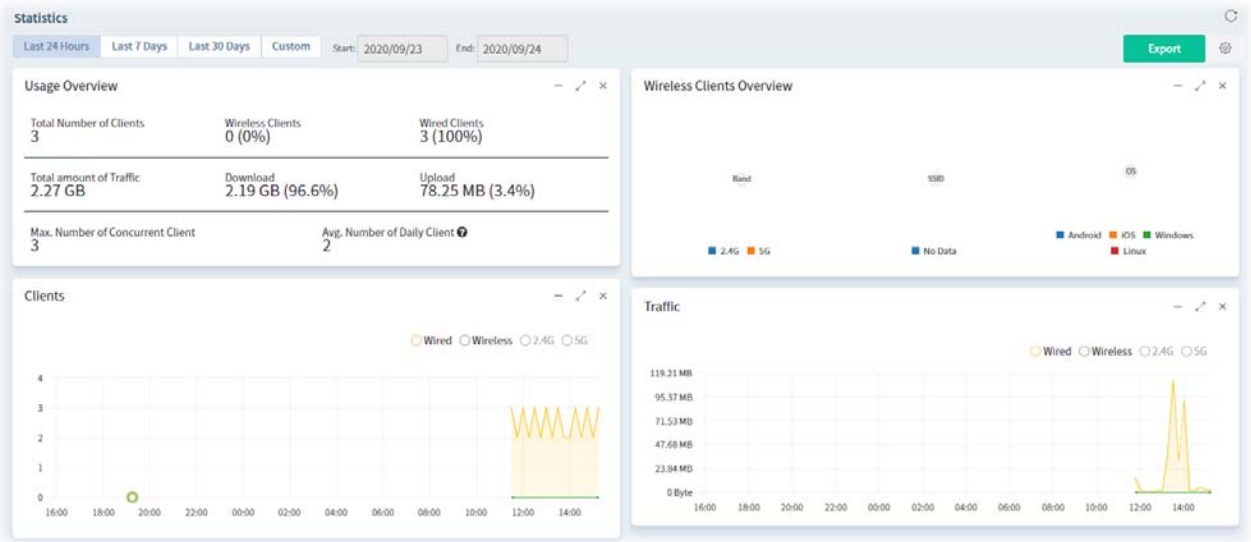


## 9.2 Statistics for CPE

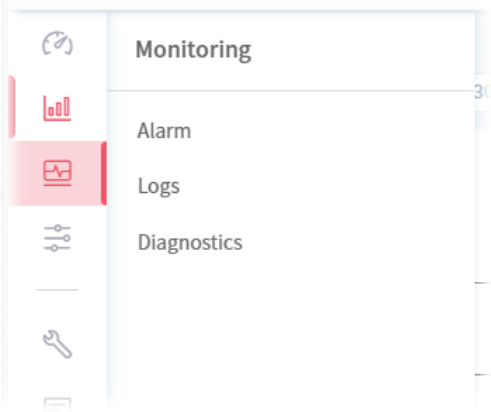
Statistics is available for a selected group network or CPE.

The page offers statistics for the selected device listed under root networks, including usage overview, wireless clients Overview, data traffic, device ranking, and client ranking. By clicking Last 24 Hours, Last 7 Days, Last 30 Days or Custom setting (define the period), the administrator can obtain various statistics within the time period.



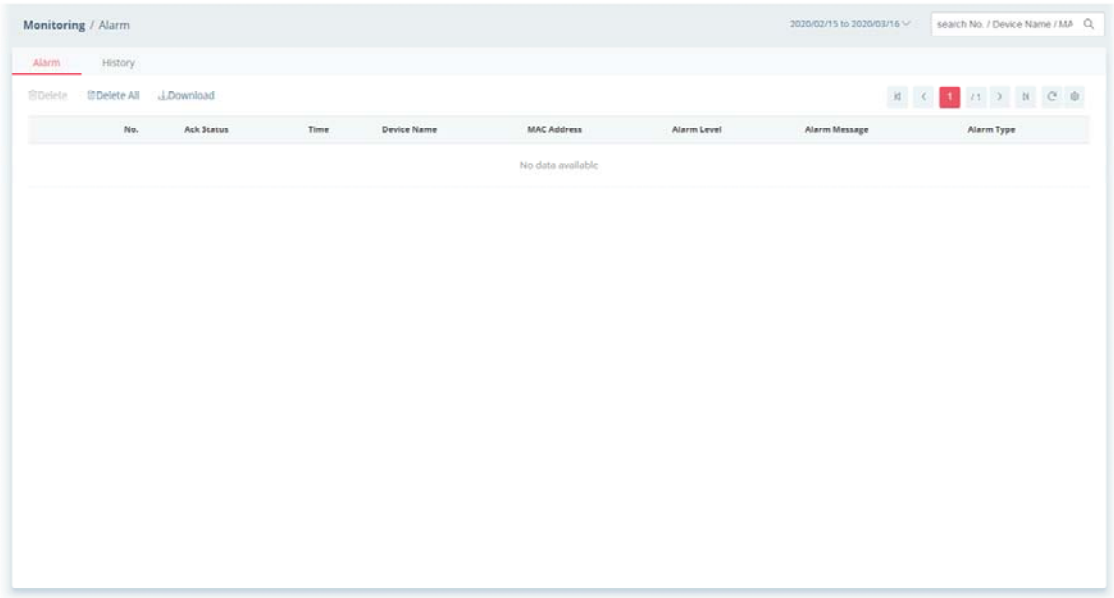
## 9.3 Monitoring

Monitoring menu offers options for monitoring the normal and abnormal actions for network, group and CPE. This section offers Monitoring menu items for a selected CPE (in this case, Vigor2862 series is used as an example).




### 9.3.1 Alarm

Alarm message will be recorded on VigorACS 3 server when there is a trouble happened to the device (CPE). Only the users within the same user group will be notified for the message.



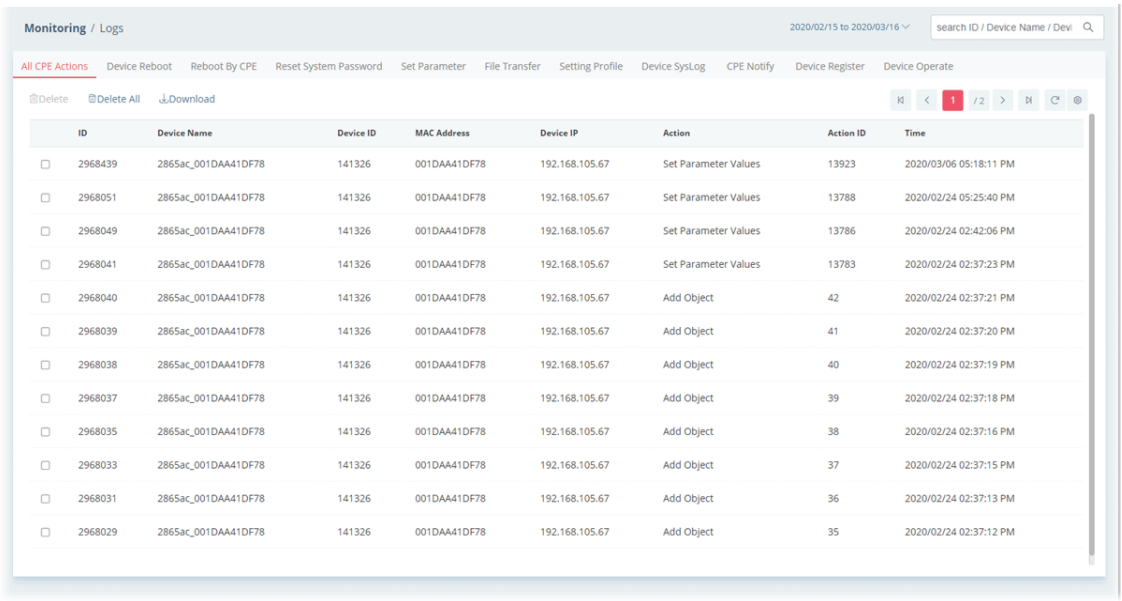

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Alarm / History** | **Alarm –** Display the alarm records recently.<br>**History –** Display all the alarm records that have been solved and cleared. |
| **Delete** | Clear the alarm record which has been solved by VigorACS 3. |
| **Delete All** | Clear all of the alarm records which have been solved by VigorACS 3. |
| **Download** | Click this button to save alarm log as a XLS file. |
| **No.** | Display the index number of the alarm. It is offered by VigorACS 3 |

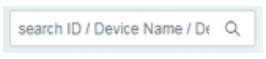
| | |
|---|---|
| | automatically. |
| **Ack Status** | Display the status of the records with the type specified here (Not Ack or Acked). |
| **Time** | Displays the time of the device to be monitored. |
| **Device Name** | Displays the name of the monitored device. |
| **MAC Address** | Displays the MAC address of the monitored device. |
| **Alarm Level** | Displays the alarm message with the severity (e.g., Critical) specified. |
| **Alarm Message** | Displays a brief explanation for the alarm sent by VigorACS 3 automatically. |
| **Alarm Type** | Displays the alarm message with the type specified. |

### 9.3.2 Logs

It provides records of action executed, name of the selected device, MAC address, Device IP, and Current Time for CPE device managed and monitored by VigorACS.




These parameters are explained as follows:

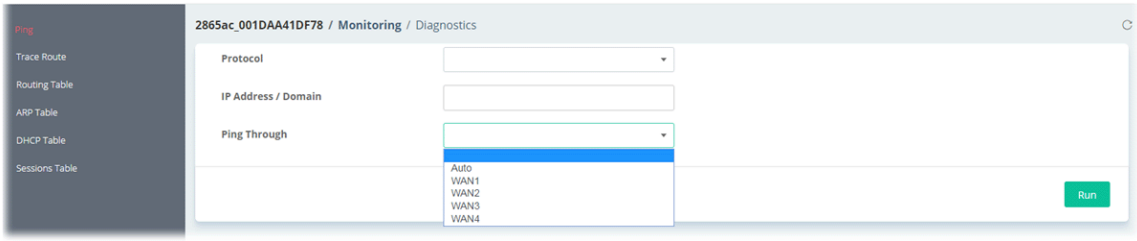
| Item | Description |
|---|---|
| **Log Type** | Click one of the tabs (e.g., All CPE Actions, Device Reboot, Reboot By CPE, Reset System Password, Set Parameter, File Transfer, Setting Profile, Device SysLog, CPE Notify, Device Register, Device Operate and etc.) to display related log on this page. |
|   | Enter the condition for VigorACS to search and display relational information. |
| **Delete** | Clear the alarm record which has been solved by VigorACS. |
| **Delete All** | Clear all of the alarm records which have been solved by VigorACS. |
| **Download** | Click this button to save the log as an XLS file. |

## 9.3.3 Diagnostics

Diagnostic Tools provide a useful way to **view** or **diagnose** the status of Vigor router. Here, Vigor2862 series is used as an example.

### 9.3.3.1 Ping

This page allows performing a ping job for the selected CPE.

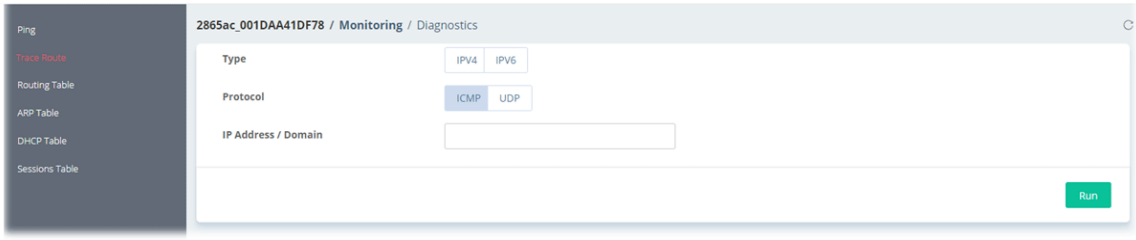



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Protocol** | Choose IPV4 /IPV6 for ping action. |
| **IP Address / Domain** | Enter the IPv4/IPv6 address of the host/IP that you want to ping. |
| **Ping Through** | Use the drop down list to choose the interface (e.g., WAN, LTE) that you want to ping through or choose **Auto** to be determined by the router automatically. |
| **Run** | Click to start the ping work. The result will be displayed on the screen. |

### 9.3.3.2 Trace Route

This page allows you to trace the routes from router to the host. Simply Enter the IP address of the host in the box and click **Run**. The result of route trace will be shown on the screen.

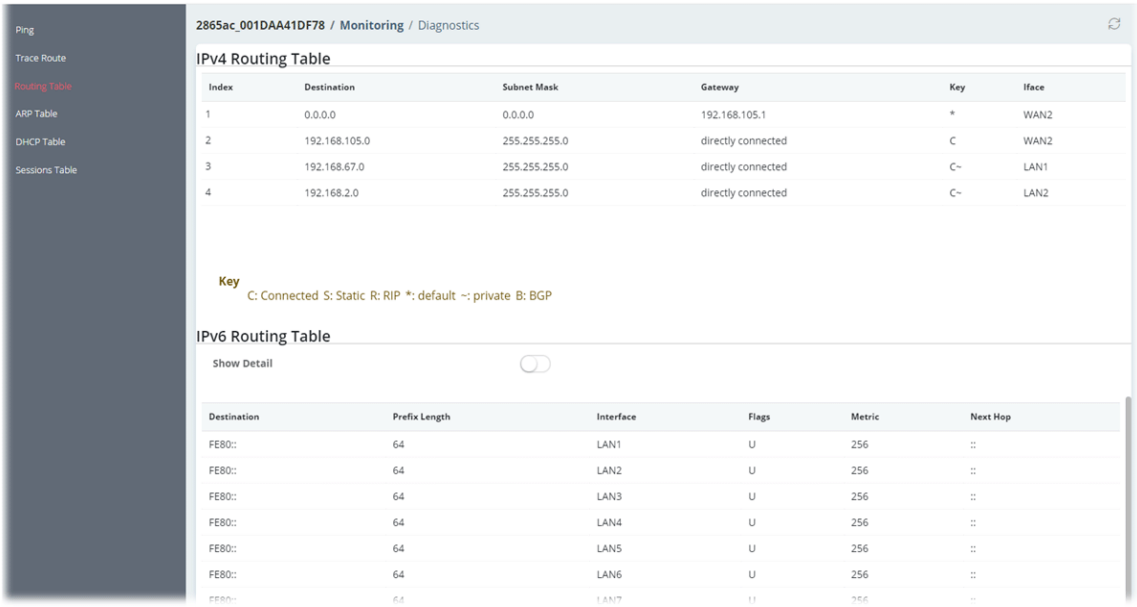



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Type** | Click IPv4 or IPv6 to display corresponding information for it. |
| **Protocol** | Click ICMP or UDP that you want to ping through. |
| **IP Address / Domain** | Enter the IPv4/IPv6 address or domain name of the host. |
| **Run** | Click to start route tracing work. |

### 9.3.3.3 Routing Table

This page displays the routing information for the selected CPE.

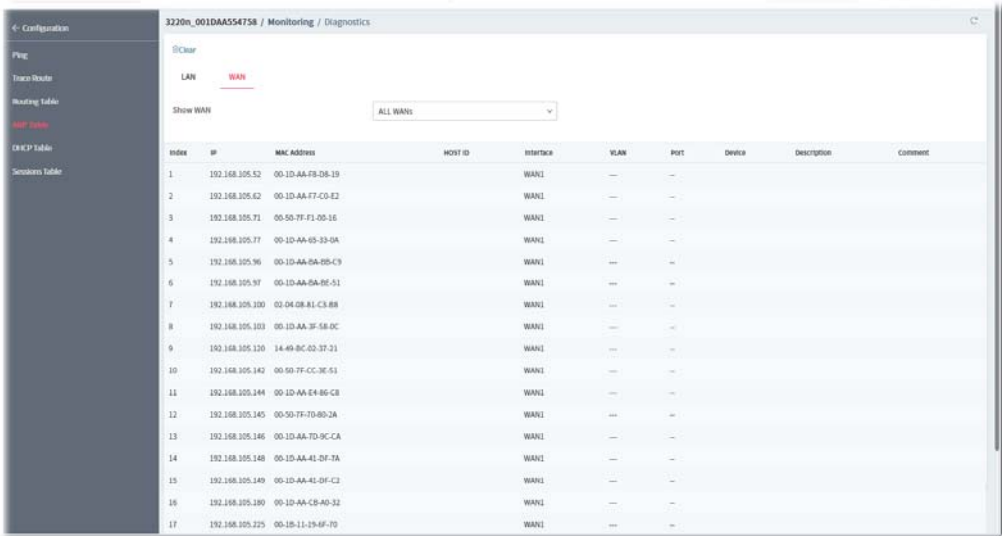



These parameters are explained as follows:

| Item | Description |
|---|---|
| **IPv4 Routing Table** | Displays the routing information including index number, destination IP, subnet mask, gateway, key and interface. |
| **IPv6 Routing Table** | **Show Detail** - Click to display more detailed information.<br>Displays the routing information including destination IP, prefix length, interface, flags, metric and next hop. |

### 9.3.3.4 ARP Table

This page displays the content, including IP address, MAC address, Host ID, interface, VLAN, port number, device name, description and comment, of the ARP (Address Resolution Protocol) cache held in the router.

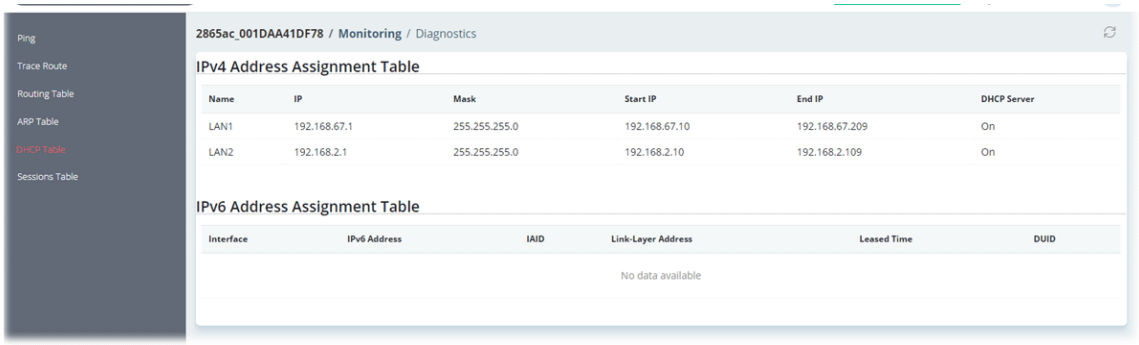


These parameters are explained as follows:

| Item | Description |
|---|---|
| **LAN/WAN** | **LAN** - Click to display the ARP table of devices on LAN, including LAN device and wireless LAN device. In default, this page will display the information for LAN and VLAN.<br>● Show LAN - Select a LAN interface / All LANS.<br>● Show VLAN - Select a VLAN tunnel / All VLANs.<br>**WAN** - Click to display the ARP table of devices on WAN. In default, this page will display information for all WANs.<br>● Show WAN - Select a WAN interface. |
| **Clear** | Delete all records. |

### 9.3.3.5 DHCP Table

This page shows the IPv4/IPv6 address of LAN device(s) which is assigned by the selected CPE.

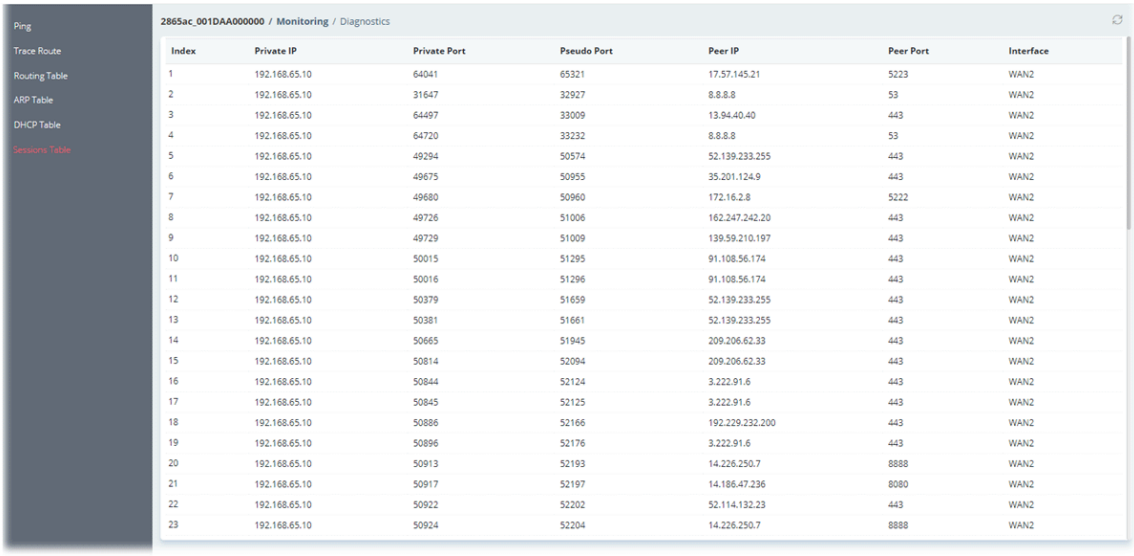



These parameters are explained as follows:

| Item | Description |
|---|---|
| **IPv4 Address Assignment Table** | Displays the IP assignment status including LAN number, IP address, mask address, start IP, end IP and DHCP server on/off. |
| **IPv6 Address Assignment Table** | Displays the IP assignment status including interface, IPv6 address, IAID, link-layer address, leased time and DUID. |

### 9.3.3.6 Sessions Table

This page displays the private IP, private port number, pseudo port number, the peer IP, the peer port, the connected interface of the remote client communicating with the selected CPE.

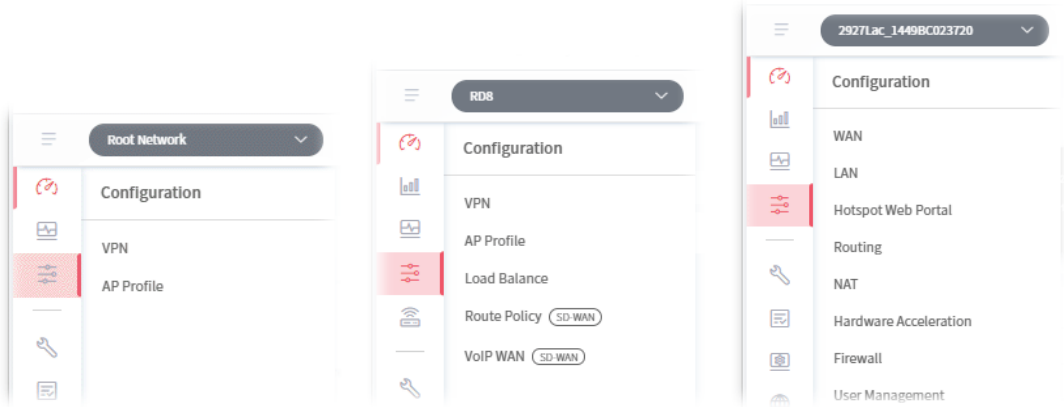



| Index | Private IP | Private Port | Pseudo Port | Peer IP | Peer Port | Interface |
|---|---|---|---|---|---|---|
| 1 | 192.168.65.10 | 64041 | 65321 | 17.57.145.21 | 5223 | WAN2 |
| 2 | 192.168.65.10 | 31647 | 32927 | 8.8.8.8 | 53 | WAN2 |
| 3 | 192.168.65.10 | 64497 | 33009 | 13.94.40.40 | 443 | WAN2 |
| 4 | 192.168.65.10 | 64720 | 33232 | 8.8.8.8 | 53 | WAN2 |
| 5 | 192.168.65.10 | 49294 | 50574 | 52.139.233.255 | 443 | WAN2 |
| 6 | 192.168.65.10 | 49675 | 50955 | 35.201.124.9 | 443 | WAN2 |
| 7 | 192.168.65.10 | 49680 | 50960 | 172.16.2.8 | 5222 | WAN2 |
| 8 | 192.168.65.10 | 49726 | 51006 | 162.247.242.20 | 443 | WAN2 |
| 9 | 192.168.65.10 | 49729 | 51009 | 139.59.210.197 | 443 | WAN2 |
| 10 | 192.168.65.10 | 50015 | 51295 | 91.108.56.174 | 443 | WAN2 |
| 11 | 192.168.65.10 | 50016 | 51296 | 91.108.56.174 | 443 | WAN2 |
| 12 | 192.168.65.10 | 50379 | 51659 | 52.139.233.255 | 443 | WAN2 |
| 13 | 192.168.65.10 | 50381 | 51661 | 52.139.233.255 | 443 | WAN2 |
| 14 | 192.168.65.10 | 50665 | 51945 | 209.206.62.33 | 443 | WAN2 |
| 15 | 192.168.65.10 | 50814 | 52094 | 209.206.62.33 | 443 | WAN2 |
| 16 | 192.168.65.10 | 50844 | 52124 | 3.222.91.6 | 443 | WAN2 |
| 17 | 192.168.65.10 | 50845 | 52125 | 3.222.91.6 | 443 | WAN2 |
| 18 | 192.168.65.10 | 50886 | 52166 | 192.229.232.200 | 443 | WAN2 |
| 19 | 192.168.65.10 | 50896 | 52176 | 3.222.91.6 | 443 | WAN2 |
| 20 | 192.168.65.10 | 50913 | 52193 | 14.226.250.7 | 8888 | WAN2 |
| 21 | 192.168.65.10 | 50917 | 52197 | 14.186.47.236 | 8080 | WAN2 |
| 22 | 192.168.65.10 | 50922 | 52202 | 52.114.132.23 | 443 | WAN2 |
| 23 | 192.168.65.10 | 50924 | 52204 | 14.226.250.7 | 8888 | WAN2 |

## 9.4 Configuration

> This section introduces the menu item used for the selected CPE (AP or router) briefly. For more detailed information on each menu item, refer to User's Guide of the selected CPE device.

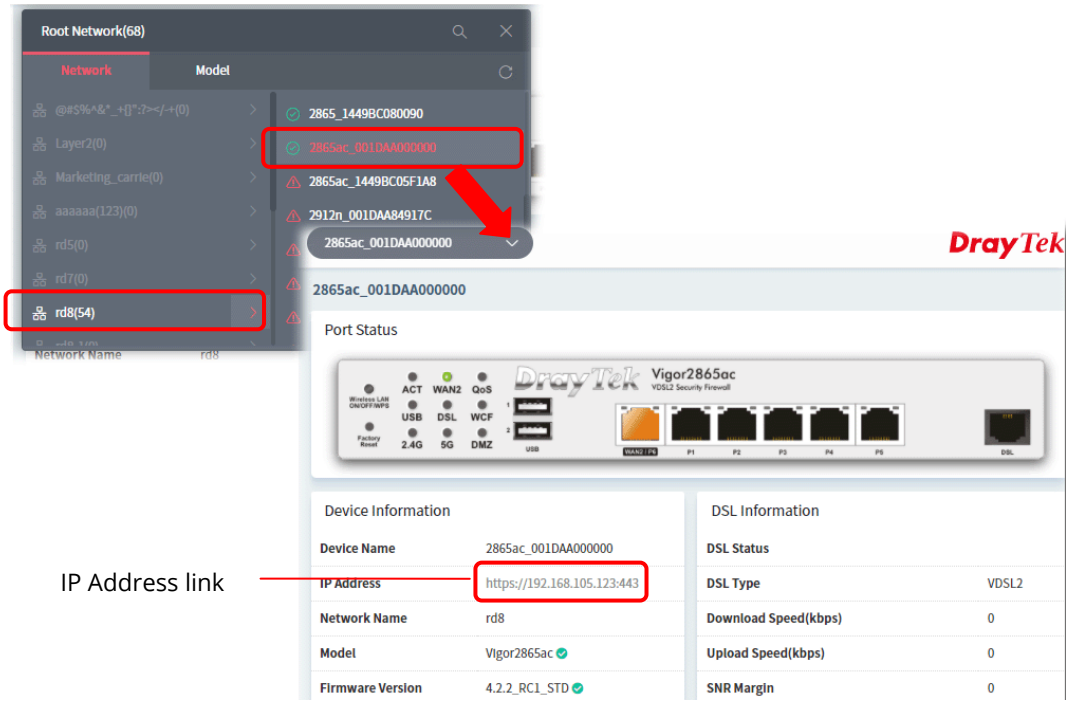
Available configuration settings will vary for root network, group network and specified CPE.



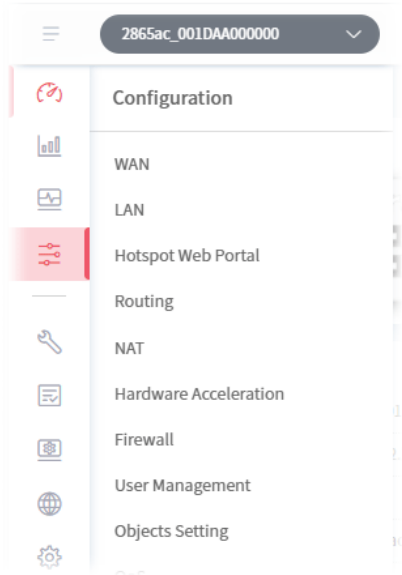

The menu items for a selected CPE device, generally, are the same as the settings on web user interface of the selected device (CPE, AP and etc.).

It is not necessary for the administrator to access into the web user interface of the selected CPE to make setting changes. If required, the administrator can modify the settings for the selected device through the options displayed under Configuration. The modifications will be applied to the selected device immediately.

How to select a CPE? On the left-top side of the home page of VigorACS 3, click the Network tab and find out the CPE you want. Then, click the CPE. A dashboard of the selected CPE will be shown on the screen.




The menu items for Configuration will vary based on the selected CPE (AP / router). Here, we take Vigor2865ac as an example.

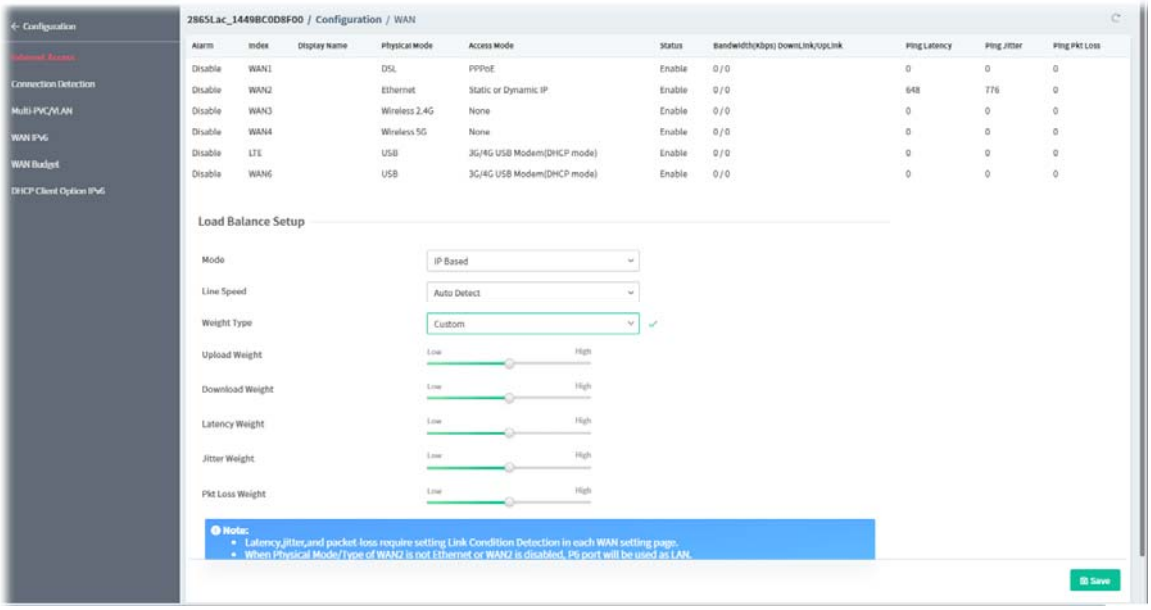



If the administrator wants to access into the web user interface of the selected CPE, click the IP address link of the selected CPE on the CPE dashboard.

### 9.4.1 WAN

WAN settings relate to access Internet for CPEs.

#### 9.4.1.1 Internet Access

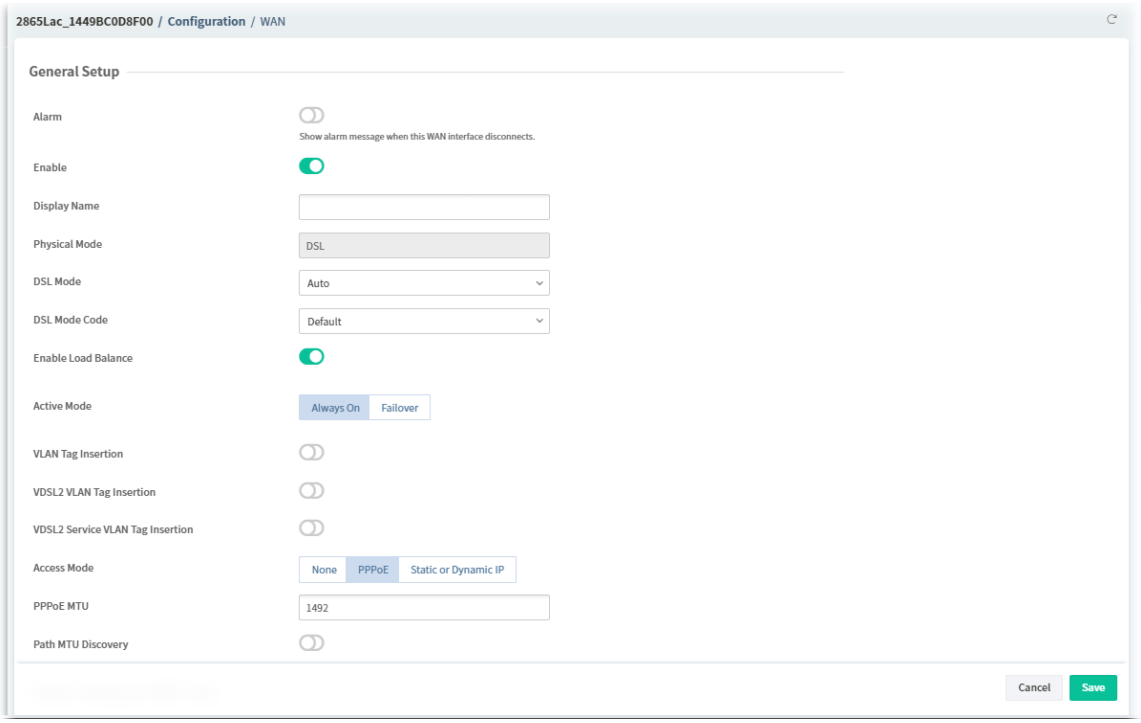



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Table** | **Alarm** - Display if the alarm function is enabled or disabled.<br>**Index** - Displays the index number of the WAN interface.<br>**Display Name** - Displays the description for the WAN interface.<br>**Physical Mode** - Display the physical mode (e.g., Wireless 2.4G / Wireless 5G) of the interface.<br>**Access Mode** - Displays the access mode for the WAN interface.<br>**Status** - Displays if the WAN interface is enabled or disabled.<br>**Bandwidth(Kbps)DownLink/UpLink** - Displays the downlink / uplink bandwidth ratio.<br>**Ping Latency / Ping Jitter / Ping Pkt Loss** - Displays the latency / jitter / packet loss value. |
| **Load Balance Setup** | **Mode** - The default is IP Based. Choose Session Based to get better transmission speed.<br>**Line Speed** - Choose **Auto Weight** to let the router reach the best load balance. According to Line Speed to let the router reach the best load balance based on line speed.<br>**Weight Type** - Choose **Bandwidth-Based / Quality-Based / Reliability-Based** as the weight type. Or choose **Custom** to define **Upload Weight, Download Weight, Latency Weight, Jitter Weight, Pkt Loss Weight** respectively.<br>● **Upload / Download Weight**- The higher the weight is, the WAN interface with higher bandwidth will get higher usage.<br>● **Latency Weight** - It defines the time taken by Vigor router when sending the packets to the IP set in Link Condition Detection. The higher the weight is, the WAN interface with lower latency will get |

| | |
|---|---|
| | higher usage.<br>● **Jitter Weight** - It defines the change rate of latency. For stable session, small jitter value will be better. The higher the weight is, the WAN interface with lower jitter will get higher usage.<br>● **Pkt Loss Weight** - It defines the proportion that packets will be discarded before arriving at the IP set in Link Condition Detection. The higher the weight is, the WAN interface with lower packet loss will get higher usage. |
| **Save** | Save the current settings. |

To modify the general setup settings for each WAN, move the mouse cursor on the WAN# under Index and Click to open the following page.




These parameters are explained as follows:

| Item | Description |
|---|---|
| | **General Setup** |
| **Alarm** | Click to show/hide an alarm message. |
| **Enable** | Click to enable/disable settings of the WAN interface. |
| **Display Name** | Enter the description for the interface. |
| **Physical Mode** | Display the physical mode (e.g., DSL) of the interface. |
| **DSL Mode** | Specify the physical mode (Auto, VDSL or ADSL) for the router manually. |
| **DSL Modem Code** | Choose the correct DSL modem code for ensuring the network connection.<br>If you have no idea about the selection, simply choose **Default** or contact the dealer for assistance. |
| **Enable Load Balance** | Click to enable **auto** load balance function for this WAN interface. |
| **Active Mode** | **Always On** - Make the WAN connection being activated always.<br>**Failover** - Make the WAN connection as a backup connection. |
| **Failover** | It is available when Failover is selected as Active Mode. |

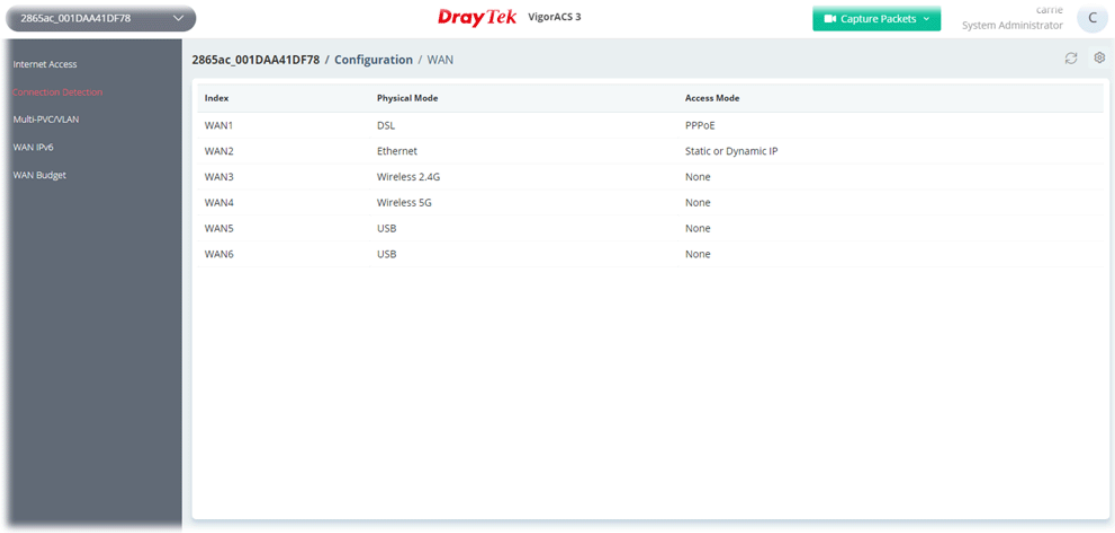
| | |
|---|---|
| | **Backup WAN** - When the active WAN failed, such WAN will be activated as the main network connection.<br>**Active When** - It is available when Failover is selected as Active Mode.<br>● **Any** - The backup WAN will be activated when any master WAN interface disconnects.<br>● **All** - The backup WAN will be activated only when all master WAN interfaces disconnect.<br>**Backup Type** - Choose **Fails to connect** or **Meet Any/all of the following condition**. When Meet Any/all of the following condition is selected:<br>● **Meet of the following conditions** - If the packet meets any one of the conditions, the failover WAN will be enabled; if the packet meets All of the conditions, the failover WAN will be enabled.<br>● **Upload traffic / Download traffic** - Set the values for upload and download respectively.<br>● **Latency** - After selecting Check Latency, enter a value as a threshold.<br>● **Jitter** - After selecting Check Jitter, enter a value as a threshold.<br>● **Packet loss** After selecting Check Packet loss, enter a value as a threshold.<br>When the data traffic of active WAN reaches the traffic threshold (specified here), the failover WAN will be enabled automatically to share the overloaded data traffic. |
| **VLAN Tag Insertion / VDSL2 VLAN Tag Insertion / VDSL2 Service VLAN Tag Insertion** | Click to enable the function of VLAN with tag. |
| **Access Mode** | Set the access mode for this WAN.<br>**None** - No mode used.<br>**PPPoE** - Click to select PPPoE as the accessing protocol of the Internet.<br>● **PPPoE MTU** - Set a number as the Max Transmit Unit for packet.<br>**Static or Dynamic IP** - Click to select a static IP or use dynamic IP as the accessing protocol of the Internet.<br>● **Static IP MTU** - Set a number as the Max Transmit Unit for packet. |
| **Path MTU Discovery** | Click to enable the path MTU discovery function for this WAN interface.<br>● **Path MTU to** – Select Host / IP, for an IPv4 address or Host / IPv6, for an IPv6 address, and then enter the IP address in the textbox.<br>● **MTU size start from** – Determine the starting point value of the packet.<br>● **MTU reduce size by** – Number of octets by which to decrease the 1500-byte MTU. Start with a 0 value for the reduce size and click the Detect button. If the message Fail is returned, increase the MTU reduce size and try again. Repeat until you see the message Success, indicating that the optimal MTU size has been reached. |
| | **Modem Settings (for ADSL only)** |
| **Multi-PVC channel** | The selections displayed here are determined by the setting page of **Multi-PVC/VLAN**. **Select M-PVCs Channel** means no selection will be chosen. |
| **VPI/VCI** | Enter the value provided by ISP. |
| **Encapsulating Type** | Choose the type provided by ISP. |

| | |
|---|---|
| **Protocol** | Choose the one (PPPoE or PPPoA) provided by ISP. |
| **Modulation Type** | Default setting is Multimode.<br>Choose the one that fits the requirement of your router. |
| | **PPPoE (available when PPPoE is selected as the Protocol** |
| **For Wired LAN /**<br>**For Wireless LAN** | **For Wired LAN** – If you check this box, PCs on the same network can use another set of PPPoE session (different with the Host PC) to access into Internet.<br>**For Wireless LAN** – It is available for *n* model. If you check this box, PCs on the same wireless network can use another set of PPPoE session (different with the Host PC) to access into Internet. |
| **PPP Service Name / PPP User Name / PPP Password** | Enter the service name, username and password provided by ISP. |
| **Schedule Setup(1-15)** | Enter four sets of time schedule for your request. |
| **PPP Authentication** | Select **PAP only** or **PAP or CHAP** for PPP. |
| **Fixed IP Enable** | Click **Yes** to enable the fixed IP setting.<br>Or, click **No** to disable the fixed IP setting. |
| **Fixed IP Address** | Enter a fixed IP address in the box. |
| | **Static or Dynamic IP (available when Static or Dynamic IP is selected as the Connection Mode)** |
| **Connection Type** | **DHCP - Click to** obtain the IP address automatically.<br>● **Router Name -** Enter the router name provided by ISP.<br>● **Domain Name -** Enter the domain name that you have assigned.<br>● **DHCP Client Identifier -** Click to enable and specify username and password as the DHCP client identifier for some ISP.<br>**Static -** Click to specify some data.<br>● **IP Address -** Enter the private IP address.<br>● **Subnet Mask -** Enter the subnet mask.<br>● **Gateway IP Address** – Enter gateway IP address. |
| **Primary DNS Server /**<br>**Secondary DNS Server** | Enter the primary IP address for the router. If necessary, Enter secondary IP address for necessity in the future. |
| **Enable RIP** | Click to enable the RIP function. |
| **Enable Bridge Mode** | **Enable -** Click to make the router work as a bridge modem. Yet, the incoming packets with VLAN tags will be discarded.<br>● **Enable Firewall -** If enabled, all of the filter rules defined and enabled in Firewall menu will be activated. |
| **Enable Full Bridge Mode** | **Click to make** the router work as a bridge modem which is able to forward incoming packets with VLAN tags. |
| **Bridge Subnet** | Make a bridge between the selected LAN subnet and such WAN interface. |
| | **WAN IP Alias (Multi-NAT)** |
| **Index** | Display the index number of the WAN IP alias. |
| **Enable** | Click to enable the selected WAN IP alias. |
| **Aux. WAN IP** | Display the IP address of the WAN IP alias. |

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

### 9.4.1.2 Connection Detection

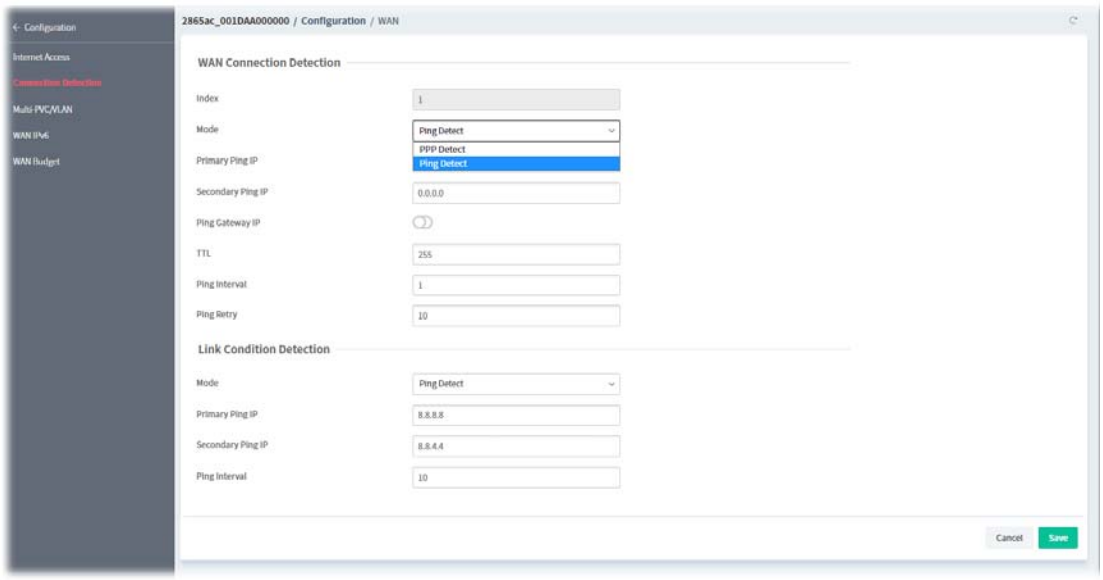
This page displays physical mode and access mode for each WAN interface.




These parameters are explained as follows:

| Item | Description |
|---|---|
| **Index** | Displays the index number of the WAN interface. |
| **Physical Mode** | Displays the physical connection for WAN interfaces according to the real network connection. |
| **Access Mode** | Displays the accessing mode of the Internet. |

To modify the setting, move the mouse cursor to any entry and click to open the setting page.

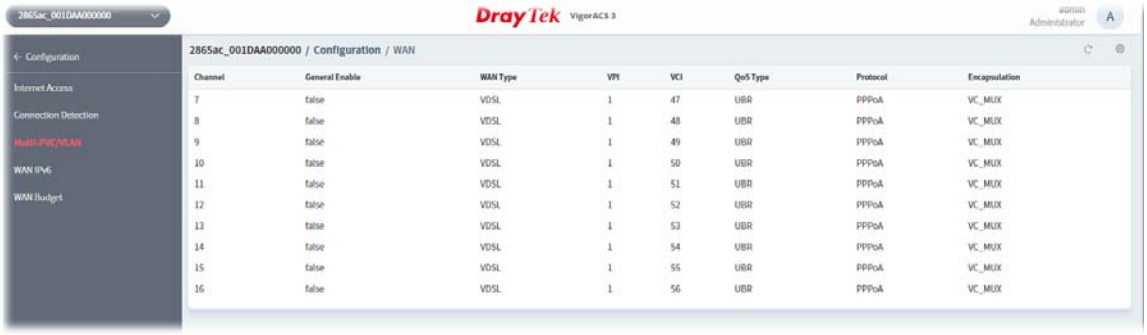



| Item | Description |
|---|---|
| | **WAN Connection Detection** |
| **Index** | Displays the index number of the WAN interface. |
| **Mode** | Choose **PPP Detect** or **Ping Detect** for the system to execute for WAN detection. If you choose **Ping Detect** as the detection mode, you have to enter required settings for the following items. |

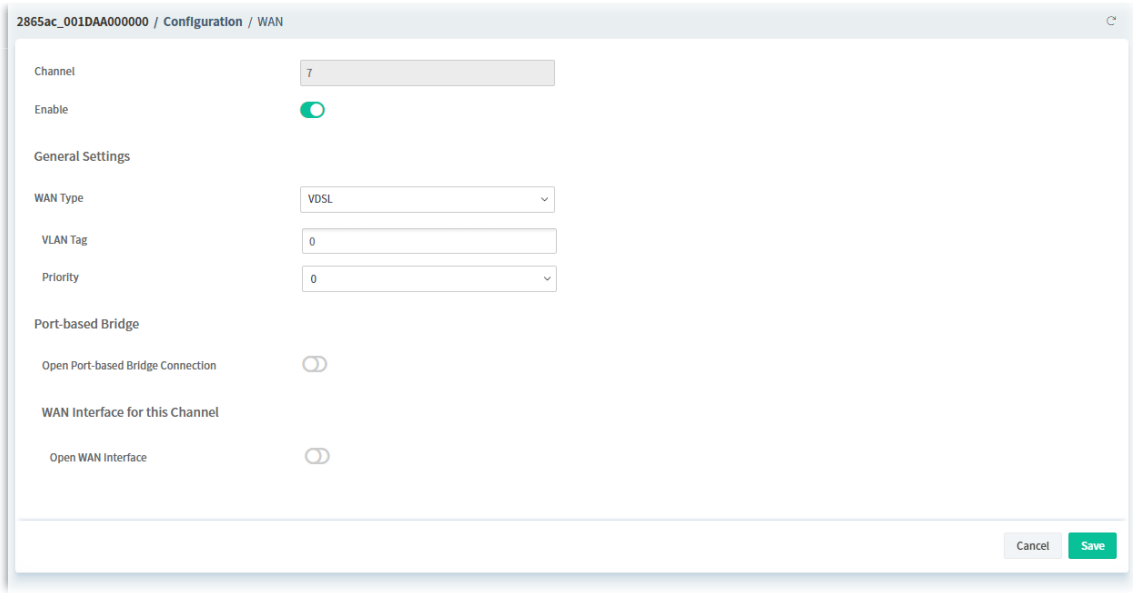
| | |
|---|---|
| | • **Primary / Secondary Ping IP** - Enter the Primary or Secondary IP address in this field for pinging.<br>• **Ping Gateway IP** - Use the WAN gateway IP address for pinging. Vigor router can check if the WAN connection is on or off.<br>• **TTL** - Set TTL value of PING operation.<br>• **Ping Interval** - 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. |
| | **Link Condition Detection** |
| **Mode** | In order for the system to detect the latency, jitter, and packet-loss status for each WAN interface, you have to specify the IP transmitting data through the interface.<br>Choose Ping Detect, Http Detect, or Disable as detection mode. If Ping Detect or Http Detect is selected, you have to configure the following option. |
| **Primary Ping IP** | Enter an IP address. |
| **Secondary Ping IP** | Enter an IP address. |
| **Ping Interval** | Set a time interval (unit: second) for the system to ping the IP address specified above. |
| **Cancel** | Discard current modification. |
| **Save** | Save the current settings. |

### 9.4.1.3 Multi-PVC/VLAN

This page allows you to configure multiple permanent virtual circuits (PVCs) and ATM QoS for channels using ADSL.




To modify the setting, move the mouse cursor to any entry and click to open the setting page.



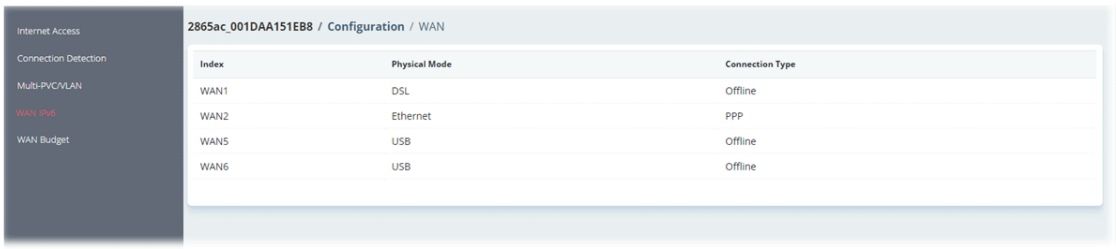

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Channel** | Display the number of the channel. |
| **Enable** | Click to enable or disable the channel. |
| | **General Settings** |
| **WAN Type** | Specify a WAN type of the PVC Channel/VLAN. |
| **VLAN Tag** | Enter the value as the VLAN ID number. |
| **Priority** | Choose the number to determine the packet priority for this VLAN. The range is from 0 to 7. |
| | **Port-based Bridge** |
| **Open Port-based Bridge Connection** | Click to enable or disable the function.<br>If enabled, you have to enter required settings for the following items.<br>**Physical Members** - Group the physical ports by checking the corresponding check box(es) for applying the port-based bridge connection. |
| | **WAN Interface for this Channel** |
| **Open WAN Interface** | Click to enable or disable the function.<br>If enabled, you have to enter required settings for the following items.<br>**WAN Application** -<br>● **Management** - The configuration for this VLAN will be effective for Web configuration/telnet/TR069.<br>● **IPTV** - The IPTV configuration will allow the WAN interface to send IGMP packets to IPTV servers.<br>**Mode** - Select **ARP Detect** or **Ping Detect**. If **Ping Detect** is selected, you have to set the following options.<br>● **Primary Ping IP / Secondary Ping IP** - Enter Primary or Secondary IP address in this field for pinging.<br>● **Ping Gateway IP** - Enable this setting to use 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** - Set a time interval (unit: second) for the system to ping the IP address specified above.<br>• **Ping Retry** - Enter the number of times that the system is allowed to execute the PING operation before WAN disconnection is judged.<br>**WAN Setup** - Choose Static_or_Dynamic_IP or PPPoE/PPPoA. |
| **WAN IP Network Settings** | It is available when **Static_or_Dynamic_IP** is selected as WAN Setup.<br>**Auto IP** - Click to enable / disable the settings.<br>If Auto IP is enabled, you have to enter required settings for the following items.<br>• **Router Name** - Enter the router name provided by ISP.<br>• **Domain Name** - Enter the domain name provided by ISP.<br>If Auto IP is disabled, you have to enter required settings for the following items.<br>• **IP Address** - Enter the IP address.<br>• **Subnet Mask** - Enter the subnet mask.<br>• **Gateway** - Enter gateway IP address.<br>**Primary DNS IP** - Enter the primary IP address for the router if you want to use **Static IP** mode.<br>**Secondary DNS IP** - If necessary, Enter secondary IP address for necessity in the future. |
| **ISP Access Setup** | It is available when **PPPoE/PPPoA** is selected as WAN Setup.<br>**ISP Name** - PPP Service Name. Enter if your ISP requires this setting; otherwise leave blank.<br>**Username** - Name provided by the ISP for PPPoE/PPPoA authentication.<br>**Password** - Password provided by the ISP for PPPoE/PPPoA authentication.<br>**Authentication** - Choose the protocol used for PPP authentication.<br>**Always On** - The router will maintain the PPPoE/PPPoA connection.<br>**Fixed IP** - If enabled, the IP address entered in the Fixed IP Address field will be used as the IP address of the virtual WAN.<br>**Fixed IP Address** - Enter an IP address. |
| **Cancel** | Discard current modification. |
| **Save** | Save the current settings. |

### 9.4.1.4 WAN IPv6

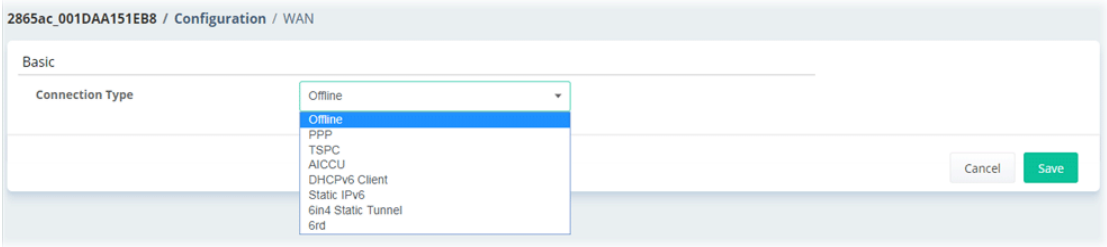
This page allows to configure IPv6 settings for each WAN interface.




These parameters are explained as follows:

| Item | Description |
|---|---|
| **Index** | Displays the index number of the WAN interface. |
| **Physical Mode** | Displays the physical connection for WAN interfaces according to the real network connection. |
| **Access Mode** | Displays the accessing mode of the Internet. |

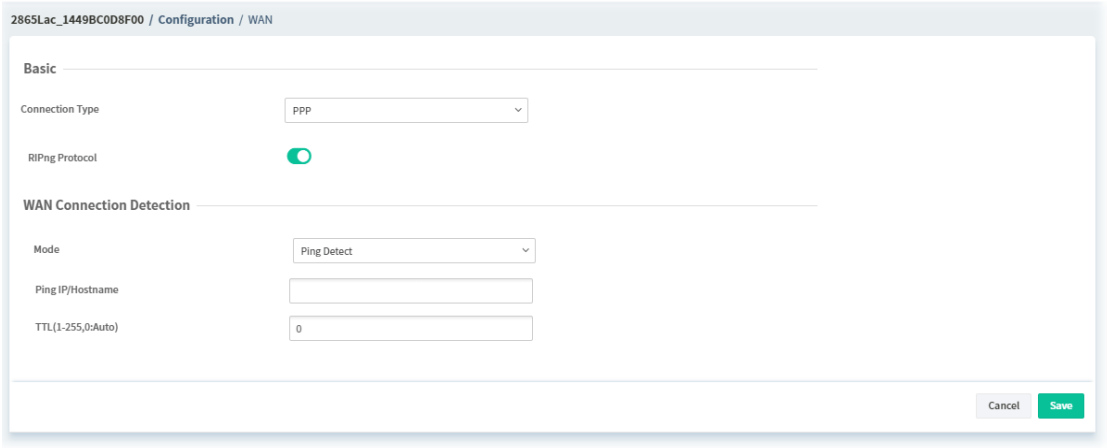
To modify the IPv6 setting, move the mouse cursor to any entry (WAN1/WAN2/WAN5/WAN6) and click to open the setting page.



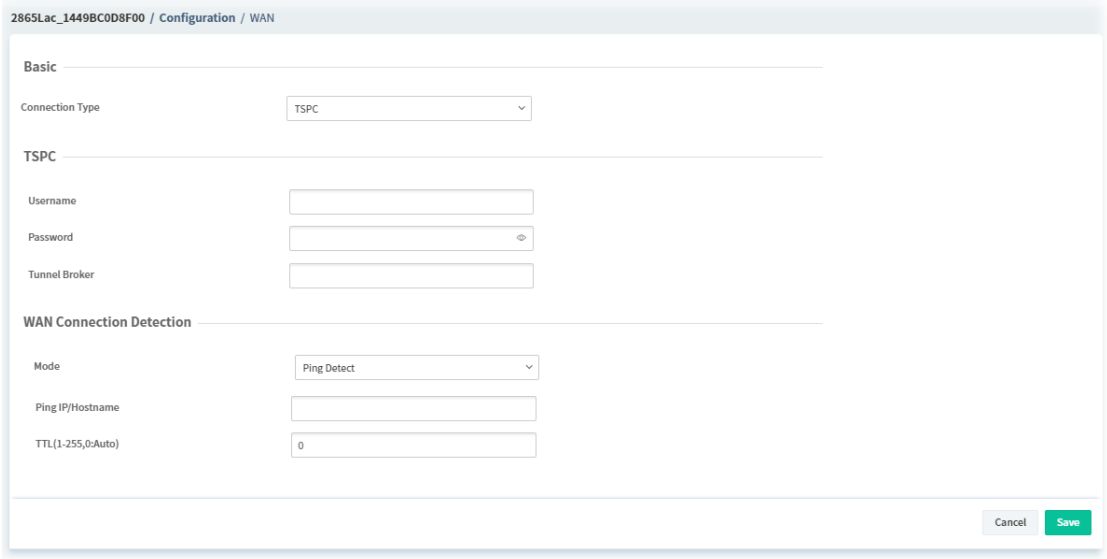

### Offline

When Offline is selected, the IPv6 connection will be disabled.

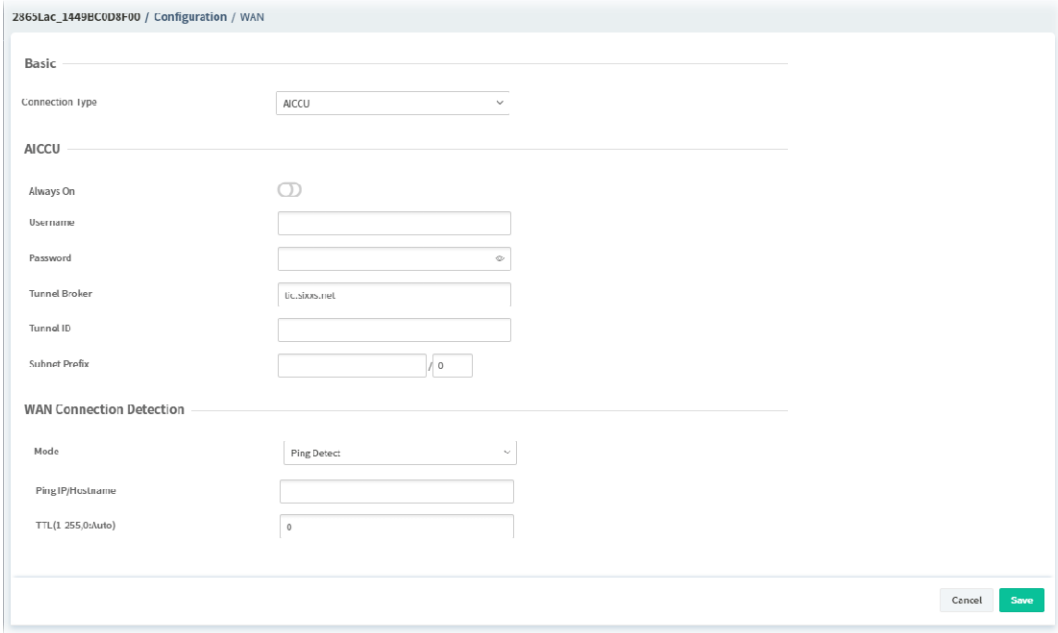
### PPP



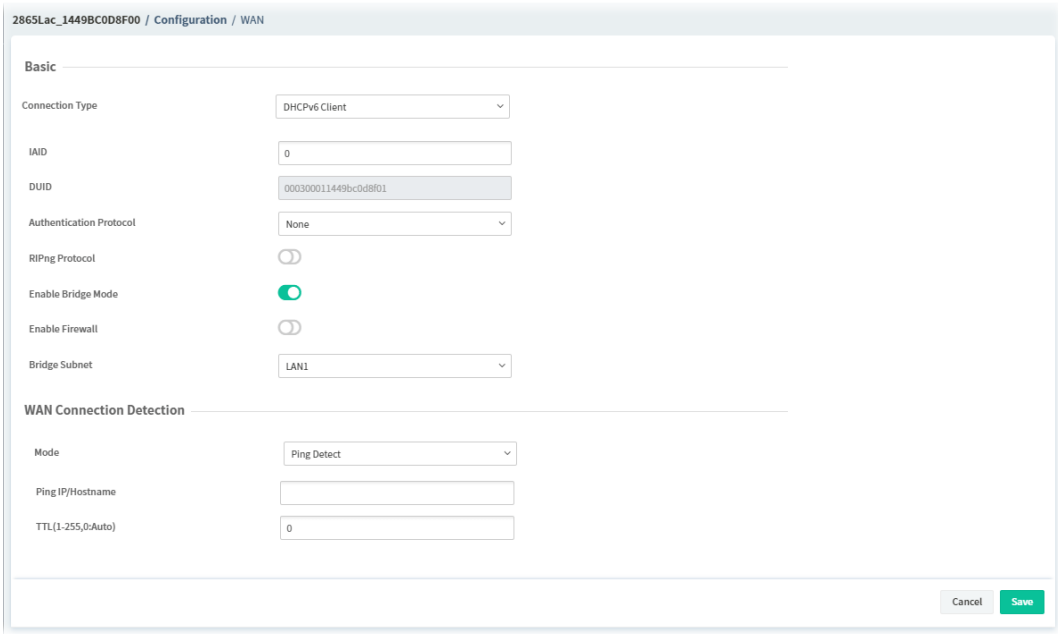

### TSPC



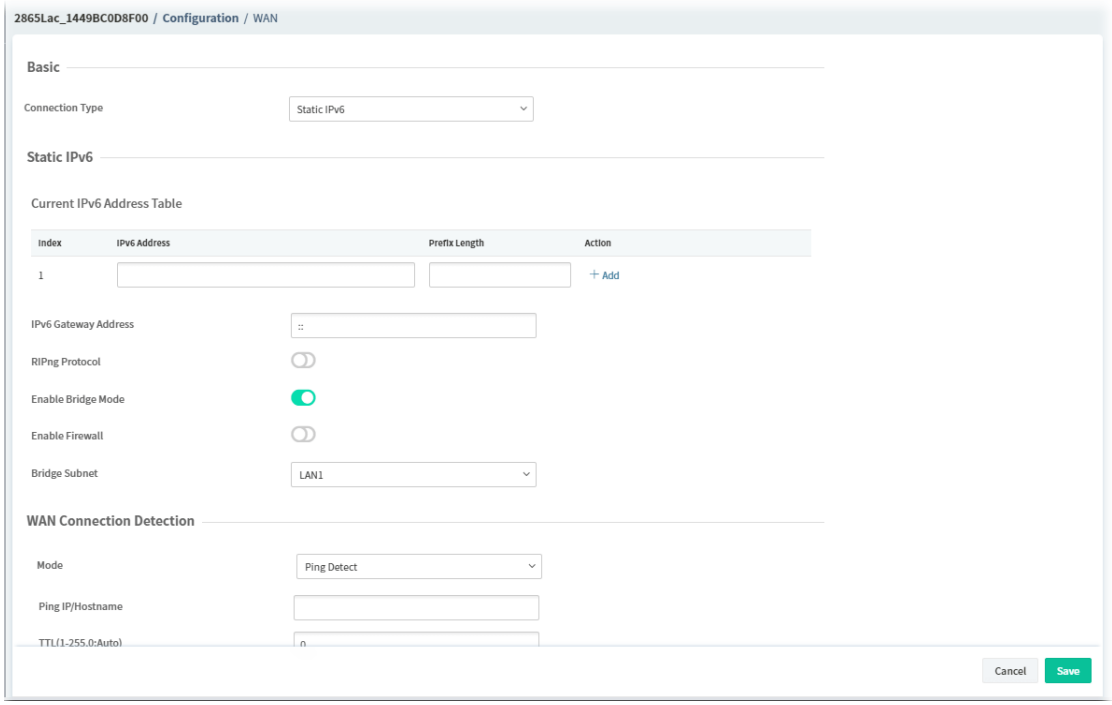
## AICCU



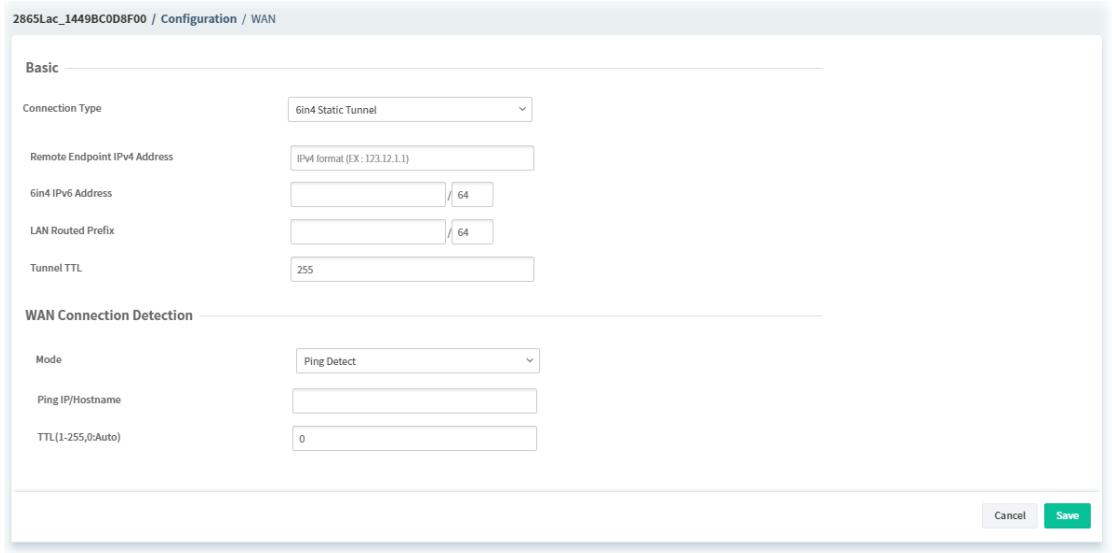

## DHCPv6 Client



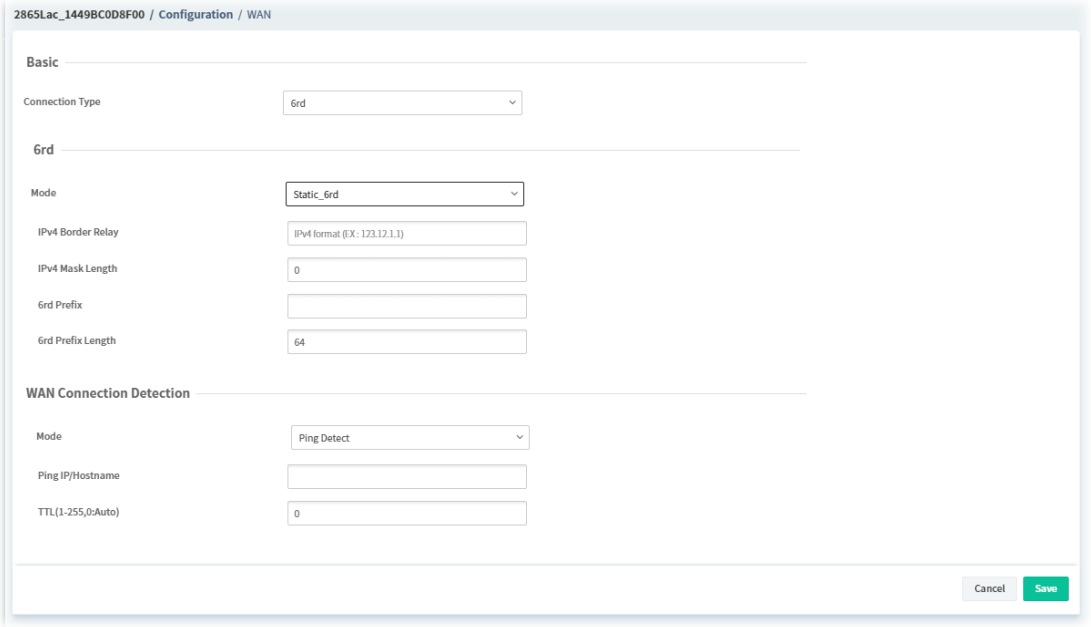
### Static IPv6




### 6in4 Static Tunnel



**6rd**




The parameters for connection type (PPP to 6rd) are explained as follows:

| Item | Description |
|---|---|
| | **PPP** |
| **RIPng Protocol** | RIPng (RIP next generation) offers the same functions and benefits as IPv4 RIP v2. |
| **WAN Connection Detection** | Such function allows you to verify whether network connection is alive or not through Ping Detect.<br>**Mode** – Choose **Always On** or **Ping Detect** for the system to execute for WAN detection. **Always On** means no detection will be executed. The network connection will be on always.<br>● **Ping IP/Hostname** – If you choose **Ping Detect** as detection mode, you have to type IP address in this field for pinging.<br>● **TTL (Time to Live)** –If you choose **Ping Detect** as detection mode, you have to type TTL value. |
| | **TSPC** |
| **TSPC** | **Username -** Enter the name obtained from the broker.<br>**Password -** Enter the password assigned with the user name.<br>**Tunnel Broker -** Enter the address for the tunnel broker IP, FQDN or an optional port number. |
| **WAN Connection Detection** | Such function allows you to verify whether network connection is alive or not through Ping Detect.<br>**Mode** – Choose **Always On** or **Ping Detect** for the system to execute for WAN detection. **Always On** means no detection will be executed. The network connection will be on always.<br>● **Ping IP/Hostname** – If you choose **Ping Detect** as detection mode, you have to type IP address in this field for pinging.<br>● **TTL (Time to Live)** –If you choose **Ping Detect** as detection mode, you have to type TTL value. |
| | **AICCU** |

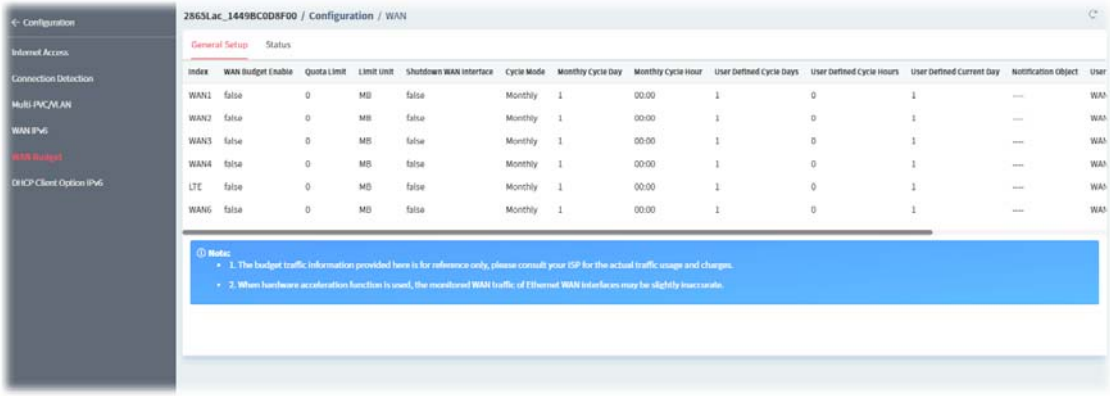
| | |
|---|---|
| **AICCU** | **Always On -** Check this box to keep the network connection always.<br>**Username -** Enter the name obtained from the broker. Please apply new account at http://www.sixxs.net/. It is suggested for you to apply another username and password.<br>**Password -** Enter the password assigned with the user name.<br>**Tunnel Broker -** It means a server of AICCU. The server can provide IPv6 tunnels to sites or end users over IPv4.<br>**Tunnel ID -** One user account may have several tunnels. And, each tunnel shall have one specified tunnel ID (e.g., T115394). Enter the ID offered by Tunnel Broker.<br>**Subnet Prefix -** Enter the subnet prefix address obtained from service provider. |
| **WAN Connection Detection** | Such function allows you to verify whether network connection is alive or not through Ping Detect.<br>**Mode** – Choose **Always On** or **Ping Detect** for the system to execute for WAN detection. **Always On** means no detection will be executed. The network connection will be on always.<br>● **Ping IP/Hostname** – If you choose **Ping Detect** as detection mode, you have to type IP address in this field for pinging.<br>● **TTL (Time to Live)** –If you choose **Ping Detect** as detection mode, you have to type TTL value. |
| | **DHCPv6 Client** |
| **DHCPv6 Client** | **IAID** - Enter a number as IAID.<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>● **Key ID** – Enter 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** –Enter a text (1 to 31 characters) as s a unique identifier for each client on each DHCP server.<br>**RIPng Protocol** - RIPng (RIP next generation) offers the same functions and benefits as IPv4 RIP v2.<br>**Enable Bridge Mode** - If the function is enabled, the router will work as a bridge modem.<br>● **Enable Firewall** - It is available when Bridge Mode is enabled. When both Bridge Mode and Firewall check boxes are enabled, the settings configured (user profiles) under User Management will be ignored. And all of the filter rules defined and enabled in Firewall menu will be activated.<br>**Bridge Subnet** - Make a bridge between the selected LAN subnet and such WAN interface. |
| **WAN Connection Detection** | Such function allows you to verify whether network connection is alive or not through Ping Detect.<br>**Mode** – Choose **Always On** or **Ping Detect** for the system to execute for WAN detection. **Always On** means no detection will be executed. The network connection will be on always.<br>● **Ping IP/Hostname** – If you choose **Ping Detect** as detection mode, you have to type IP address in this field for pinging. |

| | |
|---|---|
| | ● **TTL (Time to Live)** –If you choose **Ping Detect** as detection mode, you have to type TTL value. |
| **Cancel** | Discard current modification. |
| **Save** | Save the current settings. |

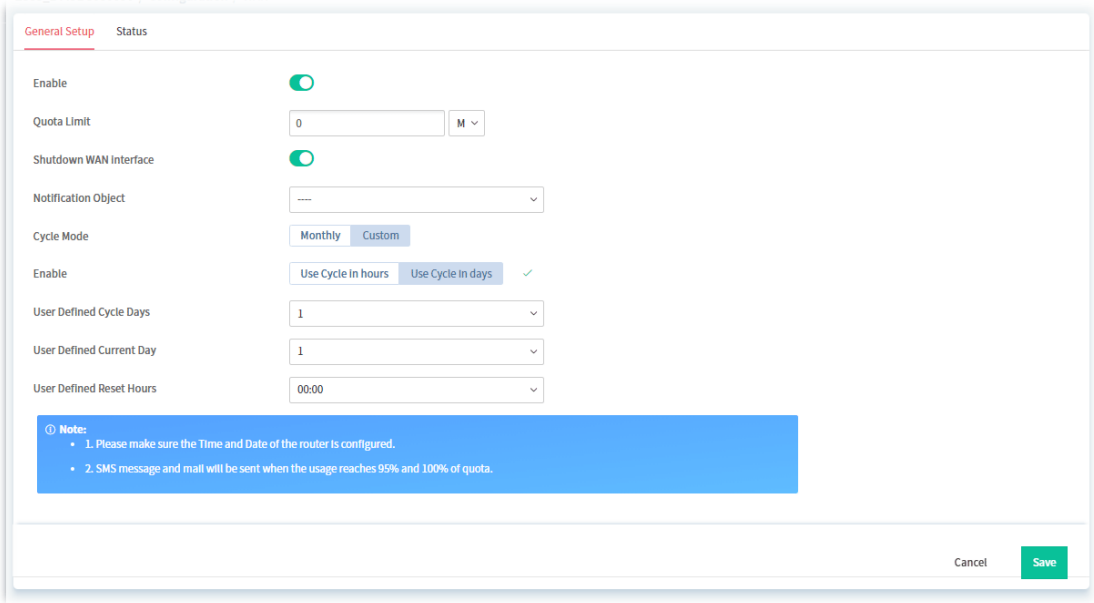
After finished the above settings, click **Save** to save the settings.

### 9.4.1.5 WAN Budget

WAN Budget determines the data *traffic volume* for each WAN interface respectively to prevent overcharges for data transmission by the ISP.




To modify the budget profile setting, move the mouse cursor to any entry (index 1 to index 6) and click to open the setting page.



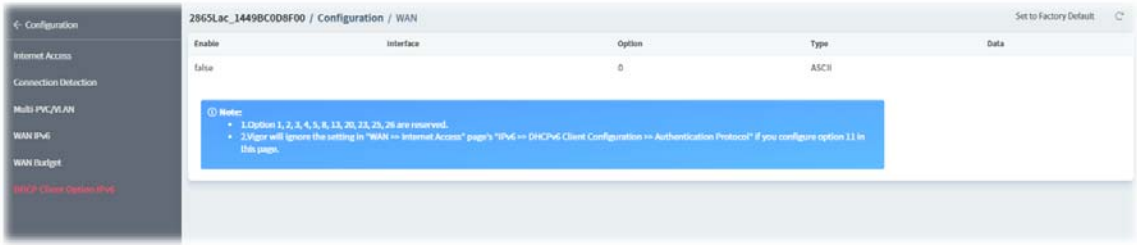

The parameters are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Click to enable the budget function. |
| **Quota Limit** | Enter the data traffic quota allowed for such WAN interface. There are two unit (MB and GB) offered for you to specify. |
| **Shutdown WAN Interface** | Click to let all the outgoing traffic through such WAN interface be terminated. |
| **Notification Object** | The system will send out a notification based on the content of the |

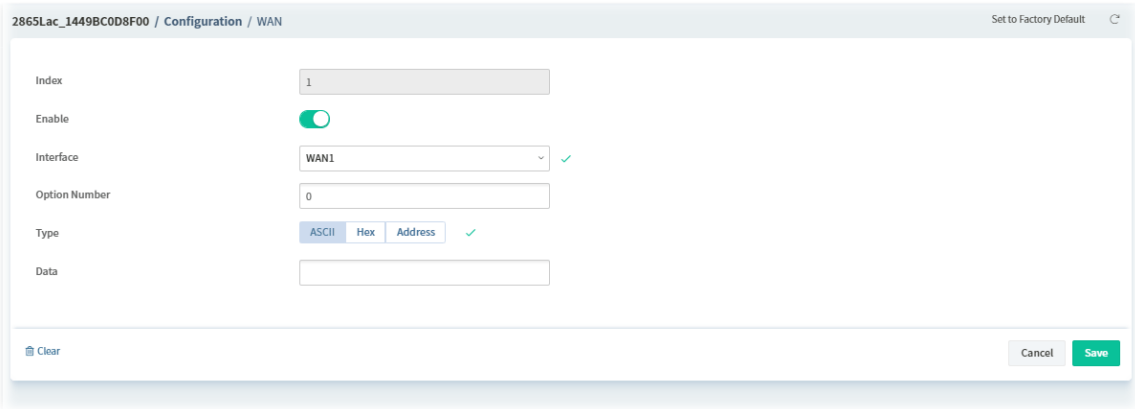
| | |
|---|---|
| | notification object. |
| **Cycle Mode** | Choose **Monthly** or **Custom** to define the billing cycle according to request.<br>Monthly is default setting. If long period or a short period is required, use **Custom**. The period of cycle duration is between 1 day and 60 days. You 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. |
| **Monthly Cycle Day / Monthly Cycle Hour** | It is available when **Monthly** is selected as **Cycle Mode.**<br>Set the day and time in a month. |
| **Enable** | It is available when **Custom** is selected as **Cycle Mode.**<br>**Use Cycle in hours** - Set a time cycle (including days and hours) for Vigor CPE to reset the data record automatically.<br>● **User Defined Cycle Days** - Select a number (1~60) of the days for a cycle. For example, 7 means 7 days.<br>● **User Defined Cycle Hours** - Select a number (0~23) of the hours for a cycle. For example, 12 means 12 hours. Based on the cycle days and cycle hours settings, Vigor CPE will reset the data record once reaching 7 days and 12 hours.<br>● **User Defined Current Day** - Select the day in the cycle as the starting point in which the Vigor router will reset the traffic record. For example, "3" means current day is the third day, within a cycle.<br>**Use Cycle in days** - Set a cycle (with days) for Vigor CPE to reset the data record on a particular hour automatically.<br>● **User Defined Cycle Days** - Select a number (1~60) of the days for a cycle. For example, 7 means 7 days.<br>● **User Defined Current Day** - Select the day in the cycle as the starting point in which the Vigor router will reset the traffic record. For example, "3" means current day is the third day, within a cycle.<br>● **User Defined Reset Hours** - Select a particular time (00:00~23:00). For example, choose 15:00. Later, the CPE will reset the data record at 15:00 for every cycle. |
| **Cancel** | Discard current modification. |
| **Save** | Save the current settings. |

### 9.4.1.6 DHCP Client Option IPv6

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




To modify the setting, move the mouse cursor to the entry and click to open the setting page.



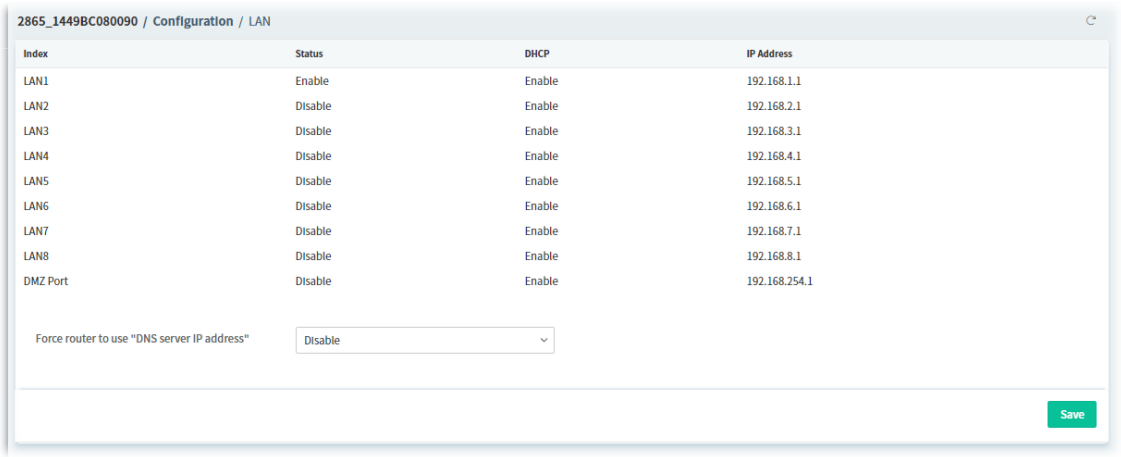

The parameters are explained as follows:

| Item | Description |
|---|---|
| **Index** | Displays the index number for the DHCP option. |
| **Enable** | If selected, DHCP option entry is enabled.<br>If unselected, DHCP option entry is disabled. |
| **Interface** | The interface(s) to which this entry is applicable. |
| **Option Number** | DHCP option number (e.g., 100). |
| **Type** | 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** | Data of this DHCP option. |
| **Cancel** | Discard current modification. |
| **Save** | Save the current settings. |

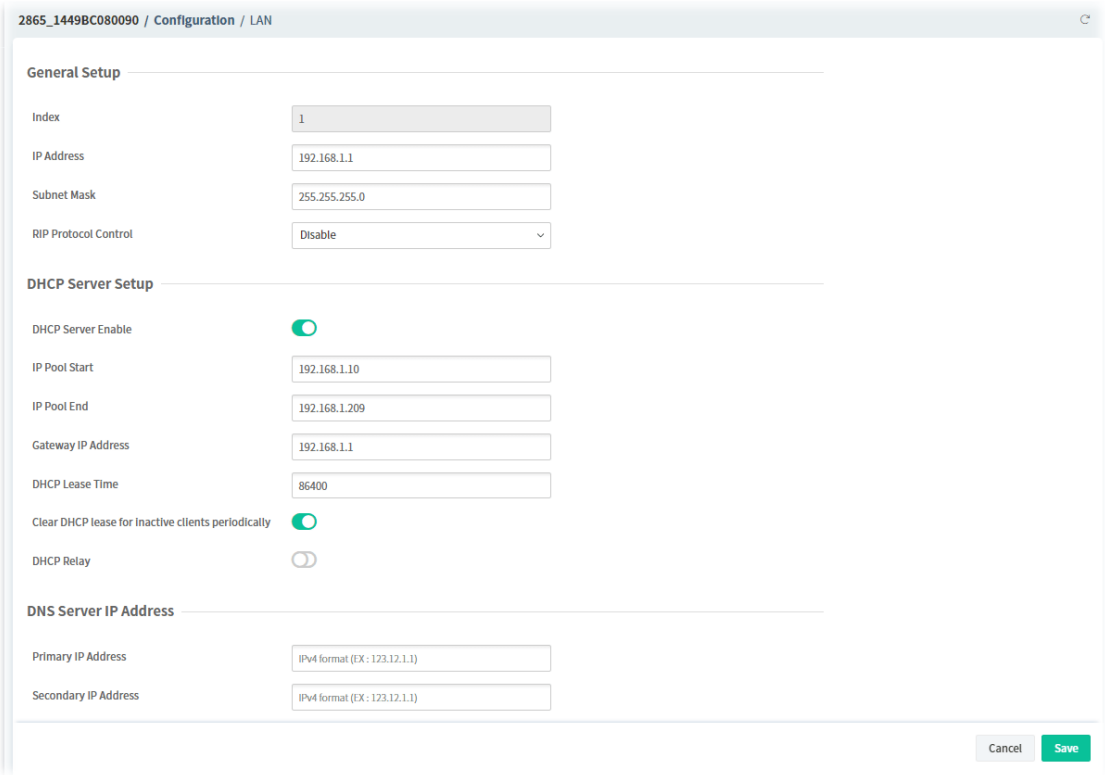
## 9.4.2 LAN

### 6.3.2.1 General Setup

This page provides you the general settings for LAN.




To modify the LAN or DMZ Port setting, move the mouse cursor to any entry and click to open the setting page.

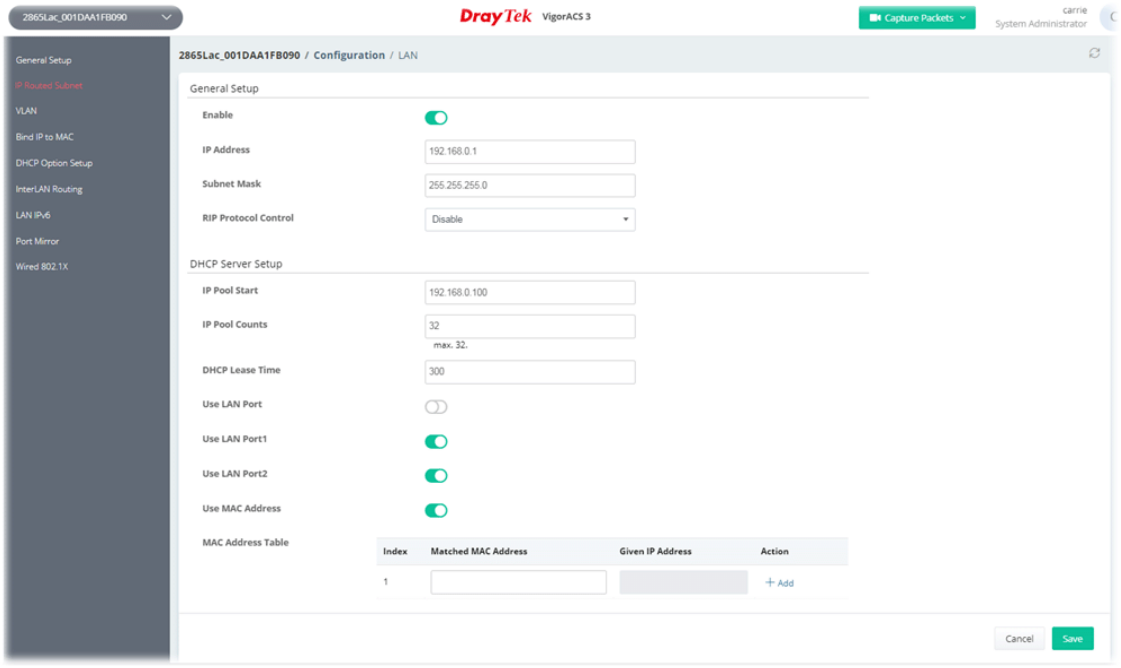



The parameters are explained as follows:

| Item | Description |
|---|---|
| | **General Setup** |
| **Index** | Display the index number of LAN item. |
| **IP Address** | Display the IP address of the router. |
| **Subnet Mask** | The subnet mask, together with the IP Address field, indicates the maximum number of clients allowed on the subnet. |

| | |
|---|---|
| **RIP Protocol Control** | It is available for LAN Port only.<br>Click to enable / disable the function. If enabled, the router will attempt to exchange routing information with neighbouring routers using the Routing Information Protocol. |
| **Usage** | It is available for DMZ Port only.<br>**NAT** - Click to invoke NAT function.<br>**Routing** - Click to invoke routing function. |
| | **DHCP Server Setup** |
| **DHCP Server Enable** | Click to enable / disable the DHCP server settings. If enabled:<br>**IP Pool Start -** Enter an IP address. The beginning LAN IP address that is given out to LAN DHCP clients.<br>**IP Pool End -** Enter an IP address. The ending LAN IP address that is given out to LAN DHCP clients.<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.<br>**DHCP Lease Time -** The maximum duration DHCP-issued IP addresses can be used before they have to be renewed.<br>**Clear DHCP lease for inactive clients periodically -** If enabled, the router sends ARP requests recycles IP addresses previously assigned to inactive DHCP clients to prevent exhaustion of the IP address pool. |
| **DHCP Relay** | Click to enable / disable the DHCP Relay settings. If enabled:<br>**DHCP Relay IP Address -** Set the IP address of the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server.<br>**DHCP 2nd Relay IP Address -** Set the second IP address for the DHCP server. |
| | **DNS Server IP Address** |
| **Primary IP Address** | Specify a DNS server IP address. |
| **Secondary IP Address** | Specify secondary DNS server IP address. |
| **Cancel** | Discard current modification. |
| **Save** | Save the current settings. |

### 7.3.2.2 IP Routed Subnet

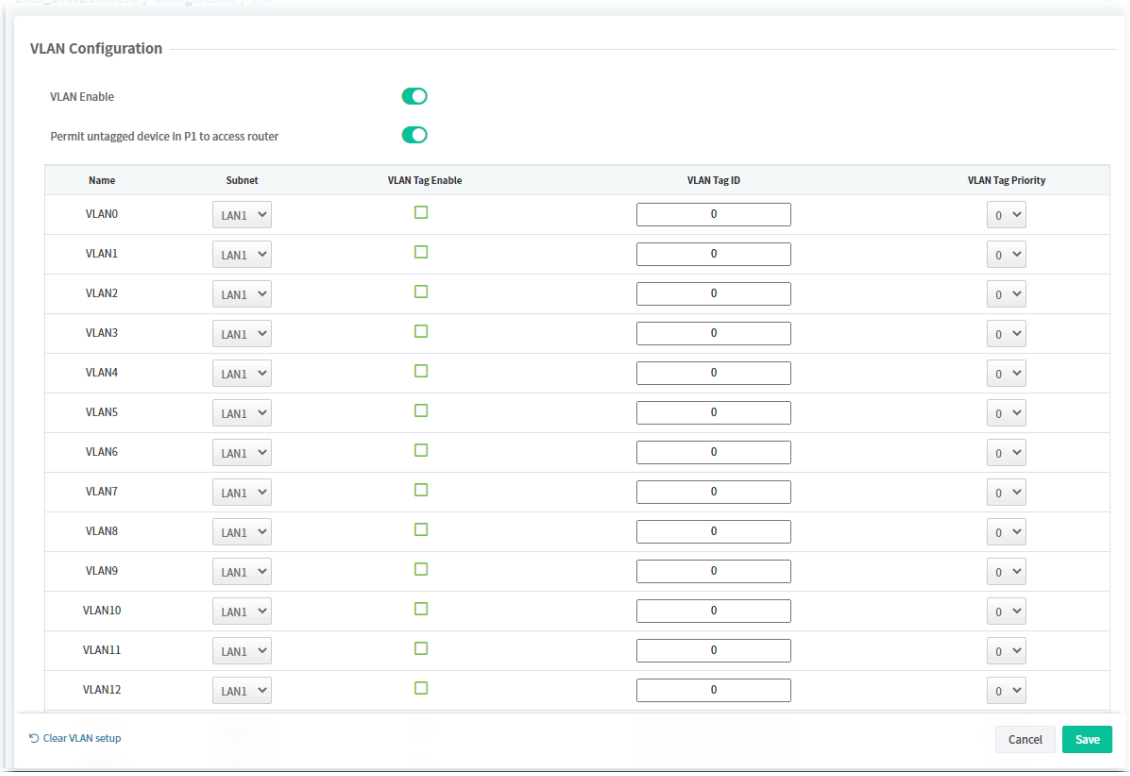



The parameters are explained as follows:

| Item | Description |
|---|---|
| | **General Setup** |
| **Enable** | **Click** to enable / disable the IP routed subnet configuration. |
| **IP Address** | It is the IP address of the router. |
| **Subnet Mask** | The subnet mask, together with the IP Address field, indicates the maximum number of clients allowed on the subnet. (Default: 255.255.255.0) |
| **RIP Protocol Control** | **Enable -** The router will attempt to exchange routing information with neighbouring routers using the Routing Information Protocol. |
| | **DHCP Server Setup** |
| **IP Pool Start** | Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. |
| **IP Pool Counts** | Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. |
| **DHCP Lease Time** | Enter the time to determine how long the IP address assigned by DHCP server can be used. |
| **Use LAN Port / Use LAN Port 1 /2** | Specify an IP for IP Route Subnet. If **Use LAN Port** is enabled, DHCP server will assign IP address automatically for the clients coming from P1 and/or P2. Please check the box of **Use LAN Port 1** and **Use LAN Port 2**. |
| **Use MAC Address** | Click to specify MAC address. |
| **MAC Address Table** | It displays the a list of MAC addresses.<br>**+Add -** Enter the MAC address in the boxes and click this button to add.<br>**+Edit -** Click to modify the address of the selected entry.<br>**Delete -** Click to remove the selected entry. |
| **Cancel** | Discard current modification. |

| | |
|---|---|
| **Save** | Save the current settings. |

### 9.4.2.3 VLAN



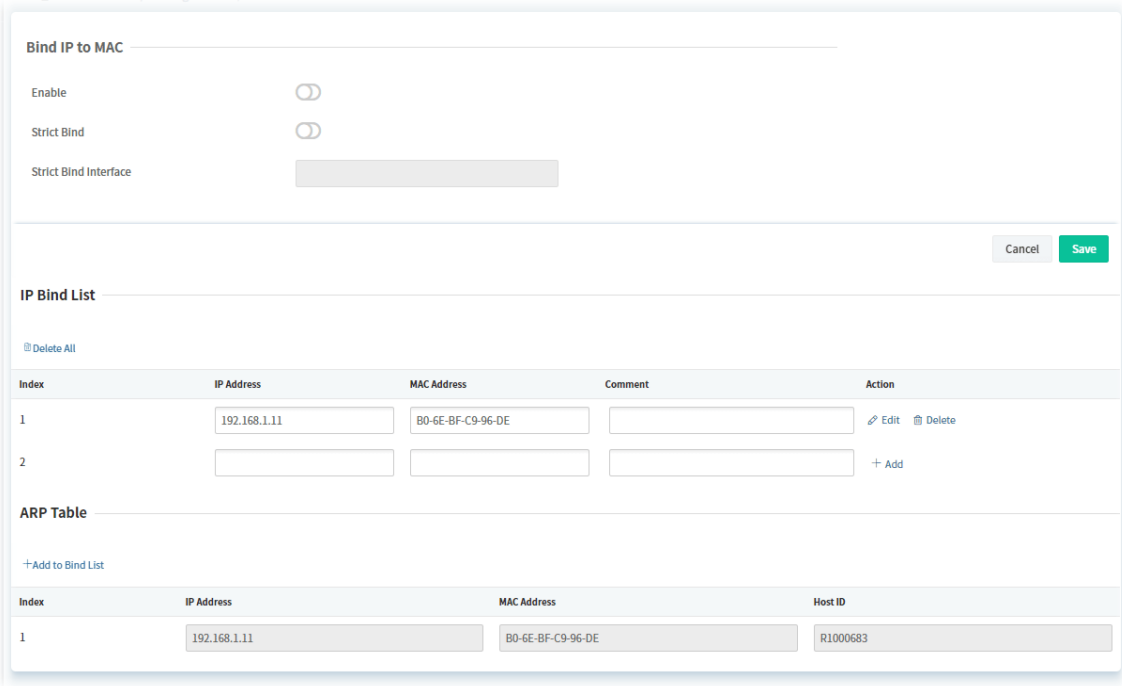

The parameters are explained as follows:

| Item | Description |
|---|---|
| | **VLAN Configuration** |
| **VLAN Enable** | Click to enable / disable the VLAN configuration. |
| **Permit untagged device P1 to access router** | Click to enable / disable the function.<br>If enabled, it allows untagged hosts connected to LAN port P1 to access the router. |
| **Subnet** | Choose one of them to make the selected VLAN mapping to the specified subnet only. |
| **VLAN Tag Enable** | Check to enable the function of VLAN with tag. |
| **VLAN Tag ID** | Enter the value as the VLAN ID number. The range is form 0 to 4095.<br>VIDs must be unique. |
| **VLAN Tag Priority** | Valid values are from 0 to 7, where 1 has the lowest priority, followed by 0, and finally from 2 to 7 in increasing order of priority. |
| | **VLAN Member(LAN)** |
| **P1 ~ P5** | Check the LAN port(s) to group them under the selected VLAN. |
| | **VLAN Member(Wireless 2.4G/5G)** |
| **SSID1~SSID4** | Check the SSID boxes to group them under the selected VLAN. |
| **Clear VLAN Setup** | Discard the modification and return to the original configuration of this page. |
| **Cancel** | Discard current modification. |

| | |
|---|---|
| **Save** | Save the current settings. |

### 9.4.2.4 Bind IP to MAC

This function is used to bind the IP and MAC address in LAN to have a strengthening control in network.

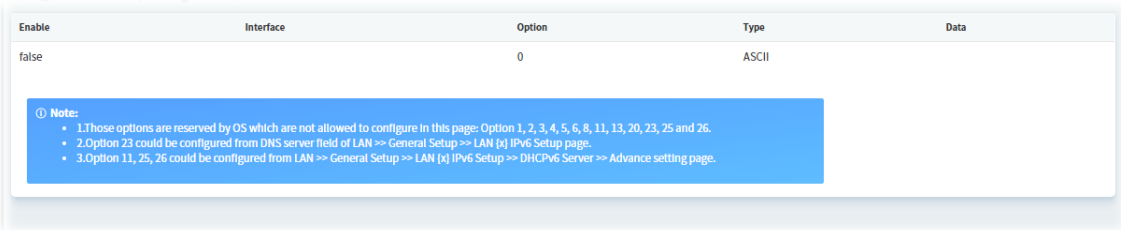



The parameters are explained as follows:

| Item | Description |
|---|---|
| | **Bind IP to MAC** |
| **Enable** | Click to enable or disable the function. |
| **Strict Bind** | Click to enable or disable the function. If enabled, the router will block the connection of the IP/MAC which is not listed in IP Bind List. |
| **Strict Bind Interface** | Choose the interface(s) for applying the rules of Bind IP to MAC. |
| **Cancel** | Discard current modification. |
| **Save** | Save the current settings. |
| | **IP Bind List** |
| **Delete All** | Delete all entries in IP Bind List. |
| **+Add** | After entering the IP address, MAC address and comment for a new entry, click +Add to create a new IP bind. |
| **Edit** | If IP address, MAC address and comment have been modified, click the Edit button to save the change. |
| **Delete** | Click the button to remove the selected index entry. |
| | **ARP Table** |
| **+Add to Bind List** | ARP table is the LAN ARP table of this router.<br>Click to add the ARP table onto the Bind List. |

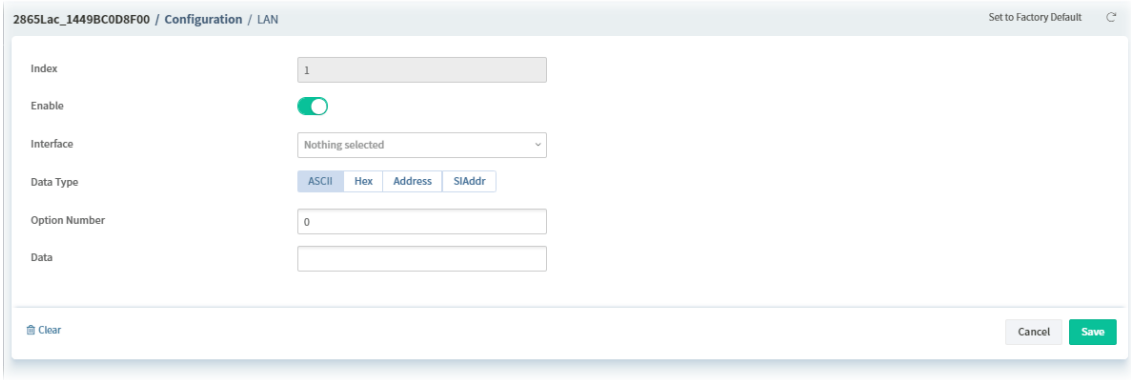
### 9.4.2.5 DHCP Server Option IPv4/IPv6

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




| Item | Description |
|---|---|
| **+Add** | Click to add a new option profile. |
| **Delete** | Click to remove a selected option profile. |

To modify the option setting, move the mouse cursor on the entry and click to open the setting page.



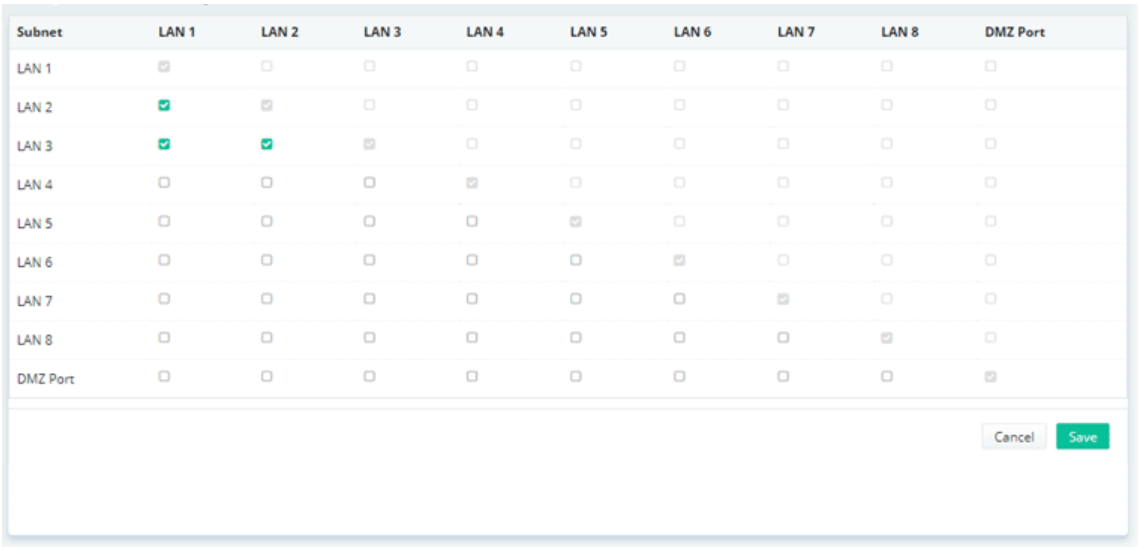

The parameters are explained as follows:

| Item | Description |
|---|---|
| **Index** | Displays the index number of the profile. |
| **Enable** | Click to enable or disable the DHCP option entry. |
| **Interface** | Select the LAN interface(s) to which this entry is applicable.<br>**Select All -** Select all LAN interfaces. |
| **Data Type** | Select the type of data in the Data field.<br>**ASCII** - A text string. Example: /path.<br>**Hex -** A hexadecimal string. Valid characters are from 0 to 9 and from a to f. Example: 2f70617468.<br>**Address -** One or more IPv4/IPv6 addresses, delimited by commas.<br>**SIAddr** - It is available for DHCP Server Option IPv4 only. Overrides the DHCP Next Server IP address (DHCP Option 66) supplied by the DHCP server. |
| **Option Number** | Enter a DHCP option number (e.g., 100). |
| **Data** | Enter the data for this DHCP option based on the data type selected. |
| **Next Server IPAddress/SIAddr** | Enter the DHCP next server IP address. It is available for DHCP Server Option IPv4 only. |
| **Cancel** | Discard current modification. |

| | |
|---|---|
| **Save** | Save the current settings. |

### 9.4.2.6 InterLAN Routing

Inter-LAN Routing allows different LAN subnets to be interconnected or isolated. It is only available when the VLAN functionality is enabled. In the Inter-LAN Routing matrix, a selected checkbox means that the 2 intersecting LANs can communicate with each other.

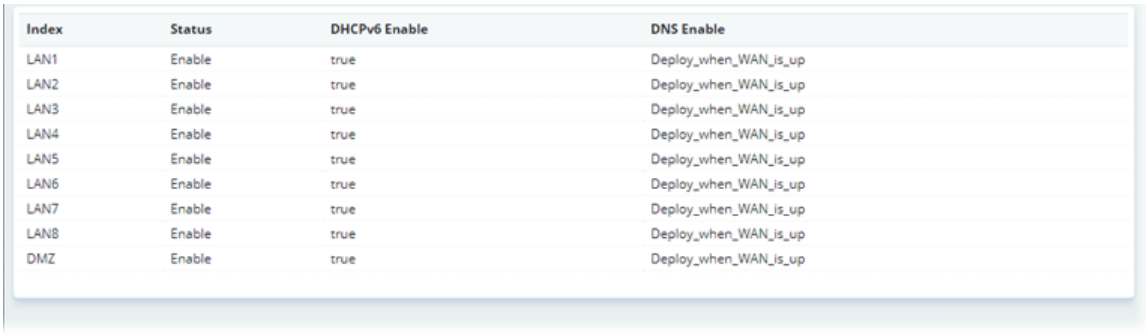



The parameters are explained as follows:

| Item | Description |
|---|---|
| **LAN1 to DMZ Port** | Check the box(es) to let the 2 intersecting LANs can communicate with each other. |
| **Cancel** | Discard current modification. |
| **Save** | Save the current settings. |

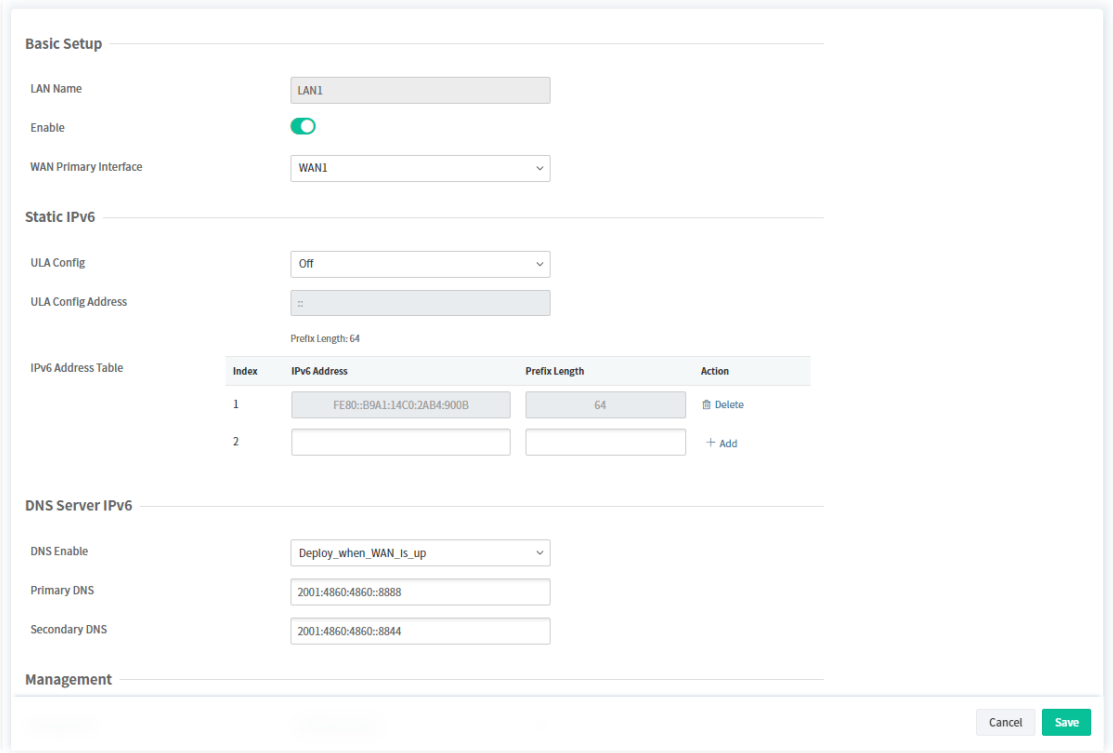
### 9.4.2.7 LAN IPv6

This page allows to configure IPv6 settings for each LAN.



| Index | Status | DHCPv6 Enable | DNS Enable |
|---|---|---|---|
| LAN1 | Enable | true | Deploy_when_WAN_is_up |
| LAN2 | Enable | true | Deploy_when_WAN_is_up |
| LAN3 | Enable | true | Deploy_when_WAN_is_up |
| LAN4 | Enable | true | Deploy_when_WAN_is_up |
| LAN5 | Enable | true | Deploy_when_WAN_is_up |
| LAN6 | Enable | true | Deploy_when_WAN_is_up |
| LAN7 | Enable | true | Deploy_when_WAN_is_up |
| LAN8 | Enable | true | Deploy_when_WAN_is_up |
| DMZ | Enable | true | Deploy_when_WAN_is_up |

To modify the IPv6 setting for each LAN, move the mouse cursor on the entry and click to open the setting page.




The parameters are explained as follows:

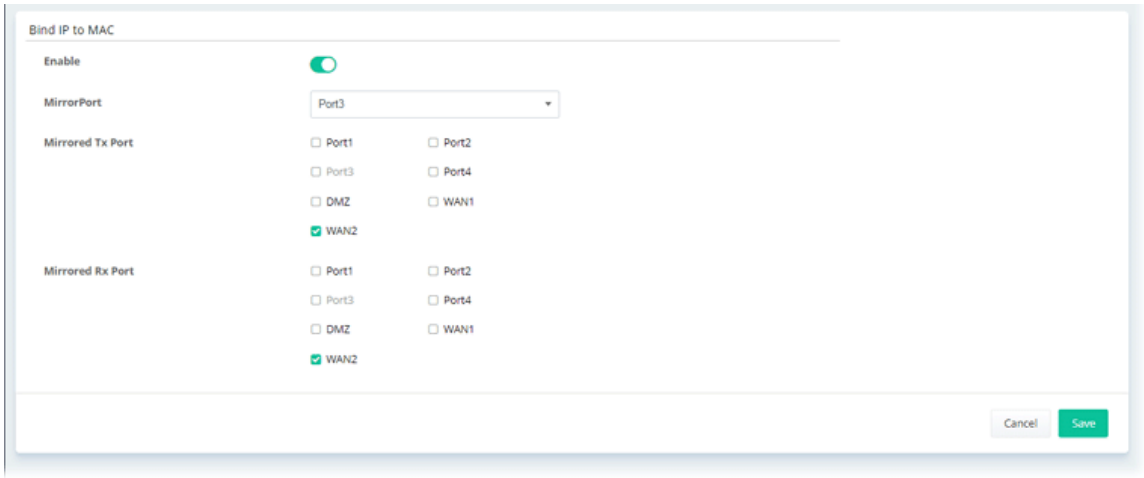
| Item | Description |
|---|---|
| | **Basic Setup** |
| **LAN Name** | Display the name of the LAN interface. |
| **Enable** | Click to enable or disable the configuration of LAN IPv6 Setup. |
| **WAN Primary Interface** | Specify a WAN interface for IPv6. |
| | **Static IPv6** |
| **ULA Config** | Select the ULA mode (off, Auto_ ULA_Prefix, Manually_ULA_Prefix). |
| **ULA Config Address** | LAN clients will be assigned ULAs generated based on the prefix manually entered. |
| **IPv6 Address Table** | Display current used IPv6 addresses. |

| | |
|---|---|
| | **DNS Server IPv6** |
| **DNS Enable** | Select Deploy_when_WAN_is_up, disable or enable.<br>**Deploy when WAN is up** - The RA (router advertisement) packets will be sent to LAN PC with DNS server information only when network connection by any one of WAN interfaces is up.<br>**Enable** - The RA (router advertisement) packets will be sent to LAN PC with DNS server information no matter WAN connection is up or not.<br>**Disable** - DNS server will not be used. |
| **Primary DNS** | Enter the IPv6 address for Primary DNS server. |
| **Secondary DNS** | Enter another IPv6 address for DNS server if required. |
| | **Management** |
| **Management** | Configures the Managed Address Configuration flag (M-bit) in Route Advertisements.<br>**Off** - No configuration information is sent using Route Advertisements.<br>**SLAAC(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 Vigor2865, or a separate DHCPv6 server. |
| **Other Option (O-bit)** | Click to enable or disable the function. If enabled, the O-bit will be enabled for obtaining additional information (e.g., DNS) from DHCPv6. |
| | **DHCPv6 Server** |
| **DHCPv6 Server Enable** | Click to enable DHCPv6 server. |
| **Auto IPv6 Range** | If enabled, Vigor router will assign the IPv6 range automatically. |
| **Start Address** | Enter the start address for IPv6 server. |
| **End Address** | Enter the end address for IPv6 server. |
| | **Router Advertisement** |
| **Enable** | Click to enable or disable the router advertisement server. |
| **Hop Limit** | The value is required for the device behind the router when IPv6 is in use. |
| **Min/Max Interval Time(sec)** | It defines the interval (between minimum time and maximum time) for sending RA (Router Advertisement) packets. |
| **Default Lifetime(sec)** | Within the period of time, Vigor router can be treated as the default gateway. |
| **Default Preference** | It determines the priority of the host behind the router when RA (Router Advertisement) packets are transmitted. |
| **MTU Auto** | If enabled, the router will determine the MTU value for LAN. |
| | **RIPng Protocol** |
| **Enable** | If enabled, RIPng (RIP next generation) offers the same functions and benefits as IPv4 RIP v2. |
| | **Extension WAN** |
| **Selected WAN** | Additional WANs selected to carry IPv6 traffic. |
| **Cancel** | Discard current modification. |

| | |
|---|---|
| **Save** | Save the current settings. |

### 9.4.2.8 Port Mirror

The LAN Port Mirror function allows network traffic of select LAN ports to be forwarded to another LAN port for analysis.

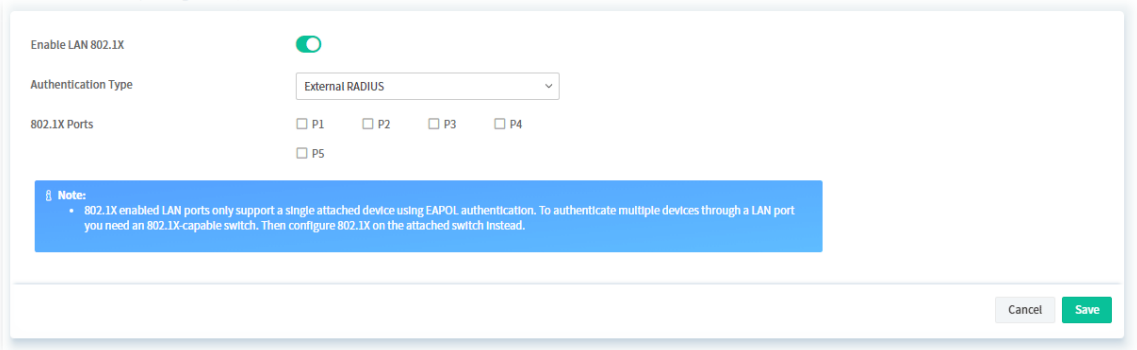



The parameters are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Enables or disables LAN Port Mirroring. |
| **Mirror Port** | One and only one port is selected as the mirror port, to which traffic is to be forwarded. |
| **Mirrored Tx Port** | Port(s) whose outbound traffic will be forwarded to the mirror port. |
| **Mirrored Rx Port** | Port(s) whose inbound traffic will be forwarded to the mirror port. |
| **Cancel** | Discard current modification. |
| **Save** | Save the current settings. |

### 9.4.2.9 Wired 802.1X

Wired 802.1X provides authentication for clients wishing to connect to the LAN by Ethernet.




The parameters are explained as follows:

| Item | Description |
|---|---|
| **Enable LAN 802.1x** | Check the box to enable LAN 802.1x function. |
| **Authentication Type** | **External RADIUS -** An external RADIUS server is to be used for 802.1X |

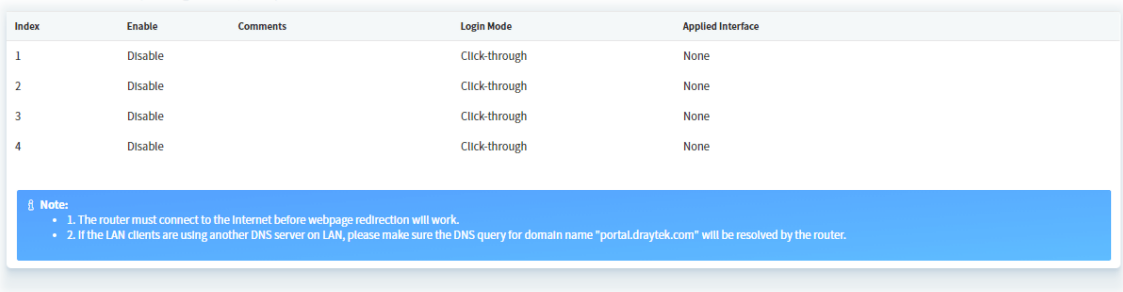
| | |
|---|---|
| | authentication.<br>**Local 802.1X** - Use the user database on the router to authenticate clients. |
| **802.1X ports** | 802.1X authentication will be available for the selected LAN ports. |
| **Cancel** | Discard current modification. |
| **Save** | Save the current settings. |

### 9.4.3 Hotspot Web Portal

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

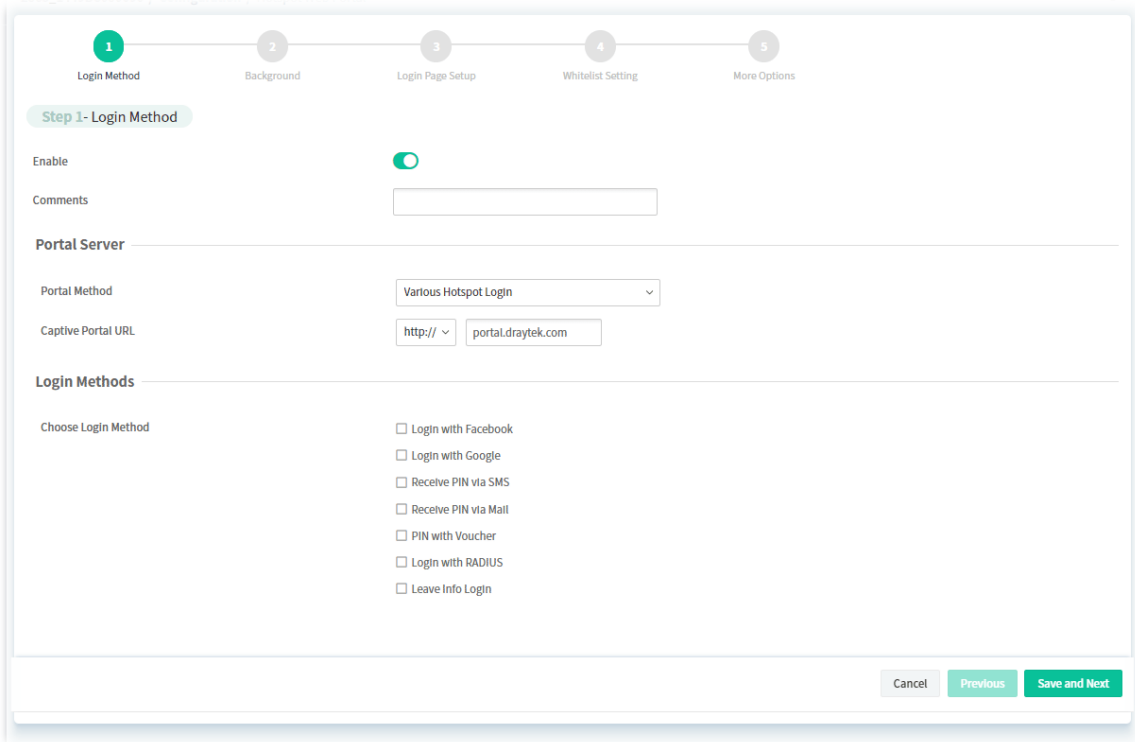
#### 9.4.3.1 Profile Setup

Profile Setup is used to create or modify Portal profiles. Up to 4 profiles can be created to meet different requirements according to LAN subnets, WLAN SSIDs, origin and destination IP addresses, etc.




To configure the profile, move the mouse cursor to any entry and click to open the setting page. Follow the on-screen steps to set the profile.

**Step (1) Login Method**




The parameters are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Check to enable this profile. |
| **Comments** | Enter a brief description to identify this profile. |

| | |
|---|---|
| | **Portal Server** |
| **Portal Method** | There are four methods to be selected as for portal server.<br>● **Skip Login, landing page only**<br>● **Click Through**<br>● **Various Hospot Login**<br>● **Leave Info Login**<br>● **External Portal Server** |
| | *When **Skip Loging, landing page only** or **Click through** is selected as Portal Method* |
| **Captive Portal URL** | Enter the captive portal URL. |
| | *When **Various Hotspot Login** is selected as Portal Method* |
| **Captive Portal URL** | Enter the captive portal URL. |
| **Login Methods** | This setting is available when **Various Hotspot Login** is selected as the portal method.<br>**Choose Login Method** - Select one or more desired login methods.<br>● Login with Facebook<br>● Login with Google<br>● Receive PIN via SMS<br>● Receive PIN via Mail<br>● PIN with Voucher<br>● Login with RADIUS<br>● Leave Info Login |
| **Facebook**<br>(Login with Facebook**)** | This setting is available when **Login with 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. |
| **Google**<br>(Login with 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. |
| **SMS Provider**<br>(Receive PIN via SMS) | This setting is available when **Receive PIN via SMS** is selected as the login method.<br>**Receiving PIN via SMS Provider** - Select the SMS Provider used to send PIN notifications SMS providers. |
| **Mail Server**<br>(Receive PIN via Mail Server) | This setting is available when **Receive PIN via Mail** is selected as the login method.<br>**Receiving PIN via Mail** - Select the SMS Provider used to send PIN notifications SMS providers. |
| **Radius Server**<br>(Login with RADIUS) | This setting is available when **Login with RADIUS** is selected as the login method.<br>**Authentication Method** – Click link to configure the external RADIUS server for authenticating web portal clients.<br>**RADIUS MAC Authentication** – Check **Enable** to activate user authentication by MAC address. |

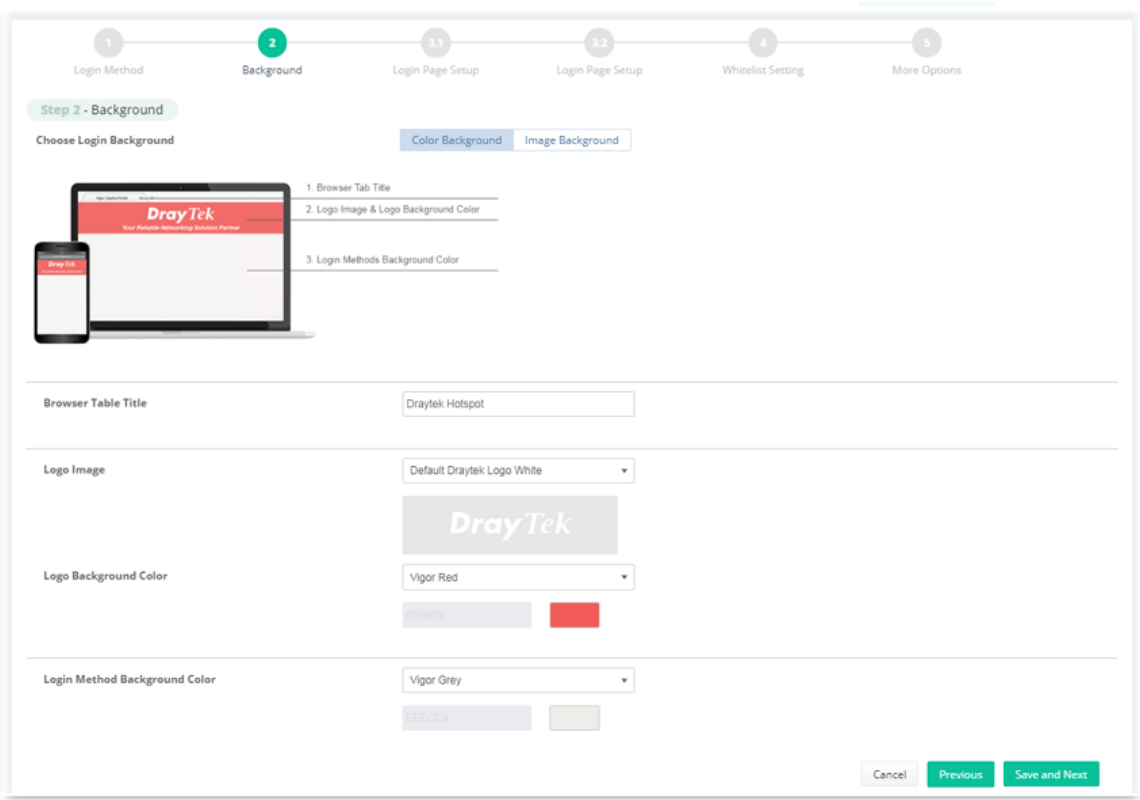
| | |
|---|---|
| | **MAC Address Format** – Select the MAC address format that is used by the RADIUS server. |
| | *When **External Portal Server** is selected as Portal Method* |
| **Redirection URL** | Enter the URL to which the client will be redirected. |
| **RADIUS Server** | **Authentication Method** - To configure the RADIUS server, click the External RADIUS Server link and you will be presented with the configuration page.<br>**RADIUS MAC Authentication** - 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 the ID (string) for RADIUS NAS-Identifier. |
| **Cancel** | Discard current modification. |
| **Previous** | Return to previous page. |
| **Save and Next** | Save the current settings and get into next page. |

If you have chosen **Skip Login, landing page only** or **External Portal Server** as the portal method, skip to step 4 *Whitelisting* below.

Otherwise, proceed to configure the login page by following steps 2 and 3.

**Step (2) Background**

Select a background for the login page.



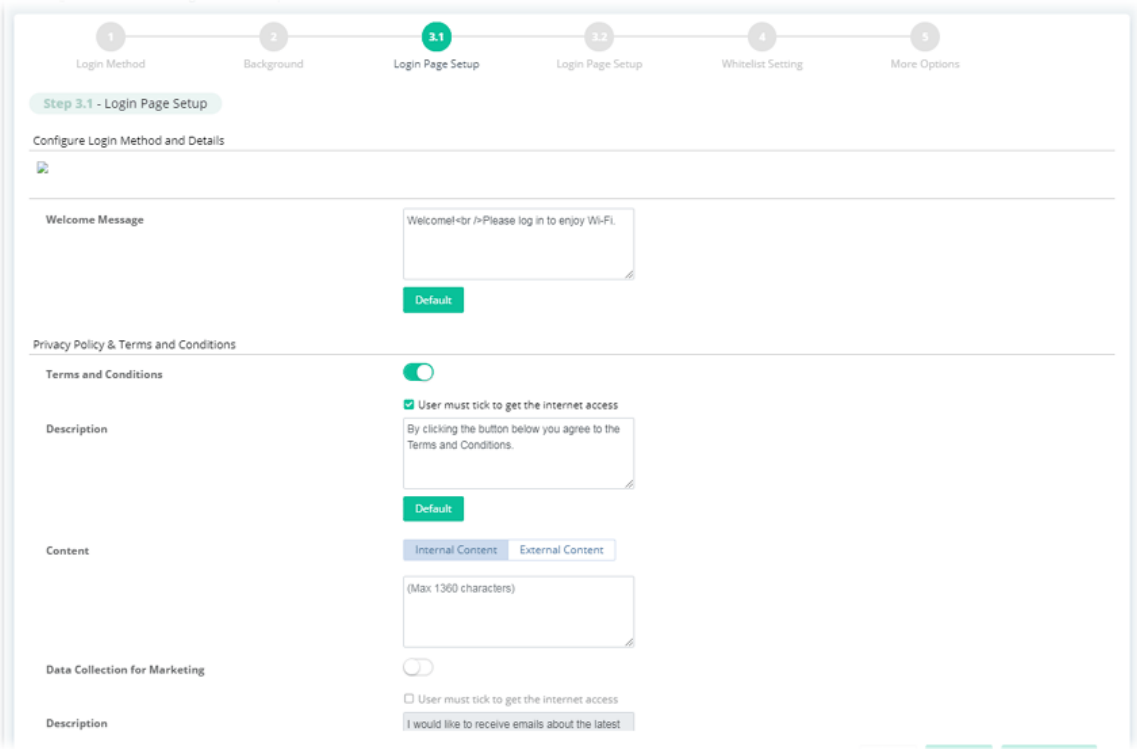

The parameters are explained as follows:

| Item | Description |
|---|---|
| **Choose Login Background** | Select either **Color Background** or **Image Background** as the login page background scheme. |

| | |
|---|---|
| **Browser Tab Title** | Enter the text to be shown as the webpage title in the browser. |
| **Logo Image** | The DrayTek Logo will be displayed by default. However, you can enter HTML text or upload an image to replace the default logo. |
| **Login Method Background Color** | Select the background color of the login panel from the predefined color list, or select **Customize Color** and enter the RGB value. Click **Preview** to preview the selected color. |
| **Opacity (10 ~ 100)** | Available when **Image Background** is selected. Set the opacity of the background image. |
| **Background Image** | Available when **Image Background** is selected. Click **Browse...** to select an image file (.JPG or .PNG format), then click **Upload** to upload it to the router. |
| **Cancel** | Discard current modification. |
| **Previous** | Return to previous page. |
| **Save and Next** | Save the current settings and get into next page. |

If you have selected **Skip Login, landing page only** or **External Portal Server** as the portal method, proceed to Step 4 *Whitelist Setting*; otherwise, continue to Step 3 *Login Page Setup.*

**Step (3) Login Page Setup**



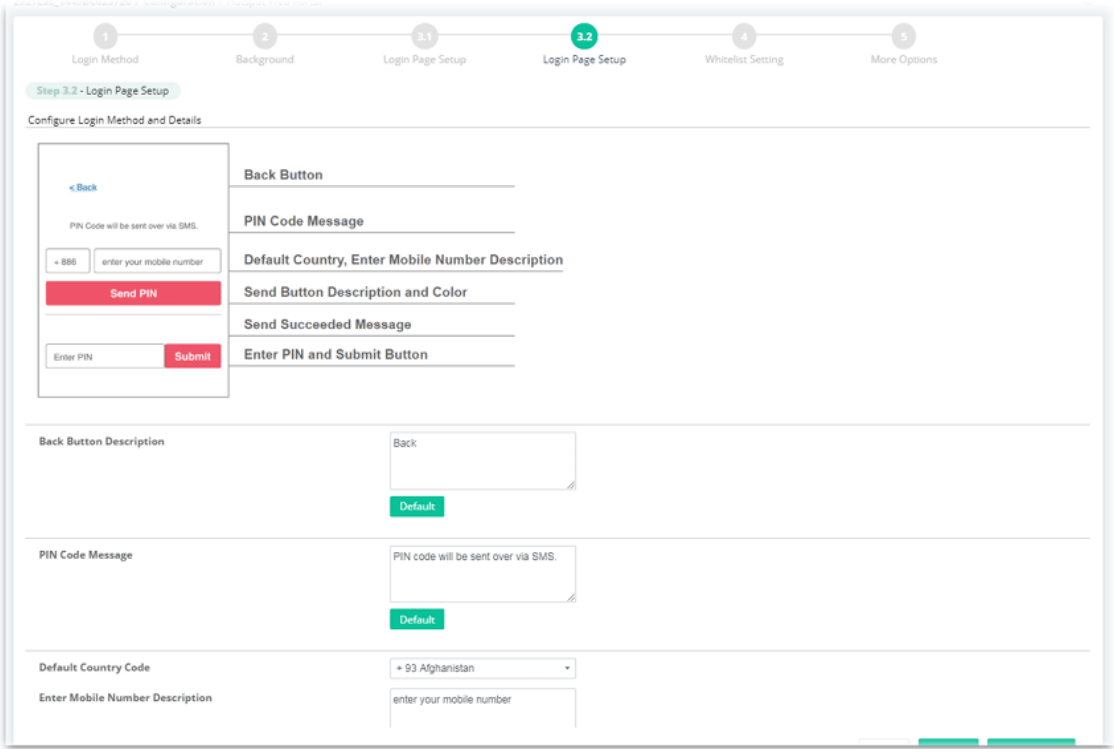

The parameters are explained as follows:

| Item | Description |
|---|---|
| | if you have selected **Click Through** as the Portal Method. |
| **Welcome Message** | Enter the text to be displayed as the welcome message. |
| **Terms and Conditions** | Click to enable/disable the function.<br>**User must tick to get the internet access** - Click to ask the user ticking the box for getting the Internet access. |
| **Description** | Enter the text to be displayed in the Terms and Conditions pop-up window. |

| | |
|---|---|
| **Content** | If enabled, a check box with a description will be shown on the web portal login page.<br>**Internal Content** - Click it for displaying the message that you want the user knows on the web portal login page.<br>● Enter the text on the box below the Internal Content button.<br>**External Content** - Click it for opening another URL web page.<br>● **External Content URL** - Enter the URL. |
| **Data Collection for Marketing** | If enabled, a check box with a description will be shown on the web portal login page.<br>**User must tick to get the internet access** - Click to ask the user ticking the box for getting the Internet access.<br>**Description** - Enter a brief description for explaining if a user wants to access the Internet, he/she must agree for data collection made by network supplier. |
| **Enter PIN Description** | Enter the existing PIN code. |
| **Submit Button Description** | Enter the text to be displayed on the Submit button |
| **Accept Button Description** | Enter the text to be displayed on the accept button |
| **Accept Button Color** | Select the color of the accept button from the predefined color list, or select **Customize Color** and enter the RGB value. Click **Preview** to preview the selected color. |
| | if you have selected **Various Hotspot Login** as the portal method. |
| **Welcome Message** | Enter the text to be displayed as the welcome message. |
| **Terms and Conditions** | Click to enable/disable the function.<br>**User must tick to get the internet access** - Click to ask the user ticking the box for getting the Internet access. |
| **Description** | Enter the text to be displayed in the Terms and Conditions pop-up window. |
| **Content** | If enabled, a check box with a description will be shown on the web portal login page.<br>**Internal Content** - Click it for displaying the message that you want the user knows on the web portal login page.<br>● Enter the text (maximum 1360 characters) on the box below the Internal Content button.<br>**External Content** - Click it for opening another URL web page.<br>● **External Content URL** - Enter the URL. |
| **Data Collection for Marketing** | If enabled, a check box with a description will be shown on the web portal login page.<br>**User must tick to get the internet access** - Click to ask the user ticking the box for getting the Internet access.<br>**Description** - Enter a brief description for explaining if a user wants to access the Internet, he/she must agree for data collection made by network supplier. |
| **Facebook Login Description** | Enter the text to be displayed on the Facebook login button. |
| **Google Login Description** | Enter the text to be displayed on the Google login button. |

| | |
|---|---|
| **Hint Message for PIN** | Enter the text used to suggest users to choose SMS authentication. |
| **Receiving PIN Description** | Enter the text to be displayed on the button that the user clicks to receive an SMS PIN. |
| **Receiving PIN via SMS Content** | Enter the message to be sent by SMS to inform the user of the PIN. The PIN variable is specified by **<PIN>** within the message. |
| **Enter PIN Description** | Enter message to be displayed in the PIN textbox to prompt the user to enter the PIN. |
| **Submit Button Description** | Enter the text to be displayed on the submit PIN button |
| **Submit Button Color** | Select the color of the submit button from the predefined color list, or select **Customize Color** and enter the RGB value. Click **Preview** to preview the selected color. |
| **Hint Message for RADIUS** | Enter the text used to prompt the user to login. |
| **RADIUS Account Description** | Enter the text to prompt the user to enter the username. |
| **RADIUS Password Description** | Enter the text to prompt the user to enter the password. |
| **Login Button Description** | Enter the text to be displayed on the login button. |
| **Login Button Color** | Select the color of the login button from the predefined color list, or select **Customize Color** and enter the RGB value. Click **Preview** to preview the selected color. |
| **Cancel** | Discard current modification. |
| **Previous** | Return to previous page. |
| **Save and Next** | Save the current settings and get into next page. |

if you have selected **Various Hotspot Login** as the portal method and selected **Receive PIN via SMS** as the login method, you will also need to configure (3.2 Login Page Setup) page.

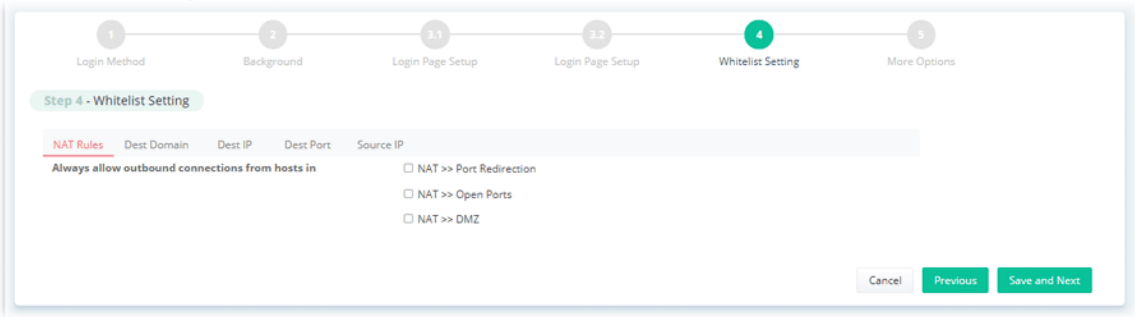



The parameters are explained as follows:

| Item | Description |
|---|---|
| **Back Button Description** | Enter text for the label of the hyperlink to return to the previous page. |
| **PIN Code Message** | Enter text to be displayed as the body text on the page. |
| **Default Country Code** | Select the default country code to be displayed using the dropdown menu. |
| **Enter Mobile Number Description** | Enter message to be displayed in the mobile number textbox to prompt the user to enter the mobile number. |
| **Send Button Description** | Enter the label text of the send button. |
| **Send Button Color** | Select the color of the send button from the predefined color list, or select **Customize Color** and enter the RGB value. Click **Preview** to preview the selected color. |
| **Send Succeeded Message** | Enter text to be displayed to notify the user after the PIN has been sent. |
| **Cancel** | Discard current modification. |
| **Previous** | Return to previous page. |
| **Save and Next** | Save the current settings and get into next page. |

### Step (4) Whitelist Setting

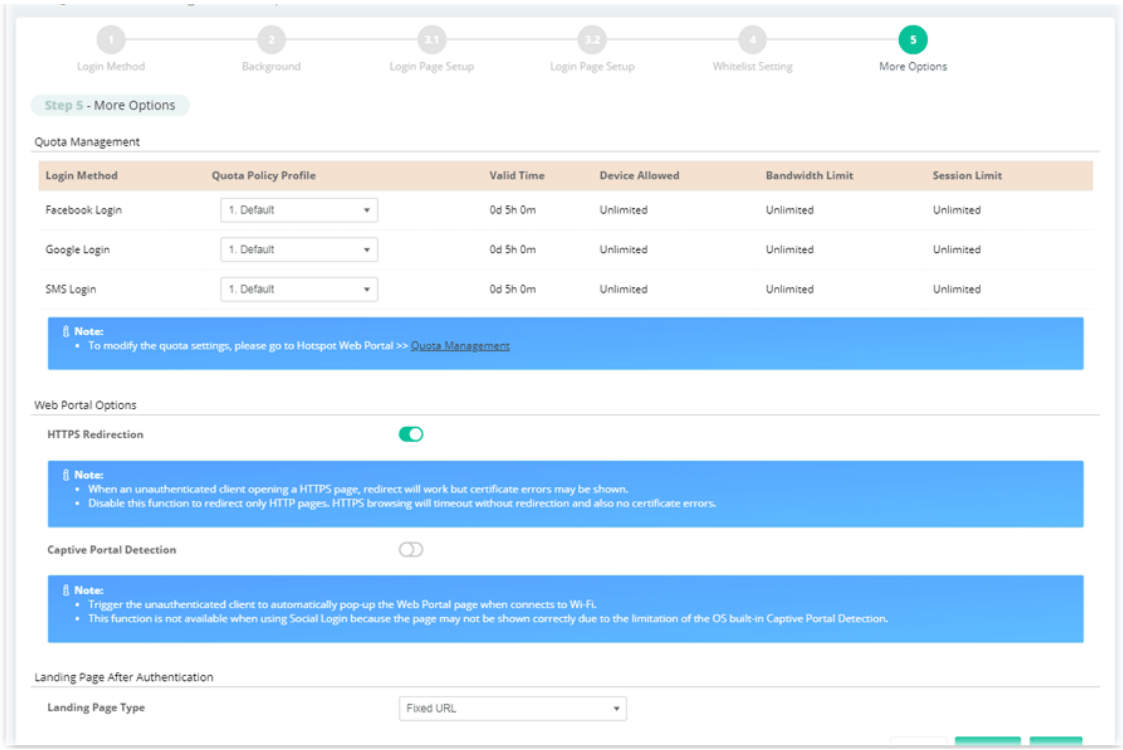
Configure the whitelist settings. Users are allowed to send and receive traffic that satisfies whitelist settings.




The parameters are explained as follows:

| Item | Description |
|---|---|
| **NAT Rules** | To prevent web portal settings from conflicting with NAT rules resulting in unexpected behavior, select the NAT rules that are allowed to bypass the web portal. Hosts listed in selected NAT rules can always access the Internet without being intercepted by the web portal. |
| **Dest Domain** | Enter up to 30 destination domains that are allowed to be accessed. |
| **Dest IP** | Enter up to 30 destination IP addresses that are allowed to be accessed. |
| **Dest Port** | Enter up to 30 destination protocols and ports that are allowed through the router. |
| **Source IP** | Enter up to 30 source IP addresses that are allowed through the router. |
| **Cancel** | Discard current modification. |
| **Previous** | Return to previous page. |
| **Save and Next** | Save the current settings and get into next page. |

### Step (5) More Options




The parameters are explained as follows:

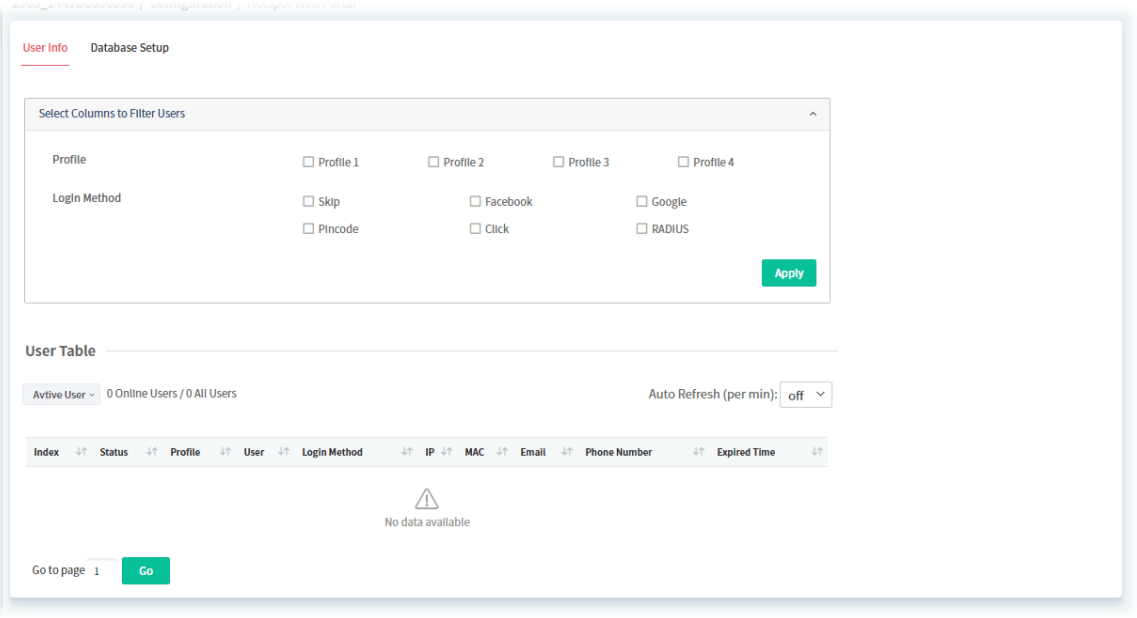
| Item | Description |
|---|---|
| | **Quota Management** |
| **Quota Policy Profile** | Choose a policy profile to apply to web portal clients. |
| | **JSON API** |
| **Enable JSON API** | If enabled, information (e.g., string, number, object and so on) will be saved as a text file on the JSON server. |
| **Server URL** | Enter the URL of the server which will store the JSON information. |
| **Get JSON and Update user status every** | Specify the time period for the JSON server sending the JSON information to other devices automatically. |
| **Update Information** | The information sent out by JSON server might include the following types:<br>● NAS-Identifier ( router's ID)<br>● MAC Address (routers' MAC address)<br>● All User Number (total number of the users connecting to the router)<br>● Wi-Fi User Number (total number of the wireless users connecting to the router) |
| | **Web Portal Options** |
| **HTTPS Redirection** | If this option is selected, unauthenticated clients accessing HTTPS websites will be redirected to the login page, but the browser may alert the user of certificate errors. If this option is not selected, attempts to access to HTTPS website will time out without redirection. |
| **Captive Portal Detection** | If this option is selected, the web portal page is triggered automatically when an unauthenticated client tries to access the Internet. This function is not available when the Login Mode is **Social Login**, as the web portal page may not be shown correctly due to the limitations of the operating system's built-in Captive Portal Detection. |

| | |
|---|---|
| | **Landing Page After Authentication** |
| **Landing Page Type** | **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.<br>**Bulletin Message -** The message configured here will be briefly shown for a few seconds to the user.<br>● **Bulletin Message Type** - Select HTML or Image Upload.<br>● **Default –** This button is enabled when **Bulletin Message** is selected. Click to load the default text into the bulletin message textbox. |
| **Force Landing Page Stay Enable** | If enabled, the landing page will stay until you close it. |
| | **Applied Interfaces** |
| **Subnet** | The current Hotspot Web Portal profile will be in effect for the selected subnets. |
| **WLAN 2.4G / 5G** | The current Hotspot Web Portal profile will be in effect for the selected WLAN SSIDs. |
| **Cancel** | Discard current modification. |
| **Previous** | Return to previous page. |
| **Finish** | Complete the configuration. |

### 9.4.3.2 Users Information

This page displays information of users accessing the Internet through the web portal.

#### 6.3.3.2.1 User Info



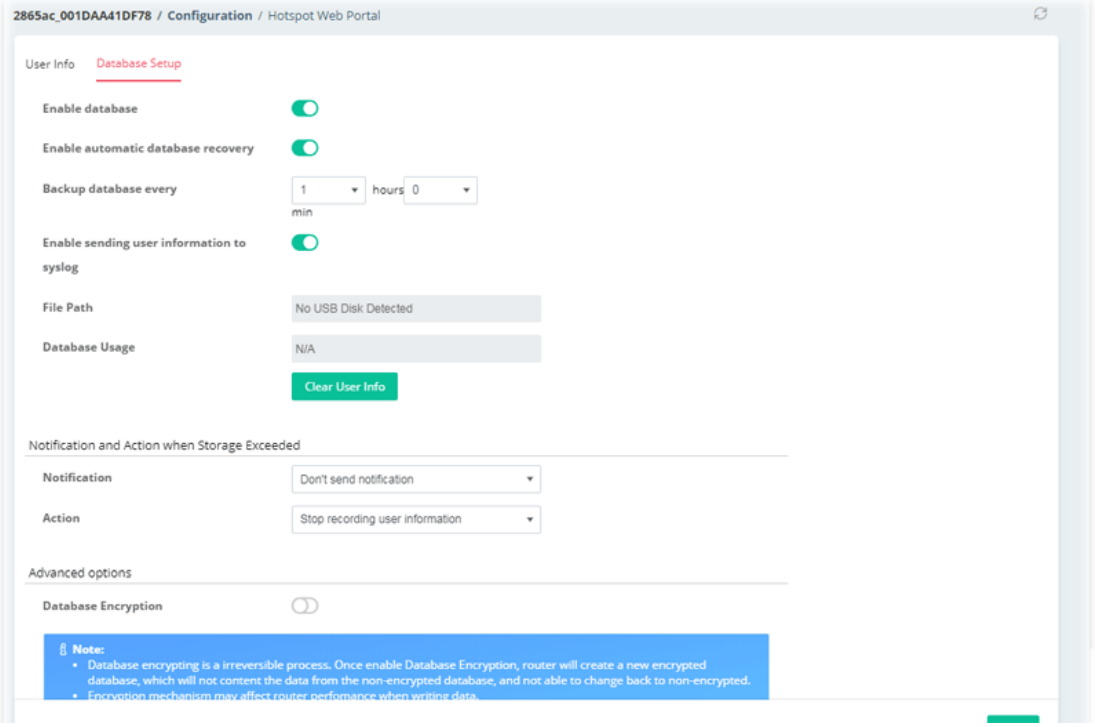

These parameters are explained as follows:

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

| | |
|---|---|
| **Select Columns to Filter Users** | Select the profiles and the login methods to filter the displayed users.<br>**Apply** - Save the settings. |
| **User Table** | Details of users accessing the Internet via Hotspot Web Portal will be displayed. |
| **Active User / All Database** | Displays the information for active user only or for all users in database. |
| **Auto Refresh** | On/off - Refresh current page automatically or not. |
| **Go** | Where there are more than one page, Click to open the page with specified number. |

#### 7.3.3.2.2 Database Setup

This page allows the user to configure settings for database on USB disk.



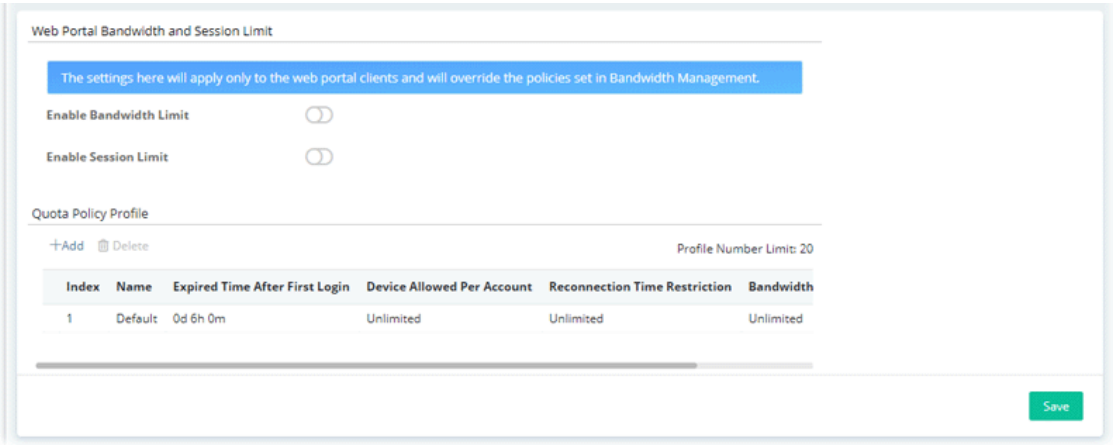

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Enable database** | Check the box to record user information on router's database. |
| **Enable automatic database recovery** | Check the box to enable the functionality of the database recovery on the USB disk.<br>**Backup database every**... - Set the interval to backup the database. |
| **Enable sending user information to syslog** | Check the box to send user information to syslog. |
| **File Path** | If a USB disk has been inserted into the USB port of Vigor router, the file path will be shown in this area. |
| **Database Usage** | Display the usage and remaining space on the database.<br>**Clear User Info** – The user information will be displayed on the page of User Info. You can delete the information by clicking this button. |
| | **Notification and Action when Storage Exceeded** |

| | |
|---|---|
| **Notification** | **Don't send notification** - Vigor router system will not send any notification to any recipient.<br>**Send notification** - Vigor router system will send a notification e-mail to specified recipient(s) that selected from **Email Notification Object** and **SMS Notification Object**.<br>● **Email Notification Object**<br>● **SMS Notification Object** |
| **Action** | **Stop recording user information** - Vigor router system will stop to record the user information onto USB disk.<br>**Backup and clean up all user info, and start a new record** - Vigor router system will backup all existed information on the USB disk onto the host and clean up the information from USB disk. Later, it will start a new record. |
| | **Advanced Options** |
| **Database Encryption** | Select to have the router create a new encrypted database. Once this is done, you will not be able to revert to an unencrypted database. |
| **Password** | Enter a password for encryption. |
| **Confirm Password** | Enter the password again for confirmation. |
| **Save** | Save the current settings. |

### 9.4.3.3 Quota Management

The system administrator can specify bandwidth and sessions quota which is only applicable to the web portal clients.

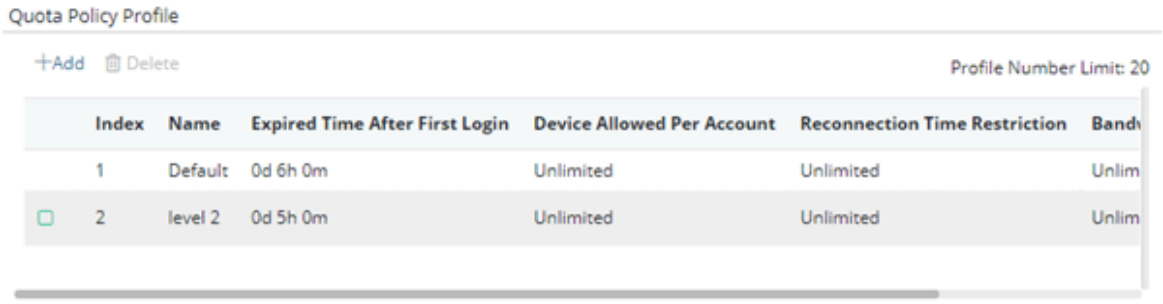



These parameters are explained as follows:

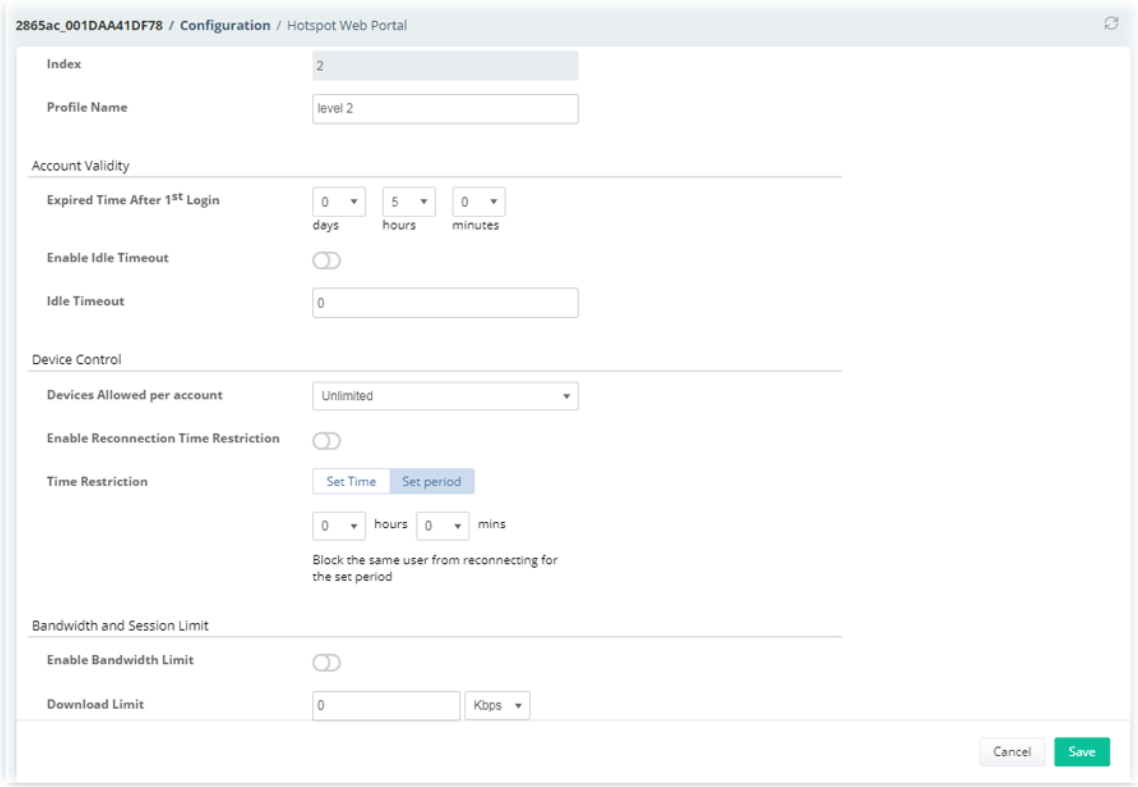
| Item | Description |
|---|---|
| | **Web Portal Bandwidth and Session Limit** |
| **Enable Bandwidth Limit** | Click to enable / disable the function.<br>If enabled, it will override the policy configured in **Bandwidth Management >> Bandwidth Limit.** |
| **Enable Session Limit** | Click to enable / disable the function.<br>If enabled, it will override the policy configured in **Bandwidth Management >> Sessions Limit.** |
| | **Quota Policy Profile** |

| | |
|---|---|
| **+Add** | Create up to 20 policy profiles. |
| **Delete** | Delete the selected policy profile. |
| **Save** | Save the current settings. |

To create a new policy profile, click **+Add** to create a new profile and display on the table.




Check the box in front of the new entry and click to open the following page.




These parameters are explained as follows:

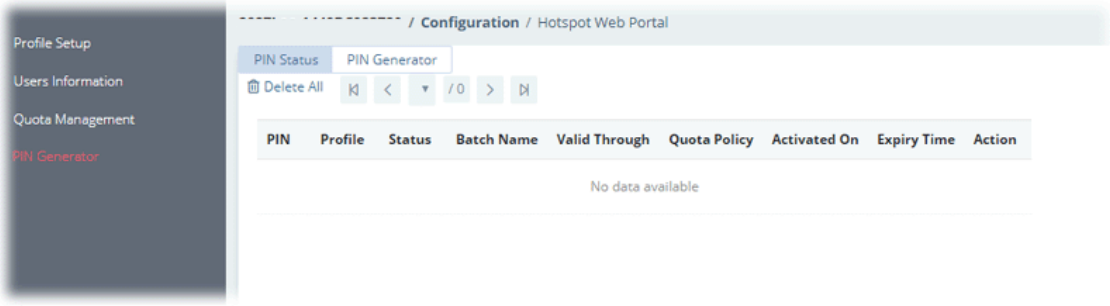
| Item | Description |
|---|---|
| **Index** | Display the index number of the profile. |
| **Profile Name** | Enter a name for a new profile. |
| | **Account Validity** |
| **Expired Time After 1st Login** | Sets the days, hours, and minutes. After the login has expired, Vigor router will block the client from accessing the network/Internet. |
| **Enable Idle Timeout** | If enabled, Vigor router will terminate the network connection if the is no activity from the user after the specified idle time has passed. |
| **Idle Timeout** | Enter a time value (unit: minutes). |

| | |
|---|---|
| | **Device Control** |
| **Devices Allowed per account** | Select the maximum number of devices that can be connected to the network using the same account. |
| **Enable Reconnection Time Restriction** | Click to enable / disable the function. |
| **Time Restriction** | Blocks the account from being used to connect devices to the network in one of two ways:<br>**Set Time (At .... Everyday)** - After the login expires, the account cannot be used to connect devices to the network until the set time of day.<br>**Set Period (Hours.. min)**- After the login expires, the account cannot be used to connect devices to the network for a set period of time. |
| | **Bandwidth and Session Limit** |
| **Enable Bandwidth Limit** | Click to enable / disable the function. |
| **Download /Upload Limit** | Set the maximum upload and download speeds. |
| **Enable Session Limit** | Click to enable / disable the function. |
| **Session Limit** | Set a maximum session limit for web portal clients. |
| **Cancel** | Discard current modification. |
| **Save** | Save the current settings. |

### 9.4.3.4 PIN Generator

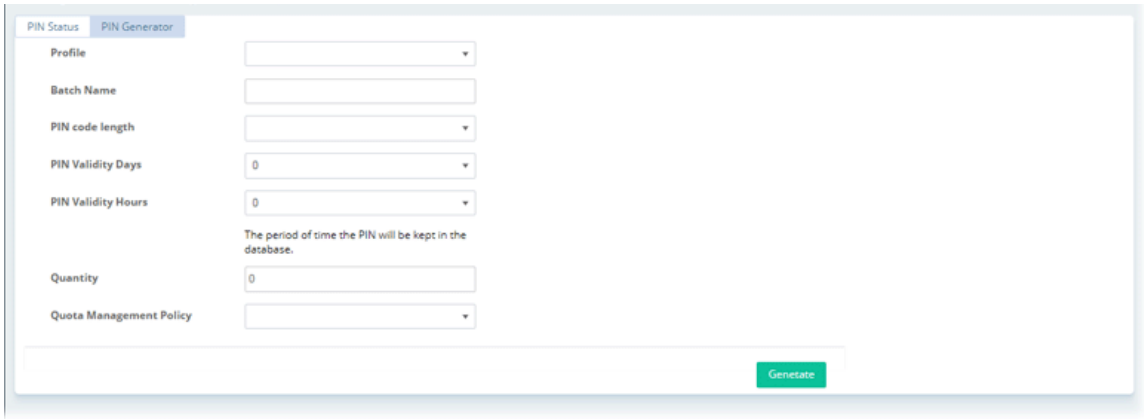
#### 9.4.3.4.1 PIN Status

This page displays the detailed information for PIN codes generated by PIN Generator.




#### 9.4.3.4.2 PIN Generator

The system administrator can generate multiple PIN codes in response to the user's (e.g., enterprise) demand.



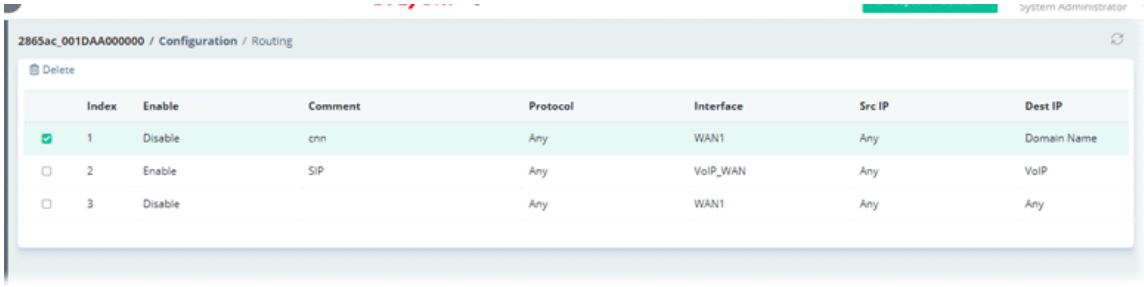

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Profile** | Use the drop down menu to specify an index number (from 1 to 4). |
| **Batch Name** | Enter a string as a batch name. |
| **PIN code length** | Specify the length of PIN code. |
| **PIN Validity Days** | Set the days for the period of validity. |
| **PIN Validity Hours** | Set the hours for the period of validity. |
| **Quantity** | Set the quantity of the PIN code. |
| **Quota Management Policy** | Use the drop down list to choose policy profile. |
| **Generate** | Click to generate a PIN code as a voucher. |

## 9.4.4 Routing

### 9.4.4.1 Load Balance/Policy Route

This page lists the configured policies coming from Vigor CPE.

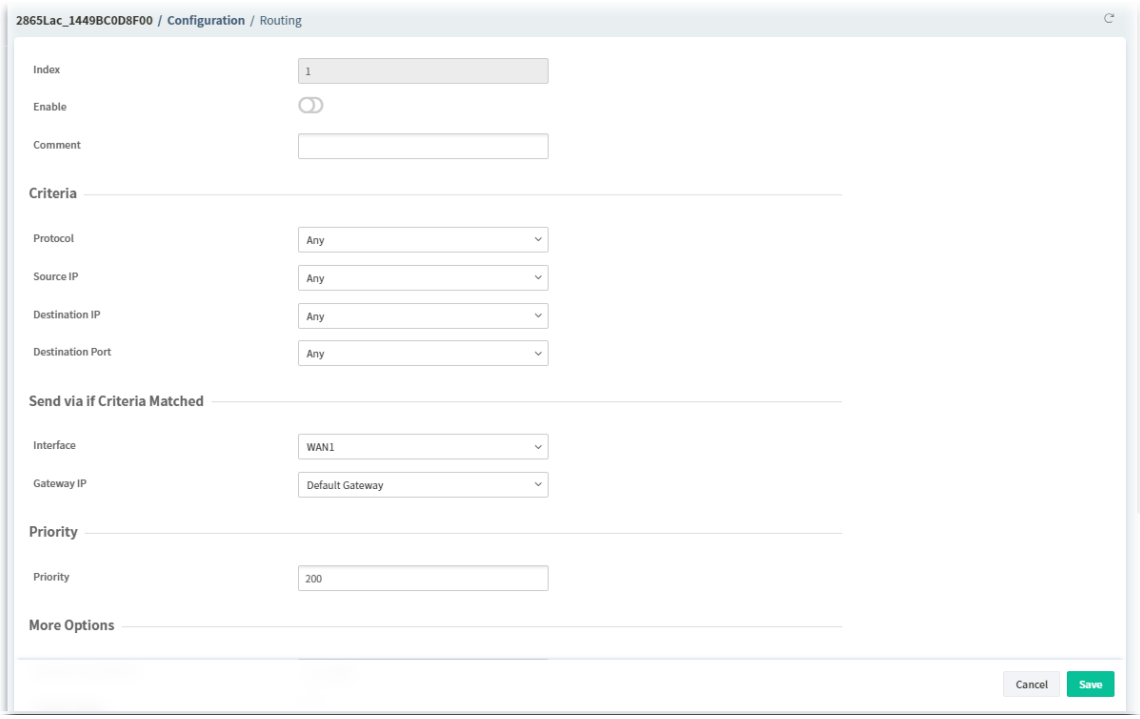



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Delete** | Click to remove the selected routing policy. |
| **Index** | Displays the index number of the routing policy. |
| **Enable** | Displays the status (enable / disable) of the routing policy. |
| **Comment** | Displays the description for the routing policy. |
| **Protocol** | Displays the protocol used for this policy. |
| **Interface** | Displays the interface to send packets to once the policy is matched. |

| | |
|---|---|
| **Src IP** | Displays the mode for the source IP. |
| **Dest IP** | Displays the mode for the destination IP. |

To configure the policy, move the mouse cursor to any entry and click to open the setting page.



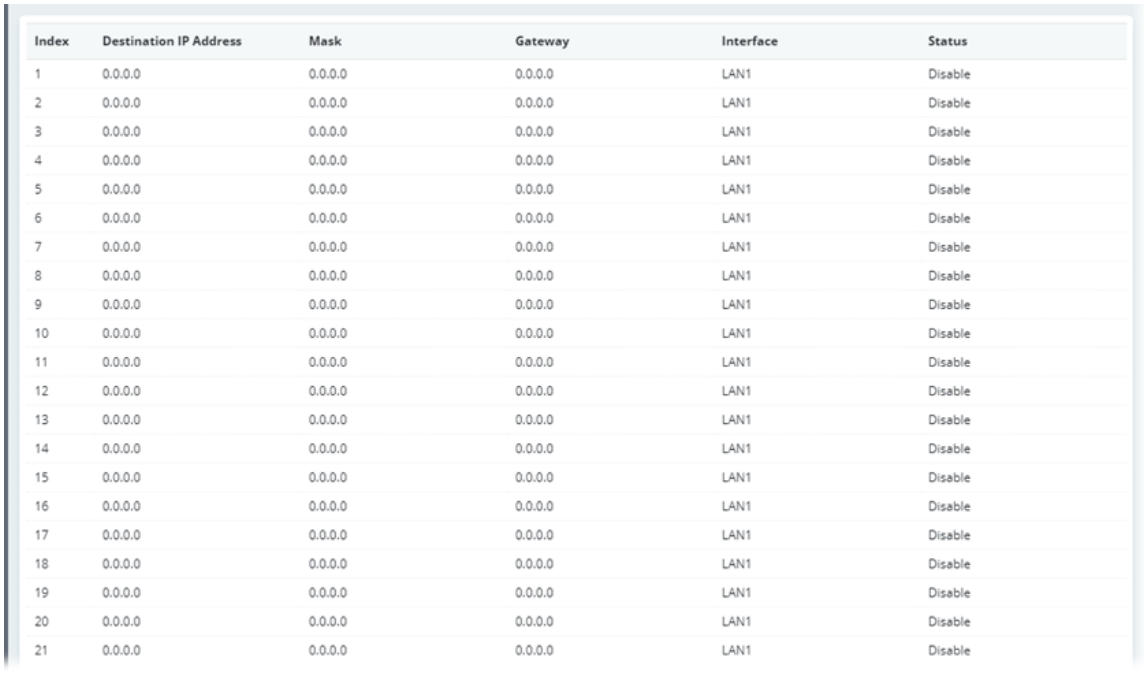

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Index** | Displays the index number of the routing policy. |
| **Enable** | Click to enable / disable the routing policy. |
| **Comment** | Enter a brief explanation for the routing policy. |
| | **Criteria** |
| **Protocol** | Use the drop-down menu to choose a proper protocol for the WAN interface. |
| **Source IP** | Select the mode (Any, IP Range, IP Subnet, IP Object or IP Group) of the source IP.<br>Enter the IP address(es), network, mask, or select IP object/group as the source IP based on the source IP mode used. |
| **Destination IP** | Select the mode (Any, IP Range, IP Subnet, Domain Name, IP Object, IP Group or Country Object) of the destination IP.<br>Enter the IP address(es), network, mask, domain name, or select an object/group as the destination IP based on the destination IP mode used. |
| **Destination Port** | Select the mode (Any or Range) for the destination port.<br>Enter the port values as the destination port based on the destination port mode used. |
| | **Send via if Criteria Matched** |
| **Interface** | Use the drop down list to choose a WAN or LAN interface or VPN profile. |
| **Gateway IP** | **Default Gateway** - Default Gateway is selected in default.<br>**Specific Gateway** - It is used only when you want to forward the packets |

| | |
|---|---|
| | to the desired gateway. |
| | **Priority** |
| **Priority** | The greater the value is, the lower the priority is. Default value for route policy is “200” which means it has higher priority than the default route. |
| | **More Options** |
| **Packet Forwarding Via** | When you choose WAN (e.g., WAN1) as the Interface for packet transmission, you have to specify the way the packet forwarded to. Choose **Force NAT** or **Force Routing**. |
| **Enable Failover** | Click to enable / disable the failover function. |
| **Failover to** | If enabled, it will lead the data passing through specific interface (e.g., WAN/LAN) automatically when the selected interface is down. |
| **Failover to Gateway IP** | Specific gateway is used only when you want to forward the packets to the desired gateway.<br>**Default Gateway** - Usually, Default Gateway is selected in default.<br>**Specific Gateway** - Enter a gateway IP address. |
| **Cancel** | Discard current modification. |
| **Save** | Save the current settings. |

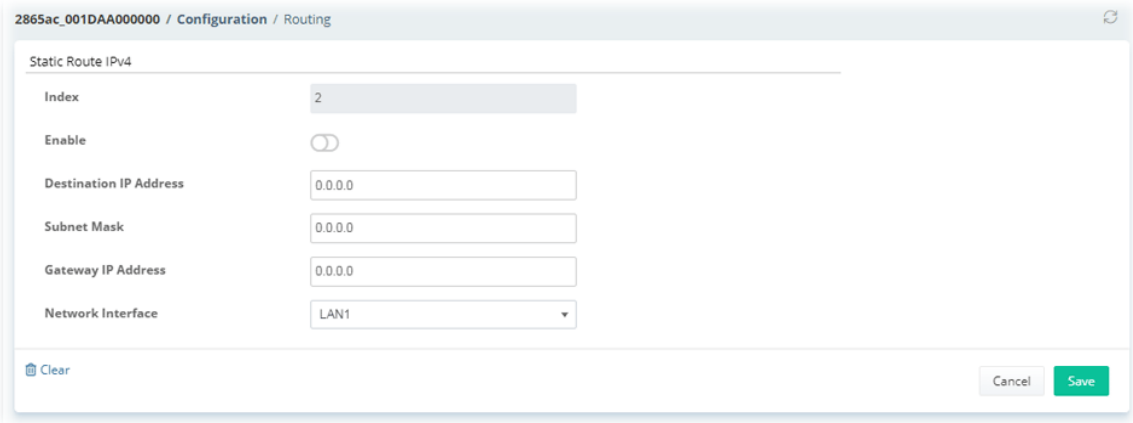
### 9.4.4.2 Static Route IPv4

The router offers IPv4 for you to configure the static route.



| Index | Destination IP Address | Mask | Gateway | Interface | Status |
|---|---|---|---|---|---|
| 1 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | LAN1 | Disable |
| 2 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | LAN1 | Disable |
| 3 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | LAN1 | Disable |
| 4 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | LAN1 | Disable |
| 5 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | LAN1 | Disable |
| 6 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | LAN1 | Disable |
| 7 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | LAN1 | Disable |
| 8 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | LAN1 | Disable |
| 9 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | LAN1 | Disable |
| 10 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | LAN1 | Disable |
| 11 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | LAN1 | Disable |
| 12 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | LAN1 | Disable |
| 13 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | LAN1 | Disable |
| 14 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | LAN1 | Disable |
| 15 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | LAN1 | Disable |
| 16 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | LAN1 | Disable |
| 17 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | LAN1 | Disable |
| 18 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | LAN1 | Disable |
| 19 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | LAN1 | Disable |
| 20 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | LAN1 | Disable |
| 21 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | LAN1 | Disable |

To configure the profile, move the mouse cursor to any entry and click to open the setting page.

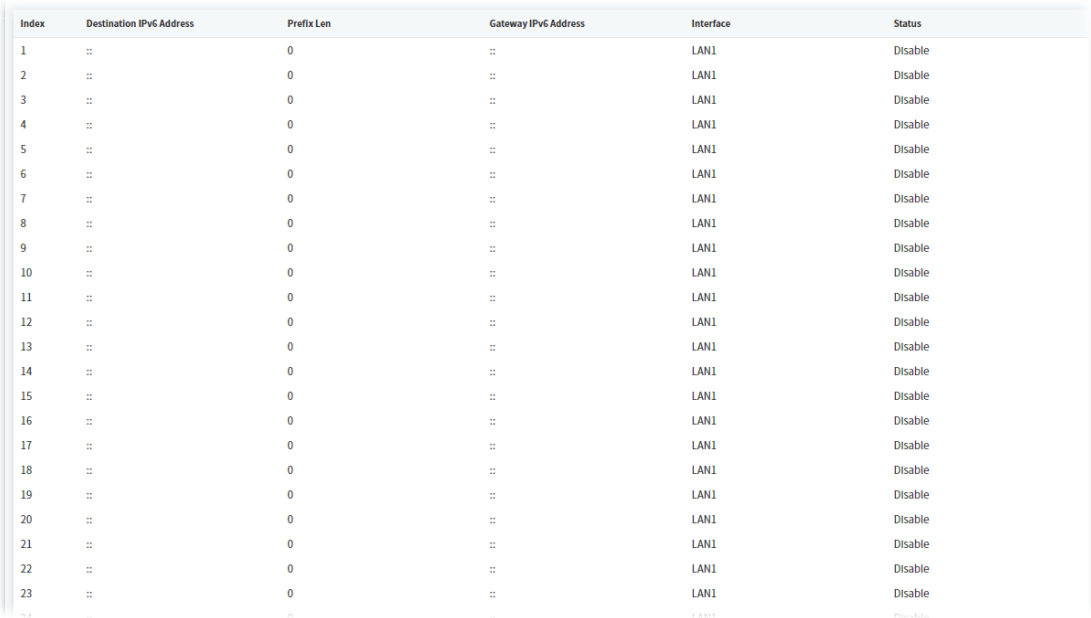



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Index** | Displays the index number of the static route policy. |
| **Enable** | Click to enable or disable the static route policy. |
| **Destination IP Address** | Enter an IP address as the destination of such static route. |
| **Subnet Mask** | Enter the subnet mask for such static route. |
| **Gateway IP Address** | Enter the IP address of the gateway. |
| **Network Interface** | Specify an interface for this static route. |
| **Clear** | Click to return to factory default setting. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

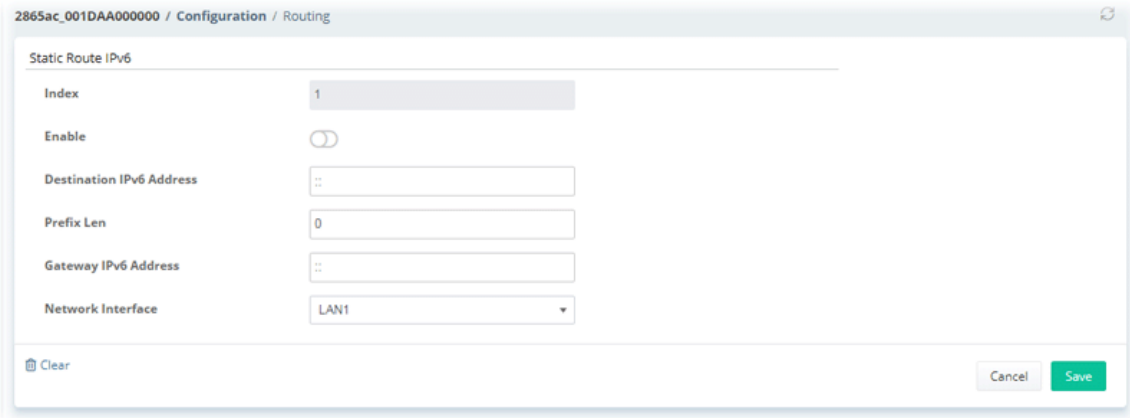
### 9.4.4.3 Static Route IPv6

The router offers IPv6 for you to configure the static route.



| Index | Destination IPv6 Address | Prefix Len | Gateway IPv6 Address | Interface | Status |
|---|---|---|---|---|---|
| 1 | :: | 0 | :: | LAN1 | Disable |
| 2 | :: | 0 | :: | LAN1 | Disable |
| 3 | :: | 0 | :: | LAN1 | Disable |
| 4 | :: | 0 | :: | LAN1 | Disable |
| 5 | :: | 0 | :: | LAN1 | Disable |
| 6 | :: | 0 | :: | LAN1 | Disable |
| 7 | :: | 0 | :: | LAN1 | Disable |
| 8 | :: | 0 | :: | LAN1 | Disable |
| 9 | :: | 0 | :: | LAN1 | Disable |
| 10 | :: | 0 | :: | LAN1 | Disable |
| 11 | :: | 0 | :: | LAN1 | Disable |
| 12 | :: | 0 | :: | LAN1 | Disable |
| 13 | :: | 0 | :: | LAN1 | Disable |
| 14 | :: | 0 | :: | LAN1 | Disable |
| 15 | :: | 0 | :: | LAN1 | Disable |
| 16 | :: | 0 | :: | LAN1 | Disable |
| 17 | :: | 0 | :: | LAN1 | Disable |
| 18 | :: | 0 | :: | LAN1 | Disable |
| 19 | :: | 0 | :: | LAN1 | Disable |
| 20 | :: | 0 | :: | LAN1 | Disable |
| 21 | :: | 0 | :: | LAN1 | Disable |
| 22 | :: | 0 | :: | LAN1 | Disable |
| 23 | :: | 0 | :: | LAN1 | Disable |

To configure the profile, move the mouse cursor to any entry and click to open the setting page.

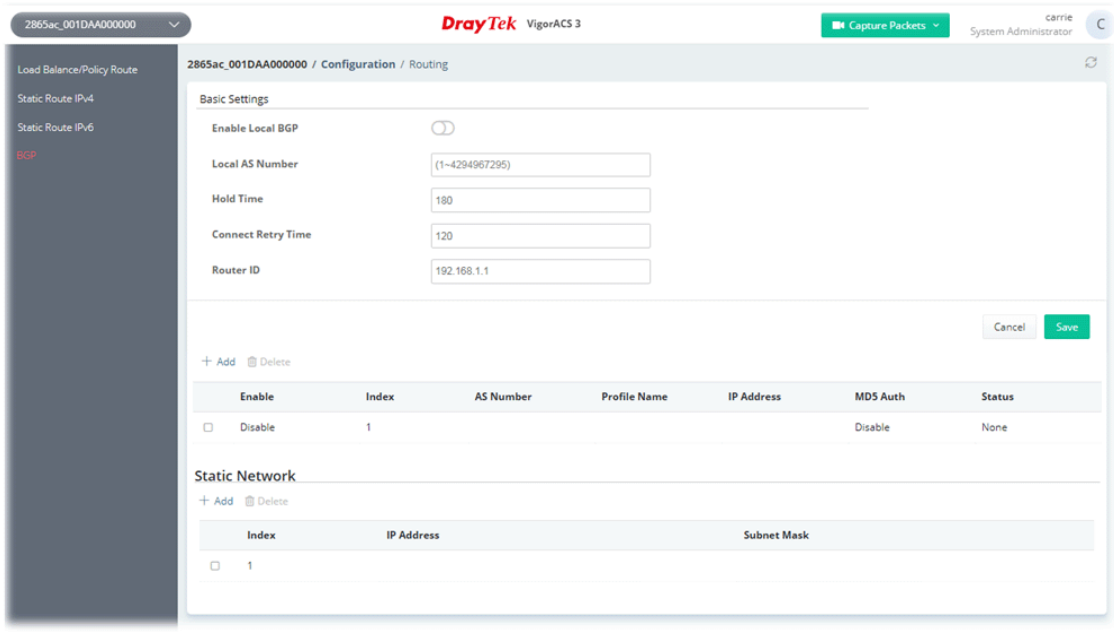



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Index** | Displays the index number of the static route policy. |
| **Enable** | Click to enable or disable the static route policy. |
| **Destination IPv6 Address / Prefix Len** | Enter the IP address with the prefix length for this entry. |
| **Gateway IPv6 Address** | Enter the gateway address for this entry. |
| **Network Interface** | Specify an interface for this static route. |
| **Clear** | Click to return to factory default setting. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

### 9.4.4.4 BGP

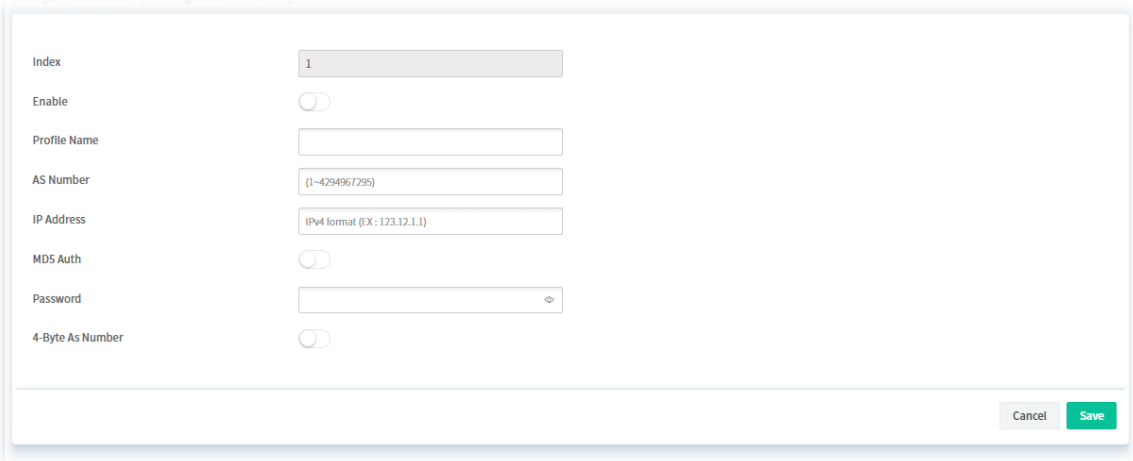
BGP is a standardized protocol designed to exchange routing and reachability information among autonomous systems (AS) on the Internet.




These parameters are explained as follows:

| Item | Description |
|---|---|
| **Enable Local BGP** | Click to enable / disable the BGP function. |
| **Local AS Number** | Enter the value as local AS nubmer. |
| **Hold Time** | Set the time interval (in seconds) to determine the peer is dead when the router is unable to receive any keepalive message from the peer within the time. |
| **Connect Retry Time** | If the router fails to connect to neighboring router, it requires a period of time to reconnect. |
| **Router ID** | Specify the LAN subnet for the router. |
| **Cancel** | Discard current modification. |
| **Save** | Save the current settings. |
| **Basic Settings** | Displays general settings for for local router and neighboring routers.<br>**+Add** - Add a new neighbor profile.<br>**Delete** - Remove a selected neighbor profile.<br>**Enable** - Displays the status of the BGP profile.<br>**Index** - Displays the index number of the BGP profile.<br>**AS Number** - Displays the value of AS number.<br>**Profile Name** - Displays the name of the BGP profile.<br>**IP Address** - Displays the IP address of the BGP profile.<br>**MD5 Auth** - Displays the status (enabled / disabled) of MD5 Auth.<br>**Status** - Display the connection status for local router and neighboring router. |
| **Static Network** | Displays the neighboring routers for exchanging the routing information with the local router.<br>**+Add** - Add a new static network profile by giving IP address and subnet mask.<br>**Delete** - Remove a selected neighbor profile.<br>**Index** - Displays the index number of the BGP profile.<br>**IP Address** - Displays the IP address of the router.<br>**Subnet Mask** - Displays the subnet mask of the router. |
| **Cancel** | Discard current modification. |
| **Save** | Save the current settings. |

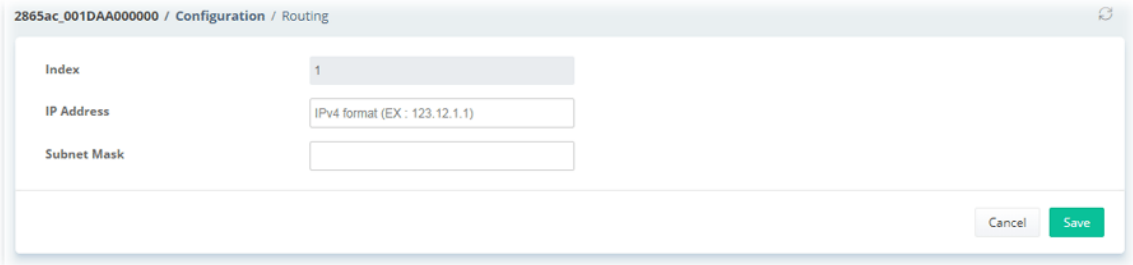
To configure the BGP profile with basic settings, move the mouse cursor to any entry and click to open the setting page.




These parameters are explained as follows:

| Item | Description |
|---|---|
| **Basic Settings** | **Index** - Displays the index number of the profile.<br>**Enable** - Click to enable / disable the profile.<br>**Profile Name** - Enter the name of the profile.<br>**AS Number** - Enter a value for AS number.<br>**IP Address** - Enter the IP address for the profile.<br>**MD5 Auth** - Click to enable / disable the MD5 authentication.<br>**Password** - Enter the password for authentication.<br>**4-Byte As Number** - Click to enable / disable the setting. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

To configure the BGP profile for static network, click **+Add** to open the setting page. Or move the mouse cursor to any existed entry and click to open the setting page.



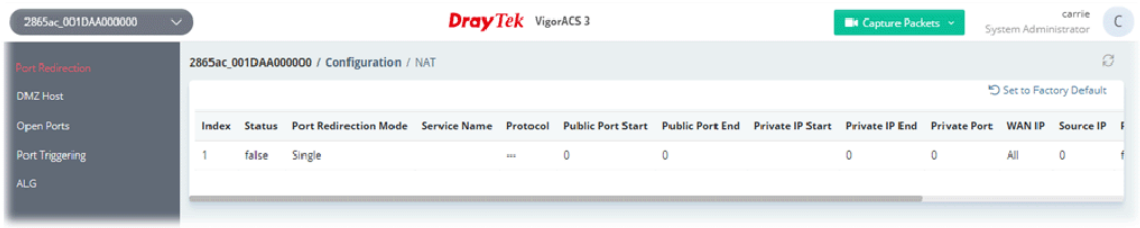

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Static Network** | **Index** - Displays the index number of the profile.<br>**IP Address** - Enter the IP address for a router.<br>**Subnet Mask** - Specify a subnet mask for the IP address. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

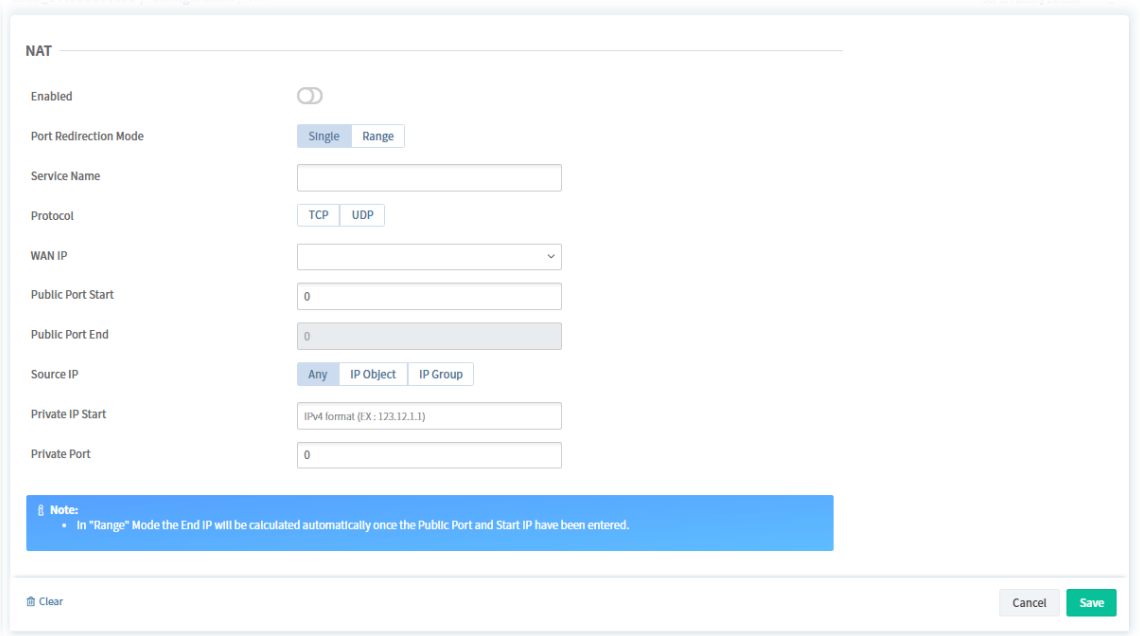
## 9.4.5 NAT

### 9.4.5.1 Port Redirection

This page lists the configured Port Redirection policies coming from Vigor CPE.




To configure the NAT profile, move the mouse cursor to any entry and click to open the setting page.



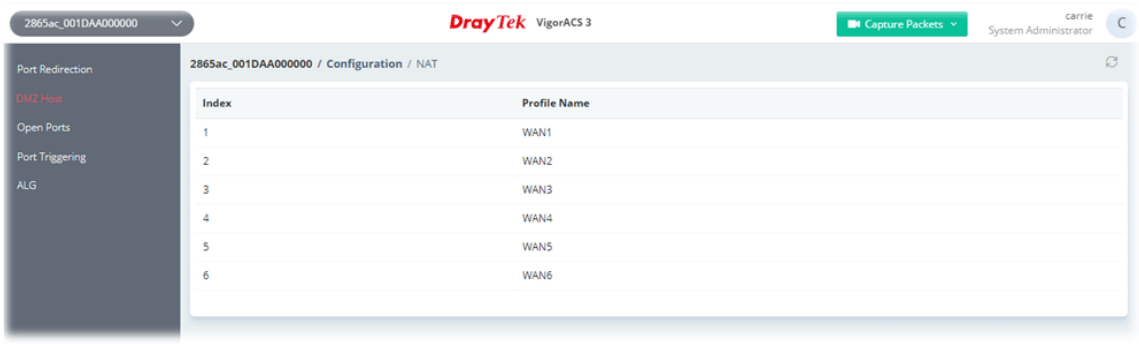

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Enabled** | Click to enable / disable the port redirection profile. |
| **Port Redirection Mode** | Two options (Single and Range) are provided here for you to choose.<br>**Single / Range** - To set a range for the specific service, select **Range**. Otherwise, select **Single**. |
| **Service Name** | Enter the description of the specific network service. |
| **Protocol** | **TCP/UDP** - Select the transport layer protocol (TCP or UDP). |
| **WAN IP** | Select the WAN interface used for port redirection. The default setting is **All** which means all the incoming data from any port will be redirected to specified range of IP address and port. |
| **Public Port Start / End** | Specify which port can be redirected to the specified **Private IP and Port** of the internal host. If you choose **Range** as the port redirection mode, you will need to enter the required number on the first box (as the starting port) and the second box (as the ending port). |
| **Source IP** | Select the source IP mode.<br>**Any** - It means any IP address.<br>**IP Object** - |

| | |
|---|---|
| | ● **IP Object** - Specify an IP object profile.<br>**IP Group** -<br>● **IP Group** - Specify an IP group profile. |
| **Private IP Start / End** | Specify the private IP address of the internal host providing the service. If you choose **Range** as the port redirection mode, you will see two boxes on this field. Type a complete IP address in the first box (as the starting point). The second one will be assigned automatically later. |
| **Private Port** | Specify the private port number of the service offered by the internal host. |
| **Clear** | Click to return to factory default setting. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

### 9.4.5.2 DMZ Host

**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.

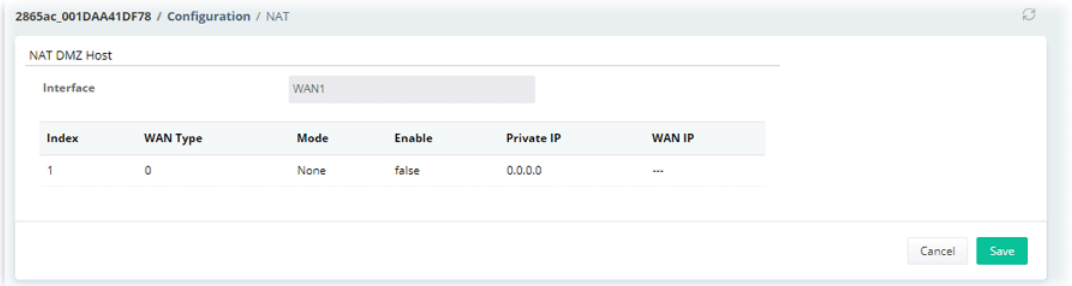



These parameters are explained as follows:

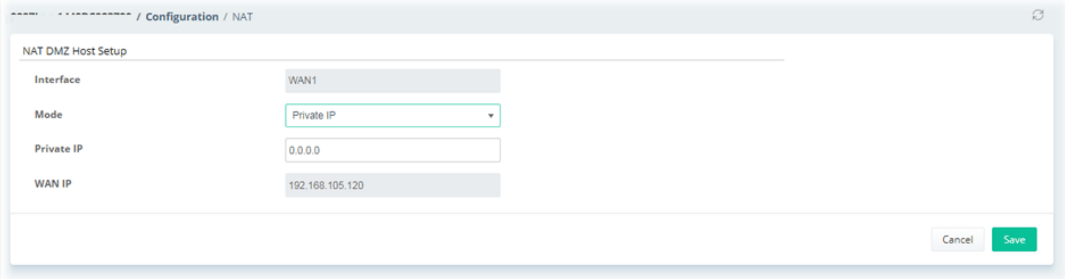
| Item | Description |
|---|---|
| **Index** | Displays the index number of the DMZ host profiles. |
| **Profile Name** | Displays the interface of the DMZ host profile. |

To configure the DMZ host profile:

1. Move the mouse cursor to any entry (1 to 6) and click to open the following page.




2. Click the index number of the profile to open the settings page.




These parameters are explained as follows:

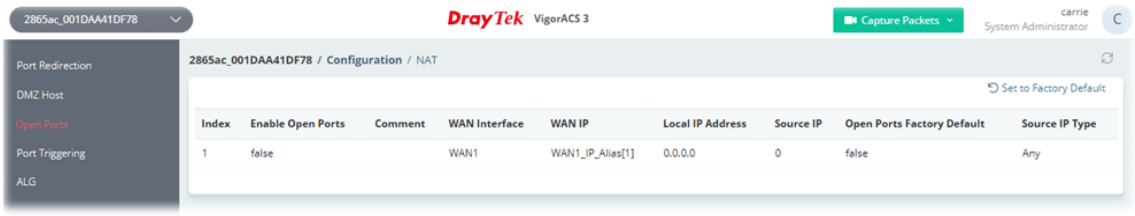
| Item | Description |
|---|---|
| **Interface** | Displays the name of the DMZ host profiles. |
| **Mode** | Select a method to enter the IP address.<br>● **Private IP**<br>● **None** |
| **Private** | Enter the private IP address of the DMZ host. |
| **WAN IP** | Displays the WAN IP alias for this interface. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

3. After finished the configuration, click **Save** to save the changes.

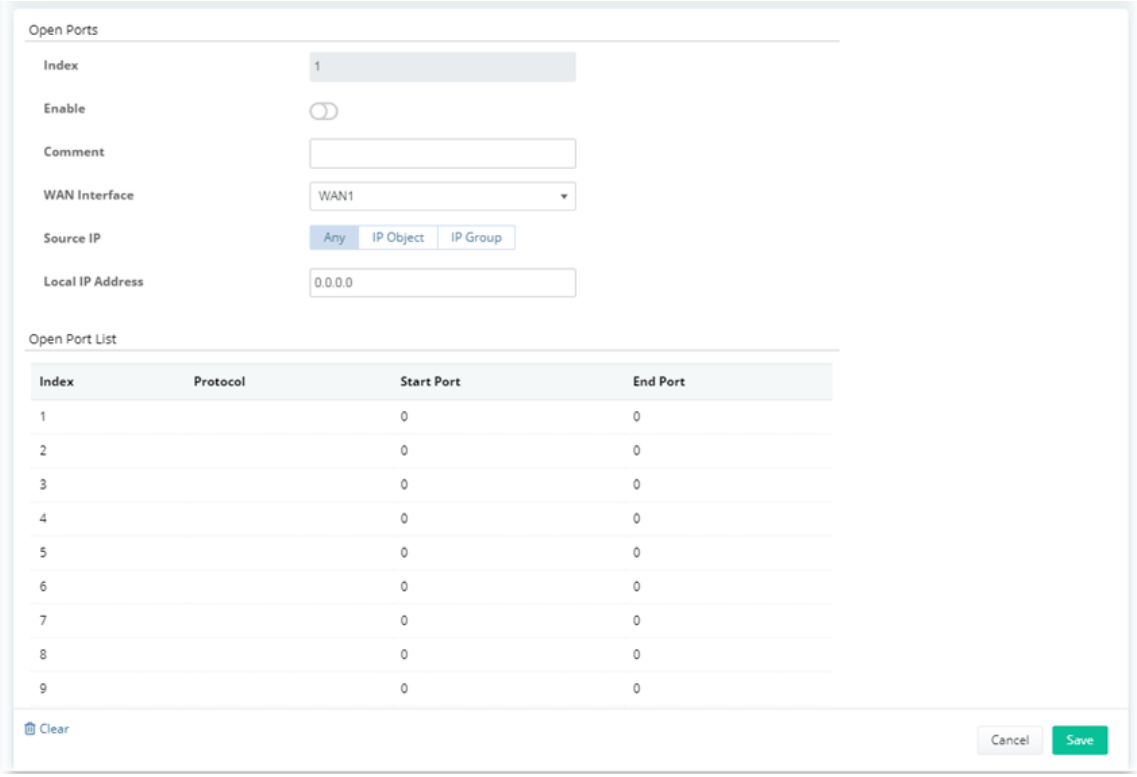
### 9.4.5.3 Open Ports

This page lists the configured Open Ports policies coming from Vigor CPE.

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




To configure the open port profile, move the mouse cursor to any entry and click to open the setting page.

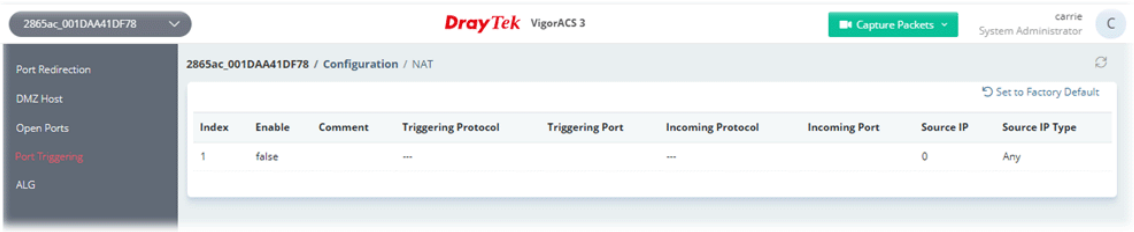



These parameters are explained as follows:

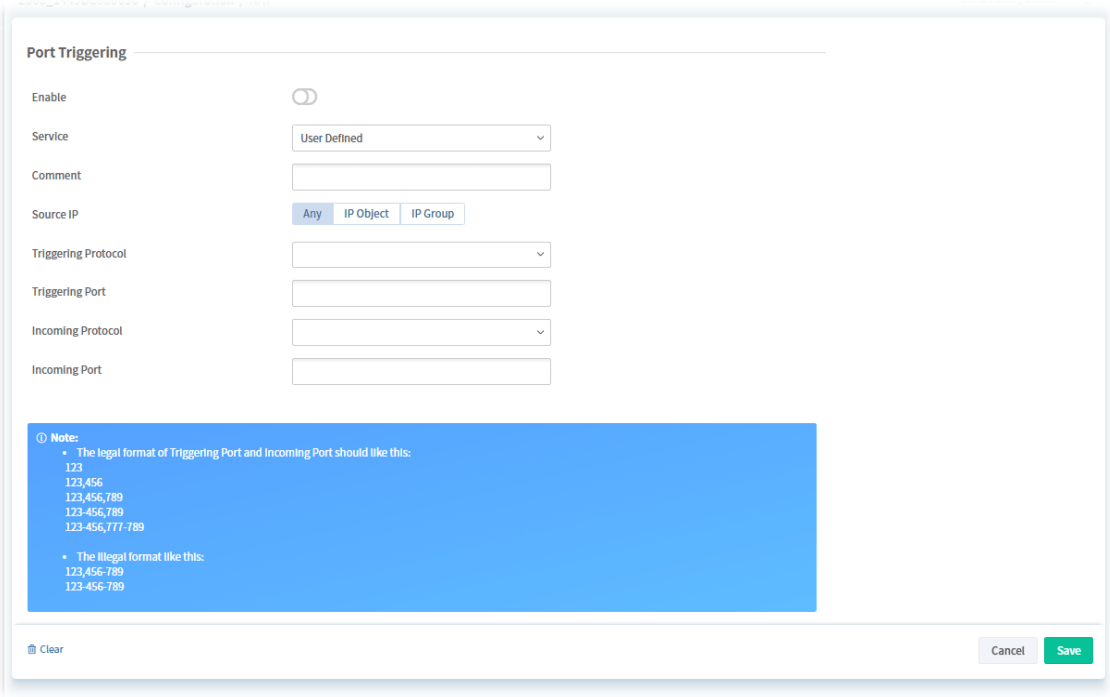
| Item | Description |
|---|---|
| | **Open Ports** |
| **Index** | Displays the index number of the Open Port profile. |
| **Enable** | Click to enable / disable the Open Port profile. |
| **Comment** | Enter the description for the Open Port profile. |
| **WAN Interface** | Choose a WAN interface that will be used for this entry. |
| **Source IP** | Select the source IP mode.<br>**Any** - It means any IP address.<br>**IP Object** -<br>● **IP Object** - Specify an IP object profile.<br>**IP Group** -<br>● **IP Group** - Specify an IP group profile. |
| **Local IP Address** | Enter the private IP address of the local host. |
| **Open Port List** | It displays 1 to 10 open port profiles.<br>Click any one of the index numbers to configure the settings for the selected open port profile. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

### 9.4.5.4 Port Triggering

Port Triggering is a variation of open ports function. This page lists the configured Port Triggering policies coming from Vigor CPE.




To configure the port triggering profile, move the mouse cursor to any entry and click to open the setting page.



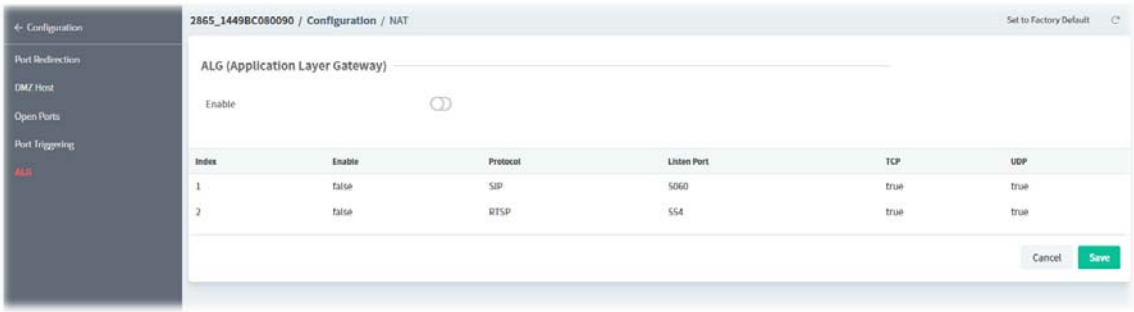

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Click to enable / disable the Port Triggering profile. |
| **Service** | Choose the service type to apply for this triggering profile. |
| **Comment** | Enter the text to memorize the application of this rule. |
| **Source IP** | Select the source IP mode.<br>**Any** - It means any IP address.<br>**IP Object**<br>● **IP Object** - Specify an IP object profile.<br>**IP Group**<br>● **IP Group** - Specify an IP group profile. |
| **Triggering Protocol** | Select the protocol (TCP, UDP or TCP/UDP) for such triggering profile. |
| **Incoming Protocol** | When the triggering packets received, it is expected the incoming packets will use the selected protocol. Select the protocol (TCP, UDP or TCP/UDP) for the incoming data of such triggering profile. |

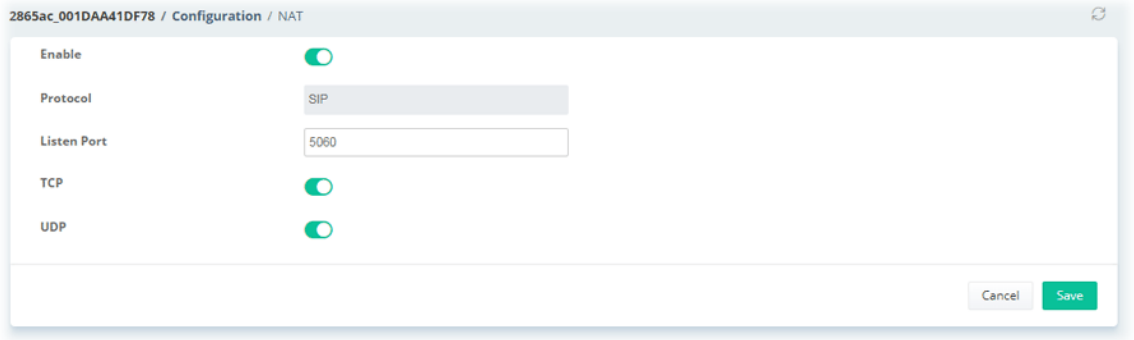
| | |
|---|---|
| **Incoming Port** | Enter the port or port range for the incoming packets. |
| **Clear** | Click to return to factory default setting. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

### 9.4.5.5 ALG

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 voice and video.




To configure the ALG profile, move the mouse cursor to any entry and click to open the setting page.

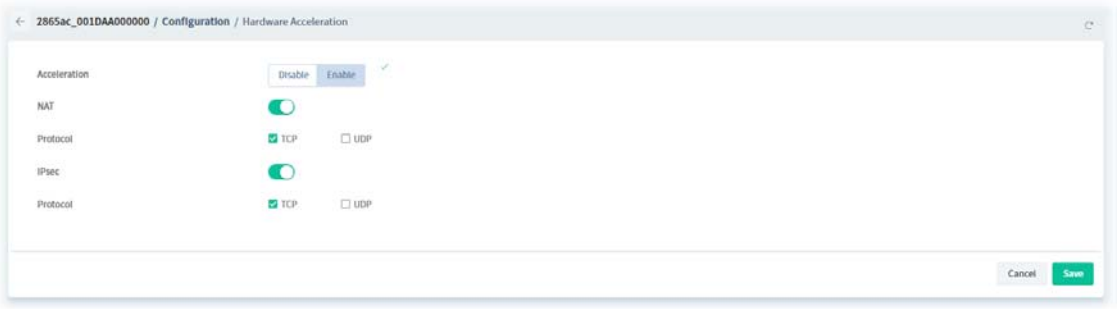



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Click to enable / disable the ALG profile. |
| **Protocol** | Displays the type (SIP, RTSP) of ALG. |
| **Listen Port** | Enter a port number for SIP or RTSP protocol. |
| **TCP/UDP** | Click to enable/disable the TCP/UDP. If enabled, it will make correspond protocol message packet from TCP/UDP transmit and receive via NAT. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

### 9.4.6 Hardware Acceleration

When the data traffic is heavy and data transmission is getting slowly and slowly, you can configure this page to accelerate the data streaming by hardware itself.



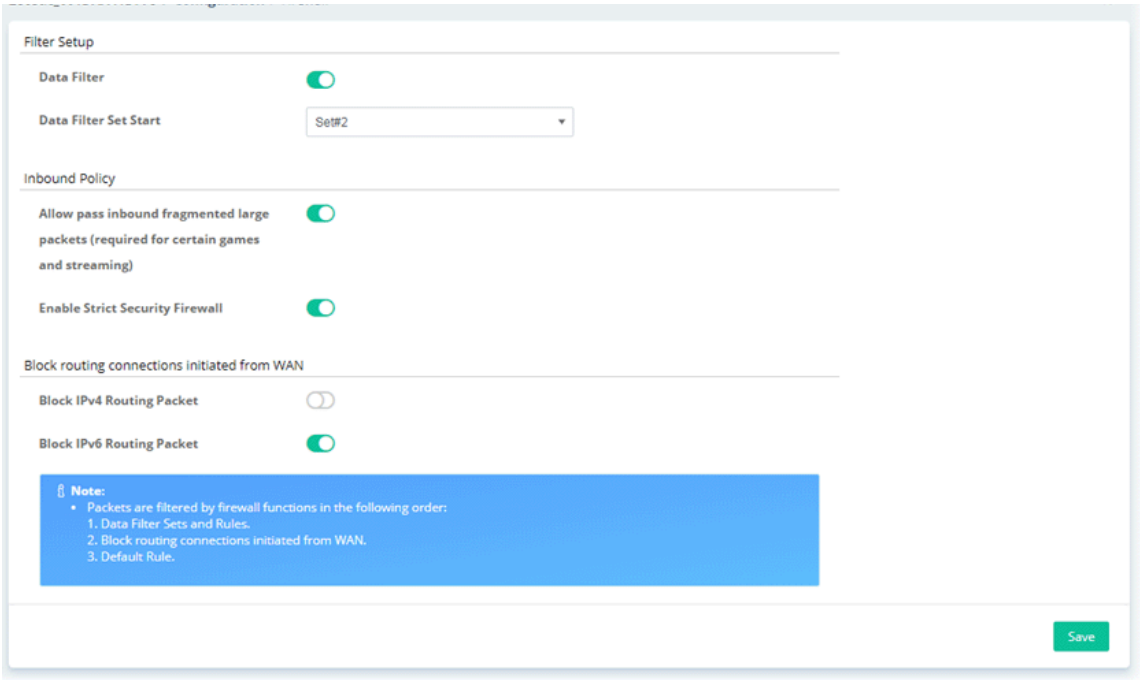

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Acceleration** | **Disable –** The default setting.<br>**Enable** - The sessions with the heaviest loading and the lower latency traffic will be added into PPA. |
| **NAT** | Click to enable / disable NAT setting. |
| **Protocol** | There are two types supported by this function, TCP and UDP. |
| **IPsec** | Click to enable / disable IPsec setting. |
| **Protocol** | There are two types supported by this function, TCP and UDP. |
| **Cancel** | Discard current modification. |
| **Save** | Save the current settings. |

## 9.4.7 Firewall

### 9.4.7.1 General Setup

It allows you to enable / disable Data Filter, determine general rule for filtering the incoming and outgoing data.

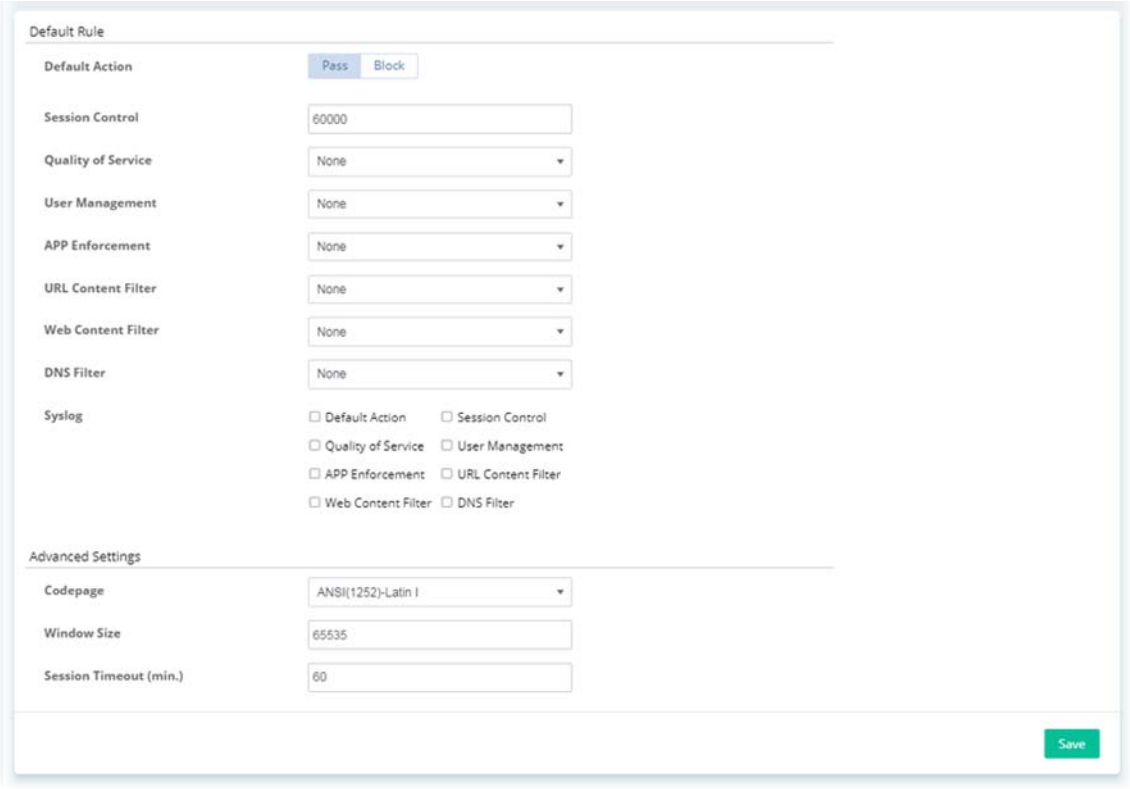



These parameters are explained as follows:

| Item | Description |
|---|---|
| | **Filter Setup** |
| **Data Filter** | Click to enable / disable the function.<br>If enabled, choose a Start Filter Set. |
| **Data Filter Set Start** | Choose a Start Filter Set. |
| | **Inbound Policy** |
| **Allow pass inbound fragmented large...** | Click to enable / disable the function.<br>Certain games and video streaming service use fragmented UDP packets to transfer data. Enabling this option allows these applications to function properly. |
| **Enable Strict Security Firewall** | Click to enable / disable the function.<br>If this option and the Web Content Filter (WCF) are both enabled, web traffic will be blocked if the WCF server fails to respond to lookup requests. |
| | **Block routing connections initiated from WAN** |
| **Block IPv4 Routing Packet** | For LAN hosts receiving WAN IPv4 addresses using the IP routed subnet, enable this option to prevent WAN hosts from connecting to LAN hosts. This option has no effect on LAN hosts on private LAN subnets. |
| **Block IPv6 Routing Packet** | 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. Enable this option to block WAN hosts from connecting to LAN hosts using IPv6. |
| **Save** | Save the current settings. |

### 9.4.7.2 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.



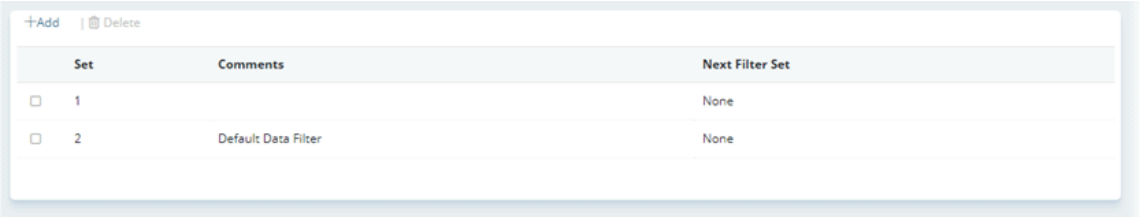

These parameters are explained as follows:

| Item | Description |
|---|---|
| | **Default Rule** |
| **Default Action** | Select **Pass** or **Block** for the packets that do not match with the filter rules. When the setting is Block, all other fields on the page are disabled because they are not applicable. |
| **Session Control** | The current number of sessions is shown before the slash, followed by the maximum number of concurrent sessions allowed, which is configurable. |
| **Quality of Service** | Select one of the QoS rules to be applied as firewall rule. For detailed information of setting QoS, please refer to the related section later. |
| **User Management** | This setting is only available when **Rule-Based** is selected in **User Management>>General Setup**. The default firewall rule will be applied to the selected user or user group. |
| **APP Enforcement** | Select an APP Enforcement profile for application blocking, or None to disable APP Enforcement for the Default Rule. |
| **URL Content Filter** | Select a URL Content Filter profile to be used, or None to disable URL Content Filter for the Default Rule. |
| **Web Content Filter** | Select a Web Content Filter profile to be used, or None to disable Web Content Filter for the Default Rule. |
| **DNS Filter** | Select the DNS Filter profile to be used, or None to disable DNS Filter for the Default Rule. |
| **Syslog** | Select the items to send and store the records to Syslog. |

| | Advanced Settings |
|---|---|
| **Codepage** | Selecting the appropriate codepage can increase the accuracy of the URL Content Filter. The default value is ANSI 1252 Latin I. If the setting is None, no decoding of URL will be performed. |
| **Window Size** | Sets the TCP window size as described in RFC 1323. Valid values are from 0 to 65535. |
| **Session Timeout** | Sets the timeout sessions are allowed to idle before they are removed from the system. |
| **Save** | Save the current settings. |

### 9.4.7.3 Filter Rules

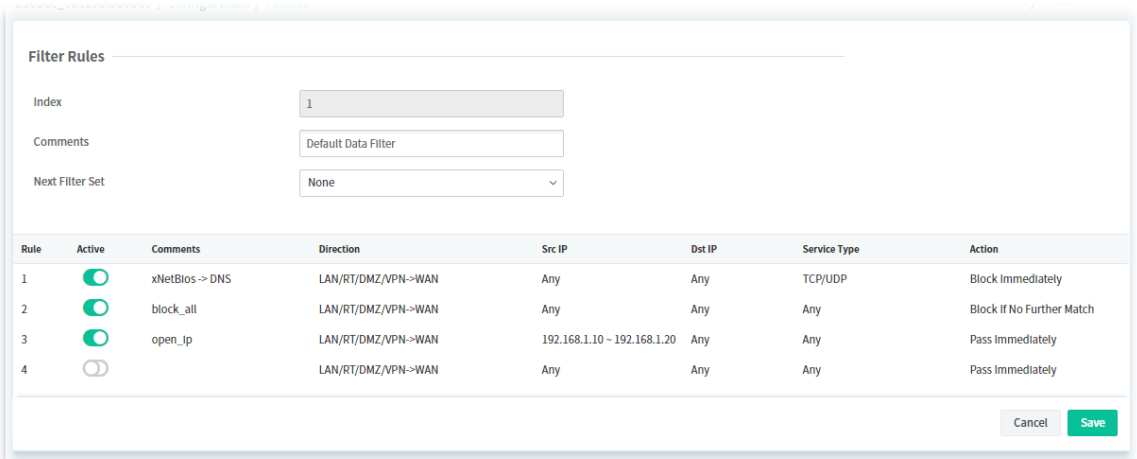
This page displays the filter rule profile and allows to create new filter rule profile(s).




These parameters are explained as follows:

| Item | Description |
|---|---|
| **+Add** | Click to add a new filter rule set. |
| **Delete** | Click to remove the selected filter rule. |
| **Set** | Displays the number of filter set. |
| **Comments** | Displays the comment of the filter rule. |
| **Next Filter Set** | Displays the name of next filter set. **None** means no filter set is specified for current filter set. |

To configure the filter rule set profile, move the mouse cursor to any entry and click to open the setting page. Or, click **+Add** to create a new filter rule profile.

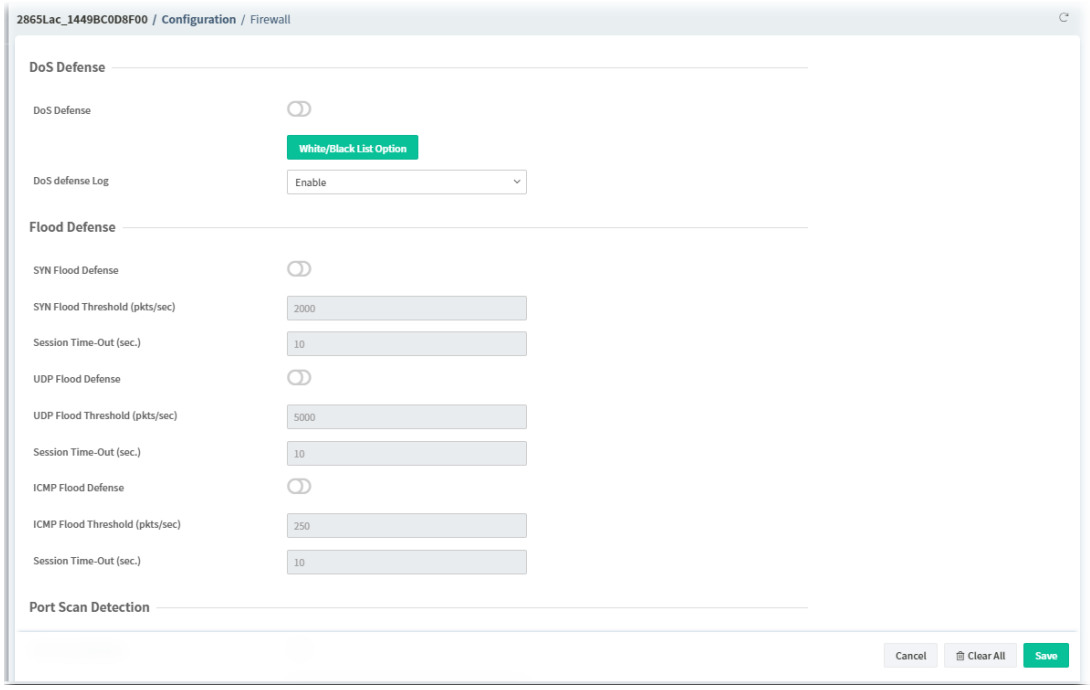



These parameters are explained as follows:

| Item | Description |
|---|---|
| | **Filter Rules** |

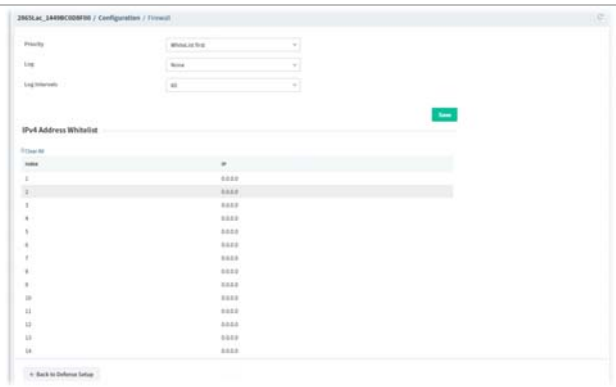
| | |
|---|---|
| **Index** | Displays the index number of the filter rule set.<br>Each filter set contains up to 7 rules. |
| **Comments** | Enter a comment to identify the filter rule. |
| **Next Filter Set** | Select the filter set for the firewall to process after the current filter set |
| | **Table** |
| **Rule** | Displays the index number of the filter rule. |
| **Active** | Click to enabled or disabled the filter rule. |
| **Comments** | Optional comment entered in the settings page to identify the rule. |
| **Direction** | Displays the direction of packet. |
| **Src IP** | Displays the IP address of source /destination. |
| **Dst IP** | Displays the type and port number of the packet. |
| **Service Type** | Displays the type and port number of the packet. |
| **Action** | Displays the packets to be passed /blocked. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

### 9.4.7.4 DoS Defense




These parameters are explained as follows:

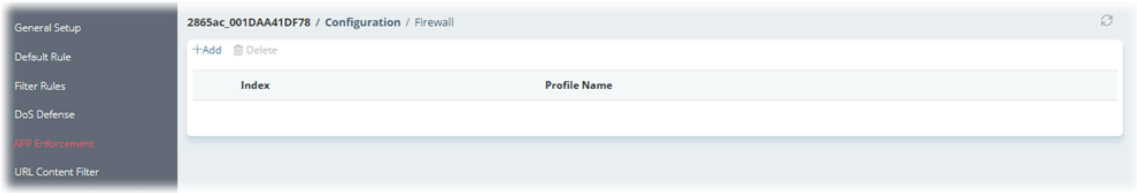
| Item | Description |
|---|---|
| | **DoS Defense** |
| **DoS Defense** | Click to enable / disable the DoS Defense. |
| **White/Black List Options** | Click to set white or black list. |

| | |
|---|---|
| |  |
| **DoS defense Log** | Click to enable / disable the function of recording DoS defense log onto Syslog. |
| | **Flood Defense** |
| **SYN Flood Defense** | Click to enable / disable the SYN flood defense.<br>If enabled,<br>● **SYN Flood Threshold** - Set a threshold value. The default values of threshold is 2000 packets per second.<br>● **Session Time-Out** - Set a threshold value. The default value of timeout is 10 seconds. |
| **UDP Flood Defense** | Click to enable / disable the UDP flood defense.<br>If enabled,<br>● **UDP Flood Threshold -** Set a threshold value. The default values of threshold is 2000 packets per second.<br>● **Session Time-Out** - Set a threshold value. The default value of timeout is 10 seconds. |
| **ICMP Flood Defense** | Click to enable / disable the ICMP flood defense.<br>If enabled,<br>● **ICMP Flood Threshold** - Set a threshold value. The default values of threshold is 250 packets per second.<br>● **Session Time-Out** - Set a threshold value. The default value of timeout is 10 seconds. |
| | **Port Scan Detection** |
| **Port Scan Detection** | Click to enable / disable the port scan defense.<br>If enabled,<br>● **Port Scan Threshold -** Set a threshold value. The default values of threshold is 2000 packets per second. |
| | **Others** |
| **Select All** | Click to select and enable all items under Others. |
| | **Spoofing Defense** |
| **ARP Spoofing Defense Log** | Click to enable / disable the store the ARP log to Syslog. |
| **ARP Spoofing Defense** | There are two types for spoofing defense**.**<br>● **Block ARP replies with inconsistent source MAC address**<br>● **Block ARP replies with inconsistent**<br>● **Decline VRRP MAC into ARP table** |

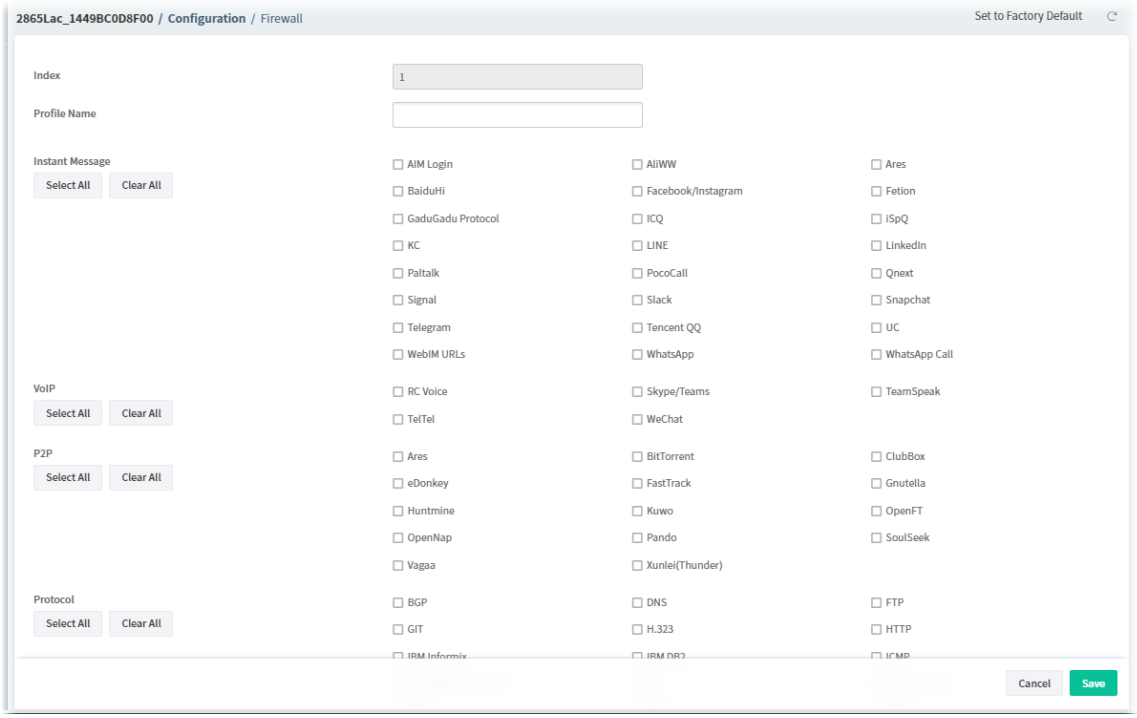
| | |
|---|---|
| **IP Spoofing Defense** | There are two types for spoofing defense**.**<br>● **Block IP packet from WAN with Inconsistent source IP addresses**<br>● **Block IP replies from LAN with Inconsistent source IP addresses** |
| **Cancel** | Discard current modification and keep current configuration. |
| **Clear All** | Discard current modification and return to factory default setting. |
| **Save** | Save the current settings. |

### 9.4.7.5 APP Enforcement

The APP Enforcement Filter can be used to prevent users from using undesirable or inappropriate network applications such as online chat and peer-to-peer programs. The filter works by detecting and blocking network traffic of applications by means of traffic patterns.




To create a new profile, click **+Add** to open the following page.

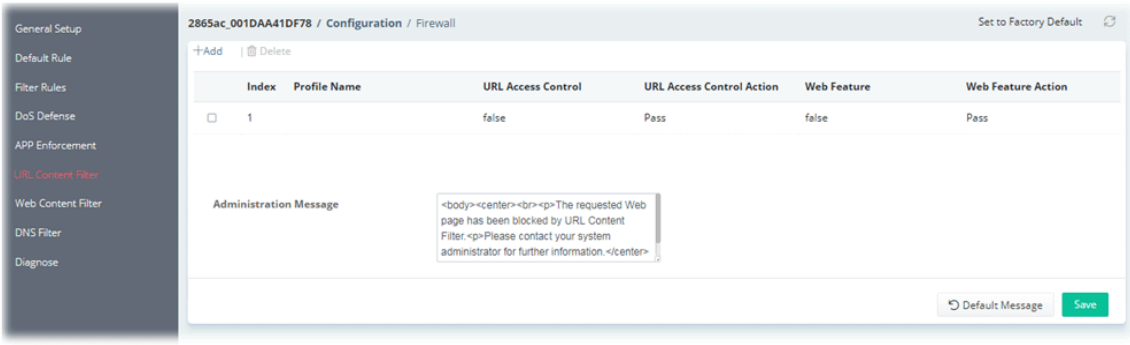



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Index** | Displays the index number of the profile. |
| **Profile Name** | Displays the name of the profile. |
| **Select All** | Click to select all of the items on this page. |
| **Clear All** | Click to deselect all selected items. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings. |

### 9.4.7.6 URL Content Filter

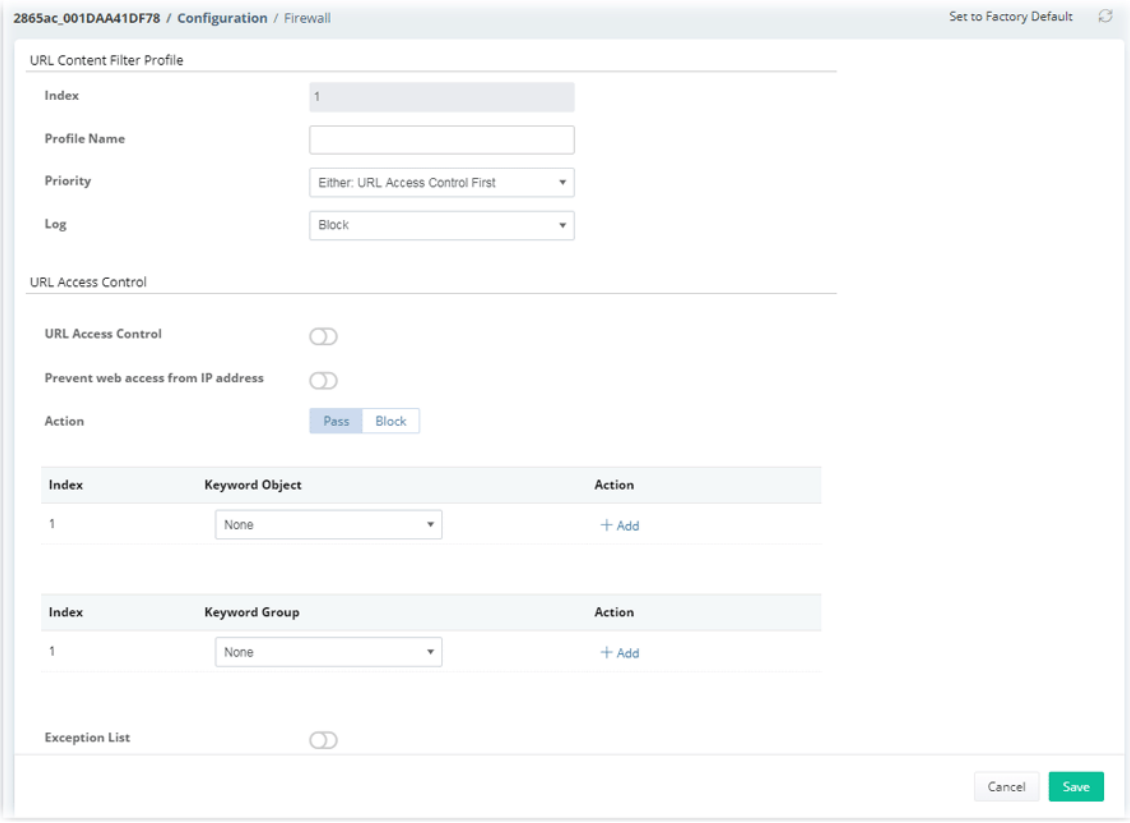
The URL Content Filter scans URL strings in HTTP requests for predefined keywords to restrict browsing activities.




These parameters are explained as follows:

| Item | Description |
|---|---|
| **+Add** | Click to create a new UCF profile. |
| **Delete** | Click to remove the selected UCF profile. |
| **Default Message** | Click to reset the administration message to the factory default. |
| **Save** | Save the current settings. |

To create a new UCF profile, click **+Add** to open the following page.



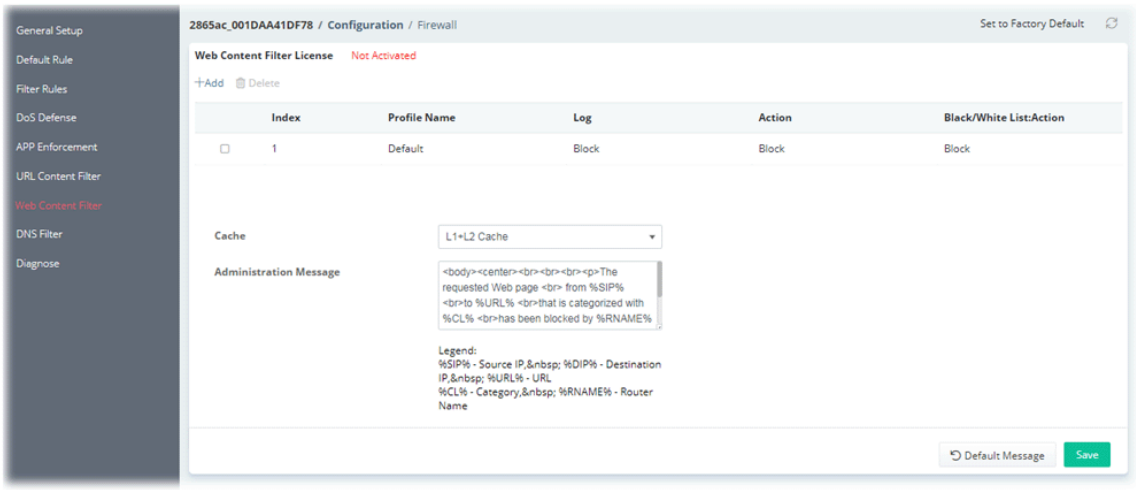

| Item | Description |
|---|---|
| | **URL Content Filter Profile** |
| **Index** | Displays the index number of the UCF profile. |

| | |
|---|---|
| **Profile Name** | Displays the name of the UCF profile. |
| **Priority** | Select the order of evaluation of URL Access Control and Web Feature. |
| **Log** | Select the access attempts (None, Pass, Block or All) to be recorded on Syslog. |
| | **URL Access Control** |
| **URL Access Control** | Click to enable or disable the URL access control. |
| **Prevent web access from IP Address** | Click to enable or disable the function of preventing users from circumventing URL Access Control. |
| **Action** | This setting is enabled only when Priority is set to Either: URL Access Control First or Either: Web Feature First.<br>**Pass -** Allows access to web pages with URLs containing keywords that are in the selected keyword groups or objects. Access to other URLs is blocked.<br>**Block -** Blocks access to web pages with URLs containing keywords that are in the selected keyword groups or objects. Access to other URLs is allowed. |
| **Keyword Object Table** | **Index -** Displays the index number of keyword object profile.<br>**Keyword Object -** Displays the name of the keyword object profile.<br>**Action - +Add -** Click to add a new entry to specify a keyword object profile. |
| **Keyword Group Table** | **Index -** Displays the index number of keyword group profile.<br>**Keyword Group -** Displays the name of the keyword group profile.<br>**Action (+Add) -** Click to add a new entry to specify a keyword group profile. |
| **Exception List** | It is available when **URL Access Control** is enabled.<br>**Index** - Displays the index number of exception object profile.<br>**Exception Keyword Object /Group** - Displays the name of the exception keyword object/group profile.<br>**Action (+Add) -** Click to add a new entry to specify an exception keyword object / group profile. |
| | **Web Feature** |
| **Web Feature Restriction** | Click to enable or disable the web feature restriction function. |
| **Action** | **Pass -** Allows access to web pages with URLs containing keywords that are in the selected keyword groups or objects.<br>**Block -** Blocks access to web pages with URLs containing keywords that are in the selected keyword groups or objects. |
| **File Extension** | Choose one of the profiles for passing or blocking the file downloading. |
| **Cookie, Proxy, Upload** | Click to enable or disable cookie function.<br>If enabled, it can block cookies from Internet websites. |
| **Proxy** | Click to enable or disable proxy function.<br>If enabled, it can block web proxy servers that relay HTTP traffic. |
| **Upload** | Click to enable or disable upload function.<br>If enabled, it can block HTTP uploads from the LAN to the Internet. |
| **Cancel** | Discard current modification and return to previous page. |

| | |
|---|---|
| **Save** | Save the current settings and return to previous page. |

### 9.4.7.7 Web Content Filter

Users can also be prevented from browsing certain types of websites by using the Web Content Filter. This filter classifies website domain names into different categories, which can be selectively blocked.

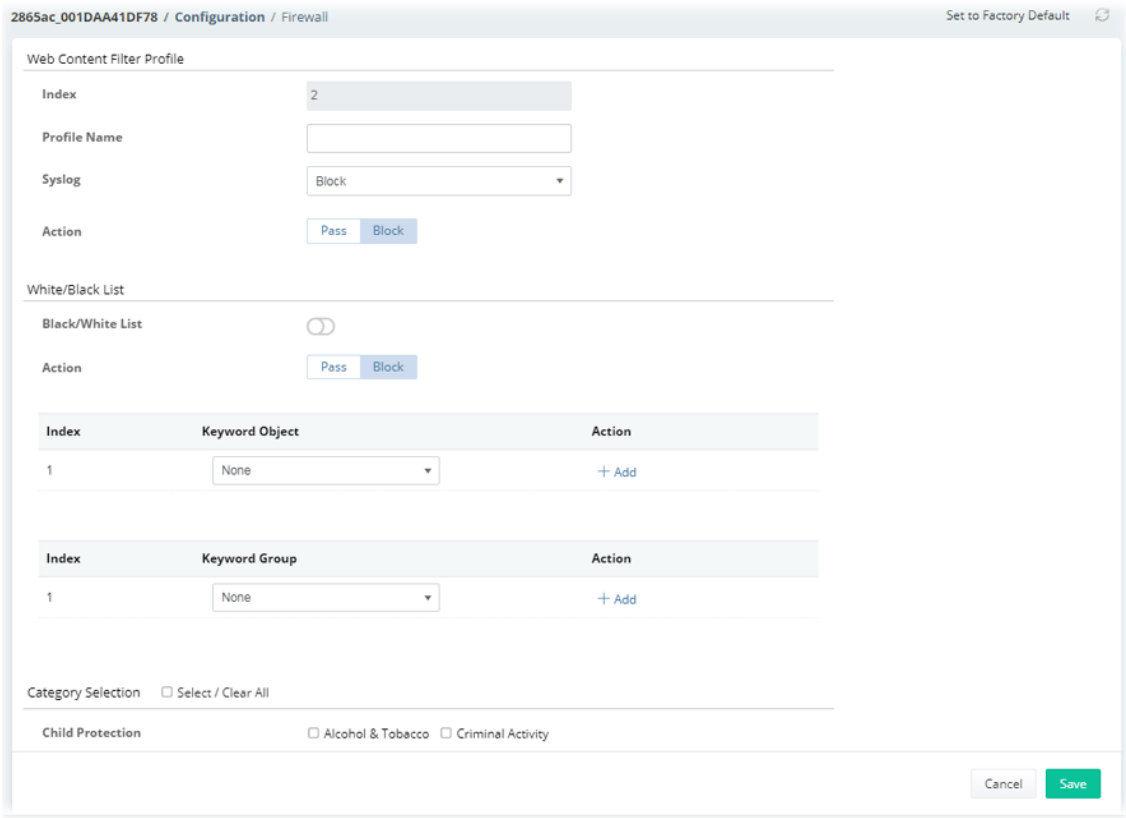



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Set to Factory Default** | Clear all profile settings. |
| **+Add** | Click to create a new WCF profile. |
| **Delete** | Click to remove the selected WCF profile. |
| **Index** | Displays the index number of the WCF profile. |
| **Profile Name** | Displays the name of the WCF profile. |
| **Log** | Displays the type (Pass or Block or All) of the log to be recorded. |
| **Action** | Displays the type (Pass or Block) of the action selected. |
| **Black/White List** | Displays the action to be taken when a WCF matches keyword group and object selections. |
| **Cache** | **None** – The router verifies every HTTP URL requested by communicating with the WCF server on the Internet.<br>**L1** – The router caches the HTTP URLs that have been checked against the WCF server. URLs will be looked up in the L1 cache before reaching out to the WCF server. When the cache is full, the oldest entry will be deleted to accommodate new URLs.<br>**L2** – After a URL has been checked and found to pass WCF, the source and destination IPs are cached for about 1 second in the L2 cache. This is to allow a webpage to be loaded without further verifying the same URLs against the L1 cache or the WCF server.<br>**L1+L2 Cache** – The router will utilize both L1 and L2 caches. |
| **Administration Message** | The message to be displayed in the browser when access to a website has been blocked. A custom message can be entered with HTML formatting in the text box. |
| **Default Message** | Click to reset the administration message to the factory default. |

| | |
|---|---|
| **Save** | Save the current settings. |

To create a new WCF profile, click **+Add** to open the following page.

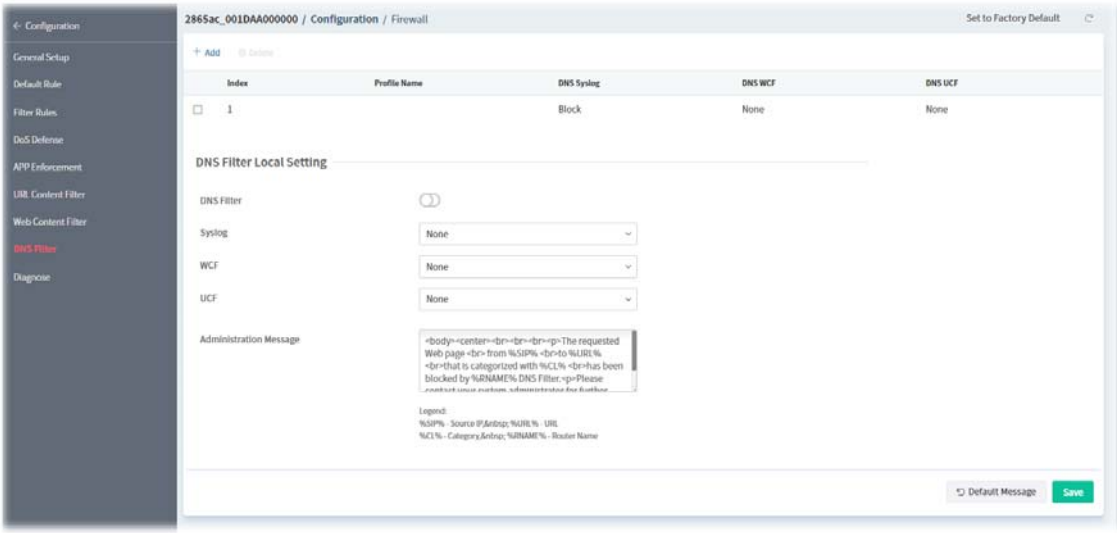



| Item | Description |
|---|---|
| | **Web Content Filter Profile** |
| **Index** | Displays the index number of the WCF profile. |
| **Profile Name** | Displays the name of the WCF profile. |
| **Syslog** | Displays the type (Pass or Block or All) of the log to be recorded. |
| **Action** | **Pass -** Only passed access attempts will be recorded in Syslog.<br>**Block -** Only blocked access attempts will be recorded in Syslog. |
| | **White/Black List** |
| **Black/White List** | Click to enable or disable the function of Black/White List. Keyword objects and groups can be applied to the URL to override WCF category filtering. |
| **Action** | Action to take when a URL matches keyword group and object selections.<br>**Pass -** Allow access to the URL.<br>**Block -** Disallow access to the URL. |
| **Keyword Object Table** | **Index -** Displays the index number of keyword object profile.<br>**Keyword Object -** Displays the name of the keyword object profile.<br>**Action - +Add -** Click to add a new entry to specify a keyword object profile. |
| **Keyword Group Table** | **Index -** Displays the index number of keyword group profile.<br>**Keyword Group -** Displays the name of the keyword group profile.<br>**Action (+Add) -** Click to add a new entry to specify a keyword group |

| | |
|---|---|
| | profile. |
| | **Category Selection** |
| **Select/Clear All** | Click to select or deselect all items under Category Selection. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

### 9.4.7.8 DNS Filter

DNS Filter blocks or allows traffic to the WAN by intercepting DNS queries, and applying UCF and WCF rules to hostnames.

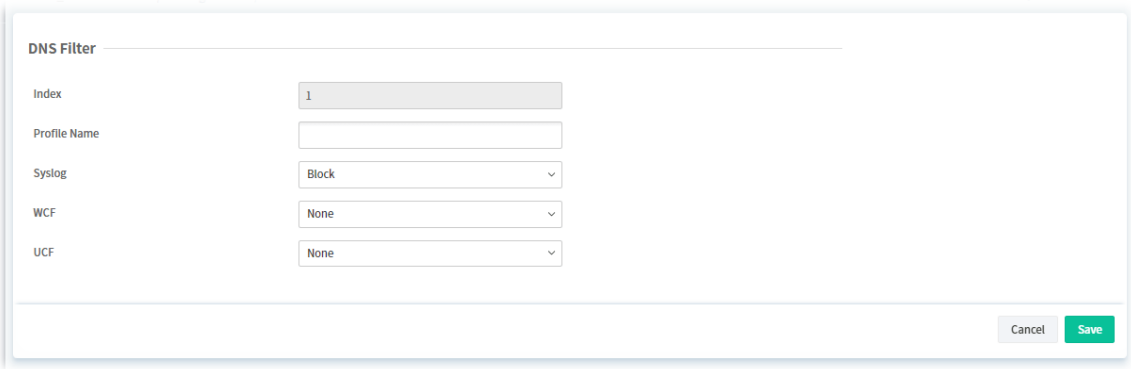



These parameters are explained as follows:

| Item | Description |
|---|---|
| **+Add** | Click to add a new DNS filter profile. |
| **Delete** | Click to remove the selected DNS filter profile. |
| **Index** | Displays the index number of the DNS filter profile. |
| **Profile Name** | Displays the name of the DNS filter profile. |
| **DNS Syslog** | Displays the filtering type (Block, Pass, All or None) of the DNS syslog. |
| **DNS WCF** | Displays the name of the WCF profile. |
| **DNS UCF** | Displays the name of the UCF profile. |
| | **DNS Filter Local Setting** |
| **DNS Filter** | Click to enable / disable the DNS filter function. |
| **Syslog** | Select the filtering type (Block, Pass, All or None) of the DNS syslog. |
| **WCF** | Select a WCF profile. |
| **UCF** | Select a UCF profile. |
| **Administration Message** | The message to be displayed in the browser when access to a website has been blocked. A custom message can be entered with HTML formatting in the text box. |
| **Default Message** | Click to reset the administration message to the factory default. |

| | |
|---|---|
| **Save** | Save the current settings. |

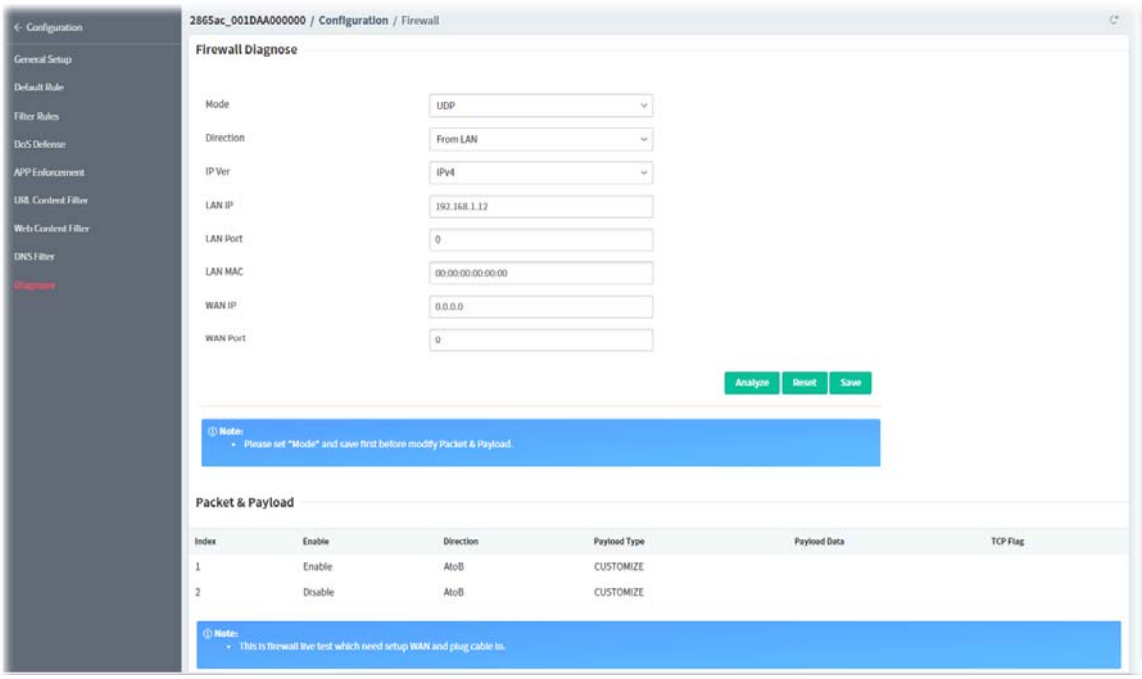
To create a new DNS profile, click **+Add** to open the following page.




| Item | Description |
|---|---|
| **Index** | Displays the index number of the DNS filter profile. |
| **Profile Name** | Enter a name of the DNS filter profile. |
| **Syslog** | Select the filtering type (Block, Pass, All or None) of the DNS syslog. |
| **WCF** | Select a WCF profile. |
| **UCF** | Select a UCF profile. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

### 9.4.7.9 Diagnose

The purpose of this function is to test when the router receiving incoming packet, which firewall rule will be applied to that packet.

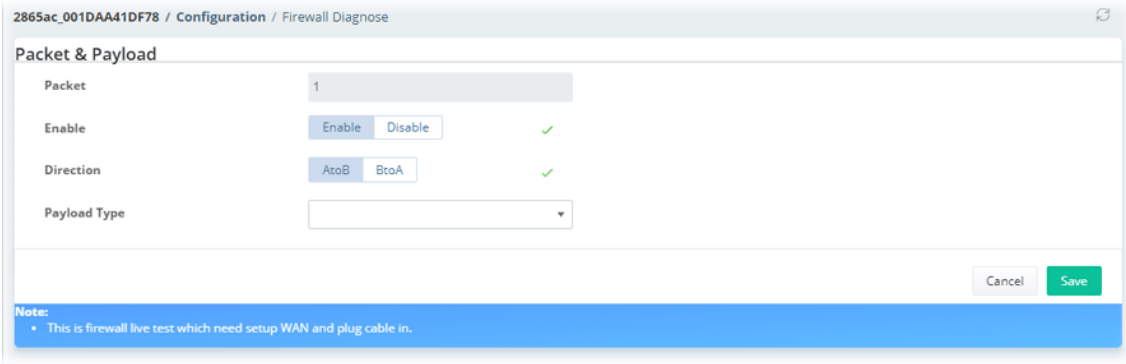



These parameters are explained as follows:

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

| | Firewall FwDiagnose |
|---|---|
| **Mode** | Specify the service type (ICMP, UDP, TCP) of the packet. |
| **Direction** | Set the way (from WAN or from LAN) that Vigor router receives the first packet for test. |
| **IP Ver** | Select the type of the IP address (IPv4/IPv6). |
| **LAN IP** | Enter the IPv4/IPv6 address of the packet's source. |
| **LAN Port** | Enter the port number of the packet's source. |
| **LAN MAC** | Enter the MAC address of the packet's source. |
| **WAN IP** | Enter the IPv4/IPv6 address of the packet's destination. |
| **WAN Port** | Enter the IPv4/IPv6 address of the packet's destination. |
| **Analyze** | Execute the test and analyze the result. |
| **Reset** | Reset the diagnose settings. |
| | **Packet & Payload** |
| **Index** | Displays the index number of the profile. |
| **Enable** | Displays if the profile is enabled or disabled. |
| **Direction** | The first packet of the firewall test will follow the direction specified above. However, the direction for the second packet might be different. Simply choose the direction (from Computer A to B or from the B to A) for the second packet. |
| **Payload Type** | Choose Customize, Ping, Trace Route / Customize, DNS, Trace Route / Customize, Http (GET). |
| **Payload Data** | It is available when Customize is selected. Simply type 16 HEX characters which represent certain packet (e.g., DNS packet) if you want to set the data transferred with protocol (ICMP/UDP/TCP) which is different to Type setting. |
| **Save** | Save the current settings. |

Click the index number (1 - 5) to configure detailed settings for Packet & Payload.



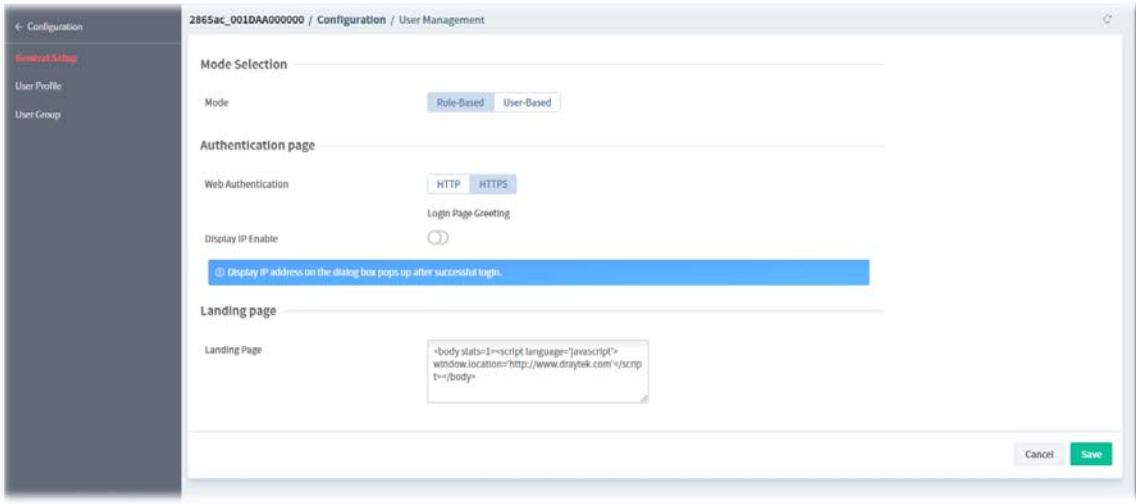

| Item | Description |
|---|---|
| **Packet** | Display the index number of the profile. |
| **Enable** | **Enable** - Enable this profile.<br>**Disable** - Disable this profile. |
| **Direction** | Select the direction for the second packet. |

| | |
|---|---|
| | • **AtoB**<br>• **BtoA** |
| **Payload Type** | Displays the mode selected above and the state. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

## 9.4.8 User Management

### 9.4.8.1 General Setup

Global settings for User Management can be configured in this section.



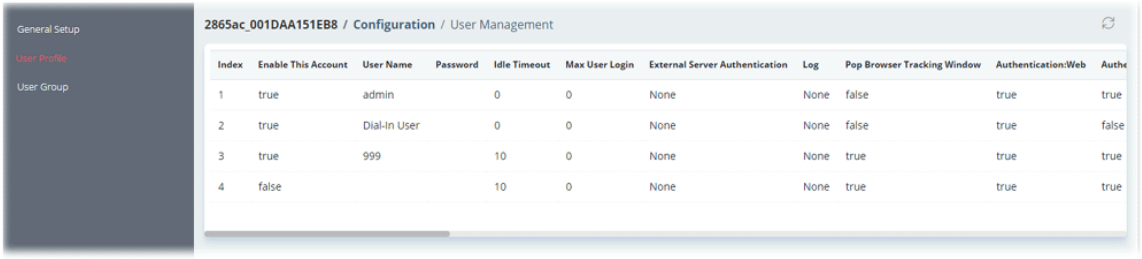

These parameters are explained as follows:

| Item | Description |
|---|---|
| | **Mode Selection** |
| **Mode** | **Rule-Based** - Router applies filter rules configured in **Firewall>>General Setup** and **Filter Rule**.<br>**User-Based** - Router applies filter rules configured in **User Management>>User Profile**. |
| | **Authentication page** |
| **Web Authentication** | **Set the** Web protocol for the web authentication page.<br>• **HTTP**<br>• **HTTPS** |
| **Login Page Greeting** | Click to be redirected to **Configuration>>Admin Account >> Login Page Greeting**, |
| **Display IP Enable** | Click to enable or disable the function.<br>If enabled, the IP address of the client will be shown on the tracking window. |
| | **Landing page** |
| **Landing Page** | HTML code to be shown on the Login Page Greeting. |
| **Cancel** | Discard current modification. |

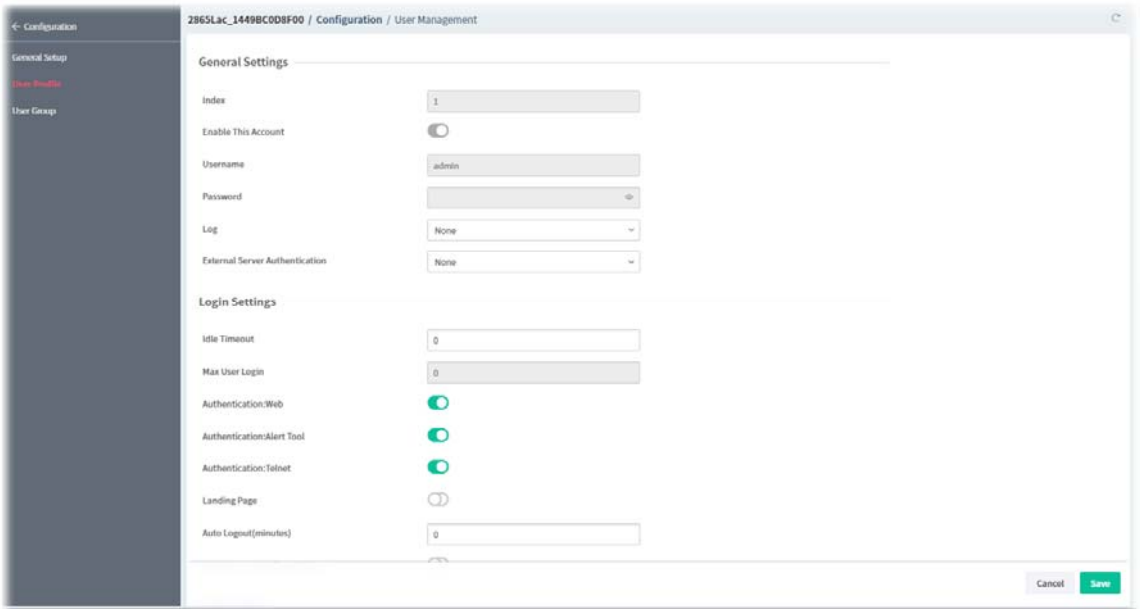
| | |
|---|---|
| **Save** | Save the current settings. |

### 9.4.8.2 User Profile

This page allows you to create up to 200 user profiles for use with User Management.




To configure the user management profile, move the mouse cursor to any entry and click to open the setting page.




These parameters are explained as follows:

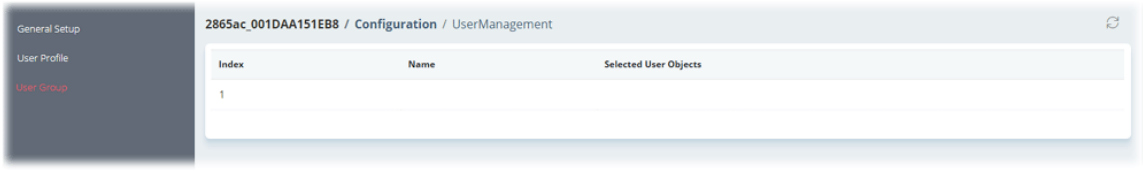
| Item | Description |
|---|---|
| | **General Settings** |
| **Index** | Displays the index number of the user profile. |
| **Enable This Account** | Click to enable or disable this user profile. |
| **Username** | Enter the login name of this user profile. |
| **Password** | Enter the password of this user profile. |
| **Log** | Select which activities (None, Login, Event or All) of the user can be recorded by Syslog. |
| **External Server Authentication** | The router will authenticate dial-in users using either a built-in (None) or external service (LDAP, Radius or TACACS+). |
| | **Login Settings** |
| **Idle Timeout** | If there is no WAN traffic to and from the LAN client for the specified amount of time (in minutes), the WAN session is reset and the user will need to re-authenticate before Internet access is once again allowed. |

| | |
|---|---|
| **Max User Login** | Enter the maximum number of concurrent logins allowed for this profile. |
| **Authentication:Web** | Click to enable or disable the function.<br>If enabled, user will need to authenticate by entering a username and password when attempting to access an external website for the first time. The user will be redirected to the external website after a successful authentication. |
| **Authentication:Alert Tool** | Click to enable or disable the function.<br>If enabled, the user can enter the user name and password into the DrayTek Alert Tool. A window with remaining time of connection for such user will be displayed. |
| **Authentication:Telnet** | Click to enable or disable the function.<br>If enabled, the user can authenticate by logging in to the router using telnet. |
| **Landing Page** | Click to enable or disable the function.<br>If enabled, when a user tries to access into the web user interface of Vigor router series with the user name and password specified in this profile, he/she will be lead into the web page configured in Landing Page field in 6.3.8.1 General Setup. |
| **Auto Logout(minutes)** | This account will be forced to logout after a certain time set here. |
| **Pop Browser Tracking Window** | Click to enable or disable the function.<br>If enabled, a browser window will pop up showing the session time remaining. |
| | **Quota Policy** |
| **Login Permission Schedule 1/2/3/4** | Enter four sets of time schedule for your request. |
| **Time Quota Enable** | Click to enable or disable the function. |
| **Time Quota:Mins** | Specify the amount of time (after a successful authentication).<br>Click + / - to increase / decrease the time quota for this profile. |
| **Data Quota Enable** | Click to enable or disable the function. |
| **Data Quota Value** | Specify the amount of data (after a successful authentication).<br>Click + / - to increase / decrease the data quota for this profile. |
| | **Reset Quota Automatically** |
| **Enable** | Click to enable or disable the function. |
| **Default Time Quota(Mins)** | Enter value for default time quota. |
| **Default Data Quota(MB)** | Enter value for default data quota. |
| **Quota reset** | **When login permission schedule expired -** When the scheduling time is up, the router will reset the quota with user-defined time/data values automatically.<br>**At the start time of Schedule -**<br>● **Quota reset schedule -** Specify a time schedule index number for this profile. |
| | **Internal Services** |

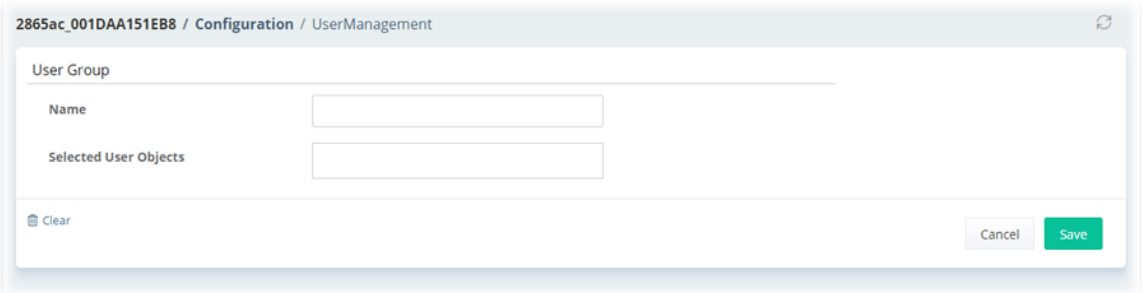
| | |
|---|---|
| **Internal RADIUS** | Click to enable or disable the function. |
| **Local 802.1x** | Click to enable or disable the function. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

#### 9.4.8.3 User Group

This page allows you to place multiple user profiles into groups. These groups can be used to set up filter rules in **Firewall>>General Setup**.




To configure the user group profile, move the mouse cursor to any entry and click to open the setting page.



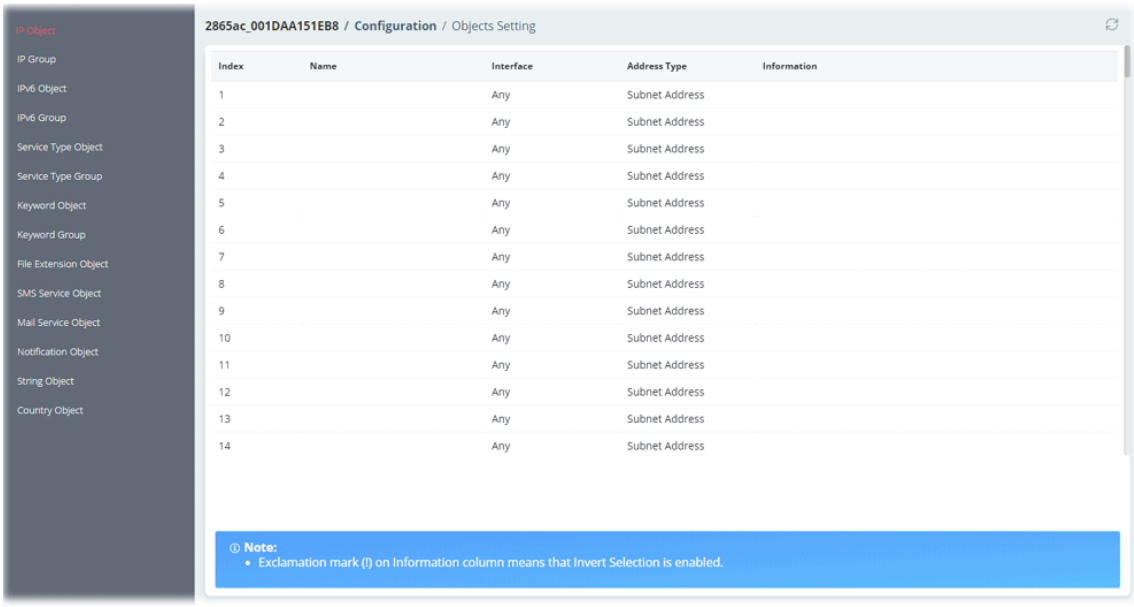

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Name** | Enter a name for identifying this user group. |
| **Selected User Objects** | Use the drop down menu to select the user object(s). |
| **Clear** | Clear all modifications on this page. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

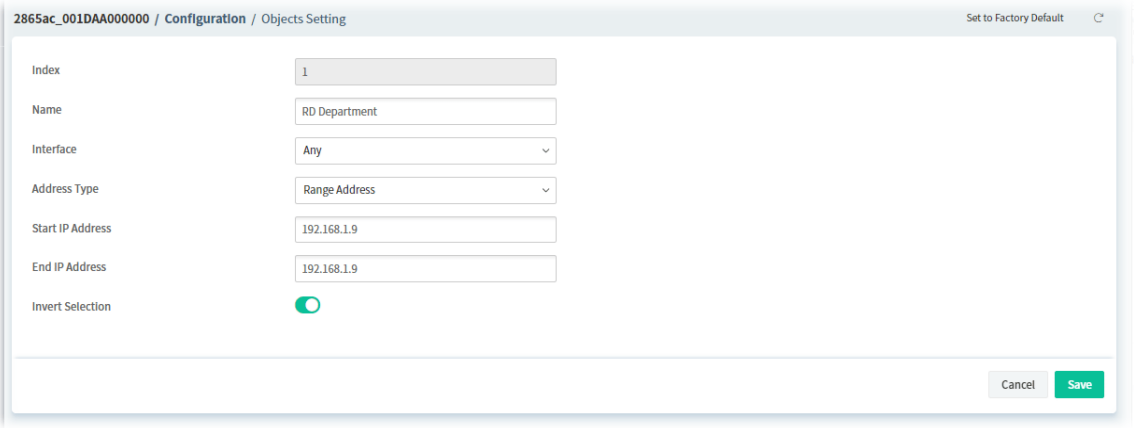
### 9.4.9 Object Setting

#### 9.4.9.1 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 them with ***groups*** for using conveniently.




To configure the IP object profile, move the mouse cursor to any entry and click to open the setting page.



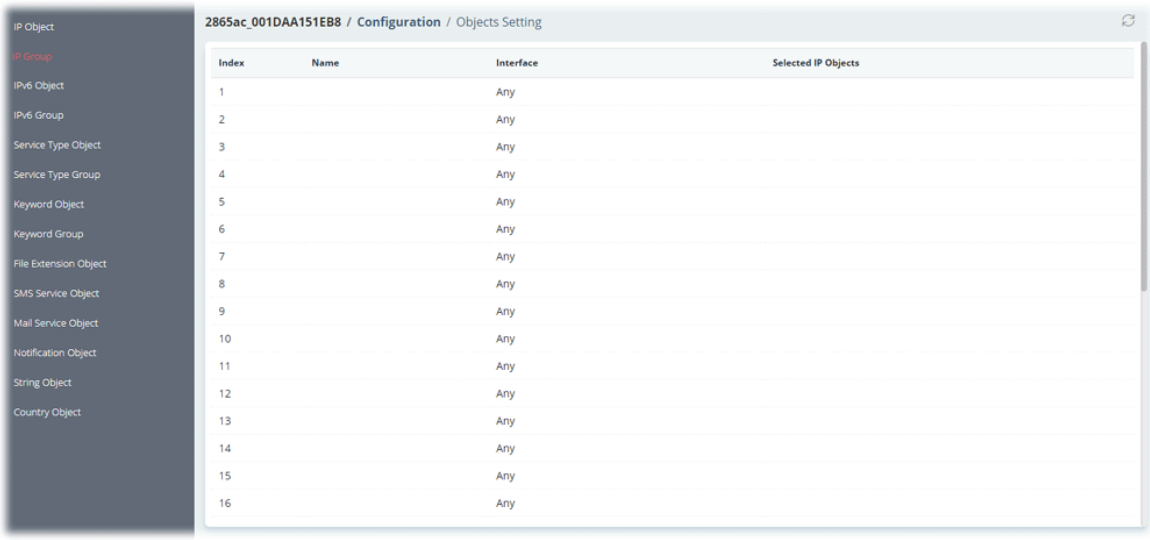

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Index** | Displays the index number of the IP object profile. |
| **Name** | Enter the name of the IP object profile. |
| **Interface** | Select the network interface on which the IP address or addresses are to be found. |
| **Address Type** | **Any Address -** Object covers all IP addresses.<br>**Mac Address -** Object contains a MAC address.<br>● **MAC Address -** Enter the MAC address.<br>**Range Address -** Object covers a range of IP addresses.<br>● **Start IP Address -** Enter an IP address as the starting point.<br>● **End IP Address -** Enter an IP address as the ending point.<br>**Single Address -** Object covers one IP address.<br>● **Start IP Address -** Enter an IP address as the starting point.<br>**Subnet Address -** Object covers a range of IP addresses specified in subnet notation.<br>● **Start IP Address -** Enter an IP address as the starting point. |

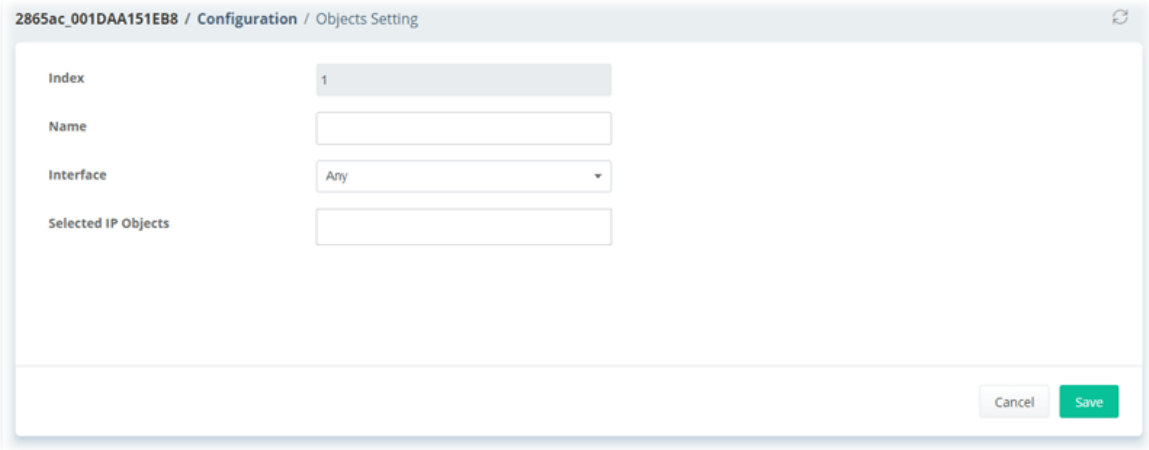
| | |
|---|---|
| | • **Subnet Mask -** Enter the subnet mask. |
| **Invert Selection** | Click to enable or disable the function.<br>If enabled, all addresses except the ones entered above will be used. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

### 9.4.9.2 IP Group

Multiple IP Objects can be placed into an IP Group.




To configure the IP group profile, move the mouse cursor to any entry and click to open the setting page.



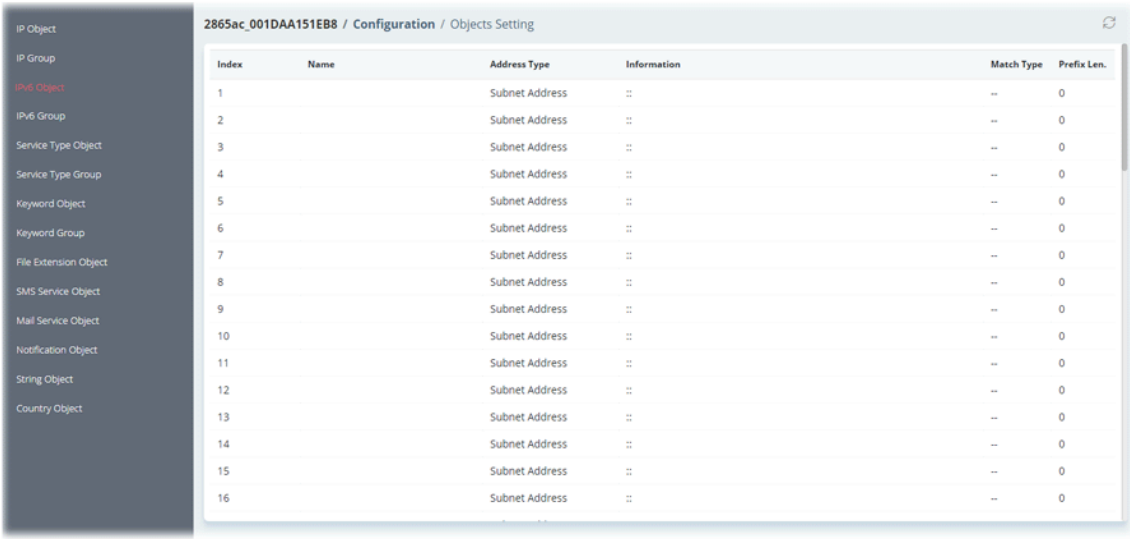

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Index** | Displays the index number of the IP object profile. |
| **Name** | Enter the name of the IP object profile. |
| **Interface** | Select WAN, LAN or Any to filter IP objects. |
| **Selected IP Objects** | Use the drop down menu to select the IP object(s). |
| **Cancel** | Discard current modification and return to previous page. |

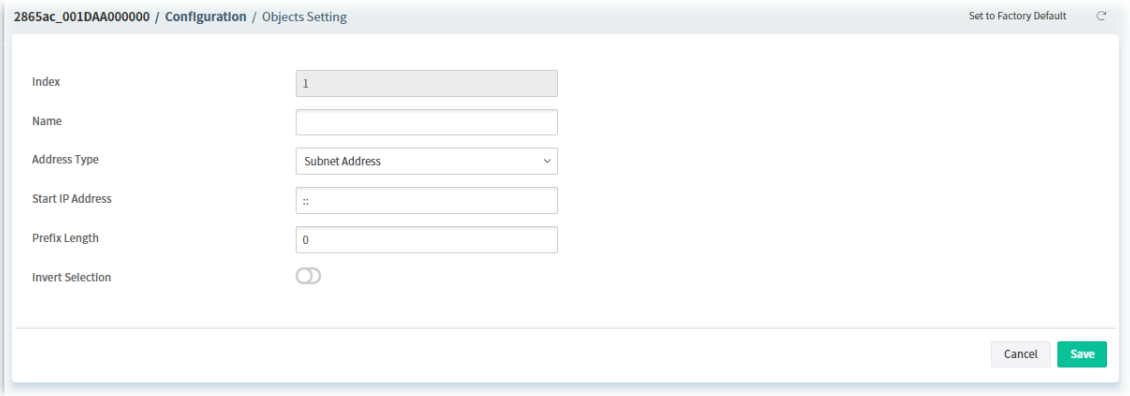
| | |
|---|---|
| **Save** | Save the current settings and return to previous page. |

### 9.4.9.3 IPv6 Object

Up to 64 IPv6 Objects can be created.




To configure the IPv6 object profile, move the mouse cursor to any entry and click to open the setting page.



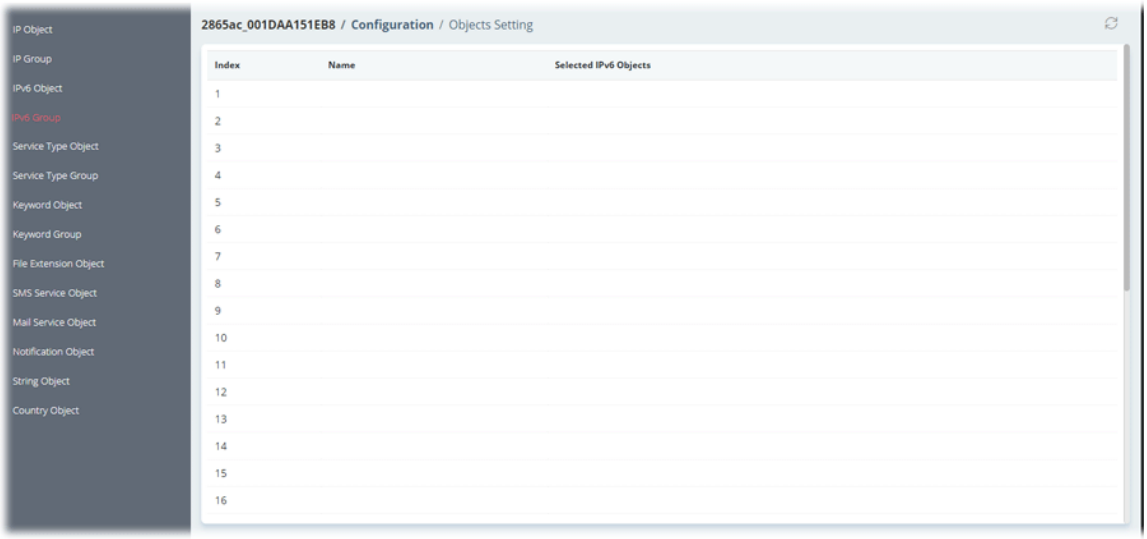

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Index** | Displays the index number of the IPv6 object profile. |
| **Name** | Enter the name of the IPv6 object profile. |
| **Address Type** | **Any Address -** Object covers all IPv6 addresses.<br>● **Match Type -** Specify the match type (128 Bits or Suffix 64 Bits) for the IPv6 address.<br>**Mac Address -** Object contains a MAC address.<br>● **Match Type -** Specify the match type (128 Bits or Suffix 64 Bits) for the IPv6 address.<br>● **MAC Address -** Enter the MAC address.<br>**Range Address -** Object covers a range of IPv6 addresses.<br>● **Match Type -** Specify the match type (128 Bits or Suffix 64 Bits) for the IPv6 address. |

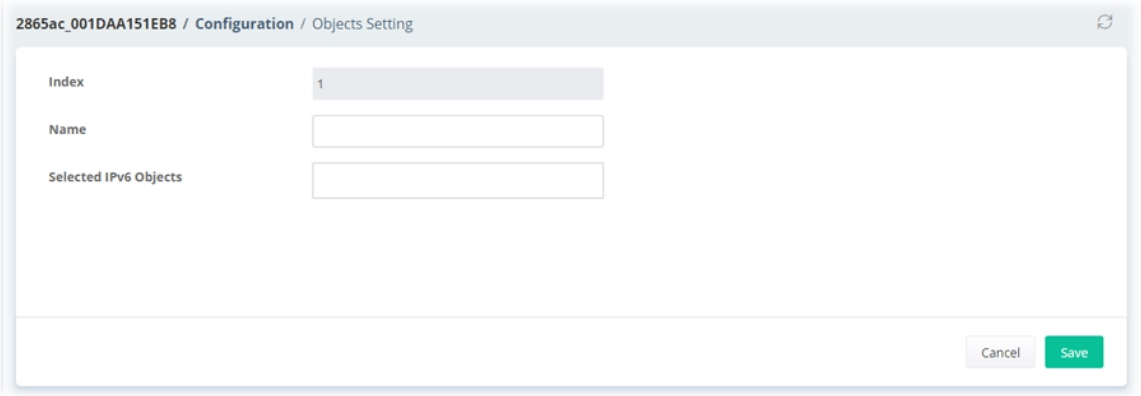
| | |
|---|---|
| | • **Start IP Address -** Enter an IPv6 address as the starting point.<br>• **End IP Address -** Enter an IPv6 address as the ending point.<br>• **Invert Selection -** If enabled, all addresses except the ones entered above will be used.<br>**Single Address -** Object covers one IPv6 address.<br>• **Match Type -** Specify the match type (128 Bits or Suffix 64 Bits) for the IPv6 address.<br>• **Start IP Address -** Enter an IPv6 address as the starting point.<br>• **Invert Selection -** If enabled, all addresses except the ones entered above will be used.<br>**Subnet Address -** Object covers a range of IPv6 addresses specified in subnet notation.<br>• **Start IP Address -** Enter an IPv6 address as the starting point.<br>• **Prefix Length -** Enter IPv6 prefix length, if Address type is Subnet Address.<br>• **Invert Selection -** If enabled, all addresses except the ones entered above will be used. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

### 9.4.9.4 IPv6 Group

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




To configure the IPv6 group profile, move the mouse cursor to any entry and click to open the setting page.

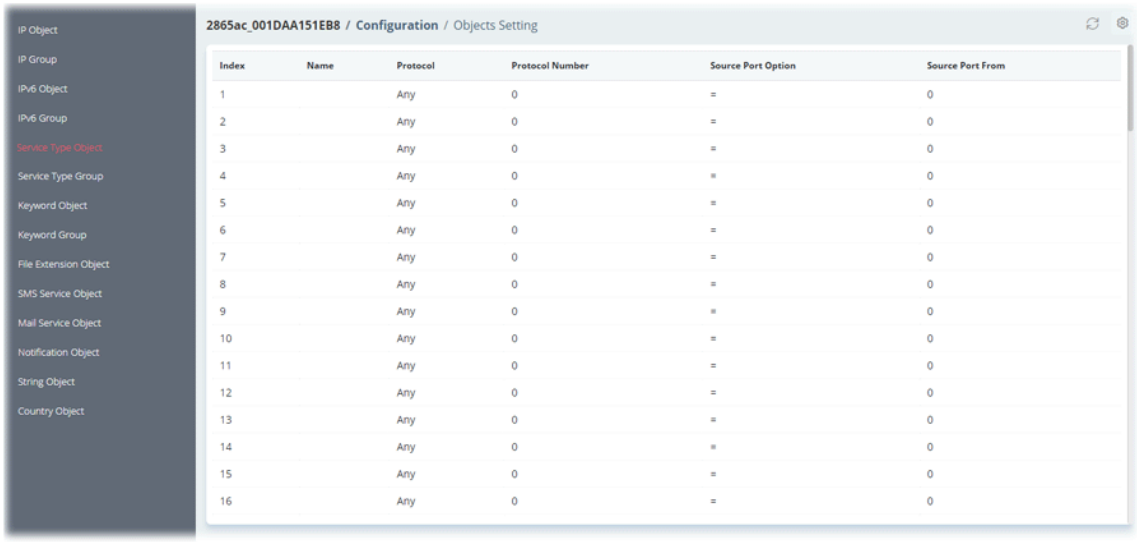



These parameters are explained as follows:

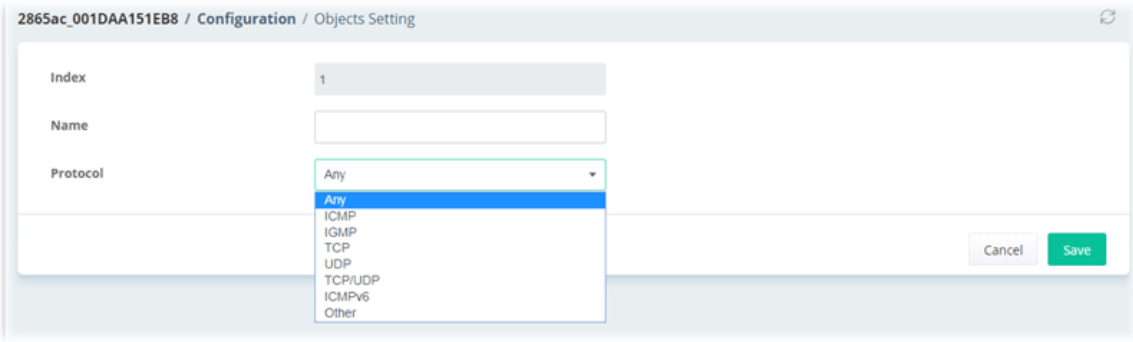
| Item | Description |
|---|---|
| **Index** | Displays the index number of the IPv6 group profile. |
| **Name** | Enter the name of the IPv6 group profile. |
| **Selected IPv6 Object** | Use the drop down menu to select the IPv6 object(s). |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

### 9.4.9.5 Service Type Object

Up to 96 Service Type Objects can be created.




To configure the service type object profile, move the mouse cursor to any entry and click to open the setting page.

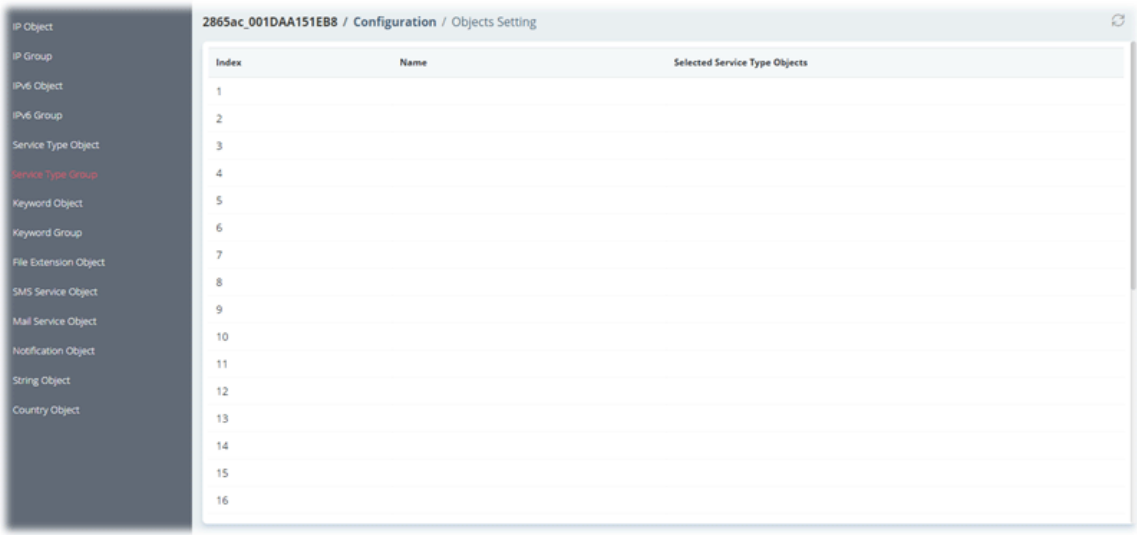



These parameters are explained as follows:

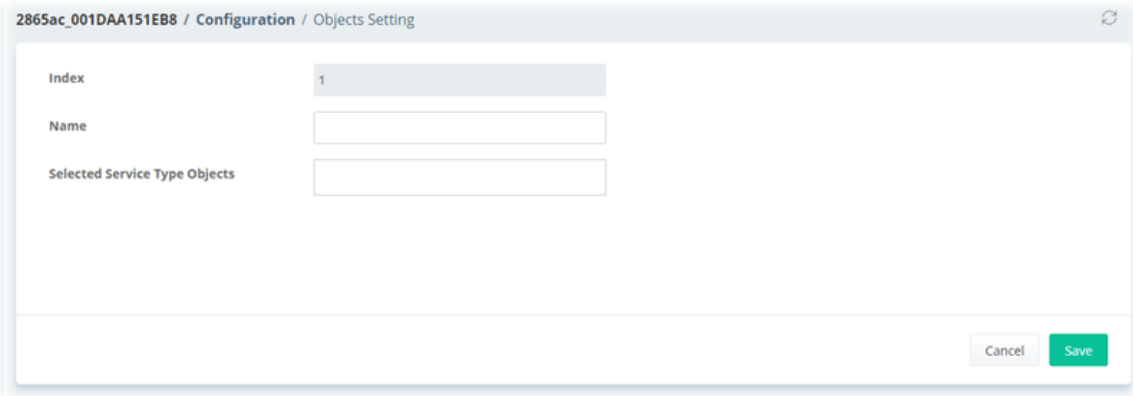
| Item | Description |
|---|---|
| **Index** | Displays the index number of the service type object profile. |
| **Name** | Enter the name of the service type object profile. |
| **Protocol** | Choose a protocol to which this profile applies. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

### 9.4.9.6 Service Type Group

Multiple **Service Type Objects** can be placed into a **Service Type Group**.




To configure the service type group profile, move the mouse cursor to any entry and click to open the setting page.

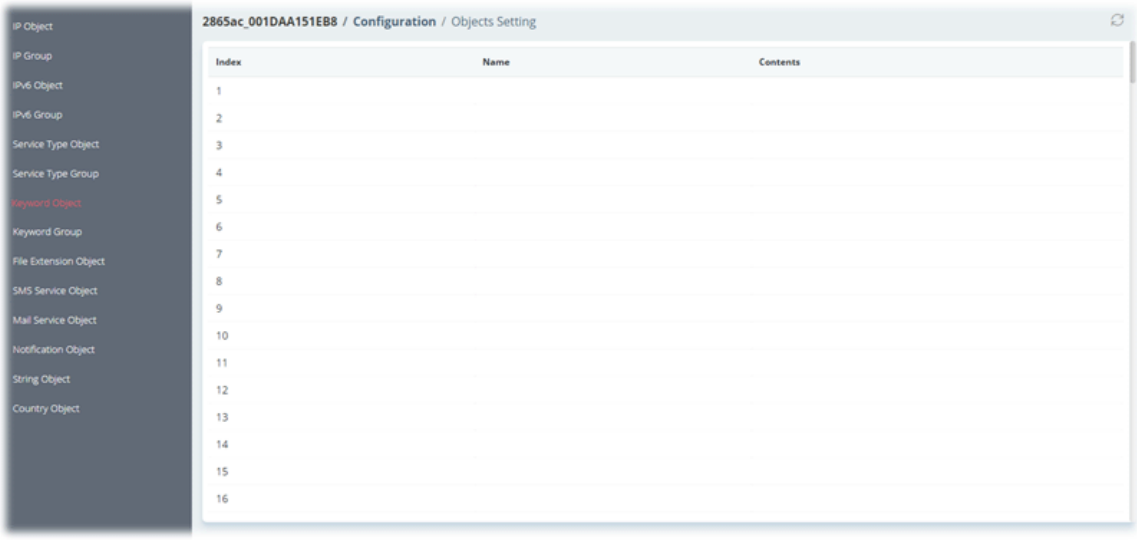



These parameters are explained as follows:

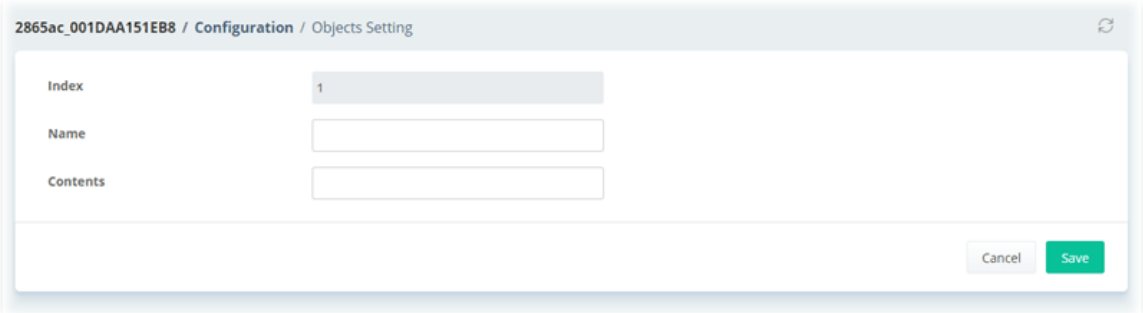
| Item | Description |
|---|---|
| **Index** | Displays the index number of the service type group profile. |
| **Name** | Enter the name of the service type group profile. |
| **Selected Service Type Objects** | Use the drop down menu to select the service type object(s). |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

### 9.4.9.7 Keyword Object

200 Keyword Object Profiles can be created for use as blacklists or white lists in **CSM >>URL Content Filter Profile** and **Web Content Filter Profile**.




To configure the keyword object profile, move the mouse cursor to any entry and click to open the setting page.

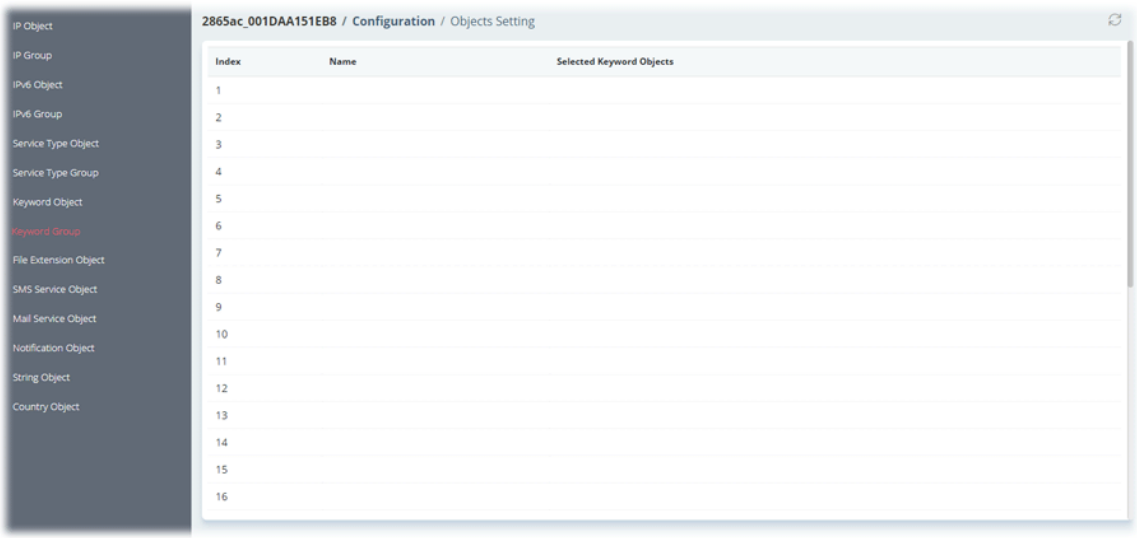



These parameters are explained as follows:

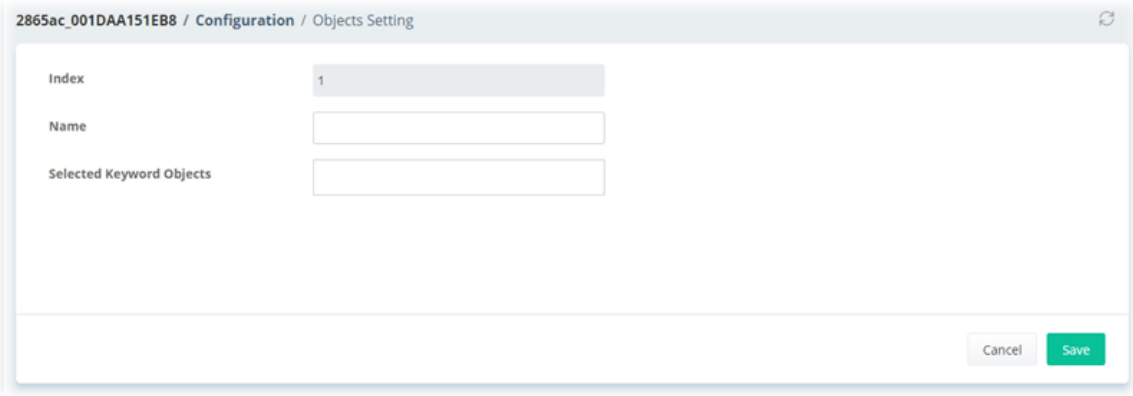
| Item | Description |
|---|---|
| **Index** | Displays the index number of the keyword object profile. |
| **Name** | Enter the name of the keyword object profile. |
| **Contents** | Enter the keywords to be matched. Up to 3 key phrases, separated by spaces, for a total length of 63 characters can be entered. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

### 9.4.9.8 Keyword Group

Multiple Keyword Objects can be placed into a Keyword Group.




To configure the keyword group profile, move the mouse cursor to any entry and click to open the setting page.

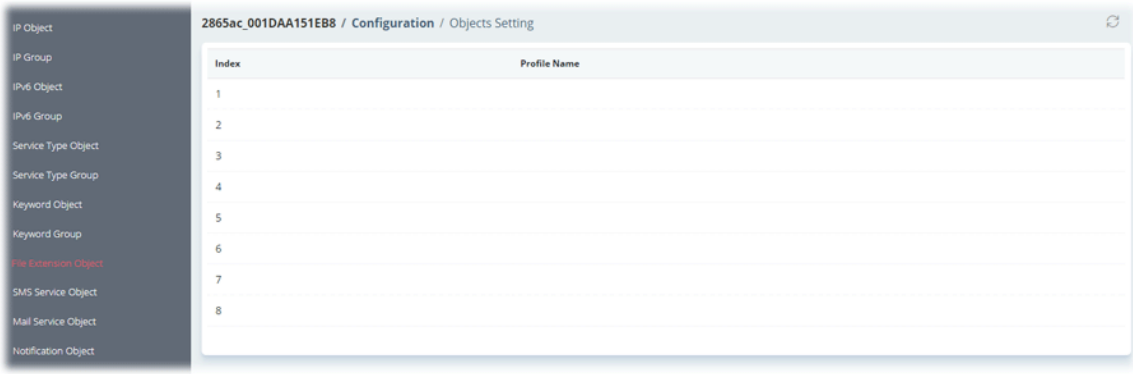



These parameters are explained as follows:

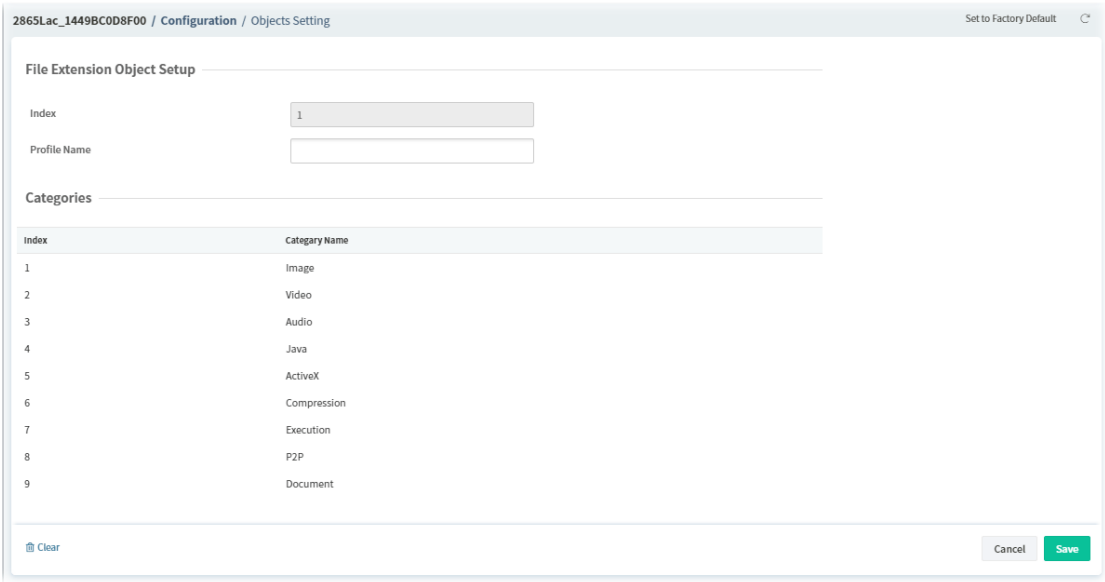
| Item | Description |
|---|---|
| **Index** | Displays the index number of the keyword group profile. |
| **Name** | Enter the name of the keyword group profile. |
| **Selected Keyword Objects** | Use the drop down menu to select the keyword object(s). |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

### 9.4.9.9 File Extension Object

Up to 8 File Extension Objects can be set up for use.




To configure the file extension object profile, move the mouse cursor to any entry and click to open the setting page.

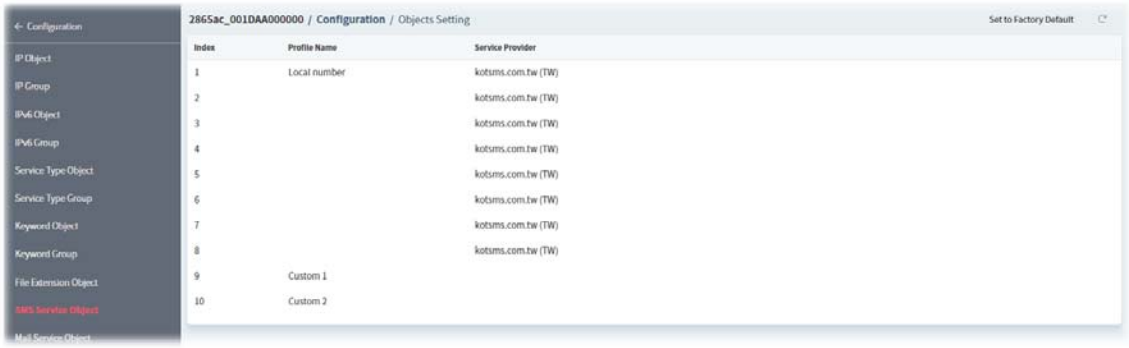



These parameters are explained as follows:

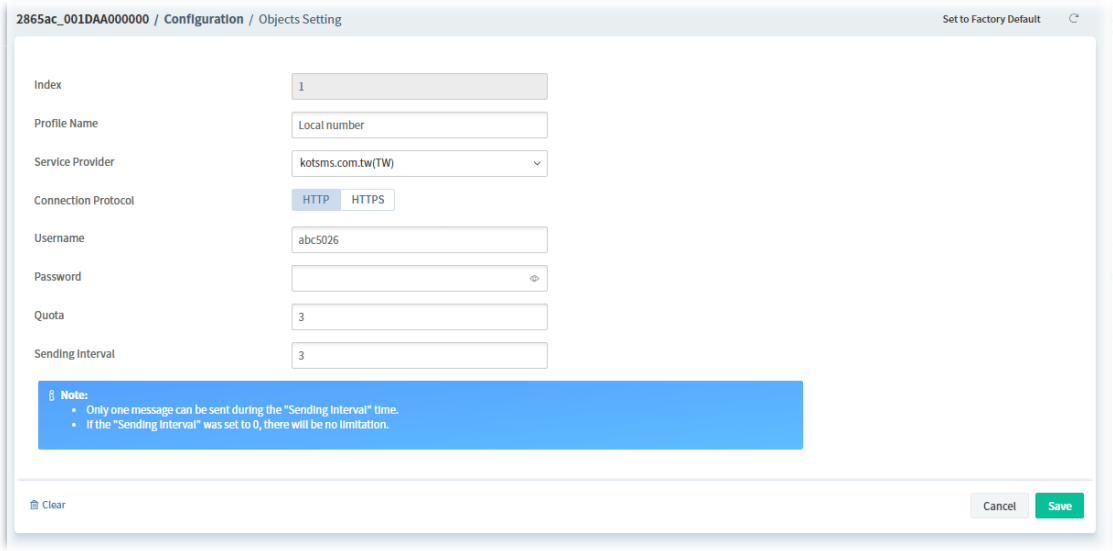
| Item | Description |
|---|---|
| **Index** | Displays the index number of the file extension object profile. |
| **Profile Name** | Enter the name of the file extension object profile. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

### 9.4.9.10 SMS Service Object

Up to 10 SMS Service Objects can be set up for use.



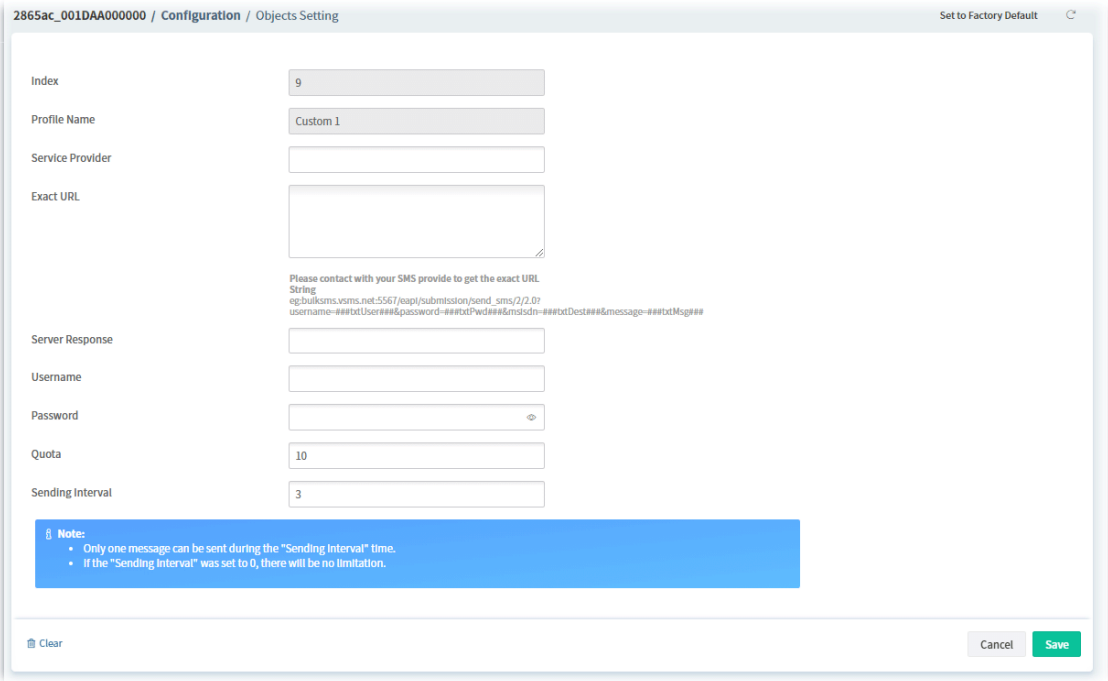

To configure the SMS service object profile, move the mouse cursor to index 1 to index 8 and click to open the setting page.




These parameters are explained as follows:

| Item | Description |
|---|---|
| **Index** | Displays the index number of the SMS service object profile. |
| **Profile Name** | Enter the name of the SMS service object profile. |
| **Service Provider** | Select a Service Provider from the dropdown list. |
| **Connection Protocol** | Select HTTP or HTTPs. |
| **Username** | Enter a name to log in to the server. |
| **Password** | Enter a password to log in to the server. |
| **Quota** | Set the remaining number of text messages allowed to be sent. |
| **Sending Interval** | Set the minimum amount of time, in seconds, to wait between sending SMS messages. |
| **Clear** | Clear all modifications on this page. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

To configure the customized SMS service object profile, move the mouse cursor to index 9 to index 10 and click to open the setting page.

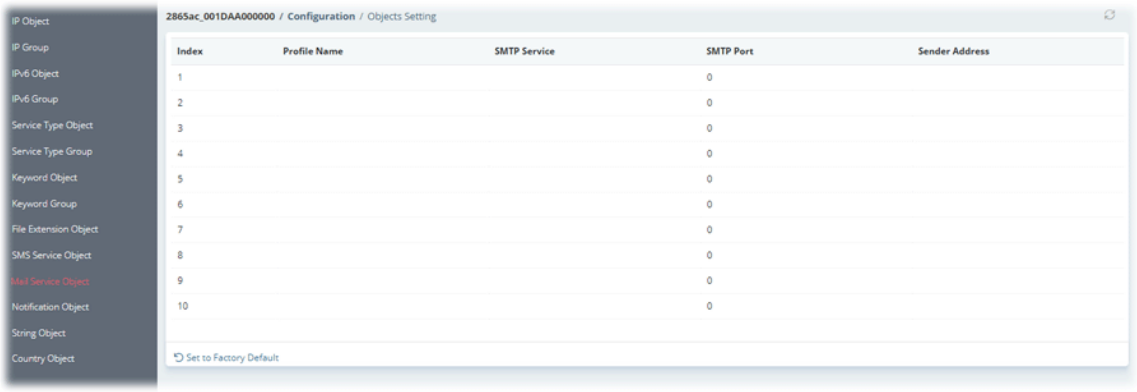



These parameters are explained as follows:

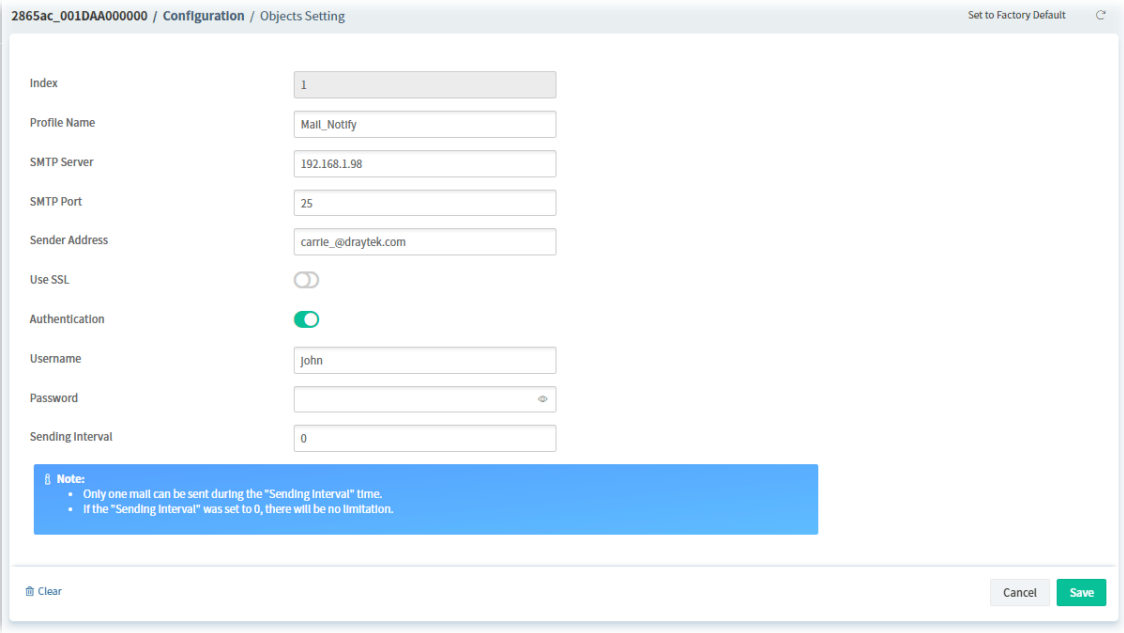
| Item | Description |
|---|---|
| **Index** | Displays the index number of the SMS service object profile. |
| **Profile Name** | Displays the name of the SMS service object profile. |
| **Service Provider** | Enter an identifier for the service provider. Maximum length is 23 characters. |
| **Exact URL** | Enter the URL for the SMS service. |
| **Username** | Enter a name to log in to the service. |
| **Password** | Enter a password to log in to the service. |
| **Quota** | Set the remaining number of text messages allowed to be sent. |
| **Sending Interval** | Set the minimum amount of time, in seconds, to wait between sending SMS messages. |
| **Clear** | Clear all modifications on this page. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

### 9.4.9.11 Mail Service Object

Up to 10 Mail Service Objects can be set up for use.




To configure the mail service object profile, move the mouse cursor to any entry and click to open the setting page.



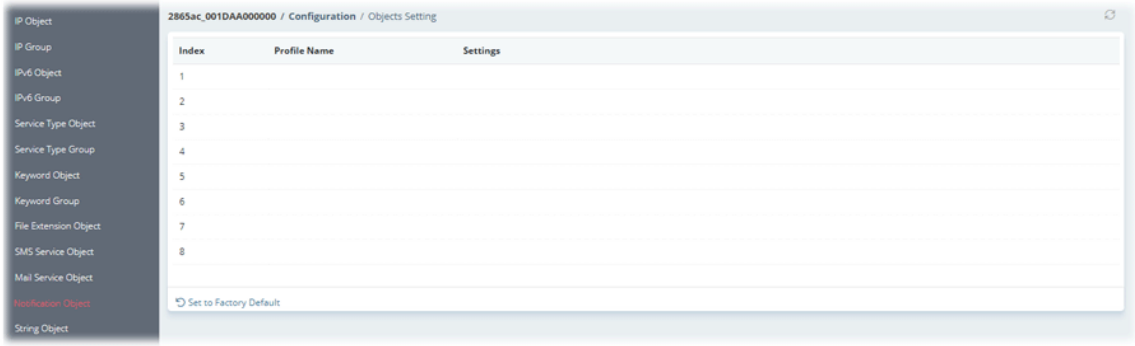

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Index** | Displays the index number of the mail service object profile. |
| **Profile Name** | Enter the name of the mail service object profile. |
| **SMTP Server** | Enter the IP address of the SMTP server. |
| **SMTP Port** | Enter the port number of the SMTP server. |
| **Sender Address** | Enter the e-mail address of the sender. |
| **Use SSL** | Click to enable or disable the function.<br>If enabled, Vigor router will use SMTPS (SMTP over SSL) to communicate with the SMTP server. |
| **Authentication** | Click to enable or disable the function.<br>**Username** - Enter a name for authentication.<br>**Password** - Enter the password for authentication. |

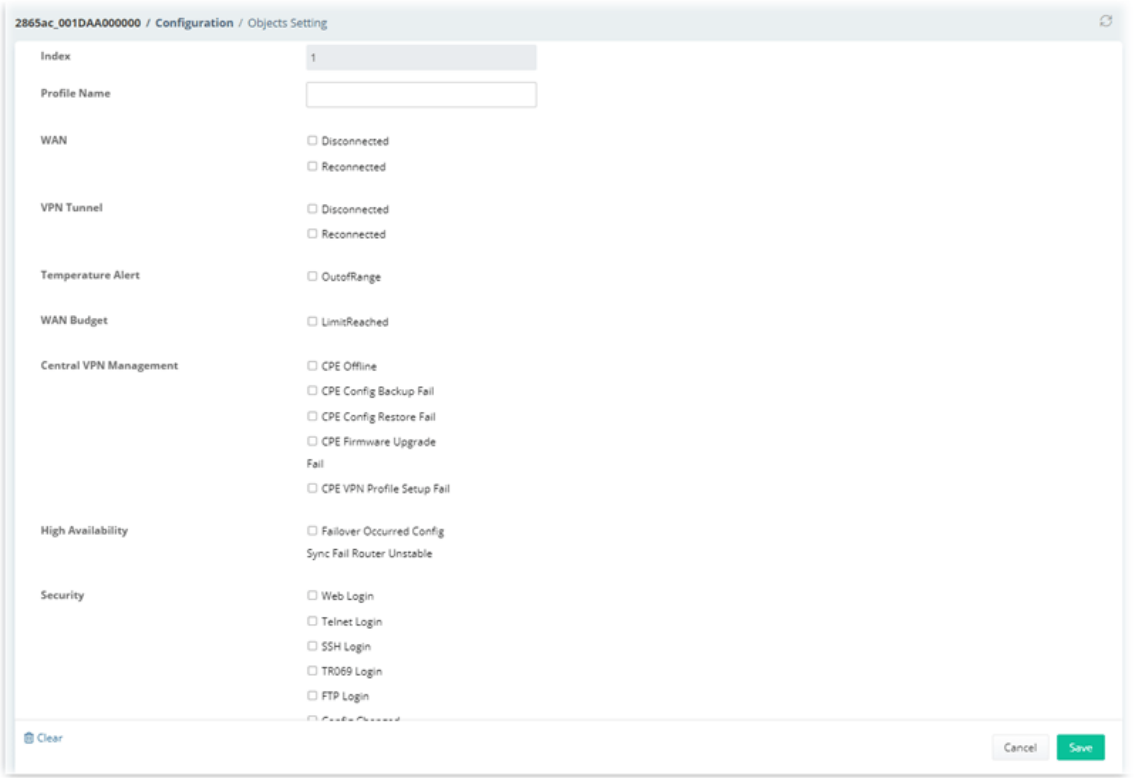
| | |
|---|---|
| **Sending Interval** | Specify the minimum amount of time, in seconds, to wait between sending e-mail messages. |
| **Clear** | Clear all modifications on this page. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

### 9.4.9.12 Notification Object

Up to 8 Notification Objects can be set up for use.




To configure the notification object profile, move the mouse cursor to any entry and click to open the setting page.



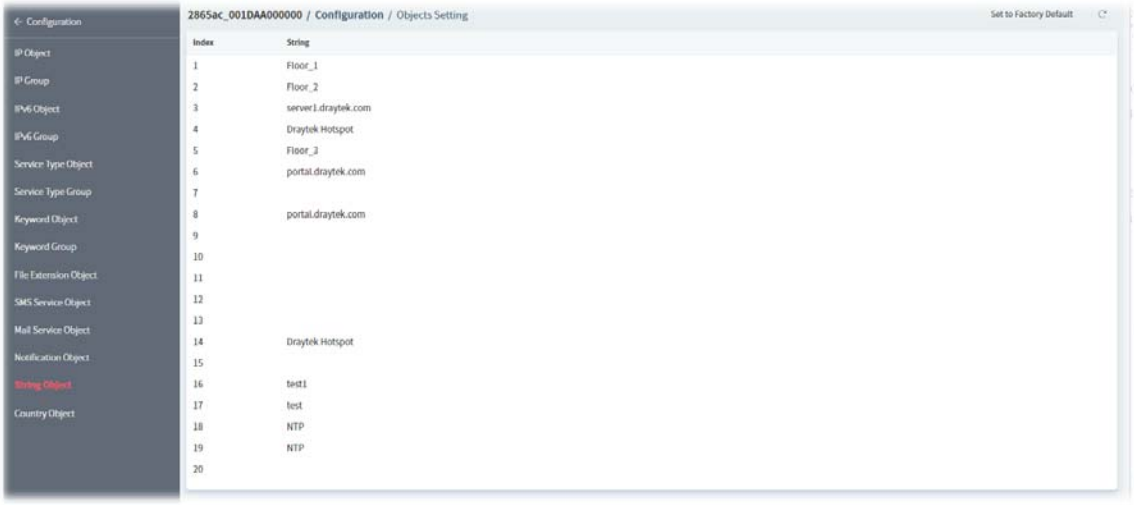

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Index** | Displays the index number of the notification object profile. |
| **Profile Name** | Enter the name of the mail service object profile. |
| **Check boxes** | Select the states to be monitored. |

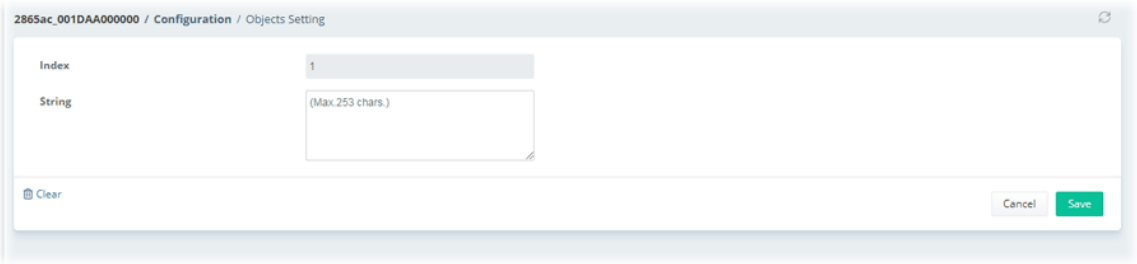
| | |
|---|---|
| **Clear** | Clear all modifications on this page. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

### 9.4.9.13 String Object

Set string profiles which will be applied in route policy.




To configure the string object profile, move the mouse cursor to any entry and click to open the setting page.

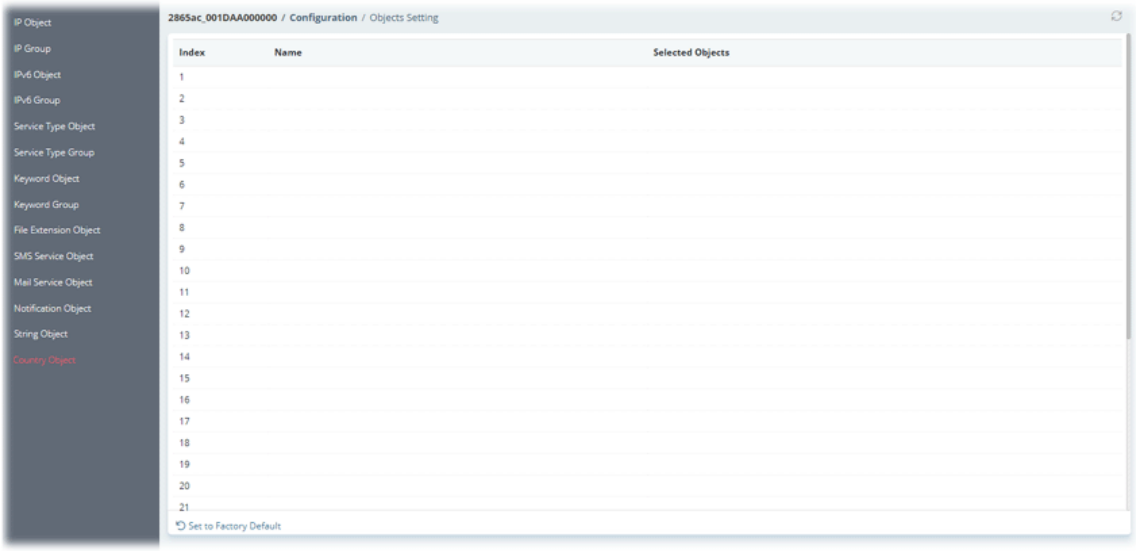



These parameters are explained as follows:

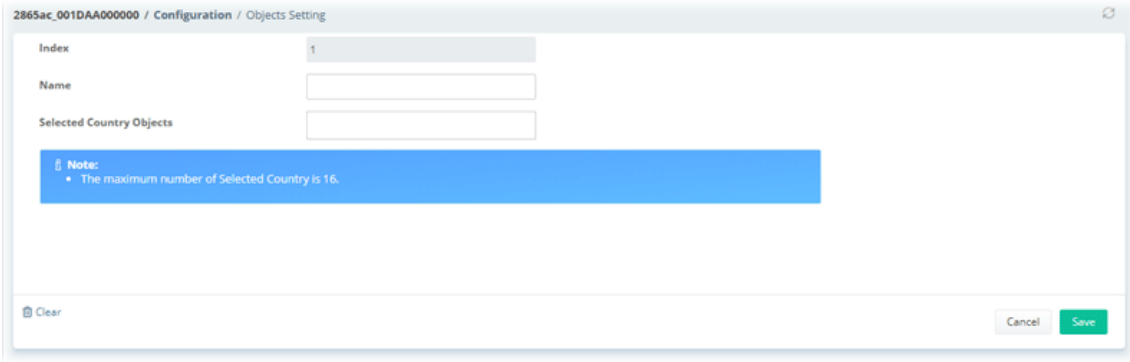
| Item | Description |
|---|---|
| **Index** | Displays the index number of the string object profile. |
| **String** | Enter a string. |
| **Clear** | Clear all modifications on this page. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

### 9.4.9.14 Country Object

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




To configure the country object profile, move the mouse cursor to any entry and click to open the setting page.

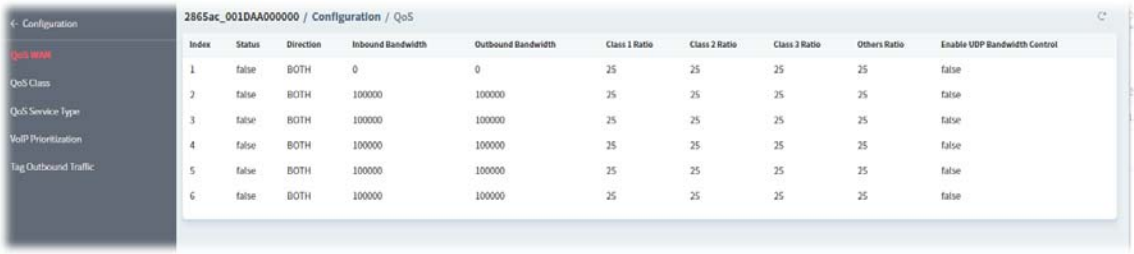



These parameters are explained as follows:

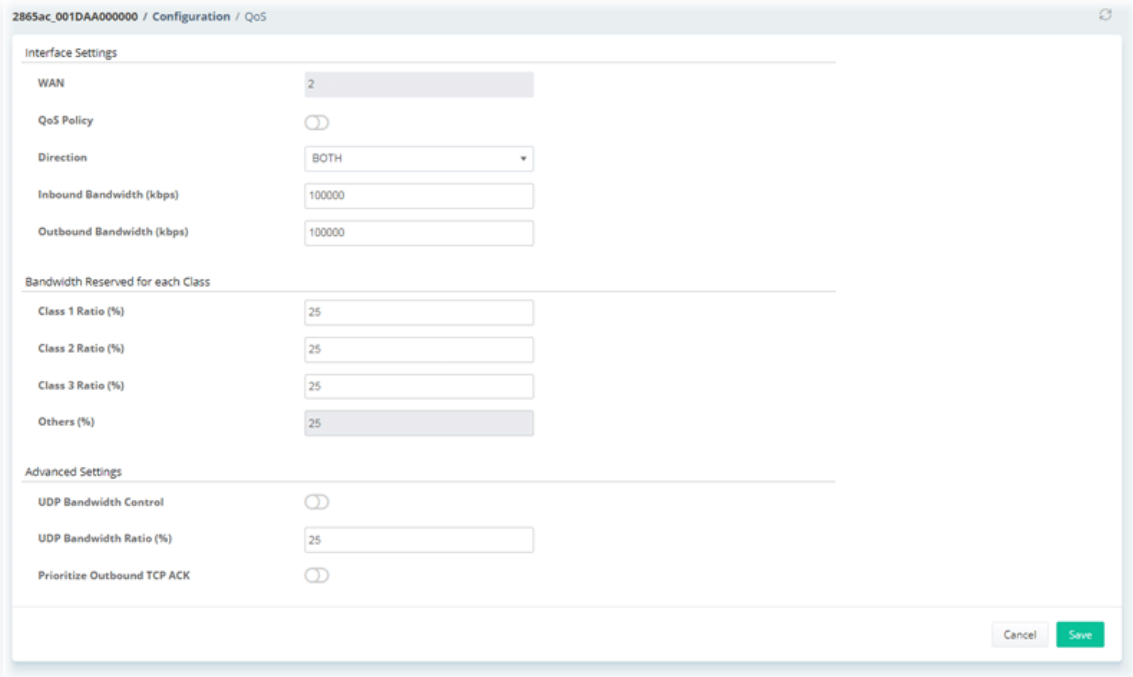
| Item | Description |
|---|---|
| **Index** | Displays the index number of the country object profile. |
| **Name** | Enter the name of the mail country object profile. |
| **Selected Country Objects** | Use the drop down menu to select the country object(s). |
| **Clear** | Clear all modifications on this page. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

## 9.4.10 QoS

### 9.4.10.1 QoS WAN




To configure the QoS WAN profile, move the mouse cursor to any entry and click to open the setting page.



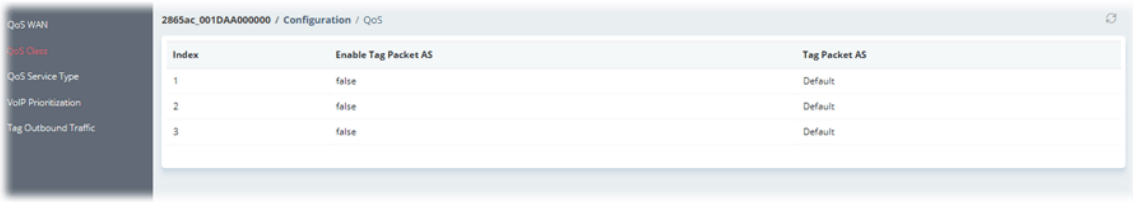

These parameters are explained as follows:

| Item | Description |
|---|---|
| | **Interface Settings** |
| **WAN** | Display the index number of the WAN interface. |
| **QoS Policy** | Click to enable or disable this QoS policy. |
| **Direction** | Use the drop-down list to set the direction of traffic to which QoS is to be applied (Inbound, Outbound, or Both). |
| **Inbound Bandwidth(kbps)** | Set the inbound bandwidth of the WAN. |
| **Outbound Bandwidth(kbps)** | Set the outbound bandwidth of the WAN. |
| | **Bandwidth Reserved for each Class** |
| **Class 1 ~3 Ratio (%)** | Set the percentage of bandwidth reserved for each class. |
| **Others (%)** | Set the percentage of bandwidth reserved for others. |

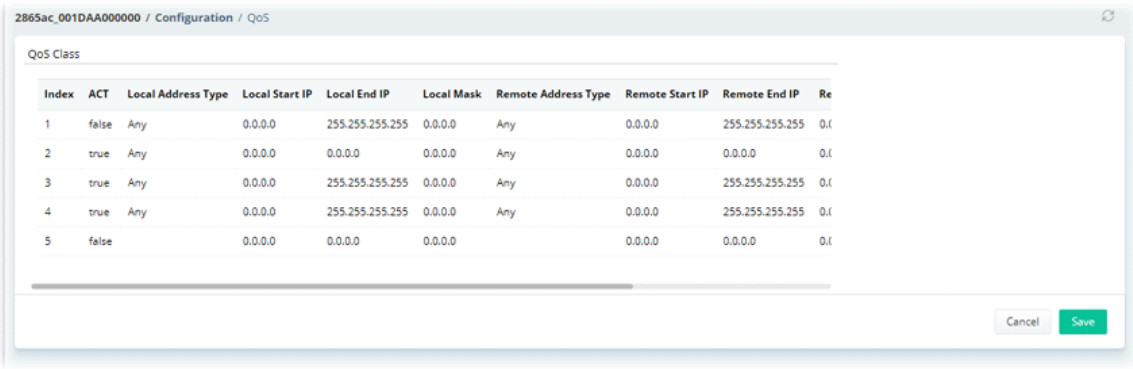
| | Advanced Settings |
|---|---|
| **UDP Bandwidth Control** | Click to enable or disable this function.<br>If enabled, the router will restrict the bandwidth available to UDP traffic. |
| **UDP Bandwidth Ratio(%)** | Enter a percentage value. |
| **Prioritize Outbound TCP ACK** | Click to enable or disable this function.<br>If enabled, the router will give outbound ACK packets priority over other packets to ensure traffic is not slowed down because the remote host is waiting for ACK packets before further traffic will be sent. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

### 9.4.10.2 QoS Class

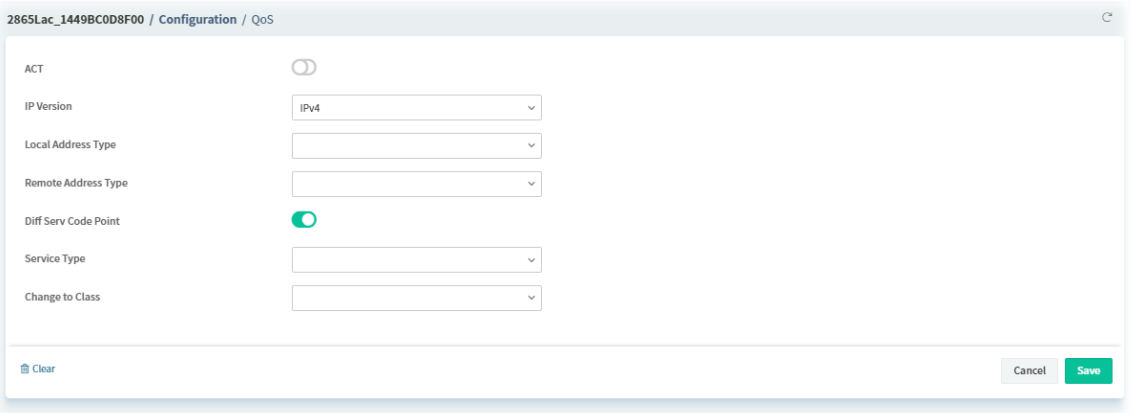
Configure Class 1 to Class 3 with detailed settings.




To configure the QoS class profile, move the mouse cursor to any entry and click to open the following page.



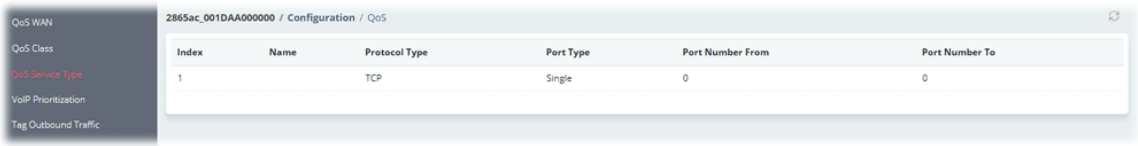

Then, click any index number to open the setting page.



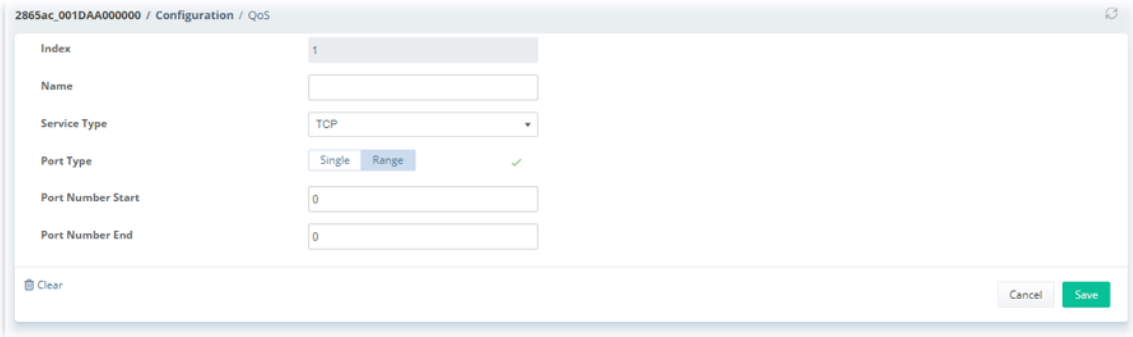

These parameters are explained as follows:

| Item | Description |
|---|---|
| **ACT** | Click to enable or disable this function. |
| **IP Version** | Select IPv4 or IPv6. |
| **Local Address Type** | Set the remote (WAN) IP address or address range for the rule.<br>**Any** - The rule covers all IP addresses.<br>**Range** - The rule covers a range of IP addresses.<br>• **Local Start IP Address** - Enter an IP address as the starting point.<br>• **Local End IP Address** - Enter an IP address as the ending point.<br>**Single** - The rule covers one IP address.<br>• **Local Start IP Address** - Enter an IP address as the starting point.<br>**Subnet** - The rule covers a range of IP addresses specified in subnet notation.<br>• **Local Start IP Address** - Enter an IP address as the starting point.<br>• **Local Mask** - Enter the subnet mask for the above IP address.<br>**Group and Object** - The rules covers a range of IP address specified in a group or object profile. |
| **Remote Address Type** | Set the remote (WAN) IP address or address range for the rule.<br>**Any** - The rule covers all IP addresses.<br>**Range** - The rule covers a range of IP addresses.<br>• **Remote Start IP** - Enter an IP address as the starting point.<br>• **Remote End IP** - Enter an IP address as the ending point.<br>**Single** - The rule covers one IP address.<br>• **Remote Start IP** - Enter an IP address as the starting point.<br>**Subnet** - The rule covers a range of IP addresses specified in subnet notation.<br>• **Remote Start IP** - Enter an IP address as the starting point.<br>• **Remote Mask** - Enter the subnet mask for the above IP address.<br>**Group and Object** - The rules covers a range of IP address specified in a group or object profile. |
| **Diff Serv Code Point** | Enable it to set DSCP or ToS precedence of packets to which this rule applies. |
| **Service Type** | Choose a service type to which this rule applies. |
| **Change to Class** | Specify a class for the QoS class profile. |
| **Clear** | Clear all modifications on this page. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

### 9.4.10.3 QoS Service Type



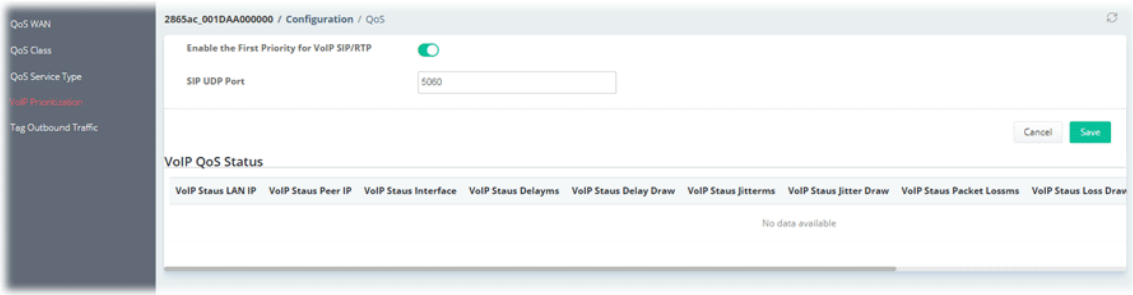

To configure the QoS service type profile, move the mouse cursor to any entry and click to open the following page.




These parameters are explained as follows:

| Item | Description |
|---|---|
| **Index** | Display the index number of the profile. |
| **Name** | Enter a name of this profile. |
| **Service Type** | Choose the type (TCP, UDP or TCP/UDP or other) for the new service. |
| **Port Type** | **Single** - Set a port number for this profile.<br>● **Port Number Start** - Enter the starting port number.<br>**Range** - You have to set the starting port number and the end porting number on the boxes below.<br>● **Port Number Start** - Enter the starting port number.<br>● **Port Number End** - Enter the end porting number. |
| **Clear** | Clear all modifications on this page. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

### 9.4.10.4 VoIP Prioritization

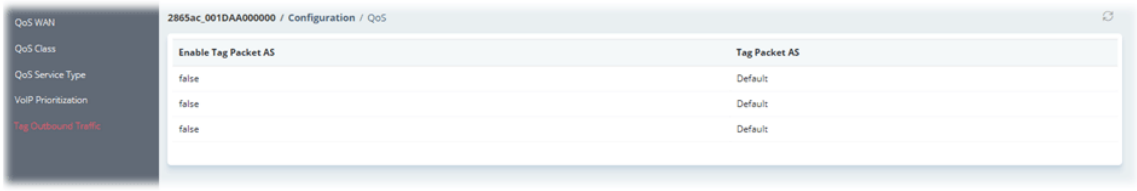



These parameters are explained as follows:

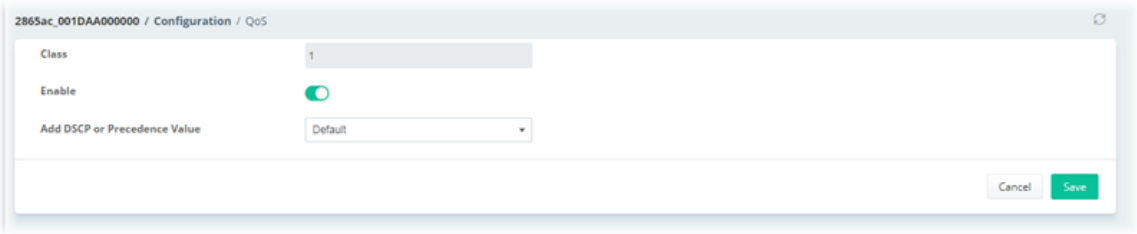
| Item | Description |
|---|---|
| **Enable the First Priority for VoIP SIP/RTP** | Click to enable or disable the function.<br>If enabled, VoIP traffic will be received with the highest priority. |
| **SIP UDP Port** | Set a port number to be monitored for SIP traffic. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |
| **VoIP QoS Status** | Displays current VoIP QoS status. |

### 9.4.10.5 Tag Outbound Traffic

Tag the outgoing traffic with the DSCP or Precedence value.




To configure the tag outbound traffic profile, move the mouse cursor to any entry and click to open the following page.



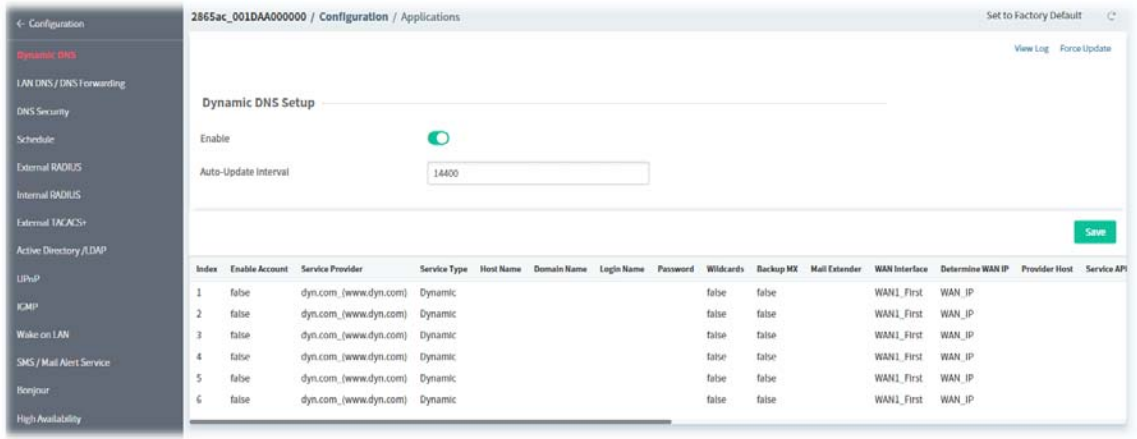

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Class** | Display the index number of the class. |
| **Enable** | Click to enable or disable the profile. |
| **Add DSCP or Precedence Value** | Use the drop-down list to choose the value for applying the DSCP or precedence value for each class. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

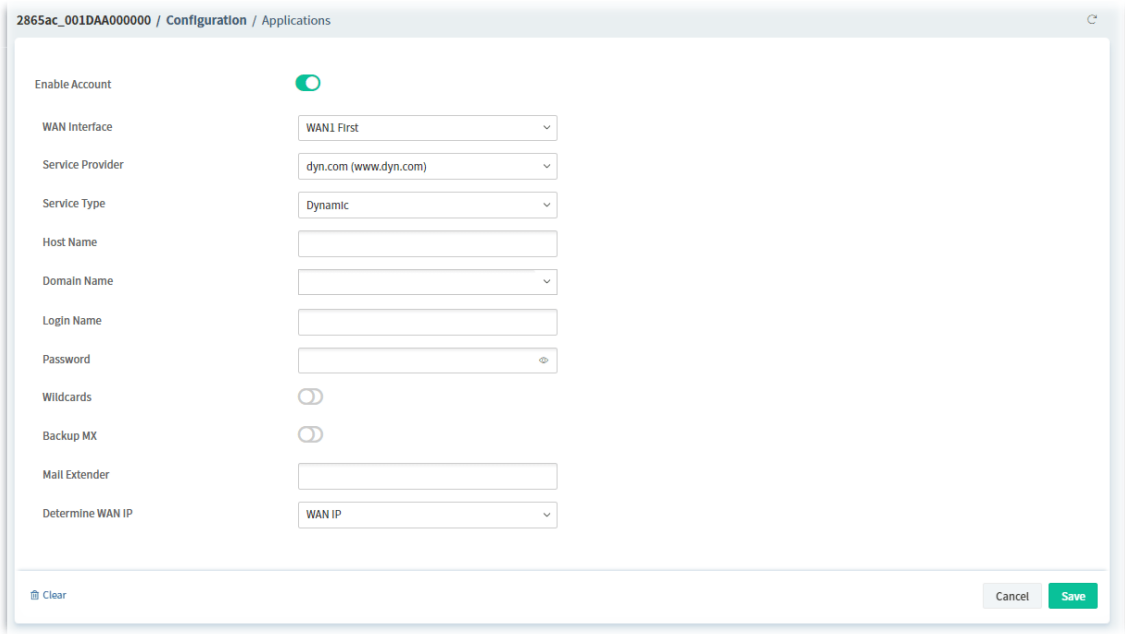
## 9.4.11 Applications

### 9.4.11.1 Dynamic DNS

The Vigor router supports a wide range of DDNS providers, such as DynDNS, No-IP.com, DtDNS, and ChangeIP. Please contact the DDNS provider of your choice to set up service before configuring DDNS on the router.




To configure the DDNS profile, move the mouse cursor to any entry (1 to 6) and click to open the following page.

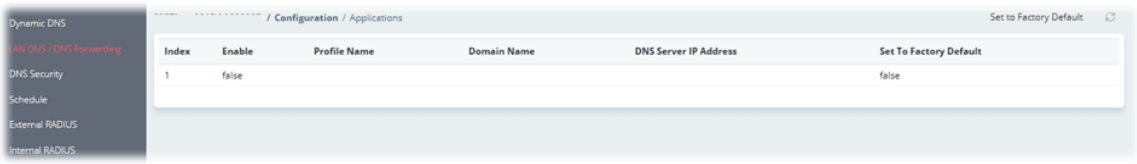



These parameters are explained as follows:

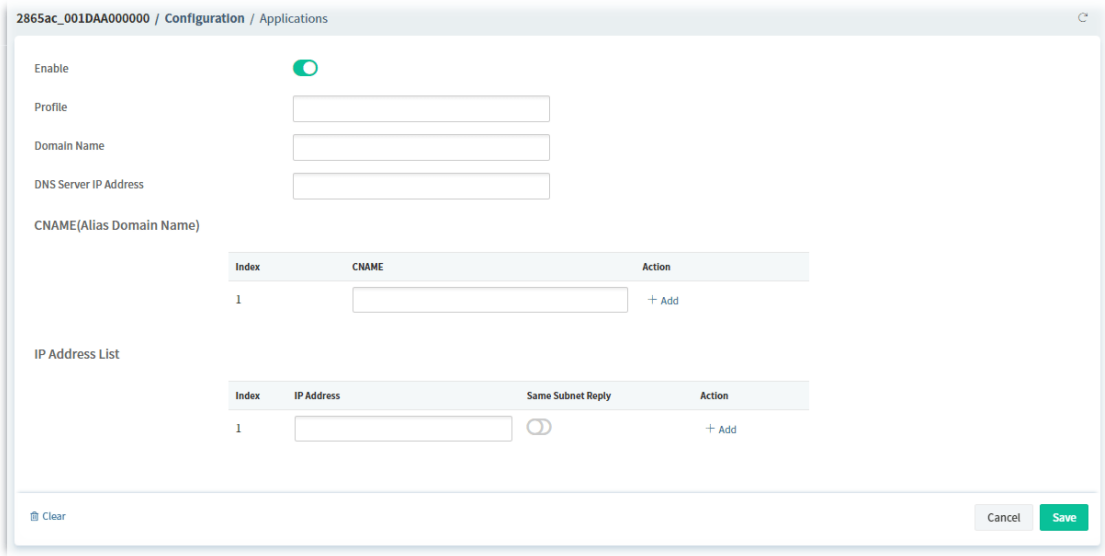
| Item | Description |
|---|---|
| **Enable Account** | Click to enable or disable the account. |
| **WAN Interface** | Select the WAN interface to monitor for IP address changes. |
| **Service Provider** | Select the DDNS provider. If your DDNS provider is not listed, select **User-Defined** and manually configure the profile. |
| **Service Type** | Select the service type (Custom, Dynamic, Static) that matches that of your DynDNS account. |
| **Host Name** | Enter the IP address or the domain name of the host which provides related service. |
| **Domain Name** | Select one domain name. |
| **Login Name** | Enter the login name of the DDNS account. |
| **Password** | Enter the password of the DDNS account. |
| **Wildcard and Backup MX** | The Wildcard and Backup MX (Mail Exchange) features are not supported for all Dynamic DNS providers. You could get more detailed information from their websites. |
| **Mail Extender** | If the mail server is defined with another name, please enter the name in this area. Such mail server will be used as backup mail exchange. |
| **Determine WAN IP** | There are two methods offered for you to choose:<br>● **WAN IP** - The IP address of the router's WAN interface will be used.<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. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

### 9.4.11.2 LAN DNS/DNS Forwarding

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.




To configure the profile, move the mouse cursor to any entry and click to open the following page.



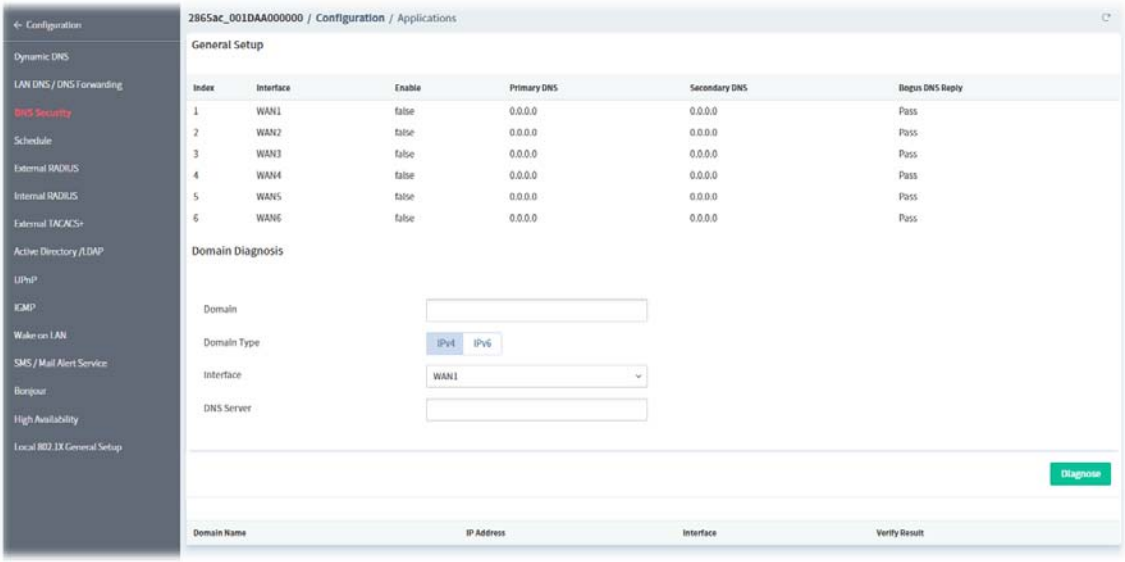

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Click to enable or disable the profile. |
| **Profile** | Enter a name to identify this profile. |
| **Domain Name** | Enter the domain name for the router to look for in DNS queries to intercept and reply to. |
| **DNS Server IP Address** | Enter the IP address of the DNS server you want to use for DNS forwarding. |
| | **CNAME(Alias Domain Name)** |
| **Index** | Displays the index number of the IP alias. |
| **CNAME** | Enter a domain name alias for the domain name. |
| **+Add** | After entering the CNAME, Click to save the setting and create a new entry. |
| | **IP Address List** |
| **Index** | Displays the index number of the IP address. |
| **IP Address** | The IP address entered here will be used for mapping with the domain name specified above. |
| **Same Subnet Reply** | Click to enable or disable the function.<br>If enabled, the router will only respond to the DNS request which coming from the same subnet of the IP address specified in this entry. |
| **+Add** | After entering the IP address, Click to save the setting and create a new |

| | |
|---|---|
| | entry. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

### 7.3.11.3 DNS Security

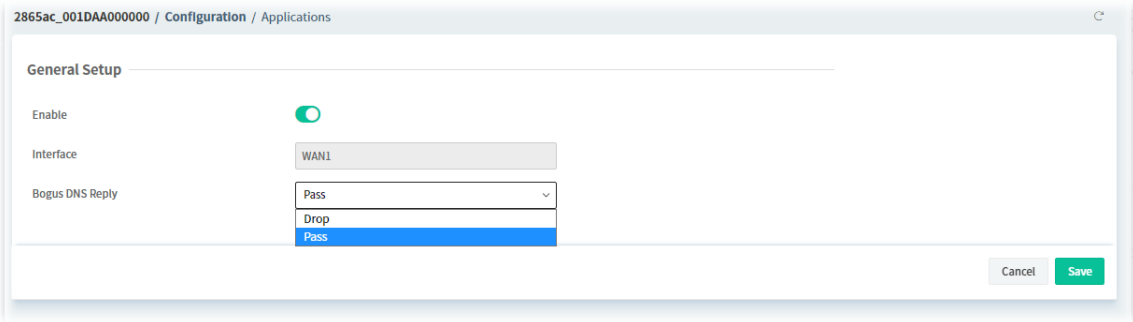
Domain Name System Security Extensions (DNSSEC) protects against DNS-based attacks by authenticating DNS responses from DNS resolvers.




These parameters are explained as follows:

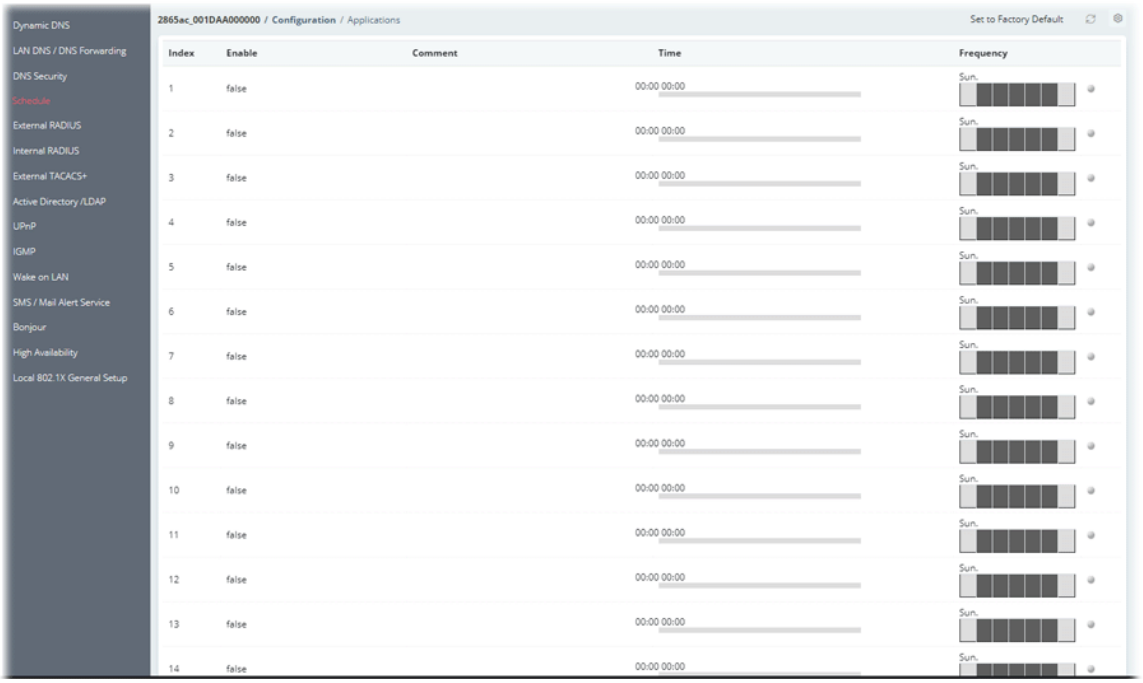
| Item | Description |
|---|---|
| | **General Setup** |
| **Index** | Displays the index number of the WAN interface. |
| **Interface** | Displays the WAN interface name for which DNS security is to be configured. |
| **Enable** | Displays if the DNS security is enabled (true) or disabled (false). |
| **Primary DNS** | Displays the primary DNS server IP address in effect for this WAN. |
| **Secondary DNS** | Displays the secondary DNS server IP address in effect for this WAN. |
| **Bogus DNS Reply** | Displays the action to be taken for DNS responses that fail authentication.<br>**Pass** – Pass DNS result.<br>**Drop** – Do not pass DNS result. |
| | **Domain Diagnosis** |
| **Domain** | Enter domain address to be diagnosed. |
| **Domain Type** | Select the type of IP address to be looked up.<br>● **IPv4**<br>● **IPv6** |
| **Interface** | Select the WAN port to be used for the lookup. |
| **DNS Service** | Enter the IPv4 / IPv6 address of the DNS server to be used for the lookup. |
| **Diagnose** | Click to begin DNS lookup. |

To configure the profile, move the mouse cursor to any index entry and click to open the following page.

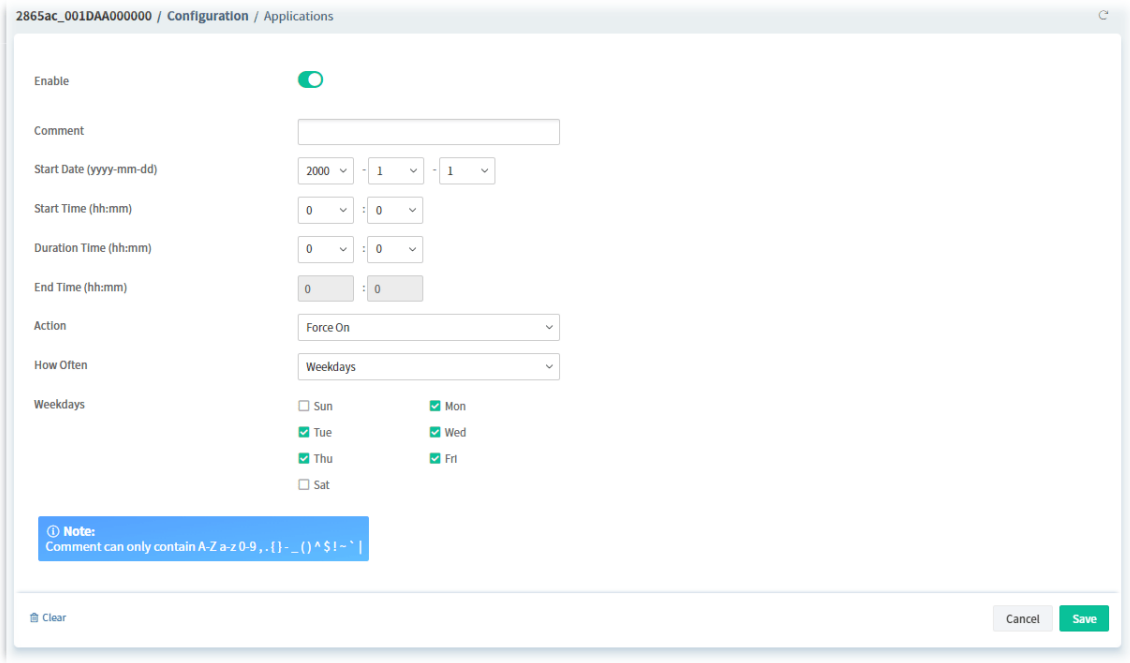



### 9.4.11.4 Schedule

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 configure the schedule profile, move the mouse cursor to any entry (1 to 15) and click to open the following page.



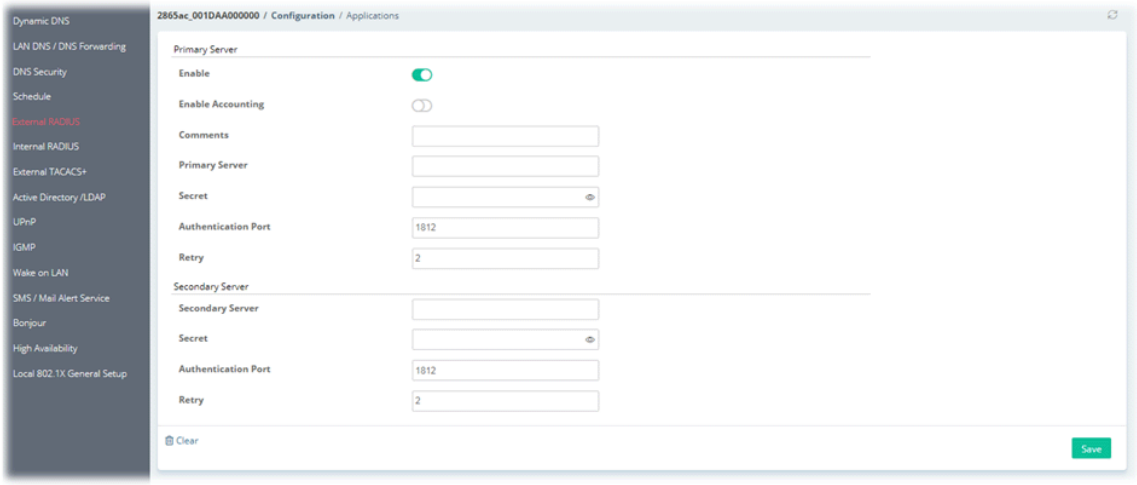

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Click to enable or disable the schedule profile. |
| **Comment** | Enter a name to identify this schedule entry. |
| **Start Date** | Select the date when the entry comes into effect. |
| **Start Time** | Select the time when the schedule is triggered. |
| **Duration Time** | Select how long the action lasts when the scheduled is triggered. |
| **End Time** | It will be calculated automatically when Start Time and Duration Time are configured well. |
| **Action** | Specify the action to take when the schedule is triggered.<br>**Force On** – The feature with which this schedule is associated will be turned on.<br>**Force Down** – The feature with which this schedule is associated will be turned off. |
| **How Often** | Specify how frequently the schedule is triggered.<br>● **Once** - The schedule is triggered once, on the **Start Date** at the **Start Time**, for the **Duration Time**.<br>● **Weekdays** - The schedule will be triggered repeatedly, starting on the **Start Date** at the **Start Time**, on the selected days of the week, at the **Start Time**, for the **Duration Time**.<br>● **Monthly, on date –** The router will only execute the action applied such schedule on the date (1 to 28) of a month.<br>● **Cycle duration –** Type a number as cycle duration. Then, any action applied such schedule will be executed per several days. For example, “3” is selected as cycle duration. That means, the action applied such schedule will be executed every three days since the date defined on the Start Date. |
| **Clear** | Clear all modifications on this page. |
| **Cancel** | Discard current modification and return to previous page. |

| | |
|---|---|
| **Save** | Save the current settings and return to previous page. |

### 9.4.11.5 External RADIUS

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

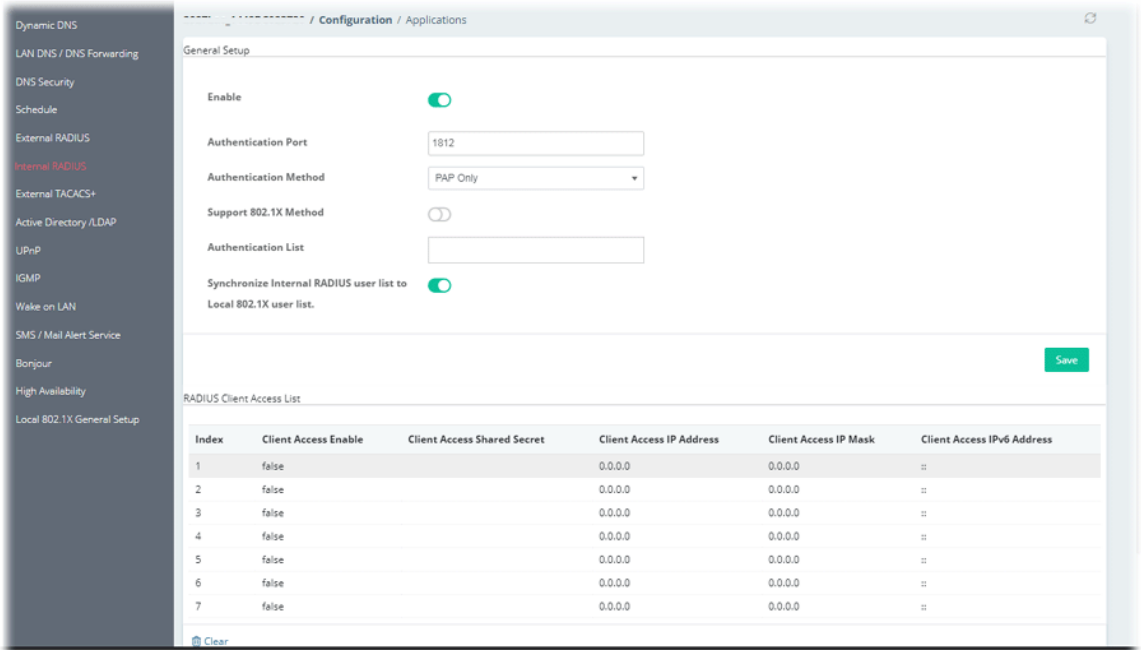



These parameters are explained as follows:

| Item | Description |
|---|---|
| | **Primary Server** |
| **Enable** | Click to enable or disable the server settings. |
| **Enable Accounting** | Click to enable or disable the accounting. |
| **Comments** | Enter a brief description for this profile. |
| **Primary Server** | Enter the IP address of RADIUS server. |
| **Secret** | The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret. |
| **Authentication Port** | Enter the UDP port number that the RADIUS server is using. |
| **Retry** | Set the number of attempts to perform reconnection with RADIUS server. |
| | **Secondary Server** |
| **Secondary Server** | Enter the IP address of RADIUS server. |
| **Secret** | The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret. |
| **Authentication Port** | Enter the UDP port number that the RADIUS server is using. |
| **Retry** | Set the number of attempts to perform reconnection with RADIUS server. |
| **Clear** | Clear all modifications on this page. |
| **Save** | Save the current settings and return to previous page. |

### 9.4.11.6 Internal 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.

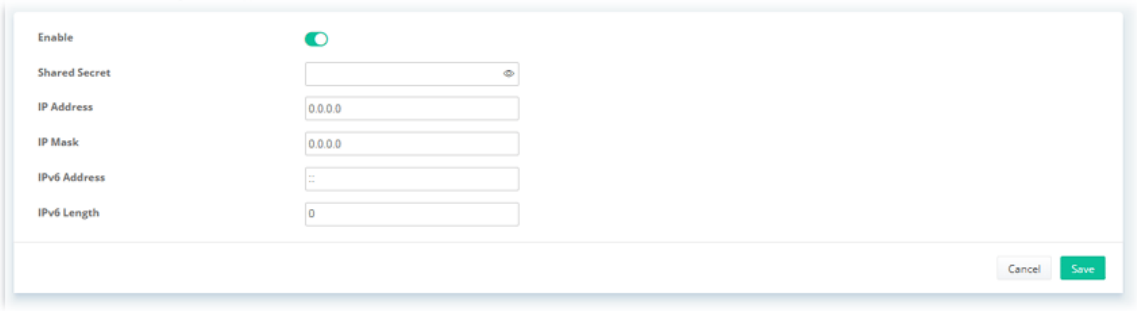



These parameters are explained as follows:

| Item | Description |
|---|---|
| | **General Setup** |
| **Enable** | Click to enable or disable the internal RADIUS server settings. |
| **Authentication Port** | Enter the UDP port for authentication messages. |
| **Authentication Method** | Specify the way to authenticate the wireless client.<br>● PAP only<br>● PAP/CHAP/MS-CHAP/MS-CHAPv2 |
| **Support 802.1X Method** | Click to enable or disable the Support 802.1X Method function**.**<br>● EAP_TTLS/PAP<br>● EAP_TTLS/MSCHAP<br>● EAP_TTLS/MSCHAPv2<br>● EAP_PEAP/MSCHAPv2 |
| **Authentication List** | Use the drop down list to choose the use profile. |
| **Synchronize Internal RADIUS user list to Local 802.1X user list** | Users can be authenticated by RADIUS server and local 802.1X to get certain network service. It is not necessary to create new user profiles (containing user accounts and user passwords) for RADIUS and local 802.1X respectively.<br>Simply select to update the 802.1X authentication list to match the RADIUS authentication list. |
| **Save** | Save the current settings |
| | **RADIUS Client Access List** |
| **Client Access Enable** | Displays the status (true or false) of the client entry.<br>Only clients that meet the criteria configured in the access list are allowed to access the RADIUS server. |
| **Client Access Shared Secret** | Displays the 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. |

| | |
|---|---|
| **Client Access IP Address** | Displays the base address of the IP block. |
| **Client Access IP Mask** | Displays the IP mask to configure the size of the IP block. |
| **Client Access IPv6 Address** | Displays the base address of the IPv6 block. |

To configure the profile, move the mouse cursor to any entry (1 to 10) and click to open the following page.

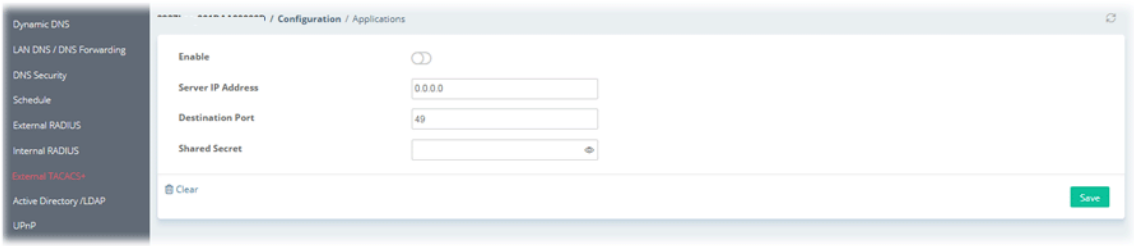



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Click to enable / disable the profile. |
| **Shared Secret** | Enter a text string. It is known to both the router's RADIUS server and the RADIUS client that is used to authenticate messages sent between them. |
| **IP Address** | Enter the base address of the IP block. |
| **IP Mask** | Enter the IP mask to configure the size of the IP block. |
| **IPv6 Address** | Enter the base address of the IPv6 block. |
| **IPv6 Length** | Enter the prefix length of the IPv6 block. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

### 9.4.11.7 External TACACS+

It means Terminal Access Controller Access-Control System Plus. It works like RADIUS does.



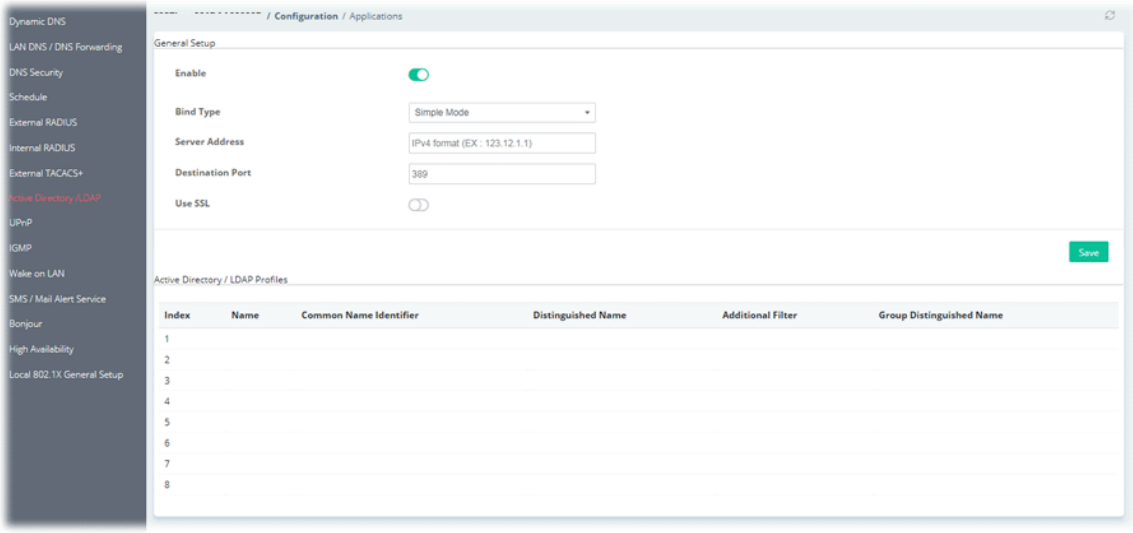

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Click to enable / disable the external TACACS+ server settings. |
| **Server IP Address** | Enter the IP address of the TACACS+ server. |
| **Destination Port** | Enter a port number used by the TACACS+ server. Port 49 is most common. |

| | |
|---|---|
| **Shared Secret** | Enter a text string. It 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. |
| **Clear** | Clear all modifications on this page. |
| **Save** | Save the current settings. |

### 9.4.11.8 Active Directory/LDAP

Lightweight Directory Access Protocol (LDAP) is an industry-standard protocol for maintaining and accessing directory information on a network. When used in conjunction with a Vigor router, LDAP can be used to authenticate VPN connection attempts.

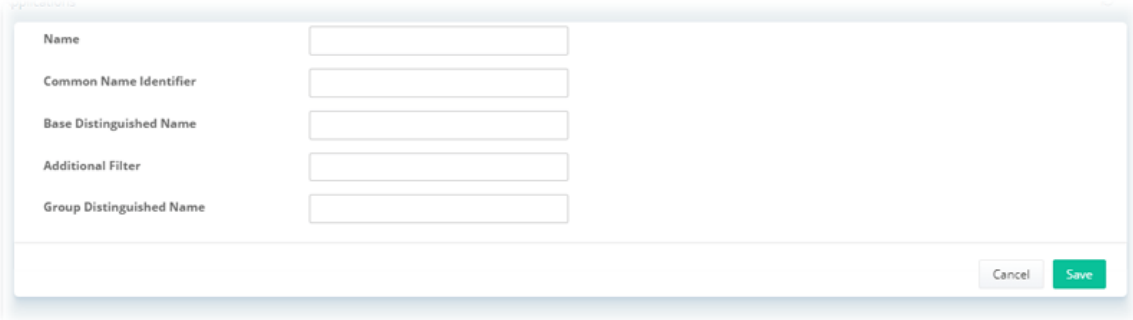



These parameters are explained as follows:

| Item | Description |
|---|---|
| | **General Setup** |
| **Enable** | Click to enable / disable the AD/LDAP function. |
| **Bind Type** | Select from one of 3 bind types:<br>● **Simple Mode** – Initiate bind operation (authentication) without performing user search.<br>● **Anonymous** – Bind anonymously, without supplying the distinguished name (DN) and password, and perform user search.<br>● **Regular Mode** – Same as Anonymous mode, except that the DN and password are sent to the server. |
| **Server Address** | Enter the network address of the LDAP server. |
| **Destination Port** | Enter a network port that the LDAP server listens on. The default ports are 389 for unsecured connections and 636 for LDAPS (LDAP over SSL) connections. |
| **Use SSL** | Click to enable or disable SSL.<br>If enabled, the router will use Secure Sockets Layer (SSL) for LDAP traffic. |
| **Regular DN** | Enter the LDAP Distinguished Name for authentication if **Bind Type** is set to **Regular Mode**. |
| **Regular Password** | Enter the LDAP Password for authentication if **Bind Type** is set to **Regular Mode**. |

| | |
|---|---|
| **Save** | Save the current settings. |
| | **Active Directory / LDAP Profiles** |
| **Index** | Displays the index number of the profile.<br>Up to 8 LDAP profiles can be configured. |
| **Name** | Displays the user-defined name that identifies this entry. |
| **Distinguished Name** | Displays the distinguished name (DN) configured in the profile. |

To configure the profile, move the mouse cursor to any entry (1 to 8) and click to open the following page.

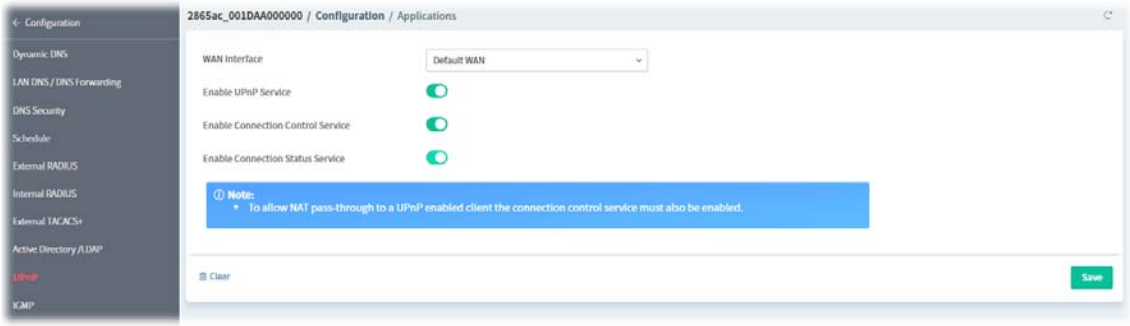



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Name** | Enter a name that identifies this profile. |
| **Common Name Identifier** | Enter a common name attribute, which is typically “cn” in most LDAP configurations. |
| **Base Distinguished Name** | Enter a starting point of user search in the LDAP directory, for example, dc=draytek,dc=com. |
| **Additional Filter** | Additional filter to be applied to the search request to identify eligible users.<br>For example,<br>– “OpenLDAP: (gidNumber=500)” |
| **Group Distinguished Name** | The base DN of the tree in the LDAP directory that contains groups, for example, ou=groups,dc=draytek,dc=com. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

### 9.4.11.9 UPnP

The Vigor supports UPnP (Universal Plug and Play), which is a suite of network protocols that simplifies network configuration.

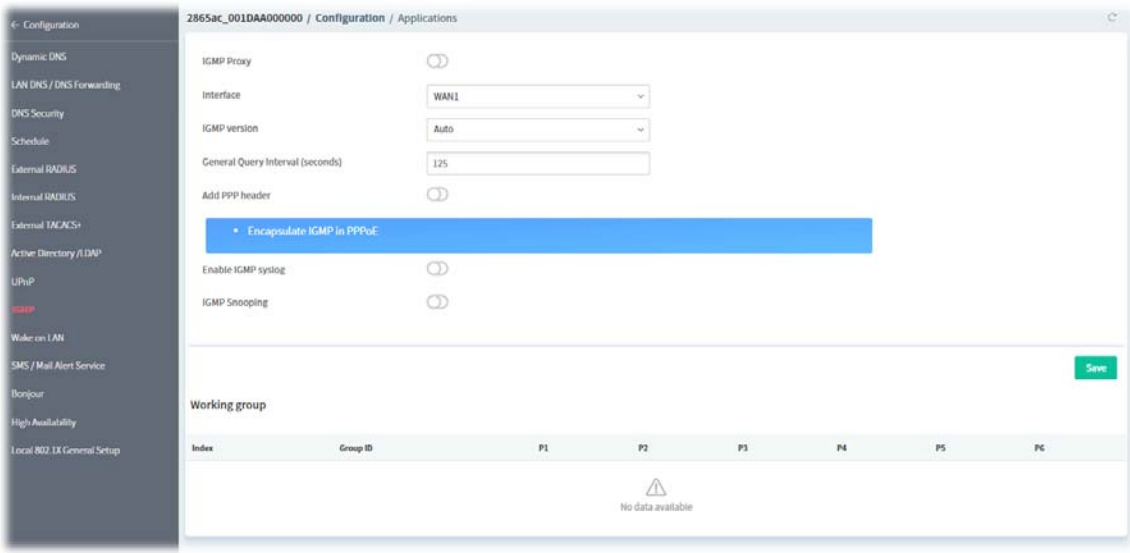



These parameters are explained as follows:

| Item | Description |
|---|---|
| **WAN Interface** | Select the WAN port on which ports will be opened in response to UPnP commands. |
| **Enable UPnP Service** | Click to enable or disable the UPnP function. |
| **Enable Connection Control Service** | Click to enable or disable the connection control service. |
| **Enable Connection Status Service** | Click to enable or disable the connection status service. |
| **Clear** | Clear all modifications on this page. |
| **Save** | Save the current settings. |

### 9.4.11.10 IGMP

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



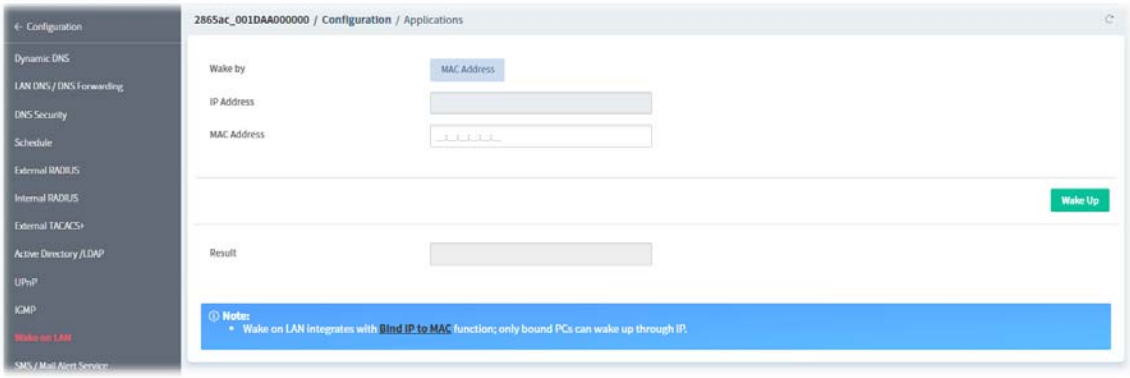

These parameters are explained as follows:

| Item | Description |
|---|---|
| **IGMP Proxy** | Click to enable or disable the IGMP proxy settings. |
| **Interface** | Select an interface for packets passing through. |
| **IGMP version** | At present, two versions (v2 and v3) are supported by Vigor router. Choose the correct version based on the IPTV service you subscribe. Or choose |

| | |
|---|---|
| | Auto. |
| **General Query Interval (seconds)** | Set a suitable time (unit: second) as the query interval to limit the frequency of query sent by Vigor router. |
| **Add PPP header** | Click to enable or disable the function.<br>If you have no idea to enable or disable, simply contact your ISP providers. |
| **Enable IGMP syslog** | Click to enable or disable the function.<br>If enabled, the router will store the IGMP status onto Syslog. |
| **Enable IGMP Snooping** | If enabled, the following option shall be configured.<br>**Enable IGMP Fast Leave** - If enabled, multicast for a group is immediately terminated when the last host in that group sends a “leave” message. |
| **Save** | Save the current settings. |
| | **Working group** |
| **Group ID** | Displays the ID port of the multicast group, which is within the IP range reserved for IGMP, 224.0.0.0 through 239.255.255.254. |
| **P1-PX** | Displays the LAN ports that have IGMP hosts joined to this multicast group. |

### 9.4.11.11 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.

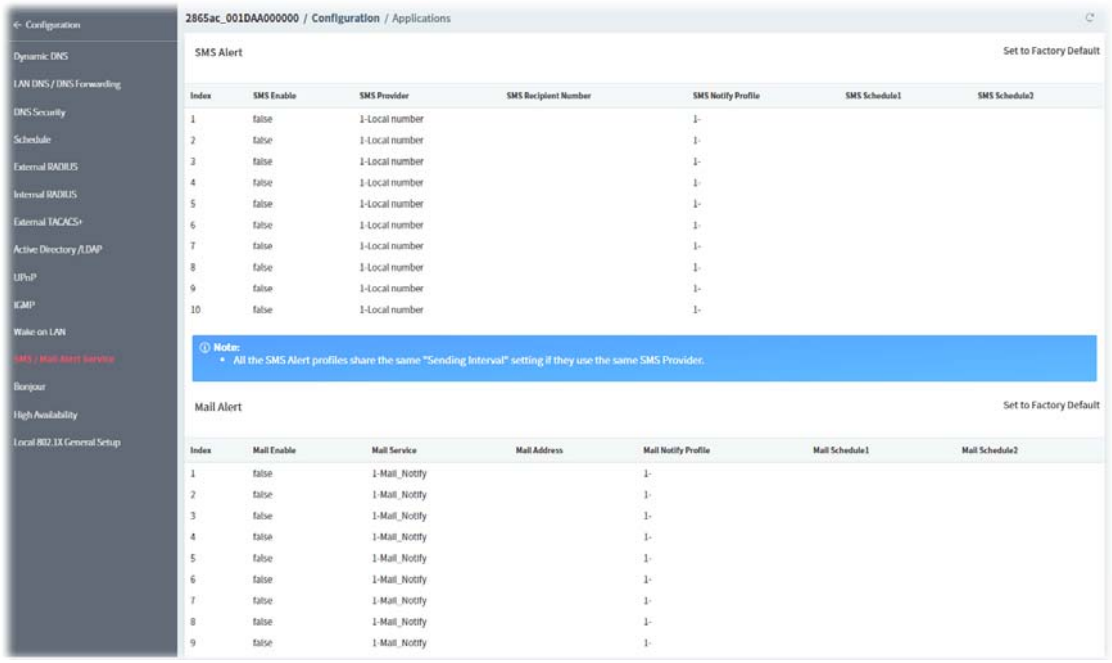



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Wake by** | To wake up the binded IP,<br>● **MAC Address** - Enter the correct MAC address of the host in MAC Address boxes. |
| **MAC Address** | Enter any one of the MAC address of the bound PCs. |
| **Result** | Displays the result of WOL execution. |
| **Wake Up** | Click to wake up the selected device. |

### 9.4.11.12 SMS/Mail Alert Service

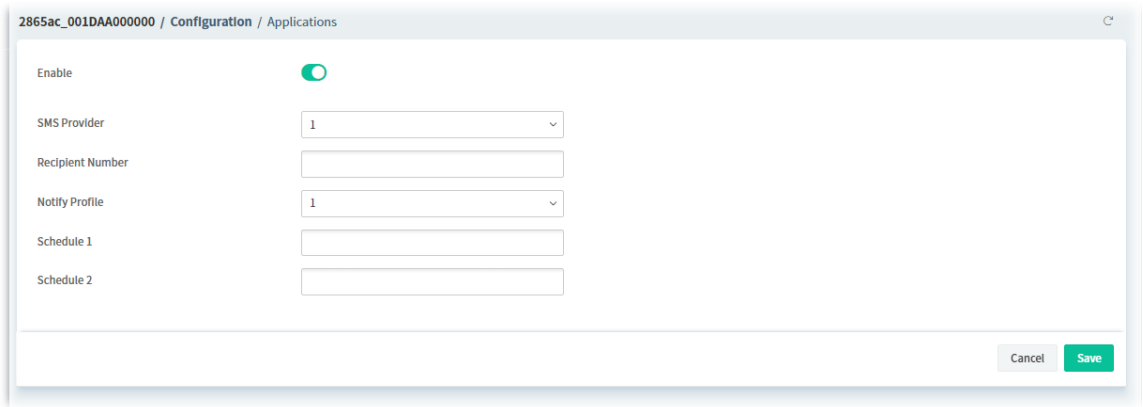
The function of SMS (Short Message Service)/Mail Alert is that Vigor router sends a message to user’s mobile or e-mail box through specified service provider to assist the user knowing the real-time abnormal situations.




These parameters are explained as follows:

| Item | Description |
|---|---|
| **SMS Alert** | It allows you to specify SMS provider, who will get the SMS, what the content is and when the SMS will be sent. |
| **Mail Alert** | It allows you to specify Mail Server profile, who will get the notification e-mail, what the content is and when the message will be sent. |

To configure the SMS alert profile, move the mouse cursor to any entry (1 to 10) and click to open the following page.

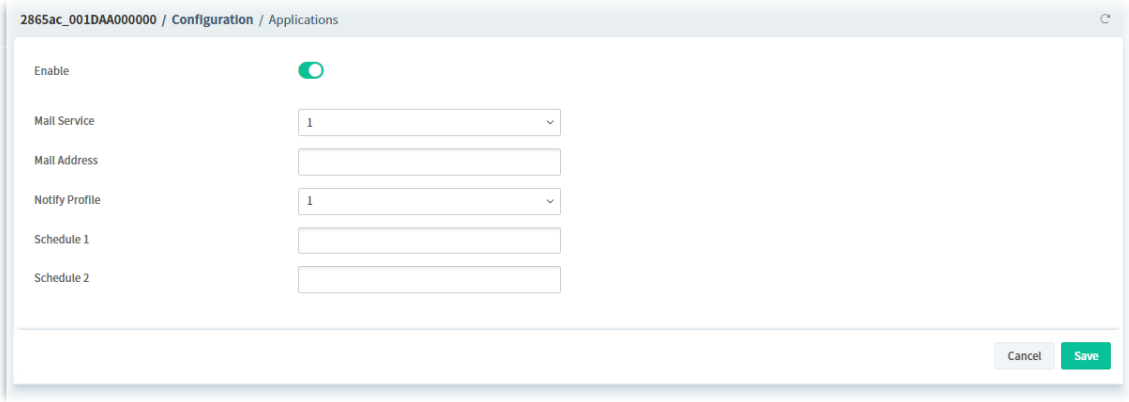



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Click to enable or disable the SMS alert profile. |
| **SMS Provider** | Use the drop down list to choose SMS service provider. |
| **Recipient Number** | Enter the phone number of the one who will receive the SMS. |
| **Notify Profile** | Use the drop down list to choose a message profile. The recipient will get the content stated in the message profile. |
| **Schedule 1 / 2** | Enter the schedule number that the SMS will be sent out. |

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

To configure the mail alert profile, move the mouse cursor to any entry (1 to 10) and click to open the following page.

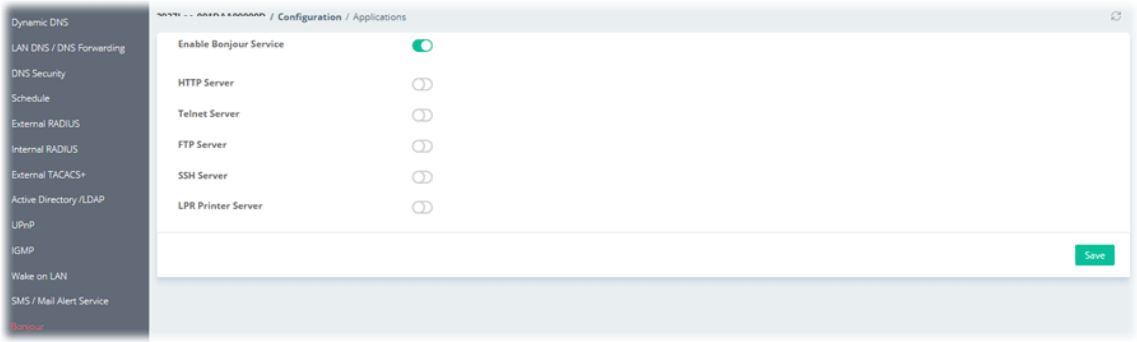



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Click to enable or disable the mail alert profile. |
| **Mail Service** | Use the drop down list to choose mail service object. |
| **Mail Address** | Enter the e-mail address of the one who will receive the notification message. |
| **Notify Profile** | Use the drop down list to choose a message profile. The recipient will get the content stated in the message profile. |
| **Schedule 1 / 2** | Enter the schedule number (0~15) that the notification will be sent out. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

### 9.4.11.13 Bonjour

Bonjour is a service discovery protocol which is a built-in service in Mac OS X; for Windows or Linux platform, there is correspondent software to enable this function for free.



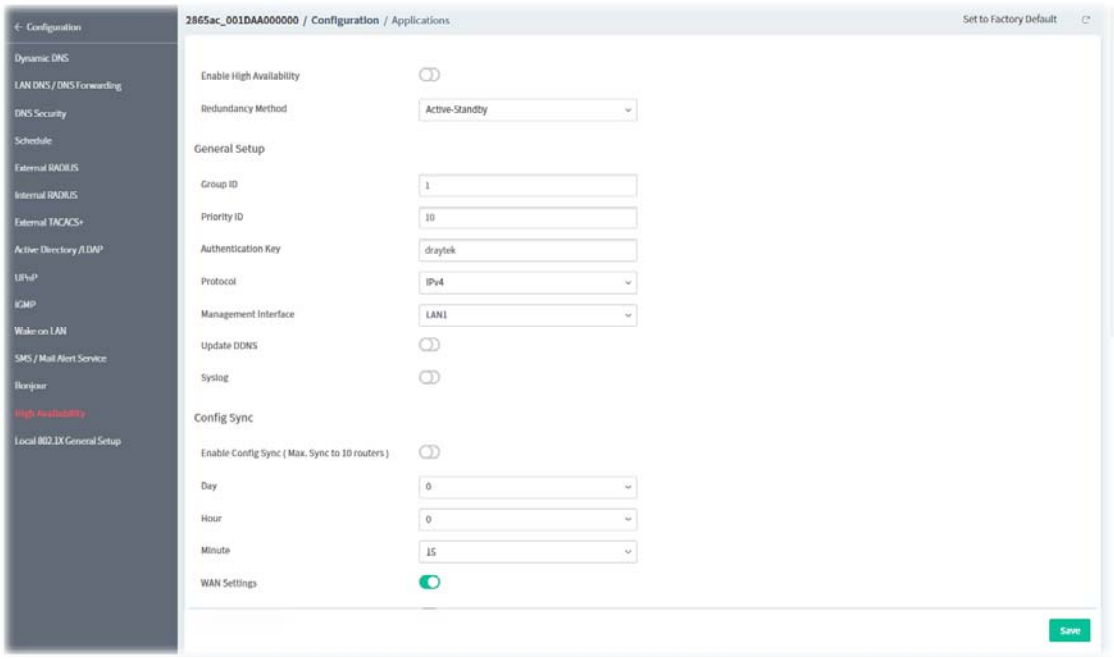

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Enable Bonjour Service** | Click to enable or disable the Bonjour service.<br>With bonjour service enabled, Vigor router can share the service (e.g., |

| | |
|---|---|
| | HTTP service, Telnet service, FTP service, SSH service, LRP Printer server and etc.) to the LAN clients. |
| **Save** | Save the current settings and return to previous page. |

### 9.4.11.14 High Availability

The High Availability (HA) feature of the router provides redundancy of network resources, and reduces downtime in case of component failure.

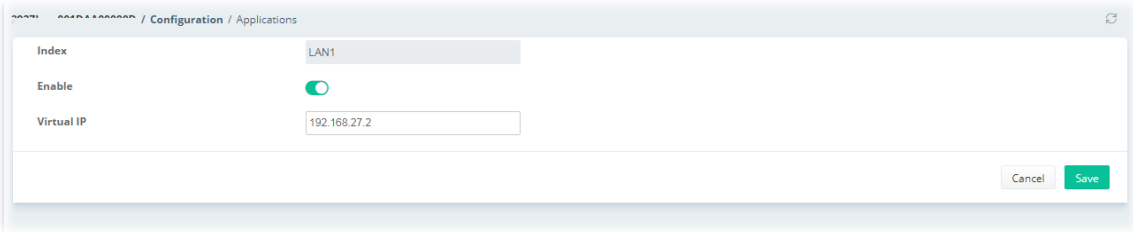



These parameters are explained as follows:

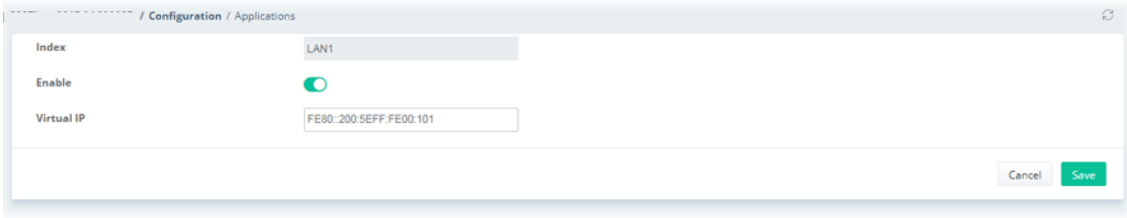
| Item | Description |
|---|---|
| **Enable High Availability** | Click to enable or disable the HA function. |
| **Redundancy Method** | Select the redundancy method (Hot-Standby or Active-Standby) for high availability. |
| | **General Setup** |
| **Group ID** | Enter a value (1~255). Each router must be specified with one group ID. Different routers with the same ID value will be categorized into the same group. |
| **Priority ID** | Enter a value (1~30). Different routers must be configured with different IDs. |
| **Authentication Key** | Enter an authentication key up to 31 characters long. |
| **Protocol** | Select the IP protocol (IPv4 or IPv6) to be used for DARP. |
| **Management Interface** | Select the interface to be used for DARP negotiation between routers. |
| **Update DDNS** | Click to enable or disable the function.<br>If enabled, the router will update the DDNS server for the secondary device when the primary router fails. |
| **Syslog** | Click to enable or disable the function. If enabled, the router will record required information on Syslog. |

| | Config Sync |
|---|---|
| **Enable Config Sync** | Click to enable or disable the Config Sync function. |
| **Day / Hour / Minute** | The primary router will synchronize its configuration with secondary routers at every specified time interval. |
| **WAN Settings** | Click to enable or disable the WAN settings.<br>WAN settings will be excluded when executing configuration synchronization. |
| **Enable Config Inherit** | Click to enable or disable the function.<br>The configuration inherits will be executed only when the device (router) plays the role of the master device.<br>Once another device with the priority ID higher than this device is ready to take over the management as the master device, after acting as the primary master for a while, this device will sync the configuration to all members in the same group and return to the role of the backup device (secondary master).<br>**Config Inherit**... for ( ) minute - Enter a value. |
| **IPv4** | Set IPv4 virtual IP for each LAN interface. |
| **IPv6** | Set IPv6 virtual IP for each LAN interface. |
| **Save** | Save the current settings and return to previous page. |

To configure the IPv4 profile, move the mouse cursor to any entry and click to open the following page.

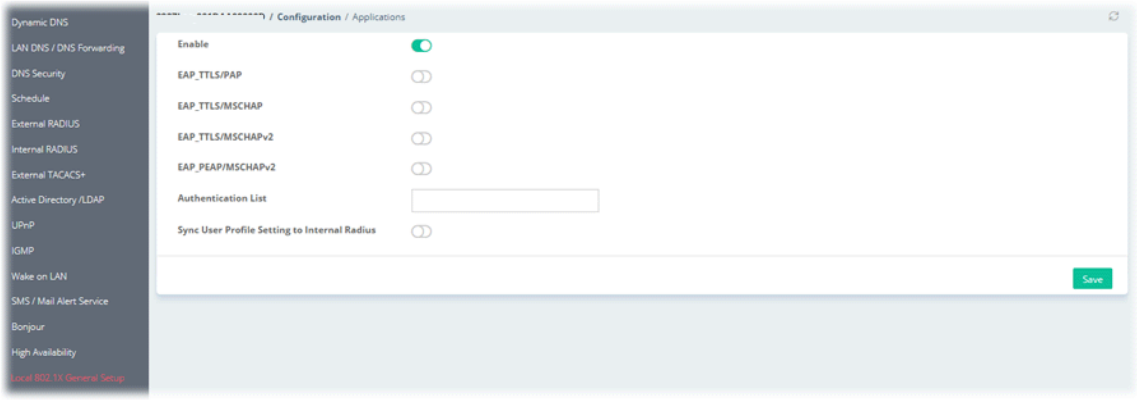



To configure the IPv6 profile, move the mouse cursor to any entry and click to open the following page.



### 9.4.11.15 Local 802.1X General Setup

It allows you to configure general settings for Local 802.1X server built in Vigor router.




These parameters are explained as follows:

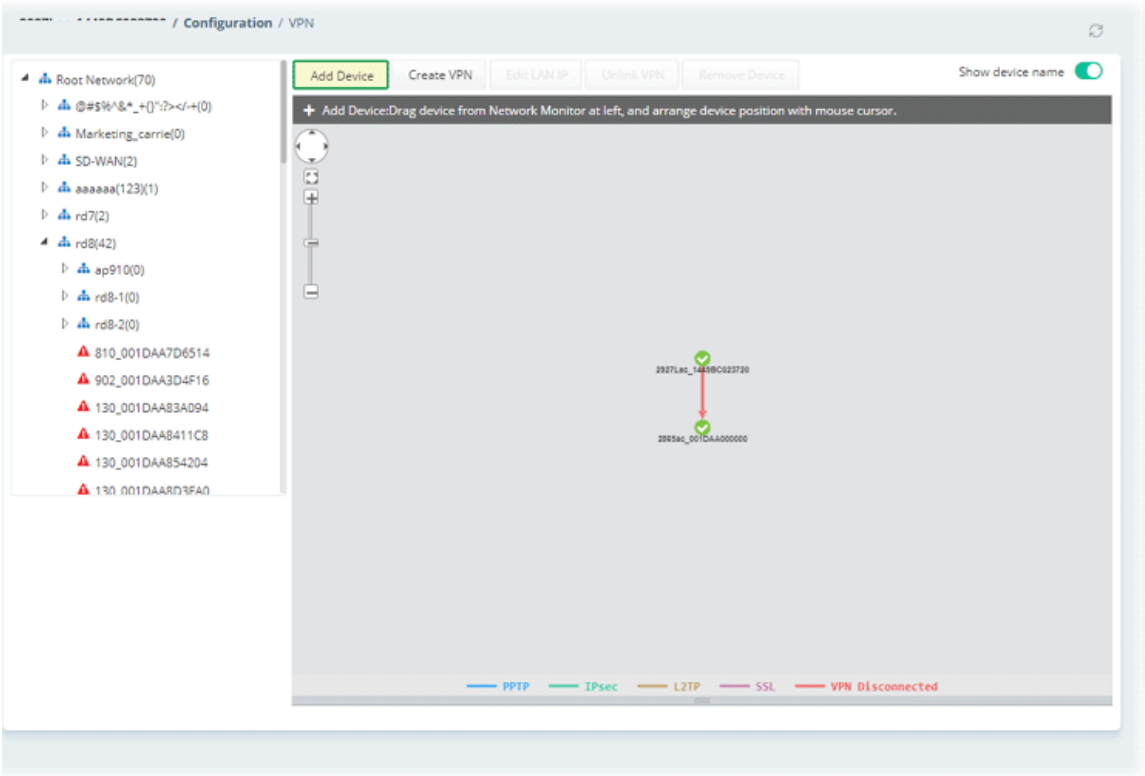
| Item | Description |
|---|---|
| **Enable** | Click to enable or disable the function. |
| **EAP_TTLS/PAP** | Click to enable or disable the EAP_TTLS/PAP server certificate. |
| **EAP_TTLS/MSCHAP** | Click to enable or disable the EAP_TTLS/MSCHAP server certificate. |
| **EAP_TTLS/MSCHAPv2** | Click to enable or disable the EAP_TTLS/MSCHAPv2 server certificate. |
| **EAP_PEAP/MSCHAPv2** | Click to enable or disable the EAP_PEAP/MSCHAPv2 server certificate. |
| **Authentication List** | Select user profiles. |
| **Sync User Profile Settings to Internal Radius** | Click to enable or disable the function.<br>It will enable/disable setting for both Internal RADIUS and Local 802.1X synchronize for all of the user profiles. |
| **Save** | Save the current settings. |

### 9.4.12 VPN

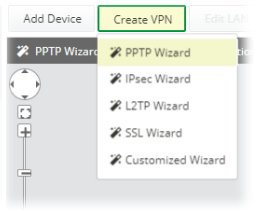
A Virtual Private Network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. In short, by VPN technology, you can send data between two computers across a shared or public network in a manner that emulates the properties of a point-to-point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

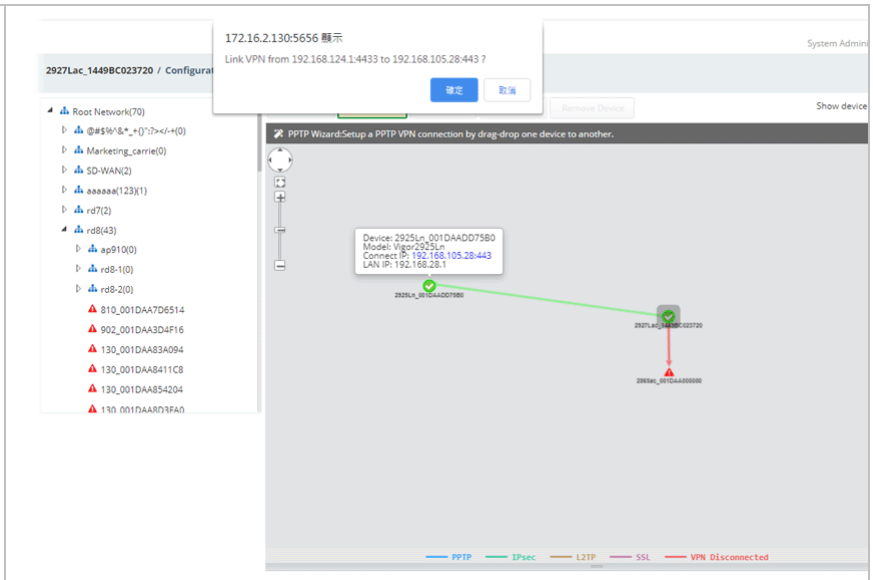
#### 9.4.12.1 VPN Wizard

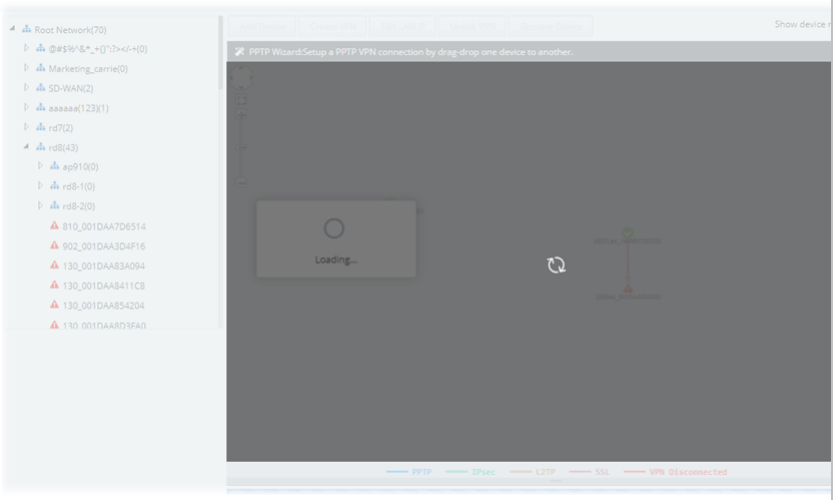
This page displays the VPN status related to the specified device.



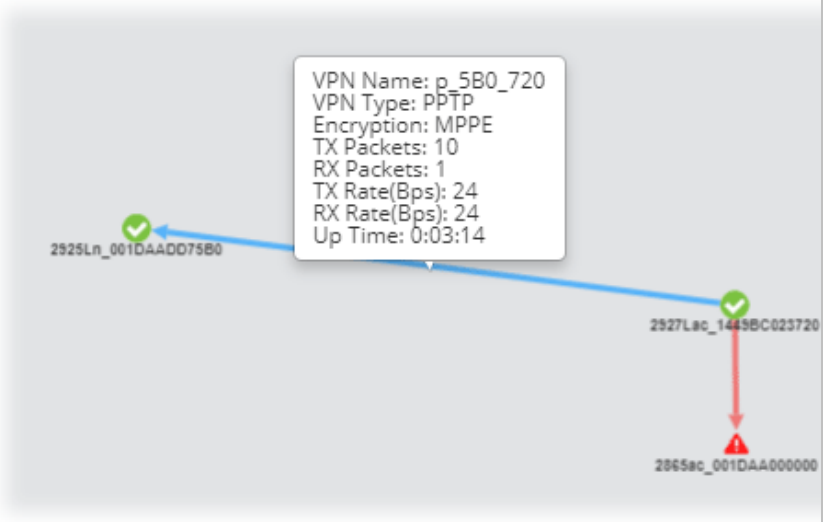

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Add Device** | Click this button to add a device for building VPN connection. If you do not click this button first, you can not drag any device from **Network** view. |
| **Create VPN**<br>  | To build a quick VPN connection with **PPTP/IPsec/L2TP/SSL/customized settings**, simply click this button and choose one of the wizards for establishing VPN. Then, drag and drop one device to another. Here we take PPTP Wizard as an example. |


172.16.2.130:5656 顯示
Link VPN from 192.168.124.1:4433 to 192.168.105.28:443 ?
確定
取消
PPTP Wizard:Setup a PPTP VPN connection by drag-drop one device to another.
Device: 2925Ln_001DAADD75B0
Model: Vigor2925Ln
Connect IP: 192.168.105.28:443
LAN IP: 192.168.28.1
PPTP
IPsec
L2TP
SSL
VPN Disconnected

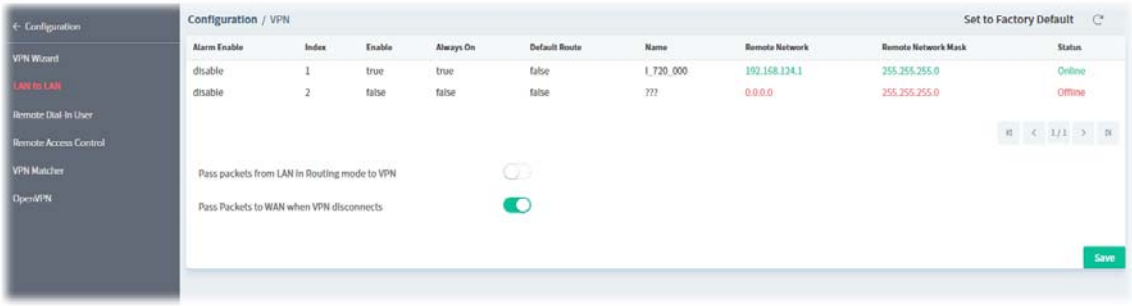

PPTP Wizard:Setup a PPTP VPN connection by drag-drop one device to another.
Loading...

Add Device
Create VPN
Add Device:Drag device from Network Monitor at left, and arrange device position with mouse cursor.
PPTP
IPsec
L2TP
SSL
VPN Disconnected

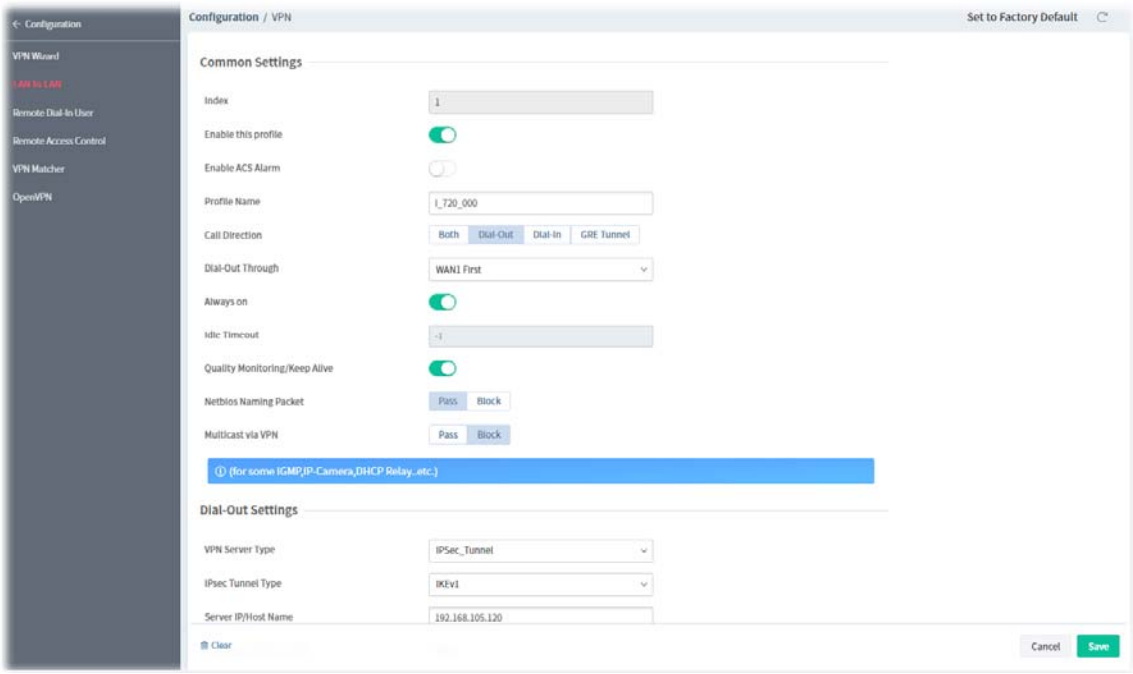
| | |
|---|---|
| |  |
| **Edit LAN IP** | If there is LAN IP segment conflict in VPN connection, please select that device and click this button to change LAN IP setting. |
| **Unlink VPN** | To disconnect a VPN connection, Click this button and move the mouse cursor to the VPN connection that you want to disconnect. |
| **Remove Device** | Click to remove the selected device without VPN connection. |
| **Show device name** | Click to display / hide the name of the device. |

### 9.4.12.2 LAN to LAN

To create a LAN to LAN connection for the selected CPE, choose **LAN to LAN.** You can create up to 32 profiles for a CPE.



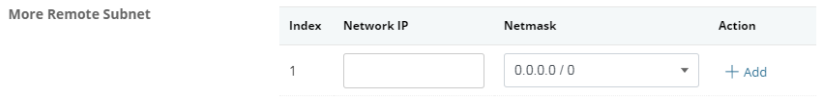
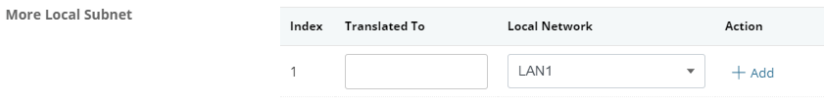
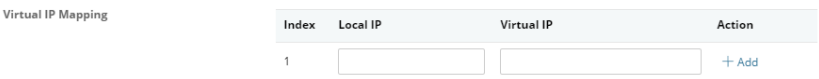

To create a new LAN to LAN profile, click the bottom one entry. To configure the LAN to LAN profile, move the mouse cursor to any entry and click to open the following page.




These parameters are explained as follows:

| Item | Description |
|---|---|
| | **Common Settings** |
| **Index** | Displays the index number of the profile. |
| **Enable this profile** | Click to enable or disable this profile. |
| **Enable ACS Alarm** | Click to enable or disable the function. |
| **Profile Name** | Enter the name of the profile. |
| **Call Direction** | Specify the allowed call direction of this LAN-to-LAN profile.<br>● **Both**<br>● **Dial-Out**<br>● **Dial-In**<br>● **GRE Tunnel** |
| **Dial-Out Through** | Select the WAN connection for connections made using this profile. This setting is useful for dial-out only. |
| **Always On** | Click to enable or disable the function to maintain an always on dial-out connection. However, if disabled,<br>**Idle Timeout** - Set a value if Always On is disabled. The router will close connection if no activity is observed in the VPN connection for this many seconds. |
| **Quality Monitoring /Keep Alive** | Click to enable or disable the function. |
| **Netbios Naming Packet** | Specifies whether to allow NetBIOS naming packets to traverse through the VPN tunnel.<br>● **Pass** – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.<br>● **Block** – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel. |

| | |
|---|---|
| **Multicast via VPN** | Specifies whether to allow multicast packets to traverse through the VPN tunnel.<br>● **Pass** – Click this button to let multicast packets pass through the router.<br>● **Block** – This is default setting. Click this button to let multicast packets be blocked by the router. |
| | **Dial-Out Settings** |
| **VPN Server** | Select the VPN protocol to be used**.** |
| **IPsec Tunnel Type** | Select IKEv1 or IKEv2. |
| **Server IP/Host Name** | Enter an IP address or DNS host name of remote VPN host. |
| **Dial-Out Schedule Profile** | Connect and disconnect according to schedule profiles.<br>Up to four schedule profiles can be specified. |
| | **IKE Phase 1 Settings** |
| **Mode** | Select IKE phase 1 mode. **Main** mode is more secure than **Aggressive** mode since more exchanges are done in a secure channel to set up the IPsec session.<br>● **Main Mode**<br>● **Aggressive Mode** |
| **Authentication** | Select **PSK**(IKE Pre-shared key) or **X509** (X.509 digital signature). |
| **Pre-Shared Key** | It is available when PSK is selected as Authentication.<br>Enter the PSK. |
| **Local ID** | Enter a string. |
| **Proposal Encryption** | Select an proposal encryption mode. |
| **Proposal ECDH Group** | Select an proposal ECDH group (e.g., G14). |
| **Proposal Authentication** | Select **SHA256** or **SHA1.** |
| | **IKE Phase 2 Settings** |
| **Security Protocol** | Select the dial-out protocol.<br>● **ESP(High)**<br>● **AH(Medium)** |
| **Proposal Encryption** | Select an proposal encryption mode. |
| **Proposal Authentication** | Select **All**, **SHA256**, **SHA1** or **None.** |
| | **IKE Advanced Settings** |
| **Phase 1 Key Lifetime** | For security reason, the lifetime of key should be defined. The default value is 28800 seconds. |
| **Phase 2 Key Lifetime** | For security reason, the lifetime of key should be defined. The default value is 3600 seconds. |
| **Phase 2 Network ID** | In **Aggressive** mode, Local ID is on behalf of the IP address while identity authenticating with remote VPN server. The length of the ID is limited to 47 characters. |
| **Enable Perfect Forward Secret** | Click to enable or disable the function.<br>If enabled, the IKE Phase 1 key will be reused to avoid the computation |

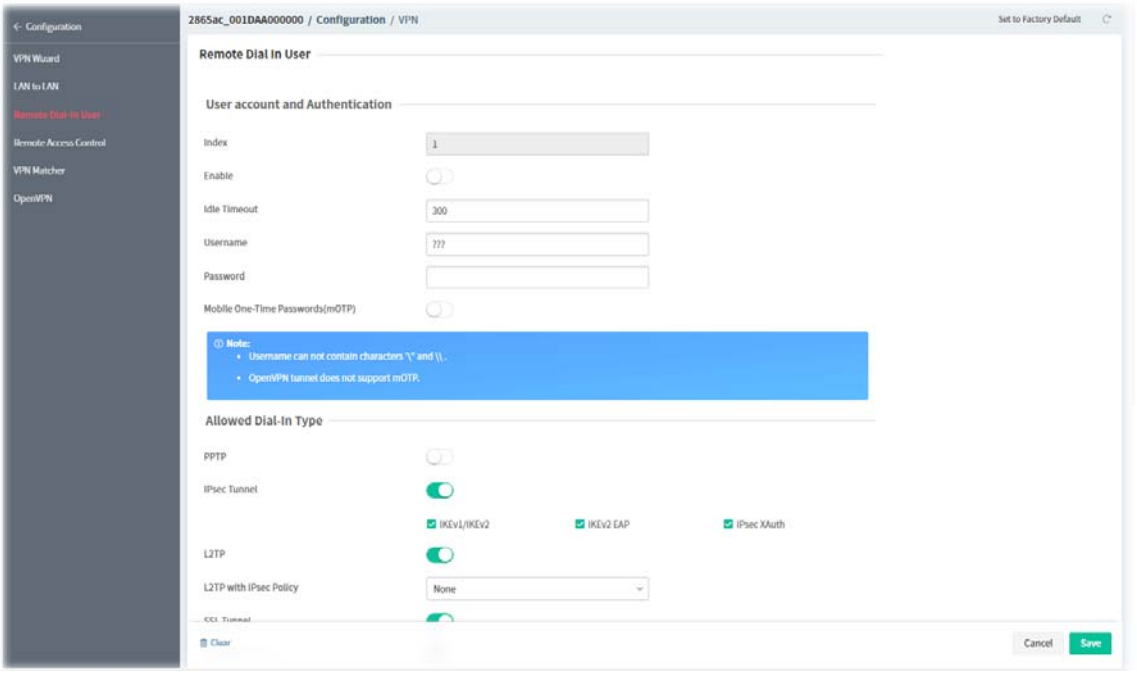
| | |
|---|---|
| | complexity in phase 2. |
| **Ping to Keep Alive** | Click to enable or disable the transmission of PING packets to a specified IP address.<br>**PING Target IP** - Enter the IP address of the remote host that located at the other-end of the VPN tunnel. |
| | **TCP/IP Network Settings** |
| **Local Network IP / Mask** | Display the local network IP and mask for TCP / IP configuration. You can modify the settings if required. |
| **Remote Network IP / Mask** | Add a static route to direct all traffic destined to this Remote Network IP Address/Remote Network Mask through the VPN connection. |
| **More Remote Subnet** | Add a static route to direct all traffic destined to ***more*** Remote Network IP Addresses/ Remote Network Masks through the VPN connection.<br>  <br>Enter the IP address and the mask address. Click +Add to save the settings and create a new entry. |
| **Mode** | If the remote network only allows one IP address for the local network, select **NAT**; otherwise, select **Routing**.<br>● **Routing**<br>● **NAT** |
| **RIP via VPN** | Specifies the direction of Routing Information Protocol (RIP) packets. |
| **Translate Local Network** | It is available when Routing is selected as Mode.<br>Click to enable or disable the function. This is usually used when you find there are several subnets behind the remote VPN router.<br>If enabled, the function of Change Default Route to this VPN tunnel will be disabled. And please configure the following options.<br>**Type** - There are two types (Translate Whole Subnet, Translate Specific IP) for you to choose.<br>For Translate Whole Subnet;<br>● **Local Subnet** - Select the LAN whose IP addresses are to be translated.<br>● **Translated IP** - Specify an IP address.<br>● **More Local Subnet** - Add more subnets.<br>  <br>For Translate Specific IP,<br>● **Virtual IP Mapping** - Specify the local IP address and the mapping virtual IP address.<br>  |
| **Change Default Route to this VPN** | Click to enable or disable this option .<br>Select this option to direct all traffic that is not LAN-bound to this VPN tunnel. |
| **Clear** | Clear all modifications on this page. |

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

### 9.4.12.3 Remote Dial-In User

The system administrator can manage remote access by maintaining a table of remote user profiles, so that users can be authenticated via VPN connection.

To configure the remote dial-in user profile, move the mouse cursor to any entry and click to open the following page.




These parameters are explained as follows:

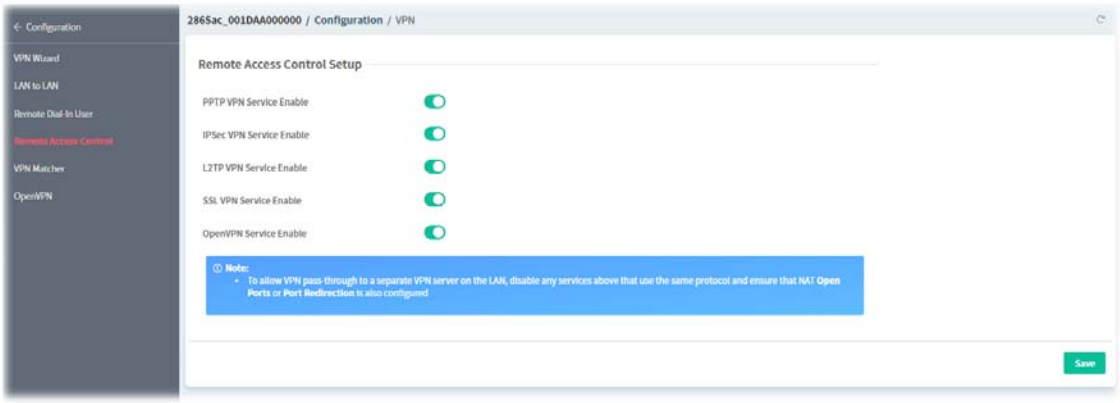
| Item | Description |
|---|---|
| | **User account and Authentication** |
| **Index** | Displays the index number of the user account profile. |
| **Enable** | Click to enable or disable the user account profile. |
| **Idle Timeout** | Set the allowed idle time before the router disconnects the VPN connection. |
| **Username** | Set a username used for PPTP, L2TP or SSL Tunnel dial-in type |
| **Password** | Set a password used for PPTP, L2TP or SSL Tunnel dial-in type |
| **Mobile One-Time Passwords (mOTP)** | Click to enable or disable one-time passwords (Mobile-OTP).<br>If enabled, please<br>**PIN Code -** Enter the code for authentication (e.g, 1234). |

| | |
|---|---|
| | **Secret -** Enter the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6). |
| | **Allowed Dial-In type** |
| **PPTP / IPsec Tunnel / L2TP / L2TP with IPsec Policy / SSL Tunnel / OpenVPN Tunnel** | Click to enable (select) or disable (deselect) the PPTP / IPsec Tunnel / L2TP / L2TP with IPsec Policy / SSL Tunnel / OpenVPN Tunnel protocol. |
| **Specify Remote Node** | Click to enable or disable the function.<br>The IP address of the remote VPN client (Remote Client IP) or the Peer ID (used in IKE aggressive mode) can be optionally specified.<br>**Remote Client IP -** Enter the IP address for remote client.<br>**Or Peer ID -** Enter the string for peer ID. |
| **Netbios Naming Packet** | It is available when Specify Remote Node is disabled.<br>Specifies whether to allow NetBIOS naming packets to traverse through the VPN tunnel.<br>● **Pass** – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.<br>● **Block** – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel. |
| **Multicast via VPN** | It is available when Specify Remote Node is disabled.<br>Specifies whether to allow multicast packets to traverse through the VPN tunnel.<br>● **Pass** – Click this button to let multicast packets pass through the router.<br>● **Block** – This is default setting. Click this button to let multicast packets be blocked by the router. |
| | **Subnet** |
| **Subnet** | Select an interface. |
| **Assign Static IP** | Click to enable or disable the function.<br>**IP Address -** Enter a static IP address. |
| **Digital Signature(X.509)** | It is available when Specify Remote Node is disabled.<br>Click to enable or disable the authentication using X.509 Peer IDs. If enabled, please<br>**Digital Signature(X.509) Index -** Select an X.509 profile. |
| | **IKE Authentication Method** |
| **Enable Pre-Shared Key** | It is available when Specify Remote Node is enabled.<br>Click to enable or disable the function. If enabled, please<br>**Pre-Shared Key -** Enter an IKE PSK. |
| **Digital Signature(X.509)** | Click to enable or disable the authentication using X.509 Peer IDs. If enabled, please<br>**Digital Signature(X.509) Index -** Select an X.509 profile. |
| | **IPsec Security Method** |
| **Medium(AH)** | Click to enable or disable the function that data will be authenticated, but not be encrypted. |

| | |
|---|---|
| **High(ESP)** | The payload (data) will be encrypted and authenticated. |
| **Local ID (optional)** | Click to enable or disable the setting.<br>Specify a local ID to be used when establishing a LAN-to-LAN VPN connection using IKE aggressive mode. |
| **Clear** | Clear all modifications on this page. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

### 9.4.12.4 Remote Access Control

The Vigor router supports several protocols for VPNs, all of which can be enabled or disabled independently of one another.

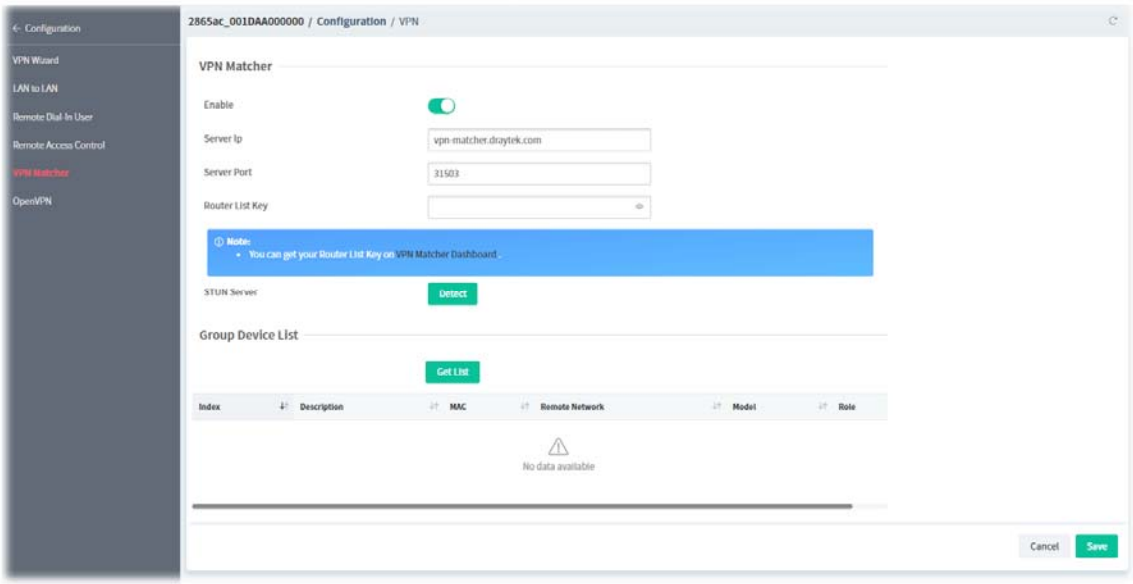



These parameters are explained as follows:

| Item | Description |
|---|---|
| **PPTP VPN Service Enable** | Click to enable or disable the service.<br>If enabled, this VPN is easy to set up, has low overhead, and moderately secure. |
| **IPsec VPN Service Enable** | Click to enable or disable the service. |
| **L2TP VPN Service Enable** | Click to enable or disable the service. |
| **SSL VPN Service Enable** | Click to enable or disable the service. |
| **OpenVPN Service Enable** | Click to enable or disable the service.<br>If enabled, this VPN offers a convenient way for users to build VPN between local end and remote end. |
| **Save** | Save the current settings |

### 9.4.12.5 VPN Matcher

The VPN Matcher server can help two Draytek routers behind NAT establish a secure VPN tunnel for data transmission between each other.



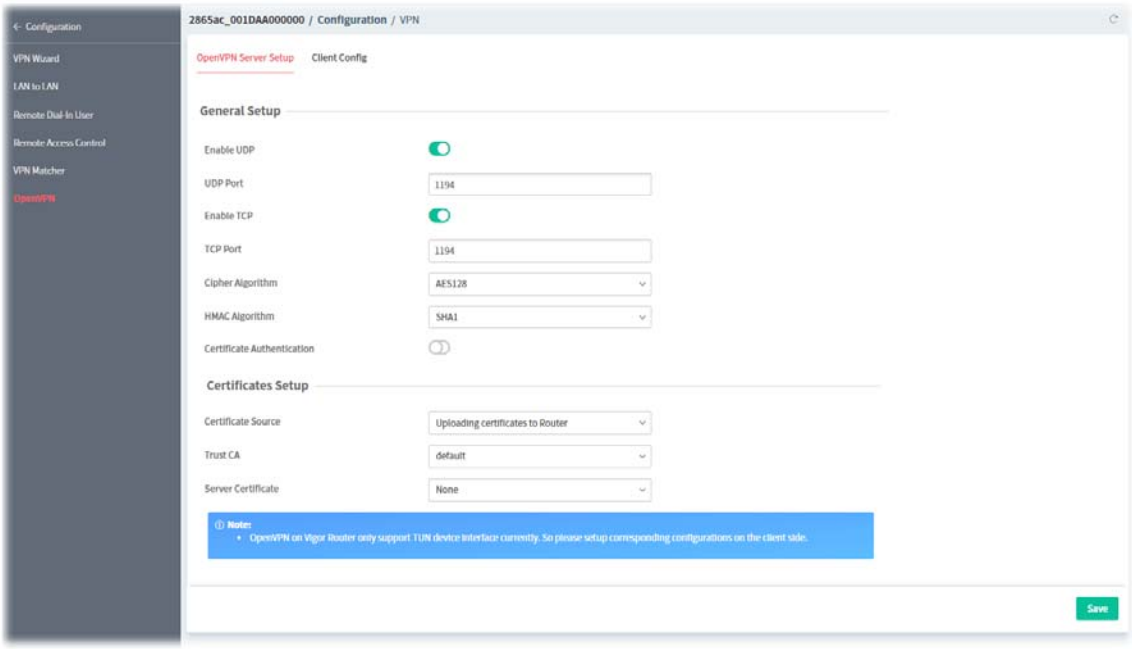

These parameters are explained as follows:

| Item | Description |
|---|---|
| | **VPN Matcher** |
| **Enable** | Click to enable or disable the function of VPN Matcher Setup. |
| **Server IP / 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. |
| | **Group Device List** |
| **Get List** | After entering the Authkey above, click to get available Vigor router which is within the same group as this device. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings |

### 9.4.12.6 OpenVPN

#### 9.4.12.6.1 OpenVPN Server Setup

OpenVPN requires the use of certificates. Certificates generated by the third party can be imported to your host and ready for use by Vigor router.



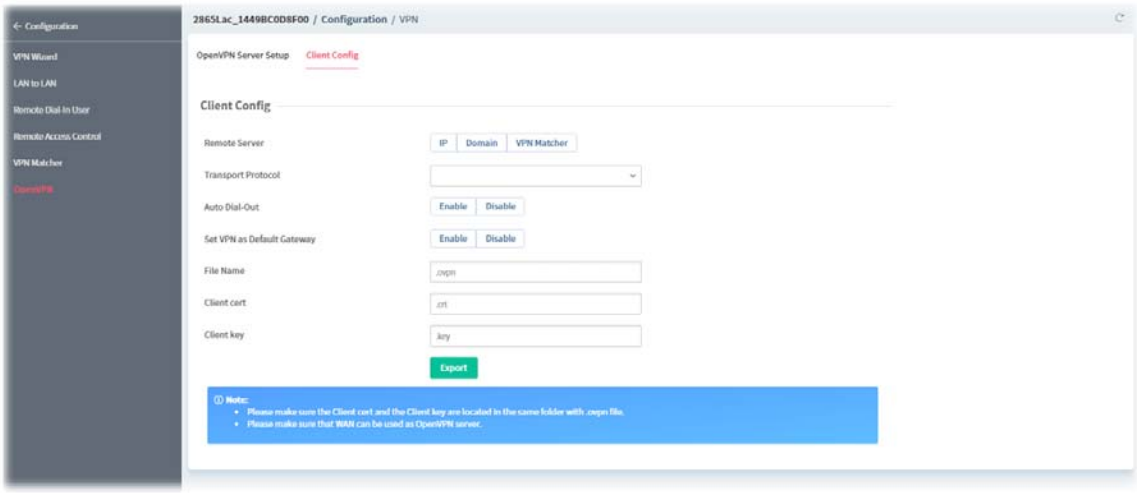

These parameters are explained as follows:

| Item | Description |
|---|---|
| | **General Setup** |
| **Enable UDP** | Click to enable or disable UDP protocol for OpenVPN connections. If enabled, please<br>**UDP Port** - Enter the UDP port number. |
| **Enable TCP** | Click to enable or disable the TCP protocol for OpenVPN connections. If enabled, please<br>**TCP Port** - Enter the TCP port number. |
| **Cipher Algorithm** | Select the desired cipher algorithm. |
| **HMAC Algorithm** | Select the desired HMAC hash algorithm. It is used to validate the data integrity and authenticity of the VPN data. |
| **Certificate Authentication** | Click to enable or disable the settings. If enabled, the router can validate that the client certificate was issued by a trusted CA. |
| | **Certificates Setup** |
| **Certificate Source** | Select a source for the certificate to be used for OpenVPN.<br>**Router generated certificates** - Router-generated certificates that will be used for OpenVPN.<br>● **GENERATE** - Click to generate a certificate.<br>● **Delete all certificates** - Click to remove all certificates generated by the router.<br>**Uploading certificates to Router** - Third-party certificates will be used for OpenVPN.<br>● **Trust CA** - Use the dropdown list to select a trusted CA certificate that has already been uploaded to the router. To upload Trusted CA certificates to the router, click the Trust CA label and you will be taken to the **Certificate Management >> Trusted CA Certificate** page to perform the operation. |

| | |
|---|---|
| | • **Server Certificate** - Use the dropdown list to select a server certificate that has already been uploaded to the router. To upload server certificates to the router, click the Server Certificate label and you will be taken to the **Certificate Management >> Local Certificate** page to perform the operation. |
| **Save** | Save the current settings |

#### 9.4.12.6.2 Client Config

Create and export the configuration required for a remote OpenVPN client to connect to the router.




These parameters are explained as follows:

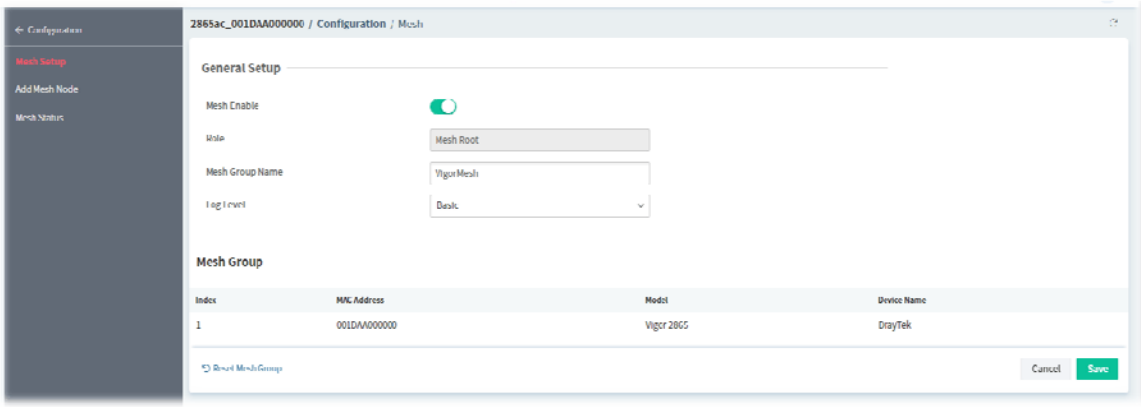
| Item | Description |
|---|---|
| | **Client Config** |
| **Remote Server** | **There are three types of the remote server.**<br>• **IP** - Use the numeric IP address as the server address.<br>• **Domain** - Use the domain as the server address.<br>• **VPN Matcher** - Use the VPN matcher as the server. |
| **IP** | If **IP** is selected as the remote server, enter the IP address of the server. |
| **Domain** | If **Domain** is selected as the remote server, enter the domain name of the server. |
| **Transport Protocol** | Select UDP or TCP for the protocol to be used by the OpenVPN client to connect to the router. |
| **Auto Dial-Out** | **Enable** - If selected, the remote client can auto-dial to this Vigor router to build an OpenVPN tunnel.<br>**Disable** - Select to disable the function. |
| **Set VPN as Default Gateway** | **Enable** - If selected, 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** - Select to disable the function. |
| **File Name** | Enter the filename of the configuration file to be downloaded from the router. |
| **Client cert** | Enter the filename of the client certificate obtained from 3rd party provider. |

| | |
|---|---|
| **Client key** | Enter the filename of the private key obtained from the 3rd party provider. |
| **Export** | Click to download the settings on this page as a file. |

## 9.4.13 Mesh

### 9.4.13.1 Mesh Setup

Vigor router is treated as a mesh root. You can search and specify mesh nodes as members under current mesh group.



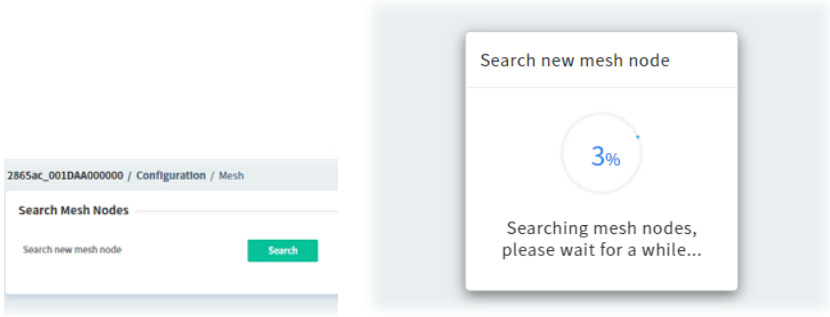

These parameters are explained as follows:

| Item | Description |
|---|---|
| | **General Setup** |
| **Mesh Enable** | Click to enable or disable the mesh network function. |
| **Role** | Displays the role of the router. For Vigor router, it is always Mesh Root. |
| **Mesh Group Name** | Displays the name of the current mesh group. |
| **Log Level** | Choose **Basic** or **Detailed**. |
| | **Mesh Group** |
| **Index, MAC Address, Model, Device Name** | Basic information including MAC address, model and device name of the members in this Mesh Group will be shown in this area. |
| **Reset Mesh Group** | Click it to clear the Mesh Group information. All mesh nodes in the group will become isolated. |
| **Cancel** | Discard current modification. |
| **Save** | Save the current settings |

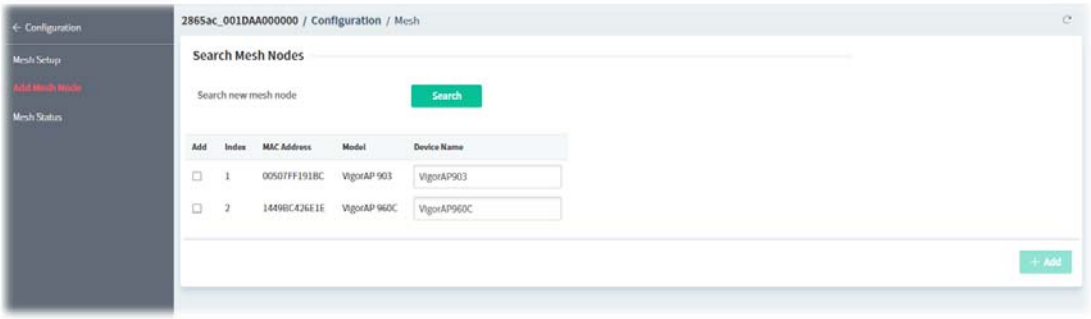
### 9.4.13.2 Add Mesh Node

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

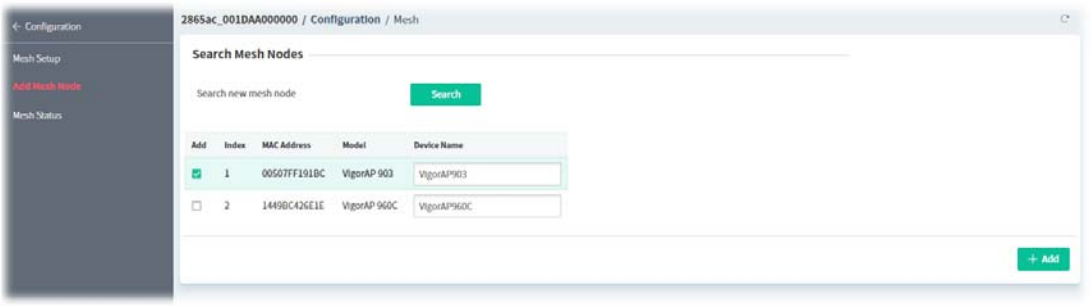
1. Click **Search**. The system will search new mesh node around.



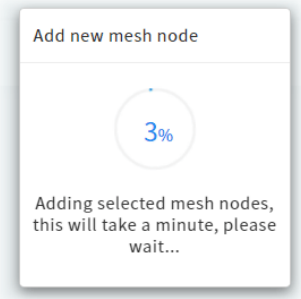

2. Available mesh nodes will be listed on this page.



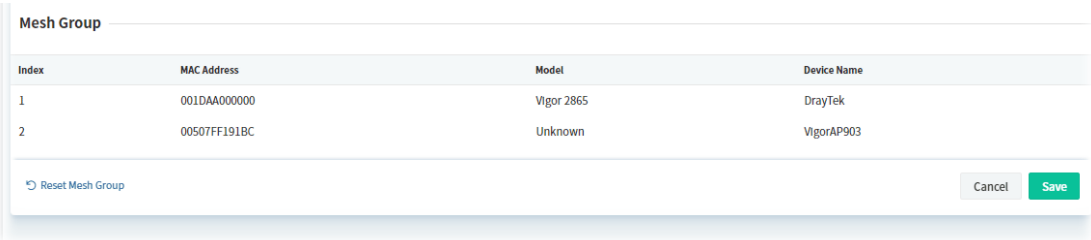

3. Select the device(s) you want to group under this mesh group and click **+Add**.




4. Wait for a moment.



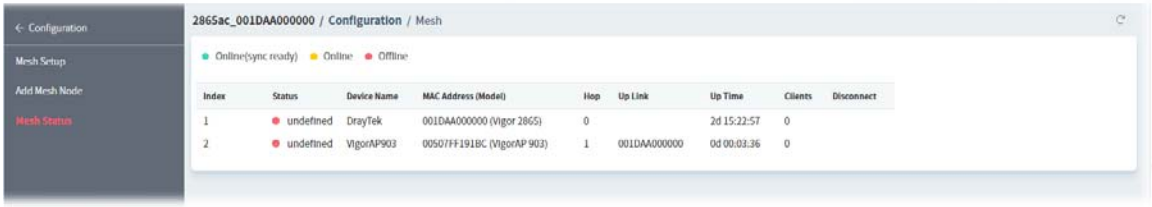

5. Open **Configuration>>Mesh Setup**. The new mesh node will be added.



### 9.4.13.3 Mesh Status

This page shows the mesh status.

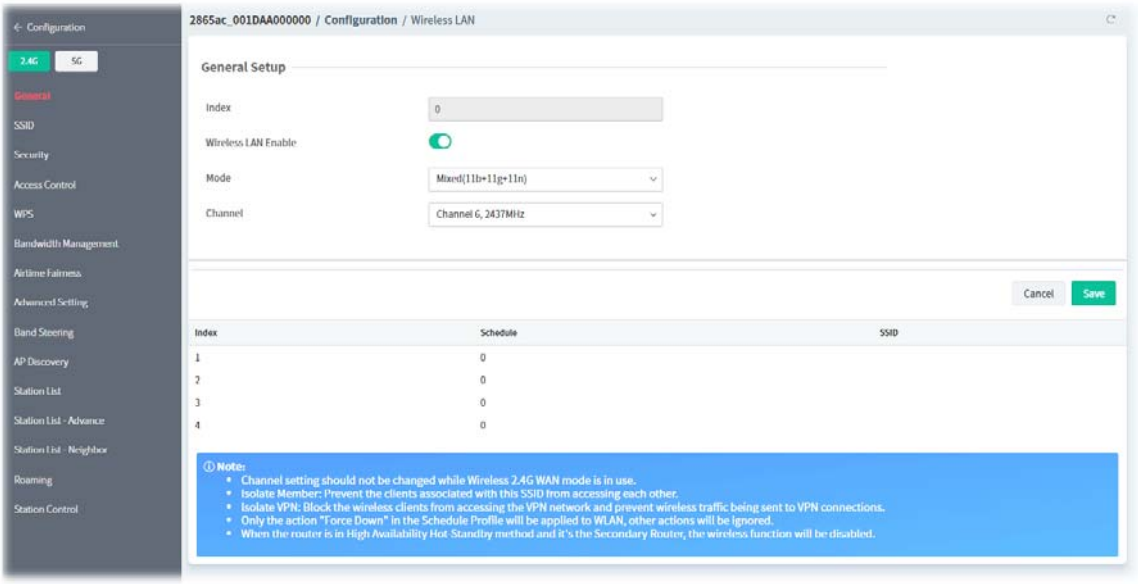
One Mesh Group can contain up to 8 devices. A Device with hop 0 is one special Ethernet Backhaul. It means this node will use Ethernet cable to join the mesh group while others use the wireless link.



## 9.4.14 Wireless LAN

### 9.4.14.1 General

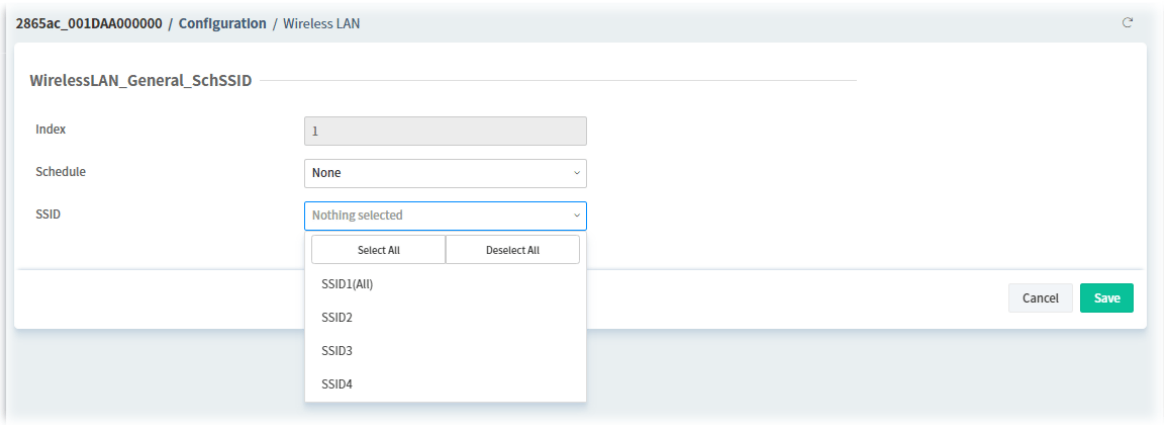
This page lets you configure the most basic settings of your wireless network, including the SSIDs, WLAN channels and bandwidth control.




These parameters are explained as follows:

| Item | Description |
|---|---|
| | **General Setup** |
| **Index** | Displays the index number of the WLAN profile. |
| **Wireless LAN Enable** | Click to enable or disable the wireless LAN function. |
| **Mode** | Select the 802.11 mode allowed on the band. |
| **Channel** | Allows you to specify a particular wireless channel to use, or let the system determine the optimal channel by selecting "**Auto**". |
| **Cancel** | Discard current modification. |
| **Save** | Save the current settings. |
| **Index** | Displays the index number of the WLAN profile. |
| **Schedule** | Displays the number of the schedule profile. |

To configure the schedule profile, move the mouse cursor to any entry (1 to 4) and click to open the following page.

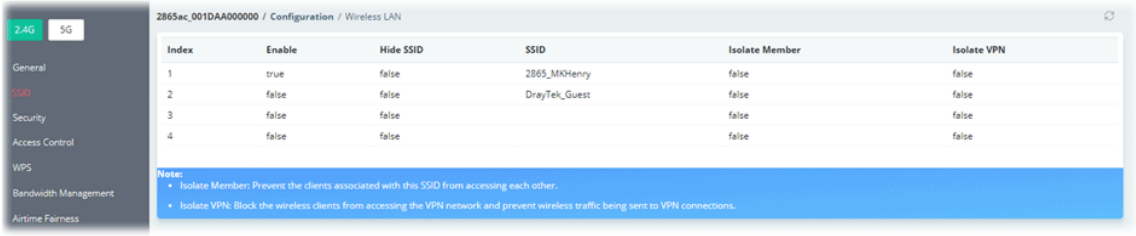



These parameters are explained as follows:

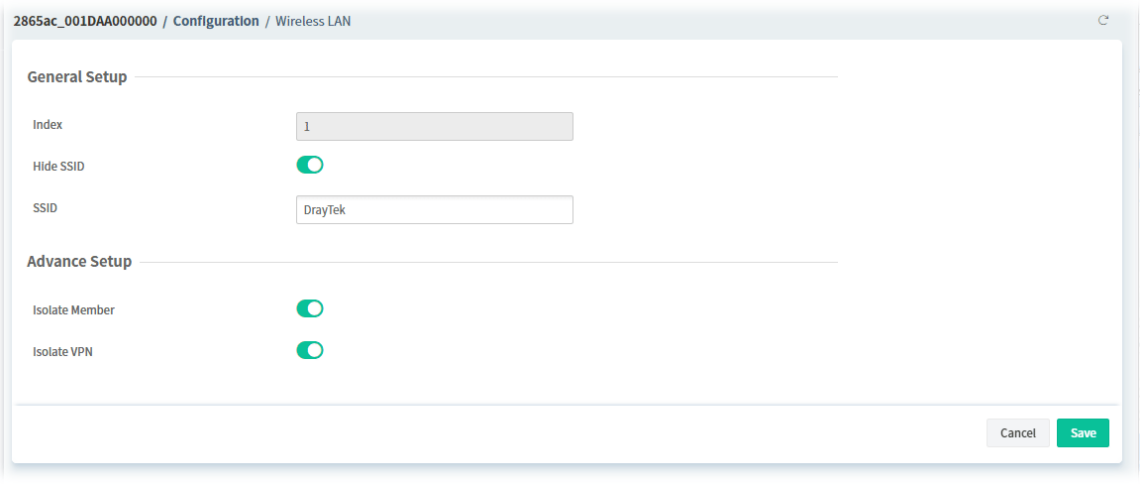
| Item | Description |
|---|---|
| **Index** | Displays the index number of the schedule profile applied to the SSID. |
| **Schedule** | Select a name of the schedule profile. |
| **SSID** | Select a number of SSID. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

### 9.4.13.2 SSID

Set Service Set Identification (SSID), which shows up as the AP identifier.




To configure the SSID profile, move the mouse cursor to any entry (1 to 4) and click to open the following page.



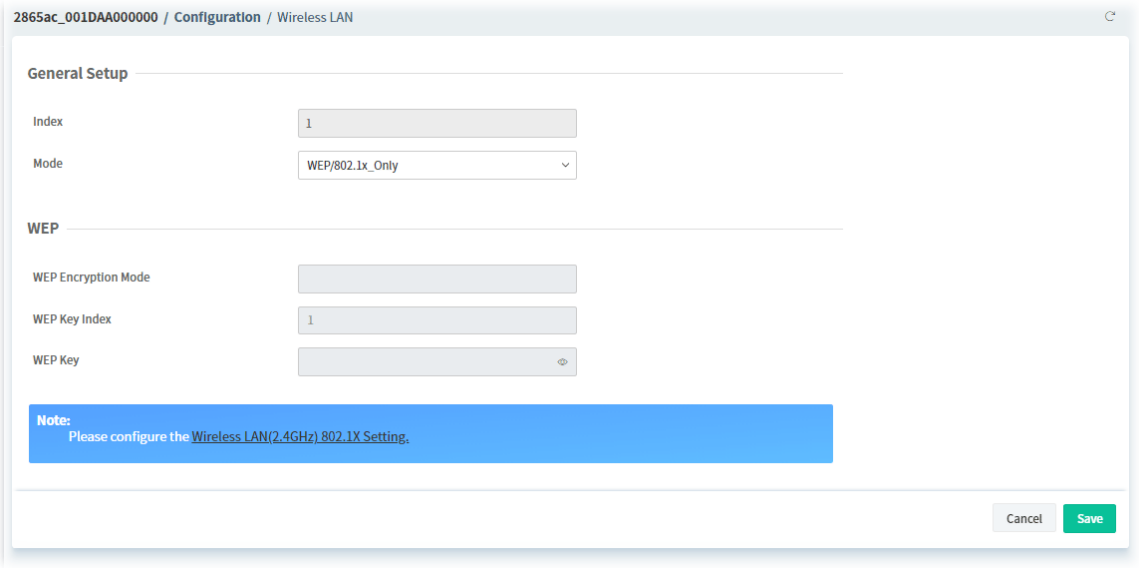
These parameters are explained as follows:

| Item | Description |
|---|---|
| | **General Setup** |
| **Index** | Display the index number of SSIDs. There are four SSIDs. |
| **Hide SSID** | Click to enable or disable the SSID settings. |
| **SSID** | Enter or display the name of SSID. |
| | **Advance Setup** |
| **Isolate Member** | Click to enable or disable the function.<br>If enabled, the router disallows communication between wireless clients (stations) on the same SSID. |
| **Isolate VPN** | Click to enable or disable the function.<br>If enabled, the router blocks wireless clients (stations) from accessing VPN clients. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

### 9.4.13.3 Security

Every router has a default wireless password (PSK) which is provided on a label attached to the bottom of the router. For extra security, you can set your own wireless password

To configure security settings, move the mouse cursor to any entry (1 to 4) and click to open the following page.

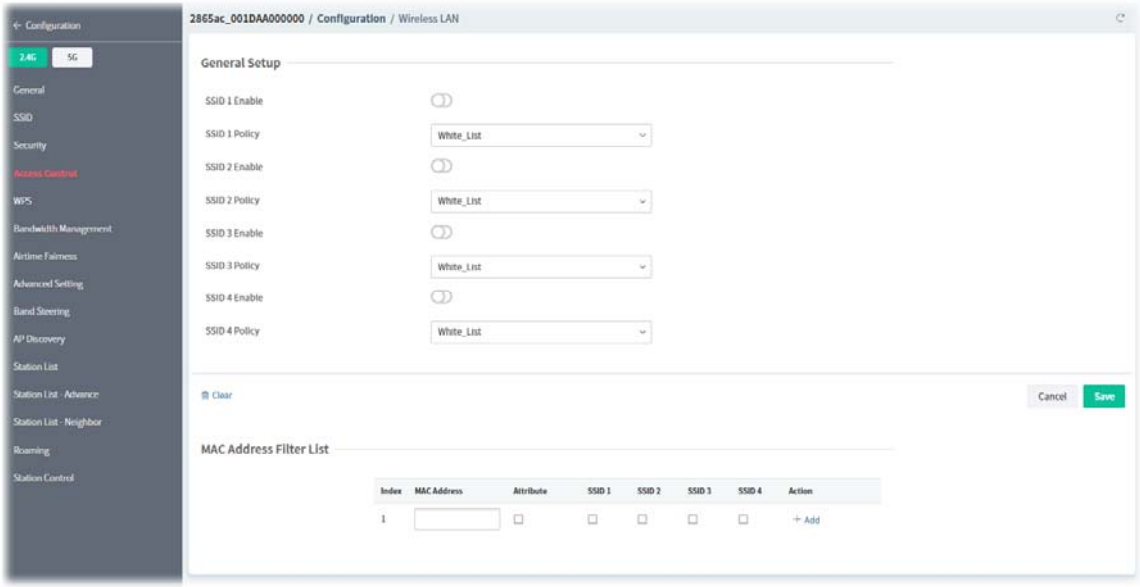


These parameters are explained as follows:

| Item | Description |
|---|---|
| | **General Setup** |
| **Index** | Displays the index number of SSID1 to SSID4. |
| **Mode** | **Disable** - Encryption mechanism is disabled.<br>**WEP** or **WEP/802.1x_Only**- Allows only connections from WEP clients.<br>**WPA/802.1x_Only or WPA2/802.1x_Only or Mixed(WPA+WPA2/802.1x_Only), WPA/PSK or WPA2/PSK or Mixed(WPA+WPA2)/PSK, WPA3/SAE, Mixed(WPA2+WPA3)/SAE** - Allows only connections from WPA clients. |
| | **WEP** or **WEP/802.1x_Only** |
| **WEP Encryption Mode** | Select 64-bit or 128-bit. |
| **WEP Key Index** | Select an index number to configure the WEP setting. |
| **WEP Key** | Enter the encryption key. |
| | **WPA/802.1x_Only or WPA2/802.1x_Only or Mixed(WPA+WPA2/802.1x_Only), WPA/PSK or WPA2/PSK or Mixed(WPA+WPA2)/PSK, WPA3/SAE, Mixed(WPA2+WPA3)/SAE** |
| **WPA Encryption Mode** | Displays the encryption mode used for WPA. |
| **WPA Pre-shared Key** | Enter 8~63 ASCII characters. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

### 9.4.13.4 Access Control

In the Access Control web page, users may configure the **white/black** list modes used by each SSID and the MAC addresses applied to their lists.

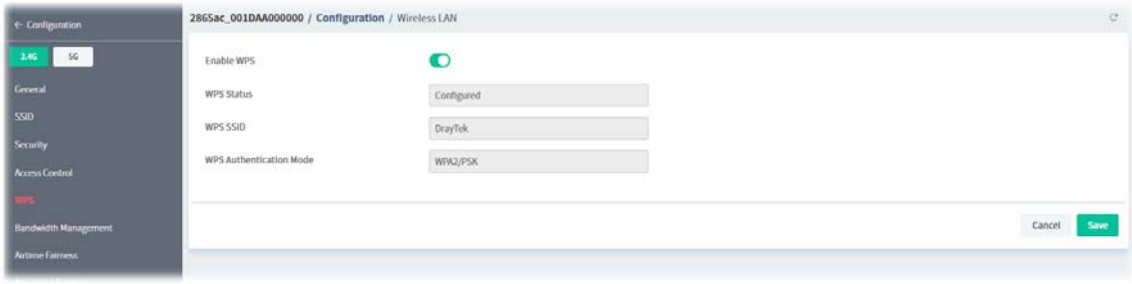



These parameters are explained as follows:

| Item | Description |
|---|---|
| | **General Setup** |
| **SSID 1 Enable ~ SSID 4 Enable** | Click to enable or disable the MAC filter. |
| **SSID 1 Policy ~ SSID 4 Policy** | **White List** - Only allow wireless clients whose MAC addresses are listed in the MAC Address Filter list.<br>**Black List** - Only allow wireless clients whose MAC addresses are not listed in the MAC Address Filter list. |
| **Clear** | Clear all modifications on this page. |
| **Cancel** | Discard current modification. |
| **Save** | Save the current settings. |
| | **MAC Address Filter List** |
| **Index** | Displays the index number of entry. |
| **MAC Address** | Enter the MAC address of wireless client. |
| **Attribute** | Select to isolate the wireless client from LAN. |
| **SSID1 ~ SSID4** | Select the SSIDs to which the above MAC address filter will be applied. |
| **Action +Add** | After entering MAC address and select SSIDs, click +Add to save the settings and create an additional setting entry. |

### 9.4.13.5 WPS

It provides an easy way to connect wireless to wireless access points and routers with WPA or WPA2 encryption.

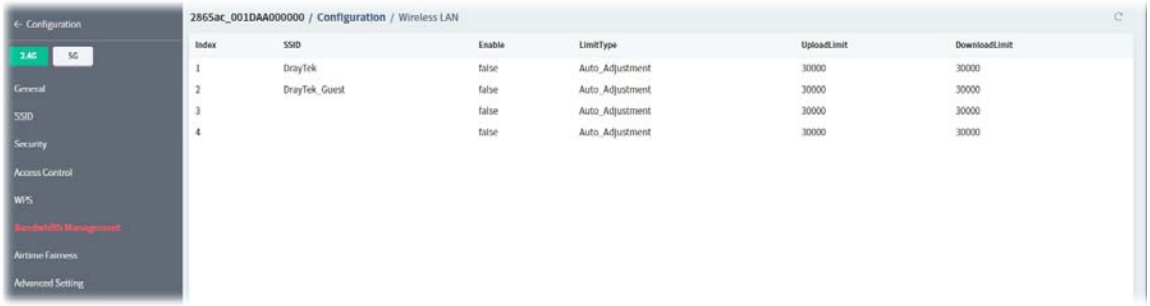



These parameters are explained as follows:

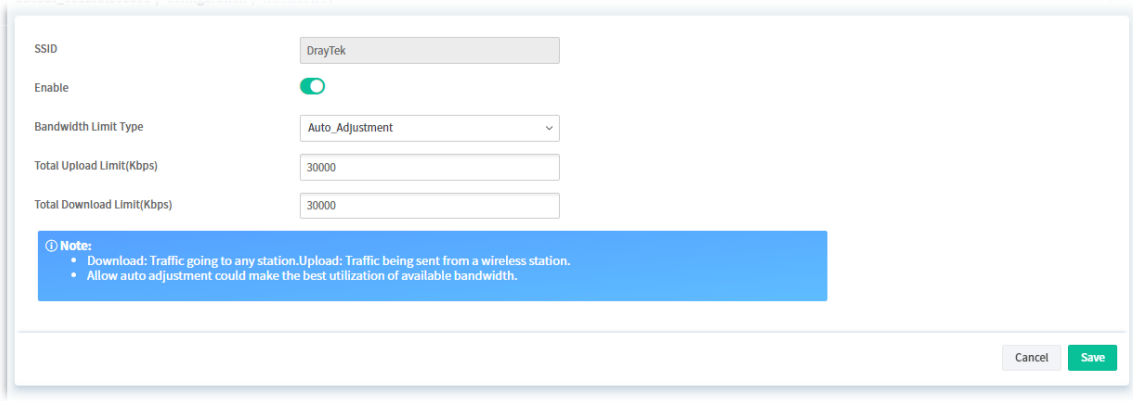
| Item | Description |
|---|---|
| **Enable WPS** | Click to enable or disable the WPS function. |
| **WPS Status** | Displays system information related to WPS. The message “Configured” means that the wireless security (encryption) function of the router is properly configured and functioning properly. |
| **WPS SSID** | Displays the name of SSID1. WPS is supported on SSID1 only. |
| **WPS Authentication Mode** | Displays the current authentication mode of the router. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

### 9.4.13.6 Bandwidth Management

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




To configure the bandwidth management settings, move the mouse cursor to any entry (1 to 4) and click to open the following page.

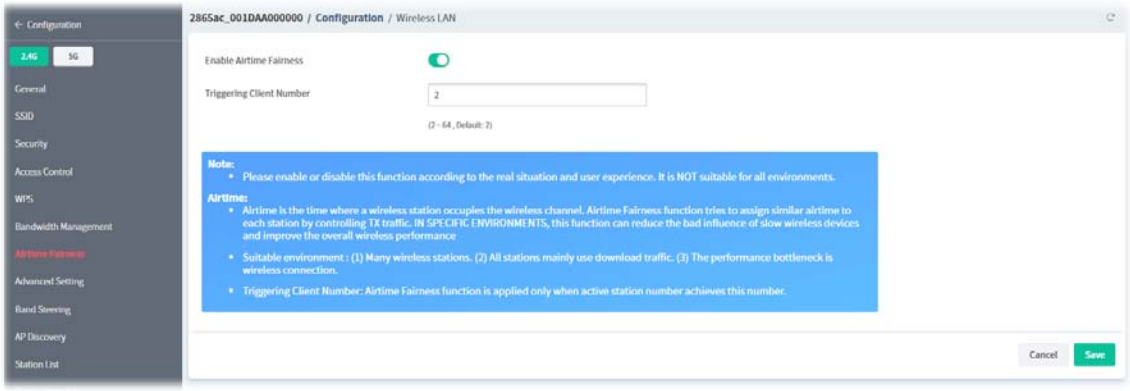



These parameters are explained as follows:

| Item | Description |
|---|---|
| **SSID** | Displays the specific SSID name. |
| **Enable** | Click to enable or disable the function. |
| **Bandwidth Limit Type** | **Auto_Adjustment** - Bandwidth limit is determined by the system automatically.<br>● **Total Upload** - Enter a value to define the maximum data traffic (uploading) for all of the wireless clients connecting to this router.<br>● **Total Download** - Enter a value to define the maximum data client(stations) connecting to this router.<br>**Per_Station_Limit** - Bandwidth limit is determined according to the limitation of the wireless client.<br>● **Upload Limit(Kbps)** - Enter a value to define the maximum data traffic (uploading) for each wireless client connecting to this router.<br>● **Download Limit(Kbps)**- Enter a value to define the maximum data traffic (downloading) for each wireless client connecting to this router. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

### 9.4.13.7 Airtime Fairness

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

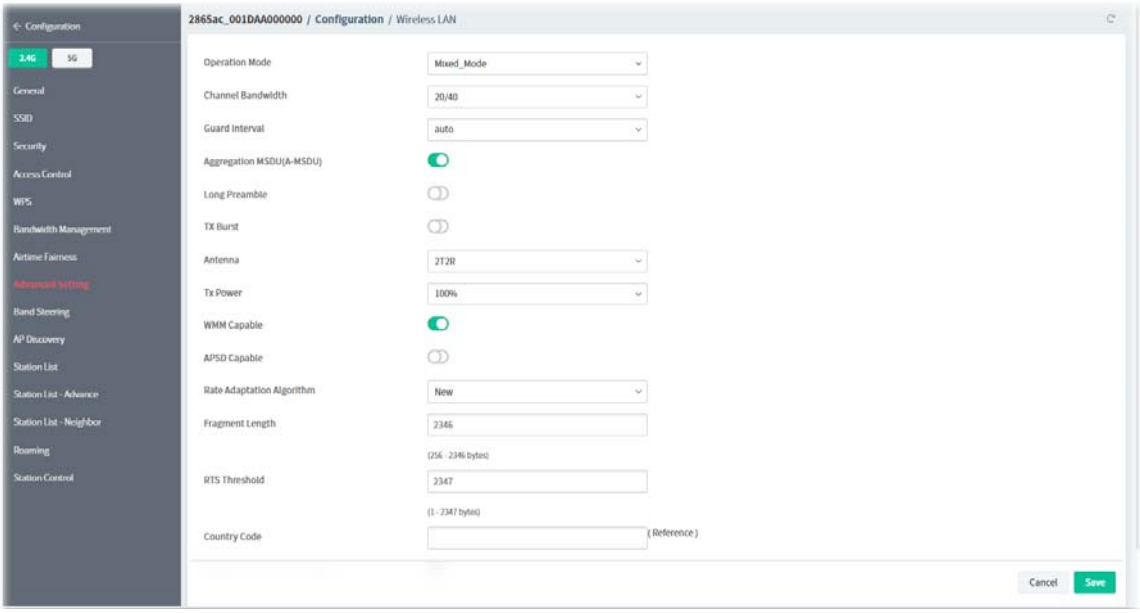



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Enable Airtime Fairness** | Click to enable or disable the airtime fairness. |
| **Triggering Client Number** | Airtime Fairness function is applied only when there are at least this many active wireless stations. |
| **Cancel** | Discard current modification. |
| **Save** | Save the current settings. |

### 9.4.13.8 Advanced Setting

This page allows you to configure advanced settings such as operation mode, channel bandwidth, guard interval, and aggregation MSDU for wireless data transmission.



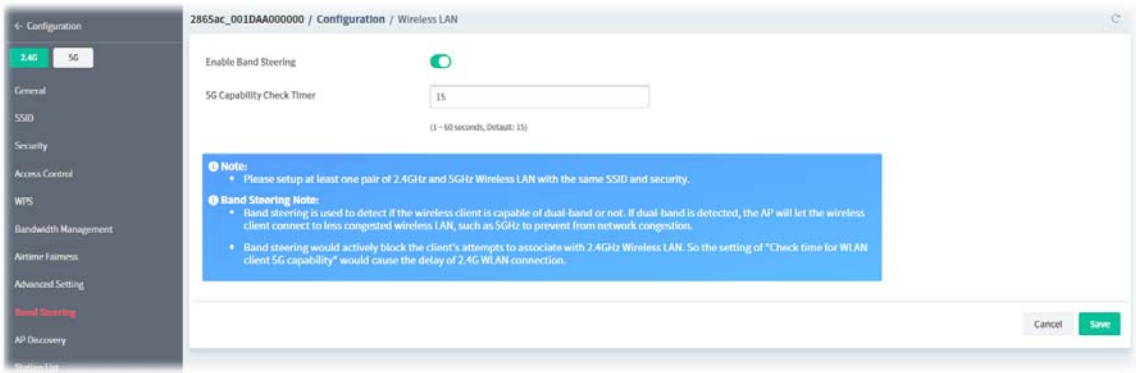

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Operation Mode** | **Mixed_Mode** - The router can transmit data using all protocols supported by 802.11a/b/g and 802.11n standards. However, all wireless |

| | |
|---|---|
| | transmissions will be slowed down when any 802.11g or 802.11b wireless client is connected.<br>**Green_Field** - Select this mode to achieve the highest throughput. This mode supports data transmission between 802.11n systems only. |
| **Channel Bandwidth** | **20 MHz** - Vigor Router will utilize 20 MHz channels for data transmission and reception between the AP and wireless stations.<br>**40 MHz** - Vigor Router will utilize 40 MHz channels for data transmission and reception between the AP and wireless stations.<br>**20/40 MHz** - Vigor Router will utilize either 20 MHz or 40 MHz for data transmission and reception depending on the number of nearby wireless APs. |
| **Guard Interval** | If you choose auto as guard interval, the router will choose short guard interval (which increases wireless performance) or long guard interval for data transmit depending on the station capability. |
| **Aggregation MSDU** | Click to enable or disable the function.<br>If enabled, it will combine frames of different sizes to improve performance at the MAC layer for clients from certain manufacturers. |
| **Long Preamble** | Click to enable or disable the function.<br>This option determines the length of the sync field in an 802.11 packet. |
| **TX Burst** | Click to enable or disable the function.<br>If enabled, this feature can enhance the performance in data transmission about 40%*. |
| **Antenna** | 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. |
| **TX 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. |
| **WMM Capable** | Click to enable or disable the function.<br>It provides basic Quality of Service (QoS) by prioritizing traffic based on four access categories defined in the IEEE 802.11e standard. |
| **APSD Capable** | Click to enable or disable the function.<br>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. |
| **Rate Adaptation Algorithm** | Wireless transmission rate is adapted dynamically. Usually, performance of "new" algorithm is better than "old". |
| **Fragment Length** | Set the Fragment threshold. You are advised to leave the default value, 2346. |
| **RTS Threshold** | Minimize the collision (unit is bytes) between hidden stations to improve wireless performance. |
| **Country Code** | Vigor router broadcasts country codes according to the 802.11d standard. Click Reference to get detailed information. |
| **Isolate 2.4GHx and 5GHz bands** | Click to enable or disable the function.<br>If enabled, the wireless client using 2.4GHz band is unable to connect to the wireless client with 5GHz band, and vice versa. |
| **Cancel** | Discard current modification. |
| **Save** | Save the current settings. |

### 9.4.13.9 Band Steering (for 2.4G only)

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




These parameters are explained as follows:

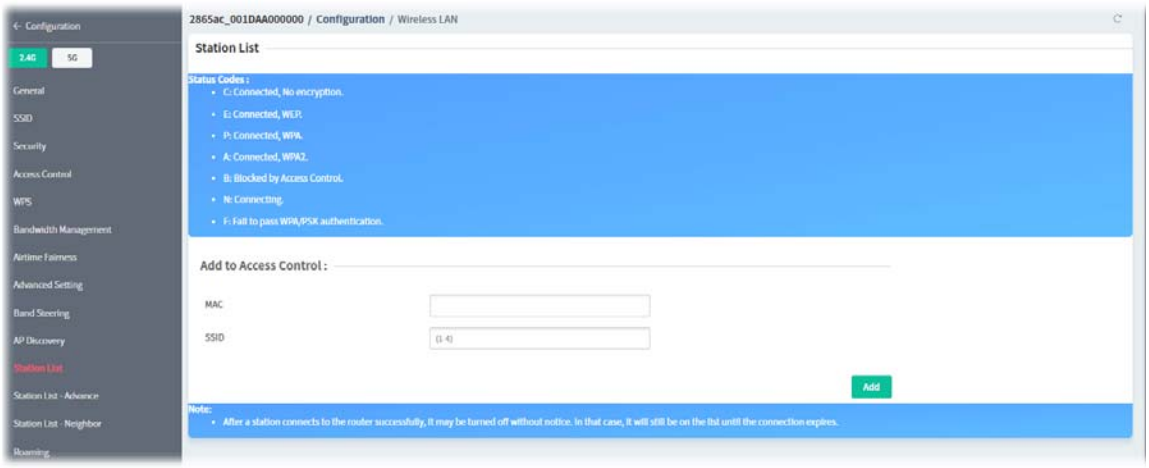
| Item | Description |
|---|---|
| **Enable Band Steering** | Click to enable to disable the Band Steering function. |
| **5G Capability Check Timer** | Set a check time value.<br>When a wireless client attempts to connect, the router will block attempts to connect to the 2.4 GHz band for the specified period of time (default is 30 seconds), which hopefully will entice the client to connect to the 5 GHz band. If the client fails to connect to the 5 GHz band within the specified interval, it will then be able to connect to the 2.4 GHz band. |
| **Cancel** | Discard current modification. |
| **Save** | Save the current settings. |

### 9.4.13.10 AP Discovery

Vigor router can scan all regulatory channels to find working APs in the neighborhood.

### 9.4.13.11 Station List

Station List provides an overview of all currently connected wireless clients and their status.

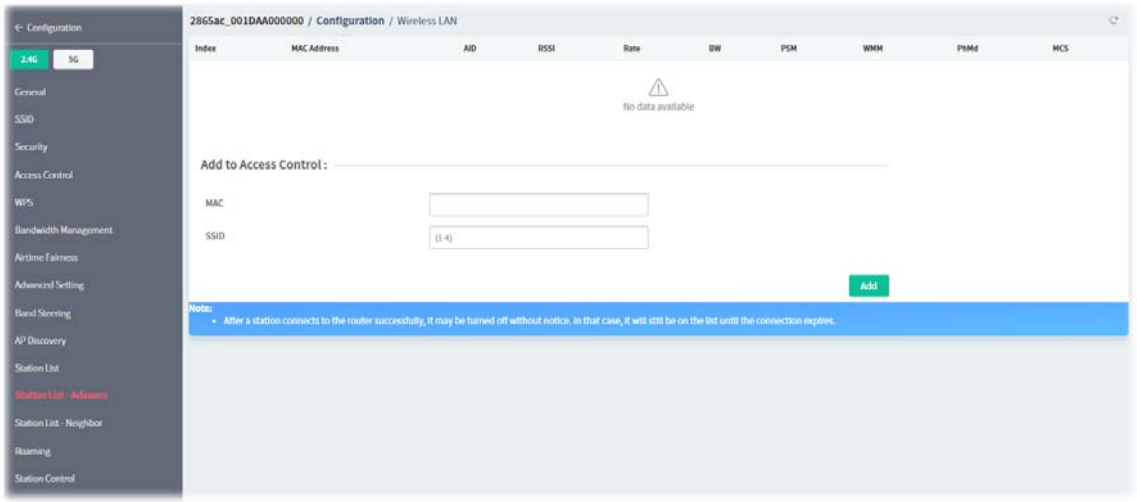



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Station List** | Displays wireless stations connected to the Vigor router. |
| **Add to Access Control** | **MAC -** Enter the MAC address.<br>**SSID -** Specify the number of SSID. |
| **Add** | Click to add a new entry to Access Control. |

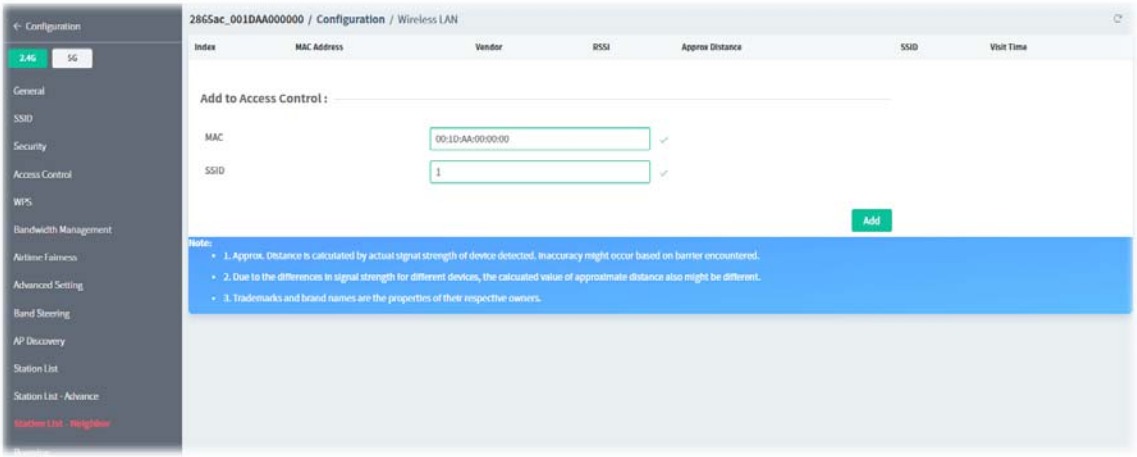
### 9.4.13.12 Station List - Advance

Displays wireless stations connected to the Vigor router with more detailed information.



### 9.4.13.13 Station List - Neighbor

This page displays the nearby wireless stations connected to other access points that are detected by the Vigor router.

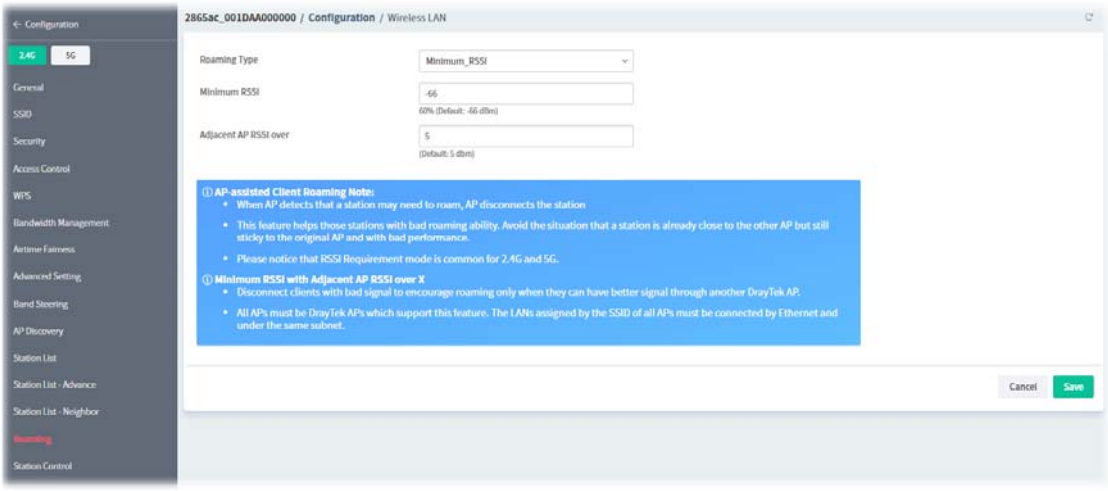



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Station List** | Displays wireless stations connected to the Vigor router. |
| **Add to Access Control** | **MAC** - Enter the MAC address.<br>**SSID** - Specify the number of SSID. |
| **Add** | Click to add a new entry to Access Control. |

### 9.4.13.14 Roaming

WiFi roaming allows wireless stations to switch connections between access points within an area to achieve better coverage and signal quality.



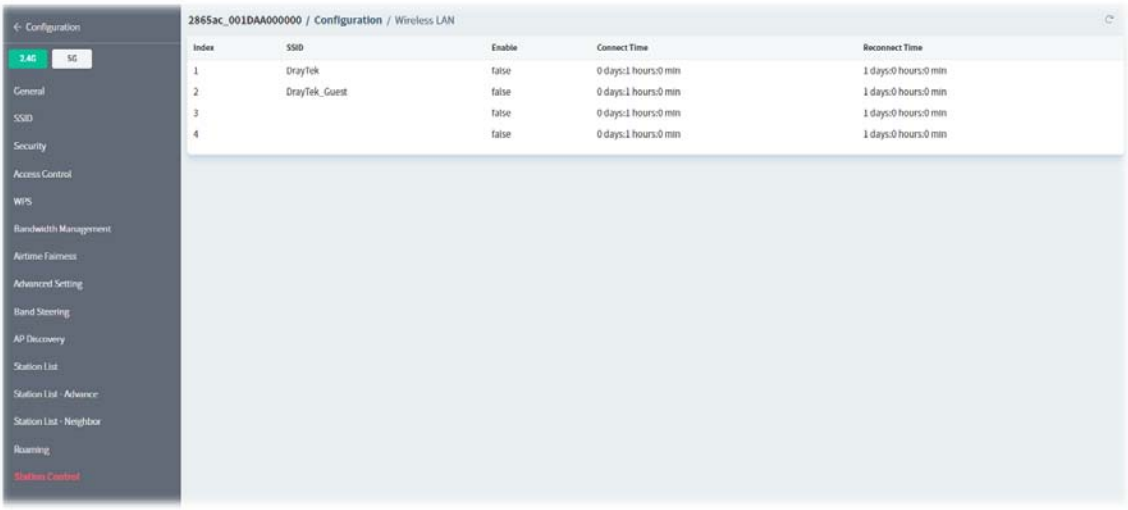

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Roaming Type** | • **Disable RSSI Requirement -** The Vigor router does not pay attention to the RSSI level of wireless stations. Selecting this option means the Vigor router will not interfere with the roaming behavior of wireless stations.<br>• **Strictly Minimum RSSI** |

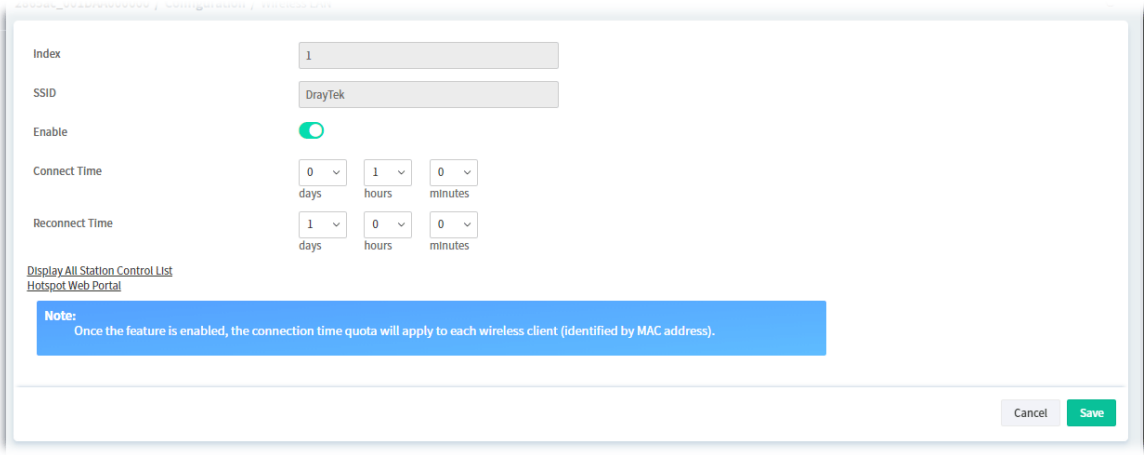
| | |
|---|---|
| | • **Minimum RSSI** |
| **Strictly Minimum RSSI** | The Vigor router will immediately disconnect the wireless station if its RSSI falls below the configured value.<br>Specify a value as a threshold. |
| **Minimum RSSI** | The Vigor router will disconnect wireless clients whose RSSI falls below the minimum threshold only if there is also a neighboring wireless host (router or AP) that has an RSSI value (defined in the field of With Adjacent AP RSSI over) higher than a certain threshold.<br>In order for this option to work, other wireless hosts connected to the same LAN subnet need to support the exchange of RSSI information with peer wireless hosts via Ethernet.<br>Specify a value as a threshold. |
| **Adjacent AP RSSI over** | Specify a value as a threshold. |
| **Cancel** | Discard current modification. |
| **Save** | Save the current settings. |

### 9.4.13.15 Station Control

Station Control is used to specify the duration that the wireless client can connect to the Vigor router. If this function is disabled, wireless clients can connect to the router as long as the router is powered on and the wireless feature is enabled.




To configure the station control settings, move the mouse cursor to any entry (1 to 4) and click to open the following page.



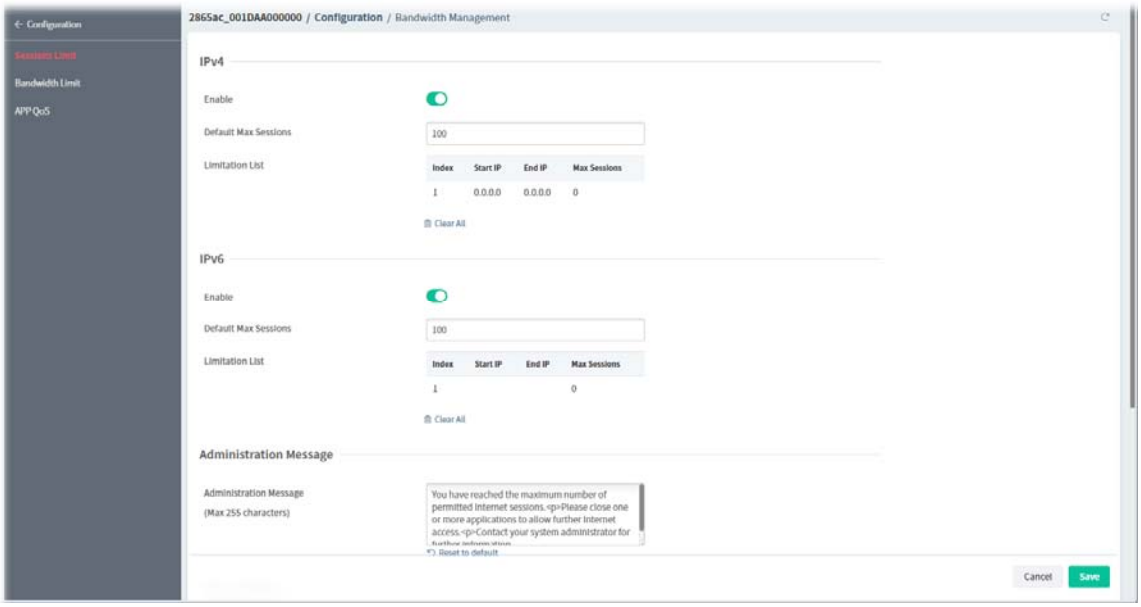

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Index** | Displays the index number of SSID profile. |
| **SSID** | Displays the name of the SSID. |
| **Enable** | Click to enable or disable the station control function for this SSID. |
| **Connect Time / Reconnect Time** | Enter the time in days, hours and minutes.<br>In the Connection Time dropdown box, select the maximum amount of time that a wireless client is allowed to connect within the period of time selected in the Reconnection Time dropdown box. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

## 9.4.14 Bandwidth Management

### 9.4.14.1 Sessions Limit

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 a finite number of sessions that can be tracked by the router. By setting session limits will ensure that the router does not run out of resources.

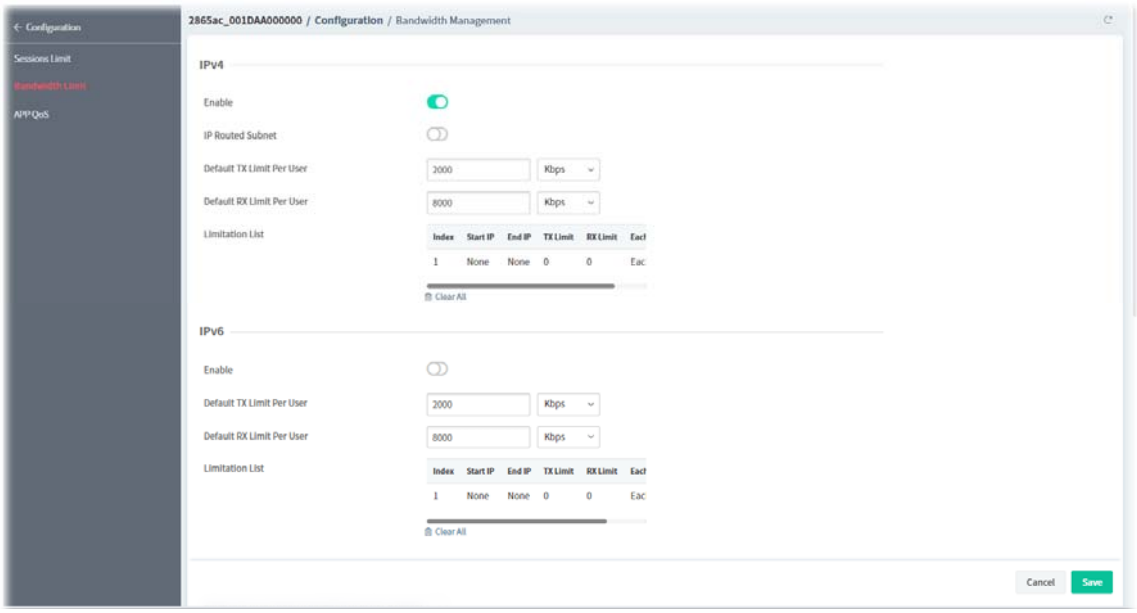



These parameters are explained as follows:

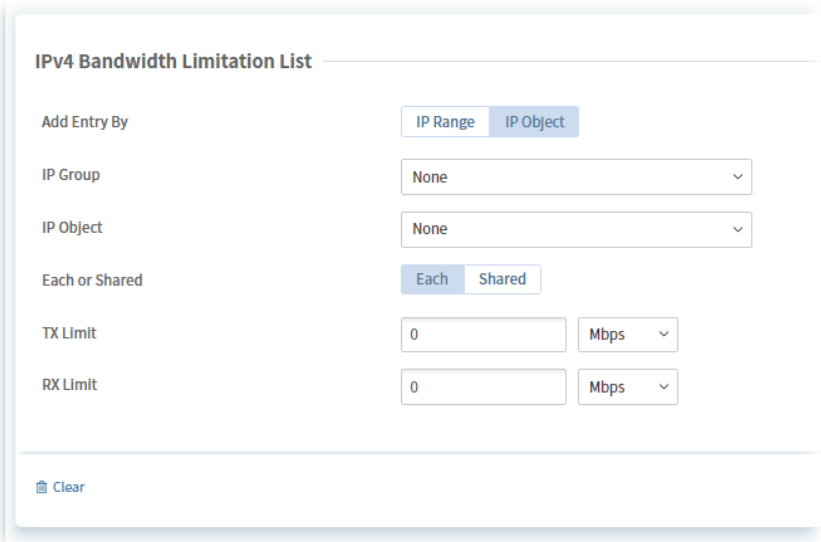
| Item | Description |
|---|---|
| | **IPv4 / IPv6** |
| **Enable** | Click to enable or disable the sessions limit function. |
| **Default Max Sessions** | The default maximum number of sessions allowed per LAN client, unless overridden by specifying a different number in the Limitation List. |
| **Limitation List** | Displays specific limitation entries. |
| **Clear All** | Clear all modifications on this page. |
| | **Administration Message** |
| **Administration Message** | Enter a message to be displayed in a web browser on the LAN client when the maximum number of NAT sessions has been reached. |
| | **Time Schedule** |
| **Schedule 1 ~ 4** | Specify up to 4 time schedule entries to enable or disable the WAN.<br>Specify up to 4 time schedule entries to apply the sessions limit management. |
| **Cancel** | Discard current modification. |
| **Save** | Save the current settings. |

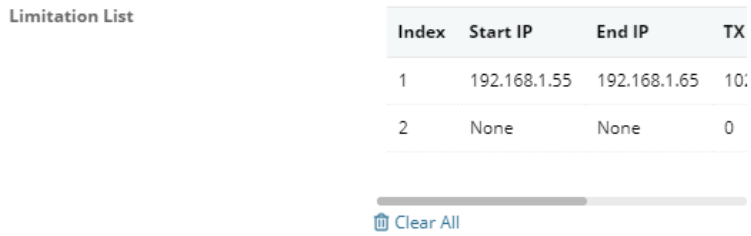
### 9.4.14.2 Bandwidth Limit

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



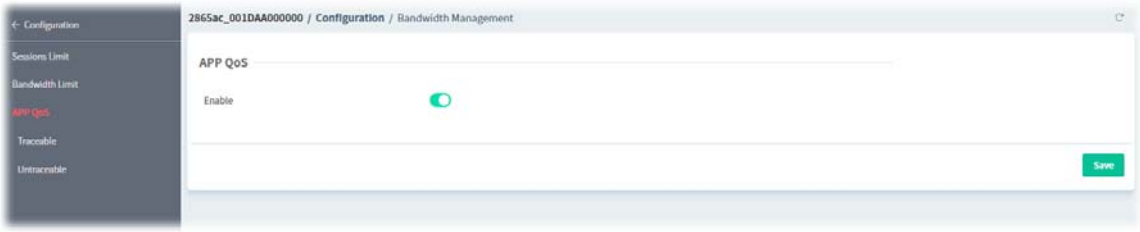

These parameters are explained as follows:

| Item | Description |
|---|---|
| | **IPv4 / IPv6** |
| **Enable** | Click to enable or disable the bandwidth limit function.<br>**IP Routed Subnet -** It is available for IPv4 only. |
| **Default TX Limit Per User** | Set default upstream speed limit for each LAN client. |
| **Default RX Limit Per User** | Set default downstream speed limit for each LAN client. |
| **Limitation List** | Displays specific limitation entries.<br>To add a new profile, click the last index number to open the setting page.<br>  <br>After finishing the settings, click Save. A new profile will be added and |

| | |
|---|---|
| | displayed on the limitation list.<br>  |
| **Clear All** | Clear all profiles in the limitation list. |
| **Allow user to use more bandwidth than the assigned...** | Click to enable or disable this function.<br>If enabled, it lets the router automatically adjust the upstream and downstream limits based on available bandwidth. |
| **Smart Bandwidth Limit** | Click to enable or disable this function.<br>If enabled, it restricts the bandwidth of LAN clients that are not in the limitation list when the network sessions exceed a predefined threshold. |
| **Apply the below limit to users not in ...** | Enter the number of sessions that a LAN client is allowed to have before Smart Bandwidth Limit activates. |
| **TX Limit** | Upstream speed limit for each LAN client. Unit can be either Kbps or Mbps. |
| **RX Limit** | Downstream speed limit for each LAN client. Unit can be either Kbps or Mbps. |
| | **Time Schedule** |
| **Schedule 1 ~ 4** | Specify up to 4 time schedule entries to apply the bandwidth limit management. |
| **Cancel** | Discard current modification. |
| **Save** | Save the current settings. |

### 9.4.14.3 APP QoS

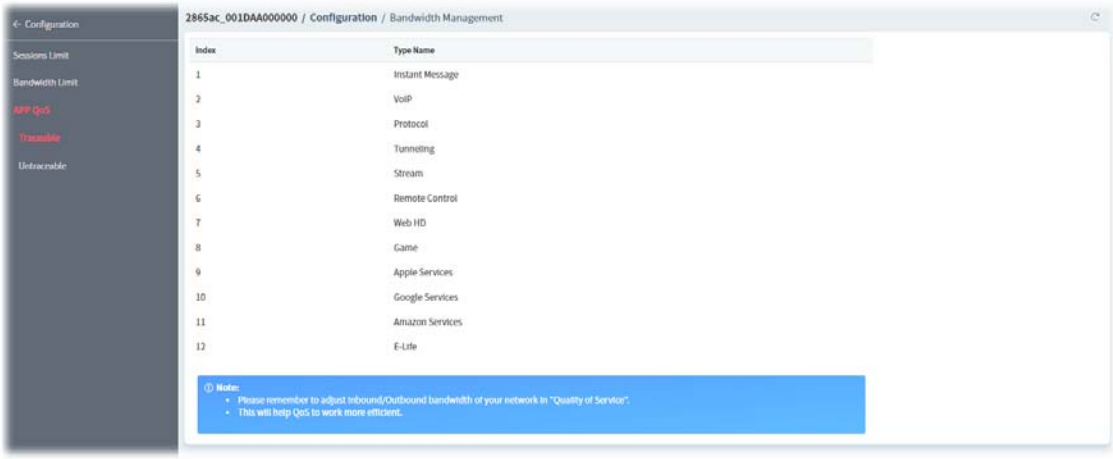
APP QoS allows QoS to be applied to select protocols and applications. Protocols and applications fall into two categories: Traceable and Untraceable.



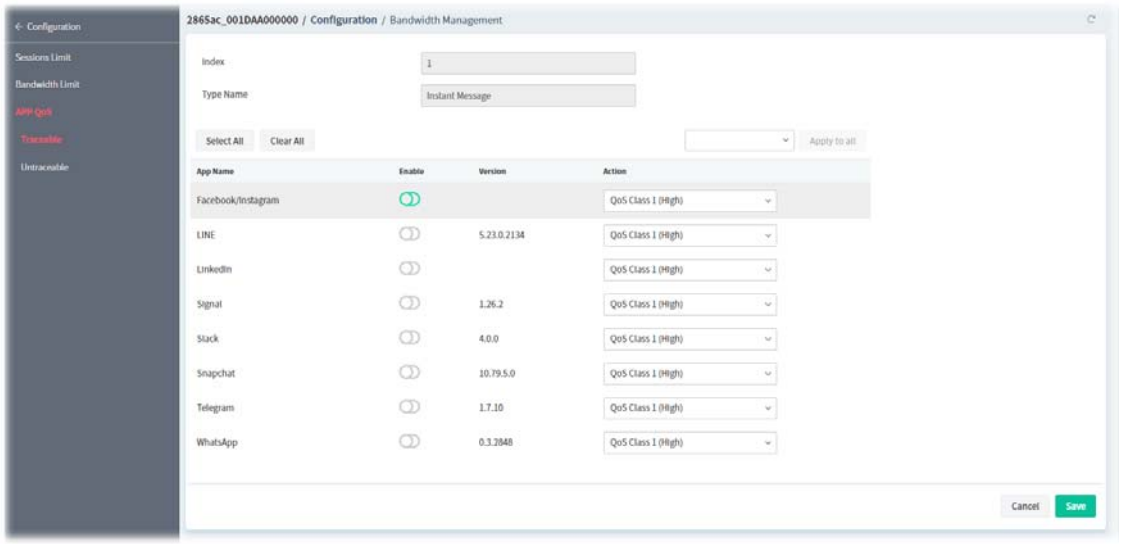

Click the **Enable** button to enable or disable the APP QoS function. Then click **Save** to save the settings.

### Traceable

Traceable applications are those whose traffic can be 100% traced, and can be assigned a specific QoS class.




Click the index number (e.g., #1) of type to get the following page. Each type will bring different setting page. Here we take #1 Instant Message as an example.

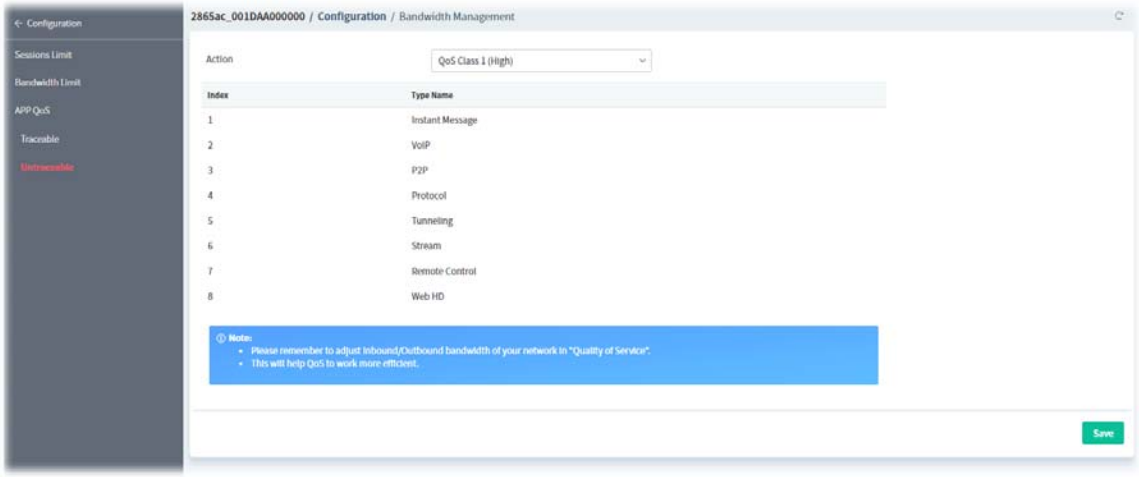



These parameters are explained as follows:

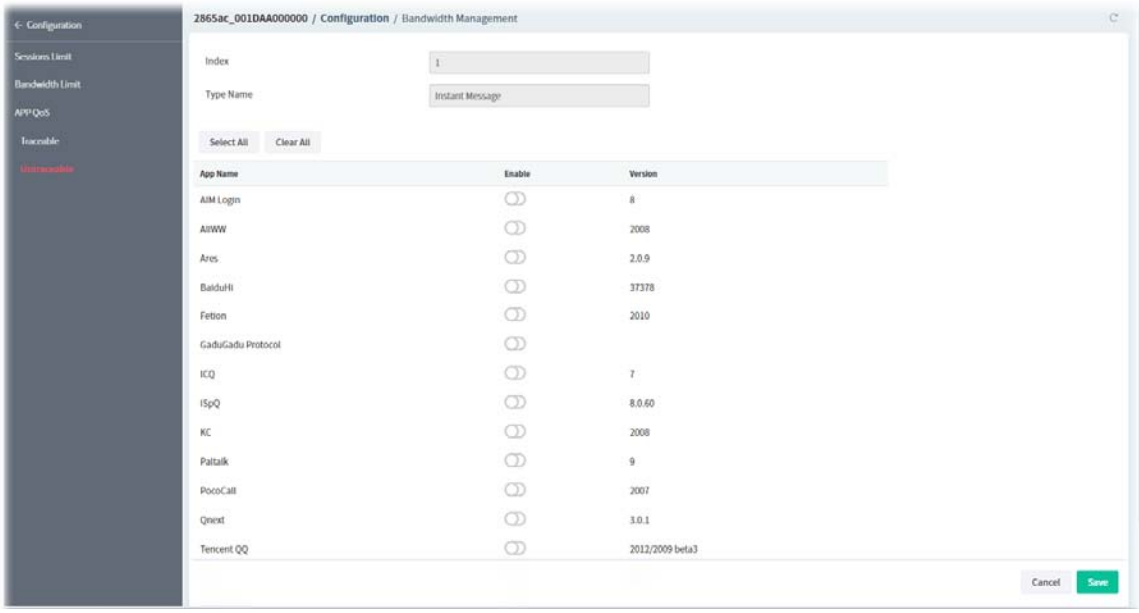
| Item | Description |
|---|---|
| **Enable** | Click to enable or disable the bandwidth limit function. |
| **Action** | Select a QoS class to be applied to the application. |
| **Cancel** | Discard current modification. |
| **Save** | Save the current settings. |

### Untraceable

Untraceable applications, on the other hand, are detected when they attempt to establish connections to remote hosts, and all traffic between the remote hosts and the local network will be placed under QoS, within the same QoS class.




Click the index number (e.g., #1) of type to get the following page. Each type will bring different setting page. Here we take #1 Instant Message as an example.



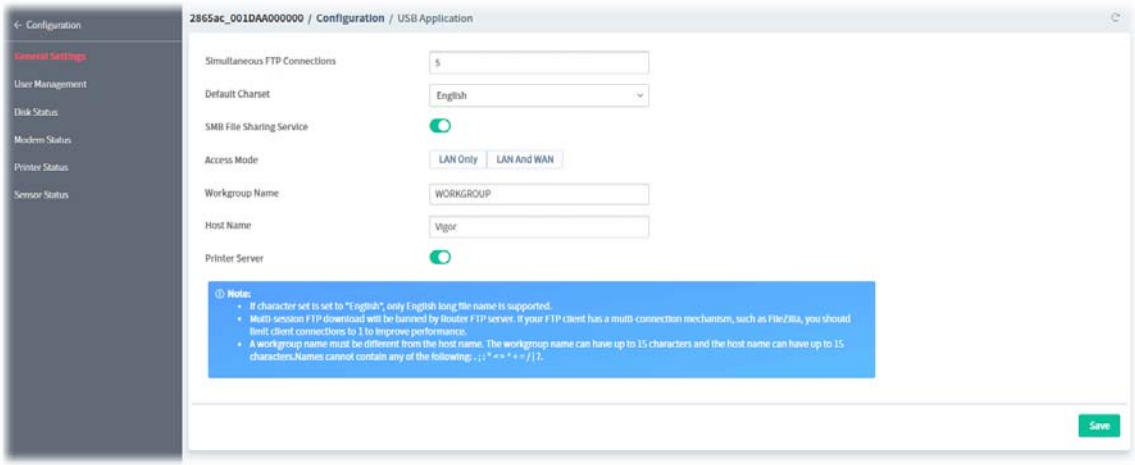

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Click to enable or disable the bandwidth limit function. |
| **Cancel** | Discard current modification. |
| **Save** | Save the current settings. |

## 9.4.15 USB Applications

### 9.4.15.1 General Settings

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.



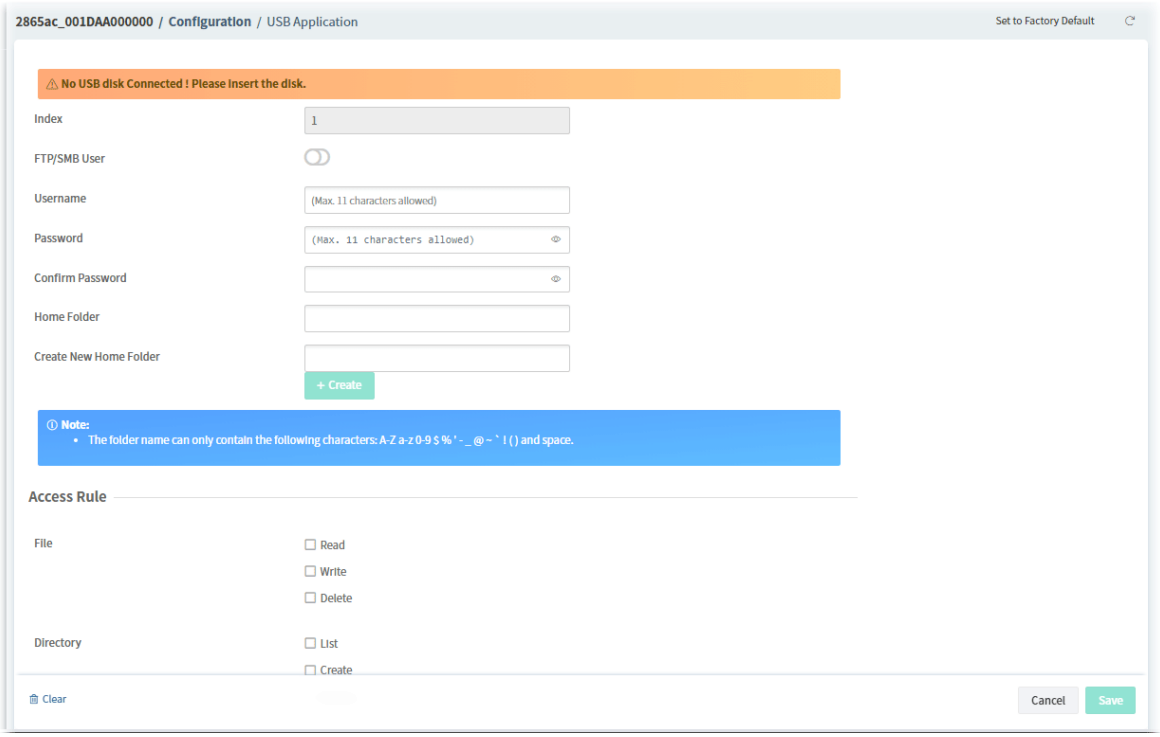

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Simultaneous FTP Connections** | Enter the maximum number of simultaneous FTP sessions allowed. |
| **Default Charset** | Select the character set for file and directory names. |
| **SMB File Sharing Service** | Click to enable / disable the function. |
| **Access Mode** | **LAN Only -** Only users on the LAN can connect access the shared USB disk.<br>**LAN and WAN -** Both LAN and WAN users can access SMB server of the router. |
| **Workgroup Name** | Enter the workgroup name. Maximum allowed length is 15 characters. |
| **Host Name** | Enter the NetBIOS hostname for the router. Maximum allowed length is 23 characters. |
| **Printer Server** | Click to enable / disable the function.<br>If enabled, the Vigor router can act as a print server for printers connected the USB. |
| **Save** | Save the current settings. |

### 9.4.15.2 User Management

This page allows you to set up profiles for FTP/SMB users.

To configure the user management settings, move the mouse cursor to any entry and click to open the following page.



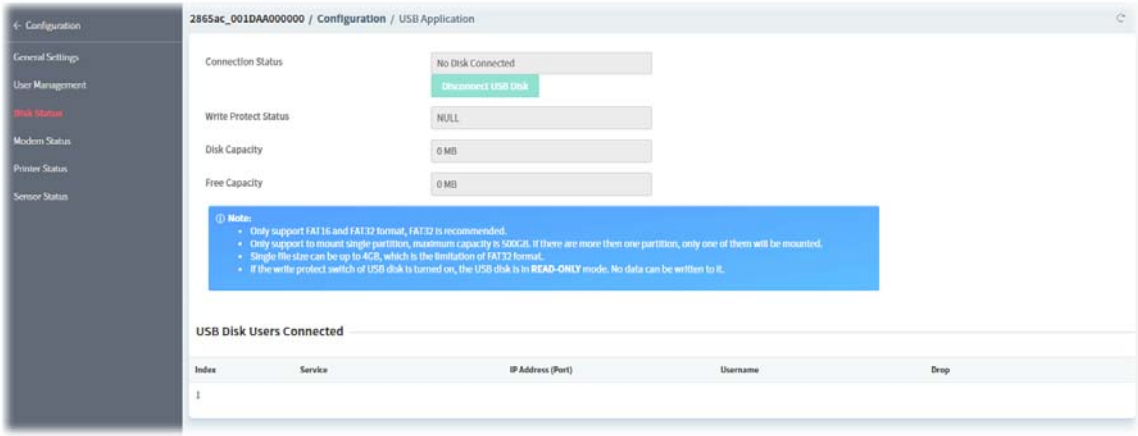

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Index** | Displays the index number of USB application profile. |
| **FTP/SMB User** | Click to enable / disable the function.<br>If enabled, this profile (account) for FTP service and / or SMB service will be activated. |
| **Username** | Enter the username for this user profile. |
| **Password** | Enter the password for this user profile. |
| **Confirm Password** | Enter the password again to confirm. |
| **Home Folder** | Enter the folder which will be the root folder for FTP and SMB sessions established using the credentials of this user profile. |
| **Create New Home Folder** | Enter a name as a new folder name.<br>**+Create** - Click to create a new folder. |
| | **Access Rule** |
| **Access Rule** | **File** – Check the items (Read, Write and Delete) for such profile.<br>**Directory** –Check the items (List, Create and Remove) for such profile. |

| | |
|---|---|
| **Clear** | Clear all modifications on this page. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

### 9.4.15.3 Disk Status

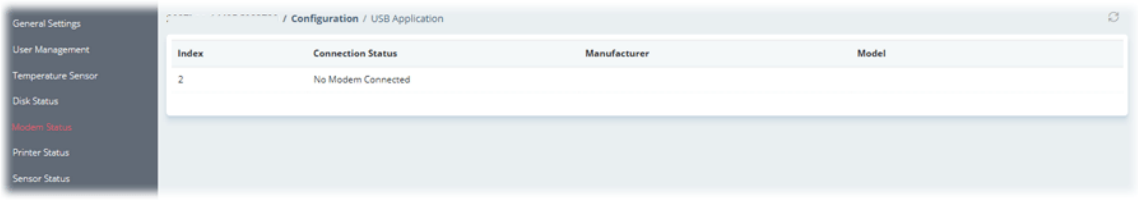
This page displays the status information for the USB disk connecting to Vigor router.



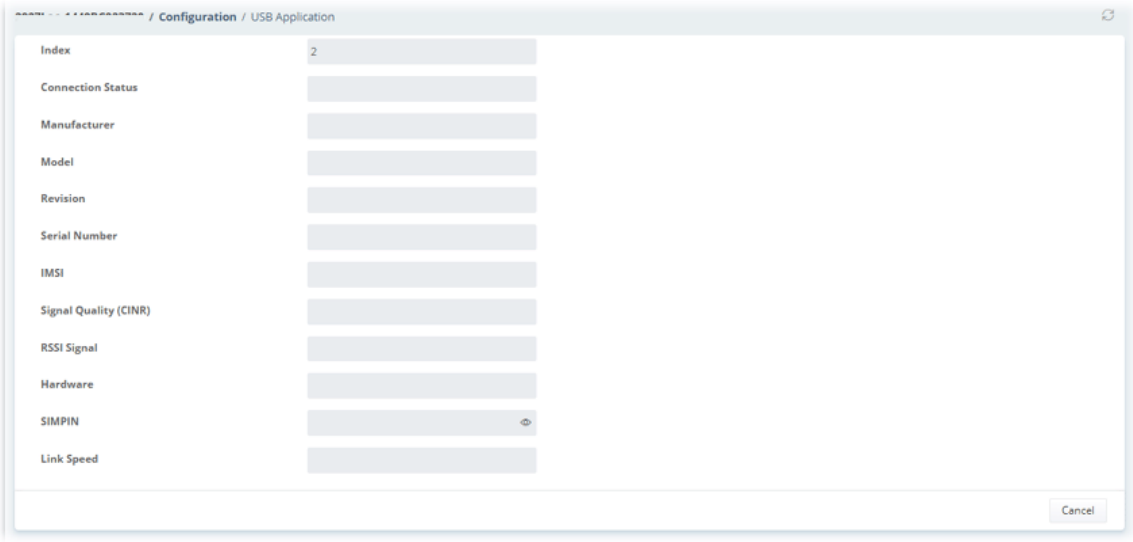

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Connection Status** | Displays if the USB is connected or disconnected.<br>**Disconnect USB Disk -** If connected, click to disconnect USB disk with the router. |
| **Write Protect Status** | Displays the total capacity of the USB storage disk. |
| **Disk Capacity** | Displays the disk capacity. |
| **Free Capacity** | Displays the free space on the USB storage disk. |
| **USB Disk Users Connected** | Displays the clients that are connected to the SMB/FTP server. |

### 9.4.15.4 Modem Status

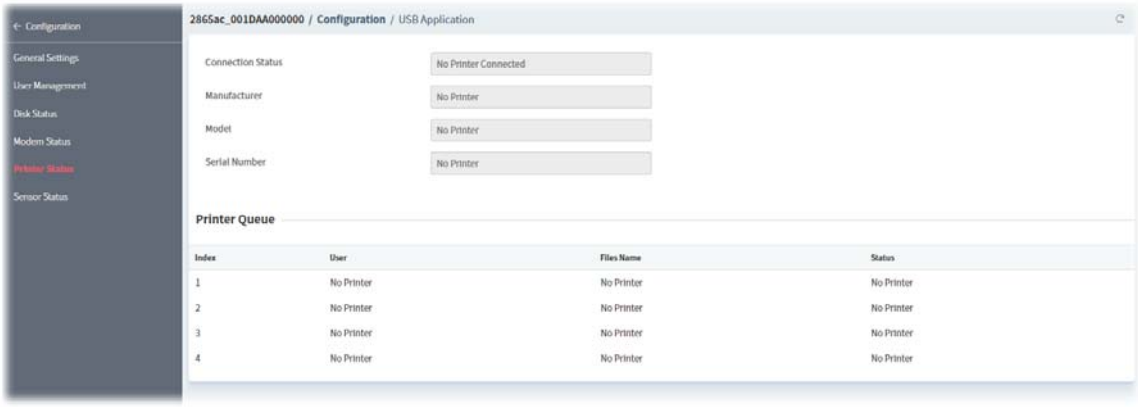



Click the index number to open the following for viewing detailed information for parameter settings.



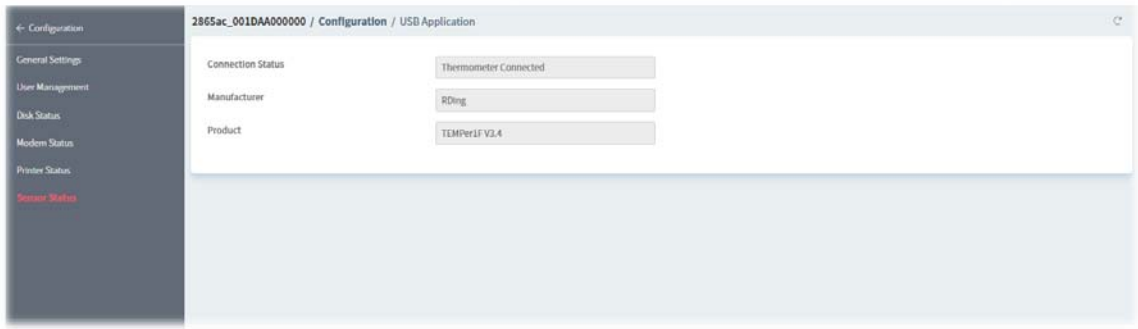

### 9.4.15.5 Printer Status

This page displays current status for the USB printer connecting to Vigor router managed by VigorACS 3.




### 9.4.15.6 Sensor Status

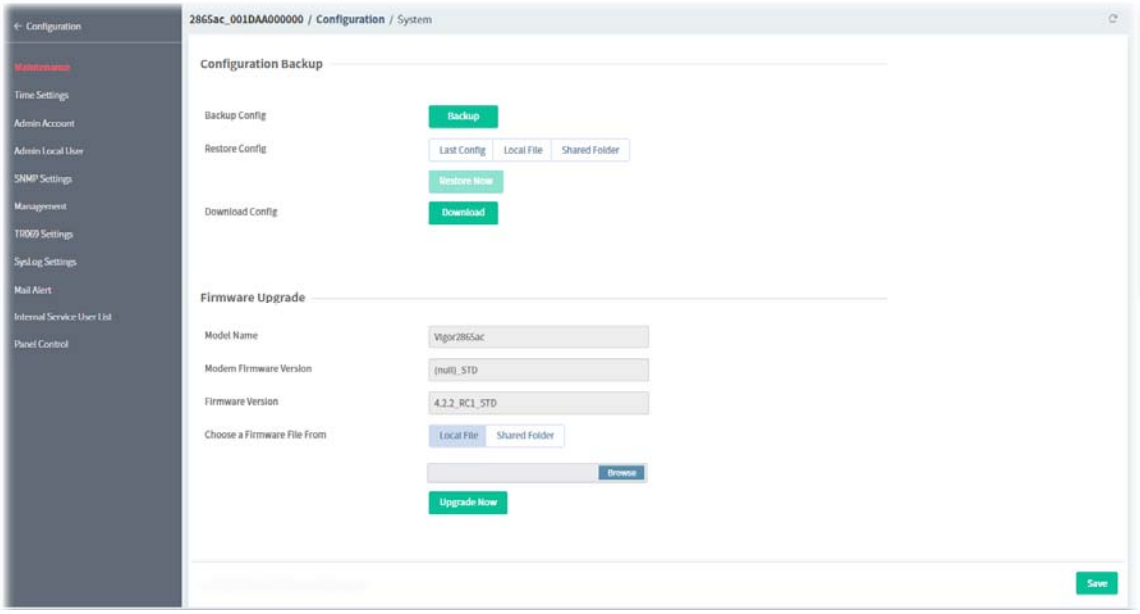
This page displays current status for the USB thermometer connecting to Vigor router managed by VigorACS 3.



## 9.4.16 System

### 9.4.16.1 Maintenance

This page can be used for backup configuration for specified CPE, restoring configuration for specified CPE, making firmware upgrade for CPE, and even reboot the specified CPE via VigorACS 3.



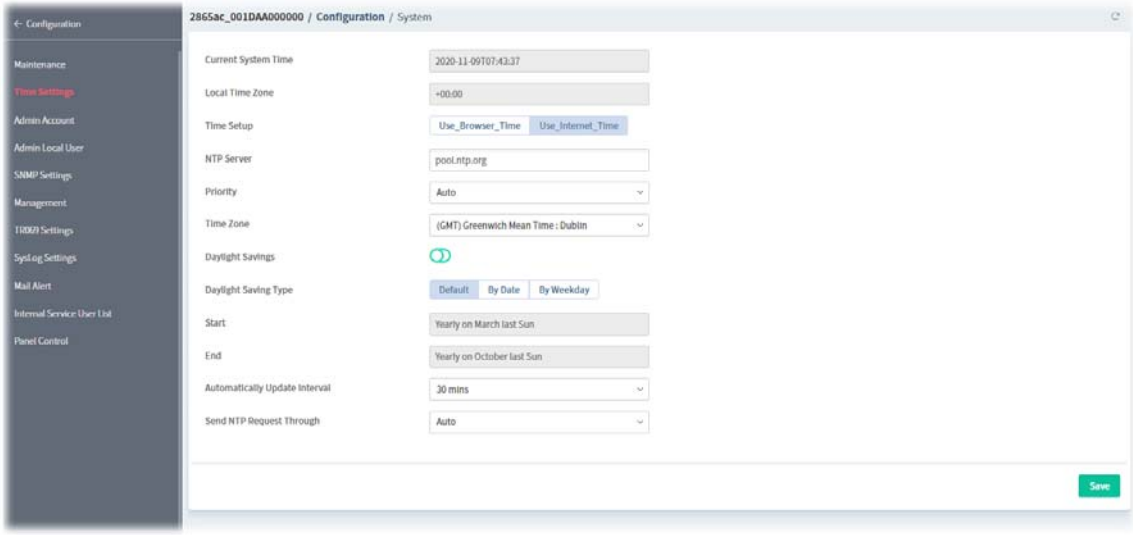

These parameters are explained as follows:

| Item | Description |
|---|---|
| | **Configuration Backup** |
| **Backup Config** | **Backup -** Click to backup the configuration from CPE to VigorACS server. |
| **Restore Config** | Select the type of configuration file.<br>● **Last Config**<br>● **Local FIle**<br>● **Shared Folder**<br>**Restore Now -** Click to initiate restoration of configuration immediately. |
| **Download Config** | **Download -** Click to download the lastest configuration backup file from VigorACS server. |
| | **Firmware Upgrade** |
| **Model Name** | Displays the model name of the CPE. |
| **Modem Firmware Version** | Displays the modem version of the CPE.<br>No DSL - It indicates the selected CPE is non-DSL device. |
| **Firmware Version** | Displays the firmware version used by the CPE. |
| **Choose a Firmware File From** | **Local File -** Select a firmware from the host by clicking **Browse**.<br>**Shared Folder -** Select a firmware from the database by click **Browse**.<br>**Upgrade Now -** Click to upgrade the firmware immediately. |
| | **Automatic Firmware Recovery** |
| **Enable** | Click to enable or disable the function. |

| | |
|---|---|
| | If enabled, when the router unexpectedly reboots three times in a row then the backup firmware will be restored to the unit on the third reboot. |
| | **Backup Setting** |
| **Backup Mode** | **Backup after reboot -** The backup will be executed after the router reboot.<br>**Backup after system uptime -** The backup of current running firmware will be executed after a period of time. The default is 24 hours (1 day).<br>**Backup manually -** The backup will be executed manually according to your request. |
| **Backup Firmware** | Displays the backup firmware version of the CPE. |
| **Last backup** | Displays the time for the last backup for the CPE. |
| | **Device Reboot** |
| **Restart the device** | **Reboot Now -** Click to reboot the router immediately. |
| | **Reset** |
| **Reset to factory default** | **Reset Now -** Click to reset the router with factory default setting immediately. |
| **Save** | Save the current settings. |

### 9.4.16.2 Time Settings

This page allows you to configure settings related to the system date and time.



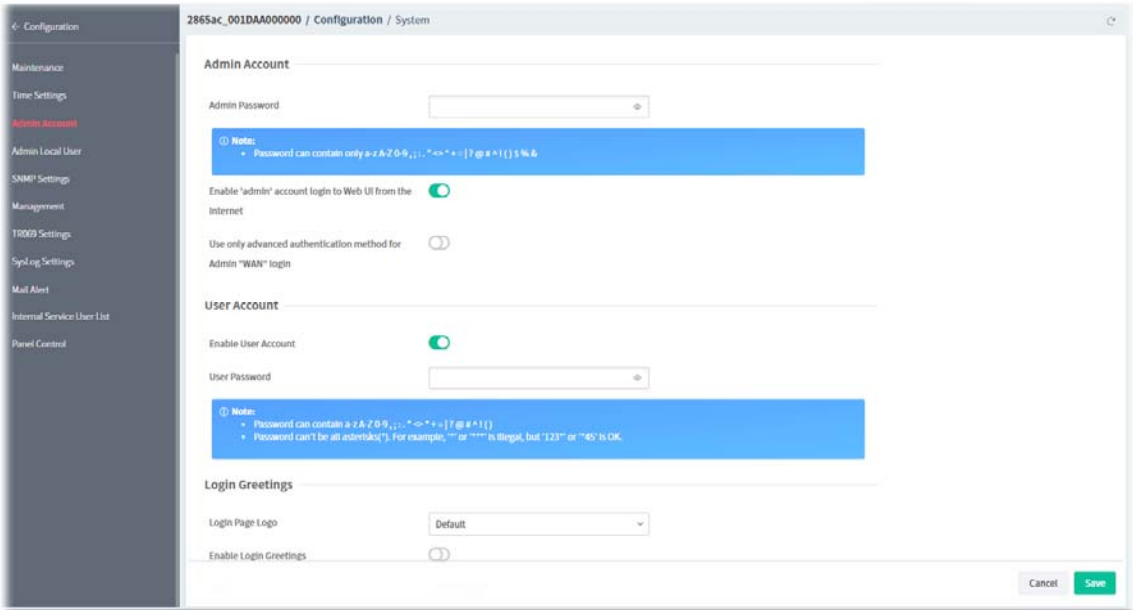

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Current System Time** | Displays the current time obtained from the time server. |
| **Local Time Zone** | Displays the time zone where the router is located. |
| **Time Setup** | **Use_Browser_Time -** Click to let the router set its system time using the time reported by the web browser.<br>**Use_Internet_Time -** Click to let the browser set its system time by retrieving time information from the specified network time server using the Network Time Protocol (NTP). |
| **NTP Server** | Enter the address of the time server. |

| | |
|---|---|
| **Priority** | Select **Auto** or **IPv6 First** as the priority. |
| **Time Zone** | Select the time zone where the router is located. |
| **Daylight Savings** | Click to enable or disable the Daylight Saving Time (DST) if it is applicable to your location. |
| **Daylight Savings Type** | **Default -** Uses the default DST schedule for the time zone.<br>**By Date -** Select this option if DST starts and ends on fixed dates.<br>**By Weekday -** Select this option if DST starts and ends on certain days of the week. |
| **Start** | It is available when By Date is selected as Daylight Saving Type.<br>Use the drop down list to select month, day and hour settings as the starting point. |
| **End** | It is available when By Date is selected as Daylight Saving Type.<br>Use the drop down list to select month, day and hour settings as the ending point. |
| **Automatically Update Interval** | Select the time interval at which the router updates the system time. |
| **Send NTP Request Through** | Select a WAN interface to send NTP request for time synchronization. |
| **Save** | Save the current settings. |

### 9.4.16.3 Admin Account

This page allows you to set or change the administrator password.



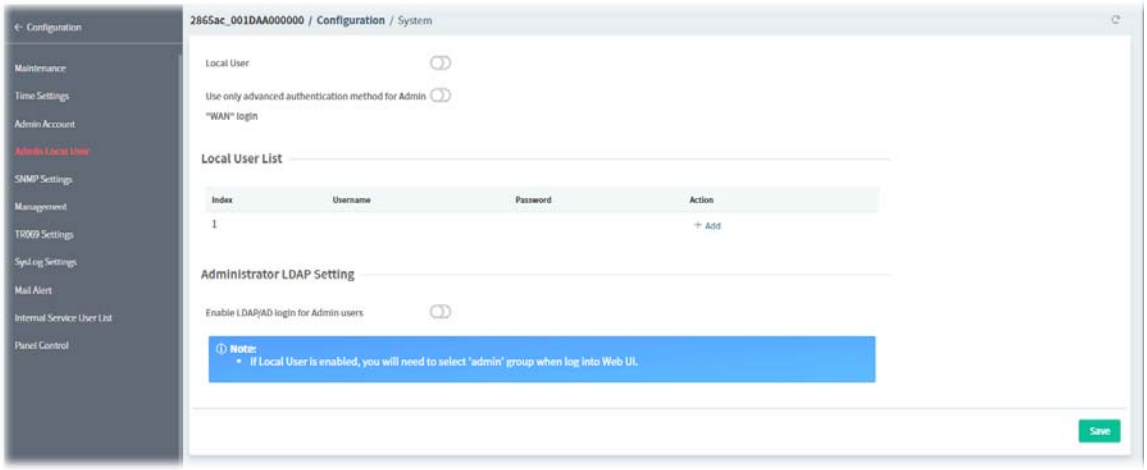

These parameters are explained as follows:

| Item | Description |
|---|---|
| | **Admin Account** |
| **Admin Password** | Enter the new password. |
| **Enable admin account login to..** | Click to enable or disable the function.<br>If enabled, it allows the administrator to log in from the Internet. This |

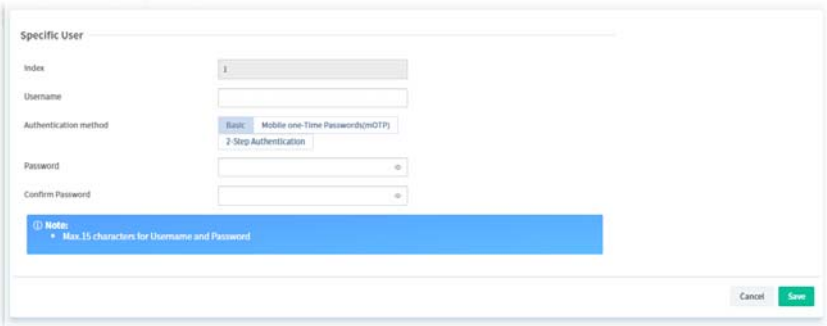
| | |
|---|---|
| | option is enabled when Administrator Local Account is enabled (see below). |
| **Use only advanced authentication..** | Click to enable or disable the function.<br>If enabled,<br>**Advanced Authentication -** Advanced authentication method can offer a **more secure** network connection. Select to require mOTP or 2-step authentication when logging in from the WAN.<br>● **Mobile one-Time Password (mOTP) -** Enter the PIN Code and Secret settings for getting one-time passwords.<br>● **2-Step Authentication -** Select the SMS and/or Mail profiles and the destination SMS number and/or email address for transmitting the password. |
| | **User Account** |
| **Enable User Account** | Click to enable or disable the function.<br>If enabled, other users are allowed to administer the router. |
| **User Password** | Enter a string as the password for the user account. |
| | **Login Greetings** |
| **Login Page Logo** | **Default** - Choose it to use the default image.<br>**Blank** - Choose it to discard the logo image.<br>**Upload a file** - Choose it to specify an image as the logo. |
| **Enable Login Greetings** | Click to enable or disable the function. |
| **Logo Image Upload** | It is available when Upload a file is selected as Login Page Logo.<br>**Browse** - Click to select an image file.<br>**+Upload** - Click to upload the selected image file to VigorACS. |
| **Title** | Enter a brief description (e.g., Welcome to DrayTek) which will be shown on the heading of the login dialog. |
| **Message** | Enter words or sentences here. It will be displayed for bulletin message. In addition, it can be displayed on the login dialog at the bottom. |
| **Cancel** | Discard current modification. |
| **Save** | Save the current settings. |

#### 9.4.16..4 Admin Local User

Usually, the system administrator has the highest privilege to modify the settings on the web user interface of the Vigor router. However, in some cases, it might be necessary to have other users in LAN to access into the web user interface of Vigor router.

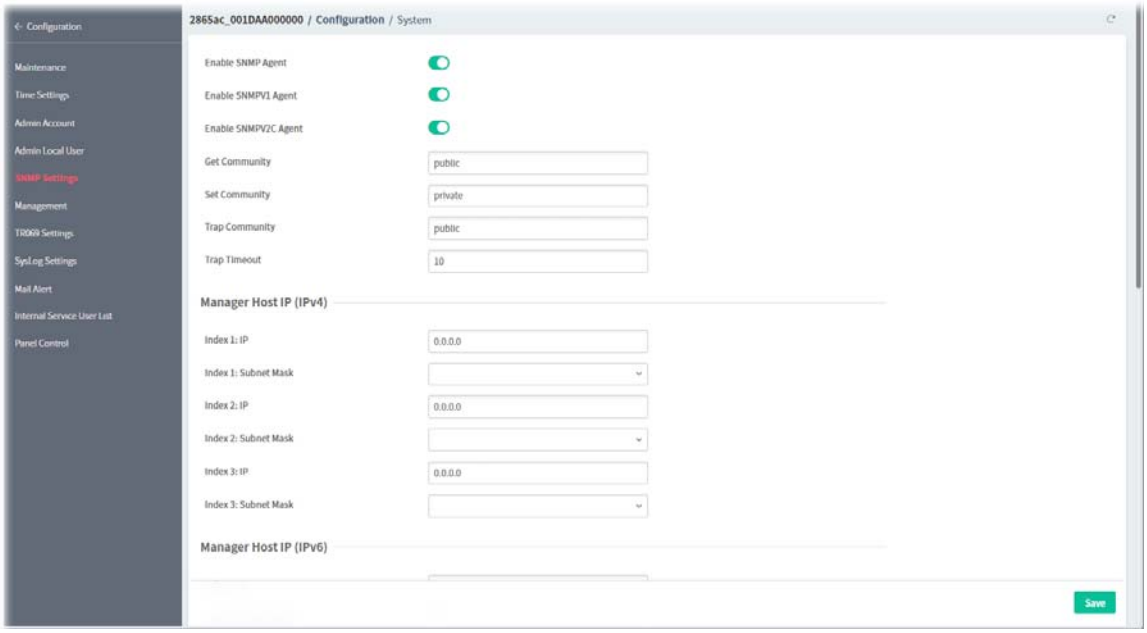



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Local User** | Click to enable or disable the local user setting. |
| **Use only advanced authentication method for Admin "WAN" login** | Advanced authentication method can offer a **more secure** network connection. Select to require mOTP or 2-step authentication when logging in from the WAN. |
| **Local User List** | **Index -** Displays the index number of local user profile.<br>**User Name -** Displays the name of the local user profile.<br>**Password -** Displays the password of the local user profile.<br>**Action +Add -** Click to create a new user profile.<br>  <br>● **Index** - Displays the index number of the profile.<br>● **Username** - Enter the name of the user profile.<br>● **Authentication method** - Choose Basic, mOTP or 2-Step Authentication.<br>○ If **Basic** is selected **-** Enter the password.<br>○ If **Mobile one-Time Password (mOTP)** is selected**-** Enter the PIN Code and Secret settings for getting one-time passwords.<br>○ If **2-Step Authentication** is selected**-** Select the SMS and/or Mail profiles and the destination SMS number and/or email address for transmitting the password. |
| | **Administrator LDAP Setting** |
| **Enable LDAP/AD login for Admin users** | Click to enable or disable the LDAP/AD login profile. |
| **Save** | Save the current settings. |

### 9.4.16.5 SNMP Settings

This page allows you to configure settings for SNMP and SNMPv3 services.



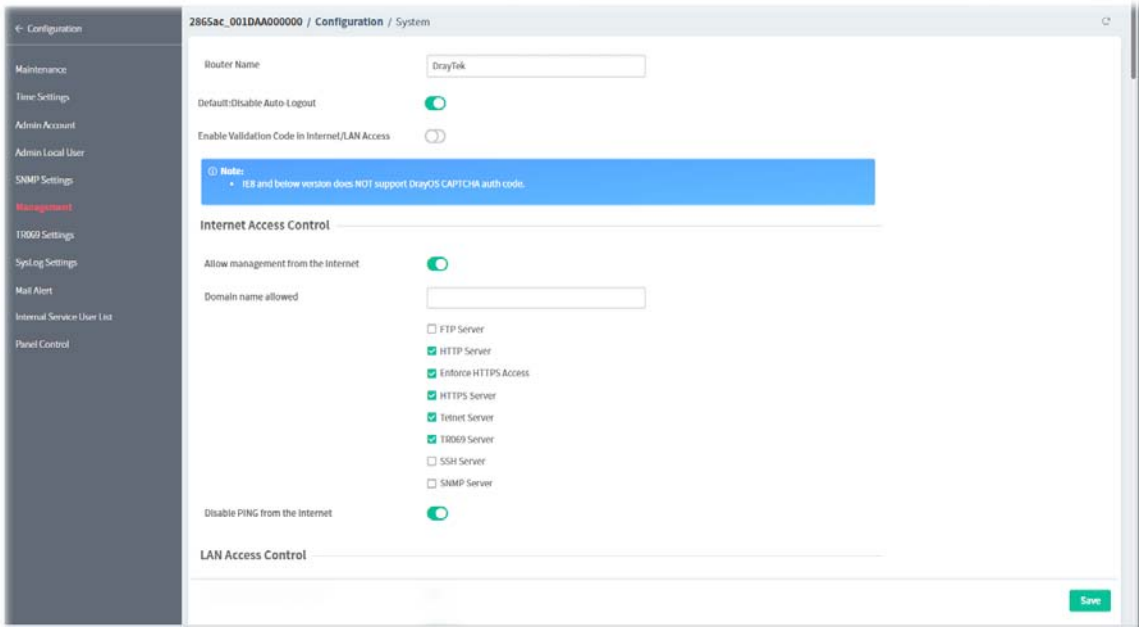

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Enable SNMP Agent / Enable SNMPV1 Agent / Enable SNMPV2C Agent** | Click to enable or disable the SNMP function. |
| **Get Community** | Enter the Get Community string. The default setting is public. |
| **Set Community** | Enter the Set Community string. The default setting is private. |
| **Trap Community** | Enter the Trap Community string. The default setting is public. |
| **Trap Timeout** | The default setting is 10 seconds. |
| | **Manager Host IP (IPv4)** |
| **Index #:IP** | Enter the IPv4 address of hosts that are allowed to issue SNMP commands. |
| **Index #: Subnet Mask** | Select a subnet mask for IP address configured above. |
| | **Manager Host IP (IPv6)** |
| **Index #: IP** | Enter the IPv6 address of hosts that are allowed to issue SNMP commands. |
| **Index #: Prefix Length** | Enter the fixed value for prefix length. |
| | **Notification Host IP (IPv4)** |
| **Index #: IP** | Enter the IPv4 address of hosts that are allowed to be sent SNMP traps. |
| | **Notification Host IP (IPv6)** |
| **Index #: IPv6 Address** | Enter the IPv6 address of hosts that are allowed to be sent SNMP traps. |
| | **SNMPV3 Agent** |
| **Enable SNMPV3 Agent** | Click to enable or disable the SNMPv3 function. |

| | |
|---|---|
| **USM User** | Enter the username to be used for authentication |
| **Auth Algorithm** | Select one of the hashing methods to be used with the authentication algorithm. |
| **Auth Password** | Enter a password for authentication. |
| **Privacy Algorithm** | Select an encryption method as the privacy algorithm. |
| **Privacy Password** | Enter a password for privacy. |
| **Save** | Save the current settings. |

### 9.4.16.6 Management

This page allows you to manage the settings for Internet/LAN Access Control, Access List from Internet, Management Port Setup, TLS/SSL Encryption Setup, CVM Access Control and Device Management.




These parameters are explained as follows:

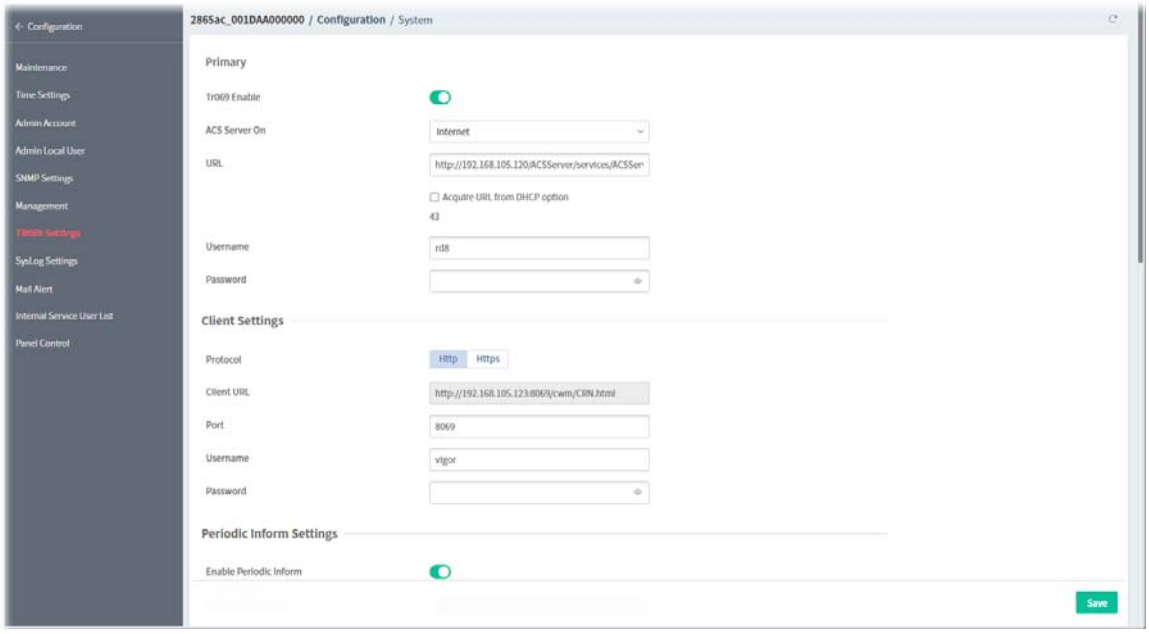
| Item | Description |
|---|---|
| **Router Name** | Enter the router name as provided by ISP. |
| **Default:Disable Auto-Logout** | Click to enable or disable the function.<br>If enabled, the auto-logout function for web user interface will be disabled |
| **Enable Validation Code in Internet/LAN Access** | Click to enable or disable the function.<br>If enabled, Vigor router will require users to enter a validation code as shown in an image when they log in. |
| | **Internet Access Control** |
| **Allow management from the Internet** | Click to enable or disable the function.<br>If enabled, it allows system administrators to login from the Internet, and then select the specific services that are allowed to be remotely administered. |
| **Domain name allowed** | Enter a domain name.<br>This setting is only available if DNS filtering is enabled, applying DNS filter profile in firewall rules, or enabling DNS Filter Local Setting. |

| | |
|---|---|
| **Disable PING from the Internet** | Click to enable or disable the function.<br>If enabled, it will reject all PING packets from the Internet. For increased security, this setting is enabled by default. |
| | **LAN Access Control** |
| **Allow management from LAN** | Click to enable or disable the function.<br>If enabled, it allows system administrators to login from LAN interface.<br>There are several servers provided by the system which allow you to manage the router from LAN interface. Check the box(es) to specify. |
| **Apply to Subnet** | Click to enable or disable the LAN interface.<br>If enabled, the selected interface can be used for accessing into web user interface of Vigor router.<br>**IP Object Enable** - Click to enable or disable the IP object setting.<br>**Index in IP Object** - Enter the index number of the IP object profile. Related IP address will appear automatically. |
| | **IPv6 Management Setup** |
| **Allow management from the Internet** | Click to enable the function. Select the servers that system administrators are allowed to manage from the Internet. |
| **Disable PING from the Internet** | Click to reject all PING packets from the Internet. For increased security, this setting is enabled by default. |
| | **IPv6 Address Security Option** |
| **Enable Random Interface Identifiers...** | Click to enable or disable the function.<br>If enabled, the IPv6 address will be generated randomly but not using LAN/WAN MAC to prevent the attack from the hacker. |
| | **Access List from the Internet** |
| **Apply Access List to PING** | Click to enable or disable the function.<br>**Access List #: IP Object** - Enter the index number of the IP object profile. Related IP address will appear automatically. |
| | **IPv6 Access List** |
| **Apply Access List to PING** | Click to enable or disable the function.<br>**Access List #: IPv6 Object** - Enter the index number of the IP object profile. Related IP address will appear automatically. |
| | **Management Port Setup** |
| **Management Port Setup** | **User Define Ports -** Specify user-defined port numbers for the Telnet, HTTP, HTTPS, FTP, TR-069 and SSH servers.<br>**Default Ports -** Use standard port numbers for the Telnet and HTTP servers. |
| | **Brute Force Protection** |
| **Enable brute force login protection** | Click to enable or disable the function.<br>If enabled, any client trying to access into Internet via Vigor router will be asked for passing through user authentication. |
| **Maximum login failure** | Specify the maximum number of failed login attempts before further login is blocked. |
| **Penalty period** | Set the lockout time after maximum number of login attempts has been exceeded. The user will be unable to attempt to log in until the specified time has passed. |

| | |
|---|---|
| | **Blocked IP List** |
| **Table** | Display, in a new browser window, IP addresses that are currently blocked from logging into the router. |
| | **TLS/SSL Encryption Setup** |
| **TLS 1.3, 1.2, 1.1, 1.0 Enable, SSL 3.0 Enable** | Check the box to enable SSL 3.0/1.0/1.1/1.2 encryption protocols. |
| | **CVM Access Control** |
| **Enable CVM Port** | Click to enable or disable the function. |
| **CVM Port** | Check the box to enable Central VPN Management port setting. |
| **Enable CVM SSL Port** | Click to enable or disable the function. |
| **CVM SSL Port** | Check the box to enable Central VPN Management SSL port setting. |
| | **AP Management** |
| **Enable AP Management** | Click to enable or disable the access point management function. |
| | **Device Management** |
| **Device Management** | Click to enable or disable the device management function. |
| **Respond to external device** | Click to enable or disable the function.<br>If enabled, the router will function as a slave device. |
| **Save** | Save the current settings. |

### 9.4.16.7 TR069 Settings

CPE device supports the TR-069 standard for remote management by VigorACS.




These parameters are explained as follows:

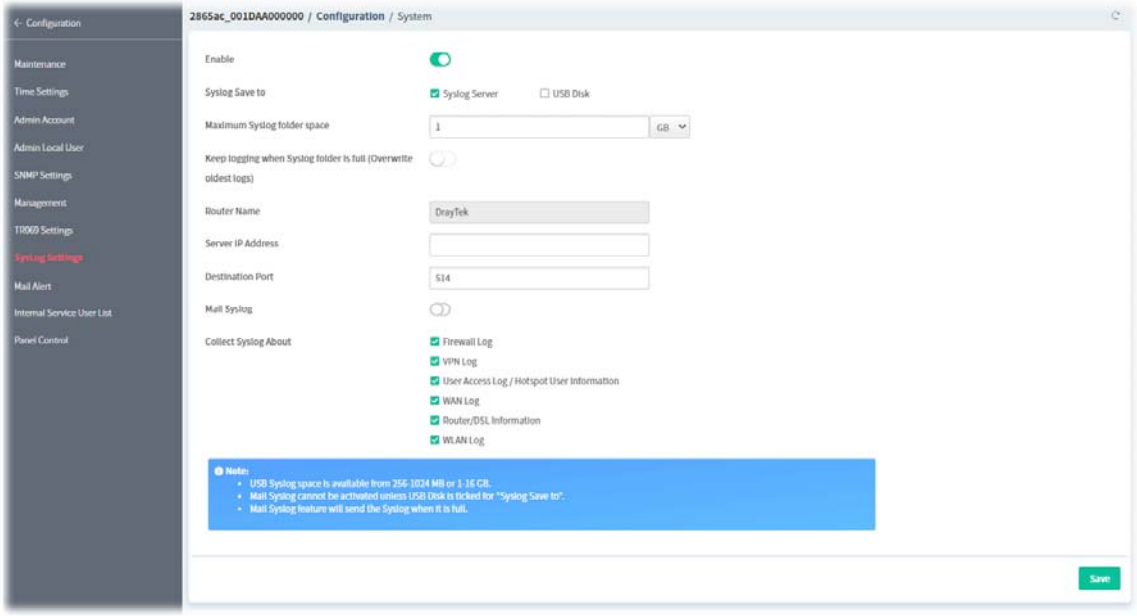
| Item | Description |
|---|---|
| | **Primary** |

| | |
|---|---|
| **Tr069 Enable** | Click to enable or disable the TR-069 functionality. |
| **ACS Server On** | Choose the interface for connecting the router to the Auto Configuration Server. |
| **URL** | Enter the URL for connecting to the ACS.<br>**Acquire URL from DHCP option 43 -** Select to acquire the ACS URL from DHCP option 43. |
| **Username** | Enter the username required to connect to the ACS server. |
| **Password** | Enter the password required to connect to the ACS server. |
| | **Client Settings** |
| **Protocol** | Select Https if the connection is encrypted; otherwise select Http. |
| **Client URL** | Displays the URL of the client. |
| **Port** | In the event of port conflicts, change the port number of the CPE. |
| **Username** | Enter the username that the VigorACS will use to connect to the CPE. |
| **Password** | Enter the password that the VigorACS will use to connect to the CPE. |
| | **Periodic Inform Settings** |
| **Enable Periodic Inform** | Click to enable or disable the function.<br>If enabled, the CPE Client will periodically connect to the ACS Server to update its connection parameters at intervals specified in the Interval Time field. |
| **Inform Interval (sec.)** | Set interval time or schedule time for the router to send notification to CPE. |
| | **STUN Settings** |
| **Enable STUN** | Click to enable or disable the function. |
| **Server Address** | Enter the IP address of the STUN server. |
| **Server Port** | Enter the port number of the STUN server. |
| **Maximum Keep Alive Period** | Enter the maximum interval between keep-alive messages that the CPE client sends to the ACS server. |
| **Minimum Keep Alive Period** | Enter the minimum interval between keep-alive messages that the CPE client sends to the ACS server. |
| | **Advanced** |
| **Disable TR069 configuration change from CPE UI** | Click to enable or disable the function. |
| | **Apply Settings to APs** |
| **Enable** | Click to enable or disable the function. |
| **AP Password** | Enter the password of the VigorAP that you want to apply Vigor router's TR-069 settings |
| **Apply Specific STUN Settings to APs** | Click to enable or disable the function of applying specific STUN settings to AP.<br>If enabled,<br>**Enable AP STUN** - Click to enable or disable the STUN server settings.<br>**Server Address** - Enter the IP address of the STUN server. |

| | |
|---|---|
| | **Server Port** - Enter the port number of the STUN server.<br>**Maximum Keep Alive Period** - Enter the maximum interval between keep-alive messages that the CPE client sends to the ACS server.<br>**Minimum Keep Alive Period** - Enter the minimum interval between keep-alive messages that the CPE client sends to the ACS server. |
| | **CPE Notification Settings** |
| **Enable** | Click to enable or disable the function.<br>If enabled, select the notification item(s) by clicking it. Vigor router will send the utilization status to VigorACS.<br>● **Web Login**<br>● **Web Configuration**<br>● **High Availability**<br>● **SSH Login**<br>● **SSH Command** |
| **Bandwidth Utilization** | **Enable** - Click to enable or disable this function. To administrator, this feature is useful to monitor the bandwidth utilization of CPE(s). When the bandwidth used is over the threshold level (percentage defined in medium and high fields), a notification will be sent to VigorACS. After a long time observation, the administrator can determine if it is necessary to increase the bandwidth setting for that CPE or not. The default is **disabled**.<br>**Time Period** – Choose the time interval (15 mins, 30 mins, 1hour, 3 hours, or 6 hours) for CPE to send a notification of bandwidth utilization to VigorACS.<br>● **Enable / WAN** – Choose the WAN interface by clicking **Enable** for applying the bandwidth utilization notification mechanism.<br>● **Threshold Level** – Set the percentage of bandwidth in transmission and receiving data as threshold values for CPE to detect bandwidth utilization.<br>● **Line Speed** – Set the transmission rate and receiving rate for specified WAN interface. |
| **Save** | Save the current settings. |

### 9.4.16.8 SysLog Settings

SysLog function is provided for users to monitor router.

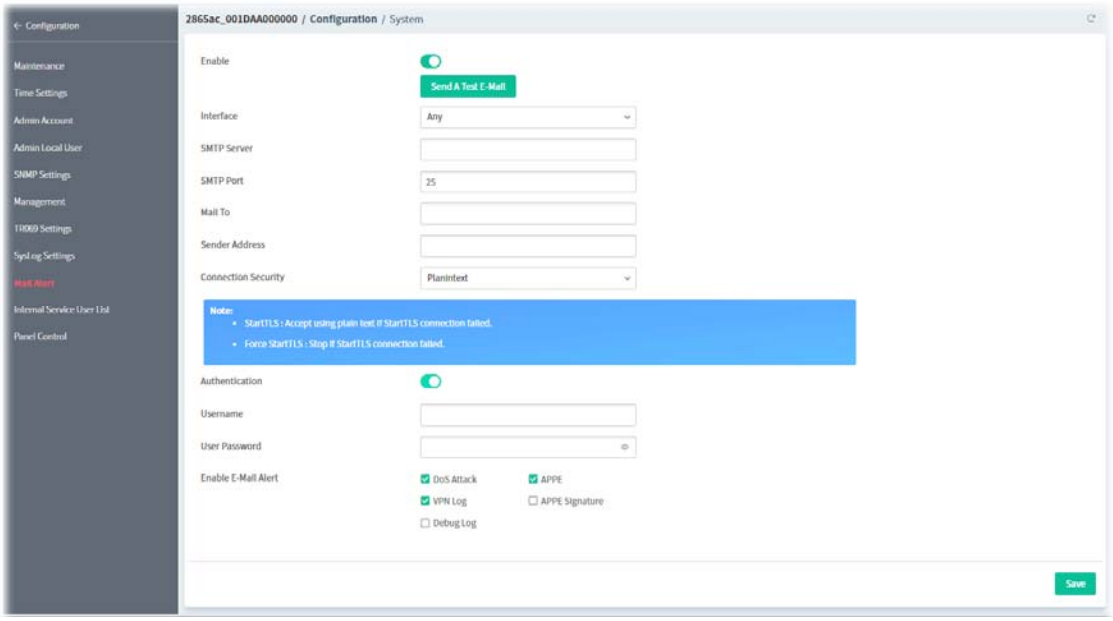



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Click to enable or disable the Syslog function. |
| **Syslog Save to** | Select Syslog Server and / or USB Disk. |
| **Maximum Syslog folder space** | Set a space (unit GB/MB) to store event logs. |
| **Keep logging when Syslog folder is full..** | Click to enable or disable the function.<br>If enabled, the action of overwriting the olderest logs or stopping logging will be executed. |
| **Router Name** | Display the name for this router. |
| **Server IP Address** | Enter the IP address of the Syslog server. |
| **Destination Port** | Enter a port for the Syslog protocol. |
| **Mail Syslog** | Click to enable or disable the function.<br>If enabled, it will record the mail event on Syslog. |
| **Collect Syslog About** | Select the type of log to send the corresponding message to syslog. |
| **Save** | Save the current settings. |

### 9.4.16.9 Mail Alert

This page allows to configure settings for Mail alert.

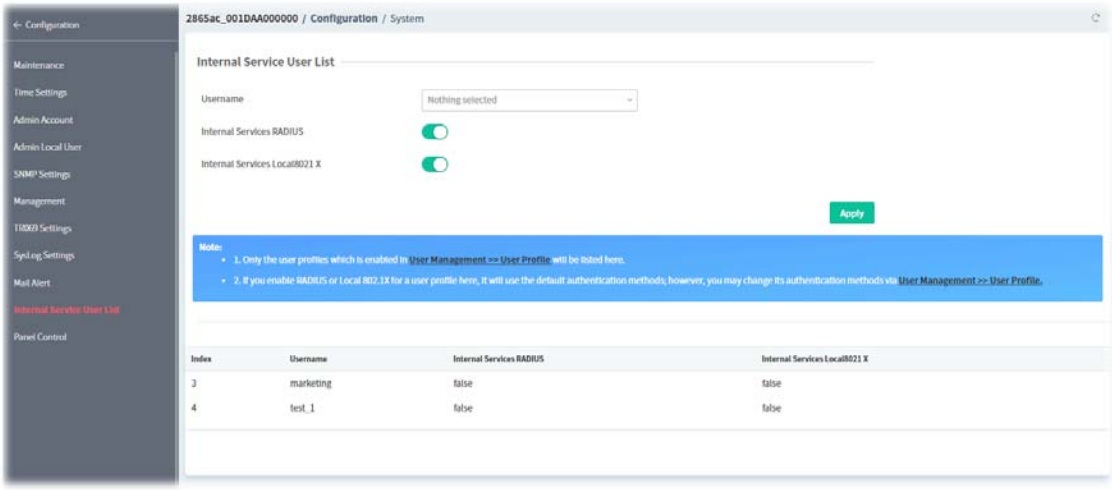



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Enable** | Click to enable or disable the mail alert function.<br>**Send Test E-Mail** - Make a simple test for the e-mail address specified in this page. |
| **Interface** | Specify an interface. |
| **SMTP Server** | Enter an IP address of the SMTP server. |
| **SMTP Port** | Enter the port number of the SMTP server. |
| **Mail To** | Specify a mail address for receiving the mail. |
| **Sender Address** | Specify a mail address for sending mails out. |
| **Connection Security** | Select a method (Plaintext, SSL, StartTLS or Force StartTLS) to ensure the connection security. SSL means to use port 465 for SMTP server for some e-mail server uses https as the transmission method.<br>● Accept using plain text if StartTLS connection failed.<br>● Force StartTLS. Stop if StartTLS connection failed. |
| **Authentication** | Click to enable or disable the function.<br>If enabled, the authentication will be activated while using an e-mail application. |
| **Username** | Enter the user name for authentication. |
| **User Password** | Enter the password for authentication. |
| **Enable E-Mail Alert** | Select the item(s) to send the alert message to the e-mail box while the router detecting the item(s) you specify here. |
| **Save** | Save the current settings. |

### 9.4.16.10 Internal Service User List

This page allows you to turn on or turn off security authentication service (offered by internal RADIUS and/or Local 802.1X) for each user profile without accessing into the User Management configuration page.

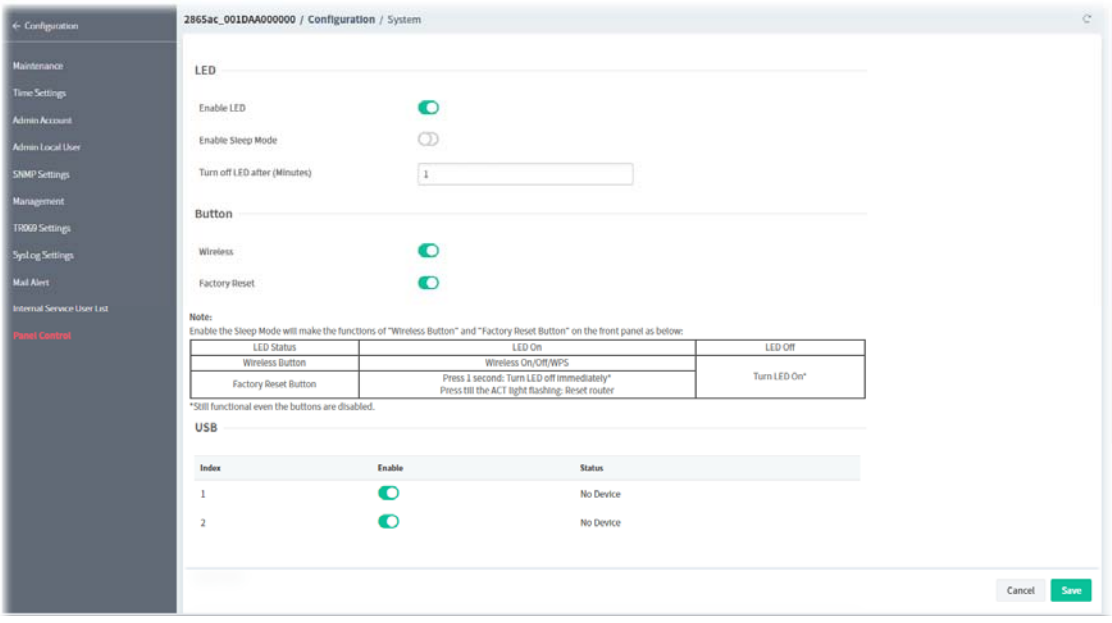



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Username** | Display the name of the existed user profile. |
| **Internal Services RADIUS** | Click to enable (turn on) or disable (turn off) the security authentication service offered by the internal RADIUS server for the user profile. |
| **Internal Services Local802.1X** | Click to enable (turn on) or disable (turn off) the security authentication service offered by the Local 802.1X server for the user profile. |
| **Apply** | Save the current settings. |

### 9.4.16.11 Panel Control

This page allows you to customize the behavior of the LEDs, buttons, WLAN, USB and LAN ports on the front panel.



These parameters are explained as follows:

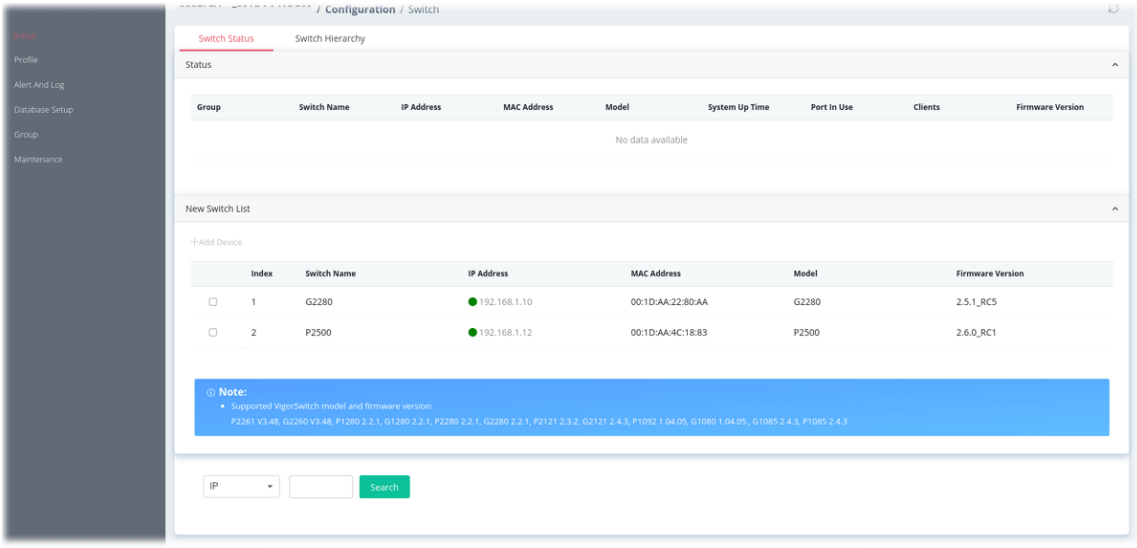
| Item | Description |
|---|---|
| | **LED** |
| **Enable LED** | Click to enable or disable the LEDs to function according to the configured settings. |
| **Enable Sleep Mode** | Click to enable (turn on) or disable (turn off) the LEDs after the specified number of minutes has elapsed. |
| **Turn off LED after (Minutes)** | Enter a number. |
| | **Button** |
| **Wireless** | Click to enable or disable the ability of the Wireless button to control WLAN and WPS functions. |
| **Factory Reset** | Click to enable or disable the reset function of the factory reset button. |
| | **USB** |
| **Enable** | Click to enable or disable the USB port. |
| | **LAN Port** |
| **Enable** | Click to enable or disable the LAN port. |
| **Status** | Displays the status of the USB port. |
| **Speed** | Displays the negotiated speed of the LAN port. |
| **Cancel** | Discard current modification. |
| **Save** | Save the current settings. |

## 9.4.17 Switch

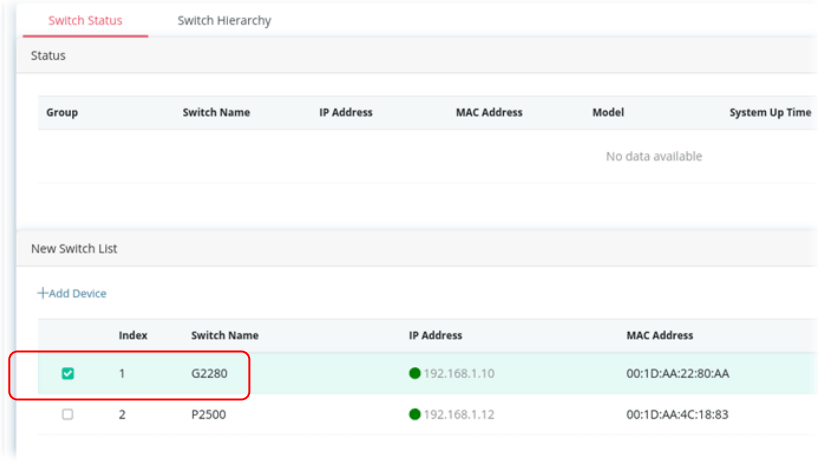
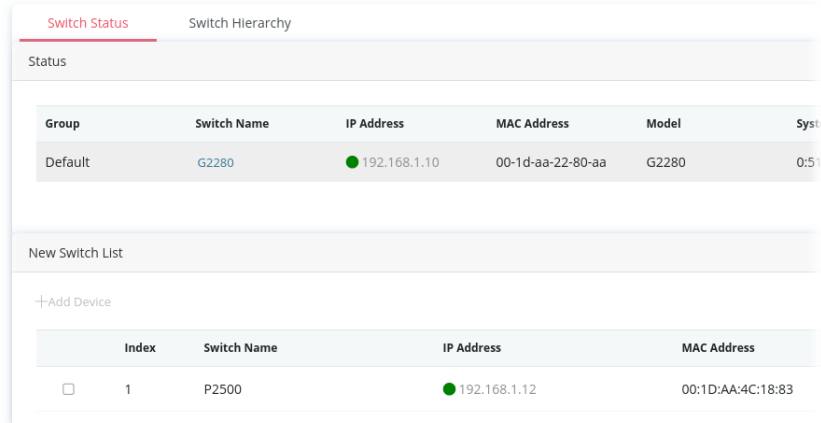
### 9.4.17.1 Status

It displays information, including Group, Switch name, IP address, model, System Up Time, Port in Use, Clients, and Firmware Version of VigorSwitch **connected to** Vigor router.

**Switch Status**



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Status** | Displays the switch which is managed by Viogr router.<br>**Group -** Displays the name link of the group. You can click the link to modify the group settings if required.<br>**Switch Name -** Displays the name link of VigorSwitch. You can click the name link to access into the switch profile.<br>**IP Address -** Displays the IP address of VigorSwitch.<br>**MAC Address -** Displays the MAC address of VigorSwitch.<br>**Model -** Displays the model name of VigorSwitch.<br>**System Up Time -** Displays the time accumulated since this Vigorwitch is powered up.<br>**Port in Use -** Displays how many devices connected to VigorSwitch.<br>**Clients -** Displays the number of LAN ports used in VigorSwitch.<br>**Firmware Version -** Displays the firmware version that VigorSwitch current used. |
| **New Switch List** | The one under New Switch List is allowed to be managed under current used group.<br>**+Add Device** - Make the selected VigorSwitch to be managed by Vigor router and be shown under Status.<br>  <br><br>Select a switch from New Switch List and click +Add Device. Then, the selected switch will be moved and displayed under Status.<br>  <br><br>**Check box -** Click to select the device.<br>**Index -** Displays the index number of Vigor Switch. |

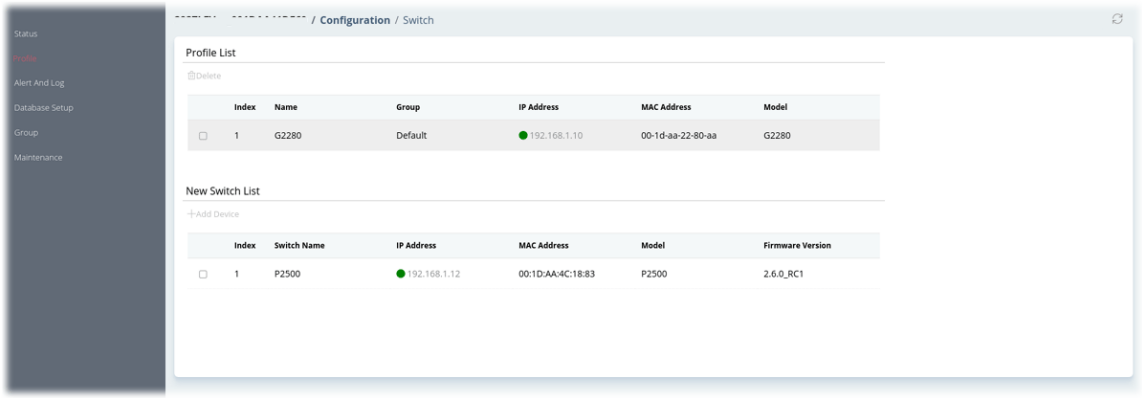
| | |
|---|---|
| | **Switch -** Displays the name of the device.<br>**IP Address -** Displays the IP address of the device.<br>**MAC Address -** Displays the MAC address of the device.<br>**Model** - Displays the model name of VigorSwitch.<br>**Firmware Version** - Displays the firmware version that VigorSwitch current used. |
| **Search** | Click to search Vigor switch. |

**Switch Hierarchy**

This page displays the hierarchy of VigorSwitch(es) managed under Vigor router.

### 9.4.17.2 Profile

This page will show general information, such as name, group, IP address, MAC address, model and password of VigorSwitch only when it connects to Vigor router. By clicking the index number link, a profile setting page for that switch will be shown. Note that each profile represents one VigorSwitch.



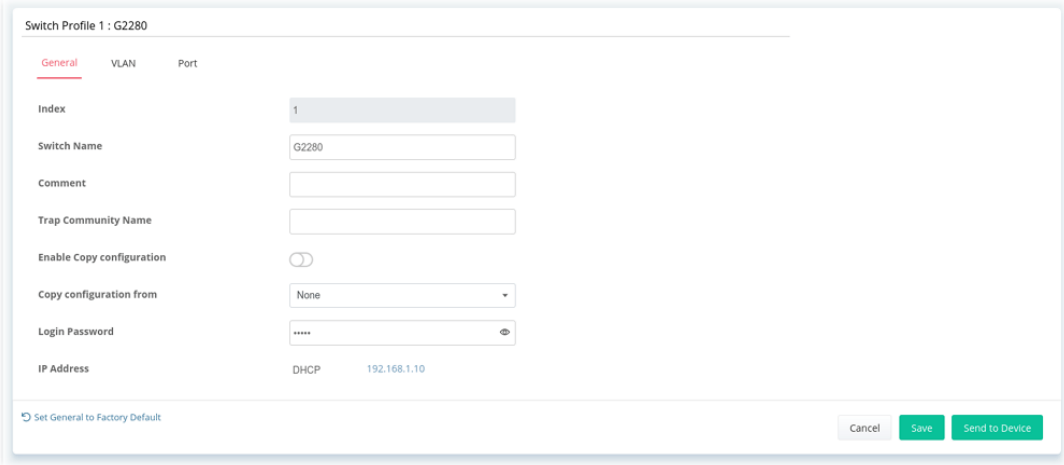

These parameters are explained as follows:

| Item | Description |
|---|---|
| | **Profile List** |
| **Delete** | Click to remove the selected entry from the profile list. |
| **Check box** | Click to select the device. |
| **Index** | Displays the index number of the switch profile. |
| **Name** | Displays the name of the switch profile. |
| **Group** | Displays the group name of VigorSwitch(es). |
| **IP Address** | Displays the IP address of VigorSwitch. |
| **MAC Address** | Displays the MAC address of VigorSwitch. |

| | |
|---|---|
| **Model** | Displays the model name of VigorSwitch. |
| | **New Switch List** |
| **+Add Device** | Make the selected VigorSwitch to be managed by Vigor router and be shown under Profile List. |
| **Index** | Displays the index number of the switch device. |
| **Switch Name** | Displays the name of the switch. |
| **IP Address** | Displays the IP address of VigorSwitch. |
| **MAC Address** | Displays the MAC address of VigorSwitch. |
| **Model** | Displays the model name of VigorSwitch. |
| **Firmware Version** | Displays the firmware version that VigorSwitch current used. |

To edit profile for the selected switch:

1. Selecting one device from the Profile List. Click on the entry to open the following page.



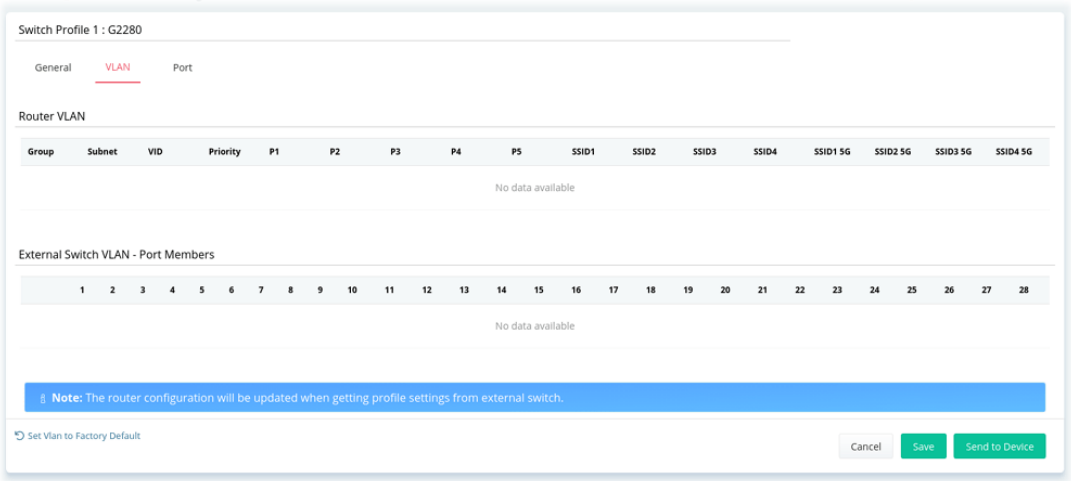

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Index** | Displays the index number of the switch profile. |
| **Switch 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. |
| **Comment** | Enter the text in such field if additional explanation for the switch is required. |
| **Trap Community Name** | Enter the text in such field as trap community. |
| **Enable Copy configuration** | Click to enable or disable the function. |
| **Copy configuration from** | Check the box to copy configuration from other device. Use the drop down list to choose the one you need.<br>Note, if there is only one VigorSwitch connected and managed by Vigor router, then such field is unavailable. |
| **Login Password** | Displays the original login password for the VigorSwitch. |

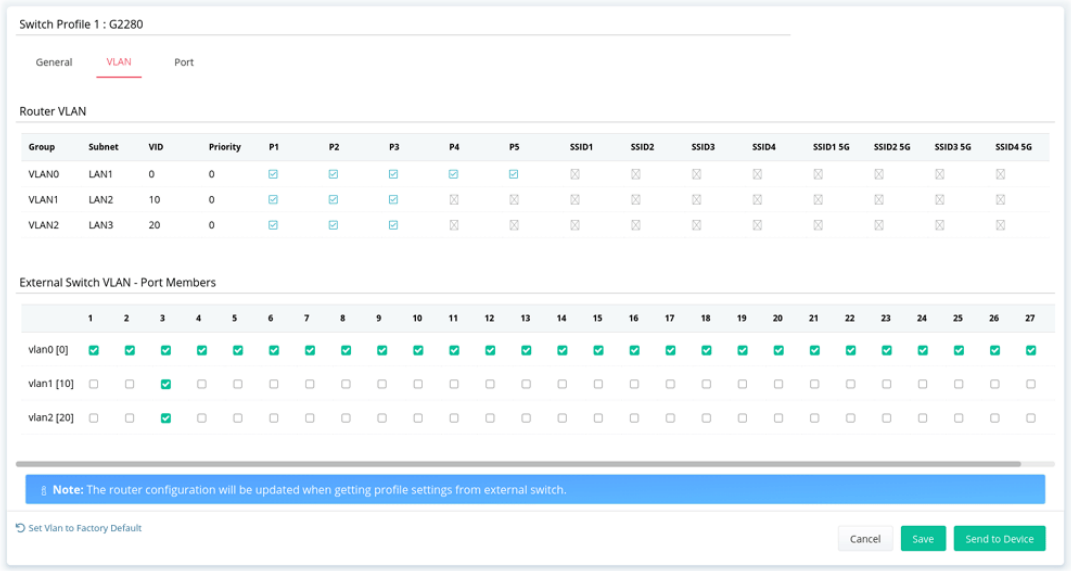
| | |
|---|---|
| **IP Address** | Display the dynamic IP address (of the connected switch) assigned by Vigor router. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings. |
| **Send to Device** | Transfers the configuration change (e.g, login password, switch name, etc.) to the VigorSwitch immediately. |

2. After finished the settings, click **VLAN** tab to open following page.

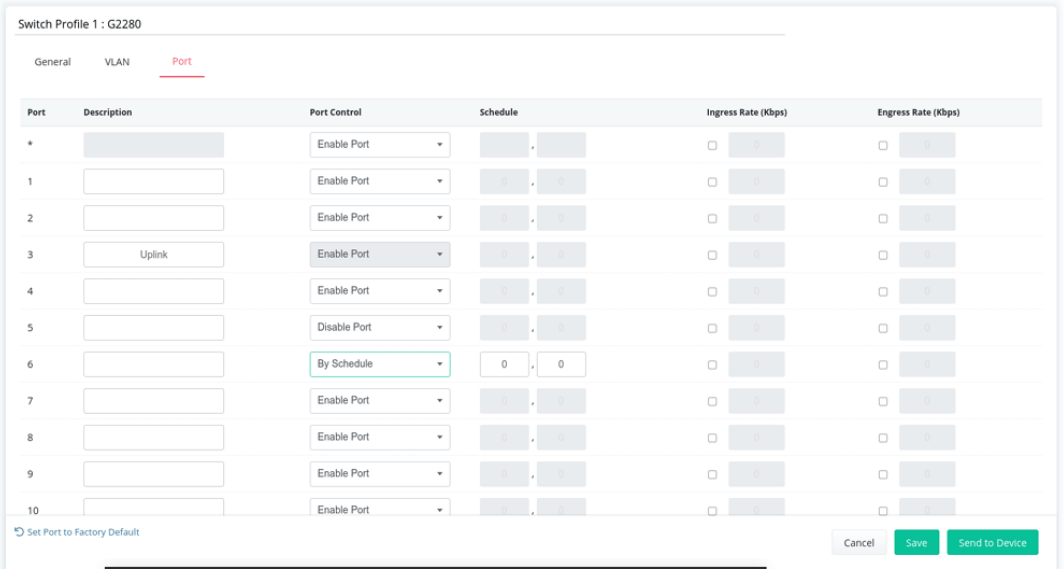
Blank page due to LAN>>VLAN not configured previously:




Setting page with LAN>>VLAN configured previously:



3. Click **Save** to save VLAN configuration. Then, click **Port** tab to access the following page:




These parameters are explained as follows:

| Item | Description |
|---|---|
| **Description** | If required, enter a brief description to explain the device connected to VigorSwitch via the LAN port. |
| **Port Control** | **Disable Port** – The port (e.g., Port 3 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 Save, the network connection between that device and VigorSwitch will be terminated.<br>**By Schedule** – Two schedule profiles can be specified here to force Vigor router executing specific action to VigorSwitch. |
| **Ingress Rate** | Check the box for entering the ingress rate for the selected VigorSwitch. After clicking **Save**, the value modified in this page will be written to VigorSwitch and enabled. |
| **Egress Rate** | Check the box for entering the egress rate for the selected VigorSwitch. After clicking **Save**, the value modified in this page will be written to VigorSwitch and enabled. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings. |
| **Send to Device** | Transfers the configuration change (e.g, login password, switch name, etc.) to the VigorSwitch immediately. |

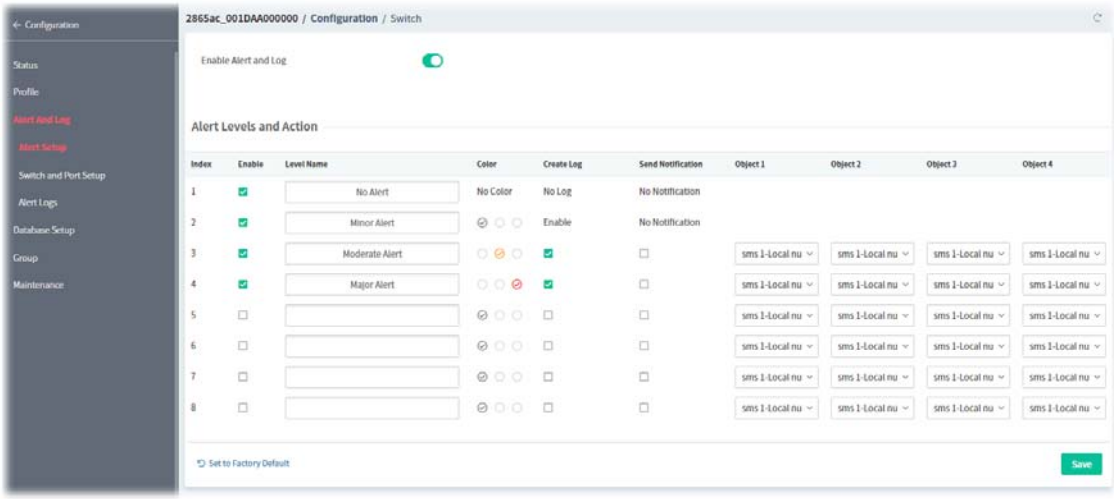
4. Click **Save** to save the changes and then click **Send to Device**. Settings will be sent to VigorSwitch immediately.

### 9.4.17.3 Alert And Log

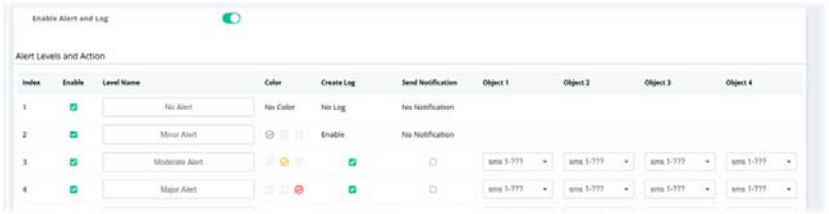
Alert and Log is helpful for the user to understand the abnormal situation occurred in VigorSwitch quickly.

**Alert Setup**

This page is used to define the name of alert, level of alert (in color), and determine to record the data in the database, or send a notification message to the user based on the level.

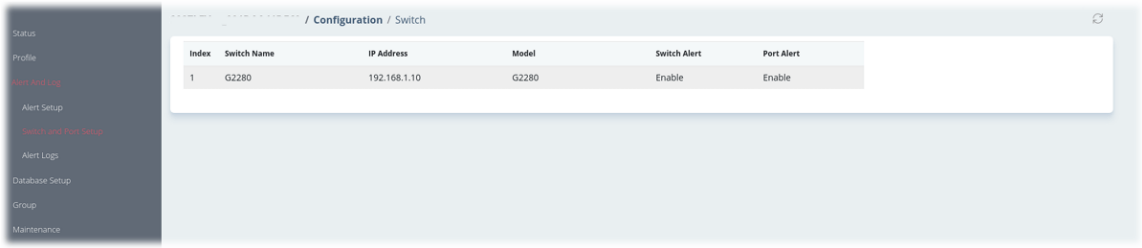



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Enable Alert and Log** | Click to enable or disable the function.<br>  |
| | **Alert Levels and Action** |
| **Index** | Displays the index number of alert profile. |
| **Enable** | Check it to enable this feature. |
| **Level Name** | Define names for representing the severity of alert event. The default names for index 1 to index 4 will be shown on each setting box. Index 5 to index 8 are reserved for user-defined. |
| **Color** | Define the color for each level of alert. However, the color of index 1 is No color and unable to be changed. |
| **Create Log** | Check the box to create log of alert. Such log will be seen on Alert Logs page. Note that No Log for index 1; and log for index 2 is enabled in default. |
| **Send Notification** | If it is checked, Vigor router's system will send notification to specified phone number via SMS. |
| **Object 1 ~ 4** | Select the SMS object which will get the SMS from Vigor router. Up to 4 objects can be selected at one time. |
| **Save** | Save the current settings. |

### Switch and Port Setup

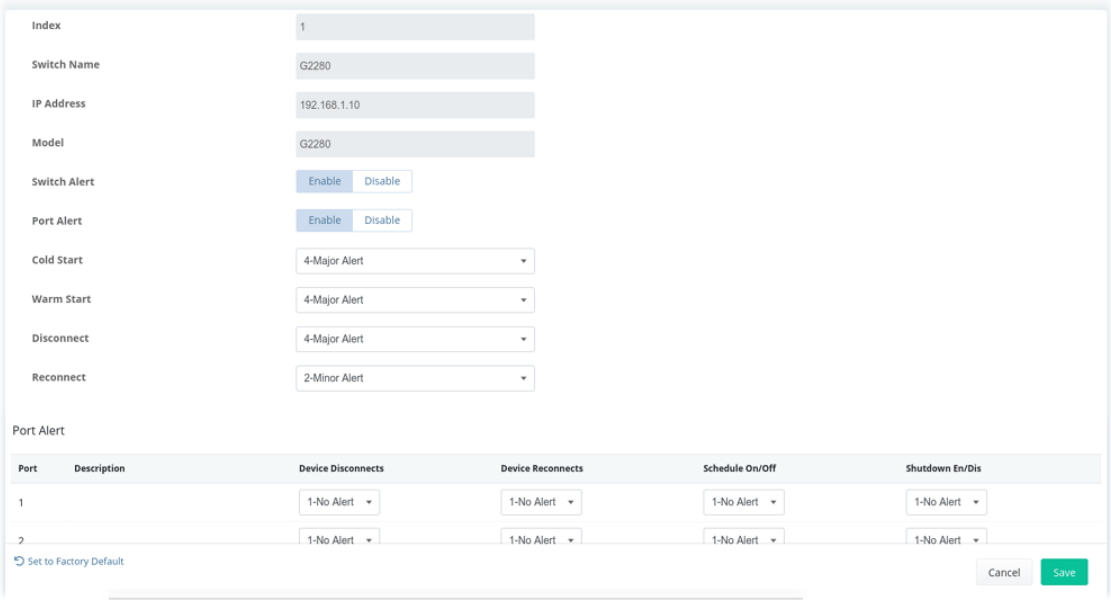
This page defines enabling switch alert and/or port alert for each switch.




These parameters are explained as follows:

| Item | Description |
|---|---|
| **Index** | Displays the index number of the alert profile for switch(es). |
| **Switch Name** | Displays the name of the switch. |
| **IP Address** | Displays the IP address of the switch. |
| **Model** | Displays the model name of the switch. |
| **Switch Alert** | Displays the switch alert status. |
| **Port Alert** | Displays the port alert status. |

To configure the switch alert settings, move the mouse cursor to any entry and click to open the setting page.



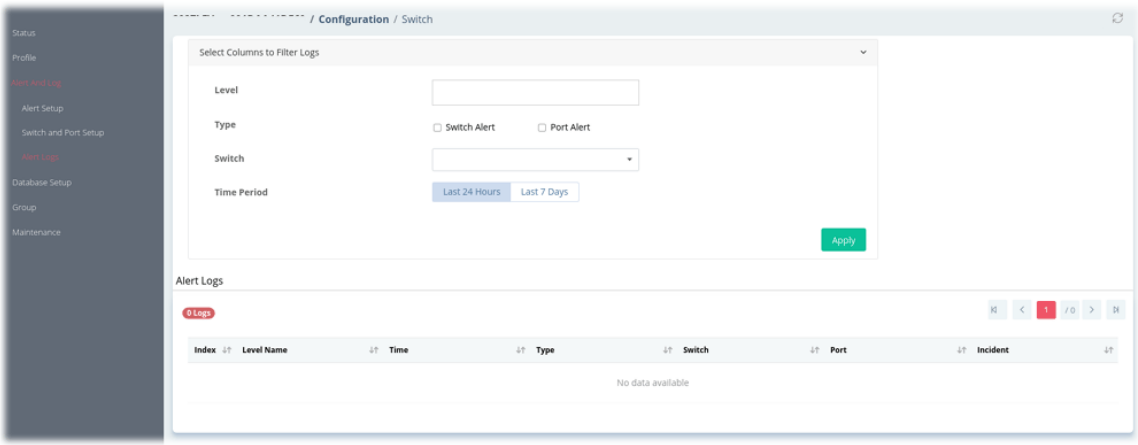

These parameters are explained as follows:

| Item | Description |
|---|---|
| **Index** | Displays the index number of the alert profile for switch(es). |
| **Switch Name** | Displays the name of the switch. |
| **IP Address** | Displays the IP address of the switch. |
| **Model** | Displays the model name of the switch. |
| **Switch Alert** | **Enable** - Click to enable the switch alert function.<br>**Cold Start, Warm Start, Disconnect, Reconnect -** When VigorSwitch encounters the alert events, alert mechanism will perform corresponding actions based on the servity level of the incident encountererd. Specify the severity level (Minor, Major, or No) for each incident. |

| | |
|---|---|
| | **Disable** - Click to disable the switch alert function. |
| **Port Alert** | **Enable** - Click to enable the port alert function.<br>Available Ethernet ports for the selected VigorSwitch (e.g., G2280 in this case) will be shown on this page. Each port can be confgiured with different alert level for diffent alert event.<br>**Disable** - Click to disable the port alert function. |
| **Port Alert table** | **Port –** Available Ethernet ports for the selected VigorSwitch (e.g., G2280 in this case) will be shown on this table. Each port can be confgiured with different **alert level** for different alert event. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

**Alert Logs**

The system administrator can get the information by filtering the collective information based on the conditions specified in this page.

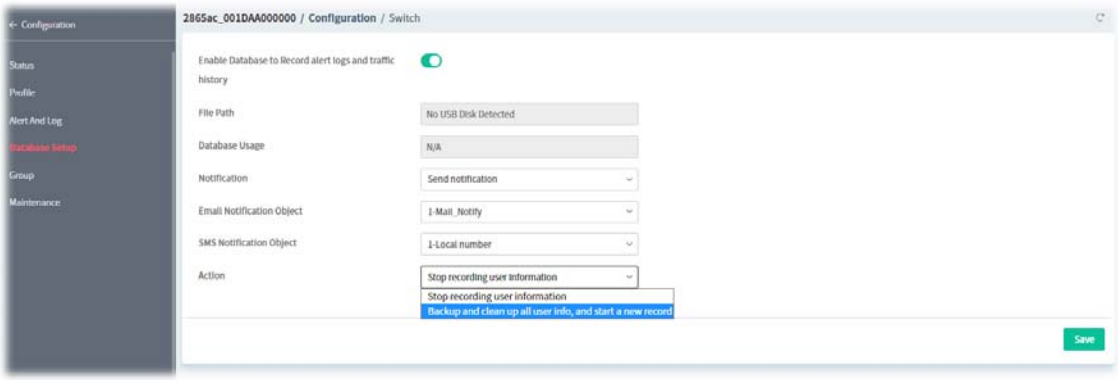



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Select Columns to Filter Logs** | **Level –** The alert can be divided into several levels, Minor Alert, Moderate Alert and Major Alert. Check the one(s) you want to check in Alert Logs list.<br>**Type –** Select the type (switch / port) of the log to be displayed in Alert Logs list.<br>**Switch –** Switch(es) connecting to Vigor router will be shown in this area. Select the one you need.<br>**Time Period** - Select Last 24 Hours or Last 7 Days as time period.<br>**Apply –** Click to save the configuration.<br>Log related to the items selected above will be shown in Alert Logs list. |
| **Alert Logs** | This area displays logs (level name, time, type, switch, port, and incident) related to VigorSwitch managed by Vigor router. |

### 9.4.17.4 Database Setup

The database of the switch can be used to record alert logs and traffic history. This page is used to determine if it is necessary for the user information to be recorded in the database of the switch.

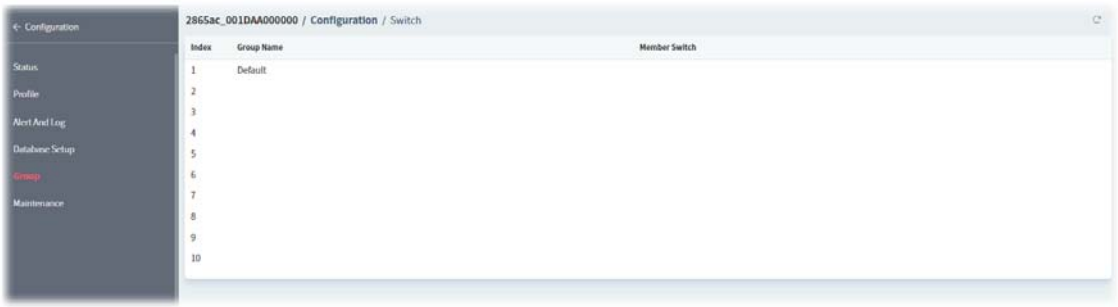



These parameters are explained as follows:

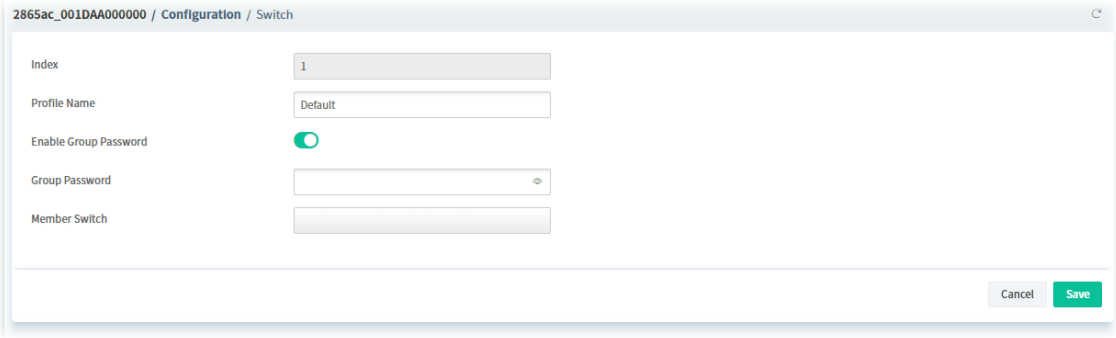
| Item | Description |
|---|---|
| **Enable Database to Record alert logs and traffic history** | Click to enable or disable the function.<br>If enabled, it will make the database (in USB disk) record the alert logs and traffic history. |
| **File Path** | Displays the file path for storing the logs. |
| **Database Usage** | Displays the used capacity. |
| **Notification** | **Send notification -** A notification will be sent out when there is no capacity for storage in USB.<br>● **Email Notification Object -** Choose an email notification object profile.<br>● **SMS Notification Object -** Choose a SMS notification object profile.<br>**Don't send notification -** No notification will be sent out when there is no capacity for storage in USB. |
| **Action** | Choose an action.<br>**Backup and clean up all user info, and start a new record -** Only the newest events will be recorded by the system.<br>**Stop recording user information -** When the capacity of log is full, the system will stop recording. |
| **Save** | Save the current settings. |

### 9.4.17.5 Group

Different switches can be classified into different group(s). There are ten switch groups available for configuration.




To configure the group settings, move the mouse cursor to any entry and click to open the following page.

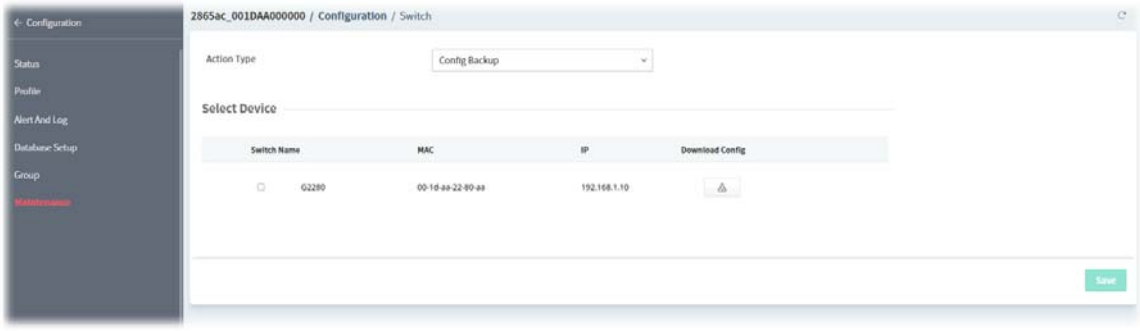



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Index** | Displays the index number of the profile. |
| **Profile Name** | Enter a name as the group name. |
| **Enable Group Password** | Click to enable or disable the group password. |
| **Group Password** | Enter a password that the system administrator can use to access into the managed VigorSwitch connecting to Vigor router. |
| **Member Switch** | Choose the switches you want to group. |
| **Cancel** | Discard current modification and return to previous page. |
| **Save** | Save the current settings and return to previous page. |

### 9.4.17.6 Maintenance

This page is able to execute configuration backup, restore, reboot or reset the VigorSwitch devices remotely.




These parameters are explained as follows:

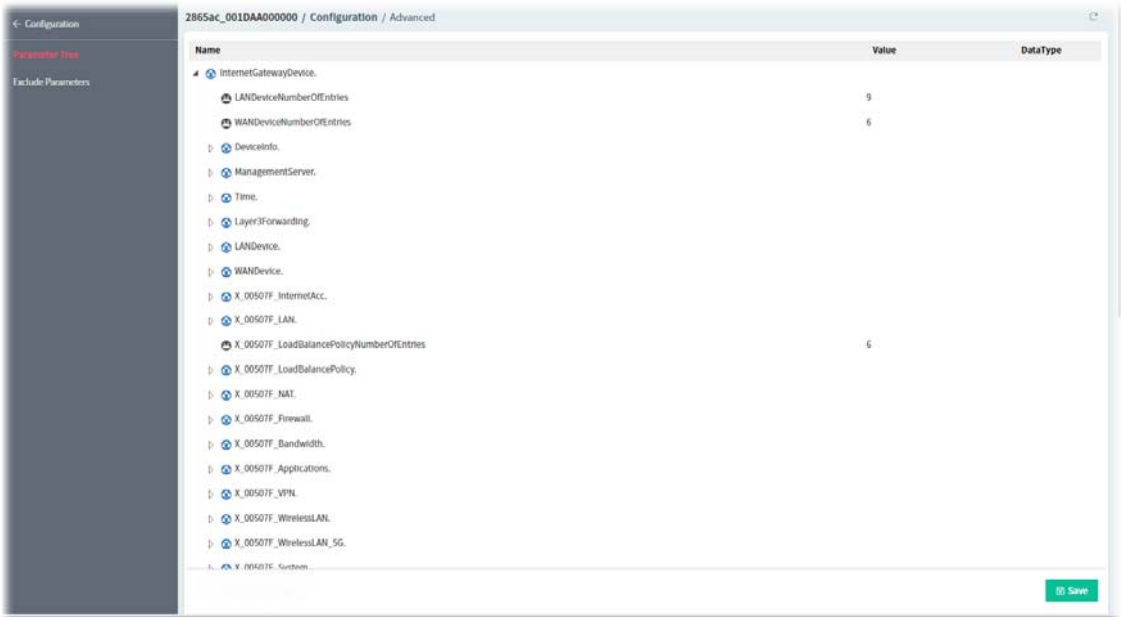
| Item | Description |
|---|---|
| **Action type** | Four actions including configuration backup, configuration restore, remote reboot and factory reset are offered by Vigor router to perform on VigorSwitch.<br>**Config Backup** - Perform the configuration backup.<br>**Config Restore** - Perform the configuration restoration.<br>● **Restore Config From** - Select **Local File** or **Shared Folder.**<br>● **File/Path** - Click **Browse** to locate a file.<br>**Remote Reboot** - Reboot the VigorSwitch devices remotely.<br>**Factory Reset** - Reset the VigorSwitch devices with factory default settings. |

| | Select Device |
|---|---|
| **Switch Name** | Displays the name of the switch. |
| **MAC** | Displays the MAC address of the switch. |
| **IP** | Displays the IP address of the switch. |
| **Download Config** | Click to download the configuration file and store on the host. |
| **Save** | Save the current settings. |

## 9.4.18 Advanced

### 9.4.18.1 Parameter Tree

All control parameters of the selected CPE will be presented on this page with a tree view that is convenient for the administrator/user to view and select.

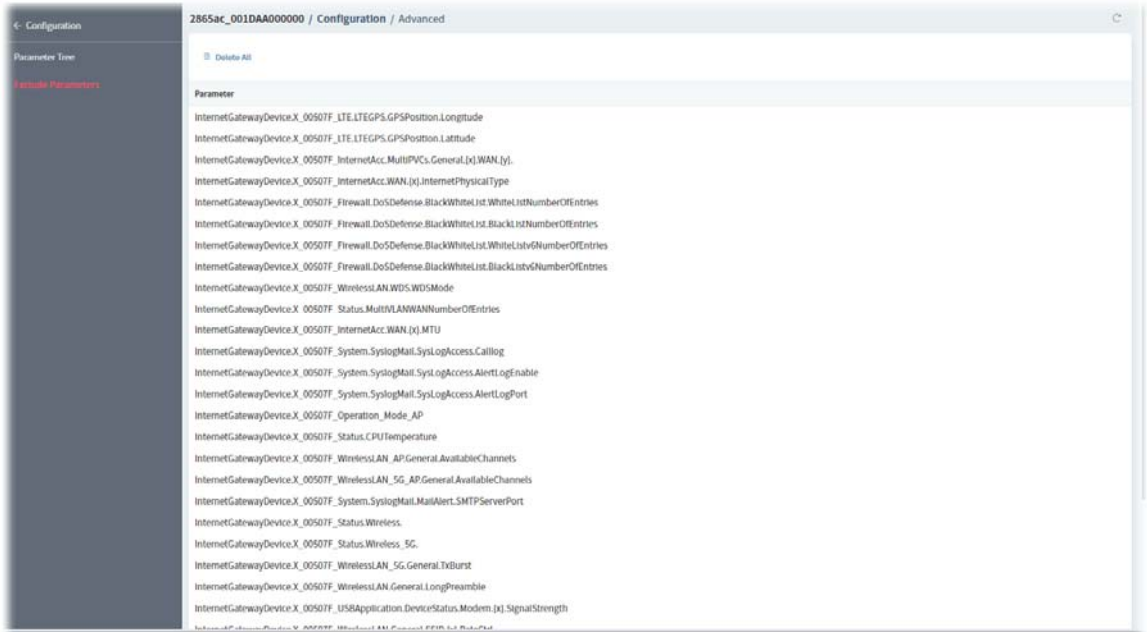



These parameters are explained as follows:

| Item | Description |
|---|---|
| **Name** | Lists the name of the parameter. |
| **Value** | Displays the setting value (true/false, numbers, selections and etc.) of the selected parameter. Sometime, It might be null. |
| **DataType** | It means the data type (e.g., string, boolean or unsignedlnt) of the parameter.<br>However, the corresponding information will be displayed in this field only if the parameter allowed to be written. |
| **Copy** | Copy the selected parameter with the value.<br>The copied parameter can be added onto the XML template downloaded from **Provisioning>>Global Parameters.** After that, the completed XML template can be saved as a sampling profile which will be selected and applied to **Provisioning>>Global Parameters.** |
| **Save** | Save the change. |

### 9.4.18.2 Exclude Parameter

The firmware version of the managed CPE might be different from the data stored on VigorACS database. Therefore VigorACS will compare the available parameters of the selected CPE with the one stored in the VigorACS database automatically. When some of the parameters not supported by the CPE, those parameters will be listed on this page.




These parameters are explained as follows:

| Item | Description |
|---|---|
| **Delete All** | Click to remove all parameters listed in this page. |